Определение 8 [1]. Назовём автомат Мура $R = < Y, Y^\tau, \Gamma, \sigma, \varphi >$ *регистром сдвига длиной* τ, если его функция переходов σ есть функция сдвига, определяемая по формуле

$$\forall y_1 y_2 \dots y_\tau \in Y^\tau \forall y \in Y [\sigma(y_1 y_2 \dots y_\tau, y) = y_2 \dots y_\tau y].$$

Определение 9 [1]. Назовём *регистром сдвига длиной* τ *с ключом* такой автомат Мили с двумя входами $R = < Y \times K, Y^\tau, \Gamma, \sigma', \varphi >$, что для любого значения $k \in K$ его проекция $R_k = < Y, Y^\tau, \Gamma, \sigma'_k, \varphi_k >$ на вход Y есть регистр сдвига длиной τ.

Определение 10 [1]. Назовём поточную шифрсистему $\Sigma_R = < X, K, Y, R, \varepsilon, \delta >$ *регистровой*, если её ГКП R есть регистр сдвига с ключом. Длина регистра R называется размерностью шифрсистемы.

Регистровая шифрсистема размерностью τ является самосинхронизирующейся с задержкой τ по конструктивному определению.

Определение 11. Назовём автоматную шифрсистему $\Sigma_A = < X, Y, K, A^e, A^d >$ *самосинхронизирующейся с задержкой* τ, если таковой является проекция A^d_k автомата A^d для любого $k \in K$:

$$\forall q_0^* \in Q^* \forall y, y' \in Y^* \forall \tilde{y} \in Y^\tau \forall u \in Y^* [\bar{\varphi}^*_k(\psi^*_k(q_0^*, y\tilde{y}), u) = \bar{\varphi}^*_k(\psi^*_k(q_0^*, y'\tilde{y}), u)].$$

Говорят, что некоторая шифрсистема *неотличима от шифрсистемы* Σ, если задаваемые ею последовательностные шифры задаются системой Σ.

Теорема 3. Любая самосинхронизирующаяся с задержкой τ автоматная шифрсистема $\Sigma_A = < X, K, Y, A^e, A^d >$, у которой все проекции A^d_k автомата расшифрования A^d суть сильно связные автоматы, неотличима от некоторой регистровой шифрсистемы $\Sigma_R = < X, K, Y, R, \varepsilon, \delta >$ размерности τ.

ЛИТЕРАТУРА

1. *Панкратов И. В.* К определению понятия самосинхронизирующегося поточного шифра // Вестник Томского госуниверситета. Приложение. 2007. № 23. С. 114–117.

УДК 519.7

ОЦЕНКА ПОКАЗАТЕЛЯ 2-ТРАНЗИТИВНОСТИ ОБОБЩЁННЫХ АЛГОРИТМОВ ШИФРОВАНИЯ ФЕЙСТЕЛЯ[1]

М. А. Пудовкина

Различные обобщения алгоритма шифрования Фейстеля рассмотрены в работах [1 – 6] и др. Некоторые из них являются обобщением конструкций блочных алгоритмов CAST, IDEA, MARS, SKIPJACK и др. В данной работе вводится единая математическая модель, описывающая единым образом разнообразные известные обобщения алгоритма шифрования Фейстеля.

Пусть натуральное $n \geqslant 2$, V_m — множество всех m-мерных двоичных векторов над полем $GF(2)$; $X^* = X \backslash \{0\}$; $P(X)$ — множество всех отображений из X в X; $S(X)$ — множество всех подстановок на X; $\oplus$ — операция покоординатного сложения векторов из V_m; o — нулевое отображение, т. е. $\alpha^o = \mathbf{0}$ для любого $\alpha \in V_m$; e — тождественное отображение; $P(V_m)^0 = \{o\}$, $S(V_m)^{[0]} = \{e\}$, $S(V_m)^{[1]} = S(V_m)$, $\Upsilon_n = \{\upsilon : \{\overline{1,n}\} \to \{0,1\} | \upsilon(1) = 1\}$.

[1]Работа выполнена при поддержке гранта Президента РФ НШ № 4.2008.10.

Для произвольной функции $\upsilon \in \Upsilon_n$ положим

$$H_i^{\upsilon} = \{s_{i,k} | k \in \mathrm{K}\}, i \in \{\overline{1, n-1}\},$$

$$\{\overline{1,n}\}_{\upsilon} = \left\{i \in \{\overline{1,n}\} | \upsilon(i) = 1\right\}, |\upsilon| = \left|\{\overline{1,n}\}_{\upsilon}\right|,$$

$$\mathrm{K}_{\upsilon} = \left\{(k_1, k_{i_2}, \ldots, k_{i_{|\upsilon|}}) \in \mathrm{K}^{|\upsilon|} | i_j \in \{\overline{1,n}\}_{\upsilon}, 1 < i_2 < \cdots < i_{|\upsilon|}\right\},$$

$$g_{k(l)}^{(\upsilon)} = g_{k_1}^{(\upsilon)} g_{k_2}^{(\upsilon)} \ldots g_{k_l}^{(\upsilon)}, k(l) \in (\mathrm{K}_{\upsilon})^l, G^{[\upsilon]} = \left\{g_k^{(\upsilon)} | k \in \mathrm{K}_{\upsilon}\right\}.$$

Также рассмотрим матрицу $\tilde{\pi}(H) = (\tilde{\pi}_{\delta_1\delta_2}(H))$, $H \subseteq P(V_m)$, элементы которой задаются как

$$\tilde{\pi}_{\delta_1\delta_2}(H) = \begin{cases} 1, & \text{если } \forall \alpha \in V_m \exists h \in H : (\alpha \oplus \delta_1)^h \oplus \alpha^h = \delta_2, \\ 0, & \text{иначе.} \end{cases}$$

Определение 1. Для функции $\upsilon : \left\{\overline{1,n}\right\} \to \{0,1\}$ и произвольного преобразования $s = (s_1, \ldots, s_n) \in P_{m,n}^{\upsilon}$ назовём преобразование $g_s^{(\upsilon)} : V_m^n \to V_m^n$, заданное равенством

$$g_s^{(\upsilon)}(\alpha_1, \ldots, \alpha_n) = (\alpha_2 \oplus \alpha_1^{s_1}, \alpha_3 \oplus \alpha_4^{s_2}, \ldots, \alpha_n \oplus \alpha_{n-1}^{s_{n-1}}, \alpha_1^{s_n}),$$

обобщённым υ-алгоритмом шифрования Фейстеля, или просто υ-алгоритмом шифрования Фейстеля.

Преобразование $s = (s_1, \ldots, s_n) \in P_{m,n}^{\upsilon}$ зависит от ключа $k \in \mathrm{K}$. Будем использовать обозначения $g_k^{(\upsilon)}$, $s_{\upsilon,k}$ и $s_{i,k}$, если требуется подчеркнуть данную зависимость.

Отметим, что:

1) если $\upsilon^{(1)} \in \Upsilon_n, \upsilon^{(1)}(i) = 0$ для всех $i \in \left\{\overline{2,n}\right\}$, то $g_s^{(\upsilon^{(1)})}$ — обобщение алгоритма шифрования CAST [5];
2) если $\upsilon^{(2)} \in \Upsilon_n$, $\upsilon^{(2)}(i) = 0$ для всех $i \in \left\{\overline{2,n-1}\right\}$, $\upsilon^{(2)}(n) = 1$ и $s_1 = s_n$, то $g_s^{(\upsilon^{(2)})}$ — обобщение алгоритма шифрования SKIPJACK [1].

Определение 2. Назовём множество $H \subseteq P(V_m)$ 2-транзитивным, если для любых различных пар $(\alpha, \beta), (\alpha', \beta') \in V_m^2, \alpha \neq \beta, \alpha' \neq \beta'$ существует преобразование $h \in H$, удовлетворяющее равенствам $\alpha^h = \alpha'$, $\beta^h = \beta'$.

Определение 3. Назовём число раундов l показателем 2-транзитивности υ-алгоритма Фейстеля, если для любых различных пар (α, β), $(\alpha', \beta') \in V_m^n \times V_m^n$, $\alpha \neq \beta$, $\alpha' \neq \beta'$, существует ключ $k(l) \in \mathrm{K}_{\upsilon}^l$, удовлетворяющий равенствам $\alpha^{g_{k(l)}^{(\upsilon)}} = \alpha'$, $\beta^{g_{k(l)}^{(\upsilon)}} = \beta'$.

Определение 4. Пусть $\upsilon \in \Upsilon_n$ и $i_j \in \{\overline{1,n}\}_{\upsilon}, 1 < i_2 < \cdots < i_{|\upsilon|}$. Назовём υ-алгоритм Фейстеля независимым, если не существует такой функции $w : P(V_m)^{|\upsilon|} \to P(V_m)^{|\upsilon|}$, что для любого преобразования $s \in \left\{s_{\upsilon,k} | k \in \mathrm{K}^{[\upsilon]}\right\}$ найдется число $j \in \{\overline{1,n}\}_{\upsilon}$, для которого $s_{i_j} = w(s_{i_1}, \ldots, s_{i_{j-1}}, s_{i_{j+1}}, \ldots, s_{i_{|\upsilon|}})$.

В работе [1] сформулирована гипотеза относительно оценки числа раундов $\upsilon^{(1)}$-алгоритма и $\upsilon^{(2)}$-алгоритма шифрования Фейстеля, после которых отсутствуют невозможные усечённые разности.

Гипотеза 1 [1]. Существуют υ-алгоритмы шифрования Фейстеля, где $\upsilon \in \left\{\upsilon^{(1)}, \upsilon^{(2)}\right\}$, у которых при любом числе раундов $l \geqslant n^2$ отсутствуют невозможные усечённые разности.

Нами получено нетривиальное доказательство этой гипотезы. Кроме того, получено существенное её усиление, а именно доказана следующая теорема.

Теорема 1. Пусть υ — произвольная функция из множества Υ_n, $\upsilon(n) = e$, и υ-алгоритм Фейстеля независим. Пусть также для всех $i \in \{\overline{1,n}\}_\upsilon$ множество $H_i^\upsilon \subseteq P(V_m)$ таково, что $\tilde{\pi}_{\delta_1\delta_2}(H_i^\upsilon) = 1$ для всех $(\delta_1, \delta_2) \in V_m^* \times V_m$. Тогда для произвольных разностей $\theta, \theta' \in (V_m^n)^*$ и произвольного вектора $\alpha \in V_m^n$ для любого $l \geqslant n^2$ существует преобразование $h \in \left\{g_{k(l)}^{(\upsilon)} | k(l) \in \mathrm{K}_\upsilon^l\right\}$, удовлетворяющее равенству $\alpha^h \oplus (\alpha \oplus \theta)^h = \theta'$.

Также показано, что для произвольного независимого υ-алгоритма Фейстеля, при условии 2-транзитивности множеств $H_i^\upsilon \subseteq P(V_m)$ для всех $i \in \{\overline{1,n}\}_\upsilon$, оценка его показателя 2-транзитивности совпадает с оценкой числа раундов, на котором отсутствуют невозможные разности.

ЛИТЕРАТУРА

1. *Sung J., Lee S., Lim J. et al.* Security for the Skipjack-like Structure against Differential Cryptanalysis and Linear Cryptanalysis // ASIACRYPT'2000, LNCS. 2000. V. 1976. P. 274–288.
2. *Feistel H., Notz W.* Some cryptographic techniques for machine-to-machine data communications // Proc. IEEE. 1975. V. 63. No. 11. P. 1545–1554.
3. *Schnorr C. P.* On the construction of random number generators and random function generators // Advances in Cryptology. Proc. Eurocrypt-88, LNCS. 1988. V. 330. P. 225–232.
4. *Zheng Y., Matsumoto T., Imai I.* On the construction of block ciphers provably secure and not relying on any unproved hypotheses // Crypto-89, LNCS. 1989.
5. *Moriai S., Vaudenay S.* On the pseudorandomness of top-level schemes of block ciphers // ASIACRYPT'2000, LNCS. 2000. V. 1976. P. 289–302.
6. *Schneier B., Kelsey J.* Unbalanced feistel networks and block cipher design // FSE, 3rd International Workshop. Springer Verlag, 1996. P. 121–144.

УДК 621.391.037.372

АНАЛИЗ СТЕГОСИСТЕМ С НАРУШЕНИЕМ КВАНТОВАНИЯ

Е. В. Разинков, Р. Х. Латыпов

Основная задача стеганографии — обеспечение скрытой передачи информации, достигаемой встраиванием секретного сообщения в не привлекающий внимания объект, который и передается по каналу связи [1, 2]. Основные средства, которыми располагает нарушитель — статистические и визуальные атаки. Если визуальная атака направлена на обнаружение секретного сообщения путем исследования стегосообщения человеком, его органами чувств, то статистическая атака основывается на исследовании статистических характеристик цифрового объекта, которые нарушаются в результате сокрытия информации [2].

Один из способов повысить устойчивость стеганографической системы — адаптивный выбор элементов стегоконтейнера для встраивания информации [2 – 5]. К примеру, информация может встраиваться в наиболее зашумленные участки изображения, что усложняет ее обнаружение нарушителем. Следует заметить, однако, что адаптивное