МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

ПРИКЛАДНАЯ ДИСКРЕТНАЯ МАТЕМАТИКА

Научный журнал

2025 № 69

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 19.09.2025. Формат $60 \times 84\frac{1}{8}$. Усл. п. л. 15. Тираж 300 экз.
Заказ № 6462. Цена свободная. Дата выхода в свет 25.09.2025.

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

СОДЕРЖАНИЕ

ТЕОРЕТИЧЕСКИЕ ОСНОВЫ ПРИКЛАДНОЙ ДИСКРЕТНОЙ МАТЕМАТИКИ

Ефимов Д. Б. Комбинаторные аспекты q-гафниана 5
Куценко А. В. Описание некоторых классов изометричных отображений, сохраняющих самодуальность обобщённой бент-функции 18
Панкратова И. А., Сорокоумова А. Д. О криптоаналитической обратимости дискретных функций 37

МАТЕМАТИЧЕСКИЕ МЕТОДЫ КРИПТОГРАФИИ

Денисов О. В., Андреев Е. Д., Батаев М. А. Характеристики атак различения на 3 и 4 раунда схемы Луби — Ракова в модели независимых подстановок 55
Иогансон И. Д., Давыдов В. В., Дакуо Ж.-М. Н., Хуцаева А. Ф. Протокол ментального покера, основанный на задачах поиска изогений между эллиптическими кривыми 68
Черемушкин А. В. Общая схема для семейства протоколов выработки общего ключа типа Диффи — Хеллмана 94

ПРИКЛАДНАЯ ТЕОРИЯ ГРАФОВ

Бызов В. А., Пушкарев И. А. Явная конструкция бесконечных семейств сильно регулярных орграфов с параметрами $((v + (2^{n+1} - 4)t)2^{n-1}, k + (2^n - 2)t, t, \lambda, t)$ ... 111

МАТЕМАТИЧЕСКИЕ ОСНОВЫ ИНФОРМАТИКИ И ПРОГРАММИРОВАНИЯ

Рузанова Д. П., Рыбалов А. Н. О генерической сложности проблем 3-раскраски графов 121

СВЕДЕНИЯ ОБ АВТОРАХ 129

CONTENTS

THEORETICAL BACKGROUNDS OF APPLIED DISCRETE MATHEMATICS

Efimov D. B. Combinatorial aspects of the q-Hafnian 5

Kutsenko A. V. Characterization of some classes of isometric mappings that preserve self-duality of generalized bent function 18

Pankratova I. A., Sorokoumova A. D. On cryptanalytic invertibility of discrete functions 37

MATHEMATICAL METHODS OF CRYPTOGRAPHY

Denisov O. V., Andreev E. D., Bataev M. A. Characteristics of distinguishing attacks on 3 and 4 rounds of the Luby — Rackoff scheme in independent permutations model 55

Ioganson I. D., Davydov V. V., Dakuo J.-M. N., Khutsaeva A. F. Mental poker protocol based on the problem of finding isogenies between elliptic curves 68

Cheremushkin A. V. General scheme for a class of Diffie — Hellman type protocols 94

APPLIED GRAPH THEORY

Byzov V. A., Pushkarev I. A. Explicit construction of infinite families of strongly regular digraphs with parameters $((v + (2^{n+1} - 4)t)2^{n-1}, k + (2^n - 2)t, t, \lambda, t)$ 111

MATHEMATICAL BACKGROUNDS OF INFORMATICS AND PROGRAMMING

Ruzanova D. P., Rybalov A. N. On the generic complexity of graph 3-coloring problems 121

BRIEF INFORMATION ABOUT THE AUTHORS 129

ТЕОРЕТИЧЕСКИЕ ОСНОВЫ ПРИКЛАДНОЙ ДИСКРЕТНОЙ МАТЕМАТИКИ

УДК 519.1+512.64 DOI 10.17223/20710410/69/1

КОМБИНАТОРНЫЕ АСПЕКТЫ q-ГАФНИАНА[1]

Д. Б. Ефимов

ФМИ ФИЦ Коми НЦ УрО РАН, г. Сыктывкар, Россия

E-mail: defimov@ipm.komisc.ru

Гафниан был введён в середине XX в. в работах итальянского физика-теоретика Э. Р. Каяньелло в связи с задачами квантовой теории поля. В дальнейшем гафниан нашёл применение в комбинаторике как перечисляющая функция числа совершенных паросочетаний графов. По своему виду гафниан близок к такой более известной функции, как пфаффиан. В отличие от последней, он задаётся на симметричных, а не кососимметричных матрицах и не учитывает знаки перестановок индексов в соответствующих мономах. В данной работе рассмотрен q-гафниан — обобщение гафниана, зависящее от формальных параметров и совпадающее с исходной функцией при единичных значениях параметров. Указан комбинаторный смысл q-гафниана как производящей функции числа перестановок и числа дуговых (линейных хордовых) диаграмм определённых классов. Доказаны несколько свойств одно- и двупараметрического q-гафниана, которые являются обобщениями свойств обычного гафниана. В частности, мы приводим аналог свойства разложения по строке и аналог свойства, выражающего гафниан матрицы смежности двудольного взвешенного графа с равными долями через перманент матрицы бисмежности. Данные понятия и свойства, помимо чисто теоретического интереса, могут быть использованы при разработке алгоритмов, изучающих статистику числа инверсий определённых классов перестановок и статистику числа взаимных пересечений и вложений рёбер определённых классов дуговых диаграмм.

Ключевые слова: *q-аналог, гафниан, дуговая диаграмма, перестановка.*

COMBINATORIAL ASPECTS OF THE q-HAFNIAN

D. B. Efimov

IPM FRC Komi SC UB RAS, Syktyvkar, Russia

The Hafnian was introduced in the middle of 20th century by the Italian theoretical physicist E. R. Caianiello in connection with problems of quantum field theory. Later, the Hafnian found its application in combinatorics as an enumeration function of the number of perfect matchings of graphs. In its form, the Hafnian is close to such a better-known function as the Pfaffian. Unlike the latter, it is defined on symmetric, not skew-symmetric matrices and does not take into account the signs of permutations of indices in the corresponding monomials. In this paper, we consider the q-Hafnian,

[1]Работа выполнена в рамках госзадания ФМИ ФИЦ Коми НЦ УрО РАН, проект № 125031203621-2.

a generalization of the Hafnian that depends on formal parameters and coincides with the original function for unit values of the parameters. We indicate the combinatorial meaning of the q-Hafnian as a generating function of the number of permutations and the number of arc (linear chord) diagrams of certain classes. We prove several properties of the one- and two-parameter q-Hafnian that are generalizations of the properties of the usual Hafnian. In particular, we present an analog of the row decomposition property and an analog of the property expressing the Hafnian of the adjacency matrix of a bipartite weighted graph with equal parts through the permanent of the biadjacency matrix. These concepts and properties, in addition to their purely theoretical interest, can be used in developing algorithms that study the statistics of the number of inversions of certain classes of permutations and the statistics of the number of crossings and nestings in various classes of arc diagrams.

Keywords: *q-analog, Hafnian, arc diagram, permutation.*

Введение

У многих математических понятий имеются так называемые q-аналоги — естественным образом возникающие обобщения, зависящие от параметра q и совпадающие при $q = 1$ с исходным понятием. При этом данные обобщения, с одной стороны, обладают свойствами, сходными со свойствами первоначальных вариантов, с другой стороны, в них заложен дополнительный потенциал. Здесь можно привести такие классические примеры, как q-аналог неотрицательного целого числа, q-факториал, q-биномиальный коэффициент (гауссов биномиальный коэффициент). Одним из разделов математики, где q-аналоги находят приложение, является комбинаторика [1–4]. Здесь они выступают в роли производящих функций числа различных объектов и по сравнению с исходными (не q-) вариантами позволяют получать более подробные комбинаторные характеристики . Так, например, если обычный факториал $n!$ равен числу всех перестановок n-го порядка, то его q-аналог $[n]_q!$ перечисляет все перестановки n-го порядка с учётом числа инверсий.

В конце 80-х–начале 90-х годов XX в. произошёл всплеск интереса к q-математике в связи с изобретением квантовых групп [5, 6]. В качестве основной мотивации здесь выступали задачи квантовой теории поля. Одними из ключевых объектов данной богатой и содержательной теории являются q- или «квантовые» аналоги классических непрерывных групп и их представлений. При этом естественным образом возникает q-аналог определителя матрицы. Элементы матрицы рассматриваются как элементы некоммутативной алгебры, квантовый определитель понимается как центральный элемент этой же алгебры. При таком подходе удаётся получить аналоги многих свойств обычного определителя.

Примерно в это же время появляются публикации, посвященные q-определителю и схожему с ним q-перманенту, в которых рассматриваются чисто математические задачи и развиваются другие подходы. Так, в работах комбинаторной направленности q-аналог определителя (перманента) определяется на обычных числовых матрицах и рассматривается как производящая функция, перечисляющая те или иные объекты (например, перестановки), связанные с матрицами [7–9]. При этом приходится считаться с тем, что многие свойства, присущие обычному определителю, перестают выполняться. Для полноты картины отметим ещё один подход, когда q-аналоги перманента также применяются к обычным матричным элементам, но акцент делается не на комбинаторных, а на алгебраических вопросах [10–13]. Существует ряд работ, находящихся на стыке разных подходов к q-перманенту [14, 15].

С парой схожих по виду функций от матричных элементов определитель / перманент тесно связана пара также схожих по виду функций от матричных элементов пфаффиан / гафниан [16, 17]. Одной из первых публикаций, в которой появляется понятие q-пфаффиана, является работа [18]. В ней используется теоретико-физический (квантовый) подход, т. е. рассматриваются матрицы с элементами из некоммутативного координатного кольца; q-пфаффиан вводится индуктивно (свойство разложения по строке берётся за определение). В работе [19] N. Jing и J. Zhang, опять же в рамках квантового подхода, устанавливают связь между q-определителем и q-пфаффианом. В качестве теоремы приводится выражение квантового пфаффиана через квантовую алгебру Грассмана (по аналогии с классическим случаем). В одной из своих следующих работ [20] данные авторы вводят понятие квантового гафниана и рассматривают некоторые его свойства, например связь с квантовым перманентом.

Предметом исследования данной работы также является q-гафниан. Но мы рассматриваем его не в рамках квантового подхода, а делаем акцент на комбинаторных свойствах (в духе работ [7–9]). Работа организована следующим образом. В п. 1 мы даём определение q-гафниана и приводим его комбинаторные интерпретации на языке перестановок и теории графов. В п. 2 приводятся простейшие свойства q-гафниана и демонстрируется их применение на некоторых характерных примерах. В п. 3 рассматривается двупараметрический вариант q-гафниана.

1. Определение q-гафниана и комбинаторный смысл

Пусть K — поле нулевой характеристики; $K[q]$ — кольцо многочленов от одной переменной q над K; $\mathrm{Sym}_n(K)$ — множество симметричных $(n \times n)$-матриц над K; S_n — множество перестановок из n элементов. Перестановка $\rho \in S_n$ имеет инверсию на паре элементов $\rho(i)$ и $\rho(j)$, если целые числа $\rho(i) - \rho(j)$ и $i - j$ имеют противоположные знаки. Общее число инверсий перестановки ρ будем обозначать через $\ell(\rho)$. Пусть n — чётное натуральное число ($n = 2m$). Через $\mathcal{P}_n$ обозначим множество перестановок $\sigma \in S_n$ вида

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & \dots & n-1 & n \\ i_1 & j_1 & i_2 & j_2 & \dots & i_m & j_m \end{pmatrix}, \tag{1}$$

где $i_1 < i_2 < \ldots < i_m$ и $i_k < j_k$ для всех k от 1 до m. Будем записывать такие перестановки в виде $\sigma = (i_1, j_1; i_2, j_2; \ldots; i_m, j_m)$. Как следует из определения, инверсии в таких перестановках могут возникать только на парах элементов j_k и i_l при $k < l$ и на парах различных элементов j_k и j_l.

Пусть $A = (a_{ij}) \in \mathrm{Sym}_n(K)$. Назовём *$q$-гафнианом* функцию

$$\mathrm{Hf}_q : \mathrm{Sym}_n(K) \to K[q], \quad \mathrm{Hf}_q(A) = \sum_{\sigma \in \mathcal{P}_n} q^{\ell(\sigma)} a_\sigma, \tag{2}$$

где $a_\sigma = a_{i_1 j_1} a_{i_2 j_2} \dots a_{i_m j_m}$. Так, например, если $A \in \mathrm{Sym}_4(K)$, то $\mathrm{Hf}_q(A) = a_{12}a_{34} + qa_{13}a_{24} + q^2 a_{14}a_{23}$. Название оправдывает себя тем, что если мы подставим $q = 1$ в (2), то получим определение обычного гафниана [21]. При $q = -1$ формально получаем определение пфаффиана [22, с. 2087] с той оговоркой, что пфаффиан обычно задаётся на кососимметричных матрицах.

Определим комбинаторный смысл q-гафниана. Каждой перестановке вида (1) можно однозначно сопоставить симметричную $(0,1)$-матрицу порядка n по следующему правилу: элементы матрицы с индексами (i_k, j_k), (j_k, i_k), $k = 1, 2, \ldots, m$, равны 1, а все остальные элементы равны 0. Назовём такую матрицу матрицей соответствующей перестановки (отметим, что это определение отличается от общепринятого). Так, перестановке $(1, 3; 2, 4)$ однозначно соответствует матрица

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

Пусть A — симметричная $(0,1)$-матрица порядка n. Тогда она задаёт некоторое семейство перестановок $\mathcal{P}_A \subset \mathcal{P}_n$, а именно: в это семейство входят те и только те перестановки из $\mathcal{P}_n$, матрицы которых поэлементно не превосходят A. Нетрудно видеть, что $\mathrm{Hf}_q(A)$ является производящей функцией количества перестановок из $\mathcal{P}_A$ с заданным числом инверсий:

$$\mathrm{Hf}_q(A) = \sum_{\sigma \in \mathcal{P}_A} q^{\ell(\sigma)}. \tag{3}$$

Дадим комбинаторную интерпретацию q-гафниана на языке теории графов. Пусть n — чётное натуральное число. *Дуговой диаграммой* на n вершинах назовём 1-регулярный граф, вершины которого пронумерованы числами от 1 до n и равномерно расположены в возрастающем порядке слева направо вдоль отрезка горизонтальной прямой, а рёбра изображены в виде дуг. Высота каждой дуги (максимальная длина перпендикуляра, опущенного из точки дуги на прямую, проходящую через все вершины диаграммы) пропорциональна расстоянию между вершинами, которые соединяет дуга (рис. 1). Такие диаграммы называют также линейными хордовыми диаграммами [23, 24] или просто линейными диаграммами [25]. Ребро дуговой диаграммы, соединяющее вершины с номерами i и j $(i < j)$, будем обозначать через (i, j); длиной ребра назовём число $j-i$. Множество всех дуговых диаграмм на n вершинах обозначим через $\mathcal{D}_n$.

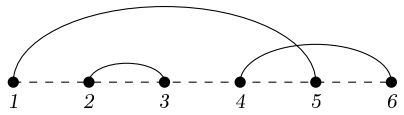

Рис. 1. Дуговая диаграмма на шести вершинах

Каждой перестановке $\sigma = (i_1, j_1; i_2, j_2; \ldots; i_m, j_m)$ из $\mathcal{P}_n$ взаимно-однозначно соответствует дуговая диаграмма из $\mathcal{D}_n$ с рёбрами (i_k, j_k), $k = 1, \ldots, m$. Так, перестановка $(1,5;2,3;4,6)$ соответствует диаграмме на рис. 1. Соответственно любая $(0,1)$-матрица $A \in \mathrm{Sym}_n(K)$ задаёт некоторое семейство дуговых диаграмм на n вершинах. Обозначим это семейство через $\mathcal{D}_A$.

Пусть $k < l$. Из определения следует, что возможны три варианта взаимного расположения двух пар смежных индексов (i_k, j_k) и (i_l, j_l):

1) $i_k < j_k < i_l < j_l$. В этом случае перестановка σ не имеет инверсий на данных индексах, а в соответствующей диаграмме ребро (i_k, j_k) расположено полностью левее ребра (i_l, j_l) (рис. 2, *а*);
2) $i_k < i_l < j_k < j_l$. В этом случае перестановка σ имеет инверсию на индексах j_k и i_l, а в диаграмме рёбра (i_k, j_k) и (i_l, j_l) пересекаются (рис. 2, *б*);
3) $i_k < i_l < j_l < j_k$. В этом случае перестановка σ имеет инверсии на индексах j_k и i_l и на индексах j_k и j_l. В диаграмме ребро (i_k, j_k) накрывает ребро (i_l, j_l) (или, по-другому, ребро (i_l, j_l) вложено в ребро (i_i, j_i) (рис. 2, *в*).

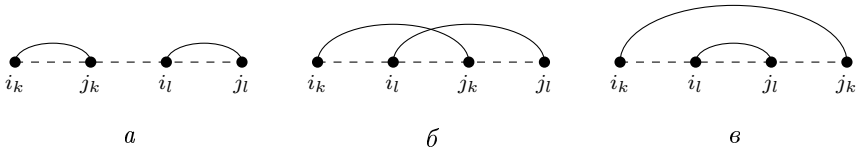

Рис. 2. Взаимное расположение двух рёбер дуговой диаграммы

Пусть δ — дуговая диаграмма. Обозначим через $s(\delta)$ общее количество взаимных пересечений рёбер, а через $t(\delta)$ — общее количество взаимных вложений-накрытий рёбер диаграммы δ. Из вышесказанного следует, что $\mathrm{Hf}_q(A)$ является производящей функцией количества дуговых диаграмм из $\mathcal{D}_A$ с заданным числом $s(\delta) + 2t(\delta)$:

$$\mathrm{Hf}_q(A) = \sum_{\delta \in \mathcal{D}_A} q^{s(\delta)+2t(\delta)}. \tag{4}$$

В заключение данного пункта отметим, что если рассматривать кольцо многочленов от переменной q как множество всевозможных значений q-гафниана и профакторизовать его по идеалу, порождённому q^2, то получим частный случай приведённых интерпретаций, связанный с перечислением чётных и нечётных перестановок и перечислением диаграмм с чётным и нечётным числом пересечений дуг. На примере сходных с дуговыми хордовых диаграмм и с использованием другой техники данный частный случай рассмотрен в работе [17].

2. Свойства q-гафниана

Напомним, что если $B = (b_{ij})$ — произвольная $(m \times m)$-матрица над полем K, то её q-перманентом называется следующий многочлен от переменной q над K:

$$\mathrm{per}_q(B) = \sum_{\rho \in S_m} q^{\ell(\rho)} b_{1\rho(1)} b_{2\rho(2)} \dots b_{m\rho(m)}.$$

Утверждение 1.

1) Пусть $A = (a_{ij}) \in \mathrm{Sym}_n(K)$. Тогда справедливо следующее разложение q-гафниана по первой строке:

$$\mathrm{Hf}_q(A) = \sum_{k=2}^{n} q^{k-2} a_{1k} \mathrm{Hf}_q(A(1,k)).$$

Здесь $A(1,k)$ — матрица, получаемая из A вычеркиванием строк и столбцов с номерами 1 и k.

2) Пусть A — симметричная блочно-диагональная матрица:

$$A = \begin{pmatrix} A_1 & 0 & \dots & 0 \\ 0 & A_2 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & A_k \end{pmatrix}.$$

Тогда

$$\mathrm{Hf}_q(A) = \mathrm{Hf}_q(A_1)\mathrm{Hf}_q(A_2)\dots\mathrm{Hf}_q(A_k).$$

3) q-Гафниан матрицы не меняется при её отражении относительно побочной диагонали:

$$\mathrm{Hf}_q(A) = \mathrm{Hf}_q(JA^{\mathrm{T}}J),$$

где J — перъединичная матрица, т. е. матрица с единицами на побочной диагонали и остальными нулевыми элементами.

4) Рассмотрим симметричную $(2m \times 2m)$-матрицу над полем K вида

$$A = \begin{pmatrix} C & B \\ B^{\mathrm{T}} & 0 \end{pmatrix},$$

где B — произвольная $(m \times m)$-матрица; C — произвольная симметричная $(m \times m)$-матрица. Справедливо равенство

$$\mathrm{Hf}_q(A) = q^{m(m-1)/2} \operatorname{per}_q(B).$$

Доказательство.

1) По определению любая перестановка из $\mathcal{P}_n$ имеет вид $(1, k; \dots)$, $2 \leqslant k \leqslant n$. Уберём в этой перестановке пару индексов 1 и k, а оставшиеся индексы перенумеруем числами от 1 до $n-2$ в порядке возрастания, начиная с самого маленького индекса. В результате получим некоторую перестановку из $\mathcal{P}_{n-2}$. Например, из перестановки $(1,4;2,5;3,6) \in \mathcal{P}_6$ при таком преобразовании получим перестановку $(1,3;2,4) \in \mathcal{P}_4$. Очевидно, что индекс k образует в исходной перестановке инверсии с индексами $2, 3, \dots, k-1$: всего $k-2$ инверсии. Также очевидно, что при перенумерации новых инверсий не появляется, а имеющиеся не пропадают. Поэтому новая перестановка содержит на $k-2$ инверсии меньше, чем исходная. Обозначим через $\mathcal{P}_{n,k}$ множество перестановок из $\mathcal{P}_n$ вида $(1, k; \dots)$, а общий элемент матрицы $A(1,k)$ обозначим через $a(1,k)_{i,j}$. Тогда можем записать

$$\mathrm{Hf}_q(A) = \sum_{k=2}^{n} \sum_{\sigma \in \mathcal{P}_{n,k}} q^{\ell(\sigma)} a_\sigma = \sum_{k=2}^{n} q^{k-2} a_{1k} \sum_{\sigma \in \mathcal{P}_{n-2}} q^{\ell(\sigma)} a(1,k)_\sigma = \sum_{k=2}^{n} q^{k-2} a_{1k} \mathrm{Hf}_q(A(1,k)).$$

2) Данное свойство непосредственно следует из определения q-гафниана.

3) Рассмотрим слагаемое $q^{\ell(\sigma)} a_\sigma$ из представления (2) q-гафниана $\mathrm{Hf}_q(A)$. При отражении матрицы A относительно побочной диагонали оно «перейдёт» в некоторое слагаемое $q^{\ell(\sigma')} a_{\sigma'}$ q-гафниана $\mathrm{Hf}_q(JA^TJ)$. При этом, очевидно, $a_\sigma = a_{\sigma'}$. Перестановка σ' получается из перестановки $\sigma = (i_1, j_1; i_2, j_2; \dots; i_m, j_m)$ заменой всех пар (i_k, j_k) на пары $(n - j_k + 1, n - i_k + 1)$ и упорядочиванием их слева направо по возрастанию по первому индексу. Нетрудно видеть, что общее число инверсий в перестановке σ равно общему числу инверсий в перестановке σ'. Таким образом, $q^{\ell(\sigma)} a_\sigma = q^{\ell(\sigma')} a_{\sigma'}$. Отсюда следует, что q-гафниан не меняется при отражении матрицы относительно побочной диагонали.

4) Рассмотрим произвольную перестановку $(i_1, j_1; i_2, j_2; \dots; i_m, j_m) \in \mathcal{P}_{2m}$. Предположим, что $i_k > m$ для некоторого k. Тогда $j_k > m$ по определению $\mathcal{P}_{2m}$. Но в этом случае элемент $a_{i_k j_k}$ матрицы A равен 0. Таким образом, мономы, содержащие такие элементы, можно не учитывать и считать, что $i_k \leqslant m$. А так как по определению индексы i_k упорядочены по возрастанию, то $i_k = k$, $j_k > m$ для любого k. Отсюда следует, что матрица C не оказывает никакого влияния на значение q-гафниана.

Рассмотрим перестановку $\sigma = (1, j_1; 2, j_2; \dots; m, j_m)$. В данном случае каждый индекс j_k образует $m - k$ инверсий с индексами $k+1, k+2, \dots, m$; общее число таких инверсий в перестановке равно $m(m-1)/2$. Кроме этого, инверсии могут быть между различными индексами j_k. Пусть $B = (b_{ij})$. Сделаем замену $l_k = j_k - m$. Тогда l_k принимают значения от 1 до m и $a_{kj_k} = b_{kl_k}$, $k = 1, 2, \dots, m$. При этом очевидно, что число

инверсий между индексами l_k равно числу инверсий между индексами j_k Рассмотрим перестановку $\rho \in S_m$, такую, что $\rho(k) = l_k$. Из сказанного следует, что числа инверсий перестановок σ и ρ связаны соотношением $\ell(\sigma) = \ell(\rho) + m(m-1)/2$. Отсюда получаем

$$\mathrm{Hf}_q(A) = \sum_{\sigma \in \mathcal{P}_n} q^{\ell(\sigma)} a_\sigma = \sum_{\rho \in S_m} q^{\ell(\rho)+m(m-1)/2} b_{1\rho(1)} b_{2\rho(2)} \dots b_{m\rho(m)} = q^{m(m-1)/2} \mathrm{per}_q(B).$$

Утверждение 1 доказано. ■

Замечание 1. В силу симметричности матрицы A и свойства 3 аналоги свойства 1 справедливы для разложения q-гафниана по первому столбцу, а также по последней строке и последнему столбцу.

Пример 1. Вычислим q-гафниан матрицы n-го порядка $\mathbf{1}_n$, все элементы которой равны 1:

$$\mathbf{1}_n = \begin{pmatrix} 1 & 1 & \dots & 1 \\ 1 & 1 & \dots & 1 \\ \vdots & \vdots & \vdots & \vdots \\ 1 & 1 & \dots & 1 \end{pmatrix}.$$

В соответствии с приведённым в п. 1 правилом матрица $\mathbf{1}_n$ задаёт множество всех перестановок $\mathcal{P}_n$ или множество $\mathcal{D}_n$ всех дуговых диаграмм на n вершинах. Соответственно q-гафниан такой матрицы является производящей функцией числа перестановок вида (1) с заданным числом инверсий или производящей функцией числа дуговых диаграмм δ на n вершинах с заданным числом $s(\delta) + 2t(\delta)$. Раскладывая q-гафниан по первой строке, получаем следующее равенство:

$$\mathrm{Hf}_q(\mathbf{1}_n) = (1+q+q^2)(1+q+q^2+q^3+q^4)\dots(1+q+\dots+q^{n-2}).$$

Выражение в правой части данного равенства является q-аналогом двойного факториала нечётного числа $n-1$ и обозначается через $[n-1]_q!!$ Таким образом, с учётом (3) и (4) можем записать

$$\sum_{\sigma \in \mathcal{P}_n} q^{\ell(\sigma)} = \sum_{\delta \in \mathcal{D}_n} q^{s(\delta)+2t(\delta)} = [n-1]_q!!$$

Пример 2. Рассмотрим класс дуговых диаграмм на n вершинах, которые содержат только дуги смежных длин k или $k+1$ для некоторого целого $k \geqslant 1$. Класс таких диаграмм задаётся симметричной теплицевой $(0,1)$-матрицей n-го порядка, у которой в первой строке единичные элементы стоят только в столбцах с номерами из множества $\{2,3,\dots,n\} \cap \{k+1, k+2\}$. Например, если $k=1$, то такая матрица 4-го порядка имеет следующий вид:

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

Очевидно, что в таких диаграммах нет вложений (накрытий) дуг (рис. 2, *в*), поэтому в силу формулы (4) q-гафниан $(0,1)$-матрицы, задающей соответствующий класс, перечисляет дуговые диаграммы данного класса с заданным числом пересечений дуг (рис. 2, *б*).

При $k = 1$ обозначим q-гафниан матрицы рассматриваемого типа порядка $2m$ через $\mathrm{Hf}_q(m)$. Применяя правило разложения q-гафниана по первой строке, приходим к следующему рекуррентному соотношению:

$$\mathrm{Hf}_q(m+2) = \mathrm{Hf}_q(m+1) + q\mathrm{Hf}_q(m),\ \mathrm{Hf}_q(1) = 1,\ \mathrm{Hf}_q(2) = 1 + q.$$

Таким образом, в данном случае последовательность q-гафнианов представляет собой последовательность одного из типов многочленов Фибоначчи [26, 27].

3. Двупараметрический q-гафниан

Понятие q-гафниана можно естественным образом обобщить на большее число параметров. Для описания аналога свойства разложения по строке необходимо в данном случае расширить область определения гафниана и рассматривать его не над матрицами с элементами из поля, а над матрицами с элементами из кольца многочленов.

Пусть q_1, q_2 — два формальных параметра; $K[q_1, q_2]$ — кольцо многочленов от q_1 и q_2 над полем K; $A = (a_{ij}) \in \mathrm{Sym}_n(K[q_1, q_2])$. Назовём *двупараметрическим q-гафнианом* следующую функцию:

$$\mathrm{Hf}_{q_1,q_2} : \mathrm{Sym}_n(K[q_1, q_2]) \to K[q_1, q_2], \quad \mathrm{Hf}_{q_1,q_2}(A) = \sum_{\delta \in \mathcal{D}_n} {q_1}^{s(\delta)} {q_2}^{t(\delta)} a_\delta.$$

Здесь суммирование идёт по всем дуговым диаграммам на $n = 2m$ вершинах; через $s(\delta)$ и $t(\delta)$, как и раньше, обозначено общее количество взаимных пересечений рёбер и общее количество взаимных вложений-накрытий рёбер диаграммы δ соответственно; $a_\delta = a_{i_1 j_1} a_{i_2 j_2} \dots a_{i_m j_m}$ для диаграммы δ с рёбрами $(i_1, j_1), (i_2, j_2) \dots (i_m, j_m)$.

Из определения следует, что если $\mathcal{D}_A$ — семейство дуговых диаграмм, задаваемое симметричной $(0,1)$-матрицей A, то $\mathrm{Hf}_{q_1,q_2}(A)$ является производящей функцией числа дуговых диаграмм из $\mathcal{D}_A$ с заданным числом пересечений и вложений рёбер:

$$\mathrm{Hf}_{q_1,q_2}(A) = \sum_{\delta \in \mathcal{D}_A} {q_1}^{s(\delta)} {q_2}^{t(\delta)}. \tag{5}$$

Нетрудно видеть, что для функции Hf_{q_1,q_2} сохраняются свойства 2 и 3 функции Hf_q из утверждения 1. Для того чтобы получить аналог разложения по первой строке, заметим, что вычёркивание строк и столбцов с номерами 1 и k разбивает матрицу A на три области (рис. 3). В первой области расположены недиагональные элементы a_{ij}, один из индексов которых находится в промежутке от 1 до k, а второй больше k: $1 < i < k < j$ или $1 < j < k < i$. С точки зрения дуговых диаграмм ребро (i, j) (или (j, i)) пересекается с ребром $(1, k)$. Умножим все элементы этой области на формальный параметр q_1. Во второй области расположены недиагональные элементы a_{ij}, номера строк и столбцов которых находятся в промежутке между 1 и k: $1 < i < j < k$ или $1 < j < i < k$. С точки зрения дуговых диаграмм ребро (i, j) (или (j, i)) накрыто ребром $(1, k)$. Умножим все элементы этой области на формальный параметр q_2. В третьей области расположены недиагональные элементы a_{ij}, номера строк и столбцов которых больше k. С точки зрения дуговых диаграмм ребро (i, j) (или (j, i)) не пересекается с ребром $(1, k)$, не накрывает его и не накрывается им. Элементы этой области оставляем без изменения.

Обозначим через $A(1, k, q_1, q_2)$ матрицу, получаемую из A вычеркиванием строк и столбцов с номерами 1 и k и умножением оставшихся элементов на формальные параметры q_1, q_2 указанным способом. Тогда

$$\mathrm{Hf}_{q_1,q_2}(A) = \sum_{k=2}^{n} a_{1k} \mathrm{Hf}_{q_1,q_2}(A(1, k, q_1, q_2)). \tag{6}$$

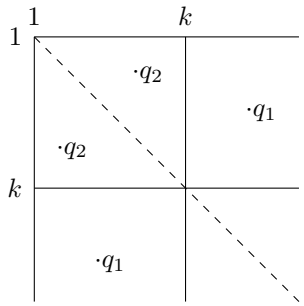

Рис. 3. Правило умножения элементов матрицы на параметры q_1 и q_2 при разложении двупараметрического q-гафниана по первой строке

Продемонстрируем свойство (6) на примере, вычислив с помощью разложения по первой строке двупараметрический q-гафниан матриц $\mathbf{1}_4$ и $\mathbf{1}_6$.

Пример 3. Разложение $\mathrm{Hf}_{q_1,q_2}(\mathbf{1}_4)$ по первой строке даёт следующий результат:

$$\mathrm{Hf}_{q_1,q_2}(\mathbf{1}_4) = \mathrm{Hf}_{q_1,q_2}(\mathbf{1}_2) + \mathrm{Hf}_{q_1,q_2}\begin{pmatrix} 1 & q_1 \\ q_1 & 1 \end{pmatrix} + \mathrm{Hf}_{q_1,q_2}\begin{pmatrix} 1 & q_2 \\ q_2 & 1 \end{pmatrix} = 1 + q_1 + q_2.$$

Раскладывая $\mathrm{Hf}_{q_1,q_2}(\mathbf{1}_6)$ по первой строке, получаем

$$\mathrm{Hf}_{q_1,q_2}(\mathbf{1}_6) = \mathrm{Hf}_{q_1,q_2}(\mathbf{1}_4) + \mathrm{Hf}_{q_1,q_2}\begin{pmatrix} 1 & q_1 & q_1 & q_1 \\ q_1 & 1 & 1 & 1 \\ q_1 & 1 & 1 & 1 \\ q_1 & 1 & 1 & 1 \end{pmatrix} + \mathrm{Hf}_{q_1,q_2}\begin{pmatrix} 1 & q_2 & q_1 & q_1 \\ q_2 & 1 & q_1 & q_1 \\ q_1 & q_1 & 1 & 1 \\ q_1 & q_1 & 1 & 1 \end{pmatrix} +$$
$$+\mathrm{Hf}_{q_1,q_2}\begin{pmatrix} 1 & q_2 & q_2 & q_1 \\ q_2 & 1 & q_2 & q_1 \\ q_2 & q_2 & 1 & q_1 \\ q_1 & q_1 & q_1 & 1 \end{pmatrix} + \mathrm{Hf}_{q_1,q_2}\begin{pmatrix} 1 & q_2 & q_2 & q_2 \\ q_2 & 1 & q_2 & q_2 \\ q_2 & q_2 & 1 & q_2 \\ q_2 & q_2 & q_2 & 1 \end{pmatrix}.$$

Продолжая раскладывать вновь получающиеся двупараметрические q-гафнианы по первой строке и приводя подобные слагаемые, получаем следующее выражение:

$$\mathrm{Hf}_{q_1,q_2}(\mathbf{1}_6) = 1 + 2q_1 + 2q_2 + 2q_1q_2 + q_1^2 + q_2^2 + 2q_1q_2^2 + 2q_1^2q_2 + q_1^3 + q_2^3.$$

Согласно (5), данное выражение представляет собой производящую функцию числа дуговых диаграмм на шести вершинах с заданным числом пересечений и накрытий рёбер. Например, присутствие слагаемого $2q_1^2q_2$ говорит о том, что имеется всего две дуговые диаграммы на шести вершинах с двумя пересечениями рёбер и одним накрытием. Эти диаграмы приведены на рис. 4.

Рис. 4. Дуговые диаграммы на шести вершинах с двумя пересечениями рёбер и одним накрытием

Заметим, что многочлены $\mathrm{Hf}_{q_1,q_2}(\mathbf{1}_4)$ и $\mathrm{Hf}_{q_1,q_2}(\mathbf{1}_6)$ являются симметрическими. Как показано в [28], это свойство справедливо для любой матрицы $\mathbf{1}_n$.

Заключение

Мы рассмотрели одно- и двупараметрические q-аналоги гафниана, дали их комбинаторную интерпретацию и доказали несколько свойств. В соответствии с концепцией q-математики при значениях параметров, равных единице, мы приходим к известным свойствам обычного гафниана. q-Аналоги по сравнению со стандартным случаем позволяют проводить более «тонкий» комбинаторный анализ. Отметим, что с вычислительной точки зрения задача нахождения значения гафниана или эквивалентная ей задача определения числа паросочетаний в графе в общем случае являются труднорешаемыми [29, 30]. Соответственно определение значения q-гафниана представляет собой задачу не меньшей вычислительной сложности. Представленный материал, помимо чисто теоретического интереса, может быть использован для построения алгоритмов, вычисляющих q-гафниан или изучающих статистики числа инверсий определённых классов перестановок и числа взаимных пересечений и вложений рёбер некоторых классов дуговых диаграмм. Дуговые (или идентичные им хордовые) диаграммы часто выступают в качестве удобной математической модели, например при кодировании топологических узлов [31] или визуализации вторичной структуры молекул РНК [32, 33]. Поэтому рассмотренные вопросы перечисления дуговых диаграмм, возможно, смогут найти применение в различных разделах математики или других науках, например биоинформатике.

Автор выражает благодарность рецензенту за внимательное прочтение статьи и ряд полезных замечаний и рекомендаций.

ЛИТЕРАТУРА

1. *Сачков В. Н.* Введение в комбинаторные методы дискретной математики. М.: Наука, 1982. 384 с.
2. *Смирнов Е. Ю.* Диаграммы Юнга, плоские разбиения и знакочередующиеся матрицы. М.: МЦНМО, 2014. 64 с.
3. *Игнатьев М. В.* Квантовая комбинаторика // Матем. просв. Сер. 3. 2014. Вып. 18. С. 66–111.
4. *Haglund J.* The q,t-Catalan Numbers and the Space of Diagonal Harmonics. AMS, 2007. 167 p.
5. *Manin Yu. I.* Quantum Groups and Non-Commutative Geometry. Montréal: CRM, 1988. 91 p.
6. *Демидов Е. Е.* Квантовые группы. М.: Факториал, 1998. 128 с.
7. *Yang K.-W.* q-Determinants and permutations // Fibonacci Quart. 1991. V. 29. No. 2. P. 160–163.
8. *Tagawa H.* A multivariable quantum determinant over a commutative ring // RIMS Kôkyûroku. 1991. V. 765. P. 91–103.
9. *Shevelev V.* Combinatorial minors for matrix functions and their applications // Zeszyty Naukowe Politechniki Śląskiej. Seria: Matematyka Stosowana. 2014. No. 4. P. 5–16.
10. *Bapat R. B. and Lal A. K.* Inequalities for the q-permanent // Linear Algebra Appl. 1994. V. 197/198. P. 397–409.
11. *Lal A. K.* Inequalities for the q-permanent. II // Linear Algebra Appl. 1998. V. 274. P. 1–16.
12. *Da Fonseca C. M.* The μ-permanent of a tridiagonal matrix, orthogonal polynomials, and chain sequences // Linear Algebra Appl. 2010. V. 432. P. 1258–1266.
13. *Da Fonseca C. M.* The μ-permanent, a new graph labeling, and a known integer sequence // Bulletin mathématique de la Sociétédes Sciences Mathématiques de Roumanie. 2018. V. 61(109). No. 3. P. 255–262.

14. *De Sá E. M.* Noncrossing partitions, noncrossing graphs, and q-permanental equations // Linear Algebra Appl. 2018. V. 541. P. 36–53.
15. *De Sá E. M.* Linear preservers for the q-permanent, cycle q-permanent expansions, and positive crossings in digraphs // Linear Algebra Appl. 2019. V. 561. P. 228–252.
16. *Kocharovsky Vit. V., Kocharovsky V. V., and Tarasov S. V.* The Hafnian Master Theorem // Linear Algebra Appl. 2022. V. 651. P. 144–161.
17. *Efimov D. B.* Enumeration of even and odd chord diagrams // J. Appl. Industr. Math. 2024. V. 18. No. 2. P. 216–226.
18. *Strickland E.* Classical invariant theory for the quantum symplectic group // Adv. Math. 1996. V. 123. P. 78–90.
19. *Jing N. and Zhang J.* Quantum Pfaffians and hyper-Pfaffians // Adv. Math. 2014. V. 265. P. 336–361.
20. *Jing N. and Zhang J.* Quantum permanents and Hafnians via Pfaffians // Lett. Math. Phys. 2016. V. 106. P. 1451–1464.
21. *Barvinok A.* Combinatorics and Complexity of Partition Functions. Cham: Springer, 2016. 309 p.
22. *Tribe R. and Zaboronski O.* Pfaffian formulae for one dimensional coalescing and annihilating systems // Electronic J. Probability. 2011. V. 16. P. 2080–2103.
23. *Sullivan E.* Linear chord diagrams with long chords // Electronic J. Combinatorics. 2017. V. 24. No. 4. Article #P4.20.
24. *Cameron N. T. and Killpatrick K.* Statistics on linear chord diagrams // Discrete Math. Theoret. Computer Sci. 2019. V. 21. No. 2. Article #11.
25. *Краско Е. С., Лабутин И. Н., Омельченко А. В.* Перечисление помеченных и непомеченных гамильтоновых циклов в полных k-дольных графах // Зап. научн. сем. ПОМИ. 2019. Т. 488. С. 119–142.
26. *Nalli A. and Haukkanen P.* On generalized Fibonacci and Lucas polynomials // Chaos, Solitons and Fractals. 2009. V. 42. P. 3179–3186.
27. *Bednarz U. and Wołowiec-Musiał M.* Distance Fibonacci polynomials // Symmetry. 2020. V. 12. No. 9. P. 1540.
28. *Klazar M.* On identities concerning the numbers of crossing and nesting of two edges in matchings // SIAM J. Discret. Math. 2005. V. 20. P. 960–976.
29. *Björklund A., Gupt B., and Quesada N.* A faster Hafnian formula for complex matrices and its benchmarking // J. Experimental Algorithmics. 2019. V. 24. Art. No. 1.11. P. 1–17.
30. *Perepechko S. N.* Counting near-perfect matchings on $C_m \times C_n$ tori of odd order in the Maple system // Programming and Computer Software. 2019. V. 45. No. 2. P. 65–72.
31. *Chmutov S., Duzhin S., and Mostovoy J.* Introduction to Vassiliev Knot Invariants. Cambridge University Press, 2012. 504 p.
32. *Reidys C.* Combinatorial Computational Biology of RNA. N.Y.: Springer, 2011. 257 p.
33. *Léger S., Costa M. B. W., and Tulpan D.* Pairwise visual comparison of small RNA secondary structures with base pair probabilities // BMC Bioinformatics. 2019. V. 20. Article No. 293.

REFERENCES

1. *Sachkov V. N.* Vvedenie v kombinatornye metody diskretnoy matematiki. [Introduction to Combinatorial Methods of Discrete Mathematics]. Moscow, Nauka, 1982. 384 p. (in Russian)
2. *Smirnov E. Yu.* Diagrammy Yunga, ploskie razbieniya i znakochereduyushchiesya matritsy [Young Diagrams, Flat Partitions and Alternating Matrices]. Moscow, MCCME, 2014. 64 p. (in Russian)

3. *Ignat'ev M. V.* Kvantovaya kombinatorika [Quantum combinatorics]. Matem. Prosv., ser. 3, 2014, vol. 18, pp. 66–111. (in Russian)
4. *Haglund J.* The q,t-Catalan Numbers and the Space of Diagonal Harmonics. AMS, 2007. 167 p.
5. *Manin Yu. I.* Quantum Groups and Non-Commutative Geometry. Montréal, CRM, 1988. 91 p.
6. *Demidov E. E.* Kvantovye gruppy [Quantum Groups]. Moscow, Factorial, 1998. 128 p. (in Russian)
7. *Yang K.-W.* q-Determinants and permutations. Fibonacci Quart., 1991, vol. 29, no. 2, pp. 160–163.
8. *Tagawa H.* A multivariable quantum determinant over a commutative ring. RIMS Kôkyûroku, 1991, vol. 765, pp. 91–103.
9. *Shevelev V.* Combinatorial minors for matrix functions and their applications. Zeszyty Naukowe Politechniki Śląskiej. Seria: Matematyka Stosowana, 2014, no. 4, pp. 5–16.
10. *Bapat R. B. and Lal A. K.* Inequalities for the q-permanent. Linear Algebra Appl., 1994, vol. 197/198, pp. 397–409.
11. *Lal A. K.* Inequalities for the q-permanent. II. Linear Algebra Appl., 1998, vol. 274, pp. 1–16.
12. *Da Fonseca C. M.* The μ-permanent of a tridiagonal matrix, orthogonal polynomials, and chain sequences. Linear Algebra Appl., 2010, vol. 432, pp. 1258–1266.
13. *Da Fonseca C. M.* The μ-permanent, a new graph labeling, and a known integer sequence. Bulletin mathématique de la Sociétédes Sciences Mathématiques de Roumanie, 2018, vol. 61(109), no. 3, pp. 255–262.
14. *De Sá E. M.* Noncrossing partitions, noncrossing graphs, and q-permanental equations. Linear Algebra Appl., 2018, vol. 541, pp. 36–53.
15. *De Sá E. M.* Linear preservers for the q-permanent, cycle q-permanent expansions, and positive crossings in digraphs. Linear Algebra Appl., 2019, vol. 561, pp. 228–252.
16. *Kocharovsky Vit. V., Kocharovsky V. V., and Tarasov S. V.* The Hafnian Master Theorem. Linear Algebra Appl., 2022, vol. 651, pp. 144–161.
17. *Efimov D. B.* Enumeration of even and odd chord diagrams. J. Appl. Industr. Math., 2024, vol. 18, no. 2, pp. 216–226.
18. *Strickland E.* Classical invariant theory for the quantum symplectic group. Adv. Math., 1996, vol. 123, pp. 78–90.
19. *Jing N. and Zhang J.* Quantum Pfaffians and hyper-Pfaffians. Adv. Math., 2014, vol. 265, pp. 336–361.
20. *Jing N. and Zhang J.* Quantum permanents and Hafnians via Pfaffians. Lett. Math. Phys., 2016, vol. 106, pp. 1451–1464.
21. *Barvinok A.* Combinatorics and Complexity of Partition Functions. Cham, Springer, 2016. 309 p.
22. *Tribe R. and Zaboronski O.* Pfaffian formulae for one dimensional coalescing and annihilating systems. Electronic J. Probability, 2011, vol. 16, pp. 2080–2103.
23. *Sullivan E.* Linear chord diagrams with long chords. Electronic J. Combinatorics, 2017, vol. 24, no. 4, article #P4.20.
24. *Cameron N. T. and Killpatrick K.* Statistics on linear chord diagrams. Discrete Math. Theoret. Computer Sci., 2019, vol. 21, no. 2, article #11.
25. *Krasko E. S., Labutin I. N., and Omel'chenko A. V.* Perechislenie pomechennyh i nepomechennyh gamil'tonovyh ciklov v polnyh k-dol'nyh grafah [Enumeration of labeled and unlabeled Hamiltonian cycles in complete k-partite graphs]. Zapiski Nauchnyh Seminarov POMI, 2019, vol. 488, pp. 119–142. (in Russian)

26. *Nalli A. and Haukkanen P.* On generalized Fibonacci and Lucas polynomials. Chaos, Solitons and Fractals, 2009, vol. 42, pp. 3179–3186.
27. *Bednarz U. and Wołowiec-Musiał M.* Distance Fibonacci polynomials. Symmetry, 2020, vol. 12, no. 9, pp. 1540.
28. *Klazar M.* On identities concerning the numbers of crossing and nesting of two edges in matchings. SIAM J. Discret. Math., 2005, vol. 20, pp. 960–976.
29. *Björklund A., Gupt B., and Quesada N.* A faster Hafnian formula for complex matrices and its benchmarking. J. Experimental Algorithmics, 2019, vol. 24, art. no. 1.11, pp. 1–17.
30. *Perepechko S. N.* Counting near-perfect matchings on $C_m \times C_n$ tori of odd order in the Maple system. Programming and Computer Software, 2019, vol. 45, no. 2, pp. 65–72.
31. *Chmutov S., Duzhin S., and Mostovoy J.* Introduction to Vassiliev Knot Invariants. Cambridge University Press, 2012. 504 p.
32. *Reidys C.* Combinatorial Computational Biology of RNA. N.Y., Springer, 2011. 257 p.
33. *Léger S., Costa M. B. W., and Tulpan D.* Pairwise visual comparison of small RNA secondary structures with base pair probabilities. BMC Bioinformatics, 2019, vol. 20, article no. 293.

УДК 519.7 DOI 10.17223/20710410/69/2

ОПИСАНИЕ НЕКОТОРЫХ КЛАССОВ ИЗОМЕТРИЧНЫХ ОТОБРАЖЕНИЙ, СОХРАНЯЮЩИХ САМОДУАЛЬНОСТЬ ОБОБЩЁННОЙ БЕНТ-ФУНКЦИИ[1]

А. В. Куценко

Новосибирский государственный университет, г. Новосибирск, Россия

E-mail: alexandrkutsenko@bk.ru

Обобщённая булева функция, обладающая равномерным спектром Уолша — Адамара, называется обобщённой бент-функцией. Обобщённая бент-функция, совпадающая со своей дуальной бент-функцией, называется самодуальной. В работе исследуются изометричные отображения множества всех обобщённых булевых функций в себя, оставляющие класс самодуальных обобщённых бент-функций от n переменных на месте. Предложено новое отображение, сохраняющее самодуальность обобщённой бент-функции. Вводится понятие действия унитарного оператора на множестве обобщённых булевых функций от n переменных, представленных своими характеристическими векторами. В рамках рассматриваемого класса унитарных операторов описаны все отображения, сохраняющие самодуальность. Исследуется обобщённый вид изометричного отображения, соответствующего комплексному сопряжению характеристического вектора.

Ключевые слова: *обобщённая бент-функция, самодуальная бент-функция, изометричное отображение.*

CHARACTERIZATION OF SOME CLASSES OF ISOMETRIC MAPPINGS THAT PRESERVE SELF-DUALITY OF GENERALIZED BENT FUNCTION

A. V. Kutsenko

Novosibirsk State University, Novosibirsk, Russia

A generalized Boolean function with flat Walsh — Hadamard spectrum is called generalized bent (gbent) function. Gbent function that coincides with its dual bent function is called self-dual. In this paper, we study isometric mappings of the set of all generalized Boolean functions into itself that preserve self-duality. A new mapping that preserves the self-duality of a gbent function is proposed. We introduce the concept of the action of an unitary operator on the set of generalized Boolean functions in n variables, represented by their characteristic vectors. Within the considered class of unitary operators, all mappings that preserve self-duality are described. A generalized form of isometric mapping corresponding to the complex conjugation of the characteristic vector is investigated.

Keywords: *generalized Boolean function, self-dual bent finction, isometric mapping.*

[1]Работа выполнена при поддержке Математического центра в Академгородке, соглашение с Министерством науки и высшего образования РФ № 075-15-2025-349.

Введение

Бент-функции образуют один из самых известных классов булевых функций, он нашёл широкое применение в различных областях алгебры и дискретной математики. Согласно определению, бент-функцией называется булева функция от чётного числа переменных, обладающая равномерным спектром Уолша — Адамара. Равномерность спектра Уолша — Адамара открывает ряд приложений в криптографии, обработке сигналов, а также теории кодирования. Термин «бент-функция» был предложен О. Ротхаусом в 70-х годах XX в. [1], но, несмотря на долгую историю изучения данного класса функций и наличие большого количества работ, связанных с ними, по-прежнему существует много открытых проблем, в ряде случаев имеющих пересечение с другими комбинаторными объектами. Известен ряд обобщений булевых бент-функций, рассматриваемых как с теоретической, так и с практической точек зрения. Более подробную информацию о бент-функциях, их свойствах, конструкциях и связанных открытых проблемах можно найти в [2].

В настоящей работе рассматриваются функции вида $\mathbb{F}_2^n \to \mathbb{Z}_q$, где $\mathbb{F}_2^n$ — пространство двоичных векторов с n координатами; q — натуральное число. Данное обобщение булевых функций нашло приложение в теории обработки сигналов и теории кодирования [3]. В рамках данного обобщения бент-функции — это обобщённые булевы функции от n переменных с равномерным спектром Уолша — Адамара, то есть функции, обладающие тем свойством, что абсолютное значение каждого коэффициента Уолша — Адамара равно $2^{n/2}$. Такие функции называются *обобщёнными бент-функциями* [3]. Свойства и конструкции обобщённых бент-функций исследуются во многих работах, например в [4–6]. Стоит отметить, что обобщённая бент-функция не обязательно зависит от чётного числа переменных. Для класса обобщённых бент-функций вводится понятие регулярной обобщённой бент-функции, то есть такой функции, для которой определена дуальная к ней обобщённая бент-функция. Известно, что при $q = 2^k, k \geqslant 2$, все обобщённые бент-функции являются регулярными как для чётного, так и для нечётного n, за исключением единственного случая, когда $k = 2$, а n — нечётное число [7]. Регулярная обобщённая бент-функция, совпадающая со своей дуальной, называется самодуальной. Класс самодуальных булевых бент-функций получил большое внимание, ему посвящено много работ, в частности [8–13]. Один из открытых вопросов о самодуальных обобщённых бент-функциях — описание изометричных отображений, сохраняющих самодуальность. Данный вопрос тесно связан с задачей исследования группы автоморфизмов этого класса функций, что подразумевает изучение его структурных и метрических свойств. Дополнительно ставятся вопросы выбора метрики и исследования группы автоморфизмов в различных метриках. Подробную информацию о других известных обобщениях бент-функций, а также их свойствах и приложениях можно найти в [2, 14].

Настоящая работа посвящена изучению изометричных отображений множества всех обобщённых булевых функций от n переменных в себя, сохраняющих самодуальность. Рассматриваются отображения вида

$$f(x) \to \gamma \cdot f(\pi(x)) + g(x), \quad x \in \mathbb{F}_2^n,$$

где $\gamma \in \{1, q-1\}$; π — подстановка на множестве $\mathbb{F}_2^n$; g — обобщённая булева функция от n переменных. Работа имеет следующую структуру. В п. 1 даются необходимые определения и обозначения. В п. 2 приводится обобщение некоторых свойств множества характеристических векторов самодуальных бент-функций. В п. 3 вводится понятие действия линейного оператора $\mathbb{C}^{2^n} \to \mathbb{C}^{2^n}$ на множестве обобщённых булевых

функций от n переменных, описываются все унитарные операторы, отображающие множество всех обобщённых булевых функций от n переменных в себя. Каждый такой оператор определяет некоторое изометричное отображение в метрике Хэмминга и метрике Ли. В п. 4 предложено новое отображение, сохраняющее самодуальность обобщённой бент-функции. В рамках рассматриваемого класса унитарных операторов (то есть при $\gamma = 1$) описаны все операторы, сохраняющие самодуальность обобщённой бент-функции. В п. 5 исследуется изометричное отображение, основанное на комплексном сопряжении характеристического вектора, а также его обобщение ($\gamma = q - 1$).

1. Используемые определения и обозначения

Весом Хэмминга $\mathrm{wt_H}(x)$ вектора $x \in \mathbb{F}_2^n$ называется число координат x, отличных от нуля. Для $x, y \in \mathbb{F}_2^n$ через $\langle x, y\rangle$ обозначим выражение $\bigoplus\limits_{i=1}^{n} x_i y_i$, где $\oplus$ — сложение по модулю 2. *Обобщённой булевой функцией* от n переменных называется произвольное отображение из пространства $\mathbb{F}_2^n$ в кольцо $\mathbb{Z}_q$ [15]. В случае $q = 2$ функция называется *булевой* функцией. *Расстоянием Хэмминга* $\mathrm{dist_H}(f, g)$ между обобщёнными булевыми функциями f, g от n переменных называется число векторов из пространства $\mathbb{F}_2^n$, на которых функции принимают разные значения. *Весом Ли* элемента $x \in \mathbb{Z}_q$ называется число $\mathrm{wt_L}(x) = \min\{x, q - x\}$. *Весом Ли* обобщённой булевой функции от n переменных называется сумма весов Ли всех её значений:

$$\mathrm{wt_L}(f) = \sum_{x \in \mathbb{F}_2^n} \mathrm{wt_L}(f(x)).$$

Расстояние Ли $\mathrm{dist_L}(f, g)$ между обобщёнными булевыми функциями f, g от n переменных есть число $\mathrm{wt_L}(f - g)$. В булевом случае $q = 2$ веса, а также расстояния Хэмминга и Ли совпадают.

Пусть $\omega = e^{2\pi i/q}$ — примитивный корень степени q из 1. *Характеристическим вектором* обобщённой булевой функции f от n переменных называется вектор

$$F = \omega^f = \left(\omega^{f_0}, \omega^{f_1}, \ldots, \omega^{f_{2^n-1}}\right)$$

с 2^n координатами, где $(f_0, f_1, \ldots, f_{2^n-1})$ — вектор значений функции f. *Преобразованием Уолша — Адамара* обобщённой булевой функции f от n переменных называется комплекснозначная функция

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

Обобщённая булева функция f от n переменных называется *обобщённой бент-функцией*, если

$$|H_f(y)| = 2^{n/2}$$

для всех $y \in \mathbb{F}_2^n$ [3] (см. также препринт 2006 г.). Если существует обобщённая булева функция $\widetilde{f}$ от n переменных, такая, что $H_f(y) = \omega^{\widetilde{f}(y)} 2^{n/2}$ для всех $y \in \mathbb{F}_2^n$, то f называется *регулярной*, а $\widetilde{f}$ — её *дуальной*. Отметим, что дуальная функция $\widetilde{f}$ также является обобщённой бент-функцией; в булевом случае $q = 2$ все бент-функции регулярные.

Регулярная обобщённая бент-функция f называется *самодуальной*, если $f = \widetilde{f}$, и *антисамодуальной*, если $f = \widetilde{f} + q/2$. Таким образом, в настоящей работе при рассмотрении антисамодуальных обобщённых бент-функций считается, что q — чётное число. Соответствующие множества функций будем обозначать через $\mathcal{SB}_n^{q,+}$ и $\mathcal{SB}_n^{q,-}$.

2. Характеристические векторы самодуальных обобщённых бент-функций

Приведём обобщение некоторых известных фактов о характеристических векторах самодуальных булевых бент-функций [8, 11, 12].

Ненулевой вектор $v \in \mathbb{C}^n$ называется *собственным вектором* $(n \times n)$-матрицы A, соответствующим *собственному числу* $\lambda \in \mathbb{C}$, если $Av = \lambda v$. Линейная оболочка собственных векторов, соответствующих собственному числу λ, называется *собственным подпространством*, соответствующим собственному числу λ. *Ядром* линейного оператора $\varphi : \mathbb{C}^n \to \mathbb{C}^n$ называется множество

$$\mathrm{Ker}(\varphi) = \{x \in \mathbb{C}^n : \varphi(x) = \mathbf{0} \in \mathbb{C}^n\},$$

где $\mathbf{0}$ — нулевой элемент пространства $\mathbb{C}^n$.

Принимая во внимание тот факт, что в фиксированном базисе каждый линейный оператор $\mathbb{C}^n \to \mathbb{C}^n$ характеризуется некоторой $(n \times n)$-матрицей, приведённые понятия можно рассматривать как по отношению к линейным операторам, так и по отношению к квадратным матрицам соответствующего порядка, что далее используется в зависимости от контекста.

Матрицей Сильвестра — Адамара (матрицей Адамара типа Сильвестра) порядка n называется $(2^n \times 2^n)$-матрица

$$H_n = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}^{\otimes n},$$

где $\otimes$ — операция кронекерова произведения. Как матрица Адамара, данная матрица обладает следующим свойством:

$$H_n H_n^{\mathrm{T}} = 2^n I_{2^n},$$

где I_{2^n} — единичная матрица порядка 2^n.

Обозначим $\mathcal{H}_n = 2^{-n/2} H_n$, данная матрица является симметричной и ортогональной. В силу того, что строки матрицы H_n соответствуют характеристическим векторам всех линейных булевых функций от n переменных, взятых в лексикографическом порядке, регулярную обобщённую бент-функцию от n переменных можно определить как функцию, чей характеристический вектор F удовлетворяет условию $\mathcal{H}_n F \in \{\pm 1\}^{2^n}$. Таким образом, характеристический вектор самодуальной обобщённой бент-функции является собственным вектором матрицы $\mathcal{H}_n$, соответствующим собственному числу $+1$. Аналогично характеристический вектор антисамодуальной обобщённой бент-функции является собственным вектором матрицы $\mathcal{H}_n$, соответствующим собственному числу -1.

В работе [8] рассматривается ортогональное разложение пространства $\mathbb{R}^{2^n}$ по собственным подпространствам матрицы $\mathcal{H}_n$:

$$\mathbb{R}^{2^n} = \mathrm{Ker}\left(\mathcal{H}_n + I_{2^n}\right) \oplus \mathrm{Ker}\left(\mathcal{H}_n - I_{2^n}\right).$$

Здесь символом $\oplus$ обозначается прямая сумма подпространств. Нетрудно видеть, что аналогичное разложение можно получить и для комплекснозначного пространства:

$$\mathbb{C}^{2^n} = \mathrm{Ker}\left(\mathcal{H}_n + I_{2^n}\right) \oplus \mathrm{Ker}\left(\mathcal{H}_n - I_{2^n}\right).$$

Известно, что

$$\dim\left(\mathrm{Ker}\left(\mathcal{H}_n + I_{2^n}\right)\right) = \dim\left(\mathrm{Ker}\left(\mathcal{H}_n - I_{2^n}\right)\right) = 2^{n-1},$$

где $\dim(V)$ есть размерность подпространства $V \subseteq \mathbb{R}^{2^n}$. Как отмечено ранее, матрица $\mathcal{H}_n$ является симметричной, следовательно, подпространства $\mathrm{Ker}\,(\mathcal{H}_n + I_{2^n})$ и $\mathrm{Ker}\,(\mathcal{H}_n - I_{2^n})$ являются взаимно ортогональными.

В работе [11] доказано, что при $n \geqslant 4$ множества характеристических векторов (анти)самодуальных булевых бент-функций от n переменных порождают собственные подпространства матрицы $\mathcal{H}_n$, то есть имеют размерность 2^{n-1}. Данный результат можно обобщить следующим образом:

Утверждение 1. Пусть $n \geqslant 4$, тогда множества характеристических векторов (анти)самодуальных обобщённых булевых бент-функций от n переменных порождают собственные подпространства матрицы $\mathcal{H}_n$, то есть имеют размерность 2^{n-1}.

Доказательство. Достаточно заметить, что в силу чётности q справедливо $(-1) = \omega^{q/2} \in \{\omega, \omega^2, \ldots, \omega^{q-1}\}$. ■

В случае $n = 2$ и $q = 2$ есть только две самодуальные обобщённые бент-функции: x_1x_2 и $x_1x_2 \oplus 1$, имеющие характеристические векторы $(1, 1, 1, -1)$ и $(-1, -1, -1, 1)$ соответственно. Данные векторы, очевидно, линейно зависимы в $\mathbb{R}^4$. Рассматривая случай произвольного чётного q, получаем систему

$$\frac{1}{2}\begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{pmatrix}\begin{pmatrix} \omega^{d_1} \\ \omega^{d_2} \\ \omega^{d_3} \\ \omega^{d_4} \end{pmatrix} = \begin{pmatrix} \omega^{d_1} \\ \omega^{d_2} \\ \omega^{d_3} \\ \omega^{d_4} \end{pmatrix}$$

с переменными $d_1, d_2, d_3, d_4 \in \mathbb{Z}_q$. Все её решения имеют вид

$$\left(\omega^d, \omega^d, \omega^d, \omega^{d+q/2}\right) = \omega^d\,(1, 1, 1, -1) \in \mathbb{C}^4,$$

где $d \in \mathbb{Z}_q$.

Случай антисамодуальных бент-функций рассматривается аналогично. Таким образом, характеристические векторы из множеств $\mathcal{SB}_2^{q,\pm}$ также линейно зависимы в $\mathbb{C}^4$.

3. Изометричные отображения и унитарные операторы

Пусть на множестве всех обобщённых булевых функций определена метрика ρ. Взаимно однозначное отображение φ множества обобщённых булевых функций от n переменных в себя называется *изометричным* относительно метрики ρ, если для любой пары обобщённых булевых функций f, g от n переменных выполняется соотношение

$$\rho(\varphi(f), \varphi(g)) = \rho(f, g).$$

Группой автоморфизмов множества всех обобщённых булевых функций от n переменных относительно метрики ρ называется группа изометричных отображений множества всех обобщённых булевых функций от n переменных в себя.

В булевом случае, как правило, в качестве метрики ρ рассматривается расстояние Хэмминга. В случае обобщённых булевых функций далее рассматриваются две метрики — расстояние Хэмминга и расстояние Ли.

В данном пункте приведено определение действия линейного оператора $\mathbb{C}^{2^n} \to \mathbb{C}^{2^n}$ на множестве обобщённых булевых функций от n переменных; охарактеризована группа всех унитарных операторов, отображающих множество всех обобщённых булевых функций от n переменных в себя; показано, что каждый оператор из этой группы соответствует некоторому изометричному отображению. Для двоичного случая отмечается связь с известными результатами применительно к группе автоморфизмов множества всех булевых функций от n переменных.

3.1. Линейные операторы и обобщённые булевы функции

Всюду далее подразумевается использование стандартного базиса пространства $\mathbb{C}^{2^n}$, который состоит из векторов $e_i \in \mathbb{C}^{2^n}$, $i = 1, \ldots, 2^n$, где e_i имеет 1 на позиции i, а остальные координаты равны нулю.

Пусть $\varphi : \mathbb{C}^{2^n} \to \mathbb{C}^{2^n}$ — линейный оператор с матрицей M_φ в стандартном базисе пространства $\mathbb{C}^{2^n}$. Будем говорить, что φ *отображает* обобщённую булеву функцию f от n переменных с характеристическим вектором F в обобщённую булеву функцию f' от n переменных с характеристическим вектором F', если $F' = M_\varphi F$, т. е. действие отображения определено на характеристических векторах длины 2^n следующим образом: $F' = M_\varphi F = \varphi(F)$.

Линейный оператор φ называется *унитарным*, если $\varphi\varphi^* = \varphi^*\varphi = \mathrm{id}$, где φ^* — эрмитово сопряжённый к φ оператор. Матрица отображения φ в этом случае является унитарной. Через $\mathcal{U}_n^q$ обозначим группу всех унитарных операторов $\mathbb{C}^{2^n} \to \mathbb{C}^{2^n}$, которые отображают множество всех обобщённых булевых функций от n переменных в себя.

Следующий результат полностью характеризует группу $\mathcal{U}_n^q$. Напомним, что квадратная матрица над полем $\mathbb{F}$ называется *обобщённой перестановочной* или *мономиальной*, если в каждой её строке, а также в каждом столбце присутствует ровно один ненулевой элемент поля $\mathbb{F}$.

Теорема 1. Существует взаимно однозначное соответствие между элементами группы $\mathcal{U}_n^q$ и обобщёнными перестановочными матрицами порядка 2^n с ненулевыми элементами из множества $\{1, \omega, \omega^2, \ldots, \omega^{q-1}\}$.

Доказательство. Нетрудно видеть, что операторы, которым соответствуют обобщённые перестановочные матрицы с элементами указанного вида, отображают множество обобщённых булевых функций от n переменных в себя. Более того, каждый такой оператор является унитарным.

Обратно, положим $\varphi \in \mathcal{U}_n^q$ и пусть $U = (u_{ij})$ — его матрица в стандартном базисе. Обозначим через $v_0 \in \mathbb{C}^{2^n}$ вектор из всех единиц, а через $v_i \in \mathbb{C}^{2^n}$, $i = 1, \ldots, 2^n$, — вектор с 1 на позиции i, все остальные координаты которого равны (-1). Пусть $v_{ij} \in \in \mathbb{C}^{2^n}$, $i, j = 1, \ldots, 2^n$, $i \neq j$, — вектор с единицами на позициях с номерами i и j, в то время как оставшиеся равны (-1).

Зафиксируем некоторые $i, j, k \in \{1, \ldots, 2^n\}$, $i < j$. Обозначим $(Uv_0)_k = \omega^{d_0}$, $(Uv_i)_k = \omega^{d_i}$, $(Uv_j)_k = \omega^{d_j}$ и $(Uv_{ij})_k = \omega^{d_{ij}}$ для некоторых $d_0, d_i, d_j, d_{ij} \in \mathbb{Z}_q$. Их суммы равны

$$\begin{aligned}
(Uv_0)_k + (Uv_i)_k &= 2u_{ki} = \omega^{d_0} + \omega^{d_i}, \\
(Uv_0)_k + (Uv_j)_k &= 2u_{kj} = \omega^{d_0} + \omega^{d_j}, \\
(Uv_0)_k + (Uv_{ij})_k &= 2\,(u_{ki} + u_{kj}) = \omega^{d_0} + \omega^{d_{ij}}.
\end{aligned}$$

После перегруппировки получаем

$$u_{ki} = (\omega^{d_0} + \omega^{d_i})/2, \qquad u_{kj} = (\omega^{d_0} + \omega^{d_j})/2, \qquad u_{ki} + u_{kj} = (\omega^{d_0} + \omega^{d_{ij}})/2,$$

то есть

$$\omega^{d_0} + \omega^{d_i} + \omega^{d_0} + \omega^{d_j} = \omega^{d_0} + \omega^{d_{ij}},$$

или, после сокращения подобных,

$$\omega^{d_0} + \omega^{d_i} + \omega^{d_j} = \omega^{d_{ij}}.$$

Это возможно лишь в случае, когда число $\omega^{d_{ij}}$ совпадает с одним из чисел $\omega^{d_0}, \omega^{d_i}, \omega^{d_j}$, в то время как два оставшихся отличаются друг от друга лишь знаком, что всегда допустимо, так как q — чётное число.

Рассмотрим два случая:

С л у ч а й 1. Пусть $\omega^{d_{ij}} = \omega^{d_0}$ и $\omega^{d_i} + \omega^{d_j} = 0$, тогда k-я строка матрицы U есть

$$U_k = \left(u_{k,1},\ \ldots,\ u_{k,i-1},\ (\omega^{d_0} - \omega^{d_j})/2,\ u_{k,i+1},\ \ldots,\ u_{k,j-1},\ (\omega^{d_0} + \omega^{d_j})/2,\ u_{k,j+1},\ \ldots,\ u_{k,2^n}\right).$$

В этом случае справедливо

$$\begin{aligned}|u_{ki}|^2 + |u_{kj}|^2 &= \frac{1}{4}\left(\left|\omega^{d_0} - \omega^{d_j}\right|^2 + \left|\omega^{d_0} + \omega^{d_j}\right|^2\right) = \\ &= \frac{1}{4}\left[\left(\omega^{d_0} - \omega^{d_j}\right)\left(\omega^{-d_0} - \omega^{-d_j}\right) + \left(\omega^{d_0} + \omega^{d_j}\right)\left(\omega^{-d_0} + \omega^{-d_j}\right)\right] = \\ &= \frac{1}{4}\left(2 \cdot \omega^{d_0}\omega^{-d_0} + 2 \cdot \omega^{d_j}\omega^{-d_j}\right) = \frac{1}{4}(2+2) = 1\end{aligned}$$

и в силу того, что U — унитарная матрица, имеем $\|U_k\|^2 = 1$ для всех $k \in \{1, \ldots, 2^n\}$. Следовательно, все координаты U_k, кроме, может быть, $u_{ki} = (\omega^{d_0} - \omega^{d_j})/2$, $u_{kj} = (\omega^{d_0} + \omega^{d_j})/2$, должны быть равну нулю.

С л у ч а й 2. Без ограничения общности предположим, что $\omega^{d_{ij}} = \omega^{d_i}$ и $\omega^{d_0} + \omega^{d_j} = 0$, тогда $u_{kj} = 0$.

Таким образом, для любых различных индексов $i, j \in \{1, \ldots, 2^n\}$ возможны две ситуации: либо по крайней мере один из элементов u_{ki}, u_{kj} k-й строки матрицы U нулевой, либо в данной строке не более двух ненулевых элементов, при этом их форма описана в случае 1.

Анализ случаев. Если для каждой строки имеет место только случай 2, то матрица U является обобщённо перестановочной, так как в каждой её строке присутствует ровно один ненулевой элемент. Предположим, что одна из строк матрицы U, например с номером k, имеет вид, описанный в случае 1. Заметим, что в матрице U найдётся ещё как минимум одна строка такого же вида.

Рассмотрим (характеристический) вектор $F \in \mathbb{C}^{2^n}$, чьи координаты с номерами $\ell = 1, \ldots, 2^n$ имеют вид

$$F_\ell = \begin{cases} \omega^{r_1}, & \ell = i, \\ \omega^{r_2}, & \ell = j, \\ 1, & \text{иначе}, \end{cases}$$

где $r_1, r_2 \in \mathbb{Z}_q$, при этом $r_1 < r_2$ и $r_2 - r_1 \neq q/2$. Обозначив $\Delta r = r_2 - r_1$, запишем

$$(UF)_k = u_{ki}\omega^{r_1} + u_{kj}\omega^{r_2} = \omega^{r_1}\left(\frac{\omega^{d_0} - \omega^{d_j}}{2} + \frac{\omega^{d_0} + \omega^{d_j}}{2}\omega^{\Delta r}\right).$$

В силу того, что UF — характеристический вектор обобщённой булевой функции от n переменных, для некоторого $s \in \mathbb{Z}_q$ имеем $(UF)_k = \omega^{r_1+s}$. Тогда справедливо

$$\frac{\omega^{d_0} - \omega^{d_j}}{2} + \frac{\omega^{d_0} + \omega^{d_j}}{2}\omega^{\Delta r} = \omega^s.$$

Используем известные тригонометрические соотношения: пусть $\alpha, \beta \in \mathbb{R}$, тогда

$$\begin{aligned}
\cos\alpha + \cos\beta &= 2\cos\big((\alpha+\beta)/2\big)\cos\big((\alpha-\beta)/2\big),\\
\cos\alpha - \cos\beta &= -2\sin\big((\alpha+\beta)/2\big)\sin\big((\alpha-\beta)/2\big),\\
\sin\alpha \pm \sin\beta &= 2\sin\big((\alpha\pm\beta)/2\big)\cos\big((\alpha\mp\beta)/2\big),\\
\sin(\alpha\pm\beta) &= \sin\alpha\cos\beta \pm \cos\alpha\sin\beta,\\
\sin 2\alpha &= 2\cos\alpha\sin\alpha.
\end{aligned}$$

Рассмотрим удвоенную вещественную часть числа ω^s:

$$\begin{aligned}
2\mathrm{Re}\,(\omega^s) &= \cos(2\pi d_0/q) - \cos(2\pi d_j/q) + \cos\big(2\pi(d_0+\Delta r)/q\big) + \cos\big(2\pi(d_j+\Delta r)/q\big) =\\
&= 2\cos\big(\pi(2d_0+\Delta r)/q\big)\cos(\pi\Delta r/q) - 2\sin\big(\pi(2d_j+\Delta r)/q\big)\sin(\pi\Delta r/q),
\end{aligned}$$

и удвоенную мнимую часть:

$$\begin{aligned}
2\mathrm{Im}\,(\omega^s) &= \sin(2\pi d_0/q) - \sin(2\pi d_j/q) + \sin\big(2\pi(d_0+\Delta r)/q\big) + \sin\big(2\pi(d_j+\Delta r)/q\big) =\\
&= 2\sin\big(\pi(2d_0+\Delta r)/q\big)\cos(\pi\Delta r/q) + \sin(\pi\Delta r/q)\cos\big(\pi(2d_j+\Delta r)/q\big).
\end{aligned}$$

Обозначим $\alpha = \pi\Delta r/q$, $\beta = \pi(2d_0+\Delta r)/q$ и $\gamma = \pi(2d_j+\Delta r)/q$. В силу того, что число ω^s является корнем из единицы, его абсолютное значение равно 1, следовательно,

$$\begin{aligned}
\mathrm{Re}^2\,(\omega^s) + \mathrm{Im}^2\,(\omega^s) &= \cos^2\alpha\cos^2\beta - 2\cos\alpha\sin\alpha\cos\beta\sin\gamma + \sin^2\alpha\sin^2\gamma +\\
&+ \cos^2\alpha\sin^2\beta + 2\cos\alpha\sin\alpha\sin\beta\cos\gamma + \sin^2\alpha\cos^2\gamma =\\
= \cos^2\alpha(\cos^2\beta + \sin^2\beta) + \sin^2\alpha\big(\cos^2\gamma + \sin^2\gamma\big) &+ 2\cos\alpha\sin\alpha(\sin\beta\cos\gamma - \cos\beta\sin\gamma) =\\
&= 1 + \sin(2\alpha)\sin(\beta-\gamma) = 1,
\end{aligned}$$

то есть $\sin(2\alpha)\sin(\beta-\gamma) = 0$. Если первый множитель равен нулю, то

$$2\alpha = 2\pi\Delta r/q = \pi m, \quad m \in \mathbb{Z}.$$

Тогда $\Delta r = mq/2$, но в силу того, что $\Delta r \in \{1, \ldots, q-1\}$, это может иметь место только при $\Delta r = q/2$, что противоречит выбору r_1, r_2. Если второй множитель нулевой, то

$$\beta - \gamma = 2\pi(d_0 - d_j)/q = \pi m', \quad m' \in \mathbb{Z},$$

и снова $d_0 = d_j$ или $|d_0 - d_j| = q/2$, так как $|d_0 - d_j| \in \{0, 1, \ldots, q-1\}$. Но тогда либо $\omega^{d_0} - \omega^{d_j} = 0$, либо $\omega^{d_0} + \omega^{d_j} = 0$, то есть в строке с номером k есть в точности один ненулевой элемент. ■

Следствие 1. Порядок группы $\mathcal{U}_n^q$ равен $|\mathcal{U}_n^q| = (2^n)! \cdot q^{2^n}$.

3.2. Связь с теоремой Маркова для двоичного случая

Из теоремы А. А. Маркова (1956) следует, что общий вид группы автоморфизмов множества всех булевых функций от n переменных в себя есть

$$f(x) \longrightarrow f(\pi(x)) \oplus g(x), \quad x \in \mathbb{F}_2^n,$$

где π — подстановка на пространстве $\mathbb{F}_2^n$ и g — булева функция от n переменных [16]. Группа таких отображений в литературе также именуется как *группа Джевонса* (см., например, [17]).

Теорема 1 может быть переформулирована следующим образом:

Теорема 2. Действие любого элемента группы $\mathcal{U}_n^q$ на множестве всех обобщённых булевых функций от n переменных единственным образом представимо в виде

$$f(x) \longrightarrow f(\pi(x)) + g(x), \quad x \in \mathbb{F}_2^n,$$

где π — подстановка на пространстве $\mathbb{F}_2^n$ и g — обобщённая булева функция от n переменных.

Следуя работе [12], будем обозначать такой оператор через $\varphi_{\pi,g} \in \mathcal{U}_n^q$. Для двоичного случая немедленно получаем

Следствие 2. При $q = 2$ группа $\mathcal{U}_n^q$ изоморфна группе автоморфизмов множества булевых функций от n переменных.

Таким образом, группа $\mathcal{U}_n^q$ есть естественное обобщение отображений из группы автоморфизмов множества всех булевых функций от n переменных на случай обобщённых булевых функций. С точки зрения метрических свойств интересно следующее

Утверждение 2. Каждый элемент $\mathcal{U}_n^q$ сохраняет расстояние Хэмминга и расстояние Ли между обобщёнными булевыми функциями от n переменных.

Таким образом, все элементы группы $\mathcal{U}_n^q$ являются изометричными отображениями относительно упомянутых метрик.

3.3. Матричное представление

По теореме 1 при фиксированном (стандартном) базисе существует взаимно однозначное соответствие между элементами группы $\mathcal{U}_n^q$ и множеством всех обобщённо перестановочных матриц размера $2^n \times 2^n$ с ненулевыми элементами из множества $\{1, \omega^1, \omega^2, \ldots, \omega^{q-1}\}$. Действительно, рассмотрим произвольное отображение $\varphi_{\pi,g} \in \mathcal{U}_n^q$. Пусть оно отображает обобщённую булеву функцию f от n переменных с характеристическим вектором

$$F = \left(\omega^{f(\mathbf{v}_0)}, \omega^{f(\mathbf{v}_1)}, \ldots, \omega^{f(\mathbf{v}_{2^n-1})}\right) \in \mathbb{C}^{2^n}$$

в функцию $f' \in \mathcal{GF}_n^q$ с характеристическим вектором

$$F' = \left(\omega^{f'(\mathbf{v}_0)}, \omega^{f'(\mathbf{v}_1)}, \ldots, \omega^{f'(\mathbf{v}_{2^n-1})}\right) \in \mathbb{C}^{2^n},$$

то есть $F' = UF$, где U — матрица, соответствующая отображению $\varphi_{\pi,g}$:

$$\begin{array}{c} \\ (i+1) \end{array} \begin{array}{c} \begin{array}{ccccccc} & & & \pi(\mathbf{v}_i) & & & \end{array} \\ \begin{pmatrix} 0 & \ldots & 0 & \omega^{g(\mathbf{v}_i)} & 0 & \ldots & 0 \end{pmatrix} \end{array}.$$

Здесь $\mathbf{v}_0, \mathbf{v}_1, \ldots, \mathbf{v}_{2^n-1}$ — все векторы пространства $\mathbb{F}_2^n$ в лексикографическом порядке; в строке с номером $(i+1) \in \{1, 2, \ldots, 2^n\}$ ненулевой элемент находится в столбце с номером $(j+1)$, где j — число с двоичной записью $\pi(\mathbf{v}_i)$. Тогда i-я координата вектора $F' = UF$ равна

$$\omega^{f'(\mathbf{v}_{i-1})} = \omega^{f(\pi(\mathbf{v}_{i-1}))} \cdot \omega^{g(\mathbf{v}_{i-1})} = \omega^{f(\pi(\mathbf{v}_{i-1}))+g(\mathbf{v}_{i-1})},$$

или, другими словами,

$$f'(x) = f(\pi(x)) + g(x), \quad x \in \mathbb{F}_2^n.$$

4. Унитарные операторы и (анти)самодуальность обобщённой бент-функции

Обозначим, следуя [18], ортогональную группу порядка n над полем $\mathbb{F}_2$ через

$$\mathcal{O}_n = \left\{ L \in \mathrm{GL}\,(n, \mathbb{F}_2) : LL^{\mathrm{T}} = I_n \right\},$$

где L^{T} — результат транспонирования L; I_n — единичная матрица порядка n над полем $\mathbb{F}_2$.

Задача исследования различных типов эквивалентности и нахождения всех соответствующих классов эквивалентности является более сложной для случая обобщённых булевых и обобщённых бент-функций. Различные типы эквивалентности для функций вида $\mathbb{F}_p^n \to \mathbb{Z}_{p^k}$, где p — простое, такие, как расширенная аффинная эквивалентность (EA), а также более общая CCZ-эквивалентность, изучаются в работе [6]. Для самодуальных обобщённых бент-функций случай $q = 4$ рассматривается в [5].

4.1. Унитарные операторы, сохраняющие (анти)самодуальность обобщённой бент-функции

В работе [10] (см. также [8]) показано, что отображения вида

$$f(x) \longrightarrow f\left(L\left(x \oplus c\right)\right) \oplus \langle c, x \rangle \oplus d, \quad x \in \mathbb{F}_2^n,$$

где $L \in \mathcal{O}_n$; $c \in \mathbb{F}_2^n$; $\mathrm{wt}(c)$ — чётное число; $d \in \mathbb{F}_2$, сохраняют самодуальность булевой бент-функции. Группа, состоящая из всех таких отображений, названа *расширенной ортогональной* группой и обозначена через $\overline{\mathcal{O}}_n$. Известно, что она является подгруппой группы $\mathrm{GL}\,(n+2, \mathbb{F}_2)$ [10].

В [12] доказано, что группы автоморфизмов множеств самодуальных и антисамодуальных бент-функций от n переменных в точности равны расширенной ортогональной группе.

Применительно к обобщённым булевым функциям известно несколько примеров отображений, оставляющих классы обобщённых бент-функций, самодуальных обобщённых бент-функций на месте. Расширенное аффинное преобразование обобщённой бент-функции f от n переменных, имеющее вид

$$f(x) \longrightarrow f(Ax \oplus b) + \lambda\langle c, x \rangle + d, \quad x \in \mathbb{F}_2^n,$$

где $A \in \mathrm{GL}\,(n, \mathbb{F}_2)$; $b, c \in \mathbb{F}_2^n$; $d \in \mathbb{Z}_q$; $\lambda \in \{0, q/2\}$, переводит данную функцию в обобщённую бент-функцию [4]. Случай $q = 4$ самодуальных бент-функций рассмотрен в [5], где показано, что отображение $f \to (-f) \bmod 4$, а также частный случай аффинного отображения вида

$$f(x) \longrightarrow f\left(Lx\right) + d, \quad x \in \mathbb{F}_2^n, \tag{1}$$

где $L \in \mathcal{O}_n$, $d \in \mathbb{Z}_4$, сохраняют самодуальность обобщённой бент-функции.

В настоящей работе предлагается новое расширеннное аффинное преобразование, сохраняющее самодуальность обобщённой бент-функции.

Утверждение 3. Отображения множества всех обобщённых булевых функций от n переменных в себя, имеющие вид

$$f(x) \longrightarrow f\left(L\left(x \oplus c\right)\right) + \frac{q}{2}\langle c, x \rangle + d, \quad x \in \mathbb{F}_2^n,$$

где $L \in \mathcal{O}_n$; $c \in \mathbb{F}_2^n$; $\mathrm{wt}(c)$ — чётное число; $d \in \mathbb{Z}_q$, сохраняют (анти)самодуальность обобщённой бент-функции от n переменных.

Доказательство. Пусть $f \in \mathcal{SB}_n^{q,+} \cup \mathcal{SB}_n^{q,-}$, то есть $\widetilde{f} = f + \dfrac{q}{2}\varepsilon$ для некоторого $\varepsilon \in \mathbb{F}_2$. Рассмотрим функцию $g(x) = f(L(x \oplus c)) + \dfrac{q}{2}\langle c, x\rangle + d$, где $L \in \mathcal{O}_n$; $c \in \mathbb{F}_2^n$; $\mathrm{wt}(c)$ — чётное число; $d \in \mathbb{Z}_q$. Её коэффициенты Уолша — Адамара имеют вид

$$H_g(y) = \sum_{x\in\mathbb{F}_2^n} \omega^{g(x)}(-1)^{\langle x,y\rangle} = \sum_{x\in\mathbb{F}_2^n} \omega^{f(L(x\oplus c))+(q/2)\langle c,x\rangle+d+(q/2)\langle x,y\rangle} = \omega^d \sum_{x\in\mathbb{F}_2^n} \omega^{(q/2)\langle x,y\oplus c\rangle+f(L(x\oplus c))} =$$
$$= \omega^d \sum_{z\in\mathbb{F}_2^n} \omega^{(q/2)\langle L^{-1}z\oplus c,y\oplus c\rangle+f(z)} = \omega^{d+(q/2)\langle c,y\rangle+(q/2)\langle c,c\rangle} \sum_{z\in\mathbb{F}_2^n} \omega^{(q/2)\langle z,L(y\oplus c)\rangle+f(z)} =$$
$$= \omega^{d+(q/2)\langle c,y\rangle} 2^{n/2} \omega^{\widetilde{f}(L(y\oplus c))} = 2^{n/2}\omega^{f(L(y\oplus c))+(q/2)\langle c,y\rangle+d+(q/2)\varepsilon} = 2^{n/2}\omega^{g(y)+(q/2)\varepsilon} = 2^{n/2}\omega^{\widetilde{g}(y)},$$

следовательно, $\widetilde{g}(y) = g(y) + (q/2)\varepsilon$ для каждого $y \in \mathbb{F}_2^n$. ■

Далее охарактеризованы все операторы из множества $\mathcal{U}_n^q$, сохраняющие самодуальность обобщённой бент-функции, и установлена их связь с отображениями из утверждения 3.

Сначала установим взаимосвязь между сохранением отображением самодуальности и антисамодуальности, а также матрицей, соответствующей такому изометричному отображению:

Утверждение 4. Для оператора $\varphi_{\pi,g} \in \mathcal{U}_n^q$ с матрицей U следующие условия эквивалентны:

1) $\varphi_{\pi,g}$ сохраняет самодуальность;
2) $\varphi_{\pi,g}$ сохраняет антисамодуальность;
3) $U\mathcal{H}_n = \mathcal{H}_n U$.

Доказательство. Достаточно заметить, что по утверждению 1 при $n \geqslant 4$ существует подмножество $\{f_i\}_{i=1}^{2^{n-1}} \subseteq \mathcal{SB}_n^{q,+}$ с линейно независимыми характеристическими векторами $\{F_i\}_{i=1}^{2^{n-1}} \subseteq \mathrm{Ker}\,(\mathcal{H}_n - I_{2^n})$ и подмножество $\{g_i\}_{i=1}^{2^{n-1}} \subseteq \mathcal{SB}_n^{q,-}$ с линейно независимыми характеристическими векторами $\{G_i\}_{i=1}^{2^{n-1}} \subseteq \mathrm{Ker}\,(\mathcal{H}_n + I_{2^n})$.

Дальнейшие рассуждения повторяют доказательство [12, Proposition 2]. ■

В работе [12] описаны все изометричные отображения множества всех булевых функций от n переменных в себя, сохраняющие самодуальность, а именно: доказано, что изометричные отображения вида $f(x) \to f(\pi(x)) \oplus g(x)$ сохраняют самодуальность, если и только если

$$\pi(x) = L(x \oplus c), \quad g(x) = \langle c, x\rangle \oplus d, \quad x \in \mathbb{F}_2^n,$$

где $L \in \mathcal{O}_n$; $c \in \mathbb{F}_2^n$; $\mathrm{wt}(c)$ — чётное число; $d \in \mathbb{F}_2$.

Следующее утверждение характеризует все операторы из множества $\mathcal{U}_n^q$, сохраняющие (анти)самодуальность обобщённой бент-функции.

Теорема 3. Оператор $\varphi_{\pi,g} \in \mathcal{U}_n^q$ сохраняет (анти)самодуальность, если и только если

$$\pi(x) = L(x \oplus c), \quad g(x) = \frac{q}{2}\langle c, x\rangle + d, \quad x \in \mathbb{F}_2^n,$$

где $L \in \mathcal{O}_n$; $c \in \mathbb{F}_2^n$; $\mathrm{wt}(c)$ — чётное число; $d \in \mathbb{Z}_q$.

Доказательство. Достаточность следует из утверждения 3.

Пусть U — матрица оператора $\varphi_{\pi,g} \in \mathcal{U}_n^q$, сохраняющего (анти)самодуальность, то есть $\varphi_{\pi,g}$ имеет вид $f(x) \longrightarrow f(\pi(x)) + g(x)$, $x \in \mathbb{F}_2^n$, где π — подстановка на $\mathbb{F}_2^n$ и g — обобщённая булева функция от n переменных.

Рассмотрим соотношение $UH_n = H_nU$, получаемое из утверждения 4. Как отмечено ранее, все строки матрицы Сильвестра — Адамара есть в точности характеристические векторы линейных булевых функций от n переменных. Тогда

$$H_n = \begin{pmatrix} (-1)^{\langle \mathbf{v}_0, \mathbf{v}_0 \rangle} & (-1)^{\langle \mathbf{v}_0, \mathbf{v}_1 \rangle} & \cdots & (-1)^{\langle \mathbf{v}_0, \mathbf{v}_{2^n-1} \rangle} \\ (-1)^{\langle \mathbf{v}_1, \mathbf{v}_0 \rangle} & (-1)^{\langle \mathbf{v}_1, \mathbf{v}_1 \rangle} & \cdots & (-1)^{\langle \mathbf{v}_1, \mathbf{v}_{2^n-1} \rangle} \\ \vdots & \vdots & \ddots & \vdots \\ (-1)^{\langle \mathbf{v}_{2^n-1}, \mathbf{v}_0 \rangle} & (-1)^{\langle \mathbf{v}_{2^n-1}, \mathbf{v}_1 \rangle} & \cdots & (-1)^{\langle \mathbf{v}_{2^n-1}, \mathbf{v}_{2^n-1} \rangle} \end{pmatrix}.$$

Выпишем в явном виде строку с номером i и столбец с номером j. Для $i = 1, 2, \ldots, 2^n$ i-я строка матрицы U является вектором с единственным ненулевым элементом $\omega^{g(\mathbf{v}_{i-1})}$ в столбце с номером j, где $(j-1)$ — число с двоичной записью $\pi(\mathbf{v}_{i-1})$. Таким образом, i-я строка имеет вид

$$\begin{matrix} & & & & j & & & \\ \big(& 0 & \cdots & 0 & \omega^{g(\mathbf{v}_{i-1})} & 0 & \cdots & 0 \big). \end{matrix}$$

Для $j = 1, 2, \ldots, 2^n$ j-й столбец матрицы U есть вектор с единственным ненулевым элементом $\omega^{g(\pi^{-1}(\mathbf{v}_{j-1}))}$ в строке с номером i, где $(i-1)$ — число с двоичной записью $\pi^{-1}(\mathbf{v}_{j-1})$. Тогда столбец j есть

$$\begin{matrix} \\ i \end{matrix} \begin{pmatrix} 0 \\ \vdots \\ 0 \\ \omega^{g\left(\pi^{-1}(\mathbf{v}_{j-1})\right)} \\ 0 \\ \vdots \\ 0 \end{pmatrix}.$$

Отсюда ясно, что

$$(H_nU)_{i+1,j+1} = (-1)^{\left\langle \mathbf{v}_i, \pi^{-1}(\mathbf{v}_j) \right\rangle} \omega^{g\left(\pi^{-1}(\mathbf{v}_j)\right)}.$$

Таким образом, для любых $i, j \in \{0, 1, \ldots, 2^n - 1\}$ получаем

$$\omega^{g(\mathbf{v}_i)} (-1)^{\langle \pi(\mathbf{v}_i), \mathbf{v}_j \rangle} = (-1)^{\left\langle \mathbf{v}_i, \pi^{-1}(\mathbf{v}_j) \right\rangle} \omega^{g\left(\pi^{-1}(\mathbf{v}_j)\right)},$$

или, эквивалентно, для любых $x, y \in \mathbb{F}_2^n$ в кольце $\mathbb{Z}_q$ должно выполняться соотношение

$$g(x) + \frac{q}{2} \langle \pi(x), y \rangle = \frac{q}{2} \left\langle x, \pi^{-1}(y) \right\rangle + g\left(\pi^{-1}(y)\right). \tag{2}$$

Подставив нулевой вектор $y = \mathbf{0} \in \mathbb{F}_2^n$ в (2), получим, что g — обобщённая булева функция вида

$$g(x) = \frac{q}{2} \left\langle x, \pi^{-1}(\mathbf{0}) \right\rangle + g\left(\pi^{-1}(\mathbf{0})\right).$$

Подставим данное выражение в (2):

$$\frac{q}{2} \left\langle x, \pi^{-1}(\mathbf{0}) \right\rangle + g(\pi^{-1}(\mathbf{0})) + \frac{q}{2} \langle \pi(x), y \rangle = \frac{q}{2} \left\langle x, \pi^{-1}(y) \right\rangle + \frac{q}{2} \left\langle \pi^{-1}(y), \pi^{-1}(\mathbf{0}) \right\rangle + g(\pi^{-1}(\mathbf{0})),$$

после преобразований получим

$$\frac{q}{2}\left\langle x,\pi^{-1}(\mathbf{0})\right\rangle+\frac{q}{2}\left\langle \pi(x),y\right\rangle=\frac{q}{2}\left\langle x,\pi^{-1}(y)\right\rangle+\frac{q}{2}\left\langle \pi^{-1}(y),\pi^{-1}(\mathbf{0})\right\rangle. \tag{3}$$

В силу того, что условие (3) рассматривается в кольце $\mathbb{Z}_q$, имеет значение только чётность обеих частей равенства, то есть для всех $x,y\in\mathbb{F}_2^n$ получаем

$$\left\langle x,\pi^{-1}(\mathbf{0})\right\rangle\oplus\left\langle \pi(x),y\right\rangle=\left\langle x,\pi^{-1}(y)\right\rangle\oplus\left\langle \pi^{-1}(y),\pi^{-1}(\mathbf{0})\right\rangle.$$

Нетрудно видеть, что подстановка π должна быть аффинной. Это следует из того, что левая часть линейная по переменной y, тогда как правая часть линейна по x. Положим $\pi(x)=L(x\oplus c)$, $x\in\mathbb{F}_2^n$, для некоторых $L\in\mathrm{GL}(n)$ и $c\in\mathbb{F}_2^n$, тогда

$$\langle x,c\rangle\oplus\langle L(x\oplus c),y\rangle=\left\langle x,L^{-1}y\oplus c\right\rangle\oplus\left\langle L^{-1}y\oplus c,c\right\rangle,$$

то есть

$$\langle L(x\oplus c),y\rangle=\left\langle x,L^{-1}y\right\rangle\oplus\left\langle L^{-1}y,c\right\rangle\oplus\langle c,c\rangle. \tag{4}$$

Дальнейшие рассуждения повторяют доказательство [12, теорема 1]. ■

4.2. Классификация самодуальных обобщённых бент-функций от четырёх переменных для $q=4$ в рамках группы $\mathcal{U}_n^q$

Используя отображение из утверждения 3, можно уточнить известную классификацию самодуальных обобщённых бент-функций от четырёх переменных для $q=4$, приведённую в работе [5] и состоящую из восьми классов эквивалентности. В [5] эквивалентными считаются такие функции, которые могут быть получены друг из друга преобразованиями вида (1).

С использованием отображения более общего вида можно показать, что функции с векторами значений (0330302132010110) и (3123231322030300) из классов 4 и 5 (см. [5]) соответственно связаны преобразованием

$$g(x)\longrightarrow f(L(x\oplus c))+\frac{q}{2}\langle c,x\rangle+d,$$

где

$$L=\begin{pmatrix}1&0&0&0\\0&1&0&0\\0&0&1&0\\0&0&0&1\end{pmatrix},\quad c=(1001),\quad d=3.$$

Аналогично, представители (2022220222020200) и (2123230332121210) классов 2 и 7 соответственно связаны преобразованием

$$f(x)\longrightarrow f(L(x\oplus c))+\frac{q}{2}\langle c,x\rangle+d,$$

где

$$L=\begin{pmatrix}0&1&0&0\\1&0&0&0\\0&0&1&0\\0&0&0&1\end{pmatrix},\quad c=(0101),\quad d=1.$$

Уточнённая классификация приведена в таблице; всего существует 400 самодуальных обобщённых бент-функций от четырёх переменных для $q=4$.

Классификация самодуальных обобщённых бент-функций от четырёх переменных для $q = 4$

Представитель класса эквивалентности	Мощность класса
0220202022000000	24
2022220222020200	64
0330313133110110	48
0330302132010110	120
1321213122010100	96
0220213023100000	48

4.3. Унитарные операторы и множества самодуальных и антисамодуальных обобщённых бент-функций

Охарактеризуем элементы группы $\mathcal{U}_n^q$, определяющие взаимно однозначные соответствия между множествами самодуальных и антисамодуальных обобщённых бент-функций от n переменных.

Изменением одного из параметров отображений, описанных в утверждении 3, можно «переключать» сохранение (анти)самодуальности на соответствие другого характера:

Утверждение 5. Отображения множества всех обобщённых булевых функций от n переменных в себя, имеющие вид

$$f(x) \longrightarrow f(L(x \oplus c)) + \frac{q}{2}\langle c, x\rangle + d, \quad x \in \mathbb{F}_2^n,$$

где $L \in \mathcal{O}_n$; $c \in \mathbb{F}_2^n$; $\mathrm{wt}(c)$ — нечётное число; $d \in \mathbb{Z}_q$, определяют взаимно однозначное соответствие между множествами $\mathcal{SB}_n^{q,+}$ и $\mathcal{SB}_n^{q,-}$.

Доказательство. Пусть $f \in \mathcal{SB}_n^{q,+} \cup \mathcal{SB}_n^{q,-}$ и $\widetilde{f} = f + (q/2)\varepsilon$ для некоторого $\varepsilon \in \mathbb{F}_2$. Нетрудно видеть, что для $g(x) = f(L(x \oplus c)) + (q/2)\langle c, x\rangle + d$, где $L \in \mathcal{O}_n$; $c \in \mathbb{F}_2^n$; $\mathrm{wt}(c)$ — нечётное число; $d \in \mathbb{Z}_q$, справедливо $H_g(y) = 2^{n/2}\omega^{\widetilde{g}(y)+q/2}$, $y \in \mathbb{F}_2^n$. ■

Из существования такого взаимно однозначного соответствия можно получить

Следствие 3. Справедливо $\left|\mathcal{SB}_n^{q,+}\right| = \left|\mathcal{SB}_n^{q,-}\right|$.

Аналогично утверждению 4, установим взаимосвязь между рассматриваемыми отображениями, а также матрицами, соответствующими таким изометричным отображениям:

Утверждение 6. Оператор $\varphi_{\pi,g} \in \mathcal{U}_n^q$ с матрицей U определяет взаимно однозначное соответствие между множествами $\mathcal{SB}^{q,+}$ и $\mathcal{SB}^{q,-}$, если и только если $U\mathcal{H}_n = -\mathcal{H}_n U$.

Доказательство. Достаточность следует из того, что если $\mathcal{H}_n A = -A\mathcal{H}_n$, то для любых характеристических векторов F, G функций $f \in \mathrm{SB}_q^+(n)$ и $g \in \mathrm{SB}_q^-(n)$ соответственно выполняется

$$\mathcal{H}_n(AF) = -A\left(\mathcal{H}_n F\right) = -AF, \quad \mathcal{H}_n(AG) = -A\left(\mathcal{H}_n G\right) = AG,$$

следовательно, рассматриваемое отображение определяет взаимно однозначное соответствие между множествами $\mathcal{SB}_n^{q,+}$ и $\mathcal{SB}_n^{q,-}$.

Необходимость доказывается аналогично утверждению 4. ■

Далее показано, что множество всех элементов группы $\mathcal{U}_n^q$, определяющих взаимно однозначные соответствия между множествами самодуальных и антисамодуальных

обобщённых бент-функций от n переменных, исчерпывается отображениями, описанными в утверждении 5. Отметим, что случай булевых функций ранее изучен в работе [12], где доказано, что изометричные отображения множества всех булевых функций от n переменных в себя, имеющие вид

$$f(x) \longrightarrow f(\pi(x)) \oplus g(x) \quad x \in \mathbb{F}_2^n,$$

определяют взаимно однозначные соответствия между множествами самодуальных и антисамодуальных бент-функций, если и только если

$$\pi(x) = L(x \oplus c), \quad g(x) = \langle c, x \rangle \oplus d, \quad x \in \mathbb{F}_2^n,$$

где $L \in \mathcal{O}_n$; $c \in \mathbb{F}_2^n$; $\mathrm{wt}(c)$ — нечётное число; $d \in \mathbb{F}_2$.

Следующий результат характеризует все элементы группы $\mathcal{U}_n^q$, определяющие взаимно однозначные соответствия между множествами $\mathcal{SB}_n^{q,+}$ и $\mathcal{SB}_n^{q,-}$.

Теорема 4. Оператор $\varphi_{\pi,g} \in \mathcal{U}_n^q$ определяет взаимно однозначное соответствие между множествами $\mathcal{SB}_n^{q,+}$ и $\mathcal{SB}_n^{q,-}$, если и только если

$$\pi(x) = L(x \oplus c), \quad g(x) = \frac{q}{2} \langle c, x \rangle + d, \quad x \in \mathbb{F}_2^n,$$

где $L \in \mathcal{O}_n$; $c \in \mathbb{F}_2^n$; $\mathrm{wt}(c)$ — нечётное число; $d \in \mathbb{Z}_q$.

Доказательство. Достаточность следует из утверждения 5.

Пусть U — матрица оператора $\varphi_{\pi,g} \in \mathcal{U}_n^q$, определяющего взаимно однозначное соответствие между множествами $\mathcal{SB}_n^{q,+}$ и $\mathcal{SB}_n^{q,+}$. Как и в доказательстве теоремы 3, используем соотношения

$$\begin{aligned} (UH_n)_{i+1,j+1} &= \omega^{g(\mathbf{v}_i)}(-1)^{\langle \pi(\mathbf{v}_i), \mathbf{v}_j \rangle}, \\ (H_nU)_{i+1,j+1} &= (-1)^{\left\langle \mathbf{v}_i, \pi^{-1}(\mathbf{v}_j) \right\rangle} \omega^{g\left(\pi^{-1}(\mathbf{v}_j)\right)}, \end{aligned}$$

справедливые для всех $i, j \in \{0, 1, \ldots, 2^n - 1\}$.

Из утверждения 6 следует, что $UH_n = -H_nU$, откуда получаем $(UH_n)_{i+1,j+1} = -(H_nU)_{i+1,j+1}$ для всех $i, j \in \{0, 1, \ldots, 2^n - 1\}$. Следовательно, должно выполняться соотношение

$$-\omega^{g(\mathbf{v}_i)}(-1)^{\langle \pi(\mathbf{v}_i), \mathbf{v}_j \rangle} = (-1)^{\left\langle \mathbf{v}_i, \pi^{-1}(\mathbf{v}_j) \right\rangle} \omega^{g\left(\pi^{-1}(\mathbf{v}_j)\right)}$$

или, что то же самое,

$$g(x) + \frac{q}{2} \langle \pi(x), y \rangle + \frac{q}{2} = \frac{q}{2} \left\langle x, \pi^{-1}(y) \right\rangle + g\left(\pi^{-1}(y)\right)$$

для всех $x, y \in \mathbb{F}_2^n$, при этом все вычисления проводятся в кольце $\mathbb{Z}_q$.

Дальнейшие рассуждения повторяют доказательство теоремы 3 с отличием в соотношении (4):

$$\langle L(x \oplus c), y \rangle = \left\langle x, L^{-1}y \right\rangle \oplus \left\langle L^{-1}y, c \right) \rangle \oplus \langle c, c \rangle \oplus 1,$$

и выражении для функции g:

$$g(x) = \frac{q}{2} \langle c, x \rangle + g(c) + \frac{q}{2}, \quad x \in \mathbb{F}_2^n,$$

при этом значение $g(c)$ можно фиксировать произвольным элементом кольца $\mathbb{Z}_q$. ■

4.4. И т о г и

Пусть $n \geqslant 4$ — чётное число и $\varphi_{\pi,g} \in \mathcal{U}_n^q$ — оператор с матрицей U, а именно:

$$\varphi_{\pi,g} : f(x) \longrightarrow f(\pi(x)) + g(x),$$

где π — подстановка на $\mathbb{F}_2^n$ и g — обобщённая булева функция от n переменных. Матрица U есть

$$\begin{array}{c} \\ (i+1) \end{array} \begin{array}{c} \begin{array}{ccccccc} & & & \pi(\mathbf{v}_i) & & & \end{array} \\ \begin{pmatrix} 0 & \dots & 0 & \omega^{g(\mathbf{v}_i)} & 0 & \dots & 0 \end{pmatrix} \end{array} \begin{array}{c} \\ \\ \begin{pmatrix} 0 \\ \vdots \\ 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix} \end{array}.$$

Здесь, как и ранее, $\mathbf{v}_0, \mathbf{v}_1, \dots, \mathbf{v}_{2^n-1}$ — все векторы пространства $\mathbb{F}_2^n$ в лексикографическом порядке; в строке с номером $(i+1) \in \{1, 2, \dots, 2^n\}$ ненулевой элемент находится в столбце с номером $(j+1)$, где j — число с двоичной записью $\pi(\mathbf{v}_i)$. Тогда:

I. Следующие условия эквивалентны:

1) $\varphi_{\pi,g}$ сохраняет самодуальность;
2) $\varphi_{\pi,g}$ сохраняет антисамодуальность;
3) $\pi(x) = L(x \oplus c)$, $g(x) = (q/2)\langle c, x\rangle + d$, где $L \in \mathcal{O}_n$; $c \in \mathbb{F}_2^n$; $\mathrm{wt}(c)$ — чётное число; $d \in \mathbb{Z}_q$;
4) $U\mathcal{H}_n = \mathcal{H}_n U$.

II. Следующие условия эквивалентны:

1) $\varphi_{\pi,g}$ определяет взаимно однозначное соответствие между множествами $\mathcal{SB}^{q,+}$ и $\mathcal{SB}^{q,-}$;
2) $\pi(x) = L(x \oplus c)$, $g(x) = (q/2)\langle c, x\rangle + d$, где $L \in \mathcal{O}_n$; $c \in \mathbb{F}_2^n$; $\mathrm{wt}(c)$ — нечётное число; $d \in \mathbb{Z}_q$;
3) $U\mathcal{H}_n = -\mathcal{H}_n U$.

Из полученных результатов следует, что подход к классификации самодуальных обобщёных бент-функций от $n \geqslant 4$ переменных на основе частного случая расширенного аффинного отображения, упомянутого в утверждении 3, является наиболее общим в рамках группы $\mathcal{U}_n^q$.

5. Отображение, соответствующее комплексному сопряжению характеристического вектора

Ещё одним изометричным отображением множества всех обобщённых булевых функций от n переменных в себя, сохраняющим самодуальность, является отображение, соответствующее комплексному сопряжению характеристического вектора. В терминах функций оно представляется как

$$f(x) \longrightarrow q - f(x), \quad x \in \mathbb{F}_2^n, \tag{5}$$

или, кратко, $f \to (-f) \bmod q$. Функцию, характеристический вектор которой комплексно сопряжён характеристическому вектору функции f, будем обозначать через $\overline{f}$.

Утверждение 7. Отображение (5) является изометричным, переводит каждую обобщённую бент-функцию в обобщённую бент-функцию и, кроме того, сохраняет (анти)самодуальность.

Доказательство. Сохранение (анти)самодуальности следует из того, что матрица Сильвестра — Адамара является вещественной. ■

Неподвижными точками отображения (5) являются обобщённые булевы функции с вещественными характеристическими векторами, и только они. Такие характеристические векторы имеют, очевидно, только обобщённые булевы функции, представимые в виде $\frac{q}{2}f$, где f — некоторая булева функция от того же числа переменных.

Таким образом, в булевом случае данное отображение является тождественным и не представляет интереса, тогда как для обобщённых булевых функций оно предлагает ряд отображений, отличных от предложенных в предыдущем пункте. Это следует из того, что комплексное сопряжение определяет антилинейное отображение, поэтому ему не может соответствовать никакой линейный оператор $\mathbb{C}^{2^n} \to \mathbb{C}^{2^n}$ и, следовательно, никакой элемент исследованной группы $\mathcal{U}_n^q$.

Отметим также, что данное отображение является частным случаем отображений вида $f \to (\gamma \cdot f) \bmod q$ для $\gamma \in \mathbb{Z}_q^*$, которые изучаются в [6].

Рассмотрим более общий вид отображений типа (5), а именно отображения

$$f(x) \longrightarrow -f(\pi(x)) + g(x), \quad x \in \mathbb{F}_2^n, \tag{6}$$

где π — подстановка на пространстве $\mathbb{F}_2^n$ и g — обобщённая булева функция от n переменных. Данная форма отображений с точностью до множителя перед функцией f аналогична форме, упомянутой в теореме 2. Легко видеть, что верно

Утверждение 8. Отображение вида (6) определяет изометрию в метриках Хэмминга и Ли на множестве всех обобщённых булевых функций от n переменных.

Следующий результат характеризует все отображения вида (6), сохраняющие (анти)самодуальность обобщённой бент-функции.

Теорема 5. Отображение вида (6) сохраняет (анти)самодуальность, если и только если

$$\pi(x) = L(x \oplus c), \quad g(x) = \frac{q}{2}\langle c, x\rangle + d, \quad x \in \mathbb{F}_2^n,$$

где $L \in \mathcal{O}_n$; $c \in \mathbb{F}_2^n$; $\mathrm{wt}(c)$ — чётное число; $d \in \mathbb{Z}_q$.

Доказательство. Рассмотрим произвольное отображение указанного типа, пусть оно отображает функцию $f \in \mathcal{SB}_n^{q,+}$ в некоторую функцию $h \in \mathcal{SB}_n^{q,+}$, то есть

$$f(x) \longrightarrow h(x) = -f(\pi(x)) + g(x), \quad x \in \mathbb{F}_2^n.$$

Согласно утверждению 7, функция $\overline{h}$ также является самодуальной, она имеет вид

$$\overline{h}(x) = f(\pi(x)) - g(x), \quad x \in \mathbb{F}_2^n,$$

следовательно, в силу произвольности выбора функции f, должно выполняться $\varphi_{\pi,-g} \in \mathcal{U}_n^q$. ■

Таким образом, самой общей формой изометричных отображений, рассмотренных в настоящей работе, является следующая:

$$f(x) \longrightarrow \gamma \cdot f(\pi(x)) + g(x), \quad x \in \mathbb{F}_2^n,$$

где $\gamma \in \{1, q-1\}$; π — подстановка на пространстве $\mathbb{F}_2^n$; g — обобщённая булева функция от n переменных.

Заключение

Предложено новое отображение, сохраняющее самодуальность обобщённой бент-функции. Вводится понятие действия унитарного оператора на множестве обобщённых булевых функций от n переменных, представленных своими характеристическими векторами. В рамках рассматриваемого класса унитарных операторов описаны все отображения, сохраняющие самодуальность. Рассмотрен класс отображений, определяемых сопряжением характеристического вектора. Интересным для дальнейшего изучения является вопрос полного описания группы автоморфизмов самодуальных обобщённых бент-функций.

ЛИТЕРАТУРА

1. *Rothaus O. S.* On "bent" functions // J. Combin. Theory. Ser. A. 1976. V. 20. No. 3. P. 300–305.
2. *Tokareva N.* Bent Functions: Results and Applications to Cryptography. Academic Press, 2015. 220 p.
3. *Schmidt K.-U.* Quaternary constant-amplitude codes for multicode CDMA // IEEE Trans. Inform. Theory. 2009. V. 55. No. 4. P. 1824–1832.
4. *Stănică P., Martinsen T., Gangopadhyay S., and Singh B. K.* Bent and generalized bent functions // Des. Codes Cryptogr. 2013. V. 69. No. 1. P. 77–94.
5. *Sok L., Shi M., and Solé P.* Classification and construction of quaternary self-dual bent functions // Cryptogr. Commun. 2018. V. 10. No. 2. P. 277–289.
6. *Çeşmelioğlu A. and Meidl W.* Equivalence for generalized Boolean functions // Adv. Math. Commun. 2024. V. 18. No. 6. P. 1590–1604.
7. *Martinsen T., Meidl W., and Stănică P.* Generalized bent functions and their Gray images // LNCS. 2017. V. 10064. P. 160–173.
8. *Carlet C., Danielsen L. E., Parker M. G., and Solé P.* Self-dual bent functions // Int. J. Inform. Coding Theory. 2010. V. 1. P. 384–399.
9. *Hou X.-D.* Classification of self dual quadratic bent functions // Des. Codes Cryptogr. 2012. V. 63. No. 2. P. 183–198.
10. *Feulner T., Sok L., Solé P., and Wassermann A.* Towards the classification of self-dual bent functions in eight variables // Des. Codes Cryptogr. 2013. V. 68. No. 1. P. 395–406.
11. *Kutsenko A.* Metrical properties of self-dual bent functions // Des. Codes Cryptogr. 2020. V. 88. No. 1. P. 201–222.
12. *Kutsenko A.* The group of automorphisms of the set of self-dual bent functions // Cryptogr. Commun. 2020. V. 12. No 5. P. 881–898.
13. *Kutsenko A.* Decomposing self-dual bent functions // Des. Codes Cryptogr. 2024. V. 92. No 1. P. 113–144.
14. *Токарева Н. Н.* Обобщения бент-функций. Обзор работ // Дискретн. анализ и исслед. опер. 2010. Т. 17. № 1. С. 34–64.
15. *Davis J. A. and Jedwab J.* Peak-to-mean power control in OFDM, Golay complementary sequences, and Reed — Muller codes // IEEE Trans. Inform. Theory. 1999. V. 45. No. 7. P. 2397–2417.
16. *Марков А. А.* О преобразованиях, не распространяющих искажения // Избранные труды. Т. II. Теория алгорифмов и конструктивная математика, математическая логика, информатика и смежные вопросы. М.: МЦНМО, 2003. С. 70–93.
17. *Погорелов Б. А., Пудовкина М. А.* Классификация дистанционно транзитивных графов орбиталов надгрупп группы Джевонса // Дискретная математика. 2018. Т. 30. № 4. С. 66–87.

18. *Janusz G. J.* Parametrization of self-dual codes by orthogonal matrices // Finite Fields Appl. 2007. V. 13. No. 3. P. 450–491.

REFERENCES

1. *Rothaus O. S.* On "bent" functions. J. Combin. Theory, Ser. A, 1976, vol. 20, no. 3, pp. 300–305.
2. *Tokareva N.* Bent Functions: Results and Applications to Cryptography. Academic Press, 2015. 220 p.
3. *Schmidt K.-U.* Quaternary constant-amplitude codes for multicode CDMA. IEEE Trans. Inform. Theory, 2009, vol. 55, no. 4, pp. 1824–1832.
4. *Stănică P., Martinsen T., Gangopadhyay S., and Singh B. K.* Bent and generalized bent functions. Des. Codes Cryptogr., 2013, vol. 69, no. 1, pp. 77–94.
5. *Sok L., Shi M., and Solé P.* Classification and construction of quaternary self-dual bent functions. Cryptogr. Commun., 2018, vol. 10, no. 2, pp. 277–289.
6. *Çeşmelioğlu A. and Meidl W.* Equivalence for generalized Boolean functions. Adv. Math. Commun., 2024, vol. 18, no. 6, pp. 1590–1604.
7. *Martinsen T., Meidl W., and Stănică P.* Generalized bent functions and their Gray images. LNCS, 2017, vol. 10064, pp. 160–173.
8. *Carlet C., Danielsen L. E., Parker M. G., and Solé P.* Self-dual bent functions. Int. J. Inform. Coding Theory, 2010, vol. 1, pp. 384–399.
9. *Hou X.-D.* Classification of self dual quadratic bent functions. Des. Codes Cryptogr., 2012, vol. 63, no. 2, pp. 183–198.
10. *Feulner T., Sok L., Solé P., and Wassermann A.* Towards the classification of self-dual bent functions in eight variables. Des. Codes Cryptogr., 2013, vol. 68, no. 1, pp. 395–406.
11. *Kutsenko A.* Metrical properties of self-dual bent functions. Des. Codes Cryptogr., 2020, vol. 88, no. 1, pp. 201–222.
12. *Kutsenko A.* The group of automorphisms of the set of self-dual bent functions. Cryptogr. Commun., 2020, vol. 12, no. 5, pp. 881–898.
13. *Kutsenko A.* Decomposing self-dual bent functions. Des. Codes Cryptogr., 2024, vol. 92, no. 1, pp. 113–144.
14. *Tokareva N. N.* Generalizations of bent functions. A survey. J. Appl. Industr. Math., 2011, vol. 5, no. 1, pp. 110–129.
15. *Davis J. A. and Jedwab J.* Peak-to-mean power control in OFDM, Golay complementary sequences, and Reed — Muller codes. IEEE Trans. Inform. Theory, 1999, vol. 45, no. 7, pp. 2397–2417.
16. *Markov A. A.* O preobrazovaniyakh, ne rasprostranyayushchikh iskazheniya [On transformations without error propagation]. Izbrannye Trudy. T. II. Teoriya Algorifmov i Konstruktivnaya Matematika, Matematicheskaya Logika, Informatika i Smezhnye Voprosy. Moscow, MCCME, 2003, pp. 70–93. (in Russian)
17. *Pogorelov B. A. and Pudovkina M. A.* Classification of distance-transitive orbital graphs of overgroups of the Jevons group. Discrete Math. Appl., 2018, vol. 30, no. 1, pp. 7–22.
18. *Janusz G. J.* Parametrization of self-dual codes by orthogonal matrices. Finite Fields Appl., 2007, vol. 13, no. 3, pp. 450–491.

УДК 519.7 DOI 10.17223/20710410/69/3

О КРИПТОАНАЛИТИЧЕСКОЙ ОБРАТИМОСТИ ДИСКРЕТНЫХ ФУНКЦИЙ

И. А. Панкратова, А. Д. Сорокоумова

Томский государственный университет, г. Томск, Россия

E-mail: pank@mail.tsu.ru, a.srkmva@mail.ru

Рассматривается понятие криптоаналитической обратимости функции по переменной, его связь с другими понятиями. Доказаны критерии криптоаналитической обратимости для функций от двух и трёх аргументов. Сформулированы алгоритмы построения функции восстановления и генерации обратимых функций.

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

ON CRYPTANALYTIC INVERTIBILITY OF DISCRETE FUNCTIONS

I. A. Pankratova, A. D. Sorokoumova

Tomsk State University, Tomsk, Russia

The function $g(x_1, \ldots, x_n)$ is invertible with respect to the variable x_k of type $K_1 \ldots K_n$, where $k \in \{1, \ldots, n\}$, $K_i \in \{\exists, \forall\}$ and $K_k = \forall$, if there exists a recovery function f such that the invertibility condition is true:

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

Criteria for cryptanalytic invertibility of functions $g : D_1 \times D_2 \times D_3 \to D$ are proven: 1) a function g is invertible with respect to the variable x_1 of the type $\forall\forall\exists$ iff there is a mapping $\varphi : D_1 \times D_2 \to D_3$ such that the following condition is satisfied:

$$\forall a, c \in D_1 \, \forall b, d \in D_2 \, \big(a \neq c \;\Rightarrow\; g(a, b, \varphi(a, b)) \neq g(c, d, \varphi(c, d))\big);$$

2) a function g is invertible with respect to the variable x_1 of the type $\forall\exists\forall$ iff there is a mapping $\varphi : D_1 \to D_2$ such that the following condition is satisfied:

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

3) a function g is invertible with respect to the variable x_3 of the type $\forall\exists\forall$ iff there is a mapping $\varphi : D_1 \to D_2$ such that the following condition is satisfied:

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

4) a function g is invertible with respect to the variable x_2 of the type $\exists\forall\forall$ iff there is $a \in D_1$ such that the following condition is satisfied ($G^{(a,b)} = \{g(a, b, x_3) : x_3 \in D_3\}$):

$$\forall b, d \in D_2 \, \big(b \neq d \;\Rightarrow\; G^{(a,b)} \cap G^{(a,d)} = \varnothing\big);$$

5) a function g is invertible with respect to the variable x_2 of the type $\exists\forall\exists$ iff there are $a \in D_1$ and a mapping $\varphi : D_2 \to D_3$ such that the following condition is satisfied:

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

Algorithms for constructing a recovery function and generating invertible functions are formulated too.

Keywords: *cryptanalytic invertibility, invertibility criterion, recovery function.*

Введение

Понятие криптоаналитической обратимости функции введено Г. П. Агибаловым в [1, 2] как обобщение понятия «обычной» обратимости функции.

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

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

Рассмотрим случай, когда области определения D_i переменных x_i для всех $i = 1, \ldots, n$ конечны. Тогда можно дать следующее эквивалентное определение:

Определение 2. Функция $g(x_1, \ldots, x_n)$ обратима по переменной x_k типа $K_1 \ldots K_n$, $k \in \{1, \ldots, n\}$, $K_i \in \{\exists, \forall\}$ и $K_k = \forall$, если выполнима формула

$$O_1 \ldots O_n \big(f(g(x_1, \ldots, x_n)) = x_k\big), \tag{1}$$

где $O_i = \bigvee\limits_{x_i \in D_i}$, если $K_i = \exists$; $O_i = \bigwedge\limits_{x_i \in D_i}$, если $K_i = \forall$, $i = 1, \ldots, n$. Любая функция f, обращающая (1) в истину, является функцией восстановления.

Равносильность определений 1 и 2 следует из выражений кванторов общности и существования на конечной области определения $D = \{d_1, \ldots, d_r\}$ через логические операции:

$$\forall x P(x) = P(d_1) \wedge P(d_2) \wedge \ldots \wedge P(d_r),$$
$$\exists x P(x) = P(d_1) \vee P(d_2) \vee \ldots \vee P(d_r).$$

Здесь $P(x)$ — произвольный предикат.

Пример 1. Пусть $n = 2$ и булева функция g в общем виде задана в табл. 1, где $a, b, c, d \in \{0, 1\}$.

Таблица 1

x_1	x_2	g
0	0	a
0	1	b
1	0	c
1	1	d

Тогда формула (1) примет следующий вид:

— для обратимости типа $\forall\forall$ по переменной x_1

$$\big(f(a) = 0 \wedge f(b) = 0\big) \wedge \big(f(c) = 1 \wedge f(d) = 1\big); \tag{2}$$

— для обратимости типа $\forall\exists$ по переменной x_1

$$\big(f(a) = 0 \vee f(b) = 0\big) \wedge \big(f(c) = 1 \vee f(d) = 1\big); \tag{3}$$

— для обратимости типа $\exists\forall$ по переменной x_2

$$\big(f(a)=0\wedge f(b)=1\big)\vee\big(f(c)=0\wedge f(d)=1\big). \tag{4}$$

Сравним с условиями критериев обратимости функций от двух переменных [3] (см. далее утверждение 1):

— для обратимости типа $\forall\forall$ по переменной x_1 должно быть $\{a,b\}\cap\{c,d\}=\varnothing$; очевидно, что в этом и только в этом случае выполнено условие функциональности для отображения f, удовлетворяющего (2);

— для обратимости типа $\forall\exists$ по переменной x_1 должно существовать такое отображение $\varphi:\{0,1\}\to\{0,1\}$, что $g(0,\varphi(0))\neq g(1,\varphi(1))$. Функцию f, удовлетворяющую (3), можно построить, если и только если $\{a,b,c,d\}=\{0,1\}$, т. е. если $g\neq\text{const}$. Пусть $g(y_1,y_2)\neq g(z_1,z_2)$. Тогда если $y_1\neq z_1$, то нужное отображение задаётся условиями $\varphi(y_1)=y_2$ и $\varphi(z_1)=z_2$. Если $y_1=z_1$, то $g(\bar{y}_1,0)\neq g(y_1,y_2)$ или $g(\bar{y}_1,0)\neq g(y_1,z_2)$. В первом случае положим $\varphi(y_1)=y_2$, $\varphi(\bar{y}_1)=0$; во втором — $\varphi(y_1)=z_2$, $\varphi(\bar{y}_1)=0$;

— для обратимости типа $\exists\forall$ по переменной x_2 необходимо и достаточно, чтобы $|\{a,b\}|=2$ или $|\{c,d\}|=2$; в первом случае положим $f(a)=0$ и $f(b)=1$, во втором — $f(c)=0$ и $f(d)=1$, тем самым условие (4) будет удовлетворено.

Введённое понятие криптоаналитической обратимости функции связано и с другими известными ранее понятиями, проясним эту связь.

Определение 3 [4, с. 31]. Функция $g(x_1,\ldots,x_n):D_1\times\ldots\times D_n\to D$ инъективна по переменной x_i, $i\in\{1,\ldots,n\}$, если при любых значениях $a_1,\ldots,a_{i-1},a_{i+1},\ldots,a_n$ переменных $x_1,\ldots x_{i-1},x_{i+1},\ldots,x_n$ отображение $g(a_1,\ldots,a_{i-1},x_i,a_{i+1},\ldots,a_n):D_i\to D$ инъективно:

$$\begin{gathered}\forall a_1\in D_1\ldots\forall a_{i-1}\in D_{i-1}\forall b,c\in D_i\,\forall a_{i+1}\in D_{i+1}\ldots\forall a_n\in D_n\\ \big(b\neq c\Rightarrow g(a_1,\ldots,a_{i-1},b,a_{i+1},\ldots,a_n)\neq g(a_1,\ldots,a_{i-1},c,a_{i+1},\ldots,a_n)\big).\end{gathered} \tag{5}$$

Условие (5) равносильно тому, что существует функция восстановления f значения переменной x_i, но не только по значению функции g, как в определении 1, а ещё и по значениям остальных аргументов:

$$\exists f\forall x_1\ldots\forall x_n\big(f(g(x_1,\ldots,x_n),x_1,\ldots x_{i-1},x_{i+1},\ldots,x_n)=x_i\big).$$

Другими словами, инъективность функции $g(x_1,\ldots,x_n)$ по переменной x_i равносильна обратимости типа $\forall\forall\ldots\forall$ по той же переменной векторной функции $\big(g,x_1,\ldots,x_{i-1},x_{i+1},\ldots,x_n\big)$. Если распространить на функции терминологию [5], применённую там к понятию обратимости конечных автоматов, то можно в этом случае говорить об обратимости функции g *степени* $\forall\forall\ldots\forall$ *порядка* $X\setminus\{x_i\}$, где $X=\{x_1,\ldots,x_n\}$ — множество переменных функции g.

Ещё одно понятие — сильно зависимых функций — применимо в случае, если $D_1=\ldots=D_n=D$.

Определение 4 [6]. Функция $g:D^n\to D$ 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.

Или, что равносильно: функция g сильно зависима, если она обратима по всем переменным x_i, $i=1,\ldots,n$, степени $\underbrace{\exists\ldots\exists}_{i-1}\forall\underbrace{\exists\ldots\exists}_{n-i}$ порядка $X\setminus\{x_i\}$.

Таким образом, определение 1 в каком-то смысле обобщает понятия инъективной по переменной и сильно зависимой функции, так как допускает большее разнообразие кванторных приставок.

В [3] рассмотрен случай $n = 2$ и для всех типов обратимости решены следующие задачи:

1) разработка критерия обратимости;
2) разработка алгоритма построения функции восстановления;
3) разработка алгоритма генерации обратимых функций.

В [7] решены те же задачи для функций от трёх переменных для тех типов обратимости, которые не сводятся к случаю $n = 2$. Однако не все критерии обратимости конструктивны, некоторые из них требуют существования отображения с определёнными свойствами. Для решения этой проблемы требуется сформулировать алгоритмы построения нужных отображений, а можно пойти другим путём: проверять выполнимость формулы (1), попутно строя функцию восстановления f. В данной работе приведены конструктивные критерии обратимости всех типов для функций от двух и трёх переменных.

1. Критерии обратимости функций от двух переменных

Рассматриваются функции вида $g : D_1 \times D_2 \to D$. Необходимым условием обратимости функции $g(x_1, x_2)$ по переменной x_k, $k \in \{1, 2\}$, является $|D| \geqslant |D_k|$; будем всюду считать, что оно выполнено. Для любого $a \in D_1$ обозначим $G^{(a)} = \{g(a, x_2) : x_2 \in D_2\}$.

Утверждение 1 [3]. Имеют место следующие критерии обратимости:

1) Функция $g(x_1, x_2)$ обратима типа $\forall\forall$ по переменной x_1, если и только если

$$\forall a, b \in D_1 \big(a \neq b \Rightarrow G^{(a)} \cap G^{(b)} = \varnothing\big). \tag{6}$$

2) Функция $g(x_1, x_2)$ обратима типа $\exists\forall$ по переменной x_2, если и только если существует такое $a \in D_1$, что

$$|G^{(a)}| = |D_2|. \tag{7}$$

3) Функция $g(x_1, x_2)$ обратима типа $\forall\exists$ по переменной x_1, если и только если существует такое отображение $\varphi : D_1 \to D_2$, что выполнено условие

$$\forall a, b \in D_1 \big(a \neq b \Rightarrow g(a, \varphi(a)) \neq g(b, \varphi(b))\big). \tag{8}$$

В утверждении 1 условия (6) и (7) легко проверяются, а вот критерий обратимости типа $\forall\exists$ требует проверки существования отображения φ со свойством (8). Функция восстановления $f : D \to D_1$ должна удовлетворять условию

$$\forall x_1 \exists x_2 \big(f(g(x_1, x_2)) = x_1\big). \tag{9}$$

Если отображение φ удалось найти, то функция f строится так:

1) для всех $a \in D_1$ положить $f(g(a, \varphi(a))) = a$;
2) для каждого $y \in D$, такого, что значение $f(y)$ не определено на шаге 1, выбрать в качестве $f(y)$ произвольное значение из D_1.

Функциональность отношения f следует из того, что, в силу условия (8), все значения $g(a, \varphi(a))$ для $a \in D_1$ попарно различны.

Сформулируем алгоритм 1 построения отображения φ. Пусть $D_1 = \{a_1, \ldots, a_n\}$, $D_2 = \{b_1, \ldots, b_m\}$, множество значений функции g равно

$$\{g(x_1, x_2) : x_1 \in D_1, x_2 \in D_2\} = \{c_1, \ldots, c_k\} \subseteq D;$$

заметим, что это множество конечно, даже если D бесконечно: $k \leqslant nm$.

Будем строить отображение φ с помощью построения дерева и обхода его в глубину. Вершинам i-го яруса, $i = 1, \ldots, n$, сопоставим значения a_i; дугам, исходящим из вершин, — значения b_j, $j = 1, \ldots, m$. Листья дерева (вершины $(n+1)$-го яруса) обозначим «$\square$». Цель — найти путь $a_1 \overset{b_{j_1}}{\to} a_2 \overset{b_{j_2}}{\to} \ldots \to a_n \overset{b_{j_n}}{\to} \square$, такой, что все значения $g(a_i, b_{j_i})$, $i = 1, \ldots, n$, попарно различны; тогда искомое отображение строится по правилу $\varphi(a_i) = b_{j_i}$, $i = 1, \ldots, n$. Уникальность значений $g(a_i, b_{j_i})$ будем проверять с помощью характеристического вектора $v \in \{0,1\}^k$; используем также вспомогательный массив B, полагая $B[i] = j$, если $\varphi(a_i) = b_j$ в текущем варианте строящегося отображения φ.

Алгоритм 1. Построение отображения φ для критерия обратимости типа $\forall\exists$

Вход: функция $g : D_1 \times D_2 \to D$.
Выход: отображение $\varphi : D_1 \to D_2$, такое, что выполнено условие (8).

1: $v = (v_1 \ldots v_k) := 0^k$; $i := 1$.
2: $j := 1$.
3: $B[i] := j$; найти s, такое, что $g(a_i, b_j) = c_s$.
4: **Если** $v_s = 0$, **то**
   $v_s := 1$.
5: **Если** $i = n$, **то**
   перейти к п. 19,
6: **иначе**
7: *// спуск по дереву*
   $i := i + 1$; переход к п. 2.
9: *// $v_s = 1 \Rightarrow$ надо перестроить отображение*
10: **Если** $j < m$, **то**
11: $j := j + 1$; переход к п. 3. *// строим дерево в ширину*
12: *// иначе — возврат по дереву*
13: **Если** $i = 1$, **то**
   выход, ответ: «Отображения φ со свойством (8) не существует».
14: **Если** $i > 1$, **то**
15: $i := i - 1$; найти s, такое, что $g(a_i, b_{B[i]}) = c_s$; $v_s := 0$; $j := B[i] + 1$.
16: **Если** $j \leqslant m$, **то**
   перейти к п. 3,
17: **иначе**
18: перейти к п. 13.
19: Положить $\varphi(a_i) = b_{B[i]}$ для $i = 1, \ldots, n$; выход.

Пример 2. Пусть $D_1 = D = \{1,2,3\}$, $D_2 = \{1,2\}$, функция g задана табл. 2. Тогда алгоритм 1 построит отображение φ (табл. 3); в свою очередь, с его помощью получим функцию восстановления f (табл. 4). Нетрудно убедиться, что для функции f выполнено условие (9):

$$f(g(1,1)) = f(1) = 1; \quad f(g(2,2)) = f(3) = 2; \quad f(g(3,2)) = f(2) = 3.$$

Таблица 2

x_1	x_2	$g(x_1, x_2)$
1	1	1
1	2	1
2	1	2
2	2	3
3	1	1
3	2	2

Таблица 3

$a \in D_1$	$\varphi(a)$
1	1
2	2
3	2

Таблица 4

$a \in D$	$f(a)$
1	1
2	3
3	2

Расмотрим теперь второй способ — по сути альтернативный критерий обратимости, состоящий в построении функции восстановления f «напрямую» — без поиска отображения φ. Условие (9) эквивалентно выполнимости формулы

$$\bigwedge_{x_1 \in D_1} \bigvee_{x_2 \in D_2} \big(f(g(x_1, x_2)) = x_1\big). \tag{10}$$

Предлагается алгоритм 2 нахождения функции восстановления f, удовлетворяющей (10).

Алгоритм 2. Построение функции восстановления f для обратимости типа $\forall\exists$

Вход: функция $g : D_1 \times D_2 \to D$, $D_1 = \{a_1, \ldots, a_n\}$.

Выход: множество F, задающее (возможно, частично) функцию восстановления, удовлетворяющую (10), или ответ «Функция g не обратима типа $\forall\exists$ по переменной x_1».

1: Построить корень дерева с меткой $F = \varnothing$, объявить его текущим узлом; $i := 1$.
2: Построить потомков текущего узла (узла с меткой F) на i-м ярусе по правилу:
3: **Для всех** $x \in G^{(a_i)}$:
4: **Если** $x \notin F_1$, **то**
добавить потомка с меткой $F \cup \{(x, a_i)\}$.
5: **Если** добавлен хотя бы один потомок, **то**
6: объявить первого из них текущим узлом; $i := i + 1$.
7: **Если** $i = n + 1$, **то**
8: // *все ярусы пройдены*
выход, ответ — F (метка текущего узла),
9: **иначе**
10: перейти к п. 2;
11: **иначе**
12: $i := i - 1$; объявить текущим предка текущего узла.
13: **Если** у него есть нерассмотренные потомки, **то**
14: объявить очередного из них текущим узлом, $i := i + 1$; перейти к п. 2;
15: **иначе**
16: **Если** $i > 0$, **то**
перейти к п. 12;
17: **иначе**
18: // *вернулись в корень и рассмотрели всех его потомков*
выход, ответ «Функция g не обратима типа $\forall\exists$ по переменной x_1».

Функция f строится с помощью обхода дерева в глубину. Узлам сопоставляются множества пар $F = \{(x, y)\} \subseteq D \times D_1$, где $f(x) = y$ для искомой функции f. Корень

дерева — узел нулевого яруса с меткой $\varnothing$; остальные ярусы соответствуют элементам $a \in D_1$. Обозначим: F_1 — проекция множества F по первой координате: $F_1 = \{x : \exists y\big((x,y) \in F\big)\}$. Цель — найти путь длины $|D_1|$, проходящий через все ярусы, такой, что для метки листа выполнено условие функциональности: $|F_1| = |F|$; или, что то же самое, — первые элементы в парах из F попарно различны. Функция восстановления строится тогда следующим образом:

1) полагаем $f(x) = y$ для всех $(x,y) \in F$;
2) для $x \notin F_1$ выбираем в качестве $f(x)$ любые значения из D_1.

Пример 3. Дерево, построенное алгоритмом 2 для функции g из примера 2, представлено на рис. 1. По метке листа на третьем ярусе строится та же функция f (табл. 4).

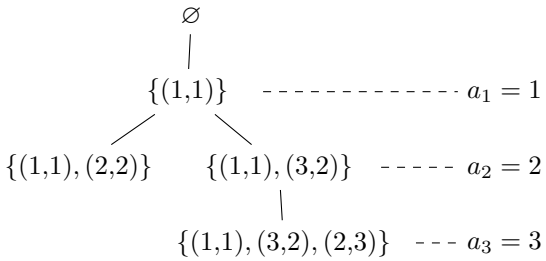

Рис. 1. Иллюстрация алгоритма 2

2. Критерии обратимости функций от трёх переменных

Рассматриваются функции вида

$$g : D_1 \times D_2 \times D_3 \to D. \tag{11}$$

Все типы обратимости функций от трёх переменных перечислены в табл. 5. Первый, четвёртый и седьмой типы эквивалентны обратимости функций от двух переменных, так как, например, функцию g вида (11) можно рассматривать как функцию $g : D_1 \times (D_2 \times D_3) \to D$ (для первого и четвёртого типов) или $g : (D_1 \times D_2) \times D_3 \to D$ (для седьмого типа). Заметим, что типы $\forall\forall\exists$ и $\exists\forall\forall$, несмотря на стоящие рядом кванторы всеобщности, не сводятся к обратимости функций от двух переменных, так как восстанавливается значение только одной переменной.

Таблица 5

№ п/п	Тип обратимости	По переменным	Экв. тип для $n = 2$
1	$\forall\forall\forall$	x_1	$\forall\forall$
2	$\forall\forall\exists$	x_1	–
3	$\forall\exists\forall$	x_1, x_3	–
4	$\forall\exists\exists$	x_1	$\forall\exists$
5	$\exists\forall\forall$	x_2	–
6	$\exists\forall\exists$	x_2	–
7	$\exists\exists\forall$	x_3	$\exists\forall$

Кроме того, ввиду коммутативности одноимённых кванторов нет смысла отдельно рассматривать обратимость по разным переменным для второго и пятого типов. Таким образом, для функций от трёх переменных интерес представляют типы обратимости $\forall\forall\exists$ (по переменной x_1); $\forall\exists\forall$ (по переменным x_1 и x_3); $\exists\forall\forall$ и $\exists\forall\exists$ (по переменной x_2).

В работе [7] сформулированы без доказательств критерии обратимости и способы построения функций восстановления для всех пяти случаев, а также алгоритм генерации функции, обратимой типа $\forall\forall\exists$, также без доказательства его полноты и корректности. В данной работе приведены все утверждения и алгоритмы с полными доказательствами и примерами.

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

Функция $g(x_1, x_2, x_3)$ является обратимой типа $\forall\forall\exists$ по переменной x_1, если существует функция $f : D \to D_1$, такая, что выполняется условие

$$\forall x_1 \forall x_2 \exists x_3 \big(f(g(x_1, x_2, x_3)) = x_1\big). \tag{12}$$

Условие (12) эквивалентно выполнимости формулы

$$\bigwedge_{x_1 \in D_1} \bigwedge_{x_2 \in D_2} \bigvee_{x_3 \in D_3} \big(f(g(x_1, x_2, x_3)) = x_1\big). \tag{13}$$

Утверждение 2 (критерий обратимости типа $\forall\forall\exists$ [7]). Функция $g : D_1 \times D_2 \times \times D_3 \to D$ обратима типа $\forall\forall\exists$ по переменной x_1, если и только если существует такое отображение $\varphi : D_1 \times D_2 \to D_3$, что выполнено следующее условие:

$$\forall a, c \in D_1 \, \forall b, d \in D_2 \, \big(a \neq c \;\Rightarrow\; g(a, b, \varphi(a, b)) \neq g(c, d, \varphi(c, d))\big). \tag{14}$$

Доказательство.

Достаточность. Функция восстановления $f : D \to D_1$, удовлетворяющая (13), строится следующим образом:

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

Функциональность отношения f следует из условия (14).

Необходимость. Пусть для функций g и f выполнено условие (12). Для всех $x_1 \in D_1$, $x_2 \in D_2$ положим $\varphi(x_1, x_2) = x_3$, такому, что $f(g(x_1, x_2, x_3)) = x_1$. Тогда

$$\forall a, c \in D_1 \, \forall b, d \in D_2 \, \big(a \neq c \;\Rightarrow\; f(g(a, b, \varphi(a, b))) \neq f(g(c, d, \varphi(c, d)))\big),$$

откуда ввиду функциональности f получаем (14).

Утверждение 2 доказано. ■

Как видно, критерий неконструктивен. Сформулируем алгоритм 3, который находит функцию восстановления f, удовлетворяющую (13), без построения отображения φ.

Функция f строится с помощью обхода дерева в глубину. Вершинам (узлам) сопоставляются множества пар $F = \{(x, y)\} \subseteq D \times D_1$, где $f(x) = y$ для искомой функции f; ярусы дерева соответствуют парам $(a, b) \in D_1 \times D_2$. Обозначим: $G^{(a,b)} = \{g(a, b, x_3) : x_3 \in D_3\}$; F_1 — проекция множества F по первой координате: $F_1 = \{x : \exists y \, (x, y) \in F\}$. Цель — найти путь длины $|D_1| \cdot |D_2|$, проходящий через все ярусы, такой, что для метки листа выполнено условие функциональности: $|F_1| = |F|$; или, что то же самое, — первые элементы в парах из F попарно различны. Функция восстановления строится тогда следующим образом:

1) полагаем $f(x) = y$ для всех $(x, y) \in F$;
2) для $x \notin F_1$ выбираем в качестве $f(x)$ любые значения из D_1.

Алгоритм 3. Построение функции восстановления f для обратимости типа $\forall\forall\exists$

Вход: функция $g : D_1 \times D_2 \times D_3 \to D$.

Выход: множество F, задающее (возможно, частично) функцию восстановления, удовлетворяющую (13), или ответ «Функция g не обратима типа $\forall\forall\exists$ по переменной x_1».

1: Стартуем с корня дерева, его метка — $F = \varnothing$.
2: Строим потомков текущего узла на следующем ярусе (a, b) по правилу:
3: **Для всех** $x \in G^{(a,b)}$:
4: **Если** $x \notin F_1$, **то**
добавляем потомка с меткой $F \cup \{(x, a)\}$.
5: **Если** $x \in F_1$, **то**
6: **если** $(x, a) \in F$, **то** удаляем всех потомков текущего узла, добавляем потомка с меткой F, объявляем его текущим узлом, переходим к шагу 2;
иначе не добавляем потомка.
7: **Если** добавлен хотя бы один потомок, **то**
8: объявляем первого из них текущим узлом.
9: **Если** все ярусы пройдены, **то**
10: **выход**, ответ — F (метка текущего узла),
11: **иначе** переходим к шагу 2;
12: **иначе** возвращаемся по пути к корню до ближайшей точки ветвления (узла, имеющего нерассмотренных потомков), объявляем очередного потомка текущим узлом, переходим к шагу 2.
13: **Если** вернулись в корень и рассмотрели всех его потомков, **то**
14: **выход**, ответ «Функция g не обратима типа $\forall\forall\exists$ по переменной x_1».

Комментарий к шагу 6 алгоритма 3: если узел имеет потомков с метками F' и F, такими, что $F \subset F'$, то первый потомок «избыточен»: его можно удалить из дерева без потери решения, так как F' задаёт более жёсткие требования к функции f, чем F, и эти множества требований связаны операцией дизъюнкции. Это соответствует применению закона поглощения $AB \vee A = A$ в формуле (13).

Пример 4. Пусть $D_1 = \{1, 2, 3\}$, $D_2 = \{4, 5\}$, $D_3 = \{0, 1\}$, $D = \{0, 1, 4, 5\}$ и функция g задана в табл. 6. На рис. 2 представлено дерево, построенное алгоритмом 3; в табл. 7 — получившаяся функция восстановления.

Таблица 6

x_1	x_2	x_3	g
1	4	0	0
1	4	1	1
1	5	0	4
1	5	1	0
2	4	0	1
2	4	1	4
2	5	0	0
2	5	1	4
3	4	0	1
3	4	1	0
3	5	0	5
3	5	1	0

Таблица 7

x	$f(x)$
0	1
1	3
4	2
5	3

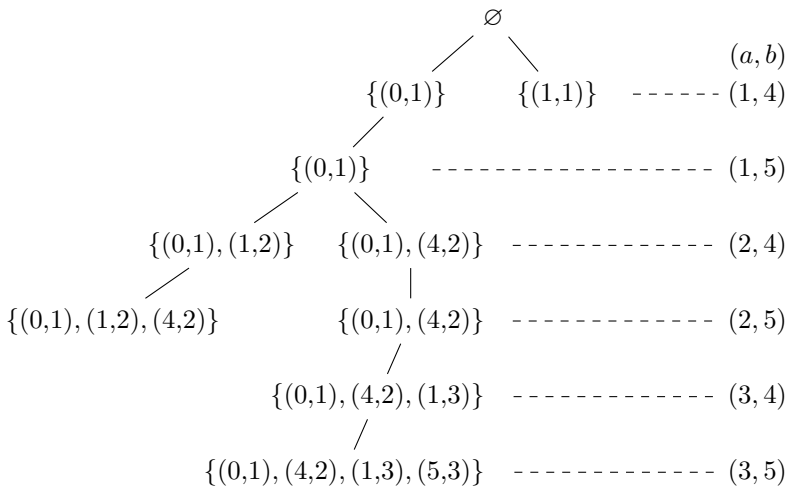

Рис. 2. Иллюстрация алгоритма 3

Алгоритм 4 задаёт способ генерации функции $g : D_1 \times D_2 \times D_3 \to D$, обратимой типа $\forall\forall\exists$ по переменной x_1.

Алгоритм 4. Генерация функции, обратимой типа $\forall\forall\exists$ по переменной x_1 [7]

1: Построить произвольное разбиение множества D на классы H_a, $a \in D_1$.
2: **Для всех** $a \in D_1$:
3: **Для всех** $b \in D_2$:
4: выбрать $y \in D_3$, $z \in H_a$;
5: положить $g(a, b, y) := z$.
6: **Для всех** $x_3 \in D_3 \setminus \{y\}$:
7: выбрать в качестве $g(a, b, x_3)$ произвольное значение $s \in D$.

Корректность алгоритма 4: построим отображение φ, где $\varphi(a, b)$ равно значению z, выбранному для этих a, b на шаге 4. Тогда для этого φ и построенной функции g выполнено условие (14), поскольку для разных $a, c \in D_1$ блоки разбиения H_a и H_c не пересекаются, а значит, $g(a, b, \varphi(a, b)) \neq g(c, d, \varphi(c, d))$ для любых $b, d \in D_2$.

Полнота алгоритма 4: пусть для некоторой функции g и отображения φ выполнено условие (14). Обозначим $G_\varphi^{(a)} = \{g(a, b, \varphi(a, b)) : b \in D_2\}$; из (14) следует, что множества $G_\varphi^{(a)}$ для $a \in D_1$ попарно не пересекаются. Поэтому в шаге 1 алгоритма 4 разбиение множества D может быть выбрано так, что $G_\varphi^{(a)} \subseteq H_a$ для всех $a \in D_1$. Тогда именно функция g будет построена алгоритмом 4 при выборе значений $y = \varphi(a, b)$ и $z = g(a, b, y) \in G_\varphi^{(a)}$ в шаге 4 и значений $g(a, b, x_3)$ в качестве соответствующих «произвольных» в шаге 7.

Полнота и корректность алгоритмов генерации обратимых функций для остальных типов обратимости (алгоритмы 6, 8–10) доказываются аналогично.

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

Функция $g(x_1, x_2, x_3)$ обратима типа $\forall\exists\forall$ по переменной x_1, если существует функция $f : D \to D_1$, такая, что

$$\forall x_1 \exists x_2 \forall x_3 \big(f(g(x_1, x_2, x_3)) = x_1\big). \tag{15}$$

Утверждение 3 (критерий обратимости типа $\forall\exists\forall$ по x_1 [7]). Функция $g : D_1 \times \times D_2 \times D_3 \to D$ обратима типа $\forall\exists\forall$ по переменной x_1, если и только если существует такое отображение $\varphi : D_1 \to D_2$, что выполнено условие

$$\forall a, c \in D_1 \, \forall b, d \in D_3 \, \big(a \neq c \;\Rightarrow\; g(a, \varphi(a), b) \neq g(c, \varphi(c), d)\big). \tag{16}$$

Доказательство.

Достаточность. Функция восстановления $f : D \to D_1$, удовлетворяющая (15), строится следующим образом:

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

Необходимость. Пусть для функций g и f выполнено условие (15). Для всех $x_1 \in D_1$, $x_2 \in D_2$ положим $\varphi(x_1) = x_2$, такому, что

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

Тогда

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

откуда ввиду функциональности f получаем (16).

Утверждение 3 доказано. ■

В алгоритме 5 описан способ построения функции восстановления f, удовлетворяющей (15). Функция f строится с помощью обхода дерева в глубину. Вершинам сопоставляются подмножества $E \subseteq D$ тех значений x, для которых $f(x)$ к данному моменту определена; ярусы дерева соответствуют элементам из $D_1 = \{a_1, \ldots, a_n\}$, дуги — элементам из $D_2 = \{b_1, \ldots, b_m\}$; в массиве B будем запоминать номера j меток b_j дуг текущего пути.

По построению (шаги 15, 16) имеем $f(g(a_i, b_j, x_3)) = a_i$ для всех $i = 1, \ldots, n$, некоторого $j \in \{1, \ldots, m\}$ и всех $x_3 \in D_3$, т. е. выполняется (15). Функциональность отношения f обеспечивается проверкой в шаге 3, в результате которой множества $G^{(a_i, b_j)}$, соответствующие дугам любого пути от корня к листу, попарно не пересекаются.

Заметим, что с помощью алгоритма 5 можно также найти отображение φ, удовлетворяющее (16): для этого на шаге 16 нужно положить $\varphi(a_i) = b_{B[i]}$.

Функция g из примера 4 не является обратимой типа $\forall\exists\forall$ по переменной x_1, что видно из рис. 3: дерево удаётся достроить только до первого яруса.

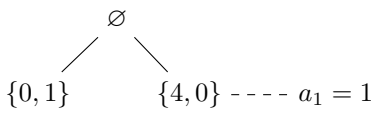

Рис. 3. Иллюстрация алгоритма 5 для функции g из примера 4

Пример 5. Пусть функция $g : \{1, 2, 3\} \times \{4, 5\} \times \{0, 1\} \to \{0, 1, 4, 5\}$ задана в табл. 8. На рис. 4 представлено дерево, построенное алгоритмом 5; в табл. 9 и 10 — функция f и отображение φ, удовлетворяющие условиям (15) и (16) соответственно.

Алгоритм 5. Построение функции восстановления для обратимости типа $\forall\exists\forall$ по переменной x_1

Вход: функция $g : D_1 \times D_2 \times D_3 \to D$.
Выход: функция f, удовлетворяющая (15), или ответ «Функция g не обратима типа $\forall\exists\forall$ по переменной x_1».

1: Построить корень дерева с меткой $E = \varnothing$, объявить его текущим узлом; $i := 1$.
2: $j := 1$.
3: **Если** $E \cap G^{(a_i,b_j)} = \varnothing$, **то**
добавить потомка с меткой $E \cup G^{(a_i,b_j)}$, объявить его текущим узлом; $B[i] := j$, $i := i + 1$.
4: **Если** $i = n + 1$, **то**
5: перейти к п. 15, // все ярусы пройдены
6: **иначе**
7: перейти к п. 2; // обход в глубину
8: **иначе**
9: **Если** $j < m$, **то**
$j := j + 1$, перейти к п. 3; // построение дерева в ширину
10: **иначе**
11: объявить текущим предка текущего узла; $j := B[i]$; // возврат по дереву
12: **Если** $i > 0$, **то**
$i := i - 1$, перейти к п. 9;
13: **иначе**
14: // *вернулись в корень и рассмотрели все возможные дуги*
выход, ответ «Функция g не обратима типа $\forall\exists\forall$ по переменной x_1».
15: **Для** $i = 1, \ldots, n$:
16: положить $f(x) = a_i$ для всех $x \in G^{(a_i,b_{B[i]})}$.

Таблица 8

x_1	x_2	x_3	g
1	4	0	1
1	4	1	1
1	5	0	5
1	5	1	1
2	4	0	4
2	4	1	0
2	5	0	4
2	5	1	5
3	4	0	0
3	4	1	0
3	5	0	1
3	5	1	0

Таблица 9

x	$f(x)$
0	3
1	1
4	2
5	2

Таблица 10

$a \in D_1$	$\varphi(a)$
1	4
2	5
3	4

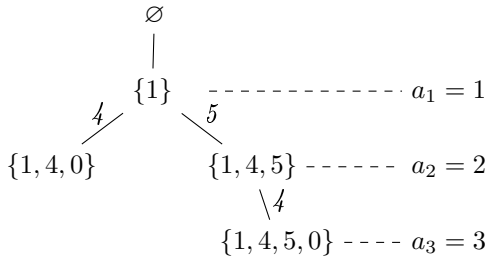

Рис. 4. Иллюстрация алгоритма 5

В алгоритме 6 описан способ генерации функции $g : D_1 \times D_2 \times D_3 \to D$, обратимой типа $\forall\exists\forall$ по переменной x_1.

Алгоритм 6. Генерация функции, обратимой типа $\forall\exists\forall$ по переменной x_1

1: Построить произвольное разбиение множества D на классы H_a, $a \in D_1$.
2: **Для всех** $a \in D_1$:
3: выбрать $b \in D_2$.
4: **Для всех** $c \in D_3$:
5: выбрать $z \in H_a$, положить $g(a, b, c) := z$.
6: **Для всех** $x_2 \in D_2 \setminus \{b\}$:
7: **Для всех** $x_3 \in D_3$:
8: выбрать в качестве $g(a, x_2, x_3)$ произвольное значение $y \in D$.

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

Функция $g(x_1, x_2, x_3)$ обратима типа $\forall\exists\forall$ по переменной x_3, если существует функция $f : D \to D_3$, такая, что

$$\forall x_1 \exists x_2 \forall x_3 \big(f(g(x_1, x_2, x_3)) = x_3\big). \tag{17}$$

Утверждение 4 (критерий обратимости типа $\forall\exists\forall$ по x_3 [7]). Функция $g : D_1 \times \times D_2 \times D_3 \to D$ обратима типа $\forall\exists\forall$ по переменной x_3, если и только если существует такое отображение $\varphi : D_1 \to D_2$, что выполнено условие

$$\forall a, c \in D_1 \, \forall b, d \in D_3 \, \big(b \neq d \;\Rightarrow\; g(a, \varphi(a), b) \neq g(c, \varphi(c), d)\big). \tag{18}$$

Доказательство полностью аналогично доказательству утверждения 3, за одним исключением: в шаге 1 построения функции восстановления f полагаем $f(g(a, \varphi(a), b)) = b$. ■

Алгоритм 7 строит функцию восстановления f, удовлетворяющую (17). Пусть $D_1 = \{a_1, \ldots, a_n\}$, $D_2 = \{b_1, \ldots, b_m\}$, $D_3 = \{c_1, \ldots, c_k\}$. Функция f строится с помощью обхода дерева в глубину. Как и в алгоритме 5, ярусы дерева соответствуют элементам из D_1, дуги — элементам из D_2. Для $a \in D_1$, $b \in D_2$ через $v(a, b)$ обозначим вектор значений подфункции $g(a, b, \cdot)$: $v(a, b) = \big(g(a, b, c_1), \ldots, g(a, b, c_k)\big) \in D^k$.

Вершине i-го яруса сопоставим множество векторов $V = \{v(a_r, b_{B[r]}) : r = 1, \ldots, i\}$, т. е. векторов $v(a, b)$ «вдоль» пути от корня до данной вершины. Для обеспечения (17) потребуем выполнения следующих условий:

1) в каждом векторе $v(a,b) \in V$ все координаты различны (что эквивалентно равенству $|G^{(a,b)}| = k$);
2) для любых $v = (v_1, \ldots, v_k), w = (w_1, \ldots, w_k) \in V$ и для всех $i, j \in \{1, \ldots, k\}$ если $v_i = w_j$, то $i = j$.

Алгоритм 7. Построение функции восстановления для обратимости типа $\forall\exists\forall$ по переменной x_3

Вход: функция $g : D_1 \times D_2 \times D_3 \to D$.
Выход: функция f, удовлетворяющая (17), или ответ «Функция g не обратима типа $\forall\exists\forall$ по переменной x_3».

1: Построить корень дерева с меткой $V = \varnothing$, объявить его текущим узлом; $i := 1$.
2: $j := 1$.
3: **Если** $|G^{(a_i,b_j)}| < k$, **то**
   перейти к п. 11.
4: Положить $w := (w_1, \ldots, w_k) = \big(g(a_i, b_j, c_1) \ldots, g(a_i, b_j, c_k)\big)$.
5: **Если** $\forall s, t \in \{1, \ldots, k\}\, \forall v = (v_1, \ldots, v_k) \in V \big(w_s = v_t \Rightarrow s = t\big)$, **то**
   добавить потомка с меткой $V \cup \{w\}$, объявить его текущим узлом; $B[i] := j$, $i := i + 1$.
6: **Если** $i = n + 1$, **то**
7: перейти к п. 17, // все ярусы пройдены
8: **иначе**
9: перейти к п. 2; // обход в глубину
10: **иначе**
11: **Если** $j < m$, **то**
   $j := j + 1$, перейти к п. 3; // построение дерева в ширину
12: **иначе**
13: объявить текущим предка текущего узла; $j := B[i]$. // возврат по дереву
14: **Если** $i > 0$, **то**
   $i := i - 1$, перейти к п. 11;
15: **иначе**
16: **выход**, ответ «Функция g не обратима типа $\forall\exists\forall$ по переменной x_3».
17: **Для всех** $v \in V$:
18: положить $f(v_i) = c_i$.

Для построения отображения φ, удовлетворяющего (18), на шаге 18 алгоритма 7 нужно положить $\varphi(a_i) = b_{B[i]}$, $i = 1, \ldots, n$.

Нетрудно убедиться, что функции g из примеров 4 и 5 не являются обратимыми типа $\forall\exists\forall$ по переменной x_3.

Пример 6. Пусть функция $g : \{1,2,3\} \times \{4,5\} \times \{0,1\} \to \{0,1,4,5\}$ задана в табл. 11. На рис. 5 представлено дерево, построенное алгоритмом 6; в табл. 12 и 13 — функция f и отображение φ, удовлетворяющие условиям (17) и (18) соответственно.

Таблица 11

x_1	x_2	x_3	g
1	4	0	1
1	4	1	5
1	5	0	5
1	5	1	5
2	4	0	1
2	4	1	4
2	5	0	1
2	5	1	0
3	4	0	4
3	4	1	5
3	5	0	0
3	5	1	1

Таблица 12

x	$f(x)$
0	1
1	0
4	0
5	1

Таблица 13

$a \in D_1$	$\varphi(a)$
1	4
2	5
3	4

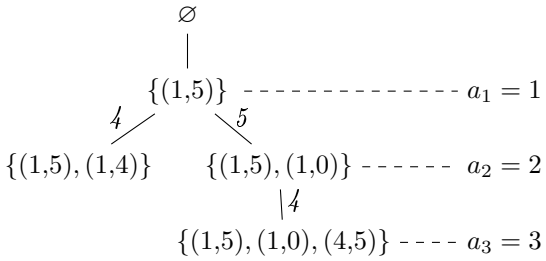

Рис. 5. Иллюстрация алгоритма 6

Алгоритм 8 строит функцию $g : D_1 \times D_2 \times D_3 \to D$, обратимую типа $\forall\exists\forall$ по переменной x_3.

Алгоритм 8. Генерация функции, обратимой типа $\forall\exists\forall$ по переменной x_3

Построить произвольное разбиение множества D на классы H_c, $c \in D_3$.
Для всех $a \in D_1$:
  выбрать $b \in D_2$.
  Для всех $c \in D_3$:
    выбрать $z \in H_c$, положить $g(a, b, c) := z$.
  Для всех $x_2 \in D_2 \setminus \{b\}$:
    Для всех $x_3 \in D_3$:
      выбрать в качестве $g(a, x_2, x_3)$ произвольное значение $y \in D$.

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

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

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

или, что то же самое, если

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

что равносильно обратимости типа $\forall\forall$ по переменной x_2 подфункции $g(a, x_2, x_3)$ для некоторого $a \in D_1$. Тогда из п. 1 утверждения 1 следует

Утверждение 5 (критерий обратимости типа $\exists\forall\forall$). Функция $g : D_1 \times D_2 \times D_3 \to D$ обратима типа $\exists\forall\forall$ по переменной x_2, если и только если существует такое значение $a \in D_1$, для которого выполнено условие

$$\forall b, d \in D_2 \big(b \neq d \;\Rightarrow\; G^{(a,b)} \cap G^{(a,d)} = \varnothing\big). \tag{19}$$

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

1) $f(g(a, b, c)) = b$ для $a \in D_1$, удовлетворяющего условию (19), и всех $b \in D_2$, $c \in D_3$;
2) $f(x)$ равна любому значению из D_2 для тех $x \in D$, значения на которых не определены на шаге 1.

Нетрудно видеть, что функция, заданная табл. 6, ни для одного $a \in \{1, 2, 3\}$ условию (19) не удовлетворяет:

$$G^{(1,4)} = \{0, 1\}, \quad G^{(1,5)} = \{4, 0\};$$
$$G^{(2,4)} = \{1, 4\}, \quad G^{(2,5)} = \{0, 4\};$$
$$G^{(3,4)} = \{1, 0\}, \quad G^{(3,5)} = \{5, 0\};$$

аналогично — для функции из табл. 8. Для функции g из табл. 11 и $a = 3$ условие выполнено: $G^{(3,4)} = \{4, 5\}$ и $G^{(3,5)} = \{0, 1\}$. Следовательно, она обратима типа $\exists\forall\forall$ по переменной x_2; функция восстановления f представлена в табл. 14.

Таблица 14

x	$f(x)$
0	5
1	5
4	4
5	4

Способ генерации функции $g : D_1 \times D_2 \times D_3 \to D$, обратимой типа $\exists\forall\forall$ по переменной x_2, описан в алгоритме 9.

Алгоритм 9. Генерация функции, обратимой типа $\exists\forall\forall$ по переменной x_2

1: Выбрать случайное $a \in D_1$.
2: Построить произвольное разбиение множества D на классы H_b, $b \in D_2$.
3: **Для всех** $b \in D_2$:
4: **Для всех** $c \in D_3$:
5: выбрать $z \in H_b$, положить $g(a, b, c) := z$.
6: **Для всех** $x_1 \in D_1 \setminus \{a\}$:
7: **Для всех** $x_2 \in D_2$:
8: **Для всех** $x_3 \in D_3$:
9: выбрать в качестве $g(x_1, x_2, x_3)$ произвольное значение $y \in D$.

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

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

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

Аналогично п. 2.4, это равносильно обратимости типа $\forall\exists$ подфункции $g(a, x_2, x_3)$ для некоторого $a \in D_1$. Тогда из п. 3 утверждения 1 следует

Утверждение 6 (критерий обратимости типа $\exists\forall\exists$ [7]). Функция $g : D_1 \times D_2 \times \times D_3 \to D$ обратима типа $\exists\forall\exists$ по переменной x_2, если и только если существуют такие значение $a \in D_1$ и отображение $\varphi : D_2 \to D_3$, для которых выполнено условие

$$\forall b, d \in D_2 \big(b \neq d \;\Rightarrow\; g(a, b, \varphi(b)) \neq g(a, d, \varphi(d))\big). \tag{20}$$

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

1) $f(g(a, b, \varphi(b))) = b$ для $a \in D_1$, удовлетворяющего условию (20), и всех $b \in D_2$;
2) $f(x)$ равна любому значению из D_2 для тех $x \in D$, значения на которых не определены на шаге 1.

Проверить обратимость функции g можно, применив алгоритм 1 (построения отображения φ) или алгоритм 2 (построения функции восстановления) поочерёдно для всех подфункций $g(a, x_2, x_3)$, $a \in D_1$.

Ввиду общезначимости формулы $\big(\forall x\, P(x) \;\Rightarrow\; \exists x\, P(x)\big)$, где $P(x)$ — произвольный предикат с непустой областью определения, получаем: из обратимости функции $g(x_1, x_2, x_3)$ типа $\exists\forall\forall$ по переменной x_2 следует её обратимость типа $\exists\forall\exists$ по той же переменной. Обратное в общем случае неверно; так, например, функция из табл. 8, которая не является обратимой типа $\exists\forall\forall$, обратима типа $\exists\forall\exists$. Отображение φ, удовлетворяющее условию (20) для $a = 1$, и соответствующая функция восстановления f представлены в табл. 15 и 16; символы «$*$» в табл. 16 означают, что $f(0)$ и $f(4)$ могут принимать любые значения из $\{4, 5\}$.

Таблица 15

$a \in D_2$	$\varphi(a)$
4	0
5	0

Таблица 16

x	$f(x)$
0	$*$
1	4
4	$*$
5	5

Способ генерации функции $g : D_1 \times D_2 \times D_3 \to D$, обратимой типа $\exists\forall\exists$ по переменной x_2, описан в алгоритме 10.

Алгоритм 10. Генерация функции, обратимой типа $\exists\forall\exists$ по переменной x_2

Выбрать случайное $a \in D_1$.
$Z := D$.
Для всех $b \in D_2$:
  выбрать $c \in D_3$, $z \in Z$;
  положить $g(a, b, c) := z$;
  $Z := Z \setminus \{z\}$.
  Для всех $x_3 \in D_3 \setminus \{c\}$:
    выбрать в качестве $g(a, b, x_3)$ произвольное значение $y \in D$.
Для всех $x_1 \in D_1 \setminus \{a\}$:
  Для всех $x_2 \in D_2$:
    Для всех $x_3 \in D_3$:
      выбрать в качестве $g(x_1, x_2, x_3)$ произвольное значение $y \in D$.

ЛИТЕРАТУРА

1. *Agibalov G. P.* Cryptanalytical finite automaton invertibility with finite delay // Прикладная дискретная математика. 2019. № 46. С. 27–37.

2. *Agibalov G. P.* Problems in theory of cryptanalytical invertibility of finite automata // Прикладная дискретная математика. 2020. № 50. С. 62–71.
3. *Бердникова Н. Ю., Панкратова И. А.* Криптоаналитическая обратимость функций двух аргументов // Прикладная дискретная математика. Приложение. 2021. № 14. С. 67–71.
4. *Фомичев В. М.* Методы дискретной математики в криптологии. М.: Диалог-МИФИ, 2010. 424 с.
5. *Агибалов Г. П.* О криптоаналитической обратимости с конечной задержкой конечных автоматов // Прикладная дискретная математика. Приложение. 2019. № 12. С. 84–86.
6. *Черемушкин А. В.* Обобщённые тождества медиальности и парамедиальности для сильно зависимых операций // Прикладная дискретная математика. 2024. № 65. С. 21–40.
7. *Панкратова И. А., Сорокоумова А. Д.* Криптоаналитическая обратимость функций трёх аргументов // Прикладная дискретная математика. Приложение. 2024. № 17. С. 44–48.

REFERENCES

1. *Agibalov G. P.* Cryptanalytical finite automaton invertibility with finite delay. Prikladnaya Diskretnaya Matematika, 2019, no. 46, pp. 27–37.
2. *Agibalov G. P.* Problems in theory of cryptanalytical invertibility of finite automata. Prikladnaya Diskretnaya Matematika, 2020, no. 50, pp. 62–71.
3. *Berdnikova N. Yu. and Pankratova I. A.* Kriptoanaliticheskaya obratimost' funktsiy dvukh argumentov [Cryptanalytic invertibility of two-argument functions]. Prikladnaya Diskretnaya Matematika. Prilozhenie, 2021, no. 14, pp. 67–71. (in Russian)
4. *Fomichev V. M.* Metody diskretnoy matematiki v kriptologii [Methods of Discrete Mathematics in Cryptology]. Moscow, Dialog-MIFI Publ., 2010. 424 p. (in Russian)
5. *Agibalov G. P.* O kriptoanaliticheskoy obratimosti s konechnoy zaderzhkoy konechnykh avtomatov [Cryptanalytic invertibility with finite delay of finite automata]. Prikladnaya Diskretnaya Matematika. Prilozhenie, 2019, no. 12, pp. 84–86.
6. *Cheremushkin A. V.* Obobshchennye tozhdestva medial'nosti i paramedial'nosti dlya cil'no zavisimykh operatsiy [Medial and paramedial general identities for strong dependance operations]. Prikladnaya Diskretnaya Matematika, 2024, no. 65, pp. 21–40. (in Russian)
7. *Pankratova I. A. and Sorokoumova A. D.* Kriptoanaliticheskaya obratimost' funktsiy trekh argumentov [Cryptanalytic invertibility of three-argument functions]. Prikladnaya Diskretnaya Matematika. Prilozhenie, 2024, no. 17, pp. 44–48. (in Russian)

МАТЕМАТИЧЕСКИЕ МЕТОДЫ КРИПТОГРАФИИ

УДК 519.23 DOI 10.17223/20710410/69/4

ХАРАКТЕРИСТИКИ АТАК РАЗЛИЧЕНИЯ НА 3 И 4 РАУНДА СХЕМЫ ЛУБИ — РАКОВА В МОДЕЛИ НЕЗАВИСИМЫХ ПОДСТАНОВОК

О. В. Денисов*, Е. Д. Андреев*, М. А. Батаев**

*ООО «Инновационные телекоммуникационные технологии», г. Москва, Россия
**ФГУП «НИИ „Квант“», г. Москва, Россия

E-mail: denisovOleg@yandex.ru, andreev5902@mail.ru, misha.bat72@gmail.com

Вычислены математические ожидания статистик Патарина, используемых в атаках различения на 3 и 4 раунда схемы Луби — Ракова по выбранным открытым текстам. В модели независимых подстановок, к каждой из которых производится по два запроса, получены оценки вероятностей ошибок и явные выражения для объёмов материала атак, построенных на аналогичных статистиках. В случае четырёх раундов при длинах блока 16–52 получены эмпирические вероятности ошибок в модели независимых подстановок и в модели запроса значений одной подстановки.

Ключевые слова: *схема Луби — Ракова, статистики Патарина, атака различения.*

CHARACTERISTICS OF DISTINGUISHING ATTACKS ON 3 AND 4 ROUNDS OF THE LUBY — RACKOFF SCHEME IN INDEPENDENT PERMUTATIONS MODEL

O. V. Denisov*, E. D. Andreev*, M. A. Bataev**

*Innovative Telecommunication Technologies, LLC, Moscow, Russia
**Federal State Unitary Enterprise “Scientific Research Institute ‘Kvant’”, Russia

We calculate the means of Patarin statistics that are used in distinguishing CPA-attacks on 3 and 4 rounds of the Luby — Rackoff scheme. We study a model of independent permutations and make two queries for each. In this model, we find estimates of error probabilities and explicit expressions for the data complexities of attacks based on similar statistics. In case of 4 rounds and block lengths 16–52 we have got empirical error probabilities in the model of independent permutations and in the model of queries for a single permutation.

Keywords: *Luby — Rackoff scheme, Patarin statistics, distinguishing attack.*

Введение

Рассмотрим R-раундовую схему Фейстеля с алфавитом полублоков $\mathbb{Z}_2^m$, операцией $\oplus$ покоординатного сложения полублоков по модулю 2 и раундовыми преобразованиями

$$(x^{r-1}, x^r) \to (x^r, x^{r-1} \oplus f_r(x^r)), \quad 1 \leqslant r \leqslant R.$$

В 1988 г. американские криптографы Луби (M. Luby) и Раков (C. Rackoff) ввели [1] вероятностную модель этой схемы, в которой раундовые функции усложнения выбираются независимо случайно равновероятно из множества всех двоичных вектор-функций от m переменных:

$$f_1, \ldots, f_R \sim U(\mathcal{F}_m),\ \mathcal{F}_m = \left\{ f \;\middle|\; f : \mathbb{Z}_2^m \to \mathbb{Z}_2^m \right\}.$$

Здесь и далее $U(\mathbb{X})$ — равномерное распределение вероятностей на множестве $\mathbb{X}$; символ $\sim$ означает «имеет распределение»; $\mathbb{S}(\mathbb{X})$ — множество подстановок на $\mathbb{X}$; $\mathbb{I}(A)$ — индикаторная функция условия A. Кратко эту вероятностную модель будем называть *ЛР-схемой* (Луби, Раков).

В течение следующих лет примерно до 2008 г. французским криптографом Жаком Патариным (J. Patarin) и другими авторами был получен ряд результатов: выведены нижние оценки объёмов материала атак различения на 3–4 раунда в разных моделях запросов (наблюдений), предложены атаки на R раундов с эвристическими асимптотическими ($m \to \infty$) оценками их объёма материала. Новый импульс к развитию эта тематика получила при разработке блочных *FPE-схем* (Format Preserving Encryption), т. е. схем шифрования, сохраняющих исходный формат шифруемых данных [2]. FPE-схемы FF1 и FF3, принятые как стандарт NIST, представляют собой схемы Фейстеля, раундовые функции усложнения которых при равновероятном выборе раундовых ключей близки к случайным равновероятным функциям. Поэтому свойства ЛР-схем используются для обоснования безопасности таких FPE-схем. Согласно [3, с. 446], идеи Патарина были использованы в [4] для построения атак восстановления сообщений. Методика Патарина использовалась также для расчёта нижних оценок стойкости схемы FEA-2 [5, с. 145–147], принятой в качестве стандарта FPE-шифрования в Южной Корее.

В работах [6; 7; 8, с. 68] приведены, в частности, статистики для атак различения на схему с $R = 3, 4$ раундами в модели запросов CPA (Chosen Plaintext Attack) — атаки на основе выбранных открытых текстов, однако критерии не были явно сформулированы и рассчитаны. В п. 1 данной работы получены точные значения математических ожиданий этих статистик при каждой из двух проверяемых гипотез.

В п. 2 в модели выбора независимых подстановок, к каждой из которых производится по два запроса, сформулированы аналогичные гипотезы, найдены математические ожидания и дисперсии аналогичных статистик. Построены критерии, размеры которых близки к заданному значению α. Даны оценки $N_1(\alpha, \beta)$ объёмов материала, при которых вероятности ошибок 2-го рода критериев близки к заданному значению β.

В п. 3 для атак на четыре раунда при длинах блоков $16 \leqslant 2m \leqslant 52$ проведены статистические эксперименты — получены эмпирические оценки вероятностей ошибок двух родов: 1) в модели запросов пар значений независимых подстановок; 2) в модели запроса значений одной подстановки на наборе из q заранее выбранных аргументов (т. е. в исходной модели Патарина) с таким выбором, что число $\binom{q}{2}$ слагаемых в статистике близко к $N_1(\alpha, \beta)$.

В п. 4 обсуждается связь полученных результатов с другими работами по разностному анализу. Пункт 1 написан авторами совместно, пп. 2–4 — первым автором. Авторы выражают признательность рецензенту за ряд полезных замечаний, способствовавших улучшению статьи.

1. Статистики Патарина в атаках на 3 и 4 раунда

1.1. Необходимые леммы

Сформулируем и докажем две леммы, необходимые для расчёта атак различения. Здесь и далее через $(x)_k = x(x-1)\dots(x-k+1)$, $k \in \mathbb{N}$, обозначаем k-ю факториальную степень числа $x \in \mathbb{R}$, а через $v^{\text{left}}, v^{\text{right}} \in \mathbb{Z}_2^m$ — левый и правый полублоки вектора $v \in \mathbb{Z}_2^{2m}$.

Лемма 1. Если пара блоков (σ_1, σ_2) выбирается случайно равновероятно без возвращения из $\mathbb{Z}_2^{2m}$, то

$$\Pr\left[(\sigma_1 \oplus \sigma_2)^{\text{left}} = x\right] = \begin{cases} 2^m/(2^{2m}-1) & \text{при } x \in \mathbb{Z}_2^m \setminus \{\mathbf{0}\}, \\ 1/(2^m+1) & \text{при } x = \mathbf{0}. \end{cases}$$

Доказательство. Так как $\Pr[\sigma_1 = a, \sigma_2 = b] = \dfrac{1}{(2^{2m})_2}$ для любых различных $a, b \in \mathbb{Z}_2^{2m}$, то при $x \neq \mathbf{0}$

$$\Pr\left[(\sigma_1 \oplus \sigma_2)^{\text{left}} = x\right] = \sum_{y \in \mathbb{Z}_2^{2m}} \Pr\left[\sigma_1 = y, \sigma_2 \in \{(y^{\text{left}} \oplus x, z) : z \in \mathbb{Z}_2^m\}\right] =$$

$$= \sum_{y \in \mathbb{Z}_2^{2m}} \sum_{z \in \mathbb{Z}_2^m} \Pr\left[\sigma_1 = y, \sigma_2 = (y^{\text{left}} \oplus x, z)\right] = \sum_{y \in \mathbb{Z}_2^{2m}} \sum_{z \in \mathbb{Z}_2^m} \frac{1}{(2^{2m})_2} =$$

$$= 2^{2m} \cdot 2^m \cdot \frac{1}{2^{2m}(2^{2m}-1)} = \frac{2^m}{2^{2m}-1}.$$

Следовательно, $\Pr\left[(\sigma_1 \oplus \sigma_2)^{\text{left}} = \mathbf{0}\right] = 1 - (2^m - 1)\dfrac{2^m}{2^{2m}-1} = \dfrac{2^m-1}{2^{2m}-1} = \dfrac{1}{2^m+1}$. ■

Известен следующий факт: если $\xi = (\xi_1, \dots, \xi_n) \sim U(A^n)$, A конечно, то $\Pr[\xi_i = \xi_j] = |A|^{-1}$ для любых фиксированных i, j. В следующей лемме этот факт обобщается на ситуацию случайного выбора пары индексов.

Лемма 2. Пусть $|A| < \infty$, $\mathcal{F} = \{F \mid F : A \to A\}$, пара (x, y) выбирается случайно из A^2 так, что $\Pr[x = y] = 0$, случайная функция $f \sim U(\mathcal{F})$ не зависит от (x, y). Тогда $\Pr[f(x) = f(y)] = |A|^{-1}$.

Доказательство. Условие равномерности распределения случайной функции f на $\mathcal{F}$ эквивалентно условию независимости и равномерной распределённости её значений на A. Поэтому для любых различных $a, b \in A$

$$\begin{aligned} \Pr[f(a) = f(b)] &= \sum_{c \in A} \Pr[f(a) = c, f(b) = c] = \\ &= \sum_{c \in A} \Pr[f(a) = c] \Pr[f(b) = c] = |A| \frac{1}{|A|^2} = \frac{1}{|A|}. \end{aligned} \tag{1}$$

Рассмотрим множество $E = \{(a, b) \in A^2 : a \neq b\}$. Так как $\Pr[(x, y) \in E] = 1$, то из аддитивности вероятности и независимости событий $\{x = a, y = b\}$ и $\{f(a) = f(b)\}$ с учётом (1) получаем

$$\Pr[f(x)=f(y)] = \sum_{(a,b)\in E} \Pr[(x,y)=(a,b), f(a)=f(b)] =$$

$$= \sum_{(a,b)\in E} \Pr[x=a, y=b] \Pr[f(a)=f(b)] = \sum_{(a,b)\in E} \Pr[x=a, y=b] \frac{1}{|A|} =$$

$$= \frac{1}{|A|} \Pr[(x,y)\in E] = \frac{1}{|A|}.$$

Лемма 2 доказана. ■

1.2. Средние значения статистик Патарина

Атаки различения на R раундов — это критерии проверки гипотез о случайной подстановке F на $\mathbb{Z}_2^{2m}$:

$$H_1 : F \sim U(\mathbb{S}(\mathbb{Z}_2^{2m})),$$
$$H_2 : F \text{ получена по } R\text{-раундовой ЛР-схеме.}$$

При входном блоке (x^0, x^1) в первой строке табл. 1 выписана последовательность полублоков схемы Фейстеля; выходом R-раундовой схемы является блок (x^R, x^{R+1}). Вывод строк 2, 3 обсуждается в п. 2 доказательства теоремы 1.

Таблица 1

Раундовые последовательности в схеме Фейстеля: полублоки, полуразности при $\Delta x^0 = \mathbf{0}$ либо при $\Delta x^1 = \mathbf{0}$

r	0	1	2	3	4
x^r	x^0	x^1	$x^0 \oplus f_1(x^1)$	$x^1 \oplus f_2(x^0 \oplus f_1(x^1))$	$x^0 \oplus f_1(x^1) \oplus f_3(x^1 \oplus f_2(x^0 \oplus f_1(x^1)))$
Δx^r	$\mathbf{0}$	Δx^1	$\Delta f_1(\Delta x^1)$	$\Delta x^1 \oplus \Delta f_2(\Delta f_1(\Delta x^1))$	$\Delta f_1(\Delta x^1) \oplus \Delta f_3(\Delta x^1 \oplus \Delta f_2(\Delta f_1(\Delta x^1)))$
Δx^r	Δx^0	$\mathbf{0}$	Δx^0	$\Delta f_2(\Delta x^0)$	$\Delta x^0 \oplus \Delta f_3(\Delta f_2(\Delta x^0))$

При $R = 3$ атака выглядит так [7, с. 225]:

1) для произвольного фиксированного x^0 выбираем (не обязательно равновероятно) q попарно различных полублоков x_i^1, $1 \leqslant i \leqslant q$;
2) запрашиваем значения $Y_i = F(x^0, x_i^1)$, $1 \leqslant i \leqslant q$;
3) вычисляем статистику $\nu_3 = \sum\limits_{1\leqslant i<j\leqslant q} \mathbb{I}\{Y_i^{\text{left}} \oplus x_i^1 = Y_j^{\text{left}} \oplus x_j^1\}$.

При $R = 4$ атака описывается аналогично [7, с. 225]:

1) для произвольного фиксированного x^1 выбираем (не обязательно равновероятно) q попарно различных полублоков x_i^0, $1 \leqslant i \leqslant q$;
2) запрашиваем значения $Y_i = F(x_i^0, x^1)$, $1 \leqslant i \leqslant q$;
3) вычисляем статистику $\nu_4 = \sum\limits_{1\leqslant i<j\leqslant q} \mathbb{I}\{Y_i^{\text{left}} \oplus x_i^0 = Y_j^{\text{left}} \oplus x_j^0\}$.

Далее через P_s и E_s обозначаем соответственно вероятностную меру и математическое ожидание при гипотезе H_s, $s = 1, 2$. В [7, с. 225] для $R = 3, 4$ без доказательства отмечается, что $\mathsf{E}_2\nu_R \approx 2\mathsf{E}_1\nu_R$. Найдём точные значения величин $\mathsf{E}_s\nu_R$ и докажем, что $\mathsf{E}_s\nu_3 = \mathsf{E}_s\nu_4$, $s \in \{1, 2\}$.

Теорема 1. При $s \in \{1, 2\}$ и $R \in \{3, 4\}$

$$\mathsf{E}_s\nu_R = \binom{q}{2} p_s, \text{ где } p_1 = \frac{2^{-m}}{1-2^{-2m}},\ p_2 = 2^{-m}(2-2^{-m}).$$

Доказательство. При фиксированных $i < j$ обозначим через $\Delta x^r = x_i^r \oplus x_j^r$ полуразности, $r \geqslant 0$. Тогда $(\Delta x^0, \Delta x^1)$ — входная разность подстановки F; через $\Delta Y = Y_i \oplus Y_j$ обозначим её выходную разность. С учётом линейности математического ожидания достаточно найти вероятности событий A_{ij} под знаком индикатора в сумме для ν_R при каждой из гипотез.

С л у ч а й $s = 1$. При $R = 3$ событие под знаком индикатора можем записать в виде $A_{ij} = \{\Delta Y^{\text{left}} = \Delta x^1\}$.

Для любого такого распределения (x_i^1, x_j^1), что $\Pr\left[x_i^1 = x_j^1\right] = 0$, при гипотезе H_1 случайные векторы (Y_i, Y_j) и (x_i^1, x_j^1) независимы. Действительно, в силу независимости набора из двух фиксированных значений равновероятной случайной подстановки F от пары входных блоков для любых $\{y_1, y_2\} \subset \mathbb{Z}_2^{2m}$, $\{x_1, x_2\} \subset \mathbb{Z}_2^m$ имеем

$$\begin{gathered}
\mathsf{P}_1\{(Y_i, Y_j) = (y_1, y_2), (x_i^1, x_j^1) = (x_1, x_2)\} = \\
= \mathsf{P}_1\{(F(x^0, x_1), F(x^0, x_2)) = (y_1, y_2), (x_i^1, x_j^1) = (x_1, x_2)\} = \\
= \mathsf{P}_1\{(F(x^0, x_1), F(x^0, x_2)) = (y_1, y_2)\}\, \mathsf{P}_1\{(x_i^1, x_j^1) = (x_1, x_2)\} = \\
= \frac{1}{(2^{2m})_2}\, \mathsf{P}_1\{(x_i^1, x_j^1) = (x_1, x_2)\},
\end{gathered}$$

и (Y_i, Y_j) имеет распределение случайной равновероятной выборки без возвращения из $\mathbb{Z}_2^{2m}$. Поэтому функции ΔY и Δx^1 от этих случайных векторов тоже независимы, и с учётом леммы 1 получаем

$$\begin{aligned}
\mathsf{P}_1(A_{ij}) &= \sum_{x \neq \mathbf{0}} \mathsf{P}_1\{(\Delta Y)^{\text{left}} = x,\, \Delta x^1 = x\} = \sum_{x \neq \mathbf{0}} \mathsf{P}_1\{(\Delta Y)^{\text{left}} = x\}\, \mathsf{P}_1\{\Delta x^1 = x\} = \\
&= \sum_{x \neq \mathbf{0}} \frac{2^m}{2^{2m} - 1}\, \mathsf{P}_1\{\Delta x^1 = x\} = \frac{2^m}{2^{2m} - 1} = \frac{1}{2^m} \frac{1}{1 - 2^{-2m}} = p_1.
\end{aligned}$$

При $r = 4$ аналогично доказывается, что событие $A_{ij} = \{\Delta Y^{\text{left}} = \Delta x^0\}$ имеет вероятность p_1.

С л у ч а й $s = 2$. Из рекуррентного соотношения $x^{r+1} = x^{r-1} \oplus f_r(x^r)$ следует $\Delta x^{r+1} = \Delta x^{r-1} \oplus \Delta f_r(\Delta x^r)$ для раундовых полуразностей схемы Фейстеля, $r \geqslant 1$; для краткости в записи приращений раундовых функций

$$\Delta f_r(x_i^r, \Delta x_i^r) = f_r(x_i^r) \oplus f_r(x_j^r) = f_r(x_i^r) \oplus f_r(x_i^r \oplus \Delta x_i^r)$$

первый аргумент опускаем.

Во второй строке табл. 1 последовательность раундовых полуразностей выписана при условии $\Delta x^0 = \mathbf{0}$, а в третьей — при $\Delta x^1 = \mathbf{0}$. При $R = 3$ с учётом второй строки имеем

$$A_{ij} = \{\Delta x^3 = \Delta x^1\} = \{\Delta f_2(\Delta f_1(\Delta x^1)) = \mathbf{0}\}.$$

Обозначая здесь для краткости $B = \{\Delta f_1(\Delta x^1) = \mathbf{0}\}$, применяя формулу полной вероятности и дважды лемму 2 (возможность применения леммы обосновывается независимостью случайных функций f_1 и f_2), находим

$$\begin{aligned}
\mathsf{P}_2(A_{ij}) &= \mathsf{P}_2(B) + \mathsf{P}_2\{\bar{B}\}\, \mathsf{P}_2\{\Delta f_2(\Delta f_1(\Delta x^1)) = \mathbf{0}) \,\big|\, \bar{B}\} = \\
&= 2^{-m} + (1 - 2^{-m})2^{-m} = 2^{-m}(2 - 2^{-m}) = p_2.
\end{aligned}$$

При $R = 4$, согласно третьей строке табл. 1, получаем

$$A_{ij} = \{\Delta x^4 = \Delta x^0\} = \{\Delta f_3(\Delta f_2(\Delta x^0)) = \mathbf{0}\}.$$

Аналогично случаю $R = 3$ доказывается, что вероятность этого события равна p_2.

Теорема 1 доказана. ■

Итак, в модели наблюдений Патарина, где запрашиваются значения одной подстановки, вычислены средние значения случайных величин ν_R при гипотезах H_1 и H_2. Но пока не вычислены значения дисперсий, из-за чего теоретический расчёт вероятностей ошибок критериев не представляется возможным. Однако эта проблема разрешима в модели наблюдения независимых двублочных текстов [9]. Условия этой модели дают независимость слагаемых в суммах для вводимых далее статистик $\nu'_{3,4}$, соответствующих статистикам $\nu_{3,4}$. Условие независимости слагаемых используется при оценке дисперсий статистик $\nu_{3,4}$ во всех известных работах Патарина, хотя оно не соответствует его модели наблюдений.

Поэтому, с одной стороны, переход к более простой модели независимых двублочных текстов позволяет более обоснованно строить критерии, рассчитывать их пороги и получать математически строгие результаты о вероятностях ошибок. Затем на этой основе строятся аналогичные критерии в исходной модели наблюдений. Соответствие параметров распределений статистик $\nu'_{3,4}$ и статистик $\nu_{3,4}$, определяющих вероятности ошибок критериев, проверяется экспериментально.

С другой стороны, в криптографии эта модель и более общая модель независимых q-блочных текстов возникает, например, когда для каждого шифртекста, полученного в режиме гаммирования, аналитик знает лишь q блоков исходного открытого текста, поэтому может вычислить лишь $\binom{q}{2}$ пар «входная/выходная разность» (подробнее см. [10, с. 98–100]).

2. Атаки на основе статистик Патарина в модели независимых двублочных текстов

Рассматривается модель наблюдений, в которой запросы делаются к случайным независимым подстановкам $F_1, \ldots, F_N$, одинаково распределённым на $\mathbb{S}(\mathbb{Z}_2^{2m})$. Требуется проверить следующие гипотезы:

$$\begin{aligned} &H_1 : F_1, \ldots, F_N \text{ выбраны равновероятно из } \mathbb{S}(\mathbb{Z}_2^{2m}),\\ &H_2 : F_1, \ldots, F_N \text{ — композиции } R \text{ раундов схемы Луби — Ракова.} \end{aligned} \tag{2}$$

При $R = 3, 4$ построим статистики $\nu'_{3,4}$, аналогичные статистикам Патарина, и на их основе — критерии проверки.

При $R = 3$: для $t = 1, \ldots, N$ запрашиваем значения $Y_{t1} = F_t(x_t^0, x_{t1}^1)$ и $Y_{t2} = F_t(x_t^0, x_{t2}^1)$, где случайные векторы $(x_t^0, x_{t1}^1, x_{t2}^1)$, $t = 1, \ldots, N$, независимы, $x_{t1}^1 \neq x_{t2}^1$; вычисляем статистику

$$\nu'_3 = \sum_{1 \leqslant t \leqslant N} \mathbb{I}\{(\Delta Y_t)^{\text{left}} = (\Delta X_t)^{\text{right}}\},$$

где $\Delta X_t = (x_t^0, x_{t1}^1) \oplus (x_t^0, x_{t1}^1)$ и $\Delta Y_t = Y_{t1} \oplus Y_{t2}$ — разности между аргументами и значениями подстановок.

При $R = 4$: для $t = 1, \ldots, N$ запрашиваем значения $Y_{t1} = F_t(x_{t1}^0, x_t^1)$ и $Y_{t2} = F_t(x_{t2}^0, x_t^1)$, где случайные векторы $(x_{t1}^0, x_{t2}^0, x_t^1)$ независимы, $x_{t1}^0 \neq x_{t2}^0$, вычисляем статистику

$$\nu'_4 = \sum_{1 \leqslant t \leqslant N} \mathbb{I}\{(\Delta Y_t)^{\text{left}} = (\Delta X_t)^{\text{left}}\}.$$

В силу независимости выбора блоков и подстановок в обоих случаях случайные величины ν'_R имеют биномиальное распределение $\mathrm{Bin}(N, p_i)$ при гипотезе H_i, $i = 1, 2$, где значения p_i определены в теореме 1. Поэтому критерии проверки гипотез (2) записываем единообразно:

$$d'_R : \nu'_R > c \Longrightarrow \text{ принимаем } H_2, \tag{3}$$

где $c \in [0, \infty)$ — параметр критерия.

Пусть $\alpha_i(d)$ — вероятность ошибки i-го рода критерия d, т. е. вероятность принятия гипотезы H_{3-i} при распределении наблюдений, соответствующих гипотезе H_i;

$$\Pi_\lambda(k) = \sum_{0 \leqslant i \leqslant k} \frac{\lambda^k e^{-\lambda}}{k!}$$

— функция распределения закона Пуассона $\mathrm{Pois}(\lambda)$; $\Phi(x)$ — функция распределения стандартного нормального закона $\mathcal{N}(0, 1)$; $\varkappa_\gamma$ — квантиль уровня γ распределения $\mathcal{N}(0, 1)$.

Обозначим $\lambda = N/2^m$, $\lambda_i = Np_i$ при $i = 1, 2$. Значения λ и $\lambda_{1,2}$ связаны неравенствами

$$\lambda = \lambda_1(1 - 2^{-2m}) < \lambda_1 < \lambda_2 = 2(1 - 2^{-m-1})\lambda < 2\lambda,$$

т. е. λ_1 практически совпадает с λ при не очень малых m, а λ_2 примерно в 2 раза больше значений λ_1 и λ.

В следующей теореме получены допредельные оценки вероятностей ошибок критериев с использованием пуассоновского приближения для распределений ν'_R (п. 1), нормального приближения (п. 2). Точность первого приближения лучше при малых значениях λ, второго — при больших. В п. 2 выписана явная оценка объёма материала.

Теорема 2. Пусть $R \in \{3, 4\}$. Тогда:

1) для любого $c \in \mathbb{N}_0$ справедливы оценки

$$|\alpha_1(d'_R) - (1 - \Pi_{\lambda_1}(c))| \leqslant \lambda_1^2/N, \quad |\alpha_2(d'_R) - \Pi_{\lambda_2}(c)| \leqslant \lambda_2^2/N \leqslant 4\lambda^2/N;$$

2) при пороге

$$c = c_\alpha = \lambda_1 + \varkappa_{1-\alpha}\sqrt{\lambda_1(1 - p_1)} = \lambda_1 + \varkappa_{1-\alpha}\sqrt{\frac{\lambda_1(1 - 2^{1-m} - 2^{-2m})}{1 - 2^{-2m}}}$$

справедлива следующая оценка размера:

$$|\alpha_1(d'_R) - \alpha| \leqslant \frac{0{,}4693(1 - 2^{-m})}{\sqrt{\lambda_1(1 - 2^{-2m})(1 - 2^{1-m})}}, \quad 0 < \alpha < 1;$$

3) если при этом пороге

$$N = N_1(\alpha, \beta) = \left(\frac{\varkappa_{1-\alpha}\dfrac{\sqrt{1 - 2^{1-m}}}{1 - 2^{-m}} + \varkappa_{1-\beta}(1 - 2^{-m})\sqrt{2 - 2^{-m}}}{1 - 2^{-m} - \dfrac{1}{2^{2m} - 1}} \right)^2 2^m,$$

то $|\alpha_2(d'_R) - \beta| \leqslant \dfrac{0{,}4693}{(1 - 2^{-m})\sqrt{2\lambda_1(1 - 2^{-2m})(1 - 2^{-m-1})}}$.

Доказательство.

1) Неравенства п. 1 вытекают из оценки [11, с. 105] точности пуассоновской аппроксимации для распределения сумм независимых одинаково распредёленных индикаторов и того, что величина 2λ чуть больше, чем λ_2.

2) Воспользуемся следующим результатом, вытекающим из оценки [12] константы в неравенстве Берри — Эссеена: если $S_N = \xi_1 + \ldots + \xi_N$ — сумма независимых одинаково распределённых случайных величин с нулевым средним и конечным третьим абсолютным моментом и $F(x)$ — функция распределения случайной величины $S_N/\sqrt{\mathsf{D}S_N}$, то для отклонения $\delta_N = \sup\limits_{x\in\mathbb{R}} |F(x) - \Phi(x)|$ выполнено неравенство

$$\delta_N\sqrt{N} \leqslant 0{,}4693\frac{\mathsf{E}|\xi_1|^3}{(\mathsf{D}\xi_1)^{3/2}}.$$

Если при этом $\xi_1 \sim \eta - p$, где $\eta \sim \mathrm{Be}(p)$, $0 < p < 1$, то $\mathsf{D}\xi_1 = \mathsf{D}\eta = pq$, $q = 1 - p$, $\mathsf{E}|\xi_1|^3 = pq^3 + qp^3 = (p^2 + q^2)\mathsf{D}\xi_1$, и тогда

$$\delta_N \leqslant 0{,}4693\frac{1 - 2pq}{\sqrt{Npq}} < \frac{0{,}4693}{\sqrt{Npq}}. \tag{4}$$

При гипотезе H_1 выражение под корнем в оценке (4) для распределения ν_R равно

$$Np_1(1 - p_1) = \frac{\lambda}{1 - 2^{-m}}\left(1 - \frac{2^{-m}}{1 - 2^{-m}}\right) = \frac{\lambda}{(1 - 2^{-m})^2}(1 - 2^{1-m}), \tag{5}$$

откуда, согласно (4), получаем оценку близости для вероятности

$$\alpha_1(d'_R) = \mathsf{P}_1\left\{\frac{\nu'_R - \lambda_1}{\sqrt{Np_1(1 - p_1)}} > \varkappa_{1-\alpha}\right\}$$

и её нормального приближения $1 - \Phi(\varkappa_{1-\alpha}) = \alpha$.

3) При гипотезе H_2 выражение под корнем в оценке (4) равно

$$Np_2(1 - p_2) = \lambda 2(1 - 2^{-m-1})(1 - 2^{-m+1} + 2^{-2m}) = 2\lambda(1 - 2^{-m-1})(1 - 2^{-m})^2, \tag{6}$$

что соответствует оценке близости вероятности

$$\alpha_2(d'_R) = \mathsf{P}_2\left\{\frac{\nu'_R - \lambda_2}{\sqrt{Np_2(1 - p_2)}} \leqslant x\right\}, \quad x = \frac{c_\alpha - \lambda_2}{\sqrt{Np_2(1 - p_2)}}$$

и её нормального приближения $\Phi(x)$.

Осталось показать, что $x = \varkappa_\beta = -\varkappa_{1-\beta}$. Обозначая здесь для краткости $t = 2^{-m}$ и учитывая (5) и (6), получаем

$$-x = \frac{2\lambda(1 - t/2) - \frac{\lambda}{1-t^2} - \varkappa_{1-\alpha}\frac{\sqrt{\lambda(1-2t)}}{1-t}}{(1 - t)\sqrt{2\lambda(1 - t/2)}} = \frac{\sqrt{\lambda}(2 - t - \frac{1}{1-t^2}) - \varkappa_{1-\alpha}\frac{\sqrt{1-2t}}{1-t}}{(1 - t)\sqrt{2 - t}}.$$

Это выражение равно $\varkappa_{1-\beta}$ при $\sqrt{\lambda} = \dfrac{\varkappa_{1-\alpha}\sqrt{1 - 2t}/(1 - t) + \varkappa_{1-\beta}(1 - t)\sqrt{2 - t}}{1 - t - t^2/(1 - t^2)}$, что выполнено при $N = N_1(\alpha, \beta)$. ■

Заметим, что абсолютная точность оценок погрешностей в пп.2–3 обратно пропорциональна величине $\sqrt{\lambda}$, которая при малых значениях 2^{-m} близка к величине $\varkappa_{1-\alpha} + \varkappa_{1-\beta}\sqrt{2}$. При $m \to \infty$ достаточное для атаки количество запрашиваемых пар выходных блоков асимптотически равно

$$N_1^*(\alpha, \beta) = (\varkappa_{1-\alpha} + \varkappa_{1-\beta}\sqrt{2})^2\, 2^m.$$

Это соответствует оценкам $q(m) = O(2^{m/2})$ числа запросов при атаках на $R = 3, 4$ раунда [7, с. 225–226], поскольку при таких $q(m)$ общее количество слагаемых в суммах статистик $\nu_{3,4}$ равно $\binom{q(m)}{2} = O(2^m)$.

При малых значениях 2^{-m} порог в п. 3 теоремы 2 близок к $c^* = \lambda + \varkappa_{1-\alpha}\sqrt{\lambda}$. Тогда при $\alpha = \beta$, $N = N_1^*(\alpha, \alpha)$ имеем

$$\varkappa_{1-\alpha} = \frac{\sqrt{\lambda}}{1+\sqrt{2}} = \sqrt{\lambda}(\sqrt{2}-1),\ \alpha = \Phi(-\sqrt{\lambda}(\sqrt{2}-1)), \quad c^* = \lambda\sqrt{2}. \tag{7}$$

При пороге $c = [\lambda\sqrt{2}]$ (целое число, ближайшее к c_α^*), согласно п. 1 теоремы, получаем, что вероятности ошибок критерия (3) будут близки к $\alpha_1^*(d) = 1 - \Pi_\lambda(c)$ и $\alpha_2^*(d) = \Pi_{2\lambda}(c)$. В табл. 2 приведены примеры вычисления этих величин.

Таблица 2

Грубая оценка α вероятностей ошибок атак и оценки вероятностей ошибок, близкие к истинным

λ	$\varkappa_{1-\alpha}$	α	c	$\alpha_1^*(d)$	$\alpha_2^*(d)$
4	0,82	0,204	6	0,11	0,31
9	1,24	0,107	13	0,073	0,142
16	1,65	0,048	23	0,026	0,06
25	2,07	0,019	35	0,022	0,016
36	2,48	0,006	51	0,007	0,005
49	2,89	0,0018	69	0,0027	0,0018
64	3,31	$4{,}6 \cdot 10^{-4}$	91	$5{,}8 \cdot 10^{-4}$	$3{,}5 \cdot 10^{-4}$

Из табл. 2 видно, что для критериев, получаемых посредством нормальной аппроксимации, формулы (7) позволяют неплохо оценивать среднее значение двух вероятностей ошибок.

3. Эксперименты при $R = 4$ в двух моделях наблюдений

Параметрами, определяющими проведение экспериментов, в обеих моделях наблюдений были длины полублока m и различные значения λ (первая часть табл. 3 — два столбца до двойной вертикали).

Во второй части табл. 3 представлены теоретические значения оценок $\alpha_1^*{=}1{-}\Pi_\lambda(c)$, $\alpha_2^* = \Pi_{2\lambda}(c)$ (при некоторых λ они были вычислены в табл. 2) вероятностей ошибок критерия (3) с порогом $c(\lambda) = [\lambda\sqrt{2}]$ (см. формулу (7)) в модели независимых двублочных текстов при объёме выборки $N_1^* = \lambda 2^m$. Количество A экспериментов выбиралось с учётом порядка малости величин α_i^*.

В третьей части табл. 3 представлены объём материала N_1^* в модели независимых двублочных текстов и полученные эмпирические вероятности ошибок $\hat{\alpha}_1(d_4')$.

В четвёртой части табл. 3 приведены условие и результаты экспериментов в модели наблюдений Патарина, т. е. при q-блочной выборке из одной подстановки: количество запросов $q = q(\lambda) = [\sqrt{2^{m+1}\lambda}] = [\sqrt{2\lambda}2^{m/2}]$, которое даёт общее число слагаемых $\binom{q}{2} \approx \lambda 2^m$ индикаторов в сумме для статистики ν_4, близкое к N_1^*, и полученные эмпирические вероятности ошибок $\hat{\alpha}_1(d_4)$. Здесь применялся критерий с тем же порогом:

$$d_4 : \nu_4 > [\lambda\sqrt{2}] \Longrightarrow \text{ принимаем } H_2. \tag{8}$$

Таблица 3

Теоретические и эмпирические характеристики атак различения на 4 раунда схемы Луби — Ракова

$2m$	λ	α_1^*	α_2^*	A	N_1^*	$\hat{\alpha}_1(d_4')$	$\hat{\alpha}_2(d_4')$	$q(\lambda)$	$\hat{\alpha}_1(d_4)$	$\hat{\alpha}_2(d_4)$
16	25	0,022	0,016	10^3	6,4 E3	0,026	0,01	113	0,032	0,03
20	25	0,022	0,016	10^3	2,5 E4	0,034	0,009	226	0,039	0,01
24	4	0,11	0,31	10^2	1,6 E4	0,22	0,19	181	0,25	0,15
24	9	0,073	0,142	10^3	3,6 E4	0,132	0,105	272	0,13	0,09
28	4	0,11	0,31	50	6,5 E4	0,16	0,24	362	0,12	0,28
32	4	0,11	0,31	50	2,6 E5	0,22	0,16	724	0,18	0,20
36	4	0,11	0,31	50	1,0 E6	0,14	0,24	1,4 E3	0,16	0,20
40	4	0,11	0,31	50	4,2 E6	0,26	0,22	2,8 E3	0,10	0,14
40	9	0,073	0,142	10^2	9,4 E6	0,12	0,05	4,3 E3	0,17	0,10
44	4	0,11	0,31	20	1,6 E7	0,2	0,15	5,7 E3	0,3	0,25
48	4	0,11	0,31	20				1,1 E4	0,1	0,15
52	4	0,11	0,31	20				2,3 E4	0,2	0,25

Статистика ν_4 вычислялась так: при фиксированном $x^1 = 0$ (здесь и далее отождествляем векторы из $\mathbb{Z}_2^m$ с числами, двоичной записью которых являются векторы) полагаем $x_i^0 = i$. Поэтому здесь

$$\nu_4 = \sum_{0 \leqslant i < j \leqslant q-1} \mathbb{I}\{Y_i^{\text{left}} \oplus i = Y_j^{\text{left}} \oplus j\}, \quad Y_i = F(i,0),\ 0 \leqslant i \leqslant q-1.$$

Как отмечается в [7, с. 225], для вычисления ν_R за $O(q)$ операций можно сохранять значения $Y_i^{\text{left}} \oplus x_i^0$ и «считать коллизии». Подробнее: 1) инициализируем нулями все элементы массива coll[ ] длины 2^m, полагаем $i = 0$; 2) увеличиваем на 1 содержимое элемента с индексом $Y_i^{\text{left}} \oplus i$; 3) если $i < q-1$, то увеличиваем i на 1 и повторяем п. 2, в противном случае завершаем подсчёт числа коллизий. Тогда верно равенство

$$\nu_4 = \sum_{0 \leqslant y \leqslant 2^m-1} \left|\left\{\{i,j\} \subset \{0,\ldots,q-1\} : Y_i^{\text{left}} \oplus i = Y_j^{\text{left}} \oplus j = y\right\}\right| = \sum_{0 \leqslant y \leqslant 2^m-1} \binom{\text{coll}[y]}{2}.$$

Временна́я сложность эксперимента $O(2^m)$ в первой модели быстро растёт, что ограничило длину блока 48 битами. Снижение сложности во второй модели наблюдений до $O(q) = O(2^{m/2})$ позволило провести эксперименты до длины блока 52 битов включительно.

Таким образом, можно сделать следующие выводы:

1. Части 2 и 3 табл. 3 показывают хорошее[1] согласие эмпирических вероятностей ошибок в модели независимых двублочных текстов и теоретических: отношения

[1] При неверных расчётах эмпирические вероятности могут отличаться от теоретических на несколько порядков.

$\hat{\alpha}_i(d_4')/\alpha_i^*$ в основном лежат в пределах от 0,5 до 2. Это подтверждает правильность расчётов в теоремах 1 и 2.

2. Аналогично части 2 и 4 табл. 3 показывают хорошее согласие эмпирических вероятностей ошибок в модели Патарина и теоретических оценок, рассчитанных в модели независимых двублочных текстов. Это говорит о том, что зависимость между слагаемыми статистики ν_4, имеющаяся в модели Патарина, не привела к существенным отклонениям её распределения от распределения аналогичной статистики ν_4' в значительно более простой модели наблюдений.

3. Разработанные подходы и полученные результаты дают основу для построения и расчёта атак на большее количество раундов ЛР-схемы.

4. Обзор связей с другими работами по разностному анализу

Статистики Патарина могут быть записаны в виде

$$\nu_3 = \sum_{1\leqslant i<j\leqslant q} \mathbb{I}\{\Delta Y_{ij}^{\text{left}} = \Delta x_{ij}^{\text{right}}\}, \quad \nu_4 = \sum_{1\leqslant i<j\leqslant q} \mathbb{I}\{\Delta Y_{ij}^{\text{left}} = \Delta x_{ij}^{\text{left}}\},$$

т. е. являются разностными. Точнее, они являются функциями от усечённых разностей [13], атаки производятся при нулевой левой (правой) входной полуразности при $R = 3$ ($R = 4$), подсчитывается число совпадений левой выходной полуразности с правой (левой) входной. Но, несмотря на одновременное развитие разностного анализа с 1990 г., даже замечаний о связи с ним в известных работах Патарина не обнаружено, в том числе в итоговой монографии [8]. Таким образом, эта ветвь разностного анализа развивалась отдельно от «основного древа». Что касается его представителей, то нам известны лишь две работы [14, 15], в которых дан некоторый анализ статистик Патарина с точки зрения разностного метода.

В русскоязычной литературе, насколько известно авторам, разностный анализ схем Луби — Ракова впервые был начат в [16], где установлено, что схема является марковским шифром, т. е. последовательность раундовых разностей образует однородную цепь Маркова. Был найден блочный вид матрицы переходных вероятностей разностей за один раунд, обозначаемой далее через $\mathbb{P} = \mathbb{P}(M)$, $M = 2^m$. Из теоремы о блочном умножении матриц [17, с. 21] следует, что все степени $\mathbb{P}$ имеют такое же разбиение на M^2 клеток размера M, как и $\mathbb{P}(M)$. В [16] найден блочный вид матриц $\mathbb{P}^2$ и $\mathbb{P}^4$; доказательства этих результатов можно найти в [18]. Заметим, что из описания [16, формула (4)] элементов $\mathbb{P}^4$ при нулевой правой входной полуразности $\Delta X^{\text{right}} = 0$ может быть выведено равенство $p_2 = M\dfrac{2M^2 - M}{M^4} = M^{-1}(2 - M^{-1})$ теоремы 1 при $R = 4$.

В [16] также построена последовательная атака различения (критерий Вальда) на 4 раунда в модели независимых двублочных текстов с входными полуразностями $\Delta X_t^{\text{right}} = 0$. Получены оценки средней длины материала при гипотезах $H_{1,2}$ и больших M

$$T_1(M) = \frac{(1-2\alpha)\ln\big((1-\alpha)/\alpha\big)}{1-\ln 2}M, \quad T_2(M) = \frac{(1-2\alpha)\ln\big((1-\alpha)/\alpha\big)}{2\ln 2 - 1}M$$

для критерия с расчётными вероятностями ошибок α. В частности, при $\alpha = 0{,}1$ эти величины равны соответственно $5{,}72M$ и $4{,}55M$, что примерно в 2 раза меньше значения $9M$, при котором, согласно табл. 2, вероятности ошибок атаки на основе аналога статистики Патарина будут близки к 0,107 и 0,073.

В [16] эксперименты проводились для длин блока от 12 до 44 битов; в данной работе в модели экспериментов с одной подстановкой «потолок» длины блоков повышен

до 52 битов благодаря малой временно́й сложности вычисления статистик Патарина. Результаты каких-либо других статистических экспериментов с ЛР-схемой нам неизвестны; их отсутствие можно частично объяснить недостаточной теоретической проработанностью материала зарубежными криптографами — отсутствием формул для порога критерия, обеспечивающего заданный размер; отсутствием явных оценок объёма материала.

ЛИТЕРАТУРА

1. *Luby M. and Rackoff C.* How to construct pseudorandom permutations from pseudorandom functions // SIAM J. Comput. 1988. V. 17. P. 373–386.
2. *Tsaregorodtsev K. D.* Format-preserving encryption: a survey // Мат. вопр. криптогр. 2022. Т. 13. Вып. 2. С. 133–153.
3. *Bellare M., Hoang V. T., and Tessaro S.* Message-recovery attacks on Feistel-based format preserving encryption // Proc. CCS'16. Vienna, Austria, 2016. P. 444–455.
4. *Bellare M., Ristenpart T., Rogaway P., and Stegers T.* Format-preserving encryption // LNCS. 2009. V. 5867. P. 295–312.
5. *Lee J., Koo B., Roh D., et al.* Format-preserving encryption algorithms using families of tweakable blockciphers // LNCS. 2015. V. 8949. P. 132–159.
6. *Patarin J.* New results on pseudorandom permutation generators based on the DES scheme // LNCS. 1992. V. 576. P. 301–312.
7. *Patarin J.* Generic attacks on Feistel schemes // LNCS. 2001. V. 2248. P. 222–238.
8. *Nachef V., Patarin J., and Volte E.* Feistel Ciphers: Security Proofs and Cryptanalysis. Cham: Springer, 2017. 309 p.
9. *Денисов О. В.* Атаки различения на блочные шифрсистемы по разностям двублочных текстов // Прикладная дискретная математика. 2020. № 48. С. 43–62.
10. *Денисов О. В.* Многомерный спектральный критерий для проверки гипотез о случайных подстановках // Мат. вопр. криптогр. 2023. Т. 14. Вып. 3. С. 85–106.
11. *Боровков А. А.* Теория вероятностей. М.: Эдиториал УРСС, 1999. 472 с.
12. *Шевцова И. Г.* Об абсолютных константах в неравенстве Берри — Эссеена и его структурных и неравномерных уточнениях // Информатика и ее примен. 2013. Т. 7. Вып. 1. С. 124–125.
13. *Knudsen L.* Truncated and higher order differentials // LNCS. 1995. V. 1008. P. 196–211.
14. *Knudsen L.* The security of Feistel ciphers with six rounds or less // J. Cryptology. 2002. V. 15. P. 207–222.
15. *Dunkelman O., Kumar A., Lambooij E., and Sanadhya S. K.* Cryptanalysis of Feistel-Based Format-Preserving Encryption. Cryptology ePrint Archive. 2020. Report 2020/1311. `https://eprint.iacr.org/2020/1311`.
16. *Денисов О. В.* Атака различения на четыре раунда шифра Люби — Ракофф по разностям двублочных текстов // Прикладная дискретная математика. Приложение. 2023. № 16. С. 32–35.
17. *Ланкастер П.* Теория матриц. М.: Наука, 1978. 280 с.
18. *Денисов О. В.* Спектральные атаки различения на схемы Луби — Ракова по независимым двублочным текстам // Мат. вопр. криптогр. 2024. Т. 15. Вып. 4. С. 23–42.

REFERENCES

1. *Luby M. and Rackoff C.* How to construct pseudorandom permutations from pseudorandom functions. SIAM J. Comput., 1988, vol. 17, pp. 373–386.

2. *Tsaregorodtsev K. D.* Format-preserving encryption: a survey. Matematicheskie Voprosy Kriptografii, 2022, vol. 13, iss. 2, pp. 133–153.
3. *Bellare M., Hoang V. T., and Tessaro S.* Message-recovery attacks on Feistel-based format preserving encryption. Proc. CCS'16, Vienna, Austria, 2016, pp. 444–455.
4. *Bellare M., Ristenpart T., Rogaway P., and Stegers T.* Format-preserving encryption. LNCS, 2009, vol. 5867, pp. 295–312.
5. *Lee J., Koo B., Roh D., et al.* Format-preserving encryption algorithms using families of tweakable blockciphers. LNCS, 2015, vol. 8949, pp. 132–159.
6. *Patarin J.* New results on pseudorandom permutation generators based on the DES scheme. LNCS, 1992, vol. 576, pp. 301–312.
7. *Patarin J.* Generic attacks on Feistel schemes. LNCS, 2001, vol. 2248, pp. 222–238.
8. *Nachef V., Patarin J., and Volte E.* Feistel Ciphers: Security Proofs and Cryptanalysis. Cham, Springer, 2017. 309 p.
9. *Denisov O. V.* Ataki razlicheniya na blochnye shifrsistemy po raznostyam dvublochnykh tekstov [Distinguishing attacks on block ciphers by differentials of two-block texts]. Prikladnaya Diskretnaya Matematika, 2020, no. 48, pp. 43–62. (in Russian)
10. *Denisov O. V.* Mnogomernyy spektral'nyy kriteriy dlya proverki gipotez o sluchaynykh podstanovkakh [Multidimensional spectral criterion for testing hypotheses on random permutations]. Matematicheskie Voprosy Kriptografii, 2023, vol. 14, iss. 3, pp. 85–106. (in Russian)
11. *Borovkov A. A.* Teoriya veroyatnostey [Probability Theory]. Moscow, URSS, 1999. 472 p. (in Russian)
12. *Shevtsova I. G.* Ob absolyutnykh konstantakh v neravenstve Berri — Esseena i ego strukturnykh i neravnomernykh utochneniyakh [On absolute constants in the Berry-Esseen inequality and its structural and uneven refinements]. Informatika i ee Primeneniya, 2013, vol. 7, no. 1, pp. 124–125. (in Russian)
13. *Knudsen L.* Truncated and higher order differentials. LNCS, 1995, vol. 1008, pp. 196–211.
14. *Knudsen L.* The security of Feistel ciphers with six rounds or less. J. Cryptology, 2002, vol. 15, pp. 207–222.
15. *Dunkelman O., Kumar A., Lambooij E., and Sanadhya S. K.* Cryptanalysis of Feistel-Based Format-Preserving Encryption. Cryptology ePrint Archive, 2020, Report 2020/1311. `https://eprint.iacr.org/2020/1311`.
16. *Denisov O. V.* Ataka razlicheniya na chetyre raunda shifra Lyubi — Rakoff po raznostyam dvublochnykh tekstov [Distinguishing attack on four rounds of the Luby — Rackoff cipher by differentials of two-block texts]. Prikladnaya Diskretnaya Matematika. Prilozhenie, 2023, No. 16, pp. 32–35. (in Russian)
17. *Lankaster P.* Theory of Matrices. N.Y.; London, Academic Press, 1969.
18. *Denisov O. V.* Spektral'nye ataki razlicheniya na skhemy Lubi — Rakova po nezavisimym dvublochnym tekstam [Spectral attacks on Luby-Rackoff schemes based on independent two-block texts]. Matematicheskie Voprosy Kriptografii, 2024, vol. 15, iss. 4, pp. 23–42. (in Russian)

УДК 003.26 DOI 10.17223/20710410/69/5

ПРОТОКОЛ МЕНТАЛЬНОГО ПОКЕРА, ОСНОВАННЫЙ НА ЗАДАЧАХ ПОИСКА ИЗОГЕНИЙ МЕЖДУ ЭЛЛИПТИЧЕСКИМИ КРИВЫМИ[1]

И. Д. Иогансон*,**,***, В. В. Давыдов*,**,***, Ж.-М. Н. Дакуо*,**,***, А. Ф. Хуцаева*,***

*Университет ИТМО, г. Санкт-Петербург, Россия
**QApp, г. Москва, Россия
***Санкт-Петербургский государственный университет аэрокосмического приборостроения, г. Санкт-Петербург, Россия

E-mail: ivan.ioganson@yandex.ru, vadimdavydov@outlook.com, jeandakuo@mail.ru, afkhutsaeva@itmo.ru

Представлен новейший квантово-устойчивый протокол ментального покера, основанный на задаче поиска изогений между эллиптическими кривыми. Данный протокол позволяет нескольким пользователям создавать и перемешивать колоду карт, а затем выдавать карту определённому пользователю. Разработаны две версии протокола: без валидации, которая позволяет защититься только от пассивного злоумышленника, и с валидацией, позволяющая обнаружить активное вмешательство в протокол с помощью протоколов доказательства с нулевым разглашением. Для валидации предложенного решения разработана программа на языке C, реализующая описанный протокол. Полученные результаты демонстрируют возможность практического применения предложенного решения, обеспечивая защиту от атак с использованием квантового компьютера.

Ключевые слова: *протокол ментального покера, эллиптические кривые, изогении, постквантовая криптография.*

MENTAL POKER PROTOCOL BASED ON THE PROBLEM OF FINDING ISOGENIES BETWEEN ELLIPTIC CURVES

I. D. Ioganson*,**,***, V. V. Davydov*,**,***, Zh.-M. N. Dakuo*,**,***, A. F. Khutsaeva*,***

*ITMO University, Saint Petersburg, Russia
**QApp, Moscow, Russia
***Saint-Petersburg State University of Aerospace Instrumentation, Saint Petersburg, Russia

In the paper, a novel isogeny-based protocol for mental poker game is presented. This protocol allows multiple users to create and shuffle a deck of cards, and then issue a card to a specific user. Two versions of the protocol are developed: one without validation, which protects only against passive adversaries, and one with validation, which also allows detecting active interference with the protocol using zero-knowledge proof protocols. To validate the resulting solution, a C program was developed that implements the described protocol. This demonstrates the practical applicability of the proposed solution while ensuring protection against quantum attacks.

Keywords: *mental poker protocol, elliptic curves, isogenies, post-quantum cryptography.*

[1]Работа выполнена в рамках госзадания (проект FSER-2025-0003).

Введение

Протокол ментального покера — криптографический протокол, позволяющий нескольким игрокам играть в карточную игру на расстоянии с использованием средств связи. Основная цель таких протоколов — позволить игрокам играть в карточные игры, не раскрывая друг другу свои карты и не используя доверенную сторону, которая могла бы контролировать процесс игры. Все операции, включая генерацию и тасование колоды, должны быть распределены между игроками таким образом, чтобы гарантировать честность процесса.

Впервые протокол ментального покера был представлен в 1979 г. в работе [1], но впоследствии было показано, что предложенная схема небезопасна [2, 3]. В дальнейшем эта область получила некоторое развитие в работах [4, 5]. Протокол перемешивания карт в ментальном покере находит широкое применение в смешивающих сетях (Mix network) и протоколах электронного голосования [6, 7].

В связи с ростом интереса к децентрализованным технологиям протоколы ментальных карточных игр представляют важное направление развития криптографических методов, способных обеспечить честность даже в условиях полного недоверия между участниками. Упомянутые выше решения основаны на задачах, уязвимых к атакам на квантовом компьютере, в связи с чем появляется необходимость создания новых квантово-защищённых протоколов, в частности протоколов ментальных карточных игр.

Одной из актуальных постквантовых областей является криптография, основанная на изогениях между эллиптическими кривыми. Данная область динамично развивается; только за последний год был предложен ряд работ: новейшие схемы цифровой подписи [8–11], проверяемая случайная функция (VRF) [12], схема электронного голосования [13], механизм инкапсуляции ключа [14] и др. [15, 16]. Данные работы демонстрируют высокий потенциал математического аппарата изогений эллиптических кривых.

В данной работе предлагаются два варианта протокола, основанного на постквантовой задаче поиска изогений между суперсингулярными эллиптическими кривыми. Протокол состоит из четырёх фаз: подготовка колоды, тасование колоды, выдача карты пользователю и открытие карты. Рассматриваются два варианта протокола: *с валидацией*, который позволяет защищаться от активного злоумышленника, имеющего возможность манипулировать передаваемой информацией с целью получения преимущества, и *без валидации*, который является «облегчённой» версией протокола с валидацией и предназначен только для честных игроков (не нарушающих ход протокола); при этом скорость выполнения второго варианта протокола в разы выше первого.

Работа имеет следующую структуру. В п. 1 представлены предварительные сведения, необходимые для описания протокола. В п. 2 описаны существующие решения, а также прототип протокола, на основе которого строится разработанное решение. В п. 3 описываются два варианта разработанного протокола — без валидации и с валидацией. Пункт 4 содержит доказательства безопасности предложенных протоколов. В п. 5 описываются результаты вычислительных экспериментов, приводятся оценки быстродействия и затрачиваемой памяти. В заключении подводятся итоги работы, описываются достоинства и недостатки предложенного протокола.

1. Предварительные сведения

Введём базовые понятия, необходимые для описания протокола [17, 18].

Пусть $\mathbb{N}, \mathbb{Z}, \mathbb{Q}$ — стандартные обозначения числовых множеств. Эллиптическая кривая E — это неособая кубическая кривая, $\mathbb{K}$ — некоторое поле, ∞ — бесконечно удалён-

ная точка на эллиптической кривой. Для задач криптографии, как правило, используются кривые в форме Вейерштрасса:

$$E_W : y^2 = x^3 + Ax + B,$$

или в форме Монтгомери:

$$E_M : By^2 = x^3 + Ax^2 + x,$$

где $A, B \in \mathbb{K}$.

Пусть $n \in \mathbb{N}$. Группой точек кручения на кривой E, заданной над полем $\mathbb{K}$, называется группа точек

$$E[n] = \{P \in E(\overline{\mathbb{K}}) : nP = \infty\},$$

где $\overline{\mathbb{K}}$ — алгебраическое замыкание поля $\mathbb{K}$.

Кривая E, заданная над конечным полем $\mathbb{F}_p$, называется суперсингулярной, если $E[p] = \{\infty\}$. Кривая E называется обычной, если $E[p] \cong \mathbb{Z}/p\mathbb{Z}$.

Пусть E_1 и E_2 — эллиптические кривые, заданные над конечным полем $\mathbb{F}_q$, где $q = p^n$, p — некоторое простое число, $n \in \mathbb{N}$. Изогенией называется нетривиальный гомоморфизм

$$\varphi : E_1 \to E_2,\ \varphi(\infty_{E_1}) = \infty_{E_2}.$$

Две кривые называются изогенными, если существует изогения между ними. Любую изогению $\varphi : E_1 \to E_2$ можно задать в явном виде:

$$\forall P \in E_1(\mathbb{F}_q)\ \exists Q \in E_2(\mathbb{F}_q)\big(\varphi(P) = Q\big), \quad P = (x, y), \quad Q = \left(\frac{p(x)}{q(x)}, y \cdot r(x)\right).$$

Здесь $p(x), q(x), r(x) \in \mathbb{F}_q[x]$. Степень изогении может быть вычислена как

$$\deg \varphi = \max\{\deg p(x), \deg q(x)\}.$$

Изогения называется сепарабельной, если $\left(\frac{p(x)}{q(x)}\right)' \neq 0$. Для сепарабельных изогений верно, что $\deg \varphi = \# \ker \varphi$, где $\ker \varphi$ — ядро изогении. При построении криптографических схем работа ведётся только с сепарабельными изогениями.

Пусть необходимо вычислить изогению $\varphi : E_1 \to E_2$, $G = \ker \varphi$. Для её вычисления могут использоваться формулы Велу [19]:

— $\forall P \in G\ \big(\varphi(P) = \infty\big)$;

— $\forall P = (x_P, y_P) \notin G\ \left(\varphi(P) = \left(x_P + \sum\limits_{Q \in G \setminus \{\infty\}} (x_{P+Q} - x_Q),\ y_P + \sum\limits_{Q \in G \setminus \{\infty\}} (y_{P+Q} - y_Q)\right)\right)$.

Ядро G определяет отображение из кривой E_1 в кривую E_2 с точностью до изоморфизма:

$$E_1/G \stackrel{\text{def}}{=} E_2.$$

Если ядро изогении φ — циклическая подгруппа, то изогения называется циклической. Сложность подсчёта изогении растёт линейно в зависимости от количества точек в $\ker \varphi$, поэтому подсчёт не всегда эффективен. Пусть φ может быть представлена как композиция изогений

$$\varphi = \psi_1 \circ \psi_2 \circ \cdots \circ \psi_m,$$

где $\deg \psi_i = p_i$, $1 \leqslant i \leqslant m$. Тогда степень изогении φ можно представить как

$$\deg \varphi = \prod_{j=1}^{n} p_j^{\ell_j},$$

где ℓ_j — количество изогений степени p_j. В таком случае $\deg \varphi$ является гладким числом и изогению можно представить как композицию из ℓ_j изогений степени p_j для $1 \leqslant j \leqslant n$, тем самым сильно упростив вычисления.

Если $\varphi : E \to E'$ — изогения степени λ, то существует единственная изогения (называемая дуальной) $\hat{\varphi} : E' \to E$, такая, что

$$\hat{\varphi} \circ \varphi = [\lambda]_E, \quad \varphi \circ \hat{\varphi} = [\lambda]_{E'},$$

где $[\lambda]$ обозначает сложение точки самой с собой λ раз.

Пусть эллиптическая кривая E задана над конечным полем K. Эндоморфизмом кривой E называется её изогения, действующая в себя: $\varphi : E(\overline{K}) \to E(\overline{K})$. Множество всех таких изогений и нулевое отображение образуют кольцо эндоморфизмов $\mathrm{End}(E)$. Различают также кольцо эндоморфизмов, заданное над полем K: $\mathrm{End}_K(E)$, в котором содержатся все изогении $\varphi' : E(K) \to E(K)$.

Пусть X — некоторое коммутативное кольцо. X-модулем называется абелева группа M, на которой X действует линейно. X-модуль M называется конечно порождённым, если существует такое конечное множество элементов $\{m_1, \ldots, m_n\}$ в X-модуле, что верно следуюшее свойство:

$$\forall m \in M \left(m = x_1 m_1 + \ldots + x_n m_n\right), \quad x_i \in X,\ i \in \{1, \ldots, n\}.$$

Пусть $f : X \to Y$ — гомоморфизм колец, а произведение элементов $x \in X$, $y \in Y$ определяется формулой

$$xy = f(x)y.$$

Всякое кольцо Y, снабжённое структурой X-модуля, называется X-алгеброй, т. е. X-алгебра — пара, состоящая из кольца Y и гомоморфизма колец $f : X \to Y$; Y называется конечно порождённой X-алгеброй, если существует конечное число таких элементов $x_1, \ldots, x_n$ в X-алгебре, что каждый элемент Y можно записать в виде многочлена от $x_1, \ldots, x_n$ с коэффициентами из X [20].

Пусть K — конечно порождённая $\mathbb{Q}$-алгебра. Порядком $\mathcal{O} \subset K$ называется подкольцо K, которое является конечно порождённым $\mathbb{Z}$-модулем максимальной размерности.

Согласно соответствию Дойринга (Deuring) об изоморфизме кольца эндоморфизмов эллиптической кривой [21, 22], для кривой, заданной над конечным полем $\mathbb{K}$, кольцо эндоморфизмов изоморфно либо порядку в мнимом квадратичном поле, либо порядку в алгебре кватернионов, заданной над $\mathbb{Q}$.

Для обычной кривой $E'/\mathbb{F}_p$ кольцо эндоморфизмов изоморфно порядку в мнимом квадратичном поле, а также $\mathrm{End}(E') = \mathrm{End}_{\mathbb{F}_p}(E')$. Для суперсингулярной кривой $E/\mathbb{F}_p$ $\mathrm{End}(E)$ изоморфно порядку в алгебре кватернионов, при этом $\mathrm{End}_{\mathbb{F}_p}(E)$ — это порядок в мнимом квадратичном поле, т. е.

$$\mathrm{End}_{\mathbb{F}_p}(E) \hookrightarrow \mathbb{Q}(\pi),$$

где π — эндоморфизм Фробениуса эллиптической кривой $E/\mathbb{F}_p$:

$$\pi : E \to E, \quad (x, y) \mapsto (x^p, y^p).$$

Обозначим такой порядок как $\mathcal{O}$. Тогда, так как $\mathrm{End}_{\mathbb{F}_p}(E) \cong \mathcal{O}$ (порядку в мнимом квадратичном поле), можно определить действие элемента $\alpha \in \mathcal{O}$ на точку кривой $P \in E$ как $\alpha(P) = \varphi_\alpha(P)$, где φ_α — это эндоморфизм кривой E, изоморфный α. Для любого ненулевого идеала $\mathfrak{a} \subset \mathcal{O}$ можно построить подгруппу

$$E[\mathfrak{a}] = \{P \in E : \forall \alpha \in \mathfrak{a}\,(\alpha(P) = 0)\}.$$

Изогения $\varphi_\mathfrak{a} : E \to E/E[\mathfrak{a}]$, соответствующая идеалу $\mathfrak{a}$, является изогенией с ядром $\ker(\varphi_\mathfrak{a}) = E[\mathfrak{a}]$. Норма идеала $\mathfrak{a} \subset \mathcal{O}$ задаётся как $N(\mathfrak{a}) = |\mathcal{O}/\mathfrak{a}|$, то есть как мощность фактор-кольца. Степень изогении $\varphi_\mathfrak{a}$ равна норме идеала: $\deg \varphi_\mathfrak{a} = \mathrm{N}(\mathfrak{a})$.

Пусть $I(\mathcal{O})$ — множество всех идеалов порядка $\mathcal{O}$. Идеалы $\mathfrak{a}, \mathfrak{b} \in I(\mathcal{O})$ называются эквивалентными, если существует $\alpha \in \mathcal{O}$, такой, что $\mathfrak{a} = \alpha \cdot \mathfrak{b} = \{\alpha \cdot \beta : \beta \in \mathfrak{b}\}$. Обозначим эквивалентность идеалов $\mathfrak{a}$ и $\mathfrak{b}$ как $\mathfrak{a} \sim \mathfrak{b}$. Классом эквивалентности идеала $\mathfrak{a}$ называется множество $[\mathfrak{a}] = \{\mathfrak{b} \in I(\mathcal{O}) : \mathfrak{a} \sim \mathfrak{b}\}$. Множество классов эквивалентности идеалов кольца $\mathcal{O}$ обозначим $Cl(\mathcal{O})$. Между классами эквивалентности можно определить операцию «$\cdot$» через соответствующую операцию кольца $\mathcal{O}$:

$$[\mathfrak{a}] \cdot [\mathfrak{b}] = [\mathfrak{a} \cdot \mathfrak{b}].$$

Для простоты далее будем считать, что $[\mathfrak{a} \cdot \mathfrak{b}] = [\mathfrak{a}\mathfrak{b}]$. Тогда $Cl(\mathcal{O})$ образует конечную абелеву группу [23] относительно операции «$\cdot$» умножения идеалов с нейтральным элементом $[\mathcal{O}]$ — класс идеала, включающего всё кольцо. Одним из свойств группы является обратимость элементов: для любого $[\mathfrak{a}] \in Cl(\mathcal{O})$ существует $[\mathfrak{a}]^{-1} \in Cl(\mathcal{O})$, такой, что $[\mathfrak{a}] \cdot [\mathfrak{a}]^{-1} = [\mathcal{O}]$.

Если идеалы $\mathfrak{a}$ и $\mathfrak{b}$ лежат в одном и том же классе из группы классов идеалов $Cl(\mathcal{O})$, то $E/E[\mathfrak{a}] \cong E/E[\mathfrak{b}]$ над полем $\mathbb{F}_p$.

Дадим определение группового действия [24]. Группа G действует на множестве X, если существует отображение $\star : G \times X \to X$, для которого выполнены следующие свойства:

1) взаимодействие с нейтральным элементом: если e — нейтральный элемент группы G, то $e \star x = x$ для всех $x \in X$;
2) совместимость: $(gh) \star x = g \star (h \star x)$ для всех $g, h \in G$ и $x \in X$.

В такой нотации групповое действие обозначается как $(G, X, \star)$. Групповые действия могут обладать дополнительными свойствами:

1) транзитивностью: групповое действие $(G, X, \star)$ транзитивно, если

$$\forall x_1, x_2 \in X\, \exists g \in G\, (x_2 = g \star x_1);$$

2) свободой: групповое действие $(G, X, \star)$ свободно, если для всех $g \in G$ элемент g является нейтральным тогда и только тогда, когда существует $x \in X$, такой, что $x = g \star x$;
3) коммутативностью: групповое действие $(G, X, \star)$ коммутативно, если

$$\forall g_1, g_2 \in G \forall x \in X \left(g_1 \star (g_2 \star x) = g_2 \star (g_1 \star x)\right).$$

Групповое действие называется криптографическим, если оно удовлетворяет следующим свойствам [24]:

1) однонаправленностью: по заданной паре элементов $(x, g \star x)$, где $g \in G$ и $x \in X$ выбраны случайным образом, вычислительно сложно найти g;

2) непредсказуемостью: пусть дано полиномиально большое количество пар элементов $(x_i, g \star x_i)$, где $g \in G$ и $x_i \in X$ выбраны случайным образом. Тогда вычислительно сложно найти $g \star x^*$ для заданного $x^* \in X$;
3) псевдослучайностью: вычислительно сложно отличить множество пар элементов $(x_i, g \star x_i)$ от множества пар элементов (x_i, u_i), где $g \in G$ и $x_i, u_i \in X$ выбраны случайным образом.

Пусть $\mathscr{E}\ell\ell(\mathcal{O})$ — множество эллиптических кривых над конечным полем $\mathbb{F}_p$, кольца эндоморфизмов которых изоморфны порядку $\mathcal{O}$ в мнимом квадратичном поле. Зададим действие группы классов идеалов $Cl(\mathcal{O})$ на множестве кривых $\mathscr{E}\ell\ell(\mathcal{O})$:

$$\star : Cl(\mathcal{O}) \times \mathscr{E}\ell\ell(\mathcal{O}) \to \mathscr{E}\ell\ell(\mathcal{O}), \quad (\mathfrak{a}, E) \mapsto [\mathfrak{a}] \star E.$$

Указанное действие выполняется следующим образом. Для идеала $\mathfrak{a}$ вычисляется подгруппа точек кручения $E[\mathfrak{a}]$. Затем по алгоритму Велу вычисляется изогения $\varphi_{\mathfrak{a}} : E \to E_1$, такая, что $\ker(\varphi_{\mathfrak{a}}) = E[\mathfrak{a}]$. Результатом выполнения группового действия является кривая $E_1 = [\mathfrak{a}] \star E$, лежащая в том же множестве [25].

Данное групповое действие является криптографическим, а также транзитивно, свободно и коммутативно. Задача обращения группового действия на множестве эллиптических кривых является вычислительно трудной [26].

Задача обратного группового действия (*Group Action Inverse Problem, GAIP*)

Пусть заданы эллиптические кривые E_0 и E над конечным полем $\mathbb{F}_p$, $\mathrm{End}_{\mathbb{F}_p}(E) = \mathcal{O}$. Вычислительно трудно найти идеал $\mathfrak{a} \subset \mathcal{O}$, такой, что $E = [\mathfrak{a}] \star E_0$. При этом идеал $\mathfrak{a}$ должен быть представлен таким образом, что групповое действие $\star$ может быть эффективно вычислено.

Данная задача лежит в основе известного протокола выработки общего ключа CSIDH [27, 28] и алгоритма цифровой подписи CSI-FiSh [26]. Её преимуществом является сложность решения не только на классических вычислительных машинах, но и на квантовых. Наиболее эффективный алгоритм в классической модели вычислений имеет экспоненциальную сложность, а в квантовой модели — субэкспоненциальную (алгоритм Куперберга [29]).

2. Существующие решения

Протоколы ментальных карточных игр можно разделить на две группы: с доверенной третьей стороной (Trusted Third Party, TTP) и без неё. Первая группа протоколов для генерации, тасования колоды и последующей раздачи карт использует TTP, а вторая группа производит все эти операции децентрализованно. В данной работе рассматриваются и строятся протоколы без участия TTP.

Протоколы ментальных карточных игр без TTP также можно разделить на две основные группы. Протоколы из первой группы называют протоколами «без перетасовок». К данному типу относится, например, протокол, описанный в [30]. К протоколам второй группы относятся протоколы «с перетасовкой» [31–33].

В протоколе «без перетасовок» выдача карты происходит путём совместной генерации зашифрованного случайного номера выдаваемой карты. Затем игроки должны проверить, что данная карта ещё ни разу не была выдана, и если это не так, то они вынуждены запускать протокол сначала. Таким образом, чем больше карт выдаётся, тем больше вероятность того, что новая карта совпадёт с одной из уже выданных, что увеличивает ожидаемое количество перезапусков протокола. Следовательно, в играх, где используется вся колода, данная группа протоколов может требовать большого

времени на генерацию карты. В данной работе рассматриваются протоколы «с перетасовкой».

Будем называть открытой колодой карт колоду до перетасовки, перетасованной (закрытой) колодой — колоду после перетасовки, открытой и закрытой картой — карту из открытой и перетасованной колод соответственно, маской карты — секретное значение, индивидуальное для каждого игрока и генерируемое при перетасовке.

В качестве прототипа предлагаемого протокола выбран протокол [33] ментального покера, состоящий из четырёх основных частей: 1) подготовка колоды (протокол 2.1); 2) тасование колоды (протокол 2.2); 3) выдача карты (протокол 2.3); 4) открытие карты.

Протокол 2.1. Подготовка колоды

Вход: M — количество карт.

Выход: открытая колода A.

1 Игроки генерируют случайное большое простое число n и группу $\langle G, \cdot \rangle$ порядка n.

2 Игроки сообща генерируют случайные значения $a_i \in G$ для $i = 0, \ldots, M$.

3 **Вернуть** $A = \{a_i : i \in \{0, \ldots, M\}\}$.

Значение a_0 не является картой, а используется в дальнейшем для верификации; общее количество игроков — N.

Протокол 2.2. Тасование колоды

Вход: A — открытая колода, n — порядок группы G, M — количество карт.

Выход: перетасованная колода B.

1 $B_0 := \{b_{0,i}\}$, где $b_{0,i} = a_i \in A$ для $i = 0, \ldots, M$.

2 **Для** $j \in \{1, \ldots, N\}$ *каждый игрок* P_j*:*

3 Выбирает случайное число $0 < x_j < n$ и запоминает его.

4 Выбирает случайную перестановку $S_j : \{0, \ldots, M\} \to \{0, \ldots, M\}$, такую, что $S_j(0) = 0$.

5 Публикует $B_j = \{b_{j,i}\}$, где $b_{j-1,i} = b_{j,S_j(i)}^{x_j} \in G$ для $i = 0, \ldots, M$.

6 Остальные игроки проверяют корректность перетасовки с помощью заранее выбранного протокола доказательства с нулевым разглашением

7 . **Вернуть** $B = B_N$ — *перетасованная колода.*

Во время выполнения протокола 2.2 на шаге 3 каждый игрок запоминает значение секретной маски x_j для последующего использования в протоколе 2.3 на шагах 5 и 8.

Для открытия карты игрок P_{j_0} публикует ранее выданную карту c, и с помощью сигма-протокола Чаума — Педерсена [34] остальные игроки проверяют, что полученное значение корректно.

Протокол 2.3. Выдача карты

Вход: c_0 — карта из перетасованной колоды, j_0 — номер игрока, получающего карту c_0, n — порядок группы G.

Выход: открытая карта c.

Для $j \in \{1, \dots, N\}$ *каждый игрок* P_j*:*
  Если $j = j_0$, **то:**
    $c_j := c_{j-1}$.
  Иначе:
    $y_j = x_j^{-1} \bmod n$, где x_j — секретная маска игрока j.
    Публикует $c_j := c_{j-1}^{y_j} \in G$.
    С помощью сигма-протокола Чаума — Педерсена [34] остальные игроки проверяют, что полученное значение корректно.
Игрок P_{j_0} вычисляет $y_{j_0} = x_{j_0}^{-1} \bmod n$, где x_{j_0} — секретная маска игрока j_0.
Игрок P_{j_0} вычисляет $c := c_N^{y_{j_0}} \in G$.
Карта c выдана игроку j_0.
Вернуть c — *открытая карта.*

3. Предлагаемое решение

3.1. Протокол без валидации

Данная версия протокола предназначена для защиты от модели злоумышленника «Honest-But-Curious». В этой модели злоумышленник не пытается активно вмешиваться в протокол, но может анализировать полученные в ходе протокола данные, чтобы получить преимущество.

Протоколы подготовки колоды, тасования колоды, выдачи карты и открытия карты описаны как протоколы 3.1, 3.2 и 3.3 соответственно. Здесь и далее операция $x \xleftarrow{\$} S$ — присвоение переменной x случайного значения, выбранного из равномерного распределения на множестве S; операция «$\star$» — действие группы классов идеалов $Cl(\mathcal{O})$ на множестве кривых $\mathscr{E}\ell\ell(\mathcal{O})$.

Протокол 3.1. Подготовка колоды

Вход: $p \in \mathbb{N}$ — простое число, $E_0/\mathbb{F}_p$ — начальная эллиптическая кривая с $\mathrm{End}_{\mathbb{F}_p}(E_0) \cong \mathcal{O}$, $Cl(\mathcal{O})$ — группа классов идеалов порядка $\mathcal{O}$, $M \in \mathbb{N}$ — количество карт, $N \in \mathbb{N}$ — количество игроков.

Выход: открытая колода $A \in \mathscr{E}\ell\ell(\mathcal{O})^M$.

Для $i = 1, \dots, M$*:*
  $a_i^{(0)} := E_0$.
  Для $j = 1, \dots, N$*:*
    Игрок P_j выбирает $[\mathfrak{x}_j] \xleftarrow{\$} Cl(\mathcal{O})$.
    Игрок P_j вычисляет $a_i^{(j)} := [\mathfrak{x}_j] \star a_i^{(j-1)}$.
    Игрок P_j передаёт $a_i^{(j)}$ игроку P_{j+1}.
$A := \{a_i^{(N)} : i = 1, \dots, M\}$
Вернуть A.

Протокол 3.2. Тасование колоды

Вход: $M \in \mathbb{N}$ — количество карт, $N \in \mathbb{N}$ — количество игроков, $A \in \mathscr{E}\ell\ell(\mathcal{O})^M$ — открытая колода, $Cl(\mathcal{O})$ — группа классов идеалов (см. протокол 3.1).

Выход: перетасованная колода $B \in \mathscr{E}\ell\ell(\mathcal{O})^M$.

1 $B^{(0)} := A$

2 **Для** $i = 1, \ldots, N$:

3 Игрок P_i выбирает случайную перестановку $S_i : \{1, \ldots, M\} \to \{1, \ldots, M\}$.

4 Игрок P_i выбирает $[\mathfrak{y}_i] \xleftarrow{\$} Cl(\mathcal{O})$ и запоминает его.

5 Игрок P_i вычисляет $B^{(i)} := \left([\mathfrak{y}_i] \star b^{(i-1)}_{S_i(1)}, [\mathfrak{y}_i] \star b^{(i-1)}_{S_i(2)}, \ldots, [\mathfrak{y}_i] \star b^{(i-1)}_{S_i(M)}\right)$, где $b^{(i-1)}_t \in B^{(i-1)}$ для $t \in \{1, \ldots, M\}$.

6 $B := B^{(N)}$.

7 **Вернуть** B.

Протокол 3.3. Выдача карты

Вход: $c^{(0)} \in \mathscr{E}\ell\ell(\mathcal{O})$ — карта из перетасованной колоды, $k \in \mathbb{N}$ — номер игрока, которому эта карта предназначена, $N \in \mathbb{N}$ — количество игроков.

Выход: открытая карта $c \in \mathscr{E}\ell\ell(\mathcal{O})$.

1 **Для** $j \in \{1, \ldots, N\} \setminus \{k\}$:

2 Игрок P_j вычисляет $c^{(j)} := [\mathfrak{y}_j]^{-1} \star c^{(j-1)}$, где $[\mathfrak{y}_j]$ — секретная маска игрока j.

3 Игрок P_k вычисляет $c := [\mathfrak{y}_k]^{-1} \star c^{(N-1)}$, где $[\mathfrak{y}_k]$ — секретная маска игрока k.

4 **Вернуть** c.

Во время выполнения протокола 3.2 на шаге 4 каждый игрок запоминает значение секретной маски $[\mathfrak{y}_i]$ для последующего использования в протоколе 3.3 на шагах 2 и 3.

Для открытия карты игрок P_j публикует ранее выданную карту c.

3.2. Протокол с валидацией

Данная версия протокола включает протоколы доказательства с нулевым разглашением (Zero-Knowledge Proof, ZKP) и предназначена для защиты от злоумышленника, который может активно подменять посылаемую информацию для получения выгоды. Если один из игроков нарушит ход протокола, то данный факт можно будет однозначно доказать. Для этого вся переданная в ходе работы протокола информация верифицируется с помощью протоколов доказательства с нулевым разглашением.

Описание работы протоколов 4.1, 4.2, 4.3 представлено в Приложении 1, протоколов доказательства с нулевым разглашением — в Приложении 2.

4. Стойкость протоколов

4.1. Стойкость протоколов без валидации

Стойкость предложенных протоколов основывается на предположении о сложности решения задачи обратного группового действия за полиномиальное время на классическом и квантовом компьютерах (см. п. 1).

Лучшим классическим алгоритмом для решения задачи обратного группового действия является атака «встреча посередине» [27], имеющая экспоненциальную сложность — $O(\sqrt{\#Cl(\mathcal{O})})$. Лучшим квантовым алгоритмом для решения GAIP является алгоритм Куперберга [29], обеспечивающий субэкспоненциальную временну́ю сложность — $2^{O(\sqrt{\log N})}$.

Свойства протокола

При разработке протокола ментального покера важными задачами являются формализация и реализация гарантий безопасности, характерных для классического оффлайн-покера, где физические ограничения и наблюдаемость процесса обеспечивают честность и справедливость. В цифровой среде отсутствие прямого контакта между участниками требует использования криптографических примитивов, которые позволяют гарантировать честность и прозрачность процесса игры. В связи с этим стойкий протокол ментального покера должен гарантировать следующие свойства:

1) при генерации колоды нельзя создать «краплёную» открытую колоду;
2) при перетасовке нельзя замешать колоду так, как это выгодно одному или нескольким игрокам;
3) при выдаче карты никто, кроме игрока, которому эта карта выдаётся, не может узнать содержимое карты;
4) для протокола с валидацией: если кто-то из игроков нарушает ход протокола, то существует доказательство этого.

Выбранные свойства напрямую отражают классические требования покера; при их выполнении протокол гарантирует честную игру или, в случае нарушений, идентификацию нечестных игроков.

Идеальная функциональность

Докажем выполнение перечисленных свойств через сведение протокола к идеальному путём использования UC-модели. В UC-модели для доказательства стойкости протокола сначала описывается идеальная функциональность протокола. Под идеальной функциональностью подразумевается версия протокола, которая получает тот же самый результат, но в которой все вычисления проводятся третьей доверенной стороной, которая работает как «чёрный ящик»: получает входные значения и выдаёт только результат работы протокола. Затем необходимо доказать, что работа настоящего протокола неотличима от его идеальной функциональности. Под неотличимостью понимается, что для стороннего наблюдателя, которому известен только вход и выход протокола, невозможно отличить, какой из протоколов использовался: настоящий или идеальный. Если настоящий протокол неотличим от идеального, то он считается стойким [35].

В протоколах 5.1–5.3 приведены три идеальные функциональности, которые полностью имитируют предлагаемый протокол ментального покера.

Протокол 5.1. Идеальный функционал протокола подготовки колоды

Вход: $\mathscr{E}\ell\ell(\mathcal{O})$ — множество эллиптических кривых, заданных над конечным полем $\mathbb{F}_p$ (p — простое число), кольца эндоморфизмов которых изоморфны порядку $\mathcal{O}$ в мнимом квадратичном поле, M — количество карт.

Выход: открытая колода A.

1 **Для** $i = 1, \ldots, M$:

2 ⌊ TTP генерирует случайное $a_i \xleftarrow{\$} \mathscr{E}\ell\ell(\mathcal{O})$.

3 $A := \{a_i\}$ для $i \in \{1 \ldots M\}$.

4 **Вернуть** A.

Протокол 5.2. Идеальный функционал протокола тасования колоды

Вход: $A = \{a_1, \ldots, a_M\}$ — открытая колода, M — количество карт, N — количество игроков, $Cl(\mathcal{O})$ — группа классов идеалов порядка $\mathcal{O}$ в мнимом квадратичном поле, $Y = \{[\mathfrak{y}_1], \ldots, [\mathfrak{y}_N]\} \subset Cl(\mathcal{O})$ — множество секретных ключей пользователей.

Выход: перетасованная колода B.

1 TTP выбирает случайную перестановку $S : \{1, \ldots, M\} \to \{1, \ldots, M\}$.

2 TTP вычисляет

$$B := \big([\mathfrak{y}_1] \star [\mathfrak{y}_2] \star \ldots [\mathfrak{y}_N] \star a_{S(1)},\ [\mathfrak{y}_1] \star [\mathfrak{y}_2] \star \ldots [\mathfrak{y}_N] \star a_{S(2)},\ \ldots,\ [\mathfrak{y}_1] \star [\mathfrak{y}_2] \star \ldots [\mathfrak{y}_N] \star a_{S(M)}\big).$$

3 **Вернуть** B.

Протокол 5.3. Идеальный функционал протокола выдачи карты

Вход: $c^{(0)}$ — карта из перетасованной колоды, N — количество игроков, $Cl(\mathcal{O})$ — группа классов идеалов порядка $\mathcal{O}$ в мнимом квадратичном поле, $Y = \{[\mathfrak{y}_1], \ldots, [\mathfrak{y}_N]\} \subset Cl(\mathcal{O})$ — множество секретных ключей пользователей.

Выход: открытая карта c.

1 TTP вычисляет $c := [\mathfrak{y}_1]^{-1} \star [\mathfrak{y}_2]^{-1} \star \cdots \star [\mathfrak{y}_N]^{-1} \star c^{(0)}$.

2 **Вернуть** c.

Модель злоумышленника

В контексте описанного протокола рассмотрим две модели злоумышленника: *Honest-But-Curious* и *Malicious* [36]. В обоих случаях злоумышленник является одним из игроков. В модели *Honest-But-Curious* злоумышленником является игрок, который честно следует протоколу, но обладает способностью анализировать полученную в ходе игры информацию для получения выгоды. В подобном случае достаточно быть уверенным, что такой игрок не сможет получить преимущество, анализируя полученную информацию. Вариант протокола без валидации направлен как раз на борьбу с подобным типом игроков. В модели *Malicious* злоумышленник может не только анализировать информацию, но и произвольно изменять отправляемые им данные. Для защиты от этого необходимо не только применять все те же методы, что и в модели *Honest-But-Curious*, но и проверять валидность полученной информации. Для этого в варианте протокола с валидацией используются протоколы доказательства с нулевым разглашением.

Введём понятие Knowledge для участника протокола. Knowledge участника протокола состоит из его секретных входных значений, случайных данных и всех сообщений, полученных в ходе выполнения протокола. Knowledge злоумышленника состоит из объединения Knowledge всех скомпрометированных сторон. Вся информация, которую злоумышленник может получить из протокола, должна быть вычисляемой за полиномиальное время из его Knowledge. Введём также понятие симулятора Sim. Под симулятором понимается некий оракул, который может вычислить Knowledge злоумышленника.

Более формально *Honest-But-Curious* злоумышленника можно описать следующим образом. Пусть есть протокол π и его идеальная функциональность $\mathcal{F}$;

$\mathcal{C} \subset \{P_1, P_2, \ldots, P_N\}$ — множество злоумышленников среди игроков; Sim — симулятор протокола. Определим следующие распределения случайных значений:

— $\mathsf{Real}_\pi(k, \mathcal{C}, x_1, \ldots, x_N)$: выполняет протокол с параметром стойкости k, где каждый участник P_i честно следует протоколу, используя входные секретные значения x_i. Пусть V_i обозначает $\mathsf{Knowledge}$ участника P_i, а y_i — его выходное значение. Выходом является $(V_1, \ldots, V_N)$, $(y_1, \ldots, y_N)$.

— $\mathsf{Ideal}_{\mathcal{F},\mathsf{Sim}}(k, \mathcal{C}, x_1, \ldots, x_N)$: вычисляет $(y_1, \ldots, y_N) = \mathcal{F}(x_1, \ldots, x_N)$. Выходом является $\mathsf{Sim}(\mathcal{C}, \{(x_i, y_i) : P_i \in \mathcal{C}\})$, $(y_1, \ldots, y_N)$.

Протокол считается стойким в *Honest-But-Curious*-модели злоумышленника, если злоумышленники в реальном протоколе имеют $\mathsf{Knowledge}$, неотличимое от их $\mathsf{Knowledge}$ в симуляторе.

Malicious злоумышленник, в отличие от *Honest-But-Curious*, может не только анализировать полученную в ходе протокола информацию, но и произвольно менять отправляемые данные. Это означает, что сообщения, посылаемые злоумышленником в данной модели, не могут быть заранее определены. Пусть $\mathcal{A}$ — алгоритм, которым руководствуется злоумышленник в реальном протоколе. Обозначим $\mathrm{corrupt}(\mathcal{A})$ множество участников, скомпрометированных злоумышленником, а $\mathrm{corrupt}(\mathsf{Sim})$ — множество участников, скомпрометированных злоумышленником в идеальной функциональности. Определим следующие распределения случайных значений:

— $\mathsf{Real}_{\pi,\mathcal{A}}(k, \{x_i : P_i \notin \mathrm{corrupt}(\mathcal{A})\})$: выполняет протокол с параметром стойкости k, где каждый участник $P_i \notin \mathrm{corrupt}(\mathcal{A})$ выполняет протокол честно, используя свои секретные входные значения x_i, а сообщения, отправляемые злоумышленниками, выбираются согласно алгоритму $\mathcal{A}$. Пусть y_i обозначает выходное значение каждого честного участника P_i, а V_i — $\mathsf{Knowledge}$ участника P_i. Выходом является $(\{V_i : P_i \in \mathrm{corrupt}(\mathcal{A})\}, \{y_i : P_i \notin \mathrm{corrupt}(\mathcal{A})\})$.

— $\mathsf{Ideal}_{\mathcal{F},\mathsf{Sim}}(k, \{x_i : P_i \notin \mathrm{corrupt}(\mathcal{A})\})$: вычисляет множество входных значений для злоумышленников $\{x_i : P_i \in \mathrm{corrupt}(\mathcal{A})\}$. Затем вычисляет $(y_1, \ldots, y_N) = = \mathcal{F}(x_1, \ldots, x_N)$, передаёт $\{y_i : P_i \in \mathrm{corrupt}(\mathcal{A})\}$ в Sim. Обозначим V^* выход Sim. Тогда выходом является $(V^*, \{y_i : P_i \notin \mathrm{corrupt}(\mathcal{A})\})$.

Протокол считается стойким в *Malicious*-модели злоумышленника, если для любого злоумышленника $\mathcal{A}$ существует симулятор Sim ($\mathrm{corrupt}(\mathcal{A}) = \mathrm{corrupt}(\mathsf{Sim})$), такой, что для любых входных значений честных участников распределения $\mathsf{Real}_{\pi,\mathcal{A}}(k, \{x_i : P_i \notin \notin \mathrm{corrupt}(\mathcal{A})\})$ и $\mathsf{Ideal}_{\mathcal{F},\mathsf{Sim}}(k, \{x_i : P_i \notin \mathrm{corrupt}(\mathcal{A})\})$ неотличимы друг от друга.

Доказательство стойкости в Honest-But-Curious-модели злоумышленника

Теорема 1. Протокол 3.1 неотличим от протокола 5.1 для модели злоумышленника *Honest-But-Curious*.

Доказательство. Протокол 5.1 генерирует набор из M случайных кривых. Докажем, что результаты протокола 3.1 неотличимы от случайных, если хотя бы один из игроков действовал честно.

Пусть существует вероятностный алгоритм $\mathcal{A}$, который для входных открытых колод A_1 и A_2 пытается угадать, какая из колод была сгенерирована с помощью протокола 3.1, и выдаёт в качестве результата значение $r \in \{1, 2\}$ — номер открытой колоды. Если для любого вероятностного алгоритма $\mathcal{A}$ при любых действиях злоумышленников вероятность успешно угадать, какая колода была сгенерирована протоколом 3.1, не превышает $1/2 + negl$, где $negl$ — пренебрежимо малая величина, то можно считать, что протоколы 3.1 и 5.1 неотличимы.

Проведём следующий эксперимент. Пусть задан порядок $\mathcal{O}$ в мнимом квадратичном поле, $Cl(\mathcal{O})$ — группа классов идеалов, $\mathscr{E}\ell\ell(\mathcal{O})$ — множество изогенных эллиптических кривых, $\star : Cl(\mathcal{O}) \times \mathscr{E}\ell\ell(\mathcal{O}) \to \mathscr{E}\ell\ell(\mathcal{O})$ — групповое действие и $b \in \{0, 1\}$. Тогда эксперимент $\mathsf{Exp}_1(b)$ с входным значением b выполняется следующим образом. Злоумышленник $\mathcal{A}$ сгенерировал колоду $X = \{x_1, x_2, \dots x_M\}$ и у него есть доступ к оракулу Oracle_b^1, который получает на вход колоду X и в зависимости от значения b вычисляет результат Y следующим образом:

1) если $b = 0$, то $Y := \{[\mathfrak{x}_i] \star x_i : x_i \in X\}$ для $i \in \{1, \dots, M\}$, где $[\mathfrak{x}_i] \xleftarrow{\$} Cl(\mathcal{O})$;
2) если $b = 1$, то $Y := \{y_1, y_2, \dots, y_M\}$, где $y_i \xleftarrow{\$} \mathscr{E}\ell\ell(\mathcal{O})$.

Злоумышленник $\mathcal{A}$ получает Y и выдаёт $b' \in \{0, 1\}$.

Преимущество злоумышленника $\mathcal{A}$ в Exp^1 определяется как

$$\mathsf{Adv}^1(\mathcal{A}) = \left|\Pr\left[\mathcal{A}(\mathsf{Exp}^1(b = 1)) \to 1\right] - \Pr\left[\mathcal{A}(\mathsf{Exp}^1(b = 0)) \to 1\right]\right|.$$

Так как в случае $b = 0$ оракул генерирует случайные значения $[\mathfrak{x}_i]$, взятые из равномерного распределения над $Cl(\mathcal{O})$, то кривая, вычисленная таким образом, также получена из равномерного распределения над $\mathscr{E}\ell\ell(\mathcal{O})$. Это ничем не отличается от результата в случае $b = 1$. Таким образом, отличить эти два случая для злоумышленника $\mathcal{A}$ наверняка невозможно. Тогда найдётся такая пренебрежимо малая функция $negl$, что $\mathsf{Adv}^1(\mathcal{A}) \leqslant negl(\lambda)$, где λ — параметр стойкости.

Очевидно, что в Exp^1 случай Oracle_0^1 соответствует протоколу 3.1 в худшем случае, где все пользователи, кроме одного, являются злоумышленниками в модели *Honest-But-Curious*, а Oracle_1^1 соответствует протоколу 5.1. ■

Следствие 1. Свойство 1 выполняется, пока есть хотя бы один честный игрок, не участвующий в сговоре.

Теорема 2. Если верно предположение о сложности задачи обратного группового действия, то протокол 3.2 неотличим от протокола 5.2 для *Honest-But-Curious*-модели злоумышленника.

Доказательство. Докажем, что перемешивание колоды протоколом 3.2 неотличимо от случайного, если хотя бы один из игроков действует честно.

Пусть существует вероятностный алгоритм $\mathcal{A}$, который для входных закрытых колод B_1 и B_2, которые получены из одной открытой колоды A, пытается угадать, какая из колод была перемешана с помощью протокола 3.2, и выдаёт значение $r \in \{1, 2\}$ — номер закрытой колоды, перемешанной протоколом 3.2. Если для любого алгоритма $\mathcal{A}$ при любых действиях злоумышленников вероятность успешно угадать, какая колода была перемешана протоколом 3.2, не превышает $1/2 + negl$, то можно считать, что протоколы 3.2 и 5.2 неотличимы.

Пусть только игрок P_j действует честно, а за всех остальных игроков действует злоумышленник. Пусть игрок P_j получает от игрока P_{j-1} (злоумышленника) частично перемешанную колоду $B^{(j-1)}$. Далее в протоколе 3.2 пользователь P_j выбирает случайную перестановку $S_i : \{1, \dots, M\} \to \{1, \dots, M\}$ и с помощью неё и своего секретного ключа $[\mathfrak{y}_j]$ получает новую колоду $B^{(j)}$:

$$B^{(j)} := ([\mathfrak{y}_j] \star b^{(j-1)}_{S_j(1)}, [\mathfrak{y}_j] \star b^{(j-1)}_{S_j(2)}, \dots, [\mathfrak{y}_j] \star b^{(j-1)}_{S_j(M)}).$$

Далее колода передаётся злоумышленнику. Единственным способом для злоумышленника найти соответствие между картами колод $B^{(j)}$ и $B^{(j-1)}$ является решение задачи GAIP. Тогда преимущество Adv^2 злоумышленника $\mathcal{A}$ равно вероятности того, что

$\mathcal{A}$ решит задачу GAIP за разумное время (время проведения игры). Так как GAIP считается сложной задачей, найдётся пренебрежимо малая функция $negl$, такая, что $\mathsf{Adv}^2 \leqslant negl(\lambda)$. Таким образом, перемешанная колода в итоге будет неотличима от случайной. ■

Следствие 2. Свойство 2 выполняется, пока есть хотя бы один честный игрок, не участвующий в сговоре, так как для того, чтобы замешать карты в нужном порядке, злоумышленнику необходимо решить задачу GAIP.

Теорема 3. Если верно предположение о сложности задачи обратного группового действия, то в протоколе 3.3 никто, кроме игрока, которому выдаётся карта, не сможет узнать содержимое карты для *Honest-But-Curious*-модели злоумышленника.

Доказательство. Пусть есть закрытая карта b и соответствующая ей открытая карта a. Тогда между ними есть зависимость

$$b = [\mathfrak{y}_1] \star [\mathfrak{y}_2] \star \cdots \star [\mathfrak{y}_N] \star a,$$

где $[\mathfrak{y}_1], [\mathfrak{y}_2], \ldots, [\mathfrak{y}_N]$ — маски игроков.

При выдаче карты игроку P_k остальные игроки последовательно снимают маски:

$$\begin{aligned}
c^{(1)} &= [\mathfrak{y}_2] \star \cdots \star [\mathfrak{y}_N] \star a,\\
c^{(2)} &= [\mathfrak{y}_3] \star \cdots \star [\mathfrak{y}_N] \star a,\\
&\cdots\\
c^{(k-1)} &= [\mathfrak{y}_k] \star \cdots \star [\mathfrak{y}_N] \star a,\\
c^{(k+1)} &= [\mathfrak{y}_k] \star [\mathfrak{y}_{k+2}] \star \cdots \star [\mathfrak{y}_N] \star a,\\
&\cdots\\
c^{(N)} &= [\mathfrak{y}_k] \star a.
\end{aligned}$$

В конце игрок P_k снимает свою маску $[\mathfrak{y}_k]$ и узнаёт открытую карту a.

В худшем случае, если все остальные игроки объединят полученную в ходе протокола информацию, а именно $b, c^{(1)}, c^{(2)}, \ldots, c^{(N)}$, они всё равно не смогут узнать открытую карту a за время игры, так как для этого необходимо решить задачу обратного группового действия. ■

Необходимо отметить, что протоколы 3.3 и 5.3 неотличимы друг от друга для злоумышленника $\mathcal{A}$, так как при одинаковых входных параметрах они выдают одну и ту же открытую карту.

4.2. Стойкость протоколов с валидацией

Протоколы 4.1, 4.2 и 4.3 (см. Приложение 1) отличаются от протоколов 5.1, 5.2 и 5.3 соответственно наличием верификации полученных пользователями значений с помощью протоколов доказательства с нулевым разглашением. Докажем, что протоколы ZKP_1, ZKP_2 и ZKP_3 (см. Приложение 2) являются протоколами с нулевым разглашением. Для доказательства воспользуемся понятием Σ-протокола.

Σ-протокол [37] — вид интерактивного доказательства с нулевым разглашением, в котором участвуют две стороны (доказывающий и проверяющий) и который состоит из трёх раундов:

1) Свидетельство: доказывающий вычисляет некоторое свидетельство на основе сгенерированного случайного значения и отправляет его проверяющему.

2) Запрос: проверяющий генерирует случайный запрос из допустимого набора и отправляет его доказывающему.
3) Ответ: доказывающий вычисляет ответ на основе секрета, свидетельства и запроса и отправляет ответ проверяющему.

Проверяющий либо принимает ответ, либо не принимает.

Σ-протокол должен удовлетворять трём свойствам:

1) Полнота. Если доказывающий и проверяющий запускают протокол и честно следуют ему, а доказывающий действительно знает секрет, то проверяющий всегда примет доказательство.
2) Корректность. Если доказывающий действительно знает секрет, то он всегда сможет убедить в этом проверяющего. Чтобы доказать это свойство, необходимо показать, что, зная передаваемую информацию для разных запросов и одного и того же свидетельства, можно найти секрет. Таким образом, свойство корректности гарантирует, что доказывающий знает секрет, а не угадывает его.
3) Нулевое разглашение для честного проверяющего (Honest Verifier Zero-Knowledge, HVZK). Проверяющий, честно следующий протоколу, не может узнать ничего о секрете доказывающего.

Доказав, что представленные в работе протоколы удовлетворяют свойствам Σ-протоколов, мы установим, что они удовлетворяют свойствам протоколов с нулевым разглашением.

Теорема 4. Протокол ZKP_1 является Σ-протоколом и обладает свойствами полноты, корректности и HVZK.

Доказательство.

1) Полнота. Предположим, что протокол выполняется честно. Пусть доказывающий выбрал $[\mathfrak{b}] \xleftarrow{\$} Cl(\mathcal{O})$ и вычислил кривую E.

Если проверяющий отправляет $c = 0$, то получает в ответ $[\mathfrak{r}] = [\mathfrak{b}]$ и вычисляет $E' = [\mathfrak{b}] \star E_1 = E$.

Если проверяющий отправляет $c = 1$, то получает в ответ $[\mathfrak{r}] = [\mathfrak{b}] \cdot [\mathfrak{x}]^{-1}$ и вычисляет

$$E' = [\mathfrak{b}] \cdot [\mathfrak{x}]^{-1} \star E_2 = [\mathfrak{b}] \cdot [\mathfrak{x}]^{-1} \cdot [\mathfrak{x}] \star E_1 = [\mathfrak{b}] \star E_1 = E.$$

В обоих случаях проверяющий получает корректный результат и протокол возвращает значение ИСТИНА. Таким образом, свойство полноты выполняется.

2) Корректность. Пусть даны два набора $(E, 0, [\mathfrak{r}_1])$ и $(E, 1, [\mathfrak{r}_2])$, которые были приняты проверяющим. Тогда $E = [\mathfrak{r}_1] \star E_1 = [\mathfrak{r}_2] \star E_2$. Отсюда следует, что $E = [\mathfrak{r}_1] \star E_1 = = [\mathfrak{r}_2] \cdot [\mathfrak{x}] \star E_1$. Следовательно, секрет может быть извлечён как $[\mathfrak{x}] = [\mathfrak{r}_1] \cdot [\mathfrak{r}_2]^{-1}$. Таким образом, свойство корректности выполняется.

3) Нулевое разглашение для честного проверяющего. Пусть проверяющий честно следует протоколу; $\mathcal{S}$ — симулятор, получающий на вход (E_1, E_2, c) и возвращающий $(E, c, [\mathfrak{r}])$ (при этом $\mathcal{S}$ не знает секрет $[\mathfrak{x}]$). Итоговая E вычисляется как

$$E = [\mathfrak{r}] \star E_{c+1}.$$

Можно заметить, что и в случае проведения самого протокола, и в случае работы симулятора $\mathcal{S}$ значение $[\mathfrak{r}]$ имеет равномерное распределение, поэтому наборы передаваемых данных в обоих случаях будут неотличимы. Таким образом, свойство нулевого разглашения для честного проверяющего выполняется.

Итак, протокол ZKP_1 является Σ-протоколом и, следовательно, протоколом с нулевым разглашением. ■

Теорема 5. Протокол ZKP_2 является Σ-протоколом и обладает свойствами полноты, корректности и HVZK.

Доказательство.

1) Полнота. Предположим, что протокол выполняется честно. На вход поступают два набора кривых $B^{(1)} = \{B_1^{(1)}, B_2^{(1)}, \ldots, B_M^{(1)}\}$ и $B^{(2)} = \{B_1^{(2)}, B_2^{(2)}, \ldots, B_M^{(2)}\}$, где $B_j^{(i)} \in \in \mathscr{E}\ell\ell(\mathcal{O})$ для $i \in \{1,2\}$ и $j \in \{1,\ldots,M\}$. Пусть доказывающий выбрал $[\mathfrak{b}] \xleftarrow{\$} Cl(\mathcal{O})$ и случайную перестановку S_b и с их помощью вычислил кривую b_0^b и набор кривых B^b. Если проверяющий отправляет $c = 0$, то получает в ответ $S_r = S_b$, $[\mathfrak{r}] = [\mathfrak{b}]$ и вычисляет

$$B' = \{[\mathfrak{r}] \star B_{S_r(i)}^{(c+1)} : i \in \{1,\ldots,M\}\} = \{[\mathfrak{b}] \star B_{S_b(i)}^{(1)} : i \in \{1,\ldots,M\}\} = B^b,$$
$$b_0' = [\mathfrak{r}] \star b_0^{(c+1)} = [\mathfrak{b}] \star b_0^{(1)} = b_0^b.$$

Если проверяющий отправляет $c = 1$, то получает в ответ $S_r = S^{-1}(S_b)$, $[\mathfrak{r}] = [\mathfrak{b}] \cdot [\mathfrak{x}]^{-1}$ и вычисляет

$$B' = \{[\mathfrak{r}] \star B_{S_r(i)}^{(c+1)} : i \in \{1,\ldots,M\}\} = \{([\mathfrak{b}] \cdot [\mathfrak{x}]^{-1}) \star B_{S^{-1}(S_b(i))}^{(2)} : i \in \{1,\ldots,M\}\} =$$
$$= \{([\mathfrak{b}] \cdot [\mathfrak{x}]^{-1} \cdot [\mathfrak{x}]) \star B_{S(S^{-1}(S_b(i)))}^{(1)} : i \in \{1,\ldots,M\}\} = \{[\mathfrak{b}] \star B_{S_b(i)}^{(1)} : i \in \{1,\ldots,M\}\} = B^b,$$
$$b_0' = [\mathfrak{r}] \star b_0^{(c+1)} = [\mathfrak{b}] \cdot [\mathfrak{x}]^{-1} \star b_0^{(2)} = [\mathfrak{b}] \cdot [\mathfrak{x}]^{-1} \cdot [\mathfrak{x}] \star b_0^{(1)} = b_0^b.$$

В обоих случаях проверяющий получает корректный результат и протокол возвращает значение ИСТИНА. Таким образом, свойство полноты выполняется.

2) Корректность. Пусть даны два набора $(B^b, b_0^b, 0, [\mathfrak{r}_1], S_{r_1})$ и $(B^b, b_0^b, 1, [\mathfrak{r}_2], S_{r_2})$, которые были приняты проверяющим. Тогда

$$b_0^b = [\mathfrak{r}_1] \star b_0^{(1)} = [\mathfrak{r}_2] \star b_0^{(2)},$$
$$B^b = \{[\mathfrak{r}_1] \star B_{S_{r_1}(i)}^{(1)} : i \in \{1,\ldots,M\}\} = \{[\mathfrak{r}_2] \star B_{S_{r_2}(i)}^{(2)} : i \in \{1,\ldots,M\}\}.$$

Отсюда следует, что

$$b_0^b = [\mathfrak{r}_1] \star b_0^{(1)} = [\mathfrak{r}_2] \cdot [\mathfrak{x}] \star b_0^{(1)},$$
$$B^b = \{[\mathfrak{r}_1] \star B_{S_{r_1}(i)}^{(1)} : i \in \{1,\ldots,M\}\} = \{[\mathfrak{r}_2] \cdot [\mathfrak{x}] \star B_{S(S_{r_2}(i))}^{(1)} : i \in \{1,\ldots,M\}\}.$$

Следовательно, секреты могут быть извлечены как $[\mathfrak{x}] = [\mathfrak{r}_1] \cdot [\mathfrak{r}_2]^{-1}$, $S = S_{r_1}(S_{r_2}^{-1})$.

3) Нулевое разглашение для честного проверяющего. Пусть проверяющий честно следует протоколу; $\mathcal{S}$ — симулятор, получающий на вход $(B^{(1)}, B^{(2)}, b_0^{(1)}, b_0^{(2)}, c)$ и возвращающий $(B^b, b_0^b, c, [\mathfrak{r}], S_r)$ (при этом $\mathcal{S}$ не знает секрет $[\mathfrak{x}], S$). Итоговые значения B^b и b_0^b вычисляются как

$$B^b = \{[\mathfrak{r}] \star B_{S_r(i)}^{(c+1)} : i \in \{1,\ldots,M\}\}, \quad b_0^b = [\mathfrak{r}] \star b_0^{(c+1)}.$$

Можно заметить, что и в случае проведения самого протокола, и в случае работы симулятора $\mathcal{S}$ значения $[\mathfrak{r}]$ и S_r имеют равномерное распределение, поэтому наборы передаваемых данных в обоих случаях будут неотличимы. Таким образом, свойство нулевого разглашения для честного проверяющего выполняется.

Необходимые свойства выполняются, поэтому протокол ZKP_2 является Σ-протоколом и, следовательно, протоколом с нулевым разглашением. ■

Теорема 6. Протокол ZKP_3 является Σ-протоколом и обладает свойствами полноты, корректности и HVZK.

Доказательство.

1) Полнота. Предположим, что протокол выполняется честно. Пусть доказывающий выбрал $[\mathfrak{b}] \xleftarrow{\$} Cl(\mathcal{O})$ и вычислил кривые E_1 и E_2.

Если проверяющий отправляет $c = 0$, то получает в ответ $[\mathfrak{r}] = [\mathfrak{b}]$ и вычисляет $E'_1 = [\mathfrak{b}] \star E_{11} = E_1$ и $E'_2 = [\mathfrak{b}] \star E_{21} = E_2$.

Если проверяющий отправляет $c = 1$, то получает в ответ $[\mathfrak{r}] = [\mathfrak{b}] \cdot [\mathfrak{x}]^{-1}$ и вычисляет

$$E'_1 = [\mathfrak{b}] \cdot [\mathfrak{x}]^{-1} \star E_{12} = [\mathfrak{b}] \cdot [\mathfrak{x}]^{-1} \cdot [\mathfrak{x}] \star E_{11} = [\mathfrak{b}] \star E_{11} = E_1,$$
$$E'_2 = [\mathfrak{b}] \cdot [\mathfrak{x}]^{-1} \star E_{22} = [\mathfrak{b}] \cdot [\mathfrak{x}]^{-1} \cdot [\mathfrak{x}] \star E_{21} = [\mathfrak{b}] \star E_{21} = E_2.$$

В обоих случаях проверяющий получает корректный результат и протокол возвращает значение ИСТИНА. Таким образом, свойство полноты выполняется.

2) Корректность. Пусть даны два набора $(E_1, E_2, 0, [\mathfrak{r}_1])$ и $(E_1, E_2, 1, [\mathfrak{r}_2])$, которые были приняты проверяющим. Тогда

$$E_1 = [\mathfrak{r}_1] \star E_{11} = [\mathfrak{r}_2] \star E_{12}, \quad E_2 = [\mathfrak{r}_1] \star E_{21} = [\mathfrak{r}_2] \star E_{22}.$$

Отсюда следует, что $E_1 = [\mathfrak{r}_1] \star E_{11} = [\mathfrak{r}_2] \cdot [\mathfrak{x}] \star E_{11}$, $E_2 = [\mathfrak{r}_1] \star E_{21} = [\mathfrak{r}_2] \cdot [\mathfrak{x}] \star E_{21}$. Следовательно, секрет может быть извлечён как $[\mathfrak{x}] = [\mathfrak{r}_1] \cdot [\mathfrak{r}_2]^{-1}$. Таким образом, свойство корректности выполняется.

3) Нулевое разглашение для честного проверяющего. Пусть проверяющий честно следует протоколу; $\mathcal{S}$ — симулятор, получающий $(E_{11}, E_{12}, E_{21}, E_{22}, c)$ и возвращающий $(E_1, E_2, c, [\mathfrak{r}])$ (при этом $\mathcal{S}$ не знает секрет $[\mathfrak{x}]$). Итоговые E_1, E_2 вычисляются как $E_1 = [\mathfrak{r}] \star E_{1(c+1)}$, $E_2 = [\mathfrak{r}] \star E_{2(c+1)}$. Можно заметить, что и в случае проведения самого протокола, и в случае работы симулятора $\mathcal{S}$ значение $[\mathfrak{r}]$ имеет равномерное распределение, поэтому наборы передаваемых данных в обоих случаях будут неотличимы. Таким образом, свойство нулевого разглашения для честного проверяющего выполняется.

Необходимые свойства выполняются, поэтому протокол ZKP_3 является Σ-протоколом и, следовательно, протоколом с нулевым разглашением. ■

Теорема 7. Если верно предположение о сложности задачи обратного группового действия, то протоколы 4.1, 4.2 и 4.3 неотличимы от протоколов 5.1, 5.2 и 5.3 соответственно для *Malicious*-модели злоумышленника.

Доказательство. Протоколы 4.1–4.3 отличаются от протоколов 5.1–5.3 наличием верификации полученных пользователями значений с помощью протоколов доказательства с нулевым разглашением. В теоремах 4–6 доказано, что протоколы ZKP_1, ZKP_2 и ZKP_3 являются Σ-протоколами, то есть они не разглашают никакой информации о секрете. Если при проверке доказательства будет выявлено нарушение, то протокол будет остановлен. Таким образом, злоумышленник не сможет действовать никак иначе, кроме как следовать протоколу, а значит, он будет действовать как *Honest-But-Curious* злоумышленник, поэтому все доводы, приведённые в теоремах 1–3, остаются достоверными и для протоколов 4.1, 4.2 и 4.3. Вследствие этого работа данных протоколов неотличима от работы протоколов 5.1, 5.2 и 5.3 соответственно. ■

5. Быстродействие протокола

Описанный протокол реализован на языке программирования C [38] с использованием сторонней библиотеки faster-csidh [39]. Для оценки быстродействия замерено

время подготовки колоды, тасования колоды и выдачи карты с валидацией и без. Все замеры производились на персональном компьютере с процессором AMD Ryzen 7 5800H.

На рис. 1 показана зависимость от количества игроков времени работы протоколов без валидации для колоды из 52 карт.

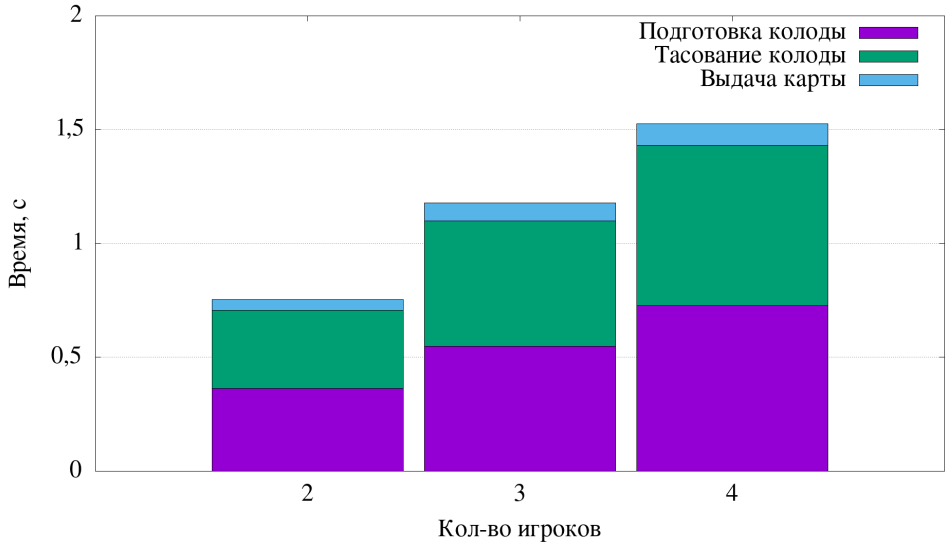

Рис. 1. Зависимость времени работы протоколов без валидации от количества игроков

На рис. 2 показана зависимость от количества игроков времени работы протоколов с валидацией для колоды из 52 карт и параметром стойкости 20 (под параметром стойкости понимается количество итераций ZKP_1, ZKP_2, ZKP_3). Так как шанс успешного обмана для каждой итерации протокола доказательства с нулевым разглашением равен $1/2$, параметр стойкости 20 обеспечивает общий шанс обмана 2^{-20}. Выбор такого уровня стойкости обусловлен его оптимальностью: при параметре стойкости 20 протокол работает за приемлемое время и за время проведения игры пользователи не смогут нарушить стойкость протокола.

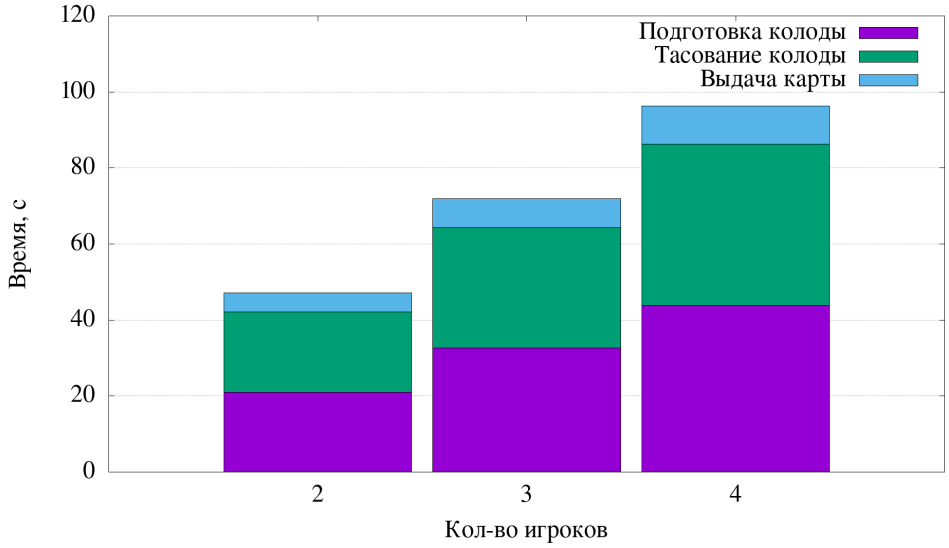

Рис. 2. Зависимость времени работы протоколов с валидацией от количества игроков

Можно заметить, что при добавлении валидации время выполнения протоколов возрастает в несколько раз, поскольку групповое действие является затратной операцией.

На рис. 3 показана зависимость от параметра стойкости времени работы протоколов с валидацией для колоды из 52 карт и для трёх игроков.

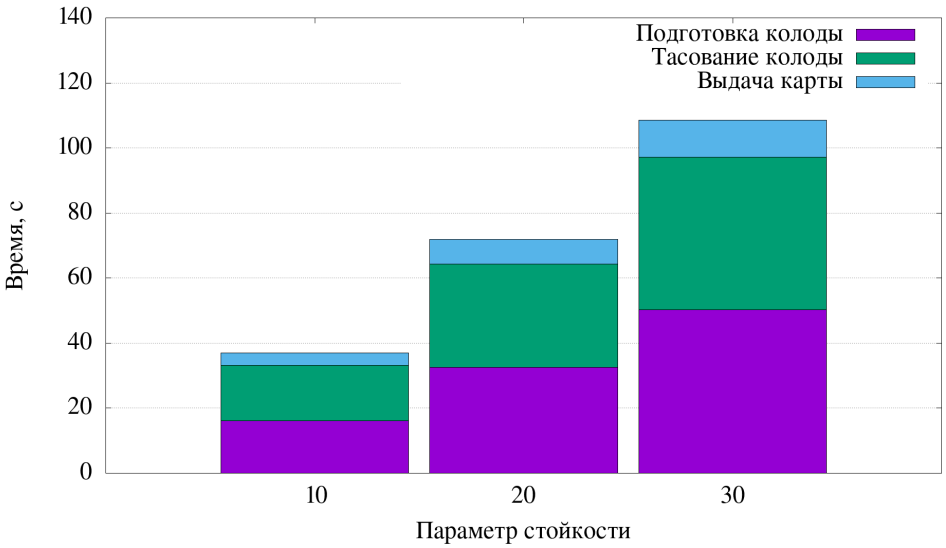

Рис. 3. Зависимость времени работы протоколов от параметра стойкости с валидацией

Замеры времени выполнения протокола с валидацией показывают, что в среднем при параметре стойкости 20 для создания перетасованной колоды требуется 21,42 с на одного игрока, что позволяет применять данное решение на практике. Решение, представленное в [33], при таком же параметре стойкости требовало 28,78 с на игрока для создания открытой колоды. Конечно, следует учитывать, что работа [33] написана в 2012 г., а с тех пор мощность среднего персонального компьютера заметно возросла.

Затраты по памяти представлены в таблице, где N — количество игроков, а λ — параметр стойкости.

Затраты памяти

Объект	Размер хранимых данных, байт
Карта	64
Колода карт	$64\,N$
Секретная маска карты	74
Протокол	**Размер передаваемых данных, байт**
ZKP_1 Commit	$(64+74)(N+1)\,\lambda$
ZKP_1 Responce	$74(N+1)\,\lambda$
ZKP_2 Commit	$(64+74)(N+1)\,\lambda$
ZKP_2 Responce	$(74+(4+64)N)\,\lambda$
ZKP_3 Commit	$(2\cdot 64+74)\,\lambda$
ZKP_3 Responce	$74\,\lambda$

Заключение

В работе представлен постквантовый протокол ментального покера, основанный на задаче поиска изогений между суперсингулярными эллиптическими кривыми. Предложено два варианта протокола: без валидации (где подразумевается, что игроки будут строго следовать протоколу, но могут «подглядывать», если у них будет такая

возможность) и с валидацией (где любое нарушение протокола может быть обнаружено). Для каждого из представленных вариантов доказана безопасность в *Honest-But-Curious*- и *Malicious*-моделях злоумышленника для классического и квантового вычислителей, получены экспериментальные оценки по времени и по памяти.

Экспериментальные результаты показали, что время выполнения протокола, особенно без валидации, позволяет применять его на практике. Создание перетасованной колоды из 52 карт занимает около 21,42 с на игрока. Тем не менее для широкого применения потребуется оптимизация протокола с целью сокращения времени выполнения, особенно в режиме с валидацией, так как сложные криптографические вычисления требуют значительных ресурсов.

Основным преимуществом представленного протокола является устойчивость перед атаками на квантовом компьютере. В качестве дальнейших исследований стоит задача по оптимизации протокола по времени.

Помимо времени выполнения, стоит отметить требования протокола к памяти, которые подробно исследованы в ходе работы. Для каждого игрока объём данных включает 64 байта на карту и 74 байта на секретную маску карты. Для протоколов доказательства с нулевым разглашением требуются дополнительные ресурсы памяти.

Таким образом, представленный протокол ментального покера является квантово-устойчивым, гибким, эффективным. Перспективы дальнейшего развития включают оптимизацию вычислительных затрат и исследование возможностей применения подобных подходов в прикладных задачах.

ЛИТЕРАТУРА

1. *Shamir A., Rivest R. L., and Adleman L. M.* Mental Poker / D. A. Klarner (eds). The Mathematical Gardner. Boston: Springer, 1981. P. 37–43.
2. *Lipton R.* How to cheat at mental poker // Proc. AMS Short Course on Cryptography. 1981. `https://cir.nii.ac.jp/crid/1570854175390364160`.
3. *Coppersmith D.* Cheating at mental poker // LNCS. 1986. V. 218. P. 104–107.
4. *Barany I. and Furedi Z.* Mental poker with three or more players // Inf. Control. 1984. V. 59. No. 1–3. P. 84–93.
5. *Jabbar Z. S. and Aboud S. J.* An efficient poker protocol for shuffling and dealing cards // Intern. J. Innovative Technol. Exploring Engin. 2019. V. 8. No. 12. P. 2175–2179.
6. *Aranha D. F., Baum C., Gjøsteen K., and Silde T.* Verifiable Mix-Nets and Distributed Decryption for Voting from Lattice-Based Assumptions. Cryptology ePrint Archive. 2022. Paper 2022/422. `https://eprint.iacr.org/2022/422`.
7. *Haines T., Goré R., and Sharma B.* Did you mix me? Formally verifying verifiable mix nets in electronic voting // Proc. SP'2021. San Francisco, CA, USA, 2021. P. 1748–1765.
8. *Lin K., Wang W., Zhao C.-A., and Zhao Y.* π-signHD: A New Structure for the SQIsign Family with Flexible Applicability. Cryptology ePrint Archive. 2024. Paper 2024/1404. `https://eprint.iacr.org/2024/1404`.
9. *Nakagawa K. and Onuki H.* SQIsign2D-East: A New Signature Scheme Using 2-dimensional Isogenies. Cryptology ePrint Archive. 2024. Paper 2024/771. `https://eprint.iacr.org/2024/771`.
10. *Borin G., Lai Y.-F., and Leroux A.* Erebor and Durian: Full Anonymous Ring Signatures from Quaternions and Isogenies. Cryptology ePrint Archive. 2024. Paper 2024/1185. `https://eprint.iacr.org/2024/1185`.

11. *Duparc M. and Fouotsa T. B.* SQIPrime: A Dimension 2 Variant of SQISignHD with Non-Smooth Challenge Isogenies. Cryptology ePrint Archive. 2024. Paper 2024/773. https://eprint.iacr.org/2024/773.
12. *Levin S. and Pedersen R.* Faster Proofs and VRFs from Isogenies. Cryptology ePrint Archive. 2024. Paper 2024/1626. https://eprint.iacr.org/2024/1626.
13. *El Baraka M. and Ezzouak S.* Isogeny-Based Secure Voting Systems for Large-Scale Elections. Cryptology ePrint Archive. 2024. Paper 2024/1472. https://eprint.iacr.org/2024/1472.
14. *Moriya T.* IS-CUBE: An Isogeny-Based Compact KEM Using a Boxed SIDH Diagram. Cryptology ePrint Archive. 2023. Paper 2023/1506. https://eprint.iacr.org/2023/1506.
15. *De Feo L., Fouotsa T. B., Kutas P., et al.* SCALLOP: Scaling the CSI-FiSh. Cryptology ePrint Archive. 2023. Paper 2023/058. https://eprint.iacr.org/2023/058.
16. *Chen M., Leroux A., and Panny L.* SCALLOP-HD: Group Action from 2-dimensional Isogenies. Cryptology ePrint Archive. 2023. Paper 2023/1488. https://eprint.iacr.org/2023/1488.
17. *Stolbunov A.* Cryptographic Schemes Based on Isogenies. https://ntnuopen.ntnu.no/ntnu-xmlui/bitstream/handle/11250/262577/529395_FULLTEXT01.pdf. 2012.
18. *Sotakova J.* Elliptic Curves, Isogenies, and Endomorphism Rings. https://janasotakova.eu/writings/ANTS_school_exposition.pdf. 2020.
19. *Velu J.* Isogenies entre courbes elliptiques // Comptes-Rendus de l'Academie des Sciences. 1971. V. 273. P. 238–241.
20. *Атья М., Макдональд И.* Введение в коммутативную алгебру. М.: Мир, 1972.
21. *Deuring M.* Die Typen der Multiplikatorenringe elliptischer Funktionenkörper // Ach. Math. Sem. Hab. 1941. P. 197–272.
22. *Eriksen J. K., Panny L., Sotáková J., and Veroni M.* Deuring for the People: Supersingular Elliptic Curves with Prescribed Endomorphism Ring in General Characteristic. Cryptology ePrint Archive. 2023. Paper 2023/106. https://eprint.iacr.org/2023/106.
23. *Conrad K.* Ideal Classes and the Kronecker Bound. https://kconrad.math.uconn.edu/blurbs/gradnumthy/classgroupKronecker.pdf.
24. *Alamati N., De Feo L., Montgomery H., and Patranabis S.* Cryptographic Group Actions and Applications. Cryptology ePrint Archive. 2020. Paper 2020/1188. https://eprint.iacr.org/2020/1188.
25. *Ростовцев А. Г., Маховенко Е. Б.* Теоретическая криптография. СПб.: АНО НПО «Профессионал», 2005.
26. *Beullens W., Kleinjung T., and Vercauteren F.* CSI-FiSh: efficient isogeny based signatures through class group computations. Cryptology ePrint Archive. 2019. Paper 2019/498. https://eprint.iacr.org/2019/498.
27. *Castryck W., Lange T., Martindale C., et al.* CSIDH: an efficient post-quantum commutative group action. Cryptology ePrint Archive. 2018. Paper 2018/383. https://eprint.iacr.org/2018/383.
28. *Campos F., Chavez-Saab J., Chi-Dominguez J.-J., et al.* Optimizations and Practicality of High-Security CSIDH. Cryptology ePrint Archive. 2023. Paper 2023/793. https://eprint.iacr.org/2023/793.
29. *Kuperberg G.* A subexponential-time quantum algorithm for the dihedral hidden subgroup problem // SIAM J. Computing. 2005. V. 35. No. 1. P. 170–188.
30. *Golle P.* Dealing cards in poker games // Proc. ITCC'05. Las Vegas, NV, USA, 2005. V. 1. P. 506–511.
31. *Castella-Roca J.* Contributions to Mental Poker. https://ddd.uab.cat/pub/tesis/2005/tdx-0131106-193157/jcr1de1.pdf. 2006.

32. *Barnett A. and Smart N. P.* Mental poker revisited // LNCS. 2003. V. 2898. P. 370–383.
33. *Wei T.-J. and Wang L.-C.* A fast mental poker protocol // J. Math. Cryptology. 2012. V. 6. No. 1. P. 39–68.
34. *Chaum D. and Pedersen T. P.* Wallet databases with observers // LNCS. 1993. V. 740. P. 89–105.
35. *Canetti R.* Universally Composable Security: A New Paradigm for Cryptographic Protocols. Cryptology ePrint Archive. 2000. Paper 2000/067. https://eprint.iacr.org/2000/067.
36. Secure Computation. https://www.cs.jhu.edu/~abhishek/classes/CS600-642-442-Fall2018/L12.pdf. 2018.
37. *Damgård I.* On Σ-protocols. https://www.cs.au.dk/~ivan/Sigma.pdf. 2010.
38. Isogeny Mental Card Game. https://github.com/IvanIoganson/isogeny_mental_card_game.git. 2024.
39. Faster-csidh. https://github.com/herumi/faster-csidh.git. 2023.

REFERENCES

1. *Shamir A., Rivest R. L., and Adleman L. M.* Mental Poker. D. A. Klarner (eds). The Mathematical Gardner. Boston, MA, Springer, 1981, pp. 37–43.
2. *Lipton R.* How to cheat at mental poker. Proc. AMS Short Course on Cryptography, 1981, https://cir.nii.ac.jp/crid/1570854175390364160.
3. *Coppersmith D.* Cheating at mental poker. LNCS, 1986, vol. 218, pp. 104–107.
4. *Barany I. and Furedi Z.* Mental poker with three or more players. Inf. Control, 1984, vol. 59, no. 1–3, pp. 84–93.
5. *Jabbar Z. S. and Aboud S. J.* An efficient poker protocol for shuffling and dealing cards. Intern. J. Innovative Technol. Exploring Engin., 2019, vol. 8, no. 12, pp. 2175–2179.
6. *Aranha D. F., Baum C., Gjøsteen K., and Silde T.* Verifiable Mix-Nets and Distributed Decryption for Voting from Lattice-Based Assumptions. Cryptology ePrint Archive, 2022, Paper 2022/422, https://eprint.iacr.org/2022/422.
7. *Haines T., Goré R., and Sharma B.* Did you mix me? Formally verifying verifiable mix nets in electronic voting. Proc. SP'2021, San Francisco, CA, USA, 2021, pp. 1748–1765.
8. *Lin K., Wang W., Zhao C.-A., and Zhao Y.* π-signHD: A New Structure for the SQIsign Family with Flexible Applicability. Cryptology ePrint Archive, 2024, Paper 2024/1404, https://eprint.iacr.org/2024/1404.
9. *Nakagawa K. and Onuki H.* SQIsign2D-East: A New Signature Scheme Using 2-dimensional Isogenies. Cryptology ePrint Archive, 2024, Paper 2024/771, https://eprint.iacr.org/2024/771.
10. *Borin G., Lai Y.-F., and Leroux A.* Erebor and Durian: Full Anonymous Ring Signatures from Quaternions and Isogenies. Cryptology ePrint Archive, 2024, Paper 2024/1185, https://eprint.iacr.org/2024/1185.
11. *Duparc M. and Fouotsa T. B.* SQIPrime: A Dimension 2 Variant of SQISignHD with Non-Smooth Challenge Isogenies. Cryptology ePrint Archive, 2024, Paper 2024/773, https://eprint.iacr.org/2024/773.
12. *Levin S. and Pedersen R.* Faster Proofs and VRFs from Isogenies. Cryptology ePrint Archive, 2024, Paper 2024/1626, https://eprint.iacr.org/2024/1626.
13. *El Baraka M. and Ezzouak S.* Isogeny-Based Secure Voting Systems for Large-Scale Elections. Cryptology ePrint Archive, 2024, Paper 2024/1472, https://eprint.iacr.org/2024/1472.
14. *Moriya T.* IS-CUBE: An Isogeny-Based Compact KEM Using a Boxed SIDH Diagram. Cryptology ePrint Archive. 2023. Paper 2023/1506. https://eprint.iacr.org/2023/1506.

15. *De Feo L., Fouotsa T. B., Kutas P., et al.* SCALLOP: Scaling the CSI-FiSh. Cryptology ePrint Archive, 2023, Paper 2023/058, https://eprint.iacr.org/2023/058.
16. *Chen M., Leroux A., and Panny L.* SCALLOP-HD: Group Action from 2-dimensional Isogenies. Cryptology ePrint Archive, 2023, Paper 2023/1488, https://eprint.iacr.org/2023/1488.
17. *Stolbunov A.* Cryptographic Schemes Based on Isogenies. https://ntnuopen.ntnu.no/ntnu-xmlui/bitstream/handle/11250/262577/529395_FULLTEXT01.pdf, 2012.
18. *Sotakova J.* Elliptic Curves, Isogenies, and Endomorphism Rings. https://janasotakova.eu/writings/ANTS_school_exposition.pdf, 2020.
19. *Velu J.* Isogenies entre courbes elliptiques. Comptes-Rendus de l'Academie des Sciences, 1971, vol. 273, pp. 238–241.
20. *Atiyah M. F. and MacDonald I. G.* Introduction To Commutative Algebra. Addison-Wesley Publishing Company, Inc., 1969.
21. *Deuring M.* Die Typen der Multiplikatorenringe elliptischer Funktionenkörper. Ach. Math. Sem. Hab., 1941, pp. 197–272.
22. *Eriksen J. K., Panny L., Sotáková J., and Veroni M.* Deuring for the People: Supersingular Elliptic Curves with Prescribed Endomorphism Ring in General Characteristic. Cryptology ePrint Archive, 2023, Paper 2023/106, https://eprint.iacr.org/2023/106.
23. *Conrad K.* Ideal Classes and the Kronecker Bound. https://kconrad.math.uconn.edu/blurbs/gradnumthy/classgroupKronecker.pdf.
24. *Alamati N., De Feo L., Montgomery H., and Patranabis S.* Cryptographic Group Actions and Applications. Cryptology ePrint Archive, 2020, Paper 2020/1188, https://eprint.iacr.org/2020/1188.
25. *Rostovtsev A. G. and Makhovenko E. B.* Teoreticheskaya kriptografiya [Theoretical Cryptography]. Saint Petersburg, Professional Publ., 2005. (in Russian)
26. *Beullens W., Kleinjung T., and Vercauteren F.* CSI-FiSh: efficient isogeny based signatures through class group computations. Cryptology ePrint Archive, 2019, Paper 2019/498, https://eprint.iacr.org/2019/498.
27. *Castryck W., Lange T., Martindale C., et al.* CSIDH: an efficient post-quantum commutative group action. Cryptology ePrint Archive, 2018, Paper 2018/383, https://eprint.iacr.org/2018/383.
28. *Campos F., Chavez-Saab J., Chi-Dominguez J.-J., et al.* Optimizations and Practicality of High-Security CSIDH. Cryptology ePrint Archive, 2023, Paper 2023/793, https://eprint.iacr.org/2023/793.
29. *Kuperberg G.* A subexponential-time quantum algorithm for the dihedral hidden subgroup problem. SIAM J. Computing, 2005, vol. 35, no. 1, pp. 170–188.
30. *Golle P.* Dealing cards in poker games. Proc. ITCC'05, Las Vegas, NV, USA, 2005, vol. 1, pp. 506–511.
31. *Castella-Roca J.* Contributions to Mental Poker. https://ddd.uab.cat/pub/tesis/2005/tdx-0131106-193157/jcr1de1.pdf, 2006.
32. *Barnett A. and Smart N. P.* Mental poker revisited. LNCS, 2003, vol. 2898, pp. 370–383.
33. *Wei T.-J. and Wang L.-C.* A fast mental poker protocol. J. Math. Cryptology, 2012, vol. 6, no. 1, pp. 39–68.
34. *Chaum D. and Pedersen T. P.* Wallet databases with observers. LNCS, 1993, vol. 740, pp. 89–105.
35. *Canetti R.* Universally Composable Security: A New Paradigm for Cryptographic Protocols. Cryptology ePrint Archive, 2000, Paper 2000/067, https://eprint.iacr.org/2000/067.

36. Secure Computation. `https://www.cs.jhu.edu/~abhishek/classes/CS600-642-442-Fall2018/L12.pdf`, 2018.
37. *Damgård I.* On Σ-protocols. `https://www.cs.au.dk/~ivan/Sigma.pdf`, 2010.
38. Isogeny Mental Card Game. `https://github.com/IvanIoganson/isogeny_mental_card_game.git`, 2024.
39. Faster-csidh. `https://github.com/herumi/faster-csidh.git`, 2023.

Приложение 1. Протокол с валидацией

Данная версия протокола включает в себя протоколы с нулевым разглашением и предназначена для защиты от злоумышленника, который может активно подменять посылаемую информацию для получения выгоды. Если один из игроков нарушит ход протокола, то данный факт можно будет однозначно доказать.

Протоколы подготовки и тасования колоды и выдачи карты описаны ниже как протоколы 4.1, 4.2 и 4.3 соответственно.

Протокол 4.1. Подготовка колоды

Вход: p — простое число, $E_0/\mathbb{F}_p$ — начальная эллиптическая кривая с $\mathrm{End}_{\mathbb{F}_p}(E_0) \cong \mathcal{O}$, $Cl(\mathcal{O})$ — группа классов идеалов порядка $\mathcal{O}$, M — количество карт, N — количество игроков.

Выход: открытая колода A, контрольное значение a_0.

Для $i = 1, \ldots, M$:
- $a_i^{(0)} := E_0$.
- **Для** $j = 1, \ldots, N$:
  - Игрок P_j выбирает $[\mathfrak{x}_j] \xleftarrow{\$} Cl(\mathcal{O})$.
  - Игрок P_j вычисляет $a_i^{(j)} := [\mathfrak{x}_j] \star a_i^{(j-1)}$.
  - Игрок P_j выполняет протокол ZKP_1 (см. Приложение 2) с остальными пользователями. В качестве открытых значений выступают $a_i^{(j-1)}$ и $a_i^{(j)}$, а в качестве секретного — $[\mathfrak{x}_j]$.

$A := \{a_i^{(N)}\}$ для $i \in \{1, \ldots, M\}$, $a_0 := a_0^{(N)}$.

Вернуть A, a_0.

Протокол 4.2. Тасование колоды

Вход: A — открытая колода, a_0 — контрольное значение, M — количество карт, N — количество игроков, $Cl(\mathcal{O})$ — группа классов идеалов (см. протокол 4.1).

Выход: перетасованная колода B, набор контрольных значений B_0.

$B^{(0)} := A$, $b_0^{(0)} := a_0$.

Для $i = 1, \ldots, N$:

- Игрок P_i выбирает случайную перестановку $S_i : \{1, \ldots, M\} \to \{1, \ldots, M\}$.
- Игрок P_i выбирает $[\mathfrak{y}_i] \xleftarrow{\$} Cl(\mathcal{O})$ и запоминает его.
- Игрок P_i вычисляет $B^{(i)} := ([\mathfrak{y}_i] \star b_{S_i(1)}^{(i-1)}, [\mathfrak{y}_i] \star b_{S_i(2)}^{(i-1)}, \ldots, [\mathfrak{y}_i] \star b_{S_i(M)}^{(i-1)})$, где $b_t^{(i-1)} \in B^{(i-1)}$, $t \in \{1, \ldots, M\}$.
- Игрок P_i вычисляет $b_0^{(i)} := [\mathfrak{y}_i] \star b_0^{(i-1)}$.
- Игрок P_i, выступая в роли доказывающего, выполняет протокол ZKP_2 (см. Приложение 2) со всеми остальными пользователями. В качестве открытыхП значений выступают $b_0^{(i-1)}$, $b_0^{(i)}$, $B^{(i-1)}$, $B^{(i)}$, а в качестве секретных — $[\mathfrak{y}_i]$ и S_i.

$B_0 := \{b_0^{(0)}, b_0^{(1)}, \ldots, b_0^{(N)}\}$, $B := B^{(N)}$.

Вернуть B, B_0.

Протокол 4.3. Выдача карты

Вход: $c^{(0)}$ — закрытая карта, $B_0 = \{b_0^{(0)}, b_0^{(1)}, \ldots, b_0^{(N)}\}$ — набор контрольных значений, k — номер игрока, которому эта карта предназначена, N — количество игроков.

Выход: карта c.

Для $j \in \{1, \ldots, N\} \setminus \{k\}$:

- Игрок P_j вычисляет $c^{(j)} := [\mathfrak{y}_j]^{-1} \star c^{(j-1)}$, где $[\mathfrak{y}_j]$ — секретная маска игрока j.
- Игрок P_j, выступая в роли доказывающего, выполняет протокол ZKP_3 (см. Приложение 2) со всеми остальными пользователями. В качестве открытых значений выступают $c^{(j-1)}, b_0^{(j)}, c^{(j)}$, $b_0^{(j-1)}$, а в качестве секретного — $[\mathfrak{y}_j]^{-1}$.

Игрок P_k вычисляет $c := [\mathfrak{y}_k]^{-1} \star c^{(N-1)}$, где $[\mathfrak{y}_k]$ — секретная маска игрока k.

Вернуть c.

Для открытия карты игрок P_j публикует ранее выданную карту c, а затем игрок P_j, выступая в роли доказывающего, выполняет протокол ZKP_3 (см. Приложение 2) со всеми остальными пользователями. В качестве открытых значений выступают $c^{(N)}, b_0^{(j)}, c, b_0^{(j-1)}$, а в качестве секретного — $[\mathfrak{y}_k]^{-1}$.

Приложение 2. Протоколы доказательства с нулевым разглашением

ZKP_1 (CSI-FiSh)
Доказать, что $E_2 = [\mathfrak{x}] \star E_1$.
Открытые значения: E_1, E_2.
Секрет: $[\mathfrak{x}] \in Cl(\mathcal{O})$.

	Доказывающий		**Проверяющий**
1 :	$[\mathfrak{b}] \xleftarrow{\$} Cl(\mathcal{O})$		
2 :	$E := [\mathfrak{b}] \star E_1$		
		$\xrightarrow{\quad E \quad}$	
3 :			$c \xleftarrow{\$} \{0,1\}$
		$\xleftarrow{\quad c \quad}$	
4 :	Если $c = 0$, то $[\mathfrak{r}] := [\mathfrak{b}]$ Иначе $[\mathfrak{r}] := [\mathfrak{b}] \cdot [\mathfrak{x}]^{-1}$		
		$\xrightarrow{\quad [\mathfrak{r}] \quad}$	
5 :			$E' := [\mathfrak{r}] \star E_{c+1}$
6 :			Если $E' = E$, то ИСТИНА, иначе ЛОЖЬ.

ZKP_2 (Перетасовка)
Доказать, что $B^{(2)}$ получен из $B^{(1)}$ с помощью перестановки S и маски $[\mathfrak{x}]$ и что $b_0^{(2)} = [\mathfrak{x}] \star b_0^{(1)}$.
Открытые значения: $B^{(1)}, B^{(2)}, b_0^{(1)}, b_0^{(2)}$.
Секрет: $[\mathfrak{x}] \in Cl(\mathcal{O}), S : \{1, \ldots, M\} \to \{1, \ldots, M\}$.

	Доказывающий		**Проверяющий**
1 :	$[\mathfrak{b}] \xleftarrow{\$} Cl(\mathcal{O})$		
2 :	Случайная перестановка $S_b : \{1, \ldots, M\} \to \{1, \ldots, M\}$		
3 :	$B^b := ([\mathfrak{b}] \star B^{(1)}_{S_b(i)} \mid i \in \{1...M\})$ $b_0^b := [\mathfrak{b}] \star b_0^{(1)}$		
		$\xrightarrow{\quad B^b, b_0^b \quad}$	
4 :			$c \xleftarrow{\$} \{0,1\}$
		$\xleftarrow{\quad c \quad}$	
5 :	Если $c = 0$: $[\mathfrak{r}] := [\mathfrak{b}]$ $S_r := S_b$ Если $c = 1$: $[\mathfrak{r}] := [\mathfrak{b}] \cdot [\mathfrak{x}]^{-1}$ $S_r := S^{-1}(S_b)$		
		$\xrightarrow{\quad [\mathfrak{r}], S_r \quad}$	
6 :			$B' := ([\mathfrak{r}] \star B^{(c+1)}_{S_r(i)} \mid i \in \{1...M\})$
7 :			$b'_0 := [\mathfrak{r}] \star b_0^{(c+1)}$
8 :			Если $B' = B^b$ и $b'_0 = b_0^b$, то ИСТИНА, иначе ЛОЖЬ.

ZKP_3 (Раскрытие)
Доказать, что $E_{12} = [\mathfrak{x}] \star E_{11}$ и $E_{22} = [\mathfrak{x}] \star E_{21}$.
Открытые значения: $E_{11}, E_{12}, E_{21}, E_{22}$.
Секрет: $[\mathfrak{x}] \in Cl(\mathcal{O})$.

	Доказывающий		**Проверяющий**
1 :	$[\mathfrak{b}] \xleftarrow{\$} Cl(\mathcal{O})$		
2 :	$E_1 := [\mathfrak{b}] \star E_{11}$		
3 :	$E_2 := [\mathfrak{b}] \star E_{21}$	$\xrightarrow{\quad E_1, E_2 \quad}$	
4 :			$c \xleftarrow{\$} \{0,1\}$
		$\xleftarrow{\quad c \quad}$	
5 :	Если $c = 0$, то $[\mathfrak{r}] := [\mathfrak{b}]$ Иначе $[\mathfrak{r}] := [\mathfrak{b}] \cdot [\mathfrak{x}]^{-1}$		
		$\xrightarrow{\quad [\mathfrak{r}] \quad}$	
6 :			$E'_1 := [\mathfrak{r}] \star E_{1(c+1)}$
7 :			$E'_2 := [\mathfrak{r}] \star E_{2(c+1)}$
8 :			Если $E'_1 = E_1$ и $E'_2 = E_2$, то ИСТИНА, иначе ЛОЖЬ.

УДК 519.719.1 DOI 10.17223/20710410/69/6

ОБЩАЯ СХЕМА ДЛЯ СЕМЕЙСТВА ПРОТОКОЛОВ ВЫРАБОТКИ ОБЩЕГО КЛЮЧА ТИПА ДИФФИ — ХЕЛЛМАНА

А. В. Черемушкин

Академия криптографии РФ, г. Москва, Россия

E-mail: avc238@mail.ru

Изучается общая схема для семейства протоколов выработки ключа по типу протокола Диффи — Хеллмана, предложенная В. А. Артамоновым и В. В. Ященко и основанная на решении функционального тождества $f(x, g(y, a)) = g(y, f(x, a))$. Рассмотрен случай с различными отображениями f, g, а также несколько примеров протоколов на основе некоммутативных и неассоциативных бинарных операций, описываемых данной общей схемой.

Ключевые слова: *протокол Диффи — Хеллмана, сильно зависимые операции, обобщённое тождество медиальности.*

GENERAL SCHEME FOR A CLASS OF DIFFIE — HELLMAN TYPE PROTOCOLS

A. V. Cheremushkin

Academy of Cryptography of the Russian Federation, Moscow, Russia

We consider a general scheme for the class of Diffie — Hellman type protocols proposed by V. Artamonov and V. Yaschenko in 1994. It is based on functional equality $f(x, g(y, a)) = g(y, f(x, a))$ with some functions f, g. We investigate the case with different functions f, g. Some examples of such protocols with nonassociative and noncommutative binary operations are considered.

Keywords: *Diffie — Hellman type protocol, strong dependent operation, general medial identity.*

1. Общая схема протокола типа Диффи — Хеллмана

В работе [1] предложена общая схема протокола Диффи — Хеллмана. Пусть S — множество формируемых общих секретных ключей, K_i — множества личных ключей абонентов, U_i, $i = 1, 2$, — множества открытых ключей абонентов. Общая схема строится на основе четырёх сюръективных отображений $f_1 : K_1 \times U_2 \to S$, $f_2 : K_2 \times U_1 \to S$, $\varphi_1 : K_1 \to U_1$ и $\varphi_2 : K_2 \to U_2$, удовлетворяющих тождеству

$$f_1(k_1, \varphi_2(k_2)) = f_2(k_2, \varphi_1(k_1))$$

при всех $k_i \in K_i$. Для практики удобным является случай, когда $U_1 = U_2 = S$ и отображения φ_i, $i = 1, 2$, задаются на основе функций f_i равенствами $\varphi_i(k_i) = f_i(k_i, a)$, $a \in S$.

1.1. Случай одинаковых функций

Для частного случая $K_1 = K_2$, $U_1 = U_2 = S$, $f_1 = f_2 = f$ и $\varphi_i(k) = f(k, a)$ при некотором фиксированном элементе $a \in S$, $i = 1, 2$, в работе [1] доказана следующая

Теорема 1 [1]. Пусть задано отображение $f : K \times S \to S$ и $a \in S$ — фиксированный элемент, для которого отображение $f_a : K \to S$, заданное равенством $f_a(k) = f(k, a)$, взаимно однозначно. Отображение f является решением функционального уравнения

$$f(k_1, f(k_2, a)) = f(k_2, f(k_1, a))$$

тогда и только тогда, когда K может быть наделено структурой коммутативного группоида с единицей, операция $*$ которого связана с отображением f тождеством $f(k_1, f(k_2, a)) = f(k_1 * k_2, a)$, а единицей является элемент $f_a^{-1}(a)$.

Приведём уточнённую формулировку этого результата. Пусть K и S — конечные множества, $|K| = |S|$ и отображение $f : K \times S \to S$ удовлетворяет условию

$$f(x, f(y, a)) = f(y, f(x, a)) \tag{1}$$

при всех $x, y \in K$ и $a \in S$. Предположим, что хотя бы для одного элемента $a_0 \in S$ отображение $f_{a_0} : K \to S$ является взаимно однозначным.

Напомним, что функция $g : K^m \to K$ называется *сильно зависимой*, если для каждой координаты существует фиксация остальных переменных, при которой получившаяся подфункция (унарная операция) является подстановкой.

Теорема 2. Пусть отображение $f : K \times S \to S$, $|K| = |S|$, удовлетворяет условию (1) и при некотором $a_0 \in K$ отображение $\varphi = f_{a_0} : K \to S$ является взаимно однозначным. Тогда:

1) бинарная операция $\tilde{f} : K \times K \to K$, определяемая равенством

$$\tilde{f}(x, z) = \varphi^{-1}(f(x, \varphi(z))), \quad x, z \in K,$$

является сильно зависимой и удовлетворяет тождеству

$$\tilde{f}(x, \tilde{f}(y, z)) = \tilde{f}(y, \tilde{f}(x, z)) \tag{2}$$

при всех $x, y, z \in K$;

2) найдутся коммутативный моноид $(K, \circ)$ и подстановка $\sigma \in S(K)$, такие, что для сильно зависимой операции $\tilde{f}$ выполнены тождества

$$\tilde{f}(x, z) = \sigma(x \circ \sigma^{-1}(z)),$$
$$\tilde{f}(x, \tilde{f}(y, z)) = \sigma(x \circ y \circ \sigma^{-1}(z))$$

при всех $x, y, z \in K$;

3) при этом для функции f выполнены тождества

$$f(x, a) = (\sigma\varphi)(x \circ (\sigma\varphi)^{-1}(a)),$$
$$f(x, f(y, a)) = (\sigma\varphi)(x \circ y \circ (\sigma\varphi)^{-1}(a))$$

при всех $x, y \in K, a \in S$. Единицей моноида $(K, \circ)$ является элемент $y_0 = \varphi^{-1}(a_0) = f_{a_0}^{-1}(a_0)$.

Доказательство.

1) Для сюръективного отображения $f_{a_0} : K \to S$ найдётся элемент $y_0 \in K$, удовлетворяющий условию $\varphi(y_0) = f(y_0, a_0) = a_0$. Тогда в силу условия (1) выполняется равенство

$$f(x, a_0) = f(x, f(y_0, a_0)) = f(y_0, f(x, a_0)),$$

или

$$\varphi(x) = f(x, \varphi(y_0)) = f(y_0, \varphi(x)),$$

а значит, $f(y_0, a)$ является тождественным отображением по второй переменной. Поэтому операция $\tilde{f}$ является сильно зависимой. Производя замену $a = \varphi(z)$, $z \in K$, в тождестве (1) и учитывая взаимную однозначность отображения φ, получаем тождество (2):

$$\begin{gathered}\tilde{f}(x, \tilde{f}(y, z)) = \varphi^{-1}(f(x, \varphi(\tilde{f}(y, z)))) = \varphi^{-1}(f(x, f(y, \varphi(z)))) = \\ = \varphi^{-1}(f(y, f(x, \varphi(z)))) = \varphi^{-1}(f(y, \varphi(\tilde{f}(x, z)))) = \tilde{f}(y, \tilde{f}(x, z)).\end{gathered}$$

2) Пусть $\tilde{g}(x, y) = \tilde{f}(y, x)$, $x, y \in K$. Тождество (2) можно переписать в виде

$$\tilde{f}(x, \tilde{g}(z, y)) = \tilde{g}(\tilde{f}(x, z), y),$$

где $x, y, z \in K$. Обозначим функцию, стоящую в левой и правой частях этого тождества, через Ф. Согласно теореме о решении уравнения общей ассоциативности из [2], должны существовать подстановки $\pi, \alpha, F_1, F_2, F_3 \in S(K)$ и моноид $(K, *)$, для которых выполняются тождества

$$\begin{gathered}\Phi(x, z, y) = \pi(F_1(x) * F_2(z) * F_3(y)), \\ \tilde{g}(x, y) = \pi(\alpha(x) * F_3(y)), \\ \tilde{f}(x, z) = \alpha^{-1}(F_1(x) * F_2(z)), \\ \tilde{f}(x, z) = F_1(x) * z, \\ \tilde{g}(z, y) = \pi(F_2(z) * F_3(y)),\end{gathered}$$

где $x, y, z \in K$, причём операция $*$ определена однозначно с точностью до изоморфизма. Достаточно ограничиться случаем, когда π является тождественной подстановкой, в противном случае надо перейти к изоморфной бинарной операции $\tilde{*}$ вида $x \,\tilde{*}\, y = \pi(\pi^{-1}(x) * \pi^{-1}(y))$, $x, y \in K$, а вместо сомножителей $F_i(.)$ рассмотреть $\pi(F_i(.))$, $i = 1, 2, 3$. Из предпоследнего тождества получаем

$$\begin{gathered}\tilde{f}(x, z) = F_1(x) * z, \\ \tilde{f}(x, \tilde{f}(y, z)) = F_1(x) * F_1(y) * z,\end{gathered}$$

где $x, y, z \in K$. Остаётся перейти к изоморфной операции $\circ$, определённой равенством $x * y = F_1(F_1^{-1}(x) \circ F_1^{-1}(y))$:

$$\begin{gathered}\tilde{f}(x, z) = F_1(x \circ F_1^{-1}(z)), \\ \tilde{f}(x, \tilde{f}(y, z)) = F_1(x \circ y \circ F_1^{-1}(z)),\end{gathered}$$

где $x, y, z \in K$, и положить $\sigma = F_1$.

Коммутативность моноида $(K, \circ)$ вытекает из условия (1) и тождества

$$F_1(x \circ y \circ F_1^{-1}(z)) = F_1(y \circ x \circ F_1^{-1}(z)).$$

Действительно, при подстановке в это тождество $z = z_0$, такого, что $F_1^{-1}(z) = e$ (единицы моноида), получаем $F_1(x \circ y) = F_1(y \circ x)$.

3) Имеем $f(x, a) = \varphi(\tilde{f}(x, \varphi^{-1}(a)))$, где $x \in K, a \in S$, откуда

$$f(x, a) = \varphi(\tilde{f}(x, \varphi^{-1}(a))) = \varphi(\sigma(x \circ \sigma^{-1}(\varphi^{-1}(a)))) = (\sigma\varphi)(x \circ (\sigma\varphi)^{-1}(a)),$$
$$f(x, f(y, a)) = (\sigma\varphi)(x \circ y \circ (\sigma\varphi)^{-1}(a))$$

при всех $x, y, z \in K$.

Покажем, что единицей моноида $(K, \circ)$ является элемент $y_0 = f_{a_0}^{-1}(a_0)$. Элемент y_0 выбран из условия выполнения равенства $f(y_0, a_0) = a_0$. С другой стороны, $a_0 = f(y_0, a_0) = (\sigma\varphi)(y_0 \circ (\sigma\varphi)^{-1}(a_0))$, откуда получаем $(\sigma\varphi)^{-1}(a_0) = y_0 \circ (\sigma\varphi)^{-1}(a_0)$. Поскольку элемент a_0 обратим, а моноид обладает единственной единицей, то $y_0 = e$, что и доказывает нужное утверждение.

Теорема 2 доказана. ■

Замечание 1. Данная конструкция является основным примитивом при построении протоколов выработки общего ключа, но поскольку она, как и основной протокол Диффи — Хеллмана, является уязвимой к атакам типа «противник в середине», для защиты от этих и подобных атак её необходимо дополнить вспомогательными конструкциями для обеспечения таких свойств протокола, как аутентификация сторон, аутентификация ключа, подтверждение правильности вычисления ключа и т. п.

Пример 1. Стандартный протокол Диффи — Хеллмана получается при $K = \mathbb{Z}_{p-1} = \{0, 1, \ldots, p-2\}$, $S = \mathbb{Z}_p^* = \{1, \ldots, p-1\}$ и $f(x, a) = a^x \bmod p$, где a — обратимый элемент поля $\mathbb{Z}_p$. Обратимое отображение φ задаётся выражением $\varphi(x) = f(x, a_0) = a_0^x \bmod p$, где a_0 — примитивный элемент поля $\mathbb{Z}_p$, при этом $\varphi^{-1}(a) = \log_{a_0} a \in \mathbb{Z}_{p-1}$. Соответствующая сильно зависимая функция на множестве $K = \mathbb{Z}_{p-1}$ после замены переменной $a = \varphi(z)$ имеет вид

$$\tilde{f}(x, z) = \varphi^{-1}(f(x, \varphi(z))) = \log_{a_0}(\varphi(z)^x \bmod p) = \log_{a_0}((a_0^z)^x \bmod p) = z \cdot x \in \mathbb{Z}_{p-1},$$

причём функция f может быть записана в виде

$$f(x, a) = \varphi(\tilde{f}(x, \varphi^{-1}(a))) = a_0^{x\varphi^{-1}(a)} \bmod p = \varphi(x\varphi^{-1}(a)),$$

где $(\cdot)$ — операция умножения кольца $\mathbb{Z}_{p-1}$. Поскольку число $p-1$ составное, полугруппа $(\mathbb{Z}_{p-1}, \cdot)$ имеет делители нуля. Поэтому при практическом использовании следует выбирать элементы $x, y \in K$ отличными от нуля, а в конце проверять условие $f(x, f(y, a)) \neq 1$.

Пример 2. Другой пример построения протокола Диффи — Хеллмана основан на использовании циклической группы простого порядка. По аналогии с предыдущим примером будем использовать мультипликативную запись, чтобы подчеркнуть имеющиеся отличия. Пусть $\mathbb{Z}_p^* = \{1, \ldots, p-1\}$ и $H = \langle h_0 \rangle = \{h_0^0, h_0^1, \ldots, h_0^{p-1}\}$ — циклическая группа простого порядка p, $h_0^p = e$, где e — нейтральный элемент группы H. Заметим, что $h_0^0 = e$ — неподвижная точка группы $\mathbb{Z}_p^*$. Пусть $K = \mathbb{Z}_p^*$ и $S = \{h_0^1, \ldots, h_0^{p-1}\}$, $|K| = |S| = p-1$, причём действие группы $\mathbb{Z}_p^*$ на S регулярно. Поэтому функция $f(x, a) = a^x$, где $x \in K$, $a \in S$, также удовлетворяет условиям теоремы 2. Здесь

$f(x,a)$ при всех $a \in S$ задаёт взаимно однозначное отображение $K \to S$. Если выбрать $\varphi(x) = f(x,h_0) = h_0^x$, $\varphi^{-1}(a) = \log_{h_0} a \in K$, то

$$f(x,a) = \varphi(\tilde{f}(x,\varphi^{-1}(a))) = \varphi(x \cdot \varphi^{-1}(a)) = h_0^{x\cdot\varphi^{-1}(a)} = a^x,$$

где $(\cdot)$ — операция умножения группы $\mathbb{Z}_p^*$. Соответствующая сильно зависимая функция $\tilde{f}$ на множестве $K = \mathbb{Z}_p^*$ после замены переменной $a = \varphi(z)$ имеет вид

$$\tilde{f}(x,z) = \varphi^{-1}(f(x,\varphi(z))) = \log_{h_0}((h_0^z)^x) = z \cdot x \in K.$$

Пример 3. Пусть $(K,\circ)$ — коммутативный моноид с левым действием на множестве S. Если обозначить действие моноида K на множестве S как $f(x,a) = x(a)$, то при всех $x,y \in K$, $a \in S$ получаем

$$f(x,f(y,a)) = (x \circ y)(a).$$

Свойства протокола определяются свойствами этого действия. В частности, необходимо, чтобы оно было точным и совпадали порядки $|K| = |S|$.

Пример 4. Некоммутативный медиальный моноид $(K,\circ)$ позволяет построить протокол, который обобщает стандартный протокол Диффи — Хеллмана. Как показано в п. 2, для такого моноида выполняется свойство перестановочности степеней

$$(a^n)^m = (a^m)^n,$$

где $a \in K$, а m,n — натуральные числа. Более подробно такой протокол описан ниже.

Пример 5. В работе [3] предлагается для построения протокола использовать неассоциативную лупу Муфанг. Это группоид $(X,\cdot)$, удовлетворяющий одному из тождеств

$$\begin{gathered}((x\cdot yz)x = xyzx,\\ x(yz\cdot x) = xy\cdot zx,\\ x(y\cdot xz) = (xy\cdot x)z,\\ (zx\cdot y)x = z(K_1\cdot yx),\end{gathered}$$

где $x,y,z \in X$. Квазигруппа, удовлетворяющая любому из этих тождеств, является лупой. Два последних тождества выделяют класс коммутативных луп. Для лупы Муфанг имеет место ассоциативность степеней, т. е. значение произведения $a\cdot a\cdot\ldots\cdot a$ не зависит от расстановки скобок. Это даёт возможность построить обобщение протокола Диффи — Хеллмана. Один из практических вариантов такого протокола описан в [3].

1.2. Случай разных функций

Рассмотрим теперь более общий вариант предыдущего протокола, когда у сторон имеются различные отображения $f : K_1 \times S \to S$, $g : K_2 \times S \to S$, $|K_1| = |K_2| = |S|$ и при этом выполняется условие

$$f(x,g(y,a)) = g(y,f(x,a)) \tag{3}$$

при всех $x \in K_1$, $y \in K_2$ и $a \in S$. Предположим, что хотя бы для одного элемента $a_0 \in S$ и одного $b_0 \in S$ отображения $f_{a_0} : K_1 \to S$ и $g_{b_0} : K_2 \to S$ являются взаимно однозначными.

Теорема 3. Пусть отображения $f : K_1 \times S \to S$ и $g : K_2 \times S \to S$ удовлетворяют условию (3), при некоторых $a_0 \in K_1$ и $b_0 \in S$ отображения $\varphi = f_{a_0}$ и $\psi = g_{b_0}$ являются взаимно однозначными и $\tau : K_1 \to K_2$ — биекция из условия $\psi\tau = \varphi$. Тогда:

1) бинарные операции $\tilde{f}, \tilde{g} : K_1 \times K_1 \to K_1$, определяемые равенствами

$$\tilde{f}(x,u) = \varphi^{-1}(f(x,\varphi(u))),\ x,u \in K_1,$$
$$\tilde{g}(x,u) = \varphi^{-1}(g(\tau(x),\varphi(u))),\ y,z \in K_1,$$

являются сильно зависимыми на множестве K_1 и удовлетворяют тождеству

$$\tilde{f}(x,\tilde{g}(y,z)) = \tilde{g}(y,\tilde{f}(x,z)) \tag{4}$$

при всех $x,y,z \in K_1$;

2) найдутся коммутативный моноид $(K_1,*)$, подстановки $\sigma,\beta \in S(K_1)$ и элемент $c \in K_1$, такие, что для сильно зависимых операций $\tilde{f}$ и $\tilde{g}$ выполнены тождества

$$\tilde{f}(x_1,z) = \sigma(x_1) * z,$$
$$\tilde{g}(x_2,x_3) = x_3 * c * \beta(x_2),$$
$$\tilde{f}(x_1,\tilde{g}(x_2,x_3)) = \sigma(x_1) * x_3 * c * \beta(x_2)$$

при всех $x_1,x_2,x_3,z \in K_1$;

3) при этом для функций f и g выполнены тождества

$$f(x,a) = \varphi(\sigma(x) * \varphi^{-1}(a)),$$
$$g(y,a) = \varphi(\varphi^{-1}(a) * c * \beta(\tau^{-1}(y))), \tag{5}$$
$$f(x,g(y,a)) = \varphi(\sigma(x) * \varphi^{-1}(a) * c * \beta(\tau^{-1}(y)))$$

при всех $x \in K_1$, $y \in K_2$, $a \in S$.

Единицей моноида $(K_1,*)$ является $\sigma(y_0)$, где элемент y_0 выбирается из условия $\varphi(y_0) = f(y_0,a_0) = a_0$.

Доказательство. Проводится аналогично доказательству теоремы 2 с учётом различия функций f и g:

1) Для сюръективного отображения $g_{b_0} : K_2 \to S$ найдётся элемент $y_0 \in K_2$, удовлетворяющий условию $\psi(y_0) = g(y_0,b_0) = a_0$. Тогда в силу условия (3) выполняется равенство

$$\varphi(x) = f(x,a_0) = f(x,g(y_0,b_0)) = g(y_0,f(x,b_0)),$$

а значит, $g(y_0,s)$ является подстановкой на множестве S.

Пусть $\tau : K_1 \to K_2$ — биекция из условия $\psi\tau = \varphi$. Производя у функции g замену переменных, получаем, что функция $\tilde{g}(x,v) = \varphi^{-1}(g(\tau(x),\varphi(v))$, $x,v \in K_1$, определена на множестве K_1 и является сильно зависимой.

Аналогично, выбирая x_0 так, чтобы $f(x_0,a_0) = b_0$, с помощью равенства

$$\psi(x) = g(y,b_0) = g(y,f(x_0,a_0)) = f(x_0,g(y,a_0))$$

можно показать, что $f(x_0,a)$ является взаимно однозначным отображением на множестве S, поэтому операция $\tilde{f}(x,u) = \varphi^{-1}(f(x,\varphi(u)))$ является сильно зависимой на K_1.

Производя замену переменных $x = x_1$, $y = \tau(x_2)$, $a = \varphi(x_3)$, $x_2,x_2,x_3 \in K_1$, в (3):

$$f(x_1,g(\tau(x_2),\varphi(x_3))) = g(\tau(x_2),f(x_1,\varphi(x_3))),$$

и переходя к функциям $\tilde{f}, \tilde{g}$, получаем тождество (4):

$$\tilde{f}(x_1, \tilde{g}(x_2, x_3)) = \varphi^{-1}(f(x_1, \varphi(\tilde{g}(\tau(x_2), x_3)))) = \varphi^{-1}(f(x_1, g(\tau(x_2), \varphi(x_3)))) =$$
$$= \varphi^{-1}(g(\tau(x_2), f(x_1, \varphi(x_3)))) = \varphi^{-1}(g(\tau(x_2), \varphi(\tilde{f}(x_1, x_3)))) = \tilde{g}(x_2, \tilde{f}(x_1, x_3)).$$

2) Обозначая через $\tilde{h}$ функцию $\tilde{h}(x_1, x_2) = \tilde{g}(x_2, x_1)$, получаем тождество

$$\tilde{f}(x_1, \tilde{h}(x_3, x_2)) = \tilde{h}(\tilde{f}(x_1, x_3), x_2).$$

Пусть Φ — функция, стоящая в левой и правой частях этого тождества. Согласно теореме о решении уравнения общей ассоциативности из [2], должны существовать подстановки $\pi, \alpha, F_1, F_2, F_3 \in S(K_1)$ и моноид $(K_1, *)$, для которых выполняются тождества

$$\begin{gathered}
\Phi(x_1, x_3, x_2) = \pi(F_1(x_1) * F_2(x_3) * F_3(x_2)), \\
\tilde{h}(z, x_2) = \pi(\alpha(z) * F_3(x_2)), \\
\tilde{f}(x_1, x_3) = \alpha^{-1}(F_1(x_1) * F_2(x_3)), \\
\tilde{f}(x_1, z) = F_1(x_1) * z, \\
\tilde{h}(x_3, x_2) = \pi(F_2(x_3) * F_3(x_2)),
\end{gathered} \tag{6}$$

где $x_1, x_2, x_3, z \in K_1$, причём операция $*$ определена однозначно с точностью до изоморфизма. Как и в теореме 2, достаточно рассмотреть случай, когда π является тождественной подстановкой, иначе надо перейти к изоморфной бинарной операции $\tilde{*}$ и вместо сомножителей $F_i(.)$ рассмотреть $\pi(F_i(.))$, $i = 1, 2, 3$.

Из равенств (6) получаем

$$\tilde{f}(x_1, z) = F_1(x_1) * z = \alpha^{-1}(F_1(x_1) * F_2(z)),$$
$$\tilde{g}(x_2, x_3) = F_2(x_3) * F_3(x_2) = \alpha(x_3) * F_3(x_2),$$

где $x_1, x_2, x_3, z \in K_1$. Отсюда $\alpha = F_2$ и $x * z = \alpha^{-1}(x * \alpha(z))$, или иначе $\alpha(x * z) = x * \alpha(z)$. Значит, $\alpha(x) = x * \alpha(e)$, где e — единица моноида $(K_1, *)$.

Обозначая $\beta = F_3$, $\sigma = F_1$ и $c = \alpha(e)$, получаем

$$\tilde{f}(x_1, z) = \sigma(x_1) * z,$$
$$\tilde{g}(x_2, x_3) = x_3 * c * \beta(x_2),$$
$$\tilde{f}(x_1, \tilde{g}(x_2, x_3)) = \sigma(x_1) * x_3 * c * \beta(x_2).$$

3) Поскольку

$$f(x, a) = \varphi(\tilde{f}(x, \varphi^{-1}(a))),$$
$$g(y, a) = \varphi(\tilde{g}(\tau^{-1}(y), \varphi^{-1}(a))),$$

где $x \in K_1$, $y \in K_2$, $a \in S$, то

$$f(x, a) = \varphi(\sigma(x) * \varphi^{-1}(a)),$$
$$g(y, a) = \varphi(\varphi^{-1}(a) * c * \beta(\tau^{-1}(y))),$$
$$f(x, g(y, a)) = \varphi(\sigma(x) * \varphi^{-1}(a) * c * \beta(\tau^{-1}(y)))$$

при всех $x \in K_1$, $y \in K_2$,$a \in S$.

Покажем, что единицей моноида $(K_1, *)$ является элемент $\sigma(y_0)$, где y_0 выбирается из условия выполнения равенства $\varphi(y_0) = f(y_0, a_0) = a_0$, т. е. $y_0 = \varphi^{-1}(a_0)$. С другой стороны, $a_0 = f(y_0, a_0) = \varphi(\sigma(y_0) * \varphi^{-1}(a_0))$, откуда получаем $\varphi^{-1}(a_0) = \sigma(y_0) * \varphi^{-1}(a_0)$. Поскольку a_0 обратим, а моноид обладает единственной единицей, то $\sigma(y_0) = e$.

Теорема 3 доказана. ■

Замечание 2. Если в п. 3 теоремы 3 вместо моноида $(K_1, *)$ использовать изоморфный моноид $(S, \circ)$ с операцией $\circ$, задаваемой равенством $x \circ y = \varphi(\varphi^{-1}(x) * \varphi^{-1}(y))$, то функции f и g можно записать в виде

$$f(x, a) = \varphi(\sigma(x)) \circ a,$$
$$g(y, a) = a * \varphi(c) \circ \varphi(\beta(\tau^{-1}(y))),$$
$$f(x, g(y, a)) = \varphi(\sigma(x)) \circ a \circ \varphi(c) \circ \varphi(\beta(\tau^{-1}(y)))$$

при всех $x \in K_1$, $y \in K_2$, $a \in S$, или в более компактной форме

$$f(x, a) = \hat{\alpha}(x) \circ a,$$
$$g(y, a) = a \circ \hat{\beta}(y),$$
$$f(x, g(y, a)) = \hat{\alpha(x)} \circ a \circ \hat{\beta}(y)$$

при $\hat{\alpha} = \sigma\varphi$, $\hat{\beta} = \tau^{-1}\beta\varphi$. Таким образом, в некоммутативном случае функции f и g задаются различными выражениями: с помощью левого и правого умножения относительно операции моноида с единицей. При этом отображения $\hat{\alpha} : K_1 \to S$ и $\hat{\beta} : K_2 \to S$ должны быть взаимно однозначными. Это следует из существования элементов a_0 и b_0 из условия теоремы 3.

Пример 6. Некоммутативный моноид $(K, *)$ с операциями, задаваемыми равенствами вида (5), может быть использован для построения протокола выработки общих ключей парной связи для любой пары (i, j) абонентов сети связи с N абонентами. Пусть i-й абонент обладает парой бинарных операций $f_i, g_i : K \times S \to S$, $|K| = |S|$, при некоторых подстановках $\alpha_i, \beta_i : K \to K$ и взаимно однозначном отображении $\varphi : K \to S$, обладающем свойством однонаправленности:

$$f_i(x, a) = \varphi(\alpha_i(x) * \varphi^{-1}(a)),$$
$$g_i(x, a) = \varphi(\varphi^{-1}(a) * \beta_i(x)), \qquad i = 1, \ldots, N.$$

Общие ключи k_{ij}, k_{ji} для направлений от i к j и от j к i вычисляются по формулам

$$k_{ij} = f_i(x_i, g_j(x_j, a)) = \varphi(\alpha_i(x_i) * \varphi^{-1}(a) * \beta_j(x_j)),$$
$$k_{ji} = f_j(x_i, g_i(x_j, a)) = \varphi(\alpha_j(x_j) * \varphi^{-1}(a) * \beta_i(x_i))$$

для случайных элементов $x_i, x_j \in K$, $a \in S$.

Пример 7. Для некоммутативных медиальных моноидов $(K, \circ)$ и $(K, *)$, операции которых удовлетворяют обобщённому тождеству медиальности, можно построить обобщение стандартного протокола Диффи — Хеллмана для случая, когда каждая из сторон использует операцию возведения в степень относительно своей бинарной операции. Более подробно такой протокол описан далее.

2. Протокол на основе медиальных бинарных операций

Сначала приведём необходимые сведения о свойстве перестановочности степеней.

2.1. Перестановочность степеней для одной бинарной операции

Пусть $Q = (X, *)$ группоид, $*$ — бинарная операция и $x \in X$. *Медиальным* называется группоид, операция которого удовлетворяет тождеству

$$(a * b) * (c * d) = (a * c) * (b * d).$$

Рассмотрим n-ю степень x^n элемента x, которая определяется индуктивно как

$$x^1 = x, \quad x^{n+1} = (x^n) * x, \ n \geqslant 1.$$

В работе [4] D. C. Murdoch заметил, что медиальные группоиды обладают свойством *перестановочности степеней* (*palintropic property*)[1].

Теорема 4 [4, Theorem 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 $*$ возможны и другие определения степени. Каждое такое произведение отличается способом расстановки скобок в последовательности $\underbrace{x * x * \ldots * x}_{n}$. Например, при $n = 3$ получаем два возможных произведения:

$$(x * x) * x, \quad x * (x * x),$$

а при $n = 4$ уже пять:

$$((x * x) * x) * x, \quad (x * (x * x)) * x, \quad (x * x) * (x * x), \quad x * ((x * x) * x), \quad x * (x * (x * x)).$$

Такие выражения называются скобочными (shapes). Общее число скобочных выражений длины m называется $(m-1)$-м числом Каталана и равно

$$A_m = \frac{1}{m}\binom{2(m-1)}{m-1}.$$

Перечисленные выше произведения можно записать в индексной форме: при $n = 3$ как $x^2 * x = x^{2+1}$ и $x * x^2 = x^{1+2}$; при $n = 4$ получаем

$$x^{(2+1)+1}, \ x^{(1+2)+1}, \ x^{2+2}, \ x^{1+(2+1)}, \ x^{1+(1+2)}.$$

Обозначим степени $(x^n)^m$ и $(x^m)^n$ как $x^{n \cdot m}$ и $x^{m \cdot n}$ соответственно. Каждое скобочное выражение можно записать как степень $x^{\mathbf{A}}$ элемента x, показатель $\mathbf{A}$ которой — формальное алгебраическое выражение над натуральными числами с использованием символов операций сложения, умножения и возведения в степень (выражается через умножение):

$$x^{\mathbf{A}+\mathbf{B}} = x^{\mathbf{A}} * x^{\mathbf{B}}, \quad x^{\mathbf{A} \cdot \mathbf{B}} = (x^{\mathbf{A}})^{\mathbf{B}}, \quad x^{\mathbf{A}^t} = \underbrace{(((x^{\mathbf{A}})^{\mathbf{A}}) \ldots)^{\mathbf{A}}}_{t},$$

[1] 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 $x * z = y * w$.

где $\mathbf{A}, \mathbf{B} \in (\mathbb{N}; +, \cdot)$ Заметим, что в силу теоремы 4 операция умножения в показателе степени коммутативна и ассоциативна, хотя операция сложения в общем случае не является ни коммутативной, ни ассоциативной. При этом закон дистрибутивности сложения относительно умножения сохраняется:

$$x^{2(1+3)} = x^{2\cdot 1+2\cdot 3} = x^{1\cdot 2+3\cdot 2} = x^{(1+3)2}.$$

Показатель $\mathbf{A}$ называют *степенны́м индексом* (power index), или просто *индексом*. Степенны́е индексы $\mathbf{A}$ и $\mathbf{B}$ называются *эквивалентными* ($\mathbf{A} \sim \mathbf{B}$) для группоида Q, если $x^{\mathbf{A}} = x^{\mathbf{B}}$ для всех $x \in X$. Множество классов эквивалентности индексов образует факторалгебру $L_Q = (\mathbb{N}; +, \cdot)/_\sim$ с двумя бинарными операциями, которую I. M. H. Etherington [5] назвал *логарифметической* (logarithmetic). Если $X = \{x_1, x_2, \ldots, x_n\}$, то изоморфным представлением для L_Q является множество различных упорядоченных наборов вида

$$\{(x_1^{\mathbf{A}}, x_2^{\mathbf{A}}, \ldots, x_n^{\mathbf{A}}) : \mathbf{A} \in (\mathbb{N}; +, \cdot)\} \subseteq X^X,$$

которые соответствуют классам эквивалентности $[\mathbf{A}]$ отношения $\sim$ и являются табличными заданиями соответствующих отображений из множества X в множество X.

Используя такие обозначения, I. M. H. Etherington [5] доказал, что если вместо степеней элементов рассматривать произвольные скобочные выражения (степенны́е индексы), то для медиальных группоидов свойство перестановочности степеней оказывается справедливым и в этом случае.

Теорема 5 [5, Theorem 10]. Пусть $\mathbf{A}$ и $\mathbf{B}$ — произвольные степенны́е индексы. Для любых элементов $x, y \in X$ медиального группоида $(X, *)$ выполнены равенства

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

В работе [6] предлагается распространение этого свойства на парамедиальные квазигруппы. В этом случае, как показали авторы, приходится уточнять свойство перестановочности степеней путём подправления индексов в правой части равенства $(x^{\mathbf{A}})^{\mathbf{B}} = (x^{\bar{\mathbf{B}}})^{\bar{\mathbf{A}}}$, где вид индексов $\bar{\mathbf{A}}$ и $\bar{\mathbf{B}}$ определяется чётностью высот деревьев, соответствующих скобочным выражениям с индексами $\mathbf{A}$ и $\mathbf{B}$.

2.2. Перестановочность степеней для двух бинарных операций

Свойство перестановочности степеней для случая, когда степени вычисляются с использованием произвольных скобочных выражений, остаётся справедливым и для двух бинарных операций, удовлетворяющих обобщённому тождеству медиальности.

Говорят, что бинарные операции $f(x, y) = x \circ y$ и $g(u, v) = u * v$ на множестве X удовлетворяют *обобщённому тождеству медиальности*, если

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

или иначе

$$(x * y) \circ (u * v) = (x \circ u) * (y \circ v).$$

Обозначим степени относительно каждой из операций следующим образом:

$$\begin{aligned} x^{\{n\}} &= (((x \circ x) \circ x) \circ \ldots \circ x)x = x^{\{n-1\}} \circ x, \\ y^{[m]} &= (((y * y) * y) * \ldots * y)y = y^{[m-1]} * y. \end{aligned} \tag{7}$$

Для записи степеней со степенны́ми индексами при различных бинарных операциях будем также использовать разные обозначения: $x^{\{\mathbf{A}\}}$ и $x^{[\mathbf{B}]}$.

Теорема 6 [7]. Пусть $\mathbf{A}$ и $\mathbf{B}$ — произвольные степенны́е индексы. Для любых группоидов $(X, \circ)$ и $(X, *)$, операции которых удовлетворяют обобщённому тождеству медиальности, для любых элементов $x, y \in X$ выполнены равенства

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

2.3. Протокол для случая одной бинарной операции

В работах [8, 9] рассмотрены способы построения протокола Диффи — Хеллмана на основе использования односторонних левых и правых степеней в квазигруппах. В [10] для построения протокола предложено рассматривать уже произвольные скобочные выражения на медиальных квазигруппах. В общем случае для медиальных группоидов теорема 5 утверждает, что для всех элементов $a \in X$ медиального группоида $Q = (X, *)$ и любых степенны́х индексов $\mathbf{A}$ и $\mathbf{B}$ выполнено тождество

$$(a^{\mathbf{A}})^{\mathbf{B}} = (a^{\mathbf{B}})^{\mathbf{A}}.$$

Поэтому в качестве множества общих ключей S можно взять подгруппоид

$$S = \langle a \rangle = \{x \in X : \exists \mathbf{A}\, (x = a^{\mathbf{A}})\} \subseteq Q$$

группоида Q для некоторого элемента $a \in X$, а в качестве ключевого множества K — соответствующую логарифметическую алгебру L_S, элементами которой являются классы эквивалентности $[\mathbf{A}]$ степенны́х индексов $\mathbf{A}$ на подгруппоиде S. Если $S = \{a_0, a_1, \ldots, a_{n-1}\}$, то изоморфным представлением для $K = L_S$ является множество различных упорядоченных наборов

$$\bar{K} = \{(a_0^{\mathbf{A}}, a_1^{\mathbf{A}}, \ldots, a_{n-1}^{\mathbf{A}}) : \mathbf{A} \in K\} \subseteq S^S.$$

В нашем случае $S = \langle a \rangle$, поэтому можно полагать $(a_0, \ldots, a_{n-1}) = (a, a^{\mathbf{A}_1}, \ldots, a^{\mathbf{A}_{n-1}})$ при некоторых $\mathbf{A}_1, \ldots, \mathbf{A}_{n-1}$. Обозначим $x^{\mathbf{A}_0} = x^1 = x$. Пусть $m = |\bar{K}|$, $m \geqslant n$. Тогда все отображения из $\bar{K}$ можно представить в виде столбцов таблицы:

$\mathbf{A}_0$	$\mathbf{A}_1$	$\ldots$	$\mathbf{A}_i$	$\ldots$	$\mathbf{A}_{m-1}$
$a_1 = a$	$a^{\mathbf{A}_1}$	$\ldots$	$a^{\mathbf{A}_i}$	$\ldots$	$a^{\mathbf{A}_{m-1}}$
$a_2 = a^{\mathbf{A}_1}$	$(a^{\mathbf{A}_1})^{\mathbf{A}_1}$	$\ldots$	$(a^{\mathbf{A}_1})^{\mathbf{A}_i}$	$\ldots$	$(a^{\mathbf{A}_1})^{\mathbf{A}_{m-1}}$
$\ldots$	$\ldots$	$\ldots$	$\ldots$	$\ldots$	$\ldots$
$a_j = a^{\mathbf{A}_j}$	$(a^{\mathbf{A}_j})^{\mathbf{A}_1}$	$\ldots$	$(a^{\mathbf{A}_j})^{\mathbf{A}_i}$	$\ldots$	$(a^{\mathbf{A}_j})^{\mathbf{A}_{m-1}}$
$\ldots$	$\ldots$	$\ldots$	$\ldots$	$\ldots$	$\ldots$
$a_{n-1} = a^{\mathbf{A}_{n-1}}$	$(a^{\mathbf{A}_{n-1}})^{\mathbf{A}_1}$	$\ldots$	$(a^{\mathbf{A}_{n-1}})^{\mathbf{A}_i}$	$\ldots$	$(a^{\mathbf{A}_{n-1}})^{\mathbf{A}_{m-1}}$

Элементы первого столбца повторяются в первой строке таблицы. Поскольку в первом столбце выписаны все различные элементы из $S = \langle a \rangle$ и в силу теоремы 5 каждое отображение из $\bar{K}$, соответствующее степенно́му индексу $\mathbf{A}_i$, однозначно определяется первым элементом в соответствующем столбце, получаем $m = n$.

Поэтому $|S| = |K|$ и отображение $\varphi : K \to S$, которое ставит в соответствие каждому классу эквивалентности $[\mathbf{A}] \in L_S$ (набору $(a_0^{\mathbf{A}}, a_1^{\mathbf{A}}, \ldots, a_{n-1}^{\mathbf{A}})$) элемент $a^{\mathbf{A}}$, является взаимно однозначным на S. Тем самым условия теоремы 2 оказываются выполненными. В этом случае тождество (1), согласно теореме 2, гарантирует, что операция умножения факторалгебры L_S должна быть коммутативной с нейтральным элементом, соответствующим тождественному отображению $\mathbf{A}_0 : x \mapsto x^1$.

Заметим, что для квазигрупп Q, не имеющих нетривиальных гомоморфных образов, в которых каждый элемент является образующим, в [11] доказано, что $|L_Q| = n^{n/r}$, где $n = |X|$ — порядок квазигруппы Q; r — порядок её группы автоморфизмов.

Способ построения протокола на основе медиальных квазигрупп рассматривается в работе [12]. Показано, что для некоторых квазигрупп решение задачи обобщённого дискретного логарифмирования (GDLP) требует больше квантовых вентилей при использовании гипотетического квантового вычислителя, чем для решения задачи дискретного логарифмирования (DLP) в абелевой группе того же порядка.

Автором [10] замечено, что эффективный квантовый алгоритм Шора, позволяющий решать задачу DLP для коммутативных групп, основан на использовании бинарного алгоритма возведения в степень путём последовательного возведения в квадрат. Но этот алгоритм работает только для коммутативных и ассоциативных операций умножения. Поэтому при использовании некоммутативных и неассоциативных операций требуется использовать другие подходы. Однако в работе [13] L. Panny заметил, что для любой медиальной бинарной операции $*$ на X в силу теоремы К. Тойода можно определить на X абелеву групповую операцию $\cdot$, такую, что при некоторых попарно коммутирующих автоморфизмах σ, τ группы $(X, \cdot)$ и некотором $b \in X$ выполняется равенство

$$x_1 * x_2 = x_1^{\sigma} \cdot x_2^{\tau} \cdot b. \tag{8}$$

Используя такое представление, он доказал, что для произвольного степенно́го индекса $\mathbf{A}$ при всех $x \in G$ степень $x^{\mathbf{A}}$ может быть записана в виде $x^{\xi} \cdot b^{\gamma}$, где $\xi, \gamma \in \mathbb{Z}[\sigma, \tau]$.

Теорема 7 [13, Lemma 2]. Для произвольного степенно́го индекса $\mathbf{A}$ при всех $x \in G$ для операции $*$ вида (8) выполнено равенство

$$x^{\mathbf{A}} = x^{1+(\sigma+\tau-1)\gamma}\, b^{\gamma},$$

где $\gamma \in \mathbb{Z}[\sigma, \tau]$. Более того, если это равенство выполнено для одного $x = a \in X$, то оно выполнено для всех $x \in \langle a \rangle$.

Таким образом, задача GDLP решения уравнения $a^{\mathbf{A}} = c$ может быть эффективно сведена к решению уравнения $a(a^{\sigma+\tau-1})^{\gamma}\, b^{\gamma} = c$ относительно неизвестного $\gamma \in \mathbb{Z}[\sigma, \tau]$.

2.4. Протокол для случая двух бинарных операций

Рассмотрим теперь вариант алгоритма типа Диффи — Хеллмана на основе двух бинарных операций $f(x, y) = x \circ y$ и $g(u, v) = u * v$ на множестве X, удовлетворяющих обобщённому тождеству медиальности. В силу теоремы 6 можно 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 вырабатывает своё случайное число и производит вычисления в соответствии с (7), а затем они обмениваются полученными значениями:

$$A \to B : a^{\{n\}},$$
$$A \leftarrow B : a^{[m]}.$$

В заключение они вычисляют общий ключ $k = \left(a^{\{n\}}\right)^{[m]} = \left(a^{[m]}\right)^{\{n\}}$.

Поскольку обобщённое свойство перестановочности степеней остаётся справедливым для случая произвольной расстановки скобок в выражениях для степеней, то в предыдущем протоколе можно использовать скобочные выражения общего вида,

причём каждая сторона вычисляет выражения обобщённой степени на основе своей бинарной операции. Будем, как и выше, использовать разные обозначения $x^{\{\mathbf{A}\}}$ и $x^{[\mathbf{B}]}$ для степеней, вычисленных с помощью этих операций. Тогда такой протокол можно записать в виде

$$A \to B : a^{\{\mathbf{A}\}},$$
$$A \leftarrow B : a^{[\mathbf{B}]},$$

причём стороны вычисляют общий ключ по формулам

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

Этот случай также может быть описан общей теоремой 3. Только здесь появляются уже два группоида $(X, \circ)$ и $(X, *)$, удовлетворяющие условию

$$S = \{x \in X : \exists \mathbf{A}\,(x = a^{\{\mathbf{A}\}})\} = \{x \in X : \exists \mathbf{B}\,(x = b^{[\mathbf{B}]})\}$$

при некоторых $a, b \in X$, и две логарифметических алгебры:

— K_1 — логарифметическая алгебра $L_S(\circ)$, элементами которой являются классы эквивалентности $\{\mathbf{A}\}$ степенны́х индексов $\mathbf{A}$ на группоиде $(S, \circ)$,

— K_2 — логарифметическая алгебра $L_S(*)$, элементами которой являются классы эквивалентности $[\mathbf{B}]$ степенны́х индексов $\mathbf{B}$ на группоиде $(S, *)$.

Если $b = a_j = a^{\{\mathbf{A}_j\}}$, то логарифметическая алгебра $L_S(*)$ описывается следующей таблицей:

$\mathbf{B}_0$	$\mathbf{B}_1$	$\dots$	$\mathbf{B}_i$	$\dots$	$\mathbf{B}_{n-1}$
$a_1 = a$	$a^{[\mathbf{B}_1]}$	$\dots$	$a^{[\mathbf{B}_i]}$	$\dots$	$a^{[\mathbf{B}_{n-1}]}$
$a_2 = a^{\{\mathbf{A}_1\}}$	$(a^{\{\mathbf{A}_1\}})^{[\mathbf{B}_1]}$	$\dots$	$(a^{\{\mathbf{A}_1\}})^{[\mathbf{B}_i]}$	$\dots$	$(a^{\mathbf{A}_1})^{[\mathbf{B}_{n-1}]}$
$\dots$	$\dots$	$\dots$	$\dots$	$\dots$	$\dots$
$a_j = a^{\{\mathbf{A}_j\}}$	$(a^{\{\mathbf{A}_j\}})^{[\mathbf{B}_1]}$	$\dots$	$(a^{\{\mathbf{A}_j\}})^{[\mathbf{B}_i]}$	$\dots$	$(a^{\{\mathbf{A}_j\}})^{[\mathbf{B}_{n-1}]}$
$\dots$	$\dots$	$\dots$	$\dots$	$\dots$	$\dots$
$a_{n-1} = a^{\{\mathbf{A}_{n-1}\}}$	$(a^{\{\mathbf{A}_{n-1}\}})^{[\mathbf{B}_1]}$	$\dots$	$(a^{\{\mathbf{A}_{n-1}\}})^{[\mathbf{B}_i]}$	$\dots$	$(a^{\{\mathbf{A}_{n-1}\}})^{[\mathbf{B}_{n-1}]}$

Для случая двух операций теорема 7 может быть переформулирована следующим образом. Согласно [7, теорема 6], сильно зависимые операции, удовлетворяющие обобщённому тождеству медиальности, должны иметь вид

$$\begin{aligned} x_1 \circ x_2 &= x_1^{\alpha} \cdot x_2^{\beta} \cdot c, \\ x_1 * x_2 &= x_1^{\sigma} \cdot x_2^{\tau} \cdot b, \end{aligned} \tag{9}$$

где $(X, \cdot)$ — коммутативный моноид; $\alpha, \beta, \sigma, \tau$ — автоморфизмы моноида $(X, \cdot)$; $c, d \in X$, удовлетворяющие соотношениям $\alpha\tau = \sigma\beta$, $\alpha\sigma = \sigma\alpha$, $\beta\tau = \tau\beta$, $c \circ d = d * c$.

Теорема 8. Для операций $\circ$ и $*$ вида (9) и для произвольных степенны́х индексов $\{\mathbf{A}\}$ и $[\mathbf{B}]$ при всех $x \in G$ выполнено равенство

$$(x^{\{\mathbf{A}\}})^{[\mathbf{B}]} = x^{1+(\sigma+\tau-1)\gamma_1+(\alpha+\beta-1)\gamma_2} \cdot b^{\gamma_1} \cdot c^{\gamma_2},$$

где $\gamma_1, \gamma_2 \in \mathbb{Z}[\alpha, \beta, \sigma, \tau]$. Более того, если это равенство выполнено для одного $x = a \in X$, то оно выполнено для всех $x \in \langle a \rangle$.

Доказательство. Представим степенно́й индекс $[\mathbf{B}]$ в виде $[\mathbf{B_1}]+[\mathbf{B_2}]$. По предположению индукции

$$\left(x^{\{\mathbf{A}\}}\right)^{[\mathbf{B_1}]} = x^{1+(\sigma+\tau-1)\gamma_1+(\alpha+\beta-1)\gamma_2}\cdot b^{\gamma_1}\cdot c^{\gamma_2},$$
$$\left(x^{\{\mathbf{A}\}}\right)^{[\mathbf{B_2}]} = x^{1+(\sigma+\tau-1)\delta_1+(\alpha+\beta-1)\delta_2}\cdot b^{\delta_1}\cdot c^{\delta_2},$$

где $\gamma_1,\gamma_2,\delta_1,\delta_2\in\mathbb{Z}[\alpha,\beta,\sigma,\tau]$. Поэтому

$$\left(x^{\{\mathbf{A}\}}\right)^{[\mathbf{B}]} = \left(x^{\{\mathbf{A}\}}\right)^{[\mathbf{B_1}]} * \left(x^{\{\mathbf{A}\}}\right)^{[\mathbf{B_2}]} =$$
$$= (x^{1+(\sigma+\tau-1)\gamma_1(\alpha+\beta-1)\gamma_2}\cdot b^{\gamma_1}\cdot c^{\gamma_2})^{\sigma}(x^{1+(\sigma+\tau-1)\delta_1+(\alpha+\beta-1)\delta_2}\cdot b^{\delta_1}\cdot c^{\delta_2})^{\tau}b =$$
$$= x^{\sigma+\tau}\cdot x^{(\sigma+\tau-1)(\gamma_1\sigma+\delta_1\tau)+(\alpha+\beta-1)(\gamma_2\sigma+\delta_2\tau)}\cdot b^{\gamma_1\sigma+\delta_1\tau}c^{\gamma_2\sigma+\delta_2\tau}\cdot b =$$
$$= x^{1+(\sigma+\tau-1)(\gamma_1\sigma+\delta_1\tau+1)+(\alpha+\beta-1)(\gamma_2\sigma+\delta_2\tau)}\cdot b^{\gamma_1\sigma+\delta_1\tau+1}\cdot c^{\gamma_2\sigma+\delta_2\tau} =$$
$$= x^{1+(\sigma+\tau-1)\xi_1+(\alpha+\beta-1)\xi_2}\cdot b^{\xi_1}\cdot c^{\xi_2},$$

где $\xi_1=\gamma_1\sigma+\delta_1\tau+1$, $\xi_2=\gamma_2\sigma+\delta_2\tau\in\mathbb{Z}[\alpha,\beta,\sigma,\tau]$. ■

Доказанные теоремы показывают, что для построения протокола желательно подобрать различные нетривиальные операции $\circ$ и $*$ вида (9). Для этого необходимо выбрать коммутативный моноид $(X,\cdot)$ с группой автоморфизмов $\mathrm{Aut}(\cdot)$, содержащей достаточно большую коммутативную подгруппу; сам моноид должен содержать большую группу обратимых элементов, чтобы при возведении элементов в высокие степени не происходило их быстрое вырождение.

3. Протокол на основе хаотического отображения

Модифицированными многочленами Чебышева (Enhanced Chebyshev polynomial) называются многочлены над кольцом $\mathbb{Z}_N$ из последовательности $T_n(x)$, $n=0,1,2,\ldots$, определяемой линейным рекуррентным соотношением второго порядка следующим образом:

$$T_n(x) = 2xT_{n-1}(x) - T_{n-2}(x) \bmod N,\ n\geqslant 2,$$

где $T_0=1$ и $T_1=x$. Нетрудно видеть, что многочлен $T_n(x)$ имеет степень n и может быть вычислен с использованием матричного равенства

$$\begin{bmatrix} T_n(x) \\ T_{n+1}(x)\end{bmatrix} = A^n\begin{bmatrix} T_0(x)\\ T_1(x)\end{bmatrix},\qquad A=\begin{bmatrix}0 & 1\\ -1 & 2x\end{bmatrix}.$$

Пусть $n=p$ — нечётное простое. Для $n,m\in\mathbb{N}$ многочлены $T_n(x)$ задают отображения $T_n:\mathbb{Z}_p\to\mathbb{Z}_p$, удовлетворяющие свойству

$$T_n(T_m(x)) = T_{n+m}(x) = T_m(T_n(x)) \pmod p.$$

При $x=a\in\mathbb{Z}_p$ последовательность $T_n(a)$ является линейной рекуррентной последовательностью над $\mathbb{Z}_p$ второго порядка с характеристическим многочленом $\lambda^2-2a\lambda+1$. Значения периодов последовательностей $\{u_n = T_n(a) \bmod p\}$, $a\in\mathbb{Z}_p$, $n=0,1,2,\ldots$, описывает следующая

Теорема 9 [14, Theorem 1]. Пусть p — нечётное простое; $a\in\mathbb{Z}_p$, $0\leqslant a<p$; k — период последовательности $T_n(a) \bmod p$, $n=0,1,2,\ldots$; многочлен $\lambda^2-2a\lambda+1$ имеет корни α_1,α_2. Тогда:

(i) если корни лежат в $\mathrm{GF}(p)$, то $k\,|\,(p-1)$;

(ii) если корни лежат в $\mathrm{GF}(p^2)$, то $k\,|\,(p+1)$.

Многочлены $T_n(x)$ можно использовать для построения протокола выработки общего ключа, полагая $f(n,a) = T_n(a)$, $n \in \{0,1,\ldots,p\} = K$. Элемент $a \in \mathbb{Z}_p = S$ выбирается так, что многочлен $\lambda^2 - 2a\lambda + 1$ является неприводимым. В этом случае по теореме 9 минимальный период последовательности $\{T_n(a) \bmod p : n = 1,2,\ldots\}$ является делителем числа $p+1$ и при некоторых значениях элемента a может с ним совпадать. Общий ключ вычисляется по формулам

$$k_{AB} = f(n, f(m,a)) = f(m, f(n,a)) = T_{m+n}(a) \bmod p,$$

где $m, n \in \{0,1,\ldots,p\}$ — случайные числа.

Однако этот вариант протокола не удовлетворяет условию теоремы 2, так как в данном случае не выполняется условие о существовании элемента a, для которого отображение $f_a : \mathbb{Z}_p \to \mathbb{Z}_p$ взаимно однозначно. В работе [14] отмечается, что порождаемая последовательность является симметричной, поэтому содержит не более половины различных элементов кольца $\mathbb{Z}_N$. Например, при $p = 11$ и $a = 3$ последовательность $\{u_n : n = 0,1,2,\ldots\}$ имеет период 12 [14]:

$$\mathbf{1,\ 3,\ 6,\ 0,\ 5,\ 8,\ 10,\ 8,\ 5,\ 0,\ 6,\ 3,}\ 1,3,6,0,5,8,10,8,5,0,6,3,\ldots$$

Сформулируем этот факт в виде следующей теоремы:

Теорема 10. Пусть в условиях теоремы 9 период последовательности $\{u_n = T_n(a) \bmod p : n = 0,1,2,\ldots\}$ равен k, $1 \leqslant k \leqslant p+1$. Тогда:

(i) $u_i = u_{k+1-i}$, $1 \leqslant i \leqslant k$;

(ii) в последовательности $\{u_n\}$ встречается не более $\lceil k/2 \rceil$ различных элементов.

Доказательство. Если последовательность $\{u_n\}$ выписать в обратном порядке, то можно заметить, что она также образует линейную рекуррентную последовательность

$$u_{n-2}(x) = 2au_{n-1}(x) - u_n(x) \mod p, \qquad n = p+1, p, \ldots, 1, 0,$$

с тем же характеристическим многочленом $\lambda^2 - 2a\lambda + 1$. Рассмотрим отрезок

$$u_0, u_1, \ldots, u_{k-1}, u_k. \tag{10}$$

По определению периода $1 = u_0 = u_k$, $a = u_1 = u_{k+1}$. Учитывая, что $u_{k-1} = 2au_k - u_{k+1} = 2a - a = a$, получаем, что начальные члены линейной рекуррентной последовательности

$$u_k, u_{k-1}, \ldots, u_1, u_0 \tag{11}$$

также равны 1 и a, а значит, отрезки (10) и (11) совпадают. Отсюда, очевидно, следуют утверждения (i) и (ii). ■

Автор выражает искреннюю благодарность К. Д. Лушникову за многочисленные полезные замечания.

ЛИТЕРАТУРА

1. *Артамонов В. А., Ященко В. В.* Многоосновные алгебры в системах открытого шифрования // УМН. 1994. Т. 49. Вып. 4. С. 149–150.
2. *Сохацкий Ф. Н.* Обобщение двух теорем Белоусова для сильно зависимых функций k-значной логики // Математические исследования. 1985. Т. 83. С. 105–115.
3. *Марков В. Т., Михалёв А. В., Грибов А. В. и др.* Квазигруппы и кольца в кодировании и построении криптосхем // Прикладная дискретная математика. 2012. № 4(18). С. 31–52.

4. *Murdoch D. C.* Quasi-groups which satisfy certain generalized associative laws // Amer. J. Math. 1939. V. 61. No. 2. P. 509–522.
5. *Etherington I. M. H.* Groupoids with additive endomorphisms // The Amer. Math. Monthly. 1958. V. 65. No. 8. P. 596–601.
6. *Глухов М. М., Карюк Н. А., Катышев С. Ю.* Исследование принципов применения неассоциативных алгебраических структур при синтезе асимметричных криптографических механизмов. CTCrypt 2024. `https://ctcrypt.ru/files/files/2024/04/pc/Катышев.pdf`.
7. *Черемушкин А. В.* Обобщённые тождества медиальности и парамедиальности для сильно зависимых операций // Прикладная дискретная математика. 2024. № 65. С. 21–40.
8. *Katyshev S. Yu., Markov V. T., and Nechaev A. A.* On constructing open key cryptosystems using non associative structures // VI Int. Conf. Non Assoc. Algebra and Appl. Spain, Zaragoza, 2011.
9. *Катышев С. Ю., Марков В. Т., Нечаев А. А.* Использование неассоциативных группоидов для реализации процедуры открытого распределения ключей // Дискретная математика. 2014. Т. 26. № 3. С. 45–64.
10. *Gligoroski D.* Entropoid Based Cryptography. Cryptology ePrint Archive. 2021. Paper 2021/469. `https://eprint.iacr.org/2021/469`.
11. *Alderson (Popova) H.* The structure of the logarithmetics of finite plain quasigroups // J. Algebra. 1974. V. 31. No. 1. P. 1–9.
12. *Baryshnikov A. V. and Katyshev S. Yu.* Key agreement schemes based on linear groupoids // Матем. вопр. криптогр. 2011. Т. 8. № 1. С. 7–12.
13. *Panny L.* Entropoids: Groups in Disguise. Cryptology ePrint Archive. 2021. Paper 2021/583. `https://eprint.iacr.org/2021/583`.
14. *Fee G. J. and Monagan M. B.* Cryptography using Chebyshev polynomials // Maple Summer Workshop. Burnaby, Canada, 2004. P. 1–15.

REFERENCES

1. *Artamonov V. A. and Yaschenko V. V.* Multibasic algebras in public key distribution systems. Russian Math. Surveys, 1994, vol. 49, no. 4, pp. 145–146.
2. *Sokhatskiy F. N.* Obobshchenie dvukh teorem Belousova dlya sil'no zavisimykh funktsiy k-znachnoy logiki [Generalization of two Belousov theorems for strongly dependent functions of k-valued logic]. Matematiceskie Issledovanija, 1985, vol. 83, pp. 105–115. (in Russian)
3. *Markov V. T., Mikhalev A. V., Gribov A. V., et al.* Kvazigruppy i kol'tsa v kodirovanii i postroenii kriptoskhem [Quasigroups and rings in coding theory and cryptography]. Prikladnaya Diskretnaya Matematika, 2012, no. 4(18), pp. 31–52. (in Russian)
4. *Murdoch D. C.* Quasi-groups which satisfy certain generalized associative laws. Amer. J. Math., 1939, vol. 61, no. 2, pp. 509–522.
5. *Etherington I. M. H.* Groupoids with additive endomorphisms. The Amer. Math. Monthly, 1958, vol. 65, no. 8, pp. 596–601.
6. *Glukhov M. M., Karyuk N. A., and Katyshev S. Yu.* Issledovanie printsipov primeneniya neassotsiativnykh algebraicheskikh struktur pri sinteze asimmetrichnykh kriptograficheskikh mekhanizmov [Study of principles of application of non-associative algebraic structures in synthesis of asymmetric cryptographic mechanisms]. CTCrypt 2024. `https://ctcrypt.ru/files/files/2024/04/pc/Катышев.pdf`. (in Russian)
7. *Cheremushkin A. V.* Obobshchennye tozhdestva medial'nosti i paramedial'nosti dlya cil'no zavisimykh operatsiy [Medial and paramedial general identities for strong dependance operations]. Prikladnaya Diskretnaya Matematika, 2024, no. 65, pp. 21–40. (in Russian)

8. *Katyshev S. Yu., Markov V. T., and Nechaev A. A.* On constructing open key cryptosystems using non associative structures. VI Int. Conf. Non Assoc. Algebra and Appl., Spain, Zaragoza, 2011.
9. *Katyshev S. Yu., Markov V. T., and Nechaev A. A.* Application of non-associative groupoids to the realization of an open key distribution procedure. Discrete Math. Appl., 2015, vol. 25, no. 1, pp. 9–24.
10. *Gligoroski D.* Entropoid Based Cryptography. Cryptology ePrint Archive, 2021, paper 2021/469, `https://eprint.iacr.org/2021/469`.
11. *Alderson* (*Popova*) *H.* The structure of the logarithmetics of finite plain quasigroups. J. Algebra, 1974, vol. 31, pp. 1–9.
12. *Baryshnikov A. V. and Katyshev S. Yu.* Key agreement schemes based on linear groupoids. Matematicheskie Voprosy Kriptografii, 2011, vol. 8, no. 1, pp. 7–12.
13. *Panny L.* Entropoids: Groups in Disguise. Cryptology ePrint Archive, 2021, paper 2021/583, `https://eprint.iacr.org/2021/583`.
14. *Fee G. J. and Monagan M. B.* Cryptography using Chebyshev polynomials. Maple Summer Workshop, Burnaby, Canada, 2004, pp. 1–15.

ПРИКЛАДНАЯ ТЕОРИЯ ГРАФОВ

УДК 519.172.3 DOI 10.17223/20710410/69/7

ЯВНАЯ КОНСТРУКЦИЯ БЕСКОНЕЧНЫХ СЕМЕЙСТВ СИЛЬНО РЕГУЛЯРНЫХ ОРГРАФОВ С ПАРАМЕТРАМИ $((v + (2^{n+1} - 4)t)2^{n-1}, k + (2^n - 2)t, t, \lambda, t)$

В. А. Бызов, И. А. Пушкарев

Вятский государственный университет, г. Киров, Россия

E-mail: vbyzov@yandex.ru, god_sha@mail.ru

Описана явная конструкция бесконечных последовательностей сильно регулярных орграфов с наборами параметров $((v + (2^{n+1} - 4)t)2^{n-1}, k + (2^n - 2)t, t, \lambda, t)$. Для поиска начальных орграфов использована компьютерная программа, остальные члены последовательности получены с помощью рекуррентного алгоритма. Найдено 11 семейств сильно регулярных орграфов. В частности, эти семейства содержат орграфы dsrg$(40, 10, 3, 1, 3)$, dsrg$(72, 18, 5, 3, 5)$, dsrg$(76, 19, 5, 4, 5)$, dsrg$(92, 23, 6, 5, 6)$ и dsrg$(104, 26, 7, 5, 7)$, вопрос существования которых ранее был открыт.

Ключевые слова: *сильно регулярный орграф, рекуррентная последовательность, обменная матрица, произведение Кронекера, Artelys Knitro.*

EXPLICIT CONSTRUCTION OF INFINITE FAMILIES OF STRONGLY REGULAR DIGRAPHS WITH PARAMETERS $((v + (2^{n+1} - 4)t)2^{n-1}, k + (2^n - 2)t, t, \lambda, t)$

V. A. Byzov, I. A. Pushkarev

Vyatka State University, Kirov, Russia

An explicit construction of infinite sequences of strongly regular graphs with parameter sets $((v + (2^{n+1} - 4)t)2^{n-1}, k + (2^n - 2)t, t, \lambda, t)$ is described. A computer program was used to find the initial digraphs. The remaining terms of the sequence are obtained automatically by the constructed recurrent algorithm. Using the described approach, 11 families of strongly regular graphs have been found. In particular, these families contain digraphs dsrg$(40, 10, 3, 1, 3)$, dsrg$(72, 18, 5, 3, 5)$, dsrg$(76, 19, 5, 4, 5)$, dsrg$(92, 23, 6, 5, 6)$ and dsrg$(104, 26, 7, 5, 7)$, the question of the existence of which was previously open.

Keywords: *strongly regular digraph, recurrent sequence, exchange matrix, Kronecker product, Artelys Knitro.*

Введение

В работе описан способ, при помощи которого построено несколько бесконечных семейств орграфов. Дадим необходимые понятия и обозначения.

Рассматриваются ориентированные графы (орграфы) без петель и кратных дуг одного направления. Матрицей смежности орграфа называется булева матрица, в которой единица стоит на пересечении i-й строки и j-го столбца, если и только если в орграфе есть дуга от вершины i к вершине j. Будем использовать следующие стандартные обозначения для матриц специального вида:

1) I_m — единичная матрица порядка m;
2) J_m — квадратная матрица порядка m, состоящая только из единиц;
3) $J_{m,l}$ — прямоугольная матрица размера $m \times l$, состоящая только из единиц;
4) K_m — обменная матрица порядка m, то есть квадратная матрица порядка m, в которой на побочной диагонали стоят единицы, а во всех остальных позициях — нули. Другими словами, $K_m(i,j) = \delta_{m+1-i,j}$, где δ — символ Кронекера.

Через $A \otimes B$ будем обозначать произведение Кронекера матриц A и B.

Понятие сильно регулярного орграфа является обобщением концепции сильно регулярного графа [1, 2]. Впервые оно, насколько нам известно, было дано А. М. Дювалем (A. M. Duval) в [3].

Определение 1. Сильно регулярным ориентированным графом с набором параметров $(v,\ k,\ t,\ \lambda,\ \mu)$ называется орграф на v вершинах, в котором выполняются следующие условия:

1) полустепень исхода и полустепень захода каждой вершины равны k;
2) для каждой вершины x существует ровно t путей длины два из x в x;
3) для каждой дуги $x \to y$ количество ориентированных путей из x в y длины два равно λ;
4) для каждой упорядоченной пары вершин (x, y), не образующей дугу орграфа, количество ориентированных путей из x в y длины два равно μ.

Равносильное определение сильно регулярного орграфа можно дать через набор условий, накладываемых на его матрицу смежности.

Определение 2. Сильно регулярным ориентированным графом с набором параметров (v, k, t, λ, μ) называется орграф, матрица смежности A которого удовлетворяет следующим условиям:

$$A^2 = tI_v + \lambda A + \mu(J_v - I_v - A),$$
$$AJ_v = J_v A = kJ_v.$$

Вместо фразы «сильно регулярный орграф с набором параметров $(v,\ k,\ t,\ \lambda,\ \mu)$» будем употреблять (как это часто делают) запись $\mathrm{dsrg}(v, k, t, \lambda, \mu)$. Используя данное обозначение, будем иметь в виду не всё множество таких орграфов, а один из них — реализующийся в рамках описываемой конструкции.

В ряде работ (например, [3, 4] и др.) приведён ряд необходимых условий существования сильно регулярных орграфов с набором параметров $(v,\ k,\ t,\ \lambda,\ \mu)$. Однако, как и в случае сильно регулярных графов, для большого количества наборов параметров вопрос существования соответствующего сильно регулярного орграфа остаётся открытым. В таблице на сайте [5] систематизируется информация об известных сильно регулярных орграфах и тех наборах параметров $(v,\ k,\ t,\ \lambda,\ \mu)$, для которых задача существования сильно регулярного орграфа не решена.

В данной работе описывается приём, который (при определённой доле везения) можно использовать для формирования бесконечного семейства сильно регулярных

орграфов, удовлетворяющих условию $\mu = t$. Конструируемые орграфы устроены рекуррентно: каждый следующий орграф получается из предыдущего члена последовательности. Параметры t, λ и μ всех орграфов в последовательности одинаковые, а количество и степени вершин растут. Будем обозначать через $G_1, G_2, \ldots$ сильно регулярные орграфы формируемой последовательности, а через $A_1, A_2, \ldots$ — соответствующие матрицы смежности. Значительной трудностью описываемого метода является получение орграфа G_2 из орграфа G_1: необходимо существование матриц, удовлетворяющих определённому набору условий. При этом нет гарантий, что данные матрицы вообще существуют. На текущем этапе авторы осуществляют поиск этих матриц при помощи компьютерной программы.

Работа имеет следующую структуру. В п. 1 описан способ получения матрицы A_2 через матрицу A_1. В п. 2 доказано, что при условии существования матриц A_1 и A_2 (нужного вида) можно построить бесконечную последовательность сильно регулярных орграфов. В п. 3 описаны найденные при помощи компьютерной программы семейства орграфов.

1. Получение орграфа G_2

Для дальнейшего изложения понадобится вспомогательная последовательность матриц P_n, определяемая следующим образом:

$$P_n = J_{2^n,1} \otimes K_{2^n} \otimes J_{t,t\cdot 2^n}. \tag{1}$$

Матрицы данной последовательности обладают рядом полезных свойств.

Лемма 1. Матрица P_n, заданная формулой (1), — квадратная матрица порядка $t\cdot 4^n$, обладающая следующими свойствами:

1) $P_n J_{t\cdot 4^n} = J_{t\cdot 4^n} P_n = t \cdot 2^n J_{t\cdot 4^n}$;
2) $P_n^2 = t J_{t\cdot 4^n}$.

Доказательство. Справедливость первого свойства почти очевидна: в каждой строке и в каждом столбце матрицы P_n по построению содержится ровно $t \cdot 2^n$ единиц.

Для доказательства второго пункта леммы воспользуемся свойствами произведения Кронекера [6]:

$$P_n^2 = ((J_{2^n,1} \otimes K_{2^n}) \otimes J_{t,t\cdot 2^n})(J_{2^n,1} \otimes (K_{2^n} \otimes J_{t,t\cdot 2^n})) = ((J_{2^n,1} \otimes K_{2^n})J_{2^n,1}) \otimes$$
$$\otimes (J_{t,t\cdot 2^n}(K_{2^n} \otimes J_{t,t\cdot 2^n})) = J_{4^n,1} \otimes t J_{t,t\cdot 4^n} = t J_{t\cdot 4^n}.$$

Лемма 1 доказана. ■

Пусть G_1 — сильно регулярный орграф с набором параметров (v, k, t, λ, t), A_1 — его матрица смежности. Известно [3], что должно выполняться условие $t > \lambda$. Введём обозначение $s = t - \lambda$ ($s > 0$). Из определения 2 следует, что матрица A_1 удовлетворяет следующим соотношениям:

$$\begin{aligned} A_1^2 + sA_1 &= tJ_v, \\ dA_1 J_v &= J_v A_1 = kJ_v. \end{aligned} \tag{2}$$

Найдём второй член последовательности орграфов — $\mathrm{dsrg}(2v + 8t, k + 2t, t, \lambda, t)$. Его матрицу смежности обозначим через A_2 и будем искать её в следующем виде:

$$A_2 = \begin{pmatrix} A_1 & 0 & B_1 & 0 \\ 0 & A_1 & 0 & B_1 \\ 0 & C_1 & 0 & P_1 \\ C_1 & 0 & P_1 & 0 \end{pmatrix}, \tag{3}$$

где B_1 и C_1 — неизвестные матрицы размеров $v \times 4t$ и $4t \times v$ соответственно. По определению 2 для матрицы A_2 должны выполняться соотношения

$$A_2^2 + sA_2 = tJ_{2v+8t}; \tag{4}$$

$$A_2 J_{2v+8t} = J_{2v+8t} A_2 = (k+2t) J_{2v+8t}. \tag{5}$$

Используя блочное представление (3) матрицы A_2, перепишем уравнение (4) в следующем виде:

$$\left(\begin{array}{c|c|c|c} A_1^2 + sA_1 & B_1C_1 & A_1B_1 + sB_1 & B_1P_1 \\ \hline B_1C_1 & A_1^2 + sA_1 & B_1P_1 & A_1B_1 + sB_1 \\ \hline P_1C_1 & C_1A_1 + sC_1 & P_1^2 & C_1B_1 + sP_1 \\ \hline C_1A_1 + sC_1 & P_1C_1 & C_1B_1 + sP_1 & P_1^2 \end{array}\right) = tJ_{2v+8t}.$$

Из леммы 1 и соотношения (2) следует, что диагональные блоки полученной блочной матрицы имеют нужный вид. Таким образом, матрицы B_1 и C_1 должны удовлетворять следующей системе матричных уравнений:

$$\begin{cases} B_1C_1 = tJ_v, \\ B_1P_1 = tJ_{v,4t}, \\ P_1C_1 = tJ_{4t,v}, \\ A_1B_1 + sB_1 = tJ_{v,4t}, \\ C_1A_1 + sC_1 = tJ_{4t,v}, \\ C_1B_1 + sP_1 = tJ_{4t}. \end{cases} \tag{6}$$

Кроме того, из (5) и вида матриц A_1 и P_1 следует, что матрицы B_1 и C_1 должны удовлетворять условиям

$$B_1J_{4t} = 2tJ_{v,4t}, \quad J_vB_1 = kJ_{v,4t}, \quad C_1J_v = kJ_{4t,v}, \quad J_{4t}C_1 = 2tJ_{4t,v}. \tag{7}$$

Добавим два дополнительных условия, которым должны удовлетворять матрицы B_1 и C_1. Эти условия не являются необходимыми для существования орграфа G_2, но понадобятся для формирования следующих орграфов в последовательности:

1) если любую строку матрицы B_1 разделить на два блока длины $2t$, то получится ровно один блок, состоящий целиком из единиц, и ровно один блок, состоящий целиком из нулей;
2) если любой столбец матрицы C_1 разделить на два блока длины $2t$, то в каждом блоке будет ровно t единиц.

Для удобства назовём данные условия, накладываемые на матрицы B_1 и C_1, *условиями блочности* этих матриц.

Замечание 1. Если матрицы B_1 и C_1 удовлетворяют условиям блочности, то первые три равенства в (6) выполняются автоматически. Это следует из того, что матрица P_1 тоже удовлетворяет обоим приведённым условиям.

Таким образом, искомые матрицы B_1 и C_1 должны удовлетворять соотношениям в (6) и (7) и условиям блочности. Если удастся найти такие матрицы, то получим матрицу смежности A_2 сильно регулярного орграфа G_2. В п. 2 показано, как продолжить эту последовательность орграфов.

2. Рекуррентные формулы для построения семейства орграфов $\mathbf{dsrg}((v+(2^{n+1}-4)t)2^{n-1}, k+(2^n-2)t, t, \lambda, t)$

Введём новую операцию над матрицами. Пусть X — матрица размера $m \times l$. Обозначим через $\alpha_s(X)$ матрицу, полученную путём взятия первых m/s строк матрицы X (подразумевается, что m делится на s).

Дадим рекуррентное определение последовательности матриц P_n.

Лемма 2. Пусть P'_n — последовательность матриц, заданная следующим образом:

$$P'_1 = J_{2,1} \otimes K_2 \otimes J_{t,2t}, \quad P'_n = J_{2^n,1} \otimes K_2 \otimes \alpha_{2^{n-1}}(P'_{n-1}) \otimes J_{1,2}.$$

Тогда последовательность P'_n совпадает с определённой ранее последовательностью матриц P_n.

Доказательство. Индукция по n.

База индукции верна: $P'_1 = P_1$.

Пусть $P'_n = P_n$. Опираясь на соотношение (1), преобразуем P'_{n+1}:

$$P'_{n+1} = J_{2^{n+1},1} \otimes K_2 \otimes \alpha_{2^n}(P'_n) \otimes J_{1,2} =$$
$$= J_{2^{n+1},1} \otimes K_2 \otimes \alpha_{2^n}(J_{2^n,1} \otimes K_{2^n} \otimes J_{t,t\cdot 2^n}) \otimes J_{1,2} = J_{2^{n+1},1} \otimes K_2 \otimes K_{2^n} \otimes J_{t,t\cdot 2^n} \otimes J_{1,2} =$$
$$= J_{2^{n+1},1} \otimes K_{2^{n+1}} \otimes J_{t,t\cdot 2^{n+1}} = P_{n+1}.$$

Индукционный переход доказан. ■

Предположим, что нам удалось найти матрицы B_1 и C_1, удовлетворяющие соотношениям в (6) и (7) и условиям блочности (размеры этих матриц — $v \times 4t$ и $4t \times v$ соответственно). Построим две последовательности матриц B_n и C_n по следующим рекуррентным правилам (здесь используется блочное представление матриц):

$$B_n = \left(\frac{K_2 \otimes B_{n-1} \otimes J_{1,2}}{I_2 \otimes P_{n-1} \otimes J_{1,2}} \right) \text{ при } n \geqslant 2; \tag{8}$$

$$C_n = \left(\; J_{2^n,1} \otimes I_2 \otimes \alpha_{2^{n-1}}(C_{n-1}) \;\middle|\; J_{2^n,1} \otimes I_2 \otimes \alpha_{2^{n-1}}(P_{n-1}) \; \right) \text{ при } n \geqslant 2. \tag{9}$$

Нетрудно показать, что матрица B_n имеет размер $(v+(2^{n+1}-4)t)2^{n-1} \times t \cdot 4^n$, а матрица C_n — размер $t \cdot 4^n \times (v+(2^{n+1}-4)t)2^{n-1}$. Для этого можно воспользоваться индукцией по n.

Замечание 2. Операция $\alpha_{2^{n-1}}$ в определении последовательности C_n корректна, поскольку количество строк матрицы C_{n-1} делится на 2^{n-1} (корректность операции доказывается индуктивно). Кроме того, видно, что в определении операции α_{2^n} применительно к последовательности C_n можно было брать не первый блок строк матрицы, а любой другой.

Лемма 3. Матрицы B_n и C_n обладают следующими свойствами:

1) в каждой строке матрицы B_n ровно $t \cdot 2^n$ единиц;
2) в каждом столбце матрицы B_n ровно $k + (2^n - 2)t$ единиц;
3) в каждой строке матрицы C_n ровно $k + (2^n - 2)t$ единиц;
4) в каждом столбце матрицы C_n ровно $t \cdot 2^n$ единиц.

Доказательство. Индукция по n.

База индукции при $n = 1$ верна (см. (7)).

Индукционный переход доказывается достаточно просто: последовательности B_n и C_n определены рекуррентно при помощи произведения Кронекера, что позволяет

проследить, как меняется количество единиц в строках и столбцах матриц: нужно воспользоваться первым пунктом леммы 1 (в нём содержится информация о количестве единиц в строках и столбцах матрицы P_n). ■

Для построенных последовательностей матриц справедлива

Лемма 4.

1) Матрицы B_n и P_n обладают следующим свойством: если любую строку этих матриц разбить на идущие подряд блоки длины $t \cdot 2^n$, то получится ровно один блок, состоящий целиком из единиц, а все остальные блоки будут состоять целиком из нулей.
2) Матрицы C_n и P_n обладают следующим свойством: если любой столбец этих матриц разбить на идущие подряд блоки длины $t \cdot 2^n$, то в каждом блоке будет ровно t единиц.

Доказательство. Во-первых, заметим, что размеры матриц меняются таким образом, что разбиение строк (столбцов) на блоки нужной длины всегда можно корректно выполнить.

Справедливость приведённых свойств для матрицы P_n следует из формулы (1).

Тот факт, что последовательности B_n и C_n удовлетворяют заявленным свойствам, можно доказать индукцией по n.

База индукции при $n = 1$ верна, поскольку по предположению матрицы B_1 и C_1 удовлетворяют условиям блочности.

Индукционный переход следует из вида рекуррентных соотношений (8) и (9). Действительно, если в строке матрицы B_{n-1} (матрицы P_{n-1}) есть блок из единиц, то в матрице $K_2 \otimes B_{n-1} \otimes J_{1,2}$ (в матрице $I_2 \otimes P_{n-1} \otimes J_{1,2}$) он преобразуется в блок, в котором в 2 раза больше единиц. Пусть в столбцах матрицы C_{n-1} (матрицы P_{n-1}) каждый блок содержит по t единиц. Тогда матрица $\alpha_{2^{n-1}}(C_{n-1})$ (матрица $\alpha_{2^{n-1}}(P_{n-1})$) содержит первые блоки столбцов, а столбцы матрицы $J_{2^n,1} \otimes I_2 \otimes \alpha_{2^{n-1}}(C_{n-1})$ (матрицы $J_{2^n,1} \otimes I_2 \otimes \alpha_{2^{n-1}}(P_{n-1})$) можно разбить на блоки в 2 раза большей длины, которые по-прежнему содержат по t единиц. ■

Перейдём к главному результату работы.

Теорема 1. Пусть A_n — последовательность матриц, в которой A_1 — матрица смежности орграфа $\mathrm{dsrg}(v, k, t, \lambda, t)$, а при $n \geqslant 1$ верно, что

$$A_{n+1} = \begin{pmatrix} A_n & 0 & B_n & 0 \\ 0 & A_n & 0 & B_n \\ 0 & C_n & 0 & P_n \\ C_n & 0 & P_n & 0 \end{pmatrix} = \begin{pmatrix} I_2 \otimes A_n & I_2 \otimes B_n \\ K_2 \otimes C_n & K_2 \otimes P_n \end{pmatrix}, \tag{10}$$

где B_n, C_n и P_n — определённые ранее последовательности (предполагаем, что матрицы B_1 и C_1 существуют).

Тогда матрицы A_n являются матрицами смежности сильно регулярных орграфов с наборами параметров $((v + (2^{n+1} - 4)t)2^{n-1}, k + (2^n - 2)t, t, \lambda, t)$.

Доказательство. Введём обозначение для порядка матрицы A_n (нетрудно показать, что он будет именно такой):

$$v_n = (v + (2^{n+1} - 4)t)2^{n-1}.$$

Необходимо доказать два утверждения (см. определение 2):

1) в каждой строке и в каждом столбце матрицы A_n ровно $k + (2^n - 2)t$ единиц;
2) $A_n^2 + sA_n = tJ_{v_n}$.

Докажем первое утверждение индукцией по n. Для матриц A_1 и A_2 этот факт верен. Пусть в каждой строке и в каждом столбце матрицы A_n ровно $k + (2^n - 2)t$ единиц. Тогда, воспользовавшись леммой 1, леммой 3 и формулой (10), получаем, что в каждой строке и в каждом столбце матрицы A_{n+1} тоже нужное число единиц.

Доказательство второго утверждения тоже проведём индукцией по n.

База индукции доказана в п. 1 путём конструирования матрицы смежности орграфа $\mathrm{dsrg}(2v + 8t, k + 2t, t, \lambda, t)$ в приведённом в формуле (10) виде.

Предположим, что $A_n^2 + sA_n = tJ_{v_n}$. Преобразуем выражение $A_{n+1}^2 + sA_{n+1}$:

$$A_{n+1}^2 + sA_{n+1} = \left(\begin{array}{c|c|c|c} A_n^2 + sA_n & B_nC_n & A_nB_n + sB_n & B_nP_n \\ \hline B_nC_n & A_n^2 + sA_n & B_nP_n & A_nB_n + sB_n \\ \hline P_nC_n & C_nA_n + sC_n & P_n^2 & C_nB_n + sP_n \\ \hline C_nA_n + sC_n & P_nC_n & C_nB_n + sP_n & P_n^2 \end{array}\right).$$

Необходимо доказать, что все блоки полученной матрицы имеют вид tJ. Блоки, лежащие на главной диагонали, имеют нужный вид по индукционному предположению и по лемме 1. Таким образом, нужно доказать следующие шесть равенств:

$$B_nC_n = tJ_{v_n}; \tag{11}$$
$$B_nP_n = tJ_{v_n,t\cdot 4^n}; \tag{12}$$
$$P_nC_n = tJ_{t\cdot 4^n,v_n}; \tag{13}$$
$$A_nB_n + sB_n = tJ_{v_n,t\cdot 4^n}; \tag{14}$$
$$C_nA_n + sC_n = tJ_{t\cdot 4^n,v_n}; \tag{15}$$
$$C_nB_n + sP_n = tJ_{t\cdot 4^n}. \tag{16}$$

Справедливость равенств (11)–(13) автоматически следует из леммы 4. Опираясь на индукционное предположение, докажем равенства (14)–(16). В процессе доказательства будем также пользоваться леммами 1 и 2.

Равенство (14):

$$(A_n + sI_{v_n})B_n = \left(\begin{array}{c|c} I_2 \otimes (A_{n-1} + sI_{v_{n-1}}) & I_2 \otimes B_{n-1} \\ \hline K_2 \otimes C_{n-1} & K_2 \otimes P_{n-1} + sI_{2t\cdot 4^{n-1}} \end{array}\right)\left(\begin{array}{c} K_2 \otimes B_{n-1} \otimes J_{1,2} \\ \hline I_2 \otimes P_{n-1} \otimes J_{1,2} \end{array}\right) =$$
$$= \left(\frac{(I_2 \otimes (A_{n-1} + sI_{v_{n-1}}))(K_2 \otimes (B_{n-1} \otimes J_{1,2})) + (I_2 \otimes B_{n-1})(I_2 \otimes (P_{n-1} \otimes J_{1,2}))}{(K_2 \otimes C_{n-1})(K_2 \otimes (B_{n-1} \otimes J_{1,2})) + (K_2 \otimes P_{n-1} + sI_{2t\cdot 4^{n-1}})(I_2 \otimes (P_{n-1} \otimes J_{1,2}))}\right) =$$
$$= \left(\frac{K_2 \otimes ((A_{n-1} + sI_{v_{n-1}})(B_{n-1} \otimes J_{1,2})) + I_2 \otimes (B_{n-1}(P_{n-1} \otimes J_{1,2}))}{I_2 \otimes (C_{n-1}(B_{n-1} \otimes J_{1,2})) + K_2 \otimes (P_{n-1}(P_{n-1} \otimes J_{1,2})) + sI_2 \otimes P_{n-1} \otimes J_{1,2}}\right) =$$
$$= \left(\frac{K_2 \otimes ((A_{n-1} + sI_{v_{n-1}})B_{n-1}) \otimes J_{1,2} + I_2 \otimes (B_{n-1} \cdot P_{n-1}) \otimes J_{1,2}}{I_2 \otimes (C_{n-1}B_{n-1} + sP_{n-1}) \otimes J_{1,2} + K_2 \otimes (P_{n-1} \cdot P_{n-1}) \otimes J_{1,2}}\right) =$$
$$= \left(\frac{K_2 \otimes tJ_{v_{n-1},t\cdot 4^{n-1}} \otimes J_{1,2} + I_2 \otimes tJ_{v_{n-1},t\cdot 4^{n-1}} \otimes J_{1,2}}{I_2 \otimes tJ_{t\cdot 4^{n-1}} \otimes J_{1,2} + K_2 \otimes tJ_{t\cdot 4^{n-1}} \otimes J_{1,2}}\right) = \left(\frac{J_2 \otimes tJ_{v_{n-1},t\cdot 4^{n-1}} \otimes J_{1,2}}{J_2 \otimes tJ_{t\cdot 4^{n-1}} \otimes J_{1,2}}\right) =$$
$$= tJ_{v_n,t\cdot 4^n}.$$

Равенство (15):

$$C_n(A_n + sI_{v_n}) = \left(J_{2^n,1} \otimes I_2 \otimes \alpha_{2^{n-1}}(C_{n-1}) \;\middle|\; J_{2^n,1} \otimes I_2 \otimes \alpha_{2^{n-1}}(P_{n-1})\right) \times$$
$$\times \left(\begin{array}{c|c} I_2 \otimes (A_{n-1} + sI_{v_{n-1}}) & I_2 \otimes B_{n-1} \\ \hline K_2 \otimes C_{n-1} & K_2 \otimes P_{n-1} + sI_{2t\cdot 4^{n-1}} \end{array}\right) =$$
$$= \left(((J_{2^n,1}\otimes I_2)\otimes\alpha_{2^{n-1}}(C_{n-1}))(I_2\otimes(A_{n-1}+sI_{v_{n-1}}))+((J_{2^n,1}\otimes I_2)\otimes\alpha_{2^{n-1}}(P_{n-1}))(K_2\otimes C_{n-1}) \;\middle|\right.$$
$$\left. \;\middle|\; ((J_{2^n,1}\otimes I_2)\otimes\alpha_{2^{n-1}}(C_{n-1}))(I_2\otimes B_{n-1})+((J_{2^n,1}\otimes I_2)\otimes\alpha_{2^{n-1}}(P_{n-1}))(K_2\otimes P_{n-1}+sI_{2t\cdot 4^{n-1}})\right) =$$
$$= \left(((J_{2^n,1} \otimes I_2)I_2) \otimes (\alpha_{2^{n-1}}(C_{n-1})(A_{n-1}+sI_{v_{n-1}}))+((J_{2^n,1} \otimes I_2)K_2) \otimes (\alpha_{2^{n-1}}(P_{n-1})C_{n-1}) \;\middle|\right.$$
$$\left. \;\middle|\; ((J_{2^n,1} \otimes I_2)I_2) \otimes (\alpha_{2^{n-1}}(C_{n-1})B_{n-1}) + ((J_{2^n,1} \otimes I_2)K_2) \otimes (\alpha_{2^{n-1}}(P_{n-1})P_{n-1})+\right.$$
$$\left.+sJ_{2^n,1} \otimes I_2 \otimes \alpha_{2^{n-1}}(P_{n-1})\right) =$$
$$= \left(J_{2^n,1} \otimes I_2 \otimes \alpha_{2^{n-1}}(tJ_{t\cdot 4^{n-1},v_{n-1}}) + J_{2^n,1} \otimes K_2 \otimes \alpha_{2^{n-1}}(tJ_{t\cdot 4^{n-1},v_{n-1}}) \;\middle|\right.$$
$$\left. \;\middle|\; J_{2^n,1} \otimes I_2 \otimes \alpha_{2^{n-1}}(tJ_{t\cdot 4^{n-1}}) + J_{2^n,1} \otimes K_2 \otimes \alpha_{2^{n-1}}(tJ_{t\cdot 4^{n-1}})\right) =$$
$$= \left(J_{2^n,1} \otimes J_2 \otimes \alpha_{2^{n-1}}(tJ_{t\cdot 4^{n-1},v_{n-1}}) \;\middle|\; J_{2^n,1} \otimes J_2 \otimes \alpha_{2^{n-1}}(tJ_{t\cdot 4^{n-1}})\right) = tJ_{t\cdot 4^n,v_n}.$$

Равенство (16):

$$C_nB_n + sP_n = \left(J_{2^n,1} \otimes I_2 \otimes \alpha_{2^{n-1}}(C_{n-1}) \;\middle|\; J_{2^n,1} \otimes I_2 \otimes \alpha_{2^{n-1}}(P_{n-1})\right) \times$$
$$\times \left(\begin{array}{c} K_2 \otimes B_{n-1} \otimes J_{1,2} \\ \hline I_2 \otimes P_{n-1} \otimes J_{1,2} \end{array}\right) + sJ_{2^n,1} \otimes K_2 \otimes \alpha_{2^{n-1}}(P_{n-1}) \otimes J_{1,2} =$$
$$= ((J_{2^n,1} \otimes I_2) \otimes \alpha_{2^{n-1}}(C_{n-1}))(K_2 \otimes (B_{n-1} \otimes J_{1,2}))+$$
$$+((J_{2^n,1} \otimes I_2) \otimes \alpha_{2^{n-1}}(P_{n-1}))(I_2 \otimes (P_{n-1} \otimes J_{1,2})) + sJ_{2^n,1} \otimes K_2 \otimes \alpha_{2^{n-1}}(P_{n-1}) \otimes J_{1,2} =$$
$$= ((J_{2^n,1} \otimes I_2)K_2) \otimes (\alpha_{2^{n-1}}(C_{n-1})(B_{n-1} \otimes J_{1,2}))+$$
$$+((J_{2^n,1} \otimes I_2)I_2) \otimes (\alpha_{2^{n-1}}(P_{n-1})(P_{n-1} \otimes J_{1,2})) + sJ_{2^n,1} \otimes K_2 \otimes \alpha_{2^{n-1}}(P_{n-1}) \otimes J_{1,2} =$$
$$= J_{2^n,1} \otimes K_2 \otimes \alpha_{2^{n-1}}(tJ_{t\cdot 4^{n-1}}) \otimes J_{1,2} + J_{2^n,1} \otimes I_2 \otimes \alpha_{2^{n-1}}(tJ_{t\cdot 4^{n-1}}) \otimes J_{1,2} =$$
$$= J_{2^n,1} \otimes J_2 \otimes \alpha_{2^{n-1}}(tJ_{t\cdot 4^{n-1}}) \otimes J_{1,2} = tJ_{t\cdot 4^n}.$$

Теорема 1 доказана. ■

3. Результаты работы программы

Для поиска семейств сильно регулярных орграфов по описанному методу написана программа на языке Julia. На вход она принимает матрицу смежности A_1 первого орграфа в последовательности, далее осуществляется поиск матрицы A_2 нужного вида и, если поиск завершился успешно, по рекуррентной формуле (см. теорему 1) строятся матрицы смежности $A_3, \ldots, A_6$.

Для формирования матрицы A_2 выполняется поиск бинарных матриц B_1 и C_1, которые удовлетворяют соотношениям (6) и (7) и условиям блочности. Для упрощения поиска применена библиотека оптимизации Artelys Knitro [7] (использована бесплатная пробная версия). В качестве целевой функции была взята формальная функция $F = 1$, а все условия, накладываемые на матрицы B_1 и C_1, добавлены как ограничения в оптимизационную задачу. Благодаря эффективным алгоритмам Artelys Knitro, используемым для нахождения точки в области допустимых решений, удалось избежать полного перебора при поиске матриц B_1 и C_1. Исходный код программы и матрицы смежности полученных орграфов доступны в репозитории [8].

Результаты работы программы приведены в таблице, где указаны параметры первых двух орграфов и параметры n-го члена последовательности. Во втором столбце

обведены те наборы параметров, для которых вопрос существования соответствующих орграфов ранее был открыт (согласно таблице на сайте [5] на момент написания работы).

В последнем столбце таблицы приводится время поиска второго орграфа в последовательности при помощи библиотеки Artelys Knitro. Запуск программы осуществлялся на компьютере с процессором Intel Core i5-7400 (3.00 ГГц), объём оперативной памяти равен 32 Гбайт (для разных наборов параметров использовались разные настройки библиотеки Artelys Knitro).

Обнаруженные семейства сильно регулярных орграфов

Параметры G_1	Параметры G_2	Параметры G_n	Время поиска G_2, с
$(6,3,2,1,2)$	$(28,7,2,1,2)$	$(2^n(2^{n+1}-1), 2^{n+1}-1, 2, 1, 2)$	3,89
$(8,4,3,1,3)$	$(40,\ 10,\ 3,\ 1,\ 3)$	$(2^n(3\cdot 2^n-2), 3\cdot 2^n-2, 3, 1, 3)$	4,03
$(10,5,3,2,3)$	$(44,11,3,2,3)$	$(2^n(3\cdot 2^n-1), 3\cdot 2^n-1, 3, 2, 3)$	9,27
$(12,6,4,2,4)$	$(56,14,4,2,4)$	$(2^n(4\cdot 2^n-2), 4\cdot 2^n-2, 4, 2, 4)$	16,23
$(14,7,4,3,4)$	$(60,15,4,3,4)$	$(2^n(4\cdot 2^n-1), 4\cdot 2^n-1, 4, 3, 4)$	2496,14
$(16,8,5,3,5)$	$(72,\ 18,\ 5,\ 3,\ 5)$	$(2^n(5\cdot 2^n-2), 5\cdot 2^n-2, 5, 3, 5)$	52,38
$(18,9,5,4,5)$	$(76,\ 19,\ 5,\ 4,\ 5)$	$(2^n(5\cdot 2^n-1), 5\cdot 2^n-1, 5, 4, 5)$	840,40
$(18,9,6,3,6)$	$(84,21,6,3,6)$	$(2^n(6\cdot 2^n-3), 6\cdot 2^n-3, 6, 3, 6)$	233,92
$(20,10,6,4,6)$	$(88,22,6,4,6)$	$(2^n(6\cdot 2^n-2), 6\cdot 2^n-2, 6, 4, 6)$	151,42
$(22,11,6,5,6)$	$(92,\ 23,\ 6,\ 5,\ 6)$	$(2^n(6\cdot 2^n-1), 6\cdot 2^n-1, 6, 5, 6)$	1260,85
$(24,12,7,5,7)$	$(104,\ 26,\ 7,\ 5,\ 7)$	$(2^n(7\cdot 2^n-2), 7\cdot 2^n-2, 7, 5, 7)$	525,10

Программа запускалась и для наборов параметров, которые не приведены в таблице, однако в других случаях поиск матрицы A_2 не завершился успехом.

Отметим, что все сильно регулярные орграфы G_1, для которых описанный метод сработал, имеют параметры вида $(2(t+\lambda), t+\lambda, t, \lambda, t)$. Авторам пока неизвестно, работает ли метод для наборов параметров, имеющих другой вид, или такое соотношение между параметрами является необходимым условием применимости описанного подхода.

Заключение

В работе рассмотрена конструкция, при помощи которой возможно построение бесконечных последовательностей сильно регулярных орграфов. Чтобы воспользоваться этой конструкцией, необходимо взять матрицу смежности A_1 первого орграфа в последовательности и выразить матрицу смежности A_2 второго орграфа через A_1 в определённом виде. Если получается это сделать, то другие орграфы в последовательности можно найти по доказанной рекуррентной формуле. При помощи описанного метода построено 11 последовательностей сильно регулярных орграфов; как минимум для пяти наборов параметров впервые найдены соответствующие сильно регулярные орграфы.

Авторы видят определённую перспективу дальнейших исследований в поиске условий, которым должен удовлетворять граф G_1, чтобы приведённый в работе приём сработал, и поиске способа выразить матрицу A_2 через матрицу A_1 без использования компьютерной программы.

ЛИТЕРАТУРА

1. *Bose R. C.* Strongly regular graphs, partial geometries and partially balanced designs // Pacific J. Math. 1963. V. 13. No. 2. P. 389–419.

2. *Brouwer A. E. and Maldeghem H. V.* Strongly Regular Graphs. Cambridge: Cambridge University Press, 2022. 425 p.
3. *Duval A. M.* A directed graph version of strongly regular graphs // J. Combinatorial Theory. Ser. A. 1988. V. 47. No. 1. P. 71–100.
4. *Jørgensen L. K.* Non-existence of directed strongly regular graphs // Discrete Math. 2003. V. 264. No. 1–3. P. 111–126.
5. `https://homepages.cwi.nl/~aeb/math/dsrg/dsrg.html` — Parameters of directed strongly regular graphs. 2025.
6. *Zhang H. and Ding F.* On the Kronecker products and their applications // J. Appl. Math. 2013. V. 2013. P. 1–8.
7. `https://www.artelys.com/solvers/knitro/` — Artelys Knitro. 2025.
8. `https://github.com/byzovv/dsrg_recurrent` — Explicit construction of infinite families of strongly regular digraphs. 2025.

REFERENCES

1. *Bose R. C.* Strongly regular graphs, partial geometries and partially balanced designs. Pacific J. Math., 1963, vol. 13, no. 2, pp. 389–419.
2. *Brouwer A. E. and Maldeghem H. V.* Strongly Regular Graphs. Cambridge, Cambridge University Press, 2022. 425 p.
3. *Duval A. M.* A directed graph version of strongly regular graphs. J. Combinatorial Theory, ser. A, 1988, vol. 47, no. 1, pp. 71–100.
4. *Jørgensen L. K.* Non-existence of directed strongly regular graphs. Discrete Math., 2003, vol. 264, no. 1–3, pp. 111–126.
5. `https://homepages.cwi.nl/~aeb/math/dsrg/dsrg.html` — Parameters of directed strongly regular graphs, 2025.
6. *Zhang H. and Ding F.* On the Kronecker products and their applications. J. Appl. Math., 2013, vol. 2013, pp. 1–8.
7. `https://www.artelys.com/solvers/knitro/` — Artelys Knitro, 2025.
8. `https://github.com/byzovv/dsrg_recurrent` — Explicit construction of infinite families of strongly regular digraphs, 2025.

МАТЕМАТИЧЕСКИЕ ОСНОВЫ ИНФОРМАТИКИ И ПРОГРАММИРОВАНИЯ

УДК 510.52 DOI 10.17223/20710410/69/8

О ГЕНЕРИЧЕСКОЙ СЛОЖНОСТИ ПРОБЛЕМ 3-РАСКРАСКИ ГРАФОВ[1]

Д. П. Рузанова, А. Н. Рыбалов

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

E-mail: alexander.rybalov@gmail.com

Изучается генерическая сложность двух вариантов проблемы о 3-раскраске графов: проблема распознавания и проблема поиска 3-раскраски графа. Для обеих проблем эффективных полиномиальных алгоритмов неизвестно. Проблема поиска 3-раскраски используется в известном криптографическом протоколе Блюма для доказательства с нулевым разглашением. Предлагается полиномиальный генерический алгоритм для проблемы распознавания 3-раскраски графа. Для проблемы поиска 3-раскраски доказывается, что если $P \neq NP$ и $P = BPP$, то существует подпроблема этой проблемы, для которой нет полиномиального генерического алгоритма. Полученный результат является теоретическим обоснованием применения проблемы поиска 3-раскраски графа в криптографии, где нужно, чтобы проблема взлома криптоалгоритма была трудной для почти всех входов.

Ключевые слова: *генерическая сложность, 3-раскраска графа.*

ON THE GENERIC COMPLEXITY OF GRAPH 3-COLORING PROBLEMS

D. P. Ruzanova, A. N. Rybalov

Sobolev Institute of Mathematics, Omsk, Russia

In this paper, we study the generic complexity of two versions of the graph 3-coloring problem: the graph 3-coloring recognition problem and the graph 3-coloring search problem. For both problems, no efficient polynomial algorithms are known. The 3-coloring search problem is used in the well-known Blum zero-knowledge cryptographic protocol. We propose a polynomial generic algorithm for the graph 3-coloring recognition problem. For the 3-coloring search problem, we prove that if $P \neq NP$ and $P = BPP$, then there is a subproblem of this problem for which there is no polynomial generic algorithm. The obtained result provides theoretical justification for applying the 3-coloring search problem in cryptography, an application where breaking a cryptographic algorithm must be difficult for almost all inputs. To prove this theorem, we use the method of generic amplification, which allows to construct generically hard problems from the problems hard in the classical sense.

Keywords: *generic complexity, 3-coloring of graphs.*

[1]Работа поддержана грантом Российского научного фонда № 25-11-20023.

Введение

Проблема о 3-раскраске графов является классической комбинаторной проблемой, изучаемой многие десятилетия. Её формулировка состоит в следующем: по заданному произвольному графу определить, можно ли раскрасить все его вершины в три цвета так, чтобы любые две вершины, соединённые ребром, были раскрашены в разные цвета. Эта проблема содержится в классическом списке из двадцати одной NP-полной проблемы из знаменитой работы Р. Карпа [1], откуда следует, что при условии неравенства классов сложности P и NP для проблемы о 3-раскраске не существует эффективных полиномиальных алгоритмов. Этот факт открывает возможности для применения данной проблемы в криптографии. Например, проблема о 3-раскраске используется в протоколе Блюма [2] для доказательства с нулевым разглашением [3].

Однако трудноразрешимости в классическом смысле в современной криптографии недостаточно. Важно, чтобы алгоритмическая проблема, лежащая в основе стойкости криптографического протокола, являясь (гипотетически) трудной в классическом смысле, оставалась трудной и в генерическом смысле [4], т. е. для почти всех входов. Это объясняется тем, что при случайной генерации ключей в криптографическом алгоритме происходит генерация входа алгоритмической проблемы, лежащей в основе алгоритма. Если эта проблема будет легкоразрешимой почти всегда, то для почти всех таких входов её можно 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 [5], дискретного логарифма [6], извлечения корня в группах вычетов [7] (проблема обращения функции RSA).

В данной работе изучается генерическая сложность двух вариантов проблемы о 3-раскраске графов. Первый вариант — проблема распознавания 3-раскраски графа. Здесь входом является произвольный граф, необходимо определить, существует ли для него 3-раскраска. Второй вариант — проблема поиска 3-раскраски графа. Для этой проблемы входом является граф, для которого заведомо существует 3-раскраска, нужно хотя бы одну такую 3-раскраску найти. Проблемы поиска, в отличие от проблем распознавания, находят применения в криптографии, где всегда известно, что решение есть и надо его найти. Для обеих проблем неизвестно эффективных полиномиальных алгоритмов. В работе предлагается полиномиальный генерический алгоритм для проблемы распознавания 3-раскраски графа. Для проблемы поиска 3-раскраски доказывается, что если $\mathrm{P} \neq \mathrm{NP}$ и $\mathrm{P} = \mathrm{BPP}$, то существует подпроблема этой проблемы, для которой нет полиномиального генерического алгоритма. 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 [8].

1. Предварительные сведения

Рассмотрим неориентированные графы без петель и кратных рёбер. Граф G — это пара (V, E), где V — множество вершин; $E \subseteq V \times V$ — множество рёбер графа G. Для любого множества A через $|A|$ будем обозначать его мощность.

Пусть имеются два графа $G_1 = (V_1, E_1)$ и $G_2 = (V_2, E_2)$. Биекция $\varphi : V_1 \to V_2$ называется *изоморфизмом* графов G_1 и G_2, если для любых $v_1, v_2 \in V_1$ имеет место

$(v_1, v_2) \in E_1$ тогда и только тогда, когда $(\varphi(v_1), \varphi(v_2)) \in E_2$. При этом графы G_1 и G_2 называются *изоморфными*, что обозначается как $G_1 \cong G_2$.

3-Раскраской графа G называется присваивание каждой вершине графа одного из трёх цветов, такое, что любые две вершины графа, соединённые ребром, раскрашены в разные цвета. Если для графа существует 3-раскраска, будем называть его *3-раскрашиваемым*. Существование 3-раскраски графа $G = (V, E)$ эквивалентно тому, что множество вершин можно разбить на три непересекающихся подмножества (возможно, пустые) $V = V_1 \cup V_2 \cup V_3$, такие, что любые две вершины из каждого подмножества V_i, $i = 1, 2, 3$, не соединены ребром.

Проблема распознавания 3-раскраски состоит в следующем: по произвольному заданному графу G определить, существует ли для него 3-раскраска. *Проблема поиска 3-раскраски* определяется несколько иначе: по произвольному заданному 3-раскрашиваемому графу G найти хотя бы одну 3-раскраску.

Под *размером* графа G будем понимать число вершин.

Определения полиномиальных детерминированных и вероятностных алгоритмов, а также вычислительных классов P, NP и BPP можно найти в [9].

Напомним основные определения генерического подхода [4]. Пусть I — некоторое множество входов, I_n — подмножество входов размера n. Для подмножества $S_n \subseteq I$ определим последовательность

$$\rho_n(S) = \frac{|S_n|}{|I_n|}, \quad n = 1, 2, 3, \ldots,$$

где $S_n = S \cap I_n$ — множество входов из S размера n. *Асимптотической плотностью* S назовём предел

$$\rho(S) = \lim_{n \to \infty} \rho_n(S).$$

Множество S называется *пренебрежимым*, если $\rho(S) = 0$.

Алгоритм $\mathcal{A}$ с множеством входов I и множеством выходов $J \cup \{\square\}$ $(\square \notin J)$ называется *генерическим*, если

1) $\mathcal{A}$ останавливается на всех входах из I;
2) множество $\{x \in I : \mathcal{A}(x) = \square\}$ является пренебрежимым.

Здесь символ $\square$ обозначает неопределённый ответ. Генерический алгоритм $\mathcal{A}$ *вычисляет* функцию $f : I \to \mathbb{N}$, если для всех $x \in I$ выполнено

$$(\mathcal{A}(x) \neq \square) \Rightarrow (f(x) = \mathcal{A}(x)).$$

Проблема распознавания множества $A \subseteq I$ *генерически разрешима за полиномиальное время*, если существует полиномиальный генерический алгоритм, вычисляющий характеристическую функцию множества A. Напомним, что *характеристической функцией* множества $A \subseteq I$ называется функция $\chi_A : I \to \{0, 1\}$, определённая следующим образом:

$$\chi_A(x) = \begin{cases} 1, & \text{если } x \in A, \\ 0, & \text{если } x \notin A. \end{cases}$$

2. Протокол Блюма

Доказательство с нулевым разглашением [3] — интерактивный вероятностный протокол между двумя акторами: Доказывающим (Prover) и Проверяющим (Verifier), позволяющий доказать, что некоторое утверждение верно, не предоставляя никакой информации о самом доказательстве данного утверждения. Данный криптографический протокол обладает тремя свойствами:

1) Полнотой: если утверждение действительно истинно, то Доказывающий убедит в этом Проверяющего с любой наперёд заданной точностью.
2) Корректностью: если утверждение неверно, то любой, даже «нечестный», Доказывающий не сможет убедить Проверяющего, за исключением пренебрежимо малой вероятности.
3) Нулевым разглашением: если утверждение верно, то любой, даже «нечестный», Проверяющий не узнает ничего, кроме самого факта, что утверждение верно.

М. Блюмом в [2] предложен протокол доказательства с нулевым разглашением, основанный на использовании вычислительно трудных проблем теории графов. Опишем этот протокол для проблемы 3-раскраски графов. Назовём проверяющую сторону Виктор (Verifier), а доказывающую — Полина (Prover). Полина знает 3-раскраску в некотором большом графе G. Виктору известен граф G, но он не знает его 3-раскраски. Полина хочет доказать Виктору, что она знает 3-раскраску, не выдавая при этом ни самой 3-раскраски, ни какой-либо другой информации о ней. Виктор хочет удостовериться, что Полина действительно знает 3-раскраску.

Для этого Виктор и Полина совместно выполняют несколько раундов протокола:

1) Полина генерирует граф H, изоморфный G. Преобразование 3-раскраски между изоморфными графами — простая задача, поэтому если Полине известна 3-раскраска G, то она также знает 3-раскраску в графе H.
2) Полина передаёт граф H Виктору.
3) Виктор выбирает случайный бит $b \in \{0, 1\}$.
4) Если $b = 0$, то Виктор просит Полину доказать изоморфизм G и H, то есть предоставить соответствующую биекцию вершин этих двух графов. Виктор может проверить, действительно ли G и H изоморфны.
5) Если $b = 1$, то Виктор просит Полину указать 3-раскраску H. Для проблемы изоморфизма графов на данный момент неизвестно полиномиальных алгоритмов, поэтому практически невозможно по 3-раскраске графа H найти 3-раскраску изоморфного ему графа G.

Проверим выполнение свойств доказательства с нулевым разглашением.

В каждом раунде Виктор выбирает новый случайный бит, который неизвестен Полине, поэтому, чтобы Полина могла ответить на оба вопроса, нужно, чтобы H был в самом деле изоморфен G и Полина должна знать 3-раскраску для H (а значит, и для G). Поэтому после достаточного числа раундов Виктор может быть уверен в том, что у Полины есть 3-раскраска G. С другой стороны, Полина не раскрывает никакой информации о 3-раскраске G. Более того, Виктору сложно будет доказать кому-либо ещё, что он сам или Полина знают 3-раскраску G.

Предположим, что Полине неизвестна 3-раскраска G, но она хочет обмануть Виктора. Тогда Полине необходим неизоморфный G граф G', в котором она знает 3-раскраску. В каждом раунде она может передавать Виктору либо граф H' — изоморфный G', либо граф H — изоморфный G. Если Виктор попросит доказать изоморфизм графов и ему был передан H, то обман не вскроется. Аналогично — если он попросит показать 3-раскраску и ему был передан H'. Вероятность того, что Полина обманет Виктора после k раундов, равна 2^{-k}, что близко к нулю при достаточном числе раундов.

Предположим, что Виктор не знает 3-раскраску, но хочет доказать третьей стороне (Борису), что Полина её знает. Если Виктор, например, заснял на видео все раунды протокола, Борис едва ли ему поверит: он может предположить, что Виктор и Полина в сговоре и в каждом раунде Виктор заранее сообщал Полине свой выбор случайного

бита, чтобы Полина могла передавать ему H для проверок изоморфизма и H' для проверок 3-раскраски. Таким образом, без участия Полины доказать, что она знает 3-раскраску, можно, лишь доказав, что во всех раундах протокола выбирались действительно случайные биты.

3. Генерический алгоритм распознавания 3-раскраски

Граф будем представлять матрицей смежности (достаточно только верхней её половины). Для краткости эти верхние половины матриц будем называть просто матрицами. Обозначим через $\mathcal{G}$ множество всех графов, через $\mathcal{G}_n$ — множество графов размера n. Легко подсчитать, что $|\mathcal{G}_n| = 2^{n(n-1)/2}$.

Теорема 1. Проблема распознавания 3-раскраски графов генерически разрешима за полиномиальное время.

Доказательство. Полиномиальный генерический алгоритм для распознавания 3-раскраски графов работает на графе G размера n следующим образом:

1) Ищет в графе G клику K_4 размера 4. Это делается перебором всевозможных подмножеств вершин G размера 4 и проверки того, что все они друг с другом соединены ребрами. Число таких подмножеств $\mathrm{C}_n^4 = O(n^4)$ полиномиально.
2) Если клика нашлась, то выдаёт ответ «НЕТ».
3) Если клики нет, то выдаёт ответ «НЕ ЗНАЮ».

Очевидно, что граф K_4 нельзя раскрасить в три цвета, а значит, если он является подграфом графа G, то и граф G также нельзя раскрасить тремя цветами.

Для доказательства генеричности алгоритма покажем, что множество графов, не содержащих подграфа K_4 (обозначим это множество S), является пренебрежимым. Рассмотрим множество графов S', в которых на вершинах $\{1,\ldots,n\}$ запрещены клики на вершинах $\{1,\ldots,4\}$, на вершинах $\{5,\ldots,8\}$, …, на вершинах $\{4([n/4]-1)+1, \ldots, 4[n/4]\}$. Так как для графов из S' запрещены не любые клики размера 4, то множество S содержится в S': $S \subseteq S'$.

Можно подсчитать, что

$$|S'_n| = 2^{n(n-1)/2-6[n/4]}(2^6-1)^{[n/4]}.$$

Это следует из того, что в матрицах смежности графов из множества S' над диагональю «запрещены» $[n/4]$ подматриц размера 4, состоящих из единиц. Эти 4×4-матрицы имеют $4(4-1)/2 = 6$ мест для расстановки нулей и единиц. Тогда

$$\rho(S') = \lim_{n\to\infty}\frac{|S'_n|}{|\mathcal{G}_n|} = \lim_{n\to\infty}\frac{2^{n(n-1)/2-6[n/4]}(2^6-1)^{[n/4]}}{2^{n(n-1)/2}} =$$
$$= \lim_{n\to\infty}\frac{(2^6-1)^{[n/4]}}{2^{6[n/4]}} = \lim_{n\to\infty}\left(1-\frac{1}{2^6}\right)^{[n/4]} = 0.$$

Это доказывает, что множество S' является пренебрежимым, а значит, его подмножество S тем более пренебрежимо. ■

4. Проблема поиска 3-раскраски

Напомним, что проблема поиска 3-раскраски состоит в том, что по произвольному 3-раскрашиваемому графу $G = (V, E)$ нужно найти хотя бы одну его 3-раскраску, то есть непересекающиеся подмножества V_1, V_2, V_3, такие, что $V_1 \sqcup V_2 \sqcup V_3 = V$ и $\forall x, y \in V_i\big((x,y) \notin E\big)$, $i \in \{1,2,3\}$. Будем обозначать эту проблему $\mathcal{SC}_3$. Для неё также неизвестно полиномиальных алгоритмов.

Рассмотрим бесконечную последовательность графов $\gamma = \{G_1, G_2, \ldots, G_n, \ldots\}$, такую, что G_n имеет n вершин, $n \in \mathbb{N}$. Для каждой последовательности γ определим подпроблему поиска 3-раскраски $\mathcal{SC}_3(\gamma)$ как ограничение исходной проблемы $\mathcal{SC}_3$ на множество входов $\{G : G \cong G_n, G_n \in \gamma, n \in \mathbb{N}\}$.

Лемма 1. Если не существует полиномиального вероятностного алгоритма для решения проблемы $\mathcal{SC}_3$, то найдётся последовательность графов γ, такая, что не существует полиномиального вероятностного алгоритма для решения проблемы $\mathcal{SC}_3(\gamma)$.

Доказательство. Пусть $P_1, P_2, \ldots$ — все полиномиальные вероятностные алгоритмы. Если не существует полиномиального вероятностного алгоритма для проблемы $\mathcal{SC}_3$, то для любого вероятностного полиномиального алгоритма P_n найдётся бесконечно много графов, для которых алгоритм P_n не может решить $\mathcal{SC}_3$. Из этого следует, что можно выбрать такую последовательность $\gamma' = \{G_1, G_2, \ldots, G_n, \ldots\}$, что алгоритм P_n не может решить $\mathcal{SC}_3$ для G_n для всех n. Более того, γ' упорядочена по возрастанию числа вершин в графах. Теперь можно расширить последовательность γ' до последовательности графов γ с графами G_n для всех размеров n. Из построения γ следует, что не существует полиномиального вероятностного алгоритма для решения проблемы $\mathcal{SC}_3(\gamma)$. ■

Отметим, что множество всех входов размера n для проблемы $\mathcal{SC}_3(\gamma)$ выглядит так: $I_n = \{G : G \cong G_n, G_n \in \gamma\}$.

Теорема 2. Пусть γ — произвольная последовательность графов. Если существует генерический полиномиальный алгоритм, решающий проблему $\mathcal{SC}_3(\gamma)$, то существует вероятностный полиномиальный алгоритм, решающий эту проблему на всём множестве входов.

Доказательство. Допустим, что существует генерический полиномиальный алгоритм $\mathcal{A}$, решающий проблему поиска 3-раскраски графов $\mathcal{SC}_3(\gamma)$. Построим вероятностный полиномиальный алгоритм $\mathcal{B}$, решающий эту проблему на всём множестве входов. На графе G с n вершинами алгоритм $\mathcal{B}$ работает следующим образом:

1) Запускает алгоритм $\mathcal{A}$ на G.
2) Если $\mathcal{A}(G) \neq \square$, то $\mathcal{B}$ выдаёт ответ $\mathcal{A}(G)$ и останавливается, иначе идёт на шаг 3.
3) Генерирует случайно и равномерно перестановку π на вершинах $\{1, \ldots, n\}$ и вычисляет граф $G' = \pi(G)$.
4) Запускает алгоритм $\mathcal{A}$ на графе G'.
5) Если $\mathcal{A}(G') = \square$, то выдаёт ответ $V_1 = \{1, 2, \ldots, [n/3]\}$, $V_2 = \{[n/3] + 1, \ldots, [2n/3]\}$, $V_3 = \{[2n/3] + 1, \ldots, n\}$ (возможно, неправильный).
6) Пусть $\mathcal{A}(G') = \{V_1, V_2, V_3\}$ — решение задачи 3-раскраски для графа G'. Тогда

$$\pi(V) = \pi^{-1}(V_1) \sqcup \pi^{-1}(V_2) \sqcup \pi^{-1}(V_3)$$

является решением задачи 3-раскраски для исходного графа $G = \pi^{-1}(G')$.

Для доказательства корректности работы вероятностного алгоритма надо показать, что вероятность того, что $A(G') = \square$, меньше $1/3$. Заметим, что $\pi(G)$ при варьировании перестановки π пробегает всё множество входов размера n. Множество $\{G : A(G) = \square\}$ пренебрежимо, поэтому вероятность того, что $A(G') = \square$, стремится к 0 при увеличении n. ■

Теорема 3. Если P $\neq$ NP и P = BPP, то существует последовательность графов γ, такая, что для решения проблемы поиска 3-раскраски $\mathcal{SC}_3(\gamma)$ не существует генерического полиномиального алгоритма.

Доказательство. Покажем сначала, что при условиях P $\neq$ NP и P = BPP не существует полиномиального вероятностного алгоритма для решения проблемы $\mathcal{SC}_3$. Действительно, пусть такой алгоритм существует. Так как проблема $\mathcal{SC}_3$ является NP-трудной, то существует полиномиально эквивалентная ей NP-проблема распознавания A. Из полиномиального вероятностного алгоритма для $\mathcal{SC}_3$ легко получается полиномиальный вероятностный алгоритм для решения проблемы A. А так как P = BPP, то существует и детерминированный полиномиальный алгоритм для A, откуда P = NP. Противоречие. Теперь нужное утверждение следует из леммы 1 и теоремы 2. ■

Авторы выражают благодарность рецензенту за полезные замечания и предложения по улучшению текста статьи.

ЛИТЕРАТУРА

1. *Karp R.* Reducibility among combinatorial problems // R. E. Miller, J. W. Thatcher, and J. D. Bohlinger (eds). Complexity of Computer Computations. The IBM Research Symposia Series. Boston: Springer, 1972. P. 85–103.
2. *Blum M.* How to prove a theorem so no one else can claim it // Proc. ICM'86. AMS, 1986. P. 1444–1451.
3. *Goldreich O., Micali S., and Wigderson A.* Proofs that yield nothing but their validity or all languages in NP have zero-knowledge proof systems // Proc. SFCS'86. IEEE Computer Society, 1986. P. 174–187.
4. *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.
5. *Рыбалов А. Н.* О генерической сложности проблемы распознавания квадратичных вычетов // Прикладная дискретная математика. 2015. № 2 (28). С. 54–58.
6. *Рыбалов А. Н.* О генерической сложности проблемы дискретного логарифма // Прикладная дискретная математика. 2016. № 3 (33). С. 93–97.
7. *Рыбалов А. Н.* О генерической сложности проблемы извлечения корня в группах вычетов // Прикладная дискретная математика. 2017. № 38. С. 95–100.
8. *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.
9. *Китаев А., Шень А., Вялый М.* Классические и квантовые вычисления. М.: МЦНМО, ЧеРо. 1999. 192 с.

REFERENCES

1. *Karp R.* Reducibility among combinatorial problems. R. E. Miller, J. W. Thatcher, and J. D. Bohlinger (eds). Complexity of Computer Computations. The IBM Research Symposia Series, Boston, Springer, 1972, pp. 85–103.
2. *Blum M.* How to prove a theorem so no one else can claim it. Proc. ICM'86, AMS, 1986, pp. 1444–1451.
3. *Goldreich O., Micali S., and Wigderson A.* Proofs that yield nothing but their validity or all languages in NP have zero-knowledge proof systems. Proc. SFCS'86, IEEE Computer Society, 1986, pp. 174–187.
4. *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.

5. *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)
6. *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)
7. *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)
8. *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.
9. *Kitaev A., Shen' A., and Vyalyy M.* Klassicheskie i kvantovye vychisleniya [Classical and Quantum Computations]. Moscow, MCCME, 1999. 192 p. (in Russian)

СВЕДЕНИЯ ОБ АВТОРАХ

АНДРЕЕВ Егор Дмитриевич — ООО «Инновационные телекоммуникационные технологии», г. Москва. E-mail: **andreev5902@mail.ru**

БАТАЕВ Михаил Алексеевич — ФГУП «НИИ „Квант“», г. Москва.
E-mail: **misha.bat72@gmail.com**

БЫЗОВ Виктор Александрович — кандидат физико-математических наук, доцент кафедры прикладной математики и информатики Вятского государственного университета, г. Киров. E-mail: **vbyzov@yandex.ru**

ДАВЫДОВ Вадим Валерьевич — кандидат технических наук, научный сотрудник факультета безопасности информационных технологий Университета ИТМО, г. Санкт-Петербург; криптограф-исследователь компании QApp, г. Москва; доцент Санкт-Петербургского государственного университета аэрокосмического приборостроения, г. Санкт-Петербург. E-mail: **vadimdavydov@outlook.com**

ДАКУО Жан-Мишель Никодэмович — аспирант факультета безопасности информационных технологий Университета ИТМО, г. Санкт-Петербург; криптограф-исследователь компании QApp, г. Москва; ассистент Санкт-Петербургского государственного университета аэрокосмического приборостроения, г. Санкт-Петербург.
E-mail: **jeandakuo@mail.ru**

ДЕНИСОВ Олег Викторович — кандидат физико-математических наук, доцент, ООО «Инновационные телекоммуникационные технологии», г. Москва.
E-mail: **denisovOleg@yandex.ru**

ЕФИМОВ Дмитрий Борисович — кандидат физико-математических наук, старший научный сотрудник ФМИ ФИЦ Коми НЦ УрО РАН, г. Сыктывкар.
E-mail: **defimov@ipm.komisc.ru**

ИОГАНСОН Иван Дмитриевич — аспирант факультета безопасности информационных технологий Университета ИТМО, г. Санкт-Петербург; младший криптограф-исследователь компании QApp, г. Москва; ассистент Санкт-Петербургского государственного университета аэрокосмического приборостроения, г. Санкт-Петербург.
E-mail: **ivan.ioganson@yandex.ru**

КУЦЕНКО Александр Владимирович — кандидат физико-математических наук, старший преподаватель Новосибирского государственного университета, г. Новосибирск. E-mail: **alexandrkutsenko@bk.ru**

ПАНКРАТОВА Ирина Анатольевна — кандидат физико-математических наук, доцент, заведующая лабораторией компьютерной криптографии Национального исследовательского Томского государственного университета, г. Томск.
E-mail: **pank@mail.tsu.ru**

ПУШКАРЕВ Игорь Александрович — кандидат физико-математических наук, доцент, доцент кафедры прикладной математики и информатики Вятского государственного университета, г. Киров. E-mail: **god_sha@mail.ru**

РУЗАНОВА Дарья Павловна — стажёр-исследователь Института математики им. С. Л. Соболева СО РАН, г. Омск. E-mail: **kaiser7lu@gmail.com**

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**

СОРОКОУМОВА Алена Дмитриевна — студентка Национального исследовательского Томского государственного университета, г. Томск.
E-mail: **a.srkmva@mail.ru**

ХУЦАЕВА Алтана Феликсовна — аспирантка факультета безопасности информационных технологий Университета ИТМО, ассистент Санкт-Петербургского государственного университета аэрокосмического приборостроения, г. Санкт-Петербург.
E-mail: **afkhutsaeva@itmo.ru**

ЧЕРЕМУШКИН Александр Васильевич — доктор физико-математических наук, академик Академии криптографии Российской Федерации, г. Москва.
E-mail: **avc238@mail.ru**