ГРУППОВЫЕ СВОЙСТВА НЕКОТОРЫХ АЛГОРИТМОВ ШИФРОВАНИЯ ФЕЙСТЕЛЯ i-ГО ТИПА

М.А. Пудовкина

Московский инженерно-физический институт (государственный университет),
Каширское шоссе 31, г. Москва, Россия
maricap@rambler.ru

Схема Фейстеля — одна из наиболее часто используемых конструкций при синтезе блочных алгоритмов шифрования. К алгоритмам шифрования на основе схемы Фейстеля относятся, например, алгоритмы ГОСТ 28147-89, CAST-128, KASUMI, Blowfish, RC5, DES, и др. В работах [1, 2] описано обобщение схемы Фейстеля. В работе [3] обобщенная схема Фейстеля названа обобщенной схемой Фейстеля 1-го типа и введены обобщенные схемы Фейстеля 2-го и 3-го типа. Обобщенная схема Фейстеля 1-го типа использовалась при синтезе алгоритма шифрования CAST-256, участвующего в конкурсе AES на стандарт шифрования США. На обобщенной схеме Фейстеля 2-го типа основан алгоритм шифрования RC6, отличающийся от исходного алгоритмов RC6 отсутствием сдвига, зависящего от входных данных. В [4] предложено еще одно обобщение схемы Фейстеля, основанное на конструкции алгоритма шифрования Mars и названное Mars-подобной схемой Фейстеля. Назовем ее обобщенной схемой Фейстеля 4-го типа. Алг оритм шифрования на основе обобщенной схемы Фейстеля i-типа будем называть алгоритмом шифрования Фейстеля i-типа.

Всюду ниже будем придерживаться следующих обозначений: $\overline{a,b} = a,\ a+1,\ldots,b, a<b$; N_0 — множество натуральных чисел с нулем; $m \in N_0,\ m \geqslant 2$ $V_m(2)$ — множество всех m-мерных двоичных векторов над полем $GF(2)$; $F \in \{GF(2^m), V_m(2)\}$; $S(X)$ — симметрическая группа, действующая на множестве X; $P(X)$ — множество всех отображения из X в X.

Пусть также

$$\Pi_{\alpha,\gamma} = \{\pi \in S(F) \mid \beta^\pi + (\beta+\alpha)^\pi = \gamma,\ \ \forall \beta \in F\},$$

где $\alpha, \gamma \in F \backslash \vec{0}$.

В алгоритме шифрования Фейстеля i-типа, $i \in \{\overline{1,4}\}$, раундовая функция осуществляет отображение $g_s^{(i)}: F^n \to F^n$,

$$g_s^{(1)}: (\beta_1, \beta_2, \ldots, \beta_n) \to (\beta_2 + \beta_1^s, \beta_3, \ldots, \beta_n, \beta_1),$$

где $s \in P(F)$,

$$g_s^{(2)}: (\beta_1, \beta_2, \ldots, \beta_n) \to (\beta_2 + \beta_1^{s_1}, \beta_3, \beta_4 + \beta_3^{s_2}, \ldots, \beta_n + \beta_{n-1}^{s_{n/2}}, \beta_1),$$

где n — четное, $s = (s_1, \ldots, s_{n/2}) \in P(F)^{n/2}$,

$$g_s^{(3)}: (\beta_1, \beta_2, \ldots, \beta_n) \to (\beta_2 + \beta_1^{s_1}, \beta_3 + \beta_2^{s_2}, \ldots \beta_n + \beta_{n-1}^{s_{n-1}}, \beta_1),$$

где $s = (s_1, \ldots, s_{n-1}) \in P(F)^{n-1}$,

$$g_s^{(4)}: (\beta_1, \beta_2, \ldots, \beta_n) \to (\beta_2 + \beta_1^{s^2}, \beta_3 + \beta_2^{s^3}, \ldots, \beta_n + \beta_{n-1}^{s^n}, \beta_1),$$

где $s \in P(F)$.

Все описанные выше преобразования s_i зависят от раундового ключа k_i, $i \geqslant 1$.

В данной работе рассматривается случай, когда $s \in S(F)$ для раундовых функций $g_s^{(1)}, g_s^{(4)}$ алгоритмов шифрования Фейстеля 1-го и 4-го типов, $s = (s_1, \ldots, s_{n/2}) \in S(F)^{n/2}$ для раундовой функции $g_s^{(2)}$ алгоритма шифрования Фейстеля 2-го типа и $s = (s_1, \ldots, s_{n-1}) \in S(F)^{n-1}$ для раундовой функции $g_s^{(3)}$ алгоритмов шифрования Фейстеля 3-го типа. Также полагаем

$$S^{[i]} = \begin{cases} S(F), & i \in \{1,4\} \\ S(F)^{n/2}, & i = 2, \\ S(F)^{n-1}, & i = 3. \end{cases}$$

Опишем ситуации, для которых справедливо включение

$$g_s^{(j)} \in S_2 \int S_{2^m n-1}, \quad s \in S^{[j]}, \quad j \in \{1,2,3,4\}.$$

Для этого понадобятся множества $\Pi_{\alpha,\gamma}$, $\alpha, \gamma \in F \backslash \vec{0}$, характеризующие линейные структуры, описание которых приведено в работе [5].

Показано, что для натурального числа $n \geqslant 2$ справедливы следующие свойства.

1. Пусть s — произвольное преобразование из $S^{[1]}$. Тогда $g_s^{(1)} \notin S_2 \int S_{2^m n-1}$.

2. Пусть n четно, вектор $\gamma = (\gamma_1, \ldots, \gamma_n) \in F^n$ и преобразование $s \in S^{[2]}$ таковы, что $\gamma_1 = \gamma_n$, $\gamma_{2j+1} = \gamma_{2j}$, и $\gamma_{2j-1} \neq \gamma_{2j}$, $j = \overline{1, n/2-1}$, и $s_j \in \prod_{\gamma_{2j-1}, \gamma_{2j-1}+\gamma_{2j}}$ для всех $j \in \{\overline{1, n/2-1}\}$. Тогда $g_s^{(2)} \in S_2 \int S_{2^m n-1}$.

3. Пусть $\gamma = (\gamma_1, \ldots, \gamma_n) \in F^n$ и преобразование $s \in S^{[3]}$ таковы, что $\gamma_1 = \gamma_n$, $\gamma_{j+1} \neq \gamma_j$, $j = \overline{1, n-1}$, и $s_j \in \prod_{\gamma_j, \gamma_j+\gamma_{j+1}}$ для всех $j \in \{\overline{1, n-1}\}$. Тогда $g_s^{(3)} \in S_2 \int S_{2^m n-1}$.

4. Пусть $\gamma = (\gamma_1, \ldots, \gamma_n) \in F^n$ и преобразование $s \in S^{[4]}$ таковы, что $\gamma_1 = \gamma_n$, $\gamma_{j+1} \neq \gamma_j$, и $s^{j+1} \in \prod_{\gamma_j, \gamma_j+\gamma_{j+1}}$ для всех $j \in \{\overline{1, n-1}\}$. Тогда $g_s^{(4)} \in S_2 \int S_{2^m n-1}$.

Также показано, что для $j \in \{1,2,3,4\}$ существуют такие преобразования $s \in S^{[j]}$ и такое множество $\Theta \subset F^n$, что преобразование $g_s^{(j)}$ стабилизирует множество Θ в целом. Данное свойство является слабость алгоритма шифрования.

Литература

1. *Feistel H., Notz W., Smith J.L.* Some cryptographic techniques for machine-to-machine data communications // Proc IEEE 1975. V. 63, N 11 P 1545-1554

2. *Schnorr C.P.* On the construction of random number generators and random function generators // Proc Eurocrypt-88, LNCS. 1988. V. 330 P. 225-232

3. *Zheng Y., Matsumoto T., Imai I.* On the construction of block ciphers provably secure and not relying on any unproved hypotheses // Proc. Crypto-89, LNCS, 1989.

4. *Moria S., Vaudenay S.* On the pseudorandomness of top-level schemes of block ciphers // ASIACRYPT'2000, LNCS. 2000. V. 1976. P. 289–302.

5. *Погорелов Б.А., Пудовкина М.А.* Линейные структуры групп подстановок векторных пространств // Проблемы безопасности и противодействия терроризму. Материалы международной конференции в МГУ 25–27 октября 2007 г. (в печати).