УДК 512.13

ЗАДАНИЕ ПОДСТАНОВОК АЛГОРИТМОВ БЛОЧНОГО ШИФРОВАНИЯ МАГМА И 2-ГОСТ С ПОМОЩЬЮ АЛГЕБРАИЧЕСКИХ ПОРОГОВЫХ ФУНКЦИЙ

Д. А. Сошин

ФГУП «НИИ «Квант», г. Москва, Россия

Предложено задание подстановок алгоритмов блочного шифрования Магма и 2-ГОСТ через линейные комбинации алгебраических пороговых функций (АПФ). Для этого приведены полученные автором результаты представимости геометрических типов булевых функций от четырёх переменных через АПФ.

Ключевые слова: *алгебраические пороговые функции, геометрические типы, подстановки, блочные шифры.*

DOI 10.17223/20710410/33/4

THE IMPLEMENTATION OF MAGMA AND 2-GOST BLOCK CIPHER SUBSTITUTIONS BY ALGEBRAIC THRESHOLD FUNCTIONS

D. A. Soshin

Technology Federal State Unitary Enterprise "Research Institute Kvant", Moscow, Russia

E-mail: danil_re@list.ru

The paper deals with the implementation of substitutions in Magma and 2-GOST block cipher algorithms by algebraic threshold functions (ATF). For this purpose, the representations of all the geometric types of Boolean functions in 4 variables by ATF are given.

Keywords: *algebraic threshold functions, geometric types, substitutions, block ciphers.*

Введение

Пороговые функции представляют интерес с точки зрения синтеза узлов переработки информации [1] благодаря простой логике их задания и возможности быстрого выполнения операций в перспективной элементной базе, например в оптической [2]. Работы [3 – 5] посвящены изучению способов синтеза подстановок на основе классических пороговых функций. В данной работе предложено задание подстановок алгоритмов блочного шифрования Магма [6] и 2-ГОСТ [7] с помощью так называемых алгебраических пороговых функций. Класс АПФ предложен в работах [8, 9] и отличается от пороговых функций добавлением свободного члена к линейной форме и приведением её по определённому модулю до выполнения операций сравнения. Основным результатом первой работы является описание некоторого класса сбалансированных АПФ, а второй — доказательство того, что только один геометрический тип булевых функций от трёх переменных не принадлежит классу АПФ. Координатные функции указанных подстановок зависят от четырёх переменных, поэтому в работе приведены представления геометрических типов булевых функций четырёх переменных через АПФ.

Полученный каталог позволил изучить представимость линейных комбинаций координатных функций исследуемых подстановок. Через линейные комбинации, являющиеся АПФ, выразилась только одна подстановка. Остальные подстановки удалось задать через линейные комбинации пяти АПФ, полученных добавлением к координатным функциям специально выбранной АПФ. Отметим, что линейные функции содержатся в классе АПФ, поэтому полученные задания подстановок реализуются на единой элементной базе.

1. Представление геометрических типов булевых функций от четырёх переменных через АПФ

Определение 1. Функцию k-значной логики $f_n^k : \Omega_k^n \longrightarrow \Omega_k$ назовём *алгебраической пороговой*, если существуют целочисленные наборы $c = (c_0, c_1, \ldots, c_n)$, $b = (b_0, b_1, \ldots, b_k)$ и модуль $m \in \mathbb{N}$, такие, что для любого $\alpha \in \Omega_k$ выполняется

$$f_n^k(x_1, x_2, \ldots, x_n) = \alpha \quad \Leftrightarrow \quad b_\alpha \leqslant r_m(c_0 + c_1x_1 + c_2x_2 + \cdots + c_nx_n) < b_{\alpha+1},$$

где $r_m(x)$ — функция взятия остатка числа x по модулю m, $r_m(x) \in \{0, 1, \ldots, m-1\}$; $\Omega_k = \{0, 1, 2, \ldots, k-1\}$. Тройку $(c; b; m)$ будем называть структурой функции f_n^k.

Далее рассмотрим двоичный случай. В случае двузначной логики АПФ будем задавать следующим образом:

$$f = 1 \quad \Leftrightarrow \quad r_m(c_0 + c_1x_1 + c_2x_2 + \cdots + c_nx_n) \geqslant b$$

и писать $f : ((c_0, c_1, c_2, \ldots, c_n); b; m)$.

В [9] изложен подход к изучению представимости булевых функций трёх переменных через АПФ. Логика подхода заключается в разбиении всех булевых функций трёх переменных на классы эквивалентности относительно трёх операций — инвертирования переменных, перестановки переменных и инвертирования функции — и рассмотрении только одного представителя из класса. Класс эквивалентности относительно указанных операций будем называть *геометрическим типом*, а произвольное множество функций, замкнутое относительно этих операций, — *геометрически замкнутым*. Корректность такого подхода следует из того, что класс АПФ геометрически замкнут [9].

Далее представлены результаты исследования представимости через АПФ булевых функций от четырёх переменных. Для этого воспользуемся каталогом геометрических типов, составленным В. Г. Никоновым [10]. Удобство использования данного каталога заключается в предложенной автором нумерации, состоящей из четвёрки чисел *a.b.c.d*. Номер a отвечает за вес функций в геометрическом типе, причём если вес функции $\|f\| > 8$, то следует искать соответствующего представителя с весом менее 8 ($\|\overline{f}\| < 8$). Номер b отвечает за количество компонент связности в графе $\mathfrak{G}_f = (X, U)$ функции f. Вершинами X графа связности $\mathfrak{G}_f$ являются точки множества Ω_2^4, в которых функция принимает значение 1 (носитель функции):

$$X = \{(a_1, a_2, a_3, a_4) \in \Omega_2^4 : f(a_1, a_2, a_3, a_4) = 1\},$$

а множеством рёбер U является множество рёбер куба, соединяющих соседние вершины графа:

$$U = \left\{((a_1, a_2, a_3, a_4), (b_1, b_2, b_3, b_4)) \in X^2 | \quad \chi\left((a_1, a_2, a_3, a_4), (b_1, b_2, b_3, b_4)\right) = 1\right\},$$

где χ — расстояние Хемминга между точками (a_1, a_2, a_3, a_4) и (b_1, b_2, b_3, b_4):

$$\chi\left((a_1, a_2, a_3, a_4), (b_1, b_2, b_3, b_4)\right) = \sum_{i=1}^{4} \mathrm{Ind}(a_i \neq b_i),$$

$$\mathrm{Ind}(a_i \neq b_i) = \begin{cases} 1, & \text{если } a_i \neq b_i, \\ 0, & \text{если } a_i = b_i. \end{cases}$$

Номер c — порядковый номер графа связности с числом вершин a и количеством компонент связности b; d — порядковый номер геометрического типа с графом связности $a.b.c$. Стоит отметить, что предложенный каталог составлен в 1994 г. вручную и был впоследствии полностью подтверждён при сверке с результатами работы компьютера.

Далее сохранена введённая нумерация, и читатель может обратиться к указанному каталогу, но представитель геометрического типа будет предложен другой, а именно минимальный по лексикографическому номеру, либо $\overline{f}$ в случае, если первый представитель геометрического типа с минимальным номером f имеет вес более 8.

В [9] доказано, что класс АПФ замкнут относительно фиксации переменных и среди булевых функций от трёх переменных только один геометрический тип не принадлежит классу АПФ (для удобства представителя данного типа будем обозначать f^*). Функция f^* задаётся вектор-строкой

$$f^* = (1, 1, 1, 0, 0, 1, 0, 0). \tag{1}$$

В табл. 1 приведены геометрические типы булевых функций от четырёх переменных с указанием фиксации переменной, при которой подфункция эквивалентна функции (1). Из 222 геометрических типов 70 обладают указанным свойством. Отметим, что если в каталоге представитель f некоторого геометрического типа не содержит подфункцию f^*, то искать её среди подфункций $\overline{f}$ нет смысла, поскольку инвертирование подфункции не выводит за геометрический тип.

Утверждение 1. Геометрические типы булевых функций от четырёх переменных, представленные в табл. 1, не принадлежат классу АПФ.

Для оставшихся 152 геометрических типов была написана программа, которая нашла структуры 101 представителя. Логика работы программы заключается в переборе всевозможных АПФ, у которых коэффициенты линейной формы $(c_0, c_1, c_2, c_3, c_4)$ ограничены некоторой константой, а модуль m и порог b ограничивались максимальным значением $c_0 + c_1 + c_2 + c_3 + c_4 + 1$ текущей линейной формы. Для каждой из полученных АПФ проверяется её наличие среди представителей геометрических типов. Программа опробовала все задания АПФ, у которых коэффициенты линейной формы не превосходили значения 40. Результаты работы программы приведены в табл. 2.

Среди полученных 101 структур представителей геометрических типов максимальный коэффициент линейной формы равен 8, а максимальный модуль — 9. Доказать, что есть соответствующие ограничения, начиная с которых новые АПФ перестанут появляться, не удалось. Подходы, предложенные для подсчёта асимптотики пороговых функций в работах [11 – 13], на данный момент результатов не дали.

Таблица 1

Геометрические типы булевых функций от четырёх переменных, содержащие в качестве подфункции функцию, не принадлежащую классу АПФ

Номер *a.b.c.d*	Вектор-столбец представителя геометрического типа *a.b.c.d*	Фиксация $x_i = \alpha$	Номер *a.b.c.d*	Вектор-столбец представителя геометрического типа *a.b.c.d*	Фиксация $x_i = \alpha$
4.1.3.1	(1,1,0,1,1,0,0,0,0,0,0,0,0,0,0,0)	$x_4 = 0$	5.1.3.1	(1,1,0,1,1,0,0,0,1,0,0,0,0,0,0,0)	$x_4 = 0$
5.1.4.2	(1,1,0,1,0,0,0,0,1,1,0,0,0,0,0,0)	$x_4 = 0$	5.2.3.1	(1,0,1,1,0,1,0,0,1,0,0,0,0,0,0,0)	$x_3 = 0$
5.2.3.2	(0,0,1,1,0,1,0,1,1,0,0,0,0,0,0,0)	$x_4 = 0$	6.1.3.1	(1,1,1,1,0,1,0,0,1,0,0,0,0,0,0,0)	$x_2 = 0$
6.1.5.1	(1,1,0,1,1,0,0,1,1,0,0,0,0,0,0,0)	$x_3 = 0$	6.1.6.1	(1,0,1,1,1,1,0,0,1,0,0,0,0,0,0,0)	$x_3 = 0$
6.1.8.1	(1,1,0,1,0,1,0,1,1,0,0,0,0,0,0,0)	$x_2 = 0$	6.1.9.1	(1,0,1,0,0,0,1,1,1,1,0,0,0,0,0,0)	$x_4 = 0$
6.1.9.2	(1,0,1,1,0,1,0,1,1,0,0,0,0,0,0,0)	$x_3 = 0$	6.2.3.1	(1,1,0,1,0,1,1,0,1,0,0,0,0,0,0,0)	$x_2 = 0$
6.2.3.2	(0,1,0,1,0,1,1,0,1,1,0,0,0,0,0,0)	$x_2 = 0$	6.2.3.3	(0,1,0,0,1,1,0,1,0,1,1,0,0,0,0,0)	$x_2 = 0$
6.2.4.4	(0,1,0,0,1,1,1,0,0,1,1,0,0,0,0,0)	$x_2 = 0$	6.2.4.5	(1,0,0,1,1,0,1,0,1,1,0,0,0,0,0,0)	$x_2 = 0$
6.2.7.1	(0,1,0,1,1,0,1,0,1,1,0,0,0,0,0,0)	$x_3 = 0$	6.2.7.2	(0,0,0,1,1,0,1,1,1,1,0,0,0,0,0,0)	$x_4 = 0$
6.3.3.1	(1,1,0,0,1,0,0,1,0,1,1,0,0,0,0,0)	$x_2 = 0$	6.3.3.2	(1,0,0,0,1,1,0,1,0,1,1,0,0,0,0,0)	$x_4 = 0$
7.1.3.1	(1,1,1,1,0,1,0,1,1,0,0,0,0,0,0,0)	$x_2 = 0$	7.1.5.1	(1,0,1,1,1,1,0,1,1,0,0,0,0,0,0,0)	$x_2 = 0$
7.1.7.1	(1,1,0,1,1,0,1,0,1,1,0,0,0,0,0,0)	$x_1 = 0$	7.1.8.1	(1,1,0,1,0,1,1,1,1,0,0,0,0,0,0,0)	$x_2 = 0$
7.1.8.2	(1,0,1,0,1,0,1,1,1,1,0,0,0,0,0,0)	$x_2 = 0$	7.1.9.1	(1,1,1,1,0,1,1,0,1,0,0,0,0,0,0,0)	$x_2 = 0$
7.1.10.1	(1,1,1,0,0,0,1,1,1,1,0,0,0,0,0,0)	$x_1 = 0$	7.1.11.1	(1,0,0,0,1,1,0,1,1,1,1,0,0,0,0,0)	$x_4 = 0$
7.1.13.1	(0,1,1,1,0,1,1,0,1,1,0,0,0,0,0,0)	$x_2 = 0$	7.1.15.1	(0,1,0,0,0,1,1,1,1,1,1,0,0,0,0,0)	$x_4 = 0$
7.1.15.2	(1,0,0,1,1,0,1,1,1,1,0,0,0,0,0,0)	$x_2 = 0$	7.1.15.4	(0,1,1,0,1,1,1,0,0,1,1,0,0,0,0,0)	$x_2 = 0$
7.2.3.1	(1,1,0,0,1,1,0,1,0,1,1,0,0,0,0,0)	$x_1 = 1$	7.2.5.1	(1,0,1,1,0,1,1,0,1,1,0,0,0,0,0,0)	$x_1 = 0$
7.2.5.2	(0,1,0,1,1,1,1,0,0,1,1,0,0,0,0,0)	$x_2 = 0$	7.2.6.1	(1,1,1,0,1,0,0,1,0,1,1,0,0,0,0,0)	$x_2 = 0$
7.2.6.2	(0,1,1,1,0,0,0,1,0,1,1,0,1,0,0,0)	$x_2 = 1$	7.2.8.1	(0,1,0,0,1,1,1,1,0,1,1,0,0,0,0,0)	$x_2 = 0$
7.2.9.1	(1,0,1,0,1,1,0,1,0,1,1,0,0,0,0,0)	$x_1 = 0$	7.2.12.1	(0,0,0,1,1,0,0,1,1,1,1,0,1,0,0,0)	$x_2 = 0$
7.2.12.2	(0,1,1,0,1,1,0,1,0,1,1,0,0,0,0,0)	$x_2 = 0$	7.2.16.1	(0,0,1,0,1,1,0,1,1,1,1,0,0,0,0,0)	$x_3 = 0$
7.3.3.1	(1,1,0,1,0,0,0,1,0,1,1,0,1,0,0,0)	$x_4 = 0$	7.3.4.1	(0,0,1,1,0,1,0,1,0,1,1,0,1,0,0,0)	$x_4 = 0$
7.3.5.1	(0,1,0,1,1,0,0,1,0,1,1,0,1,0,0,0)	$x_1 = 1$	8.1.4.1	(1,1,1,1,0,1,1,1,1,0,0,0,0,0,0,0)	$x_1 = 0$
8.1.7.1	(1,1,1,1,0,1,1,0,1,1,0,0,0,0,0,0)	$x_1 = 0$	8.1.8.1	(1,1,1,1,0,0,1,1,1,1,0,0,0,0,0,0)	$x_1 = 0$
8.1.9.1	(1,0,1,1,1,0,1,1,1,1,0,0,0,0,0,0)	$x_2 = 0$	8.1.11.1	(1,1,0,1,1,0,1,1,1,1,0,0,0,0,0,0)	$x_1 = 0$
8.1.14.1	(0,1,1,1,1,1,1,0,0,1,1,0,0,0,0,0)	$x_1 = 0$	8.1.15.1	(0,1,1,1,0,0,0,1,1,1,1,0,1,0,0,0)	$x_1 = 0$
8.1.19.1	(0,1,1,0,0,1,1,1,1,1,1,0,0,0,0,0)	$x_1 = 0$	8.1.19.2	(0,1,1,0,1,1,1,1,0,1,1,0,0,0,0,0)	$x_1 = 0$
8.1.21.1	(1,1,1,0,1,1,0,1,0,1,1,0,0,0,0,0)	$x_1 = 0$	8.1.23.1	(1,1,0,0,0,1,1,1,1,1,1,0,0,0,0,0)	$x_1 = 1$
8.1.23.2	(0,1,1,1,1,0,1,1,1,1,0,0,0,0,0,0)	$x_1 = 1$	8.1.25.1	(0,1,0,0,1,1,1,1,1,1,1,0,0,0,0,0)	$x_3 = 0$
8.1.26.1	(1,1,1,1,1,0,0,1,0,1,1,0,0,0,0,0)	$x_1 = 0$	8.1.27.1	(0,1,0,1,1,0,0,1,1,1,1,0,1,0,0,0)	$x_1 = 1$
8.1.28.1	(0,1,1,0,1,1,0,1,1,1,1,0,0,0,0,0)	$x_1 = 1$	8.1.28.2	(0,0,1,1,0,1,0,1,1,1,1,0,1,0,0,0)	$x_4 = 0$
8.1.30.1	(0,0,0,1,1,0,1,1,1,1,0,1,1,0,0,0)	$x_4 = 0$	8.1.31.1	(0,0,1,1,1,1,0,1,1,1,1,0,0,0,0,0)	$x_2 = 1$
8.2.5.1	(1,0,1,1,1,1,0,1,0,1,1,0,0,0,0,0)	$x_1 = 0$	8.2.10.1	(1,1,0,1,1,0,0,1,0,1,1,0,1,0,0,0)	$x_1 = 1$
8.2.12.1	(0,0,1,1,1,1,0,1,0,1,1,0,1,0,0,0)	$x_2 = 1$	8.2.16.1	(0,1,1,1,1,0,0,1,0,1,1,0,1,0,0,0)	$x_2 = 1$
8.2.22.1	(0,0,1,0,0,1,1,1,1,1,0,1,1,0,0,0)	$x_4 = 0$	8.3.3.1	(1,0,1,1,0,1,0,1,0,1,1,0,1,0,0,0)	$x_2 = 1$

Таблица 2

Геометрические типы булевых функций от четырёх переменных, принадлежащие классу АПФ

№ п/п	Номер класса *a.b.c.d*	Вектор-столбец представителя геометрического типа *a.b.c.d*	Структура представителя геометрического типа *a.b.c.d*
1	0.0.1.1	$(0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0)$	$((0,0,0,0,0);1;1)$
2	1.1.1.1	$(1,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0)$	$((4,1,1,1,1);4;5)$
3	2.1.1.1	$(1,1,0,0,0,0,0,0,0,0,0,0,0,0,0,0)$	$((3,0,1,1,1);3;4)$
4	2.2.1.1	$(0,1,1,0,0,0,0,0,0,0,0,0,0,0,0,0)$	$((0,5,5,2,2);5;6)$
5	2.2.1.2	$(0,0,0,1,1,0,0,0,0,0,0,0,0,0,0,0)$	$((0,1,4,5,3);5;6)$
6	2.2.1.3	$(0,0,0,0,0,0,0,1,1,0,0,0,0,0,0,0)$	$((0,1,1,1,3);3;4)$
7	3.1.1.1	$(1,1,1,0,0,0,0,0,0,0,0,0,0,0,0,0)$	$((5,1,1,2,2);5;7)$
8	3.2.1.1	$(1,0,0,1,1,0,0,0,0,0,0,0,0,0,0,0)$	$((7,3,7,1,4);7;9)$
9	3.2.1.2	$(1,0,0,0,0,0,0,1,1,0,0,0,0,0,0,0)$	$((5,5,5,5,1);5;7)$
10	3.3.1.1	$(0,1,1,0,1,0,0,0,0,0,0,0,0,0,0,0)$	$((0,4,4,4,3);4;5)$
11	3.3.1.2	$(0,0,0,1,1,0,0,0,1,0,0,0,0,0,0,0)$	$((0,2,2,4,4);4;5)$
12	3.3.1.3	$(0,1,0,0,0,0,0,1,1,0,0,0,0,0,0,0)$	$((1,6,5,5,7);7;9)$
13	4.1.1.1	$(1,1,1,1,0,0,0,0,0,0,0,0,0,0,0,0)$	$((2,0,0,1,1);2;3)$
14	4.1.2.1	$(1,1,1,0,1,0,0,0,0,0,0,0,0,0,0,0)$	$((4,1,1,1,2);4;6)$
15	4.2.1.1	$(0,1,1,1,1,0,0,0,0,0,0,0,0,0,0,0)$	$((0,6,6,5,4);5;7)$
16	4.2.1.2	$(0,0,0,1,0,1,0,1,1,0,0,0,0,0,0,0)$	$((1,2,1,1,4);4;6)$
17	4.2.1.4	$(1,0,0,1,1,0,0,0,1,0,0,0,0,0,0,0)$	$((5,4,4,1,1);5;7)$
18	4.2.2.1	$(0,0,1,1,1,1,0,0,0,0,0,0,0,0,0,0)$	$((0,0,3,3,2);3;4)$
19	4.2.2.3	$(0,0,0,0,0,0,1,1,1,1,0,0,0,0,0,0)$	$((0,0,1,1,2);2;3)$
20	4.3.1.1	$(0,1,0,1,1,0,0,0,1,0,0,0,0,0,0,0)$	$((1,6,7,5,5);6;8)$
21	4.3.1.2	$(0,0,1,1,0,1,0,0,1,0,0,0,0,0,0,0)$	$((1,1,5,4,6);6;8)$
22	4.3.1.3	$(0,0,0,1,1,0,0,1,1,0,0,0,0,0,0,0)$	$((0,3,3,6,5);5;7)$
23	4.4.1.1	$(1,0,0,1,0,1,1,0,0,0,0,0,0,0,0,0)$	$((3,2,2,2,1);3;4)$
24	4.4.1.2	$(0,1,1,0,1,0,0,0,1,0,0,0,0,0,0,0)$	$((0,3,3,3,3);3;4)$
25	4.4.1.3	$(0,1,1,0,0,0,0,1,1,0,0,0,0,0,0,0)$	$((1,5,5,4,6);6;8)$
26	4.4.1.4	$(0,0,0,1,0,1,1,0,1,0,0,0,0,0,0,0)$	$((0,2,2,2,4);4;5)$
27	4.4.1.5	$(0,0,0,0,1,0,0,1,0,1,1,0,0,0,0,0)$	$((0,2,2,3,1);3;4)$
28	4.4.1.6	$(0,0,0,0,0,1,1,0,0,1,1,0,0,0,0,0)$	$((0,1,1,2,2);3;4)$
29	5.1.1.1	$(1,1,1,1,1,0,0,0,0,0,0,0,0,0,0,0)$	$((5,1,1,2,3);5;8)$
30	5.1.2.1	$(1,1,1,0,1,0,0,0,1,0,0,0,0,0,0,0)$	$((3,1,1,1,1);3;5)$
31	5.1.4.1	$(1,0,1,1,1,1,0,0,0,0,0,0,0,0,0,0)$	$((6,8,2,2,4);6;9)$
32	5.2.1.1	$(0,1,0,1,0,1,0,1,1,0,0,0,0,0,0,0)$	$((2,3,1,1,5);5;8)$
33	5.2.2.3	$(0,0,0,1,0,1,1,1,1,0,0,0,0,0,0,0)$	$((1,1,1,1,3);3;5)$
34	5.2.4.2	$(1,0,0,1,1,0,0,1,1,0,0,0,0,0,0,0)$	$((6,5,5,1,2);6;9)$
35	5.2.4.3	$(1,0,0,0,0,0,1,1,1,1,0,0,0,0,0,0)$	$((5,7,5,5,2);5;8)$
36	5.3.1.1	$(0,1,1,1,1,0,0,0,1,0,0,0,0,0,0,0)$	$((0,5,5,4,4);4;6)$
37	5.3.1.3	$(0,1,0,1,0,1,1,0,1,0,0,0,0,0,0,0)$	$((1,4,5,5,3);4;6)$
38	5.3.1.4	$(0,1,0,0,0,1,1,0,0,1,1,0,0,0,0,0)$	$((1,5,4,2,2);6;9)$
39	5.3.2.1	$(0,0,1,1,1,1,0,0,1,0,0,0,0,0,0,0)$	$((1,1,4,4,5);5;7)$
40	5.4.1.1	$(1,0,0,1,0,1,1,0,1,0,0,0,0,0,0,0)$	$((5,4,4,4,1);5;7)$
41	5.4.1.2	$(0,0,0,1,0,1,1,0,1,1,0,0,0,0,0,0)$	$((1,1,2,2,3);4;6)$
42	5.4.1.3	$(1,0,0,0,1,0,0,1,0,1,1,0,0,0,0,0)$	$((5,3,3,1,5);5;7)$
43	5.5.1.1	$(0,1,1,0,1,0,0,1,1,0,0,0,0,0,0,0)$	$((1,4,4,4,5);5;7)$
44	5.5.1.2	$(1,0,0,0,0,0,0,1,0,1,1,0,1,0,0,0)$	$((2,1,1,1,2);2;3)$
45	5.5.1.3	$(1,0,0,0,0,1,1,0,0,1,1,0,0,0,0,0)$	$((5,3,3,5,5);5;7)$
46	6.1.1.1	$(1,1,1,1,1,1,0,0,0,0,0,0,0,0,0,0)$	$((3,0,1,1,2);3;5)$
47	6.1.2.1	$(1,1,1,1,1,0,0,0,1,0,0,0,0,0,0,0)$	$((4,1,1,2,2);4;7)$
48	6.1.7.1	$(0,1,1,1,1,1,1,0,0,0,0,0,0,0,0,0)$	$((0,5,5,5,3);4;6)$
49	6.2.1.2	$(0,1,0,1,0,1,1,1,1,0,0,0,0,0,0,0)$	$((1,5,6,6,3);4;7)$
50	6.2.2.2	$(1,0,0,0,0,0,0,1,0,0,0,1,0,1,1,1)$	$((2,3,3,3,3);2;4)$
51	6.2.4.2	$(0,1,1,1,0,1,1,0,1,0,0,0,0,0,0,0)$	$((1,6,6,7,4);5;8)$
52	6.2.4.3	$(0,1,1,1,1,1,0,0,1,0,0,0,0,0,0,0)$	$((0,7,6,6,5);5;8)$

Окончание табл. 2

№ п/п	Номер класса $a.b.c.d$	Вектор-столбец представителя геометрического типа $a.b.c.d$	Структура представителя геометрического типа $a.b.c.d$
53	6.2.5.1	$(1,1,0,0,0,0,1,1,1,1,0,0,0,0,0,0)$	$((3,0,3,3,1);3;5)$
54	6.2.6.2	$(0,0,1,0,1,0,1,1,1,1,0,0,0,0,0,0)$	$((1,1,5,5,3);4;7)$
55	6.2.8.1	$(0,1,1,0,0,1,1,0,0,1,1,0,0,0,0,0)$	$((1,3,3,1,1);4;6)$
56	6.2.8.3	$(0,0,0,0,0,1,1,1,1,1,1,0,0,0,0,0)$	$((0,1,1,2,3);3;5)$
57	6.3.4.1	$(0,0,1,1,0,1,1,0,1,1,0,0,0,0,0,0)$	$((2,1,3,2,4);5;8)$
58	6.3.5.1	$(0,0,1,1,1,1,0,0,1,1,0,0,0,0,0,0)$	$((0,0,2,2,2);2;3)$
59	6.4.1.2	$(0,0,0,1,1,1,1,0,0,1,1,0,0,0,0,0)$	$((1,2,2,4,3);5;8)$
60	6.4.1.3	$(1,1,0,0,0,0,0,1,0,1,1,0,1,0,0,0)$	$((3,1,2,2,4);3;5)$
61	6.4.2.1	$(0,1,1,0,1,0,0,1,0,1,1,0,0,0,0,0)$	$((1,3,3,4,1);4;6)$
62	6.4.2.2	$(0,1,1,0,0,0,0,1,0,1,1,0,1,0,0,0)$	$((0,4,4,3,1);4;6)$
63	6.5.1.1	$(1,0,0,1,0,0,0,1,0,1,1,0,1,0,0,0)$	$((3,3,3,4,2);3;5)$
64	6.6.1.1	$(1,0,0,1,0,1,1,0,0,1,1,0,0,0,0,0)$	$((4,3,3,4,4);4;6)$
65	6.6.1.2	$(0,0,0,1,0,1,1,0,0,1,1,0,1,0,0,0)$	$((0,1,1,1,1);2;3)$
66	7.1.1.1	$(1,1,1,1,1,1,1,0,0,0,0,0,0,0,0,0)$	$((4,1,1,1,3);4;7)$
67	7.1.2.1	$(1,1,1,1,1,1,0,0,1,0,0,0,0,0,0,0)$	$((5,1,2,2,3);5;9)$
68	7.1.14.1	$(1,0,1,1,1,1,0,0,1,1,0,0,0,0,0,0)$	$((4,6,2,2,2);4;7)$
69	7.2.1.1	$(0,1,1,1,0,1,1,1,1,0,0,0,0,0,0,0)$	$((1,7,7,8,4);5;9)$
70	7.2.2.2	$(1,0,0,0,0,0,0,1,0,0,0,1,1,1,1,1)$	$((3,5,5,4,4);3;6)$
71	7.2.7.1	$(0,1,1,1,1,1,1,0,1,0,0,0,0,0,0,0)$	$((0,4,4,4,3);3;5)$
72	7.2.10.1	$(0,0,1,1,1,0,1,1,1,1,0,0,0,0,0,0)$	$((1,1,6,7,4);5;9)$
73	7.2.11.1	$(1,0,0,0,0,0,0,1,1,0,0,1,0,1,1,1)$	$((4,2,2,2,1);3;6)$
74	7.2.13.1	$(0,0,1,1,1,1,1,0,1,1,0,0,0,0,0,0)$	$((1,6,5,5,4);4;7)$
75	7.2.14.1	$(0,0,0,0,1,1,1,1,1,1,1,0,0,0,0,0)$	$((1,1,1,3,4);4;7)$
76	7.2.15.1	$(1,0,0,0,0,1,1,1,1,1,1,0,0,0,0,0)$	$((5,7,7,5,3);5;9)$
77	7.3.4.3	$(1,1,1,0,0,0,0,1,0,1,1,0,1,0,0,0)$	$((4,2,2,3,6);4;7)$
78	7.3.6.1	$(0,0,0,1,1,1,1,0,1,1,1,0,0,0,0,0)$	$((1,1,1,2,2);3;5)$
79	7.4.1.2	$(0,1,0,1,0,1,1,0,0,1,1,0,1,0,0,0)$	$((1,3,2,2,2);4;7)$
80	7.4.2.1	$(1,0,0,1,1,0,0,1,0,1,1,0,1,0,0,0)$	$((5,3,3,1,5);4;7)$
81	7.4.3.1	$(0,1,1,0,1,0,0,1,0,1,1,0,1,0,0,0)$	$((0,3,3,3,1);3;5)$
82	7.5.1.1	$(1,0,0,1,0,1,0,1,0,1,1,0,1,0,0,0)$	$((4,4,5,5,3);4;7)$
83	7.7.1.1	$(1,0,0,1,0,1,1,0,0,1,1,0,1,0,0,0)$	$((3,3,3,3,3);3;5)$
84	8.1.1.1	$(1,1,1,1,1,1,1,1,0,0,0,0,0,0,0,0)$	$((1,0,0,0,1);1;2)$
85	8.1.2.1	$(1,1,1,1,1,1,1,0,1,0,0,0,0,0,0,0)$	$((3,1,1,1,2);3;6)$
86	8.1.5.1	$(1,1,1,1,1,1,0,0,1,1,0,0,0,0,0,0)$	$((2,0,1,1,1);2;4)$
87	8.1.16.1	$(0,1,1,1,1,1,1,0,1,1,0,0,0,0,0,0)$	$((0,7,6,6,5);4;8)$
88	8.1.29.1	$(0,1,0,1,1,1,1,0,1,1,1,0,0,0,0,0)$	$((1,6,7,5,5);4;8)$
89	8.2.1.1	$(0,1,1,1,1,1,1,1,1,0,0,0,0,0,0,0)$	$((0,5,5,5,3);3;6)$
90	8.2.9.2	$(0,1,1,1,0,1,1,0,0,1,1,0,1,0,0,0)$	$((1,3,3,2,2);4;8)$
91	8.2.11.1	$(1,1,1,0,1,0,0,1,0,1,1,0,1,0,0,0)$	$((3,2,2,2,5);3;6)$
92	8.2.13.1	$(0,0,1,1,1,1,1,1,1,1,0,0,0,0,0,0)$	$((0,0,3,3,2);2;4)$
93	8.2.17.1	$(0,0,0,1,1,1,1,1,1,1,1,0,0,0,0,0)$	$((1,1,1,2,3);3;6)$
94	8.2.20.1	$(0,0,0,0,1,1,1,1,1,1,1,1,0,0,0,0)$	$((0,0,0,1,1);1;2)$
95	8.2.21.1	$(0,0,0,1,0,1,1,1,1,1,1,0,1,0,0,0)$	$((0,1,1,1,2);2;4)$
96	8.3.4.1	$(1,1,1,0,0,1,1,1,0,0,0,1,1,0,0,0)$	$((2,1,1,3,2);2;4)$
97	8.3.5.1	$(0,1,1,0,0,1,1,1,1,0,0,1,1,0,0,0)$	$((0,4,4,1,3);3;6)$
98	8.4.2.1	$(1,0,0,0,0,1,1,1,0,1,1,1,1,0,0,0)$	$((2,3,3,2,2);2;4)$
99	8.4.3.1	$(1,1,0,0,0,0,1,1,0,0,1,1,1,1,0,0)$	$((1,0,1,1,1);1;2)$
100	8.5.1.1	$(1,0,0,1,0,1,1,1,0,1,1,0,1,0,0,0)$	$((3,4,4,4,3);3;6)$
101	8.8.1.1	$(0,1,1,0,1,0,0,1,1,0,0,1,0,1,1,0)$	$((0,1,1,1,1);1;2)$

Например, в [11, 14] предлагается использовать векторы параметров Чоу. Если f — булева функция от n переменных, то, сложив как векторы все наборы x, на которых $f(x) = 0$, получим целочисленный n-мерный вектор $(s_1, s_2, \ldots, s_n)$. Дополнив его нуле-

вой координатой $s_0 = |f^{-1}(0)|$, равной числу наборов x, на которых $f(x) = 0$, получим $(n+1)$-мерный вектор параметров Чоу. В работе [11] приведено одно из доказательств того, что если две пороговые функции различны, то они имеют разные векторы параметров Чоу. Булевы функции от двух переменных $f = x_1 + x_2$ и $g = x_1 + x_2 + 1$ имеют одинаковые векторы параметров Чоу, в то время как в работе [9] доказано, что любая линейная функция k-значной логики принадлежит классу АПФ. Поэтому использование подхода на основе векторов параметров Чоу невозможно.

В связи с тем, что ограничение на коэффициенты линейной формы не получено и гарантии, что на компьютере построены все представители геометрических типов булевых функций от четырёх переменных, нет, для оставшихся 51 геометрических типов (табл. 3) выдвигается гипотеза об их непринадлежности классу АПФ.

Таблица 3

Геометрические типы булевых функций от четырёх переменных, по отношению к которым выдвигается гипотеза об их непринадлежности к классу АПФ

Номер *a.b.c.d*	Вектор-столбец представителя геометрического типа *a.b.c.d*	Номер *a.b.c.d*	Вектор-столбец представителя геометрического типа *a.b.c.d*
4.2.1.3	(1,1,0,0,0,0,0,1,1,0,0,0,0,0,0,0)	4.2.2.2	(1,0,0,1,0,0,0,1,1,0,0,0,0,0,0,0)
5.2.2.1	(1,1,0,1,0,1,1,0,0,0,0,0,0,0,0,0)	5.2.2.2	(1,1,1,0,0,0,0,1,1,0,0,0,0,0,0,0)
5.2.4.1	(1,0,0,1,0,1,0,1,1,0,0,0,0,0,0,0)	5.3.1.2	(0,1,0,1,1,0,0,1,1,0,0,0,0,0,0,0)
5.3.1.5	(0,0,0,0,1,1,0,1,0,1,1,0,0,0,0,0)	5.3.2.2	(0,0,0,1,1,0,1,0,1,1,0,0,0,0,0,0)
6.1.4.1	(1,1,1,1,0,1,1,0,0,0,0,0,0,0,0,0)	6.1.4.2	(1,1,1,1,0,0,0,1,1,0,0,0,0,0,0,0)
6.2.1.1	(0,1,1,1,0,1,0,1,1,0,0,0,0,0,0,0)	6.2.2.1	(1,1,1,0,1,0,0,1,1,0,0,0,0,0,0,0)
6.2.4.1	(0,0,1,1,1,1,0,1,1,0,0,0,0,0,0,0)	6.2.6.1	(1,0,0,1,0,1,1,1,1,0,0,0,0,0,0,0)
6.2.8.2	(0,0,0,0,1,1,0,1,1,1,1,0,0,0,0,0)	6.2.8.4	(0,1,1,0,0,0,1,1,1,1,0,0,0,0,0,0)
6.2.8.5	(0,1,1,0,1,0,1,0,1,1,0,0,0,0,0,0)	6.3.1.1	(0,0,0,0,1,1,1,1,0,1,1,0,0,0,0,0)
6.3.2.1	(1,1,0,0,0,1,1,0,0,1,1,0,0,0,0,0)	6.3.2.2	(0,1,1,1,1,0,0,1,1,0,0,0,0,0,0,0)
6.3.4.2	(0,0,1,0,1,1,0,1,0,1,1,0,0,0,0,0)	6.4.1.1	(1,0,0,1,0,1,1,0,1,1,0,0,0,0,0,0)
6.4.2.3	(0,0,0,1,1,0,0,1,0,1,1,0,1,0,0,0)	7.1.4.1	(1,1,1,0,1,0,1,0,1,1,0,0,0,0,0,0)
7.1.6.1	(1,1,1,1,1,0,0,1,1,0,0,0,0,0,0,0)	7.1.12.1	(1,1,1,0,0,1,1,0,0,1,1,0,0,0,0,0)
7.1.15.3	(0,1,1,1,1,0,1,0,1,1,0,0,0,0,0,0)	7.2.2.1	(1,1,0,1,0,1,1,0,1,1,0,0,0,0,0,0)
7.2.4.1	(0,1,1,1,1,1,0,1,1,0,0,0,0,0,0,0)	7.2.4.2	(1,1,0,0,1,1,1,0,0,1,1,0,0,0,0,0)
7.2.15.2	(0,1,1,0,1,0,1,1,1,1,0,0,0,0,0,0)	7.3.1.1	(1,0,0,0,1,1,1,1,0,1,1,0,0,0,0,0)
7.3.2.1	(1,1,0,1,0,1,1,0,0,1,1,0,0,0,0,0)	7.3.4.2	(1,0,0,1,1,1,0,1,0,1,1,0,0,0,0,0)
7.3.6.2	(1,0,0,0,0,1,1,1,1,0,0,1,1,0,0,0)	7.4.1.1	(1,0,0,1,1,1,1,0,0,1,1,0,0,0,0,0)
8.1.3.1	(1,1,1,1,1,1,0,1,1,0,0,0,0,0,0,0)	8.1.6.1	(1,1,1,1,1,0,1,0,1,1,0,0,0,0,0,0)
8.1.10.1	(1,1,1,0,1,0,1,1,1,1,0,0,0,0,0,0)	8.1.17.1	(1,1,1,1,0,1,1,0,0,1,1,0,0,0,0,0)
8.1.20.1	(1,0,1,0,1,1,0,1,1,1,1,0,0,0,0,0)	8.1.22.1	(1,0,1,1,1,1,1,0,1,1,0,0,0,0,0,0)
8.1.24.1	(1,0,0,0,1,1,1,1,1,1,1,0,0,0,0,0)	8.1.30.2	(0,1,1,0,1,1,1,0,1,1,1,0,0,0,0,0)
8.2.6.1	(1,1,0,1,1,1,1,0,0,1,1,0,0,0,0,0)	8.2.9.1	(1,0,0,1,1,1,1,0,1,1,1,0,0,0,0,0)
8.2.11.2	(0,1,1,0,1,0,0,1,1,1,1,0,1,0,0,0)	8.2.12.2	(1,1,0,0,0,1,1,1,1,0,0,1,1,0,0,0)
8.2.21.2	(1,0,0,1,0,1,1,1,1,1,1,0,0,0,0,0)	8.3.2.1	(1,0,0,1,1,1,1,1,0,1,1,0,0,0,0,0)
8.4.1.1	(1,1,0,1,0,1,1,0,0,1,1,0,1,0,0,0)		

Вероятно, для каждого геометрического типа можно доказать его непринадлежность классу АПФ, но случай булевых функций от трёх переменных [9] показал, что данный процесс весьма затруднителен.

2. Представление подстановок алгоритма блочного шифрования Магма линейными комбинациями АПФ

В стандарте ГОСТ Р 34.12-2015 [6] в качестве нелинейного биективного преобразования выступает набор подстановок π_i, $i = 0, 1, 2, \ldots, 7$. Они заданы в виде массивов

$$\pi_0 = (12, 4, 6, 2, 10, 5, 11, 9, 14, 8, 13, 7, 0, 3, 15, 1);$$
$$\pi_1 = (6, 8, 2, 3, 9, 10, 5, 12, 1, 14, 4, 7, 11, 13, 0, 15);$$
$$\pi_2 = (11, 3, 5, 8, 2, 15, 10, 13, 14, 1, 7, 4, 12, 9, 6, 0);$$
$$\pi_3 = (12, 8, 2, 1, 13, 4, 15, 6, 7, 0, 10, 5, 3, 14, 9, 11);$$
$$\pi_4 = (7, 15, 5, 10, 8, 1, 6, 13, 0, 9, 3, 14, 11, 4, 2, 12);$$
$$\pi_5 = (5, 13, 15, 6, 9, 2, 12, 10, 11, 7, 8, 1, 4, 3, 14, 0);$$
$$\pi_6 = (8, 14, 2, 5, 6, 9, 1, 12, 15, 4, 11, 0, 13, 10, 3, 7);$$
$$\pi_7 = (1, 7, 14, 13, 0, 5, 8, 3, 4, 15, 10, 6, 9, 12, 11, 2).$$

Представим подстановки в виде координатных функций, обозначив через f_3^i, f_2^i, f_1^i, f_0^i координатные функции подстановки π_i, $i = 0, \ldots, 7$, от старших разрядов к младшим соответственно:

$$\pi_0 = \begin{pmatrix} f_3^0 \\ f_2^0 \\ f_1^0 \\ f_0^0 \end{pmatrix} = \begin{pmatrix} 1\,0\,0\,0\,1\,0\,1\,1\,1\,1\,1\,0\,0\,0\,1\,0 \\ 1\,1\,1\,0\,0\,1\,0\,0\,1\,0\,1\,1\,0\,0\,1\,0 \\ 0\,0\,1\,1\,1\,0\,1\,0\,1\,0\,0\,1\,0\,1\,1\,0 \\ 0\,0\,0\,0\,0\,1\,1\,1\,0\,0\,1\,1\,0\,1\,1\,1 \end{pmatrix}; \qquad \pi_1 = \begin{pmatrix} f_3^1 \\ f_2^1 \\ f_1^1 \\ f_0^1 \end{pmatrix} = \begin{pmatrix} 0\,1\,0\,0\,1\,1\,0\,1\,0\,1\,0\,0\,1\,1\,0\,1 \\ 1\,0\,0\,0\,0\,0\,0\,1\,1\,0\,1\,1\,1\,0\,1\,0\,1 \\ 1\,0\,1\,1\,0\,1\,0\,0\,0\,1\,0\,1\,1\,0\,0\,1 \\ 0\,0\,0\,1\,1\,0\,1\,0\,1\,0\,0\,1\,1\,1\,0\,1 \end{pmatrix};$$

$$\pi_2 = \begin{pmatrix} f_3^2 \\ f_2^2 \\ f_1^2 \\ f_0^2 \end{pmatrix} = \begin{pmatrix} 1\,0\,0\,1\,0\,1\,1\,1\,1\,0\,0\,0\,1\,1\,0\,0 \\ 0\,0\,1\,0\,0\,1\,0\,1\,1\,0\,1\,1\,1\,0\,1\,0 \\ 1\,1\,0\,0\,1\,1\,1\,0\,1\,0\,1\,0\,0\,0\,1\,0 \\ 1\,1\,1\,0\,0\,1\,0\,1\,0\,1\,1\,0\,0\,1\,0\,0 \end{pmatrix}; \qquad \pi_3 = \begin{pmatrix} f_3^3 \\ f_2^3 \\ f_1^3 \\ f_0^3 \end{pmatrix} = \begin{pmatrix} 1\,1\,0\,0\,1\,0\,1\,0\,0\,0\,1\,0\,0\,1\,1\,1 \\ 1\,0\,0\,0\,1\,1\,1\,1\,1\,0\,0\,1\,0\,1\,0\,0 \\ 0\,0\,1\,0\,0\,0\,1\,1\,1\,0\,1\,0\,1\,1\,0\,1 \\ 0\,0\,0\,1\,1\,0\,1\,0\,1\,0\,0\,1\,1\,0\,1\,1 \end{pmatrix};$$

$$\pi_4 = \begin{pmatrix} f_3^4 \\ f_2^4 \\ f_1^4 \\ f_0^4 \end{pmatrix} = \begin{pmatrix} 0\,1\,0\,1\,1\,0\,0\,1\,0\,1\,0\,1\,1\,0\,0\,1 \\ 1\,1\,1\,0\,0\,0\,1\,1\,0\,0\,0\,1\,0\,1\,0\,1 \\ 1\,1\,0\,1\,0\,0\,1\,0\,0\,0\,1\,1\,1\,0\,1\,0 \\ 1\,1\,1\,0\,0\,1\,0\,1\,0\,1\,1\,0\,1\,0\,0\,0 \end{pmatrix}; \qquad \pi_5 = \begin{pmatrix} f_3^5 \\ f_2^5 \\ f_1^5 \\ f_0^5 \end{pmatrix} = \begin{pmatrix} 0\,1\,1\,0\,1\,0\,1\,1\,1\,0\,1\,0\,0\,0\,1\,0 \\ 1\,1\,1\,1\,0\,0\,1\,0\,0\,1\,0\,0\,1\,0\,1\,0 \\ 0\,0\,1\,1\,0\,1\,0\,1\,1\,1\,0\,0\,0\,1\,1\,0 \\ 1\,1\,1\,0\,1\,0\,0\,0\,1\,1\,0\,1\,0\,1\,0\,0 \end{pmatrix};$$

$$\pi_6 = \begin{pmatrix} f_3^6 \\ f_2^6 \\ f_1^6 \\ f_0^6 \end{pmatrix} = \begin{pmatrix} 1\,1\,0\,0\,0\,1\,0\,1\,1\,1\,1\,0\,1\,1\,0\,0 \\ 0\,1\,0\,1\,1\,0\,0\,1\,1\,1\,0\,0\,1\,0\,0\,1 \\ 0\,1\,1\,0\,1\,0\,0\,0\,1\,1\,1\,0\,0\,1\,1\,1 \\ 0\,0\,0\,1\,0\,1\,1\,0\,1\,0\,1\,0\,1\,0\,1\,1 \end{pmatrix}; \qquad \pi_7 = \begin{pmatrix} f_3^7 \\ f_2^7 \\ f_1^7 \\ f_0^7 \end{pmatrix} = \begin{pmatrix} 0\,0\,1\,1\,0\,0\,1\,0\,0\,1\,1\,0\,1\,1\,1\,0 \\ 0\,1\,1\,1\,0\,1\,0\,0\,1\,1\,0\,1\,0\,1\,0\,0 \\ 0\,1\,1\,0\,0\,0\,0\,1\,0\,1\,1\,1\,0\,0\,1\,1 \\ 1\,1\,0\,1\,0\,1\,0\,1\,0\,1\,0\,0\,1\,0\,1\,0 \end{pmatrix}.$$

Задача данного пункта — представить подстановки $\pi_0, \pi_1, \ldots, \pi_7$ через линейные комбинации функций из класса АПФ, использовав при этом для каждой подстановки минимальное количество таких функций, а значит, и минимальное количество пороговых элементов при технической реализации. Минимальное количество функций, через линейные комбинации которых можно реализовать подстановки, равно 4. В этом случае соответствующие АПФ лежат в подпространстве, порождённом координатными функциями подстановок. На первом этапе была исследована представимость каждой подстановки через АПФ линейных комбинаций координатных функций. Результаты приведены в табл. 4.

Таблица 4

Представление линейных комбинаций координатных функций подстановок ГОСТ Р 34.12-2015 через АПФ

π_i	Линейные комбинации координатных функций	Структура АПФ, задающей линейную комбинацию координатных функций	π_i	Линейные комбинации координатных функций	Структура АПФ, задающей линейную комбинацию координатных функций
π_1	$f_3^{(1)}$	$((0,3,1,3,0);2;4)$	π_4	$f_3^{(4)}$	$((0,2,1,3,0);2;4)$
	$f_3^{(1)} \oplus f_2^{(1)} \oplus f_0^{(1)}$	$((7,5,1,3,6);4;8)$		$f_3^{(4)} \oplus f_2^{(4)} \oplus f_1^{(4)}$	$((0,5,5,6,2);4;8)$
	$f_3^{(1)} \oplus f_2^{(1)}$	$((6,1,3,6,3);4;8)$		$f_3^{(4)} \oplus f_2^{(4)} \oplus f_0^{(4)}$	$((0,6,1,6,3);4;8)$
	$f_2^{(1)} \oplus f_0^{(1)}$	$((6,3,3,1,6);4;8)$	π_5	$f_2^{(5)} \oplus f_0^{(5)}$	$((0,3,2,5,7);4;8)$
π_2	$f_2^{(2)}$	$((0,3,7,2,5);4;8)$		$f_2^{(5)} \oplus f_1^{(5)}$	$((6,7,5,2,6);4;8)$
	$f_1^{(2)} \oplus f_0^{(2)}$	$((1,2,5,6,3);4;8)$		$f_3^{(5)} \oplus f_2^{(5)}$	$((5,5,5,7,2);4;8)$
	$f_3^{(2)} \oplus f_2^{(2)}$	$((7,2,5,2,1);4;8)$		$f_3^{(5)} \oplus f_2^{(5)} \oplus f_0^{(5)}$	$((0,7,5,3,2);4;8)$
π_3	$f_3^{(3)} \oplus f_0^{(3)}$	$((6,7,2,3,6);4;8)$	π_6	$f_3^{(6)} \oplus f_1^{(6)}$	$((7,2,7,5,2);4;8)$
π_7	$f_0^{(7)}$	$((4,3,7,6,5);4;8)$		$f_3^{(6)} \oplus f_2^{(6)} \oplus f_1^{(6)}$	$((6,1,6,5,6);4;8)$

Из табл. 4 видно, что функции $f_3^{(1)}$, $f_2^{(2)}$, $f_3^{(4)}$, $f_0^{(7)}$ являются алгебраическими пороговыми и имеют следующие задания:

$$f_3^{(1)} = 1 \;\Leftrightarrow\; r_4(3x_1 + x_2 + 3x_3) \geqslant 2, \quad f_2^{(2)} = 1 \;\Leftrightarrow\; r_8(3x_1 + 7x_2 + 2x_3 + 5x_4) \geqslant 4,$$
$$f_3^{(4)} = 1 \;\Leftrightarrow\; r_4(2x_1 + x_2 + 3x_3) \geqslant 2, \quad f_0^{(7)} = 1 \;\Leftrightarrow\; r_8(4 + 3x_1 + 7x_2 + 6x_3 + 5x_4) \geqslant 4.$$

Важно отметить, что функции $f_3^{(1)}$ и $f_3^{(4)}$ фиктивно зависят от переменной x_4 (x_4 — старший бит входного числа). Последнее влечёт ухудшение перемешивающих свойств нелинейного слоя.

У подстановки π_5 найдено 4 независимых линейных комбинаций, представимых функциями из класса АПФ. Найдём выражение координатных функций через соответствующие АПФ. Для этого разрешим относительно $f_0^{(5)}$, $f_1^{(5)}$, $f_2^{(5)}$, $f_3^{(5)}$ следующую систему:

$$\begin{pmatrix} f_2^{(5)} \oplus f_0^{(5)} \\ f_2^{(5)} \oplus f_1^{(5)} \\ f_3^{(5)} \oplus f_2^{(5)} \\ f_3^{(5)} \oplus f_2^{(5)} \oplus f_0^{(5)} \end{pmatrix} = \begin{pmatrix} \varphi_0^{(5)} \\ \varphi_1^{(5)} \\ \varphi_2^{(5)} \\ \varphi_3^{(5)} \end{pmatrix},$$

где функции $\varphi_0^{(5)}, \varphi_1^{(5)}, \varphi_2^{(5)}, \varphi_3^{(5)}$ задают соответствующие линейные комбинации из табл. 4:

$$\varphi_0^{(5)} = 1 \;\Leftrightarrow\; r_8(3x_1 + 2x_2 + 5x_3 + 7x_4) \geqslant 4,$$
$$\varphi_1^{(5)} = 1 \;\Leftrightarrow\; r_8(6 + 7x_1 + 5x_2 + 2x_3 + 6x_4) \geqslant 4,$$
$$\varphi_2^{(5)} = 1 \;\Leftrightarrow\; r_8(5 + 5x_1 + 5x_2 + 7x_3 + 2x_4) \geqslant 4,$$
$$\varphi_3^{(5)} = 1 \;\Leftrightarrow\; r_8(7x_1 + 5x_2 + 3x_3 + 2x_4) \geqslant 4.$$

Решение системы и подстановка в целом задаются следующим образом:

$$\pi_5 = \begin{pmatrix} f_3^{(5)} \\ f_2^{(5)} \\ f_1^{(5)} \\ f_0^{(5)} \end{pmatrix} = \begin{pmatrix} \varphi_0^{(5)} \oplus \varphi_3^{(5)} \\ \varphi_0^{(5)} \oplus \varphi_2^{(5)} \oplus \varphi_3^{(5)} \\ \varphi_0^{(5)} \oplus \varphi_1^{(5)} \oplus \varphi_2^{(5)} \oplus \varphi_3^{(5)} \\ \varphi_2^{(5)} \oplus \varphi_3^{(5)} \end{pmatrix}.$$

Данное представление позволяет реализовать подстановку, используя пороговые элементы, поскольку модульное сложение также принадлежит классу АПФ. Отметим, что структуры АПФ в табл. 4 получены с помощью структур, найденных в табл. 2. Основная сложность использования данной таблицы заключается в определении преобразований, переводящих представителя в заданную функцию геометрического типа. Изменения структуры при действии указанных преобразований эквивалентности описаны в [9]. Определение самого геометрического типа не вызывает затруднений при использовании оригинального каталога геометрических типов, опубликованного в [10].

У остальных подстановок подпространство, порождённое координатными функциями, не содержит базис из класса АПФ. В предположении, что все геометрические типы из табл. 3 не являются АПФ, получаем, что только одна из восьми подстановок реализуется через линейные комбинации четырёх АПФ.

Для остальных подстановок выбиралась некоторая функция из класса АПФ произвольного веса, не лежащая в подпространстве, порождённом координатными функциями. Получив базис из пяти функций, мы искали АПФ из расширенного подпространства. Из линейных комбинаций, принадлежащих классу АПФ, составлялась расширенная система, аналогичная полученной при задании подстановки π_5, и решалась относительно координатных функций подстановки. Благоприятным исходом была разрешимость данной системы и соответственно представление подстановки через линейные комбинации пяти АПФ.

Пятая функция выбиралась так, чтобы две или три координатные функции при сложении с ней образовывали функцию из класса АПФ. Один из таких способов — взять произведение двух координатных функций. Произведение функций и их дополнение до исходных имеют вес четыре, а значит, с высокой вероятностью мы получим три функции из класса АПФ. Высокая вероятность обусловливается тем, что из всех 19 геометрических типов, представители которых имеют вес 4, только 3 типа не принадлежат классу АПФ. Кроме того, функция веса 4 не лежит среди линейных комбинаций координатных функций, а значит, линейно не выражается через них.

Второй подход — выбор системы вершин куба, на которых пятая функция принимает единичные значения, так, чтобы при её булевом суммировании (в случае, если эта функция из класса АПФ) с координатными функциями подфункции результирующих функций не были эквивалентны f^* — функции от трёх переменных, которая не представляется через АПФ. Если эта функция имеет вес менее 8, то она также линейно не выражается через линейные комбинации координатных функций. Второй подход обеспечивает получение функций из геометрических типов, перечисленных в табл. 2 и 3. С учётом того, что количество геометрических типов в табл. 2 преобладает, велика вероятность набрать необходимое количество линейных комбинаций из класса АПФ.

Применение предложенных подходов позволило получить задания всех оставшихся подстановок через линейные комбинации пяти АПФ, а если верно предположение, что в табл. 3 нет геометрических типов из класса АПФ, то данные представления минимальны по количеству используемых функций. Ниже приведены реализации подстановок через АПФ без подробного описания способа получения пятой функции:

$$\pi_0 = \begin{pmatrix} \varphi_0^{(0)} \oplus \varphi_1^{(0)} \oplus \varphi_2^{(0)} \oplus \varphi_3^{(0)} \\ \varphi_0^{(0)} \oplus \varphi_1^{(0)} \\ \varphi_2^{(0)} \oplus \varphi_4^{(0)} \\ \varphi_1^{(0)} \oplus \varphi_2^{(0)} \end{pmatrix}, \quad \begin{array}{l} \varphi_0^{(0)} : ((5,4,7,3,2);5;8), \\ \varphi_1^{(0)} : ((1,5,5,7,2);4;8), \\ \varphi_2^{(0)} : ((1,6,5,3,1);6;8), \\ \varphi_3^{(0)} : ((0,1,1,3,2);3;5), \\ \varphi_4^{(0)} : ((0,3,1,3,3);2;5); \end{array}$$

$$\pi_1 = \begin{pmatrix} \varphi_0^{(1)} \\ \varphi_0^{(1)} \oplus \varphi_1^{(1)} \\ \varphi_3^{(1)} \oplus \varphi_4^{(1)} \\ \varphi_1^{(1)} \oplus \varphi_2^{(1)} \end{pmatrix}, \qquad \begin{array}{l} \varphi_0^{(1)} : ((0,3,1,3,0);2;4), \\ \varphi_1^{(1)} : ((6,1,3,6,3);4;8), \\ \varphi_2^{(1)} : ((7,5,1,3,6);4;8), \\ \varphi_3^{(1)} : ((0,2,3,1,2);3;4), \\ \varphi_4^{(1)} : ((6,4,5,2,5);6;8); \end{array}$$

$$\pi_2 = \begin{pmatrix} \varphi_0^{(2)} \oplus \varphi_1^{(2)} \\ \varphi_0^{(2)} \\ \varphi_2^{(2)} \oplus \varphi_3^{(2)} \\ \varphi_2^{(2)} \oplus \varphi_3^{(2)} \oplus \varphi_4^{(2)} \end{pmatrix}, \qquad \begin{array}{l} \varphi_0^{(2)} : ((0,3,7,2,5);4;8), \\ \varphi_1^{(2)} : ((7,2,5,2,1);4;8), \\ \varphi_2^{(2)} : ((7,5,5,2,7);6;8), \\ \varphi_3^{(2)} : ((0,5,3,6,3);5;7), \\ \varphi_4^{(2)} : ((1,2,5,6,3);4;8); \end{array}$$

$$\pi_3 = \begin{pmatrix} \varphi_0^{(3)} \oplus \varphi_1^{(3)} \oplus \varphi_3^{(3)} \\ \varphi_0^{(3)} \oplus \varphi_1^{(3)} \oplus \varphi_2^{(3)} \oplus \varphi_4^{(3)} \\ \varphi_0^{(3)} \oplus \varphi_2^{(3)} \\ \varphi_0^{(3)} \oplus \varphi_1^{(3)} \end{pmatrix}, \qquad \begin{array}{l} \varphi_0^{(3)} : ((1,3,4,1,5);6;8), \\ \varphi_1^{(3)} : ((1,3,2,4,6);5;7), \\ \varphi_2^{(3)} : ((1,3,5,3,6);5;7), \\ \varphi_3^{(3)} : ((5,1,6,5,2);4;8), \\ \varphi_4^{(3)} : ((5,6,2,3,5);4;8); \end{array}$$

$$\pi_4 = \begin{pmatrix} \varphi_0^{(4)} \\ \varphi_0^{(4)} \oplus \varphi_2^{(4)} \oplus \varphi_3^{(4)} \oplus \varphi_4^{(4)} \\ \varphi_1^{(4)} \oplus \varphi_2^{(4)} \oplus \varphi_3^{(4)} \oplus \varphi_4^{(4)} \\ \varphi_3^{(4)} \oplus \varphi_4^{(4)} \end{pmatrix}, \qquad \begin{array}{l} \varphi_0^{(4)} : ((0,2,1,3,0);2;4), \\ \varphi_1^{(4)} : ((0,5,5,6,2);4;8), \\ \varphi_2^{(4)} : ((0,6,1,6,3);4;8), \\ \varphi_3^{(4)} : ((1,3,4,1,5);6;8), \\ \varphi_4^{(4)} : ((4,2,2,4,6);3;7); \end{array}$$

$$\pi_6 = \begin{pmatrix} \varphi_0^{(6)} \oplus \varphi_3^{(6)} \oplus \varphi_4^{(6)} \\ \varphi_2^{(6)} \oplus \varphi_3^{(6)} \\ \varphi_0^{(6)} \oplus \varphi_2^{(6)} \oplus \varphi_3^{(6)} \oplus \varphi_4^{(6)} \\ \varphi_0^{(6)} \oplus \varphi_1^{(6)} \end{pmatrix}, \qquad \begin{array}{l} \varphi_0^{(6)} : ((1,3,4,1,5);6;8), \\ \varphi_1^{(6)} : ((0,4,2,1,3);5;7), \\ \varphi_2^{(6)} : ((4,6,1,3,6);4;8), \\ \varphi_3^{(6)} : ((5,7,2,3,2);4;8), \\ \varphi_4^{(6)} : ((1,1,3,6,2);3;7); \end{array}$$

$$\pi_7 = \begin{pmatrix} \varphi_0^{(7)} \oplus \varphi_2^{(7)} \\ \varphi_2^{(7)} \oplus \varphi_3^{(7)} \\ \varphi_1^{(7)} \oplus \varphi_3^{(7)} \oplus \varphi_4^{(7)} \\ \varphi_1^{(7)} \end{pmatrix}, \qquad \begin{array}{l} \varphi_0^{(8)} : ((1,3,4,1,5);6;8), \\ \varphi_1^{(8)} : ((4,3,7,6,5);4;8), \\ \varphi_2^{(8)} : ((1,7,6,2,5);4;8), \\ \varphi_3^{(8)} : ((0,4,2,0,2);3;5), \\ \varphi_4^{(8)} : ((3,1,0,3,3);3;5). \end{array}$$

3. Представление подстановок алгоритма блочного шифрования 2-ГОСТ линейными комбинациями АПФ

В работе [7] предложен алгоритм блочного шифрования 2-ГОСТ, являющийся модификацией шифрсистемы ГОСТ 28147-89 и отличающийся от последней лишь алгоритмом развертывания ключа, а также тем, что набор S-боксов фиксирован $\pi' = \pi_0 = \pi_1 = \pi_2 = \pi_3$, $\pi'' = \pi_4 = \pi_5 = \pi_6 = \pi_7$, где π_0 и π_4 заданы нижними

строками подстановок

$$\pi' = (6, 10, 15, 4, 3, 8, 5, 0, 13, 14, 7, 1, 2, 11, 12, 9),$$
$$\pi'' = (14, 0, 8, 1, 7, 10, 5, 6, 13, 2, 4, 9, 3, 15, 12, 11).$$

Представим подстановки в виде координатных функций

$$\pi' = \begin{pmatrix} f'_3 \\ f'_2 \\ f'_1 \\ f'_0 \end{pmatrix} = \begin{pmatrix} 0\,1\,1\,0\,0\,1\,0\,0\,1\,1\,0\,0\,0\,1\,1\,1 \\ 1\,0\,1\,1\,0\,0\,1\,0\,1\,1\,1\,0\,0\,0\,1\,0 \\ 1\,1\,1\,0\,1\,0\,0\,0\,0\,1\,1\,0\,1\,1\,0\,0 \\ 0\,0\,1\,0\,1\,0\,1\,0\,1\,0\,1\,1\,0\,1\,0\,1 \end{pmatrix}, \qquad \pi'' = \begin{pmatrix} f''_3 \\ f''_2 \\ f''_1 \\ f''_0 \end{pmatrix} = \begin{pmatrix} 1\,0\,1\,0\,0\,1\,0\,0\,1\,0\,0\,1\,0\,1\,1\,1 \\ 1\,0\,0\,0\,1\,0\,1\,1\,1\,0\,1\,0\,0\,1\,1\,0 \\ 1\,0\,0\,0\,1\,1\,0\,1\,0\,1\,0\,0\,1\,1\,0\,1 \\ 0\,0\,0\,1\,1\,0\,1\,0\,1\,0\,0\,1\,1\,1\,0\,1 \end{pmatrix}.$$

Данная модификация предназначена для низкоресурсной реализации алгоритма блочного шифрования, поэтому задача реализации подстановок с помощью АПФ весьма актуальна.

Для данных подстановок применим приём, описанный в п. 2. В результате анализа каждую из них удалось задать через линейные комбинации пяти АПФ. При этом стоит отметить, что удалось получить линейные комбинации не более двух АПФ для задания координатной функции:

$$\pi' = \begin{pmatrix} f'_3 \\ f'_2 \\ f'_1 \\ f'_0 \end{pmatrix} = \begin{pmatrix} g_1 \oplus g_2 \\ g_3 \oplus g_4 \\ g_3 \\ g_5 \end{pmatrix}, \qquad \pi'' = \begin{pmatrix} f''_3 \\ f''_2 \\ f''_1 \\ f''_0 \end{pmatrix} = \begin{pmatrix} v_1 \oplus v_2 \\ v_1 \oplus v_3 \\ v_1 \oplus v_4 \\ v_4 \oplus v_5 \end{pmatrix},$$

где функции g_1, g_2, g_3, g_4, g_5, v_1, v_2, v_3, v_4, v_5 — алгебраические пороговые:

$$\begin{aligned}
g_1 = 1 &\Leftrightarrow r_9\,(x_1 + 5x_2 + 2x_3 + 2x_4) \geqslant 6, \\
g_2 = 1 &\Leftrightarrow r_7\,(5x_1 + 5x_2 + x_3 + 6x_4) \geqslant 2, \\
g_3 = 1 &\Leftrightarrow r_8\,(7 + 6x_1 + 5x_2 + 6x_3 + x_4) \geqslant 4, \\
g_4 = 1 &\Leftrightarrow r_8\,(2 + 5x_1 + 7x_2 + 3x_3 + 2x_4) \geqslant 4, \\
g_5 = 1 &\Leftrightarrow r_8\,(3 + 5x_1 + x_2 + 2x_3 + 3x_4) \geqslant 4,
\end{aligned}$$

$$\begin{aligned}
v_1 = 1 &\Leftrightarrow r_8\,(6 + 5x_1 + 5x_2 + 2x_3 + x_4) \geqslant 6, \\
v_2 = 1 &\Leftrightarrow r_8\,(3 + 2x_1 + 4x_2 + x_3 + 5x_4) \geqslant 6, \\
v_3 = 1 &\Leftrightarrow r_7\,(3 + x_1 + 6x_2 + 3x_3 + 4x_4) \geqslant 5, \\
v_4 = 1 &\Leftrightarrow r_8\,(2 + x_1 + 6x_2 + 3x_3 + 2x_4) \geqslant 4, \\
v_5 = 1 &\Leftrightarrow r_8\,(3x_1 + 2x_2 + 2x_3 + x_4) \geqslant 4.
\end{aligned}$$

Здесь x_1 — младший бит входного числа, x_4 — старший.

Выводы

В работе приведена типизация булевых функций от четырёх переменных относительно операций перестановки переменных, инвертирования переменных и инвертирования функции. Доказано, что 70 геометрических типов не принадлежат классу АПФ. Для оставшихся применён алгоритм поиска структур АПФ, и для 101 представителя найдены их структуры. По отношению к 51 геометрическому типу выдвинута гипотеза об их непринадлежности классу АПФ.

Рассмотрен вопрос об представимости подстановок из отечественных алгоритмов блочного шифрования Магма и 2-ГОСТ через линейные комбинации минимального

количества АПФ. При этом только одна подстановка представилась линейными комбинациями четырёх АПФ в алгоритме Магма, а остальные — через линейные комбинации пяти АПФ. Указаны подходы к эффективному выбору пятой функции в систему координатных функций подстановок.

Результаты работы могут быть использованы для быстрой реализации алгоритмов блочного шифрования Магма и 2-ГОСТ на перспективной элементной базе.

ЛИТЕРАТУРА

1. *Дертоузос М.* Пороговая логика. М.: Мир, 1967.
2. *Морага К.* Многозначная пороговая логика // Оптические вычисления. М.: Мир, 1993. С. 162–182.
3. *Никонов В. Г., Сидоров Е. С.* О способе построения взаимно однозначных отображений при помощи квазиадамаровых матриц // Вестник Московского государственного университета леса — Лесной вестник. 2009. № 2(65). С. 155–157.
4. *Никонов В. Г., Сошин Д. А.* Геометрический метод построения сбалансированных k-значных пороговых функций и синтез подстановок на их основе // Образовательные ресурсы и технологии. 2014. № 2(5). С. 76–80.
5. *Сошин Д. А.* Построение подстановок на основе пороговых функций многозначной логики // Прикладная дискретная математика. 2016. № 2(32). С. 20–32.
6. ГОСТ Р 34.12-2015 Информационная технология. Криптографическая защита информации. Блочные шифры. М.: Стандартинформ, 2015.
7. *Dmukh A. A., Dygin D. M., and Marshalko G. B.* A lightweight-friendly modification of GOST block cipher // Математические вопросы криптографии. 2014. Т. 5. № 2. С. 47–55.
8. *Сошин Д. А.* Конструктивный метод синтеза сбалансированных k-значных алгебраических пороговых функций // Comp. Nanotechnol. 2015. № 4. С. 31–36.
9. *Сошин Д. А.* Представление геометрических типов булевых функций от трех переменных алгебраическими пороговыми функциями // Прикладная дискретная математика. 2016. № 1(31). С. 32–45.
10. *Никонов В. Г.* Классификация минимальных базисных представлений всех булевых функций от четырех переменных // Обозрение прикладной и промышленной математики. Сер. Дискретная математика. 1994. Т. 1. № 3. С. 458–545.
11. *Зуев Ю. А.* Комбинаторно-вероятностные и геометрические методы в пороговой логике // Дискретная математика. 1991. Т. 3. № 2. С. 47–57.
12. *Ирматов А. А.* Оценки числа пороговых функций // Дискретная математика. 1996. Т. 8. № 4. С. 92–107.
13. *Ирматов А. А., Ковиянич Ж. Д.* Об асимптотике логарифма числа пороговых функций K-значной логики // Дискретная математика. 1998. Т. 10. № 3. С. 35–56.
14. *Winder R. O.* Show parametrs in threshold logic // J. Association for Computing Machinery. 1971. V. 18. No. 2. P. 265–289.

REFERENCES

1. *Dertouzos M.* Porogovaya logika [Threshold Logic]. Moscow, Mir Publ., 1967. (in Russian)
2. *Moraga K.* Mnogoznachnaya porogovaya logika [Multiple-valued threshold logic]. Opticheskie Vychisleniya. Moscow, Mir Publ., 1993, pp. 162–182. (in Russian)
3. *Nikonov V. G. and Sidorov E. S.* O sposobe postroeniya vzaimno odnoznachnykh otobrazheniy pri pomoshchi kvaziadamarovykh matrits [About the possibility of one-to-one mappings representation by the quasi-hadamard matrixes]. Vestnik Moskovskogo Gosudarstvennogo Universiteta Lesa — Lesnoy Vestnik, 2009, no. 2(65), pp. 155–157. (in Russian)

4. *Nikonov V. G. and Soshin D. A.* Geometricheskiy metod postroeniya sbalansirovannykh k-znachnykh porogovykh funktsiy i sintez podstanovok na ikh osnove [The geometric method for constructing a balanced k-valued threshold functions and construction of substitutions based on them]. Obrazovatel'nye Resursy i Tekhnologii, 2014, no. 2(5), pp. 76–80. (in Russian)
5. *Soshin D. A.* Postroenie podstanovok na osnove porogovykh funktsiy mnogoznachnoy logiki [Constructing substitutions on the basis of threshold functions of multivalued logic]. Prikladnaya Diskretnaya Matematika, 2016, no. 2(32), pp. 20–32. (in Russian)
6. GOST R 34.12-2015 Informatsionnaya tekhnologiya. Kriptograficheskaya zashchita informatsii. Blochnye shifry [GOST R 34.12-2015 Information technology. Cryptographic protection of information. Block ciphers]. Moscow, Standartinform Publ., 2015. (in Russian)
7. *Dmukh A. A., Dygin D. M., and Marshalko G. B.* A lightweight-friendly modification of GOST block cipher. Mat. Vopr. Kriptogr., 2014, vol. 5, iss. 2, pp. 47–55.
8. *Soshin D. A.* Konstruktivnyy metod sinteza sbalansirovannykh k-znachnykh algebraicheskikh porogovykh funktsiy [The constructive method for synthesis of balanced k-valued algebraic threshold functions]. Comp. Nanotechnol., 2015, no. 4, pp. 31–36. (in Russian)
9. *Soshin D. A.* Predstavlenie geometricheskikh tipov bulevykh funktsiy ot trekh peremennykh algebraicheskimi porogovymi funktsiyami [Representation of geometric types of Boolean functions in three variables by algebraic threshold functions]. Prikladnaya Diskretnaya Matematika, 2016, no. 1(31), pp. 32–45. (in Russian)
10. *Nikonov V. G.* Klassifikatsiya minimal'nykh bazisnykh predstavleniy vsekh bulevykh funktsiy ot chetyrekh peremennykh [The classification of minimal basic representations of Boolean functions of four variables]. Obozrenie Prikladnoy i Promyshlennoy Matematiki. Ser. Diskretnaya Matematika, 1994, vol. 1, no. 3, pp. 458–545. (in Russian)
11. *Zuev Yu. A.* Kombinatorno-veroyatnostnye i geometricheskie metody v porogovoy logike [Combinatorial-probability and geometric methods in threshold logic]. Diskr. Mat., 1991, vol. 3, no. 2, pp. 47–57. (in Russian)
12. *Irmatov A. A.* Otsenki chisla porogovykh funktsiy [Estimates for the number of threshold functions]. Diskr. Mat., 1996, vol. 8, iss. 4, pp. 92–107. (in Russian)
13. *Irmatov A. A., Koviyanich Zh. D.* Ob asimptotike logarifma chisla porogovykh funktsiy K-znachnoy logiki [On the asymptotics of the logarithm of the number of threshold functions of K-valued logic]. Diskr. Mat., 1998, vol. 10, iss. 3, pp. 35–56. (in Russian)
14. *Winder R. O.* Show parametrs in threshold logic. J. Association for Computing Machinery, 1971, vol. 18, no. 2, pp. 265–289.