

# ПРИКЛАДНАЯ ДИСКРЕТНАЯ МАТЕМАТИКА

---

---

*Приложение*

---

---

№ 7

Сентябрь 2014

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

ТРУДЫ  
Всероссийской конференции  
«XII Сибирская научная школа-семинар с международным участием  
“Компьютерная безопасность и криптография” — SIBECRYPT’14»  
(Екатеринбург, 8–13 сентября 2014 г.)



ТОМСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

**РЕДАКЦИОННАЯ КОЛЛЕГИЯ ЖУРНАЛА  
«ПРИКЛАДНАЯ ДИСКРЕТНАЯ МАТЕМАТИКА»**

Агибалов Г. П., д-р техн. наук, проф. (председатель); Девянин П. Н., д-р техн. наук, проф. (зам. председателя); Парватов Н. Г., д-р физ.-мат. наук, доц. (зам. председателя); Черемушкин А. В., д-р физ.-мат. наук, чл.-корр. Академии криптографии РФ (зам. председателя); Панкратова И. А., канд. физ.-мат. наук, доц. (отв. секретарь); Алексеев В. Б., д-р физ.-мат. наук, проф.; Бандман О. Л., д-р техн. наук, проф.; Быкова В. В., д-р физ.-мат. наук, проф.; Глухов М. М., д-р физ.-мат. наук, академик Академии криптографии РФ; Евдокимов А. А., канд. физ.-мат. наук, проф.; Колесникова С. И., д-р техн. наук; Костюк Ю. Л., д-р техн. наук, проф.; Логачев О. А., канд. физ.-мат. наук, доц.; Салий В. Н., канд. физ.-мат. наук, проф.; Сафонов К. В., д-р физ.-мат. наук, проф.; Фомичев В. М., д-р физ.-мат. наук, проф.; Чеботарев А. Н., д-р техн. наук, проф.; Шойтов А. М., д-р физ.-мат. наук, чл.-корр. Академии криптографии РФ; Шоломов Л. А., д-р физ.-мат. наук, проф.

Адрес редакции: 634050, г. Томск, пр. Ленина, 36  
E-mail: vestnik\_pdm@mail.tsu.ru

*Всероссийская конференция «XIII Сибирская научная школа-семинар с международным участием “Компьютерная безопасность и криптография” — SIBECRYPT’14» проведена Национальным исследовательским Томским государственным университетом и Уральским федеральным университетом имени первого Президента России Б.Н. Ельцина в сотрудничестве с Институтом криптографии, связи и информатики с 8 по 13 сентября 2014 г. в г. Екатеринбурге при финансовой поддержке РФФИ (грант № 14-07-20050-г).*

Теоретические основы прикладной дискретной математики  
Математические методы криптографии  
Псевдослучайные генераторы  
Математические методы стеганографии  
Математические основы компьютерной безопасности  
Математические основы надёжности вычислительных  
и управляющих систем  
Прикладная теория кодирования  
Прикладная теория графов  
Прикладная теория автоматов  
Математические основы информатики и программирования  
Вычислительные методы в дискретной математике

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

---

Подписано к печати 02.07.2014.  
Формат 60 × 84 $\frac{1}{8}$ . Усл. п. л. 19,4. Уч.-изд. л. 21,77. Тираж 300 экз.

---

Издательство ТГУ. 634029, Томск, ул. Никитина, 4

# СОДЕРЖАНИЕ

## Секция 1

### ТЕОРЕТИЧЕСКИЕ ОСНОВЫ ПРИКЛАДНОЙ ДИСКРЕТНОЙ МАТЕМАТИКИ

<b>Бар-Гнар Р. И., Фомичев В. М.</b> О минимальных примитивных матрицах.....	7
<b>Бондаренко Л. Н., Шарапова М. Л.</b> Числа Эйлера на множествах перестановок и аналоги теоремы Вильсона .....	9
<b>Виткуп В. А.</b> О некоторых открытых вопросах в области APN-функций .....	11
<b>Геут Кр. Л., Титов С. С.</b> Задача, эквивалентная проверке простоты чисел Ферма .....	13
<b>Городилова А. А.</b> Характеризация APN-функций через подфункции.....	15
<b>Заец М. В.</b> Классификация функций над примарным кольцом вычетов в связи с методом покоординатной линеаризации .....	16
<b>Ивачев А. С.</b> Исследование класса дифференцируемых функций в кольцах классов вычетов по примарному модулю .....	19
<b>Коломеец Н. А.</b> Верхняя оценка числа бент-функций на расстоянии $2^k$ от произвольной бент-функции от $2k$ переменных.....	22
<b>Корсакова Е. П.</b> Оценки нелинейности векторных булевых функций специального вида.....	24
<b>Курганский А. Н.</b> Проблема достижимости в непрерывных кусочно-аффинных отображениях окружности степени 2 .....	26
<b>Минаков А. А.</b> Аппроксимация распределения числа монотонных цепочек в случайной последовательности сложным пуассоновским распределением.....	29
<b>Черемушкин А. В.</b> О числе дискретных функций на циклической группе примарного порядка с заданной степенью нелинейности .....	31
<b>Шишкин В. А.</b> Некоторые свойства $q$ -ичных бент-функций.....	33
<b>Шоломов Л. А.</b> О сравнении недоопределённых алфавитов.....	34
<b>Шушуев Г. И.</b> Векторные булевы функции на расстоянии один от APN-функций .....	36
<b>Tokareva N. N.</b> Every cubic Boolean function in 8 variables is the sum of not more than 4 bent functions .....	38

## Секция 2

### МАТЕМАТИЧЕСКИЕ МЕТОДЫ КРИПТОГРАФИИ

<b>Аборнев А. В.</b> Нелинейные подстановки на пространстве, рекурсивно-порождённые над кольцом Галуа характеристики 4.....	40
<b>Авезова Я. Э., Фомичев М. В.</b> О примитивности перемешивающей матрицы генератора $(\delta, \tau)$ -самоусечения .....	42
<b>Агибалов Г. П.</b> SIBCiphers — симметричные итеративные блочные шифры из булевых функций с ключевыми аргументами .....	43
<b>Волгин А. В.</b> Асимптотические свойства множества решений искажённых систем уравнений .....	48
<b>Пестунов А. И.</b> Влияние веса Хэмминга разности на вероятность её сохранения после арифметических операций .....	49
<b>Погорелов Б. А., Пудовкина М. А.</b> Об обобщениях марковского подхода при изучении алгоритмов блочного шифрования .....	51
<b>Пудовкина М. А.</b> О вероятностях $r$ -раундовых пар разностей XSL-алгоритма блочного шифрования Маркова с приводимым линейным преобразованием .....	52

<b>Рацеев С. М.</b> Условия существования совершенных шифров с фиксированным набором параметров .....	54
<b>Романьков В. А.</b> Криптографический анализ аналога схемы Диффи — Хеллмана, использующего сопряжение и возведение в степень, на матричной платформе .....	56

## Секция 3

**ПСЕВДОСЛУЧАЙНЫЕ ГЕНЕРАТОРЫ**

<b>Былков Д. Н.</b> Об одном классе булевых функций, построенных с использованием старших разрядных последовательностей линейных рекуррент .....	59
<b>Дорохова А. М.</b> Оценки экспонентов перемешивающих графов некоторых модификаций аддитивных генераторов .....	60
<b>Ермилов Д. М.</b> Алгоритм построения системы представителей циклов максимальной длины полиномиальных подстановок над кольцом Галуа .....	64
<b>Захаров В. М., Зелинский Р. В., Шалагин С. В.</b> Модель функции усложнения в генераторе псевдослучайных последовательностей над полем $GF(2)$ .....	67
<b>Ковалевская А. О.</b> Построение транзитивных полиномов над кольцом $\mathbb{Z}_{p^2}$ .....	69
<b>Сергеева О. Е.</b> Распознавание рекуррентных последовательностей, порождаемых консервативными функциями .....	71

## Секция 4

**МАТЕМАТИЧЕСКИЕ МЕТОДЫ СТЕГАНОГРАФИИ**

<b>Анжин В. А.</b> Метод защиты от нелегального копирования в цифровых видеотрансляциях через внедрение водяных знаков при расшифровании .....	73
<b>Вершинин И. С.</b> Принципы ассоциативной стеганографии .....	75
<b>Монарев В. А.</b> Новый высокоточный стегоанализ растровых изображений .....	76
<b>Разинков Е. В., Альмеев А. Н.</b> Определение размера стеганографического сообщения в цифровых изображениях с использованием бинарного стеганоаналитического классификатора .....	78

## Секция 5

**МАТЕМАТИЧЕСКИЕ ОСНОВЫ КОМПЬЮТЕРНОЙ БЕЗОПАСНОСТИ**

<b>Глотов И. Н., Овсянников С. В., Тренькаев В. Н.</b> Защищённая СУБД с сохранением порядка .....	81
<b>Девянин П. Н.</b> Условия безопасности информационных потоков по памяти в рамках МРОСЛ ДП-модели .....	82
<b>Колегов Д. Н.</b> Общий метод аутентификации HTTP-сообщений в веб-приложениях на основе хеш-функций .....	85
<b>Колегов Д. Н., Брославский О. В., Олексов Н. Е.</b> Об информационных потоках по времени, основанных на заголовках кэширования протокола HTTP .....	89
<b>Милованов Т. И.</b> О скрытых каналах по времени в ОС Android .....	92
<b>Рыжков В. И.</b> Использование электронных сертификатов для авторизации по доверенности в ОС Linux .....	94
<b>Сорокин С. Н.</b> Формирование векторов показателей для обучения нейронных сетей при обнаружении атак на web-приложения .....	96

<b>Ткаченко Н. О.</b> Реализация монитора безопасности СУБД MySQL в DBF/DAM-системах.....	99
<b>Толопа Е. А.</b> Метод обеспечения безопасности пользователей интернет-магазинов мобильных приложений .....	101
<b>Чернов Д. В.</b> ДП-модель мандатного управления доступом с контролем целостности СУБД MySQL .....	103
<b>Sviridov P. Y., Zaytsev G. Y., Ivachev A. S.</b> The universal vulnerability exploitation platform for CTF .....	106

## Секция 6

### МАТЕМАТИЧЕСКИЕ ОСНОВЫ НАДЁЖНОСТИ ВЫЧИСЛИТЕЛЬНЫХ И УПРАВЛЯЮЩИХ СИСТЕМ

<b>Алехина М. А., Барсукова О. Ю.</b> Ненадёжность схем в базисе Россера — Туркетта .	109
<b>Алехина М. А., Лакомкина А. Е.</b> О надёжности схем в базисе из ненадёжных и абсолютно надёжных элементов.....	111
<b>Васин А. В.</b> О полных базисах с коэффициентом ненадёжности 5 .....	113

## Секция 7

### ПРИКЛАДНАЯ ТЕОРИЯ КОДИРОВАНИЯ

<b>Дружинин Д. В.</b> Гибридный алгоритм сжатия дискретно-тоновой графики .....	116
<b>Зубков А. М., Круглов В. И.</b> Вероятностные характеристики весовых спектров случайных линейных подкодов над $GF(p)$ .....	118

## Секция 8

### ПРИКЛАДНАЯ ТЕОРИЯ ГРАФОВ

<b>Быков И. С.</b> О циклах графов функционирования генных сетей циркулянтного типа с пороговыми функциями .....	122
<b>Гавриков А. В.</b> Алгоритм построения $T$ -неприводимого расширения для многоугольных орграфов .....	124
<b>Жаркова А. В.</b> Об аттракторах в конечных динамических системах двоичных векторов, ассоциированных с ориентациями палым .....	126
<b>Комаров Д. Д.</b> Построение рёберного 1-расширения для сверхстройного дерева произвольного вида .....	128
<b>Кяжин С. Н.</b> Достаточные условия локальной примитивности непримитивных орграфов .....	130
<b>Осипов Д. Ю.</b> Об одном контрпримере для $T$ -неприводимых расширений сверхстройных деревьев .....	132
<b>Салий В. Н.</b> Шпернерово свойство для многоугольных графов.....	135
<b>Фомичев В. М.</b> Об оценках экспонентов орграфов с использованием чисел Фробениуса	137

## Секция 9

### ПРИКЛАДНАЯ ТЕОРИЯ АВТОМАТОВ

<b>Катеринский Д. А.</b> Оценка кратности выходного символа в обратимом автомате.....	141
<b>Ковалев Д. С., Тренькаев В. Н.</b> Реализация на ПЛИС шифра Закревского на основе перестраиваемого автомата, заданного формулами .....	142
<b>Панкратов И. В.</b> Применение конечного автомата для одновременного поиска нескольких двоичных шаблонов в потоке данных .....	143

## Секция 10

**МАТЕМАТИЧЕСКИЕ ОСНОВЫ ИНФОРМАТИКИ  
И ПРОГРАММИРОВАНИЯ**

<b>Грибанов А. С., Сибирякова В. А.</b> Программная реализация операций над большими числами в языке ЛЯПАС-Т.....	146
<b>Жуковская А. О., Стефанцов Д. А.</b> Разработка автоматизированного средства для доказательства свойств программ .....	148

## Секция 11

**ВЫЧИСЛИТЕЛЬНЫЕ МЕТОДЫ В ДИСКРЕТНОЙ МАТЕМАТИКЕ**

<b>Анашкина Н. В., Шурупов А. Н.</b> Экспериментальное сравнение алгоритмов Балаша и имитации отжига в задаче решения систем линейных неравенств.....	151
<b>Быкова В. В.</b> Структурная декомпозиция графа и её применение для решения оптимизационных задач на разреженных графах .....	154
<b>Гоцуленко В. В.</b> Формализация комбинаторных чисел в терминах целочисленных решений систем линейных диофантовых уравнений .....	157
<b>Жуков К. Д., Рыбаков А. С.</b> Алгоритм генерации пары простых чисел специального вида .....	160
<b>Кузнецов А. А., Сафонов К. В.</b> Полиномы Холла для конечных двупорождённых групп периода семь .....	162
<b>Шангин Р. Э.</b> Эвристики построения надежной телекоммуникационной сети.....	164
СВЕДЕНИЯ ОБ АВТОРАХ .....	166
АННОТАЦИИ ДОКЛАДОВ НА АНГЛИЙСКОМ ЯЗЫКЕ .....	171

## Секция 1

ТЕОРЕТИЧЕСКИЕ ОСНОВЫ  
ПРИКЛАДНОЙ ДИСКРЕТНОЙ МАТЕМАТИКИ

УДК 519.7

## О МИНИМАЛЬНЫХ ПРИМИТИВНЫХ МАТРИЦАХ

Р. И. Бар-Гнар, В. М. Фомичев

Исследуется подход к минимизации реализации преобразований, степень которых реализует полное перемешивание входных данных. Введены понятия минимальной примитивной матрицы и высоты примитивной матрицы. Получены оценки числа минимальных примитивных матриц порядка  $n$ . Построены и проанализированы алгоритмы поиска минимальных примитивных матриц и оценки близости примитивной матрицы к множеству минимальных примитивных матриц.

**Ключевые слова:** примитивная матрица, решётка, антицепь, вычислительная сложность алгоритма.

## Введение

Для оценки свойства перемешивания входов композиции преобразований часто применяется матрично-графовый подход [1, гл. 10], основанный на определении экспонентов перемешивающих матриц (графов). Обзор основных результатов по этому направлению имеется в [2].

Аппаратная и программная реализация совершенных преобразований, реализующих полное перемешивание, затруднена необходимостью реализации большого количества связей между компонентами входных и выходных векторов. В связи с этим в работе введено и исследовано понятие минимальной примитивной матрицы, позволяющей оценить предельные возможности уменьшения количества связей между входом и выходом при сохранении свойства полного перемешивания у композиции преобразований.

## 1. Свойства минимальных примитивных матриц

Обозначим через  $M_0(n)$  множество квадратных 0, 1-матриц порядка  $n$ ,  $S(n)$  — множество подстановочных матриц,  $P(n)$  — множество примитивных матриц.

Примитивная матрица (граф) называется минимальной, если после замены любой единицы нулём (после удаления любой дуги) получается непримитивная матрица (граф). Обозначим множество минимальных примитивных матриц через  $P_{\min}(n)$ .

**Утверждение 1.** Если примитивные матрицы  $A, B \in M_0(n)$  сопряжены в  $S(n)$  и примитивны, то они одновременно минимальные или неминимальные.

Рассмотрим на множестве  $M_0(n)$  отношение частичного порядка:  $A \leq B \Leftrightarrow a_{i,j} \leq b_{i,j}$  для всех  $i, j = 1, \dots, n$ , где  $A = (a_{i,j}), B = (b_{i,j})$ . Множество  $M_0(n)$  образует решётку в смысле отношения  $\leq$ , где матрица, все элементы которой равны 1, является наибольшим элементом, а нулевая матрица — наименьшим. Подмножество примитивных

матриц  $P(n)$  множества  $M_0(n)$  является верхней полурешёткой. Минимальные примитивные матрицы — это все минимальные элементы верхней полурешётки  $P(n)$ .

В частично упорядоченном множестве  $X$  антицепь  $Y$  назовем наибольшей, если она имеет наибольшую мощность, и максимальной, если любой элемент множества  $X$  сравним с некоторым элементом антицепи  $Y$ .

**Утверждение 2.**  $P_{\min}(n)$  есть максимальная антицепь полурешётки  $P(n)$ .

Число единиц матрицы  $A \in M_0(n)$  называется весом матрицы  $A$  (обозначается  $\|A\|$ ). Назовём  $k$ -м слоем подрешётки  $R$  решётки  $M_0(n)$  подмножество (обозначается  $R^{(k)}$ ), состоящее из матриц веса  $k$ , где  $k = 0, 1, \dots, n^2$ . Заметим, что  $R^{(k)}$  есть антицепь решётки  $R$  при всех  $k$ .

**Утверждение 3.** При  $n > 3$  выполнена оценка

$$3n! \leq |P_{\min}(n)| \leq C_m^{\lfloor m/2 \rfloor}, \text{ где } m = n^2.$$

Нижняя оценка получена с использованием свойства  $P^{(n+1)}(n) \subseteq P_{\min}(n)$ , где  $P^{(n+1)}(n)$  содержит три класса орграфов, порядки которых равны  $n!$ :

- 1) полный цикл с добавленной дугой  $(i-1, i+1)$ ,  $i \in \{1, \dots, n\}$  (рис. 1, а);
- 2) полный цикл с добавленной петлей в вершине  $i \in \{1, \dots, n\}$  (рис. 1, б);
- 3) класс графов, вид которых зависит от чётности числа  $n$ : при чётном  $n$  граф состоит из двух циклов длины 2 и  $l = n-1$  (рис. 1, в); при нечётном — из двух циклов длины 2 и  $l = n$  (рис. 1, г). В обоих случаях  $(2, l) = 1$ , поэтому в соответствии с критерием [3, с. 226] графы примитивные.

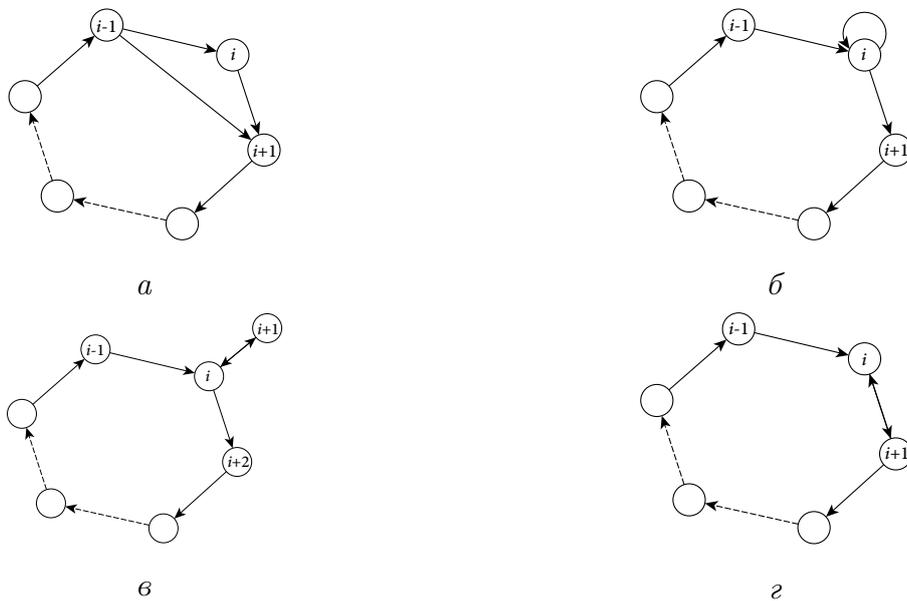


Рис. 1. Примеры минимальных графов из  $P^{(n+1)}(n)$

Улучшение нижней оценки возможно на основе обобщения случая 3 (рассмотрения некоторых классов графов из слоев  $P^{(n+r)}(n)$  при  $r > 1$ ).

## 2. Высота примитивной матрицы

Расстоянием по Хэммингу между 0, 1-матрицами  $A$  и  $B$  (обозначается  $d(A, B)$ ) называется число различных соответствующих элементов матриц  $A$  и  $B$ :

$$d(A, B) = \sum_{i,j} (a_{i,j} \oplus b_{i,j}).$$

Высотой примитивной матрицы  $A$  (обозначается  $h(A)$ ) называется расстояние по Хэммингу между  $A$  и ближайшей минимальной примитивной матрицей  $M \in P_{\min}(n)$ :

$$h(a) = \min_{M \in P_{\min}(n)} d(A, M).$$

Величина  $h(A)$  является определённой мерой избыточности при построении связей между элементами входа и выхода преобразований информации.

**Алгоритм оценивания  $h(A)$  (метод координатного спуска):**

- 1) последовательно просматривая элементы матрицы  $A$ , находим единицы;
- 2) заменяем найденный единичный элемент в матрице  $A$  нулевым и для полученной матрицы  $A'$  выполняем:
  - проверяем в  $A'$  наличие нулевых строк и столбцов; если таковые есть, возвращаемся к выполнению п. 2 для следующей единицы матрицы  $A$ ;
  - матрицу  $A'$  без нулевых строк и столбцов проверяем на примитивность;
  - если матрица  $A'$  не примитивная, возвращаемся к матрице  $A$ , восстанавливаем заменённую единицу и выполняем п. 2 для следующей единицы матрицы  $A$ ;
  - примитивную матрицу  $A'$  проверяем на минимальность;
  - если  $A'$  минимальная, то определяем  $m$  — число единиц, заменённых нулями;
  - если  $A'$  не минимальная, то переходим к выполнению п. 1 для матрицы  $A'$ .

На выходе алгоритма получим минимальную примитивную матрицу  $M$ , где

$$h(A) \leq d(A, M) = m.$$

Сложность алгоритма полиномиальная. Пусть  $\|A\| = k$ , где  $n < k \leq n^2$  для примитивной матрицы  $A$ . Тогда вычислительная сложность алгоритма в битовых операциях в худшем случае не превышает величины  $O(k^2 n^3 \log n)$ . Объём памяти требуется порядка  $O(n^2)$  битов. Данный метод можно использовать для поиска минимальных матриц, близких к перемешивающим матрицам раундовых подстановок блочных шифров (DES, ГОСТ 28147-89 и др.).

#### ЛИТЕРАТУРА

1. Фомичев В. М. Методы дискретной математики в криптологии. М.: Диалог-МИФИ, 2010.
2. Когос К. Г., Фомичев В. М. Положительные свойства неотрицательных матриц // Прикладная дискретная математика. 2012. № 4(18). С. 5–13.
3. Сачков В. Н., Тараканов В. Е. Комбинаторика неотрицательных матриц. М.: ТВП, 2000.

УДК 519.1:511.2

## ЧИСЛА ЭЙЛЕРА НА МНОЖЕСТВАХ ПЕРЕСТАНОВОК И АНАЛОГИ ТЕОРЕМЫ ВИЛЬСОНА

Л. Н. Бондаренко, М. Л. Шарапова

Определяются числа Эйлера на множествах перестановок и с их помощью доказываются аналоги теоремы Вильсона для чисел стандартных полных отображений и чисел стандартных сильных полных отображений.

**Ключевые слова:** перестановка, числа Эйлера, полные отображения, теорема Вильсона.

На симметрической группе  $S_{n-1}$  статистика  $\text{des}(\sigma) = |\{i \in [n-1] : \sigma_i > \sigma_{i+1}, \sigma_n = 0\}|$  при фиксированном  $n \geq 2$  описывает число спусков перестановки  $\sigma = \sigma_1 \dots \sigma_{n-1} \in S_{n-1}$  над алфавитом  $[n-1] = \{1, \dots, n-1\}$ . На множестве перестановок  $U \subseteq S_{n-1}$  определим производящий многочлен Эйлера  $\sum_{\sigma \in U} t^{\text{des}(\sigma)}$ , а его коэффициенты назовём числами Эйлера на  $U$ . В частности, этот многочлен на  $S_{n-1}$  совпадает с многочленом Эйлера  $A_{n-1}(t) = \sum_{k=1}^{n-1} A_{n-1,k} t^k$  степени  $n-1$ , а  $A_{n-1,k} = |\{\sigma \in S_{n-1} : \text{des}(\sigma) = k\}|$  [1].

Для простого числа  $p$  имеем  $A_{p-1}(1) = |S_{p-1}| = (p-1)! \equiv -1 \pmod{p}$ , что отвечает теореме Вильсона [2], а её усилением служит следующее утверждение.

**Теорема 1.**  $A_{p-1,k} \equiv 1 \pmod{p}$ ,  $k = 1, \dots, p-1$ .

Теорему 1 можно доказать с помощью формул для чисел Эйлера  $A_{p-1,k}$ , но интереснее получить её прямое доказательство на основе свойств перестановок  $\sigma \in S_{n-1}$ , что позволяет также найти аналоги теоремы Вильсона для чисел, связанных с трудными перечислительными проблемами полных отображений.

Определим биекцию  $\mathbf{s} : S_{n-1} \rightarrow S_{n-1}$  с помощью равенств  $\mathbf{s}\sigma_i = n - \sigma_i$ ,  $i \in [n-1]$ , для символов  $\sigma \in S_{n-1}$ , а дополнение к  $\sigma$  обозначим  $\bar{\sigma} = \mathbf{s}\sigma$ .

В криптографии сложение перестановок  $\sigma \in S_{n-1}$  часто выполняется посимвольно по  $\text{mod } n$ , т. е. на аддитивной группе  $\mathbb{Z}_n$ , отождествляемой с  $\{0, 1, \dots, n-1\}$ , причём это переносится и на умножение  $\sigma \in S_{n-1}$  на целое число. Будем также использовать формулу  $\text{des}(\sigma) = n^{-1} \sum_{i=0}^{n-1} (\sigma_{i+1} - \sigma_i)$ , в которой разности берутся по  $\text{mod } n$ , а  $\sigma_0 = \sigma_n = 0$ .

Непосредственно из определений следует, что  $\mathbf{s}$  есть инволюция, а  $\sigma + \bar{\sigma} = 0$ , причём элементарное равенство  $\text{des}(\sigma) + \text{des}(\bar{\sigma}) = n$  влечёт соотношение  $t^n A_{n-1}(t^{-1}) = A_{n-1}(t)$ .

**Определение 1.** Перестановки  $\sigma, \tilde{\sigma} \in S_{n-1}$  назовём сопряжёнными относительно  $\bar{\varepsilon} \in S_{n-1}$ , если  $\sigma + \tilde{\sigma} = \bar{\varepsilon}$ , а  $\varepsilon \in S_{n-1}$  — единичная перестановка (сопряжённость можно рассматривать относительно любой перестановки  $\tau \in S_{n-1}$ ).

Все  $\sigma \in S_{n-1}$ , сопряжённые относительно  $\varepsilon \in S_{n-1}$ , задают множество  $CM(\mathbb{Z}_n)$  всех стандартных полных отображений [3], а  $|CM(\mathbb{Z}_n)| = |\overline{CM}(\mathbb{Z}_n)|$ ,  $\overline{CM}(\mathbb{Z}_n)$  — множество всех  $\sigma \in S_{n-1}$  из определения 1. Множество всех стандартных сильных полных отображений  $SCM(\mathbb{Z}_n) = CM(\mathbb{Z}_n) \cap \overline{CM}(\mathbb{Z}_n)$ ,  $|CM(\mathbb{Z}_n)| = 0$  при чётном  $n$  и  $|SCM(\mathbb{Z}_n)| = 0$  также и при  $n$ , кратном трём, а задачи вычисления чисел  $|CM(\mathbb{Z}_n)|$  и  $|SCM(\mathbb{Z}_n)|$  являются  $\#P$ -полными [3] ( $|CM(\mathbb{Z}_n)|$  при нечётном  $n = 1, 3, \dots, 25$  приведены в [4]).

Свойства чисел Эйлера из теоремы 1 наследуются числами Эйлера  $\tilde{A}_{n-1,k}$  на  $CM(\mathbb{Z}_n)$ ,  $\hat{A}_{n-1,k}$  на  $SCM(\mathbb{Z}_n)$  и приводят к аналогам теоремы Вильсона.

**Теорема 2.**  $\tilde{A}_{p-1,k} \equiv 1 \pmod{p}$ ,  $k = 1, \dots, p-2$ ;  $\tilde{A}_{p-1,p-1} = 0$ , что влечёт  $|CM(\mathbb{Z}_p)| \equiv -2 \pmod{p}$ .

**Теорема 3.**  $\hat{A}_{p-1,1} = 0$ ;  $\hat{A}_{p-1,k} \equiv 1 \pmod{p}$ ,  $k = 2, \dots, p-2$ ;  $\hat{A}_{p-1,p-1} = 0$ , что влечёт  $|SCM(\mathbb{Z}_p)| \equiv -3 \pmod{p}$ .

Доказательство теорем базируется на следующих вспомогательных утверждениях.

**Лемма 1.** Пусть  $R_n = \{r\varepsilon : r \in [n-1], (r, n) = 1, \varepsilon \in S_{n-1}\}$  отвечает приведённой системе вычетов по  $\text{mod } n$ . Тогда  $\text{des}(r\varepsilon) = r$ , а  $|R_n| = \varphi(n)$ , где при  $n = \prod_{p|n} p^{\text{ord}_p(n)}$ ,  $n > 1$ , функция Эйлера  $\varphi(n) = n \prod_{p|n} (1 - p^{-1})$ .

Лемма 1 следует из свойств  $\text{des}$ , а её применение при нечётном  $n > 1$  с определением 1 даёт  $|(R_n \cap \overline{CM}(\mathbb{Z}_n))| = n \prod_{p|n} (1 - 2p^{-1})$  и  $|(R_n \cap \overline{SCM}(\mathbb{Z}_n))| = n \prod_{p|n} (1 - 3p^{-1})$ .

**Лемма 2.** Если  $\sigma \in \overline{CM}(\mathbb{Z}_n)$ , то  $\text{des}(\sigma) + \text{des}(\tilde{\sigma}) = n - 1$ .

Применение формулы вычисления статистики  $\text{des}$  к перестановкам из определения 1 даёт требуемое. Так как  $\deg \tilde{A}_{n-1}(t) = n - 2$ , то по лемме 2 имеем  $t^{n-1} \tilde{A}_{n-1}(t^{-1}) = \tilde{A}_{n-1}(t)$ , а также  $\deg \hat{A}_{n-1}(t) = n - 2$ ,  $\hat{A}_{n-1,1} = 0$  и  $t^n \hat{A}_{n-1}(t^{-1}) = \hat{A}_{n-1}(t)$ .

**Определение 2.**  $\tau = \tau_1 \dots \tau_{n-1} \in S_{n-1}$ ,  $\tau = \mathbf{d}\sigma$  назовём смещением  $\sigma \in S_{n-1}$ , если биекция  $\mathbf{d} : S_{n-1} \rightarrow S_{n-1}$  задана выражениями  $\tau_i = \sigma_{i+1} - \sigma_i \pmod{n}$ ,  $i = 1, \dots, n-2$ , и  $\tau_{n-1} = n - \sigma_1$ , а порядком  $d = d(\sigma)$  назовём наименьшее  $k \in \mathbb{Z}^+$ , для которого  $\mathbf{d}^k \sigma = \sigma$ .

**Лемма 3.** Если  $\sigma \in S_{n-1}$ , то  $\text{des}(\mathbf{d}\sigma) = \text{des}(\sigma)$  и  $d|n$ .

Равенство  $\text{des}(\mathbf{d}\sigma) = \text{des}(\sigma)$  получается из свойств  $\text{des}$ , а делимость  $d|n$  следует из определения 2, так как повторное применение  $\mathbf{d}$  разбивает  $S_{n-1}$  на классы эквивалентности (так,  $\mathbf{d}r\varepsilon = r\varepsilon$ ,  $r\varepsilon \in R_n$ , т.е.  $d = 1$ ). При  $n > 4$  в словах  $\mathbf{d}^k \sigma \in S_{n-1}$ ,  $k = 0, \dots, d-1$ , имеется  $n/d - 1$  неподвижных символов  $\sigma_i$ , кратных  $d$ , с индексом  $i$ , кратным  $d$ .

Теоремы 1–3 доказываются с помощью лемм 1, 2 и леммы 3, справедливой также на  $\overline{CM}(\mathbb{Z}_n)$  и  $\overline{SCM}(\mathbb{Z}_n)$ , причём применяемый метод дополнительно даёт следующие сравнения:  $|\overline{CM}(\mathbb{Z}_n)| \equiv 1 \pmod{2}$  при нечётном  $n$  и  $|\overline{SCM}(\mathbb{Z}_n)| \equiv 0 \pmod{2}$  при  $n > 1$ .

#### ЛИТЕРАТУРА

1. Стенли Р. Перечислительная комбинаторика. Т. 1. М.: Мир, 1990.
2. Айерлэнд К., Роузен М. Классическое введение в современную теорию чисел. М.: Мир, 1987.
3. Hsiang J., Hsu D. F., and Shieh Y. P. On the hardness of counting problems of complete mappings // Discr. Math. 2004. V. 277. P. 87–100.
4. <http://oeis.org/A003111> — Sloane N. J. A. The on-line encyclopedia of integer sequences.

УДК 519.7

### О НЕКОТОРЫХ ОТКРЫТЫХ ВОПРОСАХ В ОБЛАСТИ APN-ФУНКЦИЙ

В. А. Виткуп

Приведены открытые вопросы в области APN-функций, связанные с их построением. Перечислены некоторые известные результаты в данном направлении. Доказано необходимое и достаточное условие того, что сумма двух APN-функций является APN-функцией.

**Ключевые слова:** векторная булева функция, APN-функция.

Работа К. Ньюберг [1] положила начало новому направлению в исследовании векторных булевых функций — изучению совершенно и почти совершенно нелинейных векторных булевых функций, обладающих наилучшей стойкостью к дифференциальному криптоанализу.

Векторная булева функция из  $\mathbb{F}_2^n$  в  $\mathbb{F}_2^n$  называется APN-функцией (Almost Perfect Nonlinear), если уравнение  $F(x \oplus a) \oplus F(x) = b$  имеет не более двух решений для любых  $a \in \mathbb{F}_2^n \setminus \{0\}$ ,  $b \in \mathbb{F}_2^n$ . В настоящее время APN-функции активно изучаются, но

до сих пор многие важные вопросы остаются открытыми. Например, не известно точное число таких функций, нижние и верхние оценки числа APN-функций, оценка их алгебраической степени. Не так многочисленны и известные конструкции APN-функций — степенные функции вида  $F(x) = x^d$  и несколько полиномиальных (см. подробнее обзоры в [2, 3]). Очень интересен вопрос о конструкции APN-функции с помощью композиции или суммы двух функций и о нахождении итеративных конструкций [4].

Важное место в исследовании векторных функций занимает проблема существования взаимно однозначных APN-функций при чётном  $n$ . В своё время была выдвинута гипотеза, что для чётного числа переменных APN-перестановок не существует, однако в 2009 г. Дж. Диллон и др. [5] опровергли это предположение, построив взаимно однозначную APN-функцию над  $\mathbb{F}_{2^6}$ , которая  $CCZ$ -эквивалентна APN-функции, не являющейся перестановкой. Разработанный авторами [5] метод обобщался для большего числа переменных, однако с его помощью им не удалось найти APN-перестановки от 8 и 10 переменных. Интересно, что при решении этой задачи авторы [5] в неявном виде использовали для построения композицию двух перестановок.

Пусть векторная булева функция  $F$  имеет следующий вид:

$$F(x) = (f_1(x), \dots, f_n(x)), \quad \text{где } f_i(x) = a_{i,0}^F \oplus a_{i,1}^F x_1 \oplus \dots \oplus a_{i,1\dots n}^F x_1 x_2 \dots x_n.$$

**Утверждение 1.** Пусть  $F_1$  и  $F_2$  — APN-функции из  $\mathbb{F}_2^2$  в  $\mathbb{F}_2^2$ . Тогда  $F = F_1 \oplus F_2$  — APN-функция тогда и только тогда, когда  $(a_{1,12}^{F_1} \oplus a_{1,12}^{F_2}) \vee (a_{2,12}^{F_1} \oplus a_{2,12}^{F_2}) = 1$ .

Всего в  $\mathbb{F}_2^2$  существует 192 APN-функции, значит, всевозможных пар  $C_{192}^2 = 18336$ . Из них 12288 пар  $F_1$  и  $F_2$ , сумма которых является APN-функцией, что составляет около 67%.

Перечислим некоторые интересные открытые вопросы в области APN-функций, связанные с проблемой их построения.

- Как построить APN-функцию путём композиции или суммы двух векторных функций? Какими свойствами должна обладать такая пара функций?

- Можно ли представить произвольную APN-функцию в виде композиции двух векторных функций? В том числе функций, обладающих более «простыми» характеристиками (например, меньшей алгебраической степенью или более коротким полиномиальным представлением)? Так, в работе [5] приведён пример взаимно однозначной APN-функции над  $\mathbb{F}_{2^6}$  алгебраической степени 4, которую можно представить через композицию двух векторных булевых функций меньших степеней — 2 и 3.

- Пусть  $F$  — APN-функция, действующая из  $\mathbb{F}_2^n$  в  $\mathbb{F}_2^n$ . Какими свойствами обладают её подфункции? Существует ли характеристика APN-функции через её компонентные булевы функции? Одна из возможных характеристик APN-функций через подфункции предложена в [4].

- Описать группу автоморфизмов класса APN-функций, APN-перестановок. Какие преобразования не выводят функцию (перестановку) за рамки класса?

- Исследовать метрические свойства класса APN-функций. Некоторые продвижения по этому вопросу недавно получены в [6].

- Осуществить классификацию квадратичных APN-функций от  $n$  переменных. Напомним, что квадратичная APN-функция также является АВ-функцией, т. е. её компонентные функции находятся на максимальном расстоянии от класса аффинных функций, что означает оптимальную стойкость к линейному криптоанализу.

Ответы на эти вопросы помогут получить новые конструкции APN-функций, включая итеративные и композиционные, а также упростить их программную и аппаратную реализацию в симметричных шифрах.

## ЛИТЕРАТУРА

1. Nyberg K. Perfect nonlinear S-boxes // LNCS. 1991. V. 547. P. 378–386.
2. Budaghyan L. Construction and Analysis of Cryptographic Functions. Habilitation Thesis. University of Paris, 8 Sept. 2013.
3. Тужилин М. Э. Почти совершенные нелинейные функции // Прикладная дискретная математика. 2009. № 3. С. 14–20.
4. Городилова А. А. Характеризация APN-функций через подфункции // Прикладная дискретная математика. Приложение. 2014. № 7. С. 15–16.
5. McQuistan M. T., Wolfe A. J., Browning K. A., and Dillon J. F. An APN permutation in dimension six // Amer. Math. Soc. 2010. No. 518. P. 33–42.
6. Шушурев Г. И. Векторные булевы функции на расстоянии один от APN-функций // Прикладная дискретная математика. Приложение. 2014. № 7. С. 36–37.

УДК 512.62

### ЗАДАЧА, ЭКВИВАЛЕНТНАЯ ПРОВЕРКЕ ПРОСТОТЫ ЧИСЕЛ ФЕРМА

Кр. Л. Геут, С. С. Титов

Работа посвящена постановке задачи, эквивалентной проверке простоты чисел Ферма. Сформулирована задача последовательного построения неприводимых многочленов над конечными полями характеристики два и три, эквивалентная проверке простоты чисел. Показана эквивалентность построения всех неприводимых симметричных многочленов степени  $2^{k+1}$  над полем  $\text{GF}(2)$  и определения простоты числа Ферма  $2^{2^k}$ . Рассмотрена взаимосвязь между проверкой простоты чисел Ферма и построением неприводимых многочленов над  $\text{GF}(3)$ .

**Ключевые слова:** неприводимый многочлен, простые числа, числа Ферма.

Неприводимые многочлены — аналог простых чисел — имеют большую ценность в теории информации, помехоустойчивом кодировании, работе конечных автоматов, стандартах защиты информации. Поэтому актуален поиск взаимосвязи между ними [1–4].

Интерес представляют многочлены степени  $2^n$  над полем  $\text{GF}(2)$ , коэффициенты которых при преобразовании в битовые строки широко используются для работы ЭВМ. В кодировании применяются симметричные (самовозвратные) многочлены [5] порядка  $p = 2^{2^k} + 1$  степени  $N = 2^{k+1}$ . Легко показать, что если неприводимый над  $\text{GF}(2)$  многочлен имеет степень  $2m$  и порядок  $2^m + 1$ , то он симметричен.

**Утверждение 1.** Простота числа Ферма  $p = 2^{2^k} + 1$  эквивалентна равенству  $p$  порядков всех неприводимых симметричных многочленов степени  $n = 2^{k+1}$  над  $\text{GF}(2)$ .

Так, например, при  $k = 0$ ,  $p = 3$  имеется один симметричный многочлен  $x^2 + x + 1$  степени 2, порядка 3; при  $k = 1$ ,  $p = 5$  — один симметричный многочлен  $x^4 + x^3 + x^2 + x + 1$  степени 4, порядка 5; при  $k = 2$ ,  $p = 17$  — два многочлена степени 8, порядка 17:  $x^8 + x^7 + x^6 + x^4 + x^2 + x + 1$  и  $x^8 + x^5 + x^4 + x^3 + 1$ ; при  $k = 4$ ,  $p = 65537$  имеется 2048 многочленов степени 32 порядка  $p$  [6].

При  $k = 5$  число  $p = 4294967297 = 64 \cdot 6700417$  непростое, это означает, что неприводимые симметричные многочлены степени 64 имеют порядок 4294967297, или 641, или 6700417. Последовательным подбором коэффициентов были найдены 10 неприводимых симметричных многочленов степени 64 порядка 641 [4].

При  $k = 6$  получаем  $p = 18446744073709551617 = 274177 \cdot 67280421310721$ . До настоящего времени не найдено простых чисел Ферма для  $k > 4$ , есть предположение, что их больше нет.

Как известно, круговой многочлен  $x^{p-1} + \dots + x + 1$  неприводим над полем  $\text{GF}(q)$  тогда и только тогда, когда  $p$  простое и  $q$  — первообразный корень по модулю  $p$  [5]. Число Ферма  $p$  простое тогда и только тогда, когда 3 — первообразный корень по модулю  $p$  [7].

**Определение 1** [1, с. 55]. Пусть  $P = F_q$ ,  $K = \text{GF}_{q^m}$  и  $\alpha \in K$ . След  $\text{Tr}_{K/P}(\alpha)$  элемента  $\alpha$  из поля  $K$  в поле  $P$  определяется равенством  $\text{Tr}_{K/P}(\alpha) = \alpha + \alpha^q + \alpha^{q^2} + \dots + \alpha^{q^{m-1}}$ .

Переход от корней круговых многочленов при помощи функции следа к гауссовым нормальным базисам [1, с. 274] равносильно вычислению следа из поля  $\text{GF}(3^{2^s})$  в поле  $\text{GF}(3)$  корня уравнения  $x^{p-1} + \dots + x + 1 = 0$  над  $\text{GF}(3^{2^s})$ ,  $s = 2^k$ , и даёт неприводимые многочлены над  $\text{GF}(3)$ .

**Утверждение 2.** Пусть  $p = 2^{2^k} + 1$  и  $\zeta$  — корень кругового многочлена  $\zeta^{p-1} + \zeta^{p-2} + \dots + \zeta + 1 = 0$  над  $\text{GF}(3)$ , так что  $\zeta^p = 1$ . Тогда простота числа  $p$  эквивалентна неприводимости всех характеристических многочленов любого следа элемента  $\zeta$ .

**Утверждение 3.** Пусть  $p$  — число Ферма. Тогда равенство следа элемента  $\zeta \in \text{GF}(3^{p-1})$  порядка  $p$  в поле  $\text{GF}(3^2)$  корню  $X = x$  неприводимого над  $\text{GF}(3)$  многочлена второй степени  $X^2 + X + 2$  равносильно простоте числа  $p$ .

Таким образом, задача проверки простоты чисел Ферма эквивалентна построению многочленов над конечным полем  $\text{GF}(2)$  или  $\text{GF}(3)$  и проверке их на неприводимость.

#### ЛИТЕРАТУРА

1. Болотов А. А., Гашков С. Б., Фролов А. Б. Элементарное введение в эллиптическую криптографию: алгебраические и алгоритмические основы. М.: КомКнига, 2006.
2. Глушко Кр. Л., Титов С. С. О квадратичных расширениях бинарных полей // Известия Российского государственного педагогического университета им. А. И. Герцена. 2013. № 154. С. 7–16.
3. Геут Кр. Л., Титов С. С. О поликватратичном расширении бинарных полей // Прикладная дискретная математика. Приложение. 2013. № 6. С. 12–13.
4. Геут Кр. Л., Титов С. С. О генерации неприводимых многочленов простых порядков при построении дискретных устройств СЖАТиС // Транспорт Урала. 2014. № 1(40). С. 61–64.
5. Лидл Р., Нидеррайтер Г. Конечные поля. М.: Мир, 1988. 430 с.
6. Геут К. Л., Титов С. С. О генерации и применении неприводимых многочленов // III Информационная школа молодого ученого: сб. научных трудов. Екатеринбург, 2013. С. 293–298.
7. Виноградов И. М. Основы теории чисел. М.; Ижевск: НИЦ «Регулярная и хаотическая динамика», 2003. 176 с.

УДК 519.7

**ХАРАКТЕРИЗАЦИЯ APN-ФУНКЦИЙ ЧЕРЕЗ ПОДФУНКЦИИ<sup>1</sup>**

А. А. Городилова

Получена полная характеристика APN-функций от  $n$  переменных через векторные подфункции от  $n - 1$  переменной, а именно: доказано, что векторная функция от  $n$  переменных — APN-функция, если и только если каждая из её подфункций от  $n - 1$  переменной либо APN-функция, либо имеет порядок дифференциальной равномерности 4, и при этом выполнены условия допустимости.

**Ключевые слова:** векторная булева функция, дифференциально  $\delta$ -равномерная функция, APN-функция.

Векторной булевой функцией  $F$  называется любое отображение  $F : \mathbb{Z}_2^n \rightarrow \mathbb{Z}_2^n$ . Векторную функцию можно рассматривать как набор из  $n$  координатных булевых функций от  $n$  переменных, т. е.  $F = (f_1, \dots, f_n)$ . Производной по направлению  $a \in \mathbb{Z}_2^n$  функции  $F$  называется векторная функция  $D_a F$ , определённая как  $D_a F(x) = F(x) \oplus F(x \oplus a)$  для всех  $x \in \mathbb{Z}_2^n$ . Векторная функция  $F$  называется дифференциально  $\delta$ -равномерной [1], если для любых  $a \neq 0, b$  уравнение  $F(x) \oplus F(x \oplus a) = b$  имеет не более  $\delta$  решений. Назовём порядком дифференциальной равномерности  $F$  минимальное  $\delta$ , такое, что  $F$  является дифференциально  $\delta$ -равномерной. Легко видеть, что минимально возможный порядок равен двум. APN-функцией (Almost Perfect Nonlinear) называется дифференциально 2-равномерная векторная функция.

Исследованию APN-функций посвящено большое число работ как в России (М. М. Глухов, В. А. Зиновьев, М. Э. Тужилин, Д. Г. Фон-дер-Флаас и др.), так и за рубежом (К. Nyberg, L. R. Knudsen, С. Carlet, L. Budaghyan, J. Dillon и др.). APN-функции представляют интерес для криптографических приложений, в частности для использования в качестве S-блоков в блочных шифрах, поскольку обеспечивают оптимальную стойкость к дифференциальному криптоанализу. Обзор известных APN-функций приводится в работе [2].

Пусть  $S$  — векторная функция от  $n$  переменных,  $S = (s_1, \dots, s_n)$ .

**Определение 1.** Назовём функции  $F, G, f, g$  набором подфункций  $S$ , если они получены из  $S$  при фиксации координаты  $x_i$  и функции  $s_j$ , где  $i, j = 1, \dots, n$ , следующим образом:

$$\begin{aligned} F(x) &= (s_1(\bar{x}_{i,0}), \dots, s_{j-1}(\bar{x}_{i,0}), s_{j+1}(\bar{x}_{i,0}), \dots, s_n(\bar{x}_{i,0})), & f(x) &= s_j(\bar{x}_{i,0}), \\ G(x) &= (s_1(\bar{x}_{i,1}), \dots, s_{j-1}(\bar{x}_{i,1}), s_{j+1}(\bar{x}_{i,1}), \dots, s_n(\bar{x}_{i,1})), & g(x) &= s_j(\bar{x}_{i,1}), \end{aligned}$$

где  $\bar{x}_{i,0} = (x_1, \dots, x_{i-1}, 0, x_i, \dots, x_{n-1})$  и  $\bar{x}_{i,1} = (x_1, \dots, x_{i-1}, 1, x_i, \dots, x_{n-1})$ .

В случае  $i = n, j = n$  функция  $S$  представляется через набор подфункций следующим образом (здесь  $x \in \mathbb{Z}_2^{n-1}, x_n \in \mathbb{Z}_2$ ):

$$S(x, x_n) = ((x_n \oplus 1)F(x) \oplus x_n G(x), (x_n \oplus 1)f(x) \oplus x_n g(x)).$$

**Определение 2.** Назовём набор функций  $F, G, f, g$  допустимым, где  $F, G$  — векторные, а  $f, g$  — булевы функции от  $n$  переменных, если выполнены следующие условия:

<sup>1</sup>Работа поддержана грантом НШ-1939.2014.1 Президента России для ведущих научных школ.

- (\*) для всех  $x, y, a \in \mathbb{Z}_2^n$ ,  $a \neq 0$ , хотя бы одно из равенств  $D_a F(x) = D_a G(y)$  и  $D_a f(x) = D_a g(y)$  нарушается;
- (\*\*) для всех  $x, y, a \in \mathbb{Z}_2^n$ ,  $a \neq 0$ ,  $x \neq y, y \oplus a$ , хотя бы одно из равенств  $D_a H(x) = D_a H(y)$  и  $D_a h(x) = D_a h(y)$  нарушается, где  $H = F$  и  $h = f$ , либо  $H = G$  и  $h = g$ .

Получена следующая теорема о характеристизации APN-функций через набор подфункций, обобщающая результат теоремы 3 из [3].

**Теорема 1.** Векторная функция  $S$  от  $n$  переменных — APN-функция тогда и только тогда, когда набор её подфункций  $F, G, f, g$  является допустимым и каждая из векторных функций  $F$  и  $G$  либо APN-функция, либо имеет порядок дифференциальной равномерности равный 4.

При малом числе переменных получена следующая характеристизация APN-функций от  $n$  переменных через векторные подфункции  $F$  и  $G$  от  $n - 1$  переменных:

	$n = 2$	$n = 3$	$n = 4$
Количество всех APN-функций от $n$ пер.	192	668 128	18 940 805 775 360
$F, G$ — APN-функции	192	589 824 = 6/7 от всех	4 419 521 347 584 = 7/30 от всех
$F, G$ — порядка диф. рав. 4	—	98 304 = 1/7 от всех	11 995 843 657 728 = 19/30 от всех
Одна функция — APN, другая — порядка диф. рав. 4	—	—	2 525 440 770 048 = 4/30 от всех

Вычисления для случая  $n = 4$  проводились на кластере НКС-30Т ССКЦ СО РАН.

#### ЛИТЕРАТУРА

1. Nyberg K. Differentially uniform mappings for cryptography // Eurocrypt 1993. LNCS. 1994. V. 765. P. 55–64.
2. Тузиллин М. Э. Почти совершенные нелинейные функции // Прикладная дискретная математика. 2009. № 3. С. 14–20.
3. Фролова А. А. Итеративная конструкция APN-функций // Прикладная дискретная математика. Приложение. 2013. № 6. С. 24–25.

УДК 519.716.32+519.854

### КЛАССИФИКАЦИЯ ФУНКЦИЙ НАД ПРИМАРНЫМ КОЛЬЦОМ ВЫЧЕТОВ В СВЯЗИ С МЕТОДОМ ПОКООРИНАТНОЙ ЛИНЕАРИЗАЦИИ

М. В. Заец

Известно, что для решения систем полиномиальных уравнений над примарным кольцом вычетов можно применять метод покоординатной линейаризации. Рассматривается классификация функций над примарным кольцом вычетов, порождающих системы уравнений, для которых также применим указанный метод. Класс полиномиальных функций расширяется классом вариационно-координатно-полиномиальных функций (ВКП-функций), который, в свою очередь, расширяется классом квази-ВКП-функций и классом координатно-линейно разрешимых функций. Описываются свойства введенных классов функций.

**Ключевые слова:** полиномиальные функции, вариационно-координатно-полиномиальные функции, ВКП-функции, квази-ВКП-функции, координатно-линейно разрешимые функции, метод покоординатной линеаризации, системы уравнений.

Исследование систем уравнений над кольцом  $\mathbb{Z}_{p^m}$

$$\begin{cases} f_1(\mathbf{x}) = y_1, \\ \vdots \\ f_t(\mathbf{x}) = y_t, \end{cases} \quad (1)$$

позволяет выделить некоторые классы функций, для которых система (1) обладает свойством внутренней структурности.

Любой элемент  $a$  примарного кольца вычетов  $\mathbb{Z}_{p^m}$ , где  $m \in \mathbb{N}$ ,  $m > 1$  и  $p$  простое, можно однозначно представить в виде

$$a = a^{(0)} + p \cdot a^{(1)} + \dots + p^{m-1} \cdot a^{(m-1)},$$

где  $a^{(j)} \in \mathcal{B} = \{0, \dots, p-1\}$ , называемом разложением элемента  $a$  в  $p$ -ичном координатном множестве  $\mathcal{B}$ . Отображения

$$\gamma_j : \mathbb{Z}_{p^m} \rightarrow \mathcal{B}, \quad \gamma_j(a) = a^{(j)}, \quad j = 0, \dots, m-1,$$

называются координатными функциями в координатном множестве  $\mathcal{B}$ , а элементы  $a^{(j)} = \gamma_j(a) \in \mathcal{B}$  — координатами  $j$ -го порядка элемента  $a$  в координатном множестве  $\mathcal{B}$ . Если при этом ввести на  $\mathcal{B}$  операции сложения  $\oplus$  и умножения  $\otimes$  по правилу

$$a \oplus b = \gamma_0(a + b), \quad a \otimes b = \gamma_0(a \cdot b), \quad a, b \in \mathcal{B},$$

то алгебра  $(\mathcal{B}, \oplus, \otimes) \cong \text{GF}(p)$  будет являться полем из  $p$  элементов. В работе рассмотрены классы функций над примарным кольцом вычетов  $\mathbb{Z}_{p^m}$ , обобщающие в некотором смысле класс  $\mathcal{P}_{p^m}(n)$  — полиномиальных функций над данным кольцом. В [1] в общем случае для GE-колец (колец Галуа — Эйзенштейна, т. е. конечных коммутативных цепных колец) показано, что системы полиномиальных уравнений могут быть решены методом покоординатной линеаризации. Данный метод заключается в последовательном нахождении координат неизвестных переменных. Сначала находятся младшие координаты неизвестных переменных путём решения исходной системы над полем  $\mathcal{B}$ , приведённой по модулю  $p$ . Затем находятся остальные координаты путём многократного решения  $m-1$  систем линейных уравнений над полем  $\mathcal{B}$ . Показано, что данным свойством обладают не только системы полиномиальных уравнений.

**Определение 1.** Для функции  $f(\mathbf{x}) : \mathbb{Z}_{p^m}^n \rightarrow \mathbb{Z}_{p^m}$  и  $j \in \{0, \dots, m-1\}$  отображение  $\gamma_j f : \mathbb{Z}_{p^m}^n \rightarrow \mathcal{B}$ , определяемое по правилу

$$\gamma_j f(\alpha) = \gamma_j(f(\alpha))$$

для всех  $\alpha \in \mathbb{Z}_{p^m}^n$ , будем называть её  $j$ -й координатной функцией, или  $j$ -м координатным отображением.

**Определение 2.** Функцию  $f(\mathbf{x}) : \mathbb{Z}_{p^m}^n \rightarrow \mathbb{Z}_{p^m}$  назовём вариационно-координатно-полиномиальной (или ВКП-функцией), если для любого  $j \in \{0, \dots, m-1\}$  существует полиномиальная функция  $p_j(\mathbf{x}) \in \mathcal{P}_{p^m}(n)$ ,  $j$ -я координатная функция которой совпадает с  $j$ -й координатной функцией функции  $f(\mathbf{x})$ , т. е. выполняется равенство

$$\gamma_j f(\mathbf{x}) = \gamma_j p_j(\mathbf{x}), \quad j = 0, \dots, m-1.$$

**Определение 3.** Функцию  $f(\mathbf{x}): \mathbb{Z}_{p^m}^n \rightarrow \mathbb{Z}_{p^m}$  назовем квазивариационно-координатно-полиномиальной (или квази-ВКП-функцией), если выполнены условия:

- 1)  $\gamma_0 f(\mathbf{x}) = \gamma_0 f(\mathbf{x}^{(0)}) = g_0(\mathbf{x}^{(0)})$ ,  $g_0: \mathcal{B}^n \rightarrow \mathcal{B}$ ;
- 2) для любого  $j \in \{0, \dots, m-1\}$  существуют функции  $g_{ji}: \mathcal{B}^n \rightarrow \mathcal{B}$ ,  $g_j: \mathcal{B}^{j^n} \rightarrow \mathcal{B}$ ,  $i = 1, \dots, n$ , над полем  $\mathcal{B}$ , такие, что справедливо равенство

$$\gamma_j f(\mathbf{x}^{(0)}, \dots, \mathbf{x}^{(j)}) = \sum_{i=1}^n g_{ji}(\mathbf{x}^{(0)}) \otimes x_i^{(j)} \oplus g_j(\mathbf{x}^{(0)}, \dots, \mathbf{x}^{(j-1)}).$$

**Определение 4.** Функцию  $f(\mathbf{x}): \mathbb{Z}_{p^m}^n \rightarrow \mathbb{Z}_{p^m}$  назовем координатно  $\mathcal{L}$ -линейно разрешимой (или  $\mathcal{L}$ -КЛР-функцией), где  $\mathcal{L} \subseteq \{0, \dots, m-1\}$ , если  $\gamma_j f(\mathbf{x}) = \gamma_j f(\mathbf{x}^{(0)}, \dots, \mathbf{x}^{(j)})$ ,  $j = 0, \dots, m-1$ , и при любом  $j \in \mathcal{L}$ ,  $j \neq 0$ , существуют такие функции  $g_{ji}, g_j: \mathcal{B}^{n^j} \rightarrow \mathcal{B}$ ,  $i = 1, \dots, n$ , что

$$\gamma_j f(\mathbf{x}) = \sum_{i=1}^n g_{ji}(\mathbf{x}^{(0)}, \dots, \mathbf{x}^{(j-1)}) \otimes x_i^{(j)} \oplus g_j(\mathbf{x}^{(0)}, \dots, \mathbf{x}^{(j-1)}),$$

и при  $0 \in \mathcal{L}$  существуют такие  $g_{0i}, g_0 \in \mathcal{B}$ ,  $i = 1, \dots, n$ , что

$$\gamma_0 f(\mathbf{x}) = \sum_{i=1}^n g_{0i} \otimes x_i^{(0)} \oplus g_0.$$

Класс всех ВКП-функций от  $n$  переменных над  $\mathbb{Z}_{p^m}$  обозначим через  $\mathcal{CP}_{p^m}(n)$ . Класс всех квази-ВКП-функций от  $n$  переменных над кольцом  $\mathbb{Z}_{p^m}$  обозначим  $\mathcal{QCP}_{p^m}(n)$ . При заданном подмножестве  $\mathcal{L} \subseteq \{0, \dots, m-1\}$  обозначим класс всех  $\mathcal{L}$ -КЛР-функций от  $n$  переменных над  $\mathbb{Z}_{p^m}$  через  $\mathcal{CLS}_{p^m}^{\mathcal{L}}(n)$ . Обозначим через  $\mathcal{D}_{p^m}(n)$  класс всех функций над  $\mathbb{Z}_{p^m}$  от  $n$  переменных, сохраняющих отношение сравнимости по любому делителю  $p^m$  или, что то же самое, сохраняющих любую конгруэнцию кольца  $\mathbb{Z}_{p^m}$ . Соотношения между данными классами функций устанавливает следующее утверждение.

**Утверждение 1.** Если  $\mathcal{L} \subseteq \{1, \dots, m-1\}$ , то справедлива цепочка включений

$$\mathcal{P}_{p^m}(n) \subseteq \mathcal{CP}_{p^m}(n) \subseteq \mathcal{QCP}_{p^m}(n) \subseteq \mathcal{CLS}_{p^m}^{\mathcal{L}}(n) \subseteq \mathcal{D}_{p^m}(n).$$

При этом если  $\mathcal{L} \not\subseteq \{1, \dots, m-1\}$ , то  $\mathcal{QCP}_{p^m}(n) \not\subseteq \mathcal{CLS}_{p^m}^{\mathcal{L}}(n)$ .

**Теорема 1.** Пусть  $\mathcal{L} = \{1, \dots, m-1\}$ , тогда справедливы утверждения:

- 1) верна цепочка равенств

$$\mathcal{P}_{p^2}(n) = \mathcal{CP}_{p^2}(n) = \mathcal{QCP}_{p^2}(n) = \mathcal{CLS}_{p^2}^{\mathcal{L}}(n);$$

- 2) при  $m \geq 3$  верна цепочка включений

$$\mathcal{P}_{p^m}(n) \subsetneq \mathcal{CP}_{p^m}(n) \subseteq \mathcal{QCP}_{p^m}(n) \subsetneq \mathcal{CLS}_{p^m}^{\mathcal{L}}(n).$$

**Теорема 2.** Классы  $\mathcal{CLS}_{p^m}^{\mathcal{L}}(n)$  и  $\mathcal{D}_{p^m}(n)$  при  $\mathcal{L} = \{1, \dots, m-1\}$  совпадают тогда и только тогда, когда одновременно  $p = 2$  и  $n = 1$ .

**Следствие 1.** Справедливы следующие равенства классов функций над  $\mathbb{Z}_4$ :

$$\mathcal{P}_4(1) = \mathcal{CP}_4(1) = \mathcal{QCP}_4(1) = \mathcal{CLS}_4^{\{1\}}(1) = \mathcal{D}_4(1).$$

**Утверждение 2.** При любых  $n \in \mathbb{N}$  и  $\mathcal{L} \subseteq \{0, \dots, m-1\}$  класс  $\mathcal{L}$ -КЛР-функций  $\mathcal{CLS}_{p^m}^{\mathcal{L}}(n)$  является замкнутым, то есть  $[\mathcal{CLS}_{p^m}^{\mathcal{L}}(n)] = \mathcal{CLS}_{p^m}^{\mathcal{L}}(n)$ .

**Утверждение 3.** При любом  $n \in \mathbb{N}$  класс квази-ВКП-функций  $\mathcal{QCP}_{p^m}(n)$  является замкнутым, то есть  $[\mathcal{QCP}_{p^m}(n)] = \mathcal{QCP}_{p^m}(n)$ .

Последние два утверждения приводят к интересному результату. При  $m \geq 3$  в соответствии с теоремой 2 имеем цепочку включений:  $\mathcal{P}_{p^m}(n) \subsetneq \mathcal{CP}_{p^m}(n) \subseteq \mathcal{QCP}_{p^m}(n) \subsetneq \mathcal{CLS}_{p^m}^{\{1, \dots, m-1\}}(n)$ . При этом в ней классы  $\mathcal{P}_{p^m}(n)$ ,  $\mathcal{QCP}_{p^m}(n)$ ,  $\mathcal{CLS}_{p^m}^{\{1, \dots, m-1\}}(n)$  являются замкнутыми и не равными друг другу.

Все четыре рассматриваемых класса  $\mathcal{P}_{p^m}(n)$ ,  $\mathcal{CP}_{p^m}(n)$ ,  $\mathcal{QCP}_{p^m}(n)$ ,  $\mathcal{CLS}_{p^m}^{\{1, \dots, m-1\}}(n)$  обладают тем свойством, что системы уравнений (1), порождённые одним из них (т. е. системы, левые части которых  $f_i(\mathbf{x})$  принадлежат ему), могут быть решены методом покоординатной линеаризации. Данный метод на самом деле является обобщением метода, предложенного в работах А. А. Нечаева и Д. А. Михайлова для класса полиномиальных функций. Для случая примарных колец вычетов  $\mathbb{Z}_{2^m}$  его изложение опубликовано в работах [2, 3].

#### ЛИТЕРАТУРА

1. Михайлов Д. А., Нечаев А. А. Решение системы полиномиальных уравнений над кольцом Галуа — Эйзенштейна с помощью канонической системы образующих полиномиального идеала // Дискретная математика. 2004. Т. 1. Вып. 1. С. 21–51.
2. Заец М. В., Никонов В. Г., Шшиков А. Б. Функции с вариационно-координатной полиномиальностью и их свойства // Открытое образование. 2012. № 3. С. 57–61.
3. Заец М. В., Никонов В. Г., Шшиков А. Б. Класс функций с вариационно-координатной полиномиальностью над кольцом  $\mathbb{Z}_{2^m}$  и его обобщение // Матем. вопросы криптографии. 2013. Т. 4. Вып. 3. С. 19–45.

УДК 512.552.18

### ИССЛЕДОВАНИЕ КЛАССА ДИФФЕРЕНЦИРУЕМЫХ ФУНКЦИЙ В КОЛЬЦАХ КЛАССОВ ВЫЧЕТОВ ПО ПРИМАРНОМУ МОДУЛЮ

А. С. Ивачев

Для класса  $D_n$  дифференцируемых по модулю  $p^n$  функций, являющегося обобщением класса полиномиальных функций, найдены подмножества функций  $A_n$ ,  $B_n$ ,  $C_n$ , такие, что для каждой функции из  $D_n$  существует единственное представление через функции подмножеств  $A_n$ ,  $B_n$ ,  $C_n$ . С помощью этого представления получены число всех функций, число биективных функций и число транзитивных функций класса  $D_n$ . Из полученных мощностных соотношений следует, что в множество транзитивных дифференцируемых по модулю  $p^2$  функций входят только полиномиальные функции, однако при подъёме модуля множество дифференцируемых транзитивных функций начинает отличаться от множества транзитивных полиномиальных функций. Показано, что для обратимости функции из  $D_n$  необходимым и достаточным условием является её обратимость по модулю  $p$  и равенство нулю производных по всем модулям  $p^i$ ,  $i = 2, \dots, n$ . Получена рекуррентная формула для вычисления обратной функции. Найдены условия транзитивности функций, из которых следует, что из любой транзитивной дифференцируемой по модулю  $p^{n-1}$  функции можно построить транзитивную дифференцируемую по модулю  $p^n$  функцию, совпадающую с первой по модулю  $p^{n-1}$ .

**Ключевые слова:** рекуррентная последовательность, дифференцируемая функция, обратная функция, биективная функция, транзитивная функция.

Генерация последовательностей больших периодов, состоящих из элементов конечного кольца, является важной задачей. Для генерации последовательности может использоваться следующая формула:

$$x_{i+1} = f(x_i), \quad (1)$$

где  $f$  — некоторая функция над кольцом  $\mathbb{Z}_{p^n}$ .

Возникает проблема выбора такой функции  $f$ , чтобы она легко вычислялась и генерировала последовательность максимального периода  $p^n$ .

Над кольцом  $\mathbb{Z}_{p^n}$  известен класс полиномиальных функций. Существуют функции этого класса, соответствующие указанным требованиям, однако их доля среди множества всех функций над  $\mathbb{Z}_{p^n}$  мала. Так появляется задача изучения новых классов функций над  $\mathbb{Z}_{p^n}$ . В данной работе рассматривается класс дифференцируемых по модулю  $p^n$  функций. Подобный класс был определён в [1].

Для функции  $f : \mathbb{Z}_{p^n} \rightarrow \mathbb{Z}_{p^n}$  будем обозначать  $f \bmod p^i$  функцию  $g$  из  $\mathbb{Z}_{p^i}$  в  $\mathbb{Z}_{p^i}$ , такую, что  $g(x) = f(x) \bmod p^i$ , подразумевая, что  $g$  определена корректно.

**Определение 1.** Любая функция  $f : \mathbb{Z}_p \rightarrow \mathbb{Z}_p$  является дифференцируемой по модулю  $p$ . Функция  $f : \mathbb{Z}_{p^n} \rightarrow \mathbb{Z}_{p^n}$  называется *дифференцируемой по модулю  $p^n$*  ( $n > 1$ ), если:

- 1)  $f \bmod p^i$  — дифференцируемая по модулю  $p^i$  функция,  $i = 1, \dots, n-1$ ;
- 2)  $f(x + ap^{n-1}) = f(x) + ap^{n-1}f'(x) \pmod{p^n}$ , где  $f'$  — некоторая функция из  $\mathbb{Z}_{p^n}$  в  $\mathbb{Z}_{p^n}$ . Функция  $f'$  называется производной функции  $f$  по модулю  $p^n$ .

Класс дифференцируемых функций обозначается  $D_n$ .

Класс дифференцируемых функций включает в себя класс полиномиальных функций и замкнут относительно сложения, умножения, операции композиции функций. Каждую функцию  $f$  над  $\mathbb{Z}_{p^n}$  можно представить в виде

$$f(x) = \sum_{i=0}^{n-1} f_i(x)p^i,$$

где  $f_i$  принимают значение в множестве  $\{0, 1, \dots, p-1\}$ .

Такое представление назовём координатным представлением функции  $f$ , а  $f_i$  — координатными функциями, или координатами функции  $f$ . Координатные функции  $f_i$  дифференцируемой функции  $f$  обладают следующим свойством:

$$f_i(x) = f_i(x + ap^{n-1}), \quad i = 0, \dots, n-2.$$

Из определения 1 следует, что функция  $f'$  тогда и только тогда является производной некоторой функции, когда её первая координата не зависит от последней координаты  $x$ , то есть  $f'(x + ap^{n-1}) \equiv f'(x) \pmod{p}$  для любого  $a$  из  $\mathbb{Z}_{p^n}$ .

Определим следующие множества:

- 1)  $A_n = \{f : f \in D_n \wedge f_{n-1}(x) = 0\}$ ;
- 2)  $B_n = \{f : f(x + ap^{n-1}) \equiv f(x) \pmod{p^n} \wedge f(x) \equiv 0 \pmod{p^{n-1}}\}$ ;
- 3)  $C_n = \{f : f(x) = x_{n-1}p^{n-1}h'(x), h' — производная некоторой функции из  $D_n\}$ .$

Из определения множеств  $A_n, B_n, C_n$  следует, что они являются подмножествами  $D_n$ . Для функций из данных множеств справедливо следующее утверждение.

**Утверждение 1.** Для любой функции  $f$  из  $D_n$  существует единственная тройка  $(f_A, f_B, f_C)$ , где  $f_A \in A_n$ ,  $f_B \in B_n$ ,  $f_C \in C_n$ , такая, что  $f(x) = f_A(x) + f_B(x) + f_C(x)$ . Обратно, для каждой тройки  $(f_A, f_B, f_C)$ ,  $f_A \in A_n$ ,  $f_B \in B_n$ ,  $f_C \in C_n$ , существует  $f$  из  $D_n$ , такая, что  $f(x) = f_A(x) + f_B(x) + f_C(x)$ .

**Следствие 1.**  $|D_n| = |A_n| \cdot |B_n| \cdot |C_n|$ .

Между  $A_n$  и  $D_{n-1}$  существует биекция  $\pi_n$ , такая, что  $\pi_n(f) = f \bmod p^{n-1}$ , и соответственно  $|D_{n-1}| = |A_n|$ .

**Следствие 2.** Число дифференцируемых функций равно  $p^{p+2p(p^{n-1}-1)/(p-1)}$ .

**Определение 2.** Дифференцируемая по модулю  $p^n$  функция  $f$  называется *обратимой* (или *биективной*), если существует функция  $g$ , такая, что  $g(f(x)) = x$ . Функция  $g$  называется обратной для функции  $f$ .

Обратная функция для дифференцируемой биективной функции также является дифференцируемой. Следующее утверждение представляет собой критерий обратимости функции.

**Утверждение 2.** Пусть  $f \in D_n$ . Тогда  $f$  обратима тогда и только тогда, когда  $f \bmod p$  обратима и производные функций  $f \bmod p^i$ , где  $i = 2, \dots, n$ , не обращаются в 0 при любом значении  $x$ .

**Следствие 3.** Число биективных дифференцируемых функций равно

$$p!((p-1)p)^{p(p^{n-1}-1)/(p-1)}.$$

В следующем утверждении приведена формула для обратной функции:

**Утверждение 3.** Пусть  $f$  — обратимая дифференцируемая функция и  $g$  — обратная к  $f$ . Тогда справедлива следующая формула:

$$g(x) = g(x) \bmod p^{n-1} - g'(x)(f(g(x) \bmod p^{n-1}) - f(g(x) \bmod p^{n-1}) \bmod p^{n-1} - x_{n-1}p^{n-1}).$$

**Определение 3.** Дифференцируемая по модулю  $p^n$  функция называется *транзитивной*, если она индуцирует одноцикловую подстановку на  $\mathbb{Z}_{p^n}$ .

Введём следующие обозначения:

$$f^{[k]}(x) = \underbrace{f(f(\dots f(x)\dots))}_{k \text{ раз}},$$

$$a(n, m, f_A, f', x) = \prod_{k=1}^{mp^n} f'(f_A^{[mp^n-k]}(x)) \pmod{p},$$

$$b(n, m, f_A, f_B, f', x) = \sum_{k=1}^{mp^n} f_B(f_A^{[mp^n-k]}(x)) \prod_{j=1}^{k-1} f'(f_A^{[mp^n-j]}(x)).$$

**Утверждение 4.** Пусть  $f \in D_n$ . Тогда  $f$  транзитивна тогда и только тогда, когда  $f \bmod p^{n-1}$  транзитивна в  $D_{n-1}$ ,  $a(n-1, 1, f_A, f', 0) = 1$  и  $b(n-1, 1, f_A, f_B, f', 0) \neq 0$ .

**Следствие 4.** Число транзитивных дифференцируемых функций равно

$$(p-1)!(p-1)^{p(p^{n-1}-1)/(p-1)} p^{p(p^{n-1}-1)/(p-1)-n+1}.$$

Транзитивные дифференцируемые функции составляют долю  $1/p^n$  в множестве биективных дифференцируемых функций. По модулю  $p^2$  все биективные, а соответственно и транзитивные дифференцируемые функции являются полиномиальными вследствие формул для числа биективных и транзитивных полиномиальных функций, приведённых в [2]. Однако производная дифференцируемой функции зависит от  $n - 1$  первых координат  $x$  и при подъёме модуля в общем случае производная по большему модулю не зависит от производных по меньшему модулю, в то время как производная полиномиальной функции зависит только от первой координаты и при подъёме модуля не изменяется. Таким образом, по модулю  $p^n$ ,  $n > 2$ , число транзитивных дифференцируемых функций больше, чем число транзитивных полиномиальных функций. Однако ещё не известно представлений для дифференцируемых функций, позволяющих эффективно вычислять их. Таким образом, появляется задача поиска таких представлений для функций класса  $D_n$ . Если такие представления будут найдены, то дифференцируемые функции могут быть использованы для генерации последовательностей элементов из  $\mathbb{Z}_{p^n}$  по формуле (1).

#### ЛИТЕРАТУРА

1. Анашкин В. С. Равномерно распределённые последовательности целых  $p$ -адических чисел // Дискретная математика. 2002. № 14:4. С. 3–64.
2. Ларин М. В. Транзитивные полиномиальные преобразования колец вычетов // Дискретная математика. 2002. № 14:2. С. 20–32.

УДК 519.7

### ВЕРХНЯЯ ОЦЕНКА ЧИСЛА БЕНТ-ФУНКЦИЙ НА РАССТОЯНИИ $2^k$ ОТ ПРОИЗВОЛЬНОЙ БЕНТ-ФУНКЦИИ ОТ $2k$ ПЕРЕМЕННЫХ<sup>1</sup>

Н. А. Коломеец

Получена верхняя оценка числа бент-функций на расстоянии  $2^k$  от произвольной бент-функции от  $2k$  переменных. Установлено, что она достигается только для квадратичных бент-функций. Введено понятие полной аффинной расщепляемости булевой функции. Доказано, что полностью аффинно расщепляемыми могут быть только аффинные и квадратичные функции.

**Ключевые слова:** булевы функции, бент-функции, квадратичные бент-функции.

Функция  $f : \mathbb{Z}_2^n \rightarrow \mathbb{Z}_2$  называется *булевой функцией* от  $n$  переменных. Булева функция называется *аффинной*, если степень её алгебраической нормальной формы не превосходит 1, и *квадратичной*, если степень равна 2. Заметим, что любая аффинная функция от  $n$  переменных представима в виде  $f(x) = \langle a, x \rangle \oplus c$ , где  $a \in \mathbb{Z}_2^n$ ;  $c \in \mathbb{Z}_2$ ;  $\langle a, x \rangle = a_1x_1 \oplus \dots \oplus a_nx_n$ . *Расстояние* между двумя булевыми функциями от  $n$  переменных — расстояние Хэмминга между векторами их значений. *Бент-функция* — булева функция от чётного числа переменных, находящаяся на максимально возможном расстоянии от множества всех аффинных функций. Подробнее о бент-функциях можно узнать в работах [1, 2]. Множество  $s \oplus D = \{s \oplus x : x \in D\}$  называется *сдвигом* множества  $D \subseteq \mathbb{Z}_2^n$ ,  $s \in \mathbb{Z}_2^n$ . *Аффинное подпространство*  $\mathbb{Z}_2^n$  — сдвиг некоторого линейного подпространства  $\mathbb{Z}_2^n$ . *Размерностью* аффинного подпространства называется размер-

<sup>1</sup>Работа поддержана грантом НШ-1939.2014.1 Президента России для ведущих научных школ.

ность соответствующего линейного подпространства. Для краткости будем называть аффинное подпространство просто *подпространством*.

Булева функция  $f$  от  $n$  переменных *аффинна на подпространстве*  $L \subseteq \mathbb{Z}_2^n$ , если для некоторых  $a \in \mathbb{Z}_2^n$  и  $c \in \mathbb{Z}_2$  верно, что  $f(x) = \langle a, x \rangle \oplus c$  для всех  $x \in L$ . Булева функция  $f$  называется *аффинно расщепляемой по подпространству*  $L$ , если она аффинна на всех сдвигах  $L$ . Аффинность булевых функций на подпространствах рассматривали М. Л. Буряков, О. А. Логачев, А. А. Сальников, С. В. Смышляев, В. В. Яценко [1, 3, 4], а также применительно к бент-функциям Х. Доббертин, К. Карле и П. Шарпин [5–7].

Введём следующее понятие.

**Определение 1.** Булева функция  $f$  от  $n$  переменных называется *полностью аффинно расщепляемой* порядка  $k$ ,  $2 \leq k \leq n$ , если она аффинна хотя бы на одном подпространстве  $\mathbb{Z}_2^n$  размерности  $k$  и аффинно расщепляема по всем подпространствам размерности  $k$ , на которых она аффинна.

Приведём примеры полностью аффинно расщепляемых функций.

**Утверждение 1.** Справедливы следующие утверждения:

(i) Любая квадратичная функция от  $n$  переменных является полностью аффинно расщепляемой порядка  $k$  при  $2 \leq k \leq \lceil n/2 \rceil$ .

(ii) Функция  $g(x_1, \dots, x_n) = x_1x_2 \oplus x_3x_4 \oplus \dots \oplus x_{2n-2k-1}x_{2n-2k}$ , где  $\lceil n/2 \rceil \leq k < n$ , является полностью аффинно расщепляемой порядка  $k$ .

(iii) Булева функция является полностью аффинно расщепляемой любого возможного порядка тогда и только тогда, когда она аффинная.

В работе [8] установлено, что все полностью аффинно расщепляемые функции порядка  $\lceil n/2 \rceil$  являются аффинными или квадратичными ( $n$  — число переменных). В данной работе мы обобщаем этот результат.

**Теорема 1.** Пусть  $f$  — булева функция от  $n$  переменных и  $f$  полностью аффинно расщепляемая порядка  $k$ ,  $2 \leq k < n$ . Тогда

(i)  $f$  либо аффинная, либо квадратичная;

(ii) если  $k \geq \lceil n/2 \rceil$  и  $f$  не является полностью аффинно расщепляемой порядка  $k+1$ , то  $f$  аффинно эквивалентна функции  $g(x_1, \dots, x_n) = x_1x_2 \oplus x_3x_4 \oplus \dots \oplus x_{2n-2k-1}x_{2n-2k}$ .

Напомним, что две булевы функции  $f$  и  $g$  от  $n$  переменных называются *аффинно эквивалентными*, если существует невырожденная двоичная матрица  $A$  размера  $n \times n$ , вектор  $b \in \mathbb{Z}_2^n$  и аффинная функция  $\ell$  от  $n$  переменных, такие, что  $f(x) = g(Ax \oplus b) \oplus \ell(x)$  для всех  $x \in \mathbb{Z}_2^n$ .

Известно [5], что если  $f$  — бент-функция от  $2k$  переменных,  $L$  — подпространство  $\mathbb{Z}_2^{2k}$  размерности  $k$  и  $f$  аффинна на  $L$ , то  $f \oplus \text{Ind}_L$  также является бент-функцией, где  $\text{Ind}_L$  — характеристическая функция множества  $L$ . В работе [9] доказано, что все бент-функции на расстоянии  $2^k$  от бент-функции  $f$  можно построить таким способом. Заметим также, что  $2^k$  является минимальным возможным расстоянием между двумя бент-функциями от  $2k$  переменных. Таким образом, подпространства размерности  $k$ , на которых бент-функция аффинна, представляют особый интерес.

В данной работе получена верхняя оценка числа бент-функций на расстоянии  $2^k$  от произвольной бент-функции.

**Теорема 2.** Пусть  $f$  — произвольная бент-функция от  $2k$  переменных. Тогда существует не более чем  $2^k(2^1 + 1) \cdot \dots \cdot (2^k + 1)$  бент-функций на расстоянии  $2^k$  от  $f$ . При этом оценка достигается, если и только если  $f$  — квадратичная бент-функция.

Достижимость оценки только на квадратичных бент-функциях следует из теоремы 1.

#### ЛИТЕРАТУРА

1. *Логачев О. А., Сальников А. А., Смышляев С. В., Яценко В. В.* Булевы функции в теории кодирования и криптологии. 2-е изд. М.: МЦНМО, 2012.
2. *Токарева Н. Н.* Нелинейные булевы функции: бент-функции и их обобщения. Saarbrücken: LAP LAMBERT Academic Publishing, 2011.
3. *Буряков М. Л.* Алгебраические, комбинаторные и криптографические свойства параметров аффинных ограничений булевых функций: дис. ... канд. физ.-мат. наук. М., 2007.
4. *Логачев О. А.* О значениях уровня аффинности для почти всех булевых функций // Прикладная дискретная математика. 2010. №3. С. 17–21.
5. *Carlet C.* Two new classes of bent functions // EUROCRYPT'93. LNCS. 1994. V. 765. P. 77–101.
6. *Charpin P.* Normal Boolean functions // J. Complexity. 2004. V. 20. P. 245–265.
7. *Dobbertin H.* Construction of bent functions and balanced Boolean functions with high nonlinearity // LNCS. 1994. V. 1008. P. 61–74.
8. *Коломеец Н. А.* Об аффинности булевых функций на подпространствах и их сдвигах // Прикладная дискретная математика. Приложение. 2013. №6. С. 15–16.
9. *Коломеец Н. А., Павлов А. В.* Свойство бент-функций, находящихся на минимальном расстоянии друг от друга // Прикладная дискретная математика. 2009. №4. С. 5–20.

УДК 519.7

### ОЦЕНКИ НЕЛИНЕЙНОСТИ ВЕКТОРНЫХ БУЛЕВЫХ ФУНКЦИЙ СПЕЦИАЛЬНОГО ВИДА

Е. П. Корсакова

Получена верхняя оценка нелинейности векторных булевых функций, построенных из аффинных булевых функций. Построен пример функций, на которых оценка достижима. Получена нижняя оценка числа векторных функций с фиксированной нелинейностью, построенных из уравновешенных булевых функций.

**Ключевые слова:** векторная булева функция, нелинейность, аффинная функция, уравновешенность.

Векторные булевы функции, используемые в криптографических приложениях, должны обладать рядом специальных свойств для обеспечения стойкости к известным видам криптоанализа и иметь относительно простую структуру [1–3]. Задачи совмещения различных свойств функции, а также оценки числа функций с выделенными свойствами являются сложными. Данная работа посвящена изучению нелинейности векторных булевых функций при относительно простом способе их построения и совмещению свойств нелинейности и уравновешенности.

*Булевой функцией* от  $n$  переменных называется функция, действующая из  $\mathbb{Z}_2^n$  в  $\mathbb{Z}_2$ . Каждая булева функция однозначно задается своей *алгебраической нормальной формой* (АНФ), т. е. представляется в виде  $f(x) = \left( \bigoplus_{k=1}^n \bigoplus_{i_1, \dots, i_k} a_{i_1, \dots, i_k} x_{i_1} \cdot \dots \cdot x_{i_k} \right) \oplus a_0$ , где  $\{i_1, \dots, i_k\} \subseteq \{1, \dots, n\}$  и  $a_{i_1, \dots, i_k}, a_0 \in \mathbb{Z}_2$ . *Степенью*  $\deg f$  булевой функции  $f$  называется число переменных в самом длинном слагаемом её АНФ. Булева функция называется *аффинной*, если её степень не превосходит 1. Множество всех аффинных

функций от  $n$  переменных обозначим через  $\mathfrak{A}_n$ . *Нелинейностью* булевой функции  $f : \mathbb{Z}_2^n \rightarrow \mathbb{Z}_2$  называется число  $Nl(f) = \text{dist}(f, \mathfrak{A}_n)$ , где  $\text{dist}(\cdot, \cdot)$  — расстояние Хэмминга между булевыми функциями. *Векторной булевой функцией* называется функция вида  $F : \mathbb{Z}_2^n \rightarrow \mathbb{Z}_2^m$ . *Нелинейностью* векторной булевой функции  $F : \mathbb{Z}_2^n \rightarrow \mathbb{Z}_2^m$ , где  $F = (f_1, f_2, \dots, f_m)$ , называется число  $Nl(F) = \min_{b \in \mathbb{Z}_2^{m*}} \text{dist}\left(\bigoplus_{i=1}^m b_i f_i, \mathfrak{A}_n\right)$ .

Для нелинейности векторной булевой функции от  $n$  переменных имеется та же верхняя оценка, что и в случае обычной булевой функции:  $Nl(F) \leq 2^{n-1} - 2^{n/2-1}$ . При  $m \geq n - 1$  данная оценка была улучшена В. М. Сидельниковым [4].

Для класса векторных булевых функций, построенных из аффинных, найдена следующая оценка нелинейности.

**Теорема 1.** Пусть  $F_1 = (f_{11}, \dots, f_{1m})$  и  $F_2 = (f_{21}, \dots, f_{2m})$  — функции, действующие из  $\mathbb{Z}_2^{n-1}$  в  $\mathbb{Z}_2^m$ , и  $f_{ij}$  — аффинные функции для всех  $i = 1, 2, j \in \{1, \dots, m\}$ . Тогда для функции  $F : \mathbb{Z}_2^n \rightarrow \mathbb{Z}_2^m$ , определённой правилом  $F(x, 0) = F_1(x)$ ,  $F(x, 1) = F_2(x)$  для каждого  $x \in \mathbb{Z}_2^{n-1}$ , справедлива оценка  $Nl(F) \leq 2^{n-2}$ , причём при  $m \leq n/2$  данная оценка достижима.

Пусть  $(n - 1, m)$ -функция  $F = (f_1, \dots, f_m)$  с аффинными координатными функциями задаётся двоичной  $(n \times m)$ -матрицей  $A(F) = (a_{ij})$ , где  $a_{ij}$  получены из АНФ соответствующих функций  $f_j(x_1, \dots, x_{n-1}) = \bigoplus_{i=1}^{n-1} a_{ij} x_i \oplus a_{nj}$ . Тогда при  $m \leq n/2$  оценка из теоремы 1 достижима на  $(n - 1, m)$ -функциях с матрицами  $A(F_1) = \begin{pmatrix} A \\ 0 \end{pmatrix}$ ,  $A(F_2) = \begin{pmatrix} 0 \\ B \end{pmatrix}$ , где  $A$  и  $B$  —  $(m \times m)$ -матрицы полного ранга.

Полученная в теореме 1 оценка нелинейности векторных булевых функций, построенных из аффинных булевых функций, слаба по сравнению с известными оценками, поскольку  $\lim_{n \rightarrow \infty} (2^{n-1} - 2^{(n-1)/2} - 2^{n-2}) = \infty$  и  $\lim_{n \rightarrow \infty} \frac{2^{n-1} - 2^{(n-1)/2}}{2^{n-2}} = 2$ . То есть максимум нелинейности функций из описанного класса приблизительно в 2 раза меньше максимально возможного значения нелинейности. Это позволяет сделать вывод, что в данном классе нет функций с хорошими нелинейными свойствами.

Булева функция  $f : \mathbb{Z}_2^n \rightarrow \mathbb{Z}_2$  называется *уравновешенной*, если она принимает значения 0 и 1 одинаково часто. Рассмотрим множество векторных булевых функций  $F : \mathbb{Z}_2^n \rightarrow \mathbb{Z}_2^n$ ,  $F = (f_1, \dots, f_n)$ , для которых каждая  $f_i$  уравновешенная. Обозначим это множество  $Sb_n$ . Через  $N(\ell, n)$  обозначим число векторных булевых функций от  $n$  переменных из класса  $Sb_n$  с нелинейностью равной  $\ell$ . Для  $N(\ell, n)$  имеет место следующая оценка.

**Теорема 2.** Если  $n$  и  $k$  удовлетворяют неравенству  $k \leq 2^{n-2}/(n + 2)$ , то справедлива оценка

$$N(2k, n) \geq \binom{n}{2^n - 1} \binom{sn}{2^{n-1}} \binom{t}{2^{n-1} - sn}^n \frac{sn!}{(s!)^n},$$

где  $s = \lceil k/2 \rceil$ ;  $t = k - s$ .

Приведём таблицу значений верхней границы оценки Сидельникова [4] для нелинейности  $(n, n)$ -функций при малых значениях  $n$  (табл. 1).

Для тех же значений  $n$  приведём таблицу нижних оценок числа  $(n, n)$ -функций с нелинейностью  $\ell$  для подходящих параметров  $\ell$  из теоремы 2 (табл. 2).

Т а б л и ц а 1

$n$	5	6	7
$Nl$	12	26	56

Т а б л и ц а 2

$\ell \setminus n$	5	6	7
2	$2^{36}$	$2^{55}$	$2^{78}$
4	–	$2^{83}$	$2^{118}$
6	–	–	$2^{150}$
$\geq 0$	$2^{145}$	$2^{364}$	$2^{868}$

Известно, что для нечётных  $n$  оценка Сидельникова точна на классе  $AB$ -функций, причём  $AB$ -функции существуют при всех нечётных  $n$ . Из табл. 2 видно, что оценка, полученная в теореме 2, применима только к значениям нелинейности, далёким от максимальных. Однако доказательство теоремы 2 конструктивно и может оказаться полезным, поскольку описывает метод построения функций с фиксированной нелинейностью.

#### ЛИТЕРАТУРА

1. *Логачев О. А., Сальников А. А., Смышляев С. В., Яценко В. В.* Булевы функции в теории кодирования и криптологии. 2-е изд. М.: МЦНМО, 2012. 584 с.
2. *Панкратова И. А.* Булевы функции в криптографии: учеб. пособие. Томск: Издательский Дом Томского государственного университета, 2014. 88 с.
3. *Carlet C.* Boolean functions for cryptography and error-correcting codes // Boolean Models and Methods in Mathematics, Computer Science, and Engineering / eds. P. Hammer, Y. Crama. Cambridge Univ. Press, 2010. Ch. 8. P. 257–397. [www.math.univ-paris13.fr/~carlet/](http://www.math.univ-paris13.fr/~carlet/)
4. *Сидельников В. М.* О взаимной корреляции последовательностей // Проблемы кибернетики. 1971. Т. 24. С. 15–42.

УДК 510.53

### ПРОБЛЕМА ДОСТИЖИМОСТИ В НЕПРЕРЫВНЫХ КУСОЧНО-АФФИННЫХ ОТОБРАЖЕНИЯХ ОКРУЖНОСТИ СТЕПЕНИ 2

А. Н. Курганский

На примере непрерывных кусочно-аффинных отображений окружности в себя степени два, для которых в работе доказывается алгоритмическая разрешимость проблемы достижимости из точки точки, обсуждаются некоторые алгоритмические аспекты моделирования дискретных систем непрерывными в контексте криптографического преобразования информации. Все такие кусочно-аффинные отображения топологически сопряжены с хаотическим отображением  $E_2(x) = 2x \pmod{1} : \mathbb{R}/\mathbb{Z} \rightarrow \mathbb{R}/\mathbb{Z}$ . Из доказательства основного результата работы следует, что любое другое непрерывное кусочно-аффинное отображение с рациональными коэффициентами и сопряжённое с  $E_2$  показывает хаотическое поведение для некоторых рациональных чисел, что делает их интересными в задачах криптографического преобразования информации.

**Ключевые слова:** хаотические системы, криптография, кусочно-аффинные отображения, проблема достижимости.

Непрерывные хаотические динамические системы привлекают к себе внимание со стороны теории алгоритмов и дискретной математики благодаря полезным аналогиям между их наблюдаемыми свойствами и свойствами, предъявляемым к криптографическим преобразователям информации [1]. В ряде публикаций встречаются исследования непрерывных хаотических систем в качестве прототипов для конечно-автоматных криптографических преобразователей информации [2]. В связи с этим, а также в силу принципиального противопоставления языка непрерывной и дискретной (компьютерной) математики является фундаментальной проблема развития интуитивных аналогий между хаотическими и криптографическими системами до уровня математических взаимосвязей. Отсюда возникает интерес к непрерывным системам с дискретным или непрерывным временем как к моделям вычислений. Это в первую очередь связано с вопросом: можно ли с помощью рассматриваемой непрерывной динамической системы моделировать дискретные системы, в частности универсальную машину Тьюринга? Проблема доказательства вычислительной универсальности тесно связана с проблемой достижимости. Обратим внимание на следующий важный момент при изучении хаотических систем в контексте моделирования с их помощью универсальных вычислений. В [3] приведено следующее замечание: поскольку реальную хаотическую систему физически невозможно установить с бесконечной точностью в заданное состояние, в частности в рациональную точку, то для таких систем идея брать в качестве основы для определения или доказательства вычислительной универсальности проблему достижимости из точки точки (“point-to-point reachability”) имеет недостатки в силу чувствительности системы к начальным условиям, из-за которой любые возмущения могут разрушить вычисления. Однако в проблеме моделирования хаотическими системами универсальных вычислений в контексте криптографических задач речь идёт не о реальном физическом моделировании, а о компьютерном моделировании математических нелинейных моделей, и бесконечная точность начальных условий в виде рациональных чисел вполне имеет смысл. В качестве примера можно привести системы, аналогичные кусочно-аффинным, в которых вместе с аффинными отображениями используются функции  $\sqrt[3]{x}$ ,  $\sqrt{x}$ ,  $x^2$ ,  $x^3$ . Для таких кусочно-элементарных отображений было выделено [4] подмножество рациональных точек, орбиты которых остаются рациональными, благодаря чему доказана их вычислительная универсальность.

Будем рассматривать непрерывные кусочно-аффинные отображения  $f : S^1 \rightarrow S^1$  степени 2 окружности  $S^1 = \mathbb{R}/\mathbb{Z}$ . Все такие отображения топологически сопряжены с  $y = E_2(x) = 2x \pmod{1}$  и являются частными случаями кусочно-аффинных отображений с двумя интервалами. Для них доказывается алгоритмическая разрешимость проблемы достижимости, и, следовательно, такие системы не являются вычислительно универсальными. Утверждение практически тривиальное, но тем не менее важное по следующим причинам. Во-первых, проблема достижимости в кусочно-аффинных отображениях с двумя интервалами в общем случае является открытой проблемой [5]. Во-вторых, отображение  $E_2$  является классическим примером хаотической системы, в которой для почти всех точек  $x \in S^1$  их орбиты демонстрируют хаотическое поведение. Однако ни одна точка из этих «почти всех» не представима на компьютере, поскольку они являются иррациональными числами, и наоборот, для всех известных в программировании типов данных система  $E_2$  ведёт себя регулярно. Математическая теорема о хаотичности системы  $E_2$  с точки зрения дискретной (компьютерной) ма-

тематики является бессодержательной. И даже если под числом понимать алгоритм, потенциально его порождающий, то теорема о хаотичности  $E_2$  должна принять вид, раскрывающий тот факт, что сложность поведения системы заключается или скрыта не в самом отображении, а в сложности начальной точки  $x$ . Вместе с тем, как следует из доказательства ниже, любое другое топологически сопряжённое с  $E_2$  кусочно-аффинное отображение с рациональными коэффициентами показывает хаотическое поведение не только орбит иррациональных чисел, но и некоторого подмножества рациональных чисел. Рациональные числа представимы на компьютере, поэтому такие отображения уже интересны в контексте криптографического преобразования информации.

Пусть  $X = \mathbb{R}/\mathbb{Z} \cap \mathbb{Q}$ ,  $f : X \rightarrow X$  — непрерывное кусочно-аффинное отображение степени 2, т. е. такое, что  $X = X_1 \cup X_2$ ,  $X_1 = \left[0, \frac{m}{n}\right]$  и  $X_2 = \left[\frac{m}{n}, 1\right]$ ,  $f(x) = \frac{n}{m}x$  при  $x \in X_1$ ,  $f(x) = \frac{n}{n-m}\left(x - \frac{m}{n}\right)$  при  $x \in X_2$ ,  $m, n \in \mathbb{N}$ . Обозначим через  $O(x) = \{f^n(x) : n \in \mathbb{N}\}$  орбиту точки  $x$ . Проблема достижимости из точки точки звучит так: существует ли алгоритм, определяющий по произвольным точкам  $x_0, x_1 \in X$  принадлежность  $x_1 \in O(x_0)$ .

**Теорема 1.** Проблема достижимости в непрерывных кусочно-аффинных отображениях  $f$  окружности в себя степени 2 алгоритмически разрешима.

**Доказательство.** Числа  $m, n, n - m$  взаимно простые. Через  $|x|_p$  обозначим  $p$ -адическую норму  $x$ . Если простое  $s \in \mathbb{P}$  не делит  $m$  и  $n - m$ , то  $|f(x)|_s \leq \max\{|x|_s, 0\}$ . Если  $p \in \mathbb{P}$  делит  $m$ , а  $q \in \mathbb{P}$  делит  $n - m$ , то  $\left|\frac{n}{m}x\right|_p > |x|_p$ ,  $\left|\frac{n}{m}x\right|_q = |x|_q$ . Пусть  $|x|_p > \left|\frac{m}{n}\right|_p$  и  $|x|_q > \left|\frac{m}{n}\right|_q$ , тогда  $\left|\frac{n}{n-m}\left(x - \frac{m}{n}\right)\right|_q > |x|_q$ ,  $\left|\frac{n}{n-m}\left(x - \frac{m}{n}\right)\right|_p = |x|_p$  и, следовательно,  $|f^{i+1}(x)|_p + |f^{i+1}(x)|_q > |f^i(x)|_p + |f^i(x)|_q$ , т. е. для проверки  $y \in O(x)$  достаточно вычислить начальный отрезок орбиты длины  $i$ , такой, что  $|f^i(x)|_p + |f^i(x)|_q > |y|_p + |y|_q$ .

Пусть условие  $\left(|x|_p > \left|\frac{m}{n}\right|_p \text{ и } |x|_q > \left|\frac{m}{n}\right|_q\right)$  не выполняется. Если  $|f^i(x)|_p \leq |y|_p$ ,  $|f^i(x)|_q \leq |y|_q$  для всех  $i$ , то последовательность  $O(x)$  зацикленна, причём с вычислимого места, поскольку существует лишь конечное множество чисел  $0 \leq x \leq 1$ , таких, что  $|x|_s \leq \max\{0, |y|_r : r \in \mathbb{P}\}$ ,  $s \in \mathbb{P}$ . ■

**Следствие 1.** Если  $|x|_p > \left|\frac{m}{n}\right|_p$  и  $|x|_q > \left|\frac{m}{n}\right|_q$ , то  $O(x)$  не зацикливается и рациональное  $x$  ведёт себя в  $f$  как некоторое действительное число в  $E_2$ .

#### ЛИТЕРАТУРА

1. *Птицын Н. В.* Приложение теории детерминированного хаоса в криптографии. М.: Изд-во МГТУ им. Н. Э. Баумана, 2002. 80 с.
2. *Savchenko A. Ya., Kovalev A. M., Kozlovskii V. A., and Scherbak V. F.* Inverse dynamical systems in secure communication and its discrete analogs for information transfer // Proc. NDES. 2003. P. 112–116.
3. *Delvenne J.-C.* What is a universal computing machine? // Appl. Math. Comput. 2009. V. 215. No. 4. P. 1368–1374.
4. *Kurgansky O., Potapov I., and Sancho-Caparrini F.* Reachability problems in low-dimensional iterative maps // Int. J. Found. Comput. Sci. 2008. No. 19(4). P. 935–951.
5. *Asarin E., Mysore V., Pnueli A., and Schneider G.* Low dimensional hybrid systems — decidable, undecidable, don't know // Inform. Comput. 2012. V. 211. P. 138–159.

УДК 519.214

## АППРОКСИМАЦИЯ РАСПРЕДЕЛЕНИЯ ЧИСЛА МОНОТОННЫХ ЦЕПОЧЕК В СЛУЧАЙНОЙ ПОСЛЕДОВАТЕЛЬНОСТИ СЛОЖНЫМ ПУАССОНОВСКИМ РАСПРЕДЕЛЕНИЕМ

А. А. Минаков

Рассматривается распределение числа монотонных цепочек в последовательности независимых равномерно распределённых на множестве  $\{0, \dots, N - 1\}$  случайных величин. С помощью метода Стейна получена оценка расстояния по вариации между распределением числа монотонных цепочек и сложным пуассоновским распределением. На основании оценки доказана предельная теорема для числа монотонных цепочек, где аппроксимирующим распределением является распределение суммы пуассоновского числа независимых случайных величин, имеющих геометрическое распределение.

**Ключевые слова:** монотонные цепочки, оценка расстояния по вариации сложной пуассоновской аппроксимации, сложное пуассоновское распределение, метод Стейна.

Пусть  $X = (X_1, X_2, \dots, X_n)$  есть отрезок последовательности, состоящий из независимых случайных величин, каждая из которых имеет равномерное распределение на множестве  $\{0, \dots, N - 1\}$ .

**Определение 1.** Монотонной цепочкой длины  $s$  ( $s \in \mathbb{N}$ ) с началом в  $t$  назовём событие  $E_t = \{X_t, \dots, X_{t+s-1} : X_t \leq X_{t+1} \leq \dots \leq X_{t+s-1}\}$ .

Введём случайную величину  $\xi_n(s) = \sum_{t=1}^{n-s+1} \text{Ind}\{E_t\}$ , равную числу монотонных цепочек длины  $s$  в последовательности  $X$ .

J. Wolfowitz [1] сформулировал условия сходимости распределения числа монотонных серий заданной длины в конечной неповторной последовательности к распределению Пуассона и стандартному нормальному распределению. F. N. David и D. E. Barton [2] сформулировали условия для пуассоновской аппроксимации числа монотонных серий длины больше заданной в конечной неповторной последовательности. Их результаты обобщил B. G. Pittel [3], который сформулировал теорему о сходимости распределения числа монотонных серий длины больше заданной к распределению Пуассона. O. Chrysaphinou, S. Papastavridis и E. Vaggelatos [4] доказали теорему об аппроксимации распределения числа монотонных серий заданной длины в стационарной цепи Маркова пуассоновским распределением. Н. М. Меженная [5] сформулировала и доказала многомерную нормальную теорему для числа монотонных серий заданной длины.

Введём некоторые обозначения. Условимся обозначать  $d(\Phi, \Psi)$  расстояние по вариации между распределениями  $\Phi$  и  $\Psi$ . Для распределений  $\Phi$  и  $\Psi$  на множестве  $\{0, 1, \dots\}$  справедлива следующая формула (теорема Шеффе):

$$d(\Phi, \Psi) = \frac{1}{2} \sum_{m=0}^{\infty} |\Psi\{m\} - \Phi\{m\}|.$$

Распределение случайной величины  $\zeta$  будем обозначать  $L(\zeta)$ .

Пусть  $\Lambda = (\lambda_1, \lambda_2, \dots)$  — последовательность неотрицательных действительных чисел, причём сходится ряд  $\sum_{k=1}^{\infty} \lambda_k < \infty$ . Пусть  $\{\theta_1, \theta_2, \dots\}$  — последовательность незави-

симых случайных величин, причём случайная величина  $\theta_k$  имеет распределение Пуассона с параметром  $\lambda_k$ ,  $k \in \mathbb{N}$ . Распределение случайной величины  $\sum_{k=1}^{\infty} k\theta_k$  называется сложным распределением Пуассона, которое будем обозначать  $CP(\Lambda)$ .

На основе метода Стейна и результатов работ [6, 7] получена следующая теорема.

**Теорема 1.** Пусть  $(X_1, X_2, \dots, X_n)$  — отрезок последовательности, состоящий из независимых случайных величин, каждая из которых имеет равномерное распределение на множестве  $\{0, \dots, N-1\}$  и  $N \geq 3$ , тогда

$$\begin{aligned} d(L(\xi_n(s)), CP(\lambda N^{-1}(1-N^{-1}), \lambda N^{-2}(1-N^{-1}), \lambda N^{-3}(1-N^{-1}), \dots)) &\leq \\ &\leq (n-s+1)(6s-5) \binom{s+N}{s}^2 (sN^{-1}+1)^{-2} N^{-2s}. \end{aligned}$$

На основании результата теоремы 1 сформулируем предельную теорему для случайной величины  $\xi_n(s)$ .

**Теорема 2.** Пусть  $(X_1, X_2, \dots, X_n)$  — отрезок последовательности, состоящий из независимых случайных величин, каждая из которых имеет равномерное распределение на множестве  $\{0, \dots, N-1\}$  и  $N \geq 3$ . Если  $n, s \rightarrow \infty$  так, что

- 1)  $s/n \rightarrow 0$ ,
- 2) величина  $n(s+N)^{N-1} N^{-s+1} (N!)^{-1} \rightarrow \lambda$ , где  $N$  и  $\lambda$  — константы, такие, что  $N \geq 3$  и  $\lambda > 0$ ,

то  $L(\xi_n(s)) \rightarrow CP(\lambda N^{-1}(1-N^{-1}), \lambda N^{-2}(1-N^{-1}), \lambda N^{-3}(1-N^{-1}), \dots)$ .

Предельным распределением в теореме 2 является распределение суммы пуассоновского (с параметром  $\lambda$ ) числа независимых случайных величин, имеющих геометрическое распределение (с параметром  $1/N$ ). Так как  $N$  фиксировано, а  $s \rightarrow \infty$ , то число монотонных цепочек длины  $s$ , не содержащих все символы из множества  $\{0, \dots, N-1\}$ , стремится к нулю. В пределе количества монотонных цепочек длины  $s$  в сериях независимы и имеют геометрическое распределение (с параметром  $1/N$ ), а число таких серий распределено по закону Пуассона (с параметром  $\lambda$ ).

#### ЛИТЕРАТУРА

1. *Wolfowitz J.* Asymptotics distribution of runs up and down // *Ann. Math. Statist.* 1944. V. 15. P. 163–172.
2. *David F. N. and Barton D. E.* Combinatorial Chance. Hafner Publishing Co., New York, 1962.
3. *Pittel B. G.* Limiting behavior of a process of runs // *Ann. Probab.* 1981. V. 9. No. 1. P. 119–129.
4. *Chryssaphinou O., Papastavridis S., and Vaggelatos E.* Poisson approximation for the non-overlapping appearances of several words in Markov chains // *Combinatorics, Probability and Computing.* 2001. V. 10. No. 4. P. 293–308.
5. *Меженная Н. М.* Многомерная нормальная теорема для числа монотонных серий заданной длины в равновероятной случайной последовательности // *Обзорные прикладной и промышленной математики.* 2007. Т. 14. Вып. 3. С. 503–505.
6. *Roos V.* Stein's method for compound Poisson approximation: The local approach // *Ann. Appl. Probab.* 1994. V. 4. No. 4. P. 1177–1187.
7. *Barbour A. D., Chen L. H. Y., and Loh W.-L.* Compound Poisson approximation for nonnegative random variables via Stein's method // *Ann. Appl. Probab.* 1992. V. 20. No. 4. P. 1843–1866.

УДК 519.719.325

## О ЧИСЛЕ ДИСКРЕТНЫХ ФУНКЦИЙ НА ЦИКЛИЧЕСКОЙ ГРУППЕ ПРИМАРНОГО ПОРЯДКА С ЗАДАННОЙ СТЕПЕНЬЮ НЕЛИНЕЙНОСТИ

А. В. Черемушкин

Предлагается способ вычисления степени нелинейности дискретных функций, заданных на циклической группе примарного порядка, основанный на свойствах разложения Ньютона. Найдены значения степени нелинейности для базисных функций этого разложения. Для циклических групп порядков  $p^2$  и  $p^3$  приводится распределение числа функций с заданным значением степени нелинейности.

**Ключевые слова:** дискретные функции, степень нелинейности.

Напомним определения из работы [1]. Будем рассматривать функции  $F : G^m \rightarrow H$ , где  $G$  и  $H$  — циклические группы. Считаем, что циклические группы — это аддитивные группы колец вычетов. *Степенью нелинейности* функции  $F$  (обозначается  $dl F$ ) называется минимальное натуральное число  $t$ , такое, что  $\Delta_{a_1} \dots \Delta_{a_{t+1}} F(x) = 0$  при всех  $a_1, \dots, a_{t+1}, x \in G^m$ , где  $\Delta_a F(x) = F(x + a) - F(x)$ ,  $a, x \in G^m$ . Пусть  $D_t$  — множество функций со степенью нелинейности  $t$ .

Предлагается подход к описанию классов  $D_t$  на основе разложения Ньютона. Теорема 1 даёт точные значения степени нелинейности для базисных функций этого разложения.

**Лемма 1.** Пусть  $n \geq 2$ ,  $p$  простое и  $1 \leq i \leq p^n - 1$ . Тогда значения производных функции  $F_i(x) = \binom{x}{i} \pmod{p^n}$  при  $1 \leq x \leq p^n - 1$  удовлетворяют равенствам

$$\Delta_1 \binom{x}{i} \equiv \begin{cases} \binom{x}{i-1} \pmod{p^n}, & \text{если } (p^n, i) = 1, \\ \binom{x}{i-1} - \binom{p^n}{i} \binom{x}{p^n-1} \pmod{p^n}, & \text{если } (p^n, i) \neq 1. \end{cases}$$

**Теорема 1.** Пусть  $n \geq 1$  и  $p$  простое. Тогда степень нелинейности функции  $F_i(x) = \binom{x}{i} \pmod{p^n}$ ,  $1 \leq i \leq p^n - 1$ , равна

$$dl F_i = \begin{cases} i + (t-1)(p-1)p^{n-1} + p^n - p^t, & \text{если } p^t \leq i \leq p^{t+1} - 1, 1 \leq t \leq n-1, \\ i, & \text{если } 1 \leq i \leq p-1. \end{cases}$$

**Следствие 1.** В условиях теоремы 1 выполняются равенства

$$dl F_i - dl F_{i-1} = \begin{cases} (p-1)p^{n-1} + p^t - p^{t+1}, & \text{если } i = p^t, 1 \leq t \leq n-1, \\ 1, & \text{если } i \neq p^t, 1 \leq t \leq n-1. \end{cases}$$

**Следствие 2.** Пусть  $m \geq 2$ ,  $n \geq 1$ ,  $p \geq 2$  и разложение функции  $F : \mathbb{Z}_{p^n}^m \rightarrow \mathbb{Z}_{p^n}$  имеет вид

$$F(x_1, \dots, x_m) = \sum_{i_1, \dots, i_m=0}^{n-1} h(i_1, \dots, i_m) \binom{x_1}{i_1} \cdots \binom{x_m}{i_m} \pmod{p^n}.$$

Тогда следующие условия эквивалентны:

1) функция  $F$  имеет максимальную степень нелинейности, равную

$$dlF = m(p^n + (k - 1)(p - 1)p^{n-1} - 1);$$

2) коэффициент  $h(p^n - 1, \dots, p^n - 1)$  обратим в кольце  $\mathbb{Z}_{p^n}$ , т. е.

$$(h(p^n - 1, \dots, p^n - 1), p) = 1;$$

3) сумма значений функции  $F$  является обратимым элементом в кольце  $\mathbb{Z}_{p^n}$ :

$$\left( \sum_{x_1, \dots, x_m} F(x_1, \dots, x_m) \bmod p^n, p \right) = 1.$$

Данный подход позволяет подсчитать число функций малой и близкой к максимальной степени нелинейности, а также найти точное распределение числа функций с заданным значением степени нелинейности для циклических групп порядков  $p^2$  и  $p^3$ .

**Теорема 2.** Пусть  $p \geq 2$ . Тогда число функций степени нелинейности  $i$  среди функций вида  $F : G \rightarrow H$ ,  $G = H = \mathbb{Z}_{p^2}$ , равно

$$|D_i| = \begin{cases} 1, & \text{если } i = -1, \\ p^{2i}(p^2 - 1), & \text{если } 0 \leq i \leq p - 1, \\ p^{i+p}(p - 1), & \text{если } p \leq i \leq p^2 + (p - 1)p - 1. \end{cases}$$

**Теорема 3.** Пусть  $p \geq 2$ . Тогда число функций степени нелинейности  $i$  среди функций вида  $F : G \rightarrow H$ ,  $G = H = \mathbb{Z}_{p^3}$ , равно

$$|D_i| = \begin{cases} 1, & \text{если } i = -1, \\ p^{3i}(p^3 - 1), & \text{если } 0 \leq i \leq p - 1, \\ p^{2i+p}(p^2 - 1), & \text{если } p \leq i \leq p^2 - 1, \\ p^{i+p^2+p}(p - 1), & \text{если } p^2 \leq i \leq p^3 - 1, \\ p^{2i-p^3+p^2+p}(p^2 - 1), & \text{если } p^3 \leq i \leq p^3 + p^2 - p - 1, \\ p^{i+2p^2}(p - 1), & \text{если } p^3 + p^2 - p \leq i \leq p^3 + 2(p - 1)p^2 - 1. \end{cases}$$

Подробное изложение представленных результатов можно найти в [2].

#### ЛИТЕРАТУРА

1. Черемушкин А. В. Аддитивный подход к определению степени нелинейности дискретной функции на циклической группе примарного порядка // Прикладная дискретная математика. 2013. № 2(20). С. 26–38.
2. Черемушкин А. В. Вычисление степени нелинейности функции на циклической группе примарного порядка // Прикладная дискретная математика. 2014. № 2(24). С. 37–47.

УДК 512.62

НЕКОТОРЫЕ СВОЙСТВА  $q$ -ИЧНЫХ БЕНТ-ФУНКЦИЙ

В. А. Шишкин

Рассматриваются свойства бент-функций над полями характеристики 2. Расширен спектр значений параметров, при которых можно указать точные значения весовой структуры  $q$ -ичной бент-функции. Показано также, что если весовая структура  $q$ -ичной функции имеет специальный вид, то значение периода данной функции делится на определённую величину.

**Ключевые слова:** бент-функция, период функции, уравнения в конечных полях.

Пусть  $P$  — конечное поле мощности  $q = 2^l$ ,  $l \geq 1$ , и  $Q$  — расширение степени  $n$  поля  $P$ . Будем рассматривать функции вида  $F : Q \rightarrow P$ . Пусть  $\theta$  — примитивный элемент поля  $Q$ . Периодом функции  $F$  будем называть период последовательности  $u(i) = F(\theta^i)$ ,  $i \in \mathbb{N}_0$  [1]. Через  $N_a(F)$  будем обозначать число решений в поле  $Q$  уравнения  $F(x) = a$ ,  $a \in P$ . Набор чисел  $\{N_a(F) : a \in P\}$  будем называть весовой структурой отображения  $F$ .

Существует несколько подходов к обобщению понятия бент-функции на случай  $q$ -ичных отображений [2]. Мы пользуемся определением  $q$ -ичной бент-функции, впервые предложенным в работе [3].

В [4] получен ряд результатов, характеризующих период и весовую структуру  $q$ -ичных бент-функций.

**Теорема 1** [4]. Пусть  $n > 2$  и функция  $F$  является бент-функцией. Тогда

$$N_a(f) = q^{n-1} + n_a q^{n/2-1},$$

где  $n_a$  принимает целые нечётные значения в интервале  $[-(q-1), q-1]$ .

**Утверждение 1** [4]. Если  $n > 2$  и  $F$  есть бент-функция, то её период  $t$  удовлетворяет неравенству  $t \geq q^{n/2} - 1$ .

Легко показать, что приведённые результаты справедливы и при  $n = 2$ .

В [4] также продемонстрировано, что при ряде значений параметров оказывается возможным указать точные значения весовой структуры бент-функции. В данной работе приводятся результаты дальнейших исследований в этом направлении.

Заметим, что если период  $t$  бент-функции удовлетворяет неравенству  $t < q^n - 1$ , то, ввиду утверждения 1, значение  $t$  делится либо на  $q^{n/2} - 1$ , либо на  $q^{n/2} + 1$ .

**Теорема 2.** Пусть период бент-функции  $F$  удовлетворяет неравенству  $t < q^n - 1$  и  $F(0) = c$ . Тогда

1. Если период  $F(x)$  делится на  $q^{n/2} + 1$ , то

$$\begin{aligned} \forall a \in P \setminus \{c\} \quad (N_a(F) = q^{n-1} - q^{n/2-1}), \\ N_c(F) = q^{n-1} + (q-1)q^{n/2-1}. \end{aligned}$$

2. Если период  $F(x)$  делится на  $q^{n/2} - 1$ , то

$$\begin{aligned} \forall a \in P \setminus \{c\} \quad (N_a(F) = q^{n-1} + q^{n/2-1}), \\ N_c(F) = q^{n-1} - (q-1)q^{n/2-1}. \end{aligned}$$

Имеет место следующее утверждение, которое представляет в некотором роде обратный результат.

**Утверждение 2.** Пусть  $\varepsilon \in \{-1, 1\}$  и весовая структура функции  $F$  для некоторого  $c \in P$  описывается значениями

$$\begin{aligned} \forall a \in P \setminus \{c\} \quad (N_a(F) = q^{n-1} + \varepsilon q^{n/2-1}), \\ N_c(F) = q^{n-1} - \varepsilon(q-1)q^{n/2-1}. \end{aligned}$$

Тогда значение периода функции  $F$  делится на величину  $q^{n/2} - \varepsilon$ .

Представленные утверждения позволяют в ряде случаев указать точные значения весовой структуры  $q$ -ичных бент-функций. Однако, как показывает следующее утверждение, область действия данных результатов существенно ограничена.

**Утверждение 3.** Пусть  $H$  — множество всех гомоморфизмов из группы  $(Q, +)$  в группу  $(P, +)$ . Множество функций  $\{F + h : h \in H\}$  содержит не более одной функции, период которой строго меньше  $q^n - 1$ .

Таким образом, среди бент-функций вида  $F + h$  (где  $h$  — гомоморфизм соответствующих групп) не более одной функции может иметь период, значение которого удовлетворяет условиям теоремы 2.

#### ЛИТЕРАТУРА

1. Кузьмин А. С., Марков В. Т., Нечаев А. А., Шишкин В. А., Шишков А. Б. Бент-функции и гипербент-функции над полем из  $2^l$  элементов // Проблемы передачи информации. 2008. Т. 44. Вып. 1. С. 15–37.
2. Токарева Н. Н. Обобщения бент-функций. Обзор работ // Дискретн. анализ и исслед. операций. 2010. Т. 17. Вып. 1. С. 34–64.
3. Солодовников В. И. Бент-функции из конечной абелевой группы // Дискретная математика. 2002. Т. 14. Вып. 1. С. 99–113.
4. Кузьмин А. С., Нечаев А. А., Шишкин В. А. Бент- и гипербент-функции над конечным полем // Труды по дискретной математике. 2007. Т. 10. С. 86–111.

УДК 621.391: 519.728

### О СРАВНЕНИИ НЕДООПРЕДЕЛЕННЫХ АЛФАВИТОВ<sup>1</sup>

Л. А. Шоломов

Представлены несколько подходов к сравнению недоопределённых алфавитов по силе и доказана их эквивалентность. Установлено, что введённые соотношения по силе полиномиально проверяемы.

**Ключевые слова:** *недоопределённый алфавит, равносильные алфавиты, энтропия недоопределённых данных, сложность по Колмогорову.*

Задан конечный алфавит  $A_0 = \{a_i : i \in M\}$  основных символов. Каждому непустому  $T \subseteq M$  соответствует *недоопределённый символ*  $a_T$ , доопределением которого считается всякий основной символ  $a_i$ ,  $i \in T$ . Выделена система  $\mathcal{T} \subseteq 2^M$  некоторых подмножеств  $T \subseteq M$  и с ней связан *недоопределённый алфавит*  $A = \{a_T : T \in \mathcal{T}\}$ .

Пусть помимо  $A_0$  и  $A$  заданы основной алфавит  $B_0 = \{b_j : j \in L\}$ , недоопределённый алфавит  $B = \{b_U : U \in \mathcal{U} \subseteq 2^L\}$  и соответствие  $R_{AB} \subseteq A \times B$ , указывающее,

<sup>1</sup>Работа поддержана ОНИТ РАН по программе фундаментальных исследований.

каким образом символы алфавитов  $A$  и  $B$  взаимно сопоставлены друг другу (символам одного алфавита могут соответствовать несколько символов другого). Назовём алфавиты  $A$  и  $B$  с заданным для них соответствием  $R_{AB}$  *соответственными алфавитами*; последовательности  $\mathbf{a} = a_{T_1} \dots a_{T_n}$  и  $\mathbf{b} = b_{U_1} \dots b_{U_n}$ , для которых  $(a_{T_i}, b_{U_i}) \in R_{AB}$ ,  $i = 1, \dots, n$ , *соответственными последовательностями*.

В работе представлено несколько подходов к сравнению соответственных недоопределённых алфавитов по силе. Первый из них — функциональный — основан на функциональной выразимости символов одного алфавита через символы другого. Следующие три подхода терминологически связаны с подходами к введению меры информации, представленными в работе А. Н. Колмогорова [1]. Это комбинаторный, вероятностный (статистический) и алгоритмический подходы. Доказано, что все подходы приводят к одному и тому же соотношению алфавитов по силе.

**Функциональный подход.** Скажем, что алфавит  $B$  функционально выразим через  $A$ , если существует функция  $F : A_0 \rightarrow B_0$ , такая, что для всех пар  $(a_T, b_U) \in R_{AB}$  выполнено  $F(a_T) \subseteq b_U$ , где  $F(a_T) = \{F(a_i) : i \in T\}$ ,  $b_U = \{b_j : j \in U\}$ . Будем говорить, что алфавит  $A$  функционально сильнее  $B$ , и записывать  $A \succeq_f B$ , если  $B$  функционально выразим через  $A$ . Соотношение  $A \succeq_f B$  может быть эквивалентно представлено в терминах соответственных последовательностей, а именно:  $A \succeq_f B$  тогда и только тогда, когда существует такая функция  $F : A_0 \rightarrow B_0$ , что для всякой пары  $\mathbf{a} = a_{T_1} \dots a_{T_n}$ ,  $\mathbf{b} = b_{U_1} \dots b_{U_n}$  соответственных последовательностей и любого доопределения  $\mathbf{a}^0 = a_{i_1} \dots a_{i_n}$  последовательности  $\mathbf{a}$  последовательность  $F(\mathbf{a}^0) = F(a_{i_1}) \dots F(a_{i_n})$  доопределяет  $\mathbf{b}$ . В терминах соответственных последовательностей будут даны и последующие определения.

**Комбинаторный подход.** Для последовательности  $\mathbf{a}$  в алфавите  $A$  введём класс  $\mathcal{K}(\mathbf{a})$  всех последовательностей в алфавите  $A$ , в которых каждый символ  $a_T \in A$  встречается такое же, как в  $\mathbf{a}$  число раз. Обозначим через  $N(\mathbf{a})$  минимальную мощность множества последовательностей в основном алфавите  $A_0$ , среди которых имеются доопределения всех последовательностей из  $\mathcal{K}(\mathbf{a})$ . Аналогично, паре последовательностей  $\mathbf{a} = a_{T_1} \dots a_{T_n}$  и  $\mathbf{b} = b_{U_1} \dots b_{U_n}$  сопоставим класс  $\mathcal{K}(\mathbf{a}, \mathbf{b})$  всех пар последовательностей с теми же кратностями появления пар  $(a_T, b_U) \in A \times B$ , что и в  $(\mathbf{a}, \mathbf{b})$ , и минимальную мощность  $N(\mathbf{a}, \mathbf{b})$  доопределяющего  $\mathcal{K}(\mathbf{a}, \mathbf{b})$  множества пар. Будем считать, что алфавит  $A$  комбинаторно сильнее алфавита  $B$ , и записывать  $A \succeq_c B$ , если для любых соответственных последовательностей  $\mathbf{a}$  и  $\mathbf{b}$  выполнено  $N(\mathbf{a}, \mathbf{b}) = N(\mathbf{a})$ .

**Статистический подход.** Будем рассматривать *недоопределённые источники*  $X$  в алфавите  $A$ , порождающие независимо символы  $a_T \in A$  с некоторыми вероятностями  $p_T$ . Определим *энтропию*  $\mathcal{H}(X)$  источника  $X$ , положив

$$\mathcal{H}(X) = \min_Q \left\{ - \sum_{T \in T} p_T \log_2 \sum_{i \in T} q_i \right\},$$

где минимум берётся по наборам  $Q = (q_i, i \in M)$  вероятностей символов  $a_i$  основного алфавита  $A_0$ . О свойствах и роли этой энтропии см. в [2]. *Источники*  $X$  и  $Y$  в алфавитах  $A$  и  $B$ , заданные совместным распределением  $p(a_T, b_U)$ ,  $a_T \in A$ ,  $b_U \in B$ , назовём *соответственными*, если  $p(a_T, b_U) > 0$  лишь в случае  $(a_T, b_U) \in R_{AB}$ . Будем говорить, что алфавит  $A$  статистически сильнее алфавита  $B$ , и записывать  $A \succeq_s B$ , если для любых пар соответственных источников  $X$  и  $Y$  выполнено  $\mathcal{H}(XY) = \mathcal{H}(X)$ .

**Алгоритмический подход.** Модифицируя применительно к недоопределённым данным систему понятий из [1], назовём *колмогоровской сложностью*  $K(\mathbf{x})$  *недоопределённого слова*  $\mathbf{x}$  минимальную длину двоичной программы для произвольно

фиксированного оптимального алгоритма, порождающей какое-либо доопределение слова  $\mathbf{x}$ . Эта величина задана с точностью до аддитивной константы: сложности  $K(\mathbf{x})$  и  $K'(\mathbf{x})$  по различным оптимальным алгоритмам удовлетворяют соотношению  $K(\mathbf{x}) \approx K'(\mathbf{x})$ , где  $f \approx g$  означает, что разность  $f - g$  ограничена [1]. Будем говорить, что алфавит  $A$  *алгоритмически сильнее* алфавита  $B$ , и записывать  $A \succsim_a B$ , если для любых соответственных последовательностей  $\mathbf{a}$  и  $\mathbf{b}$  выполнено  $K(\mathbf{ab}) \approx K(\mathbf{a})$ .

**Теорема 1.** Введенные соотношения недоопределенных алфавитов по силе эквивалентны, т. е.

$$A \succsim_f B \Leftrightarrow A \succsim_c B \Leftrightarrow A \succsim_s B \Leftrightarrow A \succsim_a B.$$

С учётом теоремы будем применять запись  $A \succsim B$  без уточнения смысла, в каком она понимается. Будем алфавиты  $A$  и  $B$  называть *равносильными* и записывать  $A \simeq B$ , если  $A \succsim B$  и  $B \succsim A$ .

**Теорема 2.** Для соответственных алфавитов  $A$  и  $B$  существуют полиномиальные алгоритмы проверки соотношений  $A \succsim B$  и  $A \simeq B$ .

Задача сжатия недоопределённых последовательностей ставится как задача такого их кодирования, которое обеспечивает для каждой из них возможность восстановления какого-либо доопределения [2]. Если  $\mathbf{a}$  и  $\mathbf{b}$  — соответственные последовательности в равносильных алфавитах  $A$  и  $B$ , то кодирование для  $\mathbf{a}$  может рассматриваться и как кодирование для  $\mathbf{b}$ , поскольку доопределение  $\mathbf{a}^0$ , найденное по коду для  $\mathbf{a}$ , позволяет получить доопределение для  $\mathbf{b}$  в виде  $F(\mathbf{a}^0)$  (см. функциональный подход). Если кодирование для  $\mathbf{a}$  оптимально, оно оптимально и для  $\mathbf{b}$ . За счёт перехода к равносильному алфавиту иногда удаётся упростить процедуру оптимального кодирования.

#### ЛИТЕРАТУРА

1. Колмогоров А. Н. Три подхода к определению понятия «количество информации» // Проблемы передачи информации. 1965. Т. 1. № 1. С. 3–11.
2. Шоломов Л. А. Элементы теории недоопределенной информации // Прикладная дискретная математика. Приложение. 2009. № 2. С. 18–42.

УДК 519.7

### ВЕКТОРНЫЕ БУЛЕВЫ ФУНКЦИИ НА РАССТОЯНИИ ОДИН ОТ APN-ФУНКЦИЙ

Г. И. Шущев

Доказано, что на расстоянии один от произвольной APN-функции все функции являются дифференциально 4-равномерными.

**Ключевые слова:** векторная булева функция, дифференциально  $\delta$ -равномерная функция, APN-функция.

В работе исследуются метрические свойства класса векторных булевых функций, а именно APN-функций. Знание метрических свойств позволяет получать конструкции таких функций, а также сокращать перебор при поиске функций, обладающих определённым свойством. Например, метрические свойства класса бент-функций исследовались в работах [1, 2].

В 1994 г. К. Nyberg [3] было введено понятие дифференциально  $\delta$ -равномерных векторных булевых функций (differentially  $\delta$ -uniform). Векторная булева функция

$F : \mathbb{Z}_2^n \rightarrow \mathbb{Z}_2^n$  называется *дифференциально  $\delta$ -равномерной*, если при любом ненулевом векторе  $a \in \mathbb{Z}_2^n$  и произвольном векторе  $b$  уравнение  $F(x) \oplus F(x \oplus a) = b$  имеет не более  $\delta$  решений, где  $\delta$  — целое число.

Для векторной функции  $F$  и любого ненулевого вектора  $a$  определим множество

$$B_a(F) = \{F(x) \oplus F(x \oplus a) : x \in \mathbb{Z}_2^n\}.$$

Максимальная достижимая мощность множества  $B_a(F)$  равна  $2^{n-1}$ . В частности, если при любом ненулевом векторе  $a$  выполнено  $|B_a(F)| = 2^{n-1}$ , то функция  $F$  является APN, а если выполнено  $|B_a(F)| \geq 2^{n-1} - 1$ , то дифференциально 4-равномерной. Минимальное  $\delta$ , при котором функция является дифференциально  $\delta$ -равномерной, назовём *порядком* дифференциальной равномерности. *Расстоянием* между векторными булевыми функциями  $F$  и  $G$  называется мощность множества  $\{x \in \mathbb{Z}_2^n : F(x) \neq G(x)\}$ .

**Утверждение 1.** Пусть  $F$  — APN-функция от  $n$  переменных. Тогда все функции на расстоянии один от  $F$  являются дифференциально 4-равномерными.

*Доказательство.* Пусть  $F$  — APN-функция. Тогда при любом ненулевом векторе  $a \in \mathbb{Z}_2^n$  выполнено равенство  $|B_a(F)| = 2^{n-1}$ . Рассмотрим функцию  $G$ , совпадающую с  $F$  во всех точках, кроме некоторого  $x_1 \in \mathbb{Z}_2^n$ . Пусть

$$\overline{B}_a(G) = \{G(x) \oplus G(x \oplus a) : x \in \mathbb{Z}_2^n \setminus \{x_1, x_1 \oplus a\}\}.$$

При любом ненулевом векторе  $a \in \mathbb{Z}_2^n$  множество  $\overline{B}_a(F)$  совпадает с  $\overline{B}_a(G)$  и выполнено равенство  $|\overline{B}_a(G)| = 2^{n-1} - 1$ .

Заметим, что  $B_a(G) = \overline{B}_a(G) \cup \{G(x_1) \oplus G(x_1 \oplus a)\}$ . Тогда для любого значения  $G(x_1)$ , в том числе отличного от  $F(x_1)$ , и при любом ненулевом  $a \in \mathbb{Z}_2^n$  выполнено  $|B_a(G)| \geq |\overline{B}_a(G)| = 2^{n-1} - 1$ , т. е. функция  $G$  является дифференциально 4-равномерной. ■

**Гипотеза.** Пусть  $F$  — APN-функция от  $n$  переменных. Тогда все функции на расстоянии один от  $F$  являются дифференциально равномерными порядка 4.

Другими словами, на расстоянии один от APN-функций не может быть других APN-функций, т. е. минимальное расстояние между APN-функциями не меньше двух. На расстоянии два APN-функции могут быть; например, функции  $F = (0, 0, 1, 2, 1, 4, 2, 4)$  и  $G = (0, 0, 1, 2, 1, 4, 4, 2)$  отличаются двумя последними значениями и обе являются APN-функциями.

Заметим, что гипотеза верна, если и только если существует  $a \in \mathbb{Z}_2^n$ , для которого выполнено равенство  $|B_a(G)| = |\overline{B}_a(G)|$ . Для этого требуется, чтобы сумма  $G(x_1) \oplus G(x_1 \oplus a)$  принадлежала множеству  $\overline{B}_a(G)$ .

#### ЛИТЕРАТУРА

1. Коломеец Н. А., Павлов А. В. Свойства бент-функций, находящихся на минимальном расстоянии друг от друга // Прикладная дискретная математика. 2009. № 4. С. 5–20.
2. Коломеец Н. А. Перечисление бент-функций на минимальном расстоянии от квадратичной бент-функции // Дискретн. анализ и исслед. операций. 2012. Т. 19. № 1. С. 41–58.
3. Nyberg K. Differentially uniform mappings for cryptography // LNCS. 1994. V. 765. P. 55–64.

УДК 519.7

## EVERY CUBIC BOOLEAN FUNCTION IN 8 VARIABLES IS THE SUM OF NOT MORE THAN 4 BENT FUNCTIONS<sup>1</sup>

N. N. Tokareva

It is shown that any cubic Boolean function in 8 variables is the sum of not more than 4 bent functions in 8 variables.

**Keywords:** *bent function, cubic Boolean function, affine classification.*

Boolean functions with extremal nonlinear properties are called *bent functions*. They are exactly those functions that have the maximal possible Hamming distance to the class of all affine Boolean functions in  $n$  variables. Note that degree of a bent function is not more than  $n/2$ . One of the most important problem in bent functions is to find the number of them. In [1] we introduced a new approach to this problem and formulated the following hypothesis: *any Boolean function in  $n$  variables of degree not more than  $n/2$  can be represented as the sum of two bent functions in  $n$  variables ( $n$  is even,  $n \geq 2$ ).* In general, it is interesting to obtain decompositions in *constant* number of bent functions.

In this paper we study bent decompositions for Boolean functions in 8 variables. Recall that Boolean functions  $f$  and  $g$  in  $n$  variables are *affine equivalent*, if there exist nonsingular binary  $n \times n$  matrix  $A$ , vectors  $u, v$  of length  $n$  and constant  $\lambda \in \mathbb{Z}_2$ , such that  $g(x) = f(Ax + u) + \langle v, x \rangle + \lambda$ , where  $\langle v, x \rangle = x_1v_1 + \dots + x_nv_n$  is the *inner product*. We study bent decompositions only for affine nonequivalent Boolean functions due to the following facts:

- A Boolean function affine equivalent to a bent function is bent too.
- Let a Boolean function  $f$  in  $n$  variables be represented as the sum of  $k$  bent functions.

Then every Boolean function affine equivalent to  $f$  also can be represented as the sum of  $k$  bent functions.

In [2] it is proven that every quadratic Boolean function in  $n$  variables ( $n$  is even) is the sum of two bent functions in  $n$  variables. The proof of this fact was based on the known affine classification of all quadratic Boolean functions in  $n$  variables (due to the Dickson's theorem). Thus, let us consider Boolean functions of degree 3.

**Theorem 1.** Every cubic Boolean function in 8 variables is the sum of not more than 4 bent functions.

Recall that if all items of algebraic normal form of a Boolean function contain exactly  $k$  variables then such a function is called *homogeneous of degree  $k$* . In the table bellow we list all affine nonequivalent homogeneous Boolean functions of degree 3 according to classification from [3]. To be short we write monomial  $x_1x_2x_3$  as 123 and so on. Let  $f(x) = f_3(x) + f_2(x)$  be an arbitrary cubic Boolean function in 8 variables, where  $f_3(x)$  is a homogeneous part of degree 3 and  $f_2(x)$  has degree  $\leq 2$ . W.l.o.g. assume that  $f_3$  is from the table bellow (otherwise consider a function affine equivalent to  $f$ ).

It is not hard to get decompositions of the Boolean function  $f$  up to the quadratic part. It is enough to use only following nonequivalent bent functions:

$$\begin{aligned} a &= 123 + 14 + 25 + 36 + 78; \\ b &= 123 + 145 + 34 + 16 + 27 + 58; \\ c &= 123 + 145 + 346 + 35 + 16 + 15 + 27 + 48; \\ d &= 123 + 347 + 356 + 14 + 76 + 25 + 45 + 38; \\ e &= 123 + 145 + 247 + 346 + 35 + 17 + 25 + 26 + 48. \end{aligned}$$

<sup>1</sup>Work is supported by RFBR No. 14-01-00507.

We give the required decomposition in the form  $f(x) = g(\pi(x)) + h(\sigma(x)) + q(x)$ , where  $g$  and  $h$  are bent functions from the set  $\{a, b, c, d, e\}$ , substitutions  $\pi, \sigma$  are nonsingular affine transformations of variables (permutations in most cases), function  $q$  is a certain Boolean function of degree  $\leq 2$  (we do not concretize it). According to [2] any quadratic function  $q$  is the sum of two bent functions. Thus,  $f$  can be represented as the sum of not more than 4 bent functions in 8 variables.

For example, function  $f(x) = x_1x_2x_3 + x_2x_4x_6 + x_3x_5x_7 + x_1x_2x_8 + x_1x_3x_8$  (number 15 in the table) is the sum  $b(x_2 + x_3, x_1, x_8, x_4, x_6, x_3, x_5, x_7) + d(x_1 + x_2, x_2, x_3, x_4, x_5, x_7, x_6, x_8) + q(x)$ , where  $q$  is a quadratic function.

No	Affine nonequivalent homogeneous Boolean functions of degree 3	$g$	$h$	$\pi$	$\sigma$
1	123	$a$	$b$	[1, 4, 5, 2, 3, 6, 7, 8]	id
2	123 + 145	$a$	$a$	id	[1, 4, 5, 2, 3, 6, 7, 8]
3	123 + 456	$a$	$a$	id	[4, 5, 6, 1, 2, 3, 7, 8]
4	123 + 135 + 236	$a$	$b$	id	[3, 1, 5, 2, 6, 4, 7, 8]
5	123 + 124 + 135 + 236 + 456	$c$	$c$	[1 + 6, 2, 3, 4, 5, 6, 7, 8]	[3 + 4, 5, 1, 4, 6, 2, 7, 8]
6	123 + 145 + 167	$a$	$b$	id	[1, 4, 5, 6, 7, 2, 3, 8]
7	123 + 246 + 357	$b$	$d$	[4, 2, 6, 3, 8, 1, 7, 5]	[1, 2, 3, 4, 5, 7, 8, 6]
8	123 + 145 + 167 + 246	$a$	$c$	id	[1, 5, 4, 6, 7, 2, 3, 8]
9	123 + 145 + 246 + 357	$d$	$d$	[1, 2, 3, 4, 5, 7, 8, 6]	[1, 5, 4, 2, 3, 8, 6, 7]
10	123 + 124 + 135 + 236 + 456 + 167	$b$	$d$	[1 + 6, 2, 3, 4, 5, 6, 7, 8]	[2 + 5, 4, 1, 3, 6, 7, 5, 8]
11	123 + 145 + 167 + 246 + 357	$b$	$c$	[6, 1, 7, 2, 4, 3, 5, 8]	[1, 2, 3, 5, 4, 7, 6, 8]
12	123 + 478 + 568	$a$	$b$	id	[8, 4, 7, 5, 6, 1, 2, 3]
13	123 + 145 + 167 + 568	$a$	$c$	id	[1, 4, 5, 6, 7, 8, 2, 3]
14	123 + 246 + 357 + 568	$c$	$d$	[4, 2, 6, 8, 3, 5, 1, 7]	[1, 2, 3, 4, 5, 7, 8, 6]
15	123 + 246 + 357 + 128 + 138	$b$	$d$	[2 + 3, 1, 8, 4, 6, 3, 5, 7]	[1 + 2, 2, 3, 4, 5, 7, 6, 8]
16	123 + 145 + 167 + 357 + 568	$a$	$e$	id	[1, 6, 7, 5, 4, 3, 8, 2]
17	123 + 145 + 478 + 568	$a$	$c$	id	[4, 1, 5, 8, 7, 6, 2, 3]
18	123 + 124 + 135 + 236 + 456 + 167 + 258	$e$	$e$	[1, 2 + 5, 3, 5, 4, 6, 8, 7]	[1, 2 + 5, 4, 6, 7, 5, 3, 8]
19	123 + 124 + 135 + 236 + 456 + 178	$b$	$d$	[1 + 6, 2, 3, 4, 5, 6, 7, 8]	[2 + 5, 4, 1, 3, 7, 8, 5, 6]
20	123 + 145 + 246 + 357 + 568	$d$	$e$	[1, 2, 3, 4, 5, 7, 8, 6]	[5, 6, 8, 4, 1, 3, 2, 7]
21	123 + 145 + 246 + 467 + 578	$c$	$e$	[4, 3, 8, 7, 6, 5, 1, 2]	[1, 2, 3, 4, 5, 8, 6, 7]
22	123 + 145 + 357 + 478 + 568	$a$	$e$	id	[4, 7, 8, 5, 1, 6, 3, 2]
23	123 + 246 + 357 + 478 + 568	$c$	$e$	[1, 2, 3, 5, 4, 7, 6, 8]	[5, 6, 8, 4, 1, 7, 2, 3]
24	123 + 246 + 357 + 148 + 178 + 258	$c$	$c$	[1, 2, 3, 7, 8, 5, 4, 6]	[2, 5, 8, 4, 6, 1, 3, 7]
25	123 + 145 + 167 + 246 + 357 + 568	$c$	$d$	[1, 2, 3, 5, 4, 7, 6, 8]	[1, 7, 6, 2, 5, 8, 4, 3]
26	123 + 145 + 167 + 246 + 238 + 258 + 348	$c$	$e$	[1, 7 + 8, 6, 4, 5, 2, 3, 8]	[2, 1 + 8, 3, 8, 5, 4, 6, 7]
27	123 + 145 + 167 + 258 + 268 + 378 + 468	$c$	$e$	[1, 3 + 8, 2, 5, 4, 8, 6, 7]	[6, 1 + 6, 7, 8, 4, 3, 2, 5]
28	123 + 145 + 246 + 357 + 238 + 678	$c$	$c$	[1, 2, 3, 5, 4, 7, 6, 8]	[2, 3, 8, 6, 4, 7, 1, 5]
29	123 + 145 + 246 + 357 + 478 + 568	$c$	$c$	[1, 2, 3, 5, 4, 7, 6, 8]	[4, 2, 6, 8, 7, 5, 1, 3]
30	123 + 124 + 135 + 236 + 456 + 167 + 258 + 378	$c$	$e$	[1, 2, 3 + 4, 6, 7, 5, 4, 8]	[5, 8, 2 + 5, 3, 1, 6, 7, 4]
31	123 + 156 + 246 + 256 + 147 + 157 + 357 + 348 + 258 + 458	$c$	$e$	[5, 2 + 4, 8, 3, 7, 4, 1, 6]	[2, 4 + 5, 6, 1, 3, 5, 7, 8]

## BIBLIOGRAPHY

1. Tokareva N. N. On the number of bent functions from iterative constructions: lower bounds and hypotheses // Advances Math. Comm. (AMC). 2011. V. 5. Iss. 4. P. 609–621.
2. Qu L. and Li C. When a Boolean function can be expressed as the sum of two bent functions // Cryptology ePrint Archive. 2014/048.
3. Logachev O. A., Sal'nikov A. A., Smyshlyayev S. V., and Yashenko V. V. Boolean functions in coding theory and cryptology. Moscow center for the uninter. math. education, 2012. 584 p. (in Russian)

Секция 2

**МАТЕМАТИЧЕСКИЕ МЕТОДЫ КРИПТОГРАФИИ**

УДК 512.6

**НЕЛИНЕЙНЫЕ ПОДСТАНОВКИ НА ВЕКТОРНОМ ПРОСТРАНСТВЕ,  
РЕКУРСИВНО-ПОРОЖДЁННЫЕ НАД КОЛЬЦОМ ГАЛУА  
ХАРАКТЕРИСТИКИ 4**

А. В. Аборнев

Пусть  $R = \text{GR}(2^{2r}, 4)$  — кольцо Галуа характеристики 4 из  $2^{2r}$  элементов с разрядным множеством  $P = \{\beta \in R : \beta^{2^r} = \beta\}$ . В частности, если  $r = 1$ , то  $R = \mathbb{Z}_4$  и  $P = \{0, e\}$ . Строится класс нелинейных подстановок  $\pi_F$  на векторном пространстве  $\text{GF}(2^r)^m$  произвольной размерности  $m \geq 3$ , каждая из которых представляется композицией линейного рекуррентного преобразования с характеристическим многочленом  $F(x)$  и поэлементного выделения первого разряда элементов кольца  $R$ . Такие подстановки называются рекурсивно-порождёнными над кольцом Галуа  $\text{GR}(2^{2r}, 4)$ . Интерес представляет изучение многочленов  $F(x)$  с указанным свойством, которые называются разрядно-подстановочными (или РП-многочленами). Нелинейность координатных функций рекурсивно-порождённых подстановок обеспечивается применением разрядной функции кольца Галуа. В силу простоты представления подстановок из рассматриваемого класса, они допускают очень эффективную реализацию. Ранее автором были построены два класса РП-многочленов над кольцом  $R = \mathbb{Z}_4$ . В качестве криптографического приложения рассматривается применение рекурсивно-порождённых подстановок при построении итеративных криптографических примитивов.

**Ключевые слова:** *разрядно-подстановочный многочлен, РП-многочлен, кольцо Галуа.*

Пусть  $R = \text{GR}(4^r, 4)$  — кольцо Галуа характеристики 4 и мощности  $4^r$ . Множество  $P = \Gamma(R) = \{\beta \in R : \beta^{2^r} = \beta\}$  называется разрядным множеством. Каждый элемент  $a \in R$  имеет разложение

$$a = a_0 + 2a_1, \quad a_s = \gamma_s(a) \in P, \quad s \in \{0, 1\},$$

где  $\gamma_s : R \rightarrow P$ ,  $s \in \{0, 1\}$ , — *разрядные функции в разрядном множестве  $P$* . Алгебра  $(P, \oplus, \cdot)$  с умножением кольца  $R$  и операцией сложения  $a \oplus b = \gamma_0(a + b)$ ,  $a, b \in P$ , является полем из  $2^r$  элементов.

Продолжаются исследования, начатые в работе [1]. Рассматривается задача построения нелинейных подстановок на векторном пространстве  $P^m$  большой размерности  $m$  с использованием только линейного рекуррентного закона с характеристическим многочленом

$$F(x) = x^m - f_{m-1}x^{m-1} - \dots - f_1x - f_0 \in R[x]$$

и операции выделения старшего разряда элементов кольца  $R$ . В [1] впервые доказано существование таких подстановок и описаны два нетривиальных класса для случая кольца  $\mathbb{Z}_4$ . В данной работе получен новый класс нетривиальных РП-многочле-

нов  $F(x)$ , индуцирующих нелинейные подстановки на алфавите  $P^m$  сколь угодно большой мощности  $2^{rm}$ .

Пусть  $u \in L_R(F)$  — линейная рекуррентная последовательность (ЛРП) с характеристическим многочленом  $F(x) \in R[x]$ . Её знаки удовлетворяют равенству

$$u(i+m) = \sum_{k=0}^{m-1} f_k u(i+k).$$

Каждый знак ЛРП  $u$  имеет разложение

$$u(i) = u_0(i) + 2u_1(i), \quad u_0(i), u_1(i) \in P, \quad i = 0, 1, \dots$$

Обозначим через  $u[\overline{i, j}]$  отрезок  $(u(i), u(i+1), \dots, u(j))$  последовательности  $u \in L_R(F)$  и через  $L'_R(F)$  — множество всех линейных рекуррентных последовательностей  $u \in L_R(F)$ , таких, что  $u_1[\overline{0, m-1}] = \overline{0}$ .

Рассмотрим отображение  $\pi_F : P^m \rightarrow P^m$ , заданное равенством

$$\pi_F(x) = u_1[\overline{m, 2m-1}],$$

где  $u \in L'_R(F)$ ;  $u_0[\overline{0, m-1}] = x$ .

Многочлен  $F(x) \in R[x]$  степени  $m$ , для которого отображение  $\pi_F$  является биекцией, будем называть *разрядно-подстановочным* (или *РП-многочленом*). Будем говорить, что подстановка  $\pi_F$  является *рекурсивно-порождённой* над кольцом  $R$  с законом рекурсии  $F(x)$ . РП-многочлен назовём *нетривиальным*, если подстановка  $\pi_F$  нелинейна. Таким образом, каждый РП-многочлен естественным образом задаёт семейство, вообще говоря, нелинейных подстановок на пространстве  $P^m$ .

Будем использовать следующие обозначения:

$$F_0(x) = x^m \oplus \bigoplus_{i=0}^{m-1} \gamma_0(f_i)x^i, \quad F_1(x) = \bigoplus_{i=0}^{m-1} \gamma_1(f_i)x^i.$$

**Теорема 1.** Пусть  $R = \text{GR}(4^r, 4)$ ,  $F(x) \in R[x]$  — многочлен степени  $m \geq 3$ . Если  $F_0(x) = x^m \oplus x^{m-1} \oplus x \oplus e$ , то  $F(x)$  является РП-многочленом тогда и только тогда, когда для каждого  $\delta \in P$  верно равенство

$$\text{НОД}(\delta(x \oplus e) \oplus e \oplus F_1(x), F_0(x)) = e.$$

Данная теорема обобщает результат работы [1] на случай произвольного кольца Галуа характеристики 4.

#### ЛИТЕРАТУРА

1. *Nechaev A. A. and Abornev A. V.* Nonlinear permutations on a space over a finite field induced by linear transformations of a module over a Galois ring // Математические вопросы криптографии. 2013. Т. 4. № 2. С. 81–100.

УДК 519.7

## О ПРИМИТИВНОСТИ ПЕРЕМЕШИВАЮЩЕЙ МАТРИЦЫ ГЕНЕРАТОРА $(\delta, \tau)$ -САМОУСЕЧЕНИЯ

Я. Э. Авезова, В. М. Фомичев

Получены условия примитивности перемешивающей матрицы генератора  $(\delta, \tau)$ -самоусечения и его обобщения, построенного на основе нелинейных подстановок векторного пространства над конечным полем. Даны верхние оценки экспонентов указанной перемешивающей матрицы.

**Ключевые слова:** генератор  $(\delta, \tau)$ -самоусечения, примитивный граф, примитивная матрица, экспонент матрицы.

### Введение

Для генератора  $(\delta, \tau)$ -самоусечения, относящегося к классу генераторов с неравномерным движением [1, 2], известны результаты, связанные с длиной периода и линейной сложностью вырабатываемой гаммы. Работа посвящена перемешивающим свойствам преобразования состояний генератора  $(\delta, \tau)$ -самоусечения и его обобщения, построенного на основе нелинейных подстановок векторного пространства над конечным полем.

Пусть генератор  $(\delta, \tau)$ -самоусечения построен на основе регистра сдвига (не обязательно линейного) длины  $n$  над конечным полем  $P$ . Обозначим через  $h$  базовое преобразование (пространства  $P^n$ ) генератора и через  $H$  — квадратную матрицу порядка  $n$ , являющуюся перемешивающей матрицей преобразования  $h$ . Если  $x$  — состояние регистра и знак управляющей гаммы равен 1 (в частности, состояние некоторой ячейки регистра), то выполняется преобразование  $h^\delta(x)$ . Если знак управляющей гаммы равен 0, то выполняется преобразование  $h^\tau(x)$ . Следовательно, перемешивающая матрица преобразования состояний регистра равна  $H^\delta + H^\tau$ .

Предмет исследования — примитивность матрицы  $H^\delta + H^\tau$  и величина  $\exp(H^\delta + H^\tau)$ .

Графом 0,1-матрицы называется орграф  $\Gamma(A)$ , у которого матрица смежности вершин есть  $A$ .

### Теорема 1.

- 1) Если матрица  $H$  примитивная и  $\exp H = t$ , то матрица  $H^\delta + H^\tau$  также примитивная и  $\exp(H^\delta + H^\tau) \leq \lceil t/\tau \rceil$ .
- 2) Если матрица  $H$  не примитивная и  $\{l_1, \dots, l_m\}$  есть множество всех длин простых контуров орграфа  $\Gamma(H)$ , где  $(l_1, \dots, l_m) = d > 1$ , то матрица  $H^\delta + H^\tau$  примитивна, если  $\tau$  кратно  $d$  и  $(\delta, l_i) = 1, i = 1, \dots, m$ .
- 3) Пусть в условиях п. 2 число  $\tau$  кратно  $d$ ,  $\mu_i = l_i/(\tau, l_i), i = 1, \dots, m$ , и  $\{\lambda_1, \dots, \lambda_r\}$  есть множество различных чисел среди  $\mu_1, \dots, \mu_m$ , где  $r \leq m$  и  $\lambda_1 < \dots < \lambda_r$ . Тогда:
  - а) если  $\lambda_1 > 1$  и  $r > 2$ , то

$$\exp(H^\delta + H^\tau) \leq g(\lambda_1, \dots, \lambda_r) + n(r + 1) - \sum_{i=1}^r \lambda_i,$$

где  $g(\lambda_1, \dots, \lambda_r)$  — число Фробениуса от аргументов  $\lambda_1, \dots, \lambda_r$ , то есть наибольшее натуральное число, не принадлежащее аддитивной полугруппе, порождённой натуральными числами  $\lambda_1, \dots, \lambda_r$ ;

б) если  $\lambda_1 > 1$  и  $r = 2$ , то

$$\exp(H^\delta + H^\tau) \leq \lambda_1 \lambda_2 - 2\lambda_1 - \lambda_2 + 2n;$$

в) если  $\lambda_1 = 1$  и  $\mu$  — наибольшее число, делящее  $\tau$ , среди чисел  $l_1, \dots, l_m$ , то

$$\exp(H^\delta + H^\tau) \leq 2n - 1 - \mu.$$

Оценки пп. 3б и 3в получены с использованием оценок соответственно [3, с. 104] и [4, с. 408].

**Следствие 1.** Если выполнены условия п. 3а теоремы, то

$$\exp(H^\delta + H^\tau) \leq \lambda_1 \lambda_r - \lambda_1 - \lambda_r + n(r + 1) - \sum_{i=1}^r \lambda_i.$$

Следствие вытекает из оценки числа Фробениуса [5, теорема 3.1.1]  $g(\lambda_1, \dots, \lambda_r) \leq \lambda_1 \lambda_r - \lambda_1 - \lambda_r$ ,  $r > 1$ .

Данные оценки могут быть уточнены для частных классов перемешивающих матриц  $H$  базового преобразования генератора  $(\delta, \tau)$ -самоусечения.

#### ЛИТЕРАТУРА

1. Rueppel R. A. When shift registers clock themselves // Advances in Cryptology — Eurocrypt'87. LNCS. 1988. V. 304. P. 53–64.
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. Сачков В. Н., Тараканов В. Е. Комбинаторика неотрицательных матриц. М.: ТВП, 2000. 448 с.
5. Alfonsin J. R. The Diophantine Frobenius Problem. Oxford University Press, 2005.

УДК 519.113.6

### SIVCiphers — СИММЕТРИЧНЫЕ ИТЕРАТИВНЫЕ БЛОЧНЫЕ ШИФРЫ ИЗ БУЛЕВЫХ ФУНКЦИЙ С КЛЮЧЕВЫМИ АРГУМЕНТАМИ

Г. П. Агибалов

Вводится в рассмотрение класс SIVCipher много раундовых симметричных блочных шифров, в которых каждый раунд представлен инъективной системой булевых функций, зависящих существенно от ограниченного числа аргументов из информационного блока на входе раунда, и в которых раундовый ключ является подмножеством этих функций и (или) наборов их существенных аргументов. Современные симметричные блочные шифры с аддитивным раундовым ключом принадлежат этому классу. Описываются два других семейства шифров в классе SIVCipher — Фейстеля и Люцифер, построенных по известным одноимённым криптографическим схемам.

**Ключевые слова:** криптография, булевы функции, симметричные итеративные блочные шифры, сеть Фейстеля, шифр Люцифер.

## Введение

За малым исключением (Люцифер [1] и т. п.), большинство современных симметричных итеративных блочных шифров характеризуются следующими свойствами:

- 1) функция каждого раунда шифра является суперпозицией элементарных логических операций, таких, как отрицание, конъюнкция, дизъюнкция, сложение по модулю (2 или более), циклические сдвиги, перестановки и т. п., а также блоков замен — небольших фиксированных систем булевых функций от малого числа переменных;
- 2) ключ каждого раунда шифра аддитивный — входит в суперпозицию с другими операндами, в том числе и с аргументами булевых функций, посредством операции сложения (например, как  $k \oplus x$  или  $(k + x) \bmod m$ ).

Благодаря этим свойствам, такие шифры поддаются (хотя и не всегда просто) алгебраическим атакам (на основе решения систем уравнений, связывающих символы ключа с символами открытых и шифрованных текстов) [2, 3], дифференциальному криптоанализу [4, 5] и атакам на основе статистических аналогов [6], в частности линейному криптоанализу [7, 8].

Когда-то, на заре своей научной карьеры (первая половина 60-х годов XX века), автор настоящей работы предложил, говоря современным языком, симметричный поточный шифр с фильтрующим генератором ключевого потока, в котором булева фильтрующая функция существенно зависит от ограниченного числа аргументов — компонент состояния генератора — и вместе с номерами этих аргументов образует ключ шифра [9]. Криптоанализ этого шифра породил ряд публикаций [10–13]. Он заключается в определении по отрезку ключевого потока существенных аргументов фильтрующей функции и её значений на наборах значений этих аргументов и, похоже, не сводится к решению системы уравнений, дифференциальному криптоанализу и атаке на основе статистических аналогов.

В данной работе эта идея использования в качестве ключа шифра не набора символов с аддитивным вхождением в алгоритм шифрования, а набора его функциональных компонент — булевых функций вместе с ограниченным числом их существенных аргументов — реализуется в симметричных итеративных блочных шифрах. Для краткости предлагаемые шифры называются SIBCiphers — от Symmetric Iterative Block Ciphers. Ниже даётся их общая схема построения, указывается их некоторая классификация по семействам и описываются два их семейства: SIBCiphers, построенные по схеме Фейстеля, и SIBCiphers, построенные по схеме шифра Люцифер.

### 1. Общая схема шифра SIBCipher

В общей схеме  $r$ -раундового шифра SIBCipher с длиной информационного блока  $n$  раунд с номером  $l = 1, 2, \dots, r$  представляет собой систему из  $n$  булевых функций  $g_1^{(l)}, g_2^{(l)}, \dots, g_n^{(l)}$  от  $k \leq n$  переменных каждая и систему из  $n$  отображений  $\eta_i^{(l)} : \{1, 2, \dots, k\} \rightarrow \{1, 2, \dots, n\}$ ,  $i = 1, 2, \dots, n$ , обладающую свойством сюръективности: для любого  $m \in \{1, 2, \dots, n\}$  имеет место  $m = \eta_i^{(l)}(j)$  для некоторых  $i \in \{1, 2, \dots, n\}$  и  $j \in \{1, 2, \dots, k\}$ , и такую, что инъективно отображение  $g^{(l)} : \{0, 1\}^n \rightarrow \{0, 1\}^n$ , где  $g^{(l)}(u) = g_1^{(l)}(v_1)g_2^{(l)}(v_2) \dots g_n^{(l)}(v_n)$  для любого  $u = u_1u_2 \dots u_n \in \{0, 1\}^n$  и  $v_i = u_{\eta_i^{(l)}(1)}u_{\eta_i^{(l)}(2)} \dots u_{\eta_i^{(l)}(k)}$  для  $i = 1, 2, \dots, n$ . Для функции  $g_i^{(l)}$  здесь  $\eta_i^{(l)}(1), \dots, \eta_i^{(l)}(k)$  суть номера её существенных аргументов из ряда членов  $u_1, u_2, \dots, u_n$  информационного блока  $u$ , заданного на входах  $l$ -го раунда. Результатом преобразования  $l$ -м раундом

блока  $u$  является информационный блок  $g^{(l)}(u)$  на выходах этого раунда. Его обратное преобразование в  $u$  возможно ввиду инъективности  $g^{(l)}$ .

Для каждого  $l = 2, 3, \dots, r$  информационный блок на входе  $l$ -го раунда шифра совпадает с информационным блоком на выходе его  $(l - 1)$ -го раунда.

Общая схема шифра SIBCipher предполагает также наличие перестановки  $h : \{0, 1\}^n \rightarrow \{0, 1\}^n$ , определяемой как  $h(u_1 u_2 \dots u_n) = u_{i_1} u_{i_2} \dots u_{i_n}$  для некоторой подстановки  $\eta : \{1, 2, \dots, n\} \rightarrow \{1, 2, \dots, n\}$ , где  $\eta(j) = i_j$ ,  $j = 1, 2, \dots, n$ . В шифровании она применяется для перестановки символов информационного блока на выходе  $r$ -го раунда.

Если определить отображение  $h^{(l)} : \{0, 1\}^n \rightarrow \{0, 1\}^{kn}$  как  $h^{(l)}(u) = v_1 v_2 \dots v_n$  и отображение  $G^{(l)} : \{0, 1\}^{kn} \rightarrow \{0, 1\}^n$  как  $G^{(l)}(v_1 v_2 \dots v_n) = g_1^{(l)}(v_1) g_2^{(l)}(v_2) \dots g_n^{(l)}(v_n)$ , то шифрование в SIBCipher можно представить как «слоёный пирог», в котором отображения  $h^{(l)}$  чередуются с отображениями  $G^{(l)}$ , преобразуя блок открытого текста  $x$  в блок шифртекста  $y$  по правилу  $y = hG^{(r)}h^{(r)}G^{(r-1)}h^{(r-1)} \dots G^{(1)}h^{(1)}(x)$ , а расшифрование  $y$  в  $x$  — по правилу  $x = g^{(1)-1} \dots g^{(r-1)-1} g^{(r)-1} h^{-1}(y)$ . Здесь и далее в подобных выражениях для любых отображений  $f_1, f_2, \dots, f_m$  под  $f_1 f_2 \dots f_m(a)$  подразумевается  $f_1(f_2(\dots(f_m(a)) \dots))$ .

В соответствии с предназначением, булевы функции  $g_i^{(l)}$  называются далее функциональными компонентами, а связывающие их отображения  $\eta_i^{(l)}$  и  $\eta$  — соединительными компонентами шифра SIBCipher. Предполагается, что ключ шифра задаётся как подмножество из некоторых его соединительных и (или) функциональных компонент. Таким образом, любой конкретный SIBCipher однозначно определяется своими числовыми параметрами —  $n, r, k$ , своими компонентами (соединительными и функциональными) и своим ключом — подмножеством последних.

## 2. Возможные семейства шифров SIBCipher

Разные семейства шифров SIBCipher получаются путём наложения ограничений на определение входящих в них компонент и на выбор тех из них, которые образуют ключ шифра. Одно такое семейство состоит из шифров с фиксированными соединительными компонентами и с ключевыми функциональными компонентами. Другое, наоборот, содержит шифры с фиксированными (и, возможно, одинаковыми) функциональными компонентами, но с изменяемыми соединительными компонентами, совокупно выбираемыми в качестве ключа. Самое широкое семейство рассматриваемых шифров достигается, когда одновременно соединительные и функциональные компоненты (все или некоторые) образуют ключ шифра. Это именно тот случай, когда криптоанализ шифра с угрозой полного его раскрытия сводится к нахождению существенных аргументов функциональных компонент и значений последних на наборах значений этих аргументов. Насколько применимы для решения этой задачи алгоритмы из [10–13], вопрос открытый, даже при малом количестве раундов шифра.

Для предотвращения других атак, эксплуатирующих криптографические слабости булевых функций, для построения функциональных компонент в шифрах класса SIBCipher естественно рекомендовать булевы функции с высокими корреляционной и алгебраической иммунностью, нелинейностью, степенью критерия распространения и т. п. [14, 15].

Что касается симметричных итеративных блочных шифров с аддитивным раундовым ключом, то они ведь тоже образуют семейство в классе шифров SIBCipher, поскольку прибавление к аргументам булевой функции (из блока замены) символов

закрытого ключа изменяет её на неизвестную функцию и таким образом придаёт ей свойство ключа. По существу, такое применение аддитивного ключа — это такой способ выбора конкретной функции из множества возможных. Сие означает, в частности, что криптоанализ шифров из класса SIBCipher может привести к созданию новых методов криптоанализа традиционных симметричных блочных шифров с аддитивным раундовым ключом.

Есть, по крайней мере, две проблемы в построении конкретного SIBCipher: выбор компонент, гарантирующих инъективность раундовых отображений  $g^{(l)}$ , и выбор ключевого подмножества компонент с реальной длиной ключа — разумеется, с обеспечением требуемой стойкости шифра к криптоанализу. Собственно, применение аддитивного ключа — это только один из подходов к решению второй проблемы, но он значительно сужает класс рассматриваемых шифров. Ниже показывается, как первая проблема решается в SIBCiphers из семейств Фейстеля и Люцифер.

### 3. SIBCiphers семейства Фейстеля

Так мы называем шифры класса SIBCipher, в которых  $n$  чётное и информационные блоки на входе и выходе  $l$ -го раунда шифра представляются конкатенациями своих левой и правой половинок длиной  $n/2 - L_0R_0$  и  $L_1R_1$  соответственно и связаны между собой соотношениями  $L_1 = R_0$  и  $R_1 = p^{(l)}(L_0) \oplus g^{(l)}(R_0)$ , где  $p : \{0, 1\}^{n/2} \rightarrow \{0, 1\}^{n/2}$  — перестановка и, аналогично общей схеме (но без требования инъективности),  $g^{(l)} : \{0, 1\}^{n/2} \rightarrow \{0, 1\}^{n/2}$ ,  $g^{(l)}(u) = g_1^{(l)}(v_1)g_2^{(l)}(v_2) \dots g_{n/2}^{(l)}(v_{n/2})$  для любого  $u = u_1u_2 \dots u_{n/2} \in \{0, 1\}^{n/2}$  и  $v_i = u_{\eta_i^{(l)}(1)}u_{\eta_i^{(l)}(2)} \dots u_{\eta_i^{(l)}(k)}$  для сюръективной системы отображений  $\eta_i^{(l)} : \{1, 2, \dots, k\} \rightarrow \{1, 2, \dots, n/2\}$ ,  $i = 1, 2, \dots, n/2$ . Обратное преобразование  $L_1R_1$  в  $L_0R_0$  выполняется по правилу  $L_0 = p^{(l-1)}(R_1 \oplus g^{(l)}(L_1))$ ,  $R_0 = L_1$ .

Осведомлённый читатель сразу же заметит, что уравнения раунда здесь по форме близки к уравнениям Фейстеля в раунде DES, поэтому можно говорить, что сами шифры здесь построены действительно по схеме Фейстеля. Кроме того, внимательный читатель сможет без труда формально доказать, что эти шифры действительно образуют семейство шифров класса SIBCipher.

### 4. SIBCiphers семейства Люцифер

В шифре этого семейства предполагается: 1)  $n = ks$  для некоторого  $s > 1$ ; 2) для каждой пары  $(l, i)$ , где  $l = 1, 2, \dots, r$  и  $i = 1, 2, \dots, s$ , отображение  $G_i^{(l)} : \{0, 1\}^k \rightarrow \{0, 1\}^k$ , где  $G_i^{(l)}(z) = g_{(i-1)k+1}^{(l)}(z)g_{(i-1)k+2}^{(l)}(z) \dots g_{ik}^{(l)}(z)$  для всех  $z \in \{0, 1\}^k$ , есть подстановка на  $\{0, 1\}^k$ ; 3) все функции  $g_{(i-1)k+j}^{(l)}$ ,  $j = 1, 2, \dots, k$ , зависят от одного и того же набора аргументов в информационном блоке на входе  $l$ -го раунда, т.е.  $\eta_{(i-1)k+1}^{(l)} = \eta_{(i-1)k+2}^{(l)} = \dots = \eta_{ik}^{(l)}$ ; 4) отображение  $p^{(l)} : \{0, 1\}^n \rightarrow \{0, 1\}^n$ , где  $p^{(l)}(u) = p_1^{(l)}(u)p_2^{(l)}(u) \dots p_s^{(l)}(u)$  и  $p_i^{(l)}(u) = u_{\eta_{ik}^{(l)}(1)}u_{\eta_{ik}^{(l)}(2)} \dots u_{\eta_{ik}^{(l)}(k)}$  для  $p_i^{(l)} : \{0, 1\}^n \rightarrow \{0, 1\}^k$  и  $i = 1, 2, \dots, s$ , есть перестановка.

Иначе говоря, все булевы функции раунда шифра разбиты на  $s$  подсистем  $F_i^{(l)}$  по  $k$  функций в каждой, а их аргументы в информационном блоке — на  $s$  наборов  $z_i^{(l)}$  по  $k$  аргументов в каждом так, что аргументы в наборе  $z_i^{(l)}$  служат аргументами всех функций в подсистеме  $F_i^{(l)}$ , и функции в последней являются координатными функциями подстановки  $G_i^{(l)}$ ,  $i = 1, 2, \dots, s$ . Таким образом, подстановки  $G_1^{(l)}, \dots, G_s^{(l)}$  здесь выступают в роли обратимых блоков замены и  $s$  — их количество в одном раунде шифра.

Если определить отображение  $E^{(l)} : \{0, 1\}^n \rightarrow \{0, 1\}^n$  как

$$E^{(l)}(u_1 u_2 \dots u_n) = G_1^{(l)}(u_1 \dots u_k) G_2^{(l)}(u_{k+1} \dots u_{2k}) \dots G_s^{(l)}(u_{(s-1)k+1} \dots u_{sk}),$$

то шифрование и расшифрование в таком SIBCipher можно выполнить по правилам  $y = hE^{(r)}p^{(r)}E^{(r-1)}p^{(r-1)} \dots E^{(1)}p^{(1)}(x)$  и  $x = p^{(1)^{-1}}E^{(1)^{-1}} \dots E^{(r-1)^{-1}}p^{(r)^{-1}}E^{(r)^{-1}}h^{-1}(y)$  соответственно.

В состав ключа этого шифра, как и шифра по общей схеме, могут входить любые его компоненты  $g_i^{(l)}$ ,  $\eta_i^{(l)}$  и  $\eta$ . Его можно задать и подмножеством отображений  $G_i^{(l)}$ ,  $f_i^{(l)}$  и  $h$ . В частности, если в данном шифре перестановка  $f_1$  тождественная, перестановки  $f_2, \dots, f_r, h$  фиксированные, а ключ образуется только из подстановок  $G_i^{(l)}$ , то получается шифр, известный по имени Люцифер [1]. Именно поэтому описанные в этом разделе шифры SIBCiphers и отнесены к семейству под этим именем.

#### ЛИТЕРАТУРА

1. Хоффман Л. Дж. Современные методы защиты информации. М.: Сов. радио, 1980. 264 с.
2. Агibalов Г. П. Методы решения систем полиномиальных уравнений над конечным полем // Вестник Томского государственного университета. Приложение. Август 2006. № 17. С. 4–9.
3. Courtois N. and Pieprzyk J. Cryptanalysis of block ciphers with overdefined systems of equations // ASIACRYPT 2002. LNCS. 2002. V. 2501. P. 267–287.
4. Biham E. and Shamir A. Differential cryptanalysis of DES-like cryptosystems // J. Cryptology. 1991. No. 4. P. 3–72.
5. Агibalов Г. П. Элементы теории дифференциального криптоанализа итеративных блочных шифров с аддитивным раундовым ключом // Прикладная дискретная математика. 2008. № 1. С. 34–42.
6. Агibalов Г. П., Панкратова И. А. Статистические аналоги дискретных функций и их применение в криптоанализе симметричных шифров // Прикладная дискретная математика. 2010. № 3(9). С. 51–68.
7. Matsui M. Linear cryptanalysis method for DES cipher // LNCS. 1993. V. 765. P. 386–397.
8. Matsui M. The first experimental cryptanalysis of the Data Encryption Standard // LNCS. 1994. V. 839. P. 1–11.
9. Агibalов Г. П. Распознавание операторов, реализуемых в автономных автоматах // Конф. по теории автоматов и искусственному мышлению. Ташкент, 27–31 мая 1968. Аннотации докладов и программа. М.: ВЦ АН СССР, 1968. С. 7–8.
10. Агibalов Г. П., Левашиников А. А. Статистическое исследование задачи опознания булевых функций одного класса // Тез. докл. к Всесоюзному colloквиуму по автоматизации синтеза дискретных вычислительных устройств, 20–25 сентября 1966. Новосибирск, 1966. С. 40–45.
11. Агibalов Г. П. Минимизация числа аргументов булевых функций // Проблемы синтеза цифровых автоматов. М.: Наука, 1967. С. 96–100.
12. Агibalов Г. П. О некоторых доопределениях частичной булевой функции // Труды Сибирского физико-технического института. Проблемы кибернетики. 1970. Вып. 49. С. 12–19.
13. Агibalов Г. П., Сунгурова О. Г. Криптоанализ конечно-автоматного генератора ключевого потока с функцией выходов в качестве ключа // Вестник Томского государственного университета. Приложение. Август 2006. № 17. С. 104–108.
14. Введение в криптографию / под ред. В. В. Яценко. М.: МЦНМО, «ЧеРо», 1998. 272 с.

15. Паникратова И. А. Булевы функции в криптографии: учеб. пособие. Томск: Издательский Дом Томского государственного университета, 2014. 88 с.

УДК 519.24

## АСИМПТОТИЧЕСКИЕ СВОЙСТВА МНОЖЕСТВА РЕШЕНИЙ ИСКАЖЁННЫХ СИСТЕМ УРАВНЕНИЙ

А. В. Волгин

Рассматриваются две однородные системы уравнений: система уравнений, в левой части которых стоят функции  $k$ -значной логики, и система уравнений, в левой части которых стоят функции, полученные из функций первой системы путём их независимого случайного искажения. Выведены условия на вероятностные законы искажений функций, обеспечивающие три варианта взаимного поведения множеств решений этих систем при согласованном увеличении числа уравнений и числа неизвестных.

**Ключевые слова:** системы уравнений, функции  $k$ -значной логики, искажённые функции.

Пусть  $\Omega_k = \{0, 1, \dots, k-1\}$ ,  $F_k(n) = \{f : \Omega_k^n \rightarrow \Omega_k\}$  — множество всех  $n$ -местных функций  $k$ -значной логики от переменных  $x_1, \dots, x_n$ ,  $n, k \in \mathbb{N}$ . Рассмотрим систему из  $T \in \mathbb{N}$  уравнений

$$f_t(x) = 0, \quad f_t \in F_k(n), \quad t = 1, \dots, T. \quad (1)$$

Через  $S$  обозначим множество решений системы (1).

Каждой функции  $f \in F_k(n)$  сопоставим множества  $A_0(f)$  и  $A_1(f)$  тех значений аргумента, на которых она принимает значение нуль и отлична от нуля соответственно. Обозначим  $a_0(f) = |A_0(f)|$ ,  $a_1(f) = |A_1(f)|$ . Для каждой функции  $f \in F_k(n)$  и целого числа  $0 \leq d \leq a_0(f)$  рассмотрим множество функций

$$B(f, d) = \{g \in F_k(n) : |A_0(f) \cup A_1(g)| + |A_1(f) \cup A_0(g)| = d\},$$

таких, что при  $g \in B(f, d)$  число значений аргументов, в которых одна из функций  $f$  и  $g$  принимает значение нуль, а другая отлична от нуля, равно  $d$ .

На множествах  $B(f_1, d), \dots, B(f_T, d)$  зададим равномерные вероятностные распределения, в соответствии с которыми выберем случайно и независимо функции  $\tilde{f}_1, \dots, \tilde{f}_T$ . Рассмотрим систему случайных уравнений

$$\tilde{f}_t(x_1, \dots, x_n) = 0, \quad \tilde{f}_t \in B(f_t, d), \quad t = 1, \dots, T. \quad (2)$$

Множество её решений обозначим через  $\tilde{S}$ .

Рассматривается задача нахождения связи между множествами  $S$  и  $\tilde{S}$  решений систем уравнений (1) и (2) при выполнении следующих асимптотических условий: при  $T, n \rightarrow \infty$  сами функции  $f_1, \dots, f_T$  меняются так, что

- 1) число решений системы (1) имеет конечный предел, т. е.  $|S| \rightarrow \Sigma \in \mathbb{N}$ ;
- 2) число значений аргументов, на которых функции  $f_t$ ,  $t = 1, \dots, T$ , принимают значение нуль, неограниченно возрастает, т. е.  $a_0(f_t) \rightarrow \infty$ ,  $t = 1, \dots, T$ .

В [1] данная задача рассматривается для случая булевых уравнений, при этом предполагается, что каждая функция системы (1) является уравновешенной, т. е. принимает каждое из значений нуль и единица ровно на  $2^{n-1}$  значениях аргумента. В данной

работе рассматривается обобщение на случай произвольных функций  $k$ -значной логики с учётом асимптотических условий 1 и 2, при этом уравновешенности функций не требуется.

Обозначим  $a_{\min} = \min\{a_0(f_1), \dots, a_0(f_T)\}$ ,  $a_{\max} = \max\{a_0(f_1), \dots, a_0(f_T)\}$ .

**Теорема 1.** Пусть  $n, T \rightarrow \infty$ ,  $|S| \rightarrow \Sigma \in \mathbb{N}$ ,  $T/a_{\min} \rightarrow 0$ . Тогда:

1) если параметр  $d$  меняется так, что  $d \sum_{t=1}^T \frac{N^n - a_0(f_t)}{a_0(f_t)N^n} \rightarrow \infty$ , то

$$\mathbf{P}\{\tilde{S} \cap S = \emptyset\} \rightarrow 1;$$

2) если параметр  $d$  меняется так, что  $d \sum_{t=1}^T \frac{N^n - a_0(f_t)}{a_0(f_t)N^n} \rightarrow \varkappa \in (0, \infty)$  и  $\frac{Td}{a_{\min}} < c$ ,  $c = \text{const} > 0$ , то распределение случайной величины  $|\tilde{S} \cap S|$  сходится к  $\text{Bi}(\Sigma, e^{-\varkappa})$  — биномиальному распределению с параметрами  $\Sigma$  и  $e^{-\varkappa}$ ;

3) если параметр  $d$  меняется так, что  $d \sum_{t=1}^T \frac{N^n - a_0(f_t)}{a_0(f_t)N^n} \rightarrow 0$  и  $a_{\max} < \frac{N^n}{2}$ , то

$$\mathbf{P}\{S \subseteq \tilde{S}\} \rightarrow 1.$$

#### ЛИТЕРАТУРА

1. Михайлов В. Г. Оценка точности пуассоновской аппроксимации для числа пустых ячеек в равновероятной схеме размещения частиц комплектами и её применения // Труды Матем. ин-та им. В. А. Стеклова РАН. 2013. Т. 282. С. 165–180.

УДК 519.7

## ВЛИЯНИЕ ВЕСА ХЭММИНГА РАЗНОСТИ НА ВЕРОЯТНОСТЬ ЕЁ СОХРАНЕНИЯ ПОСЛЕ АРИФМЕТИЧЕСКИХ ОПЕРАЦИЙ<sup>1</sup>

А. И. Пестунов

Теоретически исследована зависимость между вероятностью сохранения разности двух величин после их сложения (вычитания) по модулю с третьей равномерно распределённой величиной и весом Хэмминга этой разности. Под разностью понимается общепринятая в криптоанализе операция XOR. Доказано, что если старший бит разности равен 0, то вероятность её сохранения равна  $2^{-h}$ , где  $h$  — вес Хэмминга разности, и равна  $2^{-(h-1)}$ , если старший бит разности равен 1.

**Ключевые слова:** дифференциальный криптоанализ, разностный анализ, блочный шифр, вес Хэмминга.

Дифференциальный криптоанализ [1] вместе со своими модификациями является распространённым подходом к анализу стойкости итеративных блочных шифров, однако далеко не всегда авторы дифференциальных атак обосновывают их строго математически. Тем не менее некоторые шаги в этом направлении предпринимаются. Так, в работе [2] предложена модель марковского шифра, в рамках которой вычисляются вероятности характеристик; там же сформулирована гипотеза стохастической эквивалентности, негласно подразумеваемая в более ранних работах. В [3] показана возможность создания шифра, доказуемо стойкого к дифференциальному криптоанализу, а в [4] разработана модель, позволяющая создать такой шифр. Работа [5] посвящена изложению дифференциального криптоанализа в общем виде применительно

<sup>1</sup>Работа поддержана грантом РФФИ, проект № 14-01-31484 (мол\_а).

к произвольным итеративным блочным шифрам с аддитивным раундовым ключом. Автор [6] аналитически вычисляет вероятность успеха дифференциальной атаки в зависимости от параметров шифра. В [7] предложена формализация основных понятий дифференциального криптоанализа и проведена их систематизация.

Другой важной проблемой является изучение того, как изменяется разность блоков или подблоков после операций, используемых в блочных шифрах. При этом оценивается вероятность того, что пара величин с определённой разностью преобразуется заданной операцией в пару величин с такой же или другой, но определённой разностью. Для некоторых операций, например циклического сдвига или XOR, данная проблема решается тривиально, но для таких часто используемых операций, как сложение, вычитание и умножение по модулю изучение изменения разности нетривиально.

В работе, посвящённой дифференциальному криптоанализу шифра RC5 [8], утверждается, что однобитовая разность остаётся неизменной после операции сложения с вероятностью  $1/2$  (или с вероятностью 1, если этот единственный бит — старший). Данное утверждение теоретически не доказывается, но проводятся эксперименты, подтверждающие достоверность разработанной атаки. В работах по дифференциальному криптоанализу шифров MARS [9] и CAST-256 [10] данный факт используется со ссылкой на [8] и последующими экспериментами, подтверждающими достоверность разработанных атак. В работе [11] этот факт доказан теоретически.

В [10] используется экспериментально найденная зависимость между весом Хэмминга разности и вероятностью её сохранения после сложения по модулю. В настоящей работе существование этой зависимости доказано теоретически и показано её существование для операции вычитания.

Используем обозначения:  $s$  — длина двоичного вектора (в битах);  $X \sim \mathcal{U}\{0, 1\}^s$  —  $X$  имеет равномерное распределение на  $\{0, 1\}^s$ ;  $\boxplus, \boxminus$  — соответственно сложение и вычитание по модулю  $2^s$ ;  $\delta_{s-1}$  — старший бит вектора  $\Delta$ ;  $H(\Delta)$  — вес Хэмминга вектора  $\Delta$ .

Основным результатом работы является следующая

**Теорема 1.** Пусть  $X, Z \sim \mathcal{U}\{0, 1\}^s$  и  $Y = X \oplus \Delta$ , где  $H(\Delta) = h$ ,  $0 \leq h \leq s - 1$ .

Тогда

- а)  $\mathbf{P}((X \boxplus Z) \oplus (Y \boxplus Z) = \Delta) = 2^{-h}$ , если  $\delta_{s-1} = 0$ ;
- б)  $\mathbf{P}((X \boxplus Z) \oplus (Y \boxplus Z) = \Delta) = 2^{-(h-1)}$ , если  $\delta_{s-1} = 1$ .

**Следствие 1.** Пусть  $X, Z \sim \mathcal{U}\{0, 1\}^s$  и  $Y = X \oplus \Delta$ , где  $H(\Delta) = h$ ,  $0 \leq h \leq s - 1$ .

Тогда

- а)  $\mathbf{P}((X \boxminus Z) \oplus (Y \boxminus Z) = \Delta) = 2^{-h}$ , если  $\delta_{s-1} = 0$ ;
- б)  $\mathbf{P}((X \boxminus Z) \oplus (Y \boxminus Z) = \Delta) = 2^{-(h-1)}$ , если  $\delta_{s-1} = 1$ .

Доказательства теоремы и следствия можно найти в [12].

#### ЛИТЕРАТУРА

1. *Biham E. and Shamir A.* Differential cryptanalysis of DES-like cryptosystems // J. Cryptology. 1991. No. 4. P. 3–72.
2. *Lai X. and Massey J.* Markov ciphers and differential cryptanalysis // LNCS. 1991. V. 547. P. 17–38.
3. *Nyberg K. and Knudsen L.* Provable security against a differential attack // J. Cryptology. 1995. No. 8. P. 27–37.
4. *Vaudenay S.* Decorrelation: a theory for block cipher security // J. Cryptology. 2003. No. 16. P. 249–286.

5. Агибалов Г. П. Элементы теории дифференциального криптоанализа итеративных блочных шифров с аддитивным раундовым ключом // Прикладная дискретная математика. 2008. № 1. С. 34–42.
6. Selcuk A. A. On probability of success in linear and differential cryptanalysis // J. Cryptology. 2007. No. 21. P. 131–147.
7. Пестунов А. И. О связях между основными понятиями разностного анализа итеративных блочных шифров // Прикладная дискретная математика. Приложение. 2013. № 6. С. 44–48.
8. Biryukov A. and Kushilevitz E. Improved cryptanalysis of RC5 // LNCS. 1998. V.1403. P. 85–99.
9. Пестунов А. И. Дифференциальный криптоанализ блочного шифра MARS // Прикладная дискретная математика. 2009. № 4. С. 56–63.
10. Пестунов А. И. Дифференциальный криптоанализ блочного шифра CAST-256 // Безопасность информационных технологий. 2009. № 4. С. 57–62.
11. Пестунов А. И. О вероятности протяжки однобитовой разности через сложение и вычитание по модулю // Прикладная дискретная математика. 2012. № 4. С. 53–60.
12. Пестунов А. И. О влиянии веса Хэмминга разности двух величин на вероятность её сохранения после сложения и вычитания // Дискретный анализ и исследование операций. 2013. Т. 20. № 5. С. 58–65.

УДК 519.7

## ОБ ОБОБЩЕНИЯХ МАРКОВСКОГО ПОДХОДА ПРИ ИЗУЧЕНИИ АЛГОРИТМОВ БЛОЧНОГО ШИФРОВАНИЯ

Б. А. Погорелов, М. А. Пудовкина

Рассматриваются свойства алгоритмов блочного шифрования Маркова при укрупнении состояний цепи Маркова, основанных на разбиениях множества открытых текстов. Показано, что такие укрупнения состояний цепи Маркова, порождённые последовательностью промежуточных шифртекстов  $i$ -го раунда,  $i = 1, 2, \dots$ , алгоритма блочного шифрования, также являются цепью Маркова.

**Ключевые слова:** алгоритм шифрования Маркова, цепь Маркова, XSL-алгоритмы шифрования, алгоритмы шифрования Фейстеля.

В работе [1] введён термин «стохастический метод криптоанализа» как обобщение большого класса методов, основанных на построении некоторых  $l$ -раундовых характеристик. Такими методами являются линейный [2], разностный [3] и их обобщения. В стохастическом методе раундовой функции  $i$ -го раунда ставится в соответствие матрица  $\mathbf{p}^{(i)}$  переходов блоков  $(i-1)$ -го раунда в блоки  $i$ -го раунда,  $i = 1, \dots, l$ . Матрица вероятностей переходов блоков разбиения открытого текста  $\mathbf{X}^{(0)}$  в блоки разбиения  $\mathbf{X}^{(l)}$  шифртекста  $l$ -го раунда предполагается равной  $\mathbf{p}^{[l]} = \prod_{i=1}^l \mathbf{p}^{(i)}$ . Для данного предположения требуется, чтобы последовательность, порождённая промежуточными текстами, являлась цепью Маркова. При этом для применения атак на основе стохастического метода существенным является предположение о независимости раундовых ключей, которое используется в линейном методе и различных обобщениях разностного метода.

В данной работе рассматриваются свойства алгоритмов блочного шифрования Маркова при укрупнении состояний цепи Маркова, основанных на таких разбиениях  $U = (U_1, \dots, U_d)$  множества  $X^\times$  (называемых далее  $U^{(\mu)}$ -разбиениями), что раз-

биение  $U$  порождает метрику на  $X$ , где  $X^\times = X \setminus \{e\}$ ,  $e$  — единичный элемент абелевой группы  $(X, \otimes)$  с бинарной операцией  $\otimes$ . Близкими к таким разбиениям являются  $W$ -разбиения, где под  $W$ -разбиением понимается разбиение множества  $X$  на блоки одинаковой мощности. В частности, если  $W_0$  — произвольная подгруппа  $(X, \otimes)$ , то рассматриваемым  $W$ -разбиением является множество смежных классов группы  $(X, \otimes)$  по подгруппе  $W_0$ . Заметим, что при рассмотрении разбиения  $\{W_0 \setminus \{e\}, \dots, W_{r-1}\}$  естественным образом получается  $U^{(\mu)}$ -разбиение. Кроме того,  $W$ -разбиения позволяют для XSL-алгоритмов блочного шифрования учитывать не только строение слоя наложения ключа, но и строение линейного слоя. Например, это возможно, если  $W_0$  — инвариантное подпространство линейного преобразования. Блоки  $U^{(\mu)}$ -разбиения интерпретируются как множества разностей пар открытого текста (шифртекста). Заметим, что разбиение  $X^\times$  с блоками единичной длины применяется в разностном методе, а усечённые разности естественным образом задают  $W$ -разбиение.

Показано, что такие укрупнения состояний цепи Маркова, порождённые последовательностями промежуточных шифртекстов  $i$ -го раунда,  $i = 1, 2, \dots$ , алгоритмов блочного шифрования, являются цепью Маркова. Для них выполнен перенос ряда результатов работы [4]. В частности, приведены условия, при которых алгоритмы блочного шифрования на основе схем XSL, Фейстеля и Лея — Мессе [5] являются марковскими относительно рассматриваемых разбиений.

#### ЛИТЕРАТУРА

1. *Minier M. and Gilbert H.* Stochastic cryptanalysis of Crypton // FSE'00. LNCS. 2000. V. 1978. P. 121–133.
2. *Matsui M.* Linear cryptanalysis method for DES cipher // Eurocrypt. LNCS. 1993. V. 765. P. 386–397.
3. *Biham E. and Shamir A.* Differential Cryptanalysis of the Data Encryption Standard. Springer Verlag, 1993.
4. *Lai X., Massey J. L., and Murphy S.* Markov ciphers and differential cryptanalysis // Eurocrypt. LNCS. 1991. V. 547. P. 17–38.
5. *Vaudenay S.* On the Lai — Massey scheme // Asiacrypt. LNCS. 1999. V. 1716. P. 8–19.

УДК 519.7

### О ВЕРОЯТНОСТЯХ $r$ -РАУНДОВЫХ ПАР РАЗНОСТЕЙ XSL-АЛГОРИТМА БЛОЧНОГО ШИФРОВАНИЯ МАРКОВА С ПРИВОДИМЫМ ЛИНЕЙНЫМ ПРЕОБРАЗОВАНИЕМ

М. А. Пудовкина

Раундовая функция XSL-алгоритма блочного шифрования является композицией трёх преобразований: преобразования сдвига (сложение с ключом), нелинейного преобразования (s-бокса) и линейного преобразования. Для XSL-алгоритма блочного шифрования Маркова с приводимым линейным преобразованием вместо «классической»  $r$ -раундовой разностной характеристики в разностном методе рассматривается  $r$ -раундовая характеристика, заданная последовательностью смежных классов инвариантного подпространства линейного преобразования.

**Ключевые слова:** алгоритм шифрования Маркова, инвариантное множество, приводимое линейное преобразование, разностная характеристика.

Пусть  $V_n$  — пространство  $n$ -мерных векторов над полем  $\text{GF}(2)$  с операцией векторного сложения  $\oplus$ ;  $x_1, \dots, x_t \in_U X$  — элементы  $x_1, \dots, x_t$  выбираются случайно равномерно и независимо из множества  $X$ ;  $S(X)$  — симметрическая группа на множестве  $X$ ;  $\alpha^g = \alpha g = g(\alpha)$  — образ элемента  $\alpha \in X$  при действии на него подстановкой  $g \in S(X)$ ;  $X^\times = X \setminus \{\vec{0}\}$ ,  $X \subseteq V_n$ ;  $n = d \cdot m$ ,  $\tilde{s} \in S(V_m)$ ,  $h \in \text{GL}_n(2)$ ,  $s = (\tilde{s}_{d-1}, \dots, \tilde{s}_0) \in S(V_m)^d$ , где  $s : \alpha \mapsto (\tilde{\alpha}_{d-1}^{\tilde{s}}, \dots, \tilde{\alpha}_0^{\tilde{s}})$ .

Рассмотрим XSL-алгоритм блочного шифрования Маркова с раундовой функцией  $g_{k^{(i)}} \in S(V_n)$ , заданной как

$$g_{k^{(i)}} : \alpha \mapsto (\alpha \oplus k^{(i)})^{sh},$$

где  $k^{(i)}$  —  $n$ -битный раундовый ключ  $i$ -го раунда,  $i \in \mathbb{N}$ .

Для преобразования  $b \in S(V_n)$  и векторов  $\varepsilon, \delta \in V_n$  положим

$$p_{\varepsilon, \delta}^{[n]}(b) = 2^{-n} \left| \left\{ \beta \in V_n \mid (\beta \oplus \varepsilon)^b \oplus \beta^b = \delta \right\} \right|.$$

Заметим, что для векторов  $\varepsilon = (\tilde{\varepsilon}_{d-1}, \dots, \tilde{\varepsilon}_0) \in V_m^d$ ,  $\delta = (\tilde{\delta}_{d-1}, \dots, \tilde{\delta}_0) \in V_m^d$  справедливо равенство

$$p_{\varepsilon, \delta}^{[n]}(s) = \prod_{i=0}^{d-1} p_{\tilde{\varepsilon}_i, \tilde{\delta}_i}^{[m]}(\tilde{s}^{(i)}).$$

Пусть  $k \in_U V_n$  и  $\alpha$  — произвольный фиксированный вектор из  $V_n$ . Тогда для векторов  $\varepsilon, \delta \in V_n^\times$  положим

$$p_{\varepsilon, \delta}(g|\alpha) = \mathbf{P} \{ \alpha^{gk} \oplus (\alpha \oplus \varepsilon)^{gk} = \delta \}.$$

Из определения алгоритма блочного шифрования Маркова [1] следует, что  $p_{\varepsilon, \delta}(g) = p_{\varepsilon, \delta}(g|\alpha)$ .

Множество  $\Lambda$ ,  $\Lambda \subset V_n^\times$ , назовём *инвариантным* относительно линейного преобразования  $h$ , если  $\Lambda^h = \Lambda$ .

Пусть  $\Lambda_0 = \Lambda \cup \{\vec{0}\}$ ,  $\Lambda_0$  — инвариантное подпространство преобразования  $h$  в  $V_n$ ,  $b_{\Lambda_0} = \dim \Lambda_0$  и  $\Lambda_\delta = \Lambda_0 \oplus \delta$ ,  $\delta \in V_n^\times$ . Положим  $\theta_0 = \vec{0}$  и  $\Lambda_{\theta_i}$  —  $i$ -й смежный класс  $V_n$  по  $\Lambda_0$ ,  $i = 0, \dots, 2^{n-b_{\Lambda_0}} - 1$ .

Зафиксируем произвольные взаимно однозначные отображения

$$\varphi_{\Lambda_{\theta_q}} : \Lambda_{\theta_q} \rightarrow \{1, \dots, |\Lambda_{\theta_q}|\}, \quad i = 1, \dots, 2^{n-b_{\Lambda_0}} - 1.$$

Смежным классам  $\Lambda_\theta$ ,  $\Lambda_\delta$  поставим в соответствие  $|\Lambda_\theta| \times |\Lambda_\delta|$ -матрицу  $\tilde{\mathbf{q}}_{\Lambda_\theta, \Lambda_\delta} = (\tilde{q}_{i,j}^{[\theta, \delta]})$ , где  $\tilde{q}_{i,j}^{[\theta, \delta]} = p_{\varphi^{-1}(i), \varphi^{-1}(j)}^{[n]}(s)$ .

В этом случае для нахождения  $r$ -раундовой разностной характеристики рассмотрим последовательность номеров смежных классов  $\bar{\theta} = (\theta_{i_0}, \theta_{i_1}, \dots, \theta_{i_r})$  и  $|\Lambda_{\theta_{i_0}}| \times |\Lambda_{\theta_{i_r}}|$ -матрицу  $\tilde{\mathbf{q}}_{\bar{\theta}}^{(r)} = (\tilde{q}_{c_1, c_2}^{[\bar{\theta}]})$ , где  $\tilde{\mathbf{q}}_{\bar{\theta}}^{(r)} = \prod_{j=1}^r \tilde{\mathbf{q}}_{\Lambda_{\theta_{i_{j-1}}}, \Lambda_{\theta_{i_j}}}$ . Тогда вероятность  $r$ -раундовой пары разностей  $(\lambda, \lambda') \in \Lambda_{\theta_{i_0}} \times \Lambda_{\theta_{i_r}}$  оценивается снизу  $\tilde{q}_{\varphi_{\theta_{i_0}}(\lambda), \varphi_{\theta_{i_r}}(\lambda')}^{[\bar{\theta}]}$ .

Таким образом, учёт инвариантного подпространства и его смежных классов может позволить улучшить оценки снизу вероятности  $r$ -раундовой пары разностей  $(\lambda, \lambda') \in \Lambda_{\theta_{i_0}} \times \Lambda_{\theta_{i_r}}$  по сравнению с нахождением вероятности «классической» разностной характеристики. Если размерность инвариантного подпространства  $\Lambda_0$  небольшая, например  $\dim \Lambda_0 \leq 16$ , то данный подход применим на практике. В этом случае в памяти

требуется хранить не больше  $r$  матриц из  $2^{2b_{\Lambda_0}}$  элементов. Полученные вероятности  $\tilde{q}_{\varphi_{\theta_{i_0}}(\omega_0), \varphi_{\theta_{i_r}}(\omega_r)}^{[\theta]}$  могут увеличить число атакуемых раундов. Поэтому приведённый подход эффективнее по сравнению со способом нахождения вероятностей «классических» разностных характеристик. Отметим, что аналогичным образом можно рассматривать матрицы, соответствующие объединению нескольких смежных классов или инвариантных непересекающихся подмножеств. Предложенный подход проиллюстрирован на примере инволютивного алгоритма блочного шифрования ICEBERG [2], представленного на конференции FSE в 2004 г. Проведено сравнение полученных результатов с результатами работы [3].

#### ЛИТЕРАТУРА

1. *Lai X., Massey J. L., and Murphy S.* Markov ciphers and differential cryptanalysis // EUROCRYPT'1991. LNCS. 1991. V. 547. P. 17–38.
2. *Standaert F. X., Piret G., Rouvroy G., et al.* ICEBERG: an involutinal cipher efficient for block encryption in reconfigurable hardware // FSE'2004. LNCS. 2004. V. 3017. P. 279–299.
3. *Sun Y., Wang M., Jiang S., and Jiang Q.* Differential cryptanalysis of reduced-round ICEBERG // AFRICACRYPT'2012. LNCS. 2012. V. 7374. P. 155–171.

УДК 519.7

### УСЛОВИЯ СУЩЕСТВОВАНИЯ СОВЕРШЕННЫХ ШИФРОВ С ФИКСИРОВАННЫМ НАБОРОМ ПАРАМЕТРОВ

С. М. Рацеев

Исследуется задача построения совершенных шифров по заданному множеству открытых текстов  $X$ , ключей  $K$  и распределению вероятностей  $P_K$  на множестве ключей. Приводится критерий, позволяющий однозначно определить, существует ли для заданных  $X$ ,  $K$ ,  $P_K$  совершенный шифр.

**Ключевые слова:** шифр, совершенный шифр.

Пусть  $X$ ,  $K$ ,  $Y$  — конечные множества открытых текстов, ключей и шифрованных текстов соответственно. Обозначим через  $\Sigma_B = (X, K, Y, E, D, P_X, P_K)$  вероятностную модель шифра [1, 2], где  $E$  и  $D$  — множества правил зашифрования и расшифрования соответственно. Напомним, что шифр  $\Sigma_B$  называется совершенным (по Шеннону), если для любых  $x \in X$ ,  $y \in Y$  выполнено равенство  $P_{X|Y}(x|y) = P_X(x)$ .

Рассмотрим следующую задачу: по заданному множеству открытых текстов  $X_0$  и множеству ключей  $K_0$  с распределением вероятностей  $P_{K_0}$  (независимо от  $P_{X_0}$ ) однозначно определить, существует ли шифр  $\Sigma_B = (X_0, K_0, Y, E, D, P_{X_0}, P_{K_0})$ , являющийся совершенным. Таким образом, по заданным  $X_0$ ,  $K_0$ ,  $P_{K_0}$  требуется определить, найдутся ли такие  $Y$ ,  $E$ ,  $D$ , для которых шифр  $\Sigma_B$  являлся бы совершенным.

**Теорема 1.** Для заданных  $X$ ,  $|X| = n$ ,  $K$ ,  $P_K$  существует совершенный шифр

$$\Sigma_B = (X, K, Y, E, D, P_X, P_K)$$

тогда и только тогда, когда найдётся такое натуральное число  $s$  и  $n$  таких разбиений множества  $K$

$$\begin{aligned} K &= K_{11} \cup K_{12} \cup \dots \cup K_{1s}, & K_{1i} \cap K_{1j} &= \emptyset, & 1 \leq i < j \leq s, \\ K &= K_{21} \cup K_{22} \cup \dots \cup K_{2s}, & K_{2i} \cap K_{2j} &= \emptyset, & 1 \leq i < j \leq s, \\ &\dots \\ K &= K_{n1} \cup K_{n2} \cup \dots \cup K_{ns}, & K_{ni} \cap K_{nj} &= \emptyset, & 1 \leq i < j \leq s, \end{aligned} \quad (1)$$

для которых выполнены следующие условия:

- 1)  $K_{it} \cap K_{jt} = \emptyset, 1 \leq i < j \leq n, t = 1, \dots, s;$
- 2) для любых  $1 \leq i < j \leq n, t = 1, \dots, s$  выполнено равенство

$$\sum_{k \in K_{it}} P_K(k) = \sum_{k \in K_{jt}} P_K(k).$$

Пусть для некоторого числа  $s$  выполнены равенства (1) и условия 1 и 2 теоремы. Тогда матрица зашифрования  $A$  для (совершенного) шифра  $\Sigma_B$  строится следующим образом. Пусть  $Y = \{y_1, \dots, y_s\}$  — некоторое множество шифрованных текстов, где  $s$  — число частей разбиений из (1). Составим матрицу зашифрования размера  $|K| \times |X|$ , где строки пронумерованы элементами множества  $K$ , а столбцы — элементами множества  $X$ , следующим образом. В  $i$ -м столбце ( $i = 1, \dots, |X|$ ) данной матрицы в строках, пронумерованных элементами множества  $K_{ij}$ , поставим элемент  $y_j, j = 1, \dots, s$ .

**Следствие 1.** Пусть для заданных  $X, K, P_K$  существует совершенный шифр. Тогда для любого множества открытых текстов  $\tilde{X}, |\tilde{X}| \leq |X|$ , и для заданных  $K, P_K$  существует совершенный шифр.

**Следствие 2.** Для заданных  $X, |X| = n, K, P_K, Y, |Y| = s$ , существует совершенный шифр  $\Sigma_B = (X, K, Y, E, D, P_X, P_K)$  тогда и только тогда, когда найдётся  $n$  таких разбиений (1), для которых выполнены условия 1 и 2 теоремы 1.

**Следствие 3.** Для заданных  $K, P_K$  существует совершенный шифр  $\Sigma_B$  тогда и только тогда, когда найдутся такие  $n$  и  $s, n \leq s$ , и такие разбиения (1), для которых выполнены условия 1 и 2 теоремы 1.

Пусть  $P_{\text{im}}$  — вероятность успеха имитации,  $P_{\text{podm}}$  — вероятность успеха подмены шифрованного сообщения для шифра  $\Sigma_B$ .

**Следствие 4.** Пусть для шифра  $\Sigma_B$  (с матрицей зашифрования  $A$ ) выполнены равенства (1) с условиями 1 и 2 теоремы 1. Тогда

$$\begin{aligned} P_{\text{im}} &= n \max_{1 \leq i \leq s} \sum_{k \in K_{1i}} P_K(k), \\ P_{\text{podm}} &= \frac{1}{n} \max_{\substack{1 \leq i, j \leq s \\ i \neq j}} \frac{\sum_{k \in K_i \cap K_j} P_K(k)}{\sum_{k \in K_{1i}} P_K(k)}, \end{aligned}$$

где  $K_i = \bigcup_{j=1}^n K_{ji}, i = 1, \dots, s$ .

Отметим, что некоторый интерес представляют совершенные шифры с дополнительными условиями, например условиями имитостойкости. О таких шифрах можно посмотреть в работах [2–4].

## ЛИТЕРАТУРА

1. Алферов А. П., Зубов А. Ю., Кузьмин А. С., Черемушкин А. В. Основы криптографии. М.: Гелиос АРВ, 2005. 480 с.
2. Зубов А. Ю. Криптографические методы защиты информации. Совершенные шифры. М.: Гелиос АРВ, 2005. 192 с.
3. Рацеев С. М. О совершенных имитостойких шифрах // Прикладная дискретная математика. 2012. № 3 (17). С. 41–47.
4. Рацеев С. М. О совершенных имитостойких шифрах замены с неограниченным ключом // Вестник Самарского государственного университета. Естественнонаучная серия. 2013. № 9/1 (110). С. 42–48.

УДК 512.62

**КРИПТОГРАФИЧЕСКИЙ АНАЛИЗ АНАЛОГА СХЕМЫ ДИФФИ — ХЕЛЛМАНА, ИСПОЛЬЗУЮЩЕГО СОПРЯЖЕНИЕ И ВОЗВЕДЕНИЕ В СТЕПЕНЬ, НА МАТРИЧНОЙ ПЛАТФОРМЕ<sup>1</sup>**

В. А. Романьков

Доказано, что смешанный обобщённый вариант протокола Диффи — Хеллмана на матричной платформе, использующий одновременное возведение в степень и сопряжение фиксированной матрицы, в генерическом случае допускает вычисление разделённого ключа за полиномиальное время, если соответствующая кратная задача дискретного логарифма решается за полиномиальное время. Алгоритм вычисления использует разработанный автором метод линейного разложения, позволяющий находить разделённый ключ без решения задачи поиска сопрягающих элементов, и подход Менезеса с соавт., сводящий вычисление степени матрицы к решению кратной задачи дискретного логарифма. Комбинация этих двух подходов не может использоваться напрямую. Доказательство основного утверждения требует анализа содержаний мономиальных матриц в смежных классах по перестановочным подгруппам группы матриц. Это, в свою очередь, требует изучения аналогичного вопроса для групп подстановок. Последнее облегчается тем, что имеется ряд известных утверждений на эту тему.

**Ключевые слова:** криптоанализ, проблема поиска, сопряжение, протокол Диффи — Хеллмана.

Идея реализации протокола Диффи — Хеллмана на различных платформах, отличных от классических мультипликативных групп конечных полей и завоевавших признание групп эллиптических кривых, использована в целом ряде работ. Чаще всего в качестве платформы выбирались матричные группы, также предлагались конечные и абстрактные бесконечные группы, почти всегда допускающие точное представление матрицами над полем (кроме конечных — это свободные, конечно порождённые нильпотентные и метабелевы, а также полициклические группы, группы кос Артина и т. п.). В данной работе мы ограничимся рассмотрением матричного случая. В начальный период схема Диффи — Хеллмана просто переносилась с мультипликативной группы поля на матричную группу, то есть фиксировался элемент  $g$  матричной группы  $G$ , первый из корреспондентов (Алиса) выбирал случайное натуральное число  $k$  и посылал по открытой сети степень  $g^k$ , второй корреспондент (Боб) аналогично выбирал  $l$  и посылал  $g^l$ . После этого Алиса и Боб легко вычисляли общий ключ  $g^{kl}$ .

<sup>1</sup>Работа поддержана грантом РФФИ, проект № 13-01-00239-а.

Впрочем, довольно быстро было замечено [1, 2], что в случае матричной группы над полем можно одновременно сопряжением одной и той же матрицей в общем случае над расширением основного поля за счёт характеристических чисел фиксированной матрицы  $g$  приводить матрицу  $g$  к жордановой форме, а матрицы  $g^k$  и  $g^l$  — к соответствующим степеням этой жордановой формы. В случае, если размер хотя бы одной клетки жордановой формы матрицы  $g$  оказывался больше единицы, а степени  $k$  и  $l$  были меньше характеристики основного поля, эти числа вычислялись элементарно.

Основным, таким образом, оказывался случай, когда матрица  $g$  имела диагональную жорданову форму. Тогда вычисление секретных параметров  $k$  и  $l$  сводилось к решению кратных проблем дискретного логарифма для соответствующих друг другу наборов диагональных элементов полученных матриц. Конечно, в общем случае кратная проблема не сложнее обычной, а при случайном выборе данных может оказаться значительно проще обычной задачи вычисления дискретного логарифма в мультипликативной группе конечного поля. Действительно, задачу достаточно решить хотя бы для одной пары соответствующих диагональных элементов. К тому же тогда не имеет смысла рассматривать данный протокол как обобщение протокола Диффи — Хеллмана на некоммутативные платформы. Для полей нулевой характеристики задача, как правило, решается ещё проще и практически не рассматривается.

По только что описанной причине стали предлагать вместо возведения в степень сопряжение матрицы  $g$  матрицами  $a$  и  $b$ , которые случайным образом генерировались корреспондентами Алисой и Бобом (см., например, хорошо известный протокол Ко, Ли и др. [3]). Напомним, что сопряжение матрицы  $g$  матрицей  $a$  записывается как  $g^a = a^{-1}ga$ . Корреспонденты передают по сети результаты сопряжений  $g^a$  и  $g^b$ , а разделённый ключ вычисляется как  $g^{ab} = g^{ba}$ . Чтобы последнее равенство было справедливым, требуется, чтобы Алиса выбирала  $a$  из подгруппы  $A$ , а Боб —  $b$  из подгруппы  $B$  группы  $G$ , таких, что любой элемент  $a$  из  $A$  перестановочен с любым элементом  $b$  из  $B$ . Это возможно, например, если  $A = B$  — абелева подгруппа группы  $G$ . Такой протокол основывался на трудности вычисления сопрягающих элементов по исходному и сопряжённому элементам. В дальнейшем происходил поиск групп, в которых эта проблема трудна. Почти всегда всё сводилось к вычислению в матричных группах. Например, как уже упоминалось выше, одна из наиболее популярных серий групп кос Артина может рассматриваться как серия матричных групп, поскольку все группы этой серии допускают точные и, что также имеет значение, эффективные представления матрицами над полем.

Однако оказалось, что в таких случаях совсем не обязательно вычислять матрицы  $a$  и  $b$ , чтобы получить разделённый ключ  $g^{ab}$ . Метод линейного разложения, описанный автором в [4] (см. также [5]), позволяет за полиномиальное время с помощью стандартных вычислений линейной алгебры найти  $g^{ab}$  без вычисления  $a$  и  $b$ . Таким образом, использованные в подобных протоколах предположения секретности, опиравшиеся на обоснования трудности решения проблемы поиска сопрягающего элемента, оказались бесполезными.

Но есть ещё один, смешанный, вариант протокола, когда Алиса выбирает число  $k$  и матрицу  $a$ , посылая по сети результат  $(g^k)^a$ , а Боб аналогично выбирает и посылает  $(g^l)^b$ . Разделённый ключ имеет вид  $(g^{kl})^{ab}$ . Этот протокол также неоднократно предлагался в различных версиях (см., например, [6]). Непосредственно вычислить этот ключ, используя метод линейного разложения, нельзя, так как возведение в степень не является автоморфизмом матричной группы. Вычислить  $k$  и  $l$  также затруднительно, поскольку сопряжения после приведения к жордановой форме содержат

диагональные элементы не в том порядке, как их содержала матрица  $g$ . Для вычисления параметров на первый взгляд нужно рассмотреть  $n!$  кратных задач дискретного логарифма, где  $n$  — размер матриц. В общем случае это нереально. Основным результатом настоящей работы является следующая теорема, показывающая, что задача тем не менее решается в генерическом случае за полиномиальное время. Это обусловлено тем, что число случаев, которые действительно необходимо рассмотреть, значительно меньше  $n!$ , и в пределе равно 1.

**Теорема 1.** Смешанный обобщённый вариант протокола Диффи — Хеллмана, описанный выше, в генерическом случае допускает вычисление разделённого ключа  $(g^{kl})^{ab}$  за полиномиальное время, если соответствующая кратная задача дискретного логарифма решается за полиномиальное время.

Слово «генерический» в данном контексте означает, что при случайном выборе коммутирующих поэлементно подгрупп  $A$  и  $B$  заявленное полиномиальное вычисление возможно «почти всегда» относительно естественной меры или асимптотически.

Поясним, что фигурирующая в формулировке кратная задача предполагается записанной для соответствующих друг другу наборов характеристических чисел исходной матрицы  $g$  и их степеней — характеристических чисел возведённой в эту степень матрицы  $g$ . Возможность полиномиального вычисления из формулировки теоремы объясняется тем, что сопрягающие элементы выбираются корреспондентами из коммутирующих поэлементно подгрупп, а в группах подстановок коммутирующие подгруппы допускают эффективное описание. В матричных группах подгруппа, элементы которой коммутируют с элементами другой достаточно «большой» подгруппы, не может содержать большой подгруппы мономиальных матриц.

#### ЛИТЕРАТУРА

1. *Menezes A. J. and Vanstone S.* A note on cyclic groups, finite fields, and the discrete logarithm problem // *Appl. Alg. Eng. Commun. Comput.* 1992. No. 3. P. 67–74.
2. *Menezes A. J. and Wu Y.-H.* The discrete logarithm problem in  $GL(n, q)$  // *Ars Combinatoria.* 1997. V. 47. P. 23–32.
3. *Ko K. H., Lee S. J., Cheon J. H., et al.* New public-key cryptosystem using braid groups // *Advances in Cryptology — CRYPTO’2000.* LNCS. 2000. V. 1880. P. 166–183.
4. *Романьков В. А.* Алгебраическая криптография. Омск: ОмГУ, 2013. 135 с.
5. *Романьков В. А.* Криптографический анализ некоторых схем шифрования, использующих автоморфизмы // *Прикладная дискретная математика.* 2013. № 3. С. 36–51.
6. *Kahrobaei D. and Khan B.* A non-commutative generalization of ElGamal key exchange using polycyclic groups // *Global Telecommun. Conf.* 2006. GLOBECOM’06, IEEE. P. 1–5.

## Секция 3

## ПСЕВДОСЛУЧАЙНЫЕ ГЕНЕРАТОРЫ

УДК 519.113.6

ОБ ОДНОМ КЛАССЕ БУЛЕВЫХ ФУНКЦИЙ, ПОСТРОЕННЫХ  
С ИСПОЛЬЗОВАНИЕМ СТАРШИХ РАЗРЯДНЫХ  
ПОСЛЕДОВАТЕЛЬНОСТЕЙ ЛИНЕЙНЫХ РЕКУРРЕНТ

Д. Н. Былков

Изучается семейство булевых функций, построенных на основе старших разрядных последовательностей линейных рекуррент над кольцом  $\mathbb{Z}_2^n$  с отмеченным характеристическим многочленом. Для данного семейства изучаются степень нелинейности функций и алгебраическая степень. Показывается, что указанное семейство содержит функции, значительно удалённые от класса всех аффинных функций.

**Ключевые слова:** *линейные рекуррентные последовательности, старшие разрядные последовательности, степень нелинейности булевой функции.*

В работе [1] изучались свойства булевых функций, построенных на основе последовательностей старших разрядов отмеченных линейных рекуррент над кольцом  $R = \mathbb{Z}_2^n$ . Получены результаты, описывающие веса функций, степень их нелинейности, расстояние между функциями и мощность всего семейства. А. А. Нечаевым предложен к рассмотрению ещё один класс булевых функций, построенных на основе последовательностей старших разрядов, отличающийся другим упорядочиванием вектора значений функции. В настоящей работе приводятся результаты о степени нелинейности и алгебраической степени функций из данного класса.

Пусть  $F(x) \in R[x]$  — унитарный (со старшим коэффициентом 1) реверсивный многочлен степени  $m$ , такой, что его период  $T(F)$  удовлетворяет условию  $T(F) = T(F \bmod 2) = 2^m - 1$ . В этом случае будем говорить, что  $F(x)$  — отмеченный многочлен максимального периода. Обозначим  $L_R(F)$  множество всех линейных рекуррентных последовательностей (ЛРП) над кольцом  $R$  с характеристическим многочленом  $F(x)$  и  $L_R(F)^*$  — множество всех ЛРП  $u \in L_R(F)$ , у которых в начальном векторе  $(u(0), u(1), \dots, u(m-1))$  есть хотя бы один обратимый элемент кольца  $R$ . Каждая последовательность  $u \in L_R(F)^*$  имеет период  $T(u) = T(F) = (2^m - 1)$ .

Подмножество  $K = \{k_0, k_1\}$  множества  $R$  назовём *разрядным множеством* кольца  $R$  (см., например, [2]), если элементы  $k_0$  и  $k_1$ , рассматриваемые как целые числа, имеют различную чётность. Примером разрядного множества кольца  $R$  является *двоичное разрядное множество*  $K = \{0, 1\}$ . Если  $K$  — разрядное множество кольца  $R$ , то каждый элемент  $a$  этого кольца однозначно представим в виде

$$a = a_0 + 2a_1 + 2^2a_2 + 2^3a_3 + \dots + 2^{n-1}a_{n-1}, \quad (1)$$

где  $a_i = \varkappa_i^K(a) \in K$  для всех  $i = 0, 1, \dots, n-1$ . Элемент  $a_i$ , участвующий в равенстве (1), будем называть  *$i$ -м разрядом* элемента  $a$  в разрядном множестве  $K$ .

Сопоставим каждой ЛРП  $u \in L_R(F)^*$  булеву функцию  $f''_{u,K}(x_1, \dots, x_m)$  по правилу  $f''_{u,K}(0, \dots, 0) = \varkappa_{n-1}^K(0) \bmod 2$ ,

$$f''_{u,K}(u_0(i), u_0(i+1), \dots, u_0(i+m-1)) = \varkappa_{n-1}^K(u(i)) \bmod 2,$$

где  $u_0(i) = u(i) \bmod 2$ ,  $0 \leq i \leq 2^m - 1$ . В силу выбора последовательности  $u$  вектор  $(u_0(i), u_0(i+1), \dots, u_0(i+m-1))$  принимает все возможные значения из множества  $\{0, 1\}^m \setminus \{(0, \dots, 0)\}$ , поэтому функция определена на всех двоичных наборах  $\{0, 1\}^m$ . Обозначим  $B_n''(K, F)$  множество всех булевых функций  $f''_{u,K}$ , соответствующих всем ЛРП  $u$  из множества  $L_R(F)^*$ .

Оказывается, что для функций  $f''_{u,K} \in B_n''(K, F)$  справедливы такие же оценки степени нелинейности и алгебраической степени, что и для функций из класса  $B_n'(K, F)$  [1].

**Теорема 1.** Для коэффициентов  $W_f(\mathbf{a})$  Уолша — Адамара булевой функции  $f = f''_{u,K}$  при всех  $n \geq 2$  имеет место оценка

$$|W_f(\mathbf{a})| \leq \left( \frac{2}{\pi} \ln(2^{n-1}) + 1 \right) (2^{n-1} - 1) 2^{m/2}.$$

**Следствие 1.** При  $n = 2$  и каждом чётном  $m$  класс  $B_n''(K, F)$  состоит из бент-функций, а при  $n = 2$  и каждом нечётном  $m$  класс  $B_n''(K, F)$  состоит из платовидных функций порядка  $m - 1$ .

**Теорема 2.** Пусть  $F(x) \in R[x]$  — отмеченный многочлен степени  $m > |R|$  максимального периода над кольцом  $R$ , тогда для любой функции  $f \in B_n''(K, F)$  справедливо соотношение  $\deg f = 2^{n-1}$ .

#### ЛИТЕРАТУРА

1. Былков Д. Н., Камловский О. В. Параметры булевых функций, построенных с использованием старших координатных последовательностей линейных рекуррент // Матем. вопр. криптогр. 2012. Т. 3. № 4. С. 25–53.
2. Kurakin V. L., Kuzmin A. S., Mikhalev A. V., and Nechaev A. A. Linear recurring sequences over rings and modules // J. Math. Sci. (New York). 1995. V. 76. No. 6. P. 2793–2915.

УДК 519.6

### ОЦЕНКИ ЭКСПОНЕНТОВ ПЕРЕМЕШИВАЮЩИХ ГРАФОВ НЕКОТОРЫХ МОДИФИКАЦИЙ АДДИТИВНЫХ ГЕНЕРАТОРОВ

А. М. Дорохова

Для модификации аддитивного генератора с помощью инволютивной перестановки координат векторов исследованы условия полного перемешивания. Доказаны достаточные условия примитивности перемешивающего графа и оценки его экспонента в некоторых случаях. Полученные оценки экспонента показывают, что полное перемешивание знаков состояния генератора может быть достигнуто после числа тактов, которое существенно меньше размера состояний.

**Ключевые слова:** аддитивный генератор, перемешивающий граф преобразования, экспонент графа.

## Введение

Положительным криптографическим свойством генератора гаммы  $\{\gamma_1, \dots, \gamma_i, \dots\}$  является полное перемешивание входных данных, то есть зависимость знаков вырабатываемой гаммы от всех знаков начального состояния. Полное перемешивание достигается для знаков гаммы  $\gamma_i$ , как правило, при  $i \geq \exp \Gamma(\varphi)$ , где  $\varphi$  — преобразование множества внутренних состояний генератора;  $\Gamma(\varphi)$  — перемешивающий граф преобразования  $\varphi$ ;  $\exp \Gamma(\varphi)$  — экспонент графа  $\Gamma(\varphi)$ . Если  $\exp \Gamma(\varphi) = t$ , то начальный отрезок гаммы  $\{\gamma_1, \dots, \gamma_{t-1}\}$  часто называют «холостым ходом» и обычно не используют в ключевой последовательности. Таким образом, определение экспонентов перемешивающих графов криптографических преобразований является важной задачей анализа и синтеза криптографических систем.

Сделана оценка экспонентов перемешивающих графов преобразований, соответствующих некоторым модификациям аддитивных генераторов (аддитивные генераторы называют также запаздывающими генераторами Фибоначчи). Интерес к модификациям вызван тем, что оригинальные схемы аддитивных генераторов полного перемешивания не достигают и вообще признаны нестойкими. В то же время на основе аддитивных генераторов построен ряд алгоритмов: Fish, Pike, Mush [1].

Обзор результатов по экспонентам графов, полученных до 2012 г., дан в [2]. Для перемешивающих графов биективных регистров сдвига над множеством двоичных векторов, к которым относятся, в частности, аддитивные генераторы и рассматриваемые модификации, общие оценки уточнены в [3, 4]. В работе эти оценки получают дальнейшее уточнение за счёт особенностей аддитивных генераторов и их модификаций.

## 1. Аддитивные генераторы

Генераторы построены на основе принципа, использованного в линейных регистрах сдвига, но оперируют с числами в кольце вычетов  $\mathbb{Z}/2^r$ , где  $r > 1$ . Обозначим  $n$  длину регистра, ячейки регистра сдвига занумеруем числами  $0, \dots, n-1$ . Обозначим  $X_0, X_1, \dots, X_{n-1}$  числа из  $\mathbb{Z}/2^r$ , образующие начальное состояние генератора. При  $i \geq n$  знак гаммы  $X_i$  образуется по формуле

$$X_i = \sum_{j=0}^n a_j X_{j+i-n} \pmod{2^r}, \quad (1)$$

где  $a_0, \dots, a_{n-1} \in \{0, 1\}$ . Следовательно, аддитивный генератор есть регистр сдвига длины  $n$  с функцией обратной связи  $f(y_0, \dots, y_{n-1}) = \sum_{j=0}^{n-1} a_j y_j \pmod{2^r}$ . Так как  $a_0 = 1$  (в противном случае длина регистра меньше  $n$ ),  $f(y_1, \dots, y_n)$  биективна по переменной  $y_0$ , то есть регистр реализует подстановку множества состояний [5, теорема 5.5]. Для изучения перемешивающих свойств подстановки генератора используем двоичное представление  $\delta(X_i)$  числа  $X_i$ ,  $i \geq 0$ , являющееся  $r$ -мерным вектором пространства  $V_r$  (младшим битом является  $r$ -й бит), состояние генератора является  $rn$ -мерным вектором пространства  $V_{rn}$ .

## 2. Перемешивающие свойства модифицированного генератора.

Критерий полного перемешивания — примитивность перемешивающего орграфа подстановки; необходимым условием является сильная связность орграфа. Заметим, что для регистра сдвига, определяемого законом рекурсии (1), перемешивающий граф не сильносвязный. Для достижения сильной связности модифицируем аддитивный

генератор с помощью инволюции  $I$  множества  $V_r: I(x_1, \dots, x_r) = (x_r, \dots, x_1)$ . Тогда при  $i \geq n$

$$\delta(X_i) = I \left( \delta \left( \left( X_{i-n} + \sum_{j=1}^{n-1} a_j X_{j+i-n} \right) \bmod 2^r \right) \right). \quad (2)$$

Используем обозначения и результаты работ [3, 4]. Пусть  $\varphi$  — подстановка регистра сдвига. Состояние регистра в текущий момент времени задано двоичной матрицей размера  $r \times n$ , где  $k$ -й столбец матрицы, обозначаемый  $y_{k+1} = (x_{1+rk}, \dots, x_{r+rk})^T$  ( $T$  — транспонирование), записан в  $k$ -й ячейке регистра сдвига,  $k = 0, 1, \dots, n-1$ . Подстановка  $\varphi$  задается системой  $rn$  булевых координатных функций  $\{\varphi_1(x_1, \dots, x_{rn}), \dots, \varphi_{rn}(x_1, \dots, x_{rn})\}$ , где функция  $\varphi_{v+rk}(x_1, \dots, x_{rn})$  вычисляет  $v$ -й бит  $x_{v+rk}$  вектора  $y_{k+1}$ ,  $v = 1, \dots, r$ ,  $k = 0, 1, \dots, n-1$ .

Обозначим  $S(\varphi_j)$  множество номеров существенных булевых переменных функции  $\varphi_j(x_1, \dots, x_{rn})$ ,  $j = 1, \dots, rn$ . Перемешивающий граф  $\Gamma(\varphi)$  подстановки  $\varphi$  есть  $rn$ -вершинный орграф, в котором есть дуга  $(i, j)$ , если и только если  $i \in S(\varphi_j)$ ,  $i, j \in \{1, \dots, rn\}$ .

Обозначим  $\theta$  функцию отождествления вершин орграфа  $\Gamma(\varphi)$ : для  $v = 1, \dots, r$  положим  $\theta(v + rk) = v$ ,  $k = 0, 1, \dots, n-1$ . Функция  $\theta$  индуцирует отображение орграфа  $\Gamma(\varphi)$  в  $r$ -вершинный орграф  $\Gamma(\psi)$ , где  $(v, u)$  есть дуга орграфа  $\Gamma(\psi)$ , если и только если функция  $\varphi_{u+r(n-1)}$  зависит существенно хотя бы от одной из переменных множества  $\{x_v, x_{v+r}, \dots, x_{v+r(n-1)}\}$ ,  $v, u \in \{1, \dots, r\}$ . Орграф  $\Gamma(\varphi)$  сильносвязный, если и только если  $\Gamma(\psi)$  сильносвязный [3, теорема 2].

Определим характеристики перемешивающего графа  $\Gamma(\varphi)$  модифицированного генератора. Из (2) следует, что  $S(\psi_u) = \{r, r-1, \dots, r-u+1\}$ ,  $u = 1, \dots, r$ . Сильная связность орграфов  $\Gamma(\varphi)$  и  $\Gamma(\psi)$  (она достигается сочетанием инволюции  $I$  с суммированием по модулю  $2^r$ ) вытекает, в частности, из наличия в  $\Gamma(\psi)$  дуг  $(r, 1)$ ,  $(r, 2)$ ,  $(r, 3)$ ,  $(r-1, 2)$ ,  $(r-1, 3)$ ,  $(r-2, 3)$ ,  $\dots$ ,  $(r, r)$ ,  $(r-1, r)$ ,  $\dots$ ,  $(3, r)$ ,  $(2, r)$ ,  $(1, r)$ . Графы  $\Gamma(\psi)$  при  $r \in \{3, 4\}$  изображены на рис. 1.

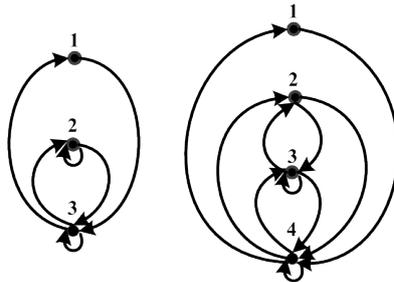


Рис. 1. Графы  $\Gamma(\psi)$  при  $r = 3$  и  $r = 4$

Определим условия примитивности орграфа  $\Gamma(\varphi)$  на основе универсального критерия [2, с. 10]. Из (2) следует, что в графе  $\Gamma(\varphi)$  имеются простые циклы длины  $2n$  вида

$$B_u = (u + r(n-1), u + r(n-2), \dots, u + r, u, r - u + 1 + r(n-1), r - u + 1 + r(n-2), \dots, r - u + 1), \quad u = 1, \dots, \lfloor r/2 \rfloor,$$

$$E_u = (u + r(n-1), u + r(n-2), \dots, u + r, u, r - z + 1 + r(n-1), r - z + 1 + r(n-2), \dots, r - z + 1), \quad u = \lceil (r+1)/2 \rceil, \dots, r-1, z = 1, \dots, u-1,$$

и простые циклы длины  $n$  вида

$$H_u = (u + r(n - 1), u + r(n - 2), \dots, u + r, u), \quad u = \lceil (r + 1)/2 \rceil, \dots, r.$$

Остальные циклы графа  $\Gamma(\varphi)$  определяются точками съёма с регистра (то есть номерами существенных переменных функции обратной связи).

**Теорема 1** (достаточное условие примитивности перемешивающего графа  $\Gamma(\varphi)$ ). Пусть обратная связь модифицированного регистра использует множество точек съёма  $D = \{m - d_0, m - d_1, \dots, m - d_k\}$ , где  $0 = d_0 < d_1 < \dots < d_k = m < n$ . Тогда

- 1)  $S(\varphi_{u+r(n-1)}) = \{x_{v+rt} : v = r, r - 1, \dots, r - u + 1, t \in D\}$ ,  $u = 1, \dots, r$ ;
- 2) граф  $\Gamma(\varphi)$  примитивен, если  $(n, d_1, \dots, d_k) = 1$ .

**Следствие.** Орграф  $\Gamma(\varphi)$  примитивный, если

- 1)  $d_i - d_{i-1} = 1$  при некотором  $i \in \{1, \dots, k\}$ ;
- 2)  $(n, m) = 1$ , в этом случае  $\exp \Gamma(\varphi) \leq n^2 + (2r - 3 - m)n + 2m$ , если  $m \leq n - 2$ ;
- 3) при  $m = n - 1$  выполнена оценка  $\exp \Gamma(\varphi) \leq 2n - 2$ .

**Пример.** Пусть обратная связь модифицированного регистра использует две точки съёма  $D = \{m, 0\}$  и  $r = 3$ . Граф  $\Gamma(\varphi)$  изображён на рис. 2, список циклов дан в таблице.

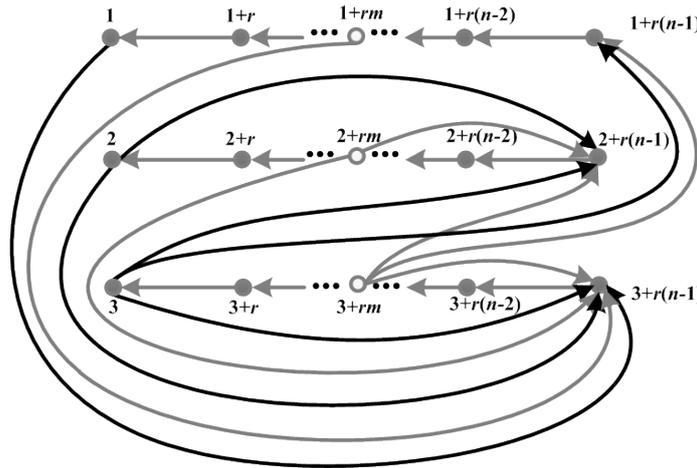


Рис. 2. Граф  $\Gamma(\varphi)$  при  $r = 3$

**Циклы графа  $\Gamma(\varphi)$  при  $r = 3$**

Цикл	Длина	Количество
$u + r(n - 1), \dots, u + r, u, r - u + 1 + r(n - 1), \dots, r - u + 1$	$2n$	$1 (u = 1)$
$u + r(n - 1), \dots, u + rm, r - u + 1 + r(n - 1), \dots, r - u + 1$	$2n - m$	$1 (u = 1)$
$u + r(n - 1), \dots, u + rm, r - u + 1 + r(n - 1), \dots, r - u + 1 + rm$	$2n - 2m$	$1 (u = 1)$
$u + r(n - 1), \dots, u + r, u, r + r(n - 1), \dots, r$	$2n - 2m$	$1 (u = 2)$
$u + r(n - 1), \dots, u + rm, r + r(n - 1), \dots, r$	$2n - m$	$1 (u = 2)$
$u + r(n - 1), \dots, u + rm, r + r(n - 1), \dots, r + rm$	$2n - 2m$	$1 (u = 2)$
$u + r(n - 1), \dots, u + r, u$	$n$	$2 (u = 2, 3)$
$u + r(n - 1), \dots, u + rm$	$n - m$	$2 (u = 2, 3)$

Данный граф  $\Gamma(\varphi)$  примитивный при  $(n, m) = 1$ . При  $r = 3$  в зависимости от  $m$  получаем оценки в соответствии со следствием теоремы:

- 1) при  $d_1 - d_0 = 1$  ( $m = 1$ ) имеет место  $\exp \Gamma(\varphi) \leq n^2 + 2n + 2$ ;

2) при  $(n, m) = 1$ ,  $2 \leq m \leq n - 2$  верна оценка  $\exp \Gamma(\varphi) \leq n^2 + (3 - m)n + 2m$  (взяты длины циклов  $n - m$  и  $n$ );

3) при  $m = n - 1$  выполняется  $\exp \Gamma(\varphi) \leq 2n - 2$ .

**Вывод:** выбор параметров модифицированного аддитивного генератора позволяет достичь полного перемешивания за число тактов работы, которое существенно меньше размера (в битах) состояний генератора.

#### ЛИТЕРАТУРА

1. Шнайер Б. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си. М.: Триумф, 2002.
2. Когос К. Г., Фомичев В. М. Положительные свойства неотрицательных матриц // Прикладная дискретная математика. 2012. № 4 (18). С. 5–13.
3. Коренева А. М., Фомичев В. М. Об одном обобщении блочных шифров Фейстеля // Прикладная дискретная математика. 2012. № 3 (17). С. 34–40.
4. Дорохова А. М., Фомичев В. М. Уточнённые оценки экспонентов перемешивающих графов биективных регистров сдвига над множеством двоичных векторов // Прикладная дискретная математика. 2014. № 1 (23). С. 77–83.
5. Фомичев В. М. Методы дискретной математики в криптологии. М.: Диалог-МИФИ, 2010.
6. Фомичев В. М. Оценки экспонентов примитивных графов // Прикладная дискретная математика. 2011. № 2 (12). С. 101–112.
7. Фомичев В. М. Свойства путей в графах и в мультиграфах // Прикладная дискретная математика. 2010. № 1 (7). С. 118–124.

УДК 512.62

### АЛГОРИТМ ПОСТРОЕНИЯ СИСТЕМЫ ПРЕДСТАВИТЕЛЕЙ ЦИКЛОВ МАКСИМАЛЬНОЙ ДЛИНЫ ПОЛИНОМИАЛЬНЫХ ПОДСТАНОВОК НАД КОЛЬЦОМ ГАЛУА

Д. М. Ермилов

В отличие от полей и колец вычетов, над кольцами Галуа не существует транзитивных полиномов, то есть биективных полиномов, которые реализуют полноцикловую подстановку. Максимальная длина цикла полиномиального преобразования над кольцом Галуа равна  $q(q - 1)p^{n-2}$ , где  $q^n$  — мощность кольца, а  $p^n$  — его характеристика. Предлагается алгоритм построения системы представителей всех циклов полиномиальных преобразований колец Галуа, имеющих максимальную длину. Сложность построенного алгоритма, выраженная в количестве операций умножения в кольце Галуа, равна  $O(lq^{n-1})$  при  $n$ , стремящемся к бесконечности, где  $l$  — степень многочлена полиномиального преобразования.

**Ключевые слова:** кольца Галуа, нелинейные рекуррентные последовательности.

Рассмотрим кольцо Галуа  $R = \text{GR}(q^n, p^n)$  мощности  $q^n$  и характеристики  $p^n$ , где  $q = p^m$ . Пусть  $f(x) \in R[x]$  — биективный полином над кольцом Галуа  $R$ . Граф преобразования, задаваемого полиномом  $f(x)$  над кольцом  $R$ , обозначим через  $G_{f,R}$ . Напомним, что цикловая структура графа — это таблица  $[l_1^{k_1}, \dots, l_t^{k_t}]$ , указывающая, что граф состоит из  $k_1$  циклов длины  $l_1, \dots, k_t$  циклов длины  $l_t$ . В работе [1] показано, что граф  $G_{f,R}$  не может содержать цикл, длина которого больше  $q(q - 1)p^{n-2}$ .

В данной работе рассматривается класс полиномов над кольцом Галуа  $R$ , граф которых содержит цикл максимальной длины  $q(q-1)p^{n-2}$ . Назовём такие полиномы полиномами с максимальной длиной цикла (МДЦ-полиномами).

Пусть  $f(x) \in R[x]$  — МДЦ-полином. В работе решается задача построения множества  $W_{f,R} \subset R$  — системы представителей всех циклов максимальной длины  $(q-1)qp^{n-2}$  графа  $G_{f,R}$ . Мощность множества  $W_{f,R}$  равна  $(q/p)^{n-2}$ , так как в графе  $G_{f,R}$  содержится  $(q/p)^{n-2}$  циклов длины  $(q-1)qp^{n-2}$  [2]. Введём необходимые обозначения.

Положим  $J = pR$  и  $R_k = R/J^k$ ,  $k \in \{1, \dots, n\}$ . Рассмотрим эпиморфизмы

$$\varphi_i : R \rightarrow R_i$$

для  $i \in \{1, \dots, n\}$ , которые естественным образом продолжаются до эпиморфизмов колец многочленов

$$\widehat{\varphi}_i : R[x] \rightarrow R_i[x].$$

Положим  $f_i(x) = \widehat{\varphi}_i(f(x))$ . Строить набор  $W_{f,R}$  будем итеративно, последовательно находя элементы в цепочке множеств

$$W_{f_1,R_1}, W_{f_2,R_2}, \dots, W_{f_n,R_n},$$

и тогда  $W_{f,R} = W_{f_n,R_n}$

Множество  $W_{f_1,R_1}$  состоит из одного элемента, так как граф  $G_{f_1,R_1}$  состоит из единственного цикла длины  $q$ . Поэтому в качестве множества  $W_{f_1,R_1}$  подойдёт любое одноэлементное множество  $\{a\}$ ,  $a \in R_1$ .

Множество  $W_{f_2,R_2}$  также состоит из одного элемента, поскольку граф  $G_{f_2,R_2}$  состоит из двух циклов длины  $q(q-1)$  и  $q$ . Следовательно, в качестве элемента множества  $W_{f_2,R_2}$  подойдёт любой элемент на цикле длины  $q(q-1)$  графа  $G_{f_2,R_2}$ .

Теперь покажем, как по известному множеству  $W_{f_k,R_k}$  построить множество  $W_{f_{k+1},R_{k+1}}$ ,  $k \geq 2$ . Рассмотрим эпиморфизмы

$$\varphi_i : R_{i+1} \rightarrow R_i$$

для  $i \in \{1, \dots, n-1\}$ . Для каждого  $a \in W_{f_k,R_k}$  обозначим через  $C_a$  цикл графа  $G_{f_k,R_k}$ , на котором лежит элемент  $a$ .

Так как прообраз  $\varphi_i^{-1}(C_a)$  состоит из  $q/p$  циклов максимальной длины  $q(q-1)p^{k-1}$  графа  $G_{f_{k+1},R_{k+1}}$ , то для построения множества  $W_{f_{k+1},R_{k+1}}$  достаточно для каждого элемента  $a \in W_{f_k,R_k}$  найти множество элементов

$$\left\{ a_1, a_2, \dots, a_{\frac{q}{p}} \right\},$$

лежащих на этих циклах, причём разные элементы должны лежать на разных циклах.

Пусть элемент  $a \in W_{f_k,R_k}$ . Установим связь между элементами кольца  $R_{k+1}$ , которые лежат на одном цикле максимальной длины и образ которых под действием эпиморфизма  $\varphi_k$  совпадает с  $a$ .

**Утверждение 1.** Пусть элемент  $a \in W_{f_k,R_k}$  является представителем цикла  $C$  максимальной длины графа  $G_{f_k,R_k}$ , тогда на любом цикле  $C'$  максимальной длины графа  $G_{f_{k+1},R_{k+1}}$ , таком, что  $\varphi_i(C') = C$ , лежат ровно  $p$  элементов, образ которых под действием эпиморфизма  $\varphi_i$  совпадает с  $a$ .

**Теорема 1.** Пусть  $a_1 = a + p^k a'_1, \dots, a_p = a + p^k a'_p$  — элементы на некотором цикле максимальной длины  $q(q-1)p^{k-1}$  графа  $G_{f_{k+1}, R_{k+1}}$ , образ которых под действием эпиморфизма  $\varphi_k$  совпадает с  $a \in W_{f_k, R_k}$ . Тогда выполняется соотношение

$$a'_{i+1} = a'_i + r, \quad i = 1, 2, \dots, p,$$

где  $r$  — некоторый элемент поля  $R_1$ .

**Следствие 1.** Пусть  $a \in W_{f_k, R_k}$ . Два элемента  $a + p^k a'$  и  $a + p^k a''$  кольца  $R_{k+1}$  лежат на одном и том же цикле максимальной длины графа  $G_{f_{k+1}, R_{k+1}}$  в том и только в том случае, если элементы  $a', a'' \in R_1$  лежат на одном цикле графа  $G_{x+r, R_1}$  полиномиального преобразования  $x + r$ , где элемент  $r \in R_1$  находится из сравнения

$$F(a) \equiv a + p^k r \pmod{J^{k+1}}.$$

Граф  $G_{x+r, R_1}$  состоит из  $q/p$  циклов длины  $p$ . Элементы каждого цикла образуют смежный класс аддитивной группы поля  $R_1 = \text{GF}(q)$  по подгруппе  $\langle r \rangle$ . Это означает, что для нахождения  $q/p$  элементов поля  $\text{GF}(q)$ , которые лежат на разных циклах графа  $G_{x+r, \text{GF}(q)}$ , достаточно найти представителей смежных классов поля  $\text{GF}(q)$  по подгруппе  $\langle r \rangle$ .

Аддитивная группа поля  $(\text{GF}(q), +)$  изоморфна группе  $(\mathbb{Z}_p^m, +)$ . Если на группе  $(\mathbb{Z}_p^m, +)$  ввести внешнюю операцию умножения на элементы поля  $\mathbb{Z}_p$ , то получим векторное пространство размерности  $m$ . Дополним до базиса пространства элемент  $r$ , получим базис  $r, r_2, \dots, r_m$  и рассмотрим представление пространства в виде прямой суммы подпространств

$$\mathbb{Z}_p^m = \langle r \rangle \dot{+} \langle r_2 \rangle \dot{+} \dots \dot{+} \langle r_m \rangle.$$

Представителями смежных классов группы  $(\text{GF}(q), +)$  по подгруппе  $(\langle r \rangle, +)$  являются все элементы множества

$$\{\langle r_2 \rangle \dot{+} \dots \dot{+} \langle r_m \rangle\}.$$

Изложим алгоритм построения системы представителей  $W_{f, R}$  циклов максимальной длины графа  $G_{f, R}$ .

В качестве  $W_{f_1, R_1}$  можно взять любое одноэлементное множество  $\{a\}$ ,  $a \in R_1$ , а в качестве  $W_{f_2, R_2}$  — одноэлементное множества  $\{a'\}$ , где  $a'$  — элемент на цикле длины  $q(q-1)$  графа  $G_{f_2, R_2}$ .

Далее покажем, как по имеющемуся элементу  $a \in W_{f_k, R_k}$  построить множество из  $q/p$  элементов  $A_a \subset W_{f_{k+1}, R_{k+1}}$ ,  $k \geq 2$ . При этом, по построению, для различных  $a_1, a_2 \in W_{f_k, R_k}$  множества  $A_{a_1}$  и  $A_{a_2}$  не пересекаются. Поскольку

$$\frac{q}{p} |W_{f_k, R_k}| = |W_{f_{k+1}, R_{k+1}}|,$$

то  $\bigcup_{a \in W_{f_k, R_k}} A_a = W_{f_{k+1}, R_{k+1}}$ .

**Алгоритм 1.** Построение множества  $A_a$

**Вход:**  $f(x) \in R[x]$ ,  $a \in W_{f_k, R_k}$

**Выход:** множество  $A_a \subset W_{f_{k+1}, R_{k+1}}$

- 1: Находим элемент  $r \in R_1$ , такой, что  $f^{[q(q-1)p^{k-2}]}(a) \equiv a + p^k r \pmod{J^{k+1}}$ .
- 2: Дополняем до базиса пространства  $\mathbb{Z}_p^m$  элемент  $r$ , получим базис  $r, r_2, \dots, r_m$ .
- 3:  $A_a := \{c_1 r_2 + \dots + c_m r_m : c_i \in \{0, \dots, p-1\}, i = 1, \dots, m\}$ .

За элементарную операцию возьмём операцию умножения в кольце Галуа  $R$ . Сложность построения множества  $W_{f_n, R_n}$  составляет  $O(lq^{n-1})$  элементарных операций при  $n$ , стремящемся к бесконечности, где  $l$  — степень многочлена  $f(x)$  на входе алгоритма.

#### ЛИТЕРАТУРА

1. Ермилов Д. М., Козлитин О. А. Цикловая структура полиномиального генератора над кольцом Галуа // Математические вопросы криптографии. 2013. Т. 4. Вып. 1. С. 27–57.
2. Ермилов Д. М. О цикловой структуре полиномиальных преобразований колец Галуа максимального периода // Обзорение прикл. и промышл. матем. 2013. Т. 20. Вып. 3.

УДК 519.711.2

### МОДЕЛЬ ФУНКЦИИ УСЛОЖНЕНИЯ В ГЕНЕРАТОРЕ ПСЕВДОСЛУЧАЙНЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ НАД ПОЛЕМ $GF(2)$

В. М. Захаров, Р. В. Зелинский, С. В. Шалагин

Предложена модель усложнения псевдослучайных последовательностей (ПСП) над полем  $GF(2)$ , основанная на представлении функции усложнения системой линейных биективных преобразований (БП) от двух двоичных переменных. Расширены алгоритмические возможности функции усложнения за счёт сведения аффинного преобразования над полем  $GF(2)$  к линейному преобразованию, представляемому невырожденными двоичными матрицами размера 3. Представлен ряд свойств, характеризующих рассматриваемые БП. Отмечены возможности этих свойств по изменению структуры и ансамбля формируемых ПСП.

**Ключевые слова:** генератор, псевдослучайная последовательность, биективное преобразование.

Рассмотрим преобразование

$$f(X) : GF(2)^n \rightarrow GF(2)^n, \quad (1)$$

где  $n$  чётное;  $GF(2)^n$  — множество  $n$ -мерных двоичных векторов.

Пусть отображение (1) является биекцией и вектор  $X$  формируется некоторым генератором псевдослучайных последовательностей со свойствами случайной равновероятной последовательности. Преобразование (1) рассматривается как функция усложнения. Предлагается модель функции усложнения, обладающая алгоритмическими возможностями изменения структуры ПСП и увеличения ансамбля формируемых ПСП.

Рассмотрим линейное преобразование вектора  $X$  в виде

$$Z_L = A_i \cdot X, \quad (2)$$

где  $A_i$  — двоичная невырожденная матрица размера  $n$  и равенство понимается по модулю 2. Число линейных невырожденных преобразований, выполняемых по формуле (2), при  $n = 2$  равно 6. Учтём, что отображению (1) при  $n = 2$  соответствует максимальное число различных биекций равное 24 [1]. Разобьём вектор  $X = x_1 x_2 \dots x_n$  на непересекающиеся пары переменных  $(x_{2i-1}, x_{2i})$ ,  $i = 1, \dots, n/2$ .

Введём в рассмотрение транспонированный кортеж вида

$$(q_1, q_2, \dots, q_m)^T, \quad (3)$$

где  $m = n/2$ ;  $q_i$  — некоторое линейное биективное преобразование над вектором  $(x_{2i-1}, x_{2i})$  в вектор  $(z_{2i-1}, z_{2i})$ ,  $i = 1, \dots, n/2$ . Пусть в (3)  $m = 24$  и число различных элементов  $q_i$  равно максимальному числу биекций от двух двоичных переменных, т.е. 24. Определение всех элементов множества  $G = \{q_i : i = 1, \dots, 24\}$  для системы (3) рассматривается как задача построения требуемой функции усложнения. Обозначим  $A = \{A_i : i = 1, \dots, 24\}$  некоторое множество невырожденных матриц  $A_i$  размера 3, позволяющих выполнить по формуле (2) 24 различных биекции. Введём векторы  $(x_{2i-1}, x_{2i}, 1)$  и  $(z_{2i-1}, z_{2i}, 1)$  как расширения соответственно векторов  $(x_{2i-1}, x_{2i})$  и  $(z_{2i-1}, z_{2i})$ ,  $i = 1, \dots, 24$ .

**Теорема 1.** В системе (3) линейное биективное преобразование  $q_i \in G$  над вектором  $(x_{2i-1}, x_{2i})$  представимо однозначно соответствующей невырожденной матрицей  $A_i \in A$ , осуществляющей преобразование вектора  $(x_{2i-1}, x_{2i}, 1)$  в вектор  $(z_{2i-1}, z_{2i}, 1)$ ,  $i = 1, \dots, 24$ .

Доказательство теоремы основано на результатах работы [2], показывающих возможность сведения аффинного преобразования к линейному.

**Следствие 1.** При  $n = 48$  для отображения (1) существует  $24!$  биективных преобразований вектора  $X$  в вектор  $Z_L$  вида (3).

Для случая  $n = 48$  на модели (3) при фиксированной  $M$ -последовательности на входе путём перестановки элементов  $q_i$  можно получить ансамбль  $V$  периодических последовательностей векторов  $Z_L$  мощности  $Q_1 = 24!$ .

Множество матриц  $A$  можно разбить на три подмножества  $M1, M2, M3$  с мощностями  $|M1| = 10, |M2| = 8, |M3| = 6$ ;  $M1 = \{E\} \cup \{A_i : O(A_i) = 2\}$ ;  $M2 = \{A_i : O(A_i) = 3\}$ ;  $M3 = \{A_i : O(A_i) = 4\}$ , где  $E$  — единичная матрица;  $O(A_i)$  — порядок матрицы  $A_i$  в группе  $GL(3)$ .

Возможность сочетания в функции усложнения (3) невырожденных матриц  $A_i$  из множеств  $M1, M2, M3$  позволяет менять строение выходной последовательности: создавать разнообразный порядок следования векторов  $Z_L$ , отличающийся от порядка следования входных векторов  $X$ ; при этом последовательности векторов  $Z_L$  из ансамбля  $V$  сохраняют величину периода и статистические свойства входной  $M$ -последовательности. В частном случае на основе определённых матриц  $A_i \in A$  можно получить тождественное преобразование вектора  $X$ .

На входе системы (3) можно использовать  $M$ -последовательности из ансамбля мощности  $Q_2 = (\varphi(2^{48} - 1))/48$ , где  $\varphi$  — функция Эйлера, при этом для  $n = 48$  выполняется  $Q_1 > Q_2$ . Тогда на выходе системы (3) можно формировать ансамбль последовательностей векторов  $Z_L$  мощности  $Q_1 \cdot Q_2$ .

## ЛИТЕРАТУРА

1. Молдовян А. А., Молдовян Н. А., Гуц Н. Д., Изотов Б. В. Криптография: скоростные шифры. СПб.: БХВ-Петербург, 2002. 496 с.
2. Колтаков А. В. Методы и алгоритмы линейных и аффинных преобразований для модели бинарных диаграмм решений: дис. ... канд. техн. наук. Казань, 2004.

УДК 519.113.6

## ПОСТРОЕНИЕ ТРАНЗИТИВНЫХ ПОЛИНОМОВ НАД КОЛЬЦОМ $\mathbb{Z}_{p^2}$

А. О. Ковалевская

Разработан метод, позволяющий строить все транзитивные полиномы по модулю  $p^2$ . Метод работает в предположении, что заранее известны все полиномы, транзитивные по модулю  $p$ .

**Ключевые слова:** полиномиальная функция над кольцом, рекуррентные последовательности, транзитивные полиномы.

В работе рассматриваются рекуррентные последовательности вида

$$a \bmod p^n, \quad f(a) \bmod p^n, \quad f(f(a)) \bmod p^n, \quad \dots, \quad (1)$$

где  $f(x) \in \mathbb{Z}[x]$ ,  $a \in \mathbb{Z}$ ,  $n \in \mathbb{N}$ . Такие последовательности находят применение в различных областях математики. В частности, в криптографии они используются в качестве псевдослучайных последовательностей. Поэтому возникает проблема построения таких полиномов  $f(x)$ , для которых указанная последовательность имеет большой период.

**Определение 1.** Полином  $f(x) \in \mathbb{Z}[x]$  будем называть транзитивным по модулю  $p^n$ , если последовательность (1) имеет период  $p^n$ , то есть максимальный.

**Определение 2.** Полином  $f(x)$  будем называть тождеством по модулю  $p^n$ , если  $f(a) \bmod p^n = 0$  для любого  $a \in \mathbb{Z}$ .

Транзитивные полиномиальные преобразования колец вычетов рассматриваются в [1]. В соответствии с этой работой, если  $p \notin \{2, 3\}$ , то полином, транзитивный по модулю  $p^2$ , транзитивен по модулю  $p^n$  для любого натурального  $n$ . Кроме того, транзитивные полиномы по модулю  $p^n$  могут быть получены из транзитивных по модулю  $p^2$  путём добавления тождества. Таким образом, важным является случай  $n = 2$ . Рассмотрим задачу получения всех транзитивных полиномов по модулю  $p^2$ .

Известны различные формы представления полиномиальных функций. Любая полиномиальная функция над  $\mathbb{Z}_{p^2}$ , в соответствии с [2], может быть представлена многочленом

$$f(x) = f_0(x) + pf_1(x) + (x^p - x)f_2(x), \quad (2)$$

где  $f_0(x)$ ,  $f_1(x)$ ,  $f_2(x)$  — полиномы над кольцом  $\mathbb{Z}_p$  степени меньше  $p$ . Из формы (2) нетрудно получить другую, которая будет использована далее:

$$f(x) = f_0(x) + pf_1(x) + (x^p - x)(f'_0(x) - f'(x)), \quad (3)$$

где  $f'(x)$  и  $f'_0(x)$  — производные для  $f(x)$  и  $f_0(x)$  с коэффициентами, приведёнными по модулю  $p$ . Обозначим  $f^p(x) = \underbrace{f(f \dots (x) \dots)}_{p \text{ раз}}$ .

Метод построения транзитивного по модулю  $p^2$  полинома  $f(x)$  состоит из следующих шагов:

- 1) Выбирается полином  $f_0(x) \in \mathbb{Z}_p[x]$ , транзитивный по модулю  $p$ .
- 2) Выбирается такой  $f'(x) \in \mathbb{Z}_p[x]$ , для которого выполняется  $\prod_{x \in \mathbb{Z}_p} f'(x) \bmod p = 1$ .
- 3) Выбирается  $f_1(x) \in \mathbb{Z}_p[x]$  — произвольный полином степени меньше  $p$ .

- 4) Многочлен  $f(x)$  строится по формуле (3).
- 5) Выполняется проверка  $f(x)$  на транзитивность: если  $f^p(a) \neq a$  для некоторого  $a \in \mathbb{Z}$ , то искомым полином получен, иначе вернуться на шаг 3 и выбрать в качестве  $f_1(x)$  другой полином.

Корректность проверки на транзитивность в шаге 5 алгоритма следует из необходимого и достаточного условия транзитивности, сформулированного в [1], а также из выбора  $f'(x)$  на шаге 2. Условие, выполнение которого требуется в шаге 2, следует из утверждений, сформулированных в [3]. Количество полиномов, удовлетворяющих данному условию, равно  $(p-1)^{p-1}$ .

Для того чтобы с помощью этого метода получить все транзитивные по модулю  $p^2$  полиномы, на шаге 3 потребуется перебрать все возможные полиномы с коэффициентами из  $\mathbb{Z}_p$ , степень которых меньше  $p$ . Их количество равно  $p^p$ . С учётом того, что количество полиномов, транзитивных по модулю  $p$ , равно  $(p-1)!$ , получаем, что метод требует перебора  $(p-2)!(p-1)^p p^p$  полиномов  $f(x)$ , из которых в соответствии с [1] транзитивными являются  $(p-2)!(p-1)^{p+1} p^{p-1}$ . Таким образом, доля нетранзитивных составляет  $1/p$ . При больших значениях  $p$  эта доля очень мала, что обеспечивает хорошую работу метода. При реализации алгоритма в системе компьютерной алгебры Sage все 15360000 транзитивных по модулю 25 полиномов были построены за 32 мин. Эксперименты проводились на компьютере с процессором Intel Core i7-3770 и оперативной памятью 15,4 Гб.

Если рассматривать задачу нахождения не всех, а какого-либо одного или нескольких транзитивных полиномов, то возможно улучшение этого метода. Оно заключается в следующем. Пусть выбранный случайным образом полином  $f_1(x)$  не привёл к транзитивному  $f(x)$ . Тогда выберем такой полином  $g(x)$ , для которого  $g(x) = 0$  при всех значениях  $x$ , кроме одного. Затем подставим в формулу (3) вместо  $f_1(x)$  сумму  $f_1(x) + g(x)$ . Такое построение гарантирует получение транзитивного по модулю  $p^2$  полинома  $f(x)$ . Пусть в результате этих действий получили многочлен  $F(x) = f(x) + pg(x)$ . Тогда  $F^p(x)$  имеет следующий вид:

$$F^p(x) = f^p(x) + p [g(x) g(f(x)) \dots g(f^{p-1}(x))] \begin{bmatrix} f'(f(x))f'(f^2(x)) \dots f'(f^{p-1}(x)) \\ f'(f^2(x)) \dots f'(f^{p-1}(x)) \\ \vdots \\ f'(f^{p-1}(x)) \\ 1 \end{bmatrix}. \quad (4)$$

В силу того, что  $f(x)$  транзитивен по модулю  $p$ , но не транзитивен по модулю  $p^2$ , имеем  $f^p(x) \bmod p^2 = x$ . Кроме того,  $g(x), g(f(x)), \dots, g(f^{p-1}(x))$  — значения полинома  $g(x)$  во всех различных точках. Среди них есть только одно ненулевое. Тогда в формуле (4) второе слагаемое не равно нулю по модулю  $p^2$ , откуда следует, что  $F(x)$  транзитивен по модулю  $p^2$ .

#### ЛИТЕРАТУРА

1. Ларин М. В. Транзитивные полиномиальные преобразования колец вычетов // Дискретная математика. 2002. №14(2). С. 20–32.
2. Frisch S. and Krenn D. Sylow  $p$ -groups of polynomial permutations on the integers mod  $p^n$  // J. Number Th. 2013. No. 133. P. 4188–4199.
3. Ермилов Д. М., Козлитин О. А. Цикловая структура полиномиального генератора над кольцом Галуа // Математические вопросы криптографии. 2013. №4(1). С. 27–57.

УДК 511.172, 510.52

## РАСПОЗНАВАНИЕ РЕКУРРЕНТНЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ, ПОРОЖДАЕМЫХ КОНСЕРВАТИВНЫМИ ФУНКЦИЯМИ

О. Е. Сергеева

Пусть  $K$  — класс функций вида  $f : R^n \rightarrow R$ , где  $n = 1, 2, 3, \dots$ , и  $S(K, N)$  — множество начальных отрезков длины  $N$  рекуррентных последовательностей, построенных при помощи функций из  $K$ . Рассматривается задача распознавания свойства « $x \in S(K, N)$ » для произвольной последовательности  $x \in R^N$ . В случае, когда  $K$  — класс консервативных функций над кольцом  $R = \mathbb{Z}_p^n$ , предлагается алгоритм решения этой задачи, битовая сложность которого  $O(N \log^2 N)$ .

**Ключевые слова:** *схема, функциональные элементы, рекуррентные последовательности, консервативные функции.*

Задача распознавания последовательностей состоит в том, чтобы по заданной последовательности сказать, возможно ли её построить рекуррентно при помощи функции из определённого класса. Так, для распознавания свойства линейности над полем используется алгоритм Берлекэмп — Мессе [1, 2], обобщённый в работах В. Л. Куракина [3] для колец и модулей.

В работах В. С. Анашина [4] предложено для построения рекуррентных последовательностей использовать полиномиальные, дифференцируемые и консервативные функции над кольцом. Такие функции имеют эффективную программную и аппаратную реализацию. В связи с этим в работе рассматриваются функции, сохраняющие систему эквивалентностей, частным случаем которых являются консервативные.

Пусть  $\Omega$  — конечное множество булевых функций, которое назовём базисом. *Схема из функциональных элементов* [5] — это ориентированный граф без циклов, где каждый вход помечен некоторой переменной, остальные вершины помечены базисными функциями. Если вершина помечена функцией от  $n$  аргументов, то её полустепень захода равна  $n$ . *Сложностью* схемы назовем число вершин в ней.

Пусть  $R$  — конечное  $k$ -элементное множество;  $R^*$  — множество всех бесконечных последовательностей с элементами из  $R$ ;  $P_R$  — класс всех функций вида  $f : R^n \rightarrow R$  при  $n = 1, 2, 3, \dots$

**Определение 1.** Последовательность  $x_1 x_2 x_3 \dots \in R^*$  называется *рекуррентной над классом  $K \subseteq P_R$* , если для некоторого  $n$  существует функция  $f$  от  $n$  аргументов в классе  $K$ , такая, что  $f(x_i, \dots, x_{n+i-1}) = x_{n+i}$  при всех  $i = 1, 2, 3, \dots$

Для любого целого положительного  $N$  обозначим через  $S(K, N)$  множество начальных отрезков длины  $N$  рекуррентных последовательностей над классом функций  $K$ . Далее рассматривается задача распознавания свойства « $x \in S(K, N)$ » для  $x \in R^N$ . Нас интересует сложность алгоритма, решающего данную задачу, как функция растущего  $N$ . Назовём  $S(K, N)$ -*схемой* схему из функциональных элементов, которая распознает названное выше свойство. При этом предполагается, что буквы алфавита  $R$  кодируются двоичными наборами фиксированной длины  $s$  и последовательности подаются на вход схемы в закодированном виде — наборами длины  $Ns$ .

Перейдём к описанию класса  $K$ .

**Определение 2.** Пусть  $\varepsilon \subset R^l$  — отношение на множестве  $R$ ,  $A \subseteq R^n$ . Частичная функция  $f : A \rightarrow R$  *сохраняет отношение  $\varepsilon$* , если для любых наборов  $(x_{11}, \dots, x_{1l}), \dots, (x_{n1}, \dots, x_{nl})$ , удовлетворяющих отношению  $\varepsilon$  и таких, что функция  $f$  определена

на наборах  $(x_{11}, \dots, x_{n1}), \dots, (x_{1l}, \dots, x_{nl})$ , набор  $(f(x_{11}, \dots, x_{n1}), \dots, f(x_{1l}, \dots, x_{nl}))$  также удовлетворяет  $\varepsilon$ .

Пусть  $\varepsilon = \{\varepsilon_1, \dots, \varepsilon_m\}$  — система эквивалентностей на множестве  $R$ , такая, что  $\varepsilon_1 \supseteq \varepsilon_2 \supseteq \dots \supseteq \varepsilon_m$ , и  $P_R^{(n)}(\varepsilon)$  — класс функций от  $n$  аргументов, сохраняющих все эквивалентности из  $\varepsilon$ . Если  $R = \mathbb{Z}_{p^m}$  и  $\varepsilon$  — система сравнимостей по модулям  $p, p^2, \dots, p^{m-1}$ , то  $P_R^{(n)}(\varepsilon)$  — это класс консервативных функций. Будем решать поставленную задачу для класса  $K = P_R^{(n)}(\varepsilon)$ . Важной является следующая

**Лемма 1.** Пусть  $A \subseteq R^n$ . Частичная функция  $f : A \rightarrow R$ , сохраняющая все эквивалентности из  $\varepsilon$ , может быть продолжена до полностью определенной функции в классе  $P_R^{(n)}(\varepsilon)$ .

Лемма 1 позволяет построить последовательность  $S(K, N)$ -схем сложности  $O(N^2)$ .

**Теорема 1.** Для любого  $n$  существует последовательность  $S(K, N)$ -схем сложности  $O(N \log^2 N)$ .

#### ЛИТЕРАТУРА

1. *Berlekamp E. R.* Algebraic Coding Theory. New York: Mc Craw-Hill, 1968. (Пер.: Берлекэмп Э. Алгебраическая теория кодирования. М.: Мир, 1971.)
2. *Massey J. L.* Shift-register synthesis and BCH decoding // IEEE Trans. Inform. Theory. 1969. V. 15. No 1. Part 1. P. 122–127.
3. *Куракин В. Л.* Алгоритм Берлекэмпа — Мэсси над конечными коммутативными кольцами // Проблемы передачи информ. 1999. № 35. С. 38–50.
4. *Анашин В. С.* Равномерно распределенные последовательности целых  $p$ -адических чисел // Математические заметки. 1994. Т. 55. № 2. С. 3–46.
5. *Wegener I.* The Complexity of Boolean Functions. John Wiley & Sons Ltd, 1987.

## Секция 4

## МАТЕМАТИЧЕСКИЕ МЕТОДЫ СТЕГАНОГРАФИИ

УДК 519.6

МЕТОД ЗАЩИТЫ ОТ НЕЛЕГАЛЬНОГО КОПИРОВАНИЯ  
В ЦИФРОВЫХ ВИДЕОТРАНСЛЯЦИЯХ ЧЕРЕЗ ВНЕДРЕНИЕ  
ВОДЯНЫХ ЗНАКОВ ПРИ РАСШИФРОВАНИИ

В. А. Анжин

Предложен метод защиты передаваемого в рамках цифровой видеотрансляции материала от копирования, в котором цифровые водяные знаки, идентифицирующие клиента, внедряются в видеоматериал на этапе его расшифровки клиентом. В основе метода лежит использование поточного шифра, позволяющего для заданного ключа зашифрования и набора позиций компонент защищаемого материала строить такой ключ расшифрования, при расшифровании на котором значения на предварительно указанных позициях инвертируются относительно их значений в исходном открытом тексте, а на всех остальных компонентах остаются совпадающими с соответствующими значениями в исходном открытом тексте.

**Ключевые слова:** защита от копирования, видеотрансляция, цифровые водяные знаки.

В наши дни абсолютное большинство информации хранится, передаётся и обрабатывается в цифровой форме. Это даёт возможность унифицировать часть этапов работы с данными, но вместе с тем порождает вопросы защиты авторских прав. Наиболее остро проблемы защиты от неограниченного нелегального копирования встали перед производителями произведений искусства, распространяемых в цифровой форме. В их числе, среди прочих, находятся и поставщики цифрового видео.

Поставщик видеоматериала может устанавливать получателям правила доступа к распространяемым данным. Они могут быть разными, но первичным является запрет на самостоятельное перераспространение полученного материала легальными клиентами. Кроме того, необходимо ограничение возможности доступа сторонних лиц к каналам связи между сервером распространения и клиентами. Для этого применяют шифрование распространяемых данных.

Основным подходом к решению проблемы нелегального копирования является юридическое ограничение такой возможности и добавление в каждую распространяемую копию скрытого идентификатора, позволяющего однозначно определить источник утечки. Такой скрытый идентификатор называют цифровым водяным знаком. Внедрение водяных знаков может осуществляться на различных этапах видеокодирования [1], в том числе и в закодированное видео.

При распространении цифрового видео возможно использование различных подходов к внедрению водяных знаков:

- использование доверенного декодера [2], работающего на стороне клиента. Водяной знак внедряется после декодирования цифрового видео до его передачи пользователю;

- предварительная подготовка множества копий с внедрёнными водяными знаками;
- внедрение водяного знака на этапе передачи.

Другим подходом, исследуемым в данной работе, является использование крипто-системы, позволяющей для данного ключа зашифрования и набора некоторых компонент цифрового видео, индивидуальных для каждого клиента, строить такой ключ расшифрования, при расшифровании на котором значения этих компонент инвертируются относительно их значений в исходном открытом тексте, а значения всех остальных его компонент сохраняются совпадающими с их значениями в исходном открытом тексте. Номера инвертируемых компонент выбираются такими, что изменение значений этих компонент не приводит к заметному искажению видеоматериала.

Для каждого из клиентов подготавливается уникальный ключ расшифрования, известный только производителю видеоматериала. Передаваемая мультимедиа информация единожды шифруется и доставляется конкретному потребителю вместе с программой расшифрования по «зашитому» в ней ключу расшифрования, сгенерированному для этого клиента. Клиент осуществляет расшифрование полученного шифртекста, в процессе которого в материал автоматически вносятся изменения, идентифицирующие получателя.

Требуемое шифрование и расшифрование можно выполнить, например, на базе поточного шифра с фильтрующим генератором ключевого потока.

Ключом в нём является тройка  $(F_1(x), F_2(x), iv)$ , где  $F_1(x)$  — фильтрующая функция;  $F_2(x)$  — используемый в регистре с линейной обратной связью (LFSR) полином;  $iv$  — начальное заполнение (состояние) регистра.

Процедура построения ключа расшифрования  $(F'_1(x), F'_2(x), iv')$  для данного ключа зашифрования  $(F_1(x), F_2(x), iv)$  и позиции  $k$ , при расшифровании на котором получится изменённый в  $k$ -й позиции открытый текст, может выглядеть следующим образом:

- 1) Отсчитываем  $k$  первых тактов работы LFSR, изначально заполненного  $iv$ , с полиномом обратной связи  $F_2(x)$ .
- 2) Фиксируем в LFSR текущее состояние  $a = a_1 a_2 \dots a_n$  и образуем моном  $x^a = x^{a_1} x^{a_2} \dots x^{a_n}$ . Здесь  $n$  — длина регистра.
- 3)  $F'_2(x) = F_2(x)$ ,  $iv' = iv$ ,  $F'_1(x) = F_1(x) + x^a$ .

Для обоснования работоспособности метода осуществлена его практическая реализация для формата видеокодирования MPEG-2 Video. Для внедрения водяных знаков в закодированное в этом формате видео использован метод «Low Complexity Watermarks for MPEG Compressed Video» из [3].

#### ЛИТЕРАТУРА

1. *Mistry D.* Comparison of digital water marking methods // Int. J. Comp. Sci. Engin. 2010. V. 2. No. 9. P. 2905–2909.
2. *Wang P.* Tamper Resistance for Software Protection. A Thesis for the Degree of Master of Science. Information and Communications University, Daejeon, Korea, 2005.
3. *Langelaar G. C.* Real-time Watermarking Techniques for Compressed Video Data. Delft: Delft University of Technology, 2000. 155 p.

УДК 681.3

## ПРИНЦИПЫ АССОЦИАТИВНОЙ СТЕГАНОГРАФИИ

И. С. Вершинин

Рассматривается стеганографический метод защиты данных с использованием аппарата маскирования, применяемого при двумерно-ассоциативной обработке стилизованных бинарных изображений.

**Ключевые слова:** *ассоциативная стеганография, двумерно-ассоциативное маскирование, защита картографической информации.*

Защита данных с использованием аппарата маскирования, применяемого при двумерно-ассоциативной обработке стилизованных бинарных изображений, относится к области стеганографии. Двумерно-ассоциативное маскирование следует рассматривать как частный случай т. н. трафаретного способа классической стеганографии.

Применительно к картографии, развиваемый подход стегозащиты обладает свойством безусловной стойкости (совершенной секретности по К. Шеннону). Выполнение критерия Шеннона означает, что в каждом сокрытом сообщении при полном переборе ключей может быть распознано любое из возможных сообщений. Поэтому метод, безусловно, стоек независимо от вычислительной сложности полного перебора ключей.

Рассматриваемый метод относится к классу вероятностных способов защиты. Случайность вносится использованием специальных механизмов пространственной кластеризации объектов, маскирования их бинарных представлений и рандомизации. Имена и координаты объектов кодируются в цифровом виде. Разряды кодов, представленные в алфавите почтовых индексов, рассматриваются как бинарные изображения. Над ними выполняется специальная процедура маскирования. Случайно сгенерированный набор масок служит секретным ключом.

Предметом защиты в данном случае является набор тематических карт-кластеров как случайно формируемых по карте таблиц в терминах «коды объектов — коды координат». Защищённые карты образуют «верхние слои» геоинформационных систем.

Суть рассматриваемого подхода заключается в следующем. Исходное бинарное изображение подвергается избирательному воздействию стохастических помех (рандомизации). При этом не затрагиваемые помехами части объектов выбираются случайным образом с выполнением некоторого условия. Но их точное знание (что является ключом) позволяет правильно идентифицировать объекты в целом методом двумерно-ассоциативного поиска.

В рассматриваемом случае кодовые знаки (цифровые символы) представляются в виде двоичных матриц определённых размеров. Каждый символ развёртывается в цепочку соответствующей длины. Метод предусматривает внедрение псевдослучайного процесса в передаваемое сообщение, оставляя истинным ограниченное подмножество бит в каждом знаке со случайным распределением этого подмножества по битовой сетке эталона.

В данном случае ключом является набор масок всевозможных цифр. Размер ключа определяется числом цифр, размерами матриц и не зависит от объёма сообщения. Наличие гаммы никак не сказывается на факте санкционированного распознавания, но создаёт непреодолимую преграду для противника.

Рассматриваются базовый алгоритм маскирования и его свойства [1], достижимая стойкость защиты объектов картографии развиваемым методом при действии разного рода атак, связь размеров ключа со стойкостью и вычислительной сложностью

метода [2], влияние помех на эффективность распознавания скрытых сообщений [3]. Предлагаются различные методы ослабления этого влияния.

#### ЛИТЕРАТУРА

1. Райхлин В. А., Вершинин И. С. Моделирование процессов двумерно-ассоциативного маскирования распределенных точечных объектов картографии // Нелинейный мир. 2010. № 5. С. 288–296.
2. Вершинин И. С. Стойкость ассоциативной защиты распределенных объектов картографии // Нелинейный мир. 2011. № 12. С. 822–825.
3. Вершинин И. С., Гибадуллин Р. Ф. Изменение результатов распознавания на множестве замаскированных бинарных матриц при действии аддитивных помех // Вестник КГТУ им. А. Н. Туполева. 2012. № 4-1. С. 198–206.

УДК 003.26

## НОВЫЙ ВЫСОКОТОЧНЫЙ СТЕГОАНАЛИЗ РАСТРОВЫХ ИЗОБРАЖЕНИЙ<sup>1</sup>

В. А. Монарев

Предложен новый подход для обнаружения информации в растровых изображениях. Предполагается, что для внедрения информации использовалась либо  $\pm 1$ -стеганография, либо LSB-замещение. Предлагается новый сценарий обнаружения информации, в котором наблюдателю известны пиксели изображения, куда производилось внедрение. Показано, что обнаружение информации возможно уже при 0,001 bpr (“bits per pixel”) внедрении.

**Ключевые слова:** *стегоанализ, стеганография, LSB-внедрение.*

Стегоанализ файлов изображений в форматах, не искажающих качество (bmp, pgm, tiff и др.), разделяется на два подхода: количественный (когда метод позволяет определить приблизительное количество внедрённой информации) и обычный (метод определяет факт наличия или отсутствия скрытой информации). К самым известным количественным методам относятся RS [1], simple pairs [2], WS [3], improved WS [4]. Все эти методы позволяют обнаружить скрытую информацию, если она была внедрена с помощью LSB-замещения. Недавно предложен новый количественный стегоанализ, который обнаруживает скрытую информацию в цветных изображениях эффективнее, чем ранее существовавшие методы [6]. Для обнаружения же  $\pm 1$ -стеганографии используется, как правило, обычный стегоанализ, который фактически производит классификацию изображений, разделяя их на два класса: пустые и непустые [5]. В случае LSB-внедрения возможно эффективно обнаружить до 0,1 bpr, и до 0,01 bpr — в случае LSB-замещения. Для классификации используются стандартные методы SVM и LDA.

В данной работе предполагается, что внедрение скрытой информации производится с помощью либо LSB-внедрения, либо  $\pm 1$ -стеганографии. Предполагается также, что известны пиксели, куда производилось внедрение, но неизвестны содержание и размер внедряемой информации, т. е. имеется устройство, с помощью которого производилось сокрытие информации (ключ для выбора случайных пикселей находится в устройстве). По заданному файлу необходимо определить, могла ли быть в него встроена информация с помощью данного устройства. Метод относится к количествен-

<sup>1</sup>Работа поддержана грантом РФФИ № 14-01-31484-мол\_а.

ным методам. Из полученных экспериментальных результатов следует, что метод позволяет определять наличие информации, если внедрено более 0,001 bpp.

Пусть  $X = \{x_1, \dots, x_n\}$ , где  $x_i \in \{0, 1, \dots, 255\}$ , — пиксели исходного изображения. Обозначим через  $\bar{S}(Y)$  вектор спам-характеристик, вычисленный для множества  $Y \subset X$  (подробно см. [5]). Обозначим через  $Y_p$  случайное множество ( $Y_p \subset X$ ), такое, что  $|Y_p|/|X| = p$ . Полагаем также, что обозначение  $Y_p$  предполагает не только выбор случайного подмножества заданного размера, но и внедрение скрытой информации с помощью  $\pm 1$ -стеганографии (или LSB-замещения). Обозначим через  $D(\dots)$  евклидову метрику;  $Z_p$  — множество ( $Z_p \subset X$ ) тех пикселей, куда производилось бы внедрение при внедрении  $p$  бит на пиксель.

---

### Алгоритм 1. Оценка количества внедрённой информации

---

- 1: Вычисляем  $\bar{S}(X)$ ,  $\bar{S}(Z_{0,001})$ ,  $\bar{S}(Z_{0,0015})$ , ...,  $\bar{S}(Z_{0,5})$ .
- 2: Вычисляем по 10 векторов  $\bar{S}(Y_p^i)$ ,  $i = 0, \dots, 9$ , для каждого значения  $p = 0,001, 0,0015, \dots, 0,5$ .
- 3: Находим

$$\arg \min_p = \left\{ \frac{D(\bar{S}(X), \bar{S}(Z_p))}{D\left(\bar{S}(X), \sum_{i=0}^9 \bar{S}(Y_p^i)/10\right)} \right\}$$

- 4: Полагаем, что  $np$  равно количеству внедрённых бит информации.
- 

Поясним принцип работы алгоритма. Хорошо известно, что спам-характеристики очень чувствительны к  $\pm 1$ -стеганографии, и если предположить, что мы знаем, куда информация была внедрена, то легко понять, что спам-характеристики этих пикселей отличаются от спам-характеристик случайно выбранных пикселей ( $Y_p$ ), если параметр  $p$  отличается от искомого параметра (количества внедрённой информации).

Для проверки эффективности метода были взяты 1000 черно-белых изображений с сайта [7]. Рассмотрены три варианта внедрения: 0,001 bpp, 0,005 bpp и 0,01 bpp ( $\pm 1$ -стеганография и LSB-замещение). Для каждого из случаев подсчитана минимальная средняя ошибка. Ошибки равны 12, 6 и 4% соответственно для LSB-замещения и 7, 4 и 3% для  $\pm 1$ -стеганографии. Таким образом, можно сделать вывод, что метод эффективно обнаруживает скрытую информацию для внедрения 0,001 bpp независимо от метода внедрения.

### ЛИТЕРАТУРА

1. *Fridrich J., Du R., and Long M.* Steganalysis of LSB encoding in color images // Proc. ICME 2000, New York City, New York, 2000. V. 3. P. 1279–1282.
2. *Dumitrescu S., Wu X., and Wang Z.* Detection of LSB steganography via sample pair analysis // LNCS. 2002. V. 2578. P. 355–372.
3. *Fridrich J. and Goljan M.* On estimation of secret message length in LSB steganography in spatial domain // Proc. SPIE, Electronic Imaging, Security, Steganography, and Watermarking of Multimedia Contents VI. San Jose, California, 2004. V. 5306. P. 23–34.
4. *Ker A. and Böhme R.* Revisiting weighted stego-image steganalysis // Proc. SPIE, Electronic Imaging, Security, Forensics, Steganography, and Watermarking of Multimedia Contents X. San Jose, 2008. V. 6819. Doi: 10.1117/12.766820.
5. *Pevny T., Bas P., and Fridrich J.* Steganalysis by subtractive pixel adjacency matrix // IEEE Trans. Info. Forensics and Security. 2010. V. 5(2). P. 215–224.

6. Монарев В. А. Сдвиговой метод стегоанализа // Вестник СибГУТИ. 2012. № 4. С. 62–68.
7. <http://bows2.ec-lille.fr/> — The 2nd BOWS Contest (Break Our Watermarking System). 2007.

УДК 621.391.037.372

## ОПРЕДЕЛЕНИЕ РАЗМЕРА СТЕГАНОГРАФИЧЕСКОГО СООБЩЕНИЯ В ЦИФРОВЫХ ИЗОБРАЖЕНИЯХ С ИСПОЛЬЗОВАНИЕМ БИНАРНОГО СТЕГОАНАЛИТИЧЕСКОГО КЛАССИФИКАТОРА

Е. В. Разинков, А. Н. Альмеев

Работа посвящена количественному стегоанализу — определению размера сообщения, встроенного в стеганографический контейнер. Предложен подход к определению размера скрытого сообщения с помощью бинарного стегоаналитического классификатора, приведена формула вычисления математического ожидания ошибки стегоаналитика. Задача определения оптимальной стратегии стегоаналитика сформулирована в виде задачи минимизации.

**Ключевые слова:** *количественный стегоанализ, бинарная классификация.*

Помимо задачи обнаружения скрытой информации, одна из актуальных задач, стоящих перед стегоаналитиком, — оценка размера скрытого стеганографического сообщения. Атаки, направленные на определение размера скрытого сообщения, называются количественными. Наилучшие на сегодняшний день методы обнаружения скрытой информации основаны на использовании бинарных универсальных классификаторов [1]. Современные количественные стегоаналитические атаки основываются на модификации этих методов [2].

Интерес представляет непосредственное применение бинарных стегоаналитических классификаторов для оценки размера скрытого сообщения. Разработка метода такого применения бинарного классификатора без модификации и исследование его свойств значительно упростили бы использование новых результатов, получаемых в области бинарной стегоаналитической классификации, в количественном стегоанализе.

Через  $C$  обозначим множество цифровых объектов, будем считать, что стегоаналитик располагает бинарным классификатором

$$Detect : C \rightarrow \{0, 1\},$$

для каждого цифрового объекта  $c \in C$  возвращающего 0, если объект классифицирован как неизменённый контейнер, или 1, если объект классифицирован как стего.

Задача состоит в построении на основе имеющегося бинарного классификатора количественной стегоаналитической атаки

$$Estimate : C \rightarrow [0; 1],$$

возвращающей относительный размер скрытого сообщения, встроенного в цифровой объект  $c \in C$ , — отношение количества изменённых коэффициентов к общему количеству коэффициентов, доступных для изменения.

Бинарный стегоаналитический классификатор может быть использован для определения размера сообщения в случае, когда стегоаналитик располагает некоторым множеством цифровых объектов, в которые были встроены скрытые сообщения одного размера. Возникновение такой ситуации на практике кажется маловероятным, но

стегоаналитик может создать подобные условия при наличии лишь одного цифрового изображения высокого разрешения.

Пусть в цифровое изображение размера  $n$  встроено сообщение относительного размера  $\theta \in [0; 1]$ . Стегоаналитик разрезает перехваченное цифровое изображение на  $k$  частей и подаёт каждую из них на вход бинарному классификатору как отдельное изображение. Естественно предположить, что внесённые скрывающим преобразованием искажения равномерно распределены в пространственной области изображения и относительный размер сообщения, встроеного в каждую из  $k$  частей, также равен  $\theta$ , размер же каждой части —  $n/k$ . Каждую из частей стегоаналитик подаёт на вход бинарному стегоаналитическому классификатору.

Наименьшие возможные вероятности ошибки первого рода  $\alpha$  и ошибки второго рода  $\beta$  бинарного стегоаналитического классификатора удовлетворяют следующему неравенству [3]:

$$\alpha \log_2 \frac{\alpha}{1-\beta} + (1-\alpha) \log_2 \frac{1-\alpha}{\beta} \leq D_{KL}(P_0||P_1), \quad (1)$$

где  $P_0$  — распределение контейнеров;  $P_1$  — распределение стего;  $D_{KL}(P_0||P_1)$  — относительная энтропия между этими распределениями. Будем считать, что стегоаналитик располагает наилучшим возможным бинарным классификатором, для которого неравенство (1) обращается в равенство.

В соответствии с [4], для небольших значений  $\theta$ , которые характерны для использования стеганографии на практике, получаем

$$\alpha \log_2 \frac{\alpha}{1-\beta} + (1-\alpha) \log_2 \frac{1-\alpha}{\beta} = D_{KL}(P_0||P_1) \approx \frac{n}{2k} \theta^2 I(0),$$

где  $I(0)$  — информация Фишера — коэффициент пропорциональности, характеризующий источник стеганографических объектов [5]. Из этого уравнения можем найти  $p = 1 - \beta$  — вероятность того, что часть изображения будет классифицирована как стего.

Пусть  $m$  частей изображения были классифицированы как стегообъекты, тогда стегоаналитик оценивает  $p$  значением  $m/k$ , а относительный размер сообщения  $\theta$  — значением

$$\theta' = \sqrt{\frac{2k}{nI(0)} \left( \alpha \log_2 \frac{\alpha k}{m} + (1-\alpha) \log_2 \frac{(1-\alpha)k}{k-m} \right)}.$$

Таким образом, можно вычислить математическое ожидание ошибки стегоаналитика для заданного размера изображения  $n$ , относительного размера секретного сообщения  $\theta$ , коэффициента  $I(0)$ , вероятности ошибки первого рода  $\alpha$  и стратегии стегоаналитика, заключающейся в выборе  $k$  — количества частей, на которые разрезается цифровое изображение, по следующей формуле:

$$M[\Delta\theta] = \sum_{m=0}^k \binom{k}{m} p^m (1-p)^{k-m} \left| \theta - \sqrt{\frac{2k}{nI(0)} \left( \alpha \log_2 \frac{\alpha k}{m} + (1-\alpha) \log_2 \frac{(1-\alpha)k}{k-m} \right)} \right|.$$

Задача нахождения оптимальной стратегии стегоаналитика сводится к выбору значения  $k$ , минимизирующего математическое ожидание ошибки:

$$M[\Delta\theta] \rightarrow \min.$$

Предложенный подход к использованию бинарных стегоаналитических классификаторов в количественном стегоанализе позволяет исследовать влияние свойств изображений, особенностей классификатора, размера изображения, размера скрытого сообщения и стратегии стегоаналитика на стойкость стеганографической системы к количественным атакам, вычислять оптимальную стратегию стегоаналитика в зависимости от этих факторов.

#### ЛИТЕРАТУРА

1. *Kodovsky J. and Fridrich J.* Steganalysis of JPEG images using rich models // Proc. SPIE, Electronic Imaging, Media Watermarking, Security, and Forensics XIV. San Francisco, CA, January 22–26, 2012. V. 8303. P. 0A 1–13.
2. *Kodovsky J., Fridrich J.* Quantitative steganalysis using rich models // Proc. SPIE, Electronic Imaging, Media Watermarking, Security, and Forensics XV. San Francisco, CA, February 3–7, 2013. V. 8665. DOI: 10.1117/12.2001563.
3. *Cachin C.* An information-theoretic model for steganography // LNCS. 1998. V. 1525. P. 306–318.
4. *Ker A. et al.* Moving steganography and steganalysis from the laboratory into the real world // 1st Information Hiding and Multimedia Security Workshop. Montpellier, France, June 17–19, 2013. P. 45–58.
5. *Filler T. and Fridrich J.* Fisher information determines capacity of  $\varepsilon$ -secure steganography // LNCS. 2009. V. 5806. P. 31–47.

## Секция 5

МАТЕМАТИЧЕСКИЕ ОСНОВЫ КОМПЬЮТЕРНОЙ  
БЕЗОПАСНОСТИ

УДК 004.65, 004.056.55

## ЗАЩИЩЁННАЯ СУБД С СОХРАНЕНИЕМ ПОРЯДКА

И. Н. Глогов, С. В. Овсянников, В. Н. Тренькаев

Работа посвящена разработке защищённой клиент-серверной СУБД при недоверенном сервере БД. Конфиденциальные данные шифруются на стороне клиента с помощью специализированных шифров, позволяющих производить операции над данными без их предварительного расшифрования. Для этого используется шифр mOPE с сохранением порядка, который позволяет производить операции сравнения над зашифрованными данными. Разработан и реализован асинхронный NoSQL-протокол взаимодействия клиента и сервера БД, поддерживающий простой набор операций над конфиденциальными данными. Разработанный протокол интегрирован в свободно распространяемую СУБД MySQL.

**Ключевые слова:** *защищённая СУБД, недоверенный сервер БД, шифр с сохранением порядка, NoSQL-протокол.*

Рассматривается задача построения защищённой клиент-серверной СУБД в случае, когда сервер БД неподконтролен пользователю БД. Такая ситуация имеет место, например, при использовании облачных услуг, когда хранение и обработка данных производится на серверах, предоставляемых в пользование третьей стороной. Предполагается, что возможна пассивная атака, когда корректно выполняются все запрашиваемые операции, но при этом ведётся наблюдение за данными, обращаемыми на сервере БД.

Проблему недоверенного сервера предлагается решать с помощью шифрования конфиденциальных данных на доверенном клиенте с последующей их передачей в неконтролируемую БД. Для этого следует использовать специализированные шифры, позволяющие выполнять безопасные вычисления — шифры, сохраняющие вычислительные операции над данными [1] и (или) порядок данных в базе [2]. В этом случае не требуется расшифрования при манипуляции с данными.

В настоящей работе используется шифр mOPE с сохранением порядка [2], так как он является единственным, для которого доказана безопасность в смысле отсутствия утечки информации об открытых текстах по шифртекстам, кроме их порядка, — стойкость к атаке IND-ОСРА [3]. Шифр mOPE ненамного увеличивает длину шифртекста по сравнению с длиной открытого текста (в отличие от других шифров с сохранением порядка, для которых длина шифртекста экспоненциально зависит от длины открытого текста). Особенности шифра mOPE являются интерактивность (алгоритм шифрования распределён между клиентом и сервером) и изменяемость шифртекстов (в процессе шифрования текущего открытого текста могут измениться шифртексты других данных).

В качестве основы при разработке защищённой СУБД с сохранением порядка взята свободно распространяемая СУБД MySQL. Экспериментальный образец защищён-

ной СУБД имеет следующую архитектуру. На стороне клиента приложению посредством специальной библиотеки предоставляется NoSQL-интерфейс доступа к данным. На стороне сервера MySQL реализован модуль расширения (*plugin*), который преобразует NoSQL-запросы приложения в низкоуровневые операции подсистемы хранения данных (*storage engine*). В дополнение к стандартному MySQL-протоколу взаимодействия клиента и сервера БД реализован дополнительный NoSQL-протокол с поддержкой выборки по диапазону над зашифрованными данными. Отличительными характеристиками NoSQL-протокола являются: 1) асинхронность (работа клиента на время обработки запроса сервером не приостанавливается); 2) поддержка интерактивного алгоритма шифрования (на сервере хранится промежуточное состояние взаимодействия); 3) обход SQL-уровня MySQL-сервера, что позволяет избежать временных затрат на синтаксический анализ и оптимизацию запросов. Наиболее близким аналогом разработанной СУБД можно назвать исследовательский проект CryptDB [4], в котором подсистема, реализующая шифрование данных, является настройкой (прокси-сервером) над СУБД MySQL.

#### ЛИТЕРАТУРА

1. Жиров А. О., Жирова А. О., Кренделев С. Ф. Безопасные облачные вычисления с помощью гомоморфной криптографии // БИТ. 2013. Т. 1. С. 6–12.
2. Popa R. A., Li F. H., and Zeldovich N. An ideal-security protocol for order-preserving encoding // IEEE Symp. Security and Privacy. San Francisco, CA, USA, May 23–24, 2013. P. 463–477.
3. Boldyreva A., Chenette N., Lee Y., and O’Neill A. Order-preserving symmetric encryption // EUROCRYPT’09. LNCS. 2009. V. 5479. P. 224–241.
4. Popa R. A., Redfield C. M. S., Zeldovich N., and Balakrishnan H. CryptDB: protecting confidentiality with encrypted query processing // Proc. Twenty-Third ACM Symp. Operating Systems Principles (SOSP’11). New York, NY, USA, 2011. P. 85–100.

УДК 004.94

### УСЛОВИЯ БЕЗОПАСНОСТИ ИНФОРМАЦИОННЫХ ПОТОКОВ ПО ПАМЯТИ В РАМКАХ МРОСЛ ДП-МОДЕЛИ

П. Н. Девянин

В рамках мандатной сущностно-ролевой ДП-модели, ориентированной на реализацию в отечественной защищённой операционной системе специального назначения *Astra Linux Special Edition*, анализируются условия безопасности информационных потоков по памяти в смысле Белла — ЛаПадулы и мандатного контроля целостности.

**Ключевые слова:** компьютерная безопасность, формальная модель, информационный поток, *Linux*.

Фундаментальным требованием безопасности операционных систем, реализующих мандатное управление доступом, является предотвращение возможности реализации информационных потоков по памяти «сверху вниз» (безопасность в смысле Белла — ЛаПадулы [1]). Кроме того, современную защищённую операционную систему трудно представить без мандатного контроля целостности, основой которой является предотвращение возможности модификации (через создание соответствующих информационных потоков по памяти) сущностей с высоким уровнем целостности субъект-сессии

ями с низким уровнем целостности. Таким образом, важным этапом при разработке мандатной сущностно-ролевой ДП-модели (МРОСЛ ДП-модели) [1–3], реализуемой в настоящее время в отечественной защищенной операционной системе специального назначения (ОССН) *Astra Linus Special Edition* [4], стало формулирование и обоснование достаточных условий безопасности в смысле Белла — ЛаПадулы и мандатного контроля целостности.

Дополнительно к использованным в перечисленных работах дадим следующие определения и обозначения.

**Определение 1.** Доверенную субъект-сессию  $y$  назовем функционально корректной относительно доверенной субъект-сессии  $y'$  и сущности или субъект-сессии  $e$ , когда  $y$  не реализует информационный поток по памяти от  $e$  к некоторой сущности  $e'$ , функционально ассоциированной с  $y'$ . Субъект-сессию  $y$  назовем абсолютно функционально корректной относительно субъект-сессии  $y'$  и сущности или субъект-сессии  $e$ , когда  $y$  не реализует информационный поток по памяти от  $e$  к некоторой сущности  $e'$ , функционально ассоциированной с  $y'$ . При этом используем следующие обозначения:

- $f\_correct : L_S \rightarrow 2^{L_S \times (E \cup S)}$  — функция, задающая для каждой доверенной субъект-сессии множество пар вида (доверенная субъект-сессия, сущность или субъект-сессия), относительно которых она функционально корректна;
- $af\_correct : S \rightarrow 2^{S \times (E \cup S)}$  — функция, задающая для каждой субъект-сессии множество пар вида (субъект-сессия, сущность или субъект-сессия), относительно которых она абсолютно функционально корректна.

**Определение 2.** Доверенную субъект-сессию  $y$  назовем параметрически корректной относительно доверенной субъект-сессии  $y'$  и сущности или субъект-сессии  $e$ , когда  $y$  не реализует информационный поток по памяти от или к  $e$  от или к некоторой сущности  $e'$ , параметрически ассоциированной с  $y'$ . Субъект-сессию  $y$  назовем абсолютно параметрически корректной относительно субъект-сессии  $y'$  и сущности или субъект-сессии  $e$ , когда  $y$  не реализует информационный поток по памяти от или к  $e$  от или к некоторой сущности  $e'$ , параметрически ассоциированной с  $y'$ . При этом используем следующие обозначения:

- $p\_correct : L_S \rightarrow 2^{L_S \times (E \cup S)}$  — функция, задающая для каждой доверенной субъект-сессии множество пар вида (доверенная субъект-сессия, сущность или субъект-сессия), относительно которых она параметрически корректна;
- $ap\_correct : S \rightarrow 2^{S \times (E \cup S)}$  — функция, задающая для каждой субъект-сессии множество пар вида (субъект-сессия, сущность или субъект-сессия), относительно которых она абсолютно параметрически корректна.

**Определение 3.** Назовём траекторию  $G_0 \vdash_{op_1} G_1 \vdash_{op_2} \dots \vdash_{op_N} G_N$  системы  $\Sigma(G^*, OP, G_0)$ , где  $N \geq 0$ , на которой доверенные субъект-сессии не инициируют выполнение де-юре правил преобразования состояний, траекторией без кооперации доверенных и недоверенных субъект-сессий. Таким образом, по определению в системе  $\Sigma(G^*, OP, G_0)$  на траекториях без кооперации доверенных и недоверенных субъект-сессий для передачи прав доступа доверенные субъект-сессии могут инициировать выполнение только де-факто правил вида  $flow\_memory\_access(x, y, \alpha_a)$ ,  $flow\_time\_access(x, y)$ ,  $find(x, y, z)$ ,  $post(x, y, z)$  и  $pass(x, y, z)$ .

**Определение 4.** Состояние  $G$  системы  $\Sigma(G^*, OP, G_0)$  назовём безопасным, когда оно удовлетворяет следующим условиям:

- для каждой субъект-сессии  $x, y \in S$ , таких, что  $y \in de\_facto\_own(x)$ , выполняется  $f_s(y) = f_s(x)$  и  $i_s(y) \leq i_s(x)$ ;
- для каждой недоверенной субъект-сессии  $x \in N_S$ , субъект-сессии  $y \in S$  и сущности  $e \in E$ , таких, что либо  $(e \in [y]$  и  $(x, e, write_m) \in F)$ , либо  $(e \in ]y[$  и либо  $(e, x, write_m) \in F$ , либо  $(x, e, read_a) \in A)$ , верны условия  $f_s(y) \leq f_s(x)$  и  $i_s(y) \leq i_s(x)$ ;
- для каждой доверенной субъект-сессии  $y \in L_S$  и каждой сущности  $c\_i\_entity \in E\_HOLE$ , где  $c \in LC$ , верно условие  $(y, c\_i\_entity, write_a) \notin A$ ;
- для каждого информационного потока  $(x, y, \alpha_f) \in F$ , где  $\alpha_f \in \{write_m, write_t\}$ , справедливо  $f_x(x) \leq f_y(y)$ , где  $f_x$  и  $f_y$  — соответствующие функции  $f_e, f_r$  или  $f_s$ , и, если  $\alpha_f = write_m$ , то справедливо  $i_x(x) \geq i_y(y)$ , где  $i_x$  и  $i_y$  — соответствующие функции  $i_e$  или  $i_s$ .

**Определение 5.** Пусть  $G_0$  — безопасное начальное состояние системы  $\Sigma(G^*, OP, G_0)$  и существует траектория без кооперации доверенных и недоверенных субъект-сессий  $G_0 \vdash_{op_1} G_1 \vdash_{op_2} \dots \vdash_{op_N} G_N$ , где  $N \geq 1$ . Будем говорить, что в состоянии  $G_N$  произошло нарушение безопасности системы, когда в нём выполняется одно из следующих условий, при этом они не выполняются в состояниях  $G_i$  траектории, где  $0 \leq i < N$ :

- существуют недоверенная субъект-сессия  $x \in N_{S_N}$  и доверенная субъект-сессия  $y \in de\_facto\_own_N(x) \cap L_{S_N}$ , такие, что  $i_{s_N}(y) = i\_high$  (нарушение безопасности в смысле мандатного контроля целостности);
- существует информационный поток по памяти  $(x, y, write_m) \in F_N$ , такой, что  $x, y \in E_N$  и не верно неравенство  $f_{e_N}(x) \leq f_{e_N}(y)$  (нарушение безопасности в смысле Белла — ЛаПадулы);
- существует информационный поток по времени  $(x, y, write_t) \in F_N$ , такой, что  $x, y \in E_N$  и не верно неравенство  $f_{e_N}(x) \leq f_{e_N}(y)$  (нарушение безопасности в смысле контроля информационных потоков по времени).

В следующей базовой теореме безопасности (БТБ-ДП) сформулированы достаточные условия безопасности системы, заданной в рамках МРОСЛ ДП-модели, в смыслах Белла — ЛаПадулы и мандатного контроля целостности. При этом анализ условий безопасности информационных потоков по времени как существенно более сложный планируется осуществить при проведении дальнейших исследований.

**Теорема 1.** Пусть  $G_0$  — безопасное начальное состояние системы  $\Sigma(G^*, OP, G_0)$ . Пусть на всех траекториях системы без кооперации доверенных или недоверенных субъект-сессий  $G_0 \vdash_{op_1} G_1 \vdash_{op_2} \dots \vdash_{op_N} G_N$ , где  $N \geq 0$ , и в каждом состоянии  $G_N$  для каждой субъект-сессии  $s \in S_N$  и сущности  $e \in E_N$  выполняются следующие условия:

- если  $e \in [s]$ , то выполняются условия  $i_{s_N}(s) \leq i_{e_N}(e)$  и  $(f_{s_N}(s) = f_{e_N}(e)$  или  $i_{e_N}(e) = i\_high)$  (корректность уровней конфиденциальности и целостности сущностей, функционально ассоциированных с субъект-сессиями);
- если  $e \in ]s[$ , то выполняется равенство  $f_{s_N}(s) = f_{e_N}(e)$  и для каждой роли или административной роли  $r \in R_N \cup AR_N$ , такой, что  $(e, read_r) \in PA_N(r)$ , выполняются условия  $i_{s_N}(s) \leq i_{e_N}(e) \leq i_{r_N}(r)$  (корректность уровней конфиденциальности и целостности, а также прав доступа на чтение к сущностям, параметрически ассоциированным с субъект-сессиями);
- для всех доверенных субъект-сессий  $s \in L_{S_N}$  верны равенства  $f\_correct_N(s) = p\_correct_N(s) = L_{S_N} \times (E_N \cup S_N)$  (функциональная и параметрическая кор-

ректность всех доверенных субъект-сессий относительно всех доверенных субъект-сессий и сущностей);

- для всех субъект-сессий  $s \in S_N$  выполняются равенства  $\{s' \in S_N : f_{s_N}(s') = f_{s_N}(s)\} \times (E_N \cup S_N) \subset af\_correct_N(s) = ap\_correct_N(s)$  (абсолютная функциональная и параметрическая корректность субъект-сессии относительно всех сущностей и субъект-сессий с совпадающим уровнем конфиденциальности).

Тогда система  $\Sigma(G^*, OP, G_0)$  безопасна в смыслах Белла — ЛаПадулы и мандатного контроля целостности.

Условия теоремы БТБ-ДП требуют от ОССН функционально и параметрически корректной (абсолютно корректной) реализации всех субъект-сессий и корректного задания соответствующих уровней конфиденциальности и целостности функционально или параметрически ассоциированных с ними сущностей. Если, например, субъект-сессия, имеющая высокий уровень доступа, некорректно обрабатывает данные («заражается») в сущностях с низким уровнем конфиденциальности и это приводит к получению фактического владения над нею субъект-сессией с низким уровнем доступа, то система защиты ОССН не сможет этому воспрепятствовать. Таким образом, условия теоремы БТБ-ДП указывают на необходимость повышения качества разработки прикладного программного обеспечения ОССН.

#### ЛИТЕРАТУРА

1. Десянин П. Н. Модели безопасности компьютерных систем. Управление доступом и информационными потоками: учеб. пособие для вузов. 2-е изд., испр. и доп. М.: Горячая линия — Телеком, 2013. 338 с.
2. Десянин П. Н. Адаптация мандатной сущностно-ролевой ДП-модели к условиям функционирования ОС семейства Linux // Системы высокой доступности. 2013. № 3. С. 98–102.
3. Десянин П. Н. Администрирование системы в рамках мандатной сущностно-ролевой ДП-модели управления доступом и информационными потоками в ОС семейства Linux // Прикладная дискретная математика. 2013. № 4(22). С. 22–40.
4. Операционные системы Astra Linux. <http://www.astra-linux.ru/>.

УДК 004.94

### ОБЩИЙ МЕТОД АУТЕНТИФИКАЦИИ НТТР-СООБЩЕНИЙ В ВЕБ-ПРИЛОЖЕНИЯХ НА ОСНОВЕ ХЕШ-ФУНКЦИЙ

Д. Н. Колегов

Предлагается метод аутентификации НТТР-сообщений в веб-приложениях, построенный на основе криптографических протоколов с ключевыми хеш-функциями. Данный метод может быть использован для защиты от многих атак на веб-приложения, использующих уязвимости в реализации механизмов аутентификации или авторизации.

**Ключевые слова:** криптографические протоколы, аутентификация сообщений, веб-приложения.

Одним из свойств, характеризующих безопасность протоколов, является свойство аутентификации сообщений, заключающееся в обеспечении аутентификации источника данных и целостности передаваемого сообщения. Аутентификация источника данных означает, что протокол обеспечивает гарантии того, что полученное сообщение или

его части были созданы одним из участников протокола в некоторый момент времени, предшествующий получению сообщения, и что никакие данные не были модифицированы или подделаны. Считается, что аутентификация источника данных включает целостность данных [1].

В веб-приложениях аутентификация сообщений, которыми обмениваются клиент и сервер по протоколу HTTP, как правило, реализуется на уровне логики самого веб-приложения и позволяет обеспечить выполнение следующих свойств безопасности:

- аутентичность источника HTTP-запроса;
- целостность имен и значений параметров, переданных клиенту в HTTP-ответе в виде HTML;
- целостность потока операций.

Кроме того, аутентификация сообщений на основе криптографических методов защиты позволяет существенно повысить уровень защищённости веб-приложения, а также его стойкость к средствам автоматизированного анализа [2]. У известных механизмов аутентификации сообщений в веб-приложениях [3–7] можно выделить следующие недостатки:

- отсутствует общая формальная модель безопасности механизма аутентификации сообщений;
- разработанные методы, как правило, ориентированы на конкретное веб-приложение и часто не учитывают особенности криптографических протоколов (например, необходимость защиты от атак повтора или от утечек CSRF-токенов, необходимость использования уникальных токенов);
- отсутствуют механизмы контроля целостности и валидации данных, генерируемых на клиентской стороне (например, данных, вводимых в поля форм).

Аутентификация HTTP-сообщений рассматривается как элемент политики атрибутного управления доступом. На основе положений модели ABAC [8] строится общая модель аутентификации сообщений.

Используются следующие обозначения:  $A$  — алфавит;  $A^*$  — множество всех слов в  $A$ ;  $[a]$  — множество букв слова  $a$ ;  $x||y$  — конкатенация строк  $x$  и  $y$ ;  $h$  — ключевая хеш-функция, построенная по алгоритму HMAC.

Построим модель аутентификации HTTP-сообщений на основе модели ABAC. Основными элементами модели являются следующие:  $O$  — множество объектов;  $S$  — множество субъект-сессий;  $E = S \cup O$  — множество сущностей;  $OA$  — множество атрибутов объектов;  $SA$  — множество атрибутов субъект-сессий;  $EA = ES \cup EO$  — множество атрибутов сущностей;  $OP$  — множество операций (видов доступа);  $TA$  — множество всех типов атрибутов;  $SAV$  — множество значений атрибутов субъект-сессий;  $OAV$  — множество значений атрибутов объектов.

В рамках модели ABAC будем считать HTTP-запросы пользовательскими субъект-сессиями; параметры и заголовки HTTP-запроса, идентификатор субъект-сессии (пользователя) — атрибутами субъект-сессии; элементы (scheme, authority, path) схемы URI HTTP-ресурсов — объектами; разрешённые параметры запроса, разрешённые идентификаторы пользователей, запрашивающих доступ к ресурсу, — атрибутами объекта; методы протокола HTTP — видами доступов. Будем также считать, что субъект-сессия имеет обязательные атрибуты *key* и *time*, а каждый объект имеет обязательный атрибут *mac*.

Определим функции:

- $type : E \rightarrow TA$  — функция, задающая тип атрибута;

- $EEA : E \rightarrow 2^{OA} \cup 2^{SA}$  — функция, задающая множество атрибутов сущности;
- $EAT : E \times T \rightarrow 2^{OA} \cup 2^{SA}$  — функция, задающая для сущности множество атрибутов данного типа;
- $AV : E \times EA \rightarrow SAV \cup OAV$  — функция, определяющая значение атрибута сущности;
- $assign\_auth : O \times 2^{EA} \times OP \rightarrow SAV \cup OAV$  — функция, вычисляющая значение переменной  $de\_jure\_auth$  для соответствующей сущности-объекта и значение переменной  $de\_facto\_auth$  для сущности субъект-сессии.

Пусть заданы множества  $S, O, OA, SA, TA, OP, EC, SAV, OAV$  и функции  $EEA, EAT, type, AV$  и  $assign\_auth$ . Определим предикат  $can\_access(s, o, op)$ , истинный тогда и только тогда, когда выполнены следующие условия:

- 1) для объекта  $o$  определен атрибут  $mac$  со значением  $AV(o, mac) = h(AV(s, key), de\_jure\_auth, AV(s, time))$ , где  $de\_jure\_auth = assign\_auth(o, 2^{EEA(o)}, op)$ ;
- 2) выполнено равенство  $AV(o, mac) = h(AV(s, key), de\_facto\_auth, AV(s, time))$ , где  $de\_facto\_auth = assign\_auth(o, 2^{EEA(s)}, op)$ .

Назовём  $P = (can\_access(s, o, op), assign\_auth)$  политикой безопасности. Будем говорить, что HTTP-запрос  $s \in S$  на доступ  $op \in OP$  к ресурсу  $o \in O$  является аутентичным, если предикат  $can\_access(s, o, op)$  является истинным.

Определим политику безопасности  $P$  так, чтобы стало возможным обеспечить выполнение одного или нескольких свойств безопасности веб-приложений.

Параметр (атрибут)  $q \in OA$  объекта  $o \in O$  называется контролируемым по значению, если политика безопасности обеспечивает выполнение условия  $AV(o, q) = AV(s, q)$ .

Параметр  $q \in OA$  объекта  $o \in O$  называется валидируемым в алфавите  $A$ , если политика безопасности обеспечивает выполнение условия  $AV(s, q) \in A^*$ .

Параметры типа  $t \in TA$  называются контролируемыми по имени, если политика безопасности обеспечивает выполнение условия  $EAT(o, t) = EAT(s, t)$ .

Аутентификатором объекта  $o \in O$  будем называть значение  $de\_jure\_auth$ , вычисленное по атрибутам объекта  $o$  в соответствии с методом вычисления функции  $assign\_auth$ .

Аутентификатором субъект-сессии  $s \in S$  будем называть значение  $de\_facto\_auth$ , вычисленное по атрибутам субъект-сессии  $s$  в соответствии с методом вычисления функции  $assign\_auth$ .

В рамках предложенной модели опишем метод построения аутентификатора, обеспечивающего выполнение следующих требований политики безопасности: базовое управление доступом пользователя к ресурсам, контроль целостности имён параметров и их значений, валидация значений параметров в заданном алфавите. Идея метода заключается в построении аутентификатора — строки, содержащей конкатенацию всех контролируемых атрибутов субъект-сессии, объекта и метода доступа, — и последующем его использовании в криптографическом протоколе аутентификации сообщений.

**Метод.** Условия применения метода: определены сущность  $e \in E$  и функция  $assign\_auth$ , задающая политику построения аутентификатора сущности.

- 1) Построить список  $L$  атрибутов сущности  $e$ , соответствующих параметрам. Перейти к его началу.
- 2) Если параметры из списка  $L$  являются контролируемыми по имени, то положить  $auth = auth || i_1 || \dots || i_m$ , где  $\{i_1, \dots, i_m\}$  — упорядоченное множество имён

атрибутов и  $EAT(e, t) = \{i_1, \dots, i_m\}$  для типа  $t$ , соответствующего типу «параметр».

- 3) Для каждого контролируемого по значению параметра  $l \in L$  положить  $auth = auth || l || AV(e, l)$  и удалить его из  $L$ .
- 4) Для каждого валидируемого параметра  $l \in L$  положить  $auth = auth || l || ([AV(e, l)] \setminus A)$  и удалить его из  $L$ .
- 5) Положить  $auth = auth || id_s || id_r || op$ , где  $id_r$  — идентификатор объекта;  $id_s$  — атрибут-идентификатор пользователя;  $op$  — метод доступа.
- 6) Выполнить протокол аутентификации сообщений, используя значение  $auth$  в качестве одного из его параметров.

Данный метод аутентификации HTTP-сообщений может быть реализован на основе криптографических протоколов с ключевыми хеш-функциями.

Особенности функционирования веб-приложений предъявляют следующие требования к протоколу: протокол должен быть прозрачен для клиента (нежелательна его реализация на клиентской стороне); протокол должен быть двухшаговым; протокол может быть реализован в рамках взаимодействия веб-браузера и веб-сервера.

Параметры протокола:  $k$  — долговременный ключ сервера;  $k_r$  — одноразовый случайный ключ сервера;  $id_r$  — идентификатор защищаемого объекта;  $id_s$  — идентификатор пользователя;  $time$  — текущее значение времени;  $L_P$  — запись политики  $P$  на некотором языке  $L$ . Действия протокола следующие:

- 1) Пользователь инициализирует отправку HTTP-запроса в рамках субъект-сессии  $s \in S$  с атрибутом-идентификатором пользователя  $id_s$ .
- 2) Сервер по полученному запросу формирует ответ, содержащий объект  $o \in O$ ; в соответствии с политикой безопасности  $P$  для объекта  $o$  вычисляет значение  $de\_jure\_auth$ , значения атрибутов  $mac = h(k_r, de\_jure\_auth, time)$  и  $policy = E_k(L_P, time, k_r)$ ; отправляет значения  $policy$  и  $mac$  вместе с описанием объекта  $o$  в HTTP-ответе.
- 3) Пользователь в рамках субъект-сессии  $s$  отправляет запрос на доступ вида  $op \in OP$  к объекту  $o$  вместе с атрибутами  $policy$  и  $mac$ .
- 4) Сервер по атрибутам субъект-сессии  $s$  получает значения  $L_P$ ,  $time$  и  $k_r$ , вычисляет значение  $de\_facto\_auth$ , находит  $mac' = h(k_r, de\_facto\_auth, time)$ , проверяет совпадение  $mac$  и  $mac'$ , а также соответствие временной метки допустимому интервалу.

Особенность базового протокола заключается в том, что никакие данные, кроме главного ключа  $k$ , на сервере не хранятся. Это позволяет реализовать stateless-механизм и обойтись без поддержки устойчивых (persistence) соединений и без хранения политики безопасности в общедоступной сессии (sharing session) при реализации протокола для веб-фермы.

## ЛИТЕРАТУРА

1. Черемухин А. В. Криптографические протоколы. Основные свойства и уязвимости: учеб. пособие для студ. учреждений высш. проф. образования. М.: Издательский центр «Академия», 2009. 272 с.
2. Reducing web application attack surface. <http://blog.spiderlabs.com/2012/07/reducing-web-apps-attack-surface.html>
3. Signing and Authenticating REST Requests. <http://docs.aws.amazon.com/AmazonS3/latest/dev/RESTAuthentication.html>

4. Facebook developers reference. <https://developers.facebook.com/docs/reference/php/facebook-getSignedRequest>
5. Barth A., Jackson C., and Mitchell J. Robust defences for cross-site request forgery // Proc. 15th ACM Conf. on Computer and Communications Security. ACM Press, 2008. P. 75–87.
6. ModSecurity Advanced Topic of the Week: HMAC Token Protection. <http://blog.spiderlabs.com/2014/01/modsecurity-advanced-topic-of-the-week-hmac-token-protection.html>
7. Understanding ASP.NET View State. <http://msdn.microsoft.com/library/ms972976.aspx>
8. NIST 800-162. Guide to Attribute Based Access Control (ABAC) Definition and Considerations. <http://nvlpubs.nist.gov/nistpubs/specialpublications/NIST.sp.800-162.pdf>

УДК 004.94

## ОБ ИНФОРМАЦИОННЫХ ПОТОКАХ ПО ВРЕМЕНИ, ОСНОВАННЫХ НА ЗАГОЛОВКАХ КЭШИРОВАНИЯ ПРОТОКОЛА HTTP

Д. Н. Колегов, О. В. Брославский, Н. Е. Олексов

Рассматриваются информационные потоки по времени через заголовки кэширования протокола HTTP. Приводятся практические примеры реализации данных потоков и их основные характеристики, в частности достижимость на практике максимальной пропускной способности таких каналов при достаточно высоком уровне точности — 99,8 %.

**Ключевые слова:** компьютерная безопасность, скрытые каналы, HTTP.

Рассматривается задача анализа и реализации информационных потоков по времени, основанных на заголовках кэширования протокола HTTP. Обнаружение информационных потоков по времени и соответствующих им скрытых каналов в компьютерных системах является одной из задач компьютерной безопасности [1]. Распространённость протокола HTTP делает выявление методов реализации информационных потоков по времени перспективным направлением для исследований.

Известные на данный момент информационные потоки в протоколе HTTP, как правило, основываются на отправке HTTP-запросов со специальными GET- или POST-параметрами или на применении стеганографических методов для сокрытия факта передачи информации в HTTP-заголовках. Однако данные методы меняют стандартную структуру HTTP-запроса, а значит, требуют соответствующей модификации веб-сервера. Информационные потоки, рассматриваемые в данной работе, не накладывают дополнительных ограничений на конфигурацию веб-сервера и, следовательно, представляют больший интерес для изучения.

Заголовки кэширования в протоколе HTTP хранят информацию о времени последнего изменения веб-страницы, тем самым позволяя клиенту не загружать веб-страницу, если она не была изменена с момента последнего запроса. Таким образом, возможна передача информации на основании данных об изменениях запрашиваемой веб-страницы. Например, ситуация, при которой некоторая веб-страница была изменена с момента последнего обращения к ней, может быть интерпретирована как получение одного бита информации.

Рассмотрим общую схему информационного потока по времени данного типа (рис. 1). Пусть  $O_1$  — объект, доступный на чтение процессу  $S_1$  на  $host_1$ ;  $O_2$  — веб-ресурс, расположенный на  $host_1$ ;  $O_3$  — HTTP-ответ;  $O_4$  — объект, доступный на запись

процессу  $S_3$  на  $host_2$ ;  $S_3$  — веб-сервер;  $S_1$  и  $S_2$  — два процесса, которым в соответствии с политикой безопасности данной компьютерной системы запрещено общаться напрямую. В каждый момент времени процесс  $S_1$  считывает один бит информации из объекта  $O_1$  и, в зависимости от значения бита, осуществляет или не осуществляет доступ на запись к веб-странице  $O_2$ . Процесс  $S_3$  выполняет HTTP-запрос к  $O_2$  и после получения HTTP-ответа  $O_3$ , основываясь на изменениях сущности  $O_2$ , пишет в объект  $O_4$  соответствующий бит (например, 1, если веб-страница была изменена, и 0 в противном случае).

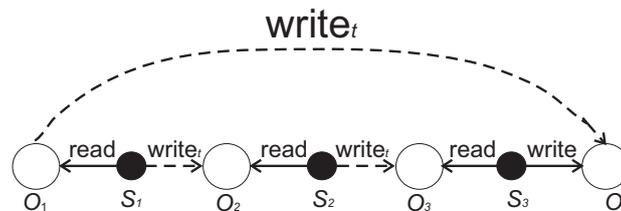


Рис. 1. Общая схема информационного потока

Информационные потоки по времени, основанные на заголовках кэширования протокола HTTP, могут быть разделены на две группы: потоки, основанные на заголовке Last-Modified, и потоки, основанные на заголовке ETag.

Заголовок Last-Modified содержит время последнего изменения сущности на веб-сервере, например, «Last-Modified: Tue, 10 Apr 2014, 12:34:56 GMT». Существует три возможных варианта реализации потока по времени на основе заголовка Last-Modified:

- 1) по значению заголовка Last-Modified:  $S_3$  обращается к  $O_2$  и получает HTTP-ответ  $O_3$ ; сравнивая полученное в  $O_3$  значение заголовка со значением, полученным в предыдущий раз,  $S_3$  делает вывод об отправленном бите — если значения не совпадают, то получена 1, иначе 0;
- 2) с помощью заголовка If-Modified-Since:  $S_3$  обращается к  $O_2$  с заголовком «If-Modified-Since:  $Date_1$ » и получает HTTP-ответ  $O_3$ . Если код ответа  $O_3$  равен 200, значит, веб-страница  $O_2$  была изменена и получена 1; если код ответа 304, то веб-страница не менялась и получен 0;
- 3) с помощью заголовка If-Unmodified-Since:  $S_3$  обращается к  $O_2$  с заголовком «If-Unmodified-Since:  $Date_1$ » и получает HTTP-ответ  $O_3$ . Если код ответа  $O_3$  равен 412, значит, веб-страница  $O_2$  была изменена и получена 1; если код ответа 200, то веб-страница не менялась и получен 0.

Для реализации рассматриваемых информационных потоков по времени необходимо, чтобы  $S_1$  имел права на запись в объект  $O_2$  и на чтение из объекта  $O_1$ ;  $S_3$  имел права на чтение  $O_2$ , то есть мог обратиться к сущности  $O_2$  на веб-сервере через HTTP. При стандартной конфигурации веб-сервера информационные потоки, основанные на заголовке Last-Modified, имеют одинаковую теоретическую максимальную скорость 1 бит/с. Данная скорость обусловлена техническими ограничениями заголовка Last-Modified: формат даты, используемый заголовком, хранит время с точностью до секунд.

В результате тестирования реализации одного из вышеописанных потоков установлено, что максимальная скорость потока достижима на практике, если пропускная способность канала между  $S_1$  и  $S_3$  позволяет  $S_3$  сделать запрос к  $O_2$  и получить ответ  $O_3$  за 1 с. Точность передачи для полученной реализации составила 99,82%.

Заголовок ETag (entity tag) используется для контроля изменений HTTP-сущностей. Среди наиболее распространенных веб-серверов только в Apache стандартизован алгоритм формирования заголовка ETag [3]. Значение ETag в соответствии с данным алгоритмом формируется из шестнадцатеричных значений идентификатора сущности (inode), размера сущности и времени последнего изменения сущности в формате mtime: «ETag: 120c7bL-32bL-4f86d4105ac62L». Соответственно могут быть рассмотрены три варианта информационных потоков, основанных на заголовке ETag:

- 1) по значению заголовка ETag:  $S_3$  обращается к  $O_2$ , получает HTTP-ответ  $O_3$  и делает вывод об отправленном бите, сравнивая полученное в  $O_3$  значение заголовка со значением, полученным в предыдущий раз;
- 2) с помощью заголовка If-Match:  $S_3$  обращается к  $O_2$  с заголовком «If-Match: ETag<sub>1</sub>» и получает HTTP-ответ  $O_3$ . Если код ответа  $O_3$  равен 412, значит, получена 1; если код ответа 200, то получен 0;
- 3) с помощью заголовка If-None-Match:  $S_3$  обращается к  $O_2$  с заголовком «If-None-Match: ETag<sub>1</sub>» и получает HTTP ответ  $O_3$ . Если код ответа  $O_3$  равен 200, значит, получена 1; если код ответа 304, то получен 0.

Реализация данных потоков требует прав доступа, аналогичных требованиям потока по заголовку Last-Modified. В стандартной конфигурации веб-сервер обновляет значения ETag не чаще чем раз в секунду, то есть, если клиент запрашивает веб-страницу более одного раза в секунду, все ответы будут содержать одно и то же значение заголовка ETag. Таким образом, при сохранении исходной конфигурации максимальная скорость потока не может превышать 1 бит/с, как и в случае с потоком по Last-Modified. Однако, в отличие от Last-Modified, ETag хранит время в формате mtime, точность которого составляет 1 мкс. Следовательно, теоретическая пропускная способность потока равна приблизительно 976 кбит/с, что намного превышает пропускную способность, достижимую на практике.

Чтобы максимально эффективно использовать пропускную способность данных потоков, необходимо, чтобы значение заголовка обновлялось при каждом изменении сущности. Для этого возможно изменить конфигурацию веб-сервера  $S_2$  или изменить тип сущности  $O_2$  со статической (html) страницы на динамическую (php). PHP позволяет вручную задавать значения и вид заголовков HTTP-ответа для отдельной страницы; соответственно возможно генерировать неотличимое от настоящего значение ETag (используя тот же алгоритм формирования), но делать это для каждого HTTP-запроса. Таким образом, максимальная скорость для данных потоков равна 1 бит в  $(2L + T)$  секунд, где  $L$  — время, затрачиваемое на передачу сообщения между  $S_2$  и  $S_3$ , и  $T$  — время, необходимое  $S_1$  и  $S_3$  для вычислительных операций: сравнения значений заголовков, чтения и записи битов и т. п. Реализации данных потоков при тестировании на скорости 2 бит/с показали 99,56 % точности передачи.

#### ЛИТЕРАТУРА

1. CWE-385: Covert Timing Channel. <https://cwe.mitre.org/data/definitions/385.html>
2. Brown E., Yuan B., Johnson D., and Lutz P. Covert channels in the HTTP Network Protocol: Channel characterization and detecting Man-in-the-Middle Attacks // Proc. 5th Intern. Conf. Information Warfare and Security. Ohio, USA, April 8–9, 2010. Air Force Institute of Technology, 2010. P. 56–65.
3. ETag header Apache specification. <http://httpd.apache.org/docs/2.2/mod/core.html#fileetag>

УДК 004.056.5

## О СКРЫТЫХ КАНАЛАХ ПО ВРЕМЕНИ В ОС ANDROID

Т. И. Милованов

Исследованы два различных скрытых канала. Первый из них найден в используемых в настоящее время версиях ОС Android. Измерены его основные характеристики, такие, как пропускная способность и процент ошибок. Канал основан на изменении количества свободного места в файловой системе и может быть использован двумя вредоносными приложениями для обмена данными. Написаны два тестовых приложения, реализующих информационный поток через найденный канал. Второй исследованный скрытый канал использует разницу во времени работы некоторой системной функции с фиксированными секретными и разными открытыми (контролируемыми любым пользователем) данными. В работе такой информационный поток реализуется от легального приложения к вредоносному без ведома легального в файловой системе `ext2` в ОС Android.

**Ключевые слова:** *скрытые каналы, вредоносные приложения, Android.*

В настоящее время наблюдается бурное распространение вредоносного программного обеспечения на платформе Android. Программы типа «троянский конь» составляют существенную часть современных вредоносных программ. Обычно такие программы запрашивают у пользователя критичные привилегии (например, возможность доступа в интернет), что позволяет реализовать утечку критичных данных пользователя. В то же время набор запрашиваемых приложением привилегий используется антивирусными средствами для обнаружения вредоносной активности.

Использование скрытых каналов позволяет вредоносным программам получать доступ к критичным данным, не имея полного набора привилегий. Одним из известных троянов, использующим скрытый канал по времени, является `Soundcomber` [1]. Данный троян для уменьшения набора привилегий не требует доступа в интернет, но устанавливает парное приложение с данной привилегией и для общения с ним использует скрытый канал, реализованный через изменение общедоступных настроек звука/вибрации. Недостаток такого канала в том, что процесс передачи данных легко сбивается пользовательскими действиями.

В результате проведённых исследований обнаружен скрытый канал по времени, основанный на изменении количества свободного места в файловой системе. Пусть имеются два вредоносных приложения  $A$  и  $B$ , и  $A$  имеет доступ к некоторым секретным данным, но не имеет доступа к сети, а  $B$  имеет доступ к сети, но не имеет доступа к секретным данным. При этом у приложений нет общих ресурсов для обмена данными, но у каждого приложения есть собственная директория, доступная для записи и чтения ему и только ему. Для передачи бита 1 приложение  $A$  изменяет количество свободного места в файловой системе, создавая в собственной директории файл с произвольным содержимым. Приложение  $B$  измеряет количество доступного места в файловой системе, фиксирует его уменьшение и делает вывод, что передан бит 1. Для передачи следующего единичного бита приложение  $A$  удаляет созданный им файл, а приложение  $B$  фиксирует увеличение свободного места. Размер файла подбирается эмпирическим путём так, чтобы действия пользователя и других приложений не спровоцировали ошибку приложения  $B$ . Приложение  $A$  передаёт бит 0, не изменяя ничего.

Основной фактор, снижающий скорость работы данного скрытого канала, — это синхронизация между приложениями. Рассмотрим два следующих способа её реализации.

1) Синхронизация посредством поочерёдного ожидания. После каждой передачи бита передающее приложение ожидает в течение времени, необходимого на считывание вторым приложением этого бита информации. Аналогично второе приложение ожидает, пока первое не передаст следующий бит. Проблема этого способа заключается в том, что время выполнения системного вызова записи в файл сильно зависит от загруженности системы и может увеличиваться в 2–3 раза. Поэтому для безошибочной передачи данных необходимо значительно увеличивать время ожидания приложений, что снижает пропускную способность канала. Максимальная скорость передачи данных, полученная при таком способе синхронизации, равна 12 бит/с.

2) Синхронизация посредством ещё одного скрытого канала. Этот способ быстрее предыдущего, но требует наличия ещё одного канала. При тестировании в качестве канала использовались общедоступные системные настройки звука/вибрации. Но пользователь своими действиями может легко вмешаться в передачу информации и сбить синхронизацию. Максимальная скорость передачи данных, полученная при таком способе синхронизации, равна 20 бит/с.

Ещё один найденный канал основан на атаке по времени. Атака по времени, или «тайминговая атака», использует время выполнения некоторой функции, которая зависит от произвольных пользовательских данных и секретных данных. Подобную функцию будем называть *уязвимой к тайминговой атаке*. Изучая время выполнения этой функции на разных пользовательских данных, можно сделать некоторые выводы о секретных данных. В файловой системе `ext2` существует функция стандартной библиотеки `stat`, которая, в свою очередь, использует функцию `strcmp`, являющуюся уязвимой к тайминговой атаке. Функция `stat` принимает в качестве аргумента имя файла и выполняет поиск требуемого файла в директории, выполняя сравнение переданного имени со всеми, хранящимися внутри.

Пусть есть приложение-злоумышленник  $A$  и приложение  $B$ , не являющееся злоумышленником. Приложение  $B$  хранит секретные данные в собственной директории, к которой имеет доступ на чтение и запись только оно. Приложение  $A$  может через скрытый канал, основанный на использовании уязвимой к тайминговой атаке функции, узнать секретные имена файлов в директории приложения  $B$  методом посимвольного подбора. Первым этапом приложение  $A$  узнаёт длину некоторого существующего файла в директории. Для этого оно выполняет в цикле вызов функции `stat`, передавая ей в качестве аргумента строки длины 1, 2, 3, ... Если цикл вызовов со строкой длины  $l$  выполняется дольше, чем хотя бы один из предыдущих циклов, то в директории существует хотя бы один файл с именем длины  $l$ . На этом первый этап считается завершённым. Вторым этапом приложение  $A$  начинает посимвольно подбирать имя файла, изменяя сначала первый символ в строке длиной  $l$ , затем второй и так далее. Символ считается подобранным верно, если цикл вызовов с этим символом на данной позиции выполняется дольше, чем с другим символом. После подбора последнего символа второй этап можно считать завершённым. Таким образом, скрытый канал от приложения  $B$  к приложению  $A$  без ведома приложения  $B$  и без непосредственного доступа приложения  $A$  к файлам реализуется посредством измерения приложением  $A$  разницы времени работы системной функции `stat` с фиксированными секретными и разными открытыми (контролируемыми любым пользователем) данными.

## ЛИТЕРАТУРА

1. *Schlegel R., Zhang K., Zhou X., et al.* Soundcomber: a stealthy and context-aware sound Trojan for smartphones // Proc. 18th Annual Network and Distributed System Security Symposium (NDSS '11), San Diego, CA, February 6–9, 2011. P. 17–33.

УДК 004.94

**ИСПОЛЬЗОВАНИЕ ЭЛЕКТРОННЫХ СЕРТИФИКАТОВ  
ДЛЯ АВТОРИЗАЦИИ ПО ДОВЕРЕННОСТИ В ОС LINUX**

В. И. Рыжков

Предлагается решение для делегирования некоторого набора прав от одного пользователя (доверителя) операционной системы другому (доверенному лицу) на определённый промежуток времени. Для этого предложено использовать «доверенности» — объекты, содержащие в себе такие поля, как идентификатор доверителя, идентификатор доверенного лица, время действия доверенности, а также набор прав, делегируемых доверенному лицу доверителем. Доверенность должна содержать также цифровую подпись на закрытом ключе доверителя под всеми вышеперечисленными полями. Предложенное решение реализовано для операционной системы Linux с помощью криптографического инструмента OpenSSL и подключаемых модулей аутентификации (PAM). В качестве доверенностей здесь выступают цифровые сертификаты стандарта X.509 v3, а делегируемые полномочия указываются по определённому формату в поле «Расширения» этих сертификатов. Сам функционал авторизации по доверенности реализован в виде модуля PAM.

**Ключевые слова:** *электронные сертификаты, X.509, Linux, PAM, OpenSSL.*

В операционных системах привилегии пользователя можно задавать, используя группы, в которые он входит.

Пусть некоторый пользователь (доверитель) хочет передать некоторые свои права другому пользователю (доверенному лицу), который изначально этими правами не обладает. Такая схема полезна в случае, когда доверителю приходится отсутствовать по той или иной причине и он хочет передать свои полномочия своему доверенному лицу. Самое очевидное решение: доверитель может добавить доверенное лицо в некоторую группу, которая обладает этими правами. При таком подходе возникают следующие проблемы:

- 1) Право переводить пользователя из группы в группу есть, как правило, далеко не у каждого.
- 2) Пусть право переводить пользователей из группы в группу у доверителя есть. Допустим, доверитель будет отсутствовать в течение месяца, но эти права необходимо делегировать на неделю. Следующие три недели доверенное лицо будет находиться в привилегированной группе, не имея в этом потребности.

Таким образом, возникает задача построения системы делегирования некоторого набора прав доступа, которыми обладает некий пользователь-доверитель (не обязательно «привилегированный» в системе), другому пользователю — доверенному лицу, который ими изначально может не обладать, на некоторый (определённый пользователем-доверителем) промежуток времени.

При этом, очевидно, должны выполняться следующие требования:

- 1) любой пользователь системы может быть доверителем для любого другого пользователя;
- 2) пользователь может делегировать только права, принадлежащие ему, и никакие другие;
- 3) только доверенное лицо может авторизоваться на делегируемые ему права;
- 4) доверитель может определять промежуток времени, в течение которого доверенное лицо наделяется делегируемыми ему правами.

Дадим формальное описание решения, удовлетворяющее перечисленным требованиям.

Пусть

- $U = \{u_1, u_2, \dots, u_n\}$  — множество пользователей, и каждый пользователь  $u_i \in U$  имеет пару  $(x_{u_i}, y_{u_i})$  — закрытый/открытый ключ. Очевидно, должно выполняться условие  $x_{u_i} \neq x_{u_j}, y_{u_i} \neq y_{u_j}$  для всех  $i \neq j$ ;
- $G = \{g_1, g_2, \dots, g_k\}$  — множество групп;
- $P = \{p_1, \dots, p_m\}$  — множество всех возможных прав доступа к объектам;
- $T = \{0, 1, 2, \dots\}$  — множество целых неотрицательных чисел (время);
- $PA : G \rightarrow 2^P$  — функция, задающая соответствие прав доступа для конкретной группы;
- $UA : U \rightarrow 2^G$  — функция, задающая множество групп, на которые может быть авторизован пользователь;
- $PROXY$  — множество доверенностей, объектов вида  $proxy_{u_i}^{u_j}(g, t_{start}, t_{end}) = (B, Sig_{x_{u_i}}(B))$ , где  $B = (u_i, u_j, g, t_{start}, t_{end})$ ;  $u_i, u_j \in U$ ;  $g \subseteq UA(u_i)$ ;  $t_{start}, t_{end} \in T$ ;  $Sig_{x_{u_i}}(B)$  — цифровая подпись  $B$  на закрытом ключе пользователя  $u_i$ . Другими словами, это сертификат, который подтверждает факт делегирования на промежуток времени  $[t_{start}, t_{end}]$  некоторого набора групп  $g$  от пользователя  $u_i$ , который изначально им обладает, пользователю  $u_j$ , который им изначально может и не обладать.

Определим условия корректности доверенности  $proxy_{u_i}^{u_j}(g, t_{start}, t_{end}) \in PROXY$  для пользователя  $u_k \in U$ , предъявляющего данную доверенность, в момент времени  $t_{current}$ :

- 1)  $t_{current} \in [t_{start}, t_{end}]$  — условие актуальности доверенности;
- 2)  $g \subseteq UA(u_i)$  — условие обладания доверителя делегируемыми правами;
- 3)  $k = j$  — условие предъявления доверенности доверенным лицом;
- 4)  $V(proxy_{u_i}^{u_j}(g, t_{start}, t_{end})) = \text{true}$  — условие корректности подписи.

Здесь  $V : PROXY \rightarrow \{\text{true}, \text{false}\}$  — функция проверки цифровой подписи.

Доверенность, удовлетворяющую условиям 1–4, далее будем называть корректной, в противном случае — некорректной.

Используем следующее обозначение: пусть  $A$  — некоторое непустое множество, тогда  $A^\emptyset = A \cup \{\emptyset\}$ .

Определим функцию  $assign : U \times PROXY^\emptyset \times T \rightarrow (2^G)^\emptyset$ , которая осуществляет авторизацию на делегированные группы при предъявлении корректной доверенности:

$$assign(u_j, z, t_{current}) = \begin{cases} \emptyset, & \text{если } z = \emptyset \text{ или } z \text{ некорректная;} \\ g, & \text{если } z = proxy_{u_i}^{u_j}(g, t_{start}, t_{end}) \text{ и } z \text{ корректная.} \end{cases}$$

Функция  $groups : U \times PROXY^\emptyset \times T \rightarrow (2^G)$  осуществляет авторизацию пользователей в системе. Определим её следующим образом:

$$groups(u_j, z, t_{current}) = UA(u_j) \cup assign(u_j, z, t_{current}).$$

Таким образом, если пользователь авторизуется без доверенности или авторизуется с некорректной доверенностью, то он получает ровно те права, которые дают ему группы, в которых он изначально состоит (посредством функции  $UA$ ). Однако при предъявлении корректной доверенности он может авторизоваться на некий набор групп, которым он изначально не обладал, но который делегировал ему пользователь-доверитель. Требования 1–4 выполняются благодаря использованию доверенностей, в которых явно указаны доверенное лицо, доверитель, определён срок действия, и все эти поля подписаны на закрытом ключе доверителя.

В реализации данного решения для операционной системы Linux в качестве доверенностей используются сертификаты X.509 версии 3 [1]. Сертификаты данного стандарта содержат следующие ключевые поля:

- имя эмитента (кто выдал сертификат);
- имя субъекта (кому выдан сертификат);
- период действия;
- расширения;
- подпись сертификата (с указанием алгоритма хэширования и подписи).

Поле «Расширения» представляет собой набор троек ( $OID, criticalityFlag, Value$ ), где  $OID$  (Object Identifier) используется для именования расширения;  $criticalityFlag$  — флаг критичности;  $Value$  — значение расширения. Расширения предоставляют возможность внедрения в сертификат произвольной информации до его создания.

Таким образом, сертификаты стандарта X.509 v3 могут использоваться в качестве доверенностей. Для этого в поле «Имя эмитента» необходимо указать имя пользователя-доверителя, в поле «Имя субъекта» — имя доверенного лица, в поле «Расширения» — набор делегируемых прав в системе. Доверителю необходимо также указать период действия доверенности в поле «Период действия» и подписать сертификат на своём закрытом ключе.

Создание доверенностей осуществляется при помощи криптографического инструмента OpenSSL [2]. Функция *assign*, авторизующая пользователя на делегированные группы (при предъявлении корректной доверенности), реализована в виде модуля PAM [3] — элемента ядра Linux.

#### ЛИТЕРАТУРА

1. <https://www.ietf.org/rfc/rfc5280.txt> — RFC 5280: Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile.
2. <http://www.openssl.org/> — OpenSSL: The Open Source toolkit for SSL/TLS.
3. <http://www.linux-pam.org/> — A Linux-PAM page.

УДК 004.94

### ФОРМИРОВАНИЕ ВЕКТОРОВ ПОКАЗАТЕЛЕЙ ДЛЯ ОБУЧЕНИЯ НЕЙРОННЫХ СЕТЕЙ ПРИ ОБНАРУЖЕНИИ АТАК НА WEB-ПРИЛОЖЕНИЯ

С. Н. Сорокин

Представлен подход к оценке качества и выбора наиболее подходящих показателей для обучения нейронных сетей при решении задач обнаружения атак на web-приложения, предложена методика формирования векторов показателей для классов атак, позволяющая уменьшить количество нейронных сетей, используемых для обнаружения различных атакующих воздействий.

**Ключевые слова:** обнаружение атак, обнаружение злоупотреблений, нейронная сеть, вектор показателей, классы атак, web-приложение.

Обнаружение различных классов атак на web-приложения является актуальной задачей. Одним из перспективных подходов к построению систем обнаружения атак является подход, предполагающий использование нейронных сетей для поиска злоупотреблений [1–3].

Для создания систем обнаружения атак на базе нейронных сетей, работающих по принципу обнаружения злоупотреблений, целесообразно решать следующие задачи:

- формирование множества показателей для обучения нейронной сети, описывающих состояние наблюдаемой системы;
- формирование векторов показателей для обучения нейронной сети, позволяющих проводить обнаружение различных классов атакующих воздействий.

При формировании множества показателей, описывающих состояние web-приложения, нужно учитывать, что активность пользователей изменяется в зависимости от времени суток, дня недели или ввиду естественного изменения популярности web-приложения. Более подробно данные вопросы рассмотрены автором в [4].

Рассмотрим процесс формирования векторов показателей для обучения нейронной сети (рис. 1).

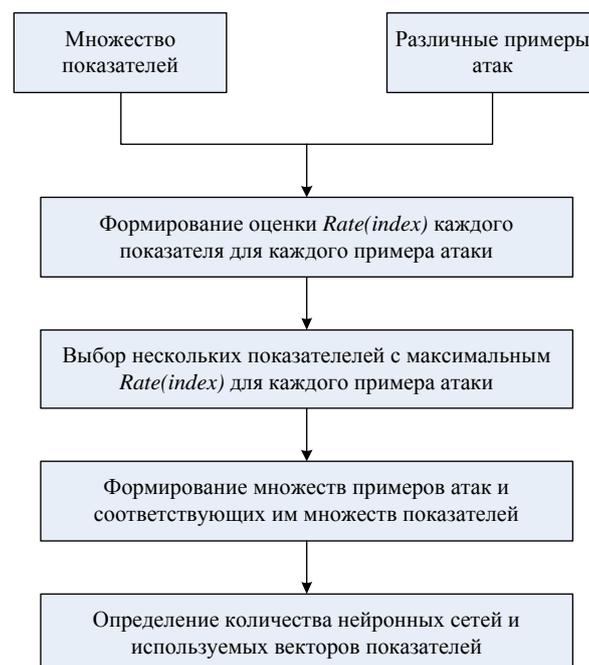


Рис. 1. Формирование векторов показателей

При формировании оценки показателя используются следующие свойства:

- амплитуда (разброс значений показателя);
- дифференциация (различие в среднем значении показателя на данных о поведении пользователей web-приложения и данных атаки);
- цикличность (свойство показателя иметь схожие значения в одинаковое время суток).

Общая оценка показателя вычисляется по формуле

$$\begin{aligned} & Rate(Index) = \\ & = (a \cdot Amplitude'(Index) + d \cdot Differentiation'(Index) + r \cdot Rhythm'(Index))/3, \end{aligned}$$

где  $Amplitude'(Index)$ ,  $Differentiation'(Index)$ ,  $Rhythm'(Index)$  — оценки в баллах амплитуды, дифференциации и цикличности соответственно;  $a$ ,  $d$ ,  $r$  — поправочные коэффициенты амплитуды, дифференциации и цикличности соответственно.

Для обнаружения атакующего воздействия выбираются показатели с наибольшей оценкой  $Rate(Index)$ . Заметим, что при таком подходе для каждого атакующего воздействия используется отдельная нейронная сеть со своим вектором показателей. Для уменьшения количества нейронных сетей может быть использована методика формирования векторов показателей для классов атак.

Введём следующие обозначения:

- $AttackQuantity$  — количество видов атак, для которых производится обучение нейронных сетей;
- $AttackType_i$  — некоторый вид атаки,  $i \in \{1, \dots, AttackQuantity\}$ ;
- $Indexes$  — множество всех показателей;
- $IndexQuantity$  — количество показателей во множестве показателей;
- $Index_j \in Indexes$  — некоторый показатель,  $j \in \{1, \dots, IndexQuantity\}$ ;
- $Rate_{AttackType_i}(Index_j)$  — оценка  $Rate(Index_j)$ , полученная при сравнении показателя  $Index_j$  на статистике нормального поведения пользователей и статистике атаки вида  $AttackType_i$ .

**Методика формирования векторов показателей для классов атак** заключается в следующем:

- 1) Для каждого показателя  $Index_j$  и вида атаки  $AttackType_i$  вычислить оценку  $Rate_{AttackType_i}(Index_j)$ .
- 2) Для каждой атаки  $AttackType_i$  сформировать множество  $\{Index_{i_1}, \dots, Index_{i_t}\}$  показателей, удовлетворяющих условию

$$\forall Index \in \{Index_{i_1}, \dots, Index_{i_t}\} \forall Index' \in Indexes \setminus \{Index_{i_1}, \dots, Index_{i_t}\} \\ (Rate_{AttackType_i}(Index) \geq Rate_{AttackType_i}(Index')).$$

- 3) Создать классы атак  $AttackClass_k$  и соответствующие им векторы  $\{Index_{i_1}, \dots, Index_{i_k}\}_k$ , помещая в один класс атаки  $AttackType_i$ , содержащие наибольшее количество  $v$  одинаковых показателей во множествах  $\{Index_{i_1}, \dots, Index_{i_t}\}$ . Для создания классов атак можно использовать итерационную процедуру (аналогичную алгоритму кластеризации методом  $k$ -средних [5]):
  - а) принять количество классов  $K = 1$ . Поместить все виды атак в один класс;
  - б) провести оценку качества обучения нейронной сети при использовании вектора показателей  $\{Index_{i_1}, \dots, Index_{i_k}\}_k$  (обычно для оценки качества обучения нейронной сети вычисляют процент правильных срабатываний и ошибок первого и второго рода [6]);
  - в) увеличить количество классов  $K$  на 1. Поместить все виды атак в  $K$  классов таким образом, чтобы два вида атак из одного класса содержали больше совпадений во множествах  $\{Index_{i_1}, \dots, Index_{i_t}\}$ , чем два вида атак из разных классов;

- г) провести оценку качества обучения нейронной сети при использовании векторов показателей  $\{Index_{i_1}, \dots, Index_{i_k}\}_k$  для каждого класса атак  $AttackClass_k$  на отдельной нейронной сети;
- д) если качество тестов ухудшилось, то вернуть множество классов атак, полученное на предыдущем шаге (при  $K - 1$ );
- е) если качество тестов улучшилось и ошибки лежат в установленных пределах, то вернуть текущее множество классов атак;
- ж) перейти к шагу «в».

В результате использования методики получено множество классов атак и соответствующее каждой атаке множество показателей для работы нейронной сети. Каждый класс атак обрабатывается отдельной нейронной сетью.

После формирования классов атак необходимо с помощью топологических тестов нейронной сети убедиться, что для различных атакующих воздействий внутри одного класса атак оптимальными являются схожие параметры архитектуры нейронной сети. В противном случае атакующие воздействия с отличными оптимальными параметрами архитектуры нейронной сети выделяются в отдельный класс атак.

#### ЛИТЕРАТУРА

1. Жульков Е. В. Построение нейронных сетей для обнаружения классов сетевых атак: дис. ... канд. техн. наук. СПб., 2007. 155 с.
2. Александров И. С. Разработка системы защиты web-приложений от автоматизированного копирования информации: дис. ... канд. техн. наук. М., 2003. 127 с.
3. Хафизов А. Ф. Нейросетевая система обнаружения атак на www-сервер: дис. ... канд. техн. наук. Уфа, 2004. 172 с.
4. Сорокин С. Н. Метод обнаружения атак типа «отказ в обслуживании» на web-приложения // Прикладная дискретная математика. 2014. № 1(23). С. 55–64.
5. Menasce D. A. and Almeida V. A. F. Capacity Planning for Web Services. Metrics, Models, and Methods. New Jersey: Prentice Hall PTR, 2001. 608 p.
6. Хайкин С. Нейронные сети: полный курс. 2-е изд., испр. М.: ООО «И.Д. Вильямс», 2006. 1104 с.

УДК 004.94

### РЕАЛИЗАЦИЯ МОНИТОРА БЕЗОПАСНОСТИ СУБД MySQL В DBF/DAM-СИСТЕМАХ

Н. О. Ткаченко

Предлагается прототип механизма, реализующего политику мандатного управления доступом типа multilevel security (MLS) и type enforcement (TE) на основе разработанной ранее формальной ДП-модели, а также механизм сокрытия структуры базы данных на основе метода переписывания запросов. Прототип реализован в виде DBF/DAM-модуля — для MySQL-проху, функционирующей между клиентом и сервером системы управления базами данных (СУБД) MySQL как прокси-сервер. При реализации модели безопасности предложен и использован подход, при котором функции в коде соответствуют де-юре правилам формальной ДП-модели.

**Ключевые слова:** компьютерная безопасность, управление доступом, реализация моделей безопасности, DBF/DAM-системы, СУБД MySQL, MySQL-проху.

В настоящее время активно развивается подход на основе DBF/DAM-технологий, заключающийся в реализации специализированного прокси-сервера, обеспечивающего базовое управление доступом, защиту от основных атак и мониторинг СУБД. Такие системы получили название *Database Firewall* (DBF) или *Database Activity Monitoring* (DAM) [1].

Все основные DBF/DAM-системы, к которым можно отнести, например, Oracle Database Firewall, GreenSQL, McAfee DAM, Imperva SecureSphere, ориентированы, как правило, на обнаружение подозрительной активности пользователя и предотвращение возможных атак. При этом механизмам управления доступом уделяется недостаточно внимания, так как предполагается, что они уже реализованы на уровне самой СУБД. В связи с этим реализация современных научно обоснованных механизмов управления доступом на уровне DBF/DAM-систем, несомненно, является перспективным направлением и позволяет решить следующие проблемы реализации политик управления доступом в изначально дискреционных СУБД:

- необходимость изменять исходный код защищаемой СУБД;
- реализацию механизма управления доступом для всех СУБД, поддерживающих язык SQL;
- необходимость изменять существующую инфраструктуру СУБД;
- уменьшение «поверхности атак» на защищаемую СУБД.

Предлагается прототип механизма управления доступом, реализующий политики мандатного управления доступом типа MLS и TE на основе разработанной ранее формальной ДП-модели [2] в виде DBF/DAM-модуля — для MySQL-проху, а также механизм сокрытия структуры БД на основе метода переписывания запросов. При реализации ДП-модели в коде используется подход, заключающийся в разделении кода на две части: функции управления доступом, соответствующие де-юре правилам преобразования ДП-модели и реализующие логику политик безопасности, и функции адаптации, необходимые для взаимодействия элементов СУБД с элементами механизмов управления доступом.

Основой прототипа является система MySQL-проху [3]. Данная система функционирует между клиентом и сервером СУБД MySQL, предназначена для балансировки нагрузки, обработки запросов, проходящих как от клиента к серверу, так и от сервера к клиенту, реализует механизм аварийного переключения. Для обработки запросов MySQL-проху использует встроенный язык Lua [4].

Реализован модуль на языке Lua для MySQL-проху, выполняющий следующие функции:

- 1) присвоение сущностям (базам данных, таблицам и столбцам) меток безопасности, а также их хранение;
- 2) синтаксический анализ запроса с целью идентификации всех сущностей;
- 3) принятие решения о продолжении обработки запроса или его прекращении на основе меток безопасности и мандатной политики управления доступом;
- 4) сокрытие внутренней структуры БД.

#### ЛИТЕРАТУРА

1. Database Activity Monitoring / Database Firewall. <http://www.provision.ro/threat-management/database-security/database-activity-monitoring-database-firewall#page1-1|page1-1>

2. Колегов Д. Н., Ткаченко Н. О., Чернов Д. В. Разработка и реализация мандатных механизмов управления доступом в СУБД MySQL // Прикладная дискретная математика. Приложение. 2013. № 6. С. 62–67.
3. Hinz S., DuBois P., and Stephens J. MySQL 5.7 Reference Manual. <http://dev.mysql.com/doc/refman/5.7/en/mysql-proxy.html>
4. Ierusalimsky R., Henrique de Figueiredo L., and Celes W. The Programming Language Lua. Lua 5.2 Reference Manual. <http://lua.org/manual/5.2/>

УДК 004.056.57

## МЕТОД ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ПОЛЬЗОВАТЕЛЕЙ ИНТЕРНЕТ-МАГАЗИНОВ МОБИЛЬНЫХ ПРИЛОЖЕНИЙ

Е. А. Толюпа

Предложен метод противодействия распространению вредоносного ПО через интернет-магазины Android-приложений. Метод основан на применении доверенных цифровых подписей (ДЦП) и алгоритма  $(n, t)$ -пороговой ДЦП с арбитром, который позволяет разработчику антивирусного ПО реализовать механизм распределения доверенности и права проверки приложений на наличие вредоносного кода между  $n$  центрами проверки таким образом, что ДЦП будет вычислена только с участием арбитра и только в том случае, если  $t$  ( $t < n$ ) центров проверки подтвердят отсутствие вирусов. Роль арбитра можно возложить на удостоверяющие центры. Таким образом, проверяющий доверяет разработчику антивирусного ПО и удостоверяющему центру (арбитру) и может не опасаться, что центр проверки окажется злоумышленником и подпишет небезопасное приложение. Предложенный метод могут использовать интернет-магазины для повышения уровня доверия к себе среди потенциальных клиентов.

**Ключевые слова:** антивирусная защита, доверенные цифровые подписи, пороговые доверенные цифровые подписи, Android, магазин приложений Android.

Бурное развитие платформы Android повлекло создание большого числа интернет-магазинов Android-приложений. На сегодняшний день популярностью пользуются Google Play, Яндекс.Store, Amazon mobile app distribution, Samsung Apps, SlideMe, GetJar. Пётр Меркулов, директор по развитию продуктов и услуг Лаборатории Касперского, утверждает: «Магазины приложений для Android — это лакомый кусочек для вирусологов. ... 99% всех обнаруженных в 2012 г. мобильных зловредов были нацелены на Android-устройства». В 2012 г. Google запустил сервис Bouncer, который представляет собой виртуальную машину, эмулирующую окружение Android и осуществляющую динамический анализ приложений. Магазин Яндекс.Store проверяет антивирусом своё приложение. Таким образом, пользователи вынуждены доверять процедуре проверки файла самого магазина. Пользователь может доверять крупным корпорациям, имеющим положительную репутацию.

Платформа Android является открытой, и любой может разрабатывать свои приложения и публиковать их в сети или создать свой магазин приложений. Пользователь вынужден доверять тому, кто публикует приложения в сети. Интернет-магазин может оказаться злоумышленником и публиковать приложения, утверждая, что они проверены антивирусом. Возможен вариант, когда интернет-магазин может отправить файл на проверку надёжному разработчику антивирусного ПО (АПО), чтобы тот, проверив файл, сформировал электронную подпись (ЭП). Наличие корректной ЭП для файла является гарантией отсутствия вредоносного ПО. В этом случае разработчик АПО

должен иметь широкую филиальную сеть по всему миру или единый мощный центр, в котором все файлы приложений будут проверяться на наличие вредоносного ПО. Таким образом, затрудняется продвижение небольших магазинов, и открытость платформы может не дать ожидаемого эффекта в её продвижении.

Выходом может служить передача процедуры проверки распределенным центрам. В работе автора [1] предложен метод антивирусной защиты конечных устройств, основанный на применении доверенных цифровых подписей [2] и алгоритма  $(n, t)$ -пороговой ДЦП с арбитром. Алгоритм  $(n, t)$ -пороговой ДЦП с арбитром позволяет разработчику АПО реализовать механизм распределения доверенности и права проверки приложений на наличие вредоносного кода между  $n$  доверенными центрами проверки таким образом, что ДЦП будет вычислена только с участием арбитра и только в том случае, если  $t$  центров проверки подтвердят отсутствие вирусов. Арбитру должны доверять все участники системы. В качестве арбитра может выступать удостоверяющий центр (элемент РКІ).

Взаимодействие участников представлено на рис. 1.

Подготовительный этап:

1. Разработчик АПО передаёт программное обеспечение для проверки файлов на наличие вредоносного кода и делегирует право проверки  $n$  центрам проверки.
2. Разработчик АПО передаёт удостоверяющему центру, который является арбитром, информацию, необходимую для вычисления ДЦП. Раскрытие информации третьим лицам ведёт к компрометации всей системы.

Проверка приложения:

3. Интернет-магазин передаёт файл с приложением (Android Package, APK-файл)  $t$  центрам проверки.
4. Каждый центр проверки с использованием программного обеспечения разработчика проверяет файл на наличие вредоносного кода и в случае успешной проверки вычисляет свою долю ДЦП и передает её арбитру.
5. Арбитр завершает вычисление ДЦП и передаёт полученное значение в интернет-магазин.
6. Интернет-магазин публикует APK-файл вместе с ДЦП.
7. Пользователь получает из интернет-магазина APK-файл и ДЦП для него. Убедившись в корректности ДЦП, вычисленной  $t$  центрами проверки, принимает решение, что приложение не содержит вредоносного кода.

В приведённой схеме пользователь доверяет разработчику АПО и арбитру. Он может не опасаться, что центр проверки окажется злоумышленником, так как ДЦП может быть сформирована только в том случае, если  $t$  из  $n$  ( $t < n$ ) центров проверки подтвердят безопасность файла, проверив его антивирусным программным обеспечением разработчика. Файл будет ненадёжным, если все  $t$  центров окажутся злоумышленниками. Таким образом, разработчику АПО нет необходимости создавать собственную филиальную сеть, а проверка файлов будет производиться на вычислительных ресурсах центров проверки, с которыми разработчик установит партнёрские отношения. Таким образом, строится модель с участниками инфраструктуры, которым доверяет пользователь. Предложенный метод антивирусной защиты могут использовать интернет-магазины для повышения уровня доверия к себе среди потенциальных клиентов.

В рамках данного исследования разработано приложение для платформы Android, которое вычисляет ДЦП для APK-файлов. Тестирование проводилось на мобильных телефонах с процессором Samsung Exynos 4412 (1,4 ГГц) и Samsung Exynos 4210



Рис. 1. Схема взаимодействия участников

(1,2 ГГц). В ходе тестирования, согласно данным приложения Android Assistant, использовалось только одно ядро многоядерных процессоров. Тестирование производилось на ARK-файлах 5,3 и 76 Мбайт. В таблице для каждого из файлов указано время проверки 10000 ДЦП.

Процессор	Файл 5,3 Мбайт	Файл 76 Мбайт
Ехynos 4412	97,4 с	1241,56 с
Ехynos 4210	143,21 с	1785,56 с

### ЛИТЕРАТУРА

1. *Толстова Е. А.* Механизм антивирусной защиты на базе  $(n, t)$ -пороговой ДЦП с арбитром // МАИС. 2014 (в печати).
2. *Mambo M., Usuda K., and Okamoto E.* Proxy signatures for delegating signing operation // Proc. of 3rd ACM Conference on Computer and Communications Security (CCS'96). ACM Press, 1996. P. 48–57.

УДК 004.94

## ДП-МОДЕЛЬ МАНДАТНОГО УПРАВЛЕНИЯ ДОСТУПОМ С КОНТРОЛЕМ ЦЕЛОСТНОСТИ СУБД MySQL

Д. В. Чернов

Работа посвящена разработке механизмов мандатного контроля целостности в мандатной ДП-модели СУБД MySQL. Вводятся основные элементы модели (решётка уровней целостности сущностей, функции избирательности контроля целостности, уровней целостности сущностей и т. д.), с помощью которых обеспечивается мандатный контроль целостности; описываются некоторые правила преобразования состояний системы; определяются состояния системы, в которых не происходит нарушения целостности, и формулируются условия, которые необходимы, чтобы система оставалась в этих состояниях.

**Ключевые слова:** управление доступом, мандатный контроль целостности, информационные потоки, формальные модели безопасности.

Рассматривается расширение мандатной ДП-модели MySQL [1], включающее в себя мандатный контроль целостности, основанный на модели Биба [2, 3]. Целью мандатного контроля целостности является предотвращение возможности получить доступ на запись сущности с высоким уровнем целостности субъект-сессией с низким уровнем целостности. Разрешается изменять сущность только таким субъект-сессиям, чьи уровни целостности не меньше уровня целостности сущности. Помимо этого, накладывается запрет на вызов процедур, целостность которых ниже целостности пользователя, от имени которого предписано их выполнение. В противном случае решение о возможности выполнить запрос процедуры, который, ввиду его низкой целостности, мог быть изменён третьим лицом, будет выполняться на основе более высокой целостности пользователя. Подобный сценарий может нарушить целостность других сущностей, что, несомненно, является недопустимым.

Для расширения модели мандатным контролем целостности вводятся следующие дополнительные элементы (недостающие специальные термины и обозначения из теории ДП-моделей см. в [3]):

1. Решётка упорядоченных уровней целостности сущностей  $(LI, \leq)$ .

2. Функция  $HLSI : O \cup (C \setminus c_0) \rightarrow \{\mathbf{true}, \mathbf{false}\}$  определяет наличие проверок мандатного контроля целостности при доступе к сущности. Если  $HLSI(e) = \mathbf{true}$ , то доступ к сущности  $e$  осуществляется с учётом проверок мандатного контроля целостности, в противном случае — без него. При этом значение функции  $HLSI(e)$  наследуется всеми сущностями, которые иерархически подчинены  $e$ , т. е.

$$\forall e' < e (HLSI(e') = HLSI(e)).$$

Предполагается, что если  $\exists e \in O \cup C (HLSI(e) = \mathbf{true})$ , то для всякого  $e' \in O_p \cup O_t$  выполняется  $HLSI(e') = \mathbf{true}$ . То есть если доступ хотя бы к одному объекту или контейнеру осуществляется с учётом мандатного контроля целостности, то так же осуществляется доступ ко всем процедурам и триггерам.

3. Функция  $id_e : OUC \rightarrow L \cup \{\emptyset\}$  определяет уровень целостности сущности-объекта или контейнера таким образом, что выполняются следующие условия для  $e \in O \cup C$ :

- если  $HLSI(e) = \mathbf{false}$ , то  $id_e(e) = \emptyset$ ;
- если  $HLSI(e) = \mathbf{true}$  и  $\neg \exists e' > e (id_e(e') \neq \emptyset)$ , то  $id_e(e) \neq \emptyset$ ;
- если  $id_e(e) \neq \emptyset$  и  $\exists e' > e (id_e(e') \neq \emptyset)$ , то  $id_e(e) > id_e(e')$ .

4. Функция  $id_s : U \rightarrow L \cup \{\emptyset\}$  определяет уровень целостности учётной записи пользователя.

Предполагается, что если значение функции  $id_e$  определено хотя бы для одной сущности  $e$ , то функция  $id_s$  определена для всех пользователей, т. е.

$$(\exists e \in O \cup C (id_e(e) \neq \emptyset)) \Rightarrow (\forall u \in U (id_s(u) \neq \emptyset)).$$

5. Функция  $ih_e : O \cup C \rightarrow L \cup \{\emptyset\}$  задаёт иерархические уровни целостности сущностей. Определена для  $e \in O \cup C$  следующим образом:

- если  $id_e(e) \neq \emptyset$ , то  $ih_e(e) = id_e(e)$ ;
- иначе
  - если  $HLSI(e) = \mathbf{true}$ ,  $\exists e' > e (HLSI(e') = \mathbf{true}, id_e(e') \neq \emptyset, \neg \exists e'' (e' > e'' > e, id_e(e'') \neq \emptyset))$ , то  $ih_e(e) = id_e(e')$ ;
  - если  $HLSI(e) = \mathbf{false}$ , то  $ih_e(e) = \emptyset$ .

Корректность определения функции  $ih_e$  обосновывает следующее

**Утверждение 1.** Если  $HLSI(e) = \text{true}$  и  $id_e(e) = \emptyset$ , то

$$\exists e' > e (HLSI(e') = \text{true}, id_e(e') \neq \emptyset).$$

В качестве примера приведём следующие правила преобразования состояний расширенной модели (таблица).

Правило	Исходное состояние $G$	Результирующее состояние $G'$
$access\_read(s, e)$	$s \in S, e \in DB \cup TAB \cup COL$ ; если $HLSI(e) = \text{true}$ , то $\neg \exists e' \in O \cup C (HLSI(e') = \text{true},$ $ih_e(e') > ih_e(e), (s, e', write_a) \in A)$	$A' = A \cup \{(s, e, read_a)\},$ $F' = F \cup \{(e, s, write_m)\}$
$access\_write(s, e)$	$s \in S, e \in DB \cup TAB \cup COL$	если $HLSI(e) = \text{true}$ , то $id_s(user(s)) \geq ih_e(e)$ и $\neg \exists e' \in O \cup C (HLSI(e') = \text{true}, ih_e(e') < ih_e(e),$ $(s, e', read_a) \in A)$ ; $A' = A \cup \{(s, e, write_a)\},$ $F' = F \cup \{(s, e, write_m)\}$
$execute\_proc(s, p)$	$s \in S, p \in O_p$ ; если $execute\_as(p) = as\_owner$ , то $w = owner(p)$ , иначе $w = user(s), id_s(w) \leq ih_e(p)$	$A' = A \cup \{(s, p, execute_a)\};$ если $execute\_as(p) = as\_owner$ , то по- ложим $user(s) = owner(p)$ , выполним после- довательно $G = G_0 \vdash_{op_1} G_1 \vdash \dots \vdash_{op_k} G_k = G'$ , где $(op_1, \dots, op_k) \in operations(p)$ . Вернём начальное значение $user(s)$

Будем говорить, что в состоянии системы не происходит нарушения целостности, если в нём выполняются следующие условия:

- $\neg \exists (e_1, e_2, write_m) \in F$ , где  $e_1, e_2 \in E$  и  $i_e(e_1) < i_e(e_2)$ ;
- $\neg \exists (s, p, execute_a) \in A$ , где  $s \in S, p \in O_p$  и  $i_e(p) < i_s(s)$ .

Говорим также, что в системе не происходит нарушения целостности, если не происходит нарушения целостности во всех её состояниях на всех траекториях функционирования системы.

**Теорема 1.** Пусть в начальном состоянии системы не происходит нарушения целостности и начальные множества доступов и информационных потоков пустые. Тогда в системе не происходит нарушения целостности.

#### ЛИТЕРАТУРА

1. Колегов Д. Н., Ткаченко Н. О., Чернов Д. В. Разработка и реализация мандатных механизмов управления доступом в СУБД MySQL // Прикладная дискретная математика. Приложение. 2013. № 6. С. 62–67.
2. Viba K. J. Integrity Considerations for Secure Computer Systems. Technical Report MTR-3153. MITRE Corp., 1975.
3. Девянин П. Н. Модели безопасности компьютерных систем. Управление доступом и информационными потоками: учеб. пособие для вузов. М.: Горячая линия-Телеком, 2012. 320 с.

УДК 004.453

## THE UNIVERSAL VULNERABILITY EXPLOITATION PLATFORM FOR CTF

P. Y. Sviridov, G. Y. Zaytsev, A. S. Ivachev

Capture the Flag (CTF) is a command educational computer security competition. The aim of all CTF games is to capture flags from vulnerable services of other teams. There are a lot of routine tasks in CTF games according to the rules. In order to automate the tasks, a big software project named *Pechkin* and implemented in C++ is built. The aim of *Pechkin* is to automate the exploitation of enemy services vulnerabilities. It runs instances of exploits, manages the instances, calculates statistics, performs logging, etc. *Pechkin* has a modular architecture. Each module implements one of the pointed functions and is started by the main one which is called a platform. The platform connects all the modules by passing messages between them. In different games, many parameters (e.g. the jury system interface and rules) may vary setting some restrictions. *Pechkin* cares about them, and the team members are free of them. The only offensive concern left for the participants is the creative process of finding vulnerabilities and writing exploits. The architecture allows the implementation of a scalable system with a load-balancing which is very important to CTF, because the game is long, unpredictable, and resource-draining.

**Keywords:** *CTF, flag, vulnerability, exploit.*

CTF, or Capture the Flag, is a computer security competition that is usually designed to serve as an educational exercise to give the participants an experience in securing a computer and in designing, developing, and reacting to the real-world sort of attacks. The aim of all CTF games is to capture *flags* from vulnerable services of other teams. The flags are some secret data that jury gives to the teams and the vulnerability is a service weakness which is caused by incorrect service usage or implementation. The only way to capture a flag is to exploit a *vulnerability*. It may seem that a team should find the greatest amount of vulnerabilities to win the game, but it is not necessary the truth. The team with the greatest number of enemies flags is awarded the victory.

To capture flags the participants write *exploits*—small programs that utilize vulnerabilities in order to make the enemies services behave in the favour of the exploits authors, i. e. to give them back enemies flags. The instances of the exploits are run against each team, and the collected flags are sent to the jury. The jury decides on success of capturing each flag using the information about the original distribution of flags and answers whether a flag was truly given to one team and then received from another, i. e. captured, or not. In the case of successful capture, the team that provided the flag to the jury scores points that are usually called *offensive points*, and the team which flag was captured receives less *defensive points* than usual. The overall scores are calculated as an aggregate of both offensive points and defensive points.

In order to automate a lot of routine tasks in CTF games, a big software project named *Pechkin* and implemented in C++ is built. Particularly, it does the following: runs instances of exploits, manages the instances, sends flags to the jury, checks whether the flag has already been sent, calculates statistics, performs logging.

*Pechkin* has a modular structure. Each module implements one of the following features:

- receiving flags from exploits;
- storing flags to the team storage (that is database);
- reading flags from the team storage;

- sending flags to the jury;
- managing instances of exploits;
- calculating statistics;
- logging the game events.

Receiving module provides the interface to the team members for accumulation of the captured flags in the team storage. The storage is a database which stores flags in a certain format.

Sending module sends flags from the storage to the jury and deals with the jury answer. Normally, the answer simply states whether the flag is accepted as properly captured or not, and some explanation is provided. However, there are some CTF games that do not allow participants to submit the captured flags to the jury under certain circumstances. In this case, the team should wait until the conditions for submission hold true and then resubmit the flag. The sending module handles this situation automatically. Another obstacle to be dealt with is the possible restriction on the number of connections from one team to the jury server. Because all team members send their flags to Pechkin, and the sending module of it has the only connection to the jury, this possible limit is also never broken.

Statistics module collects statistics and presents it at the web page. This helps the team members to understand whether their exploits are useful or not. Statistics also include the information about the teams that has already patched their services and expelled the vulnerability.

Logging module registers events and records them to the journal. It helps to analyse the game process after the game ends.

Exploit manager module starts instances of exploits, gives addresses of vulnerable hosts and takes flags returned by the instances.

Every module is started by the main one which is called a platform. The platform connects all the modules by passing messages between them. The platform has message queue for each module. If one of the modules does not cope with the tasks from its queue, the platform starts another instance of this module. All instances of one module work separately and the message mechanism allows the platform to load-balancing between their queues.

The architecture allows the implementation of a scalable system with load-balancing which is very important to CTF, because the game is long, unpredictable, and resource-draining.

All modules are C++ classes inherited from the abstract class, for they should have the same interface. The interface comprises `Init()`, `Run()`, `Pause()`, and `Stop()` methods and the pointer to its message queue. A module also must have a pointer to the platform for sending messages to other modules. However, it should not access other methods of the platform class. Therefore, a module has the pointer to the wrapper of the platform class providing only one method of the platform.

In different games, many parameters (e. g. the jury system interface and rules) may vary. When a module is initialized, it gets the name of the configuration file as an argument. The file describes some of the module parameters, e. g. database authentication parameters or the IP range of the enemy vulnerable hosts.

A module instance can be in one of the five states: `NEW`, `READY`, `RUNNING`, `PAUSED`, and `STOPPED`. After initialization, an instance goes to the state `NEW`. When the platform runs a module instance, it changes its state to `RUNNING` and starts to handle messages from its queue. If the queue is empty, state is changed to `READY`. The instance also can be paused and stopped by the platform.

The platform class implements the design pattern Singleton, for there always should be only one instance of the class. All modules classes are loaded to the platform memory dynamically [1]. The platform only has the hash table of loaded modules. This mechanism allows to create arbitrary number of modules instances and create modules during the work of the platform. The platform managing is done via the administration console. The console has the commands allowing to load the modules, run, pause, and stop them.

Pechkin automates all the attack processes in the CTF games. Team members are freed from sending flags to the jury directly or checking whether other teams have already patched the vulnerabilities. The only offensive concern left for the participants is the creative process of finding vulnerabilities and writing exploits. After submission of an exploit to Pechkin, the author can check whether his script is useful and improve it if necessary. Of course, the written exploit should correspond to the internal format of Pechkin.

#### BIBLIOGRAPHY

1. *Norton J.* Dynamic class loading for C++ on Linux // Linux Journal. 2000. Iss. 73. <http://www.linuxjournal.com/article/3687>

Секция 6

## МАТЕМАТИЧЕСКИЕ ОСНОВЫ НАДЁЖНОСТИ ВЫЧИСЛИТЕЛЬНЫХ И УПРАВЛЯЮЩИХ СИСТЕМ

УДК 519.718

### НЕНАДЁЖНОСТЬ СХЕМ В БАЗИСЕ РОССЕРА — ТУРКЕТТА<sup>1</sup>

М. А. Алехина, О. Ю. Барсукова

Рассматривается реализация функций трёхзначной логики схемами из ненадёжных функциональных элементов в базисе Россера — Туркетта. Предполагается, что все базисные элементы независимо друг от друга переходят в такие неисправные состояния, что любой базисный элемент на любом входном наборе с вероятностью  $1 - 2\varepsilon$  выдаёт правильное значение и с вероятностью, равной  $\varepsilon$ , может выдать любое из двух неправильных значений. Получены верхние и нижние оценки ненадёжности схем, которые оказались асимптотически равны для функций некоторого класса.

**Ключевые слова:** функции трёхзначной логики, схема из ненадёжных функциональных элементов, ненадёжность схемы.

Пусть  $n \in \mathbb{N}$ , а  $P_3$  — множество всех функций трёхзначной логики, т. е. функций  $f(x_1, \dots, x_n) : \{0, 1, 2\}^n \rightarrow \{0, 1, 2\}$ . Обозначим через  $\tilde{x}$  набор  $(x_1, \dots, x_n)$ .

Рассмотрим реализацию функций из множества  $P_3$  схемами из ненадёжных функциональных элементов в базисе Россера — Туркетта  $\{0, 1, 2, J_0(x_1), J_1(x_1), J_2(x_1), \max\{x_1, x_2\}, \min\{x_1, x_2\}\}$ . Будем считать, что схема из ненадёжных элементов реализует функцию  $f(\tilde{x})$ , если при поступлении на входы схемы набора  $\tilde{a}$  при отсутствии неисправностей в схеме на её выходе появляется значение  $f(\tilde{a})$ .

Предполагается, что все базисные элементы ненадёжны, переходят в неисправные состояния независимо друг от друга. Базисный элемент с приписанной ему функцией  $\varphi(x_1, x_2)$  на любом входном наборе  $(a_1, a_2)$ ,  $\varphi(a_1, a_2) = \tau$ , с вероятностью  $1 - 2\varepsilon$  ( $\varepsilon \in (0, 1/4)$ ) выдаёт значение  $\tau \bmod 3$ , с вероятностью  $\varepsilon$  — значение  $(\tau + 1) \bmod 3$  и с вероятностью  $\varepsilon$  — значение  $(\tau + 2) \bmod 3$ .

Пусть схема  $S$  реализует функцию  $f(\tilde{x})$ ,  $\tilde{a}$  — произвольный входной набор схемы  $S$ ,  $f(\tilde{a}) = \tau$ . Обозначим через  $P_{f(\tilde{a}) \neq \tau}(S, \tilde{a})$  вероятность появления ошибки на выходе схемы  $S$  при входном наборе  $\tilde{a}$ . Ясно, что  $P_{f(\tilde{a}) \neq \tau}(S, \tilde{a}) = P_{\tau+1}(S, \tilde{a}) + P_{\tau+2}(S, \tilde{a})$ .

Например, если входной набор  $\tilde{a}$  схемы  $S$  такой, что  $f(\tilde{a}) = 0$ , то вероятность ошибки на этом наборе равна  $P_{f(\tilde{a}) \neq 0}(S, \tilde{a}) = P_1(S, \tilde{a}) + P_2(S, \tilde{a})$ .

Ненадёжностью схемы  $S$  будем называть число  $P(S) = \max\{P_{f(\tilde{a}) \neq \tau}(S, \tilde{a})\}$ , где максимум берётся по всем входным наборам  $\tilde{a}$  схемы  $S$ . Надёжность схемы  $S$  равна  $1 - P(S)$ .

Пусть  $P_\varepsilon(f) = \inf P(S)$ , где инфимум берётся по всем схемам  $S$  из ненадёжных элементов, реализующим функцию  $f$ .

Схема  $A$  из ненадёжных элементов, реализующая функцию  $f$ , называется асимптотически оптимальной по надёжности, если  $P(A) \sim P_\varepsilon(f)$  при  $\varepsilon \rightarrow 0$ .

<sup>1</sup>Работа поддержана грантами РФФИ № 14-01-00273 и 14-01-31360.

Полученную ранее в работе [1] верхнюю оценку ненадёжности удалось доказать, существенно ослабив ограничение на  $\varepsilon$  (ранее эта вероятность зависела от  $n$  — числа переменных функции, а в теореме 1 её удалось ограничить константой).

**Теорема 1.** Любую функцию  $f \in P_3$  можно реализовать такой схемой  $D$ , что  $P(D) \leq 6\varepsilon + 126\varepsilon^2$  при всех  $\varepsilon \in (0, 0,001]$ .

Из теоремы 1 следует, что любую функцию из  $P_3$  можно реализовать схемой, функционирующей с ненадёжностью, асимптотически (при  $\varepsilon \rightarrow 0$ ) не больше  $6\varepsilon$ .

Обозначим через  $K(n)$  множество функций  $f(x_1, x_2, \dots, x_n)$  ( $n \geq 3$ ) из  $P_3$ , каждая из которых принимает все три значения 0, 1, 2 и не представима ни в виде  $\max\{x_k, g(\tilde{x})\}$ , ни в виде  $\min\{x_k, g(\tilde{x})\}$  ( $k \in \{1, 2, \dots, n\}$ ,  $g(\tilde{x})$  — произвольная функция из  $P_3$ ).

Обозначим через  $K$  множество  $K = \bigcup_{n=3}^{\infty} K(n)$ .

Справедлива теорема 2 о нижней оценке ненадёжности, доказательство которой аналогично доказательству теорем о нижних оценках [2, 3].

**Теорема 2.** Пусть функция  $f \in K$ . Тогда для любой схемы  $S$ , реализующей  $f$ , при  $\varepsilon \in (0, 0,001]$  верно неравенство  $P(S) \geq 6\varepsilon - 16\varepsilon^2 + 12\varepsilon^3$ .

**Утверждение 1.**  $|K(n)| \geq 3^{3^n} - 2n3^{2 \cdot 3^{n-1}} - 3 \cdot 2^{3^n}$ .

Из утверждения 1 следует, что класс  $K$  содержит почти все функции из  $P_3$ , поскольку

$$\lim_{n \rightarrow \infty} \frac{3^{3^n} - 2n3^{2 \cdot 3^{n-1}} - 3 \cdot 2^{3^n}}{3^{3^n}} = 1.$$

Из теоремы 2 следует, что функцию из класса  $K$  (содержащего почти все функции множества  $P_3$ ) нельзя реализовать схемой с ненадёжностью, асимптотически (при  $\varepsilon \rightarrow 0$ ) не меньше чем  $6\varepsilon$ . Следовательно, любая схема, удовлетворяющая условиям теоремы 1 и реализующая функцию из класса  $K$ , является асимптотически оптимальной по надёжности и функционирует с ненадёжностью, асимптотически равной  $6\varepsilon$  при  $\varepsilon \rightarrow 0$ .

Таким образом, получаем следующий результат: почти все функции из  $P_3$  можно реализовать асимптотически оптимальными по надёжности схемами, функционирующими с ненадёжностью, асимптотически равной  $6\varepsilon$  при  $\varepsilon \rightarrow 0$ .

#### ЛИТЕРАТУРА

1. *Алехина М. А., Барсукова О. Ю.* О ненадёжности схем, реализующих функции из  $P_3$  // Изв. вузов. Поволжский регион. Физико-математические науки. 2012. №1(21). С. 57–65.
2. *Алехина М. А.* О ненадёжности схем из ненадёжных функциональных элементов при однотипных константных неисправностях на выходах элементов // Дискретная математика. 1993. Т. 5. Вып. 2. С. 59–74.
3. *Alekhina M. A.* Synthesis and complexity of asymptotically optimal circuits with unreliable gates // Fundamenta Informaticae. 2010. No. 104(3). P. 219–225.

УДК 519.718

## О НАДЁЖНОСТИ СХЕМ В БАЗИСЕ ИЗ НЕНАДЁЖНЫХ И АБСОЛЮТНО НАДЁЖНЫХ ЭЛЕМЕНТОВ<sup>1</sup>

М. А. Алехина, А. Е. Лакомкина

Рассматривается реализация булевых функций схемами в стандартном базисе, содержащем конъюнкцию, дизъюнкцию и инверсию. Предполагается, что некоторые из базисных элементов (например, конъюнктор) абсолютно надёжны, а остальные (инвертор и дизъюнктор) — ненадёжные, с вероятностью  $\varepsilon \in (0, 1/2)$  подвержены инверсным неисправностям на выходах. Предполагается, что все ненадёжные элементы схемы переходят в неисправные состояния независимо друг от друга. Получены ответы на вопросы: какова ненадёжность схем, если некоторые из базисных элементов абсолютно надёжны, а другие ненадёжны?

**Ключевые слова:** *ненадёжные и абсолютно надёжные функциональные элементы, надёжность и ненадёжность схемы, инверсные неисправности на выходах элементов.*

Рассматривается реализация булевых функций схемами в стандартном базисе  $\{x_1 \& x_2, x_1 \vee x_2, \bar{x}_1\}$ . Предполагается, что некоторые из базисных элементов абсолютно надёжны, а остальные — ненадёжные, с вероятностью  $\varepsilon \in (0, 1/2)$  подвержены инверсным неисправностям на выходах. Эти неисправности характеризуются тем, что в исправном состоянии базисный элемент реализует приписанную ему булеву функцию  $\varphi$ , а в неисправном — функцию  $\bar{\varphi}$ . Считаем, что схема  $S$ , содержащая ненадёжные элементы, реализует булеву функцию  $f(x_1, \dots, x_n)$ , если при поступлении на входы схемы двоичного набора  $a$  при отсутствии неисправностей в схеме  $S$  на её выходе появляется значение  $f(a)$ . Предполагается, что все ненадёжные элементы схемы переходят в неисправные состояния независимо друг от друга.

Впервые задачу синтеза надёжных схем из ненадёжных функциональных элементов рассматривал Дж. фон Нейман [1]. Он также предполагал, что все базисные элементы с вероятностью  $\varepsilon \in (0; 1/2)$  подвержены инверсным неисправностям на выходах и переходят в неисправные состояния независимо друг от друга. Дж. фон Нейман с помощью итерационного метода установил, что любую булеву функцию можно реализовать схемой, вероятность ошибки на выходе которой не больше  $c\varepsilon$  ( $c$  — положительная, зависящая от рассматриваемого базиса константа). Для повышения надёжности некоторой исходной схемы путём многократного дублирования он использовал схему, реализующую функцию голосования  $g(x_1, x_2, x_3) = x_1x_2 \vee x_1x_3 \vee x_2x_3$ .

Число  $P(S)$ , равное максимальной вероятности ошибки на выходе схемы  $S$  при всевозможных входных наборах схемы, назовем ненадёжностью схемы  $S$ ; надёжность схемы  $S$  равна  $1 - P(S)$ .

С. В. Яблонский [2] рассматривал задачу синтеза надёжных схем в базисе  $\{x_1 \& x_2, x_1 \vee x_2, \bar{x}_1, g(x_1, x_2, x_3)\}$ . Он предполагал, что элемент, реализующий функцию голосования  $g$ , абсолютно надёжный, а конъюнктор, дизъюнктор и инвертор — ненадёжные, подвержены произвольным неисправностям, ненадёжность каждого из них не больше  $\varepsilon$ . Им доказано, что для любого  $p > 0$  существует алгоритм, который для каждой булевой функции  $f(x_1, x_2, \dots, x_n)$  для любого  $n$  строит такую схему  $S$ , что сложность схемы  $L(S) \lesssim 2^{n-1}/n$ , а  $P(S) \leq p$  (т. е. ненадёжность схемы сколь угодно мала). Такие схемы называют схемами сколь угодно высокой надёжности.

<sup>1</sup>Работа поддержана грантом РФФИ, проект № 14-01-00273.

В отличие от С. В. Яблонского, А. В. Васин [3] предполагал, что все элементы базиса  $\{x_1 \& x_2, x_1 \vee x_2, \bar{x}_1\}$  ненадёжны, с вероятностью  $\varepsilon$  подвержены инверсным неисправностям на выходах, и доказал, что любую функцию можно реализовать такой схемой  $S$ , что  $P(S) \leq 3\varepsilon + 32\varepsilon^2$  при всех  $\varepsilon \in (0, 1/128]$ .

В этой работе (в зависимости от того, какие базисные элементы ненадёжны) получены следующие результаты.

**Теорема 1.** Пусть конъюнктор и дизъюнктор абсолютно надёжны, а инвертор ненадёжный. Тогда любую функцию можно реализовать такой схемой  $S^{(k)}$ , что  $P(S) \leq 4(10\varepsilon^2)^k$  при всех  $\varepsilon \in (0, 1/128]$ ,  $k \in \mathbb{N}$ .

Из теоремы 1 следует, что любую функцию можно реализовать схемой сколь угодно высокой надёжности. Кроме того, любая неконстантная монотонная функция  $f \in [x_1 \& x_2, x_1 \vee x_2]$ , т. е. может быть представлена в виде ДНФ, в которой нет отрицаний. Поэтому такую функцию  $f$  можно реализовать абсолютно надёжно.

**Теорема 2.** Пусть конъюнктор абсолютно надёжный, а инвертор и дизъюнктор ненадёжные; или дизъюнктор абсолютно надёжный, а инвертор и конъюнктор ненадёжные. Тогда любую функцию можно реализовать такой схемой  $S$ , что  $P(S) \leq \varepsilon + 10\varepsilon^2$  при всех  $\varepsilon \in (0, 1/128]$ .

**Теорема 3.** Пусть инвертор абсолютно надёжный, а конъюнктор и дизъюнктор ненадёжные. Тогда любую функцию можно реализовать такой схемой  $S$ , что  $P(S) \leq 3\varepsilon + 32\varepsilon^2$  при всех  $\varepsilon \in (0, 1/128]$ .

**Теорема 4.** Пусть конъюнктор и инвертор абсолютно надёжные, а дизъюнктор ненадёжный; или дизъюнктор и инвертор абсолютно надёжные, а конъюнктор ненадёжный. Тогда любую функцию можно реализовать абсолютно надёжной схемой.

#### ЛИТЕРАТУРА

1. Von Neuman J. Probabilistic logics and the synthesis of reliable organisms from unreliable components // Automata Studies / eds. C. Shannon and J. McCarthy. Princeton, NJ: Princeton University Press, 1956. P. 329–378. (Рус. пер.: Автоматы. М.: ИЛ, 1956. С. 68–139.)
2. Яблонский С. В. Асимптотически наилучший метод синтеза надежных схем из ненадежных элементов // Banach Center. 1982. No. 7. P. 11–19.
3. Васин А. В. Об асимптотически оптимальных схемах в базисе  $\{x \& y, x \vee y, \bar{x}\}$  при инверсных неисправностях на выходах элементов // Изв. вузов. Поволжский регион. Физико-математические науки. 2008. № 4. С. 3–17.

УДК 519.718

## О ПОЛНЫХ БАЗИСАХ С КОЭФФИЦИЕНТОМ НЕНАДЁЖНОСТИ 5<sup>1</sup>

А. В. Васин

Рассматривается задача синтеза асимптотически оптимальных по надёжности схем, реализующих булевы функции, при инверсных неисправностях на выходах элементов в некоторых полных базисах. Доказано, что в рассматриваемых базисах почти все булевы функции можно реализовать асимптотически оптимальными по надёжности схемами, которые функционируют с ненадёжностью, асимптотически равной  $5\varepsilon$  при  $\varepsilon \rightarrow 0$ , где  $\varepsilon$  — вероятность инверсной неисправности на выходе базисного элемента.

**Ключевые слова:** ненадёжные функциональные элементы, асимптотически оптимальные по надёжности схемы, инверсные неисправности на выходах элементов, синтез схем из ненадёжных элементов.

Рассматривается реализация булевых функций схемами [1] из ненадёжных функциональных элементов в произвольном полном конечном базисе  $B$ . Предполагаем, что все элементы схемы независимо друг от друга с вероятностью  $\varepsilon \in (0, 1/2)$  подвержены инверсным неисправностям на выходах. Эти неисправности характеризуются тем, что в исправном состоянии функциональный элемент реализует приписанную ему булеву функцию  $\psi$ , а в неисправном — функцию  $\bar{\psi}$ . Считаем, что схема  $S$  из ненадёжных элементов реализует булеву функцию  $f(x_1, x_2, \dots, x_n)$ , если при поступлении на входы схемы двоичного набора  $a = (a_1, a_2, \dots, a_n)$  при отсутствии неисправностей на выходе схемы  $S$  появляется значение  $f(a)$ .

Ненадёжностью  $P(S)$  схемы  $S$  назовем максимальную вероятность ошибки на выходе схемы  $S$  при всевозможных входных наборах схемы. Надёжностью схемы  $S$  равна  $1 - P(S)$ . Пусть  $P_\varepsilon(f) = \inf P(S)$ , где инфимум берется по всем схемам  $S$  из ненадёжных элементов, реализующим булеву функцию  $f(x_1, x_2, \dots, x_n)$ . Схема  $A$  из ненадёжных элементов, реализующая функцию  $f$ , называется асимптотически оптимальной (асимптотически наилучшей) по надёжности, если  $P(A) \sim P_\varepsilon(f)$  при  $\varepsilon \rightarrow 0$ .

Число  $k$  будем называть коэффициентом ненадёжности полного базиса, если все функции в этом базисе можно реализовать схемами с ненадёжностью, асимптотически не больше  $k\varepsilon$  (при  $\varepsilon \rightarrow 0$ ), и найдётся функция  $f$ , которую нельзя реализовать схемой с ненадёжностью, асимптотически меньше чем  $k\varepsilon$  (при  $\varepsilon \rightarrow 0$ ).

В [2] обосновано, что  $k \in \{1, 2, 3, 4, 5\}$ . Эта работа посвящена полным базисам с коэффициентом ненадёжности  $k = 5$ .

Пусть

$$\begin{aligned} \Psi_1 &= \{0, 1, \bar{x}_1\} \cup \bigcup_{k=2}^{\infty} \{ \& x_i \}, \\ \Psi_2 &= \{0, 1\} \cup \bigcup_{k=2}^{\infty} \{ \& x_i \} \cup \bigcup_{k=1}^{\infty} \bigcup_{j=1}^k \{ \bar{x}_j \cdot \& x_i \}, \\ \Psi_1^* &= \{0, 1, \bar{x}_1\} \cup \bigcup_{k=2}^{\infty} \{ \bigvee x_i \}, \\ \Psi_2^* &= \{0, 1\} \cup \bigcup_{k=2}^{\infty} \{ \bigvee x_i \} \cup \bigcup_{k=1}^{\infty} \bigcup_{j=1}^k \{ \bar{x}_j \vee \bigvee x_i \}. \end{aligned}$$

<sup>1</sup>Работа поддержана грантом РФФИ, проекты № 14-01-31360 и 14-01-00273.

С. И. Аксенов сформулировал следующую теорему.

**Теорема 1** [3]. Пусть  $B$  — полный базис и  $B \not\subseteq \Psi_1$ ,  $B \not\subseteq \Psi_2$ ,  $B \not\subseteq \Psi_1^*$ ,  $B \not\subseteq \Psi_2^*$ . Тогда любую булеву функцию  $f$  можно реализовать схемой  $S$  над  $B$  с ненадёжностью  $P(S) \leq 4\varepsilon + c\varepsilon^2$  при  $\varepsilon \in (0, \varepsilon_0]$ , где константы  $c > 0$ ,  $\varepsilon_0 \in (0, 1/2)$  зависят от базиса.

Из теоремы 1 следует: если полный базис  $B$  удовлетворяет условиям  $B \not\subseteq \Psi_1$ ,  $B \not\subseteq \Psi_2$ ,  $B \not\subseteq \Psi_1^*$ ,  $B \not\subseteq \Psi_2^*$ , то его коэффициент ненадёжности  $k \in \{1, 2, 3, 4\}$ . Однако теорема 1 — только верхняя оценка ненадёжности, которая не даёт представления о коэффициенте ненадёжности базисов  $B$ , удовлетворяющих  $B \subseteq \Psi_1$ , или  $B \subseteq \Psi_2$ , или  $B \subseteq \Psi_1^*$ , или  $B \subseteq \Psi_2^*$ .

С. И. Аксеновым в [4] получена верхняя оценка ненадёжности схем в произвольном полном конечном базисе при инверсных неисправностях на выходах элементов. Он доказал, что существуют такие константы  $\varepsilon_0 \in (0, 1/2)$  и  $d > 0$ , зависящие от базиса, что любую булеву функцию  $f$  можно реализовать схемой  $S$  с ненадёжностью  $P(S) \leq 5\varepsilon + d\varepsilon^2$  при  $\varepsilon \in (0, \varepsilon_0]$ .

В работе [5] явно найдены константы  $d$ ,  $\varepsilon_0$  и доказана теорема 2.

**Теорема 2** [5]. В произвольном полном конечном базисе  $B$  любую булеву функцию  $f$  можно реализовать схемой  $A$  с ненадёжностью  $P(A) \leq 5\varepsilon + 182\varepsilon^2$  при  $\varepsilon \leq 1/960$ .

Теорема 2 справедлива и для базисов  $B$ , удовлетворяющих условию  $B \subseteq \Psi_1$ , или  $B \subseteq \Psi_2$ , или  $B \subseteq \Psi_1^*$ , или  $B \subseteq \Psi_2^*$ .

Автором в [2] решена задача построения асимптотически оптимальных по надёжности схем при инверсных неисправностях на выходах элементов в полных базисах из трёхвыходовых элементов, доказаны нижние оценки ненадёжности для базисов

$$\begin{aligned} B &\subset \{0, 1, \bar{x}_1, x_1 \& x_2, x_1 \& x_2 \& x_3\}, \\ B &\subset \{0, 1, x_1 \& x_2, x_1 \& x_2 \& x_3, \bar{x}_1 \& x_2, \bar{x}_1 \& x_2 \& x_3\}, \\ B &\subset \{0, 1, \bar{x}_1, x_1 \vee x_2, x_1 \vee x_2 \vee x_3\}, \\ B &\subset \{0, 1, x_1 \vee x_2, x_1 \vee x_2 \vee x_3, \bar{x}_1 \vee x_2, \bar{x}_1 \vee x_2 \vee x_3\} \end{aligned}$$

и показано, что коэффициент ненадёжности указанных базисов равен 5. Нетрудно видеть, что эти базисы являются подмножествами множеств  $\Psi_1$ ,  $\Psi_2$ ,  $\Psi_1^*$ ,  $\Psi_2^*$ .

Поэтому можно предположить, что в базисах  $B$ , удовлетворяющих условию  $B \subseteq \Psi_1$ , или  $B \subseteq \Psi_2$ , или  $B \subseteq \Psi_1^*$ , или  $B \subseteq \Psi_2^*$ , коэффициент ненадёжности базиса также равен 5. Для проверки справедливости последней гипотезы необходимо доказать нижние оценки ненадёжности для этих базисов.

Обозначим  $K(n)$  — множество булевых функций  $f$ , зависящих от переменных  $x_1, x_2, \dots, x_n$ , не представимых в виде  $(x_i^a \& g(\tilde{x}))^b$ , где  $i = 1, 2, \dots, n$ ,  $a, b \in \{0, 1\}$ ,  $\tilde{x} = (x_1, x_2, \dots, x_n)$ , и сформулируем теорему о нижних оценках ненадёжности для названных базисов.

**Теорема 3.** Пусть  $B$  — полный конечный базис и  $B \subset \Psi_1$ , или  $B \subset \Psi_2$ , или  $B \subset \Psi_1^*$ , или  $B \subset \Psi_2^*$ . Пусть функция  $f \in K(n)$  и  $S$  — любая схема, реализующая  $f$ . Тогда  $P(S) \geq 5\varepsilon(1 - \varepsilon)^4$  при  $\varepsilon \in (0, 1/960]$ .

Из теорем 2 и 3 следует, что в любом из полных базисов  $B$ , таких, что  $B \subset \Psi_1$ ,  $B \subset \Psi_2$ ,  $B \subset \Psi_1^*$ ,  $B \subset \Psi_2^*$ , для почти всех функций асимптотически оптимальные по надёжности схемы функционируют с ненадёжностью, асимптотически равной  $5\varepsilon$  при  $\varepsilon \rightarrow 0$ . Следовательно, коэффициент ненадёжности базисов  $B$ , удовлетворяющих условию  $B \subseteq \Psi_1$ , или  $B \subseteq \Psi_2$ , или  $B \subseteq \Psi_1^*$ , или  $B \subseteq \Psi_2^*$ , равен 5.

Таким образом, если учесть теоремы 2 и 3 и добавить теорему С. И. Аксенова из работы [3], то получим теорему 4.

**Теорема 4.** Коэффициент ненадёжности полного базиса  $B$  равен 5 тогда и только тогда, когда  $B \subset \Psi_1$ , или  $B \subset \Psi_2$ , или  $B \subset \Psi_1^*$ , или  $B \subset \Psi_2^*$ .

#### ЛИТЕРАТУРА

1. *Лупанов О. Б.* Асимптотические оценки сложности управляющих систем. М.: Изд-во МГУ, 1984.
2. *Васин А. В.* Асимптотически оптимальные по надёжности схемы в полных базисах из трехходовых элементов: дис. . . . канд. физ.-мат. наук. Пенза, 2010. 100 с.
3. *Аксенов С. И.* О надёжности схем в широком классе полных базисов // Материалы IX Междунар. семинара «Дискретная математика и её приложения», посвящённого 75-летию со дня рождения акад. О. Б. Лупанова (Москва, МГУ, 18–23 июня 2007 г.) / под ред. О. М. Касим-Заде. М.: Изд-во механико-математического факультета МГУ, 2007. С. 55–56.
4. *Аксенов С. И.* О надёжности схем над произвольной полной системой функций при инверсных неисправностях на выходах элементов // Изв. вузов. Поволжский регион. Естественные науки. 2005. № 6(21). С. 42–55.
5. *Алехина М. А., Васин А. В.* О надёжности схем в базисах, содержащих функции не более чем трёх переменных // Ученые записки Казанского государственного университета. Сер. Физико-математические науки. 2009. Т. 151. Кн. 2. С. 25–35.

## Секция 7

## ПРИКЛАДНАЯ ТЕОРИЯ КОДИРОВАНИЯ

УДК 004.627 : 004.932.2

ГИБРИДНЫЙ АЛГОРИТМ СЖАТИЯ  
ДИСКРЕТНО-ТОНОВОЙ ГРАФИКИ

Д. В. Дружинин

Представлен гибридный алгоритм — быстрый алгоритм сжатия без потерь информации, предназначенный для обработки изображений с резкими цветовыми переходами (дискретно-тоновых изображений). Гибридный алгоритм является соединением двух алгоритмов: специальной реализации RLE, способной выявлять как вертикальную, так и горизонтальную избыточность, и сдвигового алгоритма, который относится к семейству словарных методов сжатия. Сдвиговой алгоритм осуществляет замену трёх байтов, кодирующих цвет пикселя, на однобайтовую ссылку на пиксель с таким же цветом, встречавшимся ранее. Представленная реализация RLE способна выявлять области пикселей одного цвета трёх типов: вертикальные, горизонтальные линии и прямоугольники. Рассмотрены комбинированные алгоритмы, предполагающие последовательное выполнение гибридного алгоритма и некоторых известных алгоритмов сжатия. При этом каждый из результирующих наборов данных гибридного алгоритма обладает специфическим типом избыточности и поэтому сжимается по отдельности на втором этапе выполнения комбинированного алгоритма. Проводится практическое сравнение комбинированных алгоритмов между собой, а также с известными алгоритмами. Как показало тестирование, комбинированный алгоритм, основанный на гибридном алгоритме и `zlib`, позволяет значительно увеличить степень сжатия дискретно-тоновых изображений при приемлемых временных затратах.

**Ключевые слова:** *быстрые алгоритмы сжатия, сжатие без потерь, дискретно-тоновая графика.*

В соответствии с классификацией, приведённой в [1], выделяют, в частности, следующие классы изображений:

1. Цветное изображение с непрерывным тоном. Этот тип изображений может иметь много похожих цветов, причём цвета обычно сменяются плавно, без резких переходов. Изображения с непрерывным тоном являются природными (естественными). Обычно они получаются при съёмке на цифровую фотокамеру или при сканировании фотографий.

2. Цветное дискретно-тоновое (синтетическое) изображение. Обычно это изображение получается искусственным путём. В нём нет шумов и пятен естественного происхождения. Примерами таких изображений могут служить фотографии искусственных объектов, страницы текста, карты, рисунки. Искусственные объекты имеют чёткую форму, хорошо определяемые границы, контрастируют на фоне остальной части изображения. Дискретно-тоновые изображения в значительной мере отличаются от непрерывно-тоновых, поэтому требуются специальные алгоритмы для их сжатия.

При сжатии дискретно-тоновых изображений даже небольшой процент потерь может привести к значительному визуальному ухудшению качества изображения [1, с. 120].

Последняя версия гибридного алгоритма, о которой в этой работе идёт речь, подробно описана в [2]. Гибридный алгоритм является соединением двух алгоритмов: RLE и сдвигового.

**RLE.** В качестве составной части гибридного алгоритма используется специально разработанная реализация RLE, способная выявлять области пикселей одного цвета трёх типов: вертикальные, горизонтальные линии и прямоугольники. На каждом шаге происходит подсчёт количества подряд идущих одинаковых пикселей в трёх направлениях: вправо от текущего пикселя, вниз от текущего пикселя, а также в прямоугольнике, левым верхним углом которого является текущий пиксель. Затем для кодирования выбирается то направление, в котором было найдено максимальное количество одинаковых пикселей.

При кодировании и декодировании используется вспомогательная структура данных, которая представляет собой массив флагов, где один флаг соответствует одному пикселю исходного изображения. Если флаг равен 0, соответствующий ему пиксель ещё не был закодирован, иначе уже закодирован. Уже закодированные пиксели просто пропускаются при кодировании.

При этом возможна следующая ситуация: пиксель  $p[i]$  уже был закодирован ранее, попав в вертикальную или прямоугольную группу пикселей одинакового цвета. Пусть текущий пиксель — это  $p[i - 1]$ . Допустим также, что пиксель  $p[i + 1]$  имеет такой же цвет, как  $p[i - 1]$ . В этом случае  $p[i - 1]$  и  $p[i + 1]$  могут быть закодированы как горизонтальная группа пикселей.

**Сдвиговой алгоритм.** Идея алгоритма: если при прямом обходе пикселей изображения незадолго до текущего пикселя встречался пиксель такого же цвета, то три байта, кодирующие цвет пикселя, можно заменить на однобайтовую ссылку на пиксель с таким же цветом, а точнее — указать, на сколько пикселей нужно сдвинуться назад относительно текущего пикселя остаточного изображения, чтобы получить нужный цвет. Таким образом, может быть выстроено множество списков. Для ускорения работы алгоритма как при кодировании, так и при декодировании используется хэш-таблица. При кодировании ключом хэш-таблицы является цвет, а значением — номер последнего просмотренного пикселя с таким цветом в остаточном изображении. При декодировании ключом хэш-таблицы является номер последнего просмотренного пикселя с таким цветом в остаточном изображении, а значением — цвет. Алгоритм относится к группе словарных методов.

**Гибридный алгоритм.** На каждом шаге алгоритма кодирование выполняется в две стадии:

1. Выполняется часть алгоритма, основанная на сдвиговом алгоритме, то есть определяется, можно ли заменить 3 байта цвета пикселя на 1 байт ссылки.
2. Выполняется часть алгоритма, основанная на RLE. На этой стадии определяется, можно ли выявить группу пикселей одного цвета.

На выходе гибридного алгоритма получается 3 массива:

1. Массив флагов. В этом массиве избыточность данных минимальна, так как данные имеют однобитовую природу.
2. Массив сдвигов и количеств. В этом массиве также содержатся различные служебные данные (кроме флагов), используемые гибридным алгоритмом. Все данные, попадающие в этот массив, имеют однобайтовую природу. Данные в этом массиве имеют бóльшую избыточность по сравнению с массивом флагов. Действительно, для

дискретно-тонового изображения оказывается, что различные значения таких параметров, как количество подряд идущих пикселей одного цвета, а также расстояние до ближайшего встреченного пикселя такого же цвета, не являются равновероятными, то есть такие данные имеют статистическую избыточность.

3. Массив пикселей. Будем называть этот массив остаточным изображением. Это те пиксели исходного изображения, которые не были заменены в ходе кодирования гибридным алгоритмом некоторыми служебными данными. Как правило, статистическая избыточность в этом массиве невысока. Зато в этих данных присутствует некоторая пространственная избыточность. Часто в остаточном изображении можно увидеть группы подряд идущих пикселей по вертикали или горизонтали близких цветов. Такой тип пространственной избыточности характерен для остаточного изображения, так как гибридный алгоритм не может его устранить.

Каждый из результирующих наборов данных гибридного алгоритма обладает специфическим типом избыточности и поэтому сжимается по отдельности на втором этапе выполнения комбинированного алгоритма. Создано два комбинированных алгоритма, использующих гибридный алгоритм на первом этапе сжатия. При тестировании комбинированный алгоритм, использующий на втором этапе библиотеку `zlib` [3], продемонстрировал более высокую степень сжатия. В тестировании принимали участие реализации 14 алгоритмов, некоторые из них с различными настройками. Тестирование проводилось на двух наборах данных: изображениях с преобладанием текста и с преобладанием деловой графики. Комбинированный алгоритм, основанный на гибридном алгоритме и `zlib`, обеспечил наивысшую степень сжатия на обоих тестовых наборах данных, превзойдя по этому показателю следующий за ним `zlib` с уровнем сжатия 9 на 9,5 % при сжатии изображений с преобладанием деловой графики и на 4 % — изображений с преобладанием текста. При этом комбинированный алгоритм, использующий на втором этапе `zlib`, производит сжатие быстрее, чем `zlib` уровня 9, в обоих случаях.

#### ЛИТЕРАТУРА

1. Сэломон Д. Сжатие данных, изображений и звука. М.: Техносфера, 2006. 365 с.
2. Дружинин Д. В. Комбинированный алгоритм сжатия ключевых кадров экранного видео // Вестник Томского государственного университета. Управление, вычислительная техника и информатика. 2011. № 3(16). С. 67–77.
3. `zlib` [Электронный ресурс]. <http://zlib.net>

УДК 519.212.2

### ВЕРОЯТНОСТНЫЕ ХАРАКТЕРИСТИКИ ВЕСОВЫХ СПЕКТРОВ СЛУЧАЙНЫХ ЛИНЕЙНЫХ ПОДКОДОВ НАД $GF(p)$

А. М. Зубков, В. И. Круглов

Получены формулы для первых двух моментов элементов весового спектра равновероятно выбранного линейного подкода фиксированного линейного кода над конечным полем  $F_p$  в терминах его весового спектра, а также оценки для распределения минимального веса ненулевого кодового слова в выбранном подкоде. Выведены формулы для распределения веса суммы двух независимых случайных векторов над  $F_p$  с заданными весами, вычислены математическое ожидание и дисперсия этого распределения.

**Ключевые слова:** *линейные коды, случайные подкоды, весовой спектр, слово минимального веса.*

Пусть  $p$  — фиксированное простое число. Будем обозначать через  $F_p^N = \{X = (x_1, \dots, x_N) : x_1, \dots, x_N \in F_p\}$  линейное  $N$ -мерное пространство над простым полем  $F_p$ . Любое  $k$ -мерное ( $k < N$ ) подпространство  $L \subset F_p^N$  будем называть  $k$ -мерным линейным кодом.

Весом вектора  $X = (x_1, \dots, x_N) \in F_p^N$  назовём число  $w(X) = \sum_{k=1}^N I\{x_k \neq 0\}$  его ненулевых координат.

Через  $(F_p^N)_s$  и  $(F_p^N)_{\leq s}$  будем обозначать соответственно множество векторов фиксированного веса  $s$  и множество ненулевых векторов веса, не превосходящего  $s$ , в  $F_p^N$ :

$$(F_p^N)_s = \{X \in F_p^N : w(X) = s\}, \quad (F_p^N)_{\leq s} = \{X \in F_p^N : 0 < w(X) \leq s\};$$

тогда  $F_p^N = \bigsqcup_{s=0}^N (F_p^N)_s$ .

**Определение 1.** Пусть  $v_s(L) = |L \cap (F_p^N)_s|$  и  $v_{\leq s}(L) = |L \cap (F_p^N)_{\leq s}|$  — количество соответственно векторов веса  $s$  и ненулевых векторов веса не больше  $s$  в линейном коде  $L$ ; набор  $\{v_s(L)\}_{s=0}^N$  называют *весовым спектром* кода  $L$ .

Предельные пуассоновские теоремы для случайных величин  $v_s(L)$  и аналогичных им доказаны в [1, 2].

Зафиксируем некоторый  $k$ -мерный линейный код  $L$  и рассмотрим  $k^*$ -мерный случайный код  $L^*$ , выбранный случайно и равновероятно из множества всех  $k^*$ -мерных подкодов кода  $L$ . Пусть  $\{v_s(L^*)\}_{s=0}^N$  — весовой спектр выбранного случайного кода  $L^*$ .

**Теорема 1.** Если  $L \subset F_p^N$  — линейный  $k$ -мерный код в  $F_p^N$  с весовым спектром  $\{v_s = v_s(L)\}_{s=0}^N$ , а  $L^*$  — случайный равновероятный  $k^*$ -мерный подкод  $L$ ,  $1 \leq k^* < k$ , то при  $s = 1, \dots, N$

$$\begin{aligned} \mathbf{E}v_s(L^*) &= v_s(L) \frac{p^{k^*} - 1}{p^k - 1}, \\ \mathbf{D}v_s(L^*) &= v_s(L) \frac{(p^{k^*} - 1)(p^k - p^{k^*})(p - 1)}{(p^k - 1)^2} \left( 1 - \frac{v_s(L) - (p - 1)}{p^k - p} \right) \end{aligned}$$

и при  $s, t \in \{1, \dots, N\}$ ,  $s \neq t$ ,

$$\text{cov}(v_s(L^*), v_t(L^*)) = -v_s(L)v_t(L) \frac{(p^{k^*} - 1)(p^k - p^{k^*})(p - 1)}{(p^k - 1)^2(p^k - p)}.$$

Если  $L = F_p^N$ , т. е.  $1 \leq k^* < k = N$ , то, согласно теореме 1,

$$\begin{aligned} \mathbf{E}v_s(L^*) &= v_s(F_p^N) \frac{p^{k^*} - 1}{p^N - 1}, \quad \text{где} \quad v_s(F_p^N) = C_N^s (p - 1)^s, \\ \mathbf{D}v_s(L^*) &= v_s(F_p^N) \frac{(p^{k^*} - 1)(p^N - p^{k^*})(p - 1)}{(p^N - 1)^2} \left( 1 - \frac{v_s(F_p^N) - (p - 1)}{p^N - p} \right). \end{aligned}$$

Вероятностные характеристики элементов весового спектра случайно выбранного линейного кода  $L^*$ , содержащего  $p^{k^*} - 1$  ненулевых векторов, заметно отличаются от аналогичных характеристик элементов весового спектра случайного множества  $M$ ,

выбранного равновероятно из совокупности  $(p^{k^*} - 1)$ -элементных подмножеств множества  $F_p^N$ . Математические ожидания элементов весового спектра совпадают:

$$\mathbf{E}v_s(M) = v_s(F_p^N) \frac{p^{k^*} - 1}{p^N - 1} = \mathbf{E}v_s(L^*),$$

а отношение дисперсий

$$\frac{\mathbf{D}v_s(M)}{\mathbf{D}v_s(L^*)} = \frac{1}{p-1} \left( 1 + \frac{p^{k^*}}{p^N - p^{k^*}} \right) \frac{1 - \frac{p^{k^*} - 2}{p^N - 2} - v_s(F_p^N) \frac{p^N - p^{k^*}}{(p^N - 1)(p^N - 2)}}{1 - \frac{v_s(F_p^N) - (p-1)}{p^N - p}}$$

заметно меньше 1 (более того, меньше  $1/(p-1)$ ) при  $p \geq 3$ .

**Теорема 2.** Если выполнены условия теоремы 1, то

$$\mathbf{E}v_{\leq s}(L^*) = \frac{p^{k^*} - 1}{p^k - 1} v_{\leq s}(L),$$

$$\mathbf{D}v_{\leq s}(L^*) = \frac{(p^{k^*} - 1)(p^k - p^{k^*})(p-1)}{(p^k - 1)^2} \frac{p^k - 1 - v_{\leq s}(L)}{p^k - p} v_{\leq s}(L) \leq (p-1) \frac{p^k - p^{k^*}}{p^k - 1} \mathbf{E}v_{\leq s}(L^*)$$

и для минимального веса  $\mu(L^*) = \min\{w(X) : X \in L^* \setminus \{0\}\}$  ненулевых векторов в  $L^*$  справедлива оценка

$$\frac{1}{1 + \frac{p^k - p^{k^*}}{p^k - 1} (p-1)(\mathbf{E}v_{\leq s}(L^*))^{-1}} \leq \mathbf{P}\{\mu(L^*) \leq s\} \leq \mathbf{E}v_{\leq s}(L^*).$$

**Теорема 3.** Если  $X$  и  $Y$  — независимые случайные векторы, причём вектор  $X$  имеет равномерное распределение на множестве  $(F_p^N)_s$  всех векторов веса  $s$ , а вектор  $Y$  имеет равномерное распределение на множестве  $(F_p^N)_t$  всех векторов веса  $t$ , то при  $|s - t| \leq m \leq \min\{s + t, N\}$

$$\mathbf{P}\{w(X + Y) = m\} = \sum_{j=\max\{0, s+t-N\}}^s \frac{C_s^j C_{N-s}^{t-j}}{C_N^t} C_j^{m-(s+t-2j)} \frac{(p-2)^{m-(s+t-2j)}}{(p-1)^j},$$

$$\mathbf{E}w(X + Y) = s + t - \frac{p}{p-1} \frac{st}{N},$$

$$\mathbf{D}w(X + Y) = \frac{st}{N} \left( \frac{p^2}{(p-1)^2} \frac{N}{N-1} \left( 1 - \frac{t}{N} \right) \left( 1 - \frac{s}{N} \right) + \frac{p-2}{(p-1)^2} \right).$$

Доказательства теорем 1–3 опубликованы в [3]; перечисленные результаты могут применяться при исследовании системы шифрования Мак-Элис [4, 5].

#### ЛИТЕРАТУРА

1. Копытцев В. А., Михайлов В. Г. Теоремы пуассоновского типа для числа специальных решений случайного линейного включения // Дискретная математика. 2010. Т. 22. Вып. 2. С. 3–21.
2. Михайлов В. Г. Предельные теоремы для числа решений системы случайных линейных уравнений, попавших в заданное множество // Дискретная математика. 2007. Т. 19. Вып. 1. С. 17–26.

3. *Зубков А. М., Круглов В. И.* Статистические характеристики весовых спектров случайных линейных кодов над  $\text{GF}(p)$  // Математические вопросы криптографии. 2014. Т. 5. Вып. 1. С. 27–38.
4. *Berson T.* Failure of the McEliece public-key cryptosystem under message-resend and related-message attack // LNCS. 1997. V. 1294. P. 213–220.
5. *McEliece R. J.* A public-key cryptosystem based on algebraic coding theory. Jet Propulsion Lab. DSN Progress Report 42–44, 1978.

Секция 8

ПРИКЛАДНАЯ ТЕОРИЯ ГРАФОВ

УДК 51-76

О ЦИКЛАХ ГРАФОВ ФУНКЦИОНИРОВАНИЯ ГЕННЫХ СЕТЕЙ ЦИРКУЛЯНТНОГО ТИПА С ПОРОГОВЫМИ ФУНКЦИЯМИ

И. С. Быков

Рассматривается функционирование генных сетей циркулянтного типа с пороговыми функциями при значении параметра  $p = 2$ . Проведена классификация всех состояний системы в зависимости от длин серий нулей и единиц. Установлено, что все циклы графа функционирования делятся на два типа: состоящие только из состояний с длинными сериями и состоящие только из состояний с короткими сериями. Получена оценка на количество циклов в графе функционирования. Описана конструкция для построения циклов из состояний с короткими сериями.

**Ключевые слова:** *генные сети, пороговые функции, граф функционирования, циклы графа функционирования, состояния с длинными сериями, состояния с короткими сериями.*

В работе рассматривается функционирование дискретных моделей генных сетей [1]. Как и в [2], рассматриваются пороговые функции в вершинах с произвольным пороговым значением  $T$ .

Состоянием генной сети назовём кортеж  $(s_0, s_1, \dots, s_{n-1})$ , где  $s_i \in \{0, 1, \dots, p - 1\}$ . Функционированием такой системы будем называть последовательное изменение состояний

$$S, A(S), A^2(S), A^3(S), \dots,$$

где  $S$  — некоторое состояние;  $A$  — отображение, действующее на множестве всех состояний.

Отображение  $A$  задается пороговой функцией с двумя параметрами  $k$  и  $T$  следующим образом: пусть  $S = (s_0, s_1, \dots, s_{n-1})$ , тогда  $A(S) = (s'_0, s'_1, \dots, s'_{n-1})$ , где

$$s'_i = \begin{cases} s_i + 1, & \text{если } \sum_{j=1}^k s_{i+j} < T \text{ и } s_i < p - 1, \\ s_i - 1, & \text{если } \sum_{j=1}^k s_{i+j} \geq T \text{ и } s_i > 0, \\ s_i & \text{иначе.} \end{cases}$$

Здесь и далее операции в индексах выполняются по модулю  $n$ .

В работе рассматривается функционирование системы при  $p = 2$ . В этом случае

$$s'_i = \begin{cases} 0, & \text{если } \sum_{j=1}^k s_{i+j} \geq T, \\ 1 & \text{иначе.} \end{cases}$$

Графом функционирования называют ориентированный граф  $G(V, D)$ , где  $V$  — множество всех состояний;  $D = \{(S_1, S_2) : S_1, S_2 \in V; A(S_1) = S_2\}$ .

Задачей анализа функционирования называется задача описания качественных характеристик графа функционирования по заданным параметрам  $n, k, T$ .

Одной из таких задач является изучение свойств состояний, входящих в циклы графа функционирования. Рассматривая полученные свойства, можно получать оценки на количество циклов (компонент связности) графа функционирования, а также перечислять некоторые из циклов.

Выделим среди множества всех состояний два подмножества: состояния с длинными сериями и состояния с короткими сериями.

### 1. Состояния с длинными сериями

**Определение 1.** Состояние  $S$  будем называть *состоянием с длинными сериями*, если длина каждой серии из нулей не меньше  $k - T + 1$ , а длина каждой серии из единиц не меньше  $T$ .

**Теорема 1.** Любое состояние с длинными сериями лежит в цикле графа функционирования. Все состояния этого цикла также являются состояниями с длинными сериями.

В силу теоремы 1, подсчитав количество состояний с длинными сериями, можно получить, например, следующую оценку на количество циклов в графе функционирования.

**Теорема 2.** Количество циклов в графе функционирования системы с параметрами  $n, k, T$  не менее

$$1 + \sum_{i=1}^{\lfloor \frac{n}{k+1} \rfloor} \tilde{P}(n - (k - 1)i, 2i),$$

где  $\tilde{P}(a, b)$  — число циклических разбиений  $a$  на  $b$  слагаемых.

### 2. Состояния с короткими сериями

**Определение 2.** Состояние  $S$  будем называть *состоянием с короткими сериями*, если длина каждой серии из нулей не больше  $k - T$ , а длина каждой серии из единиц не больше  $T - 1$ .

**Теорема 3.** Если состояние лежит в цикле графа функционирования, то оно является либо состоянием с длинными сериями, либо состоянием с короткими сериями.

Обозначим вес состояния (количество ненулевых компонент) как  $W(S)$ .

Состояния с короткими сериями в системах с большими параметрами можно строить из подходящих систем с меньшими параметрами, используя одну из следующих двух конструкций.

**Теорема 4.** Пусть имеется  $q$  систем,  $S_i$  — состояние с длинными сериями в системе с параметрами  $n_i, k_i, T_i$  и отображением  $A_i$ . Тогда если для некоторых  $k$  и  $T$  и любого  $0 \leq j \leq q - 1$  выполняются условия

$$k = k_j + \sum_{i=0}^{q-1} n_i - n_j, \quad T = T_j + \sum_{i=0}^{q-1} W(S_i) - W(S_j), \quad W(S) = W(A_j(S_j)),$$

то состояние  $S = S_0 S_1 \dots S_{q-1}$  лежит в цикле графа функционирования системы с параметрами

$$n = \sum_{i=0}^{q-1} n_i, \quad k = k_0 + \sum_{i=0}^{q-1} n_i - n_0, \quad T = T_0 + \sum_{i=0}^{q-1} W(S_i) - W(S_0)$$

и является состоянием с короткими сериями.

**Теорема 5.** Пусть состояние  $S'$  лежит в цикле графа функционирования системы с параметрами  $n'$ ,  $k'$ ,  $T'$  и отображением  $A'$  и выполнено условие  $W(S) = W(A'(S'))$ . Тогда состояние

$$S = \underbrace{S' S' \dots S' S'}_m$$

лежит в цикле графа функционирования системы с параметрами

$$n = mn', \quad k = k' + ln', \quad T = T' + lW(S')$$

и является состоянием с короткими сериями для всех  $0 < l < m$ .

#### ЛИТЕРАТУРА

1. Евдокимов А. А., Лиховидова Е. О. Дискретная модель генной сети циркулянтного типа с пороговыми функциями // Вестник Томского государственного университета. 2008. № 2. С. 18–21.
2. Быков И. С. Функционирование дискретных моделей генных сетей циркулянтного типа с пороговыми функциями // Материалы IX молодежной научн. школы по дискретной математике и её приложениям. МГУ, 2013. С. 26–31.

УДК 519.17

### АЛГОРИТМ ПОСТРОЕНИЯ Т-НЕПРИВОДИМОГО РАСШИРЕНИЯ ДЛЯ МНОГОУГОЛЬНЫХ ОРГРАФОВ

А. В. Гавриков

Предложен полиномиальный алгоритм построения одного из Т-неприводимых расширений для многоугольного орграфа. Приведено доказательство корректности алгоритма.

**Ключевые слова:** многоугольный орграф, отказоустойчивость дискретных систем, Т-неприводимое расширение.

Под *ориентированным графом* (или *орграфом*) понимается пара  $G = (V, \alpha)$ , где  $V$  — конечное непустое множество вершин;  $\alpha$  — отношение на множестве  $V$  (дуги орграфа). *Вложение* орграфа  $G = (V, \alpha)$  в орграф  $H = (W, \beta)$  — это взаимно однозначное отображение  $\varphi : V \rightarrow W$ , такое, что  $(\forall u, v \in V)((u, v) \in \alpha \Rightarrow (\varphi(u), \varphi(v)) \in \beta)$ . При этом говорят, что орграф  $G$  вкладывается в орграф  $H$ . *Расширение* орграфа  $G = (V, \alpha)$  — это орграф  $H = (W, \beta)$ , где  $|W| = |V| + 1$ , такой, что орграф  $G$  вкладывается в каждый максимальный подграф орграфа  $H$  [1]. *Тривиальное расширение* (ТР) орграфа  $G$  — это соединение  $G + w$  орграфа  $G$  с вершиной  $w$ , обозначается через  $\text{ТР}(G)$ . *Т-неприводимое расширение* (ТНР) орграфа  $G$  — это расширение орграфа  $G$ , полученное удалением максимального множества дуг из  $\text{ТР}(G)$  [2].

Ориентированные графы представляют собой математические модели дискретных систем [3]. Вопросы отказоустойчивости на данный момент сформулированы в терминах теории графов [3, 4]. Конструкции оптимальных расширений, которыми являются

T-неприводимые расширения, широко применяются в диагностике дискретных систем и криптографии [5].

В общем случае задача определения того, является ли оргграф  $H$  расширением для оргграфа  $G$ , является NP-полной, а задача поиска ТНР по заданному оргграфу  $G$  не принадлежит классу NP [6].

Контур в оргграфе — это простой циклический путь. Контур, состоящий из  $n$  вершин, обозначим через  $C_n = v_0v_1 \dots v_{n-1}v_0$ , считая  $v_0$  выбранной начальной вершиной. Многоугольным оргграфом порядка  $n$  называется всякий оргграф  $M$ , полученный переориентацией некоторых дуг контура  $C_n$  [7]. Далее все арифметические операции над индексами вершин в многоугольных оргграфах будем производить по модулю  $n$ .

Следующий алгоритм строит одно из ТНР для многоугольного оргграфа.

**Алгоритм**

Дан многоугольный оргграф  $M = (Z, \gamma)$ . Построим его ТНР следующим образом:

1. Добавим к  $M$  вершину  $w$ .
2. Для каждой вершины  $v \in Z$  добавим дуги следующим образом:
  - если  $v \in Z$  является источником, то добавим дугу  $(v, w)$ ;
  - если  $v \in Z$  является стоком, то добавим дугу  $(w, v)$ ;
  - если  $v \in Z$  такова, что  $d^+(v) = 1$  и  $d^-(v) = 1$ , то добавим дуги  $(v, w)$  и  $(w, v)$ .

Обозначим построенный оргграф  $H_0 = (W, \beta_0)$ . Положим  $k = 0$ .

3. Рассматриваем вершины многоугольного оргграфа  $M$ , имеющие степени исхода и захода 1, в порядке возрастания их индексов.

Пусть, для определённости, вершины пронумерованы таким образом, что для вершины  $v_i \in Z$ , имеющей степени исхода и захода 1, существуют  $v_{i-1}, v_{i+1} \in Z$ , такие, что  $(v_{i-1}, v_i), (v_i, v_{i+1}) \in \gamma$ . По построению в п. 2 алгоритма вершина  $v_i$  соединена с вершиной  $w$  дугами  $(v_i, w)$  и  $(w, v_i)$  (рис. 1). Пунктирная линия на рис. 1, соединяющая две вершины, означает, что между ними может быть как одна дуга в любом из направлений, так и две дуги, если одна из инцидентных вершин является вершиной  $w$ . Возможны следующие случаи:

С л у ч а й А: многоугольный оргграф  $M$  вкладывается в оргграф  $H_k - v_{i-1} - (w, v_i)$ . Строим оргграф  $H_{k+1} = (W, \beta_{k+1})$ , такой, что  $H_{k+1} = H_k - (w, v_i)$ ,  $\beta_{k+1} = \beta_k - (w, v_i)$ . Далее алгоритм продолжает работу с оргграфом  $H_{k+1}$ , переходим к следующей вершине в п. 3.

С л у ч а й В: многоугольный оргграф  $M$  вкладывается в оргграф  $H_k - v_{i+1} - (v_i, w)$ . Строим оргграф  $H_{k+1} = (W, \beta_{k+1})$ , такой, что  $H_{k+1} = H_k - (v_i, w)$ ,  $\beta_{k+1} = \beta_k - (v_i, w)$ . Далее алгоритм продолжает работу с оргграфом  $H_{k+1}$ , переходим к следующей вершине в п. 3.

С л у ч а й С: оргграф  $M$  не вкладывается ни в оргграф  $H_k - v_{i-1} - (w, v_i)$ , ни в оргграф  $H_k - v_{i+1} - (v_i, w)$ . Не производим никаких действий, переходим к следующей вершине в п. 3.

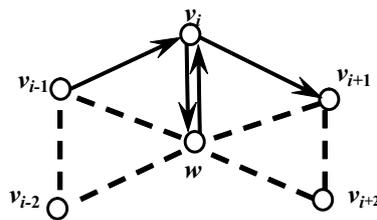


Рис. 1. Иллюстрация п. 3 алгоритма

Уточнение: если в многоугольном орграфе  $M$  каждая вершина является либо источником, либо стоком, то п. 3 алгоритма пропускается.

После того как все вершины в п. 3 рассмотрены, алгоритм завершает свою работу. Построенный из орграфа  $H_0$  оргграф  $H_k$ , где  $k$  — количество дуг, удалённых в п. 3 алгоритма, является ТНР для многоугольного орграфа  $M$ .

Асимптотическая сложность алгоритма составляет  $O(n^3)$ , где  $n = |Z|$  — количество вершин в многоугольном орграфе  $M$ .

Доказана теорема о корректности предложенного алгоритма. Алгоритм позволяет также получить верхние и нижние оценки количества добавленных дуг в ТНР для многоугольных оргграфов.

#### ЛИТЕРАТУРА

1. Богомолов А. М., Салий В. Н. Алгебраические основы теории дискретных систем. М.: Наука, Физматлит, 1997. 326 с.
2. Курносова С. Г. Т-неприводимые расширения для некоторых классов графов // Теоретические проблемы информатики и её приложений: сб. науч. тр. / под ред. проф. А. А. Сытника. Саратов: Изд-во Саратов. ун-та, 2004. С. 113–125.
3. Hayes J. P. A graph model for fault-tolerant computing systems // IEEE Trans. Comput. 1976. V. C-26. No. 9. P. 875–884.
4. Абросимов М. Б. Некоторые вопросы о минимальных расширениях графов // Известия Саратовского университета. Сер. Математика. Механика. Информатика. 2006. Т. 6. Вып. 1/2. С. 86–91.
5. Салий В. Н. Доказательства с нулевым разглашением в задачах о расширениях графов // Вестник Томского государственного университета. Приложение. 2003. № 6. С. 63–65.
6. Абросимов М. Б. О сложности некоторых задач, связанных с расширениями графов // Матем. заметки. 2010. Т. 88. № 5. С. 643–650.
7. Салий В. Н. Упорядоченное множество связанных частей многоугольного графа // Известия Саратовского университета. 2013. Т. 13. Вып. 2. С. 44–51.

УДК 519.1

### ОБ АТТРАКТОРАХ В КОНЕЧНЫХ ДИНАМИЧЕСКИХ СИСТЕМАХ ДВОИЧНЫХ ВЕКТОРОВ, АССОЦИИРОВАННЫХ С ОРИЕНТАЦИЯМИ ПАЛЬМ

А. В. Жаркова

Описываются аттракторы в конечных динамических системах двоичных векторов, ассоциированных с ориентациями пальм, определяется свойство принадлежности состояния аттрактору. Состояниями динамической системы являются все возможные ориентации данной пальмы, а эволюционная функция у данной ориентации пальмы переориентирует все дуги, входящие в стоки.

**Ключевые слова:** аттрактор, двоичный вектор, конечная динамическая система, пальма, сверхстройное (звездообразное) дерево.

Под *конечной динамической системой* понимается пара  $(S, \delta)$ , где  $S$  — конечное непустое множество, элементы которого называются *состояниями системы*,  $\delta : S \rightarrow S$  — отображение множества состояний в себя, называемое *эволюционной функцией системы*. Каждой конечной динамической системе сопоставляется карта, представляющая собой оргграф с множеством вершин  $S$  и дугами, проведёнными 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. Контур, в свою очередь, называется предельными циклами, или *аттракторами*.

Основными проблемами теории конечных динамических систем являются задачи отыскания эволюционных параметров без проведения динамики. К их числу относятся свойство принадлежности состояния аттрактору и описание аттракторов системы (их количество, вид и длина). Автором составлены программы для ЭВМ, позволяющие вычислять различные параметры динамических систем двоичных векторов, ассоциированных с некоторыми типами графов, в частности [1].

Дерево называется *пальмой*, если оно является объединением цепей, имеющих общую концевую вершину, причём все эти цепи, за исключением, быть может, одной, имеют длину 1. Пальма является частным случаем *сверхстройного (звездообразного) дерева* (дерево, в котором в точности одна вершина имеет степень больше 2).

Пусть пальма  $p$  образована объединением цепей  $p_0, p_1, \dots, p_c$ , имеющих общую концевую вершину. Будем считать, что  $p_0$  имеет среди этих цепей максимальную длину  $s \geq 1$ . Назовём  $p_0$  *стволом пальмы*  $p$ , цепи  $p_1, p_2, \dots, p_c$ , имеющие длину 1, — её *листьями*, а их совокупность — *кроной*. Будем говорить, что  $p$  является пальмой типа  $(s, c)$ . Пальма с точностью до изоморфизма определяется своим типом. При  $c = 1$  пальма вырождается в цепь [2, 3], поэтому далее не будем рассматривать этот случай, считая  $c > 1$ .

Пусть имеется пальма  $p$  типа  $(s, c)$ ,  $s + c = n$ . Зафиксируем расположение её цепей и перенумеруем рёбра пальмы  $p$ , начиная от корня (начальной вершины ствола), двигаясь к кроне (рёбра с номерами от 1 по  $s$ ), а далее рёбра кроны слева направо (рёбра с номерами от  $s + 1$  по  $s + c$ ). Придадим каждому ребру пальмы произвольную ориентацию и сопоставим полученному ориентированному графу  $n$ -мерный двоичный вектор  $v(p)$ , полагая его  $i$ -ю компоненту равной 1, если  $i$ -е ребро пальмы  $p$  ориентировано от корня, и 0 — в противном случае. Теперь можно последовательно выписать получившуюся последовательность из нулей и единиц:  $v = v_1 \dots v_s \cdot v_{s+1} \dots v_{s+c}$ , где  $v_i$ ,  $0 < i \leq s + c$ , принимает значение 0 или 1 в зависимости от ориентации  $i$ -го ребра пальмы. Таким образом, каждой ориентации пальмы сопоставляется  $n$ -мерный двоичный вектор, причём  $n = s + c$ . В свою очередь, каждый такой вектор  $v$  однозначно определяет некоторую ориентацию пальмы  $p(v)$  типа  $(s, c)$ . Таким образом, между множеством  $P_{s+c}$ ,  $s > 0$ ,  $c > 1$ , всевозможных ориентированных пальм типа  $(s, c)$  указанного вида и множеством  $B^{s+c}$ ,  $s > 0$ ,  $c > 1$ , всех двоичных векторов размерности  $n = s + c$  устанавливается взаимно однозначное соответствие. В дальнейшем ориентации пальмы для простоты также будем называть пальмами.

Опишем конечную динамическую систему ориентаций  $(s, c)$ -пальмы  $p$  на языке двоичных векторов. Пусть состоянием динамической системы в данный момент времени является вектор  $v = v_1 \dots v_s \cdot v_{s+1} \dots v_{s+c} \in B^{s+c}$ . Тогда в следующий момент времени она окажется в состоянии  $\gamma(v) = v'$ , полученном путём одновременного применения следующих правил: I) если  $v_1 = 0$ , то  $v'_1 = 1$ ; II) если  $v_i = 1$  и  $v_{i+1} = 0$  для некоторого  $0 < i < s$ , то  $v'_i = 0$  и  $v'_{i+1} = 1$ ; III) если  $v_i = 1$  для некоторого  $s < i \leq s + c$ , то  $v'_i = 0$ ; IV) если  $v_s = 1$  и  $v_i = 0$  для всех  $s < i \leq s + c$ , то  $v'_s = 0$  и  $v'_i = 1$  для всех  $s < i \leq s + c$ ; V) других отличий между  $v$  и  $\gamma(v)$  нет.

Пусть теперь имеется  $n$ -рёберная  $(s, c)$ -пальма. На языке ориентаций пальм эволюция динамической системы вводится следующим образом: если дана некоторая ориентированная пальма  $p \in P_{s+c}$ , то её динамическим образом  $\gamma(p)$  является пальма,

получаемая из  $p$  одновременным превращением всех стоков в источники. Это частный случай динамики бесконтурных связных графов, введённой в [4]. Преобразования ориентаций палм в динамической системе  $(P_{s+c}, \gamma)$ ,  $s > 0$ ,  $c > 1$ , соответствуют эволюционным преобразованиям соотносимых им двоичных векторов в динамической системе  $(B^{s+c}, \gamma)$ ,  $s > 0$ ,  $c > 1$ , и обратно, а именно  $v(\gamma(p)) = \gamma(v(p))$  [5]. Таким образом, динамические системы  $(B^{s+c}, \gamma)$  и  $(P_{s+c}, \gamma)$ ,  $s > 0$ ,  $c > 1$ , изоморфны.

**Теорема 1.** Динамическая система  $(B^{s+c}, \gamma)$ ,  $s > 0$ ,  $c > 1$ , имеет единственный бассейн и аттрактор, представляющий собой двухэлементный контур, образуемый состояниями  $(01)^{(s-1)/2}01^c$  и  $(10)^{(s-1)/2}10^c$  при нечётном  $s$  и состояниями  $(01)^{s/2}0^c$  и  $(10)^{s/2}1^c$  при чётном  $s$ .

**Следствие 1.** В динамической системе  $(B^{s+c}, \gamma)$ ,  $s > 0$ ,  $c > 1$ , состояния  $(01)^{(s-1)/2}01^c$  и  $(10)^{(s-1)/2}10^c$  при нечётном  $s$  и состояния  $(01)^{s/2}0^c$  и  $(10)^{s/2}1^c$  при чётном  $s$ , и только они, принадлежат аттрактору.

#### ЛИТЕРАТУРА

1. Власова А. В. Исследование эволюционных параметров в динамических системах двоичных векторов // Свидетельство о гос. регистрации программы для ЭВМ № 2009614409, выданное Роспатентом. Зарегистрировано в Реестре программ для ЭВМ 20 августа 2009 г.
2. Саллий В. Н. Об одном классе конечных динамических систем // Вестник Томского государственного университета. Приложение. 2005. № 14. С. 23–26.
3. Власова А. В. Аттракторы в динамической системе  $(B, \delta)$  двоичных векторов // Компьютерные науки и информационные технологии: материалы научн. конф. Саратов: Изд-во Саратов. ун-та, 2010. С. 35–41.
4. Barbosa V. C. An Atlas of Edge-reversal Dynamics. Boca Raton: Chapman&Hall/CRC, 2001. 385 p.
5. Власова А. В. Динамические системы, определяемые пальмами // Компьютерные науки и информационные технологии: материалы Междунар. научн. конф. Саратов: Изд-во Саратов. ун-та, 2009. С. 57–60.

УДК 519.17

### ПОСТРОЕНИЕ РЕБЕРНОГО 1-РАСШИРЕНИЯ ДЛЯ СВЕРХСТРОЙНОГО ДЕРЕВА ПРОИЗВОЛЬНОГО ВИДА

Д. Д. Комаров

Минимальные рёберные расширения графов можно рассматривать как модель оптимальной рёберной отказоустойчивой реализации некоторой системы. Работа посвящена верхней оценке количества дополнительных рёбер минимального рёберного 1-расширения графов специального класса — сверхстройных деревьев. Приводится схема построения рёберного 1-расширения для сверхстройного дерева произвольного вида.

**Ключевые слова:** минимальные расширения графов, сверхстройное дерево, отказоустойчивость.

Для минимальных вершинных 1-расширений графов существуют хорошие верхние и нижние оценки для количества дополнительных рёбер. Так, например, тривиальное вершинное 1-расширение для произвольного графа может выступать в качестве верхней оценки. Для рёберных же расширений произвольного графа в качестве верхней оценки можно взять лишь полный граф, учитывая при этом, что в общем случае

не для всех графов существуют рёберные расширения. В [1] рассмотрены вопросы, связанные с нижней оценкой числа дополнительных рёбер минимального рёберного 1-расширения произвольного сверхстройного дерева. В данной работе рассматривается верхняя оценка.

*Графом (неориентированным)* называется пара  $G = (V, \alpha)$ , где  $V$  — конечное множество вершин, а  $\alpha$  — симметричное и антирефлексивное бинарное отношение на  $V$  (множество рёбер). Определения в основном даются по работе [2].

Назовём граф  $G^*$  *рёберным  $k$ -расширением* графа  $G$ , если граф  $G$  вложим в каждый граф, получающийся из  $G^*$  удалением любых его  $k$  рёбер.

Граф  $G^* = (V^*, \alpha^*)$  называется *минимальным рёберным  $k$ -расширением* графа  $G = (V, \alpha)$ , если выполняются следующие условия:

- 1) граф  $G^*$  является рёберным  $k$ -расширением  $G$ ;
- 2)  $|V^*| = |V|$ ;
- 3)  $\alpha^*$  имеет минимальную мощность при выполнении условий 1 и 2.

*Сверхстройным деревом* называется корневое дерево, где степень всех вершин, кроме корня, не превосходит 2, а степень корня более 2.

Будем задавать сверхстройное дерево с помощью вектора  $(a_1, \dots, a_s)$ , где  $a_i$  — количество цепей длины  $i$ , при этом  $s$  — длина максимальной цепи.

**Теорема 1.** Пусть граф  $G$  является объединением  $s$  ( $s > 2$ ) цепей длин  $m_1, \dots, m_s$  с общей концевой вершиной, и это сверхстройное дерево задаётся вектором  $(k, 0, a_3, \dots, a_t)$ ,  $k \neq 0$ . Тогда существует граф  $G^*$  — рёберное 1-расширение графа  $G$  с количеством дополнительных рёбер  $F$ , вычисляемым по формуле

$$F = k + \sum_{i=1}^s (m_i - 1).$$

**Теорема 2.** Пусть граф  $G$  является объединением  $s$  ( $s > 2$ ) цепей длин  $m_1, \dots, m_s$  с общей концевой вершиной и не все  $m_1, \dots, m_s$  равны 1. Назовём ребро цепи  $P_i$  проблемным, если при его удалении цепь  $P_i$  разбивается на две цепи длин  $k_i$  и  $l_i$  ( $k_i + l_i + 1 = m_i$ ), причём среди длин  $m_1, \dots, m_s$  нет ни  $k_i$ , ни  $l_i$ , и  $k_i \neq 0$ ,  $l_i \neq 0$ . Назовём началом проблемного ребра вершину, инцидентную этому ребру, находящуюся ближе к корневой вершине. Тогда граф  $G^*$ , построенный из графа  $G$  путём соединения каждой вершины степени 1 из цепи длины больше 1 со всеми вершинами степени 1 других цепей, корневой вершиной и началами всех проблемных рёбер цепи, которой принадлежит эта вершина, является рёберным 1-расширением графа  $G$  (рис. 1).

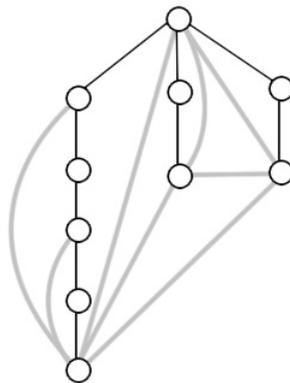


Рис. 1. Пример для схемы из теоремы 2

## ЛИТЕРАТУРА

1. *Абросимов М. Б.* О нижней оценке числа ребер минимального реберного 1-расширения сверхстройного дерева. // Изв. Саратов. ун-та. Нов. сер. 2011. Т. 11. Сер. Математика. Механика. Информатика. Вып. 3. Ч. 2. С. 111–117.
2. *Богомолов А. М., Салый В. Н.* Алгебраические основы теории дискретных систем. М.: Наука, 1997. 368 с.

УДК 519.6

ДОСТАТОЧНЫЕ УСЛОВИЯ ЛОКАЛЬНОЙ ПРИМИТИВНОСТИ  
НЕПРИМИТИВНЫХ ОРГРАФОВ

С. Н. Кяжин

В некоторых коммуникационных системах, моделируемых неотрицательными матрицами, важные свойства достигаются, если положительны определённые подматрицы степеней данной матрицы. В связи с этим известные понятия примитивности и экспонента матрицы (орграфа) обобщены до понятий локальной примитивности и локальных экспонентов матрицы (орграфа). Представлены достаточные условия локальной примитивности и оценки локальных экспонентов для непримитивных орграфов.

**Ключевые слова:** примитивная матрица, примитивный граф, локальная примитивность, локальный экспонент.

## Введение

Для объектов некоторых коммуникационных систем, моделируемых неотрицательными матрицами (орграфами), некоторые важные свойства достигаются, если положительны их подматрицы (подграфы являются полными). В связи с этим в [1] известные понятия примитивности и экспонента матрицы (орграфа) обобщены до понятий локальной примитивности и локальных экспонентов матрицы (орграфа).

Обозначим  $N_n = \{1, \dots, n\}$ , где  $n$  — натуральное число;  $I = \{i_1, \dots, i_k\}$ ,  $J = \{j_1, \dots, j_r\}$ ,  $\emptyset \neq I \subseteq N_n$ ,  $\emptyset \neq J \subseteq N_n$ . Пусть  $\Gamma$  есть  $n$ -вершинный орграф,  $A$  — матрица смежности вершин графа  $\Gamma$ ,  $A(I \times J)$  — её подматрица размера  $k \times r$ ,  $0 < k, r \leq n$ , полученная из  $A$  вычёркиванием строк с номерами  $i \notin I$  и столбцов с номерами  $j \notin J$ .

Матрица  $A$  называется  $I \times J$ -примитивной ( $i \times j$ -примитивной при  $I = \{i\}$ ,  $J = \{j\}$ ), если существует натуральное число  $\gamma$ , такое, что матрица  $A^t(I \times J)$  положительна при любом  $t \geq \gamma$ . Наименьшее такое число  $\gamma$  называется  $I \times J$ -экспонентом ( $i \times j$ -экспонентом при  $I = \{i\}$ ,  $J = \{j\}$ ) матрицы  $A$ , обозначается  $I \times J$ -exp  $A$  ( $i \times j$ -exp  $A$ ).

Орграф  $\Gamma$  называется  $I \times J$ -примитивным, если и только если матрица  $A$  является  $I \times J$ -примитивной, при этом соответствующие  $I \times J$ -экспоненты матрицы  $A$  и графа  $\Gamma$  равны. Некоторые условия  $I \times J$ -примитивности матриц (орграфов) получены в [1]. В работе развиваются и обобщаются результаты работы [1]. Приведены условия  $I \times J$ -примитивности матрицы (орграфа), не обязательно являющейся примитивной.

1. Достаточные условия  $I \times J$ -примитивности орграфов

Используем определения и обозначения работы [1]. Путь в  $\Gamma$  из  $i$  в  $j$ , проходящий через некоторые вершины множества  $Y$ , назовем  $Y$ -путём из  $i$  в  $j$ . Сильносвязный подграф  $\tilde{U}$  (множество его вершин обозначается  $U$ ) орграфа  $\Gamma$  назовём  $i, j$ -связываю-

щим, если в  $\Gamma$  существует  $U$ -путь из  $i$  в  $j$ . В частности, сильносвязный орграф есть  $i, j$ -связывающий орграф при любых  $i, j$ .

Связный циклический орграф  $\Gamma$  является  $I \times J$ -примитивным, если и только если он  $i \times j$ -примитивный для любой пары вершин  $(i, j) \in I \times J$ , при этом  $I \times J$ -exp  $\Gamma = \max_{(i,j) \in I \times J} i \times j$ -exp  $\Gamma$  [1], то есть достаточно получить условия  $i \times j$ -примитивности для связного циклического орграфа  $\Gamma$ .

При натуральном  $d$  множество натуральных чисел называется  $d$ -полным, если оно содержит полную систему вычетов по модулю  $d$ . Для  $d$ -полного множества  $M$  обозначим через  $q(M)$  такое наименьшее натуральное число, что для любого  $a \in \{q(M), q(M) + 1, \dots, q(M) + d - 1\}$  в  $M$  имеется число  $b$ , не превышающее  $a$  и  $b \equiv a \pmod{d}$ . В силу  $d$ -полноты множества  $M$  число  $q(M)$  существует и не превышает  $\max M$ .

Обозначим  $L(i, j)$  множество длин всех простых путей из  $i$  в  $j$ . Сумму  $R + R'$  множеств натуральных чисел  $R = \{r_1, r_2, \dots\}$  и  $R' = \{r'_1, r'_2, \dots\}$  определим как  $\{r_i + r'_j : i, j = 1, 2, \dots\}$ .

**Теорема 1.** Пусть в связном орграфе  $\Gamma$  имеется  $i, j$ -связывающий цикл  $\tilde{C}$  длины  $l$  и множество  $M_{i,j} = \bigcup_{\mu, \nu \in C} \{L(i, \mu) + L(\mu, \nu) + L(\nu, j)\}$  является  $l$ -полным. Тогда граф  $\Gamma$  является  $i \times j$ -примитивным и  $i \times j$ -exp  $\Gamma \leq q(M_{i,j})$ .

**Пример 1.** В 5-вершинном орграфе  $\Gamma_1$  (рис. 1) имеется 1,5-связывающий цикл  $\tilde{C} = (2, 3, 4)$  длины  $l = 3$ . Покажем  $1 \times 5$ -примитивность орграфа  $\Gamma_1$ .

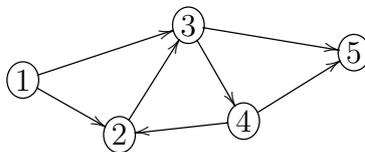


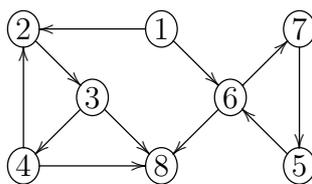
Рис. 1. Граф  $\Gamma_1$

Пусть  $\mu = \nu = 3$ , тогда  $L(1, 3) = \{1, 2\} = L(3, 5)$ ,  $L(\mu, \nu) = \{0\}$ , следовательно,  $L(1, 3) + L(3, 3) + L(3, 5) = \{2, 3, 4\} \subseteq M_{1,5}$ . Тогда  $M_{1,5}$  есть 3-полное множество, где  $q(M_{1,5}) = 2$ .

Условия теоремы 1 выполнены, следовательно, граф  $\Gamma_1$  является  $1 \times 5$ -примитивным и  $1 \times 5$ -exp  $\Gamma \leq 2$ . Заметим, что  $1 \times 5$ -exp  $\Gamma = 2$ , так как длина кратчайшего пути из 1 в 5 равна 2.

**Теорема 2.** Пусть в связном орграфе  $\Gamma$  имеются  $i, j$ -связывающие циклы  $\tilde{C}_1, \dots, \tilde{C}_k$  длины  $l$ , где  $k \geq 1$ , и множество  $M_{i,j} = \bigcup_{r=1}^k \bigcup_{\mu_r, \nu_r \in C_r} \{L(i, \mu_r) + L(\mu_r, \nu_r) + L(\nu_r, j)\}$  является  $l$ -полным. Тогда граф  $\Gamma$  является  $i \times j$ -примитивным и  $i \times j$ -exp  $\Gamma \leq q(M_{i,j})$ .

**Пример 2.** В 8-вершинном орграфе  $\Gamma_2$  (рис. 2) имеются два 1,8-связывающих цикла длины  $l = 3$ :  $\tilde{C}_1 = (2, 3, 4)$ ,  $\tilde{C}_2 = (5, 6, 7)$ . Покажем  $1 \times 8$ -примитивность орграфа  $\Gamma_2$ .

Рис. 2. Граф  $\Gamma_2$ 

Пусть  $\mu_1 = 2$ ,  $\nu_1 = 3$ ,  $\mu_2 = \nu_2 = 6$ , тогда  $L(1, 2) = \{1\}$ ,  $L(3, 8) = \{1, 2\}$ ,  $L(2, 3) = \{1\}$ ,  $L(1, 6) = \{1\}$ ,  $L(6, 8) = \{1\}$ ,  $L(6, 6) = \{0\}$ . Отсюда

$$\{L(1, 2) + L(2, 3) + L(3, 8)\} \cup \{L(1, 6) + L(6, 6) + L(6, 8)\} = \{3, 4\} \cup \{2\} = \{2, 3, 4\},$$

следовательно,  $M_{1,8}$  есть 3-полное множество, где  $q(M_{1,8}) = 2$ .

Условия теоремы 2 выполнены, следовательно, орграф  $\Gamma_2$  является  $1 \times 8$ -примитивным и  $1 \times 8$ -exp  $\Gamma \leq 2$ . Заметим, что  $1 \times 8$ -exp  $\Gamma = 2$ , так как длина кратчайшего пути из 1 в 8 равна 2.

#### ЛИТЕРАТУРА

1. Кяжсин С. Н., Фомичев В. М. Локальная примитивность графов и неотрицательных матриц // Прикладная дискретная математика. 2014. № 3(25) (в печати).

УДК 519.17

### ОБ ОДНОМ КОНТРПРИМЕРЕ ДЛЯ T-НЕПРИВОДИМЫХ РАСШИРЕНИЙ СВЕРХСТРОЙНЫХ ДЕРЕВЬЕВ

Д. Ю. Осипов

T-неприводимым расширением (ТНР) графа называется его расширение, получаемое из тривиального удалением максимально возможного количества добавленных при построении тривиального расширения рёбер. Рассматривается один из способов построения ТНР. Приводится контрпример для схемы из работы Ф. Харари и М. Хурума «One node fault tolerance for caterpillars and starlike trees», которая описывает построение одного ТНР для произвольного сверхстройного дерева. Рассматривается способ построения всех неизоморфных ТНР для подкласса сверхстройных деревьев — равнолучевых звезд.

**Ключевые слова:** граф, T-неприводимое расширение, сверхстройные деревья, равнолучевые звезды.

Все понятия и определения соответствуют понятиям и определениям в [1].

**Определение 1.** Расширением  $n$ -вершинного графа  $G$  называется граф  $H$  с  $n+1$  вершинами, такой, что граф  $G$  вкладывается в каждый максимальный подграф графа  $H$ .

Простейшим примером расширения графа  $G$  является его тривиальное расширение — соединение графа  $G$  с одноэлементным графом (т.е. к графу  $G$  добавляется вершина, которая соединяется ребром с каждой вершиной графа  $G$ ).

Понятие расширения графа тесно связано с вопросами отказоустойчивости дискретных систем. Если граф  $G$  рассматривать как функциональную модель некоторого

устройства  $\Sigma$ , то расширение  $H$  графа  $G$  можно воспринимать как схему отказоустойчивой реализации этого устройства: при отказе любого элемента (что истолковывается как удаление из  $H$  соответствующей вершины и всех связанных с ней рёбер) в неповрежденной части обнаруживается работоспособная модель для  $\Sigma$ .

При таком подходе естественно возникает вопрос об оптимальности отказоустойчивой реализации для данной системы, т. е. о получении такого расширения  $H$  графа  $G$ , которое не содержало бы «лишних» рёбер. Один из способов — конструкция минимального расширения графа [2], другой — его Т-неприводимое расширение [3].

**Определение 2.** Минимальным расширением графа  $G$  называется его расширение с минимальным количеством рёбер.

В общем случае при построении минимального расширения возникает необходимость добавлять рёбра в исходный граф, т. е. менять всю систему, моделируемую этим графом. Но иногда технически важно найти решение следующей задачи: построить оптимальное расширение данного графа, сохраняя его первоначальную конструкцию (т. е. не меняя связей внутри него). Существует следующая процедура:

- построить тривиальное расширение исходного графа;
- удалять из полученного графа рёбра до тех пор, пока выполняется свойство расширения.

Полученные графы назовем Т-неприводимыми расширениями графа  $G$ . Для произвольного графа количество неизоморфных ТНР неизвестно.

**Определение 3** [2]. Дерево называется сверхстройным, если в точности одна его вершина имеет степень больше 2. Эту вершину будем называть корнем сверхстройного дерева.

Сверхстройное дерево можно рассматривать как объединение  $k$  цепей с общей концевой вершиной. При этом дерево можно закодировать вектором, состоящим из длин цепей в порядке невозрастания:  $(m_1, \dots, m_k)$ , где  $m_1 \geq \dots \geq m_k$ . Очевидно, что такое кодирование сверхстройных деревьев при  $k > 2$  является взаимно однозначным.

**Определение 4.** Вершина  $v_{ij}$  (где  $i$  — номер цепи сверхстройного дерева;  $j$  — номер вершины в этой цепи, нумерация начинается с 1 от корня) сверхстройного дерева  $T$  называется сложной, если среди длин цепей дерева  $T$  нет цепи длины  $j - 1$  или  $m_i - j$ ;  $i = 1, \dots, k$ ,  $m_i > 1$ ,  $j = 2, \dots, m_i$ .

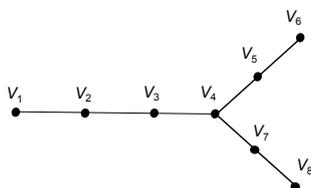
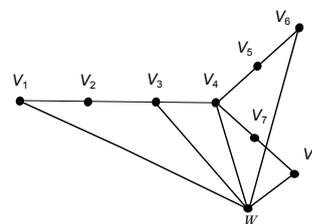
До сих пор остается нерешённой следующая задача: построить все неизоморфные ТНР для произвольного сверхстройного дерева. Попытка построить одно из таких ТНР описывается в [4].

В соответствии со схемой из [4] для построения одного из ТНР произвольного сверхстройного дерева необходимо:

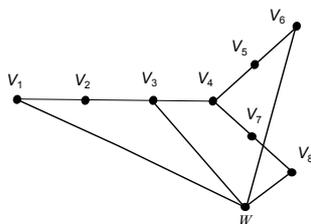
- добавить новую вершину к исходному графу;
- соединить добавленную вершину с корнем и со всеми листьями исходного сверхстройного дерева;
- если в исходном сверхстройном дереве нет сложных вершин, то полученный граф является искомым ТНР. Если есть некоторая сложная вершина  $v_{ij}$ , то соединить ребром добавленную вершину и вершину  $v_{ij-1}$ . Так поступаем для всякой сложной вершины.

Отметим, что в работе [5] уже приводились контрпримеры для утверждения из [4], что минимальное вершинное 1-расширение сверхстройного дерева с  $k$  цепями и  $p$  сложными вершинами содержит в точности  $k + p + 1$  дополнительных рёбер.

Рассмотрим сверхстройное дерево  $(3, 2, 2)$  (граф  $G$  на рис. 1) и построим ТНР для него по описанной схеме (граф  $G'$  на рис. 2).

Рис. 1. Граф  $G$ Рис. 2. Граф  $G'$ 

Однако несложно заметить, что граф  $G'$  не является ТНР для сверхстройного дерева  $G$ . На самом деле ТНР для графа  $G$  является граф  $H$  (рис. 3).

Рис. 3. Граф  $H$ 

Если сравнить графы  $G'$  и  $H$ , то несложно заметить, что они отличаются на одно ребро. Докажем, что граф  $H$  действительно является ТНР для графа  $G$ , представленного на рис. 1.

Легко проверяется, что граф  $H$  является расширением графа  $G$ . Докажем свойство неприводимости графа  $H$ , т.е. что при удалении любого ребра из него получается граф, не являющийся расширением графа  $G$ . Очевидно, при удалении ребра  $wv_6$  (или  $wv_8$ , или  $wv_1$ ) полученный граф не будет расширением для графа  $G$ , так как достаточно удалить из полученного графа вершину  $v_5$  (или  $v_7$ , или  $v_2$  соответственно), чтобы получить вершину  $v_6$  (или  $v_8$ , или  $v_1$  соответственно) степени 0, чего не может быть в графе  $G$ . При удалении ребра  $wv_3$  достаточно удалить вершину  $v_4$ . В этом случае центром графа будет вершина  $w$ , а вершина  $v_8$  будет иметь степень 1, но так как вершина  $v_8$  смежна только с  $w$ , то мы не сможем получить двухвершинную цепь, а следовательно, в полученный граф не вкладывается граф  $G$ . Таким образом, никакой граф, полученный из  $H$  удалением ребра, не является расширением для  $G$ , и свойство неприводимости графа  $H$  доказано. Следовательно, граф  $H$  является ТНР для графа  $G$ .

Граф  $G$  — это сверхстройное дерево с наименьшим числом вершин, которое является контрпримером для описанной в [4] схемы. Среди сверхстройных деревьев с числом вершин 9 такого контрпримера нет. Среди сверхстройных деревьев с числом вершин 10 существует одно такое дерево:  $(5, 2, 2)$ . Среди сверхстройных деревьев с числом вершин 11 существуют два таких дерева:  $(4, 3, 3)$  и  $(6, 2, 2)$ . Можно предположить, что

с ростом числа вершин количество контрпримеров будет возрастать, и такие графы можно выделить в некий подкласс сверхстройных деревьев.

Приведём решение задачи построения одного из ТНР для подкласса сверхстройных деревьев — равнолучевых звёзд [6].

**Определение 5.** Граф  $S_n^m = (V, \alpha)$  называется равнолучевой звездой с  $m$  лучами, каждый из которых состоит из  $n$  вершин, если  $V = \{v_0, v_1^1, \dots, v_n^1, \dots, v_1^m, \dots, v_n^m\}$ ,  $\alpha = \{v_i^j v_{i+1}^j : i = 1, \dots, n-1; j = 1, \dots, m\} \cup \{v_0 v_1^j : j = 1, \dots, m\}$ , где  $v_0$  — центр равнолучевой звезды.

**Теорема 1.** Единственным ТНР для графа  $S_n^m$ ,  $n \geq 2$ , является граф, полученный из тривиального расширения графа  $S_n^m$  удалением рёбер  $wv_{n-1}^j$ ,  $j = 1, \dots, m$ , где  $w$  — вершина, добавленная при построении тривиального расширения графа  $S_n^m$ .

#### ЛИТЕРАТУРА

1. Богомолов А. М., Салий В. Н. Алгебраические основы теории дискретных систем. М.: Наука, 2009.
2. Абросимов М. Б. Минимальные расширения объединения некоторых графов // Теоретические проблемы информатики и её приложений. 2001. № 4. С. 3–11.
3. Салий В. Н. Доказательства с нулевым разглашением в задачах о расширениях графов // Вестник Томского государственного университета. Приложение. 2003. № 6. С. 63–65.
4. Harary F. and Khurum M. One node fault tolerance for caterpillars and starlike trees // Internet J. Comput. Math. 1995. V. 6. P. 135–143.
5. Абросимов М. Б., Комаров Д. Д. Об одном контрпримере для минимальных вершинных 1-расширений сверхстройных деревьев // Прикладная дискретная математика. Приложение. 2012. № 5. С. 83–84.
6. Осипов Д. Ю. О Т-неприводимых расширениях сверхстройных деревьев // Прикладная дискретная математика. Приложение. 2013. № 6. С. 85–86.

УДК 519.17

## ШПЕРНЕРОВО СВОЙСТВО ДЛЯ МНОГОУГОЛЬНЫХ ГРАФОВ

В. Н. Салий

Конечное упорядоченное множество называется шпернеровым, если среди его максимальных по длине антицепей хотя бы одна составлена из элементов одинаковой высоты. Под многоугольным графом понимается бесконтурный граф, полученный из цикла путём некоторой ориентации его рёбер. В многоугольном графе отношение достижимости вершин является отношением порядка. Таким образом, многоугольный граф можно рассматривать как упорядоченное множество. Найдено необходимое и достаточное условие шпернеровости таких упорядоченных множеств.

**Ключевые слова:** упорядоченное множество, шпернерово свойство, многоугольный граф, цепь, зигзаг.

Пусть  $(A, \leq)$  — конечное упорядоченное множество. Высота  $h(a)$  элемента  $a$  в  $(A, \leq)$  определяется как максимальная из длин убывающих цепей, начинающихся с  $a$ .

Антицепь в упорядоченном множестве — это такое его подмножество, в котором любые два элемента несравнимы. Под длиной антицепи понимается количество элементов в ней. Антицепи максимальной длины будем называть главными. Антицепь в конечном

упорядоченном множестве называется правильной, если все её элементы имеют одинаковую высоту. Так, в упорядоченном множестве  $(\mathbb{N}_8, |)$  (первые 8 натуральных чисел с отношением делимости) среди главных антицепей  $\{2, 3, 5, 7\}$ ,  $\{3, 4, 5, 7\}$ ,  $\{3, 5, 7, 8\}$  правильной является только первая. В  $(P(\{a, b, c\}), \subseteq)$  (совокупность всех подмножеств трёхэлементного множества с отношением включения) главных антицепей две:  $\{a, b, c\}$  и  $\{ab, ac, bc\}$ , и обе они — правильные.

Конечное упорядоченное множество назовём шпернеровым, если среди его главных антицепей есть по крайней мере одна правильная. Упорядоченные множества  $(\mathbb{N}_8, |)$  и  $(P(\{a, b, c\}), \subseteq)$  являются шпернеровыми. Один из минимальных примеров упорядоченного множества, не обладающего свойством шпернеровости, образуют по включению пять подмножеств множества  $S = \{a, b, c, d\}$ , а именно  $\{a\}$ ,  $\{b\}$ ,  $\{b, c\}$ ,  $\{b, d\}$ ,  $\{a, b, c\}$ . В нём всего одна главная антицепь —  $\{a, bc, bd\}$ , и она не является правильной.

В 1928 г. Шпернер [1] доказал, что все конечные упорядоченные множества вида  $(P(S), \subseteq)$  обладают обнаруженным им свойством. Свойство шпернеровости для конечных упорядоченных множеств находит содержательные интерпретации в различных разделах математики (см., например, [2–4]), в том числе и в теории графов [5, 6].

Под (ориентированным) графом понимается пара  $G = (V, \alpha)$ , где  $V$  — конечное непустое множество и  $\alpha \subseteq V \times V$  — отношение на нём. Элементы множества  $V$  называются вершинами графа, а пары, входящие в  $\alpha$ , — его дугами.

Вершины  $u$  и  $v$ , по определению, связаны, если существуют  $v_1, v_2, \dots, v_k \in V$ , такие, что  $(u, v_1) \in \alpha \cup \alpha^{-1}$ ,  $(v_1, v_2) \in \alpha \cup \alpha^{-1}$ ,  $\dots$ ,  $(v_k, v) \in \alpha \cup \alpha^{-1}$ , т. е. если  $u$  и  $v$  можно соединить последовательностью дуг без учёта их направлений. Граф, в котором любые две вершины связаны, называется связным.

Граф  $H = (U, \beta)$  называется частью графа  $G = (V, \alpha)$ , если  $U \subseteq V$  и  $\beta \subseteq \alpha$ , т. е.  $H$  состоит из некоторых вершин графа  $G$  и некоторых дуг, соединяющих в  $G$  эти вершины.

Контур длины  $k \geq 2$  в графе  $G$  определяется как последовательность  $C_k$  его дуг вида  $(v_1, v_2), (v_2, v_3), \dots, (v_{k-1}, v_k), (v_k, v_1)$ , в которой все встречающиеся вершины различны. Граф, не содержащий контуров, называется бесконтурным.

Вершина  $v$ , по определению, достижима в графе  $G$  из вершины  $u$ , если существует последовательность примыкающих дуг  $(u, v_1), (v_1, v_2), \dots, (v_k, v)$ , соединяющая  $u$  с  $v$ . Отношение достижимости в графе обозначим через  $\delta$ . В бесконтурном графе отношение достижимости является отношением порядка (о бесконтурных графах см. [7]). Очевидно, что минимальными элементами в упорядоченном множестве  $(V, \delta)$  являются стоки графа  $G$ , т. е. те его вершины, из которых не исходит ни одна дуга в другие вершины. Максимальными элементами в  $(V, \delta)$  являются источники графа  $G$ , т. е. те его вершины, в которые не входит ни одна дуга из других вершин.

Связный бесконтурный граф  $G = (V, \alpha)$  назовём шпернеровым, если упорядоченное множество  $(V, \delta)$  обладает шпернеровым свойством.

Пусть  $n \geq 2$  — натуральное число. Под  $n$ -угольным графом будем понимать всякий граф, полученный из контура  $C_n$  переориентацией некоторого количества  $k$  его дуг. Будем считать, что  $1 \leq k < n$ . Следовательно, контуры исключаются из числа многоугольных графов, которые, таким образом, попадают в класс связных бесконтурных графов [8].

Для шестиугольного графа  $M' : v_1 \rightarrow v_2 \rightarrow v_3 \leftarrow v_4 \rightarrow v_5 \leftarrow v_6 \leftarrow v_1$   $\delta$ -упорядоченное множество его вершин содержит одну главную антицепь —  $\{2, 4, 6\}$ . Она является правильной, так что  $M'$  — шпернеров граф. Аналогично, для шестиугольного графа

$M'' : v_1 \rightarrow v_2 \rightarrow v_3 \leftarrow v_4 \leftarrow v_5 \rightarrow v_6 \leftarrow v_1$   $\delta$ -упорядоченное множество вершин содержит тоже единственную главную антицепь —  $\{2, 4, 6\}$ , но здесь она не является правильной, так что  $M''$  — не шпернеров граф.

Под цепью в многоугольном графе будем понимать его максимальную собственную связную часть, в которой 1) есть хотя бы одна вершина, не являющаяся ни источником, ни стоком, и 2) любые две соседние дуги одинаково направлены. Например, цепями в графе  $M'$  являются  $v_1 \rightarrow v_2 \rightarrow v_3$  и  $v_1 \rightarrow v_6 \rightarrow v_5$ , а в графе  $M''$  —  $v_1 \rightarrow v_2 \rightarrow v_3$  и  $v_5 \rightarrow v_4 \rightarrow v_3$ . Всякая цепь начинается в источнике и завершается стоком. Зигзагом в многоугольном графе назовём его максимальную собственную связную часть, в которой 1) каждая вершина является источником или стоком и 2) любые две соседние дуги противоположно направлены. Зигзаги классифицируются по виду их концевых вершин: в  $ss$ -зигзаге оба конца являются источниками; в  $st$ -зигзаге один конец источник, другой сток; в  $tt$ -зигзаге оба конца стоки. Так, в графе  $M'$  есть  $tt$ -зигзаг  $v_3 \leftarrow v_4 \rightarrow v_5$ , а в графе  $M''$  имеется  $ss$ -зигзаг  $v_1 \rightarrow v_6 \leftarrow v_5$ .

**Теорема.** Многоугольный граф тогда и только тогда является шпернеровым, когда в нём нет  $ss$ -зигзагов.

#### ЛИТЕРАТУРА

1. *Sperner E.* Ein Satz uber Untermengen einer endlichen Menge // *Math. Zeitschrift.* 1928. V. 27. No. 1. S. 544–548.
2. *Мешалкин Л. Д.* Обобщение теоремы Шпернера о числе подмножеств конечного множества // *Теория вероятностей и её применения.* 1963. Т. 8. № 2. С. 219–220.
3. *Stanley E. P.* Weyl groups, the hard Lefschetz theorem and the Sperner property // *SIAM J. Alg. Discr. Math.* 1980. V. 1. No. 2. P. 168–184.
4. *Wang J.* Proof of a conjecture on the Sperner property of the subgroup lattice of an abelian  $p$ -group // *Annals Comb.* 1999. V. 2. No. 1. P. 85–101.
5. *Jacobson M. S., Kezdy A. E., and Seif S.* The poset of connected induced subgraphs of a graph need not be Sperner // *Order.* 1995. V. 12. No 3. P. 315–318.
6. *Maeno T. and Numata Y.* Sperner property, matroids and finite-dimensional Gorenstein algebras // *Contemp. Math.* 2012. V. 280. No. 1. P. 73–83.
7. *Богомолов А. М., Салий В. Н.* Алгебраические основы теории дискретных систем. М.: Наука, 1997.
8. *Салий В. Н.* Упорядоченное множество связных частей многоугольного графа // *Изв. Сарат. ун-та. Нов. сер. Сер. Математика. Механика. Информатика.* 2013. Т. 13. № 2 (ч. 2). С. 44–51.

УДК 519.7

### ОБ ОЦЕНКАХ ЭКСПОНЕНТОВ ОРГРАФОВ С ИСПОЛЬЗОВАНИЕМ ЧИСЕЛ ФРОБЕНИУСА

В. М. Фомичев

Для частных классов сильносвязных орграфов получены достаточные условия примитивности и оценки экспонентов, которые выражены через числа Фробениуса. Показано, что во многих случаях полученные оценки экспонента орграфа существенно лучше известных оценок.

**Ключевые слова:** число Фробениуса, примитивный граф, экспонент графа.

## Введение

Одним из основных направлений в исследовании экспонентов примитивных неотрицательных матриц (примитивных сильносвязных графов) является уточнение известных оценок экспонентов для различных частных классов матриц (графов), важных для тех или иных приложений.

Абсолютная оценка экспонента  $n$ -вершинного орграфа  $\Gamma$  дана в [1]:  $\exp \Gamma \leq n^2 - 2n + 2$ .

Последующие результаты уточнили абсолютную оценку. Если длина кратчайшего простого контура в  $\Gamma$  равна  $l$  [2, с. 227], то  $\exp \Gamma \leq n + l(n - 2)$ . Если, в частности, в орграфе  $\Gamma$  имеется  $d$  петель [2, с. 408], то  $\exp \Gamma \leq 2n - d - 1$ .

Пусть в орграфе  $\Gamma$  известны длины  $l$  и  $\lambda$  двух простых контуров  $C$  и  $Z$  [3], где  $(l, \lambda) = 1$ ,  $1 < \lambda < l \leq n$ ,  $n > 2$  и  $h$  — число общих вершин контуров  $C$  и  $Z$ . Тогда  $\exp \Gamma \leq l\lambda - 2l - 3\lambda + 3n$ , если  $h = 0$ , и  $\exp \Gamma \leq l\lambda - l - 3\lambda + h + 2n$ , если  $h > 0$ .

Оценки экспонентов других частных классов графов имеются в работах [2, 4–6]. Обзор результатов в этом направлении, полученных до 2012 г., дан в [7].

Для новых частных классов  $n$ -вершинных орграфов приводятся достаточные условия примитивности и оценки экспонентов с использованием чисел Фробениуса.

### 1. Оценки экспонентов орграфов

Пусть  $\tilde{C} = \{C_1, \dots, C_k\}$  — система контуров в  $n$ -вершинном орграфе  $\Gamma$ , длины контуров равны  $l_1, \dots, l_k$  соответственно, где  $k \geq 2$  и  $l_1 < \dots < l_k$ . Систему  $\tilde{C}$  назовём примитивной, если  $(l_1, \dots, l_k) = 1$ . Тогда универсальный критерий примитивности орграфа  $\Gamma$  [2, с. 226] допускает следующую формулировку: сильносвязный орграф  $\Gamma$  примитивный, если и только если в  $\Gamma$  имеется примитивная система контуров.

Систему  $\tilde{C}$  назовём  $i$ -связанной, если каждый из контуров  $C_1, \dots, C_k$  содержит вершину  $i$ , где  $i \in \{1, \dots, n\}$ . В частности, система контуров перемешивающего графа биективного регистра левого (правого) сдвига длины  $n$  является  $n$ -связанной (1-связанной). Через  $g(l_1, \dots, l_k)$  обозначим число Фробениуса для натуральных аргументов  $l_1, \dots, l_k$ .

**Теорема 1.** Пусть в сильносвязном орграфе  $\Gamma$  имеется примитивная  $i$ -связанная система контуров  $\tilde{C} = \{C_1, \dots, C_k\}$ ,  $i \in \{1, \dots, n\}$ , состоящая из  $q$  вершин орграфа. Тогда

$$\exp \Gamma \leq g(l_1, \dots, l_k) + 2(n - q + l_k) - 1.$$

Обозначим через  $[i, j]_C$  простой путь, проходящий через вершины  $i, j$  и являющийся частью простого контура  $C$ . Длину пути  $w$  в  $\Gamma$ , равную числу дуг, составляющих путь, обозначим  $l(w)$ . Символом  $\cdot$  обозначим конкатенацию путей графа  $\Gamma$ .

Пусть в орграфе  $\Gamma$  контур  $C$  длины  $t$ , где  $4 \leq t \leq n$ , содержит различные вершины  $i, j$  и  $r$ , тогда возможны два варианта:

$$C = [i, r]_C \cdot [r, j]_C \cdot [j, i]_C, \tag{1}$$

в этом случае положим  $l([i, j]_C) = h > 2$ ,  $l([i, r]_C) = \tau < h$ ;

$$C = [i, j]_C \cdot [j, r]_C \cdot [r, i]_C, \tag{2}$$

в этом случае положим  $l([i, j]_C) = h < t - 2$ ,  $l([j, r]_C) = \theta < t - h$ .

#### Теорема 2.

1) Пусть  $(i, r)$  и  $(r, j)$  — дуги орграфа  $\Gamma$ , тогда  $\Gamma$  — примитивный:

— в случае равенства (1), если  $(t - h + 2, t - \tau + 1, t - h + \tau + 1) = 1$ , при этом

$$\text{exp } \Gamma \leq g(t - h + 2, t - \tau + 1, t - h + \tau + 1) + 2(n - t + \max\{\tau, h - \tau\}) - 1;$$

— в случае равенства (2), если  $(\theta + 1, t - h - \theta + 1, t) = 1$ , при этом

$$\text{exp } \Gamma \leq g(\theta + 1, t - h - \theta + 1, t) + 2n - 1.$$

2) Пусть  $(r, i)$  и  $(j, r)$  — дуги орграфа  $\Gamma$ , тогда  $\Gamma$  — примитивный:

— в случае равенства (1), если  $(\tau + 1, h - \tau + 1, t) = 1$ , при этом

$$\text{exp } \Gamma \leq g(\tau + 1, h - \tau + 1, t) + 2n - 1;$$

— в случае равенства (2), если  $(t - \theta + 1, h + 2, h + \theta + 1) = 1$ , при этом

$$\text{exp } \Gamma \leq g(t - \theta + 1, h + 2, h + \theta + 1) + 2(n - t + \max\{\theta, t - h - \theta\}) - 1.$$

**Примеры.** Пусть  $n = 100$ ,  $C = (1, \dots, 80)$ ,  $t = 80$ ,  $i = 1$ ,  $j = 41$ , тогда  $h = 40$ .

1) Пусть  $r = 33$ ,  $(1, 33)$  и  $(33, 41)$  — дуги орграфа  $\Gamma$ , тогда  $\tau = 32$  и

$$(t - h + 2, t - \tau + 1, t - h + \tau + 1) = (42, 49, 73) = 1,$$

то есть по п. 1 теоремы 2 орграф  $\Gamma$  примитивный и  $\text{exp } \Gamma \leq g(42, 49, 73) + 103$ .

Используя обозначения работы [8], определим  $g(42, 49, 73)$ . Вычисляем:  $d = (42, 49) = 7$ ,  $z = 7 \cdot 29 = 203$ , тогда  $|\langle 42, 49 \rangle| = |C(42, 49)| = 30/2 = 15$ ,

$$\overline{\langle 42, 49 \rangle} = 7 \cdot \{0, 6, 7, 12, 13, 14, 18, 19, 20, 21, 24, 25, 26, 27, 28\},$$

$$C(42, 49) = 7 \cdot \{1, 2, 3, 4, 5, 8, 9, 10, 11, 15, 16, 17, 22, 23, 29\},$$

$S(73) = \emptyset$ ,  $g(42, 49, 73) = z + (d - 1)73 = 203 + 6 \cdot 73 = 641$  и  $\text{exp } \Gamma \leq 744$ .

Оценки  $\text{exp } \Gamma$  по формулам работ [1, 2, 3] равны 9802, 4216 и 3109 соответственно.

2) Пусть  $r = 55$ ,  $(1, 55)$  и  $(55, 41)$  — дуги орграфа  $\Gamma$ , тогда  $\theta = 14$  и

$$(\theta + 1, t - h - \theta + 1, t) = (15, 27, 80) = 1,$$

то есть по п. 1 теоремы 2 орграф  $\Gamma$  примитивный и  $\text{exp } \Gamma \leq g(15, 27, 80) + 199$ .

Определим  $g(15, 27, 80)$ . Вычисляем:  $d = (15, 27) = 3$ ,  $z = 3 \cdot 31 = 93$ , тогда  $|\langle 15, 27 \rangle| = |C(15, 27)| = 32/2 = 16$ ,

$$\overline{\langle 15, 27 \rangle} = 3 \cdot \{0, 5, 9, 10, 14, 15, 18, 19, 20, 23, 24, 25, 27, 28, 29, 30\},$$

$$C(15, 27) = 3 \cdot \{1, 2, 3, 4, 6, 7, 8, 11, 12, 13, 16, 17, 21, 22, 26, 31\},$$

$S(80) = \emptyset$ ,  $g(15, 27, 80) = z + (d - 1)80 = 93 + 2 \cdot 80 = 253$  и  $\text{exp } \Gamma \leq 452$ .

Оценки  $\text{exp } \Gamma$  по формулам работ [1, 2, 3] равны 9802, 1570 и 2226 соответственно.

3) Пусть  $r = 33$ ,  $(33, 1)$  и  $(41, 33)$  — дуги орграфа  $\Gamma$ , тогда  $\tau = 32$  и

$$(\tau + 1, h - \tau + 1, t) = (33, 9, 80) = 1,$$

то есть по п. 2 теоремы 2 орграф  $\Gamma$  примитивный и  $\text{exp } \Gamma \leq g(9, 33, 80) + 199$ .

Определим  $g(9, 33, 80)$ . Вычисляем:  $d = (9, 33) = 3$ ,  $z = 3 \cdot 19 = 57$ , тогда  $|\langle 9, 33 \rangle| = |C(9, 33)| = 20/2 = 10$ ,

$$\overline{\langle 9, 33 \rangle} = 3 \cdot \{0, 3, 6, 9, 11, 12, 14, 15, 17, 18\},$$

$$C(9, 33) = 3 \cdot \{1, 2, 4, 5, 7, 8, 10, 13, 16, 19\},$$

$S(73) = \emptyset$ ,  $g(9, 33, 80) = z + (d - 1)80 = 57 + 2 \cdot 80 = 217$  и  $\text{exp } \Gamma \leq 416$ .

Оценки  $\text{exp } \Gamma$  по формулам работ [1, 2, 3] равны 9802, 982 и 814 соответственно.

4) Пусть  $r = 59$ ,  $(59, 1)$  и  $(41, 59)$  — дуги орграфа  $\Gamma$ , тогда  $\theta = 18$  и

$$(t - \theta + 1, h + 2, h + \theta + 1) = (63, 42, 59) = 1,$$

то есть по п. 2 теоремы 2 орграф  $\Gamma$  примитивный и  $\text{exp } \Gamma \leq g(42, 59, 63) + 83$ . Так как  $(42, 59) = 1$ , то  $g(42, 59, 63) \leq g(42, 59) = 2377$ , откуда получаем  $\text{exp } \Gamma \leq 2460$ .

Оценки  $\text{exp } \Gamma$  по формулам работ [1, 2, 3] равны 9802, 4216 и 2535 соответственно.

Анализ числовых примеров позволяет считать, что полученная оценка, как правило, значительно точнее известных оценок.

#### ЛИТЕРАТУРА

1. *Wielandt H.* Unzerlegbare nicht negative Matrizen // *Math. Zeitschr.* 1950. No. 52. P. 642–648.
2. *Сачков В. Н., Тараканов В. Е.* Комбинаторика неотрицательных матриц. М.: ТВП, 2000. 448 с.
3. *Фомичев В. М.* Оценки экспонентов примитивных графов // *Прикладная дискретная математика.* 2011. № 2(12). С. 101–112.
4. *Князев А. В.* Оценки экстремальных значений основных метрических характеристик псевдосимметрических графов: дис. ... докт. физ.-мат. наук. М., 2002. 203 с.
5. *Коренева А. М., Фомичев В. М.* Об одном обобщении блочных шифров Фейстеля // *Прикладная дискретная математика.* 2012. № 3(17). С. 34–40.
6. *Дорохова А. М., Фомичев В. М.* Уточненные оценки экспонентов перемешивающих графов биективных регистров сдвига над множеством двоичных векторов // *Прикладная дискретная математика.* 2014. № 1(23). С. 77–83.
7. *Когос К. Г., Фомичев В. М.* Положительные свойства неотрицательных матриц // *Прикладная дискретная математика.* 2012. № 4(18). С. 5–13.
8. *Фомичев В. М.* Оценка экспонента некоторых графов с помощью чисел Фробениуса для трёх аргументов // *Прикладная дискретная математика.* 2014. № 2(24). С. 88–96.

Секция 9

ПРИКЛАДНАЯ ТЕОРИЯ АВТОМАТОВ

УДК 519.7

ОЦЕНКА КРАТНОСТИ ВЫХОДНОГО СИМВОЛА  
В ОБРАТИМОМ АВТОМАТЕ

Д. А. Катеринский

Доказано, что максимальное количество  $\rho$  повторений некоторого выходного символа в таблице выходов автомата с  $n$  состояниями и  $m$  входными символами, при котором автомат обратим, вычисляется по формуле  $\rho = [(n+1)/2][(n+2)/2]$ , если  $[(n+2)/2] \leq m$ , и  $\rho = (n-m+1)m$  в противном случае.

**Ключевые слова:** конечные автоматы, обратимость, слабая обратимость, сильная обратимость, анализ обратимости, пороговое число обратимости.

Рассматриваются сильно и слабо обратимые конечные автоматы с конечной задержкой. В первых входная последовательность восстанавливается с задержкой по выходной последовательности, во вторых — по выходной последовательности и начальному состоянию [1, 2]. Автомат называется обратимым, если он слабо или сильно обратим. Множество всех обратимых автоматов обозначается  $Inv$ .

Пусть далее  $A$  есть произвольный конечный автомат с  $n$  состояниями,  $m$  входными символами и с множеством выходных символов  $Y$ . Пусть также  $\rho^A(y)$  — количество вхождений выходного символа  $y \in Y$  в таблице выходов автомата  $A$ ,  $\rho(A) = \max_{y \in Y} \{\rho^A(y)\}$  и  $\rho = \max_{A \in Inv} \rho(A)$ .

По определению,  $\rho$  есть максимально возможное количество повторений символа в таблице выходов автомата, при котором этот автомат обратим.

**Теорема 1.**

$$\rho = \begin{cases} \left[ \frac{n+1}{2} \right] \left[ \frac{n+2}{2} \right], & \text{если } \left[ \frac{n+2}{2} \right] \leq m; \\ (n-m+1)m, & \text{если } \left[ \frac{n+2}{2} \right] > m. \end{cases}$$

ЛИТЕРАТУРА

1. Курмит А. А. Автоматы без потери информации конечного порядка. Рига: Зинатне, 1972.
2. Тао Р. J. Finite automata and application to cryptography. Tsinghua: Springer, 2008.

УДК 004.056.55

## РЕАЛИЗАЦИЯ НА ПЛИС ШИФРА ЗАКРЕВСКОГО НА ОСНОВЕ ПЕРЕСТРАИВАЕМОГО АВТОМАТА, ЗАДАННОГО ФОРМУЛАМИ

Д. С. Ковалев, В. Н. Тренькаев

Рассмотрена реализация на ПЛИС шифра Закревского на основе перестраиваемого автомата, заданного формулами, когда функции переходов и выходов вычисляются с помощью часто используемой в симметричных шифрах операции сложения по модулю целого числа (обычно степени двойки). Установлено, что формульный (аналитический) способ представления автомата по сравнению с табличным приводит к улучшению эффективности ПЛИС-реализации шифра, в частности наблюдается рост производительности на 17–36 %.

**Ключевые слова:** шифр Закревского, перестраиваемый автомат, табличный способ задания автомата, формульный способ задания автомата, производительность, ресурсоёмкость, ПЛИС, VHDL.

Работа продолжает начатые в [1] исследования шифра Закревского на основе перестраиваемого автомата на пригодность к практическому использованию в различных вычислительных системах. Критерием оценки пригодности шифра к использованию на практике является эффективность его реализации на базе ПЛИС (программируемая логическая интегральная схема).

Шифр Закревского [2] является автоматным шифром, в котором алгоритмы шифрования и расшифрования задаются взаимно обратными сильносвязными автоматами, ключом являются начальное состояние и функции переходов и выходов обоих автоматов. В работе [3] предложено построение шифра Закревского на основе перестраиваемого автомата, функция переходов  $\psi(x, s)$  которого вычисляется следующим образом. Для любой пары  $(x, s)$ , где  $x$  — символ открытого текста, а  $s$  — текущее состояние перестраиваемого автомата, верно: если предикат  $key(x, s) = 0$ , то  $\psi(x, s) = \psi_0(x, s)$ , иначе  $\psi(x, s) = \psi_1(x, s)$ . Таким образом, следующее состояние задаётся как одно из состояний, полученных с помощью двух различных функций переходов  $\psi_0$  и  $\psi_1$ . При шифровании символ шифртекста  $y = \varphi(x, s)$  вычисляется с помощью «открытой» функции выходов  $\varphi$ , биективной в каждом состоянии. При расшифровании символ открытого текста вычисляется с помощью функции, обратной к  $\varphi$ .

В данной работе предлагается от табличной формы задания перестраиваемого автомата перейти к формульной, тем самым зафиксировать некоторые элементы структурного синтеза автомата. Далее  $x$  и  $s$  — целые положительные числа, сопоставленные символу открытого текста и состоянию соответственно, либо их двоичные представления (в зависимости от операции).

Для любой пары  $(x, s)$  верно: для  $x \neq s$  если  $key(x, s) = 0$ , то  $\psi(x, s) = x \oplus s$ , иначе  $\psi(x, s) = x \oplus \bar{s}$  (используются побитовые операции); если  $x = s$ , то  $\psi(s, x) = (s + 1) \bmod n$ , где  $n$  — количество символов алфавита открытых текстов (шифртекстов), которое равно числу состояний  $m$ . При вычислении функции выходов предлагается использовать обратимую операцию сложения целых чисел, а именно:  $\varphi(x, s) = (x + s) \bmod n$ . Таким образом, шифр Закревского на основе перестраиваемого автомата задаётся с помощью наиболее часто используемой в симметричных шифрах операции сложения по модулю.

Предложенная реализация перестраиваемого автомата описана на языке VHDL и промоделирована в САПР Xilinx WebPack ISE 14.1 на ПЛИС Spartan-3 XC3S50.

Результаты приведены в таблице (строки ШЗ-Ф), где представлены также результаты ПЛИС-реализации процедур шифрования и расшифрования шифра Закревского на основе перестраиваемого автомата, заданного таблицами переходов и выходов (строки ШЗ-Т), взятые из [1], и результаты реализации шифра AES [4]. Стоит отметить, что в работе [1] исследуется перестраиваемый автомат, у которого  $n = 16$ ,  $m = 8$ , а длина ключа 123 бита. В данной работе  $n = m = 16$  и длина ключа увеличена до 244 бит.

**Сравнение ПЛИС-реализаций шифра Закревского на основе перестраиваемого автомата при табличном и формульном задании**

Шифр	Ресурсоёмкость, Slices ( $S$ )	Производительность, Мбит/с ( $T$ )	Коэффициент эффективности $T/S$
ШЗ-Т (шифрование)	370	298	0,805
ШЗ-Т (расшифрование)	365	269	0,737
ШЗ-Ф (шифрование)	397	349	0,879
ШЗ-Ф (расшифрование)	398	366	0,920
AES	163	208	1,276

Из таблицы видно, что несмотря на некоторое усложнение конструкции (большее число состояний, большая длина ключа), производительность шифра Закревского на основе перестраиваемого автомата возросла на 17–36 %, при этом ресурсоёмкость увеличилась незначительно. Коэффициент эффективности реализации также увеличился, хотя и не достиг значения этой величины для AES. Однако AES опережает шифр Закревского на основе перестраиваемого автомата только за счёт меньшей ресурсоёмкости, что является существенным только для ПЛИС с небольшой логической ёмкостью (количеством вентиляей).

В целом, проведённые исследования показывают, что аппаратная реализация шифра Закревского на основе перестраиваемого автомата, заданного формулами, пригодна к использованию на практике.

#### ЛИТЕРАТУРА

1. Ковалев Д. С. Реализация на ПЛИС шифра Закревского на основе перестраиваемого автомата // Вестник Сибирского государственного аэрокосмического университета им. акад. М. Ф. Решетнёва. 2014. № 1 С. 16–18.
2. Закревский А. Д. Метод автоматической шифрации сообщений // Прикладная дискретная математика. 2009. № 2. С. 127–137.
3. Тренькаев В. Н. Реализация шифра Закревского на основе перестраиваемого автомата // Прикладная дискретная математика. 2010. № 3. С. 69–77.
4. Rowroy G., Standaert F. X., Quisquater J. J., and Legat J. D. Compact and efficient encryption/decryption module for FPGA implementation of the AES Rijndael very well suited for small embedded applications // Proc. Intern. Conf. Inform. Technology: Coding and Computing. 2004. V. 2. P. 583–587.

УДК 519.7

### ПРИМЕНЕНИЕ КОНЕЧНОГО АВТОМАТА ДЛЯ ОДНОВРЕМЕННОГО ПОИСКА НЕСКОЛЬКИХ ДВОИЧНЫХ ШАБЛОНОВ В ПОТОКЕ ДАННЫХ

И. В. Панкратов

Рассматривается задача поиска булевых векторов в потоке данных. Предлагается метод построения конечного автомата, который ищет одновременно несколько векторов, совершая только две простые операции на каждый бит или группу

битов. При этом с увеличением количества искомых шаблонов объём требуемой памяти растёт медленнее, чем суммарная длина шаблонов, а трудоёмкость не изменяется совсем. Приводится оценка количества состояний автомата.

**Ключевые слова:** поиск битовых последовательностей, поиск подстроки.

Рассматриваемую задачу можно сформулировать так. Имеем двоичную последовательность (поток данных) и набор булевых векторов (далее называемых *шаблонами*)  $V_1, V_2, \dots, V_n$  длин  $k_1, k_2, \dots, k_n$  соответственно. Необходимо найти вхождения всех шаблонов в последовательность.

В работе предлагается строить конечный автомат, на вход которого подаются биты или байты потока, а на выходе получается информация о найденных в потоке шаблонах. На каждый бит или байт потока автомат совершает две простейших операции: изменение состояния по таблице переходов и определение выхода по таблице выходов. При этом автомат осуществляет одновременный поиск произвольного количества шаблонов любых длин.

Опишем алгоритм построения битового автомата.

Входной алфавит автомата —  $\{0, 1\}$ .

Выходной алфавит — множество булевых векторов  $\{0, 1\}^n$ , где каждому биту сопоставлен шаблон из набора, и этот бит принимает значение 1, если шаблон закончился в текущей позиции.

Строится автомат по индукции. Сначала вводится нулевое состояние, соответствующее ситуации, когда не найден ни один префикс ни одного шаблона. Затем алгоритм поочерёдно обрабатывает все состояния условной подачей на вход автомата 0 и 1, попутно сохраняя новые полученные состояния и строя таблицы переходов и выходов автомата. Обработав таким образом все состояния автомата, получаем таблицы переходов и выходов, а также таблицу соответствия номеров состояний их описаниям: состоянию  $s$  сопоставляется набор  $T_s = (T_{s,1}, T_{s,2}, \dots, T_{s,n})$ , где  $T_{s,j}$  содержит множество длин найденных префиксов шаблона номер  $j$ .

Обозначим  $l$ -й бит вектора  $V$  через  $V[l]$ , биты нумеруем с нуля. В выходном векторе  $F$  бит  $F[j - 1]$  соответствует  $j$ -му шаблону.

---

### Алгоритм построения битового поискового автомата

---

**Вход:** набор булевых векторов (шаблонов)  $V_1, V_2, \dots, V_n$ , их длины  $k_1, k_2, \dots, k_n$

**Выход:** функции переходов  $\psi$  и выходов  $\varphi$  поискового автомата

1. Запоминаем начальное состояние  $T_0 := (\emptyset, \emptyset, \dots, \emptyset)$ ,  $s := 0$ .
2. Обрабатываем состояние  $s$  условной подачей нуля и единицы. Подаваемый бит обозначим  $b$ . Сначала зададим  $b := 0$ .
3. Строим новое состояние  $T$ , в которое автомат должен перейти после подачи бита  $b$  в состоянии  $T_s$ , и соответствующий выходной символ — вектор  $F$ ; сначала полагаем  $F := 00 \dots 0 = 0^n$ .

Для каждого  $j$  от 1 до  $n$ :

3.1. Зададим  $A := T_{s,j} \cup \{0\}$ ,  $B_j := \emptyset$ .

3.2. Для всех  $l \in A$  если  $b = V_j[l]$ , то  $B_j := B_j \cup \{l + 1\}$ .

Теперь множество  $B_j$  содержит длины всех найденных префиксов вектора  $V_j$  после подачи бита  $b$  в состоянии  $T_s$ .

3.3. Если  $k_j \in B_j$ , то вектор  $V_j$  найден; полагаем  $B_j := B_j \setminus \{l + 1\}$ ,  $F[j - 1] := 1$ .

4. Получили набор  $T := (B_1, B_2, \dots, B_n)$ , описывающий следующее состояние, и выходной символ автомата — вектор  $F$ . Ищем набор  $T$  среди имеющихся наборов  $T_0, \dots, T_s$ .  
**Если** нашли, что  $T = T_h$ , **то** присваиваем  $s' := h$ ;  
**если** такого состояния ещё нет, **то** добавляем его в таблицу в новую ячейку. Пусть номер этой ячейки  $s'$ . Тогда состояние  $T_{s'} = T$ .
5. Запоминаем  $\psi(s, b) := s'$ ,  $\varphi(s, b) := F$ .
6. **Если**  $b = 0$ , **то**  $b := 1$  и переход на шаг 3.
7.  $s := s + 1$ . **Если** в таблице есть состояние  $T_s$ , **то** переход на шаг 2.
8. Ответ: функции  $\psi$  и  $\varphi$ .

Имея автомат, принимающий на вход биты, можно построить автомат, принимающий на вход сразу пачки битов, например байты или полубайты. Будем называть такой автомат *байтовым*, а его входные векторы — байтами. Множество состояний у него такое же, как у битового автомата; входной алфавит  $\{0, 1\}^q$ , где  $q$  — число битов в байте; выходной алфавит сложнее, поскольку в байтовом автомате возможно нахождение сразу нескольких вхождений одного шаблона в различных позициях.

При наличии битового автомата таблицы переходов и выходов байтового автомата строятся просто: по очереди обрабатываются все состояния автомата и все возможные значения байта. Для каждой пары входного байта и состояния анализ происходит так: битовый автомат устанавливается в соответствующее состояние и на его вход побитно подаётся входной байт. Все выходные сигналы автомата собираются вместе и запоминаются с учётом того, при подаче какого бита был получен выходной сигнал. Новое состояние байтового автомата должно соответствовать состоянию, в которое перешёл битовый автомат после подачи всех битов байта.

Оценим количество состояний автомата.

У автомата, который ищет  $n$  векторов с длинами  $k_1, k_2, \dots, k_n$ , количество состояний ограничено сверху величиной  $\sum_{j=1}^n k_j - n + 1$ . Эта оценка достижима; в частности, автомат, ищущий один шаблон длины  $k$ , всегда имеет ровно  $k$  состояний.

Таким образом, предлагаемый поисковый автомат позволяет с очень высокой эффективностью одновременно искать в потоке данных несколько двоичных шаблонов. С увеличением количества шаблонов объём требуемой памяти растёт медленнее, чем их суммарная длина, а трудоёмкость не изменяется совсем.

Полностью результаты представлены в [1].

#### ЛИТЕРАТУРА

1. Панкратов И. В. Одновременный поиск нескольких двоичных шаблонов в потоке с помощью конечного автомата // Прикладная дискретная математика. 2014. № 2. С. 119–125.

Секция 10

## МАТЕМАТИЧЕСКИЕ ОСНОВЫ ИНФОРМАТИКИ И ПРОГРАММИРОВАНИЯ

УДК 004.43, 004.56

### ПРОГРАММНАЯ РЕАЛИЗАЦИЯ ОПЕРАЦИЙ НАД БОЛЬШИМИ ЧИСЛАМИ В ЯЗЫКЕ ЛЯПАС-Т

А. С. Грибанов, В. А. Сибирякова

Представлена информация о программной реализации в виде функций на языке Ассемблер операций языка ЛЯПАС-Т над большими числами. Эти функции вставляются компилятором в загружаемый модуль (файл с компилируемой программой). Реализованы два способа встраивания — через вызов подпрограммы и в виде макроса.

**Ключевые слова:** ЛЯПАС-Т, длинная арифметика.

В настоящее время в программировании большое внимание уделяется быстродействию программ, особенно в области задач компьютерной криптографии. Все в этой области стремятся к сокращению времени работы программ, ищут для этого альтернативные методы программирования, рассматривают возможности реализации программ на разных языках. Но, несмотря на все усовершенствования высокоуровневых языков, более быстрыми являются программы на языках, которые «ближе» к машинному языку, т. е. являются низкоуровневыми. Среди всех языков программирования язык Ассемблера является самым низкоуровневым, поэтому программы, написанные на нём должным образом, работают быстрее программ, представляющих те же алгоритмы на других языках.

В данной работе описываются функции на языке Ассемблер, реализующие арифметические операции языка программирования ЛЯПАС-Т [1] над большими числами, и способы встраивания их в загружаемый модуль.

#### Представление данных

В языке ЛЯПАС-Т все операции с длинными операндами выполняются с использованием в качестве одного из операндов собственной переменной  $\tau$ . В предлагаемой здесь программной реализации операций ЛЯПАСа-Т над большими числами последние и переменная  $\tau$  представляются логическими комплексами, как описано в [1], с той только разницей, что собственная переменная представляется фиксированным комплексом, называемым собственным. В программе этот комплекс хранится в стеке. Доступ к данным, хранящимся в стеке, осуществляется через смещение от корня стека (регистр  $\text{ebp}$ ). Младший элемент комплекса  $\tau$  расположен по адресу  $\text{ebp} - 64$ ;  $i$ -й элемент находится по адресу  $\text{ebp} - 64 - 4i$ . Мощность  $Q$  комплекса  $\tau$  хранится по адресу  $\text{ebp} + 112$ .

Когда цепочка операций начинается с некоторого комплекса  $Li$ , его значение копируется в комплекс  $\tau$ . Для любой последующей операции в цепочке комплекс  $\tau$  является первым операндом и результатом операции.

Далее опишем арифметические операции, интерпретирующие  $\tau$  как число длины  $32Q$  бит. Все они выполняются по модулю  $2^{32Q}$ . Пусть  $\circ \in \{-, +, *, /, ;\}$ . Тогда соответствующие операции могут быть выполнены следующим образом.

#### О п е р а ц и я $\circ$

Пример выполнения:  $L1 \circ L2 \Rightarrow L3$ . Операция выполнения действия  $\circ$  над числами  $L1$  и  $L2$  и занесения результата в  $L3$ . Выполняется записанная на языке ЛЯПАС-Т строка следующим образом:

- 1)  $L1$  копируется в  $\tau$ ;
- 2) над  $\tau$  и  $L2$  выполняется операция  $\circ$ . При этом результат находится в  $\tau$ , а комплекс  $L2$  не изменяется;
- 3) значение  $\tau$  копируется в комплекс  $L3$ .

Таким образом, после выполнения результата операции  $\circ$  над числами  $L1$  и  $L2$  находится в  $L3$  и в  $\tau$ .

Следующая операция отличается от предыдущих тем, что в результате её выполнения один из параметров изменяется.

#### Д е л е н и е (о п е р а ц и я «:»)

Пример выполнения:  $L1:L2 \Rightarrow L3$ .

Операция деления числа  $L1$  на число  $L2$  и занесения результата в  $L3$ . Выполняется записанная на языке ЛЯПАС-Т строка следующим образом:

- 1)  $L1$  копируется в  $\tau$ ;
- 2)  $\tau$  делится на  $L2$ . При этом результат (частное) находится в  $\tau$ , а в комплекс  $L2$  записывается остаток от деления. Таким образом,  $L2$  в результате выполнения операции «:» изменяется;
- 3) значение  $\tau$  копируется в комплекс  $L3$ .

Таким образом, после выполнения этой операции результат деления числа  $L1$  на число  $L2$  (частное) находится в  $L3$  и в  $\tau$ , а в  $L2$  — остаток от деления.

Все представленные операции используют функции, написанные на языке Ассемблер. Эти функции реализуют алгоритмы работы с длинными числами, описанные в книге Дональда Кнута [2], с минимальными изменениями.

Генерация ассемблерного кода, реализующего функции над большими операндами языка ЛЯПАС-Т, может выполняться двумя способами.

В первом случае функция оформляется как подпрограмма на языке Ассемблера с соблюдением всех соглашений о правилах определения подпрограмм в Ассемблере. Компилятором генерируются команды занесения входных аргументов операции в стек, затем команда вызова подпрограммы `call` и команды последующего анализа результатов работы подпрограммы.

Во втором случае в компиляторе определяются функции на языке C++, которые формируют строку из команд языка Ассемблера, реализующих действия над длинными операндами. Эта строка встраивается компилятором в общую строку, представляющую результат генерации целевой программы на Ассемблере.

Сравнивая эти подходы, можно сделать следующий вывод. В первом случае сокращается длина выходного кода, но увеличивается время его работы, так как вызов подпрограммы и возврат из неё занимают дополнительное время. Во втором случае имеем экономию времени работы за счёт отсутствия указанных действий, но увеличение длины кода, так как при появлении данных операций повторно соответствующий

код встраивается заново. В дальнейшем экспериментально будет проведён сравнительный анализ изложенных способов генерации.

Результатом работы является «состыковка» компилятора языка ЛЯПАС-Т, написанного на языке C++, с функциями работы с длинной арифметикой, написанными на языке Ассемблер. Таким образом, стала возможной работа с длинной арифметикой стандартными средствами языка ЛЯПАС-Т.

#### ЛИТЕРАТУРА

1. Агибалов Г. П., Липский В. Б., Панкратова И. А. О криптографическом расширении и его реализации для Русского языка программирования // Прикладная дискретная математика. 2013. № 3(21). С. 93–104.
2. Кнут Д. Искусство программирования. М.: Вильямс, 2001.

УДК 519.681.2

### РАЗРАБОТКА АВТОМАТИЗИРОВАННОГО СРЕДСТВА ДЛЯ ДОКАЗАТЕЛЬСТВА СВОЙСТВ ПРОГРАММ

А. О. Жуковская, Д. А. Стефанцов

Рассматривается метод статической верификации программ, основанный на автоматизированном доказательстве теорем. Моделью программы выбраны функции на парах списков натуральных чисел, упрощённой моделью — функции на натуральных числах. Исследуется свойство безопасности: программа может выдать секретное сведение, только если на вход был подан ключ. С помощью автоматизированного средства доказательства теорем Coq строятся доказательства для примеров функций, выводится общая схема построения доказательств, с помощью которой создаётся тактика Coq. В заключение приводятся идеи дальнейших исследований.

**Ключевые слова:** верификация программ, автоматизированное доказательство, Coq.

Для повышения надёжности компьютерных систем актуальна задача автоматической верификации программ. *Верификация программы* — доказательство её соответствия заданным формальным требованиям [1]. Существуют два основных метода верификации: *динамический*, при котором программа исследуется в процессе своей работы, и *статический*, при котором исследование происходит без запуска программы. В данной работе рассматривается статическая верификация. Под *программой* понимается синтаксически правильная последовательность команд на языке программирования, реализующая некоторую функцию. Для решения задачи верификации необходимы методы, позволяющие определить, обладает ли данная программа некоторым формально заданным свойством.

Имеет смысл рассматривать нетривиальное свойство, то есть такое, для которого существуют программы, обладающие им, но не все программы обладают им. В общем случае эта задача неразрешима в силу теоремы Райса — Успенского [2]. Поэтому алгоритм, устанавливающий, обладает ли программа заданным нетривиальным свойством, может не всегда выдавать результат или совершать ошибки первого (второго) рода.

Программа преобразует состояние потоков входа и выхода, состояние потока кодируется последовательностью чисел, поэтому за модель программы примем функцию на произведении списков  $f : \mathbb{N}^* \times \mathbb{N}^* \rightarrow \mathbb{N}^* \times \mathbb{N}^*$ . Для упрощения технических деталей

и в силу существования биективного соответствия между  $\mathbb{N}^* \times \mathbb{N}^*$  и  $\mathbb{N}$  можно принять упрощённую модель программы  $f : \mathbb{N} \rightarrow \mathbb{N}$ . Будем считать  $0 \in \mathbb{N}$  специальным значением.

В работе исследовано следующее важное свойство безопасности: программа  $f(x)$  может выдать секретное сведение  $s$ , только если на вход был подан  $x = k$ , где  $k$  — ключ. В силу принятой модели  $s, k \in \mathbb{N}$ .

Приведём примеры простейших программ (функций), обладающих данным свойством:

$$f_1(x) = \begin{cases} s, & \text{если } x = k, \\ 0 & \text{иначе;} \end{cases} \quad f_2(x) = x + (s - k); \quad f_3(x) = \begin{cases} 0, & \text{если } x = s, \\ x & \text{иначе.} \end{cases}$$

Для доказательства того, что функции обладают заданным свойством, использована система автоматизированного доказательства теорем Coq [3]. Для каждой из возможных функций  $f(x)$  построено доказательство соответствующей свойству безопасности теоремы:

$$\forall x, s, k \in \mathbb{N} \setminus \{0\} (f(x) = s \Rightarrow x = k).$$

Доказательства для разных функций схожи и строятся по следующей схеме:

- 1) рассматриваются все  $x$ ,  $0 < x < k$ , для них выполнение условия  $f(x) \neq s$  проверяется непосредственно;
- 2) значение  $f(k)$  допускается любым;
- 3) доказывается, что  $f(x)$  при  $x > k$  не может принять значения  $s$ .

Шаги 1 и 2 выполняются одинаково для всех функций; в шаге 3 возможны незначительные различия.

На основе этого написана новая тактика в системе Coq для доказательства выбранного свойства, автоматически выполняющая шаги 1 и 2 и для некоторых функций шаг 3. Тактика применима к нерекурсивным функциям.

Для облегчения трансляции с языка программирования удобнее использовать упрощённую модель представления программ в виде функций. Для функций на списках подходит такой же метод с модификацией способа реализации шагов. Рассмотрены аналогичные приведённым выше функции на списках, для них также построены доказательства соответствующей теоремы.

Наряду с рассмотрением вышеизложенного метода сделано предположение, что поставленную задачу можно решить иным способом. Для формализации программ существует система  $\lambda$ -исчисления [4]. Каждую функцию можно представить в виде терма  $\lambda$ -исчисления, которому можно присвоить тип по определённым правилам. Известен изоморфизм между типизированным  $\lambda$ -исчислением и интуиционистской логикой высказываний, являющийся частным случаем соответствия Карри — Говарда [5]. Таким образом, если сформулировать некое свойство программ в виде импликации в интуиционистской логике и представить исследуемую программу в виде терма типизированного  $\lambda$ -исчисления, можно проверить, соответствует ли полученный терм доказательству требуемого свойства, и в случае соответствия утверждать, что программа обладает данным свойством. Реализация этого метода — возможная тема для дальнейших исследований.

## ЛИТЕРАТУРА

1. Hoare T. The verifying compiler: a grand challenge for computing research // J. ACM. 2003. V. 50. No. 1. P. 63–69.

2. *Верещагин Н. К., Шень А.* Лекции по математической логике и теории алгоритмов. Ч. 3. Вычислимые функции. 4-е изд., испр. М.: МЦНМО, 2012.
3. <http://coq.inria.fr/>
4. *Барендрегт Х.* Лямбда-исчисление. Его синтаксис и семантика. М.: Мир, 1985.
5. *Пирс Б.* Типы в языках программирования. М.: Лямбда пресс & Добросвет, 2011.

Секция 11

## ВЫЧИСЛИТЕЛЬНЫЕ МЕТОДЫ В ДИСКРЕТНОЙ МАТЕМАТИКЕ

УДК 512.55

### ЭКСПЕРИМЕНТАЛЬНОЕ СРАВНЕНИЕ АЛГОРИТМОВ БАЛАША И ИМИТАЦИИ ОТЖИГА В ЗАДАЧЕ РЕШЕНИЯ СИСТЕМ ЛИНЕЙНЫХ НЕРАВЕНСТВ

Н. В. Анашкина, А. Н. Шурупов

Приводятся результаты сравнения двух эвристических методов применительно к решению систем псевдобулевых линейных неравенств — алгоритма Балаша и алгоритма имитации отжига, полученные в компьютерном эксперименте. Подтверждена большая эффективность и большее время работы алгоритма имитации отжига в сравнении с детерминированным методом Балаша. Приводятся рекомендации по совместному использованию алгоритмов. Предложена новая интерпретация случайного псевдобулевого линейного неравенства, которая может использоваться для определения эффективности эвристических методов решения указанной задачи.

**Ключевые слова:** алгоритм имитации отжига, алгоритм Балаша, линейные неравенства, случайные линейные неравенства.

Вещественное линейное неравенство от  $n$  переменных будем называть информативным, если задаваемая им гиперплоскость пересекает  $n$ -мерный булев куб. Булева пороговая функция (б.п.ф.), задаваемая неинформативным линейным неравенством, является константой. В случае, если определение б.п.ф. выглядит как  $f(x_1, \dots, x_n) = 0 \Leftrightarrow \sum_{i=1}^n w_i x_i \leq T$ , то множество б.п.ф., задаваемых информативными неравенствами указанного вида, включает в себя все б.п.ф., за исключением константной функции — единицы. Отметим, что в контексте решения систем уравнений использование только информативных неравенств в эквивалентной ей системе [1] линейных неравенств (СЛН) сокращает избыточность СЛН.

В дальнейшем будем рассматривать только целочисленные информативные линейные неравенства (ЦИЛН). Для решения СЛН были применены следующие эвристические алгоритмы, описание которых можно найти в [2, 3]: алгоритм имитации отжига и алгоритм Балаша. Задача решения СЛН интерпретируется как задача дискретной оптимизации на множестве значений булевых переменных, при этом подлежит минимизации целевая функция — невязка системы [2]. Система окрестностей алгоритма имитации отжига представляет собой шары радиуса 1 в смысле метрики Хемминга. Алгоритм Балаша использован в модификации, для которой в случае попадания алгоритма в тупиковое состояние предпринимается попытка выхода из него путём опробования состояний, находящихся от него на расстоянии 1.

Приведём описание плана эксперимента. Для алгоритма имитации отжига используются следующие значения параметров: длина стационарной цепи Маркова равна 50;

начальная температура — 20 000; тип шаговой функции для изменения температуры — закалка — со значением коэффициента 0,995; число шагов ограничено 100 000.

Для алгоритма Балаша число попаданий в тупиковые состояния ограничено 11.

Оба алгоритма применялись к каждой СЛН. Всего проведено 10 серий экспериментов по 800 систем в каждой серии. Серия состоит из восьми подсерий, при этом каждая подсерия задаётся числом переменных СЛН (30 или 60) и числом неравенств в ней, кратным числу переменных (коэффициент кратности равен 1, 2, 3 и 10).

Каждая серия задаётся типом неравенств в СЛН. Выбраны следующие характеристики СЛН: 1) наличие нулевых весов (да или нет); 2) максимальная абсолютная величина весов (1, 30 и 900); 3) использование точного значения порога (да или нет).

Отметим, что параметры эксперимента выбраны из соображений его продолжительности. Сами алгоритмы не имеют принципиальных ограничений на размер системы. Исследована также зависимость надёжности алгоритма имитации отжига от его параметров и, в частности, от системы окрестностей. Однозначной зависимости при увеличении радиуса шара с 1 до 2 обнаружить не удалось. Остальные параметры были выбраны достаточно произвольно на тестовых запусках алгоритма имитации отжига.

Для оценки в целом эффективности алгоритмов приведём суммарную таблицу, отражающую также корреляцию успеха между алгоритмами.

**Корреляция успеха между алгоритмами**

		Алг. Балаша		Итого для отжига, %
		Не решил, %	Решил, %	
Имитация отжига	Не решил, %	22	2	24
	Решил, %	15	61	76
Итого для алг. Балаша, %		37	63	

В целом, надёжность алгоритма имитации отжига выше, чем у алгоритма Балаша, хотя в одной из серий наблюдается обратное. Кроме того, в шести сериях алгоритм Балаша не решил ни одной системы, которую бы не решил алгоритм отжига. В среднем выигрыш во времени решения алгоритма Балаша составляет почти два порядка.

В качестве вывода из проведённого сравнения отметим, что подтверждена большая эффективность и большее время работы вероятностных методов локального поиска в сравнении с детерминированными. Показано, что в среднем совпадение решений происходит с вероятностью, близкой к 0,5. Таким образом, оба метода заслуживают использования при решении целочисленных СЛН.

Введём понятие случайной булевой пороговой функции (с.б.п.ф.) в соответствии с [4]. Пусть  $\xi$  — равномерно распределённая случайная величина, областью значений которой является множество всех булевых пороговых функций  $T_n$ . Тогда случайной булевой пороговой функцией  $f$  будем называть значение случайной величины  $\xi$ .

Пусть  $S$  — оракул, который задан на  $T_n$ , и при предъявлении ему б.п.ф. возвращает структуру этой б.п.ф. в виде ЦИЛН. *Случайным неравенством* будем называть случайную величину  $S(f)$ , где  $f$  — случайная б.п.ф., а *случайной системой линейных неравенств* (ССЛН) — выборку объёма  $t$  из  $S(f)$ .

В практическом плане важным является вопрос формирования ССЛН. При малом числе переменных ( $n < 9$ ) все б.п.ф. классифицированы, и для формирования ССЛН можно воспользоваться соответствующими справочниками (см., например, [5]). Этот способ становится неприемлемым при  $n > 8$ , так как в этом случае отсутствуют способы перечисления б.п.ф. Известно [6, с. 12; 7, теорема 9.12, с. 413], что для любой б.п.ф. от  $n$  переменных найдётся структура, для которой максимальные абсолютные значе-

ния весов и порога ограничены некоторой величиной  $W(n)$ . Будем считать, что на множестве целых чисел  $I(W(n)) = \{-W(n), -W(n) + 1, \dots, 0, \dots, W(n) - 1, W(n)\}$ , используемых для выбора весов, задано некоторое вероятностное распределение  $F$ . Так как структура — неоднозначный способ задания, то важной является задача подбора вероятностного распределения  $F$  для реализации равномерного распределения на  $T_n$ . Предлагается алгоритм для порождения ССЛН, в котором условие информативности формулируется как  $\frac{1}{2} \sum_{i=1}^n w_i - \|w\| \sqrt{n} \leq T \leq \frac{1}{2} \sum_{i=1}^n w_i + \|w\| \sqrt{n}$ , где  $\|w\|$  — евклидова норма вектора весов.

Неочевидно, что равномерное распределение  $F$  целых весов  $w_i$  в множестве  $I(W(n))$  и равномерное распределение порогов индуцируют равномерное распределение на множестве б.п.ф. Представляется более удачным использовать неравномерное распределение  $F$ , являющееся квантованным усеченным нормальным распределением, так как на поведение гиперплоскости в большей степени влияют знаки весов, а не их абсолютные величины. В ряде работ (например, [8]) рассмотрены случайные неравенства с весами из множества  $\{-1, 1\}$ , проходящие через центр единичного куба. Каждое такое неравенство задаёт равновероятную б.п.ф., и поэтому, очевидно, не удовлетворяет определению случайного неравенства.

Как правило, число неравенств  $m$  определяется прикладными аспектами задачи, для которой составляется СЛН.

Более подробно изложенные результаты представлены в [9].

#### ЛИТЕРАТУРА

1. Балакин Г. В., Никонов В. Г. Методы сведения булевых уравнений к системам пороговых соотношений // Обзорение прикладной и промышленной математики. 1994. Т. 1. Вып. 3. С. 389–401.
2. Анашкина Н. В. Обзор методов решения систем линейных неравенств // Вестник московского университета леса. Лесной вестник. 2004. № 1(32). С. 144–148.
3. Кочетов Ю. А. Вероятностные методы локального поиска для задач дискретной оптимизации // Дискретная математика и ее приложения: Сб. лекций молодежных и научных школ по дискретной математике и ее приложениям. М.: Изд-во центра прикл. исслед. при мех.-мат. фак. МГУ, 2001. С. 84–117.
4. Goldwasser S. and Bellare M. Lecture Notes on Cryptography. 2001. <http://theory.lcs.mit.edu/shafi>. 283 p.
5. Muroga S., Tsuboi T., and Baugh C. R. Enumeration of threshold functions of eight variables // IEEE Trans. Comput. 1970. V. C-19. Iss. 9. P. 818–825.
6. Подольский В. В. Оценки весов перцептронов (полиномиальных пороговых булевых функций): автореф. дис. ... канд. физ.-мат. наук. М.: МГУ им. М. В. Ломоносова, 2009.
7. Crama Y. and Hammer P. Boolean Functions. Theory, Algorithms and Applications. Encyclopedia of Mathematics and its Applications / eds. G.-C. Rota. Cambridge University Press, 2011.
8. Балакин Г. В. Линейные псевдобулевы неравенства // Математические вопросы криптографии. 2010. Т. 1. Вып. 3. С. 5–18.
9. Анашкина Н. В., Шурупов А. Н. Применение алгоритмов локального поиска к решению систем псевдобулевых линейных неравенств // Прикладная дискретная математика. 2014. № 3(25) (в печати).

УДК 519.178

## СТРУКТУРНАЯ ДЕКОМПОЗИЦИЯ ГРАФА И ЕЁ ПРИМЕНЕНИЕ ДЛЯ РЕШЕНИЯ ОПТИМИЗАЦИОННЫХ ЗАДАЧ НА РАЗРЕЖЕННЫХ ГРАФАХ

В. В. Быкова

Формализовано понятие разреженного графа через числовой параметр, известный как древовидная ширина графа. Предложен декомпозиционный подход решения оптимизационных задач на разреженных графах. Этот подход реализует принцип «разделяй и властвуй» и основан на атомарном представлении входного графа. Показано, что атомарное представление графа может быть построено за полиномиальное время. Приведены свойства атомов, определяющие границы применения предлагаемого подхода. Представлены результаты использования атомарного представления графа в решении двух оптимизационных задач: вычисление кратчайших путей и нахождение наибольшей клики графа. Время выполнения результирующих алгоритмов линейно зависит от числа вершин входного графа, что позволяет с их помощью обрабатывать разреженные графы большой размерности за реальное время.

**Ключевые слова:** *разреженный граф, алгоритмы на графах, древовидная ширина, дерево декомпозиции, атом графа.*

В современных приложениях приходится иметь дело с гигантскими графами, содержащими несколько миллионов вершин. Например, такие графы возникают при моделировании крупных поисковых систем, телекоммуникационных сетей, финансовых и рыночных структур. Для хранения описаний гигантских графов используется внешняя память компьютеров, а их обработка ведётся с помощью операций ввода-вывода. Всё это приводит к существенному снижению эффективности классических алгоритмов решения оптимизационных задач на графах. Решение этой проблемы следует искать в подходах, основанных на особенностях обрабатываемых графов. Замечено, что гигантским графам, возникающим в различных приложениях, присущи следующие свойства: разреженность — они имеют мало рёбер по сравнению с числом вершин; «скученность» — в этих графах наблюдаются семейства вершин с высокой степенью; сравнительно небольшой диаметр, что обеспечивает высокий уровень достижимости из одной вершины другой. Графы с подобными свойствами названы графами «тесного мира» (Small World Graphs, SWG) [1–3]. В настоящее время их изучение осуществляется с использованием вероятностных и детерминированных моделей. В первом случае моделью служат случайные графы Эрдеша — Реньи и Барабаши — Альберт [4], а во втором — обычные детерминированные разреженные графы. Вероятностные модели применяются для установления структурных характеристик SWG, таких, как коэффициент кластеризации, средняя длина пути и др. В рамках детерминированного подхода исследуются вычислительные технологии, расширяющие возможности классических алгоритмов обработки SWG. В данной работе предлагается детерминированный декомпозиционный подход решения оптимизационных задач для разреженных графов. Рассматриваются только простые графы, т. е. конечные неориентированные графы без петель и кратных рёбер. Используются понятия и обозначения, принятые в [5–7].

Уточним понятие разреженности графа. Связный граф  $G = (V, E)$  называют разреженным (или неплотным), если число его рёбер  $|E|$  удовлетворяет условию

$$|E| \leq \alpha n^\beta, \quad (1)$$

где  $\alpha > 0$ ,  $1 \leq \beta < 2$  — положительные вещественные константы и  $n = |V|$ . Считают, чем меньше значение  $\beta$ , тем более разреженным является граф  $G$ . Для сравнения, в каждом дереве число рёбер равно  $n - 1$ , что отвечает нижней границе значения  $\beta$ , а для любого полного  $n$ -вершинного графа  $|E| = n(n - 1)/2$ , что соответствует верхней границе значения  $\beta$ . Существует другое, более тонкое определение разреженного графа, которое выражается через числовой параметр, называемый древовидной шириной графа. Данный параметр в большей степени отражает внутреннюю структуру графа, чем соотношение (1). Он показывает, насколько близок граф  $G$  к дереву, а также ограничивает размеры его клик и сепараторов.

Напомним, что множество вершин  $S$  — клика графа  $G = (V, E)$ , если подграф  $G(S)$  графа  $G$ , индуцированный множеством  $S \subseteq V$ , является полным. Говорят, что множество  $S \subseteq V$  разделяет несмежные вершины  $a$  и  $b$  графа  $G = (V, E)$ , если вершины  $a$  и  $b$  принадлежат различным компонентам связности графа  $G(V \setminus S)$ . Множество  $S$  при этом называют  $(a, b)$ -сепаратором, а также — минимальным  $(a, b)$ -сепаратором, если в нём нет собственного подмножества, являющегося  $(a, b)$ -сепаратором. Сепаратор  $S$  минимальный, если в  $G$  существует такая пара вершин  $a$  и  $b$ , что  $S$  является минимальным  $(a, b)$ -сепаратором. Множество  $S \subseteq V$  считают кликовым минимальным сепаратором графа  $G$ , если  $S$  образует в  $G$  одновременно клику и минимальный сепаратор.

Древовидная ширина связного графа вычисляется через специальное представление этого графа — дерево декомпозиции. Дерево декомпозиции графа  $G = (V, E)$  определяется как пара  $(M, T)$ , задающая некоторое разбиение множества вершин и множества рёбер данного графа. При этом  $M = \{X_i \subseteq V : i \in I\}$  — семейство подмножеств множества  $V$ , именуемых «мешками», а  $T = (I, W)$  — помеченное дерево, каждому узлу которого сопоставляется некоторый «мешок» из  $M$ . Для всякого дерева декомпозиции  $(M, T)$  графа  $G = (V, E)$  семейство «мешков»  $M$  и множество рёбер  $W$  дерева  $T = (I, W)$  обязательно должны удовлетворять следующим трём условиям: объединение всех «мешков» совпадает с множеством вершин  $V$  графа  $G$ ; для всякого ребра графа  $G$  обязательно имеется хотя бы один «мешок», содержащий обе вершины этого ребра; для любой вершины графа  $G$  множество узлов дерева  $T$ , «мешки» которых содержат эту вершину, индуцирует связный подграф, являющийся поддеревом дерева  $T$  [6]. Всякое дерево декомпозиции  $(M, T)$  графа  $G$  характеризуется шириной, значение которой вычисляется по формуле  $\max\{|X_i| - 1 : i \in I\}$ . Для одного и того же графа может быть построено несколько различных деревьев декомпозиции, каждому из которых присуща некоторая ширина. Древовидная ширина графа  $G = (V, E)$  определяется как наименьшая ширина всех допустимых его деревьев декомпозиции и обозначается через  $\text{tw}(G)$ . Так, всякое  $n$ -вершинное дерево ( $n \geq 2$ ) имеет единичную древовидную ширину, а полному  $n$ -вершинному графу свойственна древовидная ширина равная  $n - 1$ .

Пусть  $k$  — некоторая заданная положительная целая константа и  $k < n = |V|$ . Если  $\text{tw}(G) \leq k$ , то говорят, что граф  $G = (V, E)$  обладает ограниченной (значением  $k$ ) древовидной шириной. Считается, чем меньше значение  $k$ , тем более разреженным является граф  $G$ . Известно, что если  $\text{tw}(G) \leq k$ , то для числа рёбер графа  $G = (V, E)$  справедливо неравенство

$$|E| \leq kn - k(k + 1)/2. \quad (2)$$

Подстановка в (2) значений  $k = 1$  и  $k = n - 1$  приводит к неравенствам (1), соответствующим деревьям и полным графам. Следовательно, ограничение на древовидную

ширину графа  $G$  не противоречит условию (1) и задает естественную меру разреженности этого графа. Подмечено, что большинство графов «тесного мира» имеют малую древовидную ширину (как правило, для них значение  $k$  не превышает 6). Далее будем полагать, что граф  $G$ , для которого требуется найти точное решение некоторой оптимизационной задачи, обладает ограниченной древовидной шириной, т. е.  $\text{tw}(G) \leq k$ , и при этом значение  $k$  намного меньше числа вершин графа  $G$ . Кроме того, будем считать, что этот граф имеет кликовые минимальные сепараторы. Эти предположения определённым образом формализуют свойства разреженности и «скученности» входного графа. Подобная формализация данных свойств объясняется следующими особенностями дерева декомпозиции [5]: это дерево представляет граф с точностью до клик и сепараторов, так как всякая клика графа всегда находится в отдельном «мешке»; пересечение «мешков» двух соседних узлов дерева декомпозиции задаёт сепаратор графа; чем меньше древовидная ширина графа, тем ближе этот граф к дереву и тем меньше у него по мощности клики и сепараторы.

Суть предлагаемого декомпозиционного подхода — это сведение решаемой задачи для разреженного графа большой размерности к конечному множеству таких задач для графов меньшей размерности. Процесс решения включает в себя три этапа. На первом этапе выполняется разбиение входного графа  $G = (V, E)$  на конечное множество атомов  $\Omega(G)$ . Множество  $\Omega(G)$  будем называть атомарным представлением графа  $G$ . Здесь атом графа  $G$  — это максимальный относительно включения связный его подграф, не имеющий кликовых минимальных сепараторов. Второй этап — это решение задачи для каждого образованного атома с помощью некоторого известного классического алгоритма. И наконец, на третьем этапе осуществляется построение решения задачи для графа  $G$  путём попарного соединения (или связывания) решений, полученных для всех его атомов. С вычислительной точки зрения такой декомпозиционный подход целесообразен, если выполнены следующие условия: атомарное представление  $\Omega(G)$  входного графа  $G = (V, E)$  может быть построено за полиномиальное время; атомарное представление  $\Omega(G)$  допускает корректное связывание решений, выполняемое на третьем этапе; количество атомов в  $\Omega(G)$  не превосходит числа вершин графа  $G$ ; число вершин каждого атома из  $\Omega(G)$  ограничено сверху некоторой положительной целой константой  $k < n = |V|$ . В работе показано, что если входной граф обладает малой древовидной шириной и содержит кликовые минимальные сепараторы, то эти требования выполнимы. При этом атомарное представление  $\Omega(G)$  графа  $G = (V, E)$  может быть построено за время  $O(n^\tau)$ ,  $2 \leq \tau < 3$ .

Заметим, что атомарное представление  $\Omega(G)$  графа  $G$  является обобщением разложения его на блоки: когда множество кликовых минимальных сепараторов состоит лишь из точек сочленения графа  $G$ , каждый атом из  $\Omega(G)$  представляет собой блок этого графа. Известно, что разложение графа на блоки уникально [7]. Аналогичное утверждение справедливо также для атомарного представления графа [5]: если множество  $\Omega(G)$  формировать лишь на основе кликовых (и никаких других) минимальных сепараторов, то  $\Omega(G)$  уникально для всякого связного графа  $G$ . Отметим наиболее важные свойства атомов: всякий атом из  $\Omega(G)$  является индуцированным подграфом графа  $G$ ; если граф  $G$  имеет ограниченную (значением  $k$ ) древовидную ширину, то число вершин каждого атома не превышает  $k$ ; множество  $\Omega(G)$  сохраняет все клики графа  $G$ , т. е. всякая клика графа  $G$  становится кликой одного из его атомов и новых клик при разложении не возникает. Таким образом, атомарное представление графа применимо к оптимизационным задачам на графах, базирующимся на отношении смежности. К ним, в частности, относятся такие задачи: поиск кратчайших пу-

тей, нахождение наибольшей клики, вычисление хроматического числа, определение наибольшего независимого множества вершин графа, поиск наименьшего пополнения графа до хордального, распознавание класса совершенных графов и др. Большинство из этих задач являются NP-трудными.

В работе атомарное представление графа применено к двум оптимизационным задачам: вычислению кратчайших путей для всех пар вершин взвешенного графа (All-Pairs Shortest-Path, APSP) и нахождению наибольшей клики графа (Maximum-Clique-Problem, MCP). Первая задача полиномиально разрешимая, а вторая NP-трудная. Совместное использование алгоритма Флойда — Уоршолла [7] и атомарного представления входного  $n$ -вершинного графа позволяет находить точное решение задачи APSP за время  $O(nk^3)$ . Применение алгоритма Уилфа [7] к каждому атому и связывание решений, полученных для всех атомов входного графа, приводит к точному решению задачи MCP за время  $O(n \cdot 1,39^k)$ . Заметим, что в обоих случаях время нахождения решения линейно зависит от  $n$ . Кроме того, чем меньше значение  $k$ , т. е. чем более разреженным является входной граф, тем быстрее работает алгоритм.

Таким образом, предложенный декомпозиционный подход даёт возможность создавать алгоритмы, способные за реальное время обрабатывать разреженные графы большой размерности.

#### ЛИТЕРАТУРА

1. Gardiner E., Willett P., and Artymiuk P. Graph-theoretic techniques for macromolecular docking // J. Chem. Inf. Comput. 2000. No. 40. P. 273–279.
2. Broder A., Kumar R., Maghoul F., et al. Graph structure in the Web // Comput. Networks. 2000. V. 33. P. 309–320.
3. Boginski V., Butenko S., and Pardalos P. M. Mining market data: A network approach // Comput. & Operat. Res. 2006. No. 33. P. 3171–3184.
4. Колчин В. Ф. Случайные графы. М.: Физматлит, 2004.
5. Быкова В. В. О разложении гиперграфа кликовыми минимальными сепараторами // Журнал Сибирского федерального университета. Математика и физика. 2012. №1(5). С. 36–45.
6. Быкова В. В. FPT-алгоритмы на графах ограниченной древовидной ширины // Прикладная дискретная математика. 2012. №2(16). С. 65–78.
7. Емеличев В. А., Мельников О. И., Сарванов В. И., Тышкевич Р. И. Лекции по теории графов. М.: Книжный дом «ЛИБРОКОМ», 2012.

УДК 519.1

### ФОРМАЛИЗАЦИЯ КОМБИНАТОРНЫХ ЧИСЕЛ В ТЕРМИНАХ ЦЕЛОЧИСЛЕННЫХ РЕШЕНИЙ СИСТЕМ ЛИНЕЙНЫХ ДИОФАНТОВЫХ УРАВНЕНИЙ

В. В. Гоцуленко

Рассмотрены некоторые обобщения числа размещений с повторениями при различных типах ограничений. Подсчёт данных комбинаторных чисел приводит к определению числа целых неотрицательных решений систем линейных диофантовых уравнений при соответствующих дополнительных ограничениях. Получены производящие функции и интегральные формулы для вычисления введённых

комбинаторных чисел и рассмотрены различные задачи, которые решаются с их применением.

**Ключевые слова:** комбинаторные числа, системы линейных диофантовых уравнений, производящие функции.

В работе вводятся в рассмотрение комбинаторные числа размещений с повторениями при различных дополнительных ограничениях [1]. Формулировка достаточно общей комбинаторной задачи, приводящей к размещениям с повторениями при рассматриваемых ограничениях, может быть следующей [2]. Предположим, что имеется  $N$  различных ящиков, в каждом из которых находится достаточно большое (например, бесконечное) число конфет  $q$  различных видов. Конфеты упакованы по коробкам. Известно, что в  $i$ -м ящике ( $i = 1, \dots, N$ ) конфеты  $j$ -го вида ( $j = 1, \dots, q$ ) упакованы в коробки вместительностью по  $r_{i,s}^j$  ( $s = 1, \dots, n_{ij}$ ) штук, где  $n_{ij}$  — число объёмов коробок  $i$ -го ящика, в которых находятся конфеты  $j$ -го вида. Пусть также имеется  $R$  детей, которым необходимо дать конфеты из этих  $N$  ящиков. При этом  $k$ -му ребёнку ( $k = 1, \dots, R$ ) необходимо дать ровно  $m_{jk}$  конфет  $j$ -го вида. Необходимо, чтобы суммарное число конфет всех коробок, взятых из  $i$ -го ящика для  $k$ -го ребёнка, было равно  $p_{ik}$ , где  $p_{ik}$  — фиксированные целые неотрицательные числа. Также требуется, чтобы суммарное число всех конфет  $j$ -го вида, розданных всем детям из  $i$ -го ящика, было равно наперёд заданному целому неотрицательному числу  $d_{ij}$ . Любое допустимое распределение конфет  $q$  видов  $R$  детям из  $N$  различных ящиков будем называть обобщённым  $q$ -размещением из  $N$  по  $R$  при жёстких ограничениях.

Если безразлично, сколько конфет каждого вида необходимо раздать детям из каждого ящика, то допустимое распределение конфет  $q$  видов  $R$  детям из  $N$  различных ящиков будем называть обобщённым  $q$ -размещением из  $N$  по  $R$  при мягких ограничениях. В последнем случае будем предполагать, что для  $k$ -го ребёнка ( $k = 1, \dots, R$ ) задано число конфет  $m_k$ , которые необходимо ему дать из всех  $N$  ящиков. Также предполагается заранее заданным  $p_i$  — суммарное число конфет, которое разрешается взять из  $i$ -го ящика ( $i = 1, \dots, N$ ).

Как в первом, так и во втором случаях на выборку конфет из ящиков возможны различные ограничения. Рассмотрим следующие три типа ограничений:

- A) Конфеты во всех ящиках находятся не в коробках, а россыпью (т.е.  $r_{i,s}^j = 1$  для всех  $i, j, s$ ) и из каждого ящика разрешается брать любое допустимое число конфет.
- B) Из каждого ящика разрешается брать не более одной допустимой коробки конфет каждого вида.
- C) Разрешается брать любое число допустимых коробок конфет каждого вида из любого ящика.

Обозначим через  $x_{ijk}$  число конфет  $j$ -го вида, взятых из  $i$ -го ящика  $k$ -му ребёнку. Тогда при жёстких ограничениях приходим к следующей системе линейных диофантовых уравнений ( $i = 1, \dots, N$ ,  $j = 1, \dots, q$ ,  $k = 1, \dots, R$ ):

$$\sum_{i=1}^N x_{ijk} = m_{jk}; \quad \sum_{j=1}^q x_{ijk} = p_{ik}; \quad \sum_{k=1}^R x_{ijk} = d_{ij}. \quad (1)$$

При мягких ограничениях получается система уравнений

$$\sum_{i=1}^N \sum_{j=1}^q x_{ijk} = m_k; \quad \sum_{j=1}^q \sum_{k=1}^R x_{ijk} = p_i, \quad i = 1, \dots, N, \quad k = 1, \dots, R. \quad (2)$$

В случае «B» областью допустимых значений для (1) и (2) являются множества

$$x_{ijk} \in \{r_{i,s}^j : 1 \leq s \leq n_{ij}\} \cup \{0\}, \quad i = 1, \dots, N, \quad j = 1, \dots, q, \quad k = 1, \dots, R. \quad (3)$$

Введём в рассмотрение множества целых чисел ( $i = 1, \dots, N, j = 1, \dots, q$ )

$$I_{ij} = I_{ij} \left( \{r_{is}^j\}_{N \times n_{ij}}^q \right) = \left\{ \sum_{s=1}^{n_{ij}} \alpha_s r_{i,s}^j : \alpha_s \in \mathbb{N} \cup \{0\}, s = 1, \dots, n_{ij} \right\},$$

$$J_{ij} = J_{ij} \left( P, \{r_{is}^j\}_{N \times n_{ij}}^q \right) = \left\{ r \in I_{ij} \left( \{r_{is}^j\}_{N \times n_{ij}}^q \right) : r \leq P \right\}, \quad P \in \mathbb{N}.$$

Тогда для задачи «C» множествами допустимых решений для (1) и (2) являются

$$x_{ijk} \in J_{ij} \left( \min \{m_{jk}, p_{ik}, d_{ij}\}, \{r_{is}^j\}_{N \times n_{ij}}^q \right), \quad i = 1, \dots, N, \quad j = 1, \dots, q, \quad k = 1, \dots, R. \quad (4)$$

Таким образом, вычисление введённых комбинаторных чисел сводится к определению числа целых неотрицательных решений систем уравнений (1) или (2) без ограничений, а также при ограничениях (3) или (4). Установлено, что число всех целых неотрицательных решений системы уравнений (1) равно коэффициенту при  $t_1^{b_1} t_2^{b_2} \dots t_K^{b_K}$  в разложении по возрастающим показателям степеней  $t_1^{r_1} t_2^{r_2} \dots t_K^{r_K}$  следующей производящей функции ( $\alpha = 1, \dots, K, \beta = 1, \dots, M$ ):

$$\Psi(t_1, t_2, \dots, t_K) = \prod_{\beta=1}^M \left( 1 - \prod_{\alpha=1}^K t_\alpha^{a_{\alpha\beta}} \right)^{-1}, \quad \text{где } M = NqR, \quad K = Nq + qR + NR, \quad (5)$$

$$\nu_{n_1, n_2}(r) = (r_1, r_2), \quad r_1 = 1 + \left\lfloor \frac{r-1}{n_2} \right\rfloor, \quad r_2 = 1 + n_2 \left\{ \frac{r-1}{n_2} \right\}, \quad r = 1, \dots, n_1 n_2,$$

$$\psi(\beta) = (i, j, k), \quad \psi_1(\beta) = i, \quad \psi_2(\beta) = j, \quad \psi_3(\beta) = k, \quad \psi_{21}(\beta) = (j, k), \quad \psi_{22}(\beta) = (i, k),$$

$$\psi_{23}(\beta) = (i, j), \quad i = 1 + \left\lfloor \frac{1}{q} \left\lfloor \frac{\beta-1}{R} \right\rfloor \right\rfloor, \quad j = 1 + q \left\{ \frac{1}{q} \left\lfloor \frac{\beta-1}{R} \right\rfloor \right\}, \quad k = 1 + R \left\{ \frac{\beta-1}{R} \right\}.$$

$$a_{\alpha\beta} = \begin{cases} 1, & \text{если } 1 \leq \alpha \leq qR, \quad \nu_{q,R}(\alpha) = \psi_{21}(\beta), \\ 1, & \text{если } qR + 1 \leq \alpha \leq qR + NR, \quad \nu_{N,R}(\alpha - qR) = \psi_{22}(\beta), \\ 1, & \text{если } qR + NR + 1 \leq \alpha \leq qR + NR + Nq, \quad \nu_{N,q}(\alpha - qR - NR) = \psi_{23}(\beta), \\ 0 & \text{в остальных случаях;} \end{cases}$$

$$b_\alpha = \begin{cases} m_{jk}, & \text{если } 1 \leq \alpha \leq qR, \quad \nu_{q,R}(\alpha) = (j, k), \\ p_{ik}, & \text{если } qR + 1 \leq \alpha \leq qR + NR, \quad \nu_{N,R}(\alpha - qR) = (i, k), \\ d_{ij}, & \text{если } qR + NR + 1 \leq \alpha \leq qR + NR + Nq, \quad \nu_{N,q}(\alpha - qR - NR) = (i, j). \end{cases}$$

Установлено также, что число всех целочисленных решений системы уравнений (1) при условии (3) равно коэффициенту при  $t_1^{b_1} t_2^{b_2} \dots t_K^{b_K}$  в разложении по возрастающим показателям степеней  $t_1^{r_1} t_2^{r_2} \dots t_K^{r_K}$  следующей производящей функции:

$$\Psi(t_1, t_2, \dots, t_K) = \prod_{\beta=1}^M \left( 1 + \sum_{k=1}^{n_{\psi_1(\beta), \psi_2(\beta)}} \prod_{\alpha=1}^K t_\alpha^{a_{\alpha\beta} r_{\psi_1(\beta), k}} \right). \quad (6)$$

Аналогично, производящей функцией для определения числа целых неотрицательных решений системы уравнений (1) при ограничениях (4) является функция

$$\Psi(t_1, t_2, \dots, t_K) = \prod_{\beta=1}^M \sum_{r \in J_{\psi_{23}(\beta)} \left( D_{\psi(\beta)}, \{r_{is}^j\}_{N \times n_{ij}}^q \right)} \prod_{\alpha=1}^K t_\alpha^{a_{\alpha\beta} r}. \quad (7)$$

Полагая в (5)–(7)  $K = R + N$ ,  $M = RN$ ,

$$a_{\alpha\beta} = \begin{cases} 1, & \text{если } 1 \leq \alpha \leq R, \psi_3(\beta) = \alpha, \\ 1, & \text{если } R + 1 \leq \alpha \leq R + N, \psi_1(\beta) = \alpha - R, \\ 0 & \text{в остальных случаях;} \end{cases}$$

$$b_\alpha = \begin{cases} m_i, & \text{если } 1 \leq \alpha \leq R, \alpha = i, \\ p_k, & \text{если } R + 1 \leq \alpha \leq R + N, \alpha - R = k, \end{cases}$$

получим производящие функции для числа целых неотрицательных решений системы (2) без ограничений, а также соответственно при ограничениях (3) и (4).

#### ЛИТЕРАТУРА

1. Яблонский С. В. Введение в дискретную математику. М.: Наука, 1986. 384 с.
2. Гоцуленко В. В. Формула для числа сочетаний с повторениями при ограничениях и её применение // Прикладная дискретная математика. 2013. № 2(20). С. 71–77.

УДК 519.6

### АЛГОРИТМ ГЕНЕРАЦИИ ПАРЫ ПРОСТЫХ ЧИСЕЛ СПЕЦИАЛЬНОГО ВИДА

К. Д. Жуков, А. С. Рыбаков

Рассматривается алгоритм генерации пары простых чисел  $p$  и  $q$ , таких, что числа  $g = \frac{1}{2}(p - 1, q - 1)$  и  $h = \frac{1}{2g}(pq - 1)$  также простые. Такие простые числа впервые рассмотрены в 2006 г. М. Дж. Хинеком в связи с предложенной им модификацией криптосистемы RSA, устойчивой к атакам на малые секретные экспоненты. Приводятся экспериментальные данные о времени работы алгоритма.

**Ключевые слова:** *простые специального вида, Common Prime RSA.*

В 2006 г. М. Дж. Хинек предложил вариант криптосистемы RSA, устойчивой к атакам на малую секретную экспоненту, которая была названа Common Prime RSA. Простые сомножители  $p$  и  $q$  модуля Common Prime RSA выбираются такими, чтобы числа

$$g = \frac{1}{2}(p - 1, q - 1), \quad h = \frac{1}{2g}(pq - 1) \quad (1)$$

были также простыми, причём число  $g$  должно быть достаточно большим.

Система Common Prime RSA не получила распространения. Этот факт связан с малым количеством публикаций по её анализу. Большинство атак на данную разновидность RSA были также предложены М. Дж. Хинеком (см., например, [2]). Не способствует распространению и отсутствие острой необходимости использовать малые секретные экспоненты; другим сдерживающим фактором использования Common Prime RSA является долгая генерация ключей.

Простейшая версия алгоритма генерации простых сомножителей модуля криптосистемы Common Prime RSA, предложенная в [1], описана ниже.

---

**Алгоритм 1.** (Хинек, [1])

---

**Вход:** натуральные  $n$  и  $m$ ,  $m < n$ **Выход:** пара  $n$ -битовых простых чисел  $p$  и  $q$ , таких, что  $g$  и  $h$ , определяемые равенствами (1), простые, а  $g$  имеет битовый размер  $m$ 1: Выбрать случайное простое  $m$ -битовое число  $g$ .2: **Повторять**3: Выбрать случайные положительные целые  $(n - m - 1)$ -битовые числа  $a$  и  $b$ ;4:  $p := 2ga + 1$ ,  $q := 2gb + 1$ ,  $h := 2gab + a + b$ 5: **Пока**  $p$ ,  $q$ ,  $h$  — не простые или  $(a, b) \neq 1$ ;6: **Вывести**  $p$ ,  $q$ .

---

В работе [1] отмечается, что алгоритм 1 не оптимизирован. Отметим, что простые числа можно генерировать в двух независимых подциклах. Кроме того, эксперименты показывают, что неудачный выбор простого числа  $g$  может привести к тому, что время работы алгоритма будет существенно больше среднего времени работы для заданных параметров  $n$  и  $m$ . Отсюда целесообразно генерировать простое число  $g$  внутри цикла.

Заметим, что самой частой и трудоёмкой операцией алгоритма является тест на простоту. На его первом этапе проверяется, что число не делится на малые простые. Этот этап можно ускорить, учитывая специальный вид простых. Например, вместо проверки условия  $r \mid (2ga + 1)$  нужно проверять условие  $a \equiv (-2g)^{-1} \pmod{r}$  для малого простого  $r$ .

---

**Алгоритм 2**

---

**Вход:** натуральные  $n$  и  $m$ ,  $m < n$ ; натуральный параметр метода  $k$ **Выход:** пара  $n$ -битовых простых чисел  $p$  и  $q$ , таких, что  $g$  и  $h$ , определяемые равенствами (1), простые, а  $g$  имеет битовый размер  $m$ 1: Построить  $k$  первых простых чисел  $p_1, \dots, p_k$ .2: **Повторять**3: Используя технику просеивания, выбрать случайное простое  $m$ -битовое число  $g$ .4: Вычислить  $g_i := (-2g)^{-1} \pmod{p_i}$  для всех  $i = 1, \dots, k$ .5: **Повторять**6: Используя технику просеивания, выбрать случайное  $(n - m - 1)$ -битовое положительное целое  $a$ , такое, что  $g_i \neq a \pmod{p_i}$ ,  $i = 1, \dots, k$ .7: Вычислить  $p := 2ga + 1$ 8: **Пока**  $p$  не простое9: Вычислить  $h_i := a(-2ga - 1)^{-1} \pmod{p_i}$  для всех  $i = 1, \dots, k$ .10: **Повторять**11: Используя технику просеивания, выбрать случайное  $(n - m - 1)$ -битовое положительное целое  $b$ , такое, что  $g_i \neq b \pmod{p_i}$ ,  $h_i \neq b \pmod{p_i}$ ,  $i = 1, \dots, k$ .12: Вычислить  $q := 2gb + 1$ 13: **Пока**  $q$  не простое и  $(a, b) \neq 1$ 14: Вычислить  $h := 2gab + a + b$ 15: **Пока**  $h$  не простое16: **Вывести**  $p$ ,  $q$ 

---

Алгоритмы реализованы на языке программирования C++ с использованием библиотеки NTL [3]. В таблице приводятся результаты экспериментов на компьютере с процессором Intel core i7 с тактовой частотой 3,33 ГГц при значении параметра  $k = 100$ .

Время работы алгоритмов варьируется в пределах, отличающихся на порядок. В связи с этим в таблице указано худшее время в трёх случайных экспериментах.

Результаты экспериментов с 1024-битовым модулем

$p$ и $q$ , биты	$g$ , биты	Время алг. 1, с	Время алг. 2, с
512	256	46	24
	320	51	31
	384	58	19
1024	512	1082	213
	640	908	660
	768	794	98

Из таблицы видно, что, несмотря на предложенное ускорение метода построения специальных простых, выработка модуля криптосистемы Common Prime RSA занимает неприемлемо большое время. Отметим, что выработка пары случайных простых чисел без дополнительных свойств занимает десятые доли секунды.

#### ЛИТЕРАТУРА

1. *Hinek M. J.* Another look at small RSA exponents // LNCS. 2006. V. 3860. P. 82–98.
2. *Hinek M. J.* Cryptanalysis of RSA and Its Variants. CRC Press, 2009.
3. *Shoup V.* NTL — a library for doing number theory // <http://www.shoup.net>

УДК 519.688

### ПОЛИНОМЫ ХОЛЛА ДЛЯ КОНЕЧНЫХ ДВУПОРОЖДЁННЫХ ГРУПП ПЕРИОДА СЕМЬ<sup>1</sup>

А. А. Кузнецов, К. В. Сафонов

Пусть  $B_k = B_0(2, 7, k)$  — максимальная конечная двупорождённая группа периода 7 степени нильпотентности  $k$ . В работе вычислены полиномы Холла для  $B_k$  при  $k \leq 4$ .

**Ключевые слова:** периодическая группа, собирательный процесс, полиномы Холла.

Пусть  $B_k = B_0(2, 7, k)$  — максимальная конечная двупорождённая группа периода 7 степени нильпотентности  $k$ . В данном классе групп наибольшей является группа  $B_{28}$ , порядок которой равен  $7^{20416}$  [1]. Для каждой из  $B_k$  получены рс-представления (power commutator presentation) [1].

Пусть  $a_1^{x_1} \dots a_n^{x_n}$  и  $a_1^{y_1} \dots a_n^{y_n}$  — два произвольных элемента в группе  $B_k$ , записанные в коммутаторном виде. Тогда их произведение равно

$$a_1^{x_1} \dots a_n^{x_n} \cdot a_1^{y_1} \dots a_n^{y_n} = a_1^{z_1} \dots a_n^{z_n}.$$

Основой для нахождения степеней  $z_i$  является собирательный процесс [2, 3], который реализован в системах компьютерной алгебры GAP и MAGMA. Кроме того, существует альтернативный способ для вычисления произведений элементов группы, предложенный Ф. Холлом [4]. Холл показал, что  $z_i$  представляют собой полиномиальные

<sup>1</sup>Работа выполнена при поддержке Министерства образования и науки Российской Федерации, проект Б 112/14.

функции (в нашем случае над полем  $\mathbb{Z}_7$ ), зависящие от переменных  $x_1, \dots, x_i, y_1, \dots, y_i$ , которые принято сейчас называть *полиномами Холла*. Согласно [4],

$$z_i = x_i + y_i + p_i(x_1, \dots, x_{i-1}, y_1, \dots, y_{i-1}).$$

Необходимость применения полиномов Холла возникает при решении задач, требующих многократного умножения элементов группы. Исследование структуры графа Кэли некоторой группы является одной из таких задач [5, 6]. Проведённые вычислительные эксперименты на ЭВМ в двупорождённых группах периода пять [7] выявили, что метод полиномов Холла имеет преимущество перед традиционным собирательным процессом. Поэтому имеются основания полагать, что при изучении графов Кэли групп  $B_k$  применение полиномов окажется предпочтительнее собирательного процесса. Следует также отметить, что данный метод легко программно реализуем, в том числе на многопроцессорных вычислительных системах.

В работе вычислены ранее неизвестные полиномы Холла для групп  $B_k$  при  $k \leq 4$ . Для  $k > 4$  полиномы вычисляются аналогично, однако их вывод занимает значительно больше места, что делает невозможным проверить доказательство без применения ЭВМ.

Основным результатом настоящей работы является

**Теорема 1.** Пусть  $a_1^{x_1} \dots a_n^{x_n}$  и  $a_1^{y_1} \dots a_n^{y_n}$  — два произвольных элемента в группе  $B_k$ , записанные в коммутаторном виде, где  $k \in \mathbb{N}$  и  $k \leq 4$ . Тогда их произведение равно  $a_1^{x_1} \dots a_n^{x_n} \cdot a_1^{y_1} \dots a_n^{y_n} = a_1^{z_1} \dots a_n^{z_n}$ , где  $z_i \in \mathbb{Z}_7$  — полиномы Холла, задаваемые формулами (1), (2) при  $k = 1$ ; (1)–(3) при  $k = 2$ ; (1)–(5) при  $k = 3$ ; (1)–(8) при  $k = 4$ :

$$z_1 = x_1 + y_1, \quad (1)$$

$$z_2 = x_2 + y_2, \quad (2)$$

$$z_3 = x_3 + y_3 + x_2y_1, \quad (3)$$

$$z_4 = x_4 + y_4 + 3x_2y_1 + x_3y_1 + 4x_2y_1^2, \quad (4)$$

$$z_5 = x_5 + y_5 + 3x_2y_1 + x_3y_2 + 4x_2^2y_1 + x_2y_1y_2, \quad (5)$$

$$z_6 = x_6 + y_6 + 5x_2y_1 + 3x_3y_1 + x_4y_1 + 3x_2y_1^2 + 6x_2y_1^3 + 4x_3y_1^2, \quad (6)$$

$$z_7 = x_7 + y_7 + 2x_2^2y_1^2 + 2x_2y_1 + x_4y_2 + x_5y_1 + 5x_2y_1^2 + 5x_2^2y_1 + 4x_2y_1^2y_2 + 3x_2y_1y_2 + x_3y_1y_2, \quad (7)$$

$$z_8 = x_8 + y_8 + 5x_2y_1 + 3x_3y_2 + x_5y_2 + 3x_2^2y_1 + 6x_2^3y_1 + 4x_3y_2^2 + 4x_2y_1y_2^2 + 4x_2^2y_1y_2 + 6x_2y_1y_2. \quad (8)$$

#### ЛИТЕРАТУРА

1. O'Brien E. A. and Vaughan-Lee M. R. The 2-generator restricted Burnside group of exponent 7 // Int. J. Algebra Comput. 2002. No. 12. P. 459–470.
2. Sims C. Computation with Finitely Presented Groups. Cambridge: Cambridge University Press, 1994. 628 p.
3. Holt D., Eick B., and O'Brien E. Handbook of Computational Group Theory. Boca Raton: Chapman & Hall/CRC Press, 2005. 514 p.
4. Hall P. Nilpotent groups: Notes of lectures given at the Canadian Mathematical Congress summer seminar, University of Alberta, 12–30 August, 1957. London: Queen Mary College, 1969.
5. Кузнецов А. А., Кузнецова А. С. Компьютерное моделирование конечных двупорождённых групп периода 5 // Вестник Сибирского государственного аэрокосмического университета. 2012. № 5. С. 59–62.

6. Кузнецов А. А., Кузнецова А. С. О взаимосвязи функций роста в симметрических группах с задачами комбинаторной оптимизации // Вестник Сибирского государственного аэрокосмического университета. 2012. №6. С. 57–62.
7. Кузнецов А. А., Кузнецова А. С. Быстрое умножение элементов в конечных двупорождённых группах периода пять // Прикладная дискретная математика. 2013. №1. С. 110–116.

УДК 519.85

## ЭВРИСТИКИ ПОСТРОЕНИЯ НАДЕЖНОЙ ТЕЛЕКОММУНИКАЦИОННОЙ СЕТИ<sup>1</sup>

Р. Э. Шангин

Рассматривается известная NP-трудная задача нахождения минимального остовного  $k$ -дерева в простом взвешенном графе. Данную задачу необходимо решать при проектировании надежной телекоммуникационной сети наименьшей стоимости. Предлагается серия эвристических алгоритмов. Определены оценки трудоёмкости алгоритмов, доказана их корректность. Проведён вычислительный эксперимент по сравнению эффективности предложенных алгоритмов, как между собой, так и с известными приближёнными и точными алгоритмами.

**Ключевые слова:** *остовное  $k$ -дерево, надёжная сеть, IFI-сеть, NP-трудность, эвристики.*

Эффективное решение проблемы надежности информационных сетей, в первую очередь, заключается в проектировании сети, устойчивой как к сбоям отдельных каналов, так и к полным отказам некоторых звеньев системы. В начале 1980-х годов А. Фарлеем введена концепция IFI-сетей (Isolated Failure Immune networks) [1]. Такие IFI-сети являются устойчивыми к сбоям трех типов:

- 1) удаление рёбер, не имеющих общую вершину;
- 2) удаление несмежных вершин;
- 3) удаление рёбер и вершин, если рёбра не инцидентны ни одной удалённой вершине или не инцидентны вершине, смежной с удалённой.

В работе [1] А. Фарлей доказал, что 2-дерево [2] есть минимальная (по включению рёбер) IFI-сеть. Отсюда задача проектирования IFI-сети может быть представлена как задача построения остовного  $k$ -дерева минимального веса, известная в зарубежной литературе как *Minimum Spanning  $k$ -tree Problem* (MSkT) и являющаяся обобщением классической задачи нахождения минимального остовного дерева (MST) [3].

**Определение 1.** Связный неориентированный граф  $T$  называется  $k$ -деревом, если его построение возможно осуществить рекурсивно по правилам: полный граф из  $k + 1$  вершин есть  $k$ -дерево;  $k$ -дерево с  $i + 1$  вершинами получается из  $k$ -дерева с  $i$  вершинами добавлением в него новой вершины  $j$  и  $k$  рёбер таким образом, чтобы новая вершина  $j$  стала смежной со всеми вершинами некоторой клики размера  $k$ .

Формулировка задачи MSkT следующая. Пусть  $G = (V, E)$  — полный взвешенный граф с множествами вершин  $V$  (телекоммуникационные терминалы) и рёбер  $E$  (возможные связи между терминалами), причём для каждого ребра  $[i, j] \in E$  задан его вес  $w(i, j) \geq 0$ , равный стоимости прокладки кабеля или трансляции сигналов между терминалами  $i$  и  $j$ . Обозначим  $T(G)$  множество всех остовных  $k$ -деревьев в гра-

<sup>1</sup>Исследование выполнено при поддержке Министерства образования и науки Российской Федерации, соглашение №14.В37.21.0395.

фе  $G$ . Пусть  $w(T)$  — суммарный вес рёбер остовного  $k$ -дерева  $T \in T(G)$ . Требуется найти остовное  $k$ -дерево  $T^*$  минимального веса в полном взвешенном графе  $G$ , то есть  $T^* = \arg \min_{T \in T(G)} \{w(T)\}$ .

Известно, что задача MSkT NP-трудна при  $k \geq 2$ . В [4] доказано, что мощность множества  $T(G)$  допустимых решений задачи MSkT равна  $|V|!(|V| + k - 1)!/k!$ , исходя из чего трудоёмкость полного перебора составляет  $O(|V|^{2|V|}/k^k)$  операций. Известен точный алгоритм, основанный на динамическом программировании, с трудоёмкостью  $O(|V|^{k+1}3^{|V|})$  операций [4]. В работах [4–6] предложены эффективные эвристики и алгоритмы с гарантированной оценкой точности для задачи MS2T.

В работе предложен жадный алгоритм *GreedyA*, находящий решение задачи MSkT, основанный на рекурсивном определении  $k$ -дерева и являющийся обобщением известного алгоритма Прима для решения задачи MST. Причём, так как *GreedyA* является обобщением алгоритма Прима, то на каждом шаге эвристика строит  $k$ -дерево. Доказано, что трудоёмкость алгоритма *GreedyA* равна  $O((|V| - k)^3 \cdot k)$  операций.

Предложен алгоритм *DPA*, основанный на динамическом программировании. Алгоритм *DPA* частично использует идею жадного алгоритма *GreedyA*, но значительно превосходит *GreedyA* с точки зрения качества найденного решения, поскольку *DPA* на каждом шаге работает с  $|V|$  различными вариантами  $k$ -деревьев, построенных на предыдущем шаге, а алгоритм *GreedyA* — только с одним. Более того, поскольку жадная эвристика *GreedyA* является частным случаем алгоритма *DPA*, то ошибка решения, найденного алгоритмом *DPA*, не больше ошибки решения, построенного *GreedyA*. Доказано, что трудоёмкость *DPA* равна  $O(|V|^4 \cdot k)$ .

Предложены также алгоритмы, основанные на итеративном улучшении начального решения, полученного с помощью алгоритмов *GreedyA* и *DPA*.

Все алгоритмы реализованы в среде MATLAB. Проведён вычислительный эксперимент по сравнению эффективности предложенных эвристических алгоритмов как между собой, так и с известными эвристическими и точными алгоритмами. Из результатов эксперимента следует, что для решения задачи MSkT малой и средней размерности целесообразней использовать эвристики, основанные на итеративном улучшении начального решения, а для большой размерности — алгоритм *DPA*, поскольку он находит решение с достаточной высокой точностью за приемлемое время.

#### ЛИТЕРАТУРА

1. Farley A. Networks immune to isolated failures // Networks. 1981. No. 11. P. 255–268.
2. Rose D. On simple characterizations of  $k$ -trees // Discr. Math. 1974. No. 7. P. 317–322.
3. Prim R. Shortest connection networks and some generalizations // Bell Systems Techn. J. 1957. No. 36. P. 1389–1397.
4. Bern M. Networks Design Problems: Steiner Trees and Spanning  $k$ -Trees. Ph.D. Thesis. University of Berkeley, 1987. 289 p.
5. Candia A. and Bravo H. A simulated annealing approach for minimum cost isolated failure immune networks // Essays and Surveys in Metaheuristics. 2002. V. 15. P. 169–183.
6. Beltran H. and Skorin-Kapov D. On minimum cost isolated failure immune network // Telecommunication Systems. 1994. No. 3. P. 183–200.

## СВЕДЕНИЯ ОБ АВТОРАХ

**АБОРНЕВ Александр Викторович** — г. Москва. E-mail: [abconf.c@gmail.com](mailto:abconf.c@gmail.com)

**АВЕЗОВА Яна Эдуардовна** — студентка Национального исследовательского ядерного университета «МИФИ», г. Москва. E-mail: [avezovayana@gmail.com](mailto:avezovayana@gmail.com)

**АГИБАЛОВ Геннадий Петрович** — доктор технических наук, профессор, заведующий кафедрой защиты информации и криптографии Национального исследовательского Томского государственного университета, г. Томск. E-mail: [agibalov@isc.tsu.ru](mailto:agibalov@isc.tsu.ru)

**АЛЕХИНА Марина Анатольевна** — доктор физико-математических наук, профессор, заведующая кафедрой Пензенского государственного университета, г. Пенза. E-mail: [ama@sura.ru](mailto:ama@sura.ru)

**АЛЬМЕЕВ Азат Наилевич** — студент института ВМиИТ Казанского (Приволжского) федерального университета, г. Казань. E-mail: [azat.almeev@gmail.com](mailto:azat.almeev@gmail.com)

**АНАШКИНА Наталия Викторовна** — кандидат технических наук, доцент, Лаборатория ТВП, г. Москва. E-mail: [6237030@mail.ru](mailto:6237030@mail.ru)

**АНЖИН Виктор Андреевич** — студент кафедры защиты информации и криптографии Национального исследовательского Томского государственного университета, г. Томск.

E-mail: [viktor.anjin@gmail.com](mailto:viktor.anjin@gmail.com)

**БАР-ГНАР Регина Игоревна** — студентка Национального исследовательского ядерного университета «МИФИ», г. Москва. E-mail: [bargnar.r@gmail.com](mailto:bargnar.r@gmail.com)

**БАРСУКОВА Оксана Юрьевна** — старший преподаватель Пензенского государственного университета, г. Пенза. E-mail: [dm@pnzgu.ru](mailto:dm@pnzgu.ru)

**БОНДАРЕНКО Леонид Николаевич** — кандидат технических наук, доцент, доцент кафедры дискретной математики Пензенского государственного университета, г. Пенза.

E-mail: [leobond5@mail.ru](mailto:leobond5@mail.ru)

**БРОСЛАВСКИЙ Олег Викторович** — студент кафедры защиты информации и криптографии Национального исследовательского Томского государственного университета, г. Томск.

E-mail: [o.v.broslavsky@gmail.com](mailto:o.v.broslavsky@gmail.com)

**БЫКОВ Игорь Сергеевич** — магистрант механико-математического факультета Новосибирского государственного университета, г. Новосибирск. E-mail: [patrick.no10@gmail.com](mailto:patrick.no10@gmail.com)

**БЫКОВА Валентина Владимировна** — доктор физико-математических наук, доцент, профессор Института математики и фундаментальной информатики Сибирского федерального университета, г. Красноярск. E-mail: [bykvalen@mail.ru](mailto:bykvalen@mail.ru)

**БЫЛКОВ Даниил Николаевич** — ООО «Центр сертификационных исследований», г. Москва. E-mail: [bilkov@gmail.com](mailto:bilkov@gmail.com)

**ВАСИН Алексей Валерьевич** — кандидат физико-математических наук, доцент кафедры дискретной математики Пензенского государственного университета, г. Пенза.

E-mail: [alvarvasin@mail.ru](mailto:alvarvasin@mail.ru)

**ВЕРШИНИН Игорь Сергеевич** — кандидат технических наук, доцент, доцент Казанского национального исследовательского технического университета им. А. Н. Туполева — КАИ, г. Казань.

E-mail: [mlsx@rambler.ru](mailto:mlsx@rambler.ru)

**ВИТКУП Валерия Александровна** — студентка механико-математического факультета Новосибирского государственного университета, г. Новосибирск. E-mail: [vvitkup@yandex.ru](mailto:vvitkup@yandex.ru)

**ВОЛГИН Артем Владимирович** — преподаватель МГТУ МИРЭА, г. Москва.

E-mail: [artem.volgin@bk.ru](mailto:artem.volgin@bk.ru)

**ГАВРИКОВ Александр Владимирович** — аспирант Саратовского государственного университета, г. Саратов. E-mail: [alexandergavrikov1989@gmail.com](mailto:alexandergavrikov1989@gmail.com)

**ГЕУТ Кристина Леонидовна** — ассистент Уральского государственного университета путей сообщения, г. Екатеринбург. E-mail: [geutkrl@yandex.ru](mailto:geutkrl@yandex.ru)

**ГЛОТОВ Игорь Никитович** — студент Национального исследовательского Томского государственного университета, г. Томск. E-mail: [igor.n.glotov@gmail.com](mailto:igor.n.glotov@gmail.com)

**ГОРОДИЛОВА Анастасия Александровна** — магистрантка механико-математического факультета Новосибирского государственного университета, г. Новосибирск.

E-mail: [gorodilova.aa@gmail.com](mailto:gorodilova.aa@gmail.com)

**ГОЦУЛЕНКО Владимир Владимирович** — кандидат технических наук, старший научный сотрудник, старший научный сотрудник отдела теплофизических основ энергосберегающих теплотехнологий института технической теплофизики НАН Украины, г. Киев. E-mail: [gusul@ukr.net](mailto:gusul@ukr.net)

**ГРИБАНОВ Андрей Сергеевич** — студент кафедры защиты информации и криптографии Национального исследовательского Томского государственного университета, г. Томск.

E-mail: [andreigribanovtsu@gmail.com](mailto:andreigribanovtsu@gmail.com)

**ДЕВЯНИН Петр Николаевич** — доктор технических наук, доцент, председатель УМС Учебно-методического объединения по образованию в области информационной безопасности, г. Москва.

E-mail: [peter\\_devyanin@hotmail.com](mailto:peter_devyanin@hotmail.com)

**ДОРОХОВА Алиса Михайловна** — аспирант кафедры криптологии и дискретной математики НИЯУ МИФИ, руководитель проектов отдела информационной безопасности ООО «Пойнтлэйн», г. Москва. E-mail: [alisa.koreneva@gmail.com](mailto:alisa.koreneva@gmail.com)

**ДРУЖИНИН Денис Вячеславович** — аспирант кафедры теоретических основ информатики Национального исследовательского Томского государственного университета, г. Томск.

E-mail: [dendru@rambler.ru](mailto:dendru@rambler.ru)

**ЕРМИЛОВ Дмитрий Михайлович** — сотрудник лаборатории ТВП, г. Москва.

E-mail: [wwermilov@gmail.com](mailto:wwermilov@gmail.com)

**ЖАРКОВА Анастасия Владимировна** — кандидат физико-математических наук, доцент кафедры теоретических основ компьютерной безопасности и криптографии Саратовского государственного университета им. Н. Г. Чернышевского, г. Саратов. E-mail: [VAnastasiyaV@gmail.com](mailto:VAnastasiyaV@gmail.com)

**ЖУКОВ Кирилл Дмитриевич** — сотрудник лаборатории ТВП, г. Москва.

**ЖУКОВСКАЯ Александра Олеговна** — студентка Национального исследовательского Томского государственного университета, г. Томск. E-mail: [zhuka157@yandex.ru](mailto:zhuka157@yandex.ru)

**ЗАЕЦ Мирослав Владимирович** — ФГУП «НИИ КВАНТ», г. Москва.

E-mail: [mirzaets@hotmail.com](mailto:mirzaets@hotmail.com)

**ЗАЙЦЕВ Георгий Юрьевич** — студент кафедры защиты информации и криптографии Национального исследовательского Томского государственного университета, г. Томск.

E-mail: [zaytsevgu@gmail.com](mailto:zaytsevgu@gmail.com)

**ЗАХАРОВ Вячеслав Михайлович** — доктор технических наук, профессор, профессор Казанского национального исследовательского технического университета им. А. Н. Туполева (КНИТУ-КАИ), г. Казань. E-mail: [gilvv@mail.ru](mailto:gilvv@mail.ru)

**ЗЕЛИНСКИЙ Руслан Владимирович** — старший преподаватель филиала «Восток» КНИТУ-КАИ, г. Чистополь. E-mail: [ruszel@mail.ru](mailto:ruszel@mail.ru)

**ЗУБКОВ Андрей Михайлович** — доктор физико-математических наук, заведующий отделом дискретной математики Математического института им. В. А. Стеклова РАН, г. Москва.

E-mail: [zubkov@mi.ras.ru](mailto:zubkov@mi.ras.ru)

**ИВАЧЕВ Артем Сергеевич** — студент кафедры защиты информации и криптографии Национального исследовательского Томского государственного университета, г. Томск.

E-mail: [ivachyou@gmail.com](mailto:ivachyou@gmail.com)

**КАТЕРИНСКИЙ Денис Аркадьевич** — студент Национального исследовательского Томского государственного университета, кафедра защиты информации и криптографии, г. Томск.

E-mail: [deniskat@isc.tsu.ru](mailto:deniskat@isc.tsu.ru)

**КОВАЛЕВ Дмитрий Сергеевич** — аспирант кафедры защиты информации и криптографии Национального исследовательского Томского государственного университета, инженер-программист отдела технических средств и ремонта вычислительной техники ОАО «Информационные спутниковые системы» им. акад. М. Ф. Решетнёва», г. Железногорск. E-mail: [dmisk@hotmail.com](mailto:dmisk@hotmail.com), [dmisk@iss-reshetnev.ru](mailto:dmisk@iss-reshetnev.ru)

**КОВАЛЕВСКАЯ Анастасия Олеговна** — студентка кафедры защиты информации и криптографии Национального исследовательского Томского государственного университета, г. Томск. E-mail: [aokovalevskaya@gmail.com](mailto:aokovalevskaya@gmail.com)

**КОЛЕГОВ Денис Николаевич** — кандидат технических наук, доцент кафедры защиты информации и криптографии Национального исследовательского Томского государственного университета, г. Томск. E-mail: [d.n.kolegov@gmail.com](mailto:d.n.kolegov@gmail.com)

**КОЛОМЕЕЦ Николай Александрович** — аспирант Института математики им. С. Л. Соболева СО РАН, г. Новосибирск. E-mail: [nkolomeec@gmail.com](mailto:nkolomeec@gmail.com)

**КОМАРОВ Дмитрий Дмитриевич** — аспирант, ассистент кафедры теоретических основ компьютерной безопасности и криптографии Саратовского государственного университета им. Н. Г. Чернышевского, г. Саратов. E-mail: [komarovdd@gmail.com](mailto:komarovdd@gmail.com)

**КОРСАКОВА Екатерина Павловна** — магистрантка механико-математического факультета Новосибирского государственного университета, г. Новосибирск. E-mail: [korsakova.katerina@gmail.com](mailto:korsakova.katerina@gmail.com)

**КРУГЛОВ Василий Игоревич** — кандидат физико-математических наук, научный сотрудник отдела дискретной математики Математического института им. В. А. Стеклова РАН, г. Москва. E-mail: [kruglov@mi.ras.ru](mailto:kruglov@mi.ras.ru)

**КУЗНЕЦОВ Александр Алексеевич** — доктор физико-математических наук, профессор, директор института Сибирского государственного аэрокосмического университета им. акад. М. Ф. Решетнёва, г. Красноярск. E-mail: [alex\\_kuznetsov80@mail.ru](mailto:alex_kuznetsov80@mail.ru)

**КУРГАНСКИЙ Алексей Николаевич** — кандидат физико-математических наук, старший научный сотрудник Института прикладной математики и механики НАН Украины, г. Донецк. E-mail: [topologia@mail.ru](mailto:topologia@mail.ru)

**КЯЖИН Сергей Николаевич** — аспирант кафедры криптологии и дискретной математики Национального исследовательского ядерного университета «МИФИ», г. Москва. E-mail: [s.kyazhin@kaf42.ru](mailto:s.kyazhin@kaf42.ru)

**ЛАКОМКИНА Александра Евгеньевна** — аспирантка Пензенского государственного университета, г. Пенза. E-mail: [dm@pnzgu.ru](mailto:dm@pnzgu.ru)

**МИЛОВАНОВ Тимофей Игоревич** — студент кафедры защиты информации и криптографии Национального исследовательского Томского государственного университета, г. Томск. E-mail: [timcess@gmail.com](mailto:timcess@gmail.com)

**МИНАКОВ Александр Александрович** — преподаватель Московского института радиотехники, электроники и информатики, г. Москва. E-mail: [minak-ski@yandex.ru](mailto:minak-ski@yandex.ru)

**МОНАРЕВ Виктор Александрович** — кандидат физико-математических наук, научный сотрудник Института вычислительных технологий СО РАН, г. Новосибирск. E-mail: [viktor.monarev@gmail.com](mailto:viktor.monarev@gmail.com)

**ОВСЯННИКОВ Станислав Владимирович** — студент Национального исследовательского Томского государственного университета, г. Томск. E-mail: [naphaso@gmail.com](mailto:naphaso@gmail.com)

**ОЛЕКСОВ Никита Евгеньевич** — студент кафедры защиты информации и криптографии Национального исследовательского Томского государственного университета, г. Томск. E-mail: [n.e.oleksov@gmail.com](mailto:n.e.oleksov@gmail.com)

**ОСИПОВ Дмитрий Юрьевич** — аспирант Саратовского государственного университета им. Н. Г. Чернышевского, г. Саратов. E-mail: [st\\_hill@mail.ru](mailto:st_hill@mail.ru)

**ПАНКРАТОВ Иван Владимирович** — г. Томск. E-mail: [ivan.pankratov2010@yandex.ru](mailto:ivan.pankratov2010@yandex.ru)

**ПЕСТУНОВ Андрей Игоревич** — кандидат физико-математических наук, доцент Новосибирского государственного университета экономики и управления, научный сотрудник Института вычислительных технологий СО РАН, г. Новосибирск. E-mail: [pestunov@gmail.com](mailto:pestunov@gmail.com)

**ПОГОРЕЛОВ Борис Александрович** — доктор физико-математических наук, профессор, действительный член Академии криптографии Российской Федерации, г. Москва.

**ПУДОВКИНА Марина Александровна** — кандидат физико-математических наук, доцент Национального исследовательского ядерного университета «МИФИ», г. Москва.

E-mail: [maricap@rambler.ru](mailto:maricap@rambler.ru)

**РАЗИНКОВ Евгений Викторович** — кандидат физико-математических наук, ассистент кафедры системного анализа и информационных технологий института ВМиИТ Казанского (Приволжского) федерального университета, г. Казань. E-mail: [Razinkov@steganography.ru](mailto:Razinkov@steganography.ru)

**РАЦЕЕВ Сергей Михайлович** — доцент кафедры информационной безопасности и теории управления Ульяновского государственного университета, г. Ульяновск. E-mail: [RatseevSM@mail.ru](mailto:RatseevSM@mail.ru)

**РОМАНЬКОВ Виталий Анатольевич** — доктор физико-математических наук, профессор, заведующий кафедрой Омского государственного университета, главный научный сотрудник Омского государственного технического университета, г. Омск. E-mail: [romankov48@mail.ru](mailto:romankov48@mail.ru)

**РЫБАКОВ Александр Сергеевич** — кандидат физико-математических наук, сотрудник лаборатории ТВП, г. Москва.

**РЫЖКОВ Виктор Игоревич** — студент Национального исследовательского Томского государственного университета, г. Томск. E-mail: [vic.ryzhkov@gmail.com](mailto:vic.ryzhkov@gmail.com)

**САЛИЙ Вячеслав Николаевич** — кандидат физико-математических наук, профессор, заведующий кафедрой теоретических основ компьютерной безопасности и криптографии Саратовского государственного университета им. Н. Г. Чернышевского, г. Саратов. E-mail: [SaliiVN@info.sgu.ru](mailto:SaliiVN@info.sgu.ru)

**САФОНОВ Константин Владимирович** — доктор физико-математических наук, профессор, заведующий кафедрой Сибирского государственного аэрокосмического университета им. акад. М. Ф. Решетнёва, г. Красноярск. E-mail: [safonovkv@rambler.ru](mailto:safonovkv@rambler.ru)

**СВИРИДОВ Павел Юрьевич** — студент кафедры защиты информации и криптографии Национального исследовательского Томского государственного университета, г. Томск.

E-mail: [p.y.sviridov@gmail.com](mailto:p.y.sviridov@gmail.com)

**СЕРГЕЕВА Ольга Евгеньевна** — студентка кафедры защиты информации и криптографии Национального исследовательского Томского государственного университета, г. Томск.

E-mail: [SergeevaOE@gmail.com](mailto:SergeevaOE@gmail.com)

**СИБИРЯКОВА Валентина Александровна** — старший преподаватель Национального исследовательского Томского государственного университета, г. Томск. E-mail: [val349@mail.ru](mailto:val349@mail.ru)

**СОРОКИН Сергей Николаевич** — старший преподаватель кафедры компьютерной безопасности ФПМ МИЭМ НИУ ВШЭ, г. Москва. E-mail: [sergey-dcm@yandex.ru](mailto:sergey-dcm@yandex.ru)

**СТЕФАНЦОВ Дмитрий Александрович** — старший преподаватель Национального исследовательского Томского государственного университета, г. Томск. E-mail: [d.a.stefantsov@isc.tsu.ru](mailto:d.a.stefantsov@isc.tsu.ru)

**ТИТОВ Сергей Сергеевич** — доктор физико-математических наук, профессор Уральского государственного университета путей сообщения, г. Екатеринбург. E-mail: [stitov@usaaa.ru](mailto:stitov@usaaa.ru)

**ТКАЧЕНКО Николай Олегович** — аспирант Национального исследовательского Томского государственного университета, г. Томск. E-mail: [n.o.tkachenko@gmail.com](mailto:n.o.tkachenko@gmail.com)

**ТОКАРЕВА Наталья Николаевна** — кандидат физико-математических наук, старший научный сотрудник Института математики им. С. Л. Соболева, г. Новосибирск.

E-mail: [tokareva@math.nsc.ru](mailto:tokareva@math.nsc.ru)

**ТОЛЮПА Евгений Алексеевич** — аспирант Ярославского государственного университета им. П. Г. Демидова, г. Ярославль. E-mail: [tolyupa@gmail.com](mailto:tolyupa@gmail.com)

**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](mailto:tvnik@sibmail.com)

**ФОМИЧЕВ Владимир Михайлович** — доктор физико-математических наук, профессор, профессор Финансового университета при Правительстве Российской Федерации, профессор Национального исследовательского ядерного университета «МИФИ», г. Москва. E-mail: [fomichev@nm.ru](mailto:fomichev@nm.ru)

**ЧЕРЕМУШКИН Александр Васильевич** — доктор физико-математических наук, член-корреспондент Академии криптографии РФ, заведующий кафедрой Института криптографии, связи и информатики, г. Москва. E-mail: [avc238@mail.ru](mailto:avc238@mail.ru)

**ЧЕРНОВ Дмитрий Владимирович** — аспирант кафедры защиты информации и криптографии Национального исследовательского Томского государственного университета, г. Томск. E-mail: [dm.vl.chernov@gmail.com](mailto:dm.vl.chernov@gmail.com)

**ШАЛАГИН Сергей Викторович** — кандидат технических наук, доцент, доцент Казанского национального исследовательского технического университета им. А. Н. Туполева (КНИТУ-КАИ), г. Казань. E-mail: [sshalagin@mail.ru](mailto:sshalagin@mail.ru)

**ШАНГИН Роман Эдуардович** — аспирант НИУ Южно-Уральского государственного университета, г. Челябинск. E-mail: [shanginre@gmail.com](mailto:shanginre@gmail.com)

**ШАРАПОВА Марина Леонидовна** — старший преподаватель кафедры математического анализа механико-математического факультета Московского государственного университета им. М. В. Ломоносова, г. Москва. E-mail: [msharapova@list.ru](mailto:msharapova@list.ru)

**ШИШКИН Василий Алексеевич** — кандидат физико-математических наук, эксперт технического комитета по стандартизации (ТК26) «Криптографическая защита информации», г. Москва. E-mail: [shishkin.vasily@gmail.com](mailto:shishkin.vasily@gmail.com)

**ШОЛОМОВ Лев Абрамович** — доктор физико-математических наук, профессор, главный научный сотрудник Института системного анализа РАН, г. Москва. E-mail: [sholomov@isa.ru](mailto:sholomov@isa.ru)

**ШУРУПОВ Андрей Николаевич** — кандидат технических наук, доцент Московского государственного института радиотехники, электроники и информатики, г. Москва. E-mail: [ashurupov@mail.ru](mailto:ashurupov@mail.ru)

**ШУШУЕВ Георгий Иннокентьевич** — студент механико-математического факультета Новосибирского государственного университета, г. Новосибирск. E-mail: [g.shushuev@gmail.com](mailto:g.shushuev@gmail.com)

## АННОТАЦИИ ДОКЛАДОВ НА АНГЛИЙСКОМ ЯЗЫКЕ

## SECTION 1

*Bar-Gnar R. I., Fomichev V. M.* **ABOUT THE MINIMAL PRIMITIVE MATRICES.** A quadratic Boolean matrix  $A$  is called a primitive matrix if some its degree does not contain 0's. A primitive matrix is called a minimal primitive matrix if it becomes non-primitive matrix after replacing any one 1 in it by 0. The height of a primitive matrix is defined as the least Hamming's distance between it and a minimal primitive matrix. In the paper, properties of minimal primitive matrices are studied. The amount of minimal primitive matrices of order  $n$  is estimated. An algorithm for estimating the height of a primitive matrix is proposed.

**Keywords:** *primitive matrix, lattice, antichain, computational complexity of the algorithm.*

*Bondarenko L. N., Sharapova M. L.* **EULER'S NUMBERS ON SETS OF PERMUTATIONS AND ANALOGUES OF WILSON'S THEOREM.** Euler's numbers on sets of permutations are defined. By using them the analogues of Wilson's theorem for the numbers of standard complete mappings and for the numbers of standard strong complete mappings are proved.

**Keywords:** *permutation, Euler's numbers, complete mappings, Wilson's theorem.*

*Vitkup V. A.* **ON SOME OPEN QUESTIONS ABOUT APN FUNCTIONS.** Some open questions in the theory of APN functions are stated. Few results obtained in this direction are listed. For the sum of two APN functions of dimension 2, a necessary and sufficient condition to be an APN function is proved.

**Keywords:** *vectorial Boolean function, APN function.*

*Geut Kr. L., Titov S. S.* **THE EQUIVALENT PROBLEM OF TESTING FERMAT PRIMES.** It is shown that the problem of testing Fermat numbers for primality is equivalent to the problem of testing some polynomials over  $\text{GF}(2)$  or  $\text{GF}(3)$  for irreducibility.

**Keywords:** *irreducible polynomial, prime numbers, Fermat numbers.*

*Gorodilova A. A.* **CHARACTERIZATION OF APN FUNCTIONS BY MEANS OF SUBFUNCTIONS.** A vectorial Boolean function  $F : \{0, 1\}^n \rightarrow \{0, 1\}^n$  is called an APN function if the equation  $F(x) \oplus F(x \oplus a) = b$  has at most 2 solutions for any vectors  $a, b$ , where  $a \neq 0$ . The complete characterization of APN functions by means of subfunctions is found. It is proved that  $F$  is APN function if and only if each of its subfunctions in  $n - 1$  variables is an APN function or has the order of differential uniformity 4 and the admissibility conditions are hold. Some numerical results of this characterization for small number  $n$  of variables are presented.

**Keywords:** *vectorial Boolean function, differentially  $\delta$ -uniform function, APN function.*

*Zaets M. V.* **CLASSIFICATION OF THE FUNCTIONS OVER PRIMARY RING OF RESIDUES CONSIDERED IN CONNECTION WITH THE METHOD OF COORDINATE LINEARIZATION.** It's known that the method of coordinate linearization may be used for solving a system of polynomial equations over primary ring of residues. Here, some classification is made for functions over primary ring of residues providing systems of equations which may be solved by using this method. The class of polynomial functions is extended to class of variative-coordinate polynomial functions (VCP-functions) which is also extended to the class of quasi-VCP-functions and to

the class of coordinate-linear solvable functions. Properties of these classes are described.

**Keywords:** *polynomial functions, variative-coordinate polynomial functions, VCP-functions, quasi-VCP-functions, coordinate-linear solvable functions, method of coordinate linearization.*

*Ivachev A. S.* **RESEARCH OF DIFFERENTIABLE MODULO  $p^n$  FUNCTIONS.**

For the class  $D_n$  of differentiable modulo  $p^n$  functions, subsets  $A_n$ ,  $B_n$ ,  $C_n$  are defined so that every function  $f$  in  $D_n$  is uniquely represented by the sum of certain functions  $f_A \in A_n$ ,  $f_B \in B_n$ ,  $f_C \in C_n$ . The numbers of functions, of bijective functions and of transitive functions in  $D_n$  are found via this representation. According to these cardinality relations, the set of transitive differentiable modulo  $p^2$  functions coincide with the set of transitive polynomial functions, but this ceases to be true with increasing the degree of the modulo. It is shown that a function  $f$  in  $D_n$  is invertible if and only if  $f$  is invertible modulo  $p$  and the derivatives of  $f$  are not equal 0 modulo  $p^i$ ,  $i = 2, \dots, n$ . A recurrent formula is presented for finding inverse differentiable modulo  $p^n$  function for a bijective function in  $D_n$ . A transitivity condition is obtained for a differentiable modulo  $p^n$  function. It is shown that any transitive function  $f$  in  $D_n$  may be constructed from a function  $\hat{f}$  in  $D_{n-1}$  such that  $f = \hat{f} \pmod{p^{n-1}}$ .

**Keywords:** *recurrent sequence, differentiable modulo function, inverse function, bijective function, transitive function.*

*Kolomeec N. A.* **AN UPPER BOUND FOR THE NUMBER OF BENT FUNCTIONS AT THE DISTANCE  $2^k$  FROM AN ARBITRARY BENT FUNCTION IN  $2k$  VARIABLES.**

An upper bound for the number of bent functions at the distance  $2^k$  from an arbitrary bent function in  $2k$  variables is obtained. The bound is reached only for quadratic bent functions. The notion of completely affine decomposable Boolean function is introduced. It is proven that only affine and quadratic Boolean functions can be completely affine decomposable.

**Keywords:** *Boolean functions, bent functions, quadratic bent functions.*

*Korsakova E. P.* **NONLINEARITY BOUNDS FOR VECTORIAL BOOLEAN FUNCTIONS OF SPECIAL FORM.**

The problem of combining different cryptographic properties of vectorial Boolean functions is considered. An upper nonlinearity bound for vectorial Boolean functions constructed using affine Boolean functions is obtained. It is shown that, for any natural  $n$ , the bound is reachable. Besides, a lower bound for the number of vectorial functions having a fixed nonlinearity and constructed from balanced Boolean functions is obtained.

**Keywords:** *vectorial Boolean function, nonlinearity, affine function, balancedness.*

*Kurgansky O. M.* **REACHABILITY PROBLEM FOR CONTINUOUS PIECEWISE-AFFINE MAPPINGS OF A CIRCLE HAVING DEGREE 2.**

For the continuous piecewise-affine mappings of a circle into itself having degree 2, the algorithmic decidability of the point-to-point reachability problem is proved. All these piecewise-affine mappings are topological conjugate to chaotic mapping  $E_2 : \mathbb{R}/\mathbb{Z} \rightarrow \mathbb{R}/\mathbb{Z}$  where  $E_2(x) = 2x \pmod{1}$ . It is known that the orbit  $O(x)$  of  $E_2$  is uniformly distributed for almost all  $x \in \mathbb{R}/\mathbb{Z}$ , i.e.  $O(x)$  is chaotic. But none of the "almost all"  $x$  is representable in a computer because they all are infinite real numbers. The behaviour complexity of  $E_2$  lies in the complexity of its initial state. Thus the mathematical fact that  $E_2$  is chaotic is vacuous from the computer science point of view. But from the proof of the main result of this work, it follows that each continuous piecewise-affine mapping with rational coefficients

that conjugate to  $E_2$  shows chaotic behaviour not only for real but also for some rational states. It makes them interesting in problems of cryptographic information transformation.

**Keywords:** *deterministic chaos, cryptography, piecewise-affine mapping, reachability problem.*

**Minakov A. A. COMPOUND POISSON APPROXIMATION FOR THE DISTRIBUTION OF THE NUMBER OF MONOTONE TUPLES IN RANDOM SEQUENCE.**

The distribution of the number of monotone tuples in the sequence of independent uniformly distributed random variables taking values in the set  $\{0, \dots, N - 1\}$  is considered. By means of the Stein method, an estimate for the variation distance between the distribution of the number of monotone tuples and compound Poisson distribution are constructed. As a corollary of this result, the limit theorem for the number of monotone tuples is proved. The approximating distribution in it is the distribution of the sum of Poisson number of independent random variables with geometric distribution.

**Keywords:** *monotone tuples, estimate for the variation distance of the compound Poisson approximation, compound Poisson distribution, Stein method.*

**Cheremushkin A. V. NUMBER OF DISCRETE FUNCTIONS ON A PRIMARY CYCLIC GROUP WITH A GIVEN NONLINEARITY DEGREE.**

Let  $F$  be a function  $F : G^m \rightarrow G$  on a cyclic group  $G$  of order  $p^n$ , and  $\Delta_a F(x) = F(x + a) - F(x)$ ,  $x \in G^m$ . The nonlinearity degree  $\text{dl } F$  is the minimal number  $t$  such that  $\Delta_{a_1} \dots \Delta_{a_{t+1}} F(x) = 0$  for all  $a_1, \dots, a_{t+1}, x \in G^m$ . A method is proposed for computing  $\text{dl } F$  on the basis of the Newton expansion for  $F$ . Theorem 1 presents the value of nonlinearity degree for all basic functions  $F_i(x) = \binom{x}{i} \bmod p^n$ ,  $1 \leq i \leq p^n - 1$ , namely:  $\text{dl } F_i = i + (t - 1)(p - 1)p^{n-1} + p^n - p^t$ ,

if  $p^t \leq i \leq p^{t+1} - 1$ ,  $1 \leq t \leq n - 1$ , and  $\text{dl } F_i = i$  otherwise. As a consequence, the number of functions with small ( $0 \leq \text{dl } F \leq p - 1$ ) or almost maximal ( $\max - p + 1 \leq \text{dl } F \leq \max$ ) nonlinearity degree is obtained. Theorems 2 and 3 give the number of functions with any prescribed nonlinearity degree for cyclic groups of order  $p^2$  and  $p^3$ .

**Keywords:** *discrete functions, nonlinearity degree.*

**Shishkin V. A. SOME PROPERTIES OF  $q$ -ARY BENT FUNCTIONS.** Let  $F$  be a function from a finite field  $Q$  to a finite field  $P$ . Here, both fields are of characteristic 2,  $|P| = q \geq 2$  and  $Q$  is the expansion of the field  $P$ . The period of  $F$  is defined as the period of the sequence  $u(i) = F(\theta^i)$  ( $\theta$  — primitive element of  $Q$ ,  $i \in \mathbb{N}_0$ ). Besides, let  $N_a(F)$  be a number of solutions in  $Q$  of equation  $F(x) = a$ ,  $a \in P$ .

Consider  $F$  to be a bent function. In this case, it is shown that if the period of  $F$  is not maximal one, then exact values of  $N_a(F)$ ,  $a \in P$ , can be derived. Moreover, if values of  $N_a(F)$ ,  $a \in P$ , are of a special form, then the value of the period of  $F$  is divisible by some exact value.

**Keywords:** *bent functions, period of a function, equations over finite fields.*

**Sholomov L. A. ON A COMPARISON OF UNDERDETERMINED ALPHABETS.**

For underdetermined alphabets, the following two concepts are defined: (a) one alphabet is stronger than another, and (b) two alphabets have equal strength. In case (b), a solution of an optimal compression problem for one of the alphabets in fact is a solution of the same problem for the other. To define concepts (a) and (b), several approaches are used. The functional approach is based on expressibility of one alphabet via another; three other approaches — combinatorial, statistical, and algorithmic — are terminologically connected with Kolmogorov's approaches to the notion of the amount of information. It is proved

that all considered approaches to comparison of alphabets are equivalent, and concepts (a) and (b) allow polynomial time verification.

**Keywords:** *underdetermined alphabet, alphabets of equal strength, entropy of underdetermined data, Kolmogorov complexity.*

*Shushuev G. I.* **VECTORIAL BOOLEAN FUNCTIONS ON DISTANCE ONE FROM APN FUNCTIONS.** The metric properties of the class of vectorial Boolean functions are studied. A vectorial Boolean function  $F$  in  $n$  variables is called a differential  $\delta$ -uniform function if the equation  $F(x) \oplus F(x \oplus a) = b$  has at most  $\delta$  solutions for any vectors  $a, b$ , where  $a \neq 0$ . In particular, if it is true for  $\delta = 2$ , then the function  $f$  is called APN. The distance between vectorial Boolean functions  $F$  and  $G$  is the cardinality of the set  $\{x \in \mathbb{Z}_2^n : F(x) \neq G(x)\}$ . It is proved that there are only differential 4-uniform functions which are on the distance 1 from an APN function.

**Keywords:** *vectorial Boolean function, differentially  $\delta$ -uniform function, APN function.*

*Tokareva N. N.* **EVERY CUBIC BOOLEAN FUNCTION IN 8 VARIABLES IS THE SUM OF NOT MORE THAN 4 BENT FUNCTIONS.** It is shown that any cubic Boolean function in 8 variables is the sum of not more than 4 bent functions in 8 variables.

**Keywords:** *bent function, cubic Boolean function, affine classification.*

## SECTION 2

*Abornev A. V.* **NONLINEAR PERMUTATIONS OF A VECTOR SPACE RECURSIVELY GENERATED OVER A GALOIS RING OF CHARACTERISTIC 4.** For any integers  $r \geq 1$  and  $m \geq 3$ , some class of nonlinear permutation of a vector space  $(\text{GF}(2^r))^m$  is constructed. Every permutation in the class is defined as a composition of two operations: (1) a linear recurring transformation with a characteristic polynomial  $F(x)$  over a Galois ring  $R$  of cardinality  $2^{2r}$  and characteristic 4; and (2) taking the first digit in an element of  $R$  represented by a pair of elements from  $\text{GF}(2^r)$ . A necessary and sufficient condition is pointed for  $F(x)$  of a certain type in the composition to provide the bijectiveness property of the composition.

**Keywords:** *digit-permutable polynomial, DP-polynomial, Galois ring.*

*Avezova Y. E., Fomichev V. M.* **ABOUT PRIMITIVENESS OF SELF-DECIMATED GENERATOR'S MIXING MATRICES.** Primitiveness conditions are obtained for mixing matrix of a  $(\delta, \tau)$ -self-decimated generator and its generalization constructed on the basis of non-linear substitutions of a vector space over a finite field. Some upper estimates for exponents of mixing matrices are given.

**Keywords:** *self-decimated generator, primitive graph, primitive matrix, exponent of matrix.*

*Agibalov G. P.* **SIBCiphers — SYMMETRIC ITERATIVE BLOCK CIPHERS COMPOSED OF BOOLEAN FUNCTIONS DEPENDING ON SMALL NUMBER OF VARIABLES.** A class of symmetric iterative block ciphers called SIBCiphers is defined. Each round of a cipher in this class encrypts bitstrings of length  $n$  into bitstrings of length  $n$  according to a system of  $n$  Boolean functions each depending on  $k \leq n$  arguments taken from the bitstring on the inputs of the round and jointly representing an injective mapping. Formally, for  $l$ -th round in a  $r$ -round SIBCipher, there exist an injection  $g^{(l)} : \{0, 1\}^n \rightarrow \{0, 1\}^n$ , Boolean functions  $g_i^{(l)} : \{0, 1\}^k \rightarrow \{0, 1\}$ , and mappings  $\eta_i^{(l)} : \{1, 2, \dots, k\} \rightarrow \{1, 2, \dots, n\}$ ,  $i = 1, 2, \dots, n$ , such that  $\{\eta_i^{(l)}(j) :$

$i = 1, 2, \dots, n; j = 1, 2, \dots, k\} = \{1, 2, \dots, n\}$  and if  $u = u_1u_2\dots u_n \in \{0, 1\}^n$ , then  $g^{(l)}(u) = g_1^{(l)}(v_1)g_2^{(l)}(v_2)\dots g_n^{(l)}(v_n)$ , where  $v_i = u_{i_1}u_{i_2}\dots u_{i_k}$  and  $i_j = \eta_i^{(l)}(j)$ ,  $i = 1, 2, \dots, n$ ;  $j = 1, 2, \dots, k$ . A round key consists of some of Boolean functions ( $g_i^{(l)}$ ) at the round and of numbers ( $\eta_i^{(l)}(j)$ ) of their actual arguments. The ciphertext bitstring is obtained by permuting the bits on the outputs of the last ( $r$ -th) round.

Contemporary symmetric iterative block ciphers with additive round keys form a subclass of SIBCiphers. Two other subclasses of SIBCiphers called by names Lucifer and Feistel are constructed according to the known cryptographic schemes originally suggested by H. Feistel and implemented in ciphers LUCIFER and DES respectively.

In SIBCipher of Feistel's subclass,  $g^{(l)}(u) = L_1R_1$  if  $u = L_0R_0$  for  $L_0, R_0 \in \{0, 1\}^{n/2}$ ,  $L_1 = R_0$  and  $R_1 = p^{(l)}(L_0) \oplus f^{(l)}(R_0)$ , where  $p : \{0, 1\}^{n/2} \rightarrow \{0, 1\}^{n/2}$  is a permutation and, for  $z = R_0$ ,  $f^{(l)}(z) = f_1^{(l)}(v_1)f_2^{(l)}(v_2)\dots f_{n/2}^{(l)}(v_{n/2})$ ,  $v_i = z_{i_1}z_{i_2}\dots z_{i_k}$ , and  $i_j = \eta_i^{(l)}(j)$  for some Boolean functions  $f_i^{(l)} : \{0, 1\}^k \rightarrow \{0, 1\}$  and for a surjective system of mappings  $\eta_i^{(l)} : \{1, 2, \dots, k\} \rightarrow \{1, 2, \dots, n/2\}$ ,  $i = 1, 2, \dots, n/2$ ;  $j = 1, 2, \dots, k$ .

SIBCipher of the subclass Lucifer is characterized by the following properties: (a)  $n = ks$ ,  $s > 1$ ; (b) for any pair  $(l, i)$ ,  $l = 1, 2, \dots, r$  and  $i = 1, 2, \dots, s$ , the mapping  $G_i^{(l)} : \{0, 1\}^k \rightarrow \{0, 1\}^k$  defined as  $G_i^{(l)}(z) = g_{(i-1)k+1}^{(l)}(z)g_{(i-1)k+2}^{(l)}(z)\dots g_{ik}^{(l)}(z)$  for all  $z \in \{0, 1\}^k$ , is a substitution; (c)  $\eta_{(i-1)k+1}^{(l)} = \eta_{(i-1)k+2}^{(l)} = \dots = \eta_{ik}^{(l)}$ ; and (d) the mapping  $p^{(l)} : \{0, 1\}^n \rightarrow \{0, 1\}^n$ , where  $p^{(l)}(u) = p_1^{(l)}(u)p_2^{(l)}(u)\dots p_s^{(l)}(u)$  and  $p_i^{(l)}(u) = u_{\eta_{ik}^{(l)}(1)}u_{\eta_{ik}^{(l)}(2)}\dots u_{\eta_{ik}^{(l)}(k)}$  for  $i = 1, 2, \dots, s$ , is a permutation.

**Keywords:** *cryptography, Boolean functions, symmetric iterative block ciphers, Feistel network, cipher LUCIFER.*

**Volgin A. V. ASYMPTOTIC PROPERTIES OF THE SET OF SOLUTIONS FOR THE DISTORTED SYSTEMS OF EQUATIONS.**

Two homogeneous systems of equations with functions of  $k$ -valued logic are considered. The functions in the second system are obtained by independent random distortions of the functions in the first one. It is proposed that the number of equations and variables in these systems increase. For the sets of their solutions, some conditions on probabilistic properties of distortions are formulated. Among them are the conditions under which (1) the probability of equality of these sets aspires to 1; (2) the probability of their intersection aspires to 1; and (3) the number of common solutions in them has a binomial limit distribution.

**Keywords:** *system of equations, functions of  $k$ -valued logic, distorted functions.*

**Pestunov A. I. INFLUENCE OF DIFFERENCE HAMMING WEIGHT ON IT'S PROPAGATION THROUGH ARITHMETIC OPERATIONS.**

Despite the fact that differential cryptanalysis is a widely used approach to cryptanalysis of iterative block ciphers, the authors of differential attacks rarely provide their strict mathematical reasoning. However, some steps in this direction have been already made. For instance, X. Lai and J. Massey (1991) suggested a model of so-called Markov iterative block cipher and formulated a hypothesis of stochastic equivalence. K. Nyberg and L. Knudsen (1994) showed that it is possible to create a cipher resistant to differential cryptanalysis, and, later, S. Vaudenay (2003) developed a model for creating such a cipher. G. P. Agibalov (2008) presented a general description of differential cryptanalysis for arbitrary iterative block ciphers with additive round keys. A. A. Selcuk analytically calculated probability of a differential attack success. A. I. Pestunov (2013) suggested a formalization of the basic differential cryptanalysis notions and used it for their systematization.

One more important, though not thoroughly investigated problem, is finding out how does two-values difference propagate through operations used in block ciphers. The problem consists in estimating the probability that a pair of values with a fixed difference is transformed by an operation into another fixed difference. For some operations (e. g. bitwise rotation or XOR) this task is rather simple, while for some commonly used operations such as modulo addition, subtraction and multiplication, it is not a trivial one.

When developing an attack on RC5, A. Biryukov and E. Kushilevitz (1998) claimed that a one-bit difference remains unchanged after modulo addition with the probability  $1/2$  (or with the probability 1 if the difference is located in the most significant bit). The claim has not been proved theoretically but the authors carried out some experiments verifying the attack. In works devoted to differential cryptanalysis of MARS and CAST-256, A. I. Pestunov (2009) used this fact referencing the paper of A. Biryukov and E. Kushilevitz and verifying developed attacks. Besides, in the second paper (about CAST-256) he used an experimentally found relation between the Hamming weight of a difference and the probability that this difference is preserved after modulo addition.

In the current paper, the existence of this relation is proved theoretically. Exactly, it is proved that the difference of two values is preserved after their modulo addition or subtraction with a third randomly chosen value with the probability  $2^{-h}$  or  $2^{-(h-1)}$ , if the most significant bit of the difference is equal to 0 or to 1 respectively. The obtained results extend the results obtained by A. I. Pestunov (2013) for one-bit differences.

**Keywords:** *differential cryptanalysis, block cipher, Hamming weight.*

*Pogorelov B. A., Pudovkina M. A.* **ON GENERALIZATIONS OF MARKOV'S APPROACH TO RESEARCH OF BLOCK CIPHERS.** For Markov block ciphers, the lumped states of Markov chains based on some partitions of the plaintexts set are considered. It is proved that such lumped states of a Markov chain generated by a sequence of intermediate ciphertexts of the Markov cipher are also a Markov chain.

**Keywords:** *Markov cipher, Markov chain, XSL block cipher, Feistel block cipher.*

*Pudovkina M. A.* **ON PROBABILITIES OF  $r$ -ROUND DIFFERENCES OF A MARKOV XSL BLOCK CIPHER WITH A REDUCIBLE LINEAR TRANSFORMATION.** Round functions in XSL block ciphers consist of three layers. The first is a key addition layer; the second is a nonlinear  $s$ -box layer; the third is a linear layer. Here, for a Markov XSL block cipher with a reducible linear transformation, instead of "classical"  $r$ -round differential characteristic used in differential technique, a  $r$ -round differential characteristic defined by the sequence of invariant subspace cosets of the linear transformation is considered.

**Keywords:** *Markov cipher, invariant set, reducible linear transformation, differential characteristic.*

*Ratseev S. M.* **CONDITIONS FOR THE EXISTENCE OF PERFECT CIPHERS WITH A FIXED SET OF PARAMETERS.** Some necessary and sufficient conditions for existence of a perfect cipher with the given sets of plaintexts and keys and a key probability distribution are presented.

**Keywords:** *cipher, perfect cipher.*

*Roman'kov V. A.* **CRYPTANALYSIS OF A DIFFIE — HELLMAN'S SCHEME ANALOGUE USING CONJUGATION AND EXPONENTIATION ON MATRIX PLATFORM.** It is proved that the mixed generalized version of the Diffie — Hellman's protocol using matrix platform with the conjugation and exponentiation in a

generic case admits computing the shared key in a polynomial time under assumption that the corresponding multiple discrete logarithm problem can be solved in a polynomial time. The computing algorithm uses the original method of linear decomposition and the approach by Menezes and others reducing the computation of the matrix exponent to the multiple discrete logarithm problem. The combination of these two approaches cannot be directly applied because the exponentiation is not automorphism. The proof of the main result is based on the analysis of belonging a monomial matrices to cosets of a matrix group by elementwise permutable subgroups. Thus, a similar question for the symmetric groups has to be studied. Fortunately, a number of results in this sphere is known.

**Keywords:** *cryptanalysis, search problem, conjugation, Diffie — Hellman's protocol.*

### SECTION 3

*Bylkov D. N.* **BOOLEAN FUNCTIONS GENERATED BY THE MOST SIGNIFICANT BITS OF LINEAR RECURRENT SEQUENCES.** The class of Boolean functions generated by the most significant bits of linear recurrent sequences over the ring  $\mathbb{Z}_2^n$  with a marked characteristic polynomial is considered. For these functions, their degree of nonlinearity is researched. It is proved that the class contains functions which are close to some bent functions.

**Keywords:** *linear recurrent sequences, most significant bit sequences, Boolean functions, degree of nonlinearity.*

*Dorokhova A. M.* **ESTIMATES FOR EXPONENTS OF MIXING GRAPHS RELATING TO SOME MODIFICATIONS OF ADDITIVE GENERATORS.** One of the positive properties of a key generator is a complete mixing of input vector sequence. It means that the all bits in output sequence  $\gamma_1\gamma_2\dots\gamma_i\dots$  depend on the all bits of the initial state. Complete mixing occurs for bits in the sequence  $\gamma_i$  when  $i \geq \exp G(\varphi)$ , where  $\varphi$  is the transformation of internal states of the generator,  $G(\varphi)$  is the mixing digraph of transformation  $\varphi$  and  $\exp G(\varphi)$  is the exponent of digraph  $G(\varphi)$ . The criterion of complete mixing is the primitiveness of digraph  $G(\varphi)$ , the necessary condition is the strong connectivity of digraph  $G(\varphi)$ . This paper is devoted to some modifications of additive generators. Well known algorithms such as Fish, Pike and Mush are based on additive generators. Native schemes of additive generators do not reach complete mixing. In order to achieve the strong connectivity of digraph  $G(\varphi)$ , the scheme of additive generator is modified by involutive permutation of vectors coordinates. The complete mixing conditions are researched for this modification of additive generator. Some sufficient conditions for primitiveness of mixing graph  $G(\varphi)$  and some estimates for  $\exp G(\varphi)$  are proved. The obtained estimates show that complete mixing of the generator output sequence can be achieved after a number of cycles, which is significantly smaller than the dimension (in bites) of the generator state.

**Keywords:** *additive generator, mixing graph of transformation, exponent of graph.*

*Ermilov D. M.* **ALGORITHM FOR CONSTRUCTING THE SYSTEM OF REPRESENTATIVES OF MAXIMAL LENGTH CYCLES OF POLYNOMIAL SUBSTITUTION OVER THE GALOIS RING.** There are no polynomials with full cycle over the Galois ring. The maximal length of cycle of polynomial mapping over the Galois ring equals  $q(q-1)p^{n-2}$ , where  $q^n$  — cardinality of ring and  $p^n$  — its characteristic. In this work, an algorithm is presented for constructing the system of representatives of all maximal length cycles of a polynomial substitution over the Galois ring. Let an elementary operation be the production in the Galois ring, then the complexity of the algorithm

equals  $O(lq^{n-1})$  elementary operations as  $n$  tends to infinity, where  $l$  is the degree of the polynomial.

**Keywords:** *nonlinear recurrent sequences, Galois ring.*

*Zakharov V. M., Zelinsky P. V., Shalagin S. V.* **MODEL OF COMPLICATION FUNCTION FOR GENERATOR OF PSEUDORANDOM SEQUENCES OVER THE FIELD  $GF(2)$ .** A complication model for pseudorandom sequences (PRS) over  $GF(2)$  is proposed. The complication function in the model is represented by the system of linear bijective transformations of bit pairs being next in turn in the sequence. Transformations in the system can vary from time to time making possible to generate a great ensemble of complicated PRS.

**Keywords:** *generator, pseudorandom sequence, the linear bijective transformation.*

*Kovalevskaya A. O.* **CONSTRUCTING TRANSITIVE POLYNOMIALS OVER THE RING  $\mathbb{Z}_{p^2}$ .** Recurrent sequences are used in cryptography as key sequences. Due to this application, it is necessary to construct polynomials with maximal period. The method for constructing all such polynomials over the ring  $\mathbb{Z}_{p^2}$  is proposed.

**Keywords:** *polynomial function over the ring, recurrent sequences, transitive polynomials.*

*Sergeeva O. E.* **THE RECOGNITION OF RECURRENT SEQUENCES GENERATED BY CONSERVATIVE FUNCTIONS.** Let  $K$  be a class of functions  $f: R^n \rightarrow R$ , where  $n = 1, 2, \dots$ . Suppose that  $S(K, N)$  is the set of all  $N$ -prefixes of recurrent sequences generated by functions from  $K$ . The recognition problem for the property “ $x \in S(K, N)$ ”, where  $x \in R^N$  and  $K$  is the class of conservative functions over the ring  $R = \mathbb{Z}_{p^m}$ , is considered. For solving this problem, an algorithm of complexity  $O(N \log^2 N)$  is offered.

**Keywords:** *conservative function, recurrent sequences, circuit of functional elements.*

#### SECTION 4

*Anjin V. A.* **CONTENT PROTECTION WITH BITSTREAM WATERMARKING AT DECRYPTION STAGE.** A new method for protecting digital video content from illegal copying is proposed. Before spreading to clients, a content is encrypted by a stream cipher with a key stream filter generator. At the same time, the latter is an encryption key of the cipher. Every client receives the content together with a decryption key which differs from the encryption key only by the filtering function. This difference is such that the decrypted content differs from the original one in several unique bits not essentially distorting the video and completely identifying the client.

**Keywords:** *content protection, bitstream watermarking, video streaming.*

*Vershinin I. S.* **PRINCIPLES OF ASSOCIATIVE STEGANOGRAPHY.** Data protection with the use of masking device which is used in two-dimensional associative processing of stylized binary images is considered to be used in the sphere of steganography. Applied to mapping, the suggested approach of stegoprotection has got an unconditional stability. The method which is under review belongs to the kind of probabilistic types of protection. Randomnicity is used with special mechanism of spatial clustering of objects masking their binary representations and randomization. The subject of protection is a set of thematic map-clusters as randomly generated (on local maps) tables in terms of “object-codes — coordinate-codes”. Protected thematic maps form the “upper layers” of geoinformation system. The original binary image is subjected to a selective effect of stochastic interference (randomization). Herewith, those parts of objects which are not

affected by interference randomly selected from the fulfilment of certain conditions. But their precise knowledge (this is the main key) allows correctly to identify objects in general by the method of two-dimensional associative search. For key generation, a basic algorithm of masking is formed.

**Keywords:** *associative steganography, two-dimensional-associative masking, protection of the cartographical data*

*Monarev V. A.* **A NEW HIGHLY ACCURATE APPROACH TO NON-DISTORTED BITMAP IMAGES QUANTITATIVE STEGANALYSIS.** The problem of detecting information, embedded into non-distorted bitmap images (such as bmp, pgm, tiff etc.) via LSB-replacement and LSB-matching methods (the latter is also known as  $\pm 1$ -steganography) is considered. There are two main approaches to address this problem in contemporary steganalysis: ordinary and quantitative. The first one is aimed at finding out only a fact of the embedding, while the second one tries to estimate a volume of the embedded information. The mostly widespread quantitative methods for detecting LSB-replacement are RS-analysis, Sample Pairs analysis, WS-steganalysis and Improved WS steganalysis. One more, a so-called shift-method, is especially effective for color images. The enlisted methods allow to detect the embedding up to 0.01 bits-per-pixel (bpp) depending on the image (in particular, noisy images are more difficult to analyse). There are no effective quantitative methods for detecting  $\pm 1$ -steganography, therefore, the most popular ones are ordinary methods Support Vector Machine and Linear Discriminant Analysis, which are able to detect up to 0.1 bpp. These methods are also can be applied to LSB-replacement and are able to detect the embedding up to 0.01 bpp. In the current paper, a new scenario and a new quantitative method within this scenario are suggested. The scenario assumes that a Warden knows exact pixels, where the information is supposed to be embedded, and it can be implemented, for instance, in the following situation. Assume that the Warden is given a device which is used for the information embedding (a key can be already injected into it). The task is to detect whether a given image has some embedded information via this device, or not. It is experimentally shown that the new method allows to detect up to 0.001 bits-per-pixel embedding, that is much more than known methods.

**Keywords:** *steganalysis, LSB-replacement, LSB-matching, embedding rate.*

*Razinkov E. V., Almeev A. N.* **QUANTITATIVE STEGANALYSIS USING BINARY CLASSIFIER.** In this paper, the problem of determining secret message length using binary steganalytic classifier is researched. It is assumed that a steganalyst is able to cut a large stego image into  $k$  smaller images and to apply the binary classification to every one of them. According to the information-theoretic approach to the steganographic security, a steganalyst's expected error calculation formula is derived. Determining the optimal choice of  $k$  depended on the properties of a binary classifier and a given image is formulated as a minimization problem. Presented approach can be used to estimate impact of various parameters on stegosystem security against quantitative steganalysis.

**Keywords:** *quantitative steganalysis, binary classification.*

## SECTION 5

*Glotov I., Ovsyannikov S., Trenkaev V.* **COMPUTATIONALLY SECURE DBMS BASED ON ORDER-PRESERVING ENCRYPTION.** The paper presents a computationally secure database management system based on order-preserving encryption.

The threat model is the following: the DB server is leased to the client thus the DB server is untrusted; the threat is a malicious database administrator who tries to learn private data by snooping on the DB server. To protect data confidentiality against this threat, it is proposed to execute queries over encrypted data on the untrusted server. Namely, to perform order operations on ciphertexts in the same way as on plaintexts, an order-preserving encryption, in particular mOPE scheme, is used. The mOPE scheme achieves IND-OCPA security, where an adversary learns no information about the plaintexts besides order. A MySQL plugin that implements a NoSQL protocol for MySQL server is developed. The NoSQL client/server protocol supports simple operations on private data, in particular it ranges queries over encrypted data. The protocol allows client applications to communicate remotely with MySQL storage engines.

**Keywords:** *secure DBMS, untrusted DB server, order-preserving encryption, NoSQL protocol.*

*Devyanin P. N.* **SECURITY CONDITIONS FOR INFORMATION FLOWS BY MEMORY WITHIN THE MROSL DP-MODEL.** Some sufficient conditions for security of information flows by memory are analysed within a mandatory entity-role security model of access and information flows control in OS Linux set (MROSL DP-model). The implementation of this conditions provides, firstly, a mandatory integrity control (MIC) preventing any modification (via a proper information flow by memory) of entities with a certain integrity level by a subject-session with a small integrity level, and, secondly, a mandatory access control (MAC) preventing information flows by memory from entities with a high level of confidentiality to entities with a low level of confidentiality.

**Keywords:** *computer security, formal model, information flow, access control.*

*Kolegov D. N.* **GENERAL METHOD FOR HTTP MESSAGES AUTHENTICATION BASED ON HASH FUNCTIONS IN WEB APPLICATIONS.** HTTP messages authentication method for web applications is offered. The method can protect web application against attack based on authentication and authorization weaknesses. It is showed how HTTP authentication can be expressed in the terms of the attribute based access control model (ABAC). Implementation of the ABAC access control decision mechanism can use an authentication cryptographic protocol.

**Keywords:** *ABAC, cryptographic protocols, message authentication, web applications.*

*Kolegov D. N., Broslavsky O. V., Oleksov N. E.* **COVERT TIMING CHANNEL OVER HTTP CACHE-CONTROL HEADERS.** The problem of detecting covert channels is known for a long time, but the detection of such channels over HTTP protocol, as one of the most used protocols, is still interesting for researchers. Known examples of covert timing channels over HTTP require changing the structure of HTTP request or modifying the web server, so it is important to discover covert channel for which there is no need to do it. Some of such channels are covert timing channels based on the cache-control headers family of HTTP protocol. The purpose of the work is the development and implementation of the covert timing channels over HTTP cache-control headers Last-Modified and ETag. As a result of the work, it is found that theoretical maximum speed of the channels based on Last-Modified (via Last-Modified value, If-Modified-Since and If-Unmodified-Since headers) is 1 bit/s. That speed is reachable in practice if latency between remote hosts allows to do the request via HTTP and to get the response in 1 second. Accuracy of implementations of the channels is 99.82% with 1 bit/s speed. Theoretical maximum speed of the channels based on ETag header (via ETag value, If-Match and If-None-Match headers) with default configuration of web server is the same as for Last-

Modified covert channels. But usage of PHP language features allows to speed up channel to 1 bit per  $(2L + T)$  seconds, where  $L$  is a latency between remote hosts and  $T$  is a time that is needed for auxiliary operations (as matching headers, storing bits, calculating sleep time etc.). These covert channels' implementations were tested on 2 bit/s speed and showed 99.55% accuracy.

**Keywords:** *computer security, covert timing channels, HTTP.*

*Milovanov T. I.* **ABOUT COVERT TIMING CHANNELS IN OS ANDROID.** Two new covert timing channels are discovered in Android software. The first one is found in the last versions of Android OS. It is based on changing the size of free space in the file system. Two malwares can use this channel for hidden communication. Two applications are developed for testing the channel. It is shown that its capacity equals 20 b/s. The second covert channel is based on a time difference for execution of a system function with some fixed secret and various open (controlled by any user) data. An information flow through the channel is realized from a legal application to a malware without permission of the legal application.

**Keywords:** *covert channels, Android, malware.*

*Ryzhkov V. I.* **USING DIGITAL CERTIFICATES FOR AUTHORIZATION BY PROXY IN OS LINUX.** In this paper, a solution for delegation of some set of rights from one user (delegator) to another (proxy user) for a fixed time period is proposed. For this goal, it is offered to use "proxies". "Proxy" is an object containing the following fields: delegator's identifier, proxy user's identifier, time period (set by delegator), list of delegated rights, and delegator's digital signature. This solution is implemented for OS Linux using OpenSSL cryptographic toolkit and pluggable authentication modules (PAM). The object "proxy" is designed as X.509 v3 certificate, and the delegated rights are specified at the field of certificate extensions. Authorization by proxy is implemented as PAM module.

**Keywords:** *electronic certificates, X.509, Linux, PAM, OpenSSL, authorization by proxy.*

*Sorokin S. N.* **FORMING INDICATORS VECTORS FOR NEURAL NETWORKS TRAINING TO DETECT ATTACKS ON WEB APPLICATIONS.** An approach for choosing the most suitable indicators to detect various types of attacks on web applications is described. A method for forming vectors of indicators for classes of attacks is proposed. The method reduces the amount of required neural networks and accelerates the process of attack detection.

**Keywords:** *intrusion detection, misuse detection, neural network, vector of indicators, intrusion classes, web application.*

*Tkachenko N. O.* **IMPLEMENTATION OF RDBMS MySQL SECURITY MONITOR IN DBF/DAM SYSTEMS.** In this article, an information is given about the development of a prototype system implementing the mandatory access control and hiding database structure features for RDBMS MySQL on the basis of a formal DP-model, database firewall and database activity monitoring solutions. Proposed prototype is implemented in Lua as a module for MySQL-proxy utility. Each transition rule of the DP-model corresponds to implemented function in the code, and special functions are added to establish interaction between elements of the MySQL-proxy system and implemented rules of the formal model.

**Keywords:** *computer security, access control implementation, DBF/DAM systems, RDBMS MySQL, MySQL-proxy.*

*Tolyupa E. A.* **METHOD TO PROVIDE SAFETY FOR CUSTOMER OF APPLICATION'S STORE.** Rapid development of Android platform is followed by creating a large number of Android applications' stores. The biggest part of mobile viruses found in 2012 is oriented on Android-devices. As a rule, the User has to trust the check procedure of the applications in store, which shares this application. Any store may be an illegal intruder intentionally sharing applications and claim that they were scanned with antivirus. In such a way, promotion of some little-known stores becomes difficult. In the present work, the method for virus extension countering through the Android stores is represented. This method is based on the usage of proxy digital signatures and of  $(n, t)$ -threshold proxy digital signature scheme with Arbitrator. The  $(n, t)$ -threshold proxy digital signature with Arbitrator allows Developer of antivirus software carrying out the sharing mechanism of a proxy and right checking applications for the presence of malicious code between  $n$  deputed Checking centres in such a manner that proxy signature can be calculated only in case of Arbitrator's participation and only if  $t$  ( $t < n$ ) Checking centres confirm the absence of viruses. The role of the Arbitrator may be laid on Certification authorities. If the User is sure of proxy signature accuracy for the file with application of the calculated  $t$  from  $n$  by Checking centres on behalf of the Developer, then he can feel certain that the application is safe and has been scanned with antivirus. Therefore, the User securely trusts the Developer of antivirus software and Certification authorities (Arbitrator) without fearing that some Checking centre will turn out to be an illegal intruder and sign insecure application. The suggested method of antivirus protection may be applied in stores for trust level increase among prospective customers.

**Keywords:** *anti-virus protection, proxy signature, threshold proxy signature, Android, application, application's store.*

*Chernov D. V.* **INTEGRITY CONTROL IN MANDATORY DP-MODEL OF DBMS MySQL.** The paper reports on mandatory integrity control mechanisms elaborated for mandatory DP-model of DBMS MySQL. The elaboration is aimed at data protection from improper modification. It allows avoid information flows from entities of lower integrity level that modify entities of higher integrity level. The paper provides new elements introduced for mandatory integrity control, describes some rules of system transformation, defines the notion of state without integrity violation and gives a necessary condition for the system to stay in this state.

**Keywords:** *access control, mandatory integrity control, information flows, formal security models.*

*Sviridov P. Y., Zaytsev G. Y., Ivachev A. S.* **THE UNIVERSAL VULNERABILITY EXPLOITATION PLATFORM FOR CTF.** Capture the Flag (CTF) is a command educational computer security competition. The aim of all CTF games is to capture flags from vulnerable services of other teams. There are a lot of routine tasks in CTF games according to many rules. In order to automate the tasks, a big software project named *Pechkin* and implemented in C++ is built. The aim of *Pechkin* is to automate the exploitation of enemy services vulnerabilities. It runs instances of exploits, manages the instances, calculates statistics, performs logging, etc. *Pechkin* has a modular architecture. Each module implements one of the pointed functions and is started by the main one called the platform. This platform connects all the modules by passing messages between them. In different games, many parameters (e.g. the jury system interface and rules) may vary setting some restrictions. *Pechkin* cares about them, and the team members are free of them. The only offensive concern left for the participants is the creative process of finding vulnerabilities

and writing exploits. The architecture allows the implementation of a scalable system with a load-balancing which is very important to CTF, because the game is long, unpredictable, and resource-draining.

**Keywords:** *CTF, flag, vulnerability, exploit.*

## SECTION 6

*Alekhina M. A., Barsukova O. U.* **UNRELIABILITY OF CIRCUITS IN THE BASIS BY ROSSER — TURKETT.** The implementation of ternary logic functions by circuits of unreliable functional gates in the basis by Rosser — Turkett is described. It is assumed that, independently of each other, any basic gate, for any input bitstring, gives the correct value with the probability  $1 - 2\varepsilon$  and can give any of two incorrect values with the probability  $\varepsilon$ . Some upper and lower bounds for the circuit reliability are obtained. It is shown, that for a certain class of functions, the bounds are found to be asymptotically equal.  
**Keywords:** *ternary logic functions, circuit of unreliable functional gates, unreliability circuit.*

*Alekhina M. A., Lakomkina A. E.* **THE RELIABILITY OF CIRCUITS IN THE BASIS OF UNRELIABLE AND ABSOLUTELY RELIABLE GATES.** The implementation of Boolean functions by circuits in the standard basis containing conjunction, disjunction and inversion is considered. It is assumed that some of the basic gates (e.g. conjunctor) are reliable, and the rest (inverter, disjunctive) are unreliable, i. e., with a probability  $\varepsilon \in (0, 1/2)$ , they are subjected to inverse faults at the outputs. It is also assumed that all unreliable circuit gates get faulty independently of each other. Some answers to the following questions are obtained: what is the unreliability of a circuit, if some of the basic elements are reliable, while others are unreliable?

**Keywords:** *absolutely reliable and unreliable functional gates, reliability of circuits, unreliability of circuits, inverse failures on outputs of gates.*

*Vasin A. V.* **ABOUT BASISES WITH UNRELIABILITY COEFFICIENT 5.** Realizations of Boolean functions by the circuits composed of unreliable elements in some complete bases are considered. It is assumed that, with probability  $\varepsilon \in (0, 1/2)$ , all elements of a circuit independently of each other are subjected to inverse failures at the outputs. It is proved that, for all considered bases, it is possible to realize almost all Boolean functions by the circuits being asymptotically optimal by reliability and functioning with the unreliability  $5\varepsilon$  as  $\varepsilon \rightarrow 0$ .

**Keywords:** *unreliable functional elements, circuits asymptotically optimal with respect to reliability, inverse failures on outputs of elements, synthesis of circuits composed of unreliable elements.*

## SECTION 7

*Druzhinin D. V.* **HYBRID COMPRESSION ALGORITHM FOR DISCRETE-TONE GRAPHICS PROCESSING.** A hybrid algorithm for fast information lossless compression of discrete-tone images is presented. The algorithm is a combination of two algorithms: special RLE implementation, which can detect vertical and horizontal redundancy, and shift algorithm, which belongs to dictionary techniques. The shift algorithm replaces three bytes, which encode pixel color, by one byte reference to pixel with the same color, which was found earlier. Presented RLE implementation can detect three region

types of pixels with the same color: vertical, horizontal lines and rectangles. Two combinations of hybrid algorithm with the known compression algorithms LZO and zlib (used on the second stage of compression) are researched. Results of practical comparison of combined algorithms among themselves and with other known algorithms are presented. As demonstrated by testing, combined algorithm, based on hybrid algorithm and zlib, gives an ability to significantly increase discrete-tone images compression ratio with an acceptable time cost.

**Keywords:** *fast compression algorithms, information lossless compression, discrete-tone graphics.*

*Zubkov A. M., Kruglov V. I.* **PROBABILISTIC CHARACTERISTICS OF WEIGHT SPECTRA OF RANDOM LINEAR SUBCODES OVER  $GF(p)$ .** For a random uniform subcode of fixed linear code over the finite field  $F_p$ , its weight spectrum is considered. Formulas for the first two moments of the weight spectrum elements and estimates for the minimal weight distribution of nonzero subcode elements are derived in terms of weight spectrum of the code. Formulas for the first two moments and the weight distribution of sum of two independent random vectors having fixed weights are also given.

**Keywords:** *linear codes, random subcodes, weight spectrum, word of minimal weight.*

## SECTION 8

*Bykov I. S.* **ON CYCLES IN FUNCTIONAL GRAPHS OF CIRCULANT TYPE GENE NETWORKS WITH THRESHOLD FUNCTIONS.** In this paper, the functioning of circulant type gene networks with threshold function are studied. All states of a system are classified according to the length of 0-series and 1-series. It is shown that all cycles of a functional graph are divided into two groups: cycles composed of states with long series and cycles composed of states with short series. Some lower estimate of the number of cycles in a functional graph is obtained. A construction for building cycles composed of states with short series is given.

**Keywords:** *gene network, threshold functions, functional graph, cycles of functional graph, states with long series, states with short series.*

*Gavrikov A. V.* **ALGORITHM FOR CONSTRUCTING T-IRREDUCIBLE EXTENSION OF POLYGONAL DIGRAPHS.** Directed graphs are mathematical models of discrete systems. T-irreducible extensions are widely used in cryptography and diagnosis of discrete systems. A polygonal graph is a digraph obtained from a circuit by some orientation of its edges. An algorithm is proposed to construct a T-irreducible extension for a polygonal graph. Correctness of the algorithm is proved.

**Keywords:** *polygonal graph, fault tolerance, T-irreducible extension.*

*Zharkova A. V.* **ON ATTRACTORS IN FINITE DYNAMIC SYSTEMS OF BINARY VECTORS ASSOCIATED WITH PALMS ORIENTATIONS.** Attractors in finite dynamic systems of binary vectors associated with the palms orientations are described, and the states belonging to them are characterized. The states of such a system are all possible orientations of a palm, and evolutionary function transforms a given palm orientation by reversing all arcs that enter into sinks.

**Keywords:** *attractor, binary vector, finite dynamic system, palm, starlike tree.*

*Komarov D. D.* **BUILDING EDGE EXTENSIONS OF STAR-LIKE TREES.** Minimal edge extension of a graph can be regarded as a model of optimal edge fault tolerant

implementation of a system. This paper is about the upper bound of the number of additional edges in a minimal edge 1-extensions for a special class of graphs — star-like trees. In this paper, a scheme for constructing an edge 1-extension for any kind of star-like trees is presented.

**Keywords:** *minimal extensions of graphs, star-like tree, fault tolerance.*

*Kyazhin S. N.* **SUFFICIENT CONDITIONS FOR LOCAL PRIMITIVENESS OF NONPRIMITIVE DIGRAPHS.** For some communication systems modelled by non-negative matrices, some important properties are reached if certain submatrices of the matrix degree are positive. In order to investigate these properties, the concepts of local primitiveness and local exponent of the matrix (digraph) connected with positivity of a certain submatrix (subgraph) of this matrix are introduced. Several sufficient conditions of local primitiveness and some bounds of local exponents for nonprimitive digraphs are presented.

**Keywords:** *primitive matrix, primitive graph, local primitiveness, local exponent.*

*Osipov D. U.* **ON A COUNTEREXAMPLE FOR A T-IRREDUCIBLE EXTENSIONS OF STAR-LIKE TREES.** T-irreducible extension of a graph  $G$  is an extension of the graph  $G$  which is obtained by removing maximal set of edges from the trivial extension of  $G$ . Here, counterexample is shown for the method by F. Harary and M. Khurum for constructing one of T-irreducible extensions for star-like trees. Besides, all nonisomorphic T-irreducible extensions are constructed for star-like trees with rays of equal length.

**Keywords:** *graph, T-irreducible extension, star-like trees, star-like trees with rays of equal length.*

*Salii V. N.* **THE SPERNER PROPERTY FOR POLYGONAL GRAPHS.** A finite partially ordered set (poset) is said to have the Sperner property if at least one of its maximum antichains is formed from elements of the same height. A polygonal graph is a directed acyclic graph derived from a circuit by some orientation of its edges. The reachability relation of a polygonal graph is a partial order. A criterion is presented for posets associated with polygonal graphs to have the Sperner property.

**Keywords:** *partially ordered set, Sperner property, polygonal graph, path, zigzag.*

*Fomichev V. M.* **ON ESTIMATIONS FOR EXPONENTS OF DIGRAPHS USING FROBENIUS'S NUMBERS.** Sufficient conditions for primitiveness of some superconnected digraphs and estimations for exponents of these digraphs are obtained using Frobenius's numbers. It is shown that these estimations are the best in many cases.

**Keywords:** *Frobenius's number, primitive graph, exponent of graph.*

## SECTION 9

*Katerinskiy D. A.* **ESTIMATION FOR AN OUTPUT SYMBOL MULTIPLICITY IN INVERTIBLE AUTOMATA.** It is shown that the maximum repetition number for an output symbol in the output table of an invertible automaton with  $n$  states and  $m$  input symbols is  $\lfloor (n+1)/2 \rfloor \lfloor (n+2)/2 \rfloor$  if  $\lfloor (n+2)/2 \rfloor \leq m$ , or  $(n-m+1)m$  otherwise.

**Keywords:** *finite automata, invertibility, weakly invertibility, strongly invertibility, output symbol multiplicity.*

*Kovalev D. S., Trenkaev V. N.* **ZAKREVSKIJ'S CIPHER FPGA IMPLEMENTATION BASED ON THE FORMULA-DEFINED RECONFIGURABLE FSM.** A new version for FPGA implementation of Zakrevskij's cipher is presented. Unlike the

previous version, here a configurable FSM is specified not by tables but by some analytical expression using the operation of modulo addition. In the paper, some numerical characteristics (throughput and area) of FPGA implementations are given for both these versions. In particular, it is shown that the throughput of PLA for the new version is up to 17–36% higher than for the previous one.

**Keywords:** *Zakrevskij's cipher, reconfigurable FSM, table-specified FSM, formula-specified FSM, throughput, area, FPGA, VHDL.*

*Pankratov I. V.* **SIMULTANEOUS SEARCH FOR SEVERAL BINARY PATTERNS IN A STREAM WITH FINITE-STATE AUTOMATON.** The task under consideration in this paper is to search for binary subsequencies in a data stream. The article offers the finite automaton able to search for a set of binary vectors simultaneously performing only two operations per every bit or even byte of the data stream. Increasing the number of searched vectors causes a slower increase in memory usage compared to overall vectors' length growth and complexity does not increase at all. The automaton is described by the transition and output tables. Estimates for the size of the automaton's tables are given. Known approaches to the problem are discussed. There is a possibility to generalize the automaton building algorithm to search for partially defined boolean patterns, but the amount of required memory may be greater than the estimate found in the paper.

**Keywords:** *bit subsequences search, string matching.*

## SECTION 10

*Gribanov A. S., Sibiryakova V. A.* **SOFTWARE IMPLEMENTATION OF OPERATIONS OVER LARGE NUMBERS IN LYaPAS-T.** In this paper, the functions working with big numbers and their integrations with the compiler LYaPAS-T are presented. These functions are inserted by the compiler into a loadable module (file with the compiled program). All these functions are written and debugged in assembly language.

**Keywords:** *LYaPAS-T, long arithmetic.*

*Zhukovskaya A. O., Stefantsov D. A.* **DEVELOPMENT OF AUTOMATED MEANS FOR PROVING PROGRAMS PROPERTIES.** A method for static program verification based on automated theorem proving is described. A function defined on the set of pairs of natural numbers lists is taken as a model for program. A function on the set of natural numbers is taken as a simplified model. The following security property is considered: only if the secret key is given to the input, the program may print the secret value to the output. The proofs for example programs are built with the Coq automated theorem prover. The common scheme for such proofs is derived and transformed into a Coq proving tactic. In conclusion, the ideas for the further researches are discussed.

**Keywords:** *verification of programs, automated proof, Coq.*

## SECTION 11

*Anashkina N. V., Shurupov A. N.* **EXPERIMENTAL COMPARISON OF SIMULATED ANNEALING AND BALAS ALGORITHMS FOR SOLVING LINEAR INEQUALITIES.** An experimental comparison of well-known heuristics — simulated annealing (SA) and Balas (BA) algorithms — are presented for solving random systems of linear inequalities (LIS) with Boolean variables. Randomness is treated in a traditional matter. Both algorithms were applied to each LIS. Experiments were divided into 10 series with 800 systems per each series. Only simultaneous inequalities were generated. The

conclusion derived from results of experiments is that probabilistic local search algorithms are more effective and time consuming in comparison with deterministic algorithms. Recommendations to joint using of BA and SA are provided. A new interpretation of random linear inequality is offered. It can be used for more exact comparison of solving algorithms for inequalities systems deduced from systems of Boolean equations.

**Keywords:** *simulated annealing, Balas algorithm, linear inequalities, random linear inequalities.*

*Bykova V. V.* **STRUCTURAL DECOMPOSITION OF GRAPHS AND ITS APPLICATION FOR SOLVING OPTIMIZATION PROBLEMS ON SPARSE GRAPHS.** The concept of a sparse graph is formalized through a numeric parameter called the treewidth of the graph. This parameter characterizes the size of cliques and separators of the graph. Sparse graphs have small treewidth. A decomposition technique for solving optimization problems on sparse graphs is proposed. This technique implements the principle of “divide and rule” and is based on the atomic representation of the input graph. By an atom of a graph is meant a maximal connected subgraph having no a clique being a minimal separator. An algorithm that creates the atomic representation of the input graph is presented. It is shown that this algorithm for graph  $G = (V, E)$  builds the atomic representation in time  $O(|V|^\tau)$ ,  $2 \leq \tau < 3$ . The atomic representation of the graph is a generalization of the decomposition of the graph into blocks using articulation points. If only clique minimum separators are used, then the set of atoms is unique to a given graph. The important properties of atoms are presented. Based on these properties, atomic representation can be used for optimization problems, which are based on the ratio of the adjacency of vertices and edges. For two problems, called All-Pairs Shortest-Path and Maximum-Clique-Problem, the results of the application of atomic representation are presented. It is shown that the time of solving these problems depends linearly on the number of vertices of the input graph. Of course, this is true if the input graph has bounded treewidth. The obtained results make it possible to handle sparse graphs, which have a very large number of vertices. For example, such graphs are Small World Graphs.

**Keywords:** *sparse graph, graph algorithms, treewidth, tree decomposition, atom graph.*

*Gotsulenko V. V.* **FORMALIZATION OF COMBINATORIAL NUMBERS IN TERMS OF ENTIRE SOLUTIONS OF SYSTEMS OF LINEAR DIOPHANTINE EQUATIONS.** Some generalizations of the number of placements with repetitions and various restrictions are considered. Counting these combinatorial numbers leads to the definition of nonnegative solutions of systems of linear Diophantine equations under appropriate additional restrictions. Generating functions and integral formulas for calculating input combinatorial numbers are obtained, and various problems that are solved with their application are discussed.

**Keywords:** *combinatorial numbers, systems of linear Diophantine equations, generating functions.*

*Zhukov K. D., Rybakov A. S.* **AN ALGORITHM FOR GENERATING A PAIR OF SPECIAL PRIMES.** In this paper, a modification is described for an algorithm generating the pair of prime integers  $p, q$  such that the integers  $g = \frac{1}{2}(p - 1, q - 1)$  and  $h = \frac{1}{2g}(pq - 1)$  are also prime. The primes  $p, q$  satisfied this condition are called *common primes*. In 2006 M. J. Hinek introduced such primes for the variant of RSA cryptosystem resistant to small private exponent attacks. The original algorithm for generating common

primes can be optimized with the modification described here. The optimized algorithm is two times faster in worst case and more times in average. It takes 19 seconds to generate a pair of 512-bit common primes  $p$ ,  $q$  with 384-bit prime  $g$ . The modification uses sieving technique which is also mentioned in the paper of M. J. Hinek. Despite the speed up of the algorithm, the generation of common primes still takes much more time than the generation of typical primes used in RSA cryptosystem.

**Keywords:** *special primes, Common Prime RSA.*

*Kuznetsov A. A., Safonov K. V.* **HALL'S POLYNOMIALS FOR FINITE TWO-GENERATOR GROUPS OF EXPONENT SEVEN.** Let  $B_k = B_0(2, 7, k)$  be the largest two-generator finite group of exponent 7 and nilpotency class  $k$ . In this class, the largest group is the group  $B_{28}$ , which has the order  $7^{20416}$ . For each  $B_k$ , a power commutator presentation is obtained.

Let  $a_1^{x_1} \dots a_n^{x_n}$  and  $a_1^{y_1} \dots a_n^{y_n}$  be two arbitrary elements in the group  $B_k$  recorded in the commutator form. Then their product is equal  $a_1^{x_1} \dots a_n^{x_n} \cdot a_1^{y_1} \dots a_n^{y_n} = a_1^{z_1} \dots a_n^{z_n}$ .

Powers  $z_i$  are to be found based on the collection process which is implemented in the computer algebra systems GAP and MAGMA. Furthermore, there is an alternative method for calculating products of elements of the group, proposed by Ph. Hall. Hall showed that  $z_i$  are polynomial functions (over the field  $\mathbb{Z}_7$  in this case) depending on the variables  $x_1, \dots, x_i, y_1, \dots, y_i$ , which are now called Hall's polynomials.

Hall's polynomials are necessary in solving problems that require multiple products of the elements of the group. Studying the structure of the Cayley graph for a group is one of these problems. The computational experiments carried out on the computer in two-generator groups of exponent five showed that the method of Hall's polynomials has an advantage over the traditional collection process. Therefore, there is a reason to believe that the use of polynomials would be preferable than the collection process in the study of Cayley graphs for  $B_k$  groups. It should be also noted that this method is easily software-implemented including multiprocessor computer systems.

Previously unknown Hall's polynomials of  $B_k$  are calculated within the framework of this paper. For  $k > 4$ , polynomials are calculated similarly but their output takes considerably more space so it makes impossible to verify the proof without use of computers.

**Keywords:** *periodic group, collection process, Hall's polynomials.*

*Shangin R. E.* **HEURISTICS FOR DESIGN OF RELIABLE TELECOMMUNICATION NETWORK.** In this paper, the problem of finding a spanning  $k$ -tree of minimum weight in a complete weighted graph is considered. Such problem has a number of applications in designing reliable telecommunication networks. This problem is known to be NP-hard and generalizes a classical problem in graphs, the Minimum Spanning Tree Problem. For solving the problem, the following four effective heuristics are offered. The first heuristic is based on the idea of a well-known Prim's algorithm, the second one is based on a dynamic programming approach, and the other two use the idea of iterative improvement of a starting solution. Preliminary numerical experiment was performed to compare the effectiveness of the proposed algorithms with known heuristics and exact algorithms. Based on the results of the computational experiment, it follows that in order to solve such problem of small and medium dimension, it is advisable to use heuristics based on iterative improvement of a starting solution, and in order to solve the problem of high dimension it is advisable to use an algorithm based on dynamic programming approach, because it computes a solution with sufficient accuracy within reasonable computing time.

**Keywords:** *spanning  $k$ -tree, invulnerable networks, NP-hard, heuristics.*