МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

ПРИКЛАДНАЯ ДИСКРЕТНАЯ МАТЕМАТИКА

Приложение

№ 17 Сентябрь 2024

Зарегистрирован в Федеральной службе по надзору
в сфере связи, информационных технологий и массовых коммуникаций
(Роскомнадзор)

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

ТРУДЫ
XXIII Международной конференции
«Сибирская научная школа-семинар
“Компьютерная безопасность и криптография” — SIBECRYPT’24»
имени Г. П. Агибалова
(Бийск, 2–7 сентября 2024 г.)

УЧРЕДИТЕЛЬ
Томский государственный университет

Адрес редакции и издателя: 634050, г. Томск, пр. Ленина, 36
E-mail: pank@mail.tsu.ru

***XXIII Международная конференция «Сибирская научная школа-семинар "Компьютерная безопасность и криптография" — SIBECRYPT'24» имени Г. П. Агибалова проведена Бийским технологическим институтом, Томским государственным университетом, Новосибирским государственным университетом и Международным математическим центром в Академгородке в сотрудничестве с Академией криптографии РФ со 2 по 7 сентября 2024 г. в г. Бийске при финансовой поддержке Международного математического центра в Академгородке** (**соглашение с Министерством науки и высшего образования РФ № 075-15-2022-282**) **и Северо-Западного центра математических исследований имени Софьи Ковалевской** (**соглашение с Министерством науки и высшего образования РФ № 075-02-2024-1430**).*

Редактор *Н. И. Шидловская*
Редактор-переводчик *Т. В. Бутузова*
Верстка *И. А. Панкратовой*

Подписано к печати 25.07.2024. Формат $60 \times 84\frac{1}{8}$. Усл. п. л. 21. Тираж 300 экз.
Заказ № 5987. Цена свободная. Дата выхода в свет 30.07.2024.

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

СОДЕРЖАНИЕ

Секция 1

ТЕОРЕТИЧЕСКИЕ ОСНОВЫ ПРИКЛАДНОЙ ДИСКРЕТНОЙ МАТЕМАТИКИ

Секция 2

ДИСКРЕТНЫЕ ФУНКЦИИ

Секция 3

МАТЕМАТИЧЕСКИЕ МЕТОДЫ КРИПТОГРАФИИ

Секция 4

МАТЕМАТИЧЕСКИЕ ОСНОВЫ ИНФОРМАТИКИ И КОМПЬЮТЕРНОЙ БЕЗОПАСНОСТИ

Секция 5

ПРИКЛАДНАЯ ТЕОРИЯ КОДИРОВАНИЯ, АВТОМАТОВ И ГРАФОВ

Секция 6

ВЫЧИСЛИТЕЛЬНЫЕ МЕТОДЫ В ДИСКРЕТНОЙ МАТЕМАТИКЕ

Секция 1

ТЕОРЕТИЧЕСКИЕ ОСНОВЫ ПРИКЛАДНОЙ ДИСКРЕТНОЙ МАТЕМАТИКИ

УДК 519.14 DOI 10.17223/2226308X/17/1

ИЗОМОРФИЗМЫ 5-КОНФИГУРАЦИЙ, ПОЛУЧАЕМЫХ ПО 2-ОРГРАФАМ

М. М. Комягин

Рассматриваются 5-конфигурации, определяемые их матрицами инциденций над полем GF(2), которые должны быть невырожденными и содержать в каждой строке и каждом столбце ровно 5 единиц, причём обратная матрица также должна обладать этим свойством. Изучаются автоморфизмы 5-конфигураций. Указывается связь между группой автоморфизмов ориентированного графа без петель и параллельных дуг с двумя входными и двумя выходными дугами при каждой вершине и группой автоморфизмов 5-конфигурации, получаемой по этому орграфу.

Ключевые слова: *k-конфигурации, k-матрицы, орграфы, группа автоморфизмов.*

Понятие k-конфигурации, введённое Ф. М. Малышевым [1], возникло в связи с производственной необходимостью в разреженных матрицах L над полем GF(2) с равномерным распределением числа единиц по строкам и столбцам матрицы, причём это свойство должно выполняться и для обратной матрицы. Матрицы с таким свойством используются в алгоритмах шифрования, например, CRYPTON [2] и ARIA [3].

Определение 1. Матрицу $L \in \mathrm{GL}(v, 2)$ называем *k-матрицей*, если у неё и у матрицы L^{-1} в каждой строке и в каждом столбце k единиц и $v - k$ нулей. Семейство из v подмножеств мощности k в множестве $X = \{1, \ldots, v\}$ с такой матрицей инциденций называем *k-конфигурацией*.

Каждая точка k-конфигурации содержится ровно в k подмножествах. Из-за невырожденности матрицы L обязательно k нечётное. Когда важен размер v матрицы L, говорим о (v, k)-матрицах.

Определение 2. Для любых подстановочных матриц $P, Q \in \mathrm{GL}(v, 2)$ матрица PLQ, получающаяся из (v, k)-матрицы L независимыми перестановками строк и столбцов, тоже (v, k)-матрица. Матрицы PLQ и L будем называть *комбинаторно эквивалентными*.

Сумму подмножеств $A, B \subseteq X$ множества X, $|X| = v$, определим равенством $A + B = (A \cup B) \setminus (A \cap B)$. Тогда множество 2^X всех подмножеств множества X с заданной на нём операцией сложения становится элементарной абелевой группой, изоморфной группе $\big(\mathrm{GF}(2)\big)^v$ по сложению. Иногда для рассматриваемых конфигураций удобнее пользоваться эквивалентным определением.

Определение 3. Совокупность $\mathcal{X} \subset 2^X$ из v подмножеств мощности k множества X, $|X| = v$, называем *k-конфигурацией*, если:

1) каждый элемент $x \in X$ принадлежит ровно k подмножествам из $\mathcal{X}$;

2) каждое одноэлементное подмножество $\{x\}$, $x \in X$, является суммой ровно k подмножеств из $\mathcal{X}$, причём каждое подмножество из $\mathcal{X}$ участвует в качестве слагаемого ровно в k суммах.

Предполагается, что соответствующий гиперграф является связным.

Матрицу инциденций для k-конфигурации $\mathcal{X}$ обозначим $L_{\mathcal{X}} = ||l_{(x,A)}||_{x\in X, A\in\mathcal{X}}$, где $l_{(x,A)} = 1 \Leftrightarrow x \in A$; k-конфигурацию с матрицей инциденций L будем обозначать $\mathcal{X}_L$.

Результаты многих авторов о строении неразложимых k-конфигураций представлены в обзоре [4]. К настоящему времени Ф. М. Малышевым получена исчерпывающая классификация $(v, 3)$-конфигураций [5]. Для $k = 5$ А. А. Фроловым найдены все $(v, 5)$-конфигурации на абелевых группах в виде 5-подмножеств, получающихся одно из другого групповым сдвигом (умножением на элемент группы) [6]. На циклических группах $(v, 5)$-конфигурации получены А. Е. Тришиным [7]. В работе [8] с помощью компьютерных вычислений найдены все $(v, 5)$-конфигурации при $v \leqslant 11$. С точностью до комбинаторной эквивалентности для ранее неизвестных $v = 9, 10, 11$ их число оказалось равным соответственно 1, 34, 386.

Не менее интересен вопрос о свойствах $(v, 5)$-конфигураций, в частности об устройстве их групп автоморфизмов. Данная работа посвящена изучению группы автоморфизмов $(v, 5)$-конфигураций, построенных по ориентированным графам без петель и параллельных дуг с двумя входными и двумя выходными дугами при каждой вершине [9].

Определение 4. Пусть на множестве X задана k-конфигурация $\mathcal{X}$, тогда подстановка $\tau \in S_X$ называется *автоморфизмом* $\mathcal{X}$, если $\mathcal{X} = \{\tau(A) : A \in \mathcal{X}\}$.

Группу автоморфизмов 5-конфигурации $\mathcal{X}$ будем обозначать $\operatorname{Aut}\mathcal{X}$.

Матрица инциденций $(v, 5)$-конфигурации является $(v, 5)$-матрицей, поэтому приведём определение автоморфизма для $(v, 5)$-матриц, эквивалентное определению 4.

Определение 5. Подстановочную матрицу P будем называть *автоморфизмом* $(v, 5)$-*матрицы* L, если существует подстановочная матрица Q, такая, что $PLQ = L$.

Группу автоморфизмов $(v, 5)$-матрицы L обозначим $\operatorname{Aut} L$.

Подстановочные матрицы будем обозначать прописными латинскими буквами, а соответствующие им подстановки — строчными латинскими буквами с крышкой, то есть если U — подстановочная матрица, то $\hat{u}$ — соответствующая ей подстановка.

Если $P \in \operatorname{Aut} L$, то $\hat{p} \in \operatorname{Aut}\mathcal{X}_L$. И наоборот, если $\hat{p} \in \operatorname{Aut}\mathcal{X}$, то $P \in \operatorname{Aut} L_{\mathcal{X}}$.

Замечание 1. Непосредственно из определений 2 и 5 следует, что группы автоморфизмов комбинаторно эквивалентных $(v, 5)$-матриц изоморфны.

Определение 6. Назовём 2-*орграфом* связный конечный ориентированный граф, без петель и параллельных дуг, у которого из каждой вершины выходит и в каждую вершину входит ровно две дуги.

Определение 7. Назовём (v, k)-матрицу L *инволютивной*, если $L^{-1} = L$.

С помощью матриц смежности 2-орграфов с t вершинами можно получать $(2t, 5)$-матрицы. Пусть B_Γ — матрица смежности 2-орграфа Γ с t вершинами. Тогда $L = \begin{pmatrix} I + B_\Gamma & B_\Gamma \\ B_\Gamma & I + B_\Gamma \end{pmatrix}$, где I — единичная матрица, является инволютивной $(2t, 5)$-матрицей. В каждой строке и в каждом столбце матрицы L ровно пять единиц и $L \cdot L = I$.

В [8] приведён критерий комбинаторной эквивалентности $(12,5)$-конфигураций, получаемых по 2-орграфам. Согласно ему, неизоморфным 2-орграфам с n вершинами отвечают комбинаторно неэквивалентные $(2n,5)$-конфигурации.

Далее будем использовать следующие обозначения:

— пусть Γ — орграф, тогда L_Γ — его матрица смежности;
— пусть L — двоичная матрица размера $n \times n$, тогда Γ_L — орграф с матрицей смежности L;
— пусть L_1, L_2 — двоичные матрицы размеров n_1, n_2 соответственно, тогда под прямой суммой матриц L_1 и L_2 будем понимать двоичную матрицу размера $n_1 + n_2$ вида $L_1 \dot{+} L_2 = \begin{pmatrix} L_1 & 0 \\ 0 & L_2 \end{pmatrix}$.

Приведём несколько фактов, полученных в ходе доказательства теоремы 1 [8].

Пусть Γ_1 и Γ_2 — 2-орграфы с n вершинами; $B = B_{\Gamma_1}$ и $D = D_{\Gamma_2}$ — их матрицы смежности; A и C — $(2n,5)$-матрицы, построенные по 2-орграфам Γ_1 и Γ_2 соответственно:

$$A = \begin{pmatrix} I+B & B \\ B & I+B \end{pmatrix}, \quad C = \begin{pmatrix} I+D & D \\ D & I+D \end{pmatrix},$$

и пусть существуют такие подстановочные матрицы $U, V \in \mathrm{GF}(2)_{2n,2n}$, что $UAV = C$. Тогда:

(1) транспозиции вида $\hat{h}_x = (x, x+n)$, где $x \in \{0, n-1\}$, лежат в группе автоморфизмов графа Γ_A;
(2) для подходящих постановочных матриц вида $H_{x_1,y_1}, \ldots, H_{x_m,y_m}, H_{z_1}, \ldots, H_{z_l}$ имеем $UH_{x_1,y_1} \ldots H_{x_m,y_m} H_{z_1} \ldots H_{z_l} A H_{x_1,y_1} \ldots H_{x_m,y_m} H_{z_1} \ldots H_{z_l} V = D$, причём $UH_{x_1,y_1} \ldots H_{x_m,y_m} H_{z_1} \ldots H_{z_l} = U_1 \dot{+} U_2$, $H_{x_1,y_1} \ldots H_{x_m,y_m} H_{z_1} \ldots H_{z_l} V = V_1 \dot{+} V_2$, где $U_1, U_2, V_1, V_2 \in \mathrm{GL}(n,2)$ — подстановочные матрицы; $\hat{h}_{x_i,y_i} = (x_i, y_i)$ — транспозиция, $x_i \in \{0, \ldots, n-1\}$, $y_i \in \{n, \ldots, 2n-1\}$, $i = 1, \ldots, m$.

Укажем несколько следствий теоремы 1 из [8].

Следствие 1. Если $(U_1 \dot{+} U_2)A(V_1 \dot{+} V_2) = C$, то $U_1 = V_1^{-1}$, $U_2 = V_2^{-1}$.

Далее $(2n,5)$-матрица L построена по 2-орграфу Γ с n вершинами.

Следствие 2. Подстановочная матрица $H_{x,y} \in \mathrm{GL}(2n,2)$, где $\hat{h}_{x,y} = (x,y)$ — транспозиция; $x \not\equiv y \pmod n$, $x \in \{0,1,\ldots,n-1\}$, $y \in \{n, n+1, \ldots, 2n-1\}$, является автоморфизмом $(2n,5)$-матрицы L тогда и только тогда, когда в матрице L_Γ и строки, и столбцы с номерами x и $y-n$ совпадают.

Лемма 1. Пусть $U = U_1 \dot{+} U_2$, $V = V_1 \dot{+} V_2$ и $ULV = L$, тогда $\hat{u}_1, \hat{u}_2 \in \mathrm{Aut}\,\Gamma$ и либо $U_2 = V_2$, либо $\hat{u}_1 \hat{u}_2^{-1} \in \mathrm{Aut}\,\Gamma$ и для любого $i \in \{0, \ldots, n-1\}$ i-я строка и i-й столбец совпадают соответственно с $\hat{u}_1\hat{u}_2^{-1}(i)$-й строкой и $\hat{u}_1\hat{u}_2^{-1}(i)$-м столбцом.

Используем следующие обозначения:

— $E = \{e_{1,1}, e_{1,2}, e_{2,1}, \ldots, e_{k,2}\}$ — подмножество множества $\{0, \ldots, n-1\}$, такое, что для любого $i \in E$ строки и столбцы матрицы B с номерами $e_{i,1}, e_{i,2}$ совпадают, а для любого $i \in \{0, \ldots, n-1\} \setminus E$ не существует $j \in \{0, \ldots, n-1\}$, $j \neq i$, такого, что строки и столбцы матрицы B с номерами i, j совпадают;
— $\bar{E} = \{0, \ldots, n-1\} \setminus E$;
— $\hat{G} = S(e_{1,1}, e_{1,2}, e_{1,1}+n, e_{1,2}+n) \times \ldots \times S(e_{k,1}, e_{k,2}, e_{k,1}+n, e_{k,2}+n)$;
— $G = \{U : \hat{u} \in \hat{G}\}$;

— $\hat{J} = \langle (s_{i.1}, s_{i,2}) : i \in \{1, \ldots, k\} \rangle$;
— $J = \{U : \hat{u} \in \hat{J}\}$;
— $\hat{H} = \big\langle (i, i+n) : i \in \bar{E} \big\rangle$ — группа, порождённая всеми транспозициями вида $(i, i+n)$, $i \in \bar{E}$;
— $H = \{U : \hat{u} \in \hat{H}\}$;
— $F = G \times H$.

С помощью фактов (1) и (2), следствий 1 и 2 и леммы 1 доказывается следующая

Теорема 1. Во введённых обозначениях имеем: F — нормальная подгруппа в $\operatorname{Aut} L$; $\hat{J}$ — нормальная подгруппа в $\operatorname{Aut} \Gamma$; $\operatorname{Aut} L/F \cong \operatorname{Aut} \Gamma/\hat{J}$.

ЛИТЕРАТУРА

1. *Малышев Ф. М., Тараканов В. Е.* О (v, k)-конфигурациях // Матем. сб. 2001. Т. 192. № 2. С. 85–108.
2. *Панасенко С. П.* Алгоритмы шифрования. Специальный справочник. СПб.: БХВ-Петербург, 2009.
3. *Kwon D.* New block cipher: ARIA // LNCS. 2009. V. 2971. P. 432–445.
4. *Малышев Ф. М.* k-Конфигурации // Труды МИАН. 2022. № 316. С. 248–269.
5. *Малышев Ф. М., Фролов А. А.* Классификация $(v, 3)$-конфигураций // Матем. заметки. 2012. Т. 91. № 5. С. 741–749.
6. *Фролов А. А.* Классификация неразложимых абелевых $(v, 5)$-групп // Дискретная математика. 2008. Т. 20. № 1. С. 94–108.
7. *Тришин А. Е.* Примеры (v, k)-матриц // Вестник ИКСИ (Сер. К). 2003. Специальный выпуск, посвященный 100-летию академика А. Н. Колмогорова. С. 179–185.
8. *Комягин М. М.* Классификация $(v, 5)$-конфигураций для $v \leqslant 11$ // Дискретная математика. 2024. Т. 36. № 1. С. 46–66.
9. *Малышев Ф. М.* Три семейства 5-конфигураций // Матем. вопр. криптогр. 2013. Т. 4. № 3. С. 83–97.

УДК 519.214 DOI 10.17223/2226308X/17/2

ТОЧНАЯ ФОРМУЛА ДЛЯ МАТЕМАТИЧЕСКОГО ОЖИДАНИЯ ЧИСЛА ПАР ОДИНАКОВЫХ s-ЦЕПОЧЕК В СЛУЧАЙНОЙ ДВОИЧНОЙ ПОСЛЕДОВАТЕЛЬНОСТИ С ЗАДАННЫМ КОЛИЧЕСТВОМ НУЛЕЙ И ЕДИНИЦ

В. И. Круглов

Рассматриваются все возможные двоичные последовательности, имеющие длину $a+b$ и состоящие из a единиц и b нулей. Для такой последовательности исследуется число пар содержащихся в ней подпоследовательностей заданной длины s (так называемых s-цепочек) с совпадающими значениями элементов этих подпоследовательностей. В предположении, что все исходные последовательности равновероятны, предлагается точная формула для числа пар s-цепочек с совпадающими значениями.

Ключевые слова: *повторения s-цепочек, математическое ожидание, урновая схема, точная формула.*

Введение

При изучении последовательностей случайных величин возникает задача о распределении числа содержащихся в них подпоследовательностей заданной длины s (так называемых s-цепочек), для которых значения соответствующих случайных величин совпадают.

В этой ситуации естественной является постановка задачи о числе точных совпадений значений s-цепочек в последовательностях независимых и одинаково распределенных случайных величин. Так, в 1974 г. А. М. Зубковым и В. Г. Михайловым в [1] доказана предельная пуассоновская теорема для числа пар s-цепочек с одинаковыми значениями случайных величин, в 1979 г. теми же авторами в [2] сформулированы достаточные условия для асимптотической нормальности числа наборов, состоящих из нескольких цепочек длины s с одинаковыми значениями.

Одним из вариантов обобщения этой задачи являются задачи о числе пар s-цепочек, для которых значения подпоследовательностей соответствующих случайных величин совпадают с точностью до перестановки, принадлежащей некоторому множеству или некоторой группе перестановок. Соответствующие исследования проводили В. Г. Михайлов, С. М. Буравлев и А. М. Шойтов [3–6].

Другим возможным направлением исследования совпадений значений s-цепочек является задача о совпадениях подпоследовательностей в последовательности таких случайных величин, которые не являются независимыми и одинаково распределёнными. В качестве такой последовательности можно рассмотреть последовательность, возникающую при извлечении без возвращения шаров из урны, содержащей шары двух цветов.

Математическое ожидание числа пар одинаковых значений s-цепочек

Пусть в урне находится a белых и b чёрных шаров, которые последовательно извлекаются из урны.

Результатом извлечения всех шаров является последовательность

$$\overrightarrow{X} = (X_1, X_2, \ldots, X_{a+b}),$$

элементы которой принимают значения 1 (белый шар) или 0 (чёрный шар), каждая такая последовательность содержит a единиц и b нулей. Будем считать, что все такие последовательности равновероятны.

Для каждого s, где $s < a$ и $s < b$, и каждого i, такого, что $1 \leqslant i \leqslant a + b - s + 1$, рассмотрим s-цепочку $Y_i = (X_i, \ldots, X_{i+s-1})$. Определим событие

$$E_{ij} = \{Y_i = Y_j\} = \{X_i = X_j, \ldots, X_{i+s-1} = X_{j+s-1}\},$$

которое заключается в совпадении значений s-цепочек Y_i и Y_j, и индикатор этого события $\eta_{ij} = \mathbb{I}(E_{ij})$. Рассмотрим случайную величину

$$\xi = \sum_{1 \leqslant i < j \leqslant a+b-s+1} \eta_{ij} = \sum_{1 \leqslant i < j \leqslant a+b-s+1} \mathbb{I}(E_{ij}),$$

равную числу совпадений s-цепочек в последовательности $\overrightarrow{X}$.

Для записи формулы математического ожидания ξ нам понадобятся следующие обозначения:

— для любых $r_a \leqslant a$ и $r_b \leqslant b$ через

$$p_{r_a,r_b} = \frac{\mathrm{C}_{a+b-r_a-r_b}^{a-r_a}}{\mathrm{C}_{a+b}^{a}}$$

будем обозначать вероятность того, что в последовательности $\overrightarrow{X}$ на заданных r_a позициях находятся белые шары и на заданных r_b позициях находятся чёрные шары;

— для каждого k из диапазона $1 \leqslant k \leqslant s-1$, разделив s на k с остатком, положим

$$s = kn + m, \quad n = \lfloor s/k \rfloor, \quad m = s - kn = s - k\lfloor s/k \rfloor,$$

и определим величину

$$f(k) = \sum_{t_1=0}^{m} \sum_{t_2=0}^{k-m} \mathrm{C}_m^{t_1} \mathrm{C}_{k-m}^{t_2} p_{t_1(n+2)+t_2(n+1),(m-t_1)(n+2)+(k-m-t_2)(n+1)}.$$

Тогда для математического ожидания ξ справедливо следующее равенство:

Теорема 1.

$$\mathsf{E}\xi = \frac{\mathrm{C}_{a+b-2s+2}^{2}}{\mathrm{C}_{a+b}^{a}} \sum_{r=0}^{s} \mathrm{C}_s^r \mathrm{C}_{a+b-2s}^{a-2r} + \sum_{i=1}^{a+b-2s+2} \sum_{k=1}^{s-1} f(k) + \sum_{i=a+b-2s+3}^{a+b-s} \sum_{k=1}^{a+b-s+1-i} f(k).$$

В таблице приведены значения $\mathsf{E}\xi$ при различных длинах цепочек s для случаев, когда числа белых и чёрных шаров в урне равны и когда число белых шаров вдвое превосходит число чёрных шаров.

$a = 100,\ b = 100$								
s	4	5	7	8	10	12	15	20
$\mathsf{E}\xi$	1182,3661	582,11936	141,04603	69,415310	16,80472	4,066233	0,483519	0,013879
$a = 200,\ b = 100$								
s	6	8	10	12	15	17	19	23
ξ	1251,2482	379,51852	115,58548	35,420300	6,120883	1,930410	0,618573	0,039026

ЛИТЕРАТУРА

1. *Зубков А. М., Михайлов В. Г.* Предельные распределения случайных величин, связанных с длинными повторениями в последовательности независимых испытаний // Теория вероятн. и её примен. 1974. Т. 19. № 1. С. 173–181.
2. *Зубков А. М., Михайлов В. Г.* О повторениях s-цепочек в последовательности независимых величин // Теория вероятн. и её примен. 1979. Т. 24. № 2. С. 267–279.
3. *Буравлев С. М.* Повторения с точностью до перестановок в последовательности независимых испытаний // Дискретная математика. 1999. Т. 11. № 1. С. 53–75.
4. *Михайлов В. Г.* Об асимптотических свойствах распределения числа пар H-связанных цепочек // Дискретная математика. 2002. Т. 14. № 3. С. 122–129.
5. *Шойтов А. М.* Предельные распределения числа наборов H-эквивалентных отрезков в равновероятной полиномиальной схеме серий // Дискретная математика. 2002. Т. 14. № 1. С. 82–98.
6. *Михайлов В. Г., Шойтов А. М.* Структурная эквивалентность s-цепочек в случайных дискретных последовательностях // Дискретная математика. 2003. Т. 15. № 4. С. 7–34.

УДК 512.772 DOI 10.17223/2226308X/17/3

ХАРАКТЕРИСТИЧЕСКИЕ МНОГОЧЛЕНЫ ГЕОМЕТРИЧЕСКИ РАЗЛОЖИМЫХ ОБЫЧНЫХ АБЕЛЕВЫХ МНОГООБРАЗИЙ РАЗМЕРНОСТИ 3[1]

С. А. Новоселов

Приводятся все возможные характеристические многочлены эндоморфизма Фробениуса геометрически разложимых обычных абелевых многообразий размерности 3 над конечным полем.

Ключевые слова: *абелевы многообразия, размерность 3, конечное поле, подсчёт точек, характеристический многочлен.*

Введение

Абелевы многообразия могут применяться в криптографии для построения криптосистем на основе задач вычисления дискретного логарифма и вычисления изогении. Как правило, для этой цели используются якобианы кривых, так как для них групповые операции наиболее эффективны. Для эксплуатации таких криптосистем необходимо уметь вычислять число точек на выбранном абелевом многообразии или, другими словами, находить порядок абелева многообразия как группы. В общем случае это сложная задача, эффективные на практике алгоритмы известны только для малой размерности. Для эллиптических кривых (абелевых многообразий размерности 1) существует быстрый алгоритм для подсчёта точек [1]. Для якобианов кривых рода 2 (абелевых многообразий размерности 2) есть полиномиальный алгоритм Годри — Шоста [2]. Однако уже в этом случае вычисление числа точек требует существенных вычислительных ресурсов. Для размерности 3 и выше вычисление числа точек уже недостижимо для криптографического размера базового конечного поля $\mathbb{F}_q$, несмотря на то, что теоретически существует полиномиальный (от $\log q$) алгоритм [3]. Опираясь на данный факт, С. Добсон, С. Галбрайт и Б. Смит предложили [4] использовать задачу подсчёта точек в качестве основы для построения криптографической функции задержки, предполагая, что атакующий не сможет быстро вычислить число точек на кривой рода 3. Геометрически разложимые абелевы многообразия изогенны над расширением базового поля декартовому произведению абелевых многообразий меньшей размерности. Это позволяет свести задачи подсчёта точек с большой размерности к более простой задаче в малой размерности.

В работе в явном виде приводятся все возможные характеристические многочлены эндоморфизма Фробениуса для обычных геометрически разложимых абелевых многообразий размерности 3 над конечным полем. Данные многочлены содержат в себе большое количество арифметической информации об абелевом многообразии, включая число точек. Более точно, если $\chi_{A,q}(T) \in \mathbb{Z}[T]$ — характеристический многочлен эндоморфизма Фробениуса абелева многообразия A, то число точек на A над конечным полем $\mathbb{F}_q$ равно $\chi_{A,q}(1)$. Наша работа — это расширение на размерность 3 известных результатов [5, §4; 6, 7] для размерности 2.

1. Характеристические многочлены для размерности 3

Над базовым полем абелево многообразие размерности 3 может быть либо простым (неразложимым), либо раскладываться как $A \sim E \times B$ или $A \sim E_1 \times E_2 \times E_3$,

[1]Работа выполнена при финансовой поддержке Минобрнауки РФ (соглашение № 075-02-2024-1430).

где E, E_1, E_2, E_3 — эллиптические кривые; B — простая абелева поверхность. Явные примеры таких разложимых абелевых многообразий размерности 3 и их характеристических многочленов можно найти в [8]. В данной работе мы рассмотрим случай, когда A — простое и обычное, но разложимое над замыканием поля (т. е. геометрически). Возможные характеристические многочлены таких абелевых многообразий размерности 3 представлены в следующей теореме.

Теорема 1. Пусть A — простое обычное геометрически разложимое абелево многообразие размерности 3, заданное над конечным полем $\mathbb{F}_q$. Предположим, что $d > 1$ — минимальное целое число, такое, что A разложимо над $\mathbb{F}_{q^d}$. Тогда $A \sim E^3$ над $\mathbb{F}_{q^d}$ и $d \in \{3, 7, 9, 14, 18\}$. Более того, пусть $t_k \in \mathbb{Z}$ такое, что $\chi_{E,q^k}(T) = T^2 - t_k T + q^k$ и $t = t_1$. Тогда выполняются следующие утверждения:

1) Если $d = 3$, то $\chi_{A,q}(T) = T^6 - t_3 T^3 + q^3$.
2) Если $d = 7$, то E — обычная эллиптическая кривая с j-инвариантом -3375 и $\chi_{A,q}(T)$ — один из двух неприводимых (над $\mathbb{Q}$) множителей многочлена
$$f_7 = T^{12} + v_1 T^{11} + v_2 T^{10} + v_3 T^9 + v_4 T^8 + v_5 T^7 + v_6 T^6 + v_5 q T^5 + v_4 q^2 T^4 + v_3 q^3 T^3 + \\ + v_2 q^4 T^2 + q^5 v_1 T + q^6,$$
где $v_1 = t$; $v_2 = (t^2 - q)$; $v_3 = t^3 - 2qt$; $v_4 = t^4 - 3qt^2 + q^2$; $v_5 = t^5 - 4qt^3 + 3q^2 t$; $v_6 = t^6 - 5qt^4 + 6q^2 t^2 - q^3$.
3) Если $d = 9$, то E — обычная эллиптическая кривая с j-инвариантом 0 и $\chi_{A,q}(T)$ — один из двух неприводимых (над $\mathbb{Q}$) множителей многочлена
$$f_9 = T^{12} + (t^3 - 3qt)T^9 + (t^6 - 6qt^4 + 9q^2 t^2 - q^3)T^6 + (q^3 t^3 - 3q^4 t)T^3 + q^6.$$
4) Если $d = 14$, то E — обычная эллиптическая кривая с j-инвариантом -3375 и $\chi_{A,q}(T)$ — один из двух неприводимых (над $\mathbb{Q}$) множителей многочлена $f_7(T)$ или $f_7(-T)$.
5) Если $d = 18$, то E — обычная эллиптическая кривая с j-инвариантом 0 и $\chi_{A,q}(T)$ — один из двух неприводимых (над $\mathbb{Q}$) множителей многочлена $f_9(T)$ или $f_9(-T)$.

Доказательство. Так как A — простое абелево многообразие, то оно изотипично (является степенью некоторого простого абелева многообразия, в нашем случае степень равна единице над базовым полем). Данное свойство сохраняется над всеми расширениями конечного поля [9, Prop. 1.2.6.1]. Поэтому если A раскладывается над $\mathbb{F}_{q^d}$, то единственный возможный вариант разложения — это $A \sim E^3$ для некоторой эллиптической кривой E. Определим теперь список возможных степеней d, над которым абелево многообразие размерности 3 может раскладываться. Пусть π — эндоморфизм Фробениуса на A над $\mathbb{F}_q$. Тогда π^d — эндоморфизм Фробениуса на A над $\mathbb{F}_{q^d}$. Благодаря результату [5, Prop. 3], известно, что для геометрически разложимых абелевых многообразий существуют два возможных случая:

1) минимальный многочлен π лежит в $\mathbb{Z}[T^d]$;
2) $\mathbb{Q}(\pi) = \mathbb{Q}(\pi^d, \zeta_d)$, где ζ_d — примитивный корень из единицы степени d. Кроме того, $\mathbb{Q}(\pi^d)$ является собственным подполем поля $\mathbb{Q}(\pi)$.

Заметим, что минимальный многочлен π равен характеристическому многочлену для обычных простых абелевых многообразий.

С л у ч а й 1. Список возможных значений d ограничен делителями $\deg \chi_{A,q} = 6$, т. е. $d = 2$ или 3. При $d = 2$ характеристический многочлен π имеет вид $\chi_{A,q}(T) = T^6 + a_2 T^4 + a_2 q T^2 + q^3$. В этом случае абелево многообразие A не может быть обычным, так

как $\operatorname{char}\mathbb{F}_q$ делит $a_3 = 0$. Поэтому этот случай мы исключаем. Пусть $d = 3$ и $\chi_{A,q}(T) = T^6 + a_3T^3 + q^3$. Тогда, используя известные рекуррентные формулы [10, § 17.1.2] для коэффициентов характеристических многочленов, можно показать, что $a_3 = -t_3$.

Случай 2. Пусть $\mathbb{Q}(\pi) = \mathbb{Q}(\pi^d, \zeta_d)$. Если $d = 2$, то $\mathbb{Q}(\pi) = \mathbb{Q}(\pi^2)$ и A тогда должно быть простым над $\mathbb{F}_{q^d}$ [5, Lemma 4]. Поэтому значение $d = 2$ мы исключаем, так как получили противоречие. Поскольку поле $\mathbb{Q}(\zeta_d)$ является подполем $\mathbb{Q}(\pi)$, то $[\mathbb{Q}(\zeta_d) : \mathbb{Q}] = \varphi(d)$ должно делить $[\mathbb{Q}(\pi) : \mathbb{Q}] = 6$. Поэтому для $\mathbb{Q}(\zeta_d) \subset \mathbb{Q}(\pi)$ допустимы только $d = 3, 4, 6$, при которых $\varphi(d) = 2$. Но $\mathbb{Q}(\pi)$ — это композит полей $\mathbb{Q}(\pi^d)$ и $\mathbb{Q}(\zeta_d)$, поэтому должно выполняться условие $[\mathbb{Q}(\pi) : \mathbb{Q}] = 6 \leqslant [\mathbb{Q}(\pi^d) : \mathbb{Q}][\mathbb{Q}(\zeta_d) : \mathbb{Q}]$. Это условие не выполняется, так как $\varphi(d) = 2$ и $[\mathbb{Q}(\pi^d) : \mathbb{Q}] = 2$ (следует из того факта, что A раскладывается на E^3 над $\mathbb{F}_{q^d}$). Поэтому случай $\mathbb{Q}(\zeta_d) \subset \mathbb{Q}(\pi)$ и соответствующие ему значения d невозможны. Остаётся рассмотреть, какие значения d возможны при $\mathbb{Q}(\pi) = \mathbb{Q}(\zeta_d)$. Здесь $\varphi(d) = 6$, соответственно $d = 7, 9, 14, 18$. Поле $\mathbb{Q}(\pi^d)$ в этом случае является, с одной стороны, квадратичным подполем $\mathbb{Q}(\zeta_d)$, с другой — кольцом эндморфизмов обычной эллиптической кривой. Круговые поля $\mathbb{Q}(\zeta_7)$, $\mathbb{Q}(\zeta_{14})$ имеют только одно квадратичное подполе — $\mathbb{Q}(\sqrt{-7})$, и существует всего один класс изоморфизмов эллиптических кривых с таким кольцом эндоморфизмов (это единственный множитель многочлена Гильберта [10, § 18.1.1]) — это эллиптические кривые с j-инвариантом -3375. Аналогично, единственное квадратичное подполе полей $\mathbb{Q}(\zeta_9)$, $\mathbb{Q}(\zeta_{18})$ — это $\mathbb{Q}(\sqrt{-3})$, которое соответствует эллиптической кривой с j-инвариантом 0. Таким образом, для случаев $d = 7, 9, 14, 18$ известны явные уравнения для кривой E, которые можно получить по стандартным формулам для j-инвариантов [10, § 18.1.1]. Найдём теперь соответствующие характеристические многочлены $\chi_{A,q}(T)$.

Так как для $d = 7, 9, 14, 18$ эллиптическая кривая E определена над базовым полем $\mathbb{F}_q$ и $A \sim E^3$ над $\mathbb{F}_{q^d}$, то абелево многообразие A — множитель [6, Prop. 3.1] спуска Вейля $W = \operatorname{Res}_{\mathbb{F}_q/\mathbb{F}_{q^d}}(E)$ кривой E. Известно, что W может быть разложено [6, Cor. 3.7] как

$$W \sim \bigoplus_{e|d} V_e(E), \tag{1}$$

где $V_e(E) \simeq \ker(\Phi_e(\pi))$; $\dim V_e(E) = \varphi(e)$; Φ_e — это e-й круговой многочлен. Так как A простое, то оно является множителем одного из абелевых многообразий $V_e(E)$ размерности $\geqslant 3$. Тогда $\chi_{A,q}(T)$ — это делитель $\chi_{V_e(E),q}(T)$ по теореме Тейта. Характеристический многочлен $\chi_{V_e(E),q}(T)$ может быть найден по формуле [6, Prop. 3.4]

$$\chi_{V_e(E),q}(T) = \alpha_1^{\varphi(e)}\alpha_2^{\varphi(e)}\Phi\left(\frac{T}{\alpha_1}\right)\Phi\left(\frac{T}{\alpha_2}\right), \tag{2}$$

где α_1, α_2 — такие, что $\chi_{E,q}(T) = (T - \alpha_1)(T - \alpha_2)$. Данную формулу можно переписать с использованием только следа Фробениуса t кривой E, заменив в ней $\alpha_1 + \alpha_2$ на t, все выражения вида $\alpha_1^k + \alpha_2^k$ на t_k и применив рекуррентную формулу из [10, Example 17.4] для выражения t_k через t.

Пусть теперь $d = 7$. Тогда $W \sim V_1(E) \oplus V_7(E)$ и A — это множитель $V_7(E)$. Эллиптическая кривая E является обычной кривой с кольцом эндоморфизмов — подполем $\mathbb{Q}(\zeta_7)$. Поэтому $V_7(E)$ изогенно декартову произведению двух неизогенных абелевых многообразий размерности 3 [6, Prop. 3.10]. Соответственно A — это одно из них. Следовательно, характеристический многочлен $\chi_{V_7(E),q}(T)$ раскладывается над $\mathbb{Q}$ на два неприводимых многочлена, один из которых равен $\chi_{A,q}(T)$. Применяя формулу (2), как описано выше, можно показать, что $\chi_{V_7(E),q}(T) = f_7$. Это завершает доказательство п. 2 теоремы 1.

Случай $d = 9$ п. 3 доказывается аналогично предыдущему. Здесь абелево многообразие A является множителем $V_9(E)$, и с помощью формулы (2) можно показать, что $\chi_{V_9(E),q}(T) = f_9$.

Пусть $d = 14$, как в п. 4 теоремы. Тогда $W \sim V_1(E) \oplus V_2(E) \oplus V_7(E) \oplus V_{14}(E)$ и A — это либо множитель $V_7(E)$, либо множитель $V_{14}(E)$. Для первого случая мы уже показали, что $f_7 = \chi_{V_7(E),q}(T)$. Многообразие $V_{14}(E)$ изогенно [6, Cor. 3.6] квадратичному кручению многообразия $V_7(E)$, поэтому $\chi_{V_{14}(E),q}(T) = \chi_{V_7(E),q}(-T) = f_7(-T)$. Случай $d = 18$ аналогичен случаю $d = 14$. ■

С помощью теоремы 1 можно легко определить характеристические многочлены для случая, когда $d = 7, 9, 14, 18$. Здесь известна явная форма кривой E с точностью до кручения и любое кручение подходит для нахождения характеристического многочлена. Эллиптическая кривая с j-инвариантом -3375 имеет уравнение $y^2 = x^3 - 125x/28 + 125/28$ для $p \neq 2, 7$, а эллиптическая кривая с j-инвариантом 0 имеет уравнение $y^2 = x^3 + 1$ для $p \neq 2, 3$. Более того, при $q = p$ кривая E с j-инвариантом -3375 может быть обычной только в случае $p \equiv 0, 1, 2, 4 \pmod 7$, в противном случае она суперсингулярна [11, § 2.2]. Аналогично, кривая E с j-инвариантом 0 может быть обычной только при $p \equiv 1 \pmod 3$.

Пример абелевого многообразия размерности 3 для случая, когда $d = 7$, можно найти в [12]. Однако нам неизвестно явных примеров для случая $d = 9$ (неявно такое многообразие можно построить с помощью спуска Вейля и его разложения по формуле (1), как показано в доказательстве теоремы 1). При этом есть примеры [13] абелевых многообразий с кольцом эндоморфизмов $\mathbb{Q}(\zeta_9)$, однако этот случай совпадает с $d = 3$.

2. Приложения

В [4] предложено использовать гиперэллиптические кривые рода 3 для построения групп с неизвестным порядком, которые являются основой для построения криптографических функций задержки. Безопасность таких криптосистем зависит от сложности решения задачи подсчёта точек. Полученные результаты предоставляют эффективный метод подсчёта точек (сведение к случаю эллиптических кривых) для гиперэллиптических кривых рода 3 с геометрически разложимым якобианом.

ЛИТЕРАТУРА

1. *Schoof R.* Counting points on elliptic curves over finite fields // J. de théorie des nombres de Bordeaux. 1995. V. 7. No. 1. P. 219–254.
2. *Gaudry P. and Schost É.* Genus 2 point counting over prime fields // J. Symbolic Comput. 2012. V. 47. No. 4. P. 368–400.
3. *Abelard S., Gaudry P., and Spaenlehauer P. J.* Improved complexity bounds for counting points on hyperelliptic curves // Foundations Comput. Math. 2019. V. 19. P. 591–621.
4. *Dobson S., Galbraith S. D., and Smith B.* Trustless groups of unknown order with hyperelliptic curves // Math. Cryptology. 2022. V. 1. No. 2. P. 25–39.
5. *Howe E. W. and Zhu H. J.* On the existence of absolutely simple abelian varieties of a given dimension over an arbitrary field // J. Number Theory. 2002. V. 92. No. 1. P. 139–163.
6. *Freeman D. M. and Satoh T.* Constructing pairing-friendly hyperelliptic curves using Weil restriction // J. Number Theory. 2011. V. 131. No. 5. P. 959–983.
7. *Chou K. M. J. and Kani E.* Simple geometrically split abelian surfaces over finite fields // J. Ramanujan Math. Soc. 2014. V. 29. No. 1. P. 31–62.

8. *Novoselov S. A. and Boltnev Yu. F.* O chisle tochek na krivoy $y^2 = x^7+ax^4+bx$ nad konechnym polem [On the number of points on the curve $y^2 = x^7+ax^4+bx$ over a finite field] // Diskretn. Anal. Issled. Oper. 2022. V. 29. No. 2. P. 62–79. (in Russian)
9. *Chai C. L., Conrad B., and Oort F.* Complex Multiplication and Lifting Problems. Providence: AMS, 2013.
10. *Cohen H., Frey G., Avanzi R., et al.* Handbook of Elliptic and Hyperelliptic Curve Cryptography. CRC Press, 2005.
11. *Arpin S., Camacho-Navarro C., Lauter K., et al.* Adventures in supersingularland // Experimental Math. 2023. V. 32. No. 2. P. 241–268.
12. Abelian variety isogeny class 3.23.al_dp_asj over $\mathbb{F}_{23}$. `https://www.lmfdb.org/Variety/Abelian/Fq/3/23/al_dp_asj`. 2024.
13. Abelian variety isogeny class 3.7.a_a_bl over $\mathbb{F}_7$. `https://www.lmfdb.org/Variety/Abelian/Fq/3/7/a_a_bl`. 2024.

УДК 519.7 DOI 10.17223/2226308X/17/4

О ПОДСТАНОВКАХ, СОВЕРШЕННО РАССЕИВАЮЩИХ КЛАССЫ РАЗБИЕНИЙ ВЕКТОРНОГО ПРОСТРАНСТВА $V_n^l(2^m)$

Б. А. Погорелов, М. А. Пудовкина

Рассматриваются разбиения $\mathbf{W}^{(n,l)}$ подмножества $\overline{V}_n^l(2^m)$ декартова произведения $V_n^l(2^m)$ векторного пространства $V_n(2^m)$ над полем $\mathbb{F}_{2^m}$, состоящего из всех l-грамм с попарно различными координатами, $l, n, m \in \mathbb{N}$, $l, n \geqslant 2$. Такие разбиения обобщают «классические» разностные разбиения при $l = 2$ и встречаются в методах криптоанализа, использующих линейность, высшие, усечённые, невозможные и кратные разности. На $V_n^l(2^m)$ задано покоординатное действие группы $S(V_n(2^m))$ на l-граммах. Описываются свойства подстановок, максимально удалённых относительно метрики Хемминга от группы, сохраняющей разбиения $\mathbf{W}$ декартова произведения $V_n^l(2^m)$. Данные подстановки названы совершенно рассеивающими разбиение $\mathbf{W}$. Указана связь между подстановками, совершенно рассеивающими разбиения $\mathbf{W}^{(n,l)}$, APN-подстановками, AB-подстановками и $2r$-разностно-равномерными подстановками, $r \geqslant 1$. Сравниваются свойства рассеивания разбиений $\mathbf{W}^{(n,3)}$ известными классами подстановок S-боксов.

Ключевые слова: *совершенное рассеивание, импримитивная группа, сплетение групп подстановок, d-разностно-равномерная подстановка, APN-подстановка, AB-подстановки, разностный метод, метод политопов, кратный разностный метод.*

Пусть $n, m, l \in \mathbb{N}$, $n \geqslant 2$, $l \geqslant 2$; $V_n(2^m)$ — n-мерное векторное пространство над полем $\mathbb{F}_{2^m}$; 0_n — вектор из $V_n(2^m)$, все координаты которого равны 0; $S(V_n(2^m))$ — симметрическая группа на $V_n(2^m)$; $\alpha^s = s(\alpha)$ — значение подстановки $s \in S(V_n(2^m))$ в точке $\alpha \in V_n(2^m)$; $AGL_n(2^m)$ — полная аффинная группа пространства $V_n(2^m)$.

Подстановка $s \in S(V_n(2^m))$ на декартовом произведении $V_n^l(2^m)$ работает следующим образом:

$$\alpha^s = (\alpha_1, \ldots, \alpha_l)^s = (\alpha_1^s, \ldots, \alpha_l^s) \quad \text{для каждого} \quad \alpha = (\alpha_1, \ldots, \alpha_l) \in V_n^l(2^m).$$

Пусть U — произвольное подмножество декартова произведения $V_n^l(2^m)$, сохраняемое $S(V_n(2^m))$, т. е. $U^g = U$ для каждой $g \in S(V_n(2^m))$. Для характеризации «рассеивания» подстановкой $s \in S(V_n(2^m))$ разбиения $\mathbf{W} = \{W_0, \ldots, W_{r-1}\}$ множества U, где

$w = |W_0| = \ldots = |W_{r-1}|$, вводится матрица $\mathbf{c}^{(\mathbf{W})}(s)$, где

$$c_{i,j}^{(\mathbf{W})}(s) = \left|\{\alpha \in W_i : \alpha^s \in W_j\}\right| = |W_i^s \cap W_j|$$

для всех $i, j \in \{0, \ldots, r-1\}$. Рассмотрим группу $\mathrm{IG}_{\mathbf{W}}$, состоящую из всех подстановок, сохраняющих разбиение $\mathbf{W}$. Она изоморфна сплетению групп подстановок $S(W_0)$ и $S(\mathbf{W})$, т. е. $\mathrm{IG}_{\mathbf{W}} \cong S_w \wr S_r$.

Для характеризации удалённости подстановки $g \in S(V_n(2^m))$ от группы $\mathrm{IG}_{\mathbf{W}}$, а также для оценивания рассеивания подстановкой s разбиения $\mathbf{W}$ введём порядок $\mathbf{W}$-примитивности

$$\chi_{\mathbf{W}}^{(U)}(s) = \min\left\{\chi_U^{(n,l)}(s,h) : h \in \mathrm{IG}_{\mathbf{W}}\right\},$$

где расстояние Хемминга $\chi_U^{(n,l)}$ на U между подстановками $s, h \in S(V_n(2^m))$ задано условием

$$\chi_U^{(n,l)}(g,h) = \left|\{\alpha \in U : \alpha^s \neq \alpha^h\}\right|.$$

Утверждение 1. Пусть $l \in \mathbb{N}$, множество $U \subseteq V_n^l(2^m)$ сохраняется группой $S(V_n(2^m))$, $\mathbf{W} = \{W_0, \ldots, W_{r-1}\}$ — разбиение множества U, $w = |W_0| = \ldots = |W_{r-1}|$. Тогда для каждой $g \in S(X)$ справедливо неравенство

$$\chi_{\mathbf{W}}^{(U)}(g) \leqslant |U| - \left\lceil w \cdot r^{-1}\right\rceil r,$$

причем равенство

$$\chi_{\mathbf{W}}^{(U)}(g) = |U| - \left\lceil w \cdot r^{-1}\right\rceil r \tag{1}$$

выполняется тогда и только тогда, когда

$$c_{i,j}^{(\mathbf{W})}(g) \leqslant \left\lceil w \cdot r^{-1}\right\rceil \text{ для всех } i, j \in \{0, \ldots, r-1\}.$$

Пусть $l \in \mathbb{N}$, множество $U \subseteq V_n^l(2^m)$ сохраняется группой $S(V_n(2^m))$, $\mathbf{W}$ — разбиение множества U на равномощные блоки. Назовём подстановку $s \in S(X)$ *совершенно рассеивающей* разбиение $\mathbf{W}$, если она находится на максимальном расстоянии Хемминга от группы $\mathrm{IG}_{\mathbf{W}}$, т. е. $\chi_{\mathbf{W}}^{(U)}(s)$ удовлетворяет равенству (1). Отметим, что свойства матрицы $\mathbf{c}^{(\mathbf{W})}(s)$, порядок $\mathbf{W}$-примитивности и аналог утверждения 1 для разбиений пространства $V_n(2)$ рассматривались ранее в [1, 2].

Пусть $\overline{V}_n^1(2^m) = V_n(2^m)$, $E^{(n,1)} = V_n(2^m) \setminus \{0_n\}$. При $l \geqslant 2$ положим

$$\overline{V}_n^l(2^m) = \left\{(\alpha_1, \ldots, \alpha_l) \in V_n^l(2^m) : \alpha_i \neq \alpha_j \text{ для всех } i, j \in \{1, \ldots, l\},\ i \neq j\right\},$$
$$E^{(n,l)} = \left\{(\varepsilon_1, \ldots, \varepsilon_l) \in V_n^l(2^m) \varepsilon_i \neq \varepsilon_j, \varepsilon_i \neq 0_n, \varepsilon_j \neq 0_n \text{ для всех } i, j \in \{1, \ldots, l\},\ i \neq j\right\}.$$

В ряде методов криптоанализа, например в разностном методе [3], методе высших разностей [4], методе усечённых разностей [5], а также в методе политопов [6, 7], кратном разностном методе [8, 9], используются разбиения множества $\overline{V}_n^l(2^m)$. В данной работе рассматривается рассеивание подстановками $s \in S(V_n(2^m))$ разбиений $\mathbf{W}^{(n,l)} = \left\{W_\varepsilon^{(n,l)} : \varepsilon \in E^{(n,l-1)}\right\}$, где

$$W_\delta^{(n,l)} = \{(\alpha, \alpha \oplus \delta_1, \ldots, \alpha \oplus \delta_{l-1}) : \alpha \in V_n(2^m)\},\ \delta = (\delta_1, \ldots, \delta_{l-1}) \in E^{(n,l-1)},$$

множества $\overline{V}_n^l(2^m)$, $l = 2, 3, \ldots$, включая разбиения, возникающие в разностном методе и его обобщениях.

Для каждого $\varepsilon \in V_n(2^m) \setminus \{0_n\}$ положим

$$A_\varepsilon(s) = \{\{\alpha_1, \alpha_2\} \subset V_n(2^m) : \alpha_1 \neq \alpha_2, (\alpha_1 \oplus \varepsilon)^s \oplus \alpha_1^s = (\alpha_2 \oplus \varepsilon)^s \oplus \alpha_2^s\}.$$

Получен критерий совершенной рассеиваемости разбиений $\mathbf{W}^{(n,l)}$ подстановкой $s \in \in S(V_n(2^m))$.

Утверждение 2. Пусть $l \geqslant 3$. Подстановка $s \in S(V_n(2^m))$ совершенно рассеивает разбиение $\mathbf{W}^{(n,l)}$ тогда и только тогда, когда $A_{\varepsilon_1}(s) \cap \ldots \cap A_{\varepsilon_{l-1}}(s) = \varnothing$ для каждого $(\varepsilon_1, \ldots, \varepsilon_{l-1}) \in E^{(n,l-1)}$.

Лемма 1. Пусть $l \geqslant 3$, $s \in S(V_n(2^m))$. Тогда для каждого $\varepsilon \in V_n(2^m) \setminus \{0_n\}$ справедливы условия $|A_\varepsilon(s)| \geqslant 2^{mn-1}$ и $\{\{\beta, \beta \oplus \varepsilon\} : \beta \in V_n(2^m)\} \subseteq A_\varepsilon(s)$.

Заметим, что $|A_\varepsilon(s)|$ — число пар элементов, для которых совпадают производные по направлению $\varepsilon \in V_n(2^m)$. Так как

$$A_\varepsilon(s) \subseteq \big\{\{\alpha_1, \alpha_2\} \subset V_n(2^m) : \alpha_1 \neq \alpha_2\big\}$$

для каждого $\varepsilon \in V_n(2^m)$, то

$$0 \leqslant |A_\varepsilon(s)| \leqslant \binom{2^{nm}}{2} = 2^{nm-1}(2^{nm} - 1). \tag{2}$$

Опишем множество подстановок $G_{n,m}^{(\varepsilon)}$, для которых достижима верхняя оценка неравенства (2).

Утверждение 3. Пусть $n \geqslant 2, \varepsilon \in V_n(2^m) \setminus \{0_n\}$, $\mathbf{W}^{(\varepsilon)} = \{\{\alpha, \alpha \oplus \varepsilon\} : \alpha \in V_n(2^m)\}$. Тогда

$$G_{n,m}^{(\varepsilon)} = \mathrm{IG}_{\mathbf{W}^{(\varepsilon)}} \cdot GL_n(2^m), \quad \left|G_{n,m}^{(\varepsilon)}\right| = 2\left(2^{nm-1}!\right)(2^{nm} - 1),$$

где $\mathrm{IG}_{\mathbf{W}^{(\varepsilon)}} \cong S_2 \wr S_{2^{m \cdot n-1}}$.

Покажем связь между подстановками, совершенно рассеивающими разбиения $\mathbf{W}^{(n,l)}$, APN-подстановками, AB-подстановками и $2r$-разностно-равномерными подстановками, $r \geqslant 1$. Напомним [10, 11], что подстановка $s \in S(V_n(2))$ называется *$2r$-разностно-равномерной*, если наибольшее число решений уравнения

$$(x \oplus \varepsilon)^s = x^s \oplus \delta$$

среди всех пар $(\varepsilon, \delta) \in (V_n(2) \setminus \{0_n\})^2$ равно $2r$. Кроме того, если $r = 1$, то 2-разностно-равномерная подстановка называется *APN-подстановкой*.

Утверждение 4. Пусть $r \geqslant 1$, s — $2r$-разностно-равномерная подстановка на $V_n(2)$. Тогда:

1) s совершенно рассеивает разбиение $\mathbf{W}^{(n,l)}$ для каждого $l \geqslant 2r + 1$;
2) s не рассеивает совершенно разбиение $\mathbf{W}^{(n,l)}$ для каждого $l \in \{1, \ldots, 2r\}$.

Пусть $\psi\colon V_{nm}(2) \to V_n(2^m)$ — естественное биективное соответствие между векторами $V_{nm}(2)$ и $V_n(2^m)$, заданное условием $\psi\colon (\beta_1, \ldots, \beta_{2^{nm}}) \mapsto (\alpha_1, \ldots, \alpha_n)$, где

$$(\beta_1, \ldots, \beta_{2^{nm}}) \in V_{nm}(2),\ \alpha_i \in \mathbb{F}_{2^m},\ \alpha_i = \big(\beta_{(i-1)m+1}, \ldots, \beta_{im}\big) \text{ для } i = 1, \ldots, n.$$

Следствие 1. Пусть $n, m \in \mathbb{N}$, $n \geqslant 2$, $s \in S(V_n(2^m))$. Тогда следующие условия эквивалентны:

1) подстановка s совершенно рассеивает разбиение $\mathbf{W}^{(n,3)}$ множества $V_n(2^m)$;
2) $|A_\varepsilon(s)| = 2^{mn-1}$ для каждого $\varepsilon \in V_n(2^m) \setminus \{0_n\}$;
3) подстановка $\tilde{s} \in S(V_{nm}(2))$, заданная условием $\tilde{s}\colon \beta \mapsto \beta^{\psi s \psi^{-1}}$ для каждого $\beta \in V_{nm}(2)$, является APN-подстановкой.

ЛИТЕРАТУРА

1. *Погорелов Б. А., Пудовкина М. А.* О расстояниях от подстановок до импримитивных групп при фиксированной системе импримитивности // Дискретная математика. 2013. Т. 25. № 3. С. 78–95.
2. *Погорелов Б. А., Пудовкина М. А.* Мультиподстановки на декартовом произведении групп и их свойства // Математические вопросы криптографии. 2023. Т. 14. № 4. С. 111–142.
3. *Biham E. and Shamir A.* Differential cryptanalysis of DES-like cryptosystems // J. Cryptology. 1991. V. 4. No. 1. P. 3–72.
4. *Lai X.* Higher order derivatives and differential cryptanalysis // Communications and Cryptography. 1994. V. 276. P. 227–233.
5. *Knudsen L. R.* Truncated and higher order differentials // LNCS. 1995. V. 1008. P. 196–211.
6. *Tiessen T.* Polytopic cryptanalysis // LNCS. 2016. V. 9665. P. 214–239.
7. *Tiessen T.* From higher-order differentials to polytopic cryptanalysis // LNCS. 2017. V. 10311. P. 544–552.
8. *Blondeau C. and Gérard B.* Multiple differential cryptanalysis: Theory and practice // LNCS. 2011. V. 6733. P. 35–54.
9. *Samajder S. and Sarkar P.* Multiple Differential Cryptanalysis: A Rigorous Analysis. Cryptology ePrint Archive. 2016. Report 2016/405. `https://eprint.iacr.org/2016/405`.
10. *Nyberg K.* Differentially uniform mappings for cryptography // LNCS. 1994. V. 765. P. 55–64.
11. *Carlet C.* Relating three nonlinearity parameters of vectorial functions and building APN functions from bent functions // Des. Codes Cryptogr. 2011. V. 59. No. 1. P. 89–109.

УДК 519.719.1 DOI 10.17223/2226308X/17/5

МЕДИАЛЬНЫЕ И ПАРАМЕДИАЛЬНЫЕ АЛГЕБРЫ СИЛЬНО ЗАВИСИМЫХ ОПЕРАЦИЙ

А. В. Черемушкин

Приводятся аналоги теорем о строении медиальных и парамедиальных квазигрупповых алгебр и некоторых их обобщений применительно к случаю сильно зависимых бинарных операций.

Ключевые слова: *n-арные квазигруппы, сильно зависимые операции, медиальные и парамедиальные операции.*

Ранее в работах автора [1–3] было показано, что многие известные результаты, формулируемые на основе бесповторных (уравновешенных) тождеств и доказанные для случая n-квазигрупп, переносятся на случай сильно зависимых операций. В данной работе продолжаются эти исследования и приводятся аналоги известных теорем о решении обобщённых медиальных и парамедиальных функциональных тождеств в классе сильно зависимых бинарных операций.

Определение 1. Группоид $(X, \cdot)$ с бинарной операцией $x \cdot y = xy$ называется *медиальным* (*парамедиальным*), если выполнено тождество (1) (соответственно (2)):

$$(1)\quad (xy)(uv) = (xu)(yv);$$
$$(2)\quad (xy)(uv) = (vy)(ux).$$

Строение медиальных и парамедиальных бинарных и n-арных квазигрупп и некоторых их обобщений описано в работах [4–8] и др., а в [9, 10] показано, что для случая сильно зависимых функций имеют место аналогичные описания.

Определение 2. Под *обобщёнными тождествами медиальности* и *парамедиальности* понимаются следующие тождества:

$$(3)\quad f_1(f_2(x,y),f_3(u,v)) = f_4(f_5(x,u),f_6(y,v));$$
$$(4)\quad f_1(f_2(x,y),f_3(u,v)) = f_4(f_5(v,y),f_6(u,x)).$$

Напомним основные определения. Пусть $n \geqslant 2$, $k \geqslant 2$ и $X = \{0,1,\ldots,k-1\}$. Функция k-значной логики (бинарная операция на множестве X) $f : X^n \to X$ называется сильно зависимой, если для всех $i = 1,\ldots,n$ найдётся фиксация всех переменных, кроме x_i, при которой полученная после фиксации функция становится подстановкой по x_i. Если $n = 2$ и $f = \circ$ — ассоциативная бинарная операция с единицей, то $(X,\circ)$ называется *моноидом*.

Решение обобщённого тождества медиальности для случая бинарных квазигрупп приведено в работах [11–14]. Для случая сильно зависимых функций имеет место аналогичное утверждение, в котором термин «группа» заменён на «моноид».

Далее будем записывать действие подстановок на X слева. Тогда произведению подстановок $\alpha\beta$ соответствует запись

$$\alpha\beta x = \beta(\alpha(x)).$$

Теорема 1. Последовательность $(f_1,\ldots,f_6)$ сильно зависимых функций на конечном множестве X является решением обобщённого тождества медиальности (3) в том и только в том случае, когда существуют коммутативный моноид $(X,\circ)$ и биекции $\alpha_1,\ldots,\alpha_6$, такие, что

$$f_1(x,z) = \alpha_5 x \circ \alpha_6 z,\quad f_2(x,y) = \alpha_5^{-1}(\alpha_1 x \circ \alpha_2 y),\quad f_3(u,v) = \alpha_6^{-1}(\alpha_3 u \circ \alpha_4 v),$$
$$f_4(z,y) = \alpha_7 z \circ \alpha_8 y,\quad f_5(x,u) = \alpha_7^{-1}(\alpha_1 x \circ \alpha_3 u),\quad f_6(y,v) = \alpha_8^{-1}(\alpha_2 y \circ \alpha_4 v).$$

Аналогичное описание получается в парамедиальном случае.

Теорема 2. Последовательность $(f_1,\ldots,f_6)$ сильно зависимых функций на конечном множестве X является решением обобщённого тождества парамедиальности (4) в том и только в том случае, когда существуют коммутативный моноид $(X,\circ)$ и биекции $\alpha_1,\ldots,\alpha_6$, такие, что выполняются равенства

$$f_1(x,z) = \alpha_5 x \circ \alpha_6 z,\quad f_2(x,y) = \alpha_5^{-1}(\alpha_1 x \circ \alpha_2 y),\quad f_3(u,v) = \alpha_6^{-1}(\alpha_3 u \circ \alpha_4 v),$$
$$f_4(z,y) = \alpha_7 z \circ \alpha_8 y,\quad f_5(v,y) = \alpha_7^{-1}(\alpha_4 v \circ \alpha_2 y),\quad f_6(u,x) = \alpha_8^{-1}(\alpha_3 u \circ \alpha_1 x).$$

Приведём несколько следствий. Пусть $\mathcal{F}_2 \colon X^2 \to X$ — множество двуместных функций и $F \subseteq \mathcal{F}_2$. Рассмотрим несколько обобщённых функциональных тождеств для произвольных функций $f, g \in F$:

$$(5)\quad f(g(x,y),g(u,v)) = g(f(x,u),f(y,v))\quad (\textit{mediality});$$
$$(6)\quad f(g(x,y),g(u,v)) = g(f(v,y),f(u,x))\quad (\textit{paramediality});$$
$$(7)\quad f(g(x,y),g(u,v)) = f(g(x,u),g(y,v))\quad (\textit{co-mediality});$$
$$(8)\quad f(g(x,y),g(u,v)) = f(g(v,y),g(u,x))\quad (\textit{co-paramediality}).$$

Определение 3. Если для любых $f, g \in F$ выполняется тождество (5), то алгебра (X,F) называется *медиальной*; если тождество (6), то *парамедиальной*; если тождество (7), то *ко-медиальной*; если тождество (8), то *ко-парамедиальной*.

Такие алгебры с квазигрупповыми операциями исследованы в работах [13–16] и др. Заметим, что в работе [17] описаны алгебры, удовлетворяющие тождествам вида (3) и (4), в которых применены всевозможные перестановки переменных в правой части. Например, для случая медиальных бинарных квазигрупповых операций справедлива

Теорема 3 [15, теорема 1]. Если алгебра $(X, \{h_1, \ldots, h_m\})$, где $h_1, \ldots, h_m$ — бинарные квазигруппы, является медиальной, то существует абелева группа $(X, +)$, такая, что

$$h_i(x, y) = \alpha_i x + \beta_i y + c_i,$$

где α_i, β_i — автоморфизмы группы $(X, +)$; $c_i \in Q$ и

$$\alpha_i\beta_j = \beta_j\alpha_i, \quad \alpha_i\alpha_j = \alpha_j\alpha_i, \quad \beta_i\beta_j = \beta_j\beta_i$$

при всех $i, j = 1, \ldots, m$. Группа $(X, +)$ определена однозначно с точностью до изоморфизма.

Теоремы 1 и 2 позволяют получить аналогичные описания для случая алгебр сильно зависимых бинарных операций.

Теорема 4. Если алгебра $(X, \{h_1, \ldots, h_m\})$, где $h_1, \ldots, h_m$ — сильно зависимые бинарные операции, является медиальной, то существует коммутативный моноид $(X, \circ)$, такой, что

$$h_i(x, y) = \alpha_i x \circ \beta_i y \circ c_i,$$

где α_i, β_i — автоморфизмы моноида $(X, \circ)$; $c_i \in X$ и

$$\alpha_i\beta_j = \beta_j\alpha_i; \quad \alpha_i\alpha_j = \alpha_j\alpha_i, \quad \beta_i\beta_j = \beta_j\beta_i, \quad h_j(c_i, c_i) = h_i(c_j, c_j)$$

при всех $i, j = 1, \ldots, m$. Моноид $(X, \circ)$ определён однозначно с точностью до изоморфизма.

Теорема 5. Если алгебра $(X, \{h_1, \ldots, h_m\})$, где $h_1, \ldots, h_m$ — сильно зависимые бинарные операции, является парамедиальной, то существует коммутативный моноид $(X, \circ)$, такой, что

$$h_i(x, y) = \alpha_i x \circ \beta_i y \circ c_i,$$

где α_i, β_i — автоморфизмы моноида $(X, \circ)$; $c_i \in X$ и

$$\alpha_i\beta_j = \alpha_j\beta_i, \quad \beta_i\alpha_j = \beta_j\alpha_i, \quad \alpha_i\alpha_j = \beta_j\beta_i, \quad h_j(c_i, c_i) = h_i(c_j, c_j)$$

при всех $i, j = 1, \ldots, m$. Моноид $(X, \circ)$ определён однозначно с точностью до изоморфизма.

Утверждение 1. Если f, g — сильно зависимые бинарные операции, удовлетворяющие тождеству (7) ко-медиальности, то существуют коммутативный моноид $(X, \circ)$, биекции α, β, обратимые элементы $b, c \in X$ и автоморфизм моноида $\xi \in \mathrm{Aut}(\circ)$, такие, что

$$f(x, y) = \xi R_c \alpha x \circ \alpha y,$$
$$g(x, y) = \alpha^{-1}(\beta x \circ R_b^{-1}\xi^{-1}\beta y).$$

Моноид $(X, \circ)$ определён однозначно с точностью до изоморфизма.

Теорема 6. Если алгебра $(X, \{f, g\})$, где f, g — сильно зависимые бинарные операции, является ко-медиальной, то существует коммутативный моноид $(X, \circ)$, биекция α, автоморфизмы моноида $\xi, \psi \in \mathrm{Aut}(\circ)$ и обратимые элементы $m, l \in X$, такие, что

$$f(x, y) = \xi\alpha x \circ \alpha y \circ m,$$
$$g(x, y) = \alpha^{-1}(\psi x \circ \xi^{-1}\psi y \circ l).$$

Моноид $(X, \circ)$ определён однозначно с точностью до изоморфизма, а α и ξ при некоторых $s, c \in X$ удовлетворяют тождеству

$$\xi(\alpha x \circ s) = \alpha(\xi x \circ c).$$

Утверждение 2. Если f, g — сильно зависимые бинарные операции, удовлетворяющие тождеству (8) ко-парамедиальности, то существуют моноид $(X, \circ)$, биекции α, β, обратимые элементы $a, c \in X$ и автоморфизм моноида $\xi \in \mathrm{Aut}(\circ)$, такие, что

$$f(x, y) = \xi R_c\alpha x \circ \alpha y,$$
$$g(x, y) = \alpha^{-1}(R_a^{-1}\xi^{-1}\beta x \circ \beta y).$$

Моноид $(X, \circ)$ определён однозначно с точностью до изоморфизма.

Теорема 7. Если алгебра $(X, \{f, g\})$, где f, g — сильно зависимые бинарные операции, является ко-парамедиальной, то существует моноид $(X, \circ)$, биекция α, автоморфизмы моноида $\xi, \psi \in \mathrm{Aut}(\circ)$ и обратимые элементы $m, l \in X$, такие, что

$$f(x, y) = \xi\alpha x \circ \alpha y \circ m,$$
$$g(x, y) = \alpha^{-1}(\xi^{-1}\psi x \circ \psi y \circ l).$$

Моноид $(X, \circ)$ определён однозначно с точностью до изоморфизма, а α и ξ при некоторых $s, c \in X$ удовлетворяют тождеству

$$\xi(\alpha x \circ s) = \alpha(\xi x \circ c).$$

ЛИТЕРАТУРА

1. *Черемушкин А. В.* Аналоги теорем Глускина — Хоссу и Малышева для случая сильно зависимых n-арных операций // Дискретная математика. 2018. Т. 30. № 2. С. 15–24.
2. *Черемушкин А. В.* Теорема Поста для сильно зависимых n-арных полугрупп // Дискретная математика. 2019. Т. 31. № 2. С. 152–157.
3. *Черемушкин А. В.* Частично обратимые сильно зависимые n-арные операции // Математический сборник. 2020. Т. 211. № 3. С. 141–158.
4. *Toyoda K.* On axioms of linear functions // Proc. Imp. Acad. Tokyo. 1941. V. 17. P. 221–227.
5. *Němec P. and Kepka T.* T-quasigroups (Part I) // Acta Univ. Carolinae. Math. Phis. 1971. V. 1. P. 39–49.
6. *Cho J. R., Ježek J., and Kepka T.* Paramedial groupoids // Czechoslovak Math. J. 1999. V. 49. No. 2. P. 277–290.
7. *Ehsani A.* Representation of the medial-like algebras // N. Galatos, A. Kurz, and C. Tsinakis (eds.). TACL 2013 (EPiC Ser. V. 25). P. 64–67.
8. *Ehsani A., Movsisyan Y., and Arslanov M.* A representation of paramedial n-ary groupoids // Asian-Europ. J. Math. 2014. V. 7. No. 1. P. 1450020-1–1450020-17.
9. *Черемушкин А. В.* Медиальные сильно зависимые n-арные операции // Дискретная математика. 2020. Т. 32. № 2. С. 112–121.

10. *Черемушкин А. В.* Парамедиальные сильно зависимые n-арные операции // Дискретная математика (принята к публикации).
11. *Aczél J., Belousov V. D., and Hossú M.* Generalized associativity and bisymmetry on quasigroups // Acta Math. Acad. Sci. Hungar. 1960. V. 11. No. 11-2. P. 127–136.
12. *Nazari E. and Movsisyan Y. M.* Transitive modes // Demonstratio Math. 2011. V. 44. No. 3. P. 511–522.
13. *Ehsani A.* Linear representation of algebras with non-associative operations which are satisfy in the balanced functional equations // J. Phys.: Conf. Ser. 2015. V. 622. Article 012037.
14. *Ehsani A., Krapež A., and Movsisyan Y.* Algebras with parastrophically uncancellable quasigroup equations // Buletinul Academiei de Stiinte a Republicii Moldova. Matematica. 2016. No. 1. P. 41–63.
15. *Ehsani A.* On medial-like functional equations // Math. Problems Computer Sci. 2012. V. 38. P. 53–55.
16. *Ehsani A. and Movsisyan Y.* Linear representation of medial-like algebras // Comm. Algebra. 2013. V. 41. No. 9. P. 3429–3444.
17. *Ehsani A., Krapež A., and Movsisyan Y.* Algebras with Medial-like Functional Equations on Quasigroups. `https://arxiv.org/abs/1505.06224`. 2015.

Секция 2

ДИСКРЕТНЫЕ ФУНКЦИИ

УДК 519.7 DOI 10.17223/2226308X/17/6

О ЧИСЛЕ БЛИЖАЙШИХ БЕНТ-ФУНКЦИЙ К НЕКОТОРЫМ БЕНТ-ФУНКЦИЯМ МЭЙОРАНА — МАКФАРЛАНДА[1]

Д. А. Быков, Н. А. Коломеец

Рассматривается количество ближайших бент-функций к некоторым бент-функциям из класса Мэйорана — МакФарланда $\mathcal{M}_{2n}$, близкое к оценкам для него: нижней $\ell_{2n} = 2^{2n+1} - 2^n$ и точной верхней $\mathcal{L}_{2n}$. Для бент-функций вида $f(x, y) = \langle x, \sigma(y)\rangle \oplus \varphi(y) \in \mathcal{M}_{2n}$, где σ построена с помощью функции инверсии элементов конечного поля, подсчитано число ближайших бент-функций при тождественно нулевой φ, а также показано, что для некоторой подходящей φ количество ближайших к f бент-функций меньше чем $\ell_{2n} + 82(2^n - 1)$, т. е. равно $\ell_{2n} + o(\ell_{2n})$ при $n \to \infty$. Получена формула числа бент-функций, ближайших к $f(x, y) = \langle x, y\rangle \oplus y_1 y_2 \dots y_m \in \mathcal{M}_{2n}$, где $3 \leqslant m \leqslant n$. Для $m = 3$ и $m = n$ это число равно $o(\mathcal{L}_{2n})$ и $\frac{1}{3}\mathcal{L}_{2n} + o(\mathcal{L}_{2n})$ соответственно при $n \to \infty$. Приведена полная классификация $\mathcal{M}_6$ по числу ближайших бент-функций.

Ключевые слова: *аффинные подпространства, бент-функции, класс Мэйорана — МакФарланда, минимальное расстояние, ближайшие функции.*

Введение

Обозначим через $\mathbb{F}_2^n$ линейное пространство двоичных векторов размерности n над полем $\mathbb{F}_2$ из двух элементов, а сложение в нём — через $\oplus$. Функция $f : \mathbb{F}_2^n \to \mathbb{F}_2$ называется *булевой*. *Расстояние Хэмминга* между $f, g : \mathbb{F}_2^n \to \mathbb{F}_2$ — количество векторов из $\mathbb{F}_2^n$, на которых значения f и g различны. *Бент-функцией* называется булева функция от $m = 2n$ переменных, находящаяся на максимально возможном расстоянии от множества всех *аффинных* функций, т. е. функций вида $\langle a, x\rangle \oplus c$, где $a, x \in \mathbb{F}_2^m$, $c \in \mathbb{F}_2$ и $\langle a, x\rangle = a_1 x_1 \oplus \ldots \oplus a_m x_m$. Бент-функции имеют приложения в криптографии, теории кодирования, комбинаторике и др. [1]. Они были введены в 1960-х годах, название «бент-функция» появилось в работе О. Ротхауса [2], а в СССР В. А. Елисеев и О. П. Степченков называли их *минималъными* (см. [1]). Самым простым классом бент-функций является класс Мэйорана — МакФарланда $\mathcal{M}_{2n}$ [3], который составляют бент-функции вида

$$f(x, y) = \langle x, \pi(y)\rangle \oplus \varphi(y),$$

где $x, y \in \mathbb{F}_2^n$, $\varphi : \mathbb{F}_2^n \to \mathbb{F}_2$ и π — подстановка на $\mathbb{F}_2^n$.

В данной работе исследуется количество ближайших бент-функций к некоторым заданным бент-функциям $f \in \mathcal{M}_{2n}$, где ближайшими являются бент-функции на расстоянии 2^n от f [4]. Такие бент-функции изучались в [5–8]. Главным образом, мы

[1]Работа выполнена при поддержке Математического центра в Академгородке, соглашение с Министерством науки и высшего образования Российской Федерации № 075-15-2022-282.

рассматриваем такие f, количество ближайших бент-функций к которым близко к соответствующим нижней и верхней оценкам

$$\ell_{2n} = 2^{2n+1} - 2^n \quad \text{и} \quad \mathcal{L}_{2n} = 2^n(2^1+1)(2^2+1)\dots(2^n+1).$$

Известно, что верхняя оценка $\mathcal{L}_{2n}$ достигается при всех n на всех квадратичных бент-функциях, и только на них [6]. Нижняя оценка ℓ_{2n} достигается, например, при простых $n \geqslant 5$ [7], а также если n является степенью таких простых чисел [8]. Заметим, что количество ближайших к f бент-функций равно количеству аффинных подпространств $\mathbb{F}_2^{2n}$ размерности n, на которых f аффинна [4]. Поскольку любая $f \in \mathcal{M}_{2n}$ «собрана» из 2^n аффинных функций от n переменных, то функции, количество ближайших бент-функций к которым близко к $\mathcal{L}_{2n}$, можно считать «простыми», а если количество близко к ℓ_{2n} — наиболее «сложными».

1. Количество ближайших бент-функций, близкое к минимальному, и классификация $\mathcal{M}_6$

Рассмотрим бент-функции $f \in \mathcal{M}_{2n}$, количество ближайших бент-функций к которым близко к нижней оценке ℓ_{2n}. В качестве подстановки будем использовать функцию $\sigma : \mathbb{F}_2^n \to \mathbb{F}_2^n$, являющуюся функцией инверсии элементов конечного поля $x \mapsto x^{2^n-2}$, $x \in \mathbb{F}_{2^n}$, если рассматривать $\mathbb{F}_{2^n}$ как $\mathbb{F}_2^n$, зафиксировав в $\mathbb{F}_{2^n}$ некоторый базис. Все дальнейшие результаты справедливы вне зависимости от выбора конкретного базиса.

Утверждение 1. Количество ближайших к $f(x,y) = \langle x, \sigma(y)\rangle \in \mathcal{M}_{2n}$ бент-функций равно

$$2^{2n+1} - 2^n + 2^{3n-1} + \sum_{k|n,\ 1<k<n} \frac{2^n-1}{2^k-1} 2^{3k-1}.$$

Данное количество существенно ниже верхней оценки $\mathcal{L}_{2n}$, но и заметно больше нижней оценки. Однако существуют бент-функции, количество ближайших бент-функций к которым имеет ту же асимптотику, что и ℓ_{2n}.

Теорема 1. Существует некоторая $\varphi : \mathbb{F}_2^n \to \mathbb{F}_2$, такая, что количество ближайших к $f(x,y) = \langle x, \sigma(y)\rangle \oplus \varphi(y) \in \mathcal{M}_{2n}$ бент-функций меньше чем $\ell_{2n} + 82(2^n-1)$. Асимптотически это $\ell_{2n} + o(\ell_{2n})$.

В некоторых случаях теорема влечёт достижимость ℓ_{2n}.

Следствие 1. Пусть k — минимальный нетривиальный делитель n, $k \geqslant 5$ и $n \leqslant 2^k - k^2 - k - 3$. Тогда количество ближайших к некоторой $f(x,y) = \langle x, \sigma(y)\rangle \oplus \varphi(y) \in \mathcal{M}_{2n}$ бент-функций равно ℓ_{2n}.

Например, данному условию на n удовлетворяют числа 11·13, 11·11·13, 11·17 и др. Известно также, что нижняя оценка ℓ_{2n}:

- достигается при $n = 1$ для всех функций из $\mathcal{M}_2$, так как $\ell_2 = \mathcal{L}_2 = 6$;
- не достигается для $n = 2$, при этом все функции из $\mathcal{M}_4$ являются квадратичными, количество ближайших бент-функций к которым равно $\mathcal{L}_4$ [5];
- не достигается для $n = 4$ [7];
- достигается для $n = 5, 6, 7$ [7];
- не известно, достигается ли для $n = 8, 9, 10$ и большинства больших n.

Вопрос достижимости оценки ℓ_{2n} прямо связан [7] с вопросом существования взаимно однозначных APN-функций [9], который является открытым для чётных $n \geqslant 8$. Для пропущенного в списке $n = 3$ оценка не достигается. Однако в этом случае можно охарактеризовать количество ближайших бент-функций к любой функции из $\mathcal{M}_6$.

Теорема 2. Пусть $f(x,y) = \langle x, \pi(y)\rangle \oplus \varphi(y) \in \mathcal{M}_6$. Тогда f имеет следующее количество ближайших бент-функций:

1) 1080, если π — аффинна и $\deg\varphi \leqslant 2$;
2) 568, если
   а) π — аффинна и $\deg\varphi = 3$,
   б) π не аффинна и $\delta(\pi) = 8$;
3) 440, если $\delta(\pi) = 4$;
4) 376, если $\delta(\pi) = 2$.

Здесь $\deg\varphi$ — степень полинома Жегалкина функции φ, а $\delta(\pi)$ — *порядок дифференциальной равномерности* π, т. е. минимальное t, для которого уравнение $\pi(x) \oplus \oplus \pi(a \oplus x) = b$ при любых параметрах $a \in \mathbb{F}_2^n \setminus \{0\}$ и $b \in \mathbb{F}_2^n$ имеет не более t решений. При $n = 3$ и взаимно однозначных $\pi : \mathbb{F}_2^3 \to \mathbb{F}_2^3$ справедливо $\delta(\pi) \in \{2, 4, 8\}$, т. е. теорема 2 характеризует все функции из $\mathcal{M}_6$.

Она также является и классификацией $\mathcal{M}_6$ относительно EA-эквивалентности: функции $f, g : \mathbb{F}_2^n \to \mathbb{F}_2$ *EA-эквивалентны*, если

$$g(x) = f(xA \oplus a) \oplus h(x) \text{ для всех } x \in \mathbb{F}_2^n,$$

где A — невырожденная двоичная матрица порядка n; $a \in \mathbb{F}_2^n$ и $h : \mathbb{F}_2^n \to \mathbb{F}_2$ — аффинная фунция (см. [10] о методах классификации). Действительно, количество ближайших бент-функций является инвариантом относительно EA-эквивалентности. В то же время известно [2], что всё множество бент-функций от шести переменных состоит из четырёх классов EA-эквивалентности. Таким образом, все эти четыре класса представлены в теореме 2.

2. Количество ближайших бент-функций, близкое к максимальному

Рассмотрим бент-функции $f \in \mathcal{M}_{2n}$, количество ближайших бент-функций к которым близко к максимально возможному $\mathcal{L}_{2n}$. Для удобства в качестве π будем рассматривать тождественное отображение, т. е. $f(x,y) = \langle x, y\rangle \oplus \varphi(y)$. Однако можно расширить подкласс функций с таким же числом ближайших к ним бент-функций.

Утверждение 2. Пусть $f, g \in \mathcal{M}_{2n}$, $f(x,y) = \langle x, y\rangle \oplus \varphi(y)$ и $g(x,y) = \langle x, \pi(y)\rangle \oplus \oplus \psi(y) \in \mathcal{M}_{2n}$, где π — аффинна и $\deg(\varphi \oplus \psi) \leqslant 2$. Тогда f и g имеют одинаковое число ближайших к ним бент-функций.

Пусть S_n^k — множество линейных подпространств $\mathbb{F}_2^n$ размерности k. Общее количество ближайших бент-функций к таким f можно подсчитать следующим образом.

Теорема 3. Количество ближайших к $f(x,y) = \langle x, y\rangle \oplus \varphi(y) \in \mathcal{M}_{2n}$ бент-функций равно

$$\sum_{k=0}^{n} \left|\{a \oplus L : a \in \mathbb{F}_2^n, L \in S_n^k \text{ и } \deg\varphi|_{a\oplus L} \leqslant 2\}\right| \cdot 2^{k(k+3)/2}.$$

В случае некоторых φ количество может быть подсчитано в явном виде.

Следствие 2. Количество ближайших к $f(x,y) = \langle x, y\rangle \oplus y_1 y_2 \dots y_m \in \mathcal{M}_{2n}$ бент-функций, где $3 \leqslant m \leqslant n$, равно

$$\mathcal{L}_{2n} - \sum_{k=0}^{n} \sum_{t=\max\{0,k-m\}}^{\min\{n-m,k-3\}} |S_{n-m}^t| \cdot |S_m^{k-t}| \cdot 2^{(k-t+1)(n-m-t)} \cdot 2^{k(k+3)/2}.$$

Заметим:

1) при $m = n$ и $m = n - 1$ формула также справедлива для функций $f(x, y) = \langle x, y\rangle \oplus \varphi(y) \in \mathcal{M}_{2n}$, где функция φ имеет ненулевое значение ровно на одном и двух векторах соответственно;
2) вместо $y_1 \dots y_m$ можно рассматривать характеристическую функцию любого аффинного подпространства $\mathbb{F}_2^n$ размерности $n - m$.

Перейдём к сравнению полученных значений с верхней оценкой $\mathcal{L}_{2n}$.

Следствие 3. Пусть $n \geqslant 3$. Тогда количество ближайших к $f_3(x, y) = \langle x, y\rangle \oplus \oplus\, y_1y_2y_3 \in \mathcal{M}_{2n}$ бент-функций равно

$$\mathcal{L}_{2n} - 2^{4n-3}(2^1 + 1)(2^2 + 1) \dots (2^{n-3} + 1).$$

Для функции $f_n(x, y) = \langle x, y\rangle \oplus y_1y_2 \dots y_n \in \mathcal{M}_{2n}$ аналогичное количество равно

$$(2^2 + 1)(2^3 + 1) \dots (2^n + 1)(2^n - 1) + \frac{32}{3}(2^{2n-1} + 1) - 3 \cdot 2^{n+2} - 3.$$

При $n \to \infty$ это $o(\mathcal{L}_{2n})$ и $\dfrac{1}{3}\mathcal{L}_{2n} + o(\mathcal{L}_{2n})$ соответственно.

Интересно, что f_3 степени 3 имеет меньше ближайших бент-функций (аффинна на меньшем количестве аффинных подпространств $\mathbb{F}_2^{2n}$ размерности n), чем функция f_n степени n при $n \geqslant 4$.

ЛИТЕРАТУРА

1. *Tokareva N.* Bent Functions: Results and Applications to Cryptography. Academic Press, 2015.
2. *Rothaus O.* On “bent” functions // J. Comb. Theory. Ser. A. 1976. V. 20. No. 3. P. 300–305.
3. *McFarland R. L.* A family of difference sets in non-cyclic groups // J. Combinat. Theory. Ser. A. 1973. V. 15. No. 1. P. 1–10.
4. *Коломеец Н. А., Павлов А. В.* Свойства бент-функций, находящихся на минимальном расстоянии друг от друга // Прикладная дискретная математика. 2009. № 4(6). С. 5–20.
5. *Коломеец Н. А.* Перечисление бент-функций на минимальном расстоянии от квадратичной бент-функции // Дискретн. анализ и исслед. опер. 2012. Т. 19. Вып. 1. С. 41–58.
6. *Коломеец Н. А.* Верхняя оценка числа бент-функций на расстоянии 2^k от произвольной бент-функции от $2k$ переменных // Прикладная дискретная математика. 2014. № 3(25). С. 28–39.
7. *Быков Д. А., Коломеец Н. А.* О нижней оценке числа бент-функций на минимальном расстоянии от бент-функции из класса Мэйорана — Макфарланда // Дискретн. анализ и исслед. опер. 2023. Т. 30. Вып. 3. С. 57–80.
8. *Быков Д. А.* О достижимости нижней оценки числа бент-функций на минимальном расстоянии от бент-функции из класса Мэйорана — МакФарланда //Прикладная дискретная математика. Приложение. 2023. № 16. С. 14–18.
9. *Nyberg K.* Differentially uniform mappings for cryptography // LNCS. 1994. V. 765. P. 245–265.
10. *Черемушкин А. В.* Методы аффинной и линейной классификации двоичных функций // Тр. по дискр. матем. 2001. Т. 4. С. 273–314.

УДК 519.7 DOI 10.17223/2226308X/17/7

ИССЛЕДОВАНИЕ БУМЕРАНГОВОЙ РАВНОМЕРНОСТИ КВАДРАТИЧНЫХ ВЗАИМНО ОДНОЗНАЧНЫХ ВЕКТОРНЫХ БУЛЕВЫХ ФУНКЦИЙ

Ю. С. Калинин

Атака методом бумеранга, предложенная в 1999 г., является разновидностью разностной атаки. Её преимущество заключается в том, что даже при невысоком показателе дифференциальной равномерности шифр всё равно может быть уязвим. Данная работа посвящена такому параметру векторной булевой функции, как бумеранговая равномерность, который характеризует стойкость функции к атаке методом бумеранга. В качестве исследуемого класса функций рассматриваются квадратичные подстановки. Изучена зависимость бумеранговой характеристики от дифференциальной для этого класса, основным результатом является выражение, связывающее бумеранговую равномерность функции со значениями её DDT-таблицы и полученное благодаря использованию матричного подхода к работе с квадратичными функциями, а также известных свойств дифференциальной и бумеранговой характеристик. Исследованы некоторые конструкции квадратичных подстановок для малого числа переменных на предмет бумеранговой характеристики и установлены другие их свойства.

Ключевые слова: *векторная булевая функция, квадратичная подстановка, дифференциальная равномерность, DDT-таблица, APN-функция, метод бумеранга, бумеранговая равномерность, BCT-таблица.*

Одним из разностных методов атаки на блочные шифры является метод бумеранга, впервые опубликованный в работе [1]. Его преимущество заключается в том, что даже при наличии невысокой дифференциальной равномерности шифр всё равно может быть уязвим для разностных атак. Ярким примером эффективности атаки методом бумеранга служит шифрсистема COCONUT98, на которую проведена успешная атака [1]. В той же работе рассматриваются такие блочные шифры, как 16-раундовый Khufu, CAST-256 и 6-раундовый FEAL. Позднее метод бумеранга был применён к 6-раундовому блочному шифру KASUMI [2], 5- и 6-раундовым AES [3], а также к хэш-функции SHA-1 [4] и другим шифрсистемам. Недавно предложена атака методом бумеранга на 4-раундовый алгоритм шифрования LILLIPUT-TBC-II-256 [5].

Данная работа посвящена такому параметру векторной булевой функции, как бумеранговая равномерность, которая характеризует стойкость функции к атаке методом бумеранга. Изучена зависимость бумеранговой характеристики от дифференциальной для класса квадратичных подстановок. Выражение, связывающее бумеранговую равномерность функции со значениями её DDT-таблицы, является основным результатом. Он получен благодаря использованию матричного подхода к работе с квадратичными функциями, а также известных свойств дифференциальной и бумеранговой характеристик. Кроме того, исследованы некоторые конструкции квадратичных подстановок для малого числа переменных на предмет бумеранговой характеристики и установлены другие их свойства.

Пусть $n \in \mathbb{N}$; $\mathbb{F}_2$ — поле из двух элементов; $x = (x_1, \ldots, x_n)$ — двоичный вектор с координатами из $\mathbb{F}_2$; $\mathbb{F}_2^n$ — пространство двоичных векторов размерности n; $\oplus$ — сложение по модулю 2.

Векторной булевой функцией (*(n,m)-функцией*) F называется произвольное отображение $F : \mathbb{F}_2^n \to \mathbb{F}_2^m$, $n, m \in \mathbb{N}$. В случае $m = 1$ говорят, что F — булева функция

от n переменных. Можно рассматривать (n, m)-функцию как набор из m координатных булевых функций от n переменных: $F = (f_1, \ldots, f_m)$. Любую (n, m)-функцию можно единственным образом записать в виде *многочлена Жегалкина*, или *алгебраической нормальной формы* (*АНФ*):

$$F(x_1, \ldots, x_n) = \bigoplus_{k=1}^{n} \bigoplus_{i_1, \ldots, i_k} a_{i_1 \ldots i_k} x_{i_1} \ldots x_{i_k} \oplus a_0,$$

где $\{i_1, \ldots, i_k\} \subseteq \{1, \ldots, n\}$ и $a_{i_1 \ldots i_k} \in \mathbb{F}_2^m$.

Алгебраической степенью $\deg F$ *функции* F называется количество переменных в самом длинном слагаемом АНФ, при котором коэффициент не равен нулевому вектору.

Пусть $\mathbb{F}_{2^n}$ — поле из 2^n элементов, $+$ — операция сложения в этом поле. Тогда в случае $n = m$ векторную булеву функцию F, действующую на $\mathbb{F}_2^n$, можно единственным образом представить в виде полинома степени не выше $2^n - 1$ над полем $\mathbb{F}_{2^n}$:

$$F(x) = \sum_{i=0}^{2^n - 1} c_i x^i \in \mathbb{F}_{2^n}[x],$$

где x — элемент $\mathbb{F}_{2^n}$. Справедливо определение алгебраической степени для такого представления векторной булевой функции:

$$\deg F = \max_{i=0,\ldots,2^n-1} \{\mathrm{wt}(i) : c_i \neq 0\},$$

где $\mathrm{wt}(i)$ — двоичный вес числа i. Функция степени не выше 1 называется *аффинной*, т. е. имеет вид $\sum\limits_{i=0}^{n-1} c_i x^{2^i} + c \in \mathbb{F}_{2^n}[x]$. В случае $c = 0$ функция *линейна*. Когда $\deg F = 2$, функция называется *квадратичной*.

В работе [6] вводится понятие дифференциальной равномерности для векторной булевой функции F.

Пусть $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ — векторная булева функция, заданная многочленом над $\mathbb{F}_{2^n}$.

Определение 1. *Дифференциальной характеристикой* называется величина

$$\delta_F(a, b) = |\{x \in \mathbb{F}_{2^n} : F(x) + F(x + a) = b\}|,$$

где a, b — элементы $\mathbb{F}_{2^n}$. *Показателем дифференциальной равномерности* называется

$$\delta_F = \max_{a,b \in \mathbb{F}_{2^n}, a \neq 0} \delta_F(a, b).$$

Таблицей дифференциальной равномерности (*DDT-таблицей*) называется таблица размера $2^n \times 2^n$ со значениями $\delta_F(a, b)$.

Определение 2. Пусть F — подстановка на $\mathbb{F}_{2^n}$. *Бумеранговой характеристикой* называется величина

$$\beta_F(a, b) = \left|\left\{x \in \mathbb{F}_{2^n} : F^{-1}(F(x) + b) + F^{-1}(F(x + a) + b) = a\right\}\right|, \tag{1}$$

где a, b — элементы $\mathbb{F}_{2^n}$. *Бумеранговая равномерность для функции* F есть максимальное значение из $\beta_F(a, b)$, за исключением случаев $a = 0$ или $b = 0$:

$$\beta_F = \max_{a,b \in \mathbb{F}_{2^n}^*} \beta_F(a, b).$$

Таблица размера $2^n \times 2^n$ со значениями $\beta_F(a, b)$ называется *таблицей бумеранговой связности* (*BCT-таблицей*).

Важно заметить, что условие «F — подстановка» не является необходимым в контексте бумеранговой равномерности [7], но в данной работе рассматриваются только подстановки. При $a = 0$ или $b = 0$ уравнению из равенства (1) удовлетворяют все элементы $\mathbb{F}_{2^n}$, поэтому эти случаи исключаются.

Бумеранговая и дифференциальная равномерности соотносятся между собой следующим образом:

$$\delta_F(a,b) \leqslant \beta_F(a,b) \quad \text{для любых} \quad a,b \in \mathbb{F}_{2^n}.$$

С позиции дифференциальной равномерности лучшими являются функции с наименьшим возможным значением $\delta_F = 2$, они называются *APN-функциями* (Almost Perfect Nonlinear). Стоит отметить, что минимальное возможное значение $\beta_F = 2$ достигается в том и только в том случае, когда F — *APN-подстановка* [8]. Есть много работ, посвящённых классу APN-функций, этой темой занимаются как русскоязычные [9–13], так и иностранные исследователи [14–17]. Но ещё больший интерес представляют взаимно однозначные APN-функции (APN-подстановки). Известно, что они существуют для нечётных n. Для чётных n известна лишь APN-подстановка размерности 6, предложенная в [14]. Для $n = 4$ доказано, что их нет. Для $n \geqslant 8$ вопрос существования APN-подстановок открыт и известен как «The Big APN Problem» [14].

Изучение области, связанной с бумеранговой равномерностью, является актуальным, об этом свидетельствует большое число опубликованных работ. В [8, 18] описаны свойства BCT-таблицы, её связь с DDT-таблицей, построены примеры для некоторых S-блоков, параметр «бумеранговая равномерность» рассмотрен относительно разных видов эквивалентности функций и установлен для конкретных классов преобразований. В [19–21] предложены обобщающие подходы к определению бумеранговой равномерности. Работы [8, 20–24] посвящены изучению некоторых мономиальных, биномиальных и других конструкций, класса квадратичных подстановок, подстановок с бумеранговой равномерностью 4, четырёхбитовых и других относительно этого параметра.

Опишем матричный подход для работы с квадратичными функциями, предложенный в [17] для исследования дифференциальной равномерности.

Квадратичную функцию, представленную полиномом над $\mathbb{F}_{2^n}$ без линейной и константной частей, будем называть *однородной квадратичной функцией*. Для $r, s > 0$ обозначим: $\mathbb{F}_{2^n}^{r\times s}$ — пространство матриц размера $r \times s$ над полем $\mathbb{F}_{2^n}$; $A[i,j]$ — элемент (i,j) матрицы A. Полагаем $\overline{\alpha} = \{\alpha_1, \ldots, \alpha_n\}$ — базис $\mathbb{F}_{2^n}$ над $\mathbb{F}_2$. Пусть $M_\alpha \in \mathbb{F}_{2^n}^{n\times n}$ — такая матрица, что $M_\alpha[i,j] = \alpha_j^{2^{i-1}}$ для $1 \leqslant i,j \leqslant n$.

Пусть $\eta_1, \ldots, \eta_m$ — различные элементы из $\mathbb{F}_{2^n}$, где $m, n \in \mathbb{N}$, $B = \{\eta_1, \ldots, \eta_m\} \in \mathbb{F}_{2^n}^m$. Положим $\mathrm{Span}(B) = \mathrm{Span}(\eta_1, \ldots, \eta_m)$ — подпространство над $\mathbb{F}_2$, порождённое элементами $\eta_1, \ldots, \eta_m$; $\mathrm{Rank}_{\mathbb{F}_2}(B) = \mathrm{Rank}_{\mathbb{F}_2}\{\eta_1, \ldots, \eta_m\}$ — размерность подпространства $\mathrm{Span}(B)$ над $\mathbb{F}_2$, которое будем называть рангом B. Раскладывая по базису $\overline{\alpha}$ элемент $\eta_i = \sum\limits_{j=1}^{n} \lambda_{i,j}\alpha_j$ для $i \in \{1, \ldots, m\}$, где $\lambda_{i,j} \in \mathbb{F}_2$ для всех i, j, получим, что $\mathrm{Rank}_{\mathbb{F}_2}\{\eta_1, \ldots, \eta_m\}$ равен рангу матрицы $\Lambda_{m\times n} = (\lambda_{i,j})_{m\times n}$.

Пусть $F(x) = \sum\limits_{1\leqslant j<i\leqslant n} c_{ij}x^{2^{i-1}+2^{j-1}} \in \mathbb{F}_{2^n}[x]$ — однородная квадратичная функция и C_F — матрица $n \times n$, такая, что $C_F[j,i] = C_F[i,j] = c_{ij}$ для $1 \leqslant j < i \leqslant n$ и $C_F[i,i] = 0$ для $i = 1, \ldots, n$. Для F положим $H = M^{\mathrm{T}}C_F M$, где $M = M_\alpha$ и $\{\alpha_1, \ldots, \alpha_n\}$ — базис $\mathbb{F}_{2^n}$ над $\mathbb{F}_2$. Тогда H — симметричная матрица с нулевой главной диагональю.

Определение 3. Пусть H — матрица размера $n \times n$ над $\mathbb{F}_{2^n}$. Тогда матрица H называется QAM (quadratic APN matrix), если:

1) H симметричная и её главная диагональ нулевая;
2) множество элементов любой ненулевой линейной комбинации n строк (столбцов) матрицы H имеет ранг $n-1$.

Согласно [17, теорема 1], для фиксированного $n \in \mathbb{N}$ дифференциальная равномерность δ_F равна 2^k тогда и только тогда, когда существует ненулевая линейная комбинация n строк (столбцов) H ранга $n-k$, а все остальные ненулевые линейные комбинации имеют ранг не меньше $n-k$.

Для $a, b \in \mathbb{F}_{2^n}$ и F — векторной булевой функции определим множества

$$U_{a,b}(F) = \{x \in \mathbb{F}_{2^n} : F(x) + F(x+a) = b\}, \quad U^*_{a,b}(F) = U_{a,b}(F) \setminus \{0, a\}.$$

Следующая теорема показывает, как бумеранговая равномерность произвольной квадратичной подстановки зависит от значений дифференциальной характеристики.

Теорема 1. Пусть $G(x)$ — квадратичная подстановка и $G = F + A$, где $F(x) = \sum\limits_{1 \leqslant t < i \leqslant n} c_{i,t} x^{2^{i-1}+2^{t-1}} \in \mathbb{F}_{2^n}[x]$; A — аффинная функция; матрицы C_F и M определены ранее и $H = M^{\mathrm{T}} C_F M$. Тогда

$$\beta_G = \beta_{F+A} = \max_{a,b \in \mathbb{F}^*_{2^n}} \left[2^k + \sum_{z \in U^*_{a,F(a)}(F)} \delta_{F+A}(z, b) \right] \tag{2}$$

в том и только в том случае, когда каждая ненулевая линейная комбинация n строк (столбцов) H имеет ранг не меньше чем $n-k$, и хотя бы для одной это значение достигается. В частности, G является квадратичной APN-подстановкой тогда и только тогда, когда H — QAM.

Из теоремы следует выражение бумеранговой равномерности для квадратичной подстановки через значения её DDT-таблицы. В случае, когда квадратичная подстановка является однородной, т. е. аффинная часть A нулевая, в условиях теоремы справедлива следующая формула:

$$\beta_F = \max_{a,b \in \mathbb{F}^*_{2^n}} \left[2^k + \sum_{z \in U^*_{a,F(a)}(F)} \delta_F(z, b) \right]. \tag{3}$$

Значение β_F в формулах (2) и (3) можно ограничить снизу и сверху в зависимости от ранга матрицы H, соответствующей квадратичной подстановке F.

Следствие 1. Пусть выполнены условия теоремы 1, тогда справедлива оценка

$$2^k \leqslant \beta_F \leqslant 2^{2k} - 2^k,$$

при условии, что $2^k - 1 \leqslant 2^{n-k}$.

Что касается достижимости оценок, в табл. 1 приведены данные для размерностей $n = 3, 4, 5, 6$ и $k = 1, 2, 3$. Нижняя граница обозначается $\beta_{\min}$, верхняя — $\beta_{\max}$, $S_{\min}$ и $S_{\max}$ — наличие подстановок с соответствующей бумеранговой равномерностью; «?» означает, что о существовании таковых пока не известно.

Исследованы некоторые конструкции квадратичных подстановок. Экспериментально установлен следующий факт: для $n = 3, 4, 5$ не существует подстановок вида $\alpha x^k + \beta x^t$, где $\mathrm{wt}(k) = \mathrm{wt}(t) = 2$ и $\alpha, \beta \in \mathbb{F}^*_{2^n}$, т. е. биномиальных однородных квадратичных, что согласуется с результатами, полученными в [26] для $n = 3, 5$. Но для $n = 4$ верно более общее

Таблица 1

n	k	$\beta_{\min}$	$S_{\min}$	$\beta_{\max}$	$S_{\max}$
3	1	2	+	2	+
4	1	2	—	2	—
4	2	4	— [8]	12	—
5	1	2	+	2	+
5	2	4	— [25]	12	+
6	1	2	+ [14]	2	+[14]
6	2	4	+	12	+
6	3	8	—	56	?

Утверждение 1. При $n = 4$ не существует однородных квадратичных подстановок, т. е. подстановок F вида, указанного в теореме 1.

Так как мономиальные и биномиальные конструкции уже немало исследовались на предмет бумеранговой равномерности [7, 21, 23], предпочтение было отдано изучению триномиальных подстановок. Для малых значений n получены следующие результаты:

1) Для $n = 3$ множество триномиальных однородных квадратичных подстановок с точностью до аффинной эквивалентности исчерпывается функциями вида

$$x^6 + \gamma x^5 + \alpha\gamma^3 x^3, \quad x^6 + \gamma x^5 + \alpha^2\gamma^3 x^3, \quad x^6 + \gamma x^5 + (\alpha + \alpha^2)\gamma^3 x^3,$$

где $\gamma \in \mathbb{F}_{2^n}^*$ — произвольный элемент; α — примитивный элемент $\mathbb{F}_{2^n}^*$. Эти подстановки являются APN- и AB-отображениями, их характеристики приведены в табл. 2 и здесь и далее определены, согласно [27]; Nl_F — нелинейность функции F.

Таблица 2

$\deg F$	$\deg F^{-1}$	δ_F	β_F	Nl_F	Количество
2	2	2	2	2	21

2) Для $n = 5$ все триномиальные однородные квадратичные подстановки, являющиеся APN- и AB-отображениями, с точностью до аффинной эквивалентности имеют вид

$$x^{2^{k_1}t} + \gamma x^{2^{k_2}t} + \beta x^{2^{k_3}t},$$

где $t \in \{3, 5\}$; $0 \leqslant k_1 < k_2 < k_3 \leqslant 4$; γ, β — произвольные элементы $\mathbb{F}_{2^n}^*$. Мощность множества функций такого вида равна 19220, а количество исследуемых подстановок — 6820; их свойства приведены в табл. 3.

Таблица 3

$\deg F$	$\deg F^{-1}$	δ_F	β_F	Nl_F	Количество
2	3	2	2	12	6820

Утверждение 2. Пусть $n = 5$. Тогда функции вида $x^t + \beta x^{2t} + \beta^2 x^{3t}$, где $t = 2^k + 2^{k-1}$, $k \in \{1, \ldots, 5\}$, $\beta \in \mathbb{F}_{2^n}^*$ — произвольный элемент, являются триномиальными однородными квадратичными подстановками с точностью до аффинной эквивалентности. Количество подстановок равно 4805, их характеристики представлены в табл. 4.

Таблица 4

$\deg F$	$\deg F^{-1}$	δ_F	β_F	Nl_F	Количество
2	3	8	16	8	4805

В дальнейшем можно изучить, как распределена β_F для квадратичной подстановки F: какие значения она принимает чаще, какие реже, какие не принимает. Исследовать функции, для которых верно, что если F — подстановка, A — аффинная, то $F+A$ тоже подстановка. Важным вопросом является следующий: можно ли выделить класс подстановок, возможно, квадратичных, сохраняющих бумеранговую равномерность при различных эквивалентных преобразованиях функций?

ЛИТЕРАТУРА

1. *Wagner D.* The boomerang attack // LNCS. 1999. V. 1636. P. 156–170.
2. *Biham E., Dunkelman O., and Keller N.* A related-key rectangle attack on the full KASUMI // LNCS. 2005. V. 3788. P. 443–461.
3. *Biryukov A.* The boomerang attack on 5 and 6-round reduced AES // LNSC. 2004. V. 3373. P. 11–15.
4. *Joux A. and Peyrin T.* Hash functions and the (amplified) boomerang attack // LNCS. 2007. V. 4622. P. 244–263.
5. *Пудовкина М. А., Смирнов А. М.* Анализ методом бумеранга 4-раундового алгоритма шифрования LILLIPUT-TBC-II-256 // Прикладная дискретная математика. Приложение. 2023. № 16. С. 81–84.
6. *Nyberg K.* Diferentially uniform mappings for cryptography // LNCS. 1994. V. 765. P. 55–64.
7. *Li K., Qu L., Sun B., and Li C.* New results about the boomerang uniformity of permutation polynomials // IEEE Trans. Inform. Theory. 2019. V. 65. P. 7542–7553.
8. *Boura C. and Canteaut A.* On the boomerang uniformity of cryptographic S-boxes // IACR Trans. Symmetric Cryptology. 2018. No. 3. P. 290–310.
9. *Глухов М. М.* О приближении дискретных функций линейными функциями // Матем. вопр. криптогр. 2016. № 7. С. 29–50.
10. *Городилова А. А.* Характеризация почти совершенно нелинейных функций через подфункции // Дискретная математика. 2015. Т. 27. № 3. С. 3–16.
11. *Gorodilova A. A.* A note on the properies of associated Boolean functions of quadratic APN functions // Прикладная дискретная математика. 2020. № 47. С. 16–21.
12. *Идрисова В. А.* О построении APN-перестановок с помощью подфункций // Прикладная дискретная математика. 2018. № 41. С. 17–27.
13. *Тужилин М. Э.* Почти совершенные нелинейные функции // Прикладная дискретная математика. 2009. № 3 (5). С. 14–20.
14. *Browning K., Dillon J., McQuistan M., and Wolfe A.* An APN permutation in dimension six // Finite Fields: Theory and Appl. 2010. V. 518. P. 33–42.
15. *Budaghyan L., Calderini M., Carlet C., et al.* On two fundamental problems on APN power functions // IEEE Trans. Inform. Theory. 2022. V. 68. P. 3389–3403.
16. *Budaghyan L., Carlet C., Helleseth T., and Kaleyski N.* On the distance between APN functions // IEEE Trans. Inform. Theory. 2020. V. 66. P. 5742–5753.
17. *Yu Y., Wang M., and Li Y.* A matrix approach for constructing quadratic APN functions // Des. Codes Cryptogr. 2014. V. 73. P. 587–600.
18. *Cid C., Huang T., Peyrin T., et al.* Boomerang connectivity table: a new cryptanalysis tool // LNCS. 2018. V. 10821. P. 683–714.

19. *Mesnager S., Mandal B., and Msahli M.* Survey on recent trends towards generalized differential and boomerang uniformities // Cryptogr. Commun. 2022. V. 14. P. 691–735.
20. *Garg K., Hasan S., and Stănică P.* Boomerang uniformity of some classes of functions over finite fields // Discret. Appl. Math. 2024. V. 343. P. 166–179.
21. *Stănică P.* Using double Weil sums in finding the c—boomerang connectivity table for monomial functions on finite fields // Appl. Algebra Eng. Commun. Comput. 2023. V. 34. P. 581–602.
22. *Kim K., Mesnager S., Choe J., and Lee D.* On permutation quadrinomials with boomerang unifomity 4 and the best-known nonlinearity // Des. Codes Cryptogr. 2022. V. 90. P. 1437–1461.
23. *Mesnager S., Tang C., and Xiong M.* On the boomerang uniformity of quadratic permutations // Des. Codes Cryptogr. 2020. V. 88. P. 2233–2246.
24. *Tu Z., Li N., Zeng X., and Zhou J.* A class of quadrinomial permutations with boomerang uniformity four // IEEE Trans. Inform. Theory. 2020. V. 66. P. 3753–3765.
25. *Božilov D., Bilgin B., and Sahin H. A.* A note on 5-bit quadratic permutations classification // IACR Trans. Symmetric Cryptology. 2017. No. 1. P. 398–404.
26. *Милосердов А. В.* Взаимно однозначные биномиальные функции над конечными полями // Дискретн. анализ исслед. опер. 2018. № 4. С. 59–80.
27. *Carlet C.* Boolean Functions for Cryptography and Coding Theory. Cambridge: Cambridge University Press, 2020.

УДК 519.7 DOI 10.17223/2226308X/17/8

О ЧИСЛЕ ФУНКЦИЙ, РАЗРУШАЮЩИХ СТРУКТУРУ ПОДПРОСТРАНСТВ РАЗМЕРНОСТИ 3 И ВЫШЕ[1]

Н. А. Коломеец

Рассматриваются оценки мощности множеств $\mathcal{P}_n^k$ обратимых функций $F : \mathbb{F}_2^n \to \mathbb{F}_2^n$, для которых любое $U \subseteq \mathbb{F}_2^n$ и его образ $F(U)$ не могут одновременно являться аффинными подпространствами $\mathbb{F}_2^n$ размерности k, где $3 \leqslant k \leqslant n-1$. Приведены нижние оценки мощности $\mathcal{P}_n^k$ и $\mathcal{P}_n^k \cap \ldots \cap \mathcal{P}_n^{n-1}$, усиливающие результаты 2007 г. (W. E. Clark и др.) о непустоте данных множеств. Доказано, что почти все подстановки на $\mathbb{F}_2^n$ принадлежат $\mathcal{P}_n^4 \cap \ldots \cap \mathcal{P}_n^{n-1}$. Для мощностей множеств $\mathcal{P}_n^3$ и $\mathcal{P}_n^3 \cap \ldots \cap \mathcal{P}_n^{n-1}$ получены асимптотические оценки сверху и снизу с точностью до $o(2^n!)$. Оценено снизу число функций из $\mathcal{P}_n^4 \cap \ldots \cap \mathcal{P}_n^{n-1}$, которые отображают ровно одно аффинное подпространство $\mathbb{F}_2^n$ размерности 3 в аффинное подпространство.

Ключевые слова: *аффинные подпространства, инвариантные подпространства, подстановки, асимптотические оценки.*

Пусть $\mathcal{P}_n$ — множество обратимых функций вида $\mathbb{F}_2^n \to \mathbb{F}_2^n$. Будем называть *подпространством* аффинное подпространство $L \subseteq \mathbb{F}_2^n$, т. е. $L = a \oplus L' = \{a \oplus x : x \in L'\}$, где L' — линейное подпространство $\mathbb{F}_2^n$ и $a \in \mathbb{F}_2^n$, его размерность $\dim L$ равна $\dim L'$. Векторная булева функция $\pi \in \mathcal{P}_n$ *сохраняет структуру* L, если $\pi(L) = \{\pi(x) : x \in L\}$ — подпространство $\mathbb{F}_2^n$. Аналогично, π *разрушает структуру* L, если $\pi(L)$ не является подпространством $\mathbb{F}_2^n$. Впервые данные свойства подстановок были рассмотрены в работе [1]. Определим

$$\mathcal{L}_k(\pi) = \{L \subseteq \mathbb{F}_2^n : L \text{ и } \pi(L) \text{ — подпространства } \mathbb{F}_2^n \text{ размерности } k\},$$

[1]Работа выполнена в рамках госзадания ИМ СО РАН (проект № FWNF–2022–0019).

а также множества функций, разрушающих структуру подпространств определённых размерностей:

$$\mathcal{P}_n^k = \{\pi \in \mathcal{P}_n : \mathcal{L}_k(\pi) = \varnothing\}, \quad \mathcal{P}_n^{\geqslant k} = \mathcal{P}_n^k \cap \mathcal{P}_n^{k+1} \cap \ldots \cap \mathcal{P}_n^{n-1}.$$

Обратим внимание, что любое подмножество $\mathbb{F}_2^n$ мощности 1, 2 или 2^n является подпространством $\mathbb{F}_2^n$, поэтому $\mathcal{P}_n^0$, $\mathcal{P}_n^1$ и $\mathcal{P}_n^n$ всегда пустые. Важное значение имеет $\mathcal{P}_n^2$, где $n > 2$: это множество всех APN-подстановок [2], с которым связан ряд открытых вопросов [3]. Некоторые свойства $|\mathcal{L}_k(\pi)|$ при произвольном k исследовались в [4, 5].

Сохранение структуры подпространства $L \subseteq \mathbb{F}_2^n$ функцией π можно интерпретировать как наличие у π обратимой «подфункции» $\pi|_L : L \to \pi(L)$ и использовать её так же, как и $f|_L$ для булевой функции $f : \mathbb{F}_2^n \to \mathbb{F}_2$: зафиксировать некоторые базисы L и $\pi(L)$ и рассматривать $\pi|_L$ как функцию вида $\mathbb{F}_2^{\dim L} \to \mathbb{F}_2^{\dim L}$. С точки зрения криптографических свойств, инвариантных относительно применения обратимых аффинных преобразований, $\pi|_L$ является полноценной подфункцией π. К таким свойствам, например, относятся нелинейность и порядок дифференциальной равномерности. Сохранение структуры подпространства связано и с инвариантными подпространствами отображений. Наличие инвариантного подпространства у раундовой функции SP-сети (учитывая прибавление раундового ключа) может быть использовано в атаке [6]. Необходимым условием наличия такого подпространства является сохранение структуры определённых подпространств её S-блоками. В [7] предложено обобщение данной атаки (см. также исследования, направленные на построение необходимых множеств, начиная с S-блоков [8, 9]). В данном контексте интересны S-блоки, разрушающие структуру как можно большего числа подпространств. Докажем асимптотические оценки для мощностей множеств $\mathcal{P}_n^3$, $\mathcal{P}_n^{\geqslant 3}$ и $\mathcal{P}_n^{\geqslant 4}$.

Пусть $3 \leqslant k \leqslant n-1$. Введём обозначения

$$\rho_{n,k} = \frac{2^{2n-2k}\binom{n}{k}_2^2}{\binom{2^n}{2^k}}, \quad \sigma_{n,k} = \sum_{i=k}^{n-1} \rho_{n,i},$$

где $\binom{2^n}{2^k}$ и $\binom{n}{k}_2$ — биномиальные и 2-биномиальные (гауссовы) коэффициенты соответственно. Например,

$$\rho_{n,3} = \rho\frac{2^n(2^n-1)(2^n-2)(2^n-4)}{(2^n-3)(2^n-5)(2^n-6)(2^n-7)}, \text{ где } \rho = \frac{5}{224}.$$

Последовательности $\rho_{n,k}$ и $\sigma_{n,k}$ обладают следующим свойством:

Утверждение 1. Зафиксируем $k \geqslant 3$. Тогда последовательности $\rho_{n,k}$ и $\sigma_{n,k}$, $n = k+1, k+2, k+3, \ldots$, монотонно убывают, при этом

$$\lim_{n\to\infty} \rho_{n,k} = \lim_{n\to\infty} \sigma_{n,k} = \begin{cases} \rho, & \text{если } k = 3, \\ 0, & \text{если } k \geqslant 4. \end{cases}$$

В табл. 1 приведены округлённые значения $\rho_{n,3}$, $\sigma_{n,3}$ и $\sigma_{n,4}$ при $4 \leqslant n \leqslant 12$. Заметим, что $\rho \approx 0{,}0223214285714286$.

Перейдём к оценкам мощностей множеств $\mathcal{P}_n^k$ и $\mathcal{P}_n^{\geqslant k}$. В [1] доказано, что $\mathcal{P}_n^{\geqslant 3}$ непусто. Более того, из доказательства [1, теорема 2.1] можно заключить, что справедливы следующие оценки.

Таблица 1

Округлённые значения $\rho_{n,3}$, $\sigma_{n,3}$ и $\sigma_{n,4}$ для $4 \leqslant n \leqslant 12$

n	$\rho_{n,3}$	$\sigma_{n,3}$	$\sigma_{n,4}$
4	0,0699300699300699	0,0699300699300699	—
5	0,0365458296492779	0,0365522248005155	$6{,}395151237590699 \cdot 10^{-6}$
6	0,0281384877529501	0,0281385016330859	$1{,}3880135807123695 \cdot 10^{-8}$
7	0,0249785705552490	0,0249785706508960	$9{,}5647023517238220 \cdot 10^{-11}$
8	0,0235940660426061	0,0235940660436301	$1{,}0240104891952223 \cdot 10^{-12}$
9	0,0229445264556499	0,0229445264556632	$1{,}3335844188797633 \cdot 10^{-14}$
10	0,0226297620233199	0,0226297620233201	$1{,}9054283870459533 \cdot 10^{-16}$
11	0,0224748023114524	0,0224748023114524	$2{,}8481291963864860 \cdot 10^{-18}$
12	0,0223979185358598	0,0223979185358598	$4{,}3530671380777510 \cdot 10^{-20}$

Теорема 1. Пусть $3 \leqslant k \leqslant n-1$. Тогда

$$|\mathcal{P}_n^k| \geqslant (1-\rho_{n,k})|\mathcal{P}_n|, \quad |\mathcal{P}_n^{\geqslant k}| \geqslant (1-\sigma_{n,k})|\mathcal{P}_n|.$$

Заметим, что числа $\rho_{n,k}$ и $\sigma_{n,k}$ имеют и более важное значение: это среднее количество аффинных подпространств $\mathbb{F}_2^n$ размерности k (размерности от k до $n-1$), сохраняемых функцией из $\mathcal{P}_n$.

Утверждение 2. Среднее количество аффинных подпространств $\mathbb{F}_2^n$ размерности k, структуру которых сохраняет подстановка на $\mathbb{F}_2^n$, равно $\rho_{n,k}$, т. е.

$$\rho_{n,k} = \frac{1}{|\mathcal{P}_n|} \sum_{\pi \in \mathcal{P}_n} |\mathcal{L}_k(\pi)| \quad \text{и} \quad \sigma_{n,k} = \frac{1}{|\mathcal{P}_n|} \sum_{\pi \in \mathcal{P}_n} \sum_{i=k}^{n-1} |\mathcal{L}_i(\pi)|.$$

Напомним, что $|\mathcal{P}_n| = 2^n!$, и оценим асимптотику $|\mathcal{P}_n^k|$ и $|\mathcal{P}_n^{\geqslant k}|$.

Следствие 1. Почти все $\pi \in \mathcal{P}_n$ разрушают структуру всех подпространств $\mathbb{F}_2^n$ размерности от 4 до $n-1$, т. е. $|\mathcal{P}_n^{\geqslant 4}| = 2^n! - o(2^n!)$ и $|\mathcal{P}_n \setminus \mathcal{P}_n^{\geqslant 4}| = o(2^n!)$.

Теорема 2. Справедливо

$$-o(1) \leqslant \frac{|\mathcal{P}_n^{\geqslant 3}|}{2^n!} - (1-\rho) \leqslant \frac{\rho^2}{2} + o(1).$$

Данные неравенства верны и для $|\mathcal{P}_n^3|$.

Можно оценить и количество функций, сохраняющих структуру ровно одного подпространства размерности 3.

Следствие 2. Количество $\pi \in \mathcal{P}_n^{\geqslant 4}$ с $|\mathcal{L}_3(\pi)| = 1$ не менее чем $\rho(1-\rho)2^n! + o(2^n!)$.

Таким образом, с высокой вероятностью случайно выбранная функция из $\mathcal{P}_n$ разрушает структуру всех подпространств размерности от 3 до $n-1$. Её можно оценить с помощью теоремы 1 и значений $\sigma_{n,3}$ из табл. 1. Например, она превышает 93, 96 и 97 % при $n = 4$, 5 и $n \geqslant 6$ соответственно. В то же время используемые в шифрах S-блоки обычно нельзя отнести к случайным подстановкам из-за накладываемых на них криптографических свойств. Значения $|\mathcal{L}_k(S)|$ для известных S-блоков из $\mathcal{P}_8$ приведены в табл. 2. Заметим, что среднее значение $|\mathcal{L}_2(\pi)|$ для $\pi \in \mathcal{P}_8$ равно примерно 2731.

Таблица 2

Значения $|\mathcal{L}_k(S)|$ для S-блоков из $\mathcal{P}_8$

S-блок	$\lvert\mathcal{L}_2(S)\rvert$	$\lvert\mathcal{L}_3(S)\rvert$	$\lvert\mathcal{L}_4(S)\rvert$	$\lvert\mathcal{L}_5(S)\rvert$	$\lvert\mathcal{L}_6(S)\rvert$	$\lvert\mathcal{L}_7(S)\rvert$
AES/ARIA/Camellia/SM4/	85	0	17	0	0	0
CLEFIA S_1/SNOW 3G S_1/ZUC S_1	85	0	17	0	0	0
Fantomas	6444	79	0	0	0	0
FLY	5968	576	16	0	0	0
Fox (8×8)	4854	225	3	0	0	0
Kuznechik	1953	0	2	0	0	0
Scream	3104	228	6	0	0	0
iScream	5472	466	2	5	0	0
SKINNY $\mathcal{S}_8$	22688	3648	320	24	0	0
SNOW 3G S_2	2570	2	1	0	0	0
ZUC S_0	3360	100	0	0	0	0
Zorro	2691	4	0	0	0	0
Anubis	2590	0	0	0	0	0
BelT	1666	0	0	0	0	0
Enocoro	2767	0	0	0	0	0
Iceberg	2669	0	0	0	0	0
Khazad	2768	0	0	0	0	0
Skipjack	2469	0	0	0	0	0
Turing	2617	0	0	0	0	0
Whirlpool	2579	0	0	0	0	0

ЛИТЕРАТУРА

1. *Clark W. E., Hou X., Mihailovs A.* The affinity of a permutation of a finite vector space // Finite Fields Their Appl. 2007. V. 13. P. 80–112.
2. *Nyberg K.* Differentially uniform mappings for cryptography // LNCS. 1994. V. 765. P. 245–265.
3. *Carlet C.* Open questions on nonlinearity and on APN functions // LNCS. 2015. V. 9061. P. 83–107.
4. *Kolomeec N. and Bykov D.* On the image of an affine subspace under the inverse function within a finite field // Des. Codes Cryptogr. 2024. V. 92. P. 467–476.
5. *Коломеец Н. А.* О сохранении структуры подпространств векторными булевыми функциями // Прикладная дискретная математика. Приложение. 2023. № 16. С. 23–26.
6. *Leander G., Abdelraheem M. A., AlKhzaimi H., and Zenner E.* A cryptanalysis of PRINTcipher: The invariant subspace attack // LNCS. 2011. V. 6841. P. 206–221.
7. *Todo Y., Leander G., and Sasaki Y.* Nonlinear invariant attack: practical attack on full SCREAM, iSCREAM, and Midori64 // LNCS. 2016. V. 10032. P. 3–33.
8. *Трифонов Д. И., Фомин Д. Б.* Об инвариантных подпространствах в XSL-шифрах // Прикладная дискретная математика. 2021. № 54. С. 58–76.
9. *Буров Д. А.* О существовании нелинейных инвариантов специального вида для раундовых преобразований XSL-алгоритмов // Дискретная математика. 2021. Т. 33. № 2. С. 31–45.

УДК 519.7 DOI 10.17223/2226308X/17/9

ХАРАКТЕРИЗАЦИЯ ОБОБЩЁННЫХ БЕНТ-ФУНКЦИЙ АЛГЕБРАИЧЕСКОЙ СТЕПЕНИ 1

А. В. Куценко

Бент-функции вида $\mathbb{F}_2^n \to \mathbb{Z}_q$, где $q \geqslant 2$ — натуральное число, называются обобщёнными бент-функциями. Обобщённые бент-функции, для которых можно опре-

делить дуальную бент-функцию, называются регулярными. Исследуются обобщённые бент-функции, алгебраическая степень которых равна 1. Получены необходимые и достаточные условия того, что обобщённая булева функция алгебраической степени 1 является бент-функцией. Исследованы условия, при которых функция будет регулярной, а также слабо регулярной. Для случая $q = 2^k$ получено описание компонентных булевых функций обобщённой бент-функции алгебраической степени 1, из которого следует, что две из них, имеющие наибольший индекс, являются квадратичными, а остальные — постоянными.

Ключевые слова: *обобщённая бент-функция, регулярная бент-функция, аффинная функция, компонентная булева функция.*

Через $\mathbb{F}_2^n$ обозначим линейное пространство всех двоичных векторов длины n над полем $\mathbb{F}_2$. Для каждой пары $x, y \in \mathbb{F}_2^n$ через $\langle x, y\rangle$ обозначается значение $\bigoplus\limits_{i=1}^{n} x_i y_i$. Пусть q — натуральное число; *обобщённой булевой функцией* от n переменных называется отображение вида $\mathbb{F}_2^n \to \mathbb{Z}_q$, где $q \geqslant 3$. При $q = 2$ функция называется *булевой*. Множество всех обобщённых булевых функций от n переменных обозначим $\mathcal{GF}_n^q$. Каждая обобщённая булева функция $f \in \mathcal{GF}_n^q$ единственным образом представима в виде многочлена степени не выше n над кольцом $\mathbb{Z}_q$ — многочлена Жегалкина (алгебраической нормальной формы, АНФ):

$$f(x_1, x_2, \ldots, x_n) = \sum_{k=1}^{n} \sum_{1 \leqslant i_1 < i_2 < \ldots < i_k \leqslant n} a_{i_1 i_2 \ldots i_k} x_{i_1} x_{i_2} \ldots x_{i_k} + a_0,$$

где $a_0, a_{i_1 i_2 \ldots i_k} \in \mathbb{Z}_q$ для всех $(i_1 i_2 \ldots i_k)$. *Алгебраической степенью функции* $f \in \mathcal{GF}_n^q$ называется максимальная из степеней одночленов, входящих в её многочлен Жегалкина с ненулевыми коэффициентами.

Преобразованием Уолша — Адамара функции $f \in \mathcal{GF}_n^q$ называется функция $H_f : \mathbb{F}_2^n \to \mathbb{C}$, заданная равенством

$$H_f(y) = \sum_{x \in \mathbb{F}_2^n} \omega^{f(x)} (-1)^{\langle x, y\rangle}, \quad y \in \mathbb{F}_2^n,$$

где $\omega = e^{2\pi i/q}$. Функция $f \in \mathcal{GF}_n^q$ называется *обобщённой бент-функцией*, если $|H_f(y)| = 2^{n/2}$ для каждого $y \in \mathbb{F}_2^n$ [1]. Множество обобщённых бент-функций обозначается через $\mathcal{GB}_n^q$. Пусть $f \in \mathcal{GB}_n^q$, тогда если существует функция $\widetilde{f} \in \mathcal{GF}_n^q$, такая, что $H_f(y) = \omega^{\widetilde{f}(y)} 2^{n/2}$, то бент-функция f называется *регулярной*, а функция $\widetilde{f}$ — дуальной к f. Дуальная функция также является регулярной обобщённой бент-функцией. Если существует функция $\widetilde{f} \in \mathcal{GF}_n^q$, такая, что $H_f(y) = \zeta \omega^{\widetilde{f}(y)} 2^{n/2}$, где $\zeta \in \mathbb{C}$ и $|\zeta| = 1$, то бент-функция f называется *слабо регулярной*. Регулярная бент-функция f, для которой справедливо $f = \widetilde{f}$, называется *самодуальной* обобщённой бент-функцией. Если $f(x) = \widetilde{f}(x) + q/2$ для любого $x \in \mathbb{F}_2^n$, то f называется *антисамодуальной* обобщённой бент-функцией.

Известны несколько подходов к обобщению бент-функций. Функции, отвечающие данному выше определению, исследовались во многих работах (см., например, [2–4]). Обзор различных обобщений бент-функций, а также связанных с ними свойств можно найти в [5, 6].

В настоящей работе исследуются структурные свойства обобщённых бент-функций алгебраической степени 1, то есть функций вида

$$f(x_1, x_2, \ldots, x_n) = \sum_{j=1}^{n} \lambda_j x_j + \lambda_0, \quad x \in \mathbb{F}_2^n, \quad \lambda_0, \lambda_1, \ldots, \lambda_n \in \mathbb{Z}_q.$$

Как известно, булева бент-функция (как следствие — и самодуальная булева бент-функция) не может быть аффинной, то есть её алгебраическая степень не может быть меньше 2. В работе [3] исследован вопрос существования обобщённых бент-функций степени 1 и доказано, что для случая, когда q кратно 4, такие функции всегда существуют. В [7] показано, что если для некоторого натурального n и чётного $q \geqslant 2$ обобщённая бент-функция от n переменных существует, то она не может быть самодуальной. Следующий результат характеризует возможные значения коэффициентов многочлена Жегалкина обобщённых бент-функций степени 1:

Теорема 1. Функция $f \in \mathcal{GF}_n^q$ степени 1 является обобщённой бент-функцией, если и только если $q \equiv 0 \pmod 4$ и $\lambda_j \in \{q/4, 3q/4\}$ для всех $j = 1, 2, \ldots, n$.

Таким образом, условие $q \equiv 0 \pmod 4$ является необходимым для существования рассматриваемых функций, поэтому далее будем полагать, что параметр q удовлетворяет данному условию.

Следующая теорема характеризует условия, при которых функция будет регулярной (слабо регулярной), и даёт описание дуальной к ней функции:

Теорема 2. Функция $f \in \mathcal{GB}_n^q$ степени 1 является регулярной тогда и только тогда, когда выполнено по крайней мере одно из условий:

1) n — чётное число;
2) $q \equiv 0 \pmod 8$.

Её дуальная функция в этом случае имеет вид

$$\widetilde{f}(x) = \sum_{j=1}^{n} (q - \lambda_j)\, x_j + \left(\lambda_0 + \frac{3q}{4} n + \frac{3}{2} \sum_{k=1}^{n} \lambda_k \right).$$

Если n — нечётное число, а $q \equiv 4 \pmod 8$, то функция является слабо регулярной и

$$H_f(y) = \zeta \omega^{\sum\limits_{j=1}^{n} (q-\lambda_j) y_j + (\lambda_0 + 3qn/4)} 2^{n/2},$$

где $\zeta = \exp\left(\dfrac{3\pi i}{q} \sum\limits_{k=1}^{n} \lambda_k \right)$.

Положим $2^{k-1} < q \leqslant 2^k$. Известно [2], что с каждой функцией $f \in \mathcal{GF}_n^q$ можно единственным образом ассоциировать набор из k *компонентных* булевых функций $a_0(x), a_1(x), \ldots, a_{k-1}(x)$ от n переменных таких, что

$$f(x) = a_0(x) + 2a_1(x) + \ldots + 2^{k-1} a_{k-1}(x), \quad x \in \mathbb{F}_2^n.$$

Утверждение 1. Для каждой функции $f \in \mathcal{GB}_n^q$ степени 1 справедливо:

$$f(x) = \lambda_0 + \frac{q}{4} \bigoplus_{j=1}^{n} x_j + \frac{q}{2} \left(\bigoplus_{h=1}^{n} b_h x_h \oplus \bigoplus_{1 \leqslant r < s \leqslant n} x_r x_s \right), \quad x \in \mathbb{F}_2^n,$$

$$\widetilde{f}(x) = \widetilde{\lambda}_0 + \frac{q}{4} \bigoplus_{j=1}^{n} x_j + \frac{q}{2} \left(\bigoplus_{l=1}^{n} x_l \oplus \bigoplus_{h=1}^{n} b_h x_h \oplus \bigoplus_{1 \leqslant r < s \leqslant n} x_r x_s \right), \quad x \in \mathbb{F}_2^n,$$

где $b_j = \dfrac{2\lambda_j}{q} - \dfrac{1}{2}$ при $j = 1, 2, \ldots, n$ и $\widetilde{\lambda}_0 = \lambda_0 + \dfrac{3q}{4} + \dfrac{3}{2} \sum\limits_{k=1}^{n} \lambda_k$.

Таким образом, в случае $q = 2^k$ компонентные функции $a_{k-2}(x), a_{k-1}(x)$ являются квадратичными бент-функциями, а остальные — постоянными.

ЛИТЕРАТУРА

1. *Schmidt K.-U.* Quaternary constant-amplitude codes for multicode CDMA // IEEE Trans. Inform. Theory. 2009. V. 55. No. 4. P. 1824–1832.
2. *Stănică P., Martinsen T., Gangopadhyay S., and Singh B. K.* Bent and generalized bent functions // Des. Codes Cryptogr. 2013. V. 69. No. 1. P. 77–94.
3. *Singh B. K.* On cross-correlation spectrum of generalized bent functions in generalized Maiorana — McFarland class // Inform. Sci. Lett. 2013. V. 2. No. 3. P. 139–145.
4. *Hodžić S., Meidl W., and Pasalic E.* Full characterization of generalized bent functions as (semi)-bent spaces, their dual, and the Gray image // IEEE Trans. Inform. Theory. 2018. V. 64. No. 7. P. 5432–5440.
5. *Токарева Н. Н.* Обобщения бент-функций. Обзор работ // Дискретный анализ и исследование операций. 2010. Т. 17. № 1. С. 33–62.
6. *Meidl W.* A survey on p-ary and generalized bent functions // Cryptogr. Commun. 2022. V. 14. No. 4. P. 737–782.
7. *Куценко А. В.* О некоторых свойствах самодуальных обобщённых бент-функций // Прикладная дискретная математика. Приложение. 2021. № 14. С. 42–45.

УДК 519.7 DOI 10.17223/2226308X/17/10

ОБ ОДНОЙ КОНСТРУКЦИИ ОБРАТИМЫХ ВЕКТОРНЫХ БУЛЕВЫХ ФУНКЦИЙ

И. А. Панкратова, П. Р. Гарчукова

Рассматривается конструкция векторной булевой функции, координаты которой получаются из одной булевой функции с помощью циклического сдвига вектора переменных. Предложен алгоритм построения такой функции, обладающей свойством обратимости; доказаны его полнота и корректность; посчитано количество доставляемых им функций, а также количество обратимых функций в обобщённой конструкции — когда к вектору переменных применяется произвольная полноцикловая перестановка.

Ключевые слова: *векторные булевы функции, обратимые функции, циклически эквивалентные векторы, слова Линдона.*

Обратимые векторные булевы функции используются во многих криптосистемах, в частности в криптосистемах с функциональными ключами [1–3]. Требование к функции как ключу криптосистемы — это возможность её компактного задания. Один из способов достижения этой цели — это построение координатных функций на основе преобразований одной булевой функции.

В [4] предложена следующая конструкция функции $G : \mathbb{F}_2^n \to \mathbb{F}_2^n$:

$$G(x) = \big(f(x), f(\pi(x)), f(\pi^2(x)), \ldots, f(\pi^{n-1}(x))\big), \tag{1}$$

где $f(x)$ — булева функция от n переменных; $\pi(i) = i \bmod n + 1$ — циклический сдвиг вектора переменных влево на 1.

В данной работе изучается обратимость функции вида (1).

Назовём два вектора $x, y \in \mathbb{F}_2^n$ *циклически эквивалентными*, если $x = y \ll k$ для некоторого $k \in \mathbb{N} \cup \{0\}$, где $\ll k$ — операция циклического сдвига влево на k разрядов. Обозначим через $[a]$ смежный класс эквивалентности, содержащий элемент $a \in \mathbb{F}_2^n$; M — множество минимальных (в лексикографическом порядке) представителей из всех классов; $|X|$ — мощность множества X.

Предлагается алгоритм 1 построения функций G и f, таких, что G обратима.

Алгоритм 1

1: Разбить $\mathbb{F}_2^n$ на классы циклически эквивалентных векторов.
2: На множестве минимальных представителей M построить биекцию h, такую, что $\big|[h(a)]\big| = \big|[a]\big|$ для всех $a \in M$.
3: **Для всех** $a \in M$:
  выбрать k_a, $0 \leqslant k_a < \big|[a]\big|$, и положить $q(a) = h(a) \ll k_a$.
4: **Для всех** $a \in M$:
5: **Для всех** $j = 0, \ldots, \big|[a]\big| - 1$:
    положить $G(a \ll j) = q(a) \ll j$.
6: Положить f равной первой координате функции G.

Утверждение 1 (полнота и корректность алгоритма 1).

1) Функция G, построенная алгоритмом 1, обратима:

$$\forall x, y \in \mathbb{F}_2^n \big(G(x) = G(y) \Rightarrow x = y\big).$$

2) Любую обратимую функцию вида (1) можно получить с помощью алгоритма 1.

Доказательство.
1) Пусть $x = a \ll i$, $y = b \ll j$ для некоторых $a, b \in M$, $0 \leqslant i < \big|[a]\big|$, $0 \leqslant j < \big|[b]\big|$. По построению

$$G(x) = (q(a) \ll i) \in [h(a)], \quad G(y) = (q(b) \ll j) \in [h(b)].$$

Тогда из $G(x) = G(y)$ следует $a = b$, поскольку классы $[h(a)]$ и $[h(b)]$ не пересекаются ввиду биективности h. Но из условия $q(a) \ll i = q(a) \ll j$ получаем, что $i = j$, так как $i, j < \big|[a]\big| = \big|[h(a)]\big| = \big|[q(a)]\big|$. Значит, $x = y$.
2) Пусть $G : \mathbb{F}_2^n \to \mathbb{F}_2^n$ — обратимая функция вида (1): $G = (g_0, \ldots, g_{n-1})$, где

$$\forall x \in \mathbb{F}_2^n \, \forall i \in \{0, \ldots, n-1\} \, g_i(x) = g_0(x \ll i). \tag{2}$$

Из (2) получаем

$$G(x \ll i) = (g_i(x), \ldots, g_{n-1}(x), g_0(x), \ldots, g_{i-1}(x)) = G(x) \ll i; \tag{3}$$

из обратимости G следует, что $\big|[x]\big| = \big|[G(x)]\big|$ для всех $x \in \mathbb{F}_2^n$. Построим отображение

$$q : M \to \mathbb{F}_2^n, \quad q : a \mapsto G(a),$$

тогда $G(a \ll j) = q(a) \ll j$ для всех $a \in M$, $j \in \big\{0, \ldots, \big|[a]\big|\big\}$; отображение

$$h : M \to M, \quad h : a \mapsto \min[G(a)]$$

является биекцией, причём $\big|[a]\big| = \big|[h(a)]\big|$; координата g_0 функции G совпадает с функцией f на выходе алгоритма 1 при таком выборе h и q.
Утверждение 1 доказано. ■

На основе алгоритма 1 посчитано количество $t(n)$ обратимых функций вида (1).

Утверждение 2. Имеет место

$$t(n) = \prod_{d|n} p(d)!\, d^{p(d)}, \tag{4}$$

где $p(d)$ — количество классов мощности d циклически эквивалентных булевых векторов длины n.

Доказательство. Заметим, что мощности классов $[x]$, $x \in \mathbb{F}_2^n$, являются делителями n; с другой стороны, для каждого $d \,\big|\, n$ существует вектор $a \in \mathbb{F}_2^n$, такой, что $\big|[a]\big| = d$ (например, $a = ((0)^{d-1}1)^{n/d}$, где для любых булева вектора x и $k \in \mathbb{N}$ через $(x)^k$ обозначена конкатенация k экземпляров вектора x). Тогда количество биекций h с условием $\big|[h(a)]\big| = \big|[a]\big|$ равно

$$\prod_{d|n} p(d)!.$$

Для каждой такой биекции h для каждого из $p(d)$ классов $\big|[a]\big|$ мощности d можем выбрать d значений сдвига k_a (при всяком новом выборе, очевидно, генерируются новые функции); в результате получаем формулу (4). ■

Выведем теперь формулу вычисления $p(d)$; заметим: $p(d)$ — это количество двоичных слов Линдона [5] длины d, т. е. векторов, не получающихся друг из друга с помощью циклического сдвига и не имеющих периода меньше d; эквивалентное определение — векторов, которые строго меньше (в лексикографическом порядке) любого своего непустого суффикса (последовательность A001037 в энциклопедии двоичных последовательностей [6]):

$$p(d) = \frac{1}{d} \sum_{k|d} \mu(d/k) 2^k. \tag{5}$$

Здесь $\mu(x)$ — функция Мёбиуса [7]:

$$\mu(x) = \begin{cases} 1, & \text{если } x = 1, \\ (-1)^k, & \text{если } x \text{ — произведение } k \text{ различных простых}, \\ 0 & \text{иначе.} \end{cases}$$

Формула (5) выводится из того, что общее количество двоичных векторов длины n равно

$$2^n = \sum_{d|n} d p(d),$$

с помощью обращения Мёбиуса [8, теорема 3.24]: если f и g — арифметические функции, то

$$g(n) = \sum_{d|n} f(d) \;\Leftrightarrow\; f(n) = \sum_{d|n} \mu(n/d) g(d).$$

Значения $\mu(n)$, $p(n)$ и $t(n)$ для $n = 1, \ldots, 6$ приведены в таблице; заметим, что с ростом n доля функций вида (1) среди всех $2^n!$ подстановок на $\mathbb{F}_2^n$ стремится к нулю.

Значения $p(d)$ совпадают с количеством различных неприводимых над $\mathbb{F}_2$ многочленов степени d [9, Remark 15.11, с. 267], а $t(n)$ — с количеством перестановочных многочленов [10] над полем $\mathbb{F}_{2^n}$, коэффициенты которых лежат в $\mathbb{F}_2$ [11, Theorem 2, Corollary] (последовательность A326932 [12]), хотя коэффициенты многочленов над $\mathbb{F}_{2^n}$, задающих перестановку G вида (1), не обязательно лежат в $\mathbb{F}_2$; «глубинную» связь между этими объектами ещё предстоит выяснить.

n	$\mu(n)$	$p(n)$	$t(n)$
1	1	2	2
2	-1	1	4
3	-1	2	36
4	0	3	1536
5	-1	6	22 500 000
6	1	9	263 303 591 362 560

Построить множество M минимальных представителей классов циклически эквивалентных векторов длины n можно следующим способом ($|w|$ — длина вектора $w \in \mathbb{F}_2^n$):

1) с помощью алгоритма Дюваля [13] найти множество L всех двоичных слов Линдона длины не больше n (алгоритм 2);
2) для каждого $w \in L$, такого, что $|w| = d \,\big|\, n$, построить слово $a \in M$ как конкатенацию n/d экземпляров слова w: $a = (w)^{n/d}$. Попутно имеет смысл запомнить значение $\big|[a]\big| = d$.

Алгоритм 2. Перечисление двоичных слов Линдона длины не более n

1: $w_1 := 0$, $i := 1$.
2: **Пока** $w_i \neq 1$:
3: $\quad w_{i+1} := \texttt{next}(w_i)$; $i := i + 1$.
4: **ПРОЦЕДУРА** `next`(w)
5: Построить слово $z{=}(w)^{[n/|w|]}w'$ длины n, где w' — префикс слова w длины $n \bmod |w|$;
6: если последний символ в z равен 0, то заменить его на 1; иначе заменить в z суффикс вида $011\ldots1$ на 1.
7: **Вернуть** z.

В работе [14] предложено следующее обобщение конструкции (1): в качестве π рассматривать любую перестановку переменных, а не только циклический сдвиг; будем обозначать эту конструкцию (1′) и для указания используемой перестановки добавим в обозначение функции индекс π:

$$G_\pi(x) = \big(f(x), f(\pi(x)), f(\pi^2(x)), \ldots, f(\pi^{n-1}(x))\big).$$

В [14] доказано, что для обратимости функции G в этом случае π должна быть полноцикловой.

Утверждение 3. Количество обратимых функций вида (1′) равно $t(n)(n-1)!$.

Доказательство. Количество полноцикловых подстановок π степени n равно $(n-1)!$; надо доказать, что при разных подстановках получаются разные функции.

Для конструкции (1′) имеет место аналог равенства (3):

$$G_\pi(\pi^i(x)) = G_\pi(x) \ll i.$$

Пусть $G_{\pi_1} \equiv G_{\pi_2}$ для некоторых π_1, π_2. Тогда для всех $x \in \mathbb{F}_2^n$ имеет место

$$G_{\pi_1}(x) = G_{\pi_2}(x) \;\Rightarrow\; G_{\pi_1}(\pi_1(x)) = G_{\pi_2}(\pi_2(x)) \;\Rightarrow\; \pi_1(x) = \pi_2(x)$$

(последняя импликация верна в силу обратимости функции), а это возможно только при $\pi_1 = \pi_2$. ■

В дальнейшем предстоит рассмотреть различные способы задания и вычисления функции G, зависимость её криптографических свойств от выбора f и π, целесообразность объявления перестановки π частью ключа и др. В частности, для вычисления значения $G(x)$ может быть полезен алгоритм нахождения минимального представителя в классе эквивалентности $[x]$ [15].

Авторы благодарят К. Д. Царегородцева, который заметил совпадение значений $t(n)$ с элементами последовательности A326932 и любезно поделился своим наблюдением; это позволило сформулировать и доказать утверждение 2.

ЛИТЕРАТУРА

1. *Agibalov G. P.* Substitution block ciphers with functional keys // Прикладная дискретная математика. 2017. № 38. С. 57–65.
2. *Агибалов Г. П., Панкратова И. А.* Криптосистемы с открытым ключом на булевых функциях // Прикладная дискретная математика. Приложение. 2018. № 11. С. 54–57.
3. *Agibalov G. P. and Pankratova I. A.* Asymmetric cryptosystems on Boolean functions // Прикладная дискретная математика. 2018. № 40. С. 23–33.
4. *Зюбина Д. А., Токарева Н. Н.* S-блоки с максимальной компонентной алгебраической иммунностью от малого числа переменных // Прикладная дискретная математика. Приложение. 2021. № 14. С. 40–42.
5. *Chen K. T., Fox R. H., and Lyndon R. C.* Free differential calculus, IV. The quotient groups of the lower central series // Ann. Math. 2nd Ser. 1958. V. 68. No. 1. P. 81–95.
6. `https://oeis.org/A001037`.
7. *Виноградов И. М.* Основы теории чисел. М.: Наука, 1972. 168 с.
8. *Лидл Р., Нидеррайтер Г.* Конечные поля. Т. 1. М.: Мир, 1988. 432 с.
9. *Bremner M. R.* Lattice Basis Reduction. Boca Raton, London, N.Y.: CRC Press, 2012. 334 p.
10. *Лидл Р., Нидеррайтер Г.* Конечные поля. Т. 2. М.: Мир, 1988. 394 с.
11. *Carlitz L. and Hayes D. R.* Permutations with coefficients in a subfield // Acta Arithmetica. 1972. V. XXI. P. 131–135.
12. `https://oeis.org/A326932`.
13. *Berstel J. and Pocchiola M.* Average cost of Duval's algorithm for generating Lyndon words // Theor. Comput. Sci. 1994. V. 132. P. 415–425.
14. *Панкратова И. А., Медведев А. А.* Построение подстановки на $\mathbb{F}_2^n$ на основе одной булевой функции // Прикладная дискретная математика. Приложение. 2023. № 16. С. 29–31.
15. Декомпозиция Линдона. Алгоритм Дюваля. Нахождение наименьшего циклического сдвига. `http://e-maxx.ru/algo/duval_algorithm`.

УДК 519.7 DOI 10.17223/2226308X/17/11

КРИПТОАНАЛИТИЧЕСКАЯ ОБРАТИМОСТЬ ФУНКЦИЙ ТРЁХ АРГУМЕНТОВ

И. А. Панкратова, А. Д. Сорокоумова

Предложены тесты криптоаналитической обратимости для функций от трёх аргументов. Сформулированы алгоритмы построения функции восстановления и генерации обратимых функций.

Ключевые слова: *обратимость функции по переменной, криптоаналитическая обратимость, тест обратимости, функция восстановления.*

Понятие криптоаналитической обратимости функции введено Г. П. Агибаловым в [1, 2] как обобщение, с одной стороны, понятия «обычной» обратимости функции, с другой — криптоаналитической обратимости конечного автомата [3].

Определение 1 [2]. Функция $g(x_1, \ldots, x_n)$ *обратима по переменной* x_k, $k \in \{1, \ldots, n\}$, *типа* $K_1 \ldots K_n$, где $K_i \in \{\exists, \forall\}$, $i = 1, \ldots, n$, и $K_k = \forall$, если существует *функция восстановления* f, такая, что верна формула

$$K_1 x_1 \ldots K_n x_n \big(f(g(x_1, \ldots, x_n)) = x_k\big).$$

Если функция обратима по всем переменным типа $\forall\forall \ldots \forall$, то она обратима в классическом смысле. Понятие обратимости функции по переменной x_i того же типа совпадает с понятием инъективности функции по переменной x_i [4, с. 31].

Пусть, например, X — множество открытых текстов; K — множество ключей; Y — множество шифртекстов. Тогда функция шифрования $g : K \times X \to Y$ должна быть инъективна по второй переменной (для каждого ключа $k \in K$ по значению $g(k, x)$ однозначно восстанавливается открытый текст $x \in X$). Инъективность функции g по первой переменной необязательна, допускается существование эквивалентных ключей.

Замена в типе обратимости квантора всеобщности на квантор существования «ослабляет» требования к функции шифрования; например, для рассылки сообщений в сети с множеством абонентов можно использовать функцию шифрования, обратимую типа $\exists\forall$ по второй переменной: сообщение расшифровывается однозначно не для всех ключей, а для некоторых (в идеале — для одного, только для ключа адресата).

Для каждого типа обратимости возникают следующие задачи:

1) разработка теста обратимости;
2) разработка алгоритма построения функции восстановления;
3) разработка алгоритма генерации обратимой функции.

В [5] эти задачи решены для случая $n = 2$, в данной работе — для $n = 3$. Отметим, что в определении обратимости конечного автомата [3] используются три квантора.

Будем рассматривать функции вида

$$g : D_1 \times D_2 \times D_3 \to D,$$

где D_1, D_2, D_3, D — произвольные множества. Некоторые из типов обратимости при $n = 3$ сводятся к случаю $n = 2$; ввиду коммутативности одноимённых кванторов не всегда нужно отдельно рассматривать обратимость по разным переменным. Все типы обратимости для $n = 3$ перечислены в таблице.

Тип обратимости	По переменным	Экв. тип для $n = 2$
$\forall\forall\forall$	x_1	$\forall\forall$
$\forall\forall\exists$	x_1	–
$\forall\exists\forall$	x_1, x_3	–
$\forall\exists\exists$	x_1	$\forall\exists$
$\exists\forall\forall$	x_2	–
$\exists\forall\exists$	x_2	–
$\exists\exists\forall$	x_3	$\exists\forall$

Поясним первую строку таблицы, для остальных рассуждения аналогичны. Следующие кванторные приставки эквивалентны:

$$\forall x_1 \in D_1 \forall x_2 \in D_2 \forall x_3 \in D_3 \;\simeq\; \forall x_2 \in D_2 \forall x_1 \in D_1 \forall x_3 \in D_3 \;\simeq$$
$$\simeq\; \forall x_3 \in D_3 \forall x_1 \in D_1 \forall x_2 \in D_2 \;\simeq\; \forall x_1 \in D_1 \forall (x_2, x_3) \in D_2 \times D_3,$$

поэтому, во-первых, нет смысла рассматривать отдельно обратимости по переменным x_1, x_2 и x_3, а во-вторых, задача сводится к обратимости типа $\forall\forall$ для функции двух переменных $g(x, y)$, где $x \in D_1$, $y \in D_2 \times D_3$.

Обратимость типа $\forall\forall\exists$ по переменной x_1

Функция $g(x_1, x_2, x_3)$ является обратимой типа $\forall\forall\exists$ по переменной x_1, если

$$\exists f \forall x_1 \forall x_2 \exists x_3 \big(f(g(x_1, x_2, x_3)) = x_1\big).$$

Утверждение 1. Функция $g : D_1 \times D_2 \times D_3 \to D$ обратима типа $\forall\forall\exists$ по переменной x_1, если и только если существует отображение $\varphi : D_1 \times D_2 \to D_3$, для которого выполнено условие

$$\forall a, c \in D_1 \, \forall b, d \in D_2 \, \big(a \neq c \;\Rightarrow\; g(a, b, \varphi(a, b)) \neq g(c, d, \varphi(c, d))\big). \tag{1}$$

Функция восстановления $f : D \to D_1$ строится следующим образом:

1) $f(g(a, b, \varphi(a, b))) = a$ для всех $a \in D_1$, $b \in D_2$;
2) $f(x)$ равна любому значению из D_1 для тех $x \in D$, значения на которых не определены на шаге 1.

Функциональность отношения f следует из условия (1).

Способ генерации обратимой функции $g : D_1 \times D_2 \times D_3 \to D$ описан в алгоритме 1.

Алгоритм 1. Генерация функции, обратимой типа $\forall\forall\exists$ по переменной x_1

Построить произвольное разбиение множества D на классы H_a, $a \in D_1$.
Для всех $a \in D_1$:
  Для всех $b \in D_2$:
    выбрать $c \in D_3$, $z \in H_a$;
    положить $g(a, b, c) := z$;
    для всех $x_3 \in D_3 \setminus \{c\}$ выбрать в качестве $g(a, b, x_3)$ произвольное значение $y \in D$.

Доказаны полнота и корректность алгоритма 1. Алгоритмы генерации функций других типов обратимости аналогичны и здесь не приводятся.

Обратимость типа $\forall\exists\forall$ по переменной x_1

Функция $g(x_1, x_2, x_3)$ обратима типа $\forall\exists\forall$ по переменной x_1, если

$$\exists f \forall x_1 \exists x_2 \forall x_3 \big(f(g(x_1, x_2, x_3)) = x_1\big).$$

Утверждение 2. Функция $g : D_1 \times D_2 \times D_3 \to D$ обратима типа $\forall\exists\forall$ по переменной x_1, если и только если существует отображение $\varphi : D_1 \to D_2$, для которого выполнено условие

$$\forall a, c \in D_1 \, \forall b, d \in D_3 \, \big(a \neq c \;\Rightarrow\; g(a, \varphi(a), b) \neq g(c, \varphi(c), d)\big).$$

Функция восстановления $f : D \to D_1$ строится следующим образом:

1) $f(g(a, \varphi(a), b)) = a$ для всех $a \in D_1$, $b \in D_3$;
2) $f(x)$ равна любому значению из D_1 для тех $x \in D$, значения на которых не определены на шаге 1.

Обратимость типа $\forall\exists\forall$ по переменной x_3

Функция $g(x_1, x_2, x_3)$ обратима типа $\forall\exists\forall$ по переменной x_3, если

$$\exists f \forall x_1 \exists x_2 \forall x_3 \big(f(g(x_1, x_2, x_3)) = x_3\big).$$

Утверждение 3. Функция $g\colon D_1 \times D_2 \times D_3 \to D$ обратима типа $\forall\exists\forall$ по переменной x_3, если и только если существует отображение $\varphi : D_1 \to D_2$, для которого выполнено условие

$$\forall a, c \in D_1 \, \forall b, d \in D_3 \, \big(b \neq d \;\Rightarrow\; g(a, \varphi(a), b) \neq g(c, \varphi(c), d)\big).$$

Функция восстановления $f : D \to D_3$ строится следующим образом:

1) $f(g(a, \varphi(a), b)) = b$ для всех $a \in D_1$, $b \in D_3$;
2) $f(x)$ равна любому значению из D_3 для тех $x \in D$, значения на которых не определены на шаге 1.

Обратимость типа $\exists\forall\forall$ по переменной x_2

Функция $g(x_1, x_2, x_3)$ обратима типа $\exists\forall\forall$ по переменной x_2, если

$$\exists f \exists x_1 \forall x_2 \forall x_3 \big(f(g(x_1, x_2, x_3)) = x_2\big).$$

Утверждение 4. Функция $g : D_1 \times D_2 \times D_3 \to D$ обратима типа $\exists\forall\forall$ по переменной x_2, если и только если существует такое значение $a \in D_1$, для которого выполнено условие

$$\forall b, d \in D_2 \, \forall y, z \in D_3 \, \big(b \neq d \;\Rightarrow\; g(a, b, y) \neq g(a, d, z)\big). \tag{2}$$

Функция восстановления $f : D \to D_2$ строится следующим образом:

1) $f(g(a, b, c)) = b$ для $a \in D_1$, удовлетворяющего условию (2), и всех $b \in D_2$, $c \in D_3$;
2) $f(x)$ равна любому значению из D_2 для тех $x \in D$, значения на которых не определены на шаге 1.

Обратимость типа $\exists\forall\exists$ по переменной x_2

Функция $g(x_1, x_2, x_3)$ обратима типа $\exists\forall\exists$ по переменной x_2, если

$$\exists f \exists x_1 \forall x_2 \exists x_3 \big(f(g(x_1, x_2, x_3)) = x_2\big).$$

Утверждение 5. Функция $g : D_1 \times D_2 \times D_3 \to D$ обратима типа $\exists\forall\exists$ по переменной x_2, если и только если существуют такие значение $a \in D_1$ и отображение $\varphi : D_2 \to D_3$, для которых выполнено условие

$$\forall b, d \in D_2 \, \big(b \neq d \;\Rightarrow\; g(a, b, \varphi(b)) \neq g(a, d, \varphi(d))\big). \tag{3}$$

Функция восстановления $f : D \to D_2$ строится следующим образом:

1) $f(g(a, b, \varphi(b))) = b$ для $a \in D_1$, удовлетворяющего условию (3), и всех $b \in D_2$;
2) $f(x)$ равна любому значению из D_2 для тех $x \in D$, значения на которых не определены на шаге 1.

Ввиду общезначимости предиката $\forall x \, \forall y \, P(x, y) \Rightarrow \forall x \, \exists y \, P(x, y)$ (при непустой области определения переменной y) функция, обратимая типа $\exists\forall\forall$ по переменной x_2, обратима типа $\exists\forall\exists$ по той же переменной. Обратное в общем случае неверно.

Открытые вопросы

1) Предложенные тесты обратимости не конструктивны, так как требуют проверки существования подходящих значений $a \in D_1$ и/или отображений φ. Нужно разработать алгоритмы поиска (построения) таких значений и отображений.

2) Интересно подсчитать (или хотя бы оценить) количество обратимых функций различных типов. Задача не кажется тривиальной, поскольку при разном выборе параметров алгоритмы генерации могут выдавать одни и те же обратимые функции.

Полное изложение результатов (со всеми алгоритмами, доказательствами и примерами) планируется опубликовать в журнале «Прикладная дискретная математика».

ЛИТЕРАТУРА

1. *Agibalov G. P.* Cryptanalytical finite automaton invertibility with finite delay // Прикладная дискретная математика. 2019. № 46. С. 27–37.
2. *Agibalov G. P.* Problems in theory of cryptanalytical invertibility of finite automata // Прикладная дискретная математика. 2020. № 50. С. 62–71.
3. *Agibalov G. P.* Cryptanalytic concept of finite automaton invertibility with finite delay // Прикладная дискретная математика. 2019. № 44. С. 34–42.
4. *Фомичев В. М.* Методы дискретной математики в криптологии. М.: Диалог-МИФИ, 2010. 424 с.
5. *Бердникова Н. Ю., Панкратова И. А.* Криптоаналитическая обратимость функций двух аргументов // Прикладная дискретная математика. Приложение. 2021. № 14. С. 67–71.

УДК 519.7 DOI 10.17223/2226308X/17/12

О ВОЗМОЖНОСТИ ПОСТРОЕНИЯ S-БЛОКА, УСТОЙЧИВОГО К АЛГЕБРАИЧЕСКОМУ КРИПТОАНАЛИЗУ, С ПОМОЩЬЮ ВЫБОРА КООРДИНАТНЫХ БУЛЕВЫХ ФУНКЦИЙ[1]

И. С. Хильчук

Изучается множество булевых функций от малого числа переменных с оптимальными показателями алгебраической и корреляционной иммунности. Исследуется возможность использования данных функций в качестве координатных функций S-блока.

Ключевые слова: *симметричное шифрование, булевы функции, векторные булевы функции, алгебраическая иммунность, корреляционная иммунность.*

Векторные булевы функции, или S-блоки, являются основными нелинейными компонентами симметричных шифров, их криптографические свойства обеспечивают стойкость шифра к различным видам криптоанализа. Из-за сложности полного перебора всего множества векторных булевых функций для поиска оптимальных по криптографическим критериям функций интерес представляет поиск способов конструировать векторные функции с хорошими криптографическими параметрами на основе булевых функций. Так, в 2016 г. при решении задания Международной олимпиады по криптографии NSUCRYPTO А. Удовенко найдены векторные функции от 5, 6 и 10 переменных с максимальной компонентной алгебраической иммунностью [1]. Эти функции получены на основе булевых функций f от n переменных с максимальной

[1]Работа выполнена при поддержке Математического центра в Академгородке, соглашение с Министерством науки и высшего образования Российской Федерации № 075-15-2022-282.

алгебраической иммунностью и перестановки π следующим образом:

$$F(x) = (f_1(x), f_2(x), \ldots, f_n(x)), \tag{1}$$

где $f_i(x) = f(\pi^{i-1}(x))$, $i = 1, \ldots, n$. В данной работе основным рассматриваемым свойством является компонентная алгебраическая иммунность, являющаяся одним из обобщений алгебраической иммунности на случай векторных булевых функций. Высокая алгебраическая иммунность используемых в шифре булевых функций обеспечивает стойкость шифра к алгебраическому криптоанализу, введённому Н. Куртуа в 2003 г. [2]. Корреляционная иммунность используется в качестве вспомогательного свойства для сокращения числа рассматриваемых булевых функций и поиска закономерностей и интересных структур, так как накладывает ограничения на расположение носителя булевой функции в булевом кубе.

Обозначим через $\mathbb{Z}_2$ множество $\{0, 1\}$, тогда $\mathbb{Z}_2^n$ — векторное пространство двоичных векторов длины n. *Булева функция* f — это произвольное отображение из $\mathbb{Z}_2^n$ в $\mathbb{Z}_2$. *Весом Хэмминга* $\mathrm{wt}(f)$ булевой функции f называется число ненулевых координат её вектора значений. Функция g называется *аннулятором* функции f, если g не равна тождественно нулю и $f \cdot g \equiv 0$. *Алгебраическая иммунность* $\mathrm{AI}(f)$ функции f — минимальная из степеней аннуляторов функций f и $f \oplus 1$. Булева функция f от n переменных называется *корреляционно-иммунной порядка* r, $1 \leqslant r \leqslant n$, если для любой её подфункции $f_{i_1,\ldots,i_r}^{a_1,\ldots,a_r}$, полученной фиксацией r переменных, выполняется равенство

$$\mathrm{wt}(f_{i_1,\ldots,i_r}^{a_1,\ldots,a_r}) = \mathrm{wt}(f)/2^r.$$

Введём обозначение для максимального порядка корреляционной иммунности: $\mathrm{CI}(f) = \max\{m \in \mathbb{N} : f$ — корреляционно-иммунная порядка $m\}$.

Векторная булева функция F — произвольное отображение из $\mathbb{Z}_2^n$ в $\mathbb{Z}_2^m$. Её можно рассматривать как набор из m *координатных функций* от n переменных: $F(x) = (f_1(x), f_2(x), \ldots, f_m(x))$. В данной работе рассматривается только случай $m = n$. *Компонентной функцией* для F называется любая нетривиальная линейная комбинация её координатных функций $v \cdot F$, где $v \in \mathbb{Z}_2^n$, $v \neq 0$. *Компонентная алгебраическая иммунность* векторной булевой функции — минимальная алгебраическая иммунность её компонентных функций. Известна оценка сверху для алгебраической иммунности булевой функции от n переменных [2] и оценка сверху на компонентную алгебраическую иммунность векторной булевой функции [3]: $\mathrm{AI}(f), \mathrm{AI}_{\mathrm{comp}}(F) \leqslant \lceil n/2 \rceil$.

Как и в работе [4], рассмотрим множество функций от 4 переменных с $\mathrm{AI}(f) = 2$ и $\mathrm{CI}(f) = 1$. Таких функций 392, из них 96 имеют вес Хэмминга 6, 96 — вес 10 и 200 — вес 8.

С помощью написанной программы исследованы всевозможные сочетания функций с весом 6 в качестве координатных функций S-блока и проверена его компонентная алгебраическая иммунность. Из 3 321 966 возможных S-блоков максимальную компонентную алгебраическую иммунность имеют 224 064 S-блока. Каждая из 96 функций используется в 9 336 S-блоках в качестве координатной функции. Аналогичные результаты получены и для функций веса 10.

Исследована также возможность построения векторной булевой функции вида (1), имеющей максимальную компонентную алгебраическую иммунность. В работе Д. А. Зюбиной, Н. Н. Токаревой [5] показано, что для функций от четырёх переменных только при полноцикловых перестановках π существуют векторные булевы функции,

которые сохраняют максимальную иммунность. Для каждой полноцикловой перестановки существует 6 144 булевых функций, таких, что построенные на их основе векторные булевы функции также имеют максимально возможную компонентную алгебраическую иммунность. Однако ни одна из рассматриваемых 392 функций не подошла для построения векторной булевой функции с максимальной компонентной алгебраической иммунностью с какой-либо из перестановок полного цикла.

Для циклического сдвига влево возможно построить 10 852 S-блока с оптимальной компонентной алгебраической иммунностью таким способом:

$$F(x) = (f_1(x), f_1(\pi(x)), f_1(\pi^2(x)), f_2(x)),$$

где $f_1(x), f_2(x)$ — произвольные функции из 392 рассматриваемых, $f_1(x) \neq f_2(x)$.

Конструкция (1) изучается также в работе [6], где приведены необходимые условия на функцию f и перестановку π для построения S-блока, допускающего однозначное расшифрование. Из 200 рассматриваемых функций веса 8 ни одна не подошла в качестве координатной функции для взаимно-однозначной векторной булевой функции при использовании какой-либо перестановки полного цикла на множестве из четырёх элементов.

ЛИТЕРАТУРА

1. *Tokareva N., Gorodilova A., Agievich S., et al.* Mathematical methods in solutions of the problems from the Third International Students' Olympiad in Cryptography // Прикладная дискретная математика. 2018. № 40. С. 34–58.
2. *Courtois N. and Meier W.* Algebraic attacks on stream ciphers with linear feedback // LNCS. 2003. V. 2656. P. 345–359.
3. *Carlet C.* On the algebraic immunities and higher order nonlinearities of vectorial Boolean Functions // Proc. NATO Advanced Research Workshop ACPTECC, Veliko Tarnovo, Bulgaria, October 6–9, 2008. Amsterdam, IOS Press, 2009. P. 104–116.
4. *Хильчук И. С., Зюбина Д. А., Токарева Н. Н.* О корреляционно-иммунных функциях с максимальной алгебраической иммунностью // Прикладная дискретная математика. Приложение. 2022. № 15. С. 34–40.
5. *Зюбина Д. А., Токарева Н. Н.* S-блоки специального вида от малого числа переменных // Дискретный анализ и исследование операций. 2023. № 30(2). С. 67–80.
6. *Панкратова И. А., Медведев А. А.* Построение подстановки на $\mathbb{F}_2^n$ на основе одной булевой функции // Прикладная дискретная математика. Приложение. 2023. № 16. С. 29–31.

Секция 3

МАТЕМАТИЧЕСКИЕ МЕТОДЫ КРИПТОГРАФИИ

УДК 004.056 DOI 10.17223/2226308X/17/13

АТАКИ НА ПРОТОКОЛЫ АУТЕНТИФИЦИРОВАННОЙ ВЫРАБОТКИ ОБЩЕГО КЛЮЧА НА ОСНОВЕ СХЕМ ПОДПИСИ ПРИ СВЯЗАННЫХ КЛЮЧАХ УЧАСТНИКОВ

Е. К. Алексеев, С. Н. Кяжин

Описываются атаки на протоколы аутентифицированной выработки общего ключа SIGMA, SIG-DH и TS3-1 при наличии у нарушителя возможности навязывания связанных долговременных ключей честным участникам при их регистрации в сети. Важным условием реализуемости описываемых атак является наличие у схем подписи, используемых в указанных протоколах, уязвимости к атаке со связанными ключами (примером уязвимой схемы подписи является схема ECDSA). В результате каждой из трёх описываемых атак реализуется угроза ложной аутентификации. Атаки отличаются используемым набором возможностей нарушителя, необходимость которых вызвана особенностями конструкции протоколов в части подписываемых сообщений. Если подписывается идентификатор инициатора, передаваемый в первом сообщении, то дополнительно требуется возможность навязывания честному участнику его идентификатора при регистрации в сети. Если подписывается эфемерный ключ ответчика, то требуется возможность компрометации будущих открытых эфемерных ключей.

Ключевые слова: *криптография, криптографический протокол, протокол аутентифицированной выработки общего ключа, связанные ключи, схема подписи.*

Введение

Протоколом аутентифицированной выработки общего ключа (Authenticated Key Establishment, AKE) между сторонами A и B будем называть криптографический протокол формирования этими сторонами общего секретного ключа путём обмена сообщениями по незащищённому каналу связи, в результате выполнения которого сторона A (B) убеждена в том, что сформированный общий секретный ключ неизвестен никому, кроме стороны B (A). Такие протоколы довольно широко распространены и имеют в определённой степени сложившуюся историю изучения; в литературе известно большое количество протоколов (см., например, работу [1]), обладающих различными достоинствами и недостатками.

При анализе AKE-протоколов используются разные модели нарушителя, определяемые особенностями использования протоколов. К классическим возможностям нарушителя относят возможности так называемого активного нарушителя в канале. Однако на практике у нарушителя зачастую возникают расширенные возможности, например навязывание связанных ключей [2].

Отметим, что наличие связанных ключей — известная особенность модели нарушителя, в которой анализируются криптографические механизмы, в том числе асиммет-

ричные. Например, в [3] представлен обзор различных моделей угроз и нарушителя, учитывающих наличие связанных ключей подписи, в [4] — обзор результатов анализа (в том числе атак) распространённых схем подписи в данных моделях.

В настоящей работе описываются атаки на три AKE-протокола в моделях нарушителя, обладающего возможностью навязывания связанных долговременных ключей участников, при использовании в этих протоколах схем подписи, уязвимых к атаке со связанными ключами. В целях удобства описание всех протоколов приводится в соответствии с принципами и обозначениями, использованными в работе [1].

1. Рассматриваемый класс протоколов

Обычно при описании криптографических протоколов не указывают конкретные криптографические примитивы, которые предлагается использовать, но ограничиваются указанием классов механизмов (например, схема подписи или схема выработки имитовставки, а не ECDSA или OMAC-AES). При этом зачастую от этих механизмов требуется наличие «стандартных» криптографических свойств. Однако порой для обеспечения стойкости протокола требуется, чтобы используемые базовые механизмы обладали дополнительными свойствами (не обладали соответствующими свойствами-уязвимостями).

В настоящей работе рассматривается случай использования AKE-протоколами схем подписи, которые обладают следующим свойством-уязвимостью: по сообщению m и значению подписи, сформированному для него на ключе sk, без знания ключа sk можно сформировать значение подписи для любого сообщения m', корректное относительно ключа $sk \cdot \delta_{m,m'}$, где значение «сдвига» $\delta_{m,m'}$ однозначно определяется значениями m, m'. Примером такой схемы подписи является схема ECDSA (соответствующая атака, применимая к схеме ECDSA, описана в [5]).

2. Модели угроз и нарушителя

К классическим угрозам для AKE-протоколов можно отнести ложную аутентификацию, при которой нарушитель обладает некоторой информацией о ключе, при этом одна из сторон убеждена в том, что ключ неизвестен никому, кроме участника-партнёра. Все три описываемых атаки приводят к реализации нарушителем угрозы ложной аутентификации: нарушитель, не зная ключа участника A, вырабатывает с участником B общий секретный ключ, но при этом участник B уверен, что этот секретный ключ он выработал с участником A.

Для реализации атак нарушитель использует следующие возможности:

— классические возможности активного нарушителя в канале;
— возможность навязывания связанных ключей при регистрации участников.

Отметим, что возможность навязывания связанных ключей не предполагает наличия возможности регистрации нарушителя в качестве легитимного участника сети; она предполагает возможность выбора нарушителем такого «сдвига» δ, что у вновь регистрируемого честного участника долговременный ключ будет равен ключу выбираемого нарушителем ранее зарегистрированного участника, умноженному на значение δ (при этом сами значения ключей нарушителю неизвестны и, тем более, нарушитель не может самостоятельно выбирать их).

Для реализации атаки на протокол SIGMA нарушителю достаточно указанных возможностей. Особенности же протоколов TS3-1 и SIG-DH вынуждают использовать дополнительные возможности:

— возможность навязывания идентификатора участника при регистрации (для атаки на протокол TS3-1);
— возможность компрометации будущих открытых эфемерных ключей (для атаки на протокол SIG-DH).

3. Атака на протокол SIGMA

Опишем атаку на протокол SIGMA [6] (рис. 1), использующий уязвимую схему подписи:

1) прослушивая канал взаимодействия между участниками A и B, узнать эфемерные открытые ключи E_A, E_B и значение подписи σ_A;
2) произвольным образом выбрать эфемерную ключевую пару $(e_{A'}, E_{A'})$;
3) отправить участнику B первое сообщение протокола $(E_{A'})$;
4) получив от участника B второе сообщение протокола, содержащее E_B^*, сформировать:
   а) значение δ и значение подписи $\sigma_{A'}$ для сообщения $(E_B^*, E_{A'})$, корректное относительно ключа $sk_{A'}^s = sk_A^s \cdot \delta$;
   б) ключи K, K^a с использованием ключей $e_{A'}$ и E_B^*;
5) навязать регистрацию участника A' с ключом $sk_{A'}^s$, неизвестным нарушителю;
6) сформировать имитовставку $\tau_{A'}$ для идентификатора A';
7) отправить участнику B третье сообщение протокола $(A', \sigma_{A'}, \tau_{A'})$.

$\mathbf{A} : sk_A^s, pk_A^s$		$\mathbf{B} : sk_B^s, pk_B^s$
$e_A \xleftarrow{U} \mathbb{Z}_q^*$		
$E_A \leftarrow e_A \cdot P$	$\xrightarrow{E_A}$	$e_B \xleftarrow{U} \mathbb{Z}_q^*$
		$E_B \leftarrow e_B \cdot P$ $K, K^a \leftarrow \mathsf{KDF}(e_B \cdot E_A)$ $\sigma_B \leftarrow \mathsf{Sig}_{sk_B^s}(E_A, E_B)$
$K, K^a \leftarrow \mathsf{KDF}(e_A \cdot E_B)$	$\xleftarrow{B, E_B, \sigma_B, \tau_B}$	$\tau_B \leftarrow \mathsf{MAC}_{K^a}(B)$
Verify σ_B, τ_B $\sigma_A \leftarrow \mathsf{Sig}_{sk_A^s}(E_B, E_A)$		
$\tau_A \leftarrow \mathsf{MAC}_{K^a}(A)$	$\xrightarrow{A, \sigma_A, \tau_A}$	Verify σ_A, τ_A
return K		**return** K

Рис. 1. Схема протокола SIGMA

Таким образом, нарушитель реализует угрозу ложной аутентификации: не зная ключа $sk_{A'}^s$ участника A', он вычисляет ключ, который вычисляет сторона B, в то же время сторона B уверена, что этот ключ могла вычислить только сторона A', которая не принимала участия в протоколе.

4. Атака на протокол TS3-1

Рассмотрим модифицированную версию протокола TS3 [7] (рис. 2). Название TS3-1 взято из работы [1]. Принципиальными отличиями данного протокола от предыдуще-

го с точки зрения реализации подобной атаки является то, что идентификатор участника-инициатора является частью подписываемого сообщения и передаётся в первом сообщении.

$\mathbf{A}: sk_A^s, pk_A^s$		$\mathbf{B}: sk_B^s, pk_B^s$
$e_A \xleftarrow{U} \mathbb{Z}_q^*$		
$E_A \leftarrow e_A \cdot P$		
$\sigma_A \leftarrow \mathsf{Sig}_{sk_A^s}(A, B, E_A)$	$\xrightarrow{A, E_A, \sigma_A}$	Verify σ_A
		$e_B \xleftarrow{U} \mathbb{Z}_q^*$
		$E_B \leftarrow e_B \cdot P$
Verify σ_B	$\xleftarrow{B, E_B, \sigma_B}$	$\sigma_B \leftarrow \mathsf{Sig}_{sk_B^s}(B, A, E_B)$
$K \leftarrow e_A \cdot E_B$		$K \leftarrow e_B \cdot E_A$
return K		**return** K

Рис. 2. Схема протокола TS3-1

Указанные отличия не позволяют осуществить атаку, полностью аналогичную описанной, по следующим причинам:

— поскольку идентификатор участника-инициатора является частью подписываемого сообщения, то значение δ, которое должно быть выбрано до регистрации, будет зависеть от идентификатора участника, назначаемого при регистрации;
— поскольку идентификатор участника-инициатора передаётся в первом сообщении, то регистрация нового участника должна быть осуществлена до передачи первого сообщения «от его имени».

Так, для реализации аналогичной атаки на протокол TS3-1, использующий уязвимую схему подписи, нарушителю необходима возможность навязывания идентификатора участника при регистрации.

Действия нарушителя описываются следующим образом:

1) прослушивая канал взаимодействия между участниками A и B, узнать эфемерный открытый ключ E_A и значение подписи σ_A;
2) произвольным образом выбрать идентификатор A' и эфемерную ключевую пару $(e_{A'}, E_{A'})$;
3) на основе значений A, A', B, E_A и $E_{A'}$ сформировать значение δ и значение подписи $\sigma_{A'}$ для сообщения $(A', B, E_{A'})$, корректное относительно ключа $sk_{A'}^s = sk_A^s \cdot \delta$;
4) навязать регистрацию участника с идентификатором A' и ключом $sk_{A'}^s$, неизвестным нарушителю;
5) отправить участнику B первое сообщение протокола (A', $E_{A'}$, $\sigma_{A'}$);
6) получив от участника B второе сообщение протокола, вычислить ключ K.

Таким образом, нарушитель реализует угрозу, полностью аналогичную случаю с протоколом SIGMA.

5. Атака на протокол SIG-DH

Рассмотрим протокол SIG-DH [8] (рис. 3). Для простоты будем считать, что значение sid пустое. Данный протокол с точки зрения реализации подобной атаки отличается от предыдущего тем, что открытый эфемерный ключ ответчика является частью подписываемого сообщения. Отметим, что такой особенностью обладает также протокол SIGMA.

$\mathbf{A} : (sk_A^s, pk_A^s)$		$\mathbf{B} : (sk_B^s, pk_B^s)$
$e_A \xleftarrow{U} \mathbb{Z}_q^*$		
$E_A \leftarrow e_A \cdot P$	$\xrightarrow{A, E_A}$	$e_B \xleftarrow{U} \mathbb{Z}_q^*$
		$E_B \leftarrow e_B \cdot P$
Verify σ_B	$\xleftarrow{B, E_B, \sigma_B}$	$\sigma_B \leftarrow \mathsf{Sig}_{sk_B^s}(B, E_B, E_A, A)$
$\sigma_A \leftarrow \mathsf{Sig}_{sk_A^s}(A, E_A, E_B, B)$	$\xrightarrow{\sigma_A}$	Verify σ_A
$K \leftarrow e_A \cdot E_B$		$K \leftarrow e_B \cdot E_A$
return K		**return** K

Рис. 3. Схема протокола SIG-DH

Поскольку открытый эфемерный ключ ответчика является частью подписываемого сообщения, то значение δ, которое должно быть выбрано до регистрации нового участника, будет зависеть от данного эфемерного ключа, получаемого в рамках выполнения протокола. Так, для реализации аналогичной атаки на протокол SIG-DH, использующий уязвимую схему подписи, нарушителю необходима возможность компрометации будущих открытых эфемерных ключей.

Предположим, что сторона B в целях оптимизации своей работы заранее формирует массив T ключевых пар $(e, e \cdot P)$. Тогда в начале каждого нового взаимодействия она не генерирует эфемерную ключевую пару, а берёт её из очередного элемента массива T, после чего удаляет из него только что прочитанные значения. На рис. 4 приведено скорректированное с учётом этого предположения описание протокола SIG-DH.

Опишем атаку на протокол SIG-DH с предвычислениями на стороне B, использующий уязвимую схему подписи:

1) прослушивая канал взаимодействия между участниками A и B, узнать эфемерные открытые ключи E_A, E_B и значение подписи σ_A;
2) узнать значение элемента $E_B^* = T[0, 1]$, которое участник B будет использовать в следующем сеансе протокола;
3) произвольным образом выбрать идентификатор A' и эфемерную ключевую пару $(e_{A'}, E_{A'})$;
4) на основе значений A, A', B, E_A, E_B, $E_{A'}$ и E_B^* сформировать значение δ;
5) навязать регистрацию участника с идентификатором A' и ключом $sk_{A'}^s = sk_A^s \cdot \delta$, неизвестным нарушителю;
6) отправить участнику B первое сообщение протокола $(A', E_{A'})$;
7) получив от участника B второе сообщение протокола, содержащее E_B^*, сформировать:

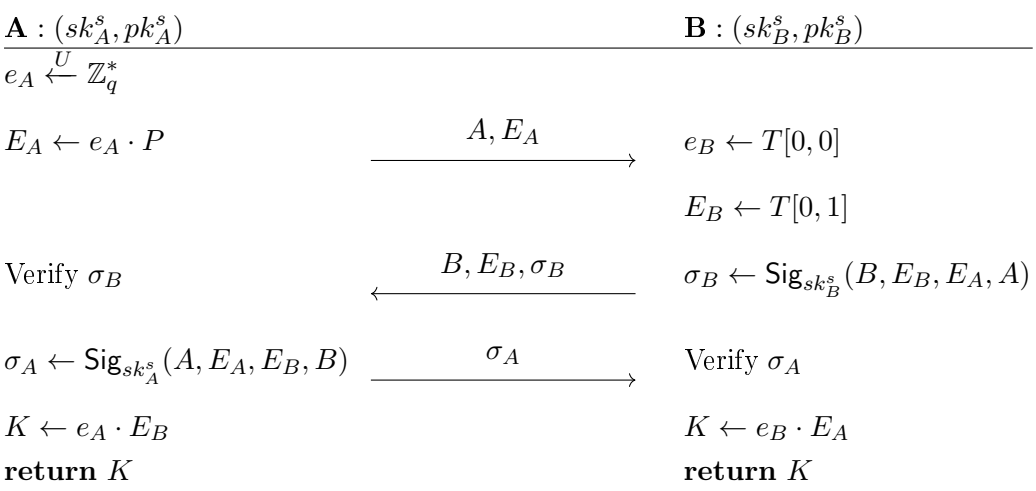

Рис. 4. Протокол SIG-DH с предвычислениями на стороне B

а) ключ $K = e_{A'} \cdot E_B^*$;
б) значение подписи $\sigma_{A'}$ для сообщения $(A', E_{A'}, E_B^*, B)$, корректное относительно ключа $sk_{A'}^s$;

8) отправить участнику B третье сообщение протокола $(\sigma_{A'})$.

Таким образом, нарушитель реализует угрозу, полностью аналогичную случаю с протоколом SIGMA.

Заключение

Описаны три атаки на различные протоколы аутентифицированной выработки общего ключа, которые предполагают наличие у нарушителя возможности навязывания связанных ключей и, в свою очередь, используют уязвимость схемы подписи, вызванную наличием связанных ключей. Две атаки требуют использования дополнительных возможностей, обусловленных особенностями протоколов:

— передача в составе первого сообщения идентификатора участника-инициатора и использование его в качестве части подписываемого сообщения требуют наличия у нарушителя возможности навязывания идентификатора при регистрации;
— передача в составе первого сообщения идентификатора участника-инициатора и использование открытого эфемерного ключа участника-ответчика в качестве части подписываемого сообщения требуют наличия у нарушителя возможности компрометации будущих открытых эфемерных ключей.

Отметим, что аналогичные атаки можно применить и для других протоколов аутентифицированной выработки общего ключа, использующих схему подписи.

ЛИТЕРАТУРА

1. *Alekseev E. K., Babueva A. A., and Zazykina O. A.* AKE Zoo: 100 Two-Party Protocols (to be continued). Cryptology ePrint Archive. 2023. Paper 2023/1044.
2. *Alekseev E. K. and Kyazhin S. N.* Probing the security landscape for authenticated key establishment protocols // 12th Workshop CTCrypt 2023. Pre-proceedings. 2023. P. 67–82.
3. *Babueva A. A. and Kyazhin S. N.* Public keys for e-coins: partially solved problem using signature with rerandomizable keys // Прикладная дискретная математика. Приложение. 2023. № 16. С. 110–114.

4. *Бабуева А. А., Кяжин С. Н.* Аддитивно связанные ключи подписи: взломать нельзя использовать // XXVI Научно-практич. конф. «РусКрипто'2024». https://www.ruscrypto.ru/resource/archive/rc2024/files/05_babueva_kyazhin.pdf.
5. *Morita H., Schuldt J. C. N., Matsuda T., et al.* On the security of the Schnorr signature scheme and DSA against related-key attacks // LNCS. 2016. V. 9558. P. 20–35.
6. *Krawczyk H.* The "SIGn-and-MAc" approach to authenticated Diffie — Hellman and its use in the IKE protocols // LNCS. 2003. V. 2729. P. 400–425.
7. *Jeong I. R., Katz J., and Lee D. H.* One-Round Protocols for Two-Party Authenticated Key Exchange. 2008. https://www.cs.umd.edu/~jkatz/papers/1round_AKE.pdf.
8. *Canetti R. and Krawczyk H.* Analysis of key-exchange protocols and their use for building secure channels // LNCS. 2001. V. 2045. P. 453–474.

УДК 519.7 DOI 10.17223/2226308X/17/14

АЛГЕБРАИЧЕСКИЕ АТАКИ НА НЕКОТОРЫЕ НИЗКОРЕСУРСНЫЕ ШИФРЫ НА ОСНОВЕ ФУНКЦИЙ С МАЛЫМ ЧИСЛОМ ВЫХОДНЫХ БИТ[1]

К. В. Антонов, А. А. Семёнов, И. В. Отпущенников, А. Л. Павленко

Вводится новый класс атак, применимых к низкоресурсным функциям симметричной криптографии. Основная идея атак основана на использовании специальных функций, получаемых из оригинальных за счёт рассмотрения малого числа выходных бит. Задачи обращения специальных функций существенно более просты для используемых в алгебраическом криптоанализе комбинаторных алгоритмов (SAT-решателей), чем задачи обращения функций, из которых они строятся. Однако для специальной функции, ввиду того, что её выход существенно короче входа, задача обращения имеет не единственное решение. Для достижения единственности по ключу описывается процедура клонирования функции, в рамках которой специальные функции строятся для одного ключа и нескольких различных фрагментов открытых данных. Операция клонирования специальных функций выполняется на And-Inverter-графах (AIG), представляющих данные функции. Во многих случаях размер AIG может быть существенно уменьшен за счёт применения алгоритмов AIG-минимизации. Результатом совместного использования перечисленных техник являются алгебраические атаки, которые для ряда поточных шифров могут быть существенно более эффективными в сравнении с аналогичными атаками на функции, представляющие рассматриваемые шифры стандартным образом.

Ключевые слова: *алгебраический криптоанализ, низкоресурсная криптография, SAT-решатели, булевы схемы.*

1. Введение и постановка задачи

Атаки, о которых идёт речь, основаны на идее, опубликованной в [1, 2]. Работа [2] довольно широко цитируется, а описанный в ней сценарий известен как «кубическая атака» (cube attack), работоспособность данной атаки демонстрируется на вариантах известного шифра Trivium [3], ослабленных по числу шагов инициализационной фазы. Основным результатом [2] заявлен подход, в рамках которого зависимость меж-

[1]Исследование выполнено в рамках госзадания Минобрнауки России по проекту «Теоретические основы, методы и высокопроизводительные алгоритмы непрерывной и дискретной оптимизации для поддержки междисциплинарных научных исследований», номер гос. регистрации 121041300065-9.

ду переменными, кодирующими ключ шифра, ищется в форме линейных уравнений над GF(2), получаемых из так называемого мастер-полинома (master-polynomial). Сам мастер-полином предполагается неизвестным (black-box), однако в [2] предлагается специальная техника, которая позволяет выводить линейные соотношения на биты ключа, исходя из предположений о его степени: используется понятие «случайного полинома степени d» (d-random polynomial). Если d не слишком велика, то линейные соотношения на биты ключа можно получать, варьируя значения некоторых переменных в соответствующем гиперкубе.

Для целей настоящей работы интересна не сама техника «tweakable black-box polynomial» [2], а функции, к которым она применяется. Мастер-полином, рассматриваемый в [2], представляет некоторую булеву функцию вида

$$f : \{0,1\}^n \times \{0,1\}^m \to \{0,1\}, \tag{1}$$

где $\{0,1\}^n$ — множество, из которого выбран секретный ключ, а $\{0,1\}^m$ — множество, из которого выбирается известная информация: инициализирующая последовательность (IV) в случае поточного шифра или блок открытого текста в случае блочного. Заметим, что выходом функции (1) является 1 бит. По-видимому, впервые задача обращения функций вида (1) в контексте криптоанализа (кстати, также шифра Trivium) рассматривалась в [1]. Особо подчеркнём характерную особенность, отличающую функции вида (1) от функций, обычно рассматриваемых в задачах алгебраического криптоанализа и имеющих вид

$$g : \{0,1\}^n \times \{0,1\}^m \to \{0,1\}^l, \tag{2}$$

где $\{0,1\}^n$ — множество секретных ключей; $\{0,1\}^m$ — множество открытых текстов или инициализирующих векторов; $\{0,1\}^l$ — множество криптограмм. Важный факт состоит в том, что в (2) для достижения единственности по ключу предполагается, что $l \geqslant n$. Например, для шифра Trivium [3] «стандартная» атака направлена на обращение функции $g : \{0,1\}^{80} \times \{0,1\}^{80} \to \{0,1\}^l$, $l \geqslant 80$: ставится задача найти 80 бит секретного ключа на основе известных l бит ключевого потока, сгенерированных алгоритмом Trivium по этому ключу и одному известному IV.

Далее задачи алгебраического криптоанализа решаются за счёт их сведения к проблеме булевой выполнимости (SAT) и использования современных SAT-решателей. В данном контексте задача обращения функций вида (2) для стойких шифров крайне сложна, тогда как обращение функций вида (1) не является сложным. Однако для функций вида (1) в общем случае, конечно, нет единственности по ключу. Далее мы несколько обобщаем исследуемый класс функций и рассматриваем функции вида

$$f : \{0,1\}^n \times \{0,1\}^m \to \{0,1\}^k, \tag{3}$$

где $k \ll n$. Очевидно, что в таких условиях при обращении (3) снова нет единственности по ключу, однако можно исследовать проблему обращения функций, полученных «клонированием» некоторого числа функций вида (3) для различных известных входных данных. Иными словами, будем рассматривать задачу поиска $z \in \{0,1\}^n$ на основе $x^i \in \{0,1\}^m$, $i \in \{1,\ldots,s\}$, таких, что для каждой пары вида (z, x^i) известно значение функции $f(z, x^i)$ вида (3). Таким образом, речь идет об обращении функций вида

$$F : \{0,1\}^n \times \{0,1\}^{sm} \to \{0,1\}^{sk}, \tag{4}$$

где $k \ll n$, $sk \geqslant n$.

Например, для шифра Trivium элементарная функция (3) строится для пары (z, IV), где z — неизвестный секретный ключ, $z \in \{0,1\}^{80}$; IV — известная инициализирующая последовательность, $\mathrm{IV} \in \{0,1\}^{80}$; выход функции — некоторые фиксированные k бит ключевого потока, генерируемого шифром Trivium по входу (z, IV). По крайней мере, для поточных шифров в роли значения (3) имеет смысл брать первые k бит соответствующего ключевого потока. Далее для s различных IV рассматриваются аналогичные функции и формируется функция вида (4).

Базовое предположение состоит в том, что для s, незначительно больших n, и для естественным образом подобранных различных IV при обращении (4) достигается единственность по ключу. Далее показано, что для ряда известных криптографических функций задачи обращения функций вида (4) существенно проще обращения функций вида (2).

Для задач обращения функций вида (4) построены атаки из класса «угадывай и определяй» (guess-and-determine), относящиеся к алгебраическому криптоанализу [4]. В таких атаках рассматриваемая задача обращения сводится к SAT, а к формулам в КНФ, ослабленным подстановками угаданных бит, применяются SAT-решатели. Конкретно, использован IBS-метод [5], основное преимущество которого состоит в том, что получаемые им оценки имеют строгие гарантии точности.

2. Предварительные сведения

Итак, главным объектом изучения являются симметричные шифры, в основном, относящиеся к низкоресурсной (lightweight) криптографии, и алгебраические атаки на них, использующие SAT-решатели. Для сведения задачи обращения функций вида (2) и (4) к SAT используются методы, базовые принципы которых изложены, например, в [6, 7]. Кратко эти принципы можно описать следующим образом. Рассматривается функция вида $f : \{0,1\}^n \to \{0,1\}^m$, определённая всюду на $\{0,1\}^n$ и заданная некоторым быстрым алгоритмом A_f, который известен. По известному $\gamma \in \mathrm{Range}\, f \subseteq \{0,1\}^m$ требуется найти такой $\alpha \in \{0,1\}^n$, что $f(\alpha) = \gamma$. По тексту A_f эффективно строится булева схема S_f (схема из функциональных элементов) над произвольным полным базисом, задающая f. По схеме S_f за линейное время от числа узлов (часто называемых гейтами) в этой схеме строится специальная КНФ C_f, называемая шаблонной (template CNF [7]). Для этой цели используются преобразования Цейтина [8].

Шаблонная КНФ обладает рядом важных свойств, одно из которых заключается в том, что интерпретация схемы S_f на произвольном входе $\alpha \in \{0,1\}^n$ может быть промоделирована последовательностью применений правила единичного дизъюнкта (Unit Propagation rule, UP) к КНФ C_f и множеству литералов $x_1^{\alpha_1}, \ldots, x_n^{\alpha_n}$, где $\alpha = (\alpha_1, \ldots, \alpha_n)$; $X^{\mathrm{in}} = \{x_1, \ldots, x_n\}$ — множество переменных, приписанных входам схемы S_f. Обозначение x^σ понимается в смысле [9]: $x^0 = \neg x$, $x^1 = x$. Последнее свойство означает, что вычисление по схеме S_f на входе $\alpha = (\alpha_1, \ldots, \alpha_n)$ можно представить как последовательность применений UP к формуле $x_1^{\alpha_1} \wedge \ldots \wedge x_n^{\alpha_n} \wedge C_f$, итогом чего будет некоторый набор литералов $y_1^{\gamma_1}, \ldots, y_m^{\gamma_m}$, где $Y = \{y_1, \ldots, y_m\}$ — множество переменных, приписанных выходам схемы S_f; $\gamma = (\gamma_1, \ldots, \gamma_m) : f(\alpha) = \gamma$.

Обозначим через $C[\beta/B]$ КНФ, полученную из исходной КНФ C в результате подстановки в C набора значений β переменных из множества B, $B \subseteq X$ (X — множество, образованное всеми переменными в КНФ C). Подстановка понимается в стандартном смысле [10], то есть как результат замены вхождений переменной соответствующей константой с последующим выполнением всех возможных элементарных преобразований. Соответственно результат применения правила UP к формуле $x_1^{\alpha_1} \wedge \ldots \wedge x_n^{\alpha_n} \wedge C_f$

можно интерпретировать как $C_f[\alpha/X^{\text{in}}]$. Результатом $C_f[\alpha/X^{\text{in}}]$ является набор значений всех переменных из X; скажем, что такой набор индуцирован входом α.

Изложим кратко суть IBS-атак [5]. Для произвольного входа $\alpha \in \{0,1\}^n$ и произвольного $B \subseteq X$ обозначим через β_α набор значений переменных из B, индуцированный входом α. Пусть $\gamma_\alpha = f(\alpha)$. Рассмотрим КНФ $C_f[\beta_\alpha/B, \gamma_\alpha/Y]$ (то есть результат подстановки в C_f наборов β_α и γ_α). К $C_f[\beta_\alpha/B, \gamma_\alpha/Y]$ применяется алгоритм A^t, время работы которого ограничено сверху величиной t (обычно t — некоторая константа); после достижения этого порога A^t прерывает работу. Предполагается, что для любой КНФ A^t выдаёт ответ из множества {SAT, UNSAT, INDET}. Ответ INDET означает, что A^t не смог определить выполнимость/невыполнимость формулы за время $\leqslant t$. Отметим, что алгоритм A^t — это фактически некоторый полиномиальный вспомогательный решатель из определения сильной лазейки (Strong Backdoor Set, SBS) [11]. Для произвольной КНФ C над переменными X, произвольного $B \subseteq X$ и алгоритма A^t обозначим через $C[\beta/B] \in \Sigma(A^t)$ ситуацию, когда результат применения A^t к $C[\beta/B]$ лежит в множестве {SAT, UNSAT}; в случае ответа INDET используем обозначение $C[\beta/B] \notin \Sigma(A^t)$.

Зададим на $\{0,1\}^n$ равномерное распределение и рассмотрим величину

$$\rho_B = |\{\alpha : C_f[\beta_\alpha/B, \gamma_\alpha/Y] \in \Sigma(A^t)\}|/2^n. \tag{5}$$

Величина (5) — это вероятность того, что решатель A^t обратит $\gamma_\alpha \in \operatorname{Range} f$ при условии известного β_α, играющего роль правильной подсказки. Множество B с $\rho_B > 0$ называется Inverse Backdoor Set (IBS). Если B — некоторый IBS, то на его основе можно построить атаку [5], которая обращает хотя бы один выход из множества $\gamma_1, \ldots, \gamma_k$, $\gamma_i \in \operatorname{Range} f$, $i \in \{1, \ldots, k\}$, с вероятностью $> 0{,}95$ за время $\approx 2^{|B|} \cdot 3t/\rho_B$.

Шаблонные КНФ для функций вида (4), построенные стандартным образом [7], для относительно большого числа s (скажем, для $s \geqslant 100$) получаются очень большими. Для нивелирования этого эффекта использованы алгоритмы минимизации булевых схем, реализованные в библиотеке ABC [12]. С этой целью схема S_F, задающая функцию (4), представляется в виде And-Inverter-графа (And-Inverter Graph, AIG) [13], после чего части входных полюсов S_F приписываются значения, соответствующие известным инициализирующим векторам либо блокам открытого текста (для поточных и блочных шифров соответственно). К такой схеме с частично означенным множеством входов (соответствующих открытым входным данным) применяется программа ABC. В итоге строится схема, задающая функцию следующего вида:

$$\tilde{F} : \{0,1\}^n \to \{0,1\}^{sk}. \tag{6}$$

В некоторых случаях схема $S_{\tilde{F}}$ по размеру (по числу вершин) в десятки раз меньше схемы S_F. Для функций вида (6) строятся IBS-атаки в соответствии со сценарием [5].

3. Вычислительные эксперименты

В экспериментах рассматривались ослабленные по числу шагов инициализации варианты известных поточных шифров Trivium [3] и Grain [14] (Grain v1.0), а также блочный низкоресурсный шифр Simon [15], ослабленный по числу раундов.

Для шифра Trivium выбирались значения числа шагов инициализации $M \in \{288, 320, 352, 384, 480, 576\}$. Задача обращения функции вида (2) является сложной уже для $M = 288$. Так, например, IBS-атака на данную функцию [16] даёт IBS B с $|B| = 63$ и оценкой трудоёмкости в секундах $\approx 2^{68}$ (на одном ядре процессора Intel E5-2695).

Для Trivium мы построили несколько вариантов функций вида (3), (4). Для каждой функции выбирались случайно и независимо $s = 100$ векторов IV из $\{0,1\}^{80}$. Для $M = 288$ сначала рассматривалась функция (3) с $k = 1$, однако в этом случае функция (4), хоть и обращается быстро обычным последовательным SAT-решателем Kissat [17], не обладает свойством единственности ключа. Единственность ключа для $M = 288$ была достигнута при параметрах $k = 8$, $s = 100$. Что оказалось весьма неожиданным, в таком варианте функция (4) не является сложной: секретный ключ находится за несколько минут решателем Kissat. Таким образом, даже на этом примере видно, насколько обращение функций вида (4) проще, чем функций вида (2). Обратить при помощи Kissat функции (4) для Trivium-M удалось для $M \in \{288, 320, 352\}$: для Trivium-352 Kissat обратил (4) с параметрами $k = 8$, $s = 100$ за 2 ч 40 мин.

Задача обращения Trivium-384 уже оказалась сложной для последовательного Kissat (не решилась за сутки); для M, начиная с 384, для функций вида (4) строились IBS-атаки. Результаты приведены в табл. 1, тут же дано сравнение построенных атак с атаками для Trivium-M на основе функций вида (2).

Таблица 1

IBS-атаки для Trivium-M

M	Функции (2), параметры: $k \geqslant 80$, $s = 1$			Функции (4), параметры: $k = 10$, $s = 100$		
	Размер КНФ, Мбайт	$\lvert B\rvert$	Оценка трудности атаки, с (одно ядро Intel E5-2695)	Размер КНФ, Мбайт	$\lvert B\rvert$	Оценка трудности атаки, с (одно ядро Intel E5-2695)
288	0,99	49	$2^{59,8}$	0,52	—	$\leqslant 300$
384	1,20	55	$2^{66,1}$	2,71	42	$2^{57,5}$
480	1,41	57	$2^{68,6}$	10,0	56	$2^{71,5}$
576	1,62	58	$2^{69,6}$	24,3	61	$2^{75,5}$

Комментарии к табл. 1. В столбце «Размер КНФ» в случае функции (2) содержится размер формулы, сгенерированной системой Transalg, в случае функции (4) — размер формулы, полученной по AIG, оптимизированному при помощи программы ABC. Можно заметить, что для относительно небольшого числа шагов инициализации задача обращения функций вида (4) проще, чем для функций (2), при том что для функций вида (4) размер кодировок существенно растёт с ростом числа шагов. Для ситуаций, когда кодировка функции (4) по размеру превосходит кодировку функции (2) в 10 раз и более, на работу решателю A^t на формулах для (4) давалось в 10 раз больше времени, чем для (2) (конкретно, 300 и 30 с соответственно).

В табл. 2 приведены результаты аналогичных экспериментов для поточного шифра Grain v1.0, который, как и Trivium, является одним из победителей конкурса eSTREAM. Данный шифр также имеет стадию инициализации, которая в соответствии со спецификацией алгоритма состоит из 160 шагов. Версии Grain v1.0 с числом шагов инициализации, равным M, обозначаются через Grain-v1-M; $M \in \{90, 100, 110, 120\}$.

Комментарии к табл. 2. В случае Grain v1.0 выигрыш по времени при обращении функций (4) в сравнении с (2) существенно больше, чем для Trivium-M. Следует отметить также, что на кодировках функций вида (4) для Grain-v1-M более явным выглядит эффект от AIG-оптимизации, чем для Trivium-M.

Наконец, в последней серии экспериментов рассмотрены атаки аналогичного типа на ослабленный по числу раундов блочный шифр Simon 32/64, конкретно — на первые его 10 раундов. К сожалению, атаки на функции вида (4), задаваемые данным шифром, не продемонстрировали большей эффективности в сравнении с IBS-атаками,

Таблица 2

IBS-атаки для Grain-v1-M

M	Функции (2), параметры: $k \geqslant 80$, $s = 1$			Функции (4), параметры: $k = 10$, $s = 100$		
	Размер КНФ, Мбайт	$\lvert B\rvert$	Оценка трудности атаки, с (одно ядро Intel E5-2695)	Размер КНФ, Мбайт	$\lvert B\rvert$	Оценка трудности атаки, с (одно ядро Intel E5-2695)
90	1,56	52	$2^{67,5}$	4,23	29	$2^{42,7}$
100	1,68	49	$2^{65,5}$	7,34	31	$2^{44,3}$
110	1,81	52	$2^{66,9}$	11,3	41	$2^{56,5}$
120	1,94	53	$2^{69,5}$	15,0	44	$2^{60,5}$

построенными для функций вида (2). Лучшая атака для функции вида (2) в случае Simon 32/64 даёт IBS из 37 переменных и оценку трудоёмкости $2^{47,6}$ секунд. В то же время для функции вида (4) с параметрами $k = 1$ и $s = 100$ имеем IBS B с $|B| = 45$, трудоёмкость $2^{59,5}$. Для работы с функциями (4) решателю A^t выделялось в 10 раз больше времени, чем для работы с функциями (2) (300 с против 30 с), поскольку кодировки (4) для Simon 32/64 превосходят кодировки (2) по объёму более чем в 10 раз.

Все вычисления проводились на кластере «Академик В. М. Матросов» Иркутского суперкомпьютерного центра [18].

Заключение

Описан новый класс алгебраических атак, базирующийся на задаче обращения специальных функций, использовавшихся ранее в кубических атаках. Такая функция имеет выход, длина которого существенно меньше длины секретного ключа, и соответственно прообраз такого выхода в общем случае не единственный. Предлагается специальная техника, которую можно условно назвать «клонированием» функций данного типа: рассматриваются несколько функций, построенных для общего секретного ключа и различных открытых входных данных (фрагментов ключевого потока или криптограмм в случае поточных и блочных шифров соответственно). Пожалуй, основной новизной предлагаемого подхода является представление таких клонированных функций в виде And-Inverter-графов с последующим применением к ним инструментов AIG-оптимизации. В вычислительных экспериментах на примерах ослабленных по числу шагов инициализации низкоресурсных поточных шифров Trivium и Grain v1.0 продемонстрировано, что алгебраические атаки на специальные функции могут быть существенно более эффективными, чем атаки на стандартные функции, задаваемые этими криптографическими алгоритмами. В ближайших планах расширить класс описанных атак за счёт сценариев, использующих выбранные открытые входные данные (chosen plaintext).

ЛИТЕРАТУРА

1. *Fischer S., Khazaei S., and Meier W.* Chosen IV statistical analysis for key recovery attacks on stream ciphers // LNCS. 2008. V. 5023. P. 236–245.
2. *Dinur I. and Shamir A* Cube attacks on tweakable black box polynomials // LNCS. 2009. V. 5479. P. 278–299.
3. *De Canniere C.* Trivium: a stream cipher construction inspired by block cipher design principles // LNCS. 2006. V. 4176. P. 171–186.
4. *Bard G.* Algebraic Cryptanalysis. Springer, 2009.
5. *Semenov A., Zaikin O., Otpuschennikov I., et al.* On cryptographic attacks using backdoors for SAT // Proc. AAAI. Palo Alto, USA, 2018. P. 6641–6648.

6. *Otpuschennikov I., Semenov A., Gribanova I., et al.* Encoding cryptographic functions to SAT using Transalg system // Proc. ECAI. Hague, Netherlands, 2016. P. 1594–1595.
7. *Semenov A., Otpuschennikov I., Gribanova I., et al.* Translation of algorithmic descriptions of discrete functions to SAT with applications to cryptanalysis problems // Logical Methods Computer Sci. 2020. V. 16. Iss. 1. P. 29:1–29:42.
8. *Цейтин Г. С.* О сложности вывода в исчислении высказываний // Записки научных семинаров ЛОМИ. 1968. Т. 8. С. 234–259.
9. *Яблонский С. В.* Введение в дискретную математику. М.: Наука, 1986.
10. *Чень Ч., Ли Р.* Математическая логика и автоматическое доказательство теорем. М.: Наука, 1983.
11. *Williams R., Gomes C., and Selman B.* Backdoors to typical case complexity // Proc. IJCAI'03. Acapulco, Mexico, 2003. P. 1173–1178.
12. *Bryton R. and Mishchenko A.* ABC: An academic industrial-strength verification tool // LNCS. 2010. V. 6174. P. 24–40.
13. *Kuehlmann A. Paruthi V., Krohm F., and Ganai M* Robust Boolean reasoning for equivalence checking and functional property verification // IEEE Trans. Computer-Aided Des. Integr. Circuits Systems. 2002. V. 21. No. 12. P. 1377–1394.
14. *Hell M., Johansson T., and Meier W.* Grain: a stream cipher for constrained environments // Intern. J. Wireless Mobile Computing. 2007. V. 2. Iss. 1. P. 86–93.
15. *Beaulieu R., Shors D., Smith J., et al.* The Simon and Speck lightweight block ciphers // 52nd Ann. Design Automation Conf. San Francisco, USA, 2015. P. 175:1–175:6.
16. *Semenov A., Antonov K., Otpuschennikov I., and Pavlenko A.* Using linearizing sets to solve multivariate quadratic equations in algebraic cryptanalysis // IEEE Access. 2023. V. 11. P. 120319–120333.
17. *Biere A., Fazekas K., Fleury M., and Heisinger M.* CaDiCaL, Kissat, Paracooba, Plingeling and Treengeling entering the SAT Competition 2020 // Proc. SAT Competition. Helsinki, 2020. P. 50–53.
18. Иркутский суперкомпьютерный центр. `https://hpc.icc.ru/hardware/index.html`.

УДК 519.7 DOI 10.17223/2226308X/17/15

О СТОЙКОСТИ НЕКОТОРЫХ АЛГОРИТМОВ НАД ГРУППОЙ ТОЧЕК ЭЛЛИПТИЧЕСКИХ КРИВЫХ

А. О. Бахарев, К. Д. Царегородцев

Приводятся результаты анализа схемы VKO и комбинированной схемы VKO+подпись в моделях обобщённой группы и биективного случайного оракула. Получена верхняя оценка сложности задачи различения выхода схемы VKO от случайной равновероятной строки (в эвристике обобщенной группы), а также показано, что возможность получения подписи сообщений по алгоритму genGOST не даёт никакой дополнительной информации противнику в этой задаче (в эвристике биективного случайного оракула).

Ключевые слова: *доказуемая стойкость, VKO, электронная подпись.*

Введение

В ходе изучения различных криптографических протоколов возникают вопросы, связанные со стойкостью алгоритмов, в основе которых лежат вычисления в различных группах (например, в группе точек эллиптической кривой). Существует несколько возможных подходов к анализу подобных задач.

Одним из подходов является поиск эффективных алгоритмов дискретного логарифмирования в общем случае [1] и в конкретных группах [2, 3]. Такой подход позволяет получать нижние оценки стойкости различных механизмов. Другим возможным подходом является сведение одних «неэлементарных» задач к другим, более «элементарным» [4, разд. 5.2]. При этом остаётся вопрос об оценке сложности решения «элементарных» задач (таких, например, как распознавательная задача Диффи — Хеллмана). Третий способ — использование идеализаций при изучении сложности различных задач, например эвристики случайного оракула [5], биективного случайного оракула [6, 7], обобщённой группы [8, 9]. Последний подход позволяет получать верхние оценки стойкости (в классе рассматриваемых методов криптоанализа).

В настоящей работе рассматриваются несколько вопросов, связанных с задачами в группе точек эллиптической кривой: 1) анализ безопасности схемы выработки ключей VKO [10] в модели обобщённой группы; 2) вопросы безопасности при одновременном использовании секретного ключа как в схеме VKO, так и в схеме электронной подписи [11] (joint key security [12]). Получена верхняя оценка сложности задачи различения выхода схемы VKO от случайных равновероятных строк (в модели обобщённой группы), а также показано, что возможность получения подписи сообщений на секретном ключе согласно схеме подписи genGOST [7] не даёт никакой дополнительной информации противнику (в эвристике биективного случайного оракула). Отметим также работу [13], в которой получены аналогичные результаты для схемы инкапсуляции ключа (KEM) совместно с подписью genGOST. Несколько упрощая, можно говорить, что доказательство стойкости, полученное в [13], опирается на стойкость режима аутентифицированного шифрования и сложность решения задачи ODH в группе точек эллиптической кривой, в то время как в настоящей работе рассматривается эвристика обобщённнной группы, которая позволяет провести дальнейший анализ задачи ODH, оценив её сложность относительно некоторго класса алгоритмов. Таким образом, представленное доказательство относится к несколько иному механизму (схеме выработки ключей) и опирается на псевдослучайность хеш-функции.

1. Предварительные сведения

Для $q \in \mathbb{N}$, $q > 1$, через $\mathbb{Z}_q$ обозначим кольцо целых чисел с операциями сложения и умножения по модулю q, $\mathbb{Z}_q^* = \mathbb{Z}_q \backslash \{0\}$. Через $x \leftarrow y$ обозначим присвоение переменной x значения y. Если $\mathcal{O}$ — вероятностный алгоритм, то под $x \xleftarrow{\$} \mathcal{O}$ мы понимаем операцию запуска $\mathcal{O}$ с присвоением результата работы $\mathcal{O}$ переменной x. Если S — конечное непустое множество, то под $x \xleftarrow{\mathcal{U}} S$ мы понимаем операцию присвоения переменной x значения из S, выбранному случайно равновероятно из S. Пустой словарь обозначается как $[\,]$. Символ $\perp$ означает либо символ ошибки (например, сбой алгоритма), либо специальный символ, означающий отсутствие элемента в словаре по заданному индексу. Нуль и нейтральный элемент аддитивной группы обозначаются через 0.

Под противником будем подразумевать некоторый вероятностный алгоритм. Будем рассматривать противников в фиксированной модели вычислений (например, машины Тьюринга); вычислительные ресурсы противника — величина, ограничивающая сумму времени работы противника (например, число тактов вычислений) и размера его программы. Запись $\mathcal{A}^{\mathcal{O}}$ означает противника $\mathcal{A}$, имеющего доступ к оракулу $\mathcal{O}$ [14, разд. 6.3]; $\mathsf{P}[\mathcal{A} \to 1]$ — вероятность того, что алгоритм $\mathcal{A}$ выдаст 1. Через $\mathbf{Exp}_{\mathcal{K}}^{\mathbf{M}}$ будем

обозначать эксперимент — вероятностный алгоритм, моделирующий для противника условия (модель) $\mathbf{M}$, в рамках которых он взаимодействует с криптосистемой $\mathcal{K}$.

Определение 1. Комбинированной схемой выработки общего ключа и подписи будем называть четвёрку (вероятностных) алгоритмов $\mathbf{CS} = (\mathsf{PairGen}, \mathsf{Comb}, \mathsf{Sign}, \mathsf{Verify})$:

- $(sk, pk) \xleftarrow{\$} \mathbf{CS}.\mathsf{PairGen}()$ — алгоритм генерации ключевой пары: возвращает случайно выбранную ключевую пару (sk, pk);
- $K \leftarrow \mathbf{CS}.\mathsf{Comb}(sk, epk)$ — алгоритм выработки ключа Comb: на основе двух ключей — закрытого sk и открытого epk — вырабатывает ключ K;
- $\sigma \xleftarrow{\$} \mathbf{CS}.\mathsf{Sign}(sk, m)$ — алгоритм формирования подписи: принимает на вход ключ подписи sk и сообщение m и возвращает подпись σ для сообщения m или ошибку $\perp$;
- $b \leftarrow \mathbf{CS}.\mathsf{Verify}(pk, m, \sigma)$ — алгоритм проверки подписи: принимает на вход открытый ключ pk, сообщение m и подпись σ и возвращает 1, если подпись верна, и 0 иначе.

При этом должны выполняться стандартные требования корректности генерации ключей и корректности подписи:

$$(sk, pk) \xleftarrow{\$} \mathbf{CS}.\mathsf{PairGen}, \quad (esk, epk) \xleftarrow{\$} \mathbf{CS}.\mathsf{PairGen} \Rightarrow$$
$$\Rightarrow \mathbf{CS}.\mathsf{Comb}(sk, epk) = \mathbf{CS}.\mathsf{Comb}(esk, pk), \quad \mathbf{CS}.\mathsf{Verify}(pk, m, \mathbf{CS}.\mathsf{Sign}(sk, m)) = 1.$$

Пару алгоритмов $\mathbf{KE} = (\mathbf{CS}.\mathsf{PairGen}, \mathbf{CS}.\mathsf{Comb})$ будем называть схемой выработки ключей, а тройку $\mathbf{SS} = (\mathbf{CS}.\mathsf{PairGen}, \mathbf{CS}.\mathsf{Sign}, \mathbf{CS}.\mathsf{Verify})$ — схемой подписи.

Рассмотрим конкретный пример комбинированной схемы $\mathbf{CS} = \mathbf{VKOST}$ (схема VKO+подпись genGOST). Пусть G — циклическая подгруппа простого порядка q группы точек эллиптической кривой $G = \langle P \rangle$ (конкретные параметры эллиптической кривой, группы точек и её подгруппы могут быть заданы, согласно [4, разд. 3.7]). Положим $S_q \subseteq \{0,1\}^{\lceil \log |G| \rceil}$ — множество кодировок элементов группы G; $\chi\colon G \to S_q$ — функция кодировки. Зададим множество открытых ключей схемы $\mathbf{VKOST}$ как $G^* = G \setminus \{0\}$, секретных ключей — $\mathbb{Z}_q^*$. Положим $D = \left(\mathbb{Z}_q^*\right)^3$ и зададим число $L \in \mathbb{N}$. Пусть Hash_1, Hash_2 — хеш-функции вида $\mathsf{Hash}_1\colon S_q \to \{0,1\}^L$, $\mathsf{Hash}_2\colon \{0,1\}^* \to \mathbb{Z}_q$. Определим функцию преобразования $f = \psi \circ \Pi \circ \varphi : G^* \to \mathbb{Z}_q$ через её компоненты

$$G^* \xrightarrow{\varphi} \{0,1\}^L \xrightarrow{\Pi} [0, 2^L - 1] \xrightarrow{\psi} \mathbb{Z}_q,$$

где φ и ψ — эффективно вычислимые функции; Π — эффективно вычислимая биекция; φ — полуинъекция, т. е. функция φ либо полностью инъективна, либо является 2-в-1-функцией, и если $\varphi(x) = \varphi(y)$, $x, y \in G^*$, то $y \in \{x, -x\}$.

Алгоритм $\mathbf{VKOST}.\mathsf{PairGen}$ генерирует закрытый ключ $sk \xleftarrow{\mathcal{U}} \mathbb{Z}_q^*$ и соответствующий ему открытый ключ $pk \leftarrow sk \cdot P$. Алгоритм $\mathbf{VKOST}.\mathsf{Comb}(sk, epk)$ возвращает значение $\mathsf{Hash}_1\left(\chi(\alpha \cdot sk \cdot epk)\right)$, где $\alpha \in \mathbb{Z}_q^*$ — некоторый параметр (кофактор), который зависит только от подгруппы G (в настоящей работе мы рассматриваем схему VKO без параметра UKM). Алгоритмы $\mathbf{VKOST}.\mathsf{Sign}$ и $\mathbf{VKOST}.\mathsf{Verify}$ определены в соответствии со схемой подписи genGOST [7] и описаны в псевдокоде на рис. 1.

Определим схему выработки ключей $\mathrm{VKO} = (\mathbf{VKOST}.\mathsf{PairGen}, \mathbf{VKOST}.\mathsf{Comb})$ и схему подписи $\mathrm{genGOST} = (\mathbf{VKOST}.\mathsf{PairGen}, \mathbf{VKOST}.\mathsf{Sign}, \mathbf{VKOST}.\mathsf{Verify})$.

VKOST.PairGen

$sk \xleftarrow{\mathcal{U}} \mathbb{Z}_q^*$
$pk \leftarrow sk \cdot P$
return (sk, pk)

VKOST.Comb(sk, pk)

$K \leftarrow \mathsf{Hash}_1(\chi(\alpha \cdot sk \cdot pk))$
return K

VKOST.Sign(sk, m)

$r \xleftarrow{\mathcal{U}} \mathbb{Z}_q$
$R \leftarrow r \cdot P$
if $(R = 0)$
  return $\perp$
fi
$t \leftarrow f(R)$
$h \leftarrow \mathsf{Hash}_2(m)$
$s \leftarrow h \cdot r + t \cdot sk$
if $(s, h, t) \notin D$
  return $\perp$
fi
return (s, t)

VKOST.Verify$(pk, m, (s, t))$

$h \leftarrow \mathsf{Hash}_2(m)$
if $(s, h, t) \notin D$
  return 0
fi
$R' \leftarrow (s \cdot h^{-1})P - (t \cdot h^{-1})pk$
if $(R' = 0)$
  return 0
fi
$t' \leftarrow f(R')$
if $(t \neq t')$
  return 0
fi
return 1

Рис. 1. Комбинированная схема **VKOST**

2. Модели безопасности

2.1. Модель обобщённой группы

Модель обобщённой группы введена В. И. Нечаевым в [8], изучалась и обобщалась во многих других работах, например [9]. Суть идеализации состоит в сокрытии от противника структуры группы G порядка q с помощью биективной функции кодирования $\tau\colon G \to S_q$, где $S_q \subseteq \{0,1\}^{\lceil \log |G| \rceil}$. Противнику в рамках рассматриваемой идеализации элементы группы доступны только посредством их меток $\tau(x)$; для умножения двух элементов группы либо обращения элемента группы он должен обратиться к групповому оракулу $\mathcal{O}_{\text{grp}}$. В подобной модели противник не может использовать какую-либо алгебраическую «структуру» группы, но вынужден применять только те алгоритмы, которые работают с любой абстрактной группой.

Определение 2. Обобщённый групповой алгоритм A — это (вероятностный) алгоритм, который получает на вход кортеж из k закодированных элементов группы $(\tau(x_1), \ldots, \tau(x_k))$, $x_i \in G$, $1 \leqslant i \leqslant k$. Алгоритм A может обращаться к групповому оракулу для выполнения вычислительных операций из множества S, проверки отношений из множества R и генерации нового элемента группы.

В настоящей работе используется модель обобщённой группы для $G = \langle P \rangle$ (подгруппа группы точек эллиптической кривой), $S = \{\pm\}$, $R = \varnothing$. Отметим, что в этой модели отношение равенства двух элементов может быть проверено обобщённым групповым алгоритмом без обращения к групповому оракулу, так как функция кодирования τ является биекцией и $x_1 \neq x_2$ эквивалентно $\tau(x_1) \neq \tau(x_2)$.

2.2. Модель биективного случайного оракула

Модель биективного случайного оракула введена в [6] для изучения стойкости схем подписи типа ElGamal. В [6] функция f из схемы подписи представляется в виде композиции трёх независимых отображений $f = \psi \circ \Pi \circ \varphi$, где Π — биекция. Основная идея подобного представления состоит в том, что свойства функции f на области определе-

ния и области значений отражаются в функциях φ и ψ соответственно, а функция Π характеризует нарушение алгебраической связи между областью определения и областью значений функции. В рамках идеализации биекция Π заменяется на *биективный случайный оракул* (общедоступная случайно выбираемая подстановка).

2.3. Модель безопасности PRH для хеш-функции

Рассмотрим модель PRH (PseudoRandom Hashing) для задачи различения значения функции F на случайно выбранном входе от случайной строки.

Определение 3. Определим преимущество противника $\mathcal{A}$ в модели PRH для функции $F\colon X \to \{0,1\}^L$ как разность

$$\mathbf{Adv}_F^{\mathsf{PRH}}(\mathcal{A}) = \mathsf{P}[\mathbf{Exp}_F^{\mathsf{PRH\text{-}1}}(\mathcal{A}) \to 1] - \mathsf{P}[\mathbf{Exp}_F^{\mathsf{PRH\text{-}0}}(\mathcal{A}) \to 1],$$

где эксперимент $\mathbf{Exp}_F^{\mathsf{PRH}\text{-}b}$, $b \in \{0,1\}$, определён следующим образом. В начале эксперимента выбирается $x \xleftarrow{\mathcal{U}} X$ и задаётся $res \leftarrow F(x)$. Если $b = 0$, то значение res переопределяется как $res \xleftarrow{\mathcal{U}} \{0,1\}^L$. Далее res поступает на вход противника $\mathcal{A}$. Значение, полученное от противника $\mathcal{A}$, является выходом эксперимента.

Определение 4. Обозначим $\mathbf{InSec}_F^{\mathsf{PRH}}(t)$ максимум среди преимуществ вида $\mathbf{Adv}_F^{\mathsf{PRH}}(\mathcal{A})$, где максимум берётся по всем противникам $\mathcal{A}$ с ограничением t на вычислительные ресурсы.

При $|X| > 2^L$ min-энтропия равномерного распределения на X превышает L, т. е. нам всего лишь необходимо «извлечь» равномерно распределённую случайную величину из источника с большей энтропией. Если функция F моделируется как случайный оракул, то $\mathbf{InSec}_F^{\mathsf{PRH}}(t) = 0$.

2.4. Модель безопасности mODH′ для схемы CS

Рассмотрим модель mODH′ (Multiple query Oracle Diffie — Hellman) для изучения безопасности комбинированной схемы **CS**. В модели mODH′ противник $\mathcal{A}$ имеет доступ к трём оракулам:

— $\mathcal{O}^b_{\mathrm{kgen}}$ генерирует либо ключи, вычисленные с помощью алгоритма **CS** (при $b = 1$), либо случайные равновероятные ключи заданной длины (при $b = 0$), с некоторыми ограничениями, исключающими тривиальные атаки (см. псевдокод на рис. 2);
— $\mathcal{O}_{\mathrm{comb}}(epk)$ генерирует ключ с помощью алгоритма **CS**.Comb, используя предоставленный ему на вход открытый ключ epk;
— $\mathcal{O}_{\mathrm{sig}}(m)$ возвращает подпись **CS**.Sign(sk, m) сообщения m на закрытом ключе sk.

Задачей противника является корректное определение бита b, зафиксированного внутри оракула $\mathcal{O}^b_{\mathrm{kgen}}$. Невозможность противника $\mathcal{A}$ с высокой вероятностью правильно определить бит b свидетельствует в пользу того, что ключи, выработанные с помощью схемы **CS**, неотличимы от случайных.

Определение 5. Определим преимущество противника $\mathcal{A}$ в модели mODH′ для схемы выработки общего ключа и подписи **CS** как разность

$$\mathbf{Adv}_{\mathbf{CS}}^{\mathsf{mODH'}}(\mathcal{A}) = \mathsf{P}[\mathbf{Exp}_{\mathbf{CS}}^{\mathsf{mODH'}\text{-}1}(\mathcal{A}) \to 1] - \mathsf{P}[\mathbf{Exp}_{\mathbf{CS}}^{\mathsf{mODH'}\text{-}0}(\mathcal{A}) \to 1],$$

псевдокод эксперимента $\mathbf{Exp}_{\mathbf{CS}}^{\mathsf{mODH'}\text{-}b}$, $b \in \{0,1\}$, приведён на рис. 2.

Определение 6. Обозначим через $\mathbf{InSec}_{\mathbf{CS}}^{\mathsf{mODH'}}(t, q_{\mathrm{gen}}, q_{\mathrm{com}}, q_{\mathrm{sign}})$ максимум среди преимуществ вида $\mathbf{Adv}_{\mathbf{CS}}^{\mathsf{mODH'}}(\mathcal{A})$, где максимум берётся по всем противникам $\mathcal{A}$, имеющим ограничение t на вычислительные ресурсы и делающим не более q_{gen} (q_{com}, q_{sign}) запросов к оракулу $\mathcal{O}^b_{\mathrm{kgen}}$ (оракулу $\mathcal{O}_{\mathrm{comb}}$ и оракулу $\mathcal{O}_{\mathrm{sig}}$ соответственно).

$\mathbf{Exp}^{\mathsf{mODH}'\text{-}b}_{\mathbf{KE},\mathsf{Sign}}(\mathcal{A})$

$(sk, pk) \xleftarrow{\$} \mathbf{CS}.\mathsf{PairGen}$
$Keys \leftarrow [\,]$
$b' \xleftarrow{\$} \mathcal{A}^{\mathcal{O}^b_{\mathrm{kgen}},\mathcal{O}_{\mathrm{comb}},\mathcal{O}_{\mathrm{sig}}}(pk)$
return b'

$\mathcal{O}_{\mathrm{sig}}(m)$

$\sigma \xleftarrow{\$} \mathbf{CS}.\mathsf{Sign}(sk, m)$
return σ

$\mathcal{O}^b_{\mathrm{kgen}}$

$(esk, epk) \xleftarrow{\$} \mathbf{CS}.\mathsf{PairGen}$
if $Keys[epk] = \perp$
  $K \leftarrow \mathbf{CS}.\mathsf{Comb}(sk, epk)$
  if $(b = 0)$
    $K \xleftarrow{\mathcal{U}} \{0,1\}^{|K|}$
  fi
  $Keys[epk] \leftarrow K$
fi
return $(epk, Keys[epk])$

$\mathcal{O}_{\mathrm{comb}}(epk)$

if $Keys[epk] = \perp$
  return $\mathbf{CS}.\mathsf{Comb}(sk, epk)$
fi
return $Keys[epk]$

Рис. 2. Псевдокод эксперимента mODH' для схемы **CS**

Для схемы выработки ключей $\mathbf{KE} = (\mathbf{CS}.\mathsf{PairGen}, \mathbf{CS}.\mathsf{Comb})$ мы можем ввести также модель безопасности mODH, в которой противник не имеет доступа к оракулу $\mathcal{O}_{\mathrm{sig}}$, а его задача аналогична задаче в модели mODH' (отличение выработанных схемой ключей от случайных). Преимущество противника в модели mODH задаётся как

$$\mathbf{InSec}^{\mathsf{mODH}}_{\mathbf{KE}}(t, q_{\mathrm{gen}}, q_{\mathrm{com}}) = \mathbf{InSec}^{\mathsf{mODH}'}_{\mathbf{CS}}(t, q_{\mathrm{gen}}, q_{\mathrm{com}}, 0)\,.$$

2.5. Идеализированные модели безопасности

Для изучения сложности тех или иных задач часто используются всевозможные идеализации (эвристики) исходных моделей безопасности, которые (за счёт некоторого упрощения ситуации) поддаются дальнейшему анализу. Применим этот подход и рассмотрим идеализированные версии моделей.

Модель g-mODH

Рассмотрим модель mODH для схемы VKO в идеализации обобщённой группы. Исходная функция кодирования элементов χ заменяется на случайную кодировку τ, согласно эвристике обобщённой группы (см. п. 2.1).

Определение 7. Преимуществом противника $\mathcal{A}$ в модели $\mathsf{g\text{-}mODH}$ называется величина

$$\mathbf{Adv}^{\mathsf{g\text{-}mODH}}_{\mathrm{VKO}}(\mathcal{A}) = \mathsf{P}[\mathbf{Exp}^{\mathsf{g\text{-}mODH\text{-}1}}_{\mathrm{VKO}}(\mathcal{A}) \to 1] - \mathsf{P}[\mathbf{Exp}^{\mathsf{g\text{-}mODH\text{-}0}}_{\mathrm{VKO}}(\mathcal{A}) \to 1],$$

псевдокод эксперимента $\mathbf{Exp}^{\mathsf{g\text{-}mODH}\text{-}b}_{\mathrm{VKO}}$, $b \in \{0,1\}$, приведён на рис. 3.

Определение 8. Обозначим через $\mathbf{InSec}^{\mathsf{g\text{-}mODH}}_{\mathrm{VKO}}(t, q_{\mathrm{gen}}, q_{\mathrm{com}}, q_{\mathrm{group}})$ максимум среди преимуществ вида $\mathbf{Adv}^{\mathsf{g\text{-}mODH}}_{\mathrm{VKO}}(\mathcal{A})$, где максимум берётся по всем противникам $\mathcal{A}$, имеющим ограничение t на вычислительные ресурсы и делающим не более q_{gen} (q_{com}, q_{group}) запросов к оракулу $\mathcal{O}^b_{\mathrm{kgen}}$ (оракулу $\mathcal{O}_{\mathrm{comb}}$, оракулу $\mathcal{O}_{\mathrm{grp}}$).

Теорема 1. Выполнено следующее неравенство:

$$\mathbf{InSec}^{\mathsf{g\text{-}mODH}}_{\mathrm{VKO}}(t, 1, q_{\mathrm{com}}, q_{\mathrm{group}}) \leqslant \frac{2(q_{\mathrm{group}} + q_{\mathrm{com}})^2}{q} + \mathbf{InSec}^{\mathsf{PRH}}_{\mathsf{Hash}_1}(t).$$

$\mathbf{Exp}_{\text{VKO}}^{\text{g-mODH-}b}(\mathcal{A})$

$sk \xleftarrow{\mathcal{U}} \mathbb{Z}_q^*$

$pk \leftarrow sk \cdot P$

$\tau \xleftarrow{\mathcal{U}} \{\pi\colon G \to S_q, \pi \text{ инъективно}\}$

$Keys \leftarrow [\,]$

$b' \xleftarrow{\$} \mathcal{A}^{\mathcal{O}^b_{\text{kgen}}, \mathcal{O}_{\text{comb}}, \mathcal{O}_{\text{grp}}}(\tau(P), \tau(pk))$

return b'

$\mathcal{O}^{\pm}_{\text{grp}}(\tau(x), \tau(y))$

return $\tau(x \pm y)$

$\mathcal{O}^{sample}_{\text{grp}}(\tau(M))$

$el \xleftarrow{\mathcal{U}} G \backslash M \quad /\!/\ M \subseteq G$

return $\tau(el)$

$\mathcal{O}_{\text{comb}}(\tau(epk))$

if $Keys[epk] = \perp$

$K \leftarrow \mathsf{Hash}_1(\tau(\alpha \cdot sk \cdot epk))$

return K

fi

return $Keys[epk]$

$\mathcal{O}^b_{\text{kgen}}$

$esk \xleftarrow{\mathcal{U}} \mathbb{Z}_q^*$

$epk \leftarrow esk \cdot P$

if $Keys[epk] = \perp$

$K \leftarrow \mathsf{Hash}_1(\tau(\alpha \cdot sk \cdot epk))$

if $(b = 0)$

$K \xleftarrow{\mathcal{U}} \{0,1\}^{|K|}$

fi

$Keys[epk] \leftarrow K$

fi

return $(\tau(epk), Keys[epk])$

Рис. 3. Псевдокод эксперимента g-mODH для схемы VKO

Заметим, что этот результат является неулучшаемым в том смысле, что существуют обобщённые алгоритмы дискретного логарифмирования в группе точек эллиптической кривой, которые требуют порядка $\mathcal{O}(\sqrt{q})$ операций. Интерпретация результата может быть следующей: любой обобщённый (не использующий специфику конкретной группы) алгоритм, который решает задачу различения ключей VKO от случайных равновероятных ключей, должен затратить порядка $\mathcal{O}(\sqrt{q})$ времени (либо атаковать хеш-функцию, используемую в схеме).

Модель mODH′-BRO

Определим модель mODH′-BRO как модель mODH′, в которой в разложении $f = \psi \circ \Pi \circ \varphi$ биекция Π моделируется как общедоступный случайный биективный оракул Π, выбранный в начале эксперимента. Определим преимущество противника $\mathcal{A}$ в модели mODH′-BRO для схемы выработки общего ключа и подписи как разность

$$\mathbf{Adv}_{\mathbf{CS}}^{\text{mODH′-BRO}}(\mathcal{A}) = \mathsf{P}[\mathbf{Exp}_{\mathbf{CS}}^{\text{mODH′-BRO-1}}(\mathcal{A}) \to 1] - \mathsf{P}[\mathbf{Exp}_{\mathbf{CS}}^{\text{mODH′-BRO-0}}(\mathcal{A}) \to 1].$$

Обозначим через $\mathbf{InSec}_{\mathbf{CS}}^{\text{mODH′-BRO}}(t, q_{\text{gen}}, q_{\text{com}}, q_{\text{sign}}, q_{\Pi})$ максимум среди преимуществ вида $\mathbf{Adv}_{\mathbf{CS}}^{\text{mODH′-BRO}}(\mathcal{A})$, где максимум берётся по всем противникам $\mathcal{A}$, имеющим ограничение t на вычислительные ресурсы и делающим не более q_{gen} (q_{com}, q_{sign}, q_{Π}) запросов к оракулу $\mathcal{O}^b_{\text{kgen}}$ (оракулу $\mathcal{O}_{\text{comb}}$, оракулу $\mathcal{O}_{\text{sig}}$ и оракулу Π соответственно).

Теорема 2. Для комбинированной схемы выработки общего ключа и подписи **VKOST** выполнено следующее неравенство:

$$\mathbf{InSec}_{\mathbf{VKOST}}^{\text{mODH′-BRO}}(t, q_{\text{gen}}, q_{\text{com}}, q_{\text{sign}}, q_{\Pi}) \leqslant$$
$$\leqslant \mathbf{InSec}_{\text{VKO}}^{\text{mODH}}(t + \mathcal{O}(q_{\text{sign}} + q_{\Pi}), q_{\text{gen}}, q_{\text{com}}) + \frac{3(q_{\text{sign}} + q_{\Pi})q_{\text{sign}}}{(q-1)/2 - q_{\Pi}}.$$

При условии $q \gg q_{\text{sign}}, q_{\Pi}$ интерпретация результата может быть следующей: если противник, решающий задачу различения ключей VKO от случайных равновероятных в присутствии оракула подписи genGOST достигает существенно большего преимущества, чем при его отсутствии, то в рассматриваемом противнике неявно существенным

образом используется алгебраическая связь между элементами группы G и элементами $\mathbb{Z}_q$, что, возможно, может быть использовано для нахождения более эффективных алгоритмов дискретного логарифмирования для группы G.

ЛИТЕРАТУРА

1. *Панкратова И. А.* Теоретико-числовые методы криптографии: Учеб. пособие. Томск: Томский государственный университет, 2009. 120 с.
2. *Adleman L.* A subexponential algorithm for the discrete logarithm problem with applications to cryptography // Proc. 20th Ann. Symp. Found. Comput. Sci. San Juan, PR, USA, 1979. P. 55–60.
3. *Menezes A., Vanstone S., and Okamoto T.* Reducing elliptic curve logarithms to logarithms in a finite field // Proc. 23th Ann. ACM Symp. Theory Comput. New Orleans, Louisiana, USA, 1991. P. 80–89.
4. *Алексеев Е. К., Ошкин И. Б., Попов В. О., Смышляев С. В.* О криптографических свойствах алгоритмов, сопутствующих применению стандартов ГОСТ Р 34.11-2012 и ГОСТ Р 34.10-2012 // Матем. вопр. криптогр. 2016. № 7(1). С. 5–38.
5. *Bellare M. and Rogaway P.* Random oracles are practical: A paradigm for designing efficient protocols // Proc. CCS'93. Fairfax, Virginia, USA, 1993. P. 62–73.
6. *Fersch M., Kiltz E., and Poettering B.* On the provable security of (EC)DSA signatures // Proc. CCS'16. Vienna, Austria, 2016. P. 1651–1662.
7. *Fersch M.* The Provable Security of ElGamal-type Signature Schemes. Doctoral dissertation, Ruhr University Bochum, 2018.
8. *Нечаев В. И.* К вопросу о сложности детерминированного алгоритма для дискретного логарифма // Матем. заметки. 1994. № 55(2). С. 91–101.
9. *Shoup V.* Lower bounds for discrete logarithms and related problems // LNCS. 1997. V. 1233. P. 256–266.
10. Рекомендации по стандартизации Р 50.1.113-2016 Информационная технология. Криптографическая защита информации. Криптографические алгоритмы, сопутствующие применению алгоритмов электронной цифровой подписи и функции хэширования. М.: Стандартинформ, 2016.
11. Межгосударственный стандарт ГОСТ 34.10.2018. Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи. М.: Стандартинформ, 2018.
12. *Paterson K. G., Schuldt J., Stam M., and Thomson S.* On the joint security of encryption and signature, revisited // LNCS. 2011. V. 7073. P. 161–178.
13. *Babueva A. A, Bozhko A. A., and Kyazhin S. N.* Joint security of encryption and signature in RuCMS: Two keys are better, but one is also fine // Proc. CTCrypt'24. 2024.
14. *Sipser M.* Introduction to the Theory of Computation. 3rd ed. Cengage Learning, 2012.

УДК 004.421.5 DOI 10.17223/2226308X/17/16

ИССЛЕДОВАНИЕ КОНСТРУКЦИЙ ПРЕОБРАЗОВАНИЯ СИГНАЛА С ФДСЧ, ОСНОВАННОГО НА КОЛЬЦЕВЫХ ОСЦИЛЛЯТОРАХ

Д. А. Бобровский, Д. А. Шиликов

Исследуются схемы для обработки сигнала, получаемого с кольцевых осцилляторов; преобразованные последовательности тестируются на свойства случайности. Предложено пять вариантов преобразования выходного сигнала. В качестве инструментов преобразования использованы комбинации метода фон Неймана и

операции XOR. Тестирование полученных последовательностей выполнено с помощью пакета тестов NIST STS. Последовательность, полученная после преобразования № 5, показала наилучший результат по итогам тестирования и была сравнена с последовательностью, зашифрованной алгоритмом AES в режиме счётчика. Сравнение показало, что количество успешно пройденных тестов преобразованной последовательности выше, чем у последовательности, зашифрованной алгоритмом AES.

Ключевые слова: *физический датчик случайных чисел, семплирование, кольцевой осциллятор, методы преобразования последовательностей.*

Неотъемлемой частью криптографической защиты информации являются случайные последовательности, используемые с целью выработки ключей и другой псевдослучайной информации. Это говорит о том, что физические датчики случайных чисел (ФДСЧ), как один из способов генерации псевдослучайных последовательностей, играют большую роль в криптографической защите информации. От качества сгенерированных последовательностей напрямую зависит криптостойкость шифра.

Одним из видов ФДСЧ является генератор на основе кольцевых осцилляторов [1]. Исследования в области данного вида ФДСЧ получили широкий рост в начале 2000-х годов [2, 3] и продолжаются в наши дни. Изучены конструктивные особенности генератора [4], уровни энергии [5], влияние посторонних физических процессов на качество выходной последовательности [6]. По причине высокой скорости генерации последовательностей данная область перспективна и обладает большими возможностями для дальнейшего исследования. Одним из таких направлений изучения являются преобразования выходного сигнала с кольцевых осцилляторов [7].

В данной работе в качестве исходных использовались данные, снятые с восьми кольцевых осцилляторов. Полученные массивы были исследованы, преобразованы и протестированы в среде программирования Python. Методами преобразования выходного сигнала являлись: операции XOR, функции экстракции.

В первую очередь выполнено изменение частоты семплирования с колец индивидуально для каждого выходного сигнала. В исследуемых данных, полученных с ФДСЧ, частота опроса составляла 60 МГц, что в 2 раза больше частоты осциллирования первого кольца. Рассматривалось изменение частоты опроса с уменьшением шага в число раз, кратное 0,5. Характеристиками при сравнении методов семплирования выступали: количество пар бит «01» в последовательности, отклонение от равномерного распределения, выборочное среднее, выборочная дисперсия и максимальное количество подряд идущих единиц. Из-за конструктивных особенностей инверторов, используемых в кольцевых осцилляторах, не представляется возможным сохранение идентичной частоты снятия данных для каждой последовательности. По результатам тестирования была выявлена частота опроса 12 МГц, что в 5 раз меньше исходной.

Следующий этап — тестирование последовательности на свойства случайности. Использованы статистические тесты NIST STS (NIST Statistical Test Suite) [8]. Пакет содержит 15 тестов, целью которых является выявление статистических отклонений последовательностей, полученных при помощи датчиков случайных и псевдослучайных чисел, от истинно случайных последовательностей.

Статистические тесты NIST STS были написаны на языке программирования Python для удобства преобразования и проверки последовательностей на случайность в одной среде программирования. В свою очередь, проделанная работа повлияла на выбор тестов, применяющихся для последовательностей.

По результатам применения пакета NIST STS сделан вывод, что использование последовательностей в криптографической защите в исходном виде невозможно. Требуются преобразования для улучшения статистических качеств.

В качестве инструментов преобразования использованы операция XOR и метод фон Неймана [9], их комбинация позволила исследовать пять схем преобразования последовательностей.

Первый способ преобразования представляет собой побитовое сложение по модулю два всех последовательностей и применение к нему метода фон Неймана (рис. 1).

Во второй схеме (рис. 2) метод фон Неймана применяется к последовательности бит, полученных с первого кольца осциллятора, после чего полученная последовательность складывается по модулю два с остальными. Заканчивается алгоритм применением метода фон Неймана к преобразованной последовательности.

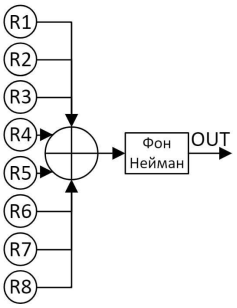

Рис. 1. Схема преобразования № 1

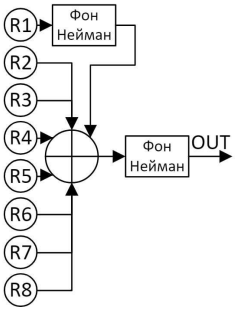

Рис. 2. Схема преобразования № 2

Схема 3 (рис. 3) представляет собой разделение последовательностей на две группы по четыре, где последовательности складываются по модулю два между собой. К полученным двум последовательностям применяется преобразование фон Неймана, после этого выполняется операция сложения по модулю два.

В схеме 4 (рис. 4) первая последовательность преобразуется с помощью метода фон Неймана, остальные семь последовательностей складываются по модулю два и полученный результат подвергается преобразованию фон Неймана. Конечной операцией является сложение двух полученных последовательностей по модулю два.

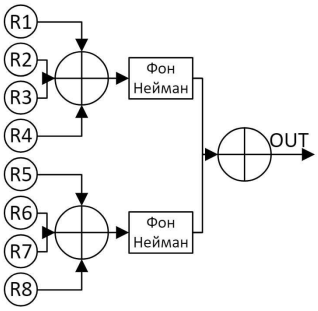

Рис. 3. Схема преобразования № 3

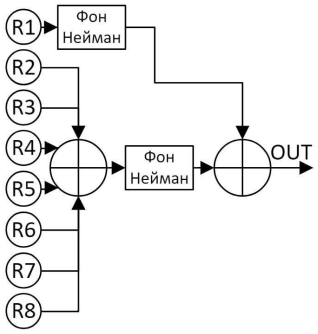

Рис. 4. Схема преобразования № 4

Пятая схема (рис. 5) может считаться обратной первой, так как в ней на первом этапе применяется метод фон Неймана к каждой последовательности, после чего происходит сложение по модулю два всех последовательностей.

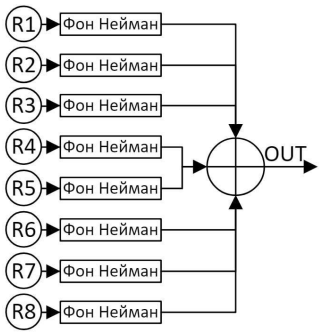

Рис. 5. Схема преобразования № 5

Необходимо уточнить, что при сложении по модулю два в случае различия длин последовательностей (например, сложение исходной последовательности бит, полученной с кольца осциллятора, и последовательности, преобразованной при помощи фон Неймана) сложение происходит по последовательности меньшей длины. В результате получается «укороченная» последовательность.

После реализации каждой схемы на языке программирования Python к последовательностям был применен пакет NIST STS. Для тестов установлен уровень значимости $\alpha = 0{,}01$. В каждом тесте рассчитывается p-уровень значимости P-value. Если P-value $< \alpha$, то нулевая гипотеза отвергается, то есть последовательность не обладает свойствами случайной. На основе p-уровня значимости делается вывод об успешном (PASSED) или безуспешном (FAILED) прохождении теста, он указан в ячейках таблицы для каждого теста и каждой последовательности.

Из полученных данных сделан вывод, что последовательность № 5 имеет следующие преимущества: сохрананение большего количества бит на выходе, чем у остальных, высокий порог прохождения тестов NIST STS. По этим причинам данная последовательность была выбрана в качестве основной для сравнения с последовательностью, зашифрованной алгоритмом AES в режиме счётчика. Сравнение показало, что количество успешно пройденных тестов для преобразованной последовательности выше, чем для последовательности, зашифрованной алгоритмом AES (см. таблицу).

Результат работы показал, что ФДСЧ, основанный на кольцевых осцилляторах, с применением методов преобразования способен генерировать такие последовательности, которые могут использоваться для выработки ключевой и другой псевдослучайной информации, о чём свидетельствует успешное прохождение тестов NIST STS на свойства случайности.

Характеристики и названия тестов	Схема № 1	Схема № 2	Схема № 3	Схема № 4	Схема № 5	AES
Кол-во тестир. бит, шт.	160000	160000	160000	160000	160000	160000
Monobit	PASSED 0,828	PASSED 0,046	PASSED 0,138	PASSED 0,701	PASSED 0,345	PASSED 0,841
Frequency Within Block	PASSED 0,383	PASSED 0,226	PASSED 0,636	PASSED 0,66	PASSED 0,625	PASSED 0,645
Runs	FAILED 0,0	FAILED 0,0	PASSED 0,649	PASSED 0,463	PASSED 0,394	PASSED 0,337
Longest Run Ones In A Block	PASSED 0,382	PASSED 0,382	PASSED 0,088	PASSED 0,369	PASSED 0,416	PASSED 0,838
Binary Matrix Rank	PASSED 0,087	PASSED 0,167	PASSED 0,59	PASSED 0,935	PASSED 0,231	PASSED 0,659
Discrete Fourier Transform	FAILED 0,0	FAILED 0,0	FAILED 0,0	FAILED 0,0	FAILED 0,0	FAILED 0,0
Non Overlapping Template Matching	FAILED 0,0	PASSED 0,014	FAILED 0,0	PASSED 0,227	PASSED 0,068	FAILED 0,0
Serial	FAILED 0,0	FAILED 0,0	FAILED 0,0	FAILED 0,0	FAILED 0,0	FAILED 0,0
Approximate Entropy	FAILED 0,0	FAILED 0,0	FAILED 0,0	FAILED 0,0	FAILED 0,0	FAILED 0,0
Cumulative Sums	PASSED 1,0	PASSED 1,0	PASSED 1,0	PASSED 1,0	PASSED 1,0	PASSED 1,0
Random Excursion	PASSED 0,971	PASSED 0,971	PASSED 0,957	PASSED 0,971	PASSED 0,971	PASSED 0,971
Random Excursion Variant	FAILED 0,0	FAILED 0,0	FAILED 0,0	FAILED 0,0	FAILED 0,0	FAILED 0,0
Кол-во успешных тестов, шт.	6	7	8	8	8	7

ЛИТЕРАТУРА

1. *Dai L. and Harjani R.* A low-phase-noise CMOS ring oscillator with differential control and quadrature outputs // Proc. 14th Ann. IEEE Intern. ASIC/SOC Conf. Arlington, USA, 2001. P. 134–138.
2. *Rezayee A. and Martin K.* A coupled two-stage ring oscillator // Proc. MWSCAS. Dayton, USA, 2001. V. 2. P. 878–881.
3. *Le H., Langley B., Cottle J., and Kopley T.* Improved ring oscillator design techniques to generate realistic AC waveforms for reliability testing // IEEE Intern. Integrated Reliability Workshop Final Report. Lake Tahoe, USA, 2000. P. 155–157.
4. *Глущенко А. А., Глущенко А. Г., Глущенко В. А.* Интерференционная картина кольцевой системы когерентных осцилляторов // Научн. обозрение. Техн. науки. 2023. № 2. С. 27–32.
5. *Свирский М. С., Свирская Л. М.* Уровни энергии кругового осциллятора // Фундаментальные исследования. 2009. № 5. С. 20–21.
6. *Комиссаров В. П.* Влияние центробежных сил инерции на частоту колебаний осциллятора кольцевой формы // Труды Междунар. симп. «Надежность и качество». 2005. Т. 1. С. 285–287.
7. *Иванюк А. А., Ярмолик В. Н.* Физически неклонируемые функции на базе управляемого кольцевого осциллятора // Безопасность информ. технологий. 2023. Т. 30. № 3. С. 90–103.
8. *Bassham L., Rukhin A., Soto J., et al.* Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications. Special Publication (NIST SP), National Institute of Standards and Technology, Gaithersburg, 2010.
9. *Von Neumann J.* Various techniques used in connection with random digits // Appl. Math. Ser. 1951. V. 12. P. 36–38.

УДК 512.552 DOI 10.17223/2226308X/17/17

СВОЙСТВА ПОСЛЕДОВАТЕЛЬНОСТЕЙ, ВЫРАБАТЫВАЕМЫХ АЛГОРИТМОМ ПОТОЧНОГО ШИФРОВАНИЯ GEA-1

А. Д. Бугров, О. В. Камловский, В. В. Мизеров

Изучаются периодические, частотные и автокорреляционные характеристики отрезков промежуточных и выходных последовательностей, вырабатываемых алгоритмом поточного шифрования GEA-1. Результаты получены с использованием известных оценок тригонометрических сумм, зависящих от знаков линейных рекуррентных последовательностей.

Ключевые слова: *линейные рекуррентные последовательности, фильтрующие генераторы, суммы аддитивных характеров, автокорреляционная функция последовательностей.*

Введение

Задача описания частотных и корреляционных характеристик линейных рекуррентных последовательностях (ЛРП) и их усложнений является классической, её решению посвящено большое количество публикаций (см., например, обзоры в [1, 2]). Один из подходов к исследованию частотных и автокорреляционных характеристик ЛРП связан с использованием метода тригонометрических сумм, предложенного в [3] и позже развивавшегося в работах [4–8].

Алгоритм поточного шифрования GEA-1 разработан в 1998 г. [9]. Он применялся для шифрования трафика в стандарте GPRS, основанном на технологии GSM (2G). В 1999 г. появилась несколько модифицированная версия алгоритма GEA-1, названная GEA-2. Последовательности в этих алгоритмах строятся на основе усложнений ЛРП с использованием некоторых нелинейных функций. В данной работе рассматривается приложение известных общих результатов о распределении элементов в ЛРП, полученных с помощью метода тригонометрических сумм, к последовательностям, вырабатываемым алгоритмом GEA-1.

1. Последовательности в алгоритме GEA-1

Опишем алгоритм поточного шифрования GEA-1 с необходимой для дальнейших исследований детализацией. Подробнее с этим алгоритмом можно познакомиться в [9]. Выработка последовательностей в шифре GEA-1 осуществляется с использованием трёх двоичных (над полем $\mathrm{GF}(2)$) линейных автономных автоматов L_1, L_2, L_3 размерностей $m_1 = 31$, $m_2 = 32$, $m_3 = 33$ соответственно [10]. Данные автоматы представляют собой двоичные линейные регистры сдвига в форме Галуа [11] с примитивными характеристическими многочленами $F_1(x)$, $F_2(x)$, $F_3(x)$ соответственно, т. е. для их периодов справедливы равенства $T(F_1) = 2^{31} - 1$, $T(F_2) = 2^{32} - 1$, $T(F_3) = 2^{33} - 1$. Состояние $(c_0^{(j)}(i), c_1^{(j)}(i), \ldots, c_{m_j-1}^{(j)}(i))$ автомата L_j, где $j = 1, 2, 3$, в момент времени $i = 0, 1, 2, \ldots$ строится по правилу

$$\begin{pmatrix} c_0^{(j)}(i) \\ c_1^{(j)}(i) \\ \vdots \\ c_{m_j-1}^{(j)}(i) \end{pmatrix} = G(F_j)^i \begin{pmatrix} c_0^{(j)}(0) \\ c_1^{(j)}(0) \\ \vdots \\ c_{m_j-1}^{(j)}(0) \end{pmatrix},$$

где $\left(c_0^{(j)}(0), c_1^{(j)}(0), \ldots, c_{m_j-1}^{(j)}(0)\right)$ — ненулевое начальное состояние; $G(F_j)$ — сопровождающая матрица многочлена $F_j(x) = x^{m_j} \oplus a_0 x^{m_j-1} \oplus a_1 x^{m_j-2} \oplus \cdots \oplus a_{m_j-2}x \oplus a_{m_j-1}$ в форме Галуа, т. е.

$$G(F_j) = \begin{pmatrix} a_0 & 1 & 0 & \ldots & 0 \\ a_1 & 0 & 1 & \ldots & 0 \\ & & & \ldots & \\ a_{m_j-2} & 0 & 0 & \ldots & 1 \\ a_{m_j-1} & 0 & 0 & \ldots & 0 \end{pmatrix}.$$

В алгоритме GEA-1 используется булева функция $f(x_0, x_1, \ldots, x_6)$ от 7 переменных. Она является сбалансированной и имеет алгебраическую степень 4. Коэффициенты Уолша — Адамара функции f принимают значения из множества $\{0, \pm 16\}$, причём число ненулевых коэффициентов среди них равно 64. Другими словами, f является платовидной функцией порядка 6 [12]. Из функции f конструируются следующие три функции:

$$f_1(x_0, x_1, \ldots, x_6) = f(x_5, x_0, x_3, x_4, x_6, x_1, x_2),$$
$$f_2(x_0, x_1, \ldots, x_6) = f(x_3, x_5, x_0, x_1, x_6, x_4, x_2),$$
$$f_3(x_0, x_1, \ldots, x_6) = f(x_3, x_5, x_6, x_1, x_4, x_0, x_2),$$

полученные из f перестановкой переменных.

Выходная последовательность $v = (v(i))_{i=0}^{\infty}$ алгоритма GEA-1 удовлетворяет равенству $v = v_1 \oplus v_2 \oplus v_3$, где последовательности v_1, v_2, v_3 являются усложнениями последовательностей $c_t^{(j)} = \left(c_t^{(j)}(i)\right)_{i=0}^{\infty}$, $j = 1, 2, 3$, $t = 0, 1, 2, \ldots, m_j - 1$, по следующим правилам:

$$v_1(i) = f_1\left(c_0^{(1)}(i), c_3^{(1)}(i), c_{10}^{(1)}(i), c_{12}^{(1)}(i), c_{17}^{(1)}(i), c_{23}^{(1)}(i), c_{27}^{(1)}(i)\right),$$
$$v_2(i) = f_2\left(c_0^{(2)}(i), c_1^{(2)}(i), c_5^{(2)}(i), c_{12}^{(2)}(i), c_{21}^{(2)}(i), c_{27}^{(2)}(i), c_{29}^{(2)}(i)\right),$$
$$v_3(i) = f_3\left(c_0^{(3)}(i), c_3^{(3)}(i), c_4^{(3)}(i), c_{10}^{(3)}(i), c_{19}^{(3)}(i), c_{30}^{(3)}(i), c_{32}^{(3)}(i)\right),$$

где $i \geqslant 0$.

Пусть t — целое неотрицательное число. Назовём сдвигом последовательности $\omega = (\omega(0), \omega(1), \omega(2), \ldots)$ на t шагов последовательность $x^t\omega = (\omega(t), \omega(t+1), \omega(t+2), \ldots)$ Согласно [4, 13], последовательности $c_0^{(j)}$, $c_1^{(j)}$, …, $c_{m_j-1}^{(j)}$, где $j = 1, 2, 3$, образуют линейно независимую систему ЛРП с характеристическим многочленом $F_j(x)$, причём их периоды равны $2^{m_j} - 1$. Рассматриваемые последовательности являются сдвигами ЛРП $c_0^{(j)} = u_j$ [14].

2. Частотные характеристики и периодические свойства

Пусть ω — произвольная последовательность элементов поля GF(2). Для каждого натурального числа l и элемента $z \in \mathrm{GF}(2)$ обозначим через $N_l(z, \omega)$ число появлений z среди элементов $\omega(0), \omega(1), \ldots, \omega(l-1)$. В случае, когда $l = T(\omega)$, где $T(\omega)$ — период последовательности ω, частоту $N_l(z, \omega)$ будем называть частотой появления z на цикле последовательности ω и обозначать $N(z, \omega)$.

Утверждение 1. Для всех $z \in \mathrm{GF}(2)$, $j = 1, 2, 3$ справедливы равенства

$$T(v_j) = T(u_j) = 2^{m_j} - 1, \quad T(v) = (2^{31} - 1)(2^{32} - 1)(2^{33} - 1),$$

$$N(z, v_j) = \begin{cases} 2^{m_j-1}, & \text{если } z = 1, \\ 2^{m_j-1} - 1, & \text{если } z = 0, \end{cases}$$
$$N(z, v) = (T(v) - (-1)^z)/2.$$

Утверждение 1 показывает, что на цикле каждой из последовательностей v_1, v_2, v_3, v частота появления нуля на 1 меньше, чем частота появлений единицы, т. е. рассматриваемые последовательности являются почти сбалансированными.

Утверждение 2. Для всех $l \leqslant 2^{m_j} - 1$, где $j = 1, 2, 3$, и $z \in \mathrm{GF}(2)$ справедлива оценка

$$\left| N_l(z, v_j) - \frac{l}{2} \right| \leqslant \left(\frac{4}{\pi^2} \ln(2^{m_j} - 1) + \frac{9}{5} \right) 2^{(m_j+4)/2}.$$

Используя утверждение 2, получаем:
при всех $l \leqslant 2^{31} - 1$

$$|N_l(z, v_1) - l/2| < 1{,}86 \cdot 2^{20};$$

при всех $l \leqslant 2^{32} - 1$

$$|N_l(z, v_2) - l/2| < 1{,}35 \cdot 2^{21};$$

при всех $l \leqslant 2^{33} - 1$

$$|N_l(z, v_3) - l/2| < 1{,}96 \cdot 2^{21}.$$

Утверждение 3. Для всех $l \leqslant T(v)$ и $z \in \mathrm{GF}(2)$ справедлива оценка

$$|N_l(z, v) - l/2| < 1{,}8 \cdot 2^{60}.$$

Полученные оценки частот появлений элементов на отрезках последовательностей оказываются содержательными только при больших длинах l отрезков последовательностей, что, по всей видимости, вызвано сложностью решаемых задач.

3. Автокорреляционная функция последовательностей

Пусть ω — двоичная чисто периодическая последовательность периода $T(\omega)$. Автокорреляционной функцией последовательности ω называется функция [15]

$$C_\omega(t) = \sum_{i=0}^{T(\omega)-1} (-1)^{\omega(i) \oplus \omega(i+t)}, \quad t = 0, 1, 2, \ldots$$

Заметим, что $C_\omega(t)$ — периодическая функция с периодом $T(\omega)$ и $C_\omega(0) = T(\omega)$. Кроме того, $C_\omega(t)$ связано с расстоянием Хэмминга $\rho_\omega(t)$ между векторами $(\omega(0), \ldots, \omega(T(\omega) - 1))$ и $(\omega(t), \ldots, \omega(t + T(\omega) - 1))$, а именно: $C_\omega(t) = T(\omega) - 2\rho_\omega(t)$ и справедливо равенство

$$|\rho_\omega(t) - T(\omega)/2| = |C_\omega(t)|/2.$$

Следующее утверждение сводит изучение автокорреляционной функции последовательности v к исследованию автокорреляционных функций последовательностей v_1, v_2, v_3.

Утверждение 4. Для всех $t \geqslant 0$ имеет место равенство $C_v(t) = C_{v_1}(t) C_{v_2}(t) C_{v_3}(t)$.

Рассмотрим автокорреляционную функцию последовательности v_j, где $j = 1, 2, 3$.

Утверждение 5. Для всех $j = 1, 2, 3$ и $t \geqslant 0$ число 2^{m_j-6} делит число $C_{v_j}(t) + 1$.

Из утверждения 5 следует, что наличие таких значений t, что $C_{v_j}(t) \neq -1$, является недостатком последовательности v_j, так как в этом случае v_j существенно коррелирует со своим сдвигом $x^t v_j$. Вопрос о существовании таких чисел t в каждом из случаев $j = 1, 2, 3$ решался с использованием вычислительных экспериментов. Величина $C_{v_j}(t)$ не зависит от начального заполнения регистра сдвига (последовательности u_j). Выбирались все значения $t \in \{1, 2, \ldots, 100\}$. Оказалось, что всегда $C_{v_j}(t) = -1$, за исключением следующих случаев:

$$C_{v_1}(4) = -2^{25} - 1,$$
$$C_{v_2}(2) = 2^{26} - 1, \quad C_{v_2}(6) = -2^{26} - 1,$$
$$C_{v_3}(1) = 2^{27} - 1, \quad C_{v_3}(4) = -2^{27} - 1.$$

Проведённые исследования иллюстрируют использование общих теоретических результатов об усложнениях ЛРП применительно к алгоритму шифрования GEA-1. Большинство идей работы переносится и на другие классы последовательностей, в частности на последовательности, вырабатываемые в алгоритме GEA-2.

ЛИТЕРАТУРА

1. *Лидл Р., Нидеррайтер Г.* Конечные поля. М.: Мир, 1988.
2. *Кузьмин А. С., Куракин В. Л., Нечаев А. А.* Псевдослучайные и полилинейные последовательности // Труды по дискретной математике. 1997. Т. 1. С. 139–202.
3. *Коробов Н. М.* Распределение невычетов и первообразных корней в рекуррентных рядах // Доклады АН СССР. 1953. Т. 88. № 4. С. 603–606.
4. *Нечаев В. И.* Распределение знаков в последовательности прямоугольных матриц над конечным полем // Труды математического института им. В. А. Стеклова. 1997. Т. 218. С. 335–342.
5. *Шпарлинский И. Е.* О распределении значений рекуррентных последовательностей // Проблемы передачи информации. 1989. Т. 25. № 2. С. 46–53.
6. *Sarwate D. V.* An upper bound on the aperiodic autocorrelation function for a maximal-length sequence // IEEE Trans. Inform. Theory. 1984. V. 30. No. 4. P. 685–687.
7. *Niederreiter H.* Distribution properties of feedback shift register sequences // Problems Control Inform. Theory. 1986. V. 15. No. 1. P. 19–34.
8. *Камловский О. В.* Количество появлений элементов в выходных последовательностях фильтрующих генераторов // Прикладная дискретная математика. 2013. № 3(21). С. 11–25.
9. *Beierle C., Derbez P., Leander G., et al.* Cryptanalysis of the GPRS encryption algorithms GEA-1 and GEA-2 // LNCS. 2021. V. 12697. P. 155–183.
10. *Гилл А.* Линейные последовательные машины. М.: Мир, 1974.
11. *Шнайер Б.* Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си. М.: Триумф, 2003.
12. *Логачев О. А., Сальников А. А., Смышляев С. В., Ященко В. В.* Булевы функции в теории кодирования и криптологии. М.: МЦНМО, 2012.
13. *Камловский О. В.* Свойства распределений строк и столбцов для матричных линейных рекуррентных последовательностей первого порядка // Математические вопросы криптографии. 2015. Т. 6. № 4. С. 65–76.
14. *Глухов М. М., Елизаров В. П., Нечаев А. А.* Алгебра: Учебник. Т. 2. М.: Гелиос АРВ, 2003.
15. *Golomb S. W. and Gong G.* Signal Design for Good Correlation. Cambridge University Press, 2005.

УДК 519.24 DOI 10.17223/2226308X/17/18

МАТРИЦА ПЕРЕХОДНЫХ ВЕРОЯТНОСТЕЙ РАЗНОСТЕЙ 8-РАУНДОВОЙ СХЕМЫ ЛУБИ — РАКОФФ

М. М Глухов, О. В. Денисов

Вычисляется восьмая степень матрицы переходных вероятностей схемы Луби — Ракофф, даются оценки объёма материала j-векторных ($j = 1, 2$) разностно-спектральных атак различения на 8 раундов схемы Луби — Ракофф в модели независимых двублочных текстов.

Ключевые слова: *марковские блочные шифры, схема Луби — Ракофф, атака различения, переходные вероятности разностей.*

В работе [1] показано, что схема Луби — Ракофф [2] является марковским шифром (над алфавитом блоков G^2, где G — произвольная абелева группа порядка $M = 2^n$) с матрицей переходных вероятностей разностей

$$\mathbb{P}(M) = \frac{1}{M}\begin{pmatrix} P_0 & Q_1 & \cdots & Q_{M-1} \\ P_1 & Q_1 & \cdots & Q_{M-1} \\ \vdots & \vdots & \cdots & \vdots \\ P_{M-1} & Q_1 & \cdots & Q_{M-1} \end{pmatrix},$$

где $P_j = Me_0^{\downarrow}\overrightarrow{e_j}$, $Q_k = e_k^{\downarrow}\overrightarrow{1}$ для всех j, k — клетки ранга 1 размера $M = 2^n$; n (бит) — длина полублока; e_j — j-й столбец или строка (зависит от приписанной стрелки) стандартного базиса; $\overrightarrow{1} = (1, 1, \ldots, 1)$. Здесь и далее разности (состояния цепи Маркова) нумеруются так, что биты правого полублока младшие.

Там же подсчитаны вторая и четвёртая степени этой матрицы, что позволило при $R = 4$ оценить объём материала разностной атаки различения (выбора из двух гипотез — H_1: подстановка выбрана равновероятно из множества всех подстановок и H_2: подстановка получена в R-раундовой схеме Луби — Ракофф), построенной на основе процедуры Вальда.

Справедливо следующее утверждение.

Теорема 1. Во введённых обозначениях

$$\mathbb{P}(M)^8 = \frac{1}{M^8}\begin{pmatrix} A_{0,0} & A_{0,1} & A_{0,1} & A_{0,1} & \cdots & A_{0,1} & A_{0,1} \\ A_{1,0} & A_{1,1} & A_{1,2} & A_{1,2} & \cdots & A_{1,2} & A_{1,2} \\ A_{1,0} & A_{1,2} & A_{1,1} & A_{1,2} & \cdots & A_{1,2} & A_{1,2} \\ A_{1,0} & A_{1,2} & A_{1,2} & A_{1,1} & \cdots & A_{1,2} & A_{1,2} \\ \vdots & \vdots & \ddots & \ddots & \ddots & \ddots & \vdots \\ A_{1,0} & A_{1,2} & A_{1,2} & A_{1,2} & \cdots & A_{1,1} & A_{1,2} \\ A_{1,0} & A_{1,2} & A_{1,2} & A_{1,2} & \cdots & A_{1,2} & A_{1,1} \end{pmatrix},$$

где $A_{i,j}$ — клетки размера $M \times M$:

$$A_{0,0} = \begin{pmatrix} M^8 & 0 & 0 & 0 & \cdots & 0 & 0 \\ 0 & a & b & b & \cdots & b & b \\ 0 & b & a & b & \cdots & b & b \\ 0 & b & b & a & \cdots & b & b \\ \vdots & \vdots & \vdots & \ddots & \ddots & \ddots & \vdots \\ 0 & b & b & b & \cdots & a & b \\ 0 & b & b & b & \cdots & b & a \end{pmatrix}, \quad A_{1,0} = \begin{pmatrix} 0 & c & c & c & \cdots & c & c \\ 0 & d & e & e & \cdots & e & e \\ 0 & e & d & e & \cdots & e & e \\ 0 & e & e & d & \cdots & e & e \\ \vdots & \vdots & \vdots & \ddots & \ddots & \ddots & \vdots \\ 0 & e & e & e & \cdots & d & e \\ 0 & e & e & e & \cdots & e & d \end{pmatrix},$$

$$A_{0,1} = (M^2+1)(M^4+1)(0,1,1,\dots,1)^{\mathrm{T}}\overrightarrow{1},$$
$$A_{1,1} = \big(M(M^5+2M^3-M-1),(M^2+1)(M^4+1),\dots,(M^2+1)(M^4+1)\big)^{\mathrm{T}}\overrightarrow{1},$$
$$A_{1,2} = \big(M(M-1)(M^4+M^3+2M^2+M+1),(M^2+1)(M^4+1),\dots,(M^2+1)(M^4+1)\big)^{\mathrm{T}}\overrightarrow{1},$$
$$a = M(M^5+2M^3-M^2-1), \quad b = M(M^2+1)(M-1)(M^2+M-1),$$
$$c = M^2(M^4+M^2+1), \quad d = M(M^5+2M^3-M^2-1), \quad e = M(M^2+1)(M^3-1).$$

Полученный результат позволяет (аналогично тому, как это сделано в [1]) оценить объём последовательной атаки различения на 8 раундов схемы Луби — Ракофф в модели независимых двублочных текстов, а также на основе дивергенции Кульбака — Лейблера получить нижние оценки объёма материала любого критерия проверки гипотез $H_{1,2}$ в этой модели.

Мы рассмотрим другое применение этого результата, связанное с разностно-спектральной атакой различения [3] на марковские шифры, которая может быть применена в более привычной модели независимых кодовых книг. Впервые такая модель наблюдений была предложена, вероятно, в [4, с. 116] при атаке на 6 и более раундов.

Основной проблемой спектральной атаки различения является построение одного или двух собственных векторов матрицы $\mathbb{P}$, соответствующих действительному собственному значению $\lambda \notin \{0,1\}$. Согласно [5], С. Е. Недоспасов решил более общую задачу полного описания спектра $\mathbb{P}$ и базисов собственных подпространств. В частности, наибольшему по модулю собственному значению $\lambda = \dfrac{1}{\sqrt{M}}$ отвечают:

1) правые собственные векторы

$$v_i = (\overrightarrow{q_0},\overrightarrow{q_-},\overrightarrow{q_0},\dots,\overrightarrow{q_0},\overrightarrow{q_+},\overrightarrow{q_0},\dots,\overrightarrow{q_0})^{\mathrm{T}}),\ i = 1,\dots,M-2,$$

где $\overrightarrow{q_+}$ стоит на $(i+2)$-м месте слева; $\overrightarrow{q_0} = \overrightarrow{q_0(i)} = -\overrightarrow{e_1} + \overrightarrow{e_{i+1}}$; $\overrightarrow{q_\pm} = \pm\sqrt{M}\overrightarrow{e_0} - \overrightarrow{e_1} + \overrightarrow{e_{i+1}}$;

2) левые собственные векторы

$$u_i = (\sqrt{M}\overrightarrow{q_0},-1,0,\dots,0,1,0,\dots,0),\ i = 1,\dots,M-2,$$

где 1 стоит на $(i+2)$-м месте слева.

Для оценки объема материала j-векторных ($j = 1,2$) разностно-спектральных атак различения [3] необходимо вычислить значения дисперсий $\sigma^2_{2j}(R)$ одного слагаемого статистики j-векторного критерия при второй гипотезе. В [5] это сделано при $R = 4$:

$$\sigma^2_{21}(4) = \frac{9}{8} - \frac{1}{8M} - \frac{5}{8M^2} - \frac{1}{8M^3} - \frac{3}{2M^4} + \frac{1}{4M^5},$$
$$\sigma^2_{22}(4) = \frac{5}{4} - \frac{1}{2M} - \frac{1}{M^2} - \frac{1}{2M^3} - \frac{1}{4M^4}.$$

Теперь это можно сделать при $R = 8$.

Теорема 2. Во введённых обозначениях

$$\sigma^2_{21}(8) = 1 - \frac{1}{16}\left(\frac{4}{M} + \frac{6}{M^2} + \frac{2}{M^3} + \frac{14}{M^4} + \frac{2}{M^5} - \frac{4}{M^7} + \frac{5}{M^8} - \frac{4}{M^9} - \frac{8}{M^{10}}\right),$$
$$\sigma^2_{22}(8) = \frac{7}{8} + \frac{1}{16}\left(\frac{4}{M^2} - \frac{7}{M^3} - \frac{12}{M^4} - \frac{3}{M^5} + \frac{9}{M^7} - \frac{6}{M^8}\right).$$

Наблюдаемое приближение дисперсий к 1 с ростом числа раундов вызвано приближением подстановок, вырабатываемых схемой Луби — Ракофф, к случайным равновероятным.

Свойства модели Луби — Ракофф используются для обоснования безопасности блочных FPE-схем (Format Preserving Encryption), т. е. схем шифрования, сохраняющих исходный формат шифруемых данных. Например, в южнокорейском стандарте FEA-1 [6] число раундов равно $R = 12, 14, 16$ соответственно для длины ключа 128, 192, 256 битов при всех длинах полублока $4 \leqslant n \leqslant 64$.

ЛИТЕРАТУРА

1. *Денисов О. В.* Атака различения на 4 раунда шифра Люби — Ракофф по разностям двублочных текстов // Прикладная дискретная математика. Приложение. 2023. № 16. С. 32–35.
2. *Luby M. and Rackoff C.* How to construct pseudorandom permutations from pseudorandom functions // SIAM J. Comput. 1988. V. 17. P. 373–386.
3. *Денисов О. В.* Спектральный вероятностно-статистический анализ марковских шифров // Прикладная дискретная математика. 2020. № 53. С. 12–31.
4. *Patarin J.* Security of random Feistel schemes with 5 or more rounds // LNCS. 2004. V. 3152. P. 106–122.
5. *Денисов О. В.* Разностно-спектральные атаки на схемы Луби — Ракофф по независимым двублочным текстам // Представлена в редакцию журнала «Матем. вопр. криптогр.».
6. *Lee J.-K., Koo B., Roh D., et al.* Format-preserving encryption algorithms using families of tweakable blockciphers // LNCS. 2015. V. 8949. P. 132–159.

УДК 519.24 DOI 10.17223/2226308X/17/19

РАЗНОСТНО-ЛИНЕЙНЫЕ АТАКИ РАЗЛИЧЕНИЯ НА БЛОЧНЫЕ ШИФРЫ

О. В. Денисов, С. М. Рамоданов

Введён класс разностно-линейных атак различения на блочные шифры. Построена атака (названная разностно-сингулярной), оптимальная в данном классе. Проведены вероятностно-статистические эксперименты с шифрсистемами семейства SmallPresent с длинами блока $n \in \{8, 12, 16\}$ и $R \in \{3, \ldots, 9\}$ раундами.

Ключевые слова: *разностно-линейные статистики, сингулярные числа, атаки различения, шифр SmallPresent.*

Пусть алфавитом входных и выходных блоков R-раундового блочного шифра является абелева группа $(\mathbb{X}, +)$. Обозначим через $\mathbb{X}' = \mathbb{X} \setminus \{0\}$ множество ненулевых блоков, $M = |\mathbb{X}'|$ — его мощность, $Q_{M\times M}$ — дважды стохастическую матрицу переходных вероятностей ненулевых разностей (МПВР) шифра.

По наблюдаемым равномерно распределённым входным разностям $\Delta X_t = X_t^* - X_t \sim U(\mathbb{X}')$ двублочных открытых текстов (X_t, X_t^*) и выходным разностям $\Delta Y_t = Y_t^* - Y_t$ соответствующих им шифртекстов (Y_t, Y_t^*), $1 \leqslant t \leqslant N$, требуется построить *атаку различения*, т. е. критерий проверки гипотезы H_1 о том, что шифртексты получены в результате применения случайных равновероятно выбираемых подстановок на $\mathbb{X}$, против гипотезы H_2 о том, что шифртексты получены применением данного блочного шифра. Обозначая через θ матрицу переходных вероятностей наблюдаемых разностей, получаем, что $\theta = \mathbb{U} = \dfrac{1}{M} 1^{\downarrow} \mathbf{1}$ (равномерная матрица) при гипотезе H_1 и $\theta = Q$ при

гипотезе H_2. Далее через e_i обозначаем векторы стандартного базиса $\mathbb{R}^M$, через P_i, E_i, D_i, $\alpha_i(d)$ — вероятностное распределение, математическое ожидание и дисперсию статистик, вероятности ошибок критериев при гипотезе H_i, $i = 1, 2$.

Матричнозначная статистика

$$\hat{\theta} = \frac{M}{N} \sum_{1 \leqslant t \leqslant N} e^{\downarrow}_{\Delta X_t} \mathbf{e}_{\Delta Y_t} \tag{1}$$

является несмещённой при каждой гипотезе оценкой МПВР, т. е. $\mathsf{E}_1\hat{\theta} = \mathbb{U}$, $\mathsf{E}_2\hat{\theta} = Q$ [1, с. 19–21].

Рассмотрим класс статистик

$$T = \mathbf{u}\,\hat{\theta}\,v^{\downarrow}, \quad |u| = |v| = 1,$$

которые назовем *разностно-линейными (р.-л.)*, поскольку T есть линейная (точнее, билинейная) форма от оценки МПВР.

Такими являются, например:

1) статистики $\nu_{ab} = \mathbf{e}_a\,\hat{\theta}\,e^{\downarrow}_b$ числа переходов из разности a в разность b [2];
2) статистики, пропорциональные количеству переходов разностей из $A \subset \mathbb{X}$ в $B \subset \mathbb{X}$, при $\mathbf{u} = \dfrac{1}{\sqrt{A}} \sum\limits_{a \in A} \mathbf{e}_a$, $v^{\downarrow} = \dfrac{1}{\sqrt{B}} \sum\limits_{b \in B} e^{\downarrow}_b$; они являются подклассом мультиразностных статистик [3], равных числу высоковероятных переходов разностей;
3) спектральные статистики [1] в случае, когда $Q = \mathbb{P}^R$ и один из векторов — собственный вектор дважды стохастической матрицы $\mathbb{P}$, соответствующий значению $\lambda \in \mathbb{R} \setminus \{0, 1\}$.

В [1] при $Q = \mathbb{P}^R$ обсуждалась проблема выбора пары, максимизирующей модуль разности средних значений

$$\mathsf{E}_2 T - \mathsf{E}_1 T = \mathbf{u}\,(\mathbb{P}^R - \mathbb{U})\,v^{\downarrow}. \tag{2}$$

Заметим, что если матрица $\mathbb{P}^R$ симметрична, то при ограничении $u = \pm v$ максимум достигается на собственных векторах, соответствующих наибольшему по модулю действительному собственному значению матрицы $\mathbb{P}^R - \mathbb{U}$. Это следует из [4, с. 108].

Исходя из спектрального разложения $\mathbb{P}^R$ в случае диагонализуемой над $\mathbb{R}$ матрицы $\mathbb{P}$, в [1, с. 22] высказано предположение о том, что близким к оптимальному при больших R будет выбор в качестве u правого собственного вектора, соответствующего $\lambda = \lambda_2$ — доминирующему собственному значению, в качестве v — левого:

$$T = \mathbf{u}\,\hat{\theta}\,v^{\downarrow}, \text{ где } \mathbb{P}\,u^{\downarrow} = \lambda_2 u^{\downarrow}, \ \mathbf{v}\,\mathbb{P} = \lambda_2 \mathbf{v}. \tag{3}$$

Легко видеть, что если

$$u = v \text{ — левый или правый собственный вектор } \mathbb{P}, \text{ соответствующий } \lambda, \tag{4}$$

то $\mathsf{E}_2 T = \lambda^R$; вектор v ортогонален $\mathbf{1}$, согласно принципу биортогональности [5, с. 78], поэтому $\mathsf{E}_1 T = 0$.

1. Решение оптимизационной задачи

С учётом возможности изменения знака одного из векторов в (2) будем искать максимум билинейной формы

$$F(u,\, v) = \mathbf{u}\, A\, v^{\downarrow} \to \max$$

при условии, что векторы $u, v \in \mathbb{R}^M$ удовлетворяют соотношениям $|u| = 1$, $|v| = 1$.

Напомним, что если $A, B \in \mathbb{R}_{M,M}$, то характеристические многочлены матриц AB и BA совпадают (см. [4, с. 104] или [6, с. 53, 7.27]), что обосновывает корректность условия следующей теоремы.

Теорема 1. Пусть $A \in \mathbb{R}_{M,M}$; $\rho_{\max}$ — наибольшее собственное значение матриц $AA^{\top}$ и $A^{\top}A$; $\mathbf{u_0}$ и $v_0^{\downarrow}$ — отвечающие ему собственные векторы длины 1 этих симметричных матриц. Тогда

$$\max_{|u|=1,\,|v|=1} F(u,v) = \mathbf{u_0} A v_0^{\downarrow} = \sqrt{\rho_{\max}}.$$

Замечание 1. Так как матрицы $AA^{\top}$ и $A^{\top}A$ неотрицательно определены, то всегда $\rho_{\max} \geqslant 0$; число $\sqrt{\rho_{\max}}$ называется доминирующим *сингулярным числом* матрицы A [5, с. 247, 493; 6, с. 79].

2. Атаки различения по случайной полной кодовой книге

Пусть далее алфавит — группа $\mathbb{X} = \big(\mathrm{GF}(2^k)\big)^n$ с операцией $\oplus$ покоординатного сложения по модулю 2, элементы $\mathbb{Z}_2^n$ отождествляем с числами, двоичной записью которых они являются.

Наблюдаются все значения $C(i)$, $0 \leqslant i \leqslant M = 2^{nk} - 1$, случайной подстановки C на $\mathbb{X}$, т. е. полная кодовая книга. Требуется проверить гипотезу H_1 о том, что C выбрана случайно равновероятно из множества всех подстановок на $\mathbb{X}$, против гипотезы H_2 о том, что она выбрана случайно равновероятно из множества суммарных шифров заданного R-раундового блочного шифра с МПВР Q.

Несмещённая оценка МПВР (1) здесь принимает вид [1, с. 24]

$$\hat{\theta}(C) := \frac{M}{\binom{M+1}{2}} \sum_{0 \leqslant i < j \leqslant M} e^{\downarrow}_{i \oplus j} \mathbf{e}_{C(i) \oplus C(j)} = \frac{1}{|\mathbb{X}|} \sum_{i \neq j} e^{\downarrow}_{i \oplus j} \mathbf{e}_{C(i) \oplus C(j)},$$

что, согласно [7, с. 10], совпадает с $P(C)$ — разностной матрицей неслучайной подстановки C. Слово «неслучайной» используется в том смысле, что усреднение частот переходов разностей происходит только по аргументам подстановки.

Нам будет удобно рассматривать далее р.-л. статистику, умноженную на $\dfrac{|\mathbb{X}|}{2}$, т. е. равную

$$T = T(C) = \frac{|\mathbb{X}|}{2} \mathbf{u}\, \hat{\theta}\, v^{\downarrow} = \sum_{0 \leqslant i < j \leqslant M} u_{i \oplus j} v_{C(i) \oplus C(j)}. \tag{5}$$

Определение 1. При фиксированных $u, v \in \mathbb{R}^M$ величину (5), равную значению билинейной формы на матрице частот переходов разностей подстановки C, будем называть *вкладом*[1] *подстановки* C.

Справедливо следующее обобщение теоремы 3 [1].

[1] В среднее значение $\mathsf{E}_2 T = 2^{nk-1} \mathbf{u}\, Q\, v^{\downarrow}$ (см. далее теорему 2).

Теорема 2. Пусть $\mathbb{X} = \bigl(\mathrm{GF}(2^k)\bigr)^n$ и хотя бы один из векторов $u, v \in \mathbb{R}^M$ ортогонален вектору $\mathbf{1}$. Тогда $\mathsf{E}_1 T = 0$, $\mathsf{E}_2 T = 2^{nk-1}\mu_2(R)$, где $\mu_2(R) = \mathbf{u}\, Q\, v^{\downarrow}$,

$$\mathsf{D}_1 T = \frac{M+1}{2(M-2)} = \frac{|\mathbb{X}|}{2(|\mathbb{X}|-3)} = \frac{1}{2 - 3/2^{nk-1}}.$$

Не ограничивая общности, далее считаем $\mu_2(R) > 0$, поскольку в противном случае можем изменить знак у одного из векторов, и с учётом выражения для $\mathsf{D}_1 T$ рассматриваем критерий

$$d:\ T(C) \geqslant \varkappa_{1-\alpha} \frac{1}{\sqrt{2 - 3/2^{nk-1}}} \Longrightarrow \text{ принимаем } H_2. \tag{6}$$

Здесь и далее $\varkappa_\gamma$ — квантиль уровня γ стандартного нормального распределения $\mathcal{N}(0,1)$.

Вероятность ошибки 2-го рода

$$\alpha_2(d) = \mathsf{P}_2 \left[T(C) < \varkappa_{1-\alpha} \frac{1}{\sqrt{2 - 3/2^{nk-1}}} \right] \tag{7}$$

определяется распределением вклада подстановки C при её случайном выборе, задаваемом распределением при гипотезе H_2. Если при гипотезе H_1 распределение $T(C)$ близко к нормальному с параметрами, найденными в теореме 2, то размер критерия (6) близок к заданному α. В экспериментах с шифрсистемами SmallPresent эти предположения близки к реальности, начиная с 4–5 и 6–7 раундов для длин блоков 8 и 12 соответственно (см. оценки дисперсий в табл. 4 и 5, а также гистограммы на рис. 1 и 2).

Оценим при этом предположении эффективность атаки (7), считая также распределение вклада $T(C)$ при гипотезе H_2 близким к $\mathcal{N}(\mathsf{E}_2 T, \mathsf{D}_1 T)$, $\mathsf{D}_1 T \approx 1/2$. Тогда оценка вероятности ошибки 2-го рода

$$\alpha_2(d) \approx \mathsf{P}_2 \left[\sqrt{2}(T - \mathsf{E}_2 T) < (\varkappa_{1-\alpha}/\sqrt{2} - \mathsf{E}_2 T)\sqrt{2} \right] \approx \Phi(\varkappa_{1-\alpha} - \sqrt{2}\mathsf{E}_2 T), \tag{8}$$

где $\Phi(x)$ — функция распределения $\mathcal{N}(0,1)$, не превосходит величины, близкой к заданному значению β, в том и только в том случае, когда следующая сумма квантилей не превосходит отношения сигнал/шум:

$$\varkappa_{1-\alpha} + \varkappa_{1-\beta} \leqslant \sqrt{2}\mathsf{E}_2 T \approx \frac{\mathsf{E}_2 T - \mathsf{E}_1 T}{\mathsf{D}_1 T} \approx 2^{nk-1/2}\mu_2(R). \tag{9}$$

Согласно теореме 1, значение $\mu_2(R)$ максимально, когда u и v — собственные векторы симметричных матриц $AA^\top$ и $A^\top A$, где $A = Q - \mathbb{U}$, соответствующие их наибольшему собственному значению $\rho_{\max}$. При этом $\mu_2(R) = \sqrt{\rho_{\max}}$. Другим словами, u и v — сингулярные векторы матрицы $Q - \mathbb{U}$, соответствующие её наибольшему доминирующему сингулярному значению $\sqrt{\rho_{\max}}$. Такую пару векторов будем называть *сингулярной*, а соответствующие статистику T и атаку (6) — *разностно-сингулярными*. Согласно теореме 1, выбор сингулярной пары векторов максимизирует разность математических ожиданий статистики, т. е. числитель отношения сигнал/шум в (9), и в этом смысле разностно-сингулярная атака близка к оптимальной в классе р.-л. атак.

При $\alpha = \beta$ из неравенства (9) вытекает, что $2\varkappa_{1-\alpha} \leqslant \sqrt{2}\mathsf{E}_2 T$, $1-\alpha \leqslant \Phi\Big(\dfrac{1}{\sqrt{2}}\mathsf{E}_2 T\Big)$. Поэтому при наших предположениях минимальная вероятность ошибки р.-л. атаки близка к величине

$$\alpha_{\min} = \Phi\Big(-\frac{1}{\sqrt{2}}\mathsf{E}_2 T\Big), \tag{10}$$

равной $\Phi(-2^{nk-1/2}\sqrt{\rho_{\max}})$ для разностно-сингулярной атаки.

2.1. Сравнение характеристик разностно-линейных атак различения на модели SmallPresent

В качестве примеров найдём характеристики р.-л. атак на модели шифрсистем SmallPresent[s] ($2 \leqslant s \leqslant 16$ — число S-боксов, $n = 4s$ бит — длина блока, R — уменьшенное число раундов). Это семейство SP-сетей предложил G. Leander [8], один из авторов шифрсистемы PRESENT. Система PRESENT, с которой совпадает SmallPresent[16], принята в 2012 г. как международный стандарт ISO/IEC блочных шифрсистем для низкоресурсных устройств. Раунд шифрования состоит из покоординатного аддитивного наложения раундового ключа, применения набора из s одинаковых параллельных S-боксов и перестановки бит, поэтому шифры являются марковскими с МПВР $\mathbb{P}$ [9, п. 5] в вероятностной модели с независимым равновероятным выбором раундовых ключей.

Рассмотрим критерии, использующие в качестве T: 1) спектральную *двухвекторную* статистику (3); 2) спектральную *одновекторную* статистику с векторами (4) билинейной формы; 3) сингулярную статистику с векторами билинейной формы u_0, v_0 из теоремы 1 для матрицы $A = \mathbb{P}^R - \mathbb{U}$. В табл. 1 приведены значения $\sqrt{\rho(R)}$ наибольших сингулярных чисел и сравнительные характеристики этих статистик — отношения квадратов величин сигнал/шум сингулярной и двухвекторной статистик к этому же параметру одновекторных статистик:

$$k_1(R) = \rho(R)/\lambda^{2R}, \quad k_2(R) = (\mathbf{u}\,\mathbb{P}^R v^{\downarrow})^2/\lambda^{2R}. \tag{11}$$

Заметим, что в модели независимых двублочных текстов [1] данные величины являются приближёнными оценками выигрышей в объёме материала для соответствующих р.-л. атак различения при всех $\alpha, \beta \in (0,1)$.

Таблица 1

Характеристики шифров SmallPresent

n	Характеристики	R							
		2	3	4	5	6	7	8	9
8	$\sqrt{\rho(R)}$	0,49	0,11	0,024	5,9E−3	1,7E−3	4,8E−4	1,3E−4	3,6E−5
	$\rho(R)/\lambda_2^{2R}$	48,5	38,7	23,4	19,3	22,9	24,3	26,2	27,1
	$(\mathbf{u}\,\mathbb{P}^R v^{\downarrow})^2/\lambda_2^{2R}$	3	6,1	7,7	9,8	14,5	17	21,3	23,8
12	$\sqrt{\rho(R)}$	0,5	0,14	0,04	0,01	2,5E−3	5,1E−4	1,0E−4	1,8E−5
	$\rho(R)/\lambda_4^{2R}$	192	439,2	904,6	1570,9	2578	2962,9	3069,4	2716,6
	$(\mathbf{u}\,\mathbb{P}^R v^{\downarrow})^2/\lambda_4^{2R}$	4,1	26,8	142,1	355,6	750,1	1061,6	1229,7	1016
16	$\sqrt{\rho(R)}$	0,48	0,11	0,019	4,5E−3	1,2E−3	2,8E−4	6,1E−5	1,4E−5
	$\rho(R)/\lambda_2^{2R}$	74,6	77,1	36,6	36,	50,8	46,7	37,5	36,4
	$(\mathbf{u}\,\mathbb{P}^R v^{\downarrow})^2/\lambda_2^{2R}$	48	59,5	28,2	30,4	46,5	45	36,4	35,9

Внесём некоторые пояснения: для шифра SmallPresent[2] ($n = 8$) модули доминирующих (т. е. наибольших по модулю при исключении значения $\lambda_1 = 1$) собственных значений матрицы $\mathbb{P}$ равны

$$-\lambda_2 = 0{,}267 > |\lambda_{3,4}| = 0{,}227 > \lambda_5 = 0{,}226 > |\lambda_{6,7}| = 0{,}225 >$$
$$> |\lambda_{8,9}| = 0{,}214 > |\lambda_{10,11}| = 0{,}210 > |\lambda_{12,13}| = 0{,}207.$$

У шифра SmallPresent[3] ($n = 12$) модули доминирующих собственных значений МПВР равны

$$|\lambda_{2,3}| = 0{,}220 > \lambda_4 = 0{,}192 > -\lambda_5 = 0{,}180 > |\lambda_{6,7}| = 0{,}170 >$$
$$> |\lambda_{8,9}| = 0{,}166 > |\lambda_{10,11}| = 0{,}165 > |\lambda_{12,13}| = 0{,}163,$$

доминирует сопряжённая пара $\lambda_{2,3} = 0{,}195 \pm 0{,}102i$. У МПВР шифра SmallPresent[4] ($n = 16$), как и для МПВР SmallPresent[2], в спектре

$$\lambda_2 = 0{,}237 > |\lambda_{3,4}| = 0{,}186 > |\lambda_{5,6}| = 0{,}158 >$$
$$> |\lambda_{7,8}| = 0{,}1576 > |\lambda_{9,10}| = 0{,}1572 > |\lambda_{11,12}| = 0{,}156,$$

модуль числа $\lambda_2 \in \mathbb{R}$ больше модулей комплексно сопряжённых значений $\lambda_{3,4} = -0{,}002 \pm 0{,}186i$.

Из табл. 1 видно, что при $n = 8$ и 16 картины поведения величин $k_1(R)$ похожи: значения убывают с ростом R от 48,5 и 74,6 до 27,1 и 36,4 соответственно. Выигрыши $k_2(R)$ двухвекторного критерия при $n = 8$ возрастают, постепенно приближаясь снизу к значениям $k_1(R)$, а при $n = 16$, напротив, убывают (причина этого различия пока непонятна), также постепенно сближаясь со значениями $k_1(R)$.

При $n = 12$ поведение значений $k_1(R)$ другое: они быстро возрастают с ростом R; это можно объяснить тем, что модуль первого действительного собственного значения λ_4 строго меньше величины $|\lambda_2|$. Значения $k_2(R)$ выигрыша двухвекторного критерия сначала возрастают до $R = 8$, а затем убывают, $k_2(10) = 538{,}4$.

Заметим, что при $n = 12$ сингулярные числа для $2 \leqslant R \leqslant 7$ больше соответствующих чисел, полученных при $n = 8$, и для всех исследуемых значений $2 \leqslant R \leqslant 9$ больше соответствующих чисел, полученных при $n = 16$.

Найденные сингулярные числа позволяют сравнить также характеристики разностно-сингулярных атак с многомерными разностно-спектральными атаками [10], в которых аналогом отношения сигнал/шум распределения одного слагаемого является расстояние Махаланобиса между возникающими при гипотезах H_1 и H_2 многомерными нормальными распределениями. При $n = 8$ для статистики, основанной на $r_1 = 10$ собственных векторах $\mathbb{P}$, эти расстояния приведены в табл. 2 (согласно [10, табл. 2]). Они не превосходят соответствующих сингулярных чисел при всех $4 \leqslant R \leqslant 9$ и имеют примерно тот же порядок.

Таблица 2

R	4	5	6	7	8	9
$n = 8, r_1 = 10$	0,01	2,7E–3	7,0E–4	1,8E–4	2,8E–5	7,4E–6

При $n = 12$, $r_1 = 40$ и $n = 16$, $r_1 = 11$ значения расстояний Махаланобиса приведены в табл. 3, они уже примерно на порядок меньше соответствующих сингулярных чисел. Поэтому при данных n, R даже одномерные разностно-сингулярные атаки будут эффективнее этих многомерных разностно-спектральных атак!

Таблица 3

R	6	7	8
$n = 12$, $r_1 = 40$	4,4E–4	9,3E–5	1,8E–5
$n = 16$, $r_1 = 11$	3,1E–4	6,8E–5	1,4E–5

2.2. Оценки возможностей р.-л. атак по полной кодовой книге

В табл. 4 и 5 приведены средние значения вкладов случайных R-раундовых подстановок шифров SmallPresent относительно сингулярной (для $n = 8$ и 12), двухвекторной и двух одновекторных форм (для $n = 8$) при гипотезе H_2, а также статистические оценки дисперсий по выборке из 1000 случайных подстановок. Напомним, что $\mathsf{E}_1 T = 0$, и при $n \geqslant 8$ имеем $\mathsf{D}_1 T = 0{,}50\ldots$, согласно теореме 2.

Таблица 4

SmallPresent[2], $n = 8$, $\mathsf{D}_1 T = 0{,}505$

R	Значение	Сингул.	Двухвект.	Правовект.	Левовект.
3	$\mathsf{E}_2 T$	15,2	6,02	2,4	2,4
	$\widehat{\mathsf{D}_2 T}$	0,19	0,28	0,47	0,54
4	$\mathsf{E}_2 T$	3,16	1,81	0,65	0,65
	$\widehat{\mathsf{D}_2 T}$	0,47	0,43	0,47	0,51
5	$\mathsf{E}_2 T$	0,76	0,54	0,17	0,17
	$\widehat{\mathsf{D}_2 T}$	0,54	0,51	0,49	0,49
6	$\mathsf{E}_2 T$	0,223	0,177	0,046	0,046
	$\widehat{\mathsf{D}_2 T}$	0,51	0,50	0,51	0,53

Таблица 5

SmallPresent[2], $n = 12$, $\mathsf{D}_1 T = 0{,}5003$

R	3	4	5	6	7	8	9
$\mathsf{E}_2 T$	301,7	82,9	20,9	5,13	1,05	0,205	0,037
$\widehat{\mathsf{D}_2 T}$	0,79	5,0	1,8	0,87	0,47	0,52	0,50

На рис. 1 приведены гистограммы вкладов для SmallPresent[2] при $R = 4$.

Согласно выражению (10) и табл. 4, минимальная вероятность ошибки р.-л. атаки на четыре раунда SmallPresent[2] близка к 0,01, а на пять раундов — к 0,29.

На рис. 2 приведены сглаженные гистограммы вкладов подстановок SmallPresent[3] при $R = 7$. Согласно выражению (10) и табл. 5, минимальная вероятность ошибки р.-л. атаки на шесть и семь раундов SmallPresent[3] близка к 1,4E–4 и 0,22 соответственно.

Значения $\mathsf{E}_2 T$ при $n = 16$, найденные по табл. 1 и теореме 2, приведены в табл. 6.

Таблица 6

R	3	4	5	6	7	8	9	10
$\mathsf{E}_2 T$	3,8E3	6,2E2	1,4E2	41,5	9,44	2,01	0,468	0,117

Отдельные эксперименты по оценке дисперсии при $n = 16$ из-за их большой продолжительности не проводились. При $R = 8$ на выборке объёма 20 получена оценка дисперсии 0,47. Таким образом, согласно выражению (10), минимальная вероятность

ошибки р.-л. атаки на восемь и девять раундов по одной книге SmallPresent[4] близка к 0,06 и 0,37 соответственно.

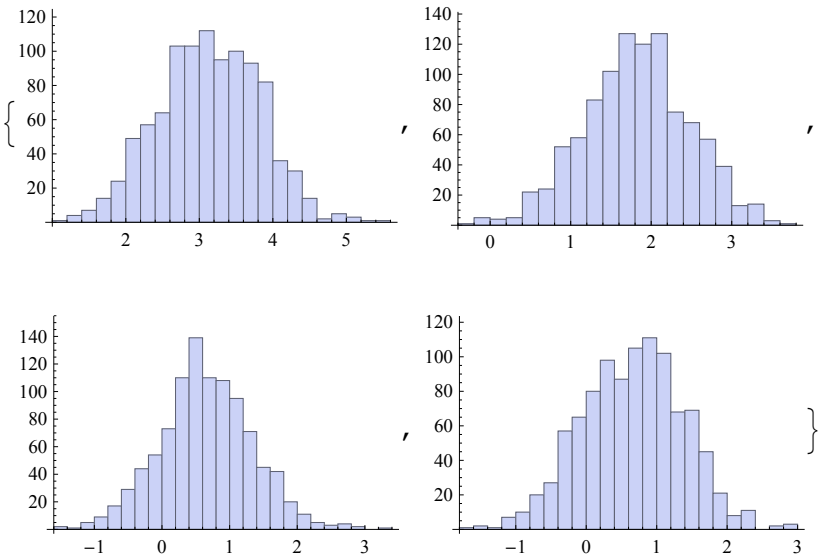

Рис. 1. Гистограммы 1000 вкладов для четырёх раундов SmallPresent[2] относительно четырёх видов линейных форм (слева направо, сверху вниз: сингулярной, двухвекторной, правовекторной и левовекторной)

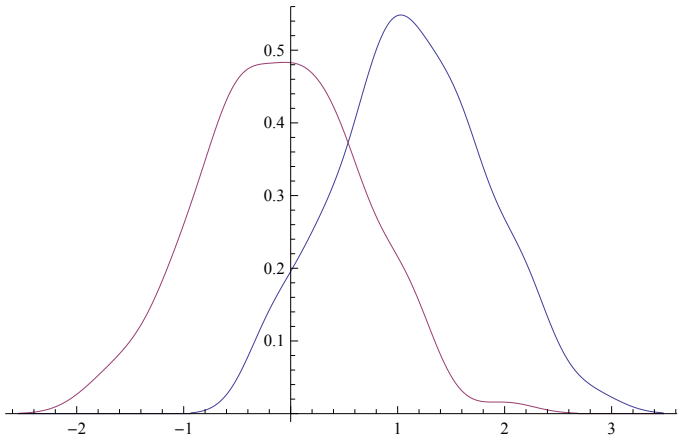

Рис. 2. Сглаженные гистограммы 100 вкладов 7-раундовых подстановок SmallPresent[3] (справа) и 100 вкладов случайных равновероятных подстановок (слева) на $\mathbb{Z}_2^{12}$ относительно сингулярной линейной формы

2.3. Экспериментальные разностно-сингулярные атаки по одной книге

Мы хотим экспериментально проверить полученные теоретически приближённые формулы для вероятностей ошибок критерия (6) и вывод о лучшей эффективности одномерных разностно-сингулярных атак по сравнению с многомерными разностно-спектральными атаками [10] на SmallPresent (расчётные вероятности ошибок $\alpha = \beta = 0{,}1$), ограничившись при этом одной книгой.

При $n = 8$ и $R = 4$ такие расчётные значения достигнуты при 1,7 кодовых книгах. Проведение $A = 100$ экспериментов на $N_b = 2$ книгах [10, табл. 2] дали значение $\hat{\alpha}_2 = 0{,}1$ эмпирической вероятности ошибки при теоретической оценке

$$\alpha_2^* = \Phi(\varkappa_{1-\alpha} - 2^{n-1/2}\sqrt{N_b}\rho_{\mathrm{Mah}}(R)),$$

согласно [10, с. 93], где $\rho_{\mathrm{Mah}}(R)$ — расстояние Махаланобиса.

Для разностно-сингулярной атаки при $\alpha = 0{,}1$ формула (8) и приведённое в табл. 4 значение $\mathsf{E}_2 T = 3{,}16$ дают оценку $\alpha_2 \approx 7{,}1\mathrm{E}{-4}$ вероятности ошибки 2-го рода атаки. Возможно, эта величина меньше точности приближения, но сейчас это несущественно. Проведённые $A = 1000$ экспериментов со случайным выбором одной книги дали следующие результаты: $\hat{\alpha}_1 = 0{,}109$, что очень близко к расчётному значению; величина $\hat{\alpha}_2 = 0$ (получено минимальное значение вклада 1,0003 при пороге 0,906 критерия (6)) значительно меньше 0,1. Таким образом, теоретически и экспериментально подтверждено, что разностно-сингулярный критерий с расчётным размером $\alpha = 0{,}1$ при работе на одной книге значительно мощнее, чем многомерный спектральный (основанный на $r_1 = 10$ собственных векторах) при работе на двух книгах. Сравнительные характеристики этого и других экспериментов представлены в табл. 7. Столбцы 3–7 — параметры многомерных спектральных атак [10, с. 104]: r_1 — количество собственных векторов; N_b — количество кодовых книг в одном эксперименте; A — число проведённых экспериментов; α_2^* — теоретическая оценка вероятности ошибки; $\hat{\alpha}_2$ — эмпирическая вероятность ошибки при гипотезе H_2. Столбцы 8–12 — аналогичные параметры проведённых разностно-сингулярных атак по одной книге. Все эксперименты показали хорошее согласие теории с практикой и преимущество разностно-сингулярных критериев.

Таблица 7

Результаты атак различения с расчётным размером $\alpha = 0{,}1$ на R раундов SmallPresent

n	R	r_1	N_b	α_2^*	A	$\hat{\alpha}_2$	$\mathsf{E}_2 T$	α_2^*	A	$\hat{\alpha}_1$	$\hat{\alpha}_2$
8	4	10	2	0,08	10^2	0,10	3,16	7,1E–4	10^3	0,109	0
	5	10	1	0,78	—	—	0,76	0,577	10^3	0,115	0,552
12	6	40	4	0,09	20	0,15	5,13	1,1E–9	10^2	0,1	0
	7	40	1	0,84	—	—	1,05	0,42	10^2	0,1	0,37
16	8	11	1	0,72	—	—	2,01	0,06	20	0,1	0,05

ЛИТЕРАТУРА

1. *Денисов О. В.* Спектральный вероятностно-статистический анализ марковских шифров // Прикладная дискретная математика. 2020. № 53. С. 12–31.
2. *Lai X., Massey J., and Murphy S.* Markov ciphers and differential cryptanalysis // LNCS. 1991. V. 547. P. 17–38.
3. *Blondeau C. and Gérard B.* Multiple differential cryptanalysis: theory and practice // LNCS. 2011. V. 6733. P. 35–54.
4. *Ланкастер П.* Теория матриц. М.: Наука, 1978.
5. *Хорн Р., Джонсон Ч.* Матричный анализ. М.: Мир, 1989.
6. *Воеводин В. В., Кузнецов Ю. А.* Матрицы и вычисления М.: Наука, 1984.
7. *Денисов О. В.* Разностные свойства случайных отображений и их композиций // Матем. вопр. криптогр. 2024. Т. 15. Вып. 1. С. 5–20.

8. *Leander G.* Small Scale Variants of the Block Cipher PRESENT. Technical University of Denmark, 2010. http://eprint.iacr.org/2010/143.pdf.
9. *Денисов О. В.* Атаки различения на блочные шифрсистемы по разностям двублочных текстов // Прикладная дискретная математика. 2020. № 48. С. 43–62.
10. *Денисов О. В.* Многомерный спектральный критерий для проверки гипотез о случайных подстановках // Матем. вопр. криптогр. 2023. Т. 14. Вып. 3. С. 85–106.

УДК 004.8 DOI 10.17223/2226308X/17/20

НАХОЖДЕНИЕ ПРООБРАЗА 44-ШАГОВОЙ ФУНКЦИИ СЖАТИЯ MD4 ПРИ ОСЛАБЛЕННОМ ПОСЛЕДНЕМ ШАГЕ[1]

О. С. Заикин

Основным компонентом криптографической хеш-функции MD4 является 48-шаговая функция сжатия. В 2007 г. прообраз 39-шаговой функции сжатия MD4 был найден с помощью CDCL — основного полного алгоритма решения проблемы булевой выполнимости (SAT). В 2022 г. с помощью параллельного SAT-алгоритма Cube-and-Conquer был найден прообраз 43-шаговой функции сжатия MD4. В настоящей работе исследуется 44-шаговая версия функции сжатия MD4, такая, что 44-й шаг ослаблен разными способами. С помощью Cube-and-Conquer найдены прообразы нескольких таких функций. На основе решённых задач предложена оценка времени, необходимого для нахождения прообраза 44-шаговой функции сжатия MD4.

Ключевые слова: *криптографическая хеш-функция, MD4, атака нахождения прообраза, логический криптоанализ, проблема булевой выполнимости, SAT.*

Введение

Криптографическая хеш-функция генерирует хеш фиксированной длины, получая на вход сообщение произвольной длины [1]. Такие функции должны быть стойкими к поиску коллизий и прообразов. Криптографические хеш-функции широко используются в современном цифровом мире. В качестве примеров можно привести хеширование паролей, проверку целостности данных и формирование электронной цифровой подписи.

Криптографическая хеш-функция MD4 предложена в 1990 г. [2]. Она генерирует 128-битный хеш, при этом функция сжатия итеративно вызывается на 512-битных блоках сообщения, каждый раз выполняя 48 шагов для смешивания этого блока со 128-битным внутренним состоянием. При этом 48 шагов разделены на три раунда по 16 шагов. В 1996 г. была опубликована практическая атака нахождения коллизий MD4 [3]. Тем не менее MD4 до сих пор является стойкой к нахождению прообраза. По этой причине в этом контексте анализируются ослабленные версии MD4, в которых несколько последних шагов функции сжатия отброшены. Первым существенным результатом в этом направлении стала практическая атака поиска прообраза 32-шаговой версии MD4, которая базировалась на Доббертиновских ограничениях [4]. Эти ограничения значительно сокращают количество прообразов для хеша, но при этом существенно упрощают соответствующую систему нелинейных уравнений.

Одним из эффективных способов анализа стойкости криптографических хеш-функций является алгебраический криптоанализ [5], согласно которому задача сводит-

[1]Работа выполнена при поддержке Математического центра в Академгородке, соглашение с Министерством науки и высшего образования Российской Федерации № 075-15-2022-282.

ся к решению системы алгебраических уравнений. Частным случаем алгебраического криптоанализа является логический криптоанализ, в котором формируются экземпляры проблемы булевой выполнимости (SAT) [6].

В 2007 г. с помощью логического криптоанализа был найден прообраз 39-шаговой функции сжатия MD4 [7]. При этом в SAT были закодированы Доббертиновские ограничения из [4], а для решения полученных экземпляров SAT использовались решатели, базирующиеся на алгоритме Conflict-Driven Clause Learning (CDCL) [8]. CDCL является основным полным SAT-алгоритмом. В последующих работах [9, 10] удалось существенно ускорить нахождение прообраза 39-шаговой функции сжатия MD4 при помощи CDCL-решателей.

В 2022 г. с помощью логического криптоанализа были найдены прообразы 43-шаговой функции сжатия MD4 [11]. При этом использовался параллельный SAT-алгоритм Cube-and-Conquer, в котором экземпляр SAT разбивается на семейство более простых экземпляров, а затем на каждом из них запускается CDCL-решатель [12]. В [11] впервые предложен алгоритм оценивания времени решения семейства подзадач при разных вариантах распараллеливания в Cube-and-Conquer. Этот алгоритм позволяет выбрать распараллеливание с лучшей оценкой.

В 2023 г. был предложен подход к ослаблению шага функции сжатия криптографической хеш-функции MD5 [13]. Рассмотрим пару последовательных шагов функции сжатия с номерами i и $i+1$, $1 \leqslant i \leqslant 63$. Первые i шагов работают как обычно, а на шаге $i+1$ вместо 32-битной части блока сообщения используется 32-битное слово, в котором j, $1 \leqslant j \leqslant 31$, битов равны соответствующим j битам части блока сообщения, а остальные $32-j$ битов равны нулю. При этом с возрастанием значения j возрастает и сложность соответствующих экземпляров SAT для современных решателей.

1. Ослабление шага функции сжатия MD4

Рассмотрим псевдокод шага функции сжатия MD4:

$$\begin{aligned} upd &\leftarrow (a + F(b,c,d) + M[t] + K) \lll s) \\ a &\leftarrow d \\ d &\leftarrow c \\ c &\leftarrow b \\ b &\leftarrow upd \end{aligned}$$

Здесь a, b, c, d — перестановка значений четырёх 32-битных регистров внутреннего состояния; F — выдающая 32-битное слово функция; $M[t]$ — 32-битное слово, являющееся t-й частью блока сообщения M, $0 \leqslant t \leqslant 15$; K — 32-битная константа; $+$ — сложение по модулю 2^{32}; $\lll$ — циклический сдвиг влево; s — целое число. При этом для каждого из 48 шагов задаются перестановка a, b, c, d и значения t и s, а F и K задаются для каждого раунда.

По аналогии с MD5, псевдокод модифицированного $(i+1)$-го шага для j-й ослабленной функции сжатия MD4 выглядит следующим образом:

$$\begin{aligned} l &\leftarrow 32 - j \\ weakM &\leftarrow (M[t] \ll l) \gg l \\ upd &\leftarrow (a + F(b,c,d) + weakM + K) \lll s) \\ a &\leftarrow d \\ d &\leftarrow c \end{aligned}$$

$$c \leftarrow b$$
$$b \leftarrow upd$$

В результате в j-й функции сжатия $32 - j$ старших битов $weakM$ равны 0, а оставшиеся j младших битов равны j младшим битам $M[t]$.

2. Нахождение прообраза с помощью Cube-and-Conquer при ослабленном 44-м шаге функции сжатия MD4

С помощью программы Transalg [14] были построены экземпляры SAT для задачи поиска прообраза единичного хеша 44-шаговой функции сжатия MD4, в которой при ослаблении 44-го шага j варьировалось от 1 до 31.

С помощью подхода из работы [11] построены оценки времени решения на компьютере с 16-ядерным процессором для следующих значений j: 2, 4, 6, 8, 10, 12. В качестве CDCL-решателя использовался Kissat версии 3.0 [15]. Для $j = 12$ оценку построить не получилось из-за того, что соответствующие подзадачи оказались слишком сложными. Для остальных упомянутых значений j оценки построены успешно, они представлены в днях в таблице.

j	Время решения, дн.
2	6,99
4	16,46
6	105,26
8	658.29
10	1786,6

Для $j = 2$ и 4 прообразы были найдены на компьютере, при этом реальное время оказалось близким к оценкам. С помощью линейной экстраполяции был построен прогноз для $j = 32$, т. е. для поиска прообраза 44 полных шагов функции сжатия MD4. Оказалось, что на упомянутом компьютере для этого необходимо около 21 млн лет. Из этих результатов следует, что для нахождения прообраза 44-шаговой функции сжатия MD4 необходимы новые алгоритмы. С другой стороны, в рамках настоящего исследования найдены прообразы для более сложной функции сжатия MD4, чем было опубликовано ранее.

ЛИТЕРАТУРА

1. *Алферов А. П., Зубов А. Ю., Кузьмин А. С., Черемушкин А. В.* Основы криптографии. 2-е изд. М.: Гелиос АРВ, 2002.
2. *Rivest R.* The MD4 message digest algorithm // LNCS. 1991. V. 537. P. 303–311.
3. *Dobbertin H.* Cryptanalysis of MD4 // LNCS. 1996. V. 1039. P. 53–69.
4. *Dobbertin H.* The first two rounds of MD4 are not one-way // LNCS. 1998. V. 1372. P. 284–292.
5. *Bard G.* Algebraic Cryptanalysis. N.Y.: Springer, 2009.
6. *Massacci F. and Marraro L.* Logical cryptanalysis as a SAT problem // J. Automated Reasoning. 2000. V. 1. P. 165–203.
7. *De D., Kumarasubramanian A., and Venkatesan R.* Inversion attacks on secure hash functions using SAT solvers // LNCS. 2007. V. 4501. P 377–382.
8. *Marques-Silva J. and Sakallah K.* GRASP: a search algorithm for propositional satisfiability // IEEE Trans. Comput. 1999. V. 48(5). P. 506–521.

9. *Грибанова И. А.* Новый алгоритм порождения ослабляющих ограничений в задаче обращения хеш-функции MD4-39 // Прикладная дискретная математика. Приложение. 2018. № 11. С. 139–141.
10. *Gribanova I. and Semenov A.* Using automatic generation of relaxation constraints to improve the preimage attack on 39-step MD4 // Proc. MIPRO. IEEE, 2018. P. 1174–1179.
11. *Zaikin O.* Inverting 43-step MD4 via Cube-and-Conquer // Proc. IJCAI-ECAI. Vienna, 2022. P. 1894–1900.
12. *Heule M. J. H., Kullmann O., Wieringa S., and Biere A.* Cube and Conquer: guiding CDCL SAT solvers by lookaheads // LNCS. 2012. V. 7261. P. 50–65.
13. *Заикин О. С.* Обращение 29-шаговой функции сжатия MD5 при помощи алгоритмов решения проблемы булевой выполнимости // Прикладная дискретная математика. Приложение. 2023. № 16. С. 37–40.
14. *Semenov A., Otpuschennikov I., Gribanova I., et al.* Translation of algorithmic descriptions of discrete functions to SAT with application to cryptanalysis problems // Logical Methods Comput. Sci. 2020. V. 16. Iss. 1. P. 29:1–29:42.
15. *Biere A. and Fleury M.* Gimsatul, IsaSAT and Kissat entering the SAT Competition 2022 // Proc. SAT Competition 2022. Solver and Benchmark Descriptions. P. 10–11.

УДК 004.056.5 DOI 10.17223/2226308X/17/21

АЛГОРИТМ БЫСТРОЙ ВЫРАБОТКИ КЛЮЧЕВОЙ ПОСЛЕДОВАТЕЛЬНОСТИ С ИСПОЛЬЗОВАНИЕМ КВАНТОВОГО КАНАЛА СВЯЗИ

С. Ю Казанцев, К. Н. Панков

Предложен способ быстрой выработки ключевой последовательности большого объёма с помощью квантового канала связи и открытого канала. По открытому каналу связи, доступному всем пользователям, передаётся последовательность независимых одинаково распределённых бит, выработанных квантовым генератором случайных чисел, а по квантовому каналу — информация о способе выбора бит из этой последовательности. Приведены оценки количества попыток перебора противником ключевых последовательностей и вероятности совпадения этих последовательностей у разных пользователей.

Ключевые слова: *квантовая криптография, информационная безопасность, передача ключевой информации, квантовый канал связи, квантовый генератор случайных чисел.*

В рамках концепции Четвёртой промышленной революции К. Шваба [1] и национальной программы «Цифровая экономика Российской Федерации» [2] можно выделить набор основных или сквозных технологий, к числу которых, в частности, относятся квантовые технологии. В соответствии с [3], они включают в качестве субтехнологии [4] квантовые коммуникации, представляющие собой технологию криптографической защиты информации, использующую для передачи ключей индивидуальные квантовые частицы. Квантовые коммуникации часто отождествляются с квантовой криптографией, хотя с точки зрения многих исследователей последнее понятие гораздо шире [5, 6]. В соответствии с определениями, включёнными в проект национального стандарта по терминологии в области криптографии [7], квантовые коммуникации относятся к криптографическим методам защиты информации, а более ранние способы классификации часто относили их к инженерно-физическим методам.

Квантовые коммуникации, в том числе и как способ обеспечения информационной безопасности, в настоящее время являются предметом, которому посвящено большое количество публикаций, для части которых приведён обзор в работе [6]. Летом 2023 г. в рамках Форума будущих технологий, который получил название «Вычисления и связь. Квантовый мир», был представлен доклад [8], в котором квантовые коммуникации и постквантовая криптография [9, 10], иначе называемая квантово-устойчивой [11], выделены в отдельное перспективное направление квантовых технологий, названное квантовой защитой информации. По мнению авторов, более корректно было бы отнести к данному направлению всю квантовую криптографию, включающую, к примеру, квантовую генерацию ключевой информации и квантовые аналоги традиционных криптографических механизмов и систем [11].

Как известно, безопасность протоколов передачи ключей в квантовых коммуникациях опирается на постулаты квантовой механики [12, 13]. К сожалению, в отличие от существующей инфраструктуры передачи ключей по открытым каналам связи с помощью классических алгоритмов криптографии с открытым ключом, линии квантового распределения ключа (без усилителей) обладают ограничением по расстоянию. Например, в 2023 г. китайскими исследователями как значительное достижение было объявлено об успешном создании системы квантового распределения ключей (КРК) на расстоянии 1,002 км [14]. Чем длиннее квантовая линия, тем ниже скорость выработки общего ключа, что иллюстрируется графиком на рис. 1 из работы [15], в которой приведены вычислительные формулы для нахождения этой скорости, зависящие от ряда физических параметров.

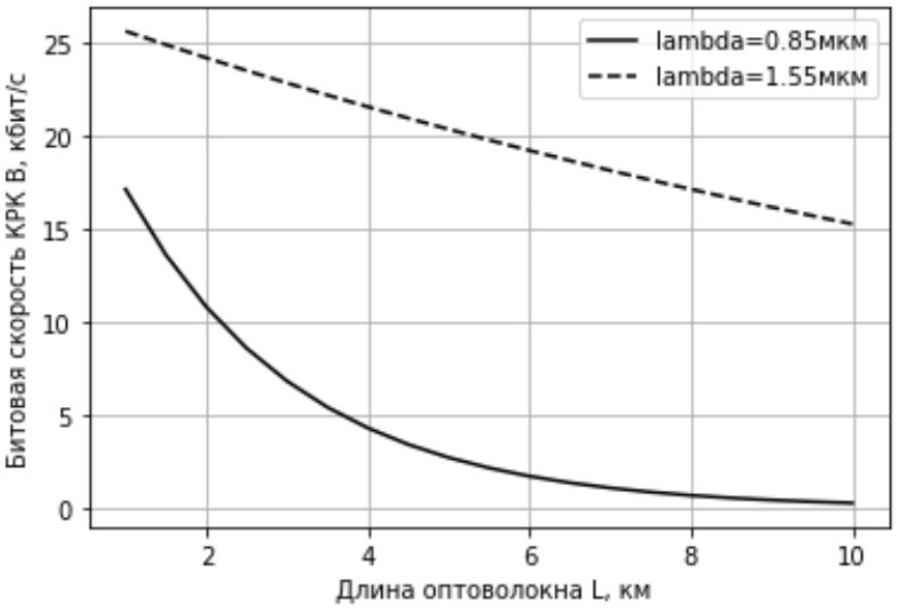

Рис. 1. Зависимость битовой скорости формирования ключа в квантовой линии от длины волоконно-оптической линии (lambda – длина волны источника фотонов) [15]

Можно привести пример для реализованной в настоящее время промышленной системы: скорость выработки ключей в системе КРК ViPNet Quandor 2 от Infotecs на расстояние до 100 км объявлена от 256 бит/мин [16].

Более того, на данную скорость значительное влияние оказывает среда передачи квантового сигнала, например атмосфера [17]. Поэтому актуальна задача разработ-

ки на базе существующих систем квантовой коммуникации комплексов, позволяющих обеспечить более быструю передачу ключевой информации.

К сожалению, если ключевая последовательность имеет значительную длину (при гаммировании или в шифре Вернама), распространённые системы КРК [18] не являются подходящими для её формирования и передачи в силу малой скорости работы. Аналогичные проблемы могут возникнуть при реализации концепции шифрования каждого IP-пакета на индивидуальном ключе, когда для передачи большого количества конфиденциальной информации требуется передать также значительный объём ключевой информации. Последний подход используется, например, в аппаратно-программном комплексе шифрования «Континент. Версия 3.7» от «Кода безопасности». Поэтому рассмотрим способ формирования ключевой последовательности заданной длины при наличии квантового канала связи с малой битовой скоростью. Для этого воспользуемся квантовым генератором случайных чисел (КГСЧ) [19]. Ключевая последовательность, выработанная этим КГСЧ, передаётся в эфир или оптоволоконную линию связи. Также построим на базе квантового канала связи систему прямой защищённой передачи информации. Одним из примеров подобной системы является схема, предложенная в [20].

Алгоритм передачи ключевой информации основывается на том, что КГСЧ порождает истинно случайную последовательность [19]. Таким образом, в открытый канал связи, доступный всем пользователям системы, поступают значения последовательности независимых одинаково распределённых случайных величин $\xi_1, \xi_2, \xi_3, \ldots$, где $\mathsf{P}[\xi_i = 0] = \mathsf{P}[\xi_i = 1] = 1/2$. В соответствии с [19], скорость генерации такой последовательности достигает 160 Мбит/с. Для повышения надёжности системы будем считать, что данные в канал связи передаются с использованием помехоустойчивого кодирования, что снижает скорость передачи информации (в зависимости от скорости кода) [21]. Используя помехоустойчивое кодирование, описанное в [22], и добавляя в последовательность служебные группы символов (через каждые N бит), мы получаем скорость 80 Мбит/с. Таким образом, каждый пользователь линии связи получает информацию $\ldots, \tau_j, \xi_{\tau_j,1}, \ldots, \xi_{\tau_j,N}, \tau_{j+1}, \xi_{\tau_{j+1},1}, \ldots$ Можно считать, что N — это 10^6 или 10^9. Точное значение N должно выбираться при реализации системы с учётом удобства пользователей и необходимости минимизации количества информации, которую нужно будет передать через построенную на базе квантового канала связи систему прямой защищённой передачи информации.

Пользователь Алиса для выработки общего ключа с пользователем Бобом (будем считать, что пользователи для передачи сообщения после получения ключа будут использовать гаммирование, которое в нашем случае становится абсолютно стойким шифром Вернама) по квантовому каналу связи (например, используя алгоритм из [20] либо любой другой подходящий) передаёт следующую информацию:

1) номер j служебной группы символов τ_j, после которой из эфира будет считываться ключевая последовательность (гамма);
2) номер бита k, $k \in \{1, \ldots, N\}$, после τ_j, начиная с которого будет считываться ключевая последовательность (т. е. первый бит гаммы — это $\xi_{\tau_j,k}$);
3) период считывания s (предполагается, что биты гаммы могут считываться не подряд, а следующим образом: $\xi_{\tau_j,k}, \xi_{\tau_j,k+s}, \xi_{\tau_j,k+2s}, \ldots$);
4) длину ключевой последовательности.

Получив данную информацию, Боб считывает ключевую последовательность из эфира и проверяет её качество, например по методике [19]. Если получившаяся после-

довательность не удовлетворяет критериям качества, Боб сообщает об этом Алисе и связь не состоится, в противном случае он сообщает о готовности к связи и принимает предназначенное ему сообщение.

Рассмотрим возможные действия противника по перехвату передаваемой информации. Будем считать, что информация, передаваемая по квантовому каналу связи, противнику недоступна, что является естественным предположением в условиях функционирования квантового канала связи. Однако в памяти противника хранится вся информация, передаваемая по открытому каналу связи со скоростью υ. Предположим, что он, наблюдая за Алисой, установил, что она начала выполнение алгоритма с Бобом и Боб сообщил ей о готовности к получению информации. Время, которое прошло между этими событиями, обозначим через T. Также будем предполагать, что противнику известна длина передаваемой ключевой последовательности.

Утверждение 1. В описанных предположениях, если $k = s = 1$, то противнику понадобится перебрать не более $[\upsilon T/N] + 1$ вариантов ключевой последовательности.

Утверждение 2. В описанных предположениях, если $s = 1$, k — любое допустимое значение, то противнику понадобится перебрать не более $([\upsilon T/N] + 1)\, N$ вариантов ключевой последовательности.

Утверждение 3. В описанных предположениях, если противник не обладает информацией о параметрах ключевой последовательности, то ему понадобится перебрать не более $([\upsilon T/N] + 1)\, N^2$ вариантов ключевой последовательности.

Стратегию противника можно связать с задачей извлечения секретного ключа из случайно выбранного подмножества [23].

Утверждение 4. В описанных предположениях, если два пользователя системы Алиса$_1$ и Алиса$_2$ решили передать ключевую информацию пользователям Боб$_1$ и Боб$_2$ соответственно в одно и то же время (это возможно в случае большого числа пользователей системы) и готовы ждать установления связи с ними t_1 и t_2 времени каждый, то вероятность того, что у них совпадёт ключевая информация, не превосходит $([\upsilon \min(t_1, t_2)/N] + 1)^{-2}\, N^{-4}$.

Таким образом, предложен алгоритм, который позволяет использовать преимущества квантового канала связи, связанные с его физической защищённостью, и обойти такой его недостаток, как небольшая скорость формирования ключа. Для алгоритма требуется наличие открытого высокоскоростного канала связи, в котором передаются значения последовательности независимых сбалансированных битовых случайных величин, выработанных квантовым генератором случайных чисел.

Предложенный алгоритм может быть реализован на существующей элементной базе, поскольку компания Infotecs производит в настоящее время соответствующий квантовый генератор случайных чисел [19], а модель квантовой линии связи реализована в виде программного комплекса, применяемого в электронных коммутационных устройствах, разрабатываемых ООО «Кьювуд» в интересах проекта Сейфнет НТИ РФ, и апробирована на площадке киберполигона ИТЦ «Ингрия» (Санкт-Петербург) в 2022 г. [20].

Предложенный алгоритм может быть модифицирован, например, при использовании в качестве линии связи многосердцевинного волокна, в отдельных каналах которого передаются свои последовательности случайных бит.

ЛИТЕРАТУРА

1. *Шваб К.* Технологии четвертой промышленной революции. М.: Эксмо, 2022, 320 с.
2. Паспорт национальной программы «Цифровая экономика Российской Федерации». http://government.ru/info/35568/.
3. Дорожная карта развития «сквозной» цифровой технологии «Квантовые технологии». https://digital.gov.ru/uploaded/files/07102019kvantyi.pdf. 2019.
4. *Панков К. Н., Эйнман А. Д.* Сертификация систем распределенного реестра как инструмент обеспечения информационной безопасности // REDS: Телекоммуникационные устройства и системы. 2021. Т. 11. № 2. С. 37–49.
5. *Корольков А. В.* О некоторых прикладных аспектах квантовой криптографии в контексте развития квантовых вычислений и появления квантовых компьютеров // Вопросы кибербезопасности. 2015. № 1(9). С. 6–13.
6. *Панков К. Н., Миронов Ю. Б.* Применение квантовых методов в задачах защиты информации. М.: Горячая линия-Телеком, 2022. 212 с.
7. Предварительный национальный стандарт Российской Федерации ПНСТ799-2022. Информационные технологии. Криптографическая защита информации. Термины и определения. М.: Российский институт стандартизации, 2022. 50 с.
8. Квантовые технологии для государства и бизнеса: настоящее и будущее. https://roscongress.org/upload/medialibrary/4b2/29ivbrarcw5pr4m3macgwra2p1kx2c1y/FTF23_bookA4_05_preview.pdf. 2023.
9. *Pankov K. N. and Glukhov M. M.* Using error-correcting codes to ensure information security of unmanned vehicles and IoT systems // Systems of Signal Synchronization, Generating and Processing in Telecommunications. 2022. V. 5. No. 1. P. 240–247.
10. *Pankov K. N. and Glukhov M. M.* Estimation of the power of algebraic geometric codes designed to construct a post-quantum algorithm for ensuring information security of on-board systems // Systems of Signal Synchronization, Generating and Processing in Telecommunications. 2023. V. 6. No. 1. P. 355–359.
11. *Панков К. Н., Миронов Ю. Б.* Использование постквантовых алгоритмов в задачах защиты информации в телекоммуникационных системах. М.: Горячая линия-Телеком, 2023. 236 с.
12. *Арбеков И. М.* Элементарная квантовая криптография: Для криптографов, не знакомых с квантовой механикой. М.: ЛЕНАНД, 2022. 168 с.
13. *Панков К. Н.* Оценки мощности классов отображений, применяемых в протоколах квантового распределения ключей // Наукоемкие технологии в космических исследованиях Земли. 2022. Т. 14. № 4. С. 4–18.
14. *Liu Y., Zhang W.-J., Jiang C., et al.* Experimental twin-field quantum key distribution over 1000 km fiber distance // Phys. Rev. Lett. 2023. V. 130. Iss. 21. P. 210801.
15. *Поляков А. В.* Скорость формирования квантового распределения ключа в волоконно-оптических системах квантовой криптографии // Квантовая электроника: Материалы XIII Междунар. науч.-технич. конф. Минск, 22–26 ноября 2021 г. Минск: БГУ, 2021. С. 275–279.
16. ViPNet Quandor 2. Квантовая криптографическая система выработки и распределения ключей с топологией «точка-точка». Infotecs. https://infotecs.ru/products/vipnet-quandor-2/.
17. *Бахус А. В., Ерохин К. Ю., Казанцев С. Ю.* Влияние фона на передачу квантового ключа в свободной атмосфере, реализованной на терминалах АОЛС М1-40GE // XIII Междунар. конф. по фотонике и информационной оптике. Москва, 24–26 января 2024 г. М.: МИФИ, 2024. С. 465–466.

18. *Казиева Т. В., Трофимов Н. С., Казанцев С. Ю. и др.* Обзор промышленных систем КРК и их компонентной базы // Невская фотоника-2023: Всерос. науч. конф. Санкт-Петербург, 09–13 октября 2023 г. С.-Пб.: ИТМО, 2023. С. 228.
19. *Арбеков И. М., Молотков С. Н.* Об экстракции квантовой случайности // УФН. 2021. Т. 191. № 6. С. 651–669.
20. *Воробьева Д. Е.* Передача информации в квантовом канале связи // Известия СПбГЭТУ «ЛЭТИ». 2023. Т. 16. № 9. С. 77–82.
21. *Безуглов Д. А., Лыков А. П., Киреев Д. Г. и др.* Исследование параметров помехоустойчивого кодирования при анализе космических систем связи // Современные проблемы науки и образования. 2012. № 6. С. 63.
22. *Золотарев В. В., Овечкин Г. В.* Применение многопороговых методов декодирования помехоустойчивых кодов в высокоскоростных системах передачи данных // Электросвязь. 2014. № 12. С. 10–14.
23. *Cachin C.* Entropy Measures and Unconditional Security in Cryptography. PhD Thesis. ETH Zurich, 1997.

УДК 003.26 DOI 10.17223/2226308X/17/22

АТАКА РАЗЛИЧЕНИЯ НА ОДИН РЕЖИМ РАБОТЫ БЛОЧНЫХ ШИФРОВ ПРИ НАЛИЧИИ У НАРУШИТЕЛЯ ДОСТУПА К КВАНТОВОМУ ОРАКУЛУ

А. М. Коренева, Г. В. Фирсов

В 2022 г. в Российской Федерации приняты рекомендации по стандартизации, определяющие режим работы блочных шифров DEC, используемый для защиты носителей информации с блочно-ориентированной структурой. Данный режим представляет собой модификацию режима гаммирования со специальным алгоритмом выработки синхропосылки и начальным значением счётчика из номера раздела и номера сектора носителя информации. В работе представлена модель доказуемой (редукционистской) стойкости, формализующая обеспечение конфиденциальности в условиях наличия у нарушителя доступа к квантовому оракулу. В рамках данной модели предложена атака различения на режим DEC, требующая единственный запрос к оракулу. Атака основана на возможности перехода к незапутанному состоянию регистров открытого и шифрованного текстов в случае зашифрования непосредственно открытого текста, переданного нарушителем, и невозможности такого перехода при зашифровании результата применения случайной подстановки к открытому тексту.

Ключевые слова: *полнодисковое шифрование, режим работы блочных шифров, симметричная криптография, криптографическая защита информации, носители информации с блочно-ориентированной структурой.*

1. Предварительные сведения

Кубит (единица информации в квантовом компьютере) описывается квантовым состоянием $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$, где $\alpha, \beta \in \mathbb{C}$ таковы, что $|\alpha|^2 + |\beta|^2 = 1$, а векторы $|0\rangle$ и $|1\rangle$ образуют ортонормированный базис в двумерном гильбертовом пространстве $\mathcal{H}$ над $\mathbb{C}$ [1, 2]. Квантовый регистр длины n описывается тензорным произведением состояний отдельных кубитов: $|\psi_1\rangle \otimes \cdots \otimes |\psi_n\rangle$, которое для краткости будем записывать как $|\psi_1\rangle \cdots |\psi_n\rangle$ или, если длина регистра ясна из контекста, как $|\psi\rangle$.

Состояние $|\psi\rangle$ переходит в состояние $|\varphi\rangle$ (в общем случае отличное от $|\psi\rangle$) при воздействии на него унитарного оператора U, что записывается следующим образом: $|\varphi\rangle = U|\psi\rangle$. Пусть $n \geqslant 1$, $U : \mathcal{H} \to \mathcal{H}$, $|\psi\rangle \in \mathcal{H}^{\otimes n}$, где $\mathcal{H}$ — некоторое гильбертово пространство. Воздействие оператора $U^{\otimes n}$ на состояние $|\psi\rangle$ будем для краткости записывать, опуская тензорную степень оператора: $U|\psi\rangle$.

Состояние $|\psi\rangle \in \mathcal{H}_1 \otimes \mathcal{H}_2$ называется запутанным, если для любых $|\psi_1\rangle \in \mathcal{H}_1$ и $|\psi_2\rangle \in \mathcal{H}_2$ выполнено $|\psi\rangle \neq |\psi_1\rangle \otimes |\psi_2\rangle$.

Через V_m обозначим множество двоичных строк длины $m \in \mathbb{N}$, V^* — множество двоичных строк конечной длины. Пусть $x \in V_m$, $y \in V_k$, обозначим результат конкатенации строк x и y через $x||y$, при этом $x||y \in V_{m+k}$. Через $\mathrm{S}(X)$ обозначим множество подстановок на множестве X.

Симметричным шифром $\mathcal{E}$ называется семейство функций $E : \mathcal{K} \times \mathcal{M} \to \mathcal{C}$, где $\mathcal{K}$ — ключевое множество; $\mathcal{M}$ — множество открытых текстов; $\mathcal{C}$ — множество шифртекстов. При этом множества $\mathcal{K}$, $\mathcal{M}$ и $\mathcal{C}$ не пустые. Для краткости будем $E(K, \cdot)$ записывать как $E_K(\cdot)$ для $K \in \mathcal{K}$. Функция E называется функцией зашифрования шифра $\mathcal{E}$. Для каждого $K \in \mathcal{K}$ функция $E_K(\cdot)$ является обратимой. Для шифра $\mathcal{E}$ выполняется свойство корректности, т. е. для любых $K \in \mathcal{K}$ и $m \in \mathcal{M}$ верно равенство $E_K^{-1}(E_K(m)) = m$, где $E_K^{-1}(\cdot)$ — обратная к $E_K(\cdot)$ функция.

Блочный шифр — симметричный шифр, в котором $\mathcal{M} = \mathcal{C} = V_l$, где $l \in \mathbb{N}$ называется длиной блока.

Настраиваемый симметричный шифр $\tilde{\mathcal{E}}$ — семейство функций $\tilde{E} : \mathcal{K} \times \mathcal{T} \times \mathcal{M} \to \mathcal{C}$, где $\mathcal{T}$ — непустое множество настроек (или модификаторов). Будем $\tilde{E}(K, \cdot, \cdot)$ записывать как $\tilde{E}_K(\cdot, \cdot)$ для $K \in \mathcal{K}$. Функция $\tilde{E}$ называется функцией зашифрования шифра $\tilde{\mathcal{E}}$ и является обратимой при любых $K \in \mathcal{K}$ и $T \in \mathcal{T}$. Для шифра $\tilde{\mathcal{E}}$ выполняется свойство корректности, т. е. для любых $K \in \mathcal{K}$, $T \in \mathcal{T}$ и $m \in \mathcal{M}$ верно равенство $\tilde{E}_K^{-1}(T, \tilde{E}_K(T, m)) = m$, где $\tilde{E}_K^{-1}(T, \cdot)$ — обратная к $\tilde{E}_K(T, \cdot)$ функция, называемая функцией расшифрования шифра $\tilde{\mathcal{E}}$.

Настраиваемый симметричный шифр с состоянием $\underline{\tilde{\mathcal{E}}}$ — кортеж $(\tilde{\mathcal{E}}, S, U, s_0)$, где $\tilde{\mathcal{E}}$ — настраиваемый симметричный шифр; $S : \mathcal{T}_{\text{out}} \times \mathcal{S} \to \mathcal{T}$ — функция выработки настройки для шифра $\tilde{\mathcal{E}}$; $U : \mathcal{K} \times \mathcal{T}_{\text{out}} \times \mathcal{S} \to \mathcal{S}$ — функция обновления состояния; $s_0 \in \mathcal{S}$ — начальное состояние; $\mathcal{S}$ — множество состояний; $\mathcal{T}_{\text{out}}$ — множество настроек шифра $\underline{\tilde{\mathcal{E}}}$; $\mathcal{T}$ — множество настроек шифра $\tilde{\mathcal{E}}$. Множества открытых текстов $\mathcal{M}$, шифртекстов $\mathcal{C}$ и ключей $\mathcal{K}$ шифра $\underline{\tilde{\mathcal{E}}}$ совпадают с соответствующими множествами для шифра $\tilde{\mathcal{E}}$. Функция зашифрования $\underline{\tilde{E}} : \mathcal{K} \times \mathcal{T}_{\text{out}} \times \mathcal{M} \to \mathcal{C}$ шифра $\underline{\tilde{\mathcal{E}}}$ функционирует следующим образом: шифртекст вычисляется при помощи функции зашифрования шифра $\tilde{\mathcal{E}}$ с использованием значения $S(T_{\text{out}}, s_{i-1})$ в качестве настройки, где $T_{\text{out}} \in \mathcal{T}_{\text{out}}$, s_{i-1} — текущее состояние, после чего производится обновление состояния: $s_i = U(K, T_{\text{out}}, s_{i-1})$, где s_i — новое состояние. Частично применённая функция $\underline{\tilde{E}}_K(T_{\text{out}}, \cdot)$ является обратимой для каждого $K \in \mathcal{K}$, каждого $T_{\text{out}} \in \mathcal{T}_{\text{out}}$ и при любом текущем состоянии, а обратная функция, называемая функцией расшифрования, обозначается $\underline{\tilde{E}}_K^{-1}(T_{\text{out}}, \cdot)$. Состояния в функциях зашифрования и расшифрования изменяются независимо друг от друга. Шифр удовлетворяет свойству корректности: для любых $K \in \mathcal{K}$, $T_{\text{out}} \in \mathcal{T}_{\text{out}}$ и $m \in \mathcal{M}$ при совпадении текущих состояний функций зашифрования и расшифрования верно равенство $\underline{\tilde{E}}_K^{-1}(T_{\text{out}}, \underline{\tilde{E}}_K(T_{\text{out}}, m)) = m$.

Следует также ввести некоторые определения, касающиеся шифрования дисков. Независимо от физической реализации, логически носитель информации (диск) состоит из разделов, которые, в свою очередь, состоят из секторов. Сектором является

наименьший последовательный массив данных, который читается с диска или записывается на него. Размер сектора в блоках обозначим через $n \in \mathbb{N}$.

Режим DEC определяется в [3]. Пусть $\mathcal{E}$ — блочный шифр; $E : \mathcal{K} \times V_l \to V_l$ — функция зашифрования, где l — длина блока шифра $\mathcal{E}$; $PN \in \mathbb{Z}_{2^{l/2}}$ и $SN \in \mathbb{Z}_{2^{l/2}}$ — номера раздела и сектора соответственно. Блочный шифр $\mathcal{E}$ в режиме DEC является настраиваемым симметричным шифром с состоянием. Внутренним состоянием является набор счётчиков, ассоциированных с каждым разделом и с каждым сектором. Изначально все счётчики равны нулю. Функция S возвращает счётчик $\mathrm{cnt}_{PN} \in \mathbb{Z}_{2^{l/2}}$, ассоциированный с разделом PN, и счётчик $\mathrm{cnt}_{SN,PN} \in \mathbb{Z}_{2^{l/2}}$, ассоциированный с сектором SN в разделе PN. Функция U увеличивает счётчик $\mathrm{cnt}_{SN,PN}$ на 1 и если в результате получен 0 (что возможно, так как операция сложения выполняется в кольце вычетов по модулю $2^{l/2}$), то увеличивает на 1 счётчик cnt_{PN}. Функция зашифрования блочным шифром $\mathcal{E}$ в режиме DEC на ключе K определена в [3]. Важным в контексте настоящей работы является факт, что шифртекст можно выразить в виде $c = m \oplus \gamma$, где $m, c, \gamma \in V_{nl}$; $\gamma = \gamma(K, SN, PN)$ — двоичная строка, выработанная из номеров раздела и сектора по алгоритму, описанному в [3].

2. Используемая модель редукционистской стойкости

С целью формализации обеспечения свойства конфиденциальности настраиваемым симметричным шифром с состоянием в условиях доступа нарушителя к квантовому оракулу дадим формальное определение модели qROP-qfdeCPA (Real Or Permutation Indistinguishability under Chosen Plaintext Attack with FDE restrictions and access to stateful quantum oracle). Префиксы «q» в названии модели обозначают, что как нарушитель, так и экспериментатор имеют доступ к квантовому вычислителю, нижнее подчеркивание означает наличие внутреннего состояния у экспериментатора. Данная модель основывается на учитывающей особенности полнодискового шифрования модели неразличимости из [4], но допускает квантовые запросы к оракулу. Задачей нарушителя является различение открытых текстов, шифруемых с помощью анализируемого шифра, а не различение шифра и случайной подстановки. Пусть $\underline{\tilde{\mathcal{E}}}$ — настраиваемый симметричный шифр с состоянием, для которого $\mathcal{M} \subseteq V^*$, и $b \in \{0, 1\}$ выбирается равновероятно. Значение b не известно нарушителю $\mathcal{A}$. Экспериментатор **Exp** (оракул зашифрования) равновероятно выбирает ключ $K \in \mathcal{K}$ для шифра $\underline{\tilde{\mathcal{E}}}$. Нарушитель совершает некоторое количество запросов к оракулу вида

$$|\mathcal{L}_i\rangle|m_i\rangle,$$

где $i \geqslant 1$ — порядковый номер запроса; $\mathcal{L}_i \in \mathcal{T}_{\text{out}}$ — расположение на носителе информации (например, номер сектора и/или раздела диска); $m_i \in \mathcal{M}$ — открытый текст. На i-й запрос нарушитель получает от оракула ответ вида

$$\big|\mathcal{L}_i\big\rangle\big|m_i\big\rangle\big|\underline{\tilde{E}}_K\left(\mathcal{L}_i, \omega_i^b(m_i)\right)\big\rangle, \tag{1}$$

где ω_i — равновероятно выбранная из $\mathrm{S}(V_{|m_i|})$ подстановка; $\omega_i^0 = e$ — тождественная подстановка. Заметим, что при $b = 0$ зашифровывается непосредственно открытый текст m_i, а при $b = 1$ — результат применения подстановки ω_i к открытому тексту m_i. На рис. 1 схематично изображён процесс формирования экспериментатором **Exp** ответа на i-й запрос нарушителя $\mathcal{A}$. Через f обозначено зашифрование шифром $\underline{\tilde{\mathcal{E}}}$ значения $\omega_i^b(m_i)$, согласно (1), где использование состояния s_{i-1} и его обновление учтены неявно. Реализующий данное преобразование оператор обозначен через U_f.

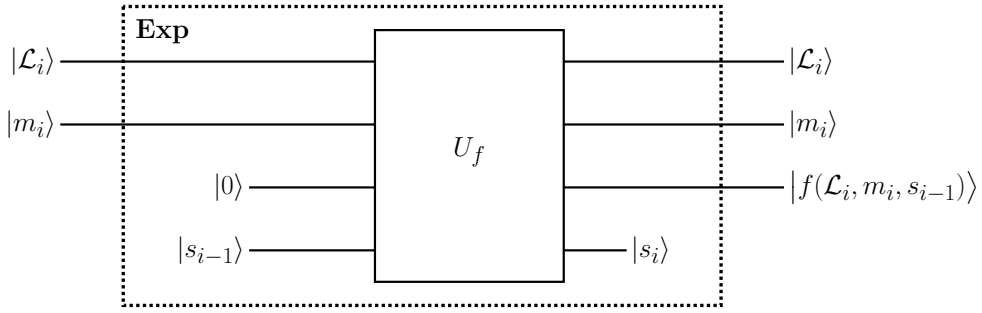

Рис. 1. Схема процесса формирования экспериментатором **Exp** ответа на i-й запрос нарушителя $\mathcal{A}$

Для запросов нарушителя справедливо

$$i \neq j \implies (\mathcal{L}_i, m_i) \neq (\mathcal{L}_j, m_j).$$

На основании полученных данных нарушитель возвращает значение $b' \in \{0, 1\}$ (будем писать $\mathcal{A} \Rightarrow b'$). Преобладанием нарушителя $\mathcal{A}$ называется величина

$$\mathbf{Adv}_{\tilde{\mathcal{E}}}^{\text{qROP-qfdeCPA}}(\mathcal{A}) = \Pr[\mathcal{A} \Rightarrow 1 | b = 1] - \Pr[\mathcal{A} \Rightarrow 1 | b = 0].$$

3. Построение атаки различения на режим DEC

В работе [5] предложена атака различения на режим гаммирования (CTR) в модели qIND-qCPA-P13 (определения и классификация моделей даны в [6]). Представляется возможным адаптировать данную атаку к модели qROP-qfdeCPA и режиму DEC.

Теорема 1. Пусть $l \in \mathbb{N}$ — размер блока блочного шифра в битах, $n \in \mathbb{N}$ — количество блоков в секторе диска, π — случайная подстановка множества V_l. Существует такой нарушитель $\mathcal{A}$, что

$$\mathbf{Adv}_{\text{DEC}^\pi}^{\text{qROP-qfdeCPA}}(\mathcal{A}) = 1 - 2^{1-nl},$$

где DEC^π — настраиваемый симметричный шифр с состоянием, в котором подстановка π используется в режиме DEC вместо функции зашифрования блочного шифра. При этом $\mathcal{A}$ совершает в точности один запрос к оракулу.

Атака основана на том, что при совершении специально подготовленного запроса к оракулу квантовые регистры открытого текста и шифртекста оказываются запутанными. В случае зашифрования переданного нарушителем открытого текста возможно перейти к незапутанному состоянию указанных регистров в силу представления шифртекста c в виде $c = m \oplus \gamma$, где $\gamma = \gamma(\pi, SN, PN)$ — двоичная строка, выработанная по описанному в [3] алгоритму с помощью подстановки π (вместо блочного шифра) и номеров раздела PN и сектора SN. Если перед зашифрованием к открытому тексту применить случайную подстановку, то переход к незапутанному состоянию регистров будет невозможен.

Отметим, что, в силу использования случайной подстановки $\pi \in \text{S}(V_l)$ вместо функции зашифрования блочного шифра в теореме 1, полученное значение преобладания справедливо для любого блочного шифра.

Заключение

В работе дано определение модели qROP-qfdeCPA, формализующей обеспечение свойства конфиденциальности настраиваемым симметричным шифром с состоянием в условиях доступа нарушителя к квантовому оракулу. В рамках данной модели рассмотрен нарушитель, различающий за один запрос к оракулу случай зашифрования в режиме DEC переданного открытого текста и случай зашифрования в режиме DEC результата применения случайной подстановки к переданному открытому тексту. Осуществляемая нарушителем атака основана на возможности перехода от запутанного состояния регистров открытого текста и шифртекста к незапутанному в первом случае и невозможности этого перехода во втором. Преобладание нарушителя близко к единице, его значение справедливо для любого блочного шифра.

ЛИТЕРАТУРА

1. *Schrottenloher A.* Quantum Algorithms for Cryptanalysis and Quantum-safe Symmetric Cryptography. Sorbonne Université, 2021.
2. *Nakahara M. and Ohmi T.* Quantum Computing: from Linear Algebra to Physical Realizations. CRC Press, 2008. 438 p.
3. Рекомендации по стандартизации Р 1323565.1.042–2022 «Информационная технология. Криптографическая защита информации. Режим работы блочных шифров, предназначенный для защиты носителей информации с блочно-ориентированной структурой». М.: Стандартинформ, 2022.
4. *Firsov G. and Koreneva A.* On one block cipher mode of operation used to protect data on block-oriented storage devices // Modern Inform. Technologies and IT-Education. 2022. No. 18(3). P. 691–701.
5. *Nemoz T., Amblard Z., and Dupin A.* Characterizing the qIND-qCPA (in)security of the CBC, CFB, OFB and CTR modes of operation // LNCS. 2023. V. 14154. P. 445–475.
6. *Carstens T. V., Ebrahimi E., Tabia G. N., and Unruh D.* Relationships between quantum IND-CPA notions // LNCS. 2021. V. 13042. P. 240–272.

УДК 512.64, 519.21, 519.72 DOI 10.17223/2226308X/17/23

НЕЗАВИСИМОСТЬ СОБЫТИЙ В ПРОСТРАНСТВАХ РАВНОВЕРОЯТНЫХ ШИФРОБОЗНАЧЕНИЙ

Н. В. Медведева, С. С. Титов

В рамках вероятностной модели шифра рассмотрена задача разложения (декомпозиции) в некоторой ортогональной системе координат дискретного пространства Ω элементарных событий на пары семейств несовместных событий, независимых с любым событием другого семейства. Показано, что для составного числа N (мощности дискретного пространства элементарных событий) существуют пары независимых подпространств пространства Ω, а для простых чисел N независимых подпространств не существует. Построены примеры, иллюстрирующие полученные теоретические утверждения.

Ключевые слова: *совершенные шифры, пространство элементарных событий, независимые события.*

В продолжение работ [1–4] в рамках вероятностной модели Σ_B шифра [5] исследуется проблема описания (построения) совершенных по Шеннону [5] шифров. Согласно подходу работ [6, 7], шифр на множестве ℓ-грамм задаётся распределением

вероятностей ключей при $\ell = 1$. Пусть $X = \{x_1, x_2, \ldots, x_\lambda\} = \{1, 2, \ldots, \lambda\}$ — множество шифрвеличин; $Y = \{y_1, y_2, \ldots, y_\mu\} = \{1, 2, \ldots, \mu\}$ — множество шифробозначений, с которыми оперирует некоторый шифр замены; $K = \{k_1, k_2, \ldots, k_\pi\}$ — множество ключей. По условию $|X| = \lambda > 1$, $|Y| = \mu \geqslant \lambda$, $|K| = \pi \geqslant \mu$. Это означает, что открытые $x = x_{i_1} x_{i_2} \ldots x_{i_\ell}$, $x_{i_j} \in X$, $j = 1, 2, \ldots, \ell$, и шифрованные $y = y_{i_1} y_{i_2} \ldots y_{i_\ell}$, $y_{i_j} \in Y$, тексты представляются словами (ℓ-граммами, $\ell \geqslant 1$) в алфавитах X и Y соответственно.

В соответствии с [6, 7] шифр Σ_B — это совокупность множеств правил зашифрования и правил расшифрования с заданными распределениями вероятностей на множествах открытых текстов и ключей. Шифры, для которых апостериорные вероятности $\mathsf{P}[x|y]$, $x \in X^\ell$, $y \in Y^\ell$, открытых текстов совпадают с их априорными вероятностями $\mathsf{P}[x]$, называются *совершенными* [6, 7].

Применение аппарата теории вероятностей для решения исследуемой проблемы предполагает введение соответствующего вероятностного пространства $(\Omega, \mathcal{F}, \mathbf{P})$. Здесь Ω — пространство элементарных событий, которое полагается измеримым, т. е. на нём определена σ-алгебра $\mathcal{F}$ его подмножеств (случайных событий). Кроме того, на измеримом пространстве $\{\Omega, \mathcal{F}\}$ задана вероятностная мера $\mathbf{P}$, т. е. для любого множества $A \in \mathcal{F}$ определена его вероятность $\mathsf{P}[A]$.

В прикладных ситуациях часто независимость случайных событий постулируется вместе с их равновероятностью. Например, в криптографии постулируется независимость ключа от шифруемого текста (если такая зависимость есть, то тогда можно не шифровать). Кроме этого, для криптографических приложений естественны дискретные пространства Ω элементарных событий, особенно конечные пространства равновероятных элементарных событий, посредством которых исследуются почти совершенные шифры [8, 9]. Поэтому разложение (декомпозиция) в некоторой ортогональной системе координат пространства Ω элементарных событий на пары семейств несовместных событий, независимых с любым событием другого семейства, является важной и нетривиальной задачей криптографии, теории кодирования, а также факторного анализа и теории надёжности.

Решение задачи разложения дискретного пространства Ω элементарных событий в декартово произведение независимых подпространств даёт компактное и удобное для приложений его описание.

Разложение на пары независимых множеств. Рассмотрим дискретное пространство Ω, состоящее из N равновероятных элементарных событий. Если события A и B — подмножества пространства Ω мощностей a и b соответственно, причём мощность их пересечения $A \cap B$ равна c, то их вероятности равны соответственно a/N, b/N и c/N. Пусть $\mathsf{P}[A \cdot B] \neq 0$, $\mathsf{P}[A] \neq 0$, $\mathsf{P}[B] \neq 0$ и $\mathsf{P}[A] \neq 1$, $\mathsf{P}[B] \neq 1$. Тогда критерием независимости событий A и B является равенство

$$\mathsf{P}[A \cdot B] = \mathsf{P}[A \cap B] = \mathsf{P}[A] \cdot \mathsf{P}[B],$$

то есть $c/N = ab/N^2$, что равносильно равенству $cN = ab$.

Следовательно, $ab \equiv 0 \pmod N$, причём $a \neq 0 \pmod N$, $b \neq 0 \pmod N$. Поэтому a и b — делители нуля в кольце $\mathbb{Z}_N$ (и, в частности, N не является простым). Справедливо

Утверждение 1. Пусть мощность дискретного пространства Ω элементарных событий равна N, а элементарные события $\varpi \in \Omega$ равновероятны. При этом $N = uv$, где $1 < u, v < N$. Тогда для любых чисел s и t, таких, что $1 \leqslant s < v$, $1 \leqslant t < u$, существуют независимые события $A \subset \Omega$ и $B \subset \Omega$, для которых выполняются равенства

$$\mathsf{P}[A] = a/N, \quad \mathsf{P}[B] = b/N, \quad \mathsf{P}[A \cdot B] = c/N, \quad \text{где} \;\; a = su, \; b = tv, \; c = st.$$

Доказательство. Отметим, что для независимых событий A и B выполняются условия $\mathsf{P}[A\cdot B]\neq 0$, $\mathsf{P}[A]\neq 0$, $\mathsf{P}[B]\neq 0$ и $\mathsf{P}[A]\neq 1$, $\mathsf{P}[B]\neq 1$, а также они не являются следствиями друг друга. Поэтому необходимо выполнение неравенств $1\leqslant c\leqslant N-2$, $1<a<N$, $1<b<N$. Из того, что a и b суть делители нуля, вытекает $a=su$, $b=tv$ для некоторых u,v, таких, что $N=uv$; $ab=sutv=cN\equiv 0 \pmod N$. Отсюда следует равенство $\mathsf{P}[A\cdot B]=\mathsf{P}[A]\cdot\mathsf{P}[B]$ при условии существования подмножеств A и B, таких, что $|A\cap B|=c\leqslant N-2$, $|A|=a<N$, $|B|=b<N$, $a+b-c\leqslant N$, $c<a$, $c<b$. Эти условия равносильны системе неравенств

$$\begin{cases} 1\leqslant st\leqslant N-2,\\ su<N,\\ tv<N,\\ su+tv-st\leqslant N,\\ st<su,\\ st<tv. \end{cases}$$

Из последних двух неравенств следует $t<u$, $s<v$. Поэтому

$$1\leqslant st=c\leqslant (u-1)(v-1)=N-(u+v)+1<N-2+1=N-1,$$

т. е. $c\leqslant N-2$ и первое неравенство справедливо. Тогда второе и третье неравенства также справедливы. Наконец,

$$su+tv-st=su+t(v-s)<su+u(v-s)=u(s+v-s)=uv=N,$$

т. е. четвёртое неравенство также выполняется. ■

Следствие 1. Если $|\Omega|=N$ — простое число, то в пространстве Ω элементарных событий не существует пар независимых событий.

Следствие 1 вытекает из необходимости наличия у числа N нетривиальных делителей u, v.

Следствие 2. Пара независимых событий не покрывает всё пространство Ω элементарных событий.

Следствие 2 вытекает из строгости неравенства $a+b-c<N$.

Пример 1. При $N=6$ имеем без ограничения общности $u=2$, $v=3$, $t=1$ и либо $s=1$, либо $s=2$. Это даёт либо $a=su=2$, $b=tv=3$, $c=st=1$ с вероятностями $\mathsf{P}[A]=a/N=1/3$, $\mathsf{P}[B]=b/N=1/2$, $\mathsf{P}[A\cdot B]=c/N=1/6$, либо $a=su=4$, $b=tv=3$, $c=st=2$ с вероятностями $\mathsf{P}[A]=a/N=2/3$, $\mathsf{P}[B]=b/N=1/2$, $\mathsf{P}[A\cdot B]=c/N=1/3$.

Разложение на пары независимых семейств. Конструкция пар независимых событий может быть естественным образом продолжена до конструкции пар независимых семейств, а именно: для декомпозиции пространства Ω элементарных событий требуется построить два семейства, обозначим их как $\mathcal{A}$ и $\mathcal{B}$, состоящие из несовместных событий, находящихся в отношении независимости с любым событием другого семейства.

Пусть $\mathcal{A} = \{A_1, A_2, \ldots, A_m\}$, $\mathcal{B} = \{B_1, B_2, \ldots, B_n\}$, требуется одновременное выполнение следующих условий:

$$\forall i, j \in \{1, \ldots, m\}\big((i \neq j) \Rightarrow \mathsf{P}[A_i \cdot A_j] = 0\big); \tag{1}$$

$$\forall k, l \in \{1, \ldots, n\}\big((k \neq l) \Rightarrow \mathsf{P}[B_k \cdot B_l] = 0\big); \tag{2}$$

$$\forall i \in \{1, \ldots, m\} \forall k \in \{1, \ldots, n\}\big(\mathsf{P}[A_i \cdot B_k] = \mathsf{P}[A_i] \cdot \mathsf{P}[B_k]\big). \tag{3}$$

В обозначениях и условиях утверждения 1 рассмотрим разложение пространства Ω в декартово произведение $X \times Y$ следующих двух пространств равновероятных элементарных событий: пространства $X = \{x_1, x_2, \ldots, x_u\}$ с вероятностями $1/u$ и пространства $Y = \{y_1, y_2, \ldots, y_v\}$ с вероятностями $1/v$.

Вероятность события (x, y), где $x \in X$, $y \in Y$, полагаем равным $1/uv = 1/N$. Для $m = [v/t]$, $n = [u/s]$, $1 \leqslant i \leqslant m$, $1 \leqslant k \leqslant n$ положим

$$A_i = \{(x, y_j) : x \in X,\ (i-1)t \leqslant j < it\}; \tag{4}$$

$$B_k = \{(x_j, y) : y \in Y,\ (k-1)s \leqslant j < ks\}. \tag{5}$$

В соответствии с конструкцией и утверждением 1 имеем

Утверждение 2. Семейства множеств (4) и (5) удовлетворяют условиям (1)–(3).

Пример 2. Пусть мощность пространства элементарных событий равна 90, т. е. $|\Omega| = 90$, и элементарные события $\varpi \in \Omega$ равновероятны: $\mathsf{P}[\varpi] = 1/90$. Тогда без ограничения общности имеем $u = 9$, $v = 10$, $t = 4$ и $s = 3$. Это даёт $a = su = 27$, $b = tv = 40$, $c = st = 12$ с вероятностями $\mathsf{P}[A_i] = a/N = 27/90 = 3/10$, $\mathsf{P}[B_k] = b/N = 40/90 = 4/9$, $\mathsf{P}[A_i \cdot B_k] = c/N = 12/90$, где $i = 1, 2, 3$; $j = 1, 2$.

Декомпозиция пространства Ω представлена на рис. 1. Здесь $\mathsf{P}[A_i \cdot A_j] = 0$ $(i \neq j)$, $\mathsf{P}[B_k \cdot B_l] = 0$ $(k \neq l)$, $\mathsf{P}[A_i \cdot B_k] = \mathsf{P}[A_i] \cdot \mathsf{P}[B_k] = c/N = 12/90$, т. е. условия (1)–(3) выполняются.

Разложение Ω на пару семейств $\mathcal{A} = \{A_1, A_2, A_3\}$ и $\mathcal{B} = \{B_1, B_2\}$ позволяет интерпретировать множество

$$\bigcup_{i,k} (A_i \cap B_k)$$

как пространство событий, определяемых семействами $\mathcal{A}$ и $\mathcal{B}$ независимо.

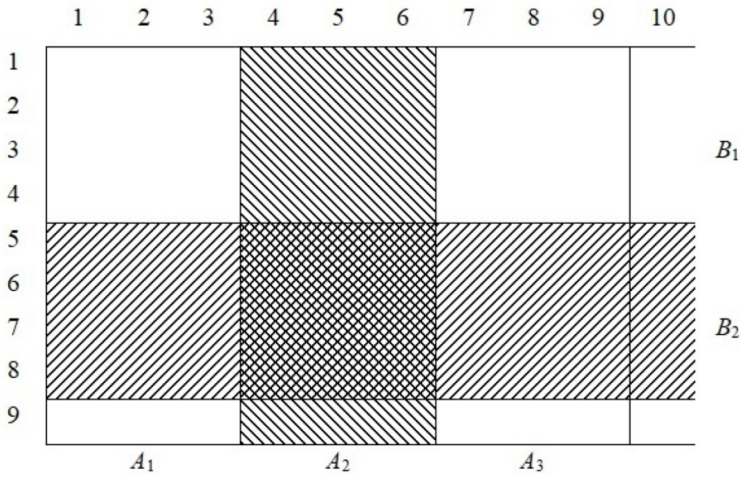

Рис. 1. Декомпозиция пространства Ω

Представление пространств элементарных событий в таком виде можно считать определением факторов A и B, независимо описывающих моделируемую ситуацию. Так, можно считать A_1, A_2, A_3 ключами, а B_1, B_2 — шифруемыми текстами. При этом шифробозначения оказываются равновероятными.

Следствие 3. Во введённых обозначениях, если u/s и v/t — целые числа, то множества семейств $\mathcal{A}$ и $\mathcal{B}$ покрывают всё пространство Ω элементарных событий.

Таким образом, бинарное отношение независимости событий связано с теоретико-числовой природой числа N — мощности пространства элементарных событий, и прояснение этой связи представляет собой нетривиальную, но важную задачу. При известном количестве равновероятных элементарных событий существует ограниченное число вариантов разложения дискретного пространства элементарных событий на независимые факторы, которые можно рассматривать как ключи и открытые тексты.

ЛИТЕРАТУРА

1. *Медведева Н. В., Титов С. С.* Описание неэндоморфных максимальных совершенных шифров с двумя шифрвеличинами // Прикладная дискретная математика. 2015. № 4 (30). С. 43–55.
2. *Медведева Н. В.* Об аналогах теоремы Шеннона для совершенных шифров // Proc. 3rd Russian Conf. MMIT. Ekaterinburg, Russia, 2016. P. 232–239.
3. *Медведева Н. В., Титов С. С.* Геометрическая модель совершенных шифров с тремя шифрвеличинами // Прикладная дискретная математика. Приложение. 2019. № 12. С. 113–116.
4. *Медведева Н. В., Титов С. С.* Критерий минимальности по включению совершенных шифров // Прикладная дискретная математика. Приложение. 2022. № 15. С. 51–54.
5. *Шеннон К.* Теория связи в секретных системах // Работы по теории информации и кибернетике. М.: Наука, 1963. С. 333–402.
6. *Алферов А. П., Зубов А. Ю., Кузьмин А. С., Черемушкин А. В.* Основы криптографии. М.: Гелиос АРВ, 2001. 478 с.
7. *Зубов А. Ю.* Совершенные шифры. М.: Гелиос АРВ, 2003. 160 с.
8. *Зубов А. Ю.* Почти совершенные шифры и коды аутентификации // Прикладная дискретная математика. 2011. № 4 (14). С. 28–33.
9. *Зубов А. Ю.* О понятии ε-совершенного шифра // Прикладная дискретная математика. 2016. № 3 (33). С. 45–52.

УДК 003.26 DOI 10.17223/2226308X/17/24

НИЗКОРЕСУРСНОЕ АУТЕНТИФИЦИРОВАННОЕ ШИФРОВАНИЕ: ОБЗОР ПОДХОДОВ

С. П. Панасенко

Работа является обзорной, она посвящена алгоритмам аутентифицированного шифрования с присоединёнными данными, а также функционально аналогичным режимам работы алгоритмов блочного симметричного шифрования. Рассмотрены стандартизованные режимы работы Galois/Counter Mode и Multilinear Galois Mode, а также алгоритмы шифрования, изначально разработанные для реализации подобных преобразований, на примере алгоритма Ascon. Показана оптимальность аутентифицированного шифрования с присоединёнными данными для использования в низкоресурсных устройствах на примере радиочастотных меток, взаимодействующих со считывателем по радиоканалу. Обозначены некоторые из

возможных критериев выбора конкретного алгоритма и/или режима работы для реализации на целевой низкоресурсной платформе.

Ключевые слова: *аутентифицированное шифрование с присоединёнными данными, низкоресурсная криптография, режимы работы блочных шифров.*

Введение

Алгоритмы аутентифицированного шифрования (Authenticated Encryption — AE) представляют собой класс алгоритмов шифрования, которые также позволяют аутентифицировать зашифрованные данные, т. е. обеспечивают возможность проверки их целостности.

Алгоритмы аутентифицированного шифрования с присоединёнными данными (Authenticated Encryption with Associated Data — AEAD) можно считать частным случаем AE-алгоритмов, поскольку они также обеспечивают как конфиденциальность, так и целостность зашифрованных данных. Помимо этого, AEAD-алгоритмы позволяют обеспечить целостность и аутентичность некоторых дополнительных данных, для которых не требуется конфиденциальность. Дополнительные данные при этом не шифруются.

Необходимость в появлении такого класса алгоритмов обусловлена тем, что во многих приложениях требуется, помимо передачи некоторых данных в зашифрованном виде, передавать также определённую открытую информацию с контролем её целостности/аутентичности. Данная возможность важна, когда взаимодействие с устройствами с небольшими ресурсами ограничено незначительным промежутком времени. В качестве примера можно привести взаимодействие с радиочастотной меткой (Radio Frequency IDentifier — RFID), обычно короткое время находящейся в зоне действия считывателя.

AEAD-алгоритмы позволяют за максимально возможно короткий промежуток времени (ограниченный однократным выполнением алгоритма) сформировать ответ, содержащий следующее:

— зашифрованную полезную информацию (например, полученные от RFID-метки данные);
— присоединённые данные (могут содержать идентификатор RFID-метки, что позволяет связать переданные меткой данные с конкретным отслеживаемым объектом, к которому привязана метка);
— код аутентификации полученных данных — тег, позволяющий проверить целостность и присоединённых данных, и полезной информации.

Применение других классов криптографических алгоритмов потребовало бы нескольких криптографических операций (например, шифрования полезной информации и хеширования присоединённых данных и полезной информации), т. е. нескольких обращений к RFID-метке, что крайне нежелательно в условиях незначительных вычислительных ресурсов RFID-метки и сжатого периода времени.

1. Аутентифицированное шифрование с присоединенными данными

На рис. 1 приведена общая схема AEAD-зашифрования с входными и выходными параметрами. Такие параметры, как вектор инициализации (IV), секретный ключ и тег обычно имеют фиксированные размеры, тогда как размеры открытого текста (следовательно, и размер шифртекста) и присоединённых данных могут быть произвольными (но на них могут накладываться ограничения). В качестве IV может использоваться как случайная последовательность, так и какой-либо инкрементируемый

с каждым применением алгоритма номер пакета, сообщения и т. п. Возможные требования, предъявляемые к вектору инициализации, рассмотрены далее.

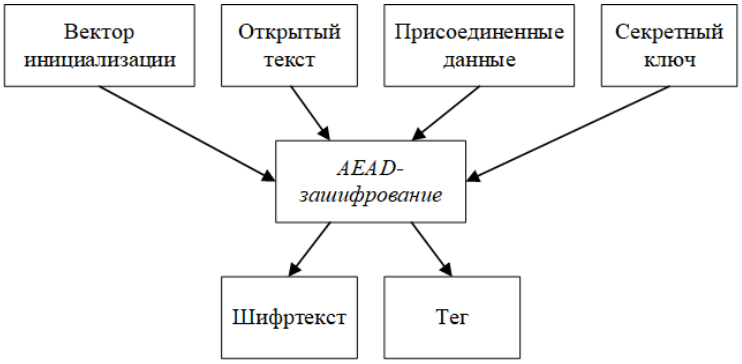

Рис. 1. Параметры зашифрования в режиме AEAD

При расшифровании данных с проверкой целостности входные данные процедуры AEAD-расшифрования, помимо тех же значений IV, присоединённых данных и секретного ключа, содержат также выходные данные, полученные при AEAD-зашифровании, а именно шифртекст и тег. Тег, аутентифицирующий данные, подлежит проверке в процессе AEAD-расшифрования, в результате которого формируются следующие выходные данные:

— признак ошибки контроля целостности в случае её нарушения;
— расшифрованный открытый текст в случае, если контроль целостности пройден успешно.

AEAD может быть реализовано различными способами, основными из которых можно считать следующие:

— применение специальных режимов работы алгоритмов блочного симметричного шифрования;
— применение AEAD-алгоритмов шифрования.

2. Режимы работы блочных шифров для аутентифицированного шифрования

Режимы работы блочных шифров, осуществляющих аутентифицированное шифрование с присоединёнными данными, можно представить как надстройки над алгоритмами блочного шифрования, в которых выполняются две основные процедуры:

— шифрование открытого текста с получением шифртекста;
— вычисление аутентифицирующего тега от шифртекста и присоединённых данных.

Именно так обработка данных производится в AEAD-режиме GCM (Galois/Counter Mode), который определён в рекомендациях NIST SP 800-38D [1]. Последовательность зашифрования данных и вычисления аутентифицирующего тега в режиме GCM представлена на рис. 2.

Основными процедурами данного режима являются:

— процедура зашифрования Enc, выполняющая поблочное шифрование на ключе K открытого текста P с помощью модифицированного режима счётчика;
— процедура ключевого хеширования GHASH, вычисляющая тег T от входных данных, которыми являются дополненные нулями до кратности размеру блока нижележащего блочного шифра (128 бит) аутентифицируемые данные A, шифртекст C и 64-битные значения их размеров до дополнения ($\mathrm{len}(A)$ и $\mathrm{len}(C)$ соответственно).

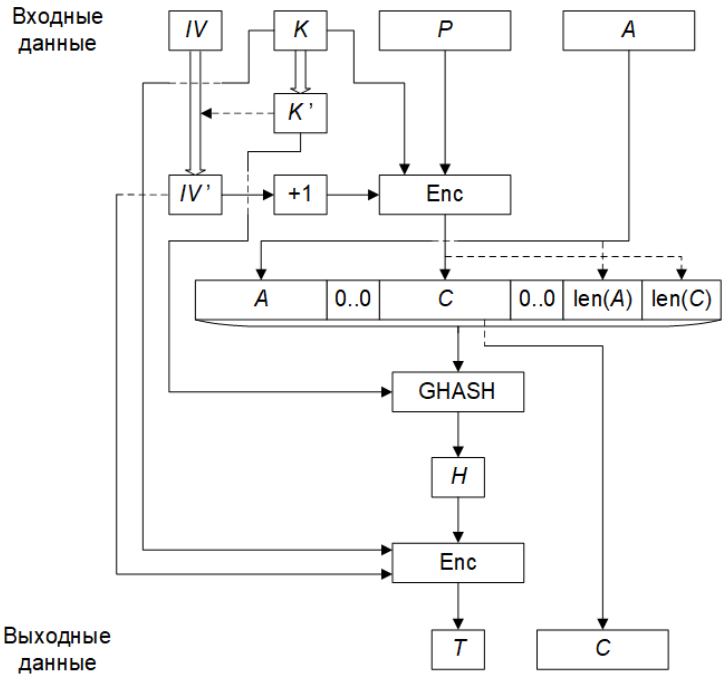

Рис. 2. Упрощённая схема режима GCM

В России стандартизован альтернативный AEAD-режим MGM (Multilinear Galois Mode), который вошел в Межгосударственный стандарт на режимы работы блочных шифров ГОСТ 34.13-2018 [2] в рамках принятия Изменения № 1 к данному стандарту [3]. Схема данного режима приведена на рис. 3.

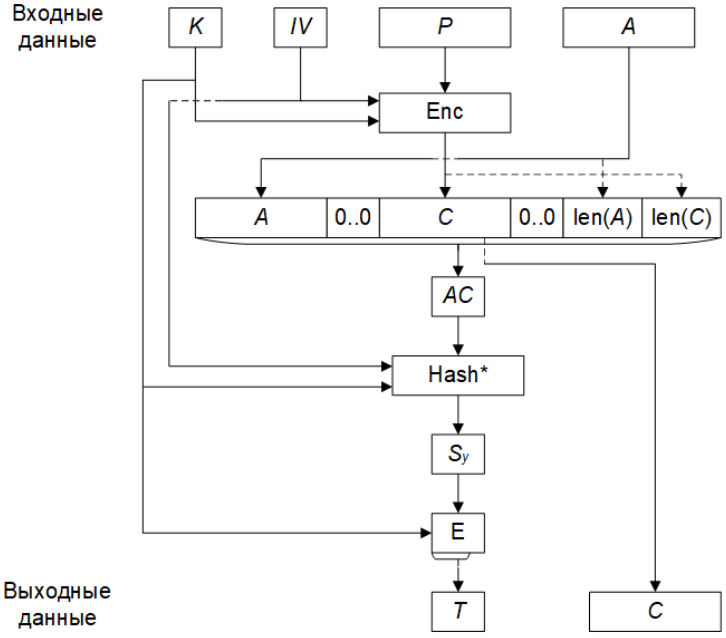

Рис. 3. Упрощённая схема режима MGM

Режим MGM концептуально схож с режимом GCM; обработка данных в процессе выполнения режима MGM состоит в поблочном зашифровании открытого текста и

последующем применении ключевого хеширования для вычисления аутентифицирующего тега.

Рассмотренные надстройки над блочным шифром, соответствующие режимам GCM и MGM, сами по себе не предъявляют значительных требований к ресурсам. Если в качестве нижележащего блочного шифра используется низкоресурсный алгоритм, то такой результирующий AEAD-алгоритм также не должен являться ресурсоёмким и может быть использован в устройствах с ограниченными ресурсами.

Именно такой вариант — использование алгоритма AES-128 в режиме GCM — рекомендуется в [4] в случаях, когда по каким-либо причинам применение низкоресурсного AEAD-алгоритма нецелесообразно или невозможно. Режим MGM определён для алгоритмов шифрования с размером блока 64 или 128 бит, поэтому в качестве еще одного примера можно привести 64-битный алгоритм Магма в режиме MGM — данный вариант можно считать достаточно низкоресурсным (см. сравнительный анализ ресурсоёмкости алгоритмов блочного шифрования в [5]).

3. Низкоресурсные алгоритмы аутентифицированного шифрования

Алгоритмы аутентифицированного шифрования с присоединёнными данными представляют собой класс алгоритмов, изначально разработанных для AEAD-шифрования. Помимо AEAD-алгоритмов, предназначенных для выполнения на устройствах общего назначения, существуют и низкоресурсные алгоритмы данного класса, предназначенные для реализации и использования в устройствах, обладающих незначительными вычислительными ресурсами.

Одним из наиболее известных представителей данного класса является семейство алгоритмов Ascon [6]. Алгоритмы Ascon основаны на дуплексном режиме структуры «криптографической губки», предложенном в [7]. Упрощённая схема работы Ascon приведена на рис. 4.

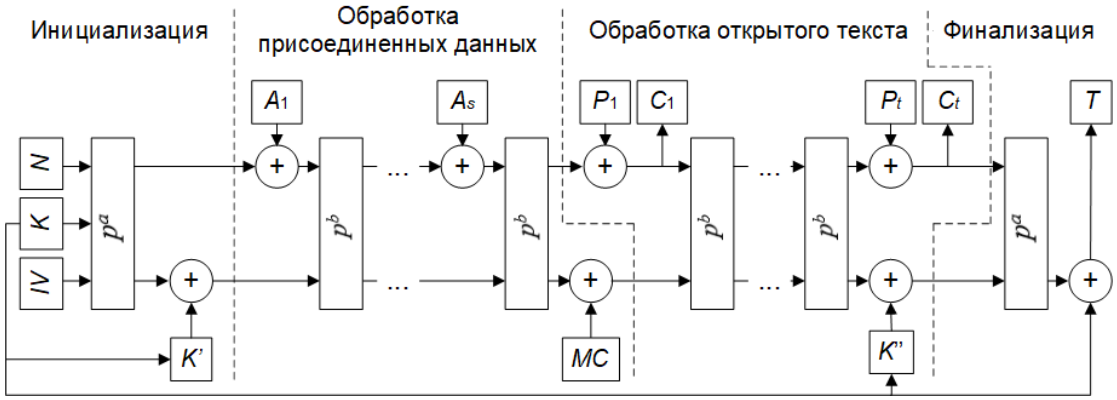

Рис. 4. Упрощённая схема основных преобразований алгоритмов Ascon

Как видно из схемы, последовательность основных операций в данном случае значительно отличается от таковой в режимах GCM и MGM:

— сначала, после инициализации внутреннего состояния алгоритма, выполняется обработка блоков аутентифицируемых данных;
— затем выполняется зашифрование открытого текста;
— последним этапом является финализация, в результате которой вычисляется тег.

4. Возможные критерии выбора

В режимах GCM и MGM могут быть применены и низкоресурсные блочные шифры, например рассмотренные в [8]. Однако, поскольку в [1, 3] режимы GCM и MGM соответственно определены для конкретных нижележащих алгоритмов блочного шифрования, при использовании других алгоритмов потребуется отдельный анализ их криптостойкости в данных режимах.

Важным критерием выбора низкоресурсного AEAD-алгоритма или режима работы может быть наличие ограничений на уникальность значений IV для шифрования данных с одним и тем же ключом в режимах GCM и MGM. Поскольку для соответствия данному ограничению может понадобиться реализация дополнительных механизмов (примеры для режима GCM приведены в документе [1]) в низкоресурсном устройстве, выбор может быть сделан в пользу низкоресурсного AEAD-алгоритма, не предъявляющего подобного требования. Алгоритм Ascon не требует уникальности значений IV, но в нём нужна уникальность значений нонса (N на рис. 3), что приводит к необходимости применения соответствующих механизмов при реализации данного алгоритма.

Кроме того, аппаратные и программные реализации алгоритмов шифрования предъявляют весьма различные требования к структуре алгоритмов и используемым в них преобразованиям, в результате чего трудно разработать алгоритм, одинаково хорошо адаптированный для различных низкоресурсных платформ, как программных, так и аппаратных. Отсюда следует, что во многих случаях нужна тестовая реализация ряда алгоритмов для сравнительного анализа их быстродействия на конкретной целевой платформе и последующего выбора наиболее оптимального.

Решающим критерием выбора в пользу применения режима MGM может являться факт его стандартизации в рамках Межгосударственного стандарта [2]. В совокупности с применением стандартизованного низкоресурсного алгоритма блочного симметричного шифрования с помощью режима MGM можно получить аутентифицированное шифрование с присоединёнными данными на основе стандартных алгоритмов и с незначительными требованиями к ресурсам.

ЛИТЕРАТУРА

1. NIST Special Publication 800-38D. Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC. 2007.
2. ГОСТ 34.13-2018. Информационная технология. Криптографическая защита информации. Режимы работы блочных шифров. М.: Стандартинформ, 2018.
3. Изменение № 1 ГОСТ 34.13-2018. Информационная технология. Криптографическая защита информации. Режимы работы блочных шифров. `https://protect.gost.ru/default.aspx/document1.aspx?control=31&baseC=6&page=10&month=11&year=2023&search=&id=255662`. 2023.
4. NIST Internal Report 8454. Status Report on the Final Round of the NIST Lightweight Cryptography Standardization Process. `https://doi.org/10.6028/NIST.IR.8454`. 2023.
5. *Poschmann A., Ling S., and Wang H.* 256 bit standardized crypto for 650 GE — GOST revisited // LNCS. 2010. V. 6225. P. 219–233.
6. *Dobraunig C., Eichlseder M., Mendel F., and Schläffer M.* Ascon. V1.2. Submission to NIST. 2019. 48 p.
7. *Bertoni G., Daemen J., Peeters M., and Van Assche G.* Duplexing the Sponge: Single-Pass Authenticated Encryption and Other Applications. IACR Cryptology ePrint Archive. 2011.
8. *Панасенко С. П.* Низкоресурсная симметричная криптография: принципы, подходы и компромиссы // Прикладная дискретная математика. Приложение. 2023. № 16. С. 74–78.

УДК 519.7 DOI 10.17223/2226308X/17/25

О СТОЙКОСТИ АЛГОРИТМА БЛОЧНОГО ШИФРОВАНИЯ КБ-256 К АТАКАМ С ИСПОЛЬЗОВАНИЕМ КВАНТОВЫХ АЛГОРИТМОВ

М. В. Поляков, А. М. Коренева

КБ-256 — алгоритм блочного шифрования, рекомендованный для защиты больших объёмов данных. Рассматриваются вопросы криптографической стойкости КБ-256 в модели атакующего, имеющего доступ к квантовому компьютеру. Оценивается трудоёмкость применения алгоритма Гровера — сложность квантовой схемы, в которой необходимо реализовать оракул алгоритма КБ-256, а также количество необходимого материала. Помимо этого, рассматривается возможность атаки с помощью алгоритмов поиска скрытого сдвига.

Ключевые слова: *квантовый компьютер, квантовый криптоанализ, КБ-256, алгоритм Гровера, алгоритм Саймона.*

Алгоритм Шора [1] является одним из самых известных алгоритмов квантового криптоанализа — он позволяет строить эффективные атаки на основные асимметричные схемы. С точки зрения стойкости симметричных криптографических алгоритмов наиболее известным является алгоритм Гровера [2], который позволяет решать задачу нахождения элемента в неупорядоченном массиве размерности N за $O(\sqrt{N})$ обращений к квантовому оракулу. Алгоритмы Бернштейна — Вазирани и Саймона также применимы к задачам криптоанализа симметричных криптографических алгоритмов, как алгоритмов шифрования, так и хеш-функций [3–7].

Блочный шифр КБ-256 представляет собой обобщённую сеть Фейстеля с длиной блока 256 бит и длиной ключа также 256 бит [8]. Функция зашифрования строится путём 18-кратного применения частичной раундовой функции зашифрования, которую можно выразить как отображение вида $R : \mathbb{Z}_2^{256} \times \mathbb{Z}_2^{96} \to \mathbb{Z}_2^{256}$. Непосредственно частичную раундовую функцию составляют следующие преобразования:

- $\Sigma(X_0, X_1, \ldots, X_7) = X_1 \boxplus X_3 \boxplus X_4 \boxplus X_6 \boxplus X_7$, $X_i \in \mathbb{Z}_2^{32}$, $\boxplus$ — операция сложения в кольце $\mathbb{Z}_{2^{32}}$;
- $f(X_0, X_1, \ldots, X_7) = (\pi_0(X_0), \pi_1(X_1), \ldots, \pi_7(X_7)) <<< 19$, $\pi_i \in S(\mathbb{Z}_2^4)$ — подстановки из ГОСТ 34.12-2018 «Магма», $<<<$ — операция циклического побитового сдвига в сторону старших разрядов.

Действие частичной раундовой функции зашифрования описывается выражением

$$\overline{X} = (X_0, X_1, X_2, X_3, X_4, X_5, X_6, X_7) \to$$
$$\to \left(X_0, X_2 \oplus f\left(\Sigma(\overline{X}) \boxplus b_0^{(i)}\right), X_3, X_4, X_5 \oplus f\left(\Sigma(\overline{X}) \boxplus b_1^{(i)}\right), X_6, X_7, X_0 \oplus f\left(\Sigma(\overline{X}) \boxplus b_2^{(i)}\right)\right),$$

где $b_0^{(i)}, b_1^{(i)}, b_2^{(i)}$ — раундовые ключи раунда с номером i; $b_j^{(i)} \in \mathbb{Z}_{2^{32}}$.

Алгоритм развёртывания ключа основан на последовательном соединении линейного конгруентного генератора (ЛКГ) и модифицированного аддитивного генератора (МАГ) [9]. Если $(X_0, \ldots, X_6)$, $X_i \in \mathbb{Z}_{2^{32}}$, — начальное состояние МАГ, а K_0 — начальное состояние ЛКГ, то выходное значение алгоритма задаётся следующей формулой:

$$X_{i+7} = ((X_i \boxplus X_{i+2} \boxplus X_{i+4} \boxplus X_{i+6}) <<< 1) \boxplus K_i \boxplus \gamma,$$

где $\gamma \in \mathbb{Z}_{2^{32}}$ — произвольное нечётное число.

Для оценки сложности реализации квантовой атаки на алгоритм КБ-256 оценим число кубитов и квантовых вентилей для реализации алгоритма в виде схемы. В работе [10] приведены оценки сложности реализации в виде квантовой схемы без дополнительных кубитов S-блоков алгоритма «Магма» — 256 квантовых вентилей. В [11] представлен алгоритм, позволяющий получить оптимальные квантовые схемы для 4-битных S-блоков. Алгоритм даёт общую оценку сложности в 240 квантовых вентилей для одного раунда КБ, так как в КБ-256 функция трижды обращается к S-блокам. В функции реализовано также наложение раундового ключа с помощью операции сложения в кольце $\mathbb{Z}_{2^{32}}$. В работе [12] показано, что реализация одного элемента, выполняющего модульное суммирование, потребует $7n - 8$ квантовых вентилей CNOT и Тоффоли, где n — разрядность складываемых чисел. Узел суммирования в кольце $\mathbb{Z}_{2^{32}}$ используется в одной итерации алгоритма развертывания ключа пять раз. При реализации узел суммирования будет вызван 12 раз, итого 2592 вентилей. Общая оценка сложности реализации КБ-256:

— количество кубитов — 544;
— количество вентилей для одного раунда — 2592;
— количество вентилей для 18 раундов с экономией кубитов — 188892.

По расстоянию единственности для атаки полным перебором ключа алгоритма КБ-256 потребуется $\lceil 256/256 \rceil = 1$ пара открытого и шифрованного текстов. Таким образом, для применения алгоритма Гровера к алгоритму КБ-256 потребуется $544 + 2 \cdot 256 = 1068$ кубитов и не менее $2^{128} \cdot 188892 \cdot \pi/4$ квантовых вентилей.

Кроме того, так как КБ-256 представляет собой обобщённую сеть Фейстеля, то целесообразно рассмотреть стойкость относительно алгоритмов поиска скрытых линейных структур раундовых функций и последующего построения квантового различителя. Для этого рассмотрим четыре раунда алгоритма КБ-256. Пусть $\overline{X}^{(0)} = \left(X_0^{(0)}, X_1^{(0)}, \ldots, X_7^{(0)}\right)$ — блок открытого текста, подлежащего зашифрованию; $f\left(\alpha^{(i)}, b_j^{(i)}\right)$ — раундовое преобразование f на i-м раунде; $b_j^{(i)}$ — раундовый ключ ($j = 0, 1, 2$) и $\alpha^{(i)} = \Sigma\left(X_0^{(i)}, X_1^{(i)}, \ldots, X_7^{(i)}\right)$. Тогда

$$
\begin{aligned}
X_0^{(4)} &= f^{(3)}\left(\alpha^{(3)}, b_0^{(3)}\right) \oplus X_4^{(0)}, \\
X_1^{(4)} &= f^{(3)}\left(\alpha^{(3)}, b_0^{(3)}\right) \oplus f^{(1)}\left(\alpha^{(1)}, b_1^{(1)}\right) \oplus X_5^{(0)}, \\
X_2^{(4)} &= f^{(3)}\left(\alpha^{(3)}, b_2^{(3)}\right) \oplus X_6^{(0)}, \\
X_3^{(4)} &= f^{(3)}\left(\alpha^{(3)}, b_1^{(3)}\right) \oplus X_7^{(0)}, \\
X_4^{(4)} &= f^{(3)}\left(\alpha^{(3)}, b_1^{(3)}\right) \oplus f^{(1)}\left(\alpha^{(1)}, b_2^{(1)}\right) \oplus X_0^{(0)}, \\
X_5^{(4)} &= f^{(3)}\left(\alpha^{(3)}, b_1^{(3)}\right) \oplus X_1^{(0)}, \\
X_6^{(4)} &= f^{(3)}\left(\alpha^{(3)}, b_0^{(3)}\right) \oplus f^{(1)}\left(\alpha^{(1)}, b_0^{(1)}\right) \oplus X_2^{(0)}, \\
X_7^{(4)} &= f^{(3)}\left(\alpha^{(3)}, b_0^{(3)}\right) \oplus f^{(2)}\left(\alpha^{(2)}, b_0^{(2)}\right) \oplus X_4^{(0)},
\end{aligned}
\tag{1}
$$

т. е. мы имеем соотношения, связывающие входной блок открытого текста с выходом 4-го раунда. Определим функцию $g : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}_{2^{32}}$, которая задаётся равенством $g(x_1, x_2) = \sigma((x_1 + x_2) \bmod 2^{32})$, где $\sigma \in S(\mathbb{Z}_{2^{32}})$. Согласно [13], функция g обладает *скрытым сдвигом*. Действительно, пусть $k \in \mathbb{Z}_{2^{32}}$, тогда $g(x_1, x_2) = g(x_1 + k, x_2 - k)$ —

в случае одного раунда КБ-256 искомым скрытым сдвигом будет раундовый ключ $b_1^{(1)}$. Оценим вероятность нахождения неизвестного значения $b_1^{(1)}$:

— пусть m — неизвестный порядок $b_1^{(1)}$ в группе $(\mathbb{Z}_{2^{32}}, +)$;

— тогда после применения квантового преобразования Фурье [13, разд. 6] имеется следующее состояние:

$$\frac{1}{qm} \sum \exp\left[2\pi i(y_1 s_1 + y_2 s_2)/m\right] |y_1, y_2, g(y_1, y_2)\rangle,$$

где сумма берётся по всем значениям $y_1, y_2, s_1, s_2 \in \mathbb{Z}_{2^{32}}$; q — порядок преобразования $g \in S(\mathbb{Z}_{2^{32}})$;

— вероятность того, что после измерения получится состояние $|s_1, s_2, b_1^{(1)}\rangle$, равна

$$\left| \frac{1}{qm} \sum \exp\left[2\pi i(y_1 s_1 + y_2 s_2)/m\right] \right|^2. \tag{2}$$

В работе [13] показано, что если $s_1 q \geqslant m$ и $s_1 q \bmod 2^{32} \leqslant 2^{32}/m$, то вероятность измерения состояния $|s_1, s_2, b_1^{(1)}\rangle$ больше $1/2$. Так как в выражениях (1) встречаются соотношения для каждого из раундовых ключей $b_j^{(0)}$, процедуру поиска таких скрытых линейных соотношений можно запускать параллельно. Более того, вероятности нахождения скрытого сдвига (т. е. получения состояния $|y_1, y_2, b_j^{(0)}\rangle$) для всех $j = 0, 1, 2$ не зависят друг от друга. Однако в раундовом преобразовании $f^{(i)}\left(\alpha^{(i)}, b_j^{(i)}\right)$ присутствует операция побитового циклического сдвига, относительно которой множество $\mathbb{Z}_{2^{32}}$ не является группой, т. е. классическая атака поиска скрытых линейных соотношений к раундовой функции КБ-256 неприменима.

Таким образом, можно заключить, что блочный шифр КБ-256 имеет параметры квантовой стойкости на уровне других современных блочных шифров, например алгоритма «Кузнечик» из стандарта ГОСТ 34.12-2018 [10]. В качестве достоинств алгоритма можно выделить устойчивость к атакам, основанным на поиске скрытых линейных соотношений.

ЛИТЕРАТУРА

1. *Shor P. W.* Algorithms for quantum computation: discrete logarithms and factoring // Proc. 35th Ann. Symp. FCS. Santa Fe, USA, 1994. P. 124–134.
2. *Grover L. K.* A fast quantum mechanical algorithm for database search // Proc. 28th Ann. ACM Symp. STOC'96. Philadelphia, Pennsylvania, USA, 1996. P. 212–219.
3. *Simon D. R.* On the power of quantum computation // SIAM J. Computing. 1997. V. 26. Iss. 5. P. 1474–1483.
4. *Bernstein E. and Vazirani U.* Quantum complexity theory // Proc. 25th Ann. ACM Symp. STOC'93. San Diego, California, USA, 1993. P. 11–20.
5. *Kaplan M., Leurent G., Leverrier A., and Naya-Plasencia M.* Breaking Symmetric Cryptosystems using Quantum Period Finding. `http://arxiv.org/abs/1602.05973v3`. 2016.
6. *Leander G. and May A.* Grover meets Simon — quantumly attacking the FX-construction // LNCS. 2017. V. 10625. P. 161–178.
7. *Dong X., Li Z., and Wang X.* Quantum cryptanalysis on some generalized Feistel schemes // Sci. China Inf. Sci. 2019. V. 62. Article 22501.
8. *Fomichev V. M. and Koreneva A. M.* Encryption performance of certain wide block ciphers // J. Computer Virology Hacking Techniques. 2020. V. 16. P. 197–216.

9. *Коренева А. М., Фомичев В. М.* Перемешивающие свойства модифицированных аддитивных генераторов // Дискретн. анализ исслед. опер. 2017. Т. 24. № 2. С. 32–52.
10. *Денисенко Д. В.* О реализации подстановок в виде квантовых схем без использования дополнительных кубитов // ЖЭТФ. 2019. Т. 155. Вып. 6. С. 999–1008.
11. *Dasu V., Baksi A., Sarkar S., and Chattopadhyay A.* LIGHTER-R: Optimized reversible circuit implementation for SBoxes // 32nd IEEE Intern. System-on-Chip Conference (SOCC). Singapore, 2019. P. 260–265.
12. *Takahashi Y., Tani S., and Kunihiro N.* Quantum Addition Circuits and Unbounded Fan-Out. `https://arxiv.org/abs/0910.2530`. 2009.
13. *Boneh D. and Lipton R. J.* Quantum cryptanalysis of hidden linear functions // LNCS. 1995. V. 963. P. 424–437.

УДК 519.7 DOI 10.17223/2226308X/17/26

АТАКА НА КЛАСС 6-РАУНДОВЫХ XSL-АЛГОРИТМОВ БЛОЧНОГО ШИФРОВАНИЯ

М. А. Пудовкина, А. М. Смирнов

Анализируется класс XSL-алгоритмов блочного шифрования с алгоритмом развертывания ключа на основе рекуррентного соотношения второго порядка и матрицей линейного преобразования, у которой существуют хотя бы два равных элемента в некоторой строке обратной матрицы. Предложена атака на 6-раундовый XSL-алгоритм блочного шифрования на основе комбинирования методов встречи посередине, невозможных разностей, а также модификации подхода «yoyo». Сначала на основе обобщения метода встречи посередине формируется множество кандидатов в раундовые ключи первого раунда. Далее для получения множества кандидатов в раундовые ключи шестого раунда строится различитель, основанный на комбинации невозможных разностей и соотношений из модифицированного подхода «yoyo». Вероятность успеха равна 0,7. Полученные результаты подтверждены на модельном XSL-алгоритме блочного шифрования с 16-битным блоком открытого текста.

Ключевые слова: *XSL-алгоритм блочного шифрования, линейное преобразование, метод невозможных разностей, метод встречи посередине, разностный метод, игра «yoyo».*

Пусть $n, m \in \mathbb{N}$; $V_n(2^m)$ — n-мерное векторное пространство над полем $\mathbb{F}_{2^m}$; $\oplus$ — операция сложения в $V_n(2^m)$; 0_n — n-мерный вектор из $V_n(2^m)$, у которого все координаты равны нулю; $\mathbb{I}(A)$ — индикатор выполнения условия A; $\mathrm{GL}_n(2^m)$ — полная линейная группа на $V_n(2^m)$; $\varepsilon^{(j)} = (0, \ldots, 0, \underset{j}{1}, 0, \ldots, 0)$ для $j = 1, \ldots, n$; $S(X)$ — симметрическая группа на множестве X; $\mathbf{h} = ||h_{i,j}||$ — матрица в стандартном базисе линейного преобразования $h \in \mathrm{GL}_n(2^m)$; $\mathbf{h}^{-1} = ||h_{i,j}^{(-1)}||$ — матрица в стандартном базисе обратного преобразования h^{-1}.

Преобразования $v_k \colon V_n(2^m) \to V_n(2^m)$, $s \in S(\mathbb{F}_{2^m})$, $\tilde{s} \in S(V_n(2^m))$, $h \in \mathrm{GL}_n(2^m)$, заданные условиями

$$v_k \colon \alpha \mapsto \alpha \oplus k, \quad \tilde{s} \colon \alpha \mapsto (s(\alpha_1), s(\alpha_2), \ldots, s(\alpha_n)),$$

для всех $k \in V_n(2^m)$, $\alpha = (\alpha_1, \ldots, \alpha_n) \in V_n(2^m)$, строятся в соответствии с неформально сформулированными К. Шенноном принципами синтеза алгоритмов шифрования (см.,

например, [1]). Алгоритмы блочного шифрования, раундовая функция $g_k\colon V_n(2^m) \to V_n(2^m)$ которых задаётся условием $g_k = h\,\tilde{s}\,v_k$, называются XSL-алгоритмами. Многие современные алгоритмы блочного шифрования являются XSL-алгоритмами, например AES, 3D, ARIA, Khazad, «Кузнечик» (ГОСТ 34.12-2015) и т. д.

Будем рассматривать XSL-алгоритмы блочного шифрования, у которых:

1) алгоритм развёртывания ключа задаётся рекуррентным соотношением порядка 2;
2) матрица преобразования h в стандартном базисе такова, что существуют $l, j_1, j_2 \in \{1, \ldots, n\}$, $j_1 \neq j_2$, удовлетворяющие условию

$$h_{l,j_1}^{(-1)} = h_{l,j_2}^{(-1)}, \quad h_{l,j_1}^{(-1)} \neq 0. \tag{1}$$

Зафиксируем линейное преобразование h и элементы $l, j_1, j_2 \in \{1, \ldots, n\}$, для которых справедливы соотношения (1), и положим $h(\alpha) = \mathbf{h}\alpha^{\mathrm{T}}$ для каждого $\alpha \in V_n(2^m)$, где $^{\mathrm{T}}$ — знак транспонирования.

Зададим отображения $w\colon V_n(2^m) \to V_n(2)$ условием

$$w\colon \alpha \mapsto (w_1^{(\alpha)}, \ldots, w_n^{(\alpha)}),$$

где для всех $i \in \{1, \ldots, n\}$, $\alpha = (\alpha_1, \ldots, \alpha_n) \in V_n(2^m)$ справедливо равенство

$$w_i^{(\alpha)} = \mathbb{I}(\alpha_i \neq 0).$$

Очевидно, что

$$w(\alpha^{(1)} \oplus \alpha^{(2)}) = w(s(\alpha^{(1)}) \oplus s(\alpha^{(2)})) \tag{2}$$

для всех $\alpha^{(1)}, \alpha^{(2)} \in V_n(2^m)$, $s \in S(V_n(2^m))$. Отметим, что равенство (2) применяется в атаке [2] на 6-раундовый алгоритм блочного шифрования AES на основе подхода «yoyo». Его модификация использована также в атаке методом бумеранга на 4-раундовый алгоритм шифрования LILLIPUT-TBC-II-256.

В данной работе анализируется 6-раундовый XSL-алгоритм блочного шифрования на основе комбинирования методов встречи посередине, невозможных разностей, а также с использованием модификаций равенства (2). Сначала на основе обобщения метода встречи посередине формируется множество K_1 кандидатов в раундовые ключи первого раунда. Далее для получения множества K_6 кандидатов в раундовые ключи шестого раунда строится различитель, основанный на алгоритме нахождения невозможных разностей из работы [3], а также на следующих утверждениях.

Лемма 1. Пусть матрица преобразования h в стандартном базисе такова, что существуют $l, j_1, j_2 \in \{1, \ldots, n\}$, $j_1 \neq j_2$, удовлетворяющие условию (1). Тогда для всех $\alpha \in V_n(2^m)$, $k \in V_n(2^m)$, $\delta \in \mathbb{F}_{2^m} \setminus \{\alpha_{j_1}\}$ уравнение

$$(\tilde{s}^{-1}h^{-1}(\alpha \oplus x \cdot \varepsilon^{(j_2)} \oplus k) \oplus \tilde{s}^{-1}h^{-1}(\alpha \oplus \delta \cdot \varepsilon^{(j_1)} \oplus (x \oplus \delta)\,\varepsilon^{(j_2)} \oplus k))_l = 0$$

имеет 2^m решений относительно $x \in \mathbb{F}_{2^m}$.

Утверждение 1. Пусть $\alpha^{(1)}, \alpha^{(2)}, k^{(1)}, k^{(2)}$ — произвольные элементы пространства $V_n(2^m)$, $\beta^{(i)} = k^{(2)} \oplus hs(k^{(1)} \oplus h(\alpha^{(i)}))$ для $i = 1, 2$. Тогда справедливо равенство

$$w(h^{-1}(\beta^{(1)} \oplus \beta^{(2)})) = w(h(\alpha^{(1)} \oplus \alpha^{(2)})). \tag{3}$$

Заметим, что равенство (3) является модификацией равенства (2).

После получения множеств K_1, K_6 для нахождения ключа достаточно выполнить $|K_1| \cdot |K_6|$ шифрований.

Показано, что для атаки требуется $2^{m(n-1)}$ текстов, 2^{2m+1} бит памяти. Её трудоёмкость оценивается как

$$7 \cdot 17^{n-2} \cdot 2^{2nm-n+2} \cdot 10^{1-n} \cdot \left(1 - \frac{n}{2^m - 1}\right)^d$$

зашифрований, где d — число повторяющихся элементов в каждом столбце матрицы линейного преобразования h. Вероятность успеха равна 0,7. Полученные результаты подтверждены на модельном XSL-алгоритме блочного шифрования SMALL-XSL при $n = m = 4$. Отметим, что предложенная атака отличается общностью и применима для любого XSL-алгоритма из рассматриваемого класса.

ЛИТЕРАТУРА

1. Словарь криптографических терминов / под ред. Б. А. Погорелова, В. Н. Сачкова. М.: МЦНМО, 2006. 50 с.
2. *Rønjom S., Bardeh N. G., and Helleseth T.* Yoyo tricks with AES // LNCS. 2017. V. 10624. P. 217–243.
3. *Shen X., Liu G., Sun B., and Li C.* Impossible differentials of SPN ciphers // LNCS. 2017. V. 10143. P. 47–63.
4. *Пудовкина М. А., Смирнов А. М.* Анализ методом бумеранга 4-раундового алгоритма шифрования LILLIPUT-TBC-II-256 // Прикладная дискретная математика. Приложение. 2023. Т. 16. С. 81–84.

УДК 519.7 DOI 10.17223/2226308X/17/27

ДЕСЯТЬ ЛЕТ МЕЖДУНАРОДНОЙ ОЛИМПИАДЕ ПО КРИПТОГРАФИИ NSUCRYPTO[1]

Н. Н. Токарева

Работа посвящена истории развития Международной олимпиады по криптографии Non-Stop University CRYPTO, её открытым проблемам и результатам.

Ключевые слова: *NSUCRYPTO, олимпиада, криптография.*

Международная олимпиада по криптографии NSUCRYPTO отметила свой юбилей. История олимпиады началась в 2014 г., когда наша новосибирская команда придумала и воплотила идею исследовательской криптографической олимпиады. С тех пор каждый октябрь олимпиада собирает своих участников и сторонников.

Non-Stop University CRYPTO — это единственная международная олимпиада по криптографии, которая объединяет профессионалов, студентов и школьников со всего мира. Принять участие в олимпиаде может любой желающий, независимо от географического положения. Официальный язык олимпиады — английский. Цель олимпиады — привлечь молодых исследователей к решению вопросов современной криптографии. Ежегодно олимпиада проводится онлайн в два независимых раунда: индивидуальный и командный. Программный комитет состоит из российских и зарубежных

[1]Работа выполнена при поддержке Математического центра в Академгородке, соглашение с Министерством науки и высшего образования Российской Федерации № 075-15-2022-282.

специалистов, которые являются экспертами в различных областях криптографии и дискретной математики. Тематика задач обширна. В задачах встречаются классические криптографические примитивы и алгоритмы, известные и новые шифры, онлайн-шифрмашины, пароли и двоичные строки, компоненты шифров и дискретные функции, криптографические протоколы, квантовые схемы и алгоритмы, эллиптические кривые, блокчейн-системы и криптовалюты, элементы стеганографии и маскирования, элементы реализация функций на микросхеме, криптоанализ и многое другое.

Все десять прошедших олимпиад были успешными. За десять лет победителями и призёрами олимпиады стали представители 36 стран, тогда как общее число стран-участниц превысило 70. В общем медальном зачете лидируют Россия, Вьетнам, Румыния, Германия, Индия, Китай и Венгрия.

Отметим некоторые особенности прошедших олимпиад. В 2014 г. олимпиада была ещё сибирской, с 2016 г. стала международной. В 2020 г. олимпиаду открывала видеолекция от одного из членов программного комитета, а в 2021 г. олимпиада была посвящена 100-летию Криптографической службы России. В 2023 г. в олимпиаде приняли участие более 1100 студентов, школьников и профессионалов из 44 стран мира. Традиционно более 95 % всех участников — в возрасте до 40 лет.

Открытые проблемы для участников олимпиады предлагают как отечественные криптографы, так и представители зарубежных школ, например разработчики стандартов AES, SHA-3, 3DES, Chaskey MAC и др. За десять лет на олимпиаде было представлено 36 нерешённых задач, 13 из которых были полностью или частично решены участниками. Каждый год по следам олимпиады выходит научная статья с разбором решений задач олимпиады, но не только: ежегодно появляются и другие публикации, связанные с решением открытых проблем олимпиады.

NSUCRYPTO является единственной олимпиадой от России (и одной из семнадцати по всему миру), которая учитывается в рейтинге вузов при анализе побед студентов в международных олимпиадах по разным областям науки; рейтинг подготовлен при поддержке Российского союза ректоров. Победы студентов на NSUCRYPTO также учитываются в рейтинге вузов RAEX-100.

В 2024 г. организаторами и партнёрами олимпиады выступают Криптографический центр (г. Новосибирск), Национальный технологический центр цифровой криптографии, Новосибирской государственный университет, Северо-Западный центр математических исследований имени Софьи Ковалевской, Университет г. Лёвена (Бельгия), компании «Криптонит» и «Актив», Южный федеральный университет, Белорусский государственный университет, Томский государственный университет.

Мы приглашаем наших старых и новых друзей к участию в олимпиаде 2024 г. [1], а также анонсируем выход книги [2] к юбилею олимпиады.

ЛИТЕРАТУРА

1. Сайт Олимпиады `www.nsucrypto.nsu.ru`.
2. *Tokareva N.* International Olympiad in Cryptography — NSUCRYPTO. History, Persons, Problems, and Solutions. Monography, to appear. 2024.

УДК 004.056 DOI 10.17223/2226308X/17/28

АНАЛИЗ ПАРАМЕТРОВ ПОСТКВАНТОВОЙ СХЕМЫ ПОДПИСИ ГИПЕРИКУМ

О.Ю. Турченко, С.Р. Усманов

Работа посвящена анализу параметров постквантовых схем подписи на основе хешей без сохранения состояния (SPHINCS$^+$, SPHINCS$^+$C и Гиперикум). Предлагаются новые наборы параметров, обеспечивающие 120-битную стойкость к подделке против квантового злоумышленника. Выбор наборов осуществлялся с учётом прикладных характеристик и возможных областей применения рассматриваемых схем.

Ключевые слова: *Гиперикум, SPHINCS$^+$, постквантовая криптография, схемы подписи.*

Схемы подписи на основе хешей без сохранения состояния являются одними из наиболее перспективных схем в постквантовую эпоху. Так, например, схема SPHINCS$^+$ [1] вошла в финал конкурса NIST [2] и является проектом стандарта FIPS 205 [3]. Данная схема имеет ряд модификаций [4–6], среди которых можно отметить схему Гиперикум [6], являющуюся проектом квантово-устойчивой цифровой подписи для стандартизации в Российской Федерации. Несмотря на активное исследование подобных схем, вопрос выбора параметров не решён до конца. Например, авторы SPHINCS$^+$ не приводят объяснения выбора наборов параметров, предлагаемых для стандартизации. На данный момент есть лишь небольшое число работ, посвящённых анализу параметров [7, 8]. В [7] авторы анализируют характеристики подписи при различных границах максимального числа подписей на одном ключе и предлагают новые наборы параметров с уменьшенной границей. Несмотря на улучшение прикладных характеристик подписи, данный подход вызывает вопросы. Во-первых, для уменьшения подписи в 2 раза граница должна быть менее 2^{20}, тогда как в оригинальном SPHINCS$^+$ она равна 2^{64}. В таком случае схема не в полной мере является подписью без сохранения состояния и теряется целесообразность использования мета-схемы SPHINCS$^+$. Например, XMSS-MT [9] с минимальным набором параметров позволяет подписывать до 2^{20} подписей и обладает более эффективными прикладными характеристиками. Во-вторых, авторы [7] при подборе параметров не придают значения времени формирования подписи и приоритезируют скорость её проверки. Такой подход обосновывается тем, что «подписание происходит нечасто». Однако для таких устройств, как смарт-карты, платёжные карты и HSM, время формирования подписи является наиболее значимой характеристикой. В работе [8] предлагаются альтернативные наборы параметров для различных уровней стойкости, но при этом игнорируется скорость проверки подписи. Авторы также не приводят описание выбора данных наборов.

В настоящей работе описывается метод выбора параметров. В силу того, что схема Гиперикум использует хеш-функцию, согласно ГОСТ 34.11-2018 [10], с длиной выхода 256 бит, исследовались только наборы параметров, обеспечивающие 120-битную стойкость к подделке против квантового злоумышленника (для получения наборов параметров со стойкостью около 96 или 64 необходимо использовать хеш-функции с длиной выхода 196 и 128 бит соответственно). В таблице приведены полученные наборы параметров. Первые пять столбцов отвечают за внутренние параметры схемы, описанные в [1]. В столбце «Подпись» указан размер подписи в байтах. Столбцы «**H** для под.»

и «**H** для пров.» обозначают приблизительное число вызовов функции хеширования для формирования и проверки подписи соответственно.

Тип	h	d	b	k	w	Подпись, байт	**H** для под.	**H** для пров.
Быстр. подпись	66	22	9	36	16	58 460	217 946	11 645
Мал. подпись	68	4	18	14	16	18 292	544 472 693	2 350
По умолчанию	64	8	14	21	16	28 068	2 770 880	4 440

Набор «Быстр. подпись» близок к набору 256f из SPHINCS$^+$, но вычисляет подпись быстрее в 1,45 раз за счёт увеличения размера подписи в 1,2 раза. Набор «Мал. подпись» подразумевает использование в областях, где время подписи не является существенным (например, для доверенной загрузки). Стоит отметить, что, несмотря на незначительное увеличение подписи относительно набора 128f, данный набор обладает в 2 раза большей стойкостью. Набор «По умолчанию» является промежуточным между новыми наборами; он очень близок к набору 256s, но превосходит его по всем характеристикам.

ЛИТЕРАТУРА

1. SPHINCS$^+$. `https://sphincs.org/data/sphincs+-r3.1-specification.pdf`.
2. NIST. `https://csrc.nist.gov/Projects/Post-Quantum-Cryptography`.
3. FIPS 205. `https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.205.ipd.pdf`.
4. *Hülsing A., Kudinov M., Ronen E., and Yogev E.* SPHINCS$^+$C: Compressing SPHINCS$^+$ with (almost) no cost // IEEE Symp. Security Privacy. San Francisco, 2023. P. 1435–1453.
5. *Zhang K., Cui H., and Yu Y.* SPHINCS-α: A Compact Stateless Hash-Based Signature Scheme. Cryptology ePrint Archive. Paper 2022/059. 2022. P. 1–23.
6. Гиперикум. Проект квантово-устойчивой цифровой подписи для стандартизации в России. `https://www.ruscrypto.ru/resource/archive/rc2023/files/02_grebnev.pdf`.
7. *Kolbl S. and Philipoom J.* A Note on SPHINCS$^+$ Parameter Sets. Cryptology ePrint Archive. Paper 2022/1725. 2022. P. 1–11.
8. *Lee J., Kang T. G., Cho K., and Yum D. H.* New parameter sets for SPHINCS$^+$ // IEICE Trans. Inform. Systems. 2021. No. 6. P. 890–892
9. XMSS: eXtended Merkle Signature Scheme. `https://datatracker.ietf.org/doc/html/rfc8391`.
10. ГОСТ 34.11-2018. `https://protect.gost.ru/document.aspx?control=7&id=232143`.

УДК 519.7 DOI 10.17223/2226308X/17/29

О ПЕРЕМЕШИВАЮЩИХ СВОЙСТВАХ РЕГИСТРОВЫХ ПРЕОБРАЗОВАНИЙ АЛГОРИТМОВ ШИФРОВАНИЯ TEA1 И TEA2

П. А. Чежегова, А. М. Коренева, М. В. Поляков, Г. В. Фирсов

С использованием матрично-графового подхода исследуются перемешивающие свойства регистровых преобразований поточных алгоритмов шифрования TEA1 и TEA2 стандарта цифровой транкинговой радиосвязи TETRA. Получены значения экспонентов перемешивающих матриц, соответствующих регистровым преобразованиям исследуемых алгоритмов. Результаты могут быть использованы для оценки числа тактов работы регистров преобразования ключа в алгоритмах поточного шифрования, необходимых для обеспечения существенной зависимости каждого бита выходной последовательности от всех битов ключа.

Ключевые слова: *матрично-графовый подход, перемешивающие свойства, экспонент матрицы, регистр сдвига, TETRA.*

1. Описание поточных шифров TEA1 и TEA2

TErrestrial Trunked RAdio (TETRA) — стандарт цифровой транкинговой радиосвязи, разработанный Европейским институтом телекоммуникационных стандартов (European Telecommunications Standards Institute, ETSI). Стандарт включает в себя четыре алгоритма поточного шифрования — TEA1, TEA2, TEA3, TEA4 (TEA — TETRA Encryption Algorithm), которые применяются для шифрования голосовых сообщений. В данной работе рассмотрены алгоритмы TEA1 и TEA2, разработанные в 1996–1997 гг. Спецификации алгоритмов TEA1, TEA2 и TEA3 впервые были опубликованы в 2023 г. независимой группой исследователей из Midnight Blue [1]. Спецификация TEA4 отсутствует в открытых источниках, а оценка свойств алгоритма TEA3 является предметом дальнейшего исследования.

Генератор гаммы алгоритмов шифрования TEA1 и TEA2 построен на основе двух регистров сдвига с обратной связью над векторным пространством V_8, один из которых является регистром, выполняющим преобразование ключа (далее — регистр преобразования ключа). Длина данного регистра для TEA1 равна 4, для TEA2 — 10. Регистр преобразования ключа инициализируется 80-битным ключом, однако в случае алгоритма TEA1 ключ предварительно сокращается до последних 32 бит, преобразованных с использованием s-бокса.

Введём следующие обозначения: V_8 — множество 8-мерных двоичных векторов; $\oplus$ — операция покомпонентного сложения векторов из V_8 по модулю 2.

В алгоритме TEA1 для преобразования ключа используется регистр R_1 с одной обратной связью (рис. 1).

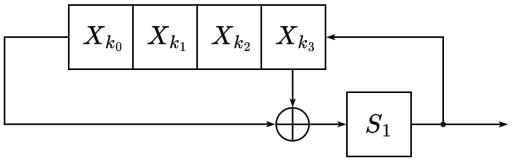

Рис. 1. Регистр R_1

Пусть $(X_{k_0}, \ldots, X_{k_3})$ — начальное состояние регистра R_1, где $X_{k_0}, \ldots, X_{k_3} \in V_8$. Тогда преобразование φ_1 множества состояний регистра имеет вид

$$\varphi_1(X_{k_0}, \ldots, X_{k_3}) = (X_{k_1}, X_{k_2}, X_{k_3}, S_1(X_{k_0} \oplus X_{k_3})),$$

где S_1 — функция s-бокса алгоритма TEA1.

В алгоритме TEA2 для преобразования ключа используется регистр R_2 с одной обратной связью (рис. 2).

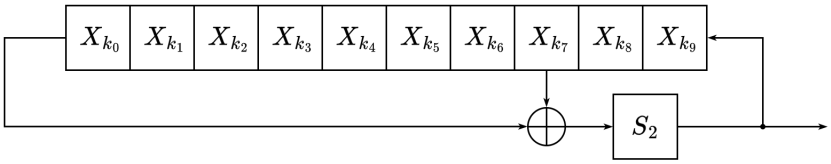

Рис. 2. Регистр R_2

Пусть $(X_{k_0}, \ldots, X_{k_9})$ — начальное состояние регистра R_2, где $X_{k_0}, \ldots, X_{k_9} \in V_8$. Тогда преобразование φ_2 множества состояний регистра имеет вид

$$\varphi_2(X_{k_0}, \ldots, X_{k_9}) = (X_{k_1}, \ldots, X_{k_9}, S_2(X_{k_0} \oplus X_{k_7})),$$

где S_2 — функция s-бокса алгоритма TEA2.

2. Методология исследования и полученные результаты

Используем матрично-графовый подход [2–5], позволяющий оценить наименьшую глубину композиции функций, при которой возможно полное перемешивание — зависимость каждого бита выходного значения от всех битов входного вектора (в данной работе — битов ключа). Матрично-графовый подход основан на построении перемешивающей матрицы преобразования — квадратной матрицы (m_{ij}), где $m_{ij} = 1$ тогда и только тогда, когда i-я координата выходного значения существенно зависит от j-й координаты входного вектора. Затем для построенной матрицы находится значение её экспонента — наименьшей степени, в которой она является положительной, то есть не содержит нулевых элементов [2].

Построены перемешивающие матрицы M_1 размера 32×32 и M_2 размера 80×80 для алгоритмов TEA1 и TEA2 соответственно. Для каждой матрицы найдено значение экспонента: $\exp M_1 = 6$, $\exp M_2 = 34$.

3. Выводы

Полученные результаты дают нижнюю оценку числа тактов работы регистров преобразования ключа, при котором достигается полное перемешивание.

В стандарте TETRA в ключевом преобразовании шифра TEA1 регистр R_1 вырабатывает первый байт гаммы за 54 такта работы, а последующие — за 19 тактов. В ключевом преобразовании шифра TEA2 первый байт гаммы вырабатывается за 51 такт, последующие — также за 19. Наши результаты не противоречат выбранным разработчиками параметрам алгоритмов. В то же время представляется возможным использование регистровых преобразований ключа рассмотренных алгоритмов с меньшим количеством тактов холостого хода без ухудшения перемешивающих свойств для криптографических приложений в условиях ограниченных ресурсов.

ЛИТЕРАТУРА

1. *Meijer C., Bokslag W., and Wetzels J.* All Cops are Broadcasting: TETRA under Scrutiny. `https://www.cryptomuseum.com/radio/tetra/files/tetra_paper.pdf`. 2023.
2. *Фомичёв В. М., Авезова Я. Э., Коренева А. М., Кяжин С. Н.* Примитивность и локальная примитивность орграфов и неотрицательных матриц // Дискретный анализ и исследование операций. 2018. Т. 25. № 3. С. 95–125.
3. *Коренева А. М., Фомичёв В. М.* Перемешивающие свойства модифицированных аддитивных генераторов // Дискретный анализ и исследование операций. 2017. Т. 24. № 2. С. 32–52.
4. *Фомичёв В. М., Мельников Д. А.* Криптографические методы защиты информации. Ч. 1. Математические аспекты: учебник для вузов. М.: Юрайт, 2024. 209 с.
5. *Fomichev V. M., Koreneva A. M., Miftakhutdinova A. R., and Zadorozhny D. I.* Evaluation of the maximum performance of block encryption algorithms // Матем. вопр. криптогр. 2019. Т. 10. № 2. С. 181–191.

Секция 4

МАТЕМАТИЧЕСКИЕ ОСНОВЫ ИНФОРМАТИКИ И КОМПЬЮТЕРНОЙ БЕЗОПАСНОСТИ

УДК 519.682 DOI 10.17223/2226308X/17/30

О РЕШЕНИИ ЛИНЕЙНЫХ ОДНОРОДНЫХ ГРАММАТИК, ПОРОЖДАЮЩИХ ЛИНЕЙНЫЕ ЯЗЫКИ

О. И. Егорушкин, И. В. Колбасина, К. В. Сафонов

Исследуются системы некоммутативных символьных линейных однородных уравнений, которые интерпретируются как линейные грамматики формальных языков. Такие системы решаются в виде формальных степенных рядов (ФСР), выражающих нетерминальные символы через терминальные символы алфавита и рассматриваемых как линейные языки. Всякому ФСР поставлен в соответствие его коммутативный образ, который получается в предположении, что все символы обозначают коммутативные переменные, действительные или комплексные. Рассматриваются системы уравнений, которые могут иметь бесконечное множество решений, параметризуемых не произвольными числами, а произвольными ФСР. Оценено количество таких параметров, что даёт некоммутативный аналог известного факта теории линейных уравнений.

Ключевые слова: *системы линейных однородных уравнений, некоммутативные переменные, формальный степенной ряд, коммутативный образ.*

Теория формальных языков имеет очень важное значение в области информационных технологий и программирования, поскольку на её основе реализуются алгоритмы машинного перевода текстов и анализа языков программирования. Все эти алгоритмы используют взаимосвязи языка (как множества возможных текстов) с грамматикой (сводом формальных правил, определяющих языковые конструкции). Во многих областях нужны быстрые качественные алгоритмы формальных построений грамматики по языку и языка по грамматике, а также синтаксического анализа конструкций, которые невозможны без серьёзного теоретического обоснования.

Контекстно-свободные, в частности линейные, грамматики активно используются для решения задач, связанных с разработкой формальных языков и анализаторов синтаксических конструкций [1–3]. Одним из основных достоинств контекстно-свободных и линейных грамматик является относительная компактность представления при возможности задания большого объёма языков [4, 5].

Продолжая исследование, начатое в работах [1, 2], рассмотрим однородную систему символьных линейных уравнений с полиномиальными коэффициентами

$$a_{i1}(x)z_1b_{i1}(x) + \ldots + a_{in}(x)z_nb_{in}(x) = 0, \quad i = 1, \ldots, k, \tag{1}$$

которая решается относительно некоммутативных символов $z = (z_1, \ldots, z_n)$ в виде ФСР, зависящих от некоммутативных символов $x = (x_1, \ldots, x_m)$, где $a_{ij}(x), b_{ij}(x)$ — многочлены [3, 4].

Такие системы имеют приложения в теории формальных языков, поскольку их можно рассматривать как грамматики, порождающие важный подкласс класса ли-

нейных языков, определяемых как однородными, так и неоднородными системами уравнений [3, 4].

При этом символы $x_1, \ldots, x_m$ называются терминальными и составляют словарь языка, а символы $z_1, \ldots, z_n$ — нетерминальными и участвуют в задании грамматических правил. В этих условиях действует конкатенация — некоммутативное умножение, а также коммутативное формальное сложение и коммутативная операция умножения на числа.

Решать символьную некоммутативную систему (1) трудно, поэтому рассмотрим её коммутативный образ [1, 2, 5]. Для этого поставим в соответствие ФСР s его коммутативный образ $\mathrm{ci}(s)$ — степенной ряд, который получается из s в предположении, что символы $x_1, \ldots, x_m$, а также $z_1, \ldots, z_n$ обозначают коммутативные переменные, принимающие значения из поля действительных или комплексных чисел [5].

Понятно, что коммутативным образом системы (1) является система коммутативных уравнений

$$\mathrm{ci}(a_{i1}(x))\mathrm{ci}(b_{i1}(x))z_1 + \ldots + \mathrm{ci}(a_{in}(x))\mathrm{ci}(b_{in}(x))z_n = 0, \quad i = 1, \ldots, k. \tag{2}$$

Назовём рангом матрицы, элементами которой являются многочлены от коммутативных переменных, число линейно независимых столбцов матрицы над полем комплексных чисел, и для системы коммутативных уравнений (2) рассмотрим её матрицу

$$\Big(\mathrm{ci}(a_{ij}(x))\mathrm{ci}(b_{ij}(x)\Big).$$

В линейной алгебре хорошо известен следующий факт: если

$$\mathrm{rank}\left(\mathrm{ci}(a_{ij}(x))\mathrm{ci}(b_{ij}(x))\right) = k,$$

то система уравнений (2) имеет бесконечное множество решений, которое параметризуется t числовыми параметрами (зависит от них), причём $t = n - k$.

Возвращаясь к системе некоммутативных символьных линейных уравнений (1), дадим следующее определение:

Определение 1. Будем говорить, что полиномиальная грамматика (1) имеет бесконечное множество решений (порождает бесконечное множество языков), если множество решений системы (1) зависит хотя бы от одного произвольного ФСР от символов $x_1, \ldots, x_m$.

Так, система из двух одинаковых уравнений

$$x_1 z_1 - z_2 x_2 = 0$$

имеет бесконечное множество решений, поскольку решения

$$z_1 = s x_2, \;\; z_2 = x_1 s$$

зависят от одного произвольного ФСР s от x_1, x_2.

Для системы некоммутативных линейных уравнений ситуация, естественно, сложнее, чем для коммутативных. Указанный факт линейной алгебры имеет следующий аналог для некоммутативного случая:

Теорема 1. Если для коммутативного образа (2) системы некоммутативных линейных уравнений (1) выполнено равенство

$$\operatorname{rank}\left(\operatorname{ci}(a_{ij}(x))\operatorname{ci}(b_{ij}(x))\right) = k,$$

то исходная система некоммутативных уравнений (1) имеет решения, зависящие от t произвольных ФСР, где $t \leqslant n - k$.

Нетрудно привести примеры, для которых неравенство строгое.

Поскольку ФСР, которые являются компонентами решения системы (1), интерпретируются как формальные языки, теорема 1 позволяет установить структуру линейного языка, порождаемого линейной грамматикой.

ЛИТЕРАТУРА

1. *Егорушкин О. И., Колбасина И. В., Сафонов К. В.* О совместности систем символьных полиномиальных уравнений и их приложении // Прикладная дискретная математика. Приложение. 2016. № 9. С. 119–121.
2. *Egorushkin O. I., Kolbasina I. V., and Safonov K. V.* On solvability of systems of symbolic polynomial equations // Журн. СФУ. Сер. Матем. и физ. 2016. Т. 9. Вып. 2. С. 166–172.
3. *Глушков В. М., Цейтлин Г. Е., Ющенко Е. Л.* Алгебра. Языки. Программирование. Киев: Наукова думка, 1973.
4. *Salomaa A. and Soitolla M.* Automata-Theoretic Aspects of Formal Power Series. N.Y.: Springer Verlag, 1978.
5. *Семёнов А. Л.* Алгоритмические проблемы для степенных рядов и контекстно-свободных грамматик // Доклады АН СССР. 1973. № 212. С. 50–52.

УДК 519.1, 004.05 DOI 10.17223/2226308X/17/31

ПРИМЕНЕНИЕ КОНЕЧНЫХ ДИНАМИЧЕСКИХ СИСТЕМ ДЛЯ ЗАЩИТЫ ИНФОРМАЦИИ И ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

А. В. Жаркова

Графовые модели занимают важное место в задачах, связанных с защитой информации и информационной безопасностью. Рассматривается конечная динамическая система, состояниями которой являются все возможные ориентации данного графа, а эволюционная функция задаётся следующим образом: динамическим образом данного орграфа является орграф, полученный из исходного путём переориентации всех дуг, входящих в стоки, других отличий между исходным орграфом и его образом нет. Предлагается, как можно применять данную систему для защиты информации и информационной безопасности, а именно: как модель обеспечения аудита и мониторинга состояния объекта, находящегося под воздействием угроз нарушения его информационной безопасности, и расследования инцидентов информационной безопасности в автоматизированных информационных системах; как модель управления непрерывным функционированием и восстановлением систем, противодействия отказам в обслуживании; как технологию идентификации и аутентификации пользователей и субъектов информационных процессов, систему разграничения доступа.

Ключевые слова: *аттрактор, аутентификация, граф, идентификация, инцидент, кибербезопасность, конечная динамическая система, отказоустойчивость, эволюционная функция.*

Основные понятия теории дискретных систем, в частности графов, используются согласно [1].

Под *конечной динамической системой* понимается пара $(S,\ \delta)$, где S — конечное непустое множество состояний системы; $\delta : S \to S$ — отображение множества состояний в себя, называемое *эволюционной функцией системы*. Каждой конечной динамической системе сопоставляется карта, представляющая собой функциональный орграф с множеством вершин S и дугами, проведёнными из каждой вершины $s \in S$ в вершину $\delta(s)$. Компоненты связности орграфа, задающего динамическую систему, называются её *бассейнами*. Каждый бассейн представляет собой контур с входящими в него деревьями. Контуры, в свою очередь, называются *предельными циклами*, или *аттракторами*. Состояние, не имеющее непосредственных предшественников, называется *недостижимым* или *начальным* состоянием системы. *Индекс* состояния — его расстояние до аттрактора того бассейна, которому оно принадлежит.

Пусть дан некоторый граф G. Пометим его вершины и придадим его рёбрам произвольную ориентацию, тем самым получив ориентированный граф $\overrightarrow{G}$. Применим к полученному орграфу эволюционную функцию α, которая одновременно переориентирует все дуги, входящие в стоки, а остальные дуги оставляет без изменения, в результате получим орграф $\alpha(\overrightarrow{G})$. Если проделать эти действия со всеми возможными ориентациями данного графа, то получим карту динамической системы. Данная динамика для бесконтурных связных орграфов введена в [2]. Итак, будем рассматривать конечную динамическую систему (Γ_G, α), где через Γ_G обозначим множество всех возможных ориентаций данного графа G, а эволюционная функция α задаётся следующим образом: если дан некоторый орграф $\overrightarrow{G} \in \Gamma_G$, то его динамическим образом $\alpha(\overrightarrow{G})$ является орграф, полученный из $\overrightarrow{G}$ одновременной переориентацией всех дуг, входящих в стоки, других отличий между $\overrightarrow{G}$ и $\alpha(\overrightarrow{G})$ нет.

В работах автора представлены разнообразные характеристики данных систем (например, [3]).

Рассмотрим, как можно применять систему (Γ_G, α) для защиты информации и информационной безопасности.

Подходы и понятия в области информационной безопасности используются согласно отечественным стандартам, в том числе [4–6].

Объект — пассивная сущность в пределах системы, которая содержит или получает информацию и над которой субъекты выполняют операции. *Субъект* — активная сущность в системе, выполняющая операции над объектами.

Любая сущность системы в произвольный момент времени может быть однозначно представлена словом некоторого языка (набором данных), которое может рассматриваться как состояние сущности [7, 8].

I. *Конечная динамическая система всех возможных ориентаций данного графа как модель обеспечения аудита и мониторинга состояния объекта, находящегося под воздействием угроз нарушения его информационной безопасности, и расследования инцидентов информационной безопасности в автоматизированных информационных системах*

Представим объект автоматизированной информационной системы (АИС) конкретной динамической системой, для чего выберем подходящий граф. Все необходимые параметры объекта последовательно закодируем соответствующими состояниями

полученной системы. Если в объекте происходят изменения в результате санкционированного доступа, то должна быть сохранена динамика. Если в какой-то момент времени не выполняются необходимые связи и элементы динамики — фиксируется инцидент. По конкретным состояниям можно отследить, с чего он начался и как развивался.

Пример 1. Пусть объектом является папка, содержащая в себе f файлов.

Для построения модели необходимо выполнить следующие действия:

1) у каждого файла последовательно зафиксировать p параметров: хеш-код, имя, тип и другие;
2) задать подходящую динамическую систему: выбрать граф G с количеством рёбер $m \geqslant \log_2(fp)$ ($|\Gamma_G| \geqslant fp$), количеством недостижимых состояний не менее чем f, максимальным индексом не менее чем p, желательно, чтобы индекс недостижимых состояний был не менее чем p;
3) создать хеш-таблицу, в которой 2^{fp} строк и 3 столбца: номер строки (индекс), параметр (ключ), состояние (значение);
4) для каждого файла последовательно занести его значения в таблицу, при этом хеш-коду файла ставится в соответствие уникальное недостижимое состояние $\overrightarrow{G}_{u_i}$, а далее для каждого следующего k-го параметра значение-состояние равно $\alpha^k(\overrightarrow{G}_{u_i})$, $1 \leqslant k < p$. Специфика организации хеш-таблицы (например, с открытой адресацией, списками, вместе или отдельно хранить одинаковые параметры) остаётся на усмотрение разработчика;
5) если в объекте происходят изменения в результате санкционированного доступа, обновить соответствующие значения в таблице;
6) при обращении к файлу по таблице проверить его динамику (вычислить значения по аналогии с действием 4, проверить и сравнить вычисленные и хранимые значения), при её нарушении зафиксировать инцидент, согласно менеджменту инцидентов информационной безопасности в данной организации. По тем элементам, где произошли изменения, отследить историю инцидента (например, у нескольких параметров нарушены состояния и динамика, а у остальных они сохранены, на основании полученных данных сделать соответствующие выводы).

Дополнительно можно хранить хеш-код таблицы для проверки её целостности; если будет обнаружено нарушение целостности, аналогично можно будет найти, где именно произошли изменения.

Например, при $f = 66864$, $p = 8$ (хеш-код, имя, тип, путь к папке, размер, дата создания, дата изменения, владелец) $fp = 534912$ ($m = 20$) и файл с хеш-таблицей займёт около 24 Мбайт (при архивации — около 76 Кбайт).

II. *Конечная динамическая система всех возможных ориентаций данного графа как модель управления непрерывным функционированием и восстановлением систем, противодействия отказам в обслуживании*

В системе есть объекты и субъекты. Каждый параметр сущностей кодируется 0 или 1, тем самым получаем (индивидуальное) состояние сущности. Все они представляются состояниями подходящей симметричной динамической системы. При возникновении отказа для непрерывности функционирования действие переходит на другую симметричную ветку. Производится анализ, в связи с чем происходит сбой, далее идёт восстановление благодаря динамике.

Пример 2. Пусть в системе есть f объектов и субъектов.

Для построения модели необходимо выполнить следующие действия:

1) у каждой сущности последовательно зафиксировать p параметров, каждый параметр закодировать 0 или 1 (получим состояние сущности);
2) задать подходящую динамическую систему: выбрать граф G с n вершинами и количеством рёбер $m \geqslant p$, $m \geqslant \log_2(2f)$ ($|\Gamma_G| \geqslant 2f$); данная система должна быть симметрична (например, G — n-рёберный цикл);
3) создать хеш-таблицу, в которой 2^m строк и 3 столбца: номер строки (индекс), состояние сущности (ключ), несколько предшествующих и последующих сущностей (значение);
4) для каждой сущности последовательно занести её значения в таблицу;
5) если в сущностях происходят изменения в результате санкционированного доступа, обновить соответствующие значения в таблице;
6) при обращении к сущности проверить значения по таблице, при выявлении нарушений зафиксировать несанкционированные изменения и отказы в системе, работу данных сущностей переключить на симметричную ветку для непрерывности функционирования;
7) произвести анализ и поиск, где именно произошёл сбой, сущности (их состояния) и всю систему восстановить благодаря динамике (по верным хранимым предшествующим и последующим сущностям и их значениям).

Для уникальности задания сущностей можно субъектам назначить недостижимые состояния, использовать биты для указания появления коллизий и соответствующего сдвига, что учитывается при задании кодировки.

Дополнительно можно хранить хеш-код таблицы для проверки её целостности.

Описание доступов субъектов к объектам можно изначально представить элементами системы, благодаря чему отслеживать динамику и аналогичным образом поддерживать непрерывность функционирования, своевременно реагировать на отказы и восстанавливать систему.

III. *Конечные динамические системы всех возможных ориентаций данных графов как технология идентификации и аутентификации пользователей и субъектов информационных процессов, система разграничения доступа*

В системе есть объекты и субъекты. Представим объекты аттракторами динамических систем, для чего выберем подходящие графы. Каждый субъект получает дополнительный идентификатор — ориентацию графа из того бассейна, которому принадлежит данный объект. При аутентификации проверяется принадлежность данного состояния бассейну и доступ к объекту предоставляется или отказывается в нём.

Пример 3. Пусть в системе субъектами являются s пользователей, объектами — f различных папок с данными.

Для построения системы необходимо выполнить следующие действия:

1) задать подходящие динамические системы: выбрать графы G_i с общим количеством бассейнов в системе не менее чем f;
2) каждому объекту поставить в соответствие один или несколько аттракторов;
3) каждому субъекту назначить (дополнительный) идентификатор — ориентацию графа из того бассейна, которому принадлежит объект, к которому субъекту необходимо предоставить доступ;
4) если в сущностях происходят санкционированные изменения (идентификатора по запросу пользователя, прав доступа по запросу администратора и другие), обновить соответствующие значения;

5) при доступе субъекта к объекту доступа для аутентификации проверить принадлежность данного идентификатора субъекта бассейну, которому принадлежит объект, при успешной проверке предоставить доступ к объекту, в противном случае отказать в доступе.

Для идентификаторов можно выбрать также недостижимые состояния. Дополнительно можно задать соответствующие виды прав доступа с помощью выбранных для этого дуг в состоянии.

ЛИТЕРАТУРА

1. *Богомолов А. М., Салий В. Н.* Алгебраические основы теории дискретных систем. М.: Наука, Физматлит, 1997.
2. *Barbosa V. C.* An Atlas of Edge-Reversal Dynamics. London: Chapman&Hall/CRC, 2001.
3. *Жаркова А. В.* О конечной динамической системе всех возможных ориентаций данного графа со всеми достижимыми и с недостижимыми состояниями // Прикладная дискретная математика. Приложение. 2022. № 15. С. 105–107.
4. ГОСТ Р ИСО/МЭК 15408-1-2012. Национальный стандарт Российской Федерации. Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Ч. 1. Введение и общая модель. М.: Стандартинформ, 2014.
5. ГОСТ Р 58833-2020. Национальный стандарт Российской Федерации. Защита информации. Идентификация и аутентификация. Общие положения. М.: Стандартинформ, 2020.
6. ГОСТ Р 59383-2021. Национальный стандарт Российской Федерации. Информационные технологии. Методы и средства обеспечения безопасности. Основы управления доступом. М.: Стандартинформ, 2021.
7. *Грушо А. А., Применко Э. А., Тимонина Е. Е.* Теоретические основы компьютерной безопасности. М.: Изд. центр «Академия», 2009.
8. *Девянин П. Н.* Модели безопасности компьютерных систем. Управление доступом и информационными потоками. М.: Горячая линия-Телеком, 2013.

УДК 004.42 DOI 10.17223/2226308X/17/32

СИСТЕМА ЗАМЕРА ЭФФЕКТИВНОСТИ ВНУТРЕННЕГО ПРЕДСТАВЛЕНИЯ СХЕМ ZK-SNARK[1]

Д. О. Кондырев

Разработана программная система замера эффективности внутреннего представления схем zk-SNARK. Система предназначена для измерения параметров схем доказательства с нулевым разглашением zk-SNARK — количества ограничений во внутреннем представлении систем ограничений ранга 1 (R1CS), времени работы алгоритмов zk-SNARK и размеров ключей доказательства. Система позволяет разработчикам схем zk-SNARK на этапе написания кода измерять различные параметры производительности и оптимизировать представления системы ограничений. Разработанная программная система может быть использована для замера эффективности произвольных схем zk-SNARK и определения их применимости для различных приложений.

Ключевые слова: *доказательство с нулевым разглашением, zk-SNARK, R1CS, ZoKrates, эффективность алгоритмов.*

[1]Работа выполнена при поддержке Математического центра в Академгородке, соглашение с Министерством науки и высшего образования Российской Федерации № 075-15-2022-282.

zk-SNARK (zero-knowledge Succinct Non-Interactive Argument of Knowledge) — это криптографический протокол неинтерактивного доказательства знания с нулевым разглашением . Преимущество zk-SNARK над другими протоколами доказательства с нулевым разглашением заключается в гарантиях эффективности: длина доказательства зависит только от параметра безопасности, а время проверки не зависит от размера схемы и секретного параметра (witness) [1].

zk-SNARK позволяет доказывать произвольные NP-утверждения. Для этого утверждение должно быть сформулировано как пример NP-полной задачи, например, как задача о выполнимости арифметической схемы.

Наиболее распространённым форматом внутреннего представления в реализациях zk-SNARK являются системы ограничений ранга 1 (Rank-1 Constraint Systems, R1CS). R1CS позволяют представить арифметическую схему в виде, удобном для дальнейшего эффективного доказательства выполнимости этой схемы с помощью zk-SNARK.

Сложность доказательства выполнения арифметической схемы с помощью zk-SNARK составляет $O(n \log n)$, где n — число операций умножения. Из этого следует, что эффективность напрямую определяется значением n [2].

В контексте реальных приложений zk-SNARK асимптотические результаты менее актуальны, и конкретная эффективность имеет решающее значение для обеспечения практической применимости. В связи с этим возникает проблема определения эффективности реализации различных алгоритмов для применения в схемах zk-SNARK.

Цель данной работы — создание универсального инструмента оценки эффективности внутреннего представления произвольных схем zk-SNARK. Для этого разработана программная система, которая позволяет оценивать различные параметры схем zk-SNARK, выраженных в виде кода на языке ZoKrates.

ZoKrates представляет собой набор программных инструментов для создания доказательств знания с нулевым разглашением, использующий zk-SNARK в качестве системы проверки. ZoKrates скрывает значительную сложность, присущую доказательствам с нулевым разглашением, и предоставляет разработчикам более высокоуровневые программные абстракции для реализации системы ограничений. Для этого он определяет предметно-ориентированный язык, который позволяет разработчикам задавать доказуемые вычисления без необходимости разбираться в низкоуровневых деталях реализации системы доказательств.

Компилятор ZoKrates транслирует код, написанный на этом языке, в доказуемые системы ограничений. Кроме того, ZoKrates позволяет выполнять реализованные программы, генерировать доказательства и выполнять проверку корректности доказательств [3].

Система предназначена для замера параметров схем доказательства с нулевым разглашением zk-SNARK — количества ограничений во внутреннем представлении систем ограничений ранга 1, времени работы алгоритмов zk-SNARK и размеров ключей доказательства.

Разработанная программная система состоит из следующих модулей:

— **Модуль взаимодействия с ZoKrates.** Осуществляет автоматизацию запуска команд компиляции кода схемы, генерации параметра безопасности, генерации и проверки доказательства, а также других команд, поддерживаемых ZoKrates. Модуль позволяет конфигурировать различные параметры работы со схемой, в нём реализована также обработка полученных результатов.
— **Модуль генерации кода.** Выполняет автоматическую генерацию кода схем на языке ZoKrates на основе шаблонов и передаваемых входных параметров. Это поз-

воляет переиспользовать код для одинаковых по логике работы схем, отличающихся только отдельными значениями.

— **Модуль организации экспериментов.** В данном модуле определён базовый класс для многократного выполнения экспериментов с замером параметров.
— **Модуль визуализации.** Осуществляет построение графиков зависимости измеряемых параметров от поданных на вход значений.
— **Интерфейс взаимодействия.** В программе реализован графический интерфейс, который позволяет пользователю писать код, выбирать параметры и запускать эксперименты. Кроме того, система предоставляет программный интерфейс и может подключаться в другие программы в виде библиотеки.

Система может использоваться для замера эффективности произвольных схем zk-SNARK, выраженных в виде кода на языке ZoKrates. С её помощью можно подобрать оптимальные параметры компиляции схемы.

Встроенный редактор кода позволяет разработчикам схем zk-SNARK на этапе написания кода измерять различные параметры производительности и оптимизировать представления системы ограничений.

Благодаря модулю проведения экспериментов и замера параметров, есть возможность выявлять ограничения и определять применимость схем zk-SNARK для различных приложений.

ЛИТЕРАТУРА

1. *Ben-Sasson E., Chiesa A., Genkin D., et al.* SNARKs for C: Verifying program executions succinctly and in zero knowledge // LNCS. 2013. V. 8043. P. 90–108.
2. *Eberhardt J.* Scalable and Privacy-preserving Off-chain Computations. Ph.D. Thesis. Technical University of Berlin, Faculty IV — Electrical Engineering and Computer Science, 2021. 284 p.
3. *Eberhardt J. and Tai S.* ZoKrates — scalable privacy-preserving off-chain computations // IEEE Intern. Conf. Blockchain. Halifax, Canada, 2018. P. 1084–1091.

УДК 004.056.5 DOI 10.17223/2226308X/17/33

ИСПОЛЬЗОВАНИЕ ПЕРЕМЕЩЕНИЙ ELF ДЛЯ ШИФРОВАНИЯ ИСПОЛНЯЕМЫХ ФАЙЛОВ

Р. К. Лебедев, В. Е. Ситнов

Рассмотрен новый подход к сокрытию кода исполняемых файлов ОС Linux при помощи таблицы перемещений, позволяющий создать криптор без встраивания в исполняемый файл кода расшифрования. Исследованы различные варианты практического применения данного подхода, реализованы соответствующие прототипы крипторов. Оценена опасность подхода для инструментов обратной разработки IDA, Ghidra, angr и антивирусного ПО.

Ключевые слова: *пакер, криптор, вредоносное программное обеспечение, таблица перемещений, ELF.*

С развитием киберпреступности было придумано множество способов сокрытия кода вредоносного программного обеспечения от исследования аналитиками и антивирусов. Среди них применение обфускаторов, генераторов полиморфного кода, а также пакеров и крипторов [1].

Пакеры и крипторы — во многом схожие инструменты для сжатия и шифрования исполняемого кода соответственно. Как правило, принцип их работы прост: ориги-

нальный исполняемый файл в результате обработки превращается в небольшой код распаковки с приложенными к нему данными, аналогично самораспаковывающимся архивам. Данные инструменты имеют законные применения, например экономия места на диске и защита проприетарных программ от взлома. Но часто они применяются и для сокрытия кода вредоносных программ, поскольку сжатие и шифрование данных позволяют нейтрализовать сигнатурный анализ, один из важнейших подходов, используемых антивирусами.

Антивирусы были частично адаптированы к данным угрозам, получив возможность распаковывать оригинальный исполняемый код для популярных инструментов сокрытия кода или хотя бы узнавать использованный инструмент по коду распаковки и, если он используется только киберпреступниками, блокировать угрозу без дальнейшего анализа [2].

В данной работе рассмотрен новый подход к сокрытию исполняемого кода, не требующий существования в исполняемом файле кода распаковки: более того, на момент начала загрузки упакованный таким способом файл не содержит ни байта исполняемого кода. Основой подхода является использование таблиц перемещений и их конкретной реализации в ОС Linux для процессорной архитектуры x86-64.

Таблица перемещений (relocation table) — информация, необходимая для загрузки кода и данных программы по актуальным адресам в виртуальной памяти, если они не соответствуют адресам, использованным в позиционно-зависимом коде программы в момент её сборки [3]. Данная информация обрабатывается самой операционной системой: ядром или её компонентами, такими, как динамический компоновщик, причём загруженный в память исполняемый файл становится готов к запуску по новому адресу только после полной её обработки.

Хотя обычно в результате обработки таблицы перемещений меняются только специально отведённые для этого данные, доступные для чтения и записи, механизм text relocations (признанный в части операционных систем небезопасным, но все же поддерживаемый в большинстве дистрибутивов Linux) позволяет менять таким образом и исполняемый код [4].

Перемещения в ОС Linux описываются следующими полями:

1) смещение — адрес, по которому требуется изменить данные;
2) тип — формула, по которой рассчитывается итоговое значение для записи в память;
3) символ — объект или функция, которые могут использоваться в качестве аргумента в формуле;
4) слагаемое — константа, имеющая размер машинного слова, которая также может использоваться в формуле, обычно складывается с результатом.

В табл. 1 представлены некоторые из типов перемещений Linux, используемые далее в данной работе [5].

Таблица 1

Типы перемещений Linux x86-64

Тип	Формула
`R_X86_64_64`	$\text{rebase}(S) + A$
`R_X86_64_SIZE64`	$\text{sizeof}(S) + A$
`R_X86_64_DTPOFF64`	$S + A$

Нетрудно видеть, что, зная значение одного символа S, через него можно выразить любое целевое значение при помощи формул перемещений, более того, на практике допустимо использовать нулевой символ с нулевыми адресом и размером. Для представления в таком виде всего исполняемого файла достаточно создать перемещения для всего диапазона адресов, занимаемого кодом и данными, в чём и заключается предложенный подход.

Рассмотрены следующие различные варианты сокрытия кода:

1) запись кода через перемещения вида `R_X86_64_64` с постоянными слагаемыми, наивный подход;
2) запись кода через перемещения вида `R_X86_64_SIZE64` с постоянными слагаемыми. Отличие от первого подхода состоит в допустимости использования данного перемещения в разделяемых библиотеках;
3) запись кода через перемещения вида `R_X86_64_DTPOFF64` с постоянными слагаемыми. Данное перемещение нетипично для исполняемых файлов и специфично для работы с локальной памятью потока (TLS), хотя в формуле она и не упомянута [6]. Отличие от предыдущих подходов в отсутствии поддержки перемещения со стороны декомпилятора Ghidra;
4) запись кода через перемещения вида `R_X86_64_64` с переменными слагаемыми. В качестве базового символа вместо нулевого выбран символ, использующий расширение `GNU_IFUNC` [7]. Данное расширение позволяет исполнить произвольный программный код в процессе подсчёта адреса символа. Отличие в возможности не просто перемешать данные, но и зашифровать их, а также потенциальной сложности обработки в рамках статического анализа.

Для проверки эффективности против антивирусов были выбраны эксплойты повышения привилегий уязвимостей CVE-2016-5195 и CVE-2022-0847 [8, 9]. Данные уязвимости широко использовались злоумышленниками и достаточно стары, чтобы содержаться во всех возможных сигнатурных базах. К эксплойтам были последовательно применены упомянутые выше преобразования, после чего полученные исполняемые файлы были проверены при помощи сайта VirusTotal [10]. Чтобы исключить попытки антивирусов распознать вирусы без анализа их кода (по иным, косвенным признакам), проводилось дополнительное тестирование с файлом, из которого удалены все секции с кодом и данными.

Для проверки декомпиляторов IDA [11], Ghidra [12] и инструмента символьного исполнения angr [13] была выбрана простая программа, код которой доступен в листинге 1. От инструмента символьного исполнения angr требовалось достижение обоих путей в программе, а от декомпиляторов — возможность загрузить код и декомпилировать функцию main.

```
1 #include <stdio.h>
2 int main() {
3     int k;
4     printf("Please enter secret key: ");
5     scanf("%d", &k);
6     if (k == 1337)
7         printf("Correct license key\n");
8     else  printf("Wrong license key\n");
9 }
```

Листинг 1. Тестовая программа

Объединённые результаты экспериментов представлены в табл. 2.

Таблица 2

Результаты экспериментов

Тест	VirusTotal	IDA	Ghidra	angr
`R_X86_64_64`	1 + 1	Успех	Успех	Ошибка
`R_X86_64_SIZE64`	1 + 1	Ошибка	Успех	Ошибка
`R_X86_64_DTPOFF64`	1 + 1	Ошибка	Ошибка	Ошибка
`R_X86_64_64` с `GNU_IFUNC`	1 + 1	Ошибка	Ошибка	Ошибка
Файлы без кода	1 + 1	—	—	—
Оригинальные файлы	20 + 19	—	—	—

Единственный антивирус, который мог определить эксплойты повышения привилегий после применения любого из преобразований, каким-то образом (предположительно, по списку используемых функций из библиотеки языка Си) обнаруживал их даже после полного удаления кода и данных. Дизассемблеры имели больший успех при обработке более простых преобразований, но не третьего и четвертого варианта.

Таким образом, предложенный метод оказался эффективен и против антивирусов, и против инструментов обратной разработки и потенциально является новым вектором атаки на информационные системы. Полученные результаты могут быть использованы для совершенствования антивирусов и инструментов обратной разработки, а также подчеркивают важность следования лучшим практикам информационной безопасности, например запрету механизма text relocations.

ЛИТЕРАТУРА

1. *Chakkaravarthy S. S., Sangeetha D., and Vaidehi V.* A survey on malware analysis and mitigation techniques // Comput. Sci. Rev. 2019. No. 32. P. 1–23.
2. *Ugarte-Pedrero X., Balzarotti D., Santos I., and Bringas P. G.* SoK: Deep packer inspection: A longitudinal study of the complexity of run-time packers // IEEE Symp. Security and Privacy. San Jose, CA, USA, 2015. P. 659–673,
3. `https://man7.org/linux/man-pages/man5/elf.5.html` — elf(5) — Linux manual page. 2024.
4. `https://flameeyes.blog/2016/01/16/textrels-text-relocations-and-their-impact-on-hardening-techniques/` — TEXTRELs (Text Relocations) and their impact on hardening techniques. 2016.
5. `https://intezer.com/blog/malware-analysis/executable-and-linkable-format-101-part-3-relocations/` — Executable and Linkable Format 101. Part 3: Relocations. 2018.
6. `http://people.redhat.com/drepper/tls.pdf` — ELF handling for thread-local storage. 2013.
7. `https://sourceware.org/glibc/wiki/GNU_IFUNC` — GNU_IFUNC. 2024.
8. `https://dirtycow.ninja/` — Dirty COW (CVE-2016-5195). 2016.
9. `https://dirtypipe.cm4all.com/` — The Dirty Pipe Vulnerability. 2022.
10. `https://www.virustotal.com/` — VirusTotal. 2024.
11. `https://www.hex-rays.com/ida-pro/` — IDA Pro. 2024.
12. `https://github.com/NationalSecurityAgency/ghidra` — Ghidra Software Reverse Engineering Framework. 2024.
13. *Shoshitaishvili Y., Wang R., Salls C., et al.* SOK: (State of) The art of war: Offensive techniques in binary analysis // IEEE Symp. Security and Privacy. San Jose, CA, USA, 2016. P. 138–157.

Секция 5

ПРИКЛАДНАЯ ТЕОРИЯ КОДИРОВАНИЯ, АВТОМАТОВ И ГРАФОВ

УДК 519.17 DOI 10.17223/2226308X/17/34

КЛАССИФИКАЦИЯ ДЕРЕВЬЕВ, ВСЕ МАКСИМАЛЬНЫЕ ПОДДЕРЕВЬЯ КОТОРЫХ ИЗОМОРФНЫ

М. Б. Абросимов, Д. А. Томилов

Рассматривается задача описания деревьев, все максимальные поддеревья которых изоморфны. Приводится характеристическая теорема для таких деревьев: все максимальные поддеревья дерева изоморфны тогда и только тогда, когда все его листья подобны. Вводится класс многоуровневых звёзд. Доказывается, что этот класс совпадает с классом деревьев, все максимальные поддеревья которых изоморфны.

Ключевые слова: *граф, дерево, реконструируемость.*

Введение

Графы являются интересными математическими объектами, которые находят применения в различных областях, в том числе и в криптографии. В теории графов большое количество NP-полных проблем, которые могут быть использованы для построения доказательств с нулевым разглашением (такие схемы есть для задачи о гамильтоновом графе, хроматическом числе, вершинном расширении). Из более свежих результатов отметим использование графов Пэли [1] и Турана [2] для построения криптосистем. В данной работе рассматриваются деревья особого вида. Основные определения по теории графов используются согласно [3, 4].

Напомним, что *неориентированным графом* (далее — просто графом) называется пара $G = (V, \alpha)$, где α — симметричное и антирефлексивное отношение на множестве вершин V, называемое отношением смежности. Степень вершины — количество рёбер графа, инцидентных этой вершине. Висячая вершина (лист) — вершина степени 1.

Дерево — связный граф, в котором нет циклов. Дерево с одной вершиной называется *тривиальным*. Будем рассматривать деревья с числом вершин больше 1. Деревья являются важным классом графов. Многие задачи, весьма сложные в общем случае, эффективно решаются для деревьев. Одной из таких задач является реконструкция графов по их частям.

Дадим необходимые определения.

Определение 1. *Подграф* — граф, получающийся удалением произвольного количества вершин и всех инцидентных им рёбер из исходного графа.

Определение 2. *Максимальный подграф* — подграф, получающийся удалением одной произвольной вершины.

Поддерево — дерево, получающееся удалением произвольного количества висячих вершин и всех смежных с ними рёбер из исходного дерева. *Максимальное поддерево* дерева — поддерево, получающееся удалением одной произвольной висячей вершины.

Напомним, что два графа $G_1 = (V_1, \alpha_1)$ и $G_2 = (V_2, \alpha_2)$ называются *изоморфными*, если можно установить взаимно однозначное соответствие $f : V_1 \to V_2$, сохраняющее отношение смежности:

$$\forall u, v \in V_1 \ \big((u, v) \in \alpha_1 \Leftrightarrow (f(u), f(v)) \in \alpha_2\big).$$

Гипотеза вершинной реконструируемости Келли — Улама говорит, что каждый граф с числом вершин $n > 2$ однозначно с точностью до изоморфизма определяется по списку своих максимальных подграфов. В [5] доказано, что деревья с числом вершин $n \geqslant 3$ могут быть с точностью до изоморфизма реконструированы по списку своих максимальных подграфов. Более того, деревья однозначно с точностью до изоморфизма определяются списком своих максимальных поддеревьев [6]. В [7] доказано, что каждое дерево с числом вершин $n > 6$ однозначно с точностью до изоморфизма определяется своими неизоморфными поддеревьями.

Основные результаты

В данной работе рассматриваются деревья, все максимальные поддеревья которых изоморфны. К таким деревьям относятся, например, цепи или звёзды.

В работе [8] анонсирован следующий результат:

Теорема 1. Все максимальные поддеревья дерева попарно изоморфны тогда и только тогда, когда все листья этого дерева подобны.

В теореме доказывается, что если удалить все листья исходного дерева, то снова получим дерево, все максимальные поддеревья которого изоморфны. Это означает, что и все ветви, выходящие из центра, подобны (для бицентральных деревьев, конечно, имеются в виду ветви, которые содержат только одну центральную вершину либо наоборот обе центральные вершины).

Пусть T — дерево, все максимальные поддеревья которого изоморфны. Исследуем случай, когда T является бицентральным деревом. Рассмотрим две ветви, которые выходят из центральных вершин и содержат обе центральные вершины. Так как соответствующие деревья изоморфны и содержат одинаковое количество вершин, то в дереве T должно быть чётное количество вершин. Таким образом, среди рассматриваемых деревьев все бицентральные имеют только чётное количество вершин; все деревья с нечётным количеством вершин являются центральными, а среди деревьев с чётным количеством вершин могут быть как центральные, так и бицентральные.

Введём обозначение SC для центральных деревьев рассматриваемого вида. Бицентральные деревья обозначим SB. В силу того, что ветви, выходящие из центральных вершин, изоморфны, будем называть такие деревья *многоуровневыми звездами*. Каждый уровень кодируется двумя параметрами — числом разветвлений и длиной ствола, при этом число разветвлений должно быть больше 1, а ствол считается от ближайшей центральной вершины.

Звёзды первого уровня кодируются двумя параметрами и обозначаются SC_{n_1,n_2} или SB_{n_1,n_2}. Число вершин n можно вычислить по следующей формуле:

$$n = \begin{cases} 1 + n_1 n_2, \text{ если дерево центральное,} \\ 2 + n_1 n_2, \text{ если дерево бицентральное.} \end{cases}$$

Звёзды второго уровня кодируются четырьмя параметрами и обозначаются SC_{n_1,n_2,n_3,n_4} или SB_{n_1,n_2,n_3,n_4}. Число вершин находится по формуле

$$n = \begin{cases} 1 + n_1(n_2 + n_3 n_4), \text{ если дерево центральное,} \\ 2 + n_1(n_2 + n_3 n_4), \text{ если дерево бицентральное.} \end{cases}$$

Звёзды последующих уровней задаются аналогичным образом. Звезды уровня k задаются $2k$ параметрами: $SC_{n_1,n_2,\ldots,n_{2k-1},n_{2k}}$ или $SB_{n_1,n_2,\ldots,n_{2k-1},n_{2k}}$. Число вершин вычисляется по формуле

$$n = \begin{cases} 1 + n_1(n_2 + n_3(n_4 + \ldots + n_{2k-1}n_{2k}), \text{ если дерево центральное,} \\ 2 + n_1(n_2 + n_3(n_4 + \ldots + n_{2k-1}n_{2k}), \text{ если дерево бицентральное.} \end{cases}$$

Основной результат работы представлен следующей теоремой.

Теорема 2. Каждая центральная SC или бицентральная звезда SB является деревом, все максимальные поддеревья которого изоморфны. Каждое n-вершинное дерево, все максимальные поддеревья которого изоморфны, является либо центральной звездой $SC_{n_1,n_2,\ldots,n_{2k-1},n_{2k}}$, такой, что

$$n = 1 + n_1(n_2 + n_3(n_4 + \ldots + n_{2k-1}n_{2k}),$$

либо бицентральной звездой $SB_{n_1,n_2,\ldots,n_{2k-1},n_{2k}}$, такой, что

$$n = 2 + n_1(n_2 + n_3(n_4 + \ldots + n_{2k-1}n_{2k}).$$

ЛИТЕРАТУРА

1. *Oumazouz Z. and Karim D.* A new symmetric key cryptographic algorithm using Paley graphs and ASCII values // E3S Web Conf. 2021. V. 297. Article 01046. 5 p.
2. *Beaula C., Venugopal P., Praba B., and Karthik B.* Block encryption and decryption of a sentence using decomposition of the Turan graph // J. Math. 2023. P. 1–8.
3. *Харари Ф.* Теория графов. М.: Мир, 1973.
4. *Богомолов А. М., Салий В. Н.* Алгебраические основы теории дискретных систем. М.: Наука, 1997.
5. *Kelly P. J.* A congruence theorem for trees // Pacific J. Math. 1957. V. 7. P. 961–968.
6. *Harary F. and Palmer E.* The reconstruction of a tree from its maximal subtrees // Canadian J. Math. 1966. V. 18. P. 803–810.
7. *Manvel B.* Reconstruction of trees // Canadian J. Math. 1970. V. 22. P. 55–60.
8. *Абросимов М. Б., Володина П. А.* О некоторых свойствах деревьев с размером приведенной колоды 1 // XIV Междунар. науч. семинар «Дискретная математика и ее приложения» имени академика О. Б. Лупанова (20–25 июня 2022 г., Москва). Т. 14. М.: ИПМ им. Келдыша, 2022. С. 172–174.

УДК 519.7 DOI 10.17223/2226308X/17/35

О КОДАХ С ОДНОЗНАЧНЫМ ДЕКОДИРОВАНИЕМ К БЛИЖАЙШЕМУ

Д. С. Ананичев, К. Л. Геут, С. С. Титов

Работа посвящена задаче № 7 Олимпиады NSUCRYPTO 2023 г. об описании интересного класса кодов C — с однозначным декодированием к ближайшему кодовому слову в метрике Хэмминга. Доказана возможность представления кода C как матроида и приведено промежуточное решение в случае, когда множество B битов, таких, что существует двухбитовое слово, его содержащее, декодирующееся не в $z = 0$, совпадает со всеми позициями битов кода C.

Ключевые слова: *NSUCRYPTO, вес Хэмминга, код, матроид.*

Одна из задач второго раунда Международной олимпиады по криптографии NSUCRYPTO'2023 [1] была посвящена классу кодов C длиной n как подмножества $\mathbb{F}_2^n$ с однозначным декодированием к ближайшему по метрике Хэмминга кодовому слову. В задаче было два вопроса:

1) какие коды C могут обеспечить наличие такого свойства и
2) какие коды C, являющиеся линейными подпространствами $\mathbb{F}_2^n$, могут обеспечить такое свойство?

В процессе решения задачи нашей командой была высказана гипотеза, что эти коды сводятся к тензорному произведению совершенных кодов. Работа посвящена проблеме 2 — о линейных кодах с таким свойством.

Поскольку вес Хэмминга конкатенации слов равен сумме весов конкатенируемых слов, тензорное произведение совершенных кодов обладает таким свойством.

Коды с минимальным расстоянием $D_{\min} = 1$ характеризуются наличием безошибочных битов, где $D_{\min}$ — это кодовое расстояние, то есть минимум расстояния Хэмминга между различными кодовыми словами. Этот случай надо признать экстремальным и рассматривать отдельно.

Пусть z и x — два кодовых слова на расстоянии 2. Тогда существуют ровно два слова веса 1, находящиеся на расстоянии 1 и от z, и от x. Следовательно, они не могут однозначно декодироваться к ближайшему и поэтому являются кодовыми. Примем в дальнейшем предположение $D_{\min} > 2$, так что в коде отсутствуют слова на единичном расстоянии и на расстоянии 2.

Всюду далее мы полагаем, что код C обладает свойством однозначности декодирования.

Лемма 1 (о нечётности). Пусть наименьшее в коде C расстояние от кодового слова z до других кодовых слов равно d. Тогда d нечётно.

Рассмотрим множество B битов, таких, что существует двухбитовое слово, его содержащее, декодирующееся не в $z = 0$. Тогда код C распадается в тензорное произведение кода на B и на его дополнение B', причём для последнего $D_{\min} > 3$.

Лемма 2 (о совершенности при $D_{\min} = 3$). Линейный код C, определённый на битах B, при $D_{\min} = 3$ является совершенным.

Определим на B следующее бинарное отношение $\sim$: $b_1 \sim b_2$, если и только если существует трёхбитовое кодовое слово, содержащее b_1 и b_2. Таким образом, $b_1 + b_2$ декодируется не в нуль, если эти биты различны. Это отношение является отношением эквивалентности.

Рассмотрим разложение кода C на B в тензорное произведение подкодов на классах эквивалентности по отношению $\sim$. Ясно, что каждый такой подкод порождается системой троек Штейнера и поэтому представляет собой совершенный код — обобщённый код Хэмминга с $D_{\min} = 3$ [2, 3].

Рассмотрим код на битах из B'. Для него $5 \leqslant D_{\min}$ по лемме о нечётности. Будем использовать обозначение $x \to y$, если битовая строка x декодируется в кодовое слово y.

Поскольку всё множество битовых строк разбивается на одинаковые по мощности окрестности кодовых слов, достаточно изучить такую окрестность для нулевого элемента $z = 0$. Можем отождествлять битовую строку с множеством позиций её единичных битов. Тогда, например, строка из одних нулей $z = 0$ отождествится с пустым множеством. Изучим окрестность нуля $z = 0$, т. е. множество тех x, что $x \to 0$, и дополнение этого множества, т. е. множество тех v, что $v \to w \neq 0$. Если $Y \to 0$ и $X \subseteq Y$, то $X \to 0$. Для любого множества A битовых позиций обозначим через $|A|$ его мощность.

Рассмотрим в семействе множеств, декодирующихся не в нуль, подсемейство минимальных по включению, а именно: назовём процикломмножество M битовых позиций, обладающее свойством: M декодируется не в нуль, а любое собственное подмножество множества M декодируется в нуль.

Лемма 3. Пусть M — процикл. Тогда $M \to M'$, где $|M'| = 1 + 2|M|$, причём M — подмножество в M'.

Лемма 4. Пусть множество P декодируется не в нуль. Тогда в P имеется подмножество, являющееся процикломм.

Лемма 5. Если M, N — различные процикломы с общим элементом e, то в множестве $E = (M \cup N) \setminus \{e\}$ имеется подмножество, являющееся процикломм.

В данной работе предлагается использовать теорию матроидов для исследования проблемы. Напомним [4], что матроиды были введены в [5] с целью аксиоматизации линейной зависимости векторов. Однако это понятие оказалось более общим, и его мощь проявилась, в том числе, в теореме Радо — Эдмондса [6, 7] об оптимизации посредством жадного алгоритма. В криптографии матроиды оказались связанными с идеальными совершенными схемами разделения секрета [8]. Матроид определяется как пара: некоторое множество M (носитель матроида) и некоторое семейство его подмножеств, которые объявляются независимыми множествами; остальные подмножества считаются зависимыми. Максимальные по включению независимые множества называются базами матроида, минимальные по включению зависимые множества — циклами (что особенно наглядно в теории графов). Переходы от аксиом для независимых множеств к другим системам аксиом (для баз, циклов и т. д.) названы в [9] криптоморфизмами.

В нашем случае удобно использовать систему аксиом для семейства циклов. Пара (M, C) задаёт структуру матроида на множестве M с семейством циклов C, если выполняются всего две аксиомы:

1) если C и D — циклы, причём $C \supset D$, то $C = D$;
2) если C и D — различные циклы, содержащие общий элемент e, то в множестве $C \cup D \setminus \{e\}$ содержится цикл.

Поскольку декодирование к ближайшему можно рассматривать как задачу комбинаторной оптимизации, представляется естественным обнаружить здесь структуру

матроида, что и является основным результатом данной работы. Такой подход позволяет использовать теорию матроидов для решения исходной задачи.

Утверждение 1. Семейство проциклов является семейством циклов некоторого матроида.

Действительно, оно удовлетворяет обеим аксиомам циклов и поэтому определяет матроид [10]. Из этого следует, что код на битах из B' можно представить как конкатенацию кодов, соответствующих разбиению этого матроида на связные компоненты.

Таким образом, в работе приведено промежуточное решение в случае, когда множество B совпадает со всеми позициями битов кода. Для решения проблемы осталось доказать, что связный матроид такого кода — пороговый, все циклы которого имеют одинаковую мощность, или целенаправленно строить несовершенные коды со связным матроидом, определённым такими циклами.

ЛИТЕРАТУРА

1. nsucrypto.nsu.ru.
2. *Ковалевская Д. И.* О вложимости систем Штейнера в совершенные коды: автореф. дис. ... канд. физ.-мат. наук. Новосибирск, 2013.
3. *Геут К. Л., Титов С. С.* Ортоморфизмы линейных троек Штейнера // Математическое моделирование и информационные технологии при решении прикладных задач в транспортном вузе. 2021. Вып. 1(241). С. 131–137.
4. *Wilson R. J.* An introduction to matroid theory // Amer. Math. Monthly. 1973. V. 80. No. 5. P. 500–525.
5. *Whitney H.* On the abstract properties of linear dependence // Amer. J. Math. 1935. V. 57. P. 509–533.
6. Rado R. A. A theorem on independence relations // Quart. J. Math. Oxford. 1942. No. 13. P. 3–89.
7. *Edmonds J.* Matroids and the greedy algorithms // Math. Programming. 1971. V. 1. P. 127–136.
8. *Ященко В. В.* Введение в криптографию // М.: МЦНМО, 2012.
9. *White N.* Theory of Matroids. Cambridge: Cambridge University Press, 1986. 316 p.
10. *Асанов М. О., Баранский В. А., Расин В. В.* Дискретная математика: графы, матроиды, алгоритмы. Ижевск: НИЦ «РХД», 2001.

УДК 003.26 DOI 10.17223/2226308X/17/36

ОБОБЩЁННЫЕ (L, G)-КОДЫ ВО ВЗВЕШЕННОЙ МЕТРИКЕ ХЭММИНГА ДЛЯ ЗАЩИТЫ ИНФОРМАЦИИ

С. В. Беззатеев

Рассматриваются возможности использования обобщённых (L, G) кодов для решения различных задач защиты информации, в частности использование таких кодов для синдромного встраивания информации, кодового сжатия, взвешенных пороговых схем распределения ключей.

Ключевые слова: *метрика взвешенного расстояния Хэмминга, обобщённые (L, G)-коды, защита информации.*

Определим двоичные обобщённые (L,G)-коды в соответствии с [1], нумераторами позиций для которых являются дроби вида $\dfrac{u_i'(x)}{u_i(x)}$, $\deg u_i(x) \leqslant l$, где $u_i(x)$ — неприводимые многочлены степени r_i с коэффициентами из $\mathrm{GF}(2^m)$.

Определение 1 [1]. Двоичный обобщённый (L,G)-код состоит из всех векторов $\mathbf{a} = (a_1 a_2 \dots a_n)$, удовлетворяющих соотношению

$$\sum_{i=1}^{n} a_i \frac{u_i'(x)}{u_i(x)} \equiv 0 \pmod{G(x)},$$

где $\deg u_i(x) = r_i \leqslant \deg G(x)$; многочлен $u_i'(x)$ — формальная производная $u_i(x)$ и $(u_i(x), G(x)) = 1$ для всех $i = 1, \dots, n$.

Очевидно, что такой неприводимый двоичный обобщённый $L,G)$-код исправляет любые ошибки, суммарный вес которых не превышает $\deg G(x)$. Это позволяет говорить о (L,G)-коде во взвешенной метрике Хэмминга.

Определение 2 [2]. Метрика взвешенного рассстояния Хэмминга $d_{\mathrm{wH}}(\mathbf{a},\mathbf{b})$ между векторами $\mathbf{a} = (a_1 a_2 \dots a_n)$ и $\mathbf{b} = (b_1 b_2 \dots b_n)$ определяется следующим образом:

$$d_{\mathrm{wH}}(\mathbf{a},\mathbf{b}) = \sum_{i=1}^{n} w_i \cdot d(a_i, b_i),$$

где $d(a_i,b_i) = 1$, если $a_i \neq b_i$, и $d(a_i,b_i) = 0$, если $a_i = b_i$.

Таким образом, взвешенное расстояние Хэмминга можно определить как

$$d_{\mathrm{wH}}(\mathbf{a},\mathbf{b}) = \sum_{\substack{i=1,\\ a_i \neq b_i}}^{n} w_i,$$

где $w_i > 0$ и называется весом позиции i. При выборе в качестве нумераторов позиций обобщённого (L,G)-кода всех неприводимых мноогочленов степени r_i получим код, лежащий на границе Хэмминга в метрике взвешенного расстояния.

Теорема 1 [3]. Двоичные обобщённые (L,G)-коды, задаваемые неприводимым многочленом $G(x)$ степени τ с коэффициентами из $\mathrm{GF}(2^m)$ и множеством нумераторов позиций

$$L = \left\{ \frac{u_i^{'(j)}(x)}{u_i^{(j)}(x)} : i = 1, \dots, n_j,\ j = 1, \dots, \tau \right\},$$

где $u_i^{(j)}(x)$ — неприводимый многочлен степени j с коэффициентами из $\mathrm{GF}(2^m)$ и $G(x) \neq u_i^{(\tau)}(x)$ при всех i, лежат на границе Хэмминга, то есть являются совершенными кодами в метрике взвешенного расстояния Хэмминга; и верно равенство

$$2^k W_\tau^n = 2^n,$$

где $n = \sum\limits_{j=1}^{\tau} n_j$ — длина кода; k — размерность кода; W_τ^n — число векторов в шаре радиуса τ в метрике взвешенного расстояния Хэмминга.

Общее число ошибок, исправляемых таким кодом, определяется неравенством $\sum\limits_{j=1}^{\tau} \tau_i r_i \leqslant \tau$, где τ_i — число возможных ошибок в i-м блоке длины n_i.

Используя предложенные обобщённые (L, G)-коды, можно модифицировать оптимальный алгоритм F5 синдромного LSB-встраивания, построив на его основе аналогичный оптимальный алгоритм WF5 [4], учитывающий значимость искажаемых бит исходного контейнера. При формировании рабочей области исходного контейнера в классических алгоритмах синдромного встраивания исходное изображение (контейнер) разделяется на две зоны: значимую и незначимую. Внесение каких-либо искажений в значимую зону не допускается, в то время как в незначимой зоне разрешены любые искажения. То есть в классическом алгоритме F5 на кодах Хэмминга и его многочисленных модификациях на других классах кодов в незначимую зону разрешено вносить любое число искажений, ограниченное лишь корректирующей способностью используемого помехоустойчивого кода. Можно сказать, что вносимые искажения в таких алгоритмах равномерно распределены между элементами незначимой зоны. Однако в изображении можно выделить несколько зон, значимость которых существенно различается. При этом для более значимых элементов допускается меньшее число искажений, чем для менее значимых; элементам различных зон можно назначить разные веса w_j, определяющие их значимость.

Таким образом, если представить разрешённую для искажения зону исходного контейнера как множество элементов, разбитое на m зон с различной значимостью (весами w_j, $j = 1, \ldots, m$), то можно рассматривать на этом множестве взвешенную метрику Хэмминга. Такой подход позволяет согласовать метод встраивания со взвешенной моделью контейнера. Кроме того, для такой взвешенной структуры удобно ввести штрафную функцию [5], учитывающую влияние искажений, вносимых в разных зонах контейнера, на их заметность в изображении, полученном после встраивания информации.

Штрафная функция добавляет штраф за появление искажений в зависимости от веса зоны, где искажение вносится. Чем больше вес зоны, тем больше вес вносимого искажения. Таким образом, штрафная функция имеет следующий вид:

$$F = \max_{\sum\limits_{i=1}^{m} t_i w_i \leqslant \tau} \sum_{j=1}^{m} t_j \nu_j,$$

где t_j — число искажений, внесенных в j-й зоне; ν_j — штраф за единицу искажения в j-й зоне.

В качестве примера рассмотрим случай использования совершенного во взвешенной метрике Хэмминга (L, G)-кода с $n = 35$, $n_1 = 8$, $r_1 = 1$, $n_2 = 27$, $r_2 = 2$ и $\deg G(x) = r_2 = 2$. Для такого кода можно считать $w_1 = 1$, $w_2 = 2$, и общий размер первой зоны определяется величиной ℓn_1, а второй зоны — ℓn_2 , где ℓ — некоторое целое. Общий размер зоны, где разрешены искажения, составит $\ell(n_1 + n_2)$. Общая длина встраиваемого сообщения при этом равна 6ℓ бит.

Кроме того, использование такого класса совершенных кодов позволяет существенно повысить эффективность кодового сжатия изображений [5], так как взвешенная структура обобщённого (L, G)-кода даёт возможность учесть неравнозначность элементов исходного файла изображения. Дополнительное введение функции штрафа [5] позволяет априори оценить качество используемой схемы и соответственно выбрать необходимые параметры используемого (L, G)-кода, то есть подобрать нумераторы позиций $u_i(x)$ и многочлен Гоппы $G(x)$ соответствующих степеней.

Используя модификацию алгоритма Мак-Элиса для расширенных (L, G)-кодов [6] и учитывая различный вес (степень многочлена $u_i(x)$) позиций кодового слова, легко

построить взвешенную пороговую схему разделения секрета [7], в которой количество голосов у пользователя системы определяется весом позиции вектора ошибки. То есть для восстановления секрета необходимо собрать значения некоторого вектора ошибки $\mathbf{e} = (e_1 e_2 \dots e_n)$, суммарный вес позиций (сумма степеней нумераторов позиций) которых не меньше заданного порога.

Действительно, предположим в качестве простейшего примера, что в схеме Мак-Элиса вместо классического двоичного кода Гоппы используется некоторый двоичный обобщённый (L, G)-код длины n во взвешенной метрике Хэмминга, степень неприводимого многочлена Гоппы $G(x)$ для которого равна t, а в множестве нумераторов позиций L используются неприводимые многочлены степеней 1 и 2. В качестве вектора ошибки будем использовать двоичный вектор e длины n с единицами на позициях различного веса (занумерованных многочленами степени 1 и 2) и с взвешенным весом Хэмминга $d_{\mathrm{wH}}(e) = t + \delta$. Тогда для успешного исправления такого вектора ошибки необходимо «удалить» из e единицы на позициях, общий вес которых не меньше δ. Очевидно, что это может быть сделано либо с помощью набора из δ единиц на позициях, занумерованных многочленами первой степени (если такие имеются в векторе e), либо с помощью набора из $\delta/2$ единиц на позициях, занумерованных многочленами второй степени (если такие имеются в векторе e), либо набора из некоторой комбинации ℓ единиц на позициях, занумерованных многочленами первой степени, и m единиц на позициях, занумерованных многочленами второй степени, так, что $\ell + 2m \geqslant \delta$. Таким образом, можно считать, что пользователь, знающий значение вектора e на позиции, занумерованной многочленом второй степени, имеет два голоса, в то время как пользователь, знающий значение вектора e на позиции, занумерованной многочленом первой степени, имеет всего один голос.

ЛИТЕРАТУРА

1. *Bezzateev S. and Shekhunova N.* One generalization of Goppa codes // Des. Codes Cryptogr. 2013. V. 66. No. 1–3. P. 391–399.
2. *Деза Е. И., Деза М. М.* Энциклопедический словарь расстояний. М.: Наука, 2008.
3. *Bezzateev S. and Shekhunova N.* Class of generalized Goppa codes perfect in weighted Hamming metric // Proc. ISIT-97. Ulm, Germany, 1997. P. 299.
4. *Bezzateev S., Voloshina N., and Zhidanov K.* Steganographic method on weighted container // Proc. XIII Int. Symp. Problems of Redundancy in Information and Control Systems. Saint-Petersburg, Russia, 2012. P. 10–12.
5. *Bezzateev S. and Voloshina N.* Image encryption in code based compression algorithms based on multilevel image structure model // 9th Intern. Congress ICUMT, Munich, Germany, 2017. P. 85–90.
6. *Bezzateev S. and Noskov I.* Using generalized (L, G)-codes for implementation the classic McEliece cryptosystem // 15th Intern. Congress ICUMT, Ghent, Belgium, 2023. P. 231–234.
7. *Massey J. L.* Some applications of coding theory in cryptography // P. G. Farrell (ed.) Codes and Cyphers: Cryptography and Coding IV. Essex, England: Formara Ltd., 1995. P. 33–47.

УДК 621.391:519.725 DOI 10.17223/2226308X/17/37

СВОЙСТВА ПОЛЯРИЗАЦИОННОЙ МАТРИЦЫ ПОЛЯРНОГО КОДА И ВЫЧИСЛЕНИЕ ПАРАМЕТРОВ БХАТТАЧАРЬИ[1]

А. Д. Болотникова, С. Г. Колесников, В. М. Леонтьев, А. И. Семенов

Работа является продолжением исследований по поиску точных формул для вычисления параметров Бхаттачарьи $Z\left(W_N^{(i)}\right)$ координатных каналов $W_N^{(i)}$ полярного кода в случае, когда канал передачи является двоичным симметричным и без памяти, требующих полиномиального числа операций. Для этого необходимо уметь строить такие базисы подпространств Z_{i-1}, порождённых первыми $i-1$ строками поляризационной матрицы G_N полярного кода длины N, и подпространств U_{i+1}, порождённых последними $N-i$ строками матрицы G_N, что вес Хемминга является аддитивной функцией на векторах базиса (или близкой к ней). Эти задачи решаются для двух последовательностей $i=2^m+1$ и $i=2^m-1$, а также при $i \geqslant N/2$. Как следствие, мы находим короткие и полиномиальные формулы для $Z\left(W_N^{(2^m+1)}\right)$ и $Z\left(W_N^{(2^m-1)}\right)$, а также полиномиально-экспоненциальные для $Z\left(W_N^{(i)}\right)$ при $i \geqslant N/2$. В заключении приводится список формул для вычисления всех параметров Бхаттачарьи кода длины 32.

Ключевые слова: *полярный код, поляризационная матрица, параметр Бхаттачарьи.*

Введение

Обозначим через W двоичный симметричный канал без памяти с вероятностью ошибки, равной p. В [1] (там же можно найти ссылки на литературу по полярным кодам и обзор известных результатов) показано, что для параметра Бхаттачарьи координатного канала $W_N^{(i)}$ полярного кода длины $N=2^n$ имеет место формула

$$Z\left(W_N^{(i)}\right) = \\ =2\sum_y \sqrt{\left[\sum_u p^{\mathrm{w}(yG_N \oplus uG_n)}(1-p)^{N-\mathrm{w}(yG_N\oplus uG_n)}\right]\left[\sum_{u'} p^{\mathrm{w}(yG_N\oplus u'G_n)}(1-p)^{N-\mathrm{w}(yG_N\oplus u'G_n)}\right]}, \quad (1)$$

где $\mathrm{w}(z)$ — вес Хэмминга вектора z (сумма координат z); суммирование во внешней сумме ведётся по $(0,1)$-векторам вида $(y_1,\ldots,y_{i-1},0,\ldots,0)$; суммирование в суммах под корнем ведётся по $(0,1)$-векторам вида $(0,\ldots,0,u_{i+1},\ldots,u_N)$ и $(0,\ldots,0,1,u'_{i+1},\ldots,u'_N)$ соответственно. Вид векторов y,u,u' и вид показателей степеней в формуле (1) показывают, что суммирования на самом деле ведутся по подпространствам Z_{i-1} и U_{i+1}, порождённым соответственно первыми $i-1$ и последними $N-i$ строками поляризационной матрицы G_N полярного кода. Очевидно, что если в этих подпространствах можно выбрать такой базис $e_1,\ldots,e_s$, что любые ненулевые координаты любых двух базисных векторов не стоят на одинаковых позициях, то

$$\mathrm{w}(\lambda_1 e_1 \oplus \ldots \oplus \lambda_s e_s) = \lambda_1 \mathrm{w}(e_1) + \ldots + \lambda_s \mathrm{w}(e_s), \quad \lambda_1,\ldots\lambda_s \in \mathbb{Z}_2.$$

Таким образом, для получения эффективных формул вычисления параметров Бхаттачарьи необходимо решить задачу описания подпространств, которые порождают стро-

[1]Работа поддержана Красноярским математическим центром, финансируемым Минобрнауки РФ (соглашение № 075-02-2024-1429).

ки поляризационной матрицы, и задачу выбора оптимальных базисов этих подпространств.

1. Свойства поляризационной матрицы

В [1] показано, что матрица G_N удовлетворяет простым рекуррентным соотношениям, а именно: её $(2i)$-я строка является повторённой два раза i-й строкой матрицы $G_{N/2}$, а её $(2i-1)$-я строка есть i-я строка матрицы $G_{N/2}$, дополненная нулями. Этот факт позволяет доказать следующие две теоремы.

Теорема 1. Пусть $N = 2^n$, $n = 2, 3, \ldots$, и m — натуральное число, $1 \leqslant i < n$. Тогда

$$Z_{2^m} = \{(\underbrace{z_1, 0, \ldots, 0}_{2^{n-m}}, \underbrace{z_2, 0, \ldots, 0}_{2^{n-m}}, \ldots, \underbrace{z_{2^m}, 0, \ldots, 0}_{2^{n-m}}) : z_i \in \mathbb{Z}_2\}$$

и $U_{2^m+2} = \{(u_1, \ldots, u_N) : u_i \in \mathbb{Z}_2,\ u_{(j-1)2^{n-m-1}+1} \oplus \ldots \oplus u_{j2^{n-m-1}} = 0,\ j = 1, \ldots, 2^{m+1}\}$.

Теорема 2. Пусть $N = 2^n$, $n = 2, 3, \ldots$, i — нечётное натуральное число, $N/2 < i < N$, $i - 1 = N/2 + N/4 + \ldots + N/2^k + i'$, где $0 \leqslant i' < N/2^{k+1}$. Тогда:

1) подпространство Z_{i-1} состоит из векторов, координаты которых одновременно можно представить в виде дизъюнктного объединения i' блоков длины 2^{k+1} и $N/2^{k+1} - 2i'$ блоков длины 2^k. Любой блок длины 2^l имеет вид $(z_1, \ldots, z_{2^l-1}, 0)$;
2) подпространство U_{i+1} раскладывается в прямую сумму подпространства

$$U_{N-N/2^{k+1}+1} = \{(\underbrace{u_1, \ldots, u_1}_{2^{k+1}}, \underbrace{u_2, \ldots, u_2}_{2^{k+1}}, \ldots, \underbrace{u_{2^{n-k-1}}, \ldots, u_{2^{n-k-1}}}_{2^{k+1}}) : u_i \in \mathbb{Z}_2\}$$

и подпространства

$$U_{i+1,N-N/2^{k+1}} = \{(\underbrace{u'_1, \ldots, u'_1}_{2^k}, \underbrace{0, \ldots, 0}_{2^k}, \ldots, \underbrace{u'_{2^{n-k-1}}, \ldots, u'_{2^{n-k-1}}}_{2^k}, \underbrace{0, \ldots, 0}_{2^k}) : u_i \in \mathbb{Z}_2\}$$

(которое может отсутствовать), где координаты u'_j связаны линейными соотношениями.

2. Серии формул для параметра Бхаттачарьи

В «хороших» случаях теоремы 1, 2 и аналогичные им позволяют свернуть формулу (1) до выражений, либо не содержащих сумм, либо имеющих полиномиальное число слагаемых, в худшем случае сократить внешнюю сумму до полиномиальной. Следующие три теоремы иллюстрируют каждый из этих случаев.

Теорема 3. Для $n = 2, 3, \ldots$ и $m = 1, \ldots, n-1$ справедливы равенства

$$Z\left(W_{2^n}^{(2^m+1)}\right) =$$

$$= 1 - \frac{1}{2^{2^m}}\left(1 + (1-2p)^{2^{n-m}}\right)^{2^m} + \sqrt{\frac{1}{2^{2^{m+1}}}\left(1 + (1-2p)^{2^{n-m}}\right)^{2^{m+1}} - (1-2p)^{2^n}}.$$

Теорема 4. Для $n = 2, 3, \ldots$ и $m = 1, \ldots, n-1$ справедливы равенства

$$Z\left(W_{2^n}^{(2^m-1)}\right) = \frac{(AB)^{2^{m-2}} B^{2^{m-1}}}{2^{2^m-1}} \times$$

$$\times \sum_{i,j=0}^{2^{m-1}-1} \binom{2^{m-1}-1}{i} \binom{2^{m-1}-1}{j} \sqrt{\left[\left(\frac{A}{B}\right)^{2^m-i-j} + \left(\frac{A}{B}\right)^{i+j}\right]\left[\left(\frac{A}{B}\right)^{i-j} + \left(\frac{A}{B}\right)^{j-i}\right]}.$$

Здесь $A = 1 + (1-2p)^{2^{n-m}}$ и $B = 1 - (1-2p)^{2^{n-m}}$.

Пусть $N = 2^n$, где $n \geqslant 2$; i — нечётное натуральное число; $N/2 < i < N$; числа i', k и подпространства Z_{i-1}, U_{i+1} построены по N и i, как в теореме 2. Тогда по этой же теореме в любом векторе $u \in U_{i+1}$ все координаты блока $u_{(j-1)2^k+1}, \ldots, u_{j2^k}$ либо одновременно равны 0, либо 1 для всех $j = 1, \ldots, 2^{n-k}$. Поэтому корректно определено отображение θ из U_{i+1} в $\mathbb{Z}_2^m$, где $m = 2^{n-k}$, которое ставит в соответствие вектору $u \in U_{i+1}$ вектор $\theta(u)$, j-я координата которого равна 1, если $u_{(j-1)2^k+1} = \ldots = u_{j2^k} = 1$, и 0 иначе. Далее, определим последовательность чисел $b_1, \ldots, b_m$, полагая $b_j = 2^k - 1$, если для любого $z \in Z_{i-1}$ имеем $z_{j2^k-1} = 0$, и $b_j = 2^k$ иначе. Наконец, для произвольных m-мерных векторов a и b положим $(a, b) = a_1 b_1 + \ldots + a_m b_m$. Справедлива

Теорема 5. Пусть $N = 2^n$, $n \geqslant 2$, i — нечётное натуральное число, $N/2 < i < N$; числа k, m, отображение θ и последовательность $b_1, \ldots, b_m$ выбраны, как и выше. Положим $U = \langle \theta(g_{i+1}), \ldots, \theta(g_N) \rangle$ и $\bar{U} = \theta(g_i) \oplus U$, где $g_i, \ldots, g_N$ — строки поляризационной матрицы G_N. Тогда справедлива формула

$$Z\left(W_{2^n}^{(i)}\right) = 2 \sum_t \binom{b_1}{t_1} \ldots \binom{b_m}{t_m} \sqrt{\left[\sum_{u \in U} p^{f(t,u)} (1-p)^{N-f(t,u)}\right] \left[\sum_{u \in \bar{U}} p^{f(t,u)} (1-p)^{N-f(t,u)}\right]},$$

где $f(t, u) = (u, b) + \mathrm{w}(t) - 2(t, u)$, а суммирование ведётся по векторам $t = (t_1, \ldots, t_m)$, таким, что $0 \leqslant t_j \leqslant b_j$ для всех $j = 1, \ldots, m$.

3. Вычисление параметров Бхаттачарьи для $N = 32$

Значения параметра Бхаттачарьи для $i = 1, 2, 4, 8, 16$ и $i = 3, 5, 9, 17, 6, 12, 24, 10, 20, 18$ можно найти, используя соответственно формулы

$$Z\left(W_{2^n}^{(2^m)}\right) = \left(1 - (1-2p)^{2^{n-m+1}}\right)^{2^{m-1}},$$

$$Z\left(W_{2^n}^{(2^k(2^m+1))}\right) =$$

$$= \left(1 - \frac{1}{2^{2^m}} \left(1 + (1-2p)^{2^{n-m-k}}\right)^{2^m} + \sqrt{\frac{1}{2^{2^{m+1}}} \left(1 + (1-2p)^{2^{n-m-k}}\right)^{2^{m+1}} - (1-2p)^{2^{n-k}}}\right)^{2^k}.$$

Значения параметра для $i = 7, 14, 15$ находим, используя теорему 4 и равенство $Z\left(W_{N2^k}^{(i2^k)}\right) = \left[Z\left(W_N^{(i)}\right)\right]^{2^k}$, справедливое для любого натурального k. Последнее соотношение, теорема 5, описанные ниже подпространства U и $\bar{U}$, а также указанный вектор $b = (b_1, \ldots, b_m)$ позволяют вычислить параметр Бхаттачарьи для $i = 19, 21, 22, 23, 25, 26, 27, 28, 29, 30, 31$.

Случай $i = N - 1$: $U = \langle (1, 1) \rangle$, $\bar{U} = (1, 0) \oplus U$; $b = (N/2 - 1, N/2 - 1)$.

Случай $i = N - 3$: $U = \langle (1, 0, 1, 0), (1, 1, 0, 0), (0, 0, 1, 1) \rangle$, $\bar{U} = (1, 0, 0, 0) \oplus U$; $b = (N/4 - 1, N/4 - 1, N/4 - 1, N/4 - 1)$.

Случай $i = N - 5$: $U = \langle (1, 0, 1, 0, 1, 0, 1, 0), (1, 1, 0, 0, 0, 0, 0, 0), \ldots, (0, 0, 0, 0, 0, 0, 1, 1) \rangle$, $\bar{U} = (1, 0, 1, 0, 0, 0, 0, 0) \oplus U$; $b = (b', b')$, где $b' = (N/8, N/8 - 1, N/8 - 1, N/8 - 1)$.

Случай $i = N - 7$: $U = \langle (1, 1, 0, 0, 0, 0, 0, 0), (0, 1, 1, 0, 0, 0, 0, 0), \ldots, (0, 0, 0, 0, 0, 0, 1, 1) \rangle$, $\bar{U} = (1, 0, 0, 0, 0, 0, 0, 0) + U$; $b = (b', b')$, где $b' = (N/8 - 1, N/8 - 1, N/8 - 1, N/8 - 1)$.

Случай $i = N - 9$: $U = \langle (1010101010101010), (110 \ldots 0), \ldots, (0 \ldots 011) \rangle$, $\bar{U} = (10101010 \ldots 0) \oplus U$; $b = (b', b')$, где $b' = \big(N/16, N/16 - 1, N/16, N/16 - 1, N/16, N/16 - 1, N/16 - 1, N/16 - 1\big)$.

Случай $i{=}N{-}11$: $U{=}\langle(1010000010100000),(10101010\ldots0),(10\ldots10),(110\ldots0)),$ $(00110\ldots0),\ldots,(0\ldots011)\rangle$, $\bar{U}=(1010\ldots0)\oplus U$; $b=(b',b')$, где $b'=\big(N/16,N/16-1,$ $N/16-1,N/16-1,N/16,N/16-1,N/16-1,N/16-1\big)$.

Случай $i=N-13$: $U=\langle((1000100010001000),(1010\ldots0),(1010000010100000),$ $(10101010\ldots0),(10\ldots10),(110\ldots0)),(00110\ldots0),\ldots,(0\ldots011)\rangle$, $\bar{U}=(100010\ldots0)\oplus U$; $b=(b',b')$, где $b'=\big(N/16,N/16-1,N/16-1,N/16-1,N/16-1,N/16-1,N/16-1,$ $N/16-1\big)$.

Например, чтобы вычислить $Z\left(W_{32}^{(22)}\right)$, сначала находим $Z\left(W_{16}^{(11)}\right)$, используя случай $i=N-5$ при $N=16$, а затем полученное значение возводим в квадрат.

Для $Z\left(W_{32}^{(11)}\right)$ и $Z\left(W_{32}^{(13)}\right)$ найдены соответственно следующие формулы:

$$2(4Q_1+32Q_2+112Q_3+4Q_4+4Q_5+224Q_6+16Q_7+16Q_8+256Q_9+24Q_{10}+16Q_{11}+$$
$$+Q_{13}+128Q_{14}+16Q_{15}+2Q_{17}+16(\sqrt{Q_4Q_5}+\sqrt{Q_{15}Q_{16}})+64(\sqrt{Q_7Q_8}+\sqrt{Q_{10}Q_{11}})+$$
$$+8\sqrt{Q_{10}Q_{12}}+\sqrt{Q_{13}Q_{18}}),$$
$$2(81Q_1'+4326Q_2'+864Q_+'108Q_4'+768Q_6'+432Q_7'+576Q_{10}'+54Q_{11}'+144Q_{14}'+12Q_{17}'+$$
$$+256\sqrt{Q_4'Q_5'}+96\sqrt{Q_{12}'Q_{13}'}+16\sqrt{Q_{15}'Q_{16}'}+\sqrt{Q_{18}'Q_{19}'}),$$

где Q_i и Q_i' — известные многочлены от p степени 16.

Наконец, $Z\left(W_{32}^{(32)}\right)=2^{32}p^{16}(1-p)^{16}$.

ЛИТЕРАТУРА

1. *Колесников С. Г., Леонтьев В. М.* Серии формул для параметров Бхаттачарьи в теории полярных кодов // Проблемы передачи информации. 2023. Т. 59. Вып. 1. С. 1–13.

УДК 519.17 DOI 10.17223/2226308X/17/38

КВАЗИЦИКЛИЧЕСКИЕ АЛЬТЕРНАНТНЫЕ КОДЫ И АНАЛИЗ ИХ БЕЗОПАСНОСТИ В КРИПТОГРАФИЧЕСКИХ ПРИЛОЖЕНИЯХ[1]

А. А. Кунинец

Представлен обзор квазициклических альтернантных кодов и их структурный анализ относительно классификации автоморфизмов. Детализированы методы восстановления структурной информации о коде. Привлекательность рассматриваемого семейства кодов заключается в его возможном криптографическом приложении и, как следствие, в уменьшении длины ключа постквантовых схем на кодах, исправляющих ошибки. К тому же данный метод построения кодов является универсальным и может быть применён для получения альтернантных кодов квазициклических алгеброгеометрических кодов, ассоциированных с произвольной кривой с известной группой автоморфизмов. Однако, как показано в работе, ввиду особенностей построения квазициклических альтернантных кодов возникает возможность редукции ключевой безопасности оригинального кода к ключевой безопасности кода с меньшими параметрами, который может не являться стойким к структурной атаке.

Ключевые слова: *квазициклические коды, альтернантные коды, инвариантные коды, алгеброгеометрические коды, функциональные поля, группа автоморфизмов кода.*

[1]Работа поддержана грантом Российского научного фонда № 22-41-0441.

Введение

Активное развитие квантовых технологий и стремительный рост вычислительной мощности квантового компьютера ставит под угрозу безопасность современных криптографических стандартов. Это связано с тем, что криптостойкость большинства асимметричных алгоритмов основывается на сложности задач факторизации целых чисел и дискретного логарифмирования, что делает их неустойчивыми к атакам с использованием квантового компьютера. В конце 2016 г. Национальный институт стандартов и технологий США (NIST) объявил о начале конкурса по стандартизации постквантовых алгоритмов. Одним из перспективных направлений в области постквантовой криптографии стала криптография на кодах, исправляющих ошибки. Главным недостатком данного синтезного метода постквантовых схем является большой размер открытого ключа, исчисляющийся в сотнях килобайт, а иногда и в мегабайтах. Эта проблема сильно препятствует практическому применению схем, построенных на кодах, и поэтому в качестве решения было предложено использование квазициклических кодов.

В данной работе рассмотрен принцип построения квазициклических кодов Гоппы, представлено редуцирование ключевой безопасности рассматриваемого кода к ключевой безопасности инвариантного кода с меньшими параметрами и детализирована структурная атака, описанная в [1].

1. Предварительные сведения

Мы опускаем базовые сведения из теории функциональных полей и алгебраической геометрии, предполагая, что читатель с ними ознакомлен. Для более подробного изучения можно обратиться к работам [2, 3].

Пусть $\mathbf{P}^1/\mathbb{F}_{q^m} : y = x$ — проективная прямая, $\mathbb{F}_{q^m}(\mathbf{P}^1) = \mathbb{F}_{q^m}(x)$ — её функциональное поле, также называющееся *полем рациональных функций* над $\mathbb{F}_{q^m}$, а полюс функции x является бесконечно удалённой точкой P_∞ прямой $\mathbf{P}^1$. Рациональные точки проективной прямой имеют вид $P_i = (x_i : 1)$.

Дивизором $D = P_1 + \ldots + P_n$ является формальная сумма попарно различных рациональных точек $\mathbf{P}^1$. *Носителем дивизора* называют множество $\mathrm{supp}(D) = \{P_1, \ldots, P_n\}$. Через G обозначим дивизор, такой, что $\mathrm{supp}(D) \cap \mathrm{supp}(G) = \varnothing$. АГ-код $\mathcal{C}$, ассоциированный с $\mathbf{P}^1$, будем обозначать $\mathcal{C} = \mathcal{C}_{\mathscr{L}}(D, G)$. *Пространство Римана — Роха*, ассоциированное с дивизором G, имеет вид $\mathscr{L}(G) = \{hx^i : i \in \{0, \ldots, \deg(G)\}\}$, где $G \sim \deg(G)P_\infty$ и $G + (h) = \deg(G)P_\infty$, $h \in \mathbb{F}_{q^m}(x)$.

Алгеброгеометрический способ построения классического кода Гоппы описывает следующая

Теорема 1. Пусть $D = P_1 + \ldots + P_n$ — дивизор, состоящий из n попарно различных рациональных точек $\mathbf{P}^1$ над $\mathbb{F}_{q^m}$; $G = G_0 - P_\infty$ — дивизор функционального поля $\mathbb{F}_{q^m}(\mathbf{P}^1)$, такой, что $\mathrm{supp}(D) \cap \mathrm{supp}(G) = \varnothing$, где $G_0 = (\Gamma)_0$ — дивизор нулей функции $\Gamma \in \mathbb{F}_q(\mathbf{P}^1)$; $\mathcal{C}_{\mathscr{L}}(D, G)$ — АГ-код над $\mathbb{F}_{q^m}$. Тогда классический код Гоппы имеет вид

$$\mathscr{G}_q(\mathbf{x}, \Gamma) = \mathcal{C}_{\mathscr{L}}(D, G_0 - P_\infty)^\perp \cap \mathbb{F}_q^n = \mathcal{C}_{\mathscr{L}}(D, A - G_0) \cap \mathbb{F}_q^n,$$

$\mathcal{C}_{\mathscr{L}}(D, G_0 - P_\infty)^\perp$ — дуальный к $\mathcal{C}_{\mathscr{L}}(D, G)$; $A = (h'(z)) + (n-1)P_\infty$; $h(z) = \prod\limits_{x_i \in \mathbf{x}} (z - x_i)$.

Обозначим через $\mathfrak{S}_n$ группу перестановок множества $\{1, \ldots, n\}$.

Определение 1. Пусть $\mathcal{C}$ — линейный код длины n над полем $\mathbb{F}_q$, $\sigma \in \mathfrak{S}_n$ и $\sigma(\mathbf{c}) = \left(c_{\sigma(1)}, \ldots, c_{\sigma(n)}\right)$. Тогда $\mathcal{C}$ называется *инвариантным относительно* σ, если $\sigma(\mathcal{C}) = \mathcal{C}$, а *группа автоморфизмов* кода $\mathcal{C}$ имеет вид

$$\mathrm{Aut}(\mathcal{C}) = \{\sigma \in \mathfrak{S}_n : \sigma(\mathcal{C}) = \mathcal{C}\}.$$

Так как альтернантные коды являются подполевыми подкодами GRS-кодов, в качестве автоморфизмов будем рассматривать проективную линейную группу, которая индуцирует всю группу автоморфизмов [4]:

$$\mathrm{PGL}_2(\mathbb{F}_{q^m}) = \left\{ \begin{matrix} \mathbf{P}^1 \to \mathbf{P}^1 \\ (x:y) \mapsto (ax+by : cx+dy) \end{matrix} \;\middle|\; \begin{matrix} a,b,c,d \in \mathbb{F}_{q^m}, \\ ad-bc \neq 0 \end{matrix} \right\}.$$

Элементы $\mathrm{PGL}_2(\mathbb{F}_{q^m})$ также имеют матричное представление, а именно: любой $\sigma \in \mathrm{PGL}_2(\mathbb{F}_{q^m})$ можно представить как $\sigma = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$, где $ad - bc \neq 0$.

Определение 2. Пусть $D = P_1 + \ldots + P_n$ — дивизор, носителем которого являются n попарно различных рациональных точек; G, G' — дивизоры на $\mathbf{P}^1$, такие, что $\{\mathrm{supp}(G), \mathrm{supp}(G')\} \cap \mathrm{supp}(D) = \varnothing$. Определим *отношение эквивалентности дивизоров относительно дивизора* D следующим образом: $G \sim_D G'$, если существует $f \in \mathbb{F}_{q^m}(\mathbf{P}^1)$, что $f \neq 0$, $G - G' = (f)$ и $f(P) = 1$ для всех $P \in \mathrm{supp}(D)$.

Следующая теорема определяет всевозможные автоморфизмы АГ-кода.

Теорема 2 [4, Теорема 3.1]. Пусть $\mathcal{C} = \mathcal{C}_{\mathscr{L}}(D, G) \subseteq \mathbb{F}_{q^m}^n$ — АГ-код; $1 \leqslant \deg(G) \leqslant n - 3$. Тогда

$$\mathrm{Aut}(\mathcal{C}) = \{\sigma \in \mathrm{Aut}\left(\mathbf{P}^1\right) : \sigma(D) = D \text{ и } \sigma(G) \sim_D G\}.$$

2. Квазициклические альтернантные коды

Пусть $\mathbb{F}$ — конечное поле, ℓ — положительное целое.

Определение 3. Определим циклический и квазициклический сдвиги, σ_ℓ и σ:

$$\sigma_\ell : \begin{cases} \mathbb{F}^\ell \to \mathbb{F}^\ell, \\ (x_0, x_1, \ldots, x_{\ell-1}) \mapsto (x_{\ell-1}, x_0, \ldots, x_{\ell-2}), \end{cases} \qquad \sigma : \begin{cases} \mathbb{F}^n \to \mathbb{F}^n, \\ (\mathbf{b}_1 | \ldots | \mathbf{b}_{n/\ell}) \mapsto \left(\sigma_\ell(\mathbf{b}_1) | \ldots | \sigma_\ell(\mathbf{b}_{n/\ell})\right). \end{cases}$$

Пусть n — целое и $\ell | n$. Тогда σ является ℓ-квазициклическим сдвигом, полученным поблочным применением σ_ℓ, где $\mathbf{b}_i$ — блоки длины ℓ, $i = 1, \ldots, n/\ell$.

Определение 4. Код $\mathcal{C} \subseteq \mathbb{F}^n$ называется *ℓ-квазициклическим* (ℓ-QC), если для всех $c \in \mathcal{C}$ выполняется $\sigma(c) \in \mathcal{C}$, где σ — операция квазициклического сдвига.

Определение 5. Пусть $\mathcal{C} \subseteq \mathbb{F}^n$ — ℓ-QC код. *Инвариантный код* и *проколотый инвариантный код* определяются следующим образом:

$$\mathcal{C}^\sigma = \{c \in \mathcal{C} : \sigma(c) = c\}, \quad \overline{\mathcal{C}}^\sigma = \mathrm{Punct}_{\mathcal{I}_\ell}(\mathcal{C}^\sigma),$$

где $\mathcal{I}_\ell = \{1, \ldots, n\} \backslash \{1, \ell+1, \ldots, n-\ell+1\}$.

Замечание 1. Инвариантность коммутирует с операцией вычисления подполевого подкода. Действительно, если $\mathcal{C}$ — ℓ-QC код над $\mathbb{F}_{q^m}$, то

$$(\mathcal{C} \cap \mathbb{F}_q^n)^\sigma = \{c \in \mathcal{C} : c \in \mathbb{F}_q^n \text{ и } \sigma(c) = c\} = \mathcal{C}^\sigma \cap \mathbb{F}_q^n.$$

Рассмотрим метод построения квазициклических альтернантных кодов, определённых над $\mathbb{F}_q$, с помощью заранее заданного автоморфизма.

Пусть $\sigma \in \mathrm{PGL}_2(\mathbb{F}_{q^m})$ и $\mathrm{ord}(\sigma) = \ell$. Для точки $P \in \mathbf{P}^1$ определим её орбиту

$$\mathrm{Orb}_\sigma(P) = \left\{\sigma^i(P) : i \in \{0, \ldots, \ell - 1\}\right\},$$

тогда

$$D = \sum_{i=1}^{n/\ell} \sum_{P \in \mathrm{Orb}_\sigma(P_i)} P, \quad \mathrm{supp}(D) = \coprod_{i=1}^{n/\ell} \mathrm{Orb}_\sigma(P_i), \tag{1}$$

где $P_i \in \mathbf{P}^1(\mathbb{F}_{q^m})$ — попарно различные не являющиеся инвариантными относительно заданного отображения σ точки с непересекающимися орбитами, не содержащими точку в бесконечности. Затем определим дивизор

$$G = \sum_{i=1}^{s} t_i \sum_{Q \in \mathrm{Orb}(Q_i)} Q, \tag{2}$$

где Q_i — точки $\mathbf{P}^1$, не содержащие в своих орбитах точку в бесконечности, такие, что $\mathrm{supp}(D) \cap Q_i = \varnothing$, $s \in \mathbb{N}$, $t_i \in \mathbb{Z}$ для $i \in \{1, \ldots, s\}$. При этом $\deg(G) = \sum\limits_{i=1}^{s} t_i \ell \deg(Q_i)$.

Таким образом, альтернантный код $\mathcal{A}_{r,q}(D, G) = \mathcal{C}_{\mathscr{L}}(D, G)^{\perp} \cap \mathbb{F}_q^n$ является квазициклическим при соответствующем упорядочивании точек.

3. Структурный анализ инвариантных кодов

Для упрощения рассуждений будем предполагать, что G строится с использованием орбиты одной рациональной точки Q, не содержащей точки в бесконечности, то есть $G = t \sum\limits_{R_j \in \mathrm{Orb}_\sigma(Q)} R_j$, где $R_j = \sigma^j(Q) = (\gamma_j, \delta_j) \neq P_\infty$ и $j \in \{0, \ldots, \ell - 1\}$. В общем случае, при построении дивизора G с помощью непересекающихся орбит нескольких точек полученный результат останется корректным. Покажем, что ключевую безопасность QC-альтернантного кода можно редуцировать к ключевой безопасности его инвариантного кода. Рассмотрим автоморфизм $\sigma \in \mathrm{PGL}_2(\mathbb{F}_{q^m})$ и альтернантный код

$$\mathcal{A}_{r,q}(D, G) = \mathcal{C}_{\mathscr{L}}(D, G)^{\perp} \cap \mathbb{F}_q^n.$$

Дивизоры D и G определены в (1) и (2). Зная порождающую матрицу кода $\mathcal{A}_{r,q}(D, G)$ и индуцированный автоморфизм σ, можно вычислить инвариантный код $\overline{\mathcal{A}_{r,q}(D, G)}^{\sigma}$. Обозначим через инвариантный код альтернантный код $\mathcal{A}_{r,q}(\tilde{D}, \tilde{G})$ для некоторых дивизоров $\tilde{D}$ и $\tilde{G} = t\widetilde{Q}$ с малыми параметрами. Существует взаимосвязь между $\tilde{D}$ и $\tilde{G}$ инвариантного кода с дивизорами D и G исходного альтернантного кода, позволяющая восстановить исходные дивизоры, зная $\tilde{D}$ и $\tilde{G}$.

Автоморфизм $\sigma \in \mathrm{PGL}_2(\mathbb{F}_{q^m})$ представим в виде матрицы $M \in \mathrm{GL}_2(\mathbb{F}_{q^m})$. Нотация $M \sim N$, где $M, N \in \mathrm{PGL}_2(\mathbb{F}_{q^m})$, означает, что существует матрица $P \in \mathrm{PGL}_2(\mathbb{F}_{q^m})$, такая, что $M = PNP^{-1}$.

Замечание 2. Если $\mathcal{C} = \mathcal{C}_{\mathscr{L}}(D, G)$ — АГ-код, такой, что $\sigma(\mathcal{C}) = \mathcal{C}$ и $\rho \in \mathrm{PGL}_2(\mathbb{F}_{q^m})$, то $\sigma' = \rho \circ \sigma \circ \rho^{-1}$ индуцирует тот же автоморфизм кода $\mathcal{C}$, что и σ.

В зависимости от собственных векторов матрицы M можно выделить три случая:

1. $M \sim \begin{pmatrix} a & 0 \\ 0 & 1 \end{pmatrix}$, где $a \in \mathbb{F}_{q^m}$ (σ — диагонализируемый в $\mathbb{F}_{q^m}$).

Восстановление G: если $\tilde{Q} \neq P_\infty$, для всех $i \in \{0, \ldots, \ell - 1\}$ имеем

$$\tilde{Q} = \left((-1)^{\ell-1} \left(a^i\right)^{\ell(\ell-1)/2} \left(\frac{\gamma_i}{\delta_i}\right)^{\ell} : 1 \right), \quad G = t \sum_{\gamma \in \Gamma} (\gamma : 1),$$

где Γ — множество корней многочлена $a^{\ell(\ell-1)/2} X^\ell - \tilde{\gamma}$.

Восстановление D' (отличается от оригинального дивизора на перестановку):

$$\begin{cases} x^\ell - \tilde{\alpha}_i = 0, \\ y^\ell - \tilde{\beta}_i = 0, \quad \text{где } (\tilde{\alpha}_i, \tilde{\beta}_i) \in \operatorname{supp}(\tilde{D}); \end{cases} \tag{3}$$

$$\operatorname{supp}(D') = \left\{ \left(a^j \frac{\alpha'_i}{\beta'_i} : 1 \right) : j \in \{0, \ldots, \ell - 1\}, i \in \{1, \ldots, n/\ell\} \right\}, \text{ где } (\alpha'_i, \beta'_i) \text{ — корни (3).}$$

2. $M \sim \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix}$, где $b \in \mathbb{F}_{q^m}$ (σ — тригонализируемый в $\mathbb{F}_{q^m}$).

Восстановление G: если $\tilde{Q} \neq P_\infty$, для всех $i \in \{0, \ldots, \ell - 1\}$ имеем

$$P_b = \text{НОД}\left(\left\{ \operatorname{Res}_X \left(X^p - Y^{p-1} X - \tilde{\alpha}_i, X^{q^m} - X \right) : i \in \{1, \ldots, n/\ell\} \right\}, Y^{q^m} - Y \right),$$

$$\tilde{Q} = \left(\left(\frac{\gamma_i}{\delta_i} \right)^p - b^{p-1} \frac{\gamma_i}{\delta_i} : 1 \right), b - \text{корни}(P_b),$$

$$G = t \sum_{\gamma \in \Gamma} (\gamma : 1), \text{ где } \Gamma \text{ — множество корней многочлена } X^p - b^{p-1} X - \tilde{\gamma}.$$

Восстановление D':

$$\begin{cases} x^p - b^{p-1} x - \tilde{\alpha}_i = 0, \\ y^p - \tilde{\beta}_i = 0, \end{cases} \tag{4}$$

$$\operatorname{supp}(D') = \left\{ \left(\frac{\alpha'_i}{\beta'_i} + bj : 1 \right) : j \in \{0, \ldots, \ell - 1\}, i \in \{1, \ldots, n/\ell\} \right\}, \text{ где } (\alpha'_i, \beta'_i) \text{ — корни (4).}$$

3. $M \sim \begin{pmatrix} \xi & 0 \\ 0 & \xi^{q^m} \end{pmatrix}$, где $\xi \in \mathbb{F}_{q^{2m}}$ (σ — диагонализируемый в $\mathbb{F}_{q^{2m}}$).

Поскольку σ_d диагонален в $\mathbb{F}_{q^{2m}}$, мы можем восстановить носитель $D^\otimes$ и дивизор $G^\otimes$ в $\mathbb{F}_{q^{2m}}$, используя те же методы, что и ранее.

Рассмотрим минимальный многочлен $\pi_\xi = X^2 + aX + b \in \mathbb{F}_{q^m}[X]$ элемента ξ. Тогда

$$M_{\sigma_d} = \begin{pmatrix} \xi & 0 \\ 0 & \xi^{q^m} \end{pmatrix} \sim \begin{pmatrix} 0 & -b \\ 1 & -a \end{pmatrix} = M_{\sigma'}$$

и существует $\rho' \in \mathrm{GL}_2(\mathbb{F}_{q^{2m}})$, такой, что $\sigma_d = \rho' \circ \sigma' \circ \rho'^{-1}$, где $\sigma' \in \mathrm{PGL}_2(\mathbb{F}_{q^m})$ ассоциирован с $M_{\sigma'}$. Согласно замечанию 2, мы можем предположить, что $\sigma = \sigma'$. Чтобы восстановить ρ', достаточно диагонализировать матрицу $M_{\sigma'}$. Зная ρ', носитель дивизора $D^\otimes$ и дивизор $G^\otimes$ в $\mathbb{F}_{q^{2m}}$, можно восстановить оригинальный дивизор $D = \rho'^{-1}(D^\otimes)$ и дивизор $G = \rho'^{-1}(G^\otimes)$ в $\mathbb{F}_{q^m}$.

Восстановим перестановку Π между $\mathcal{A}_{r,q}(D', G)$ и $\mathcal{A}_{r,q}(D, G)$:

$$\mathbf{G}_{\text{pub}} \cdot \Pi \cdot \mathbf{H}'^{\top} = 0, \tag{5}$$

где $\mathbf{G}_{\text{pub}}$ — порождающая матрица кода $\mathcal{A}_{r,q}(D,G)$; $\mathbf{H}'$ — проверочная матрица кода $\mathcal{A}_{r,q}(D',G)$. Перестановочная матрица Π имеет следующий вид:

$$\begin{pmatrix} \sum\limits_{i=1}^{\ell} x_{1,i}\mathbf{J}^i & \dots & (0) \\ \vdots & \ddots & \vdots \\ (0) & \dots & \sum\limits_{i=1}^{\ell} x_{n/\ell,i}\mathbf{J}^i \end{pmatrix}, \text{ где } \mathbf{J} = \begin{pmatrix} 0 & \dots & \dots & 0 & 1 \\ 1 & \ddots & & & 0 \\ 0 & \ddots & \ddots & & \vdots \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ 0 & \dots & 0 & 1 & 0 \end{pmatrix}.$$

Отметим, что $\mathbf{J}$ — матрица размера $\ell\times\ell$, $x_{j,i}\in\{0,1\}$ — неизвестные для $j\in\{1,\dots,n/\ell\}$ и $i\in\{1,\dots,\ell\}$. В таком случае система (5) имеет n неизвестных. Если предположить, что $k\neq n$, то мы можем найти с большой вероятностью единственное решение для Π ввиду того, что в системе $(n-k)k$ уравнений и $n\leqslant(n-k)k$ неизвестных.

ЛИТЕРАТУРА

1. *Barelli E.* On the security of short McEliece keys from algebraic and algebraic geometry codes with automorphisms. University of Paris-Saclay, France, 2018. (in French)
2. *Кунинец А. А., Малыгина Е. С.* Вычисление пар, исправляющих ошибки, для алгеброгеометрического кода // Прикладная дискретная математика. 2023. № 63. С. 65–90.
3. *Малыгина Е. С., Кунинец А. А., Раточка В. Л. и др.* Алгеброгеометрические коды и декодирование на основе пар, исправляющих ошибки // Прикладная дискретная математика. 2023. № 62. С. 83–105.
4. *Stichtenoth H.* On automorphisms of geometric Goppa codes // J. Algebra. 1990. No. 130(1). P. 113–121.

УДК 519.7 DOI 10.17223/2226308X/17/39

КОНЕЧНО-АВТОМАТНЫЕ ГЕНЕРАТОРЫ МАКСИМАЛЬНОГО ПЕРИОДА

Е. С. Прудников

Сформулированы некоторые необходимые и некоторые достаточные условия максимальности периода конечно-автоматного генератора. Предложен способ построения генератора с максимальным периодом.

Ключевые слова: *конечно-автоматный генератор, максимальный период, подстановки.*

Рассматривается двухкаскадный конечно-автоматный криптографический генератор $G=A_1\cdot A_2$ — последовательное соединение автономного автомата $A_1=(\mathbb{F}_2^n,\mathbb{F}_2,g_1,f_1)$ и автомата $A_2=(\mathbb{F}_2,\mathbb{F}_2^m,\mathbb{F}_2,g_2,f_2)$, $n,m\geqslant 1$. В каждый момент времени t автомат A_1, находясь в состоянии $x(t)\in\mathbb{F}_2^n$, выдаёт выходной символ $u(t)=f_1(x(t))$ и переходит в следующее состояние $x(t+1)=g_1(x(t))$, а автомат A_2, находясь в состоянии $y(t)\in\mathbb{F}_2^m$, принимает от A_1 символ $u(t)$, выдаёт на выход генератора выходной символ $z(t)=f_2(u(t),y(t))$ и переходит в следующее состояние $y(t+1)=g_2(u(t),y(t))$. Выходную последовательность автомата A_1 обозначим $u=\big(u(t):t=1,2,\dots\big)$.

Генератор G является, с одной стороны, обобщением конечно-автоматного генератора (δ,τ)-шагов [1] (функция g_2 произвольна), а с другой — частным случаем последовательной композиции в модели автоматов с функциональными ключами, предложенной Г. П. Агибаловым в [2] (A_1 — автомат Мура). В [3] изучены некоторые задачи криптоанализа такого генератора, а в [4] — его периодические свойства.

Периодом генератора назовём длину периода его выходной последовательности. В [4] показано, что период G не превосходит 2^{n+m} и сформулированы некоторые необходимые условия максимальности периода (достижимости этой границы), в частности доказано, что если период G максимальный, то подфункции $g_2^\sigma = g_2(\sigma, \cdot)$, $\sigma \in \{0,1\}$, функции g_2 являются подстановками, а функция g_1 — полноцикловой подстановкой.

Дополним список необходимых условий.

Утверждение 1. Если период генератора G равен 2^{n+m}, то:

1) последовательность u чисто периодическая и её период равен 2^n;
2) вес функции f_1 нечётный;
3) подстановки g_2^0 и g_2^1 имеют разную чётность.

Следующее утверждение даёт достаточные условия максимальности периода генератора; здесь через G_u обозначена композиция подстановок: $G_u = g_2^{u(1)} g_2^{u(2)} \dots g_2^{u(2^n)}$.

Утверждение 2. Пусть для генератора G выполнены условия утверждения 1; кроме того:

1) последовательность u и подстановки g_2^0 и g_2^1 таковы, что G_u — полноцикловая подстановка;
2) функция $g_2(u, y)$, $u \in \mathbb{F}_2$, $y \in \mathbb{F}_2^m$, инъективна по u;
3) функция f_2 имеет нечётный вес.

Тогда период G равен 2^{n+m}.

Отметим, что полученные условия не могут рассматриваться как критерий: выполнение условий утверждения 1 не гарантирует максимальность периода, как и максимальность периода не обязательно означает выполнение условий утверждения 2. Однако с помощью утверждения 2 можно построить автомат A_2, такой, что для любого автомата A_1, удовлетворяющего условиям 1 и 2 утверждения 1, генератор $G = A_1 \cdot A_2$ будет иметь максимальный период.

Утверждение 3. Пусть g_2^0 — произвольная полноцикловая подстановка, g_2^1 — произвольная её чётная степень. Тогда:

1) функция $g_2(u, y)$ инъективна по u;
2) композиция G_u является полноцикловой подстановкой для любой чисто периодической последовательности u с длиной периода 2^n и такой, что вес отрезка $u(1) \dots u(2^n)$ нечётный.

Таким образом, для построения генератора G, имеющего максимальный период, достаточно:

1) в качестве g_1 выбрать произвольную полноцикловую подстановку на $\mathbb{F}_2^n$;
2) в качестве f_1 взять произвольную булеву функцию нечётного веса от n переменных;
3) в качестве g_2^0 взять произвольную полноцикловую подстановку на $\mathbb{F}_2^m$, а в качестве g_2^1 — любую её чётную степень (или наоборот);
4) в качестве f_2 взять произвольную булеву функцию нечётного веса от $(m+1)$ переменных.

ЛИТЕРАТУРА

1. *Агибалов Г. П., Панкратова И. А.* О двухкаскадных конечно-автоматных криптографических генераторах и методах их криптоанализа // Прикладная дискретная математика. 2017. № 35. С. 38–47.

2. *Агибалов Г. П.* Криптоавтоматы с функциональными ключами // Прикладная дискретная математика. 2017. № 36. С. 59–72.
3. *Боровкова И. В., Панкратова И. А., Семенова Е. В.* Криптоанализ двухкаскадного конечно-автоматного генератора с функциональным ключом // Прикладная дискретная математика. 2018. № 42. С. 48–56.
4. *Обухов П. К., Панкратова И. А.* Периодические свойства конечно-автоматного генератора // Прикладная дискретная математика. Приложение. 2023. № 16. С. 141–143.

УДК 519.17 DOI 10.17223/2226308X/17/40

К ВОПРОСУ О СТРУКТУРЕ ТУРНИРОВ, СОСТОЯЩИХ ИЗ ОДНИХ КОРОЛЕЙ

А. О. Шабаркова, М. Б. Абросимов

Рассмотрена структура некоторых классов турниров, состоящих из одних королей, и их количество. Вершина v турнира называется королём, если длина пути из v до любой другой вершины составляет не более чем 2. Турнир называется простым, если его решётка конгруэнций двухэлементна и содержит только тождественную и универсальную конгруэнции. Основной результат работы состоит в том, что турниры, состоящие из одних королей, не являются простыми.

Ключевые слова: *теория графов, турнир, матрица расстояний.*

Турниром называется полный направленный граф. Основные определения по теории графов используются, согласно работе [1].

Ориентированный граф называется регулярным, если все его вершины имеют одинаковые степени захода и исхода. Вершина v турнира $\overrightarrow{T}$ — король, если длина пути из v до любой другой вершины не более 2.

Конгруэнция турнира $\overrightarrow{T} = (V, \alpha)$ — это такая эквивалентность на множестве его вершин, что фактор-граф по ней является турниром. То есть конгруэнция турнира $\overrightarrow{T} = (V, \alpha)$ — это такая эквивалентность $\theta \subseteq V \times V$, что никакие два различных θ-класса не имеют встречных дуг [1]. Известно, что совокупность всех конгруэнций турнира $\overrightarrow{T}$ образует решётку [2]. Особый интерес представляют простые турниры — это турниры, чья решётка конгруэнций двухэлементна и содержит только тождественную и универсальную конгруэнции.

Строению турниров посвящено много работ (см., например, [3]). Простые турниры рассматриваются в [4]. Известно, что не существует турниров, имеющих в точности два короля [5]. Показано, что для каждого положительного n, такого, что $n \neq 2$, $n \neq 4$, существует турнир размерности n, где каждая вершина является королём [6]. Турниры являются важным классом ориентированных графов. Отметим интересное применение турниров для построения криптосистем: в [7] предлагается симметричная криптосистема, основанная на турнирах Пэли.

Обозначим $(1^n, 2^m)$ строку матрицы расстояний, в которой n единиц и m двоек.

Теорема 1. Турнир $\overrightarrow{T}$ размерности n, где n нечётное и $n > 5$, состоящий из одних королей, пять строк матрицы расстояний которого имеют вид $(1^{(n-1)/2}, 2^{(n-1)/2})$, а остальные — $(1^{(n-i-1)}, 2^i)$, $i \in \{1, \ldots, (n-1)/2 - 2, (n-1)/2 + 2, \ldots, n-2\}$, не является простым и имеет следующую структуру: в основании 5-вершинный регулярный турнир, к которому последовательно добавляют по две вершины v_1 и v_2 следующим образом: из вершины v_1 ведут дуги во все вершины турнира $\overrightarrow{T^*}$; из каждой вершины

турнира $\overrightarrow{T^*}$ ведут дуги в вершину v_2; а также есть дуга из v_2 в v_1, где $\overrightarrow{T^*}$ — турнир, полученный на предыдущем шаге, пока размерность полученного турнира не будет равна n. Такой турнир $\overrightarrow{T}$ для каждого нечётного $n > 5$ один.

Теорема 2. Турнир $\overrightarrow{T}$ размерности n, где n нечётное и $n > 3$, состоящий из одних королей, три строки матрицы расстояний которого имеют вид $(1^{(n-1)/2}, 2^{(n-1)/2})$, а остальные — $(1^{(n-i-1)}, 2^i)$, $i \in \{1, \ldots, (n-1)/2 - 1, (n-1)/2 + 1, \ldots, n-2\}$, не является простым и имеет следующую структуру: в основании 3-вершинный регулярный турнир, к которому последовательно добавляют по две вершины v_1 и v_2 следующим образом: из вершины v_1 ведут дуги во все вершины турнира $\overrightarrow{T^*}$; из каждой вершины турнира $\overrightarrow{T^*}$ ведут дуги в вершину v_2; а также есть дуга из v_2 в v_1, где $\overrightarrow{T^*}$ — турнир, полученный на предыдущем шаге, пока размерность полученного турнира не будет равна n. Такой турнир $\overrightarrow{T}$ для каждого нечётного $n > 3$ один.

Теорема 3. Турнир $\overrightarrow{T}$ размерности n, где n нечётное, состоящий из одних королей, матрица расстояний которого состоит из следующих строк:

1) $(1^{n-2}, 2^1)$ — одна строка;
2) $(1^{(n-1)/2}, 2^{(n-1)/2})$ — $(n-2)$ строки;
3) $(1^1, 2^{n-2})$ — одна строка,

не является простым и получается добавлением вершин v_1 и v_2 к регулярному турниру $\overrightarrow{T^*}$ с числом вершин $n-2$ следующим образом: из вершины v_1 ведут дуги во все вершины турнира $\overrightarrow{T^*}$; из каждой вершины турнира $\overrightarrow{T^*}$ ведут дуги в вершину v_2; а также есть дуга из v_2 в v_1.

Теоремы 1–3 можно обобщить и расширить на любую размерность регулярного турнира, лежащего в основании.

Теорема 4. Турнир $\overrightarrow{T}$ размерности n, где n нечётное, состоящий из одних королей, k строк матрицы расстояний которого имеют вид $(1^{(n-1)/2}, 2^{(n-1)/2})$, а остальные — $(1^{(n-i-1)}, 2^i)$, $i \in \{1, \ldots, (n-k)/2, (n+k)/2-1, \ldots, n-2\}$ (т. е. элементов слева и справа от центрального по $(n-k)/2$), имеет следующую структуру: в основании регулярный турнир размерности k, к которому последовательно добавляют по две вершины v_1 и v_2 следующим образом: из вершины v_1 ведут дуги во все вершины турнира $\overrightarrow{T^*}$; из каждой вершины турнира $\overrightarrow{T^*}$ ведут дуги в вершину v_2; а также есть дуга из v_2 в v_1, где $\overrightarrow{T^*}$ — турнир, полученный на предыдущем шаге, пока размерность полученного турнира не будет равна n. Такой турнир не является простым и для каждого n таких турниров столько же, сколько существует регулярных турниров с числом вершин, как у турнира в основании (3-вершинный $\overrightarrow{T^*}$ — один турнир $\overrightarrow{T}$; 5-вершинный $\overrightarrow{T^*}$ — один турнир $\overrightarrow{T}$; 7-вершинный $\overrightarrow{T^*}$ — три турнира $\overrightarrow{T}$ и т. д.).

ЛИТЕРАТУРА

1. *Богомолов А. М., Салий В. Н.* Алгебраические основы теории дискретных систем. М.: Физматлит, 1997.
2. *Киреева А. В.* Конгруэнции турниров // Студенты — ускорению научного прогресса: Сб. студ. науч. раб. Саратов: Изд-во Сарат. ун-та, 1990. С. 3–5.
3. *Moon J. W.* Topics on Tournaments. N.Y.: Holt, Rinehart and Winston, 1968.
4. *Erdös P., Fried E., Hajnal A., and Milner E. C.* Some remarks on simple tournaments // Algebra Universalis. 1972. V. 2. No. 2. P. 238–245.
5. *Moon J. W.* Solution to problem 463 // Math. Mag. 1962. No. 35. P. 189.

6. *Maurer S.* The king chicken theorems // Math. Magazine. 1980. V. 53. No. 2. P. 67–80.
7. *Oumazouz Z. and Karim D.* A new symmetric key cryptographic algorithm using Paley graphs and ASCII values // E3S Web Conf. 2021. V. 297. Article 01046. 5 p.

Секция 6

ВЫЧИСЛИТЕЛЬНЫЕ МЕТОДЫ В ДИСКРЕТНОЙ МАТЕМАТИКЕ

УДК 519.7 DOI 10.17223/2226308X/17/41

ИССЛЕДОВАНИЕ АЛГОРИТМА k-ПРОСЕИВАНИЯ ДЛЯ РЕШЕНИЯ ЗАДАЧИ НАХОЖДЕНИЯ КРАТЧАЙШЕГО ВЕКТОРА В РЕШЁТКЕ[1]

А. О. Бахарев

Квантовые вычисления активно развиваются в последние десятилетия: увеличивается количество кубитов, с которыми оперирует квантовый компьютер, и снижается вероятность вычислительных ошибок. Поэтому возникает необходимость в разработке и анализе постквантовых криптосистем — криптосистем, устойчивых к атакам с использованием квантового компьютера. Одним из основных подходов к построению таких криптосистем является теория решёток. В данном подходе стойкость большинства криптосистем сводится к решению задачи нахождения кратчайшего вектора в решётке (SVP). В работе приводятся результаты анализа алгоритма 8-просеивания для решения SVP. Предлагается новый компромисс между временем работы и количеством используемой памяти алгоритма 8-просеивания. Приводится сравнение с известными алгоритмами k-просеивания. На отрезке $(2^{0{,}157n}, 2^{0{,}189n})$ используемой памяти предложенный алгоритм имеет минимальное время работы среди известных алгоритмов k-просеивания.

Ключевые слова: *теория решёток, k-просеивание, SVP, постквантовая криптография.*

Введение

Задача поиска кратчайшего вектора в решётке заключается в поиске кратчайшего ненулевого вектора в решётке и является одной из основных задач, к которой сводится стойкость большинства криптосистем, построенных на решётках. Например, вариации задач обучения с ошибками (LWE) и нахождения короткого целочисленного решения (SIS), на которых строятся современные схемы инкапсуляции ключей и подписи соответственно, могут быть представлены как аппроксимационный случай задачи SVP или сводиться к ней.

Выделяют два больших семейства алгоритмов, решающих задачу SVP: алгоритмы перечисления [1, 2] и просеивания [3–10]. Алгоритмы просеивания имеют экспоненциальное время работы и используют экспоненциальное количество памяти в зависимости от размерности решётки; алгоритмы перечисления используют полиномиальное количество памяти, но уступают алгоритмам просеивания по времени работы.

В настоящей работе предложен новый компромисс между временем работы и используемой памятью алгоритма 8-просеивания для решения задачи SVP.

[1]Работа выполнена при поддержке Математического центра в Академгородке, соглашение с Министерством науки и высшего образования Российской Федерации № 075-15-2022-282.

1. Основные определения и обозначения

1.1. Решётки

Определение 1. Пусть векторы $\mathbf{v}_1, \ldots, \mathbf{v}_n \in \mathbb{R}^d$ линейно независимы. *Решёткой, порождённой векторами* $\mathbf{v}_1, \ldots, \mathbf{v}_n$, называется набор линейных целочисленных комбинаций векторов $\mathbf{v}_1, \ldots, \mathbf{v}_n$:

$$\mathcal{L} = \{a_1\mathbf{v}_1 + a_2\mathbf{v}_2 + \ldots + a_n\mathbf{v}_n : a_1, a_2, \ldots, a_n \in \mathbb{Z}\}.$$

Определение 2. *Базисом* для $\mathcal{L}$ является любой линейно независимый набор векторов, порождающий $\mathcal{L}$. Базисные векторы могут быть представлены в виде базисной матрицы $B = [\mathbf{v}_1|\mathbf{v}_2|\ldots|\mathbf{v}_n]$.

Любые два базиса $\mathcal{L}$ связаны преобразованием с целочисленной матрицей, определитель которой равен ± 1 (унимодулярная матрица).

Определение 3. *Ранг решётки* — число векторов в базисе $\mathcal{L}$, *размерность решётки* $\mathcal{L}$ равна d.

В случае, когда $n = d$, решётка $\mathcal{L}$ называется *решёткой полного ранга*. В настоящей работе рассматриваются только такие решётки.

Определение 4. *Минимальным расстоянием* λ_1 называется норма кратчайшего ненулевого вектора в решетке $\mathcal{L}$, то есть

$$\lambda_1(\mathcal{L}) = \min_{\mathbf{x} \in \mathcal{L} \setminus \{\mathbf{0}\}} \|\mathbf{x}\|.$$

Определение 5 (*задача поиска кратчайшего вектора* — *SVP*). Дан базис $\mathbf{B}$, который задаёт решетку $\mathcal{L}$; требуется найти ненулевой вектор $\mathbf{v} \in \mathcal{L}$, такой, что $\|\mathbf{v}\| = \lambda_1(\mathcal{L})$.

SVP является NP-трудной задачей [11].

1.2. Алгоритмы просеивания

Впервые алгоритмы просеивания были описаны в [3]. Современные алгоритмы просеивания используют следующую эвристику, что существенно сокращает время работы алгоритма.

Эвристика 1. Векторы решётки длины $\leqslant R$ асимптотически почти наверное распределены равномерно на сфере радиуса R.

Данная эвристика была предложена и изучена в [4]. Самой трудоёмкой частью алгоритмов просеивания является шаг просеивания, который принимает на вход список L, содержащий N векторов длины не больше R, параметр $\gamma < 1$ и выдаёт в качестве ответа список L_{out}, содержащий N векторов длины не больше γR. Обычно γ предполагается равной $1 - \text{poly}(n)^{-1} \approx 1$. Подавая на вход список, полученный на выходе предыдущего шага, полиномиальное количество раз, находим кратчайший вектор в решётке. Первый входной список может быть сгенерирован, например, алгоритмом Клейна [12]. Будем рассматривать следующие упрощения, которые асимптотически не влияют на оценки алгоритмов: $R = 1$ и $\gamma = 1$.

Впервые алгоритм k-просеивания был представлен в работе [5]. Его основная идея состоит в нахождении в заданном списке L кортежей $(\mathbf{x}_1, \ldots, \mathbf{x}_k) \in L^k$, удовлетворяющих условию $\|\mathbf{x}_1 \pm \cdots \pm \mathbf{x}_k\| \leqslant 1$, в отличие от рассматриваемых ранее алгоритмов,

в которых искались пары $(\mathbf{x}_1, \mathbf{x}_2) \in L^2$, удовлетворяющие условию $\|\mathbf{x}_1 \pm \mathbf{x}_2\| \leqslant 1$ (условие $\|\mathbf{x}_1 \pm \mathbf{x}_2\| \leqslant 1$ означает, что $\|\mathbf{x}_1 + \mathbf{x}_2\| \leqslant 1$ или $\|\mathbf{x}_1 - \mathbf{x}_2\| \leqslant 1$, для $k > 2$ аналогично). Задачу нахождения N таких кортежей будем называть *задачей k-просеивания*. Расширение на $k > 2$ позволяет уменьшить количество используемой алгоритмом памяти, т. е. размер входного списка L, но вместе с этим увеличивается время работы. Данный компромисс между используемой памятью и временем работы алгоритма может быть полезен при вычислении кратчайшего вектора в решётке. Например, в конкурсе «SVP challenge» [13], направленном на нахождение коротких векторов в решётке, для небольших размерностей решёток экспоненциальный размер L приводит к использованию большого объёма оперативной памяти (1–2 Тбайт).

Определение 6. Будем говорить, что кортеж $(\mathbf{x}_1, \ldots, \mathbf{x}_k) \in L^k$ *удовлетворяет конфигурации* $C \in \mathbb{R}^{k \times k}$, если и только если $\forall\, i, j\ \langle \mathbf{x}_i | \mathbf{x}_j \rangle \leqslant C_{ij}$, где $\langle \mathbf{x}_i | \mathbf{x}_j \rangle$ — скалярное произведение векторов $\mathbf{x}_i$ и $\mathbf{x}_j$.

В [6] показано, что задача k-просеивания сводится к задаче поиска кортежа $(\mathbf{x}_1, \ldots, \mathbf{x}_k) \in L^k$, удовлетворяющего некоторой конфигурации.

Определение 7. Для конфигурации $C \in \mathbb{R}^k$ и угла α определим *конфигурацию остатков* $C' \in \mathbb{R}^k$ следующим образом:

$$C'_{ij}(\alpha) = \begin{cases} \dfrac{1}{\sin^2 \alpha} \left(C_{ij} + \dfrac{\cos^2 \alpha}{k-1} \right), & \text{если } i \neq j, \\ 1 & \text{иначе.} \end{cases}$$

Для уменьшения времени работы алгоритма используются также локально-чувствительные фильтры, появившиеся впервые в [7] и представляемые случайным произведением кодов с равномерно распределёнными кодовыми словами на сфере единичного радиуса и эффективным алгоритмом декодирования. Подробнее о случайном произведении кодов и его вариации для алгоритмов k-просеивания можно узнать в [8].

1.3. Концепция k-просеивания

В [8] представлена новая концепция алгоритма k-просеивания (алгоритм 1).

Алгоритм 1. Концепция алгоритма k-просеивания (A. Chailloux, J. Loyer, 2023)

Вход: список L, содержащий N векторов; параметр k; угол α; конфигурация C.
Выход: список L_{out}, содержащий N редуцированных векторов.

1: Сгенерировать наборы фильтров. Фильтрация L: добавить каждый $\mathbf{x} \in L$ к ближайшему фильтру.
2: Для каждого набора фильтров найти все решения (FAS), удовлетворяющие конфигурации C, и добавить их в L_{out}.
3: Повторять шаги 1 и 2, пока $|L_{\text{out}}| < N$.

В [8] получено выражение для времени работы данной концепции:

$$T(k\text{-sieve}) = \text{NbRep}_{\alpha,C} \left(|L| + \text{NbFiltres}_\alpha \cdot T(\text{FAS}_{C'(\alpha)}) \right),$$

где $\text{NbFiltres}_\alpha = \mathcal{O}(\mathcal{V}(\alpha)^{-1})$, $\text{NbRep}_{\alpha,C} = \mathcal{O}\left(\max\left\{ 1, \dfrac{\det(C)^{n/2}}{\mathcal{V}^{k-1}(\alpha) \det(C'(\alpha))^{n/2}} \right\} \right)$ и $\mathcal{V}(\alpha) = \text{poly}(d) \cdot \sin^n \alpha$.

2. 8-просеивание

В настоящей работе предложен новый алгоритм 8-просеивания. Используется концепция алгоритма 1, поэтому вместо всего алгоритма просеивания приведём внутренний алгоритм $\mathrm{FAS}_{C'(\alpha)}$ (алгоритм 2). Он использует следующие промежуточные списки:

1) Для $j = 1, 5$ и $i = 1, 2, 3$ пусть

$$L_{j,j+i} = \{(\mathbf{x}_j, \mathbf{x}_{j+i}) \in L_j \times L_{j+i} : \langle \mathbf{x}_j | \mathbf{x}_{j+i} \rangle \leqslant C_{j,j+i}\}.$$

2) Для каждого $\mathbf{x}_j \in L_j$, $j = 1, 5$ и $i = 1, 2, 3$ пусть

$$L_{j+i}(\mathbf{x}_j) = \{\mathbf{x}_{j+i} \in L_{j+i} : (\mathbf{x}_j, \mathbf{x}_{j+i}) \in L_{j,j+i}\}.$$

3) Для каждого $\mathbf{x}_j \in L_j$, $j = 1, 5$ и $i = 2, 3$ пусть

$$L_{j+1,j+i}(\mathbf{x}_j) = \{(\mathbf{x}_{j+1}, \mathbf{x}_{j+i}) \in L_{j+1}(\mathbf{x}_j) \times L_{j+i}(\mathbf{x}_j) : \langle \mathbf{x}_{j+1} | \mathbf{x}_{j+i} \rangle \leqslant C_{j+1,j+i}\}.$$

4) Для каждых $\mathbf{x}_j \in L_j$, $j = 1, 5$, $\mathbf{x}_{j+1} \in L_{j+1}(\mathbf{x}_j)$ и $i = 2, 3$ пусть

$$L_{j+i}(\mathbf{x}_j, \mathbf{x}_{j+1}) = \{\mathbf{x}_{j+i} \in L_{j+i} : (\mathbf{x}_{j+1}, \mathbf{x}_{j+i}) \in L_{j+1,j+i}(\mathbf{x}_j)\}.$$

5) Для каждых $\mathbf{x}_j \in L_1$, $j = 1, 5$ и $\mathbf{x}_{j+1} \in L_{j+1}(\mathbf{x}_j)$ пусть

$$L_{j+2,j+3}(\mathbf{x}_j, \mathbf{x}_{j+1}) =$$
$$= \{(\mathbf{x}_{j+2}, \mathbf{x}_{j+3}) \in L_{j+2}(\mathbf{x}_j, \mathbf{x}_{j+1}) \times L_i(\mathbf{x}_j, \mathbf{x}_{j+1}) : \langle \mathbf{x}_{j+2} | \mathbf{x}_{j+3} \rangle \leqslant C_{j+2,j+3}\}.$$

6) Для $j = 1, 5$

$$L_{j,j+1,j+2,j+3} = \{(\mathbf{x}_j, \mathbf{x}_{j+1}, \mathbf{x}_{j+2}, \mathbf{x}_{j+3}) \in L_j \times L_{j+1}(x_j) \times L_{j+2,j+3}(\mathbf{x}_j, \mathbf{x}_{j+1})\}.$$

Алгоритм 2. FAS для 8-просеивания

Вход: списки $L_1, \ldots, L_8$ равномерно распределённых на сфере единичного радиуса векторов, $|L_1| = \ldots = |L_8|$; конфигурация $C \in \mathbb{R}^{8\times 8}$, такая, что $C_{12} = C_{13} = C_{14} = C_{56} = C_{57} = C_{58}$, $C_{23} = C_{24} = C_{67} = C_{68}$, $C_{34} = C_{78}$ и $C_{15} = C_{16} = C_{17} = C_{18} = C_{25} = C_{26} = C_{27} = C_{28} = C_{35} = C_{36} = C_{37} = C_{38} = C_{45} = C_{46} = C_{47} = C_{48}$.

Выход: список L_{out} всех кортежей $(\mathbf{x}_1, \ldots, \mathbf{x}_8) \in L_1 \times \ldots \times L_8$, удовлетворяющих конфигурации C.

Для $j = 1, 5$:
  $L_{j,j+1,j+2,j+3} := \varnothing$.
  Построить списки $L_{j,j+1}, L_{j,j+2}$ и $L_{j,j+3}$, используя алгоритм 2-просеивания, из которых можно восстановить списки $L_{j+1}(\mathbf{x}_j), L_{j+2}(\mathbf{x}_j)$ и $L_{j+3}(\mathbf{x}_j)$.
  Для $\mathbf{x}_j \in L_j$:
    Построить списки $L_{j+1,j+2}(\mathbf{x}_j)$ и $L_{j+1,j+3}(\mathbf{x}_j)$, используя алгоритм 2-просеивания, из которых можно восстановить списки $L_{j+2}(\mathbf{x}_j, \mathbf{x}_{j+1})$ и $L_{j+3}(\mathbf{x}_j, \mathbf{x}_{j+1})$.
    Для $\mathbf{x}_{j+1} \in L_{j+1}(\mathbf{x}_j)$:
      Построить список $L_{j+2,j+3}(\mathbf{x}_j, \mathbf{x}_{j+1})$, используя алгоритм 2-просеивания.
      Для $(\mathbf{x}_{j+2}, \mathbf{x}_{j+3}) \in L_{j+2,j+3}(\mathbf{x}_j, \mathbf{x}_{j+1})$:
        $L_{j,j+1,j+2,j+3} = L_{j,j+1,j+2,j+3} \cup \{(\mathbf{x}_j, \mathbf{x}_{j+1}, \mathbf{x}_{j+2}, \mathbf{x}_{j+3})\}$.
Построить список L_{out}, используя алгоритм 2-просеивания для списков L_{1234} и L_{5678}.
Вернуть L_{out}.

Для алгоритма 2 получены выражения для времени работы и количества используемой памяти.

Теорема 1. Пусть $\mathcal{V}(\alpha) = \dfrac{1}{|L_1|}$, $Y = \dfrac{1}{\sin^2(\alpha)(8 + 12C_{12} + 8C_{23} + 4C_{34})} - 1$, $Y_{23} = \dfrac{C_{23} - C_{12}^2}{(1 - C_{12}^2)}$, $Y_{234} = \dfrac{C_{34} - C_{12}^2 - (1 - C_{12}^2)Y_{23}}{1 - C_{12}^2 - (1 - C_{12}^2)Y_{23}^2}$. Тогда время выполнения алгоритма 2 равно $T = 6T_{12} + 4T_{123} + 2T_{1234} + T_{12345678}$, где

$$T_{12} = \mathcal{O}\left(|L_1|^2 \frac{(1 - C_{12}^2)^{n/2}}{(1 - C'_{12}(\alpha)^2)^{n/2}}\right), \quad L_{12} = |L_1|^2(1 - C_{12}^2)^{n/2},$$

$$T_{123} = \mathcal{O}\left(|L_1||L_2(\mathbf{x}_1)|^2 \frac{(1 - Y_{23}^2)^{n/2}}{(1 - Y_{23}'^2)^{n/2}}\right), \quad L_{123} = |L_1||L_2(\mathbf{x}_1)|^2(1 - Y_{23}^2)^{n/2},$$

$$T_{1234} = \mathcal{O}\left(|L_1||L_2(\mathbf{x}_1)||L_3(\mathbf{x}_1, \mathbf{x}_2)|^2 \frac{(1 - Y_{234}^2)^{n/2}}{(1 - Y'_{234}(\alpha)^2)^{n/2}}\right),$$

$$L_{1234} = |L_1||L_2(\mathbf{x}_1)||L_3(\mathbf{x}_1, \mathbf{x}_2)|^2(1 - Y_{234}^2)^{n/2},$$

$$T_{12345678} = \mathcal{O}\left(|L_{1234}|^2 \frac{(1 - Y^2)^{n/2}}{(1 - Y'(\alpha)^2)^{n/2}}\right), \quad L_{12345678} = |L_{1234}|^2(1 - Y^2)^{n/2}.$$

Количество памяти, используемой алгоритмом, равно

$$M = \max\left\{|L_1|, |L_{12}|, |L_{123}|, |L_{1234}|, |L_{12345678}|\right\}.$$

Для получения численных значений (рис. 1) времени работы и количества используемой памяти алгоритма 8-просеивания с внутренним алгоритмом FAS написана программа на языке Sage, реализующая минимизацию для конфигурации C и угла α.

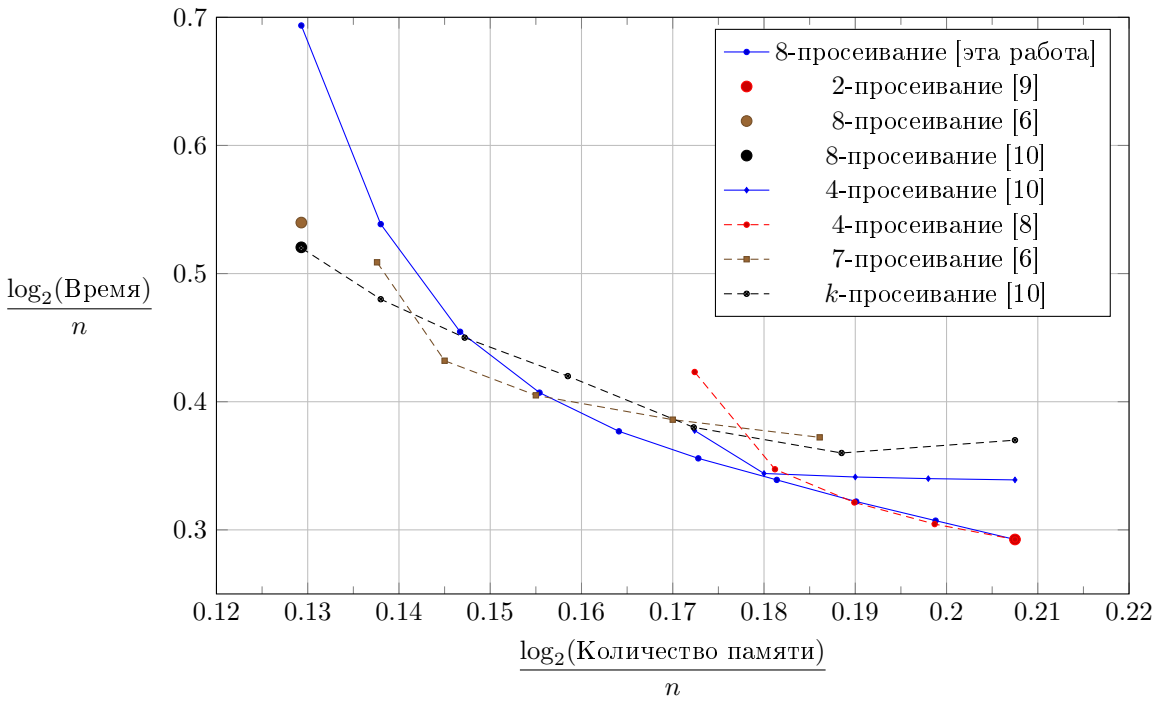

Рис. 1. Компромисс для алгоритма 8-просеивания

При количестве используемой памяти $2^{0,2075n}$ предлагаемый алгоритм совпадает по времени работы и объёму памяти с алгоритмом из [9], который является оптимальным

по времени работы алгоритмом, известным на сегодняшний день. Для объёма памяти, близкого к минимальным значениям, предлагаемый алгоритм работает дольше, что совпадает с поведением алгоритма 4-просеивания [8], построенном на концепции из алгоритма 1. Для объёма памяти из отрезка $(2^{0{,}157n}, 2^{0{,}189n})$ предложенный алгоритм показывает минимальное время работы из известных алгоритмов k-просеивания.

ЛИТЕРАТУРА

1. *Kannan R.* Improved algorithms for integer programming and related lattice problems // Proc. 15th Ann. ACM Symp. Theory Comput. Boston, Massachusetts, USA, April 25–27, 1983. N.Y.: ACM, 1983. P. 193–206.
2. *Fincke U. and Pohst M.* Improved methods for calculating vectors of short length in a lattice, including a complexity analysis // Math. Comput. 1985. V. 44. No. 170. P. 463–471.
3. *Ajtai M., Kumar R., and Sivakumar D.* A sieve algorithm for the shortest lattice vector problem // Proc. 33rd Ann. ACM Symp. Theory Comput. Hersonissos, Greece, July 6–8, 2001. N.Y.: ACM, 2001. P. 601–610.
4. *Nguyen P. Q. and Vidick T.* Sieve algorithms for the shortest vector problem are practical // J. Math. Cryptol. 2008. V. 2. No. 2. P. 181–207.
5. *Bai S., Laarhoven T., and Stehlé D.* Tuple lattice sieving // LMS J. Comput. Math. 2016. V. 19. No. A. P. 146–162.
6. *Herold G. and Kirshanova E.* Improved algorithms for the approximate k-list problem in Euclidean norm // LNCS. 2017. V. 10174. P. 16–40.
7. *Becker A., Ducas L., Gama G., and Laarhoven T.* New directions in nearest neighbor searching with applications to lattice sieving // Proc. 27th Ann. ACM-SIAM Symp. Discrete Algorithms. Arlington, VA, USA, Jan. 10–12, 2016. Philadelphia, PA: SIAM, 2016. P. 10–24.
8. *Chailloux A. and Loyer J.* Classical and quantum 3 and 4-sieves to solve SVP with low memory // LNCS. 2023. V. 14154. P. 225–255.
9. *Laarhoven T.* Search Problems in Cryptography, From Fingerprinting to Lattice Sieving. Ph.D. Thesis. Eindhoven University of Technology, 2016.
10. *Herold G., Kirshanova E., and Laarhoven T.* Speed-ups and time–memory trade-offs for tuple lattice sieving // LNCS. 2018. V. 10769. P. 407–436.
11. *Ajtai M.* The shortest vector problem in L_2 is NP-hard for randomized reductions (extended abstract) // Proc. 30th Ann. ACM Symp. Theory Comput. Dallas, Texas, USA, May 24–26, 1998. N.Y.: ACM, 1998. P. 10–19.
12. *Klein P.* Finding the closest lattice vector when it's unusually close // Proc. 11th Ann. ACM-SIAM Symp. Discrete Algorithms. San Francisco, California, USA, Jan. 9–11, 2000. Philadelphia, PA: SIAM, 2000. P. 937–941.
13. `https://latticechallenge.org/svp-challenge`.

УДК 004.056.55 DOI 10.17223/2226308X/17/42

ОПТИМИЗАЦИЯ МОДУЛЬНОЙ АРИФМЕТИКИ В МЕХАНИЗМЕ ИНКАПСУЛЯЦИИ КЛЮЧА KYBER

А. С. Зеленецкий, П. Г. Ключарев

Kyber представляет собой постквантовый механизм инкапсуляции ключа (Key Encapsulation Mechanism, KEM). Более того, на текущий момент Kyber является единственным постквантовым KEM, рекомендованным к стандартизации в США по итогам конкурса, проводимого NIST (National Institute of Standards and Technology). Предлагается алгоритмическая оптимизация модульной арифме-

тики, используемой в Kyber, который значительно снижает количество операций приведения по модулю. Предложенная оптимизация позволяет достичь ускорения декапсуляции ключа в 1,83 раз, инкапсуляции ключа — в 1,58 раз и генерации ключевой пары — в 1,41 раз для программной реализации Kyber.

Ключевые слова: *Kyber, модульная арифметика, постквантовая криптография, криптография на решётках.*

Введение

Kyber [1] является постквантовым механизмом инкапсуляции ключа, рекомендованным к стандартизации в США по итогам третьего раунда конкурса NIST. Kyber относится к криптографии на решётках, то есть его стойкость основывается на сложности решения определённых задач из теории алгебраических решёток, а именно: стойкость Kyber обосновывается сложностью задачи Module Learning With Errors (MLWE) [2]. Как и любой другой KEM, Kyber состоит из трёх основных алгоритмов: генерации ключевой пары, инкапсуляции ключа и декапсуляции ключа. В силу того, что постквантовая криптография в сравнении с классической является гораздо более требовательной к ресурсам, возникает серьёзная потребность в оптимизации существующих постквантовых решений. В работе предлагается способ алгоритмической оптимизации модульной арифметики, используемой в Kyber. Наш подход позволяет одновременно ускорить все три алгоритма, составляющих Kyber.

1. Арифметика в Kyber KEM

Основным математическим объектом в Kyber выступает кольцо $R_q = \mathbb{Z}_q[x]/(x^n+1)$, где $q = 3329$ — простое, а $n = 256$ для всех наборов параметров. Единственными арифметическими операциями в Kyber являются операции умножения и сложения элементов R_q. Сложение полиномов из R_q покоординатное, поэтому требуется реализовать сложение элементов по модулю q. Умножение в R_q является более сложной операцией, в Kyber оно реализуется через использование теоретико-числового преобразования (Number-Theoretic Transform, NTT) [3] — аналога дискретного преобразования Фурье над конечным полем для кольца R_q. Использование NTT позволяет представить многочлены кольца R_q в таком виде, что для подсчёта их произведения достаточно произвести обычное поокординатное умножение. Для определения NTT-представления используется следующее представление кольца R_q:

$$\mathbb{Z}_q[x]/(x^n+1) \cong \prod_{i=0}^{127} \mathbb{Z}_q[x]/(x^2-\zeta^{2i+1}),$$

где ζ — некоторый примитивный корень 256-й степени из единицы в поле $\mathbb{Z}_q$, в Kyber в качестве ζ используется 17. Таким образом, любой элемент $a(x) \in R_q$ представляется единственным образом в виде вектора $\big(a(x) \bmod (x^2-\zeta), a(x) \bmod (x^2-\zeta^3), \ldots, a(x) \bmod (x^2-\zeta^{255})\big)$ длины 128, координатами которого являются линейные многочлены над полем $\mathbb{Z}_q$. Этот вектор (с точностью до перестановки координат) является NTT-представлением элемента $a(x)$. Наивный алгоритм вычисления $\mathrm{NTT}(a(x))$ имеет сложность $O(n^2)$, такую же сложность имеет и наивный алгоритм получения многочлена $a(x)$ по известному $\mathrm{NTT}(a(x))$, то есть алгоритм вычисления обратного теоретико-числового преобразования, который для краткости будем называть INVNTT. Однако в Kyber используется более быстрый алгоритм [4] как для вычисления NTT, так и для вычисления INVNTT. Оба алгоритма имеют сложность $O(n \log n)$. Единственными арифметическими операциями в этих алгоритмах являются операции сложения

и умножения в поле $\mathbb{Z}_q$. Очевидно, что произведение многочленов, заданных своими NTT-представлениями, вычисляется также с помощью только сложения и умножения по модулю q. Таким образом, единственными арифметическими операциями, использующимися для реализации арифметики в Kyber, являются сложение и умножение по модулю q.

Для реализации модульной арифметики в референсной реализации Kyber применяются алгоритмы Монтгомери [5] и Барретта [6]. Сама референсная реализация выложена на GitHub и доступна по ссылке[1]. Элементы поля $\mathbb{Z}_q$ представлены целыми числами из интервала $(-q/2, q/2)$, а для их хранения используются 16-битные знаковые целые числа. Как обычно, алгоритм Монтгомери выполняет умножение по модулю q, а алгоритм Барретта — приведение по модулю, как правило, после нескольких операций сложения. Это позволяет реализовать модульную арифметику при помощи только умножения и сложения целых чисел, а также битового сдвига. Все перечисленные операции являются константными по времени, то есть время их выполнения зависит только от длины входных данных, а не от самих данных. Данное условие необходимо для реализации, устойчивой к атакам по времени.

2. Предлагаемая оптимизация

Основная идея предлагаемого подхода — хранить элементы поля $\mathbb{Z}_q$ в 32-битных целых числах. Заметим, что результат умножения двух чисел из $\mathbb{Z}_q$ помещается в 24 бита. Алгоритмы Kyber таковы, что в них не происходит несколько умножений многочленов подряд, а именно: умножение многочленов производится только при вычислении скалярных произведений вида $\langle \mathbf{a}, \mathbf{s} \rangle$, где $\mathbf{a}, \mathbf{s}$ — векторы, коэффициентами которых выступают многочлены из R_q. Причём результаты таких скалярных произведений не задействованы далее в других умножениях. Поэтому увеличение размеров представлений элементов из $\mathbb{Z}_q$ в битах позволяет избавиться от использования алгоритма Монтгомери для реализации умножения по модулю q, а также от необходимости осуществления переходов между представлением Монтгомери и обычным представлением вычета по модулю q. Длина векторов $\mathbf{a}, \mathbf{s}$ не превосходит 4, поэтому скалярное умножение может быть выполнено без использования промежуточных сведений по модулю. Для приведения окончательного результата по модулю q применяется алгоритм Барретта. В результате мы, как и авторы референсной реализации, используем для реализации модульной арифметики в Kyber исключительно операции целочисленного умножения и сложения совместно с битовыми сдвигами. Это гарантирует константность по времени (в смысле атак по времени) для всех арифметических операций.

В табл. 1–3 приведено сравнение алгоритмов, связанных с умножением многочленов в R_q, референсной реализации с аналогичными операциями, использующими предложенную оптимизацию, по числу выполняемых элементарных действий.

Таблица 1

Сравнение алгоритмов умножения многочленов

Версия алгоритма	Число умножений	Число сложений	Число битовых сдвигов
Оригинальный	1920	896	640
Предлагаемый	896	512	128

[1] `https://github.com/pq-crystals/kyber`

Таблица 2

Сравнение алгоритмов INVNTT

Версия алгоритма	Число умножений	Число сложений	Число битовых сдвигов
Оригинальный	5248	4736	2048
Предлагаемый	3456	4096	1152

Таблица 3

Сравнение алгоритмов NTT

Версия алгоритма	Число умножений	Число сложений	Число битовых сдвигов
Оригинальный	3200	3200	1152
Предлагаемый	3200	4096	1152

Для первых двух алгоритмов достигнуто существенное сокращение количества всех элементарных операций. Для алгоритма, вычисляющего NTT, такого результата достичь не удалось. Однако легко заметить, что алгоритм, использующий нашу реализацию модульной арифметики, не намного затратнее оригинального и выигрыш, получаемый в других двух алгоритмах, значительно превышает проигрыш алгоритма вычисления NTT.

Проведено также измерение времени выполнения основных алгоритмов Kyber KEM для референсной реализации и реализации, использующей оптимизацию. Измерения проведены для трёх основных наборов параметров Kyber: Kyber512, Kyber768 и Kyber1024. В качестве тестов скорости использовались тесты, предоставленные разработчиками Kyber, они могут быть найдены по ссылке[2]. Все измерения проводились с использованием одного ядра процессора Apple M1 и 8 Гбайт RAM. Обе реализации были скомпилированы с помощью gcc версии 13.2.0 с флагами, указанными в Makefile для референсной реализации. Результаты представлены в табл. 4–6. Оптимизированная реализация также выложена на GitHub и доступна по ссылке[3].

Таблица 4

Время работы алгоритмов Kyber для параметров Kyber512

Реализация	Генерация ключей, нс	Инкапсуляция, нс	Декапсуляция, нс
Референсная	20750	24291	28083
Предлагаемая	16708	16083	15333

Таблица 5

Время работы алгоритмов Kyber для параметров Kyber768

Реализация	Генерация ключей, нс	Инкапсуляция, нс	Декапсуляция, нс
Референсная	33125	37375	42625
Предлагаемая	23916	23625	23333

[2] `https://github.com/pq-crystals/kyber/blob/main/ref/test_speed.c`

[3] `https://github.com/azelenetskiy/Kyber_arithmetic_optimization`

Таблица 6

Время работы алгоритмов Kyber для параметров Kyber1024

Реализация	Генерация ключей, нс	Инкапсуляция, нс	Декапсуляция, нс
Референсная	50792	54333	61000
Предлагаемая	35917	35208	35250

Заключение

Предложена оптимизация модульной арифметики для Kyber KEM, которая существенно повышает производительность составляющих его алгоритмови при программной реализации, а именно: удаётся достичь ускорения декапсуляции ключа максимум в 1,83 раз, инкапсуляции ключа — в 1,58 раз и генерации ключевой пары — в 1,41 раз. Основная идея оптимизации состоит в выделении большей памяти под хранение чисел по модулю q, что позволяет сократить число приведений по модулю. Используемый подход эксплуатирует малый размер модуля q и особенности арифметики схемы Kyber. Для многих других криптографических схем, стойкость которых основана на вычислительной сложности задачи LWE и её вариаций, данный подход также может принести результаты.

ЛИТЕРАТУРА

1. *Bos J., Ducas L., Kiltz E., et al.* CRYSTALS — Kyber: a CCA-secure Module-Lattice-Based KEM. `https://eprint.iacr.org/2017/634.pdf`. 2017.
2. *Langlois A. and Stehle D.* Worst-case to average-case reductions for module lattices // Des. Codes Cryptogr. 2015. No. 3. P. 565–599.
3. *Liang Z. and Zhao Y.* Number Theoretic Transform and its Applications in Lattice-based Cryptosystems: A Survey. `https://doi.org/10.48550/arXiv.2211.13546`.
4. *Chung C.-M. M., Hwangt V., Kannwischer M. J., et al.* NTT multiplication for NTT-unfriendly rings: New speed records for Saber and NTRU on Cortex-M4 and AVX2 // IACR Trans. Cryptogr. Hardware Embedded Systems. 2021. No. 2. P. 159–188.
5. *Montgomery P. L.* Modular multiplication without trial division // Math. Comput. 1985. No. 44. P. 519–521.
6. *Barrett P.* Implementing the Rivest Shamir and Adleman public key encryption algorithm on a standard digital signal processor // LNCS. 1987. V. 263.P. 311–323.

СВЕДЕНИЯ ОБ АВТОРАХ

АБРОСИМОВ Михаил Борисович — доктор физико-математических наук, доцент, заведующий кафедрой теоретических основ компьютерной безопасности и криптографии Саратовского национального исследовательского государственного университета имени Н. Г. Чернышевского, г. Саратов.
E-mail: **mic@rambler.ru**

АЛЕКСЕЕВ Евгений Константинович — кандидат физико-математических наук, начальник отдела криптографических исследований ООО «КРИПТО-ПРО», г. Москва.
E-mail: **alekseev@cryptopro.ru**

АНАНИЧЕВ Дмитрий Сергеевич — кандидат физико-математических наук, доцент, доцент Уральского федерального университета, г. Екатеринбург. E-mail: **ananichev.dima@mail.ru**

АНТОНОВ Кирилл Валентинович — ассистент ИИКС НИЯУ МИФИ, г. Москва.
E-mail: **KVAntonov@mephi.ru**

БАХАРЕВ Александр Олегович — младший специалист-исследователь АО «НПК «Криптонит», студент Новосибирского государственного университета, г. Новосибирск.
E-mail: **a.bakharev@kryptonite.ru**

БЕЗЗАТЕЕВ Сергей Валентинович — доктор технических наук, доцент, заведующий кафедрой Санкт-Петербургского государственного университета аэрокосмического приборостроения, г. Санкт-Петербург. E-mail: **bsv@guap.ru**

БОБРОВСКИЙ Дмитрий Александрович — ведущий системный аналитик ООО «Код Безопасности», г. Москва. E-mail: **d.bobrovskiy@securitycode.ru**

БОЛОТНИКОВА Алина Дмитриевна — студентка Сибирского федерального университета, г. Красноярск. E-mail: **lybimka.811@gmail.com**

БУГРОВ Алексей Дмитриевич — кандидат физико-математических наук, доцент кафедры РТУ МИРЭА, г. Москва. E-mail: **bugrovalexey1@yandex.ru**

БЫКОВ Денис Александрович — студент Новосибирского государственного университета, г. Новосибирск. E-mail: **den.bykov.2000i@gmail.com**

ГАРЧУКОВА Полина Романовна — студентка Национального исследовательского Томского государственного университета, г. Томск. E-mail: **polina.garchukova@mail.ru**

ГЕУТ Кристина Леонидовна — старший преподаватель Уральского государственного университета путей сообщения, г. Екатеринбург. E-mail: **geutkrl@yandex.ru**

ГЛУХОВ Михаил Михайлович — кандидат физико-математических наук, доцент, РТУ МИРЭА, г. Москва. E-mail: **glukhovmm@rambler.ru**

ДЕНИСОВ Олег Викторович — кандидат физико-математических наук, доцент, ООО «Инновационные телекоммуникационные технологии», г. Москва. E-mail: **DenisovOleg@yandex.ru**

ЕГОРУШКИН Олег Игоревич — кандидат физико-математических наук, доцент Сибирского государственного университета науки и технологий имени академика М. Ф. Решетнёва, г. Красноярск.
E-mail: **olegegoruschkin@yandex.ru**

ЖАРКОВА Анастасия Владимировна — кандидат физико-математических наук, доцент, доцент кафедры теоретических основ компьютерной безопасности и криптографии Саратовского национального исследовательского государственного университета имени Н. Г. Чернышевского, г. Саратов.
E-mail: **ZharkovaAV3@gmail.com**

ЗАИКИН Олег Сергеевич — кандидат технических наук, ведущий научный сотрудник Математического центра в Академгородке, г. Новосибирск, ведущий сотрудник ИДСТУ СО РАН, г. Иркутск.
E-mail: **oleg.zaikin@icc.ru**

ЗЕЛЕНЕЦКИЙ Алексей Сергеевич — криптограф-исследователь ООО «КуАпп», ассистент кафедры ИУ8 МГТУ им. Н. Э. Баумана, г. Москва. E-mail: **azelenetskiy@qapp.tech**

КАЗАНЦЕВ Сергей Юрьевич — доктор физико-математических наук, заведующий сектором КРК в проводных и беспроводных линиях связи Квантового центра, профессор кафедры направляющих телекоммуникационных сред МТУСИ, г. Москва. E-mail: **s.i.kazantsev@mtuci.ru**

КАЛИНИН Юрий Сергеевич — ФУМО ВО ИБ, г. Москва. E-mail: **shzikarev1703@gmail.com**

КАМЛОВСКИЙ Олег Витальевич — доктор физико-математических наук, доцент кафедры теории вероятностей и прикладной математики МТУСИ, г. Москва. E-mail: **ov-kam@yandex.ru**

КЛЮЧАРЕВ Петр Георгиевич — доктор технических наук, профессор кафедры ИУ8 МГТУ им. Н. Э. Баумана. E-mail: **pk.iu8@yandex.ru**

КОЛБАСИНА Ирина Валерьевна — старший преподаватель Сибирского государственного университета науки и технологий имени академика М. Ф. Решетнёва, г. Красноярск.
E-mail: **kabaskina@yandex.ru**

КОЛЕСНИКОВ Сергей Геннадьевич — доктор физико-математических наук, доцент, профессор Сибирского федерального университета, профессор Сибирского государственного университета науки и технологий, г. Красноярск. E-mail: **sklsnkv@mail.ru**

КОЛОМЕЕЦ Николай Александрович — кандидат физико-математических наук, научный сотрудник Института математики им. С. Л. Соболева СО РАН, г. Новосибирск.
E-mail: **kolomeec@math.nsc.ru**

КОМЯГИН Максим Михайлович — эксперт НКО «Фонд содействия развитию безопасных информационных технологий», г. Москва. E-mail: **komyagin.mm@mail.ru**

КОНДЫРЕВ Дмитрий Олегович — младший научный сотрудник Математического центра в Академгородке, г. Новосибирск. E-mail: **dkondyrev@gmail.com**

КОРЕНЕВА Алиса Михайловна — кандидат физико-математических наук, начальник отдела криптографического анализа ООО «Код Безопасности», доцент кафедры информационной безопасности Финансового университета при Правительстве РФ, г. Москва.
E-mail: **A.Koreneva@securitycode.ru**

КРУГЛОВ Василий Игоревич — кандидат физико-математических наук, научный сотрудник Математического института им. В. А. Стеклова РАН, г. Москва. E-mail: **kruglov@mi-ras.ru**

КУНИНЕЦ Артем Андреевич — студент специальности «Компьютерная безопасность» ОНК «Институт высоких технологий» БФУ им. И. Канта, г. Калининград.
E-mail: **artkuninets@yandex.ru**

КУЦЕНКО Александр Владимирович — кандидат физико-математических наук, старший преподаватель механико-математического факультета Новосибирского государственного университета, г. Новосибирск. E-mail: **alexandrkutsenko@bk.ru**

КЯЖИН Сергей Николаевич — кандидат физико-математических наук, ведущий инженер-аналитик ООО «КРИПТО-ПРО», г. Москва. E-mail: **kyazhin@cryptopro.ru**

ЛЕБЕДЕВ Роман Константинович — старший преподаватель Новосибирского государственного университета, г. Новосибирск. E-mail: **n0n3m4@gmail.com**

ЛЕОНТЬЕВ Владимир Маркович — аспирант Сибирского федерального университета, г. Красноярск. E-mail: **v.m.leontiev@outlook.com**

МЕДВЕДЕВА Наталья Валерьевна — кандидат физико-математических наук, доцент, доцент кафедры Уральского государственного университета путей сообщения, г. Екатеринбург.
E-mail: **medvedeva_n_v@mail.ru**

МИЗЕРОВ Виктор Владимирович — доктор физико-математических наук, ведущий научный сотрудник ООО «Центр сертификационных исследований», г. Москва. E-mail: **ov-kam02@yandex.ru**

НОВОСЕЛОВ Семен Александрович — кандидат физико-математических наук, младший научный сотрудник лаборатории математических методов защиты информации Северо-Западного центра математических исследований имени С. Ковалевской, г. Калининград.
E-mail: **novsem@gmail.com**

ОТПУЩЕННИКОВ Илья Владимирович — кандидат технических наук, научный сотрудник ИДСТУ СО РАН, г. Иркутск. E-mail: **otilya@yandex.ru**

ПАВЛЕНКО Артём Леонидович — аспирант Университета ИТМО, г. Санкт-Петербург. E-mail: **alpavlenko@itmo.ru**

ПАНАСЕНКО Сергей Петрович — кандидат технических наук, директор по научной работе компании «Актив», г. Москва. E-mail: **panasenko@guardant.ru**

ПАНКОВ Константин Николаевич — кандидат физико-математических наук, доцент, ведущий научный сотрудник НИЛ-24, заведующий сектором постквантовой криптографии Квантового центра, заведующий кафедрой теории вероятностей и прикладной математики Московского технического университета связи и информатики, эксперт ТК-159 и ТК-362, г. Москва. E-mail: **pankov_kn@mtuci.ru**

ПАНКРАТОВА Ирина Анатольевна — кандидат физико-математических наук, доцент, заведующая лабораторией компьютерной криптографии Национального исследовательского Томского государственного университета, г. Томск. E-mail: **pank@mail.tsu.ru**

ПОГОРЕЛОВ Борис Александрович — доктор физико-математических наук, профессор, действительный член Академии криптографии Российской Федерации, г. Москва.

ПОЛЯКОВ Михаил Вадимович — старший аналитик отдела криптографического анализа ООО «Код Безопасности», старший преподаватель кафедры ИУ-8 «Информационная безопасность» МГТУ им. Н. Э. Баумана, г. Москва. E-mail: **M.Polyakov@securitycode.ru**

ПРУДНИКОВ Егор Сергеевич — студент Национального исследовательского Томского государственного университета, г. Томск. E-mail: **egorprudnikov71@gmail.com**

ПУДОВКИНА Марина Александровна — доктор физико-математических наук, профессор кафедры криптографии и безопасности компьютерных систем НИЯУ МИФИ, г. Москва. E-mail: **maricap@rambler.ru**

РАМОДАНОВ Сергей Михайлович — доктор физико-математических наук, доцент, ведущий научный сотрудник лаборатории прецизионной оптомехатроники МФТИ, г. Москва. E-mail: **ramodanov.sm@mipt.ru**

САФОНОВ Константин Владимирович — доктор физико-математических наук, профессор, заведующий кафедрой Сибирского государственного университета науки и технологий имени академика М. Ф. Решетнёва, г. Красноярск. E-mail: **safonovkv@rambler.ru**

СЕМЁНОВ Александр Анатольевич — кандидат технических наук, ведущий научный сотрудник ИДСТУ СО РАН, г. Иркутск. E-mail: **biclop.rambler@yandex.ru**

СЕМЁНОВ Артём Иванович — студент Сибирского государственного университета науки и технологий, г. Красноярск. E-mail: **art25sem12i2000@yandex.ru**

СИТНОВ Владимир Евгеньевич — аспирант Новосибирского государственного университета, г. Новосибирск. E-mail: **vladimirsitnov@gmail.com**

СМИРНОВ Антон Михайлович — аспирант кафедры криптографии и безопасности компьютерных систем НИЯУ МИФИ, г. Москва. E-mail: **amsmirnov@mephi.ru**

СОРОКОУМОВА Алена Дмитриевна — студентка Национального исследовательского Томского государственного университета, г. Томск. E-mail: **a.srkmva@mail.ru**

ТИТОВ Сергей Сергеевич — доктор физико-математических наук, профессор, профессор кафедры Уральского государственного университета путей сообщения, г. Екатеринбург. E-mail: **stitov@usaaa.ru**

ТОКАРЕВА Наталья Николаевна — доцент Новосибирского государственного университета, г. Новосибирск. E-mail: **crypto1127@mail.ru**

ТОМИЛОВ Дмитрий Александрович — аспирант Саратовского национального исследовательского государственного университета имени Н. Г. Чернышевского, г. Саратов. E-mail: **tomilov.d.a@mail.ru**

ТУРЧЕНКО Олег Юрьевич — кандидат технических наук, исследователь-криптограф ООО «КуАпп», г. Москва. E-mail: **oturchenko@qapp.tech**
УСМАНОВ Сергей Равильевич — разработчик-алгоритмист ООО «Куборд», г. Москва.
E-mail: **s.usmanov@rqc.ru**
ФИРСОВ Георгий Валентинович — руководитель группы разработки ООО «Код Безопасности», аспирант кафедры криптологии и кибербезопасности НИЯУ МИФИ, г. Москва.
E-mail: **G.Firsov@securitycode.ru**
ХИЛЬЧУК Ирина Сергеевна — ассистент механико-математического факультета Новосибирского государственного университета, аспирантка Новосибирского государственного университета, г. Новосибирск. E-mail: **irina.khilchuk@gmail.com**
ЦАРЕГОРОДЦЕВ Кирилл Денисович — старший специалист-исследователь АО «НПК «Криптонит», г. Москва. E-mail: **k.tsaregorodtsev@kryptonite.ru**
ЧЕЖЕГОВА Полина Алексеевна — студентка кафедры информационной безопасности Финансового университета при Правительстве РФ, г. Москва. E-mail: **ChezhegovaPA@gmail.com**
ЧЕРЕМУШКИН Александр Васильевич — доктор физико-математических наук, профессор, академик Академии криптографии Российской Федерации, г. Москва. E-mail: **avc238@mail.ru**
ШАБАРКОВА Александра Олеговна — аспирантка Саратовского национального исследовательского государственного университета имени Н. Г. Чернышевского, г. Саратов.
E-mail: **shabarkova_alex.andra@mail.ru**
ШИЛИКОВ Дмитрий Александрович — студент Финансового университета при Правительстве РФ, стажёр отдела криптографического анализа ООО «Код Безопасности», г. Москва.
E-mail: **d.shilikov@securitycode.ru**

АННОТАЦИИ ДОКЛАДОВ НА АНГЛИЙСКОМ ЯЗЫКЕ

SECTION 1

Komyagin M. M. **ISOMORPHISMS OF 5-CONFIGURATIONS OBTAINED FROM 2-DIGRAPHS.** We consider 5-configurations defined by their incident matrices over the field GF(2), which must be nonsingular and contain exactly 5 units in each row and each column, and the inverse matrix must also have this property. Automorphisms of 5-configurations are studied. The relationship is shown between the group of automorphisms of an oriented graph without loops and parallel arcs with two input and two output arcs at each vertex and the group of automorphisms of the 5-configuration obtained from this digraph.

Keywords: *k-configurations, k-matrices, digraphs, group of automorphisms.*

Kruglov V. I. **EXACT FORMULA FOR EXPECTATION OF NUMBER OF PAIRS OF COINCIDING S-CHAINS IN A RANDOM BINARY SEQUENCE WITH FIXED NUMBER OF ZEROES AND ONES.** We consider all possible binary sequences $X = (X_1, X_2, \ldots, X_{a+b})$ of length $a + b$ consisting of a ones and b zeroes. For each such a sequence, we count the number of pairs of its subsequences of a given length s (so called s-chains) that have coinciding values of their elements. Assuming all these sequences X to be equiprobable, we propose exact formula for expectation of number of pairs of coinciding s-chains. For any s, $s < a$ and $s < b$, and any i, $1 \leqslant i \leqslant a+b-s+1$, consider s-chain $Y_i = (X_i, \ldots, X_{i+s-1})$ and event $E_{ij} = \{Y_i = Y_j\}$. Let $\eta_{ij} = \mathbb{I}(E_{ij})$ be the indicator of this event, then the number of pairs of coinciding s-chains in the sequence X is equal to the random variable $\xi = \sum\limits_{1 \leqslant i < j \leqslant a+b-s+1} \eta_{ij}$. For any $r_a \leqslant a$ and $r_b \leqslant b$ denote by $p_{r_a,r_b} = \mathrm{C}_{a+b-r_a-r_b}^{a-r_a} / \mathrm{C}_{a+b}^{a}$ the probability that in sequence X on fixed r_a positions there are ones and on fixed r_b positions are zeroes. For any k such that $1 \leqslant k \leqslant s-1$, we define the values $n = \lfloor s/k \rfloor$, $m = s - kn$, and the function

$$f(k) = \sum_{t_1=0}^{m} \sum_{t_2=0}^{k-m} \mathrm{C}_m^{t_1} \mathrm{C}_{k-m}^{t_2} p_{t_1(n+2)+t_2(n+1),(m-t_1)(n+2)+(k-m-t_2)(n+1)}.$$

Then for the expectation of ξ we obtain the formula

$$\mathsf{E}\xi = \frac{\mathrm{C}_{a+b-2s+2}^{2}}{\mathrm{C}_{a+b}^{a}} \sum_{r=0}^{s} \mathrm{C}_s^r \mathrm{C}_{a+b-2s}^{a-2r} + \sum_{i=1}^{a+b-2s+2} \sum_{k=1}^{s-1} f(k) + \sum_{i=a+b-2s+3}^{a+b-s} \sum_{k=1}^{a+b-s+1-i} f(k).$$

Keywords: *repetitions of s-chains, expectation, urn scheme, exact formula.*

Novoselov S. A. **THE CHARACTERISTIC POLYNOMIALS OF GEOMETRICALLY SPLIT ORDINARY ABELIAN VARIETIES OF DIMENSION 3.** In the paper, we explicitly describe all possible characteristic polynomials of the Frobenius endomorphism for ordinary geometrically decomposable Abelian varieties of dimension 3 over a finite field. These polynomials encode many arithmetic properties of abelian varieties including number of points. More precisely, if $\chi_{A,q}(T)$ is the characteristic polynomial of the Frobenius endomorphism on A over $\mathbb{F}_q$, then the number of points on A is equal to $\chi_{A,q}(1)$.

Keywords: *Abelian threefold, characteristic polynomial, point-counting, finite field.*

Pogorelov B. A., Pudovkina M. A. **ON PERMUTATIONS PERFECTLY DIFFUSING CLASSES OF PARTITIONS OF $V_n^l(2^m)$.** Let $V_n(2^m)$ be an n-dimensional vector space over $\mathbb{F}_{2^m}$ and $\overline{V}_n^l(2^m)$ consists of all pairwise different elements from the Cartesian product $V_n^l(2^m)$, $l, n, m \in \mathbb{N}$, $n, l \geqslant 2$. We consider permutations from the symmetrical group $S(V_n(2^m))$ acting coordinate-wise on vectors from $V_n^l(2^m)$, and partitions of $\overline{V}_n^l(2^m)$, which are generalizations of classical differential partitions ($l = 2$) and are used in high order differential, truncated differential, impossible differential, polytopic and multiple differential techniques. For a partition $\mathbf{W}^{(n,l)}$ of $\overline{V}_n^l(2^m)$, we study the minimum Hamming distance $\mathrm{d}_{\mathbf{W}^{(n,l)}}(s)$ between a permutation s and the set $\mathrm{IG}_{\mathbf{W}}$ consisting of all permutations from $S(V_n(2^m))$ preserving $\mathbf{W}^{(n,l)}$. We describe properties of permutations s with the maximum distance $\mathrm{d}_{\mathbf{W}^{(n,l)}}(s)$, which perfectly diffuse $\mathbf{W}^{(n,l)}$. We get a criterion of perfect diffusion of $\mathbf{W}^{(n,l)}$ for any $l \in \mathbb{N}$. We show the connection between permutations perfectly diffusing $\mathbf{W}$, APN-permutations, AB-permutations, and differentially $2r$-uniform permutations, $r \geqslant 1$.

Keywords: *perfect diffusion, imprimitive group, wreath product, differentially d-uniform permutation, APN-permutation, AB-permutation, differential technique, polytopic technique.*

Cheremushkin A. V. **MEDIAL AND PARAMEDIAL ALEBRAS WITH STRONG DEPENDABLE OPERATIONS.** We consider general functional medial and paramedial equations with four object variables. We give analogous results to those known for quasigroup operations for a class of strongly dependable operations. As a consequence of these results analogous linear representation for every operation of a binary algebra satisfying one of these hyperidentities is obtained.

Keywords: *n-ary quasigroup, strong dependant operation, medial and paramedial operations.*

SECTION 2

Bykov D. A., Kolomeec N. A. **ON THE NUMBER OF THE CLOSEST BENT FUNCTIONS TO SOME MAIORANA–MCFARLAND BENT FUNCTIONS.** We consider the numbers of bent functions that are closest to some bent functions from the Maiorana — McFarland class $\mathcal{M}_{2n}$, specifically, the numbers near to their lower $\ell_{2n} = 2^{2n+1} - 2^n$ and tight upper $\mathcal{L}_{2n}$ bounds. For a bent function $f(x, y) = \langle x, \sigma(y)\rangle \oplus \varphi(y) \in \mathcal{M}_{2n}$, where σ is a function based on the inverse function of elements of the finite field, the number of closest bent functions is calculated for identically zero φ. Moreover, it is shown that this number is less than $\ell_{2n} + 82(2^n - 1)$ and asymptotically equals to $\ell_{2n} + o(\ell_{2n})$ for some φ. An explicit formula for the number of bent functions closest to $f(x, y) = \langle x, y\rangle \oplus y_1 y_2 \dots y_m$, where $3 \leqslant m \leqslant n$, has been derived. The values for $m = 3$ and $m = n$ are equal to $o(\mathcal{L}_{2n})$ and $\frac{1}{3}\mathcal{L}_{2n} + o(\mathcal{L}_{2n})$ respectively as $n \to \infty$. A complete classification of $\mathcal{M}_6$ using the number of closest bent functions is obtained.

Keywords: *affine subspaces, bent functions, Maiorana — McFarland class, minimal distance, the closest functions.*

Kalinin Y. S. **RESEARCH OF BOOMERANG UNIFORMITY OF QUADRATIC PERMUTATIONS.** The boomerang attack, proposed in 1999, is a variation of the difference attack. Its advantage is that even in the presence of low differential uniformity the cipher can still be vulnerable to boomerang attack. This paper is devoted to such

a parameter of a vector Boolean function as boomerang uniformity, which characterizes the function's resistance to the boomerang attack. Quadratic permutations are considered and the dependence of the boomerang characteristic on the differential characteristic for this class has been studied. The main result is an expression connecting the boomerang uniformity of a function with the values of its DDT table and obtained using the matrix approach for working with quadratic functions, as well as the known properties of differential and boomerang characteristics In addition, for the boomerang characteristic, some constructions of quadratic substitutions in a small number of variables have been studied and other properties have been established.

Keywords: *vector Boolean function, quadratic permutation, differential uniformity, DDT-table, APN-function, boomerang attack, boomerang uniformity, BCT-table.*

Kolomeec N. A. **ON THE NUMBER OF FUNCTIONS THAT BREAK SUBSPACES OF DIMENSION 3 AND HIGHER.** We consider the sets $\mathcal{P}_n^k$ consisting of invertible functions $F : \mathbb{F}_2^n \to \mathbb{F}_2^n$ such that any $U \subseteq \mathbb{F}_2^n$ and its image $F(U)$ are not simultaneously k-dimensional affine subspaces of $\mathbb{F}_2^n$, where $3 \leqslant k \leqslant n-1$. We present lower bounds for the cardinalities of all such $\mathcal{P}_n^k$ and $\mathcal{P}_n^k \cap \ldots \cap \mathcal{P}_n^{n-1}$ that improve the result of W. E. Clark et al., 2007 providing that these sets are not empty. We prove that almost all permutations of $\mathbb{F}_2^n$ belong to $\mathcal{P}_n^4 \cap \ldots \cap \mathcal{P}_n^{n-1}$. Asymptotic lower and upper bounds of $|\mathcal{P}_n^3|$ and $|\mathcal{P}_n^3 \cap \ldots \cap \mathcal{P}_n^{n-1}|$ up to $o(2^n!)$ are obtained as well. The number of functions from $\mathcal{P}_n^4 \cap \ldots \cap \mathcal{P}_n^{n-1}$ that map exactly one 3-dimensional affine subspace of $\mathbb{F}_2^n$ to an affine subspace is estimated.

Keywords: *affine subspaces, invariant subspaces, permutations, asymptotic bounds.*

Kutsenko A. V. **CHARACTERIZATION OF GENERALIZED BENT FUNCTIONS OF ALGEBRAIC DEGREE 1.** Bent functions of the form $\mathbb{F}_2^n \to \mathbb{Z}_q$, where $q \geqslant 2$ is a positive integer, are known as generalized bent (gbent) functions. A gbent function for which it is possible to define a dual gbent function is called regular. We study gbent functions of degree 1. Criterion of the generalized Boolean function of degree 1 to be gbent is obtained. The conditions under which the function is regular or weakly regular are described. Component Boolean functions are investigated, it follows that for the case $q = 2^k$ two of them, having maximal indices, are quadratic, while the rest are constant.

Keywords: *generalized bent function, regular gbent function, affine function, component Boolean function.*

Pankratova I. A., Garchukova P. R. **ON THE CONSTRUCTION OF INVERTIBLE VECTOR BOOLEAN FUNCTIONS.** The following construction of a vector Boolean function is considered: $G(x) = \big(f(x), f(\pi(x)), f(\pi^2(x)), \ldots, f(\pi^{n-1}(x))\big)$, where $\pi(i) = i \bmod n+1$, f is a n-dimensional Boolean function. An algorithm for constructing such a function with the invertibility property has been proposed; its completeness and correctness have been proven; the number $t(n)$ of invertible functions of type G has been calculated: $t(n) = \prod\limits_{d|n} p(d)!\, d^{p(d)}$, where $p(d)$ is the number of binary Lyndon words of length d. If π is an arbitrary full-cycle substitution (not necessarily a cyclic shift), then the number of invertible functions of type G is $(n-1)!$ times greater.

Keywords: *vector Boolean functions, invertible functions, cyclically equivalent vectors, Lyndon words.*

Pankratova I. A., Sorokoumova A. D. **CRYPTANALYTIC INVERTIBILITY OF THREE-ARGUMENT FUNCTIONS.** Tests of cryptanalytic invertibility for functions $g : D_1 \times D_2 \times D_3 \to D$ are proposed: 1) function g is invertible with respect to the

variable x_1 of the type $\forall\forall\exists$ iff there is a mapping $\varphi : D_1 \times D_2 \to D_3$ such that the following condition is satisfied:

$$\forall a, c \in D_1\, \forall b, d \in D_2 \left(a \neq c \;\Rightarrow\; g(a, b, \varphi(a, b)) \neq g(c, d, \varphi(c, d))\right);$$

2) function g is invertible with respect to the variable x_1 of the type $\forall\exists\forall$ iff there is a mapping $\varphi : D_1 \to D_2$ such that the following condition is satisfied:

$$\forall a, c \in D_1\, \forall b, d \in D_3 \left(a \neq c \;\Rightarrow\; g(a, \varphi(a), b) \neq g(c, \varphi(c), d)\right);$$

3) function g is invertible with respect to the variable x_3 of the type $\forall\exists\forall$ iff there is a mapping $\varphi : D_1 \to D_2$ such that the following condition is satisfied:

$$\forall a, c \in D_1\, \forall b, d \in D_3 \left(b \neq d \;\Rightarrow\; g(a, \varphi(a), b) \neq g(c, \varphi(c), d)\right);$$

4) function g is invertible with respect to the variable x_2 of the type $\exists\forall\forall$ iff there is $a \in D_1$ such that the following condition is satisfied:

$$\forall b, d \in D_2\, \forall y, z \in D_3 \left(b \neq d \;\Rightarrow\; g(a, b, y) \neq g(a, d, z)\right);$$

5) function g is invertible with respect to the variable x_2 of the type $\exists\forall\exists$ iff there are $a \in D_1$ and a mapping $\varphi : D_2 \to D_3$ such that the following condition is satisfied:

$$\forall b, d \in D_2 \left(b \neq d \;\Rightarrow\; g(a, b, \varphi(b)) \neq g(a, d, \varphi(d))\right).$$

Algorithms for constructing a recovering function and generating invertible functions are formulated too.

Keywords: *cryptanalytic invertibility, invertibility test, recovering function.*

Khilchuk I. S. **ON POSSIBILITY TO CONSTRUCT ALGEBRAIC IMMUNE S-BOXES BY CHOOSING COORDINATE BOOLEAN FUNCTIONS.** Vectorial Boolean functions, or S-boxes, are the main nonlinear components of symmetric ciphers, and their properties ensure the cipher's resistance to various types of cryptanalysis. S-box can be presented as a set of Boolean functions called coordinate functions. One good way of constructing S-boxes is to carefully choose these coordinate Boolean functions with necessary cryptographic properties. We continue the study of the set of Boolean functions in a small number of variables with optimal algebraic and correlation immunity orders. The possibility of using these functions as coordinate functions of S-box resistant to algebraic cryptanalysis has been verified programmatically. However, these Boolean functions cannot be used to construct a permutation on $\mathbb{Z}_2^4$ as well as S-box with optimal component algebraic immunity using only a single Boolean function and a permutation.

Keywords: *symmetric-key encryption, Boolean functions, S-boxes, algebraic immunity, correlation immunity.*

SECTION 3

Alekseev E. K., Kyazhin S. N. **RELATED-KEY ATTACKS ON SIGNATURE-BASED AUTHENTICATED KEY ESTABLISHMENT PROTOCOLS.** We describe impersonation attacks on SIGMA, SIG-DH, and TS3-1 protocols with related keys. The attacks use an attack on the signature with related keys (for example, ECDSA). Attacks differ in adversary capabilities caused by the synthesis principles of protocols: the use

of the initiator's identifier as part of the signed message and as part of the first message requires the adversary to have the capability to force an identifier upon registration; the use of the responder's public ephemeral key as part of the signed message requires the adversary to have the capability to compromise future public ephemeral keys.
Keywords: *cryptography, cryptographic protocol, authenticated key establishment, related keys, signature.*

Antonov K. V., Semenov A. A., Otpushchennikov I. V., Pavlenko A. L. **CONSTRUCTING ALGEBRAIC ATTACKS ON LIGHTWEIGHT SYMMETRIC CIPHERS USING FUNCTIONS WITH SMALL NUMBER OF OUTPUT BITS.** We propose a new class of algebraic attacks on lightweight cryptographic functions. The main idea is based on the use of special functions that produce significantly fewer output bits than the original functions specified by the ciphers under consideration (hereafter referred to as standard functions). Examples of similar functions can be found in the so-called cube attacks. The inversion of such special functions is much simpler compared to the inversion of standard ones, but the image of a special function has more than one preimage. To achieve uniqueness, a cloning procedure is proposed: several special functions are constructed for different fragments of the plaintext and a common secret key, and then they are combined into a new function for which the inversion problem has a unique solution. The cloning is performed using the And-Inverter Graphs (AIGs) representing the considered special functions. In addition, we use the well-known AIG minimization algorithms to reduce the size of the resulting representations. The combined application of the mentioned techniques made it possible to construct new algebraic attacks which turned out to be more efficient compared to standard SAT-based attacks for some well-known lightweight stream ciphers with truncated initialization phase.
Keywords: *algebraic cryptanalysis, lightweight cryptography, SAT solvers, Boolean schemes.*

Bakharev A. O., Tsaregorodtsev K. D. **ON THE SECURITY OF SOME ALGORITHMS OVER A GROUP OF POINTS OF ELLIPTIC CURVES.** The results of the analysis of the VKO scheme and the combined VKO+GOST signature scheme in "generalized group" and "bijective random oracle" heuristics are presented. Two security models have been introduced. In the model for VKO scheme, the adversary has to tell whether the key that it obtains as a challenge is chosen uniformly random or it is generated via VKO scheme. The adversary has an access to Combine oracle, which takes ephemeral public key *epk* as an input and returns a shared key obtained via VKO scheme using long-term secret key *sk*. In the model for combined VKO+GOST signature scheme, the adversary has the additional opportunity to obtain GOST signatures on the long-term secret key *sk* (i.e., the key *sk* is used as a static component of VKO scheme and as a long-term secret key for the signature scheme). It has been shown that in the generic group heuristic the advantage of the adversary making at most q_{com} queries to the Combine oracle and at most q_{group} queries to the group oracle can be upper bounded by $2\,q^{-1}\,(q_{\text{group}} + q_{\text{comb}})^2$ (plus a minor summand responsible for the possibility of attacks on the hash function used in the scheme), where q is the base group order. The result is tight due to the existence of discrete-log finding algorithms with the $\mathcal{O}(\sqrt{q})$ complexity. For the combined VKO+GOST scheme, it has been shown that in the Bijective Random Oracle heuristic the problem can be reduced to the model for VKO scheme without signing oracle (i.e., GOST signatures do not leak any useful information).
Keywords: *provable security, VKO, signature scheme, joint security.*

Bobrovskiy D. A., Shilikov D. A. **INVESTIGATION OF SIGNAL CONVERSION DESIGNS WITH TRNG BASED ON RING OSCILLATORS.** This paper presents circuits for processing signals generated by a ring oscillator and the results of testing the generated sequences for randomness. A total of 5 methods are presented for converting bit sequences obtained using the ring oscillator. The von Neumann approach and the XOR operation are used as conversion techniques. The NIST STS test suite is employed to validate the generated sequences. The sequence with the best results from the test is compared with the sequence encrypted using AES in counter mode.
Keywords: *physical random number generator, sampling, ring oscillator, sequence conversion methods.*

Bugrov A. D., Kamlovskii O. V., Mizerov V. V. **SOME PROPERTIES OF SEQUENCES GENERATED BY THE GEA-1 ENCRYPTION ALGORITHM.** We consider distribution properties and autocorrelation coefficients of sequences generated by the GEA-1 encryption algorithm. We use known estimates of exponential sums from linear recurrence sequences. Let $v = (v(i))_{i=0}^{\infty}$ be the keystream sequence of the GEA-1 algorithm. We prove that the period of sequence v equals to $T(v) = (2^{31}-1)(2^{32}-1)(2^{33}-1)$. We also prove that the number of occurrences of elements $z \in \{0,1\}$ in the vector $(v(0),\dots,v(l-1))$ satisfies the following relations: $N(z,v) = (T(v) - (-1)^z)/2$ and $|N_l(z,v) - l/2| < 1{,}8 \cdot 2^{60}$ for all $l \leqslant T(v)$.
Keywords: *linear recurrence sequences, filter generators, discrete functions, additive character sums, cross-correlation function.*

Glukhov M. M., Denisov O. V. **MATRIX OF TRANSITION PROBABILITIES OF DIFFERENTIALS OF 8-ROUND LUBY — RACKOFF SCHEME.** The Luby — Rackoff scheme is a Markov cipher. The eighth power of the matrix of transition probabilities of differentials of the Lyubi — Rakoff scheme is calculated, estimates of the volume of material for a j-vector ($j = 1, 2$) discriminative attack are given for an 8-round scheme in the model of independent two-block texts.
Keywords: *Markov block ciphers, Luby — Rackoff scheme, distinguishing attack, transition probabilities of differentials.*

Denisov O. V., Ramodanov S. M. **DIFFERENTIAL-LINEAR DISTINGUISHING ATTACKS ON BLOCK CIPHERS.** We define a class of differential-linear distinguishing attacks on block ciphers and construct the optimal attack (called differential-singular) in this class. We carry out statistical experiments on SmallPresent ciphers with block length $n \in \{8, 12, 16\}$ and $R \in \{3,\dots,9\}$ rounds.
Keywords: *differential-linear statistics, singular numbers, distinguishing attacks, SmallPresent cipher.*

Zaikin O. S. **PREIMAGE ATTACK ON 44-STEP MD4 COMPRESSION FUNCTION WITH WEAKENED LAST STEP.** The main component of the cryptographic hash function MD4 is a 48-step compression function. In 2007, a preimage of the 39-step MD4 compression function was found via CDCL — the main complete SAT solving algorithm. In 2022, a preimage of the 43-step MD4 compression function was found via the parallel SAT solving algorithm Cube-and-Conquer. In the present paper, 44-step compression function MD4 is studied such that the 44th step is weakened in different ways. Preimages of several such functions were found via Cube-and-Conquer. Based on these results, a runtime estimate of a preimage attack on the 44-step MD4 compression function is calculated.

Keywords: *cryptographic hash function, MD4, preimage attack, logical cryptanalysis, SAT.*

Kazantsev S. Yu., Pankov K. N. **ALGORITHM FOR QUICKLY GENERATING A KEY SEQUENCE USING A QUANTUM COMMUNICATION CHANNEL.** This paper proposes a method for quickly generating a key sequence for use in the Vernam cipher using a quantum channel and an open communication channel. A sequence of independent identically distributed bits generated by a quantum random number generator is transmitted over an open communication channel, accessible to all users, and information about the method for selecting bits from this sequence is transmitted over the quantum channel. Estimates of the number of enemy attempts to brute force key sequences and the probability of these sequences matching between different users are given.
Keywords: *quantum cryptography, information security,key distribution, quantum channel, quantum random number generator.*

Koreneva A. M., Firsov G. V. **POST-QUANTUM DISTINGUISHING ATTACK ON ONE BLOCK CIPHERS MODE OF OPERATION.** At the end of 2022, in Russian Federation, standardisation recommendations were adopted that define a block cipher mode of operation for block-oriented storage devices protection. This mode is called Disk Encryption with Counter (DEC). The DEC mode is a modification of CTR mode, where initialization vector and initial counter value are derived from sector and partition numbers. In this paper, we define a provable security model that provides a notion of confidentiality when a quantum oracle is accessible to an adversary. A single-query distinguishing attack on the DEC mode is discussed. The attack relies on the possibility to disentangle plaintext and ciphertext registers from each other when the provided plaintext is encrypted directly, and the impossibility of such a transition when a random permutation is applied to the plaintext before encryption.
Keywords: *full disk encryption, block cipher mode of operation, symmetric cryptography, cryptographic protection of information, block-oriented storage devices.*

Medvedeva N. V., Titov S. S. **INDEPENDENCE OF EVENTS IN SPACES OF EQUALLY PROBABLE CIPHERVALUES.** Within the framework of the probabilistic cipher model, the problem of decomposition in some orthogonal coordinate system of the discrete space Ω of elementary events into pairs of families of incompatible events independent of any event of another family is considered. It is shown that the binary event independence relation is related to the number-theoretic nature of the number N — the power of the discrete space Ω of elementary events. It is proved that for a composite number N there are pairs of independent subspaces of the space Ω, and for prime N there are no independent subspaces. Examples illustrating the obtained theoretical statements are constructed.
Keywords: *perfect ciphers, space of elementary events, independent events.*

Panasenko S. P. **LIGHTWEIGHT AUTHENTICATION ENCRYPTION: A REVIEW OF APPROACHES.** This review paper is dedicated to the algorithms of authenticated encryption with associated data, as well as functionally similar modes of operation of symmetric block ciphers. It considers such standardized modes of operation as Galois/ Counter Mode and Multilinear Galois Mode, as well as encryption algorithms originally developed to implement such transformations, using Ascon algorithm as an example. The applicability of authenticated encryption with associated data for the use in low-resourced devices is shown using the example of radio frequency tags interacting with the reader via a

radio channel. In conclusion, some possible criteria for choosing a specific algorithm and/or operating mode for implementation in a target low-resource platform are shown.
Keywords: *authenticated encryption with associated data, lightweight cryptography, block cipher modes of operation.*

Polyakov M. V., Koreneva A. M. **QUANTUM CRYPTANALYSIS OF THE KB-256 BLOCK CIPHER.** In this paper, we present the results of a quantum cryptanalysis of the KB-256 block cipher. First of all, we have obtained the complexity of quantum circuit implementation. This quantum circuit is a part of the oracle in Grover's algorithm. As a result, such an attack would require at least 1068 qubits and 188892 quantum gates. Also, in our analysis we have found that the cipher is resistant to attacks based on searching hidden linear structures.
Keywords: *quantum cryptanalysis, Grover's search, quantum circuits, hidden linear functions.*

Pudovkina M. A., Smirnov A. M. **AN ATTACK ON 6-ROUND XSL-BLOCK CIPHERS.** We study XSL block cipher with a key schedule algorithm based on a second-order recurrence relation and an inverse matrix of linear transform such that there exists a row with at least two equal elements. In this paper, we propose an attack on reduced 6-round XSL block ciphers based on combining of meet-in-the-middle technique, impossible differential technique, and zero-difference pattern. Firstly, we use meet-in-the-middle technique to form a set of the first round key candidates. Secondly, we use impossible differential technique and zero-difference pattern to get a distinguisher to obtain a set of the sixth round key candidates. The probability of success is 0.7. We check our attack on 16-bit XSL block ciphers.
Keywords: *XSL block cipher, linear transform, impossible differential technique, meet-in-the-middle technique, zero-difference pattern, differential technique.*

Tokareva N. N. **TEN YEARS OF THE INTERNATIONAL OLYMPIAD IN CRYPTOGRAPHY NSUCRYPTO.** The paper is devoted to a history of the development of the International Cryptography Olympiad Non-Stop University CRYPTO, its open problems and results.
Keywords: *NSUCRYPTO, Olympiad, cryptography.*

Turchenko O. Y., Usmanov S. R. **PARAMETER ANALYSIS OF THE POST-QUANTUM HYPERICUM SIGNATURE SCHEME.** The paper is devoted to the parameter analysis of the of post-quantum stateless hash-based signature schemes (SPHINCS$^+$, SPHINCS$^+$C, and Hypericum). New parameter sets are proposed to provide 120-bit security against forgery by a quantum adversary. The selection of sets was carried out taking into account the application characteristics and possible areas of application of the schemes under consideration.
Keywords: *Hypericum, SPHINCS$^+$, post-quantum cryptography, signature schemes.*

Chezhegova P. A., Koreneva A. M, Polyakov M. V., Firsov G. V. **ON MIXING PROPERTIES OF REGISTER TRANSFORMATIONS OF CIPHERS TEA1 AND TEA2.** In 2023, stream ciphers TEA1, TEA2, TEA3 were revealed as a part of TETRA standard. We study the mixing properties of register transformations of stream ciphers TEA1 and TEA2. Using the matrix-graph approach, we have calculated the exponents of these register transformations' mixing matrices, it is equal to 6 and 34 respectively. As a result, we can conclude that the calculated exponents for TEA1 and TEA2 are fitting the parameters chosen by developers. Moreover, it is possible to use key registers with lesser

number of warm-up rounds for lightweight ciphers implementation.
Keywords: *matrix-graph approach, mixing properties, exponent of matrix, shift register, TETRA.*

SECTION 4

Egorushkin O. I., Kolbasina I. V., Safonov K. V. **ON SOLVING LINEAR HOMOGENEOUS GRAMMARS GENERATING LINEAR LANGUAGES.** We investigate systems of noncommutative symbolic linear homogeneous equations, which are interpreted as linear grammars of formal languages. Such systems are solved in the form of formal power series (FPS) expressing nonterminal symbols through terminal symbols of the alphabet and considered as linear languages. Each FPS is matched by its commutative image, which is obtained under the assumption that all symbols denote commutative variables, real or complex. In this paper, we consider systems of equations that can have an infinite number of solutions, parameterized not by arbitrary numbers, but by arbitrary FPS. We estimate the number of such parameters, which gives a noncommutative analogue of the well-known fact of the theory of linear equations.
Keywords: *systems of linear homogeneous equations, noncommutative variables, formal power series, commutative image.*

Zharkova A. V. **APPLICATION OF FINITE DYNAMIC SYSTEMS FOR INFORMATION SECURITY.** Graph models occupy an important place in problems related to information security. Finite dynamic system (Γ_G, α) is considered, the states of which are all possible orientations of a given graph G, and the evolutionary function α transforms a given state $\overrightarrow{G}$ by reversing all arcs in $\overrightarrow{G}$ that go into sinks, and there are no other differences between the given $\overrightarrow{G}$ and the next $\alpha(\overrightarrow{G})$ states. The paper suggests how this system can be used for information security, namely: as a model for ensuring audit and monitoring the state of an object under the influence of threats to its information security, and investigating information security incidents in automated information systems, as a model for managing the continuous operation of systems and system recovery, countering denials of service, as a technology for identifying and authenticating users and subjects of information processes, and an access control system.
Keywords: *attractor, authentication, graph, identification, incident, cybersecurity, finite dynamic system, fault-tolerance, evolutionary function.*

Kondyrev D. O. **EFFICIENCY MEASUREMENT SYSTEM FOR ZK-SNARK CIRCUITS INTERNAL REPRESENTATION.** A software system for measuring the efficiency of zk-SNARK circuits internal representation has been developed. The system is designed to measure the parameters of zk-SNARK zero-knowledge proof circuits: the number of constraints in the rank 1 constraint systems (R1CS), the time of protocol initialization phase, the time of proof generation, and the lengths of the proving keys. The system allows zk-SNARK circuit developers to measure various parameters during the circuit coding phase and optimize constraint system representations. The developed software system can be used to measure the efficiency of arbitrary zk-SNARK circuits and determine their suitability for various applications.
Keywords: *zero-knowledge proof, zk-SNARK, R1CS, ZoKrates, algorithm efficiency.*

Lebedev R. K., Sitnov V. E. **USING ELF RELOCATIONS FOR EXECUTABLE ENCRYPTION.** A new approach to hiding the code of Linux executable files using a relocation table is proposed, which allows you to create a crypter without embedding the

decryption code in the executable file. Various applications of this approach are evaluated and the respective crypter prototypes are implemented. The dangers of this approach for the reverse engineering tools IDA, Ghidra, angr, as well as for antivirus software are assessed.
Keywords: *packer, crypter, malware, relocation table, ELF.*

SECTION 5

Abrosimov M. B., Tomilov D. A. **CLASSIFICATION OF TREES WHOSE MAXIMAL SUBTREES ARE ALL ISOMORPHIC.** Trees are an important class of graphs that are used in various applications. One of these problems is the problem of restoring a system from its known subsystems. Known problems of reconstructibility with respect to the list of maximal subgraphs (Kelly — Ulam conjecture) and the list of pairwise non-isomorphic maximal subgraphs (Harary conjecture) for trees have a solution: each tree is determined, up to isomorphism, by the set of its maximal subgraphs (Kelly's theorem) and by the set of its pairwise non-isomorphic maximal subgraphs (Harari — Palmer theorem). Harary and Palmer also proved a stronger result: every tree is determined, up to isomorphism, by its maximal subtrees, that is, the trees obtained by removing one leaf from the original tree. Finally, Manvel proved that all but four trees are determined, up to isomorphism, by their pairwise non-isomorphic maximal subtrees. The paper considers the problem of describing trees whose maximal subtrees are all isomorphic. A characteristic theorem is given for such trees: all maximal subtrees of a tree are isomorphic if and only if all its leaves are similar. A class of multilevel stars is introduced. It is proved that this class coincides with the class of trees whose all maximal subtrees are isomorphic.
Keywords: *graph, tree, reconstructibility.*

Ananichev D. S., Geut K. L., Titov S. S. **ON CODES WITH UNIQUE DECODING TO THE NEAREST.** The paper is devoted to the problem No. 7 of the NSUCRYPTO 2023 Olympiad on the description of an interesting class of codes: with unique decoding to the nearest codeword in the Hamming metric. The possibility of representing the code C as a matroid is proved and an intermediate solution is given in the case when a set of bits B such that there is a two-bit word containing it that is decoded not at $z = 0$ coincides with all positions of the code bits.
Keywords: *NSUCRYPTO, Hamming weight, code, matroid.*

Bezzateev S. V. **GENERALIZED (L, G)-CODES IN WEIGHTED HAMING METRIC FOR INFORMATION SECURITY.** Possibilities of using generalized (L, G)-codes for solving various problems of information security are considered. In particular, the variant of using such codes for syndrome based information embedding, code based compression, threshold key distribution schemes is considered.
Keywords: *weighted Hamming distance metric, generalized (L, G)-codes, information security.*

Bolotnikova A. D., Kolesnikov S. G., Leontiev V. M., Semenov A. I. **PROPERTIES OF THE POLARIZING MATRIX OF A POLAR CODE AND CALCULATION OF BHATTACHARYYA PARAMETERS.** This work is a continuation of research to find exact formulas (requiring a polynomial number of operations) for calculating the Bhattacharyya parameters $Z\left(W_N^{(i)}\right)$ of the coordinate channels $W_N^{(i)}$ of a polar code in the case when the transmission channel is binary symmetric and memoryless. It turns out that for this it is necessary to be able to construct such bases of the subspaces Z_{i-1} generated

by the first $i-1$ rows of the polarizing matrix G_N of the polar code of length N and the subspaces U_{i+1} generated by the last $N-i$ rows of G_N that the Hamming weight is an additive function on the basis vectors (or close to it). In this work, these problems are solved for two sequences $i = 2^m + 1$ and $i = 2^m - 1$, and also for $i \geqslant N/2$. As a consequence, we find short and polynomial formulas for $Z\left(W_N^{(2^m+1)}\right)$ and $Z\left(W_N^{(2^m-1)}\right)$, and also polynomial-exponential formulas for $Z\left(W_N^{(i)}\right)$, $i \geqslant N/2$. In conclusion, a list of formulas for calculating all the Bhattacharyya parameters for a code of length 32 is given.
Keywords: *polar code, polarizing matrix, Bhattacharyya parameter.*

Kuninets A. A. **QUASI-CYCLIC ALTERNANT CODES AND ANALYSIS OF THEIR SECURITY IN CRYPTOGRAPHIC APPLICATIONS.** The paper presents an overview of quasi-cyclic alternant codes and their structural analysis regarding the classification of automorphisms. Also, we describe in detail methods for restoring the structure of a given code. The attractiveness of the family of considered codes lies in its cryptographic applications, and, as in theory, in reducing the key length of post-quantum code-based schemes. In addition, this method of constructing codes is universal and can be used to obtain alternant codes of quasi-cyclic algebraic-geometric codes associated with an arbitrary curve with a known group of automorphisms. However, as shown in the work, as a result of constructing quasi-cyclic alternant codes, it becomes possible to reduce the key security of the source code to a code with smaller parameters, which may not be resistant to a structural attack.
Keywords: *quasi-cyclic codes, alternant codes, invariant codes, algebraic-geometric code, function fields, automorphism group of a code.*

Prudnikov E. S. **FINITE-STATE GENERATORS WITH MAXIMAL PERIOD.** The periodic properties of a two-stage finite-state generator $G = A_1 \cdot A_2$ are studied, where $A_1 = (\mathbb{F}_2^n, \mathbb{F}_2, g_1, f_1)$ (it is autonomous), $A_2 = (\mathbb{F}_2, \mathbb{F}_2^m, \mathbb{F}_2, g_2, f_2)$, $n, m \geqslant 1$. Some necessary conditions for such a generator with the maximum period are formulated, namely: 1) the output sequence of A_1 is purely periodic and the period length is 2^n; 2) the function f_1 has an odd weigth; 3) substitutions $g(0,\cdot)$ and $g(1,\cdot)$ have different parities. Some sufficient conditions have been also formulated, for example, the function $g_2(u,y)$ must be injective in u and the weigth of the function f_2 must be odd. A method for constructing a generator having maximum period has been proposed.
Keywords: *finite-state generator, maximum period, substitutions.*

Shabarkova A. O., Abrosimov M. B. **ON THE STRUCTURE OF TOURNAMENTS CONSISTING OF ONLY KINGS.** The structure of some classes of tournaments consisting of only kings and their number are considered, and it is also shown that such tournaments are not simple. A tournament is called regular if all its vertices have the same entry and exit degrees. The vertex v of the tournament is king if the length of the path from v to any other vertex is no more than 2. The following main result has been obtained: tournament T of dimension n, where n is odd, consisting of only kings, k rows of the distance matrix of which have the form $(1^{(n-1)/2}, 2^{(n-1)/2})$, and the rest $(1^{(n-i-1)}, 2^i)$, where $i \in \{1, \ldots, (n-k)/2, (n+k)/2-1, \ldots, n-2\}$, has the following structure: at the base there is a regular tournament of dimension k, to which two vertices v_1 and v_2 are sequentially added as follows: arcs lead from vertex v_1 to all vertices of tournament T^*; from each vertex of T^* there are arcs leading to vertex v_2; and there is also an arc from v_2 to v_1, where T^* is the tournament obtained at the previous step, until the dimension of the resulting tournament is equal to n. Such a tournament is not simple, and for each n

there are as many such tournaments as there are regular tournaments with the number of vertices equal to that of the tournament at the base.
Keywords: *graph theory, tournament, distance matrix.*

SECTION 6

Bakharev A. O. **RESEARCH OF k-SIEVE ALGORITHM FOR SOLVING THE SHORTEST VECTOR PROBLEM IN A LATTICE.** Quantum computing has been actively developing in recent decades: the number of qubits operated by a quantum compute is increasing and the probability of computational errors is decreasing. Therefore, there is a need to design and analyze post-quantum cryptosystems — cryptosystems resistant to attacks using a quantum computer. One of the main approaches to designing such cryptosystems is lattice theory. In this approach, the security of most cryptosystems is reduced to solving the problem of finding the shortest vector in the lattice (SVP). The results of the analysis of the 8-sieve algorithm for solving SVP are presented. We propose a new trade-off between runtime and amount of memory used by the 8-sieve algorithm. A comparison with known k-sieve algorithms is given. The proposed algorithm has the minimum running time on the segment $(2^{0.155n}, 2^{0.189n})$ of memory used among the known k-sieve algorithms.
Keywords: *lattice-based cryptography, k-sieve, SVP, post-quantum cryptography.*

Zelenetsky A. S., Klyucharev P. G. **MODULAR ARITHMETIC OPTIMIZATION IN KYBER KEM.** Kyber is a post-quantum key encapsulation mechanism that has been selected as a finalist in the third round of the NIST Post-Quantum Cryptography Competition. Today, Kyber is the only post-quantum key encapsulation mechanism recommended for standardization by NIST. The paper presents a new approach to optimize arithmetic operations in Kyber KEM. It reduces the number of modular reductions by increasing the bit size of numbers. The proposed optimization is appropriate for the general purpose systems with 32 or 64-bit CPUs. According to the benchmarking, our optimization speeds up the decapsulation algorithm by up to 1.83 times, the encapsulation algorithm — by up to 1.58 times, and the key generation — by up to 1.41 times.
Keywords: *Kyber, modular arithmetic, post-quantum cryptography, lattice-based cryptography.*