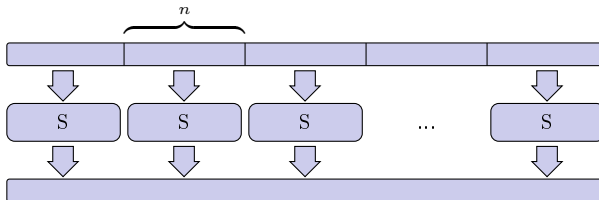


О БУМЕРАНГОВОЙ РАВНОМЕРНОСТИ
КУСОЧНО-МОНОМИАЛЬНЫХ ПОДСТАНОВОК
ПОЛЯ $\mathbb{F}_{2^n}$

Калинин Юрий Сергеевич,
Куценко Александр Владимирович,
Менячихин Андрей Валерьевич

Принципы Шеннона¹

- 1 наложение ключа,
- 2 нелинейное перемешивающее отображение,
- 3 рассеивающее преобразование.



Замечание

По ряду причин, связанных с особенностями реализации шифрсистем на различных программно-аппаратных платформах, значение n , как правило, выбирается четным (чаще $n = 2^k$, $k \in \mathbb{N}$).

Среди множества криптографических параметров s-боксов в настоящей работе особое внимание будет уделено бумеранговой характеристике.

¹ Шеннон К. Работы по теории информации и кибернетике.— М.:ИЛ, 1963.— 829с.

Замечание

Метод бумеранга¹ был предложен Д. Вагнером в 1999 году и неоднократно применялся для анализа различных шифрсистем, включая AES², ГОСТ Р 34.12-2015³ и ГОСТ 28147-89^{4,5}.

Один из подходов к повышению стойкости шифрсистем относительно метода бумеранга связан с выбором подстановок с минимально возможным значением Λ .

Подстановки поля $\mathbb{F}_{2^n}$, бумеранговая характеристика которых не превосходит величины Λ , называют *бумерангово Λ -равномерными*.

Замечание

Известно⁶, что подстановка $g \in S(\mathbb{F}_{2^n})$ является бумерангово 2-равномерной тогда и только тогда, когда g – APN-подстановка (существование APN-подстановок $\mathbb{F}_{2^n}$ при четных значениях $n > 6$ является известной открытой проблемой⁷). Бумерангово 4-равномерные подстановки существуют для нечётного n и $n \equiv 2 \pmod{4}$, для $n = 4$ их не существует. В ряде работ ставится вопрос о существовании бумерангово 4-равномерных подстановок для $n = 8$.

¹ Wagner D. The boomerang attack. FSE-1999, LNCS, 1636 (1999), P. 156-170.

² Biryukov A. The Boomerang Attack on 5 and 6-Round Reduced AES. In: Dobbertin H., Rijmen V., Sowa A. (eds) Advanced Encryption Standard – AES. LNCS, 3373 (2004), P. 11-15.

³ Кирюхин В.А. Атака методом бумеранга на связанных ключах на 5 раундов шифра Кузнечик. Обзорные прикладной и промышленной математики, 26:3 (2019), С. 268-270.

⁴ Rudskoy V. On zero practical significance of "Key recovery attack on full GOST block cipher with zero time and memory". <http://eprint.iacr.org/2010>.

⁵ Пудовкина М. А., Хоруженко Г. И. Атака на шифрсистему ГОСТ 28147-89 с 12 связанными ключами. Матем. вopr. криптогр., 4:2 (2013), С. 127-152.

⁶ Bours C., Canteaut A. On the boomerang uniformity of cryptographic S-boxes. IACR Trans. Symmetric Cryptology, 3 (2018), P. 290-310.

⁷ Carlet C. Open questions on nonlinearity and on APN functions, Proceedings of Arithmetic of Finite Fields 5th International Workshop. WAIFI 2014, LNCS, 9061 (2015), P. 83-107.

Основные определения

Пусть $H < \mathbb{F}_{2^n}^\times$ – подгруппа порядка l мультипликативной группы поля $\mathbb{F}_{2^n}^\times$, $0 < l < 2^n - 1$, $2^n - 1 = l \cdot r$, где $r \in \mathbb{N}$, ζ – примитивный элемент поля $\mathbb{F}_{2^n}$, $H = \langle \zeta^r \rangle$. Группа $\mathbb{F}_{2^n}^\times$ раскладывается в объединение смежных классов по подгруппе H :

$$\mathbb{F}_{2^n}^\times = \bigcup_{i=0}^{r-1} H_i, H_i = \zeta^i H, i = 0, \dots, r-1.$$

Определение 1

*Кусочно-мономиальным*¹⁻⁶ называется отображение $g: \mathbb{F}_{2^n} \rightarrow \mathbb{F}_{2^n}$ вида

$$g(x) = \begin{cases} 0, & \text{если } x = 0, \\ \zeta^{a_i} x^\gamma, & \text{если } x \in H_i, \end{cases}$$

где $a_i \in \{0, \dots, 2^n - 2\}$, $i = 0, \dots, r-1$, $\gamma \in \{0, \dots, l-1\}$.

Известно (см., например⁵), что преобразование g – биективно тогда и только тогда, когда $\text{НОД}(\gamma, l) = 1$ и биективно преобразование $\pi: \mathbb{Z}_r \rightarrow \mathbb{Z}_r$,

$$\pi(i) = (a_i + \gamma i) \bmod r, i = 0, \dots, r-1.$$

Множество всех кусочно-мономиальных подстановок, удовлетворяющих условиям определения, будем обозначать $M_{r,\gamma}(\mathbb{F}_{2^n})$.

¹ Wells C. Groups of permutation polynomials. Monatsh. Math., 71 (1967), pp. 248-262.

² Evans A. Orthomorphisms graphs and groups. Springer-Verlag, Berlin, 1992, 114 p.

³ Тришин А.Е. О показателе нелинейности кусочно-линейных подстановок аддитивной группы поля $\mathbb{F}_{2^n}$. Прикладная дискретная математика, 4:30 (2015), С. 32-42.

⁴ Бугров А.Д. Кусочно-аффинные подстановки конечных полей. Прикладная дискретная математика, 4:30 (2015), С. 5-23.

⁵ Burov D., Kostarev S., Menyachikhin A. Class of piecewise-monomial mappings: differentially 4-uniform permutations of $\mathbb{F}_{2^8}$ with graph algebraic immunity 3 exist. In: Pre-proceedings of CTRCrypT'23-Volgograd, Russia, (2023), P. 219-235.

⁶ Погорелов Б.А., Пудовкина М.А. Классы кусочно-квазиаффинных преобразований на обобщенной 2-группе кватернионов. Дискретная математика, 34:1 (2022), С. 103-125.

Обозначим через $g_M: M \rightarrow \mathbb{F}_{2^n}$ – *ограничение* преобразования $g: \mathbb{F}_{2^n} \rightarrow \mathbb{F}_{2^n}$ на множество $M \subseteq \mathbb{F}_{2^n}$.

Определение 2

Бумеранговой характеристикой^{1,2} b_{g_M} отображения g_M назовем величину

$$b_{g_M} = \max_{\alpha, \beta \in \mathbb{F}_{2^n}^\times} b_{\alpha, \beta}^{g_M},$$

где

$$b_{\alpha, \beta}^{g_M} = \left| \left\{ x \in M \left| \begin{array}{l} x + \alpha \in M, g^{-1}(g(x) + \beta) \in M, g^{-1}(g(x + \alpha) + \beta) \in M, \\ g^{-1}(g(x) + \beta) + g^{-1}(g(x + \alpha) + \beta) = \alpha \end{array} \right. \right\} \right|.$$

В случае, когда M – собственное подмножество множества $\mathbb{F}_{2^n}$, величину b_{g_M} будем также называть *частичной бумеранговой характеристикой* преобразования g на множестве M .

Один из подходов к повышению стойкости шифрсистем относительно методов криптографического анализа типа «бумеранг» связан с минимизацией значения b_g преобразования $g \in S(\mathbb{F}_{2^n})$. Известно, что

$$2 \leq b_g \leq 2^n.$$

¹ Калинин Ю.С. Исследование бумеранговой равномерности квадратичных взаимно однозначных векторных булевых функций. Прикладная дискретная математика. Приложение., 17 (2024), С. 28-34.

² Погорелов В.А., Пудовкина М.А. Общие свойства бумеранг-матриц над абелевыми группами. Математические вопросы криптографии, 16:4 (2025), С. 87-119.

Замечания

- ① Множество $M \subset \mathbb{F}_{2^n}$ может быть не замкнуто относительно операции $+$ в поле $\mathbb{F}_{2^n}$.
- ② Введенное определение бумеранговой характеристики совпадает с общепринятым в случае, когда множество $M = \mathbb{F}_{2^n}$.
- ③ Для цепочки подмножеств $M_0 \subseteq M_1 \subseteq \dots \subseteq M_{s-1} \subseteq \mathbb{F}_{2^n}$ справедлива цепочка неравенств

$$b_{g_{M_0}} \leq b_{g_{M_1}} \leq \dots \leq b_{g_{M_{s-1}}} \leq b_g.$$

Матрица B_{g_M} размеров $(2^n - 1) \times (2^n - 1)$, составленная из элементов $b_{\alpha, \beta}^{g_M}$ называется *бумеранг-матрицей* отображения g_M .

Пример

APN-подстановка $g \in M_{7,1}(\mathbb{F}_{2^3})$	Тожд. подстановка $g \in M_{1,1}(\mathbb{F}_{2^3})$
0 2 0 2 2 2 0	8 8 8 8 8 8 8
0 0 2 0 2 2 2	8 8 8 8 8 8 8
2 2 2 0 0 2 0	8 8 8 8 8 8 8
0 2 2 2 0 0 2	8 8 8 8 8 8 8
2 2 0 0 2 0 2	8 8 8 8 8 8 8
2 0 0 2 0 2 2	8 8 8 8 8 8 8
2 0 2 2 2 0 0	8 8 8 8 8 8 8

О бумеранговом спектре кусочно-линейных подстановок

Для отображения g_M и каждого числа $i = 0, 1, \dots, |M|$ определим множество

$$B_{g_M, i} = \left\{ (\alpha, \beta) \in \mathbb{F}_{2^n}^\times \times \mathbb{F}_{2^n}^\times \mid b_{\alpha, \beta}^{g_M} = i \right\}.$$

Определение 3

Бумеранговым спектром отображения g_M называется упорядоченный набор

$$\vec{B}_{g_M} = (|B_{g_M, 0}|, |B_{g_M, 1}|, |B_{g_M, 2}|, \dots, |B_{g_M, |M|}|).$$

При детальном рассмотрении бумерангового спектра каждой из подстановок $g \in M_{r, \gamma}(\mathbb{F}_{2^n})$ нетрудно видеть, что каждое из значений указанного спектра кратно $l = |H|$, $l \cdot r = 2^n - 1$. Указанное наблюдение является простым следствием следующего утверждения.

Утверждение 1

Пусть $g \in M_{r, \gamma}(\mathbb{F}_{2^n})$, ζ - примитивный элемент поля $\mathbb{F}_{2^n}$. Тогда $x_0 \in \mathbb{F}_{2^n}$ является решением уравнения $g^{-1}(g(x) + \beta_0) + g^{-1}(g(x + \alpha_0) + \beta_0) = \alpha_0$, $\alpha_0, \beta_0 \in \mathbb{F}_{2^n}$, в том и только том случае, когда $x_j = x_0 \zeta^{rj}$ является решением уравнения $g^{-1}(g(x) + \beta_j) + g^{-1}(g(x + \alpha_j) + \beta_j) = \alpha_j$, $\alpha_j = \alpha_0 \zeta^{rj}$, $\beta_j = \beta_0 \zeta^{r\gamma j}$, $j = 1, 2, \dots, l - 1$.

Следствие

Для любого преобразования $g \in M_{r, \gamma}(\mathbb{F}_{2^n})$ и любого числа $c = 0, 1, \dots, 2^n$ справедливо $|B_{g, c}| \equiv 0 \pmod{l}$.

Эффективное вычисление бумеранговой характеристики и бумерангового спектра кусочно-линейных подстановок

Определим отображение $\psi: \mathbb{F}_{2^n}^\times \rightarrow \{1, \zeta, \zeta^2, \dots, \zeta^{r-1}\}$ равенством $\psi(x) = \zeta^i$, если $x \in H_i$, $i \in \{0, \dots, r-1\}$, и для элементов $x \in \mathbb{F}_{2^n}^\times$ и $\gamma \in \mathbb{F}_{2^n}$ подстановку $\sigma_{x,\gamma} \in S(\mathbb{F}_n)$ – равенством $\sigma_{x,\gamma}(y) = y(x^{-1}\psi(x))^\gamma$.

В бумеранг-матрице B_g подстановки $g \in M_{r,\gamma}(\mathbb{F}_{2^n})$ утверждение 1 позволяет каждой строке с номером α вида

$$(b_{\alpha,0}^g, b_{\alpha,1}^g, b_{\alpha,\zeta}^g, \dots, b_{\alpha,\zeta^{2^n-2}}^g)$$

поставить в соответствие строку с номером $\psi(\alpha)$ вида

$$\begin{aligned} & (b_{\psi(\alpha),0}^g, b_{\psi(\alpha),1}^g, b_{\psi(\alpha),\zeta}^g, \dots, b_{\psi(\alpha),\zeta^{2^n-2}}^g) = \\ & = (b_{\alpha,\sigma_{\alpha,\gamma}(0)}^g, b_{\alpha,\sigma_{\alpha,\gamma}(1)}^g, b_{\alpha,\sigma_{\alpha,\gamma}(\zeta)}^g, \dots, b_{\alpha,\sigma_{\alpha,\gamma}(\zeta^{2^n-2})}^g), \end{aligned}$$

представляющую собой перестановку $\sigma_{\alpha,\gamma}$ элементов исходной строки. Следовательно, в бумеранг-матрице B_g подстановки $g \in M_{r,\gamma}(\mathbb{F}_{2^n})$ уникальными (требуемыми вычисления) являются не более r строк (например строки с номерами $1, \zeta, \zeta^2, \dots, \zeta^{r-1}$). Каждая из оставшихся строк с номером $\alpha \notin \{1, \zeta, \zeta^2, \dots, \zeta^{r-1}\}$ получена из уникальной строки с номером $\psi(\alpha)$ перестановкой $\sigma_{\alpha,\gamma}^{-1}$ ее элементов.

Таким образом, для вычисления бумеранговой характеристики b_g и бумерангового спектра $\vec{B}_g$ подстановки $g \in M_{r,\gamma}(\mathbb{F}_{2^n})$ достаточно вычисления элементов подматрицы $B_g \begin{pmatrix} 1, \zeta, \zeta^2, \dots, \zeta^{r-1} \\ 1, \zeta, \zeta^2, \dots, \zeta^{2^n-2} \end{pmatrix}$ бумеранг-матрицы B_g подстановки $g \in M_{r,\gamma}(\mathbb{F}_{2^n})$.

Эффективное вычисление бумеранговой характеристики и бумерангового спектра кусочно-линейных подстановок

Пример

Пусть $H < \mathbb{F}_{2^4}^\times$, $\mathbb{F}_{2^4} = \mathbb{F}_2[x]/x^4 + x + 1$, $|H| = 5$, $\zeta = 2$. Группа $\mathbb{F}_{2^4}^\times$ раскладывается в объединение смежных классов по подгруппе H :

$$\mathbb{F}_{2^4}^\times = \underbrace{\{8, c, a, f, 1\}}_{H_0} \cup \underbrace{\{3, b, 7, d, 2\}}_{H_1} \cup \underbrace{\{6, 5, e, 9, 4\}}_{H_2}.$$

Нижняя строка подстановки $g \in M_{3,7}(\mathbb{F}_{2^4})$															
0	2	a	1	9	e	6	f	b	5	3	c	d	8	4	7
Матрица $B_g = \left(b_{\alpha,\beta}^g\right)_{15 \times 15}$ подстановки g															
$\alpha \backslash \beta$	1	2	4	8	3	6	c	b	5	a	7	e	f	d	9
1	0	2	0	0	2	0	0	2	2	0	2	2	2	0	2
2	10	0	0	6	2	0	0	0	0	2	0	4	4	0	4
4	0	4	4	0	2	4	2	0	0	2	2	0	2	2	2
8	0	2	2	2	0	2	0	2	0	0	2	0	0	2	2
3	2	0	4	4	0	4	10	0	0	6	2	0	0	0	0
6	0	2	2	0	2	2	0	0	4	4	0	2	4	2	0
c	0	2	0	0	2	2	0	2	2	2	0	2	0	2	0
b	6	2	0	0	0	0	2	0	4	4	0	4	10	0	0
5	4	0	2	4	2	0	0	2	2	0	0	2	0	0	4
a	2	0	2	0	2	0	0	2	0	0	2	2	0	2	2
7	4	0	4	10	0	0	6	2	0	0	0	0	2	0	4
e	0	2	2	0	0	4	4	0	2	4	2	0	0	2	2
f	0	2	2	0	2	2	2	0	2	0	2	0	0	2	0
d	0	0	0	2	0	4	4	0	4	10	0	0	6	2	0
9	4	2	0	0	2	2	0	2	2	0	0	4	4	0	2

Эффективное вычисление бумеранговой характеристики и бумерангового спектра кусочно-линейных подстановок

Обозначим через $H_{(i_0, \dots, i_{s-1})} = \bigcup_{j=0}^{s-1} H_{i_j} \cup \{0\}$, где $s \in \{1, \dots, r\}$, и рассмотрим отображение $g_{H_{(i_0, \dots, i_{s-1})}} : H_{(i_0, \dots, i_{s-1})} \rightarrow \mathbb{F}_{2^n}$, представляющее собой ограничение подстановки $g \in M_{r, \gamma}(\mathbb{F}_{2^n})$ на множество $H_{(i_0, \dots, i_{s-1})}$. Утверждение 1 позволяет сформулировать следующий алгоритм вычисления бумерангового спектра отображения $g_{H_{(i_0, \dots, i_{s-1})}} : H_{(i_0, \dots, i_{s-1})} \rightarrow \mathbb{F}_{2^n}$ (см. рис. 1).

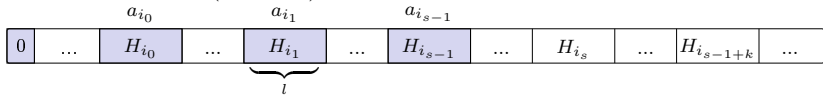


Рис. 1. Идея алгоритма 1

Утверждение 2

Бумеранговый спектр $\vec{B}_{g_{H_{(i_0, \dots, i_{s-1})}}}$ отображения $g_{H_{(i_0, \dots, i_{s-1})}} : H_{(i_0, \dots, i_{s-1})} \rightarrow \mathbb{F}_{2^n}$, $s \in \{1, \dots, r\}$, может быть вычислен с помощью алгоритма 1 с трудоемкостью t ,

$$t \leq cl^2s^3, c = \text{const.}$$

Замечание

При $s = r$ трудоемкость вычисления бумеранговой характеристики p_g подстановки $g \in M_{r, \gamma}(\mathbb{F}_{2^n})$ с помощью алгоритма 1 в l раз ниже трудоемкости классического подхода.

Эффективное вычисление бумеранговой характеристики и бумерангового спектра кусочно-линейных подстановок

Алгоритм 1 может быть легко модифицирован для случая, когда по известным отображению $g_H(i_0, \dots, i_{s-1})$, бумеранг-матрице $B_{g_H(i_0, \dots, i_{s-1})}$ и бумеранговому спектру $\vec{D}_{g_H(i_0, \dots, i_{s-1})}$ требуется вычислить бумеранговый спектр $\vec{D}_{g_H(i_0, \dots, i_{s-1+k})}$ отображения $g_H(i_0, \dots, i_{s-1+k})$ (см. рис. 2).

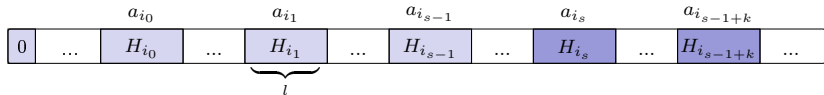


Рис. 2. Идея алгоритма 2

Утверждение 3

Бумеранговый спектр $\vec{B}_{g_H(i_0, \dots, i_{s-1+k})}$ отображения $g_H(i_0, \dots, i_{s-1+k}) : H(i_0, \dots, i_{s-1+k}) \rightarrow \mathbb{F}_2^n$, $s \in \{1, \dots, r-1\}$, может быть вычислен из бумерангового спектра $\vec{B}_{g_H(i_0, \dots, i_{s-1})}$ и подматрицы $B_{g_H(i_0, \dots, i_{s-1})} \begin{pmatrix} 1, \zeta, \zeta^2, \dots, \zeta^{r-1} \\ 1, \zeta, \zeta^2, \dots, \zeta^{2^n-2} \end{pmatrix}$ бумеранг-матрицы $B_{g_H(i_0, \dots, i_{s-1})}$ отображения $g_H(i_0, \dots, i_{s-1}) : H(i_0, \dots, i_{s-1}) \rightarrow \mathbb{F}_2^n$ с помощью алгоритма 2 с трудоемкостью t ,

$$t \leq cl^2s^2, c = \text{const.}$$

Применение адаптированного спектрального метода для построения кус.-мон. подстановок с низким значением бумеранговой равномерности

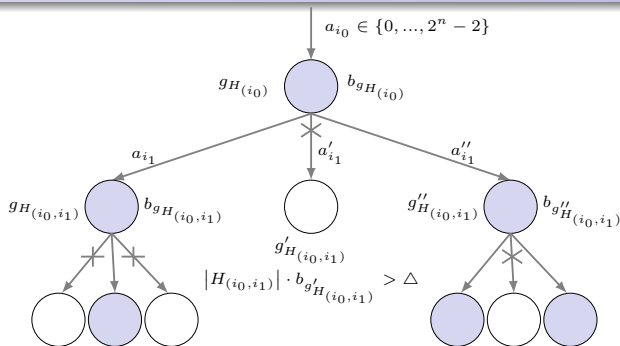


Рис. 3. Основная идея алгоритма 3, реализующего адаптированный спектральный метод¹

Утверждение 4

При $n, r, w \in \mathbb{N}$, $r \mid 2^n - 1$, справедлива следующая оценка трудоемкости t алгоритма 3:

$$t \leq cw2^n (r - 1) (2^{2n-1} + 2^{n-2} (r - 1) + n + \log w), \text{ где } c = \text{const.}$$

¹ Менячихин А.В. Адаптированный спектрально-разностный метод построения дифференциально 4-равномерных кусочно-линейных подстановок, ортоморфизмов, инволюций поля $\mathbb{F}_{2^n}$. Дискретная математика, 35:2 (2023), С. 42-77.

Оценки бумеранговой характеристики кусочно-линейных подстановок поля $\mathbb{F}_{2^n}$

Известно, что для любых $\alpha, \beta \in \mathbb{F}_{2^n}$ элементы бумеранг-матрицы и разностной матрицы преобразования $g: \mathbb{F}_{2^n} \rightarrow \mathbb{F}_{2^n}$ удовлетворяют неравенству

$$p_{\alpha, \beta}^g \leq b_{\alpha, \beta}^g.$$

Приведенные ниже оценки бумеранговой характеристики кусочно-линейных подстановок являются простым следствием полученных А.В. Менячихиным^{1,2} оценок разностной характеристики подстановок этого класса.

Теорема

Пусть $n, r, l \in \mathbb{N}$, $2^n - 1 = rl$, ζ - примитивный элемент поля $\mathbb{F}_{2^n}$, $H = \langle \zeta^r \rangle$ - подгруппа группы $\mathbb{F}_{2^n}^\times$ порядка l , $g \in M_{r,1}(\mathbb{F}_{2^n})$, заданная упорядоченным набором чисел $(a_0, a_1, \dots, a_{r-1})$. Тогда выполнено неравенство

$$b_g \geq \max \left\{ \sum_{s=1}^t (-1)^{s+1} \sum_{n_1 \leq \dots \leq n_s} 2^{\text{НОД}(n_1, n_2, \dots, n_s)}, 2 \left\lfloor \frac{l+1}{2r} \right\rfloor \right\},$$

где $2^{n_1} - 1 < \dots < 2^{n_s} - 1$ - делители числа l .

¹ Менячихин А.В. О разностной характеристике кусочно-линейных подстановок поля $\mathbb{F}_{2^n}$. Дискретная математика, 35:4 (2023), С. 58-68.

² Менячихин А.В., Спиридонов С.В. Оценки разностной характеристики кусочно-аффинных подстановок поля $\mathbb{F}_q$. Дискретная математика, 37:2 (2025), С. 51-65.

Достижимость нижних оценок бумеранговой характеристики кусочно-линейных подстановок

Пусть $n = 6$, $2^6 - 1 = rl$, $r, l \in \mathbb{N}$, ζ - примитивный элемент поля $\mathbb{F}_{2^6}$, $H = \langle \zeta^r \rangle$ подгруппа группы $\mathbb{F}_{2^6}^\times$ порядка l . Следующая таблица для различных значений $l \in \{1, 3, 7, 9, 21, 63\}$ содержит минимальные значения величины b_g среди всех подстановок $g \in M_{r,1}(\mathbb{F}_{2^6})$. Таблица также содержит полученные в теореме нижние оценки значений b_g .

$ H $	Нижняя оценка величины b_g	$\min_{g \in M_{r,1}(\mathbb{F}_{2^6})} b_g$
1	2	2
3	4	4
7	8	10
9	4	4
21	10	10
63	64	64

Достижимость нижних оценок бумеранговой характеристики кусочно-линейных подстановок

Пусть $n = 8$, $2^8 - 1 = rl$, $r, l \in \mathbb{N}$, ζ - примитивный элемент поля $\mathbb{F}_{2^8}$, $H = \langle \zeta^r \rangle$ подгруппа группы $\mathbb{F}_{2^8}^\times$ порядка l . Следующая таблица для различных значений $l \in \{1, 3, 5, 15, 17, 51, 85, 255\}$ содержит лучшие известные значения величины b_g для подстановок $g \in M_{r,1}(\mathbb{F}_{2^8})$. Таблица также содержит полученные в теореме нижние оценки значений b_g .

$ H $	Нижняя оценка величины b_g	Лучший известный пример
1	2	6
3	4	6
5	2	6
15	16	18
17	$2(4^1)$	6
51	12	14
85	30	34
255	256	256

¹ Оценка $b_g \geq 4$ при $|H| = 17$ непосредственно следует из результатов работы:

Beierle C., Brinkmann M., Leander G. Linearly self-equivalent APN permutations in small dimension. IEEE Trans. Inf. Theory, 67:7 (2020), pp. 4863-4875.

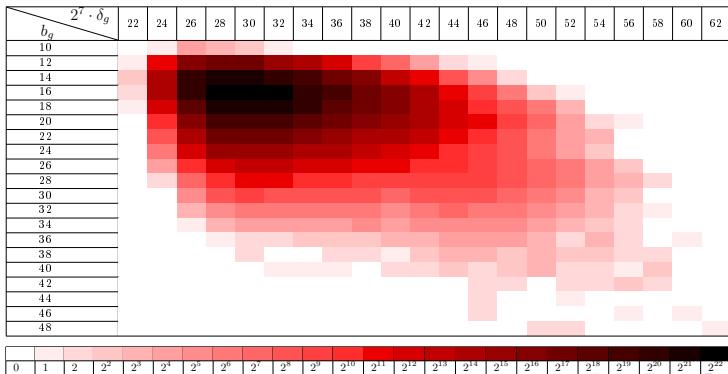
Результаты применения адаптированного спектрального метода и псевдослучайного поиска на основе выборки объема $5 \cdot 10^7$

Таблица 1.

Подстановки $g \in M_{15,1}(\mathbb{F}_{2^8})$,

$\mathbb{F}_{2^8} = \mathbb{F}_2[x]/x^8 + x^4 + x^3 + x + 1$, определяемые при $\zeta = 3$ векторами $\vec{a}_g \in \{0, \dots, 2^8 - 2\}^{15}$ в шестнадцатеричной записи

$\vec{a}_g = (a_0, a_1, \dots, a_{14})$															$2^8 p_g$	$ D_{g,p_g} $	b_g	$ B_{g,b_g} $	$2^7 \delta_g$	$ L_{g,\delta_g} $	$\bar{\lambda}_g$
bb	9b	5c	43	7d	2b	dd	ad	8a	4	8d	5b	6b	34	72	6	221	8	986	24	51	7
54	49	21	c1	4f	f7	27	be	e4	9f	c3	46	3d	7e	cb	6	306	8	1190	24	68	7



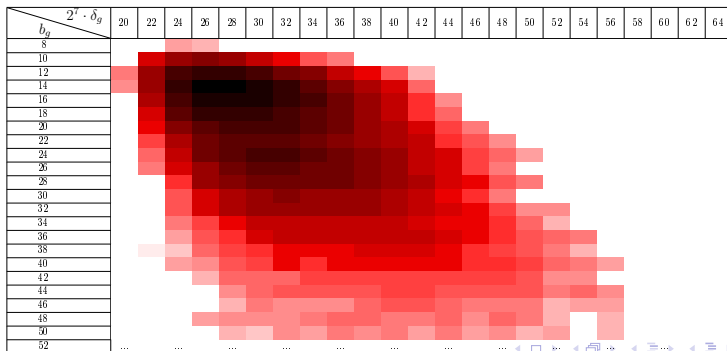
Результаты применения адаптированного спектрального метода и псевдослучайного поиска на основе выборки объема $5 \cdot 10^7$

Таблица 2.

Подстановки $g \in M_{5,19}(\mathbb{F}_{2^8})$,

$\mathbb{F}_{2^8} = \mathbb{F}_2[x]/x^8 + x^4 + x^3 + x + 1$, определяемые при $\zeta = 3$ векторами $\vec{a}_g \in \{0, \dots, 2^8 - 2\}^5$ в шестнадцатеричной записи

$\vec{a}_g = (a_0, a_1, \dots, a_4)$	$2^8 p_g$	$ D_{g,p_g} $	b_g	$ B_{g,b_g} $	$2^7 \delta_g$	$ L_{g,\delta_g} $	$\overline{\lambda}_g$
8 d4 a1 6e 3b	4	255	6	510	16	1275	7
8 cf fb f0 2c	8	51	8	1071	26	51	7
8 4d 38 37 e0	6	357	8	1479	24	51	7



Результаты применения адаптированного спектрального метода и псевдослучайного поиска на основе выборки объема 10^8

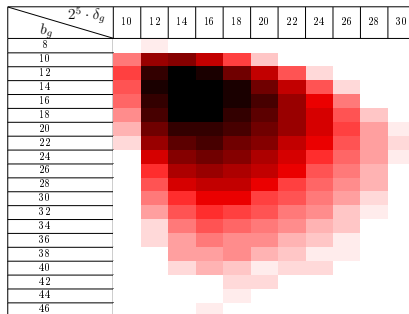
Таблица 3.

Подстановки $g \in M_{21,1}(\mathbb{F}_{2^6})$,

$\mathbb{F}_{2^6} = \mathbb{F}_2[x]/x^6 + x + 1$, определяемые при $\zeta = 2$ векторами

$\vec{a}_g \in \{0, \dots, 2^6 - 2\}^{21}$ в шестнадцатеричной записи

$\vec{a}_g = (a_0, a_1, ..., a_{20})$																				$2^6 p_g$	$ D_{g,p_g} $	b_g	$ B_{g,b_g} $	$2^5 \delta_g$	$ L_{g,\delta_g} $	$\overline{\lambda}_g$	
25	18	20	3d	19	38	b	38	27	18	32	1e	12	17	0	25	1c	31	38	32	1d	4	63	4	189	8	189	5
25	3b	2c	3e	2f	13	20	4	13	4	13	14	10	30	2b	29	1a	3	1d	18	37	4	117	4	351	8	279	5
25	2	7	26	b	27	24	39	29	16	3b	f	22	2f	29	27	16	39	2b	25	1e	4	171	6	72	10	18	5
25	d	1a	15	19	1f	2e	12	33	21	37	32	39	1c	19	39	3c	9	24	2d	36	4	180	6	126	12	9	5
25	29	2c	e	2c	34	d	31	2d	3d	34	21	30	12	10	23	11	1c	32	18	23	4	225	6	135	10	18	4
25	29	2c	e	2c	34	d	31	2d	3d	34	21	30	12	10	23	26	1c	32	18	23	4	252	6	171	10	18	4
25	35	1a	18	0	6	25	3b	0	2e	34	f	3	11	1c	3a	16	3c	1a	0	28	6	21	6	222	12	6	5



Спасибо за внимание