А. В. Саранцев, Свойства подстановок, порождаемых одним классом фильтрующих генераторов, *Матем. вопр. криптогр.*, 2023, том 14, выпуск 1, 99–114

DOI: 10.4213/mvk433

МАТЕМАТИЧЕСКИЕ ВОПРОСЫ КРИПТОГРАФИИ
2023 Т. 14 № 1 С. 99–114

УДК 519.719.2 DOI https://doi.org/10.4213/mvk433

Свойства подстановок, порождаемых одним классом фильтрующих генераторов

А. В. Саранцев

ООО «Центр сертификационных исследований», Москва

Получено 12.V.2022

Аннотация. Рассматривается класс подстановок на множестве двоичных строк длины n, координатные функции которых эквивалентны относительно преобразования, реализуемого аффинным регистром сдвига. Описаны нелинейные двоичные функции f, существенно зависящие только от первых трех переменных, и аффинные функции l обратной связи регистра сдвига, для которых фильтрующий генератор с этим регистром сдвига и функцией усложнения f порождает совокупность координатных функций подстановки. Вычислены степень нелинейности и разностная характеристика этого класса подстановок. С помощью этих подстановок построен класс нелинейных регистров сдвига с периодом $2^n - 1$.

Ключевые слова: сбалансированное отображение, подстановка, эквивалентные функции, координатные функции, характеристики нелинейности, нелинейные регистры сдвига

Properties of substitutions generated by a class of filtering generators

A. V. Sarantsev

LLC «Sertification Research Center», Moscow

Abstract. We consider a class of substitutions on a set of binary strings of length n whose coordinate functions are equivalent with respect to the transformation implemented by the affine shift register. We describe nonlinear Boolean functions f depending significantly only on the first three variables and affine feedback functions l of the shift register such that this shift register along with the filter function f generates a system of coordinate functions of substitution. The degree of nonlinearity and the difference characteristic for substitutions from this class are calculated. By means of these substitutions a class of nonlinear shift registers of period $2^n - 1$ is constructed.

Citation: Matematicheskie Voprosy Kriptografii, 2023, v. 14, № 1, pp. 99–114 (Russian)

Keywords: balanced mapping, substitution, equivalent functions, coordinate functions, characteristics of nonlinearity, nonlinear shift register

1. Подстановки, координатные функции которых эквивалентны

Пусть $\mathbb{F}_2^n$ — векторное пространство размерности n над полем $\mathbb{F}_2$, $G < S(\mathbb{F}_2^n)$ — некоторая группа подстановок на $\mathbb{F}_2^n$, $F_2(n)$ — множество двоичных функций от n переменных. Для подстановки $\alpha \in G$ и функции $f \in F_2(n)$ определим функцию f^α следующим образом:

$$f^\alpha(x) \stackrel{\text{def}}{=} f\left(x^{\alpha^{-1}}\right), \quad \forall x \in \mathbb{F}_2^n, \tag{1}$$

где $x^{\alpha^{-1}}$ обозначает результат применения подстановки α^{-1} к строке x. Напомним, что функции $f, g \in F_2(n)$ называются *эквивалентными* [8] относительно группы G, если для некоторого $\alpha \in G$ выполнено равенство $g = f^\alpha$.

Любое отображение $\varphi\colon \mathbb{F}_2^n \to \mathbb{F}_2^n$ может быть задано системой координатных функций $(f_1, \ldots, f_n)$: если $\varphi\colon x \mapsto y$, $x = (x_1, \ldots, x_n)$, $y = (y_1, \ldots, y_n)$, то $y_i = f_i(x)$, $i = \overline{1, n}$. Систему координатных функций отображения φ будем обозначать $\mathcal{C}_\varphi$.

Рассмотрим семейство подстановок, координатные функции которых эквивалентны относительно группы G. В этом случае для задания подстановки достаточно задать одну функцию и $n-1$ подстановок из группы G. Очевидно, что для заданной группы G таким образом может быть задана не каждая подстановка на $\mathbb{F}_2^n$. Выбор группы подстановок G играет существенную роль. В [5] показано, что при выборе подходящей подстановки $\alpha \in S(\mathbb{F}_2^n)$ любую подстановку $\pi \in S(\mathbb{F}_2^n)$, первая координатная функция которой есть функция f, можно задать системой координатных функций $\mathcal{C}_\pi = \left(f(x), f(x^\alpha), \ldots, f\left(x^{\alpha^{n-1}}\right)\right)$. Такую систему для краткости будем обозначать $\mathcal{C}(f; \alpha)$. Для минимизации сложности задания подстановки необходимо выбирать подстановку α, допускающую простую реализацию. Например, подстановку, реализуемую линейным регистром сдвига. Для фиксированной подстановки α множество подстановок, задаваемых системами координатных функций вида $\mathcal{C}(f; \alpha)$, будем обозначать $\mathcal{C}[\alpha]$:

$$\mathcal{C}[\alpha] = \left\{ \pi \in S(\mathbb{F}_2^n) \;\middle|\; \mathcal{C}_\pi = \mathcal{C}(f; \alpha), f \in F_2(n) \right\}. \tag{2}$$

Поскольку элементами множества $\mathcal{C}[\alpha]$ являются подстановки на $\mathbb{F}_2^n$, их координатные функции являются сбалансированными функциями, т. е. имеют вес 2^{n-1}. В частности, в формуле (2) функция $f \in F_2(n)$ является сбалансированной.

2. Подстановки, порождаемые фильтрующим генератором

Пусть ρ_l — преобразование, реализуемое регистром сдвига с аффинной функцией обратной связи $l \in F_2(n)$ от n переменных:

$$\rho_l : x = (x_1, \ldots, x_n) \mapsto (x_2, \ldots, x_n, l(x)), \quad x \in \mathbb{F}_2^n. \tag{3}$$

Далее рассматриваются только биективные преобразования ρ_l, поэтому функция l линейна по x_1. В частности, преобразование ρ_{x_1} реализует циклический сдвиг набора x влево на одну позицию.

Подстановки из класса $\mathcal{C}[\rho_l]$ рассматривались, например, в [2, 3, 6]. В [3] предложен метод, который сводит проверку сбалансированности отображения к проверке сбалансированности отображений на двоичных наборах меньшей длины. Напомним, что отображение $\varphi\colon X^n \to X^m$, где X — произвольное конечное множество, называется сбалансированным, если для всех $x \in X^m$ мощности полных прообразов $\varphi^{-1}(x)$ одинаковы [7]. С помощью этого метода описаны аффинные функции $l \in F_2(n)$ обратной связи регистров сдвига и соответствующие им нелинейные функции $f = f(x_1, \ldots, x_k)$ от k, $k \leqslant 6$, переменных, для которых система функций $\mathcal{C}(f; \rho_l)$ является системой координатных функций некоторой подстановки. В этой же работе отмечается актуальность исследований подстановок, координатные функции которых имеют вид $\mathcal{C}(f; \rho_l)$, в связи с исследованием классов регистров сдвига, обладающих одинаковой цикловой структурой, и построения на их основе нелинейных регистров сдвига большого периода (2^n или $2^n - 1$).

В [4] получено описание таких пар функций (f, l), где $f \in F_2(n)$ — нелинейная функция, зависящая существенно только от первых трех переменных, $l \in F_2(n)$ — аффинная, что система функций $\left(f(x), f(x^{\rho_l}), \ldots, f\left(x^{\rho_l^{n-2}}\right)\right)$ является системой координатных функций сбалансированного отображения из V_n в V_{n-1}. Отметим, что в [4] такие системы функций назывались *ортогональными*, а в [2] — *регулярными*. Развивая результаты [4], опишем классы функций f и l, задающих подстановки $\pi \in S(\mathbb{F}_2^n)$, $\mathcal{C}_\pi = \mathcal{C}(f; \rho_l)$.

Лемма 1. *Пусть* $f, l \in F_2(n)$, $f(x) = x_2 + x_3 + x_1x_2$, l *линейна по* x_1,

$$\left\{ f\left(x^{\rho_l^i}\right) = y_{i+1}, \quad i = \overline{0, n-1}\,. \right. \tag{4}$$

Положим $c_3 = y_1$, $c_4 = y_2$, $c_t = y_{t-2} + y_{t-3}(1 + c_{t-2})$, $t \geqslant 5$.
Тогда для $t \in \overline{3, n}$ *верны соотношения*:

$$x_t = c_t + \begin{cases} y_2y_4 \cdot \ldots \cdot y_{t-3}\overline{x}_1x_2, & \text{если } t \text{ нечетно}, \\ y_1y_3 \cdot \ldots \cdot y_{t-3}\overline{x}_2, & \text{если } t \text{ четно}, \end{cases} \tag{5}$$

$$c_ty_1y_3 \cdot \ldots \cdot y_{t-2} = y_1y_3 \cdot \ldots \cdot y_{t-2}, \quad \text{если } t \text{ нечетно}, \tag{6}$$

$$c_ty_2y_4 \cdot \ldots \cdot y_{t-2} = y_2y_4 \cdot \ldots \cdot y_{t-2}, \quad \text{если } t \text{ четно}. \tag{7}$$

Доказательство. Для нечетного t, $t = 2r + 1$, $r \in \overline{1, \frac{n-1}{2}}$, докажем равенство (5) индукцией по r. При $r = 1$ равенство (5) верно, поскольку из (4) следует, что

$$x_3 = x_2 + x_1x_2 + y_1 = y_1 + \overline{x}_1x_2.$$

Допустим, что при любом $k \in \overline{1, \frac{n-3}{2}}$ равенство (5) верно для всех нечетных t, $t = 2r+1$, $r \in \overline{1, k-1}$, и докажем его для $t = 2k+1$. Из $(2k-1)$-го и $(2k-2)$-го уравнений системы (4) находим:

$$\begin{aligned} x_{2k+1} &= y_{2k-1} + x_{2k} + x_{2k-1}x_{2k} = y_{2k-1} + \overline{x}_{2k-1}x_{2k} \\ &= y_{2k-1} + \overline{x}_{2k-1}(y_{2k-2} + \overline{x}_{2k-2}x_{2k-1}) = y_{2k-1} + y_{2k-2}\overline{x}_{2k-1}. \end{aligned}$$

Отсюда по предположению индукции

$$\begin{aligned} x_{2k+1} &= y_{2k-1} + y_{2k-2}\,(1 + c_{2k-1} + y_2y_4 \cdot \ldots \cdot y_{2k-4}\overline{x}_1x_2) \\ &= y_{2k-1} + y_{2k-2}\,(1 + c_{2k-1}) + y_2y_4 \cdot \ldots \cdot y_{2k-4}y_{2k-2}\overline{x}_1x_2. \end{aligned}$$

Таким образом, для нечетных t равенство (5) верно.

Для четного t с помощью соотношений

$$\begin{aligned} x_4 &= y_2 + y_1\overline{x}_2, \\ x_{2k} &= y_{2k-2} + \overline{x}_{2k-2}x_{2k-1} = y_{2k-2} + y_{2k-3}\overline{x}_{2k-2} \end{aligned}$$

аналогично доказывается равенство (5).

Для нечетного t, $t = 2r + 1$, $r \in \overline{1, \frac{n-1}{2}}$, докажем равенство (6) индукцией по r. При $r = 1$ имеем:

$$c_3y_1 = y_1y_1 = y_1.$$

Пусть $k \in \mathbb{N}$ и (6) верно для всех нечетных t, $t = 2r+1$, $r \leqslant k-1$, докажем его для $t = 2k+1$. Имеем:

$$c_{2k+1}y_1y_3 \cdot \ldots \cdot y_{2k-1} = (y_{2k-1} + y_{2k-2}(1 + c_{2k-1}))\, y_1y_3 \cdot \ldots \cdot y_{2k-1}$$
$$= y_1y_3 \cdot \ldots \cdot y_{2k-1} + y_1y_3 \cdot \ldots \cdot y_{2k-1} \cdot y_{2k-2} + c_{2k-1} \cdot y_1y_3 \cdot \ldots \cdot y_{2k-3} \cdot y_{2k-1} \cdot y_{2k-2}.$$

Используя предположение индукции, находим:

$$c_{2k+1}y_1y_3 \cdot \ldots \cdot y_{2k-1} = y_1y_3 \cdot \ldots \cdot y_{2k-1} + y_1y_3 \cdot \ldots \cdot y_{2k-1} \cdot y_{2k-2}$$
$$+ y_1y_3 \cdot \ldots \cdot y_{2k-3} \cdot y_{2k-1} \cdot y_{2k-2} = y_1y_3 \cdot \ldots \cdot y_{2k-1}.$$

Равенство (7) для четного t доказывается аналогично. □

Теорема 1. *Пусть* $f, l \in F_2(n)$, $n \geqslant 5$, f *— нелинейная функция, существенно зависящая от первых трех переменных,* $l = x_1 + \sum\limits_{i=2}^{n} b_i x_i + b_0$, $b_0, b_i \in \mathbb{F}_2$, $i = \overline{2,n}$. *Отображение* φ, *задаваемое системой координатных функций* $\mathcal{C}(f; \rho_l)$, *сбалансировано в том и только том случае, когда* $n \geqslant 5$ *нечетно, а функции* f *и* l *удовлетворяют одному из следующих условий*:

1) $f = x_2 + x_3 + x_1x_2 + a$ *и* $l = x_1 + bx_{n-1}$,
2) $f = x_1 + x_3 + x_1x_2 + a$ *и* $l = x_1 + bx_{n-1} + b$,
3) $f = x_1 + x_2 + x_2x_3 + a$ *и* $l = x_1 + bx_3$,
4) $f = x_1 + x_3 + x_2x_3 + a$ *и* $l = x_1 + bx_3 + b$,

где $a, b \in \mathbb{F}_2$.

Доказательство. Заметим, что необходимым условием сбалансированности отображения множества $\mathbb{F}_2^n$, задаваемого системой координатных функций, является условие сбалансированности отображения, задаваемого его первыми $n-1$ функциями [1]. Из результатов работы [4] следует, что рассматриваемые функции f и l должны удовлетворять одному из условий:

1) $f = x_2 + x_3 + x_1x_2 + a$ и $b_3 = b_5 = \ldots = b_n = 0$,
2) $f = x_1 + x_3 + x_1x_2 + a$ и $b_3 = b_5 = \ldots = b_n = 0$,
3) $f = x_1 + x_2 + x_2x_3 + a$ и $b_2 = b_4 = \ldots = b_{n-1} = 0$,
4) $f = x_1 + x_3 + x_2x_3 + a$ и $b_2 = b_4 = \ldots = b_{n-1} = 0$.

Очевидно, что система $(f_1, \ldots, f_n)$, $f_i \in F_2(n)$, $i = \overline{1,n}$, является системой координатных функций подстановки на $\mathbb{F}_2^n$ в том и только том случае, когда система уравнений

$$\left\{ f_i(x) = z_i, \quad i = \overline{1,n} \right., \tag{8}$$

относительно $x \in \mathbb{F}_2^n$ имеет единственное решение для любого $(z_1, \ldots, z_n) \in \mathbb{F}_2^n$.

Далее для каждого из четырех необходимых условий выбора функций f и l получим условие однозначного решения системы нелинейных уравнений

$$\left\{ f\left(x^{\rho_l^i}\right) = y_{i+1}, \quad i = \overline{0,n-1}, \right. \tag{9}$$

для любого $(y_1, \ldots, y_n) \in \mathbb{F}_2^n$.

В первом случае, когда $f = x_2 + x_3 + x_1x_2$ и $l(x) = x_1 + \sum_{j=1}^{\frac{n-1}{2}} b_{2j}x_{2j} + b_0$, функции системы $\mathcal{C}(f; \rho_l)$ имеют вид

$$\begin{aligned}
f\left(x^{\rho_l^i}\right) &= x_{i+2} + x_{i+3} + x_{i+1}x_{i+2}, \qquad i \in \overline{0, n-3}, \\
f\left(x^{\rho_l^{n-2}}\right) &= x_n + x_1 + \sum_{j=1}^{\frac{n-1}{2}} b_{2j}x_{2j} + b_0 + x_{n-1}x_n, \\
f\left(x^{\rho_l^{n-1}}\right) &= x_1 + x_2 + \sum_{j=1}^{\frac{n-1}{2}} b_{2j}x_{2j} + \sum_{j=1}^{\frac{n-1}{2}} b_{2j}x_{2j+1} + x_n\left(x_1 + \sum_{j=1}^{\frac{n-1}{2}} b_{2j}x_{2j} + b_0\right).
\end{aligned}$$

Используя лемму 1, получим:

$$\begin{aligned}
c_n y_1 y_3 \cdot \ldots \cdot y_{n-4} &= y_1 y_3 \cdot \ldots \cdot y_{n-2}, \\
x_1 x_n &= c_n x_1, \\
x_{n-1} x_n &= c_{n-1}c_n + y_1 y_3 \cdot \ldots \cdot y_{n-2}\overline{x}_2 + y_2 y_4 \cdot \ldots \cdot y_{n-3}\overline{x}_1 x_2, \\
x_n + x_{n-1}x_n &= c_n + c_{n-1}c_n + y_1 y_3 \cdot \ldots \cdot y_{n-2}\overline{x}_2, \\
x_{2j}x_n &= c_{2j}c_n + c_n y_1 y_3 \cdot \ldots \cdot y_{2j-3}\overline{x}_2 + y_2 y_4 \cdot \ldots \cdot y_{n-3}\overline{x}_1 x_2
\end{aligned}$$

для $j \in \overline{1, \frac{n-3}{2}}$.

Тогда

$$f\left(x^{\rho_l^{n-2}}\right) = c_n + y_2y_4\cdot\ldots\cdot y_{n-3}\overline{x}_1x_2 + x_1 + b_2x_2 + \sum_{j=2}^{\frac{n-1}{2}} b_{2j}c_{2j}$$
$$+ \sum_{j=2}^{\frac{n-1}{2}} b_{2j}y_1y_3\cdot\ldots\cdot y_{2j-3}\overline{x}_2 + b_0 + c_{n-1}c_n + c_{n-1}y_2y_4\cdot\ldots\cdot y_{n-3}\overline{x}_1x_2$$
$$+c_ny_1y_3\cdot\ldots\cdot y_{n-4}\overline{x}_2 = x_1 + \left[b_2 + \sum_{j=2}^{\frac{n-1}{2}} b_{2j}y_1y_3\cdot\ldots\cdot y_{2j-3} + y_1y_3\cdot\ldots\cdot y_{n-2}\right]x_2$$
$$+ c_n + c_{n-1}c_n + \sum_{j=2}^{\frac{n-1}{2}} b_{2j}c_{2j} + \sum_{j=2}^{\frac{n-1}{2}} b_{2j}y_1y_3\cdot\ldots\cdot y_{2j-3} + b_0 + y_1y_3\cdot\ldots\cdot y_{n-2},$$

$$f\left(x^{\rho_l^{n-1}}\right) = x_1 + x_2 + b_2x_2 + \sum_{j=2}^{\frac{n-1}{2}} b_{2j}c_{2j} + \sum_{j=2}^{\frac{n-1}{2}} b_{2j}y_1y_3\cdot\ldots\cdot y_{2j-3}\overline{x}_2$$
$$+ \sum_{j=2}^{\frac{n-1}{2}} b_{2j}c_{2j+1} + \sum_{j=1}^{\frac{n-1}{2}} b_{2j}y_2y_4\cdot\ldots\cdot y_{2j-2}\overline{x}_1x_2 + c_nx_1 + \sum_{j=1}^{\frac{n-1}{2}} b_{2j}c_nc_{2j}$$
$$+\sum_{j=1}^{\frac{n-1}{2}} b_{2j}c_ny_1y_3\cdot\ldots\cdot y_{2j-3}\overline{x}_2 + \sum_{j=1}^{\frac{n-1}{2}} b_{2j}y_2y_4\cdot\ldots\cdot y_{n-3}\overline{x}_1x_2 + c_nb_0 + b_0y_2y_4\cdot\ldots\cdot y_{n-3}\overline{x}_1x_2$$
$$= [1 + c_n]x_1 + \left[1 + b_2 + \sum_{j=2}^{\frac{n-1}{2}} b_{2j}y_1y_3\cdot\ldots\cdot y_{2j-3} + \sum_{j=1}^{\frac{n-1}{2}} b_{2j}y_2y_4\cdot\ldots\cdot y_{2j-2}\right.$$
$$\left.+\sum_{j=1}^{\frac{n-1}{2}} b_{2j}c_ny_1y_3\cdot\ldots\cdot y_{2j-3} + \sum_{j=1}^{\frac{n-1}{2}} b_{2j}y_2y_4\cdot\ldots\cdot y_{n-3} + b_0y_2y_4\cdot\ldots\cdot y_{n-3}\right]x_2$$
$$+\left[\sum_{j=1}^{\frac{n-1}{2}} b_{2j}y_2y_4\cdot\ldots\cdot y_{2j-2} + \sum_{j=1}^{\frac{n-1}{2}} b_{2j}y_2y_4\cdot\ldots\cdot y_{n-3} + b_0y_2y_4\cdot\ldots\cdot y_{n-3}\right]x_1x_2$$
$$+ c_nb_0 + \sum_{j=2}^{\frac{n-1}{2}} b_{2j}c_{2j} + \sum_{j=2}^{\frac{n-1}{2}} b_{2j}c_{2j+1} + \sum_{j=1}^{\frac{n-1}{2}} b_{2j}c_nc_{2j} + \sum_{j=2}^{\frac{n-1}{2}} b_{2j}y_1y_3\cdot\ldots\cdot y_{2j-3}$$

$$+\sum_{j=1}^{\frac{n-1}{2}} b_{2j}c_n y_1 y_3 \cdot \ldots \cdot y_{2j-3}.$$

Полученное аналитическое задание функций системы (9) позволяет сделать вывод о том, что в этой системе переменные $x_3, x_4, \ldots, x_n$ однозначно выражаются через переменные x_1 и x_2 и известные константы $y_2, \ldots, y_{n-2}$. Поэтому система уравнений

$$\begin{cases} f\left(x^{\rho_l^{n-2}}\right) = y_{n-1}, \\ f\left(x^{\rho_l^{n-1}}\right) = y_n, \end{cases} \tag{10}$$

являющаяся следствием системы (9), может быть записана в виде

$$\begin{cases} x_1 + g_2 x_2 + g_0 = y_{n-1}, \\ h_1 x_1 + h_2 x_2 + h_{12} x_1 x_2 + h_0 = y_n, \end{cases} \tag{11}$$

в которой коэффициенты $g_2, g_0, h_1, h_2, h_{12}$ и h_0 зависят только от $y_1, y_2, \ldots, y_{n-2}$. Значит, при рассматриваемых f и l система (9) имеет единственное решение в том и только том случае, когда система (11) имеет единственное решение. Последнее равносильно тому, что функции, стоящие в левых частях уравнений системы (11), являются сбалансированными при всех $y_1, y_2, \ldots, y_n$. Это означает, что для всех $y_1, y_2, \ldots, y_n$ коэффициент h_{12} при $x_1 x_2$ в системе (11) должен быть равен 0. Таким образом, при всех $y_1, \ldots, y_n$

$$\sum_{j=1}^{\frac{n-1}{2}} b_{2j} y_2 y_4 \cdot \ldots \cdot y_{2j-2} + \sum_{j=1}^{\frac{n-1}{2}} b_{2j} y_2 y_4 \cdot \ldots \cdot y_{n-3} + b_0 y_2 y_4 \cdot \ldots \cdot y_{n-3} = 0.$$

Последнее возможно только при $b_0 = b_2 = \ldots = b_{n-3} = 0$.

Поэтому в рассматриваемом случае система $\mathcal{C}(f; \rho_l)$ является системой координатных функций сбалансированного отображения тогда и только тогда, когда

$$f = x_2 + x_3 + x_1 x_2, l(x) = x_1 + b_{n-1} x_{n-1}, \qquad b_{n-1} \in \mathbb{F}_2. \tag{12}$$

Во втором случае функция l остается прежней — $l(x) = x_1 + \sum_{j=1}^{\frac{n-1}{2}} b_{2j} x_{2j} + b_0$, а порождающая функция системы $\mathcal{C}(h; \rho_l)$ — $h(x) = x_1 + x_3 + x_1 x_2$, поэтому координатные функции системы $\mathcal{C}(h; \rho_l)$ имеют

вид

$$h\left(x^{\rho_l^i}\right) = x_{i+1} + x_{i+3} + x_{i+1}x_{i+2}, \qquad i \in \overline{0, n-3},$$

$$h\left(x^{\rho_l^{n-2}}\right) = x_{n-1} + x_1 + \sum_{j=1}^{\frac{n-1}{2}} b_{2j}x_{2j} + b_0 + x_{n-1}x_n,$$

$$h\left(x^{\rho_l^{n-1}}\right) = x_n + x_2 + \sum_{j=1}^{\frac{n-1}{2}} b_{2j}x_{2j+1} + x_n\left(x_1 + \sum_{j=1}^{\frac{n-1}{2}} b_{2j}x_{2j} + b_0\right).$$

Пусть $\varphi, \theta : V_n \to V_n$ такие отображения, что

$$\mathcal{C}_\varphi = \mathcal{C}(h; \rho_l), \qquad \theta : x = (x_1, \ldots, x_n) \mapsto (\overline{x}_1, \ldots, \overline{x}_n) \text{ для всех } x \in \mathbb{F}_2^n.$$

Координатные функции $g_0, \ldots, g_{n-1}$ отображения $\theta\varphi\theta$ имеют вид

$$g_i = x_{i+2} + x_{i+3} + x_{i+1}x_{i+2}, \qquad i \in \overline{0, n-3},$$

$$g_{n-2} = x_n + x_1 + \sum_{j=1}^{\frac{n-1}{2}} b_{2j}x_{2j} + b_0 + x_{n-1}x_n + \sum_{j=1}^{\frac{n-1}{2}} b_{2j},$$

$$g_{n-1} = x_1 + x_2 + \sum_{j=1}^{\frac{n-1}{2}} b_{2j}x_{2j} + \sum_{j=1}^{\frac{n-1}{2}} b_{2j}x_{2j+1} + x_n\left(x_1 + \sum_{j=1}^{\frac{n-1}{2}} b_{2j}x_{2j} + b_0 + \sum_{j=1}^{\frac{n-1}{2}} b_{2j}\right) + b_0.$$

Сравним координатные функции системы $\mathcal{C}_{\theta\varphi\theta}$ и системы $\mathcal{C}(f; \rho_l)$, $f = x_2 + x_3 + x_1x_2$, рассмотренной в предыдущем случае. Первые $(n-2)$ функций совпадают. Функции $g_{n-2}(x)$ и $f\left(x^{\rho_l^{n-2}}\right)$ связаны равенством $g_{n-2} = f\left(x^{\rho_l^{n-2}}\right) + \sum_{j=1}^{\frac{n-1}{2}} b_{2j}$. Многочлены функций $g_{n-1}(x)$ и $f\left(x^{\rho_l^{n-1}}\right)$ различаются тем, что в многочлене функции $g_{n-1}(x)$ присутствует свободный член $b_0 \in \mathbb{F}_2$ и у слагаемого вида $x_n\left(x_1 + \sum_{j=1}^{\frac{n-1}{2}} b_{2j}x_{2j} + c\right)$ константа $c \in \mathbb{F}_2$ равна b_0 для функции $f\left(x^{\rho_l^{n-1}}\right)$ и равна $b_0 + \sum_{j=1}^{\frac{n-1}{2}} b_{2j}$ для функции $g_{n-1}(x)$. Поскольку θ — подстановка на $\mathbb{F}_2^n$, из доказанного выше условия (12) следует, что отображение $\theta\varphi\theta$ сбалансировано в том и только том случае, когда $b_{n-1} = b_0$ и $b_2 = \ldots = b_{n-3} = 0$. Таким

образом, система $\mathcal{C}(x_1 + x_3 + x_1x_2; \rho_l)$, $l(x) = x_1 + \sum_{j=1}^{\frac{n-1}{2}} b_{2j}x_{2j} + b_0$, является системой координатных функций сбалансированного отображения в том и только том случае, когда

$$l(x) = x_1 + b_{n-1}x_{n-1} + b_{n-1}, \qquad b_{n-1} \in \mathbb{F}_2.$$

Третий и четвертый случаи выбора порождающей функции f сводятся к рассмотрению первого и второго случаев соответственно. □

В 2006 году А. Е. Тришин отметил, что единственное нелинейное преобразование χ в функции хеширования Keccak (стандарт SHA-3 [9]) соответствует подстановке $\pi \in S(\mathbb{F}_2^5)$ с координатными функциями $\mathcal{C}_\pi = \mathcal{C}(x_1 + x_3 + x_2x_3; \rho_{x_1})$. Поэтому представляет интерес изучение свойств этого преобразования.

Отметим, что подстановки, задаваемые системами координатных функций, описанными в теореме 1, аффинно эквивалентны.

Утверждение 1. *Пусть нечетное* $n \geqslant 5$, *подстановки* $\pi_i \in S(\mathbb{F}_2^n)$ *таковы, что* $\mathcal{C}_{\pi_i} = \mathcal{C}(f_i; \rho_{l_i})$, $i = \overline{1,4}$, *для*

$$\begin{aligned}
f_1 &= x_2 + x_3 + x_1x_2 + a, \quad & l_1 &= x_1 + bx_{n-1},\\
f_2 &= x_1 + x_3 + x_1x_2 + a, \quad & l_2 &= x_1 + bx_{n-1} + b,\\
f_3 &= x_1 + x_2 + x_2x_3 + a, \quad & l_3 &= x_1 + bx_3,\\
f_4 &= x_1 + x_3 + x_2x_3 + a, \quad & l_4 &= x_1 + bx_3 + b.
\end{aligned}$$

Тогда

$$\pi_2 = \eta\pi_1\eta, \tag{13}$$

$$\pi_3 = \omega\rho_{l_1}^{-2}\pi_1\omega, \tag{14}$$

$$\pi_4 = \eta\pi_3\eta = \eta\omega\rho_{l_1}^{-2}\pi_1\omega\eta, \tag{15}$$

где

$$\begin{aligned}
\eta &: (a_1, \ldots, a_n) \mapsto (\overline{a}_1, \ldots, \overline{a}_n),\\
\omega &: (a_1, \ldots, a_n) \mapsto (a_n, \ldots, a_1).
\end{aligned}$$

Доказательство проводится непосредственной проверкой совпадения координатных функций соответствующих подстановок. □

Поскольку рассмотренные подстановки аффинно эквивалентны, они имеют одинаковые характеристики нелинейности: степень нелинейности и разностную (см. формулы (16) и (17)). Эти характеристики для

отображения $\varphi\colon V_n \to V_m$, задаваемого системой координатных функций $\mathcal{C}_\varphi = (f_1, \ldots, f_m)$, $f_i \in F_2(n)$, $i = \overline{1,m}$, определяются следующим образом:

$$\lambda_\varphi = \min_{(b_1,\ldots,b_m)\in V_m\setminus\{0\}} \deg\left(b_1 f_1 + \ldots + b_m f_m\right), \tag{16}$$

$$p_\varphi = \max_{a\in V_n\setminus\{0\}, b\in V_m} \mathsf{P}(x^\varphi + (x+a)^\varphi = b^\varphi), \tag{17}$$

в формуле (16) $\deg g$ — алгебраическая степень нелинейности многочлена, представляющего функцию $g \in F_2(n)$, в формуле (17) вероятность вычисляется в предположении, что x выбирается из V_n случайно и равновероятно.

Теорема 2. *При условиях утверждения* 1 *верны равенства*

1) $\lambda_{\pi_1} = \lambda_{\pi_2} = \lambda_{\pi_3} = \lambda_{\pi_4} = 2$,

2) $\lambda_{\pi_1^{-1}} = \lambda_{\pi_2^{-1}} = \lambda_{\pi_3^{-1}} = \lambda_{\pi_4^{-1}} = \frac{n+1}{2}$,

3) $p_{\pi_1} = p_{\pi_2} = p_{\pi_3} = p_{\pi_4} = \frac{1}{4}$.

Доказательство. Для вычисления степени нелинейности подстановки π обратимся к ее заданию, полученному при доказательстве теоремы 1. Заметим, что многочлен каждой координатной функции подстановки π содержит уникальный моном степени нелинейности 2, поэтому любая нетривиальная линейная комбинация этих функций будет содержать хотя бы один моном степени нелинейности 2. Поэтому $\deg \pi = 2$.

Найдем теперь $\lambda_{\pi^{-1}}$. Если для $x = (x_1, \ldots, x_n)$ и $y = (y_1, \ldots, y_n)$, $x, y \in \mathbb{F}_2^n$, $\pi\colon x \mapsto y$ и $\pi^{-1}\colon y \mapsto x$, то координатные функции $g_1, \ldots, g_n$ системы $\mathcal{C}_{\pi^{-1}}$ можно рассматривать как функции от переменных $y_1, \ldots, y_n$. Для исследования многочленов этих функций воспользуемся доказательством теоремы 1. После приведения подобных членов систему (11) можно переписать в виде

$$\begin{cases} x_1 + (b_{n-1} + c_n) y_1 y_3 \cdot \ldots \cdot y_{n-4} x_2 = & g, \\ (1 + c_n) x_1 + (1 + (1 + c_n) b_{n-1} y_1 y_3 \cdot \ldots \cdot y_{n-4}) x_2 = & h, \end{cases} \tag{18}$$

где

$$\begin{aligned} g =& c_n + b_{n-1} c_{n-1} + c_{n-1} c_n + (b_{n-1} + c_n) y_1 y_3 \cdot \ldots \cdot y_{n-4} + y_{n-1}, \\ h =& b_{n-1}(c_{n-1} + (1 + c_n) y_1 y_3 \cdot \ldots \cdot y_{n-4} + c_n + c_{n-1} c_n) + y_n. \end{aligned}$$

Решая эту систему линейных уравнений, находим единственное решение:

$$x_1 = y_1y_3 \cdot \ldots \cdot y_{n-4}[b_{n-1} + y_{n-2} + b_{n-1}y_{n-1} + b_{n-1}y_n + b_{n-1}y_{n-2}y_{n-1} + y_{n-2}y_n] + b_{n-1}c_{n-1} + c_n + c_{n-1}c_n + y_{n-1},$$

$$x_2 = y_{n-1} + c_ny_{n-1} + b_{n-1}c_n + y_n.$$

Остальные переменные $x_2, \ldots, x_n$, как следует из леммы 1, выражаются через x_1, x_2 и $y_1, \ldots, y_n$, т. е. в конечном счете через $y_1, \ldots, y_n$.

Значение координатной функции $g_i(y_1, \ldots, y_n)$ на наборе $y_1, \ldots, y_n$ определяется значением x_i при $i = \overline{1, n}$.

Определим функцию $h_t \in F_2(n)$ на наборе $(y_1, \ldots, y_n) \in \mathbb{F}_2^n$ значением c_t. Тогда из выражения c_t через $y_1, \ldots, y_n$ в лемме 1 получаем, что $\deg h_t = \left[\frac{t-1}{2}\right]$.

Таким образом, $\deg g_i = \frac{n+1}{2}$, $i = \overline{1, n}$. Поскольку в многочлене каждой функции g_i содержится уникальный для нее моном степени $\frac{n+1}{2}$, любая нетривиальная линейная комбинация этих функций также будет иметь степень нелинейности $\frac{n+1}{2}$. Поэтому $\lambda_{\pi^{-1}} = \frac{n+1}{2}$.

Пусть $f = x_2 + x_3 + x_1x_2 + a$, $l = x_1 + bx_{n-1}$, $a, b \in \mathbb{F}_2$, тогда координатные функции подстановки π, $\mathcal{C}_\pi = \mathcal{C}(f; \rho_l) = (f_1, \ldots, f_n)$, имеют вид

$$f_{i+1} = f\left(x^{\rho_l^i}\right) = x_{i+2} + x_{i+3} + x_{i+1}x_{i+2} + a, \quad i = \overline{0, n-3}, \tag{19}$$

$$f_{n-1} = f\left(x^{\rho_l^{n-2}}\right) = x_1 + x_n + bx_{n-1} + x_{n-1}x_n + a, \tag{20}$$

$$f_n = f\left(x^{\rho_l^{n-1}}\right) = x_1 + x_2 + bx_{n-1} + bx_n + x_1x_n + bx_{n-1}x_n + a. \tag{21}$$

Оценим количество решений разностного уравнения

$$x^\pi + (x+u)^\pi = v \text{ для } u, v \in \mathbb{F}_2^n, u \neq 0. \tag{22}$$

Выпишем координатные функции отображения $\varphi\colon x \mapsto x^\pi + (x+u)^\pi$. Имеем

$$f_{i+1}(x) + f_{i+1}(x+u) = u_{i+2}x_{i+1} + u_{i+1}x_{i+2} + u_{i+2} + u_{i+3}, \quad i = \overline{0, n-3},$$

$$f_{n-1}(x) + f_{n-1}(x+u) = u_nx_{n-1} + u_{n-1}x_n + bu_{n-1} + \overline{\overline{u}_{n-1}\overline{u}_n},$$

$$f_n(x) + f_n(x+u) = u_nx_1 + bu_nx_{n-1} + (u_1 + bu_{n-1})\,x_n + u_1 + u_2 + b\overline{\overline{u}_{n-1}\overline{u}_n}.$$

Поскольку координатные функции отображения φ линейны, количество решений разностного уравнения (22) совпадает с количеством решений системы линейных уравнений

$$Ux^\downarrow = \tilde{u}^\downarrow + v^\downarrow, \tag{23}$$

где

$$v^{\downarrow} = (v_1, \dots, v_n)^T,$$
$$\tilde{u}^{\downarrow} = \left(u_2+u_3, u_3+u_4, \dots, u_{n-1}+u_n, bu_{n-1}+\overline{\overline{u}_{n-1}\overline{u}_n}, u_1+u_2+b\overline{\overline{u}_{n-1}\overline{u}_n}\right)^T,$$

$$U = \begin{pmatrix}
u_2 & u_1 & 0 & \dots & & & & 0 \\
0 & u_3 & u_2 & 0 & \dots & & & 0 \\
0 & 0 & u_4 & u_3 & 0 & \dots & & 0 \\
\vdots & & \ddots & \ddots & \ddots & \ddots & & \vdots \\
\vdots & & & \ddots & \ddots & \ddots & \ddots & \vdots \\
\vdots & & & & \ddots & \ddots & \ddots & \vdots \\
\vdots & & & & & \ddots & \ddots & \vdots \\
0 & \dots & & & 0 & u_{n-2} & u_{n-1} & 0 \\
0 & \dots & & & 0 & u_n & u_{n-1} & \\
u_n & 0 & \dots & & 0 & bu_n & bu_{n-1}+u_1 &
\end{pmatrix}. \quad (24)$$

Если $b = 1$, то, прибавив к последней строке матрицы U в (24) ее предпоследнюю строку, получим матрицу

$$\tilde{U} = \begin{pmatrix}
u_2 & u_1 & 0 & \dots & & & & 0 \\
0 & u_3 & u_2 & 0 & \dots & & & 0 \\
0 & 0 & u_4 & u_3 & 0 & \dots & & 0 \\
\vdots & & \ddots & \ddots & \ddots & \ddots & & \vdots \\
\vdots & & & \ddots & \ddots & \ddots & \ddots & \vdots \\
\vdots & & & & \ddots & \ddots & \ddots & \vdots \\
\vdots & & & & & \ddots & \ddots & \vdots \\
0 & \dots & & & 0 & u_{n-2} & u_{n-1} & 0 \\
0 & \dots & & & 0 & u_n & u_{n-1} & \\
u_n & 0 & \dots & & 0 & u_1 &
\end{pmatrix}. \quad (25)$$

Если $b = 0$, то $\tilde{U} = U$. Таким образом, при любых $b \in \mathbb{F}_2$ определители матриц U и $\tilde{U}$ совпадают. Поскольку $u \neq 0$, определитель матрицы $\tilde{U}$ не меньше 2 и достигает значения 2, когда вес набора u равен 1. Таким образом, разностное уравнение (22) при всех $u, v \in \mathbb{F}_2^n$, $u \neq 0$, имеет не более 2^{n-2} решений, и эта граница достижима, например, при $u = (1, 0, \dots, 0)$. Тогда $p_\pi = \frac{2^{n-2}}{2^n} = \frac{1}{4}$. □

3. Об одном способе построения нелинейного регистра сдвига периода 2^n-1

В работе [3] отмечается возможность использования подстановок, задаваемых системами координатных функций вида $\mathcal{C}(f;\rho_l)$, для построения нелинейных регистров сдвига периода 2^n-1. Если $\mathcal{C}(f;\rho_l)$ — система координатных функций подстановки π, то регистры сдвига с функциями обратной связи l и F, где $F(x)=f\left(x^{\pi^{-1}\rho_l^n}\right)$, имеют одинаковую цикловую структуру. В частности, если линейный регистр сдвига, реализующий отображение ρ_l, будет регистром сдвига максимального периода 2^n-1, то такой же период будет и у регистра, реализующего отображение ρ_F.

Далее для класса подстановок $\pi\in S(\mathbb{F}_2^n)$, $\mathcal{C}_\pi=\mathcal{C}(f;\rho_l)$, описанного в теореме 1, получено представление функции F многочленом Жегалкина.

Пусть сначала $f=x_2+x_3+x_1x_2$ и $l=x_1+bx_{n-1}$, где $b\in\mathbb{F}_2$. Если $b=0$, т. е. $l=x_1$, то $F=x_1$ и отображение ρ_F линейное. Поэтому далее полагаем $b=1$.

Утверждение 2. *Пусть* $f,l\in F_2(n)$, $n\geqslant 5$ *нечетно*, $f=x_2+x_3+x_1x_2$ *и* $l=x_1+x_{n-1}$; $\pi\in S(\mathbb{F}_2^n)$, $\mathcal{C}_\pi=\mathcal{C}(f;\rho_l)$; $\rho_F=\pi\cdot\rho_l\cdot\pi^{-1}$. *Тогда функция* F *обратной связи регистра, реализующего отображение* ρ_F, *имеет вид*

$$F(x_1,\dots,x_n)=x_1+\overline{x}_{n-3}x_{n-2}+x_{n-3}x_n+\overline{x}_{n-3}\overline{x}_{n-2}x_{n-1}\\+\overline{c}_{n-3}(x_{n-4}x_{n-2}+x_{n-4}x_n+x_{n-4}\overline{x}_{n-2}x_{n-1}),\quad(26)$$

где $c_t=x_{t-2}+x_{t-3}(1+c_{t-2})$, $t\geqslant 5$, $t\in\mathbb{N}$, $c_2=0$, $c_3=x_1$, $c_4=x_2$.

При этом $\deg F=\frac{n+1}{2}$.

Доказательство. Заметим, что

$$f\left(x^{\rho_l^n}\right)=x_1+x_2+x_3+x_{n-1}+x_n+x_1x_2+x_1x_n+x_2x_{n-1}+x_{n-1}x_n.$$

Воспользовавшись решением системы (9), полученным при доказательстве теоремы 1, и выражением переменных x_3, x_{n-1} и x_n через x_1 и x_2, выпишем многочлен Жегалкина функции F:

$$F=x_1+\overline{c}_{n-1}\overline{c}_nx_{n-1}+c_{n-1}x_n+\overline{c}_{n-1}c_n.$$

Здесь c_t имеет следующий вид (см. лемму 1):

$$c_t=x_{t-2}+x_{t-3}(1+c_{t-2}),\qquad c_3=x_1,c_4=x_2.$$

Заметим, что

$$\overline{c}_{n-1}c_n = (\overline{x}_{n-3} + x_{n-4}\overline{c}_{n-3})(x_{n-2} + x_{n-3}c_{n-3}) = \overline{x}_{n-3}x_{n-2} + x_{n-4}x_{n-2}\overline{c}_{n-3}.$$

Поскольку

$$\begin{aligned} x_{n-4}x_{n-3}\overline{c}_{n-3}\overline{c}_{n-2} &= x_{n-4}x_{n-3}\overline{c}_{n-3}(\overline{x}_{n-4} + x_{n-5}\overline{c}_{n-4}) \\ &= x_{n-5}x_{n-4}x_{n-3}\overline{c}_{n-3}\overline{c}_{n-4} = x_{n-5}x_{n-4}x_{n-3}\overline{c}_{n-4}(\overline{x}_{n-5} + x_{n-6}\overline{c}_{n-5}) \\ &= x_{n-6}x_{n-5}x_{n-4}x_{n-3}\overline{c}_{n-4}\overline{c}_{n-5} = \ldots = x_3x_4\ldots x_{n-4}x_{n-3}\overline{c}_4\overline{c}_5 \\ &= x_3x_4\ldots x_{n-4}x_{n-3}\overline{x}_2(\overline{x}_3 + \overline{x}_1x_2) = 0, \end{aligned}$$

имеем

$$\overline{c}_{n-1}\overline{c}_n = \overline{x}_{n-3}\overline{x}_{n-2} + x_{n-4}\overline{x}_{n-2}\overline{c}_{n-3}.$$

Отсюда следует, что

$$\begin{aligned} F = x_1 + \overline{x}_{n-3}x_{n-2} + x_{n-3}x_n + \overline{x}_{n-3}\overline{x}_{n-2}x_{n-1} \\ + \overline{c}_{n-3}(x_{n-4}x_{n-2} + x_{n-4}x_n + x_{n-4}\overline{x}_{n-2}x_{n-1}), \end{aligned}$$

где $c_{n-3} = 0$ при $n = 5$.

Поскольку в выражении c_t через $x_1, \ldots, x_{t-3}$ присутствует моном степени $\left[\frac{t-1}{2}\right]$, а c_{n-3} не зависит от x_{n-4}, x_{n-2} и x_{n-1}, то

$$\deg F = \left[\frac{n-4}{2}\right] + 3 = \left[\frac{n+2}{2}\right].$$

В рассматриваемом случае n нечетно, поэтому окончательно получаем

$$\deg F = \frac{n+1}{2}.$$

□

В приведенной ниже таблице с использованием утверждения 1 представлена связь между нелинейными функциями обратной связи регистров сдвига, соответствующих функциям f и l, описанным в теореме 1. Здесь строки помечены нелинейными функциями f, а столбцы — линейными функциями l. Если система $\mathcal{C}(f; \rho_l)$ задает подстановку, то на пересечении соответствующих строки и столбца записана функция обратной связи нелинейного регистра сдвига, цикловая структура которого совпадает с цикловой структурой линейного регистра, реализующего отображение ρ_l. Функция F, используемая в таблице, задается многочленом (26), отображения ω и η определены в условии утверждения 1. Как видно из таблицы, нелинейные функции обратной связи рассмотренных регистров сдвига аффинно эквивалентны друг другу. Поэтому у них степени нелинейности совпадают и равны $\frac{n+1}{2}$.

Пары нелинейных функций обратной связи регистров сдвига

	$x_1 + x_{n-1}$	$x_1 + x_{n-1} + 1$	$x_1 + x_3$	$x_1 + x_3 + 1$
$x_2 + x_3 + x_1x_2$	$F(x)$	–	–	–
$x_2 + x_3 + x_1x_2 + 1$	$\overline{F}(x^\eta)$	–	–	–
$x_1 + x_3 + x_1x_2$	–	$F(x)$	–	–
$x_1 + x_3 + x_1x_2 + 1$	–	$\overline{F}(x^\eta)$	–	–
$x_1 + x_2 + x_2x_3$	–	–	$F(x^{\rho_{x_1}\omega})$	–
$x_1 + x_2 + x_2x_3 + 1$	–	–	$\overline{F}(x^{\rho_{x_1}\omega\eta})$	–
$x_1 + x_3 + x_2x_3$	–	–	–	$F(x^{\rho_{x_1}\omega})$
$x_1 + x_3 + x_2x_3 + 1$	–	–	–	$\overline{F}(x^{\rho_{x_1}\omega\eta})$

Список литературы

[1] Лидл Р., Нидеррайтер Г., *Конечные поля*: *В* 2 *т.*, **2**, М.: Мир, 1988.

[2] Никонов В. Г., Саранцев А. В., “О сложности совместной реализации в базисе ДНФ регулярных систем булевых функций”, *Математические вопросы криптографии*, **1**:1 (2010), 45–65.

[3] Рожков М. И., “Биективные отображения, порождаемые фильтрующим генератором”, *Прикладная дискретная математика*, **1**:23 (2014), 27–39.

[4] Рожков М. И., “К вопросу построения ортогональных систем двоичных функций с использованием регистра сдвига”, *Лесной вестник*, **3**:3 (2011), 180–185.

[5] Рожков М. И., “О некоторых классах нелинейных регистров сдвига, обладающих одинаковой цикловой структурой”, *Дискретная математика*, **22**:2 (2010), 96–119.

[6] Саранцев А. В., “Построение регулярных систем однотипных двоичных функций с использованием регистра сдвига”, *Лесной вестник*, **32**:1 (2004), 164–169.

[7] *Словарь криптографических терминов*, ред. Б. А. Погорелов и В. Н. Сачков, М.: МЦНМО, 2006, 94 с.

[8] Черемушкин А. В., “Методы аффинной и линейной классификации двоичных функций”, *Труды по дискретной математике*, **4** (2001), 273–314.

[9] “SHA-3 Standard: Permutation-Based Hash and Extenable-Output Functions”, FIPS PUBS 202, 2015.