МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

ПРИКЛАДНАЯ ДИСКРЕТНАЯ МАТЕМАТИКА

Научный журнал

2024 № 65

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

Свидетельство о регистрации ПИ № ФС 77-33762 от 16 октября 2008 г.

Подписной индекс в объединённом каталоге «Пресса России» 38696

УЧРЕДИТЕЛЬ
Томский государственный университет

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

В журнале публикуются результаты фундаментальных и прикладных научных исследований отечественных и зарубежных ученых, включая студентов и аспирантов, в области дискретной математики и её приложений в криптографии, компьютерной безопасности, кибернетике, информатике, программировании, теории надёжности, интеллектуальных системах.

Периодичность выхода журнала: 4 номера в год.

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

Подписано к печати 18.09.2024. Формат $60 \times 84\frac{1}{8}$. Усл. п. л. 15,2. Тираж 300 экз.
Заказ № 6027. Цена свободная. Дата выхода в свет 26.09.2024.

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

СОДЕРЖАНИЕ

CONTENTS

ТЕОРЕТИЧЕСКИЕ ОСНОВЫ ПРИКЛАДНОЙ ДИСКРЕТНОЙ МАТЕМАТИКИ

УДК 519.7 DOI 10.17223/20710410/65/1

О ПОДСТАНОВКАХ, РАЗРУШАЮЩИХ СТРУКТУРУ ПОДПРОСТРАНСТВ ОПРЕДЕЛЁННЫХ РАЗМЕРНОСТЕЙ[1]

Н. А. Коломеец

Институт математики им. С. Л. Соболева СО РАН, г. Новосибирск, Россия

E-mail: kolomeec@math.nsc.ru

Рассматриваются асимптотические 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, X. Hou, A. Mihailovs) 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 мощности множества $\mathcal{P}_n^3$ получены асимптотические оценки снизу и сверху с точностью до $o(2^n!)$: $o(1) \leqslant |\mathcal{P}_n^3|/2^n! - (1-\rho) \leqslant \rho^2/2 + o(1)$, где $\rho = 5/224$. Данные оценки справедливы и для мощности $\mathcal{P}_n^3 \cap \ldots \cap \mathcal{P}_n^{n-1}$. Схожим образом 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. Приведена связь ограничений компонентных функций F со случаем, когда и U, и $F(U)$ — аффинные подпространства $\mathbb{F}_2^n$. Предложена характеризация дифференциально 4-равномерных подстановок в рассматриваемых терминах.

Ключевые слова: *аффинные подпространства, асимптотические оценки, нелинейность, дифференциальная равномерность, APN-функции.*

ON PERMUTATIONS THAT BREAK SUBSPACES OF SPECIFIED DIMENSIONS

N. A. Kolomeec

Sobolev Institute of Mathematics, Novosibirsk, Russia

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, X. Hou, and A. Mihailovs, 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 $|\mathcal{P}_n^3|$ up to $o(2^n!)$ are obtained: $o(1) \leqslant |\mathcal{P}_n^3|/2^n! - (1-\rho) \leqslant \rho^2/2 + o(1)$, where $\rho = 5/224$. They are correct for $|\mathcal{P}_n^3 \cap \ldots \cap \mathcal{P}_n^{n-1}|$ 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.

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

The connection between the restrictions of component functions of F and the case when both U and $F(U)$ are affine subspaces of $\mathbb{F}_2^n$ is obtained. The characterization of differentially 4-uniform permutations in the mentioned terms is provided.

Keywords: *affine subspaces, asymptotic bounds, nonlinearity, differential uniformity, APN functions.*

Введение

В работе рассматриваются ограничения взаимно однозначных отображений на аффинные подпространства $\mathbb{F}_2^n$ в случае, когда их образ также является аффинным подпространством $\mathbb{F}_2^n$. Обозначая множество всех подстановок на $\mathbb{F}_2^n$ через $\mathcal{P}_n$, будем говорить, что $\pi \in \mathcal{P}_n$ *сохраняет структуру* аффинного подпространства $L \subseteq \mathbb{F}_2^n$, если $\pi(L) = \{\pi(x) : x \in L\}$ — аффинное подпространство $\mathbb{F}_2^n$; в противном случае π *разрушает структуру* L. Определим

$$\mathcal{L}_k(\pi) = \{L \subseteq \mathbb{F}_2^n : L \text{ и } \pi(L) \text{ — аффинные подпространства } \mathbb{F}_2^n \text{ размерности } k\} \quad (1)$$

и множества функций, разрушающих структуру подпространств определённых размерностей:

$$\mathcal{P}_n^k = \{\pi \in \mathcal{P}_n : \mathcal{L}_k(\pi) = \varnothing\} \quad \text{и} \quad \mathcal{P}_n^{\geqslant k} = \mathcal{P}_n^k \cap \mathcal{P}_n^{k+1} \cap \ldots \cap \mathcal{P}_n^{n-1}. \quad (2)$$

Основное внимание в работе будем уделять именно этим множествам. Заметим, что $\mathcal{P}_n^0$, $\mathcal{P}_n^1$ и $\mathcal{P}_n^n$ всегда пусты, так как все подмножества $\mathbb{F}_2^n$ из 1, 2 и 2^n элементов являются аффинными подпространствами. Будем называть такие размерности *тривиальными*.

Впервые данные свойства подстановок были рассмотрены в работе [1]. Сохранение структуры подпространства $L \subseteq \mathbb{F}_2^n$ функцией $\pi \in \mathcal{P}_n$ позволяет использовать $\pi|_L : L \to \pi(L)$ 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 перейти к подстановке вида $\mathbb{F}_2^{\dim L} \to \mathbb{F}_2^{\dim L}$. При этом её криптографические свойства (см. [2–6]), инвариантные относительно применения обратимых аффинных преобразований, не зависят от выбора базисов. К таким свойствам, например, относятся алгебраическая степень, нелинейность и порядок дифференциальной равномерности. Одним из подходов к построению функций могут быть их конструкции как подфункций [7]. Для этого использовались и схожие концепции подфункций [8–10]. Разрушение структуры подпространств связано с инвариантными подпространствами отображений (см., например, [11]), которые могут быть использованы в атаке с помощью инвариантного подпространства [12] (см. также обобщение атаки [13] и работы о построении таких подпространств, начиная с S-блоков [14, 15]). Одним из важнейших классов криптографических функций является множество APN-подстановок [16], которое в точности совпадает с $\mathcal{P}_n^2$.

Во-первых, в работе рассматривается характеризация множеств $L \in \mathcal{L}_k(\pi)$ через компонентные функции $\pi \in \mathcal{P}_n$, постоянные на L (следствие 1). Данное свойство можно связать и с нелинейностью π. Также через свойства элементов $\mathcal{L}_2(\pi)$ охарактеризованы дифференциально 4-равномерные подстановки: мощность пересечения двух его различных элементов-множеств не должна превышать 1 (см. утверждение 4). Далее мы усиливаем результаты [1] о непустоте $\mathcal{P}_n^{\geqslant 3}$, т. е. о существовании функций, разрушающих структуру всех аффинных подпространств $\mathbb{F}_2^n$ размерностей от 3 до $n-1$. Для этого используется среднее число $\rho_{n,k}$ (и $\sigma_{n,k}$) элементов в $\mathcal{L}_k(\pi)$ (и $\mathcal{L}_k(\pi) \cup \ldots \cup \mathcal{L}_{n-1}(\pi)$) для $\pi \in \mathcal{P}_n$ (см. утверждения 5, 6 и 7 об их свойствах). Главным образом, результаты касаются их мощности при $n \to \infty$. Показано, что почти

все функции разрушают структуру всех аффинных подпространств $\mathbb{F}_2^n$ размерности от 4 до $n-1$, т. е. $|\mathcal{P}_n^{\geqslant 4}| = 2^n! - o(2^n!)$ (см. следствие 5). Получены следующие оценки для $|\mathcal{P}_n^3|$, справедливые и для $|\mathcal{P}_n^{\geqslant 3}|$: $o(1) \leqslant |\mathcal{P}_n^3|/2^n! - (1-\rho) \leqslant \rho^2/2 + o(1)$, где $\rho = 5/224$ (см. теорему 2). Оценено также количество функций, сохраняющих структуру ровно одного аффинного подпространства $\mathbb{F}_2^n$ (см. следствие 6).

1. Определения

Пусть $\mathbb{F}_2^n$ — векторное пространство размерности n над полем $\mathbb{F}_2$, состоящем из двух элементов. Сложение в $\mathbb{F}_2^n$ обозначим через $\oplus$. Для $x = (x_1, \ldots, x_n), y = (y_1, \ldots, y_n) \in \mathbb{F}_2^n$ определим $\langle x, y\rangle = x_1y_1 \oplus \ldots \oplus x_ny_n$. *Аффинное подпространство* $L \subseteq \mathbb{F}_2^n$ определяется как $L = a \oplus L' = \{a \oplus x : x \in L'\}$, где L' — линейное подпространство $\mathbb{F}_2^n$ и $a \in \mathbb{F}_2^n$, его размерность $\dim L$ равна $\log_2 |L|$. Множества всех линейных и аффинных подпространств $\mathbb{F}_2^n$ размерности k обозначим через $\mathcal{S}_n^k$ и $\widehat{\mathcal{S}}_n^k$ соответственно. Для $L' \in \mathcal{S}_n^k$ существует *ортогональное* подпространство $L'^{\perp} = \{y \in \mathbb{F}_2^n : \langle x, y\rangle = 0 \text{ для всех } x \in L'\}$, при этом $L'^{\perp} \in \mathcal{S}_n^{n-k}$. Через $\langle S\rangle$ и $\langle S\rangle_{\mathcal{A}}$ обозначим *линейную* и *аффинную оболочки* множества $S \subseteq \mathbb{F}_2^n$, т. е. пересечение всех $L \in \mathcal{S}_n^0 \cup \ldots \cup \mathcal{S}_n^n$ ($L \in \widehat{\mathcal{S}}_n^0 \cup \ldots \cup \widehat{\mathcal{S}}_n^n$), содержащих S.

Функция вида $F : \mathbb{F}_2^n \to \mathbb{F}_2^m$ называется *векторной булевой функцией*, а если $m = 1$, то *булевой функцией*. Её *компонентной функцией* называется $F_a : x \mapsto \langle a, F(x)\rangle$, где $a \in \mathbb{F}_2^m \setminus \{0\}$. Любая F может быть единственным образом представлена в виде *полинома Жегалкина* (*алгебраической нормальной формы, АНФ*):

$$F(x_1, x_2, \ldots, x_n) = \bigoplus_{a \in \mathbb{F}_2^n} g_a x_1^{a_1} x_2^{a_2} \ldots x_n^{a_n}, \text{ где } g_a \in \mathbb{F}_2^m \text{ и } 0^0 = 1.$$

Степенью $\deg F$ называется степень её полинома Жегалкина. Функция F называется *аффинной*, если $\deg F \leqslant 1$, и *квадратичной*, если $\deg F = 2$. *Вес Хэмминга* булевой функции $f : \mathbb{F}_2^n \to \mathbb{F}_2$ — количество $x \in \mathbb{F}_2^n$, таких, что $f(x) = 1$; f *сбалансирована*, если её вес равен 2^{n-1}. *Расстояние Хэмминга* между $f, g : \mathbb{F}_2^n \to \mathbb{F}_2$ — количество $x \in \mathbb{F}_2^n$, на которых $f(x) \neq g(x)$.

Нелинейностью N_f функции f называется расстояние Хэмминга от f до ближайшей к ней аффинной булевой функции. Нелинейность N_F векторной функции $F : \mathbb{F}_2^n \to \mathbb{F}_2^m$ определяется как

$$N_F = \min_{b \in \mathbb{F}_2^m \setminus \{0\}} N_{F_b}.$$

Это инвариант относительно *аффинной эквивалентности*: $F, G : \mathbb{F}_2^n \to \mathbb{F}_2^m$ аффинно эквивалентны, если существуют обратимые аффинные преобразования $A : \mathbb{F}_2^n \to \mathbb{F}_2^n$ и $B : \mathbb{F}_2^m \to \mathbb{F}_2^m$, такие, что $G(x) = B(F(A(x)))$ для всех $x \in \mathbb{F}_2^n$. Нетрудно видеть, что $|\mathcal{L}_k(\pi)|$, определённое в (1), также является инвариантом относительно аффинной эквивалентности, а множества $\mathcal{P}_n^k$ и $\mathcal{P}_n^{\geqslant k}$ из (2) замкнуты относительно аффинной эквивалентности.

Более подробную информацию о функциях и их криптографических свойствах можно найти в [2–6].

2. Связь с криптографическими свойствами

Приведём связь множеств $\mathcal{L}_k(\pi)$ с компонентными функциями π, её нелинейностью и порядком дифференциальной равномерности. Начнём с тривиального свойства элементов $\mathcal{L}_0(\pi) \cup \ldots \cup \mathcal{L}_n(\pi)$.

Утверждение 1. Пусть $\pi \in \mathcal{P}_n$ сохраняет структуру аффинных подпространств $L, U \subseteq \mathbb{F}_2^n$. Тогда π сохраняет структуру $L \cap U$.

Доказательство. Ясно, что для любого $x \in L \cap U$ справедливо $x \in \pi(L) \cap \pi(U)$, т. е. $\pi(L \cap U) \subseteq \pi(L) \cap \pi(U)$. Учитывая существование π^{-1}, получаем $\pi(L \cap U) = \pi(L) \cap \pi(U)$. ■

2.1. Компонентные функции и нелинейность

Утверждение 2. Пусть $F : \mathbb{F}_2^n \to \mathbb{F}_2^m$ и U — подпространство $\mathbb{F}_2^n$. Тогда

$$\{a \in \mathbb{F}_2^m : x \in U \mapsto \langle a, F(x)\rangle \text{ — постоянна}\} = (F(u) \oplus \langle F(U)\rangle_{\mathcal{A}})^{\perp}, \text{ где } u \in U,$$

т. е. ровно $2^{m-\dim\langle F(U)\rangle_{\mathcal{A}}} - 1$ компонентных функций F постоянны на U.

Доказательство. Пусть $a \in \mathbb{F}_2^m$, $u \in U$, $v = F(u)$ и $V = F(U) \subseteq \mathbb{F}_2^m$. Тогда функция $F_a : x \mapsto \langle a, F(x)\rangle$ постоянна на U, если и только если

$$\langle a, v \oplus y\rangle = 0 \text{ для всех } y \in V.$$

Это эквивалентно тому, что $a \in \langle v \oplus V\rangle^{\perp}$. Убрав $a = 0$, получим ровно $2^{m-\dim\langle v\oplus V\rangle} - 1$ различных компонентных функций. Для завершения доказательства осталось показать, что

$$\langle V\rangle_{\mathcal{A}} = v \oplus \langle v \oplus V\rangle. \tag{3}$$

Действительно, любое аффинное подпространство $V' \subseteq \mathbb{F}_2^m$, содержащее V, содержит и v, т. е. $v \oplus V' \supseteq v \oplus V$ и $v \oplus V'$ — линейное. Следовательно, $v \oplus V'$ содержит $\langle v \oplus V\rangle$. Значит, $\langle V\rangle_{\mathcal{A}} \supseteq v \oplus \langle v \oplus V\rangle$. Но $v \oplus \langle v \oplus V\rangle$ — это также аффинное подпространство $\mathbb{F}_2^m$, содержащее V, т. е. (3) доказано. ■

Для взаимно однозначных функций справедлив следующий критерий.

Следствие 1. Пусть $\pi \in \mathcal{P}_n$ и U — аффинное подпространство $\mathbb{F}_2^n$. Тогда π сохраняет структуру U, если и только если ровно $2^{n-\dim U} - 1$ компонентных функций π постоянны на U.

Доказательство. Пусть $u \in U, V \subseteq \mathbb{F}_2^m, |V| = 2^{n-\dim U}, 0 \in V$ и $\langle v, \pi(x)\rangle$ постоянна на U тогда и только тогда, когда $v \in V$. Ясно, что V — линейное подпространство $\mathbb{F}_2^n$, так как множество постоянных функции замкнуто относительно сложения. Следовательно, $\pi(u) \oplus \pi(U) \subseteq V^{\perp}$. Но тогда $\dim\langle \pi(U)\rangle_{\mathcal{A}} \leqslant n - (n - \dim U) = \dim U$. С учётом взаимной однозначности π, $\pi(U)$ может быть только аффинным подпространством $\mathbb{F}_2^n$. Доказательство в другую сторону напрямую следует из утверждения 2. ■

Отметим, что булевы функции, постоянные на некотором аффинном подпространстве $\mathbb{F}_2^n$ размерности k, называются k-нормальными [17–19]. Если $\dim\langle F(U)\rangle_{\mathcal{A}} < m$ для $F : \mathbb{F}_2^n \to \mathbb{F}_2^m$ (или $U \in \mathcal{L}_k(F)$ в случае обратимой F и $k < n$), то F имеет $\dim U$-нормальную компонентную функцию. Известно, что нелинейность таких функций (а значит, и N_F) можно оценить сверху как $2^{n-1} - 2^{\dim U-1}$ [20, 21]. Эту и другие оценки нелинейности можно найти в работе [7]. Оценка $2^{n-1} - 2^{\dim U-1}$ при $U \in \mathcal{L}_k(F)$ следует также из [12]. Таким образом, функции с высокой нелинейностью разрушают структуру аффинных подпространств $\mathbb{F}_2^n$ больших размерностей.

Интересным является и критерий сохранения структуры гиперплоскостей, доказанный в одну сторону в [7].

Следствие 2. Пусть $\pi \in \mathcal{P}_n$. Тогда $L \in \mathcal{L}_{n-1}(\pi) \iff a \oplus L \in \mathcal{L}_{n-1}(\pi)$ для всех $a \in \mathbb{F}_2^n$. При этом

$$|\mathcal{L}_{n-1}(\pi)| = 2|\{b \in \mathbb{F}_2^n \setminus \{0\} : x \mapsto \langle b, \pi(x)\rangle \text{ — аффинна}\}|$$

и $N_\pi = 0 \iff \mathcal{L}_{n-1}(\pi) \neq \varnothing$.

Доказательство. Если $L \in \mathcal{L}_{n-1}(\pi)$, то $\pi(\mathbb{F}_2^n \setminus L) = \mathbb{F}_2^n \setminus \pi(L)$, где $\mathbb{F}_2^n \setminus L$ и $\mathbb{F}_2^n \setminus \pi(L)$ являются аффинными подпространствами $\mathbb{F}_2^n$ размерности $n-1$ (гиперплоскостями). Следовательно, $\mathbb{F}_2^n \setminus L \in \mathcal{L}_{n-1}(\pi)$, т. е. $\mathcal{L}_{n-1}(\pi)$ разбивается на пары $\{L, \mathbb{F}_2^n \setminus L\}$. При этом $\mathbb{F}_2^n \setminus L = a \oplus L$ для некоторого $a \in \mathbb{F}_2^n$, и в целом $s \oplus L$ для $s \in \mathbb{F}_2^n$ совпадает либо с L, либо с $\mathbb{F}_2^n \setminus L$.

Далее, по следствию 1: $L \in \mathcal{L}_{n-1}(\pi) \iff$ ровно одна компонентная функция π_b постоянна на L, $b \in \mathbb{F}_2^n \setminus \{0\}$. Но так как π обратима, её компонентная функция π_b должна быть сбалансированной [5]. Следовательно, π_b постоянна и на $\mathbb{F}_2^n \setminus L$, т. е. она является аффинной. Таким образом, пара $\{L, \mathbb{F}_2^n \setminus L\} \subseteq \mathcal{L}_{n-1}(\pi)$ соответствует некоторой одной аффинной π_b.

В обратную сторону справедливо аналогичное соответствие, так как аффинность некоторой компонентной функции означает, что она постоянна на некоторой гиперплоскости $L \in \mathcal{S}_n^k$ и её сдвиге $\mathbb{F}_2^n \setminus L$ [5], т. е. аффинная (и сбалансированная) π_b соответствует ровно одной паре $\{L, \mathbb{F}_2^n \setminus L\} \subseteq \mathcal{L}_{n-1}(\pi)$. Обратим внимание, что компонентные функции π_b и π_c при различных $b, c \in \mathbb{F}_2^n$, являющиеся аффинными, не могут иметь одно и то же L: тогда их сумма $\pi_b \oplus \pi_c$, являющаяся компонентной функцией $\pi_{b \oplus c}$, не будет сбалансированной.

Осталось воспользоваться определением: $N_\pi = 0 \iff$ некоторая из компонентных функций π аффинна. ■

2.2. Дифференциальная равномерность и APN-функции

Порядком дифференциальной равномерности $\delta(G)$ функции $G : u \oplus L \to u' \oplus L'$, где L и L' — линейные подпространства $\mathbb{F}_2^n$ и $\mathbb{F}_2^m$ соответственно, $u \in \mathbb{F}_2^n$ и $u' \in \mathbb{F}_2^m$, называется минимальное t, такое, что при любых параметрах $a \in L \setminus \{0\}$ и $b \in L'$ уравнение $G(x) \oplus G(x \oplus a) = b$ имеет не более t решений относительно $x \in u \oplus L$. Если $|L| = |L'|$ и $\delta(G) = 2$, то G называется *APN-функцией*. Обратим внимание, что в литературе также встречается термин *порядок разностной равномерности* (по аналогии с разностным криптоанализом).

Отметим, что свойства $\delta(G)$ полностью соответствуют свойствам $\delta(G')$ для функций $G' : \mathbb{F}_2^{\dim L} \to \mathbb{F}_2^{\dim L'}$; для $\pi \in \mathcal{P}_n$ и $L \in \mathcal{L}_k(\pi)$, выполняется $\delta(\pi|_L) \leqslant \delta(\pi)$. Данное свойство активно используется, например, в [7]. Одним из эквивалентных определений APN-подстановок является следующее: $\pi \in \mathcal{P}_n$ — APN-функция $\iff \mathcal{L}_2(\pi) = \varnothing$.

В общем случае сохранение структуры подпространств определённых размерностей не ограничивает порядок дифференциальной равномерности функции, примером чего является функция обращения элементов конечного поля, порядок дифференциальной равномерности которой равен 2 и 4 при нечётном и чётном числе переменных соответственно [16]. Согласно [11], справедливо следующее

Утверждение 3 (Н. А. Коломеец, Д. А. Быков, 2024). Пусть $\pi(x) = x^{2^n-2}$ для $x \in \mathbb{F}_{2^n}$ и $2 \leqslant k \leqslant n$. Тогда $|\mathcal{L}_k(\pi)| = (2^n - 1)/(2^k - 1)$ при $k \mid n$, иначе $\mathcal{L}_k(\pi) = \varnothing$.

Однако можно гарантировать пустоту некоторых $\mathcal{L}_k(\pi)$ в случае APN-подстановок.

Следствие 3. Пусть $n > 2$ и $\pi \in \mathcal{P}_n$ — APN-функция. Тогда $\mathcal{L}_2(\pi) = \mathcal{L}_4(\pi) = \mathcal{L}_{n-1}(\pi) = \varnothing$. Если π — квадратичная, то $\mathcal{L}_k(\pi) = \varnothing$ для всех чётных k, $1 \leqslant k \leqslant n$.

Доказательство. Пусть $L \in \mathcal{L}_k(\pi)$. Поскольку $\delta(\pi|_L) \leqslant \delta(\pi)$, $\pi|_L$ также должна быть APN-подстановкой. Таким образом, $\mathcal{L}_2(\pi)$ пусто в силу эквивалентного определения APN-подстановок. Множество $\mathcal{L}_4(\pi)$ пусто в силу несуществования APN-подстановок от 4 переменных; если $\mathcal{L}_{n-1}(\pi)$ непусто, то по следствию 2 нелинейность π равна 0, что также невыполнимо для APN-функции [4]. Из [22] известно, что не существует квадратичных APN-подстановок от чётного числа переменных. ■

Для некоторых небольших n существуют функции, разрушающие структуру всех подпространств $\mathbb{F}_2^n$ нетривиальных размерностей. Например, при $n \in \{3, 5, 7\}$ функция инверсии элементов конечного поля принадлежит $\mathcal{P}_n^{\geqslant 2}$. Множество $\mathcal{P}_4^{\geqslant 2}$ пусто, а вот $\mathcal{P}_6^{\geqslant 2}$ содержит APN-подстановку, найденную в [23]: $\mathcal{L}_2(\pi)$, $\mathcal{L}_4(\pi)$ и $\mathcal{L}_5(\pi)$ для неё пусты по следствию 3 и, согласно экспериментальным данным, $\mathcal{L}_3(\pi)$ также пусто.

2.3. Классификация функций с $\delta(\pi) = 4$

Нетрудно классифицировать дифференциально 4-равномерные функции, исходя из структуры $\mathcal{L}_2(\pi)$.

Утверждение 4. Пусть $\pi \in \mathcal{P}_n$ и $\mathcal{L}_2(\pi) \neq \varnothing$. Тогда $\delta(\pi) = 4 \iff$ любые два различных элемента $\mathcal{L}_2(\pi)$ пересекаются по не более чем одному элементу.

Доказательство. Условие $\mathcal{L}_2(\pi) \neq \varnothing$ гарантирует, что $\delta(\pi) \geqslant 4$.

Пусть $\delta(\pi) = 4$. От противного: пусть $|L \cap U| = 2$ для некоторых $L, U \in \mathcal{L}_2(\pi)$, т. е. в силу взаимной однозначности π справедливо $|\pi(L)| = |\pi(U)| = 4$ и $|\pi(L) \setminus \pi(L \cap U)| = |\pi(U) \setminus \pi(L \cap U)| = 2$.

Обозначим $L \cap U = \{a, a \oplus v\}$ и $\pi(L \cap U) = \{\pi(a), \pi(a) \oplus v')\}$, где $a, v, v' \in \mathbb{F}_2^n$ и $v, v' \neq 0$. Но тогда $L \setminus (L \cap U) = \{b, b \oplus v\}$ и $U \setminus (L \cap U) = \{c, c \oplus v\}$ для некоторых $b, c \in \mathbb{F}_2^n$, где a, b, c попарно различны, так как суммы всех элементов L и U должны быть равны нулю. Так как $\pi(L)$ и $\pi(U)$ — тоже аффинные подпространства $\mathbb{F}_2^n$, аналогично получаем $\pi(L) \setminus \pi(L \cap U) = \{\pi(b), \pi(b) \oplus v'\}$ и $\pi(U) \setminus \pi(L \cap U) = \{\pi(c), \pi(c) \oplus v'\}$. Отсюда уравнение $\pi(x) \oplus \pi(x \oplus v) = v'$ имеет как минимум шесть решений $a, a \oplus v, b, b \oplus v, c, c \oplus v$, что противоречит $\delta(\pi) = 4$. Таким образом, любые различные $L, U \in \mathcal{L}_2(\pi)$ либо не пересекаются, либо пересекаются по одному элементу.

Пусть любые различные $L, U \in \mathcal{L}_2(\pi)$ пересекаются по не более чем одному элементу. От противного: пусть $\delta(\pi) > 4$. Тогда для некоторых $a \in \mathbb{F}_2^n \setminus \{0\}$ и $b \in \mathbb{F}_2^n$ существуют шесть различных $x, x \oplus a$, $y, y \oplus a$, $z, z \oplus a$, $x, y, z \in \mathbb{F}_2^n$, таких, что $\pi(x) \oplus \pi(x \oplus a) = \pi(y) \oplus \pi(y \oplus a) = \pi(z) \oplus \pi(z \oplus a) = b$. Но тогда $\{\pi(x), \pi(x \oplus a), \pi(y), \pi(y \oplus a)\}$ и $\{\pi(z), \pi(z \oplus a), \pi(y), \pi(y \oplus a)\}$ являются аффинными подпространствами $\mathbb{F}_2^n$, размерность которых равна 2 в силу взаимной однозначности π, и пересекаются они ровно по двум элементам, т. е. мы пришли к противоречию. ■

Результаты работы [24] позволяют оценить сверху мощность $\mathcal{L}_2(\pi)$ при $\delta(\pi) = 4$. В ней рассматриваются количества четвёрок $x_1, x_2, x_3, x_1 \oplus x_2 \oplus x_3 \in \mathbb{F}_2^n$, таких, что $F(x_1) \oplus F(x_2) \oplus F(x_3) = F(x_1 \oplus x_2 \oplus x_3)$ для $F : \mathbb{F}_2^n \to \mathbb{F}_2^n$. Если F взаимно однозначна, то это в точности $|\mathcal{L}_2(F)|$. Например, [24, теорема 2.3] позволяет по дифференциальному спектру подсчитать $|\mathcal{L}_2(F)|$:

$$|\mathcal{L}_2(F)| = \frac{1}{3} \sum_{a \in \mathbb{F}_2^n \setminus \{0\}} \sum_{b \in \mathbb{F}_2^n} \binom{\delta_{a,b}(F)/2}{2},$$

где $\delta_{a,b}(F)$ — количество решений уравнения $F(x) \oplus F(x \oplus a) = b$. Поскольку $\sum\limits_{b \in \mathbb{F}_2^n} \delta_{a,b}(F) = 2^n$, то для дифференциально 4-равномерных функций справедлива следующая оценка, достигающаяся в точности при $\delta_{a,b} \in \{0, 4\}$:

Следствие 4. Пусть $\pi \in \mathcal{P}_n$ и $\delta(\pi) = 4$. Тогда $|\mathcal{L}_2(\pi)| \leqslant \frac{1}{3}2^{n-2}(2^n - 1)$.

Нетрудно видеть, что оценка не является целым числом при нечётных n. При этом она гарантированно достигается при $n = 2m + 2$. Например, для функций Голда вида

$$F(x) = x^{2^{2i}+1}, \quad \text{где} \quad x \in \mathbb{F}_{2^{2m+2}},\ 1 \leqslant i \leqslant m \quad \text{и} \quad (i, m+1) = 1,$$

выполняется $\delta_{a,b} \in \{0, 2^{(2i,2m+2)}\}$, и они являются взаимно однозначными [3, 4, 25]. Таким образом, для них достигается оценка следствия 4. Данное количество для всех функций Голда (в том числе необратимых) на языке четвёрок подсчитано в [24, теорема 3.4]. Достигается ли данная оценка при $n = 4m$, остаётся открытым вопросом.

3. Подстановки, разрушающие структуру подпространств определённых размерностей

Имея заданную подстановку, непросто доказать, что она разрушает структуру каких-либо аффинных подпространств $\mathbb{F}_2^n$. Однако можно оценить число таких функций. Например, в [1] доказано, что $\mathcal{P}_n^{\geqslant 3}$ непусто. Оценим доли $|\mathcal{P}_n^k|$ и $|\mathcal{P}_n^{\geqslant k}|$ к $|\mathcal{P}_n|$ при $n \to \infty$. Введём следующие обозначения:

$$\rho_{n,k} = |\widehat{\mathcal{S}}_n^k|^2 \Big/ \binom{2^n}{2^k}, \quad \sigma_{n,k} = \sum_{i=k}^{n-1} \rho_{n,i}.$$

Напомним также, что

$$|\mathcal{S}_n^k| = \frac{\prod\limits_{i=0}^{k-1}(2^n - 2^i)}{\prod\limits_{i=0}^{k-1}(2^k - 2^i)} = \frac{\prod\limits_{i=0}^{k-1}(2^{n-i} - 1)}{\prod\limits_{i=0}^{k-1}(2^{i+1} - 1)} \quad \text{и} \quad |\widehat{\mathcal{S}}_n^k| = 2^{n-k}|\mathcal{S}_n^k|.$$

Из доказательства [1, теорема 2.1] можно заключить, что справедливы следующие оценки:

Теорема 1 (W. E. Clark, X. Hou, and A. Mihailovs, 2007). Пусть $3 \leqslant k < n$. Тогда

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

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 $n-1$), которое сохраняет функция из $\mathcal{P}_n$. Действительно, если это средние значения, то

$$\rho_{n,k}|\mathcal{P}_n| = \sum_{\pi \in \mathcal{P}_n} |\mathcal{L}_k(\pi)| = \sum_{\pi \in \mathcal{P}_n \setminus \mathcal{P}_n^k} |\mathcal{L}_k(\pi)| \geqslant |\mathcal{P}_n \setminus \mathcal{P}_n^k| = |\mathcal{P}_n| - |\mathcal{P}_n^k|$$

и аналогично для $\sigma_{n,k}$, что является доказательством теоремы 1. Далее мы детально рассмотрим это и другие свойства $\rho_{n,k}$ и $\sigma_{n,k}$.

3.1. Среднее количество подпространств, структуру которых сохраняет подстановка

Начнём с утверждения о средней мощности $\mathcal{L}_k(\pi)$.

Утверждение 5. 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.

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

Доказательство. Пусть $\tau(\pi, L) = 1$, если $\pi(L) \in \widehat{\mathcal{S}}_n^k$, и 0 иначе, где $\pi \in \mathcal{P}_n$ и $L \in \widehat{\mathcal{S}}_n^k$. Перепишем сумму из условия следующим образом:

$$\sum_{\pi\in\mathcal{P}_n} |\mathcal{L}_k(\pi)| = \sum_{\pi\in\mathcal{P}_n} \sum_{L\in\widehat{\mathcal{S}}_n^k} \tau(\pi, L) = \sum_{L\in\widehat{\mathcal{S}}_n^k} \sum_{\pi\in\mathcal{P}_n} \tau(\pi, L) = \sum_{L\in\widehat{\mathcal{S}}_n^k} |\{\pi \in \mathcal{P}_n : \pi(L) \in \widehat{\mathcal{S}}_n^k\}|. \quad (4)$$

Выберем любое $L \in \widehat{\mathcal{S}}_n^k$ и подсчитаем количество различных $\pi \in \mathcal{P}_n$, для которых $\pi(L) \in \widehat{\mathcal{S}}_n^k$. Во-первых, мы можем выбрать любое из $\widehat{\mathcal{S}}_n^k$ в качестве $\pi(L)$, при этом разные $\pi(L)$ влекут и различие π, т. е. получаем $|\widehat{\mathcal{S}}_n^k|$ вариантов $\pi(L)$. Далее, $\pi|_L$ можно выбрать $|\pi(L)| = 2^k!$ способами, так как мы зафиксировали $\pi(L)$. Каждое такое $\pi|_L$ нужно продолжить на всё $\mathbb{F}_2^n$, т. е. оставшиеся $2^n - 2^k$ элементов нужно расположить всевозможными $(2^n - 2^k)!$ способами на $\mathbb{F}_2^n \setminus L$. Итого, учитывая, что начальное L из $|\widehat{\mathcal{S}}_n^k|$, запишем

$$\sum_{\pi\in\mathcal{P}_n} |\mathcal{L}_k(\pi)| = |\widehat{\mathcal{S}}_n^k| \cdot |\widehat{\mathcal{S}}_n^k| \cdot 2^k! \, (2^n - 2^k)!.$$

Поделив всё на $|\mathcal{P}_n| = 2^n!$, получим то, что требуется доказать. ■

Для тривиальных аффинных подпространств $\rho_{n,k}$ также находится тривиально:

$$\rho_{n,0} = 2^n, \quad \rho_{n,1} = 2^{n-1}(2^n - 1), \quad \rho_{n,n} = 1.$$

Приведём в явном виде выражения для $\rho_{n,2}$ и $\rho_{n,3}$.

Утверждение 6. Справедливо

$$\rho_{n,2} = \frac{2^{n-3}(2^n-1)(2^n-2)}{3(2^n-3)} = \frac{2^{2n-3}}{3} + \frac{1}{12} + \frac{1}{2^{n+2}-12},$$
$$\rho_{n,3} = \rho\frac{2^n(2^n-1)(2^n-2)(2^n-4)}{(2^n-3)(2^n-5)(2^n-6)(2^n-7)}, \quad \text{где} \quad \rho = \frac{5}{224}.$$

Для доказательства достаточно воспользоваться общей формулой и выполнить несложные приведения.

3.2. Свойства $\rho_{n,k}$ и $\sigma_{n,k}$ при $k \geqslant 3$

Рассмотрим свойства $\rho_{n,k}$ и $\sigma_{n,k}$ при $k \geqslant 3$, т. е. когда их значение меньше 1. Сосредоточим внимание на $\rho_{n,3}$, $\sigma_{n,3}$ и $\sigma_{n,4}$.

Лемма 1. Пусть $2 \leqslant k < n - 1$. Тогда

$$\rho_{n,k+1} < \frac{\rho_{n,k}}{2^{2n-6}(2^{n-k-1}-1)^{2^k-4}}.$$

Доказательство. Имеет место

$$|\widehat{\mathcal{S}}_n^{k+1}| = 2^{n-k-1}\frac{\prod\limits_{i=0}^{k}(2^{n-i}-1)}{\prod\limits_{i=0}^{k}(2^{i+1}-1)} = \frac{1}{2}\,\frac{2^{n-k}-1}{2^{k+1}-1}|\widehat{\mathcal{S}}_n^k| < \frac{2(2^{n-k-1}-1)}{2^{k+1}-1}|\widehat{\mathcal{S}}_n^k|.$$

При этом

$$\binom{2^n}{2^{k+1}} = \prod_{i=0}^{2^{k+1}-1}(2^n - i)/2^{k+1}! = \prod_{i=0}^{2^k-1}\frac{2^n - 2^k - i}{2^k + i + 1}\binom{2^n}{2^k} > (2^{n-k-1}-1)^{2^k}\binom{2^n}{2^k}.$$

Подставив неравенства в выражение для $\rho_{n,k+1}$ из утверждения 5, получим

$$\rho_{n,k+1} < \frac{4(2^{n-k-1}-1)^2\rho_{n,k}}{(2^{n-k-1}-1)^{2^k}(2^{k+1}-1)^2} = \frac{4\rho_{n,k}}{(2^{n-k-1}-1)^{2^k-4}(2^n-2^{n-k-1}-2^{k+1}+1)^2}.$$

Учитывая, что $2^n - 2^{n-k-1} - 2^{k+1} + 1 > 2^{n-2}$, получаем требуемое неравенство. ■

Рассмотрим поведение $\rho_{n,k}$ при увеличении n.

Лемма 2. Пусть $4 \leqslant k \leqslant n$. Тогда

$$\rho_{n+1,k} < 2^{2k+4-2^k}\rho_{n,k}. \tag{5}$$

Доказательство. Ясно, что

$$|\widehat{\mathcal{S}}^k_{n+1}| = 2^{n+1-k}\frac{\prod\limits_{i=0}^{k-1}(2^{n+1-i}-1)}{\prod\limits_{i=0}^{k-1}(2^{i+1}-1)} = \frac{2^{n+2}-2}{2^{n-k+1}-1}|\widehat{\mathcal{S}}^k_n| < \frac{2^{n+2}}{2^{n-k}}|\widehat{\mathcal{S}}^k_n| = 2^{k+2}|\widehat{\mathcal{S}}^k_n|.$$

В то же время $\binom{2^{n+1}}{2^k} = \prod\limits_{i=0}^{2^k-1}(2^{n+1}-i)/2^k! = \prod\limits_{i=0}^{2^k-1}\frac{2^{n+1}-i}{2^n-i}\binom{2^n}{2^k} \geqslant 2^{2^k}\binom{2^n}{2^k}$.
Подставив неравенства в формулу для $\rho_{n+1,k}$, получим (5). ■

Докажем основные свойства $\rho_{n,k}$ и $\sigma_{n,k}$ при $k \geqslant 3$.

Утверждение 7. 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

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

Доказательство. По утверждению 5

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

т. е. оно представляется в виде произведения ρ и монотонно убывающих сомножителей.

Монотонное убывание $\rho_{n,k}$ при $k \geqslant 4$ следует из леммы 2:

$$2^{-4} \geqslant 2^{2k+4-2^k} > \frac{\rho_{n+1,k}}{\rho_{n,k}}. \tag{6}$$

Докажем, что $\sigma_{k,n} = \rho_{k,n} + \ldots + \rho_{n-1,n}$ также монотонно убывает. Учитывая убывание $\rho_{n,k}$, достаточно показать, что $\rho_{n,n-1} > \rho_{n+1,n-1} + \rho_{n+1,n}$. Так как $n \geqslant 4$, то $\rho_{n+1,n} < \rho_{n+1,n-1}$ по лемме 1. Далее достаточно воспользоваться (6).

Найдём пределы $\rho_{n,k}$ и $\sigma_{n,k}$. Очевидно, что $\rho_{n,3}$ стремится к ρ. Для нахождения всех оставшихся пределов достаточно показать, что $\sigma_{n,4}$ сходится к нулю. Воспользуемся убыванием $\sigma_{n,4}$ и леммой 1:

$$\sigma_{n,4} = \sum_{k=4}^{n-1}\rho_{n,k} < \frac{n-4}{2^{2n-6}}\cdot\rho_{n,3},$$

т. е. $\sigma_{n,4}$ сходится к нулю. ■

Таким образом, $\rho_{n,3} = \sigma_{n,3} = \rho + o(1)$ и $\rho_{n,k} = \sigma_{n,k} = o(1)$ при $k \geqslant 4$. Используя монотонное убывание $\rho_{n,k}$ и $\sigma_{n,k}$, можно оценивать сверху их значения при больших n начальными значениями. Например, $\rho_{n,3} < \rho_{5,3} < \rho_{4,3}$ для всех $n \geqslant 6$, где

$$\rho_{4,3} = \frac{10}{143} \quad \text{и} \quad \rho_{5,3} = \frac{124}{3393}.$$

В табл. 1 приведены округлённые значения наиболее используемых далее $\rho_{n,3}$, $\sigma_{n,3}$ и $\sigma_{n,4}$ для небольших n, при этом $\rho \approx 0{,}0223214285714286$. Заметим также, что вероятность события $\pi \in \mathcal{P}_n^{\geqslant 3}$ при случайном выборе $\pi \in \mathcal{P}_n$ превышает 93, 96 и 97 % для $n = 4$, 5 и $n \geqslant 6$ соответственно.

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	1
5	0,0365458296492779	0,0365522248005155	$6{,}3951512375906990 \cdot 10^{-06}$
6	0,0281384877529501	0,0281385016330859	$1{,}3880135807123695 \cdot 10^{-08}$
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	$4{,}3530671380777510 \cdot 10^{-20}$

Далее для построения оценок воспользуемся тем, что $\rho_{n,k}$ и $\sigma_{n,k}$ меньше 1 при $k \geqslant 3$ и не будем рассматривать $\rho_{n,2}$. Однако среднее значение $\rho_{n,2} = \dfrac{2^{2n-3}}{3} + \dfrac{1}{12} + \dfrac{1}{2^{n+2} - 12}$ для $|\mathcal{L}_2(\pi)|$ по $\pi \in \mathcal{P}_n$ (см. утверждение 6) можно соотнести с верхней оценкой $|\mathcal{L}_2(\pi)|$ при $\delta(\pi) = 4$ (см. следствие 4), достижимой в случае $n = 2m+2$: $|\mathcal{L}_2(\pi)| \leqslant \dfrac{2^{2n-2} - 2^{n-2}}{3}$. Это подтверждает, что низкий порядок дифференциальной равномерности π в общем случае не является существенным ограничителем на количество элементов в $\mathcal{L}_k(\pi)$.

3.3. Мощность $\mathcal{P}_n^{\geqslant k}$ при $n \to \infty$

Воспользовавшись свойствами $\rho_{n,k}$ и $\sigma_{n,k}$, оценим асимптотику числа подстановок из $\mathcal{P}_n^k$ и $\mathcal{P}_n^{\geqslant k}$ при $k \geqslant 4$.

Следствие 5. Почти все $\pi \in \mathcal{P}_n$ разрушают структуру всех аффинных подпространств размерности от 4 до $n-1$, т. е.

$$\lim_{n \to \infty} \frac{|\mathcal{P}_n^{\geqslant 4}|}{|\mathcal{P}_n|} = 1.$$

Это справедливо и для каждого $\mathcal{P}_n^k$ и $\mathcal{P}_n^{\geqslant k}$ при $k \geqslant 4$.

Доказательство очевидно следует из теоремы 1 и утверждения 7.

Для получения асимптотики размера $\mathcal{P}_n^3$ и $\mathcal{P}_n^{\geqslant 3}$ нам потребуется следующая

Лемма 3. Пусть U — аффинное подпространство $\mathbb{F}_2^n$ размерности k. Тогда количество аффинных подпространств $\mathbb{F}_2^n$ размерности m, пересекающихся с U по аффинному подпространству размерности t, равно $2^{(k-t)(m-t)} \cdot |\widehat{\mathcal{S}}_k^t| \cdot |\mathcal{S}_{n-k}^{m-t}|$.

Доказательство. Без ограничения общности можно считать, что $\mathbb{F}_2^n = \mathbb{F}_2^{n-k} \times \mathbb{F}_2^k$ и $U = \{0\} \times \mathbb{F}_2^k$. Подсчитаем только линейные подпространства $\mathbb{F}_2^{n-k} \times \mathbb{F}_2^k$, для нахождения количества аффинных подпространств домножим полученный результат на 2^{k-t}.

Далее достаточно воспользоваться представлением базиса линейного подпространства $\mathbb{F}_2^n$ размерности m в виде приведённой ступенчатой матрицы (матрицы Гаусса — Жордана): первая слева единица в каждой её последующей строке находится правее предыдущей (эти единицы называются ведущими), и ведущая единица — единственный ненулевой элемент столбца. Любое линейное подпространство имеет единственную такую базисную матрицу [26]. Составим матрицу Гаусса — Жордана размера $m \times n$ из четырёх частей:

$$M = \begin{pmatrix} L & T \\ 0 & R \end{pmatrix},$$

где L и R — матрицы Гаусса — Жордана размера $(m-t) \times (n-k)$ и $t \times k$ соответственно; T — матрица размера $(m-t) \times k$ с единственным ограничением: над ведущими единицами R (их t штук) стоят нули. Пересечением U с линейным подпространством $\mathbb{F}_2^n$, базисом которого являются строки M, будет $\{0\} \times R'$, где R' — линейное подпространство $\mathbb{F}_2^k$, базис которого — строки R. Таким образом, чтобы перебрать все нужные M, требуется выбрать L ($|\mathcal{S}_{n-k}^{m-t}|$ способов), выбрать R ($|\mathcal{S}_k^t|$ способов) и оставшиеся элементы T ($2^{k(m-t)-t(m-t)}$ способов). ■

Теорема 2. Справедливо

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

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

Доказательство. Оценка снизу напрямую следует из теоремы 1. Для доказательства оценки сверху воспользуемся утверждением 5 и равенством (4):

$$\rho_{n,k}|\mathcal{P}_n| = \sum_{\pi \in \mathcal{P}_n} |\mathcal{L}_k(\pi)| = \sum_{L \in \widehat{\mathcal{S}}_n^k} |\{\pi \in \mathcal{P}_n : \pi(L) \in \widehat{\mathcal{S}}_n^k\}|.$$

Пусть $m = |\widehat{\mathcal{S}}_n^3|$ и $\widehat{\mathcal{S}}_n^3 = \{L_1, L_2, \ldots, L_m\}$, т. е. пронумеруем все аффинные подпространства $\mathbb{F}_2^n$ размерности 3. Определим множества A_i, $i \in \{1, \ldots, m\}$, следующим образом:

$$A_i = \{\pi \in \mathcal{P}_n : \pi(L_i) \in \widehat{\mathcal{S}}_n^3\}, \text{ т. е. } |A_1| + \ldots + |A_m| = \rho_{n,3}|\mathcal{P}_n|. \tag{7}$$

Обозначив через $\overline{A_i}$ множество $\mathcal{P}_n \setminus A_i$, по методу включений — исключений получим

$$\mathcal{P}_n^3 = |\overline{A_1} \cap \ldots \cap \overline{A_m}| = |\mathcal{P}_n| - \sum_{1 \leqslant i \leqslant m} |A_i| + \sum_{1 \leqslant i < j \leqslant m} |A_i \cap A_j| + \ldots + (-1)^n |A_1 \cap \ldots \cap A_m|. \tag{8}$$

Мы не будем искать все пересечения, воспользуемся только следующей оценкой:

$$|\mathcal{P}_n^3| \leqslant |\mathcal{P}_n| - \sum_{1 \leqslant i \leqslant m} |A_i| + \sum_{1 \leqslant i < j \leqslant m} |A_i \cap A_j|. \tag{9}$$

Действительно, если какая-то $\pi \in \mathcal{P}_n$ принадлежит k различным A_i, то в выражении $|\mathcal{P}_n| - |A_1| - \ldots - |A_m|$ будет вычтена k раз из $|\mathcal{P}_n|$ вместо одного, т. е. лишние $(k-1)$ раз. Но после добавления пересечений она будет добавлена ещё $k(k-1)/2$ раз.

При этом $k(k-1)/2 \geqslant k-1$ при $k \geqslant 1$. При $k=0$ функция не будет вычтена, так как принадлежит $\mathcal{P}_n^3$. Таким образом, в правой части получим не меньше чем $|\mathcal{P}_n^3|$.

Следовательно, (7) и (9) гарантируют

$$\frac{|\mathcal{P}_n^3|}{|\mathcal{P}_n|} - (1-\rho_{n,3}) \leqslant \sum_{1\leqslant i<j\leqslant m} |A_i \cap A_j| = T_n. \tag{10}$$

Вместо точной формулы для T_n далее рассмотрим только её асимптотику по старшему слагаемому. Разделив все пары (i,j), $i<j$, по мощности пересечения $L_i \cap L_j$, разделим и T_n на соответствующие группы:

$$T_n = T_n^0 + T_n^1 + T_n^2 + T_n^{\varnothing},$$
$$\text{где} \quad T_n^t = \sum_{\substack{1\leqslant i<j\leqslant m,\\ \dim L_i\cap L_j = t}} |A_i \cap A_j| \quad \text{и} \quad T_n^{\varnothing} = \sum_{\substack{1\leqslant i<j\leqslant m,\\ L_i\cap L_j = \varnothing}} |A_i \cap A_j|.$$

1. Найдём T_n^t, т. е. $L_i \cap L_j \in \widehat{\mathcal{S}}_n^t$, где $0 \leqslant t \leqslant 2$. Зафиксируем некоторое t. Первое L_i можно выбрать $|\widehat{\mathcal{S}}_n^3|$ способами, т. е. произвольным образом. Далее лемма 3 гарантирует, что способов выбрать L_j существует ровно

$$2^{(3-t)^2} \cdot |\widehat{\mathcal{S}}_3^t| \cdot |\mathcal{S}_{n-3}^{3-t}|. \tag{11}$$

Таким образом, получаем $\dfrac{1}{2} 2^{(3-t)^2} \cdot |\widehat{\mathcal{S}}_3^t| \cdot |\mathcal{S}_{n-3}^{3-t}| \cdot |\widehat{\mathcal{S}}_n^3|$ способов выбрать $1 \leqslant i < j \leqslant m$, таких, что $\dim L_i \cap L_j = t$ (так как $i<j$, мы поделили общее количество способов выбора упорядоченной пары (L_i, L_j) на два). Найдём для них $|A_i \cap A_j|$. Аналогично предыдущим рассуждениям, образ $\pi(L_i)$ для $\pi \in A_i \cap A_j$ можем выбрать $\widehat{\mathcal{S}}_n^3$ способами, т. е. произвольно. Количество способов выбрать образ $\pi(L_j)$ равно (11), поскольку $|\pi(L_i) \cap \pi(L_j)| = |L_i \cap L_j|$.

Значения π на $L_i \cap L_j$ можно выбрать $2^t!$ способами, переставляя элементы $\pi(L_i) \cap \cap \pi(L_j)$; на оставшихся частях подпространств — $(2^3 - 2^t)!^2$ способами; вне $L_i \cup L_j$ — $(2^n - (16 - 2^t))!$ способами, т. е. получаем

$$T_n^t = \frac{1}{2} 2^{2(3-t)^2} \cdot |\widehat{\mathcal{S}}_3^t|^2 \cdot |\mathcal{S}_{n-3}^{3-t}|^2 \cdot |\widehat{\mathcal{S}}_n^3|^2 \cdot (2^n - (16-2^t))! \cdot 2^t! \cdot (2^3 - 2^t)!^2.$$

Но $T_n^t / 2^n! = o(1)$. Действительно,

$$\frac{T_n^t}{2^n!} = s_t \frac{|\mathcal{S}_{n-3}^{3-t}|^2 \cdot |\widehat{\mathcal{S}}_n^3|^2 \, (2^n - (16-2^t))!}{2^n!} = s_t \frac{|\mathcal{S}_{n-3}^{3-t}|^2 \cdot |\widehat{\mathcal{S}}_n^3|^2}{2^n(2^n-1)\dots(2^n-15+2^t)},$$

где s_t не зависит от n. При этом

$$|\widehat{\mathcal{S}}_n^3| = O(2^{4n}), \quad |\mathcal{S}_{n-3}^{3-t}| = O(2^{(3-t)n}), \quad 2^n(2^n-1)\dots(2^n-r+1) = O(2^{rn}). \tag{12}$$

Таким образом,

$$\frac{T_n^t}{2^n!} = O(2^{(2(3-t)+2\cdot 4-16+2^t)n}) = O(2^{(2^t-2t-2)n}).$$

Подставляя $t \in \{0,1,2\}$, получим $O(2^{-n})$, $O(2^{-2n})$ и $O(2^{-2n})$ соответственно. Это означает, что $T_n^0 + T_n^1 + T_n^2$ можно не учитывать.

2. Найдём $T_n^{\varnothing}$, т. е. $L_i \cap L_j = \varnothing$. Здесь L_i можем выбрать $|\widehat{\mathcal{S}}_n^3|$ способами, L_j — $|\widehat{\mathcal{S}}_n^3| - \sum\limits_{t=0}^{2} \left(2^{(3-t)^2} \cdot |\widehat{\mathcal{S}}_3^t| \cdot |\mathcal{S}_{n-3}^{3-t}|\right) - 1$ способами, согласно (11), и поделить на 2 в силу $i < j$.

Так как $L_i \cap L_j = \varnothing$, то и $\pi(L_i) \cap \pi(L_j) = \varnothing$. Аналогично подсчёту T_n^t, получим

$$T_n^{\varnothing} = \frac{1}{2}|\widehat{\mathcal{S}}_n^3|^2(|\widehat{\mathcal{S}}_n^3| - \sum_{t=0}^{3} \left(2^{(3-t)^2} \cdot |\widehat{\mathcal{S}}_3^t| \cdot |\mathcal{S}_{n-3}^{3-t}|) - 1\right)^2 \cdot 2^3! \cdot 2^3! \, (2^n - 16)!.$$

Согласно (12), старший член $T_n^{\varnothing}/2^n!$ равен

$$\frac{|\widehat{\mathcal{S}}_n^3|^4 \cdot 8! \cdot 8!}{2 \cdot 2^n(2^n-1)\dots(2^n-15)} = \frac{2^6 \cdot 7^2 \cdot 6^2 \cdot 5^2 \cdot 4^2 \cdot 6^2}{(8-1)^4(8-2)^4(8-4)^4 2^{13}} \, \frac{2^{4n}(2^n-1)^4(2^n-2)^4(2^n-4)^4}{2^n(2^n-1)\dots(2^n-15)}.$$

Таким образом,

$$\frac{T_n^{\varnothing}}{|\mathcal{P}_n|} = \frac{5^2}{7^2 2^{11}} + o(1) = \frac{\rho^2}{2} + o(1) \quad \text{и} \quad \frac{T_n}{|\mathcal{P}_n|} = \frac{\rho^2}{2} + o(1), \tag{13}$$

поскольку $T_n^t/|\mathcal{P}_n| = o(1)$. Неравенство (10) завершает доказательство. Оценки для $\mathcal{P}_n^{\geqslant 3}$ очевидно следуют из доказанного и следствия 5. ■

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

Следствие 6. Количество $\pi \in \mathcal{P}_n^{\geqslant 4}$ с $|\mathcal{L}_3(\pi)| = 1$ не менее чем $\rho(1-\rho)2^n! + o(2^n!)$.

Доказательство. Обозначим через D_n количество функций из условия. Воспользуемся обозначениями $A_1, \dots, A_m$ из (7) и (8), а также суммой мощностей их пересечений T_n из (10). Тогда

$$D_n \geqslant |A_1| + \dots + |A_m| - 2T_n.$$

Действительно, если такая π принадлежит ровно k множествам из $A_1, \dots, A_m$ и $k = 1$, то функция будет учтена ровно один раз в обоих частях. Если $k \geqslant 2$, то до вычитания $2T_n$ будет учтена лишние k раз в правой части. Но затем при вычитании $2T_n$ данная функция будет вычтена $k(k-1)$ раз. Поскольку $k \leqslant k(k-1)$, то оценка верна. Согласно (7) и (13), получим

$$D_n \geqslant \rho|\mathcal{P}_n| - \rho^2|\mathcal{P}_n| + o(|\mathcal{P}_n|),$$

что влечёт оценку в следствии. ■

В табл. 2 приведены значения $|\mathcal{L}_k(S)|$, $2 \leqslant k \leqslant 5$, для S-блоков размера 8×8 различных шифров. Обратим внимание, что $|\mathcal{L}_6(S)| = |\mathcal{L}_7(S)| = 0$ для всех S из табл. 2. При построении S-блоков используются разные стратегии, поэтому данные значения имеют вариативность: некоторые схожи с таковыми у «случайных» функций, а некоторые — нет, см., например, S-блоки AES, ARIA и др., построенные с помощью инверсии элементов конечного поля ($|\mathcal{L}_k(S)|$ для них приведены в утверждении 3). Напомним, что утверждение 6 позволяет подсчитать среднее количество $\rho_{8,k}$ элементов в $\mathcal{L}_k(\pi)$ среди $\pi \in \mathcal{P}_8$:

$$\rho_{8,2} \approx 2730{,}7509881422924991,$$
$$\rho_{8,3} \approx 0{,}0235940660426061,$$
$$\sigma_{8,4} = \rho_{8,4} + \rho_{8,5} + \rho_{8,6} + \rho_{8,7} \approx 1{,}0240104891952223 \cdot 10^{-12}.$$

Таблица 2

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

S-блок	$\lvert\mathcal{L}_2(S)\rvert$	$\lvert\mathcal{L}_3(S)\rvert$	$\lvert\mathcal{L}_4(S)\rvert$	$\lvert\mathcal{L}_5(S)\rvert$	N_S	$\delta(S)$
AES/ARIA/Camellia/SM4/	85	0	17	0	112	4
CLEFIA S_1/SNOW 3G S_1/ZUC S_1	85	0	17	0	112	4
Fantomas	6444	79	0	0	96	16
FLY	5968	576	16	0	96	16
Fox (8-bit)	4854	225	3	0	96	16
Kuznechik	1953	0	2	0	100	8
Scream	3104	228	6	0	96	10
iScream	5472	466	2	5	96	16
SKINNY $\mathcal{S}_8$	22688	3648	320	24	64	64
SNOW 3G S_2	2570	2	1	0	96	8
ZUC S_0	3360	100	0	0	96	8
Zorro	2691	4	0	0	96	10
Anubis	2590	0	0	0	94	8
BelT	1666	0	0	0	102	8
Enocoro	2767	0	0	0	96	10
Iceberg	2669	0	0	0	96	8
Khazad	2768	0	0	0	96	8
Skipjack	2469	0	0	0	100	12
Turing	2617	0	0	0	94	12
Whirlpool	2579	0	0	0	100	8

ЛИТЕРАТУРА

1. *Clark W. E., Hou X., and Mihailovs A.* The affinity of a permutation of a finite vector space // Finite Fields Their Appl. 2007. V. 13. P. 80–112.
2. *Tokareva N.* Bent Functions: Results and Applications to Cryptography. N.Y.: Academic Press, 2015.
3. *Budaghyan L.* Construction and Analysis of Cryptographic Functions. Springer, Cham, 2015.
4. *Carlet C.* Boolean Functions for Cryptography and Coding Theory. Cambridge: Cambridge University Press, 2021.
5. *Логачев О. А., Сальников А. А., Смышляев С. В., Ященко В. В.* Булевы функции в теории кодирования и криптологии. М.: МЦНМО, 2012.
6. *Панкратова И. А.* Булевы функции в криптографии: учеб. пособие. Томск: Издательский Дом Томского государственного университета, 2014.
7. *Carlet C. and Piccione E.* On vectorial functions mapping strict affine subspaces of their domain into strict affine subspaces of their co-domain, and the strong D-property // Adv. Math. Commun. 2024. https://www.aimsciences.org/article/doi/10.3934/amc.2024025.
8. *Городилова А. А.* Характеризация почти совершенно нелинейных функций через подфункции // Дискретная математика. 2015. Т. 27. № 3. С. 3–16.
9. *Idrisova V.* On an algorithm generating 2-to-1 APN functions and its applications to "the big APN problem" // Cryptogr. Commun. 2019. V. 11. No. 1. P. 21–39.
10. *Beierle C., Leander G., and Perrin L.* Trims and extensions of quadratic APN functions // Des. Codes Cryptogr. 2022. V. 90. P. 1009–1036.
11. *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.
12. *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.

13. *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.
14. *Трифонов Д. И., Фомин Д. Б.* Об инвариантных подпространствах в XSL-шифрах // Прикладная дискретная математика. 2021. № 54. С. 58–76.
15. *Буров Д. А.* О существовании нелинейных инвариантов специального вида для раундовых преобразований XSL-алгоритмов // Дискретная математика. 2021. Т. 33. № 2. С. 31–45.
16. *Nyberg K.* Differentially uniform mappings for cryptography // LNCS. 1994. V. 765. P. 245–265.
17. *Charpin P.* Normal Boolean functions // J. Complexity. 2004. V. 20. No. 2–3. P. 245–265.
18. *Буряков М. Л., Логачев О. А.* Об уровне аффинности булевых функций // Дискретная математика. 2005. Т. 17. № 4. С. 98–107.
19. *Логачев О. А.* О значениях уровня аффинности для почти всех булевых функций // Прикладная дискретная математика. 2010. № 3(9). С. 17–21.
20. *Canteaut A., Carlet C., Charpin P., and Fontaine C.* On cryptographic properties of the cosets of $R(1, m)$ // IEEE Trans. Inform. Theory. 2001. V. 47. P. 1494–1513.
21. *Carlet C. and Feukoua S.* Three parameters of Boolean functions related to their constancy on affine spaces // Adv. Math. Commun. 2020. V. 14. No. 4. P. 651–676.
22. *Berger T., Canteaut A., Charpin P., and Laigle-Chapuy Y.* On almost perfect nonlinear functions // IEEE Trans. Inform. Theory. 2006. V. 52. No. 9. P. 4160–4170.
23. *Browning K. A., Dillon J. F., McQuistan M. T., and Wolfe A. J.* An APN permutation in dimension six // Finite Fields: Theory Appl. 2010. Iss. 518. P. 33–42.
24. *Li S., Meidl W., Polujan A., et al.* Vanishing flats: A combinatorial viewpoint on the planarity of functions and their application // IEEE Trans. Inform. Theory. 2020. V. 66. No. 11. P. 7101–7112.
25. *Blondeau C., Canteaut A., and Charpin P.* Differential properties of power functions // Int. J. Inform. Coding Theory. 2010. V. 1. No. 2. P. 149–170.
26. *Knuth D. E.* Subspaces, subsets, and partitions // J. Combinatorial Theory. Ser. A. 1971. V. 10. No. 2. P. 178–180.

REFERENCES

1. *Clark W. E., Hou X., and Mihailovs A.* The affinity of a permutation of a finite vector space. Finite Fields Their Appl., 2007, vol. 13, pp. 80–112.
2. *Tokareva N.* Bent Functions: Results and Applications to Cryptography. N.Y., Academic Press, 2015.
3. *Budaghyan L.* Construction and Analysis of Cryptographic Functions. Springer, Cham, 2015.
4. *Carlet C.* Boolean Functions for Cryptography and Coding Theory. Cambridge, Cambridge University Press, 2021.
5. *Logachev O. A., Salnikov A. A., and Yashchenko V. V.* Boolean Functions in Coding Theory and Cryptography. Providence, Rhode Island, AMS, 2012.
6. *Pankratova I. A.* Bulevy funktsii v kriptografii [Boolean Functions in Cryptography]. Tomsk, TSU Publ., 2014. (in Russian)
7. *Carlet C. and Piccione E.* On vectorial functions mapping strict affine subspaces of their domain into strict affine subspaces of their co-domain, and the strong D-property. Adv. Math. Commun., 2024, https://www.aimsciences.org/article/doi/10.3934/amc.2024025.
8. *Gorodilova A. A.* Characterization of almost perfect nonlinear functions in terms of subfunctions. Discrete Math. Appl., 2016, vol. 26, no. 4, pp. 193–202.

9. *Idrisova V.* On an algorithm generating 2-to-1 APN functions and its applications to "the big APN problem". Cryptogr. Commun., 2019, vol. 11, no. 1, pp. 21–39.
10. *Beierle C., Leander G., and Perrin L.* Trims and extensions of quadratic APN functions. Des. Codes Cryptogr., 2022, vol. 90, pp. 1009–1036.
11. *Kolomeec N. and Bykov D.* On the image of an affine subspace under the inverse function within a finite field. Des. Codes Cryptogr., 2024, vol. 92, pp. 467–476.
12. *Leander G., Abdelraheem M. A., AlKhzaimi H., and Zenner E.* A cryptanalysis of PRINTcipher: The invariant subspace attack. LNCS, 2011, vol. 6841, pp. 206–221.
13. *Todo Y., Leander G., and Sasaki Y.* Nonlinear invariant attack: practical attack on full SCREAM, iSCREAM, and Midori64. LNCS, 2016, vol. 10032, pp. 3–33.
14. *Trifonov D. I. and Fomin D. B.* Ob invariantnykh podprostranstvakh v XSL-shifrakh [Invariant subspaces in SPN block cipher]. Prikladnaya Diskretnaya Matematika, 2021, no. 54, pp. 58–76. (in Russian)
15. *Burov D. A.* On the existence of special nonlinear invariants for round functions of XSL-ciphers. Discrete Math. Appl., 2023, vol. 33, no. 2, pp. 65–75.
16. *Nyberg K.* Differentially uniform mappings for cryptography. LNCS, 1994, vol. 765, pp. 245–265.
17. *Charpin P.* Normal Boolean functions. J. Complexity, 2004, vol. 20, no. 2–3, pp. 245–265.
18. *Buryakov M. L. and Logachev O. A.* On the affinity level of Boolean functions. Discrete Math. Appl., 2005, vol. 15, no. 5, pp. 479–488.
19. *Logachev O. A.* O znacheniyakh urovnya affinnosti dlya pochti vsekh bulevykh funktsiy [On values of affinity level for almost all Boolean functions]. Prikladnaya Diskretnaya Matematika, 2010, no. 3(9), pp. 17–21. (in Russian)
20. *Canteaut A., Carlet C., Charpin P., and Fontaine C.* On cryptographic properties of the cosets of $R(1, m)$. IEEE Trans. Inform. Theory, 2001, vol. 47, pp. 1494–1513.
21. *Carlet C. and Feukoua S.* Three parameters of Boolean functions related to their constancy on affine spaces. Adv. Math. of Commun., 2020, vol. 14, no. 4, pp. 651–676.
22. *Berger T., Canteaut A., Charpin P., and Laigle-Chapuy Y.* On almost perfect nonlinear functions. IEEE Trans. Inform. Theory, 2006, vol. 52, no. 9, pp. 4160–4170.
23. *Browning K. A., Dillon J. F., McQuistan M. T., and Wolfe A. J.* An APN permutation in dimension six. Finite Fields: Theory Appl., 2010, iss. 518, pp. 33–42.
24. *Li S., Meidl W., Polujan A., et al.* Vanishing flats: A combinatorial viewpoint on the planarity of functions and their application. IEEE Trans. Inform. Theory, 2020, vol. 66, no. 11, pp. 7101–7112.
25. *Blondeau C., Canteaut A., and Charpin P.* Differential properties of power functions. Int. J. Inform. Coding Theory, 2010, vol. 1, no. 2, pp. 149–170.
26. *Knuth D. E.* Subspaces, subsets, and partitions. J. Combinatorial Theory, Ser. A, 1971, vol. 10, no. 2, pp. 178–180.

УДК 519.719.1 DOI 10.17223/20710410/65/2

ОБОБЩЁННЫЕ ТОЖДЕСТВА МЕДИАЛЬНОСТИ И ПАРАМЕДИАЛЬНОСТИ ДЛЯ СИЛЬНО ЗАВИСИМЫХ ОПЕРАЦИЙ

А. В. Черемушкин

Академия криптографии РФ, г. Москва, Россия

E-mail: avc238@mail.ru

Доказываются аналоги теорем о решении обобщённых тождеств медиальности и парамедиальности квазигрупп применительно к случаю сильно зависимых бинарных операций. Показано, что алгебры медиальных и парамедиальных сильно зависимых бинарных операций допускают описание, аналогичное случаю квазигрупп. В то же время ко-медиальные и ко-парамедиальные алгебры бинарных операций уже могут содержать нелинейные бинарные операции.

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

MEDIAL AND PARAMEDIAL GENERAL IDENTITIES FOR STRONG DEPENDANCE OPERATIONS

A. V. Cheremushkin

Academy of Cryptography of the Russian Federation, Moscow, Russia

We consider general functional medial and paramedial equations with four object variables. We give analogous of khown results with quasigroup operations for a class of strong dependable operations. As a consequence of these results, an analogous linear representation for every operation of a binary algebra satisfying one of these hyperidentities is obtained. Nevertheless, co-medial and co-paramedial algebras may have nonlinear binary operations.

Keywords: *n-ary quasigroup, strong dependent operation, medial and paramedial operations, linear representation.*

1. Необходимые определения

Пусть $n \geqslant 0$, $k \geqslant 2$ и $X = \{0, 1, \ldots, k-1\}$. Функция k-значной логики (n-арная 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 при фиксации любых $n-1$ переменных любыми значениями функция будет подстановкой по оставшейся переменной, то n-арный группоид (X, f) называется *n-квазигруппой*. Если $n = 2$ и $f = *$ — ассоциативная бинарная операция с единицей, то $(X, *)$ называется *моноидом*. Произведению подстановок $\alpha\beta$ соответствует запись

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

В работах автора [1–3] показано, что многие известные результаты, формулируемые на основе бесповторных (уравновешенных) тождеств и доказанные для n-квазигрупп,

переносятся на случай сильно зависимых операций. В данной работе продолжаются эти исследования и показано, что для сильно зависимых n-арных операций с условием парамедиальности также имеет место результат, полностью аналогичный доказанному для n-квазигрупп.

Группоид $(X, \cdot)$ с бинарной операцией $x \cdot y = xy$ называется *медиальным* (*парамедиальным*), если выполнено тождество

$$(xy)(uv) = (xu)(yv) \quad \big((xy)(uv) = (vy)(ux)\big).$$

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

Теорема 1 [9, теорема 3]. Любая конечная медиальная бинарная сильно зависимая операция $(\cdot)$ может быть представлена как линейная операция вида (1), у которой автоморфизмы ξ_1, ξ_2 удовлетворяют условию $\xi_1\xi_2 = \xi_2\xi_1$.

Теорема 2 [10, теорема 5]. Любая конечная парамедиальная бинарная сильно зависимая операция $(\cdot)$ может быть представлена как линейная операция вида (1), у которой автоморфизмы ξ_1, ξ_2 удовлетворяют условию $\xi_1^2 = \xi_2^2$.

Бинарная сильно зависимая операция $(\cdot)$ на множестве X называется *линейной*, если найдутся коммутативный моноид $(X, \circ)$ и обратимый элемент $b \in X$, такие, что при некоторых автоморфизмах ξ_1, ξ_2 моноида $(X, \circ)$ выполняется тождество

$$x \cdot y = \xi_1 x \circ \xi_2 y \circ b. \tag{1}$$

2. Обобщённые тождества медиальности и парамедиальности

Рассмотрим теперь обобщённые тождества медиальности и парамедиальности, которые имеют соответственно вид

$$f_1(f_2(x, y), f_3(u, v)) = f_4(f_5(x, u), f_6(y, v)); \tag{2}$$
$$f_1(f_2(x, y), f_3(u, v)) = f_4(f_5(v, y), f_6(u, x)). \tag{3}$$

Решение обобщённых тождеств медиальности и парамедиальности для случая бинарных квазигрупп приведено в работах [11–14].

Целью настоящей работы является доказательство того, что для случая сильно зависимых функций имеют место аналогичные утверждения, отличающиеся только тем, что в них термин «группа» следует заменить на термин «моноид».

Рассмотрим сначала случай обобщённого тождества медиальности.

Лемма 1. Пусть $(X, \circ)$ — моноид. Если выполнено тождество

$$\alpha(x) \circ \beta(y) = \gamma(y) \circ \delta(x),$$

где $\alpha, \beta, \gamma, \delta$ — некоторые подстановки, то операция $\circ$ коммутативная.

Доказательство. Пусть $e_\circ$ — нейтральный элемент моноида $(X, \circ)$. Подставляя в это тождество элементы x_0, y_0, удовлетворяющие равенствам $\alpha(x_0) = \beta(y_0) = e_\circ$, получаем

$$\alpha(x) = \gamma(y_0) \circ \delta(x), \quad \beta(y) = \gamma(y) \circ \delta(x_0),$$

где $\gamma(y_0)$ и $\delta(x_0)$ должны быть обратимыми элементами. Отсюда

$$\gamma(y_0) \circ \delta(x) \circ \gamma(y) \circ \delta(x_0) = \gamma(y) \circ \delta(x).$$

Произведём замену переменных $\gamma(y_0) \circ \delta(x) = w$, $\gamma(y) \circ \delta(x_0) = z$:

$$w \circ z = z \circ \delta(x_0)^{-1} \circ \gamma(y_0)^{-1} \circ w.$$

При $w = z = e_\circ$ получаем $\gamma(x_0)^{-1} \circ \delta(y_0)^{-1} = e_\circ$, откуда $w \circ z = z \circ w$. Коммутативность для произвольных w, z вытекает из взаимной однозначности соответствия $(x, y) \mapsto (w, z)$. ■

Теорема 3. Последовательность $(f_1, \ldots, f_6)$ сильно зависимых функций на конечном множестве X является решением обобщённого тождества медиальности (2) в том и только в том случае, когда существуют коммутативный моноид $(X, \circ)$ и биекции $\alpha_1, \ldots, \alpha_8$, такие, что

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

Доказательство. Обозначим функцию, стоящую в левой и правой части тождества (2), через $F(x, y, u, v)$. Поскольку эта функция допускает четыре простые декомпозиции с наборами переменных $\{x, y\}, \{u, v\}, \{x, u\}$ и $\{y, v\}$, то все переменные функции F эквивалентны. По теореме 6(i) из [15] каноническая декомпозиция этой функции должна иметь вид $\circ$-разложения $\alpha_1(x_{i_1}) \circ \alpha_2(x_{i_2}) \circ \alpha_3(x_{i_3}) \circ \alpha_4(x_{i_4})$, где $(X, \circ)$ — моноид; α_i — подстановки на множестве X, $1 \leqslant i \leqslant 4$; $\{x_{i_1}, x_{i_2}, x_{i_3}, x_{i_4}\} = \{x, y, u, v\}$.

Докажем коммутативность операции $\circ$. Так как каждая каноническая декомпозиция функции может быть получена путём доразбиения бесповторных декомпозиций, стоящих в левой и правой частях тождества (2), то для порядка переменных возможны два варианта:

$$\alpha_1(x) \circ \alpha_2(y) \circ \alpha_3(u) \circ \alpha_4(v) = \beta_1(x) * \beta_2(u) * \beta_3(y) * \beta_4(v),$$

где моноиды $(X, \circ)$ и $(X, *)$ в силу теоремы 7(1) из [15] должны быть связаны соотношениями вида $x * y = x \circ a \circ y$ либо $x * y = y \circ b \circ x$ при некоторых обратимых элементах a, b моноида $(X, \circ)$.

В первом случае получаем тождество

$$\alpha_1(x) \circ \alpha_2(y) \circ \alpha_3(u) \circ \alpha_4(v) = \beta_1(x) \circ a \circ \beta_2(u) \circ a \circ \beta_3(y) \circ a \circ \beta_4(v).$$

Заменив, где это необходимо, подстановки $\beta_i(.) \circ a$ на $\beta_i'(.)$, достаточно ограничиться рассмотрением тождества

$$\alpha_1(x) \circ \alpha_2(y) \circ \alpha_3(u) \circ \alpha_4(v) = \beta_1(x) \circ \beta_2(u) \circ \beta_3(y) \circ \beta_4(v).$$

Выберем значения $x = x_0$ и $v = v_0$ так, чтобы $\alpha_1(x_0) = \alpha_4(v_0) = e_\circ$ — единичный элемент моноида $(X, \circ)$. Тогда

$$\alpha_2(y) \circ \alpha_3(u) = \beta_1(e_\circ) \circ \beta_2(u) \circ \beta_3(y) \circ \beta_4(e_\circ).$$

Из леммы 1 следует коммутативность операции $\circ$.

Во втором случае аналогично получаем тождество

$$\alpha_1(x) \circ \alpha_2(y) \circ \alpha_3(u) \circ \alpha_4(v) = \beta_4(v) \circ \beta_3(y) \circ \beta_2(u) \circ \beta_1(x).$$

Выберем значения $y = y_0$ и $u = u_0$ так, чтобы $\alpha_2(y_0) = \alpha_3(u_0) = e_\circ$, тогда

$$\alpha_1(x) \circ \alpha_4(v) = \beta_4(v) \circ \beta_3(e_\circ) \circ \beta_2(e_\circ) \circ \beta_1(x).$$

Аналогично в силу леммы 1 получаем коммутативность операции $\circ$.

Теперь по теореме 7(1) из [15] получаем, что достаточно рассмотреть случай, когда левая функция из тождества (2) допускает каноническую декомпозицию вида

$$f_1(f_2(x,y), f_3(u,v)) = \alpha_1(x) \circ \alpha_2(y) \circ \alpha_3(u) \circ \alpha_4(v). \tag{4}$$

Подставляя в это тождество значения $u = u_0$ и $v = v_0$, такие, что $\alpha_3(u_0) = \alpha_4(v_0) = e_\circ$, получаем

$$f_1(f_2(x,y), f_3(u_0,v_0)) = \alpha_1(x) \circ \alpha_2(y).$$

Поскольку в правой части стоит сильно зависимая функция, то унарная операция $f_1(w, f_3(u_0,v_0)) = \alpha_5(w)$ должна быть подстановкой, удовлетворяющей равенству $f_2(x,y) = \alpha_5^{-1}(\alpha_1 x \circ \alpha_2 y)$.

Аналогично рассуждая, получаем, что унарная операция $f_1(f_2(x_0,y_0),w) = \alpha_6(w)$ также является подстановкой и удовлетворяет равенству $f_3(u,v) = \alpha_6^{-1}(\alpha_3 u \circ \alpha_4 v)$.

Возвращаясь к равенству (4), убеждаемся, что $f_1(x,z) = \alpha_5 x \circ \alpha_6 z$.

Рассматривая правую часть тождества (2), аналогично получаем при некоторых подстановках α_7 и α_8 равенства

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

Теорема доказана. ■

Получим аналогичное описание для тождества парамедиальности.

Теорема 4. Последовательность $(f_1, \ldots, f_6)$ сильно зависимых функций на конечном множестве X является решением обобщённого тождества парамедиальности (3) в том и только в том случае, когда существует коммутативный моноид $(X, \circ)$ и биекции $\alpha_1, \ldots, \alpha_8$, такие, что выполняются равенства

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

Доказательство. Поступаем аналогично. Так как все переменные функции, стоящей в левой и правой частях тождества (2), эквивалентны, то по теореме 6(i) из [15] каноническая декомпозиция этой функции должна иметь вид $\circ$-разложения $\alpha_1(x_{i_1}) \circ \alpha_2(x_{i_2}) \circ \alpha_3(x_{i_3}) \circ \alpha_4(x_{i_4})$, где $(X, \circ)$ — моноид; α_i — подстановки на множестве X, $1 \leqslant i \leqslant 4$; $\{x_{i_1}, x_{i_2}, x_{i_3}, x_{i_4}\} = \{x, y, u, v\}$.

Докажем коммутативность операции $\circ$. Так как каждая каноническая декомпозиция функции может быть получена путём доразбиения некоторой бесповторной декомпозиции, то из тождества (2) следует, что для порядка переменных возможны два варианта:

$$\alpha_1(x) \circ \alpha_2(y) \circ \alpha_3(u) \circ \alpha_4(v) = \beta_1(v) * \beta_2(y) * \beta_3(u) * \beta_4(x),$$

где моноиды $(X, \circ)$ и $(X, *)$ в силу теоремы 7(1) из [15] могут быть связаны соотношениями вида $x * y = x \circ a \circ y$ либо $x * y = y \circ b \circ x$ при некоторых обратимых элементах a, b моноида $(X, \circ)$.

В первом случае получаем тождество

$$\alpha_1(x) \circ \alpha_2(y) \circ \alpha_3(u) \circ \alpha_4(v) = \beta_1(v) \circ a \circ \beta_2(y) \circ a \circ \beta_3(u) \circ a \circ \beta_4(x).$$

Заменив, где это необходимо, подстановки $\beta_i(.) \circ a$ на $\beta'_i(.)$, достаточно ограничиться рассмотрением тождества

$$\alpha_1(x) \circ \alpha_2(y) \circ \alpha_3(u) \circ \alpha_4(v) = \beta_1(v) \circ \beta_2(y) \circ \beta_3(u) \circ \beta_4(x).$$

Выберем значения $y = y_0$ и $u = u_0$ так, чтобы $\alpha_2(y_0) = \alpha_3(u_0) = e_\circ$ — единичный элемент моноида $(X, \circ)$, тогда

$$\alpha_1(x) \circ \alpha_4(v) = \beta_1(v) \circ \beta_2(e_\circ) \circ \beta_3(e_\circ) \circ \beta_4(x).$$

Из леммы 1 следует коммутативность операции $\circ$.

Во втором случае аналогично получаем тождество

$$\alpha_1(x) \circ \alpha_2(y) \circ \alpha_3(u) \circ \alpha_4(v) = \beta_4(x) \circ \beta_3(u) \circ \beta_2(y) \circ \beta_1(v).$$

Выберем значения $x = x_0$ и $v = v_0$, такие, что $\alpha_1(x_0) = \alpha_4(v_0) = e_\circ$, тогда

$$\alpha_2(y) \circ \alpha_3(u) = \beta_4(e_\circ) \circ \beta_3(u) \circ \beta_2(y) \circ \beta_1(e_\circ).$$

Аналогично в силу леммы 1 получаем коммутативность операции $\circ$.

По теореме 7(1) из [15] получаем, что достаточно рассмотреть случай, когда левая функция из тождества (2) допускает каноническую декомпозицию вида

$$f_1(f_2(x, y), f_3(u, v)) = \alpha_1(x) \circ \alpha_2(y) \circ \alpha_3(u) \circ \alpha_4(v). \tag{5}$$

Подставляя в это тождество значения $u = u_0$ и $v = v_0$, такие, что $\alpha_3(u_0) = \alpha_4(v_0) = e_\circ$, получаем

$$f_1(f_2(x, y), f_3(u_0, v_0)) = \alpha_1(x) \circ \alpha_2(y).$$

Поскольку в правой части стоит сильно зависимая функция, то унарная операция $f_1(w, f_3(u_0, v_0)) = \alpha_5(w)$ должна быть подстановкой, удовлетворяющей равенству $f_2(x, y) = \alpha_5^{-1}(\alpha_1 x \circ \alpha_2 y)$.

Аналогично рассуждая, получаем, что унарная операция $f_1(f_2(x_0, y_0), w) = \alpha_6(w)$ также является подстановкой и удовлетворяет равенству $f_3(u, v) = \alpha_6^{-1}(\alpha_3 u \circ \alpha_4 v)$.

Возвращаясь к равенству (5), убеждаемся, что $f_1(x, z) = \alpha_5 x \circ \alpha_6 z$.

Рассматривая правую часть тождества (2), полностью аналогично получаем при некоторых подстановках α_7 и α_8 равенства

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

Теорема доказана. ■

Замечание 1. В работе [16] исследован вопрос об однозначности решения тождества (2) относительно набора квазигрупповых бинарных операций $(f_1, \ldots, f_6)$. Показано, что набор $(+, \alpha_1, \ldots, \alpha_8)$, с помощью которого описываются эти функции, определяется по ним неоднозначно. Например, при любом автоморфизме θ абелевой группы $(X, +)$ последовательность $(+, \theta\alpha_1, \ldots, \theta\alpha_8)$ определяет то же решение. Для получения однозначного (канонического) вида решения достаточно зафиксировать произвольный элемент $a \in X$, который будет играть роль нейтрального элемента для изоморфного представления $(X, *, a)$ группы $(X, +, 0)$, и потребовать, чтобы $\alpha_1 a = \alpha_5 a = \alpha_7 a = a$. Аналогичный результат справедлив и для сильно зависимых функций.

3. Применение к алгебрам двуместных функций

Приведём несколько следствий. Пусть $\mathcal{F}_2\colon X^2 \to X$ — множество двуместных функций. Рассмотрим несколько обобщённых функциональных тождеств, в которых участвует две функции $f, g \in \mathcal{F}_2$:

$$\begin{array}{ll}(a) & f(g(x,y),g(u,v)) = g(f(x,u),f(y,v)) \quad (\textit{mediality}),\\ (b) & f(g(x,y),g(u,v)) = g(f(v,y),f(u,x)) \quad (\textit{paramediality}),\\ (c) & f(g(x,y),g(u,v)) = f(g(x,u),g(y,v)) \quad (\textit{co-mediality}),\\ (d) & f(g(x,y),g(u,v)) = f(g(v,y),g(u,x)) \quad (\textit{co-paramediality}).\end{array}$$

Определение 1. Пусть $F \subset \mathcal{F}_2$. Если для любых $f, g \in F$ выполняется тождество (a), то алгебра (X, F) называется *медиальной*; если тождество (b), то — *парамедиальной*; если тождество (c), то — *ко-медиальной*; если тождество (d), то — *ко-парамедиальной*.

Алгебры с квазигрупповыми операциями исследованы в работах [13, 14, 17, 18] и др. Описание всех таких алгебр для случая бинарных квазигрупповых операций приведено, в частности, в работе [6]. Показано, что для всех случаев алгебры состоят только из операций, допускающих линейные представления. Например, для случая медиальных бинарных квазигрупповых операций справедлива

Теорема 5 [17, теорема 1]. Если алгебра $(X, \{h_1, \dots, h_m\})$, где $h_1, \dots, h_m$ — 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

$$\alpha_i\beta_j = \beta_j\alpha_i, \quad \alpha_i\alpha_j = \alpha_j\alpha_i, \quad \beta_i\beta_j = \beta_j\beta_i \quad \text{при всех} \quad i, j = 1, \dots, m.$$

Группа $(X, +)$ определена однозначно с точностью до изоморфизма.

Заметим, что в [19] описаны алгебры, удовлетворяющие тождествам вида (a) и (b), в которых применены всевозможные перестановки переменных в правой части.

В данной работе, в отличие от обычного определения, предполагается, что функции f, g должны быть различными. Если допустить совпадение функций $f = g$, то мы попадаем в условия теорем 1 и 2, из которых следует, что все функции в алгебре должны иметь соответствующее линейное представление. Если же исходить из того, что $f \neq g$, то, как показано ниже в теоремах 8 и 9, в случаях (c) и (d) возможны алгебры с функциями, не имеющими линейного представления.

Покажем, что из теорем 3 и 4 для алгебр сильно зависимых бинарных операций в случаях (c) и (d) следует аналогичное описание. Нам потребуется описание групп автотопий коммутативных моноидов.

Лемма 2.

1) Группа автотопий $\mathrm{Atp}(\circ)$ коммутативного моноида $(X, \circ)$ состоит из преобразований вида

$$(\alpha, \beta, \gamma) = (\xi, \xi, \xi)(R_a, R_b, R_c) = (\xi R_a, \xi R_b, \xi R_c),$$

где $\xi \in \mathrm{Aut}(\circ)$ — некоторый автоморфизм и $a, b \in X$ — обратимые элементы, $c = a \circ b$, или иначе

$$\gamma^{-1}(\alpha x \circ \beta y) = \xi^{-1}(\xi(x) \circ a \circ \xi(y) \circ b \circ c^{-1}) = x \circ y.$$

Если $e \in X$ — единица моноида, то $(\alpha(e), \beta(e), \gamma(e)) = (a, b, c)$.

2) Если для коммутативного моноида $(X, \circ)$ и преобразований изотопии $(\alpha_i, \beta_i, \gamma_i)$, $i = 1, 2$, выполняется тождество

$$\gamma_1^{-1}(\alpha_1 x \circ \beta_1 y) = \gamma_2^{-1}(\alpha_2 x \circ \beta_2 y),$$

то для некоторого автоморфизма $\xi \in \mathrm{Aut}(\circ)$ и обратимых элементов $a, b \in X$ и $c = a \circ b$ выполнено равенство

$$(\alpha_1, \beta_1, \gamma_1) = (\xi, \xi, \xi)(R_a, R_b, R_c)(\alpha_2, \beta_2, \gamma_2) = (\xi R_a \alpha_2, \xi R_b \beta_2, \xi R_c \gamma_2),$$

или в другой форме

$$(\alpha_1(x), \beta_1(y), \gamma_1(z)) = (\xi(\alpha_2(x)) \circ a, \xi(\beta_2(y)) \circ b, \xi(\gamma_2(z)) \circ c).$$

Доказательство получается как следствие теоремы 3 из [15]. Напомним, что каждая компонента автотопии моноида $(X, \circ)$ является *квазиавтоморфизмом*, т. е. представима в виде $\psi(x) \circ b$ при некотором автоморфизме моноида $\psi(x)$ и обратимом элементе $b \in X$. Все квазиавтоморфизмы моноида образуют группу $\mathrm{Hol}(\circ)$, являющуюся полупрямым произведением группы автоморфизмов $\mathrm{Aut}(\circ)$ и подгруппы обратимых элементов моноида.

Теорема 6. 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 $1 \leqslant i, j \leqslant m$. Моноид $(X, \circ)$ определён однозначно с точностью до изоморфизма.

Доказательство. Пусть $f, g \in \{h_1, \ldots, h_m\}$ — произвольная пара функций, удовлетворяющая тождеству (a). Применим к этому тождеству теорему 3. Имеем $f = f_1 = f_5 = f_6$ и $g = f_2 = f_3 = f_4$, причём

$$f(x, y) = \alpha_5 x \circ \alpha_6 y = \alpha_7^{-1}(\alpha_1 x \circ \alpha_3 y) = \alpha_8^{-1}(\alpha_2 x \circ \alpha_4 y),$$
$$g(x, y) = \alpha_5^{-1}(\alpha_1 x \circ \alpha_2 y) = \alpha_6^{-1}(\alpha_3 x \circ \alpha_4 y) = \alpha_7 x \circ \alpha_8 y.$$

Значит, изотопии $(\alpha_5, \alpha_6, \mathrm{id})$, $(\alpha_1, \alpha_3, \alpha_7)$ и $(\alpha_2, \alpha_4, \alpha_8)$ лежат в одном смежном классе по группе автотопий моноида $(X, \circ)$ (здесь через id обозначено тождественное отображение). Отсюда по лемме 2 получаем, что при некоторых автоморфизмах ξ_1, ξ_2 справедливы равенства

$$(\alpha_1, \alpha_3, \alpha_7) = (\xi_1, \xi_1, \xi_1)(R_{a_1}, R_{b_1}, R_{c_1})(\alpha_5, \alpha_6, \mathrm{id}) = (\xi_1 R_{a_1} \alpha_5, \xi_1 R_{b_1} \alpha_6, \xi_1 R_{c_1}),$$
$$(\alpha_2, \alpha_4, \alpha_8) = (\xi_2, \xi_2, \xi_2)(R_{a_2}, R_{b_2}, R_{c_3})(\alpha_5, \alpha_6, \mathrm{id}) = (\xi_2 R_{a_2} \alpha_5, \xi_2 R_{b_2} \alpha_6, \xi_2 R_{c_2}).$$

Аналогично получаем, что при некоторых автоморфизмах ξ_3, ξ_4 справедливы равенства

$$(\alpha_1, \alpha_2, \alpha_5) = (\xi_3 R_{a_3} \alpha_7, \xi_3 R_{a_3} \alpha_8, \xi_3 R_{a_3}),$$
$$(\alpha_3, \alpha_4, \alpha_6) = (\xi_4 R_{a_4} \alpha_7, \xi_4 R_{a_4} \alpha_8, \xi_4 R_{a_4}).$$

Отсюда $\alpha_7 = \xi_1 R_{c_1}$, $\alpha_8 = \xi_2 R_{c_2}$, $\alpha_5 = \xi_3 R_{a_3}$, $\alpha_6 = \xi_4 R_{a_4}$, причём

$$\alpha_1 = \xi_1 R_{a_1}\alpha_5 = \xi_3 R_{a_3}\alpha_7, \quad \alpha_2 = \xi_2 R_{a_2}\alpha_5 = \xi_3 R_{a_3}\alpha_8,$$
$$\alpha_3 = \xi_1 R_{b_1}\alpha_6 = \xi_4 R_{a_4}\alpha_7, \quad \alpha_4 = \xi_2 R_{b_2}\alpha_6 = \xi_4 R_{a_4}\alpha_8,$$

или иначе

$$\alpha_1 = \xi_1 R_{a_1}\xi_3 R_{a_3} = \xi_3 R_{a_3}\xi_1 R_{c_1}, \quad \alpha_2 = \xi_2 R_{a_2}\xi_3 R_{a_3} = \xi_3 R_{a_3}\xi_2 R_{c_2},$$
$$\alpha_3 = \xi_1 R_{b_1}\xi_4 R_{a_4} = \xi_4 R_{b_4}\xi_1 R_{c_1}, \quad \alpha_4 = \xi_2 R_{b_2}\xi_4 R_{a_4} = \xi_4 R_{b_4}\xi_2 R_{c_2}.$$

Отсюда, вычисляя значение этих биекций на единичном элементе, получаем

$$\begin{gathered} a_1 = c_1, \quad b_1 = e, \quad \xi_1\xi_3 = \xi_3\xi_1, \\ a_2 = c_2, \quad b_2 = e, \quad \xi_2\xi_3 = \xi_3\xi_2, \\ a_3 = c_1 \circ b_4, \quad \xi_1\xi_4 = \xi_4\xi_1, \\ a_4 = c_2 \circ b_4, \quad \xi_2\xi_4 = \xi_4\xi_2. \end{gathered} \tag{6}$$

Таким образом, $\alpha_1, \ldots, \alpha_8 \in \mathrm{Hol}(\circ)$ — квазиавтоморфизмы моноида $(Q, \circ)$.

Осталось привести полученные представления к виду, приведённому в формулировке теоремы 6. Введём новые обозначения для автоморфизмов, участвующих в записи функций f и g:

$$f(x,y) = \alpha_5 x \circ \alpha_6 y = \xi_3 R_{a_3} x \circ \xi_4 R_{a_4} y = \xi_3 x \circ \xi_4 y \circ a_3 \circ a_4 = \alpha'_1 x \circ \beta'_1 y \circ c'_1,$$
$$g(x,y) = \alpha_7 x \circ \alpha_8 y = \xi_1 R_{c_1} x \circ \xi_2 R_{c_2} y = \xi_1 x \circ \xi_2 y \circ c_1 \circ c_2 = \alpha'_2 x \circ \beta'_2 y \circ c'_2,$$

где $\alpha'_1 = \xi_3$, $\alpha'_2 = \xi_1$, $\beta'_1 = \xi_4$, $\beta'_2 = \xi_2$, $c'_1 = c_3 \circ c_4$, $c'_2 = c_1 \circ c_2$. Теперь равенства для автоморфизмов из (6) можно переписать в виде

$$\alpha'_1\alpha'_2 = \alpha'_2\alpha'_1, \quad \beta'_2\alpha'_1 = \alpha'_1\beta'_2, \quad \alpha'_2\beta'_1 = \beta'_1\alpha'_2, \quad \beta'_1\beta'_2 = \beta'_2\beta'_1.$$

При этом должно выполняться $f(c'_2, c'_2) = g(c'_1, c'_1)$. ■

Теорема 7. 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 $1 \leqslant i, j \leqslant m$. Моноид $(X, \circ)$ определён однозначно с точностью до изоморфизма.

Доказательство. Пусть $f, g \in \{h_1, \ldots, h_m\}$ — произвольная пара функций. Она должна удовлетворять тождеству (b). Применим к этому тождеству теорему 4. Имеем $f = f_1 = f_5 = f_6$ и $g = f_2 = f_3 = f_4$, или

$$f(x,y) = \alpha_5 x \circ \alpha_6 y = \alpha_7^{-1}(\alpha_4 x \circ \alpha_2 y) = \alpha_8^{-1}(\alpha_3 x \circ \alpha_1 y),$$
$$g(x,y) = \alpha_5^{-1}(\alpha_1 x \circ \alpha_2 y) = \alpha_6^{-1}(\alpha_3 x \circ \alpha_4 y) = \alpha_7 x \circ \alpha_8 y.$$

Значит, изотопии $(\alpha_5, \alpha_6, \mathrm{id})$, $(\alpha_4, \alpha_2, \alpha_7)$ и $(\alpha_3, \alpha_1, \alpha_8)$ лежат в одном смежном классе по группе автотопий моноида $(X, \circ)$. Отсюда по лемме 2 получаем, что при некоторых автоморфизмах ξ_1, ξ_2 справедливы равенства

$$(\alpha_4, \alpha_2, \alpha_7) = (\xi_1, \xi_1, \xi_1)(R_{a_1}, R_{b_1}, R_{c_1})(\alpha_5, \alpha_6, \mathrm{id}) = (\xi_1 R_{a_1}\alpha_5, \xi_1 R_{a_2}\alpha_6, \xi_1 R_{c_1}),$$
$$(\alpha_3, \alpha_1, \alpha_8) = (\xi_2, \xi_2, \xi_2)(R_{a_2}, R_{b_2}, R_{c_2})(\alpha_5, \alpha_6, \mathrm{id}) = (\xi_2 R_{a_2}\alpha_5, \xi_2 R_{b_2}\alpha_6, \xi_2 R_{c_2}).$$

Аналогично получаем, что при некоторых автоморфизмах ξ_3, ξ_4 справедливы равенства

$$(\alpha_1, \alpha_2, \alpha_5) = (\xi_3 R_{a_3}\alpha_7, \xi_3 R_{b_3}\alpha_8, \xi_3 R_{c_3}), \quad (\alpha_3, \alpha_4, \alpha_6) = (\xi_4 R_{a_4}\alpha_7, \xi_4 R_{b_4}\alpha_8, \xi_4 R_{c_4}).$$

Тогда $\alpha_7 = \xi_1 R_{c_1}$, $\alpha_8 = \xi_2 R_{c_2}$, $\alpha_5 = \xi_3 R_{c_3}$, $\alpha_6 = \xi_4 R_{c_4}$, причём

$$\alpha_1 = \xi_3 R_{a_3}\xi_1 R_{c_1} = \xi_2 R_{b_2}\xi_4 R_{c_4}, \quad \alpha_2 = \xi_1 R_{a_2}\xi_4 R_{c_4} = \xi_3 R_{b_3}\xi_2 R_{c_2},$$
$$\alpha_3 = \xi_2 R_{a_2}\xi_3 R_{c_3} = \xi_4 R_{a_4}\xi_1 R_{c_1}, \quad \alpha_4 = \xi_1 R_{a_1}\xi_3 R_{c_3} = \xi_4 R_{b_4}\xi_2 R_{c_2}.$$

Вычисляя значения этих биекций на единичном элементе моноида, получаем

$$\begin{aligned} c_1 \circ a_3 &= c_4 \circ b_2, \quad & \xi_3\xi_1 &= \xi_2\xi_4, \\ c_4 \circ a_2 &= c_2 \circ b_3, \quad & \xi_1\xi_4 &= \xi_3\xi_2, \\ c_3 \circ a_2 &= c_1 \circ a_4, \quad & \xi_2\xi_3 &= \xi_4\xi_1, \\ c_3 \circ a_1 &= c_2 \circ b_4, \quad & \xi_1\xi_3 &= \xi_4\xi_2. \end{aligned} \tag{7}$$

Таким образом, $\alpha_1, \ldots, \alpha_8$ являются автоморфизмами моноида $(Q, \circ)$.

Осталось привести полученные представления к виду, приведенному в формулировке теоремы 7:

$$f(x, y) = \alpha_5 x \circ \alpha_6 y = \xi_3 R_{c_3} x \circ \xi_4 R_{c_4} y = \xi_3 x \circ \xi_4 y \circ c_3 \circ c_4 = \alpha'_1 x \circ \beta'_1 y \circ c'_1,$$
$$g(x, y) = \alpha_7 x \circ \alpha_8 y = \xi_1 R_{c_1} x \circ \xi_2 R_{c_2} y = \xi_1 x \circ \xi_2 y \circ c_1 \circ c_2 = \alpha'_2 x \circ \beta'_2 y \circ c'_2,$$

где $\alpha'_1 = \xi_3$, $\alpha'_2 = \xi_1$, $\beta'_1 = \xi_4$, $\beta'_2 = \xi_2$, $c'_1 = c_3 \circ c_4$, $c'_2 = c_1 \circ c_2$. Теперь равенства (7) можно переписать в виде

$$\alpha'_2\alpha'_1 = \beta'_1\beta'_2, \quad \alpha'_2\beta'_1 = \alpha'_1\beta'_2, \quad \beta'_2\alpha'_1 = \beta'_1\alpha'_2, \quad \alpha'_1\alpha'_2 = \beta'_2\beta'_1.$$

Необходимость выполнения равенства $h_j(c'_i, c'_i) = h_i(c'_j, c'_j)$ очевидна. ■

Перейдём к рассмотрению тождеств ко-медиальности и ко-парамедиальности. Вначале приведем критерий для свойства квазиавтоморфизма.

Лемма 3. Пусть $\phi : X \to X$ — биекция и $(X, \circ)$ — коммутативный моноид. Тогда тождество

$$\phi(x \circ y) \circ \phi(e) = \phi(x) \circ \phi(y)$$

выполняется в том и только в том случае, когда $\phi(x) = \alpha(x) \circ b$ при некотором автоморфизме $\alpha \in \mathrm{Aut}(\circ)$ и обратимом элементе b моноида $(X, \circ)$.

Доказательство. Достаточность очевидна. Докажем необходимость. Единица моноида является обратимым элементом. Покажем, что $\phi(e)$ — также обратимый элемент моноида $(X, \circ)$. По условию $\phi(x \circ y) \circ \phi(e) = \phi(x) \circ \phi(y)$, причём ϕ — биекция. Выберем y_0 так, что $\phi(y_0) = e$. Тогда

$$\phi(x \circ y_0) \circ \phi(e) = \phi(x).$$

Справа стоит подстановка, значит, слева тоже должна быть подстановка. Поэтому $\phi(e)$ должен быть обратимым элементом.

Рассмотрим $\alpha(x) = \phi(x) \circ \phi(e)^{-1}$. Имеем

$$\alpha(x \circ y) = \phi(x \circ y) \circ \phi(e)^{-1} = (\phi(x) \circ \phi(y) \circ \phi(e)^{-1}) \circ \phi(e)^{-1} = \alpha(x) \circ \alpha(y).$$

Значит, α — эндоморфизм моноида $(X, \circ)$. С другой стороны, $\phi(x) = \alpha(x) \circ \phi(e)$ — биекция. Поэтому α должен быть автоморфизмом. ■

Утверждение 1. Если f, g — сильно зависимые бинарные операции, удовлетворяющие тождеству (c) ко-медиальности, то существует 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.

Доказательство. Имеем $f = f_1 = f_4$ и $g = f_2 = f_3 = f_5 = f_6$, или

$$f(x, y) = \alpha_5 x \circ \alpha_6 y = \alpha_7 x \circ \alpha_8 y,$$
$$g(x, y) = \alpha_5^{-1}(\alpha_1 x \circ \alpha_2 y) = \alpha_6^{-1}(\alpha_3 x \circ \alpha_4 y) = \alpha_7^{-1}(\alpha_1 x \circ \alpha_3 y) = \alpha_8^{-1}(\alpha_2 x \circ \alpha_4 y),$$

при этом

$$f(g(x, y), g(u, v)) = \alpha_1 x \circ \alpha_2 y \circ \alpha_3 u \circ \alpha_4 v,$$
$$f(g(x, u), g(y, v)) = \alpha_1 x \circ \alpha_2 u \circ \alpha_3 y \circ \alpha_4 v.$$

Поэтому для выполнения тождества ко-медиальности необходимо, чтобы $\alpha_2 = \alpha_3$.

Из совпадения функций следует, что преобразования изотопии $(\alpha_5, \alpha_6, \mathrm{id})$ и $(\alpha_7, \alpha_8, \mathrm{id})$, а также $(\alpha_1, \alpha_2, \alpha_5)$, $(\alpha_3, \alpha_4, \alpha_6)$, $(\alpha_1, \alpha_3, \alpha_7)$ и $(\alpha_2, \alpha_4, \alpha_8)$ лежат в одних смежных классах по группе автотопий моноида $(X, \circ)$. Поэтому по лемме 2 получаем, что при некоторых автоморфизмах ξ_1, ξ_2, ξ_3 справедливы равенства

$$(\alpha_1, \alpha_2, \alpha_5) = (\xi_1 R_{a_1} \alpha_3, \xi_1 R_{b_1} \alpha_4, \xi_1 R_{c_1} \alpha_6) = (\xi_2 R_{a_2} \alpha_1, \xi_2 R_{b_2} \alpha_3, \xi_2 R_{c_2} \alpha_7) =$$
$$= (\xi_3 R_{a_3} \alpha_2, \xi_3 R_{b_3} \alpha_4, \xi_3 R_{c_3} \alpha_8),$$
$$(\alpha_5, \alpha_6, \mathrm{id}) = (R_{a_4} \alpha_7, R_{b_4} \alpha_8, \mathrm{id}), \quad a_4 \circ b_4 = e.$$

Отсюда

$$\alpha_1 = \xi_1 R_{a_1} \alpha_3 = \xi_2 R_{a_2} \alpha_1 = \xi_3 R_{a_3} \alpha_2,$$
$$\alpha_2 = \xi_1 R_{b_1} \alpha_4 = \xi_2 R_{b_2} \alpha_3 = \xi_3 R_{b_3} \alpha_4,$$
$$\alpha_5 = \xi_1 R_{c_1} \alpha_6 = \xi_2 R_{c_2} \alpha_7 = \xi_3 R_{c_3} \alpha_8 = R_{a_4} \alpha_7,$$
$$\alpha_6 = R_{b_4} \alpha_8.$$

Заметим, что:

— $\alpha_1 = \xi_2 R_{a_2} \alpha_1$, откуда $a_2 = e$, $\xi_2 = e$;
— $\alpha_5 = R_{a_4} \alpha_7 = \xi_2 R_{c_2} \alpha_7$, откуда $\xi_2 = \mathrm{id}$, $a_4 = c_2$;
— $\alpha_5 = \xi_1 R_{c_1} R_{b_4} \alpha_8 = \xi_3 R_{c_3} \alpha_8$, откуда $b_4 \circ c_1 = c_3$, $\xi_1 = \xi_3$;
— $\alpha_2 = \xi_1 R_{b_1} \alpha_4 = \xi_3 R_{b_3} \alpha_4$, откуда $b_1 = b_3$;
— $\alpha_3 = R_{b_2}^{-1} \alpha_2$, откуда $b_2 = e$.

Таким образом, $\alpha_1 = \xi_1 R_{a_3}\alpha_2$, $\alpha_3 = \alpha_2$, $\alpha_4 = R_{b_3}^{-1}\xi_1^{-1}\alpha_2$, $\alpha_5 = \xi_1 R_{c_1}\alpha$, а значит,

$$f(x,y) = \alpha_5 x \circ \alpha_6 y = \xi_1 R_{c_1}\alpha_6 x \circ \alpha_6 y,$$
$$g(x,y) = \alpha_5^{-1}(\alpha_1 x \circ \alpha_2 y) = \alpha_5^{-1}(\xi_1 R_{a_3}\alpha_2 x \circ \alpha_2 y) =$$
$$= \alpha_6^{-1}(\alpha_3 x \circ \alpha_4 y) = \alpha_6^{-1}(\alpha_2 x \circ R_{b_3}^{-1}\xi_1^{-1}\alpha_2 y).$$

При этом

$$f(g(x,u),g(y,v)) = (\alpha_1 x \circ \alpha_2 u) \circ (\alpha_3 y \circ \alpha_4 v) = \xi_1 R_{a_3}\alpha_2 x \circ \alpha_2 u \circ \alpha_2 y \circ R_{b_3}^{-1}\xi_1^{-1}\alpha_2 v.$$

После замены обозначений $\alpha_2 = \beta$, $\alpha_6 = \alpha$, $\xi_1 = \xi$, $c_1 = c$, $a_3 = a$, $b_3 = b$ получаем требуемые равенства

$$f(x,y) = \xi R_c\alpha x \circ \alpha y = \xi R_c\alpha x \circ \alpha y,$$
$$g(x,y) = (\xi R_c\alpha)^{-1}(\xi R_{a_3}\beta x \circ \beta y) = \alpha^{-1}(\beta x \circ R_b^{-1}\xi^{-1}\beta y).$$

Заметим, что функция g должна удовлетворять условию

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

или после замены переменной $\beta y' = R_b^{-1}\xi^{-1}\beta y$

$$\alpha^{-1}R_c^{-1}\xi^{-1}(R_a\beta x \circ \xi R_b\beta y') = \alpha^{-1}(\beta x \circ \beta y').$$

Отсюда следует, что должно выполняться равенство $c = a \circ b$, что вытекает из того, что тройка $(R_a\beta, \xi R_b, \xi R_c)$ должна быть автотопией операции $\circ$.

Окончательно получаем, что левая часть тождества (c), имеющая вид

$$f(g(x,u),g(y,v)) = \xi R_c\alpha((\xi R_c\alpha)^{-1}(\xi R_a\beta x \circ \beta u)) \circ \alpha(\alpha^{-1}(\beta y \circ R_b^{-1}\xi^{-1}\beta v)) =$$
$$= (\alpha_1 x \circ \beta u) \circ (\alpha_3 y \circ \alpha_4 v) = \xi R_a\beta x \circ \beta u \circ \beta y \circ R_b^{-1}\xi^{-1}\beta v,$$

должна, очевидно, совпадать с выражением в правой части этого тождества. ■

Теорема 8. 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

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

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

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

Доказательство. Пусть для функций f, g выполнено тождество (c). Рассмотрим второе тождество, отличающееся от (c) порядком следования функций:

$$g(f(x,y),f(u,v)) = g(f(x,u),f(y,v)).$$

Согласно утверждению 1, левая и правая части тождества должны иметь вид

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

Поэтому при $R_{c_1}\xi x = x'$ это тождество можно записать в виде

$$\beta(\alpha x' \circ \alpha y) \circ R_b^{-1}\xi^{-1}\beta(\xi R_c \alpha u \circ \alpha v) = \beta(\alpha x' \circ \alpha u) \circ R_b^{-1}\xi^{-1}\beta(\xi R_c \alpha y \circ \alpha v). \qquad (8)$$

При $\alpha x_0' = \alpha v_0 = e$ и u_0 из условия $R_b^{-1}\xi^{-1}\beta(\xi R_c \alpha u_0) = e$ получаем

$$\beta(\alpha y) = d \circ R_b^{-1}\xi^{-1}\beta(\xi R_c \alpha y), \qquad (9)$$

где элемент $d = \beta\alpha u_0$ должен быть обратимым, так как слева стоит подстановка.

Подставляя $\alpha v_0 = \alpha u_0' = e$, получаем тождество

$$\beta(\alpha x' \circ \alpha y) \circ R_b^{-1}\xi^{-1}\beta(\xi R_c \alpha u_0') = \beta(\alpha x') \circ R_b^{-1}\xi^{-1}\beta(\xi R_c \alpha y).$$

Используя равенство (9), преобразуем это тождество к виду

$$\beta(\alpha x' \circ \alpha y) \circ d^{-1} \circ \beta(\alpha u_0') = \beta(\alpha x') \circ d^{-1} \circ \beta(\alpha y),$$

где после замены переменных $z = \alpha x', w = \alpha y$ и сокращения d^{-1} получаем тождество

$$\beta(z \circ w) \circ \beta(e) = \beta(z) \circ \beta(w).$$

В силу леммы 3 биекция β является квазиавтоморфизмом. Пусть $\beta(x) = \psi(x) \circ h$, $\psi \in \mathrm{Aut}(\circ)$, $h \in X$. Тогда тождество (8) можно записать в виде

$$\psi(\alpha x' \circ \alpha y) \circ h \circ R_b^{-1}\xi^{-1}\psi(\xi R_c \alpha u \circ \alpha v) \circ h = \psi(\alpha x' \circ \alpha u) \circ h \circ R_b^{-1}\xi^{-1}\psi(\xi R_c \alpha y \circ \alpha v) \circ h.$$

После сокращения констант и использования свойства автоморфизма ψ получаем тождество

$$(\alpha x' \circ \alpha y) \circ R_b^{-1}\xi^{-1}(\xi R_c \alpha u \circ \alpha v) = (\alpha x' \circ \alpha u) \circ R_b^{-1}\xi^{-1}(\xi R_c \alpha y \circ \alpha v).$$

Выберем $x' = x_0'$ так, чтобы $\alpha x_0'$ был обратимым элементом. Тогда это эквивалентно равенству

$$\alpha y \circ R_b^{-1}\xi^{-1}(\xi R_c \alpha u) = \alpha u \circ R_b^{-1}\xi^{-1}(\xi R_c \alpha y),$$

или

$$\alpha y \circ \xi^{-1}(\xi R_c \alpha u) = \alpha u \circ \xi^{-1}(\xi R_c \alpha y).$$

Зафиксируем $u = u_0$ так, чтобы $\xi^{-1}(\xi R_c \alpha u_0) = e$:

$$\alpha y = \alpha u_0 \circ \xi^{-1}(\xi R_c \alpha y).$$

Поскольку α является подстановкой, элемент αy_0 должен быть обратимым. Обозначая $s = (\alpha y_0)^{-1}$, получаем

$$\alpha y \circ s = \xi^{-1}(\xi R_c \alpha y)$$

при некотором $s \in X$, или иначе

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

Следовательно,

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

Обозначая $m = \xi(s)$, $l = \xi^{-1}\psi b^{-1}$, получаем необходимый вид функций из условия теоремы. ■

Пример 1. Покажем, что в теореме 8 обе операции f и g могут быть нелинейными. Пусть $X = \mathbb{Z}_3^2$ рассматривается как прямая сумма $\mathbb{Z}_3 + \mathbb{Z}_3$ групп с операцией покоординатного сложения; $\xi(x) = xA$ — линейное преобразование, задаваемое матрицей $A = \begin{pmatrix} 0 & 1 \\ 2 & 1 \end{pmatrix}$ и являющееся автоморфизмом группы $(\mathbb{Z}_3^2, +)$. В цикловой записи ξ имеет вид $(00)(11,22)(01,21,20,02,12,10)$. Пусть подстановка α является транспозицией $(11,22)$. Она удовлетворяет равенству $\alpha\xi = \xi\alpha$, но не является автоморфизмом группы $\mathbb{Z}_3^2$, так как её координатные функции $\alpha(x_1, x_2) = (x_1', x_2')$ описываются нелинейными уравнениями

$$x_1' = x_1 - x_1x_2(x_1 + x_2),$$
$$x_2' = x_2 - x_1x_2(x_1 + x_2).$$

При этом α также не является квазиавтоморфизмом, так как не выполнено, например, равенство $\alpha(12) + \alpha(00) = \alpha(11) + \alpha(01)$ (см. лемму 3).

Рассмотрим бинарные квазигрупповые операции

$$f(x, y) = \xi\alpha x + \alpha y,$$
$$g(x, y) = \alpha^{-1}(x + \xi^{-1}y).$$

Они не являются линейными, но удовлетворяют обоим тождествам ко-медиальности:

$$f(g(x, y), g(u, v)) = f(g(x, u), g(y, v)),$$
$$g(f(x, y), f(u, v)) = g(f(x, u), f(y, v)).$$

Действительно, после подстановки в них операций f и g получаем тождества

$$\alpha^{-1}\xi\alpha(x + \xi^{-1}y) + (u + \xi^{-1}v) = \alpha^{-1}\xi\alpha(x + \xi^{-1}u) + (y + \xi^{-1}v),$$
$$\alpha^{-1}((\xi\alpha x + \alpha y) + \xi^{-1}(\xi\alpha u + \alpha v)) = \alpha^{-1}((\xi\alpha x + \alpha u) + \xi^{-1}(\xi\alpha y + \alpha v)),$$

которые в силу перестановочности автоморфизма ξ и биекции α можно преобразовать соответственно к виду

$$\xi x + y + u + \xi^{-1}v = \xi x + u + y + \xi^{-1}v,$$
$$\alpha^{-1}(\alpha\xi x + \alpha y + \alpha u + \alpha\xi^{-1}v) = \alpha^{-1}(\alpha\xi x + \alpha u + \alpha y + \alpha\xi^{-1}v).$$

Полностью аналогично рассматривается случай тождества ко-парамедиальности.

Утверждение 2. Если f, g — сильно зависимые бинарные операции, удовлетворяющие тождеству (d) ко-парамедиальности, то существует коммутативный 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.

Доказательство. Имеем $f = f_1 = f_4$ и $g = f_2 = f_3 = f_5 = f_6$, или

$$f(x, y) = \alpha_5 x \circ \alpha_6 y = \alpha_7 x \circ \alpha_8 y,$$
$$g(x, y) = \alpha_5^{-1}(\alpha_1 x \circ \alpha_2 y) = \alpha_6^{-1}(\alpha_3 x \circ \alpha_4 y) = \alpha_7^{-1}(\alpha_4 v \circ \alpha_2 y) = \alpha_8^{-1}(\alpha_3 x \circ \alpha_1 y).$$

Значит, изотопии $(\alpha_5, \alpha_6, \mathrm{id})$ и $(\alpha_7, \alpha_8, \mathrm{id})$, а также $(\alpha_1, \alpha_2, \alpha_5)$, $(\alpha_3, \alpha_4, \alpha_6)$, $(\alpha_4, \alpha_2, \alpha_7)$ и $(\alpha_3, \alpha_1, \alpha_8)$ лежат в одном смежном классе по группе автотопий моноида $(X, \circ)$. Отсюда по лемме 2 получаем, что при некоторых автоморфизмах ξ_1, ξ_2, ξ_3 справедливы равенства

$$\begin{gathered}(\alpha_1, \alpha_2, \alpha_5) = (\xi_1 R_{a_1}\alpha_3, \xi_1 R_{b_1}\alpha_4, \xi_1 R_{c_1}\alpha_6) = (\xi_2 R_{a_2}\alpha_4, \xi_2 R_{b_2}\alpha_2, \xi_2 R_{c_2}\alpha_7) = \\ = (\xi_3 R_{a_3}\alpha_3, \xi_3 R_{b_3}\alpha_1, \xi_3 R_{c_3}\alpha_8), \\ (\alpha_5, \alpha_6, \mathrm{id}) = (R_{a_4}\alpha_7, R_{b_4}\alpha_8, \mathrm{id}), \quad a_4 \circ b_4 = e.\end{gathered}$$

Тогда $\alpha_5 = \alpha_7 R_{a_4}$, $\alpha_6 = \alpha_8 R_{b_4}$, причём

$$\begin{aligned}\alpha_1 &= \xi_1 R_{a_1}\alpha_3 = \xi_2 R_{a_2}\alpha_4 = \alpha_3 R_{a_3}\xi_3, \\ \alpha_2 &= \xi_1 R_{b_1}\alpha_4 = \xi_2 R_{b_2}\alpha_2 = \xi_3 R_{b_3}\alpha_1, \\ \alpha_5 &= \xi_1 R_{c_1}\alpha_6 = \xi_2 R_{c_2}\alpha_7 = \alpha_8 R_{c_3}\xi_3.\end{aligned}$$

Значит, $\xi_1 R_{a_1} = \xi_3 R_{a_3}$, $\alpha_1 = \alpha_4$, $\xi_2 = \mathrm{id}$, $a_2 = e$,

$$\alpha_1 = \xi_1 R_{a_1}\alpha_3, \quad \alpha_2 = \xi_1 R_{b_1}\alpha_1, \quad \alpha_5 = \xi_1 R_{c_1}\alpha_6.$$

Подставим функции f и g в исходное тождество:

$$\begin{gathered}f(x, y) = \alpha_5 x \circ \alpha_6 y = \xi_1 R_{c_1}\alpha_6 x \circ \alpha_6 y, \\ g(x, y) = \alpha_5^{-1}(\alpha_1 x \circ \alpha_2 y) = (\xi_1 R_{c_1}\alpha_6)^{-1}(\alpha_1 x \circ \xi_1 R_{b_1}\alpha_1 y) = \\ = (\alpha_6)^{-1}(\alpha_3 x \circ \alpha_4 y) = (\alpha_6)^{-1}(R_{a_3}^{-1}\xi_1^{-1}\alpha_1 x \circ \alpha_1 y), \\ f(g(v, y), g(u, x)) = \alpha_5\alpha_5^{-1}(\alpha_1 v \circ \alpha_2 y)) \circ \alpha_6(\alpha_6^{-1}(\alpha_3 u \circ \alpha_4 x)) = \\ = (\alpha_1 v \circ \alpha_2 y) \circ (\alpha_3 u \circ \alpha_4 x) = \alpha_1 v \circ \xi_1 R_{b_1}\alpha_1 y \circ R_{a_3}^{-1}\xi_1^{-1}\alpha_1 u \circ \alpha_1 x.\end{gathered}$$

При $\alpha_1 = \beta$, $\alpha_6 = \alpha$, $\xi_1 = \xi$, $R_{c_1}\xi u = u'$, $c_1 = c$, $a_3 = a$ получаем требуемый вид операций. ■

Теорема 9. Если алгебра $(X, \{f, g\})$, где f, g — сильно зависимые бинарные операции, является ко-парамедиальной, 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

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

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

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

Доказательство. Пусть для функций f, g выполнено тождество (d). Рассмотрим второе тождество, отличающееся от (d) порядком следования функций

$$g(f(x, y), f(u, v)) = g(f(v, y), f(u, x)),$$

где, согласно утверждению 2,

$$\begin{aligned}g(f(x, y), f(u, v)) &= \alpha^{-1}(R_a^{-1}\xi^{-1}\beta(\xi R_c\alpha x \circ \alpha y) \circ \beta(\xi R_c\alpha u \circ \alpha v)), \\ g(f(v, y), f(u, x)) &= \alpha^{-1}(R_a^{-1}\xi^{-1}\beta(\xi R_c\alpha v \circ \alpha y) \circ \beta(\xi R_c\alpha u \circ \alpha x)).\end{aligned}$$

При $\xi R_c u = u'$ получаем

$$R_a^{-1}\xi^{-1}\beta(\xi R_c\alpha x \circ \alpha y) \circ \beta(\alpha u' \circ \alpha v) = R_a^{-1}\xi^{-1}\beta(\xi R_c\alpha v \circ \alpha y) \circ \beta(\alpha u' \circ \alpha x). \tag{10}$$

При $\alpha y_0 = e$, $\alpha u'_0 = e$ тождество (10) принимает вид

$$R_a^{-1}\xi^{-1}\beta(\xi R_c\alpha x) \circ \beta(\alpha v) = R_a^{-1}\xi^{-1}\beta(\xi R_c\alpha v) \circ \beta(\alpha x),$$

при v_0 из условия $R_a^{-1}\xi^{-1}\beta(\xi R_c\alpha v_0) = e$ получим

$$R_a^{-1}\xi^{-1}\beta(\xi R_c\alpha x) \circ d = \beta(\alpha x), \tag{11}$$

где $d = \beta(\alpha v_0)$ должен быть обратимым элементом.

Полагая $\alpha u'_0 = e$ в тождестве (10), получаем

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

после замены $R_c\xi x = x'$ с использованием равенства (11) тождество (10) будет иметь следующий вид:

$$R_a^{-1}\xi^{-1}\beta(\alpha x' \circ \alpha y) \circ R_a^{-1}\xi^{-1}\beta(\xi R_c\alpha v) \circ d = R_a^{-1}\xi^{-1}\beta(\xi R_c\alpha v \circ \alpha y) \circ R_a^{-1}\xi^{-1}\beta(\alpha x') \circ d.$$

Обозначим $\phi = R_a^{-1}\xi^{-1}\beta, \alpha v' = \xi\alpha R_c v$. Тогда последнее равенство принимает вид

$$\phi(\alpha x' \circ \alpha y) \circ \phi(\alpha v') \circ d = \phi(\alpha v' \circ \alpha y) \circ \phi(\alpha x') \circ d.$$

Сокращая на d и полагая $\alpha v' = e$, получаем

$$\phi(\alpha x' \circ \alpha y) \circ \phi(e) = \phi(\alpha y) \circ \phi(\alpha x').$$

Значит, по лемме 3 биекция ϕ, а потому и β являются квазиавтоморфизмами.

Пусть $\beta(x) = \psi(x) \circ h$, $\psi \in \mathrm{Aut}(\circ)$, $h \in X$. Тогда тождество (11) можно записать в виде

$$R_a^{-1}\xi^{-1}\psi(\xi R_c\alpha x) \circ h \circ \psi(\alpha v) \circ h = R_a^{-1}\xi^{-1}\psi(\xi R_c\alpha v) \circ h \circ \psi(\alpha x) \circ h.$$

Сокращая константы и используя свойство автоморфизма ψ, получаем тождество

$$R_a^{-1}\xi^{-1}(\xi R_c\alpha x) \circ \alpha v = R_a^{-1}\xi^{-1}(\xi R_c\alpha v) \circ \alpha x,$$

что эквивалентно

$$\xi^{-1}(\xi R_c\alpha x) \circ \alpha v = \xi^{-1}(\xi R_c\alpha v) \circ \alpha x.$$

Фиксируя переменную v значением v_0 так, чтобы $\xi^{-1}(\xi R_c\alpha v_0) = e$, имеем

$$\xi^{-1}(\xi R_c\alpha x) \circ \alpha v_0 = \alpha x.$$

Так как в правой части стоит подстановка, то элемент αv_0 обратим и выполнение этого тождества эквивалентно выполнению тождества

$$\alpha x \circ s = \xi^{-1}(\xi R_c\alpha x),$$

где $s = (\alpha v_0)^{-1}$, или иначе

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

или $\alpha R_s\xi x = \xi R_c\alpha x$. Следовательно,

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

где $m = \xi(s)$, $l = \xi^{-1}\psi a^{-1}$. ■

4. Свойство перестановочности степеней

В работе [20] D. C. Murdoch заметил, что медиальные группоиды обладают свойством *перестановочности степеней* (*palintropic property*). Ранее для медиальных группоидов использовался термин *entropoid*, а свойство медиальности называлось *entropic property* и определялось так: для всех $x, e, z, w \in G$ если $x * y = z * w$, то $x * z = y * w$.

Теорема 10 [20, теорема 10]. Для любых элементов $x, y \in X$ медиального группоида $(X, *)$ и всех $m, n \geqslant 1$ выполнены равенства

$$(x * y)^n = x^n * y^n, \quad (x^n)^m = (x^m)^n.$$

Для некоммутативной и неассоциативной бинарной операции $*$ помимо стандартного определения $x^n = x^{n-1} * x$ возможны и другие определения степени, отличающиеся способом расстановки скобок в последовательности $\underbrace{x * x * \ldots * x}_{n}$. Каждое скобочное выражение можно обозначить как степень $x^{\mathbf{A}}$ элемента x, показатель $\mathbf{A}$ которой записан в виде формального алгебраического выражения над натуральными числами с использованием символов операций сложения и умножения. Показатель $\mathbf{A}$ называют *степенны́м индексом* (*power index*). Например, степенно́й индекс $\mathbf{A} = (2+1)\cdot 3+(1+2)^2$ соответствует следующему скобочному выражению:

$$((((x * x) * x) * ((x * x) * x)) * ((x * x) * x)) * ((x * (x * x)) * ((x * (x * x)) * (x * (x * x)))).$$

Степенны́е индексы $\mathbf{A}$ и $\mathbf{B}$ называются эквивалентными, если $x^{\mathbf{A}} = x^{\mathbf{B}}$ для всех $x \in X$. Множество классов эквивалентности индексов образует алгебру $(\mathbb{Z}; +, \cdot)$ с двумя бинарными операциями

$$x^{\mathbf{A}+\mathbf{B}} = x^{\mathbf{A}} * x^{\mathbf{B}}, \quad x^{\mathbf{A}\cdot\mathbf{B}} = \left(x^{\mathbf{A}}\right)^{\mathbf{B}},$$

которую I. M. H. Etherington [21] назвал *логарифметикой* (*logarithmetic*).

Заметим, что в силу теоремы 10 операция умножения в записи степенно́го индекса коммутативна и ассоциативна, хотя операция сложения в общем случае не является ни коммутативной, ни ассоциативной. При этом закон дистрибутивности сложения относительно умножения сохраняется. В [21] доказано, что если вместо обычных степеней рассматривать произвольные скобочные выражения (степенны́е индексы), то для медиальных группоидов свойство перестановочности степеней оказывается справедливым и в общем случае.

Теорема 11 [21, теорема 10]. Пусть $\mathbf{A}$ и $\mathbf{B}$ — произвольные степенны́е индексы. Для любых элементов $x, y \in X$ медиального группоида $(X, *)$ выполнены равенства

$$(x * y)^{\mathbf{A}} = x^{\mathbf{A}} * y^{\mathbf{A}}, \quad \left(x^{\mathbf{A}}\right)^{\mathbf{B}} = \left(x^{\mathbf{B}}\right)^{\mathbf{A}}. \tag{12}$$

Покажем, что равенства (12) выполняются и в случае двух бинарных операций $f(x, y) = x \circ y$ и $g(u, v) = u * v$ на множестве X, удовлетворяющих обобщённому тождеству медиальности (a). Обозначим степени относительно каждой из операций следующим образом:

$$x^{\{n\}} = (((x \circ x) \circ x) \circ \ldots \circ x)x = x^{\{n-1\}} \circ x,$$
$$y^{[m]} = (((y * y) * y) * \ldots * y)y = y^{[m-1]} * y.$$

Будем также обозначать степенны́е индексы как $\{\mathbf{A}\}$ и $[\mathbf{B}]$ для степеней, вычисленных с помощью операций $\circ$ и $*$ соответственно.

Теорема 12. Пусть $\mathbf{A}$ и $\mathbf{B}$ — произвольные степенны́е индексы. Для любых группоидов $(X, \circ)$ и $(X, *)$, удовлетворяющих обобщённому тождеству медиальности, для любых элементов $x, y \in X$ выполнены равенства

$$(x * y)^{\{\mathbf{A}\}} = x^{\{\mathbf{A}\}} * y^{\{\mathbf{A}\}}, \quad \left(x^{\{\mathbf{A}\}}\right)^{[\mathbf{B}]} = \left(x^{[\mathbf{B}]}\right)^{\{\mathbf{A}\}}.$$

Доказательство. Каждый степенно́й индекс $\mathbf{A}$ можно записать в виде формального алгебраического выражения над натуральными числами с использованием символов некоммутативной операции сложения и коммутативной операции умножения. Воспользуемся индукцией по числу операций в записи индекса $\mathbf{A}$. Рассмотрим два случая в зависимости от последней операции в записи степенно́го индекса: $\mathbf{A} = \mathbf{A_1} + \mathbf{A_2}$, $\mathbf{A} = \mathbf{A_1} \cdot \mathbf{A_2}$. Докажем второе равенство. По предположению индукции это равенство выполняется для степенны́х индексов $\mathbf{A_1}$ и $\mathbf{A_2}$. Имеем:

$$\begin{aligned}
(x * y)^{\{\mathbf{A}\}} &= (x * y)^{\{\mathbf{A_1}\cdot\mathbf{A_2}\}} = \\
&= \left((x * y)^{\{\mathbf{A_1}\}}\right)^{\{\mathbf{A_2}\}} = \\
&= \left(x^{\{\mathbf{A_1}\}} * y^{\{\mathbf{A_1}\}}\right)^{\{\mathbf{A_2}\}} = \\
&= \left(x^{\{\mathbf{A_1}\}}\right)^{\{\mathbf{A_2}\}} \circ \left(y^{\{\mathbf{A_1}\}}\right)^{\{\mathbf{A_2}\}} = \\
&= \left(x^{\{\mathbf{A_1}\}}\right)^{\{\mathbf{A_2}\}} * \left(y^{\{\mathbf{A_1}\}}\right)^{\{\mathbf{A_2}\}} = \\
&= x^{\{\mathbf{A}\}} * y^{\{\mathbf{A}\}}.
\end{aligned}$$

Аналогично рассматривается первый случай.

Второе равенство доказывается с использованием первого, только теперь надо рассмотреть четыре случая в зависимости от последних операций в записи степенны́х индексов $\mathbf{A}$ и $\mathbf{B}$:

$$\mathbf{A} = \mathbf{A_1} + \mathbf{A_2},\ \mathbf{B} = \mathbf{B_1} + \mathbf{B_2},\ \mathbf{A} = \mathbf{A_1} \cdot \mathbf{A_2},\ \mathbf{B} = \mathbf{B_1} \cdot \mathbf{B_2}.$$

В случае, когда обе операции — сложение $(+)$, имеем:

$$\begin{aligned}
\left(x^{\{\mathbf{A}\}}\right)^{[\mathbf{B}]} &= \left(x^{\{\mathbf{A_1}+\mathbf{A_2}\}}\right)^{[\mathbf{B_1}+\mathbf{B_2}]} = \\
&= \left(x^{\{\mathbf{A_1}\}} \circ x^{\{\mathbf{A_2}\}}\right)^{[\mathbf{B_1}+\mathbf{B_2}]} = \\
&= \left(x^{\{\mathbf{A_1}\}} \circ x^{\{\mathbf{A_2}\}}\right)^{[\mathbf{B_1}]} * \left(x^{\{\mathbf{A_1}\}} \circ x^{\{\mathbf{A_2}\}}\right)^{[\mathbf{B_2}]} = \\
&= \left(\left(x^{\{\mathbf{A_1}\}}\right)^{[\mathbf{B_1}]} \circ \left(x^{\{\mathbf{A_2}\}}\right)^{[\mathbf{B_1}]}\right) * \left(\left(x^{\{\mathbf{A_1}\}}\right)^{[\mathbf{B_2}]} \circ \left(x^{\{\mathbf{A_2}\}}\right)^{[\mathbf{B_2}]}\right) = \\
&= \left(\left(x^{[\mathbf{B_1}]}\right)^{\{\mathbf{A_1}\}} \circ \left(x^{[\mathbf{B_1}]}\right)^{\{\mathbf{A_2}\}}\right) * \left(\left(x^{[\mathbf{B_2}]}\right)^{\{\mathbf{A_1}\}} \circ \left(x^{[\mathbf{B_2}]}\right)^{\{\mathbf{A_2}\}}\right) = \\
&= \left(x^{[\mathbf{B_1}]}\right)^{\{\mathbf{A_1}+\mathbf{A_2}\}} * \left(x^{[\mathbf{B_2}]}\right)^{\{\mathbf{A_1}+\mathbf{A_2}\}} = \\
&= \left(x^{[\mathbf{B_1}+\mathbf{B_2}]}\right)^{\{\mathbf{A_1}+\mathbf{A_2}\}} = \\
&= \left(x^{[\mathbf{B}]}\right)^{\{\mathbf{A}\}}.
\end{aligned}$$

Остальные три случая рассматриваются аналогично. ■

Свойство перестановочности степеней оказывается удобным для построения протокола Диффи — Хеллмана. В [22] для построения протокола предложено рассматривать произвольные скобочные выражения на медиальных квазигруппах. Теорема 12 позволяет построить протокол типа Диффи — Хеллмана, в котором каждый из участников выполняет вычисления с использованием своей бинарной операции. Сначала

они договариваются об образующем элементе $a \in X$. Каждый участник выбирает своё скобочное выражение. Затем они обмениваются сообщениями

$$\begin{aligned} A \to B: &\quad a^{\{\mathbf{A}\}}, \\ A \leftarrow B: &\quad a^{[\mathbf{B}]}. \end{aligned}$$

Общий ключ вычисляется по формулам

$$k = \left(a^{\{\mathbf{A}\}}\right)^{[\mathbf{B}]} = \left(a^{[\mathbf{B}]}\right)^{\{\mathbf{A}\}}.$$

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. 138–147.
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 // Матем. сб. 2020. Т. 211. № 2. 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. *Ehsani A.* Representation of the medial-like algebras // TACL 2013. N. Galatos, A. Kurz, and C. Tsinakis (eds.). EPiC Ser. 2013. V. 25. P. 64–67.
7. *Cho J. R., Ježek J., and Kepka T.* Paramedial groupoids // Czechoslovak Math. J. 1999. V. 49. No. 2. P. 277–290.
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. 2024. Т. 26. № 3. С. 115–126.
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. *Черемушкин А. В.* Бесповторная декомпозиция сильно зависимых функций // Дискретная математика. 2004. Т. 16. № 3. С. 3–42.
16. *Sokhatsky F. and Kirka D.* Canonical decompositions of solutions of functional equation of generalized mediality // XII Intern. Algebraic Conf. Ukraine, 2019. P. 107–108.
17. *Ehsani A.* On medial-like functional equations // Math. Problems of Computer Sci. 2021. V. 38. P. 53–55.
18. *Ehsani A. and Movsisyan Y.* Linear representation of medial-like algebras // Comm. Algebra. 2013. V. 41. No. 9. P. 3429–3444.
19. *Ehsani A., Krapež A., and Movsisyan Y.* Algebras with Medial-Like Functional Equations on Quasigroups. `https://arxiv.org/abs/1505.06224`. 2015.

20. *Murdoch D. C.* Quasi-groups which satisfy certain generalized associative laws // Amer. J. Math. 1939. V. 61.2. P. 509–522.
21. *Etherington I. M. H.* Groupoids with additive endomorphisms // Amer. Math. Monthly. 1958. V. 65(8P1). P. 596–601.
22. *Gligoroski D.* Entropoid Based Cryptography. IACR Cryptology ePrint Archive 2021/469. `https://eprint.iacr.org/2021/469`. 2021.

REFERENCES

1. *Cheremushkin A. V.* Analogues of Gluskin — Hosszú and Malyshev theorems for strongly dependent n-ary operations. Discrete Math. Appl., 2019, vol. 29, no. 5, pp. 295–302.
2. *Cheremushkin A. V.* Teorema Posta dlya sil'no zavisimykh n-arnykh polugrupp [Post's theorem for strongly dependent n-ary semigroups]. Diskretnaya Matematika, 2019, vol. 31, no. 2, pp. 152–157. (in Russian)
3. *Cheremushkin A. V.* Partially invertible strongly dependent n-ary operations. Sb. Math., 2020, vol. 211, no. 2, pp. 291–308.
4. *Toyoda K.* On axioms of linear functions. Proc. Imp. Acad. Tokyo, 1941, vol. 17, pp. 221–227.
5. *Němec P. and Kepka T.* T-quasigroups (Part I). Acta Univ. Carolinae, Math. Phis., 1971, vol. 1, pp. 39–49.
6. *Ehsani A.* Representation of the medial-like algebras. TACL 2013, N. Galatos, A. Kurz, and C. Tsinakis (eds.). EPiC Ser., 2013, vol. 25, pp. 64–67.
7. *Cho J. R., Ježek J., and Kepka T.* Paramedial groupoids. Czechoslovak Math. J., 1999, vol. 49, no. 2, pp. 277–290.
8. *Ehsani A., Movsisyan Y., and Arslanov M.* A representation of paramedial n-ary groupoids. Asian-Europ. J. Math., 2014, vol. 7, no. 1, pp. 1450020-1–1450020-17.
9. *Cheremushkin A. V.* Medial strongly dependent n-ary operations. Discrete Math. Appl., 2021, vol. 31, no. 4, pp. 251–258.
10. *Cheremushkin A. V.* Paramedial'nye cil'no zavisimye n-arnye operatsii [Paramedial strong dependance n-ary operations]. Diskret. Math., 2024, vol. 26, no. 3, pp. 115–126. (in Russian)
11. *Aczél J., Belousov V. D., and Hossú M.* Generalized associativity and bisymmetry on quasigroups. Acta Math. Acad. Sci. Hungar., 1960, vol. 11, no. 11-2, pp. 127–136.
12. *Nazari E. and Movsisyan Y. M.* Transitive modes. Demonstratio Math., 2011, vol. 44, no. 3, pp. 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, vol. 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, pp. 41–63.
15. *Cheremushkin A. V.* Repetition-free decomposition of strongly dependent functions. Discrete Math. Appl., 2004, vol. 14, no. 5, pp. 439–478.
16. *Sokhatsky F. and Kirka D.* Canonical decompositions of solutions of functional equation of generalized mediality. XII Intern. Algebraic Conf., Ukraine, 2019, pp. 107–108.
17. *Ehsani A.* On medial-like functional equations. Math. Problems of Computer Sci., 2021, vol. 38, pp. 53–55.
18. *Ehsani A. and Movsisyan Y.* Linear representation of medial-like algebras. Comm. Algebra, 2013, vol. 41, no. 9, pp. 3429–3444.
19. *Ehsani A., Krapež A., and Movsisyan Y.* Algebras with Medial-Like Functional Equations on Quasigroups. `https://arxiv.org/abs/1505.06224`. 2015.

20. *Murdoch D. C.* Quasi-groups which satisfy certain generalized associative laws. Amer. J. Math., 1939, vol. 61.2, pp. 509–522.
21. *Etherington I. M. H.* Groupoids with additive endomorphisms. Amer. Math. Monthly, 1958, vol. 65(8P1), pp. 596–601.
22. *Gligoroski D.* Entropoid Based Cryptography. IACR Cryptology ePrint Archive 2021/469. `https://eprint.iacr.org/2021/469`, 2021.

МАТЕМАТИЧЕСКИЕ МЕТОДЫ КРИПТОГРАФИИ

УДК 519.7 DOI 10.17223/20710410/65/3

О СВОЙСТВЕ НЕПОДДЕЛЫВАЕМОСТИ СХЕМЫ ПОДПИСИ ВСЛЕПУЮ ШАУМА — ПЕДЕРСЕНА

Л. Р. Ахметзянова, А. А. Бабуева

КриптоПро, г. Москва, Россия

E-mail: {lah, babueva}@cryptopro.ru

Анализируется свойство неподделываемости схемы подписи вслепую Шаума — Педерсена в условиях, когда нарушитель имеет возможность открывать параллельные сеансы протокола формирования подписи. Показано, что схема не обеспечивает свойство неподделываемости в сильном смысле, т. е. позволяет строить подделки для «старого» сообщения, которое было подписано легитимным образом в результате взаимодействия с подписывающим. Проведён анализ свойства неподделываемости в слабом смысле (задача нарушителя — построение подделки для нового сообщения). С помощью метода сведений получена оценка стойкости схемы относительно свойства слабой неподделываемости в модели с алгебраической группой и случайным оракулом. Полученная оценка позволяет выделить базовые задачи, сложность которых лежит в основе стойкости схемы.

Ключевые слова: *схема подписи вслепую, схема Шаума — Педерсена, ROS-атака.*

ON THE UNFORGEABILITY OF THE CHAUM — PEDERSEN BLIND SIGNATURE SCHEME

L. R. Akhmetzyanova, A. A. Babueva

CryptoPro, Moscow, Russia

The paper is devoted to the analysis of the unforgeability property of the Chaum — Pedersen blind signature scheme in case an adversary is able to initiate parallel sessions of the signature generation protocol. It is shown that the scheme does not ensure strong unforgeability, i.e., it allows to create the forgeries for “old” messages that were legitimately signed. An analysis of the weak unforgeability property (the adversary’s task is to create a forgery for a new message) is also conducted. Using the reduction method, we obtain a security bound on the weak unforgeability property in the algebraic group model and random oracle model. This estimation identifies the base problems whose complexity underpins the scheme security.

Keywords: *blind signature scheme, Chaum — Pedersen blind signature, ROS attack.*

Введение

Механизм подписи вслепую был впервые предложен Д. Шаумом в 1982 г. [1]. Формирование подписи вслепую представляет собой интерактивный протокол, выполняемый между подписывающей стороной (сервером) и клиентом. В результате клиент получает подпись для некоторого сообщения, при этом подписывающий не получает информации ни о сообщении, ни о сформированном значении подписи (свойство неотслеживаемости), а клиент не может сформировать корректное значение подписи без взаимодействия с подписывающим (свойство неподделываемости). Как показывает история развития схем подписи вслепую, построение схем на основе стандартных эллиптических кривых, обеспечивающих свойство неподделываемости в условиях, когда нарушитель имеет возможность открывать параллельные сеансы протокола формирования подписи, — нетривиальная задача. Заметим, что подобные условия актуально рассматривать для приложений, где множество клиентов единовременно подключаются к серверу выдачи подписи вслепую и при этом важна высокая скорость получения подписи. Ярким примером таких систем являются системы дистанционного электронного голосования [2].

Существующие работы. Классической схемой подписи вслепую на основе стандартных эллиптических кривых является схема Шнорра, предложенная в 1996 г. в [3]. Анализ стойкости данной схемы проведен в 2001 г. в [4]. Свойство неподделываемости было доказано в предположении сложности задачи ROS (Random inhomogeneities in a Overdetermined Solvable system of linear equations) в генерической модели со случайным оракулом. Задача ROS на протяжении 20 лет считалась сложной. Однако в 2020 г. был предложен полиномиальный алгоритм решения этой задачи [5], который позволил построить полиномиальную атаку, приводящую к нарушению свойства неподделываемости для схемы подписи вслепую Шнорра в случае, если нарушитель имеет возможность открыть $\ell \geqslant \lceil \log q \rceil$ параллельных сеансов протокола формирования подписи с подписывающим, где q — простой порядок группы точек эллиптической кривой.

Оказалось [5, 6], что аналогичная атака применима не только к схеме подписи вслепую Шнорра, но и к ряду других схем на основе стандартных эллиптических кривых: схеме Окамото— Шнорра [7], схеме Абе [8], обеспечивающей частичную неотслеживаемость, схемам на основе уравнения Эль-Гамаля [6], а также схеме Брандса [9]. При этом для схемы Брандса атака позволяет строить подделки только для одного и того же «номера аккаунта». Схема Брандса, в свою очередь, построена на основе схемы подписи вслепую Шаума — Педерсена [10]. Для схемы Шаума— Педерсена в литературе не представлено ни атак, ни формального обоснования свойства неподделываемости, поэтому вопрос её стойкости является открытым.

Формальное обоснование свойства неподделываемости для схем подписи вслепую сопряжено с некоторыми трудностями. В литературе представлен ряд работ, которые показывают невозможность обоснования стойкости схемы подписи вслепую Шнорра в стандартных моделях безопасности [11, 12], а именно: без идеализаций криптографических примитивов (модель со случайным оракулом [13]) и ограничений множества рассматриваемых нарушителей (модели с генерической [14] или алгебраической [15] группой). Более того, в работе [16] показано, что для схемы подписи вслепую Шнорра [3], Окамото — Шнорра [7] и схемы Брандса [9] невозможно построить сведение с использованием всех известных техник доказательств для таких схем (например, Random oracle replay и forking lemma) на основе предположений о сложности базовых задач даже в модели со случайным оракулом. Существующие сведения верны толь-

ко в моделях с генерической или алгебраической группой со случайным оракулом, которые являются упрощением стандартных моделей. Насколько известно авторам настоящей работы, на сегодняшний день не предложено каких-либо принципиально новых техник построения сведений для схем подписи вслепую.

С момента публикации ROS-атаки в литературе было предложено несколько схем подписи вслепую [17–19] на основе стандартных эллиптических кривых, стойких (при некоторых предположениях) даже в том случае, когда нарушитель имеет возможность открывать параллельные сеансы протокола формирования подписи. Оценка стойкости всех этих схем получена в модели со случайным оракулом, а при обосновании схем [18, 19] используется также модель с алгебраической группой.

Наши результаты. В настоящей работе проводится анализ схемы Шаума — Педерсена с точки зрения обеспечения свойства неподделываемости при наличии у нарушителя возможности открывать несколько параллельных сеансов протокола формирования подписи.

Показано, что схема Шаума — Педерсена не обеспечивает свойство неподделываемости в сильном смысле, т. е. позволяет строить подделки для «старого» сообщения, которое было подписано легитимным образом в результате взаимодействия с подписывающим. Построена модификация ROS-атаки, аналогичная ROS-атаке на схему Брандса. При этом конструкция схемы не позволяет расширить данную атаку на случай построения подделки для «нового» сообщения, это означает, что схема Шаума — Педерсена потенциально обеспечивает свойство неподделываемости в слабом смысле (задача нарушителя — построение подделки для нового сообщения).

Проведён формальный анализ свойства неподделываемости в слабом смысле. Построено сведение в модели с алгебраической группой и случайным оракулом, которое демонстрирует, что достаточным условием стойкости схемы является сложность решения двух задач: задачи REPR и SOMDL. Задача REPR является модификацией задачи Representation, определённой в работе [9], её сложность также является необходимым условием стойкости схемы Шаума — Педерсена. Задача SOMDL является новой задачей, определённой для группы точек эллиптической кривой. Показано, что настоящая задача не сложнее задачи OMDL (One-More Discrete Logarithm, введена в [20]) и задачи SDL (определена в [21] как задача q-dlog). Для задачи SDL показано также, что её сложность является необходимым условием стойкости схемы Шаума — Педерсена. Таким образом, выделены базовые задачи, дальнейшее изучение которых необходимо для получения больших гарантий безопасности схемы Шаума — Педерсена.

Структура работы. В п. 1 даются основные определения и обозначения, п. 2 посвящён формальному определению схемы подписи вслепую Шаума — Педерсена. В п. 3 вводится свойство неподделываемости для схем подписи вслепую. Пункты 4 и 5 посвящены анализу свойства неподделываемости в сильном и слабом смысле соответственно. В приложении A формально определяется модель wUF, а в приложении B приводится доказательство теоремы 1 о стойкости этой модели.

1. Определения и обозначения

Если p — простое число, то через $\mathbb{Z}_p$ обозначается поле вычетов по модулю p; каждый ненулевой элемент x поля $\mathbb{Z}_p$ имеет обратный элемент $1/x$; $\mathbb{Z}_p^*$ — множество $\mathbb{Z}_p$ без нулевого элемента, т. е. мультипликативная группа поля $\mathbb{Z}_p$.

Группа точек эллиптической кривой, определённой над полем $\mathbb{Z}_p$, простого порядка q обозначается через $\mathbb{G}$, точка эллиптической кривой порядка q — через P, нулевая точка кривой — через $\mathcal{O}$; $\mathbb{G}^*$ — множество точек кривой без нулевой точки; H — хеш-

функция, отображающая двоичные строки в элементы $\mathbb{Z}_q^*$; $\mathcal{H} : \{0,1\}^* \to \mathbb{G}^*$ — хеш-функция, отображающая двоичные строки в точки кривой. Через $\mathrm{DLog}_B(A)$, $A, B \in \mathbb{G}$, обозначается число $\alpha \in \mathbb{Z}_q$, такое, что $A = \alpha B$.

Запись $x \xleftarrow{U} X$ означает, что элемент x выбирается из множества X случайно в соответствии с равновероятным распределением, будем называть такой элемент x случайным. Событие, что алгоритм A вернул значение val в качестве результата работы, обозначается через $A \to val$ ($val \leftarrow A$).

Определение 1. Схема подписи вслепую BS задается следующими алгоритмами:

— $(\mathsf{sk}, \mathsf{pk}) \leftarrow \mathsf{KGen}()$: алгоритм выработки ключей, возвращающий пару ключей $(\mathsf{sk}, \mathsf{pk})$, где sk — ключ подписи; pk — ключ проверки подписи;

— $(b, \sigma) \leftarrow \langle \mathsf{Sign}(\mathsf{sk}, \mathsf{pk}), \mathsf{User}(\mathsf{pk}, m) \rangle$: интерактивный протокол, выполняемый между подписывающим, обладающим ключом подписи sk и ключом проверки подписи pk, и клиентом, обладающим сообщением m и ключом проверки подписи pk; подписывающий выдаёт $b = 1$, если взаимодействие успешно завершилось, и $b = 0$ в противном случае; клиент выдаёт значение подписи σ в случае успешного завершения протокола и $\perp$ в противном случае;

— $b \leftarrow \mathsf{Verify}(\mathsf{pk}, m, \sigma)$: детерминированный алгоритм проверки подписи, принимающий на вход ключ проверки подписи pk, сообщение m и подпись σ и возвращающий единицу, если значение подписи верное, и нуль в противном случае.

При этом для любой пары ключей $(\mathsf{sk}, \mathsf{pk}) \leftarrow \mathsf{KGen}()$ и любого сообщения m требуется, чтобы в результате выполнения

$$(b, \sigma) \leftarrow \langle \mathsf{Sign}(\mathsf{sk}, \mathsf{pk}), \mathsf{User}(\mathsf{pk}, m) \rangle,$$
$$b' \leftarrow \mathsf{Verify}(\mathsf{pk}, m, \sigma)$$

было выполнено $b = b' = 1$.

2. Схема Шаума — Педерсена

Приведём описание алгоритмов, задающих работу схемы подписи вслепую Шаума — Педерсена. Далее будем называть эту схему $\mathsf{CP\text{-}BS}$.

Оригинальное описание схемы Шаума — Педерсена [10] представлено для мультипликативной группы конечного поля, при этом подписываемое сообщение представляет собой элемент группы. В настоящей работе мы приводим описание для группы точек эллиптической кривой, при этом для перевода сообщения в элемент группы, т. е. точку кривой, мы предлагаем использовать функцию хеширования $\mathcal{H}$ в группу точек эллиптической кривой. Заметим, что в литературе известны подходы к построению таких функций (см., например, [22]).

Алгоритм выработки ключей задаётся следующим образом:

$\mathsf{CP\text{-}BS.KGen}()$

$d \xleftarrow{U} \mathbb{Z}_q^*$

$Q \leftarrow dP$

return (d, Q)

Протокол формирования подписи состоит из двух раундов, инициатором взаимодействия является клиент. Клиент вычисляет элемент группы $M' = \mathcal{H}(m)$, маскирует это значение, вычисляя $M = \alpha^{-1} M'$ для случайно выбранного значения $\alpha \in \mathbb{Z}_q^*$, и посылает точку M серверу. Сервер вычисляет значение $Z = dM$, после

чего клиент и сервер выполняют интерактивный протокол доказательства равенства дискретных логарифмов Шаума — Педерсена [10] для значений $\mathrm{DLog}_P Q = \mathrm{DLog}_M Z$, при этом для вычисления значения c (challenge в протоколе доказательства Шаума — Педерсена) клиент маскирует все значения, полученные от сервера. Значение $Z' = \alpha Z$ и сформированное доказательство (в маскированном виде) составляют подпись.

Алгоритм проверки подписи для сообщения m представляет собой проверку доказательства равенства

$$\mathrm{DLog}_P Q = \mathrm{DLog}_{M'} Z',$$

где $M' = \mathcal{H}(m)$. Заметим, что $\mathrm{DLog}_{M'} Z' = \mathrm{DLog}_{\alpha M}(\alpha Z) = \mathrm{DLog}_M Z$.

Протокол формирования и алгоритм проверки подписи формально определены на рис. 1 и 2 соответственно.

Sign (d, Q)		User (Q, m)
		$\alpha \xleftarrow{\mathcal{U}} \mathbb{Z}_q^*$
		$M' \leftarrow \mathcal{H}(m)$
	$\xleftarrow{\quad M \quad}$	$M \leftarrow \alpha^{-1} M'$
if $M \notin \mathbb{G}$: **return** 0		
$k \xleftarrow{\mathcal{U}} \mathbb{Z}_q^*$		
$Z \leftarrow dM$		
$A \leftarrow kP$		
$B \leftarrow kM$	$\xrightarrow{\quad Z, A, B \quad}$	
		if $Z, A, B \notin \mathbb{G}$: **return** $\perp$
		$u, v \xleftarrow{\mathcal{U}} \mathbb{Z}_q^*$
		$A' \leftarrow uA + vP$
		$B' \leftarrow u\alpha B + vM'$
		$Z' \leftarrow \alpha Z$
		$c' \leftarrow H(M' \Vert Z' \Vert A' \Vert B')$
	$\xleftarrow{\quad c \quad}$	$c \leftarrow c' u^{-1}$
if $c = 0$: **return** 0		
$s \leftarrow k + cd$	$\xrightarrow{\quad s \quad}$	
		if $sP \neq A + cQ$: **return** $\perp$
		if $sM \neq B + cZ$: **return** $\perp$
		$s' \leftarrow us + v$
		$\sigma \leftarrow (s', c', Z')$
return 1		**return** σ

Рис. 1. Протокол формирования подписи в схеме CP-BS

CP-BS.Verify$(Q, m, (s', c', Z'))$

if $Z' \notin \mathbb{G}$: **return** 0
$M' \leftarrow \mathcal{H}(m)$
if $c' = H(M' \| Z' \| (s'P - c'Q) \| (s'M' - c'Z'))$: **return** 1
else : **return** 0

Рис. 2. Алгоритм проверки подписи в схеме CP-BS

В отличие от оригинального описания схемы, в представленном описании значение подписи определяется набором (s', c', Z'), а не (s', A', B', Z'). Заметим, что с точки зрения стойкости схемы эти способы задания подписи являются эквивалентными, поскольку по первому набору можно однозначно восстановить второй набор и наоборот. Вместе с тем подпись (s', c', Z') является более короткой, а потому представляет больший интерес с практической точки зрения.

3. Свойства безопасности схем подписи вслепую

Для схем подписи вслепую традиционно рассматривают [1, 3] следующие два свойства безопасности:

— неотслеживаемость (blindness): нарушитель, выступающий в роли подписывающего, в результате выполнения протокола формирования подписи не получает никакой информации о паре (сообщение, подпись), сформированной клиентом;
— неподделываемость (unforgeability): нарушитель, выступающий в роли клиента, может сформировать корректную подпись только в результате успешного взаимодействия с подписывающим.

Поскольку настоящая работа посвящена анализу свойства неподделываемости, рассмотрим подробнее именно данное свойство.

Возможности нарушителя. Нарушителю, выступающему в роли клиента, предоставляется возможность получать от подписывающего корректные подписи для адаптивно выбираемых им сообщений, при этом предполагается, что подписывающий функционирует корректным образом. Наиболее сильной возможностью нарушителя, которую целесообразно рассматривать, является проведение атаки с параллельными сеансами: нарушитель может начинать выполнение новых сеансов протокола формирования подписи до завершения предыдущих.

Угроза. Угроза формализуется с помощью понятия «ещё одной подделки» (one-more forgery). Задача нарушителя состоит в создании $(\ell + 1)$ корректной пары (сообщение, подпись) в результате ℓ успешных взаимодействий с подписывающим. Тривиальной атакой, доступной нарушителю, является дублирование пары (сообщение, подпись), сформированной в результате успешного взаимодействия с подписывающим. Поэтому, как и в стандартных моделях безопасности для схем подписи, на формируемые пары накладываются дополнительные ограничения:

— слабая угроза: все пары (сообщение, подпись) должны быть различными;
— сильная угроза: все сообщения должны быть различными.

Соответствующие данным угрозам свойства будем называть свойствами сильной неподделываемости для слабой угрозы и слабой неподделываемости для сильной угрозы.

4. Анализ безопасности относительно свойства сильной неподделываемости

В работе [5] построена атака на свойство неподделываемости для схемы подписи вслепую Брандса [9], применимая в модели с параллельными сеансами и позволяющая сформировать $(\ell+1)$ подпись для одного и того же «номера аккаунта» в результате $\ell \geqslant \lceil \log q \rceil$ успешных взаимодействий с подписывающим.

Оказалось, что аналогичная атака применима и к схеме Шаума — Педерсена. При этом для данной схемы атака позволяет построить $(\ell+1)$ подпись для одного и того же сообщения, т. е. реализовать слабую угрозу. Опишем данную атаку, а также условия её применимости в случае формирования $(\ell+1)$ подписи для различных сообщений.

Атака типа ROS. Пусть нарушитель $\mathcal{A}$:

1) Выбирает сообщение $m \in \{0,1\}^*$, для которого будет построена $(\ell+1)$ подпись, пусть $M' = M = \mathcal{H}(m)$.
2) Открывает ℓ параллельных сеансов, отправляя подписывающему ℓ одинаковых запросов с точкой M.
3) Получает в ответ ℓ наборов (Z, A_i, B_i), $0 \leqslant i \leqslant \ell-1$, удовлетворяющих условиям

$$Z = dM,\ A_i = k_i P,\ B_i = k_i M,$$

где k_i выбирается подписывающим случайно и равновероятно для каждого открытого сеанса.
4) Выбирает u_i^0, u_i^1, $0 \leqslant i \leqslant \ell-1$, таким образом, чтобы $c_{i0} \neq c_{i1}$, где

$$c'_{i0} = H(M\|Z\|u_i^0 A_i\|u_i^0 B_i), \quad c'_{i1} = H(M\|Z\|u_i^1 A_i\|u_i^1 B_i),$$
$$c_{i0} = (u_i^0)^{-1} c'_{i0}, \quad c_{i1} = (u_i^1)^{-1} c'_{i1}.$$

5) Определяет $\rho_0, \rho_1, \ldots, \rho_\ell$ как коэффициенты перед x_i в выражении

$$\sum_{i=0}^{\ell-1} 2^i \frac{x_i - c_{i0}}{c_{i1} - c_{i0}} = \sum_{i=0}^{\ell-1} \rho_i x_i + \rho_\ell.$$

6) Полагает $A_\ell = \sum\limits_{i=0}^{\ell-1} \rho_i A_i - \rho_\ell Q$, $B_\ell = \sum\limits_{i=0}^{\ell-1} \rho_i B_i - \rho_\ell Z$.
7) Вычисляет $c'_\ell = H(M\|Z\|A_\ell\|B_\ell)$.
8) Определяет $b_0, \ldots, b_{\ell-1}$ как $c'_\ell = \sum\limits_{i=0}^{\ell-1} 2^i b_i$.
9) Полагает $c_i = c_{ib_i}, c'_i = c'_{ib_i}, u_i = u_i^{b_i}, 0 \leqslant i \leqslant \ell-1$, таким образом, $c'_\ell = \sum\limits_{i=0}^{\ell-1} \rho_i c_i + \rho_\ell$.
10) Отправляет подписывающему значения $c_0, \ldots, c_{\ell-1}$ в соответствующих открытых сеансах.
11) Получает в ответ от подписывающего значения $s_0, \ldots, s_{\ell-1}$, такие, что

$$s_i P = A_i + c_i Q, \quad s_i M = B_i + c_i Z.$$

12) Полагает $s'_i = u_i s_i, , 0 \leqslant i \leqslant \ell-1$.
13) Полагает $s'_\ell = \sum\limits_{i=0}^{\ell-1} \rho_i s_i$.
14) Выдаёт $\{\big(m, (s'_i, c'_i, Z)\big) : i = 0, \ldots, \ell\}$.

Действительно, для $0 \leqslant i \leqslant \ell - 1$ подпись (s'_i, c'_i, Z) будет корректной для сообщения m, так как

$$s'_i P - c'_i Q = u_i s_i P - u_i c_i Q = u_i(s_i P - c_i Q) = u_i A_i,$$
$$s'_i M - c'_i Z = u_i s_i M - u_i c_i Z = u_i(s_i M - c_i Z) = u_i B_i,$$

а по построению $c'_i = H(M\|Z\|u_i A_i\|u_i B_i)$.

Для $i = \ell$ подпись (s'_ℓ, c'_ℓ, Z) будет корректной для сообщения m, так как

$$s'_\ell P - c'_\ell Q = \sum_{i=0}^{\ell-1} \rho_i s_i P - \sum_{i=0}^{\ell-1} \rho_i c_i Q - \rho_\ell Q = \sum_{i=0}^{\ell-1} \rho_i (s_i P - c_i Q) - \rho_\ell Q = \sum_{i=0}^{\ell-1} \rho_i A_i - \rho_\ell Q = A_\ell,$$
$$s'_\ell M - c'_\ell Z = \sum_{i=0}^{\ell-1} \rho_i s_i M - \sum_{i=0}^{\ell-1} \rho_i c_i Z - \rho_\ell Z = \sum_{i=0}^{\ell-1} \rho_i (s_i M - c_i Z) - \rho_\ell Z = \sum_{i=0}^{\ell-1} \rho_i B_i - \rho_\ell Z = B_\ell,$$

а по построению $c'_\ell = H(M\|Z\|A_\ell\|B_\ell)$.

Условие $\ell \geqslant \lceil \log q \rceil$ необходимо для того, чтобы было возможно осуществить шаг 8.

В настоящей атаке нарушитель не использует значения маскирующих факторов α и v (полагает их равными единице и нулю соответственно), в связи с этим пары (сообщение, подпись), построенные на шаге 14, можно соотнести с соответствующими стенограммами протокола, т. е. для них не выполняется свойство неотслеживаемости. Однако представляется, что атака может быть расширена с целью обеспечения неотслеживаемости для сформированных пар.

Модификация атаки на случай разных сообщений. Рассмотрим структурные особенности схемы Шаума — Педерсена, не позволяющие расширить данную атаку на случай формирования подписей для различных сообщений. Ключевым отличием схемы Шаума — Педерсена от схемы Шнорра является наличие первой пересылки $M = \alpha^{-1} M'$ от пользователя к подписывающему, содержимое которой существенно зависит от сообщения, и добавление в подпись элемента $Z' = dM'$. Для построения подделки для нового сообщения m, которому соответствует точка $M' = \mathcal{H}(m)$, нарушителю необходимо вычислить значение $Z' = dM'$.

Заметим, однако, что если дискретный логарифм точки M' по основанию P известен нарушителю (пусть $\mathrm{DLog}_P(M') = \beta$), то соответствующая точка Z' может быть вычислена как $\beta Q = d(\beta P) = dM'$. В этом случае описанная выше атака может быть расширена на случай подписания различных сообщений в каждом сеансе (а значит, различных точек $M'_i = M_i$ и Z_i в каждом сеансе). Все шаги атаки выполняются аналогично, за исключением алгоритма вычисления точек Z_ℓ и B_ℓ. Точка Z_ℓ, как уже было сказано, вычисляется как βQ, а точка B_ℓ полагается равной βA_ℓ. Нетрудно проверить, что подпись $(s'_\ell, c'_\ell, Z_\ell)$ будет корректной подписью для сообщения m, соответствующего точке $M' = \beta P$.

Таким образом, для безопасности схемы критично важно формировать точку M' таким образом, чтобы её дискретный логарифм был неизвестен нарушителю. Именно поэтому для формирования M' в схеме Шаума — Педерсена предлагается использовать функцию хеширования в кривую.

Замечание 1. В оригинальной схеме подписи вслепую Брандса [9], а также в модификации данной схемы для группы точек эллиптической кривой, используемой в системе U-Prove [23], элемент группы M' формируется как линейная комбинация элементов с взаимно неизвестным дискретным логарифмом, таким образом, дискретный логарифм M' неизвестен нарушителю. Однако в вариации данной схемы, определённой

в работе [16], элемент M' формируется как αP, поэтому по построению пользователю всегда известен дискретный логарифм M'. Таким образом, для этой вариации схемы свойство неподделываемости не обеспечивается даже в слабом смысле.

Если дискретный логарифм точки M' по основанию P неизвестен, то описанная атака неприменима из-за сложности построения точек Z_ℓ, B_ℓ, для которых выполнено условие

$$B_\ell = \sum_{i=0}^{\ell-1} \rho_i B_i = \sum_{i=0}^{\ell-1} \rho_i (s_i M_i - c_i Z_i) = s_\ell M_\ell - c_\ell Z_\ell.$$

5. Анализ безопасности относительно свойства слабой неподделываемости

Получим оценку стойкости схемы Шаума — Педерсена относительно свойства слабой неподделываемости с помощью метода сведений.

Сведение удалось построить в модели wUF (weak UnForgeability), см. формальное определение в Приложении А, при некоторых дополнительных ограничениях на возможности нарушителя: в модели с алгебраической группой и случайным оракулом. Рассмотрим подробнее, какие ограничения налагают данные модели.

Модель со случайным оракулом введена в [13] и подразумевает, что на этапе инициализации экспериментатор выбирает случайную функцию, после чего предоставляет нарушителю доступ к ней через так называемый случайный оракул. Нарушитель может получать значения случайной функции на произвольном входе α, подавая запрос вида α к случайному оракулу, при этом он не может вычислять значения случайной функции самостоятельно. При обосновании свойства неподделываемости схемы Шаума — Педерсена будем предполагать, что хеш-функции H и $\mathcal{H}$ моделируются как случайные оракулы. Анализ в данной модели можно интерпретировать следующим образом: при получении оценки стойкости не рассматриваются методы криптоанализа, основанные на структурных свойствах конкретных функций H и $\mathcal{H}$, определяющих связь между областью определения и областью значений данных функций.

Модель с алгебраической группой предложена в работе [15]. На алгоритм нарушителя накладывается следующее требование: для любого элемента группы, который появляется на выходе алгоритма нарушителя в процессе его работы, нарушитель должен предоставить коэффициенты разложения данного элемента в линейную комбинацию всех элементов, пришедших ему на вход к данному моменту. То есть если нарушитель возвращает элемент группы Z и на данный момент он получил элементы $X_1, \ldots, X_n$, то вместе с Z он передаёт набор коэффициентов $z = (z_1, \ldots, z_n)$, таких, что $Z = \sum_{i=1}^{n} z_i X_i$. Анализ в данной модели можно интерпретировать следующим образом: при получении оценки стойкости не рассматриваются методы криптоанализа, использующие структурные особенности конкретной группы для формирования новых элементов группы.

5.1. Базовые задачи

Сведение стойкости схемы CP-BS построено к следующим базовым задачам: задаче SOMDL и задаче REPR. Определим их формально.

Задача SOMDL (Strong One-More Discrete Logarithm)

Параметрами настоящей задачи являются $k, \ell \in \mathbb{N}$.

Определение 2. Для нарушителя $\mathcal{A}$, группы $\mathbb{G}$, параметров ℓ и k положим

$$\mathsf{Adv}^{\mathrm{SOMDL}}_{\mathbb{G},k,\ell}(\mathcal{A}) = \Pr\bigl[\mathbf{Exp}^{\mathrm{SOMDL}}_{\mathbb{G},k,\ell}(\mathcal{A}) \to 1\bigr],$$

где эксперимент $\mathbf{Exp}^{\mathrm{SOMDL}}_{\mathbb{G},k,\ell}(\mathcal{A})$ определяется следующим образом:

$\mathbf{Exp}^{\mathrm{SOMDL}}_{\mathbb{G},k,\ell}(\mathcal{A})$

$x_1,\ldots,x_{\ell+1} \xleftarrow{\mathcal{U}} \mathbb{Z}_q^*$
$ctr_1, ctr_2 \leftarrow 0$
$(x'_1,\ldots,x'_{\ell+1}) \leftarrow \mathcal{A}^{O_1,O_2}(x_1P,\ldots,x_{\ell+1}P)$
return $(x_1 = x'_1) \wedge \ldots \wedge (x_{\ell+1} = x'_{\ell+1})$

Oracle $O_1(i, Y)$

if $ctr_1 > k$: **return** $\perp$
if $i \notin \{1,\ldots,\ell+1\}$: **return** $\perp$
if $Y \notin \mathbb{G}$: **return** $\perp$
$ctr_1 \leftarrow ctr_1 + 1$
return x_iY

Oracle $O_2(Y)$

if $ctr_2 > \ell$: **return** $\perp$
if $Y \notin \mathbb{G}$: **return** $\perp$
$ctr_2 \leftarrow ctr_2 + 1$
return $\mathrm{DLog}_P(Y)$

Нарушитель получает на вход набор точек $x_1P,\ldots,x_{\ell+1}P$, его задача — найти значения $x_1,\ldots,x_{\ell+1}$. Нарушитель имеет доступ к двум оракулам O_1 и O_2, он может делать не более k запросов к первому оракулу и не более ℓ — ко второму. Эти ограничения контролируются с помощью счётчиков ctr_1, ctr_2.

Оракул O_1 в ответ на запрос нарушителя вида (i, Y), $i \in \{1,\ldots,\ell+1\}$, $Y \in \mathbb{G}$, возвращает значение x_iY. Оракул O_2 в ответ на запрос $Y \in \mathbb{G}$ возвращает дискретный логарифм этой точки по основанию P. Запросы к оракулам O_1 и O_2 могут быть выполнены в произвольном порядке.

О соотношении с другими задачами. В результате обзора существующих в литературе задач для конечных групп найдены две наиболее «близкие» к задаче SOMDL: задачи SDL и OMDL. Определим их формально.

Задача SDL (*Strong Discrete Logarithm*) определена в работе [21] как задача q-dlog и является модификацией задачи SDH (*Strong Diffie — Hellman*), предложенной в [24], её параметром является значение $s \in \mathbb{N}$.

Определение 3. Для нарушителя $\mathcal{A}$, группы $\mathbb{G}$ и параметра s положим

$$\mathsf{Adv}^{\mathrm{SDL}}_{\mathbb{G},s}(\mathcal{A}) = \Pr\big[\mathbf{Exp}^{\mathrm{SDL}}_{\mathbb{G},s}(\mathcal{A}) \to 1\big],$$

где эксперимент $\mathbf{Exp}^{\mathrm{SDL}}_{\mathbb{G},s}(\mathcal{A})$ определяется следующим образом:

$\mathbf{Exp}^{\mathrm{SDL}}_{\mathbb{G},s}(\mathcal{A})$

$x \xleftarrow{\mathcal{U}} \mathbb{Z}_q^*$
$x' \leftarrow \mathcal{A}(xP,\ldots,x^sP)$
return $(x = x')$

Нарушитель получает на вход набор точек $xP,\ldots,x^sP$, его задача — найти значение x.

Покажем, что доступ к оракулу O_1 в задаче SOMDL может предоставлять нарушителю такие же возможности, как в задаче SDL. Действительно, подавая на вход оракулу O_1 сначала запрос $(1, x_1P)$, а потом запросы вида $(1, Y)$, где Y — ответ оракула O_1 на предыдущий запрос, нарушитель может накопить значения $x_1P, x_1^2P,\ldots,x_1^{k+1}P$, что аналогично получению на вход таких значений в задаче SDL с параметром $s = k+1$. Отсюда следует

Утверждение 1. Для любого нарушителя $\mathcal{A}$, решающего задачу SDL с параметром $k+1$, существует нарушитель $\mathcal{B}$ с такими же вычислительными ресурсами, решающий задачу SOMDL с параметрами (k,ℓ) для произвольного $\ell \in \mathbb{N}$, такой, что

$$\mathsf{Adv}^{\mathrm{SDL}}_{\mathbb{G},k+1}(\mathcal{A}) \leqslant \mathsf{Adv}^{\mathrm{SOMDL}}_{\mathbb{G},k,\ell}(\mathcal{B}).$$

Таким образом, задача SOMDL с параметрами (k,ℓ) не сложнее задачи SDL с параметром $k+1$.

Задача OMDL (*One-More Discrete Logarithm*) предложена в работе [20], её параметром является значение $\ell \in \mathbb{N}$.

Определение 4. Для нарушителя $\mathcal{A}$, группы $\mathbb{G}$ и параметра ℓ положим

$$\mathsf{Adv}^{\mathrm{OMDL}}_{\mathbb{G},\ell}(\mathcal{A}) = \Pr\bigl[\mathbf{Exp}^{\mathrm{OMDL}}_{\mathbb{G},\ell}(\mathcal{A}) \to 1\bigr],$$

где эксперимент $\mathbf{Exp}^{\mathrm{OMDL}}_{\mathbb{G},\ell}(\mathcal{A})$ определяется следующим образом:

$\mathbf{Exp}^{\mathrm{OMDL}}_{\mathbb{G},\ell}(\mathcal{A})$	Oracle $\mathrm{DLog}(Y)$
$x_1,\ldots,x_{\ell+1} \xleftarrow{\mathcal{U}} \mathbb{Z}_q^*$	**if** $ctr > \ell$: **return** $\perp$
$ctr \leftarrow 0$	**if** $Y \notin \mathbb{G}$: **return** $\perp$
$(x'_1,\ldots,x'_{\ell+1}) \leftarrow \mathcal{A}^{\mathrm{Dlog}}(x_1P,\ldots,x_{\ell+1}P)$	$ctr \leftarrow ctr + 1$
return $(x_1 = x'_1) \wedge \ldots \wedge (x_{\ell+1} = x'_{\ell+1})$	**return** $\mathrm{DLog}_P(Y)$

Нарушитель получает на вход набор точек $x_1P,\ldots,x_{\ell+1}P$, его задача — найти значения $x_1,\ldots,x_{\ell+1}$. Нарушитель имеет доступ к оракулу DLog, который в ответ на запрос $Y \in \mathbb{G}$ возвращает дискретный логарифм этой точки по основанию P. Он может делать не более ℓ запросов к этому оракулу, это ограничение контролируется с помощью счётчика ctr. Заметим, что оракул в задаче OMDL в точности совпадает с оракулом O_2 в задаче SOMDL. Отсюда следует

Утверждение 2. Для любого нарушителя $\mathcal{A}$, решающего задачу OMDL с параметром ℓ, существует нарушитель $\mathcal{B}$ с такими же вычислительными ресурсами, решающий задачу SOMDL с параметрами (k,ℓ) для произвольного $k \in \mathbb{N}$, такой, что

$$\mathsf{Adv}^{\mathrm{OMDL}}_{\mathbb{G},\ell}(\mathcal{A}) \leqslant \mathsf{Adv}^{\mathrm{SOMDL}}_{\mathbb{G},k,\ell}(\mathcal{B}).$$

Таким образом, задача SOMDL с параметрами (k,ℓ) не сложнее задачи OMDL с параметром ℓ.

Утверждения 1 и 2 показывают, что из сложности задачи SOMDL следует сложность известных задач SDL и OMDL, однако на данный момент не удалось получить результатов, что сложность этих базовых задач является достаточным условием сложности SOMDL. Таким образом, задача SOMDL — это новая задача, требующая отдельных исследований.

Задача REPR

Эта задача — модификация задачи Representation [9], её параметром является значение $s \in \mathbb{N}$.

Определение 5. Для нарушителя $\mathcal{A}$, группы $\mathbb{G}$ и параметра s положим

$$\mathsf{Adv}^{\mathrm{REPR}}_{\mathbb{G},s}(\mathcal{A}) = \Pr\bigl[\mathbf{Exp}^{\mathrm{REPR}}_{\mathbb{G},s}(\mathcal{A}) \to 1\bigr],$$

где эксперимент $\mathbf{Exp}^{\mathrm{REPR}}_{\mathbb{G},s}(\mathcal{A})$ определяется следующим образом:

$\mathbf{Exp}^{\mathrm{REPR}}_{\mathbb{G},s}(\mathcal{A})$

$x_1, \ldots, x_s \xleftarrow{\mathcal{U}} \mathbb{Z}_q^*$

$(\alpha_1, \ldots, \alpha_s, \beta) \leftarrow \mathcal{A}(x_1 P, \ldots, x_s P)$

return $(\alpha_1 x_1 + \ldots + \alpha_s x_s + \beta = 0) \wedge (\exists i : \alpha_i \neq 0)$

Нарушитель получает на вход набор точек $x_1 P, \ldots, x_s P$, его задача — найти такие значения $\alpha_1, \ldots, \alpha_s, \beta$, что линейная комбинация $x_1, \ldots, x_s$ с коэффициентами $\alpha_1, \ldots, \alpha_s$ равна $(-\beta)$.

5.2. Оценка стойкости в модели wUF

Через $\mathsf{Adv}^{\mathrm{wUF}}_{\mathsf{CP\text{-}BS}}(\mathcal{A})$ будем обозначать преимущество нарушителя $\mathcal{A}$ для схемы CP-BS в модели wUF со случайным оракулом и алгебраической группой (вероятность построения подделки).

Теорема 1. Для любого нарушителя $\mathcal{A}$ для схемы CP-BS в модели wUF с алгебраической группой, делающего не более t и ℓ запросов к оракулам Sign_1 и Sign_2 соответственно и не более q_1 и q_2 запросов к случайным оракулам, моделирующим работу хеш-функций $\mathcal{H}$ и H соответственно, существуют нарушитель $\mathcal{B}$, решающий задачу SOMDL с параметрами $(2t, t)$, и нарушитель $\mathcal{C}$, решающий задачу REPR с параметром $(q_1 + \ell + 1)$, такие, что

$$\mathsf{Adv}^{\mathrm{wUF}}_{\mathsf{CP\text{-}BS}}(\mathcal{A}) \leqslant 2\,\mathsf{Adv}^{\mathrm{SOMDL}}_{\mathbb{G},2t,t}(\mathcal{B}) + \mathsf{Adv}^{\mathrm{REPR}}_{\mathbb{G},q_1+\ell+1}(\mathcal{C}) + \frac{2(\ell+1)+q_2}{q}.$$

При этом $T_{\mathcal{B}} \approx 2T_{\mathcal{A}}$, $T_{\mathcal{C}} \approx T_{\mathcal{A}}$, где $T_{\mathcal{A}}, T_{\mathcal{B}}, T_{\mathcal{C}}$ — вычислительные ресурсы нарушителей $\mathcal{A}, \mathcal{B}, \mathcal{C}$ соответственно.

Доказательство теоремы 1 приведено в Приложении В.

Интерпретация оценки. Полученная оценка стойкости свидетельствует о том, что сложность задач SOMDL и REPR является достаточным условием стойкости схемы CP-BS в модели wUF со случайным оракулом и алгебраической группой при соответствующих значениях параметров схемы. Более того, рассмотрение каждого из слагаемых, входящих в оценку, позволяет сделать вывод о некоторых необходимых условиях стойкости схемы. Далее сопоставим каждое слагаемое конкретным методам взлома схемы CP-BS.

Первое слагаемое учитывает атаки на схему CP-BS, направленные на восстановление ключа подписи d или эфемерного значения k хотя бы в одном из сеансов (в частности, за счёт совпадения значений k в нескольких сеансах).

Для задачи SOMDL на текущий момент неизвестно более эффективных методов решения, чем за счёт решения либо задачи SDL, либо задачи OMDL. Для задачи OMDL неизвестно более эффективных методов решения, чем решение задачи дискретного логарифмирования [25]. Для задачи SDL известен метод решения, вычислительная трудоёмкость которого ниже, чем трудоёмкость известных методов решения задачи дискретного логарифмирования, — метод, предложенный в [26] для случая, когда параметр s является делителем $(q-1)$. Он требует $T_{\mathrm{op}} = c_1 \log q\,(\sqrt{q/s} + \sqrt{s})$ вычислений групповых операций и $T_{\mathrm{mem}} = c_2 \max(\sqrt{q/s}, \sqrt{s})$ памяти, где c_1, c_2 — константы, зависящие только от используемой модели вычислений.

Заметим, что метод [26] позволяет восстановить ключ подписи схемы CP-BS. Действительно, нарушитель, выступающий в роли клиента, может последовательно открыть t сеансов, посылая в первом сеансе в первой пересылке значение $M_1 = Q = dP$,

а в последующих сеансах — значения $M_i = Z_{i-1} = dM_{i-1} = d^iP$, $2 \leqslant i \leqslant t$, где Z_{i-1} — значение Z, полученное в ответ от сервера в $(i-1)$-м сеансе. Таким образом, в качестве значений Z_i, $1 \leqslant i \leqslant t$, в открытых сеансах нарушитель получит значения $d^2P, \ldots, d^{t+1}P$. Тогда, используя метод решения задачи SDL с параметром $s = t+1$ из работы [26], нарушитель восстанавливает ключ подписи d и успешно реализует угрозу.

Пусть количество t открытых сеансов протокола формирования подписи вслепую не превышает 2^{64}. Обозначим через s_m максимальный делитель числа $(q-1)$ для заданной кривой $\mathcal{E}$, такой, что $s_m \leqslant 2^{64}+1$. В таблице приведены значения s_m и параметры метода для стандартизированных в России эллиптических кривых простого порядка, определённых в [27].

Кривая	$\log q$	s_m	op	mem
id-tc26-gost-3410-2012-256-paramSetB	256	$\approx 2^{32}$	2^{120}	2^{112}
id-tc26-gost-3410-2012-256-paramSetC	256	$\approx 2^{62}$	2^{105}	2^{97}
id-tc26-gost-3410-2012-256-paramSetD	256	$\approx 2^{64}$	2^{104}	2^{96}
id-tc26-gost-3410-12-512-paramSetA	512	$\approx 2^{25}$	2^{252}	2^{243}
id-tc26-gost-3410-12-512-paramSetB	512	$\approx 2^{11}$	2^{259}	2^{250}

Значения T_{op} и T_{mem} рассматриваемого метода равны $c_1 \cdot \text{op}$ и $c_2 \cdot \text{mem}$ соответственно.

Таким образом, в схеме CP-BS рекомендуется использовать эллиптические кривые с как можно меньшим значением s_m.

Второе слагаемое учитывает атаки на схему CP-BS, направленные на поиск соотношений между точками $M'_i = \mathcal{H}(m_i)$ для различных сообщений m_i и генерационной точкой P.

Для задачи REPR неизвестно лучших методов решения, чем решение задачи дискретного логарифмирования [9]. Заметим, что решение задачи дискретного логарифмирования хотя бы для одной точки $M'_i = \mathcal{H}(m_i)$, $1 \leqslant i \leqslant q_1$, позволяет реализовать атаку типа ROS, описанную в п. 4.

Третье слагаемое учитывает атаки на схему CP-BS, направленные на перебор значения c' в подписи. Действительно, для фиксированных значений Z', s' и сообщения m вероятность найти значение c', такое, что алгоритм проверки подписи завершится успешно, можно оценить как $\dfrac{q_2}{q-1}$, где q_2 — количество вычислений хеш-функции H.

Вывод. Полученная оценка указывает, что достаточным условием стойкости схемы CP-BS в модели wUF со случайным оракулом и алгебраической группой является сложность задач SOMDL и REPR. На данный момент не удалось доказать, что сложность задачи SOMDL является необходимым условием стойкости схемы в указанной модели. Исходя из рассуждений выше, необходимым условием является сложность другой задачи в группе — задачи SDL. Для задачи SDL, в свою очередь, в [21] получены результаты, косвенно свидетельствующие в пользу того, что эта задача в общем случае может быть легче, чем задача дискретного логарифмирования. Более того, так как решение задачи SOMDL не удалось пока свести только к решению SDL, могут быть обнаружены другие методы, решающие задачу SOMDL и приводящие к взлому схемы CP-BS. Таким образом, из-за слабой изученности как необходимых, так и достаточных для стойкости схемы базовых задач требуется проведение дополнительных исследований их сложности.

ЛИТЕРАТУРА

1. *Chaum D.* Blind signatures for untraceable payments // D. Chaum, R. L. Rivest, and A. T. Sherman (eds.). Advances in Cryptology. Boston, MA: Springer, 1983. P. 199–203.
2. *Fujioka A., Okamoto T., and Ohta K.* A practical secret voting scheme for large scale elections // LNCS. 1993. V. 718. P. 244–251.
3. *Pointcheval D. and Stern J.* Provably secure blind signature schemes // LNCS. 1996. V. 1163. P. 252–265.
4. *Schnorr C. P.* Security of blind discrete log signatures against interactive attacks // LNCS. 2001. V. 2229. P. 1–12.
5. *Benhamouda F., Lepoint T., Loss J., et al.* On the (in) security of ROS // J. Cryptology. 2022. V. 35. No. 4. Article 25.
6. *Akhmetzyanova L., Alekseev E., Babueva A., and Smyshlyaev S.* On the (im)possibility of secure ElGamal blind signatures // Матем. вопр. криптогр. 2023. Т. 14. № 2. С. 25–42.
7. *Pointcheval D. and Stern J.* Security arguments for digital signatures and blind signatures // J. Cryptology. 2000. V. 13. P. 361–396.
8. *Abe M. and Okamoto T.* Provably secure partially blind signatures // LNCS. 2000. V. 1880. P. 271–286.
9. *Brands S.* Untraceable off-line cash in wallets with observers // LNCS. 1994. V. 773. P. 302–318.
10. *Chaum D. and Pedersen T. P.* Wallet databases with observers // LNCS. 1993. V. 740. P. 89–105.
11. *Fischlin M. and Schroder D.* On the impossibility of three-move blind signature schemes // LNCS. 2010. V. 6110. P. 197–215.
12. *Pass R.* Limits of provable security from standard assumptions // Proc. 43rd Ann. ACM Symp. Theory Computing. San Jose, California, USA, 2011. P. 109–118.
13. *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.
14. *Nechaev V. I.* Complexity of a determinate algorithm for the discrete logarithm // Math. Notes. 1994. V. 55. No. 2. P. 165–172.
15. *Fuchsbauer G., Kiltz E., and Loss J.* The algebraic group model and its applications // LNCS. 2018. V. 10992. P. 33–62.
16. *Baldimtsi F. and Lysyanskaya A.* On the security of one-witness blind signature schemes // LNCS. 2013. V. 8270. P. 82–99.
17. *Chairattana-Apirom R., Tessaro S., and Zhu C.* Pairing-Free Blind Signatures from CDH Assumptions. Cryptology ePrint Archive. 2023. Paper 2023/1780. `https://eprint.iacr.org/2023/1780`.
18. *Crites E., Komlo C., Maller M., et al.* Snowblind: A threshold blind signature in pairing-free groups // LNCS. 2023. V. 14081. P. 710–742.
19. *Tessaro S. and Zhu C.* Short pairing-free blind signatures with exponential security // LNCS. 2022. V. 13276. P. 782–811.
20. *Bellare M., Namprempre C., Pointcheval D., and Semanko M.* The one-more-RSA-inversion problems and the security of Chaum's blind signature scheme // J. Cryptology. 2003. V. 16. No. 3. P. 185–215.
21. *Bauer B., Fuchsbauer G., and Loss J.* A classification of computational assumptions in the algebraic group model // LNCS. 2020. V. 12171. P. 121–151.
22. *Faz-Hernandez A., Scott S., Sullivan N., et al.* Hashing to Elliptic Curves. `https://datatracker.ietf.org/doc/rfc9380/`.

23. *Paquin C. and Zaverucha G.* U-Prove Cryptographic Specification V1.1 (Revision 3). https://www.microsoft.com/en-us/research/publication/u-prove-cryptographic-specification-v1-1-revision-3/. 2013.
24. *Boneh D. and Boyen X.* Short signatures without random oracles // LNCS. 2004. V. 3027. P. 56–73.
25. *Koblitz N. and Menezes A.* Another look at non-standard discrete log and Diffie — Hellman problems // J. Math. Cryptology. 2008. V. 2. No. 4. P. 311–326.
26. *Cheon J. H.* Security analysis of the strong Diffie — Hellman problem // LNCS. 2006. V. 4004. P. 1–11.
27. Р 1323565.1.024-2019 «Информационная технология. Криптографическая защита информации. Параметры эллиптических кривых для криптографических алгоритмов и протоколов». М.: Стандартинформ, 2019.
28. *Van der Meer N.* Root Finding over Finite Fields for Secure Multiparty Computation. Bachelor Thesis. Eindhoven University of Technology, 2021.

REFERENCES

1. *Chaum D.* Blind signatures for untraceable payments. D. Chaum, R. L. Rivest, and A. T. Sherman (eds.). Advances in Cryptology, Boston, MA, Springer, 1983, pp. 199–203.
2. *Fujioka A., Okamoto T., and Ohta K.* A practical secret voting scheme for large scale elections. LNCS, 1993, vol. 718, pp. 244–251.
3. *Pointcheval D. and Stern J.* Provably secure blind signature schemes. LNCS, 1996, vol. 1163, pp. 252–265.
4. *Schnorr C. P.* Security of blind discrete log signatures against interactive attacks. LNCS, 2001, vol. 2229, pp. 1–12.
5. *Benhamouda F., Lepoint T., Loss J., et al.* On the (in) security of ROS. J. Cryptology, 2022, vol. 35, no. 4, Article 25.
6. *Akhmetzyanova L., Alekseev E., Babueva A., and Smyshlyaev S.* On the (im)possibility of secure ElGamal blind signatures. Matem. Vopr. Kriptogr., 2023, vol. 14, no. 2, pp. 25–42.
7. *Pointcheval D. and Stern J.* Security arguments for digital signatures and blind signatures. J. Cryptology, 2000, vol. 13, pp. 361–396.
8. *Abe M. and Okamoto T.* Provably secure partially blind signatures. LNCS, 2000, vol. 1880, pp. 271–286.
9. *Brands S.* Untraceable off-line cash in wallets with observers. LNCS, 1994, vol. 773, pp. 302–318.
10. *Chaum D. and Pedersen T. P.* Wallet databases with observers. LNCS, 1993, vol. 740, pp. 89–105.
11. *Fischlin M. and Schroder D.* On the impossibility of three-move blind signature schemes. LNCS, 2010, vol. 6110, pp. 197–215.
12. *Pass R.* Limits of provable security from standard assumptions. Proc. 43rd Ann. ACM Symp. Theory Computing, San Jose, California, USA, 2011, pp. 109–118.
13. *Bellare M. and Rogaway P.* Random oracles are practical: A paradigm for designing efficient protocols. Proc. CCS'93, Fairfax, Virginia, USA, 1993, pp. 62–73.
14. *Nechaev V. I.* Complexity of a determinate algorithm for the discrete logarithm. Math. Notes, 1994, vol. 55, no. 2, pp. 165–172.
15. *Fuchsbauer G., Kiltz E., and Loss J.* The algebraic group model and its applications. LNCS, 2018, vol. 10992, pp. 33–62.
16. *Baldimtsi F. and Lysyanskaya A.* On the security of one-witness blind signature schemes. LNCS, 2013, vol. 8270, pp. 82–99.

17. *Chairattana-Apirom R., Tessaro S., and Zhu C.* Pairing-Free Blind Signatures from CDH Assumptions. Cryptology ePrint Archive, 2023, Paper 2023/1780, https://eprint.iacr.org/2023/1780.
18. *Crites E., Komlo C., Maller M., et al.* Snowblind: A threshold blind signature in pairing-free groups. LNCS, 2023, vol. 14081, pp. 710–742.
19. *Tessaro S. and Zhu C.* Short pairing-free blind signatures with exponential security. LNCS, 2022, vol. 13276, pp. 782–811.
20. *Bellare M., Namprempre C., Pointcheval D., and Semanko M.* The one-more-RSA-inversion problems and the security of Chaum's blind signature scheme. J. Cryptology, 2003, vol. 16, no. 3, pp. 185–215.
21. *Bauer B., Fuchsbauer G., and Loss J.* A classification of computational assumptions in the algebraic group model. LNCS, 2020, vol. 12171, pp. 121–151.
22. *Faz-Hernandez A., Scott S., Sullivan N., et al.* Hashing to Elliptic Curves. https://datatracker.ietf.org/doc/rfc9380/.
23. *Paquin C. and Zaverucha G.* U-Prove Cryptographic Specification V1.1 (Revision 3). https://www.microsoft.com/en-us/research/publication/u-prove-cryptographic-specification-v1-1-revision-3/, 2013.
24. *Boneh D. and Boyen X.* Short signatures without random oracles. LNCS, 2004, vol. 3027, pp. 56–73.
25. *Koblitz N. and Menezes A.* Another look at non-standard discrete log and Diffie — Hellman problems. J. Math. Cryptology, 2008, vol. 2, no. 4, pp. 311–326.
26. *Cheon J. H.* Security analysis of the strong Diffie — Hellman problem. LNCS, 2006, vol. 4004, pp. 1–11.
27. R 1323565.1.024-2019 «Informatsionnaya tekhnologiya. Kriptograficheskaya zashchita informatsii. Parametry ellipticheskih krivyh dlya kriptograficheskih algoritmov i protokolov» [R 1323565.1.024-2019 "Information Technology. Cryptographic Data Security. Elliptic Curve Parameters for the Cryptographic Algorithms and Protocols"]. Moscow, Standartinform Publ., 2019. (in Russian)
28. *Van der Meer N.* Root Finding over Finite Fields for Secure Multiparty Computation. Bachelor Thesis, Eindhoven University of Technology, 2021.

Приложение А. Модель wUF (weak UnForgeability)

Определим формально модель wUF, в которой предполагается, что нарушитель имеет возможность проводить атаку с параллельными сеансами, а его задача — сформировать $(\ell + 1)$ корректную пару (сообщение, подпись) для различных сообщений в результате ℓ успешных взаимодействий с подписывающим.

Данную модель определим для двухраундовых схем подписи вслепую. Протокол формирования подписи $\langle \mathsf{Sign}, \mathsf{User} \rangle$ в таких схемах можно формально задать следующим образом:

$$
\begin{aligned}
&(msg_{U,0}, state_{U,0}) \leftarrow \mathsf{BS.User}_0(\mathsf{pk}, m)\\
&(msg_{S,1}, state_{S,1}) \leftarrow \mathsf{BS.Sign}_1(\mathsf{sk}, \mathsf{pk}, msg_{U,0})\\
&(msg_{U,1}, state_{U,1}) \leftarrow \mathsf{BS.User}_1(state_{U,0}, msg_{S,1})\\
&(msg_{S,2}, b) \leftarrow \mathsf{BS.Sign}_2(state_{S,1}, msg_{U,1})\\
&\sigma \leftarrow \mathsf{BS.User}_2(state_{U,1}, msg_{S,2})
\end{aligned}
$$

Здесь $msg_{role,i}$ означает сообщение с порядковым номером i, отправляемое стороной $role \in \{U, S\}$ в рамках протокола, а переменная $state_{role,i}$ позволяет стороне взаимо-

действия *role* сохранить некоторое внутреннее состояние на i-м раунде и использовать его на последующем раунде.

Определение 6. Для двухраундовой схемы подписи вслепую BS положим

$$\mathsf{Adv}^{\mathrm{wUF}}_{\mathsf{BS}}(\mathcal{A}) = \Pr\bigl[\mathbf{Exp}^{\mathrm{wUF}}_{\mathsf{BS}}(\mathcal{A}) \to 1\bigr],$$

где эксперимент $\mathbf{Exp}^{\mathrm{wUF}}_{\mathsf{BS}}(\mathcal{A})$ определяется следующим образом:

$\mathbf{Exp}^{\mathrm{wUF}}_{\mathsf{BS}}(\mathcal{A})$

1 : $(\mathsf{sk}, \mathsf{pk}) \leftarrow \mathsf{BS.KGen}(\,)$
2 : $\mathsf{sid}, \ell \leftarrow 0, \mathcal{I}_{\mathsf{fin}} \leftarrow \varnothing$
3 : $\{(m^*_k, \sigma^*_k)\}_{k=1}^{\ell+1} \leftarrow \mathcal{A}^{\mathrm{Sign}_1, \mathrm{Sign}_2}(\mathsf{pk})$
4 : **return** $(\forall k_1 \neq k_2 \in \{1, \ldots, \ell+1\} : m^*_{k_1} \neq m^*_{k_2}$
5 : $\quad \wedge \forall k \in \{1, \ldots, \ell+1\} : \mathsf{BS.Verify}(\mathsf{pk}, m^*_k, \sigma^*_k) = 1)$

Oracle $\mathrm{Sign}_1(msg)$

1 : $\mathsf{sid} \leftarrow \mathsf{sid} + 1$
2 : $(msg', state_{\mathsf{sid}}) \leftarrow \mathsf{BS.Sign}_1(\mathsf{sk}, \mathsf{pk}, msg)$
3 : **return** (sid, msg')

Oracle $\mathrm{Sign}_2(j, msg)$

1 : **if** $j \notin [\mathsf{sid}] \setminus \mathcal{I}_{\mathsf{fin}}$: **return** $\perp$
2 : $(msg', b) \leftarrow \mathsf{BS.Sign}_2(state_j, msg)$
3 : **if** $b = 1 : \ell \leftarrow \ell + 1$
4 : $\mathcal{I}_{\mathsf{fin}} \leftarrow \mathcal{I}_{\mathsf{fin}} \cup \{j\}$
5 : **return** msg'

Приложение B. Доказательство теоремы 1

Пусть $\mathcal{A}$ — нарушитель для схемы подписи CP-BS в модели wUF. У него есть доступ к четырём оракулам: $\mathrm{Sign}_1, \mathrm{Sign}_2, \mathrm{RO}_1, \mathrm{RO}_2$. Оракул RO_1 моделирует работу хеш-функции $\mathcal{H}$ и возвращает точки эллиптической кривой (за исключением нулевой точки). Оракул RO_2 моделирует работу хеш-функции H и возвращает элементы $\mathbb{Z}_q^*$. Пусть нарушитель $\mathcal{A}$ делает не более t запросов к оракулу Sign_1, не более ℓ запросов к оракулу Sign_2, $\ell \leqslant t$, не более q_1 запросов к оракулу RO_1, не более q_2 запросов к оракулу RO_2. Таким образом, нарушитель $\mathcal{A}$ завершит ℓ сеансов протокола формирования подписи и откроет t сеансов. В результате своей работы нарушитель $\mathcal{A}$ возвращает $(\ell+1)$ пару (сообщение, подпись).

Ш а г 1. Нарушитель $\mathcal{A}$ для любой точки, которую он выдаёт, обязан предоставить разложение по элементам группы, которые появлялись до этого момента в рамках эксперимента (в силу того, что рассматривается модель с алгебраической группой).

За время эксперимента нарушитель $\mathcal{A}$ получает от экспериментатора точки P, Q, A_i, B_i, Z_i, $i = 1, \ldots, t$, M'_i, $i = 1, \ldots, q_1$.

Нарушитель $\mathcal{A}$ подаёт точки M_j, $1 \leqslant j \leqslant t$, на вход оракулу Sign_1, точки M'_j, Z'_j, A'_j, B'_j, $j = 1 \ \ldots, q_2$, — на вход оракулу RO_2, а также точки Z'_i, $1 \leqslant i \leqslant \ell+1$, — в составе подписей в подделке. Для всех этих точек он должен предоставить разложение.

Зафиксируем наборы коэффициентов

$$\bigl(\alpha_i, \beta_i, \{\gamma_{ij} : j = 1, \ldots, t\}, \{\sigma_{ij} : j = 1, \ldots, t\}, \{\eta_{ij} : j = 1, \ldots, t\}, \{\xi_{ij} : j = 1, \ldots, q_1\}\bigr),$$

определяющие разложение точек B'_i, $1 \leqslant i \leqslant q_2$, подаваемых нарушителем на вход оракулу RO_2. Пусть

$$B'_i = \alpha_i P + \beta_i Q + \sum_{j=1}^{t} \gamma_{ij} A_j + \sum_{j=1}^{t} \sigma_{ij} B_j + \sum_{j=1}^{t} \eta_{ij} Z_j + \sum_{j=1}^{q_1} \xi_{ij} M'_j.$$

Зафиксируем также наборы коэффициентов

$$\big(\hat\alpha_j, \hat\beta_j, \{\hat\gamma_{ji} : i{=}1,\dots,j-1\}, \{\hat\sigma_{ji} : i{=}1,\dots,j-1\}, \{\hat\eta_{ji} : i{=}1,\dots,j-1\}, \{\hat\xi_{ji} : i{=}1,\dots,q_1\}\big),$$

определяющие разложение точек M_j, $1 \leqslant j \leqslant t$, подаваемых нарушителем на вход оракулу Sign_1. Пусть

$$M_j = \hat\alpha_j P + \hat\beta_j Q + \sum_{i=1}^{j-1} \hat\gamma_{ji} A_i + \sum_{i=1}^{j-1} \hat\sigma_{ji} B_i + \sum_{i=1}^{j-1} \hat\eta_{ji} Z_i + \sum_{i=1}^{q_1} \hat\xi_{ji} M'_i.$$

Ш а г 2. Пусть нарушитель $\mathcal{A}$ выдал некоторую корректную пару $(m, (s', c', Z'))$ в качестве подделки. Нарушитель $\mathcal{A}$ мог делать запрос $M' \parallel Z' \parallel A' \parallel B'$ к оракулу RO_2, где $M' = \mathcal{H}(m)$, $A' = s'P - c'Q$, $B' = s'M' - c'Z'$, или не делать его.

Если нарушитель $\mathcal{A}$ не делал запрос, то в процессе проверки подписи будет определено новое значение случайной функции, поэтому вероятность того, что функция Verify вернёт 1, не будет превосходить $(q-1)^{-1}$ для конкретного значения подделки. Поскольку количество подделок равно $\ell + 1$, то суммарная вероятность того, что не был сделан хотя бы один запрос, не превышает $(\ell+1)/(q-1)$.

Далее будем рассматривать только те эксперименты, в которых каждой выданной подделке соответствует запрос нарушителя $\mathcal{A}$ к оракулу RO_2.

Ш а г 3. Серверная часть протокола формирования подписи схемы подписи вслепую Шаума — Педерсена в точности повторяет действия доказывающего в протоколе доказательства с нулевым разглашением Шаума — Педерсена [10]. Это протокол доказательства равенства двух дискретных логарифмов:

$$\mathrm{DLog}_P Q = \mathrm{DLog}_M Z.$$

Проверка доказательства осуществляется аналогично проверке подписи в схеме Шаума — Педерсена.

Аналогично протоколу доказательства Шаума — Педерсена, можно показать, что если некоторая подпись (s', c', Z') успешно проходит проверку для сообщения m, то значение Z' в составе этой подписи с большой вероятностью равно dM', где $M' = \mathcal{H}(m)$.

Действительно, пусть для этой подписи $\mathrm{DLog}_{M'} Z' = x \neq d$. Согласно алгоритму проверки подписи, восстановим значения $A' = s'P - c'Q$ и $B' = s'M' - c'Z'$ и рассмотрим соответствующий данной подписи запрос $(M' \parallel Z' \parallel A' \parallel B')$ к оракулу RO_2. Заметим, что в силу шага 2 этот запрос обязательно был сделан. Пусть $k_1 = \mathrm{DLog}_P A'$ и $k_2 = \mathrm{DLog}_{M'} B'$. Тогда для данных значений должны быть выполнены равенства

$$k_1 = s' - c'd, \quad k_2 = s' - c'x.$$

Получаем $s' = k_1 + c'd = k_2 + c'x$, откуда $c' = (k_1 - k_2)/(x - d)$, $d \neq x$. Таким образом, уравнения выполнены (а значит, подпись успешно проверяется) при единственном значении c', которое зафиксировано на момент подачи запроса случайному оракулу. Вероятность того, что для конкретного запроса выход случайного оракула примет значение $(k_1 - k_2)/(x - d)$, равна $(q-1)^{-1}$.

Поскольку нарушитель $\mathcal{A}$ делает не более q_2 запросов к случайному оракулу RO_2, вероятность того, что хотя бы для одного запроса будет выполнено условие выше, не превосходит $q_2/(q-1)$. Таким образом, с вероятностью не больше $q_2/(q-1)$ среди точек Z'_i, $1 \leqslant i \leqslant \ell+1$, в составе всех подделок есть хотя бы одна точка, не равная dM'_i.

Далее рассмотрим только те эксперименты, в которых нарушитель возвращает подделки, для каждой из которых верно, что $Z'_i = dM'_i$, $1 \leqslant i \leqslant \ell + 1$.

Таким образом, мы перешли от исходного эксперимента $\mathbf{Exp}(\mathcal{A}) = \mathbf{Exp}^{\mathrm{wUF}}_{\mathsf{CP\text{-}BS}}(\mathcal{A})$ к модифицированному эксперименту $\mathbf{Exp}'$, работающему так же, как исходный эксперимент, за исключением наступления определённых событий (см. шаги 2–3). Разницу преимуществ нарушителя в исходном и модифицированном экспериментах можно оценить как

$$\Pr[\mathbf{Exp}(\mathcal{A}) \Rightarrow 1] - \Pr[\mathbf{Exp}'(\mathcal{A}) \Rightarrow 1] \leqslant \frac{\ell + 1 + q_2}{q - 1}.$$

Будем строить двух нарушителей: нарушителя $\mathcal{B}$ для задачи SOMDL и нарушителя $\mathcal{C}$ для задачи REPR, использующих нарушителя $\mathcal{A}$ в качестве чёрного ящика. Покажем, что если нарушитель $\mathcal{A}$ успешно решает свою задачу, т. е. строит $(\ell + 1)$ подделку в результате ℓ успешных взаимодействий с подписывающим, то хотя бы один из нарушителей $\mathcal{B}$ или $\mathcal{C}$ успешно решает свою задачу.

Построение нарушителя $\mathcal{B}$. Пусть у нарушителя $\mathcal{B}$ на входе есть точки $A_1, \ldots, A_t, Q$. Нарушитель $\mathcal{B}$ заводит два множества Π_1, Π_2, изначально полагая их пустыми, запускает нарушителя $\mathcal{A}$, подавая ему на вход точку Q, и моделирует ответы на запросы к случайным оракулам, используя так называемую технику «lazy sampling», следующим образом:

$\mathrm{SimRO}_1(m)$	$\mathrm{SimRO}_2(str)$
1 : **if** $m \in \Pi_1$:	1 : **if** $str \in \Pi_2$:
2 : **return** $\Pi_1(m)P$	2 : **return** $\Pi_2(str)$
3 : $x \xleftarrow{\mathcal{U}} \mathbb{Z}_q^*$	3 : $c \xleftarrow{\mathcal{U}} \mathbb{Z}_q^*$
4 : $\Pi_1 \leftarrow \Pi_1 \cup \{m, x\}$	4 : $\Pi_2 \leftarrow \Pi_2 \cup \{str, c\}$
5 : **return** xP	5 : **return** c

Нарушитель $\mathcal{B}$ фиксирует переходы случайных функций адаптивно по мере запросов нарушителя $\mathcal{A}$ к соответствующим случайным оракулам, сохраняет в множество Π_2 все пары (запрос, ответ), соответствующие работе оракула RO_2, а в множество Π_1 — все запросы к оракулу RO_1 и дискретные логарифмы ответов, соответствующих данным запросам. Если запрос к определённой функции повторяется, то нарушитель $\mathcal{B}$ возвращает то же значение, что и в прошлый раз, используя значения, сохраненные в множествах Π_1, Π_2. Заметим, что по построению нарушитель $\mathcal{B}$ знает дискретные логарифмы точек M' относительно точки P.

Нарушитель $\mathcal{B}$ симулирует работу оракулов Sign_1 и Sign_2 следующим образом:

$\mathrm{SimSign}_1(M)$	$\mathrm{SimSign}_2(i, c)$
1 : // i-й запрос нарушителя $\mathcal{A}$	1 : $Y \leftarrow A_i + cQ$
2 : $A \leftarrow A_i$	2 : $s \leftarrow O_2(Y)$
3 : $B \leftarrow O_1(i, M)$	3 : **return** s
4 : $Z \leftarrow O_1(t + 1, M)$	
5 : **return** (A, B, Z)	

Пусть нарушитель $\mathcal{A}$ делает i-й запрос вида M к оракулу Sign_1. Тогда нарушитель $\mathcal{B}$ полагает точку A равной очередной точке $A_i = k_i P$, полученной на входе.

Для получения точки B нарушитель делает запрос (i, M) к оракулу O_1 и получает в ответ точку $k_i M$. Для получения точки Z нарушитель делает запрос $(t+1, M)$ к оракулу O_1 и получает в ответ точку dM. Тройку (A, B, Z) нарушитель возвращает в качестве ответа на запрос к оракулу Sign_1. В результате нарушитель $\mathcal{B}$ делает не более $2t$ запросов к собственному оракулу O_1.

Работу оракула Sign_2 нарушитель $\mathcal{B}$ симулирует следующим образом: получив запрос (i, c), формирует точку $Y = A_i + cQ$, делает запрос Y своему оракулу O_2 и возвращает полученный ответ $\mathrm{DLog}_P(A_i + cQ) = k_i + cd$ нарушителю $\mathcal{A}$.

В результате своей работы нарушитель $\mathcal{A}$ возвращает $(\ell+1)$ пару (сообщение, подпись) $\big(m_i, (s'_i, c'_i, Z'_i)\big)$, $i = 1, \ldots, \ell+1$. В силу шага 2 для каждого значения подделки можно найти соответствующий запрос (M'_i, Z'_i, A'_i, B'_i) к оракулу RO_2. В рамках этого запроса нарушитель $\mathcal{A}$ был обязан подать разложение всех точек (см. шаг 1), в частности точки B'_i.

Тогда для каждой подделки нарушитель $\mathcal{B}$ может выписать соотношение

$$s'_i M'_i - c'_i Z'_i = B'_i = \alpha_i P + \beta_i Q + \sum_{j=1}^{t} \gamma_{ij} A_j + \sum_{j=1}^{t} \sigma_{ij} B_j + \sum_{j=1}^{t} \eta_{ij} Z_j + \sum_{j=1}^{q_1} \xi_{ij} M'_j, \qquad (1)$$

где $i \in \{1, \ldots, \ell+1\}$. Таким образом, нарушитель $\mathcal{B}$ получит систему из $(\ell+1)$ уравнения.

Левое представление точки B'_i справедливо в силу того, что подпись является корректной; правое — это представление, поданное нарушителем $\mathcal{A}$ при запросе к RO_2.

Заметим, что для всех завершённых сеансов нарушитель $\mathcal{B}$ может представить точки A_j и B_j как $(s_j P - c_j Q)$ и $(s_j M_j - c_j Z_j)$ соответственно. Для всех незавершённых сеансов нарушитель $\mathcal{B}$ не делал запрос к оракулу O_2 (так как нарушитель $\mathcal{A}$ не делал запрос к Sign_2), а потому не знает представление k_j через линейную комбинацию $(s_j - c_j d)$. Пусть для всех незавершённых сеансов с некоторым номером j нарушитель $\mathcal{B}$ после окончания работы нарушителя $\mathcal{A}$ подаёт запросы вида A_j к своему оракулу O_2. Тогда он получает в ответ соответствующие значения k_j и может в явном виде представить все точки A_j и B_j из незавершённых сеансов как $k_j P$ и $k_j M_j$ соответственно. В результате количество запросов нарушителя $\mathcal{B}$ к оракулу O_2 равно t.

Заметим также, что все значения Z_j в разложении (1) можно представить как dM_j, а точка Z'_i, согласно шагу 3 и порядку симулирования оракула RO_1, равна $dM'_i = dx_i P$.

Будем обозначать через $\mathsf{З} \subseteq \{1, \ldots, t\}$ множество номеров завершённых сеансов, $\mathsf{НЗ} \subseteq \{1, \ldots, t\}$ — незавершённых. Рассмотрим уравнение (1) относительно неизвестного d:

$$\begin{gathered} s'_i x_i P - c'_i d x_i P = B'_i = \\ = \alpha_i P + \beta_i dP + \sum_{j \in \mathsf{З}} \gamma_{ij} (s_j P - c_j dP) + \sum_{j \in \mathsf{НЗ}} \gamma_{ij} k_j P + \\ + \sum_{j \in \mathsf{З}} \sigma_{ij} (s_j M_j - c_j dM_j) + \sum_{j \in \mathsf{НЗ}} \sigma_{ij} k_j M_j + \sum_{j=1}^{t} \eta_{ij} dM_j + \sum_{j=1}^{q_1} \xi_{ij} x_j P. \end{gathered} \qquad (2)$$

Покажем, что в этом разложении можно переформировать коэффициенты таким образом, чтобы избавиться от сумм вида $\sum\limits_{j \in \mathsf{НЗ}}$.

Прибавим к α_i значение $\sum\limits_{j \in \mathsf{НЗ}} \gamma_{ij} k_j$, известное нарушителю $\mathcal{B}$. Обозначим результирующий коэффициент через α_i^*, избавившись тем самым от суммы $\sum\limits_{j \in \mathsf{НЗ}} \gamma_{ij} k_j P$. Заметим, что коэффициент α_i^* фиксируется в момент подачи запроса оракулу RO_2 нарушителем $\mathcal{A}$, так как коэффициенты α_i, γ_{ij} подаются в составе этого запроса, а значения k_j,

соответствующие $\gamma_{ij} \neq 0$, уже были выбраны экспериментатором нарушителя $\mathcal{B}$. Действительно, $\mathcal{A}$ подаёт разложение только по тем точкам, которые возвращались ему в результате эксперимента, а значит, он уже делал запросы Sign_1 в j-х сеансах.

Рассмотрим точки M_j, соответствующие незавершённым сеансам. Точка M_j из первого незавершённого сеанса, очевидно, не зависит от других точек из незавершённых сеансов, а потому может быть представлена как линейная комбинация точек только из завершённых сеансов. Второй незавершённый сеанс (пусть его номер равен j') может зависеть от точек из завершённых сеансов, а также от значений A_j, B_j, Z_j первого незавершённого сеанса с номером j. В этом случае можно представить точки A_j, B_j, Z_j как k_jP, k_jM_j и dM_j, где M_j зависит только от точек из завершённых сеансов. Таким образом, перегруппировав коэффициенты, получим представление точки $M_{j'}$ через точки, соответствующие завершённым сеансам. Далее аналогично можно представить все точки A_j, B_j из незавершённых сеансов как линейные комбинации точек из завершённых сеансов.

Можно переписать систему уравнений (2) как

$$\begin{gathered} s'_i x_i P - c'_i d x_i P = \alpha'_i P + \beta'_i dP + \sum_{j \in \mathsf{З}} \gamma'_{ij}(s_j P - c_j dP) + \\ + \sum_{j \in \mathsf{З}} \sigma'_{ij}(s_j M_j - c_j dM_j) + \sum_{j=1}^{t} \eta'_{ij} dM_j + \sum_{j=1}^{q_1} \xi'_{ij} x_j P. \end{gathered} \tag{3}$$

Аналогично значения всех коэффициентов $\alpha'_i, \beta'_i, \gamma'_{ij}, \sigma'_{ij}, \eta'_{ij}, \xi'_{ij}$ фиксируются в момент подачи запроса оракулу RO_2 нарушителем $\mathcal{A}$.

Каждая точка M_j также имеет некоторое представление, нарушитель $\mathcal{A}$ подаёт его при запросе к оракулу Sign_1. При этом точки M_j можно представить в виде

$$M_j = \sum_{t=0}^{j} \tilde{l}_{j,t} d^t P,$$

где $\tilde{l}_{j,t}$ — аффинная функция от значений $x_1, \ldots, x_{q_1}$. Действительно, точка M_1 является разложением только по точкам $P, Q = dP$, $M'_i = x_i P$, $1 \leqslant i \leqslant q_1$, т. е. разложение содержит только первую степень d. Следующая точка M_2 может содержать в разложении точку $Z_1 = dM_1$, а потому степень d в разложении может увеличиться на единицу. Далее аналогично точка M_j содержит в разложении не более j-й степени d. В силу того, что в результате запроса к Sign_1 ни одна из точек не умножается на значения x_i, эти значения никогда не умножаются друг на друга и могут входить в разложения только в первой степени через замешивание точек M'_i. Таким образом, каждый коэффициент перед $d^t P$ можно представить как аффинную функцию от значений $x_1, \ldots, x_{q_1}$.

Получить такое представление точки M_j можно за полиномиальное время. В ходе эксперимента нарушитель сам подаёт разложения точек M_j, а в результате запроса к оракулу Sign_1 через это разложение однозначно определяется разложение точек B_j, Z_j за счёт домножения всех коэффициентов на k_j и d соответственно и представления точек $M_{j'}$ из предыдущих запросов. Таким образом, нарушитель на каждом шаге контролирует разложения всех точек.

Тогда, прологарифмировав по основанию P, можно записать систему уравнений (3) следующим образом:

$$\begin{gathered} s'_i x_i - c'_i d x_i = \alpha'_i + \beta'_i d + \sum_{j \in \mathsf{З}} \gamma'_{ij}(s_j - c_j d) + \\ + \sum_{j \in \mathsf{З}} \sigma'_{ij}(s_j - c_j d) \sum_{t=0}^{j} \tilde{l}_{j,t} d^t + \sum_{j=1}^{t} \eta'_{ij} d \sum_{t=0}^{j} \tilde{l}_{j,t} d^t + \sum_{j=1}^{q_1} \xi'_{ij} x_j. \end{gathered} \tag{4}$$

Для нарушителя $\mathcal{B}$ единственным неизвестным в этой системе является значение d. Каждое уравнение представляет собой полином от d степени не больше $\ell+1$. При этом в силу того, что подписи корректные и нарушитель предоставляет корректное разложение точек, корень d обязательно существует. Если хотя бы одно из уравнений системы существенно зависит от d, то нарушитель $\mathcal{B}$ может найти значение d с помощью вероятностного алгоритма факторизации полиномов, описанного в [28, алгоритм 4]. Положим количество итераций данного алгоритма равным $2(\log \ell+1)$. Тогда трудоёмкость поиска всех корней полинома составляет $O(\ell)$ операций. Событие, что алгоритм успешно решает задачу, обозначим через factor, вероятность успешного запуска алгоритма составляет $\Pr[\mathsf{factor}] \geqslant 1/2$. Нарушитель $\mathcal{B}$, найдя все корни системы (4), может найти правильное значение ключа d перебором по всем корням d_i, $1 \leqslant i \leqslant \ell$, и сравнением d_iP с открытым ключом Q, трудоёмкость этого шага составляет $O(\ell)$ операций. Трудоёмкость поиска ключа d, таким образом, не превосходит $T_{\mathcal{A}}$. Если нарушитель $\mathcal{B}$ успешно восстанавливает значение d, то он успешно решает задачу SOMDL, так как может восстановить все остальные значения k_j из линейных комбинаций, полученных им от оракула O_2.

Единственным случаем, при котором нарушитель $\mathcal{B}$ не может найти корень d, является случай, когда система (4) является тривиальной относительно d, т. е. если во всех уравнениях коэффициент перед всеми степенями d равен 0. В частности, в этом случае свободный член (коэффициент перед нулевой степенью d) во всех уравнениях равен 0. Выпишем это условие:

$$s'_i x_i = \alpha'_i + \sum_{j\in\mathfrak{Z}} \gamma'_{ij} s_j + \sum_{j\in\mathfrak{Z}} \sigma'_{ij} s_j \tilde{l}_{j,0} + \sum_{j=1}^{q_1} \xi'_{ij} x_j, \quad i = 1, \ldots, \ell+1. \tag{5}$$

Обозначим через event событие, когда не выполнено условие (5). Тогда

$$\mathsf{Adv}^{\mathrm{SOMDL}}_{\mathbb{G},2t,t}(\mathcal{B}) = \Pr\bigl[\mathbf{Exp}^{\mathrm{SOMDL}}_{\mathbb{G},2t,t}(\mathcal{B}) \to 1\bigr] = \Pr[(\mathbf{Exp}'(\mathcal{A}) \to 1) \wedge \mathsf{event} \wedge \mathsf{factor}] =$$
$$= \Pr[(\mathbf{Exp}'(\mathcal{A}) \to 1) \wedge \mathsf{event}] \Pr[\mathsf{factor}] \geqslant \frac{1}{2} \cdot \Pr[(\mathbf{Exp}'(\mathcal{A}) \to 1) \wedge \mathsf{event}].$$

Далее покажем, что если событие event не произошло, т. е. условие (5) выполнено, то нарушитель $\mathcal{C}$ с большой вероятностью успешно решает задачу OMDL.

Построение нарушителя $\mathcal{C}$. Сначала построим нарушителя $\mathcal{C}$, решающего задачу REPR. Пусть нарушитель $\mathcal{C}$ получает на вход точки $x_1P, \ldots, x_{q_1}P$, где значения x_i выбраны случайно равновероятно из $\mathbb{Z}_q^*$.

Нарушитель $\mathcal{C}$ самостоятельно генерирует ключ подписи d и значения k_i, поэтому моделирует работу оракулов Sign_1 и Sign_2 точно так же, как экспериментатор нарушителя $\mathcal{A}$. Работу оракула RO_2 нарушитель $\mathcal{C}$ симулирует так же, как и нарушитель $\mathcal{B}$. Работу оракула RO_1 противник $\mathcal{C}$ симулирует, отдавая на каждый новый запрос m очередную точку x_iP, полученную нарушителем $\mathcal{C}$ на вход от своего собственного экспериментатора.

Нарушитель $\mathcal{C}$ так же, как и нарушитель $\mathcal{B}$, может составить систему уравнений (1), получив $(\ell+1)$ подделку от нарушителя $\mathcal{A}$. Заметим, что для нарушителя $\mathcal{C}$ неизвестными в этом уравнении будут являться только величины x_i. Значения d и k_i ему известны, поскольку он генерирует их самостоятельно. Нарушитель $\mathcal{C}$ может преобразовать это уравнение точно так же, как и нарушитель $\mathcal{B}$, выразив k_j от завершённых сеансов через d и подставив известные ему k_j для незавершённых сеансов.

Покажем, что если выполнено условие (5), то нарушитель $\mathcal{C}$ с большой вероятностью успешно решает задачу REPR, т. е. находит нетривиальную линейную комбинацию значений $x_1, \ldots, x_{q_1}$.

Пусть есть $(\ell + 1)$ уравнение относительно переменных $x_1, \ldots, x_{q_1}$. Если хотя бы в одном из этих уравнений перед некоторым x_i стоит ненулевой коэффициент, то это уравнение задаёт нетривиальную линейную комбинацию. Таким образом, «плохим» случаем является следующий: коэффициенты перед всеми x_i во всех уравнениях равны нулю.

Прежде чем выписать это условие, сделаем два технических преобразования:

1) Перенумеруем подделки таким образом, чтобы они были упорядочены по порядку соответствующих им запросов к случайному оракулу RO_2. В силу шага 2 для каждой подделки можно найти запрос к RO_2. Тогда получим, что запрос для i-й подделки выполнен раньше, чем запрос для $(i+1)$-й подделки, $1 \leqslant i \leqslant \ell$. Технически это преобразование означает, что мы поменяли местами уравнения в системе (4). Очевидно, что подобное изменение не влияет на решение системы и может быть сделано за полиномиальное время.
2) Переобозначим переменные $x_1, \ldots, x_{q_1}$ таким образом, чтобы сообщению m_i в составе i-й подделки (номер подделки в результате преобразования 1) соответствовала переменная x_i, т. е. чтобы было выполнено $\mathcal{H}(m_i) = x_i P$. Если переменная x_i не соответствует ни одной подделке, то её индекс может быть произвольным. Очевидно, что подобное изменение также не влияет на решение системы и может быть сделано за полиномиальное время.

В результате этих преобразований получаем систему уравнений (4), уравнения в которой упорядочены по порядку запросов к RO_2, а переменные x_i — по вхождению в набор подделок. Напомним условие (5), при котором нарушитель $\mathcal{B}$ не может успешно решить свою задачу:

$$\left\{ s'_i x_i = \alpha'_i + \sum_{j=1}^{l} \gamma'_{ij} s_j + \sum_{j=1}^{l} \sigma'_{ij} s_j \tilde{l}_{j,0}(x_1, \ldots, x_{q_1}) + \sum_{j=1}^{q_1} \xi'_{ij} x_j, \quad 1 \leqslant i \leqslant \ell + 1. \right.$$

Выпишем в матричном виде условие, означающее, что во всех уравнениях этой системы коэффициенты перед всеми x_j равны нулю, т. е. условие, при котором нарушитель $\mathcal{C}$ не может успешно решить свою задачу:

$$\ell + 1 \left\{ \overbrace{\begin{pmatrix} s'_1 & 0 & 0 & \ldots & 0 & 0 & \ldots & 0 \\ 0 & s'_2 & 0 & \ldots & 0 & 0 & \ldots & 0 \\ 0 & 0 & s'_3 & \ldots & 0 & 0 & \ldots & 0 \\ & & & \ddots & & & & \\ 0 & 0 & 0 & \ldots & s'_{\ell+1} & 0 & \ldots & 0 \end{pmatrix}}^{q_1} \right. = \tag{6}$$

$$= \underbrace{\begin{pmatrix} \ddots & & \\ & \sigma'_{ij} s_j & \\ & & \ddots \end{pmatrix}}_{\ell} \cdot \underbrace{\begin{pmatrix} \ddots & & \\ & \tilde{l}_{j,0} & \\ & & \ddots \end{pmatrix}}_{q_1} + \underbrace{\begin{pmatrix} \ddots & & \\ & \xi'_{ij} & \\ & & \ddots \end{pmatrix}}_{q_1}$$

Заметим, что коэффициенты ξ'_{ij}, составляющие матрицу справа, фиксируются при подаче запросов к случайному оракулу RO_2. Они определяются коэффициентами раз-

ложения точки B'_i на входе случайного оракула и коэффициентами разложений точек M_j, которые на текущий момент уже были отправлены оракулу Sign_1, при этом значения ξ'_{ij} фиксируются в момент подачи нарушителем $\mathcal{A}$ соответствующего запроса к оракулу RO_2. Тогда при подаче первого запроса к RO_2 фиксируется первая строка матрицы $\left(\xi'_{ij}\right)$, при подаче второго запроса — вторая и так далее.

Если сделан запрос $(M' \parallel Z' \parallel A' \parallel B')$ к оракулу RO_2, то зафиксировано в том числе значение $k' = \mathrm{DLog}_{M'}B'$, значение d также фиксировано. В результате подачи запроса выбирается некоторое случайное c'. Поскольку подпись (s', c', Z) является корректной, должно быть верно условие $B' = s'M' - c'Z'$, откуда следует $s' = k' + c'd$. Тогда, поскольку значения k' и d фиксированные, а c' выбирается случайно равновероятно из множества мощности $(q-1)$, можно считать, что значение s' также выбирается случайно равновероятно из множества мощности $(q-1)$. Значит, можно считать, что элементы матрицы, стоящей слева в уравнении (6), выбираются случайно равновероятно после фиксации определённым образом матрицы справа, состоящей из значений ξ'_{ij}.

Перепишем матричное уравнение (6) следующим образом:

$$\ell+1\left\{\overbrace{\begin{pmatrix} s'_1-\xi'_{11} & \cdot & \cdot & \dots & \cdot & \dots \\ \cdot & s'_2-\xi'_{22} & \cdot & \dots & \cdot & \dots \\ \cdot & \cdot & s'_3-\xi'_{33} & \dots & \cdot & \dots \\ & & & \ddots & & \\ \cdot & \cdot & \cdot & \dots & s'_{\ell+1}-\xi'_{(\ell+1)(\ell+1)} & \dots \end{pmatrix}}^{q_1}\right. =$$

$$= \underbrace{\begin{pmatrix} \ddots & & \\ & \sigma'_{ij}s_j & \\ & & \ddots \end{pmatrix}}_{\ell} \cdot \underbrace{\begin{pmatrix} \ddots & & \\ & \tilde{l}_{j,0} & \\ & & \ddots \end{pmatrix}}_{q_1}$$

Справа в этом уравнении стоит произведение двух матриц, ранг каждой из которых не превосходит ℓ (их размер $(\ell+1)\times\ell$ и $\ell\times q_1$ соответственно). Тогда ранг произведения также не превосходит ℓ.

Оценим, с какой вероятностью ранг матрицы слева будет отличен от $(\ell+1)$. Для этого будем рассматривать квадратную подматрицу размера $(\ell+1)\times(\ell+1)$, взяв левые $(\ell+1)$ столбцов исходной матрицы. Можно считать, что элементы, стоящие на главной диагонали этой подматрицы, выбираются случайно равновероятно из множества мощности $(q-1)$ (так как s' выбираются случайно). Подматрица, согласно рассуждениям выше, формируется следующим образом: фиксируется определённым произвольным образом первая строка, кроме элемента, стоящего на главной диагонали, после чего случайно выбирается этот элемент. Далее фиксируется вторая строка и случайно выбирается элемент, стоящий на главной диагонали, и так далее.

Ранг квадратной матрицы размера $m\times m$ отличен от m тогда и только тогда, когда её определитель равен нулю. Будем обозначать квадратную подматрицу размера t, стоящую в левом верхнем углу, через A_t. Искомую вероятность можно оценить как

$$\Pr[\det(A_{\ell+1})=0] = \Pr[\det(A_{\ell+1})=0 \wedge \det(A_\ell)=0] + \Pr[\det(A_{\ell+1})=0 \wedge \det(A_\ell)\neq 0] \leqslant$$
$$\leqslant \Pr[\det(A_\ell)=0] + \Pr[\det(A_{\ell+1})=0 \mid \det(A_\ell)\neq 0] \leqslant$$
$$\leqslant \ldots \leqslant \Pr[\det(A_1)=0] + \sum_{i=1}^{\ell} \Pr[\det(A_{i+1})=0 \mid \det(A_i)\neq 0].$$

Матрица A_1 состоит только из элемента $s'_1 - \xi'_{11}$, который выбирается случайно. Определитель будет равен нулю, если этот элемент равен нулю, вероятность такого события равна $(q-1)^{-1}$, т. е. $\Pr[\det(A_1) = 0] = (q-1)^{-1}$. Далее — индукция по размеру t матрицы A_t.

Пусть $\det(A_i) = d_i \neq 0$. Оценим $\Pr[\det(A_{i+1}) = 0 \mid \det(A_i) \neq 0]$. Матрица A_{i+1} получается из матрицы A_i приписыванием справа и снизу ещё одного столбца и ещё одной строки, при этом сначала произвольным образом фиксируются все элементы, кроме элемента с номером $(i+1, i+1)$, после чего он выбирается случайно равновероятно. Разложим $\det(A_{i+1})$ по последней строке, тогда $\det(A_{i+1})$ равен сумме $(s'_{i+1,i+1} - \xi'_{i+1,i+1}) \det(A_i)$ и некоторых фиксированных значений. Таким образом, $\det(A_{i+1}) = 0$ только в том случае, когда $s'_{i+1,i+1}$ принимает фиксированное значение, т. е. с вероятностью $(q-1)^{-1}$. Получаем, что

$$\Pr[\det(A_{i+1}) = 0 \mid \det(A_i) \neq 0] = (q-1)^{-1},$$

откуда следует

$$\Pr[\det(A_{\ell+1}) = 0] \leqslant \frac{\ell+1}{q-1}.$$

Итак, в (6) слева с вероятностью больше либо равной $\big(1 - (\ell+1)/(q-1)\big)$ стоит матрица ранга $(\ell+1)$, справа — матрица ранга не больше ℓ. Это означает, что условие (6) с большой вероятностью не выполнено, а значит, среди уравнений системы (5) есть нетривиальная линейная комбинация переменных x_i.

Замечание 2. Если нарушитель $\mathcal{A}$ в составе подделок выдаёт сообщения, для которых он не делал запросы к оракулу RO_1, то в системе (5) слева будут одни значения x_i (от подделок), а справа — другие (от разложений). Тогда в этой системе точно есть нетривиальные комбинации x_i от подделок, так как s'_i ненулевые. В общем случае нарушитель $\mathcal{C}$ принимает на вход и использует для формирования ответов случайного оракула $(q_1 + \ell + 1)$ точек, т. е. параметр s в задаче REPR равен $q_1 + \ell + 1$.

Обозначим через eqrank событие, что $\det(A_{\ell+1}) = 0$. Если условие (5) выполнено (т. е. произошло событие $\overline{\mathsf{event}}$) и событие eqrank не произошло, то нарушитель $\mathcal{C}$ успешно решает свою задачу. Тогда

$$\Pr[\mathbf{Exp}'(\mathcal{A}) \to 1 \wedge \overline{\mathsf{event}}] =$$
$$= \underbrace{\Pr\big[\mathbf{Exp}'(\mathcal{A}) \to 1 \wedge \overline{\mathsf{event}} \wedge \overline{\mathsf{eqrank}}\big]}_{=\Pr\left[\mathbf{Exp}^{\mathrm{REPR}}_{\mathbb{G},q_1+\ell+1}(\mathcal{C})\right]} + \underbrace{\Pr[\mathbf{Exp}'(\mathcal{A}) \to 1 \wedge \overline{\mathsf{event}} \wedge \mathsf{eqrank}]}_{\leqslant \Pr[\mathsf{eqrank}]} \leqslant$$
$$\leqslant \Pr\left[\mathbf{Exp}^{\mathrm{REPR}}_{\mathbb{G},q_1+\ell+1}(\mathcal{C}) \to 1\right] + \Pr[\mathsf{eqrank}] \leqslant \mathsf{Adv}^{\mathrm{REPR}}_{\mathbb{G},q_1+\ell+1}(\mathcal{C}) + \frac{\ell+1}{q-1}.$$

Итоговая оценка

Таким образом, мы построили двух нарушителей $\mathcal{B}$ и $\mathcal{C}$, хотя бы один из которых с большой вероятностью решает свою задачу, если нарушитель $\mathcal{A}$ успешно строит подделки. В итоге получаем

$$\Pr[\mathbf{Exp}'(\mathcal{A}) \to 1] = \Pr[\mathbf{Exp}'(\mathcal{A}) \to 1 \wedge \mathsf{event}] + \Pr[\mathbf{Exp}'(\mathcal{A}) \to 1 \wedge \overline{\mathsf{event}}] \leqslant$$
$$\leqslant 2\,\mathsf{Adv}^{\mathrm{SOMDL}}_{\mathbb{G},t,2t}(\mathcal{B}) + \mathsf{Adv}^{\mathrm{REPR}}_{\mathbb{G},q_1+\ell+1}(\mathcal{C}) + \frac{\ell+1}{q-1},$$
$$\mathsf{Adv}^{\mathrm{wUF}}_{\mathsf{CP\text{-}BS}}(\mathcal{A}) \leqslant 2\,\mathsf{Adv}^{\mathrm{SOMDL}}_{\mathbb{G},t,2t}(\mathcal{B}) + \mathsf{Adv}^{\mathrm{REPR}}_{\mathbb{G},q_1+\ell+1}(\mathcal{C}) + \frac{2(\ell+1)+q_2}{q-1}.$$

УДК 519.218+004.056.5 DOI 10.17223/20710410/65/4

О ВЛИЯНИИ ВЕРОЯТНОСТНЫХ ХАРАКТЕРИСТИК ДИСКРЕТНЫХ ИСТОЧНИКОВ, ФОРМИРУЮЩИХ КРИПТОГРАФИЧЕСКИЕ КЛЮЧИ, НА ПРАКТИЧЕСКУЮ СЕКРЕТНОСТЬ КЛЮЧА

А. С. Логачев*, В. О. Миронкин**

*Лаборатория ТВП, г. Москва, Россия

**МИРЭА — Российский технологический университет, г. Москва, Россия

E-mail: mironkin.v@mail.ru

Предложена математическая модель двоичного дискретного источника, приближенная к практическим условиям функционирования устройств генерации криптографических ключей. Модель допускает нестационарность таких устройств, а также наличие статистических зависимостей между их выходными битами. В рамках модели получена достижимая и легко вычислимая оценка снизу практической секретности ключа. Показано, что при определённых параметрах модели оценка позволяет делать содержательные выводы о криптографическом качестве ключей, в то время как другие известные оценки не справляются с этим.

Ключевые слова: *практическая секретность ключа, алгоритм опробования до успеха, усечённый алгоритм опробования.*

ON THE INFLUENCE OF PROBABILISTIC CHARACTERISTICS OF DISCRETE SOURCES FORMING CRYPTOGRAPHIC KEYS ON THE PRACTICAL SECRECY OF THE KEY

A. S. Logachev*, V. O. Mironkin**

*TVP Laboratory, Moscow, Russia

**MIREA — Russian Technological University, Moscow, Russia

The mathematical model of a binary discrete source is proposed, which is close to the practical conditions for the operation of cryptographic key generation devices. The model takes into account the non-stationarity of such devices, as well as the presence of statistical dependencies between their output bits. Within the framework of the model, an achievable and easily computable lower estimate of the practical secrecy of the key is obtained. It is shown that with certain parameters of the model, the assessment allows us to draw meaningful conclusions about the cryptographic quality of keys, while other well-known estimates do not cope with this.

Keywords: *the practical secrecy of the key, algorithm of testing to success, truncated algorithm of testing.*

Введение

В соответствии с принципом Керкгоффса [1, 2] защищённость информационных систем держится на секретности используемых в них криптографических ключей. Поэтому совершенно не удивительно, что оценка практической секретности ключа

является не только неотъемлемой составляющей анализа широкого класса алгоритмических методов защиты информации (далее — АМЗИ), в том числе имеющих квантовую природу [3], но и синтеза ряда аппаратно-программных средств, используемых для генерации случайных последовательностей [4], на основе которых формируются ключи шифрования, ключи электронной подписи, пароли, пин-коды и т. д.

Криптографический смысл практической секретности ключа, а также результаты её теоретико-вероятностного исследования достаточно полно изложены в работах [5, 6]. Публикацию И. М. Арбекова [5], без сомнения, можно считать основополагающей работой по анализу практической секретности ключа, положившей начало дальнейшим исследованиям в этой области [3, 6].

Напомним, что в соответствии с [5] для произвольных фиксированных $n \in \mathbb{N}$ и π, $0 < \pi \leqslant 1$, практическая секретность ключа $Q_n^{(\pi)}$ равна минимальному среди средних значений трудоёмкостей $R_{A_n(\tilde{\pi})}$ всех возможных усечённых алгоритмов $A_n(\tilde{\pi})$ опробования ключа из $\{0,1\}^n$ с вероятностями успеха $\tilde{\pi}$, $\tilde{\pi} \geqslant \pi$:

$$Q_n^{(\pi)} = \min_{A(\tilde{\pi})\colon\, \tilde{\pi} \geqslant \pi} \left(R_{A_n(\tilde{\pi})}\right).$$

В работе [6] указанная величина изучается в рамках математической модели, в которой ключ представляет собой реализацию дискретного источника без памяти (далее — ДИБП) [7], функционирующего в соответствии с некоторой полиномиальной схемой:

$$\mathcal{A} \sim \begin{pmatrix} \omega_1 & \omega_2 & \dots & \omega_{2^n} \\ p_1 & p_2 & \dots & p_{2^n} \end{pmatrix}, \tag{1}$$

где $\omega_i \in \{0,1\}^n$, $n \in \mathbb{N}$, $i = 1, 2, \dots, 2^n$, а компоненты вектора распределения $\overline{p} = (p_1, p_2, \dots, p_{2^n})$ удовлетворяют соотношениям

$$p_1 + p_2 + \ldots + p_{2^n} = 1 \quad \text{и} \quad 1 > p_1 \geqslant p_2 \geqslant \ldots \geqslant p_{2^n} > 0. \tag{2}$$

Для этой модели автором [6] получена следующая оценка снизу практической секретности ключа:

$$Q_n^{(\pi)}(\delta) \geqslant \left(1 - \frac{2\delta}{\pi}\right) \frac{2^n\,(1 - 8\delta) + 1}{2}, \tag{3}$$

где $\delta = \dfrac{1}{2} \displaystyle\sum_{j=1}^{2^n} |p_j - 2^{-n}|$ — расстояние по вариации между распределениями $(p_1, p_2, \dots, p_{2^n})$ и $(2^{-n}, 2^{-n}, \dots, 2^{-n})$.

Замечание 1. Оценка (3) получена для алгоритма оптимального опробования ключей, заключающегося в переборе элементов ключевого множества в порядке невозрастания их вероятностей (2), начиная с наиболее вероятного. При произвольном фиксированном распределении (1) такой алгоритм, очевидно, минимизирует среднюю трудоёмкость опробования.

Отметим один из недостатков оценки (3) — для её вычисления необходимо суммирование 2^n достаточно малых слагаемых, что требует существенных вычислительных мощностей, а также высокой точности расчётов. Кроме того, в соответствии с [6] оценка (3) является содержательной лишь при справедливости неравенства

$$\delta < \min\left(1/8, \pi/2\right). \tag{4}$$

Формула (3) активно используется на практике. В частности, в классических условиях анализа АМЗИ [6, с. 32], когда элементы ключевого множества имеют равновероятное распределение

$$p_1 = p_2 = \ldots = p_{2^n} = 2^{-n} \tag{5}$$

и, как следствие, $\delta = 0$, выполняется известное равенство [5, с. 46]

$$Q_n^{(1)}(0) = (2^n + 1)/2.$$

Таким образом, в «рафинированных» условиях, соответствующих (5), оценка (3) практической секретности ключа является достижимой и её использование в связи с этим не вызывает никаких сомнений. Вместе с тем при синтезе АМЗИ могут возникать достаточно естественные вопросы: возможно ли на практике обеспечить выполнение модельных предположений вида (1), характерных лишь для стационарных источников [7]? И если их нельзя обеспечить, то что использовать в качестве аналога оценки (3)? Или никакие аналоги не требуются и её использование является допустимым?

Отвечая на первый вопрос, к сожалению, мы получим отрицательный ответ. Действительно, в общем случае учесть влияние всех возможных внешних факторов на процесс формирования криптографических ключей некоторым, вообще говоря, физическим источником достаточно проблематично. Кроме того, сама элементная база реального источника подвержена естественной деградации, влияющей на вероятностные свойства и характеристики формируемых последовательностей.

В таком случае становятся актуальными пока ещё открытые второй и третий вопросы, которые мы рассмотрим в рамках настоящей работы, попутно предлагая некоторые способы построения оценки снизу практической секретности ключа в более общих модельных предположениях, характерных для практики.

Исследование будем проводить в три этапа. На первом этапе построим оценку снизу для средней трудоёмкости алгоритма опробования ключа до успеха, на втором этапе — оценку снизу для средней трудоёмкости процедуры опробования ключа на основе усечённых алгоритмов с некоторыми фиксированными вероятностями успеха и, наконец, на третьем — искомую оценку для практической секретности ключа.

Для решения указанных задач построим теоретико-вероятностную модель источника формирования криптографических ключей.

1. Модель источника формирования криптографических ключей

Рассмотрим невырожденный двоичный дискретный источник — вероятностное пространство $(\{0,1\}^\infty, \mathcal{F}, \Pr)$, где $\mathcal{F}$ — наименьшая по включению σ-алгебра на $\{0,1\}^\infty$, содержащая все цилиндрические множества [7] общего вида, а вероятность $\Pr$ такова, что для её конечномерных распределений $P_{t_1,t_2,\ldots,t_k}$, $1 \leqslant t_1 < t_2 < \ldots < t_k$, $k = 1, 2, \ldots$, выполняется соотношение

$$\left(\frac{1}{2} - \varepsilon\right)^k \leqslant P_{t_1,t_2,\ldots,t_k}(x_1, x_2, \ldots, x_k) \leqslant \left(\frac{1}{2} + \varepsilon\right)^k \tag{6}$$

для произвольных $(x_1, x_2, \ldots, x_k) \in \{0,1\}^k$, где $0 \leqslant \varepsilon \leqslant 1/2$.

Здесь последовательность элементов $t_1, t_2, \ldots, t_k$ определяет моменты времени формирования источником $(\{0,1\}^\infty, \mathcal{F}, \Pr)$ значений $x_1, x_2, \ldots, x_k$, в нашем случае представляющих биты ключа.

Замечание 2. Ограничение вида (6) на вероятностные свойства источника является достаточно слабым по сравнению с (1), допускающим, в частности, его нестационарность или даже зависимость формируемых им битов ключа. Более того, при $\varepsilon \to 1/2$ это ограничение в принципе вырождается.

Подобная математическая модель источника использовалась в [8] при обосновании качества криптографических преобразований.

В частном случае, когда $\varepsilon = 0$, неравенство (6) принимает вид

$$2^{-k} \leqslant P_{t_1,t_2\ldots,t_k}(x_1, x_2, \ldots, x_k) \leqslant 2^{-k},$$

что при $k = n$ соответствует ДИБП с распределением (5).

Итак, мы построили модель дискретного источника формирования криптографических ключей. В рамках этой модели перейдём к оценке средней трудоёмкости алгоритма опробования ключа до успеха.

2. Оценка снизу средней трудоёмкости алгоритма опробования ключа до успеха

Согласно (6), для произвольного фиксированного ε, $0 \leqslant \varepsilon \leqslant 1/2$, уместно говорить о формировании ключей из $\{0,1\}^n$ в соответствии с полиномиальной схемой, зависящей от вектора $\bar{t} = (t_1, t_2, \ldots, t_n)$:

$$\mathcal{A}_\varepsilon(\bar{t}) \sim \begin{pmatrix} \omega_1 & \omega_2 & \ldots & \omega_{2^n} \\ p_1(\bar{t}) & p_2(\bar{t}) & \ldots & p_{2^n}(\bar{t}) \end{pmatrix}, \tag{7}$$

где $\omega_i \in \{0,1\}^n$, $i = 1, 2, \ldots, 2^n$, а компоненты вектора распределения $\overline{p}(\bar{t}) = \big(p_1(\bar{t}), p_2(\bar{t}), \ldots, p_{2^n}(\bar{t})\big)$ удовлетворяют системе соотношений

$$\begin{cases} p_1(\bar{t}) + p_2(\bar{t}) + \ldots + p_{2^n}(\bar{t}) = 1, \\ 1 > p_1(\bar{t}) \geqslant p_2(\bar{t}) \geqslant \ldots \geqslant p_{2^n}(\bar{t}) > 0, \\ (1/2 - \varepsilon)^n \leqslant p_j(\bar{t}) \leqslant (1/2 + \varepsilon)^n, \ j = 1, 2, \ldots, 2^n. \end{cases} \tag{8}$$

Общая теория [5] позволяет выписать формулу для средней трудоёмкости $\mathbf{E}T_{\mathcal{A}_\varepsilon(\bar{t})}$ алгоритма опробования ключа, сформированного источником в соответствии с вероятностной схемой $\mathcal{A}_\varepsilon(\bar{t})$, до успеха:

$$\mathbf{E}T_{\mathcal{A}_\varepsilon(\bar{t})} = \sum_{j=1}^{2^n} j p_j(\bar{t}). \tag{9}$$

Для произвольных $n \in \mathbb{N}$ и ε, $0 \leqslant \varepsilon \leqslant 1/2$, введём обозначение

$$T_n^{(1)}(\varepsilon) = \min_{\bar{t}} \left(\min_{p_1(\bar{t}),\ldots,p_{2^n}(\bar{t})} \big(\mathbf{E}T_{\mathcal{A}_\varepsilon(\bar{t})}\big) \right),$$

где $\bar{t} = (t_1, t_2, \ldots, t_n)$, $1 \leqslant t_1 < t_2 < \ldots < t_n$, а $\big(p_1(\bar{t}), p_2(\bar{t}), \ldots, p_{2^n}(\bar{t})\big)$ — векторы, удовлетворяющие (8).

Кроме того, через $[z]$ обозначим наибольшее целое число, меньшее или равное z. Тогда имеет место

Утверждение 1. Для произвольных $n \in \mathbb{N}$ и ε, $0 < \varepsilon < 1/2$, справедливо равенство

$$T_n^{(1)}(\varepsilon) = s + 1 + \frac{(2^n - s - 1)(2^n - s)}{2}\left(\frac{1}{2} - \varepsilon\right)^n - \frac{s(s+1)}{2}\left(\frac{1}{2} + \varepsilon\right)^n, \qquad (10)$$

где $s = \left[2^n \dfrac{1 - (1-2\varepsilon)^n}{(1+2\varepsilon)^n - (1-2\varepsilon)^n}\right]$. При этом для $\varepsilon \in \{0, 1/2\}$

$$T_n^{(1)}(0) = (2^n + 1)/2, \quad T_n^{(1)}(1/2) = 1. \qquad (11)$$

Доказательство. Равенства в (11) очевидны. Перейдём к обоснованию соотношения (10). Зафиксировав произвольные ε, $0 < \varepsilon < 1/2$, и $\bar{t} = (t_1, t_2, \ldots, t_n)$, $1 \leqslant t_1 < t_2 < \ldots < t_n$, построим вероятностную схему

$$\hat{\mathcal{A}}_\varepsilon(\bar{t}) \sim \begin{pmatrix} \omega_1 & \omega_2 & \ldots & \omega_{2^n} \\ \hat{p}_1(\bar{t}) & \hat{p}_2(\bar{t}) & \ldots & \hat{p}_{2^n}(\bar{t}) \end{pmatrix}, \qquad (12)$$

минимизирующую величину (9). Очевидно, что количество значений $\hat{\mathcal{A}}_\varepsilon(\bar{t})$, имеющих максимальную вероятность $(1/2 + \varepsilon)^n$, совпадает с наибольшим натуральным $s < 2^n$, удовлетворяющим неравенству

$$s\,(1/2 + \varepsilon)^n + (2^n - s)\,(1/2 - \varepsilon)^n \leqslant 1, \qquad (13)$$

т. е. с величиной

$$s = \left[\frac{1 - 2^n\,(1/2 - \varepsilon)^n}{(1/2 + \varepsilon)^n - (1/2 - \varepsilon)^n}\right] = \left[2^n \frac{1 - (1-2\varepsilon)^n}{(1+2\varepsilon)^n - (1-2\varepsilon)^n}\right].$$

Таким образом,

$$\hat{p}_1(\bar{t}) = \ldots = \hat{p}_s(\bar{t}) = (1/2 + \varepsilon)^n. \qquad (14)$$

В свою очередь, количество значений $\hat{\mathcal{A}}_\varepsilon(\bar{t})$, имеющих минимальную вероятность $(1/2 - \varepsilon)^n$, больше либо равно $2^n - s - 1$. При этом

$$\hat{p}_{s+2}(\bar{t}) = \ldots = \hat{p}_{2^n}(\bar{t}) = (1/2 - \varepsilon)^n. \qquad (15)$$

Наконец, с учётом (13)

$$\hat{p}_{s+1}(\bar{t}) = 1 - \sum_{j=1}^{s} \hat{p}_i(\bar{t}) - \sum_{j=s+2}^{2^n} \hat{p}_i = 1 - s\,(1/2 + \varepsilon)^n - (2^n - s - 1)\,(1/2 - \varepsilon)^n \geqslant 0. \qquad (16)$$

По построению все значения $\hat{p}_1(\bar{t}), \ldots, \hat{p}_{2^n}(\bar{t})$ удовлетворяют (8). Для $j = 1, \ldots, s$, $s + 2, \ldots, 2^n$ это очевидный факт. Остаётся убедиться в справедливости неравенства $(1/2 - \varepsilon)^n \leqslant \hat{p}_{s+1}(\bar{t}) \leqslant (1/2 + \varepsilon)^n$. Действительно, в соответствии с определением величины s выполняются следующие цепочки соотношений:

$$\begin{gathered} \hat{p}_{s+1}(\bar{t}) = 1 - s(1/2 + \varepsilon)^n - (2^n - s)\,(1/2 - \varepsilon)^n + (1/2 - \varepsilon)^n \geqslant \\ \geqslant 1 - 1 + (1/2 - \varepsilon)^n = (1/2 - \varepsilon)^n, \\ \hat{p}_{s+1}(\bar{t}) = 1 - (s+1)(1/2 + \varepsilon)^n - (2^n - s - 1)\,(1/2 - \varepsilon)^n + (1/2 + \varepsilon)^n < \\ < 1 - 1 + (1/2 + \varepsilon)^n = (1/2 + \varepsilon)^n. \end{gathered}$$

Итак, распределение вероятностной схемы (12), удовлетворяющее (14)–(16), минимизирует (9). Таким образом,

$$\min_{p_1(\bar{t}),\ldots,p_{2^n}(\bar{t})} \left(\mathbf{E}T_{\mathcal{A}_\varepsilon(\bar{t})}\right) = \mathbf{E}T_{\hat{\mathcal{A}}_\varepsilon(\bar{t})} = \sum_{j=1}^{2^n} j\hat{p}_j(\bar{t}) = \sum_{j=1}^{s} i\hat{p}_j(\bar{t}) + (s+1)\hat{p}_{s+1}(\bar{t}) + \sum_{j=s+2}^{2^n} j\hat{p}_j(\bar{t}) =$$

$$= \sum_{j=1}^{s} j(1/2+\varepsilon)^n + (s+1)(1 - s(1/2+\varepsilon)^n - (2^n - s - 1)(1/2-\varepsilon)^n) + \sum_{j=s+2}^{2^n} j(1/2-\varepsilon)^n =$$

$$= s + 1 + \frac{(2^n - s - 1)\,(2^n - s)}{2}\left(\frac{1}{2} - \varepsilon\right)^n - \frac{s(s+1)}{2}\left(\frac{1}{2} + \varepsilon\right)^n.$$

Полученное выражение не зависит от $\bar{t}$ и поэтому представляет собой искомый результат (10). ■

Для $0 < \varepsilon < 1/2$ оценка (10) является достижимой, имеет достаточно простой аналитический вид и эффективно вычислима при больших значениях $n \in \mathbb{N}$. В качестве примера приведём значения величин $Q_n^{(1)}(\delta)$ и $T_n^{(1)}(\varepsilon)$, рассчитанные с использованием формул (3) и (10) для наиболее часто применяемых на практике значений $n \in \mathbb{N}$ с указанием соответствующих АМЗИ (табл. 1).

Таблица 1

Оценка	ε						
	10^{-4}	$5\cdot10^{-4}$	10^{-3}	$5\cdot10^{-3}$	10^{-2}	$5\cdot10^{-2}$	10^{-1}
$n = 56$ (DES)							
$Q_n^{(1)}(0)$	$3{,}60\cdot10^{16}$	$3{,}60\cdot10^{16}$	$3{,}60\cdot10^{16}$	$3{,}60\cdot10^{16}$	$3{,}60\cdot10^{16}$	$3{,}60\cdot10^{16}$	$3{,}60\cdot10^{16}$
$T_n^{(1)}(\varepsilon)$	$3{,}58\cdot10^{16}$	$3{,}50\cdot10^{16}$	$3{,}40\cdot10^{16}$	$2{,}62\cdot10^{16}$	$1{,}78\cdot10^{16}$	$2{,}71\cdot10^{14}$	$1{,}46\cdot10^{12}$
$Q_n^{(1)}(\delta)$	$3{,}40\cdot10^{16}$	$2{,}64\cdot10^{16}$	$1{,}77\cdot10^{16}$	–	–	–	–
$n = 112$ (3DES)							
$Q_n^{(1)}(0)$	$2{,}60\cdot10^{33}$	$2{,}60\cdot10^{33}$	$2{,}60\cdot10^{33}$	$2{,}60\cdot10^{33}$	$2{,}60\cdot10^{33}$	$2{,}60\cdot10^{33}$	$2{,}60\cdot10^{33}$
$T_n^{(1)}(\varepsilon)$	$2{,}57\cdot10^{33}$	$2{,}45\cdot10^{33}$	$2{,}31\cdot10^{33}$	$1{,}28\cdot10^{33}$	$5{,}00\cdot10^{32}$	$7{,}95\cdot10^{28}$	$3{,}55\cdot10^{24}$
$Q_n^{(1)}(\delta)$	$2{,}31\cdot10^{33}$	$1{,}27\cdot10^{33}$	$2{,}17\cdot10^{32}$	–	–	–	–
$n = 128$ (AES, DEAL, KASUMI, Present, SEED, Speck)							
$Q_n^{(1)}(0)$	$1{,}70\cdot10^{38}$	$1{,}70\cdot10^{38}$	$1{,}70\cdot10^{38}$	$1{,}70\cdot10^{38}$	$1{,}70\cdot10^{38}$	$1{,}70\cdot10^{38}$	$1{,}70\cdot10^{38}$
$T_n^{(1)}(\varepsilon)$	$1{,}68\cdot10^{38}$	$1{,}59\cdot10^{38}$	$1{,}48\cdot10^{38}$	$7{,}40\cdot10^{37}$	$2{,}44\cdot10^{37}$	$1{,}10\cdot10^{33}$	$1{,}25\cdot10^{28}$
$Q_n^{(1)}(\delta)$	$1{,}49\cdot10^{38}$	$7{,}25\cdot10^{37}$	–	–	–	–	–
$n = 160$ (SEAL)							
$Q_n^{(1)}(0)$	$7{,}31\cdot10^{47}$	$7{,}31\cdot10^{47}$	$7{,}31\cdot10^{47}$	$7{,}31\cdot10^{47}$	$7{,}31\cdot10^{47}$	$7{,}31\cdot10^{47}$	$7{,}31\cdot10^{47}$
$T_n^{(1)}(\varepsilon)$	$7{,}19\cdot10^{47}$	$6{,}72\cdot10^{47}$	$6{,}15\cdot10^{47}$	$2{,}46\cdot10^{47}$	$5{,}72\cdot10^{46}$	$2{,}10\cdot10^{41}$	$1{,}57\cdot10^{35}$
$Q_n^{(1)}(\delta)$	$6{,}17\cdot10^{47}$	$2{,}22\cdot10^{47}$	–	–	–	–	–
$n = 168$ (3DES)							
$Q_n^{(1)}(0)$	$1{,}87\cdot10^{50}$	$1{,}87\cdot10^{50}$	$1{,}87\cdot10^{50}$	$1{,}87\cdot10^{50}$	$1{,}87\cdot10^{50}$	$1{,}87\cdot10^{50}$	$1{,}87\cdot10^{50}$
$T_n^{(1)}(\varepsilon)$	$1{,}84\cdot10^{50}$	$1{,}71\cdot10^{50}$	$1{,}56\cdot10^{50}$	$5{,}88\cdot10^{49}$	$1{,}26\cdot10^{49}$	$2{,}46\cdot10^{43}$	$9{,}33\cdot10^{36}$
$Q_n^{(1)}(\delta)$	$1{,}56\cdot10^{50}$	$5{,}13\cdot10^{49}$	–	–	–	–	–
$n = 192$ (AES, DEAL, Speck)							
$Q_n^{(1)}(0)$	$3{,}14\cdot10^{57}$	$3{,}14\cdot10^{57}$	$3{,}14\cdot10^{57}$	$3{,}14\cdot10^{57}$	$3{,}14\cdot10^{57}$	$3{,}14\cdot10^{57}$	$3{,}14\cdot10^{57}$
$T_n^{(1)}(\varepsilon)$	$3{,}08\cdot10^{57}$	$2{,}84\cdot10^{57}$	$2{,}54\cdot10^{57}$	$8{,}03\cdot10^{56}$	$1{,}32\cdot10^{56}$	$4{,}06\cdot10^{49}$	$1{,}97\cdot10^{42}$
$Q_n^{(1)}(\delta)$	$2{,}55\cdot10^{57}$	$5{,}95\cdot10^{56}$	–	–	–	–	–
$n = 256$ («Кузнечик», «Магма», AES, DEAL, Speck, Threefish)							
$Q_n^{(1)}(0)$	$5{,}79\cdot10^{76}$	$5{,}79\cdot10^{76}$	$5{,}79\cdot10^{76}$	$5{,}79\cdot10^{76}$	$5{,}79\cdot10^{76}$	$5{,}79\cdot10^{76}$	$5{,}79\cdot10^{76}$
$T_n^{(1)}(\varepsilon)$	$5{,}64\cdot10^{76}$	$5{,}05\cdot10^{76}$	$4{,}34\cdot10^{76}$	$8{,}31\cdot10^{75}$	$6{,}88\cdot10^{74}$	$1{,}58\cdot10^{66}$	$3{,}11\cdot10^{56}$
$Q_n^{(1)}(\delta)$	$4{,}37\cdot10^{76}$	–	–	–	–	–	–

Из табл. 1 видно, что результат утверждения 1 позволяет точнее оценить среднюю трудоёмкость опробования ключа до успеха по сравнению с формулой (3). Вместе с этим при малых значениях ε (например, меньших 10^{-4}) разность значений оценок $T_n^{(1)}(\varepsilon)$ и $Q_n^{(1)}(\delta)$ не столь велика и использование оценки (3), вообще говоря, допустимо. А вот в области больших отклонений ($\varepsilon \geqslant 5 \cdot 10^{-3}$) формула (3) в принципе не работает (в табл. 1 этот факт отмечен символом «–»).

Нетрудно понять, что причиной отсутствия данных в ячейках табл. 1, соответствующих значениям величины $Q_n^{(1)}(\delta)$, является невыполнение условия (4) для соответствующих значений параметров n и ε. Разберемся подробнее с этим вопросом.

Сначала определим область значений ε из (8), для которых возможно использование оценки (3) при фиксированном $n \in \mathbb{N}$.

Утверждение 2. Для любого $n \in \mathbb{N}$ и вероятностной схемы (12) оценка (3) корректна при выполнении неравенства

$$0 \leqslant \varepsilon < \frac{1}{2}\left(\sqrt[n]{1+\frac{1}{4+2^{3-n}}}-1\right). \tag{17}$$

Доказательство. Очевидно, для $\varepsilon = 0$ оценка (3) корректна. Зафиксируем произвольные значения $n \in \mathbb{N}$ и ε, $0 < \varepsilon < 1/2$. Тогда для для расстояния по вариации δ между распределениями $\left(\hat{p}_1(\bar{t}), \ldots, \hat{p}_{2^n}(\bar{t})\right)$ и $(2^{-n}, \ldots, 2^{-n})$ справедливо равенство

$$\begin{gathered}\delta = \frac{1}{2}\sum_{j=1}^{2^n}\left|\hat{p}_j(\bar{t})-\frac{1}{2^n}\right| = \frac{s}{2}\left(\left(\frac{1}{2}+\varepsilon\right)^n-\frac{1}{2^n}\right)+\\ +\frac{1}{2}\left|1-s\left(\frac{1}{2}+\varepsilon\right)^n-(2^n-s-1)\left(\frac{1}{2}-\varepsilon\right)^n-\frac{1}{2^n}\right|+\\ +\frac{(2^n-s-1)}{2}\left(\frac{1}{2^n}-\left(\frac{1}{2}-\varepsilon\right)^n\right).\end{gathered} \tag{18}$$

Используя вытекающее из (13) соотношение

$$(s+1)\,(1/2+\varepsilon)^n + (2^n-s-1)\,(1/2-\varepsilon)^n > 1,$$

оценим сверху второе слагаемое в правой части (18):

$$\begin{gathered}\frac{1}{2}\left|1-s\left(\frac{1}{2}+\varepsilon\right)^n-(2^n-s-1)\left(\frac{1}{2}-\varepsilon\right)^n-\frac{1}{2^n}\right| =\\ =\frac{1}{2}\left|1-(s+1)\left(\frac{1}{2}+\varepsilon\right)^n-(2^n-s-1)\left(\frac{1}{2}-\varepsilon\right)^n+\left(\frac{1}{2}+\varepsilon\right)^n-\frac{1}{2^n}\right| \leqslant\\ \leqslant\frac{1}{2}\left|1-(s+1)\left(\frac{1}{2}+\varepsilon\right)^n-(2^n-s-1)\left(\frac{1}{2}-\varepsilon\right)^n\right|+\frac{1}{2}\left|\left(\frac{1}{2}+\varepsilon\right)^n-\frac{1}{2^n}\right| =\\ =\frac{1}{2}\left((s+1)\left(\frac{1}{2}+\varepsilon\right)^n+(2^n-s-1)\left(\frac{1}{2}-\varepsilon\right)^n-1\right)+\frac{1}{2}\left(\frac{1}{2}+\varepsilon\right)^n-\frac{1}{2^{n+1}}.\end{gathered} \tag{19}$$

Подставив (19) в (18), получим следующую оценку для δ:

$$\delta \leqslant (s+1)\left((1/2+\varepsilon)^n - 2^{-n}\right).$$

В свою очередь, из (4) следует, что выполнение неравенства

$$\begin{gathered}(s+\omega+1)\left(\left(\frac{1}{2}+\varepsilon\right)^n-\frac{1}{2^n}\right)= \\ =\left(2^n\frac{1-(1-2\varepsilon)^n}{(1+2\varepsilon)^n-(1-2\varepsilon)^n}+1\right)\left(\left(\frac{1}{2}+\varepsilon\right)^n-\frac{1}{2^n}\right)<\frac{1}{8},\end{gathered} \tag{20}$$

где $\omega=\left(2^n\dfrac{1-(1-2\varepsilon)^n}{(1+2\varepsilon)^n-(1-2\varepsilon)^n}-s\right)$ — дробная часть числа $2^n\dfrac{1-(1-2\varepsilon)^n}{(1+2\varepsilon)^n-(1-2\varepsilon)^n}$, является достаточным условием корректного использования оценки (3).

Рассмотрим (20) подробнее. Используя справедливое при $-1<x<1$, $k\in\mathbb{N}$ неравенство

$$1-kx\leqslant(1-x)^k,$$

обращающееся в равенство при $x=0$, а также разложение

$$(1+2\varepsilon)^n-(1-2\varepsilon)^n=2\sum_{k=1}^{]n/2[}\mathrm{C}_n^{2k-1}(2\varepsilon)^{2k-1}, \tag{21}$$

где $]z[$ — наименьшее целое число, большее или равное z, выпишем вспомогательное соотношение

$$\frac{1-(1-2\varepsilon)^n}{(1+2\varepsilon)^n-(1-2\varepsilon)^n}<\frac{1-1+2n\varepsilon}{4n\varepsilon}=\frac{1}{2},$$

позволяющее записать достаточное условие выполнения (20):

$$\left(2^{n-1}+1\right)\left(\left(\frac{1}{2}+\varepsilon\right)^n-\frac{1}{2^n}\right)<\frac{1}{8}\ \Leftrightarrow\ \varepsilon<\frac{1}{2}\left(\sqrt[n]{1+\frac{1}{4+2^{3-n}}}-1\right). \tag{22}$$

Утверждение доказано. ■

На рис. 1 представлена зависимость размера определённой в (17) области допустимых для корректного использования оценки (3) значений ε от величины $n\in\mathbb{N}$.

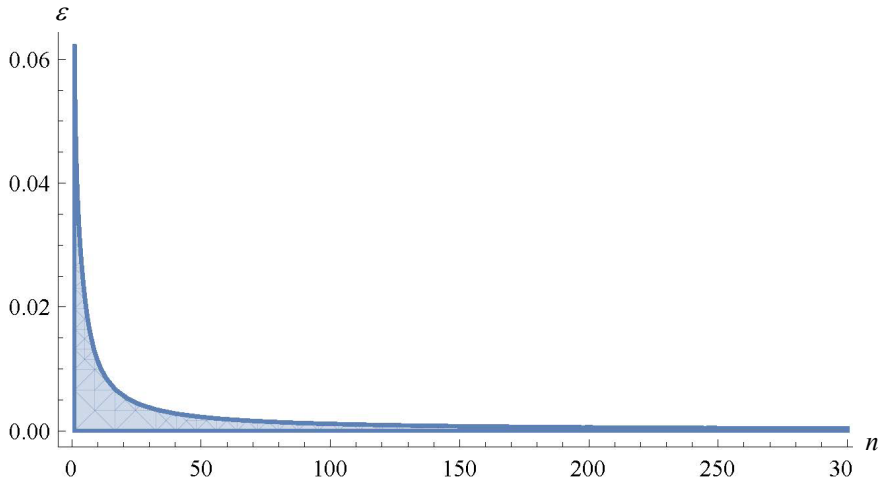

Рис. 1. Область значений ε, удовлетворяющих (17)

В табл. 2 приведены значения правых границ интервалов допустимых значений ε, рассчитанных для указанных в табл. 1 значений $n\in\mathbb{N}$.

Таблица 2

n	56	112	128	160	168	192	256
Макс. знач. ε	$2{,}00 \cdot 10^{-3}$	$9{,}97 \cdot 10^{-4}$	$8{,}72 \cdot 10^{-4}$	$6{,}98 \cdot 10^{-4}$	$6{,}65 \cdot 10^{-4}$	$5{,}81 \cdot 10^{-4}$	$4{,}36 \cdot 10^{-4}$

Замечание 3. Данные табл. 2 в достаточной мере соответствуют информации, приведённой в табл. 1. При необходимости интервал (17) допустимых значений ε может быть скорректирован за счёт более точного оценивания в (21).

Перейдём теперь к оценке длины криптографического ключа, для которой возможно использование оценки (3) при фиксированном значении ε, $0 < \varepsilon < 1/2$.

Утверждение 3. Для любого ε, $0 < \varepsilon < 5/16$, и вероятностной схемы (12) оценка (3) корректна при выполнении неравенства

$$1 \leqslant n < \log_{1+2\varepsilon}(5/4 - 4\varepsilon). \tag{23}$$

Доказательство. Рассмотрим левую часть первого из неравенств (22). Используя разложения [9]

$$(1+2\varepsilon)^n = \sum_{k=0}^{n} \mathrm{C}_n^k (2\varepsilon)^k, \quad \sum_{k=0}^{n} \mathrm{C}_n^k = 2^n$$

и учитывая, что $\varepsilon < 1/2$, выпишем цепочку соотношений

$$\begin{gathered}\left(2^{n-1}+1\right)\left(\left(\frac{1}{2}+\varepsilon\right)^n - \frac{1}{2^n}\right) = \frac{(1+2\varepsilon)^n - 1}{2} + \frac{(1+2\varepsilon)^n - 1}{2^n} = \\ = \frac{(1+2\varepsilon)^n - 1}{2} + \frac{1}{2^n}\left(2\varepsilon C_n^1 + C_n^2 (2\varepsilon)^2 + \ldots + C_n^n (2\varepsilon)^n\right) = \frac{(1+2\varepsilon)^n - 1}{2} + \\ + \frac{\varepsilon}{2^{n-1}}\left(C_n^1 + 2\varepsilon C_n^2 + \ldots + C_n^n (2\varepsilon)^{n-1}\right) < \frac{(1+2\varepsilon)^n - 1}{2} + \\ + \frac{\varepsilon}{2^{n-1}}\left(C_n^1 + C_n^2 + \ldots + C_n^n\right) < \frac{(1+2\varepsilon)^n - 1}{2} + 2\varepsilon,\end{gathered} \tag{24}$$

позволяющую записать достаточное условие выполнения (3):

$$\left((1+2\varepsilon)^n - 1\right)/2 + 2\varepsilon < 1/8 \;\Leftrightarrow\; n < \log_{1+2\varepsilon}(5/4 - 4\varepsilon).$$

Здесь $0 < \varepsilon < 5/16$. ■

На рис. 2 в логарифмической шкале представлена зависимость размера определённой в (23) области допустимых для корректного использования оценки (3) значений n от величины ε, $0 < \varepsilon < 5/16$.

Для значений ε, указанных в табл. 1, приведём результаты оценки правых границ интервалов допустимых значений n (табл. 3).

Таблица 3

ε	10^{-4}	$5 \cdot 10^{-4}$	10^{-3}	$5 \cdot 10^{-3}$	10^{-2}	$5 \cdot 10^{-2}$	10^{-1}
Макс. знач. n	1114	221	110	20	9	–	–

Замечание 4. Данные табл. 3 в целом соответствуют информации, приведённой в табл. 1. При необходимости интервал (23) может быть скорректирован за счёт более точного оценивания в (24).

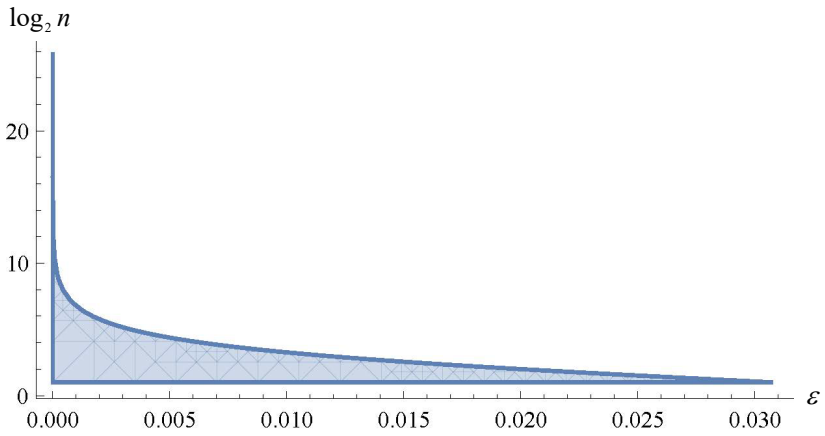

Рис. 2. Область значений n, удовлетворяющих (23)

Результаты утверждений 2 и 3 позволяют оценить связь параметров δ и n, ε, а также описывают ограничения, возникающие при использовании оценки (3) в случаях больших отклонений вероятностных характеристик источников формирования криптографических ключей от «идеальных».

Далее от модели применения одного алгоритма опробования, достоверно приводящего к успеху, перейдём к модели последовательного применения алгоритмов, завершающихся успехом с некоторыми фиксированными вероятностями, не меньшими π, где $0 < \pi \leqslant 1$.

3. Оценка снизу средней трудоёмкости процедуры опробования ключа на основе усечённых алгоритмов

В соответствии с [5] для определения истинного ключа в общем случае используется последовательность разнесённых по времени выполнения усечённых алгоритмов опробования, имеющих некоторые фиксированные вероятности успеха, не меньшие π, $0 < \pi \leqslant 1$. Так, в случае $\pi = 1$ указанная последовательность состоит из одного алгоритма опробования до успеха и, как следствие, средняя трудоёмкость такой процедуры опробования ключа совпадает со средней трудоёмкостью этого алгоритма. Её мы оценили в п. 2. Перейдём к рассмотрению случая $0 < \pi < 1$.

Согласно [5, 6, 10], для каждого такого усечённого алгоритма «успехом» считается событие, состоящее в определении истинного ключа (каждый раз нового, выбираемого в соответствии с распределением (1)). При этом в [5] для вычисления средней трудоёмкости процедуры определения ключа, заключающейся в последовательном применении усечённых алгоритмов опробования, используется модель независимых испытаний с фиксированной вероятностью успеха π. Число таких испытаний представляет собой случайную величину τ, имеющую геометрическое распределение с параметром π (далее будем обозначать $\tau \sim \mathrm{Geom}(\pi)$).

Замечание 5. Как и в п. 2, мы откажемся от жёстких условий стационарности источника и независимости битов формируемых им ключей, позволяющих применять для анализа классическую модель независимых испытаний.

Для источника, функционирующего в соответствии с вероятностной схемой (7), через ξ_i, $i = 1, 2, \ldots$, обозначим случайную величину, равную трудоёмкости определения истинного ключа при применении i-го усечённого алгоритма.

В силу возможной зависимости битов ключей, формируемых источником (6), в общем случае величины $\xi_1, \xi_2, \ldots$ являются зависимыми.

Для произвольного $i = 1, 2, \ldots$ через $\overline{p}_i(\bar{t}_i)$ обозначим распределение вероятностной схемы (7) в момент применения i-го усечённого алгоритма:

$$\overline{p}_i(\bar{t}_i) = \left(p_1(\bar{t}_i), p_2(\bar{t}_i), \ldots, p_{2^n}(\bar{t}_i)\right).$$

Здесь $\bar{t}_i = \left(t_1^{(i)}, t_2^{(i)}, \ldots, t_n^{(i)}\right)$ — вектор соответствующих моментов времени формирования битов ключа. Отметим, что для источника, не являющегося в общем случае стационарным, $\overline{p}_i(\bar{t}_i) \neq \overline{p}_j(\overline{t_j})$ и, как следствие, $\mathbf{E}\xi_i \neq \mathbf{E}\xi_j$, $i, j \geqslant 1$, $i \neq j$.

Для произвольного $i = 1, 2, \ldots$ и $k \in \{1, 2, \ldots, 2^n\}$ положим

$$\pi_k^{(i)} = \sum_{j=1}^{k} p_j(\bar{t}_i).$$

Тогда по формуле полной вероятности для отдельно взятого i-го усечённого алгоритма

$$\mathbf{E}\xi_i = \left(1 - \pi_{l_i}^{(i)}\right) l_i + \sum_{j=1}^{l_i} j p_j(\bar{t}_i), \tag{25}$$

где $l_i = \min\left\{k \in \{1, 2, \ldots, 2^n\} \colon \pi_k^{(i)} \geqslant \pi\right\}$.

Замечание 6. Поскольку в общем случае $\pi_{l_i}^{(i)} \neq \pi$, то фактически i-й усечённый алгоритм имеет вероятность успеха $\pi_{l_i}^{(i)} \geqslant \pi$.

Наконец, через τ обозначим случайную величину, равную порядковому номеру усечённого алгоритма опробования, при применении которого определяется истинный ключ.

С учётом изложенного, трудоёмкость процедуры определения ключа, сформированного в соответствии с (7), заключающейся в последовательном применении усечённых алгоритмов опробования с вероятностями успеха не меньшими π, представляется в следующем виде:

$$T^{(\pi)}_{\mathcal{A}_\varepsilon(\bar{t}_1), \ldots, \mathcal{A}_\varepsilon(\overline{t_\tau})} = \sum_{i=1}^{\tau} \xi_i.$$

Для произвольных параметров $n \in \mathbb{N}$ и ε, $0 < \varepsilon < 1/2$, вероятностной схемы (7), а также для произвольного π, $0 < \pi \leqslant 1$, введём обозначение

$$T_n^{(\pi)}(\varepsilon) = \min_{\bar{t}_1, \ldots, \bar{t}_\tau} \left(\min_{\substack{p_1(\bar{t}_1), \ldots, p_{2^n}(\bar{t}_1) \\ \cdots \\ p_1(\bar{t}_\tau), \ldots, p_{2^n}(\bar{t}_\tau)}} \left(\mathbf{E} T^{(\pi)}_{\mathcal{A}_\varepsilon(\bar{t}_1), \ldots, \mathcal{A}_\varepsilon(\bar{t}_\tau)} \right) \right),$$

где $1 \leqslant t_1^{(i)} < t_2^{(i)} < \ldots < t_n^{(i)}$; $\left(p_1(\bar{t}_i), p_2(\bar{t}_i), \ldots, p_{2^n}(\bar{t}_i)\right)$ — векторы, удовлетворяющие (8), $i = 1, \ldots, \tau$. Тогда справедливо

Утверждение 4. Для произвольных $n \in \mathbb{N}$, ε, $0 < \varepsilon < 1/2$, и π, $0 < \pi \leqslant 1$, справедливы следующие равенства:

— если $0 < \pi \leqslant s\,(1/2 + \varepsilon)^n$, то

$$T_n^{(\pi)}(\varepsilon) = \frac{2^n}{(1+2\varepsilon)^n} - \left]\frac{2^n\pi}{(1+2\varepsilon)^n}\right[+ \frac{(1+2\varepsilon)^n}{2^{n+1}} \left(\left(\left]\frac{2^n\pi}{(1+2\varepsilon)^n}\right[\right)^2 + \left]\frac{2^n\pi}{(1+2\varepsilon)^n}\right[\right); \tag{26}$$

— если $s(1/2+\varepsilon)^n < \pi \leqslant 1-(2^n-s-1)\,(1/2-\varepsilon)^n$, то

$$T_n^{(\pi)}(\varepsilon) = \frac{2^n(s+1)}{2^n-(2^n-s-1)\,(1-2\varepsilon)^n} - \\ -(s+1)\left(\frac{s}{2}\,(1/2+\varepsilon)^n + (2^n-s-1)\,(1/2-\varepsilon)^n\right); \tag{27}$$

— если $1-(2^n-s-1)\,(1/2-\varepsilon)^n < \pi \leqslant 1$, то

$$T_n^{(\pi)}(\varepsilon) = \left(\left(2^n - \left[\frac{2^n(1-\pi)}{(1-2\varepsilon)^n}\right]\right)\left[\frac{2^n(1-\pi)}{(1-2\varepsilon)^n}\right](1-2\varepsilon)^n\right) \Big/ \left(2^n - \left[\frac{2^n(1-\pi)}{(1-2\varepsilon)^n}\right](1-2\varepsilon)^n\right) + \\ +s+1-\frac{s(s+1)}{2}\left(\frac{1}{2}+\varepsilon\right)^n + \\ +\frac{1}{2}\left(2^{2n}-2^{n+1}s-2^n+\left[\frac{2^n(1-\pi)}{(1-2\varepsilon)^n}\right]\left(\left[\frac{2^n(1-\pi)}{(1-2\varepsilon)^n}\right]-2^{n+1}-1\right)+s^2+s\right)(1/2-\varepsilon)^n, \tag{28}$$

где $s = \left[2^n \dfrac{1-(1-2\varepsilon)^n}{(1+2\varepsilon)^n-(1-2\varepsilon)^n}\right]$. При этом для $\varepsilon \in \{0, 1/2\}$

$$T_n^{(\pi)}(0) = 2^n -]2^n\pi[+ \frac{(]2^n\pi[)^2 +]2^n\pi[}{2^{n+1}}, \quad T_n^{(\pi)}(1/2) = 1. \tag{29}$$

Доказательство. Зафиксируем произвольное значение π, $0 < \pi \leqslant 1$. Тогда по определению условного математического ожидания [11, с. 54]

$$\mathbf{E}T^{(\pi)}_{\mathcal{A}_\varepsilon(\bar{t}_1),\ldots,\mathcal{A}_\varepsilon(\bar{t}_\tau)} = \mathbf{E}\sum_{i=1}^{\tau}\xi_i = \sum_{j=1}^{\infty}\mathbf{E}\left(\sum_{i=1}^{\tau}\xi_i\Big|\tau=j\right)\Pr\{\tau=j\},$$

где $\Pr\{\tau=j\} = \pi_{l_j}^{(j)}\prod\limits_{i=1}^{j-1}\left(1-\pi_{l_i}^{(i)}\right)$. При этом по построению процедуры опробования, а также с учётом соотношения (25)

$$\mathbf{E}\left(\sum_{i=1}^{\tau}\xi_i\Big|\tau=j\right) = \sum_{i=1}^{j-1}l_i + \sum_{i=1}^{l_j} i p_i(\bar{t}_j). \tag{30}$$

Выпишем (30) для минимизирующей его вероятностной схемы (12) с распределением (14)–(16). Рассмотрим сначала два граничных случая: $\varepsilon \in \{0, 1/2\}$.

Пусть $\varepsilon = 0$. Тогда для $i = 1, \ldots, j$ справедливы равенства $l_i =]2^n\pi[$ и $\pi_{l_i}^{(i)} = l_i/2^n$. Таким образом, (30) принимает следующий вид:

$$\mathbf{E}\left(\sum_{i=1}^{\tau}\xi_i\Big|\tau=j\right) = (j-1)\,]2^n\pi[+ \frac{1}{2^n}\sum_{i=1}^{]2^n\pi[} i = (j-1)\,]2^n\pi[+ \frac{]2^n\pi[+1}{2^{n+1}}\,]2^n\pi[.$$

При этом $\Pr\{\tau=j\} = \dfrac{]2^n\pi[}{2^n}\left(1-\dfrac{]2^n\pi[}{2^n}\right)^{j-1}$, т. е. $\tau \sim \mathrm{Geom}\left(\dfrac{]2^n\pi[}{2^n}\right)$. Тогда

$$\mathbf{E}\tau = \frac{2^n}{]2^n\pi[} \quad \text{и} \quad \mathbf{E}T^{(\pi)}_{\mathcal{A}_0(\bar{t}_1),\ldots,\mathcal{A}_0(\bar{t}_\tau)} =]2^n\pi[\underbrace{\sum_{j=1}^{\infty}(j-1)\frac{]2^n\pi[}{2^n}\left(1-\frac{]2^n\pi[}{2^n}\right)^{j-1}}_{\mathbf{E}(\tau-1)} + \\ +\frac{]2^n\pi[+1}{2^{n+1}}\,]2^n\pi[\underbrace{\sum_{j=1}^{\infty}\frac{]2^n\pi[}{2^n}\left(1-\frac{]2^n\pi[}{2^n}\right)^{j-1}}_{1} = 2^n -]2^n\pi[+ \frac{(]2^n\pi[)^2+]2^n\pi[}{2^{n+1}}.$$

С учётом отсутствия зависимости полученного выражения от $\bar{t}_1, \ldots, \bar{t}_\tau$ выполняется первое из равенств (29).

Пусть $\varepsilon = 1/2$. Тогда $l_i = 1$ и $\pi_{l_i}^{(i)} = 1$. Таким образом,

$$\Pr\{\tau = 1\} = 1 \quad \text{и} \quad \mathbf{E}T^{(\pi)}_{\mathcal{A}_{1/2}(\bar{t}_1),\ldots,\mathcal{A}_{1/2}(\bar{t}_\tau)} = 1,$$

откуда следует второе из равенств (29).

Пусть теперь $0 < \varepsilon < 1/2$. Рассмотрим отдельно три случая.

Если $\pi \leqslant s(1/2+\varepsilon)^n$, то $l_i = \left]\dfrac{2^n\pi}{(1+2\varepsilon)^n}\right[$ и $\pi_{l_i}^{(i)} = l_i(1/2+\varepsilon)^n$ для $i = 1, \ldots, j$. Таким образом, (30) принимает следующий вид:

$$\mathbf{E}\left(\sum_{i=1}^{\tau}\xi_i\Big|\tau = j\right) = (j-1)\left]\frac{2^n\pi}{(1+2\varepsilon)^n}\right[+ (1/2+\varepsilon)^n \sum_{i=1}^{]2^n\pi/(1+2\varepsilon)^n[} i =$$
$$= (j-1)\left]\frac{2^n\pi}{(1+2\varepsilon)^n}\right[+ \frac{(1+2\varepsilon)^n}{2^{n+1}}\left(\left]\frac{2^n\pi}{(1+2\varepsilon)^n}\right[+ 1\right)\left]\frac{2^n\pi}{(1+2\varepsilon)^n}\right[.$$

В рассматриваемом случае $\Pr\{\tau{=}j\}{=}(1/2{+}\varepsilon)^n\left]\dfrac{2^n\pi}{(1+2\varepsilon)^n}\right[\left(1{-}\left(\dfrac{1}{2}{+}\varepsilon\right)^n\right]\dfrac{2^n\pi}{(1{+}2\varepsilon)^n}\left[\right)^{j-1}$, т. е. $\tau \sim \mathrm{Geom}\left(\left(\dfrac{1}{2}+\varepsilon\right)^n\right]\dfrac{2^n\pi}{(1+2\varepsilon)^n}\left[\right)$, поэтому $\mathbf{E}\tau = 2^n\Big/\left((1+2\varepsilon)^n\right]\dfrac{2^n\pi}{(1+2\varepsilon)^n}\left[\right)$. В результате

$$\mathbf{E}T^{(\pi)}_{\mathcal{A}_\varepsilon(\bar{t}_1),\ldots,\mathcal{A}_\varepsilon(\bar{t}_\tau)} = \left]\frac{2^n\pi}{(1+2\varepsilon)^n}\right[\mathbf{E}(\tau-1) + \frac{(1+2\varepsilon)^n}{2^{n+1}}\left(\left(\left]\frac{2^n\pi}{(1+2\varepsilon)^n}\right[\right)^2 + \left]\frac{2^n\pi}{(1+2\varepsilon)^n}\right[\right) =$$
$$= \frac{2^n}{(1+2\varepsilon)^n} - \left]\frac{2^n\pi}{(1+2\varepsilon)^n}\right[\frac{(1+2\varepsilon)^n}{2^{n+1}}\left(\left(\left]\frac{2^n\pi}{(1+2\varepsilon)^n}\right[\right)^2 + \left]\frac{2^n\pi}{(1+2\varepsilon)^n}\right[\right),$$

откуда следует (26).

Если $s(1/2+\varepsilon)^n < \pi \leqslant 1 - (2^n - s - 1)\,(1/2-\varepsilon)^n$, то для $i = 1, \ldots, j$ получаем

$$l_i = s+1 \quad \text{и} \quad \pi_{l_i}^{(i)} = s(1/2+\varepsilon)^n + 1 - s(1/2+\varepsilon)^n - (2^n - s - 1)\,(1/2-\varepsilon)^n +$$
$$+(l_i - s - 1)(1/2-\varepsilon)^n = 1 - (2^n - s - 1)\,(1/2-\varepsilon)^n,$$

поэтому

$$\mathbf{E}\left(\sum_{i=1}^{\tau}\xi_i\Big|\tau = j\right) = (j-1)(s+1) + (1/2+\varepsilon)^n\sum_{i=1}^{s} i +$$
$$+(s+1)\left(1 - s\,(1/2+\varepsilon)^n - (2^n - s - 1)\,(1/2-\varepsilon)^n\right) =$$
$$= j(s+1) - \frac{s(s+1)}{2}\left(\frac{1}{2}+\varepsilon\right)^n - (s+1)\,(2^n - s - 1)\left(\frac{1}{2}-\varepsilon\right)^n.$$

При этом $\Pr\{\tau = j\} = \left(1 - (2^n - s - 1)\,(1/2-\varepsilon)^n\right)\left((2^n - s - 1)\,(1/2-\varepsilon)^n\right)^{j-1}$, т. е. $\tau \sim$ $\sim \mathrm{Geom}\left(1 - (2^n - s - 1)\,(1/2-\varepsilon)^n\right)$. Таким образом, $\mathbf{E}\tau = \dfrac{2^n}{2^n - (2^n - s - 1)\,(1-2\varepsilon)^n}$ и

$$\mathbf{E}T^{(\pi)}_{\mathcal{A}_\varepsilon(\bar{t}_1),\ldots,\mathcal{A}_\varepsilon(\bar{t}_\tau)} = (s+1)\mathbf{E}\tau - \frac{s(s+1)}{2}\left(\frac{1}{2}+\varepsilon\right)^n - (s+1)\,(2^n - s - 1)\left(\frac{1}{2}-\varepsilon\right)^n =$$

$$= (s+1)\left(\frac{2^n}{2^n-(2^n-s-1)(1-2\varepsilon)^n} - \frac{s}{2}\left(\frac{1}{2}+\varepsilon\right)^n - (2^n-s-1)\left(\frac{1}{2}-\varepsilon\right)^n\right),$$

откуда получаем (27).

Наконец, если $1-(2^n-s-1)(1/2-\varepsilon)^n < \pi \leqslant 1$, то для $i=1,\ldots,j$ справедливы равенства $l_i = 2^n - \left[\dfrac{2^n(1-\pi)}{(1-2\varepsilon)^n}\right]$ и $\pi_{l_i}^{(i)} = 1 - \left[\dfrac{2^n(1-\pi)}{(1-2\varepsilon)^n}\right]\left(\dfrac{1}{2}-\varepsilon\right)^n$, поэтому

$$\mathbf{E}\left(\sum_{i=1}^{\tau}\xi_i\Big|\tau=j\right) = (j-1)\left(2^n - \left[\frac{2^n(1-\pi)}{(1-2\varepsilon)^n}\right]\right) + \left(\frac{1}{2}+\varepsilon\right)^n\sum_{i=1}^{s} i +$$

$$+(s+1)\left(1-s\left(\frac{1}{2}+\varepsilon\right)^n - (2^n-s-1)\left(\frac{1}{2}-\varepsilon\right)^n\right) + \left(\frac{1}{2}-\varepsilon\right)^n \sum_{i=s+2}^{2^n-[2^n(1-\pi)/(1-2\varepsilon)^n]} i =$$

$$= (j-1)\left(2^n - \left[\frac{2^n(1-\pi)}{(1-2\varepsilon)^n}\right]\right) + s + 1 - \frac{s(s+1)}{2}\left(\frac{1}{2}+\varepsilon\right)^n - (s+1)(2^n-s-1)\left(\frac{1}{2}-\varepsilon\right)^n +$$

$$+\frac{1}{2}\left(2^n - \left[\frac{2^n(1-\pi)}{(1-2\varepsilon)^n}\right] - s - 1\right)\left(2^n - \left[\frac{2^n(1-\pi)}{(1-2\varepsilon)^n}\right] + s + 2\right)\left(\frac{1}{2}-\varepsilon\right)^n =$$

$$= (j-1)\left(2^n - \left[\frac{2^n(1-\pi)}{(1-2\varepsilon)^n}\right]\right) + s + 1 - \frac{s(s+1)}{2}\left(\frac{1}{2}+\varepsilon\right)^n +$$

$$+\frac{1}{2}\left(2^{2n} - 2^{n+1}s - 2^n + \left[\frac{2^n(1-\pi)}{(1-2\varepsilon)^n}\right]\left(\left[\frac{2^n(1-\pi)}{(1-2\varepsilon)^n}\right] - 2^{n+1} - 1\right) + s^2 + s\right)\left(\frac{1}{2}-\varepsilon\right)^n.$$

При этом $\Pr\{\tau=j\} = \left(1 - \left[\dfrac{2^n(1-\pi)}{(1-2\varepsilon)^n}\right]\left(\dfrac{1}{2}-\varepsilon\right)^n\right)\left(\left[\dfrac{2^n(1-\pi)}{(1-2\varepsilon)^n}\right]\left(\dfrac{1}{2}-\varepsilon\right)^n\right)^{j-1}$, т. е. $\tau \sim \mathrm{Geom}\left(1-\left[\dfrac{2^n(1-\pi)}{(1-2\varepsilon)^n}\right]\left(\dfrac{1}{2}-\varepsilon\right)^n\right)$. Следовательно, $\mathbf{E}\tau = \left(1-\left[\dfrac{2^n(1-\pi)}{(1-2\varepsilon)^n}\right]\left(\dfrac{1}{2}-\varepsilon\right)^n\right)^{-1}$ и выполняется равенство

$$\mathbf{E}T^{(\pi)}_{\mathcal{A}_\varepsilon(\bar{t}_1),\ldots,\mathcal{A}_\varepsilon(\bar{t}_\tau)} = \frac{\left(2^n - \left[\dfrac{2^n(1-\pi)}{(1-2\varepsilon)^n}\right]\right)\left[\dfrac{2^n(1-\pi)}{(1-2\varepsilon)^n}\right](1-2\varepsilon)^n}{2^n - \left[\dfrac{2^n(1-\pi)}{(1-2\varepsilon)^n}\right](1-2\varepsilon)^n} + s + 1 - \frac{s(s+1)}{2}\left(\frac{1}{2}+\varepsilon\right)^n +$$

$$+\frac{1}{2}\left(2^{2n} - 2^{n+1}s - 2^n + \left[\frac{2^n(1-\pi)}{(1-2\varepsilon)^n}\right]\left(\left[\frac{2^n(1-\pi)}{(1-2\varepsilon)^n}\right] - 2^{n+1} - 1\right) + s^2 + s\right)\left(\frac{1}{2}-\varepsilon\right)^n,$$

из которого следует (28). ■

Замечание 7. Верификация выражений (26)–(28) выполнена с использованием автоматизированной системы упрощения алгебраических выражений пакета Wolfram Mathematica 12.1.

Проиллюстрируем характер зависимости $T_n^{(\pi)}(\varepsilon)$ от величины π, $0 < \pi \leqslant 1$, при $n=7$ и некоторых фиксированных значениях параметра ε (рис. 3).

Из графиков на рис. 3 видно, что с увеличением значения ε эффективность (с точки зрения трудозатрат) последовательности разнесённых по времени выполнения усечённых алгоритмов опробования становится выше, чем у алгоритма опробования до успеха.

Приведённые результаты и примеры ещё раз подтверждают тезис о важности обоснования выбора модели опробования ключа — до успеха или на основе нескольких

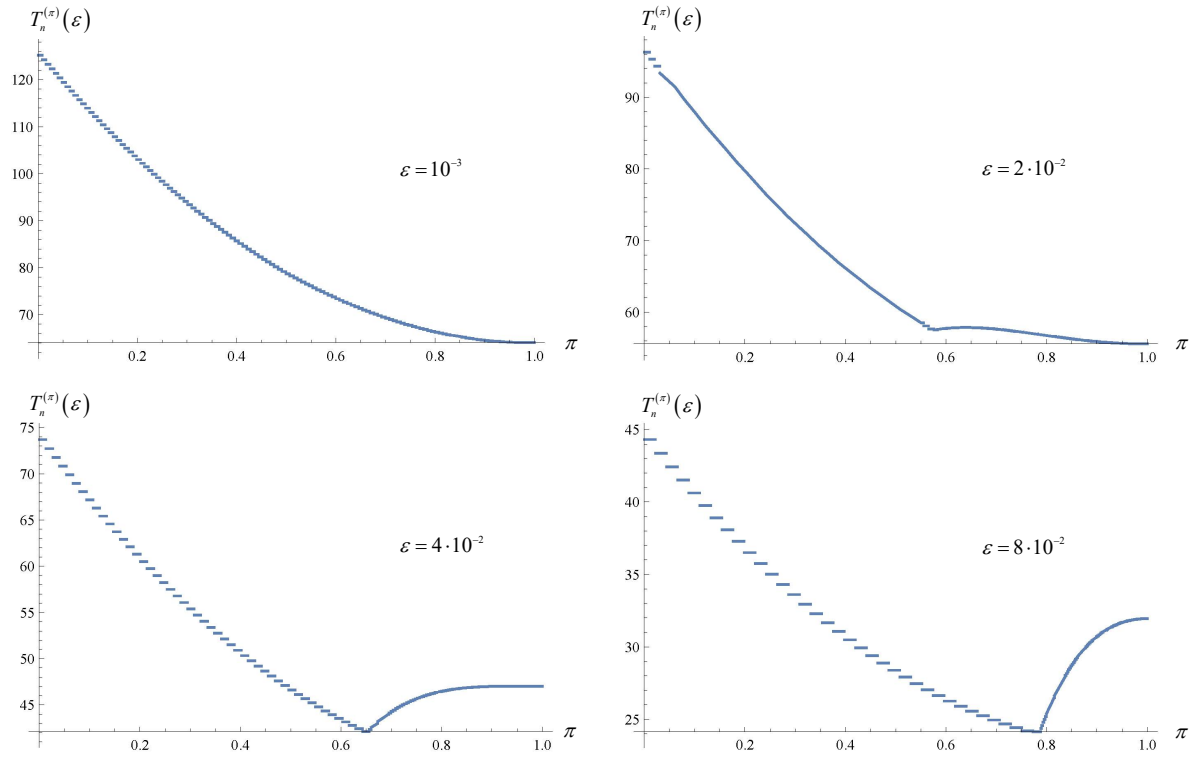

Рис. 3. Зависимость $T_n^{(\pi)}(\varepsilon)$ от π при $n = 7$ и некоторых значениях ε

усечённых алгоритмов. В отдельных случаях та или иная модель может давать существенный выигрыш по трудоёмкости.

Итак, мы получили точные и достижимые оценки снизу для средней трудоёмкости процедуры опробования ключа на основе усечённых алгоритмов с вероятностями успеха, не меньшими некоторой заданной границы π, $0 < \pi \leqslant 1$. Перейдём к финальному этапу исследования — оценке практической секретности ключа.

4. Оценка снизу практической секретности ключа

Для произвольных параметров $n \in \mathbb{N}$ и ε, $0 < \varepsilon < 1/2$, вероятностной схемы (7) через $T_n(\varepsilon)$ обозначим практическую секретность ключа, сформированного источником (6).

Согласно общей теории [5, 6] и результатам предыдущих пунктов настоящей работы, справедливо равенство

$$T_n(\varepsilon) = \min_{0<\pi\leqslant 1}\left(\min_{\bar{t}_1,\ldots,\bar{t}_\tau}\left(\min_{\substack{p_1(\bar{t}_1),\ldots,p_{2^n}(\bar{t}_1)\\ \ldots\\ p_1(\bar{t}_\tau),\ldots,p_{2^n}(\bar{t}_\tau)}} \mathbf{E}T^{(\pi)}_{\mathcal{A}_\varepsilon(\bar{t}_1),\ldots,\mathcal{A}_\varepsilon(\bar{t}_\tau)}\right)\right), \tag{31}$$

где $\bar{t}_i = \left(t_1^{(i)}, t_2^{(i)}, \ldots, t_n^{(i)}\right)$, $1 \leqslant t_1^{(i)} < t_2^{(i)} < \ldots < t_n^{(i)}$, векторы $\left(p_1(\bar{t}_i), p_2(\bar{t}_i), \ldots, p_{2^n}(\bar{t}_i)\right)$ удовлетворяют (8), $i = 1, \ldots, \tau$, а π — нижняя граница вероятностей успеха усечённых алгоритмов опробования, $0 < \pi \leqslant 1$.

С учётом введённых в п. 3 обозначений выражение (31) может быть записано в компактном виде

$$T_n(\varepsilon) = \min_{0<\pi\leqslant 1} \left(T_n^{(\pi)}(\varepsilon)\right). \tag{32}$$

Таким образом, процесс вычисления $T_n(\varepsilon)$ сводится к определению минимума кусочно-постоянной функции, описанной в утверждении 4.

В табл. 4 приведены достижимые оценки снизу практической секретности ключа $T_n(\varepsilon)$, вычисленные с использованием формул (32) и (26)–(28) для значений $n \in \mathbb{N}$ и ε, $0 < \varepsilon < 1/2$, указанных в табл. 1, и показано, на каких значениях π достигаются эти оценки.

Таблица 4

Оценка	ε						
	10^{-4}	$5\cdot 10^{-4}$	10^{-3}	$5\cdot 10^{-3}$	10^{-2}	$5\cdot 10^{-2}$	10^{-1}
$n = 56$							
$T_n(\varepsilon)$	$3{,}58\cdot 10^{16}$	$3{,}50\cdot 10^{16}$	$3{,}40\cdot 10^{16}$	$2{,}33\cdot 10^{16}$	$1{,}26\cdot 10^{16}$	$1{,}73\cdot 10^{14}$	$1{,}33\cdot 10^{12}$
π	1	1	1	0,639	0,758	0,997	0,999
$n = 112$							
$T_n(\varepsilon)$	$2{,}57\cdot 10^{33}$	$2{,}45\cdot 10^{33}$	$2{,}31\cdot 10^{33}$	$9{,}02\cdot 10^{32}$	$2{,}85\cdot 10^{32}$	$6{,}00\cdot 10^{28}$	$3{,}52\cdot 10^{24}$
π	1	1	1	0,756	0,906	0,999	0,999
$n = 128$							
$T_n(\varepsilon)$	$1{,}68\cdot 10^{38}$	$1{,}59\cdot 10^{38}$	$1{,}48\cdot 10^{38}$	$4{,}98\cdot 10^{37}$	$1{,}36\cdot 10^{37}$	$8{,}56\cdot 10^{32}$	$1{,}25\cdot 10^{28}$
π	1	1	1	0,784	0,930	0,999	1
$n = 160$							
$T_n(\varepsilon)$	$7{,}19\cdot 10^{47}$	$6{,}72\cdot 10^{47}$	$6{,}15\cdot 10^{47}$	$1{,}53\cdot 10^{47}$	$3{,}08\cdot 10^{46}$	$1{,}74\cdot 10^{41}$	$1{,}57\cdot 10^{35}$
π	1	1	1	0,834	0,962	0,999	1
$n = 168$							
$T_n(\varepsilon)$	$1{,}84\cdot 10^{50}$	$1{,}71\cdot 10^{50}$	$1{,}56\cdot 10^{50}$	$3{,}60\cdot 10^{49}$	$6{,}72\cdot 10^{48}$	$2{,}08\cdot 10^{43}$	$9{,}33\cdot 10^{36}$
π	1	1	1	0,845	0,968	0,999	1
$n = 192$							
$T_n(\varepsilon)$	$3{,}08\cdot 10^{57}$	$2{,}84\cdot 10^{57}$	$2{,}49\cdot 10^{57}$	$4{,}72\cdot 10^{56}$	$7{,}01\cdot 10^{55}$	$3{,}54\cdot 10^{49}$	$1{,}97\cdot 10^{42}$
π	1	1	0,595	0,874	0,980	0,999	1
$n = 256$							
$T_n(\varepsilon)$	$5{,}64\cdot 10^{76}$	$5{,}05\cdot 10^{76}$	$3{,}96\cdot 10^{76}$	$4{,}56\cdot 10^{75}$	$3{,}64\cdot 10^{74}$	$1{,}47\cdot 10^{66}$	$3{,}11\cdot 10^{56}$
π	1	1	0,626	0,929	0,994	0,999	1

Заключение

Для математической модели дискретного источника (6), приближённой к реальным условиям функционирования физических устройств, используемых для формирования криптографических ключей, в том числе допускающей нестационарность таких устройств, а также наличие зависимости между битами формируемых ключей, получены достижимые оценки снизу практической секретности ключа.

Результаты работы обобщают ранее известные оценки, выписанные в достаточно «рафинированных» модельных предположениях [5, 6].

ЛИТЕРАТУРА

1. *Kahn D.* The Codebreakers: the Story of Secret Writing. N.Y.: Scribner, 1996. 1181 p.
2. *Шнайер Б.* Прикладная криптография. Протоколы, алгоритмы и исходные тексты на языке С. М.: Триумф, 2002. 816 с.
3. *Арбеков И. М.* Элементарная квантовая криптография: Для криптографов, не знакомых с квантовой механикой. М.: URSS, 2022. 168 с.

4. *Turam M., Barker E., Kelsey J., and McKay K.* Recommendation for the Entropy Sources Used for Random Bit Generation. NIST Special Publ. 800-90B. 2018. 76 p.
5. *Арбеков И. М.* Критерии секретности ключа // Матем. вопр. криптогр. 2016. Т. 7. Вып. 1. С. 39–56.
6. *Arbekov I. M.* Lower bounds for the practical secrecy of a key // Матем. вопр. криптогр. 2017. Т. 8. Вып. 2. С. 29–38.
7. *Лось А. Б., Миронкин В. О.* Теоретико-информационные аспекты защиты информации. М.: URSS, 2023. 144 с.
8. *Лось А. Б., Нестеренко А. Ю., Рогачева О. А.* О влиянии неравновероятности выходной последовательности на качество криптографических преобразований // Алгебра, теория чисел, дискретная геометрия и многомасштабное моделирование: современные проблемы, приложения и проблемы истории. Материалы XXII Междунар. конф., посвящённой 120-летию со дня рождения академика А. Н. Колмогорова и 60-летию со дня открытия школы-интерната № 18 при Московском университете. Тула: ТГПУ им. Л. Н. Толстого, 2023. С. 151–157.
9. *Феллер В.* Введение в теорию вероятностей и ее приложения. Т. 1. 2-е изд. М.: Мир, 1963. 498 с.
10. *Карпов А. А., Миронкин В. О., Михайлов М. М.* Об энтропийных характеристиках последовательной процедуры опробования элементов полиномиальной схемы // Обозр. прикл. и промышл. матем. 2021. Т. 28. № 1. С. 9–12.
11. *Кельберт М. Я., Сухов Ю. М.* Вероятность и статистика в примерах и задачах. Т. I: Основные понятия теории вероятностей и математической статистики. 2-е изд., доп. М.: МЦНМО, 2010. 486 с.

REFERENCES

1. *Kahn D.* The Codebreakers: the Story of Secret Writing. N.Y., Scribner, 1996. 1181 p.
2. *Schneier B.* Applied Cryptography: Protocols, Algorithms, and Source Code in C. John Wiley & Sons, 1996.
3. *Arbekov I. M.* Elementarnaya kvantovaya kriptografiya: Dlya kriptografov, ne znakomykh s kvantovoy mekhanikoy. [Elementary Quantum Cryptography: For Cryptographers who are not Familiar with Quantum Mechanics]. Moscow, URSS Publ., 2022. 168 p. (in Russian)
4. *Turam M., Barker E., Kelsey J., and McKay K.* Recommendation for the Entropy Sources Used for Random Bit Generation. NIST Special Publication 800-90B, 2018. 76 p.
5. *Arbekov I. M.* Kriterii sekretnosti klyucha [Key secrecy criteria]. Matem. Vopr. Kriptogr., 2016, vol. 7, no. 1, pp. 39–56. (in Russian)
6. *Arbekov I. M.* Lower bounds for the practical secrecy of a key. Matem. Vopr. Kriptogr., 2017, vol. 8, no. 2, pp. 29–38.
7. *Los A. B. and Mironkin V. O.* Teoretiko-informatsionnye aspekty zashchity informatsii [Information-Theoretical Aspects of Information Security]. Moscow, URSS Publ., 2023. 144 p. (in Russian)
8. *Los A. B., Nesterenko A. Yu., and Rogacheva O. A.* O vliyanii neravnoveroyatnosti vykhodnoy posledovatel'nosti na kachestvo kriptograficheskikh preobrazovaniy [On the effect of the nonprobability of the output sequence on the quality of cryptographic transformations]. Algebra, teoriya chisel, diskretnaya geometriya i mnogomasshtabnoe modelirovanie: Sovremennye problemy, prilozheniya i problemy istorii. Materialy XXII Mezhdunar. konf., posvyashchennoy 120-letiyu so dnya rozhdeniya akademika A. N. Kolmogorova i 60-letiyu so dnya otkrytiya shkoly-internata № 18 pri Moskovskom universitete. Tula, TGPU im. L. N. Tolstogo, 2023, pp. 151–157. (in Russian)

9. *Feller W.* An Introduction to Probability Theory and its Applications, vol. I. John Wiley & Sons, 1957.
10. *Karpov A. A., Mironkin V. O., and Mikhaylov M. M.* Ob entropiynykh kharakteristikakh posledovatel'noy protsedury oprobovaniya elementov polinomial'noy skhemy [On the entropy characteristics of a sequential procedure for testing elements of a polynomial scheme]. Obozr. Prikl. i Promyshl. Matem., 2021, vol. 28, no. 1, pp. 9–12. (in Russian)
11. *Kel'bert M. Ya. and Sukhov Yu. M.* Veroyatnost' i statistika v primerakh i zadachakh. T. I: Osnovnye ponyatiya teorii veroyatnostey i matematicheskoy statistiki [Probability and Statistics in Examples and Problems. Vol. I: Basic Concepts of Probability Theory and Mathematical Statistics]. 2nd ed. Moscow, MCCME Publ., 2010. 486 p. (in Russian)

ПРИКЛАДНАЯ ТЕОРИЯ КОДИРОВАНИЯ

УДК 519.17 DOI 10.17223/20710410/65/5

ПОСТРОЕНИЕ КВАЗИЦИКЛИЧЕСКИХ АЛЬТЕРНАНТНЫХ КОДОВ И ИХ ПРИЛОЖЕНИЕ В КОДОВЫХ КРИПТОСИСТЕМАХ[1]

А. А. Кунинец*, Е. С. Малыгина**

*Балтийский федеральный университет им. И. Канта, г. Калининград, Россия
**НИУ ВШЭ, г. Москва, Россия

E-mail: artkuninets@yandex.ru, emalygina@hse.ru

Представлен обзор квазициклических альтернантных кодов и их структурный анализ относительно классификации автоморфизмов. Детализированы методы восстановления структурной информации о коде, которые, в свою очередь, снабжены подробными примерами. 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 подполевых подкодов квазициклических алгеброгеометрических кодов, ассоциированных с произвольной кривой с известной группой автоморфизмов. Однако 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.*

CONSTRUCTION OF QUASI-CYCLIC ALTERNANT CODES AND THEIR APPLICATION IN CODE-BASED CRYPTOGRAPHY

A. A. Kuninets*, E. S. Malygina**

*Immanuel Kant Baltic Federal University, Kaliningrad, Russia
**HSE, Moscow, Russia

The paper presents an overview of quasi-cyclic alternant codes and their structural analysis regarding the classification of automorphisms. We also have detailed methods for recovering the structure of a given code. The attractiveness of the family of considered codes lies in their 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 subfield subcodes of quasi-cyclic algebraic-geometric codes associated with an arbitrary curve with a known

[1]Работа первого автора выполнена за счет гранта Российского научного фонда №22-41-0441 (https://rscf.ru/project/22-41-04411/); работа второго автора подготовлена в рамках Программы фундаментальных исследований НИУ ВШЭ.

group of automorphisms. However, 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.*

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 (например, криптосистема RSA) и дискретного логарифмирования (например, протокол Диффи — Хеллмана), что делает их неустойчивыми к атакам с использованием квантового компьютера. Однако в последние несколько лет успешно развивается направление постквантовой криптографии, к которому относятся алгоритмы, основывающиеся на сложности задач, для которых не существует полиномиального алгоритма решения, даже на квантовом компьютере.

В конце 2016 г. Национальный институт стандартов и технологий США (The National Institute of Standards and Technology — NIST) объявил о начале конкурса по стандартизации постквантовых алгоритмов. Одним из перспективных направлений в этой области стала криптография на кодах, исправляющих ошибки.

В данной работе рассмотрен принцип построения квазициклических кодов Гоппы. Далее описано редуцирование ключевой безопасности квазициклических кодов Гоппы к ключевой безопасности инвариантного кода с меньшими параметрами [1]; под термином «ключевая безопасность» понимается стойкость кода относительно атак, направленных на восстановление секретного ключа криптосистемы. Детализирована и снабжена примерами структурная атака на рассматриваемый квазициклический код.

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].

1.1. АГ-коды, ассоциированные с проективной прямой

Введём понятия обобщённого кода Рида — Соломона (GRS-кода) и алгеброгеометрического кода (АГ-кода), ассоциированного с проективной прямой, а также его подполевого подкода, и покажем возможность построения кода Гоппы с помощью алгеброгеометрического подхода. В заключение рассмотрим связь между многочленом Гоппы и дивизорами, используемыми при построении кода в алгеброгеометрическом случае.

Определение 1. Зададим вектор $\mathbf{x} = (x_1, x_2, \ldots, x_n) \in \mathbb{F}_{q^m}^n$, состоящий из n различных элементов, и вектор $\mathbf{y} = (y_1, y_2, \ldots, y_n) \in (\mathbb{F}_{q^m}^*)^n$, состоящий из n ненулевых элементов. Пусть $k \in \mathbb{Z}^+$. *Обобщённый код Рида — Соломона* (GRS-код) размерности k задаётся следующим образом:

$$\mathbf{GRS}_k(\mathbf{x}, \mathbf{y}) = \{(y_1 f(x_1), \ldots, y_n f(x_n)) : f \in \mathbb{F}_{q^m}[z] \text{ и } \deg(f) < k\}.$$

Вектор $\mathbf{x}$ называется *носителем*, а вектор $\mathbf{y}$ — *множителем* кода $\mathbf{GRS}_k(\mathbf{x}, \mathbf{y})$.

Отметим, что любой рациональный АГ-код является обобщённым кодом Рида — Соломона. Доказательство этого факта можно найти в [4]. Покажем, что аналогичную конструкцию кода можно получить, используя алгеброгеометрический подход.

Пусть $\mathbf{P}^1$ — это проективная прямая над полем $\mathbb{F}_{q^m}$, тогда $\mathbb{F}_{q^m}(\mathbf{P}^1) = \mathbb{F}_{q^m}(x)$ — функциональное поле проективной прямой $y = x$, где $\mathbb{F}_{q^m}(x)$ — *поле рациональных функций* над $\mathbb{F}_{q^m}$. Полюс функции x является бесконечно удалённой точкой прямой $\mathbf{P}^1$, которую будем обозначать P_∞. Рациональные точки, то есть точки степени один проективной прямой, имеют вид $P_i = (x_i : 1)$.

Обозначим $D = P_1 + \ldots + P_n$ — дивизор, являющийся формальной суммой попарно различных рациональных точек проективной прямой. Носителем дивизора называют множество точек, входящих в него: $\mathrm{supp}(D) = \{P_1, \ldots, P_n\}$. Через G обозначим дивизор, носитель которого не пересекается с носителем дивизора D. АГ-код $\mathcal{C}$, ассоциированный с проективной прямой $\mathbf{P}^1$, будем обозначать

$$\mathcal{C} = \mathcal{C}_{\mathscr{L}}(D, G).$$

Чтобы провести аналогию с классическим определением GRS-кодов, построим порождающую матрицу кода $\mathcal{C}$. Будем считать, что $G \sim \deg(G)P_\infty$. Это означает, что $G + (h) = \deg(G)P_\infty$, где (h) — главный дивизор некоторой функции $h \in \mathbb{F}_{q^m}(x)$. Более того, для любого $s \in \mathbb{N}$ пространство Римана — Роха, ассоциированное с дивизором sP_∞, имеет вид

$$\mathscr{L}(sP_\infty) = \{x^i : i \in \{0, \ldots, s\}\}.$$

Теперь запишем пространство Римана — Роха, ассоциированное с дивизором G:

$$\mathscr{L}(G) = \{hx^i : i \in \{0, \ldots, s\}\}.$$

Согласно [4, следствие 2.2.3], размерность кода, ассоциированного с проективной прямой, равна $k = \deg(G) + 1$. Пусть $x = (x(P_1), \ldots, x(P_n)) = (x_1, \ldots, x_n)$ и $y = (h(P_1), \ldots, h(P_n))$, тогда матрица

$$\mathbf{V}(\mathbf{x}, \mathbf{y}) = \begin{pmatrix} y_1 & \ldots & y_n \\ y_1x_1 & \ldots & y_nx_n \\ y_1x_1^2 & \ldots & y_nx_n^2 \\ \vdots & & \vdots \\ y_1x_1^{k-1} & \ldots & y_nx_n^{k-1} \end{pmatrix} \tag{1}$$

является порождающей матрицей кода $\mathcal{C}$.

Определение 2. Пусть $\mathbf{x} \in \mathbb{F}_{q^m}^n$ — это носитель, а $\mathbf{y} \in (\mathbb{F}_{q^m}^*)^n$ — множитель кода $\mathbf{GRS}_r(\mathbf{x}, \mathbf{y})$, тогда *альтернантный код* над $\mathbb{F}_q$ задаётся следующим образом:

$$\mathcal{A}_{r,q}(\mathbf{x}, \mathbf{y}) = \mathbf{GRS}_r(\mathbf{x}, \mathbf{y})^\perp \cap \mathbb{F}_q^n,$$

где $\mathbf{GRS}_r(\mathbf{x}, \mathbf{y})^\perp$ — дуальный код к коду $\mathbf{GRS}_r(\mathbf{x}, \mathbf{y})$ и r — размерность кода $\mathbf{GRS}_r(\mathbf{x}, \mathbf{y})$.

Так как по построению альтернантные коды являются подполевыми подкодами GRS-кодов и соответственно являются подполевыми подкодами АГ-кодов, далее будем использовать алгеброгеометрическую нотацию:

$$\mathcal{A}_{r,q}(D, G) = \mathcal{C}_{\mathscr{L}}(D, G)^\perp \cap \mathbb{F}_q^n.$$

Определение 3. Пусть $\mathbf{x} \in \mathbb{F}_{q^m}^n$ — вектор с попарно различными координатами и $\Gamma \in \mathbb{F}_{q^m}[z]$ — многочлен, такой, что $\Gamma(x_i) \neq 0$ для любых $i \in \{0, \ldots, n-1\}$. *Классический код Гоппы* $\mathscr{G}_q(\mathrm{x}, \Gamma)$, ассоциированный с Γ и порождённый $\mathbf{x}$, определяется следующим образом:

$$\mathscr{G}_q(\mathbf{x}, \Gamma) = \mathcal{A}_{r,q}\left(\mathbf{x}, \Gamma(\mathbf{x})^{-1}\right).$$

Здесь $r = \deg \Gamma$. Многочлен Γ называют *многочленом Гоппы*, а m — *степенью расширения кода Гоппы.*

Покажем явный вид дивизоров и алгеброгеометрический способ построения классического кода Гоппы.

Теорема 1. Пусть $D = P_1 + \ldots + P_n$ — дивизор, носителем которого являются n попарно различных рациональных точек проективной прямой $\mathbf{P}^1$ над $\mathbb{F}_{q^m}$; $G = G_0 - P_\infty$ — дивизор функционального поля $\mathbb{F}_{q^m}(\mathbf{P}^1)$, носитель которого не пересекается с носителем дивизора D, где $G_0 = (\Gamma)_0$ — дивизор нулей многочлена $\Gamma \in \mathbb{F}_q(\mathbf{P}^1)$; код $\mathcal{C}_{\mathscr{L}}(D, G)$ является АГ-кодом, определённым над $\mathbb{F}_{q^m}$. Тогда классический код Гоппы представим в следующей алгеброгеометрической форме:

$$\mathscr{G}_q(\mathbf{x}, \Gamma) = \mathcal{C}_{\mathscr{L}}(D, G_0 - P_\infty)^\perp \cap \mathbb{F}_q^n = \mathcal{C}_{\mathscr{L}}(D, A - G_0) \cap \mathbb{F}_q^n,$$

где $\mathcal{C}_{\mathscr{L}}(D, G_0 - P_\infty)^\perp$ — дуальный к исходному коду; $A = (h'(z)) + (n-1)P_\infty$; $h(z) = \prod\limits_{x_i \in \mathbf{x}} (z - x_i)$.

Доказательство. Пусть $\mathbf{x} = \{x(P_1), \ldots, x(P_n)\} = \{x_1, \ldots, x_n\}$ и $\Gamma(z) \in \mathbb{F}_q(\mathbf{P}^1)$, где $P_i = (x_i : 1) \in \mathbf{P}^1$ — попарно различные точки; $\deg(\Gamma(z)) = r$, $1 \leqslant r \leqslant n-1$; $\Gamma(x_i) \neq 0$ для всех $x_i \in \mathbf{x}$. Рассмотрим код с порождающей матрицей

$$V = \begin{pmatrix} \Gamma(x_1)^{-1} & \Gamma(x_2)^{-1} & \ldots & \Gamma(x_n)^{-1} \\ x_1\Gamma(x_1)^{-1} & x_2\Gamma(x_2)^{-1} & \ldots & x_n\Gamma(x_n)^{-1} \\ \vdots & \vdots & & \vdots \\ x_1^{r-1}\Gamma(x_1)^{-1} & x_2^{r-1}\Gamma(x_2)^{-1} & \ldots & x_n^{r-1}\Gamma(x_n)^{-1} \end{pmatrix}.$$

Нетрудно заметить, что вид данной матрицы полностью совпадает с видом матрицы (1), являющейся порождающей для GRS-кода. Очевидно, что код с такой порождающей матрицей удовлетворяет определению 1, то есть является $\mathbf{GRS}_r(\mathbf{x}, \mathbf{y})$-кодом, где $\mathbf{y} = \left(\Gamma(x_i)^{-1} : x_i \in \mathbf{x}\right)$.

Докажем, что

$$\mathbf{GRS}_r(\mathbf{x}, \mathbf{y}) = \mathcal{C}_{\mathscr{L}}(D, G) = \mathcal{C}_{\mathscr{L}}(D, G_0 - P_\infty). \tag{2}$$

Для этого достаточно показать, что $z^j \cdot \Gamma(z)^{-1} \in \mathscr{L}(G_0 - P_\infty)$ для всех $j \in \{0, \ldots, r-1\}$. Рассмотрим дивизор нулей и дивизор полюсов функции $z^j \cdot \Gamma(z)^{-1}$, затем найдём её главный дивизор:

$$\begin{aligned} &(z^j \cdot \Gamma(z)^{-1})_0 = jP_0 + rP_\infty - jP_\infty, \text{ где } P_0 \text{ — нуль функции } z; \\ &(z^j \cdot \Gamma(z)^{-1})_\infty = G_0; \\ &(z^j \cdot \Gamma(z)^{-1}) = j(P_0 - P_\infty) - (G_0 - rP_\infty). \end{aligned}$$

Таким образом,

$$j(P_0 - P_\infty) - (G_0 - rP_\infty) = -G_0 + jP_0 + (r-j)P_\infty \geqslant -G_0 + P_\infty.$$

Так как $\dim(\mathscr{L}(G_0 - P_\infty)) = r$, то базис пространства Римана — Роха $\mathscr{L}(G_0 - P_\infty)$ имеет вид $\{z^j \cdot \Gamma(z)^{-1} : j = 0, \ldots, r-1\}$. Равенство (2) доказано.

Теперь докажем равенство кодов

$$\mathcal{C}_{\mathscr{L}}(D, G_0 - P_\infty)^\perp = \mathcal{C}_{\mathscr{L}}(D, A - G_0).$$

Для этого потребуется ввести понятие вычета дифференциала $\omega = f\delta t_P$ [4, 2] в точке P, где $f \in \mathbb{F}_q(\mathcal{X})$ и t_P — локальный параметр. Разложим функцию f в ряд Лорана по степеням t_P:

$$f = \sum_{i=s}^{\infty} a_i t_P^i.$$

Здесь $s \in \mathbb{Z}$. *Вычетом дифференциала ω в точке P* называется коэффициент a_{-1} в представленном разложении; обозначается $\mathrm{Res}_\omega(P)$.

Лемма 1 [4, Лемма 2.3.6]. Пусть $\mathbf{P}^1$ — проективная прямая над полем $\mathbb{F}_{q^m}$; $\mathbb{F}_{q^m}(\mathbf{P}^1) = \mathbb{F}_{q^m}(z)$ — рациональное функциональное поле; $\alpha = \{\alpha_1, \ldots, \alpha_n\}$ — различные элементы поля $\mathbb{F}_{q^m}$; $P_i \in \mathbf{P}^1$ — нули функций $z - \alpha_i$; $h(z) = \prod\limits_{\alpha_i \in \alpha} (z - \alpha_i)$. Пусть $\zeta \in \mathbb{F}_{q^m}(\mathbf{P}^1)$, такой, что $\zeta(P_i) = 1$ для любой P_i. Тогда существует дифференциал Вейля ω:

$$v_{P_i}(\omega) = -1,\ \mathrm{Res}_\omega(P_i) = 1,\ i = 1, \ldots, n,$$
$$(\omega) = (\zeta) + (h'(z)) - (h(z)) - 2P_\infty,$$

где $v_{P_i}(\omega)$ — нормирование ω в точке P_i [4, 2].

Предложение 1 [4, Предложение 2.2.10]. Пусть $D = P_1 + \ldots + P_n$ — дивизор, носителем которого являются n попарно различных рациональных точек проективной прямой; G — дивизор функционального поля $\mathbb{F}_{q^m}(\mathbf{P}^1)$; η — дифференциал Вейля, такой, что $v_{P_i}(\eta) = -1$ и $\mathrm{Res}_\eta(P_i) = 1$ для всех $i = 1, \ldots, n$. Тогда

$$\mathcal{C}_{\mathscr{L}}(D, G)^\perp = \mathcal{C}_{\mathscr{L}}(D, D - G + (\eta)),\ \text{где } D = \sum_{i=1}^{n} P_i.$$

Теперь мы можем явно задать вид дивизоров дуального кода, используя предложение 1:

$$\mathcal{C}_{\mathscr{L}}(D, G_0 - P_\infty)^\perp = \mathcal{C}_{\mathscr{L}}(D, D - (G_0 - P_\infty) + (h'(z)) - (h(z)) - 2P_\infty). \tag{3}$$

Здесь $(h(z)) = (h(z))_0 - (h(z))_\infty = \sum\limits_{i=1}^{n} P_i - nP_\infty = D - nP_\infty$. Таким образом, равенство (3) принимает вид

$$\mathcal{C}_{\mathscr{L}}(D, G_0 - P_\infty)^\perp = \mathcal{C}_{\mathscr{L}}(D, -G_0 + P_\infty + (h'(z)) + nP_\infty - 2P_\infty) = \mathcal{C}_{\mathscr{L}}(D, A - G_0),$$

следовательно, выполняется равенство и для исходного кода Гоппы:

$$\mathscr{G}_q(\mathbf{x}, \Gamma) = \mathcal{C}_{\mathscr{L}}(D, G_0 - P_\infty)^\perp \cap \mathbb{F}_q^n = \mathcal{C}_{\mathscr{L}}(D, A - G_0) \cap \mathbb{F}_q^n.$$

Теорема 1 доказана. ■

1.2. Группа автоморфизмов альтернантных кодов

Пусть $\mathfrak{S}_n$ — группа перестановок множества $\{1, \ldots, n\}$. Определим группу автоморфизмов кода.

Определение 4. Пусть $\mathcal{C}$ — линейный код длины n над полем $\mathbb{F}_q$; $\sigma \in \mathfrak{S}_n$ — перестановка, действующая на кодовое слово как $\sigma(\mathbf{c}) = \big(c_{\sigma(1)}, \ldots, c_{\sigma(n)}\big)$. *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, сначала необходимо исследовать GRS-коды и их автоморфизмы.

Дадим определение *проективной линейной группы*:

$$\mathrm{PGL}_2(\mathbb{F}_{q^m}) = \begin{cases} \mathbf{P}^1 \to \mathbf{P}^1, \\ (x : y) \mapsto (ax + by : cx + dy), \end{cases} \qquad a, b, c, d \in \mathbb{F}_{q^m},\ ad - bc \neq 0.$$

В [5] рассмотрено алгеброгеометрическое построение GRS-кодов, а также доказано, что вся группа автоморфизмов кода индуцирована действием проективной линейной группы $\mathrm{PGL}_2(\mathbb{F}_{q^m})$, являющейся группой автоморфизмов проективной прямой $\mathbf{P}^1$.

Элементы $\mathrm{PGL}_2(\mathbb{F}_{q^m})$ имеют также матричное представление, а именно: любой элемент $\sigma \in \mathrm{PGL}_2(\mathbb{F}_{q^m})$ можно представить как

$$\sigma = \begin{pmatrix} a & b \\ c & d \end{pmatrix},\ ad - bc \neq 0.$$

Определение 5. 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 $(\mathrm{supp}(G) \cup \mathrm{supp}(G')) \cap \mathrm{supp}(D) = \varnothing$. Определим отношение эквивалентности дивизоров относительно дивизора D следующим образом:

$$G \sim_D G' \Leftrightarrow \exists f \in \mathbb{F}_{q^m}(\mathbf{P}^1)\big(f \neq 0 \ \ \& \ \ G - G' = (f) \ \ \& \ \ \forall P \in \mathrm{supp}(D)\, f(P) = 1\big).$$

Лемма 2 [5, Лемма 2.1]. Пусть $\mathrm{supp}(D) \subseteq \mathbf{P}^1$ и G, G' — два дивизора $\mathbf{P}^1$, такие, что $(\mathrm{supp}(G) \cup \mathrm{supp}(G')) \cap \mathrm{supp}(D) = \varnothing$. Если $G \sim_D G'$, то $\mathcal{C}_{\mathscr{L}}(D, G) = \mathcal{C}_{\mathscr{L}}(D, G')$.

Следующая теорема определяет всевозможные автоморфизмы АГ-кода, ассоциированного с дивизором G.

Теорема 2 [5, 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

$$\mathrm{Aut}(\mathcal{C}) = \left\{\sigma \in \mathrm{Aut}\left(\mathbf{P}^1\right) : \sigma(D) = D \ \ \& \ \ \sigma(G) \sim_D G\right\}.$$

Теперь перейдём непосредственно к построению GRS-кодов с помощью автоморфизма. Пусть $\sigma \in \mathrm{PGL}_2\left(\mathbb{F}_{q^m}\right)$ — автоморфизм, действующий на носитель дивизора D и дивизор $G \in \mathrm{Div}\left(\mathbf{P}^1\right)$. Тогда σ индуцирует автоморфизм кода $\mathcal{C} = \mathcal{C}_{\mathscr{L}}(D, G)$:

$$\tilde{\sigma} : \begin{cases} \mathcal{C} \longrightarrow \mathcal{C}, \\ \big(f(P_1), \ldots, f(P_n)\big) \longmapsto \big(f(\sigma(P_1)), \ldots, f(\sigma(P_n))\big). \end{cases}$$

Поскольку альтернантные коды являются подполевыми подкодами GRS-кодов, то их группа автоморфизмов включает в себя группу автоморфизмов исходного GRS-кода.

Замечание 1. Пусть $\mathcal{A}_{r,q}(D, G)$ — альтернантный код над $\mathbb{F}_q$ и $\sigma \in \mathrm{Aut}\left(C_{\mathscr{L}}(D, G)\right)$, тогда $\sigma \in \mathrm{Aut}(\mathcal{A}_{r,q}(D, G))$.

2. Квазициклические альтернантные коды

2.1. Квазициклические коды

Пусть $\mathbb{F}$ — конечное поле, ℓ — положительное целое.

Определение 6. Определим циклический и квазициклический сдвиги σ_ℓ и σ:

$$\sigma_\ell\colon \begin{cases} \mathbb{F}^\ell \to \mathbb{F}^\ell, \\ (x_0, x_1, \ldots, x_{\ell-1}) \mapsto (x_{\ell-1}, x_0, \ldots, x_{\ell-2}), \end{cases} \qquad \sigma\colon \begin{cases} \mathbb{F}^n \to \mathbb{F}^n, \\ (\mathbf{b}_1 \| \ldots \| \mathbf{b}_{n/\ell}) \mapsto (\sigma_\ell(\mathbf{b}_1) \| \ldots \| \sigma_\ell(\mathbf{b}_{n/\ell})). \end{cases}$$

Пусть n — целое и $\ell | n$. Тогда σ называется ℓ-квазициклическим сдвигом, полученным поблочным применением σ_ℓ, где $\mathbf{b}_i$ — блоки длины ℓ, $i = 1, \ldots, n/\ell$.

Определение 7. 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 ℓ-квазициклического сдвига. При этом ℓ называется *порядком* квазицикличности кода.

Определение 8. Матрица $\mathbf{M}$ называется *ℓ-блочно-циркулянтной*, если она состоит из циркулянтных матриц $\mathbf{M}_i$ порядка ℓ:

$$\mathbf{M} = \left(\begin{array}{c|c|c} & & \\ \hline \ldots & \mathbf{M}_i & \ldots \\ \hline & & \end{array}\right), \quad \text{где} \quad \mathbf{M_i} = \begin{pmatrix} a_0 & a_1 & \ldots & a_{\ell-1} \\ a_{\ell-1} & a_0 & \ldots & a_{\ell-2} \\ \vdots & \ddots & \ddots & \vdots \\ a_1 & \ldots & a_{\ell-1} & a_0 \end{pmatrix}.$$

Матрица такого типа может быть представлена первыми строками каждого блока размера ℓ. Таким образом, можно восстановить ℓ-блочно-циркулянтную матрицу $\mathbf{M}$ из k строк, зная её строки с индексами $1, \ell+1, \ldots, k-\ell+1$.

Замечание 2. Код $\mathcal{C}$, имеющий ℓ-блочно-циркулянтную порождающую матрицу, является ℓ-QC-кодом. Отметим, что QC-код $\mathcal{C}$ размерности k не обязан иметь ℓ-блочно-циркулянтную порождающую матрицу, однако существует ℓ-блочно-циркулянтная матрица $\mathbf{G}$, состоящая из $k' \geqslant k$ строк, которая порождает данный код $\mathcal{C}$.

Для оптимального уменьшения размера открытого ключа криптосистемы Мак-Элиса можно рассматривать ℓ-QC-коды $\mathcal{C}$ с параметрами $[n, k]$, имеющие порождающую матрицу в систематическом виде

$$\mathbf{G} = \left(\mathbf{I}_k \,|\, \mathbf{M}\right),$$

где $\mathbf{I}_k$ — единичная матрица порядка k; $\mathbf{M}$ — ℓ-блочно-циркулянтная матрица. В этом случае будем называть код $\mathcal{C}$ *систематическим квазициклическим.*

Замечание 3. Для выполнения предыдущего условия размерность ℓ-QC-кода должна быть кратна ℓ.

Определение 9. Для матрицы $\mathbf{G}$ в систематической форме определим $\rho(\mathbf{G})$ как матрицу, полученную путём удаления всех строк каждого блока матрицы $\mathbf{M}$, кроме первой, т.е. $\rho(\mathbf{G})$ получается путём записывания строк из $\mathbf{M}$ с индексами 1, $\ell+1$, $2\ell+1$, …, $k-\ell+1$. Отсюда имеем следующее соотношение:

$$\text{Число строк матрицы } \mathbf{G} = \ell \cdot (\text{Число строк матрицы } \rho(\mathbf{G})).$$

Определение 10. Пусть $\mathcal{C} \subseteq \mathbb{F}^n$ — ℓ-QC-код. *Инвариантный код* определяется следующим образом:

$$\mathcal{C}^\sigma = \{c \in \mathcal{C} : \sigma(c) = c\}.$$

Так как инвариантный код имеет повторяющиеся элементы, далее будем использовать *проколотый инвариантный код*, который определяется следующим образом:

$$\overline{\mathcal{C}}^{\sigma} = \mathrm{Punct}_{\mathcal{I}_\ell}(\mathcal{C}^{\sigma}),$$

где $\mathcal{I}_\ell = \{1, \ldots, n\} \setminus \{1, \ell+1, \ldots, n-\ell+1\}$. Пусть $\sigma_{\mathcal{C}}$ — ℓ-QC-сдвиг σ, суженный на код $\mathcal{C}$, тогда можно записать $\overline{\mathcal{C}}^{\sigma} = \mathrm{Punct}_{\mathcal{I}_\ell}(\ker(\sigma_{\mathcal{C}} - \mathrm{id}))$.

Далее под инвариантным кодом будем иметь в виду и инвариантный, и проколотый инвариантный код, однако обозначения останутся разными.

Замечание 4. Инвариантность коммутирует с операцией вычисления подполевого подкода. Действительно, если $\mathcal{C}$ — ℓ-QC-код над $\mathbb{F}_{q^m}$, то

$$(\mathcal{C} \cap \mathbb{F}_q^n)^{\sigma} = \{c \in \mathcal{C} : c \in \mathbb{F}_q^n \ \ \& \ \ \sigma(c) = c\} = \mathcal{C}^{\sigma} \cap \mathbb{F}_q^n.$$

2.2. Построение квазициклических альтернантных кодов

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:

$$\mathrm{Orb}_\sigma(P) = \left\{\sigma^i(P) : i \in \{0, \ldots, \ell-1\}\right\},$$

обозначим

$$D = \sum_{i=1}^{n/\ell} \sum_{P \in \mathrm{Orb}_\sigma(P_i)} P, \quad \mathrm{supp}(D) = \coprod_{i=1}^{n/\ell} \mathrm{Orb}_\sigma(P_i), \tag{4}$$

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. Определим дивизор

$$G = \sum_{i=1}^{s} t_i \sum_{Q \in \mathrm{Orb}(Q_i)} Q, \tag{5}$$

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 $\deg(G) = \sum\limits_{i=1}^{s} t_i \ell \deg(Q_i)$.

Как показано в п. 1.2, автоморфизм σ индуцирует автоморфизм кода $\mathcal{C}_{\mathscr{L}}(D, G)$. Для краткости и автоморфизм проективной прямой $\mathbf{P}^1$, и индуцированный автоморфизм будем обозначать через σ. Тогда, согласно лемме 1, σ также является автоморфизмом кода $\mathcal{A}_{r,q}(D, G) = \mathcal{C}_{\mathscr{L}}(D, G)^{\perp} \cap \mathbb{F}_q^n$. Таким образом, альтернантный код, полученный описанным способом, является квазициклическим при соответствующем упорядочивании точек.

3. Структурный анализ инвариантных кодов

Покажем, что инвариантный код для QC-альтернантного кода также является альтернантным кодом, но с меньшими параметрами. Так как инвариантность коммутирует с операцией взятия подполевого подкода, для анализа структуры инвариантных кодов Гоппы достаточно рассмотреть инвариантный код GRS-кода. Данные утверждения в дальнейшем позволят описать процесс восстановления параметров QC-альтернантного кода Гоппы, используя инвариантный проколотый код.

Для упрощения рассуждений будем предполагать, что G строится с использованием одной рациональной точки Q, т.е. $G = t \sum\limits_{R \in \mathrm{Orb}_\sigma(Q)} R$. В случае использования нескольких точек также возможно восстановить секретные параметры, однако алгоритмы восстановления принимают более громоздкий вид, поэтому в данной работе они опущены.

Зададим

$$\sigma^j(P_i) = (\alpha_{i\ell+j} : \beta_{i\ell+j}) \text{ для } i \in \{0, \ldots, n/\ell - 1\},\ j \in \{0, \ldots, \ell - 1\},$$
$$\sigma^j(Q) = (\gamma_j : \delta_j) \text{ для } j \in \{0, \ldots, \ell - 1\}.$$

Лемма 3. Пусть $G = t \sum\limits_{R \in \mathrm{Orb}_\sigma(Q)} R$, тогда пространство Римана — Роха, ассоциированное с дивизором G, имеет следующий вид:

$$\mathscr{L}(G) = \left\{ F(X,Y) \Big/ \prod_{j=0}^{\ell-1} (\delta_j X - \gamma_j Y)^t \colon F \in \mathbb{F}_{q^m}[X,Y] \text{ — однородный многочлен степени } t\ell \right\}.$$

Доказательство. Пусть $\mathbf{P}^1$ — проективная прямая над полем $\mathbb{F}_{q^m}$, тогда $\mathbb{F}_{q^m}(\mathbf{P}^1) = \mathbb{F}_{q^m}(x)$ — рациональное функциональное поле. Исходя из определения проективного многообразия, базис пространства Римана — Роха, в случае проективной прямой, имеет следующий вид:

$$\mathscr{L}(\mathbf{P}^1) = \left\{ \frac{f}{g} : f, g \in \mathbb{F}_{q^m}[X,Y] \text{ — однородные многочлены одинаковой степени}, g \neq 0 \right\}.$$

Рассмотрим дивизор $G = t \sum\limits_{R \in \mathrm{Orb}_\sigma(Q)} R$ и докажем, что

$$z = F(X,Y) \Big/ \prod_{j=0}^{\ell-1} (\delta_j X - \gamma_j Y)^t \in \mathscr{L}(G),$$

где $F \in \mathbb{F}_{q^m}[X,Y]$ — однородный многочлен степени $t\ell$. Пусть $\mathcal{Z}(f)$ — множество нулей функции f, тогда соответствующие дивизоры нулей и полюсов, а также главный дивизор функции z имеют следующий вид:

$$(z)_0 = \sum_{P \in \mathcal{Z}(F(X,Y)) \setminus P_\infty} v_P(F(X,Y))P + v_{P_\infty}(z) = \sum_{P \in \mathcal{Z}(F(X,Y)) \setminus P_\infty} v_P(F(X,Y))P,$$
$$(z)_\infty = \sum_{(\gamma_j : \delta_j) \in \mathrm{Orb}_\sigma(Q)} t(\gamma_j : \delta_j) = t \sum_{R \in \mathrm{Orb}_\sigma(Q)} R = G,$$
$$(z) = \sum_{P \in \mathcal{Z}(F(X,Y)) \setminus P_\infty} v_P(F(X,Y))P - G \geqslant -G.$$

Лемма 3 доказана. ■

Следующая лемма определяет понятие инвариантной функции. Так как мы рассматриваем QC-альтернантные коды с точки зрения АГ-кодов, необходимо понимать, какие функции из пространства Римана — Роха являются инвариантными относительно действия автоморфизма.

Лемма 4 [1, Лемма 3.3]. Пусть $\mathcal{C} = C_{\mathscr{L}}(D,G)$ и $\sigma \in \mathrm{Aut}(\mathcal{C})$. Если $c = (f(P_1), \ldots, f(P_n)) \in \mathcal{C}$ такое, что $\sigma(c) = c$, то f является σ-инвариантной функцией, т.е. $f \circ \sigma = f$.

Теорема 3 [1, Теорема 3.5]. Пусть $C_{\mathscr{L}}(D,G) \subseteq \mathbb{F}_{q^m}^n$ — АГ-код длины n, размерности k, с действующим на него автоморфизмом $\sigma \in \mathrm{PGL}_2(\mathbb{F}_{q^m})$ порядка ℓ, где $\ell \mid n$. Пусть, как и ранее, определены D и G. Тогда инвариантный код $\overline{C_{\mathscr{L}}(D,G)}^{\sigma}$ является АГ-кодом длины n/ℓ и размерности $[k/\ell]$.

Следствие 1. Пусть $\mathcal{A}_{r,q}(D,G) = C_{\mathscr{L}}(D,G) \cap \mathbb{F}_q^n$ — альтернантный код длины n, порядка r, с действующим на него автоморфизмом $\sigma \in \mathrm{PGL}_2(\mathbb{F}_{q^m})$ порядка ℓ, где $\ell \mid n$. Пусть D и G определены, как в (4) и (5). Тогда инвариантный код $\overline{\mathcal{A}_{\lfloor r/\ell \rfloor,q}(D,G)}^{\sigma}$ является альтернантным кодом длины n/l и порядка $[r/\ell]$.

Далее изучим действие автоморфизма $\sigma \in \mathrm{PGL}_2(\mathbb{F}_{q^m})$ на пространство Римана — Роха $\mathscr{L}(G)$. Рассмотрим $\sigma \in \mathrm{PGL}_2(\mathbb{F}_{q^m})$ и $\mathrm{ord}(\sigma) = \ell$, а также дивизоры D и G, определённые ранее. Автоморфизм $\sigma \in \mathrm{PGL}_2(\mathbb{F}_{q^m})$ можно представить 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 $M = PNP^{-1}$. 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 $\mathbb{F}_{q^m}$);
2) $M \sim \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix}$, где $b \in \mathbb{F}_{q^m} \setminus \{0\}$ (σ — тригонализируемый в $\mathbb{F}_{q^m}$);
3) $M \sim \begin{pmatrix} \xi & 0 \\ 0 & \xi^{q^m} \end{pmatrix}$, где $\xi \in \mathbb{F}_{q^{2m}}$ (σ — диагонализируемый в $\mathbb{F}_{q^{2m}}$).

Возможность диагонализации или тригонализации зависит от собственных векторов матрицы. Поясним подробнее, когда можно привести матрицу M к одному из вышеописанных видов.

Теорема 4 [6, Теорема 2.2]. Пусть $M \in M_n(\mathbb{F})$, тогда матрица M диагонализируема в поле $\mathbb{F}$ тогда и только тогда, когда сумма размерностей собственных подпространств в точности равна n, что верно тогда и только тогда, когда существует базис в $\mathbb{F}^n$, состоящий из собственных векторов M.

Далее рассмотрим матрицы над конечным полем $\mathbb{F}_{q^m}$. Любое конечное поле является алгебраически незамкнутым, следовательно, минимальный многочлен $\pi_M(T)$ не обязательно раскладывается на линейные множители, как и характеристический многочлен. В таком случае количество собственных значений у матрицы $M \in M_n(\mathbb{F}_{q^m})$ меньше n, а условия теоремы 4 не выполняются.

Заметим, что если характеристический многочлен имеет кратный корень, то в общем случае при размерности больше 2 данный факт не говорит о том, что матрицу нельзя диагонализировать. Однако, рассматривая $M \in M_2(\mathbb{F}_{q^m})$, можно утверждать, что размерность собственных подпространств может быть равна $0, 1$ или 2. В первом случае условия теоремы 4 не выполняются, второй случай говорит о том, что матрица обязательно диагонализируема над $\mathbb{F}_{q^m}$, а в третьем случае условия выполнимы, только если матрица M уже является диагональной.

Теорема 5 [7]. Пусть $M \in M_2(\mathbb{F}_{q^m})$ не является диагональной. Матрица M диагонализируема в $\mathbb{F}_{q^m}$ тогда и только тогда, когда размерности всех собственных подпространств матрицы M равны 1, то есть характеристический многочлен имеет два различных корня кратности 1, что эквивалентно наличию двух различных собственных значений матрицы M.

Если характеристический многочлен разложим на множители, но имеет кратные корни, то можно тригонализировать матрицу M. В противном случае M всегда можно

диагонализировать в поле $\mathbb{F}_{q^{2m}}$, построенном при помощи добавления корня характеристического многочлена матрицы M.

При использовании минимального многочлена $\pi_M(T)$ матрицы M эти рассуждения можно представить в виде следующей теоремы:

Теорема 6 [7]. Пусть $M \in M_2(\mathbb{F}_{q^m})$, $\pi_M(T)$ — минимальный многочлен матрицы M. Тогда:

1) матрица M диагонализируема в $\mathbb{F}_{q^m} \iff \pi_M(T)$ раскладывается на различные линейные множители в $\mathbb{F}_{q^m}$;
2) матрица M тригонализируема в $\mathbb{F}_{q^m} \iff \pi_M(T)$ разложим в $\mathbb{F}_{q^m}$ на линейные множители, но имеет кратные корни;
3) матрица M диагонализируема в $\mathbb{F}_{q^{2m}} \iff \pi_M(T)$ сепарабельный.

Лемма 5 [1, Лемма 3.4]. Пусть $\mathcal{C} = \mathcal{C}_{\mathscr{L}}(D, G)$ — АГ-код, такой, что $\sigma(\mathcal{C}) = \mathcal{C}$, и $\rho \in \mathrm{PGL}_2(\mathbb{F}_{q^m})$. Тогда $\sigma' = \rho \circ \sigma \circ \rho^{-1}$ индуцирует тот же автоморфизм кода $\mathcal{C}$, что и σ.

Лемма 5 показывает, что изучение GRS-кодов, инвариантных относительно индуцированного автоморфизма σ, сводится к одному из трёх случаев, описанных ранее. Далее рассмотрим инвариантные проколотые коды, для которых теорема 3 выполняется в каждом из этих случаев.

3.1. Случай, когда автоморфизм σ является диагонализируемым в $\mathbb{F}_{q^m}$

Следующее предложение позволяет получить структуру однородных многочленов, инвариантных относительно диагонализируемого автоморфизма σ.

Предложение 2 [1, Предложение 3.8]. Пусть $F \in \mathbb{F}_{q^m}[X, Y]$ — однородный многочлен степени $t\ell$, элемент $a \in \mathbb{F}_{q^m}$ имеет порядок ℓ. Если $F(aX, Y) = F(X, Y)$, то $F(X, Y) = R\left(X^\ell, Y^\ell\right)$, где $R \in \mathbb{F}_{q^m}[X, Y]$ является однородным многочленом степени t.

Исходя из вида инвариантных относительно диагонализируемого автоморфизма многочленов, следующее предложение позволяет показать справедливость теоремы 3 в данном случае.

Предложение 3 [1, Предложение 3.9]. Пусть $\mathcal{C} = \mathcal{C}_{\mathscr{L}}(D, G)$ — АГ-код с параметрами $[n, k]$ и

$$\sigma : \begin{cases} \mathbf{P}^1 \to \mathbf{P}^1, \\ (x : y) \mapsto (ax : y). \end{cases}$$

Определим $\tilde{D} = \sum \tilde{P}_i$, где $\tilde{P}_i \in \left\{\left(\alpha_i^\ell : \beta_i^\ell\right) : i \in \{1, \dots n\}\right\} = \mathrm{supp}(\tilde{D})$, и $\tilde{G} = t\left((-1)^{\ell-1} a^{\ell(\ell-1)/2} (\gamma_0/\delta_0)^\ell : 1\right)$ или $\tilde{G} = tP_\infty$. Тогда справедливо $\overline{\mathcal{C}}^\sigma = \mathcal{C}_{\mathscr{L}}(\tilde{D}, \tilde{G})$, а также $|\mathrm{supp}(\tilde{D})| = n/\ell$ и $\deg(\tilde{G}) = \deg(G)/\ell$.

Замечание 5. Инвариантный проколотый код $\overline{\mathcal{C}}^\sigma$ в предложении 3 имеет параметры $[n/\ell, \lceil k/\ell \rceil]$.

Стоит отметить, что элемент $a \in \mathbb{F}_{q^m}$ является корнем из единицы степени ℓ и не известен злоумышленнику. Исходя из того, что параметр ℓ относительно мал, даже не владея информацией об элементе a, возможно восстановить параметры D, G исходного кода, перебрав всех кандидатов для данного элемента.

3.2. Случай, когда автоморфизм σ является тригонализируемым в $\mathbb{F}_{q^m}$

Аналогично предыдущему случаю, рассмотрим структуру однородных многочленов, инвариантных относительно заданного тригонализируемого автоморфизма σ. Заметим, что данный случай возможен только тогда, когда $\mathrm{ord}(\sigma) = \mathrm{char}(\mathbb{F}_q) = p$.

Предложение 4 [8, Предложение 4]. Пусть $F \in \mathbb{F}_{q^m}[X,Y]$, $\deg(F) \leqslant tp$ и $b \in \mathbb{F}_q^*$. Если $F(X+bY,Y) = F(X,Y)$, то $F(X,Y) = R(X^p - b^{p-1}XY^{p-1}, Y^p)$, где p — характеристика поля $\mathbb{F}_{q^m}$ и $R \in \mathbb{F}_{q^m}[X,Y]$ — однородный многочлен степени $\deg(R) \leqslant t$.

Исходя из вида инвариантных многочленов, можно сделать вывод о структуре инвариантного проколотого кода в случае тригонализируемого автоморфизма.

Предложение 5 [1, Предложение 3.11]. Пусть $\mathcal{C} = C_{\mathscr{L}}(D,G)$ — АГ-код и

$$\sigma : \begin{cases} \mathbf{P}^1 \to \mathbf{P}^1, \\ (x:y) \mapsto (x+by:y). \end{cases}$$

Определим $\tilde{D} = \sum \tilde{P}_i$, где $\tilde{P}_i \in \{(\alpha_i^p - b^{p-1}\alpha_i\beta_i^{p-1} : \beta_i^p) : i \in \{1,\dots n\}\} = \operatorname{supp}(\tilde{D})$ и $\tilde{G} = t\left((\gamma_0/\delta_0)^p - b^{p-1}(\gamma_0/\delta_0) : 1\right)$ или $\tilde{G} = P_\infty$. Тогда справедливо $\overline{\mathcal{C}}^\sigma = C_{\mathscr{L}}(\tilde{D},\tilde{G})$, а также $|\operatorname{supp}(\tilde{D})| = n/\ell$ и $\deg(\tilde{G}) = \deg(G)/\ell$.

Замечание 6. Инвариантный проколотый код $\overline{\mathcal{C}}^\sigma$ в данном случае также имеет параметры $[n/\ell, \lceil k/\ell \rceil]$.

3.3. Случай, когда автоморфизм σ является диагонализируемым в $\mathbb{F}_{q^{2m}} \setminus \mathbb{F}_{q^m}$

Изучим GRS-код, определённый над $\mathbb{F}_{q^m}$, и построенный с его помощью проколотый инвариантный код относительно индуцированного автоморфизма $\sigma = \rho \circ \sigma_d \circ \rho^{-1}$, где автоморфизм σ_d — диагональный в $\mathrm{GL}_2(\mathbb{F}_{q^{2m}})$ и $\rho \in \mathrm{PGL}_2(\mathbb{F}_{q^{2m}})$.

Для кода $\mathcal{C} = \mathcal{C}_{\mathscr{L}}(D,G)$ над $\mathbb{F}_{q^m}$ рассмотрим расширенный код $\tilde{\mathcal{C}} = \mathcal{C}_{\mathscr{L}}(D^\otimes, G^\otimes)$ над $\mathbb{F}_{q^{2m}}$, такой, что $\mathcal{C}$ является его подполевым подкодом, т. е. $\mathcal{C} = \tilde{\mathcal{C}} \cap \mathbb{F}_{q^m} = \tilde{\mathcal{C}}|_{\mathbb{F}_{q^m}}$. Тогда, во-первых, из леммы 5 следует, что $\overline{\tilde{\mathcal{C}}}^\sigma = \overline{\tilde{\mathcal{C}}}^{\sigma_d}$. Во-вторых, полагая, что $\mathrm{char}(\mathbb{F}_{q^{2m}}) \nmid \ell$, учтём следующие замечание и лемму:

Замечание 7. Характеристика p поля $\mathbb{F}_{q^m}$ не делит порядок ℓ автоморфизма σ.

Лемма 6 [1, Утверждение 3.1]. Пусть ℓ — положительное целое и $\mathcal{C}$ — ℓ-квазициклический код. Тогда

$$\phi_\ell(\mathcal{C}) \subseteq \overline{\mathcal{C}}^\sigma,$$

где ϕ_ℓ — функция свёртки, определённая следующим образом:

$$\phi_\ell : \begin{cases} \mathbb{F}^n \longrightarrow \mathbb{F}^{n/\ell}, \\ (x_1,\dots,x_n) \longmapsto \left(\sum\limits_{i=0}^{\ell-1} x_{\sigma^i(1)}, \sum\limits_{i=0}^{\ell-1} x_{\sigma^i(\ell+1)}, \dots, \sum\limits_{i=0}^{\ell-1} x_{\sigma^i(n-\ell+1)}\right). \end{cases}$$

Кроме того, если $\mathrm{char}(\mathbb{F}) \nmid \ell$, то $\phi_\ell(\mathcal{C}) = \overline{\mathcal{C}}^\sigma$.

Таким образом, имеем

$$\overline{\tilde{\mathcal{C}}}^\sigma = \phi_\ell(\{(f(P_1^\otimes),\dots,f(P_n^\otimes)) : f(P_i^\otimes) \in \mathbb{F}_{q^{2m}}\}) = \Big\{\Big(\sum_{i=0}^{\ell-1} f(P^\otimes_{\sigma^i(1)}), \dots, \sum_{i=0}^{\ell-1} f(P^\otimes_{\sigma^i(n-\ell+1)})\Big) :$$
$$f(P^\otimes_{\sigma^i(j)}) \in \mathbb{F}_{q^{2m}},\ i = 0,\dots,\ell-1,\ j = 1,\ell+1,\dots,n-\ell+1\Big\} = \phi_\ell(\tilde{\mathcal{C}}),$$

где $f \in \mathscr{L}(G^\otimes)$; $P_i^\otimes \in \operatorname{supp}(D^\otimes)$.

Если $\tilde{C}$ — GRS-код с параметрами $[n,k]$, то, согласно п. 3.1, $\overline{\tilde{\mathcal{C}}}^\sigma$ также является GRS-кодом с параметрами $\left[n/\ell, [k/\ell]\right]$.

Теперь изучим сужение автоморфизма σ на $\mathbb{F}_{q^m}$:

$$\sigma|_{\mathbb{F}_{q^m}} = (\rho \circ \sigma_d \circ \rho^{-1})|_{\mathbb{F}_{q^m}} = \rho|_{\mathbb{F}_{q^m}} \circ \sigma_d|_{\mathbb{F}_{q^m}} \circ \rho^{-1}|_{\mathbb{F}_{q^m}}.$$

Следовательно, $\sigma|_{\mathbb{F}_{q^m}} \in \mathrm{GL}_2(\mathbb{F}_{q^m}) \subset \mathrm{GL}_2(\mathbb{F}_{q^{2m}})$ и $\sigma_d|_{\mathbb{F}_{q^m}}$ — диагональный в $\mathrm{GL}_2(\mathbb{F}_{q^m})$. Рассмотрим диаграмму на рис. 1, где $\overline{\tilde{\mathcal{C}}^{\sigma}}|_{\mathbb{F}_{q^m}}$ — подполевой подкод кода $\overline{\tilde{\mathcal{C}}^{\sigma}}$. Покажем, что $\overline{\tilde{\mathcal{C}}^{\sigma}}|_{\mathbb{F}_{q^m}}$ является образом $\tilde{\mathcal{C}}|_{\mathbb{F}_{q^m}}$ при отображении $\phi_\ell|_{\mathbb{F}_{q^m}}$.

$$\begin{array}{ccc} \tilde{\mathcal{C}} & \xrightarrow{\phi_\ell} & \overline{\tilde{\mathcal{C}}^{\sigma}} \\ \downarrow & & \downarrow \\ \mathcal{C} = \tilde{\mathcal{C}}|_{\mathbb{F}_{q^m}} & \xrightarrow{\phi_\ell|_{\mathbb{F}_{q^m}}} & \overline{\tilde{\mathcal{C}}^{\sigma}}|_{\mathbb{F}_{q^m}} \end{array}$$

Рис. 1

Поскольку σ коммутирует с операцией построения подполевого подкода, учитывая замечание 4 и определение инвариантности, получаем $\overline{\tilde{\mathcal{C}}^{\sigma}}|_{\mathbb{F}_{q^m}} = \overline{\tilde{\mathcal{C}}|_{\mathbb{F}_{q^m}}}^{\sigma}$. Кроме того, $\phi_\ell|_{\mathbb{F}_{q^m}}(\tilde{\mathcal{C}}|_{\mathbb{F}_{q^m}}) = \overline{\tilde{\mathcal{C}}|_{\mathbb{F}_{q^m}}}^{\sigma}$.

Окончательно заключаем, что $\overline{\tilde{\mathcal{C}}|_{\mathbb{F}_{q^m}}}^{\sigma}$ является GRS-кодом, поскольку является подполевым подкодом GRS-кода. Если код $\tilde{\mathcal{C}}|_{\mathbb{F}_{q^m}}$ имеет параметры $[n, k']$, то в силу отображения

$$\phi_\ell|_{\mathbb{F}_{q^m}}(\tilde{\mathcal{C}}|_{\mathbb{F}_{q^m}}) = \phi_\ell(\{(f(\tilde{P}_1), \ldots, f(\tilde{P}_n)) : f(\tilde{P}_i) \in \mathbb{F}_{q^m}\}) =$$
$$= \left\{ \left(\sum_{i=0}^{\ell-1} f(\tilde{P}_{(\sigma|_{\mathbb{F}_{q^m}})^i(1)}), \ldots, \sum_{i=0}^{\ell-1} f(\tilde{P}_{(\sigma|_{\mathbb{F}_{q^m}})^i(n-\ell+1)}) \right) : f(\tilde{P}_{(\sigma|_{\mathbb{F}_{q^m}})^i(j)}) \in \mathbb{F}_{q^m} \right\},$$

где $i = 0, \ldots, \ell-1$, $j = 1, \ell+1, \ldots, n-\ell+1$, $f \in \mathscr{L}(\tilde{G})$, $\tilde{P}_i \in \tilde{D}$, согласно п. 3.1, код $\overline{\tilde{\mathcal{C}}|_{\mathbb{F}_{q^m}}}^{\sigma}$ имеет параметры $[n/\ell, k'/\ell]$.

4. Анализ безопасности квазициклических альтернантных кодов

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 (4) и (5). 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 за инвариантный альтернантный код $\mathcal{A}_{r,q}(\tilde{D}, \tilde{G})$ для некоторых дивизоров $\tilde{D}$ и $\tilde{G}$ 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 при знании $\tilde{D}$ и $\tilde{G}$.

Будем предполагать, что $\tilde{D} = \sum_{i=1}^{n/\ell} \left(\tilde{\alpha}_i : \tilde{\beta}_i\right)$ и $\tilde{G} = t \cdot \tilde{Q}$ для инвариантного кода $\mathcal{A}_{r,q}(\tilde{D}, \tilde{G})$ известны и что G строится с помощью орбиты одной рациональной точки Q. Для исходного кода используем следующие обозначения:

$$\operatorname{supp}(D) = \{(\alpha_{i,j} : 1) : i \in \{1, \ldots, n/\ell\},\ j \in \{0, \ldots, \ell - 1\}\},$$
$$G = t \sum_{j=0}^{\ell-1} \sigma^j(Q),$$

где $\sigma^j(Q) = (\gamma_j : \delta_j) \neq P_\infty$ для всех $j \in \{0, \ldots, \ell - 1\}$.

4.1. Восстановление дивизора и носителя

Как показано в п.3, в зависимости от вида автоморфизма σ справедливы разные формульные соотношения, определяющие вид дивизоров, участвующих в построении инвариантного проколотого кода, следовательно, процесс восстановления дивизора и носителя исходного кода будет отличаться в зависимости от вида автоморфизма. Рассмотрим подробно данный процесс в каждом отдельном случае.

Случай, когда автоморфизм σ является диагонализируемым в $\mathbb{F}_{q^m}$

Замечание 8. Если $\tilde{Q} \neq P_\infty$, то для всех $i \in \{0, \ldots, \ell - 1\}$ имеем

$$\tilde{Q} = \left((-1)^{\ell-1} \left(a^i\right)^{\ell(\ell-1)/2} (\gamma_i/\delta_i)^\ell : 1\right).$$

Далее будем предполагать, что точка $\tilde{Q}$ и дивизор $\tilde{G}$ известны. Покажем возможность восстановления исходного дивизора G.

Обозначим $\mu_\ell = \{\sigma^i(a) : i \in \{0, \ldots, \ell - 1\}\}$ и для каждого $a \in \mu_\ell$ восстановим соответствующую точку носителя дивизора G. Отметим, что множество μ_ℓ состоит из примитивных корней степени ℓ из единицы. Мощность множества равна количеству элементов порядка ℓ в поле $\mathbb{F}_{q^m}$, то есть $\varphi(\ell) < n$. Следовательно, существует всего $\varphi(\ell)$ вариантов выбора элемента a, что позволяет перебрать всевозможные варианты за приемлемое время.

Более детально вычисление дивизора G на основании знания $\tilde{G}$ описано в алгоритме 1. Основной и наиболее затратный шаг — вычисление корней многочлена $p(X) = a^{\ell(\ell-1)/2} X^\ell - \tilde{\gamma} \in \mathbb{F}_{q^m}[X]$, которые можно найти, используя, например, алгоритм Берлекэмпа.

Алгоритм 1. Восстановление дивизора G

Вход: $\tilde{G}$ — дивизор инвариантного кода $\overline{\mathcal{A}_{r,q}(D, G)}^\sigma$.
Выход: дивизор G.

1: $a := a^\ell \equiv 1 \pmod{q^m}$.
2: **Если** $\widetilde{Q} \neq P_\infty$, **то**
3: $\quad \Gamma :=$ корни $(a^{\ell(\ell-1)/2} X^\ell - \tilde{\gamma})$,
4: $\quad G := t \sum_{\gamma \in \Gamma} (\gamma : 1)$,
5: **иначе**
6: $\quad G := t \cdot \ell \cdot P_\infty$.
7: **Вернуть** G.

Далее восстановим носитель дивизора D' при условии, что коды $\mathcal{A}_{r,q}(D', G)$ и $\mathcal{A}_{r,q}(D, G)$ отличаются перестановкой координат. Координаты точки $P = (x : y) \in \in \operatorname{supp}(D)$ удовлетворяют системе

$$\begin{cases} x^\ell - \tilde{\alpha}_i = 0, \\ y^\ell - \tilde{\beta}_i = 0, \end{cases} \tag{6}$$

для $i \in \{1, \ldots, n/\ell\}$, где $(\tilde{\alpha}_i : \tilde{\beta}_i) = \tilde{P}_i$. Зная $\tilde{D}$, можно восстановить все элементы носителя D, однако они будут представлять собой неупорядоченное множество. Найдём решение (α'_i, β'_i) в (6) для каждого $i \in \{1, \ldots, n/\ell\}$ и выберем $a \in \mu_\ell$. Будем полагать, что множество

$$\operatorname{supp}(D') = \left\{ \left(a^j \frac{\alpha'_i}{\beta'_i} : 1 \right) : j \in \{0, \ldots, \ell - 1\},\ i \in \{1, \ldots, n/\ell\} \right\}$$

является носителем кода $\mathcal{A}_{r,q}(D', G)$, являющегося перестановочным относительно кода $\mathcal{A}_{r,q}(D, G)$. Для каждого множества решений $S = \{(\alpha'_i, \beta'_i) : i \in \{1, \ldots, n/\ell\}\}$ и всякого $a \in \mu_\ell$ имеем различные соответствующие им носители D'.

Случай, когда автоморфизм σ является тригонализируемым в $\mathbb{F}_{q^m}$

Замечание 9. Если $\tilde{Q} \neq P_\infty$, то для всех $i \in \{0, \ldots, \ell - 1\}$ имеем

$$\tilde{Q} = \left(\left(\frac{\gamma_i}{\delta_i} \right)^p - b^{p-1} \frac{\gamma_i}{\delta_i} : 1 \right).$$

В случае диагонализируемого автоморфизма σ поиск элемента a, такого, что $\operatorname{ord}(a) = \ell$, является тривиальным. Достаточно перебрать все корни степени ℓ из единицы. Существует следующий способ нахождения кандидатов для параметра b в случае тригонализируемого автоморфизма σ.

Лемма 7 [1, Лемма 4.1]. Число b — один из корней многочлена

$$P_b = \text{НОД}\left(\left\{ \operatorname{Res}_X \left(X^p - Y^{p-1}X - \tilde{\alpha}_i, X^{q^m} - X \right) : i \in \{1, \ldots, n/\ell\} \right\}, Y^{q^m} - Y \right),$$

где $\operatorname{Res}_X(F_1(X), F_2(X))$ — результант двух многочленов относительно переменной X.

Таким образом, $b \in \operatorname{roots}(P_b)$. Стоит отметить, что все элементы из орбиты b также являются корнями многочлена P_b, то есть $B = \{b, 2b, \ldots, (\ell-1)b\} \subseteq \operatorname{roots}(P_b)$. В общем случае $\deg(P_b) \geqslant |B|$. Для полей большого порядка ($\sim 2^m$, где $m \geqslant 10$) на практике всегда выполняется $B = \operatorname{roots}(P_b)$.

Далее будем предполагать, что точка $\tilde{Q}$ и дивизор $\tilde{G}$ известны. Алгоритм 2 восстанавливает исходный дивизор G, используя только параметры инвариантного проколотого кода $\overline{\mathcal{A}_{r,q}(D, G)}^{\sigma}$.

Алгоритм 2. Восстановление дивизора G

Вход: $\tilde{G}$, $\tilde{D}$ — дивизоры инвариантного кода $\overline{\mathcal{A}_{r,q}(D, G)}^{\sigma}$.
Выход: дивизор G и множество $B' \supseteq \{b, 2b, \ldots, (\ell - 1)b\}$.

$P_b := \text{НОД}\left(\left\{ \operatorname{Res}_X \left(X^p - Y^{p-1}X - \tilde{\alpha}_i, X^{q^m} - X \right) : i \in \{1, \ldots, n/\ell\} \right\}, Y^{q^m} - Y \right)$
$B' :=$ корни (P_b)
Если $\tilde{Q} \neq P_\infty$, **то**
    $\Gamma :=$ корни $(X^p - b^{p-1}X - \tilde{\gamma})$, $\quad // \ b \in B'$
    $G := t \sum\limits_{\gamma \in \Gamma} (\gamma : 1)$,
иначе
    $G := t \cdot P_\infty$.
Вернуть G, B'.

Замечание 10. Самым сложным шагом алгоритма 2 является нахождение результантов, а также последующее нахождение наибольшего общего делителя двух

многочленов над полем $\mathbb{F}_{q^m}$. В свою очередь, самым трудозатратным шагом в вычислении результанта является нахождение определителя матрицы, которое выполняется за $\mathcal{O}((q^m+p)^\omega(q^m+p)(p-1))$ шагов в поле $\mathbb{F}_{q^m}$, где ω — экспонента в сложности умножения матриц. Сложность вычисления наибольшего общего делителя двух многочленов степени $q^m(p-1)$ в кольце $\mathbb{F}_{q^m}[Y]$ ограничена $\mathcal{O}(q^{2m}p^2)$, что меньше сложности вычисления определителей. Таким образом, учитывая, что данные алгоритмы срабатывают n/p раз, получаем итоговую сложность алгоритма $\mathcal{O}(n(q^m+p)^{\omega+1})$.

Далее восстановим носитель дивизора D' при условии, что $\mathcal{A}_{r,q}(D',G)=\mathcal{A}_{r,q}(D,G)$. Координаты точки $P=(x:y)\in\operatorname{supp}(D)$ удовлетворяют системе

$$\begin{cases} x^p - b^{p-1}x - \tilde{\alpha}_i = 0, \\ y^p - \tilde{\beta}_i = 0 \end{cases} \tag{7}$$

для $i\in\{1,\dots,n/\ell\}$, где $(\tilde{\alpha}_i:\tilde{\beta}_i)=\tilde{P}_i$. Зная $\tilde{D}$, мы можем восстановить все элементы носителя дивизора D, однако они будут представлять собой неупорядоченное множество. Найдём решение (α'_i,β'_i) в (7) для каждого $i\in\{1,\dots,n/\ell\}$ и выберем $b\in B'$. Множество

$$\operatorname{supp}(D')=\left\{\left(\frac{\alpha'_i}{\beta'_i}+b\cdot j:1\right):j\in\{0,\dots,\ell-1\},\ i\in\{1,\dots,n/\ell\}\right\}$$

составляет носитель кода $\mathcal{A}_{r,q}(D',G)$, являющегося перестановочным относительно кода $\mathcal{A}_{r,q}(D,G)$. Для каждого множества решений $S=\{(\alpha'_i,\beta'_i):i\in\{1,\dots,n/\ell\}\}$ и всякого $b\in B'$ имеем различные соответствующие им носители D'.

Случай, когда автоморфизм σ является диагонализируемым в $\mathbb{F}_{q^{2m}}\backslash\mathbb{F}_{q^m}$

В этом случае $\sigma=\rho\circ\sigma_d\circ\rho^{-1}$, где $\rho\in\mathrm{PGL}_2(\mathbb{F}_{q^{2m}})$ и

$$\sigma_d:\begin{cases}\mathbf{P}^1\to\mathbf{P}^1,\\ (x:y)\mapsto(\xi x:\xi^{q^m}y),\end{cases}$$

где $\xi\in\mathbb{F}_{q^{2m}}$ — корень степени ℓ из единицы. Поскольку σ_d диагонален в $\mathbb{F}_{q^{2m}}$, мы можем восстановить носитель дивизора $D^\otimes$ и дивизор $G^\otimes$ в $\mathbb{F}_{q^{2m}}$, используя те же методы, что и в случае диагонализируемости и тригонализируемости в $\mathbb{F}_{q^m}$.

Для восстановления дивизоров D и G в $\mathbb{F}_{q^m}$ 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 лемме 5, можем предположить, что $\sigma=\sigma'$. Нахождение элемента ξ не составляет труда ввиду использования малого параметра ℓ, соответственно легко можем вычислить a и b. 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 $\mathbb{F}_{q^m}$.

4.2. Восстановление перестановки

Восстановим перестановку между $\mathcal{A}_{r,q}(D', G)$ и $\mathcal{A}_{r,q}(D, G)$. Пусть $\mathbf{G}_{\text{pub}}$ — порождающая матрица кода $\mathcal{A}_{r,q}(D, G)$, $\mathbf{H}'$ — проверочная матрица кода $\mathcal{A}_{r,q}(D', G)$. Перестановку между $\mathcal{A}_{r,q}(D, G)$ и $\mathcal{A}_{r,q}(D', G)$ зададим с помощью матрицы $\mathbf{\Pi}$:

$$\mathbf{G}_{\text{pub}} \cdot \mathbf{\Pi} \cdot \mathbf{H}'^{\top} = 0. \tag{8}$$

Предположим, мы выбрали $a \in \mu_\ell$, тогда перестановочная матрица $\mathbf{\Pi}$ 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 (8) имеет n неизвестных. Если мы предположим, что $k \neq n$, то мы можем найти с большой вероятностью единственное решение для $\mathbf{\Pi}$ ввиду того, что в системе $(n-k)k$ уравнений и $n \leqslant (n-k)k$ неизвестных.

В алгоритме 3 представлено восстановление перестановочной матрицы $\mathbf{\Pi}$ при верном выборе элементов $a \in \mu_\ell$, $b \in \text{roots}(P_b)$.

Алгоритм 3. Восстановление $\text{supp}(D)$. Случай σ — диагонализируемый/тригонализируемый в $\mathbb{F}_{q^m}$

Вход: $\mathbf{G}_{\text{pub}}$ — порождающая матрица квазициклического альтернантного кода; дивизоры G, $\tilde{D}$.

Выход: $\varnothing$, если решение не найдено; в противном случае — D', такое, что $\mathcal{A}_{r,q}(D', G) = \mathcal{A}_{r,q}(D, G)$.

Для всех $i \in \{1, \dots, n\}$
  $\alpha'_i :=$ корни $(x^\ell - \tilde{\alpha}_i)$, // $\alpha'_i :=$ *корни* $(x^p - b^{p-1}x - \tilde{\alpha}_i)$
  $\beta'_i :=$ корни $(y^\ell - \tilde{\beta}_i)$. // $\beta'_i :=$ *корни* $(y^p - \tilde{\beta}_i)$
Для $a \in \mu_\ell$ // **для** $b \in B'$
  $\text{supp}(D') := \left\{ \left(a^j \dfrac{\alpha'_i}{\beta'_i} : 1 \right) : j \in \{0, \dots, \ell - 1\},\ i \in \{1, \dots, n/l\} \right\}$, // *supp*$(D') :=$
  $:= \left\{ \left(\dfrac{\alpha_i}{\beta_i} + b \cdot j : 1 \right) \right\}$
  $\mathcal{C} := \mathcal{A}_{r,q}(D', G)$.
  Если $\mathcal{C} = \mathcal{A}_{r,q}(D, G)$, **то**
    Вернуть D',
  иначе
    $\mathbf{H}' :=$ проверочная матрица $(\mathcal{C})$,
    $S :=$ решения $\mathbf{G}_{\text{pub}} \cdot \mathbf{\Pi} \cdot \mathbf{H}'^{\top} = 0$, где $\mathbf{\Pi}$ — перестановочная матрица.
    Если $\dim(S) = \ell$, **то**
      Вернуть $\pi(D')$. // $\pi \in \mathfrak{S}_n$ *ассоциирована с* $\mathbf{\Pi}$
Вернуть $\varnothing$.

Замечание 11. Размерность пространства решений в случае единственности решения равна ℓ, однако эти решения эквивалентны в контексте поиска перестановки для носителя квазициклического кода. Если представить решение системы в виде вектора, то, очевидно, по свойствам QC-кодов квазициклический сдвиг его блоков длины ℓ также является решением системы (8). Единственность решения нельзя гарантировать для произвольных параметров, так как возможно получение большого числа линейно зависимых уравнений в системе, однако для полей большого порядка ($\sim 2^m$, где $m \geqslant 10$) и параметров кода $[n \geqslant 2048, k \geqslant n/2]$, используемых на практике, данная проблема не возникает.

5. Примеры

Приведём примеры построения квазициклического альтернантного кода $\mathcal{A}_{r,q}(D,G) = \mathcal{C}_{\mathscr{L}}(D,G)^{\perp} \cap \mathbb{F}_q^n$ с помощью GRS-кода, а также рассмотрим примеры восстановления параметров оригинального кода через параметры кода $\overline{\mathcal{A}_{r,q}(D,G)}^{\sigma}$ для всех описанных случаев. Все вычисления выполнены в системах компьютерной алгебры Sage и Magma.

5.1. Случай, когда автоморфизм σ является диагонализируемым в $\mathbb{F}_{q^m}$

Построим QC-GRS-код $\mathcal{C}_{\mathscr{L}}(D,G)$ над полем $\mathbb{F}_{2^6}$ с параметрами $[21,4]$ с помощью диагонализируемого автоморфизма

$$\sigma = \begin{pmatrix} \alpha^{21} & 0 \\ 0 & 1 \end{pmatrix},$$

где $\operatorname{ord}(\sigma) = \ell = 3$ и $\alpha^6 + \alpha^4 + \alpha^3 + \alpha + 1 = 0$.

Рассмотрим проективную прямую $\mathbf{P}^1$ над полем $\mathbb{F}_{64}$, а в качестве носителя дивизора D выберем следующие рациональные точки проективной прямой:

$$\begin{aligned}
\operatorname{Orb}_\sigma(P_1) &= \big\{(\alpha:1), (\alpha^4+\alpha^3+\alpha^2:1), (\alpha^4+\alpha^3+\alpha^2+\alpha:1)\big\},\\
\operatorname{Orb}_\sigma(P_2) &= \big\{(\alpha^2:1), (\alpha^5+\alpha^4+\alpha^3:1), (\alpha^5+\alpha^4+\alpha^3+\alpha^2:1)\big\},\\
\operatorname{Orb}_\sigma(P_3) &= \big\{(\alpha^3:1), (\alpha^5+\alpha^3+\alpha+1:1), (\alpha^5+\alpha+1:1)\big\},\\
\operatorname{Orb}_\sigma(P_4) &= \big\{(\alpha^4:1), (\alpha^3+\alpha^2+1:1), (\alpha^4+\alpha^3+\alpha^2+1:1)\big\},\\
\operatorname{Orb}_\sigma(P_5) &= \big\{(\alpha^5:1), (\alpha^4+\alpha^3+\alpha:1), (\alpha^5+\alpha^4+\alpha^3+\alpha:1)\big\},\\
\operatorname{Orb}_\sigma(P_6) &= \big\{(\alpha^4+\alpha^3+\alpha+1:1), (\alpha^5+\alpha^4+\alpha^2:1), (\alpha^5+\alpha^3+\alpha^2+\alpha+1:1)\big\},\\
\operatorname{Orb}_\sigma(P_7) &= \big\{(\alpha^5+\alpha^4+\alpha^2+\alpha:1), (\alpha^5+\alpha^4+\alpha+1:1), (\alpha^2+1:1)\big\},\\
\operatorname{supp}(D) &= \coprod_{i=1}^{n/\ell} \operatorname{Orb}_\sigma(P_i).
\end{aligned}$$

Замечание 12. Для наполнения носителя дивизора D необходимо выбирать точки с непересекающимися орбитами.

Для построения дивизора G используем единственную точку $Q = (\alpha^3+1:1)$ и параметр $t = 1$. В результате дивизор примет вид $G = \sum\limits_{R \in \operatorname{Orb}(Q)} R = (\alpha^3+1:1) + (\alpha^5 + \\ + \alpha^2+1:1) + (\alpha^5+\alpha^3+\alpha^2:1)$.

В соответствии с леммой 3 базис пространства Римана — Роха, ассоциированного с дивизором G, выглядит так:

$$\mathscr{L}(G) = \Big\{ \frac{X^3+Y^3}{X^3+(\alpha^5+\alpha^2+\alpha+1)},\ \frac{X\cdot Y^2}{X^3+(\alpha^5+\alpha^2+\alpha+1)},\\ \frac{X^2\cdot Y}{X^3+(\alpha^5+\alpha^2+\alpha+1)},\ \frac{X^3}{X^3+(\alpha^5+\alpha^2+\alpha+1)} \Big\}.$$

Таким образом, порождающая матрица кода $\mathcal{C}_{\mathscr{L}}(D,G)$ имеет следующий вид:

$$G_{\mathcal{C}_{\mathscr{L}}} = \begin{pmatrix} 1&0&0&0&\alpha^{21}&\alpha^{9}&\alpha^{12}&\alpha^{40}&\alpha^{13}&\alpha^{35}&\alpha^{32}&\alpha^{55}&\alpha^{30}&\alpha^{35}&\alpha^{3}&\alpha^{35}&\alpha^{19}&\alpha^{54}&\alpha^{39}&\alpha^{32}&\alpha^{14}\\ 0&1&0&0&\alpha^{9}&\alpha^{61}&\alpha^{30}&1&\alpha^{29}&\alpha^{10}&\alpha^{58}&\alpha^{48}&\alpha^{41}&\alpha^{56}&\alpha^{28}&\alpha^{2}&\alpha^{56}&\alpha^{44}&\alpha^{44}&\alpha^{13}&\alpha^{22}\\ 0&0&1&0&\alpha^{61}&\alpha^{21}&\alpha^{18}&\alpha^{53}&\alpha^{24}&\alpha^{38}&\alpha^{5}&\alpha^{46}&\alpha^{38}&\alpha^{39}&\alpha^{21}&\alpha^{27}&\alpha^{58}&\alpha^{53}&\alpha^{24}&\alpha^{53}&\alpha^{38}\\ 0&0&0&1&1&1&\alpha^{43}&\alpha^{43}&\alpha^{43}&\alpha^{37}&\alpha^{37}&\alpha^{37}&\alpha^{27}&\alpha^{27}&\alpha^{27}&\alpha^{5}&\alpha^{5}&\alpha^{5}&\alpha^{10}&\alpha^{10}&\alpha^{10} \end{pmatrix}.$$

Далее вычислим код $\mathcal{A}_{r,q}(D,G) = \mathcal{C}_{\mathscr{L}}(D,G)^{\perp} \cap \mathbb{F}_q^n$. В результате получим квазициклический альтернантный код с параметрами $[21,3]$ и порождающей матрицей

$$\mathbf{G}_{\text{pub}} = \begin{pmatrix} 1&0&0&0&0&1&1&1&1&1&1&1&1&0&1&1&0&1&0&1&1\\ 0&1&0&1&0&0&1&1&1&1&1&1&1&1&0&1&1&0&1&0&1\\ 0&0&1&0&1&0&1&1&1&1&1&1&0&1&1&0&1&1&1&1&0 \end{pmatrix}.$$

Теперь покажем, что знание $\overline{\mathcal{A}_{r,q}(D,G)}^{\sigma} = \mathcal{A}_{r,q}(\tilde{D},\tilde{G})$, дивизоров $\tilde{D}$ и $\tilde{G}$ с малыми параметрами позволит восстановить оригинальные параметры кода $\mathcal{A}_{r,q}(D,G)$.

Сначала восстановим дивизор G. Как сказано ранее, если $\sigma \sim \begin{pmatrix} a & 0 \\ 0 & 1 \end{pmatrix}$, то дивизор G можно восстановить, применив алгоритм 1:

$$\tilde{G} = 1\cdot(\alpha^5+\alpha^2+\alpha+1:1),\\ a^{\ell(\ell-1)/2}X^{\ell} - \tilde{\gamma} = X^3 + (\alpha^5+\alpha^2+\alpha+1), \tag{9}$$

где $a = \alpha^{21}$ — корень из единицы степени ℓ.

Корням многочлена (9) соответствуют следующие точки проективной прямой:

$$(\alpha^3+1:1),\ (\alpha^5+\alpha^2+1:1),\ (\alpha^5+\alpha^3+\alpha^2:1).$$

Данные точки входят в носитель оригинального дивизора G. Таким образом, дивизор G полностью восстановлен.

Перейдём к восстановлению носителя дивизора D. В первую очередь необходимо найти одно решение системы (6) для каждой точки $(\tilde{\alpha}_i : \tilde{\beta}_i) \in \operatorname{supp}(\tilde{D})$, принимая во внимание, что

$$\operatorname{supp}(\tilde{D}) = \{(\alpha^3:1),\ (\alpha^4+\alpha^3+\alpha+1:1),\ (\alpha^5+\alpha^4+\alpha^2+1:1),\ (\alpha^5+\alpha^3+1:1),\\ (\alpha^5+\alpha^2,1),\ (\alpha^4+\alpha^2+\alpha+1:1),\ (\alpha^3+\alpha^2+\alpha:1)\}.$$

Корням системы соответствуют следующие точки проективной прямой:

$$(\alpha^4+\alpha^3+\alpha^2+\alpha:1),\ (\alpha^5+\alpha^4+\alpha^3+\alpha^2:1),\ (\alpha^5+\alpha^3+\alpha+1:1),\\ (\alpha^3+\alpha^2+1:1),\ (\alpha^4+\alpha^3+\alpha:1),\ (\alpha^4+\alpha^3+\alpha+1:1),\ (\alpha^5+\alpha^4+\alpha^2+\alpha:1).$$

При этом

$$\operatorname{supp}(D') = \left\{\left(a^j\frac{\alpha'_i}{\beta'_i} : 1\right) : j\in\{0,\dots,\ell{-}1\}, i\in\{1,\dots,n/l\}\right\} = \{(\alpha^4{+}\alpha^3{+}\alpha^2{+}\alpha : 1), (\alpha : 1),$$
$$(\alpha^4+\alpha^3+\alpha^2 : 1), (\alpha^5+\alpha^4+\alpha^3+\alpha^2 : 1), (\alpha^2 : 1), (\alpha^5+\alpha^4+\alpha^3 : 1), (\alpha^5+\alpha^3+\alpha+1 : 1),$$
$$(\alpha^5+\alpha+1 : 1), (\alpha^3 : 1), (\alpha^3+\alpha^2+1 : 1), (\alpha^4+\alpha^3+\alpha^2+1 : 1), (\alpha^4 : 1), (\alpha^4+\alpha^3+\alpha : 1),$$
$$(\alpha^5+\alpha^4+\alpha^3+\alpha : 1), (\alpha^5 : 1), (\alpha^4+\alpha^3+\alpha+1 : 1), (\alpha^5+\alpha^4+\alpha^2 : 1),$$
$$(\alpha^5+\alpha^3+\alpha^2+\alpha+1 : 1), (\alpha^5+\alpha^4+\alpha^2+\alpha : 1), (\alpha^5+\alpha^4+\alpha+1 : 1), (\alpha^2+1 : 1)\}.$$

Нетрудно заметить, что носители оригинального дивизора D и дивизора D' отличаются перестановкой. Последний шаг — восстановление перестановки между $\mathcal{A}_{r,q}(D',G)$ и $\mathcal{A}_{r,q}(D,G)$ путём решения матричного уравнения (8), где

$$\mathbf{H}'^{\top} = \begin{pmatrix}
1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0\\
1&1&1&1&1&1&1&1&1&1&1&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1\\
0&1&1&1&1&0&0&0&0&0&0&1&1&0&0&1&1&1\\
1&1&0&1&0&1&0&0&0&0&0&1&0&1&1&1&0&1
\end{pmatrix}.$$

В результате найденная перестановочная матрица имеет вид

$$\mathbf{\Pi} = \begin{pmatrix}
\mathbf{1}&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&\mathbf{1}&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&\mathbf{1}&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&\mathbf{1}&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&\mathbf{1}&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&\mathbf{1}&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&\mathbf{1}&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&\mathbf{1}&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&\mathbf{1}&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&\mathbf{1}&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&\mathbf{1}&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&\mathbf{1}&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&\mathbf{1}&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&\mathbf{1}&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&\mathbf{1}&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&\mathbf{1}&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&\mathbf{1}&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&\mathbf{1}&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&\mathbf{1}&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&\mathbf{1}&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&\mathbf{1}
\end{pmatrix}.$$

Отметим, что в носителе $\mathrm{supp}(D')$ в блоках 1 и 2 на первом месте стоят третьи элементы из орбит соответствующих точек носителя оригинального дивизора, что соответствует единицам на главной диагонали матрицы $\mathbf{\Pi}$. В блоках 6 и 7 элементы не переставлены, а в блоках 3, 4 и 5 на первое место встали вторые элементы из орбит. Таким образом, найдя перестановку $\mathbf{\Pi}$, мы восстановили оригинальный носитель $\mathrm{supp}(D)$.

5.2. Случай, когда автоморфизм σ является тригонализируемым в $\mathbb{F}_{q^m}$

Сначала построим QC-GRS-код $\mathcal{C}_{\mathscr{L}}(D, G)$ над $\mathbb{F}_{3^4}$ с параметрами $[15, 4]$ с помощью тригонализируемого автоморфизма

$$\sigma = \begin{pmatrix} 1 & 2\alpha^3 + \alpha^2 + \alpha + 1 \\ 0 & 1 \end{pmatrix},$$

где $\mathrm{ord}(\sigma) = \ell = \mathrm{Char}(\mathbb{F}_{q^m}) = 3$.

Рассмотрим проективную прямую $\mathbf{P}^1$ над полем $\mathbb{F}_{81}$, а в качестве носителя дивизора D выберем следующие рациональные точки проективной прямой:

$$\begin{aligned}
\mathrm{Orb}_\sigma(P_1) &= \big\{(1:1), (2\alpha^3 + \alpha^2 + \alpha + 2:1), (\alpha^3 + 2\alpha^2 + 2\alpha:1)\big\},\\
\mathrm{Orb}_\sigma(P_2) &= \big\{(2:1), (2\alpha^3 + \alpha^2 + \alpha:1), (\alpha^3 + 2\alpha^2 + 2\alpha + 1:1)\big\},\\
\mathrm{Orb}_\sigma(P_3) &= \big\{(2\alpha:1), (2\alpha^3 + \alpha^2 + 1:1), (\alpha^3 + 2\alpha^2 + \alpha + 2:1)\big\},\\
\mathrm{Orb}_\sigma(P_4) &= \big\{(2\alpha + 1:1), (2\alpha^3 + \alpha^2 + 2:1), (\alpha^3 + 2\alpha^2 + \alpha:1)\big\},\\
\mathrm{Orb}_\sigma(P_5) &= \big\{(2\alpha + 2:1), (2\alpha^3 + \alpha^2:1), (\alpha^3 + 2\alpha^2 + \alpha + 1:1)\big\}.
\end{aligned}$$

Для построения дивизора G используем единственную точку $Q = (\alpha^2 + \alpha + 2 : 1)$ и параметр $t = 1$. В результате дивизор примет вид

$$G = \sum_{R \in \mathrm{Orb}(Q)} R = (\alpha^2 + \alpha + 2:1) + (\alpha^3 + 1:1) + (2\alpha^3 + 2\alpha^2 + 2\alpha:1)\,.$$

В соответствии с леммой 3 базис пространства Римана — Роха, ассоциированного с дивизором G, можно записать так:

$$\mathscr{L}(G) = \Big\{\frac{X^3}{X^3 + \alpha^{54}XY^2 + \alpha^7Y^3}, \ \frac{Y^3}{X^3 + \alpha^{54}XY^2 + \alpha^7Y^3}, \ \frac{XY^2}{X^3 + \alpha^{54}XY^2 + \alpha^7Y^3}, \ \frac{X^2Y}{X^3 + \alpha^{54}XY^2 + \alpha^7Y^3}\Big\}.$$

Таким образом, порождающая матрица кода $\mathcal{C}_{\mathscr{L}}(D, G)$ имеет следующий вид:

$$G_{\mathcal{C}_{\mathscr{L}}} = \begin{pmatrix}
\alpha^{77} & \alpha^{23} & \alpha^{29} & \alpha^{6} & \alpha^{38} & \alpha^{32} & \alpha^{25} & \alpha^{50} & \alpha^{67} & \alpha^{16} & \alpha^{26} & \alpha^{76} & \alpha^{65} & \alpha^{58} & 1 \\
\alpha^{77} & \alpha^{77} & \alpha^{77} & \alpha^{46} & \alpha^{46} & \alpha^{46} & \alpha^{62} & \alpha^{62} & \alpha^{62} & \alpha^{65} & \alpha^{65} & \alpha^{65} & \alpha^{21} & \alpha^{21} & \alpha^{21} \\
\alpha^{77} & \alpha^{59} & \alpha^{61} & \alpha^{6} & \alpha^{70} & \alpha^{68} & \alpha^{23} & \alpha^{58} & \alpha^{37} & \alpha^{22} & \alpha^{52} & \alpha^{42} & \alpha^{9} & \alpha^{60} & \alpha^{14} \\
\alpha^{77} & \alpha^{41} & \alpha^{45} & \alpha^{46} & \alpha^{14} & \alpha^{10} & \alpha^{64} & \alpha^{54} & \alpha^{12} & \alpha^{59} & \alpha^{39} & \alpha^{19} & \alpha^{77} & \alpha^{19} & \alpha^{7}
\end{pmatrix}.$$

Далее вычислим код $\mathcal{A}_{r,q}(D, G) = \mathcal{C}_{\mathscr{L}}(D, G)^{\perp} \cap \mathbb{F}_q^n$. В результате получим квазициклический альтернантный код с параметрами $[15, 3]$ и порождающей матрицей

$$\mathbf{G}_{\mathrm{pub}} = \begin{pmatrix}
1 & 0 & 0 & 1 & 2 & 2 & 2 & 2 & 1 & 2 & 2 & 2 & 0 & 2 & 2 \\
0 & 1 & 0 & 2 & 1 & 2 & 1 & 2 & 2 & 2 & 2 & 2 & 2 & 0 & 2 \\
0 & 0 & 1 & 2 & 2 & 1 & 2 & 1 & 2 & 2 & 2 & 2 & 2 & 2 & 0
\end{pmatrix}.$$

Покажем, что знание $\overline{\mathcal{A}_{r,q}(D,G)}^{\sigma} = \mathcal{A}_{r,q}(\tilde{D},\tilde{G})$, дивизоров $\tilde{D}$ и $\tilde{G}$ с малыми параметрами позволит восстановить оригинальные параметры кода $\mathcal{A}_{r,q}(D,G)$.

Сначала вычислим возможных кандидатов для элемента b, используя лемму 7:

$$P_b = \text{НОД}\left(\left\{\text{Res}_X(X^p - Y^{p-1}X - \tilde{\alpha}_i, X^{q^m} - X) : i \in \{1,\dots,n/\ell\}\right\}, Y^{q^m} - Y\right) = \\ = Y^9 + (\alpha^3 - \alpha^2 - \alpha)\,Y^7 + (-\alpha^3 - \alpha^2 - \alpha - 1)\,Y.$$

Таким образом, элемент b — один из корней многочлена P_b. Соответственно

$$B' = \text{roots}\,(P_b) = \{1,\ 2\alpha^3 + 2\alpha + 2,\ 2\alpha^2 + 2\alpha,\ \alpha^3 + \alpha + 1, \alpha^3 + 2\alpha^2 + 2\alpha + 1, \\ \alpha^3 + 2\alpha^2 + 2\alpha + 2,\ \alpha^2 + \alpha,\ 2\alpha^3 + \alpha^2 + \alpha + 1,\ 2\alpha^3 + \alpha^2 + \alpha + 2\}.$$

Далее покажем восстановление дивизора G при правильном выборе b. Если $\sigma \sim \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix}$, то дивизор G можно восстановить, применив алгоритм 2:

$$\tilde{G} = 1 \cdot (\alpha^3 + 2\alpha^2 + 2\alpha + 2 : 1), \\ X^p - b^{p-1}X - \tilde{\gamma} = X^3 + (2\alpha^3 + 2\alpha^2 + 2\alpha + 1)X + 2\alpha^3 + \alpha^2 + \alpha + 1, \qquad (10)$$

где $b = 2\alpha^3 + \alpha^2 + \alpha + 1$.

Корням многочлена (10) соответствуют следующие точки проективной прямой:

$$(\alpha^2 + \alpha + 2 : 1),\ (\alpha^3 + 1 : 1),\ (2\alpha^3 + 2\alpha^2 + 2\alpha : 1).$$

Данные точки входят в носитель оригинального дивизора G. Таким образом, дивизор G полностью восстановлен.

Перейдём к восстановлению носителя дивизора D. В первую очередь необходимо найти одно решение системы (7) для каждой точки $(\tilde{\alpha}_i : \tilde{\beta}_i) \in \text{supp}(\tilde{D}) = \{(2\alpha^3 + 2\alpha^2 + \\ + 2\alpha + 2 : 1), (\alpha^3 + \alpha^2 + \alpha + 1 : 1), (\alpha^3 + \alpha^2 + 2\alpha + 1 : 1), (\alpha : 1), (2\alpha^3 + 2\alpha^2 + 2 : 1)\}$. Корням системы соответствуют следующие точки проективной прямой:

$$(1 : 1),\ (2\alpha^3 + \alpha^2 + \alpha : 1),\ (\alpha^3 + 2\alpha^2 + \alpha + 2 : 1),\ (\alpha^3 + 2\alpha^2 + \alpha : 1),\ (2\alpha^3 + \alpha^2 : 1).$$

При этом

$$\text{supp}(D') = \left\{\left(\frac{\alpha'_i}{\beta'_i} + b \cdot j : 1\right) : j \in \{0,\dots,\ell-1\}, i \in \{1,\dots,n/\ell\}\right\} = \{(1 : 1), \\ (2\alpha^3 + \alpha^2 + \alpha + 2 : 1),\ (\alpha^3 + 2\alpha^2 + 2\alpha : 1),\ (2\alpha^3 + \alpha^2 + \alpha : 1),\ (\alpha^3 + 2\alpha^2 + 2\alpha + 1 : 1), \\ (2 : 1),\ (\alpha^3 + 2\alpha^2 + \alpha + 2 : 1),\ (2\alpha : 1),\ (2\alpha^3 + \alpha^2 + 1 : 1),\ (\alpha^3 + 2\alpha^2 + \alpha : 1), \\ (2\alpha + 1 : 1),\ (2\alpha^3 + \alpha^2 + 2 : 1),\ (2\alpha^3 + \alpha^2 : 1),\ (\alpha^3 + 2\alpha^2 + \alpha + 1 : 1),\ (2\alpha + 2 : 1)\}.$$

Нетрудно заметить, что носители оригинального дивизора D и дивизора D' отличаются перестановкой. Последний шаг — восстановление перестановки между $\mathcal{A}_{r,q}(D',G)$ и $\mathcal{A}_{r,q}(D,G)$ путём решения матричного уравнения (8), где

$$\mathbf{H'}^{\top} = \begin{pmatrix}
1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\
2 & 1 & 2 & 0 & 2 & 2 & 2 & 0 & 2 & 1 & 1 & 1 \\
2 & 2 & 1 & 2 & 0 & 2 & 2 & 2 & 0 & 1 & 1 & 1 \\
1 & 2 & 2 & 2 & 2 & 0 & 0 & 2 & 2 & 1 & 1 & 1
\end{pmatrix}.$$

В результате найденная перестановочная матрица имеет вид

$$\mathbf{\Pi} = \begin{pmatrix}
0 & 0 & \mathbf{1} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
\mathbf{1} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & \mathbf{1} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & \mathbf{1} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & \mathbf{1} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & \mathbf{1} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & \mathbf{1} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & \mathbf{1} & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \mathbf{1} & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \mathbf{1} & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \mathbf{1} & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \mathbf{1} & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \mathbf{1} & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \mathbf{1} & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \mathbf{1}
\end{pmatrix}$$

Отметим, что в носителе $\operatorname{supp}(D')$ в блоке 1 все элементы стоят на своих местах, в блоках 2 и 5 на первое место встали вторые элементы из орбит, а в блоках 3 и 4 на первом месте стоят третьи элементы из орбит соответствующих точек носителя оригинального дивизора, что соответствует единицам на главной диагонали матрицы $\mathbf{\Pi}$. Таким образом, найдя перестановку $\mathbf{\Pi}$, мы восстановили оригинальный носитель $\operatorname{supp}(D)$.

Замечание 13. В данном примере параметр b, а также перестановка, являющаяся решением системы (8), находятся неоднозначно, однако для полей большего порядка и параметров $[n \geqslant 2048, k \geqslant n/2]$, использующихся в криптографических схемах, экспериментально не удалось получить ни одного случая множественности решений. Ввиду этого выбор правильных параметров в примере был опущен.

5.3. Случай, когда автоморфизм σ является диагонализируемым в $\mathbb{F}_{q^{2m}} \backslash \mathbb{F}_{q^m}$

Будем полагать, что злоумышленнику известен оригинальный автоморфизм σ. В таком случае вычисление параметров исходного кода тривиально. В прошлых примерах поиск эквивалентного автоморфизма σ' был опущен, так как данная задача легко разрешима при использовании малого параметра ℓ. Здесь же рассмотрим, как осуществляется вычисление параметров кода $\overline{\tilde{\mathcal{C}}}^{\sigma}$, определённого над $\mathbb{F}_{q^{2m}}$, и покажем, что, зная автоморфизм, можно найти параметры оригинального кода, не используя алгоритмы, представленные в п. 4.

Сначала построим QC-GRS-код $\mathcal{C}_{\mathscr{L}}(D,G)$ над полем $\mathbb{F}_{125}$ с параметрами $[15,4]$ с помощью автоморфизма

$$\sigma = \begin{pmatrix} 3\alpha & 3\alpha^2+1 \\ 2\alpha^2+4 & 2\alpha+4 \end{pmatrix},$$

где $\operatorname{ord}(\sigma) = \ell = 3$.

Рассмотрим проективную прямую $\mathbf{P}^1$ над полем $\mathbb{F}_{125}$, а в качестве носителя дивизора D выберем следующие рациональные точки проективной прямой:

$$\begin{aligned}
&\operatorname{Orb}_\sigma(P_1) = \big\{(2:1),(2\alpha^2+2\alpha+1:1),(3\alpha^2+4\alpha+3:1)\big\},\\
&\operatorname{Orb}_\sigma(P_2) = \big\{(2\alpha:1),(3\alpha+3:1),(\alpha^2+2\alpha:1)\big\},\\
&\operatorname{Orb}_\sigma(P_3) = \big\{(2\alpha+1:1),(4\alpha^2+4\alpha+1:1),(2\alpha^2+3\alpha+4:1)\big\},\\
&\operatorname{Orb}_\sigma(P_4) = \big\{(2\alpha+2:1),(\alpha^2+4:1),(4\alpha^2+2\alpha+3:1)\big\},\\
&\operatorname{Orb}_\sigma(P_5) = \big\{(2\alpha+3:1),(\alpha+1:1),(\alpha^2+4\alpha:1)\big\}.
\end{aligned}$$

Для построения дивизора G используем единственную точку $Q = (\alpha^2+4\alpha+3:1)$ и параметр $t=1$. В результате дивизор примет вид

$$G = \sum_{R\in\operatorname{Orb}(Q)} R = (\alpha^2+4\alpha+3:1) + (\alpha^2+4\alpha+2:1) + (\alpha^2+2\alpha+1:1).$$

В соответствии с леммой 3 базис пространства Римана — Роха, ассоциированного с дивизором G, запишется так:

$$\mathscr{L}(G) = \Big\{\frac{X^3+Y^3}{T(X)}, \frac{XY^2}{T(X)}, \frac{X^2Y}{T(X)}, \frac{X^3}{T(X)}\Big\}, \text{ где } T(X) = X^3 + \alpha^{87}X^2Y + \alpha^{41}XY^2 + \alpha^{89}Y^3.$$

Таким образом, порождающая матрица кода $\mathcal{C}_{\mathscr{L}}(D,G)$ будет иметь следующий вид:

$$G_{\mathcal{C}_{\mathscr{L}}} = \begin{pmatrix}
\alpha^{118} & \alpha^{106} & \alpha^{6} & \alpha^{116} & \alpha^{64} & \alpha^{81} & \alpha^{39} & \alpha^{38} & \alpha^{98} & \alpha^{30} & \alpha^{123} & \alpha^{102} & \alpha^{42} & \alpha^{82} & \alpha^{30} \\
\alpha^{87} & \alpha^{85} & \alpha^{3} & \alpha^{72} & \alpha^{73} & \alpha^{2} & \alpha^{44} & \alpha^{64} & 4 & 3 & \alpha^{86} & \alpha^{40} & \alpha^{101} & \alpha^{55} & \alpha^{121} \\
\alpha^{118} & \alpha^{47} & \alpha^{54} & \alpha^{104} & \alpha^{14} & \alpha^{79} & \alpha^{70} & \alpha^{116} & \alpha^{85} & \alpha^{96} & \alpha^{37} & \alpha^{26} & \alpha^{111} & \alpha^{27} & \alpha^{101} \\
\alpha^{25} & \alpha^{9} & \alpha^{105} & \alpha^{12} & \alpha^{79} & \alpha^{32} & \alpha^{96} & \alpha^{44} & \alpha^{108} & \alpha^{99} & \alpha^{112} & \alpha^{12} & \alpha^{121} & \alpha^{123} & \alpha^{81}
\end{pmatrix}.$$

Далее вычислим код $\mathcal{A}_{r,q}(D,G) = \mathcal{C}_{\mathscr{L}}(D,G)^{\perp} \cap \mathbb{F}_5^n$. В результате получим квазициклический альтернантный код с параметрами $[15,5]$ и порождающей матрицей

$$\mathbf{G}_{\text{pub}} = \begin{pmatrix}
1 & 0 & 0 & 0 & 0 & 3 & 4 & 4 & 1 & 0 & 4 & 4 & 4 & 1 & 4 \\
0 & 1 & 0 & 0 & 0 & 3 & 3 & 0 & 1 & 4 & 4 & 0 & 2 & 3 & 4 \\
0 & 0 & 1 & 0 & 0 & 3 & 3 & 4 & 2 & 0 & 3 & 0 & 2 & 1 & 1 \\
0 & 0 & 0 & 1 & 0 & 4 & 1 & 3 & 1 & 0 & 2 & 3 & 4 & 2 & 4 \\
0 & 0 & 0 & 0 & 1 & 4 & 2 & 4 & 4 & 3 & 2 & 0 & 3 & 1 & 1
\end{pmatrix}.$$

Теперь покажем, что знание кода $\overline{\tilde{\mathcal{C}}}^{\sigma}$ и дивизоров $\tilde{D}^{\otimes}$ и $\tilde{G}^{\otimes}$ с малыми параметрами позволит восстановить оригинальные параметры кода $\mathcal{A}_{r,q}(D,G)$.

Сначала восстановим дивизор G. Если $\sigma = \rho\circ\sigma_d\circ\rho^{-1}$, где $\rho \in \mathrm{PGL}_2(\mathbb{F}_{5^6})$, то дивизор G можно восстановить, применив алгоритм 1 к коду, однако это полностью дублирует пример в п. 5.1, поэтому покажем нахождение дивизора при знании автоморфизма σ:

$$M_{\sigma_d} = \begin{pmatrix} \xi & 0 \\ 0 & \xi^{q^m} \end{pmatrix}, \quad \tilde{G} = 1\cdot(3\alpha^2+1:1),$$
$$\xi^{\ell(\ell-1)/2}X^{\ell} - \tilde{\gamma} = X^3 + (2\alpha^2+4), \tag{11}$$

где $\xi = 4\beta + 3$ — корень из единицы степени ℓ поля $\mathbb{F}_{5^6} \cong \mathbb{F}_{5^3}[x]/(X^2 + 3X + 3)$; β — корень неприводимого над $\mathbb{F}_{5^3}$ многочлена $X^2 + 3X + 3$.

Замечание 14. В данном случае выполнение условия $\xi \in \mathbb{F}_{q^{2m}} \setminus \mathbb{F}_{q^m}$ должно быть обязательным, иначе автоморфизм σ можно диагонализировать над $\mathbb{F}_{q^m}$. Нахождение ξ не составляет труда, так как всего существует $\phi(\ell)$ элементов порядка ℓ в $\mathbb{F}_{q^{2m}}$.

Корнями многочлена (11) являются следующие элементы:

$$(\alpha^2 + 4\alpha + 3),\ ((4\alpha^2 + \alpha + 2)\beta + 3\alpha^2 + 2\alpha + 4),\ ((\alpha^2 + 4\alpha + 3)\beta + \alpha^2 + 4\alpha + 3),$$

причём один из корней всегда лежит в поле $\mathbb{F}_{q^m}$ и входит в орбиту оригинального дивизора G. Предыдущее утверждение легко проверить, рассмотрев вид точки $\tilde{Q}$:

$$\tilde{Q}^{\otimes} = \left((-1)^{\ell-1}\xi^{\ell(\ell-1)/2}\left(\frac{\gamma_0}{\delta_0 \cdot \xi^{q^m}}\right)^{\ell} : 1\right) \overset{\ell-\text{нечёт.}}{=} \left(\left(\frac{\gamma_0}{1}\right)^{\ell} : 1\right).$$

Таким образом, среди корней многочлена (11) всегда есть элемент γ_0, которому соответствует точка $(\gamma_0 : 1)$, входящая в оригинальный дивизор G. Поэтому при известном автоморфизме σ дальнейшее восстановление дивизора не требует рассмотрения оставшихся корней и соответствующих им точек из поля $\mathbb{F}_{5^6}$. Достаточно применить автоморфизм σ к найденной точке ℓ раз:

$$G = (\alpha^2 + 4\alpha + 3 : 1) + (\alpha^2 + 4\alpha + 2 : 1) + (\alpha^2 + 2\alpha + 1 : 1).$$

Перейдём к восстановлению носителя дивизора $D^{\otimes}$. В первую очередь необходимо найти одно решение системы (6) для каждой точки $(\tilde{\alpha}_i : \tilde{\beta}_i) \in \operatorname{supp}(\tilde{D}^{\otimes})$, принимая во внимание, что

$$\operatorname{supp}(\tilde{D}^{\otimes}) = \{(3 : 1),\ (\alpha + 1 : 1),\ (2\alpha^2 + 2\alpha + 2 : 1),\ (4\alpha^2 + 4 : 1),\ (\alpha^2 + 3 : 1)\}.$$

Как и в случае нахождения дивизора G, очевидно, среди корней системы будут те, что соответствуют точкам, входящим в носитель оригинального дивизора D, следовательно, применив автоморфизм σ к каждому решению ℓ раз, восстановим оригинальный носитель. Если решать систему над полем $\mathbb{F}_{5^6}$, то получаем

$$\operatorname{supp}(D'^{\otimes}) = \left\{\left(a^j \frac{\alpha_i'^{\otimes}}{\beta_i'^{\otimes}} : 1\right) : j \in \{0, \ldots, \ell - 1\}, i \in \{1, \ldots, n/l\}\right\} = \Big\{(2 : 1), (3\beta + 1 : 1),$$
$$(2\beta + 2 : 1), (2\alpha : 1), (3\alpha\beta + \alpha : 1), (2\alpha\beta + 2\alpha : 1), (2\alpha + 1 : 1), ((3\alpha + 4)\beta + \alpha + 3 : 1),$$
$$((2\alpha + 1)\beta + 2\alpha + 1 : 1), (2\alpha + 2 : 1), ((3\alpha + 3)\beta + \alpha + 1 : 1), ((2\alpha + 2)\beta + 2\alpha + 2 : 1),$$
$$(2\alpha + 3 : 1), ((3\alpha + 2)\beta + \alpha + 4 : 1), ((2\alpha + 3)\beta + 2\alpha + 3 : 1)\Big\},$$

что подтверждает предыдущее замечание.

При этом без знания автоморфизма σ необходимо восстанавливать перестановку, решая систему уравнений (8) над полем $\mathbb{F}_{5^6}$, чтобы получить исходный носитель. Затем, как показано в п. 4.1, необходимо найти отображение ρ', такое, что $\sigma_d = \rho' \circ \sigma' \circ \rho'^{-1}$, чтобы получить исходные дивизоры.

ЛИТЕРАТУРА

1. *Barelli E.* On the Security of Some Compact Keys for McEliece Scheme. `https://arxiv.org/abs/1803.05289`. 2018.
2. *Кунинец А. А., Малыгина Е. С.* Вычисление пар, исправляющих ошибки, для алгеброгеометрического кода // Прикладная дискретная математика. 2024. № 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.* Algebraic Function Fields and Codes. Springer Verlag, 1991.
5. *Stichtenoth H.* On automorphisms of geometric Goppa codes // J. Algebra. 1990. No. 130(1). P. 113–121.
6. *Conrad K.* The Minimal Polynomial and some Applications. `https://kconrad.math.uconn.edu/blurbs/linmultialg/minpolyandappns.pdf`. 2008.
7. *Clark P. L.* Linear Algebra: Invariant Subspaces. `http://alpha.math.uga.edu/~pete/invariant_subspaces.pdf`. 2013.
8. *Faugére J.-C., Otmani A., Perret L., et al.* Folding alternant and Goppa codes with non-trivial automorphism groups // IEEE Trans. Inform. Theory. 2016. No. 62(1). P. 184–121.

REFERENCES

1. *Barelli E.* On the Security of Some Compact Keys for McEliece Scheme. `https://arxiv.org/abs/1803.05289`, 2018.
2. *Kuninets A. A. and Malygina E. S.* Vychislenie par, ispravlyayushchikh oshibki, dlya algebro-geometricheskogo koda [Calculation of error-correcting pairs for an algebraic-geometric code]. Prikladnaya Diskretnaya Matematika, 2024, no. 63, pp. 65–90. (in Russian)
3. *Malygina E. S., Kuninets A. A., Ratochka V. L., et al.* Algebrogeometricheskie kody i dekodirovanie na osnove par, ispravlyayushchikh oshibki [Algebraic-geometry codes and decoding by error-correcting pairs]. Prikladnaya Diskretnaya Matematika, 2023, no. 62, pp. 83–105. (in Russian)
4. *Stichtenoth H.* Algebraic Function Fields and Codes. Springer Verlag, 1991.
5. *Stichtenoth H.* On automorphisms of geometric Goppa codes. J. Algebra, 1990, no. 130(1), pp. 113–121.
6. *Conrad K.* The Minimal Polynomial and some Applications. `https://kconrad.math.uconn.edu/blurbs/linmultialg/minpolyandappns.pdf`, 2008.
7. *Clark P. L.* Linear Algebra: Invariant Subspaces. `http://alpha.math.uga.edu/~pete/invariant_subspaces.pdf`, 2013.
8. *Faugére J.-C., Otmani A., Perret L., et al.* Folding alternant and Goppa codes with non-trivial automorphism groups. IEEE Trans. Inform. Theory, 2016, no. 62(1), pp. 184–121.

МАТЕМАТИЧЕСКИЕ ОСНОВЫ ИНФОРМАТИКИ И ПРОГРАММИРОВАНИЯ

УДК 510.52 DOI 10.17223/20710410/65/6

О ГЕНЕРИЧЕСКОЙ СЛОЖНОСТИ ПРОБЛЕМЫ ВЫЧИСЛЕНИЯ ФУНКЦИИ ЭЙЛЕРА[1]

А. Н. Рыбалов

Институт математики им. С. Л. Соболева СО РАН, г. Омск, Россия

E-mail: alexander.rybalov@gmail.com

Изучается генерическая сложность проблемы вычисления функции Эйлера, имеющей важное значение для современной криптографии. Например, на предположении о её трудноразрешимости основывается криптостойкость знаменитой системы шифрования с открытым ключом RSA. Доказывается, что при условии трудноразрешимости этой проблемы в худшем случае и P = BPP для её решения не существует полиномиального сильно генерического алгоритма. Для сильно генерического полиномиального алгоритма нет эффективного метода случайной генерации входов, на которых этот алгоритм не может решить проблему. Таким образом, этот результат обосновывает применение проблемы вычисления функции Эйлера в криптографии с открытым ключом. Для доказательства теоремы используется метод генерической амплификации, который позволяет строить генерически трудные проблемы из проблем, трудных в худшем случае. Основной идеей этого метода является объединение эквивалентных входов в достаточно большие множества. Эквивалентность входов означает, что рассматриваемая проблема на них решается одинаково.

Ключевые слова: *генерическая сложность, функция Эйлера.*

ON THE GENERIC COMPLEXITY OF THE PROBLEM OF COMPUTING THE EULER FUNCTION

A. N. Rybalov

Sobolev Institute of Mathematics, Omsk, Russia

We study the generic complexity of the problem of the Euler function computation. This problem has important applications in modern cryptography. For example, the cryptographic strength of the famous public key encryption system RSA is based on the assumption of its hardness. We prove that under the condition of worst-case hardness and P = BPP there is no polynomial strongly generic algorithm for this problem. For a strongly generic polynomial algorithm, there is no efficient method for random generation of inputs on which the algorithm cannot solve the problem. Thus, this result justifies the application of the problem of computing the Euler function in public key cryptography. To prove this theorem, we use the method of generic amplification,

[1]Работа поддержана грантом Российского научного фонда № 22-11-20019.

which allows us to construct generically hard problems from the problems that are hard in the classical sense. The main feature of this method is the cloning technique, which combines the input data of a problem into sufficiently large sets of equivalent input data. Equivalence is understood in the sense that the problem is solved in a similar way for them.

Keywords: *generic complexity, Euler function.*

Введение

В современной криптографии интересны такие алгоритмические проблемы, которые, являясь (гипотетически) трудными в классическом смысле, остаются трудными и в генерическом смысле [1], т. е. для почти всех входов. Это объясняется тем, что при случайной генерации ключей в криптографическом алгоритме происходит генерация входа некоторой трудной алгоритмической проблемы, лежащей в основе криптостойкости алгоритма. Если проблема легкоразрешима почти всегда, то для почти всех таких входов её можно будет быстро решить и ключи почти всегда будут нестойкими. Поэтому проблема должна быть трудной для почти всех входов. Например, таким поведением обладают классические алгоритмические проблемы криптографии: распознавания квадратичных вычетов [2], дискретного логарифма [3], извлечения корня в группах вычетов [4].

Функция Эйлера $\varphi(x)$, равная количеству натуральных чисел, меньших x и взаимно простых с x, играет важную роль в современной криптографии. Для её вычисления до сих пор неизвестно эффективных (полиномиальных) алгоритмов [5]. Этот факт, среди прочего, используется для обоснования стойкости знаменитого алгоритма шифрования с открытым ключом RSA [6]. Проблема вычисления функции Эйлера тесно связана с известной проблемой факторизации (разложения на множители) целых чисел: если бы существовал полиномиальный алгоритм для проблемы факторизации, то его можно было бы использовать для эффективного вычисления функции Эйлера. Однако для проблемы факторизации также неизвестно эффективных алгоритмов [5].

В данной работе изучается генерическая сложность проблемы вычисления функции Эйлера. Доказывается, что при условии трудноразрешимости этой проблемы в худшем случае и $\mathrm{P} = \mathrm{BPP}$ для неё не существует полиномиального сильно генерического алгоритма. Для сильно генерического полиномиального алгоритма нет эффективного метода случайной генерации входов, на которых этот алгоритм не может решить проблему. Таким образом, этот результат обосновывает применение проблемы вычисления функции Эйлера в криптографии с открытым ключом. Здесь класс BPP состоит из проблем, разрешимых за полиномиальное время на вероятностных машинах Тьюринга. Считается, что класс BPP совпадает с классом P, то есть любой полиномиальный вероятностный алгоритм можно эффективно дерандомизировать, построив полиномиальный алгоритм, не использующий генератор случайных чисел и решающий ту же самую проблему. Хотя равенство $\mathrm{P} = \mathrm{BPP}$ до сих пор не доказано, имеются веские основания в его пользу [7].

1. Предварительные сведения

В данной работе множеством входов для алгоритмов является множество натуральных чисел $\mathbb{N}$, записанных в двоичной форме. Под размером $\mathrm{size}(x)$ натурального числа x понимается длина его двоичной записи.

Для подмножества $S \subseteq \mathbb{N}$ определим *последовательность относительных плотностей*

$$\rho_n(S) = \frac{|S_n|}{|\mathbb{N}_n|},\ n = 1, 2, 3, \ldots,$$

где $\mathbb{N}_n$ — множество натуральных чисел размера n; $S_n = S \cap \mathbb{N}_n$. Здесь для любого конечного множества через $|A|$ обозначено число его элементов. Легко проверить, что $|\mathbb{N}_n| = 2^{n-1}$.

Асимптотической плотностью множества S назовём верхний предел

$$\rho(S) = \overline{\lim_{n\to\infty}} \rho_n(S).$$

Множество S называется *генерическим*, если $\rho(S) = 1$, и *пренебрежимым*, если $\rho(S) = 0$. Назовём множество S *сильно пренебрежимым*, если последовательность $\rho_n(S)$ экспоненциально быстро сходится к нулю, т. е. существуют константы σ, $0 < \sigma < 1$, и $C > 0$, такие, что для любого n

$$\rho_n(S) < C\sigma^n.$$

Множество S называется *сильно генерическим*, если его дополнение $\mathbb{N} \setminus S$ сильно пренебрежимо.

Алгоритм $\mathcal{A} : \mathbb{N} \to \mathbb{N} \cup \{?\}$ называется (*сильно*) *генерическим*, если:

1) $\mathcal{A}$ останавливается на всех входах из $\mathbb{N}$;
2) множество $\{x \in \mathbb{N} : \mathcal{A}(x) \neq ?\}$ является (сильно) генерическим.

Генерический алгоритм $\mathcal{A}$ вычисляет функцию $f : \mathbb{N} \to \mathbb{N}$, если для всех $x \in \mathbb{N}$

$$\big(\mathcal{A}(x) \neq ?\big) \ \Rightarrow \big(\mathcal{A}(x) = f(x)\big).$$

Имеется существенное различие между генерически разрешимыми проблемами и сильно генерически разрешимыми проблемами. Для сильно генерического полиномиального алгоритма нет эффективного метода случайной генерации входов, на которых этот алгоритм не может решить проблему. Допустим, имеется проблема S, разрешимая на некотором разрешимом за полиномиальное время генерическом множестве $G \subseteq \mathbb{N}$, для которого

$$\frac{|G \cap \mathbb{N}_n|}{|\mathbb{N}_n|} = \frac{n-1}{n}.$$

Таким образом, G — генерическое, но не сильно генерическое множество. Теперь хоть и проблема S разрешима для почти всех входов, тем не менее есть эффективный способ получить «плохой» вход, на котором генерический алгоритм не работает. Полиномиальный алгоритм для генерации плохих входов следующий:

1) сгенерировать равномерно случайный вход x размера n;
2) если $x \in G$, повторить шаг 1, иначе закончить.

Действительно, вероятность получить только хорошие входы за n^2 раундов равна

$$\left(\frac{n-1}{n}\right)^{n^2} = \left(\left(1 - \frac{1}{n}\right)^n\right)^n \to e^{-n}.$$

Поэтому с вероятностью, очень близкой к 1, будет получен плохой вход. С другой стороны, легко видеть, что если проблема разрешима на сильно генерическом множестве, то такой алгоритм генерации потребует экспоненциального числа раундов и

будет неэффективным. Для приложений к криптографии это означает, что просто генерическая легкоразрешимость проблемы не делает эту проблему бесполезной для создания на ее основе криптосистемы, так как для неё существует эффективная процедура генерации трудных входов. В то же время сильно генерически легкоразрешимые проблемы в этом смысле бесполезны для криптографии.

Напомним некоторые понятия классической теории сложности вычислений [8]. *Время работы* $t_M(x)$ машины Тьюринга M на входе $x \in \mathbb{N}$ — это число шагов машины от начала работы до остановки. Машина Тьюринга M *полиномиальна*, если существует полином $p(n)$, такой, что для любого $x \in \mathbb{N}$ имеет место $t_M(x) < p(\mathrm{size}(x))$. Класс P состоит из подмножеств $\mathbb{N}$, распознаваемых полиномиальными машинами Тьюринга.

Вероятностная машина Тьюринга — это машина Тьюринга, в программе которой допускаются пары недетерминированных правил, которые одновременно применимы в данной ситуации. В процессе работы такой машины с вероятностью $1/2$ выбирается первое правило и с вероятностью $1/2$ — второе.

Время работы $t_M(x, \tau)$ вероятностной машины Тьюринга на входе x зависит от вычислительного пути (последовательности выполненных команд) τ. Вероятностная машина Тьюринга M называется *полиномиальной*, если существует полином $p(n)$, такой, что для любого x и для любого вычислительного пути τ машины M на x имеет место $t_M(x, \tau) < p(\mathrm{size}(x))$.

Обозначим через $\Pr[M(x) = y]$ вероятность того, что машина M на входе x выдаёт ответ y. Вероятностная машина M *вычисляет* функцию $f : \mathbb{N} \to \mathbb{N}$, если для любого $x \in \mathbb{N}$ имеет место

$$\big(f(x) = y\big) \;\Rightarrow \Pr[M(x) = y] > 2/3.$$

Проблема распознавания множества $S \subseteq \mathbb{N}$ принадлежит классу BPP, если существует вероятностная полиномиальная машина Тьюринга M, вычисляющая характеристическую функцию множества S:

$$\chi_S(x) = \begin{cases} 1, & \text{если } x \in S, \\ 0, & \text{если } x \notin S. \end{cases}$$

Вероятностные машины Тьюринга формализуют понятие алгоритма, использующего генератор случайных чисел. Класс BPP — это класс проблем, эффективно решаемых такими вероятностными алгоритмами.

2. Функция Эйлера

Функция Эйлера $\varphi(x)$ для любого натурального числа x возвращает количество натуральных чисел, меньших x и взаимно простых с x. Важным свойством этой функции является её мультипликативность: для любых взаимно простых x и y имеет место $\varphi(xy) = \varphi(x)\varphi(y)$. Если $x = p_1^{k_1} \dots p_m^{k_m}$ — разложение числа x по степеням простых, то

$$\varphi(x) = (p_1^{k_1} - p_1^{k_1-1}) \dots (p_m^{k_m} - p_m^{k_m-1}) = x\Big(1 - \frac{1}{p_1}\Big) \dots \Big(1 - \frac{1}{p_m}\Big). \tag{1}$$

В частности, $\varphi(p) = p - 1$ для любого простого p.

Формула (1) показывает связь проблемы вычисления функции Эйлера с известной проблемой факторизации (разложения на множители) целых чисел: если бы существовал полиномиальный алгоритм для проблемы факторизации, то его можно было бы использовать для эффективного вычисления функции Эйлера. Однако до сих пор для этих двух проблем неизвестно полиномиальных алгоритмов [5].

Лемма 1. Существует полиномиальный алгоритм, который для любого натурального числа x и любого простого p, такого, что p не делит x, по входу $(x, p, \varphi(xp))$ находит значение $\varphi(x)$.

Доказательство. Из свойства мультипликативности функции Эйлера следует, что $\varphi(xp) = (p-1)\varphi(x)$. Таким образом, искомый полиномиальный алгоритм работает следующим образом: на вход ему подаются числа x, p и $\varphi(xp)$; алгоритм делит $\varphi(xp)$ на $p-1$ и находит значение $\varphi(x)$. Это делается за полиномиальное от размеров чисел x, p и $\varphi(xp)$ время. ■

Для произвольного натурального числа a размера n определим множество

$$S(a) = \{pa : p \ - \text{простое}, \ \text{size}(p) = n^2\}.$$

Лемма 2. Для любого достаточно большого a имеет место

$$\frac{|S(a)|}{|\mathbb{N}_{n^2+n}|} > \frac{1}{n^2 2^{n+1}}.$$

Доказательство. Оценим снизу число $|S(a)|$. Заметим, что

$$|S(a)| = \pi(2^{n^2}) - \pi(2^{n^2-1}), \tag{2}$$

где функция $\pi(x)$ определяет число простых чисел, не превосходящих x. Из асимптотического закона распределения простых чисел следует, что для достаточно больших x имеют место оценки

$$0{,}9 \cdot \log e \cdot \frac{x}{\log x} < \pi(x) < 1{,}1 \cdot \log e \cdot \frac{x}{\log x},$$

где $\log x$ — двоичный логарифм x. Поэтому, учитывая (2), имеем

$$|S(a)| > 0{,}9 \cdot \log e \cdot \frac{2^{n^2}}{n^2} - 1{,}1 \cdot \log e \cdot \frac{2^{n^2-1}}{n^2-1} = \log e \cdot 2^{n^2-1}\left(\frac{1{,}8}{n^2} - \frac{1{,}1}{n^2-1}\right) >$$
$$> \log e \cdot 2^{n^2-1}\left(\frac{1{,}8}{n^2} - \frac{1{,}2}{n^2}\right) = \frac{0{,}6 \cdot \log e \cdot 2^{n^2-1}}{n^2} > \frac{2^{n^2-2}}{n^2}.$$

Так как $|\mathbb{N}_{n^2+n}| = 2^{n^2+n-1}$, получаем

$$\frac{|S(a)|}{|\mathbb{N}_{n^2+n}|} > \frac{2^{n^2-2}}{n^2 \cdot 2^{n^2+n-1}} = \frac{1}{n^2 2^{n+1}}.$$

Лемма 2 доказана. ■

Лемма 3. Полиномиальный алгоритм для вычисления функции Эйлера $\varphi(x)$ существует тогда и только тогда, когда существует полиномиальный алгоритм для распознавания множества $EF = \{(x, k) : \varphi(x) \leqslant k \leqslant x\}$.

Доказательство. Пусть существует полиномиальный алгоритм для вычисления функции Эйлера. Тогда для того, чтобы определить, принадлежит ли пара (x, k) множеству EF, надо просто вычислить значение $\varphi(x)$ и сравнить его с k.

Обратно, пусть существует полиномиальный алгоритм $\mathcal{A}$ для распознавания множества EF. Тогда для вычисления значения $\varphi(x)$ нужно действовать следующим образом:

1) $L := 1$, $R := x - 1$;
2) $C := [(L + R)/2]$;
3) если $(x, C) \in EF$, то $R := C$, иначе $L := C$;
4) если $L \neq R$, то вернуться на шаг 2, иначе перейти на шаг 5;
5) выдать $\varphi(x) = R$.

Здесь через $[x]$ обозначена целая часть числа x. В этом алгоритме на каждой итерации уточняются границы $L \leqslant \varphi(x) \leqslant R$ до тех пор, пока отрезок $[L, R]$ не «схлопнется» в точку и мы не получим точное значение $\varphi(x)$. Так как длина отрезка на каждой итерации делится пополам, число итераций ограничено значением $[\log x]$ — размером числа x. Поэтому алгоритм полиномиален. ■

3. Основной результат

Теорема 1. Если существует сильно генерический полиномиальный алгоритм, вычисляющий функцию Эйлера, то существует вероятностный полиномиальный алгоритм, вычисляющий функцию Эйлера на всём множестве входов.

Доказательство. Пусть существует сильно генерический полиномиальный алгоритм $\mathcal{A}$, вычисляющий функцию Эйлера. Построим по $\mathcal{A}$ вероятностный полиномиальный алгоритм $\mathcal{B}$, вычисляющий функцию Эйлера на всём множестве входов. На натуральном числе a размера n алгоритм $\mathcal{B}$ работает следующим образом:

1) Повторяет $4n^2$ раз шаги 2–9.
2) Генерирует случайно равновероятно натуральное нечётное число p размера n^2.
3) С помощью полиномиального алгоритма Агравала — Каяла — Саксены [9] проверяет, является ли p простым числом.
4) Если p простое, переходит на шаг 7.
5) Возвращается на шаг 2.
6) Если за $4n^2$ шагов не получено простое число, то останавливается и выдаёт ответ 0.
7) Иначе запускает алгоритм $\mathcal{A}$ на числе ap.
8) Если $\mathcal{A}(ap) = \varphi(ap)$, то, по лемме 1, находит за полиномиальное время значение функции Эйлера для a.
9) Если $\mathcal{A}(ap) = ?$, то выдаёт ответ 0.

Заметим, что полиномиальный вероятностный алгоритм $\mathcal{B}$ выдаёт правильный ответ на шаге 8, а на шагах 6 и 9 — неправильный. Нужно доказать, что вероятность того, что ответ выдаётся на шаге 6 или шаге 9, меньше $1/3$.

Оценим вероятность выдачи ответа на шаге 6. Это бывает, только если за n^2 раундов генерации числа p не было получено простое число. Вероятность того, что простое число не получается за один раунд, равна

$$1 - \frac{\pi(2^{n^2}) - \pi(2^{n^2-1})}{2^{n^2-1}} < 1 - \frac{2^{n^2-2}}{n^2 \cdot 2^{n^2-1}} = 1 - \frac{1}{2n^2}.$$

Здесь верхняя оценка получается аналогично доказательству леммы 2. Вероятность того, что простое число не получится за все $4n^2$ раундов, не превосходит

$$\left(1 - \frac{1}{2n^2}\right)^{4n^2} < e^{-2} < 0{,}15.$$

Оценим теперь вероятность выдачи ответа на шаге 9. Число a имеет размер n, значит, размер числа ap равен n^2+n. Вероятность того, что $\mathcal{A}(ap)=?$, не больше

$$\frac{|\{x\in\mathbb{N}:\mathcal{A}(x)=?\}_{n^2+n}|}{|S(a)|}=\frac{|\{x\in\mathbb{N}:\mathcal{A}(x)=?\}_{n^2+n}|}{|\mathbb{N}_{n^2+n}|}\,\frac{|\mathbb{N}_{n^2+n}|}{|S(a)|}.$$

По лемме 2

$$\frac{|\mathbb{N}_{n^2+n}|}{|S(a)|}<n^2 2^{n+1}.$$

Так как множество $\{x\in\mathbb{N}:\mathcal{A}(x)=?\}$ сильно пренебрежимое, то существует константа $\alpha>0$, такая, что

$$\frac{|\{x\in\mathbb{N}:\mathcal{A}(x)=?\}_{n^2+n}|}{|\mathbb{N}_{n^2+n}|}<\frac{1}{2^{\alpha(n^2+n)}}$$

для любого n. Поэтому искомая вероятность ответа на шаге 9 не больше

$$\frac{n^2 2^{n+1}}{2^{\alpha(n^2+n)}}=\frac{n^2}{2^{\alpha(n^2+n)-n-1}}<0{,}15$$

при больших n. Таким образом, вероятность ответа на шагах 6 и 9 не превосходит $0{,}15+0{,}15<1/3$. ■

Теорема 2. Если для вычисления функции Эйлера не существует полиномиального алгоритма и P = BPP, то для её вычисления не существует сильно генерического полиномиального алгоритма.

Доказательство. Пусть существует сильно генерический алгоритм, вычисляющий функцию Эйлера. Тогда, по теореме 1, существует вероятностный полиномиальный алгоритм, вычисляющий её на всём множестве входов. Этот же алгоритм решает проблему распознавания множества EF, которая, по лемме 3, полиномиально эквивалентна проблеме вычисления функции Эйлера. Таким образом, проблема EF лежит в классе BPP. Так как P = BPP, то она лежит и в классе P, а значит, для проблемы вычисления функции Эйлера существует полиномиальный алгоритм. Противоречие. ■

ЛИТЕРАТУРА

1. *Kapovich I., Miasnikov A., Schupp P., and Shpilrain V.* Generic-case complexity, decision problems in group theory and random walks // J. Algebra. 2003. V. 264. No. 2. P. 665–694.
2. *Рыбалов А. Н.* О генерической сложности проблемы распознавания квадратичных вычетов // Прикладная дискретная математика. 2015. № 2 (28). С. 54–58.
3. *Рыбалов А. Н.* О генерической сложности проблемы дискретного логарифма // Прикладная дискретная математика. 2016. № 3 (33). С. 93–97.
4. *Рыбалов А. Н.* О генерической сложности проблемы извлечения корня в группах вычетов // Прикладная дискретная математика. 2017. № 38. С. 95–100.
5. *Adleman L. M. and McCurley K. S.* Open problems in number theoretic complexity, II // LNCS. 1994. V. 877. P. 291–322.
6. *Rivest R., Shamir A., and Adleman L.* A method for obtaining digital signatures and public-key cryptosystems // Commun. ACM. 1978. V. 21. Iss. 2. P. 120–126.
7. *Impagliazzo R. and Wigderson A.* P = BPP unless E has subexponential circuits: Derandomizing the XOR Lemma // Proc. 29th STOC. El Paso, ACM, 1997. P. 220–229.
8. *Вялый М., Китаев А., Шень А.* Классические и квантовые вычисления. М.: МЦНМО, ЧеРо. 1999. 192 с.
9. *Agrawal M., Kayal N., and Saxena N.* PRIMES is in P // Ann. Math. 2004. V. 160. No. 2. P. 781–793.

REFERENCES

1. *Kapovich I., Miasnikov A., Schupp P., and Shpilrain V.* Generic-case complexity, decision problems in group theory and random walks. J. Algebra, 2003, vol. 264, no. 2, pp. 665–694.
2. *Rybalov A. N.* O genericheskoy slozhnosti problemy raspoznavaniya kvadratichnykh vychetov [On generic complexity of the quadratic residuosity problem]. Prikladnaya Diskretnaya Matematika, 2015, no. 2 (28), pp. 54–58. (in Russian)
3. *Rybalov A. N.* O genericheskoy slozhnosti problemy diskretnogo logarifma [On generic complexity of the discrete logarithm problem]. Prikladnaya Diskretnaya Matematika, 2016, no. 3 (33), pp. 93–97. (in Russian)
4. *Rybalov A. N.* O genericheskoy slozhnosti problemy izvlecheniya kornya v gruppakh vychetov [On generic complexity of the problem of finding roots in groups of residues]. Prikladnaya Diskretnaya Matematika, 2017, no. 38, pp. 95–100. (in Russian)
5. *Adleman L. M. and McCurley K. S.* Open problems in number theoretic complexity, II. LNCS, 1994, vol. 877, pp. 291–322.
6. *Rivest R., Shamir A., and Adleman L.* A method for obtaining digital signatures and public-key cryptosystems. Commun. ACM, 1978, vol. 21, iss. 2, pp. 120–126.
7. *Impagliazzo R. and Wigderson A.* P = BPP unless E has subexponential circuits: Derandomizing the XOR Lemma. Proc. 29th STOC, El Paso, ACM, 1997, pp. 220–229.
8. *Vyalyy M., Kitaev A., and Shen' A.* Klassicheskie i kvantovye vychisleniya [Classical and Quantum Computations]. Moscow, MCCME, CheRo, 1999. 192 p. (in Russian)
9. *Agrawal M., Kayal N., and Saxena N.* PRIMES is in P. Ann. Math., 2004, vol. 160, no. 2, pp. 781–793.

ВЫЧИСЛИТЕЛЬНЫЕ МЕТОДЫ В ДИСКРЕТНОЙ МАТЕМАТИКЕ

УДК 519.816 DOI 10.17223/20710410/65/7

О СТРУКТУРЕ ПРОСТРАНСТВА ВЕСОВ ГОЛОСУЮЩИХ ПРОЦЕДУР

С. К. Иванов

Московский государственный университет технологий и управления им. К. Г. Разумовского, г. Москва, Россия

E-mail: sergey.k.ivanov@gmail.com

Изучена структура пространства весов самодвойственных пороговых функций, используемых в процедурах голосования при принятии решений, для размерностей 2–6. Найдены экстремальные векторы многогранных конусов, представляющих эти пороговые функции в пространстве весов.

Ключевые слова: *голосующие процедуры, алгоритмы голосования, пороговые фукции, принятие решений.*

ON A STRUCTURE OF VOTING PROCEDURES WEIGHTS SPACE

S. K. Ivanov

Moscow State University of Technology and Management named after K. G. Razumovsky, Moscow, Russia

The structure of the self-dual threshold functions space of weights used in voting decision-making procedures has been studied for dimensions 2–6. Extremal vectors of polyhedral cones representing these threshold functions in the space of weights have been found.

Keywords: *voting procedures, voting algorithms, threshold functions, decision making.*

Введение

Исторически изучение процедур голосования при принятии решений (которые далее кратко будем называть просто голосующими процедурами) восходит к работам Н. Кондорсе [1] и А. Пуанкаре [2]. Кондорсе систематически изучил правило голосования по большинству с вероятностной точки зрения и применил его к практике анализа свидетельских показаний и вынесения решений присяжными. Позже Пуанкаре критиковал его за склонность слишком прямолинейно применять абстрактные вероятностные результаты к реальной жизни человеческих судебных процессов. Но во времена Кондорсе трудно было найти область применения его исследований вне гуманитарных наук.

Ситуация коренным образом изменилась в XX в., когда вопрос достоверности остро встал практически в каждой задаче, связанной с приёмом сообщений, распознаванием образов, принятием решений и другими видами обработки информации. Общий подход к решению этих проблем, предполагающий дублирование информационных каналов и использование мажоритарного голосования для принятия решений, впервые появился, по-видимому, в работе фон Неймана [3], рассматривавшего проблему повышения надёжности логических автоматов. В. Пирс [4] изучил общее взвешенное голосование, нашёл оптимальное решающее правило для случая независимых голосователей и предложил принцип самообучения для взвешенного голосования, подразумевающий подстройку весов на основании результатов сравнения решения проголосовавшей системы с решениями отдельных голосователей.

Описанный подход может использоваться во многих ситуациях, таких, как: а) экспертные решения или анализ показаний свидетелей; б) распознавание образов, когда одновременно используются разные алгоритмы распознавания; в) логические схемы, которые используют резервные блоки для повышения надёжности; г) многоканальные системы телеметрии и радиосвязи с разнесением каналов, например по несущей частоте, и т. д.

С формальной точки зрения голосующие процедуры описываются самодвойственными пороговыми булевыми функциями с положительными весами. В [5–7] изучены различные аспекты голосующих процедур, включая вероятностные характеристики их надёжности и процессы обучения и самообучения соответствующих пороговых функций. В работе [8] получена асимптотика логарифма числа пороговых функций, которая была несколько улучшена в [9]. Кроме того, достаточно полный обзор теории пороговых функций можно найти, например, в [10, 11]. Многие полученные к настоящему времени результаты носят асимптотический характер. Это обусловлено упрощением математической техники при таком подходе. Однако с точки зрения приложений представляет особый интерес получение точных результатов для конечных размерностей, возможно, с применением численных методов. Численные методы в теории пороговых функций с успехом применялись для определения количества различных классов пороговых функций [11, 12].

Для того чтобы перейти к рассмотрению характеристик взвешенного голосования для конечных размерностей, необходимо прежде понять структуру пространства их весов. Каждой самодвойственной пороговой функции с положительными весами соответствует некоторый многогранный конус, лежащий в неотрицательном ортанте пространства весов. При этом конусы весов всех таких функций заполняют весь ортант. Такие конусы являются зонами нечувствительности голосующих процедур к изменению весов соответствующих им пороговых функций, т. е. если рассматривать вероятность ошибки принятия решения как функцию вектора весов, то она имеет дискретный (ступенчатый) вид. Получение информации о явном виде этих зон нечувствительности полезно для разработки и анализа алгоритмов самообучения систем, основанных на принципе взвешенного голосования. Указанные конусы весов задаются экстремальными векторами, выпуклыми оболочками которых они являются. Экстремальные векторы могут быть найдены как решения некоторых систем однородных линейных неравенств, что позволяет перечислить и в явном виде указать все конусы.

Данная работа посвящена нахождению экстремальных векторов для нескольких конечных размерностей. Для практических надобностей, как правило, используются нечётные размерности и бывает вполне достаточно голосующих процедур размерности 5.

1. Голосующие процедуры принятия решений

Традиционно при анализе голосующих процедур принятия решений мы рассматриваем абстрактную информационную систему, состоящую из n каналов, по которым передаются одни и те же данные в виде двоичных символов. Реальная природа канала не представляет интереса. Это может быть отдельный эксперт, свидетель, алгоритм распознавания, радиоканал и т. п. Когда символ $z \in \{-1, 1\}$ передаётся по каждому из n каналов, на выходе i-го канала появляется некоторый символ $y_i \in \{-1, 1\}$, из-за шумов в канале не обязательно совпадающий с z. Возникает задача отыскания булевой функции $f(\mathbf{y}) = f(y_1, \ldots, y_n) : \{-1, 1\}^n \to \{-1, 1\}$, дающей наиболее надёжную оценку z.

Даже не имея информации о вероятностях ошибок в каналах, можно тем не менее провести некоторый качественный анализ.

Во-первых, если нет информации о каналах и нет причин предпочесть один канал другому, нужно выбрать $f(\mathbf{y})$, которая не меняет значения ни при каких перестановках аргументов, т. е. $f(\mathbf{y})$ должна быть симметричной.

Во-вторых, если мы считаем многоканальную информационную систему симметричной относительно 1 и -1, то $f(\mathbf{y})$ должна удовлетворять соотношению $f(-\mathbf{y}) = -f(\mathbf{y})$, т. е. $f(\mathbf{y})$ должна быть самодвойственной.

В-третьих, если каналы не являются «лжецами», нужно выбрать такую $f(\mathbf{y})$, которая не уменьшается при замене некоторого из y_i с -1 на 1, т. е. $f(\mathbf{y})$ должна быть монотонной. Оказывается, что при чётном n такой функции нет, а при нечётном n единственной булевой функцией, удовлетворяющей этим трём требованиям, является мажоритарная пороговая функция $f(\mathbf{y}) = \operatorname{sign}(y_1 + y_2 + \ldots + y_n)$.

Действительно, для каждого $\mathbf{y} \in \{-1, 1\}^n$ обозначим через $|\mathbf{y}|$ количество компонент, равных 1, и положим $L_i = \{\mathbf{y} \in \{-1, 1\}^n : |\mathbf{y}| = i\}$. Поскольку $f(\mathbf{y})$ симметрична, она постоянна на каждом L_i. Кроме того, $f(\mathbf{y})$ монотонна, так что если $f(\mathbf{y}) = 1$ на L_i, то $f(\mathbf{y}) = 1$ на L_j при всех $j > i$. Пусть $f(\mathbf{y}) = -1$ на L_k и $f(\mathbf{y}) = 1$ на L_{k+1}. Из самодвойственности $f(\mathbf{y})$ следует, что $f(\mathbf{y}) = -1$ на L_{n-k-1} и $f(\mathbf{y}) = 1$ на L_{n-k}. Отсюда следует, что $n - k = k + 1$, то есть $n = 2k + 1$ и $f(\mathbf{y})$ является мажоритарной функцией. Этот результат в некоторой степени объясняет, почему голосование по большинству так широко используется.

Для получения более полного представления о состоянии дел в данной предметной области приведём ряд результатов, следуя [5–7]. Предполагается, что $\Pr[z = 1] = \Pr[z = -1] = 1/2$, $\Pr[y_i = 1 \,|\, z = 1] = \Pr[y_i = -1 \,|\, z = -1] = p_i \geqslant 1/2$, каналы статистически независимы, $n = 2k + 1$.

Теорема 1. При $p_1 = \ldots = p_n$ принятие решения большинством голосов (то есть использование мажоритарной функции) является оптимальным решающим правилом, минимизирующим вероятность ошибки.

Это частный случай следующей более общей теоремы.

Теорема 2. Оптимальное решающее правило, минимизирующее вероятность ошибки, даёт самодвойственная пороговая булева функция вида

$$f(\mathbf{y}) = \operatorname{sign}(\mathbf{a}, \mathbf{y}) = \operatorname{sign}(a_1 y_1 + \ldots + a_n y_n),$$

где $a_i = \log(p_i/(1 - p_i))$, $i = 1, \ldots, n$.

Теорема 3. Если $1/2 < m \leqslant p_i \leqslant M < 1$, $i = 1, \ldots, n$, а $\mathrm{Pr}_{\mathrm{err}}$ — вероятность ошибки при использовании оптимального решающего правила, то

$$\frac{1-M}{M}\binom{n}{[n/2]}\prod_{i=1}^{n}\sqrt{p_i(1-p_i)} \leqslant \mathrm{Pr}_{\mathrm{err}} \leqslant \frac{m}{2m-1}\binom{n}{[n/2]}\prod_{i=1}^{n}\sqrt{p_i(1-p_i)}.$$

Теорема 4. Пусть $\mathrm{Pr}_{\mathrm{err}}$ — вероятность ошибки для решающего правила, задаваемого самодвойственной пороговой функцией $f(\mathbf{y}) = \mathrm{sign}(\mathbf{a}, \mathbf{y}) = \mathrm{sign}(a_1 y_1 + \ldots + a_n y_n)$ с произвольным вектором весов $\mathbf{a}$. Тогда имеют место следующие оценки:

— если $(\mathbf{a}_\beta, \mathbf{a}) \geqslant 0$, то $\mathrm{Pr}_{\mathrm{err}} \leqslant \exp\big(-(\mathbf{a}_\beta, \mathbf{a}^{(0)})^2/2\big)$;

— если $(\mathbf{a}_\pi, \mathbf{a}) \geqslant 0$, то $\mathrm{Pr}_{\mathrm{err}} \leqslant \prod\limits_{i=1}^{n} 2\sqrt{p_i(1-p_i)}\exp\big((\mathbf{a}_\pi^2 - (\mathbf{a}_\pi, \mathbf{a}^{(0)})^2)/2\big)$.

Здесь $\mathbf{a}_\beta = (2p_1 - 1, \ldots, 2p_n - 1)$; $\mathbf{a}_\pi = \left(\frac{1}{2}\log\left(\frac{p_1}{1-p_1}\right), \ldots, \frac{1}{2}\log\left(\frac{p_n}{1-p_n}\right)\right)$; $\mathbf{a}^{(0)} = \mathbf{a}/|\mathbf{a}|$ — нормированный вектор весов.

Если веса фиксированы по величине, но могут переставляться, то вероятность ошибки является функцией перестановки весов. Пусть $a_1 \geqslant a_2 \geqslant \ldots \geqslant a_n$, $p_1 \geqslant p_2 \geqslant \ldots \geqslant p_n$, $\mathbb{S}_n$ — симметрическая группа перестановок множества $\{1, \ldots, n\}$. Обычным образом определим для перестановки $\sigma \in \mathbb{S}_n$ множество беспорядков $\mathbf{X}(\sigma)$: $(\sigma(i_1), \sigma(i_2)) \in \mathbf{X}(\sigma) \Leftrightarrow i_1 \leqslant i_2 \;\&\; \sigma(i_1) \geqslant \sigma(i_2)$. Пусть $\prec$ — отношение частичного порядка на $\mathbb{S}_n$: $\sigma_1 \prec \sigma_2 \Leftrightarrow \mathbf{X}(\sigma_1) \subseteq \mathbf{X}(\sigma_2)$. Минимальным элементом является тождественная перестановка, максимальным — обратная.

Теорема 5. Вероятность ошибки — монотонная функция по отношению к частичному порядку $\prec$, то есть $\sigma_1 \prec \sigma_2 \Rightarrow P(\sigma_1) \leqslant P(\sigma_2)$.

В условиях теоремы 5 можно рассматривать выбор весов как двухходовую игру человека с природой, в которой человек делает первый ход, выбором весов a_i минимизируя вероятность ошибки, а природа делает второй ход, максимизируя её перестановкой вероятностей p_i.

Теорема 6. Оптимальная стратегия человека состоит в том, чтобы выбирать равные веса, т. е. использовать правило голосования по большинству; оптимальная стратегия природы заключается в использовании обратной перестановки вероятностей.

2. Пространство весов

Самодвойственной пороговой функции $f(\mathbf{y}) = \mathrm{sign}(\mathbf{a}, \mathbf{y})$ соответствует система из 2^n неравенств вида

$$f(\mathbf{y})(\mathbf{a}, \mathbf{y}) = f(\mathbf{y})(a_1 y_1 + \ldots + a_n y_n) > 0,$$

где $\mathbf{y} = (y_1, \ldots, y_n)$ пробегает весь набор элементов множества $\{-1, 1\}^n$. Эта система определяет все значения весов $\mathbf{a}$, допустимые для $f(\mathbf{y})$. Обратно, каждая совместная система неравенств вида $S(\mathbf{y})(\mathbf{a}, \mathbf{y}) > 0$, где $S(\mathbf{y})$ — заданное для вектора $\mathbf{y}$ значение, равное 1 или -1, определяет самодвойственную пороговую функцию $S(\mathbf{y}) = \mathrm{sign}(\mathbf{a}, \mathbf{y})$, а решения системы — допустимые для неё веса $\mathbf{a}$.

Общее неотрицательное решение $\mathbf{a}$ однородной системы линейных неравенств

$$c_{i1}a_1 + c_{i2}a_2 + \ldots + c_{in}a_n \geqslant 0, \qquad i = 1, 2, \ldots, m, \tag{1}$$

представляет собой многогранный конус [13], то есть линейную комбинацию вида $\mathbf{a} = \sum\limits_{i=1}^{s} \lambda_i \mathbf{a}_i$, где векторы $\mathbf{a}_i$ — базисные неотрицательные решения этой системы

и $\lambda_i \geqslant 0$. Назовём вырожденным вектором весов вектор, для которого в (1) достигается равенство. Очевидно, такие векторы могут появляться только на границе конуса. Это соответствует случаю, когда задающая самодвойственную пороговую функцию гиперплоскость проходит через некоторую вершину булева куба. Требование $\lambda_i > 0$ устраняет вырожденные векторы из рассмотрения. Чтобы избежать появления вырожденных пороговых функций размерности меньше n, мы должны рассматривать только системы неравенств, для которых $s \geqslant n$.

Таким образом, в пространстве весов каждая самодвойственная пороговая функция представлена выпуклым многогранным конусом размерности n, экстремальными векторами которого являются $\mathbf{a}_i$. В качестве характеристического вектора весов самодвойственной пороговой функции $f(\mathbf{y})$ удобно взять барицентрический вектор её конуса весов $\mathbf{a}^{(\beta)} = \sum_{i=1}^{s} \mathbf{a}_i$. Отметим, что если добавить к нему s в качестве нулевой компоненты, то получим обобщённый вектор параметров Чоу [10] для множества $\{\mathbf{a}_1, \ldots, \mathbf{a}_s\}$, что является дополнительным аргументом в пользу выбора $\mathbf{a}^{(\beta)}$ для характеризации $f(\mathbf{y})$. Задавшись некоторым вектором весов, с помощью выражения $f(\mathbf{y}) = \operatorname{sign}(\mathbf{a}, \mathbf{y})$ можно легко построить таблицу истинности для $f(\mathbf{y})$.

Утверждение 1. Рассмотрим две различные самодвойственные пороговые функции f_1 и f_2 размерности n. Пусть A_1 и A_2 — их конусы весов. Тогда $\dim(A_1 \cap A_2) < n$.

Доказательство. При $A_1 \cap A_2 = \varnothing$ имеем $\dim(A_1 \cap A_2) = 0 < n$.

Максимальная размерность границ конусов равна $(n-1)$, поскольку каждый такой конус является пересечением конечного числа полупространств [14], а полупространство задаётся гиперплоскостью размерности $(n-1)$. То есть если A_1 и A_2 — «соседи», имеющие общую границу, то $\dim(A_1 \cap A_2) = (n-1) < n$.

Обозначим A_1^0 и A_2^0 внутренние части рассматриваемых конусов, то есть множества векторов весов вида $\mathbf{a} = \sum_{i=1}^{s} \lambda_i \mathbf{a}_i$, где $\lambda_i > 0$, и предположим, что $A_1^0 \cap A_2^0 \neq \varnothing$. Тогда в этом пересечении можно выбрать невырожденный характеристический вектор весов, общий для f_1 и f_2, с помощью которого построить таблицы истинности, одинаковые для f_1 и f_2. Полученное противоречие завершает доказательство. ■

Утверждение 2. Объединение многогранных конусов весов всех самодвойственных пороговых функций размерности n совпадает с неотрицательным ортантом n-мерного линейного пространства весов.

Доказательство. Предположим противное: разность между неотрицательным ортантом и объединением конусов не пуста. Неотрицательный ортант является замкнутым множеством размерности n. Каждый конус — также замкнутое множество размерности n. Поскольку рассматриваемых конусов имеется конечное число, то их объединение — также замкнутое множество размерности n. Отсюда следует, что непустая разность указанных множеств имеет размерность n. Тогда в этой разности можно выбрать невырожденный характеристический вектор весов, не принадлежащий ни одному из имеющихся конусов. Он задаёт самодвойственную пороговую функцию размерности n, не совпадающую ни с одной из имеющихся. Полученное противоречие завершает доказательство. ■

Рассмотрим симплекс n-мерного пространства весов. Как следует из утверждений 1 и 2, соответствующие самодвойственным пороговым функциям многогранные конусы разбивают симплекс на некоторые выпуклые многогранники и сумма объёмов этих

многогранников равна объёму симплекса. Такое представление может быть удобно для визуализации структуры пространства весов самодвойственных пороговых функций.

Итак, голосующие процедуры задаются самодвойственными пороговыми функциями. Число этих функций с ростом n очень быстро растёт. В табл. 1 приведены количества самодвойственных пороговых функций, согласно данным из [11].

Таблица 1

Число голосующих процедур

n	2	3	4	5	6	7
Число процедур	2	4	12	81	1684	123565

Для сокращения количества рассматриваемых структур и соответственно облегчения анализа и представления данных введём понятие алгоритма голосования. Зададим каждую самодвойственную пороговую функцию её характеристическим вектором весов (например, барицентрическим вектором $\mathbf{a}^{(\beta)}$) и рассмотрим группу подстановок, действующую на компонентах этих векторов.

Определим отношение R на множестве характеристических векторов весов следующим образом: $R(\mathbf{a}, \mathbf{b})$, если существует подстановка, переводящая вектор a в вектор b. Поскольку подстановки образуют группу, ясно, что R — отношение эквивалентности. Классы эквивалентности по отношению R будем называть алгоритмами голосования. Характеристическим представителем алгоритма голосования будем считать принадлежащий ему вектор весов $\mathbf{a}$, у которого $a_1 \geqslant a_2 \geqslant \ldots \geqslant a_n$. Из табл. 2, полученной в результате расчётов, видно, насколько меньше алгоритмов голосования, чем голосующих процедур.

Таблица 2

Число алгоритмов голосования

n	2	3	4	5	6
Число алгоритмов	1	2	3	7	19

Отметим, что та же подстановка, которая переводит характеристический вектор весов функции f_1 в характеристический вектор весов функции f_2, переводит и экстремальные векторы конуса весов f_1 в экстремальные векторы конуса весов f_2.

3. Отыскание экстремальных векторов

Процесс отыскания экстремальных векторов подразумевает двухэтапную процедуру. На первом этапе формируются системы линейных неравенств вида $S(\mathbf{y})(\mathbf{a}, \mathbf{y}) > 0$, где $\mathbf{y} = (y_1, \ldots, y_n)$ в каждой из них пробегает весь набор из $N = 2^n$ элементов множества $\{-1, 1\}^n$, а $S(\mathbf{y})$ в процессе формирования систем — весь набор из 2^N элементов множества $\{-1, 1\}^N$. Таким образом в итоге перечисляется полный комплект из 2^N систем из N линейных неравенств для определения $\mathbf{a} = (a_1, \ldots, a_n)$. Дубликаты неравенств из каждой системы устраняются. На втором этапе производится решение полученных систем неравенств.

Для отыскания экстремальных векторов применим алгоритм решения систем однородных линейных неравенств, предложенный в [15]. Рассмотрим систему неравенств (1), все c_{ij} равны 1 или -1. Отыскание экстремальных векторов сводится к по-

следовательным однотипным преобразованиям матрицы

$$\left\| \begin{array}{ccccccc} 1 & 0 & \cdots & 0 & c_{11} & \ldots & c_{m1} \\ 0 & 1 & \cdots & 0 & c_{12} & \ldots & c_{m2} \\ & & \cdots & & & \ldots & \\ 0 & 0 & \cdots & 1 & c_{1n} & \ldots & c_{mn} \end{array} \right\|,$$

в которой левая часть — единичная матрица n-го порядка, а правая — транспонированная матрица коэффициентов системы неравенств. Преобразования производятся по следующему правилу. За основной столбец матрицы принимается один из таких столбцов её правой части, в котором имеется хотя бы один отрицательный элемент (если такие столбцы есть).

В новую матрицу переносятся без изменения те строки, на пересечении которых с основным столбцом стоят неотрицательные числа (если такие строки есть).

Затем перебираются поочередно те пары строк, в которых элементы основного столбца имеют противоположные знаки. Для каждой такой пары просматриваются все столбцы левой части матрицы и неотрицательные столбцы правой части и проверяется, есть ли среди этих столбцов такие, на пересечении которых с обеими строками рассматриваемой пары стоят нули.

Если таких столбцов нет или если есть ещё хотя бы одна строка, на пересечении которой со всеми такими столбцами стоят нули, то рассматриваемая пара пропускается. В противном случае в новую матрицу переносится линейная комбинация рассматриваемой пары строк с такими положительными коэффициентами, чтобы её элемент в основном столбце оказался равным нулю.

Когда просмотр закончится, новая матрица принимается за исходную, по тому же правилу составляется следующая и так далее.

В том особом случае, когда матрица состоит из одной пары строк и знаки элементов основного столбца противоположны, указанный критерий отбора пар перестаёт действовать. В этом случае следует выбрать строку с положительным элементом в основном столбце, составить линейную комбинацию строк таблицы с положительными коэффициентами, подобранными с тем же расчётом, что и в общем случае, и сравнить её с выбранной строкой. Если эти вектор-строки коллинеарны, то указанная линейная комбинация в новую таблицу не включается, если не коллинеарны — включается.

После конечного числа шагов наступит одна из двух ситуаций, означающих конец процесса:

1) в очередной матрице все столбцы правой части неотрицательны;
2) в столбце матрицы, который принят за основной, все элементы отрицательны (так что следующая матрица пуста).

В первом случае вектор-строки левой части последней матрицы (взятые с произвольными положительными коэффициентами) составляют совокупность всех существенно различных экстремальных векторов конуса неотрицательных решений системы неравенств. Все неотрицательные её решения исчерпываются всевозможными линейными комбинациями этих векторов с неотрицательными коэффициентами. Таким образом, если $\mathbf{a}_1, \mathbf{a}_2, \ldots, \mathbf{a}_s$ — найденные экстремальные векторы, то искомая общая формула для решений рассмотренной системы имеет вид

$$\mathbf{a} = \lambda_1 \mathbf{a}_1 + \lambda_2 \mathbf{a}_2 + \ldots + \lambda_s \mathbf{a}_s; \quad \lambda_i \geqslant 0, \quad i = 1,\ 2,\ \ldots,\ s.$$

Во втором случае система имеет единственное неотрицательное решение — нулевое.

4. Проведение расчётов и их результаты

Расчёты производились с использованием программы, написанной на языке C#. Первая процедура для заданной размерности формирует системы линейных неравенств, подлежащие решению. Вторая процедура находит решение системы, если она оказывается совместной, и записывает в файл полученные экстремальные векторы каждого найденного алгоритма голосования и соответствующий характеристический вектор. В качестве характеристических векторов мы берём барицентрические векторы, все компоненты которых для упрощения поделены на общий целый множитель, если это оказалось возможным.

Тестирование программы производилось на контрольных примерах как в отдельности для проверки правильности формирования систем неравенств и проверки правильности их решения, так и в комплексе. В качестве контрольного примера для комплексного тестирования использовалось пространство весов размерности 3, достаточно ненапряжённо просчитывающееся вручную.

В табл. 3–7 приведены найденные экстремальные векторы многогранных конусов и соответствующие характеристические векторы для размерностей $n = 2, \ldots, 6$ и количество голосующих процедур для каждого алгоритма голосования, которое выражается полиномиальным коэффициентом, соответствующим данному характеристическому вектору. Суммарное их число для каждого n совпадает с данными табл. 1, что также говорит о точности расчётов.

Таблица 3

Результаты для $n = 2$

Алгоритм голосования	Экстремальные векторы	Характеристический вектор	Число голосующих процедур
1	(1, 0), (1, 1)	(2, 1)	$\frac{2!}{1! \cdot 1!} = 2$

Таблица 4

Результаты для $n = 3$

Алгоритм голосования	Экстремальные векторы	Характеристический вектор	Число голосующих процедур
1	(1, 0, 0), (1, 0, 1), (1, 1, 0)	(3, 1, 1)	$\frac{3!}{1! \cdot 2!} = 3$
2	(1, 0, 1), (0, 1, 1), (1, 1, 0)	(1, 1, 1)	$\frac{3!}{3!} = 1$

Таблица 5

Результаты для $n = 4$

Алгоритм голосования	Экстремальные векторы	Характеристический вектор	Число голосующих процедур
1	(1, 0, 0, 0), (1, 0, 0, 1), (1, 0, 1, 0), (1, 1, 0, 0)	(4, 1, 1, 1)	$\frac{4!}{1! \cdot 3!} = 4$
2	(1, 0, 0, 1), (1, 0, 1, 0), (1, 1, 0, 0), (1, 1, 1, 1)	(2, 1, 1, 1)	$\frac{4!}{1! \cdot 3!} = 4$
3	(1, 0, 1, 0), (0, 1, 1, 0), (1, 1, 0, 0), (1, 1, 1, 1)	(3, 3, 3, 1)	$\frac{4!}{3! \cdot 1!} = 4$

Таблица 6

Результаты для $n = 5$

Алгоритм голосования	Экстремальные векторы	Характеристический вектор	Число голосующих процедур
1	(1, 0, 0, 0, 0), (1, 0, 0, 0, 1), (1, 0, 0, 1, 0), (1, 0, 1, 0, 0), (1, 1, 0, 0, 0)	(5, 1, 1, 1, 1)	$\frac{5!}{1! \cdot 4!} = 5$
2	(1, 0, 0, 0, 1), (1, 0, 0, 1, 0), (1, 0, 1, 0, 0), (1, 1, 0, 0, 0), (2, 1, 1, 1, 1)	(3, 1, 1, 1, 1)	$\frac{5!}{1! \cdot 4!} = 5$
3	(1, 0, 0, 1, 0), (1, 0, 1, 0, 0), (1, 1, 0, 0, 0), (1, 1, 1, 1, 0), (2, 1, 1, 1, 1)	(6, 3, 3, 3, 1)	$\frac{5!}{1! \cdot 3! \cdot 1!} = 20$
4	(1, 0, 1, 0, 0), (1, 1, 0, 0, 0), (1, 1, 1, 0, 1), (1, 1, 1, 1, 0), (2, 1, 1, 1, 1)	(3, 2, 2, 1, 1)	$\frac{5!}{1! \cdot 2! \cdot 2!} = 30$
5	(0, 1, 1, 0, 0), (1, 0, 1, 0, 0), (1, 1, 0, 0, 0), (1, 1, 1, 0, 1), (1, 1, 1, 1, 0)	(4, 4, 4, 1, 1)	$\frac{5!}{3! \cdot 2!} = 10$
6	(1, 1, 0, 0, 0), (1, 1, 0, 1, 1), (1, 1, 1, 0, 1), (1, 1, 1, 1, 0), (1, 2, 1, 1, 1), (2, 1, 1, 1, 1)	(7, 7, 4, 4, 4)	$\frac{5!}{2! \cdot 3!} = 10$
7	(0, 1, 1, 1, 1), (1, 0, 1, 1, 1), (1, 1, 0, 1, 1), (1, 1, 1, 0, 1), (1, 1, 1, 1, 0), (2, 1, 1, 1, 1), (1, 2, 1, 1, 1), (1, 1, 2, 1, 1), (1, 1, 1, 2, 1), (1, 1, 1, 1, 2)	(1, 1, 1, 1, 1)	$\frac{5!}{5!} = 1$

Таблица 7

Результаты для $n = 6$

Алгоритм голосования	Экстремальные векторы	Характеристический вектор	Число голосующих процедур
1	2	3	4
1	(1, 0, 0, 0, 0, 0), (1, 0, 0, 0, 0, 1), (1, 0, 0, 0, 1, 0), (1, 0, 0, 1, 0, 0), (1, 0, 1, 0, 0, 0), (1, 1, 0, 0, 0, 0)	(6, 1, 1, 1, 1, 1)	$\frac{6!}{1! \cdot 5!} = 6$
2	(1, 0, 0, 0, 0, 1), (1, 0, 0, 0, 1, 0), (1, 0, 0, 1, 0, 0), (1, 0, 1, 0, 0, 0), (1, 1, 0, 0, 0, 0), (3, 1, 1, 1, 1, 1)	(4, 1, 1, 1, 1, 1)	$\frac{6!}{1! \cdot 5!} = 6$
3	(1, 0, 0, 0, 1, 0), (1, 0, 0, 1, 0, 0), (1, 0, 1, 0, 0, 0), (1, 1, 0, 0, 0, 0), (2, 1, 1, 1, 1, 0), (3, 1, 1, 1, 1, 1)	(9, 3, 3, 3, 3, 1)	$\frac{6!}{1! \cdot 4! \cdot 1!} = 30$
4	(1, 0, 0, 1, 0, 0), (1, 0, 1, 0, 0, 0), (1, 1, 0, 0, 0, 0), (2, 1, 1, 1, 0, 1), (2, 1, 1, 1, 1, 0), (3, 1, 1, 1, 1, 1)	(5, 2, 2, 2, 1, 1)	$\frac{6!}{1! \cdot 3! \cdot 2!} = 60$
5	(1, 0, 0, 1, 0, 0), (1, 0, 1, 0, 0, 0), (1, 1, 0, 0, 0, 0), (1, 1, 1, 1, 0, 0), (2, 1, 1, 1, 0, 1), (2, 1, 1, 1, 1, 0)	(8, 4, 4, 4, 1, 1)	$\frac{6!}{1! \cdot 3! \cdot 2!} = 60$
6	(1, 0, 1, 0, 0, 0), (1, 1, 0, 0, 0, 0), (2, 1, 1, 0, 1, 1), (2, 1, 1, 1, 0, 1), (2, 1, 1, 1, 1, 0), (3, 2, 2, 1, 1, 1), (3, 1, 1, 1, 1, 1)	(14, 7, 7, 4, 4, 4)	$\frac{6!}{1! \cdot 2! \cdot 3!} = 60$

Окончание табл. 7

1	2	3	4
7	(1, 0, 1, 0, 0, 0), (1, 1, 0, 0, 0, 0), (1, 1, 1, 1, 0, 0), (2, 1, 1, 1, 0, 1), (2, 1, 1, 1, 1, 0), (3, 2, 2, 1, 1, 1)	(5, 3, 3, 2, 1, 1)	$\frac{6!}{1!\cdot 2!\cdot 1!\cdot 2!} = 180$
8	(1, 0, 1, 0, 0, 0), (1, 1, 0, 0, 0, 0), (1, 1, 1, 0, 1, 0), (1, 1, 1, 1, 0, 0), (2, 1, 1, 1, 1, 0), (3, 2, 2, 1, 1, 1)	(9, 6, 6, 3, 3, 1)	$\frac{6!}{1!\cdot 2!\cdot 2!\cdot 1!} = 180$
9	(1, 0, 1, 0, 0, 0), (1, 1, 0, 0, 0, 0), (1, 1, 1, 0, 0, 1), (1, 1, 1, 0, 1, 0), (1, 1, 1, 1, 0, 0), (3, 2, 2, 1, 1, 1)	(4, 3, 3, 2, 2, 2)	$\frac{6!}{1!\cdot 2!\cdot 3!} = 60$
10	(1, 0, 1, 0, 0, 0), (0, 1, 1, 0, 0, 0), (1, 1, 0, 0, 0, 0), (1, 1, 1, 0, 0, 1), (1, 1, 1, 0, 1, 0), (1, 1, 1, 1, 0, 0)	(5, 5, 5, 1, 1, 1)	$\frac{6!}{3!\cdot 3!} = 20$
11	(1, 1, 0, 0, 0, 0), (1, 1, 1, 1, 0, 0), (2, 2, 1, 1, 1, 1), (2, 1, 1, 1, 0, 1), (2, 1, 1, 1, 1, 0), (3, 2, 1, 2, 1, 1), (3, 2, 2, 1, 1, 1)	(14, 10, 7, 7, 4, 4)	$\frac{6!}{1!\cdot 1!\cdot 2!\cdot 2!} = 180$
12	(1, 1, 0, 0, 0, 0), (1, 1, 1, 0, 1, 0), (1, 1, 1, 1, 0, 0), (2, 2, 1, 1, 1, 1), (2, 1, 1, 1, 1, 0), (3, 2, 2, 1, 1, 1)	(5, 4, 3, 2, 2, 1)	$\frac{6!}{1!\cdot 1!\cdot 1!\cdot 2!\cdot 1!} = 360$
13	(1, 1, 0, 0, 0, 0), (1, 1, 1, 0, 0, 1), (1, 1, 1, 0, 1, 0), (1, 1, 1, 1, 0, 0), (2, 3, 2, 1, 1, 1), (2, 2, 1, 1, 1, 1), (3, 2, 2, 1, 1, 1)	(11, 11, 8, 4, 4, 4)	$\frac{6!}{2!\cdot 1!\cdot 3!} = 60$
14	(1, 1, 0, 0, 0, 0), (1, 1, 0, 1, 1, 0), (1, 1, 1, 0, 1, 0), (1, 1, 1, 1, 0, 0), (1, 2, 1, 1, 1, 0), (2, 2, 1, 1, 1, 1), (2, 1, 1, 1, 1, 0)	(9, 9, 5, 5, 5, 1)	$\frac{6!}{2!\cdot 3!\cdot 1!} = 60$
15	(1, 1, 1, 1, 1, 1), (1, 1, 1, 1, 0, 0), (2, 1, 2, 1, 1, 1), (2, 2, 1, 1, 1, 1), (2, 1, 1, 2, 1, 1), (2, 1, 1, 1, 0, 1), (2, 1, 1, 1, 1, 0), (3, 1, 2, 2, 1, 1), (3, 2, 1, 2, 1, 1), (3, 2, 2, 1, 1, 1)	(21, 13, 13, 13, 8, 8)	$\frac{6!}{1!\cdot 3!\cdot 2!} = 60$
16	(1, 1, 1, 1, 1, 1), (1, 1, 1, 0, 1, 0), (1, 1, 1, 1, 0, 0), (2, 1, 2, 1, 1, 1), (2, 2, 1, 1, 1, 1), (2, 1, 1, 1, 1, 0), (3, 2, 2, 1, 1, 1)	(12, 9, 9, 6, 6, 4)	$\frac{6!}{1!\cdot 2!\cdot 2!\cdot 1!} = 180$
17	(1, 1, 1, 1, 1, 1), (1, 1, 1, 0, 0, 1), (1, 1, 1, 0, 1, 0), (1, 1, 1, 1, 0, 0), (2, 2, 3, 1, 1, 1), (1, 2, 2, 1, 1, 1), (2, 3, 2, 1, 1, 1), (2, 1, 2, 1, 1, 1), (2, 2, 1, 1, 1, 1), (3, 2, 2, 1, 1, 1)	(2, 2, 2, 1, 1, 1)	$\frac{6!}{3!\cdot 3!} = 20$
18	(1, 1, 1, 1, 1, 1), (1, 1, 0, 1, 1, 0), (1, 1, 1, 0, 1, 0), (1, 1, 1, 1, 0, 0), (1, 2, 1, 1, 1, 0), (2, 2, 1, 1, 1, 1), (2, 1, 1, 1, 1, 0)	(9, 9, 6, 6, 6, 2)	$\frac{6!}{2!\cdot 3!\cdot 1!} = 60$
19	(1, 0, 1, 1, 1, 0), (0, 1, 1, 1, 1, 0), (1, 1, 1, 1, 1, 1), (1, 1, 0, 1, 1, 0), (1, 1, 1, 0, 1, 0), (1, 1, 1, 1, 0, 0), (1, 1, 2, 1, 1, 0), (1, 2, 1, 1, 1, 0), (1, 1, 1, 2, 1, 0), (1, 1, 1, 1, 2, 0), (2, 1, 1, 1, 1, 0)	(11, 11, 11, 11, 11, 1)	$\frac{6!}{5!\cdot 1!} = 6$

На рис. 1 показаны разбиения соответствующих симплексов многогранными конусами векторов весов голосующих процедур для $n = 2$ и 3.

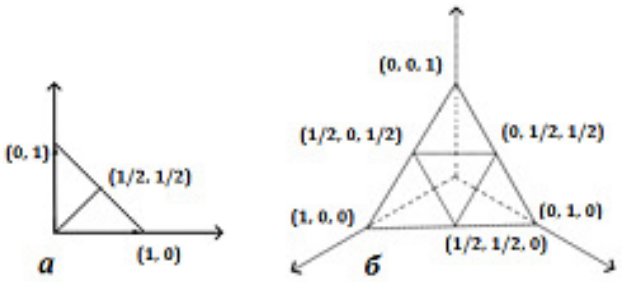

Рис. 1. Результаты для $n = 2$ ($а$) и 3 ($б$)

На рис. 2 показаны разбиения симплекса многогранными конусами голосующих процедур для $n = 4$.

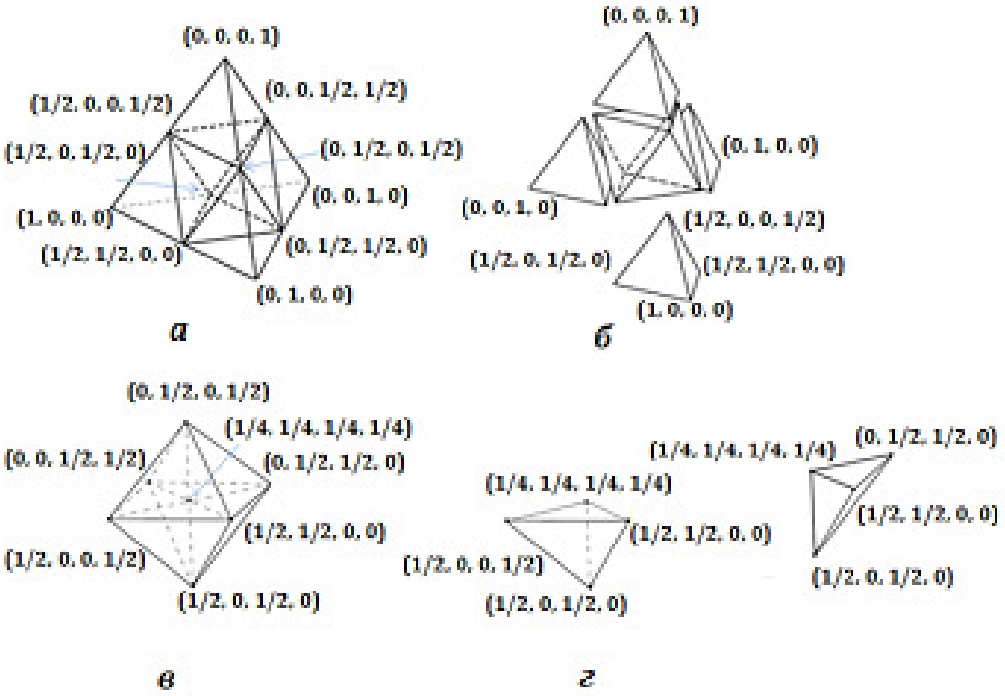

Рис. 2. Результаты для $n = 4$

На рис. 2,$а$ выделены разбиения, соответствующие голосующим процедурам, работающим по алгоритму голосования 1 (табл. 5). На рис. 2,$б$ отдельно показан многогранник, соответствующий характеристическому вектору весов этого алгоритма (для которого $a_1 \geqslant a_2 \geqslant \ldots \geqslant a_n$). На рис. 2,$в$ показаны дальнейшие разбиения симплекса, соответствующие голосующим процедурам, работающим по алгоритмам голосования 2 и 3 (табл. 5). На рис. 2,$г$ показаны многогранники, соответствующие характеристическим векторам весов данных алгоритмов голосования (для которых $a_1 \geqslant a_2 \geqslant \ldots \geqslant a_n$).

Заключение

В работе найдены экстремальные и характеристические векторы весов алгоритмов голосования размерностей 2–6 и определено количество голосующих процедур, соответствующих каждому алгоритму голосования. Для размерностей 2, 3 и 4 визуализированы разбиения симплексов конусами, соответствующими алгоритмам голосования и голосующим процедурам. В качестве следующего этапа мы рассмотрим разработ-

ку методов сокращения множества перебираемых систем неравенств для получения аналогичных результатов для размерностей 7–9.

ЛИТЕРАТУРА

1. *De Condorcet N.* Essai sur l'Application de l'Analyse a la Probabilite des Desisions Rendues a la Pluralite des Vox. Paris: 1785. 304 p. (in French)
2. *Poincare J. H.* Science et Methode. Paris: Ernest Flammarion, 1908. 308 p. (in French)
3. *Von Neumann J.* Probabilistic Logic and the Synthesis of Reliable Organisms from Unreliable Components. Princeton: Princeton University Press, 1956. 58 p.
4. *Pierce W. J.* Failure-Tolerant Computer Design. N.Y.: Academic Press, 1965. 256 p.
5. *Зуев Ю. А., Иванов С. К.* Взвешенное голосование в многоканальных системах передачи дискретных сигналов // Проблемы передачи информации. 1995. Т. 31. № 4. С. 22–36.
6. *Зуев Ю. А., Иванов С. К.* Обучение и самообучение в процедурах взвешенного голосования // Журн. вычисл. матем. и матем. физ. 1995. Т. 35. № 1. С. 104–121.
7. *Zuev Yu. A. and Ivanov S. K.* Voting as a way to increase the decision reliability // J. Franklin Institute. 1999. V. 336. No. 2. P. 361–378.
8. *Зуев Ю. А.* Асимптотика логарифма числа пороговых функций алгебры логики // Докл. АН СССР. 1989. Т. 306. № 3. С. 528–530.
9. *Ирматов А. А.* О числе пороговых функций // Дискретная математика. 1993. Т. 5. № 3. С. 40–43.
10. *Зуев Ю. А.* Пороговые функции и пороговые представления булевых функций // Математические вопросы кибернетики. 1994. № 3. С. 5–61.
11. *Muroga S.* Threshold Logic and its Applications. N.Y.: Wiley, 1971. 478 p.
12. *Muroga S., Tsuboi N., and Baugh R. S.* Enumeration of threshold functions of eight variables // IEEE Trans. Computers. 1970. V. C-19. No. 9. P. 818–825.
13. *Черников С. Н.* Линейные неравенства. М.: Наука, 1968. 488 с.
14. *Ziegler G. M.* Lectures on Polytopes. N.Y.: Springer Verlag, 1995. 370 p.
15. *Черникова Н. В.* Алгоритм для нахождения общей формулы неотрицательных решений системы линейных неравенств // Журн. вычисл. матем. и матем. физ. 1965. Т. 5. № 2. С. 334–337.
16. *Розенфельд Н. В.* Многомерные пространства. М.: Наука, 1966. 648 с.

REFERENCES

1. *De Condorcet N.* Essai sur l'Application de l'Analyse a la Probabilite des Desisions Rendues a la Pluralite des Vox. Paris, 1785. 304 p. (in French)
2. *Poincare J. H.* Science et Methode. Paris, Ernest Flammarion, 1908. 308 p. (in French)
3. *Von Neumann J.* Probabilistic Logic and the Synthesis of Reliable organisms from Unreliable Components. Princeton, Princeton University Press, 1956. 58 p.
4. *Pierce W. J.* Failure-Tolerant Computer Design. N.Y., Academic Press, 1965. 256 p.
5. *Zuev Yu. A. and Ivanov S. K.* Vzveshennoe golosovanie v mnogokanal'nykh sistemakh peredachi diskretnykh signalov [Weighted voting in multichannel systems of discrete signal transmission]. Problemy Peredachi Informatsii, 1995, vol. 31, no. 4, pp. 22–36. (in Russian)
6. *Zuev Yu. A. and Ivanov S. K.* Obuchenie i samoobuchenie v protsedurakh vzveshennogo golosovaniya [Taught and self-taught weighted voting procedures]. Zhurnal Vychislitel'noy Matematiki i Matematicheskoy Fiziki, 1995, vol. 35, no. 1, pp. 104–121. (in Russian)
7. *Zuev Yu. A. and Ivanov S. K.* Voting as a way to increase the decision reliability. J. Franklin Institute, 1999, vol. 336, no. 2, pp. 361–378.

8. *Zuev Yu. A.* Asimptotika logarifma chisla porogovykh funktsiy algebry logiki [Asymptotics of the logarithm of the number of Boolean threshold functions]. Dokl. AN SSSR, 1989, vol. 306, no. 3, pp. 528–530. (in Russian)
9. *Irmatov A. A.* O chisle porogovykh funktsiy [On the number of threshold functions]. Diskretnaya Matematika, 1993, vol. 5, no. 3, pp. 40–43. (in Russian)
10. *Zuev Yu. A.* Porogovye funktsii i porogovye predstavleniya bulevykh funktsiy [Threshold functions and threshold representations of Boolean functions]. Matematicheskie Voprosy Kibernetiki, 1994, no. 3, pp. 5–61. (in Russian)
11. *Muroga S.* Threshold Logic and its Applications. N.Y., Wiley, 1971. 478 p.
12. *Muroga S., Tsuboi N., and Baugh R. S.* Enumeration of threshold functions of eight variables. IEEE Trans. Computers, 1970, vol. C-19, no. 9, pp. 818–825.
13. *Chernikov S. N.* Lineynye neravenstva [Linear Inequalities]. Moscow, Nauka Publ., 1968. 488 p. (in Russian)
14. *Ziegler G. M.* Lectures on Polytopes. N.Y., Springer Verlag, 1995. 370 c.
15. *Chernikova N. V.* Algoritm dlya nakhozhdeniya obshchey formuly neotritsatel'nykh resheniy sistemy lineynykh neravenstv [Algorithm for finding a general formula for the non-negative solutions of a system of linear inequalities]. Zhurnal Vychislitel'noy Matematiki i Matematicheskoy Fiziki, 1965, vol. 5, no. 2, pp. 334–337. (in Russian)
16. *Rozenfel'd N. V.* Mnogomernye prostranstva [Multidimensional Spaces]. Moscow, Nauka Publ., 1966. 648 p. (in Russian)

СВЕДЕНИЯ ОБ АВТОРАХ

АХМЕТЗЯНОВА Лилия Руслановна — кандидат физико-математических наук, заместитель начальника отдела криптографических исследований ООО «КРИПТО-ПРО», г. Москва. E-mail: **lah@cryptopro.ru**

БАБУЕВА Александра Алексеевна — ведущий инженер-аналитик отдела криптографических исследований ООО «КРИПТО-ПРО», г. Москва.
E-mail: **babueva@cryptopro.ru**

ИВАНОВ Сергей Константинович — кандидат технических наук, доцент кафедры высшей математики Московского государственного университета технологий и управления им. К. Г. Разумовского, г. Москва. E-mail: **sergey.k.ivanov@gmail.com**

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**

КУНИНЕЦ Артем Андреевич — студент специальности «Компьютерная безопасность» ОНК «Институт высоких технологий» БФУ им. И. Канта, г. Калининград.
E-mail: **artkuninets@yandex.ru**

ЛОГАЧЕВ Александр Станиславович — кандидат физико-математических наук, ведущий научный сотрудник Лаборатории ТВП, г. Москва.

МАЛЫГИНА Екатерина Сергеевна — кандидат физико-математических наук, доцент департамента прикладной математики МИЭМ НИУ ВШЭ, г. Москва.
E-mail: **emalygina@hse.ru**

МИРОНКИН Владимир Олегович — кандидат физико-математических наук, доцент базовой кафедры № 252 информационной безопасности МИРЭА — Российского технологического университета, г. Москва. E-mail: **mironkin.v@mail.ru**

РЫБАЛОВ Александр Николаевич — кандидат физико-математических наук, старший научный сотрудник лаборатории комбинаторных и вычислительных методов алгебры и логики Института математики им. С. Л. Соболева СО РАН, г. Омск.
E-mail: **alexander.rybalov@gmail.com**

ЧЕРЕМУШКИН Александр Васильевич — доктор физико-математических наук, академик Академии криптографии Российской Федерации, г. Москва.
E-mail: **avc238@mail.ru**

Журнал «Прикладная дискретная математика» входит в перечень ВАК рецензируемых научных изданий, в которых должны быть опубликованы основные результаты диссертаций на соискание учёной степени кандидата и доктора наук по специальностям 2.3.5. «Математическое и программное обеспечение вычислительных систем, комплексов и компьютерных сетей» (технические науки), 2.3.6. «Методы и системы защиты информации, информационная безопасность» (физико-математические и технические науки), 1.1.5. «Математическая логика, алгебра, теория чисел и дискретная математика» (физико-математические науки), 1.2.3. «Теоретическая информатика, кибернетика» (физико-математические науки), а также в перечень журналов, рекомендованных ФУМО ВО ИБ в качестве учебной литературы по специальности «Компьютерная безопасность».

Журнал индексируется в базах данных Web of Science (Emerging Sources Citation Index (ESCI) и Russian Science Citation Index (RSCI)), Scopus, MathSciNet и Zentralblatt MATH. По решению ВАК от 21.12.2023 он отнесён к первой категории (К1) научных журналов, входящих в Перечень ВАК.

Журнал «Прикладная дискретная математика» распространяется по подписке; его подписной индекс 38696 в объединённом каталоге «Пресса России». Полнотекстовые электронные версии вышедших номеров журнала доступны на его сайте journals.tsu.ru/pdm и на Общероссийском математическом портале www.mathnet.ru. На сайте журнала можно найти также правила подготовки рукописей статей для публикации в журнале.

Тематика публикаций журнала:

- *Теоретические основы прикладной дискретной математики*
- *Математические методы криптографии*
- *Математические методы стеганографии*
- *Математические основы компьютерной безопасности*
- *Математические основы надёжности вычислительных и управляющих систем*
- *Прикладная теория кодирования*
- *Прикладная теория автоматов*
- *Прикладная теория графов*
- *Логическое проектирование дискретных автоматов*
- *Математические основы информатики и программирования*
- *Вычислительные методы в дискретной математике*
- *Математические основы интеллектуальных систем*
- *Исторические очерки по дискретной математике и её приложениям*