МАТЕМАТИЧЕСКИЕ ВОПРОСЫ КРИПТОГРАФИИ
2020 Т. 11 № 4 С. 133–149

УДК 519.719.2 DOI https://doi.org/10.4213/mvk344

Об алгебраической степени и дифференциальной равномерности подстановок пространства V_{2m}, построенных с использованием $(2m, m)$-функций

Д. Б. Фомин

Национальный исследовательский университет «Высшая школа экономики», Москва

Получено 6.VII.2020

Аннотация. Исследуются параметры некоторых подстановок, основанных на конструкции типа «Бабочка», и их влияние на значение алгебраической степени подстановки и показателя дифференциальной равномерности.

Ключевые слова: подстановка, векторная булева функция, дифференциальная равномерность, алгебраическая степень

On the algebraic degree and differential uniformity of permutations on the space V_{2m} constructed via $(2m, m)$-functions

D. B. Fomin

National Research University Higher School of Economics, Moscow

Abstract. We study parameters of some permutations constructed by the «Butterfly» scheme. The influence of these parameters on the algebraic degree of permutation and its differential uniformity is investigated.

Keywords: substitution, vectorial Boolean function, differential uniformity, algebraic degree

Citation: Matematicheskie Voprosy Kriptografii, 2020, v. 11, № 4, pp. 133–149 (Russian)

Введение

TU-представление подстановок (см., например, [1–3]) изучалось в связи с исследованиями декомпозиции подстановок. В то же время интересна обратная задача — построение подстановок с гарантированными криптографическими и эксплуатационными характеристиками, имеющих TU-представление. В [4] был предложен подход к построению подстановок пространства V_8 с криптографическими характеристиками, позволяющими потенциально использовать такие подстановки при синтезе стойких криптографических алгоритмов. При этом подстановки предложенных классов представляли дополнительный интерес ввиду эффективности их аппаратной реализации, что невозможно для случайных подстановок пространства V_8, см. [5]. В [6] исследовалась более общая задача о построении подстановок пространства V_{2m} с нелинейностью не ниже заданной границы.

Настоящая работа построена следующим образом. В разделе 1 даны основные определения и кратко изложены результаты, полученные в [6]. В разделе 2 приведены необходимые и достаточные условия, позволяющие гарантировать максимально возможную алгебраическую степень подстановки, построенной с использованием алгоритма из [6]. В разделе 3 сформулирована лемма, позволяющая осуществлять направленный поиск дифференциально δ-равномерных подстановок с использованием алгоритма из [6], и с ее помощью проведено теоретическое обоснование результатов, полученных экспериментально в [4].

1. Основные понятия

Будем использовать следующие определения и обозначения. Полем из двух элементов назовем множество $\mathbb{F}_2 = \{0, 1\}$ с заданными естественным образом операциями сложения $+$ и умножения $\cdot$. Пусть $(V_n, +) = \left\{(a_0, a_1, \ldots, a_{n-1}), a_i \in \mathbb{F}_2, i \in \overline{0, n-1}\right\}$ — арифметическое векторное пространство размерности n, $\theta = (0, 0, \ldots, 0)$ — нуль векторного пространства. Если рассмотреть аддитивную группу векторного пространства $(V_n, +)$ и задать специальным образом операцию умножения, то можно построить поле, которое будем обозначать $(\mathbb{F}_{2^n}, +, \cdot)$.

Для $a \in V_n$, $b \in V_m$ через $a\|b \in V_{n+m}$ обозначим конкатенацию двух векторов.

Для произвольных $a, b \in V_n$ скалярным произведением векторов на-

зывается элемент поля $\mathbb{F}_2$, определяемый формулой

$$\langle a, b\rangle = \sum_{i=0}^{n-1} a_i \cdot b_i,$$

где сложение и умножение проводятся в поле $\mathbb{F}_2$.

Определение 1. Векторной булевой функцией (или (n, m)-функцией) S называется отображение $V_n \to V_m$, $n, m \in \mathbb{N}$.

Любую векторную булеву функцию S можно представить в виде упорядоченного набора ее координатных функций: $S(x) = (f_1(x), f_2(x), \ldots, f_m(x))$, где $x \in V_n$, $f_i(x)$ — булевы функции, $i \in \overline{1, m}$.

В случае когда значения n и m понятны из контекста, вместо термина «(n, m)-функция» будем использовать термин «функция». Биективная (n, n)-функция — это элемент симметрической группы $S(V_n)$, или подстановка.

Линейными подстановками будем называть элементы $GL(n, 2)$ — полной линейной группы преобразований, аффинными подстановками — элементы группы $AGL(n, 2) = GL(n, 2)H_n$, где H_n — группа сдвигов пространства V_n.

Определим основные криптографические характеристики векторных булевых функций, рассматриваемых в статье.

Определение 2. Значение преобразования Уолша – Адамара (WHT) $W_S(a, b)$ (n, m)-функции S для значений $a \in V_n$, $b \in V_m$ определяется равенством

$$W_S^{a,b} = \sum_{x \in V_n} (-1)^{\langle a,x\rangle + \langle b,S(x)\rangle}.$$

Определение 3. Нелинейность (n, m)-функции S обозначается N_S и определяется равенством

$$N_S = 2^{n-1} - \frac{1}{2} \max_{\substack{a \in V_n, \\ b \in V_m \setminus \theta}} \left| W_S^{a,b} \right|.$$

Определение 4. Алгебраической степенью $\deg(S)$ (n, m)-функции S называется минимальная степень многочлена Жегалкина среди всевозможных линейных комбинаций ее координатных функций $\langle a, S(x)\rangle$ по всем возможным $a \in V_m \setminus \theta$:

$$\deg(S) = \min_{a \in V_m \setminus \theta} \deg\left(\langle a, S(x)\rangle\right).$$

Для подстановок пространства V_n максимально возможная степень нелинейности равна $n-1$, см. [7].

Определение 5. Для произвольных $a \in V_n \backslash \theta, b \in V_m$ положим

$$\delta_S^{a,b} = \left|\{x \in \mathbb{F}_{2^n} | S(x+a) + S(x) = b\}\right|.$$

Будем говорить, что S является дифференциально δ_S-равномерной функцией, если

$$\delta_S = \max_{\substack{a \in V_n \backslash \theta, \\ b \in V_m}} \delta_S^{a,b},$$

а значение δ_S будем называть показателем дифференциальной равномерности подстановки S.

При синтезе криптографических примитивов, как правило, используют подстановки с минимально возможным показателем дифференциальной равномерности. Наименьшим возможным значением является 2, однако с точностью до CCZ-эквивалентности известна только одна 2-равномерная подстановка пространства V_m в случае четного m, см. [3]. При синтезе стойких криптографических алгоритмов используются и дифференциально 8-равномерные подстановки, как, например, в отечественном алгоритме хеширования ГОСТ Р 34.11-2012.

Будем говорить, что две (n,m)-функции S_1 и S_2 являются линейно эквивалентными, если существуют такие линейные подстановки $L_1 \in GL(n,2)$ и $L_2 \in GL(m,2)$, что $S_1 = L_2 \cdot S_2 \cdot L_1$. Будем также говорить, что две (n,m)-функции являются аффинно-эквивалентными, если существуют две такие аффинные подстановки $A_1 \in AGL(n,2)$ и $A_2 \in AGL(m,2)$, что $S_1 = A_2 \cdot S_2 \cdot A_1$.

Элементу $v \in V_{2m}$ можно поставить в соответствие пару элементов (x_1, x_2), $x_1, x_2 \in V_m$, по следующему правилу: если $v = (v_0, \ldots, v_{m-1}, v_m, \ldots, v_{2m-1})$, то $v \cong (x_1, x_2)$, где $x_1 = (v_0, \ldots, v_{m-1}) \in V_m$, $x_2 = (v_m, \ldots, v_{2m-1}) \in V_m$. Таким образом, задавая подстановку на множестве пар векторов (x_1, x_2), определяем подстановку пространства V_{2m}.

Определение 6. Пусть функции F_1, $F_2 \colon V_m \times V_m \to V_m$ при любой фиксации второго аргумента являются биекциями по первому аргументу. Определим преобразование $F(x_1, x_2) = (y_1, y_2)$, которое будем называть *F-конструкцией* (см. рис.), следующим образом:

$$\begin{cases} y_1 = F_1(x_1, x_2), \\ y_2 = F_2(x_2, y_1). \end{cases} \tag{1}$$

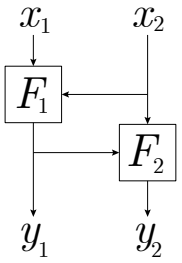

Рис. F-конструкция

Определение 7. $(2m, m)$-функцию $s'(x, y)$ назовем функцией с одной выколотой точкой $\dot{y}$, если для всех $y \neq \dot{y}$ функция $s'(x, y)$ является подстановкой по переменной x и $s'(x, \dot{y})$ не является подстановкой по переменной x. Если при этом $s'(x, \dot{y}) = \text{const}$, то такую функцию будем называть C-функцией с выколотой точкой $\dot{y}$.

В случае когда значение выколотой точки ясно из контекста, будем говорить просто о C-функции.

В [6] предложен и обоснован алгоритм 1, который строит функции F_1 и F_2 по формуле (1) с использованием C-функций s'_i с выколотыми точками $\dot{y}_i$ и подстановок $\widehat{\pi}_i$, $i \in \{1, 2\}$:

$$y_1 = F_1(x_1, x_2) = \begin{cases} s'_1(x_1, x_2), & x_2 \neq \dot{y}_1, \\ \widehat{\pi}_1(x_1), & x_2 = \dot{y}_1, \end{cases} \tag{2}$$

$$y_2 = F_2(x_2, y_1) = \begin{cases} s'_2(x_2, y_1), & y_1 \neq \dot{y}_2, \\ \widehat{\pi}_2(x_2), & y_1 = \dot{y}_2. \end{cases} \tag{3}$$

Согласно определению при фиксации произвольного $x_2 \neq \dot{y}_i$ функции $s'_i(x_1, x_2)$ являются биекциями по переменной x_1, $i \in \{1, 2\}$. Тогда для $x_2 \neq \dot{y}_i$ корректно определены биективные отображения $s'^{-1}_i(y, x_2)$ как функции от одной переменной y при фиксированном $x_2 \neq \dot{y}_i$. Аналогично, корректно определены функции $F_i^{-1}(y, x_2)$ как подстановки по переменной y при фиксированном значении $x_2 \in V_m$.

Выпишем выражение для подстановки $F^{-1}(y_1, y_2) = (x_1, x_2)$, обратной к F из формулы (1), с учетом (2)–(3):

$$x_2 = F_2^{-1}(y_1, y_2) = \begin{cases} s'^{-1}_2(y_2, y_1), & y_1 \neq \dot{y}_2, \\ \widehat{\pi}_2^{-1}(y_2), & y_1 = \dot{y}_2, \end{cases} \tag{4}$$

$$x_1 = F_1^{-1}(y_1, x_2) = \begin{cases} s'^{-1}_1(y_1, x_2), & x_2 \neq \dot{y}_1, \\ \widehat{\pi}_1^{-1}(y_1), & x_2 = \dot{y}_1. \end{cases} \tag{5}$$

Заметим, что согласно формуле (3) значение y_2 определяется по x_2 и y_1, а значение x_1 определяется по y_1 и x_2 формулой (5). В [6] показано (см. предложение 5, алгоритм 1), что при дополнительных ограничениях на функции s'_i и подстановки $\widehat{\pi}_i$, $i \in \{1, 2\}$, величину y_2 можно представить как функцию от x_1 и x_2 с использованием $(2m, m)$-функций s''_2 с одной выколотой точкой $\pi_1^{-1}(\dot{y}_2)$ по формуле

$$y_2 = FI_2(x_1, x_2) = \begin{cases} s''_2(x_2, x_1), & x_1 \neq \widehat{\pi}_1^{-1}(\dot{y}_2), \\ \widehat{\pi}_2(x_2), & x_1 = \widehat{\pi}_1^{-1}(\dot{y}_2), \end{cases} \tag{6}$$

а x_1 можно представить как функцию от y_1 и y_2 с использованием $(2m, m)$-функций s''_1 с одной выколотой точкой $\dot{y}_1$ по формуле

$$x_1 = FI_1(y_1, y_2) = \begin{cases} s''_1(y_1, y_2), & y_2 \neq \dot{y}_1, \\ \widehat{\pi}_1^{-1}(y_1), & y_2 = \dot{y}_1. \end{cases} \tag{7}$$

В этом случае подстановки F и F^{-1} определяются формулами

$$(y_1, y_2) = F(x_1, x_2) = (F_1(x_1, x_2), FI_2(x_1, x_2)), \tag{8}$$

$$(x_1, x_2) = F^{-1}(y_1, y_2) = \left(FI_1(y_1, y_2), F_2^{-1}(y_1, y_2)\right).$$

В [6] дополнительно считается, что $(2m, m)$-функции s_i^{-1}, s''_i должны быть C-функциями.

2. Алгебраическая степень подстановок, построенных при помощи F-конструкции

Покажем, как можно гарантировать максимально возможную алгебраическую степень подстановок F и F^{-1}. Верно следующее предложение.

Предложение 1. *Пусть подстановка F задается формулой (8). Тогда*

- *если* $\deg(s'_i) \neq 2m-1$ *и* $(2m, m)$*-функция* s'_i *является* C*-функцией, то*
$$\deg(F_i) = 2m - 1 \Leftrightarrow \deg(\widehat{\pi}_i) = m - 1, i \in \{1, 2\},$$
- *если* $\deg\left(s_i'^{-1}\right) \neq 2m-1$ *и* $(2m, m)$*-функция* $s_i'^{-1}$ *является* C*-функцией, то*
$$\deg\left(F_i^{-1}\right) = 2m - 1 \Leftrightarrow \deg(\widehat{\pi}_1) = m - 1, i \in \{1, 2\},$$

– *если* $\deg(s_i'') \neq 2m-1$ *и* $(2m, m)$*-функция* s_i'' *является* C*-функцией, то*

$$\deg(FI_i) = 2m-1 \Leftrightarrow \deg(\widehat{\pi}_2) = m-1, i \in \{1, 2\}.$$

Доказательство. Докажем утверждение для функции F_1. Остальные случаи рассматриваются аналогично.

Определим функцию $I_a(y)\colon V_m \to \mathbb{F}_2$, принимающую значение 1, если $a = y$, и значение 0 в противном случае. Заметим, что $\deg(I_a) = m$. Функцию $F_1(x_1, x_2)$ можно представить следующим образом:

$$F_1(x_1, x_2) = s_1'(x_1, x_2) \oplus I_{\dot{y}_1}(x_2) \cdot (s_1'(x_1, \dot{y}_1) \oplus \widehat{\pi}_1(x_1)).$$

Далее,

$$\deg(I_{\dot{y}_1}(x_2) \cdot \widehat{\pi}_1(x_1)) = m + \deg(\widehat{\pi}_1),$$

$$\deg(I_{\dot{y}_1}(x_2) \cdot s_1'(x_1, \dot{y}_1)) \leqslant m.$$

Последнее неравенство выполняется в силу условий предложения: $s_1'(x_1, \dot{y}_1) = \text{const}$. Тогда, так как $\deg(s_1'(x_1, x_2)) \neq 2m-1$, то

$$\deg(F_1) = 2m-1 \Leftrightarrow \deg(\widehat{\pi}_1) = m-1.$$

□

Следствие. *Пусть выполняются все условия предложения 1 и*

$$\deg(F_i) = \deg\left(F_i^{-1}\right) = \deg(FI_i) = 2m-1.$$

Тогда подстановка F *и подстановка* F^{-1} *имеют максимально возможную алгебраическую степень, равную* $2m-1$.

Доказательство. Докажем утверждение для подстановки F, для подстановки F^{-1} оно доказывается аналогично. Подстановка $F(x_1, x_2) = (y_1, y_2)$ задается с помощью функций $F_1(x_1, x_2)$ и $FI_2(x_1, x_2)$ (см. формулу (8)). В предложении 1 было показано, что

$$\deg(F_1) = 2m-1 \Leftrightarrow \deg(\widehat{\pi}_1) = m-1$$

и

$$\deg(FI_2) = 2m-1 \Leftrightarrow \deg(\widehat{\pi}_2) = m-1.$$

Для доказательства следствия необходимо показать, что произвольная невырожденная линейная комбинация координатных функций F_1

и FI_2 имеет алгебраическую степень, равную $2m-1$. Пусть $\alpha, \beta \in V_m$, $\alpha, \beta \neq \theta$. Рассмотрим

$$\langle \alpha, F_1(x_1, x_2)\rangle + \langle \beta, F_2(x_1, x_2)\rangle .$$

Пусть $x_1 = (v_0, \ldots, v_{m-1})$, $x_2 = (v_m, \ldots, v_{2m-1})$, $v_i \in \mathbb{F}_2$. Заметим, что при выполнении условий следствия существует моном степени $2m-1$ вида $\langle \alpha, F_1(x_1, x_2)\rangle$:

$$v_{i_1} \cdot \ldots v_{i_{m-1}} \cdot v_m \cdot v_{m+1} \cdot \ldots \cdot v_{2m-1},$$

где $i_1, \ldots, i_{m-1}$ — попарно различные числа из множества $\overline{0, m-1}$, и моном степени $2m-1$ вида $\langle \beta, FI_2(x_1, x_2)\rangle$:

$$v_0 \cdot v_1 \cdot \ldots v_{m-1} \cdot v_{j_1} \cdot \ldots v_{j_{m-1}},$$

где $j_1, \ldots, j_{m-1}$ — попарно различные числа из множества $\overline{m, 2m-1}$ и при сложении эти два монома не сократятся. □

Как правило, условия предложения 1 легко проверяются, что позволяет гарантировать высокую алгебраическую степень подстановки.

3. Дифференциальная равномерность подстановок, построенных при помощи F-конструкции

Рассмотрим вопрос о связи показателя дифференциальной равномерности подстановки F с параметрами преобразований, используемых при ее построении.

Лемма. *Пусть подстановка F вычисляется по формуле (8), $a_1, a_2, b_1, b_2 \in V_m$, тогда $\delta_F^{a_1\|a_2, b_1\|b_2}$ не меньше количества решений системы уравнений*

$$\begin{cases} s_1'(x_1, x_2) \oplus s_1'(x_1 \oplus a_1, x_2 \oplus a_2) = b_1, \\ s_2''(x_1, x_2) \oplus s_2''(x_1 \oplus a_1, x_2 \oplus a_2) = b_2, \end{cases} \tag{9}$$

со следующими ограничениями на значения переменных x_1 и x_2:

1) $x_2 \neq \dot{y}_1$, $x_2 \neq \dot{y}_1 \oplus a_2$,

2) $x_1 \neq \widehat{\pi}_1^{-1}(\dot{y}_2)$, $x_1 \neq \widehat{\pi}_1^{-1}(\dot{y}_2) \oplus a_1$.

Доказательство. Доказательство предложения очевидно, так как при ограничениях $x_2 \neq \dot{y}_1$, $x_2 \neq \dot{y}_1 \oplus a_2$ и $x_1 \neq \widehat{\pi}_1^{-1}(\dot{y}_2)$, $x_1 \neq \widehat{\pi}_1^{-1}(\dot{y}_2) \oplus a_1$ уравнения, задающие подстановку, имеют вид (9). □

Замечание. Лемма позволяет осуществлять направленный поиск пар функций $s'_1(x_1, x_2)$ и $s''_2(x_1, x_2)$ так, чтобы показатель дифференциальной равномерности построенной подстановки F был не выше заранее заданной границы Δ. Необходимым условием дифференциальной Δ-равномерности подстановки F является то, что количество решений системы (9) не превосходит Δ.

Покажем на примере параметрических семейств подстановок, рассмотренных в [4], что лемма позволяет ограничить возможные значения параметров, при которых подстановка F имеет показатель дифференциальной равномерности не меньше заданного.

3.1. Конструкция «A»

Пусть

$$y_1 = F_1(x_1, x_2) = \begin{cases} \pi_1(x_1) \cdot x_2, & x_2 \neq \theta, \\ \widehat{\pi}_1(x_1), & x_2 = \theta, \end{cases} \tag{10}$$

$$y_2 = F_2(x_2, y_1) = \begin{cases} \pi_2(x_2 \cdot y_1), & y_1 \neq \theta, \\ \widehat{\pi}_2(x_2), & y_1 = \theta, \end{cases} \tag{11}$$

где подстановки π_i, $\widehat{\pi}_i$, $i \in \{1, 2\}$, являются параметрами семейства подстановок, задаваемых формулой (1).

Заметим, что функции

$$s'_1(x_1, x_2) = \pi_1(x_1) \cdot x_2 \quad \text{и} \quad s'_2(x_2, y_1) = \pi_2(x_2 \cdot y_1)$$

есть C-функции, имеющие по одной выколотой точке $x_2 = \theta$ и $y_1 = \theta$ соответственно. К этим функциям применимы предложение 3 и следствие 3 из [6]. Стоит отметить, что s'_1 является бент-функцией, принадлежащей классу Майораны – Макфарленда, а функция s'_2 принадлежит расширенному классу бент-функций Майораны – Макфарленда, если π_2 — линейная подстановка (см. например, [7]).

Представим y_2 как функцию от x_1 и x_2, используя предложение 5 из [6]. Для выполнения условий указанного предложения необходимо, чтобы

$$F_1\left(\widehat{\pi}_1^{-1}(\theta), x_2\right) = \theta, \tag{12}$$

$$F_2(\theta, y_1) = \widehat{\pi}_2(\theta). \tag{13}$$

Из равенства (12) следует, что $\pi_1(x_1) = \theta \Leftrightarrow \widehat{\pi}\,(x_1) = \theta$, а из равенства (13) следует, что $\pi_2(\theta) = \widehat{\pi}_2(\theta)$. Тогда

$$y_2 = \begin{cases} \pi_2\left((x_2)^2 \cdot \pi_1\,(x_1)\right), & x_1 \neq \widehat{\pi}^{-1}(\theta), \\ \widehat{\pi}_2\,(x_2)\,, & x_1 = \widehat{\pi}^{-1}(\theta). \end{cases} \tag{14}$$

Пусть $\widehat{\pi}_1^{-1}(\theta) = c_1$, $\widehat{\pi}_2(\theta) = c_2$, подстановка $F(x_1, x_2) = (y_1, y_2)$ определяется формулами (10), (14). Тогда аффинно-эквивалентная подстановка $G = F(x_1 + c_1, x_2) + (\theta, c_2)$, очевидно, также определяется формулами (10), (14) (с другими параметрами). В связи с этим далее будем, не теряя общности, рассматривать только случай, когда θ является неподвижной точкой для π_i, $\widehat{\pi}_i$, $i \in \{1, 2\}$.

Определение 8. Подстановку $F_A(x_1, x_2) = (y_1, y_2)$, определяемую равенствами

$$y_1 = \begin{cases} \pi_1\,(x_1) \cdot x_2, & x_2 \neq \theta, \\ \widehat{\pi}_1\,(x_1)\,, & x_2 = \theta, \end{cases}$$

$$y_2 = \begin{cases} \pi_2\left((x_2)^2 \cdot \pi_1\,(x_1)\right), & x_1 \neq \theta, \\ \widehat{\pi}_2\,(x_2)\,, & x_1 = \theta, \end{cases}$$

где $x_1, x_2 \in V_m$, $\pi_i, \widehat{\pi}_i \in S\,(V_m)$, $\pi_i(\theta) = \theta$, $\widehat{\pi}_i(\theta) = \theta$, $i \in \{1, 2\}$, будем называть подстановкой из параметрического семейства типа «A» или просто подстановкой типа «A».

Следующее предложение позволяет существенно сократить параметрическое семейство типа «A». Можно не рассматривать подстановки с линейным параметром π_2, так как они являются дифференциально δ_{F_A}-равномерными с $\delta_{F_A} \geqslant 2^m - 2$, что не позволяет использовать их при синтезе стойких криптографических примитивов.

Предложение 2. *Пусть F_A — подстановка из параметрического семейства типа «A». Если параметр π_2 есть линейная подстановка, то $\delta_{F_A} \geqslant 2^m - 2$.*

Доказательство. Воспользуемся леммой, где $s'(x_1, x_2) = \pi_1(x_1) \cdot x_2$, $s''(x_1, x_2) = \pi_2\,(x_2^2 \cdot \pi_1(x_1))$. Пусть $x_i, a_i, b_i \in V_m$, $i \in \{1, 2\}$, $x_2 \neq \theta$, $x_2 \neq a_2$, $x_1 \neq \theta$, $x_1 \neq a_1$. Рассмотрим разностные соотношения, соответствующие подстановке F_A. Тогда:

$$\begin{cases} \pi_1\,(x_1 + a_1) \cdot (x_2 + a_2) + \pi_1\,(x_1) \cdot x_2 = b_1, \\ \pi_2\left((x_2 + a_2)^2 \cdot \pi_1\,(x_1 + a_1)\right) + \pi_2\,(x_2^2 \cdot \pi_1\,(x_1)) = b_2. \end{cases}$$

Рассмотрим случай $a_1 = \theta$, $a_2 \neq \theta$. Так как π_2 — подстановка и $a_2 \neq \theta$, то

$$\begin{cases} \pi_1(x_1) \cdot (x_2 + a_2) + \pi_1(x_1) \cdot x_2 = b_1 \\ \pi_2\left((x_2 + a_2)^2 \cdot \pi_1(x_1)\right) + \pi_2(x_2^2 \cdot \pi_1(x_1)) = b_2 \end{cases} \Rightarrow$$

$$\begin{cases} \pi_1(x_1) = b_1 \cdot a_2^{-1} \\ \pi_2\left((x_2^2 + a_2^2) \cdot \pi_1(x_1) + x_2^2 \cdot \pi_1(x_1)\right) = b_2 \end{cases} \Rightarrow$$

$$\begin{cases} \pi_1(x_1) = b_1 \cdot a_2^{-1} \\ \pi_2(a_2^2 \cdot \pi_1(x_1)) = b_2 \end{cases} \Rightarrow \begin{cases} \pi_1(x_1) = b_1 \cdot a_2^{-1} \\ \pi_2(a_2 \cdot b_1) = b_2 \end{cases}$$

Отсюда следует, что если $x_1 = \pi^{-1}\left(b_1 \cdot a_2^{-1}\right)$ и $\pi_2(a_2 \cdot b_1) = b_2$, то x_2 может принимать любые допустимые значения. Так как такое b_2 всегда существует и $x_2 \neq \theta$, $x_2 \neq a_1$, то при фиксации подходящего b_2 количество решений рассматриваемой системы не меньше $2^m - 2$. □

Ранее было отмечено, что в случае когда π_2 — линейная функция, функция s_1', определенная в этом разделе, является бент-функцией и обладает наибольшей возможной нелинейностью, но согласно предложению 2 построенная подстановка в целом будет иметь высокий показатель дифференциальной равномерности.

Остается вопрос о выборе конкретных подстановок π_i, $\widehat{\pi}_i$, $i \in \{1, 2\}$. В [4] рассматривались подстановки типа «A» для случая $m = 4$.

Для простоты параметры π_i, $i \in \{1, 2\}$, будем фиксировать мономиальными подстановками. Такие подстановки имеют вид x^d, где НОД$(d, 2^m - 2) = 1$. В силу малой теоремы Ферма можно рассматривать только $d < 2^m - 2$.

В этом случае формулы, задающие подстановку, можно переписать в следующем виде:

$$y_1 = \begin{cases} x_1^{\alpha} \cdot x_2, & x_2 \neq \theta, \\ \widehat{\pi}_1(x_1), & x_2 = \theta, \end{cases}$$

$$y_2 = \begin{cases} (x_2^2 \cdot x_1^{\alpha})^{\beta} = x_2^{2\beta} \cdot x_1^{\alpha\beta}, & x_1 \neq \theta, \\ \widehat{\pi}_2(x_2), & x_1 = \theta. \end{cases}$$

При этом согласно предложению 2 преобразование x^{β} должно быть нелинейным преобразованием. Такие подстановки рассматривались в [4] для случая $m = 4$, где экспериментально исследовались подстановки типа «A» с мономиальными значениями параметров. Для случая

$m = 4$ существует 8 таких значений d, что НОД $(d, 2^4 - 2) = 1$: это 1, 2, 4, 7, 8, 11, 13, 14. Если $d \in \{1, 2, 4, 8\}$, то x^d задает линейную подстановку. Согласно предложению 2 подстановка π_2 не может быть линейной. В [4] для произвольных $\alpha \in \{1, 2, 4, 7, 8, 11, 13, 14\}$ и $\beta \in \{7, 11, 13, 14\}$ при подходящем выборе $\widehat{\pi}_i$ получены подстановки со следующими криптографическими характеристиками:

– нелинейность — 108,

– показатель дифференциальной равномерности — 6,

– алгебраическая степень нелинейности — 7.

Таким образом, в случае $m = 4$ и мономиальных подстановок π_1, π_2 в предложении 2 содержится достаточное условие для существования подстановок с «хорошими» криптографическими характеристиками.

3.2. Конструкция «Б»

Пусть

$$F_1(x_1, x_2) = \begin{cases} x_1 \cdot \pi_1(x_2), & \pi_1(x_2) \neq \theta, \\ \widehat{\pi}_1(x_1), & \pi_1(x_2) = \theta, \end{cases}$$

$$F_2(x_2, y_1) = \begin{cases} x_2 \cdot \pi_2(y_1), & \pi_2(y_2) \neq \theta, \\ \widehat{\pi}_2(x_2), & \pi_2(y_2) = \theta, \end{cases}$$

где подстановки π_i, $\widehat{\pi}_i$, $i \in \{1, 2\}$, являются параметрами семейства подстановок, задаваемых выражением (1).

Отметим, что функции $s'(x_1, x_2) = x_1 \cdot \pi_1(x_2)$ и $s'(x_2, y_1) = x_2 \cdot \pi_2(y_1)$ есть C-функции, а также бент-функции Майораны – Макфарленда, см. [7].

Как и в разделе 3.1, представим y_2 как функцию от x_1 и x_2, используя предложение 5 из [6], и будем рассматривать только случай, когда θ является неподвижной точной для π_i, $\widehat{\pi}_i$, $i \in \{1, 2\}$.

Определение 9. Подстановку $F_B(x_1, x_2) = (y_1, y_2)$, определяемую равенствами

$$y_1 = \begin{cases} x_1 \cdot \pi_1(x_2), & x_2 \neq \theta, \\ \widehat{\pi}_1(x_1), & x_2 = \theta, \end{cases}$$

$$y_2 = \begin{cases} x_2 \cdot \pi_2(x_1 \cdot \pi_1(x_2)), & x_1 \neq \theta, \\ \widehat{\pi}_2(x_2), & x_1 = \theta, \end{cases}$$

где $x_1, x_2 \in V_m$, $\pi_i, \widehat{\pi}_i \in S(V_m)$, $\pi_i(\theta) = \theta$, $\widehat{\pi}_i(\theta) = \theta$, $i \in \{1, 2\}$, будем называть подстановкой из параметрического семейства типа «Б» или просто подстановкой типа «Б».

Зададим подстановку, обратную к подстановке типа «Б»:

$$x_1 = \begin{cases} y_1 \cdot \pi_2(y_2)^{-1}, & \pi_2(y_2) \neq \theta, \\ \widehat{\pi}_2^{-1}(y_1), & \pi_2(y_2) = \theta, \end{cases}$$

$$x_2 = \begin{cases} y_2 \cdot \pi_1(x_2)^{-1}, & \pi_1(x_2) \neq \theta, \\ \widehat{\pi}_1^{-1}(y_2), & \pi_1(x_2) = \theta. \end{cases}$$

Таким образом, подстановка, обратная к подстановке типа «Б», сама является подстановкой типа «Б».

Воспользуемся леммой и опишем значения параметров, при которых подстановка заведомо будет иметь высокий показатель дифференциальной равномерности.

Предложение 3. *Пусть $H < S(V_m)$ — множество линейных подстановок. Если $\pi_2 \in H$ или $\pi_1 \in x^{-1}H$, то $\delta_{S_B} \geqslant 2^m - 2$.*

Доказательство. Рассмотрим случай $\pi_2 \in H$. Пусть $a_1, b_1, b_2 \in V_m$ и $x_2 \neq \theta$, $x_1 \neq a_1$, $x_1 \neq \theta$. Найдем количество решений системы уравнений

$$\begin{cases} x_1 \cdot \pi_1(x_2) + (x_1 + a_1) \cdot \pi_1(x_2) = b_1, \\ x_2 \cdot \pi_2(x_1 \cdot \pi_1(x_2)) + x_2 \cdot \pi_2((x_1 + a_1) \cdot \pi_1(x_2)) = b_2. \end{cases}$$

Так как π_2 — линейная функция, то

$$\begin{cases} x_1 \cdot \pi_1(x_2) + (x_1 + a_1) \cdot \pi_1(x_2) = b_1, \\ x_2 \cdot \pi_2(x_1 \cdot \pi_1(x_2)) + x_2 \cdot \pi_2((x_1 + a_1) \cdot \pi_1(x_2)) = b_2, \end{cases} \Rightarrow$$

$$\Rightarrow \begin{cases} a_1 \cdot \pi_1(x_2) = b_1, \\ \pi_2(b_1) = b_2 \cdot x_2^{-1}. \end{cases}$$

Последняя система не зависит от значения переменной x_1. Осталось заметить, что при любой фиксации x_2 существуют такие b_1, a_1 и b_2, что равенства в последней системе будут выполняться. Последнее доказывает, что показатель дифференциальной равномерности не меньше $2^m - 2$.

Случай $\pi_2 \in x^{-1}H$ рассматривается аналогично, так как обратная подстановка к подстановке типа «Б» есть подстановка типа «Б». □

Рассмотрим случай мономиальных подстановок: $\pi_1 = x^\alpha$, $\pi_2 = x^\beta$, где α, β удовлетворяют равенствам НОД$(\alpha, 2^4 - 2) = 1$, НОД$(\beta, 2^4 - 2) = 1$. Тогда

$$y_2 = \begin{cases} x_1 \cdot x_2^\alpha, & x_2 \neq \theta, \\ \widehat{\pi}_1(x_1), & x_2 = \theta, \end{cases}$$

$$y_1 = \begin{cases} x_2 \cdot (x_1 \cdot x_2^\alpha)^\beta = x_1^\beta \cdot x_2^{\alpha\beta+1}, & x_1 \neq \theta, \\ \widehat{\pi}_2(x_2), & x_1 = \theta. \end{cases}$$

В [4] были экспериментально исследованы подстановки типа «Б» в случае $m = 4$. По предложению 3 параметры α и β должны удовлетворять условиям $\alpha \in \{1, 2, 4, 8\}$, $\beta \in \{7, 11, 13, 14\}$. Покажем, что при фиксации α существует единственное β, при котором подстановка может иметь высокий показатель дифференциальной δ-равномерности.

Предложение 4. *Пусть* $m = 4$ *и* $\pi_1 = x^\alpha$, $\pi_2 = x^\beta$, *где* α, β *удовлетворяют равенствам* НОД$(\alpha, 2^4 - 2) = 1$, НОД$(\beta, 2^4 - 2) = 1$. *Тогда если* $\alpha\beta + 1 \neq 14 \pmod{15}$, *то* $\delta_{F_B} \geqslant 2^m - 2$.

Доказательство. Величина $\alpha\beta + 1$ может принимать четыре значения: 0, 8, 12 и 14. Доказательство для случаев 0 и 8 проводится аналогично доказательству предложения 3 (рассматривается аналогичная система).

В случае когда $\alpha\beta + 1 = 12$ и x_i, $i \in \{1, 2\}$, отличны от θ и единицы поля 1, рассмотрим систему

$$\begin{cases} x_1 \cdot x_2^\alpha + (x_1 + 1) \cdot (x_2 + 1)^\alpha = 1, \\ x_1^\beta \cdot x_2^{12} + (x_1 + 1)^\beta \cdot (x_2 + 1)^{12} = 1, \end{cases} \Rightarrow$$

$$\begin{cases} x_1 = x_2^\alpha, \\ x_2^{\beta\alpha} \cdot x_2^{12} + (x_2^\beta + 1^\beta)^\alpha \cdot (x_2 + 1)^{12} = 1, \end{cases} \Rightarrow$$

$$\begin{cases} x_1 + 1 = (x_2 + 1)^\alpha, \\ x_2^{\beta\alpha} \cdot x_2^{12} + (x_2 + 1)^{\alpha\beta} \cdot (x_2 + 1)^{12} = 1, \end{cases} \Rightarrow$$

$$\begin{cases} x_1 + 1 = (x_2 + 1)^\alpha, \\ x_2^8 + (x_2 + 1)^8 = 1, \end{cases} \Rightarrow \begin{cases} x_1 + 1 = (x_2 + 1)^\alpha, \\ 1 = 1. \end{cases}$$

Фиксируя x_1, однозначно находим x_2, что завершает доказательство предложения. □

Таким образом, возможны следующие случаи, которые были экспериментально обнаружены в [4]:

1) $\pi_1(x) = x$, $\pi_2(x) = x^{13}$,

2) $\pi_1(x) = x^2$, $\pi_2(x) = x^{14}$,

3) $\pi_1(x) = x^4$, $\pi_2(x) = x^7$,

4) $\pi_1(x) = x^8$, $\pi_2(x) = x^{11}$.

Случаи 2 и 4 являются обратными соответственно случаям 1 и 3. Для указанных случаев при правильном выборе $\widehat{\pi}_i$ в [4] были построены подстановки со следующими криптографическими характеристиками:

– нелинейность — 108,

– показатель дифференциальной равномерности — 6,

– алгебраическая степень нелинейности — 7.

3.3. Обобщенная конструкция

Опишем семейство подстановок, которые обобщают подстановки типов «А» и «Б» при фиксации мономиальных параметров подстановок, рассмотренных в разделах 3.1, 3.2. Рассмотрим семейство подстановок, параметрами которого являются четверка степеней $(\alpha, \beta, \gamma, \delta)$ и подстановки $\widehat{\pi}_i$, $i \in \{1, 2\}$:

$$\begin{aligned} G_1(x_1, x_2) = y_1 &= \begin{cases} x_1^{\alpha} \cdot x_2^{\beta}, & x_2 \neq \theta, \\ \widehat{\pi}_1(x_1), & x_2 = \theta, \end{cases} \\ G_2(x_1, x_2) = y_2 &= \begin{cases} x_1^{\gamma} \cdot x_2^{\delta}, & x_1 \neq \theta, \\ \widehat{\pi}_2(x_2), & x_1 = \theta. \end{cases} \end{aligned} \tag{15}$$

Для того чтобы уравнение (15) задавало биективное преобразование, достаточно, чтобы система уравнений

$$\begin{cases} G_1(x_1, x_2) = a_1, \\ G_2(x_1, x_2) = a_2, \end{cases}$$

имела решение для произвольных $a_1, a_2 \in V_m$.

Рассмотрим случай $m = 4$. По малой теореме Ферма всего имеется 8 различных мономиальных подстановок поля $\mathbb{F}_{2^4}$. Воспользовавшись

леммой, можно ограничить значения параметров $(\alpha, \beta, \gamma, \delta)$ в уравнении (15) с использованием ЭВМ, аналогично работе [4]. Как и в [4], при правильном выборе параметров $\widehat{\pi}_i$, $i \in \{1, 2\}$, получаются подстановки, обладающие следующими криптографическими характеристиками:

– нелинейность — 108,

– показатель дифференциальной равномерности — 6,

– алгебраическая степень нелинейности — 7.

Экспериментально проверено, что указанные значения криптографических характеристик достигаются, например, в случае, когда $\widehat{\pi}_i(x) = x^d$, $d \in \{7, 11, 13, 14\}$.

Заметим, что если четверка $\alpha, \beta, \gamma, \delta$ при правильном выборе $\widehat{\pi}_i$, $i \in \{1, 2\}$, задает подстановку с «хорошими» криптографическими свойствами, то

– если x^d задает линейную подстановку, то набор $\alpha \cdot d \pmod{2^m - 1}$, $\beta \cdot d \pmod{2^m - 1}, \gamma \cdot d \pmod{2^m - 1}, \delta \cdot d \pmod{2^m - 1}$ задает подстановку с такими же свойствами,

– $\beta, \alpha, \delta, \gamma$ и $\delta, \gamma, \beta, \alpha$ задают подстановку с такими же свойствами.

Таким образом, на множестве наборов можно задать отношение эквивалентности, и в случае $m = 4$ каждый класс состоит из 16 элементов, всего имеется $768/16 = 48$ классов. Следующая таблица содержит по одному представителю каждого класса.

α	β	γ	δ	α	β	γ	δ	α	β	γ	δ	α	β	γ	δ
1	1	7	11	1	4	7	11	1	11	7	13	1	14	7	7
1	1	7	14	1	4	7	14	1	11	11	14	1	14	11	11
1	1	11	13	1	4	11	7	1	11	13	7	1	14	13	13
1	1	13	14	1	4	13	11	1	11	14	11	1	14	14	14
1	2	7	7	1	7	7	2	1	13	7	8	7	7	7	11
1	2	7	13	1	7	7	11	1	13	7	14	7	7	7	14
1	2	11	11	1	7	11	1	1	13	11	4	7	7	11	13
1	2	11	14	1	7	11	13	1	13	11	7	7	7	13	14
1	2	13	7	1	7	13	8	1	13	13	2	7	11	7	13
1	2	13	13	1	7	13	14	1	13	13	11	7	11	11	14
1	2	14	11	1	7	14	4	1	13	14	1	7	11	13	7
1	2	14	14	1	7	14	7	1	13	14	13	7	11	14	11

Заключение

В работе дано теоретическое обоснование результатов, приведенных в [4]. Доказан ряд утверждений, позволяющий оптимизировать алгоритм 1 для поиска подстановок с высокой алгебраической степенью и низким показателем дифференциальной равномерности.

Список литературы

[1] Biryukov A., Perrin L., Udovenko A., "Reverse-engineering the S-box of Streebog, Kuznyechik and Stribobr1", EUROCRYPT 2016, Lect. Notes Comput. Sci., **9665**, 2016, 372–402.

[2] Perrin L., *Cryptanalysis, Reverse-Engineering and Design of Symmetric Cryptographic Algorithms*, Univ. Luxembourg, 2017, 368 pp.

[3] Perrin L., Udovenko A., Biryukov A., "Cryptanalysis of a theorem: Decomposing the only known solution to the big APN problem", CRYPTO 2016, Lect. Notes Comput. Sci., **9815**, 2016, 93–122.

[4] Fomin D. B., "New classes of 8-bit permutations based on a butterfly structure", *Математические вопросы криптографии*, **10**:2 (2019), 169–180.

[5] Фомин Д. Б., Трифонов Д. И., "Об аппаратной реализации одного класса байтовых подстановок", *Прикладная дискретная математика. Приложение*, **12** (2019), 134–137.

[6] Фомин Д. Б., "О способе построения подстановок пространства V_{2m} с использованием $(2m, m)$-функций", *Математические вопросы криптографии*, **11**:3 (2020), 121–138.

[7] Carlet C., Crama Y., Hammer P. L., "Vectorial Boolean Functions for Cryptography", *Boolean Models and Methods*, Cambridge Univ. Press, 2010, 398–470.