МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

# ПРИКЛАДНАЯ ДИСКРЕТНАЯ МАТЕМАТИКА

*Приложение*

**№ 12** **Сентябрь 2019**

Зарегистрирован в Федеральной службе по надзору
в сфере связи и массовых коммуникаций

Свидетельство о регистрации ПИ № ФС 77-50702 от 17 июля 2012 г.

**ТРУДЫ**
**Всероссийской конференции**
**«XVIII Сибирская научная школа-семинар с международным участием**
**“Компьютерная безопасность и криптография” — SIBECRYPT’19»**
**(Томск, 9–14 сентября 2019 г.)**

**УЧРЕДИТЕЛЬ**
**Томский государственный университет**



**Адрес редакции:** 634050, г. Томск, пр. Ленина, 36
**E-mail:** vestnik_pdm@mail.tsu.ru

***Всероссийская конференция* «XVIII *Сибирская научная школа-семинар с международным участием "Компьютерная безопасность и криптография" — SIBECRYPT'19» проведена Национальным исследовательским Томским государственным университетом в сотрудничестве с Институтом криптографии, связи и информатики с 9 по 14 сентября 2019 г. в Томске.***

**Теоретические основы прикладной дискретной математики**
**Дискретные функции**
**Математические методы криптографии**
**Математические основы компьютерной безопасности**
**Прикладная теория автоматов и графов**
**Математические основы информатики и программирования**
**Вычислительные методы в дискретной математике**

Редактор *Н. И. Шидловская*
Верстка *И. А. Панкратовой*

Подписано к печати 15.08.2019. Формат $60 \times 84\frac{1}{8}$. Усл. п. л. 30,4. Тираж 300 экз.
Заказ № 3923. Цена свободная. Дата выхода в свет 27.08.2019.

Отпечатано на оборудовании
Издательского Дома Томского государственного университета
634050, г. Томск, пр. Ленина, 36
Тел.: 8(3822)53-15-28, 52-98-49

# СОДЕРЖАНИЕ

Секция 1

## ТЕОРЕТИЧЕСКИЕ ОСНОВЫ ПРИКЛАДНОЙ ДИСКРЕТНОЙ МАТЕМАТИКИ



Секция 2

## ДИСКРЕТНЫЕ ФУНКЦИИ

Секция 3

## МАТЕМАТИЧЕСКИЕ МЕТОДЫ КРИПТОГРАФИИ

Секция 4

## МАТЕМАТИЧЕСКИЕ ОСНОВЫ КОМПЬЮТЕРНОЙ БЕЗОПАСНОСТИ



Секция 5

## ПРИКЛАДНАЯ ТЕОРИЯ АВТОМАТОВ И ГРАФОВ



Секция 6

## МАТЕМАТИЧЕСКИЕ ОСНОВЫ ИНФОРМАТИКИ И ПРОГРАММИРОВАНИЯ



Секция 7

## ВЫЧИСЛИТЕЛЬНЫЕ МЕТОДЫ В ДИСКРЕТНОЙ МАТЕМАТИКЕ

Секция 1

# ТЕОРЕТИЧЕСКИЕ ОСНОВЫ ПРИКЛАДНОЙ ДИСКРЕТНОЙ МАТЕМАТИКИ

УДК 514.14 DOI 10.17223/2226308X/12/1

## О БЛОКИРОВКЕ ДВУМЕРНЫХ АФФИННЫХ МНОГООБРАЗИЙ

К. Л. Геут, С. С. Титов

Рассмотрена проблема блокировки семейств подмножеств и предложена конструкция расширения блокирующих множеств семейства двумерных аффинных многообразий в пространстве битовых строк при увеличении его размерности. Рассмотрены приложения этой конструкции к решению задачи «A secret sharing» олимпиады NSUCRYPTO не только для чётной, но и для нечётной размерности пространства. Приведены примеры и вычислены мощности дополнений блокирующих множеств этого семейства многообразий для высоких нечётных размерностей.

**Ключевые слова:** *аффинные многообразия, блокирующее множество, NSUCRYPTO.*

При построении отображений конечных полей, обладающих хорошими криптографическими свойствами, в том числе при разделении секрета, построении APN-функций и т. п., естественным образом возникает подзадача блокировки семейств подмножеств, т. е. задача построения блокирующего множества — такого, что в каждом подмножестве блокируемого семейства найдётся элемент этого множества. Эта задача аналогична классической задаче нахождения трансверсали — системы различных представителей. Так, задачу «A secret sharing» олимпиады по криптографии NSUCRYPTO-2015 [1] можно трактовать как задачу блокировки двумерных аффинных многообразий над полем GF(2). Эта задача частично решена [2, 3], а именно: предложена конструкция дополнения $L$ блокирующего множества $M$ для чётной размерности пространства над полем GF(2). В данной работе для полного решения задачи предлагается конструкция дополнения блокирующего множества, пригодная и для нечётных размерностей пространства, на основе построения расширения множества $L$ при увеличении размерности на единицу.

Под задачей блокировки семейства $S$ подмножеств $T$ множества $E$ понимается задача построения такого минимального по включению подмножества $M$, что любое подмножество $T$ из семейства $S$ имеет непустое пересечение с подмножеством $M$. Каждое такое подмножество $M$ называется блокирующим множеством семейства $S$, а подмножество $L = E \setminus M$ — дополнением блокирующего множества. Так, если $E$ — множество точек конечной плоскости, семейство $S$ включает в себя все прямые линии $T$ на этой плоскости, то известная задача блокировки прямых [4, 5] состоит в построении минимального нетривиального множества $M$ точек, такого, что в каждой прямой найдётся хотя бы одна точка из $M$. Таким образом, блокирующее множество на плоскости — это множество точек, пересекающих множество линий. Блокирующее множество называется тривиальным, если оно содержит линию. Семейство прямых в конечной плоско-

сти естественным образом связано с $O(2)$-стойкими шифрами [6, 7], являясь при этом семейством гиперплоскостей однозначно определённого матроида, элементы которого (точки) могут быть интерпретированы как участники некоторой идеальной схемы разделения секрета [8].

В задаче «A secret sharing» $E$ есть множество битовых строк длины $n$, семейство $S$ включает в себя все двумерные аффинные многообразия над $\mathrm{GF}(2)$, т. е. такие четырёхэлементные подмножества $T = \{x_1, x_2, x_3, x_4\}$ множества $E$, что $x_1+x_2+x_3+x_4 = 0$, и требуется предложить конструкцию блокирующего множества $M$ (или, что равносильно, его дополнения $L$). В информационной безопасности, если пользоваться метафорой семейства $S$ множеств как семейства контролируемых пространств или возможных траекторий движения злоумышленника, то элементы блокирующего множества $M$ представляют собой в этой метафоре [9] блок-посты или контролирующие устройства (типа датчиков движения, камер видеонаблюдения и т. п.); так что если эти семейства и множества имеют конкретную математическую (в частности, геометрическую) природу, то можно ставить соответствующие математические задачи блокировки.

Пусть $L = \bar{M}$ даёт решение задачи блокировки двумерных аффинных многообразий в $\mathbb{F}_2^n$. Можно ли включить $L$ в множество $L^+$, дающее решение этой задачи в пространстве $\mathbb{F}_2^{n+1}$?

Если $L^+ = L \cup L'$, $L' \subset \mathbb{F}_2^{n+1} \setminus \mathbb{F}_2^n$, то $L' = \{f + t : t \in T\}$, где $f$ — фиксированный элемент $f \in \mathbb{F}_2^{n+1} \setminus \mathbb{F}_2^n$, $T \subset \mathbb{F}_2^n$. Необходимым и достаточным условием того, что $L^+$ даёт решение, является $|L^+ \oplus L^+ \setminus \{0\}| = \mathrm{C}^2_{l^+}$ (где $l^+ = |L^+|$) при максимальном $L^+$ (по включению) с таким равенством.

**Утверждение 1.** Подмножество $L = \bar{M}$ даёт решение задачи блокировки двумерных аффинных многообразий в $\mathbb{F}_2^n$ тогда и только тогда, когда $L$ — максимальное по включению подмножество, такое, что $|L \oplus L\setminus\{0\}| = \mathrm{C}^2_l$, где $l = |L|$.

Это свойство равносильно тому, что для любых двух различных пар $\{u, v\} \neq \{w, t\}$, $u \neq v$, $w \neq t$, $\{u, v, w, t\} \subset L$, имеем $u \oplus v \neq w \oplus t$.

**Утверждение 2.** Если множество $L = \bar{M}$, дающее решение задачи блокировки двумерных аффинных многообразий в $\mathbb{F}_2^n$, можно включить в множество $L^+$, дающее решение этой задачи в пространстве $\mathbb{F}_2^{n+1}$, то найдётся такое подмножество $T \subset \mathbb{F}_2^n$, что $(L \oplus L) \cap (T \oplus T) = \{0\}$ и $|(T \oplus T) \setminus \{0\}| = \mathrm{C}^2_{|T|}$.

При этом если $T$ — максимальное по включению такое подмножество, то множество $L^+ = L \cup \{f \oplus t : t \in T\} = L \cup (\{f\} \oplus T)$, где $f$ — произвольный элемент в $\mathbb{F}_2^{n+1} \setminus \mathbb{F}_2^n$, даёт решение этой задачи.

**Конструкция.**

Пусть $n = 2m$. Тогда $\mathbb{F}_2^n = \mathbb{F}_2^m \times \mathbb{F}_2^m$, имеется конструкция [3] множества $L$ в виде $L = \{(x, x^3) : x \in \mathrm{GF}(2^m)\}$. Пусть $L^-$ есть дополнение блокирующего множества в $\mathbb{F}_2^m = \mathrm{GF}(2^m)$.

Положим $T = \{(0, t) : t \in L^-\}$ для любого $m$, так что условие инъективности выполняется.

Проверяя условие отсутствия общих ненулевых сумм, видим, что если $(x_1, x_3) + (x_2, x_2^3) = (0, t_1) + (0, t_2)$, то $x_1 + x_2 = 0$, откуда $x_1 = x_2$, и поэтому $x_1^3 + x_2^3 = 0 = t_1 + t_2$, откуда $t_1 = t_2$. Следовательно, $(L \oplus L) \cap (T \oplus T) = \{(0, 0)\}$ и для решения задачи блокировки в $\mathbb{F}_2^{n+1}$ требуется установить только максимальность $T$.

Возьмём без ограничения общности $f = (0, \ldots, 0, 1) \in \mathbb{F}_2^{n+1} \setminus \mathbb{F}_2^n$, так что $L' = \{f + t : t \in L^-\}$ удовлетворяет условию инъективности. Будем представлять эле-

менты из $\mathbb{F}_2^{n+1} = \mathbb{F}_2^{2m+1}$ в виде троек $(x, y, z)$, где $x \in \mathbb{F}_2^m = \mathrm{GF}(2^m)$, $y \in \mathbb{F}_2^m = \mathrm{GF}(2^m)$, $z \in \mathbb{F}_2$. Тогда $L = \{(x, x^3, 0) : x \in \mathrm{GF}(2^m)\}$, $L' = \{(0, t, 1) : t \in L^-\}$ и $L^+ = L \cup L'$ удовлетворяет условию инъективности.

Для проверки условия максимальности возьмём элемент $e = (a, b, c) \in \mathbb{F}_2^{n+1}$.

Если $c = 0$, то либо $e \in L$, либо $e$ представим в виде суммы трёх различных элементов из $L$ по построению. Если же $c = 1$, то при $a = 0$ либо $e \in L'$, либо $e$ представим в виде суммы трёх различных элементов из $L'$ согласно выбору $L^-$, поскольку $1 \oplus 1 \oplus 1 = 1$.

Пусть, наконец, $c = 1$ и $a \neq 0$. Тогда при $b = a^3$ имеем $e = (a, a^3, 0) + (0, 0, 0) + (0, 0, 1)$, где первые два слагаемых принадлежат $L$, а третье — $L'$ (предполагается, без ограничения общности, что $0 \in L^-$). При $b \neq a^3$ положим $b = a^3 + d$. Здесь $a \neq 0$, $d \neq 0$, так что единственный возможный вариант представления $e$ в виде суммы трёх элементов из $L^+$ — взять два слагаемых из $L$ и одно из $L'$. Будем искать представление $e$ в виде

$$e = (a, b, 1) = (x_1, x_1^3, 0) + (x_2, x_2^3, 0) + (0, t, 1). \tag{1}$$

Это даёт систему уравнений $x_1 + x_2 = a$, $x_1^3 + x_2^3 + t = b$. Обозначим $x_1 = x$, тогда $x_2 = x + a$ и последнее уравнение принимает вид $x^3 + (a + x)^3 + t = a^3 + d$. Раскрывая скобки и приводя подобные, получим $ax^2 + a^2x + t = d$. Деля на $a^3 \neq 0$, приходим к уравнению $y^2 + y = (t' + d')$ для $y = x/a$, где обозначено $t' = t/a^3$, $d' = d/a^3$. Как известно [10], решение $y$ существует тогда и только тогда, когда (абсолютный) след правой части равен нулю, т. е. $\mathrm{Tr}(t' + d') = 0$. Итак, наличие представления (1) равносильно возможности подбора для данного $d$ такого $t \in L^-$, что $\mathrm{Tr}(t') = \mathrm{Tr}(d')$. Поскольку областью значений функции следа является двухэлементное поле $\mathbb{F}_2 = \{0, 1\}$, для существования такого $t$ при любом $d$ достаточно, чтобы в $L^-/a^3$ имелись как элементы с нулевым, так и элементы с единичным следом. Докажем две леммы.

**Лемма 1.** Пусть $L$ — дополнение блокирующего множества в $\mathbb{F}_2^k = \mathrm{GF}(2^k)$. Тогда для любого ненулевого $h \in \mathrm{GF}(2^k)$ множество $L^* = hL$ также является дополнением блокирующего множества.

***Доказательство.*** Если $l_i^* \in L^*$ $(i = 1, \ldots, 4)$ различны и $l_1^* + l_2^* + l_3^* + l_4^* = 0$, то $l_i^* = hl_i$, $i = 1, \ldots, 4$, причём $l_1 + l_2 + l_3 + l_4 = 0$ и все $l_i$ тоже различны, что невозможно. Если $m^* \notin L^*$, то $m^* = hm$, где $m \notin L$, так что имеется представление $m$ в виде суммы трёх различных элементов из $L$, т. е. $m = l_1 + l_2 + l_3$, $l_i \in L$ $(i = 1, 2, 3)$. Однако тогда имеется и представление для $m^*$, так как $m^* = hl_1 + hl_2 + hl_3 = l_1^* + l_2^* + l_3^*$, где $l_1^*, l_2^*, l_3^*$ — три различных элемента из $L^*$. ■

**Лемма 2.** Пусть $L$ — дополнение блокирующего множества в $\mathbb{F}_2^k = \mathrm{GF}(2^k)$. Тогда в $L$ есть элемент с нулевым следом и есть элемент с единичным следом.

***Доказательство.*** Пусть, от противного, в $L$ нет ни одного элемента с нулевым следом. Значит, все элементы в $L$ имеют след равный единице. Следовательно, все суммы троек элементов из $L$ имеют след, тоже равный единице, так как $1 \oplus 1 \oplus 1 = 1$, что противоречит представимости элементов дополнения $L$, содержащего элементы и с нулевым следом, в виде сумм троек элементов из $L$. Аналогично — для $L$ без элементов с единичным следом. ■

Применяя эти леммы, получаем при $k = m$ и $h = 1/a^3$

**Утверждение 3.** Для произвольного $L^-$, являющегося дополнением блокирующего множества в $\mathbb{F}_2^m$ (без ограничения общности содержащего нуль), предложенная

конструкция даёт множество $L^+$, являющееся дополнением блокирующего множества в $\mathbb{F}_2^{2m+1}$.

Таким образом, для решения задачи «A secret sharing» предложена конструкция множества, блокирующего двумерные многообразия, не только для чётной, но и для нечётной размерности. Необходимо применить описанную процедуру расширения конечное число раз в зависимости от числа $n$ — размерности пространства. Если $n$ чётно, то имеем конструкцию работы [3]. Если $n = 2k + 1$ и множество $L_k$ известно (например, если $k$ чётно), то применяем процедуру расширения, получив $|L_n| = 2^k + |L_k|$. Если $n = 4k - 1$, то, в случае необходимости, можно применить процедуру ещё один раз, при этом мощность дополнения $L_n$ блокирующего множества равна $|L_n| = 2^{2k} + 2^k$. Так, из того, что $|L_5| = 7$, находим $|L_{11}| = 2^5 + 7 = 39$, а из $|L_3| = 4$ находим $|L_7| = 2^3 + 4 = 12$. Поэтому множества $L_{23}$ и $L_{15}$ находятся «в два действия», т. е. повторным применением описанной процедуры, при этом получается $|L_{23}| = 2^{11} + 2^5 + 7 = 2087$, $|L_{15}| = 2^7 + 2^3 + 4 = 2^7 + 12 = 140$. В три действия находим, например, $|L_{47}| = 2^{23} + |L_{23}| = 8390695$. Очевидно, что для любого $n$ число процедур расширения не превосходит $\log_2 n$, оно достигает максимума $s$ для $n = 2^s - 1$. Например, при $s = 5$ имеем, применяя процедуру четыре раза, $|L_{31}| = 2^{15} + |L_{15}| = 32908$, а при $s = 8$ имеем, применяя процедуру семь раз, $|L_{255}| = 2^{127} + 2^{63} + 2^{31} + 2^{15} + 2^7 + 2^3 + 4$. Этот метод может быть применён и к другим криптографическим задачам [11].

## ЛИТЕРАТУРА


1. Сайт олимпиады NSUCRYPTO. `http://nsucrypto.nsu.ru/`
2. *Tokareva N., Gorodilova A., Agievich S., et al.* Mathematical methods in solutions of the problems from the Third International Students' Olympiad in Cryptography // Прикладная дискретная математика. 2018. № 40. С. 34–58.
3. *Геут К. Л., Кириенко К. А., Садков П. О. и др.* О явных конструкциях для решения задачи "A secret sharing" // Прикладная дискретная математика. Приложение. 2017. № 10. С. 68–70.
4. *Szonyi T.* Blocking sets in desarguesian affine and projective planes // Finite Fields and their Appl. 1997. V. 3. Iss. 3. P. 187–202.
5. *Polverino O.* Linear sets in finite projective spaces // Discrete Mathematics. 2010. V. 310. Iss. 22. P. 3096–3107.
6. *Зубов А. Ю.* Совершенные шифры. М.: Гелиос АРВ, 2003.
7. *Болотова Е. А., Коновалова С. С., Титов С. С.* Свойства решёток разграничения доступа, совершенные шифры и схемы разделения секрета // Проблемы безопасности и противодействия терроризму. Материалы IV Междунар. науч. конф. М.: МЦНМО, 2009. Т. 2. С. 71–86.
8. *Парватов Н. Г.* Совершенные схемы разделения секрета // Прикладная дискретная математика. 2008. № 2(2). С. 50–57.
9. *Башуров В. В., Филимоненкова Т. И.* Математические модели безопасности. Новосибирск: Наука, 2009. 87 с.
10. *Лидл Р., Нидеррайтер Г.* Конечные поля. М.: Книга по Требованию, 2013. Т. 1–2. 812 с.
11. *Городилова А. А.* От криптоанализа щифра к криптографическому свойству булевой функции // Прикладная дискретная математика. 2016. № 3(33). С. 16–44.

УДК 512.742 DOI 10.17223/2226308X/12/2

# О ПОРЯДКЕ ДЕЙСТВИЯ ЭНДОМОРФИЗМА ФРОБЕНИУСА НА ГРУППУ $l$-КРУЧЕНИЯ АБЕЛЕВЫХ ПОВЕРХНОСТЕЙ[1]

Н. С. Колесников, С. А. Новоселов

Исследуется вероятностное распределение порядков действия эндоморфизма Фробениуса на группу $l$-кручения абелевых поверхностей. Получены числовые характеристики соответствующей случайной величины — дисперсия и среднеквадратическое отклонение. Описанные величины могут быть использованы для ускорения нахождения характеристических многочленов Фробениуса по модулю $l$ в обобщении алгоритма Шуфа на абелевы поверхности.

**Ключевые слова:** *абелевы поверхности, гиперэллиптические кривые, подсчёт числа точек, многочлен Фробениуса.*

## Введение

Построение криптосистем на абелевых многообразиях и, в частности, на гиперэллиптических кривых является в настоящее время альтернативой эллиптической криптографии. Они позволяют обеспечить сравнимый уровень криптостойкости при меньшей длине ключа. Сдерживающим фактором в развитии таких криптосистем является трудоёмкость вычислений в якобианах гиперэллиптических кривых. Кроме того, на практике возникает задача подсчёта точек в якобианах, которая на данный момент решена лишь для некоторых частных случаев. Для эллиптических кривых есть эффективный алгоритм Шуфа — Элкиса — Аткина [1]. Для гиперэллиптических кривых рода 2 есть алгоритм Годри — Шоста [2], который является обобщением алгоритма Шуфа. Обобщение оптимизаций Элкиса и Аткина на случай кривых рода 2 и выше является открытой проблемой.

В общем случае для любого абелева многообразия есть теоретический алгоритм подсчёта точек на абелевых многообразиях (обобщение алгоритма Шуфа) [3]. В его основе лежит поиск характеристического многочлена эндоморфизма Фробениуса $\chi_l$, действующего на группу $l$-кручения. При этом $\chi_l$ находится простым перебором коэффициентов.

Одна из оптимизаций Аткина, в случае эллиптических кривых, заключается в нахождении порядка действия Фробениуса на группу $l$-кручения и его использование для ускорения перебора $\chi_l$. При этом сам порядок вычисляется из разложения модулярных многочленов.

Для гиперэллиптических кривых рода 2 модулярные многочлены имеют большой размер, что делает их малопригодными для практических вычислений. Поэтому мы изучаем вероятностный подход для нахождения порядка действия Фробениуса.

В [4] представлена идея улучшения алгоритма за счёт оценки вероятностного распределения порядка действия эндоморфизма Фробениуса. В настоящей работе получены дополнительные характеристики распределения порядков матриц, соответствующих действию эндоморфизма Фробениуса на группу $l$-кручения. Вычислены дисперсия распределения и среднеквадратическое отклонение.

[1]Исследование выполнено при финансовой поддержке РФФИ, проект № 18-31-00244.

## 1. Распределение порядков действия эндоморфизма Фробениуса

Пусть $A$ — абелева поверхность над конечным полем $\mathbb{F}_q$ нечётной характеристики $p$. Будем рассматривать действие эндоморфизма Фробениуса на группу $l$-кручения $A[l]$, где $l$ — простое число, такое, что $q \equiv 1 \mod l$. В этом случае действие эндоморфизма Фробениуса на группу $l$-кручения как линейного оператора может быть представлено симплектической матрицей $F_l \in PSp_{2g}(\mathbb{F}_l)$, где $g = 2$ — размерность абелева многообразия.

Введём случайную величину $\xi$, которая принимает значения порядков $r = \mathrm{Ord}(F_l)$ симплектических матриц как элементов группы $PSp_4(\mathbb{F}_l)$. Отношение подобия разбивает симплектическую группу на классы эквивалентности $[A_i]$, в каждом из которых встречаются матрицы одного порядка $r_i = \mathrm{Ord}(A_i)$. Эти порядки вычислены для каждого класса в [4]. Там же приводится формула для вычисления математического ожидания $\mathrm{M}(\xi)$. Определим числовые характеристики этой случайной величины:

$$\mathsf{P}(\xi = r_k) = \frac{\#\{A \in PSp_4(\mathbb{F}_l) : \mathrm{Ord}(A) = r_k\}}{\#PSp_4(\mathbb{F}_l)} = \frac{\#[A_{i_1}] + \ldots + \#[A_{i_s}]}{\#PSp_4(\mathbb{F}_l)},$$

где $A_{i_1}, \ldots, A_{i_s}$ — представители всех классов, таких, что $\mathrm{Ord}(A_{i_1}) = \ldots = \mathrm{Ord}(A_{i_s}) = r_k$. Из [4] имеем

$$\mathrm{M}(\xi) = \sum_{i=1}^{k} r_k \frac{\#[A_{i_1}] + \ldots + \#[A_{i_s}]}{\#PSp_4(\mathbb{F}_l)} = \sum_{i=1}^{n} \mathrm{Ord}(A_i) \frac{\#[A_{i_1}]}{\#PSp_4(\mathbb{F}_l)} \approx$$
$$\approx \frac{\pi^2}{48} \frac{2l^5 + 16l^4 - 48l^3 + 65l - 37}{l(l^2-1)} \frac{1}{\log(l)}.$$

Последнее выражение получено при помощи аппроксимации функции НОД из работы [5].

**Теорема 1.** Пусть $A$ — абелева поверхность над конечным полем $\mathbb{F}_q$ характеристики $p$ и $l \neq p$ — простое число, такое, что $q \equiv 1 \mod l$. Тогда при $q \gg l$ дисперсия распределения порядков действия эндоморфизма Фробениуса на $A[l]$ и его среднеквадратическое отклонение могут быть вычислены по следующим формулам:

$$D(\xi) \approx \left(\frac{\pi^2}{48}\right)^2 \frac{\psi(l)}{l^2(l^2-1)^2} \frac{1}{\log^2(l)}, \quad \sigma(\xi) = \sqrt{D(\xi)} \approx \frac{\pi^2}{48} \frac{\sqrt{\psi(l)}}{l(l^2-1)} \frac{1}{\log(l)},$$

где

$$\psi(l) = 2l^{10} + 56l^9 - 316l^8 + 1344l^7 - 1948l^6 - 1770l^5 + 6660l^4 - 3516l^3 - 3831l^2 + 4684l - 1369.$$

ЛИТЕРАТУРА


1. *Schoof R.* Counting points on elliptic curves over finite fields // J. Theor. Nombres Bordeaux. 1995. V. 7. No. 1. P. 219–254.
2. *Gaudry P. and Schost É.* Genus 2 point counting over prime fields // J. Symb. Comput. 2012. V. 47. No. 4. P. 368–400.
3. *Pila J.* Frobenius maps of abelian varieties and finding roots of unity in finite fields // Mathematics of Computation. 1990. V. 55. No. 192. P. 745–763.
4. *Novoselov S. A. and Kolesnikov N. S.* On expected order of Frobenius action on $l$-torsion of abelian surfaces // Submitted at NuTMiC. 2019.
5. *Diaconis P. and Erdös P.* On the distribution of the greatest common divisor // Lecture Notes — Monograph Series. Institute of Mathematical Statistics. 2004. V. 45. P. 56–61.

УДК 512.772.7 DOI 10.17223/2226308X/12/3

# ВЫЧИСЛЕНИЕ ИДЕАЛА 3-КРУЧЕНИЯ ДЛЯ НЕКОТОРОГО КЛАССА ГИПЕРЭЛЛИПТИЧЕСКИХ КРИВЫХ

Е. С. Малыгина

Рассмотрены гиперэллиптические кривые рода 2, определяемые многочленом Диксона. Для таких кривых представлено вычисление идеала 3-кручения, в частности получены его четыре образующие с использованием представления Мамфорда — Кантора для дивизора 3-кручения и теории $\theta$- и $\wp$-функций.

**Ключевые слова:** *гиперэллиптическая кривая, многочлен Диксона, идеал $l$-кручения, дивизор $l$-кручения, модулярное уравнение.*

## Введение

Модулярные уравнения, связывающие инварианты $l$-изогенных эллиптических кривых, являются фундаментальным инструментом в арифметической геометрии. Одним из важных приложений модулярных уравнений является вычисление порядка точек эллиптической кривой над конечным полем. Наилучшим методом является алгоритм Шуфа — Элкиса — Аткина [1], в котором широко используются точки $l$-кручения. На сегодняшний день такие уравнения могут быть эффективно вычислены даже для больших значений $l$.

Однако для кривых рода $g \geqslant 2$ информации о вычислении модулярных уравнений крайне мало. Будем рассматривать гиперэллиптические кривые рода 2, определяемые многочленом Диксона [2], и для них представим формулы для вычисления идеала $l$-кручения в случае $l = 3$. Следует отметить, что идеал $l$-кручения является главной составляющей при вычислении модулярного уравнения.

В свою очередь, модулярное уравнение можно использовать для исследования изогений абелевых многообразий, что является важным инструментом не только для изучения абелевых многообразий, но и для криптографических приложений, основанных на изогениях.

Использование специального класса гиперэллиптических кривых на основе многочленов Диксона обусловлено рядом причин. Во-первых, якобиан кривой с уравнением $C : y^2 = x^{2g+1} + ax^{g+1} + bx$ допускает разложение [3]

$$\mathrm{Jac}_{\mathbb{F}_q[\sqrt[g]{b}]}(C) \sim \mathrm{Jac}_{\mathbb{F}_q[\sqrt[g]{b}]}(C_1) \times \mathrm{Jac}_{\mathbb{F}_q[\sqrt[g]{b}]}(C_2)$$

в случае, если $g(C)$ нечётно, и

$$\mathrm{Jac}_{\mathbb{F}_q[\sqrt[g]{b}]}(C) \sim \mathrm{Jac}_{\mathbb{F}_q[\sqrt[g]{b}]}(\mathbb{F}_q[\sqrt[g]{b}]) \times \mathrm{Jac}_{\mathbb{F}_q[\sqrt[g]{b}]}(\tilde{C}_3),$$

если $g(C)$ чётно. При этом кривые $C_1, C_2, C_3, \tilde{C}_3$ определены многочленами Диксона $D_g(x, \alpha)$. Во-вторых, в [4] мы получили явные формулы для многочленов деления и, как следствие, представление Мамфорда — Кантора для дивизоров 3-кручения. Вычисление точек в якобиане исходной кривой $C$, таким образом, может быть сведено к более лёгкой задаче, а именно к вычислению числа точек в якобианах соответствующих кривых $C_1, C_2$ и $C_3, \tilde{C}_3$.

## 1. Модулярное уравнение

Пусть гиперэллиптическая кривая $C/\mathbb{F}_q$ рода $g(C) = 2$ определена уравнением

$$C : Y^2 = f(X) = \sum_{i=0}^{2g+1} f_i X^i = X^5 + f_4 X^4 + f_3 X^3 + f_2 X^2 + f_1 X + f_0.$$

Обозначим $\mathrm{Jac}_{\mathbb{F}_q}(C)[l]$ подгруппу $l$-кручения элементов якобиана $\mathrm{Jac}_{\mathbb{F}_q}(C)$ кривой $C$, где $l$ — простое число и $l \neq \mathrm{char}(\mathbb{F}_q)$.

Далее пусть $l = 3$ и $D \in \mathrm{Jac}_{\mathbb{F}_q}(C)[3]$ — дивизор 3-кручения веса 2, то есть

$$D = [3](P_1 - \infty) + [3](P_2 - \infty),$$

где $P_1 = (x_1, y_1)$ и $P_2 = (x_2, y_2)$ — точки кривой $C$. Данный дивизор можно записать с помощью представления Мамфорда — Кантора, вычислив прежде многочлены деления:

$$D = (u(X), v(X)) = (X^2 + u_1 X + u_0, v_1 X + v_0).$$

Тогда существует радикальный идеал $I_3 \subset \mathbb{F}_p[x_1, x_2, y_1, y_2]$, такой, что

$$D \in \mathrm{Jac}_{\mathbb{F}_q}(C)[3] \Leftrightarrow f(x_1, x_2, y_1, y_2) = 0,\ \forall f \in I_3.$$

По аналогии с эллиптическими многочленами деления идеал $I_3$ называется 3-идеалом деления или идеалом 3-кручения. Согласно гипотезе Манина — Мамфорда [5], все ненулевые дивизоры 3-кручения имеют вес 2, следовательно, степень идеала $I_3$ равна $3^4 - 1$.

Определим $t_3(D) = u_1(D)$, где $u_1(D)$ соответствует коэффициенту $u_1$ в представлении Мамфорда — Кантора дивизора $D$. Необходимо вычислить значение $t_3(D)$ по модулю $I_3$. Положим $h_{1,3} \in \mathbb{F}_p[x_1, x_2, y_1, y_2]$ — многочлен, принимающий значение $u_1(D)$ на дивизоре 3-кручения $D$. Чтобы получить $h_{1,3}$, необходимо вычислить координаты Мамфорда — Кантора для дивизора $(P_1 - \infty) + (P_2 - \infty)$. Тогда $\chi_3 = \prod_{D \in \mathrm{Jac}_{\mathbb{F}_q}(C)[3] \setminus \{0\}} (T - t_3(D))$ является характеристическим многочленом $h_{1,3} \bmod I_3$. Зная $\chi_3$, можно вывести модулярное уравнение $\Phi_3$, где $\chi_3 = \Phi_3^2$ и $\deg \Phi_3 = (3^4 - 1)/2$.

## 2. Идеал 3-кручения

Напомним, что

$$\forall f \in I_3\ \big([3](P_1 - \infty) = -[3](P_2 - \infty) \Leftrightarrow D \in \mathrm{Jac}_{\mathbb{F}_q}(C)[3] \Leftrightarrow f(x_1, x_2, y_1, y_2) = 0\big)$$

и

$$D = (u(X), v(X)) = (X^2 + u_1 X + u_0, v_1 X + v_0).$$

Идеал 3-кручения $I_3$ является идеалом в кольце $\mathbb{F}_q[x_1, x_2, y_1, y_2]$ с алгебраическим множеством $V(I_3) = (\mathrm{Jac}_{\mathbb{F}_q}(C) - \Theta)[3] = (\mathrm{Jac}_{\mathbb{F}_q}(C) - \Theta) \cap \mathrm{Jac}_{\mathbb{F}_q}(C)[3]$. Здесь $\Theta$ является дополнением к образу $\sigma(Z)$ в $\mathrm{Jac}_{\mathbb{F}_q}(C)$ при отображении $\sigma : C^2 \to \mathrm{Jac}_{\mathbb{F}_q}(C)$ и $Z \subset C^2$, то есть $\Theta = \{[P - \infty]\}$, где $P$ — точка кривой $C$.

Согласно [6], идеал 3-кручения определён следующим образом:

$$I_3 = (F_1(\wp(z), \wp'(z), \wp''(z), \wp'''(z)), F_2(\wp(z), \wp'(z), \wp''(z), \wp'''(z)), F_3(\wp(z), \wp'(z), \wp''(z), \wp'''(z)),$$
$$F_4(\wp(z), \wp'(z), \wp''(z), \wp'''(z))).$$

Здесь $\wp$ является $\wp$-функцией Вейерштрасса для гиперэллиптического случая, то есть

$$\wp(z) = -4D_\infty^2(\log\theta[\delta](z)),$$

где $\delta = \begin{bmatrix} a \\ b \end{bmatrix} \in \frac{1}{2}\mathbb{Z}^2$ и

$$\theta[\delta](z) = \theta[\delta](z, \tau) = \sum_{m \in \mathbb{Z}^2} \exp(\pi i (m + a)^t \tau (m + a) + 2\pi i (m + a)^t (z + b))$$

является классической $\theta$-функцией с характеристикой $\delta$. Для вычисления идеала $I_3$ нам понадобится следующая

**Теорема 1** [6]. Морфизм

$$\varphi : \begin{cases} \mathrm{Jac}_k(C) - \Theta \to \mathbb{C}^{2g}, \\ z \mapsto (\wp(z), \wp'(z), \ldots, \wp^{(2g-1)}(z)) \end{cases}$$

есть вложение, такое, что $\wp^{(i)}(z)$ для $i \in \{0, \ldots, 2g-1\}$ порождают аффинное кольцо в $\mathrm{Jac}_{\mathbb{F}_q}(C) - \Theta$. С помощью уравнения кривой $C : Y^2 = f(X)$ величины $\wp^{(i)}(z)$ выражаются через универсальный многочлен с коэффициентами, зависящими от $u(t), v(t), w(t)$ модели

$$\mathrm{Jac}_{\mathbb{F}_q}(C) - \Theta = \{(u(t), v(t), w(t)) : f(t) - v^2(t) = u(t)w(t), \deg u = g, \deg v \leqslant g-1, \deg w = g+1\}.$$

Коэффициенты многочленов $u(t), v(t), w(t)$ выражаются также с помощью универсального многочлена от переменных $\wp^{(i)}(z)$.

Принимая во внимание, что мы работаем с дивизором 3-кручения, являющимся представителем класса $[D] \in (\mathrm{Jac}_{\mathbb{F}_q}(C) - \Theta)[3]$, и что представление Мамфорда — Кантора для дивизоров $[3](P_1 - \infty)$ и $[3](P_1 - \infty)$, сумма которых есть дивизор $D = (X^2 + u_1 X + u_0, v_1 X + v_0)$, задано явно в [4], введём следующие обозначения:

$$X_1 = -u_1(x_1, x_2, y_1, y_2) + \frac{1}{2} f_1, \quad X_2 = -v_1(x_1, x_2, y_1, y_2),$$
$$X_3 = -\frac{1}{2} f_2 + f_1 \cdot u_1(x_1, x_2, y_1, y_2) - \frac{3}{2} u_1^2(x_1, x_2, y_1, y_2),$$
$$X_4 = f_1 \cdot v_1(x_1, x_2, y_1, y_2) - 3v_1(x_1, x_2, y_1, y_2) u_1(x_1, x_2, y_1, y_2).$$

Для гиперэллиптической кривой $C/\mathbb{F}_p$ рода $g = 2$ с уравнением

$$Y^2 = (X-2)(D_4(X) + c) = X^5 - 2X^4 - 4\alpha X^3 + 8\alpha X^2 + (2\alpha^2 + c)X - 4\alpha^2 - 2c,$$

где $D_4(X) = X^4 - 4\alpha X^2 + 2\alpha^2$ — многочлен Диксона, положим $\alpha = 1$, тогда окончательно уравнение кривой примет вид

$$Y^2 = X^5 - 2X^4 - 4X^3 + 8X^2 + (c+2)X + (-2c-4).$$

Формулы для первых двух образующих $F_1$ и $F_2$ идеала 3-кручения:

$$F_1(X_1, X_2, X_3, X_4) = -2 - c + 8u_1 + 4u_1^2 + 8v_1^2 - 2u_1^3 - u_1^4 + 11v_1^2 \cdot u_1,$$

$$F_2(X_1, X_2, X_3, X_4) := 2c - \frac{6488065}{294912} u_1 - \frac{25362425}{1179648} u_1^2 + 20v_1^2 + \frac{32440325}{589824} u_1^3 + 44v_1^2 \cdot u_1 + \\ + \frac{23789569}{393216} u_1^4 + 33v_1^2 \cdot u_1^2 + 15u_1^5 - \frac{589825}{294912}.$$

Формула для $F_3$ слишком объёмная и связана с вычислением $\theta$-констант, поэтому упростим её представление следующим образом:

$$F_3(X_1, X_2, X_3, X_4) = \frac{1}{d}(3X_2^3 + X_3X_4 - X_2X_5)((X_1 - \tilde{F}_1)^3 + 2(X_2^2 - \tilde{F}_2{}^2) + 2(\tilde{F}_1 - X_1)(\tilde{F}_3 + X_3)),$$

где

$$X_5 = -8 + 22u_1^2(x_1, x_2, y_1, y_2) + 10u_1^3(x_1, x_2, y_1, y_2) + \frac{5}{2} v_1^2(x_1, x_2, y_1, y_2);$$

$$\tilde{F}_1 = d\,\frac{-27X_2^4X_3^2+27X_2^5X_4+18X_2X_3^3X_4-9X_2^2X_3X_4^2-X_4^4-18X_2^2X_3^2X_5-3X_2^3X_4X_5+}{+2X_3X_4^2X_5-2X_2X_4X_5^2}{(3X_2^3+X_3X_4-X_2X_5)^2};$$

$$\tilde{F}_2 = -\frac{1}{2}\,\frac{4X_2X_3X_4X_5^3-60X_2^3X_3X_4X_5^2+45X_2^2X_3^2X_4^2X_5+54X_2^2X_3^2X_4X_5+243X_2^5X_3X_4X_5+}{+36X_2X_3^4X_4X_5+324X_2^6X_3^3-81X_2^8X_5+54X_2^6X_5^2-18X_3^5X_4^2+27X_2^5X_4^3-3X_2^4X_5^3-}$$
$$\underline{-2X_2^2X_5^4+54X_2^3X_3^4X_4-54X_2^4X_3^3X_5-243X_2^7X_3X_4-27X_2^4X_3^2X_4^2-162X_2^4X_3^2X_4-}$$
$$\underline{-54X_2X_3^3X_4^2-18X_2^2X_3^3X_5^2+18X_2X_3^3X_4^3+9X_2^2X_3X_4^4-3X_2^3X_4^3X_5+2X_3X_4^4X_5-}$$
$$\underline{-2X_2X_4^3X_5^2-2X_3^2X_4^2X_5^2-486dX_2^6X_3^3+54dX_2^5X_4^3-2dX_4^6-216dX_2^4X_3^2X_4^2+}$$
$$\underline{+486dX_2^7X_3X_4+324dX_2^3X_3^4X_4+36dX_2X_3^3X_4^3-36dX_2^2X_3X_4^4-324dX_2^4X_3^3X_5-}$$
$$\underline{-6dX_2^3X_4^3X_5+4dX_3X_4^4X_5-4dX_2X_4^3X_5^2-54dX_2^5X_3X_4X_5-36dX_2^3X_3X_4X_5^2}{(3X_2^3+X_3X_4-X_2X_5)^3};$$

$$\tilde{F}_3 = -\frac{1}{4}\,\frac{972X_2^{10}X_3X_5-2754X_2^6X_3^3X_4^2-1512X_2^3X_4^3X_4^3+8X_2X_4^5X_5^2-1944X_2^7X_3^2X_5^2+}{+1620X_2^8X_4^2X_5-801X_2^6X_4^2X_5^2+2916X_2^9X_3^2X_5+972X_2^4X_3^4X_5^2+27X_2^4X_3^2X_4^4-}$$
$$\underline{-648X_2^4X_3^3X_4X_5^2+180X_2X_3^4X_4^3X_5+1512X_2^5X_3^2X_4X_5^2+648X_2^4X_3^3X_4^2X_5-}$$
$$\underline{-6156X_2^7X_3^2X_4X_5-1944X_2^3X_3^5X_4X_5+1944X_2^6X_3^3X_4X_5+324X_2^3X_3^4X_4^2X_5+}$$
$$\underline{+5832X_2^9X_3^2X_4+324X_2^5X_3^2X_5^3-486X_2^5X_3X_4^3X_5+972X_2^2X_3^6X_4^2-8748X_2^8X_3^4-}$$
$$\underline{-729X_2^{10}X_4^2+18X_3^5X_4^4-54X_3^5X_4^3-108X_2^5X_4^5+6dX_4^8+144dX_2^2X_3X_4^6+}$$
$$\underline{+162X_2^8X_3X_5^2-657X_2^6X_3X_5^3+5346X_2^6X_3^3X_4+1620X_2^3X_3^4X_4^2-972X_2^7X_3X_4^2+}$$
$$\underline{+108X_2X_3^3X_4^4-486X_2^7X_3^2X_5+324X_2^5X_3^2X_5^2-54X_2^3X_3^2X_5^3-18X_2X_3^3X_4^5+}$$
$$\underline{+78X_2^4X_4^2X_5^3+168X_2^4X_3X_5^4+12X_3^2X_4^4X_5^2+12X_2^2X_4^2X_5^4-X_3^3X_4^2X_5^3-X_2^2X_3X_5^5-}$$
$$\underline{-36X_2^2X_3X_4^6+12X_2^3X_4^5X_5-252X_2^2X_3^3X_4^2X_5^2-1944X_2^4X_3^3X_4X_5+54X_2X_3^4X_4^2X_5+}$$
$$\underline{+54X_2^2X_3^3X_4X_5^2+648X_2^5X_3X_4^2X_5-108X_2^3X_3X_4^2X_5^2-114X_2^3X_3^2X_4X_5^3-}$$
$$\underline{-270X_2^2X_3^2X_4^4X_5+210X_2^3X_3X_4^3X_5^2-24X_2X_3X_4^3X_5^3+2X_2X_3^2X_4X_5^4+7776dX_2^6X_3^3X_4^2-}$$
$$\underline{-1944dX_2^3X_3^4X_4^3+16dX_2X_4^5X_5^2-2916dX_2^7X_3X_4^3+1350dX_2^4X_3^2X_4^4-11664dX_2^9X_3^2X_4-}$$
$$\underline{-7776dX_2^5X_3^5X_4+7776dX_2^6X_3^4X_5-144dX_2X_3^3X_4^5-8X_3X_4^6X_5+1080dX_2^5X_3^2X_4X_5^2+}$$

$$\underline{+10206dX_2^8X_3^4 - 216dX_2^5X_4^5 + 864dX_2^4X_3^3X_4^2X_5 - 648dX_2^7X_3^2X_4X_5 + 540dX_2^5X_3X_4^3X_5+}$$

$$\underline{+24dX_2^3X_4^5X_5 - 16dX_3X_4^6X_5 - 324dX_2^8X_4^2X_5 - 198dX_2^6X_4^2X_5^2 + 648dX_2^4X_3^4X_5^2+}$$

$$\underline{+648dX_2^2X_3^6X_4^2 + 24dX_2^4X_4^2X_5^3 + 8dX_3^2X_4^4X_5^2 + 8dX_2^2X_4^2X_5^4 - 72dX_2^2X_3^2X_4^4X_5+}$$

$$\underline{+192dX_2^3X_3X_4^3X_5^2 + 144dX_2X_3^4X_4^3X_5 + 1458dX_2^{10}X_4^2 - 1296dX_2^3X_3^5X_4X_5-}$$

$$\underline{-288dX_2^2X_3^3X_4^2X_5^2 + 144dX_2^3X_3^2X_4X_5^3 - 16dX_2X_3X_4^3X_5^3}$$
$$(3X_2^3 + X_3 * X_4 - X_2 * X_5)^4$$

и константа $d$ сопряжена с вычислением $\theta$-констант:

$$\theta \begin{bmatrix} 0 \\ 0 \\ 0 \\ 0 \end{bmatrix} (0), \quad \theta \begin{bmatrix} 1/2 \\ 1/2 \\ 0 \\ 1/2 \end{bmatrix} (0).$$

Четвёртая образующая $F_4$ идеала 3-кручения имеет следующий вид:

$$F_4(X_1, X_2, X_3, X_4) = \frac{1}{2} \underline{-27dX_2^4X_3^2 + 27dX_2^5X_4 + 18dX_2X_3^3X_4 - 9dX_2^2X_3X_4^2 - dX_4^4-}$$
$$\underline{-18dX_2^2X_3^2X_5 - 3dX_2^3X_4X_5 + 2dX_3X_4^2X_5 - 2dX_2X_4^2X_5^2 + 9X_1X_2^6+}$$
$$\underline{+6X_1X_2^3X_3X_4 - 6X_1X_2^4X_5 + X_1X_3^2X_4^2 - 2X_1X_2X_3X_4X_5 + X_1X_2^2X_5^2}$$
$$(3X_2^3 + X_3X_4 - X_2X_5)^2 + \tilde{F}_4,$$

где выражение $\tilde{F}_4$ сопряжено с вычислением $\wp$- и $\theta$-функций.

## ЛИТЕРАТУРА


1. *Cohen H. and Frey G.* Handbook of Elliptic and Hyperelliptic Curve Cryptography. Chapman and Hall/CRC, 2005.
2. *Lidl R., Mullen G. L., and Turnwald G.* Dickson Polynomials. Chapman and Hall/CRC, 1993.
3. *Novoselov S. A.* Counting points on hyperelliptic curves of type $y^2 = x^{2g+1} + ax^{g+1} + bx$. arXiv: 1902.05992. 2019.
4. *Malygina E. S. and Novoselov S. A.* Division polynomials for hyperelliptic curves defined by Dickson polynomials // Proc. 8th Workshop on Current Trends in Cryptology. Svetlogorsk, Kaliningrad region, June 4–7, 2019. `https://ctcrypt.ru/ematerials2019`.
5. *Hindry M. and Silverman J.* Diophantine Geometry. An Introduction. Graduate Texts in Mathematics. V. 201. Springer Verlag, 2000.
6. *Kampkötter W.* Explizite Gleichungen für Jacobische Varietätenhyperelliptisher Rurven.Ph. D. Thesis, Universität Gesamthochschule Essen, 1991.

УДК 519.214 DOI 10.17223/2226308X/12/4

# О ЧИСЛЕ $f$-РЕКУРРЕНТНЫХ СЕРИЙ И ЦЕПОЧЕК В КОНЕЧНОЙ ЦЕПИ МАРКОВА

Н. М. Меженная

Будем называть $f$-рекуррентной цепочкой отрезок дискретной последовательности, знаки которого получаются последовательным применением функции $f$ к $l$ предыдущим знакам, а цепочку, которую нельзя продлить ни в одну сторону с сохранением свойства $f$-рекуррентности, — $f$-рекуррентной серией. При помощи метода Чена — Стейна получена оценка расстояния по вариации между распределением числа $\xi$ $f$-рекуррентных серий длины не меньше $s$ в отрезке длины $n$ конечной эргодической стационарной цепи Маркова и сопровождающим законом распределения Пуассона, т. е. распределением Пуассона с параметром $\lambda_s = \mathsf{E}\xi$, порядка $\mathrm{O}\big(s\lambda_s/n + \mathrm{e}^{us}\sqrt{\lambda_s}\big)$ при некотором $u > 0$. Из этой оценки стандартными методами выведены пуассоновская и нормальная предельные теоремы для случайной величины $\xi$ (при стремлении длины $n$ отрезка цепи Маркова и параметра $s$ к бесконечности). Также полученная оценка позволяет показать, что вероятность наличия $f$-рекуррентных цепочек длины не меньше $s$ стремится к $1 - \mathrm{e}^{\lambda}$, если $n, s \to \infty$ так, что $s/n \to 0$, $\lambda_s/n \to 0$ и $\lambda_s \to \lambda$. Свойства распределений частот $f$-рекуррентных серий или цепочек с определёнными свойствами могут быть использованы при разработке статистических критериев для проверки качества псевдослучайных последовательностей.

**Ключевые слова:** *цепь Маркова, $f$-рекуррентная серия, $f$-рекуррентная цепочка, предельная теорема Пуассона, нормальная предельная теорема, метод Чена — Стейна.*

Пусть $\{X_j, j = 1, \ldots, n\}$ — эргодическая стационарная цепь Маркова с множеством состояний $\mathscr{A}_N = \{1, \ldots, N\}$, $N \geqslant 2$, матрицей переходных вероятностей $P = ||p_{a,b}||_{a,b\in\mathscr{A}_N}$ и распределением вероятностей $\{\pi_a, a \in \mathscr{A}_N\}$. Элементы матрицы $P^n$ обозначим $p^{(n)}_{a,b}$, $p^{(1)}_{a,b} = p_{a,b}$.

Известно [1, ч. 2, § 2, с. 100], что существуют константы $C, \gamma > 0$, при которых

$$|p^{(n)}_{a,b} - \pi_b| \leqslant C\pi_b \mathrm{e}^{-\gamma n},\ n \geqslant 1. \tag{1}$$

Пусть $f : \mathscr{A}^l_N \to \mathscr{A}_N$ — числовая функция, $s \geqslant 2$. Приведём определение $f$-рекуррентной цепочки и серии [2].

**Определение 1.** Случайные величины $X_{j+1}, \ldots, X_{j+l+s}$ образуют *$f$-рекуррентную цепочку* длины не меньше $s$, если

$$X_{j+l+1} = f(X_j, \ldots, X_{j+l-1}),\ \ldots,\ X_{j+l+s} = f(X_{j+s}, \ldots, X_{j+l+s-1}). \tag{2}$$

**Определение 2.** Случайные величины $X_j, \ldots, X_{j+l+s}$ образуют *$f$-рекуррентную серию* длины не меньше $s$, если

$$\begin{gathered} X_{j+l} \neq f(X_j, \ldots, X_{j+l-1}), \\ X_{j+l+1} = f(X_{j+1}, \ldots, X_{j+l}),\ \ldots,\ X_{j+l+s} = f(X_{j+s}, \ldots, X_{j+l+s-1}). \end{gathered} \tag{3}$$

Обозначим $A_j$ и $B_j$ индикаторы событий (2) и (3) соответственно.

Определение $f$-рекуррентной серии обобщает известное определение серии из одинаковых знаков [3, с. 62]. Действительно, если $l = 1$, функция $f \equiv a$, $a \in \mathscr{A}_N$, то

$$B_j = \{X_{j+1} \neq a, X_{j+2} = a, \ldots, X_{j+s+1} = a\}$$

и $f$-рекуррентная серия длины не меньше $s$ совпадает с обычной серий знаков $a$ длины не меньше $s$.

Точные распределения чисел серий в двоичных марковских цепях изучены в [4, 5], а их предельные распределения в цепях Маркова с любым числом состояний получены в [6]. Распределение длины наибольшей серии одинаковых знаков рассмотрено в [7 – 9] для последовательности независимых случайных величин, в [10 – 12] — для цепи Маркова.

Распределение числа $f$-рекуррентных серий в последовательности независимых случайных величин изучено в [2, 13]. В [14] получены аналогичные результаты для $f$-рекуррентных серий с возможными пропусками знаков.

Большинство современных криптографических систем предполагает использование псевдослучайных последовательностей, обладающих свойствами, близкими к свойствам случайных равновероятных последовательностей. Для оценки их качества используются различные статистические критерии, в том числе основанные на статистиках от частот значений функций от $s$-цепочек: тест частот встречаемости $s$-грамм, покер-тест, тест линейной сложности, тест ранга случайной матрицы, тест интервалов и др. [15]. Для построения таких критериев могут быть использованы и частоты появлений $f$-рекуррентных цепочек и серий при подходящем выборе функции $f$.

Будем считать, что задана функция $f$ от $l \geqslant 1$ переменных. Пусть $\Gamma = \{1, \ldots, n-s-l\}$; $\{\alpha_j = I_{A_j} : j \in \Gamma\}$ и $\{\beta_j = I_{B_j} : j \in \Gamma\}$ — наборы случайных индикаторов, соответствующих событиям $\{A_j : j \in \Gamma\}$ и $\{B_j : j \in \Gamma\}$; $Q_s = \mathsf{P}\{B_j\}$ — вероятность любого события из набора $\{B_j : j \in \Gamma\}$.

Определим случайную величину $\xi = \sum\limits_{j=1}^{n-s} \beta_j$, равную числу $f$-рекуррентных серий в $\{X_j, j = 1, \ldots, n\}$, и её математическое ожидание $\lambda_s = \mathsf{E}\xi = (n-s-l)Q_s$, а также случайную величину $\xi^* = \sum\limits_{j=1}^{n-s} \alpha_j$, равную числу $f$-рекуррентных цепочек в $\{X_j, j = 1, \ldots, n\}$.

Будем использовать следующие обозначения: $\mathcal{L}(\xi)$ — для закона распределения случайной величины $\xi$; $\mathrm{Pois}(\lambda)$ — для распределения Пуассона с параметром $\lambda$; $\mathcal{N}(0,1)$ — для стандартного нормального распределения; $\rho\left(\mathcal{L}(\xi), \mathcal{L}(\eta)\right)$ — для расстояния по вариации между $\mathcal{L}(\xi)$ и $\mathcal{L}(\eta)$. Для неотрицательных целочисленных случайных величин $\eta_1$ и $\eta_2$ оно задаётся формулой

$$\rho\left(\mathcal{L}(\eta_1), \mathcal{L}(\eta_2)\right) = \frac{1}{2} \sum_{u=0}^{\infty} \left|\mathsf{P}\{\eta_1 = u\} - \mathsf{P}\{\eta_2 = u\}\right|.$$

**Теорема 1.** Пусть $s, l, m \geqslant 1$ и $\lambda_s \geqslant 1$. Тогда

$$\rho\left(\mathcal{L}(\xi), \mathrm{Pois}(\lambda_s)\right) \leqslant \left(2(s+l+2m) + 1 + \frac{2C}{\mathrm{e}^{\gamma} - 1}\right) Q_s + \\ + C\mathrm{e}^{-\gamma(m+1)} \sqrt{\lambda_s} \left(2 + C\mathrm{e}^{-\gamma(m+1)} + \mathrm{e}^{-\gamma(s+l+m+1)}\right),$$

где константы $C$ и $\gamma$ определены в (1).

**Следствие 1.** Пусть число $l \geqslant 1$ фиксировано, $s, n \to \infty$, так что

$$\frac{s}{n} \to 0, \quad Q_s \to 0, \quad \lambda_s \to \lambda \in (0, \infty).$$

Тогда

1) $\mathcal{L}(\xi) \to \mathrm{Pois}(\lambda)$;
2) $\mathsf{P}\{\xi^* \geqslant 1\} \to 1 - e^{-\lambda}$.

**Следствие 2.** Пусть число $l \geqslant 1$ фиксировано, $s, n \to \infty$, так что

$$\lambda_s \to \infty, \quad \frac{s}{n}\lambda_s \to 0,$$

и существует константа $u > 0$, для которой $\lambda_s = \mathrm{o}(e^{us})$. Тогда

$$\mathcal{L}\left(\frac{\xi - \lambda_s}{\sqrt{\lambda_s}}\right) \to \mathcal{N}(0,1).$$

**Замечание 1.** Для доказательства теоремы 1 использованы метод Чена — Стейна (см. теорему 1.A из [16, с. 9]) и схема рассуждений, предложенная в [17, 18].

## ЛИТЕРАТУРА


1. *Розанов Ю. А.* Случайные процессы. Краткий курс. М.: Наука, 1979. 184 с.
2. *Михайлов В. Г.* Об асимптотических свойствах числа серий событий // Тр. по дискр. матем. 2006. Т. 9. С. 152–163.
3. *Феллер В.* Введение в теорию вероятностей и ее приложения. В 2-х т. Т. 1. М.: Мир, 1984. 528 с.
4. *Савельев Л. Я., Балакин С. В., Хромов Б. В.* Накрывающие серии в двоичных марковских последовательностях // Дискрет. матем. 2003. Т. 15. № 1. С. 50–76.
5. *Савельев Л. Я., Балакин С. В.* Некоторые применения стохастической теории серий // Сиб. журн. индустр. матем. 2012. Т. 15. № 3. С. 111–123.
6. *Тихомирова М. И.* Предельные распределения числа непоявившихся цепочек одинаковых исходов // Дискрет. матем. 2008. Т. 20. № 3. С. 293–300.
7. *Erdos P. and Revesz P.* On the length of the longest head-run // Topics in Inform. Theory. Colloquia Math. Soc. J. Bolyai 16 Keszthely. 1975. P. 219–228.
8. *Fu J. C.* Distribution theorem of runs and patterns associated with a sequence of multi-state trials // Statist. Sinica. 1996. V. 6. P. 957–974.
9. *Lou W. Y. W.* On runs and longest runs tests: a method of finite Markov chain imbedding // J. Amer. Statist. Assoc. 1996. V. 91. P. 1595–1601.
10. *Vaggelatou E.* On the length of the longest run in a multi-state Markov chain // Statist. Probab. Let. 2003. V. 62. P. 211–221.
11. *Chryssaphinou O., Papastavridis S., and Vaggelatou E.* Poisson approximation for the number of non-overlapping appearances of several words in Markov chain // Combinatorics Probab. 2001. V. 10. P. 293–308.
12. *Zhang Y. Z. and Wu X. Y.* Some results associated with the longest run in a strongly ergodic Markov chain // Acta Mathematica Sinica. 2013. V. 29. No. 10. P. 1939–1948.
13. *Михайлов В. Г.* О предельной теореме Б. А. Севастьянова для сумм зависимых случайных индикаторов // Обозрение прикладной и промышленной математики. 2003. Т. 10. № 3. С. 571–578.
14. *Меженная Н. М.* Предельные теоремы для числа плотных $F$-рекуррентных серий и цепочек в последовательности независимых случайных величин // Вестник Московского государственного технического университета им. Н. Э. Баумана. Сер. Естественные науки. 2014. № 3. С. 11–25.
15. *Шойтов А. М.* Вероятностные модели псевдослучайных последовательностей в криптографии // Материалы Второй Междунар. науч. конф. по проблемам безопасности и противодействия терроризму. МГУ им. М. В. Ломоносова. М.: МЦНМО, 2006. С. 116–134.

16. *Barbour A. D., Holst L., and Janson S.* Poisson Approximation. Oxford: Oxford Univ. Press, 1992. 277 p.
17. *Михайлов В. Г., Шойтов А. М.* О длинных повторениях цепочек в цепи Маркова // Дискрет. матем. 2014. Т. 26. № 3. С. 79–89.
18. *Minakov A. A.* Poisson approximation for the number of non-decreasing runs in Markov chains // Матем. вопр. криптогр. 2018. Т. 9. № 2. С. 103–116.

УДК 512.772 DOI 10.17223/2226308X/12/5

# ХАРАКТЕРИСТИЧЕСКИЕ МНОГОЧЛЕНЫ НЕКОТОРЫХ ГИПЕРЭЛЛИПТИЧЕСКИХ КРИВЫХ РОДОВ 2,3 И $p$-РАНГА 1[1]

Е. М. Мельничук, С. А. Новоселов

Исследуются характеристические многочлены некоторых классов гиперэллиптических кривых рода $2, 3$ $p$-ранга 1 над конечным полем. $p$-Ранг является важным инвариантом кривой, который накладывает ограничения на характеристический многочлен кривой и, следовательно, на число точек в её якобиане. Получены сравнения (по модулю характеристики) и ограничения на коэффициенты для характеристических многочленов кривых $p$-ранга 1 с автоморфизмами.

**Ключевые слова:** *гиперэллиптические кривые, p-ранг, характеристические многочлены, группа автоморфизмов.*

## Введение

Гиперэллиптическая кривая $C$ рода $g$ над конечным полем $\mathbb{F}_q$ задаётся уравнением

$$y^2 + h(x)y = f(x),$$

где $h(x), f(x) \in \mathbb{F}_q[x]$ и $\deg h(x) \leqslant g+1$, $\deg f(x) = 2g+1$ или $\deg f(x) = 2g+2$ и многочлен $f(x)$ является унитарным.

В настоящее время гиперэллиптические кривые изучаются как альтернатива эллиптическим кривым. Гиперэллиптические кривые требуют меньший размер ключа при сравнимом уровне безопасности. Одними из перспективных направлений в криптографии на (гипер)эллиптических кривых являются классическая криптография на дискретном логарифме, криптография на билинейных спариваниях, постквантовая криптография на изогениях.

Для криптографии на дискретном логарифме необходимы кривые рода 2 и 3 с большим простым числом точек в якобиане. Для кривых больших родов имеются атаки методом исчисления индексов. Для криптографии на билинейных спариваниях, помимо требований для стойкости дискретного логарифма, необходимы кривые с малой степенью вложения. Ярким примером применения криптосистем на билинейных спариваниях является механизм Zk-Snark, применяемый в криптовалюте Zcash. В основе Zk-Snark лежит редуцированное эйт-спаривание. Криптография на изогениях гиперэллиптических кривых в настоящее время только начинает развиваться. Основной проблемой является отсутствие эффективных формул для вычисления изогений.

Множество точек гиперэллиптических кривых рода 2 и 3 не образует группу, в отличие от эллиптических кривых, поэтому для использования таких кривых в криптографии строится ассоциированная с кривой группа — якобиан кривой.

[1]Исследование выполнено при финансовой поддержке РФФИ, проект № 18-31-00244.

**Определение 1.** Якобианом гиперэллитической кривой $C$ называется факторгруппа

$$J_C = Div^0(C)/Pr(C),$$

где $Div^0(C)$ — множество дивизоров степени 0; $Pr(C)$ — множество главных дивизоров кривой $C$.

Важным инвариантом гиперэллиптической кривой является $p$-ранг.

**Определение 2.** Пусть $C$ — гиперэллиптическая кривая. Тогда $J_C[p^e] \cong (\mathbb{Z}/p^e\mathbb{Z})^r$ для $0 \leqslant r \leqslant g$ и $e \geqslant 1$. Число $r$ называется $p$-рангом кривой $C$.

Хорошо исследованы кривые с $p$-рангом 0, которые имеют маленькую степень вложения, и $p$-рангом 2, подавляющее большинство которых имеют большую степень вложения. Для суперсингулярных абелевых многообразий ($p$-ранг равен 0) известны [1] полные списки возможных характеристических многочленов. Соответственно задача подсчёта точек на суперсингулярных кривых может быть решена простым перебором возможных вариантов. Для кривых $p$ ранга 1 подобных списков в настоящее время не составлено.

В данной работе исследуются характеристические многочлены для кривых $p$-ранга 1. В силу того, что данные кривые являются промежуточным случаем, мы предполагаем возможность существования как классов кривых с маленькой степенью вложения, так и кривых с большой степенью вложения.

Будем рассматривать классы кривых рода 2, чей $p$-ранг не превосходит 2, и кривые рода 3, чей $p$-ранг меньше или равен 3. Среди них выделим кривые $p$-ранга 1.

## 1. Характеристический многочлен и $p$-ранг

$L$-многочлен кривой связан с $p$-рангом посредством следующей теоремы.

**Теорема 1** (Штихтенот). Пусть $L(T) = a_0 + a_1T + a_2T^2 + \ldots + a_{2g}T^{2g}$, тогда $p$-ранг кривой $C$ равен

$$\max\{i : a_i \not\equiv 0 \pmod{p}\}.$$

Если кривая имеет автоморфизмы, определённые над некоторым расширением конечного поля, то, в силу следующей теоремы, это накладывает дополнительные ограничения на характеристический многочлен данной кривой.

**Теорема 2** [4]. Пусть $k$ — поле, $K$ — расширение поля $k$, $A$ — абелево многообразие над полем $k$ и $\tau \in \mathrm{End}_K^0(A_K)$, такой, что

1) действие группы $\mathrm{Gal}(K|k)$ на $\mathrm{End}_K^0(A_K)$ отображает подпространство $\mathbb{Q}[\tau] \subset \subset \mathrm{End}_K^0(A_K)$ в себя;
2) $\tau$ не определено ни над одним промежуточным полем $\mu$ расширения $K|k$, где $\mu \subsetneq K$;
3) $\mathbb{Q}[\tau]$ — поле.

Тогда характеристический многочлен эндоморфизма Фробениуса абелева многообразия $A$ имеет вид $f(T^{[K:k]})$ для некоторого многочлена $f(T) \in \mathbb{Z}[T]$ степени $2\dim(A)/[K:k]$.

Так как якобиан гиперэллиптической кривой является абелевым многообразием, то теорема 2 применима и к гиперэллиптическим кривым. Это позволяет получить следующий результат.

**Теорема 3.** Пусть дана гиперэллиптическая кривая $C$ рода $g$, такая, что выполняются условия теоремы 2. Тогда $r_C \geqslant [K:k]$.

Кроме того, имеет место следствие для кривых рода $g$ и $p$-ранга 1.

**Следствие 1.** Кривая $C$ рода $g$ может иметь $p$-ранг 1 только при условии $[K:k]=1$.

Заметим, что следствие не гарантирует наличия $p$-ранга 1 у кривой $C$, однако это необходимое условие в контексте теоремы 2. Применим эти результаты к некоторым классам гиперэллиптических кривых.

## 2. Кривые $p$-ранга 1 и их характеристические многочлены

Для кривых рода 3 с нетривиальной группой автоморфизмов $p$-ранг может быть определён с помощью результатов из [3], что позволяет выделить кривые $p$-ранга 1.

**Теорема 4.** Пусть гиперэллиптическая кривая $C/\mathbb{F}_p$ рода 3 имеет группу автоморфизмов $C_{14}$. Тогда уравнение кривой имеет вид $y^2=x^7+1$. Положим

$$v=\binom{(p-1)/2}{5(p-1)/14}+\binom{(p-1)/2}{3(p-1)/14}+\binom{(p-1)/2}{(p-1)/14},\ w=\binom{(p-1)/2}{5(p-1)/14}\binom{(p-1)/2}{3(p-1)/14}+$$
$$+\binom{(p-1)/2}{5(p-1)/14}\binom{(p-1)/2}{(p-1)/14}+\binom{(p-1)/2}{3(p-1)/14}\binom{(p-1)/2}{(p-1)/14}.$$

Тогда кривая $C$ имеет $p$-ранг 1, если $p\equiv 1 \pmod 7$, $v\not\equiv 0 \pmod p$ и $w\equiv 0 \pmod p$. Кроме того, характеристический многочлен эндоморфизма Фробениуса имеет следующий вид:

$$\chi(\lambda)\equiv\lambda^{2g}+v\lambda^{2g-1} \pmod p.$$

**Теорема 5.** Пусть группа автоморфизмов $G$ кривой $C$ равна $D_{12}$. Тогда кривая имеет модель $y^2=x(x^6+\alpha x^3+1)$, где $\alpha\in K$. Обозначим $c=P_{(p-1)/2}(\rho)$, $d=P_{(p-1)/6}(\rho)$, $e=P_{(p-5)/6}(\rho)$, где $\rho=-\alpha/2$ и $P_n$ — многочлены Лежандра. Тогда если $\alpha\neq 0$, то

1) $p$-ранг кривой равен 1 при $p\equiv 1 \pmod 3$, $c+2d\not\equiv 0 \pmod p$ и $c^2+2cd\equiv\equiv 0 \pmod p$. В этом случае многочлен Фробениуса по модулю $p$ равен

$$\chi(\lambda)\equiv\lambda^{2g}+(c+2d)\lambda^{2g-1} \pmod p;$$

2) $p$-ранг равен 1 при $p\equiv 2 \pmod 3$, $c\not\equiv 0 \pmod p$ и $e\equiv 0 \pmod p$. В этом случае многочлен Фробениуса по модулю $p$ равен

$$\chi(\lambda)\equiv\lambda^{2g}+c\lambda^{2g-1} \pmod p.$$

**Теорема 6.** Пусть группа автоморфизмов $G$ кривой $C$ равна $V_8$. Тогда данная кривая имеет вид $y^2=x^8-1$. Пусть

$$s=\binom{(p-1)/2}{3(p-1)/8}+\binom{(p-1)/2}{(p-1)/4}+\binom{(p-1)/2}{(p-1)/8},$$
$$t=\binom{(p-1)/2}{3(p-1)/8}\binom{(p-1)/2}{(p-1)/4}+\binom{(p-1)/2}{3(p-1)/8}\binom{(p-1)/2}{(p-1)/8}+\binom{(p-1)/2}{(p-1)/4}\binom{(p-1)/2}{(p-1)/8}.$$

Тогда

1) если $p\equiv 1 \pmod 8$, то при $s\not\equiv 0, t\equiv 0 \pmod p$ кривая имеет $p$-ранг 1. В этом случае многочлен Фробениуса по модулю $p$ равен

$$\chi(\lambda)\equiv\lambda^{2g}+w\lambda^{2g-1} \pmod p;$$

2) если $p \equiv 5 \pmod 8$ и $r = \binom{(p-1)/2}{(p-1)/4}$, то при $r \not\equiv 0 \pmod p$ кривая имеет $p$-ранг 1. В этом случае многочлен Фробениуса по модулю $p$ равен

$$\chi(\lambda) \equiv \lambda^{2g} + r\lambda^{2g-1} \pmod p.$$

**Теорема 7.** Пусть группа автоморфизмов $G$ кривой $C$ равна $D_8 \times C_2$. Тогда кривая имеет модель $y^2 = x^8 + \alpha x^4 + 1$, где $\alpha \in K$. Пусть $a = P_{(p-1)/4}(\rho)$, $b = P_{(p-3)/4}(\rho)$, $c = P_{(p-1)/2}(\rho)$, где $\rho = -\alpha/2$. Тогда

1) если $p \equiv 1 \pmod 4$, то $p$-ранг кривой равен 1 при $a \equiv 0$, $c \not\equiv 0 \pmod p$. В этом случае многочлен Фробениуса по модулю $p$ равен

$$\chi(\lambda) \equiv \lambda^{2g} + c\lambda^{2g-1} \pmod p;$$

2) если $p \equiv 3 \pmod 4$, то $p$-ранг кривой равен 1 при $b \equiv 0$, $c \not\equiv 0 \pmod p$. В этом случае многочлен Фробениуса по модулю $p$ равен

$$\chi(\lambda) \equiv \lambda^{2g} + c\lambda^{2g-1} \pmod p.$$

## Заключение

В работе получены характеристические многочлены $\pmod p$ гиперэллиптических кривых рода $2, 3$ и $p$-ранга 1 для кривых с автоморфизмами.

В дальнейшем на основе полученных результатов планируется построить алгоритм подсчёта числа точек на кривых, изоморфных кривым с автоморфизмами над расширением конечного поля, по аналогии с работой [5] и исследовать их степени вложения с целью анализа возможности применения таких кривых как в классических криптосистемах, так и в криптосистемах на основе билинейных спариваний и изогений.

## ЛИТЕРАТУРА

1. *Singh V., Zatysev A., and McGuire G.* On the Characteristic Polynomial of Frobenius of Supersingular Abelian Varieties of Dimension up to 7 over Finite Fields. arXiv preprint arXiv:1011.2257. 2010.
2. *Novoselov S. A.* Hyperelliptic curves, Cartier — Manin matrices and Legendre polynomials // Прикладная дискретная математика. 2017. № 37. С. 20–31.
3. *Мельничук Е. М., Новоселов С. А.* $p$-Ранги гиперэллиптических кривых рода 3 с нетривиальной группой автоморфизмов // Труды математического центра имени Н. И. Лобачевского. 2018. Т. 56. С. 188–192.
4. *Bouw I. I., Diem C., and Scholten J.* Ordinary elliptic curves of high rank over with constant $j$-invariant // Manuscripta Mathematica. 2004. V. 114. No. 4. P. 487–501.
5. *Novoselov S. A.* Counting points on hyperelliptic curves of type $y^2 = x^{2g+1} + ax^{g+1} + bx$. `https://arxiv.org/abs/1902.05992`. 2019.

УДК 519.7 DOI 10.17223/2226308X/12/6

# ВАРИАЦИИ ОРТОМОРФИЗМОВ И ПСЕВДОАДАМАРОВЫХ ПРЕОБРАЗОВАНИЙ НА НЕАБЕЛЕВОЙ ГРУППЕ

Б. А. Погорелов, М. А. Пудовкина

В криптографии ортоморфизмы на абелевой группе используются как $S$-боксы в схемах Лея — Месси, квази-Фейстеля, в блочной шифрсистеме FOX, в режиме

блочного шифрования Дэвиса — Мейера, а также в кодах аутентификации. В работе рассматриваются ортоморфизмы, полные преобразования и их вариации на конечной неабелевой группе $(X,\cdot)$ наложения ключа. В алгоритме блочного шифрования SAFER для обеспечения принципа рассеивания используется псевдоадамарово преобразование. Предложено десять аналогов псевдоадамарова преобразования, задаваемых подстановкой $s$ на неабелевой группе $(X,\cdot)$. Доказано, что биективность аналогов псевдоадамарова преобразования равносильна справедливости следующего условия: подстановка $s$ является ортоморфизмом, полным преобразованием или их вариацией.

**Ключевые слова:** *ортоморфизм, полное преобразование, конечная неабелева группа, псевдоадамарово преобразование, алгоритм блочного шифрования SAFER.*

Пусть $S(X)$ — симметрическая группа на конечном множестве $X$, $g(\alpha)$ — образ элемента $\alpha \in X$ при действии на него подстановкой $g \in S(X)$, $\alpha^g = \alpha g = g(\alpha)$. Рассмотрим произвольную конечную неабелеву группу $(X,\cdot)$. Каждой подстановке $s \in S(X)$ поставим в соответствие преобразования $\pi_i^{(s)} : X \to X$, $i = 1,\dots,4$, заданные условиями

$$\pi_1^{(s)} : \alpha \mapsto \alpha^{-1}\alpha^s, \quad \pi_2^{(s)} : \alpha \mapsto \alpha\alpha^s, \quad \pi_3^{(s)} : \alpha \mapsto \alpha^s\alpha^{-1}, \quad \pi_4^{(s)} : \alpha \mapsto \alpha^s\alpha.$$

**Определение 1.** Пусть $s \in S(X)$, тогда

1) если $\pi_1^{(s)} \in S(X)$, то $s$ называется *ортоморфизмом* [1];
2) если $\pi_2^{(s)} \in S(X)$, то $s$ называется *полным преобразованием* [1];
3) если $\pi_3^{(s)} \in S(X)$, то $s$ называется *левым ортоморфизмом*;
4) если $\pi_4^{(s)} \in S(X)$, то $s$ называется *полным левым преобразованием.*

Очевидно, что для коммутативной группы $\pi_1^{(s)} = \pi_3^{(s)}$, $\pi_2^{(s)} = \pi_4^{(s)}$. В этом случае говорят, что $\pi_1^{(s)}$ — ортоморфизм, а $\pi_2^{(s)}$ — полное преобразование. Заметим, что для неабелевой группы $\pi_1^{(s)}$ можно называть правым ортоморфизм, а $\pi_2^{(s)}$ — полным правым преобразованием.

В дискретной математике ортоморфизмы и полные преобразования находят применение, например, при построении систем ортогональных латинских квадратов, квазигрупп [2–4]. В настоящее время открытым является вопрос полной классификации всех ортоморфизмов и полных преобразований на произвольной конечной группе. В криптографии ортоморфизмы используются как $S$-боксы [5], компоненты функции шифрования в схемах Лея — Месси [6], квази-Фейстеля [7], в алгоритме блочного шифрования FOX [8], в режиме блочного шифрования Дэвиса — Мейера [9], а также в кодах аутентификации.

Известно [1], что каждому ортоморфизму $s \in S(X)$ соответствует полное преобразование $\pi_1^{(s)}$. Наоборот, каждому полному преобразованию $s \in S(X)$ соответствует ортоморфизм $\pi_2^{(s)}$. Аналогичная связь существует между левым ортоморфизмом и полным левым преобразованием.

В алгоритме блочного шифрования SAFER [10] для обеспечения принципа рассеивания используется псевдоадамарово преобразование $h : \mathbb{Z}_{256}^2 \to \mathbb{Z}_{256}^2$, заданное условием

$$h : (\alpha_1, \alpha_2) \mapsto (2\alpha_1 + \alpha_2, \alpha_1 + \alpha_2),\ (\alpha_1, \alpha_2) \in \mathbb{Z}_{256}^2.$$

Очевидно, что $h$ — подстановка на $\mathbb{Z}_{256}^2$. При этом преобразование $x \mapsto 2x \bmod 256$ не является биективным ортоморфизмом.

Для подстановки $s \in S(X)$ и каждого $\alpha \in X$ положим

$$\mathrm{A}^{(s)}(\alpha) = \left\{\alpha, \alpha^{-1}, \alpha^s, (\alpha^s)^{-1}\right\}.$$

Пусть $d = \left(d_1^{(1)}, d_2^{(1)}, d_1^{(2)}, d_2^{(2)}\right)$ — набор отображений, удовлетворяющих условиям $d_i^{(j)} : X^2 \to X$, $d_i^{(j)}(\alpha_1, \alpha_2) \in \mathrm{A}^{(s)}(\alpha_1) \cup \mathrm{A}^{(s)}(\alpha_2)$ для каждой пары $(\alpha_1, \alpha_2) \in X^2$, $i, j = 1, 2$. Обозначим через $D^{(s)}$ множество всех таких наборов отображений.

Для алгоритма блочного шифрования с неабелевой группой наложения ключа $(X, \cdot)$ рассмотрим аналог псевдоадамарова преобразования $h^{(s,d)} : X^2 \to X^2$, $d \in D^{(s)}$, заданного условием

$$h^{(s,d)} : (\alpha_1, \alpha_2) \mapsto \left(d_1^{(1)}(\alpha_1, \alpha_2) d_2^{(1)}(\alpha_1, \alpha_2), d_1^{(2)}(\alpha_1, \alpha_2) d_2^{(2)}(\alpha_1, \alpha_2)\right).$$

Для $s \in S(X)$ рассмотрим преобразования $h_i^{(s)} : X^2 \to X^2$ при $i = 1, \ldots, 10$, заданные условиями

$$\begin{aligned}
&h_1^{(s)} : (\alpha_1, \alpha_2) \mapsto (\alpha_1^s \alpha_2, \alpha_1 \alpha_2), && h_2^{(s)} : (\alpha_1, \alpha_2) \mapsto (\alpha_1^s \alpha_2^{-1}, \alpha_2 \alpha_1),\\
&h_3^{(s)} : (\alpha_1, \alpha_2) \mapsto (\alpha_1^s \alpha_2, \alpha_1 \alpha_2^{-1}), && h_4^{(s)} : (\alpha_1, \alpha_2) \mapsto (\alpha_1^s \alpha_2^{-1}, \alpha_1 \alpha_2^{-1}),\\
&h_5^{(s)} : (\alpha_1, \alpha_2) \mapsto ((\alpha_1^s)^{-1} \alpha_2, \alpha_1 \alpha_2), && h_6^{(s)} : (\alpha_1, \alpha_2) \mapsto ((\alpha_1^s)^{-1} \alpha_2^{-1}, \alpha_1 \alpha_2^{-1}),\\
&h_7^{(s)} : (\alpha_1, \alpha_2) \mapsto (\alpha_1 \alpha_2^s, \alpha_1 \alpha_2), && h_8^{(s)} : (\alpha_1, \alpha_2) \mapsto (\alpha_1 (\alpha_2^s)^{-1}, \alpha_1 \alpha_2),\\
&h_9^{(s)} : (\alpha_1, \alpha_2) \mapsto (\alpha_1 \alpha_2^s, \alpha_1 \alpha_2^{-1}), && h_{10}^{(s)} : (\alpha_1, \alpha_2) \mapsto (\alpha_1 (\alpha_2^s)^{-1}, \alpha_1 \alpha_2^{-1}).
\end{aligned}$$

Очевидно, что $h_i^{(s)} \in \left\{h^{(s,d)} : d \in D^{(s)}\right\}$ для $i = 1, \ldots, 10$.

Получен критерий биективности преобразования $h_j^{(s)}$ для каждого $j \in \{1, \ldots, 10\}$.

**Теорема 1.** Пусть $s \in S(X)$.

1. Для каждого $j \in \{1, 4\}$ тогда и только тогда $h_j^{(s)} \in S(X^2)$, когда $\pi_3^{(s)} \in S(X)$.
2. Для каждого $j \in \{2, 3, 8\}$ тогда и только тогда $h_j^{(s)} \in S(X^2)$, когда $\pi_4^{(s)} \in S(X)$.
3. Для каждого $j \in \{5, 6, 9\}$ тогда и только тогда $h_j^{(s)} \in S(X^2)$, когда $\pi_2^{(s)} \in S(X)$.
4. Для каждого $j \in \{7, 10\}$ тогда и только тогда $h_j^{(s)} \in S(X^2)$, когда $\pi_1^{(s)} \in S(X)$.

Кроме того, пусть $\mathrm{Aut}(X)$ — группа автоморфизмов. Доказано, что если $s \in \mathrm{Aut}(X)$, то для каждого $\{i, j\} \in \{\{1, 3\}, \{2, 4\}\}$ условия $\pi_i^{(s)} \in S(X)$ и $\pi_j^{(s)} \in S(X)$ равносильны.

## ЛИТЕРАТУРА


1. *Evans A.* Orthomorphisms Graphs and Groups. Berlin: Springer Verlag, 1992.
2. *Johnson D. M., Dulmage A. L., and Mendelsohn N. S.* Orthomorphisms of groups and orthogonal Latin squares // Canad. J. Math. 1961. V. 13. P. 356–372.
3. *Глухов М. М.* О применениях квазигрупп в криптографии // Прикладная дискретная математика. 2008. Т. 2. № 2. С. 28–32.
4. *Глухов М. М.* О методах построения систем ортогональных квазигрупп с использованием групп // Математические вопросы криптографии. 2011. Т. 2. № 4. С. 5–24.
5. *Mittenthal L.* Block substitutions using orthomorphic mappings // Adv. Appl. Math. 1995. V. 16. No. 1. P. 59–71.
6. *Vaudenay S.* On the Lai — Massey schemes // ASIACRYPT'99. LNCS. 1999. V. 1716. P. 8–19.
7. *Yun A., Park J., and Lee J.* On Lai — Massey and quasi-Feistel ciphers // Des. Codes Cryptogr. 2011. V. 58. P. 45–72.

8. *Junod P. and Vaudenay S.* FOX: A new family of block ciphers // Selected Areas in Cryptography'04. LNCS. 2005. V. 3357. P. 114–129.
9. *Gilboa S. and Gueron S.* Balanced permutations Even-Mansour ciphers // Cryptology ePrint Archive. 2014. Report 2014/642.
10. *Massey J. L.* SAFER K-64: a byte-oriented block-ciphering algorithm // FSE'94. LNCS. 1994. V. 809. P. 1–17.

УДК 519.7 DOI 10.17223/2226308X/12/7

# О КЛАССЕ СТЕПЕННЫХ КУСОЧНО-АФФИННЫХ ПОДСТАНОВОК НА НЕАБЕЛЕВОЙ ГРУППЕ ПОРЯДКА $2^m$, ОБЛАДАЮЩЕЙ ЦИКЛИЧЕСКОЙ ПОДГРУППОЙ ИНДЕКСА ДВА

Б. А. Погорелов, М. А. Пудовкина

Четыре неабелевы группы порядка $2^m$, $m \geqslant 4$, имеют циклические подгруппы индекса два. Примерами являются широко известная группа диэдра и обобщённая группа кватернионов. Произвольная неабелева группа $G$ порядка $2^m$, обладающая циклической подгруппой индекса два, в определённом смысле близка к встречающейся в качестве группы наложения ключа аддитивной абелевой группе кольца вычетов $\mathbb{Z}_{2^m}$. В данной работе на группе $G$ задаются два класса преобразований, названных степенными кусочно-аффинными, для которых доказаны критерии биективности. Они позволят далее провести полную классификацию ортоморфизмов, полных преобразований и их вариаций во множестве всех степенных кусочно-аффинных подстановок.

**Ключевые слова:** *неабелева группа, группа диэдра, обобщённая группа кватернионов, критерий биективности, ортоморфизм.*

В ARX-шифрсистемах используются просто реализуемые операции сложения в кольце вычетов, в векторном пространстве над полем GF(2), а также циклический сдвиг. Возникает вопрос о переходе к просто реализуемой группе наложения ключа, относительно которой вместе с некоторым преобразованием $g$ могут эффективно обеспечиваться перемешивающие и рассеивающие свойства.

Неабелевы группы порядка $2^m$, обладающие циклической подгруппой индекса два, в определенном смысле преемственны широко встречающимся в качестве групп наложения ключа аддитивным абелевым группами $m$-мерного векторного пространства $V_m(2)$ над полем GF(2) и кольца вычетов $\mathbb{Z}_{2^m}$. В [1] описана связь между неабелевостью группы наложения ключа и свойством марковости алгоритмов блочного шифрования.

Из теоремы 12.5.1 [2] следует, что неабелевыми группами порядка $2^m$, имеющими циклическую подгруппу индекса два, являются только четыре группы с двумя образующим $a$, $u$, удовлетворяющими следующим определяющим соотношениям:

1) обобщённая группа кватернионов $Q_{2^m}$, $m \geqslant 3$,

$$a^{2^{m-1}} = e,\ u^2 = a^{2^{m-2}},\ ua = a^{-1}u;$$

2) группа диэдра $D_{2^{m-1}}$, $m \geqslant 3$,

$$a^{2^{m-1}} = e,\ u^2 = e,\ ua = a^{-1}u;$$

3) $m \geqslant 4$,

$$a^{2^{m-1}} = e,\ u^2 = e,\ ua = a^{1+2^{m-2}}u;$$

4) $m \geqslant 4$,

$$a^{2^{m-1}} = e,\ u^2 = e,\ ua = a^{-1+2^{m-2}}u.$$

На произвольной неабелевой группе $G = \langle a, u\rangle$ порядка $2^m$, имеющей циклическую подгруппу $\langle a\rangle$ индекса два, рассмотрим преобразования двух видов $\theta^{(r_1,r_2,q_1,q_2)}_{(c_1,c_2,b_1,b_2)} : G \to G$ и $\tilde{\theta}^{(r_1,r_2,q_1,q_2)}_{(c_1,c_2,b_1,b_2)} : G \to G$, заданные условиями

$$\theta^{(r_1,r_2,q_1,q_2)}_{(c_1,c_2,b_1,b_2)} : a^i \mapsto \begin{cases} a^{r_1 i+c_1}, & \text{если } i \in \{0,\dots,2^{m-2}-1\},\\ a^{r_2 i+c_2}u, & \text{если } i \in \{2^{m-2},\dots,2^{m-1}-1\},\end{cases}$$

$$\theta^{(r_1,r_2,q_1,q_2)}_{(c_1,c_2,b_1,b_2)} : a^i u \mapsto \begin{cases} a^{q_1 i+b_1}u, & \text{если } i \in \{0,\dots,2^{m-2}-1\},\\ a^{q_2 i+b_2}, & \text{если } i \in \{2^{m-2},\dots,2^{m-1}-1\},\end{cases}$$

$$\tilde{\theta}^{(r_1,r_2,q_1,q_2)}_{(c_1,c_2,b_1,b_2)} : a^i \mapsto \begin{cases} a^{r_1 i+c_1}, & \text{если } i \in \{0,\dots,2^{m-2}-1\},\\ a^{r_2 i+c_2}u, & \text{если } i \in \{2^{m-2},\dots,2^{m-1}-1\},\end{cases}$$

$$\tilde{\theta}^{(r_1,r_2,q_1,q_2)}_{(c_1,c_2,b_1,b_2)} : a^i u \mapsto \begin{cases} a^{q_1 i+b_1}, & \text{если } i \in \{0,\dots,2^{m-2}-1\},\\ a^{q_2 i+b_2}u, & \text{если } i \in \{2^{m-2},\dots,2^{m-1}-1\},\end{cases}$$

где $b_1, b_2, c_1, c_2 \in \{0,\dots,2^{m-1}-1\}$, $r_1, r_2, q_1, q_2 \in \{0,\dots,2^{m-1}-1\}$.

Далее преобразования $\theta^{(r_1,r_2,q_1,q_2)}_{(c_1,c_2,b_1,b_2)}$ и $\tilde{\theta}^{(r_1,r_2,q_1,q_2)}_{(c_1,c_2,b_1,b_2)}$ будем называть *степенными кусочно-аффинными*. Для каждого из этих преобразований получены критерии биективности. Приведём критерий для преобразования $\theta^{(r_1,r_2,q_1,q_2)}_{(c_1,c_2,b_1,b_2)}$.

**Теорема 1.** Пусть $m \geqslant 4$, $G = \langle a, u\rangle$, $G$ — неабелева группа порядка $2^m$ с циклической подгруппой $\langle a\rangle$ индекса два. Преобразование $\theta^{(r_1,r_2,q_1,q_2)}_{(c_1,c_2,b_1,b_2)} : G \to G$ является подстановкой тогда и только тогда, когда элементы $b_1, b_2, c_1, c_2 \in \{0,\dots,2^{m-1}-1\}$, $r_1, r_2, q_1, q_2 \in \{0,\dots,2^{m-1}-1\}$ удовлетворяют одному из следующих условий:

1. Если $r_1 \equiv r_2 \equiv 1 \pmod 2$, то
   - 1.1. $r_1 = q_2$, $r_2 = q_1$, $c_1 = b_2$, $c_2 = b_1$;
   - 1.2. $r_1 = q_2$, $r_2 = 2^{m-1} - q_1$, $c_1 = b_2$, $b_1 - c_2 + 2^{m-2} \equiv q_1 \pmod{2^{m-1}}$;
   - 1.3. $r_2 = q_1$, $r_1 = 2^{m-1} - q_2$, $c_2 = b_1$, $b_2 - c_1 + 2^{m-2} \equiv q_2 \pmod{2^{m-1}}$;
   - 1.4. $r_2 = 2^{m-1} - q_1$, $r_1 = 2^{m-1} - q_2$, $b_1 - c_2 + 2^{m-2} \equiv q_1 \pmod{2^{m-1}}$, $b_2 - c_1 + 2^{m-2} \equiv q_2 \pmod{2^{m-1}}$.
2. Если $r_1 \equiv 1 \pmod 2$, $r_2 \equiv q_1 \equiv 2 \pmod 4$, то
   - 2.1. $r_1 = q_2$, $c_1 = b_2$, $b_1 + c_2 \equiv 1 \pmod 2$;
   - 2.2. $r_1 = 2^{m-1} - q_2$, $b_1 + c_2 \equiv 1 \pmod 2$, $b_2 - c_1 + 2^{m-2} \equiv q_2 \pmod{2^{m-1}}$.
3. Если $r_2 \equiv 1 \pmod 2$, $r_1 \equiv q_2 \equiv 2 \pmod 4$, то
   - 3.1. $r_2 = q_1$, $c_2 = b_1$, $b_2 + c_1 \equiv 1 \pmod 2$;
   - 3.2. $r_2 = 2^{m-1} - q_1$, $c_1 = b_2$, $b_1 + c_2 \equiv 1 \pmod 2$.
4. Если $r_1 \equiv r_2 \equiv 2 \pmod 4$, то
   - 4.1. $q_1 \equiv q_2 \equiv 2 \pmod 4$, $b_1 + c_2 \equiv 1 \pmod 2$, $b_2 + c_1 \equiv 1 \pmod 2$.

Полученные критерии биективности в дальнейшем позволят для каждой из четырёх неабелевых групп порядка $2^m$, обладающих циклической подгруппой индекса два, классифицировать ортоморфизмы, полные преобразования, а также левые ортоморизмы и полные левые преобразования [3] в множестве всех степенных кусочно-аффинных подстановок $\theta^{(r_1,r_2,q_1,q_2)}_{(c_1,c_2,b_1,b_2)}$, $\tilde{\theta}^{(r_1,r_2,q_1,q_2)}_{(c_1,c_2,b_1,b_2)}$.

ЛИТЕРАТУРА

1. *Погорелов Б. А., Пудовкина М. А.* О неабелевых группах наложения ключа и марковости алгоритмов блочного шифрования // Прикладная дискретная математика. Приложение. 2018. № 11. С. 79–81.
2. *Холл М.* Теория групп. М.: ИЛ, 1962. 468 с.
3. *Погорелов Б. А., Пудовкина М. А.* Вариации ортоморфизмов и псевдоадамаровых преобразований на неабелевой группе // Прикладная дискретная математика. Приложение. 2019. № 12. С. 24–27.

УДК 519.1 DOI 10.17223/2226308X/12/8

# ТОЧНАЯ ФОРМУЛА ЭКСПОНЕНТА ПЕРЕМЕШИВАЮЩЕГО ОРГРАФА РЕГИСТРОВОГО ПРЕОБРАЗОВАНИЯ

В. М. Фомичев, Я. Э. Авезова

Для примитивного перемешивающего $n$-вершинного орграфа $\Gamma(g)$ преобразования $g$ двоичного регистра сдвига длины $n$, где обратная связь $f(x_0, \ldots, x_{n-1})$ имеет $m$ существенных переменных с множеством номеров $D(g) = \{d_1, \ldots, d_m\}$, $n \geqslant 3$, $2 \leqslant m \leqslant n$, $0 = d_1 < \ldots < d_m$, при $d_m \in \{n-1, n-2\}$ получена точная формула экспонента $\exp \Gamma(g)$ и элементарных локальных экспонентов $\gamma_{u,v}$, $0 \leqslant u, v < n$.

**Ключевые слова:** *локально примитивный орграф, перемешивающий орграф, примитивный орграф, регистр сдвига, экспонент орграфа.*

## Введение

Изучение экспонентов примитивных матриц и графов началось в 1912 г. с работы Фробениуса [1]. Основные понятия и научные достижения отражены в обзоре [2] и ряде других работ. Получение точной аналитической формулы экспонента для того или иного класса матриц и орграфов — сложная комбинаторная задача, в связи с чем большинство работ в этой области посвящены верхним оценкам экспонентов, важным для приложений.

Исследован класс преобразований $g$ пространства $n$-мерных векторов, реализуемых регистром левого сдвига с нелинейной обратной связью $f(x_0, \ldots, x_{n-1})$, имеющей $m$ существенных переменных, в том числе $x_0$ (иначе реальная длина регистра меньше $n$), $n \geqslant 3$, $2 \leqslant m \leqslant n$. Анализ перемешивающих свойств преобразований данного класса имеет прикладное значение для ряда систем защиты информации.

Пусть множество вершин перемешивающего орграфа $\Gamma(g)$, соответствующих номерам входных переменных преобразования $g$, есть $\{0, \ldots, n-1\}$. Получены точные формулы экспонентов и локальных экспонентов двух частных классов перемешивающих орграфов регистровых преобразований. Первый класс орграфов имеет петлю в вершине $n-1$, второй класс содержит контур $(n-1, n-2)$ длины 2.

## 1. Структурные свойства перемешивающих орграфов регистровых преобразований

Рассмотрим преобразование $g$ двоичного регистра левого сдвига длины $n$ с нелинейной функцией обратной связи $f(x_0, \ldots, x_{n-1})$. Обозначим $D(g) = \{d_1, \ldots, d_m\}$ множество номеров всех существенных переменных функции $f$, где $0 = d_1 < \ldots < d_m \leqslant n-1$. Тогда преобразованию $g$ соответствует $n$-вершинный перемешивающий орграф $\Gamma(g)$, имеющий $n+m-1$ дуг, где $n$ дуг составляют гамильтонов контур $(n-1, \ldots, 0)$ и остальные дуги суть $(d_2, n-1), \ldots, (d_m, n-1)$. Таким образом, связный орграф $\Gamma(g)$ есть объ-

единение простых контуров $C_1, \ldots, C_m$, где $C_t = (n-1, n-2, \ldots, d_t)$, $t = 1, \ldots, m-1$, $C_m = (n-1, n-2, \ldots, d_m)$ при $d_m < n-1$ и $C_m$ есть петля в вершине $n-1$ при $d_m = n-1$. Вершины $d_m, \ldots, n-1$ являются общими для всех простых контуров.

Обозначим: $n - D(g) = \{n - d_i : i = 1, \ldots, m\}$; $\Lambda W(u,v)$ — множество длин всех путей из вершины $u$ в вершину $v$; $\overline{\Lambda W(u,v)} = \mathbb{N}_0 \backslash \Lambda W(u,v)$, где $\mathbb{N}_0$ — множество целых неотрицательных чисел. Определим элементарные локальные экспоненты орграфа $\Gamma(g)$. По определению локальный экспонент (обозначается $\gamma_{u,v}$) есть наименьшее натуральное число $\gamma$, такое, что из $u$ в $v$ есть путь длины $t$ при любом $t \geqslant \gamma$ [3]. В соответствии с определением

$$\gamma_{u,v} = 1 + \max \overline{\Lambda W(u,v)}, \quad 0 \leqslant u, v < n,$$
$$\exp \Gamma(g) = \max_{0 \leqslant u,v < n} \gamma_{u,v}.$$

## 2. Формулы экспонента и локальных экспонентов при $d_m = n-1$

При $0 \leqslant u, v < n$ и $d_m \in \{n-1, n-2\}$ обозначим:

- $\tau(u)$ — наибольшее число множества $\{1, \ldots, m\}$, такое, что $d_{\tau(u)} \leqslant u$;
- $l_t(u,v) = u - d_t + n - v$, $t = 1, \ldots, \tau(u)$, $u < n-1$;
- $L(u,v) = \{l_1(u,v), \ldots, l_{\tau(u)}(u,v)\}$, $u < n-1$;
- $\Delta(D) = \max\{d_2 - d_1, \ldots, d_m - d_{m-1}\}$.

Если $u = v = n-1$, то положим $\gamma_{n-1,n-1} = 1$.

**Теорема 1.** Если орграф $\Gamma(g)$ примитивный, $n \geqslant 3$, то при $d_m = n-1$

$$\gamma_{u,v} = \begin{cases} n - v - 1, & u = n-1,\ v < u, \\ l_{\tau(u)}(u,v), & u < n-1. \end{cases}$$

Приведём формулу экспонента орграфа $\Gamma(g)$.

**Теорема 2.** Пусть орграф $\Gamma(g)$ примитивный, $n \geqslant 3$, тогда при $d_m = n-1$

$$\exp \Gamma(g) = n + \Delta(D) - 1.$$

**Пример 1.** $n = 5$, $D(g) = \{0, 2, 4\}$. Вычисляем $\Delta(D) = 2$, тогда в соответствии с теоремой 2 $\exp \Gamma(g) = 5 + 2 - 1 = 6$. Локальные экспоненты $\gamma_{u,v}$ приведены в таблице.

| $u$ | $v$ | | | | |
|---|---|---|---|---|---|
| | 0 | 1 | 2 | 3 | 4 |
| 0 | 5 | 4 | 3 | 2 | 1 |
| 1 | 6 | 5 | 4 | 3 | 2 |
| 2 | 5 | 4 | 3 | 2 | 1 |
| 3 | 6 | 5 | 4 | 3 | 2 |
| 4 | 4 | 3 | 2 | 1 | 1 |

## 3. Формулы экспонента и локальных экспонентов при $d_m = n-2$

Получим формулы для $\gamma_{u,v}$ и $\exp \Gamma(g)$ при $d_m = n-2$. По условию $\Gamma(g)$ содержит контур длины 2 и, в силу примитивности орграфа $\Gamma(g)$, содержит контур нечётной длины.

Заметим, что при $d_m = n-2$ множество $D(g)$ содержит нечётные числа. Действительно, если $n$ нечётное, то число $(n-2) \in D(g)$ также нечётное; если $n$ чётное, то оба множества $n - D(g)$ и $D(g)$ содержат хотя бы одно нечётное число в силу примитивности орграфа $\Gamma(g)$.

Введём следующие обозначения:

— $I(L(u,v))$ и $J(L(u,v))$ — множества нечётных и чётных чисел множества $L(u,v)$ соответственно;
— $l^0(u,v) = \min J(L(u,v))$, если $J(L(u,v)) \neq \varnothing$;
— $l^1(u,v) = \min I(L(u,v))$, если $I(L(u,v)) \neq \varnothing$;
— $\chi(u,v) = |l^1(u,v) - l^0(u,v)|$;
— $d_\mu$ — наибольшее число множества $D(g)$, чётность которого не совпадает с чётностью числа $n$;
— $d_\lambda$ — наименьшее нечётное число множества $D(g)$.

При $u \geqslant d_\lambda$ выполнены следующие свойства:

1) величины $l^0(u,v)$ и $l^1(u,v)$ существуют и $l_{\tau(u)} = \min\{l^0(u,v), l^1(u,v)\}$;
2) величина $\chi(u,v)$ существует и не зависит от $v$, $\chi(u,v) = \chi(u) = |\mu(u) - \eta(u)|$, где $\mu(u)$ и $\eta(u)$ — наибольшие числа различной чётности множества $\{d_1, \ldots, d_{\tau(u)}\}$.

**Теорема 3.** Если орграф $\Gamma(g)$ примитивный, $n \geqslant 3$, то при $d_m = n-2$

$$\gamma_{u,v} = \begin{cases} 2n - d_\mu - v - 2, & u = n-1, \\ 2n - d_\mu - v - 1 + u - d_{\tau(u)}, & u < d_\lambda, \\ n + \min\{n - d_\mu, \chi(u)\} - v - 1 + u - d_{\tau(u)}, & d_\lambda \leqslant u < n-1. \end{cases}$$

Приведём формулу экспонента орграфа $\Gamma(g)$.

**Теорема 4.** Пусть орграф $\Gamma(g)$ примитивный, $n \geqslant 3$, тогда при $d_m = n-2$

$$\exp\Gamma(g) = \begin{cases} 2n - d_\mu - 2 + \Delta(D), & d_\lambda = d_m, \\ 2n - d_\mu - 2 + \max\{\Delta(D_{[\lambda]}), p_\lambda, \ldots, p_{m-1}\}, & d_\lambda < d_m, \end{cases}$$

где $\Delta(D_{[\lambda]}) = \max\{d_2 - d_1, \ldots, d_\lambda - d_{\lambda-1}\}$, $p_s = d_{s+1} - d_s + \min\{0, \chi(d_s) - n + d_\mu\}$, $s = \lambda, \ldots, m-1$.

**Пример 2.** $n = 8$, $D(g) = \{0,2,5,6\}$. Найдём $\exp\Gamma(g)$, используя теорему 4. Вычисляем: $d_\mu = d_\lambda = 5$, $d_m = 6$. Тогда при $d_\lambda < d_m$ находим: $\Delta(D_{[\lambda]}) = \max\{2,3\} = 3$, $\chi(d_2) = 1$, $p_3 = 6 - 5 + \min\{0, 1 - 8 + 5\} = -1$. Следовательно, $\exp\Gamma(g) = 16 - 5 - 2 + {} + \max\{3, -1\} = 12$.

## ЛИТЕРАТУРА


1. *Frobenius G.* Über Matrizen aus nicht negativen Elementen // Sitzungsber K. Preuss. Akad. Wiss. 1912. P. 456–477.
2. *Fomichev V. M., Avezova Ya. E., Koreneva A. M., and Kyazhin S. N.* Primitivity and local primitivity of digraphs and nonnegative matrices // J. Appl. Industr. Math. 2018. V. 12. No. 3. P. 453–469.
3. *Fomichev V. M. and Kyazhin S. N.* Local primitivity of matrices and graphs // J. Appl. Industr. Math. 2017. V. 11. No. 1. P. 26–39.

УДК 519.1 DOI 10.17223/2226308X/12/9

# ОЦЕНКА С ПОМОЩЬЮ МАТРИЧНО-ГРАФОВОГО ПОДХОДА ХАРАКТЕРИСТИК ЛОКАЛЬНОЙ НЕЛИНЕЙНОСТИ ИТЕРАЦИЙ ПРЕОБРАЗОВАНИЙ ВЕКТОРНЫХ ПРОСТРАНСТВ

В. М. Фомичёв, В. М. Бобров

В порядке обобщения матрично-графового подхода к исследованию характеристик нелинейности преобразований векторных пространств, предложенного В. М. Фомичевым, развивается математический аппарат для локальной нелинейности преобразований. Пусть $G = \{0, 1, 2\}$ — мультипликативная полугруппа, где $a0 = 0$ для любого $a \in G$; $ab = \max\{a, b\}$ для любых $a, b \neq 0$. Троичная матрица (то есть матрица над $G$) называется $\alpha$-матрицей, $\alpha \in \Pi(2) = \{\langle 2c\rangle; \langle 2s\rangle; \langle 2sc\rangle; \langle 2\rangle\}$, если все её строки ($\langle 2s\rangle$-матрица), столбцы ($\langle 2c\rangle$-матрица), строки и столбцы ($\langle 2sc\rangle$-матрица) содержат 2 или если все элементы равны 2 ($\langle 2\rangle$-матрица). Обозначим $M_n^\alpha(I \times J)$ множество троичных матриц $M$ порядка $n$, чьи $I \times J$-подматрицы (полученные вычеркиванием строк с номерами не из $I$ и столбцов с номерами не из $J$) являются $\alpha$-матрицами, $I, J \in \{1, \ldots, n\}$. На множестве троичных матриц определено умножение. Если $A = (a_{i,j})$, $B = (b_{i,j})$, то $AB = C = (c_{i,j})$, где $c_{i,j} = \max\{a_{i,1}b_{1,j}, \ldots, a_{i,n}b_{n,j}\}$ и для любых допустимых $i, j$ умножение элементов выполняется в группе $G$. Матрицу $M$ назовём $I{\times}J$-$\alpha$-примитивной, если существует $\gamma \in \mathbb{N}$, такое, что $M^t \in M_n^\alpha(I \times J)$ при всех натуральных $t \geqslant \gamma, \alpha \in \Pi(2)$. Наименьшее из таких чисел $\gamma$ обозначим $I \times J$-$\alpha$-$\exp M$ и назовём $I \times J$-$\alpha$-экспонентом матрицы $M$. Троичным матрицам порядка $n$ биективно соответствуют $n$-вершинные орграфы с множеством $G$ меток дуг, поэтому на орграфы распространены определения $I \times J$-$\alpha$-примитивности и $I \times J$-$\alpha$-экспонента. Получены достаточные условия того, что $I \times J$-$\alpha$-экспонент матрицы равен наименьшей её степени, в которой $I \times J$-подматрица является $\alpha$-матрицей, $\alpha \in \Pi(2)$. При $I = \{i\}$, $J = \{j\}$ для частных классов помеченных орграфов получены верхние оценки $I{\times}J$-$\alpha$-экспонентов, в частности для орграфа, в котором имеется путь из $i$ в $j$, проходящий через компоненту сильной связности.

**Ключевые слова:** *матрично-графовый подход, троичная матрица, помеченный орграф, локальная нелинейность, локальный $\alpha$-экспонент.*

## Введение

В некоторых приложениях, в том числе криптографических, важно определить множество переменных, от которых нелинейно зависит каждая функция из заданного подмножества координатных функций преобразования векторного пространства. Эта информация может быть использована для оценки эффективности некоторых методов линеаризации при получении оценки стойкости криптографических алгоритмов.

Представленные результаты направлены на получение оценок множеств переменных, по которым нелинейны те или иные координатные функции преобразования векторного пространства, построенного по итеративному принципу.

Приведём ряд определений [1]. Преобразованию $g(x_1, \ldots, x_n)$ множества $V_n$ двоичных $n$-мерных векторов с координатными функциями $g_1(x_1, \ldots, x_n), \ldots, g_n(x_1, \ldots, x_n)$ соответствует $n$-вершинный орграф $\Gamma_\theta(g)$, где дуга $(i, j)$ помечена числом 0, 1 или 2 тогда и только тогда, когда $g_j(x_1, \ldots, x_n)$ зависит от $x_i$ соответственно фиктивно, линейно или нелинейно, $1 \leqslant i, j \leqslant n$. Преобразование $g(x_1, \ldots, x_n)$ называется $I \times J$-$\langle 2\rangle$-нелинейным, если любая дуга $(i, j) \in I{\times}J$ в орграфе $\Gamma_\theta(g)$ помечена символом «2». Преобразование $g(x_1, \ldots, x_n)$ называется $I \times J$-$\langle 2\rangle$-перфективным, если при некотором на-

туральном $t$ преобразование $g^t$ является $I{\times}J$-нелинейным, наименьшее такое $t$ называется показателем полной $I{\times}J$- $\langle 2\rangle$-нелинейности преобразования $g(x_1,\ldots,x_n)$ (обозначается $I{\times}J$- $\langle 2\rangle$-nlg). Характеристики орграфа $\Gamma_\theta(g^t)$ можно оценить с помощью матрицы меток орграфа $\Gamma_\theta(g)$, обозначаемой $M_\theta(g)$, что следует из неравенства для любых преобразований $g^{(1)},\ldots,g^{(t)}$ множества $V_n$ [1]: $M_\theta\left(g^{(1)},\ldots,g^{(t)}\right)\geqslant M_\theta\left(g^{(1)}\right)\ldots M_\theta\left(g^{(t)}\right)$. Проекция этого неравенства на подмножества $I\times J$ даёт следующую оценку:

$$M_\theta\left(g^{(1)},\ldots,g^{(t)}\right)(I\times J)\geqslant M_\theta\left(g^{(1)}\right)(I\times J)\ldots M_\theta\left(g^{(t)}\right)(I\times J),\quad I,J\subseteq\{1,\ldots,n\}.$$

Таким образом, локальные характеристики матрицы нелинейности $M_\theta\left(g^{(1)},\ldots,g^{(t)}\right)$ можно оценить с помощью локальных характеристик матрицы $M_\theta\left(g^{(1)}\right)\ldots M_\theta\left(g^{(t)}\right)$. В частности, локальные характеристики матрицы нелинейности $M_\theta(g^t)$ можно оценить с помощью локальных характеристик $t$-й степени матрицы нелинейности $M_\theta(g)$.

## 1. Локальная $\alpha$-примитивность троичных матриц и помеченных орграфов

Троичная матрица называется особенной, если она имеет нулевую строку или нулевой столбец. Обозначим: $M_n$ — множество квадратных неособенных троичных матриц порядка $n$; $M(I\times J)$ — подматрица матрицы $M\in M_n$ (называемая $I{\times}J$-подматрицей), полученная вычеркиванием из $M$ строк с номерами из $I$ и столбцов с номерами из $J$, где $I,J\subseteq\{1,\ldots,n\}$.

Неособенная матрица называется:

— $\langle 2c\rangle$-матрицей, если каждый столбец матрицы содержит элемент 2;
— $\langle 2s\rangle$-матрицей, если каждая строка матрицы содержит элемент 2;
— $\langle 2sc\rangle$-матрицей, если она является $\langle 2c\rangle$-матрицей и $\langle 2s\rangle$-матрицей;
— $\langle 2\rangle$-матрицей, если каждый элемент матрицы равен 2.

Для $\alpha\in\Pi(2)$ обозначим $M_n^\alpha(I\times J)$ множество всех матриц $M\in M_n$, чьи $I\times J$-подматрицы являются $\alpha$-матрицами.

Матрицу $M$ назовём $I\times J$-$\alpha$-примитивной, если существует $\gamma\in\mathbb{N}$, такое, что $M^t\in$ $\in M_n^\alpha(I\times J)$ при всех натуральных $t\geqslant\gamma$, $\alpha\in\Pi(2)$. Наименьшее из таких чисел $\gamma$ обозначим $I\times J$-$\alpha$-$\exp M$ и назовём $I\times J$-$\alpha$-экспонентом матрицы $M$.

Обобщённо назовём свойства $I\times J$-$\alpha$-примитивности матриц в случае $I$ и $J$, не равных $\{1,\ldots,n\}$, свойством локальной $\alpha$-примитивности матриц для всех $\alpha\in\Pi(2)$. Случай $I=J=\{1,\ldots,n\}$ называется $\alpha$-примитивностью и исследован в [1].

В случае $\alpha$-примитивности наименьшее $t\in\mathbb{N}$, такое, что $M^t\in M_n^\alpha$, равно $\alpha$-экспоненту, в то время как для локальной $\alpha$-примитивности в общем случае это не верно.

Обозначим $Q_s(I\times J)$, $Q_c(I\times J)$ множества матриц $M\in M_n$, чьи $I\times J$-подматрицы не имеют нулевых строк и столбцов соответственно; $Q_{sc}(I\times J)=Q_s(I\times J)\cap Q_c(I\times J)$. Для случая $I=J$ обозначим эти множества $Q_s(I^2)$, $Q_c(I^2)$, $Q_{sc}(I^2)$.

Если $M^t\in M_n^\alpha(I\times J)$, то в соответствии с определением этого недостаточно для того, чтобы выполнялось равенство $t=I\times J$-$\alpha$-$\exp M$. Укажем условие, когда наименьшее $t\in\mathbb{N}$, при котором $M^t\in M_n^\alpha(I\times J)$, равно $I\times J$-$\alpha$-экспоненту матрицы.

**Теорема 1** (обобщение утверждения 1,а [2]). Пусть $t\in N$ — наименьшее натуральное число, при котором $A^t\in M_n^\alpha(I\times J)$, $\alpha\in\Pi(2)$, тогда $A$ является $I\times J$-$\alpha$-примитивной и $t=I\times J$-$\alpha$-$\exp A$, если

$$\alpha=\langle 2s\rangle,\ A\in Q_s\left(I^2\right)\cup Q_s\left(J^2\right);$$
$$\alpha=\langle 2c\rangle,\ A\in Q_c\left(I^2\right)\cup Q_c\left(J^2\right);$$

$$\alpha = \langle 2sc \rangle\,,\ A \in Q_{sc}\left(I^2\right) \cup Q_{sc}\left(J^2\right);$$
$$\alpha = \langle 2 \rangle\,,\ A \in Q_{s}\left(I^2\right) \cup Q_{c}\left(J^2\right).$$

При $n > 1$ троичной матрице $M = (m_{i,j})$ порядка $n$ биективно соответствует помеченный $n$-вершинный орграф $\Gamma$, у которого дуга $(i, j)$ имеет метку $m_{i,j}$, $0 \leqslant i, j < n$, где метка «0» равносильна отсутствию дуги в орграфе [1]. Неособенной матрице соответствует орграф, каждая вершина которого имеет ненулевые полустепени исхода и захода, такие орграфы назовём также неособенными. Помеченный орграф называется $I \times J$-$\alpha$-примитивным, если $I \times J$-$\alpha$-примитивна его матрица меток $(m_{i,j})$.

На множестве $\Gamma_n$ неособенных помеченных орграфов порядка $n$ определена полугрупповая операция умножения орграфов $\Gamma$ и $\Gamma'$: если в $\Gamma$ имеется дуга $(i, m_{i,r}, r)$, а в $\Gamma'$ имеется дуга $(r, \mu_{r,i}, j)$, то в орграфе $\Gamma\Gamma'$ имеется дуга $(i, m_{i,r}\mu_{r,j}, j)$, где операция умножения меток выполняется в полугруппе $G$. Доказано [1, следствие 1], что в орграфе $\Gamma^t$ дуга $(i, j)$ имеет метку «0», если и только если в $\Gamma$ вершина $j$ недостижима из вершины $i$ за $t$ шагов; «1», если и только если в $\Gamma$ любой путь из $i$ в $j$ длины $t$ состоит только из дуг с меткой «1»; «2», если и только если в $\Gamma$ имеется путь из $i$ в $j$ длины $t$, содержащий дугу с меткой «2».

## 2. Оценки локальных $\alpha$-экспонентов некоторых классов орграфов

В случае $I = \{i\}, J = \{j\}$ свойства $I \times J$-$\alpha$-примитивности для любого $\alpha \in \Pi(2)$ одинаковы. Назовём этот случай $i \times j$- $\langle 2 \rangle$-примитивностью, а соответствующий экспонент орграфа $\Gamma$ обозначим $i \times j$- $\langle 2 \rangle \exp \Gamma$.

Сильносвязный подграф $\Gamma'$ с множеством вершин $V$ орграфа $\Gamma$ называется $i, j$-связывающим, если в $\Gamma$ существует путь из $i$ в $j$, проходящий через некоторую вершину множества $V \subseteq \{1, \ldots, n\}$.

**Теорема 2.**

а) Орграф $\Gamma$ $I \times J$- $\langle 2 \rangle$-примитивный, если и только если $\Gamma$ $i \times j$- $\langle 2 \rangle$-примитивный для всех $(i, j) \in I \times J$; в этом случае $I \times J$- $\langle 2 \rangle \exp \Gamma = \max\limits_{(i,j) \in I \times J} \{i \times j\text{- } \langle 2 \rangle \exp \Gamma\}$.

б) Орграф $\Gamma$ $I \times J$- $\langle 2s \rangle$-примитивный, если и только если $\Gamma$ $i \times J$- $\langle 2s \rangle$-примитивный для всех $i \in I$; в этом случае $I \times J$- $\langle 2s \rangle \exp \Gamma = \max\limits_{i \in I} \{i \times J\text{- } \langle 2s \rangle \exp \Gamma\}$.

в) Орграф $\Gamma$ $I \times J$- $\langle 2c \rangle$-примитивный, если и только если $\Gamma$ $I \times j$- $\langle 2c \rangle$-примитивный для всех $j \in J$; в этом случае $I \times J$- $\langle 2c \rangle \exp \Gamma = \max\limits_{j \in J} \{I \times j\text{- } \langle 2c \rangle \exp \Gamma\}$.

Обозначим $\rho(i, V)$ — наименьшее расстояние от вершины $i$ до подмножества вершин $V$; $\rho(V, j)$ — расстояние от подмножества вершин $V$ до вершины $j$; $d(i, V)$ $(d(V, j))$ — длина кратчайшего пути из $i$ до $V$ (от $V$ до $j$), содержащего дугу с меткой «2».

**Теорема 3** (обобщение теоремы 2, а [2]). Если связный помеченный орграф $\Gamma$ содержит примитивный $i, j$-связывающий подграф $\Gamma'$ с множеством вершин $V$, $|V| = n$, то $\Gamma$ является $i \times j$- $\langle 2 \rangle$-примитивным, если выполняется хотя бы одно из следующих условий:

а) в подграфе $\Gamma'$ есть дуга с меткой «2», тогда

$$i \times j\text{- } \langle 2 \rangle \exp \Gamma \leqslant \rho(i, V) + n + \exp \Gamma' + \rho(V, j);$$

б) в кратчайшем пути из $i$ до множества вершин подграфа $V$ или от множества вершин подграфа $V$ до вершины $j$ есть дуга с меткой «2», тогда

$$i \times j\text{-}\langle 2 \rangle \exp \Gamma \leqslant \rho(i, V) + \exp \Gamma' + \rho(V, j);$$

в) существует путь из $i$ до множества вершин подграфа $V$, содержащий дугу с меткой «2», тогда

$$i\times j\text{-}\langle 2\rangle\exp\Gamma \leqslant d\,(i,V)+\exp\Gamma'+\rho\,(V,j)\,;$$

г) существует путь от множества вершин подграфа $V$ до вершины $j$, содержащий дугу с меткой «2», тогда

$$i\times j\text{-}\langle 2\rangle\exp\Gamma \leqslant \rho\,(i,V)+\exp\Gamma'+d\,(V,j)\,.$$

**Пример 1.** Рассмотрим преобразование регистра левого сдвига длины 6 с функцией обратной связи $f\,(x_0,x_1,x_2,x_3,x_4,x_5)=x_0\oplus x_2x_4\oplus x_5$. Орграф $\Gamma$ этого преобразования представлен на рис. 1, матрица $M$ — на рис. 2. Определим оценку значения $1\times3$-$\langle2\rangle$-экспонента для этого орграфа. Вершины 5 и 4 образуют 1,3-связывающий подграф $\Gamma'$, где $n=|V|=2$, $\exp\Gamma'=1$, $\rho\,(1,V)=2$, $\rho\,(V,3)=1$, $d\,(1,V)=4$, $d\,(V,3)=3$. Оценки $1\times3$-$\langle2\rangle$-экспонента графа $\Gamma$ приведены в таблице.

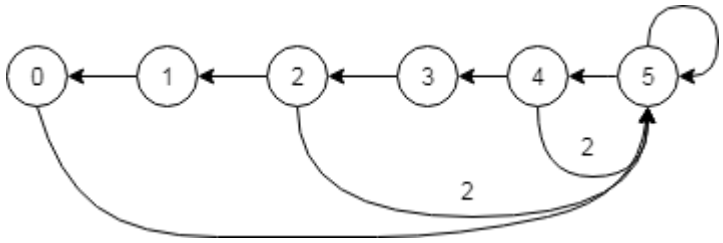


Рис. 1. Орграф нелинейности преобразования регистра сдвига

$$\begin{pmatrix}0&0&0&0&0&1\\1&0&0&0&0&0\\0&1&0&0&0&2\\0&0&1&0&0&0\\0&0&0&1&0&2\\0&0&0&0&1&1\end{pmatrix}$$

Рис. 2. Матрица нелинейности преобразования регистра сдвига

**Сравнение оценок $1\times3$-$\langle2\rangle$-экспонента графа $\Gamma$**

| Значение оценки $i\times j$-$\langle2\rangle$-экспонента | Формула оценки $i\times j$-$\langle2\rangle$-экспонента |
|---|---|
| 6 | $i\times j\text{-}\langle2\rangle\exp\Gamma\leqslant\rho\,(i,V)+n+\exp\Gamma'+\rho\,(V,j)$ |
| 6 | $i\times j\text{-}\langle2\rangle\exp\Gamma\leqslant d\,(i,V)+\exp\Gamma'+\rho\,(V,j)$ |
| 6 | $i\times j\text{-}\langle2\rangle\exp\Gamma\leqslant\rho\,(i,V)+\exp\Gamma'+d\,(V,j)$ |

При возведении матрицы $M$ в степень получаем, что $1\times3$-$\langle2\rangle$-$\exp\Gamma=6$, что соответствует полученным оценкам.

## ЛИТЕРАТУРА

1. *Фомичёв В. М.* О производительности некоторых итеративных алгоритмов блочного шифрования из класса WBC // New Trends in Coding Systems and Techniques. LDN: Intech Publishing, 2019. P. 14.
2. *Кяжин С. Н.* Локальная примитивность графов и неотрицательных матриц // Прикладная дискретная математика. 2014. № 3(25). С. 68–80.

УДК 512.538 DOI 10.17223/2226308X/12/10

# СВОЙСТВА СИЛЬНО ЗАВИСИМЫХ $n$-АРНЫХ ПОЛУГРУПП

А. В. Черемушкин

Приводится обзор результатов о свойствах сильно зависимых $n$-арных полугрупп, обобщающих известные результаты о строении и свойствах $n$-арных групп. Класс сильно зависимых функций является расширением класса $n$-арных квазигрупп. Рассмотрены варианты обобщения понятия существенной зависимости функции от переменной. Поясняется, что класс сильно зависимых функций, с одной стороны, наследует многие важные свойства квазигрупп с точки зрения применения операции бесповторной суперпозиции. С другой стороны, в некоторых случаях он является очень широким и в него попадают почти все функции. Приведены аналоги теорем Поста и Глускина — Хоссу, содержащие общее описание строения сильно зависимых $n$-арных полугрупп. Описано строение групп автотопий таких операций.

**Ключевые слова:** *$n$-арные полугруппы, сильно зависимые функции, группа автотопий.*

## 1. Варианты определения понятия зависимости функции от переменной

Для двоичных функций важную роль играет понятие существенной зависимости функции от переменной. При переходе к функциям $k$-значной логики понятие зависимости может быть определено различными способами. Рассмотрим четыре варианта такого определения.

Пусть $X$ — непустое конечное множество. Рассмотрим следующие классы функций вида $f : X^n \to X$ при $n \geqslant 2$.

Класс $\Phi_0$ состоит из всех функций, существенно зависящих от всех своих переменных, т. е. $\forall i$, $1 \leqslant i \leqslant n$, $\exists a_1, \ldots, a_{i-1}, a_{i+1}, \ldots, a_n \in X$ $\exists x, y \in X$, такие, что

$$f(a_1, \ldots, a_{i-1}, x, a_{i+1}, \ldots, a_n) \neq f(a_1, \ldots, a_{i-1}, y, a_{i+1}, \ldots, a_n). \tag{1}$$

Класс $\Phi_1$ состоит из всех сюръективных функций $f$, таких, что $\forall i$ $\forall x, y \in X$ $\exists a_1, \ldots, a_{i-1}, a_{i+1}, \ldots, a_n \in X$, такие, что выполнено неравенство (1). Этот класс был введён в [1] при изучении свойств операций, удовлетворяющих тождествам $(i, j)$-ассоциативности для пар $\{i, j\}$, содержащихся в некотором множестве $M$. Как показано в [1], для функций из этого класса выполнение тождеств ассоциативности для множества $M$ равносильно выполнению тождества ассоциативности только для некоторой одной пары.

Класс $\Phi_2$ состоит из сильно зависимых функций, т. е. $\forall i$ $\exists a_1, \ldots, a_{i-1}, a_{i+1}, \ldots, a_n \in X$, такие, что унарная функция $f(a_1, \ldots, a_{i-1}, x_i, a_{i+1} \ldots, a_n)$ является подстановкой по переменной $x_i$. Для конечных множеств $X$ этот класс функций замкнут относительно операции бесповторной суперпозиции, т. е. бесповторная суперпозиция таких функций является сильно зависимой в том и только в том случае, когда каждая из функций, участвующих в суперпозиции, также является сильно зависимой [2].

Класс $\Phi_3$ состоит из $n$-квазигрупп на множестве $X$, т. е. $\forall i$ $\forall a_1, \ldots, a_{i-1}, a_{i+1}, \ldots, a_n \in X$ унарная функция $f(a_1, \ldots, a_{i-1}, x_i, a_{i+1}, \ldots, a_n)$ является подстановкой по переменной $x_i$. Изучению свойств $n$-квазигрупп уделялось наибольшее внимание в связи с их многочисленными применениями в области комбинаторики, теории кодирования, планировании эксперимента и т. д. (см., например, [3]). Этот класс также замкнут относительно операции бесповторной суперпозиции.

В общем случае имеют место включения $\Phi_3 \subset \Phi_2 \subseteq \Phi_1 \subseteq \Phi_0$, причём при $k = 2$ $\Phi_0 = \Phi_1 = \Phi_2$ и при каждом $n \geqslant 1$ класс $\Phi_0$ содержит только две функции, а при $k > 2$ все включения оказываются строгими. Приведём оценки мощностей этих классов. Для классов $\Phi_0$ и $\Phi_1$ из определения вытекают неравенства

$$k^{k^n} - nk^{k^{n-1}} \leqslant |\Phi_0| \leqslant k^{k^n} - k^{k^{n-1}},$$
$$k^{k^n} - nk^{(k-1)k^{n-1}} \leqslant |\Phi_1| \leqslant k^{k^n} - k^{(k-1)k^{n-1}}.$$

Значит, $1 > |\Phi_0|/k^{k^n} \geqslant |\Phi_1|/k^{k^n} \to 1$ при $n \geqslant 2$, $k \geqslant 2$ и $\max\{n, k\} \to \infty$, так как всегда

$$\frac{nk^{k^{n-1}}}{k^{k^n}} = \frac{n}{k^{(k-1)k^{n-1}}} \leqslant \frac{nk^{(k-1)k^{n-1}}}{k^{k^n}} = \frac{n}{k^{k^{n-1}}} \to 0.$$

Для класса $\Phi_2$ имеем

$$k^{k^n} - n(k^k - k!)^{k^{n-1}} \leqslant |\Phi_2| \leqslant k^{k^n} - (k^k - k!)^{k^{n-1}}.$$

Поэтому при $n \to \infty$ и фиксированном $k$ почти все функции $k$-значной логики являются сильно зависимыми, а при $k \to \infty$ в общем случае имеет место

**Утверждение 1** [4, 5]. Пусть $\varepsilon > 0$ и $k \to \infty$. При $n > k/\ln\, k + 1/2 + \varepsilon$ почти все функций $k$-значной логики от $n$ переменных являются сильно зависимыми. Если $n < k/\ln\, k + 1/2 - \varepsilon$, то почти все функции $k$-значной логики от $n$ переменных не являются сильно зависимыми.

Так как классы $\Phi_0$ и $\Phi_1$ не замкнуты относительно операции бесповторной суперпозиции, то при изучении полугрупповых операций, удовлетворяющих тождествам ассоциативности, имеет смысл рассматривать только сильно зависимые функции.

## 2. Строение сильно зависимых $n$-арных полугрупп

Напомним, что *моноидом* называется бинарная полугруппа с единицей. *Подмоноид* моноида $G = (X, \circ)$ — это подмножество $H$ моноида $G$, которое замкнуто относительно операции $\circ$. Единица моноида $H$ должна совпадать с единицей моноида $G$.

При $n = 2$ каждая бинарная полугруппа $(X, *)$ с сильно зависимой операцией $*$ является моноидом. В частности, ассоциативная квазигруппа является группой. Этот факт вытекает из следующих утверждений, доказанных в [6, с. 57]:

1) Если для бинарной операции $*$ найдутся элементы $a, b \in X$, такие, что трансляции $L_a = \binom{x}{a*x}$ и $R_b = \binom{x}{x*b}$ являются подстановками, то операция $*$ главноизотопна операции с единицей, причём изотопия имеет вид $(R_b^{-1}, L_A^{-1}, id)$.
2) Если бинарная операция с единицей $\circ$ изотопна ассоциативной операции $*$, то операция $\circ$ изоморфна операции $*$, при этом изоморфизм имеет вид $\varphi = L_a^{-1}R_b^{-1}$ (теорема А. А. Алберта).

Пусть $n \geqslant 3$. Непустое конечное множество $X$ с заданной на нём $n$-арной операцией $f$ называется $n$-арной *полугруппой* ($n$-*полугруппой*), если при всех $i, j$, $1 \leqslant i < j \leqslant n$, выполняются тождества $\{i, j\}$-ассоциативности

$$f(x_1, \ldots, x_{i-1}, f(x_i, \ldots, x_{i+n-1}), x_{i+n}, \ldots, x_{2n-1}) =$$
$$= f(x_1, \ldots, x_{j-1}, f(x_j, \ldots, x_{j+n-1}), x_{j+n}, \ldots, x_{2n-1}),$$

$x_1, \ldots, x_n \in X$. Если при этом $n$-полугруппа является $n$-квазигруппой, то она называется $n$-*группой*. Строение произвольной $n$-арной групповой операции впервые описано Э. Постом в [7] в терминах так называемой обёртывающей группы. Оказывается, что в случае сильно зависимых $n$-арных полугрупп можно получить аналогичное описание. В данном случае вместо группы используется моноид.

**Определение 1.** Назовём моноид $G = (\hat{X}, \circ)$ *обёртывающим* для $n$-арной полугруппы $(X, f)$ с сильно зависимой операцией $f$, если $X \subset \hat{X}$, множество $X$ порождает моноид $G$, а $n$-арная операция $f$ связана с бинарной операцией в моноиде $G$ равенством

$$f(x_1, x_2, \ldots, x_n) = x_1 \circ x_2 \circ \ldots \circ x_n, \quad x_1, x_2, \ldots, x_n \in X. \tag{2}$$

**Теорема 1** (аналог теоремы Э. Поста [8]). Пусть $n \geqslant 3$. Для конечной $n$-арной полугруппы $(X, f)$ с сильно зависимой операцией $f$ найдётся обёртывающий моноид $G = (\hat{X}, \circ)$, такой, что при некотором обратимом элементе $a \in X$ множеству $X_0 = X \circ a^{-1}$ соответствует подмоноид $H = (X_0, \circ)$, удовлетворяющий условиям $G = \langle X \rangle$, $a \circ X_0 \circ a^{-1} = X_0$ и $|\hat{X}| \,\big|\, |X_0|(n-1)$.

Если элемент $g$ обратим, то $|H * g| = |H|$ и при $0 \leqslant i < j \leqslant t-1$, где $t$ — минимальное натуральное число с условием $g^t \in H$, выполняются равенства $|H \circ g^i| = |H \circ g^j|$ и $(H \circ g^i) \cap (H \circ g^j) = \varnothing$. Если $G = \langle H, g \rangle$, то для моноида $G$ справедливо равенство $|G| = |H| \cdot t$. Поэтому в этом случае можно говорить, что моноид $G$ допускает разложение на смежные классы по подмоноиду $H$.

Таким образом, теорема Поста утверждает, что операция исходной $n$-арной полугруппы $(X, f)$ по сути совпадает с ограничением операции $x_1 \circ x_2 \circ \ldots \circ x_n$ на смежный класс $X = X_0 \circ a$ обёртывающего моноида $G = (\hat{X}, \circ)$.

Другой способ описания строения $n$-арной групповой операции получен в работах Л. М. Глускина [9] и М. Хоссу [10]. Аналог их результата для случая сильно зависимых функций имеет следующий вид:

**Теорема 2** (аналог теоремы Глускина — Хоссу [5]). Если $f$ — ассоциативная сильно зависимая $n$-арная операция на конечном множестве $X$, то для некоторого моноида $(X, *)$, обратимого элемента $a$ и автоморфизма $\theta$ этого моноида, таких, что $\theta^{n-1}(x) = a * x * a^{-1}$, $\theta(a) = a$, справедливо тождество

$$f(x_1, \ldots, x_n) = x_1 * \theta(x_2) * \theta^2(x_3) * \ldots * \theta^{n-1}(x_n) * a, \tag{3}$$

$x_i \in X$, $i = 1, \ldots, n$.

В работе [11] обсуждается взаимосвязь теорем Поста и Глускина — Хоссу и утверждается, что они, по-сути, являются различными формами одного и того же результата. В данном случае это также справедливо и легко устанавливается при переходе от записи функции $f$ с использованием операции $\circ$ в обёртывающем моноиде к записи функции $f$ с использованием операции $*$ на самом смежном классе $X = X_0 \circ a$.

Если исходить из теоремы 1, то обозначим через $\varphi$ внутренний автоморфизм обертывающего моноида $\varphi(x) = a \circ x \circ a^{-1}$ и соответственно подмоноида $X_0$. Записывая элементы смежного класса $X = X_0 \circ a$ как $x_i = z_i \circ a$, где $x_i, a \in X$, $z_i \in X_0$, $i = 1, \ldots, n$, получаем

$$\begin{aligned} f(x_1, x_2, \ldots, x_n) &= x_1 \circ x_2 \circ \ldots \circ x_n = \\ &= (z_1 \circ a) \circ (z_2 \circ a) \circ \ldots \circ (z_n \circ a) = \\ &= z_1 \circ (a \circ z_2 \circ a^{-1}) \circ (a^2 \circ z_2 \circ a^{-2}) \circ \ldots \circ (a^{n-1} \circ z_n \circ a^{-(n-1)}) \circ a^n = \\ &= z_1 \circ \varphi(z_2) \circ \varphi^2(z_3) \circ \ldots \circ \varphi^{n-1}(z_n) \circ a^n. \end{aligned}$$

С другой стороны, поскольку $\varphi(X_0) = X_0$ и $\varphi(a) = a$, то $\varphi$ оставляет на месте смежный класс $X$, так как $\varphi(X) = \varphi(X_0 \circ a) = \varphi(X_0) \circ a = \varphi(X)$. Пусть $x * y = x \circ a^{-1} \circ y$. Если $x, y \in X$, то $x * y \in X$. Потому $*$ может рассматриваться как операция на смежном

классе $X$. При этом отображение $\varphi$ также является гомоморфизмом относительно операции $*$ на $X$, так как $\varphi(x*y)=\varphi(x\circ a^{-1}\circ y)=\varphi(x)\circ a^{-1}\circ\varphi(y)=\varphi(x)*\varphi(y)$.

Произведём обратную замену переменных $z_i$ на $x_i$:

$$\begin{aligned} f(x_1,x_2,\ldots,x_n) &= z_1\circ\varphi(z_2)\circ\varphi^2(z_3)\circ\ldots\circ\varphi^{n-1}(z_n)\circ a^n = \\ &= (x_1\circ a^{-1})\circ\varphi(x_2\circ a^{-1})\circ\varphi^2(z_3\circ a^{-1})\circ\ldots\circ\varphi^{n-1}(x_n\circ a^{-1})\circ a^n = \\ &= x_1\circ a^{-1}\circ\varphi(x_2)\circ a^{-1}\circ\varphi^2(z_3)\circ a^{-1}\circ\ldots\circ\varphi^{n-1}(x_n)\circ a^{-1}\circ a^n = \\ &= x_1*\varphi(x_2)*\varphi^2(x_3)*\ldots*\varphi^{n-1}(x_n)*a^n. \end{aligned}$$

Элемент $b=a^n$ принадлежит $X$, причём $\varphi^{n-1}(x)=a^{n-1}\circ x\circ a^{-(n-1)}=a^n*x*a^{-n+2}$. Переходя к операции $*$, заметим, что обратным к элементу $b$ относительно этой операции является элемент $b^{-1}=a^{-n+2}$, так как $a^n*a^{-n+2}=a^n\circ a^{-1}\circ a^{n+2}=a$, причём элемент $a$ является нейтральным элементом (единицей) моноида $(X,*)$. Поэтому $\varphi^{n-1}(x)=b*x*b^{-1}$ и $\varphi(b)=b$ и справедливо представление (3) утверждения теоремы 2.

Обратно, если исходить из представления (3) теоремы 2, то можно доказать существование обертывающего моноида (подробнее см. доказательство теоремы 3 в [8]) и, повторив приведённые выше рассуждения в обратном порядке, показать справедливость представления (2) теоремы 1.

### 3. Группа автотопий сильно зависимых $n$-арных полугрупп

На основании описания строения сильно зависимых $n$-арных полугрупп, полученного в теоремах 1 и 2, и общего описания групп автотопий бесповторной суперпозиции сильно зависимых функций из [12, 13] нетрудно получить описание строения их групп автотопий. Для случая $n$-арных квазигрупп оно получено в работе [14].

Пусть $G=(X,*)$ — моноид, $b\in G^*$ и $\theta\in\mathrm{Aut}(*)$. Рассмотрим операции

$$\begin{aligned} f_*(x_1,\ldots,x_n) &= x_1*\cdots*x_n, \\ f_{\theta,*}(x_1,\ldots,x_n) &= x_1*\theta(x_2)*\theta^2(x_3)*\ldots*\theta^{n-1}(x_n), \\ f_{\theta,*,b}(x_1,\ldots,x_n) &= x_1*\theta(x_2)*\theta^2(x_3)*\ldots*\theta^{n-1}(x_n)*b. \end{aligned}$$

Для действия подстановок на множестве $X$ будем использовать запись, соответствующую правому действию: $\alpha\beta(x)=x^{\alpha\beta}=\beta(\alpha(x))$. Заметим, что $f_*(x)=f^T_{\theta,*}(x)=f_{\theta,*}(x^{T^{-1}})$, где $T=(id,\theta,\theta^2,\ldots,\theta^{n-1},id)$ — главная автотопия, и поэтому

$$\mathrm{Atp}(f_{\theta,*})=T\mathrm{Atp}(f_*)T^{-1}. \tag{4}$$

Действительно, если $\alpha=(\alpha_1,\alpha_2,\ldots,\alpha_n,\alpha_{n+1})\in\mathrm{Atp}(f_*)$, то

$$\begin{gathered} \alpha_{n+1}^{-1}f_{\theta,*}(\alpha_1(x_1),\theta\alpha_1\theta^{-1}(x_2),\ldots,\theta^{n-1}\alpha_n\theta^{1-n}(x_n))= \\ =\alpha_{n+1}^{-1}(\alpha_1(x_1)*\theta(\theta\alpha_1\theta^{-1}(x_2))*\ldots*\theta^{n-1}(\theta^{n-1}\alpha_n\theta^{1-n}(x_n)))= \\ =\alpha_{n+1}^{-1}(\alpha_1(x_1)*\alpha_1(\theta(x_2))*\ldots*\alpha_n(\theta^{n-1}(x_n)))=x_1*\theta(x_2)*\ldots*\theta^{n-1}(x_n)=f_{\theta,*}(x_1,\ldots,x_n). \end{gathered}$$

Группа автотопий операции $f_*(x_1,\ldots,x_n)$ описывается следующим образом:

**Лемма 1** [12]. Пусть $G=(\Omega,*)$ — моноид и $f_*(x_1,\ldots,x_n)=x_1*\cdots*x_n$. Тогда

а) если операция $*$ неабелева, то группа $\mathrm{Atp}\,(f)$ имеет порядок $|G^*|^{n+1}\,|\mathrm{Aut}\,(G)|$ и состоит из преобразований вида $(\alpha_1,\ldots,\alpha_n,\alpha_{n+1})$, где

$$\begin{aligned} \alpha_i(x) &= a_i^{-1}*\xi(x)*a_{i+1}, \qquad i=\overline{1,n}, \\ \alpha_{n+1}(x) &= a_1^{-1}*\xi(x)*a_{n+1}, \end{aligned}$$

при некоторых $a_1,\ldots,a_{n+1}\in G^*$, $\xi\in\mathrm{Aut}\,(G)$;

б) если операция $*$ абелева, то группа $\mathrm{Atp}\,(f)$ имеет порядок $|G^*|^n\,|\mathrm{Aut}\,(G)|$ и состоит из преобразований вида $(\alpha_1,\ldots,\alpha_n,\alpha_{n+1})$, где

$$\alpha_i(x)=\xi(x)*a_i,\quad i=1,\ldots,n,$$
$$\alpha_{n+1}(x)=\xi(x)*a_1*\cdots*a_n$$

при некоторых $a_1,\ldots,a_n\in G^*$, $\xi\in\mathrm{Aut}\,(G)$.

Применяя лемму 1 и равенство (4), получаем описание групп автотопий функции $f_{\theta,*}$.

**Теорема 3.** Пусть $G=(\Omega,*)$ — моноид и $\theta\in\mathrm{Aut}(*)$.

1. Если операция $*$ неабелева, то группа автотопий операции

$$f_{\theta,*}(x_1,\ldots,x_n)=x_1*\theta(x_2)*\theta^2(x_3)*\ldots*\theta^{n-1}(x_n)$$

состоит из таких наборов подстановок $(\alpha_1,\alpha_2,\ldots,\alpha_n,\alpha_{n+1})$, что при некоторых обратимых относительно $*$ элементах $a_1,a_2,\ldots,a_{n+1}\in X$ и $\xi\in\mathrm{Aut}(*)$ выполнены равенства

$$\begin{cases}\alpha_1(x_1)=&a_1^{-1}*\xi(x_1)*a_2,\\ \alpha_2(x_2)=&\theta^{-1}(a_2^{-1}*\xi(\theta(x_2))*a_3),\\ \alpha_3(x_3)=&\theta^{-2}(a_3^{-1}*\xi(\theta^2(x_3)*a_4),\\ &\ldots\\ \alpha_{n-1}(x_{n-1})=&\theta^{2-n}(a_{n-1}^{-1}*\xi(\theta^{n-2}(x_{n-1}))*a_n),\\ \alpha_n(x_n)=&\theta^{1-n}(a_n^{-1}*\xi(\theta^{n-1}(x_n))*a_{n+1}),\\ \alpha_{n+1}(y)=&a_1^{-1}*\xi(y)*a_{n+1}.\end{cases}$$

При этом всякий набор подстановок $(\alpha_1,\ldots,\alpha_n,\alpha_{n+1})$ при произвольных обратимых $a_1,\ldots,a_{n+1}\in G^*$ и $\xi\in\mathrm{Aut}\,(G)$, удовлетворяющий этим равенствам, является автотопией операции $f_{\theta,*}$.

2. Если операция $*$ абелева, то группа автотопий операции $f_{\theta,*}(x_1,\ldots,x_n)$ состоит из таких наборов подстановок $(\alpha_1,\alpha_2,\ldots,\alpha_n,\alpha_{n+1})$, что при некоторых обратимых относительно $*$ элементах $a_1,a_2,\ldots,a_n\in X$ и $\xi\in\mathrm{Aut}(*)$ выполнены равенства

$$\begin{cases}\alpha_1(x_1)=&a_1^{-1}*\xi(x_1)*a_1,\\ \alpha_2(x_2)=&\theta^{-1}(\xi(\theta(x_2))*a_2),\\ \alpha_3(x_3)=&\theta^{-2}(\xi(\theta^2(x_3)*a_3),\\ &\ldots\\ \alpha_{n-1}(x_{n-1})=&\theta^{2-n}(\xi(\theta^{n-2}(x_{n-1}))*a_{n-1}),\\ \alpha_n(x_n)=&\theta^{1-n}(\xi(\theta^{n-1}(x_n))*a_n),\\ \alpha_{n+1}(y)=&\xi(y)*a_1\ldots*a_n.\end{cases}$$

При этом всякий набор подстановок $(\alpha_1,\ldots,\alpha_n)$ при произвольных обратимых $a_1,\ldots,a_n\in G^*$ и $\xi\in\mathrm{Aut}\,(G)$, удовлетворяющий этим равенствам, является автотопией операции $f_{\theta,*}$.

Группы автотопий операции $f_{\theta,*,b}$ описываются аналогично. В силу очевидного равенства $f_{\theta,*,b}=f_{\theta,*}^S$, где $S=(id,\ldots,id,R_b)$, для групп автотопий выполняется соотношение

$$\mathrm{Atp}(f_{\theta,*,b})=S^{-1}\mathrm{Atp}(f_{\theta,*})S.$$

Поэтому описание группы автотопий функции $f_{\theta,*,b}$ отличается тем, что в теореме 3 надо заменить значение подстановки $\alpha_{n+1}(y)$ на $R_b^{-1}\alpha_{n+1}R_b(y)=\alpha_{n+1}(y*b^{-1})*b$.

ЛИТЕРАТУРА


1. *Сохацкий Ф. Н.* Об ассоциативности многоместных операций // Дискретная математика. 1992. Т. 4. № 1. С. 66–84.
2. *Сосинский Л. М.* О представлении функций бесповторными суперпозициями в трехзначной логике // Проблемы кибернетики. М.: Наука, 1964. Вып. 12. С. 57–68.
3. *Белоусов В. Д.* $n$-Арные квазигруппы. Кишинев: Штиинца, 1972. 277 с.
4. *Черемушкин А. В.* Некоторые асимптотические оценки для класса сильно зависимых функций // Вестник Томского госуниверситета. Приложение. 2006. № 17. С. 87–94.
5. *Черемушкин А. В.* Аналоги теорем Глускина — Хоссу и Малышева для сильно зависимых $n$-арных операций // Дискретная математика, 2018. Т. 30. Вып. 2. С. 15–24.
6. *Bruck R. H.* A survey of binary systems. Berlin; Heidelberg; New York: Springer, 1958. 185 p.
7. *Post E. L.* Polyadic groups // Trans. Amer. Math. Soc. 1940. V. 48. No. 2. P. 208–350.
8. *Черемушкин А. В.* Теорема Поста для сильно зависимых $n$-арных полугрупп // Дискретная математика. 2019. Т. 31. № 2. С. 153–158.
9. *Глускин Л. М.* Позиционные оперативы // Математич. сборник. 1965. Т. 68 (110). № 3. С. 444–472.
10. *Hosszu M.* On the explicit form of $n$-group operations // Publ. Math. 1963. V. 10. No. 1–4. P. 88–92.
11. *Гальмак А. М., Воробьев Г. Н.* О теореме Поста — Глускина — Хоссу // Проблемы физики, математики и техники. 2013. Вып. 1(14). С. 55–59.
12. *Черемушкин А. В.* Бесповторная декомпозиция сильно зависимых функций // Дискретная математика. 2004. Т. 16. Вып. 3. С. 3–42.
13. *Черемушкин А. В.* Декомпозиция и классификация дискретных функций. М.: Курс, 2018. 288 с.
14. *Khodabandeh H. and Shahryari M.* On the automorphisms and representations of polyadic groups // Commun. Algebra. 2012. V. 40. No. 6. P. 2199–2212.


УДК 519.728 DOI 10.17223/2226308X/12/11

# МИНИМАЛЬНОЕ ПРЕДСТАВИТЕЛЬНОЕ МНОЖЕСТВО ДЛЯ СИСТЕМЫ ЧАСТОТНЫХ КЛАССОВ НЕДООПРЕДЕЛЁННЫХ СЛОВ

Л. А. Шоломов

Частотный класс недоопределённых слов — это множество всех слов в некотором недоопределённом алфавите, имеющих заданную длину и заданные частоты вхождения символов. Рассматривается задача доопределения произвольной системы частотных классов. Предложен метод выделения из этой системы минимальной по мощности подсистемы, такой, что достаточно получить доопределения для классов этой подсистемы, а по ним доопределения других классов системы находятся просто.

**Ключевые слова:** *недоопределённые данные, доопределение, частотный класс, представительное множество.*

Пусть $M = \{0, 1, \ldots, m-1\}$ и выделена система $\mathcal{T} \subseteq 2^M$ некоторых непустых подмножеств $T \subseteq M$. С множеством $M$ связан алфавит $A_0 = \{a_i : i \in M\}$ *основных* символов, с множеством $\mathcal{T}$ — алфавит $A = \{a_T : T \in \mathcal{T}\}$ *недоопределённых* символов. *Доопределением символа* $a_T$ считается всякий основной символ $a_i$, $i \in T$, *доопределением слова* $v$ в алфавите $A$ — любое слово, полученное из $v$ заменой каждого символа каким-либо его доопределением, а *доопределением множества* $V$ слов в алфавите $A$ —

любое множество слов в алфавите $A_0$, содержащее для каждого слова $v \in V$ некоторое его доопределение. Символ $a_M$, доопределимый любым основным символом, называется *неопределённым* и обозначается $*$. Подробнее о недоопределённых данных в [1].

Будем говорить, что недоопределённый символ $a_T$ *чётче символа* $a_{T'}$, если $T \subseteq T'$, и что слово $v = a_{T_1} \dots a_{T_l}$ *чётче слова* $v' = a_{T'_1} \dots a_{T'_l}$, если каждый символ $a_{T_i}$ слова $v$ чётче соответствующего символа $a_{T'_i}$ слова $v'$. Ясно, что если $v$ чётче $v'$, то любое доопределение слова $v$ доопределяет $v'$.

Для заданного набора $\mathbf{r} = (r_T : T \in \mathcal{T})$ натуральных чисел положим $l = \sum\limits_{T \in \mathcal{T}} r_T$ и обозначим через $\mathcal{K}_l(\mathbf{r})$ класс всех слов длины $l$ в алфавите $A$, в которых каждый символ $a_T$ встречается $r_T$ раз (т. е. с частотой $r_T/l$). Такие классы называют *частотными*.

Скажем, что класс $\mathcal{K}_{l_1}(\mathbf{r}_1)$ *представительнее* класса $\mathcal{K}_{l_2}(\mathbf{r}_2)$, если $l_1 \geqslant l_2$ и, каково бы ни было доопределение $\mathcal{D}_{l_1}(\mathbf{r}_1)$ класса $\mathcal{K}_{l_1}(\mathbf{r}_1)$, множество $\mathcal{D}_{l_1}(\mathbf{r}_1)|_{l_2}$ начал длины $l_2$ слов, входящих в $\mathcal{D}_{l_1}(\mathbf{r}_1)$, образует некоторое доопределение класса $\mathcal{K}_{l_2}(\mathbf{r}_2)$. Отметим, что если в качестве возможных доопределений для $\mathcal{K}_{l_2}(\mathbf{r}_2)$ использовать вместо начал слов из $\mathcal{D}_{l_1}(\mathbf{r}_1)$ другие их фрагменты, расположенные в $l_2$ различных фиксированных разрядах, это не повлияет на введённое понятие, поскольку частотные классы замкнуты относительно перестановок символов в словах.

Пусть $\mathfrak{K}$ — некоторая конечная система частотных классов, заданная перечислением параметров $(l, \mathbf{r})$ входящих в неё классов $\mathcal{K}_l(\mathbf{r})$. Подсистему $\mathfrak{M} \subseteq \mathfrak{K}$ назовём *представительным множеством системы* $\mathfrak{K}$, если для любого $\mathcal{K}_l(\mathbf{r}) \in \mathfrak{K}$ в $\mathfrak{M}$ имеется класс, который представительнее $\mathcal{K}_l(\mathbf{r})$. Представительное множество $\mathfrak{M}$ называется *минимальным*, если не существует представительного множества для $\mathfrak{K}$, содержащего меньшее число частотных классов.

Цель данной работы — построение минимального представительного множества для заданной системы частотных классов. Такая задача возникает в некоторых методах сжатия недоопределённых данных и реализации недоопределённых функций (см., например, [2]). Они обобщают подход Э. И. Нечипорука [3]. Эти методы требуют нахождения доопределений для всех частотных классов подходящей системы. Решение задачи упрощается за счёт сведения к задаче доопределения минимального представительного множества этой системы.

Пусть заданы классы $\mathcal{K}_{l_1}(\mathbf{r}_1)$ и $\mathcal{K}_{l_2}(\mathbf{r}_2)$, $l_1 \geqslant l_2$, и требуется выяснить, является ли $\mathcal{K}_{l_1}(\mathbf{r}_1)$ более представительным. Образуем класс $\mathcal{K}_{l_1}(\mathbf{r}_2^+)$, слова которого получены из слов класса $\mathcal{K}_{l_2}(\mathbf{r}_2)$ добавлениями $l_1 - l_2$ символов $*$. Компоненты $r_{2,T}$ и $r'_{2,T}$ наборов $\mathbf{r}_2$ и $\mathbf{r}_2^+$ связаны соотношениями $r'_{2,*} = r_{2,*} + l_1 - l_2$ и $r'_{2,T} = r_{2,T}$, $a_T \neq *$.

**Лемма 1.** Класс $\mathcal{K}_{l_1}(\mathbf{r}_1)$ представительнее $\mathcal{K}_{l_2}(\mathbf{r}_2)$ тогда и только тогда, когда найдётся пара слов $(v, v')$, $v \in \mathcal{K}_{l_1}(\mathbf{r}_1)$, $v' \in \mathcal{K}_{l_1}(\mathbf{r}_2^+)$, в которой $v$ чётче $v'$.

***Доказательство.*** Пусть такая пара $(v, v')$ существует. Рассмотрим произвольное слово $w$ класса $\mathcal{K}_{l_2}(\mathbf{r}_2)$. Образуем слово $w' \in \mathcal{K}_{l_1}(\mathbf{r}_2^+)$ путём дописывания к $w$ в конце $l_1 - l_2$ символов $*$. Найдётся перестановка $\sigma$ символов слова $w'$, для которой $\sigma(w') = v'$. Построим слово $u = \sigma^{-1}(v)$. Оно чётче $w'$ и принадлежит классу $\mathcal{K}_{l_1}(\mathbf{r}_1)$. Любое доопределение слова $u$ доопределяет $w'$, а его начало длины $l_2$ доопределяет $w$.

Допустим теперь, что пара $(v, v')$ с указанным свойством отсутствует, т. е. для любых $v \in \mathcal{K}_{l_1}(\mathbf{r}_1)$ и $v' \in \mathcal{K}_{l_1}(\mathbf{r}_2^+)$ слово $v$ не чётче $v'$. Возьмём некоторое слово $w \in \mathcal{K}_{l_2}(\mathbf{r}_2)$ и образуем из него слово $v' \in \mathcal{K}_{l_1}(\mathbf{r}_2^+)$ приписыванием $l_1 - l_2$ символов $*$. Всякое слово $v \in \mathcal{K}_{l_1}(\mathbf{r}_1)$ не чётче $v'$, а потому в нём присутствует символ $a_{T_i}$, хотя бы одно из доопределений которого не доопределяет соответствующий символ $a_{T'_i}$ слова $v'$. По-

скольку последними $l_1 - l_2$ символами слова $v'$ являются $*$, символ $a_{T_i}$ принадлежит началу слова $v$. Это означает возможность доопределить слово $v$ так, чтобы начало этого доопределения не являлось доопределением слова $w$. В силу произвольности слова $v \in \mathcal{K}_{l_1}(\mathbf{r}_1)$ отсюда следует существование для класса $\mathcal{K}_{l_1}(\mathbf{r}_1)$ такого доопределения, среди начал слов которого нет доопределений слова $w \in \mathcal{K}_{l_2}(\mathbf{r}_2)$, а потому $\mathcal{K}_{l_1}(\mathbf{r}_1)$ не представительнее класса $\mathcal{K}_{l_2}(\mathbf{r}_2)$. ■

Пусть, как и раньше, $\mathbf{r}_1 = (r_{1,T} : T \in \mathcal{T}_1)$, $\mathbf{r}_2^+ = (r'_{2,T'} : T' \in \mathcal{T}_2)$, где

$$\sum_{T \in \mathcal{T}_1} r_{1,T} = \sum_{T' \in \mathcal{T}_2} r'_{2,T'} = l_1.$$

Построим ориентированную потоковую сеть [4] с полюсами $s$ (источник) и $t$ (сток), с внутренними вершинами $\alpha_T$, $T \in \mathcal{T}_1$, и $\beta_{T'}$, $T' \in \mathcal{T}_2$, с дугами $(s, \alpha_T)$, имеющими пропускные способности $r_{1,T}$, с дугами $(\beta_{T'}, t)$, имеющими пропускные способности $r'_{2,T'}$, а также с дугами $(\alpha_T, \beta_{T'})$, $T \subseteq T'$, обладающими достаточно большими пропускными способностями (например, равными $l_1$).

**Лемма 2.** Пара слов $(v, v')$, такая, что $v \in \mathcal{K}_{l_1}(\mathbf{r}_1)$, $v' \in \mathcal{K}_{l_1}(\mathbf{r}_2^+)$ и $v$ чётче $v'$, существует тогда и только тогда, когда максимальный поток в построенной сети равен $l_1$.

***Доказательство.*** Пусть максимальный поток равен $l_1$. Поскольку совокупность дуг $(s, \alpha_T)$, $T \in \mathcal{T}_1$, образует разрез, из равенства $\sum\limits_T r_{1,T} = l_1$ следует, что в каждой из них поток совпадает с пропускной способностью $r_{1,T}$. Аналогичные рассуждения показывают, что и в дугах $(\beta_{T'}, t)$, $T' \in \mathcal{T}_2$, достигается пропускная способность $r'_{2,T'}$.

Обозначим через $z_{TT'}$ поток в дуге $(\alpha_T, \beta_{T'})$. В соответствии с теоремой Форда — Фалкерсона величины $z_{TT'}$ можно считать целыми. По набору чисел $z_{TT'}$, где $T \in \mathcal{T}_1$, $T' \in \mathcal{T}_2$, $T \subseteq T'$, образуем слова $v$ и $v'$ так, чтобы в них имелось ровно $z_{TT'}$ позиций, в которых в слове $v$ находится символ $a_T$, а в слове $v'$ — символ $a_{T'}$. Из конструкции сети и сказанного выше о достижимости в дугах $(s, \alpha_T)$ и $(\beta_{T'}, t)$ пропускных способностей следует, что $\sum\limits_{T'} z_{TT'} = r_{1,T}$, $\sum\limits_T z_{TT'} = r'_{2,T'}$, а потому $v \in \mathcal{K}_{l_1}(\mathbf{r}_1)$, $v' \in \mathcal{K}_{l_1}(\mathbf{r}_2^+)$. Кроме того, $v$ очевидно чётче $v'$ и, следовательно, пара слов $(v, v')$ обладает требуемыми свойствами.

Эти рассуждения допускают обращение. По паре $(v, v')$ с указанными свойствами может быть построен поток, равный $l_1$, который максимален. ■

**Лемма 3.** Существует полиномиальный алгоритм выяснения по наборам параметров $(l_1, \mathbf{r}_1)$ и $(l_2, \mathbf{r}_2)$, является ли класс $\mathcal{K}_{l_1}(\mathbf{r}_1)$ более представительным, чем $\mathcal{K}_{l_2}(\mathbf{r}_2)$.

***Доказательство.*** Если $l_1 < l_2$, то ответ отрицателен. Дальше считаем $l_1 \geqslant l_2$.

Образуем из $\mathbf{r}_2$ набор $\mathbf{r}_2^+$ заменой компоненты $r_{2,*}$ на $r_{2,*} + l_1 - l_2$ и построим по $(l_1, \mathbf{r}_1)$ и $(l_2, \mathbf{r}_2^+)$ потоковую сеть описанным выше способом. Применением полиномиального алгоритма найдём в ней максимальный поток [4]. Из лемм 1 и 2 следует, что класс $\mathcal{K}_{l_1}(\mathbf{r}_1)$ представительнее $\mathcal{K}_{l_2}(\mathbf{r}_2)$ тогда и только тогда, когда этот поток равен $l_1$. ■

**Теорема 1.** Для любой системы $\mathfrak{K}$ частотных классов имеется единственное минимальное представительное множество $\mathfrak{M}$. Оно может быть найдено со сложностью, ограниченной полиномом от максимальной длины $l$ слов из $\mathfrak{K}$.

***Доказательство.*** Отношение представительности частотных классов — частичный порядок. В конечной системе $\mathfrak{K}$ частотных классов имеется единственная подсистема классов, максимальных по этому отношению, которая и образует минимальное

представительное множество. Оно может быть найдено путём попарного сравнения частотных классов системы $\mathfrak{K}$ по отношению представительности с использованием леммы 3. Мощность системы $\mathfrak{K}$ ограничена числом частотных классов с длиной слов не выше $l$, которое не превосходит $l^{|A|}$, где $|A|$ — мощность алфавита $A$, а число пар классов из $\mathfrak{K}$ не больше $l^{2|A|}$. Поскольку $|A|$ — константа, а трудоёмкость сравнения одной пары по представительности полиномиальна, процедура выделения минимального представительного множества полиномиальна по $l$. ■

ЛИТЕРАТУРА

1. *Шоломов Л. А.* Элементы теории недоопределённой информации // Прикладная дискретная математика. Приложение. 2009. № 2. С. 18–42.
2. *Шоломов Л. А.* О функционалах, характеризующих сложность систем недоопределенных булевых функций // Проблемы кибернетики. Вып. 19. М.: Физматлит, 1967. С. 123–139.
3. *Нечипорук Э. И.* О сложности вентильных схем, реализующих булевские матрицы с неопределенными элементами // ДАН СССР. 1965. Т. 163. № 1. С. 40–42.
4. *Адельсон-Вельский Г. М., Диниц Е. А., Карзанов А. В.* Потоковые алгоритмы. М.: Наука, 1975.

UDC 512.772.7 DOI 10.17223/2226308X/12/12

## CHARACTERISTIC POLYNOMIALS OF THE CURVE $y^2 = x^7 + ax^4 + bx$ OVER FINITE FIELDS

S. A. Novoselov[1], Y. F. Boltnev

In this work, we list all possible characteristic polynomials of the Frobenius endomorphism for genus 3 hyperelliptic curves of type $y^2 = x^7 + ax^4 + bx$ over finite field $\mathbb{F}_q$ of characteristic $p > 3$.

**Keywords:** *hyperelliptic curves, characteristic polynomials, point-counting, genus* 3.

### Introduction

Let $\mathbb{F}_q$ be a finite field of size $q = p^n$, $p > 2$. In this note, we study the hyperelliptic curves of genus $g = 3$ of the form

$$C : y^2 = x^{2g+1} + ax^{g+1} + bx.$$

The Jacobian $J_C$ of the curves is split [1] over certain finite field extension:

$$J_C \sim J_{D_1} \times J_{D_2},$$

where $D_1$ and $D_2$ are explicitly given curves. This fact allows us to reduce the problem of point-counting on the curve $C$ to counting points on the curves $D_1$ and $D_2$.

For genus 2 case it was done in the works [2, 3]. The work [1] contains algorithms for $g > 2$ case. In this work, we give explicit formulae for the number of points on the Jacobian in the case of $g = 3$.

The point-counting on the curve is equivalent to finding of zeta-function of the curve

$$Z(C/\mathbb{F}_q; T) = \exp\left(\sum_{k=1}^{\infty} \#C(\mathbb{F}_{q^k})\frac{T^k}{k}\right) = \frac{L_{C,q}(T)}{(1-T)(1-qT)},$$

[1]The author is supported by RFBR according to the research project No. 18-31-00244.

where $L_{C,q}(T) = q^g T^{2g} + a_1 q^{g-1} T^{2g-1} + \ldots + a_g T^g + a_{g-1} T^{g-1} + \ldots + a_1 T + 1$ and $a_i \in \mathbb{Z}$, $|a_i| \leqslant \binom{2g}{i} q^{i/2}$ for $i = 1, \ldots, g$.

Let $\chi_{C,q}(T)$ be a characteristic polynomial of the Frobenius endomorphism. Then $L_{C,q}(T) = T^{2g}\chi_{C,q}(1/T)$ and $\#J_C(\mathbb{F}_q) = L_{C,q}(1) = \chi_{C,q}(1)$. Therefore, the computation of $\#J_C(\mathbb{F}_q)$ is equivalent to the computation of the characteristic polynomial.

In this work, we enumerate all possible characteristic polynomials for the curve $C$ in the case of $g = 3$.

## 1. Characteristic polynomials for genus 3 curves

Let $C : y^2 = x^7 + ax^4 + bx$ be a genus 3 hyperelliptic curve defined over a finite field $\mathbb{F}_q$, $q = p^n$, $p > 3$. Since, there is a map

$$(x, y) \mapsto (x^3, xy)$$

from $C$ to an elliptic curve $E_1 : y^2 = x^3 + ax^2 + bx$, we have

$$J_C \sim E_1 \times A$$

over $\mathbb{F}_q$ for some abelian surface $A$. Therefore,

$$\chi_{C,q}(T) = \chi_{E_1,q}(T)\chi_{A,q}(T).$$

The characteristic polynomial for $E_1$ can be efficiently computed using SEA-algorithm [4]. So, we only have to determine the coefficients of $\chi_{A,q}(T) = T^4 - b_1 T^3 + b_2 T^2 - b_1 q T + q^2$.

From [1, Th. 2], we have

$$J_C \sim E_2 \times J_D$$

over $\mathbb{F}_q[\sqrt[3]{b}]$, where $E_2$ is an elliptic curve with equation

$$y^2 = x^3 - 3\sqrt[3]{b}x + a$$

and $D$ is a hyperelliptic curve with equation

$$y^2 = (x^2 - 4\sqrt[3]{b})(x^3 - 3\sqrt[3]{b}x + a).$$

Moreover, the Jacobian $J_D$ is also split, since $E_1 \not\sim E_2$ in general.

First we describe the characteristic polynomials in the simplest case when $b$ is a cubic residue. In this case for each cubic root, we have a map to an elliptic curve, so we obtain the following theorem.

**Theorem 1.** Let $C : y^2 = x^7 + ax^4 + bx$ be a genus 3 hyperelliptic curve defined over a finite field $\mathbb{F}_q$, $q = p^n$, $p > 3$, and let $b$ be a cubic residue. Then

1) if $q \equiv 1 \pmod 6$, then $J_C \sim E_1 \times E_2^2$ over $\mathbb{F}_q$ and

$$\chi_{C,q}(T) = (T^2 - t_1 T + q)(T^2 - t_2 T + q)^2,$$

where $E_1 : y^2 = x^3 + ax^2 + bx$, $E_2 : y^2 = x^3 - 3\sqrt[3]{b}x + a$ are elliptic curves and $t_1, t_2$ are their traces of the Frobenius endomorphism;

2) if $q \equiv 5 \pmod 6$, then $J_C \sim E_1 \times E_2 \times \tilde{E}_2$ over $\mathbb{F}_q$ and

$$\chi_{C,q}(T) = (T^2 - t_1 T + q)(T^2 - t_2 T + q)(T^2 + t_2 T + q),$$

where $\tilde{E}_2$ is a quadratic twist of $E_2$.

In general case, we have $J_C \sim E_1 \times A$, where $A$ can be simple.

**Theorem 2.** Let $C : y^2 = x^7 + ax^4 + bx$ be a genus 3 hyperelliptic curve defined over a finite field $\mathbb{F}_q$, $q = p^n$, $p > 3$. Then

1) $J_C \sim E_1 \times A$ over $\mathbb{F}_q$, where $E_1$ is an elliptic curve with equation $y^2 = x^3 + ax^2 + bx$ and $A$ is an abelian surface;
2) if $q \equiv 5 \pmod 6$, we have $J_C \sim E_1 \times E_2 \times \tilde{E}_2$ and

$$\chi_{C,q}(T) = (T^2 - t_1T + q)(T^2 - t_2T + q)(T^2 + t_2T + q),$$

where $E_1, E_2, t_1, t_2$ are the same as in Theorem 1;
3) if $q \equiv 1 \pmod 6$ and $\sqrt[3]{b} \in \mathbb{F}_q$, then $J_C \sim E_1 \times E_2^2$ over $\mathbb{F}_q$ and

$$\chi_{C,q}(T) = (T^2 - t_1T + q)(T^2 - t_2T + q)^2;$$

4) if $q \equiv 1 \pmod 6$, $\sqrt[3]{b} \notin \mathbb{F}_q$ and $E_2$ is ordinary, then $\chi_{C,q}(T) = (T^2 - t_1T + q)\chi_A(T)$, where $\chi_A(T)$ is one of the following polynomials:
   - $(T^4 - \tilde{t}_2T^3 + (\tilde{t}_2^2 - q)T^2 - \tilde{t}_2qT + q^2)$, $\sqrt{b} \notin \mathbb{F}_q$;
   - $(T^4 + \tilde{t}_2T^3 + (\tilde{t}_2^2 - q)T^2 + \tilde{t}_2qT + q^2)$, $\sqrt{b} \in \mathbb{F}_q$;
   - $(T^4 - 2\tilde{t}_2T^3 + (\tilde{t}_2^2 + 2q)T^2 - 2\tilde{t}_2qT + q^2)$, $\sqrt{b} \notin \mathbb{F}_q$, $A$ is split;
   - $(T^4 + 2\tilde{t}_2T^3 + (\tilde{t}_2^2 + 2q)T^2 + 2\tilde{t}_2qT + q^2)$, $\sqrt{b} \in \mathbb{F}_q$, $A$ is split.

   Here, $\tilde{t}_2$ is a trace of Frobenius of elliptic curve $\tilde{E}_2 : y^2 = x^3 - 3bx + ab$;
5) if $q \equiv 1 \pmod 6$, $\sqrt[3]{b} \notin \mathbb{F}_q$ and $E_2$ is supersingular, then $A$ is supersingular and $\chi_{C,q}(T) = (T^2 - t_1T + q)\chi_{A,q}(T)$ where $\chi_{A,q}(T)$ is one of the following polynomials:
   - $(T^4 - qT^2 + q^2)$;
   - $(T^4 + 2qT^2 + q^2)$;
   - $(T^2 + q)(T \pm \sqrt{q})^2$, $p \equiv 7 \pmod{12}$, $n$ is even, $A$ is split;
   - $(T \pm \sqrt{q})^2$, $n$ is even, $A$ is split;
   - $(T^2 \pm T\sqrt{q} + q)^2$, $n$ is even, $A$ is simple;
   - $(T^4 + \sqrt{q}T^3 + qT^2 + q^{3/2}T + q^2)$, $p \not\equiv 1 \pmod 5$, $n$ is even, $A$ is simple;
   - $(T^4 - \sqrt{q}T^3 + qT^2 - q^{3/2}T + q^2)$, $p \not\equiv 1 \pmod{10}$, $n$ is even, $A$ is simple.

## Conclusion

In this work, we obtained the complete list of the characteristic polynomials for the genus 3 curve $y^2 = x^7 + ax^4 + bx$ in terms of traces of Frobenius of certain elliptic curves. Since $\#J_C(\mathbb{F}_q) = \chi_{C,q}(T)$, this gives us the explicit formulae for the number of points on the Jacobian.

## REFERENCES

1. *Novoselov S. A.* Counting Points on Hyperelliptic Curves of Type $y^2 = x^{2g+1} + ax^{g+1} + bx$. `https://arxiv.org/abs/1902.05992`. 2019.
2. *Satoh T.* Generating genus two hyperelliptic curves over large characteristic finite fields. LNCS, 2009, vol. 5479, pp. 536–553.
3. *Guillevic A. and Vergnaud D.* Genus 2 hyperelliptic curve families with explicit Jacobian order evaluation and pairing-friendly constructions. LNCS, 2012, vol. 7708, pp. 234–253.
4. *Schoof R.* Counting points on elliptic curves over finite fields. J. de théorie des nombres de Bordeaux, 1995, vol. 7, no. 1, pp. 219–254.

Секция 2

# ДИСКРЕТНЫЕ ФУНКЦИИ

УДК 519.7 DOI 10.17223/2226308X/12/13

## ПЕРЕМЕШИВАЮЩИЕ СВОЙСТВА НЕКОТОРЫХ КЛАССОВ ПОДСТАНОВОК НА $\mathbb{F}_2^n$[1]

Л. А. Карпова, И. А. Панкратова

Рассматриваются два класса подстановок на $\mathbb{F}_2^n$, таких, что каждая их координатная функция существенно зависит ровно от $k$ переменных. Приведены алгоритм вычисления матэкса перемешивающей матрицы функций из данных классов и результаты экспериментального исследования их перемешивающих свойств.

**Ключевые слова:** *существенная зависимость функции от переменной, перемешивающие свойства функций, элементарный экспонент, матэкс.*

Для $n \in \mathbb{N}$ обозначим через $\mathcal{F}_{n,k}$ класс функций $F : \mathbb{F}_2^n \to \mathbb{F}_2^n$, где $F = (f_1 \dots f_n)$, таких, что координатные функции $f_i : \mathbb{F}_2^n \to \mathbb{F}_2$, $i = 1, \dots, n$, существенно зависят ровно от $k$ переменных. В [1] описаны два метода построения таких функций.

При использовании подстановок в качестве раундовых преобразований в итеративных блочных шифрах важно оценить их «перемешивающие» свойства [2], т. е. распространение существенной зависимости выходных переменных каждого раунда от входов первого раунда. В данной работе рассматриваются перемешивающие свойства функций двух подклассов класса $\mathcal{F}_{n,k}$. Под умножением матриц понимается их логическое умножение — с дизъюнкцией и конъюнкцией в качестве операций сложения и умножения соответственно.

### 1. Основные определения

**Определение 1** [2]. *Перемешивающей матрицей* функции $F : \mathbb{F}_2^n \to \mathbb{F}_2^n$, $F(x_1, \dots, x_n) = (f_1(x_1, \dots, x_n), \dots, f_n(x_1, \dots, x_n))$, называется булева матрица $M(F) = (m_{ij})$ порядка $n$, где $m_{ij} = 1$, если и только если координатная функция $f_j$ существенно зависит от переменной $x_i$.

**Определение 2** [3]. Булева матрица $M$ называется *положительной* ($M > 0$), если все её элементы равны 1; она называется *примитивной*, если $M^t > 0$ при некотором $t \in \mathbb{N}$; наименьшее $t$ с таким свойством называется *экспонентом матрицы* $M$, обозначается $\exp M$; для непримитивной матрицы $M$ будем считать $\exp M = \infty$.

**Определение 3** [4]. Пусть $M$ — булева матрица порядка $n$ и $i, j \in \{1, \dots, n\}$. *Элементарным экспонентом* (*$(i,j)$-экспонентом*) матрицы $M$ называется наименьшее число $\gamma$, такое, что для любого $t > \gamma$ элемент $m_{ij}^{(t)}$ матрицы $M^t$ равен 1; обозначается $(i,j)\text{-}\exp M$. Матрица элементарных экспонентов $\mathfrak{M}(M) = \big((i,j)\text{-}\exp M\big)$ порядка $n$ называется *матэксом матрицы* $M$.

[1]Работа поддержана грантом РФФИ, проект № 17-01-00354.

Проясним связь степени перемешивающей матрицы функции $F$ и существенной зависимости выходов многораундового шифра от входов первого раунда при использовании $F$ в качестве раундового преобразования. Если $m_{ij}^{(t)} = 0$ в матрице $(M(F))^t = \left(m_{ij}^{(t)}\right)$, то $j$-й выход $t$-го раунда не зависит от переменной $x_i$; если $m_{ij}^{(t)} = 1$, то не обязательно такая зависимость есть. Таким образом, $(i,j)$-$\exp M(F)$ — это оценка снизу количества раундов, после которых $j$-й выход зависит от переменной $x_i$, так же как $\exp M(F)$ — оценка снизу количества раундов, при котором достигается полное перемешивание (существенная зависимость всех выходов от всех входных переменных).

**Пример 1.** Пусть $F(x_1, x_2, x_3) = (x_2 \oplus x_3, x_1 \oplus x_3, x_3)$. Тогда

$$M(F) = \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 1 & 1 & 1 \end{pmatrix}, \quad (M(F))^2 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 1 & 1 & 1 \end{pmatrix},$$

$m_{31}^{(2)} = m_{32}^{(2)} = 1$, но после второго раунда имеем $F(F(x_1, x_2, x_3)) = (x_1 \oplus x_3 \oplus x_3, x_2 \oplus \oplus x_3 \oplus x_3, x_3) = (x_1, x_2, x_3)$ — зависимости первого и второго выходов от $x_3$ нет.

## 2. Класс функций $S_{n,k}$

В [1, 5] предложен следующий метод построения функций $F(x_1, \ldots, x_n) = (f_1(x_1, \ldots, x_n), \ldots, f_n(x_1, \ldots, x_n)) \in \mathcal{F}_{n,k}$:

1) строим функцию $G(x_1, \ldots, x_k) = (g_1(x_1, \ldots, x_k), \ldots, g_k(x_1, \ldots, x_k)) \in \mathcal{F}_{k,k}$ (например, способом, описанным в [6]);
2) для $i = 1, \ldots, k$ полагаем $f_i(x_1, \ldots, x_n) = g_i(x_1, \ldots, x_k)$, переменные $x_{k+1}, \ldots, x_n$ фиктивны для $f_i$;
3) для $i = k+1, \ldots, n$ полагаем $f_i(x_1, \ldots, x_n) = x_i \oplus h_i(x_1, \ldots, x_{i-1})$, где $h_i$ — любая функция, существенно зависящая от любых $(k-1)$ переменных из $x_1, \ldots, x_{i-1}$.

В [5] доказано, что полученная функция $F$ является подстановкой на $\mathbb{F}_2^n$.

Обозначим $S_{n,k}$ класс функций, которые можно построить таким способом. По построению, каждая координатная функция $f_i$ функции $F \in S_{n,k}$ существенно зависит ровно от $k$ переменных; таким образом, $S_{n,k} \subseteq \mathcal{F}_{n,k}$.

Перемешивающая матрица функции $F \in S_{n,k}$ имеет следующий вид:

$$M(F) = \begin{pmatrix} \overbrace{1\,1\,\ldots\,1}^{k} & 0\,0\,\ldots\,0 \\ 1\,1\,\ldots\,1 & 0\,0\,\ldots\,0 \\ \ldots & \ldots \\ 1\,1\,\ldots\,1 & 0\,0\,\ldots\,0 \\ *\;*\;\ldots\;* & 1\,0\,\ldots\,0 \\ *\;*\;\ldots\;* & *\,1\,\ldots\,0 \\ \ldots & \ldots \\ *\;*\;\ldots\;* & *\;*\;\ldots\,1 \end{pmatrix}.$$

Здесь $m_{ij} = 1$ для всех $i, j \leqslant k$; $m_{ij} = 0$ для всех $i \leqslant k$, $j > k$; $m_{ii} = 1$ для всех $i = 1, \ldots, n$; в позициях, отмеченных «$*$», могут быть как нули, так и единицы (по $k$ единиц в каждой строке). Таким образом, при всех $t \in \mathbb{N}$ для матрицы $(M(F))^t = \left(m_{ij}^{(t)}\right)$ выполняется $m_{ij}^{(t)} = 0$ для всех $i \leqslant k$, $j > k$, поэтому матрица $M(F)$ непримитивная и $\exp M(F) = \infty$.

Оценим элементарные экспоненты матрицы $M(F)$. Из [7] (утверждение $1, a$ при $I = \{i\}$, $J = \{j\}$) следует, что если $a_{ii} = 1$ или $a_{jj} = 1$ в матрице $A = (a_{ij})$ и $a_{ij}^{(\gamma)} = 1$ в матрице $A^\gamma = \left(a_{ij}^{(\gamma)}\right)$, причём $\gamma$ — минимальное с таким условием, то $(i, j)$-$\exp A = \gamma$. В матрице $M(F)$ все диагональные элементы единичные, поэтому при возведении матрицы в степень единицы в ней ведут себя «монотонно»: если $m_{ij}^{(k)} = 1$ в матрице $(M(F))^k$, то $m_{ij}^{(t)} = 1$ в матрице $(M(F))^t$ для всех $t \geqslant k$. Получаем алгоритм 1 вычисления матэкса матрицы $M(F)$, который состоит в возведении матрицы в степень до тех пор, пока в ней не перестанут появляться новые единицы.

**Алгоритм 1.** Вычисление матэкса матрицы с единичной диагональю

**Вход:** $M = (m_{ij})$ — булева матрица порядка $n$; $m_{ii} = 1$ для всех $i = 1, \ldots, n$.
**Выход:** $\mathfrak{M}(M) = (r_{ij})$.

1: **Для** $i = 1, \ldots, n$
2: **Для** $j = 1, \ldots, n$

$$r_{ij} := \begin{cases} 1, & m_{ij} = 1, \\ \infty & \text{иначе.} \end{cases}$$

3: $C := M$.
4: **Для** $k = 2, 3, \ldots$
5: $B := C$; $C := BM$; $D := B \oplus C$ (поэлементно), пусть $D = (d_{ij})$.
6: **Если** $D$ — нулевая матрица, **то**
выход.
7: **Для** $i = 1, \ldots, n$
8: **Для** $j = 1, \ldots, n$
9: **Если** $d_{ij} = 1$, **то**
$r_{ij} := k$.

Для $\mathfrak{M}(M(F)) = (r_{ij})$ обозначим $\gamma_F = \max\limits_{i,j}\{r_{ij} : r_{ij} \neq \infty\}$ — максимальный конечный элементарный экспонент перемешивающей матрицы функции $F$. Содержательный смысл этой величины следующий: при использовании $F$ в качестве раундового преобразования в итеративном блочном шифре для количества раундов $\gamma_F$ достигается максимально возможная «степень перемешивания» — зависимость выходов последнего раунда от входов первого раунда, которая не изменится при увеличении числа раундов.

Алгоритм 1 вычисления матэкса и алгоритм генерации случайной функции класса $S_{n,k}$ реализованы программно. Эксперименты показали, что $\gamma_F$ принимает значения от 2 до 5 для функций $F \in S_{n,k}$ при $n = 4, \ldots, 26$; как и ожидалось, $\gamma_F$ возрастает с ростом разности $n - k$, т. е. с увеличением числа нулей в перемешивающей матрице функции $F$.

## 3. Класс функций $P_{n,k}$

Если $k|n$, то можно предложить следующий способ построения функций $F = (f_1, \ldots, f_n) \in \mathcal{F}_{n,k}$. Пусть $s = n/k$, построим $s$ функций $G_1, \ldots, G_s \in \mathcal{F}_{k,k}$, $G_i = \left(g_1^{(i)}, \ldots, g_k^{(i)}\right)$, $i = 1, \ldots, s$, и положим $f_{tk+i}(x_1, \ldots, x_n) = g_i^{(t+1)}(x_{tk+1}, \ldots, x_{(t+1)k})$, $t = 0, \ldots, s-1$, $i = 1, \ldots, k$. Класс функций, полученных таким способом, будем обозначать $P_{n,k}$. Схема построения функции $F$ приведена на рис. 1, её перемешивающая матрица — на рис. 2.

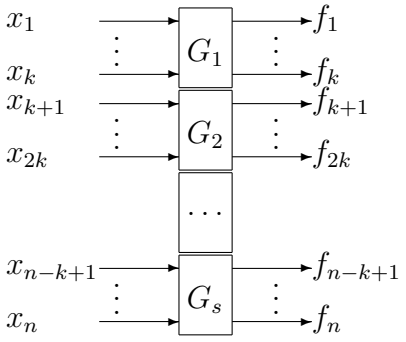


Рис. 1

$$M(F) = \begin{pmatrix} \overbrace{11\dots1}^{k} & 00\dots0 & \dots & 00\dots0 \\ \dots & \dots & \dots & \dots \\ 11\dots1 & 00\dots0 & \dots & 00\dots0 \\ 00\dots0 & 11\dots1 & \dots & 00\dots0 \\ \dots & \dots & \dots & \dots \\ 00\dots0 & 11\dots1 & \dots & 00\dots0 \\ \dots & \dots & \dots & \dots \\ 00\dots0 & 00\dots0 & \dots & 11\dots1 \\ \dots & \dots & \dots & \dots \\ 00\dots0 & 00\dots0 & \dots & 11\dots1 \end{pmatrix}.$$

Рис. 2

Видно, что $(M(F))^t = M(F)$ для всех $t \in \mathbb{N}$, поэтому

$$(i,j)\text{-}\exp M(F) = \begin{cases} 1, & \text{если } m_{ij} = 1, \\ \infty & \text{иначе,} \end{cases}$$

где $M(F) = (m_{ij})$. Для достижения перемешивающих свойств функции класса $P_{n,k}$ можно применять в качестве преобразований замены только в SP-сетях [2, с. 290], чередуя их с преобразованиями перестановки.

## ЛИТЕРАТУРА


1. *Agibalov G. P.* Substitution block ciphers with functional keys // Прикладная дискретная математика. 2017. № 38. С. 57–65.
2. *Фомичев В. М.* Методы дискретной математики в криптологии. М.: Диалог-МИФИ, 2010. 424 с.
3. *Фомичев В. М.* Оценки экспонентов примитивных графов // Прикладная дискретная математика. 2011. № 2(12). С. 101–112.
4. *Фомичев В. М.* О характеристиках локально примитивных орграфов и матриц // Прикладная дискретная математика. Приложение. 2017. № 10. С. 96–99.
5. *Панкратова И. А.* Об обратимости векторных булевых функций // Прикладная дискретная математика. Приложение. 2015. № 8. С. 35–37.
6. *Pankratova I. A.* Construction of invertible vectorial Boolean functions with coordinates depending on given number of variables // Материалы Междунар. науч. конгресса по информатике: Информационные системы и технологии. Республика Беларусь, Минск, 24–27 окт. 2016. Минск: БГУ, 2016. С. 519–521.
7. *Кяжин С. Н., Фомичев В. М.* Локальная примитивность графов и неотрицательных матриц // Прикладная дискретная математика. 2014. № 3. С. 68–80.


УДК 519.7 DOI 10.17223/2226308X/12/14

# О СВОЙСТВАХ БЕНТ-ФУНКЦИЙ, ПОСТРОЕННЫХ ПО НЕКОТОРОЙ БЕНТ-ФУНКЦИИ С ПОМОЩЬЮ ПОДПРОСТРАНСТВ

Н. А. Коломеец

Рассматриваются свойства конструкции $f \oplus \mathrm{Ind}_L$, где $f$ — бент-функция от $2k$ переменных, а $L$ — аффинное подпространство, при определённых условиях порождающей бент-функции. Доказано, что с помощью подпространств размерности $k+1$ конструкция порождает одинаковое число функций и по $f$, и по её дуальной

бент-функции. Приведён ряд экспериментальных результатов для бент-функций от 6 и 8 переменных, отражающих количество порождаемых конструкцией бент-функций, равенство и неравенство этого количества для бент-функции и её дуальной, а также отсутствие бент-функций при подпространствах некоторых размерностей. Усилена теорема 2018 г. о связи подпространств для бент-функций $f$ и $f(x_1, \ldots, x_{2k}) \oplus x_{2k+1}x_{2k+2}$ в контексте рассматриваемой конструкции.

**Ключевые слова:** *булевы функции, бент-функции, подпространства, аффинность.*

Данная работа является продолжением исследований, начатых в [1]. Центральный объект исследований — *бент-функции* [2]. Это булевы функции от чётного числа переменных, обладающие максимальной возможной нелинейностью. В первую очередь они представляют интерес для криптографии. Подробную информацию об этом классе булевых функций можно найти в [3, 4].

Введём необходимые обозначения. Отображение вида $f : \mathbb{F}_2^n \to \mathbb{F}_2$ называется *булевой функцией* от $n$ переменных. Пусть $\langle x, y\rangle = x_1y_1 \oplus \ldots \oplus x_ny_n$, где $x, y \in \mathbb{F}_2^n$. Обозначим через $\mathrm{Ind}_S$ характеристическую булеву функцию множества $S \subseteq \mathbb{F}_2^n$ и через $\mathcal{B}_{2k}$ — множество всех бент-функций от $2k$ переменных. Для любой бент-функции $f \in \mathcal{B}_{2k}$ существует дуальная к ней бент-функция $\widetilde{f} \in \mathcal{B}_{2k}$, определяемая знаками коэффициентов Уолша — Адамара функции $f$.

Как и в [1], в работе исследуются свойства конструкции бент-функций

$$f \oplus \mathrm{Ind}_L, \text{ где } f \in \mathcal{B}_{2k} \text{ и } L \subseteq \mathbb{F}_2^{2k} \text{ — аффинное подпространство.} \tag{1}$$

К. Карле [5] доказал критерий принадлежности $f \oplus \mathrm{Ind}_L$ множеству бент-функций $\mathcal{B}_{2k}$.

Обозначим через $C(f, m)$, где $f \in \mathcal{B}_{2k}$, множество всех бент-функций, порождаемых конструкцией (1) по функции $f$ с помощью аффинных подпространств размерности $m$. Рассмотрим, как связаны мощности $C(f, m)$ и $C(\widetilde{f}, m)$. Во-первых, отметим, что при $m < k$ конструкция не может порождать бент-функции. Во-вторых, размерности $m = 2k$ и $2k - 1$ являются тривиальными, так как для подпространств таких размерностей конструкция порождает бент-функции при любой заданной начальной бент-функции, т. е.

$$|C(f, m)| = |C(\widetilde{f}, m)| \text{ при } m \in \{0, \ldots, k - 1, 2k - 1, 2k\}.$$

Таким образом, нетривиальными размерностями можно считать $m \in \{k, \ldots, 2k - 2\}$.

Из [5] известно взаимно-однозначное соответствие между функциями из $C(f, k)$ и $C(\widetilde{f}, k)$, таким образом, $|C(f, k)| = |C(\widetilde{f}, k)|$. Оказывается, аналогичное утверждение справедливо и для $m = k + 1$.

**Теорема 1.** Пусть $f \in \mathcal{B}_{2k}$. Тогда $|C(f, k + 1)| = |C(\widetilde{f}, k + 1)|$.

Приведём экспериментальные результаты с учётом известной аффинной классификации бент-функций. В табл. 1–4 для функции $f$ указаны $|C(f, m)|$ и $|C(\widetilde{f}, m)|$ при $m \in \{k, \ldots, 2k - 2\}$ (или одно число, если эти мощности совпадают).

Для всех бент-функций из $\mathcal{B}_6$ количество функций в $C(\cdot, m)$ совпадает с $|C(f, m)|$ для некоторой $f$ из табл. 1. Для всех бент-функций из $\mathcal{B}_8$ степени не выше 3 количество функций в $C(\cdot, m)$ совпадает с $|C(f, m)|$ для некоторой $f$ из табл. 2. Начиная уже с 8 переменных, в $C(f, m)$ может не быть функций даже в нетривиальных случаях. Хорошо иллюстрируют это свойство мономиальные функции с показателем Касами (табл. 3).

Отметим, что для всех приведённых в табл. 1–3 функций $f \in \mathcal{B}_{2k}$ и всех $m$ справедливо $|C(f,m)| = |C(\widetilde{f},m)|$. Напомним, что [5] и теорема 1 гарантируют это только при $m = k$ и $m = k+1$. Более того, в классе бент-функций Мэйорана — МакФарланда [6], начиная уже с 8 переменных, есть функции с $|C(f,6)| \neq |C(\widetilde{f},6)|$ (табл. 4).

Таблица 1

| № п/п | Функция $f$ (6 переменных) | 3 | 4 |
|---|---|---|---|
| 1 | $x_1x_2 \oplus x_3x_4 \oplus x_5x_6$ | 1080 | 1260 |
| 2 | $x_1x_2x_3 \oplus x_1x_4 \oplus x_2x_5 \oplus x_3x_6$ | 568 | 364 |
| 3 | $x_1x_2x_3 \oplus x_2x_4x_5 \oplus x_1x_2 \oplus x_1x_4 \oplus x_2x_6 \oplus x_3x_5 \oplus x_4x_5$ | 440 | 140 |
| 4 | $x_1x_2x_3 \oplus x_2x_4x_5 \oplus x_3x_4x_6 \oplus x_1x_4 \oplus x_2x_6 \oplus x_3x_4 \oplus x_3x_5 \oplus x_3x_6 \oplus x_4x_5 \oplus x_4x_6$ | 376 | 28 |

Таблица 2

| № п/п | Функция $f$ (8 переменных) | 4 | 5 | 6 |
|---|---|---|---|---|
| 1 | $x_1x_2 \oplus x_3x_4 \oplus x_5x_6 \oplus x_7x_8$ | 36720 | 91800 | 21420 |
| 2 | $x_1x_2x_3 \oplus x_1x_4 \oplus x_2x_5 \oplus x_3x_6 \oplus x_7x_8$ | 12144 | 16024 | 7084 |
| 3 | $x_1x_2x_3 \oplus x_2x_4x_5 \oplus x_1x_7 \oplus x_2x_6 \oplus x_3x_4 \oplus x_5x_8$ | 6000 | 5272 | 3500 |
| 4 | $x_1x_2x_3 \oplus x_2x_4x_5 \oplus x_1x_3 \oplus x_1x_5 \oplus x_2x_6 \oplus x_3x_4 \oplus x_7x_8$ | 6000 | 4760 | 3500 |
| 5 | $x_1x_2x_7 \oplus x_3x_4x_7 \oplus x_5x_6x_7 \oplus x_1x_4 \oplus x_2x_5 \oplus x_3x_6 \oplus x_4x_5 \oplus x_7x_8$ | 4464 | 3096 | 2604 |
| 6 | $x_1x_2x_3 \oplus x_2x_4x_5 \oplus x_3x_4x_6 \oplus x_1x_6 \oplus x_2x_7 \oplus x_3x_5 \oplus x_4x_8$ | 2928 | 1944 | 1708 |
| 7 | $x_1x_2x_3 \oplus x_2x_4x_5 \oplus x_3x_4x_6 \oplus x_1x_7 \oplus x_2x_5 \oplus x_2x_6 \oplus x_3x_5 \oplus x_4x_8$ | 2928 | 1432 | 1708 |
| 8 | $x_1x_2x_3 \oplus x_2x_4x_5 \oplus x_3x_4x_6 \oplus x_1x_3 \oplus x_1x_4 \oplus x_2x_7 \oplus x_3x_5 \oplus x_6x_8$ | 2928 | 1432 | 1708 |
| 9 | $x_1x_2x_3 \oplus x_2x_4x_5 \oplus x_3x_4x_6 \oplus x_1x_2 \oplus x_1x_3 \oplus x_1x_4 \oplus x_2x_5 \oplus x_2x_6 \oplus \oplus x_3x_5 \oplus x_7x_8$ | 2928 | 1048 | 1708 |
| 10 | $x_1x_2x_3 \oplus x_1x_4x_7 \oplus x_2x_4x_5 \oplus x_3x_4x_6 \oplus x_1x_5 \oplus x_1x_6 \oplus x_2x_7 \oplus x_3x_5 \oplus x_4x_8$ | 1392 | 792 | 812 |

Таблица 3

| Функция $f$ (8 переменных) | 4 | 5 | 6 |
|---|---|---|---|
| $\mathrm{tr}(\alpha x^{57})$, $x \in \mathbb{F}_{2^8}$, $\alpha$ — порождающий элемент $\mathbb{F}_{2^8}^*$ | 493 | 0 | 0 |

Таблица 4

| Функция $f$ (8 переменных) | 4 | 5 | 6 |
|---|---|---|---|
| $\langle x, \pi_1(y)\rangle \oplus \varphi_1(y)$, где $x, y \in \mathbb{F}_2^4$ и<br>$\pi_1 = (9,10,4,3,5,7,11,13,12,14,2,15,1,6,8,0)$,<br>$\varphi_1(y) = y_1y_2y_3 \oplus y_1y_3y_4 \oplus y_2y_3y_4 \oplus y_1y_3 \oplus y_2y_3 \oplus y_2y_4 \oplus y_1 \oplus y_3 \oplus y_4 \oplus 1$ | 1392 | 408 | 300/236 |

Усилим теорему 3 из [1]. Пусть $S \subseteq \mathbb{F}_2^{2k+2}$ и

$$\widehat{S} = \{x \in \mathbb{F}_2^{2k} : (x,a,b) \in S \text{ для некоторых } a,b \in \mathbb{F}_2\}, \quad F_{00}^{2k} = \{(x,0,0) : x \in \mathbb{F}_2^{2k}\}.$$

**Теорема 2.** Пусть для $g(x_1,\ldots,x_{2k+2}) = f(x_1,\ldots,x_{2k}) \oplus x_{2k+1}x_{2k+2} \in \mathcal{B}_{2k+2}$ верно $g \oplus \mathrm{Ind}_{a\oplus U} \in \mathcal{B}_{2k+2}$, где $U \subseteq \mathbb{F}_2^{2k+2}$ — линейное подпространство и $a \in \mathbb{F}_2^{2k+2}$. Тогда существует линейное подпространство $L \subseteq \mathbb{F}_2^{2k}$, такое, что

$$f \oplus \mathrm{Ind}_{b\oplus L} \in \mathcal{B}_{2k} \text{ для некоторого } b \in \mathbb{F}_2^{2k},$$

причём $\widehat{U \cap F_{00}^{2k}} \subseteq L \subseteq \widehat{U}$ и $\dim L < \dim U$.

Теорема 2 отличается от теоремы из [1] соотношением $\widehat{U \cap F_{00}^{2k}} \subseteq L \subseteq \widehat{U}$.

ЛИТЕРАТУРА

1. *Коломеец Н. А.* О некоторых свойствах конструкции бент-функций с помощью подпространств произвольной размерности // Прикладная дискретная математика. Приложение. 2018. № 11. С. 41–43.
2. *Rothaus O.* On bent functions // J. Combin. Theory. Ser. A. 1976. V. 20. No. 3. P. 300–305.
3. *Логачев О. А., Сальников А. А., Смышляев С. В., Ященко В. В.* Булевы функции в теории кодирования и криптологии. 2-е изд. М.: МЦНМО, 2012. 584 с.
4. *Tokareva N. N.* Bent Functions, Results and Applications to Cryptography. Acad. Press. Elsevier, 2015.
5. *Carlet C.* Two new classes of bent functions // LNCS. 1994. V. 765. P. 77–101.
6. *McFarland R. L.* A family of difference sets in non-cyclic groups // J. Combin. Theory. Ser. A. 1973. V. 15. P. 1–10.

УДК 519.7 DOI 10.17223/2226308X/12/15

# О КУБИЧЕСКОЙ ЧАСТИ АЛГЕБРАИЧЕСКОЙ НОРМАЛЬНОЙ ФОРМЫ ПРОИЗВОЛЬНОЙ БЕНТ-ФУНКЦИИ

Т. А. Кузьмина

Доказано, что кубическая часть бент-функции от $n$ переменных не может быть произвольной при $n = 6, 8$.

**Ключевые слова:** *булева функция, бент-функция, линейная функция, квадратичная функция, кубическая функция, однородная функция.*

Булевы функции, максимально удалённые в метрике Хэмминга от множества всех аффинных функций, называются бент-функциями. Известно, что каждая булева функция может быть единственным образом представлена в её алгебраической нормальной форме (АНФ). Одна из проблем в области бент-функций: верно ли, что произвольная однородная булева функция степени $k$ от $n$ переменных ($n$ чётное) является частью АНФ некоторой бент-функции от $n$ переменных? Известно, что линейная часть в АНФ бент-функции может быть произвольной [1]. Доказано, что любая однородная квадратичная булева функция является квадратичной частью некоторой бент-функции [2].

В данной работе доказано, что при $n = 6, 8$ не каждую однородную кубическую булеву функцию можно достроить до бент-функции от $n$ переменных. Для случая $n = 8$ лишь часть однородных кубических булевых функций может быть достроена до бент-функций от восьми переменных с помощью добавления однородных функций второй и/или четвёртой степеней.

Далее будем использовать индексные обозначения АНФ функции; например, 12+34 означает булеву функцию $x_1x_2 \oplus x_3x_4$.

Всего существует пять неэквивалентных кубических булевых форм от шести переменных [3], а именно: $123; 123+145; 123+456; 124+135+236; 123+124+135+236+456$.

**Теорема 1.** Для $n = 6$ функции $123; 123 + 145; 124 + 135 + 236$ можно дополнить до бент-функций с помощью добавления однородных квадратичных булевых функций от шести переменных; функции $123 + 456; 123 + 124 + 135 + 236 + 456$ нельзя дополнить до бент-функций от шести переменных.

Существует 31 неэквивалентных кубических форм от восьми переменных [3]. В [4] приведена классификация форм четвёртой степени от восьми переменных, которые можно достроить до бент-функций [4], всего таких форм 536.

В таблице приведены результаты для кубических форм от восьми переменных. Во втором столбце представлена однородная кубическая форма, в третьем указано, можно ли достроить её до бент-функции, в четвёртом столбце — число $k$, показывающее, с помощью скольких форм четвёртой степени можно достроить кубические формы в том случае, если они достраиваются.

| № | Однородная кубическая форма | Бент-функция | $k$ |
|---|---|---|---|
| $f_1$ | 123 | Достраивается | 60 |
| $f_2$ | 123+145 | Достраивается | 58 |
| $f_3$ | 123+456 | Не достраивается | – |
| $f_4$ | 124+135+236 | Достраивается | 38 |
| $f_5$ | 123+124+135+236+456 | Не достраивается | – |
| $f_6$ | 123+145+167 | Достраивается | 53 |
| $f_7$ | 123+246+357 | Достраивается | 25 |
| $f_8$ | 123+145+167+246 | Достраивается | 44 |
| $f_9$ | 123+145+246+357 | Не достраивается | – |
| $f_{10}$ | 123+124+135+236+456+167 | Достраивается | 42 |
| $f_{11}$ | 123+145+167+246+357 | Не достраивается | – |
| $f_{12}$ | 123+476+568 | Не достраивается | – |
| $f_{13}$ | 123+145+167+568 | Достраивается | 17 |
| $f_{14}$ | 123+246+357+568 | Достраивается | 24 |
| $f_{15}$ | 123+246+357+128+138 | Не достраивается | – |
| $f_{16}$ | 123+145+167+357+568 | Не достраивается | – |
| $f_{17}$ | 123+145+478+568 | Достраивается | 46 |
| $f_{18}$ | 123+124+135+236+456+167+258 | Не достраивается | – |
| $f_{19}$ | 123+124+135+236+456+178 | Не достраивается | – |
| $f_{20}$ | 123+145+246+357+568 | Достраивается | 12 |
| $f_{21}$ | 123+145+246+467+578 | Достраивается | 11 |
| $f_{22}$ | 123+145+357+478+568 | Достраивается | 43 |
| $f_{23}$ | 123+246+357+478+568 | Не достраивается | – |
| $f_{24}$ | 123+246+357+148+178+258 | Не достраивается | – |
| $f_{25}$ | 123+145+167+246+357+568 | Не достраивается | – |
| $f_{26}$ | 123+145+167+246+238+258+348 | Не достраивается | – |
| $f_{27}$ | 123+145+167+258+268+378+468 | Достраивается | 34 |
| $f_{28}$ | 123+145+246+357+238+678 | Достраивается | 29 |
| $f_{29}$ | 123+145+246+357+478+568 | Не достраивается | – |
| $f_{30}$ | 123+124+135+236+456+167+258+378 | Не достраивается | – |
| $f_{31}$ | 123+156+246+256+147+157+357+348+258+458 | Не достраивается | – |

**Теорема 2.** Функции $f_1, f_2, f_4, f_6, f_8$ от восьми переменных можно дополнить до бент-функций с помощью добавления булевых функций второй степени от восьми переменных; остальные функции $f_3, f_5, f_7, f_9, f_{10}, \ldots, f_{31}$ нельзя дополнить до бент-функций таким образом.

**Теорема 3.** Функции $f_1, f_2, f_4, f_6, f_7, f_8, f_{10}, f_{13}, f_{14}, f_{17}, f_{20}, f_{21}, f_{22}, f_{27}, f_{28}$ от восьми переменных можно дополнить до бент-функций с помощью добавления слагаемых второй и четвёртой степеней от восьми переменных; остальные функции $f_3, f_5, f_9, f_{11}, f_{12}, f_{15}, f_{16}, f_{18}, f_{19}, f_{23}, f_{24}, f_{25}, f_{26}, f_{29}, f_{30}, f_{31}$ нельзя дополнить до бент-функций таким способом.

ЛИТЕРАТУРА

1. *Tokareva N.* Bent Functions: Results and Applications to Cryptography. Acad. Press. Elsevier, 2015.
2. *Tokareva N.* Algebraic Normal Form of a Bent Function: Properties and Restrictions. IACR Cryptology ePrint Archive. https://eprint.iacr.org/2018/1160.
3. *Черемушкин А. В.* Методы аффинной и линейной классификации булевых функций // Труды по дискретной математике. М.: Физматлит, 2001. Т. 4. С. 273–314.
4. *Langevin P.* Classification of Boolean Quartics Forms in Eight Variables. http://langevin.univ-tln.fr/project/quartics/quartics.html.

УДК 519.7 DOI 10.17223/2226308X/12/16

# ИЗОМЕТРИЧНЫЕ ОТОБРАЖЕНИЯ МНОЖЕСТВА ВСЕХ БУЛЕВЫХ ФУНКЦИЙ В СЕБЯ, СОХРАНЯЮЩИЕ САМОДУАЛЬНОСТЬ И ОТНОШЕНИЕ РЭЛЕЯ[1]

А. В. Куценко

Изучаются изометричные отображения множества всех булевых функций от $n$ переменных в себя. Получено полное описание изометричных отображений, сохраняющих самодуальность функций. Доказано, что каждое такое отображение сохраняет также антисамодуальность. Найдены все изометричные отображения, определяющие взаимно-однозначные соответствия между множествами самодуальных и антисамодуальных бент-функций. Получены все изометричные отображения, сохраняющие отношение Рэлея каждой булевой функции. Следствием данных результатов является полное описание всех изометричных отображений, сохраняющих максимальную нелинейность и расстояние Хэмминга между каждой бент-функцией и дуальной к ней.

**Ключевые слова:** *булева функция, изометричное отображение, самодуальная бент-функция, отношение Рэлея.*

*Булевой функцией* от $n$ переменных называется любое отображение $f : \mathbb{F}_2^n \to \mathbb{F}_2$. *Скалярным произведением* $\langle x, y\rangle$ двух векторов $x = (x_1, x_2, \ldots, x_n) \in \mathbb{F}_2^n$, $y = (y_1, y_2, \ldots, y_n) \in \mathbb{F}_2^n$ называется значение $\bigoplus\limits_{i=1}^{n} x_i y_i$. *Весом Хэмминга* $\mathrm{wt}(x)$ вектора $x \in \mathbb{F}_2^n$ называется количество единиц в нём. *Расстояние Хэмминга* $\mathrm{dist}(f, g)$ между булевыми функциями $f, g$ от $n$ переменных — число двоичных векторов длины $n$, на которых эти функции принимают различные значения. Через $\mathcal{O}_n$ обознается ортогональная группа $\mathcal{O}_n = \left\{L \in GL(n, 2) : LL^T = I_n\right\}$, где $L^T$ — операция транспонирования $L$; $I_n$ — единичная матрица порядка $n$ над полем $\mathbb{F}_2$ [1]. *Преобразованием Уолша — Адамара* булевой функции $f$ от $n$ переменных называется целочисленная функция $W_f : \mathbb{F}_2^n \to \mathbb{Z}$, заданная равенством $W_f(y) = \sum\limits_{x \in \mathbb{F}_2^n} (-1)^{f(x) \oplus \langle x, y\rangle}$, $y \in \mathbb{F}_2^n$.

Булева функция $f$ от чётного числа переменных $n$ называется *бент-функцией*, если $|W_f(y)| = 2^{n/2}$ для каждого $y \in \mathbb{F}_2^n$ [2]. Для множества бент-функций от $n$ переменных используется обозначение $\mathcal{B}_n$. Для каждой $f \in \mathcal{B}_n$ однозначным образом определяется *дуальная* к ней бент-функция $\widetilde{f} \in \mathcal{B}_n$, значения которой находятся из соответствия $W_f(y) = (-1)^{\widetilde{f}(y)} 2^{n/2}$ для каждого $y \in \mathbb{F}_2^n$. Бент-функция $f$ называется *самодуальной*

[1]Исследование выполнено при финансовой поддержке РФФИ (проекты №18-07-01394 и 18-31-00374).

(*антисамодуальной*), если $f = \tilde{f}$ (соответственно $f = \widetilde{f} \oplus 1$). Множества самодуальных и антисамодуальных бент-функций от $n$ переменных обозначаются через $\mathrm{SB}^+(n)$ и $\mathrm{SB}^-(n)$ соответственно [3].

Открытой проблемой является полная характеризация и описание класса самодуальных бент-функций. Этому и другим вопросам, связанным с самодуальными бент-функциями, посвящён ряд работ (C. Carlet, L. E. Danielson, M. G. Parker, P. Solé, X. Hou, T. Feulner, L. Sok, A. Wassermann и др.). В частности, в работе [4] приведена аффинная классификация самодуальных бент-функций от $2, 4, 6$ переменных и всех квадратичных самодуальных бент-функций от 8 переменных относительно преобразования, сохраняющего самодуальность. В [3] приведена классификация всех квадратичных самодуальных бент-функций. Аффинную классификацию квадратичных и кубических самодуальных бент-функций от 8 переменных относительно преобразования, сохраняющего самодуальность, можно найти в [5]. В [6] найден полный спектр расстояний Хэмминга между самодуальными бент-функциями из класса Мэйорана — МакФарланда.

Согласно [4, 7], *отношением Рэлея* (the Rayleigh quotient) $S_f$ булевой функции $f$ от $n$ переменных называется число

$$S_f = \sum_{x,y \in \mathbb{F}_2^n} (-1)^{f(x) \oplus f(y) \oplus \langle x,y \rangle} = \sum_{y \in \mathbb{F}_2^n} (-1)^{f(y)} W_f(y).$$

Из соотношения

$$\mathrm{dist}\left(f, \widetilde{f}\right) = 2^{n-1} - \frac{1}{2^{n/2+1}} S_f$$

следует, что отношение Рэлея полностью характеризует расстояние Хэмминга между бент-функцией $f \in \mathcal{B}_n$ и дуальной к ней функцией $\widetilde{f} \in \mathcal{B}_n$. Известно [4], что абсолютное значение $S_f$ не превосходит $2^{3n/2}$, при этом данная оценка достигается только на самодуальных бент-функциях $\left(+2^{3n/2}\right)$ и антисамодуальных бент-функциях $\left(-2^{3n/2}\right)$.

Отображение всех булевых функций от $n$ переменных в себя называется *изометричным*, если оно сохраняет расстояние Хэмминга для каждой пары функций. Известно, что каждое такое отображение однозначно представляется в виде

$$f(x) \longrightarrow f(\pi(x)) \oplus g(x),$$

где $\pi$ — перестановка на множестве $\mathbb{F}_2^n$; $g$ — булева функция от $n$ переменных [8]. Единственным изометричным отображением множества всех булевых функций от $n$ переменных в себя, оставляющим множество $\mathcal{B}_n$ на месте, является композиция аффинного преобразования координат и прибавления аффинной функции от $n$ переменных [9].

Всюду далее предполагается, что $n$ — чётное натуральное число.

В работе [5] (см. также [4]) доказано, что отображение всех булевых функций от $n$ переменных в себя, имеющее вид

$$f(x) \longrightarrow f\left(L\left(x \oplus c\right)\right) \oplus \langle c, x \rangle \oplus d,$$

где $L \in \mathcal{O}_n$; $c \in \mathbb{F}_2^n$; $\mathrm{wt}(c)$ — чётное число; $d \in \mathbb{F}_2$, сохраняет самодуальность бент-функции. Нетрудно видеть, что все отображения данного вида являются изометричными.

В [7] приведены примеры отображений всех булевых функций от $n$ переменных в себя, сохраняющих максимальную нелинейность и отношение Рэлея. Показано, что для каждой бент-функции $f \in \mathcal{B}_n$ и любых $L \in \mathcal{O}_n, c \in \mathbb{F}_2^n, d \in \mathbb{F}_2$ для бент-функций

$g, h \in \mathcal{B}_n$, определённых как $g(x) = f(Lx) \oplus d$ и $h(x) = f(x \oplus c) \oplus \langle c, x \rangle$, справедливо $S_g = S_f$ и $S_h = (-1)^{\langle c,c \rangle} S_f$.

В [3] отмечено, что отображение всех булевых функций от $n$ переменных в себя, имеющее вид

$$f(x) \longrightarrow f(x \oplus c) \oplus \langle c, x \rangle,$$

где $c \in \mathbb{F}_2^n$, $\mathrm{wt}(c)$ — нечётное число, определяет биекцию между множествами $\mathrm{SB}^+(n)$ и $\mathrm{SB}^-(n)$. Очевидно, что такое отображение сохраняет расстояние Хэмминга. Частный случай отображения данного вида — при $c = (1, 0, 0, \ldots, 0) \in \mathbb{F}_2^n$ — ранее был рассмотрен в работе [4], на основании чего был сделан вывод о том, что между множествами $\mathrm{SB}^+(n)$ и $\mathrm{SB}^-(n)$ существует взаимно-однозначное соответствие.

В настоящей работе получено обобщение известных результатов в рамках класса изометричных отображений.

Пусть $\varphi$ — изометричное отображение всех булевых функций от $n$ переменных в себя, то есть

$$f(x) \longrightarrow f(\pi(x)) \oplus g(x),$$

где $\pi$ — перестановка на множестве $\mathbb{F}_2^n$; $g$ — булева функция от $n$ переменных.

**Теорема 1.** Следующие условия эквивалентны:

- $\varphi$ сохраняет самодуальность;
- $\varphi$ сохраняет антисамодуальность;
- $\varphi$ сохраняет отношение Рэлея каждой булевой функции от $n$ переменных;
- $\pi(x) = L(x \oplus c)$ и $g(x) = \langle c, x \rangle \oplus d$, где $L \in \mathcal{O}_n$; $c \in \mathbb{F}_2^n$; $\mathrm{wt}(c)$ — чётное число; $d \in \mathbb{F}_2$.

**Следствие 1.** Отображение $\varphi$ сохраняет максимальную нелинейность и расстояние Хэмминга между каждой бент-функцией и дуальной к ней тогда и только тогда, когда $\pi(x) = L(x \oplus c)$ и $g(x) = \langle c, x \rangle \oplus d$, где $L \in \mathcal{O}_n$; $c \in \mathbb{F}_2^n$; $\mathrm{wt}(c)$ — чётное число; $d \in \mathbb{F}_2$.

**Теорема 2.** Следующие условия эквивалентны:

- $\varphi$ определяет взаимно-однозначное соответствие между множествами $\mathrm{SB}^+(n)$ и $\mathrm{SB}^-(n)$;
- $\varphi$ меняет знак отношения Рэлея каждой булевой функции от $n$ переменных;
- $\pi(x) = L(x \oplus c)$ и $g(x) = \langle c, x \rangle \oplus d$, где $L \in \mathcal{O}_n$; $c \in \mathbb{F}_2^n$; $\mathrm{wt}(c)$ — нечётное число; $d \in \mathbb{F}_2$.

Из полученных результатов следует, что более общего подхода к эквивалентности самодуальных бент-функций на основе изометричных отображений, чем предложенный в работах [4, 5], не существует.

## ЛИТЕРАТУРА


1. *Janusz G. J.* Parametrization of self-dual codes by orthogonal matrices // Finite Fields Appl. 2007. No. 13 (3). P. 450–491.
2. *Rothaus O.* On bent functions // J. Combin. Theory. Ser. A. 1976. No. 20 (3). P. 300–305).
3. *Hou X.-D.* Classification of self dual quadratic bent functions // Des. Codes Cryptogr. 2012. No. 63 (2). P. 183–198.
4. *Carlet C., Danielson L. E., Parker M. G., and Solé P.* Self dual bent functions // Int. J. Inform. Coding Theory. 2010. No. 1. P. 384–399.
5. *Feulner T., Sok L., Solé P., and Wassermann A.* Towards the classification of self-dual bent functions in eight variables // Des. Codes Cryptogr. 2013. No. 68 (1). P. 395–406.

6. *Куценко А. В.* Спектр расстояний Хэмминга между самодуальными бент-функциями из класса Мэйорана — МакФарланда // Дискретный анализ и исследование операций. 2018. Т. 25. № 1. С. 98–119.
7. *Danielsen L. E., Parker M. G., and Solé P.* The Rayleigh quotient of bent functions // LNCS. 2009. V. 5921. P. 418–432.
8. *Марков А. А.* О преобразованиях, не распространяющих искажения // Избранные труды. Т. II. Теория алгорифмов и конструктивная математика, математическая логика, информатика и смежные вопросы. М.: МЦНМО, 2003. С. 70–93.
9. *Tokareva N. N.* The group of automorphisms of the set of bent functions // Discr. Math. Appl. 2010. No. 20 (5). P. 655–664.

УДК 519.7 DOI 10.17223/2226308X/12/17

# О КЛАССАХ БУЛЕВЫХ ФУНКЦИЙ ОГРАНИЧЕННОЙ СЛОЖНОСТИ[1]

А. И. Метальникова, И. А. Панкратова

Рассматриваются классы булевых функций от $n$ переменных, имеющих короткое (по сравнению с $2^n$) представление. Подсчитаны мощности этих классов, приведены тесты на принадлежность функции классам и алгоритм доопределения частично заданной булевой функции до функции ограниченной степени.

**Ключевые слова:** *существенная зависимость функции от переменной, степень булевой функции, алгебраическая нормальная форма.*

Во многих шифрсистемах используются булевы функции. Если функция является ключом, как, например, в [1, 2], то она должна зависеть от большого числа переменных. Поскольку длина вектора значений булевой функции от $n$ переменных равна $2^n$ и формула (в любом базисе) произвольной функции имеет ту же длину (порядка $2^n$), представляют интерес классы функций, которые зависят от большого числа переменных, но имеют короткое задание. В связи с этим возникают следующие задачи: подсчёт количества функций в классе; разработка теста на принадлежность функции классу; разработка алгоритма доопределения частичной функции до функции из заданного класса.

Обозначим $P_2(n)$ множество всех булевых функций от $n$ переменных; будем рассматривать следующие классы функций в $P_2(n)$ и называть их классами ограниченной сложности:

— $C_{n,k}$ — с заданным (равным $k$) числом существенных переменных;
— $C_{n,\leqslant k}$ — с ограниченным (не больше $k$) числом существенных переменных;
— $D_{n,k}$ — заданной степени ($\deg f = k$);
— $D_{n,\leqslant k}$ — ограниченной степени ($\deg f \leqslant k$);
— $L_{n,k}$ — с заданной (равной $k$) длиной алгебраической нормальной формы (АНФ);
— $L_{n,\leqslant k}$ — с ограниченной (не больше $k$) длиной АНФ;
— $NR_n$ — имеющие бесповторную АНФ (каждая переменная входит в АНФ не более одного раза).

В таблице приведены мощности этих классов, здесь $\mathbb{S}_k$ — количество функций от $k$ переменных, существенно зависящих от всех своих переменных (последовательность A000371 из [3]), $\mathbb{S}_k = \sum\limits_{i=0}^{k}(-1)^i\binom{k}{i}2^{2^{k-i}}$; $\mathbb{B}_k$ — число Белла, или количество всех

[1]Работа поддержана грантом РФФИ, проект № 17-01-00354.

неупорядоченных разбиений $k$-элементного множества (последовательность A000110 из [3]), задаваемое рекуррентной формулой $\mathbb{B}_0 = 1$, $\mathbb{B}_{k+1} = \sum\limits_{i=0}^{k} \binom{k}{i} \mathbb{B}_i$.

| Класс | Мощность |
|---|---|
| $C_{n,k}$ | $\binom{n}{k}\mathbb{S}_k$ |
| $C_{n,\leqslant k}$ | $\sum\limits_{i=0}^{k} \lvert C_{n,i}\rvert = \sum\limits_{i=0}^{k} \binom{n}{i}\mathbb{S}_i$ |
| $D_{n,k}$ | $2^{\sum\limits_{i=0}^{k}\binom{n}{i} - \sum\limits_{i=0}^{k-1}\binom{n}{i}}$ |
| $D_{n,\leqslant k}$ | $2^{\sum\limits_{i=0}^{k}\binom{n}{i}}$ |
| $L_{n,k}$ | $\binom{2^n}{k}$ |
| $L_{n,\leqslant k}$ | $\sum\limits_{i=0}^{k}\binom{2^n}{i}$ |
| $NR_n$ | $2\mathbb{B}_{n+1}$ |

Принадлежность функции $f$ классу ограниченной сложности определяется свойствами её АНФ, например, $\deg f$ равна длине самого длинного слагаемого в АНФ; количество существенных переменных — количеству переменных, входящих в АНФ. АНФ, в свою очередь, строится с помощью преобразования Мёбиуса $\mu : P_2(n) \to P_2(n)$ [4]:

$$f(x) = \bigoplus_{a \in \mathbb{Z}_2^n} g(a)x^a, \quad g = \mu(f),$$
$$g(a) = \bigoplus_{x \leqslant a} f(x). \tag{1}$$

Для $g = \mu(f)$ обозначим $\{a_1, \ldots, a_r\}$ множество всех векторов, на которых $g(a_i) = 1$, $i = 1, \ldots, r$; единичным компонентам в $a_i$ соответствуют переменные, входящие в $i$-е слагаемое АНФ функции $f$. Через $\mathrm{w}(x)$ ($\mathrm{w}(f)$) обозначим вес булева вектора $x$ (функции $f$). Тогда $t = \mathrm{w}\left(\bigvee\limits_{i=1}^{k} a_i\right)$ — количество существенных переменных функции $f$; $d = \max\limits_{i=1,\ldots,r} \mathrm{w}(a_i)$ — её степень. Получаем следующие тесты принадлежности функции $f$ классам ограниченной сложности:

— если $t = k$, то $f \in C_{n,k}$; если $t \leqslant k$, то $f \in C_{n,\leqslant k}$;
— если $d = k$, то $f \in D_{n,k}$; если $d \leqslant k$, то $f \in D_{n,\leqslant k}$;
— если $\mathrm{w}(g) = k$, то $f \in L_{n,k}$; если $\mathrm{w}(g) \leqslant k$, то $f \in L_{n,\leqslant k}$.

Чуть сложнее проверяется принадлежность функции классу $NR_n$. Составим матрицу $A$ размера $r \times n$, строками которой являются векторы $a_i$, $i = 1, \ldots, r$. Тогда $f \in NR_n$, если и только если веса всех столбцов матрицы $A$ не больше 1; другими словами, $f \notin NR_n$, если и только если какой-либо столбец матрицы $A$ содержит хотя бы две единицы. Соответствующая проверка выполняется в алгоритме 1.

Задача доопределения функции до функции из заданного класса $\mathcal{C} \subseteq P_2(n)$ ставится так: частично определённая функция $f \in P_2(n)$ задана множествами $M_0 = \{x \in \mathbb{Z}_2^n : f(x) = 0\}$ и $M_1 = \{x \in \mathbb{Z}_2^n : f(x) = 1\}$, $M_0 \cap M_1 = \varnothing$; найти все такие функции $g \in \mathcal{C}$, что $g(x) = f(x)$ для всех $x \in M_0 \cup M_1$. Рассмотрим случай $\mathcal{C} = D_{n,\leqslant k}$.

АНФ функции $f \in D_{n,\leqslant k}$ обладает следующим свойством: $g(x) = 0$ для всех $x$, таких, что $\mathrm{w}(x) > k$, где $g = \mu(f)$. Обозначим вектор значений функции $f$ как $\mathbf{b} =$

**Алгоритм 1.** Тест на принадлежность функции $f$ классу $NR_n$

**Вход:** Функция $f \in P_2(n)$; матрица $A$ со строками $\{a_1, \ldots, a_r\}$.

1: $x := a_1$.
2: **Для** $i = 2, \ldots, r$
3: $\quad y := x \oplus a_i$.
4: $\quad$ **Если** $x\&\bar{y} = \mathbf{0}$, **то**
$\qquad$ выход, ответ: $f \notin NR_n$.
5: $\quad x := y$.
6: Ответ: $f \in NR_n$.

$= (b_0 b_1 \ldots b_{2^n-1})$, $b_i = f(i)$ (здесь мы не различаем число в диапазоне от 0 до $2^n - 1$ и его представление в виде булева вектора длины $n$).

В самом общем виде (если $M_0 = M_1 = \varnothing$) решение задачи состоит в следующем: для каждого $x$, такого, что $\mathrm{w}(x) > k$, в соответствии с формулой (1) составляем уравнение $\bigoplus\limits_{i \leqslant x} b_i = 0$. Обозначим матрицу полученной системы линейных однородных уравнений (СЛОУ) $B_{n,k}$. Все решения получившейся СЛОУ

$$B_{n,k}\mathbf{b} = \mathbf{0} \tag{2}$$

являются векторами значений функций из $D_{n,\leqslant k}$.

Для поиска доопределений частично заданной функции (если $M_0 \neq \varnothing$ или $M_1 \neq \varnothing$) решаем ту же систему относительно переменных множества $\{b_i : i \notin M_0 \cup M_1\}$, объявив константами 0 и 1 переменные $b_i$ с номерами из множеств $M_0$ и $M_1$ соответственно. Таким образом, СЛОУ (2) преобразуется к системе уже не обязательно однородных уравнений.

## ЛИТЕРАТУРА

1. *Agibalov G. P.* Substitution block ciphers with functional keys // Прикладная дискретная математика. 2017. № 38. С. 57–65.
2. *Агибалов Г. П.* SIBCiphers — симметричные итеративные блочные шифры из булевых функций с ключевыми аргументами // Прикладная дискретная математика. Приложение. 2014. № 7. С. 43–48.
3. *Sloan N. J. A.* The On-line Encyclopedia of Integer Sequences. `https://oeis.org/`
4. *Логачев О. А., Сальников А. А., Ященко В. В.* Булевы функции в теории кодирования и криптологии. М.: МЦНМО, 2004.

УДК 519.7 DOI 10.17223/2226308X/12/18

# О СВЯЗИ НЕЛИНЕЙНЫХ И ДИФФЕРЕНЦИАЛЬНЫХ СВОЙСТВ ВЕКТОРНЫХ БУЛЕВЫХ ФУНКЦИЙ[1]

А. В. Милосердов

Исследуются связи таблиц линейного приближения (LAT) и распределения разностей (DDT) векторных булевых функции. Доказано, что наличие совпадающих строк в DDT и LAT является инвариантом относительно аффинной эквивалентности, а также относительно EA-эквивалентности для нормированных DDT- и

[1]Работа поддержана грантами РФФИ, проекты № 18-07-01394 и 18-31-00374.

LAT-таблиц. Выдвинута гипотеза о том, что если в LAT (DDT)-таблице векторной булевой функции $F$ все строки попарно различны, то в её DDT (LAT)-таблице все строки также попарно различны. Данная гипотеза проверена для функций от малого числа переменных и для известных APN-функций от не более чем 10 переменных.

**Ключевые слова:** *APN-функция, AB-функция, дифференциальная равномерность, нелинейность.*

При создании и использовании какого-либо шифра необходимо, чтобы он был устойчив к различным видам криптоанализа. Один из таких методов криптоанализа — дифференциальный [1]. Шифр устойчив к данному методу криптоанализа, если для функции $F$, лежащей в его основе, уравнение $F(x)\oplus F(x\oplus a) = b$ для любых $a \neq \mathbf{0}, b$ имеет как можно меньше решений. Число решений данного уравнения при различных парах $(a, b)$ формулируют *таблицу распределения разностей* (DDT) размера $2^n \times 2^n$. Если в данной таблице при $a \neq \mathbf{0}$ для функции $F$ все элементы равны 0 или 2, то такая функция называется *почти совершенно нелинейной функцией* (*APN-функцией*).

Для функции можно рассмотреть также *таблицу линейного приближения* (LAT) размера $2^n \times 2^n$, в ячейке $(v, u)$ которой хранится квадрат коэффициента Уолша — Адамара $W_F(u, v) = \sum\limits_{x\in\mathbb{F}_2^n} (-1)^{\langle v,F(x)\rangle\oplus\langle u,x\rangle}$. Данная таблица рассматривается при исследовании шифра на устойчивость к линейному криптоанализу [2]. LAT-таблица отражает нелинейность функции $F$. Если каждый коэффициент Уолша — Адамара функции $F$ при $v \neq 0$ лежит в множестве $\{0, \pm 2^{(n+1)/2}\}$, то такая функция называется *почти бент-функцией* (*AB-функцией*).

Известно, что AB-функции и APN-функции тесно связаны.

**Теорема 1** [3]. Каждая AB-функция является APN-функцией.

Интересно рассмотреть связи данных таблиц. Выдвинута следующая

**Гипотеза 1.** Если в LAT (DDT)-таблице векторной булевой функции $F$ все строки попарно различны, то в её DDT (LAT)-таблице все строки попарно различны.

Гипотеза 1 подтверждена для всех векторных булевых функций от 3 переменных и для известных APN-функций от не более чем 10 переменных.

Гипотеза 1 верна для квадратичных APN-функций от чётного числа переменных.

**Утверждение 1.** Для любой квадратичной APN-функции от чётного числа переменных в LAT- и DDT-таблицах есть совпадающие строки.

Интересно понять, при каких преобразованиях наличие совпадающих строк LAT- и DDT-таблиц является инвариантом.

Векторные булевы функции $F : \mathbb{F}_2^n \to \mathbb{F}_2^n$ и $G : \mathbb{F}_2^n \to \mathbb{F}_2^n$ называются *расширенно аффинно эквивалентными* (*EA-эквивалентными*), если $F = A_1 \circ G \circ A_2 \oplus A$, где $A_1$, $A_2 : \mathbb{F}_2^n \to \mathbb{F}_2^n$ — взаимно-однозначные аффинные функции и $A : \mathbb{F}_2^n \to \mathbb{F}_2^n$ — аффинная функция. Если $A \equiv \mathbf{0}$, то функции называются *аффинно эквивалентными*.

**Теорема 2.** Если функции $F$ и $G$ аффинно эквивалентны и в DDT (LAT)-таблице функции $F$ есть совпадающие строки, то в DDT (LAT)-таблице функции $G$ также есть совпадающие строки.

Аналогичную теорему можно сформулировать и для EA-эквивалентности, но для этого нужно рассматривать немного модифицированные DDT- и LAT-таблицы.

*Нормированной* DDT-таблицей функции $F$ будем называть таблицу, в ячейке $(a, b)$ которой записано количество решений уравнения

$$F(x) \oplus F(x \oplus a) \oplus F(a) \oplus F(\mathbf{0}) = b.$$

*Нормированной* LAT-таблицей функции $F$ будем называть LAT-таблицу функции $F$ без линейной части.

**Теорема 3.** Если функции $F$ и $G$ EA-эквивалентны и в нормированной DDT (LAT)-таблице функции $F$ есть совпадающие строки, то в нормированной DDT (LAT)-таблице функции $G$ также есть совпадающие строки.

ЛИТЕРАТУРА

1. *Biham E. and Shamir A.* Differential cryptanalysis of DES-like cryptosystems // J. Cryptology. 1991. V. 4. Iss. 1. P. 3–72.
2. *Matsui M. and Yamagishi A.* A new method for known plaintext attack of FEAL cipher // EUROCRYPT'1992. LNCS. 1992. V. 658. P. 81–91.
3. *Carlet C.* Vectorial Boolean functions for cryptography // Boolean Models and Methods in Mathematics, Computer Science, and Engineering / eds. Y. Crama and P. Hammer. Cambridge: Cambridge University Press, 2010. P. 398–470.

УДК 519.7 DOI 10.17223/2226308X/12/19

# РЕКУРРЕНТНЫЕ ФОРМУЛЫ ДЛЯ ЧИСЛА $k$-ЭЛАСТИЧНЫХ И КОРРЕЛЯЦИОННО-ИММУННЫХ ДВОИЧНЫХ ОТОБРАЖЕНИЙ

К. Н. Панков

Получены рекуррентные формулы для распределения части вектора весов подфункций $w_I^J$ и части вектора спектральных коэффициентов $\Delta_I^J$ линейных комбинаций координатных функций двоичного отображения из векторного пространства $V_n$ двоичных $n$-мерных векторов в векторное пространство $V_m$. С помощью этих формул получены рекуррентные формулы для числа корреляционно-иммунных порядка $k$ двоичных отображений и для числа $k$-эластичных двоичных отображений.

**Ключевые слова:** *веса подфункций, спектральные коэффициенты, рекуррентные формулы, устойчивые вектор-функции, эластичные вектор-функции, корреляционно-иммунные функции.*

Системы распределённого реестра, основанные на блокчейн-технологии, являются одной из сквозных цифровых технологий программы «Цифровая экономика Российской Федерации». В последние годы различные аспекты данной технологии стали предметом пристального изучения исследователей и разработчиков программного обеспечения. Одной из многообещающих возможностей её применения являются системы хранения важных данных, включая персональные. Однако применение норм российского и европейского законодательства, занимающегося правовым регулированием персональных данных, приводит на практике к противоречию с самой концепцией блокчейн-систем, которые предполагают неизменность данных. В информационных системах (ИС) с реестром с ограничениями на добавление информации (согласно терминологии [1]), к примеру, задача удаления персональных данных может решаться изменением всей цепочки данных («forking»), в открытых же ИС с реестром наиболее

многообещающим способом решения этой задачи может служить шифрование каждого блока персональной информации на своём ключе и удаление ключа, который хранится за пределами цепочки данных, при поступлении запроса на удаление [2]. В работе [3] этот метод разобран достаточно подробно и связан с задачей оценки числа $(n, m, k)$-устойчивых и корреляционно-иммунных двоичных отображений, используемых в качестве комбинирующих в поточных системах шифрования.

Обозначим через $V_n$ множество двоичных векторов размерности $n$. Корреляционная иммунность и эластичность (или $(n, m, k)$-устойчивость) двоичного отображения $f(\alpha) = (f_1(\alpha), f_2(\alpha), \ldots, f_m(\alpha)) : V_n \to V_m$, согласно [4], сводится к обладанию этими свойствами всеми ненулевыми линейными комбинациями координатных функций $f(\alpha)$, называемыми в [5] компонентными функциями или компонентами. Свойства компонент могут быть, в частности, выражены в терминах весов их подфункций (в обозначениях [6]):

$$w_I^J(f) = \left\| (\psi_m(J), f)_{i_1,\ldots,i_{|I|}}^{1,\ldots,1} \right\|.$$

Здесь $f = (f_1, \ldots, f_m)$; $\|f_1\|$ — вес булевой функции $f_1$; $|J|$ — мощность множества $J = \{j_1, \ldots, j_{|J|}\} \subset \{1, \ldots, m\}$; $I = \{i_1, \ldots, i_{|I|}\} \subset \{1, \ldots, n\}$; $\psi_m(J)$ — двоичный вектор длины $m$, у которого в $j_1, \ldots, j_{|J|}$ координатах стоят единицы, а в остальных нули (согласно [7], $\psi_m(J)$ называется индикаторным вектором множества $J$); $(a, b) = a_1 b_1 \oplus \ldots \oplus a_n b_n$ — скалярное произведение векторов $a$ и $b$ из $V_m$; $(\psi_m(J), f)_{i_1,\ldots,i_{|I|}}^{1,\ldots,1}$ — подфункция компоненты $(\psi_m(J), f)$ отображения $f$, получаемая, если у аргумента компоненты $(\psi_m(J), f)$ значения координат с номерами $i_1, \ldots, i_{|I|}$ положить равными единице.

Для компоненты $(\psi_m(J), f)$ можно определить спектральный коэффициент Фурье — Уолша — Адамара

$$\Delta_I^J(f) = F_I^J(f) = \frac{1}{2} \sum_{x \in V_n} (-1)^{(\psi_m(J), f)(x) \oplus x_{i_1} \oplus \ldots \oplus x_{i_{|I|}}} = 2^{n-1} - \|(\psi_m(J), f)(x) \oplus (\psi_n(I), x)\|,$$

где $(\psi_n(I), x) = x_{i_1} \oplus \ldots \oplus x_{i_{|I|}}$. Согласно [8], $\Delta_I^J(f)$ называется коэффициентом статистической структуры компоненты $(\psi_m(J), f)$.

В [9] доказаны формулы однозначной связи $w_I^J$ с коэффициентами статистической структуры

$$\Delta_I^J = \sum_{L \subset I} (-1)^{|L|} \left(2^{n-1} - 2^{|L|} w_L^J\right), \quad w_I^J - 2^{n-|I|-1} = 2^{-|I|} \sum_{L \subset I} (-1)^{|L|+1} \Delta_L^J,$$

называемые тождеством Саркара (можно назвать тождеством Денисова — Саркара). Рассмотрим для произвольной функции $f$ из множества $B_n^m$ вектор весов подфункций

$$\overline{W}_k(f) = \left(w_I^J(f) : \varnothing \neq J \subset \{1, \ldots, m\}, I \subset \{1, \ldots, n\}, |I| \leqslant k\right)$$

и вектор коэффициентов статистической структуры

$$\bar{\Delta}_k(f) = \left(\Delta_I^J(f) : \varnothing \neq J \subset \{1, \ldots, m\}, I \subset \{1, \ldots, n\}, |I| \leqslant k\right)$$

длины $N = N(n, m, k) = (2^m - 1) \sum\limits_{s=0}^{k} \binom{n}{s}$.

Многие свойства двоичных отображений зависят от того, чему равен вектор, состоящий из определённых выше характеристик всех компонент или их части. Поэтому задача нахождения мощности множества функций с фиксированным начальным

вектором весов подфункций или коэффициентов статистической структуры является важной. В настоящее время имеются только асимптотические оценки, полученные в [10 – 14].

Рассмотрим класс функций из $B_n^m$

$$W_n^m(\bar{z}) = W_n^m\left(z_I^J : \varnothing \neq J \subset \{1,\dots,m\}; I \subset \{1,\dots,n\}; |I| \leqslant k\right) =$$
$$= \left\{f \in B_n^m : w_I^J(f) = 2^{n-|I|-1} - z_I^J, \varnothing \neq J \subset \{1,\dots,m\}; I \subset \{1,\dots,n\}; |I| \leqslant k\right\},$$

чьи первые (в лексикографическом порядке) веса подфункций $\overline{W}_k(f) = \overline{W} \in \mathbb{Z}^N$ равны

$$\overline{W} = \left(w_I^J(f) = 2^{n-|I|-1} - z_I^J(f) : I \subset \{1,\dots,n\}; \varnothing \neq J \subset \{1,\dots,m\}; |I| \leqslant k\right).$$

**Теорема 1.** Пусть $n, m \in \mathbb{N}$, $k \in \{1,\dots,n-1\}$, тогда

$$|W_n^m(\bar{z})| = \left|W_n^m\left(z_I^J : I \subset \{1,\dots,n\}; \varnothing \neq J \subset \{1,\dots,m\}; |I| \leqslant k\right)\right| =$$
$$= \sum_{\substack{z_{I\cup\{n\}}^J \in \mathbb{Z}: \varnothing \neq J \subset \{1,\dots,m\},\\ I \subset \{1,\dots,n-1\}, |I|=k}} \left|W_{n-1}^m\left(z_{I\cup\{n\}}^J : \varnothing \neq J \subset \{1,\dots,m\}; I \subset \{1,\dots,n-1\}; |I| \leqslant k\right)\right| \times$$
$$\times \left|F_{n-1}^m\left(z_I^J - z_{I\cup\{n\}}^J : \varnothing \neq J \subset \{1,\dots,m\}; I \subset \{1,\dots,n-1\}; |I| \leqslant k\right)\right|.$$

В теореме 1 суммирование на самом деле происходит не по всем $z_{I\cup\{n\}}^J \in \mathbb{Z}$, а только по $z_{I\cup\{n\}}^J \in \left\{-2^{n-k-2}, -2^{n-k-2}+1, \dots, 2^{n-k-2}\right\}$.

Обозначим через $S_n^m\left(\bar{\Delta}\right)$ класс функций из $B_n^m$, обладающих следующим начальным вектором коэффициентов статистической структуры:

$$\bar{\Delta} = \left(\Delta_I^J(f) : \varnothing \neq J \subset \{1,\dots,m\}; I \subset \{1,\dots,n\}; |I| \leqslant k\right).$$

Используя тождества Денисова — Саркара, можно доказать

**Теорема 2.** Пусть $n, m \in \mathbb{N}$, $k \in \{1,\dots,n-1\}$, тогда

$$\left|S_n^m\left(\bar{\Delta}\right)\right| = \left|S_n^m\left(\Delta_I^J : I \subset \{1,\dots,n\}; \varnothing \neq J \subset \{1,\dots,m\}; |I| \leqslant k\right)\right| =$$
$$= \sum_{\substack{\Delta_{I\cup\{n\}}^J \in \mathbb{Z}:\\ \varnothing \neq J \subset \{1,\dots,m\},\\ I \subset \{1,\dots,n-1\}, |I|=k}} \left|S_{n-1}^m\left(\frac{\Delta_I^J - \Delta_{I\cup\{n\}}^J}{2} : \varnothing \neq J \subset \{1,\dots,m\}; I \subset \{1,\dots,n-1\}; |I| \leqslant k\right)\right| \times$$
$$\times \left|S_{n-1}^m\left(\frac{\Delta_I^J + \Delta_{I\cup\{n\}}^J}{2} : \varnothing \neq J \subset \{1,\dots,m\}; I \subset \{1,\dots,n-1\}; |I| \leqslant k\right)\right|.$$

В теореме 2 суммирование также происходит только по тем $\Delta_{I\cup\{n\}}^J$, что лежат в множестве $\left\{-2^{n-1}, -2^{n-1}+1, \dots, 2^{n-1}\right\}$.

**Определение 1.** Отображение $f$ из множества $B_n^m$ всех $m$-мерных двоичных функций от $n$ переменных называется $k$-эластичным ($(n,m,k)$-устойчивым), если для любых $I, J$, $\varnothing \neq J \subset \{1,\dots,m\}$, $I \subset \{1,\dots,n\}$, $|I| \leqslant k$, выполняется $\Delta_I^J(f) = 0$.

Обозначим $R(n,m,k)$ множество всех $k$-эластичных двоичных отображений из $B_n^m$.

**Следствие 1.** В условиях теорем 1 и 2 верно

$$|R(n,m,k)| = \sum_{\substack{\Delta(I,J)\in\left\{-2^{n-k-2},\ldots,2^{n-k-2}\right\}:\\ \varnothing\neq J\subset\{1,\ldots,m\},\\ I\subset\{1,\ldots,n-1\},|I|=k}} \left|\left\{f\in B_{n-1}^m : \Delta_I^J(f)=0 : I\subset\{1,\ldots,n-1\},|I|<k;\right.\right.$$
$$\Delta_I^J(f) = 2^k\Delta(I,J) : I\subset\{1,\ldots,n-1\},|I|=k;\varnothing\neq J\subset\{1,\ldots,m\}\Big\}\Big|\times$$
$$\times\left|\left\{h\in B_{n-1}^m : \Delta_I^J(h)=0 : I\subset\{1,\ldots,n-1\},|I|<k;\right.\right.$$
$$\left.\left.\Delta_I^J(h) = -2^k\Delta(I,J) : I\subset\{1,\ldots,n-1\},|I|=k;\varnothing\neq J\subset\{1,\ldots,m\}\right\}\right|.$$

В работе [3] следствие 1 доказано как отдельный результат, причём в формулировке допущена опечатка.

**Определение 2.** Отображение $f$ из множества $B_n^m$ всех $m$-мерных двоичных функций от $n$ переменных называется корреляционно-иммунным порядка $k$, если для любого $J$, $\varnothing\neq J\subset\{1,\ldots,m\}$, существует такая величина $r_J\in\left\{-2^{n-k-1},\ldots,2^{n-k-1}\right\}$, что для любого $I$, $I\subset\{1,\ldots,n\}$, $|I|\leqslant k$, выполняется $w_I^J(f)=2^{n-|I|-1}+r_J2^{k-|I|}$.

Определение 2 эквивалентно тому, что для любых $I,J$, $\varnothing\neq J\subset\{1,\ldots,m\}$, $I\subset$ $\subset\{1,\ldots,n\}$, $1\leqslant|I|\leqslant k$, выполняется $\Delta_I^J(f)=0$.

Обозначим через $K(n,m,k)$ множество всех корреляционно-иммунных порядка $k$ двоичных отображений из $B_n^m$. Из утверждения в [15] следует, что если $f\in K(n,m,k)$, то $\|f\|\equiv 0\equiv\Delta_\varnothing^J \pmod{2^k}$

**Следствие 2.** В условиях теорем 1 и 2 верно

$$|K(m,n,k)| = \sum_{s=-2^{-n-k-1}}^{2^{-n-k-1}} \sum_{\substack{\Delta(I,J)\in\left\{-2^{n-k-1},\ldots,2^{n-k-1}\right\}:\varnothing\neq J\subset\{1,\ldots,m\},\\ I\subset\{1,\ldots,n-1\},|I|=k}} \left|\left\{f\in B_{n-1}^m : \Delta_\varnothing^J(f)=2^{k-1}s;\right.\right.$$
$$\Delta_I^J(f)=0 : I\subset\{1,\ldots,n-1\},|I|<k;$$
$$\Delta_I^J(f) = 2^{k-1}\Delta(I,J) : I\subset\{1,\ldots,n-1\},|I|=k;\varnothing\neq J\subset\{1,\ldots,m\}\Big\}\Big|\times$$
$$\times\left|\left\{h\in B_{n-1}^m : \Delta_\varnothing^J(h)=2^{k-1}s;\Delta_I^J(h)=0 : I\subset\{1,\ldots,n-1\},|I|<k;\right.\right.$$
$$\left.\left.\Delta_I^J(h) = -2^{k-1}\Delta(I,J) : I\subset\{1,\ldots,n-1\},|I|=k;\varnothing\neq J\subset\{1,\ldots,m\}\right\}\right|.$$

Полученные рекуррентные формулы позволяют вычислять точные значения мощностей множеств $R(t,m,k)$ и $K(t,m,k)$ для $t>n$ при фиксированных значениях переменных $m$ и $k$, предварительно экспериментально находя распределение мощности множеств $S_n^m\left(\bar{\Delta}\right)$ соответствующего вида.

## ЛИТЕРАТУРА


1. МР 26.4.001-2018 «Термины и определения в области технологий цепной записи данных (блокчейн) и распределенных реестров». `https://tc26.ru/standarts/metodicheskie-rekomendatsii/`
2. *Michels D.* Here's how GDPR and the blockchain can coexist. `https://thenextweb.com/syndication/2018/07/26/gdpr-blockchain-cryptocurrency/`
3. *Pankov K.* Enumeration of Boolean mapping with given cryptographic properties for personal data protection in blockchain data storage // Proc. 24th Conf. of Open Innovations Association FRUCT, Moscow, Russia, 2019. P. 300–306.
4. *Логачев О. А., Сальников А. А., Смышляев С. В., Ященко В. В.* Булевы функции в теории кодирования и криптологии. М.: МЦНМО, 2012.

5. *Carlet C.* Vectorial Boolean functions for cryptography // Boolean Models and Methods in Mathematics, Computer Science, and Engineering. Encyclopedia of Mathematics and its Applications. V. 134. N.Y.: Cambridge University Press, 2010. P. 398–472.
6. *Панков К. Н.* Оценки скорости сходимости в предельных теоремах для совместных распределений части характеристик случайных двоичных отображений // Прикладная дискретная математика. 2012. № 4. С. 14–30.
7. *Сачков В. Н.* Курс комбинаторного анализа. Ижевск: НИЦ «Регулярная и хаотическая динамика», 2013, 336 с.
8. Словарь криптографических терминов. М.: МЦНМО, 2016. 94 с.
9. *Денисов О. В.* Локальная предельная теорема для распределения части спектра случайной двоичной функции // Дискретная математика. 2000. № 1. С. 82–95.
10. *Панков К. Н.* Уточнённые асимптотические оценки для числа $(n, m, k)$-устойчивых двоичных отображений // Прикладная дискретная математика. Приложение. 2017. № 10. С. 46–49.
11. *Панков К. Н.* Уточнённые асимптотические оценки для числа корреляционно-иммунных двоичных функций и отображений // Прикладная дискретная математика. Приложение. 2018. № 11. С. 49–52.
12. *Canfield E. R., Gao Z., Greenhill C., et al.* Asymptotic enumeration of correlation-immune Boolean functions // Cryptography and Communications. 2010. No. 1. P. 111–126.
13. *Панков К. Н.* Асимптотические оценки для чисел двоичных отображений с заданными криптографическими свойствами // Математические вопросы криптографии. 2014. № 4. С. 73–97.
14. *Панков К. Н.* Улучшенные асимптотические оценки для числа корреляционно-иммунных и $k$-эластичных двоичных вектор-функций // Дискретная математика. 2018. № 2. С. 73–98.
15. *Денисов О. В.* Асимптотическая формула для числа корреляционно-иммунных порядка $k$ булевых функций // Дискретная математика. 1991. № 2. С. 25–46.

УДК 519.7 DOI 10.17223/2226308X/12/20

# О КОМПОНЕНТАХ НЕКОТОРЫХ КЛАССОВ ОБРАТИМЫХ ВЕКТОРНЫХ БУЛЕВЫХ ФУНКЦИЙ[1]

И. А. Панкратова

В классе обратимых векторных булевых функций от $n$ переменных, координатные функции которых существенно зависят от всех переменных, рассматриваются подклассы $\mathcal{K}_n$ и $\mathcal{K}'_n$, функции в которых получены с помощью $n$ независимых транспозиций из тождественной подстановки и из подстановки, каждая координатная функция которой существенно зависит от одной переменной, соответственно. Приводятся некоторые свойства компонент функций из этих классов.

**Ключевые слова:** *векторная булева функция, обратимые функции, нелинейность векторной булевой функции, компонентная алгебраическая иммунность.*

Для $n \in \mathbb{N}$ рассмотрим обратимые векторные булевы функции $F = (f_1 \dots f_n)$ на $\mathbb{F}_2^n$, такие, что координатные функции $f_i : \mathbb{F}_2^n \to \mathbb{F}_2$, $i = 1, \dots, n$, существенно зависят от всех $n$ переменных. В [1] предложен алгоритм 1 построения некоторой такой функции, который состоит в следующем: стартуя с тождественной подстановки $G : \mathbb{F}_2^n \to \mathbb{F}_2^n$, на $i$-м шаге, $i = 1, \dots, n$, выбираем два соседних по $i$-й координате и не выбранных на предыдущих шагах вектора $a, b \in \mathbb{F}_2^n$ и меняем местами значения $G(a)$ и $G(b)$.

[1]Работа поддержана грантом РФФИ, проект № 17-01-00354.

Обозначим класс функций, которые можно получить алгоритмом 1, через $\mathcal{K}_n$. В [1] доказано, что $\mathcal{K}_n \neq \varnothing$ для всех $n > 2$; в [2] описаны некоторые свойства координат функций из $\mathcal{K}_n$.

В [1] предложена модификация алгоритма 1 построения функций из класса $\mathcal{K}_n$, состоящая в том, что отправной точкой алгоритма является не обязательно тождественная подстановка $G$, а такая, что каждая координатная функция существенно зависит ровно от одной переменной, т. е. $G = (g_1 \dots g_n)$, $g_i = x_{j_i}^{\sigma_i}$, где $\{j_1, \dots, j_n\} = \{1, \dots, n\}$, $\sigma_i \in \{0, 1\}$ и $x_i^0 = \overline{x_i}$, $x_i^1 = x_i$, $i = 1, \dots, n$. Будем называть эту модификацию алгоритмом $1'$, а класс функций, которые можно таким образом получить, обозначим $\mathcal{K}'_n$.

**Утверждение 1.** Пусть $F = (f_1 \dots f_n) \in \mathcal{K}_n$. Тогда для всех $i = 1, \dots, n$ функция $f_i$ имеет единственную линейную переменную $x_i$.

Пусть $v = (v_1 \dots v_n) \in (\mathbb{F}_2^n)^* = \mathbb{F}_2^n \setminus \{00 \dots 0\}$. *Компонентой функции* $F = (f_1 \dots f_n)$ называется скалярное произведение $vF : \mathbb{F}_2^n \to \mathbb{F}_2$, $vF(x) = \bigoplus\limits_{i=1}^{n} v_i f_i(x) = \bigoplus\limits_{v_i=1} f_i(x)$. Через $\mathrm{w}(v)$ обозначим вес вектора $v$ (количество единиц в нём).

**Утверждение 2.** Пусть $F = (f_1 \dots f_n) \in \mathcal{K}'_n$ и $F$ получена алгоритмом $1'$ из начальной подстановки $G = (x_{j_1}^{\sigma_1} \dots x_{j_n}^{\sigma_n})$. Тогда $f_i$ имеет единственную линейную переменную $x_{j_i}$, $i = 1, \dots, n$.

**Утверждение 3.** Пусть $F = (f_1 \dots f_n) \in \mathcal{K}'_n$. Тогда для всех $v = v_1 \dots v_n \in \mathbb{F}_2^n$, таких, что $\mathrm{w}(v) > 2$, компонентная функция $vF$ не имеет фиктивных и линейных переменных.

**Утверждение 4.** $|\mathcal{K}'_n| = 2^n\, n! |\mathcal{K}_n|$.

Приведём определения некоторых криптографических характеристик векторных булевых функций [3]. *Нелинейность* $N_F$ функции $F$ — минимальная нелинейность её компонент. *Степень* $\deg F$ функции $F$ — максимальная степень её компонент (совпадает с максимальной степенью координатных функций). *Компонентная алгебраическая иммунность* $\mathrm{AI}_{\mathrm{comp}}(F)$ функции $F$ — минимальная алгебраическая иммунность её компонент.

**Утверждение 5.** Для функции $F \in \mathcal{K}'_n$ выполняются следующие свойства:

1) $N_F = 2$;
2) $\deg F = n - 1$;
3) $\mathrm{AI}_{\mathrm{comp}}(F) = 2$;
4) если $v \in \mathbb{F}_2^n$ и $\mathrm{w}(v) \leqslant 2^{n-3}$, то нелинейность компонентной функции $vF$ равна $N_{vF} = 2\mathrm{w}(v)$.

Подробное изложение представленных результатов и доказательства утверждений можно найти в [4].

## ЛИТЕРАТУРА

1. *Pankratova I. A.* Construction of invertible vectorial Boolean functions with coordinates depending on given number of variables // Материалы Междунар. науч. конгресса по информатике: Информационные системы и технологии. Республика Беларусь, Минск, 24–27 окт. 2016. Минск: БГУ, 2016. С. 519–521.
2. *Карпова Л. А., Панкратова И. А.* Свойства координатных функций одного класса подстановок на $\mathbb{F}_2^n$ // Прикладная дискретная математика. Приложение. 2017. № 10. С. 38–40.

3. *Carlet C.* Vectorial Boolean Functions for Cryptography. Cambridge: Cambridge University Press, 2010. 93 p.
4. *Панкратова И. А.* Свойства компонент некоторых классов векторных булевых функций // Прикладная дискретная математика. 2019. № 44. С. 5–11.

УДК 519.713.2+519.714.5 DOI 10.17223/2226308X/12/21

# ЛИНЕЙНОЕ РАЗЛОЖЕНИЕ ДИСКРЕТНЫХ ФУНКЦИЙ В ТЕРМИНАХ ОПЕРАЦИИ СДВИГ-КОМПОЗИЦИИ

И. В. Чередник

Исследуется операция сдвиг-композиции дискретных функций, возникающая при гомоморфизмах конечных регистров сдвига. Для произвольной функции над конечным полем описаны все возможные представления в виде сдвиг-композиции двух функций, правая из которых линейная. Кроме того, изучена возможность представления произвольной функции над конечным полем сдвиг-композицией трёх функций, в которой обе крайние функции линейные. Доказано, что в случае простого поля для линейных функций, а также для квадратичных функций, линейных по крайней переменной, понятия приводимости и линейной приводимости совпадают.

**Ключевые слова:** *дискретные функции, конечные поля, регистр сдвига, сдвиг-композиция.*

## Введение

Пусть $\Omega_q$ — конечное множество из $q$ элементов. В данной работе будем использовать множество переменных $\{x_0, x_1, x_2, \ldots\}$, а множество всех функций $q$-значной логики от переменных $x_0, x_1, x_2, \ldots$ будем обозначать через $F_q$. Произвольную функцию $f \in F_q$ всегда можно рассматривать как функцию от соответствующего допустимого набора переменных $x_0, x_1, \ldots, x_n$. В работах отечественных криптографов К. Г. Таболова, В. А. Башева, А. Я. Прососова, В. И. Солодовникова и др. была введена и исследована (преимущественно в терминах гомоморфизмов регистров сдвига) операция сдвиг-композиции на множестве всех функций $F_q$:

$$f(x_0, \ldots, x_n) \lhd g(x_0, \ldots, x_m) = f(g(x_0, \ldots, x_m), \ldots, g(x_n, \ldots, x_{n+m})).$$

В работах перечисленных авторов в разной степени общности и направленности достаточно подробно исследована связь между представлением функции $f$ в виде сдвиг-композиции $f = g \lhd h$ и существованием гомоморфизма регистра сдвига, соответствующего функции $f$, на меньший регистр сдвига, соответствующий функции $g$ (все основные результаты по данной тематике единым образом изложены в [1]). Так, например, в [2] описаны все возможные представления функции $f$ над конечным полем $\mathbb{F}_q$ в виде $f = l \lhd g$, где $l$ — линейная, что позволило указать все возможные гомоморфизмы регистра сдвига с обратной связью $f$ на линейные регистры сдвига.

В настоящей работе предлагается описание всех возможных представлений произвольной функции $f$ над конечным полем $\mathbb{F}_q$ в виде $f = g \lhd l$, где $l$ — линейная. Кроме того, изучена возможность представления произвольной функции $f$ над конечным полем $\mathbb{F}_q$ в виде $f = l_1 \lhd g \lhd l_2$, где $l_1, l_2$ — линейные. Доказано, что в случае простого поля для линейных функций, а также для квадратичных функций, линейных по крайней переменной, понятия приводимости и линейной приводимости совпадают.

## 1. Основные определения и обозначения

В данной работе, если не оговорено противное, полагается, что $q = p^t$, где $p$ — простое, $t \in \mathbb{N}$, а на множестве $\Omega_q$ задана структура поля $(\mathbb{F}_q, +, \cdot)$. Известно [3], что каждая функция $f \in F_q$ представляется единственным приведённым многочленом из $\mathbb{F}_q[x_0, x_1, \dots]$, который для удобства будем отождествлять с функцией $f$.

Для полноты и простоты изложения примеры в данной работе рассматриваются преимущественно в булевом случае, при этом операция сложения в поле $\mathbb{F}_2$ выделяется символом «$\oplus$».

Множество всех $q$-значных функций, которые биективны по первой (последней) переменной, будем обозначать через ${}^*F_q$ ($F_q^*$); множество всех $q$-значных функций, которые линейны по первой (последней) переменной, будем обозначать через ${}^+F_q$ ($F_q^+$); множество всех функций, сохраняющих константу 0, будем обозначать $\widehat{F}_q$. При этом естественны производные обозначения

$$ {}^*F_q^* = F_q^* \cap {}^*F_q, \quad {}^+F_q^+ = {}^+F_q \cap F_q^+, \quad {}^*\widehat{F}_q = {}^*F_q \cap \widehat{F}_q, \quad \dots $$

Как нетрудно убедиться, каждое из множеств ${}^+F_q \subset {}^*F_q \subset F_q$ образует полугруппу относительно операции $\lhd$ с нейтральным элементом $x_0$. При этом несложный пример

$$ (x_0 \oplus x_1) \lhd (x_0 \oplus x_1) = (x_0 \oplus x_1) \lhd (x_0 \oplus x_1 \oplus 1) $$

показывает, что даже в рамках моноида $({}^+F_q, \lhd)$ не всегда возможно производить правое сокращение в равенствах. Однако возможность правого и левого сокращений всё же присутствует в достаточно широких классах практически значимых функций.

**Утверждение 1.** Множества ${}^*\widehat{F}_q$, $\widehat{F}_q^*$, ${}^*\widehat{F}_q^*$ и ${}^+\widehat{F}_q$, $\widehat{F}_q^+$, ${}^+\widehat{F}_q^+$ образуют моноиды с возможностью левого и правого сокращений.

Будем говорить, что *функция $g$ делит справа функцию $f$*, если существует такая функция $h$, для которой выполняется равенство $f = h \lhd g$. Для каждой перестановки $\pi$ элементов множества $\Omega_q$ произвольная функция $f$ всегда делится справа на $\pi(x_0), \pi(f)$ — такие делители функции $f$ будем называть *несобственными*. Аналогичным образом определяются соответствующие понятия левой делимости. Если у функции $f$ существует собственный правый, а следовательно, и собственный левый делители, то будем говорить, что функция $f$ *приводима*.

**Замечание 1.** Пусть $f \in F_q$ и $f(0, \dots, 0) = c_f$. Существует тесная связь между приводимостью $f$ в моноиде $(F_q, \lhd)$ и приводимостью $\hat{f} = f - c_f$ в подмоноиде $(\widehat{F}_q, \lhd)$:

$$ f = g \lhd h \iff \hat{f} = (x_0 - c_f) \lhd g \lhd (x_0 + c_h) \lhd \hat{h}, \quad \text{где } (x_0 - c_f) \lhd g \lhd (x_0 + c_h), \hat{h} \in \widehat{F}_q. $$

Таким образом, исследование приводимости в моноиде $(F_q, \lhd)$ во многом сводится к исследованию приводимости в подмоноиде $(\widehat{F}_q, \lhd)$.

## 2. Линейное разложение

Множество $L_q$ всех функций, представимых линейными, но не аффинными многочленами над $\mathbb{F}_q$

$$ c_{i_0} x_{i_0} + c_{i_1} x_{i_1} + \dots + c_{i_k} x_{i_k} \ : \ i_0 < i_1 < \dots < i_k, k \in \mathbb{N}, \ c_{i_0}, c_{i_1}, \dots, c_{i_k} \in \mathbb{F}_q, $$

образует коммутативное кольцо $(L_q, +, \lhd)$, а отображение

$$ c_{i_0} x^{i_0} + c_{i_1} x^{i_1} + \dots + c_{i_k} x^{i_k} \mapsto c_{i_0} x_{i_0} + c_{i_1} x_{i_1} + \dots + c_{i_k} x_{i_k} $$

является изоморфизмом колец $(\mathbb{F}_q[x], +, \cdot)$ и $(L_q, +, \lhd)$ [1, 2, 4]. Подразумевая этот изоморфизм, далее будем формулировать известные понятия и использовать известные утверждения о делимости многочленов применительно к линейным функциям.

По понятным причинам класс $L_q$ является важным с практической точки зрения подмоноидом в $(F_q, \lhd)$ и выделение у произвольной функции левых или правых линейных делителей представляется естественной и актуальной задачей. Функцию $f \in F_q$ будем называть *линейно приводимой справа*, если у нее существует собственный правый делитель $l \in L_q$. В противном случае функцию $f$ будем называть *линейно неприводимой справа*. Аналогичным образом определяется левая линейная приводимость функций. Функцию будем называть *линейно неприводимой*, если она линейно неприводима и справа, и слева.

В. И. Солодовников в [2] описал все возможные левые линейные разложения для произвольной функции из $\widehat{F}_q$.

**Теорема 1** [2]. Произвольная функция $f \in \widehat{F}_q$ однозначно представляется в виде

$$f = \sum_{\substack{1 \leqslant i_1 < \ldots < i_k, \\ 1 \leqslant a_0, a_1, \ldots, a_k < q}} l_{i_1,\ldots,i_k;a_0,a_1,\ldots,a_k} \lhd x_0^{a_0} x_{i_1}^{a_1} \ldots x_{i_k}^{a_k},$$

где $l_{i_1,\ldots,i_k;a_0,a_1,\ldots,a_k} \in L_q$ для всех $1 \leqslant i_1 < \ldots < i_k,\ 0 < a_0, a_1, \ldots, a_k < q$.

При этом все левые линейные делители функции $f$ исчерпываются делителями $l = \text{НОД}(l_{i_1,\ldots,i_k;a_0,a_1,\ldots,a_k} : 1 \leqslant i_1 < \ldots < i_k,\ 0 < a_0, a_1, \ldots, a_k < q)$. В частности, функция $f$ линейно неприводима слева в том и только в том случае, когда $l = x_0$.

Линейную функцию вида $x_0 + a_1 x_{i_1} + \ldots + a_k x_{i_k}$ будем называть *унитарной по переменной* $x_0$.

**Следствие 1** [2]. Произвольная функция $f \in \widehat{F}_q$ однозначно представляется в виде $f = x_s \lhd l \lhd g$, где $x_s$ — крайняя левая переменная, от которой $f$ зависит существенным образом; $l \in L_q$ — унитарная по переменной $x_0$; $g$ — линейно неприводимая слева.

Для описания правых делителей потребуются дополнительные обозначения. Известно [5, 6], что в случае $q = p^t$, где $p$ — простое, $t > 1$, степень нелинейности приведённого одночлена $x^a \in \mathbb{F}_q[x]$, $a < q$, лучше оценивать не самим числом $a$, а его $p$-ичным весом

$$\|a\|_p = a_0 + \ldots + a_{t-1},$$

определяемым из $p$-ичного представления

$$a = a_0 + \ldots + a_{t-1} p^{t-1},\ 0 \leqslant a_0, \ldots, a_{t-1} < p.$$

В связи с этим одночлен $x^a$ часто расписывают в виде $x^{a_0} \ldots x^{p^{t-1} a_{t-1}}$, а произвольный приведённый моном $\mathbf{x}^{\mathbf{a}} = x_0^{a_0} \ldots x_n^{a_n}$, где $0 \leqslant a_0, \ldots, a_n < q$ и $a_i = a_{i0} + \ldots + a_{it-1} p^{t-1}$, $i \in \{0, \ldots, n\}$, — в виде

$$\mathbf{x}^{\mathbf{a^p}} = x_0^{a_{00}} \ldots x_0^{p^{t-1} a_{0t-1}} \ldots x_n^{a_{n0}} \ldots x_n^{p^{t-1} a_{nt-1}},$$

подразумевая при этом $\mathbf{a^p} = (a_{00}, \ldots, a_{0t-1}, \ldots, a_{n0}, \ldots, a_{nt-1})$.

Отношение градуированного лексикографического порядка на $\mathbb{N}_0^{(n+1)t}$ индуцирует отношение порядка на множестве приведенных мономов из $\mathbb{F}_q[x_0, \ldots, x_n]$

$$\mathbf{x}^{\mathbf{a^p}} \geqslant \mathbf{x}^{\mathbf{b^p}} \quad \Leftrightarrow \quad \mathbf{a^p} \geqslant_{\text{grlex}} \mathbf{b^p},$$

при котором мономы сначала упорядочиваются по степени нелинейности, а мономы одной степени нелинейности упорядочиваются «лексикографически» при условии

$$x_0 > \ldots > x_0^{p^{t-1}} > \ldots > x_n > \ldots > x_n^{p^{t-1}}.$$

При простом $q$ введённое отношение порядка совпадает со стандартным градуированным лексикографическим порядком на множестве всех приведённых мономов из $\mathbb{F}_q[x_0, \ldots, x_n]$.

Пусть

$$\mathbf{x}^{\mathbf{a^P}} = x_{i_0}^{a_{00}} \ldots x_{i_0}^{p^{t-1}a_{0t-1}} \ldots x_{i_k}^{a_{k0}} \ldots x_{i_k}^{p^{r-1}a_{kr-1}} x_{i_k}^{p^r a_{kr}}, \quad 0 < a_{kr} < p.$$

Тогда мономы

$$x_{i_0}^{a_{00}} \ldots x_{i_0}^{p^{t-1}a_{0t-1}} \ldots x_{i_k}^{a_{k0}} \ldots x_{i_k}^{p^{r-1}a_{kr-1}} x_{i_k}^{p^r(a_{kr}-1)} x_{i_k+j}^{p^r}, \quad j \geqslant 1,$$

и только их будем называть *линейно связанными с мономом* $\mathbf{x}^{\mathbf{a^P}}$.

**Теорема 2.** Произвольная функция $f \in F_q$ однозначно представляется в виде

$$f = c + \sum_{i=0}^{m} c_i \, \mathbf{x}^{\mathbf{a}_i^{\mathbf{P}}} \lhd l_i(x_0, \ldots),$$

где $c \in \Omega_q$; $\mathbf{x}^{\mathbf{a}_0^{\mathbf{P}}} > \ldots > \mathbf{x}^{\mathbf{a}_m^{\mathbf{P}}}$ — убывающая последовательность линейно несвязанных мономов, и для каждого $i \in \{0, \ldots, m\}$ коэффициент $c_i \in \Omega_q$ отличен от 0, а $l_i(x_0, \ldots)$ — линейная функция, унитарная по переменной $x_0$.

При этом если $f$ существенно зависит от переменной $x_0$, то все правые линейные делители функции $f$ исчерпываются делителями НОД$\,(l_0, \ldots, l_m)$. В частности, функция $f$ линейно неприводима справа в том и только в том случае, когда НОД$\,(l_0, \ldots, l_m) = x_0$.

**Следствие 2.** Произвольная функция $f \in F_q$ однозначно представляется в виде $f = x_s \lhd g \lhd l$, где $x_s$ — крайняя левая переменная, от которой $f$ зависит существенным образом; $g$ — линейно неприводимая справа; $l \in L_q$ — унитарная по переменной $x_0$.

**Замечание 2.** Представление, доказанное в теореме 2, существенным образом зависит от условий $x_0 > \ldots > x_0^{p^{t-1}} > \ldots\ldots > x_n > \ldots > x_n^{p^{t-1}}$. Так, для функции

$$f = x_0^3 + x_0^2 x_2 + x_0 x_1^2 + x_0 x_2^2$$

над полем $\mathbb{F}_4$ при условии $x_0 > x_0^2 > x_1 > x_1^2 > x_2 > x_2^2$ справедливо разложение

$$f = x_0 x_0^2 \lhd (x_0 + x_1 + x_2) + x_1 x_1^2 \lhd (x_0 + x_1) + x_0^2 x_1 \lhd x_0,$$

а при условии $x_0^2 > x_0 > x_1^2 > x_1 > x_2^2 > x_2$ — разложение

$$f = x_0^2 x_0 \lhd (x_0 + x_2) + x_0 x_1^2 \lhd x_0 + x_2^2 x_2 \lhd x_0.$$

### 3. Особенности двустороннего линейного разложения

**Теорема 3.** Пусть $q$ простое и функция $f \in F_q$ делится слева на $l_1 \in L_q$, а справа на $l_2 \in L_q$. Тогда если $l_1$ и $l_2$ взаимно просты, то справедливо разложение

$$f = l_1 \lhd g \lhd l_2.$$

Если, дополнительно, $l_1$ и $l_2$ — максимальные левый и правый делители функции $f$, то $g$ — линейно неприводимая.

**Замечание 3.** Условие простоты $q$ является существенным в теореме 3. Так, например, если $q = p^t$, $t \geqslant 2$ и $\alpha \in \mathbb{F}_q \backslash \mathbb{F}_p$, то $\alpha^p \neq \alpha$ и, очевидно, линейные функции $x_0 + \alpha x_1$, $x_0 + \alpha^p x_1$ взаимно просты. Однако при этом справедливы разложения

$$(x_0 + \alpha^p x_1^p) \lhd x_0^p = x_0^p + \alpha^p x_1^p = x_0^p \lhd (x_0 + \alpha x_1)$$

и легко убедиться в невозможности представления

$$x_0^p + \alpha^p x_1^p = (x_0 + \alpha^p x_1^p) \lhd g \lhd (x_0 + \alpha x_1).$$

**Замечание 4.** Условие взаимной простоты левого и правого линейных делителей является существенным в теореме 3. Так, например, для булевой функции

$$f = (x_0 \oplus x_1) \lhd x_0 x_1 \lhd (x_0 \oplus x_1) \oplus (x_0 \oplus x_1)$$

справедливы разложения

$$f = (x_0 \oplus x_1) \lhd (x_0 x_1 \oplus x_0 x_2 \oplus x_1 x_2 \oplus x_0 \oplus x_1) = (x_0 \oplus x_1) \lhd g_1,$$
$$f = (x_0 x_1 \oplus x_1 x_2 \oplus x_0) \lhd (x_0 \oplus x_1) = g_2 \lhd (x_0 \oplus x_1),$$

но при этом $g_1$ — линейно неприводимая справа, $g_2$ — линейно неприводимая слева, а потому невозможно представление

$$f = (x_0 \oplus x_1) \lhd g \lhd (x_0 \oplus x_1).$$

### 4. Квадратичные функции над простым полем

Ввиду изоморфизма колец $(L_q, +, \lhd)$ и $(\mathbb{F}_q, +, \cdot)$ описание всех линейных делителей произвольной функции $f \in L_q$ равносильно определению канонического разложения соответствующего многочлена.

Для описания линейных делителей произвольной квадратичной функции можно использовать результаты теорем 2 и 3 и, как показывает следующий результат, в случае линейных по крайней переменной квадратичных функций над простым полем это позволяет описать вообще все возможные делители.

**Теорема 4.** Если $q$ — простое число, то для композиции $f \lhd g$ произвольных функций $f \in F_q$ и $g \in {}^+F_q \cup F_q^+$ справедливы следующие утверждения:

1) $\deg(f \lhd g) = 0$ тогда и только тогда, когда $\deg f = 0$;
2) $\deg(f \lhd g) = 1$ тогда и только тогда, когда $\deg f = \deg g = 1$;
3) $\deg(f \lhd g) = 2$ тогда и только тогда, когда либо $\deg f = 1$ и $\deg g = 2$, либо $\deg f = 2$ и $\deg g = 1$.

**Замечание 5.** Пункт 2 теоремы 4 в частном случае $q = 2$ был доказан В. И. Солодовниковым в 1978 г. [1].

**Замечание 6.** Простой пример

$$(x_1 x_4 \oplus x_2 x_3 x_4) \lhd (x_0 \oplus x_1 x_2 \oplus x_2) = x_1 x_4 \oplus x_1 x_5 x_6 \oplus x_1 x_6 \oplus x_3 x_4 \oplus x_3 x_5 x_6 \oplus x_3 x_6$$

показывает, что уже в случае кубических функций понятие приводимости становится шире понятия линейной приводимости.

ЛИТЕРАТУРА

1. *Солодовников В. И.* Регистры сдвига и криптоалгоритмы на их основе. LAP LAMBERT Academic Publishing, 2017.
2. *Солодовников В. И.* Гомоморфизмы регистров сдвига в линейные автоматы // Дискретная математика. 2008. № 4. С. 87–101.
3. *Лидл Р., Нидеррайтер Г.* Конечные поля. М.: Мир, 1988.
4. *Солодовников В. И.* Гомоморфизмы двоичных регистров сдвига // Дискретная математика. 2005. № 1. С. 73–88.
5. *Кузьмин А. С., Нечаев А. А., Шишкин В. А.* Бент- и гипербент-функции над конечным полем // Труды по дискретной математике. 2007. № 10. С. 97–122.
6. *Черемушкин А. В.* Аддитивный подход к определению степени нелинейности дискретной функции // Прикладная дискретная математика. 2010. № 2. С. 22–33.

УДК 519.7 DOI 10.17223/2226308X/12/22

# О ВЗАИМОСВЯЗИ МЕЖДУ КВАТЕРНАРНЫМИ И БУЛЕВЫМИ БЕНТ-ФУНКЦИЯМИ[1]

А. С. Шапоренко

Исследуются кватернарные бент-функции вида $f : \mathbb{Z}_4^n \to \mathbb{Z}_4$. Показано представление коэффициентов Уолша — Адамара кватернарной функции через коэффициенты двух булевых функций. Получено, что любая кватернарная бент-функция является регулярной. Изучается связь кватернарных бент-функций от одной и двух переменных с булевыми бент-функциями от двух и четырёх переменных соответственно.

**Ключевые слова:** *кватернарные функции, булевы функции, регулярные бент-функции.*

Пусть $\langle x, y\rangle$ — скалярное произведение векторов, где суммирование производится по модулю 2, а $x.y$ — скалярное произведение векторов с суммированием по модулю 4.

*Преобразованием Уолша — Адамара булевой функции* $f$ от $n$ переменных называется целочисленная функция $W_f(x)$, заданная на множестве $\mathbb{Z}_2^n$ равенством

$$W_f(x) = \sum_{y \in \mathbb{Z}_2^n} (-1)^{\langle x,y\rangle \oplus f(y)}.$$

Булева функция $f$ от $n$ ($n$ — чётное) переменных называется *бент-функцией*, если $|W_f(x)| = 2^{n/2}$ для любого $x \in \mathbb{Z}_2^n$.

Функция $g : \mathbb{Z}_4^n \to \mathbb{Z}_4$ называется *кватернарной функцией* от $n$ переменных [1]. *Преобразование Уолша — Адамара кватернарной функции* $g$ определяется следующим образом:

$$W_g(x) = \sum_{y \in \mathbb{Z}_4^n} i^{x.y+g(y)}.$$

Здесь «+» означает сложение по модулю 4.

Кватернарная функция $g$ от $n$ переменных называется *бент-функцией*, если $|W_g(x)| = 4^{n/2}$ для любого $x \in \mathbb{Z}_4^n$.

[1]Работа выполнена при финансовой поддержке РФФИ (проект № 18-07-01394), Министерства образования и науки (Задание № 1.13559.2019/13.1 и Программа 5-100).

Пусть кватернарная функция $g$ от $n$ переменных задается для любых $x, y \in \mathbb{Z}_2^n$ следующим образом:

$$g(x + 2y) = a(x, y) + 2b(x, y),$$

где сложение производится по модулю 4; $a$ и $b$ — булевы функции от $2n$ переменных.

**Лемма 1.** Справедлива следующая связь коэффициентов Уолша — Адамара функций $g, b$ и $a \oplus b$:

$$W_g(x + 2y) = \frac{1}{2}(W_b(x \oplus y, y) + W_{a\oplus b}(y, x) - 2c_1 - 2d_1) +$$
$$+\frac{i}{2}(W_b(y, x) - W_{a\oplus b}(x \oplus y, x) - 2c_2 + 2d_2),$$

где

$$c_1 = \sum_{x'\in X_1, y'\in\mathbb{Z}_2^n} (-1)^{b(x',y')\oplus\langle x,y'\rangle\oplus\langle y,x'\rangle\oplus\langle x,x'\rangle},\ c_2 = \sum_{x'\in X_1, y'\in\mathbb{Z}_2^n} (-1)^{b(x',y')\oplus\langle x,y'\rangle\oplus\langle y,x'\rangle},$$
$$d_1 = \sum_{x'\in X_1, y'\in\mathbb{Z}_2^n} (-1)^{b(x',y')\oplus a(x',y')\oplus\langle x,y'\rangle\oplus\langle y,x'\rangle},\ d_2 = \sum_{x'\in X_1, y'\in\mathbb{Z}_2^n} (-1)^{b(x',y')\oplus a(x',y')\oplus\langle x,y'\rangle\oplus\langle y,x'\rangle\oplus\langle x,x'\rangle}.$$

Множество $X_1$ состоит из всех таких $x' \in \mathbb{Z}_2^n$, для которых равенство $\langle x, x'\rangle = x.x'$ не выполняется.

Кватернарная бент-функция $g : \mathbb{Z}_4^n \to \mathbb{Z}_4$ называется *регулярной* [2], если каждый коэффициент Уолша — Адамара этой функции может быть представлен в виде $W_g(x) = 4^{n/2} i^{h(x)}$, где $h(x)$ — некоторая кватернарная функция.

**Теорема 1.** Кватернарная бент-функция $g : \mathbb{Z}_4^n \to \mathbb{Z}_4$ является регулярной при любом $n$.

Из леммы 1 следует, что для $n = 1$

$$W_g(x + 2y) = \frac{1}{2}(W_b(x \oplus y, y) + W_{a\oplus b}(y, x)) + \frac{i}{2}(W_b(y, x) - W_{a\oplus b}(x \oplus y, x)),$$

так как множество $X_1$ пусто для любого $x$.

**Утверждение 1.** Пусть функция $g(x + 2y) = a(x, y) + 2b(x, y)$, где $x, y \in \mathbb{Z}_2$; $a$ и $b$ — булевы функции от двух переменных, является бент-функцией. Тогда $b$ и $a \oplus b$ — бент-функции. Обратное, вообще говоря, не верно.

Так, функция $g(x_1+2x_2) = x_2+2x_1x_2$ не является бент-функцией, но $b(x_1, x_2) = x_1x_2$ и $a(x_1, x_2) \oplus b(x_1, x_2) = x_1x_2 \oplus x_2$ — бент-функции.

Компьютерные вычисления показали, что количество кватернарных бент-функций от одной переменной равно 32. Чтобы получить каждую из них, достаточно взять в качестве функции $b(x_1, x_2)$ любую из восьми булевых бент-функций от двух переменных и использовать одну из четырёх функций $0, 1, x_1$ или $x_1 \oplus 1$ в качестве функции $a(x_1, x_2)$.

Количество кватернарных бент-функций при $n = 2$ равно 200704. Среди них 98304 — таких, что ни одна из булевых функций $a, b$ и $a \oplus b$ не является бент-функцией, но при этом для 3072 из них $a$ линейная. Существуют 36864 функции, таких, что $b$ и $a \oplus b$ — бент-функции, при этом для 33792 из них функция $a$ нелинейная, а для 2304 и 768 является линейной функцией и константой соответственно. Количество кватернарных функций, для которых каждая из функций $a, b$ и $a \oplus b$ — бент-функция, равно 16384. Для оставшихся 49152 функций $a$ является бент-функцией, а $b$ и $a \oplus b$ — нелинейные булевы функции. Интересно, что среди всех кватернарных бент-функций нет ни одной, для которой $b$ или $a \oplus b$ были бы линейными или константами.

ЛИТЕРАТУРА

1. *Kumar P. V., Scholtz R. A., and Welch L. R.* Generalized bent functions and their properties // J. Combin. Theory. Ser. A40. 1985. P. 90–107.
2. *Tokareva N.* Bent Functions: Results and Applications to Cryptography. Acad. Press, 2015.

УДК 621.391:519.7 DOI 10.17223/2226308X/12/23

# КЛАСС БУЛЕВЫХ ФУНКЦИЙ, ПОСТРОЕННЫХ С ИСПОЛЬЗОВАНИЕМ ДВОИЧНЫХ РАЗРЯДНЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ ЛИНЕЙНЫХ РЕКУРРЕНТ НАД КОЛЬЦОМ $\mathbb{Z}_{2^n}$

Д. У. Эрнандес Пилото

Рассматривается класс булевых функций, построенных на основе двоичных разрядных последовательностей линейных рекуррент над кольцом $\mathbb{Z}_{2^n}$ с отмеченным характеристическим многочленом максимального периода. Для этого класса изучаются веса функций, степень нелинейности функций, расстояние между функциями. Кроме того, рассматривается расстояние между функциями из разных классов.

**Ключевые слова:** *булевы функции, линейные рекуррентные последовательности, двоичные разрядные последовательности.*

## Введение

Пусть $R = \mathbb{Z}_{2^n}$ — кольцо вычетов по модулю $2^n$, $F(x)$ — отмеченный многочлен степени $m$ максимального периода $T(F) = 2^m - 1$ над кольцом $R$ [1]. Введём обозначения: $P = \mathbb{Z}_2$; $\bar{F}(x)$ — многочлен, полученный из $F(x)$ приведением всех его коэффициентов по модулю 2. Тогда $T(\bar{F}) = 2^m - 1$ и $\bar{F}(x)$ является примитивным многочленом над полем $P$. Пусть $\omega_1, \ldots, \omega_m$ — линейно независимая система линейных рекуррентных последовательностей (ЛРП) над полем $P$ с характеристическим многочленом $\bar{F}(x)$. Обозначим через $L_R(F)^*$ множество всех ЛРП $u$ над кольцом $R$, у которых среди элементов $u(0), \ldots, u(m-1)$ есть хотя бы один обратимый элемент кольца $R$. Рассмотрим функцию $\psi : R \longrightarrow P$, действующую на каждый элемент $a \in R$ с двоичным представлением

$$a = a_0 + 2a_1 + 2^2a_2 + \ldots + 2^{n-1}a_{n-1}, \quad a_0, a_1, \ldots a_{n-1} \in P$$

по правилу

$$\psi(a) = a_{n-1} \oplus a_{n-2}a_{n-3} \ldots a_{n-k}, \tag{1}$$

где $n \geqslant 3$; $k \in \{3, \ldots, n\}$. Для каждой ЛРП $u \in L_R(F)^*$ рассмотрим булеву функцию $f(x_1, \ldots, x_m) = f_{u,\psi}(x_1, \ldots, x_m)$, определённую по следующему правилу: $f(0, \ldots, 0) = \psi(0)$ и для всех $i \in \{0, \ldots, 2^m - 2\}$

$$f(\omega_1(i), \ldots, \omega_m(i)) = \psi(u(i)). \tag{2}$$

Пусть $\chi : R \longrightarrow \mathbb{C}^*$ — аддитивный характер кольца $R$, определённый равенством

$$\chi(x) = e^{2\pi i x/2^n}, \ x \in R.$$

Группа всех аддитивных характеров кольца $R$ имеет вид $\{\chi(ax) : a \in R\}$. Множество всех отображений из $R$ в $\mathbb{C}^*$ образует унитарное пространство со скалярным произведением, определённым для отображений $g$ и $h$ по правилу

$$\langle g, h \rangle = \sum_{x \in R} g(x)\bar{h}(x).$$

Система функций $\chi(ax)$, $a \in R$, образует ортогональный базис рассматриваемого пространства, поэтому найдутся однозначно определённые числа $\nu_j = \nu_j(\psi) \in \mathbb{C}$, такие, что

$$(-1)^{\psi(x)} = \sum_{j \in R} \nu_j \chi(jx),\ x \in R.$$

Они однозначно вычисляются по формуле

$$\nu_j = \frac{1}{2^n} \sum_{a \in R} (-1)^{\psi(a)} \chi(-aj).$$

Введём обозначение $\sigma(\psi) = \sum\limits_{j \in R} |\nu_j|$.

## 1. Свойства функций нового класса

Для суммы модулей чисел $\nu_j$ получим следующую оценку:

**Теорема 1.** Пусть отображение $\psi$ задано равенством (1) и $k = 3$, тогда

$$\sigma(\psi) \leqslant \frac{2}{\pi} \ln(2^{n-1}) + 1.$$

Эта оценка позволяет доказать теорему:

**Теорема 2.** Пусть $f$ — функция, определённая равенством (2) и $k = 3$, тогда

1) вес $f$ удовлетворяет неравенствам

$$2^{m-1} - \left(\frac{2}{\pi} \ln(2^{n-1}) + 1\right)(2^{n-1} - 1)2^{m/2-1} \leqslant \|f\| \leqslant$$
$$\leqslant 2^{m-1} + \left(\frac{2}{\pi} \ln(2^{n-1}) + 1\right)(2^{n-1} - 1)2^{m/2-1};$$

2) если $f = f_{u,\psi}$, $g = f_{v,\psi}$ и ЛРП $u, v$ не пропорциональны в $R^*$, то расстояние Хэмминга $\rho(f, g)$ между столбцами значений рассматриваемых функций удовлетворяет соотношениям

$$2^{m-1} - \left(\frac{2}{\pi} \ln(2^{n-1}) + 1\right)^2 (2^{n-1} - 1)2^{m/2-1} \leqslant \rho(f, g) \leqslant$$
$$\leqslant 2^{m-1} + \left(\frac{2}{\pi} \ln(2^{n-1}) + 1\right)^2 (2^{n-1} - 1)2^{m/2-1};$$

3) для нелинейности $\mathrm{nl}(f)$ верна оценка

$$\mathrm{nl}(f) \geqslant 2^{m-1} - \left(\frac{2}{\pi} \ln(2^{n-1}) + 1\right)(2^{n-1} - 1)2^{m/2-1}.$$

Для произвольных значений $k$ аналогичные результаты получить не удаётся. В общем виде справедливо

**Утверждение 1.** Пусть

$$\begin{aligned} \psi_1(a) &= a_{n-1} \oplus a_{n-2} \ldots a_{n-k}, \\ \psi_2(a) &= a_{n-1} \oplus a_{n-2} \ldots a_{n-k} a_{n-k-1}, \end{aligned}$$

где $k \in \{3, \ldots, n-1\}$. Тогда для $|\nu_j(\psi_2)|$ верна оценка

$$|\nu_j(\psi_2)| \leqslant \frac{1 + 2^{n-1} \sin(\pi j / 2^n) |\nu_j(\psi_1)|}{2^n \sin(\pi j / 2^n) |\cos(\pi j / 2^{k+1})|}.$$

Это утверждение позволяет оценить модули чисел $\nu_j(\psi_2)$, зная аналогичные коэффициенты для отображения $\psi_1$.

## 2. Расстояние Хэмминга между функциями

Изучим теперь для двух функций $f$ и $g$ из разных классов величину $\rho(f, g)$.

**Утверждение 2.** Пусть отображение $\psi_1$ задано равенством (1) и $\psi_2(a) = a_{n-1}$, $f = f_{u,\psi_1}$, $g = f_{u,\psi_2}$. Тогда

$$2^{m-k+1} - \frac{(2^n-1)(2^{n-1}-1)}{3}2^{m/2-k+2} \leqslant \rho(f,g) \leqslant 2^{m-k+1} + \frac{(2^n-1)(2^{n-1}-1)}{3}2^{m/2-k+2}.$$

Обозначим через $\varepsilon_1$, $\varepsilon_2$ соответственно левую и правую части неравенства из утверждения 2.

**Утверждение 3.** Пусть отображение $\psi_1$ задано равенством (1), $\psi_2(a) = a_{n-1} \oplus \oplus a_{n-2} \oplus a_{n-3} \oplus \ldots \oplus a_{n-k}$, где $k \in \{3, \ldots, n\}$, $f = f_{u,\psi_1}$, $g = f_{u,\psi_2}$. Тогда

$$\begin{array}{ll} (2^{k-2}+1)\varepsilon_1 \leqslant \rho(f,g) \leqslant (2^{k-2}+1)\varepsilon_2 & \text{для нечётного } k; \\ (2^{k-2}-1)\varepsilon_1 \leqslant \rho(f,g) \leqslant (2^{k-2}-1)\varepsilon_2 & \text{для чётного } k. \end{array}$$

## Заключение

В данной работе для класса булевых функций, построенных на основе двоичных разрядных последовательностей линейных рекуррент над кольцом $\mathbb{Z}_{2^n}$, получены оценки для веса функций, нелинейности и расстояний между функциями. Отметим, что ранее в работах [2–4] аналогичные вопросы были рассмотрены только для случая, когда $\psi$ — линейное отображение по всем двоичным разрядам.

## ЛИТЕРАТУРА


1. *Нечаев А. А.* Цикловые типы линейных подстановок над конечными коммутативными кольцами // Математический сборник. 1993. Т. 184. № 3. С. 21–56.
2. *Быльков Д. Н., Камловский О. В.* Параметры булевых функций, построенных с использованием старших координатных последовательностей линейных рекуррент // Математические вопросы криптографии. 2012. Т. 3. № 4. С. 25–53.
3. *Камловский О. В.* Нелинейность одного класса булевых функций, построенных с использованием двоичных разрядных последовательностей линейных рекуррент над кольцом $\mathbb{Z}_{2^n}$ // Математические вопросы криптографии. 2016. Т. 7. № 3. С. 29–46.
4. *Быльков Д. Н.* Об одном классе булевых функций, построенных с использованием старших разрядных последовательностей линейных рекуррент // Прикладная дискретная математика. Приложение. 2014. № 7. С. 59–60.


UDC 519.7 DOI 10.17223/2226308X/12/24

## PROPERTIES OF ASSOCIATED BOOLEAN FUNCTIONS OF QUADRATIC APN FUNCTIONS[1]

A. A. Gorodilova

For a function $F : \mathbb{F}_2^n \to \mathbb{F}_2^n$, it is defined the associated Boolean function $\gamma_F$ in $2n$ variables as follows: $\gamma_F(a, b) = 1$ if $a \neq \mathbf{0}$ and equation $F(x) + F(x + a) = b$ has solutions. A vectorial Boolean function $F$ from $\mathbb{F}_2^n$ to $\mathbb{F}_2^n$ is called almost perfect nonlinear (APN) if equation $F(x) + F(x + a) = b$ has at most 2 solutions for all vectors $a, b \in \mathbb{F}_2^n$, where $a$ is nonzero. In case when $F$ is a quadratic APN function its associated function has the form $\gamma_F(a, b) = \Phi_F(a) \cdot b + \varphi_F(a) + 1$ for appropriate

[1]The work is supported by RFBR, projects no. 18-31-00479 and 18-07-01394.

functions $\Phi_F : \mathbb{F}_2^n \to \mathbb{F}_2^n$ and $\varphi_F : \mathbb{F}_2^n \to \mathbb{F}_2$. We study properties of functions $\Phi_F$ and $\varphi_F$, in particular their degrees.

**Keywords:** *APN functions, associated Boolean functions, differential equivalence.*

## 1. Introduction

Let $\mathbb{F}_2^n$ be the $n$-dimensional vector space over $\mathbb{F}_2$. Let $\mathbf{0}$ denote the zero vector of $\mathbb{F}_2^n$; $x \cdot y = x_1y_1 + \ldots + x_ny_n$ denote the *inner product* of vectors $x, y \in \mathbb{F}_2^n$. A set $M \subseteq \mathbb{F}_2^n$ form a *linear subspace* if $x + y \in M$ for any $x, y \in M$. Here $+$ denotes the coordinate-wise sum of vectors modulo 2. A mapping $f : \mathbb{F}_2^n \to \mathbb{F}_2$ is a *Boolean function* of $n$ variables. The *Hamming weight* of $f$ is the number $\mathrm{wt}(f) = |\{x \in \mathbb{F}_2^n : \ f(x) = 1\}|$.

We consider a *vectorial Boolean function* $F : \mathbb{F}_2^n \to \mathbb{F}_2^n$, $F = (f_1, \ldots, f_n)$, where $f_i$ is the $i$-th *coordinate* function of $F$; a function $v \cdot F$ is a *component* function of $F$ for a nonzero $v \in \mathbb{F}_2^n$. The *algebraic normal form* (ANF) of $F$ is the following unique representation: $F(x) = \sum\limits_{I \in \mathcal{P}(N)} a_I \big( \prod\limits_{i \in I} x_i \big)$, where $\mathcal{P}(N)$ is the power set of $N = \{1, \ldots, n\}$ and each $a_I$ belongs to $\mathbb{F}_2^n$. The *algebraic degree* of $F$ is degree of its ANF: $\deg(F) = \max\{|I| : a_I \neq \mathbf{0}, I \in \mathcal{P}(N)\}$. Functions of algebraic degree 2 are called *quadratic*.

A function $F$ from $\mathbb{F}_2^n$ to itself is called *almost perfect nonlinear* (APN) (according to K. Nyberg [1]) if for any $a, b \in \mathbb{F}_2^n$, $a \neq \mathbf{0}$, equation $F(x) + F(x + a) = b$ has at most 2 solutions. APN functions are of special interest for using as S-boxes in block ciphers due to their optimal differential characteristics. Despite to fact that APN functions are intensively studied (see, for example, survey [2] of M. M. Glukhov), there are a lot of open problems on finding new constructions, classifications, etc.

In [3] C. Carlet, P. Charpin, and V. Zinoviev introduced the *associated Boolean function* $\gamma_F(a, b)$ in $2n$ variables for a given vectorial Boolean function $F$ from $\mathbb{F}_2^n$ to itself. It takes value 1 if $a \neq \mathbf{0}$ and equation $F(x) + F(x + a) = b$ has solutions. It is easy to see that $F$ is APN if and only if $\mathrm{wt}(\gamma_F) = 2^{2n-1} - 2^{n-1}$.

Two functions are called *differentially equivalent* [4] (or *$\gamma$-equivalent* according to K. Boura et al. [5]) if their associated functions coincide. The problem of describing the differential equivalence class of an APN function remains open even for quadratic case. That is why we are interested in obtaining some properties of $\gamma_F$. We will focus on quadratic APN functions.

Let $F$ be a quadratic APN function. Then $\gamma_F$ is of the form $\gamma_F(a, b) = \Phi_F(a) \cdot b + \varphi_F(a) + 1$, where $\Phi_F : \mathbb{F}_2^n \to \mathbb{F}_2^n$, $\varphi_F : \mathbb{F}_2^n \to \mathbb{F}_2$ are uniquely defined from

$$\{F(x) + F(x + a) : x \in \mathbb{F}_2^n\} = \{y \in \mathbb{F}_2^n : \ \Phi_F(a) \cdot y = \varphi_F(a)\}$$

for all $a \neq \mathbf{0}$ and $\Phi_F(\mathbf{0}) = \mathbf{0}$, $\varphi_F(\mathbf{0}) = 1$.

## 2. Properties of $\Phi_F$ and $\varphi_F$

In this section, we summarize known results and present new ones about properties of $\Phi_F$ and $\varphi_F$. As it usually happens the cases of even and odd number of variables are different.

P r o p e r t y 1: the image set of $\Phi_F$.

**Theorem 1** [3, 6]. Let $F$ be a quadratic APN function in $n$ variables.

1) If $n$ is odd, then $\Phi_F$ is a permutation.
2) If $n$ is even, then the preimage $\Phi_F$ of any nonzero vector is a linear subspace of even dimension together with the zero vector.

**Corollary 1.** Let $F$ be a quadratic APN function. Then $\Phi_F$ takes an odd number of distinct nonzero values.

P r o p e r t y 2: the degree of $\Phi_F$.

**Theorem 2** [4]. Let $F$ be a quadratic APN function in $n$ variables, $n \geqslant 3$, $n$ is odd. Then $\deg(\Phi_F) \leqslant n-2$.

**Theorem 3.** Let $F$ be a quadratic APN function in $n$ variables, $n \geqslant 4$, $n$ is even. Then each coordinate function of $\Phi_F$ is represented as $(\Phi_F)_i(x) = f_i(x) + \lambda_i\big(x_2 \dots x_n + x_1x_3 \dots x_n + \dots + x_1x_2 \dots x_{n-1} + x_1 \dots x_n\big)$, where $\deg(f_i) \leqslant n-2$ and $\lambda_i \in \mathbb{F}_2$.

**Remark 1.** For all known quadratic APN functions in not more than 11 variables, we computationally verified that

— for even $n$, the case $\deg((\Phi_F)_i) = n$ is not realized;
— any component function of $\Phi_F$ has degree exactly $n-2$.

Based on computational experiments we can formulate the following

**Hypothesis 1.** Let $F$ be a quadratic APN function in $n$ variables, $n \geqslant 3$. Then $\deg(v \cdot \Phi_F) = n-2$ for any nonzero $v \in \mathbb{F}_2^n$.

P r o p e r t y 3: the degree of $\varphi_F$.

**Proposition 1.** Let $F$ be a quadratic APN function in $n$ variables, $n$ is even. Then $\deg(\varphi_F) = n$, or, equivalently, $\mathrm{wt}(\varphi_F)$ is odd.

The case of odd $n$ remains open, but based on our computational experiments we can formulate the following

**Hypothesis 2.** Let $F$ be a quadratic APN function in $n$ variables, $n$ is odd. Then $\deg(\varphi_F) < n$, or, equivalently, $\mathrm{wt}(\varphi_F)$ is even.

REFERENCES

1. *Nyberg K.* Differentially uniform mappings for cryptography. EUROCRYPT'93, LNCS, 1994, vol. 765, pp. 55–64.
2. *Glukhov M. M.* O priblizhenii diskretnykh funktsiy lineynymi funktsiyami [On the approximation of discrete functions by linear functions]. Matematicheskie Voprosy Kriptografii, 2016, vol. 7, no. 4, pp. 29–50. (in Russian)
3. *Carlet C., Charpin P., and Zinoviev V.* Codes, bent functions and permutations suitable for DES-like cryptosystems. Designs, Codes and Cryptography, 1998, vol. 15, iss. 2, pp. 125–156.
4. *Gorodilova A.* On the differential equivalence of APN functions. Cryptography and Communications, 2019. `https://link.springer.com/article/10.1007/s12095-018-0329-y`.
5. *Boura C., Canteaut A., Jean J., and Suder V.* Two notions of differential equivalence on S-boxes. Designs, Codes and Cryptography, 2019, vol. 87, iss. 2–3, pp. 185–202.
6. *Gorodilova A.* Lineynyy spektr kvadratichnykh APN-funktsiy [The linear spectrum of quadratic APN functions]. Prikladnaya Diskretnaya Matematika, 2016, no 4(34), pp. 5–16. (in Russian)

Секция 3

# МАТЕМАТИЧЕСКИЕ МЕТОДЫ КРИПТОГРАФИИ

УДК 519.1 DOI 10.17223/2226308X/12/25

## О ПЕРЕМЕШИВАЮЩИХ СВОЙСТВАХ НЕСТАЦИОНАРНОГО РЕГИСТРА СДВИГА

Я. Э. Авезова

Для регистра сдвига длины $n$, функция обратной связи которого зависит от двоичного знака управляющей последовательности (на каждом такте реализуется одно из двух регистровых преобразований), исследовано минимальное число $\gamma$ тактов регистра, после которых достигнуто полное перемешивание, то есть существенная зависимость каждой координатной функции композиции преобразований от всех переменных. Эффект полного перемешивания оценен с помощью множества $\hat{\Gamma}$ перемешивающих $n$-вершинных орграфов регистровых преобразований, имеющих общий гамильтонов контур. Дана оценка экспонента $\exp\hat{\Gamma}$ примитивного множества $\hat{\Gamma}$, которая позволяет оценить снизу число $\gamma$:

$$\exp\hat{\Gamma} \leqslant 2n-2+\sum_{\alpha=0}^{1}\left(F(n-S(\varphi_\alpha))+d_\alpha+s^\alpha_{m(\alpha)}\right),$$

где $S(\varphi_\alpha)=\left\{s^\alpha_1,\ldots,s^\alpha_{m(\alpha)}\right\}$ — множество номеров существенных переменных функции обратной связи $\varphi_\alpha(x_0,\ldots,x_{n-1})$; $n-S(\varphi_\alpha)=\{n-s^\alpha_j : j=1,\ldots,m(\alpha)\}$; $d_\alpha=\text{НОД}\{n-S(\varphi_\alpha)\}$; $F(n-S(\varphi_\alpha))=d_\alpha\Phi((n-S(\varphi_\alpha))/d_\alpha)$; $\Phi((n-S(\varphi_\alpha))/d_\alpha)$ — число Фробениуса. Проведён вычислительный эксперимент при $n=6$ и 10 по вычислению точного значения $\gamma$ с учётом управляющей последовательности. Установлено, что полное перемешивание возможно за число тактов, превышающее значение экспонента менее чем в 2 раза.

**Ключевые слова:** *гамильтонов контур, примитивность множества орграфов, экспонент орграфа, экспонент множества орграфов.*

### Введение

Принцип перемешивания, описанный К. Шенноном [1], важен при построении криптографических систем, устойчивых к дифференциальному анализу и атакам, основанным на последовательном опробовании элементов ключа. Для хорошего перемешивания необходимо, чтобы преобразование было совершенным, т. е. чтобы каждая координатная функция существенно зависела от всех переменных [2]. Одним из способов построения совершенного преобразования является использование композиции нескольких преобразований, каждое из которых не является совершенным, но допускает относительно несложную реализацию.

Объектом исследования является нестационарный регистр сдвига (НРС) над пространством двоичных векторов $V_n$. Функция обратной связи НРС зависит от знака управляющей двоичной гаммы, за счёт чего на каждом такте реализуется одно из двух преобразований пространства $V_n$. Таким образом, за $t$ тактов работы НРС реа-

лизуется композиция преобразований длины $t$. Актуальной задачей является оценка перемешивающих свойств НРС в зависимости от управляющей последовательности.

## 1. Определяющие свойства перемешивания с помощью композиции функций

Пусть $G = \{g_1, \ldots, g_p\}$ — множество преобразований пространства двоичных векторов $V_n$, где $p, n > 1$. Преобразованию $g_\tau \in G$ поставим в соответствие орграф $\Gamma(g_\tau)$, в котором пара вершин $(i, j)$ является дугой, если и только если переменная $x_i$ преобразования $g_\tau$ является существенной для координатной функции с номером $j$. Орграф $\Gamma(g_\tau)$ называется перемешивающим графом преобразования $g_\tau$, $\tau = 1, \ldots, p$. Композиции функций $g(w) = g_{w_1} \ldots g_{w_s}$, где $g_{w_1}, \ldots, g_{w_s} \in G$, $s > 1$, соответствует перемешивающий граф $\Gamma(g(w)) = \Gamma(g_{w_1} \ldots g_{w_s})$. Преобразование $g(w)$ совершенное, если и только если $\Gamma(g(w))$ полный.

Пусть $\hat{\Gamma} = \{\Gamma_1, \ldots, \Gamma_p\}$ — множество орграфов, где $\Gamma_\tau = \Gamma(g_\tau)$, $\tau = 1, \ldots, p$. Тогда порождённая множеством $\hat{\Gamma}$ полугруппа имеет вид $\langle\hat{\Gamma}\rangle = \{\Gamma(w)\colon w \in N_p^*\}$, где $\Gamma(w) = \Gamma_{w_1} \ldots \Gamma_{w_s}$ при $w = w_1 \ldots w_s$; $N_p^*$ — множество всех слов в алфавите $\{1, \ldots, p\}$; умножение орграфов определяется как умножение бинарных отношений. Множество $\hat{\Gamma}$ называется примитивным, если полугруппа $\langle\hat{\Gamma}\rangle$ содержит полный орграф. Наименьшая длина произведения, соответствующего полному орграфу, называется экспонентом множества $\hat{\Gamma}$ и обозначается $\exp\hat{\Gamma}$. Известно [2], что орграф $\Gamma(g(w))$ является частью орграфа $\Gamma(w)$. Следовательно, если орграф $\Gamma(w)$ не полный, то преобразование $g(w)$ не является совершенным.

Таким образом, примитивность множества $\hat{\Gamma}$ является необходимым условием существования совершенной композиции преобразований из множества $G$. Если найден экспонент примитивного множества $\hat{\Gamma}$, то исключена необходимость проверять совершенность любой композиции, длина которой меньше $\exp\hat{\Gamma}$.

## 2. Перемешивающие свойства НРС

Нестационарным регистром левого сдвига над $V_n$ с обратной связью $\varphi(x_0, \ldots, x_{n-1}, \alpha)$ назовём отображение $g\colon V_{n+1} \to V_n$, если

$$g(x_0, \ldots, x_{n-1}, \alpha) = (x_1, \ldots, x_{n-1}, \varphi(x_0, \ldots, x_{n-1}, \alpha)),$$

где $\alpha$ — случайный или псевдослучайный двоичный знак управления; $\varphi(x_0, \ldots, x_{n-1}, \alpha) = (\alpha\oplus 1)\varphi_0(x_0, \ldots, x_{n-1}) \oplus \alpha\varphi_1(x_0, \ldots, x_{n-1})$; $\varphi_0$ и $\varphi_1$ — различные булевы функции от переменных $x_0, \ldots, x_{n-1}$.

Схема функционирования НРС представлена на рис. 1. Управляющую двоичную последовательность обозначим $\{\alpha_k\}$. В зависимости от знака гаммы $\alpha_k$ на $k$-м такте работы регистра сдвига реализуется одно преобразование из множества преобразований $\{g_0, g_1\}$, где $g_\alpha(x_0, \ldots, x_{n-1})$ — преобразование $V_n$, реализуемое регистром сдвига с функцией обратной связи $\varphi_\alpha(x_0, \ldots, x_{n-1})$, $\alpha \in \{0, 1\}$.

Перемешивающие свойства НРС моделируются множеством перемешивающих орграфов $\hat{\Gamma} = \{\Gamma(g_0), \Gamma(g_1)\}$, длины контуров которых определяются ячейками съёма регистра. Обозначим $S(\varphi_\alpha) = \left\{s_1^\alpha, \ldots, s_{m(\alpha)}^\alpha\right\}$ множество номеров существенных переменных функции $\varphi_\alpha(x_0, \ldots, x_{n-1})$, где $0 = s_1^\alpha < \ldots < s_{m(\alpha)}^\alpha \leqslant n-1$; $n - S(\varphi_\alpha) = \{n - s_j^\alpha\colon j = 1, \ldots, m(\alpha)\}$.

Орграф $\Gamma(g_\alpha)$ имеет множество простых контуров $\hat{C}(\varphi_\alpha) = \{C_1(\varphi_\alpha), \ldots, C_{m(\alpha)}(\varphi_\alpha)\}$, где $C_j(\varphi_\alpha) = (n-1, \ldots, s_j^\alpha + 1, s_j^\alpha)$ — контур длины $n - s_j^\alpha$, $j = 1, \ldots, m(\alpha)$. В каж-

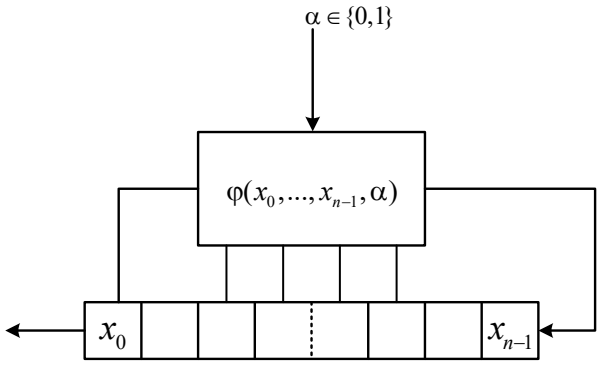


Рис. 1. Нестационарный регистр левого сдвига

дом орграфе множества $\hat{\Gamma}$ есть гамильтонов контур $(n-1,\dots,0)$. Согласно критерию примитивности множества орграфов с общим гамильтоновым контуром [3, теорема 4], множество $\hat{\Gamma}$ примитивное, если и только если орграф $U^{(2)}$ примитивный, где $U^{(2)}$ суть объединение орграфов $\Gamma(g_0)\cup\Gamma(g_1)$ с отождествлением кратных дуг. Поскольку $n-S(\varphi_\alpha)$ — множество длин простых контуров $\Gamma(g_\alpha)$, то орграф $U^{(2)}$ примитивный, если и только если НОД$\{n-(S(\varphi_0)\cup S(\varphi_1))\}=1$. Для экспонента примитивного множества справедлива оценка, которая следует из [3, теорема 4]:

$$\exp\hat{\Gamma}\leqslant 2n-2+\sum_{\alpha=0}^{1}\left(F(n-S(\varphi_\alpha))+d_\alpha+s^\alpha_{m(\alpha)}\right). \tag{1}$$

Здесь $d_\alpha=$ НОД$\{n-s^\alpha_j\colon j=1,\dots,m(\alpha)\}$; $F(n-S(\varphi_\alpha))=d_\alpha\Phi((n-S(\varphi_\alpha))/d_\alpha)$; $\Phi((n-S(\varphi_\alpha))/d_\alpha)$ — число Фробениуса; $(n-S(\varphi_\alpha))/d_\alpha=\{(n-s^\alpha_j)/d_\alpha\colon j=1,\dots,m(\alpha)\}$.

### 3. Экспериментальное исследование перемешивающих свойств НРС

Обозначим: $g_{\alpha_k}=g(x_0,\dots,x_{n-1},\alpha_k)$ — преобразование множества $V_n$, реализуемое НРС при знаке управляющей гаммы $\alpha_k$; $g(\alpha,t)=g_{\alpha_t}\dots g_{\alpha_1}$ — композиция преобразований, реализуемая за $t$ тактов при управляющей последовательности $\alpha=\{\alpha_k\}$, $\alpha_k\in\{0,1\}$, $k=1,2,\dots$; $\{f_0^{g(\alpha,t)},\dots,f_{n-1}^{g(\alpha,t)}\}$ — система координатных функций преобразования $g(\alpha,t)$; $S(f_j^{g(\alpha,t)})$ — множество номеров существенных переменных координатной функции $f_j^{g(\alpha,t)}$, $j=0,\dots,n-1$.

В соответствии с определением [2], $i\in S(f_j^{g(\alpha,t)})$, если найдутся такие векторы $(\beta_0,\dots,\beta_{i-1},0,\beta_{i+1},\dots,\beta_{n-1}),(\beta_0,\dots,\beta_{i-1},1,\beta_{i+1},\dots,\beta_{n-1})\in V_n$, что

$$f_j^{g(\alpha,t)}(\beta_0,\dots,\beta_{i-1},0,\beta_{i+1},\dots,\beta_{n-1})\neq f_j^{g(\alpha,t)}(\beta_0,\dots,\beta_{i-1},1,\beta_{i+1},\dots,\beta_{n-1}).$$

Приведём алгоритм проверки условия $i\in S(f_j^{g(\alpha,t)})$. Для заданной управляющей последовательности $\alpha$ и всех возможных начальных состояний регистра (векторов $V_n$ в лексикографическом порядке) вычислим значение преобразования $g(\alpha,t)$, т. е. составим таблицы значений координатных функций $f_0^{g(\alpha,t)},\dots,f_{n-1}^{g(\alpha,t)}$. Далее для функции $f_j^{g(\alpha,t)}$ и переменной $x_i$, $i,j=0,\dots,n-1$:

1) вычислим величины $c=2^i$, $l=2^{n-i}$;
2) разделим столбец значений функции $f_j^{g(\alpha,t)}$ на $c$ равных отрезков длины $l$: $(f_1,\dots,f_c)$, $f_1,\dots,f_c\in V_l$;

3) каждый из полученных на предыдущем шаге отрезков разделим на две половины: $f_b = (f_b^{(1)}, f_b^{(2)}) \in V_{l/2} \times V_{l/2}$, тогда если $f_b^{(1)} = f_b^{(2)}$ для всех $b = 1, \ldots, c$, то $i \notin S(f_j^{g(\alpha,t)})$, иначе $i \in S(f_j^{g(\alpha,t)})$.

Для исследования перемешивающих свойств отображения НРС при различных значениях его параметров проведён вычислительный эксперимент. Реализована компьютерная программа, которая позволяет вычислить результат $t$ тактов при управляющей последовательности $\alpha = \{\alpha_k\}$, $k = 1, \ldots, t$, и проверить совершенность преобразования $g(\alpha, t)$, используя вышеописанный алгоритм. Минимальное число тактов работы НРС, после которых каждая координатная функция существенно зависит от всех переменных, обозначим $\gamma$. В таблице для $n = 6$ и 10 приведены управляющие последовательности, при которых получены минимальные значения $\gamma$, близкие к точным значениям экспонента множества $\hat{\Gamma}$. Запись $\alpha^m$ означает конкатенацию $m$ символов $\alpha$, $\alpha \in \{0, 1\}$.

| $n$ | $\varphi_0$ | $\varphi_1$ | Оценка (1) $\exp\hat{\Gamma}$ | Значение $\exp\hat{\Gamma}$ | $\gamma$ | $\alpha_1 \ldots \alpha_\gamma$ |
|---|---|---|---|---|---|---|
| 6 | $x_0 \oplus x_3$ | $x_0 \oplus x_2x_4$ | 17 | 11 | 18 | $0^6 1^6 0^3 1^3$ |
| 10 | $x_0 \oplus x_5$ | $x_0 \oplus x_2 \oplus x_4 \oplus x_6x_8$ | 31 | 17 | 30 | $0^{10} 1^{10} 0^5 1^5$ |
| | | $x_0 \oplus x_2x_4x_8$ | 31 | 19 | 30 | $0^{10} 1^{10} 0^5 1^5$ |
| | | $x_0 \oplus x_2x_4x_6$ | 33 | 19 | 34 | $0^{10} 1^{14} 0^5 1^5$ |

## Выводы

Функциям обратной связи $\varphi_0(x_0, \ldots, x_{n-1})$ и $\varphi_1(x_0, \ldots, x_{n-1})$, рассмотренным в ходе вычислительного эксперимента, соответствуют непримитивные перемешивающие орграфы $\Gamma(g_0)$, $\Gamma(g_1)$. Однако множество орграфов $\hat{\Gamma} = \{\Gamma(g_0), \Gamma(g_1)\}$ примитивное, согласно критерию примитивности множества орграфов с общим гамильтоновым контуром. Вычислительный эксперимент показал, что в этом случае композиция преобразований из множества $\{g_0, g_1\}$ может быть совершенной. Наименьшее число тактов, начиная с которого композиция преобразований совершенная, при псевдослучайной управляющей последовательности превосходит точное значение экспонента множества $\hat{\Gamma}$. Показано, что при определённых начальных знаках управляющей последовательности возможно получить полное перемешивание входных данных за число тактов, которое превосходит точное значение экспонента менее чем в 2 раза.

## ЛИТЕРАТУРА

1. *Shannon C. E.* Communication theory of secrecy systems // Bell System Technical J. 1949. V. 28. P. 656–715.
2. *Фомичев В. М., Мельников Д. А.* Криптографические методы защиты информации. В 2 ч. Ч. 1. Математические аспекты. М.: Юрайт, 2016. 209 с.
3. *Авезова Я. Э.* Свойства примитивных множеств ориентированных графов с общим множеством контуров // Прикладная дискретная математика. 2019. № 43, С. 101–114.

крипт
УДК 519.7 DOI 10.17223/2226308X/12/26

# О КРИПТОАНАЛИТИЧЕСКОЙ ОБРАТИМОСТИ С КОНЕЧНОЙ ЗАДЕРЖКОЙ КОНЕЧНЫХ АВТОМАТОВ

Г. П. Агибалов

Рассматривается свойство обратимости с конечной задержкой конечных автоматов с позиции криптоаналитика, а именно в зависимости от априорной информации, доступной алгоритму обращения. В криптоанализе, например симметричных конечно-автоматных шифров атакой с известным шифртекстом, типична ситуация, когда задачу обращения автомата приходится решать частично осведомлённому криптоаналитику. В зависимости от этой осведомлённости можно определить 208 различных типов обратимости и обратимых автоматов, изучить их свойства и установить соотношения между ними. Общеизвестные понятия сильной и слабой обратимости автоматов — это только два из этих типов. Целью настоящего доклада является обсуждение понятия криптоаналитической обратимости автоматов. Назван ряд математических задач (от характеризации автоматов, криптоаналитически обратимых разного типа, до создания на их основе криптосистем с открытым и закрытым ключом и их криптоанализа), которые представляют собой интересный предмет для дальнейших исследований и публикаций.

**Ключевые слова:** *конечные автоматы, автоматы без потери информации, обратимость автоматов, криптоаналитическая обратимость.*

Предлагаемые вниманию тезисы доклада являются расширенным рефератом работы автора [1], содержащей определение обратимости с конечной задержкой конечных автоматов с криптоаналитической точки зрения, по которой обращение автоматного преобразования осуществляется с целью восстановления входного слова автомата по его выходной последовательности при наличии некоторой частичной информации об этом преобразовании. Разные типы этой информации определяют разные типы и классы криптоаналитической обратимости автоматов и порождают многочисленные теоретико-автоматные и криптографические задачи, требующие математического решения. Обширный список этих задач включает в себя такие задачи, как, например, установление необходимых и достаточных условий автоматной обратимости каждого типа, построение конструктивных тестов принадлежности автоматов конкретным классам обратимости, алгоритмический синтез автоматов в заданных классах обратимости, характеризация обратимых автоматов, допускающих обратные автоматы, алгоритмический синтез обратных автоматов каждого типа, разработка эффективных алгоритмов восстановления входных последовательностей обратимых автоматов в конкретных классах обратимости, создание криптосистем с закрытым и открытым ключами на базе обратимых автоматов определённых классов обратимости, алгоритмический криптоанализ таких криптосистем с оценками его вычислительной сложности.

Произвольный конечный автомат представляется как $A = (X, Q, Y, \psi, \varphi)$, где $X$, $Q$ и $Y$ суть его входной алфавит, множество состояний и выходной алфавит соответственно; $\psi$ и $\varphi$ — его функции соответственно переходов и выходов, $\psi : X \times Q \to Q$ и $\varphi : X \times Q \to Y$. Последние, будучи определёнными для пар $xq \in X \times Q$, распространяются на пары $\alpha q \in X^* \times Q$ индукцией по длине $|\alpha|$ слова $\alpha \in X^*$, а именно определяются функции $\psi : X^* \times Q \to Q$ и $\bar{\varphi} : X^* \times Q \to Y^*$ как $\psi(\Lambda, q) = q$, $\psi(\alpha\beta, q) = \psi(\beta, \psi(\alpha, q))$,

$\bar{\varphi}(\Lambda, q) = \Lambda$, $\bar{\varphi}(x, q) = \varphi(x, q)$ и $\bar{\varphi}(\alpha\beta, q) = \bar{\varphi}(\alpha, q)\bar{\varphi}(\beta, \psi(\alpha, q))$. Символ $\Lambda$ здесь обозначает пустое слово в любом алфавите.

Таким образом, $\psi(\alpha, q)$ — это состояние, в которое автомат $A$ переходит из состояния $q$ под действием входного слова $\alpha$, а $\bar{\varphi}(\alpha, q)$ — это выходное слово, которое он при этом выдает.

Наконец, всюду далее под $\tau$ подразумевается произвольное целое неотрицательное число, называемое задержкой, и в отсутствие дополнительных оговорок в записи логических формул предполагается, что $a \in X$, $b \in X$, $\alpha \in X^*$, $\beta \in X^*$, $\delta \in X^\tau$, $\varepsilon \in X^\tau$, $q \in Q$, $s \in Q$.

Рассмотрим произвольный конечный автомат $A = (X, Q, Y, \psi, \varphi)$. Пусть $q, \alpha, \delta$ — переменные со значениями в $Q, X^*, X^\tau$, обозначающими соответственно начальное состояние, префикс (начало) и суффикс (окончание) входного слова $\alpha\delta$ автомата $A$, и $K = \{\forall q, \forall\alpha, \forall\delta, \exists q, \exists\delta\}$ — множество кванторов общности и существования по этим переменным. Заметим, что в $K$ нет квантора $\exists\alpha$. Это связано с тем, что для криптоаналитика префикс $\alpha$ входного слова автомата предполагается неизвестным и не некоторым, но любым. Пусть также $\theta = \psi(\alpha, q)$, $t = \psi(\alpha\delta, q)$ и $V = \{\Lambda, q, \theta, t, \delta, q\theta, qt, q\delta, \theta t, \theta\delta, t\delta, q\theta t, q\theta\delta, qt\delta, \theta t\delta, q\theta t\delta\}$. Символами $\theta$ и $t$ обозначены, как видно, промежуточное и заключительное состояния, в которые автомат $A$ переходит из состояния $q$ под действием входных слов $\alpha$ и $\alpha\delta$ соответственно. Элементы множества $V$ предназначены для задания того, что называется здесь порядком обратимости автомата $A$. Они являются по существу функциями от $q, \alpha, \delta$.

Мы говорим, что автомат $A$ *обратим с задержкой* $\tau$, если существуют кванторы $K_1, K_2, K_3$ в $K$ с разными переменными из $\{q, \alpha, \delta\}$, а также функция $f : Y^* \times V \to X^*$ и элемент $\upsilon(q, \alpha, \delta) \in V$, такие, что истинна формула

$$F = K_1K_2K_3(f(\bar{\varphi}(\alpha\delta, q), \upsilon(q, \alpha, \delta)) = \alpha);$$

в этом случае $(K_1K_2K_3, \upsilon)$ называется *типом обратимости* автомата $A$, $K_1K_2K_3$ — *степенью обратимости*, $\upsilon$ — *порядком обратимости*, $f$ — *функцией восстановления* (входного префикса), $\tau$ — *задержкой восстановления*, или *обратимости* и выражение $\exists f[F]$ — *условием обратимости* данного типа автомата $A$. Тип обратимости, в котором все кванторы являются кванторами общности, называется впредь *универсальным*.

В определении обратимого автомата степень обратимости $(K_1K_2K_3)$ своими кванторами $(\forall, \exists)$ указывает на степень полноты областей используемых (всех или некоторых) значений переменных $q, \alpha, \delta$, а их последовательностью — на зависимость значений одних (последующих) переменных от других (предшествующих). Порядок обратимости в нём содержит дополнительную информацию, известную криптоаналитику априорно. Это может быть и начальное состояние $q$ автомата, и его промежуточное состояние $\theta = \psi(\alpha, q)$, и заключительное состояние $t = \psi(\alpha\delta, q)$, и суффикс $\delta$ входного слова.

Степень обратимости $(K_1K_2K_3)$ может принимать тринадцать различных значений, а порядок обратимости $\upsilon$ — шестнадцать значений, поэтому количество всех типов обратимости $(K_1K_2K_3, \upsilon)$ с фиксированной задержкой автомата $A$ равно 208. Два из них, а именно (сильная) обратимость и слабая обратимость, хорошо известные и в теории автоматов и в криптографии [2, 3], в нашей теории универсальные и представлены наборами $(\forall q\forall\alpha\forall\delta, \varnothing)$ и $(\forall q\forall\alpha\forall\delta, \{q\})$, обозначающими произвольность (полноту областей) значений переменных $q, \alpha, \delta$, а также отсутствие у криптоаналитика дополнительной информации и известность ему начального состояния автомата

соответственно. Условия обратимости этих двух типов выглядят следующим образом: $\exists f \forall q \forall \alpha \forall \delta (f(\bar{\varphi}(\alpha\delta, q)) = \alpha)$ и $\exists f \forall q \forall \alpha \forall \delta (f(\bar{\varphi}(\alpha\delta, q), q) = \alpha)$.

Пример ещё одного типа обратимости автомата $A$ содержится в условии

$$\exists f \forall \alpha \exists \delta \forall q (f(\bar{\varphi}(\alpha\delta, q), q, \psi(\alpha\delta, q), \delta) = \alpha).$$

Это есть условие обратимости степени $\forall\alpha\exists\delta\forall q$ и порядка $\upsilon(q, \alpha, \delta) = (q, \psi(\alpha\delta, q), \delta)$. В нём утверждается возможность восстановления функцией $f$ префикса $\alpha$ входного слова $\alpha\delta$ автомата по его выходному слову $\bar{\varphi}(\alpha\delta, q)$ при известных начальном состоянии $q$, заключительном состоянии $t = \psi(\alpha\delta, q)$ и суффиксе $\delta$ входного слова в предположении, что в автомате для каждого префикса $\alpha$ входного слова суффикс $\delta$ этого слова не любой, но свой, и для этого входного слова $\alpha\delta$ начальное состояние $q$ может быть любым.

Каждому типу обратимости с фиксированной задержкой ставится в соответствие класс автоматов, обратимых этого типа. Показано, что граф отношения включения между этими классами представляет собой объединение двадцати девяти решёток, где каждая решётка по определению есть частично упорядоченное множество с точными верхней и нижней гранями для каждой пары его элементов. Доказано, что автомат $A$ обратим типа $(\forall q \forall \alpha \forall \delta, \upsilon(q, \alpha, \delta))$, если и только если

$$\forall q \forall \alpha \forall \delta \forall s \forall \beta \forall \varepsilon (\alpha \neq \beta \Rightarrow (\bar{\varphi}(\alpha\delta, q), \upsilon(q, \alpha, \delta)) \neq (\bar{\varphi}(\beta\varepsilon, s), \upsilon(s, \beta, \varepsilon)),$$

и что для любых символов кванторов $Q_i \in \{\forall, \exists\}$, $i \in \{1, 2, 3\}$, если автомат $A$ обратим типа $(Q_1 x_1 Q_2 x_2 Q_3 x_3, \upsilon(q, \alpha, \delta))$, то

$$Q_1 x_1 Q_2 x_2 Q_3 x_3 Q_1 y_1 Q_2 y_2 Q_3 y_3 (\alpha \neq \beta \Rightarrow (\bar{\varphi}(\alpha\delta, q), \upsilon(q, \alpha, \delta)) \neq (\bar{\varphi}(\beta\varepsilon, s), \upsilon(s, \beta, \varepsilon)),$$

где $x_1, x_2, x_3$ и $y_1, y_2, y_3$ — различные переменные из множеств $\{q, \alpha, \delta\}$ и $\{s, \beta, \varepsilon\}$ соответственно, такие, что если $x_i$ есть $q$, $\alpha$ или $\delta$, то $y_i$ есть $s$, $\beta$ или $\varepsilon$ соответственно, и если $x_i = \alpha$, то $Q_i = \forall$.

## ЛИТЕРАТУРА

1. *Agibalov G. P.* Cryptanalytic concept of finite automaton invertibility with finite delay // Прикладная дискретная математика. 2019. № 44. С. 34–42.
2. *Агибалов Г. П.* Конечные автоматы в криптографии // Прикладная дискретная математика. Приложение. 2009. № 2. С. 43–73.
3. *Tao R.* Finite Automata and Application to Cryptography. N.Y.: Springer, 2009. 406 p.

УДК 519.7 DOI 10.17223/2226308X/12/27

# О ВЕРОЯТНОСТЯХ РАЗНОСТНЫХ ТРАЕКТОРИЙ SPONGE-ФУНКЦИИ BASH-F

С. В. Агиевич, А. С. Маслов, Ю. С. Ярошеня

Предлагаются два метода оценки снизу весов разностных траекторий sponge-функции Bash-f. Оценки ограничивают сверху вероятности траекторий и могут использоваться при обосновании стойкости основанных на Bash-f криптографических алгоритмов к разностным атакам. Для полных 24-тактовых траекторий лучшая из оценок ограничивает вероятности величиной $2^{-386}$.

**Ключевые слова:** *sponge-функция, S-блок, разностный криптоанализ, разностная траектория.*

## 1. Sponge-функции и разностные траектории

Sponge-функция — это бесключевая подстановка, действующая на двоичные слова достаточно большой (по криптографическим меркам) размерности. Располагая sponge-функцией, можно построить целую линейку симметричных криптографических алгоритмов разнообразного назначения — от древовидного хэширования до аутентифицированного шифрования. Эти алгоритмы достаточно просты и имеют высокий потенциал быстродействия на распространённых аппаратных платформах.

Обычная sponge-функция $F$ преобразует слово $X \in \{0,1\}^n$ в слово $Y \in \{0,1\}^n$, выполняя $d$ тактов (итераций)

$$X_i = F_i(X_{i-1}), \quad i = 1, 2, \ldots, d,$$

с $X_0 = X$ и $Y = X_d$. Здесь $F_i$ — тактовые подстановки.

Слова $X_i$ интерпретируются как векторы над двоичным полем $\mathbb{F}_2$. Преобразования $F_i$ представляют собой композиции линейных и нелинейных преобразований этих векторов. Нелинейные преобразования, как правило, действуют локально на подвекторы $x \in \mathbb{F}_2^m$, где $m$ невелико. Действие задаётся подстановками $S\colon \mathbb{F}_2^m \to \mathbb{F}_2^m$, которые в криптографии принято называть *S-блоками*.

В разностном криптоанализе рассматривается обработка не одного, а сразу двух слов: $X$ и $X'$. Пусть $\Delta X = X \oplus X'$ — их сумма, $\Delta X_i$ — сумма слов, полученных в результате применения $i$ тактов к $X$ и $X'$, $i = 1, 2, \ldots, d$. Поскольку сложение по модулю два равносильно вычитанию, суммы $\Delta X_i$ являются также *разностями* (отсюда и название — «разностный криптоанализ»). Ненулевые биты разностей будем называть *активными*.

Последовательность разностей $\Delta X$, $\Delta X_1$, $\Delta X_2$, …, $\Delta X_r$ называется ($r$-тактовой разностной) *траекторией*. Траектории с нулевой входной разностью $\Delta X$ тривиальны (состоят из нулей), мы их далее не рассматриваем. Пусть траектория порождается случайными $X$ и $X'$ с фиксированной разностью $\Delta X$. Возможность достаточно точного прогнозирования $\Delta X_r$ при $r$, близких к $d$, является предпосылкой для разностных атак. При обосновании стойкости $F$ требуется оценить точность прогнозов и, в частности, получить оценки сверху для вероятностей траекторий.

Мы строили разностную траекторию, суммируя промежуточные результаты обработки входных слов. Можно поступить по-другому. Представим себе вероятностную машину $M$, которая работает исключительно с разностями, последовательно применяя к ним преобразования $F_1, \ldots, F_r$, точнее, их композиционные элементы. Линейные преобразования применяются к разностям (или их фрагментам) так же, как если бы речь шла о первоначальных словах. Остаётся рассмотреть действие S-блока $S$ на фрагмент разности $\Delta x$. Если $\Delta x = 0$, то разность $\Delta y$ на выходе $S$ также нулевая. Если же $\Delta x = \alpha \neq 0$, то $M$ выбирает $\Delta y$ случайным образом в соответствии с вероятностным распределением

$$\mathsf{P}\{\Delta y = \beta \mid \Delta x = \alpha\} = \frac{1}{2^m} \sum_{u \in \mathbb{F}_2^m} \mathbf{I}\{S(u \oplus \alpha) \oplus S(u) = \beta\},$$

индуцируемым $S$ (здесь $\mathbf{I}\{\mathcal{E}\}$ — индикатор наступления события $\mathcal{E}$).

Случайный выбор $\Delta y$ мотивируется случайным выбором входов $F$, которые порождают разностную траекторию. Следует понимать, что $M$ только моделирует разностные траектории. Но это моделирование достаточно точно, точность считается удовлетворительной в практических случаях.

Подача на вход $S$ ненулевой разности $\Delta x$ называется *активацией* S-блока. Активация является точкой ветвления — после неё выходная разность $\Delta y$ определяется неоднозначно. Если активация произошла во время обработки разности $\Delta X_{i-1}$, то речь идёт о нескольких вариантах следующей разности $\Delta X_i$. Во время обработки $\Delta X_i$ могут происходить новые активации, которые приводят к новым ветвлениям, и так далее. Другими словами, $M$ на фиксированном входе $\Delta X$ порождает несколько вариантов траекторий. Число вариантов, как правило, экспоненциально быстро растёт с увеличением длины траектории $r$.

Пусть во время генерации траектории $\Delta X, \Delta X_1, \ldots, \Delta X_r$ произошло $s_A$ активаций S-блоков и $p$ — произведение соответствующих вероятностей $\mathsf{P}\{\Delta y = \beta \mid \Delta x = \alpha\}$. Величина $p$ и есть интересующая нас вероятность траектории.

Далее вместо $p$ будет удобнее использовать характеристику $w_A = -\log_2 p$, которую называют *весом* траектории [1, 2]. Мы получим оценки снизу для веса траекторий sponge-функции Bash-f.

## 2. Sponge-функция Bash-f

Sponge-функция Bash-f введена в работе [3]. Функция преобразует двоичные слова длины $n = 1536$, называемые *состояниями*. Состояние разбивается на 24 подслова длины 64. Слова записываются в матрицу размера $3 \times 8$. Строки и столбцы матрицы называются *плоскостями*: горизонтальными и вертикальными.

Функция Bash-f построена как многократная композиция преобразований усложнения и перемешивания. За усложнение отвечает преобразование $S3$, которое применяется к тройке 64-разрядных слов. Тройки соответствующих друг другу битов этих слов (*вертикальные линии*) одновременно подвергаются действию фиксированного трёхбитового S-блока. Одновременность достигается формульным заданием $S3$ с помощью логических операций AND, OR, NOT и сложения XOR.

За перемешивание в Bash-f отвечают преобразования $L3$ и $P$. Первое преобразование также применяется к тройке 64-разрядных слов. Слова суммируются по правилу XOR, циклически сдвигаются, снова суммируются и т. д. Всего выполняется шесть сложений и четыре сдвига. Преобразование $P$ переставляет местами 24 обрабатываемых слова.

Выполняется $d = 24$ такта. На каждом такте сначала к вертикальным плоскостям применяется $L3$, затем $S3$, затем плоскости перемешиваются с помощью $P$. Дополнительно, для разрушения однородностей, к 24-му слову добавляется тактовая константа.

S-блок $S\colon \mathbb{F}_2^3 \to \mathbb{F}_2^3$ выбран так, что для любого ненулевого $\alpha \in \mathbb{F}_2^3$ существует в точности четыре ненулевых $\beta \in \mathbb{F}_2^3$, для которых

$$\mathsf{P}\{\Delta y = \beta \mid \Delta x = \alpha\} = \frac{1}{4}.$$

Таким образом, вес $w_A$ и число активных S-блоков $s_A$ связаны соотношением $w_A = 2s_A$.

Пусть $s_A(r)$ — минимальное число активных S-блоков на нетривиальных траекториях Bash-f длины $r$ и $w_A(r) = 2s_A(r)$ — минимальный вес траекторий.

## 3. Результаты

Мы получили оценки снизу для величины $w_A(24)$ двумя различными методами. Первый метод почти полностью автоматизирован, он реализуется компьютерной программой и, как всякий автоматизированный метод, имеет перспективы быстрого улучшения и точной верификации результатов. Второй метод почти полностью ручной, он

реализуется прямыми расчётами на основе известных свойств $L3$ и $P$ и, как всякий ручной метод, опережает автоматизированный, если не требует вычислений большого объема. Методы появились в ходе разработки Bash-f, в настоящей работе они усиливаются.

В [1, 2] получены аналогичные оценки для величины $w_A(24)$, только применительно к sponge-функции Keccak-f (точнее, Keccak-f[1600]). Эта функция является ядром известного семейства алгоритмов хэширования SHA-3. В Keccak-f также выполняется $d = 24$ такта, длина состояния несколько больше: $n = 1600$.

Оценки представлены в таблице. Как видим, на сегодняшний день оценки для Bash-f лучше оценок для Keccak-f.

**Оценки снизу для** $w_A(24)$

| Год, источник | Bash-f | | Keccak-f |
|---|---|---|---|
| | метод 1 | метод 2 | |
| 2012 [1] | | | 296 |
| 2015 (разработка Bash-f) | 300 | 324 | |
| 2017 [2] | | | 368 |
| 2019 (настоящая работа) | 386 | 372 | |

Опишем суть наших методов. Будем работать с характеристиками $s_A(r)$.

**Метод 1**. Оценивание $s_A(r)$ предполагает перебор разностных траекторий длины $r$. Прямой перебор затруднён уже при $r = 3$. Для сокращения перебора использовано сжатое описание траектории, фиксирующее только частичную информацию об их разностях. Такую частичную информацию мы назвали *проекцией*.

Использовались следующие проекции:

1) `avl` — число активных S-блоков (вертикальных линий);
2) `avp` — число активных (т. е. хотя бы с одним активным битом) вертикальных плоскостей;
3) `avls` — число активных S-блоков для каждой из вертикальных плоскостей (упорядоченный набор из восьми чисел).

Пусть $[\mathtt{p}](i)$ — проекция `p` разности $i$-го такта; $[\mathtt{p}_1, \ldots, \mathtt{p}_k](i, \ldots, j)$ — набор проекций $([\mathtt{p}_u](v))$, $1 \leqslant u \leqslant k$, $i \leqslant v \leqslant j$.

Некоторые проекции однозначно определяют другие. Например, сумма чисел в $[\mathtt{avls}](i)$ совпадает с $[\mathtt{avl}](i)$, количество ненулевых чисел в $[\mathtt{avls}](i)$ — с $[\mathtt{avp}](i)$. В этом смысле `avls` можно считать расширением проекций `avl` и `avp`. Очевидно, что сумма

$$[\mathtt{avl}](1) + \ldots + [\mathtt{avl}](r) \qquad (\star)$$

представляет собой число активных S-блоков подразумеваемой $r$-траектории, а минимум суммы $(\star)$ по всем допустимым наборам проекций и есть искомое значение $s_A(r)$.

Оценивание $s_A(r)$ выполняется в три этапа по схеме метода ветвей и границ. На первом (подготовительном) этапе рассчитываются характеристики линейного преобразования $L3$, которые позволяют отсеивать недопустимые наборы проекций на третьем этапе. На втором этапе перебираются проекции $[\mathtt{avl}, \mathtt{avp}](1, \ldots, r)$ и вычисляется минимум суммы $(\star)$. При этом наборы проекций, на которых он достигается, сохраняются. На третьем этапе перебираются расширенные проекции $[\mathtt{avls}](1, \ldots, r)$, соответствующие проекциям, сохранённым на втором этапе. Если для некоторых $i$ и $j$ не существует

допустимого набора $[\mathtt{avls}](i,\ldots,j)$, соответствующего $[\mathtt{avl},\mathtt{avp}](i,\ldots,j)$ из сохранённого набора, то набор $[\mathtt{avl},\mathtt{avp}](i,\ldots,j)$ помечается как недопустимый и вычисления возвращаются ко второму этапу для уточнения минимума.

**Метод 2**. Во втором методе оценивается снизу число активных S-блоков на четырёх тактах. Использованы свойства преобразований $L3$, $S3$, $P$, заложенные при проектировании Bash-f [3]. Особую важность имеет следующий факт: если на выходе $L3$ получена вертикальная плоскость с малым числом активных линий, то на вход была подана плоскость с большим числом активных линий. Базовые свойства преобразований выступают в роли аксиом, из которых аналитически выводятся теоремы — новые свойства, имеющие отношение к оцениванию.

Затем просматриваются допустимые конфигурации, представляющие собой пары «число активных вертикальных линий на входах $L3$ на втором такте, проекция $[\mathtt{avp}](2)$». Для каждой конфигурации оценивается снизу проекция $[\mathtt{avl}](1)$ (как будто бы от второго такта мы возвращаемся к первому) и проекции $[\mathtt{avl}](3,4)$. В итоге получена оценка

$$s_A(4) = \min\left([\mathtt{avl}](1) + [\mathtt{avl}](2) + [\mathtt{avl}](3) + [\mathtt{avl}](4)\right) \geqslant 31,$$

откуда $s_A(24) \geqslant 6s_A(4) \geqslant 186$.

## ЛИТЕРАТУРА

1. *Daemen J. and Van Assche G.* Differential propagation analysis of Keccak // FSE'2012. LNCS. 2012. V. 7549. P. 422–441.
2. *Mella S., Daemen J., and Van Assche G.* New techniques for trail bounds and application to differential trails in Keccak // IACR Trans. Symmetric Cryptology. 2017. No. 1. P. 329–357.
3. *Agievich S., Marchuk V., Maslau A., and Semenov V.* Bash-f: another LRX sponge function // Математические вопросы криптографии. 2017. Т. 8. № 2. С. 7–28.

УДК 519.7 DOI 10.17223/2226308X/12/28

# КРИПТОАНАЛИЗ ШИФРСИСТЕМЫ ACBF[1]

И. В. Боровкова, И. А. Панкратова

Рассматривается асимметричная шифрсистема на булевых функциях с функциональным ключом. Предлагаются атаки с известным открытым текстом для двух подмножеств ключевых параметров.

**Ключевые слова:** *криптосистема ACBF, векторные булевы функции, асимметричная криптосистема, криптоанализ.*

Рассматривается шифрсистема ACBF (Asymmetric Cryptosystem on Boolean Functions) [1]. Она строится на основе двух операций — перестановки и отрицания, — применяемых к переменным и координатам обратимой векторной булевой функции. Открытый ключ $f(x)$ получается по формуле $f(x) = \pi_2(g^{\sigma_2}(\pi_1(x^{\sigma_1})))$, где $g\colon \mathbb{F}_2^n \to \mathbb{F}_2^n$ — биективная векторная булева функция; функции $g$ и $g^{-1}$ известны; $\sigma_1, \sigma_2 \in \mathbb{F}_2^n$ — операции отрицания; $\pi_1, \pi_2 \in \mathbb{S}_n$ — операции перестановки. Закрытый ключ — функция $f^{-1}$.

Ключевыми параметрами криптосистемы являются элементы любого непустого подмножества $J \subseteq \{\pi_1, \pi_2, \sigma_1, \sigma_2\}$; операции из $\{\pi_1, \pi_2, \sigma_1, \sigma_2\}\setminus J$ считаются тождественными. Таким образом, существует 15 различных подмножеств ключевых параметров.

[1]Работа поддержана грантом РФФИ, проект № 17-01-00354.

Целью работы является нахождение ключевых параметров по известным парам открытых текстов и соответствующих шифртекстов. Рассмотрены два базовых случая: $J = \{\pi_1\}$ и $J = \{\pi_1, \pi_2\}$. Для каждого из них разработана атака.

### 1. Случай $J = \{\pi_1\}$

Пусть $x, y \in \mathbb{F}_2^n$ — пара «открытый текст — соответствующий шифртекст». По определению криптосистемы ACBF получаем

$$y = f(x) = g(\pi_1(x)); \quad \pi_1(x) = g^{-1}(y).$$

**Утверждение 1.** Пусть $P$ — матрица размера $m \times n$ со строками открытых текстов $P_1, \ldots, P_m$ в $\mathbb{F}_2^n$, с множеством $Q$ векторов-столбцов в $\mathbb{F}_2^m$, разбитым на классы $Q_1, \ldots, Q_k$ одинаковых, $1 \leqslant k \leqslant n$, так, что $|Q_j| = r_j$, $j = 1, \ldots, k$, $r_1 + \ldots + r_k = n$. Пусть также $C_i = g(\pi_1(P_i))$ для некоторой перестановки $\pi_1 \in \mathbb{S}_n$, $i = 1, \ldots, m$. Тогда количество различных перестановок $\pi \in \mathbb{S}_n$, для которых $C_i = g(\pi(P_i))$, $i = 1, \ldots, m$, равно

$$I = \prod_{i=1}^{k} r_i!$$

Таким образом, перестановка $\pi_1$ определяется однозначно, если и только если все столбцы в матрице $P$ различны. Экспериментально установлено, что для этого в среднем понадобится $2 \log_2 n$ открытых текстов при их случайном равновероятном выборе.

**Следствие 1.** Если производится атака с выбираемым открытым текстом, то можно подобрать такие $P_i$, что при рассмотрении $m = \lceil \log_2 n \rceil$ пар $(P_i, C_i)$ искомая перестановка $\pi_1$ найдётся однозначно.

Пусть имеется $m$ пар $(P_i, C_i)$. Рассмотрим матрицу $P'$ со строками $g^{-1}(C_i) = \pi_1(P_i)$, $i = 1, \ldots, m$; заметим, что $P'$ содержит те же вектор-столбцы, что и матрица $P$, только в другом порядке — определяемом перестановкой $\pi_1$. Алгоритм 1 находит все возможные ключи шифрсистемы ACBF.

---

**Алгоритм 1.** Нахождение всех возможных ключей в случае $J = \{\pi_1\}$

---

**Вход:** $(P_i, C_i)$, $i = 1, \ldots, m$.
**Выход:** все $\pi_1 \in \mathbb{S}_n$, такие, что $C_i = g(\pi_1(P_i))$, $i = 1, \ldots, m$.

1: Построим матрицы $P = \begin{pmatrix} P_1 \\ P_2 \\ \vdots \\ P_m \end{pmatrix}$, $P' = \begin{pmatrix} g^{-1}(C_1) \\ g^{-1}(C_2) \\ \vdots \\ g^{-1}(C_m) \end{pmatrix}$.

2: Для каждого столбца $s$ матрицы $P$ запоминаем номера столбцов $k_{i_1}, \ldots, k_{i_l}$, равных $s$. Для матрицы $P'$ делаем то же самое.

3: Строим конструкцию следущего вида:

$$\begin{pmatrix} k_{i_1} & \ldots & k_{i_l} \\ k_{t_1} & \ldots & k_{t_l} \end{pmatrix} \qquad \begin{pmatrix} \ldots \\ \ldots \end{pmatrix} \qquad \begin{pmatrix} k_{j_1} & \ldots & k_{j_q} \\ k_{r_1} & \ldots & k_{r_q} \end{pmatrix}.$$

Здесь каждая скобка соответствует одному значению столбца $s$; в верхней строке находятся позиции, на которых столбец $s$ встречается в $P$; в нижней — в $P'$.

4: Переставляя элементы нижней строки в каждой скобке всеми способами, получим всевозможные искомые перестановки $\pi_1$.

---

### 2. Случай $J = \{\pi_1, \pi_2\}$

По определению получаем

$$y = f(x) = \pi_2(g(\pi_1(x))).$$

**Утверждение 2.** Пусть имеется $m$ пар открытых текстов и шифртекстов вида $(P_i, C_i)$, $i = 1, \ldots, m$. Составим матрицы $P$ и $C$ из открытых текстов $P_i$ и шифртекстов $C_i$ соответственно:

$$P = \begin{pmatrix} P_1 \\ P_2 \\ \vdots \\ P_m \end{pmatrix}, \quad C = \begin{pmatrix} C_1 \\ C_2 \\ \vdots \\ C_m \end{pmatrix}.$$

Необходимым условием единственности решения системы уравнений

$$C_i = \pi_2(g(\pi_1(P_i))), \quad i = 1, \ldots, m, \tag{1}$$

является отсутствие одинаковых столбцов в каждой из матриц $P$ и $C$.

Поиск всех решений системы (1) представлен в алгоритме 2.

---

**Алгоритм 2.** Нахождение всех возможных пар перестановок $(\pi_1, \pi_2)$

---

**Вход:** $(P_i, C_i)$, $i = 1, \ldots, m$.
**Выход:** все пары $(\pi_1, \pi_2)$, такие, что $C_i = \pi_2(g(\pi_1(P_i))), i = 1, \ldots, m$.

1: Строим матрицу $P'$ из $C_i$.
2: Среди $P_i$, $i = 1, \ldots, m$, выбираем такой открытый текст $P_j$, который уравновешен или больше всего приближен к уравновешенности по сравнению с другими открытыми текстами. Пусть $C_j$ — соответствующий шифртекст.
3: Ищем все $x$, такие, что $\mathrm{w}(x) = \mathrm{w}(P_j)$ и $\mathrm{w}(g(x)) = \mathrm{w}(C_j)$, где $\mathrm{w}(x)$ — вес вектора $x$.
4: **Для каждого** такого $x$ по алгоритму 1 с исходными данными $(P_j, x)$, $m = 1$ находим все перестановки $\pi_1$ со свойством $g^{-1}(x) = \pi_1(P_j)$.
5: **Для всех** найденных перестановок $\pi_1$:
6: строим матрицу

$$P = \begin{pmatrix} g(\pi_1(P_1)) \\ g(\pi_1(P_2)) \\ \vdots \\ g(\pi_1(P_m)) \end{pmatrix}.$$

7: **Если** каждый столбец матрицы $P$ встречается в ней столько же раз, сколько и в $P'$, **то**, выполняя шаги 2–4 алгоритма 1, находим все перестановки $\pi_2$ и пары $(\pi_1, \pi_2)$ записываем в ответ.

---

Алгоритмы 1 и 2 реализованы программно, проведена серия экспериментов при значениях $n$ от 3 до 29, количестве входных текстов, достаточных для однозначного определения ключа, и табличном задании функции $g$. Алгоритм 1 при всех $n$ находит перестановку $\pi_1$ за доли секунды; алгоритм 2 работает гораздо дольше и время его работы зависит не только от $n$, но и от количества таких $x$, что $\mathrm{w}(x) = \mathrm{w}(P_j)$ и $\mathrm{w}(g(x)) = \mathrm{w}(C_j)$. Это количество растёт экспоненциально с ростом $n$ и, например, для $n = 15$ в среднем равно 664.

ЛИТЕРАТУРА

1. *Agibalov G. P. and Pankratova I. A.* Asymmetric cryptosystems on Boolean functions // Прикладная дискретная математика. 2018. № 40. С. 23–33.

УДК 519.151, 519.725, 519.165 DOI 10.17223/2226308X/12/29

# БЛОКИРОВКА ЛИНЕЙНЫХ МНОГООБРАЗИЙ И ТРОЙКИ ШТЕЙНЕРА

М. В. Ведунова, А. О. Игнатова, К. Л. Геут

Рассматриваются задачи блокировки троек Штейнера, применимые в схемах разделения секрета. Описан метод построения блокирующего множества минимальной и максимальной мощности. Для дополнительного множества найден метод оценки минимальной мощности дополнения как в линейных, так и в нелинейных системах троек Штейнера. Для соответствующих матроидов реализованы идеальные схемы разделения секрета на основе интерполяционных многочленов с нулевым следом. В нелинейной системе троек Штейнера с 13 элементами найдены максимальные и минимальные мощности дополнения блокирующего множества.

**Ключевые слова:** *системы троек Штейнера, схемы разделения секрета, блокирующие множества.*

Во втором раунде международной интернет-олимпиады по криптографии NSUCRYPTO-2015 [1] была предложена задача на специальный приз программного комитета «A secret sharing», в 2016 и 2017 гг. отмеченная как всё ещё не решённая [2, 3]. Решение этой задачи рассматривается с точки зрения блокировки двумерных аффинных многообразий над полем GF(2). Здесь под задачей блокировки семейства $S$ подмножеств $T$ множества $E$ понимается задача построения такого минимального по включению подмножества $M$, что любое подмножество $T$ из семейства $S$ имеет непустое пересечение с $M$. Каждое такое подмножество $M$ называется блокирующим множеством семейства $S$, а подмножество $L = E \setminus M$ — дополнением блокирующего множества. Задача блокировки троек Штейнера может трактоваться как вспомогательная при решении исходной задачи NSUCRYPTO, поскольку каждое такое многообразие является сдвигом однозначно определённого двумерного линейного многообразия, соответствующего линейной тройке Штейнера [4]. Проблеме вложимости произвольной системы троек Штейнера в совершенный двоичный код посвящена работа [5]. Проблеме реализации связи блок-схем с семейством троек Штейнера, где однородный матроид, когиперплоскости которого — это тройки Штейнера, соответствует идеальной схеме разделения секрета, посвящена работа [6]. Линейные системы троек Штейнера $S_n$ — системы с $v = 2^n - 1$ элементами — ненулевыми битовыми строками длины $n$, $n \geqslant 3$, в которых бинарная операция квазигруппы Штейнера есть побитовое сложение по модулю два. Для матроидов линейных троек Штейнера ниже построены соответствующие им схемы разделения секрета [7, 8], а также рассмотрены методы построения блокирующих множеств минимальной и максимальной мощности.

**Утверждение 1.** Мощность $l$ дополнения $L$ блокирующего множества удовлетворяет неравенству $l(l+1)/2 \geqslant v$.

Используя данное неравенство, получим, что для нелинейной тройки Штейнера при $v = 13$ минимальная мощность дополнения $l = 5$, а для $v = 31$ не может быть меньше восьми.

Линейные системы троек Штейнера можно трактовать как систему предписанных соотношений в конечных бинарных полях. В зависимости от их интерпретации задачу блокировки можно рассматривать в связи с реализацией схем разделения секрета (СРС) в конечных полях. Так, проблема «A secret sharing» как проблема блокировки аффинных многообразий приводит к задаче реализации СРС, сохраняющих предписанные соотношения в виде семейства $H_4$ четвёрок в $\mathrm{GF}(2^n)$, таких, что $X_1+X_2+X_3+X_4=0$, а проблема блокировки линейных троек Штейнера приводит к задаче реализации СРС, сохраняющих предписанные соотношения в виде семейства $H_3$ троек в $\mathrm{GF}(2^n)$, таких, что $X_1+X_2+X_3=0$. Эти зависимости можно трактовать как циклы [9] в некоторых матроидах.

**Утверждение 2.** Семейство $H_4$ с добавлением пятиэлементных подмножеств, никакие четыре элемента которых не дают в сумме нуль, удовлетворяет аксиомам циклов матроида.

**Утверждение 3.** Семейство $H_3$ с добавлением четырёхэлементных подмножеств, никакие три элемента которых не дают в сумме нуль, удовлетворяет аксиомам циклов матроида.

Оказывается, эти матроиды являются матроидами идеальных СРС, реализация которых аналогична реализации схемы Шамира и основывается на интерполяционных многочленах с нулевым следом.

**Утверждение 4.** Классом многочленов, разделяющих секрет посредством циклов семейства $H_4$ построенного матроида, является класс многочленов вида $f(x)=ax^4+bx^2+cx+d$, где $a$, $b$, $c$, $d$ — произвольные элементы поля $\mathrm{GF}(2^n)$.

**Утверждение 5.** Классом многочленов, разделяющих секрет посредством циклов семейства $H_3$ построенного матроида, является класс многочленов вида $f(x)=ax^3+bx+c$, где $a$, $b$, $c$ — произвольные элементы поля $\mathrm{GF}(2^n)$.

Для нелинейных троек Штейнера мощность блокирующего множества может быть получена только полным перебором, например:

**Утверждение 6.** Для $v=13$ максимальные и минимальные мощности дополнительного множества равны $|L|_{\min}=5$, $|L|_{\max}=6$.

Система троек, построенная на тринадцати элементах, не относится к линейным. Рекуррентная конструкция блокирующего множества $M$ и его дополнения $L$ такова:

**Утверждение 7.** Для любого дополнительного множества $L$ существует $L_k$ в $S_k$ (при $k>n$, $k$ — мощность множества битовых строк, в которых первые $n$ битов равны нулю), имеющее мощность $|L_k|=|L|\cdot 2^{k-n}$.

Максимальность такого $L$ вытекает из условия, что для любого элемента из тройки $u\in M$ существуют $x_1,x_2\in L$, что $u=x_1\oplus x_2$ и $L$ не включает в себя ни одной тройки с нулевой суммой.

Конструкция минимального блокирующего множества $M$ и его дополнения $L$ такова: $G=M\cup\{0\}$ есть подгруппа группы $(\mathbb{F}_2^n;\oplus)$ индекса два (линейное пространство), а $L=G\oplus h$ $(h\notin G)$ — её смежный класс (аффинное пространство). Эта конструкция, очевидно, даёт решение задачи блокировки в общем случае линейной тройки Штейнера при $n\geqslant 3$, при этом $|L|=2^{n-1}$, $|M|=2^{n-1}-1$.

Итак, предложены конструкции блокирующих множеств троек Штейнера и оценки возможных значений их мощности.

ЛИТЕРАТУРА

1. Сайт олимпиады NSUCRYPTO. http://nsucrypto.nsu.ru/
2. *Tokareva N., Gorodilova A., Agievich S., et al.* Mathematical methods in solutions of the problems from the Third International Students' Olympiad in Cryptography // Прикладная дискретная математика. 2018. № 40. С. 34–58.
3. *Геут К. Л., Кириенко К. А., Садков П. О. и др.* О явных конструкциях для решения задачи «A secret sharing» // Прикладная дискретная математика. Приложение. 2017. № 10. С. 68–70.
4. *Холл М.* Комбинаторика: пер. с англ. М.: Мир, 1970. 424 с.
5. *Ковалевская Д. И., Соловьева Ф. И., Филимонова Е. С.* О системах троек Штейнера малого ранга, вложимых в совершенные двоичные коды // Дискретный анализ и исследование операций. 2013. Т. 20. № 3(111). С. 3–25.
6. *Медведев Н. В., Титов С. С.* Об однородных матроидах и блок-схемах // Прикладная дискретная математика. Приложение. 2017. № 10. С. 21–23.
7. *Shamir A.* How to share a secret // Commun. ACM. 1979. No. 22. P. 612–613.
8. *Парватов Н. Г.* Совершенные схемы разделения секрета // Прикладная дискретная математика. 2008. № 2(2). С. 50–57.
9. *Асанов М. О., Баранский В. А., Расин В. В.* Дискретная математика: графы, матроиды, алгоритмы. Ижевск: НИЦ Регулярная и хаотическая динамика, 2001. 288 с.

УДК 519.7 DOI 10.17223/2226308X/12/30

# ОБ АРГУМЕНТАЦИИ ОТСУТСТВИЯ СВОЙСТВ СЛУЧАЙНОГО ОРАКУЛА У НЕКОТОРЫХ КРИПТОГРАФИЧЕСКИХ ХЕШ-ФУНКЦИЙ[1]

И. А. Грибанова, А. А. Семёнов

Представлены новые алгебраические атаки на хеш-функции вида MD4-$k$, где $k$ — число шагов базового алгоритма MD4, $39 \leqslant k \leqslant 48$. Для решения алгебраических уравнений используются SAT-решатели. Представленные атаки демонстрируют отсутствие свойств случайного оракула у рассматриваемых хеш-функций. Более точно, мы строим оценки доли легко обратимых выходов этих функций и показываем, что даже для полнораундовой функции MD4 эта доля весьма высока. Для построения оценок с каждой функцией вида MD4-$k$ связывается специальная функция, длина входа которой существенно меньше 512. Показано, что любое значение такой функции является значением MD4-$k$. Задача обращения специальной функции, как правило, существенно проще, чем задача обращения MD4-$k$. Оценка доли векторов в $\{0,1\}^{128}$, являющихся значениями специальной функции, даёт оценку доли легко обратимых значений исходной функции MD4-$k$.

**Ключевые слова:** *криптографические хеш-функции, поиск прообразов хеш-функций, MD4, MD4-39, SAT.*

Случайный оракул — это гипотетический объект, обладающий рядом привлекательных с точки зрения криптографии свойств. Строго (см., например, [1]) случайный оракул определяется как отображение вида $O : \{0,1\}^* \to \{0,1\}^\infty$, которое произвольному конечному двоичному слову сопоставляет слово, являющееся бесконечной

[1]Работа выполнена при финансовой поддержке Российского научного фонда, проект № 16-11-10046. Грибанова И. А. поддержана стипендией Президента РФ СП-3545.2019.5.

последовательностью испытаний Бернулли с $p = 1/2$. Однако такое определение полностью неконструктивно. Для практических приложений необходимы функции вида $\{0,1\}^* \to \{0,1\}^*$ или даже $\{0,1\}^n \to \{0,1\}^m$, которые обладают (гипотетически) свойствами случайного оракула, но могут быть заданы посредством некоторых алгоритмов. Более точно, требуется, чтобы алгоритм, задающий функцию, был детерминированным (то есть выдавал одинаковые выходы для одинаковых входов). Почти все выходы (длины $m$) функции, выполняющей роль случайного оракула, должны выглядеть как последовательности Бернулли с $p = 1/2$. Соответственно для случайно сгенерированного входа такой функции сложность задачи обращения соответствующего выхода должна быть сопоставима со сложностью повторения фиксированной последовательности Бернулли в результате $m$-кратного подбрасывания идеальной монеты.

Существование случайных оракулов вида $O : \{0,1\}^n \to \{0,1\}^m$ было бы чрезвычайно полезно для многих криптографических приложений. Скажем, некто может сгенерировать свой секретный идентификатор $\alpha \in \{0,1\}^n$, а затем многократно доказывать свою аутентичность, используя $\alpha$ и несекретный алгоритм $O$. В [1] отмечено, что на роль реальных прототипов случайного оракула подходят стойкие криптографические хеш-функции. Эта идея получила серьезное развитие в [2, 3], после появления которых возникло целое направление, известное как «доказательства в модели случайного оракула». В настоящей работе показано, что некоторые известные криптографические хеш-функции не обладают свойствами случайного оракула. Более точно, будем рассматривать задачу обращения криптографической хеш-функции $h : \{0,1\}^* \to \{0,1\}^C$. Такие функции обычно разбивают хешируемое сообщение на блоки фиксированной длины $n$, соответственно рассматриваются задачи обращения функций вида $f : \{0,1\}^n \to \{0,1\}^C$ (для функций из семейств MD и SHA $n = 512$).

Основная цель работы — показать для некоторых криптографических хеш-функций, что легко обратимые выходы этих функций составляют значительную долю в $\{0,1\}^C$. Интуитивно, любая такая функция $h$ не может быть случайным оракулом, поскольку выбор случайного входа $\alpha$ с высокими шансами даст выход $\gamma$, обращение которого потребует меньше вычислительных ресурсов, чем простой подбор такого $\alpha' \in \{0,1\}^n$, что $h(\alpha') = \gamma$. Будем исследовать хеш-функции вида MD4-$k$, где $k$ — число базовых шагов алгоритма MD4 [4].

В основе описываемых далее атак лежат результаты [5, 6]. Основная идея этих атак заключается в использовании «ослабляющих ограничений». Впервые использовать подобные ограничения предложил Г. Доббертин в [7]. Новизна подхода из [5, 6] заключается в том, что ослабляющие ограничения строятся в автоматическом режиме в процессе решения задачи оптимизации специальной псевдобулевой функции [9], оценивающей некоторую эвристическую меру эффективности соответствующих ограничений. Ослабляющие ограничения — это нулевые значения некоторых переменных сцепления (chaining variables). Изначально Г. Доббертин предложил приравнять произвольной константе значения 12 переменных сцепления, используемых в первых двух раундах алгоритма MD4. Для решения получающейся системы булевых уравнений Г. Доббертин предложил алгоритм, позволяющий обращать на персональном компьютере функцию MD4-32. В [8] описан, по сути, вариант атаки Доббертина (т. е. ослабляющие ограничения накладываются на те же переменные сцепления), в котором для решения уравнений используется SAT-решатель, а для построения ослабляющих ограничений — константа 0. При помощи метода, предложенного в [5, 6], удалось построить различные виды ослабляющих ограничений, среди которых оказались такие, которые дали существенно более эффективную атаку на MD4-39, чем в работе [8]. Один из набо-

ров ослабляющих ограничений из [5, 6] позволил обращать менее чем за 1 мин работы SAT-решателя MINISAT2.2 примерно 65 % случайных векторов из $\{0,1\}^{128}$, рассматривая их как значения функции MD4-39.

Анализируя различные ослабляющие ограничения, построенные в [5, 6], можно заметить, что с исходной обращаемой функцией вида $f_{\text{MD4-}k} : \{0,1\}^{512} \to \{0,1\}^{128}$ естественным образом связываются специальные функции вида $g^{\lambda}_{\text{MD4-}k} : \{0,1\}^{d} \to \{0,1\}^{128}$, обладающие целым рядом интересных свойств (через $\lambda$ здесь обозначен булев вектор, задающий некоторый набор ослабляющих ограничений). Во-первых, любое значение функции $g^{\lambda}_{\text{MD4-}k}$ является значением функции $f_{\text{MD4-}k}$. Во-вторых, что очень важно, $d$ может оказаться существенно меньше, чем 512. Так, один из векторов ослабляющих ограничений для задачи обращения $f_{\text{MD4-39}}$, обозначаемый $\lambda_1$, даёт функцию $g^{\lambda_1}_{\text{MD4-39}} : \{0,1\}^{128} \to \{0,1\}^{128}$. Наконец, если $\gamma$ — значение функции вида $g_{\text{MD4-}k}$ и $\alpha' \in \{0,1\}^{d}$ — его прообраз, то от $\alpha'$ можно эффективно перейти к такому $\alpha \in \{0,1\}^{512}$, что $f_{\text{MD4-}k}(\alpha) = \gamma$.

Функции вида $g^{\lambda}_{\text{MD4-}k}$ могут быть определены не всюду на $\{0,1\}^{d}$ и далеко не каждый $\gamma \in \{0,1\}^{128}$ является образом функции $g^{\lambda}_{\text{MD4-}k}$. Однако задача обращения функции $g_{\text{MD4-}k}$ может оказаться существенно проще, чем задача обращения $f_{\text{MD4-}k}$. Так, на обращение каждого значения функции $g^{\lambda_1}_{\text{MD4-39}}$ тратится менее минуты работы обычного последовательного SAT-решателя MINISAT2.2. При этом примерно 65 % векторов из $\{0,1\}^{128}$ имеют $g^{\lambda_1}_{\text{MD4-39}}$-прообразы. Сказанное означает, что примерно 65 % выходов функции MD4-39 являются легко обратимыми, поскольку такова доля выходов MD4-39, совпадающих с выходами функции $g^{\lambda_1}_{\text{MD4-39}}$. Это означает, что MD4-39 не удовлетворяет свойствам случайного оракула, поскольку, выбрав случайный вход $\alpha \in \{0,1\}^{512}$, с вероятностью $\approx 65\,\%$ получим $\gamma = f_{\text{MD4-39}}(\alpha)$, который имеет $g^{\lambda_1}_{\text{MD4-39}}$-прообраз. Найдя этот прообраз, мы эффективно построим по нему такой $\tilde{\alpha} \in \{0,1\}^{512}$, что $f_{\text{MD4-39}}(\tilde{\alpha}) = \gamma$.

В таблице представлены ослабляющие ограничения, задающие функции вида $g^{\lambda}_{\text{MD4-}k}$, для которых задачи обращения решаются в среднем за время $< t$ при помощи однопоточного SAT-решателя.

| Ослабляющие ограничения | | $d$ | $k$ | $t$, с |
|---|---|---|---|---|
| $\lambda_1$ | 00000000000001101110111011101000000000000000000000 | 128 | 39 | 12 |
| $\lambda_2$ | 00000000000001101110111011101100000000000000000000 | 96 | 43 | 4,5 |
| $\lambda_3$ | 00000000000011101110111011101000000000000000000000 | 96 | 44 | 20 |
| $\lambda_4$ | 00000000010111111011101110100000000000000000000000 | 64 | 41 | 5,7 |
| $\lambda_5$ | 00000000000011101110111011101100000000000000000000 | 64 | 47 | 914 |
| $\lambda_6$ | 00000000000011101110111011101110000000000000000000 | 32 | 48 | 509 |

В таблице приведены булевы векторы $\lambda_i \in \{0,1\}^{48}$, $i \in \{1,\ldots,6\}$, задающие ослабляющие ограничения в форме значений «переменных переключения» [5, 6]: единичные компоненты вектора $\lambda_i$ означают, что переменные сцепления, вычисляемые на шагах с соответствующими номерами, заменяются в системе уравнений, кодирующей криптоанализ функции MD4-$k$, 32-битной константой $K = 0$. Каждый такой набор ослабляющих ограничений позволяет построить семейство специальных функций вида $g^{\lambda_i}_{\text{MD4-}k} : \{0,1\}^{d} \to \{0,1\}^{128}$. Так, например, вектор $\lambda_3$ задаёт набор ослабляющих ограничений, в которых константой $K = 0$ означиваются переменные сцепления, вычисляемые на шагах с номерами 13, 14, 15, 17, 18, 19, 21, 22, 23, 25, 26, 27, 29. Для $\lambda_3$ можно построить специальные функции вида $g^{\lambda_3}_{\text{MD4-}k} : \{0,1\}^{96} \to \{0,1\}^{128}$. Для $k = 44$ функция $g^{\lambda_3}_{\text{MD4-44}}$ определена на $\approx 50\,\%$ случайных входов, а задача обраще-

ния $g^{\lambda_3}_{\text{MD4-44}}$-образа случайного входа из $\{0,1\}^{96}$ решается за время $\leqslant 20$ с работы SAT-решателя MINISAT2.2. Для соответствующих входов доказывается отсутствие коллизий за относительно небольшое время работы MINISAT2.2 (все эксперименты проводились на вычислительном кластере «Академик В. М. Матросов» ИДСТУ СО РАН [10]). Следовательно, доля значений функции $g^{\lambda_3}_{\text{MD4-44}}$ в $\{0,1\}^{128}$ составляет приблизительно $2^{-32}$. Это означает, что вероятность для случайно выбранного входа из $\{0,1\}^{512}$ получить легкообратимое значение функции MD4-44 составляет примерно $2^{-32}$ — весьма большая вероятность в сравнении с $2^{-128}$. Таким образом, функция MD4-44 не удовлетворяет свойствам случайного оракула. Интересно, что для полнораундовой функции MD4 (т. е. функции MD4-48) доля легко обратимых значений, как следует из шестой строки таблицы, составляет $2^{-96}$, что тоже недопустимо много для случайного оракула.

## ЛИТЕРАТУРА


1. *Bellare M. and Rogaway P.* Random oracles are practical: a paradigm for designing efficient protocols // Proc. CCS'93. N.Y.: ACM, 1993. P. 62–73.
2. *Pointcheval D. and Stern J.* Security proofs for signature schemes // EUROCRYPT'96. LNCS. 1996. V. 1070. P. 387–398.
3. *Pointcheval D. and Stern J.* Security arguments for digital signatures and blind signatures // J. Cryptology. 2000. V. 13. No. 3. P. 361–396.
4. *Rivest R. L.* The MD4 message digest algorithm // CRYPTO'90. LNCS. 1990. V. 537. P. 303–311.
5. *Gribanova I. and Semenov A.* Using automatic generation of relaxation constraints to improve the preimage attack on 39-step MD4 // Proc. MIPRO-2018. IEEE, 2018. P. 1174–1179.
6. *Грибанова И. А.* Новый алгоритм порождения ослабляющих ограничений в задаче обращения хеш-функции MD4-39 // Прикладная дискретная математика. Приложение. 2018. № 11. С. 139–141.
7. *Dobbertin H.* The first two rounds of MD4 are not one-way // Proc. FSE'1998. LNCS. 1998. V. 1372. P. 284–292.
8. *De D., Kumarasubramanian A., and Venkatesan R.* Inversion attacks on secure hash functions using SAT solvers // Proc. FSE'2007. LNCS. 2007. V. 4501. P. 377–382.
9. *Boros E. and Hammer P. L.* Pseudo-boolean optimization // Discr. Appl. Math. 2002. V. 123 (1–3), P. 155–225.
10. Иркутский суперкомпьютерный центр СО РАН. `http://hpc.icc.ru`.


УДК 003.26, 519.725 DOI 10.17223/2226308X/12/31

# ПОИСК ЭКВИВАЛЕНТНЫХ КЛЮЧЕЙ КРИПТОСИСТЕМЫ МАК-ЭЛИСА — СИДЕЛЬНИКОВА, ПОСТРОЕННОЙ НА ДВОИЧНЫХ КОДАХ РИДА — МАЛЛЕРА

А. М. Давлетшина

Предлагается новый способ восстановления эквивалентного секретного ключа криптосистемы Мак-Элиса — Сидельникова, построенной на двоичных кодах Рида — Маллера. Рассматривается криптосистема, для построения которой используются только две копии кода. Задача восстановления эквивалентного секретного ключа криптосистемы Мак-Элиса — Сидельникова сводится к двум задачам поиска эквивалентного секретного ключа криптосистемы Мак-Элиса. Доказано, что предложенный способ имеет полиномиальную сложность. Проведены численные эксперименты на различных параметрах кода Рида — Маллера, подтверждающие

возможность восстановления эквивалентного секретного ключа криптосистемы Мак-Элиса — Сидельникова за полиномиальное время.

**Ключевые слова:** *криптосистема Мак-Элиса — Сидельникова, код Рида — Маллера, полиномиальная атака.*

Криптосистема Мак-Элиса — Сидельникова является криптосистемой с открытым ключом, стойкость которой основана на сложности задачи декодирования произвольного кода, исправляющего ошибки. В 1994 г. В. М. Сидельников [1] несколько изменил схему криптосистемы Мак-Элиса, предложив использовать не одну, а $u$ копий кода, что повысило скорость передачи и стойкость криптосистемы. Предложенная схема получила название криптосистемы Мак-Элиса — Сидельникова. В качестве линейного кода, имеющего эффективный алгоритм декодирования, в работе Сидельникова используются коды Рида — Маллера. В 2007 г. Л. Миндер и А. Шокроллахи [2] построили структурную атаку на криптосистему Мак-Элиса. В 2013 г. М. Бородин и И. Чижов в работе [3] существенно понизили стойкость криптосистемы Мак-Элиса, при некоторых параметрах кода реализовав полиномиальную атаку на открытый ключ. Таким образом, вопрос стойкости криптосистемы Мак-Элиса — Сидельникова является достаточно актуальным.

Секретным ключом криптосистемы Мак-Элиса — Сидельникова является кортеж $(H, P)$, где $H$ — невырожденная матрица над полем $\mathrm{GF}(2)$; $P$ — перестановочная матрица. Открытым ключом является матрица $G = (R||HR)P$, где $R$ — порождающая матрица кода Рида — Маллера $\mathrm{RM}(r, m)$.

**Определение 1.** Код с порождающей матрицей вида $G = (R||HR)$ называется сегментарным кодом Рида — Маллера $\mathrm{RM}(r, m)[H]$.

Таким образом, необходимо найти такие матрицы $H'$ и $P'$, что $(R||HR)P = (R||H'R)P'$. Для этого необходимо выполнить следующие шаги:

1) построить формулу $U$ над операциями произведения Шура $\odot$ кодов и взятия ортогонального $\perp$ кода, такую, что

$$U(\mathrm{RM}(r, m)[H]) \subseteq \mathrm{RM}(m - r\,(\lceil m/r \rceil - 1) - 1, m) \times \mathrm{RM}(m - r(\lceil m/r \rceil - 1) - 1, m);$$

2) используя алгоритм Сендрие [4], разделить $\mathrm{RM}(m - r(\lceil m/r \rceil - 1) - 1, m) \times \times \mathrm{RM}(m - r(\lceil m/r \rceil - 1) - 1, m)$ на две копии кода $\mathrm{RM}(m - r(\lceil m/r \rceil - 1) - 1, m)$;
3) найти перестановку для каждого сегмента, используя алгоритм Чижова — Бородина, если $(r, m - 1) = 1$, либо алгоритм Миндера — Шокроллахи, если $(r, m - 1) \neq 1$;
4) найти матрицу $H'$ секретного ключа криптосистемы.

Полученные теоретические результаты можно разделить на два случая и кратко представить следующими теоремами.

С л у ч а й 1:

$$U(\mathrm{RM}(r, m)[H]) = \mathrm{RM}(d, m) \times \mathrm{RM}(d, m), \text{где } d = (r, m - 1).$$

**Теорема 1.** Если $(r, m - 1) = 1$, то существует алгоритм, который по порождающей матрице кода $\mathrm{RM}^P(r, m)[H]$ находит перестановку $P'$, такую, что $\mathrm{RM}^{PP'}(r, m)[H] = \mathrm{RM}(r, m)[H]$. Сложность алгоритма $\mathrm{O}(n^4 \log_2 n)$.

Если $(r, m-1) \neq 1$, то существует алгоритм, который по порождающей матрице кода $\mathrm{RM}^P(r, m)[H]$ находит перестановку $P'$, такую, что $\mathrm{RM}^{PP'}(r, m)[H] = \mathrm{RM}(r, m)[H]$. Сложность алгоритма $\mathrm{O}(n^d)$.

С л у ч а й 2:

$$U(\mathrm{RM}(r,m)[H]) \subset \mathrm{RM}(m - r(\lceil m/r \rceil - 1) - 1, m) \times \mathrm{RM}(m - r(\lceil m/r \rceil - 1) - 1, m).$$

**Теорема 2.** Если $m$ делится на $r$ без остатка, то существует алгоритм, который по порождающей матрице кода $\mathrm{RM}^P(r,m)[H]$ находит перестановку $P'$, такую, что $\mathrm{RM}^{PP'}(r,m)[H] = \mathrm{RM}(r,m)[H]$. Сложность алгоритма $\mathrm{O}(n^{2^r})$.

Если $m$ не делится на $r$ без остатка и $(r, m-1) = 1$, то существует алгоритм, который по порождающей матрице кода $\mathrm{RM}^P(r,m)[H]$ находит перестановку $P'$, такую, что $\mathrm{RM}^{PP'}(r,m)[H] = \mathrm{RM}(r,m)[H]$. Сложность алгоритма $\mathrm{O}(n^{2^{m-r\lfloor m/r \rfloor}})$.

Если $m$ не делится на $r$ без остатка и $(r, m-1) \neq 1$, то существует алгоритм, который по порождающей матрице кода $\mathrm{RM}^P(r,m)[H]$ находит перестановку $P'$, такую, что $\mathrm{RM}^{PP'}(r,m)[H] = \mathrm{RM}(r,m)[H]$. Сложность алгоритма $\mathrm{O}(\max(n^{2^{m-r\lfloor m/r \rfloor}}, n^{d+1}))$.

Теоретические результаты подтверждаются практическими экспериментами: алгоритм реализован программно и исследован на ноутбуке с процессором 2,5 ГГц. Результаты приведены в табл. 1 для случая 1 и в табл. 2 для случая 2.

Т а б л и ц а 1

| Данные | Параметры кодов $(r,m)$ | | | | | | |
|---|---|---|---|---|---|---|---|
| | (2,6) | (2,8) | (3,8) | (3,9) | (2,10) | (4,10) | (3,11) |
| Время работы | 1,747 с | 46,218 с | 52,165 с | 11 м 9 с | 2 ч 39 м | 4 ч 32 м | 8 ч 19 м |
| Размер ключа | 352 б | 2,3 Кб | 5,8 Кб | 16,25 Кб | 14 Кб | 96,5 Кб | 116 Кб |

Т а б л и ц а 2

| Данные | Параметры кодов $(r,m)$ | | | | | | |
|---|---|---|---|---|---|---|---|
| | (3,8) | (3,9) | (2,10) | (4,10) | (3,11) | (3,12) | (4,12) |
| Время работы | 5 м 34 с | 3 ч 13 м | 4 ч 1 м | 5 ч 28 м | 12 ч 49 м | 32 ч 54 м | 51 ч 54 с |
| Размер ключа | 5,8 Кб | 16,25 Кб | 14 Кб | 96,5 Кб | 116 Кб | 299 Кб | 795 Кб |

## ЛИТЕРАТУРА


1. *Сидельников В. М.* Открытое шифрование на основе двоичных кодов Рида — Маллера // Дискретная математика. 1994. Т. 6. № 2. С. 3–20.
2. *Minder L. and Shokrollahi A.* Cryptanalysis of the Sidelnikov cryptosystem // Ann. Intern. Conf. Theory and Appl. of Cryptographic Techniques. Berlin; Heidelberg: Springer, 2007. P. 347–360.
3. *Бородин М. А., Чижов И. В.* Эффективная атака на криптосистему Мак-Элиса, построенную на основе кодов Рида — Маллера // Дискретная математика. 2014. Т. 26. № 1. С. 10–20.
4. *Sendrier N.* On the structure of a randomly permuted concatenated code // Proc. EUROCODE'94. Cote d'Or, France, 1994. P. 169–173.

УДК 519.1 DOI 10.17223/2226308X/12/32

# ОБ АЛГОРИТМИЧЕСКОЙ РЕАЛИЗАЦИИ S-БОКСОВ 16×16 СО СТРУКТУРАМИ ARX И «БАБОЧКА»

С. М. Комиссаров

Предложены способы алгоритмической реализации новых s-боксов размера 16×16 бит, вычислительная сложность и криптографические характеристики которых улучшены по сравнению со способами, исследованными ранее. Первый способ реализует s-боксы на основе ARX (Add-Rotate-Xor)-структуры; второй — на основе структуры «Бабочка» с использованием нелинейных подстановочных s-боксов размера 8×8 бит. Максимальная разностная характеристика (МРХ) предложенных s-боксов с ARX-структурой равна $18/2^{16}$, со структурой «Бабочка» — $10/2^{16}$. Максимальная линейная характеристика (МЛХ) s-боксов с ARX-структурой равна $764/2^{15}$, со структурой «Бабочка» — $512/2^{15}$. Минимальная степень нелинейности среди всех нетривиальных линейных комбинаций координатных функций предложенных s-боксов равна 15. Установлено, что использование предложенных s-боксов размера 16×16 бит в раундовых подстановках алгоритмов AES и «Кузнечик» позволяет улучшить их некоторые криптографические свойства. Для усечённых алгоритмов AES и «Кузнечик», реализующих несколько раундов шифрования, существенно снижены верхние оценки МРХ и МЛХ по сравнению с версиями алгоритмов, использующих штатные s-боксы.

**Ключевые слова:** *s-бокс* 16×16*, алгоритмическая реализация, ARX, «Бабочка», максимальная разностная характеристика, максимальная линейная характеристика, степень нелинейности.*

Цель работы — оценить важнейшие характеристики некоторых способов реализации s-боксов (узлов замены) размера 16×16 бит и перспективы их использования в итеративных алгоритмах блочного шифрования.

Нелинейные отображения векторного пространства $V_n$ (s-боксы размера $n \times n$ бит) в симметричных алгоритмах блочного шифрования обычно реализуются в виде таблиц, содержащих множество всех образов. Для хранения одного такого массива требуется $n^2$ бит памяти. Это вынуждает в алгоритмах блочного шифрования использовать s-боксы малых размеров (8×8 бит в алгоритме «Кузнечик», 4×4 в алгоритме «Магма», 6×4 в DES, 8×8 в AES). В данной работе предложены способы алгоритмической реализации новых s-боксов большого размера (16×16 бит). При алгоритмическом вычислении значений s-боксов больших затрат памяти не требуется.

Обозначим $b : \mathbb{Z}_{2^n} \to V_n$ — биективное отображение числа $X \in \mathbb{Z}_{2^n}$ в его двоичное представление, $b(X) = \bar{X} = (x_0, \ldots, x_{n-1})$; $(\bar{X}_1, \bar{X}_2)$ — конкатенация двух векторов; $X_1, X_2 \in \mathbb{Z}_{2^n}$ — полублоки входного блока $X$ s-бокса, $X = (X_1, X_2) \in \mathbb{Z}_{2^{16}}$; $b(X_1) = \bar{X}_1 = (x_0, \ldots, x_7)$, $b(X_2) = \bar{X}_2 = (x_8, \ldots, x_{15})$, $b(X) = (x_0, \ldots, x_{15})$; $Y \ggg t$ ($Y \lll t$) — циклический сдвиг координат вектора $Y$ на $t$ бит вправо (влево); $\otimes$ — умножение в поле $\mathbb{F}(2^8) = \mathbb{F}_2[x]/(x^8 + x^4 + x^3 + x + 1)$; $a^{254} = a^{-1}$ — обратный к ненулевому элементу $a$ поля $\mathbb{F}(2^8)$; $S : V_m \to V_m$ — функция s-бокса размера $m \times m$ бит.

Для $x \in V_m$ и $x' = x \oplus a \in V_m$ (пар текстов с фиксированной разностью $a \in V_m$) и s-бокса $S : V_m \to V_m$ определим разностную характеристику (РХ) $DP^S(a, b) = |\{x \in V_m : S(x) \oplus S(x') = b\}|/2^m$ — вероятность появления случайной величины — разности $b \in V_m$ выходных текстов $S(x)$ и $S(x')$. Максимальная разностная характеристика (МРХ) s-бокса определена как $p_s = \max\limits_{a,b \in V_m^{\times}} DP^S(a, b)$. Для векто-

ра $a = (a_0, \ldots, a_{m-1}) \in V_m$ определим линейную булеву функцию $l_a(x_0, \ldots, x_{m-1}) = \bigoplus_{i=0}^{m-1} a_i x_i$. Для некоторых $a, b \in V_m$ и s-бокса $S : V_m \to V_m$ с компонентными функциями $(S_0, \ldots, S_{m-1})$ определим линейную характеристику (ЛХ) $LP^S(a,b) = 2^{1-m}|\{x \in V_m : l_a(x) = l_b(S(x))\}| - 1$. Максимальную линейную характеристику (МЛХ) s-бокса $S$ определим как $\delta_S = \max_{a,b \in V_m^\times} LP^S(a,b)$. Пусть $\deg f$ — степень нелинейности функции $f$. Минимальная степень нелинейности среди всевозможных линейных комбинаций координатных функций определена в [1] как $\lambda_S = \min_{a,b \in V_m^\times} \{\deg(l_a(S(x)))\}$. Производительность s-боксов измеряется в Мбайт/с, ёмкость памяти — в байтах.

Алгоритмы AES и «Кузнечик» при использовании в них s-боксов размера 16×16 бит вместо стандартных обозначим AES16 и K16.

## 1. Описание метода алгоритмической реализации s-бокса 16×16 с ARX-структурой

s-Боксы на основе ARX-структуры используют операции сложения, циклического сдвига и побитового XOR-сложения векторов. Эти операции не требуют существенных затрат памяти на хранение предварительно вычисленных таблиц [2, 3], характеризуются низкой ресурсоёмкостью в программных и аппаратных реализациях и выполняются менее чем за половину такта процессора.

Раундовые подстановки $g_i : V_{16} \to V_{16}$, $i = 1, 2$, s-боксов 16×16 с ARX-структурой, предлагаемые в данной работе, в общем виде представимы в виде композиции двух преобразований $f_{i1}, f_{i2} : V_{16} \to V_{16}$:

$$g_i(X) = f_{i2} \circ f_{i1}(X). \tag{1}$$

Построены перспективные схемы с ARX-структурой с точки зрения сочетания положительных криптографических характеристик с высокой производительностью программной реализации.

Первый вариант раундового преобразования (1) s-бокса обозначим $g_1$, для него

$$f_{11}(X) = (b(((X_1 \ggg 2) + X_2) \bmod 2^8), \bar{X}_2),\ f_{12}(X) = (\bar{X}_1, b(((X_2 \lll 1) + C) \bmod 2^8) \oplus \bar{X}_1).$$

Второй вариант раундового преобразования (1) s-бокса обозначим $g_2$, для него

$$f_{21}(X) = (b(((X_1 \lll 1) + X_2) \bmod 2^8), \bar{X}_2),\ f_{22}(X) = (\bar{X}_1, b(((X_2 \ggg 2) + C) \bmod 2^8) \oplus \bar{X}_1).$$

Здесь $C \in \mathbb{Z}_{2^8}$ — константа, $C = 185$ для $g_1$ и $C = 100$ для $g_2$. Обозначим $\varphi_1 = g_1^6$, $\varphi_2 = g_2^6$ — предложенные s-боксы с ARX-структурой.

Экспериментально установлено, что для предложенных s-боксов $p_{\varphi_1} = p_{\varphi_2} = 18/2^{16}$, $\delta_{\varphi_1} = 762/2^{15}$, $\delta_{\varphi_2} = 764/2^{15}$, $\lambda_{\varphi_1} = \lambda_{\varphi_2} = 15$.

В табл. 1 приведены частоты значений $DP$ в таблицах разностей $\varphi_1$ и $\varphi_2$. Видно, что частота встречаемости MPX невелика, поэтому при реализации разностной атаки сложно подобрать несколько s-боксов с MPX более чем в одном рауде шифрования.

Таблица 1

**Частота встречаемости значений $DP$ в таблицах разностей $\varphi_1$ и $\varphi_2$**

| $2^{16} \cdot DP$ | 0 | 2 | 4 | 6 | 8 | 10 | 12 | 14 | 16 | 18 |
|---|---|---|---|---|---|---|---|---|---|---|
| $\varphi_1$ | $2{,}6 \cdot 10^9$ | $1{,}3 \cdot 10^9$ | $3{,}3 \cdot 10^8$ | $5{,}4 \cdot 10^7$ | $6{,}8 \cdot 10^6$ | 678529 | 56603 | 4062 | 280 | 14 |
| $\varphi_2$ | $2{,}6 \cdot 10^9$ | $1{,}3 \cdot 10^9$ | $3{,}3 \cdot 10^8$ | $5{,}4 \cdot 10^7$ | $6{,}8 \cdot 10^6$ | 677386 | 56885 | 4058 | 256 | 7 |

## 2. Об алгоритмической реализации s-бокса 16×16 со структурой «Бабочка»

В [4, 5] предложены способы построения s-боксов 8×8 со структурой «Бабочка» с использованием умножения в $\mathrm{GF}(2^4)$ и подстановок меньших размеров (4×4 бит), реализующих мономы в $\mathrm{GF}(2^4)$. В данной работе предложены два типа s-боксов 16×16 со структурой «Бабочка» с использованием умножения в $\mathrm{GF}(2^8)$ и подстановок меньших размеров (8×8 бит), реализующих мономы в $\mathrm{GF}(2^8)$. Обозначим $\psi_i : V_{16} \to V_{16}$, $i = 1, 2$:

$$\psi_i(X) = \psi_i(\bar{X}_1, \bar{X}_2) = (b(F_{i1}(X_1, X_2)), b(F_{i2}(X_2, F_{i1}(X_1, X_2)))) = (\bar{X}'_1, \bar{X}'_2).$$

За основу первого типа s-боксов 16×16 взята структура из [4]. Обозначим его $\psi_1$, для него

$$F_{11}(X_1, X_2) = X'_1 = \begin{cases} h_1(X_1), & X_2 = 0, \\ (X_1 \otimes X_2)^{254}, & X_2 \neq 0, \end{cases}$$

$$F_{12}(X_2, X'_1) = X'_2 = \begin{cases} h_2(X_2), & X'_1 = 0, \\ X'_1 \otimes (X_2)^{254}, & X'_1 \neq 0, \end{cases}$$

где $F_{11}(X_1, X_2), F_{12}(X_2, X_1) : \mathbb{F}(2^{16}) \to \mathbb{F}(2^8)$ — биективные функции по $X_1$ и $X_2$ соответственно; $h_1, h_2 : \mathbb{F}(2^8) \to \mathbb{F}(2^8)$ — нелинейные подстановки, реализующие мономы в $\mathbb{F}_2[x]/(x^8 + x^4 + x^3 + x + 1)$. При $h_2(x) \in \{x^{254}, x^{253}\}$ и $h_1(x) = x^k$, где $k \in \{28, 37, 56, 73, 74, 131, 146, 148, 164, 191, 193, 239, 247, 251, 253, 254\}$, отображение $\psi_1$ биективно, $p_{\psi_1} = 10/2^{16}$, $\lambda_{\psi_1} = 15$ и $\delta_{\psi_1} = 512/2^{15}$.

За основу второго типа s-боксов 16×16 взята структура из [5]. Обозначим его $\psi_2$, для него

$$F_{21}(X_1, X_2) = X'_1 = \begin{cases} (X_1)^{254}, & X_2 = 0, \\ X_1 \otimes h_1(X_2), & X_2 \neq 0, \end{cases}$$

$$F_{22}(X_2, X'_1) = X'_2 = \begin{cases} (X_2)^{254}, & X'_1 = 0, \\ X_2 \otimes h_2(X'_1), & X'_1 \neq 0, \end{cases}$$

где $F_{21}(X_1, X_2), F_{22}(X_2, X_1) : \mathbb{F}(2^{16}) \to \mathbb{F}(2^8)$ — биективные функции по $X_1$ и $X_2$ соответственно. При $h_2(x) = x^{254}$ и $h_1(x) = x^2$ отображение $\psi_2$ биективно, $p_{\psi_2} = 10/2^{16}$, $\lambda_{\psi_2} = 15$ и $\delta_{\psi_2} = 512/2^{15}$. При $h_2(x) \in \{x^{254}, x^{253}\}$ и $h_1(x) \in \{x^{32}, x^{16}\}$ отображение $\psi_2$ биективно, $p_{\psi_2} = 10/2^{16}$, $\lambda_{\psi_2} = 15$ и $\delta_{\psi_2} = 544/2^{15}$.

При алгоритмической реализации $\psi_1$ и $\psi_2$ мономы $h_1, h_2$ и $x^{-1}$ реализуются в виде таблиц, каждая из которых занимает $8 \cdot 2^8$ бит памяти. Требуются также две предварительно рассчитанные таблицы подстановок 8×8 бит для быстрой реализации произведения в $\mathbb{F}_2[x]/(x^8 + x^4 + x^3 + x + 1)$. Обозначим $\psi$ — s-бокс 16×16 со структурой «Бабочка», реализующий $\psi_1$ при $h_1 = h_2 = x^{254} = x^{-1}$. При алгоритмической реализации он требует одну предварительно рассчитанную таблицу, задающую моном $x^{254}$, и имеет следующие характеристики: $p_\psi = 10/2^{16}$, $\lambda_\psi = 15$ и $\delta_\psi = 512/2^{15}$. В табл. 2 приведено распределение разностных характеристик в его таблице разностей.

В табл. 3 приведено сравнение МРХ, МЛХ и минимальной степени нелинейности среди всевозможных линейных комбинаций компонентных функций известных и предложенных s-боксов.

Таблица 2

**Частота встречаемости значений $DP$ в таблице разностей $\psi$**

| $2^{16} \cdot DP$ | 0 | 2 | 4 | 6 | 8 | 10 |
|---|---|---|---|---|---|---|
| $\psi$ | 2507045091 | 1602586456 | 12279975 | 171659076 | 1328564 | 2598 |

Таблица 3

**Сравнение $p_s$, $\delta_s$ и $\lambda_s$ для s-боксов**

| s-Бокс | AES | Skipjack | «Кузнечик» | $\varphi_1$ | $\varphi_2$ | $\psi$ | $x^{-1}$, таблица [6] |
|---|---|---|---|---|---|---|---|
| Размер | $8 \times 8$ | $8 \times 8$ | $8 \times 8$ | $16 \times 16$ | $16 \times 16$ | $16 \times 16$ | $16 \times 16$ |
| $p_s$ | $4/2^8$ | $12/2^8$ | $8/2^8$ | $18/2^{16}$ | $18/2^{16}$ | $10/2^{16}$ | $4/2^{16}$ |
| $\delta_s$ | $12/2^7$ | $28/2^7$ | $28/2^7$ | $762/2^{15}$ | $764/2^{15}$ | $512/2^{15}$ | $256/2^{15}$ |
| $\lambda_s$ | 7 | 6 | 7 | 15 | 15 | 15 | 15 |

## 3. Верхние оценки разностной и линейной характеристик для алгоритмов AES16 и K16

При реализации разностной атаки s-бокс называется активным для раунда итеративного алгоритма блочного шифрования, если разность поступающих на этом раунде ему на вход текстов не равна нулю.

Пусть $L : V_m^n \to V_m^n$ — линейное преобразование алгоритма блочного шифрования на основе SP-сети с размером блока $m{\cdot}n$ бит. Обозначим $\beta_i$, $i = 1, \ldots, 4$, число активных s-боксов на $i$-м раунде.

Степень ветвления (branch number) линейного преобразования $L$ (обозначим $\beta_2^L$ или $\beta_2$ в случае, когда $L$ является композицией всех используемых в алгоритме линейных преобразований) есть

$$\beta_2^L = \min_{x \in V_n^*} \{w(x) + w(L(x))\},$$

где $w(x) = w(x_1, x_2, \ldots, x_n) = |\{x_i \neq 0 : x_i \in V_m, i = 1, \ldots, n\}|$.

Степень ветвления алгоритма блочного шифрования на основе SP-сети можно определить как минимальное возможное число активных s-боксов, участвующих в первых двух раундах шифрования. Известно [7], что для AES $\beta_2 = 5$, $\beta_4 = (\beta_2)^2 = 25$, для алгоритма «Кузнечик» $\beta_2 = 17$ [8]. Для AES16 $\beta_2 = 5$, $\beta_4 = 15$; для K16 $\beta_2 = 9$.

Обозначим $a^k, b^k \in V_m^n$ разности пар входных и выходных текстов размера $mn$ бит $k$-го раунда алгоритма блочного шифрования на основе SP-сети с s-боксами $S_i : V_m \to V_m$, $i = 1, \ldots, n$; $DP_2(a^1, b^2)$ $(DP_4(a^1, b^4))$ — РХ двух (четырёх) раундов алгоритма шифрования на основе SP-сети; $LP_2(a^1, b^2)$ $(LP_4(a^1, b^4))$ — ЛХ двух (четырёх) раундов алгоритма шифрования на основе SP-сети.

**Теорема 1** [9]. Для любой ненулевой разности $a^1 \in V_{m \cdot n}^{\times}$ пары входных текстов РХ двух раундов алгоритма шифрования на основе SP-сети верно неравенство

$$DP_2(a^1, b^2) \leqslant \max \left\{ \max_{1 \leqslant i \leqslant n} \max_{1 \leqslant u \leqslant 2^m - 1} \sum_{j=1}^{2^m - 1} \{DP^{S_i}(u, j)\}^{\beta_2}, \max_{1 \leqslant i \leqslant n} \max_{1 \leqslant u \leqslant 2^m - 1} \sum_{j=1}^{2^m - 1} \{DP^{S_i}(j, u)\}^{\beta_2} \right\}.$$

В табл. 4 и 5 приведено сравнение посчитанных по лемме 1 [9] и теореме 1 верхних оценок РХ двух и четырёх раундов AES16 и K16 с оценками версий алгоритмов, использующих штатные s-боксы.

Приведём другие оценки РХ/ЛХ двух и четырёх раундов AES16 и K16, основанные на МРХ/МЛХ используемого s-бокса, аналогичные оценкам AES в [7]. Обозна-

Таблица 4

**Верхние оценки PX для AES и AES16 по теоремам [9]**

| Алгоритм | AES [9] | AES16 с $\varphi_1$ | AES16 с $\varphi_2$ | AES16 с $\psi$ |
|---|---|---|---|---|
| $DP_2(a,b) \leqslant$ | $1{,}234 \cdot 2^{-28}$ | $1{,}177 \cdot 2^{-56}$ | $1{,}217 \cdot 2^{-56}$ | $1{,}362 \cdot 2^{-56}$ |
| $DP_4(a,b) \leqslant$ | $1{,}144 \cdot 2^{-111}$ | $1{,}240 \cdot 2^{-209}$ | $0{,}950 \cdot 2^{-208}$ | $0{,}956 \cdot 2^{-208}$ |

Таблица 5

**Оценки PX для алгоритмов «Кузнечик» и K16 по теоремам [9]**

| Алгоритм | «Кузнечик» [9] | K16 с $\varphi_1$ | K16 с $\varphi_2$ | K16 с $\psi$ |
|---|---|---|---|---|
| $DP_2(a,b) \leqslant$ | $0{,}909 \cdot 2^{-106}$ | $0{,}932 \cdot 2^{-112}$ | $1{,}395 \cdot 2^{-113}$ | $1{,}015 \cdot 2^{-120}$ |

чим $DP_2^S(a,b), DP_4^S(a,b)$ ($LP_2^S(a,b), LP_4^S(a,b)$) PX (ЛХ) двух и четырёх раундов алгоритма шифрования на основе SP-сети, использующего единственный s-бокс $S$; $\varphi$ — любой из предложенных s-боксов с ARX-структурой ($\varphi_1$ или $\varphi_2$). Для любой ненулевой разности $a \in V_{m \cdot n}^{\times}$ имеет место $DP_2^S(a,b) \leqslant p_S^{\beta_2}$, $LP_2^S(a,b) \leqslant \delta_S^{\beta_2}, DP_4^S(a,b) \leqslant p_S^{\beta_4}$, $LP_4^S(a,b) \leqslant \delta_S^{\beta_4}$ [7]. Для AES16:

$$DP_2^{\varphi}(a,b) \leqslant p_{\varphi}^{\beta_2} = (18 \cdot 2^{-16})^5 \approx 0{,}9 \cdot 2^{-59};\ DP_4^{\varphi}(a,b) \leqslant p_{\varphi}^{\beta_4} = (18 \cdot 2^{-16})^{15} \approx 1{,}46 \cdot 2^{-178};$$

$$DP_2^{\psi}(a,b) \lesssim 1{,}52 \cdot 2^{-64};\ DP_4^{\psi}(a,b) \lesssim 1{,}78 \cdot 2^{-191};$$

$$LP_2^{\varphi_1}(a,b) \leqslant \delta_{\varphi_1}^{\beta_2} = (762 \cdot 2^{-15})^5 \approx 0{,}913 \cdot 2^{-27};$$

$$LP_4^{\varphi_1}(a,b) \leqslant \delta_{\varphi_1}^{\beta_4} = (762 \cdot 2^{-15})^{15} \approx 1{,}521 \cdot 2^{-82};$$

$$LP_2^{\varphi_2}(a,b) \lesssim 0{,}924 \cdot 2^{-27};\ LP_4^{\varphi_2}(a,b) \lesssim 1{,}582 \cdot 2^{-82};\ LP_2^{\psi}(a,b) \leqslant 2^{-30};\ LP_4^{\psi}(a,b) \leqslant 2^{-90}.$$

Для K16:

$$DP_2^{\varphi}(a,b) \leqslant p_{\varphi}^{\beta_2} = (18 \cdot 2^{-16})^9 \approx 1{,}443 \cdot 2^{-107};\ LP_2^{\varphi_1}(a,b) \lesssim 1{,}119 \cdot 2^{-49};$$

$$LP_2^{\varphi_2}(a,b) \lesssim 1{,}146 \cdot 2^{-49};\ DP_2^{\psi}(a,b) \lesssim 0{,}931 \cdot 2^{-114};\ LP_2^{\psi}(a,b) \leqslant 2^{-54}.$$

В табл. 6 и 7 приведено сравнение полученных оценок с оценками версий алгоритмов, использующих штатные s-боксы, в табл. 8 и 9 — сравнение производительности и затрат памяти s-боксов.

Таблица 6

**Оценки PX и ЛХ для AES и AES16 на основе MPX и MЛХ s-бокса**

| Алгоритм | AES [7] | AES16 с $\varphi_1$ | AES16 с $\varphi_2$ | AES16 с $\psi$ |
|---|---|---|---|---|
| $DP_2(a,b) \leqslant$ | $2^{-30}$ | $0{,}9 \cdot 2^{-59}$ | $0{,}9 \cdot 2^{-59}$ | $1{,}52 \cdot 2^{-64}$ |
| $DP_4(a,b) \leqslant$ | $2^{-150}$ | $1{,}46 \cdot 2^{-178}$ | $1{,}46 \cdot 2^{-178}$ | $1{,}78 \cdot 2^{-191}$ |
| $LP_2(a,b) \leqslant$ | $2^{-15}$ | $0{,}913 \cdot 2^{-27}$ | $0{,}924 \cdot 2^{-27}$ | $2^{-30}$ |
| $LP_4(a,b) \leqslant$ | $2^{-75}$ | $1{,}521 \cdot 2^{-82}$ | $1{,}582 \cdot 2^{-82}$ | $2^{-90}$ |

Таблица 7

**Оценки PX и ЛХ для алгоритмов «Кузнечик» и K16 на основе MPX и MЛХ s-бокса**

| Алгоритм | «Кузнечик» | K16 с $\varphi_1$ | K16 с $\varphi_2$ | K16 с $\psi$ |
|---|---|---|---|---|
| $DP_2(a,b) \leqslant$ | $2^{-85}$ | $1{,}443 \cdot 2^{-107}$ | $1{,}443 \cdot 2^{-107}$ | $0{,}931 \cdot 2^{-114}$ |
| $LP_2(a,b) \leqslant$ | $0{,}826 \cdot 2^{-27}$ | $1{,}119 \cdot 2^{-49}$ | $1{,}146 \cdot 2^{-49}$ | $2^{-54}$ |

Таблица 8

**Сравнение производительности s-боксов (Intel Core i7-7700K, 4,2 ГГц)**

| s-Бокс | 16×16 на основе МАГ [3] | 16×16, $\varphi_1$ | 16×16, $\varphi_2$ | 16×16, $\psi$ | 8×8, «Кузнечик» |
|---|---|---|---|---|---|
| Мбайт/с | 136,239 | 444,604 | 383,773 | 200,141 | 449,846 |

Таблица 9

**Сравнение затрат памяти s-боксов**

| s-Бокс | 16×16, $\varphi_1$, $\varphi_2$ | | 16×16, $\psi$ | 16×16, табличный s-бокс [6] | 8×8, «Кузнечик», AES |
|---|---|---|---|---|---|
| Память | код, x86 | код, x64 | 768 байт | 128 кбайт | 256 байт |
| | 74 байта | 102 байта | | | |

## Выводы

Предложены новые конструкции s-боксов размера 16×16 бит: s-боксы на основе ARX-структуры, имеющие высокопроизводительную алгоритмическую реализацию, и s-боксы со структурой «Бабочка», использующие нелинейные подстановки меньшего размера — 8×8 бит. Предложенные s-боксы обладают рядом положительных криптографических свойств: высокой степенью нелинейности, низкой МРХ и МЛХ. МРХ предложенных s-боксов «Бабочка» равна $10/2^{16}$. Это наименьшее значение МРХ среди известных s-боксов 16×16, не реализующих поиск обратного элемента в конечном поле. В рамках вычислительного эксперимента производительность предложенных s-боксов с ARX-структурой не уступает производительности таблично реализуемого s-бокса 8×8. Предложенные s-боксы требуют небольшое количество памяти (75 байт на хранение машинных инструкций — ARX, 768 байт — «Бабочка»), в то время как табличная реализация s-бокса 16×16 требует 128 кбайт. Отмечено положительное влияние предложенных s-боксов на стойкость алгоритмов AES и «Кузнечик» к дифференциальному и линейному методам криптоанализа при их встраивании и существенное уменьшение верхних оценок максимальной разностной и линейной характеристик AES16 и K16. Данные результаты позволяют сделать предположение о возможности уменьшения количества раундов в рассмотренных стандартах блочного шифрования при встраивании в них s-боксов размера 16×16 бит с сохранением стойкости. Это позволит увеличить скорость шифрования с использованием рассмотренных алгоритмов.

Поиск новых конструкций нелинейных подстановок степени $2^{16}$ является перспективным направлением исследований.

## ЛИТЕРАТУРА

1. *Menyachikhin A.* Spectral-linear and spectral-difference methods for generating cryptographically strong S-boxes // CTCrypt Preproc. Yaroslavl, 2016. P. 232–252. https://mjos.fi/doc/rus/CTCrypt2016Preproceedings.pdf
2. *Фомичев В. М., Лолич Д. М., Юзбашев А. В.* Алгоритмическая реализация s-боксов на основе модифицированных аддитивных генераторов // Прикладная дискретная математика. Приложение. 2017. № 10. С. 102–104.
3. *Бобров В. М., Комиссаров С. М.* О свойствах двух классов s-боксов размера 16×16 // Прикладная дискретная математика. Приложение. 2018. № 11. С. 57–61.
4. *Jimenez R. A.* Generation of 8-bit s-boxes Having Almost Optimal Cryptographic Properties Using Smaller 4-bit s-boxes and Finite Field Multiplication. Havana: Havana University, Institute of Cryptography, 2017. http://www.cs.haifa.ac.il/~orrd/LC17/paper60.pdf
5. *Fomin D. B.* New Classes of 8-bit Permutations Based on a Butterfly Structure. CTCrypt. Suzdal, 2018. https://ctcrypt.ru/files/files/2018/09_Fomin.pdf

6. *Wood C. A.* Large Substitution Boxes with Efficient Combinational Implementations. Thesis. Rochester Institute of Technology, 2013.
7. *Daemen J. and Rijmen V.* The Design of Rijndael, AES — the Advanced Encryption Standard. Springer Verlag, 2002.
8. *AlTawy R. and Youssef A. M.* A meet in the middle attack on reduced round Kuznyechik // IEICE Trans. 2015. V. 98-A. P. 2194–2198.
9. *Park S., Sung S.H., Lee S., and Lim J.* Improving the upper bound on the maximum differential and the maximum linear hull probability for SPN structures and AES // LNCS. 2003. V. 2887. P. 247–260.

УДК 519.17 DOI 10.17223/2226308X/12/33

# ОЦЕНКА ХАРАКТЕРИСТИК ПЕРЕМЕШИВАНИЯ ХЭШ-ФУНКЦИЙ СЕМЕЙСТВА MD

А. М. Коренева

Матрично-графовый подход (МГП), нашедший успешное применение к оценке свойств итеративных блочных шифров и генераторов ключевого расписания, впервые представлен как инструмент оценивания перемешивающих свойств алгоритмов хэширования. Особенность применения МГП к хэш-функциям связана с неочевидностью построения перемешивающих матриц, характеризующих зависимость битов сгенерированного хэш-значения от битов исходного сообщения. Для хэш-функций MD4, MD5, SHA-1, SHA-256 построены перемешивающие матрицы порядка $512 + n$, где $n$ — длина блока, с которым оперирует односторонняя функция сжатия алгоритма хэширования при обработке 512-битового блока входного сообщения ($n = 128$ для MD4 и MD5, $n = 160$ для SHA-1 и $n = 256$ для SHA-256). К исследованным характеристикам перемешивания относятся локальные экспоненты перемешивающих матриц, то есть для каждой матрицы $M$ определено наименьшее натуральное число $\gamma$, такое, что при любом натуральном $\tau \geqslant \gamma$ положительны все столбцы матрицы $M^\tau$ с номерами $513, 514, \ldots, 512 + n$. Значения локальных экспонентов являются нижними оценками числа итераций, после которых каждый бит сгенерированного хэш-значения может существенно зависеть от всех битов исходного сообщения. Полученные значения ($\gamma = 21$ для MD4, MD5, SHA-256 и $\gamma = 23$ для SHA-1) косвенно свидетельствуют о схожих криптографических качествах рассмотренных алгоритмов хэширования, несмотря на варианты их усиления за счёт увеличения длины блока и усложнения функции сжатия.

**Ключевые слова:** *алгоритмы хэширования, структура Меркла — Дамгарда, матрично-графовый подход, перемешивающие свойства.*

## Введение

В основе принципа перемешивания, важного для многих криптографических алгоритмов, лежит существенная нелинейная зависимость выходных данных от элементов входа. Для оценки множества существенных переменных композиции преобразований векторного пространства применяется матрично-графовый подход, теоретические основы которого изложены в [1]. Глубина итерации преобразования, при которой каждый бит выходного значения может зависеть от всех битов входа, оценивается снизу значением экспонента примитивного перемешивающего орграфа. В течение последних лет МГП нашёл успешное применение для исследования свойств итеративных блочных шифров и генераторов ключевого расписания [2 – 4], для которых перемешиваю-

щие матрицы, характеризующие зависимость координатных функций выхода от переменных входа, строятся достаточно просто, в отличие от аналогичных матриц для алгоритмов хэширования. В работе представлен способ применения МГП для оценки характеристик перемешивания хэш-функций, реализующих структуру Меркла — Дамгарда (алгоритмы MD4, MD5, SHA-1, SHA-2).

## 1. Конструкция MD

Конструкция Меркла — Дамгарда, представленная в 1979 г. в диссертации Ральфа Меркла, лежит в основе большинства хэш-функций, разработанных в период с 1990 по 2008 г. Суть конструкции заключается в итеративном процессе последовательных преобразований, когда на вход каждой итерации поступает блок исходного текста и выход предыдущей итерации. Меркл и Дамгард независимо друг от друга показали, что если функция сжатия устойчива к коллизиям, то и хэш-функция будет также устойчива. В докладе рассматриваются известные хэш-функции из семейства MD с длиной блока текста 512 бит. Дадим краткое описание алгоритмов [5, 6].

Обозначим через $V_r$ множество всех двоичных векторов длины $r$, $\oplus$ — операция XOR-сложения двоичных векторов, $\boxplus$ — операция сложения по модулю $2^{32}$. Пусть $X$ — исходное сообщение, разбитое на $t \geqslant 1$ блоков $x_1, \ldots, x_t$, $x_i \in V_{512}$, $i = 1, 2, \ldots, t$, последний блок $x_t$ дополняется битовой строкой $1||0 \ldots 0$ до получения блока размером 448 бит, к которому затем добавляют длину исходного (недополненного) сообщения $X$, представленную в виде 64-битовой строки. Хэш-функции семейства MD построены на основе односторонней функции сжатия $\varphi(x_i, H_{i-1}) = H_i$, $i = 1, \ldots, t$, $H_i \in V_n$, $H_0$ — фиксированное начальное заполнение, $n = 128$ для MD4 и MD5, $n = 160$ для SHA-1 и $n = 256$ для SHA-256. Роль функции сжатия может осуществлять любой блочный шифр $E_X$, $\varphi(X, H) = E_X(H) \oplus H$.

Преобразования $E_X$ алгоритмов MD4, MD5, SHA-1, SHA-2 построены на основе регистров сдвига с 32-битовыми ячейками. Регистры имеют схожие принципы функционирования. Блок открытого текста длиной 512 бит записывается в первый регистр сдвига длины 16 над $V_{32}$ (изображён слева на рис. 1–3), выход с каждого такта подаётся на вход второго регистра над $V_{32}$ (изображён справа на рис. 1–3), начальным заполнением которого является значение $H_0$. Последнее состояние, в которое перейдёт второй регистр после выполнения всех тактов, определяет искомое хэш-значение $H_t$. Для усложнения на каждом такте с номером $j$ происходит суммирование с заранее заданными константами $C_j$ и применяются функции $f$ обратных связей нелинейных регистров, которые меняются в зависимости от такта.

Алгоритм MD4 (рис. 1, без пунктирной стрелки) реализует 48 тактов, MD5 (рис. 1, с пунктирной стрелкой) — 64 такта. В спецификации RFC 1321 для каждого такта с номером $j$ определены циклические сдвиги влево $s_j$, константы $C_j$ и функции $f$. Алгоритмы MD4 и MD5 не считаются надёжными, для них найдены способы нахождения коллизий с приемлемой вычислительной сложностью.

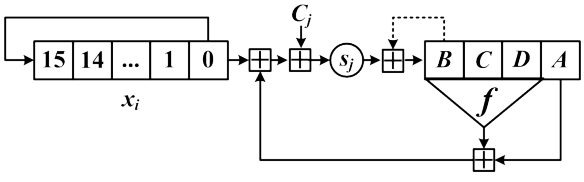


Рис. 1. Регистровое преобразование алгоритмов MD4 и MD5

Алгоритм SHA-1 реализует 80 тактов и считается усиленной версией MD5. Несмотря на известные успешные атаки, SHA-1 продолжает использоваться в почтовых программах, приложениях и сетевых протоколах передачи данных. В схеме на рис. 2 числа в кругах обозначают циклические сдвиги влево на соответствующее число бит, константы $C_j$ и функции $f$ определены в спецификации RFC 3174.

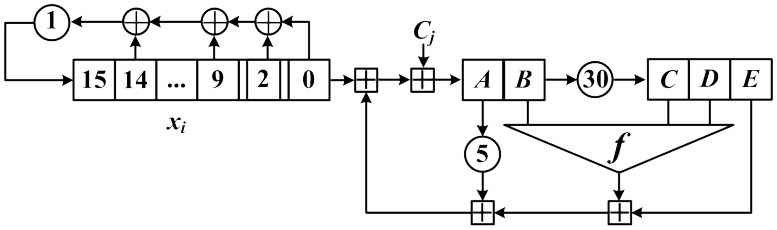


Рис. 2. Регистровое преобразование алгоритма SHA-1

К семейству SHA-2 относятся идентичные алгоритмы (SHA-224, SHA-256, SHA-384, SHA-512, SHA-512/256 и SHA-512/224), которые усиливают SHA-1 и считаются достаточно надёжными, но работают в несколько раз медленнее своих предшественников. На рис. 3 представлена схема SHA-256, алгоритм реализует 64 такта, константы $C_j$ и преобразования $Maj, Ch, \Sigma_0, \Sigma_1, \sigma_0, \sigma_1$ описаны в стандарте FIPS PUB 180-4.

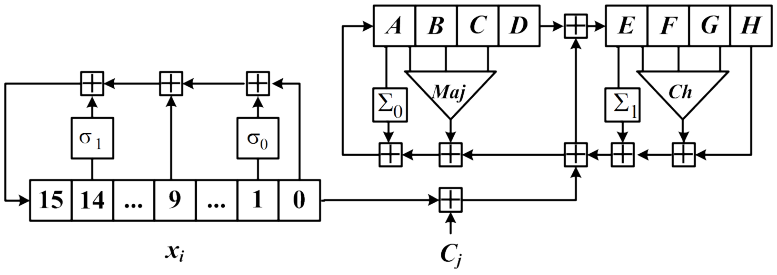


Рис. 3. Регистровое преобразование алгоритма SHA-256

## 2. Оценка перемешивающих свойств с использованием МГП

Особенность применения МГП к оценке перемешивающих свойств алгоритмов хэширования связана с неочевидностью построения перемешивающих матриц, характеризующих зависимость битов сгенерированного хэш-значения от битов исходного сообщения. Опишем способ построения перемешивающих матриц для регистровых преобразований хэш-функций MD4, MD5, SHA-1, SHA-256.

Используем следующие обозначения:

— $M(\varphi_1)$ — перемешивающая матрица размера $512 \times 512$ преобразования $\varphi_1$ первого регистра сдвига (слева на рис. 1–3);
— $M(\varphi_2)$ — перемешивающая матрица размера $n \times n$ преобразования $\varphi_2$ второго регистра сдвига (справа на рис. 1–3);
— $J$ — перемешивающая матрица размера $32 \times n$, определяющая зависимость состояния регистра $\varphi_2$ от выходного значения регистра $\varphi_1$ на каждом такте;
— $O_{m\times r}$ — матрица из $m$ нулевых строк и $r$ нулевых столбцов.

В соответствии со схемами из п. 1, перемешивающие матрицы $M$ регистровых преобразований MD4 и MD5 имеют порядок 640, SHA-1 — 672, SHA-256 — 768. Блоковый вид перемешивающих матриц $M$ представлен на рис. 4.

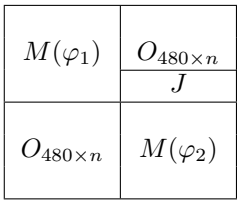


Рис. 4. Блоковый вид перемешивающих матриц $M$

Для каждого алгоритма хэширования построена перемешивающая $(0,1)$-матрица и применён МГП в соответствии с определениями [1]. Подсчитаны значения локальных экспонентов, то есть для каждой матрицы $M$ определено наименьшее натуральное число $\gamma$, такое, что при любом натуральном $\tau \geqslant \gamma$ положительны все столбцы матрицы $M^\tau$ с номерами $513, 514, \ldots, 512 + n$. Получены значения $\gamma = 21$ для MD4, MD5, SHA-256 и $\gamma = 23$ для SHA-1.

## Выводы

Впервые матрично-графовый подход применён для оценки свойств алгоритмов хэширования. Представлен способ построения перемешивающих матриц для регистровых преобразований хэш-функций MD4, MD5, SHA-1, SHA-256. Предложенный подход не требует трудоёмких вычислений и позволяет быстро получить существенную информацию о криптографических характеристиках алгоритмов. Подсчитаны значения локальных экспонентов перемешивающих матриц, которые являются нижними оценками числа итераций, после которых каждый бит сгенерированного хэш-значения может существенно зависеть от всех битов исходного сообщения. Полученные значения косвенно свидетельствуют о схожих перемешивающих свойствах рассмотренных алгоритмов хэширования, несмотря на варианты их усиления за счёт увеличения длины блока и усложнения функции сжатия.

## ЛИТЕРАТУРА

1. *Fomichev V. M., Avezova Ya. E., Koreneva A. M., and Kyazhin S. N.* Primitivity and local primitivity of digraphs and nonnegative matrices // J. Appl. Industr. Math. 2018. V. 12. No. 3. P. 453–469.
2. *Fomichev V. M., Koreneva A. M., Miftahutdinova A. R., and Zadorozhniy D. I.* Evaluation of the maximum productivity for block encryption algorithms // VII Симп. «Современные тенденции в криптографии» CTCrypt 2018. `https://ctcrypt.ru/files/files/2018/17_Koreneva.pdf`
3. *Fomichev V. M. and Koreneva A. M.* Mixing properties of modified additive generators // J. Appl. Industr. Math. 2017. V. 11. No. 2. P. 215–226.
4. *Коренева А. М., Мартышин В. Н.* Экспериментальное исследование экспонентов раундовых перемешивающих матриц обобщённых сетей Фейстеля // Прикладная дискретная математика. Приложение. 2016. № 9. С. 48–51.
5. *Авезова Я. Э.* Современные подходы к построению хеш-функций на примере финалистов конкурса SHA-3 // Вопросы кибербезопасности. 2015. № 3 (11). С. 60–67.
6. *Черемушкин А. В.* Криптографические протоколы. Основные свойства и уязвимости: учеб. пособие для студ. учреждений высш. проф. образования. М.: Издательский центр «Академия», 2009. 272 с.

УДК 519.151, 519.725, 519.165 DOI 10.17223/2226308X/12/34

# ОДНОРОДНЫЕ МАТРОИДЫ И БЛОК-СХЕМЫ

Н. В. Медведев, С. С. Титов

Работа посвящена исследованию однородных матроидов, т. е. таких, все циклы которых имеют одинаковую мощность. Эта задача связана с задачей описания идеальных однородных схем разделения секрета, т. е. таких схем, в которых все разрешённые коалиции имеют одинаковую мощность, а также с задачей описания матроидов, соответствующих идеальным совершенным схемам разделения секрета. Изучается возможность представления семейства когиперплоскостей однородного матроида как блоков блок-схемы $D(v, b, r, k, \lambda)$ с некоторым набором параметров, в том числе соответствующих системе троек Штейнера. Установлена взаимосвязь однородных матроидов с системой троек Штейнера. Доказано, что разделяющий матроид является однородным матроидом с трёхэлементными когиперплоскостями тогда и только тогда, когда его когиперплоскости образуют систему троек Штейнера, т. е. $k = 3$ и $\lambda = 1$.

**Ключевые слова:** *схемы разделения секрета, однородные матроиды, блок-схемы, циклы, системы троек Штейнера.*

Схема разделения секрета (СРС) — это система разраничения доступа, при которой участникам раздаются доли секрета таким образом, чтобы заранее заданные коалиции участников (разрешённые коалиции) могли однозначно восстановить секрет (совокупность этих множеств называется структурой доступа), а неразрешённые не получали никакой дополнительной информации, к имеющейся априорной, о возможном значении секрета. Такие СРС называются совершенными. Особый интерес вызывают идеальные СРС, т. е. такие, где размер доли секрета, предоставляемой участнику, не больше размера секрета. При этом разрешённые коалиции идеальной совершенной схемы разделения секрета определяются циклами некоторого связного матроида, изучение которого и даёт структуру доступа [1 – 4].

Актуальной задачей является описание однородных СРС [5 – 7], т. е. таких, где мощность всех разрешённых коалиций равна $k$, но, возможно, не все $k$-элементные множества входят в структуру доступа СРС. Под однородностью матроида понимается одинаковость мощностей его циклов, равная $n$, где, возможно, не все $n$-элементные множества — циклы; таким образом, для матроида однородной СРС справедливо равенство $n = k + 1$. При этом если все его $n$-элементные подмножества — циклы, то такой матроид называется пороговым (равномерным). Матроид называется связным, если для любых двух его элементов существует содержащий их цикл. Для исключения незаменимых участников идеальной СРС имеет смысл рассматривать только разделяющие матроиды. Матроид разделяющий тогда и только тогда, когда для любых $x \neq y$ существует разделяющий их цикл $C$, т. е. $x \notin C$, $y \in C$.

Будем понимать под блок-схемой $D(v, b, r, k, \lambda)$, согласно [8], такое размещение $v$ различных элементов по $b$ блокам, что каждый блок содержит точно $k$ различных элементов, каждый элемент появляется точно в $r$ различных блоках и каждая пара различных элементов появляется в $\lambda$ блоках.

Согласно [8], блок-схема с $k = 3$ вполне естественно называется системой троек. При этом параметры должны удовлетворять аксиомам $3b = rv$, $2r = \lambda(v - 1)$. Система троек с $\lambda = 1$ называется системой троек Штейнера. Условие $v \equiv 1, 3 \pmod 6$ необходимо и достаточно для существования штейнеровской системы троек.

В [9] выдвинута гипотеза о том, что однородный матроид определяется некоторой блок-схемой. В данной работе рассматривается связь однородных матроидов с частным случаем блок-схем — системами троек Штейнера.

Пусть все когиперплоскости (дополнения циклов) однородного матроида $M = (E, \mathcal{C})$, где $E$ — носитель, а $\mathcal{C}$ — семейство циклов с мощностью $n$, трехэлементны, т. е. $|E| = n + 3 = n + k$. Пусть $F$ — максимальное по включению подмножество носителя $E$ этого матроида, такое, что каждое его $n$-элементное подмножество является циклом. Поскольку, очевидно, $F$ является плоскостью матроида $M$, имеем $n \leqslant |F| \leqslant |E| - 2 = n + 1$, если $M$ не является равномерным, и при $|F| = n + 1$ имеем $|E \setminus F| = 2$, так что множество $E \setminus F = \{a, b\}$ двухэлементно, а любой цикл, не содержащийся в $F$, содержит $\{a, b\}$ (иначе $F$ было бы незамкнутым). Это противоречит тому, что $M$ — разделяющий. Следовательно, $|F| = n$ и $F$ есть цикл.

Пусть $G^* = \{a, b, c\}$ и $H^* = \{a, b, d\}$ — две когиперплоскости, пересекающиеся по двухэлементному подмножеству $\{a, b\}$. Тогда симметрическая разность дополнений $G^*$ и $H^*$ равна $\{c, d\}$, т. е. двухэлементна, и поэтому в объединении дополнений $G^*$ и $H^*$, мощность которого равна $(n + 1)$, каждое его $n$-элементное подмножество является циклом, что противоречит доказанному выше. Следовательно, любые две когиперплоскости матроида $M$ пересекаются не более чем по одноэлементному множеству.

Из свойства матроида быть разделяющим в терминах когиперплоскостей следует, что каждый элемент лежит хотя бы в одной когиперплоскости. Связность равносильна тому, что любая пара элементов лежит вне некоторой когиперплоскости. Из доказанного выше вытекает, что любая пара элементов лежит не более чем в одной когиперплоскости.

Докажем, что любая пара $\{a, b\}$ элементов, $a \neq b$, лежит в единственно определённой когиперплоскости. Поскольку матроид $M$ является разделяющим, существуют когиперплоскости $H_a$ и $H_b$, такие, что $a$ принадлежит $H_a$, но не принадлежит $H_b$, и $b$ принадлежит $H_b$, но не принадлежит $H_a$. Пусть элемент $c$ принадлежит $H_a$, но $a \neq c$. Тогда из того, что матроид $M$ является разделяющим, вытекает, что существуют когиперплоскости $H_c$ и $H$, такие, что $c$ принадлежит $H_c$, но не принадлежит $H$, и $a$ принадлежит $H$, но не принадлежит $H_c$. Отсюда $H \neq H_a$, так что элемент $a$ принадлежит не менее чем двум различным когиперплоскостям. Если и $b$ принадлежит $H$, то всё доказано. Если же нет, то, поскольку $b$ не принадлежит ни когиперплоскости $H$, ни когиперплоскости $H_a$, причём $H \neq H_a$, по второй аксиоме гиперплоскостей должна существовать когиперплоскость, содержащая $b$ и пересечение $H \cap H_a = \{a\}$, что и требовалось доказать.

Покажем, что семейство когиперплоскостей рассматриваемого матроида есть блок-схема $D(v, b, r, k, \lambda)$ с набором параметров, соответствующих системе троек Штейнера.

Из трёхэлементности когиперплоскостей следует, что $k = 3$. Из того, что каждая пара элементов лежит в единственной когиперплоскости, следует, что $\lambda = 1$. Из предположения однородности матроида следует, что $v = |E| = n + 3$, и так как каждая пара определяет единственным образом тройку, а в тройке таких пар три, получаем $b = (v(v - 1)/2)/3 = v(v - 1)/6$. Поскольку пересекающиеся когиперплоскости имеют одноэлементное пересечение, для каждого элемента $e$ множество $E \setminus \{e\}$ разбивается на двухэлементные подмножества когиперплоскостями, проходящими через $e$, поэтому $r = (v - 1)/2$.

Таким образом, доказано

**Утверждение 1.** Разделяющий матроид является однородным матроидом с трёхэлементными когиперплоскостями тогда и только тогда, когда его когиперплоскости образуют систему троек Штейнера, т. е. $k = 3$ и $\lambda = 1$.

Итак, в работе показана связь однородных матроидов с тройками Штейнера. Описанный метод может быть применён к решению более сложных задач обобщения связи матроидов с блок-схемами с $\lambda = 1$, согласно выдвинутой ранее гипотезе.

ЛИТЕРАТУРА


1. Введение в криптографию / под общ. ред. В. В. Ященко. СПб.: Питер, 2001.
2. *Блейкли Г. Р., Кабатянский Г. А.* Обобщенные идеальные схемы, разделяющие секрет, и матроиды // Проблемы передачи информации. 1997. Т. 33. № 3. С. 102–110.
3. *Парватов Н. Г.* Совершенные схемы разделения секрета // Прикладная дискретная математика. 2008. №2 (2). С. 50–57.
4. *Welsh D. J. A.* Matroid Theory. Academic Press, 1976.
5. *Marti-Farre J. and Padro C.* Secret sharing schemes on sparse homogeneous access structures with rank three // Electronic J. Combinatorics. 2004. No. 1 (1). Research Paper 72. 16 p.
6. *Алексейчук А. Н.* Совершенные схемы разделения секрета и конечные универсальные алгебры // Реєстрація, зберігання і оброб. даних. 2005. Т. 7. № 2. С. 55–65.
7. *Alekseychuk A. N.* Lattice-Theoretic Characterization of Secret Sharing Representable Connected Matroids. Cryptology ePrint Archive: Report 2010/348.
8. *Холл М.* Комбинаторика. М.: Мир, 1970.
9. *Медведев Н. В., Титов С. С.* Об однородных матроидах и блок-схемах // Прикладная дискретная математика. Приложение. 2017. № 10. С. 21–23.


УДК 512.64, 519.21, 519.72 DOI 10.17223/2226308X/12/35

## ГЕОМЕТРИЧЕСКАЯ МОДЕЛЬ СОВЕРШЕННЫХ ШИФРОВ С ТРЕМЯ ШИФРВЕЛИЧИНАМИ

Н. В. Медведева, С. С. Титов

Рассматривается проблема описания совершенных по Шеннону (абсолютно стойких к атаке по шифртексту) шифров с мощностью шифрвеличин равной трём. Показано, что не существует минимальных по включению совершенных шифров с четырьмя шифробозначениями и пятью или шестью ключами зашифрования. Определено количество минимальных по включению совершенных шифров, содержащих семь ключей зашифрования, а также количество совершенных шифров с числом ключей равным восьми. Построены примеры минимальных по включению совершенных шифров.

**Ключевые слова:** *совершенные шифры, эндоморфные шифры, неэндоморфные шифры.*

Рассмотрим вероятностную модель $\Sigma_B$ шифра [1 – 3]. Пусть $X, Y$ — конечные множества соответственно шифрвеличин и шифробозначений, с которыми оперирует некоторый шифр замены; $K$ — множество ключей, причём $|X| = \lambda$, $|Y| = \mu$, $|K| = \pi$, где $\lambda > 1$, $\mu \geqslant \lambda$. Это означает, что открытые и шифрованные тексты представляются словами ($\ell$-граммами, $\ell \geqslant 1$) в алфавитах $X$ и $Y$ соответственно. Согласно [2, 3], под *шифром* $\Sigma_B$ будем понимать совокупность множеств правил зашифрования и правил

расшифрования с заданными распределениями вероятностей на множествах открытых текстов и ключей. Шифры, для которых апостериорные вероятности открытых текстов совпадают с их априорными вероятностями, называются *совершенными*. В работе [1] полностью описаны *эндоморфные* ($X = Y$) совершенные шифры с минимально возможным числом ключей ($|K| = |Y|$). Согласно теореме К. Шеннона [1], эндоморфные совершенные шифры с минимально возможным числом ключей исчерпываются шифрами табличного гаммирования со случайной равновероятной гаммой.

Данная работа является продолжением исследования [4] проблемы описания совершенных по Шеннону шифров. Здесь для обобщений теоремы Шеннона и построения примеров используется вероятностная модель $\Sigma_B$ шифра, в которой, согласно подходу [2, 3], шифр задаётся распределением вероятностей ключей при $\ell = 1$.

Для эндоморфного ($X = Y$) и неэндоморфного ($|X| < |Y|$) шифров перечисляются в некотором порядке все возможные $\pi_{\max} = \mu(\mu - 1) \cdot \ldots \cdot (\mu - \lambda + 1)$ инъекций зашифрования, соответствующие ключам $k \in K$ и их вероятностям $\mathsf{P}_k$. При этом допускается, что некоторые вероятности $\mathsf{P}_k$ могут быть равны нулю. Это означает, что соответствующая инъекция не используется в данном шифре. Получившийся $\pi_{\max}$-мерный набор $\mathsf{P}$ вероятностей $\mathsf{P}_k$ ключей будем рассматривать как точку $\pi_{\max}$-мерного пространства $\mathbb{R}^{\pi_{\max}}$. Распределение биграмм, триграмм и т. д. может задаваться распределениями вероятностей при $\ell = 2, 3, \ldots$, что приводит к усложнению геометрической модели.

Задача описания шифров в вероятностной модели $\Sigma_B$ приводит к описанию множества точек в пространстве $\mathbb{R}^{\pi_{\max}}$, которые являются распределениями вероятностей ключей того или иного шифра.

По теореме Шеннона, минимальные по числу ключей эндоморфные совершенные шифры соответствуют тем точкам пространства $\mathbb{R}^{\pi_{\max}}$, у которых все координаты равны нулю, кроме $\lambda$ ненулевых координат, равных $1/\lambda$, а сам набор координат соответствует набору ключей (инъекций), образующих латинский квадрат. Поскольку множество точек пространства $\mathbb{R}^{\pi_{\max}}$, соответствующих совершенным шифрам, образует выпуклое множество (полиэдр [5]), то и выпуклая оболочка этих точек также соответствует совершенным шифрам. Однако могут быть совершенные шифры, соответствующие точкам вне этой выпуклой оболочки.

В работе [4] показано, что в случае, когда мощность алфавита шифрвеличин равна двум, множество возможных значений априорных вероятностей шифробозначений $p_s = \mathsf{P}\{y = y_s\} = \mathsf{P}\{y = s\}$, где $s = 1, \ldots, \mu$, допускает описание на основе теоремы Биркгофа о классификации дважды стохастических матриц [6]. В [4] описано выпуклое множество (полиэдр) матриц вероятностей ключей и множество вероятностей шифробозначений неэндоморфных совершенных шифров в случае, когда мощность множества шифрвеличин равна двум. Полиэдр описан через указание его вершин (экстремальных точек), которые представляют собой так называемые нормальные циклы.

В [7] в терминах комбинаторного анализа выпуклых множеств многомерного пространства сформулированы и доказаны некоторые обобщения (аналоги) теоремы Шеннона для совершенных по Шеннону эндоморфных неминимальных ($|K| > |Y|$) шифров. В частности, показано, что для любого эндоморфного совершенного шифра с мощностью множества шифрвеличин $\lambda = \mu = 3$ искомый полиэдр — это отрезок в шестимерном пространстве. Построены примеры, показывающие, что минимальность шифра по числу ключей и минимальность по включению (т. е. шифры, содержащие минимально возможное множество ключей зашифрования с ненулевыми вероятностями) приводят к разным постановкам задач обобщения теоремы Шеннона. Неэндоморф-

ные совершенные шифры с $\lambda = 3$ и $\mu = 4$ дополняются до эндоморфных, и притом единственным образом.

**Утверждение 1.** При $\pi = 5$ или 6 не существует минимальных по включению совершенных шифров.

**Утверждение 2.** При $\pi = 7$ существует $4! = 24$ минимальных по включению совершенных шифров.

Все такие шифры получены перестановкой столбцов в таблице зашифрования эндоморфного совершенного шифра, составленной из единичной подстановки и всех шести полноцикловых подстановок группы $S_4$ [7] (табл. 1).

**Утверждение 3.** При $\pi = 8$ существует $4 \cdot 4! = 96$ минимальных по включению совершенных шифров.

Рассмотрим восемь подстановок (табл. 2), где $\{a, b, c, d\} = \{1, 2, 3, 4\}$. Данное множество подстановок не содержит латинских квадратов. Перестановкой столбцов и переименованием элементов $a, b, c, d$ снова получаются восемь подстановок ключей с вероятностями 1/8.

Таблица 1

| № | $K$ | $x_1$ | $x_2$ | $x_3$ | $x_4$ | $\mathsf{P}_k$ |
|---|---|---|---|---|---|---|
| 1 | $k_1$ | 1 | 2 | 3 | 4 | 1/4 |
| 2 | $k_2$ | 2 | 4 | 1 | 3 | 1/8 |
| 3 | $k_3$ | 3 | 1 | 4 | 2 | 1/8 |
| 4 | $k_4$ | 4 | 3 | 1 | 2 | 1/8 |
| 5 | $k_5$ | 3 | 4 | 2 | 1 | 1/8 |
| 6 | $k_6$ | 2 | 3 | 4 | 1 | 1/8 |
| 7 | $k_7$ | 4 | 1 | 2 | 3 | 1/8 |

Таблица 2

| № | $K$ | $x_1$ | $x_2$ | $x_3$ | $x_4$ | $\mathsf{P}_k$ |
|---|---|---|---|---|---|---|
| 1 | $k_1$ | $a$ | $d$ | $b$ | $c$ | 1/8 |
| 2 | $k_2$ | $a$ | $d$ | $c$ | $b$ | 1/8 |
| 3 | $k_3$ | $b$ | $c$ | $d$ | $a$ | 1/8 |
| 4 | $k_4$ | $b$ | $a$ | $d$ | $c$ | 1/8 |
| 5 | $k_5$ | $c$ | $a$ | $b$ | $d$ | 1/8 |
| 6 | $k_6$ | $c$ | $b$ | $a$ | $d$ | 1/8 |
| 7 | $k_7$ | $d$ | $b$ | $c$ | $a$ | 1/8 |
| 8 | $k_8$ | $d$ | $c$ | $a$ | $b$ | 1/8 |

В случае равновероятных шифробозначений совершенный шифр с мощностью множества шифрвеличин, равной трём, и $\mu > 4$ может быть дополнен до эндоморфного, но не едиственным способом.

**Пример 1.** Рассмотрим неэндоморфный шифр с множеством из трёх шифрвеличин. Пусть $X = \{x_1, x_2, x_3\} = \{1, 2, 3\}$ — множество шифрвеличин; $Y = \{y_1, y_2, y_3, y_4, y_5\} = \{1, 2, 3, 4, 5\}$ — множество шифробозначений; $K = \{k_1, k_2, \ldots, k_\pi\}$ — множество ключей. Таблица зашифрования данного шифра (табл. 3) не содержит латинских прямоугольников размера $5 \times 3$.

Таблица 3

| № | $K$ | $x_1$ | $x_2$ | $x_3$ | $\mathsf{P}_k$ |
|---|---|---|---|---|---|
| 1 | $k_1$ | 1 | 2 | 3 | 1/5 |
| 2 | $k_2$ | 2 | 3 | 4 | 1/10 |
| 3 | $k_3$ | 2 | 1 | 5 | 1/10 |
| 4 | $k_4$ | 3 | 4 | 5 | 1/10 |
| 5 | $k_5$ | 3 | 5 | 1 | 1/10 |
| 6 | $k_6$ | 4 | 5 | 2 | 1/10 |
| 7 | $k_7$ | 4 | 3 | 1 | 1/10 |
| 8 | $k_8$ | 5 | 1 | 4 | 1/10 |
| 9 | $k_9$ | 5 | 4 | 2 | 1/10 |

Это совершенный эндоморфный шифр, дополняемый двумя способами (при фиксировании первой строки) до эндоморфного совершенного шифра с $\lambda = \mu = 5$ без латинских квадратов (табл. 4 и 5).

Таблица 4

| № | $K$ | $x_1$ | $x_2$ | $x_3$ | $x_4$ | $x_5$ | $\mathsf{P}_k$ |
|---|---|---|---|---|---|---|---|
| 1 | $k_1$ | 1 | 2 | 3 | 4 | 5 | 1/5 |
| 2 | $k_2$ | 2 | 3 | 4 | 5 | 1 | 1/10 |
| 3 | $k_3$ | 2 | 1 | 5 | 3 | 4 | 1/10 |
| 4 | $k_4$ | 3 | 4 | 5 | 1 | 2 | 1/10 |
| 5 | $k_5$ | 3 | 5 | 1 | 2 | 4 | 1/10 |
| 6 | $k_6$ | 4 | 5 | 2 | 1 | 3 | 1/10 |
| 7 | $k_7$ | 4 | 3 | 1 | 5 | 2 | 1/10 |
| 8 | $k_8$ | 5 | 1 | 4 | 2 | 3 | 1/10 |
| 9 | $k_9$ | 5 | 4 | 2 | 3 | 1 | 1/10 |

Таблица 5

| № | $K$ | $x_1$ | $x_2$ | $x_3$ | $x_4$ | $x_5$ | $\mathsf{P}_k$ |
|---|---|---|---|---|---|---|---|
| 1 | $k_1$ | 1 | 2 | 3 | 4 | 5 | 1/5 |
| 2 | $k_2$ | 2 | 3 | 4 | 5 | 1 | 1/10 |
| 3 | $k_3$ | 2 | 1 | 5 | 3 | 4 | 1/10 |
| 4 | $k_4$ | 3 | 4 | 5 | 1 | 2 | 1/10 |
| 5 | $k_5$ | 3 | 5 | 1 | 2 | 4 | 1/10 |
| 6 | $k_6$ | 4 | 5 | 2 | 3 | 1 | 1/10 |
| 7 | $k_7$ | 4 | 3 | 1 | 5 | 2 | 1/10 |
| 8 | $k_8$ | 5 | 1 | 4 | 3 | 2 | 1/10 |
| 9 | $k_9$ | 5 | 4 | 2 | 1 | 3 | 1/10 |

Таким образом, в работе рассмотрена задача построения геометрической модели совершенных по Шеннону шифров с мощностью множества шифрвеличин равной трём. Показано, что не существует минимальных по включению совершенных шифров с четырьмя шифробозначениями и пятью или шестью ключами зашифрования. Определено количество минимальных по включению совершенных шифров, содержащих семь ключей зашифрования, а также количество совершенных шифров с числом ключей равным восьми. Построены примеры минимальных по включению совершенных шифров.

## ЛИТЕРАТУРА


1. *Шеннон К.* Теория связи в секретных системах // Работы по теории информации и кибернетике. М.: Наука, 1963. С. 333–402.
2. *Алферов А. П., Зубов А. Ю., Кузьмин А. С., Черемушкин А. В.* Основы криптографии. М.: Гелиос АРВ, 2001.
3. *Зубов А. Ю.* Совершенные шифры. М.: Гелиос АРВ, 2003.
4. *Медведева Н. В., Титов С. С.* Описание неэндоморфных максимальных совершенных шифров с двумя шифрвеличинами // Прикладная дискретная математика. 2015. № 4 (30). С. 43–55.
5. *Носов В. А., Сачков В. Н., Тараканов В. Е.* Комбинаторный анализ (неотрицательные матрицы, алгоритмические проблемы) // Итоги науки и техн. Сер. Теор. вероятн. Мат. стат. Теор. Кибернет. Т. 21. М.: ВИНИТИ, 1977. С. 120–178.
6. *Birkhoff G. D.* Tres observations sobre el algebra lineal // Revista Universidad Nacional Tucuman. 1946. Ser. A. V. 5. P. 147–151.
7. *Медведева Н. В., Титов С. С.* Аналоги теоремы Шеннона для эндоморфных неминимальных шифров // Прикладная дискретная математика. Приложение. 2016. № 9. С. 62–65.

УДК 003.26 DOI 10.17223/2226308X/12/36

# ЭФФЕКТИВНЫЕ МЕТОДЫ АЛГЕБРАИЧЕСКОГО КРИПТОАНАЛИЗА И ЗАЩИТА ОТ НИХ[1]

В. А. Романьков

Работа состоит из двух частей. В первой части даётся представление авторских методов криптографического анализа алгоритмов алгебраической криптографии. Описываются основные элементы метода линейного разложения. Приводятся примеры его использования для эффективных атак на известные алгоритмы. Даётся представление об альтернативном подходе Б. Тсабана, также базирующемся на линейной алгебре и некоторых теоретико-вероятностных результатах. Кроме этого, приводится описание основных элементов метода нелинейного разложения с соответствующими примерами его применения. Вторая часть посвящена построению эффективных методов защиты от атак, использующих средства линейной алгебры. Для этого вводится новое понятие маргинального множества элементов группы относительно данного слова от порождающих элементов. Показывается, как использование маргинальных множеств позволяет уходить от проблемы нахождения сопрягающего элемента, лежащей в основе многих алгоритмов алгебраической криптографии, к значительно более сложной проблеме вхождения-сопряжённости.

**Ключевые слова:** *алгебраическая криптография, алгебраический криптоанализ.*

## 1. Методы криптоанализа алгебраической криптографии

### 1.1. Метод линейного разложения

Метод введён в рассмотрение автором в [1, 2], получил дальнейшее развитие в [3 – 5] и ряде других публикаций, подробно освещён в монографии [6]. Метод детерминированный и доказуемый, применим как к конечным, так и к бесконечным объектам. Его отличительной особенностью является то, что построенный по этому методу алгоритм криптографического анализа находит распределяемый ключ или передаваемое сообщение, не вычисляя секретных параметров, использованных при зашифровании. Алгоритм не решает алгоритмической проблемы, лежащей в основе криптографических построений, обходя тем самым построенную авторами защиту и не преодолевая трудностей, заложенных при построении криптографической схемы.

Метод использован для криптографического анализа криптографических алгоритмов Маркова — Михалева и др., Грибова — Золотых и др., Росошека, Харли, Мегрелишвили, Шпильрайна — Ушакова, Кахроби — Шпильрайна и др., Ко — Ли и др., Ванга и др., Курта, Хехта и ряда других авторов.

Метод работает в тех случаях, когда платформа шифрования $G$ является частью линейного пространства $V$, например группой матриц над некоторым конструктивным полем $\mathbb{F}$ (конечным или бесконечным), рассматриваемой как подмножество линейного пространства $\mathrm{M}(n, \mathbb{F})$ матриц размера $n \times n$. Типичными элементами метода являются: построение базиса линейного подпространства, порождённого подмножеством из $G$ определённого вида в пространстве $V$; использование свойств этого подпространства для определения секрета.

[1]Работа поддержана грантом РФФИ, проект № 18-41-550001а.

В криптографии с открытым ключом хорошо известна *проблема Диффи — Хеллмана*: для группы $G$ и её элемента $g \in G$ определить по двум значениям $g^k$ и $g^l$, где $k, l$ — натуральные числа, значение $g^{kl}$.

В алгебраической криптографии рассматриваются следующие её некоммутативные аналоги:

— Аналог с сопряжениями: для группы $G$ и её элемента $g \in G$ определить по двум сопряжённым к $g$ элементам $g^a = aga^{-1}$ и $g^b = bgb^{-1}$, где $a, b \in G$, $ab = ba$, элемент $g^{ab} = abga^{-1}b^{-1} = bagb^{-1}a^{-1}$.

— Аналог с двусторонними домножениями: для группы $G$ и её элемента $g \in G$ определить по двум элементам вида $aga'$ и $bgb'$, где $a, b \in G$, $ab = ba$, $a'b' = b'a'$, элемент $abga'b' = bagb'a'$.

— Аналог с автоморфизмами: для группы $G$ и её элемента $g \in G$ определить по двум элементам вида $\alpha(g)$ и $\beta(g)$, где $\alpha, \beta \in \mathrm{Aut}(G)$, $\alpha\beta = \beta\alpha$, элемент $\alpha(\beta(g)) = \beta(\alpha(g))$.

Метод линейного разложения при некоторых естественных условиях на группу $G$ (прежде всего это существование эффективного вложения в конечномерное линейное пространство) эффективно решает каждую из этих проблем.

### 1.2. Span-метод Б. Тсабана

В [7] (см. также [8]) Б. Тсабан и др. ввели в рассмотрение полиномиальный по времени вероятностный метод алгебраического криптоанализа, названный ими *линейным span-методом*. Метод позволяет разрабатывать способы эффективного решения вычислительных проблем в группах матриц над конечными полями, значит, и в группах, допускающих эффективные представления матрицами над конечными полями. Метод улучшает более ранние методы, описанные в [9, 10].

Как и в методе линейного разложения, span-метод предполагает построение базисов некоторых линейных подпространств, определяемых матричной группой $G$ над конечным полем $\mathbb{F}_q$ порядка $q$.

Приведём типичный пример использования метода. Допустим, нужно решить проблему поиска сопрягающего элемента $X$ для данных матриц $A$ и $B = XAX^{-1}$ из группы $\mathrm{GL}(n, \mathbb{F}_q)$. Данное уравнение заменяется на систему линейных однородных уравнений, соответствующую матричному уравнению $XA = BX$. Строится базис $E = \{e_1, \ldots, e_s\}$ пространства решений и записывается общее решение $X = \sum\limits_{i=1}^{s} \alpha_i e_i$. Теперь нужно, варьируя коэффициенты $\alpha_i$, $i = 1, \ldots, s$, найти среди решений невырожденную матрицу $X$. Нам известно, что невырожденное решение существует. Тогда можно воспользоваться следующей леммой.

**Лемма 1** (лемма обратимости [7, Lemma 9]). Пусть элементы $e_1, \ldots, e_s$ кольца матриц $\mathrm{M}(n, \mathbb{F}_q)$ таковы, что некоторая их линейная комбинация $\sum\limits_{i=1}^{s} \alpha_i e_i$ с коэффициентами из $\mathbb{F}_q$ является обратимой матрицей. Если коэффициенты выбираются в соответствии с равномерным распределением на $\mathbb{F}_q$, то вероятность получения невырожденного решения будет не меньше чем $p = 1 - n/q$.

Метод эффективен, если $n$ существенно мало по отношению к $q$.

### 1.3. Метод нелинейного разложения

Данный метод введён автором в [11] как дополнение к методу линейного разложения. Он работает в тех случаях, когда группа не допускает представления матрицами или это представление имеет слишком большой размер для возможного использования. Конечно, здесь также предполагается выполнение ряда условий, связанных

с разрешимостью проблемы вхождения в конечно порождённые подгруппы группы, выбранной в качестве платформы для криптографической схемы. Эти условия, как правило, выполняются в конечно порождённых нильпотентных и полициклических группах, часто предлагаемых для такого применения в последние годы. Относительно соответствующей теории см. [6], приложения можно найти в [4, 5, 12].

Метод нелинейного разложения при некоторых естественных предположениях о группе $G$ (прежде всего, они касаются эффективной разрешимости проблемы представления элемента конечно порождённой подгруппы в виде слова от её порождающих элементов) эффективно решает перечисленные выше три проблемы, аналогичные проблеме Диффи — Хеллмана.

### 1.4. Примеры использования методов линейного и нелинейного разложения

Рассмотрим общую схему, под которую подпадает большое число алгоритмов, использующих двусторонние домножения. Далее приведены два примера конкретных протоколов, показывающие широкую применимость методов линейного и нелинейного разложения для построения алгоритмов криптографического анализа.

**Общая схема алгоритмов, использующих двусторонние домножения**

Данный раздел основан на работе автора [13]. Большинство известных схем алгебраической криптографии, использующих двусторонние домножения, являются частными случаями одной общей схемы (см. описание ниже). Часто такие схемы строятся на группах, являющихся подгруппами линейных пространств, например на матричных группах. Метод линейного разложения позволяет эффективно вычислять в данном случае распределяемый ключ или передаваемое сообщение без вычисления секретных параметров [1 – 4, 14 – 17]. Далее описаны некоторые основные элементы такого вычисления и приведены примеры его использования.

Некоторые такие схемы предложены М. Андрекутом [18], Л. Гу и др. [19, 20], Б. и Т. Харли [21, 22], В. Шпильрайном и А. Ушаковым [23], Е. Стикелем [24], Х. Вангом и др. [25]. Ряд схем описан в [26, 27]. Схемы, использующие сопряжения, например известная схема Ко — Ли и др. [28], рассматриваемая как некоммутативный аналог классической схемы Диффи — Хеллмана [29], также могут анализироваться указанным способом.

Пусть $G$ — группа, выбранная в качестве платформы для схемы распределения ключа. Предположим, что $G$ — подмножество конечномерного линейного пространства $V$. Два корреспондента, Алиса и Боб, соглашаются относительно элемента $h \in G$ и двух конечно порождённых подгрупп $A$ и $B$ группы $G$, заданных конечными множествами порождающих элементов. Предположим, что любой элемент $a \in A$ перестановочен с любым элементом $b \in B$. Все эти данные открыты.

Корреспонденты, начиная с $h$, попеременно публикуют элементы вида $\varphi_{a,a'}(u) = aua'$, где $a, a' \in A$ (Алиса), и $\varphi_{b,b'}(u) = bub'$, где $b, b' \in B$ (Боб), а $u$ равен $h$ или совпадает с одним из ранее построенных элементов. Алиса, как и Боб, может публиковать сразу несколько элементов. Распределённый ключ имеет вид

$$K = \varphi_{c_l,c'_l}(\varphi_{c_{l-1},c'_{l-1}}(\dots(\varphi_{c_1,c'_1}(g)))) = c_l c_{l-1} \dots c_1 g c'_1 \dots c'_{l-1} c'_l,$$

где каждая пара $(c_t, c'_t)$ совпадает либо с парой вида $(a, a')$, $a, a' \in A$, либо с парой вида $(b, b')$, $b, b' \in B$.

**Криптоанализ общей схемы**

Следующая лемма говорит о возможности эффективного построения базиса линейного подпространства пространства $V$, порожденного элементами группы $G$ определённого вида. Различные версии этой леммы доказаны в [1–4, 13], см. также [6].

**Лемма 2.** Пусть $A$ — конечно порождённая подгруппа группы $G$, являющейся подмножеством конечномерного пространства $V$ над полем $\mathbb{F}$, и $h$ — фиксированный элемент из $G$. Предположим, что все основные операции в $V$, то есть сложение и умножение на скаляр, эффективно вычислимы. В этом случае эффективно строится базис $E = \{e_1, \ldots, e_s\}$ любого линейного подпространства $\mathrm{Lin}(AhA)$, порождённого всеми элементами вида $aha'$, где $a, a' \in A$.

Следующая лемма является ключевым утверждением для алгебраического криптоанализа схем с двусторонними домножениями. Предполагается выполнение условий, данных выше.

**Лемма 3.** Пусть $v = \varphi_{a,a'}(u)$, где $a, a' \in A$ — закрытые параметры Алисы. Тогда для любого элемента $w = \varphi_{b,b'}(u)$, где $b, b' \in B$ (другими словами, $w \in BuB$), эффективно строится элемент $z = \varphi_{a,a'}(w)$. Построение этого элемента основывается на структуре линейного пространства $V$.

**Пример 1.** Рассмотрим протокол Ванга и др. из [25]. В нём корреспонденты выбирают в качестве платформы одну из групп $B_n$ кос Артина. В 1990 г. Р. Лоуренс описала семейство представлений групп $B_n$ матрицами. Примерно через 10 лет С. Бигелоу [30] и Д. Краммер [31] независимо доказали линейность групп $B_n$. В частности, было установлено, что представления Лоуренс $\rho_n : B_n \to \mathrm{GL}_{n(n-1)/2}(\mathbb{Z}[t^{\pm 1}, s^{\pm 1}])$ являются вложениями для любого $n \in \mathbb{N}$. Они стали называться представлениями *Лоуренс — Краммера*. Образ $\rho_n(g)$ эффективно строится по любому $g \in B_n$. Более того, существует эффективная процедура восстановления косы $g \in B_n$ по её образу $\rho_n(g)$. В [9] показано, что это может быть сделано за $\mathrm{O}(2m^3 \log d_t)$ умножений элементов матриц $\rho_n(g)$. Здесь $m = n(n-1)/2$ и $d_t$ — параметр, эффективно вычислимый по $\rho_n(g)$ (см. [9] относительно деталей).

Таким образом, можно предположить, что $G$ является частью линейного пространства $V$.

Перейдём к описанию протокола. Алиса и Боб выбирают группу $G$ и случайный элемент $h \in G$. Также они выбирают две конечно порождённые подгруппы $A$ и $B$ группы $G$, такие, что $ab = ba$ для любой пары элементов $a \in A$ и $b \in B$. Эти данные открыты.

*Алгоритм.*

1) Алиса выбирает элементы $c_1, c_2, d_1, d_2 \in A$, вычисляет и публикует $x = d_1 c_1 h c_2 d_2$ для Боба.
2) Боб выбирает элементы $f_1, f_2, g_1, g_2, g_3, g_4 \in B$, вычисляет и публикует $y = g_1 f_1 h f_2 g_2$ и $w = g_3 f_1 x f_2 g_4$ для Алисы.
3) Алиса выбирает элементы $d_3, d_4 \in A$, вычисляет и публикует $z = d_3 c_1 y c_2 d_4$ и $u = d_1^{-1} w d_2^{-1}$ для Боба.
4) Боб вычисляет и публикует $v = g_1^{-1} z g_2^{-1}$ для Алисы.
5) Алиса вычисляет распределённый ключ $K_A = d_3^{-1} v d_4^{-1} = c_1 f_1 h f_2 c_2$.
6) Боб вычисляет распределённый ключ $K_B = g_3^{-1} u g_4^{-1} = c_1 f_1 h f_2 c_2$ равный $K_A$.
7) Распределённый ключ: $K = K_A = K_B$.

*Криптоанализ.*

Протокол использует следующие преобразования:

$$\varphi_{d_1c_1,c_2d_2},\ \varphi_{g_1f_1,f_2g_2},\ \varphi_{g_3f_1,f_2g_4},\ \varphi_{d_3c_1,c_2d_4},\ \varphi^{-1}_{d_1,d_2},\ \varphi^{-1}_{g_1,g_2}.$$

Прямым вычислением получаем выражение $K$:

$$K = \varphi_{c_1f_1,f_2c_2}(h) = \varphi^{-1}_{d_1,d_2}(\varphi_{d_1c_1,c_2d_2}(\varphi^{-1}_{g_1,g_2}(\varphi_{g_1f_1,f_2g_2}(h)))).$$

Покажем, что ключ $K$ эффективно вычислим по леммам 2 и 3.
Выход первого преобразования $y = \varphi_{g_1f_1,f_2g_2}(h)$ открыт.
Выход второго преобразования $\varphi^{-1}_{g_1,g_2}(y)$ эффективно вычислим:

$$v = \varphi^{-1}_{g_1,g_2}(z)\ \&\ y \in AzA \Rightarrow\ \varphi^{-1}_{g_1,g_2}(y) = f_1hf_2.$$

Выход третьего преобразования эффективно вычислим:

$$x = \varphi_{d_1c_1,c_2d_2}(h)\ \&\ f_1hf_2 \in BhB \Rightarrow\ \varphi_{d_1c_1,c_2d_2}(f_1hf_2) = d_1c_1f_1hf_2c_2d_2.$$

Выход четвёртого преобразования эффективно вычислим:

$$u = \varphi^{-1}_{d_1,d_2}(w)\ \&\ d_1c_1f_1hf_2c_2d_2 \in BwB \Rightarrow\ \varphi^{-1}_{d_1,d_2}(d_1c_1f_1hf_2c_2d_2) = c_1f_1hf_2c_2 = K.$$

Таким образом вычислен $K$.

**Пример 2.** Следующий протокол Махалонобиса [32] можно рассматривать как некоммутативный аналог классического протокола Масси — Омуры. Естественно предположить, что в группе $G$ эффективно выполнимы основные операции умножения и взятие обратного, а также что эффективно задаются автоморфизмы группы $G$, для которых эффективно вычисляются обратные элементы. Также необходимо считать, что в группе эффективно разрешима проблема равенства.

Алиса и Боб выбирают группу $G$ и конечно порождённую абелеву подгруппу $S$ её группы автоморфизмов $\mathrm{Aut}(G)$.

*Алгоритм.*

1) Алиса выбирает (случайным образом) автоморфизм $\alpha \in S$, вычисляет и публикует элемент $\alpha(h)$ для Боба.
2) Боб выбирает случайным образом автоморфизм $\beta \in S$, вычисляет и публикует элемент $\beta(\alpha(h))$ для Алисы.
3) Алиса вычисляет элемент $\alpha^{-1}(\beta(\alpha(h))) = \beta(h)$, затем выбирает случайным образом автоморфизм $\gamma \in S$, вычисляет и публикует элемент $\gamma(\beta(h))$ для Боба.
4) Боб вычисляет элемент $\beta^{-1}(\gamma(\beta(h))) = \gamma(h)$, являющийся переданным ему ключом.

*Криптоанализ.*

Предположим, что можно эффективно выбрать из элементов вида $s(f)$, $s \in S$, где $f \in G$ — фиксированный элемент, конечное множество порождающих элементов $\{\lambda_i(f) : \lambda_i \in S,\ i = 1, \ldots, k\}$ подгруппы $Sf = \mathrm{gp}(sf : s \in S)$, а также эффективно записать через эти порождающие элементы любой элемент группы $Sf$.

Пусть $f = \beta(\alpha(h))$. Тогда можно найти выражение открытого элемента $\gamma(\beta(h)) = \beta(\gamma(h))$ в виде значения некоторого слова $u(\lambda_1(f), \ldots, \lambda_k(f))$. Вынося за значение слова $u$ автоморфизм $\beta$ и сокращая на него обе части, получим требуемое значение $\gamma(h) = u(\lambda_1(\alpha(h)), \ldots, \lambda_k(\alpha(h))$. Значит, это значение можно вычислить по слову $u$, автоморфизмам $\lambda_i$, $i = 1, \ldots, k$, и открытому элементу $\alpha(h)$.

## 2. Способы защиты от атак, использующих линейную алгебру

Данный раздел основан на работе автора [33]. Далее введено понятие множества маргинальных наборов, соответствующих выражению и значению группового слова $w$ в группе $G$, существенно обобщающему понятие маргинальной подгруппы $w^*(G)$, определяемой $w$ в $G$. На основе этого понятия вводится новая улучшенная версия знаменитого AAG-протокола Аншель — Аншеля — Гольдфельда [34]. Улучшенная версия, в отличие от оригинальной, оказывается защищённой относительно span-метода. Она основана на смешанной проблеме вхождения-сопряжённости, в то время как оригинальная версия базируется на трудной разрешимости проблемы поиска сопрягающего элемента.

Дадим краткое описание оригинальной версии AAG -протокола. Рассматривается группа $G$, для которой фиксируются открытые наборы элементов $\bar{a} = (a_1, \ldots, a_k)$ и $\bar{b} = (b_1, \ldots, b_l)$. Алиса выбирает закрытый элемент $u \in \mathrm{gp}(a_1, \ldots, a_k)$ и публикует набор $\bar{b}^u = (b_1^u, \ldots, b_l^u)$. Боб выбирает закрытый элемент $v \in \mathrm{gp}(b_1, \ldots, b_l)$ и публикует набор $\bar{a}^v = (a_1^v, \ldots, a_k^v)$. Затем каждый из корреспондентов вычисляет элемент

$$u^{-1}u(a_1^v, \ldots, a_k^v) = v(b_1^u, \ldots, b_l^u)^{-1}v = [u, v],$$

являющийся распределённым ключом.

### 2.1. Маргинальные множества

**Определение 1.** Пусть $w = w(x_1, \ldots, x_n)$ обозначает групповое слово от $n$ переменных, $G$ — группа и $\bar{g} = (g_1, \ldots, g_n)$ — набор её элементов. Говорим, что набор $\bar{c} = (c_1, \ldots, c_n) \in G^n$ является *маргинальным набором*, определяемым $w$ и $\bar{g}$, если имеет место равенство

$$w(c_1 g_1, \ldots, c_n g_n) = w(g_1, \ldots, g_n).$$

Будем писать $\bar{c} \perp w(\bar{g})$ в этом случае. Множество $\bar{C} \subseteq G^n$ называется *маргинальным* по отношению к $w$ и $\bar{g}$ ($\bar{C} \perp w(\bar{g})$), если $\bar{c} \perp w(\bar{g})$ для любого набора $\bar{c} \in \bar{C}$.

В общем случае маргинальное множество $\bar{C}$, $\bar{C} \perp w$, не является подгруппой. Оно может быть выбрано как множество без всякой структуры, в случае бесконечной группы оно может быть выбрано нерекурсивным.

Дадим простой и эффективный способ построения маргинального множества $\bar{C}$ по слову $w$. Этот способ универсален, так как он не зависит от структуры группы $\bar{G}$.

Пусть $w = w(a_1, \ldots, a_k) = a_1 a_2 \ldots a_k$, $a_i \in G$, $i = 1, \ldots, k$, — выражение через произведение элементов произвольного слова $f \in G$, при этом допускаются равенства $a_i = a_j$ или $a_i = a_j^{-1}$ для $i \neq j$. Выражение не обязано быть редуцированным. Рассмотрим уравнение

$$x_1 a_1 x_2 a_2 \ldots x_k a_k = f. \tag{1}$$

Любое решение этого уравнения может быть включено в маргинальное множество $\bar{C}$, $\bar{C} \perp w$. Зафиксировав какое-то $i$ и выбрав произвольные значения $x_j = c_j$, $j \neq i$, $c_j \in G$, можно получить решение уравнения (1), полагая

$$x_i = a_{i-1}^{-1} c_{i-1}^{-1} \ldots a_1^{-1} c_1^{-1} f a_k^{-1} c_k^{-1} \ldots a_{i+1}^{-1} c_{i+1}^{-1}. \tag{2}$$

**Улучшенная версия AAG-протокола**

Предположим, что два корреспондента, Алиса и Боб, хотят распределить между собой ключ. Они выбирают открытую группу $G$, эффективно заданную порождающими элементами и определяющими соотношениями. Группа $G$ используется как платформа

для распределения ключа. Как обычно, предполагаем, что операции в группе вычисляются эффективно и что в группе $G$ эффективно разрешима проблема равенства.

Для распределения ключа корреспонденты действуют следующим образом.

Алиса выбирает натуральное число $k$ и набор элементов $\bar{a} = (a_1, \ldots, a_k)$. Эти данные открыты. Затем она выбирает секретное групповое слово $u = u(x_1, \ldots, x_k)$ и вычисляет его значение $u(\bar{a}) = u(a_1, \ldots, a_k)$ в группе $G$. Она строит также маргинальное множество $\bar{C} \subseteq G^k$, $\bar{C} \perp u(\bar{a})$. Боб фиксирует натуральное число $l$ и выбирает открытый набор элементов $\bar{b} = (b_1, \ldots, b_l)$. Затем он выбирает секретное слово $v = v(y_1, \ldots, y_l)$ и вычисляет его значение $v(\bar{b}) = v(b_1, \ldots, b_l)$ в группе $G$. Далее он строит открытое маргинальное множество $\bar{D} \subseteq G^l$, $\bar{D} \perp v(\bar{b})$. Всё это составляет установку системы для распределения секретного ключа между корреспондентами. Впрочем, она может быть измененена, как объясняется далее.

**Замечание 1.** Алиса публикует элементы $a_1, \ldots, a_k$ как $a_{\pi(1)}, \ldots, a_{\pi(k)}$, где $\pi \in \in \mathbb{S}_k$ — случайная подстановка. Та же самая подстановка применяется к элементам набора $\bar{c} \in \bar{C}$. Боб действует аналогичным образом.

*Виртуальные и скрытые элементы.* Алиса может ввести виртуальные элементы $h$, не задействованные в записи $u(\bar{a})$. Затем она может присоединить соответствующие виртуальные компоненты к $\bar{c} \in \bar{C}$, $\bar{C} \perp w$. Например, она может присоединить ряд виртуальных элементов и соответствующих компонент с целью скрыть длину слова $u$, или завуалировать уравнение (2), или выбрать элемент $h$ с большим централизатором, или, наоборот, с малым централизатором, чтобы сделать решение проблемы более затруднительным для потенциального взломщика систем. Боб действует аналогично.

Алиса может также скрыть некоторые элементы $a_i$ следующим образом. Пусть $a_i = a_j$ и соответствующие им компоненты любого из элементов маргинального множества равны между собой, то есть $c_i = c_j$ для всех $\bar{c} \in \bar{C}$. Тогда Алиса может не публиковать некоторые $a_j$, исключая соответствующие $j$-компоненты из $\bar{c}$. Необходимая информация восстанавливается очевидным образом. Боб может действовать аналогично.

Эти операции рекомендуются. После их выполнения параметры $k$ и $l$ заменяются на новые параметры $k'$ и $l'$.

*Алгоритм.*

1) Алиса выбирает набор $\bar{d} = (d_1, \ldots, d_{l'}) \in \bar{D}$ и вычисляет $\bar{d}\bar{b} = (d_1 b_1, \ldots, d_{l'} b_{l'})$. Затем она посылает набор $\bar{d}\bar{b}^{u(\bar{a})} = ((d_1 b_1)^{u(\bar{a})}, \ldots, (d_{l'} b_{l'})^{u(\bar{a})})$ Бобу.
2) Боб выбирает набор $\bar{c} = (c_1, \ldots, c_{k'}) \in \bar{C}$ и вычисляет $\bar{c}\bar{a} = (c_1 a_1, \ldots, c_k a_k)$. Затем он посылает набор $\bar{c}\bar{a}^{v(\bar{b})} = ((c_1 a_1)^{v(\bar{b})}, \ldots, (c_{k'} a_{k'})^{v(\bar{b})})$ Алисе.
3) Алиса, используя скрытые компоненты, вычисляет значение

$$u(\bar{a})^{-1} u((c_1 a_1)^{v(\bar{b})}, \ldots, (c_k a_k)^{v(\bar{b})} = u(\bar{a})^{-1} u(c_1 a_1, \ldots, c_k a_k)^{v(\bar{b})} = [u(\bar{a}), v(\bar{b})].$$

4) Боб аналогично вычисляет

$$v((d_1 b_1)^{u(\bar{a})}, \ldots, (d_l b_l)^{u(\bar{a})})^{-1} v(\bar{b}) = (v(d_1 b_1, \ldots, d_l b_l)^{u(\bar{a})})^{-1} v(\bar{b}) = [u(\bar{a}), v(\bar{b})].$$

Коммутатор $K = [u(\bar{a}), v(\bar{b})]$ является секретным распределённым ключом.

*Криптоанализ.*

**Определение 2.** *Проблема вхождения-сопряжённости* разрешима в $G$ по отношению к $\bar{C} \subseteq G^k$, если существует алгоритм, решающий для двух любых наборов

$\bar{a} = (a_1, \ldots, a_k)$ и $\bar{f} = (f_1, \ldots, f_k)$ элементов группы $G$, существует или нет элемент $y \in G$, такой, что $(f_1^y a_1^{-1}, \ldots, f_k^y a_k^{-1}) \in \bar{C}$. Короче говоря, существует ли $y \in G$, для которого $\bar{f}^y \bar{a}^{-1} \in \bar{C}$? Соответствующая проблема поиска — это вопрос о существовании алгоритма, находящего решение указанной проблемы, если такое решение существует.

Предложенная версия AAG-протокола основывается на трудной разрешимости поисковой проблемы вхождения-сопряжённости в случае, когда $\bar{C}$ — маргинальное множество, $\bar{C} \perp u(a_1, \ldots, a_k)$, для неизвестного слова $u(x_1, \ldots, x_n)$ (или аналогично, когда $\bar{D}$ — маргинальное множество, $\bar{D} \perp v(b_1, \ldots, b_l)$). В самом деле, предположим, что взломщик находит $\bar{c}' \in \bar{C}$ и $y \in G$, такие, что $\bar{c}\bar{a}^{v(\bar{b})} = \bar{c}'a^y$, и аналогично находит $\bar{d}' \in \bar{D}$ и $x \in G$, такие, что $\bar{d}\bar{b}^{u(\bar{a})} = \bar{d}'b^x$. Тогда он может вычислить распределяемый ключ $K = [x, y] = [u(\bar{a}), v(\bar{b})]$, как в оригинальной версии AAG.

Существуют также другие проблемы, которые следует решить перед тем, как пытаться взломать предложенный алгоритм. Присутствие виртуальных и скрытых элементов не позволяет вычислить длины слов $u$ и $v$. Заметим, что каждое решение уравнения (1) является решением уравнения вида $a_i a_{i+1} \ldots a_k a_1 \ldots a_{i-1} = f$, $i = 2, \ldots, k$, а также ряда других уравнений. Следовательно, открытые данные не позволяют определить $f^{v(\bar{b})}$, даже если взломщик знает длину $v$ и все буквы $v(\bar{b})$ вместе с их кратностью.

## ЛИТЕРАТУРА


1. *Романьков В. А.* Криптографический анализ некоторых схем шифрования, использующих автоморфизмы // Прикладная дискретная математика. 2013. № 3(21). С. 35–51.
2. *Романьков В. А.* Алгебраическая криптография. Омск: ОмГУ, 2013.
3. *Myasnikov A. and Roman'kov V.* A linear decomposition attack // Groups, Complexity, Cryptology. 2015. V. 7. P. 81–94.
4. *Романьков В. А., Обзор А. А.* Общая алгебраическая схема распределения криптографических ключей и её криптоанализ // Прикладная дискретная математика. 2017. № 37. С. 52–61.
5. *Романьков В. А., Обзор А А.* Метод нелинейного разложения для анализа криптографических схем, использующих автоморфизмы групп // Прикладная дискретная математика. 2018. № 41. С. 38–45.
6. *Roman'kov V. A.* Essays in Algebra and Cryptology. Algebraic Cryptanalysis. Omsk: OmSU, 2018.
7. *Tsaban B.* Polynomial-time solutions of computational problems in noncommutative-algebraic cryptography // J. Cryptology. 2015. V. 28. P. 601–622.
8. *Ben-Zvi A., Kalka A., and Tsaban B.* Cryptanalysis via algebraic spans // CRYPTO 2018. LNCS. 2018. V. 10991. P. 1–20.
9. *Cheon J. H. and Jun B.* A polynomial time algorithm for the braid Diffie — Hellman Conjugacy Problem // CRYPTO-2003. LNCS. 2003. V. 2729. P. 212–225.
10. *Tsaban B.* The Conjugacy Problem: Cryptoanalytic Approaches to a Problem of Dehn. Minicourse, Dusseldorf University, Germany, July–August 2012. `http://reh.math.uni-duesseldorf.de/gagta/slides/Tsabanminicourses.pdf`.
11. *Roman'kov V.* A non-linear decomposition attack // Groups, Complexity, Cryptology. 2015. V. 8. P. 197–207.
12. *Романьков В. А.* Криптографический анализ модифицированной матричной модулярной криптосистемы // Вестник Омского ун-та. 2018. Т. 23. С. 44–50.
13. *Roman'kov V.* Two general schemes of algebraic cryptography // Groups, Complexity, Cryptology. 2018. V. 10. P. 83–98.

14. *Roman'kov V. A.* A Polynomial Time Algorithm for the Braid Double Shielded Public Key Cryptosystems. Bulletin of the Karaganda University. Mathematics Ser. 2016. No. 4(84). P. 110–115. arXiv math.:1412.5277v1 [math.GR], 17 Dec. 2014. 7 p.
15. *Горнова М. Н., Кукина Е. Г., Романьков В. А.* Криптографический анализ протокола аутентификации Ушакова — Шпильрайна, основанного на проблеме бинарно скрученной сопряжённости // Прикладная дискретная математика. 2015. № 2(28). С. 46–53.
16. *Романьков В. А.* Метод линейного разложения анализа протоколов скрытой информации на алгебраических платформах // Алгебра и логика. 2015. Т. 54. № 1. С. 119–128.
17. *Roman'kov V. A. and Menshov A. V.* Cryptanalysis of Andrecut's Public Key Cryptosystem. arXiv math.: 1507.01496v1 [math.GR], 6 Jul 2015, 5 p.
18. *Andrecut M.* A Matrix Public Key Cryptosystem. arXiv math.:1506.00277v1 [cs.CR], 31 May 2015. 11 p.
19. *Gu L., Wang L., Ota K., et al.* New public key cryptosystems based on non-abelian factorization problems // Security and Communication Networks. 2013. V. 6. P. 912–922.
20. *Gu L. and Zheng S.* Conjugacy systems based on nonabelian factorization problems and their applications in cryptography // J. Appl. Math. 2014. Article ID 630607. 10 p.
21. *Hurley B. and Hurley T.* Group Ring Cryptography. arXiv math.: 1104.17.24v1 [math.GR] 9 Apr 2011. 20 p.
22. *Hurley T.* Cryptographic schemes, key exchange, public key. arXiv math.: 1305.4063v1 [cs.CR] May 2013. 19 p.
23. *Shpilrain V. and Ushakov A.* A new key exchange protocol based on the decomposition problem // Algebraic Methods in Cryptography. Contemp. Math. 2006. V. 418. P. 161–167.
24. *Stickel E.* A new method for exchanging secret keys // Proc. Third Intern. Conf. ICITA 05. Contemp. Math. 2005. V. 2. P. 426–430.
25. *Wang X., Xu C., Li G., et al.* Double shielded public key cryptosystems. Cryptology ePrint Archive. Report 2014/558. Version 20140718:185200, 2014. P. 1–14. `https://eprint.iacr.org/2014/558`.
26. *Myasnikov A., Shpilrain V., and Ushakov A.* Group-Based Cryptography. Barselona, Basel: CRM, 2008 (Advances Courses in Math.).
27. *Myasnikov A., Shpilrain V., and Ushakov A.* Non-Commutative Cryptography and Complexity of Group-Theoretic Problems. Math. Surveys and Monographs. V. 177. Providence RI: AMS, 2011.
28. *Ko K. H., Lee S. J., Cheon J. H., et al.* New public-key cryptosystem using braid groups // CRYPTO 2000. LNCS. 2000. V. 1880. P. 166–183.
29. *Романьков В. А.* Введение в криптографию. М.: Форум, 2012.
30. *Bigelow S.* Braid groups are linear // J. Amer. Math. Soc. 2001. V. 14. P. 471–486.
31. *Krammer D.* Braid groups are linear // Ann. Math. 2002. V. 155. P. 131–156.
32. *Mahalanobis A.* The Diffie — Hellman key exchange protocol and non-abelian nilpotent groups // Israel J. Math. 2008. V. 165. P. 161–187.
33. *Roman'kov V. A.* An improved version of the AAG cryptographic protocol // Groups, Complexity, Cryptology. 2019. V. 11.
34. *Anshel I., Anshel M., and Goldfeld D.* An algebraic method for public-key cryptography // Math. Res. Lett. 1999. V. 6. P. 287–291.

УДК 519.17 DOI 10.17223/2226308X/12/37

# ОЦЕНКА ХАРАКТЕРИСТИК НЕЛИНЕЙНОСТИ КОМПОЗИЦИЙ ФУНКЦИЙ ВЕКТОРНЫХ ПРОСТРАНСТВ С ПОМОЩЬЮ МАТРИЧНО-ГРАФОВОГО ПОДХОДА

М. Д. Сапегина

Развивается разработанный В. М. Фомичевым матрично-графовый подход к оценке характеристик нелинейности преобразований векторных пространств с помощью троичных матриц над мультипликативной полугруппой $\{0,1,2\}$ или орграфов, дуги которых помечены числами из $\{0,1,2\}$. Орграф $\Gamma$ с множеством вершин $\{1,\dots,n\}$ называется $\langle 2\rangle$-примитивным, если при некотором натуральном $t$ для любых $i,j \in \{1,\dots,n\}$ найдётся путь из $i$ в $j$ длины $t$, проходящий через дугу с меткой «2», наименьшее такое $t$ называется $\langle 2\rangle$-экспонентом орграфа $\Gamma$ (обозначается $\langle 2\rangle$-$\exp\Gamma$). Преобразованию $g(x_1,\dots,x_n)$ множества $V_n$ с координатными функциями $g_1(x_1,\dots,x_n),\dots,g_n(x_1,\dots,x_n)$ соответствует $n$-вершинный орграф $\Gamma_\Theta(g)$, где дуга $(i,j)$ помечена числом 0, 1 или 2 тогда и только тогда, когда $g_j$ зависит от $x_i$ соответственно фиктивно, линейно или нелинейно, $1 \leqslant i,j \leqslant n$. Преобразование $g$ называют вполне нелинейным, если метка каждой дуги орграфа есть «2». Преобразование $g$ называется $\langle 2\rangle$-перфективным, если при некотором натуральном $t$ все дуги орграфа $\Gamma_\Theta(g^t)$ помечены числом «2», наименьшее такое $t$ называется показателем полной нелинейности преобразования $g$ (обозначается $\langle 2\rangle$-$nlg$). Доказано: если в помеченном примитивном орграфе $\Gamma$ метка каждого простого контура содержит число «2» и $\exp\Gamma = n$, то орграф $\Gamma$ является $\langle 2\rangle$-примитивным и $\langle 2\rangle$-$\exp\Gamma = \exp\Gamma$. Получена оценка $\langle 2\rangle$-экспонента матрицы нелинейности $M$ порядка $2n$ раундовой функции блочных алгоритмов на основе сети Фейстеля с помощью $\langle 2\rangle$-экспонента матрицы нелинейности $\Phi$ порядка $n$ функции усложнения: $\langle 2\rangle$-$\exp M \leqslant \langle 2\rangle$-$\exp\Phi + 2$. Эти результаты позволяют снизить сложность вычисления показателя полной нелинейности для некоторых преобразований $g$. Представлены алгоритмы распознавания полной нелинейности преобразования $g$ и оценки показателя $\langle 2\rangle$-$nlg$. Для случайных преобразований средняя сложность не превышает $2\gamma(\gamma+1)\log 8n$, где $\langle 2\rangle$-$nlg = \gamma$ и элементарная операция есть вычисление любой функции на любом входном наборе. Алгоритм применён для получения точных значений $\langle 2\rangle$-$nlg$ раундовых подстановок $g$ алгоритмов DES и Магма, получены значения 5 и 6 соответственно.

**Ключевые слова:** *матрица нелинейности отображения, $\langle 2\rangle$-примитивная матрица (орграф), $\langle 2\rangle$-экспонент матрицы (орграфа), показатель полной нелинейности.*

## Введение

Необходимым требованием к свойствам функций, применяемых в алгоритмах защиты данных в информационных системах, является нелинейность, иначе секретный параметр системы может быть раскрыт противником с помощью вычислительно несложного решения системы линейных уравнений [1].

Для решения актуальных задач, направленных на изучение свойства нелинейности композиций отображений векторных пространств, используется оценочный матрично-графовый подход (МГП). В работе представлены результаты, развивающие предложенный В. М. Фомичевым в [2] МГП для оценки характеристик нелинейности отображений на основе свойств троичных матриц над мультипликативной полугруппой

{0,1,2}. Этот подход обобщает МГП к исследованию примитивности и экспонентов 0,1-матриц и соответствующих орграфов.

### 1. Мультипликативный моноид троичных матриц (помеченных орграфов)

Пусть $G = \{0, 1, 2\}$ — мультипликативная коммутативная полугруппа с операцией, определяемой равенствами: $a0 = 0$ для любого $a \in G$; $ab = \max\{a, b\}$ для любых $a, b \neq 0$. Матрица любого размера над $G$ называется троичной матрицей. Троичная матрица называется особенной, если она имеет нулевую строку или нулевой столбец.

Умножение троичной матрицы $A = (a_{i,j})$ размера $n \times m$ на матрицу $B = (b_{i,j})$ размера $m \times r$ задается следующим образом: $AB = C = (c_{i,j})$, где $C$ — матрица размера $n \times r$, $c_{i,j} = \max\{a_{i,1}b_{1,j}, \ldots, a_{i,m}b_{m,j}\}$ для любых допустимых $i, j$, умножение элементов выполнено в полугруппе $G$.

Неособенная матрица называется 2-матрицей, если каждый элемент матрицы равен 2. При $n > 1$ троичной матрице $M = (m_{i,j})$ порядка $n$ биективно соответствует помеченный $n$-вершинный орграф $\Gamma$, у которого дуга $(i, j)$ имеет метку $m_{i,j}$, $0 \leqslant i, j < n$, где метка «0» равносильна отсутствию дуги в орграфе. Матрица $M$ над полугруппой $G$ называется матрицей меток орграфа $\Gamma$ и обозначается $M(\Gamma)$.

Помеченный орграф $\Gamma$ с матрицей меток $M(\Gamma) = (2)^n$, где $(2)^n$ – матрица, все элементы которой равны 2, называется полным 2-графом. Помеченный орграф $\Gamma$ называется $\langle 2\rangle$-примитивным, если $\Gamma^t$ является полным 2-графом при некотором $t \in \mathbb{N}$, и наименьшее $t$ с таким свойством называется $\langle 2\rangle$-экспонентом орграфа $\Gamma$ (обозначается $\langle 2\rangle$-$\exp\Gamma$).

Матрица $M$ над $G$ при $n = m$ называется $\langle 2\rangle$-примитивной, если $M^t$ есть 2-матрица при некотором $t \in \mathbb{N}$. Наименьшее $t$ с таким свойством обозначается $\langle 2\rangle$-$\exp M$ и называется $\langle 2\rangle$-экспонентом матрицы $M$. Если $M^t$ есть 2-матрица при некотором $t \in \mathbb{N}$, то $M^\tau$ есть 2-матрица при любом $\tau > t$. Указанное соответствие троичных матриц и помеченных орграфов есть биекция [2], поэтому орграф $\Gamma$ $\langle 2\rangle$-примитивный, если и только если $\langle 2\rangle$-примитивна матрица $M(\Gamma)$, и $\langle 2\rangle$-$\exp\Gamma = \langle 2\rangle$-$\exp M$.

### 2. Нелинейные свойства преобразований векторных пространств

Приведём необходимые определения [2]. Пусть $P$ — конечное поле. Обозначим $\{f_j(x_0, \ldots, x_{n-1}) : j = 0, \ldots, m-1\}$ множество координатных функций отображения $\varphi : P^n \to P^m$. Функции $\varphi$ соответствует троичная матрица $M_\Theta(\varphi) = (m_{i,j})$ над полугруппой $G$ размера $n \times m$, называемая матрицей нелинейности функции $\varphi$, где элемент $m_{i,j}$ равен 0, 1 или 2, если и только если $f_j$ зависит от $x_i$ соответственно фиктивно, линейно или нелинейно, $0 \leqslant i < n$, $0 \leqslant j < m$. Равносильно можно рассматривать орграф $\Gamma_\Theta(\varphi)$ нелинейности функции $\varphi$. Заметим, что преобразование, удовлетворяющее строгому лавинному критерию, является вполне нелинейным [3].

Показателем полной нелинейности преобразования $g$ множества $P^n$ (обозначим $\langle 2\rangle$-$nlg$) называется наименьшее натуральное $t$ (если такое существует), при котором преобразование $g^t$ является вполне нелинейным. Известно [2], что $\langle 2\rangle$-$nlg \geqslant \langle 2\rangle$-$\exp M_\Theta(g)$.

### 3. Оценки $\langle 2\rangle$-экспонентов новых классов матриц нелинейности

Известно [2], что если примитивный помеченный орграф $\Gamma$ имеет дугу с меткой «2», то $\Gamma$ $\langle 2\rangle$-примитивный и $\langle 2\rangle$-$\exp\Gamma \leqslant \exp\Gamma + n$. Уточним эту оценку для некоторых орграфов.

**Теорема 1.** Если в примитивном помеченном орграфе $\Gamma$ любой простой контур проходит через дугу с меткой «2» и $\exp\Gamma \geqslant n$, то $\Gamma$ является $\langle 2\rangle$-примитивным и $\langle 2\rangle\text{-}\exp\Gamma = \exp\Gamma$.

**Теорема 2.** Если блоковая запись матрицы нелинейности $M$, в которой каждый элемент есть подматрица размера $n \times n$, имеет вид

$$M = \begin{pmatrix} 0 & E \\ E & \Phi \end{pmatrix},$$

где $0$ — нулевая подматрица; $E$ — единичная подматрица; $\Phi$ — $\langle 2\rangle$-примитивная матрица и $\langle 2\rangle\text{-}\exp\Phi = t$, то $\langle 2\rangle\text{-}\exp M \leqslant t + 2$.

Данная теорема может применяться для оценки $\langle 2\rangle$-экспонента матрицы нелинейности раундовой функции алгоритмов, построенных на основе сети Фейстеля, с помощью $\langle 2\rangle$-экспонента матрицы нелинейности функции усложнения. Это существенно сокращает расчёты, поскольку для оценки вычисляется $\langle 2\rangle$-экспонент матрицы нелинейности функции усложнения, порядок которой меньше порядка матрицы нелинейности раундовой функции в 2 раза.

Обозначим: $V_n$ — множество двоичных $n$-мерных векторов; $g(x_1, \ldots, x_n)$ — преобразование множества $V_n$; $g_1(x_1, \ldots, x_n), \ldots, g_n(x_1, \ldots, x_n)$ — координатные булевы функции преобразования $g$; $I(x)$ — множество номеров единичных координат вектора $x \in V_n$; $e_i \in V_n$, где $I(e_i) = \{i\}$, $i = 1, \ldots, n$.

Приведём алгоритмы распознавания полной нелинейности преобразования $g$ и оценки показателя $\langle 2\rangle$-$nlg$.

**Лемма 1.** Пусть для тройки векторов $a, b, e_i \in V_n$ выполнено $g(a \oplus e_i) \oplus g(a) \oplus \oplus g(b \oplus e_i) \oplus g(b) = \varepsilon_i$, тогда координатная функция $g_j(x_1, \ldots, x_n)$ преобразования $g$ зависит нелинейно от переменной $x_i$ для любого $j \in I(\varepsilon_i)$, $i = 1, \ldots, n$.

Обозначим $\vee(\varepsilon_1, \ldots, \varepsilon_t)$ покоординатную дизъюнкцию векторов $\varepsilon_1, \ldots, \varepsilon_t \in V_n$.

**Следствие 1.** Пусть имеется множество троек векторов $(a_s, b_s, e_i)$, $s = 1, \ldots, t(i)$, такое, что $g(a_s \oplus e_i) \oplus g(a_s) \oplus g(b_s \oplus e_i) \oplus g(b_s) = \varepsilon_{i,s}$ и $I(\vee(\varepsilon_{i,1}, \ldots, \varepsilon_{i,t(i)})) = \{1, \ldots, n\}$, $i = 1, \ldots, n$. Тогда преобразование $g(x_1, \ldots, x_n)$ является вполне нелинейным.

**Лемма 2.** Если преобразование $g(x_1, \ldots, x_n)$ случайное, то для всех $i = 1, \ldots, n$ $\mathsf{P}[I(\vee(\varepsilon_{i,1}, \ldots, \varepsilon_{i,t})) = \{1, \ldots, n\}] = (1 - 2^{-t})^n$, $t = 1, 2, \ldots$

**Следствие 2.** Для случайного преобразования $g(x_1, \ldots, x_n)$ $\mathsf{P}[I(\vee(\varepsilon_{i,1}, \ldots, \varepsilon_{i,t})) = = \{1, \ldots, n\}] > 1 - n2^{-t}$.

**Лемма 3.** При $n > 3$ среди всех преобразований множества $V_n$ доля вполне нелинейных преобразований не меньше $1 - n^2 2^{-2^{n-1}+1}$.

На основе леммы 1 реализован алгоритм распознавания полной нелинейности различных степеней преобразования $g$. Для этого для всех $i = 1, \ldots, n$ фиксируем вектор $e_i$ и генерируем пары случайных векторов $(a_s, b_s)$, $s = 1, \ldots, t(i)$, и при $h = 1, 2, 3, \ldots$ вычисляем $\varepsilon^h_{i,s} = g^h(a_s \oplus e_i) \oplus g^h(a_s) \oplus g^h(b_s \oplus e_i) \oplus g^h(b_s)$. Если при некоторых $s \leqslant t(i)$ и $h \in \mathbb{N}$ (из вероятностных соображений по отношению к случайным функциям взято $t(i) = \log 4n$, т. е. $s = 1, \ldots, \log 4n$, так как при $t = \log 4n$ $\mathsf{P}[I(\vee(\varepsilon_{i,1}, \ldots, \varepsilon_{i,t})) = \{1, \ldots, n\}] > 0{,}75$) выполнено $I(\vee(\varepsilon^h_{i,1}, \ldots, \varepsilon^h_{i,t(i)})) = \{1, \ldots, n\}$ для всех $i = 1, \ldots, n$, то преобразование $g^h$ вполне нелинейное и $\langle 2\rangle$-$nlg \leqslant h$. Данный алгоритм позволяет оценить сверху показатель полной нелинейности преобразования $g$.

Оценим вычислительную сложность алгоритма. Элементарной операцией будем считать вычисление значения любой функции на любом входном наборе.

**Теорема 3.** Пусть $g$ есть $\langle 2\rangle$-перфективное преобразование множества $V_n$ и $\langle 2\rangle$-$nlg = \gamma$. Если при случайном независимом и равновероятном выборе из $V_n \times V_n$ пар векторов $(a_s, b_s)$ величины $\varepsilon^h_{i,s}$, $s = 1, \ldots, t$, независимы и распределены равномерно, $h = 1, 2, \ldots$, где $\varepsilon^h_{i,s} = g^h(a_s \oplus e_i) \oplus g^h(a_s) \oplus g^h(b_s \oplus e_i) \oplus g^h(b_s)$, то средняя сложность алгоритма с параметром $t = \log 4n$ не превышает $2\gamma(\gamma + 1) \log 8n$.

С помощью разработанного алгоритма с параметром $t = 100$ (поскольку тогда $\mathsf{P}[I(\vee(\varepsilon_{i,1}, \ldots, \varepsilon_{i,t})) = \{1, \ldots, 64\}] \to 1$) определены верхние оценки показателей полной нелинейности раундовых подстановок алгоритмов DES и Магма. Для алгоритма DES она равна 5, для алгоритма Магма — 6.

В [5] с помощью МГП на основе свойств троичных матриц получены нижние оценки показателей полной нелинейности для раундовых подстановок алгоритмов DES и Магма. Они совпадают с полученными верхними оценками показателей полной нелинейности. Таким образом, для алгоритма DES наименьшая степень, в которой раундовая подстановка является вполне нелинейной, равно 5, для алгоритма Магма — 6.

## Выводы

Разработан и реализован алгоритм для вычисления верхней оценки показателя полной нелинейности отображений со сложностью, не превышающей $2\gamma(\gamma + 1) \log 8n$, где показатель полной нелинейности исследуемого преобразования $\langle 2\rangle$-$nlg = \gamma$ и элементарная операция есть вычисление любой функции на любом входном наборе. Получены точные значения показателей полной нелинейности раундовых подстановок алгоритмов DES и Магма, они равны 5 и 6 соответственно. Доказано достаточное условие равенства $\langle 2\rangle$-$\exp \Gamma = \exp \Gamma$. Получена оценка $\langle 2\rangle$-экспонента матрицы нелинейности $M$ порядка $2n$ раундовой функции блочных алгоритмов на основе сети Фейстеля с помощью $\langle 2\rangle$-экспонента матрицы нелинейности $\Phi$ порядка $n$ функции усложнения, а именно: $\langle 2\rangle$-$\exp M \leqslant \langle 2\rangle$-$\exp \Phi + 2$. Эта оценка позволяет снизить сложность вычисления показателя полной нелинейности.

## ЛИТЕРАТУРА

1. *Фомичев В. М.* Методы дискретной математики в криптологии. М.: Диалог-МИФИ, 2010.
2. *Фомичев В. М.* О производительности некоторых итеративных алгоритмов блочного шифрования из класса WBC // New Trends in Coding Systems and Techniques. LDN: Intech Publishing, 2019. С. 14.
3. *Фомичев В. М.* Криптографические методы защиты информации. В 2 ч. Ч. 1. Математические аспекты: учебник для академического бакалавриата. М.: ЮРАЙТ, 2016.
4. *Сапегина М. Д.* Оценка характеристик нелинейности раундовых подстановок алгоритмов «DES» и «Магма» // Информационная безопасность в банковско-финансовой сфере. Сб. науч. работ участников Междунар. молодежной науч.-практич. конф. в рамках V Междунар. форума «Как попасть в пятерку?». М.: Прометей, 2018. С. 6.

УДК 519.7 DOI 10.17223/2226308X/12/38

# ПОИСК ЛИНЕАРИЗУЮЩИХ МНОЖЕСТВ В АЛГЕБРАИЧЕСКОМ КРИПТОАНАЛИЗЕ КАК ЗАДАЧА ПСЕВДОБУЛЕВОЙ ОПТИМИЗАЦИИ[1]

А. А. Семёнов, К. В. Антонов, И. В. Отпущенников

Вводится понятие линеаризующего множества, которое можно рассматривать как обобщение известного понятия линеаризационного множества. Линеаризующие множества используются в основе алгебраических атак, относящихся к классу «угадывай и определяй» (guess-and-determine). В таких атаках угадываются значения переменных из некоторого множества, затем эти значения подставляются в систему алгебраических уравнений, которая связывает входные и выходные данные рассматриваемого шифра. В некоторых случаях результатом такой подстановки является линейная система, которая решается эффективно. Рассматриваются алгебраические уравнения над полем GF(2). Значения переменных из линеаризующего множества (в отличие от линеаризационного) линеаризуют систему уравнений с некоторой вероятностью, которая, вообще говоря, может быть существенно меньше 1. Оценка трудоёмкости атаки на основе конкретного линеаризующего множества строится через специально определяемую псевдобулеву функцию. Минимальное значение этой функции даёт оценку трудоёмкости лучшей по эффективности атаки. Для минимизации таких функций используется метаэвристический алгоритм из класса «поиск с запретами». На данном этапе построены атаки описанного типа для ряда криптографических генераторов. В частности, для известного генератора A5/1 построена атака с оценкой трудоёмкости в 4,5 раз ниже трудоёмкости известной атаки Андерсона.

**Ключевые слова:** *атаки из класса «угадывай и определяй», линеаризующие множества, псевдобулева оптимизация.*

Понятие линеаризационного множества введено Г. П. Агибаловым в 2003 г. [1] в контексте проблемы построения атак на некоторые генераторы ключевого потока. Атаки, рассмотренные в [1], относятся к классу алгебраических [2]. В основе алгебраических атак лежат эффективные процедуры, сводящие задачи обращения (поиска прообразов) рассматриваемых криптографических функций к поиску решений алгебраических уравнений. Обычно такие уравнения — это уравнения над полем GF(2). Как правило, в результате такой сводимости получается система, не все уравнения которой являются линейными. Известно (см., например, [3]), что задача определения совместности даже квадратичной системы над GF(2) является NP-полной и соответственно не может быть решена в общем случае за полиномиальное время известными алгоритмами. Тем не менее может оказаться так, что угадывание значений относительно небольшого числа переменных в такой системе с последующими эффективными преобразованиями превратит эту систему в линейную. Решая все возможные такие линейные системы, в ряде случаев можно построить атаки, которые существенно эффективнее атаки методом грубой силы.

Более точно, рассмотрим всюду определённую функцию $f : \{0,1\}^n \to \{0,1\}^m$, заданную некоторым алгоритмом. Требуется по произвольному $\gamma \in \mathrm{Range}\, f$ найти такой $\alpha \in \{0,1\}^n$, что $f(\alpha) = \gamma$. Известны теоретические результаты (аналогичные теореме Кука — Левина [3]), в соответствии с которыми сформулированную задачу можно

[1]Работа выполнена при финансовой поддержке Российского научного фонда, проект № 16-11-10046.

эффективно свести к проблеме поиска решения совместной системы алгебраических уравнений над полем GF(2) (кратко мы опишем такую сводимость ниже). Обозначим такую систему через $E_f(\gamma)$. Пусть $X$ — множество переменных, присутствующих в системе $E_f(\gamma)$. В соответствии с [1], множество $B \subseteq X$ называется линеаризационным (для системы $E_f(\gamma)$), если подстановка любого $\beta \in \{0,1\}^{|B|}$ в $E_f(\gamma)$ превращает эту систему в линейную. Через $\{0,1\}^{|B|}$ обозначено множество всех наборов значений переменных, входящих в $B$. Подстановка подразумевается в том смысле, как в [1] (или, по сути, в том же смысле, как в [4]). В [1] предъявлены примеры линеаризационных множеств для целого ряда генераторов ключевого потока (Геффе, пороговый, генератор переменного шага). Следует отметить, что в каждом из этих примеров вид множества $B$ не зависит от $\gamma \in \operatorname{Range} f$ (как правило, такое множество образовано переменными, соответствующими одному или нескольким LFSR, входящим в состав генератора). Получаемые на основе данных множеств атаки оказываются существенно более эффективными, чем атаки методом грубой силы.

Введём понятие линеаризующего множества. Главное отличие таких множеств от линеаризационных множеств из [1] заключается в том, что «вероятность линеаризации» рассматриваемой системы наборами значений переменных, образующих такое множество, вообще говоря, меньше 1.

Для понимания сути вводимого понятия удобно задать функцию $f$ схемой $S_f$ из функциональных элементов базиса $\{\wedge, \neg\}$. Припишем входным полюсам схемы переменные, образующие множество $X = \{x_1, \ldots, x_n\}$. Внутренним узлам схемы, которые соответствуют функциональным элементам, припишем переменные, образующие множество $V = \{v_1, \ldots, v_N\}$, $V \cap X = \varnothing$. В множестве $V$ выделим подмножество $Y = \{y_1, \ldots, y_m\}$, переменные которого приписаны выходам $S_f$. Отметим, что любому $\alpha \in \{0,1\}^{|X|}$, поданному на вход $S_f$, однозначно соответствует набор значений всех переменных из $V$, получаемый в результате последовательного вычисления значений функций, соответствующих внутренним узлам $S_f$.

Построим по $S_f$ систему алгебраических уравнений над полем $\mathrm{GF}(2) = \langle \{0,1\}, \oplus, \wedge \rangle$ по следующим правилам. Пусть $g$ — произвольный внутренний узел схемы $S_f$ и $v(g) \in$ $\in V$ — приписанная ему переменная. Если $g$ — это И-узел, то он имеет в графе, представляющем $S_f$, двух прямых предшественников, пусть им приписаны переменные $u$ и $w$. Если $g$ — это НЕ-узел, то $g$ имеет единственного предшественника, пусть $u$ — приписанная ему переменная. Сопоставим каждому $g$ уравнение над GF(2):

1) если $g$ — И-узел, то ему сопоставляется уравнение $u \wedge w \oplus v(g) = 0$;
2) если $g$ — НЕ-узел, то ему сопоставляется уравнение $u \oplus v(g) = 1$.

Объединим уравнения по всем внутренним узлам схемы $S_f$ в общую систему, которую обозначим через $E_f$.

В систему $E_f$ будем подставлять значения некоторых переменных из множества $U = X \cup V$. Подстановку определим в соответствии с [4], т. е. для произвольной переменной $x \in U$ и константы $\lambda \in \{0,1\}$ скажем, что происходит подстановка $x = \lambda$ в систему $E_f$, если все вхождения переменной в $E_f$ заменены вхождением константы $\lambda$. После подстановки к соответствующим уравнениям применяются преобразования, называемые элементарными. Например, результат подстановки $w = 1$ и соответствующего элементарного преобразования в отношении уравнения $u \wedge w \oplus v = 0$ — линейное уравнение $u \oplus v = 0$. Иногда результатом подстановки и последующих преобразований могут стать значения некоторых переменных. Например, подстановка $v = 1$ и последующие преобразования в отношении $u \wedge w \oplus v = 0$ дают уравнение $u \wedge w = 1$, откуда

следует $u = w = 1$. Назовём эти значения индуцированными подстановкой $v = 1$. Индуцированные значения также могут быть подставлены в систему. Подстановка значений для упорядоченного множества переменных определяется индуктивно: подставляется значение первой переменной и все индуцированные данной подстановкой значения, затем значение второй переменной и т. д.

Рассмотрим произвольный $\gamma \in \operatorname{Range} f$ как набор значений переменных из $Y$ и подставим его в $E_f$. Обозначим полученную систему через $E_f(\gamma)$. Можно показать, что система $E_f(\gamma)$ совместна, и если найдено некоторое её решение, то из него можно эффективно выделить такой $\alpha \in \{0,1\}^n$, что $f(\alpha) = \gamma$.

Зададим на $\{0,1\}^n$ равномерное распределение и выберем в соответствии с ним $\alpha \in \{0,1\}^n$. Пусть $\gamma_\alpha = f(\alpha)$ и $B$ — произвольное подмножество в множестве $U \setminus Y$. Как было сказано выше, подав $\alpha$ на вход схеме $S_f$, мы эффективно (в общем случае за линейное от числа узлов в $S_f$ время) вычислим значения всех переменных из $V$, в том числе значения переменных, входящих в $B$. Обозначим соответствующий набор через $\beta_\alpha$. Теперь подставим в $E_f$ наборы $\gamma_\alpha$ и $\beta_\alpha$. Результат этой подстановки и последующих элементарных преобразований обозначим через $E_f(\gamma_\alpha, \beta_\alpha)$. Действуя по аналогии с [5], введём случайную величину $\xi$, которая принимает значение 1, если система $E_f(\gamma_\alpha, \beta_\alpha)$ — линейная система над GF(2). В противном случае полагаем, что $\xi = 0$. Пусть $p_B$ — доля таких векторов $\alpha \in \{0,1\}^n$, для которых $\xi = 1$. Таким образом, $p_B$ — это некоторая числовая характеристика множества $B$. Очевидно, что $p_B = M[\xi]$. Тогда для конкретного $B$ по схеме, которая аналогична предложенной в [5], можно оценить $p_B$ при помощи метода Монте-Карло [6].

**Определение 1.** В контексте рассмотренной задачи назовём множество $B$ линеаризующим множеством с вероятностью линеаризации $p_B$.

Для произвольного $B \subseteq U \setminus Y$ и вероятности линеаризации $p_B$ можно описать следующую стратегию поиска прообразов функции $f$. Полагаем, что $\alpha$ выбран из $\{0,1\}^n$ в соответствии с равномерным распределением. Известен алгоритм вычисления $f$ и $\gamma_\alpha = f(\alpha)$. Требуется найти $\alpha$. Пусть известно некоторое множество $B$ с вероятностью линеаризации $p_B$. Для каждого $\beta \in \{0,1\}^{|B|}$ будем рассматривать систему $E_f(\gamma_\alpha, \beta)$. Если $E_f(\gamma_\alpha, \beta)$ не является линейной системой, то не делаем в её отношении никаких действий и переходим к следующему $\beta$. Вероятность события «$E_f(\gamma_\alpha, \beta_\alpha)$ — линейная» равна $p_B$. Если $E_f(\gamma_\alpha, \beta_\alpha)$ — линейная, то, решив её, найдём $\alpha$. Таким образом, для конкретного $\gamma_\alpha$ и конкретного $B$, перебрав всё множество $\{0,1\}^{|B|}$, мы линеаризуем систему с помощью вектора $\beta_\alpha \in \{0,1\}^{|B|}$ (и соответственно находим $\alpha$) с вероятностью $p_B$. Если для конкретного $\gamma_\alpha$ описанная стратегия не даёт результата (то есть при переборе всех векторов из $\{0,1\}^{|B|}$ вектор $\beta_\alpha$ не линеаризует соответствующую систему), то рассматриваем следующий выход функции $f$ (полагаем, что он также построен по случайно выбранному из $\{0,1\}^n$ входу). Вероятность того, что для случайно и независимо выбранных входов $\alpha_1, \ldots, \alpha_r$ при помощи описанной стратегии удастся обратить хотя бы один $\gamma_{\alpha_1}, \ldots, \gamma_{\alpha_r}$ $\left(\gamma_{\alpha_j} = f\left(\alpha_j\right), j \in \{1, \ldots, r\}\right)$ есть $P_B(r) = 1 - (1 - p_B)^r$ и стремится к 1 с ростом $r$. Если мы хотим, чтобы $P_B(r) > 95\,\%$, то, как нетрудно видеть, при малых $p_B$ ($p_B < 0{,}2$) $r$ должно быть не меньше $3/p_B$ (аналогичная ситуация разобрана в [5]). Будем считать единицей трудоёмкости операцию подстановки $\beta$ в систему $E_f(\gamma_\alpha)$ и проверки получаемой системы на линейность. Тогда трудоёмкость описанной атаки при условии, что $P_B(r) > 95\,\%$, составит $\approx 2^{|B|} \cdot 3/p_B$ таких единиц.

Отметим, что линеаризационные множества, примеры которых приведены в [1] в отношении генераторов Геффе, порогового и переменного шага (Alternating Step Generator), — это линеаризующие множества с $p_B = 1$.

Нетрудно понять, что, например, $B = X$ — это тривиальный пример линеаризующего множества с $p_B = 1$. Соответственно нетривиальные такие множества, вероятность $p_B$ для которых может быть существенно меньше 1, можно искать как подмножества $X$. С этой целью, действуя по аналогии с [5], введём специальную функцию $\Phi(B)$, оценивающую трудоёмкость атаки описанного типа и использующую множество $B$. На вход она получает булев вектор, единицы в котором означают присутствие переменных из $X$ в множестве $B$. Значение функции — это оценка величины $2^{|B|} \cdot 3/p_B$, для построения которой вероятность $p_B$ оценивается методом Монте-Карло. Функция $\Phi(B)$ — это «псевдобулева» функция [7]. Множество $B$, на котором значение $\Phi(B)$ минимально, даст атаку описанного типа с лучшей трудоёмкостью. Для минимизации псевдобулевых функций, которые не заданы аналитически (как в нашем случае), используются различные метаэвристические алгоритмы. Мы использовали для этих целей метаэвристику, известную как «поиск с запретами» (Tabu Search) [8]. Соответствующий алгоритм реализован в форме многопоточного приложения и запускался на одном рабочем узле кластера «Академик В. М. Матросов» Иркутского суперкомпьютерного центра [9] (36 ядер процессора Intel Xeon E5-2695). Для построения систем вида $E_f$ использовались возможности программы Transalg [10, 11] (в частности, схема $S_f$ строилась в виде И-НЕ-графа).

Полученные на данном этапе вычислительные результаты можно оценивать как предварительные. Так, для ASG-192 (генератора переменного шага с ключом длиной 192 бит) в автоматическом режиме (как результат минимизации функции $\Phi(B)$) найдено линеаризующее множество, состоящее из переменных управляющего регистра (т. е. фактически линеаризационное множество из [1]). Для ASG-96 лучшая оценка трудоёмкости достигнута для множества с $p_B \approx 99\,\%$. Интересный результат получен для известного генератора A5/1. Одна из первых атак на данный генератор, описанная в [12] (атака Андерсона), фактически использовала линеаризационное множество, состоящее из 53 бит (в A5/1 используется ключ длиной 64 бита). То есть «множество Андерсона» из [12] — это линеаризующее множество с $p_B = 1$. С использованием процедуры минимизации функции вида $\Phi(B)$ для A5/1 было найдено линеаризующее множество, состоящее из 47 переменных с $p_B \approx 0{,}071$. Оценка трудоёмкости атаки на основе этого множества оказалась примерно в 4,5 раз ниже, чем трудоёмкость атаки Андерсона.

## ЛИТЕРАТУРА

1. *Агибалов Г. П.* Логические уравнения в криптоанализе генераторов ключевого потока // Вестник Томского госуниверситета. Приложение. 2003. № 6. С. 31–41.
2. *Bard G.* Algebraic Cryptanalysis. Springer Publishing Company, Inc., 2009.
3. *Goldreich O.* Computational Complexity: A Conceptual Perspective. Cambridge: Cambridge University Press, 2008.
4. *Чень Ч., Ли Р.* Математическая логика и автоматическое доказательство теорем. М.: Наука, 1983.
5. *Semenov A., Zaikin O., Otpuschennikov I., et al.* On cryptographic attacks using backdoors for SAT // Thirty-Second AAAI Conf., 2018. P. 6641–6648. `https://arxiv.org/abs/1803.04646`.

6. *Metropolis N. and Ulam S.* The Monte Carlo method // J. Amer. Statistical Association. 1949. V. 44. No. 247. P. 335–341.
7. *Boros E. and Hammer P.* Pseudo-Boolean optimization // Discr. Appl. Math. 2002. V. 123, Iss. 1–3. P. 155–225.
8. *Glover F. and Laguna M.* Tabu Search. Norwell: Kluwer Academic Publishers, 1997.
9. ЦКП Иркутский суперкомпьютерный центр СО РАН. `http://hpc.icc.ru`
10. *Отпущенников И. В., Семенов А. А.* Технология трансляции комбинаторных проблем в булевы уравнения // Прикладная дискретная математика. 2011. № 1(11). С. 96–115.
11. *Otpuschennikov I., Semenov A., Gribanova I., et al.* Encoding cryptographic functions to SAT using TRANSALG system // Frontiers in Artificial Intelligence and Applications. 2016. V. 285. P. 1594–1595.
12. *Anderson R.* A5 (Was: Hacking digital phones). Newsgroup Communication. 1994. `http://yarchive.net/phone/gsmcipher.html`.

УДК 519.719.2 DOI 10.17223/2226308X/12/39

# ОБ АППАРАТНОЙ РЕАЛИЗАЦИИ ОДНОГО КЛАССА БАЙТОВЫХ ПОДСТАНОВОК

Д. Б. Фомин, Д. И. Трифонов

Рассмотрены вопросы реализации на ПЛИС и СБИС одного класса подстановок и проведено сравнение с реализациями произвольных байтовых отображений. Изучен способ реализации произвольной подстановки. Показано, что любая подстановка на множестве $V_8$ может быть реализована с использованием 40 LUT (812 GE). Для одного класса подстановок на множестве $V_8$, обладающего высокими криптографическими свойствами, показана возможность реализации с использованием 19 LUT (147 GE).

**Ключевые слова:** *S-Box, подстановка, ПЛИС, СБИС.*

Согласно критерию Шеннона [1], каждая криптографически безопасная функция должна представлять собой композицию функций, реализующих свойство перемешивания и рассеивания. Наиболее широко распространённый способ обеспечить свойство перемешивания — использование нелинейных преобразований, в частности подстановок. Подстановки являются неотъемлемой частью большого класса криптографических функций, таких, как поточные и блочные шифры, хэш-функции. К подстановкам предъявляются требования, позволяющие гарантировать невозможность применимости известных методов криптографического анализа, таких, как линейный, алгебраический и разностный.

Помимо криптографических требований, также предъявляются требования и к реализации подстановок, что порождает подходы к построению подстановок больших размерностей с использованием преобразований меньших размерностей. Это позволяет добиться возможности:

— программной реализации с большими таблицами замен;
— программной реализации с меньшим количеством битовых преобразований (bitslice-реализации [2]);
— использования подстановок для низкоресурсной реализации на ПЛИС и СБИС;
— эффективного аппаратного маскирования [3, 4].

Известно большое количество способов построения подстановок с использованием преобразований меньшей размерности: на основе сети Фейстеля [5 – 7], с использовани-

ем конструкции типа Misty [5, 8, 9], SPN-сети [10 – 12] и др. [13 – 15]. В данной работе рассмотрен ещё один класс подстановок и исследованы вопросы его аппаратной реализации.

Обозначим $\mathbb{F}_{2^n}$ — конечное поле из $2^n$ элементов и $V_n$ — векторное пространство размерности $n$ элементов поля $\mathbb{F}_2$. Каждый элемент поля $a \in \mathbb{F}_{2^n}$ может быть представлен как $n$-битовый вектор $a = (a_0, a_1, \ldots, a_{n-1})$, $a_i \in \mathbb{F}_2$, $i = 0, \ldots, n-1$.

Рассмотрим один способ построения $2m$-битовых подстановок, задав подстановку на прямом произведении $\mathbb{F}_{2^m} \times \mathbb{F}_{2^m}$.

**Определение 1.** Пусть $\overline{x}_1, \overline{x}_2 \in \mathbb{F}_{2^m}$, $\pi_1$, $\pi_2$, $\widehat{\pi}_1$, $\widehat{\pi}_2$ — подстановки на $\mathbb{F}_{2^m}$. Подстановку $F_A : \mathbb{F}_{2^m} \times \mathbb{F}_{2^m} \to \mathbb{F}_{2^m} \times \mathbb{F}_{2^m}$, определяемую уравнениями

$$\overline{y}_1 = \begin{cases} \pi_2\left((\overline{x}_2)^2 \cdot \pi_1\left(\overline{x}_1\right)\right), & \overline{x}_1 \neq 0; \\ \widehat{\pi}_2\left(\overline{x}_2\right), & \overline{x}_1 = 0, \end{cases}$$

$$\overline{y}_2 = \begin{cases} \pi_1\left(\overline{x}_1\right) \cdot \overline{x}_2, & \overline{x}_2 \neq 0; \\ \widehat{\pi}_1\left(\overline{x}_1\right), & \overline{x}_2 = 0, \end{cases}$$

будем называть подстановкой типа «A».

Данная подстановка предложена в [16] и её криптографические характеристики (как и криптографические характеристики некоторых других классов подстановок) теоретически обоснованы в [17]. В наиболее интересном с точки зрения практического применения случае $m = 4$ такая конструкция при подходящем выборе параметров позволяет построить 6-равномерную подстановку с нелинейностью 20 и алгебраической степенью 7.

Рассмотрим вопрос сложности реализации подстановок типа «A» на ПЛИС, который может быть оценён количеством используемых ресурсов ПЛИС, таких, как количество ячеек памяти и таблиц замены (LUT), которые в современных ПЛИС фирмы «Xilinx» реализуют произвольную булеву функцию от шести переменных. Для этого реализуем подстановки такого типа с использованием системы автоматизированного проектирования (САПР) Xilinx Vivado 2018.2 на ПЛИС Kintex-7 KC705 Evaluation Platform (xc7k325tffg900-2). В качестве стратегии оптимизации в части Synthysis выбрана стратегия «Flow Area Optimized high», а в части Implemetation — стратегия «Area Explore». Исследуем также вопрос эффективности реализации на СБИС, который оценивается в условных вентилях (GE). Количество GE оценивалось в САПР ISE 9.2i на ПЛИС XC5VLX3 семейства Virtex5.

Для корректности сравнения рассмотрим три варианта реализации 8-битовой подстановки типа «A»:

— реализация «в лоб», с помощью которой можно реализовать произвольное отображение $V_8 \to V_8$;
— реализация произвольного отображения $V_8 \to V_8$ с использованием координатных функций, которое позволяет существенно сократить используемые ресурсы;
— реализация подстановки типа «A».

В случае реализации произвольного отображения $V_8 \to V_8$ «в лоб» происходит запись таблицы значений преобразования в память. Экспериментальные исследования показали, что тип памяти, в которой хранится данная таблица, не влияет на оценку GE, необходимых для её хранения. Таким образом, будем рассматривать память

типа BRAM. При реализации на ПЛИС будем использовать встроенные ячейки памяти. Результаты оценки количества GE, необходимых для реализации данной памяти, показали, что для реализации отображения в табличном виде необходимо 65 558 GE.

Для уменьшения количества GE, необходимых для реализации отображения $V_8 \to V_8$, применим следующий подход. Так как LUT рассматриваемых ПЛИС реализуют произвольную булеву функцию от шести переменных, можно разбить входной вектор на две части: первые 2 бита и оставшиеся 6 бит соответственно. Рассмотрим отображение $f : V_8 \to V_8$, а также функции $f_i$, $i = 1, 2, 3, 4$, $f_i : V_8 \to V_8$, которые существенным образом зависят лишь от шести переменных, причём

$$f(x_1, x_2, x_3, \ldots, x_8) = \begin{cases} f_1(0, 0, x_3, \ldots, x_8), & \text{если } x_1 = 0, x_2 = 0; \\ f_2(0, 1, x_3, \ldots, x_8), & \text{если } x_1 = 0, x_2 = 1; \\ f_3(1, 0, x_3, \ldots, x_8), & \text{если } x_1 = 1, x_2 = 0; \\ f_4(1, 1, x_3, \ldots, x_8), & \text{если } x_1 = 1, x_2 = 1. \end{cases}$$

Таким образом, для реализации каждой функции $f_i$, $i = 1, 2, 3, 4$, необходимо 6 LUT (ровно по одному LUT для реализации каждой из шести координатных функций). Для реализации мультиплексора (т. е. функции выбора выходной функции) необходимо ещё 8 LUT. Суммарное количество LUT, необходимых для данной реализации функции $f$, равно 40.

Экспериментальные исследования показали, что для реализации отображения $f : V_8 \to V_8$ потребовалось 812 GE. Это примерно в 80 раз меньше, чем при реализации этого же отображения с использованием памяти.

Для реализации подстановки типа «A» требуется реализовать четыре подстановки на двоичных векторах длины 4, две операции сравнения, две операции сложения и два мультиплексора (см. определение 1). Экспериментальные исследования показали, что для реализации данной конструкции на ПЛИС необходимо 19 LUT. Это более чем в 2 раза меньше по сравнению с реализацией 8-битовой подстановки с использованием координатных функций. Результаты оценки количества GE, необходимых для реализации подстановки типа «A», показали, что необходимо лишь 147 GE — примерно в 5,5 раз меньше, чем требуется для реализации произвольной 8-битовой подстановки при помощи координатных функций, и почти в 446 раз меньше, чем при реализации этого же отображения с использованием памяти.

Полученные результаты позволяют утверждать, что подстановки, рассмотренные в [16], могут быть использованы при синтезе стойких низкоресурсных примитивов. В [17, 18] подстановки, обобщающие конструкции [16], потенциально могут использовать меньше ресурсов ПЛИС и СБИС, как, например, следующая подстановка $S(\overline{x}_1, \overline{x}_2) = (\overline{y}_1, \overline{y}_2)$, $\overline{x}_i, \overline{y}_i \in \mathbb{F}_{2^m}$, $i = 1, 2$, для реализации которой необходимо реализовать две подстановки на двоичных векторах длины 4, по две операции сравнения и сложения и два мультиплексора (подстановка типа «G», рассмотренная в [17]):

$$a = \overline{x}_1^{-1},\ b = \overline{x}_2^{-1},\ c = a \cdot b,\ d = a \cdot \overline{x}_2;$$

$$S(\overline{x}_1, \overline{x}_2) = (\overline{y}_1, \overline{y}_2),$$

$$\text{где} \quad \overline{y}_1 = \begin{cases} a, & c \neq 0, \\ c, & c = 0, \end{cases} \quad \overline{y}_2 = \begin{cases} b, & d \neq 0, \\ d, & d = 0. \end{cases}$$

## ЛИТЕРАТУРА

1. *Shannon C.* Communication theory of secrecy systems. // Bell System Technical J. 1949. No. 28. P. 656–715.

2. *Rebeiro C., Selvakumar D., and Devi A. S. L.* Bitslice implementation of AES // Cryptology and Network Security. 2006. P. 203–212. https://link.springer.com/chapter/10.1007/11935070_14.
3. *Boss E., Grosso V., Tim Güneysu T., et al.* Strong 8-bit sboxes with efficient masking in hardware // J. Cryptographic Engineering. 2017. No. 7(2). P. 149–165.
4. *Kutzner S., Nguyen P. H., and Poschmann A.* Enabling 3-share threshold implementations for all 4-bit s-boxes // LNCS. 2013. V. 8565. P. 91–108.
5. *Canteaut A., Duval S., and Leurent G.* Construction of lightweight s-boxes using Feistel and MISTY structures (full version) // Cryptology ePrint Archive. 2015. No. 2015(711).
6. *Lim C. H.* CRYPTON: A New 128-bit Block Cipher — Specification and Analysis. http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.52.5771. 1998.
7. *Gérard B., Grosso V., Naya-Plasencia M., and Standaert F.-X.* Block ciphers that are easier to mask: How far can we go? // LNCS. 2013. V. 8086. P. 383–399.
8. *Matsui M.* New block encryption algorithm MISTY // LNCS. 1997. V. 1267. P. 54–68.
9. *Grosso V., Leurent G., Standaert F.-X., and Varici K.* Ls-designs: Bitslice encryption for efficient masked software implementations // LNCS. 2014. V. 8540. P. 18–37.
10. *Standaert F.-X., Piret G., Rouvroy G., et al.* ICEBERG : An involutional cipher efficient for block encryption in reconfigurable hardware // LNCS. 2004. V. 3017. P. 279–299.
11. *Rijmen V. and Barreto P.* The Khazad Legacy-Level Block Cipher. https://www.researchgate.net/publication/228924670_The_Khazad_legacy-level_block_cipher. 2018.
12. *Lim C.-H.* A revised version of Crypton — Crypton v1.0 // LNCS. 1999. V. 1636. P. 31–45.
13. *Stallings W.* The Whirlpool secure hash function // Cryptologia. 2006. No. 30(1). P. 55–67.
14. *Perrin L., Udovenko A., and Biryukov A.* Cryptanalysis of a theorem: Decomposing the only known solution to the big APN problem (full version) // Cryptology ePrint Archive. 2016. No. 2016(539).
15. *De la Cruz Jiménez R. A.* On some methods for constructing almost optimal s-boxes and their resilience against side-channel attacks // Cryptology ePrint Archive. 2018. No. 2018(618).
16. *Fomin D.* New classes of 8-bit permutations based on a butterfly structure // CTCrypt'18. 2018. https://ctcrypt.ru/files/files/2018/09_Fomin.pdf
17. *Fomin D.* On the way of constructing $2n$-bit permutations from $n$-bit ones // CTCrypt'19. 2019 (в печати).
18. *Фомин Д. Б.* О подходах к построению низкоресурсных нелинейных преобразований // Обозрение прикладной и промышленной математики. 2018. Т. 25(4). С. 379–381.

УДК 519.17 DOI 10.17223/2226308X/12/40

## О ПАРАМЕТРАХ ГЕНЕРАТОРА РАУНДОВЫХ КЛЮЧЕЙ АЛГОРИТМА 2-ГОСТ

В. М. Фомичев, А. М. Коренева, А. И. Тулебаев

Необходимость защиты информации в условиях ограниченных ресурсов определяет актуальность построения облегченных реализаций для известных криптографических алгоритмов. В 2014 г. была представлена низкоресурсная реализация ГОСТ 28147-89 под названием 2-ГОСТ. Несмотря на достоинства, схема имела потенциал в части усиления криптографической стойкости, в том числе за счёт модификации ключевого расписания. В 2018 г. предложен новый алгоритм генерации раундовых ключей для 2-ГОСТ на основе регистра сдвига длины 8 над множеством двоичных векторов длины 32. Вместе с тем параметры обратной свя-

зи регистра не были достаточно обоснованы. Работа посвящена определению наилучших (или близких к наилучшим) трёх точек съёма функции обратной связи регистра сдвига и обоснованию предложенного решения. Критерий качества поиска решения определяется характеристиками перемешивания исходных данных с помощью регистрового преобразования и экономичностью реализации, выраженной через «площадь реализации». В качестве характеристики перемешивания использован показатель локальной совершенности регистрового преобразования — число итераций (тактов работы генератора), после которых каждый бит сгенерированного раундового ключа существенно зависит от всех битов начального состояния (основного ключа алгоритма). Большее число точек съёма функции обратной связи не рассматривалось, так как эти варианты менее экономичны. Найдена наилучшая тройка точек съёма функции обратной связи регистра сдвига и проведено сравнение характеристик, определяющих качество ключевого расписания для предложенной и исходной схем. Установлено, что в исходной схеме значение показателя локальной совершенности наибольшее в классе всех функций обратной связи с тремя точками съёма (наихудший показатель с точки зрения перемешивания). Предложена альтернативная схема с наименьшим показателем локальной совершенности и аналогичной площадью реализации. Для исходной и альтернативной схемы проведено статистическое тестирование выходных последовательностей генератора.

**Ключевые слова:** *2-ГОСТ, генератор ключей, локальная совершенность, матрично-графовый подход, перемешивающие свойства, регистр сдвига.*

## Введение

Ключевое расписание блочного шифра является важным компонентом строения, определяющим его криптографическую стойкость. Применение многих методов криптоанализа затруднено, если алгоритм развертывания ключа обеспечивает сложную нелинейную зависимость битов раундовых ключей от битов основного ключа. В 2014 г. представлена предназначенная для низкоресурсной реализации модификация блочного шифра ГОСТ 28147-89 под названием 2-ГОСТ [1]. Для усиления криптографических свойств в модификации предложена новая, более сложная по сравнению с ГОСТ 28147-89 схема ключевой развёртки на основе регистра сдвига длины 8 над множеством двоичных векторов длины 32 с функцией обратной связи, имеющей три точки съёма. Методы и результаты исследования предложенной схемы полностью представлены не были.

Цель данной работы — усилить криптографические характеристики схемы ключевой развёртки за счёт выбора наилучшей тройки точек съёма и представить обоснование выбранного решения. Для обоснования решения использован, в частности, математический аппарат, изложенный в [2].

Установлено [3], что предложенная в [4] модификация обладает не лучшими перемешивающими свойствами. С целью устранения недостатка выполнен перебор всех троек точек съёма вида $(0, i, j)$, где $0 < i, j \leqslant 7$, чтобы оценить для каждой тройки характеристики перемешивания, в том числе с использованием матрично-графового подхода (если 0 — не точка съёма, то реальная длина регистра меньше 8). Для регистровых преобразований получены значения локальных экспонентов их перемешивающих орграфов и экспериментально вычислены показатели локальной совершенности. Для оригинальной и предложенной схемы проведено статистическое тестирование выходных последовательностей генераторов.

## 1. Схема генератора 2-ГОСТ

Схема генератора построена на основе регистра сдвига длины 8 над множеством двоичных векторов длины 32 [4]. Преобразование $g_{i,j}$ множества 256-мерных двоичных векторов определено формулой (схема регистра при $(i,j)=(7,5)$ дана на рис.1)

$$g_{i,j}(X_0,\dots,X_7)=(X_1,\dots,X_7,\tau(S(X_0\oplus X_i))\oplus X_j),$$

где $\tau$ и $S$ — определённые в [4] подстановки степени 32, обеспечивающие зависимость младших разрядов вектора $\tau(S(X_0\oplus X_i))\oplus X_j$ от старших разрядов.

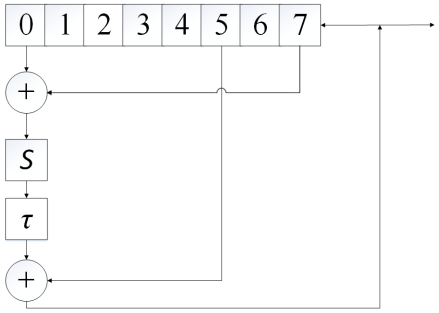


Рис. 1. Схема регистра сдвига при точках съема $(i,j)=(7,5)$

## 2. Оптимизация параметров генератора

Поиск наилучшей пары точек $i,j$ выполнен с помощью перебора всех значений $i,j$, при которых перемешивающий орграф примитивный. Для каждой такой пары посчитана оценка $\gamma$ локального (7,256)-экспонента перемешивающего орграфа $\Gamma(g)$ преобразования $g$, оценивающего число тактов, после которых каждый из 32-х разрядов вектора в ячейке 7 может зависеть от всех битов начального заполнения регистра, иначе говоря, все столбцы с номерами $225,\dots,256$ перемешивающей матрицы в степени $\gamma$ не содержат нулей. Затем с учётом полученной оценки локального экспонента определён показатель $\gamma_7(i,j)$ локальной совершенности преобразования $g$ (равный наименьшему числу итераций, после которых указанная зависимость необходимо имеется).

Пусть для краткости $g_{i,j}=g$. Обозначим $g_k^t$ координатную $k$-ю функцию преобразования $g^t$, $k=1,\dots,256$, $t=1,2,\dots$ Экспериментально найдено наименьшее значение $\gamma_7(i,j)$ степени $t$ преобразования $g$, при которой для $k=225,\dots,256$ и $l=1,\dots,256$ функция $g_k^t(x_1,\dots,x_{256})$ существенно зависит от $x_l$, то есть найдены векторы $a$, $a\oplus e_l$, где $e_l$ — вектор веса 1, у которого $l$-я координата равна 1, $1\leqslant l\leqslant 256$, такие, что

$$g_k^{\gamma_7(i,j)}(a)\oplus g_k^{\gamma_7(i,j)}(a\oplus e_l)=1.$$

В таблице приведены значения показателей локальной совершенности преобразования $g$ для всех указанных пар $(i,j)$ точек съёма. Из таблицы видно, что для генератора, предложенного в [4], величина $\gamma_7(2,1)$ совпала с локальным (7,256)-экспонентом и равна 43, т. е. в оригинальной схеме с точками съёма (0,1,2) характеристики перемешивания наихудшие. Наилучшие характеристики перемешивания имеет модификация генератора с точками съёма (0,5,7) с наименьшим показателем локальной совершенности. При фиксации точек 7 и 5 (рис. 1) получено наименьшее значение $\gamma_7(7,5)=10$.

| $i,j$ | 1,2 | 1,3 | 1,4 | 1,5 | 1,6 | 1,7 | 2,1 | 2,3 | 2,5 | 2,7 | 3,1 | 3,2 | 3,4 | 3,5 | 3,6 | 3,7 | 4,1 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| $\gamma_7(i,j)$ | 40 | 32 | 28 | 28 | 28 | 28 | 43 | 34 | 26 | 24 | 39 | 38 | 26 | 38 | 22 | 20 | 34 |
| $i,j$ | 4,3 | 4,5 | 4,7 | 5,1 | 5,2 | 5,4 | 5,6 | 5,7 | 6,1 | 6,3 | 6,5 | 6,7 | 7,2 | 7,3 | 7,4 | 7,5 | 7,6 |
| $\gamma_7(i,j)$ | 28 | 22 | 16 | 23 | 40 | 21 | 18 | 14 | 18 | 17 | 19 | 12 | 11 | 12 | 13 | 10 | 15 |

## 3. Статистическое тестирование выходных последовательностей генератора

Для оценки качества генерируемых последовательностей исходного и предложенного генераторов выполнено их статистическое тестирование. Для этого использован пакет NIST Statistical Test Suit (NIST STS) версии 2.1.2. Выбор параметров и интерпретация результатов осуществлялась в соответствии с рекомендациями NIST [5].

Для проверки статистических свойств генераторов при $(i,j)=(2,1)$ и $(i,j)=(7,5)$ сформированы файлы по $N=2048000000$ бит выходных данных, анализируемый материал разбивался на $m=100$ подпоследовательностей. Тестирование проводилось при нескольких наборах параметров, в каждом случае проведено по 188 тестов, уровень значимости $\alpha=0{,}05$. В результате тестирования подсчитаны:

— $C_1,\dots,C_{10}$ — количество значений p-value, попавших в соответствующий подынтервал (сумма значений $C_1,\dots,C_{10}$ равна $m$);
— P-VALUE — результирующее значение вероятности статистики теста (для всей последовательности длины $N$);
— PROPORTION — доля подпоследовательностей, прошедших тест с заданным уровнем значимости $\alpha$.

При анализе результатов проверялись условия

$$\text{P-VALUE} \geqslant \alpha \text{ и } 0{,}9 \leqslant \text{PROPORTION}.$$

При начальном заполнении регистров значениями, полученными с качественного генератора псевдослучайных чисел, проверяемые файлы успешно прошли статистическое тестирование. Доля непройденных тестов невелика: для $(i,j)=(2,1)$ — не более 9 из 188, для $(i,j)=(7,5)$ — не более 4 из 188.

При начальном заполнении регистров значением с регулярной структурой, например $(X_0,X_1,X_2,X_3,X_4,X_5,X_6,X_7)=(\overline{0},\overline{1},\overline{0},\overline{1},\overline{0},\overline{1},\overline{0},\overline{1})$, где $\overline{0}=(0,\dots,0)\in V_{32}$, $\overline{1}=(1,\dots,1)\in V_{32}$, проверяемые файлы не прошли статистическое тестирование. Для $(i,j)=(2,1)$ не пройдено 180 тестов из 188, для $(i,j)=(7,5)$ — 181 тест из 188. Кроме того, при указанном начальном заполнении наблюдались повторы выходных значений.

## Выводы

Исследован показатель локальной совершенности преобразований, связанных со схемой, представленной на РусКрипто'2018. Предложен альтернативный вариант точек съёма регистрового преобразования с аналогичной площадью реализации и наименьшим значением показателя совершенности (10 вместо 43 в оригинальной схеме). Это позволяет существенно сократить число тактов, необходимых для генерации раундовых ключей, каждый бит которых зависит от всех битов основного ключа.

Проведено статистическое тестирование выходных последовательностей обеих схем. Обнаружены начальные заполнения, при которых выходные последовательности имеют небольшую длину периода. Для гарантирования длины периода выходных последовательностей не меньше $2^{32}$ можно рекомендовать схемы на основе последова-

тельного соединения указанного регистра с полноцикловым линейным конгруэнтным генератором, использующим модуль $2^{32}$ и нечётный сдвиг [6, с. 156].

## ЛИТЕРАТУРА


1. *Dmukh A. A., Dygin D. M., and Marshalko G. B.* A lightweight-friendly modification of GOST block cipher // Матем. вопр. криптогр. 2014. Т. 5. № 2. С. 47–55.
2. *Fomichev V. M., Avezova Ya. A., Koreneva A. M., and Kyazhin S. N.* Primitivity and local primitivity of digraphs and nonnegative matrices // J. Appl. Industr. Math. 2018. V. 12. No. 3. P. 453–469.
3. *Коренева А. М., Полеводин А. В.* Перемешивающие свойства генератора раундовых ключей алгоритма шифрования 2-ГОСТ // Информационная безопасность в банковско-финансовой сфере: Сб. научн. работ участников. М.: Прометей, 2018. С. 107–111.
4. *Дмух А., Трифонов Д., Чухно А.* О модификации отечественного низкоресурсного криптографического алгоритма 2-ГОСТ и вопросах его реализации на ПЛИС. Москва, РусКрипто-2018. `https://www.ruscrypto.ru/resource/archive/rc2018/files/02_Dmukh_Trifonov_Chukhno.pdf`.
5. A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications. Special Publication (NIST SP) 800–22 Rev 1a. `https://www.nist.gov/publications/statistical-test-suite-random-and-pseudorandom-number-generators-cryptographic`.
6. *Фомичёв В. М.* Методы дискретной математики в криптологии. М.: ДИАЛОГ-МИФИ, 2010. 424 с.


УДК 519.17 DOI 10.17223/2226308X/12/41

# О ПЕРЕМЕШИВАЮЩИХ СВОЙСТВАХ МОДИФИЦИРОВАННЫХ МНОГОМЕРНЫХ ЛИНЕЙНЫХ ГЕНЕРАТОРОВ

И. И. Хайруллин

Описан новый класс регистров сдвига длины $n$ с $r$-битовыми ячейками, $n > 1$, $r > 1$, названных модифицированными многомерными линейными генераторами (ММЛГ). Проведено экспериментальное исследование перемешивающих свойств регистров сдвига длины 8 над $V_{32}$ из класса ММЛГ, функция обратной связи которых построена на основе раундовой подстановки низкоресурсного блочного шифра SPECK. Для таких ММЛГ с различными множествами точек съёма $D \subseteq \{0, \ldots, 7\}$ рассчитаны локальные (0,256)-экспоненты перемешивающих матриц, то есть для каждой матрицы $M$ определено наименьшее натуральное число $\gamma$, такое, что при любом натуральном $t \geqslant \gamma$ положительны все столбцы матрицы $M^t$ с номерами 1,. . . ,32. Вычислены показатели 0-совершенности, то есть наименьшие значения степеней регистрового преобразования, при которых каждая координатная функция выхода существенно зависит от всех переменных входа. Для ММЛГ с точками съёма 0 и 7 значения локального экспонента и локального показателя совершенности равны 17. Полученные значения сравниваются с локальными экспонентами и локальными показателями совершенности для конструктивно схожих аналогов, построенных на основе модифицированных аддитивных генераторов. Сравнение показало, что генераторы обладают схожими перемешивающими свойствами, однако в отличие от рассмотренных схем класс ММЛГ представляет интерес для использования в условиях ограниченных ресурсов.

**Ключевые слова:** *модифицированный многомерный линейный генератор, пере-*

*мешивающие свойства, матрично-графовый подход, перемешивающая матрица, показатель совершенности, регистр сдвига, экспонент, SPECK.*

## Введение

Одним из важных криптографических свойств итеративных криптографических алгоритмов является перемешивание входных данных. В основе принципа перемешивания лежит свойство существенной зависимости выходных функций от входных переменных. Для функции над двоичным конечномерным векторным пространством существенную зависимость каждого бита выхода от всех битов входа называют свойством полного перемешивания. Функции со свойством полного перемешивания называются совершенными [1].

Одним из методов оценки перемешивающих свойств преобразований является матрично-графовый подход (МГП) [2], который заключается в исследовании свойства примитивности и экспонентов для специального класса орграфов (перемешивающих орграфов) и соответствующих матриц смежности вершин этих орграфов (перемешивающих матриц). Неотрицательная матрица $M$ называется примитивной, если $M^t$ не содержит нулевых элементов при некотором $t \in \mathbb{N}$. Наименьшее $t$ с таким свойством называют экспонентом матрицы $M$. С применением МГП в данной работе исследуется класс преобразований, построенных на основе регистров сдвига с нелинейной комбинирующей обратной связью — ММЛГ. Регистры сдвига над множеством двоичных $r$-мерных векторов широко используются при построении генераторов раундовых ключей итеративных блочных шифров [3 – 5].

Экспериментально определены множества точек съёма, при которых перемешивающая матрица преобразования множества состояний ММЛГ примитивна. Для различных множеств точек съёма получены значения $\gamma$ локальных экспонентов перемешивающих матриц, оценивающих число тактов, после которых каждый из 32 разрядов вектора в ячейке с номером 0 может зависеть от всех битов начального заполнения регистра, иначе говоря, все столбцы с номерами 1,. . . ,32 перемешивающей матрицы в степени $\gamma$ не содержат нулей. С учётом полученных значений локальных экспонентов определён показатель локальной совершенности преобразования ММЛГ, равный наименьшему числу тактов работы генератора, после которых указанная зависимость имеется.

## 1. Конструкция ММЛГ

Рассмотрим многомерный линейный генератор – генератор, построенный на основе регистра сдвига длины $n$ над кольцом вычетов по модулю $2^r$, $r > 1$. При $i \geqslant n$ знак гаммы $X_i$ образуется в соответствии с законом рекурсии

$$X_i = b^{-1}\left(\bigoplus_{j=0}^{n-1} b(a_j X_{j+i-n})\right),$$

где $a_1, \ldots, a_{n-1} \in \{0, 1\}$; $a_0 = 1$; $b$ — биекция $\mathbb{Z}_{2^r} \leftrightarrow V_r$, определяющая двоичное $r$-разрядное представление числа $X \in \mathbb{Z}_{2^r}$ по правилу: если $X = 2^{r-1}x_0 + \ldots + 2x_{r-2} + x_{r-1}$, то $b(X) = \bar{X} = x_0 \ldots x_{n-1}$, $\bar{X} \in V_r$; $b^{-1}$ — обратная к $b$ функция.

Модифицируем многомерный линейный генератор с помощью преобразования $g : V_r \to V_r$, назовём такой генератор ММЛГ, закон рекурсии для выходного знака $X_i$ имеет вид

$$X_i = b^{-1}\left(g\left(\bigoplus_{j=0}^{n-1} b(a_j X_{j+i-n})\right)\right).$$

Обозначим через $\varphi^g : V_{nr} \to V_{nr}$ преобразование множества состояний ММЛГ

$$\varphi^g(\bar{X}_0, \ldots, \bar{X}_{n-1}) = (\bar{X}_1, \ldots, \bar{X}_{n-1}, f^g(\bar{X}_0, \ldots, \bar{X}_{n-1})),$$

где $f^g(\bar{X}_0, \ldots, \bar{X}_{n-1}) = g(f(\bar{X}_0, \ldots, \bar{X}_{n-1})) = g\left(\bigoplus\limits_{k \in D} b(X_k)\right)$ — функция обратной связи $f^g : V_{nr} \to V_r$ ММЛГ; $D = \{d_0, \ldots, d_q\} \subseteq \{0, \ldots, n-1\}$ — множество точек съёма (номеров существенных переменных функции $f$).

Схема ММЛГ приведена на рис. 1, через $Q$ обозначен выход генератора.

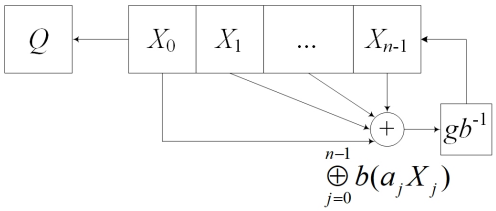


Рис. 1. Схема функционирования ММЛГ

Рассмотрим класс ММЛГ, построенных на основе регистров сдвига длины 8 над $V_{32}$. В качестве модифицирующего преобразования используем раундовую подстановку низкоресурсного блочного алгоритма шифрования SPECK с блоком длины 32 бита и соответствующими для данного размера блока параметрами алгоритма, описанными в [6]. Обозначим такое модифицирующее преобразование через $\hat{S}_{32}$. Оно обладает рядом позитивных свойств:

— экспонент перемешивающей матрицы преобразования $\hat{S}_{32}$ равен 4, что сравнимо со значениями экспонентов других современных низкоресурсных алгоритмов блочного шифрования;
— имеет малые показатели ресурсоёмкости в сравнении с другими современными низкоресурсными алгоритмами блочного шифрования, в частности по площади аппаратной реализации. Это свойство особенно полезно с учётом современных тенденций, направленных на построение низкоресурсных алгоритмов.

## 2. Экспериментальное исследование перемешивающих свойств

В ходе эксперимента исследованы ММЛГ, построенные на основе регистров сдвига длины 8 над $V_{32}$ с модифицирующим преобразованием $\hat{S}_{32}$ и различными множествами точек съёма $D \subseteq \{0, \ldots, 7\}$. Для каждого регистрового преобразования построена перемешивающая матрица $M$ и определено значение локального (0,256)-экспонента, то есть наименьшее натуральное число $\gamma$, такое, что при любом натуральном $t \geqslant \gamma$ положительны все столбцы матрицы $M^t$ с номерами {1,. . . ,32}. Проведён вычислительный эксперимент по определению показателя 0-совершенности, то есть наименьшего числа тактов работы ММЛГ, после которого каждая координатная функция нулевого блока существенно зависит от всех знаков начального состояния.

В табл. 1 представлены значения локальных характеристик перемешивания для некоторых представителей $\hat{S}_{32}$-модификации ММЛГ с различными множествами точек съёма.

Исходя из соображений экономичности аппаратной реализации, рассмотрим $\hat{S}_{32}$-модификацию ММЛГ с множеством точек съёма $D = \{0, 7\}$. Сравним полученные значения локальных экспонентов и локальных показателей совершенности с аналогичными характеристиками для конструктивно схожих аналогов генератора. Рассмотрим

Таблица 1

**Значения локальных характеристик перемешивания для $\hat{S}_{32}$-модификаций**

| Мощность множества точек съёма | Множество точек съёма | Показатель 0-совершенности | Локальный (0,256)-экспонент |
|---|---|---|---|
| 2 | {0,7} | 17 | 17 |
| 3 | {0,3,7} | 14 | 14 |
| 4 | {0,1,4,7} | 13 | 13 |
| 5 | {0,1,3,5,7} | 12 | 12 |

схемы МАГ-$\mu_1$ и МАГ-$\mu_2$ [6], а также МАГ-$\hat{S}_{32}$ — преобразование аддитивного генератора, модифицированного с использованием SPECK. Сравнение перемешивающих характеристик приведено в табл. 2.

Таблица 2

**Сравнение перемешивающих характеристик**

| Схема регистра сдвига | МАГ-$\mu_1$ | МАГ-$\mu_2$ | МАГ-$\hat{S}_{32}$ | ММЛГ-$\hat{S}_{32}$ |
|---|---|---|---|---|
| (0,256)-экспонент | 15 | 14 | 15 | 17 |
| Показатель 0-совершенности | 29 | 16 | 16 | 17 |

## Выводы

С помощью матрично-графового подхода исследованы перемешивающие свойства нового класса регистровых преобразований — многомерных линейных генераторов, модифицированных с использованием преобразования SPECK. По результатам исследования предложена схема на основе регистра сдвига с двумя точками обратной связи, которая обеспечивает паритет по качеству перемешивающих свойств и площади аппаратной реализации. Значения перемешивающих характеристик для предложенной схемы близки к аналогичным характеристикам для конструктивно схожих схем генераторов, однако, в отличие от рассмотренных схем, ММЛГ представляет интерес для использования в условиях ограниченных ресурсов.

Автор выражает благодарность д.ф.-м.н. профессору В. М. Фомичеву и к.ф.-м.н. А. М. Кореневой за постановку задачи и внимание к проводимым исследованиям.

## ЛИТЕРАТУРА

1. *Фомичев В. М., Мельников Д. А.* Криптографические методы защиты информации. Ч. 1. Математические аспекты. М.: Юрайт, 2017.
2. *Fomichev V. M., Avezova Ya. A., Koreneva A. M., and Kyazhin S. N.* Primitivity and local primitivity of digraphs and nonnegative matrices // J. Appl. Industr. Math. 2018. V. 12. No. 3. P. 453–469.
3. *Fomichev V. M. and Koreneva A. M.* On Efficiency of Block Encryption by Improved Key Schedule. Ярославль, CTCrypt-2016. `https://ctcrypt.ru/files/files/2016/12fomichev.pdf`.
4. *Фомичев В. М., Задорожный Д. И., Коренева А. М., Тулебаев А. И.* О ключевом расписании на основе модифицированного аддитивного генератора. Москва, РусКрипто-2018. `https://www.ruscrypto.ru/resource/archive/rc2018/files/02_Koreneva.pdf`.
5. *Дмух А., Трифонов Д., Чухно А.* О модификации отечественного низкоресурсного криптографического алгоритма 2-ГОСТ и вопросах его реализации на ПЛИС.

Москва, РусКрипто-2018. https://www.ruscrypto.ru/resource/archive/rc2018/files/02_Dmukh_Trifonov_Chukhno.pdf.

6. *Beaulieu R., Shors D., Smith J., et al.* The SIMON and SPECK families of lightweight block ciphers. https://eprint.iacr.org/2013/404.pdf.

UDC 621.391:519.7 DOI 10.17223/2226308X/12/42

# A METHOD FOR CONSTRUCTING PERMUTATIONS, INVOLUTIONS AND ORTHOMORPHISMS WITH STRONG CRYPTOGRAPHIC PROPERTIES

R. A. de la Cruz Jiménez

S-Boxes are crucial components in the design of many symmetric ciphers. To construct permutations having strong cryptographic properties is not a trivial task. In this work, we propose a new scheme based on the well-known Lai-Massey structure for generating permutations of dimension $n = 2k$, $k \geqslant 2$. The main cores of our constructions are: the inversion in $\mathrm{GF}(2^k)$, an arbitrary $k$-bit non-bijective function (which has no pre-image for 0) and any $k$-bit permutation. Combining these components with the finite field multiplication, we provide new 8-bit permutations without fixed points possessing a very good combination for nonlinearity, differential uniformity and minimum degree — (104; 6; 7) which can be described by a system of polynomial equations with degree 3. Also, we show that our approach can be used for constructing involutions and orthomorphisms with strong cryptographic properties.

**Keywords:** *S-Box, permutation, Boolean functions.*

Let $V_n$ be $n$-dimensional vector space over the field $\mathrm{GF}(2)$, by $S(V_n)$ we denote the symmetric group on set of $2^n$ elements. The finite field of size $2^n$ is denoted by $\mathrm{GF}(2^n)$, where $\mathrm{GF}(2^n) = \mathrm{GF}(2)[\xi]/g(\xi)$, for some irreducible polynomial $g(\xi)$ of degree $n$. We use the notation $\mathbb{Z}/2^n$ for the ring of the integers modulo $2^n$. There are bijective mappings between $\mathbb{Z}/2^n$, $V_n$, and $\mathrm{GF}(2^n)$ defined by the correspondences:

$$\left[a_{n-1} \cdot 2^{n-1} + \ldots + a_0\right] \quad \leftrightarrow \quad (a_{n-1}, \ldots, a_0) \quad \leftrightarrow \quad \left[a_{n-1} \cdot \xi^{n-1} + \ldots + a_0\right].$$

Using these mapping in what follows, we make no difference between vectors of $V_n$ and the corresponding elements in $\mathbb{Z}/2^n$ and $\mathrm{GF}(2^n)$.

Throughout the article, we shall use the following operations and notations:

$a \| b$ — concatenation of the vectors $a, b$ of $V_l$, i.e. a vector from $V_{2l}$;
$0$ — the null vector of $V_l$;
$\oplus$ — bitwise eXclusive-OR — addition in $\mathrm{GF}(2^l)$;
$\langle a, b \rangle$ — the scalar product of vectors $a = (a_{l-1}, \ldots, a_0), b = (b_{l-1}, \ldots, b_0)$ of $V_l$, $\langle a, b \rangle = a_{l-1}b_{l-1} \oplus \ldots \oplus a_0 b_0$;
$\mathrm{w}_H(a)$ — the Hamming weight of a binary vector $a \in V_l$;
$\otimes$ — finite field multiplication;
$\Lambda \circ \Psi$ — a composition of mappings, where $\Psi$ is the first to operate;
$\Psi^{-1}$ — the inverse transformation to some bijective mapping $\Psi$.

Now, we introduce some basic concepts needed to describe and analyze S-Boxes with respect to linear, differential, and algebraic attacks. For this purpose, we consider an $n$-bit S-Box $\Phi$ as a vector of Boolean functions:

$$\Phi = (f_{n-1}, \ldots, f_0), \ \ f_i : V_n \to V_1, \ \ i = 0, 1, \ldots n-1.$$

For some fixed $i \in \{0, 1, \ldots, n-1\}$, every Boolean function $f_i$ can be written as a sum over $V_1$ of distinct $t$-order products of its arguments, $0 \leqslant t \leqslant n-1$; this is called the algebraic normal form of $f_i$. Functions $f_i$ are called coordinate Boolean functions of the S-Box $\Phi$ and it is well known that most of the desirable cryptographic properties of $\Phi$ can be defined in terms of their linear combinations (also-called S-Box component Boolean functions).

**Definition 1.** For $a, b \in V_n$ the Walsh transform $\mathcal{W}_\Phi(a, b)$ of an $n$-bit S-Box $\Phi$ is defined as

$$\mathcal{W}_\Phi(a, b) = \sum_{x \in V_n} (-1)^{\langle b, \Phi(x)\rangle \oplus \langle a, x\rangle}.$$

**Definition 2.** The nonlinearity of an $n$-bit S-Box $\Phi$, denoted by $\mathcal{NL}(\Phi)$, is defined as

$$\mathcal{NL}(\Phi) = \min_{a \in V_n \setminus \{0\}} \{\mathcal{NL}(a_{n-1} f_{n-1} \oplus \ldots \oplus a_0 f_0)\},$$

where $\mathcal{NL}(a_{n-1} f_{n-1} \oplus \ldots \oplus a_0 f_0)$ is the nonlinearity of the component Boolean function.

The nonlinearity $\mathcal{NL}(\Phi)$ of an arbitrary $n$-bit S-Box $\Phi$ can be calculated as follows

$$\mathcal{NL}(\Phi) = 2^{n-1} - \frac{1}{2} \max_{a \neq 0, b \in V_n} |\mathcal{W}_\Phi(a, b)|.$$

**Definition 3.** The differential uniformity of an $n$-bit S-Box $\Phi$, denoted by $\delta_\Phi$, is defined as

$$\delta(\Phi) = \max_{a \neq 0, b \in V_n} \delta_\Phi(a, b),$$

where $\delta_\Phi(a, b) = |\{x \in V_n : \Phi(x \oplus a) \oplus \Phi(x) = b\}|$.

**Definition 4.** The minimum degree of an S-Box $\Phi$, denoted by $\deg(\Phi)$, is defined as

$$\deg(\Phi) = \min_{a \in V_n \setminus \{0\}} \{\deg(a_{n-1} f_{n-1} \oplus \ldots \oplus a_0 f_0)\}.$$

**Definition 5.** Let $U$ be a non-empty subset of $V_{2n}$, then the annihilating set of $U$ is defined as $\{p \in \mathrm{GF}(2)[z_1, \ldots, z_{2n}] : p(U) = 0\}$.

**Definition 6.** The algebraic immunity of $U$ is defined as

$$\mathcal{AI}(U) = \min\{\deg p : 0 \neq p \in \mathrm{GF}(2)[z_1, \ldots, z_{2n}],\ p(U) = 0\}.$$

**Definition 7.** The graph algebraic immunity of $n$-bit S-Box $\Phi$, denoted by $\mathcal{AI}_{\mathrm{gr}}(\Phi)$, is defined as

$$\mathcal{AI}_{\mathrm{gr}}(\Phi) = \min\{\deg p : 0 \neq p \in \mathrm{GF}(2)[z_1, \ldots, z_{2n}],\ p(\mathrm{gr}(\Phi)) = 0\},$$

where $\mathrm{gr}(\Phi) = \{(x, \Phi(x)) : x \in V_n\} \subseteq V_{2n}$.

Thus, we focus on the graph algebraic immunity of S-Box $\Phi$ and also on the parameter $r_\Phi^{(\mathcal{AI}_{\mathrm{gr}}(\Phi))}$ referred to as the number of all the independent equations in input and output values of the S-Box $\Phi$, i.e., equations of the form $p(x, \Phi(x)) = 0$, $x \in V_n$.

**Definition 8.** An element $a \in V_n$ is called a fixed point of an $n$-bit S-Box $\Phi$ if $\Phi(a) = a$.

**Definition 9.** Two $n$-bit S-Boxes $\Phi_1$ and $\Phi_2$ are affine/linear equivalent if there exist a pair of invertible affine/linear permutation $A_1(x)$ and $A_2(x)$ such that $\Phi_1(x) = A_2 \circ \Phi_2 \circ$ $\circ A_1(x)$.

## 1. Constructing permutations from smaller ones and finite field multiplication

In this section, we present a special algorithmic-algebraic scheme which utilize the Lai-Massey structure for constructing $2k$-bits permutations from smaller ones and finite field multiplication. Our goal is to construct permutations with good cryptographic properties that were enumerated above.

Let $n = 2k$ be a natural number, where $k \geqslant 2$. Choosing

— the permutation polynomial $\mathcal{I} = \mathcal{P}_{2^k-2}(x)$;
— non-bijective $k$-bit function $\psi$ which has no pre-image for 0;
— arbitrary permutation $h \in S(V_k)$,

we construct the following $2k$-bit vectorial Boolean function $\mathcal{G}$ from $V_{2k}$ to $V_{2k}$ as follows (Fig. 1).

**Construction of $\mathcal{G}$**

For the input value $(l\|r) \in V_{2k}$, we define the corresponding output value $\mathcal{G}(l\|r) = (l_1\|r_1)$, where
$l_1 = \mathcal{I}(l) \otimes \psi(l \otimes r)$;
$r_1 = h(r \otimes \psi(l \otimes r))$.

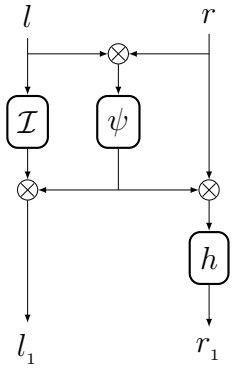

Fig. 1. High level structure of $\mathcal{G}$

The construction of $\mathcal{G}$ share similarities with 1-round of Lai-Massey structure replacing in the latter the XORs by finite field multiplications. The non-bijective $k$-bit function $\psi$ (which has no pre-image for 0) is chosen in such a way to make invertible the structure of $\mathcal{G}$. Moreover, from the following construction

$$\begin{aligned} \mathcal{G}^{-1}(l_1\|r_1) &= l\|r, \\ l &= h^{-1}(l_1) \otimes \mathcal{I}\big(\psi(h^{-1}(l_1) \otimes \mathcal{I}(r_1))\big), \\ r &= \mathcal{I}\big(r_1 \otimes \mathcal{I}\big(\psi(h^{-1}(l_1) \otimes \mathcal{I}(r_1))\big)\big) \end{aligned}$$

we can easy derive the bijectivity of $\mathcal{G}$ which is a necessary design criterion for SPN ciphers and quite useful for Feistel and Lai-Massey ciphers.

When $n = 8$, in correspondence with the suggested construction of $\mathcal{G}$, we need to construct the 4-bit non-bijective function $\psi$, the 4-bit permutation $h \in S(V_4)$ and the inversion function $\mathcal{I}$ over the finite field $\mathrm{GF}(2^4) = \mathrm{GF}(2)[\xi]/g(\xi)$, constructing the latter with the irreducible polynomial $g(\xi) = \xi^4 + \xi + 1 \in \mathrm{GF}(2)[\xi]$.

The main advantage offered by construction of $\mathcal{G}$ is that its allows to perform a search based on random generation of 4-bit non-bijective function $\psi$ and 4-bit permutation $h$ for finding 8-bit S-Boxes with actual cryptographic parameters. We have implemented the above construction in SAGE [1] obtaining as a result a lot of affine nonequivalent 8-bit permutations without fixed points with the following parameters:

— minimum degree — 7;
— graph algebraic immunity — 3 (with 441 equations);
— 6 and 8 — uniform;
— nonlinearity in range of 100 up to a value of 104.

### 1.1. Constructing involutions

In this section, we study how to build involutive S-Boxes with strong cryptographic properties using constructions presented in the previous section. Involutions, i.e. permutations with the property $\Phi \circ \Phi(x) = x$, have an particular interest in cryptography because in the case of lightweight block ciphers, these components are used to decrease the cost of the implementation of decryption process.

Exploring the construction of $\mathcal{G}$, we have found 8-bit involutions having few fixed points with the following properties:

— minimum degree — 7;
— graph algebraic immunity — 3 (with 441 equations);
— 6 and 8 — uniform;
— nonlinearity in range of 100 up to a value of 104.

Also, we have tried to design directly involutions without fixed points using our scheme. To achieve the fulfilment of condition $\Phi \circ \Phi(x) = x$, our strategy was to combine our constructions into two rounds. Choosing two arbitrary $k$-bit involutions $h_1, h_2$, the following constructions are able to produce $2k$-bit involutions with strong cryptographic properties (Fig. 2).

**Construction of $\mathcal{G}^{\text{invol}}$**

For the input value $(l\|r) \in V_{2k}$, we define the corresponding output value

$$\mathcal{G}^{\text{invol}}(l\|r) = \left(\mathcal{G}_2^* \circ \mathcal{G}_1^*\right)(l\|r) = l_1\|r_1, \text{ where}$$

$$\mathcal{G}^*{}_1(l\|r) = h_1(l \otimes \mathcal{I}(\psi(l \otimes r)))\Big\|h_2(l \otimes \psi(l \otimes r));$$

$$\mathcal{G}_2^*(l\|r) = \Big(l \otimes \psi(l \otimes r)\Big)\Big\|\Big(l \otimes \mathcal{I}(\psi(l \otimes r))\Big).$$

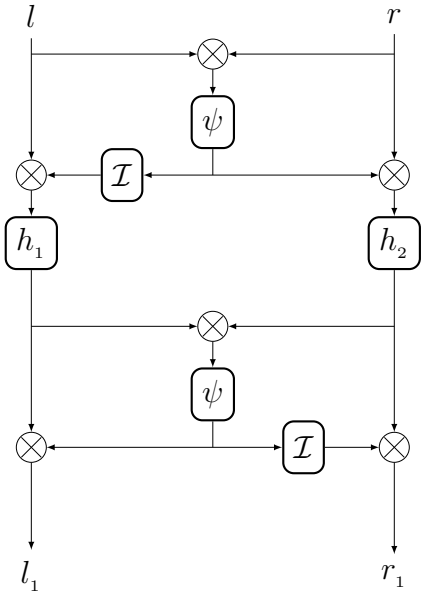


Fig. 2. Structure of $\mathcal{G}^{\text{invol}}$

As we can see from Fig. 2, the construction of $\mathcal{G}^{\text{invol}}$ represents a composition of two functions $\mathcal{G}_2^*$ and $\mathcal{G}_1^*$, each of which has similarities with 1-round of Lai-Massey scheme. The function $\mathcal{G}_2^*$ is chosen in such a way to make the whole structure an involution. In fact, by direct computations, it is not difficult to show that $\mathcal{G}^{\text{invol}} \circ \mathcal{G}^{\text{invol}}(x) = x$ for all $x \in V_{2k}$.

Implementing the construction of $\mathcal{G}^{\text{invol}}$ in SAGE [1], we have obtained affine non-equivalent 8-bit involutions without fixed points (in contrast to the construction of $\mathcal{G}$) with the following parameters:

— minimum degree — 7;

— 8 — uniform;

— graph algebraic immunity — 3 (with 441 equations);

— nonlinearity in range of 100 up to a value of 102.

The possibility of having no fixed points in those involutions constructed under the $\mathcal{G}^{\text{invol}}$ scheme has some significances. In fact, the cryptographic properties related to linear and differential cryptanalysis of involutions based on $\mathcal{G}$-construction are stronger in comparison with those generated by $\mathcal{G}^{\text{invol}}$.

### 1.2. Searching of highly-nonlinear orthomorphisms

In this section, we study the possibility of using ours methods to find permutations $\Phi$ such that $\Phi(x) \oplus x$ are permutations too. In the public literature, these permutations are called orthomorphisms. Orthomorphisms are pertinent to the construction of mutually orthogonal Latin squares and can be used to design check digit systems. In cryptography, applications of orthomorphisms of the group $(V_n, \oplus)$ are found in the construction of block ciphers, stream ciphers and hash functions (in the Lai — Massey scheme most famously in well-known FOX [2] family of block ciphers, Chinese stream cipher LOISS [3] and hash function EDON-R [4]). More recently, orthomorphisms have been used to strengthen the Even-Mansour block cipher against a cryptographic attack which makes the use of the nonuniformity of $\Phi(x) \oplus x$ when $\Phi$ is a random permutation [5].

Exploring and exploiting the construction of $\mathcal{G}$, we have found highly-nonlinear orthomorphisms with the following parameters:

— minimum degree — 7;

— 8 — uniform;

— graph algebraic immunity — 3 (with 441 equations);

— nonlinearity in range of 100 up to a value of 102.

### 1.3. Some examples

We include in Table some permutations generated by our method, one ordinary permutation with the best founded cryptographic parameters, two involutions and one orthomophism.

**Some constructed 8-bit S-Boxes**

| S-Box $\mathcal{G}_1$ | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| $\mathcal{NL}(\mathcal{G}_1) = 104$, $\delta(\mathcal{G}_1) = 6$, $\deg(\mathcal{G}_1) = 7$, $\mathcal{AI}_{\text{gr}}(\mathcal{G}_1) = 3$, $r^{(3)}_{\mathcal{G}_1} = 441$ | | | | | | | | | | | | | | | |
| 6e | e8 | 5f | a8 | 32 | 24 | a7 | 0e | 1d | 64 | 87 | 14 | c3 | 6f | 95 | 92 |
| fb | 4c | 82 | 99 | 3d | 19 | ac | 45 | 9f | fe | de | 15 | b9 | f9 | e2 | 8a |
| ec | f5 | 0d | ea | 3a | 77 | 47 | 12 | 11 | 01 | 97 | c5 | 13 | 10 | 81 | 9d |
| ed | 75 | 88 | 68 | fa | a4 | c0 | ca | ba | b2 | 3b | 61 | ae | 0a | 6c | 65 |
| d5 | 42 | 5d | dc | f2 | 85 | 9b | a6 | 67 | 50 | 63 | 91 | c7 | 34 | 80 | d7 |
| 96 | 1b | 8e | 5e | 94 | 2f | b1 | ad | a0 | 93 | 2c | 52 | d0 | 29 | 07 | c8 |
| 8d | 7f | 49 | 6b | 36 | 2e | d9 | e0 | 37 | cd | 83 | af | 6d | 57 | ce | b3 |
| 5c | c6 | 60 | d8 | 3f | e4 | 4f | ab | 56 | a1 | 72 | e7 | 69 | f1 | dd | 9c |
| 84 | 90 | 25 | 4b | 76 | 5a | 6a | da | f0 | e5 | 53 | 5b | 7e | 2a | 2b | d3 |
| 35 | a3 | 1c | a2 | 28 | 9e | 30 | a9 | b4 | 06 | 0b | ef | aa | 43 | e9 | 7d |
| e1 | 3e | 31 | 44 | 54 | db | 79 | c9 | 41 | fc | f7 | 66 | 7a | b7 | 51 | 38 |
| df | 62 | 40 | bb | 26 | 09 | f3 | cf | d2 | 1a | 20 | 0c | 04 | 16 | 33 | 22 |
| 4e | a5 | 58 | 9a | d6 | 02 | e6 | cb | be | eb | 86 | 7b | bd | d1 | 03 | f6 |
| ee | 8f | 0f | 55 | 8b | 4a | 7c | 23 | 2d | b6 | 1f | c2 | 17 | bf | 73 | 08 |
| cc | 70 | 1e | 59 | 46 | e3 | 27 | ff | 78 | b8 | 18 | 21 | d4 | bc | 98 | f4 |
| c1 | c4 | 74 | 39 | 89 | f8 | fd | 48 | 71 | 4d | b0 | 3c | 00 | 8c | b5 | 05 |

| Involution $\mathcal{G}_2$ | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| $\mathcal{NL}(\mathcal{G}_2) = 104$, $\delta(\mathcal{G}_2) = 6$, $\deg(\mathcal{G}_2) = 7$, $\mathcal{AI}_{\mathrm{gr}}(\mathcal{G}_2) = 3$, $r^{(3)}_{\mathcal{G}_2} = 441$ | | | | | | | | | | | | | | | |
| 00 | 10 | 90 | e0 | d0 | b0 | 70 | 60 | f0 | 20 | c0 | 50 | a0 | 40 | 30 | 80 |
| 01 | 11 | 19 | 85 | 2f | 2c | 8b | f5 | 2e | 12 | fa | 9a | 8c | 98 | fb | 93 |
| 09 | 2d | 4e | 3c | 47 | d5 | 36 | dc | 3b | 29 | db | 46 | 15 | 21 | 18 | 14 |
| 0e | b3 | b8 | 64 | b4 | 81 | 26 | 3f | 86 | 6b | 89 | 28 | 23 | 65 | 3e | 3 |
| 0d | 87 | 8a | 63 | 6c | 9c | 2b | 24 | 66 | 4f | 96 | 9b | 83 | 4d | 22 | 49 |
| 0b | ad | 62 | be | 61 | 5c | b7 | a8 | 69 | b2 | a3 | 5b | 55 | ed | e1 | e9 |
| 07 | 54 | 52 | 43 | 33 | 3d | 48 | 67 | c2 | 58 | 6e | 39 | 44 | cc | 6a | cb |
| 06 | bd | bf | 7c | aa | e2 | 76 | df | a5 | b9 | dd | e4 | 73 | ee | de | a9 |
| 0f | 35 | c6 | 4c | c3 | 13 | 38 | 41 | c8 | 3a | 42 | 16 | 1c | 8e | 8d | 8f |
| 02 | 94 | 92 | 1f | 91 | d7 | 4a | e7 | 1d | d3 | 1b | 4b | 45 | d6 | ea | e5 |
| 0c | c1 | c9 | 5a | cd | 78 | ab | f9 | 57 | 7f | 74 | a6 | ac | 51 | fd | ff |
| 05 | c4 | 59 | 31 | 34 | b5 | cf | 56 | 32 | 79 | bb | ba | ce | 71 | 53 | 72 |
| 0a | a1 | 68 | 84 | b1 | c7 | 82 | c5 | 88 | a2 | ca | 6f | 6d | a4 | bc | b6 |
| 04 | f6 | d8 | 99 | d4 | 25 | 9d | 95 | d2 | fc | fe | 2a | 27 | 7a | 7e | 77 |
| 03 | 5e | 75 | e3 | 7b | 9f | e8 | 97 | e6 | 5f | 9e | f1 | f2 | 5d | 7d | f7 |
| 08 | eb | ec | f4 | f3 | 17 | d1 | ef | f8 | a7 | 1a | 1e | d9 | ae | da | af |

| Involution $\mathcal{G}_3^{\mathrm{invol}}$ | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| $\mathcal{NL}(\mathcal{G}_3^{\mathrm{invol}}) = 100$, $\delta(\mathcal{G}_3^{\mathrm{invol}}) = 8$, $\deg(\mathcal{G}_3^{\mathrm{invol}}) = 7$, $\mathcal{AI}_{\mathrm{gr}}(\mathcal{G}_3^{\mathrm{invol}}) = 3$, $r^{(3)}_{\mathcal{G}_3^{\mathrm{invol}}} = 441$ | | | | | | | | | | | | | | | |
| a0 | af | 61 | 7b | 5e | 2f | 12 | 27 | be | 38 | b6 | 6a | 76 | 33 | 71 | 36 |
| 80 | 67 | 06 | a4 | e4 | 59 | 17 | 16 | 9d | 6e | d5 | 51 | de | ec | a7 | 93 |
| 40 | 37 | 78 | 9e | d9 | fa | ff | 07 | 58 | 3e | 9c | b1 | b2 | 3f | d6 | 05 |
| 90 | 6c | e9 | 0d | a1 | 75 | 0f | 21 | 09 | 74 | b7 | 69 | ea | bc | 29 | 2d |
| 20 | a3 | f1 | ed | b3 | db | c4 | fc | df | 8e | bf | e7 | c2 | 8f | a5 | 8d |
| 70 | 1b | 62 | cf | bd | f4 | 89 | cc | 28 | 15 | 87 | f8 | f3 | 63 | 04 | b8 |
| d0 | 02 | 52 | 5d | 86 | ce | 77 | 11 | 83 | 3b | 0b | aa | 31 | a8 | 19 | cb |
| 50 | 0e | 96 | 7c | 39 | 35 | 0c | 66 | 22 | 88 | 9f | 03 | 73 | da | 8c | d7 |
| 10 | e2 | c6 | 68 | fd | cd | 64 | 5a | 79 | 56 | eb | f5 | 7e | 4f | 49 | 4d |
| 30 | c7 | ca | 1f | c5 | a9 | 72 | 9b | f2 | f6 | ad | 97 | 2a | 18 | 23 | 7a |
| 00 | 34 | c9 | 41 | 13 | 4e | e6 | 1e | 6d | 95 | 6b | e8 | e3 | 9a | c3 | 01 |
| e0 | 2b | 2c | 44 | c1 | d4 | 0a | 3a | 5f | c8 | d2 | d8 | 3d | 54 | 08 | 4a |
| f0 | b4 | 4c | ae | 46 | 94 | 82 | 91 | b9 | a2 | 92 | 6f | 57 | 85 | 65 | 53 |
| 60 | d3 | ba | d1 | b5 | 1a | 2e | 7f | bb | 24 | 7d | 45 | e1 | e5 | 1c | 48 |
| b0 | dc | 81 | ac | 14 | dd | a6 | 4b | ab | 32 | 3c | 8a | 1d | 43 | fe | f7 |
| c0 | 42 | 98 | 5c | 55 | 8b | 99 | ef | 5b | fb | 25 | f9 | 47 | 84 | ee | 26 |

| Orthomorphism $\mathcal{G}_4$ | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| $\mathcal{NL}(\mathcal{G}_4) = 102$, $\delta(\mathcal{G}_4) = 8$, $\deg(\mathcal{G}_4) = 7$, $\mathcal{AI}_{\mathrm{gr}}(\mathcal{G}_4) = 3$, $r^{(3)}_{\mathcal{G}_4} = 441$ | | | | | | | | | | | | | | | |
| a1 | f9 | 70 | 7e | a7 | c2 | 12 | d2 | 88 | ed | 62 | d5 | 2a | 2e | 08 | 79 |
| c6 | fc | b0 | 90 | ba | de | cc | 66 | 58 | c1 | 5b | 00 | 15 | e0 | 64 | 25 |
| 37 | f8 | 9e | 28 | 83 | 4e | 17 | 7d | 16 | a2 | 67 | 2b | 7a | 29 | 57 | a9 |
| 31 | f7 | e2 | b6 | 21 | 98 | 6a | d1 | 92 | 71 | 74 | 97 | 85 | 8d | 0a | e3 |
| 18 | f4 | be | a0 | 1b | 32 | 39 | 27 | 80 | db | 6e | 0e | d4 | d6 | 5e | 61 |
| 65 | f5 | ce | a6 | 6d | 50 | 5c | 6c | 4b | 36 | 19 | 0b | 02 | eb | c4 | 8b |
| 33 | f2 | 82 | e1 | ec | ab | 13 | c7 | 9a | 73 | b7 | 8a | a3 | 9d | 89 | 45 |
| 72 | fb | b8 | 35 | 3b | c8 | d9 | 1e | 48 | d0 | 68 | e4 | 30 | c3 | 1a | 24 |
| 8e | f1 | 46 | 9c | 2c | 01 | 07 | cd | b5 | 3d | 03 | 54 | ac | bb | 43 | 8c |
| 51 | f3 | 6b | 40 | 26 | bd | e8 | b2 | 05 | 76 | 0d | 4c | 11 | e6 | b3 | 86 |
| c5 | f6 | b4 | 94 | dc | 60 | 55 | 56 | 44 | 47 | cb | 69 | 53 | 7c | 38 | 84 |
| 52 | fa | e7 | 81 | 2d | 42 | 1d | dd | ea | 96 | ee | 87 | ad | 0c | 20 | 93 |
| 3a | fe | 3c | 78 | 77 | ca | 23 | da | a4 | 22 | b9 | e9 | 91 | ae | 5a | a8 |
| d8 | f0 | 9b | 5d | 14 | c9 | aa | 3e | 49 | 10 | d7 | 09 | 34 | 7b | 59 | 1c |
| 6f | ff | 8f | 2f | 3f | 0f | cf | 5f | ef | 1f | 4f | 9f | df | af | bf | 7f |
| 4a | fd | 06 | 95 | d3 | b1 | 63 | 99 | c0 | 75 | 4d | bc | a5 | e5 | 41 | 04 |

## 2. Conclusion and Future Work

In this work, we have presented a new algorithmic-algebraic scheme based in the Lai — Massey structure for constructing permutations of dimension $n = 2k$, $k \geqslant 2$. For the common case $k = 8$, we have obtained new cryptographically strong 8-bit permutations having better resistance to algebraic attacks in comparison with the inversion function in $\mathrm{GF}(2^8)$ which so far has the best-known values for nonlinearity and differential uniformity. Compared to the best nonlinearity (108, for $k = 4$) offered by the construction presented in [6] and later generalized in [7], the nonlinearity for the permutations obtained by our scheme slightly decrease up to 104, but to the best of our knowledge the schemes presented in [6, 7] can not produce involutions and orthomorphisms with strong cryptographic properties, so we can conclude that the new structure presented in this work is more powerful and attractive due to the diversity of permutations that can be constructed. Interestingly, the involutions and orthomorphisms founded in this work have comparable classical cryptographic properties like those constructed by using spectral-linear and spectral-difference methods [8]. The main advantage of our 8-bit permutations is that they can be constructed using smaller 4-bit components which could be useful for the implementation of the S-Box in hardware or using a bit-sliced approach. We only presented a new scheme that can help to find permutations, involutions and orthomophisms with rather good cryptographic properties. There are several questions (theoretical results, hardware and bit-sliced implementations, efficient methods of masking) about the construction suggested in this work which are left as future work.

REFERENCES

1. `http://www.sagemath.org`. Sage Mathematics Software (Version 8.1). 2018.
2. *Vaudenay S. and Junod P.* Fox, a New Family of Block Ciphers. `http://crypto.junod.info/sac04a.pdf`. 2004.
3. *Feng D., Feng X., Zhang W., et al.* Loiss: a byte oriented stream cipher. LNCS, 2011, vol. 6639, pp. 109–125.
4. *Gligoroski D., Odegard R. S., Mihova M., et al.* Cryptographic hash function Edon-R. Proc. IWSCN, Trondheim, 2009, pp. 1–9.
5. *Gilboa Sh. and Gueron Sh.* Balanced Permutations Even-Mansour Ciphers. Cryptology ePrint Archive, Report 2014.
6. *De la Cruz Jiménez R. A.* Generation of 8-bit S-Boxes Having Almost Optimal Cryptographic Properties Using Smaller 4-bit S-Boxes and Finite Field Multiplication. 2017. `www.cs.haifa.ac.il/orrd/LC17/paper60.pdf`.
7. *Fomin D.* New classes of 8-bit permutations based on a butterfly structure. Pre-proc. CTCrypt'18-Suzdal, 2016, pp. 199–211.
8. *Menyachikhin A.* Spectral-linear and spectral-difference methods for generating cryptographically strong S-Boxes. Pre-proc. CTCrypt'16-Yaroslavl, 2016, pp. 232–252.

UDC 621.391:519.7 DOI 10.17223/2226308X/12/43

# SOME PROPERTIES OF THE OUTPUT SEQUENCES OF COMBINED GENERATOR OVER FINITE FIELDS

Aulet R. Rodriguez

The sequences are an important part of the cryptography and analysis of their properties is of great interest. In this paper, the following characteristics of combined

generator are analyzed: period of output sequences and the distribution of elements in the output sequences over finite field.

**Keywords:** *finite field, correlation-immune function, resilient function, balanced function, combined generator.*

## Introduction

The randomness is an important property in the cryptographic scheme. One of the components that ensure this property is the random sequence that is built by generators. The elements of random sequences can be used as initialization vectors, in cyclic codes, as keys in block cipher, and in stream cipher. The combined generator presents one class of generators that are used to obtain pseudorandom sequence. Examples of its use are stream ciphers: A.1 of standard GSM [1], Grain, Trivium [2]. The most results belong to generators over the field GF(2) [1, 3, 4].

In this work, we analyze the following characteristics for combined generator: period of the output sequence and distribution elements in output sequence over finite field.

Let $P = \mathrm{GF}(q)$ be a finite field with $q$ elements, $F_1(x), \ldots, F_k(x)$ be polynomials with coefficients in $P$ of degrees $m_1, \ldots, m_k$ respectively. We assume that $F_1(x), \ldots, F_k(x)$ are primitive polynomials [5], also $\gcd(m_i, m_j) = 1$ for each $i \neq j$. For each function $\varphi : P^k \to P$, we consider the combined generator [1, 6, 7] with the output sequence

$$v(i) = \varphi(u_1(i), u_2(i), \ldots, u_k(i)), \quad i \geqslant 0,$$

where $u_j$ is a linear recurring sequence over $P$ with minimal polynomial $F_j(x)$.

## 1. Period

In [6] the general bounds for the period of combined generator and the exact equality in the case GF(2) is presented. In this work, we give bounds for the period of a given generator for one class of function over any finite field and show, how this period can be calculated.

**Theorem 1.** If $\varphi$ has the form

$$\varphi(x_1, \ldots, x_k) = \sum_{s=1}^{k} \sum_{1 \leqslant i_1 < i_2 < \ldots < i_s \leqslant k} c_{i_1 i_2 \ldots i_s} x_{i_1} x_{i_2} \ldots x_{i_s},$$

then period $T(v)$ of sequence $v$ satisfies the conditions

$$\frac{(q^{m_1} - 1) \ldots (q^{m_k} - 1)}{(q-1)^k} \,\Big|\, T(v) \quad \text{and} \quad T(v) \,\Big|\, \frac{(q^{m_1} - 1) \ldots (q^{m_k} - 1)}{(q-1)^{k-1}}.$$

**Theorem 2.** In conditions of theorem 1, if $b_i = F_i(0)(-1)^{m_i}$, $i = 1, \ldots, k$, and $m = m_1 \ldots m_k$, then

$$T(v) = \frac{(q^{m_1} - 1) \ldots (q^{m_k} - 1)}{(q-1)^k} d,$$

where $d = \mathrm{lcm}(\mathrm{ord}(b_{i_1}^{m/m_{i_1}} \ldots b_{i_s}^{m/m_{i_s}}) : c_{i_1 i_2 \ldots i_s} \neq 0)$. Moreover, $d$ is the minimal number in $\mathbb{N}$ for which

$$\varphi(x_1, \ldots, x_k) = \varphi(b_1^{dm/m_1} x_1, \ldots, b_k^{dm/m_k} x_k).$$

**Corollary 1.** In conditions of theorem 1, if exist such $i_1, \ldots, i_k$ for which $b_{i_1}^{m/m_{i_1}} \ldots b_{i_s}^{m/m_{i_s}}$ is a primitive element or function $\varphi(x_1, \ldots, x_k)$ is linear in variables $x_1$, …, $x_k$, then

$$T(v) = \frac{(q^{m_1} - 1) \ldots (q^{m_k} - 1)}{(q-1)^{k-1}}.$$

## 2. Frequencies

For each element $c \in P^*$, we define the following function $\psi_c : P^k \to \mathbb{C}^*$, where $\mathbb{C}^*$ is multiplicative group of complex numbers, as follows

$$\psi_c(x_1, \ldots, x_k) = \chi(c\varphi(x_1, \ldots, x_k)),$$

where $\chi$ is character of $(P, +)$, $\chi(x) = e^{2\pi i \mathrm{tr}_{P_0}^P(x)/p}$, for all $x \in P$, $P_0 = \mathrm{GF}(p)$ is the prime field and $\mathrm{tr}_{P_0}^P(x)$ is the trace of $x$ over $P_0$. For every function $\psi : P^k \to \mathbb{C}^*$, it is shown [8], that, for any $(x_1, \ldots, x_k) \in P^k$,

$$\psi_c(x_1, \ldots, x_k) = \frac{1}{q^k} \sum_{\mathbf{a} \in P^k} W_\psi(\mathbf{a}) \chi_{\mathbf{a}}(x_1, \ldots, x_k), \quad W_{\psi_c}(\mathbf{a}) = \sum_{\mathbf{b} \in P^k} \psi_c(\mathbf{b}) \overline{\chi}(\mathbf{ab}),$$

where $\overline{\chi}$ is the conjugate character.

The class of correlation-immune and resilient function over any field is defined in [9]. In this work, we analyze $(k-1)$-resilient function. We shall calculate the value

$$N_l(z, v) = |\{i \in \{0, \ldots, l-1\} : v(i) = z\}|,$$

where $l \in \mathbb{N}$, $l \leqslant T = (q^{m_1} - 1) \ldots (q^{m_k} - 1)/(q-1)^{k-1}$.

**Theorem 3.** If $\varphi(x_1, \ldots, x_k)$ is $(k-1)$-resilient function and $m = m_1 + \cdots + m_k$, then

$$\left| N_l(z, v) - \frac{l}{q} \right| \leqslant \frac{(q-1)^{(k+2)/2}}{q} C_l,$$

where

$$C_l = \begin{cases} \left( \dfrac{4}{\pi^2} \ln(T) + \dfrac{9}{5} \right) q^{m/2}, & \text{if } l < T, \\ (q^m - T)^{1/2}, & \text{if } l = T. \end{cases}$$

**Corollary 2.** If $\varphi(x_1, \ldots, x_k) = a_1 x_1 + \ldots + a_k x_k$, then

$$\left| N_l(z, v) - \frac{l}{q} \right| \leqslant \frac{q-1}{q} C_l.$$

For a linear function the Niederreiter's bounds [10, theorem 2] are better than our bounds in whole period. But for to use the Niederreiter's bounds, it is necessary to know the whole period, in practice we have only an interval of the period, which makes our bounds more accurate in the latter case. Now, we shall show that, in general, for other $(k-1)$-resilient functions we can use our bounds when the Niederreiter's bounds does not work, or vice-versa.

Denoting by $R_{k-1}$ the set of all $(k-1)$-resilient functions, in $R_{k-1}$ we define the binary relation $\sim$ as follows:

$$\forall \varphi_1, \varphi_2 \in R_{k-1} \Big( \varphi_1 \sim \varphi_2 \Leftrightarrow$$

$$\Leftrightarrow \exists \text{ permutation } \pi \left( \forall (x_1, \ldots, x_k) \in P^k \left( \varphi_2(x_1, \ldots, x_k) = \pi(\varphi_1(x_1, \ldots, x_k)) \right) \right) \Big).$$

This relation is an equivalence. If we can determine the period and the distribution of elements for the function $\varphi_1$, we can also make it for the function $\varphi_2$. Let us show that it cannot always take the function linear like representatives of the classes.

**Proposition 1.** Let $P = \mathrm{GF}(2^2)$, $\varphi(x_1, x_2) = x_1^2 + x_2$. A permutation polynomial $\pi(x)$ and $a_1, a_2$ for which $\pi(\varphi(x_1, x_2)) = a_1 x_1 + a_2 x_2$, do not exist.

For function $\varphi$ in proposition 1, it is necessary to use the bound of theorem 3. But if $\varphi(x_1, x_2) = x_1^2 + x_2^2$, we can use the Niederreiter's bounds.

REFERENCES

1. *Alferov A. P., Zubov A. Y., Kuz'min A. S., and Cheremushkin A. V.* Osnovy kriptografii [Basics of Cryptography]. Moscow, Gelios ARV Publ., 2001. (in Russian)
2. *Matthew R. and Oliver B.* New Stream Ciphers Designs. Springer, 2008.
3. *Andreas K.* Stream Cipher. Springer, 2013.
4. *Bilyak I. B. and Kamlovskii O. V.* Chastotnye kharakteristiki tsiklov vykhodnykh posledovatel'nostey kombiniruyushchikh generatorov nad polem iz dvukh elementov [The frequency characteristics of cycle of output sequences combining generator over the field of two elements]. Prikladnaya Diskretnaya Matematika, 2015, no. 3(29), pp. 17–31. (in Russian)
5. *Lidl R. and Niederreiter H.* Finite Fields. Encyclopedia of Mathematics and its Applications. Cambridge University Press, 1997.
6. *Fomichev V. M.* Fomichev V.M. Diskretnaya matematika i kriptologiya Diskretnaya matematika i kriptologiya [Discrete Mathematics and Cryptology. Moscow, Dialog-MEPhI Publ., 2010. (in Russian)
7. *Rueppel R. A.* Analysis and Design of Stream Ciphers. Springer Verlag, 1986.
8. *Kamlovskii O. V.* Kolichestvo poyavleniy elementov v vykhodnykh posledovatel'nostyakh fil'truyushchikh generatorov [Distribution properties of sequences produced by filtering generators]. Prikladnaya Diskretnaya Matematika, 2013, no. 3(21), pp. 11–25. (in Russian)
9. *Camion P. and Canteaut A.* Correlation-Immune and Resilient Function over a Finite Alphabet and Their Application in Cryptography. Springer, 1998.
10. *Niederreiter H.* Weights of cyclic codes. Information and Control, 1997, vol. 34, pp. 130–140.

UDC 003.26 DOI 10.17223/2226308X/12/44

# DISCRETE LOGARITHM FOR NILPOTENT GROUPS AND CRYPTANALYSIS OF POLYLINEAR CRYPTOGRAPHIC SYSTEM[1]

V. A. Roman'kov

We present an efficient algorithm to compute a discrete logarithm in a finite nilpotent group, or more generally, in a finitely generated nilpotent group. Special cases of a finite $p$-group ($p$ is a prime) and a finitely generated torsion free nilpotent group are considered. Then we show how the derived algorithm can be generalized to an arbitrary finite or finitely generated nilpotent group respectively. We suppose that group is presented by generating elements and defining relators or as a subgroup of a triangular matrix group over a prime finite field (in finite case) or over the ring of integers (in torsion-free case). On the base of the derived algorithm we give a cryptanalysis of some schemes of polylinear cryptography known in the literature.

**Keywords:** *discrete logarithm, nilpotent group, polylinear system, cryptanalysis.*

## Introduction

Let $G$ be a group. We say that the *discrete logarithm* is (efficiently) *computable* in $G$ if there is an efficient algorithm that finds an exponent $x \in \mathbb{Z}$ for any expression of the form $f = g^x$, where $g, f \in G$. The problem of determining $x$ given $g$ and $f = g^x$ is called the *discrete logarithm problem* in $G$. The classical Diffie — Hellman exchange protocol, the ElGamal system and many other cryptographic schemes, protocols and systems are based

[1]The author is supported by RFBR, project No. 18-41-550001a.

on assumption about difficult solvability of the discrete logarithm problem in the groups chosen as platforms for them. See for examples [1 – 3].

Most of these schemes, protocols and systems use abelian groups as platforms. Multiplicative groups of finite fields and groups of elliptic curves over finite fields are most popular for this using. The security of currently popular algorithms relies on one of three hard mathematical problem: the integer factorization problem, the discrete logarithm problem on the multiplicative group of a finite field or the elliptic-curve discrete logarithm problem.

It turned out that main of public-key algorithms can be efficiently broken by a sufficiently strong hypothetical quantum computer. Shor [4] and Grover [5] algorithms provided a quantum way to break a many of public-key protocols. Even though current, publicly known, quantum computers lack processing power to break any real cryptographic algorithm, the cryptographic community take a great attention on constructing of new so-called *post-quantum* cryptographic algorithms that based on non-commutative algebraic structures. Now the *Post-Quantum Cryptography* is a specific area for investigation. Most popular cryptographic platforms in this new area are: matrix groups, nilpotent and polycyclic groups, Artin braid groups, some other infinite abstract groups, and so on. See [6, 7] for survey of the current state of this area. Cryptographic analysis of the main algorithms of algebraic cryptography can be found in [8 – 13].

In this paper, we consider the discrete logarithm problem in a finite nilpotent group, specifically, in a group $\mathrm{UT}(n, \mathbb{F}_p)$ of unitriangular $n \times n$ matrices over a prime finite field $\mathbb{F}_p$ of characteristic $p$. We introduce an efficient algorithm that solves the problem by computing the discrete logarithm in any finite nilpotent group. This approach can be applied to computing of the discrete logarithm in any finitely generated nilpotent group, in particular, this algorithm can be applied to a group $\mathrm{UT}(n, \mathbb{Z})$ of unitriangular matrices over the ring $\mathbb{Z}$ of integers.

Since every finite nilpotent group $G$ is a direct product of its Sylow $p$-subgroups for $p \in \pi(G)$, in the finite case, it is sufficient to describe an algorithm in the case when $G$ is a finite $p$-group for a prime $p$. Then a corresponding version the Chinese Remainder Theorem allows to compute the discrete logarithm in any finite nilpotent group. Any finitely generated torsion free nilpotent group has a finite normal central series with free abelian of a finite rank quotients, also it embeds into $\mathrm{UT}(n, \mathbb{Z})$ for suitable $n$. All elements of finite orders in a finitely generated nilpotent group $G$ forms a finite subgroup $T = T(G)$ (*torsion subgroup*). Then $G_0 = G/T$ is torsion-free, and we can use $G_0$ and $T$ to obtain a generalization of the constructed algorithm to any finitely generated nilpotent group. Fundamentals of the theory of nilpotent groups see, for example, in [14 – 16], a short introduction can be found in [17].

Note that matrix groups, as one of the most widely studied classes of non-abelian groups, were considered as suitable platforms for algorithms of the group-based cryptography from the very begiinning. In [18] and in some of other papers, different authors proposed (using the Jordan theory) to reduce the discrete logarithm problem for a matrices to the simultaneous discrete logarithm problem for some extension of the underlined field. This approach does not work in the case when all characteristic numbers are 1, as in the case of unitriangular matrices. So we need in different approaches to solve this specific case.

## 1. The discrete logarithm in a nilpotent group

Let $G$ be a finite $p$-group. Consider a normal series

$$G = G_0 > G_1 > \ldots > G_k = 1, \tag{1}$$

where $G_{i+1} = G_i^p G_i'$, $i = 0, \ldots, k-1$. Here $G_i^p = \mathrm{gp}(g^p : g \in G_i)$ and $G_i'$ is the derived subgroup of $G_i$ generated by all commutators of the form $[g, f] = g^{-1}f^{-1}gf$, $g, f \in G_i$. Any quotient $B_i = G_i/G_{i+1}$ is an elementary abelian $p$-group of a rank $r_i$, i.e., is a direct product $\prod_{j=1}^{r_i} C_j(p)$, $C_j(p) \simeq C_p$, where $C_p$ is a cyclic group of order $p$.

For any $g \in G$, we have that $g^p \in G_1$, and inductively, that $g^{p^l} \in G_l$, hence $g^{p^k} = 1$. Suppose that

$$g^x = f, \tag{2}$$

where $g, f$ are known elements of $G$ and $x$ ($x \in \mathbb{N}$, $1 \leqslant x < |g|$) is unknown exponent. Here $|g|$ denotes an order of $g$. We'll compute $x$ in the form

$$x = x_0 + x_1 p + \ldots + x_{k-1}p^{k-1}, \text{ where } 0 \leqslant x_i \leqslant p, \ i = 0, 1, \ldots, k-1.$$

**Algorithm**

1) For any $h \in G$, $\bar{h}$ means a standard image of $h$ in $B_0$. Suppose that $\bar{f} \neq 1$, then $\bar{g} \neq 1$, and $\bar{g}^{x_0} = \bar{f}$. This exponent $x_0$ is uniquely computed by usual computation with vectors in $B_0$. Then we set $g_1 = g^p$, $f_1 = g^{-x_0}f \in G_1$ and reduce our computation to equation
$$g_1^{(x-x_0)/p} = f_1$$
in $G_1$.
If $\bar{f} = 1$ and $\bar{g} = 1$, then $g, f \in G_1$ from the beginning and we continue with equation
$$g^{x - x_{k-1}p^{k-1}} = f$$
in $G_1$ because in this case $g^{p^{k-1}} = 1$.
If $\bar{f} = 1$ ($f \in G_1$) and $\bar{g} \neq 1$, then we have $x_0 = 0$, we set $g_1 = g^p \in G_1$ and continue with equation
$$g_1^{x/p} = f$$
in $G_1$.
2) Continuing this process we obtain a solution $x = \log_g(f)$.

In a specific case, when $G = \mathrm{UT}(n, \mathbb{F}_p)$ series (1) is as follows: $G_i$ ($i = 1, \ldots, n-1$) consists of all matrices with zero first $i$ diagonals above the main diagonal. Since each finite $p$-group embeds into $\mathrm{UT}(n, \mathbb{F}_p)$ for suitable $n$ one can apply the described above algorithm to the corresponding matrix group $\mathrm{UT}(n, \mathbb{F}_p)$. Note that we compute the minimal discrete logarithm $x$.

Now let $G$ be a finite nilpotent group. Then $G$ is a direct product $\prod_{p \in \pi(G)} G_p$, where $G_p$ denotes Sylow $p$-subgroup of $G$. Let $g = \prod_{p \in \pi(G)} g_p$ and $f = \prod_{p \in \pi(G)} f_p$ be expressions of $g$ and $f$ respectively as elements of this direct product. Let $x_p$ be a solution of $g_p^{x_p} = f_p$ in $G_p$, $p \in \pi(G)$. A solution $x$ of (2) can be efficiently computed by the Chinese Remainder Theorem as a solution of the following system of equations:

$$x = x_p \pmod{p^{t_p}}, \text{ where } p^{t_p} \text{ is order of } g_p, \ p \in \pi(G).$$

Similar algorithm works for any group $\mathrm{UT}(n, \mathbb{Z})$, and so for every finitely generated torsion free nilpotent group $G$, because every such group embeds into $\mathrm{UT}(n, \mathbb{Z})$ for sufficiently large $n$. Also, we can use a central series of $G$ with torsion free quotients, that are free abelian groups of finite ranks.

Let $G$ be a finitely generated nilpotent group and let $T = T(G)$ be its the torsion subgroup consisting of all elements of finite order, which is known is finite. The elements $g$ and $f$ in (2) simultaneously lie or not in $T$. If $g, f \in T$, we apply the algorithm to compute $x$ in finite group $T$. If $g, f \notin T$, then exponent $x$ is uniquely determined for the corresponding equation $\bar{g}^x = \bar{f}$ in torsion free group $\bar{G} = G/T$. Hence we succeeded again.

## 2. Applications

In recent years polylinear (in other words, multilinear) maps attracted attention of cryptographers. Now it is a new hot topic in cryptography because they offer a significant number of applications. The main open problem in this area is constructing a secure and efficiently computable polylinear map. The idea has been first proposed by D. Boneh and A. Silverberg [19], see also [20 – 22]. In [23], the authors proposed two polylinear protocols using finite $p$-groups as platforms, in which the security is based on the chosen discrete logarithm problem. Below we describe these two protocols and give a cryptanalysis to show a vulnerability of them.

At first, we will introduce the idea of a *cryptographic polylinear map*. Let $C_p(1)$ and $C_p(2)$ be two cyclic groups of prime order $p$. Let

$$\alpha : C_1(p) \times \ldots \times C_1(p) \to C_2(p)$$

be a non-degenerate polylinear map. Here non-degenerate means that if $g(1)$ is generator for $C_p(1)$, then $\alpha(g(1), \ldots, g(1))$ is a generator $g(2)$ for $C(2)$. Polylinear means that

$$\alpha(g_1^{k_1}, \ldots, g_n^{k_n}) = \alpha(g_1, \ldots, g_n)^{k_1 \ldots k_n} \text{ for any } g_1, \ldots, g_n \in C_p(1).$$

More generally, we can define a polylinear map as

$$\alpha : G_1 \times \ldots \times C_n \to G,$$

where $G_1, \ldots, G_n, G$ are arbitrary groups such that

$$\alpha(g_1^{k_1}, \ldots, g_n^{k_n}) = \alpha(g_1, \ldots, g_n)^{k_1 \ldots k_n} \text{ for any } g_i \in G_i,\ i = 1, \ldots, n,$$

with some natural non-degeneracy property.

Obviously, that a polylinear map with good cryptographic properties, namely, efficient computability of main operations in both the groups $C_p(i)$, $i = 1, 2$, efficient computability of $\alpha$ and difficult the discrete logarithm problem in $C_p(1)$, can be used in constructing cryptographic schemes. For example, a version of the famous Diffie — Hellman protocol can be based on a polylinear map.

Now we will consider two protocols proposed in [23].

**Protocol 1.**

Let $A_1, \ldots, A_{n+1}$ be the users. They choose a public nilpotent group $G$ of nilpotency class $n > 1$. Denote inductively simple commutators on elements of $G$ as follows. An usual commutator $[g_1, g_2]$ is said to be *simple of length* 2. Suppose that $[g_1, \ldots, g_q]$ is a simple commutator of length $q$, then $[[g_1, \ldots, g_q], g_{q+1}]$ is *simple commutator of length* $q+1$. A group $G$ is *nilpotent of nilpotency class* $n$ if every simple commutator of length $n+1$ is 1 and $n$ is minimal with this property. Then the following identity is true.

For any $l_i \in \mathbb{N}$, $i = 1, \ldots, n$, and any tuple $(g_1, \ldots, g_n)$ of elements of $G$

$$[g_1^{l_1}, \ldots, g_n^{l_n}] = [g_1, \ldots, g_n]^l \text{ for } l = \prod_{i=1}^{n} l_i.$$

The key exchange works as follows:

— The users $A_j$'s choose in random positive integers $k_j$, $j = 1, \ldots, n+1$, respectively, and transmit in public channel elements $g_i^{k_j}$ for $i = 1, \ldots, n$.

— The user $A_j$ computes $[g_1^{k_1}, \ldots, g_{j-1}^{k_{j-1}}, g_{j+1}^{k_{j+1}}, \ldots, g_n^{k_n}]^{k_j} = [g_1, \ldots, g_n]^k$, $k = \prod\limits_{j=1}^{n+1} k_j$.

— $K = [g_1, \ldots, g_n]^k$ is the exchanged-key.

**Cryptanalysis.** By any pair of public elements $g_j, g_j^{k_j}$ we efficiently compute $\tilde{k}_j$ such that $g_i^{\tilde{k}_j} = g_i^{k_j}$ by the algorithm described in Section 1. Then we can compute $K$ as $A_j$'s does. A possible difference between $k_j$ and $\tilde{k}_j$ obviously does not matter.

**Protocol 2.**

Let the users $A_1, \ldots, A_{n+1}$ choose a public nilpotent group $G$ of nilpotency class $n > 1$ as above. In addition, $G$ should be non-$n$-Engel group. It means that there are elements $f$ and $g$ such that the simple commutator $[f, g; n] = [f, g, \ldots, g]$ of length $n+1$ is not 1.

The key exchange works as follows.

— The users $A_j$'s choose in random elements $k_j$, respectively, $j = 1, \ldots, n+1$, and transmit in public channel elements $g^{k_j}$ for $j = 1, \ldots, n+1$.

— The user $A_j$ computes

$$[f^{k_j}, g^{k_1}, \ldots, g^{k_{j-1}}, g^{k_{j+1}}, \ldots, g^{k_{n+1}}] = [f, g; n]^k, \ k = \prod_{j=1}^{n+1} k_j.$$

— $K = [f, g; n]^k$ is the exchanged-key.

**Cryptanalysis.** By any pair of elements $g, g^{k_j}$ we efficiently compute $\tilde{k}_j$ such that $g^{\tilde{k}_j} = g^{k_j}$ by the algorithm described in Section 1. Then we can compute $K$ as $A_j$'s does. A possible difference between $k_j$ and $\tilde{k}_j$ obviously does not matter in this case too.

**Remark 1.** Considering the Protocols 1 and 2 above we supposed that elements of the plaform group are written either as words on given generators, or as matrices in the matrix setting. In [23], the authors do not explain what is the form of expression of an element. Note, that we assume that we can efficiently compute an exponent in any expression of the form $g^x = f$ in an elementary abelian $p$-group. Obviously, we can if elements of this group are written as vectors over $\mathbb{F}_p$. It is possible for both of the forms of expressing of elements we talk about.

In [23], the authors proposed the following group as platform. Take $q = 2p^3 + 1$ where $p$ and $q$ are large primes. Let $X = \mathrm{gp}(x)$ and $Y = \mathrm{gp}(y)$ be the subgroups of $\mathbb{F}_q^*$ of orders $p^3$ and $p^2$, respectively. Selecting a nontrivial automorphism $\alpha$ of $X$ amounts to choose a positive integer $m < p^3$, relatively prime to $p$, such that $\alpha(x) = x^m$. Define $G = Y \rtimes_\alpha X$, that is a semidirect product of $X$ by $Y$. We identify $x$ with $(1, x)$ and $y$ with $(y, 1)$. Suppose that $m = p + 1$. Then we have for $G$ the following presentation:

$$G = \langle x, y : x^{p^3} = y^{p^2} = 1, x^y = x^{p+1} \rangle.$$

Then $G$ is a finite $p$-group of order $p^5$ and nilpotency class 3, which is not 2-Engel.

The group $G$ is suggested as a platform for Protocols 1 and 2 for 4 and 3 users, respectively.

Consider for example Protocol 2. Then one can take $f = x$ and $g = y$. Indeed, $[x, y] = x^{-1}x^y = x^p$, $[x, y; 2] = x^{p^2}$, and $[x, y; 3] = 1$. The algorithm constructing above works if

we can efficiently solve the discrete logarithm problem in $\mathbb{F}_q^*$. Unfortunately, the authors of [23] do not explain details of expressions of the elements. Anyway, our the approach reduces the problem to the computations in abelian groups, hence Protocols 1 and 2 cannot be considered as pure post-quantum protocols.

There are other approach as follows. Let $\tilde{\mathbb{F}}_q(z)$ be an extension of $\mathbb{F}_q$, where $z^p = x$. Then we define $z^y = z^{p+1}$ and $z^x = z$ and obtain group $\tilde{G}$ that contains $G$ as a subgroup. We see that

$$[z, y^{k_1}, y^{k_2}, y^{k_3}] = [x, y; 2]^k, \ k = \prod_{j=1}^{3} k_j,$$

that is the exchanged key.

## REFERENCES


1. *Menezes A. J., van Oorchot P. C., and Vanstone S. A.* Handbook of Applied Cryptography. N.Y., CRC Press, 1997.
2. *Koblitz N.* A Course in Number Theory and Cryptography. N.Y., Springer, 1987.
3. Roman'kov V. A. Vvedenie v kriptografiyu [Introduction to Cryptography]. Moscow, Forum Publ., 2012 (in Russian).
4. *Shor P.* Polynomial-time algorithm for prime factorization and discrete logarithms on a quantum computer. SIAM J. Comput., 1997, no. 5, pp. 1484–1509.
5. *Grover L. K.* A fast quantum mechanical algorithm for database search. Proc. 28th Ann. ACM Symp. on Theory of Comput., 1997, no. 5, pp. 212–219.
6. *Myasnikov A., Shpilrain V., and Ushakov A.* Group-Based Cryptography. Barselona-Basel, CRM, 2008 (Advances Courses in Math.).
7. *Myasnikov A., Shpilrain V., and Ushakov A.* Non-commutative Cryptography and Complexity of Group-Theoretic Problems. With Appendix by Natalia Mosina. Math. Surveys and Monographs, 2011, vol. 177, Providence RI, AMS.
8. *Roman'kov V. A.* Algebraicheskaya kriptografiya [Algebraic cryptography]. Omsk, OmSU Publ., 2013. (in Russian)
9. *Myasnikov A. and Roman'kov V.* A linear decomposition attack. Groups, Complexity, Cryptology, 2015, vol. 7, pp. 81–94.
10. *Roman'kov V.* A non-linear decomposition attack. Groups, Complexity, Cryptology, 2015, vol. 8, pp. 197–207.
11. *Roman'kov V. A.* Essays in Algebra and Cryptology. Algebraic Cryptanalysis. Omsk, OmSU Publ., 2018.
12. *Tsaban B.* Polynomial-time solutions of computational problems in noncommutative-algebraic cryptography. J. Cryptology, 2015, vol. 28, pp. 601–622.
13. *Ben-Zvi A., Kalka A., and Tsaban B.* Cryptanalysis via algebraic spans. LNCS, 2018, vol. 109991, pp. 1–20.
14. *Kargapolov M. I. and Merzlyakov Y. I.* Fundamentals of the Theory of Groups. N.Y., Springer Verlag, 1979.
15. *Hall P.* Nilpotent Groups. Edmonton Notes on Nilpotent Groups. Queen Mary College Math. Notes Math. Dept., London, Queen Mary College, 1969.
16. *Lennox J. C. and Robinson D. J. S.* The Theory of Infinite Soluble Groups. Oxford, Clarendon Press, 2004 (Oxford Math. Monographs).
17. *Roman'kov V. A. and Khisamiev N. G.* Nil'potentnye grruppy [Nilpotent Groups]. Ust-Kamenogorsk, EKSTU Publ., 2013. (in Russian)
18. *Menezes A. J. and Vanstone S. A.* A note on cyclic groups, finite fields and discrete logarithm problem. AAECC, 1992, vol. 3, pp. 67–74.

19. *Boneh D. and Silverberg A.* Applications of multilinear forms in cryptography. Contemporary Math., 2003, vol. 324, pp. 71–90.
20. *Lin H. and Tessaro S.* Indistinguishability Obfuscation from Trilinear Maps and Block-Wise Local PRGs. Cryptology ePrint Archive, Report 2017/250, 2017. `https://eprint.iacr.org/2017/250`
21. *Huang M. A.* Trilinear Maps for Cryptography. arXiv: 1803.10325, 2018.
22. *Mahalanobis A.* The Diffie — Hellman key exchange protocol and non-abelian nilpotent groups. Israel J. Math., 2008, vol. 165, pp. 161–187.
23. *Kahrobaei D., Tortora A., and Tota M.* Multilinear Cryptography Using Nilpotent Groups. arXiv: 1902.08777v1 [cs. CR] 23 Feb 2019. 8 p.

Секция 4

# МАТЕМАТИЧЕСКИЕ ОСНОВЫ КОМПЬЮТЕРНОЙ БЕЗОПАСНОСТИ

УДК 004.94 DOI 10.17223/2226308X/12/45

## О МОДЕЛИРОВАНИИ В РАМКАХ МРОСЛ ДП-МОДЕЛИ МАНДАТНЫХ КОНТРОЛЯ ЦЕЛОСТНОСТИ И УПРАВЛЕНИЯ ДОСТУПОМ В СУБД PostgreSQL

П. Н. Девянин

Интеграция в операционную систему специального назначения (ОССН) Astra Linux Special Edition прикладного программного обеспечения, включающего собственные механизмы управления доступом, требует, во-первых, соответствующей инженерной реализации по их сопряжению с базовыми для ОССН мандатными управлением доступом и контролем целостности, а во-вторых, обеспечения при этом доверия к безопасности такого сочетания механизмов управления доступом, в том числе для предотвращения информационных потоков (скрытых каналов) по памяти или по времени. Важным примером такого штатного для ОССН программного обеспечения является СУБД *PostgreSQL*, изначально реализующая развитый механизм ролевого управления доступом. Сертификация ОССН по требованиям утверждённого ФСТЭК России профиля защиты операционных систем общего назначения первого (высшего) класса защиты, в ходе которой разрабатывалась и верифицировалась формальная модель управления доступом, а также сертификация ОССН по требованиям других отечественных регуляторов, говорят о целесообразности подготовки к выполнению аналогичных требований применительно к СУБД. В этой связи рассматриваются результаты завершения формирования уровней мандатных управления доступом и контроля целостности СУБД *PostgreSQL* на базе иерархического представления мандатной сущностно-ролевой ДП-модели (МРОСЛ ДП-модели), являющейся научной основой разработки механизма управления доступом ОССН.

**Ключевые слова:** *компьютерная безопасность, формальная модель, управление доступом, PostgreSQL.*

Система требований к средствам защиты информации, формируемая отечественными регуляторами, непрерывно развивается, вбирая в себя достижения науки и передовой мировой опыт. Так, в применяемых с 1 июня 2019 г. «Требованиях по безопасности информации, устанавливающих уровни доверия к средствам технической защиты информации и средствам обеспечения безопасности информационных технологий», утверждённых ФСТЭК России [1], указывается на необходимость разработки модели безопасности (с четвёртого уровня доверия) и её верификации с применением инструментальных средств (с третьего уровня доверия), а также идентификации и анализа скрытых каналов (информационных потоков) по памяти (с пятого уровня доверия) и по времени (с третьего уровня доверия).

Поскольку отечественная защищённая ОССН Astra Linux Special Edition [2, 3] сертифицирована по требованиям утвержденного ФСТЭК России профиля защиты опе-

рационных систем общего назначения самого высокого — первого класса защиты (соответствующего первому уровню доверия) [4], то при реализации её механизма управления доступом использована верифицированная мандатная сущностно-ролевая ДП-модель (МРОСЛ ДП-модель) в её иерархическом представлении [5, 6]. Вместе с тем логично предположить, что в дальнейшем требования соответствующих уровней доверия будут распространены на прикладное программное обеспечение, включающее собственные механизмы управления доступом, например на штатную для ОССН СУБД *PostgreSQL*. С целью удовлетворения этим требованиям заблаговременно [7] проведены исследования по развитию МРОСЛ ДП-модели для «охвата» ею механизма управления доступом СУБД *PostgreSQL*. В настоящее время они завершены, их итогом стало формирование в дополнение к четырём уровням в иерархическом представлении модели для ОССН: ролевого управления доступом (1.1), мандатного контроля целостности (2.1), мандатного управления доступом с информационными потоками по памяти (3.1) и по времени (4.1) и аналогичных взаимосвязанных с ними уровней (1.2–4.2) для СУБД (рис. 1).

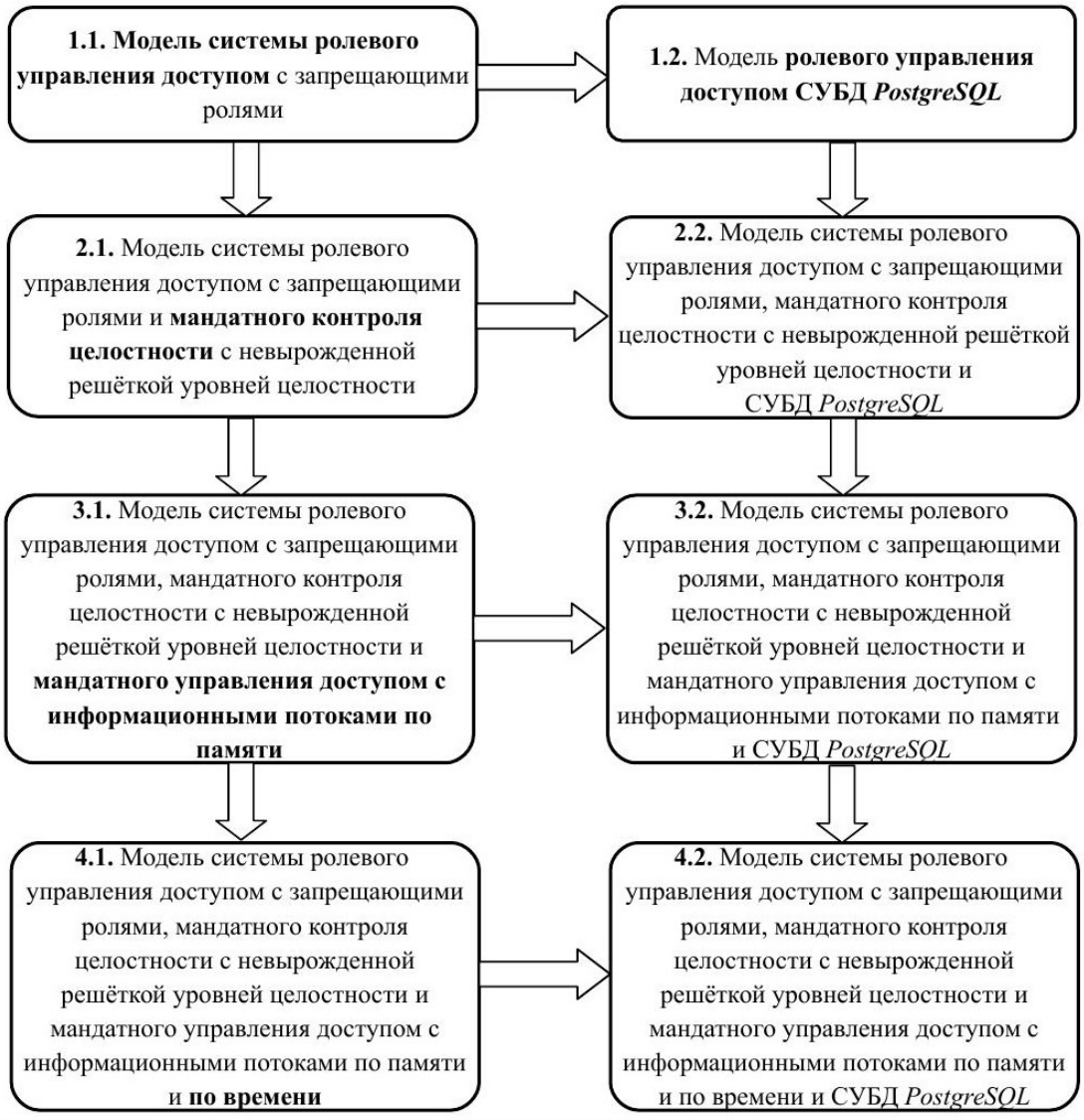


Рис. 1. Иерархическое представление МРОСЛ ДП-модели для ОССН и СУБД *PostgreSQL*

С учётом существенных отличий основанного на стандарте SQL механизма управления доступом СУБД *PostgreSQL* от реализованного в ОССН, начиная с уровня ролевого управления доступом (1.2), были использованы:

— множества: ролей СУБД, административных привилегий СУБД (*SUPERUSER*, *CREATEROLE*, *CREATEDB*, *LOGIN*, *REPLICATION*, *INHERIT*), административных ролей СУБД, специальных ролей СУБД, общих ролей СУБД, элементов СУБД, элементов-объектов СУБД (каталоги по событию, расширения, сопоставления, домены, конфигурации, словари, парсеры, шаблоны, функции, последовательности, строки, ограничения, индексы, правила, триггеры, триггерные функции, репликации), элементов-контейнеров СУБД (кластеры, базы данных, схемы, таблицы, столбцы, представления, табличные пространства), видов привилегий СУБД (*SELECT*, *INSERT*, *UPDATE*, *DELETE*, *TRUNCATE*, *REFERENCES*, *TRIGGER*, *USAGE*, *CREATE*, *CONNECT*, *TEMPORARY*, *TEMP*, *EXECUTE*, *OWN*), сущностей СУБД (на этом уровне модели сущностями являются элементы СУБД от её схем и далее выше по иерархии, например, базы данных, кластеры), привилегий к элементам СУБД;

— функции: административных привилегий ролей СУБД, ролей входа субъект-сессий в СУБД, наследования привилегий ролей к элементам СУБД, управления подчинённостью ролей в иерархии, административных прав доступа административных ролей ОССН и СУБД к ролям СУБД, привилегий к элементам СУБД ролей СУБД, соответствия административных привилегий и видов привилегий к элементам СУБД правам доступа, эффективных прав доступа ролей СУБД.

Кроме того, на этом уровне переопределены: множество доступов субъект-сессий к ролям, запрещающим ролям, административным ролям и ролям СУБД; функции: имён сущностей и элементов СУБД, имён ролей, запрещающих ролей, административных ролей, ролей СУБД, доступа субъект-сессий к сущностям и элементам СУБД в контейнерах; иерархия сущностей и элементов СУБД; иерархия ролей, запрещающих ролей, административных ролей и ролей СУБД; состояние системы.

На последующих уровнях модели (2.2–4.2) добавлены множества: доверенных субъект-сессий СУБД, функций СУБД, доверенных субъект-сессий СУБД, корректных относительно информационных потоков по времени, и функция, определяющая для каждой функции СУБД режим её выполнения: `false` — выполнение функции с правами роли СУБД, являющейся владельцем функции СУБД (в СУБД *PostgreSQL* этому соответствует атрибут *SECURITY DEFINER*), `true` — выполнение функции с правами текущих ролей СУБД субъект-сессии, инициировавшей вызов функции (в СУБД *PostgreSQL* этому соответствует атрибут *SECURITY INVOKER*). Были также переопределены:

— множества: информационных потоков, сущностей, параметрически ассоциированных с ролями, запрещающими ролями, административными ролями и ролями СУБД;

— функции: уровней целостности и конфиденциальности ролей, мандатных атрибутов конфиденциальности и целостности контейнеров;

— состояние системы;

— траектория без кооперации доверенных и недоверенных субъект-сессий;

— безопасное состояние системы;

На уровне 1.2 ролевого управления доступом СУБД *PostgreSQL* по сравнению с уровнем 1.1 не задано новых де-юре правил преобразования состояний, хотя боль-

шая их часть была модифицирована путём добавления в правила новых параметров, условий и результатов применения, учитывающих специфику управления доступом в СУБД. Начиная с уровня мандатного контроля целостности СУБД, кроме внесения аналогичных изменений добавлено новое де-юре правило $db\_execute(x, x', y)$, позволяющее задать порядок активизации функций СУБД. Состав де-факто правил при моделировании управления доступом в СУБД не изменился. В итоге определены 39 де-юре и 10 де-факто правил преобразования состояний, общих для ОССН и СУБД, что создаёт условия для формирования единых подходов к их реализации, в том числе для противодействия запрещённым информационным потокам по памяти и по времени.

При задании требований к мандатным управлению доступом и контролю целостности в СУБД *PostgreSQL*, чтобы не снижать её производительности, предложено назначать уровни целостности и конфиденциальности элементам СУБД до схем включительно, т. е. не назначать их таблицам, функциям, триггерам.

Для каждого из уровней модели для СУБД сформулированы и обоснованы утверждения о соответствии (корректности) правил преобразования состояний системы условиям, которым должно удовлетворять соответственно ролевое управление доступом, мандатный контроль целостности, мандатное управление доступом с информационными потоками по памяти и по времени. С учётом внесённых на уровнях СУБД изменений переформулированы и доказаны утверждения о достаточных условиях безопасности системы в смыслах мандатного контроля целостности, контроля информационных потоков по памяти (в смысле Белла — ЛаПадулы) и контроля информационных потоков по времени. Именно для третьего случая на уровне 4.2 потребовались наибольшие изменения по сравнению с уровнем 4.1. Они заключались, во-первых, в запрете передачи роли СУБД права на дальнейшую передачу привилегии (с использованием в СУБД *PostgreSQL* права *WITH GRANT OPTION*), во-вторых, в отсутствии функций СУБД, содержащихся в сущностях-схемах СУБД, имеющих высокий уровень целостности и уровень конфиденциальности выше минимального.

Таким образом, в рамках иерархического представления МРОСЛ ДП-модели удалось полностью смоделировать управление доступом в СУБД *PostgreSQL* аналогично тому, как это было выполнено для ОССН Astra Linux Special Edition. В дальнейшем предполагается дедуктивная верификация соответствующих СУБД уровней модели с применением инструментальных средств, что соответствует утверждённым ФСТЭК России требованиям высоких уровней доверия к средствам защиты информации.

## ЛИТЕРАТУРА

1. ФСТЭК России. Информационное сообщение от 29 марта 2019 г. № 240/24/1525. `https://fstec.ru/component/attachments/download/2286`.
2. Astra Linux — универсальная операционная система. `http://www.astralinux.ru`.
3. Astra Linux. `https://ru.wikipedia.org/wiki/Astra_Linux`.
4. Родина в кибербезопасности: российской ОС откроют все секреты. `https://iz.ru/871218/olga-kolentcova/rodina-v-kiberbezopasnosti-rossiiskoi-os-otkroiut-vse-sekrety/`.
5. *Буренин П. В., Девянин П. Н., Лебеденко Е. В. и др.* Безопасность операционной системы специального назначения Astra Linux Special Edition: учеб. пособие для вузов. / под ред. П. Н. Девянина. 3-е изд., перераб. и доп. М.: Горячая линия-Телеком, 2019. 404 с.
6. *Девянин П. Н., Кулямин В. В., Петренко А. К. и др.* Моделирование и верификация политик безопасности управления доступом в операционных системах. М.: Горячая линия-Телеком, 2019. 214 с.

7. *Девянин П. Н.* Подходы к моделированию управления доступом в СУБД PostgreSQL в рамках МРОСЛ ДП-модели // Прикладная дискретная математика. Приложение. 2018. № 11. С. 95–98.

УДК 004.056.53, 004.032.26 DOI 10.17223/2226308X/12/46

# ИСКУССТВЕННЫЕ НЕЙРОННЫЕ СЕТИ КАК МЕХАНИЗМ ОБФУСКАЦИИ ВЫЧИСЛЕНИЙ

В. Л. Елисеев

Рассмотрены возможности использования искусственных нейронных сетей в качестве механизма строгой обфускации вычислительного алгоритма. Обсуждается задача обфускации, основные положения и современные подходы к её реализации. Вводится понятие нейросетевого обфускатора и доказываются его свойства. Приводятся достоинства и недостатки предложенного подхода.

**Ключевые слова:** *искусственная нейронная сеть, обфускация.*

## Введение

Обфускация (сокрытие) представляет собой преобразование алгоритма к форме, затрудняющей изучение его свойств. Актуальность рассмотрения подобных механизмов основана на том факте, что программное обеспечение в подавляющем большинстве случаев представляет собой объект интеллектуальной собственности, но при этом используется в вычислительной среде, не контролируемой владельцем прав на программу. Наиболее часто обфускации подвергаются части программы, реализующие механизмы защиты от копирования и иного использования в обход лицензии. Примитивные механизмы обфускации применяются также для защиты от изучения человеком исходного кода библиотек, поставляемых на интерпретируемых языках (PHP, Python, JavaScript, Java).

Значительное число работ, посвящённых обфускации исходного кода программ (например, [1]), предлагает разнообразные эвристические методы, автоматизирующие эквивалентную трансформацию программы с целью запутывания оригинальной структуры алгоритма путём изменения представления используемых данных и констант. Такое преобразование даёт визуально достаточно впечатляющие результаты, однако для каждого из эвристических обфусцирующих алгоритмов есть деобфусцирующий, восстанавливающий исходную структуру. По этой причине эвристическая обфускация не может считаться надёжным подходом для защиты алгоритмов, содержащих конфиденциальную информацию, в том числе криптографические ключи и «ноу хау» (скоринговые алгоритмы страховых компаний и банков). Ряд задач, решение которых могло бы упроститься при создании стойких обфускаторов, приведено в [2].

## 1. Обзор

Начиная с момента появления до работы [3], все методы обфускации представляли собой эвристики, которые было трудно оценивать и сравнивать друг с другом в части стойкости к действиям злоумышленника, пытающегося восстановить исходный алгоритм. Общеизвестно, что любые эвристические подходы всегда имеют ограничения по области применения. В случае с обфускацией для каждого эвристического метода можно построить алгоритм деобфускации, восстанавливающий исходный алгоритм.

В работе [3] впервые введено строгое понятие стойкой обфускации. Неформально обфускатор $\mathcal{O}$ — это транслятор, принимающий на вход программу $P$ и производящий программу $\mathcal{O}(P)$, такую, что выполняются два условия:

— функциональность $\mathcal{O}(P)$ эквивалентна функциональности $P$;
— всё, что может быть эффективно вычислено из $\mathcal{O}(P)$, может быть эффективно вычислено случайным оракулом при доступе к $P$.

Второе свойство получило название виртуального чёрного ящика, поскольку случайный оракул — это идеализированная хэш-функция со случайным детерминированным выходом. По сути это свойство означает, что нет более эффективного способа для изучения обфусцированного алгоритма, чем его многократный запуск. Иногда добавляется также свойство эффективности обфускации [2], которое обуславливает ограничение на размер и вычислительную сложность $\mathcal{O}(P)$ по сравнению с $P$.

Вместе с тем сразу было показано, что существует класс программ (схем), для которого свойство виртуального черного ящика недостижимо [3]. Для снижения планки требований в той же работе введено понятие обфускации неразличимости (*indistinguishability obfuscation*). В соответствии с этим определением две различные, но функционально эквивалентные программы $P_1$ и $P_2$ ($\forall x\,(P_1(x) = P_2(x))$), подвергнутые обфускации, неразличимы за полиномиальное время. Это означает, что невозможно эффективно определить, является ли $\mathcal{O}(P_1)$ обфускацией $P_1$ или $P_2$.

Для обфускации неразличимости в [4] доказано, что это лучший из возможных обфускаторов, то есть такой, который сообщает об исходной программе не больше, чем любая другая программа с функциональностью, эквивалентной исходной.

В 2013 г. представлен первый и до настоящего времени единственный класс методов обфускации, доказуемо реализующих свойство неразличимости, — это так называемое градуированное кодирование (graded encoding) [5]. Известно, что реализация этого подхода для прикладных применений существенно неэффективна с вычислительной точки зрения [6], что делает как процедуру обфускации, так и сам полученный обфускатор малопригодными в реальных задачах.

В одной из работ, посвященных эмпирической обфускации [7], для сокрытия логики переходов в условных операторах предложено использовать искусственную нейронную сеть (далее нейросеть), функционально эквивалентную вычисляемому предикату на множестве допустимых значений аргументов. Отмечено, что после обучения, то есть собственно процедуры обфускации, нейросеть несущественно снижает производительность программы при скромных расходах памяти на хранение матрицы весовых коэффициентов. В то же время применение нейросетей для задачи обфускации подвергнуто критике в [8] главным образом за непредказуемость результатов за пределами обучающей выборки.

Известны многочисленные варианты формальных конструкций, причисляемых к нейросетям, достаточно полный перечень и описание которых приведены в [9]. Далее будем говорить только о нейросетях типа *многослойный персептрон* (*multilayer perceptron — MLP*). Многослойный персептрон вычисляет выходной вектор по входному $x^{(N)} = f(x^{(0)})$, при этом реализует алгебраическое преобразование вида

$$x_i^{(k)} = s\left(\sum_{j=1}^{m_{k-1}} w_{ij}^{(k)} x_j^{(k-1)}\right),\ k = 1, \ldots, N,\ i = 1, \ldots, m_k,$$

где $N$ — количество слоёв нейросети; $x^{(k)} \in \mathbb{R}^{m_k}$ — вектор выходов слоя $k$; $x^{(0)} \in \mathbb{R}^{m_0}$ — вектор входов нейросети; $m_k$ — количество нейронов слоя $k$; $m_0$ — количество вхо-

дов первого слоя нейросети; $w_{ij}^{(k)} \in \mathbb{R}$ — весовой коэффициент $j$-го входа $i$-го нейрона слоя $k$; $s(.)$ — дифференцируемая функция, называемая также функцией активации. Как правило, эта функция имеет вид сигмоиды, например логистической: $s(t) = 1/(1 + e^{-t})$.

В 1987 г. Р. Хехт-Нильсен на основе работ А. Н. Колмогорова доказал представимость непрерывной функции многих переменных с помощью двухслойной нейросети [10]. Этот результат неконструктивен, однако даёт основание считать нейросети универсальными аппроксиматорами одномерных и многомерных непрерывных функций многих переменных. Разработаны не имеющие гарантий успешности, но показавшие высокую результативность методы обучения нейросетей. Под обучением нейросети понимают процедуру задания или, что обычно, итеративного изменения весовых коэффициентов $w_{ij}^{(k)}$ в процессе решения оптимизационной задачи для получения заданной точности аппроксимации таблично заданной неизвестной непрерывной функции. Для обучения нейросетей используется большой спектр методов оптимизации, использующих градиентные, стохастические и другие подходы, а также их комбинации [9].

Следует отметить, что выбор структуры нейросети — числа слоёв и количества нейронов в них — до сих пор является плохо изученной проблемой и на практике обычно используются различные эвристики. Значимым результатом в этой области является получение оценки VC-измерения нейросети с сигмоидальными функциями активации — $\mathrm{O}(W^2)$, где $W = \sum\limits_{k=1}^{N-1} m_{k-1}m_k$ — количество настраиваемых параметров $w_{ij}^{(k)}$ нейросети [9].

## 2. Предложение

Рассмотрим задачу обфускации программы $P$ с помощью нейросети. Определим $P$ в общем виде как детерминированную функцию вектора переменных $x$ из множества допустимых векторов $X \subseteq \mathbb{R}^n$, вычисляющую значение $y$ из множества $Y \subseteq \mathbb{R}^m$:

$$y = P(x),\ x \in X,\ y \in Y.$$

**Определение 1.** Назовём *нейросетевым обфускатором функции* $P$ нейросеть $\mathcal{N}$ с количеством входов $n$ и количеством выходов $m$, достаточно точно аппроксимирующую эту функцию.

В дальнейшем рассмотрении ограничимся программами, оперирующими булевыми векторами конечного размера: $X \subseteq \mathbb{B}^n$, $Y \subseteq \mathbb{B}^m$, где $\mathbb{B} = \{0, 1\}$.

**Определение 2.** *Нейросетевым обфускатором векторной булевой функции* $P$ является нейросеть $\mathcal{N}$ с количеством входов $n$ и количеством выходов $m$, такая, что

$$\forall x \in X \left((y = P(x)\ \&\ \hat{y} = \mathcal{N}(x)) \Rightarrow |y_i - \hat{y}_i| < 0{,}5,\ i = 1, \ldots, m\right).$$

Отметим, что при обучении нейросетей аппроксимации неизвестной функции, заданной множеством точек ограниченного размера $\{(x_i, y_i) : i = 1, \ldots, N\}$, возникают трудности, связанные с достижением точности аппроксимации, а также с контролем обобщающей способности нейросети (проблема переобучения нейросети [9]). Для их преодоления имеющееся в наличии множество точек разделяют на обучающее, тестовое и контрольное, что является эвристикой, не дающей гарантий успешного результата.

В рассматриваемом здесь случае нейросеть обучается аппроксимировать заведомо известную функцию $P$. В этом случае не возникает проблемы переобучения и всё множество данных $\{(x_i, y_i) : i = 1, \ldots, N\}$ должно использоваться как обучающее.

**Теорема 1.** Нейросетевой обфускатор булевой функции $P$ обладает свойством функциональности.

***Доказательство.*** Построим какую-либо непрерывную функцию $\tilde{P}$, проходящую через все значения функции $P$ на области её определения. По теореме Хехт-Нильсена [11] для функции $\tilde{P}$ можно построить двухслойную нейросеть, аппроксимирующую эту функцию с любой наперёд заданной точностью. Эта нейросеть в точках $x \in X$ будет также аппроксимировать $P$. ■

**Теорема 2.** Нейросетевой обфускатор булевой функции $P$ обладает свойством неразличимости.

***Доказательство.*** Возьмём две различные программы $P_1$ и $P_2$, реализующие функцию $P$. Для них можно построить нейросетевые обфускаторы $\mathcal{N}_1$ и $\mathcal{N}_2$ соответственно. Поскольку для построения каждого из обфускаторов используется один и тот же набор данных, обусловленный значениями функции $P$, то невозможно определить, какая из нейросетей построена как обфускатор конкретной программы $P_1$ или $P_2$. ■

Приведённые выкладки могут быть обобщены на векторные функции с элементами, принадлежащими конечному множеству значений. Например, в качестве элементов векторов $x$ и $y$ можно использовать подмножество целых чисел или элементы конечного поля.

## 3. Обсуждение

Полученный результат позволяет утверждать, что нейросети обеспечивают обфускацию неразличимости для достаточно широкого класса алгоритмов. В то же время известный опыт применения нейросетей позволяет сформулировать следующие особенности предложенного метода обфускации:

1) объём выборки для обучения нейросети экспоненциально растёт с ростом размерности векторов $x$ и $y$;
2) пока не существует однозначно эффективного метода для выбора структуры нейросети под конкретную задачу;
3) вычислительные ресурсы для обучения нейросети как минимум пропорциональны произведению размера выборки $N$ на количество обучаемых параметров $W$;
4) вычислительные ресурсы для работы нейросетевого обфускатора пропорциональны количеству обучаемых параметров $W$.

Оценка вычислительной сложности для обучения нейросети, а также неопределённость с выбором её структуры однозначно являются существенными недостатками предложенного подхода. В то же время следует отметить, что работа нейросетевого обфускатора требует существенно меньших ресурсов. Кроме того, в настоящее время существуют аппаратные устройства для обучения и работы нейросетей, обеспечивающие ускорение до трёх десятичных порядков относительно универсальных процессоров.

Представляется важным исследовать вопросы, связанные с проектированием структуры нейросетевого обфускатора и получением уточнённых оценок вычислительной сложности его обучения. Тем не менее, учитывая большой накопленный опыт применения нейросетей, есть основания считать предложенный метод обфускации прак-

тически значимым и имеющим потенциал по применению в актуальных задачах, требующих надёжного сокрытия алгоритмов.

## Выводы

Предложен новый механизм обфускации на основе искусственных нейронных сетей и доказано его соответствие требованиям функционального обфускатора неразличимости. Отмечены его основные свойства, перспективы дальнейших исследований и практического применения.

## ЛИТЕРАТУРА


1. *Venkatesh S. and Ertaul L.* Novel obfuscation algorithms for software security // Proc. Intern. Conf. SERP'05. 2005. V. 1. P. 209–215.
2. *Варновский Н. П., Захаров В. А., Кузюрин Н. Н.* Математические проблемы обфускации // Математика и безопасность информационных технологий. Материалы конф. в МГУ 28–29 октября 2004 г. М.: МЦНМО, 2005. С. 65–91.
3. *Barak B., Goldreich O., Impagliazzo R., et al.* On the (im)possibility of obfuscating programs // Crypto'01. LNCS. 2001. V. 2139. P. 1–18.
4. *Goldwasser S. and Guy N. R.* On best-possible obfuscation // J. Cryptology. 2007. No. 27. P. 480–505.
5. *Garg S., Gentry C., Halevi S., et al.* Candidate indistinguishability obfuscation and functional encryption for all circuits // Proc. 54th IEEE Ann. Symp. FOCS'13. October 26–29, 2013. P. 40–49.
6. *Albrecht M. R., Cocis C., Laguillaumie F. and Langlois A.* Implementing candidate graded encoding schemes from ideal lattices // ASIACRYPT 2015. LNCS. 2015. V. 9453. P. 752–775.
7. *Ma H., Ma X., Liu W., et al.* Control flow obfuscation using neural network to fight concolic testing // 10th Intern. ICST Conf., SecureComm 2014, Beijing, China, September 24–26, 2014. Part I. P. 287–304.
8. *Yan Wang* Obfuscation with Turing Machine. A Thesis in Information Sciences and Technology. Pennsylvania State University, 2017. 42 p.
9. *Хайкин С.* Нейронные сети: полный курс. 2-е изд. М.: Вильямс, 2008.
10. *Алексеев Д. В.* Приближение функций нескольких переменных нейронными сетями // Фундаментальная и прикладная математика. 2009. Т. 15б. № 3. С. 9–21.
11. *Hecht-Nielsen R.* Kolmogorov's mapping neural network existence theorem // IEEE First Ann. Int. Conf. Neural Networks. San Diego, 1987. V. 3. P. 11–13.


УДК 519.21 DOI 10.17223/2226308X/12/47

# ОЦЕНКА ВЕРОЯТНОСТИ УСПЕШНОЙ АТАКИ НАРУШИТЕЛЯ В БЛОКЧЕЙН-СЕТИ

И. В. Семибратов, В. М. Фомичев

Рассмотрена вероятностная модель, определяющая начала активных периодов функционирования злоумышленника и майнера как случайные величины, распределённые по биномиальному закону. Получены оценки вероятностей успешной атаки злоумышленника (создания ложного блока данных) при различных исходных условиях. Результаты вычислений подтвердили естественные предположения, что вероятность успешной атаки злоумышленника убывает как с ростом положительной разности длительностей сеансов майнера и злоумышленника, так и с ростом числа активных майнеров, и возрастает с ростом в положительном

диапазоне разницы между ожидаемым временем начала сеанса майнера и временем начала сеанса злоумышленника.

**Ключевые слова:** *блокчейн, майнер, механизм консенсуса, хеш-функция, биномиальное распределение вероятностей.*

## Введение

Технология блокчейн (БЧ) направлена на создание в децентрализованной системе цепей, состоящих из блоков достоверных данных. Последующие блоки цепи возникают после подтверждения аутентичности предыдущих блоков в результате поиска входного слова $x$ хэш-функции по её значению. Центральный вопрос успешности технологии БЧ состоит в необходимости достичь консенсуса пользователей информационной системы в вопросе добавления блоков в цепь при отсутствии взаимного доверия. Один из базовых тезисов в части безопасности состоит в том, что число злоумышленников, стремящихся создавать блоки ложных данных, должно быть меньше числа майнеров — добропорядочных пользователей, участвующих в создании новых блоков данных.

Представлена вероятностная модель креативной деятельности одного злоумышленника и $m$ майнеров в течение временного периода (суток), $m \geqslant 1$. В рамках модели при различных параметрах оценена вероятность $P_{1,m}$ успешной атаки злоумышленника (создания блока ложных данных).

## 1. Оценка вероятности успешной атаки злоумышленника

Длительность временных отрезков измеряется в условных единицах (у.е.), где за 1 у.е. принят 10-минутный отрезок, который в настоящее время считается достаточным для того, чтобы некоторые майнеры отыскали слово $x$. Разделим временную ось на периоды длины $t = 144$ у.е., что соответствует одним суткам. Положим, что за период длины $t$ каждый участник отрабатывает отрезок времени (сеанс), где длительность сеанса злоумышленника равна $\theta$ и майнера — $\tau$, $0 < \theta, \tau \leqslant t/2$. При $m \geqslant 1$ положим $r = \tau - \theta \geqslant 0$, иначе злоумышленник гарантированно совершает успешную атаку.

Пусть начало сеанса совпадает с началом одного из отрезков, то есть с одним из моментов времени $0, 1, \ldots, t - t_0$, где $t_0 = \theta$ для злоумышленника и $t_0 = \tau$ для майнера. Тогда конец сеанса совпадает с одним из моментов времени $t_0, t_0 + 1, \ldots, t$. В данных условиях $t - \theta$ и $t - \tau$ суть суммарные длительности отрезков времени, когда пассивны (то есть не участвуют в действиях по развитию БЧ) злоумышленник и майнер соответственно.

Пусть вычислительные мощности всех участников равны. Атаку злоумышленника в период длины $t$ признаем успешной, если найдётся отрезок, когда злоумышленник активен, а майнер пассивен.

Обозначим $\xi_{\text{з}}$ и $\xi_{\text{м}}$ случайные моменты начала сеанса злоумышленника и майнера соответственно. Рассчитаем вероятность успешной атаки злоумышленника в предположении, что данные величины распределены по биномиальному закону [1] на сегментах $[a_{\text{з}} - \theta/2, a_{\text{з}} + \theta/2]$ и $[a_{\text{м}} - \tau/2, a_{\text{м}} + \tau/2]$ со средними значениями $a_{\text{з}}$ и $a_{\text{м}}$ соответственно:

$$b_i = \mathsf{P}[\xi_{\text{з}} = a_{\text{з}} \pm i] = 2^{-\theta} \mathrm{C}_{\theta}^{\theta/2-i}, \ i = 0, 1, \ldots, \theta/2; \tag{1}$$

$$a_i = \mathsf{P}[\xi_{\text{м}} = a_{\text{м}} \pm i] = 2^{-\tau} \mathrm{C}_{\tau}^{\tau/2-i}, \ i = 0, 1, \ldots, \tau/2. \tag{2}$$

Функции вероятности для биномиального распределения случайных величин $\xi_{\text{з}}$ и $\xi_{\text{м}}$ симметричны относительно точек $a_{\text{з}}$ и $a_{\text{м}}$ соответственно. Злоумышленник и майнеры выбирают начало сеанса случайно и независимо друг от друга с вероятностью, заданной формулами (1) и (2).

Рассмотрим некоторые случаи с одним злоумышленником и с различным числом майнеров при $t = 144$. При фиксированных $\tau$ и $\theta$ обозначим $P_m(\tau, \theta)$ вероятность успешной атаки злоумышленника, которому противодействуют $m$ майнеров, $m \geqslant 1$; $p_i = \mathsf{P}[\xi_{\text{м}} > i]$, $q_i = \mathsf{P}[\xi_{\text{м}} < i]$, $a_{\text{м}} - \tau/2 \leqslant i \leqslant a_{\text{м}} + \tau/2$. Из (2) следует:

$$p_i = \sum_{j=i+1}^{a_{\text{м}}+\tau/2} a_j = 2^{-\tau} \sum_{j=i+1}^{\tau} \mathrm{C}_\tau^j, \quad q_i = \sum_{j=a_{\text{м}}-\tau/2}^{i-1} a_j = 2^{-\tau} \sum_{j=0}^{i-1} \mathrm{C}_\tau^j = 1 - p_i - \mathrm{C}_\tau^i, \ i = 1, \ldots, \tau.$$

По формуле полной вероятности из (1) и (2) получаем

$$P_{1,m}(\tau, \theta) = \sum_{i=a_{\text{з}}-\theta/2}^{a_{\text{з}}-\theta/2+r} b_i p_i^m + \sum_{i=a_{\text{з}}-\theta/2+r+1}^{a_{\text{з}}+\theta/2-\tau} b_i (q_{i-r} + p_i)^m + \sum_{i=a_{\text{з}}+\theta/2-\tau+1}^{a_{\text{з}}+\theta/2} b_i q_{i-r}^m.$$

Данное равенство можно записать иначе:

$$P_{1,m}(\tau, \theta) = \sum_{i=a_{\text{з}}-\theta/2}^{a_{\text{з}}+\theta/2} b_i (q_{i-r} + p_i)^m. \tag{3}$$

Здесь $q_i = 0$ при $i \leqslant a_{\text{м}} - \tau/2$ и $p_i = 0$ при $i \geqslant a_{\text{м}} + \tau/2$.

По формуле (3) посчитаны вероятности $P_{1,m}(\tau, \theta)$ при параметрах $(a_{\text{з}}, a_{\text{м}}) \in \in \{(36, 36); (36, 40); (36, 44); (36, 48)\}$. Результаты даны в табл. 1–3.

Таблица 1

**Значения вероятностей** $P_{1,1}(\tau, \theta)$

| $(\tau, \theta)$ | $a_{\text{з}} = a_{\text{м}} = 36$ | $a_{\text{з}} = 36, a_{\text{м}} = 40$ | $a_{\text{з}} = 36, a_{\text{м}} = 44$ | $a_{\text{з}} = 36, a_{\text{м}} = 48$ |
|---|---|---|---|---|
| (72,4) | 0,4544 | 0,7889 | 0,9577 | 0,9960 |
| (72,8) | 0,4555 | 0,7830 | 0,9535 | 0,9952 |
| (72,12) | 0,4566 | 0,7774 | 0,9494 | 0,9942 |
| (72,16) | 0,4576 | 0,7721 | 0,9454 | 0,9931 |
| (72,20) | 0,4585 | 0,7671 | 0,9413 | 0,9920 |
| (72,24) | 0,4594 | 0,7624 | 0,9373 | 0,9908 |
| (72,28) | 0,4602 | 0,7579 | 0,9334 | 0,9895 |
| (72,32) | 0,4610 | 0,7537 | 0,9295 | 0,9882 |
| (72,36) | 0,4617 | 0,7496 | 0,9257 | 0,9868 |
| (72,40) | 0,4624 | 0,7457 | 0,9220 | 0,9853 |
| (72,44) | 0,4630 | 0,7420 | 0,9183 | 0,9839 |
| (72,48) | 0,4637 | 0,7385 | 0,9147 | 0,9823 |
| (72,52) | 0,4643 | 0,7351 | 0,9111 | 0,9808 |
| (72,56) | 0,4665 | 0,7320 | 0,9077 | 0,9792 |
| (72,60) | 0,4799 | 0,7307 | 0,9044 | 0,9776 |
| (72,64) | 0,5382 | 0,7416 | 0,9031 | 0,9761 |
| (72,68) | 0,6898 | 0,7981 | 0,9148 | 0,9768 |
| (72,72) | 0,9336 | 0,9468 | 0,9726 | 0,9910 |

Таблица 2

**Значения вероятностей $P_{1,4}(\tau, \theta)$**

| $(\tau, \theta)$ | $a_з = a_м = 36$ | $a_з = 36, a_м = 40$ | $a_з = 36, a_м = 44$ | $a_з = 36, a_м = 48$ |
|---|---|---|---|---|
| (72,4) | 0,0532 | 0,4037 | 0,8436 | 0,9843 |
| (72,8) | 0,0637 | 0,4072 | 0,8324 | 0,9809 |
| (72,12) | 0,0737 | 0,4104 | 0,8220 | 0,9773 |
| (72,16) | 0,0832 | 0,4133 | 0,8124 | 0,9734 |
| (72,20) | 0,0922 | 0,4159 | 0,8036 | 0,9694 |
| (72,24) | 0,1006 | 0,4183 | 0,7954 | 0,9653 |
| (72,28) | 0,1086 | 0,4205 | 0,7878 | 0,9610 |
| (72,32) | 0,1161 | 0,4226 | 0,7807 | 0,9568 |
| (72,36) | 0,1233 | 0,4245 | 0,7741 | 0,9525 |
| (72,40) | 0,1301 | 0,4262 | 0,7679 | 0,9482 |
| (72,44) | 0,1365 | 0,4279 | 0,7621 | 0,9439 |
| (72,48) | 0,1427 | 0,4294 | 0,7566 | 0,9336 |
| (72,52) | 0,1485 | 0,4309 | 0,7515 | 0,9354 |
| (72,56) | 0,1541 | 0,4322 | 0,7467 | 0,9313 |
| (72,60) | 0,1599 | 0,4337 | 0,7421 | 0,9272 |
| (72,64) | 0,1749 | 0,4387 | 0,7390 | 0,9233 |
| (72,68) | 0,2760 | 0,4860 | 0,7528 | 0,9237 |
| (72,72) | 0,7634 | 0,8087 | 0,8993 | 0,9660 |

Таблица 3

**Значения вероятностей $P_{1,16}(\tau, \theta)$**

| $(\tau, \theta)$ | $a_з = a_м = 36$ | $a_з = 36, a_м = 40$ | $a_з = 36, a_м = 44$ | $a_з = 36, a_м = 48$ |
|---|---|---|---|---|
| (72,4) | 0,0001 | 0,0438 | 0,5283 | 0,9395 |
| (72,8) | 0,0004 | 0,0608 | 0,5231 | 0,9281 |
| (72,12) | 0,0011 | 0,0764 | 0,5195 | 0,9167 |
| (72,16) | 0,0023 | 0,0906 | 0,5168 | 0,9056 |
| (72,20) | 0,0041 | 0,1035 | 0,5148 | 0,8950 |
| (72,24) | 0,0062 | 0,1153 | 0,5132 | 0,8849 |
| (72,28) | 0,0088 | 0,1262 | 0,5119 | 0,8754 |
| (72,32) | 0,0117 | 0,1362 | 0,5109 | 0,8664 |
| (72,36) | 0,0148 | 0,1454 | 0,5100 | 0,8579 |
| (72,40) | 0,0182 | 0,1540 | 0,5093 | 0,8499 |
| (72,44) | 0,0216 | 0,1620 | 0,5086 | 0,8423 |
| (72,48) | 0,0252 | 0,1695 | 0,5081 | 0,8352 |
| (72,52) | 0,0289 | 0,1765 | 0,5076 | 0,8284 |
| (72,56) | 0,0326 | 0,1830 | 0,5072 | 0,8220 |
| (72,60) | 0,0364 | 0,1892 | 0,5068 | 0,8160 |
| (72,64) | 0,0405 | 0,1954 | 0,5068 | 0,8104 |
| (72,68) | 0,0538 | 0,2100 | 0,5153 | 0,8092 |
| (72,72) | 0,3686 | 0,4735 | 0,7007 | 0,8889 |

## Выводы

Судя по табл. 1–3, вероятность успешной атаки злоумышленника убывает с ростом $r$; убывает с ростом числа активных майнеров; возрастает с ростом $a_м - a_з$ в положительном диапазоне.

## ЛИТЕРАТУРА

1. *Чистяков В. П.* Курс теории вероятностей. 5-е изд. М.: Агар, 2000. 256 с.

Секция 5

# ПРИКЛАДНАЯ ТЕОРИЯ АВТОМАТОВ И ГРАФОВ

УДК 519.17 DOI 10.17223/2226308X/12/48

## О ГЕНЕРАЦИИ НЕИЗОМОРФНЫХ РАСКРАСОК МЕТОДОМ РИДА — ФАРАДЖЕВА

М. Б. Абросимов, П. В. Разумовский

Рассматривается задача генерации всех неизоморфных вершинных $k$-раскрасок заданного графа. Предлагается алгоритм решения задачи без проверки на изоморфизм методом Рида — Фараджева.

**Ключевые слова:** *раскраска вершин графа, изоморфизм, генерация раскрасок.*

### Введение

Отказоустойчивость — одно из важных свойств, которое необходимо учитывать при разработке безопасных систем. Для исследования полной отказоустойчивости дискретных систем в 1976 г. John P. Hayes [1] предложил теоретическую модель, основанную на графах. Вершины графа соответствуют элементам системы, а рёбра — связям между элементами. Если элементы системы имеют разный тип, то соответствующие им вершины получают метку, обозначающую тип или цвет. Аналогично можно рассматривать систему, в которой и связи могут иметь разный тип. В соответствующем графе рёбра будут раскрашены в цвет, обозначающий тип связи. Если элементы и связи системы имеют одинаковый тип, то рассматривается обыкновенный граф, в котором вершины и рёбра не окрашены. Большинство полученных результатов по исследованию отказоустойчивости систем относятся именно к этому случаю, то есть к неокрашенным графам [2]. При переходе к цветным графам возникает задача их генерации по заданному неокрашенному графу. В данной работе рассматривается именно такая задача. Очевидно, что эта задача может представлять интерес и без привязки к исследованию отказоустойчивых систем.

**Определение 1.** Пусть $G = (V, \alpha)$ — неориентированный граф, $k$ — натуральное число. Функция вида $f : V \to \{1, \ldots, k\}$ называется *вершинной $k$-раскраской* графа $G$, $f(v)$ — цветом вершины $v \in V$, а граф $G$, каждой вершине которого сопоставляется какой-нибудь цвет, называется *цветным* либо *графом с цветными вершинами*. Цветной граф будем обозначать $G = (V, \alpha, f)$.

**Определение 2.** *Изоморфизмом цветных графов* $G_1 = (V_1, \alpha_1, f_1)$ и $G_2 = (V_2, \alpha_2, f_2)$ называется изоморфизм графов $G_1 = (V_1, \alpha_1)$ и $G_2 = (V_2, \alpha_2)$, сохраняющий цвета, т. е. биекция $\varphi : V_1 \to V_2$, при которой выполняются следующие два условия:

1) $\forall\, u, v \in V_1 \big((u, v) \in \alpha_1 \Leftrightarrow (\varphi(u), \varphi(v)) \in \alpha_2\big)$;
2) $\forall\, v \in V_1 \big(f_1(v) = f_2(\varphi(v))\big)$.

Изоморфизм цветных графов также называется *цветным изоморфизмом*. Аналогично вводится понятие изоморфизма *графов с цветными рёбрами*.

Графы с применённой на них функцией раскраски будем называть *раскраской*. Таким образом, генерация раскрасок подразумевает поиск всех таких функций вида $f : V \to \{1, \ldots, k\}$, при которых цветные графы, полученные раскраской заданного графа, будут неизоморфны друг другу.

**Определение 3.** *Цветной автоморфизм графа* — это изоморфизм цветного графа на себя. Множество всех цветных автоморфизмов, включая тождественный, образует *группу автоморфизмов графа*.

**Определение 4.** Две вершины графа называются *подобными*, если существует автоморфизм, отображающий одну вершину на другую. Множество подобных вершин называется *орбитой*.

## 1. Задача генерации неизоморфных $k$-раскрасок графа

Генерация всех неизоморфных раскрасок вершин заданного графа ровно в $k$ цветов не имеет эффективного решения. Существуют различные подходы для решения данной задачи, наиболее результативными из которых являются методы с использованием техники «isomorphism rejection» (без непосредственной проверки на изоморфизм), хороший обзор которой можно найти в работе [3].

Ранее был описан алгоритм генерации неизоморфных раскрасок, в основе которого лежит метод МакКея [4]. В этой работе рассматривается другой подход — алгоритм генерации методом Рида — Фараджева.

## 2. Метод Рида — Фараджева порождения объектов без проверки на изоморфизм

Одним из наиболее распространённых методов порождения комбинаторных объектов без проверки на изоморфизм является метод канонических представителей. Идея метода в общем виде состоит в следующем:

1) определяется способ кодирования объектов;
2) среди всех кодов изоморфных объектов выбирается канонический код (представитель);
3) порождаются все возможные уникальные структуры вместе с их кодами;
4) порождённая структура принимается, если её код канонический, в противном случае исключается.

В методе Рида — Фараджева дополнительно к методу канонических представителей производится раннее отсечение вариантов, которые не могут привести к каноническому представителю.

## 3. Схема поиска неизоморфных раскрасок методом Рида — Фараджева

Схема поиска базируется на принципе перебора с отсечениями. На каждой итерации вычисляется множество орбит для заданной раскраски, выбирается по одному представителю из каждой орбиты и каждый представитель раскрашивается во все цвета выбранным способом. Из полученного набора отсекаются раскраски, не подходящие под условия, описанные ниже. Генерация продолжается до тех пор, пока не останется неотсечённых вариантов раскрасок графа.

Данная схема предполагает следующий ход генерации: на вход подаётся вектор цветов (раскраска) вершин графа, инициализированный первым цветом 1. Строится множество орбит. Из каждой орбиты выбирается наибольший представитель, то есть вершина с максимальным номером. Каждый представитель раскрашивается во все

цвета от 2 до $k$. Все получающиеся раскраски проверяются перекрашиванием — если перекрашенная раскраска меньше проверяемой, то проверяемая раскраска отсекается.

Раскраска перекрашивается следующим образом: инициализируем переменную $l$ первым цветом; циклически проходимся по всем вершинам; если текущая вершина ранее не встречалась в раскраске, присваиваем ей цвет $l$ и увеличиваем $l$ на единицу; если вершина уже присутствовала в раскраске, раскрашиваем её в присвоенный ей цвет. Генерация заканчивается, когда на очередном шаге не останется неотсеченных раскрасок.

## 4. Алгоритм генерации неизоморфных раскрасок методом Рида — Фараджева

Алгоритмы 1–3 формализуют процедуру генерации неизоморфных раскрасок методом Рида — Фараджева. Для вычисления орбит по заданному разбиению используется программа nauty [5], реализованная по разработанному Б. МакКеем алгоритму [6].

Полученные алгоритмом 1 раскраски удовлетворяют условию неизоморфности. Проверка на изоморфизм не используется.

**Алгоритм 1.** Генерация неизоморфных раскрасок методом Рида — Фараджева

**Вход:** $g$ — граф $G = (V, \alpha)$; $k$ — количество цветов, $1 \leqslant k \leqslant |V|$.

1: $clr := (1, \ldots, 1)$, $|clr| = |V|$ *// $clr_i$ — цвет вершины $i$*
2: genecolor_procedure$(g, k, clr)$ *// вызов процедуры перебора раскрасок*

**Алгоритм 2.** Перебор раскрасок genecolor_procedure

**Вход:** $g$ — граф $G = (V, \alpha)$; $k$ — количество цветов, $1 \leqslant k \leqslant |V|$; $clr$ — вектор цветов вершин графа.

1: $orbs :=$ nauty_calculate_orbits$(g, clr)$ *// вызов функции программы nauty*
2: **Для всех** $orb$ in $orbs$
3: $maxorb \leftarrow \max(orb)$, $current := 2$.
4: **Пока** $current \leqslant k$
5: $prevcolor := clr[maxorb]$, $clr[maxorb] := current$;
6: $reclr :=$ recolor_procedure$(clr)$; *// вызов процедуры перекрашивания*
7: $less :=$ `true`.
8: **Для** $i$ от 0 до $n - 1$
9: $less := less$ & $(reclr[i] < clr[i])$;
10: $clrcnt :=$ количество различных цветов в $clr$.
11: **Если** $less =$ `true` и $clrcnt = k$, **то**
12: **Вывести** $clr$.
13: genecolor_procedure$(g, k, clr)$ *// рекурсивный вызов процедуры перебора раскрасок*
14: $clr[maxorb] := clr[maxorb]$, $current := current + 1$.

**Алгоритм 3.** Перекрашивание раскраски recolor_procedure

**Вход:** $clr$ — вектор цветов вершин графа.
**Выход:** $reclr$ — вектор цветов вершин графа, подвергшийся процедуре перекраски.

```
1: cur := 1, clrmap := (−1, ..., −1), |clrmap| = |clr|, i := 0.
2: Пока i < n
3:    Если clrmap[clr[i]] = −1, то
4:       reclr[i] := cur, clrmap[clr[i]] := cur, cur := cur + 1,
5:    иначе
6:       reclr[i] := clrmap[clr[i]].
7:    i := i + 1.
```

ЛИТЕРАТУРА

1. *Hayes J. P.* A graph model for fault-tolerant computing system // IEEE Trans. Comput. 1976. V. C.25. No. 9. P. 875–884.
2. *Абросимов М. Б.* Графовые модели отказоустойчивости. Саратов: Изд-во Сарат. ун-та, 2012. 192 с.
3. *Brinkmann G.* Isomorphism rejection in structure generation programs // Discrete Mathematical Chemistry. DIMACS Ser. Discr. Math. Theor. Comput. Sci. 2000. V. 51. P. 25–38.
4. *Абросимов М. Б., Разумовский П. В.* О генерации неизоморфных вершинных $k$-раскрасок // Прикладная дискретная математика. Приложение. 2017. № 10. С. 136–138.
5. *McKay B. D.* Nauty and Traces: Graph canonical labeling and automorphism group computation // `http://users.cecs.anu.edu.au/~bdm/nauty/nug26.pdf`. 2017.
6. *McKay B. D. and Piperno A.* Practical graph isomorphism // J. Symbolic Computation. 2013. V. 2. No. 60. P. 94–112.

УДК 519.1 DOI 10.17223/2226308X/12/49

## ОБ ИНДЕКСАХ СОСТОЯНИЙ В КОНЕЧНЫХ ДИНАМИЧЕСКИХ СИСТЕМАХ ОРИЕНТАЦИЙ ПОЛНЫХ ГРАФОВ

А. В. Жаркова

Рассматриваются конечные динамические системы ориентаций полных графов. Состояниями системы являются все возможные ориентации данного полного графа, а эволюционная функция задаётся следующим образом: динамическим образом данного орграфа является орграф, полученный из исходного путём переориентации всех дуг, входящих в стоки, других отличий между исходным орграфом и его образом нет. Предлагается алгоритм вычисления индексов состояний системы, находится максимальный из индексов состояний, приводятся соответствующие таблицы для данных конечных динамических систем ориентаций полных графов с количеством вершин от двух до семи включительно.

**Ключевые слова:** *граф, индекс, конечная динамическая система, ориентация графа, полный граф, турнир, эволюционная функция.*

Графовые модели, в которых отказы процессоров интерпретируются как удаление соответствующих вершин, а отказы сетевых каналов — как удаление дуг, занимают важное место в задачах, связанных с отказоустойчивостью компьютерных сетей. При изучении модельных графов можно применять идеи и методы теории конечных

динамических систем (см., например, [1 – 3]). В модели [1] в качестве механизма восстановления работоспособности сети предлагается так называемая SER-динамика бесконтурных связных ориентированных графов. В настоящей работе полные графы изучаются с точки зрения динамического подхода к отказоустойчивости графовых систем.

Под *ориентированным графом* (*орграфом*) понимается пара $\overrightarrow{G} = (V, \beta)$, где $V$ — конечное непустое множество вершин, а $\beta \subseteq V \times V$ — отношение (смежности) на множестве $V$ (пара $(u, v) \in \beta$ называется *дугой* орграфа с *началом* $u$ и *концом* $v$). Отсутствие петель в орграфе $\overrightarrow{G}$ означает антирефлексивность его отношения смежности. *Неориентированным графом* (*графом*) называется пара $G = (V, \beta)$, где $\beta$ — симметричное и антирефлексивное отношение на множестве вершин $V$. Дуги неориентированного графа называют *рёбрами*. Орграф $\overrightarrow{G} = (V, \beta)$ называется *направленным графом* (*диграфом*), если отношение $\beta$ антисимметрично. Пусть $\overrightarrow{G} = (V, \beta)$ — некоторый орграф, $v \in V$ — одна из его вершин. *Степенью исхода* вершины $v \in V$ называется число $d^+(v)$ дуг орграфа $\overrightarrow{G} = (V, \beta)$, имеющих своим началом $v$; *степень захода* вершины $v$ — это количество $d^-(v)$ дуг, имеющих $v$ своим концом. Граф $G = (V, \beta)$ называется *полным*, если любые две его вершины соединены ребром. Полный граф с $n$ вершинами обозначается символом $K_n$. Маршрут, в котором никакая дуга не встречается более одного раза, называется *путём*. Путь, каждая вершина которого принадлежит не более чем двум его дугам, называется *простым*; простой циклический путь в орграфе — *контуром*. *Турниром* называется полный направленный граф [4].

Под *конечной динамической системой* понимается пара $(S, \delta)$, где $S$ — конечное непустое множество *состояний системы*, $\delta : S \to S$ — *эволюционная функция системы*. Таким образом, каждой конечной динамической системе сопоставляется карта, представляющая собой орграф с множеством вершин $S$ и дугами из каждой вершины $s \in S$ в вершину $\delta(s)$. Компоненты связности графа, задающего динамическую систему, называются её *бассейнами*. Каждый бассейн представляет собой контур с входящими в него деревьями. Контуры, в свою очередь, называются предельными циклами или *аттракторами*.

Основными проблемами теории конечных динамических систем являются задачи отыскания эволюционных параметров системы без проведения динамики. К их числу относится *индекс* состояния (расстояние от него до аттрактора того бассейна, которому оно принадлежит), а также максимальный из индексов состояний. Автором написаны программы для ЭВМ, позволяющие вычислять различные параметры конечных динамических систем, ассоциированных с некоторыми типами графов, в частности [5]. Предложены алгоритмы вычисления индексов состояний в конечных динамических системах ориентаций некоторых типов графов [6, 7]. В данной работе предлагается алгоритм вычисления индексов состояний в конечных динамических системах ориентаций полных графов, находится максимальный из индексов состояний системы.

Пусть дан полный граф $G = (V, \beta)$, $V = \{v_1, v_2, \ldots, v_n\}$, $n > 1$, $m = n(n-1)/2$ — число рёбер. Придадим его рёбрам произвольную ориентацию, тем самым получив направленный граф (турнир) $\overrightarrow{G} = (V, \beta)$, где отношение смежности $\beta$ антирефлексивно и антисимметрично. Применим к полученному орграфу эволюционную функцию $\alpha$, которая у данного орграфа одновременно переориентирует все дуги, входящие в *стоки* (вершины с нулевой степенью исхода), а остальные дуги оставляет без изменения, в результате чего получаем орграф $\alpha(\overrightarrow{G})$. Если проделать указанные действия со всеми возможными ориентациями данного графа, то получим карту данной конечной динамической системы, состоящую из одного или нескольких бассейнов.

Таким образом, будем рассматривать конечную динамическую систему $(\Gamma_{K_n}, \alpha)$, $n > 1$, где $\Gamma_{K_n}$ — множество всех возможных ориентаций полного графа $K_n$, $|\Gamma_{K_n}| = 2^m$, а эволюционная функция $\alpha$ задаётся следующим образом: если дан некоторый орграф $\overrightarrow{G} \in \Gamma_{K_n}$, то его динамическим образом $\alpha(\overrightarrow{G})$ является орграф, полученный из $\overrightarrow{G}$ одновременной переориентацией всех дуг, входящих в стоки, других отличий между $\overrightarrow{G}$ и $\alpha(\overrightarrow{G})$ нет.

На рис. 1 изображена карта конечной динамической системы $(\Gamma_{K_3}, \alpha)$.

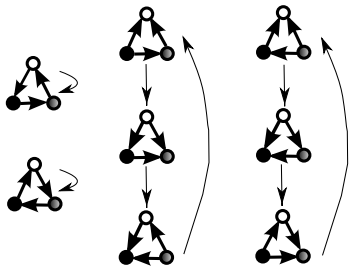

Рис. 1. Карта конечной динамической системы $(\Gamma_{K_3}, \alpha)$

**Определение 1.** Под *вектором степеней захода* ориентированного графа $\overrightarrow{G} = (V, \beta)$ будем понимать вектор, компонентами которого являются степени захода всех его вершин, то есть $(d^-(v_1), d^-(v_2), \ldots, d^-(v_n))$.

**Теорема 1.** В конечной динамической системе $(\Gamma_{K_n}, \alpha)$, $n > 1$, индекс состояния $\overrightarrow{G} \in \Gamma_{K_n}$ равен 0 тогда и только тогда, когда орграф $\overrightarrow{G}$ удовлетворяет одному из следующих условий:

1) у него нет стока;
2) его вектор степеней захода представляет собой некоторую перестановку чисел $\{0, 1, \ldots, n-1\}$.

**Теорема 2.** Пусть состояние $\overrightarrow{G} \in \Gamma_{K_n}$ конечной динамической системы $(\Gamma_{K_n}, \alpha)$, $n > 1$, имеет сток и вектор степеней захода $(d^-(v_1), d^-(v_2), \ldots, d^-(v_n))$, отличный от любой из перестановок чисел $\{0, 1, \ldots, n-1\}$, и $f$ — мощность наибольшего множества вида $\{n-1, n-2, \ldots, n-f\} \subseteq \{d^-(v_1), d^-(v_2), \ldots, d^-(v_n)\}$, тогда индекс состояния $\overrightarrow{G}$ равен $f$.

**Алгоритм 1.** Алгоритм вычисления индекса состояния системы $(\Gamma_{K_n}, \alpha)$, $n > 1$

1: Для состояния $\overrightarrow{G}$ построить его вектор степеней захода $(d^-(v_1), d^-(v_2), \ldots, d^-(v_n))$.
2: **Если** $n - 1 \notin \{d^-(v_1), d^-(v_2), \ldots, d^-(v_n)\}$, **то**
3: $\quad i(\overrightarrow{G}) := 0$, конец алгоритма.
4: **Если** Если вектор степеней захода $(d^-(v_1), d^-(v_2), \ldots, d^-(v_n))$ представляет собой перестановку чисел $\{0, 1, \ldots, n-1\}$, **то**
5: $\quad i(\overrightarrow{G}) := 0$, конец алгоритма.
6: Построить наибольшее множество вида $\{n-1, n-2, \ldots, n-f\} \subseteq \{d^-(v_1), d^-(v_2), \ldots, d^-(v_n)\}$.
7: $i(\overrightarrow{G}) := f$, конец алгоритма.

**Теорема 3.** Алгоритм 1 корректен.

**Теорема 4.** В конечной динамической системе $(\Gamma_{K_n}, \alpha)$ максимальный из индексов состояний равен 0 при $n = 2$ и $n - 3$ при $n > 2$.

В таблице приведены данные о количестве состояний с разными индексами в конечных динамических системах $(\Gamma_{K_n}, \alpha)$ для $1 < n < 8$, полученные с помощью вычислительных экспериментов. Можно заметить, что большинство состояний имеют индекс 0 (являются циклическими).

| $n$ | Индекс | | | | |
|---|---|---|---|---|---|
| | 0 | 1 | 2 | 3 | 4 |
| 2 | 2 | – | – | – | – |
| 3 | 8 | – | – | – | – |
| 4 | 56 | 8 | – | – | – |
| 5 | 824 | 160 | 40 | – | – |
| 6 | 27344 | 4224 | 960 | 240 | – |
| 7 | 1872816 | 186368 | 29568 | 6720 | 1680 |

## ЛИТЕРАТУРА


1. *Barbosa V. C.* An Atlas of Edge-Reversal Dynamics. London: Chapman & Hall/CRC, 2001.
2. *Colon-Reyes O., Laubenbacher R., and Pareigis B.* Boolean monomial dynamical systems // Ann. Combinatorics. 2004. V. 8. P. 425–439.
3. *Салий В. Н.* Об одном классе конечных динамических систем // Вестник Томского гос. ун-та. Приложение. 2005. № 14. С. 23–26.
4. *Богомолов А. М., Салий В. Н.* Алгебраические основы теории дискретных систем. М.: Наука, Физматлит, 1997.
5. *Власова А. В.* Исследование эволюционных параметров в динамических системах двоичных векторов. Свидетельство о государственной регистрации программы для ЭВМ № 2009614409, выданное Роспатентом. Заявка № 2009613140. Дата поступления 22 июня 2009 г. Зарегистрировано в Реестре программ для ЭВМ 20 августа 2009 г.
6. *Жаркова А. В.* Индексы в динамической системе $(B, \delta)$ двоичных векторов // Изв. Сарат. ун-та. Нов. сер. Сер. Математика. Механика. Информатика. 2011. Т. 11. Вып. 3. Ч. 1. С. 116–122.
7. *Жаркова А. В.* Индексы состояний в динамической системе двоичных векторов, ассоциированных с ориентациями пальм // Изв. Сарат. ун-та. Нов. сер. Сер. Математика. Механика. Информатика. 2016. Т. 16. Вып. 4. С. 475–484.


УДК 519.17 DOI 10.17223/2226308X/12/50

# ПОСТРОЕНИЕ МИНИМАЛЬНЫХ РАСШИРЕНИЙ ГРАФА МЕТОДОМ КАНОНИЧЕСКИХ ПРЕДСТАВИТЕЛЕЙ

И. А. К. Камил, Х. Х. К. Судани, А. А. Лобов, М. Б. Абросимов

Граф $G^*$ называется вершинным (рёберным) $k$-расширением графа $G$, если после удаления любых $k$ вершин (рёбер) из графа $G^*$ граф $G$ вкладывается в получившийся граф. Вершинное (рёберное) $k$-расширение графа $G$ называется минимальным, если оно имеет наименьшее число вершин и рёбер среди всех вершинных (рёберных) $k$-расширений графа $G$. Предлагается алгоритм построения всех неизоморфных минимальных вершинных (рёберных) $k$-расширений заданного графа без проверки на изоморфизм.

**Ключевые слова:** *отказоустойчивость, расширение графа, изоморфизм, канонический код, метод канонических представителей.*

В разработке безопасных систем большое значение имеет отказоустойчивость. Под отказоустойчивостью понимается свойство системы сохранять работоспособность после отказа. В 1976 г. John P. Hayes [1] предложил основанную на графах модель для исследования отказоустойчивости элементов. Позднее модель была распространена на отказы связей [2]. Формализацией отказоустойчивой реализации системы является расширение графа системы [3].

Граф $G^* = (V^*, \alpha^*)$ называется *минимальным вершинным $k$-расширением* $n$-вершинного графа $G = (V, \alpha)$, если выполняются следующие условия:

1) граф $G^*$ является вершинным $k$-расширением графа $G$, то есть $G$ вкладывается в каждый граф, получающийся из $G^*$ удалением любых его $k$ вершин;
2) граф $G^*$ содержит $n + k$ вершин, то есть $|V^*| = |V| + k$;
3) $\alpha^*$ имеет минимальную мощность при выполнении условий 1 и 2.

Граф $G^* = (V^*, \alpha^*)$ называется *минимальным рёберным $k$-расширением* $n$-вершинного графа $G = (V, \alpha)$, если выполняются следующие условия:

1) граф $G^*$ является рёберным $k$-расширением графа $G$, то есть $G$ вкладывается в каждый граф, получающийся из $G^*$ удалением любых его $k$ рёбер;
2) граф $G^*$ содержит $n$ вершин, то есть $|V^*| = |V|$;
3) $\alpha^*$ имеет минимальную мощность при выполнении условий 1 и 2.

Определение минимального рёберного $k$-расширения отличается тем, что дополнительные вершины не добавляются. Задача построения минимальных вершинных и рёберных $k$-расширений является вычислительно сложной [4]. Для построения минимальных $k$-расширений графов с малым числом вершин можно использовать переборный алгоритм 1 [3].

**Алгоритм 1.** Построение всех минимальных вершинных $k$-расширений графа

1: $m := 0$.
2: $m := m + 1$.
3: Строим все графы, получающиеся из графа $G$ добавлением $k$ вершин и $m$ дополнительных рёбер.
4: Выбираем среди построенных графов вершинные $k$-расширения графа $G$.
5: Если на шаге 4 не было найдено графов, то переходим на шаг 2.
6: Среди графов, выбранных на шаге 4, оставляем по одному представителю от классов изоморфных графов.

Для построения минимальных рёберных $k$-расширений на шаге 3 не нужно добавлять $k$ вершин, а на шаге 4 нужно проверять, является ли граф рёберным $k$-расширением. Далее будем рассматривать задачу построения минимальных вершинных $k$-расширений, хотя все идеи применимы и для построения минимальных рёберных $k$-расширений.

У алгоритма 1 можно выделить несколько недостатков, связанных с избыточным перебором. Один из них состоит в следующем: если на шаге 3 могут появляться изоморфные графы, то необходимо хранить все построенные расширения, чтобы на шаге 6 исключить изоморфные копии. Если на шаге 3 строить только неизоморфные графы, то необходимость хранения всех построенных расширений исчезнет. Можно использовать метод канонических представителей, при котором из каждого класса изоморф-

ных графов выбирается один канонический представитель. Идея метода в общем виде состоит в следующем [5]:

1) определяется способ кодирования графов;
2) среди всех кодов изоморфных графов выбирается канонический код (представитель);
3) порождаются все возможные коды графов;
4) порождённый граф принимается, если его код канонический, в противном случае исключается.

Получим алгоритм 2.

**Алгоритм 2.** Построение всех минимальных вершинных $k$-расширений графа без проверки на изоморфизм

1: $m := 0$.
2: $m := m + 1$.
3: Строим все неизоморфные графы, получающиеся из графа $G$ добавлением $k$ вершин и $m$ рёбер.
4: Выбираем среди построенных графов вершинные $k$-расширения графа $G$.
5: Если на шаге 4 не было найдено графов, то переходим на шаг 2.
6: Полученные на шаге 4 графы являются минимальными вершинными $k$-расширениями графа $G$.

Для использования метода канонических представителей самым важным является выбор канонического кода. Предлагается взять код, основанный на матрице смежности графа. Для простых неориентированных графов матрица смежности симметрична относительно главной диагонали, а на главной диагонали расположены нули.

Через $G$ обозначим граф, для которого требуется найти минимальное вершинное или рёберное $k$-расширение, через $H$ — граф, для которого будем строить код. Если число вершин в графе $G$ меньше числа вершин графа $H$, то добавляем к графу $G$ изолированные вершины. Определим код $C_G(H)$ графа $H$ следующим образом: будем дважды просматривать элементы матрицы смежности графа $G$, находящиеся выше главной диагонали, по столбцам слева направо и выписывать соответствующие элементы матрицы смежности графа $H$ по следующим правилам:

1) в первый раз выписываем элемент матрицы смежности $H$, если в матрице смежности $G$ стоит 1;
2) во второй раз выписываем элемент матрицы смежности $H$, если в матрице смежности $G$ стоит 0.

В столбце элементы матрицы смежности перечисляются сверху вниз. На рис. 1 приведён пример построения кода.

Будем называть граф $H$ каноническим относительно $G$ (либо просто каноническим) и его код каноническим, если среди всех графов, изоморфных $H$, код графа $H$ является лексикографически наибольшим:

$$\forall\, R \cong H, R \neq H\big(C_G(R) < C_G(H))\big).$$

Если $G$ является частью графа $H$, то $C_G(G) \leqslant C_G(H)$, иначе $C_G(G) > C_G(H)$.

Справедливо следующее утверждение: граф $G$ вкладывается в граф $H$ тогда и только тогда, когда существует $W \cong H$, такой, что $C_G(W) \geqslant C_G(G)$. Это означает, что


Рис. 1. Пример построения кода $C_G(H)$

если граф $G$ вкладывается в граф $H$, то существует изоморфный ему канонический граф $W$, для которого $C_G(W) \geqslant C_G(G)$. Таким образом, канонический представитель класса изоморфизма каждого графа, в который вкладывается $G$, может быть получен добавлением рёбер в граф $G$. Следовательно, алгоритм 2 является корректным.

## ЛИТЕРАТУРА

1. *Hayes J. P.* A graph model for fault-tolerant computing system // IEEE Trans. Comput. 1976. V. C.25. No. 9. P. 875–884.
2. *Harary F. and Hayes J. P.* Edge fault tolerance in graphs // Networks. 1993. V. 23. P. 135–142.
3. *Абросимов М. Б.* Графовые модели отказоустойчивости. Саратов: Изд-во Сарат. ун-та, 2012. 192 с.
4. *Абросимов М. Б.* О сложности некоторых задач, связанных с расширениями графов // Матем. заметки. 2010. № 5(88). С. 643–650.
5. *Brinkmann G.* Isomorphism rejection in structure generation programs // DIMACS Series Discr. Math. Theor. Comput. Sci. 2000. V. 51. P. 25–38

УДК 519.17 DOI 10.17223/2226308X/12/51

# К ВОПРОСУ О КРИТЕРИИ РАВЕНСТВА ЭКСПОНЕНТА РЕГУЛЯРНОГО ПРИМИТИВНОГО ГРАФА ЧИСЛУ 3

И. В. Лось, М. Б. Абросимов

Рассматривается вопрос поиска критерия равенства числу 3 экспонента регулярного примитивного графа. Получено несколько необходимых и несколько достаточных условий и показано, что ни одно из них не может быть критерием. Проведён вычислительный эксперимент для определения доли примитивных регулярных графов с экспонентом 3, на которых полученные условия не являются критериями. Получен критерий для графов диаметра 2.

**Ключевые слова:** *примитивный граф, регулярный граф, экспонент графа.*

Будем рассматривать простые неориентированные графы. Напомним некоторые определения.

*Регулярным* или *однородным* графом *порядка* $p$ называется граф, все вершины которого имеют степень $p$. *Диаметром* $\mathrm{d}(G)$ связного графа $G$ называется наибольшая длина кратчайшего пути между всеми парами вершин графа $G$. Связный граф $G$ называется *примитивным*, если между любыми двумя вершинами этого графа (в том числе из вершины в саму себя) существует маршрут длины $k$ для некоторого $k \in \mathbb{N}$.

Минимальное $k$ с таким свойством называется *экспонентом* этого примитивного графа и обозначается $\exp(G)$.

Ряд работ посвящены исследованию примитивных регулярных графов [1 – 3]. Данная работа направлена на поиск критерия равенства экспонента примитивного графа числу 3. Некоторые результаты получены в [4], здесь они дополняются.

Завершён вычислительный эксперимент с использованием кластера высокопроизводительных вычислений ПРЦ НИТ СГУ по подсчёту регулярных графов с экспонентом 3, в рамках которого построена таблица числа примитивных регулярных графов со степенью $p \leqslant 9$, числом вершин $n \leqslant 16$ и экспонентом 3.

В табл. 1 приводится результат работы программы — число графов с экспонентом 3 для различных $n$ и $p$. Символ «–» означает, что графов с такими $n$ и $p$ не существует ($p \geqslant n$ или произведение $pn$ нечётно). Серый фон клетки означает, что все связные регулярные графы со степенью $p$ и числом вершин $n$ имеют экспонент 2. В [5] показано, что это верно при $p > n/2$.

Таблица 1

**Число графов с экспонентом 3 для различных $n$ и $p$**

| $n$ | $p$ | | | | | | |
|---|---|---|---|---|---|---|---|
| | 3 | 4 | 5 | 6 | 7 | 8 | 9 |
| 4 | 0 | – | – | – | – | – | – |
| 5 | – | 0 | – | – | – | – | – |
| 6 | 1 | 0 | 0 | – | – | – | – |
| 7 | – | 0 | – | 0 | – | – | – |
| 8 | 1 | 3 | 0 | 0 | 0 | – | – |
| 9 | – | 11 | – | 0 | – | 0 | – |
| 10 | 1 | 41 | 35 | 0 | 0 | 0 | 0 |
| 11 | – | 143 | – | 0 | – | 0 | – |
| 12 | 1 | 568 | 7 506 | 2 391 | 0 | 0 | 0 |
| 13 | – | 2 403 | – | 232 080 | – | 0 | – |
| 14 | 0 | 10 377 | 3 093 569 | 18 801 129 | 2 757 433 | 0 | 0 |
| 15 | – | 42 197 | – | 1 429 344 906 | – | 0 | – |
| 16 | 0 | 151 684 | 1 797 671 946 | 112 705 503 963 | 467 764 092 656 | 34 831 303 586 | 0 |

Очевидно, что у примитивного графа с экспонентом 3 диаметр может быть 2 или 3. Для упрощения дальнейших рассуждений доказано вспомогательное утверждение — необходимое условие примитивности графа с экспонентом 3.

**Утверждение 1.** В примитивном графе с экспонентом 3 каждая вершина должна лежать хотя бы на одном цикле длины 3.

Условие не является достаточным. Например, в полном 3-вершинном графе $K_3$ каждая вершина лежит на цикле длины 3, однако его экспонент равен 2. Очевидно, что данный контрпример является минимальным по числу вершин.

Помимо этого, нетрудно найти такие регулярные графы и с экспонентом больше 3. Например, на рис. 1 приводится 3-регулярный примитивный граф с 12 вершинами и экспонентом 4, в котором каждая вершина также лежит хотя бы на одном цикле длины 3. Данный контрпример также является минимальным по числу вершин и рёбер.

Таким образом приходим к выводу, что в достаточное условие требуется включить ограничение на диаметр графа. Рассмотрим несколько таких достаточных условий, которые, однако, не являются необходимыми.

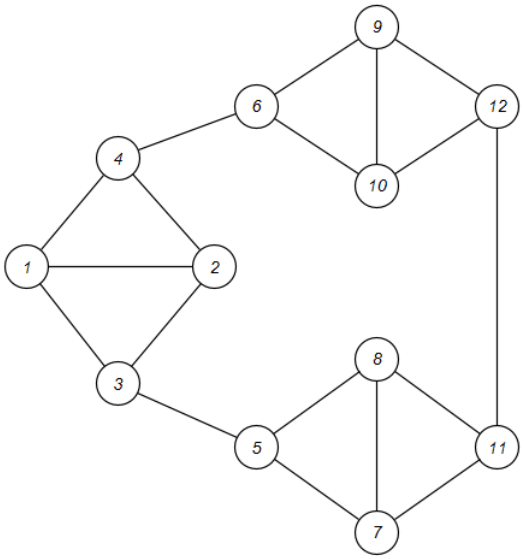


Рис. 1

**Утверждение 2.** Если в графе $G$ с диаметром $\mathrm{d}(G) \leqslant 3$ каждое ребро входит в состав некоторого цикла длины 3, то граф $G$ является примитивным с экспонентом $\exp(G) \leqslant 3$, причём если $\mathrm{d}(G) = 3$, то $\exp(G) = 3$.

На рис. 2 представлен минимальный по числу вершин регулярный граф, который показывает, что данное условие не является необходимым: в нём ребро между вершинами *3* и *5* (аналогично для ребра между вершинами *4* и *6*) не лежит ни на одном цикле длины 3.

В табл. 2 приведено количество контрпримеров для различных $n$ и $p$. Можно сделать вывод, что большая доля примитивных регулярных графов с экспонентом 3 не удовлетворяет условию утверждения 2. Поэтому усилим его.

**Утверждение 3.** Если в графе $G$ с диаметром $\mathrm{d}(G) \leqslant 3$ из каждой пары смежных рёбер хотя бы одно входит в состав некоторого цикла длины 3, то граф $G$ является примитивным с экспонентом $\exp(G) \leqslant 3$, причём если $\mathrm{d}(G) = 3$, то $\exp(G) = 3$.

Условие утверждения 3 также не является необходимым. На рис. 3 изображён минимальный по числу вершин регулярный граф, для которого условие не выполняется: рёбра (*5*,*6*) и (*5*, *8*) смежны и оба не лежат ни на одном цикле длины 3.

Табл. 3 аналогична табл. 2. Из неё видно, что число контрпримеров уменьшилось в несколько раз, однако всё ещё велико.

Однако удалось получить критерий для графов с диаметром 2.

**Теорема 1.** В графе с диаметром 2, в котором каждая вершина лежит хотя бы на одном цикле длины 3, между любыми двумя вершинами (в том числе из вершины в себя) существует маршрут длины 3.

**Следствие 1.** Граф с диаметром 2, в котором каждая вершина лежит хотя бы на одном цикле длины 3, является примитивным и его экспонент меньше или равен 3.

**Теорема 2.** Граф с диаметром 2 является примитивным и имеет экспонент 3 тогда и только тогда, когда каждая его вершина лежит хотя бы на одном цикле длины 3 и существует хотя бы одно ребро, не лежащее ни на одном цикле длины 3.

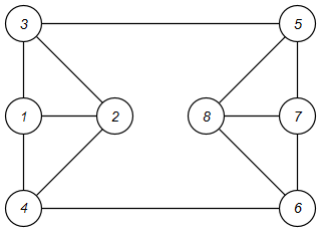


Рис. 2. 8-Вершинный граф, для которого условие, обратное утверждению 2, не выполняется

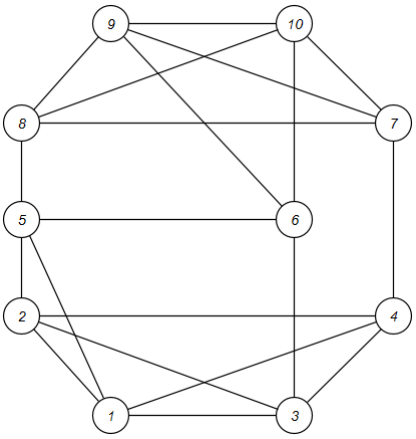


Рис. 3. 10-Вершинный граф, для которого условие, обратное утверждению 2, не выполняется

Таблица 2

**Число графов с экспонентом 3, для которых условие, обратное утверждению 2, не выполняется**

| $n$ | $p$ | | | | |
|---|---|---|---|---|---|
| | 3 | 4 | 5 | 6 | 7 |
| 4 | 0 | – | – | – | – |
| 5 | – | 0 | – | – | – |
| 6 | 0 | 0 | 0 | – | – |
| 7 | – | 0 | – | 0 | – |
| 8 | 1 | 0 | 0 | 0 | 0 |
| 9 | – | 0 | – | 0 | – |
| 10 | 1 | 24 | 0 | 0 | 0 |
| 11 | – | 123 | – | 0 | – |
| 12 | 1 | 553 | 2 235 | 0 | 0 |
| 13 | – | 2 395 | – | 0 | – |
| 14 | 0 | 10 368 | 2 858 557 | 2 401 761 | 0 |

Таблица 3

**Число графов с экспонентом 3, для которых условие, обратное утверждению 3, не выполняется**

| $n$ | $p$ | | | | |
|---|---|---|---|---|---|
| | 3 | 4 | 5 | 6 | 7 |
| 4 | 0 | – | – | – | – |
| 5 | – | 0 | – | – | – |
| 6 | 0 | 0 | 0 | – | – |
| 7 | – | 0 | – | 0 | – |
| 8 | 0 | 0 | 0 | 0 | 0 |
| 9 | – | 0 | – | 0 | – |
| 10 | 0 | 18 | 0 | 0 | 0 |
| 11 | – | 109 | – | 0 | – |
| 12 | 0 | 524 | 1 463 | 0 | 0 |
| 13 | – | 2 345 | – | 0 | – |
| 14 | 0 | 10 290 | 2 634 777 | 946 878 | 0 |

## ЛИТЕРАТУРА

1. *Jin M., Lee S. G., and Seol H. G.* Exponents of $r$-regular primitive matrices // Inform. Center Math. Sci. 2003. V. 6. No. 2. P. 51–57.
2. *Bueno M. I. and Furtado S.* On the exponent of $r$-regular primitive matrices // ELA. Electr. J. Linear Algebra. 2008. V. 17. P. 28–47.
3. *Kim B., Song B., and Hwang W.* Nonnegative primitive matrices with exponent 2 // Linear Algebra and its Appl. 2005. No. 407. P. 162–168.
4. *Лось И. В., Абросимов М. Б.* К вопросу о максимальном числе вершин в примитивных регулярных графах с экспонентом 3 // Прикладная дискретная математика. Приложение. 2018. № 11. С. 112–114.
5. *Абросимов М. Б., Костин С. В.* К вопросу о примитивных однородных графах с экспонентом, равным 2 // Прикладная дискретная математика. Приложение. 2017. № 10. С. 131–134.

УДК 519.7 DOI 10.17223/2226308X/12/52

# ПРИБЛИЖЁННЫЙ АЛГОРИТМ ПОИСКА ОПТИМАЛЬНОГО МАРШРУТА В СЕТИ С ОГРАНИЧЕНИЕМ

А. А. Солдатенко

Предлагается приближённый алгоритм RevTree решения NP-трудной задачи RCSP (Resource Constrained Shortest Path). Задача RCSP является расширением задачи о кратчайшем пути в ориентированном графе $G = (V, E)$, когда для каждой дуги $e \in E$ кроме основной весовой функции $w(e)$ дополнительно задаются функции $r_i(e)$, $i = 1, \ldots, k$, численно отражающие потребности в ресурсах, которые необходимы для передвижения по этой дуге. Задача RCSP возникает при проектировании и эксплуатации компьютерных и мультисервисных сетей. Показано, что алгоритм RevTree всегда находит допустимое решение задачи RCSP, если оно существует, за полиномиальное время, отклоняясь от оптимального решения на величину, зависящую от значений $w(e)$ и $r_i(e)$, $e \in E$.

**Ключевые слова:** *ресурсоограниченный кратчайший путь, алгоритмы на графах, оптимальная маршрутизация, компьютерные и мультисервисные сети.*

## Введение

Задача RCSP традиционно формулируется в терминах теории графов и целочисленного линейного программирования. В теоретико-графовой формулировке рассматриваемая сеть представляется ориентированным графом, вершины которого соответствуют узлам сети, а дуги — каналам связи. Предполагается, что всякая дуга обладает основным весом, например стоимостью, а также некоторыми дополнительными весами, отражающими потребности в ресурсах, которые нужны для передвижения по этой дуге. Требуется найти кратчайший путь между двумя заданными узлами сети, который удовлетворял бы заданным ограничениям на итоговые ресурсные затраты, необходимые для прохождения этого пути. Известно, что даже при одном ограничении задача RCSP является NP-трудной [1].

В настоящее время выделяют три класса методов и соответствующих им алгоритмов, способных находить точное или приближённое решение задачи RCSP: 1) методы ранжирования путей [2], 2) методы маркировки вершин [1, 3, 4] и 3) методы лагранжевой релаксации [5, 6]. Первые два класса основаны на теоретико-графовой постановке задачи, в то время как методы третьего класса исходят из постановки задачи RCSP на языке целочисленного линейного программирования. К сожалению, большинство существующих алгоритмов решения задачи RCSP медленно работают на сетях большой размерности, для многих современных приложений совершенно неприемлемы временные характеристики данных алгоритмов и их многочисленных усовершенствованных версий [3]. Поэтому остаётся актуальной разработка приближённых алгоритмов решения задачи RCSP, способных быстро находить решение на сетях большой размерности [3, 6].

## 1. Теоретико-графовая постановка задачи

Пусть сеть описана взвешенным ориентированным графом (далее — просто графом) $G = (V, E)$ без кратных дуг и петель, в котором каждая вершина $v \in V$ представляет узел сети, а каждая дуга $e \in E$ — канал связи между соответствующими узлами сети, при этом $n = |V|$ и $m = |E|$. Считаем, что на множестве дуг графа $G = (V, E)$ задана функция $w(e)\colon E \to \mathbb{R}^+$, ставящая в соответствие каждой дуге $e \in E$ её вес

$w(e) > 0$. Пусть для вершин $s, d \in V$ в графе $G$ существует путь $P$, идущий от вершины $s$ к вершине $d$. Полагаем, что вес этого $(s,d)$-пути $P$ вычисляется как сумма весов всех входящих в него дуг:

$$w(P) = \sum_{e \in P} w(e), \tag{1}$$

т. е. функция $w(e)$ является аддитивной. Если $w(e)$ — стоимость передвижения по дуге $e$, то $w(P)$ можно интерпретировать как стоимость прохождения $(s,d)$-пути $P$ в графе $G$.

Пусть для каждой дуги графа $G$ также заданы функции $r_i(e)\colon E \to \mathbb{R}^+$, $i = 1, \ldots, k$, отражающие ресурсные потребности, которые необходимы для передвижения по этой дуге, и всегда $r_i(e) > 0$. Предполагается, что все эти функции аддитивные, т. е. для любого $(s,d)$-пути $P$ верны равенства

$$r_i(P) = \sum_{e \in P} r_i(e), \ \ i = 1, \ldots, k. \tag{2}$$

Кроме того, определены величины $R_i \in \mathbb{R}^+$, $i = 1, \ldots, k$, задающие ресурсные ограничения рассматриваемой мультисервисной сети. Всякий $(s,d)$-путь $P$ называется допустимым, если он удовлетворяет ресурсным ограничениям:

$$r_i(P) \leqslant R_i, \ \ i = 1, \ldots, k. \tag{3}$$

Требуется найти $(s,d)$-путь $P$, который минимизирует целевую функцию (1) и удовлетворяет ограничениям (3). Такой путь определяет оптимальное решение задачи RCSP и называется ресурсноограниченным кратчайшим $(s,d)$-путём в графе $G = (V,E)$. Вес этого пути обозначим через OPT. Всякий допустимый $(s,d)$-путь можно рассматривать в качестве приближённого решения данной задачи. В [7] предложен эвристический алгоритм поиска приближённого решения. В настоящей работе предлагается алгоритм RevTree, который находит допустимое решение задачи RCSP за полиномиальное время, отклоняясь от оптимального решения на величину, зависящую от значений $w(e)$ и $r_i(e)$, $e \in E$, т. е. получены оценки его сложности и точности.

## 2. Описание алгоритма RevTree

Под размерностью задачи RCSP понимаются значения $n$ и $m$ — число вершин и дуг графа $G = (V,E)$ соответственно, а под её параметрами — значения функций $w(e), r_i(e)$. Для краткости вместо $r_i(e)$ и $R_i$ будем писать $r(e)$ и $R$. Опишем алгоритм RevTree для случая, когда имеется только один ресурс $R_i$ и $w(e), r_i(e)$ — положительные вещественнозначные функции.

Алгоритм RevTree состоит из двух фаз, на каждой из которых однократно выполняется известный алгоритм Дейкстры [8]. На первой фазе, исходя из функций $r(e)$, $e \in E$, вычисляется дерево путей минимального веса с корнем в вершине $d$. Это дерево определяет для каждой вершины $u \in V$ такой $(u,d)$-путь, вес которого указывает минимальный ресурс для прохождения $(u,d)$-пути. Обозначим $(u,d)$-путь через $P_2$.

Пусть $P_1$ — путь из стартовой вершины $s$ в текущую вершину $v$, найденный как некоторое допустимое решение задачи RCSP для вершин $s$ и $v$. Согласно формуле (2), для прохождения этого $(s,v)$-пути затрачен ресурс величины $r(P_1)$. Множество $\Gamma(v)$ определяет возможные направления дальнейшего движения по дугам графа $G$ из вершины $v$. Тогда для перемещения из вершины $v$ в вершину $u \in \Gamma(v)$ необходимо выполнение условия

$$r(P_1) + r(v,u) + \pi(u) \leqslant R, \tag{4}$$

где $\pi(u) = \sum\limits_{e \in P_2} r(e)$. Условие (4) гарантирует, что путь $(P_1, e, P_2)$, где $e = (v, u) \in E$, является допустимым решением задачи RCSP.

На второй фазе вновь выполняется алгоритм Дейкстры, но только с усечёнными окрестностями вершин. Усечение окрестности $\Gamma(v)$ для текущей вершины $v \in V$ осуществляется следующим образом: если для $u \in \Gamma(v)$ нарушается условие (4), то она удаляется из $\Gamma(v)$. Таким образом, алгоритм RevTree уменьшает мощность множеств $\Gamma(v)$ с учётом ресурсного ограничения $R$, что позволяет находить допустимое решение задачи RCSP, если оно существует (алгоритм 1).

**Алгоритм 1.** RevTree

**Вход:** граф $G = (V, E)$, $w(e)$, $r(e)$ для всех $e \in E$, величина $R$, вершины $s, d \in V$.
**Выход:** значение веса и последовательность вершин допустимого $(s, d)$-пути.

И н и ц и а л и з а ц и я
$w[s] := 0$; $r[s] := 0$; $p[s] := \texttt{null}$; $Passed := \varnothing$; $\pi_r[d] := 0$.
П е р в а я ф а з а
**Для всех** $v \in V \setminus \{d\}$
  $\pi_r[v] := \infty$.
**Пока** $\exists u \notin Passed$
  выбираем $u \notin Passed$ с минимальным $\pi_r[u]$; $Passed := Passed \cup \{u\}$.
  **Для всех** $v \notin Passed$ & $e = (u, v) \in E$:
    **Если** $\pi_r[v] > \pi_r[u] + r(e)$, **то**
      $\pi_r[v] := \pi_r[u] + r(e)$.
$Passed := \varnothing$.
В т о р а я ф а з а
**Для всех** $v \in V \setminus \{s\}$
  $w[v] := \infty$; $p[v] := \texttt{null}$; $r[v] := 0$.
**Пока** $\exists u \notin Passed$
  выбираем $u \notin Passed$ с минимальным $w[u]$ и $r[u] + \pi_r[v] < R$;
  $Passed := Passed \cup \{u\}$.
  **Для всех** $v \notin Passed$ & $e = (u, v) \in E$:
    **Если** $w[v] > w[u] + w(e)$, **то**
      $w[v] := w[u] + w(e)$; $r[v] := r[u] + r(e)$; $p[v] := u$.

## 3. Оценки сложности и точности алгоритма RevTree

Известно, что алгоритм Дейкстры требует $\mathcal{O}(n^2)$ времени и $\mathcal{O}(n)$ памяти [8]. На первой фазе с помощью алгоритма Дейкстры находится дерево путей минимального веса с корнем в вершине $d$, для сохранения которого необходимо $\mathcal{O}(n)$ памяти. На второй фазе в алгоритм Дейкстры добавляется проверка условия (4), которая не влияет на оценку вычислительной сложности. Поскольку обе фазы алгоритма RevTree выполняются последовательно, в целом для нахождения решения задачи RCSP затрачивается $\mathcal{O}(n^2)$ времени и $\mathcal{O}(n)$ памяти.

Оценим точность приближённого решения, формируемого алгоритмом RevTree. Для этого вычислим $\lambda_{\min} = \min\limits_{e \in E} (r(e)/w(e)) > 0$, $\lambda_{\max} = \max\limits_{e \in E} (r(e)/w(e)) > 0$. Заметим, что функции $\lambda_{\max}, \lambda_{\min}$ определены для любого $e \in E$, поскольку в формулировке задачи RCSP предполагается, что $w(e) > 0$ и $r(e) > 0$ для всех $e \in E$.

Пусть алгоритм RevTree на некотором шаге нашёл путь $P_1$, идущий из стартовой вершины $s$ в текущую вершину $v$, как оптимальное решение задачи RCSP для вершин $s$ и $v$. Если вершина $v$ совпадает с целевой вершиной $d$, то найдено оптимальное решение исходной задачи. Если вершина $v$ совпадает с $s$, то путь $P_1$ содержит пустое множество дуг и для него $w(P_1) = r(P_1) = 0$. В общем случае вершина $v$ определяет начало ещё не пройденной части искомого $(s, d)$-пути. Рассмотрим неусечённую окрестность $\Gamma(v)$ текущей вершины $v$ как множество концов дуг, исходящих из вершины $v$ и обладающих временными метками. Пусть $x \in \Gamma(v)$ — вершина, для которой $w(v, x) = \min\limits_{u \in \Gamma(v)} w(v, u)$, но не выполняется условие (4), т. е. верно соотношение

$$r(P_1) + r(v, x) + \pi(x) > R. \tag{5}$$

Именно эту вершину выбирает алгоритм Дейкстры, если окрестность $\Gamma(v)$ не подверглась усечению. При выборе вершины $u \in \Gamma(v)$, удовлетворяющей условию (4), алгоритм RevTree отклоняется от кратчайшего пути в смысле (1) без учёта ресурсного ограничения (3). Обозначим $(v, d)$-путь, найденный с помощью неусечённых окрестностей, как $P^*_{\text{rest}}$, а с помощью усечённых окрестностей — $P_{\text{rest}}$. Для путей $(P_1, P_{\text{rest}})$ и $(P_1, P^*_{\text{rest}})$ справедливы следующие неравенства:

$$w(P_1) + w(P^*_{\text{rest}}) \leqslant \text{OPT} \leqslant w(P_1) + w(P_{\text{rest}}). \tag{6}$$

В (6) величина $w(P_1)+w(P^*_{\text{rest}})$ определяет значение целевой функции для кратчайшего пути без учёта ресурсных ограничений, а $w(P_1)+w(P_{\text{rest}})$ — значение целевой функции пути, найденного алгоритмом RevTree. Предполагается, что решение задачи RCSP существует. Следовательно, найдётся хотя бы один допустимый $(s, d)$-путь, а значит, всегда существует определённый выше путь $P_{\text{rest}}$. Для прохождения всякого $(v, d)$-пути доступен ресурс $R_{\text{rest}} = R - r(P_1)$. Согласно условию (4), справедливо неравенство $R_{\text{rest}} \geqslant \pi(v)$. Исходя из определения функции $\lambda(e)$, для всякой дуги $e \in E$ имеют место соотношения

$$0 < \lambda_{\min} w(e) \leqslant r(e) \leqslant \lambda_{\max} w(e).$$

Поскольку функции $w(e)$ и $r(e)$ аддитивные, получим подобные соотношения для любого $(v, d)$-пути, в том числе $P^*_{\text{rest}}$ и $P_{\text{rest}}$:

$$0 < \lambda_{\min} w(P^*_{\text{rest}}) \leqslant r(P^*_{\text{rest}}) \leqslant \lambda_{\max} w(P^*_{rest}); \tag{7}$$

$$0 < \lambda_{\min} w(P_{\text{rest}}) \leqslant r(P_{\text{rest}}) \leqslant \lambda_{\max} w(P_{\text{rest}}). \tag{8}$$

Путь $P^*_{\text{rest}}$ по построению проходит через вершину $x$, поэтому с учётом (5) верны соотношения

$$r(P^*_{\text{rest}}) \geqslant r(v, x) + \pi(x) > R - r(P_1) = R_{\text{rest}}.$$

Здесь $\pi(x)$ — минимально необходимый ресурс для передвижения из вершины $x$ в вершину $d$. Следовательно, $r(P^*_{\text{rest}}) > R_{\text{rest}}$. Отсюда с учётом (7) получим

$$R_{\text{rest}}/\lambda_{\max} < w(P^*_{\text{rest}}). \tag{9}$$

Из соотношений (8) имеем неравенство $w(P_{\text{rest}}) \leqslant r(P_{\text{rest}})/\lambda_{\min}$. Поскольку всегда $w(P^*_{\text{rest}}) \leqslant w(P_{\text{rest}})$ и $r(P_{\text{rest}}) \leqslant R_{\text{rest}}$, то

$$w(P^*_{\text{rest}}) \leqslant r(P_{\text{rest}})/\lambda_{\min} \leqslant R_{\text{rest}}/\lambda_{\min}. \tag{10}$$

Из (9) и (10) следует

$$R_{\text{rest}}/\lambda_{\max} < w(P^*_{\text{rest}}) \leqslant R_{\text{rest}}/\lambda_{\min}. \tag{11}$$

Оценим решение, найденное алгоритмом RevTree, исходя из неравенств (6). В результате получим

$$\frac{w(P_1) + w(P_{\text{rest}}) - \text{OPT}}{\text{OPT}} \leqslant \frac{w(P_{\text{rest}}) - w(P^*_{\text{rest}})}{w(P_1) + w(P^*_{\text{rest}})}. \tag{12}$$

Наибольшее отклонение найденного решения от оптимального достигается при $v = s$ и $w(P_{\text{rest}}) = R_{\text{rest}}/\lambda_{\min}$. Тогда неравенство (12) принимает вид

$$\frac{R_{\text{rest}}/\lambda_{\min} - \text{OPT}}{\text{OPT}} \leqslant \frac{R_{\text{rest}}/\lambda_{\min} - w(P^*_{\text{rest}})}{w(P^*_{\text{rest}})}.$$

Согласно (11), справедливо $R_{\text{rest}}/\lambda_{\max} < w(P^*_{\text{rest}})$. Отсюда окончательно имеем

$$\frac{R_{\text{rest}}/\lambda_{\min} - \text{OPT}}{\text{OPT}} \leqslant \frac{R_{\text{rest}}/\lambda_{\min} - R_{\text{rest}}/\lambda_{\max}}{R_{\text{rest}}/\lambda_{\max}} = \frac{\lambda_{\max}}{\lambda_{\min}} - 1 = \varepsilon.$$

Таким образом, допустимое решение, найденное алгоритмом RevTree, отклоняется от оптимального решения задачи RCSP не более чем на величину $\varepsilon = \lambda_{\max}/\lambda_{\min} - 1$.

## 4. Вычислительные эксперименты

Для оценки результативности алгоритма RevTree проведены вычислительные эксперименты на компьютере с процессором Intel Core i7-7700K Processor (8 MB Cache, 3,60 ГГц) и ОЗУ объёмом 16 Гбайт. Осуществлялось сравнение программной реализации алгоритма RevTree и пакета IBM ILOG CPLEX [9] по времени работы, числу выполненных запросов, точности найденного решения. Заметим, что обе программы находят решение задачи RCSP, если множество допустимых решений не пусто, при этом CPLEX находит оптимальное (точное) решение. Эксперименты проводились на случайно сгенерированных графах $G_1$–$G_3$ для последовательности из 1000 случайно сгенерированных $(s, d)$-запросов (табл. 1). Для случайной генерации графов применялся метод Ваксмена с параметрами $\alpha = 0{,}15$, $\beta = 0{,}25$, который традиционно используется для генерации графов, топологически схожих с реальными компьютерными сетями [10]. Запрос считался выполненным, если для него было найдено допустимое решение задачи RCSP. Результаты экспериментов представлены в табл. 2. Согласно этим результатам, алгоритм RevTree для рассматриваемых графов находит столько же допустимых решений, что и CPLEX, при этом они совпадают и являются оптимальными. Однако во всех случаях алгоритм RevTree работает значительно быстрее пакета программ CPLEX.

Таблица 1

**Размерность и параметры задачи RCSP**

| Название графа | $n$ — число вершин | $m$ — число дуг | $\lambda_{\max}$ | $\lambda_{\min}$ | $\varepsilon$ |
|---|---|---|---|---|---|
| $G_1$ | 500 | 3923 | 0,75 | 0,6 | 0,25 |
| $G_2$ | 1000 | 16345 | 0,75 | 0,6 | 0,25 |
| $G_3$ | 1500 | 36655 | 0,75 | 0,6 | 0,25 |

Таблица 2

**Результаты сравнения алгоритма RevTree и пакета CPLEX**

| Название графа | CPLEX | | RevTree | | |
|---|---|---|---|---|---|
| | Время обработки серии запросов, с | Число выполненных запросов | Время обработки серии запросов, с | Число выполненных запросов, из них для $q$ найдено приближённое решение | |
| | | | | Всего | $q$ |
| $G_1$ | 428,265 | 910 | 2,69 | 910 | 0 |
| $G_2$ | 1607,58 | 967 | 47,524 | 967 | 0 |
| $G_3$ | 7571,22 | 676 | 94,217 | 676 | 0 |

## Заключение

Предложен полиномиальный приближённый алгоритм RevTree решения задачи RCSP при наличии только одного ресурса. Алгоритм имеет сложность по времени $\mathcal{O}(n^2)$ и всегда находит допустимое решение задачи, если оно существует, отклоняясь от оптимального решения на величину, не превышающую $\varepsilon = \lambda_{\max}/\lambda_{\min} - 1$, зависящую от параметров задачи RCSP. Эксперименты подтверждают результативность алгоритма RevTree и положений, высказанных в п. 3. Целесообразны дальнейшие исследования специальной маркировки вершин, заложенной в алгоритме RevTree.

ЛИТЕРАТУРА


1. *Joksch H. C.* The shortest route problem with constraints // J. Math. Analysis Appl. 1966. V. 14. P. 191–197.
2. *Di Puglia Pugliese L. and Guerriero F.* A survey of resource constrained shortest path-problems: exact solution approaches // J. Networks. 2013. V. 62. Iss. 3. P. 183–200.
3. *Zhu X. and Wilhelm W. E.* A three-stage approach for the resource-constrained shortest path as a sub-problem in column generation // J. Computers & Operations Research. 2012. V. 39. Iss. 2. P. 164–178.
4. *Dumitrescu I. and Boland N.* Improved preprocessing, labeling and scaling algorithms for the weight-constrained shortest path problem // J. Networks. 2003. V. 42. P. 135–153.
5. *Jepsen M., Petersen B., Spoorendonk S., and Pisinger D.* A branch-and-cut algorithm for the capacitated profitable tour problem // J. Discrete Optimization. 2014. V. 14. P. 78–96.
6. *Horvath M. and Kis T.* Solving resource constrained shortest path problems with LP-based methods // J. Computers & Operations Research. 2016. V. 73. P. 150–164.
7. *Солдатенко А. А.* Алгоритм оптимальной маршрутизации в мультисервисных телекоммуникационных сетях // Прикладная дискретная математика. Приложение. 2018. № 11. С. 122–127.
8. *Кормен Т. Х., Лейзерсон Ч. И., Ривест Р. Л., Штайн К.* Алгоритмы. Построение и анализ. М.: Вильямс, 2018. 1328 с.
9. `https://www.ibm.com/support/knowledgecenter/SSSA5P_12.6.2/ilog.odms.studio.help/pdf/usrcplex.pdf` — IBM Corp.: IBM ILOG CPLEX Optimizer Studio. CPLEX User's Manual. Version 12 Release 6, 2015.
10. *Pathan A. K., Monowar M. M., and Khan S.* Simulation Technologies in Networking and Communications: Selecting the Best Tool for the Test. CRC Press, 2017. 648 p.

УДК 519.713 DOI 10.17223/2226308X/12/53

# ПЕРЕСТРАИВАЕМЫЕ АВТОМАТЫ НА ПОДСТАНОВКАХ

В. Н. Тренькаев

Предлагается структура перестраиваемого автомата, поведение которого определяется набором базовых подстановок. Настройка автомата заключается в «сборке» функции переходов и функции выходов из базовых подстановок. Вариант «сборки» фиксируется заданием трёх изменяемых подстановок: для входного алфавита, для функции выходов, для функции переходов. Показано, что любая настройка перестраиваемого автомата соответствует приведённому сильносвязному обратимому автомату, а следовательно, предлагаемый перестраиваемый автомат может быть использован при реализации автоматных шифров, в частности шифра Закревского.

**Ключевые слова:** *перестраиваемый автомат, обратимый автомат, автоматный шифр.*

Перестраиваемые автоматы — цифровые автоматы, имеющие возможность внесения изменений в алгоритм функционирования, что реализуется с помощью настройки. Существует много вариантов архитектур перестраиваемых автоматов [1, 2], ориентированных на разные прикладные области (сети, встраиваемые системы, обработка сигналов и пр.), использующих разные способы настройки (на базе ПЗУ, ОЗУ, ПЛИС и пр.).

В данной работе рассматривается архитектура с функциональной настройкой, когда не изменяются связи между элементами автомата, но изменяется их функциональность. Областью приложения является криптография, а именно автоматные шифры [3, 4], в которых алгоритм шифрования (расшифрования) задаётся конечным автоматом. В случае автоматного шифрования каждой настройке перестраиваемого автомата, читай ключу, должен соответствовать некоторый обратимый автомат из заданного класса. Для дальнейшего изложения введём некоторые определения из [4].

**Определение 1.** *Конечным автоматом* $A$ называется пятёрка $(X, S, Y, \psi, \varphi)$, где $S$ — конечное непустое множество состояний; $X$ и $Y$ — конечные входной и выходной алфавиты соответственно; $\psi : X \times S \to S$ и $\varphi : X \times S \to Y$ — функции переходов и выходов соответственно. Далее считаем, что $X = Y = S$.

Четвёрку $s - x/y \to s'$, где $s' = \psi(x, s)$ и $y = \varphi(x, s)$, называют *переходом* автомата $A$. Говорят, что входное слово $x_1x_2 \dots x_n \in X^*$ *переводит* автомат $A$ из состояния $s$ в состояние $s'$ с выдачей выходного слова $y_1y_2 \dots y_n \in Y^*$, если существует последовательность переходов $s = s_1 - x_1/y_1 \to s_2$, $s_2 - x_2/y_2 \to s_3$, $\dots$, $s_n - x_n/y_n \to s_{n+1} = s'$.

Автомат $A$ при фиксированном состоянии $s$ реализует алфавитное отображение $f_s : X^* \to Y^*$, для которого $f_s(x_1x_2 \dots x_n) = y_1y_2 \dots y_n$.

**Определение 2.** Автомат $A$ называется *сильносвязным*, если для любых состояний $s$ и $s'$ существует входное слово, которое переводит автомат из состояния $s$ в состояние $s'$.

**Определение 3.** Автомат $A$ называется *приведённым*, если для любого состояния $s$ не существует другого состояния $s'$, такого, что $s \neq s'$ и $f_s = f_{s'}$.

**Определение 4.** Автомат $A$ *обратим*, если при любом состоянии $s$ для отображения $f_s$ существует обратное отображение $f_s^{-1}$.

Структура перестраиваемого автомата на подстановках представлена на рис. 1, где $SubX$, $SubY$, $SubS$ реализуют отображения $SubX : X \times K_X \to X$, $SubY : S \times K_Y \to S$, $SubS : S \times K_S \to S$ соответственно. Базовые компоненты $Sub1$, $Sub2$, …, $SubN$, а также настраиваемые компоненты $SubX$, $SubY$, $SubS$ при фиксированных ключах из $K_X$, $K_Y$, $K_S$ соответственно реализуют подстановки. Все базовые подстановки различны. Количество базовых подстановок совпадает с количеством состояний. Мультиплексоры $M1$ и $M2$ в зависимости от управляющего символа «пропускают» далее значение одной из базовых подстановок. $M1$ отвечает за «сборку» функции выходов, а $M2$ — функции переходов. Компонента $Reg$ в каждый момент автоматного времени хранит текущее состояние. Таким образом, перестраиваемый автомат имеет большую жёсткую логику — $N$ базовых компонент, малую программируемую логику — три компоненты $SubX$, $SubY$, $SubS$ и два мультиплексора для управления процессом «сборки». Жёсткая логика дает высокое быстродействие, а программируемая логика — гибкость.

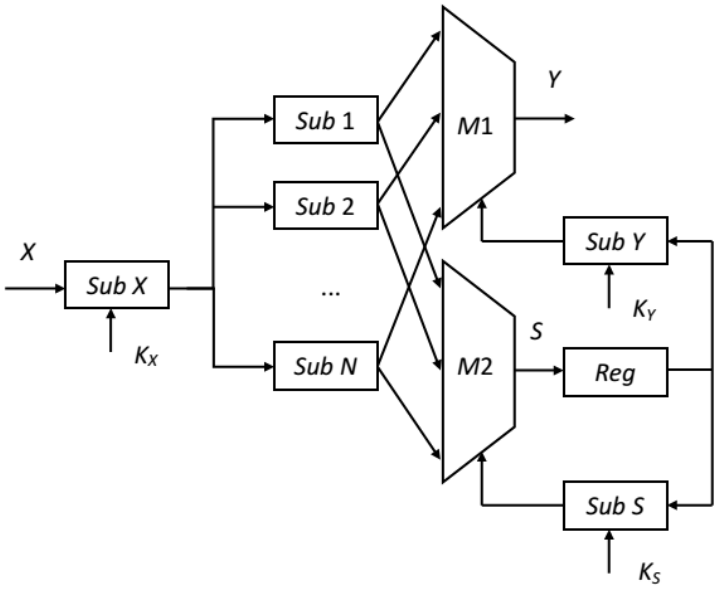


Рис. 1. Структура перестраиваемого автомата на подстановках

**Утверждение 1.** Перестраиваемый автомат на подстановках при фиксированных ключах из $K_X$, $K_Y$, $K_S$ есть приведённый сильносвязный обратимый автомат.

## ЛИТЕРАТУРА

1. *Das N. and Priya P. A.* FPGA implementation of reconfigurable Finite State Machine with input multiplexing architecture using Hungarian method // Intern. J. Reconfigurable Computing. 2018. Article ID 6831901. 15 p.
2. *Teich J. and Koster M.* (Self-)reconfigurable Finite State Machines: Theory and Implementation // Proc. DATE'02. 2002. P. 559–566.
3. *Агибалов Г. П.* Конечные автоматы в криптографии // Прикладная дискретная математика. Приложение. 2009. № 2. С. 43–73.
4. *Тренькаев В. Н.* Реализация шифра Закревского на основе перестраиваемого автомата // Прикладная дискретная математика. 2010. № 3. С. 69–77.

Секция 6

# МАТЕМАТИЧЕСКИЕ ОСНОВЫ ИНФОРМАТИКИ И ПРОГРАММИРОВАНИЯ

УДК 519.682 DOI 10.17223/2226308X/12/54

## СИНТАКСИЧЕСКИЙ АНАЛИЗ МОНОМОВ КОНТЕКСТНО-СВОБОДНЫХ ЯЗЫКОВ С УЧЁТОМ ПОРЯДКА ПРИМЕНЕНИЯ ПРОДУКЦИЙ

В. В. Кишкан, К. В. Сафонов

Ставится задача синтаксического анализа мономов контекстно-свободных языков с учётом порядка применения продукций в процессе вывода мономов. Проблема синтаксического анализа дополняется следующим образом: разработать беступиковый алгоритм для определения, можно ли вывести моном из начального символа с помощью продукций данного контекстно-свободного языка, определить, какие продукции и сколько раз были использованы для получения этого монома, а также установить, по возможности, порядок использования этих продукций. Предложен расширенный метод мономиальных меток, который позволяет установить порядок применения продукций.

**Ключевые слова:** *синтаксический анализ мономов, контекстно-свободные языки, мономиальные метки.*

Начальным объектом в теории формальных языков и грамматик является алфавит, разделённый на два подмножества, первое из которых образуют нетерминальные (вспомогательные) символы $z_1, \ldots, z_n$, необходимые для задания грамматических правил, а второе — терминальные символы $x_1, \ldots, x_m$, образующие словарь языка [1, 2].

Практически все языки программирования принадлежат важному с точки зрения приложений классу контекстно-свободных языков (КС-языков). КС-язык определяется его грамматикой — совокупностью правил подстановки (продукций)

$$z_j \to \ q_{jk}(z, x), \ j = 1, \ldots, n, \ k = 1, \ldots, p_j, \tag{1}$$

где $q_{jk}(z, x)$ — заданные мономы. Таким образом, грамматика КС-языка характеризуется тем, что один нетерминальный символ независимо от его окружения (контекста) заменяется на группу символов. Правила подстановки можно применять к начальному символу $z_1$, а затем к другим символам в мономах неограниченное число раз в любом порядке, что позволяет выводить новые мономы, которые и образуют КС-язык.

Проблема синтаксического анализа мономов (программ) КС-языка состоит в том, чтобы разработать алгоритм, позволяющий определить, можно ли вывести моном из начального символа с помощью заданных правил подстановки, а также определить, какие продукции и сколько раз были использованы при выводе этого монома. Известно, что для произвольной грамматики КС-языка беступикового алгоритма синтаксического анализа не существует, поэтому алгоритм синтаксического анализа достаточно сложен, поскольку предусматривает возвраты [1].

Традиционно считается, что порядок применения продукций устанавливать не требуется [1]. Однако без знания этого порядка невозможно вывести тот моном, который

исследуется, поскольку применение продукций в различном порядке может приводить к разным мономам.

В связи с этим предлагается расширить проблему синтаксического анализа следующим образом: разработать беступиковый алгоритм, позволяющий установить, можно ли вывести данный моном, какие продукции и сколько раз следует использовать, а также, если возможно, порядок применения этих продукций.

Для того чтобы решить расширенную проблему синтаксического анализа, мы предлагаем не только включать в моном информацию о каждой использованной продукции в виде мономиальной метки [3, 4], но и устанавливать иерархию скобок (слева от открывающейся скобки всегда «привязана» мономиальная метка, а соответствующая закрывающаяся скобка может быть однозначно найдена); иерархия скобок позволяет определить порядок использования продукций.

Рассмотрим «расширенную» грамматику для рассматриваемого КС-языка:

$$z_j \to t_{jk}[\ q_{jk}(z,x)],\ j=1,\ldots,n,\ k=1,\ldots,p_j.$$

Здесь $t_{jk}$ — символ из расширенного алфавита: мономиальная метка, соответствующая правилу вывода $z_j \to t_{jk}q_{jk}(z,x)$ и «привязанная» слева к открывающейся скобке. Расширенная грамматика позволяет определять порядок применения продукций.

**Пример 1.** Рассмотрим продукции $z_1 \to z_1z_2^3,\ \ z_1 \to z_1z_2$ и запишем их в виде расширенной грамматики:

$$z_1 \to t_{11}[\ z_1z_2^3\ ],\ z_1 \to t_{12}[\ z_1z_2\ ].$$

Применяя к начальному символу первую продукцию, а затем вторую, получим моном

$$t_{11}[\ t_{12}[\ z_1z_2\ ]\ z_2^3\ ].$$

Теперь можно видеть порядок применения продукций: внешние скобки показывают, что первая продукция с меткой $t_{11}$ применена первой, а внутренние скобки — что вторая продукция с меткой $t_{12}$, привязанной к отрывающейся скобке, применена во вторую очередь.

Иерархия скобок позволяет установить порядок применения продукций и в общем случае. Для этого рассмотрим расширенную систему уравнений Хомского — Щутценберже, которая имеет вид

$$z_j = Q_j^*(z,x,t) \stackrel{\text{def}}{=} t_{j1}[\ q_{j1}(z,x)\ ] + \ \ldots\ + t_{jp_j}[\ q_{jp_j}(z,x)\ ],\ j=1,\ \ldots\ ,n. \qquad (2)$$

Решение этой системы можно получить методом последовательных приближений [2]:

$$z^{(k+1)}(x,t) = Q^*(z^{(k)}(x,t),x,t);\ k=0,1,\ldots;\ z^{(0)}=0.$$

В результате решение получается в виде формальных степенных рядов

$$z_j = z_j^*(x,t) = \sum_{i=0}^{\infty}\langle z_j^*, w_i\rangle\ w_i,\ j=1,\ldots,n,$$

где $w_i$ — мономы от символов $x_1,\ldots,x_m,t_{11},t_{12},\ldots,t_{np_n}$ с числовыми коэффициентами $\langle z_j^*, w_i\rangle$, содержащие также систему открывающихся и закрывающихся скобок.

Считывая мономы соответствующей степени формального степенного ряда $z_1^*(x,t)$ относительно символов $x_1,\ldots,x_m$ и пропуская символы $t_{11},t_{12},\ldots,t_{np_n}$, можно выяснить, есть ли среди них нужный моном [3, 4]. При этом мономиальные метки укажут на использованные продукции, а иерархия скобок установит порядок их использования (внутренние скобки соответствуют продукциям, которые использованы позже).

**Теорема 1.** Решая расширенную систему уравнений Хомского — Щутценберже (2) методом последовательных приближений и считывая мономы нужной степени относительно терминальных символов, можно за конечное число шагов провести беступиковый синтаксический анализ (с учётом порядка применения продукций) любого монома КС-языка, заданного грамматикой (1).

ЛИТЕРАТУРА

1. *Глушков В. М., Цейтлин Г. Е., Ющенко Е. Л.* Алгебра. Языки. Программирование. Киев: Наукова думка, 1973.
2. *Salomaa A. and Soitolla M.* Automata-Theoretic Aspects of Formal Power Series. N.Y.: Springer Verlag, 1978.
3. *Egorushkin O. I., Kolbasina I. V., and Safonov K. V.* On solvability of systems of symbolic polynomial equations // Журн. СФУ. Сер. Матем. и физ. 2016. Т. 9. Вып. 2. С. 166–172.
4. *Егорушкин О. И., Колбасина И. В., Сафонов К. В.* Аналог теоремы о неявном отображении для формальных грамматик // Прикладная дискретная математика. Приложение. 2017. № 10. С. 149–151.

УДК 519.682 DOI 10.17223/2226308X/12/55

# УСЛОВИЕ РАЗРЕШИМОСТИ ПРОИЗВОЛЬНЫХ ФОРМАЛЬНЫХ ГРАММАТИК

И. В. Колбасина, К. В. Сафонов

Продолжено исследование систем некоммутативных полиномиальных уравнений, которые интерпретируются как грамматики формальных языков. Такие системы решаются в виде формальных степенных рядов (ФСР), выражающих нетерминальные символы через терминальные символы алфавита и рассматриваемых как формальные языки. Всякому ФСР поставлен в соответствие его коммутативный образ, который получается в предположении, что все символы обозначают коммутативные переменные, принимающие значения из поля комплексных чисел. В продолжение исследований совместности систем некоммутативных полиномиальных уравнений, которая напрямую не связана с совместностью её коммутативного образа, получено достаточное условие совместности в виде обобщения теоремы о неявном отображении на формальные грамматики, содержащие произвольное число уравнений. Доказано, что если для коммутативного образа системы ранг матрицы Якоби коммутативного образа системы уравнений в начале координат максимален, то исходная система некоммутативных уравнений имеет единственное решение в виде ФСР.

**Ключевые слова:** *системы полиномиальных уравнений, некоммутативные переменные, формальный степенной ряд, коммутативный образ, матрица Якоби.*

Продолжая исследование, начатое в работах [1, 2], рассмотрим систему полиномиальных уравнений

$$P_j(z, x) = 0, \quad P_j(0, 0) = 0, \quad j = 1, \ldots, k, \tag{1}$$

которая решается относительно символов $z = (z_1, \ldots, z_n)$ в виде ФСР, зависящих от символов $x = (x_1, \ldots, x_m)$.

Такие системы имеют приложения в теории формальных языков, поскольку являются грамматиками, порождающими важные классы формальных языков: контекстно-свободных, языков непосредственно составляющих, языков в нормальной форме Грейбах и др. [3, 4].

В теории формальных языков символы $x_1, \ldots, x_m$ называются терминальными и образуют словарь (алфавит) данного языка, а символы $z_1, \ldots, z_n$ называются нетерминальными и необходимы для задания грамматических правил. Над всеми символами определена некоммутативная операция умножения (конкатенации) и коммутативная операция формальной суммы, а также определена коммутативная операция умножения на комплексные числа, и потому можно рассматривать символьные многочлены и ФСР с числовыми (комплексными) коэффициентами. Наконец, мономы от терминальных символов интерпретируются как предложения языка, а каждый ФСР, который является решением системы (1), рассматривается как порождённый грамматикой формальный язык, т. е. формальная сумма всех «правильных» предложений этого языка [3, 4].

Исследовать решения символьных систем (1) достаточно трудно, поскольку некоммутативность умножения и отсутствие деления не дают возможности исключать неизвестные, и потому в работах [1, 2] наряду с некоммутативной системой (1) рассмотрен её коммутативный образ, который получается в предположении, что все переменные, входящие в систему, принимают значения из поля комплексных чисел.

Так, предположим, следуя [1], что все мономы от $x_1, \ldots, x_m$ занумерованы в лексикографическом порядке по возрастанию степеней в последовательность $u_0, u_1, \ldots$, играющую роль базиса, тогда каждый ряд $s$ можно единственным образом записать в виде разложения по этому базису с числовыми коэффициентами $\langle s, u_i \rangle$ при мономах $u_i$:

$$s = \sum_{i=0}^{\infty} \langle s, u_i \rangle u_i. \tag{2}$$

Теперь поставим в соответствие ФСР (2) его коммутативный образ $ci(s)$ — степенной ряд, который получается из $s$ в предположении, что символы $x_1, \ldots, x_m$ (равно как и $z_1, \ldots, z_n$) обозначают коммутативные переменные, принимающие значения из поля комплексных чисел [5].

В работе [1] рассмотрен коммутативный образ системы уравнений (1)

$$ci(P_j(z, x)) = 0, \quad j = 1, \ldots, k, \tag{3}$$

и отмечено, что из совместности некоммутативной системы (1) следует совместность коммутативной системы (3), однако обратное утверждение неверно. Как результат, вопрос о достаточном условии совместности системы уравнений (1), важный для приложений, оставался открытым.

В [2] получено достаточное условие совместности и единственности решения исходной некоммутативной системы (1) в терминах якобиана коммутативной системы (3), в котором предполагается, что число уравнений равно числу неизвестных.

Однако формальные полиномиальные грамматики, возникающие в приложениях, могут иметь любое число уравнений. В связи с этим обобщим аналог теоремы о неявном отображении на случай произвольных формальных грамматик, содержащих произвольное число уравнений.

Пусть

$$J(z, x) = ((ci(P_i(z, x)))'_{z_j})$$

— матрица Якоби системы уравнений (3) относительно переменных $z_1, \ldots, z_n$.

Обобщением дискретного (символьного) аналога теоремы о неявном отображении на произвольные формальные грамматики является следующая

**Теорема 1.** Если для некоммутативной символьной системы уравнений (1) выполнено условие

$$\operatorname{rank}(J(0,0)) = n,$$

то она имеет единственное решение в виде ФСР.

**Замечание 1.** Из условия теоремы вытекает существование и единственность решения для коммутативного образа системы полиномиальных уравнений; кроме того, оказывается, что из этого условия вытекает также существование и единственность решения исходной некоммутативной символьной системы уравнений (1).

Поскольку ФСР, которые являются компонентами решения системы (1), интерпретируются как формальные языки, порождённые грамматикой (1), то теорема 1 позволяет установить случаи, когда грамматика действительно определяет формальный язык.

ЛИТЕРАТУРА

1. *Egorushkin O. I., Kolbasina I. V., and Safonov K. V.* On solvability of systems of symbolic polynomial equations // Журн. СФУ. Сер. Матем. и физ. 2016. Т. 9. Вып. 2. С. 166–172.
2. *Егорушкин О. И., Колбасина И. В., Сафонов К. В.* Аналог теоремы о неявном отображении для формальных грамматик // Прикладная дискретная математика. Приложение. 2017. № 10. С. 149–151.
3. *Глушков В. М., Цейтлин Г. Е., Ющенко Е. Л.* Алгебра. Языки. Программирование. Киев: Наукова думка, 1973.
4. *Salomaa A. and Soitolla M.* Automata-Theoretic Aspects of Formal Power Series. N.Y.: Springer Verlag, 1978.
5. *Семёнов А. Л.* Алгоритмические проблемы для степенных рядов и контекстно-свободных грамматик // Докл. АН СССР. 1973. № 212. С. 50–52.

УДК 510.52 DOI 10.17223/2226308X/12/56

# О ГЕНЕРИЧЕСКОЙ СЛОЖНОСТИ ПРОБЛЕМЫ ДЕКОДИРОВАНИЯ ЛИНЕЙНЫХ КОДОВ[1]

А. Н. Рыбалов

Изучается генерическая сложность проблемы декодирования линейных кодов. Эта проблема лежит в основе известной криптосистемы Мак-Эллиса. Доказывается, что её естественная подпроблема генерически трудноразрешима (то есть трудна для почти всех входов) при условии, что проблема декодирования линейных кодов трудноразрешима в классическом смысле.

**Ключевые слова:** *генерическая сложность, линейные коды, криптосистема Мак-Эллиса.*

## Введение

Криптосистема Мак-Эллиса [1] является одной из первых криптосистем с открытым ключом. В отличие от популярных криптосистем с открытым ключом, использующих теоретико-числовые и алгебраические конструкции [2], система Мак-Эллиса основана на теории кодов, исправляющих ошибки. В этой области были найдены эффективные семейства методов преобразования и восстановления информационных блоков —

[1]Работа поддержана грантом РФФИ, проект № 18-41-550001.

так называемые коды, которые позволяют исправлять ошибки, возникающие при передаче этих блоков по каналам связи. Наиболее известные коды — это коды Рида — Маллера, Рида — Соломона, Боуза — Чоудхури — Хоквингема, Гоппы и др. Для этих кодов известны эффективные алгоритмы кодирования и декодирования [3]. Идея, лежащая в основе работы криптосистемы Мак-Эллиса, состоит в том, что «хороший» код, для которого известны эффективные алгоритмы декодирования, некоторым образом «маскируется» под более общий код — линейный. Для линейных кодов есть только эффективные алгоритмы кодирования, но неизвестно эффективных алгоритмов декодирования. Более того, доказано [4], что проблема их декодирования является NP-полной, то есть, при условии $\mathrm{P} \neq \mathrm{NP}$, таких эффективных алгоритмов не существует. Криптостойкость системы Мак-Эллиса как раз и основана на трудности проблемы декодирования линейных кодов.

В [5] развита теория генерической сложности вычислений. В рамках этого подхода алгоритмическая проблема рассматривается не на всём множестве входов, а на некотором подмножестве «почти всех» входов. Такие входы образуют так называемое генерическое множество. Понятие «почти все» формализуется введением естественной меры на множестве входных данных. С точки зрения современной криптографии интересны такие алгоритмические проблемы, которые, являясь (гипотетически) трудными в классическом смысле, остаются трудными и в генерическом смысле, т. е. для почти всех входов. Это объясняется тем, что при случайной генерации ключей в криптографическом алгоритме происходит генерация входа некоторой трудной алгоритмической проблемы, лежащей в основе алгоритма. Если проблема является генерически легкоразрешимой, то для почти всех таких входов её можно быстро решить и ключи почти всегда будут нестойкими. Поэтому проблема должна быть генерически трудной.

В работе доказывается, что естественная подпроблема проблемы декодирования линейных кодов над конечными полями $\mathrm{GF}(p)$ генерически неразрешима за полиномиальное время при условии отсутствия полиномиального вероятностного алгоритма для её решения в худшем случае. Существует правдоподобная гипотеза о том, что любой полиномиальный вероятностный алгоритм можно эффективно дерандомизировать, т. е. построить полиномиальный детерминированный алгоритм, решающий ту же задачу. Хотя это пока не доказано, имеются серьезные результаты в пользу этого [6].

## 1. Генерические алгоритмы

Пусть $I$ есть множество всех входов некоторой алгоритмической проблемы и $I_n$ — множество всех входов размера $n$. Для подмножества $S \subseteq I$ определим последовательность

$$\rho_n(S) = \frac{|S \cap I_n|}{|I_n|},\ n = 1, 2, 3, \ldots$$

Заметим, что $\rho_n(S)$ — это вероятность попасть в $S$ при случайной и равновероятной генерации входов из $I_n$. *Асимптотической плотностью* $S$ назовём предел (если он существует)

$$\rho(S) = \lim_{n\to\infty} \rho_n(S).$$

Множество $S$ называется *генерическим*, если $\rho(S) = 1$, и *пренебрежимым*, если $\rho(S) = 0$. Очевидно, что $S$ генерическое тогда и только тогда, когда его дополнение $I \setminus S$ пренебрежимо.

Алгоритм $\mathcal{A}$ с множеством входов $I$ и множеством выходов $J \cup \{?\}$ $(? \notin J)$ называется *генерическим*, если

1) $\mathcal{A}$ останавливается на всех входах из $I$;
2) множество $\{x \in I : \mathcal{A}(x) =?\}$ пренебрежимо.

Генерический алгоритм $\mathcal{A}$ вычисляет функцию $f : I \to J$, если для любого $x \in I$, такого, что $\mathcal{A}(x) \neq?$, имеет место $\mathcal{A}(x) = f(x)$. Ситуация $\mathcal{A}(x) =?$ означает, что $\mathcal{A}$ не может вычислить функцию $f$ на аргументе $x$. Условие 2 гарантирует, что $\mathcal{A}$ корректно вычисляет $f$ на почти всех входах (входах из генерического множества).

## 2. Проблема декодирования линейных кодов

Пусть $G$ — порождающая $k \times n$-матрица линейного $(n, k)$-кода над конечным полем $\mathrm{GF}(q)$, исправляющего $t$ ошибок. Проблема декодирования данного линейного кода состоит в вычислении функции $\mathrm{dec}_G : I_G \to \mathrm{GF}(q)^k$, где $I_G$ — это множество векторов $\mathbf{y} \in \mathrm{GF}(q)^n$, таких, что $\mathbf{y} = \mathbf{x}G + \mathbf{e}$, где $\mathbf{x} \in \mathrm{GF}(q)^k$, а $\mathbf{e} \in \mathrm{GF}(q)^n$ такой, что его вес Хэмминга (число ненулевых компонент) $\omega(\mathbf{e}) \leqslant t$. Обозначим также через $I_{G,e}$ множество векторов $\mathbf{y} \in \mathrm{GF}(q)^n$, таких, что $\mathbf{y} = \mathbf{x}G+\mathbf{e}$, где $\mathbf{x} \in \mathrm{GF}(q)^k$. Сама функция $\mathrm{dec}_G$ определяется следующим образом:

$$\mathrm{dec}_G(\mathbf{y}) = \mathbf{x}, \text{ если } \mathbf{y} = \mathbf{x}G + \mathbf{e}, \ \mathbf{x} \in \mathrm{GF}(q)^k, \ \omega(\mathbf{e}) \leqslant t.$$

Под размером входа понимается размерность вектора $\mathbf{y}$, то есть кодовая длина $n$.

Пусть $\mathrm{GF}(q)^* = \bigcup\limits_{k=1}^{\infty} \mathrm{GF}(q)^k$, а $I$ есть множество пар $(G, I_G)$ по всем порождающим матрицам линейных кодов $G$. Теперь определим проблему декодирования линейных кодов как проблему вычисления функции $\mathrm{dec} : I \to \mathrm{GF}(q)^*$ так, что $\mathrm{dec}(G, I_G) = \mathrm{dec}_G$. В настоящее время неизвестно полиномиальных алгоритмов (даже вероятностных) для вычисления функции dec. Более того, доказано [4], что проблема вычисления этой функции является NP-трудной, то есть, при условии $\mathrm{P} \neq \mathrm{NP}$, таких эффективных алгоритмов не существует.

Для изучения генерической сложности этой проблемы необходимо провести некоторую стратификацию на множестве входов. Рассмотрим любую бесконечную последовательность пар порождающих матриц линейных кодов и векторов ошибок над $\mathrm{GF}(q)$

$$\gamma = \{(G_1, e_1), (G_2, e_2), \ldots, (G_n, e_n), \ldots\},$$

таких, что для любого $n$ имеет место:

1) число столбцов матрицы $G_n$ равно $n$;
2) размер вектора $e_n$ равен $n$;
3) $\omega(e_n)$ не превосходит числа ошибок, которые код с матрицей $G_n$ может исправлять.

Определим функцию $\mathrm{dec}_\gamma$ как ограничение функции dec на множество $\bigcup\limits_{(G_n,e_n)\in\gamma} I_{G_n,e_n}$. Очевидно, что проблема вычисления $\mathrm{dec}_\gamma$ является подпроблемой вычисления dec. Следующая лемма показывает, что некоторые такие подпроблемы так же трудны, как и оригинальная проблема.

**Лемма 1.** Если не существует полиномиального вероятностного алгоритма для вычисления dec, то найдётся такая последовательность пар порождающих матриц линейных кодов и векторов ошибок $\gamma$, что и для вычисления $\mathrm{dec}_\gamma$ нет полиномиального вероятностного алгоритма.

***Доказательство.*** Пусть $P_1, P_2, \ldots$ — все полиномиальные вероятностные алгоритмы. Из предположения о том, что не существует полиномиального вероятностного

алгоритма для вычисления dec, следует, что для любого алгоритма $P_n$ существует бесконечно много пар $(G, e)$, для которых он не может вычислить dec. Из этого следует, что можно выбрать последовательность $\gamma' = \{(G_1, e_1), (G_2, e_2), \ldots, (G_n, e_n), \ldots\}$ так, чтобы алгоритм $P_n$ не вычислял dec для $(G_n, e_n)$ и чтобы число столбцов матриц в этой последовательности возрастало. В последовательность $\gamma'$ можно добавить пары так, чтобы для каждого $n$ там была матрица с числом столбцов $n$ — для любого $n$ существует линейный код с повторениями длины $n$. Получится нужная последовательность $\gamma$, такая, что для вычисления функции $\mathrm{dec}_\gamma$ не существует полиномиального алгоритма. ■

## 3. Основной результат

Следующий результат говорит о том, что проблема декодирования линейных кодов остаётся вычислительно трудной и в генерическом случае при условии её трудноразрешимости в худшем случае.

**Теорема 1.** Пусть $\gamma$ — любая последовательность пар порождающих матриц линейных кодов и векторов ошибок. Если существует полиномиальный генерический алгоритм, вычисляющий функцию $\mathrm{dec}_\gamma$, то существует полиномиальный вероятностный алгоритм, вычисляющий $\mathrm{dec}_\gamma$ для всех входов.

***Доказательство.*** Пусть существует полиномиальный генерический алгоритм $\mathcal{A}$, вычисляющий функцию $\mathrm{dec}_\gamma$. Построим вероятностный полиномиальный алгоритм $\mathcal{B}$, вычисляющий $\mathrm{dec}_\gamma$ на всём множестве входов. Зафиксируем размер $n$. Напомним, что множество входов $I_{G_n,e_n}$ размера $n$ есть множество векторов $\mathbf{y} \in \mathrm{GF}(q)^n$, таких, что $\mathbf{y} = \mathbf{x}G + \mathbf{e_n}$, где $\mathbf{x}$ пробегает всё множество $\mathrm{GF}(q)^k$. Алгоритм $\mathcal{B}$ на входе $\mathbf{y}$ работает следующим образом:

1) Генерирует случайно и равномерно $\mathbf{z} \in \mathrm{GF}(q)^k$.
2) Вычисляет $\mathbf{y}' = \mathbf{y} + \mathbf{z}G_n$.
3) Запускает алгоритм $\mathcal{A}$ на $\mathbf{y}'$.
4) Если $\mathcal{A}(\mathbf{y}') =?$, то выдаёт $\mathbf{0}$.
5) Если $\mathcal{A}(\mathbf{y}') = \mathbf{x}'$, то $\mathbf{x}' = \mathbf{x} + \mathbf{z}$. Выдаёт ответ $\mathbf{x} = \mathbf{x}' - \mathbf{z}$ для исходной задачи $\mathbf{y}$.

Заметим, что алгоритм $\mathcal{B}$ может выдать неправильный ответ только на шаге 4. Докажем, что вероятность этого меньше $1/2$. Действительно, множество

$$\{\mathbf{y}' = \mathbf{y} + \mathbf{z}G_n : \mathbf{z} \in \mathrm{GF}(q)^k\}$$

совпадает с множеством $I_{G_n,e_n}$ всех входов размера $n$. Но алгоритм $\mathcal{A}$ генерический, поэтому доля тех входов $\mathbf{y}'$, на которых он выдаёт неопределённый ответ, стремится к нулю с ростом $n$ и с некоторого момента становится меньше $1/2$. ■

Непосредственным следствием теоремы 1 и леммы 1 является следующее утверждение.

**Теорема 2.** Если для вычисления функции dec не существует полиномиального вероятностного алгоритма, то существует последовательность пар порождающих матриц линейных кодов и векторов ошибок $\gamma$, такая, что для вычисления функции $\mathrm{dec}_\gamma$ не существует генерического полиномиального алгоритма.

## ЛИТЕРАТУРА

1. *McEliece R. J.* A public-key cryptosystem based on algebraic coding theory // DSN Progress Report. 1978. V. 42. No. 44. P. 111–116.
2. *Романьков В. А.* Введение в криптографию. 2-е изд., испр. М.: ФОРУМ, 2012. 240 с.

3. *Рыбалов А. Н.* Введение в теорию кодов, исправляющих ошибки. Омск: Изд-во Ом. ун-та, 2007. 131 с.
4. *Berlekamp E., McEliece R., and Van Tilborg H.* On the inherent intractability of certain coding problems // IEEE Trans. Inform. Theory. 1978. V. 24(3). P. 384–386.
5. *Kapovich I., Miasnikov A., Schupp P., and Shpilrain V.* Generic-case complexity, decision problems in group theory and random walks // J. Algebra. 2003. V. 264. No. 2. P. 665–694.
6. *Impagliazzo R. and Wigderson A.* P=BPP unless E has subexponential circuits: Derandomizing the XOR lemma // Proc. 29th STOC. El Paso: ACM, 1997. P. 220–229.

Секция 7

# ВЫЧИСЛИТЕЛЬНЫЕ МЕТОДЫ В ДИСКРЕТНОЙ МАТЕМАТИКЕ

УДК 519.7 DOI 10.17223/2226308X/12/57

## О СВОЙСТВАХ МАКСИМАЛЬНОГО ЭЛЕМЕНТА МАТРИЦЫ ВЕРОЯТНОСТЕЙ ПЕРЕХОДОВ РАЗНОСТЕЙ БИЕКТИВНОГО ОТОБРАЖЕНИЯ ОТНОСИТЕЛЬНО РАЗЛИЧНЫХ ГРУППОВЫХ ОПЕРАЦИЙ

В. В. Власова, М. А. Пудовкина

Рассматриваются конечные группы $(G_1, \otimes)$, $(G_2, \odot)$ с бинарными операциями $\otimes$ и $\odot$. На практике $G_1, G_2$ обычно равны аддитивной группе $(V_m, \oplus)$ $m$-мерного векторного пространства $V_m$ над полем GF(2) или аддитивной группе $(\mathbb{Z}_{2^m}, \boxplus)$ кольца вычетов $\mathbb{Z}_{2^m}$. Среди неабелевых групп порядка $2^m$ аддитивной группе $(\mathbb{Z}_{2^m}, \boxplus)$ кольца вычетов в определённом смысле ближе всего группы, содержащие циклическую подгруппу индекса 2. Такими группами являются группа диэдра $(D_{2(m-1)}, \diamond)$ и обобщённая группа кватернионов $(Q_{2^m}, \boxtimes)$. В разностном методе и его обобщениях биективному отображению ставится в соответствие матрица вероятностей переходов разностей. В работе для всех $\otimes, \odot \in \{\oplus, \boxplus, \boxtimes, \diamond\}$ экспериментально исследуется случайная величина $q^{(\otimes,\odot)}$, равная $|G_1|p^{(\otimes,\odot)}$, где $p^{(\otimes,\odot)}$ — наибольший элемент матрицы вероятностей переходов разностей случайного биективного отображения $s : G_1 \to G_2$.

**Ключевые слова:** *матрица вероятностей переходов разностей, разностно d-равномерные отображения, S-боксы, обобщённая группа кватернионов, группа диэдра.*

Пусть $(G_1, \otimes)$, $(G_2, \odot)$ — конечные группы с бинарными операциями $\otimes$, $\odot$ и нейтральными элементами $e_1, e_2$ соответственно, $G_i^\times = G_i \setminus \{e_i\}$ для $i = 1, 2$. В симметричных шифрсистемах группа $G_1$ часто интерпретируется как группа наложения ключа, а на группе $G_2$ задаются отображения, реализующие неформально сформулированные К. Шенноном принципы рассеивания или перемешивания. На практике группы $G_1, G_2$ обычно равны аддитивной группе $(V_m, \oplus)$ $m$-мерного векторного пространства $V_m$ над полем GF(2) или аддитивной группе $(\mathbb{Z}_{2^m}, \boxplus)$ кольца вычетов $\mathbb{Z}_{2^m}$.

Произвольному биективному отображению $s : G_1 \to G_2$ поставим в соответствие матрицу переходов разностей $\mathbf{q}^{(\otimes,\odot)}(s) = \left\| q_{\varepsilon,\delta}^{(\otimes,\odot)}(s) \right\|$, элементы которой для всех $\varepsilon \in G_1^\times$, $\delta \in G_2^\times$ заданы условием

$$q_{\varepsilon,\delta}^{(\otimes,\odot)}(s) = \left| \{\alpha \in G_1 : s(\alpha \otimes \varepsilon) = s(\alpha) \odot \delta\} \right|.$$

Посредством матрицы $\mathbf{q}^{(\otimes,\odot)}(s)$ определяется матрица вероятностей переходов разностей $\hat{\mathbf{p}}^{(\otimes,\odot)}(s) = |G_1|^{-1}\mathbf{q}^{(\otimes,\odot)}(s)$ отображения $s$. Один из этапов разностного метода и его обобщений заключается в оценках элементов матрицы $\mathbf{q}^{(\otimes,\odot)}(s)$. Все элементы матрицы $\mathbf{q}^{(\otimes,\odot)}(s)$ удаётся вычислить только при небольшом порядке группы $G_1$, например 16 или 256. Если группа $G_1$ большого порядка, например $|G_1| \in \{2^{64}, 2^{128}\}$, то,

как правило, ищутся нетривиальные нижние или верхние оценки некоторых элементов матрицы $\mathbf{q}^{(\otimes,\odot)}(s)$. Одной из величин, характеризующей матрицу $\mathbf{q}^{(\otimes,\odot)}(s)$ в целом, является её максимальный элемент. Положим

$$q^{(\otimes,\odot)}(s) = \max\left\{q^{(\otimes,\odot)}_{\varepsilon,\delta}(s) : \varepsilon \in G_1^{\times}, \delta \in G_2^{\times}\right\}.$$

Через величину $q^{(\otimes,\odot)}(s)$ задаются классы криптографических отображений. Так, отображение $g : G_1 \to G_2$ называется *разностно d-равномерным*, если $d = q^{(\otimes,\odot)}(s)$ [1]. Если $d = 2$, то $g$ — *APN-отображение* [2].

Для противодействия разностному методу при синтезе XSL-алгоритмов блочного шифрования в качестве $S$-бокса, как правило, выбирается отображение $g : G_1 \to G_2$ с наименьшим значением $q^{(\otimes,\odot)}(g)$ среди всех отображений (часто биективных) из $G_1$ в $G_2$. В работах [3, 4] приведены примеры биективных отображений, для которых достигаются равенства $q^{(\oplus,\oplus)}(s) = 2$ и $q^{(\boxplus,\boxplus)}(s) = 2$ соответственно.

Пусть $F(G_1, G_2)$ — множество всех биективных отображений из $G_1$ в $G_2$. Если подстановка $s$ выбирается из множества $F(G_1, G_2)$ случайно и равновероятно, то $q^{(\otimes,\odot)}(s)$ является случайной величиной, которую будем обозначать через $q^{(\otimes,\odot)}$. Для криптографии представляет интерес нахождение распределения случайной величины $q^{(\otimes,\odot)}$, а также её различных моментов.

В [5] статистически исследована случайная величина $q^{(\otimes,\odot)}$ для следующих пар групповых операций: $(\otimes,\odot) \in \{(\oplus,\oplus), (\boxplus,\boxplus), (\boxdot,\boxdot)\}$, $\boxdot$ — умножение в $\mathbb{Z}^*_{2^m+1}$, где $2^m + 1$ — простое. В [5] при фиксированном $m \in \{4,\ldots,8\}$ для нескольких тысяч случайным образом сгенерированных $m$-битных подстановок получена выборка случайной величины $q^{(\otimes,\odot)}$ и найдено её выборочное среднее. Показано, что выборочное среднее $q^{(\oplus,\oplus)}$ больше, чем каждое из выборочных средних $q^{(\boxplus,\boxplus)}$ и $q^{(\boxdot,\boxdot)}$.

Среди неабелевых групп порядка $2^m$ аддитивной группе $(\mathbb{Z}_{2^m}, \boxplus)$ кольца вычетов в определённом смысле ближе всего группы, содержащие циклическую подгруппу индекса 2. Такими группами являются обобщённая группа кватернионов $(Q_{2^m}, \boxtimes)$ и группа диэдра с двумя образующими $u, a$ и циклической подгруппой $\langle a\rangle$ индекса 2 [6].

В настоящей работе для каждого $m \in \{4,\ldots,8\}$ с использованием классического способа [7] сгенерированы 10000 псевдослучайных $m$-битных подстановок. Для всех $\otimes, \odot \in \{\oplus, \boxplus, \boxtimes, \diamond\}$ получена выборка случайной величины $q^{(\otimes,\odot)}$ и найдено её выборочное среднее. Результаты приведены в табл. 1 для $\otimes, \odot \in \{\oplus, \boxplus, \boxtimes\}$.

Таблица 1

**Выборочное среднее выборки случайной величины $q^{(\otimes,\odot)}$ для псевдослучайных $m$-битных подстановок**

| $m$ | $(\oplus,\oplus)$ | $(\oplus,\boxplus)$ | $(\oplus,\boxtimes)$ | $(\boxplus,\oplus)$ | $(\boxplus,\boxplus)$ | $(\boxplus,\boxtimes)$ | $(\boxtimes,\oplus)$ | $(\boxtimes,\boxplus)$ | $(\boxtimes,\boxtimes)$ |
|---|---|---|---|---|---|---|---|---|---|
| 4 | 6,69896 | 4,74291 | 4,72011 | 4,73179 | 4,42389 | 4,47999 | 4,72041 | 4,4844 | 4,42092 |
| 5 | 7,94352 | 5,53062 | 5,5322 | 5,53519 | 5,17748 | 5,21568 | 5,5268 | 5,21399 | 5,19629 |
| 6 | 9,10926 | 6,24734 | 6,24682 | 6,24594 | 5,89826 | 5,91497 | 6,25189 | 5,91757 | 5,911 |
| 7 | 10,31922 | 6,88711 | 6,88434 | 6,88417 | 6,58556 | 6,59382 | 6,88643 | 6,59206 | 6,59326 |
| 8 | 11,34672 | 7,62034 | 7,62162 | 7,62201 | 7,26284 | 7,27024 | 7,62459 | 7,26751 | 7,26852 |

В работе использовалась кодировка $\nu : \{0,\ldots,2^m-1\} \to Q_{2^m}$ элементов аддитивной группы кольца вычетов $(\mathbb{Z}_{2^m}, \boxplus)$ элементами обобщённой группы кватернионов $(Q_{2^m}, \boxtimes)$, заданная условием

$$\nu : i \mapsto \begin{cases} a^{\lfloor i/2\rfloor}, & \text{если } i \text{ чётно,} \\ a^{\lfloor i/2\rfloor}u, & \text{если } i \text{ нечётно.} \end{cases}$$

Аналогичная кодировка применена для диэдральной группы.

Для 8-битных подстановок $S$-боксов алгоритмов блочного шифрования Aes, Anubis, Belt, Crypton, Fantomas, iScream, Kalyna, Khazad, Kuznyechik, Picaro, Safer, Scream, Zorro и 4-битных подстановок алгоритмов Gift, Panda, Pride, Prince, Prost, Klein, Noekeon, Piccolo вычислена $q^{(\otimes,\odot)}(s)$ для всех $\otimes, \odot \in \{\oplus, \boxplus, \boxtimes, \diamond\}$. Результаты приведены в табл. 2 для $\otimes, \odot \in \{\oplus, \boxplus, \boxtimes\}$.

Таблица 2

**$q^{(\otimes,\odot)}(s)$ для некоторых $S$-боксов**

| S-боксы | $(\oplus,\oplus)$ | $(\oplus,\boxplus)$ | $(\oplus,\boxtimes)$ | $(\boxplus,\oplus)$ | $(\boxplus,\boxplus)$ | $(\boxplus,\boxtimes)$ | $(\boxtimes,\oplus)$ | $(\boxtimes,\boxplus)$ | $(\boxtimes,\boxtimes)$ |
|---|---|---|---|---|---|---|---|---|---|
| Aes | 4 | 6 | 7 | 7 | 7 | 7 | 6 | 7 | 8 |
| Anubis | 8 | 8 | 8 | 8 | 8 | 6 | 8 | 7 | 6 |
| Belt | 8 | 6 | 6 | 3 | 7 | 6 | 4 | 7 | 7 |
| Crypton S0 | 10 | 7 | 7 | 8 | 9 | 7 | 9 | 9 | 8 |
| Crypton S1 | 10 | 8 | 7 | 8 | 9 | 10 | 9 | 9 | 10 |
| Crypton S2 | 10 | 8 | 7 | 7 | 9 | 7 | 6 | 9 | 8 |
| Crypton S3 | 10 | 8 | 7 | 8 | 9 | 8 | 7 | 9 | 8 |
| Fantomas | 16 | 16 | 16 | 20 | 12 | 13 | 16 | 12 | 13 |
| iScream | 16 | 16 | 16 | 16 | 11 | 14 | 16 | 11 | 14 |
| Kalyna pi0 | 8 | 6 | 6 | 6 | 8 | 6 | 7 | 8 | 7 |
| Kalyna pi1 | 8 | 6 | 7 | 7 | 6 | 7 | 6 | 7 | 7 |
| Kalyna pi2 | 8 | 7 | 8 | 7 | 7 | 7 | 6 | 7 | 6 |
| Kalyna pi3 | 8 | 7 | 7 | 7 | 7 | 7 | 7 | 6 | 7 |
| Khazad | 8 | 8 | 8 | 8 | 8 | 8 | 8 | 8 | 7 |
| Kuznyechik | 8 | 7 | 6 | 7 | 7 | 7 | 8 | 8 | 6 |
| Picaro | 4 | 7 | 7 | 7 | 8 | 7 | 6 | 8 | 7 |
| Safer | 128 | 10 | 10 | 128 | 2 | 4 | 128 | 4 | 8 |
| Scream | 8 | 10 | 12 | 12 | 11 | 12 | 10 | 10 | 12 |
| Zorro | 10 | 8 | 8 | 7 | 6 | 7 | 8 | 8 | 7 |
| Prost | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 5 |
| PRINCE | 4 | 4 | 4 | 4 | 5 | 4 | 4 | 4 | 4 |
| Pride | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 5 |
| Gift | 6 | 4 | 4 | 4 | 3 | 4 | 4 | 3 | 4 |
| Panda | 4 | 4 | 4 | 4 | 4 | 3 | 4 | 4 | 3 |
| Klein | 4 | 3 | 4 | 3 | 5 | 4 | 3 | 4 | 4 |
| Noekeon | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 3 |
| Piccolo | 4 | 4 | 4 | 4 | 6 | 5 | 4 | 4 | 5 |

## ЛИТЕРАТУРА


1. *Canteaut A., Duval S., and Leurent G.* Construction of lightweight $S$-boxes using Feistel and Misty structures // SAC'2015. LNSC. 2016. V. 9566. P. 373–393.
2. *Nyberg K. and Knudsen L. R.* Provable security against differential cryptanalysis // CRYPTO'92. LNCS. 1993. V. 740. P. 566–574.
3. *Nyberg K.* Differential uniform mappings for cryptography // EUROCRYPT'93. LNCS. 1993. V. 765. P. 55–64.
4. *Massey J. L.* SAFER K-64: A byte-oriented block ciphering algorithm // FSE'93. LNCS. 1994. V. 809. P. 1–16.
5. *Hawkes P. and O'Connor L.* XOR and Non-XOR differential probabilities // EUROCRYPT'99. LNCS. 1999. V. 1592. P. 272–285.
6. *Холл М.* Теория групп. М.: ИЛ, 1962.
7. *Knuth D.* The Art of Computer Programming. V. 2. Addison-Wesley, 1981.

УДК 512.55 DOI 10.17223/2226308X/12/58

# О ПРОБЛЕМЕ РАСПОЗНАВАНИЯ АЛГЕБРАИЧЕСКИХ ПОРОГОВЫХ ФУНКЦИЙ

С. В. Женевский, С. Л. Мельников, А. Н. Шурупов

Доказано существование переборного алгоритма распознавания алгебраических булевых пороговых функций путём нахождения верхних оценок абсолютных значений модуля и коэффициентов линейной формы. Оценка для модуля имеет вид $(n+3)^{(n+5)/2}/2^{n+2}$, а сложность алгоритма — $\mathrm{O}((n/2)^{n^2})$.

**Ключевые слова:** *алгебраическая булева пороговая функция, проблема распознавания.*

Интерес к алгебраическим булевым пороговым функциям обуславливается простотой их задания, а также тем, что класс алгебраических пороговых функций содержит как собственно пороговые (или линейные пороговые) булевы функции, так и линейные булевы функции. Впервые понятие и свойства алгебраических пороговых функций (булевых и многозначных) введено в [1]. Несмотря на то, что понятие алгебраической булевой пороговой функции близко к понятию булевой пороговой функции, проблема распознавания для алгебраических булевых пороговых функций пока не имеет таких ясных способов решения, которые известны для булевых пороговых функций [2]. В работе доказано существование переборного алгоритма путём нахождения верхних оценок абсолютных значений модуля и коэффициентов линейной формы.

Будем использовать следующие обозначения: $\Omega_k = \{0, 1, \ldots, k-1\}$; $r_m(a)$ — функция взятия остатка при делении целого числа $a$ на $m$; $F_k(n)$ — множество всех $k$-значных функций от $n$ переменных; $T_k(n)$ — класс всех $k$-значных пороговых функций от $n$ переменных; $AT_k(n)$ — класс всех $k$-значных алгебраических пороговых функций от $n$ переменных; $L_k(n)$ — множество всех линейных функций $k$-значной логики от $n$ переменных вида $c_0 + c_1x_1 + c_2x_2 + \ldots + c_nx_n \pmod k$.

**Определение 1.** Функцию $f : \Omega_2^n \longrightarrow \Omega_2$ назовем алгебраической булевой пороговой (а.б.п.ф.), если существуют $\omega = (\omega_0, \omega_1, \ldots, \omega_n) \in \mathbb{Z}^{n+1}$, $\theta \in \mathbb{Z}$, $m \in \mathbb{N} \setminus \{1\}$, такие, что

$$f(x_1, \ldots, x_n) = 0 \quad \Leftrightarrow \quad r_m(\omega_0 + \omega_1x_1 + \omega_2x_2 + \ldots + \omega_nx_n) < \theta,$$
$$f(x_1, \ldots, x_n) = 1 \quad \Leftrightarrow \quad r_m(\omega_0 + \omega_1x_1 + \omega_2x_2 + \ldots + \omega_nx_n) \geqslant \theta,$$

где вычисление линейной формы $\omega_0 + \omega_1x_1 + \omega_2x_2 + \ldots + \omega_nx_n$ происходит в кольце $\mathbb{Z}$, а операции сравнения производятся над полем действительных чисел $\mathbb{R}$.

Рассмотрим понятие *расшифровки* булевой функции из заданного класса $F' \subset F_k(n)$, допускающего некоторый специфичный способ задания [2]. Пусть функция $f \in F'$ задана оракулом, позволяющим по произвольной точке $x \in \Omega_2^n$ определить значение функции $f(x)$. Расшифровкой неизвестной нам функции $f \in F'$ называется процедура однозначного определения специфичного способа задания этой функции по её значениям $f(x^{(1)}), \ldots, f(x^{(t)})$ в точках $x^{(1)}, \ldots, x^{(t)}$.

В [3] вводится понятие *характеризации* пороговой функции. Под характеризацией пороговой функции понимается процедура нахождения вектора весов $\omega$ и вектора порогов $\theta$, задающих функцию. Понятие характеризации распространяется на случай алгебраических пороговых функций (а.п.ф.) — в поиск добавляется модуль.

Более общим является понятие *распознавания* пороговой функции (алгебраической пороговой). Его можно встретить в [4] как *recognition*. Распознавание пороговой функции есть процедура определения принадлежности данной функции к классу пороговых и, при положительном ответе, нахождения вектора весов и вектора порогов. Аналогично это понятие распространяется на а.п.ф.

Легко показать, что для а.п.ф. (в частности, для а.б.п.ф.) структура является неоднозначным способом задания. Приведём доказательство существования у любой а.б.п.ф. $f \in AT_2(n)$ структуры, элементы которой ограничены по абсолютной величине константой, зависящей только от количества переменных $n$. Этот факт доказывает алгоритмическую разрешимость задачи характеризации а.б.п.ф.

**Утверждение 1.** Для любой а.б.п.ф. $f \neq \text{const}$ со структурой $(\omega, \theta, m)$ верно, что $0 < \theta < m$ и всегда найдётся структура $(\omega', \theta, m)$, такая, что $0 \leqslant \omega_i' < m$, $i = 0, \ldots, n$.

***Доказательство.*** Пусть $f \neq \text{const}$. Заметим, что для любой структуры верно $0 \leqslant r_m(\omega_0 + \omega_1 x_1 + \ldots + \omega_n x_n) < m$. Если $\theta \geqslant m$, то $f \equiv 0$, так как для всех $x \in \Omega_2^n$ верно $r_m(\omega_0 + \omega_1 x_1 + \ldots + \omega_n x_n) < \theta$. Аналогично, при $\theta \leqslant 0$ может быть задана только функция $f \equiv 1$. Таким образом, имеем $0 < \theta < m$. Рассмотрим произвольную функцию $f \in AT_2(n)$. Из свойств колец вычетов следует, что

$$r_m(\omega_0 + \omega_1 x_1 + \ldots + \omega_n x_n) = r_m(r_m(\omega_0) + r_m(\omega_1)x_1 + \ldots + r_m(\omega_n)x_n).$$

То есть вектор весов $\omega' = (r_m(\omega_0), r_m(\omega_1), \ldots, r_m(\omega_n))$, порог $\theta$ и модуль $m$ образуют структуру функции $f$. ■

Далее будем рассматривать функции из множества $AT_2(n) \setminus \{\mathbf{0}, \mathbf{1}\}$ и соответствующие им структуры с весами из множества $\mathbb{Z}_m^{n+1}$ и порогами из множества $(0, m) \subset \mathbb{R}$. Заметим, что для таких функций множества $T(f)$ и $F(f)$ непусты. Из утверждения 1 следует, что для алгоритмической разрешимости задачи распознавания а.б.п.ф. достаточно доказать существование структуры с модулем, не превосходящим некоторую константу, зависящую только от числа переменных $n$. Обозначим $\dot{x} = (1, x)$. Тогда линейная комбинация $\omega_0 + \omega_1 x_1 + \omega_2 x_2 + \ldots + \omega_n x_n$ может быть записана как скалярное произведение $(\omega, \dot{x})$ векторов $\dot{x}$ и $\omega$.

Для любой функции $f$ из класса $AT_2(n) \setminus \{\mathbf{0}, \mathbf{1}\}$ справедливо следующее: существует набор $\{t_x\}_{x \in \Omega_2^n}$ целых чисел, таких, что выполняется система линейных неравенств (СЛН)

$$\begin{cases} m > (\omega, \dot{x}) + m t_x \geqslant \theta, \ x \in T(f), \\ 0 \leqslant (\omega, \dot{x}) + m t_x < \theta, \ x \in F(f). \end{cases} \tag{1}$$

**Утверждение 2.** Для всех $x \in \Omega_2^n$ верно $-n - 1 < t_x \leqslant 0$.

***Доказательство.*** Неравенство $t_x \leqslant 0$ следует из первого неравенства в (1) и того, что $\omega_i \geqslant 0$. Докажем неравенство $-n < t_x$. Предположим противное. Пусть $\exists x' \in \Omega_2^n \, (t_{x'} \leqslant -n - 1)$. Заметим, что $\forall \omega \in \mathbb{Z}_m^{n+1} \ \forall x \in \Omega_2^n \ (0 \leqslant (\omega, \dot{x}) < m(n+1))$, так как $0 \leqslant \omega_i < m$ и $0 \leqslant x_i \leqslant 1$. Тогда $(\omega, \dot{x}') + m t_{x'} \leqslant (\omega, \dot{x}') - m(n+1) < 0$. Противоречие.

Следующая система равносильна системе (1) — двойные неравенства представляются двумя одинарными:

$$\begin{cases} -(\omega, \dot{x}) - m(t_x - 1) > 0, \ x \in T(f), \\ (\omega, \dot{x}) + m t_x - \theta \geqslant 0, \ x \in T(f), \\ -(\omega, \dot{x}) - m t_x + \theta > 0, \ x \in F(f), \\ (\omega, \dot{x}) + m t_x \geqslant 0, \ x \in F(f). \end{cases} \tag{2}$$

Положим $\omega' = (\omega, -\theta, m)$, а также определим две функции $t(x)$ и $q(x)$ из $\Omega_2^{n+1}$ в $\mathbb{Z}^{n+3}$ следующим образом:

$$t(x) = \begin{cases} (\dot{x}, 1, t_x), \ x \in T(f), \\ (-\dot{x}, -1, -t_x), \ x \in F(f), \end{cases} \qquad q(x) = \begin{cases} (-\dot{x}, 0, 1 - t_x), \ x \in T(f), \\ (\dot{x}, 0, t_x), \ x \in F(f). \end{cases}$$

Эти функции являются инъективными. Перепишем систему (2), используя обозначения $\omega', x' = t(x), x'' = q(x)$, и получим эквивалентную ей систему из $2^{n+1}$ неравенств:

$$\begin{cases} (x'', \omega') > 0, \ x \in T(f), \\ (x', \omega') \geqslant 0, \ x \in T(f), \\ (x', \omega') > 0, \ x \in F(f), \\ (x'', \omega') \geqslant 0, \ x \in F(f). \end{cases} \tag{3}$$

Тогда для СЛН

$$\begin{cases} (x'', \omega') \geqslant 1, \ x \in T(f), \\ (x', \omega') \geqslant 0, \ x \in T(f), \\ (x', \omega') \geqslant 1, \ x \in F(f), \\ (x'', \omega') \geqslant 0, \ x \in F(f) \end{cases} \tag{4}$$

система (3) является следствием. ■

**Лемма 1.** Если система (1) совместна относительно неизвестных $(\omega, \theta, m)$, то система (4) совместна относительно $\omega'$.

***Доказательство.*** Пусть $(\tilde{\omega}, \tilde{\theta}, \tilde{m})$ — решение системы (1). Это решение является также решением системы (2). Значит, выполняется система

$$\begin{cases} -(\tilde{\omega}, \dot{x}) - \tilde{m}(t_x - 1) = a_x, \ x \in T(f), \\ (\tilde{\omega}, \dot{x}) + \tilde{m}t_x - \tilde{\theta} = b_x, \ x \in T(f), \\ -(\tilde{\omega}, \dot{x}) - \tilde{m}t_x + \tilde{\theta} = a_x, \ x \in F(f), \\ (\tilde{\omega}, \dot{x}) + \tilde{m}t_x = b_x, \ x \in F(f), \end{cases}$$

где $a_x > 0$, $b_x \geqslant 0$. Пусть $a' = \min\limits_{x \in \Omega_2^n} a_x$. Рассмотрим тройку $(\hat{\omega}, \hat{\theta}, \hat{m}) = \dfrac{1}{a'}(\tilde{\omega}, \tilde{\theta}, \tilde{m})$. Очевидно, что она является решением системы (2). Кроме того, $(\hat{\omega}, \hat{\theta}, \hat{m})$ — решение системы

$$\begin{cases} -(\omega, \dot{x}) - m(t_x - 1) \geqslant 1, \ x \in T(f), \\ (\omega, \dot{x}) + mt_x - \theta \geqslant 0, \ x \in T(f), \\ -(\omega, \dot{x}) - mt_x + \theta \geqslant 1, \ x \in F(f), \\ (\omega, \dot{x}) + mt_x \geqslant 0, \ x \in F(f). \end{cases} \tag{5}$$

Системы (5) и (4) совпадают. ■

**Лемма 2.** Пусть $A$ — матрица размера $n \times n$ с элементами $a_{ij} \in \{0, 1\}$. Тогда $|\det(A)| \leqslant (n+1)^{(n+1)/2}/2^n$.

***Доказательство.*** Рассмотрим матрицу $\widehat{A} = \begin{pmatrix} 1 & (-\mathbf{1})^T \\ \mathbf{1} & 2A - J \end{pmatrix}_{(n+1)\times(n+1)}$, где $J$ — матрица, полностью состоящая из единиц. Прибавив первый столбец этой матрицы ко всем остальным, получим

$$\det(\widehat{A}) = 2^n \det(A). \tag{6}$$

Из неравенства Адамара известно, что $\det(\widehat{A})^2 \leqslant \prod\limits_{i=1}^{n+1}(\sum\limits_{j=1}^{n+1}\widehat{a}_{ij}^2) \leqslant (n+1)^{n+1}$. Подставив (6) в неравенство Адамара, получим требуемое. ■

**Теорема 1.** Для любой а.б.п.ф. $f \in AT_2(n)$ существует структура с таким модулем $m$, что верно неравенство

$$m \leqslant \frac{(n+3)^{(n+5)/2}}{2^{n+2}}.$$

***Доказательство.*** Используем идеи из [5]. Пусть $f \in AT_2(n)\setminus\{\mathbf{0},\mathbf{1}\}$. Тогда система (1) совместна. Значит, по лемме 1 совместна и система (4). Рассмотрим множество решений системы (4) в пространстве $\mathbb{R}^{n+3}$. Это замкнутое множество, граничные точки которого обращают $n+3$ неравенства из СЛН (2) в равенства. Пусть $\omega^{'}$ — такая точка. Тогда имеем СЛУ $M\omega^{'} = b^{\downarrow}$, где $M$ — матрица размера $(n+3)\times(n+3)$ вида

$$\begin{pmatrix}
-x^{(1)} & 0 & 1-t_1 \\
\vdots & \vdots & \vdots \\
-x^{(l_1)} & 0 & 1-t_{l_1} \\
x^{(l_1+1)} & 1 & t_{l_1+1} \\
\vdots & \vdots & \vdots \\
x^{(l_2)} & 1 & t_{l_2} \\
-x^{(l_2+1)} & -1 & -t_{l_2+1} \\
\vdots & \vdots & \vdots \\
-x^{(l_3)} & -1 & -t_{l_3} \\
x^{(l_3+1)} & 0 & t_{l_3+1} \\
\vdots & \vdots & \vdots \\
x^{(n+2)} & 0 & t_{n+2}
\end{pmatrix},$$

а вектор $b^{\downarrow}$ лежит в $\Omega_2^{n+3}$. По правилу Крамера имеем $\omega_{n+3}^{'} = \det(M_{n+3})/\det(M)$, где $M_{n+3}$ — матрица, полученная из матрицы $M$ заменой $(n+3)$-го столбца на столбец $b^{\downarrow}$. Разложим определитель матрицы $M_{n+3}$ по $(n+3)$-му столбцу:

$$\det(M_{n+3}) = \sum_{j=1}^{n+3}(-1)^{n+3+j}\, b_j\, \det(M_{n+3\,j}).$$

Здесь матрица $M_{n+3\,j}$ — подматрица $M_{n+3}$, полученная удалением $j$-й строки и $(n+3)$-го столбца, $b_j$ — $j$-й элемент вектора $b^{\downarrow}$. Заметим, что при умножении вектора $\omega^{'}$ на любое $\alpha \geqslant 1$ мы получим решение системы (2). Тогда домножением вектора $\omega^{'}$ на $|\det(M)|$ получим целое решение СЛН (2):

$$\omega_{n+3}^{''} = \operatorname{sign}(\det(M)) \sum_{j=1}^{n+3}(-1)^{n+3+j}\, b_j\, \det(M_{n+3\,j}).$$

Оценим элемент $\omega_{n+3}^{''}$. Из леммы (2) известно, что определитель матрицы размера $n\times n$, состоящей из 0 и 1, не превосходит $(n+1)^{(n+1)/2}/2^n$. В нашем случае матрица $M_{n+3\,j}$

состоит из элементов $0, 1, -1$, но любая её строка не может содержать 1 и $-1$ одновременно. Значит, $\det(M_{n+3\,j}) = (-1)^q |\det(M_{n+3\,j})|$, где $q$ — количество неположительных строк матрицы $M_{n+3\,j}$. Для матриц $M_{ij}$ верно аналогичное. Итак, имеем

$$|\omega''_{n+3}| \leqslant \sum_{j=1}^{n+3} |b_j \det(M_{n+3\,j})| = \sum_{j=1}^{n+3} |\det(M_{n+3\,j})| \leqslant \frac{(n+3)^{(n+5)/2}}{2^{n+2}}.$$

Теорема доказана. ■

Теорема 1 позволяет сформулировать переборный алгоритм 1 распознавания а.б.п.ф. Можно ограничиться рассмотрением случая, когда веса и порог меньше модуля. На каждом шаге алгоритма фиксируется параметр $m$ и перебираются значения остальных параметров от 0 до $m-1$.

**Алгоритм 1.** Распознавание алгебраических булевых пороговых функций

**Вход:** функция $f \in F_2(n)$, заданная оракулом.

**Выход:** структура функции в случае, если $f \in AT_2(n)$, либо ответ, что функция не принадлежит классу $AT_2(n)$.

1: $m := 2$.

2: Для всех векторов $(\omega, \theta) \in \mathbb{Z}_m^{n+2}$ проверяем выполнимость системы неравенств (1). Если какой-либо вектор $(\omega_1, \theta_1)$ привёл к тому, что все неравенства оказались верными, то функция $f$ является алгебраической пороговой, а тройка $(\omega_1, \theta_1, m)$ — её структурой.

3: Если $m < (n+3)^{(n+5)/2}/2^{n+2}$, то $m := m+1$ и перейти на шаг 2, иначе функция не является а.б.п.ф. Выход.

**Утверждение 3.** Оценка сложности алгоритма распознавания а.б.п.ф. имеет вид $\mathrm{O}((n/2)^{n^2})$.

***Доказательство.*** Параметр $m$, согласно теореме 1, перебирается от 2 до $(n+3)^{(n+5)/2}/2^{n+2}$. Вектор весов и порог перебираются от 0 до $m-1$. Значит, сложность алгоритма оценивается величиной

$$\sum_{m=2}^{(n+3)^{(n+5)/2}/2^{n+2}} m^{n+2} = \frac{(n+3)^{(n^2+7n+10)/2}}{2^{n^2+4n+4}} = \mathrm{O}\left((n/2)^{n^2}\right).$$

Утверждение доказано. ■

## ЛИТЕРАТУРА


1. *Сошин Д. А.* Конструктивный метод синтеза сбалансированных $k$-значных алгебраических пороговых функций // Computational Nanotechnology. 2015. No. 4. P. 31–36.
2. *Золотых Н. Ю.* Расшифровка пороговых и близких к ним пороговых функций многозначной логики: дис. ... канд. физ.-мат. наук. Нижегородский госуниверситет. Н. Новгород, 1998.
3. *Бурделев А. В., Никонов В. Г.* О построении аналитического задания $k$-значной пороговой функции // Computational Nanotechnology. 2015. No. 2. P. 5–13.
4. *Crama Y. and Hammer P. L.* Boolean Functions: Theory, Algorithms and Applications. Encyclopedia of Mathematics and its Applications. Cambridge: Cambridge University Press, 2011.

5. *Antony M.* Discrete Mathematics of Neural Networks: Selected Topics. SIAM, Philadelphia, 2001.

УДК 621.391:519.7 DOI 10.17223/2226308X/12/59

# MDS-МАТРИЦЫ, ПОСТРОЕННЫЕ С ПОМОЩЬЮ СОПРОВОЖДАЮЩИХ МАТРИЦ МНОГОЧЛЕНОВ И ПОДСТАНОВОЧНЫХ МАТРИЦ

О. Кой Пуэнте

Предлагается новый метод построения MDS-матриц порядка $k = 4, 6$ над полем GF(256), основанный на возведении в степень сопровождающих матриц некоторых многочленов и последующим сложением с подстановочной матрицей. Оценивается число операций сложения по модулю 2, необходимых для вычисления образов векторов при действии соответствующих линейных преобразований. Построенные матрицы представляют интерес для использования в шифрсистемах, ориентированных на низкоресурсную реализацию.

**Ключевые слова:** *MDS-матрицы, сопровождающие матрицы многочленов, подстановочные матрицы, конечные поля, низкоресурсная криптография, XOR-сложность.*

## Введение

Пусть $Q = \mathrm{GF}(2^n) = \mathrm{GF}(2)[x]/g(x)$ — конечное поле из $2^n$ элементов, где $g(x)$ — неприводимый многочлен степени $n$ над полем GF(2). Множество всех вектор-строк длины $k$ над полем $Q$ обозначим через $Q^k$, а множество всех матриц размера $k \times k$ над полем $Q$ — через $Q_{k,k}$.

**Определение 1** [1]. Показатель рассеивания $\rho$ матрицы $A \in Q_{k,k}$ определяется равенством

$$\rho(A) = \min_{\mathbf{a} \neq \mathbf{0}} \{\mathrm{w}(\mathbf{a}) + \mathrm{w}(\mathbf{a}A)\},$$

где $\mathrm{w}(\mathbf{a})$ — вес Хэмминга вектора $\mathbf{a} \in Q^k$, то есть количество его ненулевых элементов.

**Определение 2** [1, 2]. Матрица $A \in Q_{k,k}$ называется MDS-матрицей, если $\rho(A) = k + 1$.

**Определение 3** [2]. Пусть $f(x) = a_0 + a_1 x + a_2 x^2 + \ldots + a_{k-1} x^{k-1} + x^k \in Q[x]$. Матрица $S_f \in Q_{k,k}$, определённая равенством

$$S_f = \begin{pmatrix} 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & & \vdots \\ 0 & 0 & 0 & \cdots & 1 \\ a_0 & a_1 & a_2 & \cdots & a_{k-1} \end{pmatrix},$$

называется сопровождающей матрицей многочлена $f(x)$.

В [3] предложено оценивать сложность реализации линейного слоя в блочных шифрсистемах подсчётом количества вентилей XOR, необходимых для реализации

умножения элемента над полем. Показано, что, в отличие от распространённого мнения, элементы с высоким весом Хэмминга также могут иметь низкую сложность реализации. Будем использовать эту новую характеристику для расчёта сложности реализации линейного слоя.

**Определение 4** [3]. XOR-сложностью элемента $\alpha \in Q$ в фиксированном базисе назовём количество операций XOR, необходимых для реализации умножения $\alpha$ на произвольный элемент $\beta \in Q$.

**Пример 1** [3]. Пусть $\mathrm{GF}(2^3) = \mathrm{GF}(2)[x]/(x^3+x+1)$ и $\{1, \alpha, \alpha^2\}$ — базис пространства $\mathrm{GF}(2^3)$ над полем $\mathrm{GF}(2)$. Умножение элемента $\alpha^4 = \alpha \oplus \alpha^2$ на произвольный элемент $\beta = b_0 \oplus b_1\alpha \oplus b_2\alpha^2$, где $b_i \in \mathrm{GF}(2)$, имеет вид

$$(b_0 \oplus b_1\alpha \oplus b_2\alpha^2)(\alpha \oplus \alpha^2) = (b_0 \oplus b_2) \oplus (b_0 \oplus b_1)\alpha \oplus (b_0 \oplus b_1 \oplus b_2)\alpha^2.$$

Элемент $\alpha^4\beta$ можно отождествить с элементом из $\mathrm{GF}(2)^3$ вида

$$(b_0 \oplus b_2,\ b_0 \oplus b_1,\ b_0 \oplus b_1 \oplus b_2),$$

в котором есть четыре операции XOR. Таким образом, XOR-сложность элемента $\alpha^4$ равна 4.

Будем обозначать XOR-сложность элемента $\alpha \in Q$ как $\mathsf{XOR}(\alpha)$. Нетрудно проверить, что $\mathsf{XOR}(0) = \mathsf{XOR}(1) = 0$. XOR-сложность строки с номером $i$ матрицы $M = (m_{i,j})_{k\times k}$ можно найти по формуле [3]

$$\sum_{j=1}^{k} \mathsf{XOR}(m_{i,j}) + (l_i - 1)n,$$

где $l_i$ — количество ненулевых элементов в $i$-й строке. Тогда можно определить XOR-сложность матрицы $M = (m_{i,j}) \in Q_{k,k}$ по формуле

$$\mathsf{XOR}(M) = \sum_{i=1}^{k}\sum_{j=1}^{k} \mathsf{XOR}(m_{i,j}) + n\sum_{i=1}^{k}(l_i - 1).$$

Пусть $f(x) = a_0 + a_1x + a_2x^2 + \ldots + a_{k-1}x^{k-1} + x^k$ и $\{c_1, \ldots, c_s\}$ — множество всех различных ненулевых коэффициентов многочлена $f(x)$. В [4] показано, что

$$\mathsf{XOR}(S_f) = \sum_{j=1}^{s} \mathsf{XOR}(c_j) + (l_f - 1)n; \tag{1}$$

$$\mathsf{XOR}(S_f^r) = r \cdot \mathsf{XOR}(S_f) \tag{2}$$

для любого $r \in \mathbb{N}$, где $l_f$ — количество ненулевых элементов в последней строке матрицы $S_f$.

## 1. Построение MDS-отображений

**Определение 5.** Будем говорить, что линейное отображение $L : Q^k \longrightarrow Q^k$, заданное по правилу

$$L(\mathbf{a}) = \mathbf{a} \cdot A_\gamma(L),$$

является MDS-отображением, если $\rho(A_\gamma(L)) = k + 1$, где $A_\gamma(L)$ — матрица линейного отображения $L$ в фиксированном базисе $\gamma$ пространства $Q^k$.

В шифрсистемах, ориентированных на низкоресурсную реализацию, существенное значение имеет XOR-сложность используемых криптографических примитивов. Нахождение MDS-отображений с небольшим значением данного параметра является актуальной проблемой.

Предложим способ построения MDS-отображений над полем $\mathrm{GF}(2^8)$ вида

$$\mathcal{L}^k_{f,P} : \mathbf{a} \mapsto \mathbf{a}(S_f^{3k/2} \oplus P)^{\mathrm{T}}, \tag{3}$$

где $S_f$ — сопровождающая матрица многочлена $f(x) \in \mathrm{GF}(2^8)[x]$ степени $k$; $P$ — подстановочная матрица порядка $k$. С целью эффективной реализации коэффициенты многочлена $f(x)$ выберем из множества $\{0, 1, \alpha, \alpha^{-1}, \alpha^2, \alpha^3\}$, где $\alpha$ — произвольный примитивный элемент поля $\mathrm{GF}(2^8)$.

Пусть $k = 4$, $\lambda_1(x) = x^4 + \alpha x^3 + \alpha$, $\lambda_2 = x^4 + \alpha^2 x^3 + \alpha^2$, $\lambda_3 = x^4 + \alpha x^3 + \alpha^{-1}$, $\lambda_4 = x^4 + \alpha^3 x^3 + \alpha^3$ и

$$P_1 = \begin{pmatrix} 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}.$$

Тогда $\mathcal{L}^4_{\lambda_i,P_1}(\mathbf{a}) = \mathbf{a}(S^6_{\lambda_i} \oplus P_1)^{\mathrm{T}}$, $i = 1, \ldots, 4$.

Пусть $\Lambda_i$ — линейное преобразование, осуществляемое регистром сдвига с характеристическим многочленом $\lambda_i(x)$, $i = 1, \ldots, 4$. Тогда действие отображения $\mathcal{L}^4_{\lambda_i,P_1}$ на вектор $\mathbf{a} = (a_0, a_1, a_2, a_3) \in \mathrm{GF}(2^8)^4$ можно схематично представить в виде рис. 1.

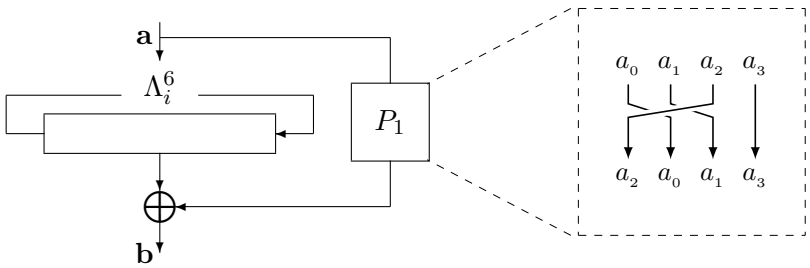


Рис. 1. Действие отображения $\mathcal{L}^4_{\lambda_i,P_1}$ при $i = 1, 2, 3, 4$

**Теорема 1.** Для любого $i = 1, \ldots, 4$ отображение $\mathcal{L}^4_{\lambda_i,P_1}$ является MDS-отображением.

Рассмотрим теперь отображения вида (3) в случае $k = 6$. Пусть $\alpha \in \mathrm{GF}(2^8)$ — корень многочлена $x^8 + x^7 + x^6 + x + 1$, $\tau_1(x) = x^6 + \alpha^{-1}x^5 + \alpha x^4 + \alpha$, $\tau_2(x) = x^6 + \alpha x^5 + {} + \alpha^{-1}x^4 + \alpha$, $\tau_3(x) = x^6 + \alpha^3 x^5 + x^4 + \alpha$, $\tau_4(x) = x^6 + \alpha^3 x^5 + x^4 + \alpha^{-1}$ и

$$P_2 = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}.$$

Тогда $\mathcal{L}^6_{\tau_i,P_2}(\mathbf{a}) = \mathbf{a}(S^9_{\tau_i} \oplus P_2)^{\mathrm{T}}$, $i = 1, \ldots, 4$.

Пусть $T_i$ — линейное преобразование, осуществляемое регистром сдвига с характеристическом многочленом $\tau_i(x)$ для любого $i = 1, \ldots, 4$. Тогда действие отображения $\mathcal{L}^6_{\tau_i,P_2}$ на вектор $\mathbf{a} = (a_0, a_1, a_2, a_3, a_4, a_5) \in \mathrm{GF}(2^8)^6$ можно схематично представить в виде рис. 2.

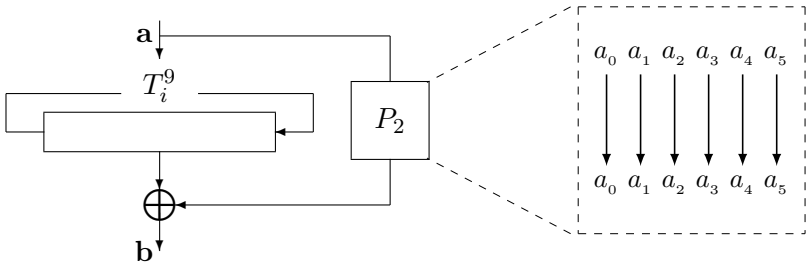


Рис. 2. Действие отображения $\mathcal{L}^6_{\tau_i,P_2}$ при $i = 1, \ldots, 4$

**Теорема 2.** Для любого $i = 1, \ldots, 4$ отображение $\mathcal{L}^6_{\tau_i,P_2}$ является MDS-отображением.

## 2. XOR-сложность некоторых MDS-отображений

Пусть $Q = \mathrm{GF}(2^8) = \mathrm{GF}(2)[x]/x^8 + x^7 + x^6 + x + 1$, $\theta$ — корень многочлена $x^8 + x^7 + x^6 + x + 1$. Записи табл. 1 соответствуют XOR-сложности элементов поля $Q$, заданных в шестнадцатеричном виде. Например, для элемента $\beta = \theta^5 + \theta^2 + \theta + 1 \in \mathrm{GF}(2^8)$ используется запись 0x27. Тогда $\mathsf{XOR}(\beta) = \mathsf{XOR}(\mathrm{0x27}) = 28$.

Таблица 1

**XOR-сложность элементов поля $Q$**

| XOR | .0 | .1 | .2 | .3 | .4 | .5 | .6 | .7 | .8 | .9 | .a | .b | .c | .d | .e | .f |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 0. | 0 | 0 | 3 | 9 | 5 | 11 | 10 | **14** | 7 | 11 | 12 | 18 | 14 | 20 | 13 | 21 |
| 1. | 12 | 18 | 11 | 19 | 13 | 17 | 18 | **24** | 17 | 23 | 22 | 26 | 12 | 20 | 23 | 29 |
| 2. | **16** | **22** | **21** | **25** | **11** | **19** | **22** | **28** | **17** | **23** | **16** | **24** | **18** | **22** | **23** | **29** |
| 3. | 20 | 24 | 25 | 31 | 27 | 33 | 26 | **34** | 11 | 19 | 22 | 28 | 24 | 30 | 29 | 33 |
| 4. | 20 | 24 | 23 | 29 | 25 | 31 | 26 | **34** | 11 | 19 | 20 | 26 | 22 | 28 | 29 | 33 |
| 5. | 18 | 24 | 25 | 29 | 15 | 23 | 24 | **30** | 19 | 25 | 20 | 28 | 22 | 26 | 25 | 31 |
| 6. | 24 | 30 | 25 | 33 | 27 | 31 | 30 | **36** | 29 | 35 | 36 | 40 | 26 | 34 | 35 | 41 |
| 7. | 10 | 18 | 19 | 25 | 21 | 27 | 28 | **32** | 25 | 29 | 28 | 34 | 30 | 36 | 31 | 39 |
| 8. | 25 | 21 | 26 | 20 | 24 | 22 | 31 | **27** | 30 | 26 | 33 | 31 | 27 | 21 | 36 | 32 |
| 9. | 11 | 5 | 20 | 16 | 22 | 18 | 25 | **23** | 22 | 20 | 29 | 25 | 31 | 27 | 32 | 26 |
| a. | 19 | 17 | 26 | 22 | 28 | 24 | 29 | **23** | 14 | 8 | 23 | 19 | 25 | 21 | 28 | 26 |
| b. | 21 | 17 | 24 | 22 | 18 | 12 | 27 | **23** | 22 | 18 | 23 | 17 | 21 | 19 | 28 | 24 |
| c. | 27 | 23 | 32 | 30 | 26 | 20 | 33 | **29** | 28 | 24 | 31 | 25 | 29 | 27 | 34 | 30 |
| d. | 31 | 29 | 36 | 32 | 38 | 34 | 41 | **35** | 26 | 20 | 33 | 29 | 35 | 31 | 40 | 38 |
| e. | 9 | 3 | 16 | 12 | 18 | 14 | 23 | **21** | 20 | 18 | 25 | 21 | 27 | 23 | 30 | 24 |
| f. | 25 | 21 | 28 | 22 | 26 | 24 | 31 | **27** | 30 | 26 | 35 | 33 | 29 | 23 | 36 | 32 |

Используя результаты из табл. 1, рассмотрим отображения из теорем 1 и 2. Для вычисления $\mathbf{a}(S^6_{\lambda_i})^{\mathrm{T}} \oplus \mathbf{a}(P_1)^{\mathrm{T}} = \mathbf{b}$ необходимо $4 \cdot 8 = 32$ операции XOR. Аналогично, для вычисления $\mathbf{a}(S^9_{\tau_i})^{\mathrm{T}} \oplus \mathbf{a}(P_2)^{\mathrm{T}} = \mathbf{b}$ необходимо $6 \cdot 8 = 48$ операций XOR. Тогда с помощью равенств (2) получим, что для пары

$$(f,P)=\begin{cases}(\lambda_i,P_1), & k=4,\\ (\tau_i,P_2), & k=6\end{cases}$$

справедливо равенство $\mathsf{XOR}(\mathcal{L}^k_{f,P})=\dfrac{3k}{2}\mathsf{XOR}(S_f)+8k$.

Пусть $h_1(x)=x^4+\beta^2x^3+x^2+\beta x+1$, $h_2(x)=x^4+(\beta+1)x^3+x^2+\beta x+1$, $h_3(x)=x^4+\beta^2x^3+x^2+x+\beta\in\mathrm{GF}(2^n)[x]$. В [5] показано, что при некоторых $\beta\in\mathrm{GF}(2^n)$ матрица $S^4_{h_i}$ является MDS-матрицей для любого $i=1,2,3$.

В работе [2] авторы использовали многочлены $g_1(x)=x^6+2x^5+8x^4+5x^3+8x^2+2x+1$ и $g_2(x)=x^6+4x^5+x^4+2x^3+x^2+3x+2$ для построения MDS-матриц размеров $6\times6$, используемых в семействе хэш-функции PHOTON, ориентированных на низкоресурсную реализацию. Они получили, что над полем $\mathrm{GF}(2^8)=\mathrm{GF}(2)[x]/x^8+x^4+x^3+x+1$ матрица $S^6_{g_i}$ является MDS-матрицей, $i=1,2$. Заметим, что среди многочленов вида

$$g'_1(x)=x^6+\beta x^5+\beta^3x^4+(\beta^2\oplus1)x^3+\beta^3x^2+\beta x+1,$$
$$g'_2(x)=x^6+\beta^2x^5+x^4+\beta x^3+x^2+(\beta\oplus1)x+\beta$$

для некоторого $\beta\in\mathrm{GF}(2^8)$ найдутся многочлены $g_1(x)$ и $g_2(x)$ соответственно.

С помощью значений из табл. 1 и равенств (1) и (2) при $\alpha=\beta=$ 0x02 получены результаты, приведённые в табл. 2 и 3. Из таблиц следует, что метод построения MDS-отображений на множествах $Q^k$ при $k=4$ и 6, предложенный в данной работе, позволяет осуществить менее затратную реализацию, чем с использованием отображений из работ [2, 5].

Таблица 2

**Сравнение параметра XOR-сложность для MDS-отображений множества $Q^4$**

| MDS-отображения | $S^4_{h_1}$ | $S^4_{h_2}$ | $S^4_{h_3}$ | $\mathcal{L}^4_{\lambda_1,P_1}$ | $\mathcal{L}^4_{\lambda_2,P_1}$ | $\mathcal{L}^4_{\lambda_3,P_1}$ | $\mathcal{L}^4_{\lambda_4,P_1}$ |
|---|---|---|---|---|---|---|---|
| XOR-сложность | 128 | 144 | 128 | 98 | 110 | 116 | 122 |

Таблица 3

**Сравнение параметра XOR-сложность для MDS-отображений множества $Q^6$**

| MDS-отображения | $S^6_{g'_1}$ | $S^6_{g'_2}$ | $\mathcal{L}^6_{\tau_1,P_2}$ | $\mathcal{L}^6_{\tau_2,P_2}$ | $\mathcal{L}^6_{\tau_3,P_2}$ | $\mathcal{L}^6_{\tau_4,P_2}$ |
|---|---|---|---|---|---|---|
| XOR-сложность | 366 | 342 | 246 | 246 | 282 | 282 |

## Заключение

В работе предложен новый метод построения MDS-матрицы. Полученные MDS-матрицы обладают хорошими эксплуатационными характеристиками с точки зрения реализации на вычислительных платформах с ограниченными ресурсами.

## ЛИТЕРАТУРА

1. *Augot D. and Finiasz M.* Direct construction of recursive MDS diffusion layers using shortened BCH codes // LNCS. 2014. V. 8540. P. 3–17.
2. *Guo J., Peyrin T., and Poschmann A.* The PHOTON family of lightweight hash functions // LNCS. 2011. V. 6841. P. 222–239.

3. *Sarkar S. and Sim S. M.* A deeper understanding of the XOR count distribution in the context of lightweight cryptography // LNCS. 2016. V. 9646. P. 167–182.
4. *Toh D., Teo J., Khoo K., and Sim S. M.* Lightweight MDS serial-type matrices with minimal fixed XOR count // LNCS. 2018. V. 10831. P. 51–71.
5. *Gupta K. C. and Ray I. G.* On constructions of MDS matrices from companion matrices for lightweight cryptography // LNCS. 2013. V. 8128. P. 29–43.

УДК 519.688 DOI 10.17223/2226308X/12/60

# ВЫЧИСЛИТЕЛЬНЫЕ ЭКСПЕРИМЕНТЫ В КОНЕЧНЫХ ДВУПОРОЖДЁННЫХ БЕРНСАЙДОВЫХ ГРУППАХ ПЕРИОДА 5

А. А. Кузнецов

Пусть $B_0(2,5) = \langle a_1, a_2 \rangle$ — наибольшая конечная двупорождённая бернсайдова группа периода 5, порядок которой равен $5^{34}$. Для каждого элемента данной группы существует единственное представление вида $a_1^{\alpha_1} \cdot a_2^{\alpha_2} \cdot \ldots \cdot a_{34}^{\alpha_{34}}$, где $\alpha_i \in \mathbb{Z}_5$, $i = 1, 2, \ldots, 34$. Здесь $a_1$ и $a_2$ — порождающие элементы $B_0(2,5)$, $a_3, \ldots, a_{34}$ — коммутаторы, которые вычисляются рекурсивно через $a_1$ и $a_2$. Определим факторгруппу группы $B_0(2,5)$ следующего вида: $B_k = B_0(2,5)/\langle a_{k+1}, \ldots, a_{34} \rangle$. Очевидно, что $|B_k| = 5^k$. На основе проведённых вычислительных экспериментов сформулирована гипотеза о диаметре группы $B_k$ для симметричного порождающего множества $\{a_1, a_1^{-1}, a_2, a_2^{-1}\}$.

**Ключевые слова:** *функция роста группы, группа Бернсайда.*

Настоящая работа продолжает исследования, начатые в [1, 2], которые посвящены разработке алгоритмов для исследования роста в конечных двупорождённых группах периода 5. В [1] основной упор сделан на создании алгоритмов минимальной вычислительной сложности, а в [2] разработан ресурсно-эффективный алгоритм, который имеет низкую пространственную сложность и сохраняет вычислительную сложность на приемлемом уровне.

Напомним основные определения [1]. Пусть $G = \langle X \rangle$. *Шаром* $K_s$ радиуса $s$ группы $G$ будем называть множество всех её элементов, которые могут быть представлены в алфавите $X$ в виде несократимых групповых слов длины не больше $s$. Все элементы одинаковой длины $i$ образуют *сферу* $P_i$ радиуса $i$. Единица группы $e$ является пустым словом, длина которого равна нулю. Согласно данным определениям, $K_s = \bigcup\limits_{i=0}^{s} P_i$.

Для каждого целого неотрицательного $i$ можно определить (сферическую) функцию роста группы $F(G)$, которую будем записывать в виде вектора $F(G) = (F_0, F_1, \ldots, F_i, \ldots)$, где $F_i = |P_i|$. Пусть $F_{s_0} > 0$, но $F_{s_0+1} = 0$, тогда $s_0$ является диаметром графа Кэли группы $G$ в алфавите порождающих $X$, который будем обозначать $D_X(G)$. Средний диаметр $\overline{D}_X(G)$ равен $\dfrac{1}{|G|} \sum\limits_{s=0}^{s_0} sF_s$.

Заметим, что решение некоторых задач теории кодирования и криптографии сводится к исследованию соответствующих графов Кэли. Например, открытая проблема эффективного восстановления вершин в графе Хэмминга является одной из таких задач [3].

Кратко опишем алгоритмы из [1, 2].

Алгоритм 1 вычисляет шар $K_s$ фиксированного радиуса $s$ произвольной конечной группы $G$, заданной порождающим множеством $X$. Данный алгоритм имеет низкую

вычислительную сложность, однако при его реализации каждый элемент группы необходимо хранить в памяти компьютера, и если группа имеет большой порядок, то применение алгоритма 1 становится невозможным.

Пусть $\varphi$ — гомоморфизм $G$ на группу $Q$ и $N$ — ядро $\varphi$, т. е. $Q = G/N$. По аналогии с группой, для каждого смежного класса $qN$ определим сферу $P_i(q)$, шар $K_s(q)$ и функцию роста $F_i(q)$:

$$P_i(q) = \{g : g \in P_i \text{ и } \varphi(g) = q\}, \quad K_s(q) = \bigcup_{i=0}^{s} P_i(q), \quad F_i(q) = |P_i(q)|.$$

Пусть $F_d(q) > 0$, но $F_{d+1}(q) = 0$, тогда $d$ будем называть диаметром смежного класса $qN$ и обозначать $D_X(qN)$.

Если $Q$ — сравнительно большая группа, то множество $K_{2s}(q)$ будет значительно меньше, чем $K_{2s}(G)$. Данный факт взят за основу построения алгоритма 2, который, получив на входе шар $K_s$ группы $G$ радиуса $s$, фактор-группу $Q = G/N$ и некоторый элемент $q \in Q$, возвращает функцию роста $F(q) = (F_0(q), \ldots, F_{2s}(q))$ для шара $K_{2s}(q)$ смежного класса $qN$ радиуса $2s$.

Объединив алгоритмы 1 и 2, получим алгоритм 3, который вычисляет функцию роста $F(G) = \sum\limits_{q \in Q} F(q)$ шара $K_{2s}$ фиксированного радиуса $2s$ произвольной конечной группы $G$, заданной порождающим множеством $X$.

Пусть $B_0(2,5) = \langle a_1, a_2 \rangle$ — максимальная конечная двупорождённая бернсайдова группа периода 5, порядок которой равен $5^{34}$ [4]. При помощи системы компьютерной алгебры GAP легко получить коммутаторное представление данной группы [5]. В этом случае каждый элемент $g \in B_0(2,5)$ может быть однозначно записан в виде $a_1^{\alpha_1} \cdot a_2^{\alpha_2} \cdot \cdot \ldots \cdot a_{34}^{\alpha_{34}}$, где $\alpha_i \in \mathbb{Z}_5$ и $i = 1, 2, \ldots, 34$. Здесь $a_1$ и $a_2$ — порождающие элементы $B_0(2,5)$; $a_3, \ldots, a_{34}$ — коммутаторы, которые вычисляются рекурсивно через $a_1$ и $a_2$ [4].

Определим фактор-группу $B_k = B_0(2,5)/\langle a_{k+1}, \ldots, a_{34} \rangle$. Очевидно, что $|B_k| = 5^k$ и $g = a_1^{\alpha_1} \cdot a_2^{\alpha_2} \cdot \ldots \cdot a_k^{\alpha_k}$ для всех $g \in B_k$.

Пусть $A_4 = \{a_1, a_1^{-1}, a_2, a_2^{-1}\}$ — симметричное порождающее множество групп $B_k$.

Отметим, что на сегодняшний день при помощи компьютерных вычислений удалось получить функции роста групп $B_k$ при $k \leqslant 19$ [1, 2]. В настоящее время ведутся расчёты функции роста группы $B_{20} = \langle A_4 \rangle$ по алгоритму 3, при этом $s = 20$, $Q = B_{10}$ и $N = \langle a_{11}, \ldots, a_{20} \rangle$.

При суммировании получаемых функций роста $F(q)$ смежных классов $qN$ отмечено, что, начиная с некоторого шага (не более 10 % от порядка группы), промежуточные функции роста группы $F(B_{20})$ сохраняют области возрастания и убывания. Рис. 1 наглядно отражает данный факт. Вычислительные эксперименты в группах $B_k$ при $k \leqslant 19$ показали, что и в них промежуточные функции роста ведут себя аналогично. Кроме того, выяснилось, что при $k \leqslant 19$ смежный класс $eN_k$ всегда включает слова максимальной длины группы, на основании чего можно сформулировать гипотезу для всех $2 \leqslant k \leqslant 34$:

**Гипотеза 1.** $D_{A_4}(eN_k) = D_{A_4}(B_k)$, где $|N_k| \sim |Q_k| \sim |B_k|^{1/2}$.

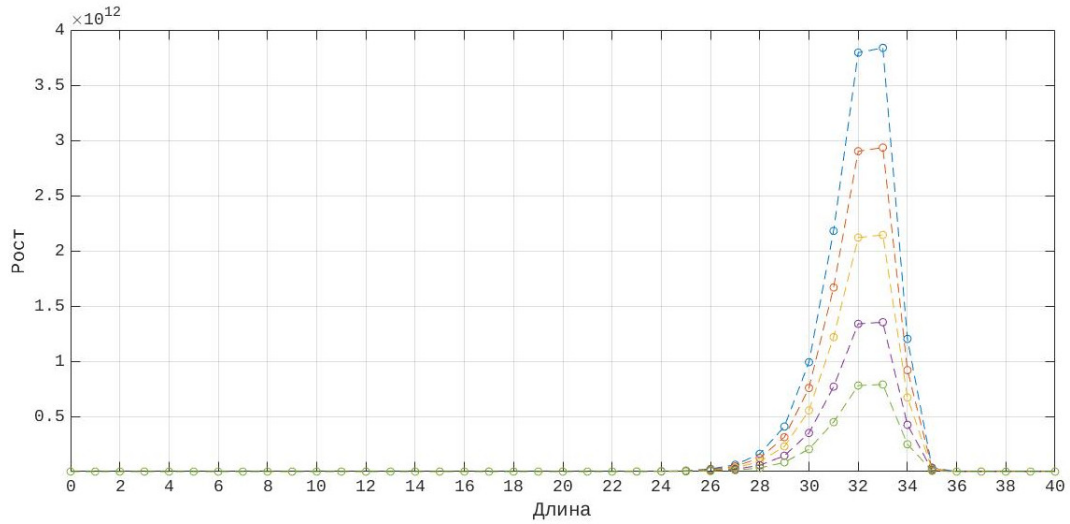


Рис. 1. Промежуточные функции роста $F(B_{20})$

Результаты вычислительных экспериментов в группах $B_k$ при $20 \leqslant k \leqslant 25$ представлены в таблице.

| $k$ | 20 | 21 | 22 | 23 | 24 | 25 |
|---|---|---|---|---|---|---|
| $D_{A_4}(eN_k)$ | 38 | 39 | 41 | 44 | 44 | 46 |

Если гипотеза верна, то значения диаметров смежных классов $eN_k$ в таблице равны диаметрам соответствующих групп $B_k$ относительно порождающего множества $A_4$.

## ЛИТЕРАТУРА

1. *Кузнецов А. А.* Об одном алгоритме вычисления функций роста в конечных двупорождённых группах периода 5 // Прикладная дискретная математика. 2016. № 3(33). С. 116–125.
2. *Кузнецов А. А., Кузнецова А. С.* Ресурсно-эффективный алгоритм для исследования роста в конечных двупорождённых группах периода 5 // Прикладная дискретная математика. 2018. № 42. С. 94–103.
3. *Константинова Е. В.* Комбинаторные задачи на графах Кэли. Новосибирск: НГУ, 2010. 110 с.
4. *Havas G., Wall G., and Wamsley J.* The two generator restricted Burnside group of exponent five // Bull. Austral. Math. Soc. 1974. No. 10. P. 459–470.
5. *Sims C.* Computation with Finitely Presented Groups. Cambridge: Cambridge University Press, 1994. 628 p.

УДК 512.55 DOI 10.17223/2226308X/12/61

# СРАВНИТЕЛЬНЫЙ АНАЛИЗ ЭФФЕКТИВНОСТИ РЕШЕНИЯ ПСЕВДОБУЛЕВЫХ СИСТЕМ ЛИНЕЙНЫХ НЕРАВЕНСТВ АЛГОРИТМАМИ ИМИТАЦИИ ОТЖИГА, БАЛАША И ВНУТРЕННЕЙ ТОЧКИ

Г. О. Маняев, А. Н. Шурупов

Целью работы является разработка и исследование надёжности релаксационного алгоритма решения псевдобулевых систем линейных неравенств, построенного

на основе алгоритма внутренней точки. Экспериментальный анализ показал высокую (86 %) среднюю надёжность алгоритма, превосходящую аналогичные результаты некоторых эвристических алгоритмов локального поиска при решении случайно выбираемых псевдобулевых систем линейных неравенств. Выявлены классы систем неравенств, на которых сравниваемые эвристические алгоритмы существенно различаются в эффективности решения.

**Ключевые слова:** *псевдобулевы линейные неравенства, алгоритм внутренней точки, релаксация, линейное программирование.*

## Введение

Одной из важных прикладных задач является решение псевдобулевых систем линейных неравенств (СЛН). Методы сведения булевых систем нелинейных уравнений (СНУ) к псевдобулевым СЛН предложены в [1, 2]. Общий метод решения СЛН для неотрицательных значений действительных переменных приведён в [3], однако его трудоёмкость не является полиномиальной в общем случае, верхняя оценка является экспоненциальной и эксперименты показывают быстрый рост числа экстремальных лучей при увеличении числа неравенств. Необходимость решения СЛН обусловила привлечение эвристических методов для решения СЛН. В частности, разработаны полиномиальные алгоритмы решения действительных СЛН, такие, как алгоритм Хачияна (эллипсоидов) [4], алгоритм Кармаркара (внутренней точки) [5]. Алгоритм Хачияна можно применить для решения псевдобулевых СЛН с использованием релаксационного подхода [6].

В работе исследуется возможность применения алгоритма Кармаркара для решения псевдобулевых СЛН. Нетривиальность указанной задачи обусловлена, во-первых, тем, что алгоритм Кармаркара в оригинальной публикации разработан для решения задач линейного программирования (ЛП), и, во-вторых, особенностями использования линейной целевой функции в вычислениях алгоритма Кармаркара. Напомним, что лобовое (стандартное) сведение решения СЛН к задаче ЛП требует минимизации кусочно-линейной целевой функции с линейными ограничениями.

## 1. Псевдобулевые системы линейных неравенств

**Определение 1.** Под *псевдобулевой системой линейных неравенств* (ПСЛН) понимается система вида

$$Ax \geqslant b, \tag{1}$$

где $A \in \mathbb{Z}_{m,n}$ — целочисленная матрица размера $m \times n$ с элементами $a_{ij}$, $i = 1, \ldots, m$, $j = 1, \ldots, n$, и $b \in \mathbb{Z}^m$ — целочисленный вектор. Искомые булевы переменные составляют вектор $x \in V_2^n$.

Рассмотрим функцию $\mathrm{tob}(x') : [0,1]^n \to V_2^n$, которая отображает действительный вектор $x' \in [0,1]^n$ в булев $x \in V_2^n$ покоординатно, т. е. $x_i = [[x'_i]]$, где $[[a]]$ — ближайшее к $a$ по модулю целое число. Значение $[[1/2]]$ определяется произвольным фиксированным образом.

**Определение 2.** Под *релаксацией* ПСЛН будем понимать ослабление требования булевости переменных до произвольных действительных значений.

Заметим, что такой приём является эвристическим и позволяет использовать для решения задачи алгоритмы, ориентированные на непрерывные переменные. Надёжность решения с использованием релаксации меньше единицы в силу ошибок округления при возврате в булеву область. Как правило, исследование надёжности алго-

ритмов, построенных на основе релаксации исходной задачи и последующего применения непрерывных алгоритмов, например алгоритмов решения непрерывных задач линейного программирования, представляет собой самостоятельную проблему. Экспериментальный анализ надёжности алгоритма решения ПСЛН с помощью алгоритма Кармаркара изложен далее в п.5.

## 2. Сведение задачи решения ПСЛН к стандартной задаче ЛП

**Определение 3.** Пусть задана некая линейная функция $J(x) = \sum\limits_{i=1}^{n} c_i x_i$ на множестве $U = \{x \in \mathbb{R}^n : Ax \geqslant b\}$. Задача ЛП заключается в нахождении минимума функции $J(x)$ на множестве $U$, элементы которого называются допустимыми точками, решениями и т. п. Задачу ЛП можно записать следующим образом:

$$J(x) \xrightarrow{U} \inf : U = \{x \in \mathbb{R}^n : Ax \geqslant b\}.$$

**Определение 4.** Стандартной задачей ЛП (СЗЛП) называется задача ЛП вида

$$\begin{aligned} & c^{\mathrm{T}} x \to \min, \\ & \begin{cases} Ax \geqslant b, \\ x \geqslant 0, \end{cases} \end{aligned} \tag{2}$$

где $x = (x_1, \ldots, x_n)^{\mathrm{T}} \in \mathbb{R}^n$; $c \in \mathbb{Z}^n$; $A \in \mathbb{Z}_{m,n}$.

Здесь и далее под векторами понимаются вектор-столбцы. Чтобы свести задачу решения ПСЛН к СЗЛП, используем следующие понятия.

**Определение 5.** *Невязкой линейного неравенства* $Ux \geqslant v$, где $U \in \mathbb{Z}^n$ и $v \in \mathbb{Z}$, называется неотрицательная кусочно-линейная функция

$$F_{U,v}(x) = \begin{cases} 0, & \text{если неравенство выполнено,} \\ v - Ux & \text{в противном случае.} \end{cases}$$

**Определение 6.** *Невязкой системы линейных неравенств* вида (1) называется функция $F_{A,b}(x) = \sum\limits_{i=1}^{m} F_{A_i,b_i}(x)$.

**Замечание 1.** Как и невязка линейного неравенства, невязка ПСЛН, вообще говоря, не является линейной функцией. Однако в алгоритме Кармаркара по существу используется линейная целевая функция (ц.ф.).

Введём в рассмотрение функцию $g(A) : \mathbb{R}_{m,n} \to \mathbb{R}^n$, заданную следующим образом: $g(A) = y = (y_1, \ldots, y_n)$, где $y_i = \sum\limits_{t=1}^{m} a_{ti}$.

Традиционно, например в алгоритме Балаша, невязка СЛН для решения задачи ЛП используется в качестве её ц.ф. В алгоритме Кармаркара линейная ц.ф. по существу используется для вычисления очередного состояния алгоритма, поэтому применение невязок из алгоритмов Балаша и Хачияна (невязка в алгоритме Хачияна получается заменой суммирования на взятие максимума в определении 6) не представляется возможным. Поэтому в настоящей работе в качестве ц.ф. алгоритма Кармаркара используется линейная функция $g(A)^{\mathrm{T}} x$. В качестве возможных вариантов ц.ф. в дальнейших исследованиях могут быть рассмотрены функции взятия среднего значения или взвешенная сумма. Алгоритм А1 описывает преобразование задачи решения ПСЛН к СЗЛП.

**Алгоритм 1.** A1

**Вход:** $A \in \mathbb{Z}_{m,n}$, $b \in \mathbb{Z}^m$.

Инициализация переменных $A' \in \mathbb{Z}_{m+n,n}$, $b' \in \mathbb{Z}^{m+n}$, $c \in \mathbb{Z}^n$

1: $A' := 0$, $b' := -1$, $c := 0$ // покоординатная инициализация константами

2: $A' \begin{pmatrix} 1 \dots m \\ 1 \dots n \end{pmatrix} := A$ // добавление к матрице $A'$ неравенств исходной системы. В левой части использовано обозначение для подматрицы матрицы $A'$, образованной элементами на пересечении строк с номерами $1 \dots m$ и столбцов с номерами $1 \dots n$

3: $b'(1 \dots m) := b$.

Релаксация исходной задачи // Заключается в ослаблении требований булевости к переменным ПСЛН, т. е. $0 \leqslant x_i \leqslant 1$. Ограничение $x \geqslant 0$ является требованием алгоритма Кармаркара. Для учёта ограничения $x \leqslant 1$ дополним систему $n$ неравенствами вида $x_i \leqslant 1$, $i = 1, 2, \dots, n$, или, что то же самое, неравенствами $-x \geqslant -1$.

4: $A'(i, i-m) := -1$, $i = m+1, \dots, m+n$.

Вычисление коэффициентов линейной целевой функции

5: **Для** $j = 1, \dots, n$

6: **Для** $i = 1, \dots m+n$

7: $c_j := c_j + A'_{ij}$.

**Выход:** $A'$, $b'$, $c$.

## 3. Сведение стандартной задачи линейного программирования к форме Кармаркара

**Определение 7.** *Формой Кармаркара* задачи ЛП будем называть задачу ЛП, если она имеет вид

$$c^{\mathrm{T}}x \to \min,$$
$$\begin{cases} Ax = 0, \\ \sum\limits_i x_i = 1, \\ x \geqslant 0, \end{cases}$$

где $x = (x_1, \dots, x_n) \in \mathbb{R}^n$, $c \in \mathbb{Z}^n$, $A \in \mathbb{Z}_{m,n}$.

Сформулируем план действий по преобразованию СЗЛП к ЗЛП в форме Кармаркара, следуя [5]:

1) Рассмотрим двойственную к СЗЛП (2) задачу

$$b^T u \to \max,$$
$$\begin{cases} A^{\mathrm{T}}u \leqslant c, \\ u \geqslant 0. \end{cases}$$

2) Комбинируем прямую и двойственную задачи:

$$\begin{cases} Ax \geqslant b, \\ A^{\mathrm{T}}u \leqslant c, \\ c^{\mathrm{T}}x - b^{\mathrm{T}}u = 0, \\ x \geqslant 0,\ u \geqslant 0. \end{cases}$$

Согласно теории двойственности, эта комбинированная задача допустима, если и только если исходная СЗЛП имеет конечный оптимум.

3) Введём вспомогательные переменные для перехода от неравенств к равенствам в системах ограничений:

$$\begin{cases} Ax - y = b, \\ A^{\mathrm{T}}u + v = c, \\ c^{\mathrm{T}}x - b^{\mathrm{T}}u = 0, \\ x \geqslant 0,\ v \geqslant 0, \\ y \geqslant 0,\ u \geqslant 0. \end{cases}$$

4) Введём фиктивную переменную $\lambda$, чтобы получить внутреннюю допустимую начальную точку. Пусть $x_0, y_0, v_0, u_0$ — строго внутренние точки соответствующих неотрицательных ортантов размерностей $n, m, n, m$. Рассмотрим следующую задачу:

$$\lambda \to \min,$$
$$\begin{cases} Ax - y + (b - Ax_0 + y_0)\lambda = b, \\ A^{\mathrm{T}}u + v + (c - A^{\mathrm{T}}u_0 + v_0)\lambda = c, \\ c^{\mathrm{T}}x - b^{\mathrm{T}}u + (-c^{\mathrm{T}}x_0 - b^{\mathrm{T}}u_0)\lambda = 0, \\ x \geqslant 0,\ u \geqslant 0,\ y \geqslant 0,\ v \geqslant 0,\ \lambda \geqslant 0. \end{cases}$$

Заметим, что $x = x_0$, $y = y_0$, $v = v_0$, $u = u_0$, $\lambda = 1$ — строго внутреннее допустимое решение, которое можно выбрать в качестве начальной (стартовой) точки. Минимальное значение $\lambda$ равно 0, если и только если задача в п. 3 допустима.

5) Для удобства дальнейшего описания сделаем замену обозначений и запишем задачу из п. 4 в виде

$${c_2}^{\mathrm{T}} z \to \min \quad \text{при ограничениях} \quad \begin{cases} A_2 z = b_2, \\ z \geqslant 0, \end{cases}$$

где $m_2 = m + n + 1$; $n_2 = 2m + 2n + 1$;

$$A_2 = \begin{bmatrix} (b - Ax_0 + y_0)_{m\times 1} & A_{m\times n} & 0_{m\times m} & -E_{m\times m} & 0 \\ \left(c - A^{\mathrm{T}}u_0 + v_0\right)_{n\times 1} & 0_{n\times n} & A^{\mathrm{T}}_{n\times m} & 0 & E_{n\times n} \\ (-c^{\mathrm{T}}x_0 - b^{\mathrm{T}}u_0) & c^{\mathrm{T}}_{1\times n} & -b^{\mathrm{T}}_{1\times m} & 0 & 0 \end{bmatrix}_{m_2\times n_2};$$

$z^{\mathrm{T}} = (\lambda, x, u, y, v)$ и $c_2^{\mathrm{T}} = (1, 0, 0, 0, 0)$ — векторы размера $n_2$; $b_2^{\mathrm{T}} = (b, c_0)$ имеет размер $m_2$.

6) Опишем отображение неотрицательного ортанта в симплекс.

Пусть $P_+ = \{z \in \mathbb{R}^{n_2} : z \geqslant 0\}$ — неотрицательный ортант, $\Delta = \left\{z' \in \mathbb{R}^{n_2+1} : z' \geqslant 0, \sum\limits_{i=1}^{n_2+1} {z'}_i = 1\right\}$. Обозначим через $a = (1, x_0, y_0, v_0, u_0)$ некоторую строго внутреннюю точку $P_+$. Зададим $T : P_+ \to \Delta$ следующим образом: пусть $z' = T(z)$, тогда $z' = ({z'}_1, \ldots, {z'}_{n_2+1})$ и

$${z'}_i = \frac{z_i/a_i}{1 + \sum\limits_j (z_j/a_j)},\ i = 1, \ldots, n_2, \quad {z'}_{n_2+1} = 1 - \sum_{i=1}^{n_2} {z'}_i.$$

Заметим, что отображение $T$ обладает следующими свойствами:

1) $T$ биективно. Обратное отображение $T^{-1}$ $(z')$ задаётся следующим образом: $z_i = \dfrac{a_i z'_i}{z'_{n_2+1}}$, $i = 1, \ldots, n_2$.

2) $T$ отображает точку $a$ в центр симплекса $a_0 = \dfrac{1}{n_2+1} I$, где $I$ — вектор из единиц.

Выражая переменные $z_i$ через $z'_i$ в системе из п. 5, получаем

$$\begin{cases} A'_2 z' = 0, \\ \sum\limits_{i=1}^{n_2} z'_i = 1, \\ z' \geqslant 0, \end{cases}$$

где $A'_2 = (A_2 \cdot \operatorname{diag}(a_1, \ldots, a_{n_2}), -b_2)$.

Завершает приведение СЗЛП к форме Кармаркара преобразование целевой функции $c_2^{\mathrm{T}} z$ в $c_2'^{\mathrm{T}} z'$, где $(c'_2)_i = (c_2)_i a_i$ для $i = 1, \ldots, n_2$ и $(c'_2)_{n_2+1} = 0$.

**Замечание 2.** Если применение алгоритма внутренней точки к этой задаче даст решение с нулевым значением $c_2'^{\mathrm{T}} z'$, то обратное отображение $T^{-1}$ даст оптимальное решение исходной задачи. В случае получения решения с положительным значением целевой функции исходная задача не имеет конечного оптимума, т. е. либо она недопустима, либо не ограничена.

## 4. Алгоритм внутренней точки для решения ПСЛН

Алгоритм внутренней точки опубликован в 1984 г. [5]. Он имеет полиномиальную сложность. Этот алгоритм в идейном плане близок к алгоритму эллипсоидов и применяется к задачам линейного программирования, приведённым к некоторой специальной форме. Кармаркар предложил свой алгоритм в качестве замены алгоритма эллипсоидов, поскольку последний имеет проигрыш по времени работы по отношению к алгоритму внутренней точки порядка $\mathrm{O}(n^{2,5})$. Алгоритм 2 вырабатывает последовательность точек $x^{(0)}, x^{(1)}, \ldots x^{(i)}, \ldots$ пространства поиска.

**Алгоритм 2.** Алгоритм внутренней точки для решения ПСЛН

**Вход:** ПСЛН с $m$ неравенствами и $n$ переменными.
**Выход:** решение ПСЛН или символ $\perp$.

1: С помощью алгоритма А1 преобразовать задачу решения ПСЛН в СЗЛП.
2: С помощью процедуры п. 3 преобразовать СЗЛП в форму Кармаркара.
3: Задать стартовую точку $x^{(0)} := a_0$ (центр симплекса в пространстве размерности $2(m + 2n + 1)$), $i := 0$.
4: Вычислить очередную точку последовательности: $i := i + 1$, $x^{(i)} := \varphi(x^{(i-1)})$.
*// Функция $\varphi$ полностью соответствует оригинальному описанию [5] и здесь не приводится. Это же замечание справедливо для следующих двух шагов.*
5: Проверить допустимость полученного результата. Если не выполняется условие допустимости $x^{(i)}$, то завершить алгоритм и вернуть $\perp$.
6: Проверить оптимальность. Если не выполняется условие оптимальности для $x^{(i)}$, то перейти на шаг 4.
7: Преобразовать полученное решение в решение ПСЛН.

Пусть $z \in \mathbb{R}^{n_2+1}$ — решение задачи ЛП в форме Кармаркара, полученное в результате работы алгоритма Кармаркара, а $z' = z(2, \ldots, n+1)$ — подвектор этого решения

размерности $n$, где $n$ — число неизвестных исходной СЗЛП. Тогда решением исходной СЗЛП является вектор $x \in \mathbb{R}^n$, такой, что

$$x_j = \frac{z'_j(a_0)_j}{z_{n_2+1}}, \quad j = 1, \ldots, n.$$

Переход к булевому решению исходной ПСЛН заключается в применении к вектору $x$ функции tob.

## 5. Сравнение надёжностей решения ПСЛН алгоритмами внутренней точки, имитации отжига, Балаша и БИО

Для оценки надёжности описанного выше способа (использующего эвристические приемы) применения алгоритма внутренней точки (АВТ) к решению ПСЛН проведены экспериментальные исследования. План эксперимента в точности совпадает с таковым из работы [7], что позволяет провести сравнительный анализ надёжности АВТ с другими ранее применёнными эвристическими алгоритмами. Для АВТ используются значения параметров $\alpha = 0{,}25$, $q = 5$, все координаты векторов $x_0$, $y_0$, $v_0$, $u_0$ выбраны равными 2. План эксперимента предполагает применение алгоритма к 9600 случайным совместным ПСЛН, которые разбиваются на 12 серий по 800 систем в зависимости от сочетания трёх параметров. Один из этих параметров ограничивает максимальный абсолютный вес коэффициентов, остальные подробно описаны в [7]. В каждой серии системы делятся на 8 подсерий по 100 систем. Подсерия определяется числом переменных (30 или 60) и числом неравенств, которое выражается через число переменных с помощью мультипликативного фактора со значениями 1, 2, 3, 10. Смысл рассмотрения двух выбранных вариантов числа переменных заключается в том, что число переменных 30 позволяет перебрать все булевы векторы этой размерности, следовательно, при увеличении числа шагов эвристического алгоритма доля опробованных векторов может составить заметную долю всего пространства поиска. Для 60 переменных перебрать за приемлемое время на персональном компьютере сколько-нибудь заметную часть пространства поиска не представляется возможным.

В работах [7, 8] произведено сравнение надёжностей эвристических алгоритмов имитации отжига, Балаша и их сочетания, названного в [8] алгоритмом БИО. Последний применялся в двух вариантах — с различными целевыми функциями (невязками) на основе суммирования или взятия максимума. Результаты экспериментов продемонстрировали преимущество алгоритма БИО, хотя по скорости работы он уступает алгоритму Балаша. По этим соображениям, а также с целью придания большей наглядности АВТ сравнивается ниже только с алгоритмом БИО, который вычисляет невязку системы как сумму невязок отдельных неравенств. Результаты этого сравнения по сериям и факторам приведены в табл. 1.

Средняя надёжность АВТ превосходит надежность алгоритма БИО на 2 %, что может считаться статистической погрешностью, и по этому показателю оба алгоритма не имеют явных преимуществ друг перед другом. Однако только в двух сериях (7 и 8) АВТ проигрывает БИО со средним проигрышем 73 %. В остальных 10 сериях АВТ выигрывает у БИО со средним значением выигрыша 16 % (при этом средняя надёжность по 10 сериям равна 99 %). Такое контрастное поведение АВТ не характерно для других рассмотренных в [7, 8] алгоритмов, для которых надёжность ни по одной подсерии не падает ниже 50 %.

АВТ демонстрирует относительную независимость надёжности решения от размера системы, в то время как другие эвристические алгоритмы более чувствительны

Таблица 1

**Сравнение усреднённых значений надёжностей АВТ и БИО по сериям и в зависимости от размера системы**

| Серия | Отношение числа неравенств к числу переменных | | | | | | | | Итого | |
|---|---|---|---|---|---|---|---|---|---|---|
| | 1 | | 2 | | 3 | | 10 | | | |
| | БИО | АВТ | БИО | АВТ | БИО | АВТ | БИО | АВТ | БИО | АВТ |
| 1 | 57 % | 99 % | 96 % | 100 % | 100 % | 100 % | 100 % | 100 % | 88 % | 100 % |
| 2 | 48 % | 99 % | 78 % | 100 % | 92 % | 100 % | 96 % | 100 % | 78 % | 100 % |
| 3 | 33 % | 100 % | 93 % | 100 % | 100 % | 100 % | 100 % | 100 % | 82 % | 100 % |
| 4 | 36 % | 100 % | 91 % | 100 % | 100 % | 100 % | 100 % | 100% | 82 % | 100 % |
| 5 | 33 % | 100 % | 94 % | 100 % | 100 % | 100 % | 100 % | 100 % | 82 % | 100 % |
| 6 | 26 % | 100 % | 91 % | 100 % | 100 % | 100 % | 100 % | 100 % | 79 % | 100 % |
| 7 | 100 % | 17 % | 100 % | 7 % | 99 % | 6 % | 100 % | 80 % | 100 % | 28 % |
| 8 | 100 % | 4 % | 99 % | 1 % | 97 % | 1 % | 100 % | 96 % | 99 % | 26 % |
| 9 | 41 % | 71 % | 95 % | 100 % | 100 % | 100 % | 100 % | 100 % | 84 % | 93 % |
| 10 | 42 % | 75 % | 94 % | 100 % | 100 % | 100 % | 100 % | 100 % | 84 % | 94 % |
| 11 | 34 % | 99 % | 91 % | 99 % | 99 % | 100 % | 100 % | 100 % | 81 % | 100 % |
| 12 | 34 % | 99 % | 93 % | 100 % | 100 % | 100 % | 100 % | 100 % | 82 % | 100 % |
| Итого | 49 % | 80 % | 93 % | 84 % | 99 % | 84 % | 100 % | 98 % | 85 % | 86 % |

к этому показателю, хотя для переопределённых систем (с фактором 10) все алгоритмы успешно справляются почти со всеми системами.

По результатам работы [7] можно убедиться, что разные эвристические алгоритмы по-разному добиваются успеха. Так, таблица корреляции успехов из [7] показывает, что 22 % всех систем не решили оба алгоритма (имитации отжига и Балаша), однако алгоритм отжига решил 15 % от общего числа систем, которые не решил алгоритм Балаша. Аналогично, алгоритм Балаш решил 2 % систем, с которыми не справился алгоритм имитации отжига. Экспериментальный анализ АВТ позволил выявить две труднорешаемые им серии систем.

В табл. 2 приводятся сведения о суммарном покрытии в смысле решения систем линейных неравенств обоими алгоритмами (БИО и АВТ). Для наглядности приведены результаты как для варианта алгоритма БИО со взятием максимума (БИО MAX), так и для варианта с суммированием при вычислении невязки (БИО SUM). Легко видеть, что в каждой серии есть задачи, которые представляют трудности для каждого алгоритма. Так, в первой и второй сериях ни одним алгоритмом не решены одни и те же четыре системы. В то же время суммарное покрытие для АВТ и БИО SUM составило 98,9 %. Серии 7 и 8 оказались трудны для АВТ, БИО MAX справился с ними более чем в 2 раза эффективнее, а БИО SUM решил практически все системы из этих серий (доля нерешённых 0,7 %). С другой стороны, по сериям 3–6 АВТ решил все 609 систем, с которыми не справился алгоритм БИО SUM, и показал на этих сериях надёжность 100 %.

Таблица 2

**Суммарное покрытие СЛН алгоритмом БИО и АВТ**

| Серия | Количество нерешённых задач | | | | | |
|---|---|---|---|---|---|---|
| | АВТ | | АВТ и БИО MAX | | АВТ и БИО SUM | |
| | % | шт. | % | шт. | % | шт. |
| 1 | 0,4 | 3 | 0,4 | 3 | 0,4 | 3 |
| 2 | 0,1 | 1 | 0,1 | 1 | 0,1 | 1 |
| 3, 4, 5, 6 | | 0 | | 0 | | 0 |
| 7 | 72,6 | 581 | 25,0 | 200 | 0,4 | 3 |
| 8 | 74,6 | 597 | 23,8 | 190 | 1,0 | 8 |
| 9 | 7,4 | 59 | 5,0 | 40 | 6,0 | 48 |
| 10 | 6,4 | 51 | 4,8 | 38 | 5,8 | 46 |
| 11 | 0,2 | 2 | | 0 | 0,1 | 1 |
| 12 | 1,1 | 9 | 0,1 | 1 | | 0 |
| Итого | 13,6 | 1303 | 4,9 | 473 | 1,1 | 110 |

## Заключение

Проведённое исследование показало, что алгоритм внутренней точки может быть применен к задаче решения псевдобулевых систем линейных неравенств в модифицированном виде, так как оригинальный алгоритм не рассчитан на решение дискретных задач. Модификация характеризуется высокой средней надёжностью решения ПСЛН — 86 %. Аналогичные показатели имеет и другой эвристический алгоритм БИО с невязкой на основе суммирования, сочетающий в своем поведении алгоритмы Балаша и имитации отжига. Детальный анализ выявляет, что как для модификации алгоритма внутренней точки, так и для алгоритма БИО находятся псевдобулевы системы линейных неравенств, которые один алгоритм решает, а другой нет. В целом, оба алгоритма не справились только с 1,1 % систем, поэтому в качестве практической рекомендации при решении ПСЛН можно предложить последовательное использование алгоритмов внутренней точки и БИО. Отметим, что алгоритм внутренней точки требует проведения большого числа матричных вычислений, при этом размерности матриц в соответствии с выбранным способом сведения исходной задачи решения ПСЛН к форме Кармаркара задачи линейного программирования включают в себя сумму числа неравенств и числа переменных. Указанное обстоятельство может приводить к значительным затратам (или даже нехватке) вычислительных ресурсов при больших значениях указанных параметров СЛН, решаемых с помощью алгоритма внутренней точки.

## ЛИТЕРАТУРА

1. *Балакин Г. В., Никонов В. Г.* Методы сведения булевых уравнений к системам пороговых соотношений // Обозрение прикл. промышл. матем. Сер. дискрет. матем. 1994. Т. 1. № 3. С. 389–401.
2. *Никонов В. Г.* Пороговые представления булевых функций // Обозрение прикл. промышл. матем. Сер. дискрет. матем. 1994. Т. 1. № 3. С. 402–457.
3. *Черникова Н. В.* Алгоритм для нахождения общей формулы неотрицательных решений системы линейных неравенств // Журн. вычисл. матем. и матем. физики. 1965. Т. 5. № 2. С. 334–337.
4. *Хачиян Л. Г.* Избранные труды. М.: МЦНМО, 2009.
5. *Karmarkar N.* A new polynomial-time algorithm for linear programming // Combinatorica. 1984. No. 4. P. 373–395.

6. *Бурделев А. В., Никонов В. Г., Лапиков И. И.* Распознавание параметров узла защиты информации, реализованного пороговой $k$-значной функцией // Труды СПИИРАН. 2016. № 46. С. 108–127.
7. *Анашкина Н. В., Шурупов А. Н.* Экспериментальное сравнение алгоритмов Балаша и имитации отжига в задаче решения систем линейных неравенств // Прикладная дискретная математика. Приложение. 2014. № 7. С. 151–153.
8. *Анашкина Н. В., Шурупов А. Н.* Применение алгоритмов локального поиска к решению систем псевдобулевых линейных неравенств // Прикладная дискретная математика. Приложение. 2015. № 8. С. 136–138.

УДК 519.7 DOI 10.17223/2226308X/12/62

# АЛГОРИТМ «БЕЗОПАСНОЙ» ДЕКОМПОЗИЦИИ ФОРМАЛЬНОГО КОНТЕКСТА

Ч. М. Монгуш

Исследуется #P-полная задача нахождения всех формальных понятий заданного формального контекста. Предлагается алгоритм, который на практике позволяет решать данную задачу за полиномиальное время. Алгоритм основан на методе «безопасной» декомпозиции формального контекста на части, названные боксами. При «безопасной» декомпозиции формального контекста на боксы ни одно формальное понятие исходного контекста не теряется и не возникают новые формальные понятия. Процесс декомпозиции направлен на последовательное уменьшение размеров боксов формального контекста и реализуется итерационно. Установлены правила остановки процесса декомпозиции формального контекста на боксы, гарантирующие полиномиальное время его работы: задание порогового значения на плотность боксов и числа итераций разложения.

**Ключевые слова:** *формальный контекст, формальное понятие, декомпозиция формального контекста, алгоритм декомпозиции.*

## Введение

Объектно-признаковая таблица — модель представления данных некоторой предметной области, в которой каждый столбец соответствует некоторому признаку, а каждая строка определяет признаковое описание отдельного объекта. Такая модель часто используется при решении прикладных задач в интеллектуальном анализе данных, в том числе в анализе формальных понятий.

Анализ формальныйх понятий (АФП) — прикладная ветвь алгебраической теории решёток Г. Биркгофа [1]. Основные идеи АФП были сформулированы в начале 80-х годов XX века в работах Р. Вилле и Б. Гантера и развиты в исследованиях С. О. Кузнецова, С. А. Объедкова, Д. И. Игнатова [2 – 4]. В рамках АФП объектно-признаковая таблица представляется формальным контекстом, отражающим наличие или отсутствие признаков, характерных для изучаемого множества объектов, и моделируется 0,1-матрицей. В АФП формальные понятия определяются с помощью соответствий Галуа и представляют собой пары множеств вида (объём, содержание).

В настоящее время применение методов АФП ограничивается высокой трудоёмкостью процесса нахождения всех формальных понятий заданного формального контекста. В данной работе предлагается алгоритм, который на практике позволяет разложить данную задачу на подзадачи (уменьшенные копии исходной задачи) за полиномиальное время.

## 1. Основные положения анализа формальных понятий

Приведём основные положения и обозначения АФП [2, 3]. Пусть для предметной области определены два непустых конечных множества $G$ и $M$ объектов и признаков (или свойств) и задано непустое отношение инцидентности $I \subseteq G \times M$. Данное отношение содержит информацию о выполнимости свойств из $M$ на объектах из $G$, т. е. $(g, m) \in I$ означает, что объект $g$ обладает признаком $m$, и наоборот — признак $m$ присущ объекту $g$. Тройку $K = (G, M, I)$ принято называть формальным контекстом.

Будем полагать, что множества $G$ и $M$ линейно упорядочены (например, лексикографически). В этом случае формальный контекст $K = (G, M, I)$ однозначно задается 0,1-матрицей $T = (t_{ij})$: $t_{ij} = 0$ при $(g_i, m_j) \notin I$ и $t_{ij} = 1$ при $(g_i, m_j) \in I$ $(i = 1, 2, \ldots, |G|$; $j = 1, 2, \ldots, |M|)$.

Выберем в $K = (G, M, I)$ два произвольных подмножества $A \subseteq G$ и $B \subseteq M$ и определим для них отображения $(\cdot)'$ Галуа: $A' = \bigcap\limits_{g \in A} g'$, $B' = \bigcap\limits_{m \in B} m'$, где $g' = \{m \in M : (g, m) \in I\}$; $m' = \{g \in G : (g, m) \in I\}$. Согласно этому определению, множество $A'$ — набор признаков, присущих объектам из $A$, а множество $B'$ задаёт семейство объектов, обладающих признаками из $B$. Двойное применение $(\cdot)'$ определяет оператор замыкания $(\cdot)''$ на $2^M$ в алгебраическом смысле. Множество $(B)''$ можно трактовать как набор признаков, которые неизменно появляются в объектах формального контекста $K = (G, M, I)$ вместе с признаками из $B$, причём это множество является наибольшим по включению в пределах этого формального контекста. Если $B = B''$, то $B$ называется замкнутым множеством относительно оператора $(\cdot)''$.

Пара множеств $(A, B)$, таких, что $A \subseteq G$, $B \subseteq M$, $A' = B$ и $B' = A$, называется формальным понятием формального контекста $K = (G, M, I)$ с объёмом $A$ и содержанием $B$. Далее для краткости в ряде случаев определение «формальный» перед словами «контекст» или «понятие» будем опускать. Пара множеств $(A, B)$ является формальным понятием тогда и только тогда, когда $A = A''$ и $B = B''$. Очевидно, что всякое формальное понятие уникально в заданном контексте, т. е. отличается от других формальных понятий объёмом и/или содержанием. Если формальный контекст представлен 0,1-матрицей $T$, то при $A \neq \varnothing$ и $B \neq \varnothing$ формальному понятию $(A, B)$ отвечает максимальная полная подматрица матрицы $T$.

Обозначим через $FC$ множество всех формальных понятий формального контекста $K = (G, M, I)$. Пусть $(A_1, B_1), (A_2, B_2) \in FC$. Множество $FC$ частично упорядочено отношением $(A_1, B_1) \sqsubseteq (A_2, B_2) \Leftrightarrow A_1 \subseteq A_2$. Отметим, что последнее эквивалентно условию $B_2 \subseteq B_1$. Каждое формальное понятие $(A, B) \in FC$ определяет для исследуемой предметной области совокупность однородных объектов $A$ со своим специфичным набором признаков $B$. Если $(G, \varnothing) \in FC$, $(\varnothing, M) \in FC$, то формальные понятия $(G, \varnothing)$, $(\varnothing, M)$ называются тривиальными.

Определим на $FC$ операции пересечения $\sqcap$ и объединения $\sqcup$ через одноимённые теоретико-множественные операции $\cap$ и $\cup$ следующим образом:

$$(A_1, B_1) \sqcap (A_2, B_2) = (A_1 \cap A_2, (A_1 \cap A_2)'), \quad (A_1, B_1) \sqcup (A_2, B_2) = ((B_1 \cap B_2)', B_1 \cap B_2).$$

Тогда $(FC, \sqsubseteq)$ образует полную решётку $L = (FC, \sqcap, \sqcup)$, называемую в АФП решёткой формальных понятий контекста $K = (G, M, I)$.

## 2. Постановка задачи и метод «безопасной» декомпозиции

В рамках АФП задача нахождения всех формальных понятий формулируется следующим образом. Задан формальный контекста $K = (G, M, I)$. Требуется для $K$ най-

ти множество $FC$. На сегодняшний день для определения множества $FC$ разработано много алгоритмов, в их числе NextClosure, Close-by-One, Norris [3, 4]. Время их выполнения в худшем случае составляет $O(|FC| \cdot |G|^2 \cdot |M|)$. Поскольку величина $|FC|$ может экспоненциально зависеть от $|G|$ и $|M|$, время выполнения данных алгоритмов также может быть экспоненциальным. Повысить производительность можно путём применения метода «безопасной» декомпозиции формального контекста на боксы [5].

Пусть $g \in G$ и $m \in M$ — произвольные элементы контекста $K = (G, M, I)$. Пары множеств $(g'', g')$ и $(m', m'')$ образуют формальные понятия, первое из которых назовём объектным, а второе — признаковым формальным понятием контекста $K = (G, M, I)$. Обозначим через $O = \{(g'', g') : g \in G\} \subseteq FC$ множество всех объектных формальных понятий и через $S = \{(m', m'') : m \in M\} \subseteq FC$ — множество всех признаковых формальных понятий контекста $K = (G, M, I)$.

Пара формальных понятий $(g'', g') \in O$, $(m', m'') \in S$ определяет бокс $\omega = (m', g', J)$ контекста $K = (G, M, I)$, если $(g'', g') \sqsubseteq (m', m'')$, что эквивалентно $g'' \subseteq m'$ (или $m'' \subseteq g'$). Про такой бокс будем говорить, что он образован элементами $g \in G$ и $m \in M$. Далее вместо $\omega = (m', g', J)$ будем кратко писать $\omega = (m', g')$ или $(m', g')$.

**Утверждение 1** [6]. Для всякого формального контекста $K = (G, M, I)$ и любых $(g'', g') \in O$, $(m', m'') \in S$ отношение порядка $(g'', g') \sqsubseteq (m', m'')$ выполняется тогда и только тогда, когда $(g, m) \in I$.

Утверждение 1 устанавливает оценку числа боксов, получаемых на каждой итерации разложения: число различных боксов, порождаемых всевозможными элементами контекста $K = (G, M, I)$, не превышает веса 0,1-матрицы $T$, т. е. величины $\|T\|$ — числа единичных элементов этой матрицы. Очевидно, что $1 \leqslant \|T\| \leqslant |G| \cdot |M|$.

Будем говорить, что формальное понятие $(A, B) \in FC$ вложено в бокс $(m', g')$ контекста $K = (G, M, I)$, и записывать $(A, B) \preceq (m', g')$, если $A \subseteq m'$, $B \subseteq g'$. Всякий бокс $(m', g')$ не является пустым, поскольку, согласно определению бокса, он всегда содержит формальные понятия $(g'', g') \in O$ и $(m', m'') \in S$.

**Утверждение 2** [6]. Всякое нетривиальное формальное понятие $(A, B)$ контекста $K = (G, M, I)$, которое вложено в бокс $(m', g')$, образованный элементами $g \in G$ и $m \in M$, содержит эти элементы и их замыкания, т. е. если $(A, B) \preceq (m', g')$, то $g \in A$ и $m \in B$; $g'' \subseteq A$ и $m'' \subseteq B$.

Согласно утверждению 2, пару $(g'', m'')$ можно рассматривать в качестве типичного представителя не только бокса $(m', g')$, но и всех формальных понятий контекста $K = (G, M, I)$, вложенных в этот бокс. Переход от боксов к их типичным представителям в большинстве случаев уменьшает на практике время выполнения алгоритмов нахождения всех формальных понятий для заданного формального контекста. Соответствие между боксами и формальными понятиями контекста устанавливает следующая теорема.

**Теорема 1** [6]. Для всякого формального контекста $K = (G, M, I)$, множества $FC$ всех его формальных понятий и любой пары множеств $(A, B)$, $\varnothing \neq A \subseteq G$, $\varnothing \neq B \subseteq M$, справедливо:

1) если $(A, B) \in FC$, то в $K$ существует бокс $\omega = (m', g')$, $g \in G$ и $m \in M$, возможно, не единственный, в который это формальное понятие вложено;
2) если $(A, B)$ — формальное понятие некоторого бокса $\omega = (m', g')$ формального контекста $K$, то оно также принадлежит $FC$.

Согласно теореме 1, разложение контекста $K = (G, M, I)$ на боксы является «безопасным» для любого формального понятия из $FC$ [5]. Очевидно, что процесс разложения заданного контекста на боксы может быть организован итерационно, поскольку каждый выявленный на первой итерации бокс можно рассматривать в качестве исходного контекста и вновь подвергать декомпозиции. Определим сложность процесса разложения и правила его остановки. Пусть $|m'| \cdot |g'|$ — размер бокса $(m', g')$, а $\|(m', g')\|$ — число его единичных элементов. Плотностью бокса $(m', g')$ назовём величину $\sigma(m', g') = \|(m', g')\|/(|m'| \cdot |g'|)$. Верны естественные границы $0 < \sigma(m', g') \leqslant 1$.

**Утверждение 3** [6]. Всякий бокс $(m', g')$ с плотностью $\sigma(m', g') = 1$ содержит ровно одно нетривиальное формальное понятие $(A, B)$ контекста $K = (G, M, I)$, совпадающее с ним, т. е. $A = m'$ и $B = g'$.

Из утверждения 3 следует, что бокс $(m', g')$ с плотностью 1 вырождается в нетривиальное формальное понятие и не подлежит дальнейшему разложению. Заметим, что время формирования одного бокса для формального контекста $K = (G, M, I)$ составляет $\mathrm{O}(|G| \cdot |M|)$. В целом, время, необходимое на однократное разложение этого контекста на боксы, в худшем случае составляет $\mathrm{O}\big(\sigma(G, M)\,|G|^2 \cdot |M|^2\big)$.

## 3. Алгоритм «безопасной» декомпозиции формального контекста на боксы

Алгоритм FindBoxes (алгоритм 1) реализует метод «безопасной» декомпозиции формального контекста на боксы. Теоретическим обоснованием этого алгоритма являются теорема 1 и утверждения 1–3, входными данными служат исходный контекст $K = (G, M, I)$ и целое положительное число $k$ — число итераций. Результат работы алгоритма FindBoxes: $\Omega$ — множество боксов и $H$ — множество типичных представителей боксов, входящих в $\Omega$.

Алгоритм FindBoxes включает следующие основные процедуры: Boxes, Delete, SearchChains. Процедура Boxes разлагает заданный бокс $\omega$, плотность которого отлична от 1, на более мелкие боксы и находит для них типичных представителей. Процедура Delete удаляет кратные боксы и боксы, совпадающие с исходным. Процедура SearchChains выявляет вложенные боксы, выполняет построение взаимно непересекающихся цепей частично упорядоченного множества боксов $\Omega_1$ и находит для этих цепей максимальные элементы. Данная процедура позволяет уменьшать число боксов, получаемых на каждой итерации разложения.

Если число итераций процесса декомпозиции равно $k$, то разложение можно осуществить за время $\mathrm{O}\Big(|G|^{2k} \cdot |M|^{2k}\Big)$; при $k = 1$ алгоритм FindBoxes выполняется за время $\mathrm{O}\big(|G|^2 \cdot |M|^2\big)$. Для дополнительного ограничения числа частей, получаемых на каждой итерации, можно устанавливать пороговое значение на плотность боксов, подлежащих дальнейшему разложению. Это достигается заменой на шаге 8 алгоритма FindBoxes условия $\sigma(\omega) \neq 1$ условием $\sigma(\omega) < \sigma_0$, где $\sigma_0$ — пороговое значение плотности боксов, которые подлежит дальнейшему разложению.

Для оценки результативности алгоритма FindBoxes проведены вычислительные эксперименты при $k = 1$ и без задания ограничения на плотность боксов. Эксперименты проводились с помощью программы FCACorpus [7], осуществляющей нахождение всех формальных понятий. Использовались контексты, сгенерированные случайным образом. Для каждого контекста $K = (G, M, I)$ осуществлялось нахождение множества $FC$ всех формальных понятий без разбиения на боксы и с итеративным разбиением на боксы. Анализировались два случая при проверке вложенности боксов: случай 1 — проверка производится без типичных представителей боксов, случай 2 —

**Алгоритм 1.** FindBoxes

**Вход:** исходный контекст $K = (G, M, I)$, $k$ — количество итераций.
**Выход:** $\Omega$ — множество боксов, $H$ — множество типичных представителей боксов из $\Omega$.

$\Omega_1 := (G, M, I)$ // *множество боксов, подлежащих дальнейшему разложению*
$\Omega_2 := \varnothing$ // *множество боксов, не подлежащих дальнейшему разложению*
$H_1 := (G'', M'')$ // *множество типичных представителей боксов, входящих в* $\Omega_1$
$H_2 := \varnothing$ // *множество типичных представителей боксов, входящих в* $\Omega_2$
**Пока** $(k \neq 0 \;\&\; \Omega_1 \neq \varnothing)$
  $Q := \varnothing$, $V := \varnothing$.
  **Для всех** $\omega \in \Omega_1$
    **Если** $\sigma(\omega) \neq 1$, **то**
      Boxes$(\omega, X, Y)$; $Q := Q \cup X$; $R := R \cup Y$,
    **иначе**
      $\Omega_2 := \Omega_2 \cup \omega$; $H_2 := H_2 \cup H_1$.
  $W_1 := Q$; $H_1 := R$; Delete $(\Omega_1 \cup \Omega_2, H_1 \cup H_2)$.
  **Если** $\Omega_1 \neq \varnothing$ **то**
    SearchChains$(\Omega_1, H_1)$.
  $k := k - 1$.
$\Omega := \Omega_1 \cup \Omega_2$; $H := H_1 \cup H_2$.

с помощью типичных представителей. Результаты эксперимента приведены в таблице, где $N$ — количество образованных боксов; $|FC|$ — число найденных формальных понятий; $t$ — время выполнения программы. Эксперименты выполнялись на компьютере с процессором Intel Core i7-720QM Processor (6M Cache, 1,60 ГГц) и ОЗУ размером 4 Гбайт.

**Оценка эффективности процесса декомпозиции формального контекста**

| Случаи | Характеристика исходного контекста | | | | Результаты | | |
|---|---|---|---|---|---|---|---|
| | $\lvert G\rvert$ | $\lvert M\rvert$ | $\lVert T\rVert$ | $\sigma(G, M)$ | $N$ | $\lvert FC\rvert$ | $t$, мс |
| Без разложения на боксы | 100 | 20 | 1000 | 0,5 | – | 4962 | 145125 |
| С разложением на боксы (случай 1) | | | | | 883 | 4962 | 2878 |
| С разложением на боксы (случай 2) | | | | | 883 | 4962 | **2200** |
| Без разложения на боксы | 200 | 30 | 2940 | 0,49 | – | 10567 | 794520 |
| С разложением на боксы (случай 1) | | | | | 2895 | 10567 | 97906 |
| С разложением на боксы (случай 2) | | | | | 2895 | 10567 | **90908** |

Из таблицы видно, что значения $|FC|$ в случаях без разложения и с разложением на боксы полностью совпадают; число боксов, образованных при разложении контекста, не превышает величины $\|T\|$; алгоритм FindBoxes даёт значительный выигрыш по времени: время выполнения программы FCACorpus при разложении контекста на боксы уменьшается в несколько раз.

## Заключение

Представленный алгоритм FindBoxes реализует метод «безопасной» декомпозиции формального контекста и на практике позволяет разложить задачу нахождения всех формальных понятий на подзадачи за полиномиальное время. Алгоритм также приме-

ним для ускорения существующих алгоритмов решения родственных задач, связанных с нахождением максимальных полных подматриц 0,1-матрицы.

ЛИТЕРАТУРА

1. *Биркгоф Г.* Теория решеток. М.: Наука, 1984. 568 с.
2. *Ganter B. and Wille R.* Formal Concept Analyses: Mathematical Foundations. Springer Science and Business Media, 2012. 314 p.
3. *Ganter B. and Obiedkov S. A.* Conceptual Exploration. Berlin; Heidelberg: Springer, 2016. 315 p.
4. *Kuznetsov S. O. and Obiedkov S. A.* Comparing performance of algorithms for generating concept lattices // J. Exper. Theor. Artificial Intelligence. 2002. V. 14. No. 2. P. 189–216.
5. *Mongush Ch. M. and Bykova V. V.* On decomposition of a binary context without losing formal concepts // J. Siberian Federal University. Mathematics and Physics. 2019. No. 3. P. 323–330.
6. *Быкова В. В., Монгуш Ч. М.* Декомпозиционный подход к исследованию формальных контекстов // Прикладная дискретная математика. 2019. №. 44. С. 111–124.
7. *Монгуш Ч. М., Быкова В. В.* Программа FCACorpus концептуального моделирования тувинских текстов методами анализа формальных понятий. Свид. о гос. регистрации программы для ЭВМ № 2018618907, выдано Федеральной службой по интеллектуальной собственности РФ, 2018.

УДК 519.7 DOI 10.17223/2226308X/12/63

# ОБ ИСПОЛЬЗОВАНИИ ТЕХНОЛОГИЙ МАШИННОГО ОБУЧЕНИЯ ДЛЯ ПРОВЕРКИ СТАТИСТИЧЕСКИХ СВОЙСТВ СИММЕТРИЧНЫХ КРИПТОГРАФИЧЕСКИХ АЛГОРИТМОВ

А. А. Перов

Рассматривается применение технологий машинного обучения к задачам криптографии, в частности проведению статистического анализа блочных шифров. Изложена идея адаптации шифртекстов к алгоритму модели нейронной сети Inception V3. Приведены результаты экспериментов.

**Ключевые слова:** *криптография, машинное обучние, статистический анализ, раунд шифрования, итеративные блочные шифры.*

## Введение

Традиционно статистический анализ проводится с помощью тестов, определяющих степень случайности выходной последовательности [1] с применением методов математической статистики. Исследования показывают, что современные итеративные алгоритмы шифрования обеспечивают удовлетворительные статистические свойства на меньшем, чем полное, числе раундов. Использование технологий машинного обучения для решения подобных задач является новым направлением. Для разработки методики проведения статистического анализа была использована нейронная сеть Inception v3, обычно применяющаяся для распознавания и классификации графических образов. Inception v3 является свёрточной нейронной сетью, состоящей из 17 слоёв, обученной на большом количестве изображений из базы ImageNet.

## 1. Преобразование шифртекстов

Для решения задачи по обучению нейронной сети для статистического анализа выполнено преобразование зашифрованных сообщений в формат графических изображе-

ний. Для конвертации разработана утилита на языке C++, которая считывает в бинарном виде текстовый файл с зашифрованным сообщением и каждый байт зашифрованного текста записывает в качестве значения компонент палитры RGB, формируя изображения формата JPEG. При подаче на вход такой программе текстового файла с одним и тем же раскопированным символом на выходе будет получено однотонное изображение. При подаче циклически повторяющегося набора символов изображение принимает характер узорчатого, что подтверждает корректность реализации.

Вторым подготовительным этапом является формирование базы шифртекстов различных алгоритмов на разном числе раундов шифрования. С помощью библиотеки «Униблокс-2015» [2] получены шифртексты различных криптоалгоритмов на разном числе раундов. После завершения подготовительных этапов проведены эксперименты, ставшие основой методики проведения тестирования средствами технологии машинного обучения.

**Эксперимент 1:** были сгенерированы по 1000 шифртекстов алгоритма Simon на 3 и 30 раундах. Отличия на этих выборках видны человеку визуально: для последовательностей на 3 раундах очевидно прослеживаются зависимости, тогда как отображения 30-раундовых шифртекстов визуально имеют равномерное распределение. В данном эксперименте модель отличила 100 % поданных на тестовой выборке шифртекстов.

**Эксперимент 2:** сравнивались значения соседних раундов итеративного блочного шифра. В качестве обучающей выборки были поданы зашифрованные последовательности алгоритма Simon с 3 по 21 раунд (по 500 изображений на каждый). Модель должна была обнаружить, происходят ли изменения в структурах шифртекстов с каждым раундовым преобразованием. В отличие от эксперимента 1, разницу между соседними раундами определить визуально невозможно. На рис. 1 приведён график зависимости процента верных решений при различении раундов от их числа. Отмечается, что выборки шифра Simon на 3 и 4 раундах проходят одинаково малое число статистических тестов NIST, то есть для классического способа проведения статистического анализа выборки одинаковы, тогда как нейросеть отличила их более чем в 92 % случаев. Следует отметить, что после 15-го раунда модель правильно различала соседние раунды с вероятностью, стремящейся к 0,5, что может свидетельствовать о том, что качество выходной последовательности уже не улучшается и выборка обладает удовлетворительными статистическими свойствами.

**Эксперимент 3:** модель была обучена на выборках алгоритмов Speck и Present до 9-го раунда шифрования. Выбор этих шифров обусловлен схожим поведением при традиционном статистическом тестировании: на раундах до 9 оба алгоритма проходят примерно одинаковое число тестов. Несмотря на то, что алгоритмы по своей структуре выполняют разные преобразования над открытым текстом, модель способна успешно отличать друг от друга шифртексты до 7-го раунда (на первых шести раундах модель различила 100 % тестовых шифртекстов, к седьмому раунду процент понизился до 90,9 %). На 10-м раунде нейросеть при различении изображений приняла только 52 % правильных решений (статистические тесты определили именно эту границу минимального числа раундов, обеспечивающих удовлетворительные статистические свойства [2]). Найденное значение правильных решений модели может свидетельствовать о том, что оба алгоритма уже к 10-му раунду дают статистически качественный шифртекст.

**Эксперимент 4:** нейронная сеть была переобучена на изображениях шифртекстов разных шифров. На основании данных, полученных с помощью тестов NIST, на вход

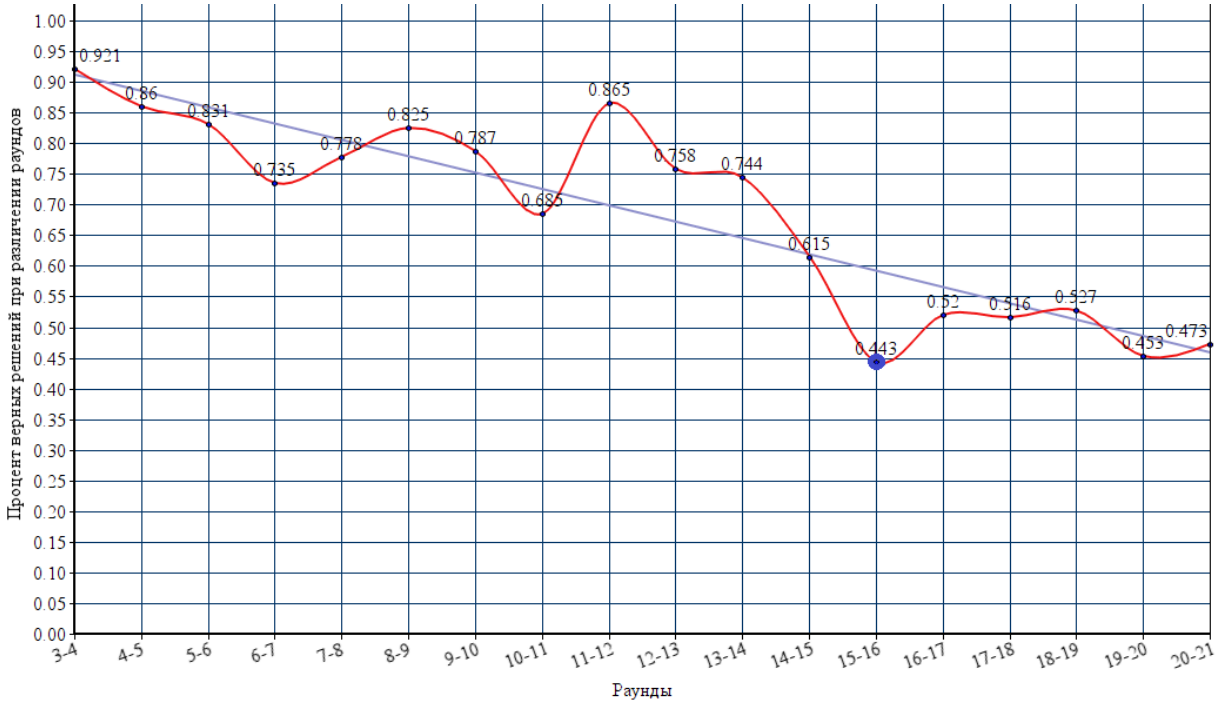


Рис. 1. График зависимости процента правильных решений модели от числа раундов шифра Simon

сети было суммарно подано более 10000 шифртекстов всех алгоритмов библиотеки, зашифрованных на числе раундов, не обеспечивающих удовлетворительных статистических свойств. В качестве второй половины обучающей выборки использовалось также более 10000 шифртекстов, зашифрованных на полном числе раундов разными алгоритмами. В качестве тестовой выборки нейросеть получила более 2100 изображений, которые были случайным образом выбраны из базы сгенерированных шифртекстов. В 98 % случаев алгоритм машинного обучения верно определил степень случайности шифртекста.

## Выводы

Широкое применение машинного обучения и, в частности, компьютерного зрения в самых разных областях жизни на сегодняшний день обусловлено высокими показателями результативности этих технологий. Описанные эксперименты подтвердили гипотезу о возможности применения нейронных сетей для решения задач анализа статистических свойств, так как полученные результаты согласуются с традиционными методами анализа посредством статистических тестов. Результаты экспериментов 2–4, в частности, свидетельствуют о том, что анализ статистических свойств для итеративных блочных шифров может проходить по разным сценариям, которые построены как на сравнении между собой шифртекстов одного алгоритма, зашифрованных на разном числе раундов, так и на сравнении зашифрованных последовательностей с эталонными, полученными в результате работы алгоритма на полном числе раундов.

## ЛИТЕРАТУРА

1. *Ryabko B. and Monarev V.* Using information theory approach to randomness testing // J. Statistical Planning and Inference. 2005. V. 133. No. 1. P. 95–110.

2. *Перов А. А., Пестунов А. И.* Статистическое тестирование современных итеративных блочных шифров с помощью программной библиотеки «УНИБЛОКС-2015» // Инновации в жизнь. 2016. № 2. С. 89–97.

УДК 519.6 DOI 10.17223/2226308X/12/64

# СПОСОБ РЕШЕНИЯ НЕДООПРЕДЕЛЁННЫХ СИСТЕМ ЛИНЕЙНЫХ УРАВНЕНИЙ НАД GF(2) С ИСКАЖЁННЫМИ ПРАВЫМИ ЧАСТЯМИ И ОГРАНИЧЕНИЕМ НА МАЛЫЙ ВЕС РЕШЕНИЯ

Н. Ю. Руменко, А. В. Костюк

Рассматриваются недоопределённые случайные системы линейных булевых уравнений с искажёнными правыми частями, истинное решение которых имеет малый вес Хемминга. Экспериментально показывается, что для малых вероятностей искажения такие системы могут быть эффективно решены применением алгоритмов декодирования по информационным множествам.

**Ключевые слова:** *случайные системы линейных булевых уравнений, декодирование по информационным множествам.*

Рассмотрим систему из фиксированного числа $m < n$ линейных булевых уравнений (СЛУ)

$$Ax = b = Ax_0 \oplus \xi, \tag{1}$$

где $A$ — случайная двоичная матрица размера $m \times n$; $\xi^{\mathrm{T}} = (\xi_0, \ldots, \xi_{m-1})$ — случайный двоичный вектор ошибок, координаты которого независимы и принимают значения с вероятностями $\mathsf{P}\{\xi_i = 1\} = 1 - \mathsf{P}\{\xi_i = 0\} = p$, $i \in \{0, \ldots, m-1\}$, $p \in [0, 1/2)$; $x_0$ — вектор истинного решения, $||x_0|| = w$, $||.||$ — вес Хемминга.

Для малых значений $w$ известны алгоритмы решения таких систем, основанные на переборе возможных значений истинного решения [1, 2].

В алгоритме максимума правдоподобия [1] непосредственно вычисляются все возможные векторы $y$ длины $n$ веса $w$ и в качестве решения выдаётся вектор с наименьшим значением $||Ay||$. Алгоритм имеет асимптотическую сложность $\mathrm{O}((1-2p)^{-2} n^w \log n)$ при использовании $\mathrm{O}(1)$ бит дополнительной (помимо хранения системы уравнений) памяти [2].

В работе [2] рассматривается вычислительно более эффективный алгоритм на основе метода «встречи посередине» с емкостной сложностью $\mathrm{O}(n^{w/2})$ и вычислительной сложностью $\mathrm{O}(n^{w/2} l((m-t)\log n^{w/2} + wm))$, где $t$ — пороговое значение $||Ay||$; $l$ — число итераций.

Вычислительная сложность алгоритмов данного класса более всего зависит от параметра $w$, что делает их малоприменимыми для слабоискажённых систем с достаточно большим весом истинного решения.

С другой стороны, матрицу $A$ можно рассматривать как проверочную матрицу некоторого случайного линейного блокового кода $M(n, n-m)$, для которого вектор $b$ является синдромом ошибки веса $w$, причём каждый бит синдрома дополнительно искажён с вероятностью $p$. Задача решения системы (1), таким образом, состоит в декодировании случайного кода по искажённому синдрому.

Составим расширенную систему

$$Ch = b, \tag{2}$$

где $C = \left[\, I \,\middle|\, A \,\right]$, $I$ — единичная матрица размера $m \times m$; $h^{\mathrm{T}} = [\, \xi \,|\, x_0 \,]$ и $[\, \cdot \,|\, \cdot \,]$ обозначает конкатенацию.

В системе (2) правая часть уже «неискажённая», при этом вектор решения имеет некоторый случайный вес $w + t$, где $t$ зависит только от $m$ и $p$. По условию $p \ll 1/2$, поэтому с большой вероятностью вес решения по-прежнему останется малым. В рассмотренной постановке матрица $C$ является проверочной матрицей для некоторого случайного кода $M'(n + m, n)$.

Известно [3], что почти все случайные коды лежат на границе Варшамова — Гилберта, т. е. код $M'(n + m, n)$ почти наверное исправляет все ошибки кратности до $\lfloor (d-1)/2 \rfloor$, где $d$ удовлетворяет неравенству $2^m \leqslant \sum\limits_{i=0}^{d-2} \binom{n+m-1}{i}$. Таким образом, при достаточно малых значениях вероятности искажения $p$ для решения системы (2) могут быть использованы алгоритмы декодирования по информационным множествам, большое количество которых было разработано в рамках криптоанализа систем Мак-Элиса и Нидеррайтера [4].

Для оценки эффективности предлагаемого способа использован алгоритм Мэя — Мюэра — Томае [4] (ALGORITHM 2), сравнение проводилось с алгоритмом из работы [2] (ALGORITHM 1), результаты среднего времени выполнения приведены в табл. 1 и 2. Проведённые эксперименты показывают, что для достаточно малых вероятностей искажения предложенный способ позволяет находить истинное решение более эффективно, чем перебор возможных решений.

Таблица 1

**СЛУ с искажённой правой частью,**
$n = 256$, $m = 128$, $w = 8$

| Вероятность искажения $p$ | Среднее время выполнения, с | |
|---|---|---|
| | ALGORITHM 1 | ALGORITHM 2 |
| 0,001 | 144,284 | 0,062 |
| 0,005 | 164,131 | 0,120 |
| 0,010 | 191,219 | 0,355 |
| 0,020 | 305,235 | 1,625 |

Таблица 2

**СЛУ с искажённой правой частью,**
$n = 512$, $m = 200$, $w = 10$

| Вероятность искажения $p$ | Среднее время выполнения, с | |
|---|---|---|
| | ALGORITHM 1 | ALGORITHM 2 |
| 0,001 | $> 7200$ | 12,100 |
| 0,005 | $> 7200$ | 49,021 |
| 0,010 | $> 7200$ | 109,960 |
| 0,020 | $> 7200$ | 576,460 |

## ЛИТЕРАТУРА

1. *Балакин Г. В.* Введение в теорию случайных систем уравнений // Труды по дискретной математике. М.: ТВП, 1997. Т. 1. С. 1–18.
2. *Алексейчук А. Н., Грязнухин А. Ю.* Быстрый алгоритм восстановления истинного решения фиксированного веса системы линейных булевых уравнений с искажённой правой частью // Прикладная дискретная математика. 2013. Т. 20. № 2. С. 59–70.

3. *Варшамов Р. Р.* Оценка числа сигналов в кодах с коррекцией ошибок // Доклады АН СССР. 1957. С. 739–741.
4. *May A., Meurer A., and Thomae E.* Decoding random linear codes in $O(2^{0.054n})$ // Proc. Asiacrypt'2011. Seoul, South Korea, December 04–08, 2011. P. 107–124.

УДК 519.7 DOI 10.17223/2226308X/12/65

# О ПОЧТИ СОВЕРШЕННЫХ НЕЛИНЕЙНЫХ ПРЕОБРАЗОВАНИЯХ И РАЗДЕЛЯЮЩЕМ СВОЙСТВЕ МУЛЬТИМНОЖЕСТВ

М. А. Сорокин, М. А. Пудовкина

Рассматриваются некоторые классы APN-преобразований относительно возможности построения интегральных различителей с помощью разделяющего свойства. Проведён вычислительный эксперимент по определению величины $\lceil n/d \rceil$ для выбранных APN-преобразований $\mathrm{GF}(2^n) \to \mathrm{GF}(2^n)$, где $d$ — алгебраическая степень. Из полученных результатов следует, что не все APN-преобразования имеют наилучшее значение $\lceil n/d \rceil = 2$. Выделены APN-преобразования с параметрами, наиболее оптимальными для противодействия интегральному анализу с помощью разделяющего свойства.

**Ключевые слова:** *APN-преобразование, разделяющее свойство, интегральный различитель, интегральный метод.*

Разностный метод и его обобщения являются одними из основных методов анализа симметричных шифрсистем. Один из этапов разностного метода заключается в нахождении элементов матрицы вероятностей переходов разностей компонент функции зашифрования, включая $S$-боксы. В работе [1] для противодействия разностному методу при синтезе алгоритмов блочного шифрования в качестве S-бокса предложено использовать APN-преобразование (если оно существует).

**Определение 1** [1]. Преобразование $s : \mathrm{GF}(2^n) \to \mathrm{GF}(2^n)$ называется APN-преобразованием, если для каждых ненулевых элементов $\alpha, \beta \in \mathrm{GF}(2^n)$ уравнение $s(x + \alpha) - s(x) = \beta$ имеет два или нуль решений.

Актуальной задачей является исследование APN-преобразований относительно других методов криптоанализа, в частности относительно интегрального метода. В [2] приводится способ построения интегрального различителя с использованием разделяющего свойства (англ. division property).

Пусть $V_n$ — $n$-мерное векторное пространство над полем $\mathrm{GF}(2)$; $\|\alpha\|$ — вес Хэмминга вектора $\alpha$; $\alpha_i$ — $i$-я координата вектора $\alpha = (\alpha_1, \ldots, \alpha_n) \in V_n$, $i \in \{1, \ldots, n\}$.

Для каждого элемента $\beta \in \mathrm{GF}(2)$ положим $\beta^1 = \beta$, $\beta^0 = 1$. Тогда корректно определено отображение $\pi : V_n \times V_n \to V_n$, заданное условием

$$\pi : (\alpha, \delta) \mapsto \prod_{i=1}^{n} \alpha_i^{\delta_i}, \quad \alpha = (\alpha_1, \ldots, \alpha_n) \in V_n, \ \delta = (\delta_1, \ldots, \delta_n) \in V_n.$$

Далее будем рассматривать отображение $\pi(x, \delta)$ только при фиксированном $\delta \in V_n$.

**Определение 2** [2]. Пусть $n \in \mathbb{N}$, $k \in \{1, \ldots, n\}$, $S_k^{(n)} = \{\alpha \in V_n : k \leqslant \|\alpha\|\}$. Говорят, что мультимножество $X$ с носителем $V_n$ имеет разделяющее свойство $D_k^{(n)}$, если для каждого $\delta \in V_n \setminus S_k^{(n)}$ выполняется равенство $\bigoplus\limits_{\alpha \in X} \pi(\alpha, \delta) = 0$.

Будем говорить, что мультимножество $Y$ с носителем $V_n$ получено *применением* векторной булевой функции $g : \mathrm{GF}(2^n) \to \mathrm{GF}(2^n)$ к мультимножеству $X$ с носителем $V_n$, если элементы $Y$ есть результаты применения функции $g$ к каждому элементу мультимножества $X$.

**Теорема 1** [2]. Пусть $s : \mathrm{GF}(2^n) \to \mathrm{GF}(2^n)$ — преобразование алгебраической степени $d$ и мультимножество $X$ с носителем $V_n$ имеет разделяющее свойство $D_k^{(n)}$, $k \in \{1, \ldots, n-1\}$. Тогда мультимножество, полученное применением $s$ к $X$, имеет разделяющее свойство $D_{\lceil k/d \rceil}^{(n)}$.

Из теоремы 1 следует, что чем больше значение $\lceil n/d \rceil$, тем для большего числа раундов существует интегральный различитель, получаемый посредством применения предложенного в работе [2] алгоритма.

В настоящей работе проведён вычислительный эксперимент по определению величины $\lceil n/d \rceil$ для некоторых APN-преобразований $\mathrm{GF}(2^n) \to \mathrm{GF}(2^n)$, приведённых в [3]. Из полученных результатов следует, что не все APN-преобразования имеют наилучшее значение $\lceil n/d \rceil = 2$. Результаты отражены в табл. 1–3 (указаны лучшие параметры, если они найдены).

Таблица 1

**APN-преобразования и их параметры, при которых $\lceil n/d \rceil = 2$**

| Формула и условия | Параметры |
|---|---|
| $x^j$, $j = 2^n - 2$, $n = 2k + 1$ | $n \in \{3, 5, \ldots, 11\}$ |
| $x^j$, $j = 2^t + 2^{0,5t} - 1$, если $t = 2k, k \in \mathbb{N}$; $j = 2^t + 2^{1,5t+0,5} - 1$, если $t = 2k+1, k \in \mathbb{N}$; $n = 2t + 1$ | Для $n = 7, t = 3$ и $n = 11, t = 5$ имеем $d = 4$ и $d = 6$ соответственно |
| $x^j$, $j = 2^{2t} - 1$, $n = 2t + 1$, $t \in \mathbb{N}$ | $t \in \{1, \ldots, 6\}$ |
| $x^j$, $j = 2^{2i} - 2^i + 1$, $(i, n) = 1$ | $(n, i) \in \{(9, 4), (9, 5)\}$, $d = 5$ |
| $x^j$, $j = 2^{4i} + 2^{3i} + 2^{2i} + 2^i - 1$, $n = 5i$, $i \in \mathbb{N}$ | $i \in \{1, 2\}$ |
| $\left(x + \mathrm{tr}_{n/3}\left(x^{2(2^i+1)} + x^{4(2^i+1)}\right) + \right.$ $\left. + \mathrm{tr}(x)\mathrm{tr}_{n/3}\left(x^{2^i+1} + x^{2^{2i}(2^i+1)}\right)\right)^{2^i+1}$, $n = 3k$, $k = 2l$, $l \in \mathbb{N}$, $(i, n) = 1$ | $n = 6$ |

Таблица 2

**APN-преобразования и их параметры, при которых $\lceil n/d \rceil = 6$**

| Формула и условия | Параметры |
|---|---|
| $x^{2^s+1} + wx^{2^{ik}+2^{mk+s}}$, $n = 3k$, $k \in \mathbb{N}$, $(k, 3) = (s, 3k) = 1$, $k \geqslant 4$, $i \equiv sk \pmod 3$, $m = 3i$, $\mathrm{ord}(w) = 2^{2k} + 2^k + 1$ | $n = 12$ |
| $x^{2^s+1} + wx^{2^{ik}+2^{mk+s}}$, $n = 4k$, $k \in \mathbb{N}$, $(k, 2) = (s, 2k) = 1$, $k \geqslant 3$, $i \equiv sk \pmod 4$, $m = 4i$, $\mathrm{ord}(w) = 2^{3k} + 2^{2k} + 2^k + 1$ | $n = 12$ |

Таблица 3

**APN-преобразования, для которых $\lceil n/d \rceil$ растёт с ростом $n$**

| Формула и условия | Параметры |
|---|---|
| $x^j$, $j = 2^i + 1$, $(i, n) = 1$ | $n \in \{2, \ldots, 12\}$, $d = 2$ |
| $x^{2^i+1} + \left(x^{2^i} + x + 1\right) \operatorname{tr}\left(x^{2^i+1}\right)$, $n \geqslant 4$, $n = 2k + 1$, $k \in \mathbb{N}$, $(i, n) = 1$ | $n \in \{4, 6, \ldots, 12\}$, $d = 3$ |
| $x^3 + \operatorname{tr}(x^9)$, $n > 2p \geqslant 7$ для такого наименьшего $p$, что $p > 1$, $p \neq 3$ и $(p, n) = 1$ | $n \in \{7, 9, 11, 12, 13\}$, $d = 2$ |

## ЛИТЕРАТУРА

1. *Nyberg K. and Knudsen L.R.* Provable security against differential cryptanalysis // CRYPTO 1992. LNCS. 1993. V. 740. P. 566–574.
2. *Todo Y.* Structural evaluation by generalized integral property // EUROCRYPT 2015. P. I. LNCS. 2015. V. 9056. P. 287–314.
3. *Тужилин М. Э.* Почти совершенные нелинейные функции // Прикладная дискретная математика. 2009. Т. 5. № 3. С. 14–20.

# СВЕДЕНИЯ ОБ АВТОРАХ

**АБРОСИМОВ Михаил Борисович** — доктор физико-математических наук, заведующий кафедрой Саратовского национального исследовательского государственного университета им. Н. Г. Чернышевского, г. Саратов. E-mail: **mic@rambler.ru**

**АВЕЗОВА Яна Эдуардовна** — аналитик АО «Позитив Текнолоджиз», г. Москва. E-mail: **avezovayana@gmail.com**

**АГИБАЛОВ Геннадий Петрович** — доктор технических наук, профессор, главный научный сотрудник лаборатории компьютерной криптографии Томского государственного университета, г. Томск. E-mail: **agibalov@isc.tsu.ru**

**АГИЕВИЧ Сергей Валерьевич** — кандидат физико-математических наук, заведующий НИЛ проблем безопасности информационных технологий НИИ прикладных проблем математики и информатики Белорусского государственного университета, г. Минск. E-mail: **agievich@bsu.by**

**АНТОНОВ Кирилл Валентинович** — студент ИМЭИ Иркутского государственного университета, г. Иркутск. E-mail: **aknitr@mail.ru**

**БОБРОВ Владимир Михайлович** — студент кафедры № 42 криптологии и кибербезопасности НИЯУ МИФИ, г. Москва. E-mail: **bvm_15@mail.ru**

**БОЛТНЕВ Юрий Федорович** — доцент ИФМНиИТ Балтийского федерального университета им. И. Канта, г. Калининград. E-mail: **yuri.boltnev@gmail.com**

**БОРОВКОВА Ирина Вячеславовна** — студентка Национального исследовательского Томского государственного университета, г. Томск. E-mail: **iborovkova95@gmail.com**

**ВЕДУНОВА Марина Викторовна** — студентка электротехнического факультета Уральского государственного университета путей сообщения, г. Екатеринбург. E-mail: **marina.vedunova.13.99@gmail.com**

**ВЛАСОВА Виктория Владимировна** — аспирантка кафедры информационной безопасности Московского государственного технического университета им. Н. Э. Баумана, г. Москва. E-mail: **victvlasova@yandex.ru**

**ГЕУТ Кристина Леонидовна** — старший преподаватель кафедры естественно-научных дисциплин Уральского государственного университета путей сообщения, г. Екатеринбург. E-mail: **geutkrl@yandex.ru**

**ГОРОДИЛОВА Анастасия Александровна** — кандидат физико-математических наук, научный сотрудник Института математики им. С. Л. Соболева СО РАН, старший преподаватель Новосибирского государственного университета, г. Новосибирск. E-mail: **gorodilova@math.nsc.ru**

**ГРИБАНОВА Ирина Александровна** — аспирантка Института динамики систем и теории управления им. В. М. Матросова СО РАН, г. Иркутск. E-mail: **the42dimension@gmail.com**

**ДАВЛЕТШИНА Александра Маратовна** — аспирантка факультета ВМК МГУ имени М. В. Ломоносова, исследователь Центра научных исследований и перспективных разработок ОАО «ИнфоТеКС», г. Москва. E-mail: **Aleksandra.Davletshina@infotecs.ru**

**ДЕВЯНИН Петр Николаевич** — доктор технических наук, профессор, член-корреспондент Академии криптографии РФ, главный научный сотрудник АО «НПО РусБИТех», г. Москва. E-mail: **devyanin.peter@yandex.ru**

**Де Ла КРУС ХИМЕНЕС Рейнер Антонио** — научный сотрудник Института криптографии Гаванского университета, г. Гавана, Куба. E-mail: **djr.antonio537@gmail.com**

**ЕЛИСЕЕВ Владимир Леонидович** — кандидат технических наук, руководитель Центра научных исследований и перспективных разработок ОАО «ИнфоТеКС», доцент кафедры управления и информатики Национального исследовательского университета «Московский энергетический институт», г. Москва. E-mail: **vlad-eliseev@mail.ru**

**ЖАРКОВА Анастасия Владимировна** — кандидат физико-математических наук, доцент кафедры теоретических основ компьютерной безопасности и криптографии Саратовского национального исследовательского государственного университета имени Н. Г. Чернышевского, г. Саратов.
E-mail: **ZharkovaAV3@gmail.com**
**ЖЕНЕВСКИЙ Степан Викторович** — сотрудник ФУМО ВО «Информационная безопасность», г. Москва. E-mail: **zhenevski@yandex.ru**
**ИГНАТОВА Анастасия Олеговна** — студентка электротехнического факультета Уральского государственного университета путей сообщения, г. Екатеринбург.
E-mail: **anastasiaignatova101@gmail.com**
**КАМИЛ Ихаб Абдулджаббар Камил** — аспирант Саратовского национального исследовательского государственного университета им. Н. Г. Чернышевского, г. Саратов.
E-mail: **kamil.iehab@mail.ru**
**КАРПОВА Любовь Александровна** — студентка Национального исследовательского Томского государственного университета, г. Томск. E-mail: **lubakarpova1135@gmail.com**
**КИШКАН Владимир Владимирович** — аспирант кафедры прикладной математики Сибирского государственного университета науки и технологий имени академика М. Ф. Решетнёва, г. Красноярск.
E-mail: **kishkan@mail.ru**
**КОЙ ПУЭНТЕ Оливер** — научный сотрудник ООО «Центр сертификационных исследований», г. Москва. E-mail: **o.coypuente@gmail.com**
**КОЛБАСИНА Ирина Валерьевна** — ассистент кафедры прикладной математики Сибирского государственного университета науки и технологий имени академика М. Ф. Решетнёва, г. Красноярск.
E-mail: **kabaskina@yandex.ru**
**КОЛЕСНИКОВ Никита Сергеевич** — аспирант Балтийского федерального университета им. И. Канта, г. Калининград. E-mail: **NiKolesnikov@stud.kantiana.ru**
**КОЛОМЕЕЦ Николай Александрович** — кандидат физико-математических наук, научный сотрудник Института математики им. С. Л. Соболева СО РАН, г. Новосибирск.
E-mail: **kolomeec@math.nsc.ru**
**КОМИССАРОВ Семён Михайлович** — студент НИЯУ МИФИ, г. Москва.
E-mail: **semenkomissarov@gmail.com**
**КОРЕНЕВА Алиса Михайловна** — ведущий системный аналитик ООО «Код Безопасности», г. Москва. E-mail: **alisa.koreneva@gmail.com**
**КОСТЮК Александр Владимирович** — кандидат технических наук, старший научный сотрудник Московского технического университета связи и информатики, г. Москва.
E-mail: **av_kost@mail.ru**
**КУЗНЕЦОВ Александр Алексеевич** — доктор физико-математических наук, профессор, директор института Сибирского государственного университета науки и технологий им. акад. М. Ф. Решетнёва, г. Красноярск. E-mail: **alex_kuznetsov80@mail.ru**
**КУЗЬМИНА Татьяна Андреевна** — студентка механико-математического факультета Новосибирского государственного университета, г. Новосибирск. E-mail: **tanya11_95@mail.ru**
**КУЦЕНКО Александр Владимирович** — аспирант механико-математического факультета Новосибирского национального исследовательского государственного университета, г. Новосибирск.
E-mail: **AlexandrKutsenko@bk.ru**
**ЛОБОВ Александр Андреевич** — старший лаборант Саратовского национального исследовательского государственного университета им. Н. Г. Чернышевского, г. Саратов.
E-mail: **aisanekai@mail.ru**
**ЛОСЬ Илья Викторович** — аспирант Саратовского государственного университета им. Н. Г. Чернышевского, г. Саратов. E-mail: **los.ilia.ru@gmail.com**
**МАЛЫГИНА Екатерина Сергеевна** — кандидат физико-математических наук, доцент Балтийского федерального университета им. И. Канта, г. Калининград. E-mail: **Ekkat@inbox.ru**

**МАНЯЕВ Глеб Олегович** — сотрудник ФУМО ВО «Информационная безопасность», г. Москва. E-mail: **gmolymp@yandex.ru**

**МАСЛОВ Александр Сергеевич** — кандидат физико-математических наук, старший научный сотрудник НИЛ проблем безопасности информационных технологий, НИИ прикладных проблем математики и информатики Белорусского государственного университета, г. Минск.
E-mail: **maslov@bsu.by**

**МЕДВЕДЕВ Никита Владимирович** — кандидат технических наук, доцент кафедры ИТиЗИ Уральского государственного университета путей сообщения, г. Екатеринбург.
E-mail: **itcrypt@gmail.com**

**МЕДВЕДЕВА Наталья Валерьевна** — кандидат физико-математических наук, доцент, доцент Уральского государственного университета путей сообщения, г. Екатеринбург.
E-mail: **medvedeva_n_v@mail.ru**

**МЕЖЕННАЯ Наталья Михайловна** — кандидат физико-математических наук, доцент, доцент кафедры прикладной математики Московского государственного технического университета им. Н. Э. Баумана, г. Москва. E-mail: **natalia.mezhennaya@gmail.com**

**МЕЛЬНИКОВ Сергей Леонидович** — сотрудник ФУМО ВО «Информационная безопасность», г. Минск. E-mail: **msl23021996@mail.ru**

**МЕЛЬНИЧУК Евгений Михайлович** — аспирант Балтийского федерального университета им. И. Канта, г. Калининград. E-mail: **emelnichuk39@gmail.com**

**МЕТАЛЬНИКОВА Анастасия Игоревна** — студентка Национального исследовательского Томского государственного университета, г. Томск. E-mail: **xwaim21@gmail.com**

**МИЛОСЕРДОВ Алексей Васильевич** — студент механико-математического факультета Новосибирского государственного университета, г. Новосибирск. E-mail: **amiloserdov6@gmail.com**

**МОНГУШ Чодураа Михайловна** — аспирантка Сибирского федерального университета, г. Красноярск; преподаватель Тувинского государственного университета, Республика Тыва.
E-mail: **mongushchod91@yandex.ru**

**НОВОСЕЛОВ Семен Александрович** — ассистент Балтийского федерального университета им. И. Канта, г. Калининград. E-mail: **snovoselov@kantiana.ru**

**ОТПУЩЕННИКОВ Илья Владимирович** — кандидат технических наук, научный сотрудник лаборатории 6.2 ИДСТУ СО РАН, г. Иркутск. E-mail: **otilya@yandex.ru**

**ПАНКОВ Константин Николаевич** — кандидат физико-математических наук, старший научный сотрудник отдела безопасности критической информационной инфраструктуры, доцент кафедры информационной безопасности, начальник отдела аспирантуры Московского технического университета связи и информатики, эксперт ТК-159 и ISO 307, г. Москва. E-mail: **k.n.pankov@gmail.com**

**ПАНКРАТОВА Ирина Анатольевна** — кандидат физико-математических наук, доцент, заведующая лабораторией компьютерной криптографии Национального исследовательского Томского государственного университета, г. Томск. E-mail: **pank@isc.tsu.ru**

**ПЕРОВ Артём Андреевич** — старший преподаватель, аспирант кафедры информационных технологий НГУЭУ, г. Новосибирск. E-mail: **perov_artem@inbox.ru**

**ПОГОРЕЛОВ Борис Александрович** — доктор физико-математических наук, профессор, действительный член Академии криптографии Российской Федерации, г. Москва.

**ПУДОВКИНА Марина Александровна** — доктор физико-математических наук, профессор кафедры информационной безопасности Московского государственного технического университета им. Н. Э. Баумана, г. Москва. E-mail: **maricap@rambler.ru**

**РАЗУМОВСКИЙ Петр Владимирович** — аспирант Саратовского государственного университета, г. Саратов. E-mail: **shprotby@gmail.com**

**РОДРИГЕС Аулет Рамсес** — научный сотрудник Института криптографии Гаванского университета, г. Гавана, Куба. E-mail: **rodriguezra@yandex.com**

**РОМАНЬКОВ Виталий Анатольевич** — доктор физико-математических наук, профессор, заведующий кафедрой Омского государственного университета им. Ф. М. Достоевского, г. Омск.
E-mail: **romankov48@mail.ru**

**РУМЕНКО Никита Юрьевич** — аспирант Московского технического университета связи и информатики, г. Москва. E-mail: **nrum90@yandex.ru**

**РЫБАЛОВ Александр Николаевич** — кандидат физико-математических наук, доцент кафедры компьютерной математики и программирования Омского государственного университета им. Ф. М. Достоевского, г. Омск. E-mail: **alexander.rybalov@gmail.com**

**САПЕГИНА Марина Дмитриевна** — студентка кафедры № 42 криптологии и кибербезопасности НИЯУ МИФИ, г. Москва. E-mail: **mdsapegina@gmail.com**

**САФОНОВ Константин Владимирович** — доктор физико-математических наук, профессор, заведующий кафедрой Сибирского государственного университета науки и технологий имени академика М. Ф. Решетнёва, г. Красноярск. E-mail: **safonovkv@rambler.ru**

**СЕМЁНОВ Александр Анатольевич** — кандидат технических наук, доцент, заведующий лабораторией 6.2 ИДСТУ СО РАН, г. Иркутск. E-mail: **biclop.rambler@yandex.ru**

**СЕМИБРАТОВ Илья Валериевич** — студент Финансового университета при Правительстве Российской Федерации, г. Москва. E-mail: **semibratovilya@gmail.com**

**СОЛДАТЕНКО Александр Александрович** — аспирант Института математики и фундаментальной информатики Сибирского федерального университета, г. Красноярск.
E-mail: **glinckon@gmail.com**

**СОРОКИН Михаил Артёмович** — студент кафедры криптологии и кибербезопасности НИЯУ МИФИ, г. Москва. E-mail: **sorokin.michael.96@yandex.ru**

**СУДАНИ Хайдер Хуссейн Карим** — аспирант Саратовского национального исследовательского государственного университета им. Н. Г. Чернышевского, г. Саратов. E-mail: **hayder.1977@mail.ru**

**ТИТОВ Сергей Сергеевич** — доктор физико-математических наук, профессор Уральского государственного университета путей сообщения, г. Екатеринбург. E-mail: **sergey.titov@usaaa.ru**

**ТРЕНЬКАЕВ Вадим Николаевич** — кандидат технических наук, доцент, доцент кафедры защиты информации и криптографии Национального исследовательского Томского государственного университета, г. Томск. E-mail: **tvnik@sibmail.com**

**ТРИФОНОВ Дмитрий Игоревич** — эксперт технического комитета по стандартизации «Криптографическая защита информации», г. Москва. E-mail: **d.arlekino@gmail.com**

**ТУЛЕБАЕВ Азат Ирикович** — программист ООО «Код Безопасности».
E-mail: **a.tulebaev@securitycode.ru**

**ФОМИН Денис Бонифатович** — старший преподаватель национального исследовательского университета «Высшая Школа Экономики», г. Москва. E-mail: **dfomin@hse.ru**

**ФОМИЧЕВ Владимир Михайлович** — доктор физико-математических наук, профессор, профессор Финансового университета при Правительстве Российской Федерации, профессор НИЯУ МИФИ, ведущий научный сотрудник ФИЦ ИУ РАН, г. Москва. E-mail: **fomichev.2016@yandex.ru**

**ХАЙРУЛЛИН Ильяс Ильдарович** — студент кафедры № 42 криптологии и кибербезопасности НИЯУ МИФИ, г. Москва. E-mail: **ildar97-97@mail.ru**

**ЧЕРЕДНИК Игорь Владимирович** — преподаватель Российского технологического университета (МИРЭА), г. Москва. E-mail: **p.n.v.k.s@mail.ru**

**ЧЕРЕМУШКИН Александр Васильевич** — доктор физико-математических наук, научный консультант ФГУП «НИИ «Квант», г. Москва. E-mail: **avc238@mail.ru**

**ШАПОРЕНКО Александр Сергеевич** — студент Новосибирского государственного университета, г. Новосибирск. E-mail: **shaporenko.alexandr@gmail.com**

**ШОЛОМОВ Лев Абрамович** — профессор, доктор физико-математических наук, главный научный сотрудник Федерального исследовательского центра «Информатика и управление» РАН, г. Москва. E-mail: **levshol@mail.ru**

**ШУРУПОВ Андрей Николаевич** — кандидат технических наук, доцент, сотрудник ФУМО ВО «Информационная безопасность», г. Москва. E-mail: **ashurupov@mail.ru**

**ЭРНАНДЕС ПИЛОТО Даниэль Умберто** — научный сотрудник ООО «Центр сертификационных исследований», г. Москва. E-mail: **dhhernandez2410@gmail.com**

**ЯРОШЕНЯ Юлия Сергеевна** — младший научный сотрудник НИЛ проблем безопасности информационных технологий НИИ прикладных проблем математики и информатики Белорусского государственного университета, г. Минск. E-mail: **yuliya_10.06@mail.ru**

# АННОТАЦИИ ДОКЛАДОВ НА АНГЛИЙСКОМ ЯЗЫКЕ

## SECTION 1

*Geut K. L., Titov S. S.* **ON THE BLOCKING OF TWO-DIMENSIONAL AFFINE VARIETIES.** The paper considers the problem of blocking families of subsets and proposes a construction for expanding the blocking sets of a family of two-dimensional affine manifolds in the space of bit strings when its dimension $n$ increases. Examples are given and the cardinality of the complements of the blocking sets of this family of varieties are calculated for high odd dimension. The main construction of the complement of the blocking set for $n = 2m+1$ is its construction in the form of a set of elements in the form $(x, y, z)$, where $z$ is a bit, $y = x^3$ for the bit string $x$ from the complement of the blocking set in the field $\mathrm{GF}(2^m)$. The construction is applied to solve the "A secret sharing" problem of the NSUCRYPTO Olympiad not only for even, but also for an odd dimension of the space.
**Keywords:** *affine manifolds, blocking set, NSUCRYPTO.*

*Kolesnikov N. S., Novoselov S. A.* **ON THE ORDER OF THE FROBENIUS ENDOMORPHISM ACTION ON $L$-TORSION SUBGROUP OF ABELIAN SURFACES.** One of the most powerful tools for point-counting on elliptic curves over finite fields is the Schoof — Elkies — Atkin algorithm. Its main idea is to construct characteristic polynomials for the action of the Frobenius endomorphim on $l$-torsion group. In this work, we study a probabilistic approach to find these characteristic polynomials in case of abelian surface. To do this, we introduce a random variable $\xi$ that takes values from a list $r_1, \ldots, r_n$, where $r_i$ is a possible order of Frobenius action on $l$-torsion subgroup. As soon as we have an explicit distribution of orders, we can obtain a characteristic polynomial in more effective way than in a classical Schoof-like algorithm. In this work, we derive formulas for calculating variance and standard deviation of the random variable $\xi$:

$$D(\xi) \approx \left(\frac{\pi^2}{48}\right)^2 \frac{\psi(l)}{l^2(l^2-1)^2} \frac{1}{\log^2(l)}, \quad \sigma(\xi) = \sqrt{D(\xi)} \approx \frac{\pi^2}{48} \frac{\sqrt{\psi(l)}}{l(l^2-1)} \frac{1}{\log(l)},$$

where

$$\psi(l) = 2l^{10} + 56l^9 - 316l^8 + 1344l^7 - 1948l^6 - 1770l^5 + 6660l^4 - 3516l^3 - 3831l^2 + 4684l - 1369.$$

**Keywords:** *Abelian surfaces, hyperelliptic curves, point-counting, Frobenius endomorphism, $l$-torsion.*

*Malygina E. S.* **CALCULATION OF 3-TORSION IDEAL FOR SOME CLASS OF HYPERELLIPTIC CURVES.** In the paper, we consider hyperelliptic curves of genus two defined by the Dickson polynomials. For such curves, we calculate the 3-torsion ideal, namely we obtain the four generators of this ideal by using the Mumford — Cantor representation for the 3-torsion divisor and by using of $\theta$- and $\wp$-functions.
**Keywords:** *hyperelliptic curve, Dickson polynomial, $l$-torsion ideal, $l$-torsion divisor, modular equation.*

*Mezhennaya N. M.* **ON THE NUMBER OF $f$-RECURRENT RUNS AND TUPLES IN A FINITE MARKOV CHAIN.** $f$-Recurrent tuple is a segment of a discrete

sequence with the letters obtained by sequential applying a function $f$ to $l$ previous letters, and $f$-recurrent run is a tuple that cannot be extended in both directions while maintaining the $f$-recurrence property. Using the Chen — Stein method, we obtain the estimate for the total variation distance between the distribution of the number $\xi$ of $f$-recurrent runs of at least $s$ length in a segment of a finite stationary ergodic Markov chain of length $n$ and the accompanying Poisson distribution, i.e., Poisson distribution with parameter $\lambda_s = \mathsf{E}\xi$, of the order $\mathrm{O}\big(s\lambda_s/n + \mathrm{e}^{us}\sqrt{\lambda_s}\big)$ for some $u > 0$. The Poisson and normal limit theorems for the random variable $\xi$ are derived from the estimate by standard methods (as the length $n$ of a segment of a Markov chain and parameter $s$ tend to infinity). Moreover, the estimate results in that the probability for the presence of $f$-recurrent tuples of at least $s$ length tends to $1 - \mathrm{e}^{\lambda}$ if $n, s \to \infty$ such as $s/n \to 0$, $\lambda_s/n \to 0$, and $\lambda_s \to \lambda$. The properties of distributions of frequencies of $f$-recurrent runs or tuples with certain parameters can be used in the development of statistical tests for the quality of pseudo-random sequences.
**Keywords:** *Markov chain, $f$-recurrent run, $f$-recurrent tuple, Poisson limit theorem, normal limit theorem, Chen — Stein method.*

*Melnichuk E. M., Novoselov S. A.* **ON CHARACTERISTIC POLYNOMIALS FOR SOME GENUS 2 AND 3 CURVES WITH $p$-RANK 1.** In the paper, we study characteristic polynomials for some families of $p$-rank 1 genus 2 and 3 hyperelliptic curves over finite field. $p$-Rank is an important invariant of the curves. It imposes restrictions on the coefficients of the characteristic polynomials and, therefore, on the order of the Jacobian. In this work, we distinguish several classes of $p$-rank 1 curves among curves with authomorphims and find characteristic polynomials for these curves modulo $p$.
**Keywords:** *hyperelliptic curves, p-rank, characteristic polynomial, authomorphism group.*

*Pogorelov B. A., Pudovkina M. A.* **VARIATIONS OF ORTHOMORPHISMS AND PSEUDO-HADAMARD TRANSFORMATIONS ON NONABELIAN GROUPS.** An orthomorphism of a group $(X, \cdot)$ is a permutation $g : X \to X$ such that the mapping $x \mapsto x^{-1}g(x)$ is also a permutation. In the field of symmetric-key cryptography, orthomorphisms of Abelian groups have been used in the Lai — Massey scheme, the FOX family of block ciphers, the quasi-Feistel network, block ciphers in Davies — Meyer mode, and authentication codes. In this paper, we study orthomorphisms, complete mappings and their variations of nonabelian key-addition groups. In the SAFER block cipher, a linear transformation, called the pseudo-Hadamard transformation, has been used to provide the diffusion that a good cipher requires. We describe ten variations of the pseudo-Hadamard transformations on nonabelian groups, which are defined by a permutation $g : X \to X$. We have proved that our ten variations are permutations iff $g$ is an orthomorphism or its variation.
**Keywords:** *orthomorphism, complete mapping, nonabelian group, pseudo-Hadamard transformation, SAFER block cipher.*

*Pogorelov B. A., Pudovkina M. A.* **ON A CLASS OF POWER PIECEWISE AFFINE PERMUTATIONS ON NONABELIAN GROUPS OF ORDER $2^m$ WITH CYCLIC SUBGROUPS OF INDEX 2.** It is known that four nonabelian groups of order $2^m$, where $m \geqslant 4$, have cyclic subgroups of index 2. Examples are well-known dihedral groups and generalized quaternion groups. Any nonabelian group $G$ of order $2^m$ with cyclic subgroups of index 2 can be considered similar to the additive abelian group of the residue ring $\mathbb{Z}_{2^m}$, which is used as a key-addition group of ciphers. In this paper, we define two classes of transformations on $G$, which are called power piecewise affine. For each class we prove a bijection criterion. Using these criteria, we can fully classify orthomorphisms or

their variations among described classes of power piecewise affine permutations.
**Keywords:** *nonabelian group, dihedral group, generalized quaternion group, bijection criterion, orthomorphism.*

*Fomichev V. M., Avezova Ya. E.* **EXACT FORMULA FOR EXPONENT OF MIXING DIGRAPH OF FEEDBACK SHIFT REGISTER.** Let $g$ be a binary $n$-stage nonlinear shift register with feedback $f(x_0, \ldots, x_{n-1})$ and $\Gamma(g)$ denotes a mixing digraph of transformation $g$. By $d_m$ we denote the greatest number of essential variable of $f$. For primitive digraph $\Gamma(g)$, we obtain the exact formulas for exponent of $\Gamma(g)$ for $d_m \in \{n-1, n-2\}$ and of local exponents $\gamma_{u,v}$ for $0 \leqslant u, v < n$.
**Keywords:** *local primitivity of digraph, mixing digraph, primitive digraph, shift register, digraph exponent.*

*Fomichev V. M., Bobrov V. M.* **ESTIMATION OF LOCAL NONLINEARITY CHARACTERISTICS OF VECTOR SPACE TRANSFORMATION ITERATION USING MATRIX-GRAPH APPROACH.** To generalize the matrix-graph approach to examination of nonlinearity characteristics of vector spaces transformations proposed by V. M. Fomichev, we propose mathematical tools for local nonlinearity of transformations. Let $G = \{0, 1, 2\}$ be multiplicative semigroup where $a0 = 0$ for each $a \in G$, $ab = \max\{a, b\}$ for each $a, b \neq 0$. Ternary matrix (matrix over $G$) is called $\alpha$-matrix, $\alpha \in \Pi(2) = \{\langle 2c\rangle; \langle 2s\rangle; \langle 2sc\rangle; \langle 2\rangle\}$, if all its lines ($\langle 2s\rangle$-matrix), columns ($\langle 2c\rangle$-matrix) or lines and columns ($\langle 2sc\rangle$-matrix) contain 2 or if all its elements are equal to 2 ($\langle 2\rangle$-matrix). Set of all ternary matrices $M$ of order $n$ whose $I \times J$-submatrices are $\alpha$-matrices is denoted $M_n^\alpha(I \times J)$, $I, J \subseteq \{1, \ldots, n\}$. For the set of ternary matrices, multiplication operation is defined. If $A = (a_{i,j})$, $B = (b_{i,j})$, then $AB = C = (c_{i,j})$, where $c_{i,j} = \max\{a_{i,1}b_{1,j}, \ldots, a_{i,n}b_{n,j}\}$ and for all $i, j$ multiplication is executed in semigroup $G$. Matrix $M$ is called $I \times J$-$\alpha$-primitive if there is such $\gamma \in \mathbb{N}$ that $M^t \in M_n^\alpha(I \times J)$ for all natural $t \geqslant \gamma$, $\alpha \in \Pi(2)$. The smallest such $\gamma$ is denoted $I \times J$-$\alpha$-exp$M$ and called $I \times J$-$\alpha$-exponent of matrix $M$. There is bijective mapping between the set of ternary matrices of order $n$ and the set of labeled digraphs with $n$ vertices and with elements from $G$ as labels, so the definitions of $I \times J$-$\alpha$-primitivity and $I \times J$-$\alpha$-exponent can be transferred to digraphs. Some sufficient conditions for $I \times J$-$\alpha$-exponent of a matrix to be the smallest its power, raised to which $I \times J$-submatrix is $\alpha$-matrix, $\alpha \in \Pi(2)$, have been established. For $I = \{i\}$, $J = \{j\}$ upper estimates of $I \times J$-$\alpha$-exponents have been obtained for some classes of labeled digraphs, particularly, for digraph in which a path from $i$ to $j$ goes through primitive component of strong connectivity.
**Keywords:** *matrix-graph approach, ternary matrix, labeled digraph, local nonlinearity, local $\alpha$-exponent.*

*Cheremushkin A. V.* **PROPERTIES OF STRONG DEPENDANCE $n$-ARY SEMIGROUPS.** The paper presents results about the structure of strongly dependent $n$-ary operations on a finite set that satisfy the associativity identities for the $n$-ary semigroup, $n \geqslant 3$. It is shown that their description is reduced to the description of binary semigroups with a unit satisfying certain properties. The information is based on the proof of analogues of the Post and Gluskin — Hossu theorems for the case of strongly dependent operations. It is also proved that any strong dependence binary semigroup is a monoid. A description of autotopy groups of strongly dependent $n$-ary semigroup is also given.
**Keywords:** *$n$-ary semigroup, strongly dependent function, autotopy group.*

*Sholomov L. A.* **MINIMAL REPRESENTATIVE SET FOR A SYSTEM OF FREQUENCY CLASSES OF UNDERDETERMINED WORDS.** Let a finite set $M$ and a system $\mathcal{T}$ of some non-empty subsets $T \subseteq M$ be given. Associated with the sets $M$ and $\mathcal{T}$ are the alphabets $A_0 = \{a_i,\ i \in M\}$ of basic symbols and $A = \{a_T,\ T \in \mathcal{T}\}$ of underdetermined symbols. The set of all words of length $l$ in the alphabet $A$, in which each symbol $a_T$ is present $r_T$ times, $\sum\limits_{T\in\mathcal{T}} r_T = l$, is called frequency class and denoted by $\mathcal{K}_l(\mathbf{r})$ where $\mathbf{r} = (r_T,\ T \in \mathcal{T})$. The specification of the word $v$ in the alphabet $A$ is any word obtained from $v$ by replacing each symbol $a_T$ with some $a_i$, $i \in T$. The specification of the set $V$ of words in the alphabet $A$ is any set of words in the alphabet $A_0$, containing for each word $v \in V$ some specification of it. The class $\mathcal{K}_{l_1}(\mathbf{r}_1)$ is considered to be more representative than the class $\mathcal{K}_{l_2}(\mathbf{r}_2)$, if $l_1 \geqslant l_2$ and, whatever the specification of the class $\mathcal{K}_{l_1}(\mathbf{r}_1)$, the set of beginnings of the length $l_2$ of all words from the specification forms some specification for the class $\mathcal{K}_{l_2}(\mathbf{r}_2)$. Let $\mathfrak{K}$ be some system of frequency classes. A subsystem of $\mathfrak{K}$ is called a representative set of the system $\mathfrak{K}$ if, for any $\mathcal{K}_l(\mathbf{r}) \in \mathfrak{K}$, the subsystem contains a class that is more representative than $\mathcal{K}_l(\mathbf{r})$. The paper presents a method for finding the smallest representative set for an arbitrary system of frequency classes. This setting arises in the problems of underdetermined data compression and of underdetermined functions implementation.

**Keywords:** *underdetermined data, specification, frequency class, representative set.*

*Novoselov S. A., Boltnev Y. F.* **CHARACTERISTIC POLYNOMIALS OF THE CURVE $y^2 = x^7 + ax^4 + bx$ OVER FINITE FIELDS.** In this work, we list all possible characteristic polynomials of the Frobenius endomorphism for genus 3 hyperelliptic curves of type $y^2 = x^7 + ax^4 + bx$ over finite field $\mathbb{F}_q$ of characteristic $p > 3$.

**Keywords:** *hyperelliptic curves, characteristic polynomials, point-counting, genus* 3.

## SECTION 2

*Karpova L. A., Pankratova I. A.* **MIXING PROPERTIES FOR SOME CLASSES OF PERMUTATIONS ON $\mathbb{F}_2^n$.** In the class $\mathcal{F}_{n,k}$ of permutations on $\mathbb{F}_2^n$ with coordinate functions essentially depending on exactly $k$ variables, $k < n$, we consider two subclasses $S_{n,k}$ and $P_{n,k}$. The method for constructing a function $F(x_1, \ldots, x_n) = (f_1, \ldots, f_n) \in \in S_{n,k}$ starts from some function $G(x_1, \ldots, x_k) = (g_1, \ldots, g_k) \in \mathcal{F}_{k,k}$. Then we set $f_i(x_1, \ldots, x_n) = g_i(x_1, \ldots, x_k)$ for $i = 1, \ldots, k$ and $f_i(x_1, \ldots, x_n) = x_i \oplus h_i(x_1, \ldots, x_{i-1})$ for $i = k+1, \ldots, n$, where $h_i$ is any function essentially depending on exactly $k-1$ variables from $x_1, \ldots, x_{i-1}$. The method for constructing a function $F \in P_{n,k}$ is used in the case when $k|n$, i.e. $n = sk$ for some $s \in \mathbb{N}$. We construct $s$ functions $G_1, \ldots, G_s \in \mathcal{F}_{k,k}$, $G_i = \left(g_1^{(i)}, \ldots, g_k^{(i)}\right)$, $i = 1, \ldots, s$, and set $f_{tk+i}(x_1, \ldots, x_n) = g_i^{(t+1)}(x_{tk+1}, \ldots, x_{(t+1)k})$, $t = 0, \ldots, s-1$, $i = 1, \ldots, k$. Mixing properties of such function are discussed, an algorithm for calculating elementary exponents is given.

**Keywords:** *essential dependence of a function on a variable, mixing properties of the function, elementary exponent.*

*Kolomeec N. A.* **PROPERTIES OF BENT FUNCTIONS CONSTRUCTED BY A GIVEN BENT FUNCTION USING SUBSPACES.** Properties of a construction $f \oplus \mathrm{Ind}_L$, where $f$ is a bent function in $2k$ variables and $L$ is an affine subspace, generating bent functions under some conditions are considered. It is proven that the numbers of bent functions generated by $(k+1)$-dimensional subspaces for a given bent function and its dual

function are equal. Some experimental results for bent functions in 6 and 8 variables reflecting the number of generated bent functions, equality and inequality of this number for a given bent function and its dual function and nonexistence of generated bent functions if subspaces have some fixed dimensions are presented. Theorem (2018) on subspace connections for bent functions $f$ and $f(x_1, \ldots, x_{2k}) \oplus x_{2k+1}x_{2k+2}$ (in context of the considered construction) is strengthened.

**Keywords:** *Boolean functions, bent functions, subspaces, affinity.*

*Kuzmina T. A.* **ABOUT THE CUBIC PART OF THE ALGEBRAIC NORMAL FORM OF ARBITRARY BENT FUNCTIONS.** Maximally nonlinear Boolean functions in $n$ variables, where $n$ is even, are called bent functions. The algebraic normal form (ANF) is one of the most useful ways for representing Boolean functions. What can we say about ANF of bent functions? Is it true that linear, quadratic, cubic, etc. parts of bent functions can be arbitrary? Cases with linear and quadratic parts were studied previously. In this paper, we prove that cubic part of ANF of a bent function can not be arbitrary if $n = 6, 8$.

**Keywords:** *Boolean function, bent function, linear function, quadratic function, cubic function, homogeneous function.*

*Kutsenko A. V.* **ISOMETRIC MAPPINGS OF THE SET OF ALL BOOLEAN FUNCTIONS INTO ITSELF WHICH PRESERVE SELF-DUALITY AND THE RAYLEIGH QUOTIENT.** In the paper, we study isometric mappings of the set of all Boolean functions in $n$ variables into itself which preserve self-duality and the Rayleigh quotient of Boolean function and generalize known results. It is proved that isometric mapping preserves self-duality if and only if it preserves anti-self-duality. The complete characterization of these mappings is obtained. Based on this result, the set of isometric mappings which preserve the Rayleigh quotient of a Boolean function is described. As a corollary, all isometric mappings which preserve bentness and the Hamming distance between bent function and its dual are given.

**Keywords:** *Boolean function, isometric mapping, self-dual bent function, Rayleigh quotient.*

*Metalnikova A. I., Pankratova I. A.* **CLASSES OF BOOLEAN FUNCTIONS WITH LIMITED COMPLEXITY.** The following classes of Boolean functions are considered: with given or limited number of essential variables, of given or limited degree, with given or limited ANF length, having non-repeated ANF. The numbers of functions in the classes and the affiliation tests are given. The algorithm for specifying of a partially defined function to a function of limited degree is presented.

**Keywords:** *essential dependence of a function on a variable, Boolean function degree, algebraic normal form.*

*Miloserdov A. V.* **ON THE RELATIONSHIP BETWEEN NONLINEAR AND DIFFERENTIAL PROPERTIES OF VECTORIAL BOOLEAN FUNCTIONS.** The relations between the linear approximation table (LAT) and the differences distribution table (DDT) of the vectorial Boolean functions are investigated. Let $F$ be a function from $\mathbb{F}_2^n$ into $\mathbb{F}_2^n$. DDT of $F$ is a $2^n \times 2^n$ table defined by $\mathrm{DDT}(a, b) = |\{x \in \mathbb{F}_2^n | F(x) \oplus F(x \oplus a) = b\}|$ for each $a, b \in \mathbb{F}_2^n$. LAT of $F$ is a $2^n \times 2^n$ table, in the cell $(v, u)$ of which the squared Walsh — Hadamard coefficient is stored. It is proved that the presence of coinciding rows in DDT and LAT is an invariant under affine equivalence as well as under EA-equivalence for normalized DDT and LAT. It is hypothesized that if all rows in the LAT (DDT) of a

vectorial Boolean function $F$ are pairwise different, then all rows in its DDT (LAT) are also pairwise different. This hypothesis is checked for functions in a small number of variables and for known APN functions in not more than 10 variables.
**Keywords:** *APN function, AB function, differential uniformity, nonlinearity.*

*Pankov K. N.* **RECURSION FORMULAS FOR THE NUMBER OF $(n, m, k)$-RESILIENT AND CORRELATION-IMMUNE BOOLEAN MAPPINGS.** For linear combinations of coordinate functions of mapping from the vectorspace $V_n$ of all binary vectors of length $n$ to the vectorspace $V_m$, recursive formulas for the distribution of weights of some their subfunctions $w_I^J$ and for the distribution of subsets of their spectral coefficients $\Delta_I^J$ are obtained. By mean of these formulas, we obtain the recursive formula for the number of correlation-immune of order $k$ mappings and the recursive formula for the number of $(n, m, k)$-resilient Boolean mappings.
**Keywords:** *weights of subfunctions, spectral coefficient, recursion formula, resilient vectorial Boolean function, correlation-immune function.*

*Pankratova I. A.* **ABOUT THE COMPONENTS OF SOME CLASSES OF INVERTIBLE VECTORIAL BOOLEAN FUNCTIONS.** In the class of invertible vectorial Boolean functions in $n$ variables with coordinate functions depending on all variables, we consider the subclasses $\mathcal{K}_n$ and $\mathcal{K}'_n$, the functions in which are obtained using $n$ independent transpositions, respectively, from the identity permutation and from the permutation, each coordinate function of which essentially depends on some one variable. It is shown that, for any $F = (f_1 \dots f_n) \in \mathcal{K}_n \cup \mathcal{K}'_n$ and $i = 1, \dots, n$, the coordinate function $f_i$ has a single linear variable, the component function $vF$ has no nonessential and linear variables for each vector $v \in \mathbb{F}_2^n$ weight of which is greater than 1, the nonlinearity, the degree, and the component algebraic immunity are 2, $n - 1$, and 2 respectively.
**Keywords:** *vectorial Boolean functions, invertible functions, nonlinearity, component algebraic immunity.*

*Cherednik I. V.* **LINEAR DECOMPOSITION OF DISCRETE FUNCTIONS IN TERMS OF SHIFT-COMPOSITION OPERATION.** We investigate the shift-composition operation of discrete functions that arises under shift register's homomorphisms. For an arbitrary function over a finite field, all right linear decompositions are described in terms of shift-composition. Moreover, we study the possibility for representing an arbitrary function by a shift-composition of three functions such that both external functions are linear. It is proved that in the case of a simple field, the concepts of reducibility and linear reducibility coincide for linear functions and quadratic functions that are linear in the external variable.
**Keywords:** *discrete functions, finite fields, shift register, shift-composition.*

*Shaporenko A. S.* **CONNECTIONS BETWEEN QUATERNARY AND BOOLEAN BENT FUNCTIONS.** This work is related to quaternary bent functions $f : \mathbb{Z}_4^n \to \mathbb{Z}_4$. The relation between Walsh — Hadamard transform coefficients of quaternary and two Boolean functions is explored. It is proved that any quaternary bent function is a regular bent function for any $n$. The number of quaternary bent functions in one and two variables is counted. For quaternary bent function in one variable $g(x + 2y) = a(x, y) + 2b(x, y)$, it is proved that $b$ and $a \oplus b$ are Boolean bent functions, where $x, y \in \mathbb{Z}_2$. Properties of Boolean functions $a, b$ and $a \oplus b$ in representation of quaternary bent function in two variables as $g(x + 2y) = a(x, y) + 2b(x, y)$ are described.
**Keywords:** *quaternary functions, Boolean functions, regular bent functions.*

*Hernández Piloto D. H.* **CLASS OF BOOLEAN FUNCTIONS CONSTRUCTED USING SIGNIFICANT BITS OF LINEAR RECURRENCES OVER THE RING $\mathbb{Z}_{2^n}$.** In this paper, we study a class of functions built with the help of significant bits sequences on the ring $\mathbb{Z}_{2^n}$. This class is built with the use of a function $\psi : \mathbb{Z}_{2^n} \to \mathbb{Z}_2$. In public literature, there are results for a linear function $\psi$. Here, we use a non-linear $\psi$ function for this set. The period of a polynomial $F$ in the ring $\mathbb{Z}_{2^n}$ is equal to $T(F \bmod 2)2^\alpha$, where $\alpha \in \{0, \ldots, n-1\}$. The polynomials for which $T(F) = T(F \bmod 2)$, i.e. $\alpha = 0$, are called marked polynomials. For our class, we use a marked polynomial of the maximum period. We show the bounds of the given class: non-linearity, the weight of the functions, the Hamming distance between functions. The Hamming distance between these functions and functions of other known classes is also given.
**Keywords:** *Boolean functions, linear recurrent sequences, significant bits sequences.*

*Gorodilova A. A.* **PROPERTIES OF ASSOCIATED BOOLEAN FUNCTIONS OF QUADRATIC APN FUNCTIONS.** For a vectorial Boolean function function $F : \mathbb{F}_2^n \to \mathbb{F}_2^n$, the associated Boolean function $\gamma_F$ in $2n$ variables is defined as follows: $\gamma_F(a, b) = = 1$ if $a \neq \mathbf{0}$ and the equation $F(x) + F(x + a) = b$ has solutions. In case when $F$ is a quadratic APN function, its associated function has the form $\gamma_F(a, b) = \Phi_F(a) \cdot b + \varphi_F(a) + 1$ for appropriate functions $\Phi_F : \mathbb{F}_2^n \to \mathbb{F}_2^n$ and $\varphi_F : \mathbb{F}_2^n \to \mathbb{F}_2$. In this paper, we show the following properties of functions $\Phi_F$ and $\varphi_F$: 1) if $n$ is odd, then $\Phi_F$ is a permutation; 2) if $n$ is even, then the preimage $\Phi_F$ of any nonzero vector together with the zero vector is a linear subspace of even dimension; 3) $\Phi_F$ takes an odd number of distinct nonzero values; 4) $\deg(\Phi_F) \leqslant n - 2$ for odd $n \geqslant 3$; 5) for even $n \geqslant 4$, each coordinate function of $\Phi_F$ is represented as $(\Phi_F)_i(x) = f_i(x) + \lambda_i\big(x_2 \ldots x_n + x_1 x_3 \ldots x_n + \ldots + x_1 x_2 \ldots x_{n-1} + x_1 \ldots x_n\big)$, where $\deg(f_i) \leqslant n - 2$ and $\lambda_i \in \mathbb{F}_2$; 6) $\deg(\varphi_F) = n$ for even $n$.
**Keywords:** *APN functions, associated Boolean functions, differential equivalence.*

## SECTION 3

*Avezova Ya. E.* **ON MIXING PROPERTIES OF NON-STATIONARY SHIFT REGISTER.** In this paper, we examine mixing properties of a non-stationary shift register, i.e., a binary non-linear $n$-stage shift register with feedback function depending on a binary sign of a control sequence. One of two register transformations is implemented at every clock cycle. We evaluate the minimal number $\gamma$ of register clock cycles after which the complete mixing is achieved, that is, each coordinate function of the transformation composition essentially depends on all variables. Mixing properties are rated by means of the set $\hat{\Gamma}$ of mixing $n$-vertex digraph with a common Hamiltonian cycle. An exponent bound allowing to estimate $\gamma$ from below is given for a primitive set $\hat{\Gamma}$. A computational experiment was carried out for $n = 6$ and 10 to calculate the exact value of $\gamma$, taking into account the control sequence. We have established that the complete mixing is possible in a number of cycles, which is less than double exponent. These results can be used for constructing cryptographic algorithms based on a composition of shift register transformations.
**Keywords:** *primitivity of digraphs set, exponent of digraph, exponent of digraphs set.*

*Agibalov G. P.* **CRYPTANALYTIC INVERTIBILITY WITH FINITE DELAY OF FINITE AUTOMATA.** This conference paper is a review of the author's paper from the journal PDM, 2019, no.44 where the cryptanalytical concept of the automaton invertibility with a finite delay $\tau$ is first introduced and where some first mathematical results related to this concept are presented. The notion of cryptanalytical automaton

invertibility means the theoretical possibility for recreating, under some limitations (so called clause), the prefix of a length $n$ in an unknown input sequence of an automaton, knowing its output sequence of the length $n + \tau$ and perhaps an additional information such as initial, intermediate or final state of the automaton and the suffix of a length $\tau$ in its input sequence. The limitations imposed on the recreating action may require for the initial state and for the suffix in the input sequence to be arbitrary or existent. As for prefix under recreating, it is not restricted and can be just arbitrary. So, the 208 different types of the automaton invertibility are defined at all. The early known types, (strong) invertibility and weak invertibility, are among them. Each type of the automaton invertibility with a fixed delay defines a class of all the finite automata invertible of this type. It is shown that the set of all these classes partially ordered by the inclusion relation is the union of twenty nine lattices. A constructive necessary condition for an automaton to be invertible of any invertibility type with a finite delay is established. In the case of universal invertibility type where initial state and input suffix are arbitrary, this condition is a constructive test of invertibility, that is, it is both necessary and sufficient condition for an automaton to be invertible of universal type.
**Keywords:** *finite-state automata, information-lossless automata, automaton invertibility, cryptanalytical invertibility.*

*Agievich S. V., Maslau A. S., Yarashenya Yu. S.* **ON PROBABILITIES OF DIFFERENTIAL TRAILS IN THE BASH-F SPONGE FUNCTION.** We propose two methods to obtain lower bounds on the weights of differential trails in the Bash-f sponge function. Our bounds restrict the probabilities of the trails from above and can be used to justify the security of cryptographic algorithms based on Bash-f against differential attacks. For the full 24-round trails, our best bound on the probabilities is $2^{-386}$.
**Keywords:** *sponge function, S-box, differential cryptanalysis, differential trail.*

*Borovkova I. V., Pankratova I. A.* **CRYPTANALYSIS OF THE ACBF ENCRYPTION SYSTEM.** The ACBF encryption system with a functional key is considered. A public key in the cryptosystem is a vectorial Boolean function $f$ in $n$ variables obtained by permutation and negation operations on variables and coordinate functions of a bijective vectorial Boolean function $g$, that is, $f(x) = \pi_2(g^{\sigma_2}(\pi_1(x^{\sigma_1})))$, $\pi_1, \pi_2 \in \mathbb{S}_n$ and $\sigma_1, \sigma_2 \in \mathbb{F}_2^n$ are key parameters. A private key is $f^{-1}$. For two subsets of key parameters, namely for $\{\pi_1\}$ and $\{\pi_1, \pi_2\}$, attacks with known plaintexts are proposed.
**Keywords:** *cryptosystem ACBF, vectorial Boolean functions, asymmetric cryptosystem, cryptanalysis.*

*Vedunova M. V., Ignatova A. O., Geut K. L.* **BLOCKING VARIETIES IN STEINER TRIPLES.** The problems of Steiner triples blocking applicable in the secret sharing scheme are considered. This paper describes a method for constructing a blocking set of minimum and maximum powers. For the complement blocking set, a method for estimating the minimum complement power in both linear and nonlinear Steiner triples systems is given. For the corresponding matroids, the ideal secret sharing schemes based on interpolation polynomials with zero trace are implemented. For the nonlinear Steiner triples system with 13 elements, the maximum and minimum cardinalities of the complement of the blocking set are found.
**Keywords:** *system of Steiner triples, blocking sets, secret sharing scheme.*

*Gribanova I. A., Semenov A. A.* **ON THE ARGUMENT OF THE ABSENCE OF PROPERTIES OF A RANDOM ORACLE FOR SOME CRYPTOGRAPHIC**

**HASH FUNCTIONS.** The paper presents new preimage attacks related to the class of algebraic attacks on hash functions MD4-$k$, $39 \leqslant k \leqslant 48$. Hash function MD4-$k$ consists of first $k$ steps used in MD4 algorithm. To solve the corresponding systems of algebraic equations, SAT-solvers are used. The proposed attacks demonstrate that MD4-$k$ functions are not random oracles. More precisely, we estimate the fraction of easy-invertible outputs of these functions and show that even for full-round version of hash function MD4, the obtained fraction is very big. To construct such estimations with each function of the kind MD4-$k$, we associate a special function, which input length is much smaller than 512. In most cases the preimage finding problem for such function is significantly simpler than the original one. We show that any value of the special function is the value of function MD4-$k$ and estimate the fraction of these values in $\{0,1\}^{128}$. This approach allows us to obtain an estimation for the fraction of easy-invertible outputs of original hash function MD4-$k$.

**Keywords:** *cryptographic hash functions, preimage attack on hash functions, MD4, MD4-39, SAT.*

*Davletshina A. M.* **SEARCH FOR EQUIVALENT KEYS OF THE MCELIECE — SIDELNIKOV CRYPTOSYSTEM BUILT ON THE REED — MULLER BINARY CODES.** A new method is proposed for recovering equivalent secret keys of the McEliece — Sidelnikov cryptosystem built on the Reed — Muller binary codes. It is proved that using the superposition of Schur product and taking the orthogonal code we can obtain from the code with generating matrix $(R||HR)$ the code belonging to the Cartesian product of codes $\mathrm{RM}(m - r\,(\lceil m/r \rceil - 1) - 1, m) \times \mathrm{RM}(m - r(\lceil m/r \rceil - 1) - 1, m)$. Here, $R$ is the generating matrix of the Reed — Muller code of order $r$ and length $2^m$. Thus, proposed method reduces the problem of recovering equivalent secret keys of the McEliece — Sidelnikov cryptosystem to two problems of finding the equivalent secret key of the McEliece cryptosystem. It is proved that the offered algorithm works in a polynomial time. Numerical experiments confirm the theoretical results.

**Keywords:** *McEliece — Sidelnikov cryptosystem, Reed — Muller code, polynomial attack.*

*Komissarov S. M.* **ON ALGORITHMIC IMPLEMENTATION OF 16-BIT S-BOXES WITH ARX AND BUTTERFLY STRUCTURES.** Implementations of nonlinear mappings of vector space $V_n$ (s-boxes $n \times n$) as lookup-tables are memory intensive. It requires $n2^n$ bits to store $n$-bit s-box. That is why the existing block ciphers use s-boxes of relatively small size (8×8 bit — AES, Kuznyechik, 6×4 bit — DES). New constructions of 16-bit algorithmically implementable s-boxes with improved performance and cryptographic properties (in comparison with the existing methods) are proposed. The first method is based on ARX (Add-Rotate-XOR) structure, using low-cost computations in software and hardware. The second method is based on butterfly structure, using 8-bit precomputed s-boxes to build 16×16 ones. Maximum expected differential probability, maximum expected linear probability and minimum nonlinear order over all linear combinations of the components of proposed s-boxes with ARX structure are $18/2^{16}$, $764/2^{15}$ and 15, respectively and of suggested s-boxes with Butterfly structure are $10/2^{16}$, $512/2^{15}$ and 15, respectively. It is established that the use of the proposed 16-bit s-boxes in the round substitutions of AES and Kuznyechik block ciphers significantly lowers the upper bounds of differential and linear probabilities for two and four rounds of these algorithms.

**Keywords:** *16-bit s-box, algorithmic implementation of s-boxes, ARX, Butterfly, maximum differential probability, maximum linear probability, nonlinear order.*

*Koreneva A. M.* **EVALUATION OF MIXING CHARACTERISTICS FOR MERKLE — DAMGARD HASH FUNCTIONS.** The matrix-graph approach (MGA), which has been successfully applied to the evaluation of iterative block ciphers and key generators, is presented for the first time as a tool for estimating the mixing properties of hash algorithms. Feature of MGA application to hash functions is connected with the possibility of construction the mixing matrices which characterize dependence of the bits of the hash value on the bits of the input message. Mixing matrices of the order $512 + n$ are constructed for hash functions MD4, MD5, SHA-1, SHA-256, where $n$ is the size of the digest produced by the compression function processing the 512-bit block of the input message ($n = 128$ for MD4 and MD5, $n = 160$ for SHA-1 and $n = 256$ for SHA-256). We calculate the local exponents of mixing matrices, i.e., for each matrix $M$, we obtain the smallest positive integer $\gamma$ such that for any natural $\tau \geqslant \gamma$ all the columns of $M^\tau$ with the numbers $513, 514, \ldots, 512 + n$ are positive. The values of the local exponents are the lower bounds for the number of iterations, after which each bit of the output hash may essentially depend on all bits of the input message. The obtained values ($\gamma = 21$ for MD4, MD5, SHA-256 and $\gamma = 23$ for SHA-1) indirectly indicate the similar mixing properties of the considered hash algorithms despite the increase of block length and complexity of the compression function.

**Keywords:** *hash functions, Merkle — Damgard structure, matrix-graph approach, mixing properties.*

*Medvedev N. V., Titov S. S.* **HOMOGENEOUS MATROIDS AND BLOCK-SCHEMES.** This paper concerns the homogeneous matroids in which all the cycles have the same power. The research is related to the problem of describing homogeneous matroids corresponding to ideal homogeneous secret sharing schemes. A possibility for representing the family of cohyperplanes of a homogeneous matroid like blocks of blocks-schemes including the Steiner triple systems is shown. It is proved that a separating matroid is a homogeneous matroid with three-element cohyperplanes, if and only if its cohyperplanes form Steiner triple systems.

**Keywords:** *secret sharing schemes, homogeneous matroids, block-schemes, cycles, Steiner triple systems.*

*Medvedeva N. V., Titov S. S.* **GEOMETRIC MODEL OF PERFECT CIPHERS WITH THREE CIPHER PLAINTEXT VALUES.** In this work we deal with the problem of describing Shannon perfect ciphers (which are absolutely immune against the attack on ciphertext, according to Shannon) when cardinality of alphabet of cipher plaintext values is equal to three. It is shown that there is no minimum by inclusion perfect ciphers with five or six encryption keys. The number of minimum by inclusion perfect ciphers with seven and eight keys are determined. Examples of minimal ciphers with respect to inclusion are built.

**Keywords:** *perfect ciphers, endomorphic ciphers, non-endomorphic ciphers.*

*Roman'kov V. A.* **EFFICIENT METHODS OF ALGEBRAIC CRYPTANALYSIS AND PROTECTION AGAINST THEM.** The paper contains the basic information about methods of cryptanalysis used in algebraic cryptography. Main elements of linear and non-linear decomposition attacks by the author and so-called span-method by B. Tsaban are described as well as the examples of using them. To protect existing cryptographic algorithms against the cryptanalytic attacks, some improvements of this algorithms are proposed. For this purpose, the author has introduced the concept of a marginal set and with the use of it has protected the widely known key distibution protocol AAG against

the attack by the span-method.
**Keywords:** *algebraic cryptography, algebraic cryptanalysis.*

*Sapegina M. D.* **NONLINEARITY CHARACTERISTICS ESTIMATIONS FOR FUNCTION COMPOSITIONS OVER VECTOR SPACES BY THE MATRIX-GRAPH APPROACH.** We expand the matrix-graph approach developed by V. M. Fomichev to assessing the nonlinearity characteristics of vector space transformations using ternary matrices over the multiplicative semigroup {0,1,2} or digraphs with arcs labeled with the numbers from the set {0,1,2}. A digraph $\Gamma$ with the set of vertices $\{1,\dots,n\}$ is said to be $\langle 2\rangle$-primitive if, for some natural $t$ for any $i,j\in\{1,\dots,n\}$, there is a path from $i$ to $j$ of length $t$ that passes through the arc labeled "2". The smallest such $t$ is called the $\langle 2\rangle$-exponent of the digraph $\Gamma$ and is denoted by $\langle 2\rangle$-$\exp\Gamma$. A transformation $g(x_1,\dots,x_n)$ of the vector space $V_n$ with coordinate functions $g_1(x_1,\dots,x_n),\dots,g_n(x_1,\dots,x_n)$ corresponds to the $n$-vertex digraph $\Gamma_\Theta(g)$, in which an arc $(i,j)$ is marked with the number 0, or 1, or 2 if $g_j(x_1,\dots,x_n)$ depends on $x_i$ fictitiously, or linearly, or nonlinearly respectively, $1\leqslant i,j\leqslant n$. The transformation $g(x_1,\dots,x_n)$ is called totally nonlinear if the label of each arc of the digraph is "2". The transformation $g(x_1,\dots,x_n)$ is called $\langle 2\rangle$-perfective if, for some natural $t$, all arcs of the digraph $\Gamma_\Theta(g^t)$ are marked with the number 2. The smallest such $t$ is called an total nonlinearity index of the transformation $g(x_1,\dots,x_n)$ and is denoted by $\langle 2\rangle$-$nlg$. It is proved that if in the labeled primitive digraph $\Gamma$ the label of each simple contour contains the number 2 and $\exp\Gamma=n$, then the digraph $\Gamma$ is $\langle 2\rangle$-primitive and $\langle 2\rangle$-$\exp\Gamma=\exp\Gamma$. An estimate of the $\langle 2\rangle$-exponent of the round function nonlinearity matrix $M$ of order $2n$ of block algorithms based on the Feistel network is obtained using the $\langle 2\rangle$-exponent of the complication function nonlinearity matrix $\Phi$ of order $n$: $\langle 2\rangle$-$\exp M\leqslant\langle 2\rangle$-$\exp\Phi+2$. These results decrease the complexity of calculating the total nonlinearity index for some transformations $g$. Algorithms for recognition of the total nonlinearity of the transformation $g(x_1,\dots,x_n)$ and estimates of $\langle 2\rangle$-$nlg$ index are presented. For random transformations, the average complexity (number of elementary operations) does not exceed $2\gamma(\gamma+1)\log 8n$ where $\langle 2\rangle$-$nlg=\gamma$ and the elementary operation is the computation of any function on any input set. The algorithm was applied to obtain exact values of $\langle 2\rangle$-$nlg$ of round substitutions $g$ of the algorithms DES and Magma, the values 5 and 6, respectively, were obtained.
**Keywords:** *nonlinearity matrix of function, $\langle 2\rangle$-primitive matrix (digraph), $\langle 2\rangle$-exponent of the matrix (digraph), total nonlinearity index.*

*Semenov A. A., Antonov K. V., Otpuschennikov I. V.* **SEARCH FOR LINEARIZING SETS IN ALGEBRAIC CRYPTANALYSIS AS A PROBLEM OF PSEUDO-BOOLEAN OPTIMIZATION.** The paper introduces the concept of linearizing sets that can be considered as a generalization of known linearization sets. Linearization sets are used in algebraic attacks related to the class of guess-and-determine attacks. The idea of such attacks is to guess values of variables from a certain set and then to substitute them into a system of algebraic equations that connects the input and output data of the cipher under consideration. In some cases, the result of such procedure is a linear system that can be solved effectively. In the present paper, we consider algebraic equations over the field GF(2). The values of variables from the linearizing set (as opposed to the linearization set) linearize the system of equations with a certain probability, which, generally speaking, can be substantially less than 1. The complexity estimation for guess-and-determine attack based on a particular linearizing set is constructed using a specially defined pseudo-Boolean function. The minimum value of this function gives a complexity estimation for the attack

with best efficiency. To minimize such functions, a metaheuristic algorithm from the class of tabu search algorithms is used. At the current stage, attacks of the described type are built for some cryptographic generators. In particular, for the well-known A5/1 generator, the presented method allows to construct a guess-and-determine attack which complexity is 4.5 times lower than the complexity of Anderson's attack.
**Keywords:** *guess-and-determine attacks, linearizing sets, pseudo-Boolean optimization.*

*Fomin D. D., Trifonov D. I.* **HARDWARE IMPLEMENTATION OF ONE CLASS OF 8-BIT PERMUTATIONS.** The paper studies the issues of implementation of one class of S-Boxes on FPGA and ASIC and compares them with the implementation of arbitrary mappings $V_8 \to V_8$. The way of implementation of arbitrary S-Box is studied. It's shown that any S-Box over $V_8$ can be implemented using 40 LUTs (812 GE). For one class of S-Boxes over $V_8$ with high cryptographic properties, the possibility of their implementation using 19 LUTs (147 GE) is shown.
**Keywords:** *S-Box, permutation, FPGA, ASIC.*

*Fomichev V. M., Koreneva A. M., Tulebaev A. I.* **ON THE PARAMETERS OF 2-GOST ROUND KEY GENERATOR.** Information security with low resources determines the importance of construction lightweight implementations for known cryptographic algorithms. In 2014, a low-resource implementation of GOST 28147-89 called 2-GOST was presented. Despite attained advantages, the scheme had yet a potential to enhance cryptographic strength by, for example, modifying the key schedule. In 2018, a new algorithm for the generation of round keys for 2-GOST was proposed. The round key generator was based on the shift register of length 8 over the set of binary vectors of length 32. At the same time, the register feedback parameters were not sufficiently substantiated. The aim of this paper is to determine the best (or close to the best) three feedback taps for feedback function and justification of the proposed solution. The first quality criterion is defined by the characteristics of the input data mixing by the register transformation, the second one — by the efficiency of the implementation. As a characteristic of mixing, we use the index of local perfection of register transformation, namely the number of iterations, after which each bit of the generated round key depends essentially on all bits of the initial state. The optimal three feedback taps are identified and the characteristics of the key schedule quality for the proposed and original schemes are compared. It is established that in the initial scheme the value of the local perfection index is the highest among all the feedback functions in the class under the study (the worst index in terms of mixing). We offer the alternative scheme with the smallest index of local perfection and the similar implementation. For both schemes (original and alternative), we carry out the statistical testing of the generator output sequences.
**Keywords:** *2-GOST, local perfection, matrix-graph approach, mixing properties, round key generator, shift register.*

*Khairullin I. I.* **ON MIXING PROPERTIES OF MODIFIED MULTIDIMENSIONAL LINEAR GENERATORS.** A new class of shift registers of length $n$ with $r$-bit cells, $n, r > 1$, called modified multidimensional linear generators (MMLG) is described. An experimental study of the mixing properties of shift registers of length 8 over $V_{32}$ from the MMLG class is carried out. The feedback function of these registers is based on the round transformation of the lightweight block cipher SPECK. For such MMLG with different sets of pickup points $D \subseteq \{0, \ldots, 7\}$, the local (0,256)-exponents of mixing matrices $M$ are calculated as the smallest positive integer $\gamma$ such that, for any natural $t \geqslant \gamma$, all the columns of the matrix $M^t$ with numbers 1, ..., 32 are positive. The 0-indexes of perfec-

tion are calculated as the smallest values of the degrees of the register transformations, for which each coordinate functions of output cell essentially depends on all input variables. For MMLG with pickup points with numbers 0 and 7, the values of the local exponent and the local index of perfection are equal to 17. The obtained values are compared with the local exponents and local indexes of perfection for structurally similar schemes based on modified additive generators (MAG). The comparison shows that the generators have similar mixing properties. However, unlike the considered class of shift registers based on MAG, the MMLG class is interesting for usage in conditions of limited resources.
**Keywords:** *modified multidimensional linear generator, mixing properties, matrix-graph approach, mixing matrix, index of perfection, shift register, exponent, SPECK.*

*De la Cruz Jiménez R. A.* **A METHOD FOR CONSTRUCTING PERMUTATIONS, INVOLUTIONS AND ORTHOMORPHISMS WITH STRONG CRYPTOGRAPHIC PROPERTIES.** S-Boxes are crucial components in the design of many symmetric ciphers. To construct permutations having strong cryptographic properties is not a trivial task. In this work, we propose a new scheme based on the well-known Lai — Massey structure for generating permutations of dimension $n = 2k$, $k \geqslant 2$. The main cores of our constructions are: the inversion in $\mathrm{GF}(2^k)$, an arbitrary $k$-bit non-bijective function (which has no pre-image for 0) and any $k$-bit permutation. Combining these components with the finite field multiplication, we provide new 8-bit permutations without fixed points possessing a very good combination for nonlinearity, differential uniformity and minimum degree — (104; 6; 7) which can be described by a system of polynomial equations with degree 3. Also, we show that our approach can be used for constructing involutions and orthomorphisms with strong cryptographic properties.
**Keywords:** *S-Box, permutation, Boolean functions.*

*Rodriguez Aulet R.* **SOME PROPERTIES OF THE OUTPUT SEQUENCES OF COMBINED GENERATOR OVER FINITE FIELDS.** The sequences are an important part of the cryptography and analysis of their properties is of great interest. In this paper, the following characteristics of combined generator are analyzed: period of output sequences and the distribution of elements in the output sequences over finite field.
**Keywords:** *finite field, correlation-immune function, resilient function, balanced function, combined generator.*

*Roman'kov V. A.* **DISCRETE LOGARITHM FOR NILPOTENT GROUPS AND CRYPTANALYSIS OF POLYLINEAR CRYPTOGRAPHIC SYSTEM.** We present an efficient algorithm to compute a discrete logarithm in a finite nilpotent group, or more generally, in a finitely generated nilpotent group. Special cases of a finite $p$-group ($p$ is a prime) and a finitely generated torsion free nilpotent group are considered. Then we show how the derived algorithm can be generalized to an arbitrary finite or finitely generated nilpotent group respectively. We suppose that group is presented by generating elements and defining relators or like a subgroup of a triangular matrix group over a prime finite field (in finite case) or over the ring of integers (in torsion-free case). On the base of the derived algorithm we give a cryptanalysis of some schemes of polylinear cryptography known in the literature.
**Keywords:** *discrete logarithm, nilpotent group, polylinear system, cryptanalysis.*

**SECTION 4**

*Devyanin P. N.* **ABOUT MODELING OF MIC AND MAC IN PostgreSQL WITHIN FRAMEWORK OF THE MROSL DP-MODEL.** It is an urgent task to use complex software programs in the OS Astra Linux. Especially when these software programs implement their own access control. Firstly, an appropriate technical implementation is required for interfacing access control in software with OS Astra Linux mandatory integrity control (MIC) and mandatory access control (MAC). Secondly, it is important to ensure confidence in the security of such combination of access control of software programs and the OS Astra Linux. This is also necessary to ensure the safety of informational flows by memory or by time. The important example of such regular of the OS Astra Linux software program is PostgreSQL with initially implemented role-based access control (RBAC). Recently, certification of the OS Astra Linux was held on demand of the protection profile of general-purpose OS of the first (highest) protection class. The mandatory entity-role DP-model (MROSL DP-model) was developed and was verified in the course of the certification. This model is the scientific basis for the development of OS Astra Linux access control. This says about the feasibility of preparing to meet similar requirements with respect to PostgreSQL. In this regard, the results of the completion of the formation MIC, MAC and RBAC for PostgreSQL within framework of hierarchical representation of the MROSL DP-model are considered in the article. It is said about introducing changes in the levels for the OS Astra Linux and also about additions to sufficient conditions of security of access control.
**Keywords:** *computer security, formal model, access control, PostgreSQL.*

*Eliseev V. L.* **ARTIFICIAL NEURAL NETWORKS AS A MECHANISM FOR OBFUSCATION OF COMPUTATIONS.** The subject of the paper is the possibility of using artificial neural networks as a mechanism for strongly obfuscating computations. The problem of the obfuscation and the main ideas and methods for solving this problem are discussed. The concept of a neural network obfuscator is introduced and its properties are proved. The advantages and disadvantages of the proposed approach are discussed.
**Keywords:** *artificial neural network, obfuscation.*

*Semibratov I. V., Fomichev V. M.* **EVALUATION OF THE PROBABILITY OF A SUCCESSFUL ATTACK IN BLOCKCHAIN NETWORK.** A probabilistic model, describing the beginning of active periods for an attacker and a miner as a random values with binomial distribution, is presented. Creating a false information block is meant by a successful attack. Estimates for the probability of intruder's successful attack under different conditions are obtained. Results of calculation confirm that attacker's probability of a successful attack decreases with the increase of positive difference between the attacker's and miner's session durations as well as with the growth of the number of active miners. Also, the probability of a successful attack increases with the growth of the positive difference between the expected start time of the miner's session and the start time of the attacker's session.
**Keywords:** *blockchain, miner, consensus mechanism, hash function, binomial probability distribution.*

**SECTION 5**

*Abrosimov M. B., Razumovsky P. V.* **ABOUT NON-ISOMORPHIC GRAPH COLOURING GENERATING BY READ — FARADZHEV METHOD.** We consider

the problem of generating all the non-isomorphic vertex $k$-colourings of a graph. The main point is to provide an algorithm for solving the problem without isomorphism testing technique proposed in Read — Faradzhev method. The algorithm is based on the backtracking method. Each iteration calculates the set of orbits for a given colouring, selects one representative from each orbit, and each representative is coloured in all colors in a selected way. From the set of colourings thus obtained, not canonical are cut off. The generation proceeds until canonical colourings remain.

**Keywords:** *graph colouring, graph isomorphism, isomorphism rejection.*

*Zharkova A. V.* **ON INDICES OF STATES IN FINITE DYNAMIC SYSTEMS OF COMPLETE GRAPHS ORIENTATIONS.** Finite dynamic systems of complete graphs orientations are considered. The states of such a system $(\Gamma_{K_n}, \alpha)$, $n > 1$, are all possible orientations of a given complete graph $K_n$, and evolutionary function $\alpha$ transforms a given state (tournament) $G$ by reversing all arcs in $G$ that enter into sinks, and there are no other differences between the given $G$ and the next $\alpha(G)$ states. In this paper, the algorithm for calculating indices of states in finite dynamic systems of complete graphs orientations is proposed. Namely, in the considered system $(\Gamma_{K_n}, \alpha)$, $n > 1$, the index of the state $G \in \Gamma_{K_n}$ is 0 if and only if it hasn't a sink or its indegrees vector $(d^-(v_1), d^-(v_2), \ldots, d^-(v_n))$ is a permutation of numbers $\{0, 1, \ldots, n-1\}$. If these conditions for this state $G$ are not met, then its index is $f$, where $f$ is the power of the largest set of the form $\{n-1, n-2, \ldots, n-f\} \subseteq \{d^-(v_1), d^-(v_2), \ldots, d^-(v_n)\}$. The maximal index of the states in the system is found: it is equal to 0 for $n = 2$ and $n - 3$ for $n > 2$. The corresponding table is given for the finite dynamic systems of orientations of complete graphs with the number of vertices from 2 to 7.

**Keywords:** *complete graph, evolutionary function, finite dynamic system, graph, graph orientation, index, tournament.*

*Kamil I. A. K., Sudani H. H. K., Lobov A. A., Abrosimov M. B.* **ON THE GENERATION OF MINIMAL GRAPH EXTENSIONS BY THE METHOD OF CANONICAL REPRESENTATIVES.** A graph $G^*$ is a $k$-vertex (edge) extension of a graph $G$ if every graph obtained by removing any $k$ vertices (edges) from $G^*$ contains $G$. A $k$-vertex (edge) extension $G^*$ of graph $G$ is said to be minimal if it contains minimum possible vertices and has the minimum number of edges among all $k$-vertex (edge) extension of graph $G$. The paper proposes an algorithm for generating all non-isomorphic minimal vertex (edge) $k$-extensions of a given graph with isomorphism rejection technique by using method of generating canonical representatives.

**Keywords:** *fault tolerance, graph extension, isomorphism, canonical code, generating canonical representatives*

*Los I. V., Abrosimov M. B.* **ABOUT A CRITERION OF EQUALITY TO 3 FOR EXPONENT OF REGULAR PRIMITIVE GRAPH.** This paper presents some results related to finding criterion of equality to 3 for the exponent of regular primitive graph. Several necessary and several sufficient conditions are found. We show that no one of them could be criterion. For that purpose, we have also run a computation experiment for counting the number of primitive regular graphs with the exponent 3, that don't satisfied those conditions. As for a graph of the diameter 2, the following criterion is found for it: graph with diameter 2 is primitive with exponent 3 iff each vertex in that graph lies on at least one cycle of length 3 and there is at least one edge that does not lie on cycles with length 3.

**Keywords:** *primitive graph, regular graph, graph exponent.*

*Soldatenko A. A.* **APPROXIMATE ALGORITHM FOR SEARCHING SHORTEST PATH IN MULTISERVICE NETWORK WITH CONSTRAINED RESOURCE.** In the paper, we consider the Resource Constrained Shortest Path problem (RCSP). This problem is NP-hard extension of a well-known shortest path problem in the directed graph $G = (V, E)$. In the RCSP problem each arc $e$ from $E$ has a cost $w(e)$ and additional weight functions $r_i(e)$, $i = 1, \ldots, k$, which specifying its requirements from a finite set of resource. The RCSP problem has various practical applications, including design and operation of multi-service network. Nowadays, multi-service networks grow at a rapid pace. Therefore, it is relevant to search for a new approximation algorithms that can solve the RCSP problem quickly. This paper reviews existing approximation algorithms for the RCSP problem. A polynomial time $\varepsilon$-approximation algorithm RevTree based on node labeling method is presented in the paper. The main advantage of the RevTree algorithm over existing ones is its ability to produce $\varepsilon$ approximation of the RCSP problem in $\mathcal{O}(|V|^2)$ time. For real networks, $\varepsilon$ can be calculate using values of $w(e)$ and $r_i(e)$, $e \in E$. The paper provides a description of the RevTree algorithm and results of computational experiments, which justify the effectiveness of proposed algorithm.
**Keywords:** *resource constrained shortest path, graph-based algorithm, optimal routing, computer and multi-service networks.*

*Trenkaev V. N.* **RECONFIGURABLE FINITE STATE MACHINES BASED ON SUBSTITUTIONS.** A structure of reconfigurable finite state machine (FSM) is proposed for using as a ciphering automata. The reconfigurable FSM consists of the following parts: basic substitutions, key substitutions, couple multiplexers and the state register. The input and output alphabets coincide with the set of states. All basic substitutions are different. The number of them equals the number of states. There are three modifiable (programmable) key substitutions. Reconfiguration or FSM consists in constructing the certain output and transition functions from substitutions. It is shown that any fixing of key substitutions produces strongly connected reduced and invertible FSM.
**Keywords:** *reconfigurable finite state machine, invertible finite state machine, automata cipher.*

## SECTION 6

*Kishkan V. V., Safonov K. V.* **SYNTACTICAL ANALYSIS OF MONOMIALS IN CONTEXT-FREE LANGUAGES TAKING INTO ACCOUNT THE PRODUCTIONS APPLICATION ORDER.** The problem of syntactical analysis under consideration is the development of a deadlock algorithm to determine whether it is possible to obtain a monomial from the initial symbol using the productions of a given context-free language, to find out which productions and how many times are used to derive this monomial and also to establish, if possible, the order of using these productions. We propose a method of monomial labels which allows to establish the order of productions application.
**Keywords:** *syntactical analysis of monomials, context-free languages, monomial labels.*

*Kolbasina I. V., Safonov K. V.* **A SOLVABILITY CONDITION FOR ARBITRARY FORMAL GRAMMARS.** In the paper, approaches to solving the systems of non-commutative polynomial equations in the form of formal power series (FPS) based on the connection with the corresponding commutative equations are developed. Every FPS is mapped to its commutative image — power series, which is obtained under the assumption that the symbols denote commutative variables assigned as values in the field of complex

numbers. The consistency of the system of noncommutative polynomial equations, which is not directly connected with the consistency of its commutative image, is investigated. However, the analogue of implicit mapping theorem to arbitrary formal grammars (noncommutative systems) is obtained, namely if the rank of Jacoby matrix for the commutative image of a system of equations is maximal, then the initial noncommutative system of equations has a unique solution in the form of FPS.
**Keywords:** *systems of polynomial equations, non-commutative variables, formal power series, commutative image, Jacobian.*

*Rybalov A. N.* **ON THE GENERIC COMPLEXITY OF THE DECODING PROBLEM FOR LINEAR CODES.** Generic-case approach to algorithmic problems was introduced by Miasnikov, Kapovich, Schupp and Shpilrain in 2003. This approach studies behavior of an algorithm on typical (almost all) inputs and ignores the rest of inputs. Many classical undecidable or hard algorithmic problems become feasible in the generic case. But there are generically hard problems. In this paper, we consider generic complexity of the decoding problem for linear codes over finite fields. We fit this problem in the frameworks of generic complexity and prove that its natural subproblem is generically hard provided that this problem is hard in the worst case.
**Keywords:** *generic complexity, linear codes, McEliece cryptosystem.*

## SECTION 7

*Vlasova V. V., Pudovkina M. A.* **ON PROPERTIES OF THE LARGEST PROBABILITY FOR DIFFERENCE TRANSITION UNDER A RANDOM BIJECTIVE GROUP MAPPING.** We consider two finite groups $(G_1, \otimes)$, $(G_2, \odot)$ with binary operations $\otimes$, $\odot$. In practice, $G_1$ and $G_2$ are usually equal to the additive group $(V_m, \oplus)$ of the $m$-dimensional vector space $V_m$ over GF(2) or the additive group $(\mathbb{Z}_{2^m}, \boxplus)$ of the residues ring $\mathbb{Z}_{2^m}$. Nonabelian group of order $2^m$ having a cyclic subgroup of index 2 can be considered as the nearest one to the additive group $(\mathbb{Z}_{2^m}, \boxplus)$. These groups are the dihedral group $(D_{2^{(m-1)}}, \diamond)$ and the generalized quaternion group $(Q_{2^m}, \boxtimes)$. In differential technique and its generalizations, each bijective mapping is associated with the differences table. In this paper, for all $\otimes, \odot \in \{\oplus, \boxplus, \boxtimes, \diamond\}$, we experimentally study a random value $q^{(\otimes,\odot)}$ that is equal to $|G_1|p^{(\otimes,\odot)}$, where $p^{(\otimes,\odot)}$ is the largest element of the differences table corresponding to a random mapping $s : G_1 \to G_2$. We consider randomly chosen bijective mappings as well as real S-boxes. As for all $\otimes, \odot \in \{\oplus, \boxplus, \boxtimes, \diamond\}$, we compute $q^{(\otimes,\odot)}$ for $S$-boxes of ciphers Aes, Anubis, Belt, Crypton, Fantomas, iScream, Kalyna, Khazad, Kuznyechik, Picaro, Safer, Scream, Zorro, Gift, Panda, Pride, Prince, Prost, Klein, Noekeon, Piccolo.
**Keywords:** *differences table, differentially d-uniform mapping, S-boxes, generalized quaternion group, dihedral group.*

*Jenevsky S. V., Melnikov S. L., Shurupov A. N.* **ON THE RECOGNITION PROBLEM FOR ALGEBRAIC THRESHOLD FUNCTIONS.** We prove the existence of recognition algorithm for algebraic Boolean threshold functions by calculating upper bounds of absolute values of modulo and coefficients of a linear form. The modulo bound looks like $(n+3)^{(n+5)/2}/2^{n+2}$ and the bound of algorithm complexity is $\mathrm{O}((n/2)^{n^2})$.
**Keywords:** *recognition problem, algebraic threshold functions.*

*Coy Puente O.* **CONSTRUCTION METHODS FOR MDS MATRICES USING COMPANION AND PERMUTATION MATRICES FOR LIGHTWEIGHT CRYPTOGRAPHY.** In this work, we propose a new construction method of MDS-

matrices of dimension $k = 4, 6$ by means of summation of a power $r$ of the companion matrix of a certain polynomial and a fixed permutation matrix over the finite field $\mathrm{GF}(2^8)$. The method is represented by the expression $S_f^r + P$ for a polynomial $f(x) = x^k + f_{k-1}x^{k-1} + \ldots + f_1 x + f_0$, where $S_f$ is the companion matrix of the polynomial $f(x)$, $P$ is a permutation matrix, $r = 3k/2$, and the coefficients $f_i \in \{0, 1, \alpha, \alpha^{-1}, \alpha^2, \alpha^3\}$. For its effective implementation, it is proposed to apply $S_f$ as a linear feedback shift register with characteristic polynomial $f(x)$ and $P$ as a Feistel network with $k$ entrances. The XOR-count metric is used to show the effectiveness of the proposed method in algorithms that require low implementation cost.

**Keywords:** *MDS-matrices, companion matrices, permutation matrices, LFSR, finite field, lightweight cryptography, XOR-count.*

*Kuznetsov A. A.* **COMPUTATIONAL EXPERIMENTS IN FINITE TWO GENERATOR BURNSIDE GROUPS OF EXPONENT FIVE.** Let $B_0(2, 5) = \langle a_1, a_2 \rangle$ be the largest two generator Burnside group of exponent five. It has the order $5^{34}$. There is a power commutator presentation of $B_0(2, 5)$. In this case every element of the group can be represented uniquely as $a_1^{\alpha_1} \cdot a_2^{\alpha_2} \cdot \ldots \cdot a_{34}^{\alpha_{34}}$, $\alpha_i \in \mathbb{Z}_5$, $i = 1, 2, \ldots, 34$. Here $a_1$ and $a_2$ are generators of $B_0(2, 5)$, commutators $a_3, \ldots, a_{34}$ are defined recursively by $a_1$ and $a_2$. We define $B_k = B_0(2, 5)/\langle a_{k+1}, \ldots, a_{34} \rangle$ as a quotient of $B_0(2, 5)$, $|B_k| = 5^k$. Let $\varphi$ be the homomorphism of $B_k$ onto the group $Q_k$ and $N_k$ be the kernel of $\varphi$. We have done some computational experiments and now formulate a hypothesis about the diameter $D_{A_4}(B_k)$ of the $B_k$ relative to the symmetric generating set $A_4 = \{a_1, a_1^{-1}, a_2, a_2^{-1}\}$: $D_{A_4}(eN_k) = D_{A_4}(B_k)$ for all $2 \leqslant k \leqslant 34$ where $|N_k| \sim |Q_k| \sim |B_k|^{1/2}$, $e$ is the identity of $B_k$ and $D_{A_4}(eN_k)$ is the diameter of the coset $eN_k$. Note that this hypothesis is correct for $k \leqslant 19$.

**Keywords:** *Burnside group, the growth function.*

*Manyaev G. O., Shurupov A. N.* **ON EFFECTIVENESS OF SOLVING PSEUDO-BOOLEAN SYSTEMS OF LINEAR INEQUALITIES BY SIMULATED ANNEALING, BALAS ALGORITHM AND INTERIOR POINT ALGORITHM.** The aim of this paper is the development and reliability research of the algorithm for solving systems of linear inequalities with Boolean variables, based on variables relaxation, application of the internal point method and the consequent return to Boolean solution. Experimental analysis shows that reliability of the algorithm is about 86 %. This value is higher than the reliability of other heuristic algorithms, applied to the same problem. As the result of experimental research, we have found some classes of systems of inequalities, which are solved by different algorithms with the significantly different reliabilities.

**Keywords:** *pseudo Boolean linear inequalities, interior point method, relaxation, linear programming.*

*Mongush Ch. M.* **ALGORITHM FOR "SAFETY" DECOMPOSITION OF THE FORMAL CONTEXT.** The #P-complete problem of finding all formal concepts of a given formal context is investigated. An algorithm which we propose, allows in practice to solve this problem in a polynomial time. This algorithm is based on the method of "safety" decomposition of the formal context into parts called boxes. With "safety" decomposition of a formal context into boxes, no formal concept of the original context is lost and no new formal concepts arise. The decomposition process is aimed at consistently reducing the size of the boxes of the formal context and is implemented iteratively. The rules for stopping the process of decomposition of the formal context into boxes, which guarantee the polynomial

time of the entire decomposition process, are established: setting the threshold value for the density of boxes and the number of iterations of the decomposition.
**Keywords:** *formal context, formal concept, decomposition of formal context, algorithm of decomposition.*

*Perov A. A.* **ABOUT USING MACHINE LEARNING TECHNOLOGIES FOR CHECKING STATISTICAL PROPERTIES OF SYMMETRIC CRYPTOGRAPHY ALGORITHMS.** This paper describes the use of machine learning technologies in cryptography, in particular, for carrying out the statistical analysis of block ciphers. The idea to adaptate ciphertexts to a model of neural network Inception V3 is stated. The author has developed a software utility for converting texts into JPEG. Conversion of ciphertexts for conducting experiments is completed. In the first experiment, the model distinguished absolutely all the ciphertexts of the Simon algorithm. The second experiment was to distinguish Simon cipher sequences on different rounds. The percentage of correct decisions on each subsequent round decreased. The total value approached 50 %. The third experiment showed an interesting scientific result, which consists in the ability to distinguish ciphertexts of different algorithms in the early rounds. In the fourth experiment, the model was trained on samples of early and full rounds. In 92 % of cases, the neural network made the right decisions to distinguish ciphertexts.
**Keywords:** *cryptography, machine learning, statistical analysis, encryption round, iterative block cipher.*

*Rumenko N. Yu., Kostyuk A. V.* **SOLVING UNDETERMINED SYSTEMS OF LINEAR BOOLEAN EQUATIONS WITH CORRUPTED RIGHT-HAND SIDE AND LOW-WEIGHT TRUE SOLUTION.** Undetermined systems of random linear Boolean equations with corrupted right-hand side and with a true solution of little Hamming weight are studied. Experimentally, we show that, for small bit-error rates, these systems can be efficiently solved by decoding algorithms with regard to information symbols.
**Keywords:** *random systems of linear Boolean equations, information-set decoding.*

*Sorokin M., Pudovkina M.* **ON APN-FUNCTIONS AND DIVISION PROPERTY OF MULTISETS.** In 2015, the division property was proposed as a tool to construct an integral distinguisher. According to this technique, the less the number $\lceil n/d \rceil$ is for a $n$-bit S-box of degree $d$, the fewer rounds might be in an integral distinguisher. In this paper, the number $\lceil n/d \rceil$ for some binary APN-transformations is studied. The best parameters of the APN-transformations are identified to reduce the number of rounds in the integral distinguisher.
**Keywords:** *APN-transformations, division property, integral distinguisher, integral cryptanalysis.*