

УДК 519.7

СТРУКТУРНЫЕ СВОЙСТВА X, S -СЛОЁВ

М. А. Пудовкина

Блочные шифрсистемы, у которых раундовая функция является композицией трёх типов преобразований: наложения ключа (X -слой), преобразования над отдельными частями блока текста (S -слой) и линейного преобразования (L -слой), — называются XSL-сетями. В работе [1] для блочных шифрсистем XSL рассмотрены комбинаторные свойства группы, порождённой X, L -слоями. В данной работе рассматриваются свойства группы, порождённой X, S -слоями.

Пусть $\mathbb{R}$ — множество всех действительных чисел; $\mathbb{N}$ — множество всех натуральных чисел; $\mathbb{N}_0 = \mathbb{N} \cup \{0\}$; $S(X)$ — множество всех подстановок на множестве X ; $X^\times = X \setminus \{0\}$; V_m — векторное пространство размерности m над $\text{GF}(2)$; $\mathbb{R}^+ = \{a \in \mathbb{R} : a \geq 0\}$; $n, m, d \in \mathbb{N}$, $n = md$; $\text{ord}(g)$ — порядок подстановки $g \in S(X)$; $s = (s_{d-1}, \dots, s_0)$, $s_i \in S(X)$; $IG_W = (S_b \wr S_r, W)$ — группа сплетения в её импримитивном действии, где $W = \{W_1, \dots, W_r\}$ — фиксированная система импримитивности с r блоками мощности b ; $\mathbf{p}(g) = (p_{\varepsilon\delta}(g))$ — матрица разностей переходов подстановки $g \in S(X)$ на группе $(X, +)$. Для произвольного вектора $\alpha \in X$ зададим преобразование $h_\alpha : X \rightarrow X$ как $h_\alpha : \beta \rightarrow \beta + \alpha$, $H_n = \{h_\alpha : X \rightarrow X \mid \alpha \in X\}$. С матрицей $\mathbf{a} = (a_{ij})$ над $\mathbb{R}^+$ свяжем матрицу $\bar{\mathbf{a}} = (\bar{a}_{ij})$, у которой

$$\bar{a}_{ij} = \begin{cases} 1, & a_{ij} > 0, \\ 0, & a_{ij} = 0. \end{cases}$$

Пусть X — регулярная абелева группа. Рассмотрим группы $C(s) = \langle s, h_\alpha : \alpha \in X^n \rangle$, $C(s_i) = \langle s_i, h_\alpha : \alpha \in X \rangle$, $i = 1, \dots, d$. Очевидно, что $C(s) = C(s_1) \times \dots \times C(s_d)$.

Зафиксируем произвольное число $i \in \{1, \dots, d\}$.

Если $X = V_m$ и группа $C(s_i)$ импримитивна, то для произвольного вектора $\alpha \in V_m$ выполняется равенство $(W + \alpha)^s = W + \beta_\alpha$ для некоторых подпространства $W < V_m$ и вектора $\beta_\alpha \in V_m$. Из работы [2] следует, что в этом случае $C(s_i) = IG_W$ и подстановка s_i обладает фактор-структурой. Отсюда получаем, что если $s_i \notin IG_W$ для любого подпространства $W < V_m$, то группа $C(s_i)$ примитивна. Для числа $t \geq 2$ и множества X положим

$$X^{[t]} = \{(\alpha_{t-1}, \dots, \alpha_0) \in X^t : \alpha_i \neq \alpha_j, i, j \in \{0, \dots, t-1\}, i \neq j\},$$

$$X^{\times[t]} = \{(\alpha_{t-1}, \dots, \alpha_0) \in (X^\times)^t : \alpha_i \neq \alpha_j, i, j \in \{0, \dots, t-1\}, i \neq j\}.$$

Рассмотрим матрицу $\mathbf{p}^{(t)}(g) = (p_{\varepsilon\delta}^{(t)}(g))$ разностей t -грамм переходов подстановки $g \in S(X)$ на группе $(X, +)$, где

$$p_{\varepsilon\delta}^{(t)}(g) = |X|^{-1} |\{\alpha \in X : (\alpha + \varepsilon_i)^g = \alpha^g + \delta_i, i = 0, \dots, t-1\}|,$$

$\varepsilon = (\varepsilon_{t-1}, \dots, \varepsilon_0) \in X^{\times[t]}$, $\delta = (\delta_{t-1}, \dots, \delta_0) \in X^{\times[t]}$. Положим $\mathbf{p}(g) = \mathbf{p}^{(1)}(g)$.

Лемма 1. Для произвольных подстановки $g \in S(X)$ и числа $t \in \mathbb{N}$ справедливы следующие равенства:

- 1) $\overline{\mathbf{p}^{(t)}(g^i)} = \overline{(\mathbf{p}^{(t)}(g))^i}$ для $i \in \mathbb{N}$;
- 2) для произвольных фиксированных чисел $j_1, \dots, j_c \in \mathbb{N}_0$ и наборов $(\theta_{t-1}, \dots, \theta_0) \in X^{[t]}$, $(\gamma_{t-1}, \dots, \gamma_0) \in X^{[t]}$ существуют элементы $\beta_1, \dots, \beta_c \in X$, одновременно

удовлетворяющие равенствам

$$(\dots((\theta_i + \beta_1)^{g^{j_1}} + \beta_2 - \beta_1^{g^{j_1}})^{g^{j_2}} + \beta_3 - \beta_2^{g^{j_2}})^{g^{j_3}} \dots + \beta_{c-1} - \beta_c^{g^{j_{c-1}}})^{g^{j_c}} - (\beta_c)^{g^{j_c}} = \gamma_i,$$

$$i = 0, \dots, t-1, \text{ тогда и только тогда, когда } \overline{\overline{p_{\theta, \gamma}^{(t)}(g^{j_1+\dots+j_c})}} > 0.$$

Назовём матрицу $\mathbf{p}$ положительной, если все её элементы больше нуля. В этом случае будем использовать запись $\mathbf{p} > 0$. (Матрица $\mathbf{p}$ называется эргодической, если $\mathbf{p}^q > 0$ для некоторого числа $q \in \mathbb{N}$.)

Утверждение 1.

- 1) Пусть g — произвольная подстановка из $S(X)$, $l = \text{ord}(g)$, $t \in \mathbb{N}$, $t \geq 2$. Группа $C(g)$ является t -транзитивной тогда и только тогда, когда $\sum_{i=1}^l (\mathbf{p}^{(t-1)}(g))^i > 0$.
- 2) Пусть $(\mathbf{p}^{(t-1)}(g))^b > 0$ для некоторого числа $b \in \mathbb{N}$. Тогда для любых векторов $\delta, \delta' \in X^{[t]}$ существует элемент $h_{\beta_1}g \dots h_{\beta_b}gh_{\beta_{b+1}} \in C(g)$, $\beta_1, \dots, \beta_{b+1} \in X$, удовлетворяющий равенству $(\delta)h_{\beta_1}g \dots h_{\beta_b}gh_{\beta_{b+1}} = \delta'$.

Следствие 1. Если $t \in \mathbb{N}$, $t \geq 2$ и матрица $\mathbf{p}^{(t-1)}(g)$ эргодическая, то группа $C(g)$ t -транзитивна.

Приведём пример того, что группа $C(g)$ может быть 2-транзитивной, но матрица $\mathbf{p}(g)$ не является эргодической. Пусть g — линейное преобразование с примитивным характеристическим многочленом. Тогда $\mathbf{p}(g)$ — подстановочная матрица порядка $2^m - 1$. Очевидно, что матрица $\mathbf{p}(g)$ не является эргодической, но матрица $\sum_{j=1}^{2^m-1} \overline{\overline{\mathbf{p}(g^j)}}$ положительная.

Рассмотрим классы подстановок с одинаковыми матрицами $\mathbf{p}^{(t)}(g)$. Для подстановки $g \in S(X)$ и $t \in \mathbb{N}$ положим $P^{(t)}(g) = \{s \in S(X) : \mathbf{p}^{(t)}(g) = \mathbf{p}^{(t)}(s)\}$. Ясно, что для любых подстановок $g_1, g_2 \in S(X)$ справедливо соотношение

$$P^{(t)}(g_1) \cap P^{(t)}(g_2) \in \{\emptyset, P^{(t)}(g_1)\}.$$

Подстановке $g \in S(X)$ и векторам $\delta, \lambda \in X$ поставим в соответствие такое преобразование $g_{(\delta, \lambda)} : X \rightarrow X$, что $(\alpha)g_{(\delta, \lambda)} = (\alpha + \delta)^g + \lambda$. Очевидно, что $g_{(\delta, \lambda)}$ — подстановка на множестве X . Множество всех таких подстановок обозначим как $AP(g)$.

Для $t \in \mathbb{N}$, $\delta \in X^{\times[t]}$, $i \in \{0, \dots, t\}$ положим

$$B_{t,i}(\delta) = \{(\theta_t, \dots, \theta_0) \in X^{\times[t+1]} : (\theta_t, \dots, \theta_{i+1}, \theta_{i-1}, \dots, \theta_0) = \delta\},$$

$$U_t(\delta) = \{(\delta_{(t-1)^b}, \dots, \delta_{0^b}) : b \in S_t\}.$$

Лемма 2. Для любых $g \in S(X)$, $t \in \mathbb{N}$ справедливы такие соотношения:

- 1) $p_{\varepsilon\delta}^{(t)}(g) = p_{\lambda\theta}^{(t)}(g)$ для элементов $\varepsilon, \delta \in X^{\times[t]}$, $\lambda \in U_t(\varepsilon)$, $\theta \in U_t(\delta)$;
- 2) $p_{\varepsilon\delta}^{(t)}(g) = \sum_{i=0}^t \sum_{\lambda \in B_{t,i}(\varepsilon)} \sum_{\theta \in B_{t,i}(\delta)} p_{\lambda\theta}^{(t+1)}(g)$ для элементов $\varepsilon, \delta \in X^{\times[t]}$;
- 3) $AP(g) \subseteq P^{(t)}(g)$;
- 4) $P^{(1)}(g) \supseteq P^{(2)}(g) \supseteq \dots \supseteq P^{(t)}(g)$;
- 5) $p_{\varepsilon\delta}^{(t)}(g) = 0$, если $p_{\lambda\theta}^{(t+1)}(g) = 0$ для всех $\lambda \in B_{t,i}(\varepsilon)$, $\theta \in B_{t,i}(\delta)$, $i = 0, \dots, t$.

Утверждение 2. Для $a_1, a_2 \in GL(X)$, $g \in S(X)$, $t \in \mathbb{N}$ тогда и только тогда $a_1ga_2^{-1} \in P^{(t)}(g)$, когда $p_{\varepsilon\delta}^{(t)}(a_1ga_2^{-1}) = p_{\varepsilon a_1\delta a_2}^{(t)}(g)$ для любых $\varepsilon, \delta \in X^{\times[t+1]}$.

ЛИТЕРАТУРА

1. Погорелов Б. А., Пудовкина М. А. О комбинаторных свойствах группы, порождённой X, L -слоями // Прикладная дискретная математика. Приложение. 2012. № 5. С. 22–23.
2. Пудовкина М. А. Линейные структуры групп подстановок над конечным модулем // Прикладная дискретная математика. 2008. № 1. С. 25–28.

УДК 519.7

СОВЕРШЕННАЯ УРАВНОВЕШЕННОСТЬ ДИСКРЕТНЫХ ФУНКЦИЙ И УСЛОВИЕ ГОЛИЧА

С. В. Смышляев

Для всяких $n \geq 1, k \geq 2$ через E_k будем обозначать множество $\{0, 1, \dots, k-1\}$, через $P_k^{(n)}$ — множество k -значных функций n переменных $f: E_k^n \rightarrow E_k$; $P_k = \bigcup_{n=0}^{\infty} P_k^{(n)}$. Для

всякого натурального l и всякой функции $f \in P_k^{(n)}$ будем рассматривать отображение $f_l: E_k^{l+n-1} \rightarrow E_k^l$, $f_l(x_1, x_2, \dots, x_{l+n-1}) = (f(x_1, \dots, x_n), \dots, f(x_l, \dots, x_{l+n-1}))$.

Определение 1. Функция $f \in P_k^{(n)}$ называется совершенно уравновешенной (обозначение $f \in \mathcal{PB}_k^{(n)}$), если для всякого натурального l и всякого $y \in E_k^l$ верно равенство $|f_l^{-1}(y)| = k^{n-1}$.

Определение 2. Функция $f \in P_k^{(n)}$ имеет правый барьер длины $b \geq 1$, если из равенства $f_b(x_1, x_2, \dots, x_{n-1}, x'_n, \dots, x'_{b+n-1}) = f_b(x_1, x_2, \dots, x_{n-1}, x''_n, \dots, x''_{b+n-1})$ следует $x'_n = x''_n$.

Абсолютно аналогично случаю $k = 2$ (см. [1]) для произвольного $k \geq 2$ доказывалось, что наличие барьера влечет совершенную уравновешенность в P_k .

Й. Голичем в работе [2] в 1996 г. рассмотрен (при $k = 2$) вопрос о важном для используемых в фильтрующих генераторах функций свойстве, являющемся естественным усилением свойства совершенной уравновешенности.

Определение 3. Функция $f \in \mathcal{PB}_k^{(n)}$ называется сильно совершенно уравновешенной, если при добавлении любого числа фиктивных переменных между существенными она сохраняет совершенную уравновешенность.

Нетрудно показать, что перестановочность дискретной функции по первой или последней существенной переменной влечет за собой сильную совершенную уравновешенность. Голич в работе [2] предположил, что верно и обратное; данная гипотеза позже, начиная с работы М. Дихтла [3], стала называться гипотезой Голича.

Гипотеза 1 [2]. При $k = 2$ из сильной совершенной уравновешенности некоторой k -значной функции следует её перестановочность (т. е. линейность) по первой или последней существенной переменной.

Косвенное подтверждение справедливости гипотезы Голича было впервые получено в [1] (2008 г.). В работе [4] (2012 г.) гипотеза Голича полностью доказана. Таким образом, известно, что невозможно построить кодирующее устройство на основе регистра сдвига и фильтрующей функции (над алфавитом $\{0, 1\}$), обеспечивающее сохранение истинной случайности битовой последовательности при любом выборе точек входа (см. [2]). Интересен вопрос о возможности построения таких кодирующих