$$\overline{\lambda}_{\varphi_A} \le \max\left\{\left(j^{(s_j)}\right)^2 : j \in \overline{0, p-1}\right\}. \qquad (11)$$

Отметим, что неравенства (6) и (11) позволяют оценивать снизу сложность билинейных атак на шифр, удовлетворяющий условиям теоремы 3, непосредственно по таблицам его узлов замены (подстановок $s^{(j)}$, $j \in \overline{0, p-1}$).

Результаты статистического оценивания распределения параметра (10) для случайной и равновероятной подстановки s степени 2^4 показывают, что для более чем 21 тысячи (из 25 тысяч сгенерированных) подстановок значение указанного параметра заключено в пределах от 0,31 до 0,35.

Литература

1. Biryukov A. Block ciphers and stream ciphers: the state of the art // http://eprint.iacr.org/2004/094.

2. Vaudenay S. Decorrelation: a theory for block cipher security // J. of Cryptology. – 2003. – Vol. 16. – № 4. – P. 249 – 286.

3. Wagner D. Towards a unifying view of block cipher cryptanalysis // Fast Software Encryption. – FSE'04, Proceedings. – Springer Verlag, 2004. – P. 116 – 135.

4. Lai X., Massey J.L., Murphy S. Markov ciphers and differential cryptanalysis // Advances in Cryptology – EUROCRYPT'91, Proceedings. – Springer Verlag, 1991. – P. 17 – 38.

5. Matsui M. Linear cryptanalysis methods for DES cipher // Advances in Cryptology – EUROCRYPT'93, Proceedings. – Springer Verlag, 1994. – P. 386 – 397.

6. Harpes C., Kramer G.G., Massey J.L. A generalization of linear cryptanalysis and the applicability of Matsui's piling-up lemma // Advances in Cryptology – EUROCRYPT'95, Proceedings. – Springer Verlag, 1995. – P. 24 – 38.

7. Junod P. On the complexity of Matsui's attack // Fast Software Encryption. – FSE'01, Proceedings. – Springer Verlag, 2001. – P. 199 – 211.

8. Courtois N.T. Feistel schemes and bi-linear cryptanalysis // Advances in Cryptology – CRYPTO'04, Proceedings. – Springer Verlag, 2004. – P. 23 – 40.

9. Логачев О.А., Сальников А.А., Ященко В.В. Булевы функции в теории кодирования и криптологии. – М.: МЦНМО, 2004. – 470 с.

10. Harpes C., Massey J.L. Partitioning cryptanalysis // Fast Software Encryption. – FSE'97, Proceedings. – Springer Verlag, 1997. – P. 13 – 27.

11. Alekseychuk A.N., Kovalchuk L.V. Upper bounds of maximum values of average differential and linear characteristic probabilities of Feistel cipher with adder modulo 2^m // Theory of Stohastic Processes. – 2006. – Vol. 12(28). – № 1, 2. – P. 20 – 32.

УТОЧНЕННЫЕ ОЦЕНКИ ПРАКТИЧЕСКОЙ СТОЙКОСТИ ГОСТ-ПОДОБНЫХ БЛОЧНЫХ ШИФРОВ ОТНОСИТЕЛЬНО МЕТОДОВ ЛИНЕЙНОГО И РАЗНОСТНОГО КРИПТОАНАЛИЗА

А. Н. Алексейчук, Л. В. Ковальчук, Л. В. Скрыпник
Украина, г. Киев

Линейный криптоанализ [1] и разностный криптоанализ [2] относятся к числу наиболее мощных статистических методов криптографического анализа

блочных шифров. В настоящее время хорошо известны общие способы оценки или обоснования стойкости марковских шифров [3] относительно линейного и разностного криптоанализа (см. работы [4 – 7]) и приведенную в них библиографию). При этом в доступных публикациях уделяется существенно меньше внимания исследованию стойкости немарковских шифров (относительно операции $\oplus$ поразрядного булева сложения на множестве двоичных векторов), к которым относится ГОСТ 28147-89 (далее – ГОСТ).

Следует отметить, что линейному и разностному криптоанализу шифра ГОСТ посвящено немало работ, основной задачей которых является построение высоковероятных дифференциальных или линейных характеристик данного шифра, исходя из определенных эвристических предположений относительно функционирования его ключевого сумматора (см., например, [8 – 10]).

Однако в этих работах не приводятся теоретически обоснованные оценки стойкости шифра ГОСТ относительно линейного или разностного криптоанализа. Общий метод построения таких оценок для произвольных ГОСТ-подобных шифров предложен в [11] и развит в [12, 13].

В докладе представлены уточненные верхние границы параметров, характеризующих стойкость ГОСТ-подобных шифров относительно методов линейного и разностного криптоанализа, которые обобщают и усиливают ранее известные оценки [11 – 13].

Обозначим V_l множество булевых векторов длины $l \in \mathbf{N}$, S^{V_l} – симметрическую группу подстановок на множестве V_l. Для любых векторов $\alpha = (\alpha_1, \ldots, \alpha_l)$, $\beta = (\beta_1, \ldots, \beta_l) \in V_l$ положим

$\alpha\beta = \alpha_1\beta_1 \oplus \ldots \oplus \alpha_l\beta_l$, $\alpha \oplus \beta = (\alpha_1 \oplus \beta_1, \ldots, \alpha_l \oplus \beta_l)$.

Отождествим произвольный вектор $(x_1, \ldots, x_l) \in V_l$ с целым числом $x = 2^{l-1}x_1 + \ldots + 2^0 x_l$. При этом символом $x + y$ обозначим сумму по модулю 2^l чисел $x, y \in V_l$, а символом $\nu(x, y)$ – бит переноса в самый старший (то есть l-й) разряд суммы чисел x и y в кольце $\mathbf{Z}$.

Пусть $g \in S^{V_l}$, $k, \alpha, \beta \in V_l$. Положим $g_k(x) = g(x + k)$, $x \in V_l$,

$$C_g(\alpha,\beta) = 2^{-l}\sum_{x\in V_l}(-1)^{\alpha g(x)\oplus\beta x}, \tag{1}$$

$$I^{(g)}(\alpha,\beta) = 2^{-l}\sum_{k\in V_l}\left(C_{g_k}(\beta,\alpha)\right)^2, \tag{2}$$

$$\Lambda^{(g)}(\alpha,\beta) = 2^{-l}\sum_{k\in V_l}\left(2^{-l}\sum_{a\in\{0,1\}}\left|\sum_{x\in V_l}\sum_{\nu(x,k)=a}(-1)^{\beta g(x+k)\oplus\alpha x}\right|\right)^2, \tag{3}$$

$$d^{(g)}(\alpha,\beta) = 2^{-l}\sum_{k\in V_l}\delta\left(g(k+\alpha)\oplus g(k),\beta\right), \tag{4}$$

$$d_a^{(g)}(\alpha,\beta) = 2^{-l}\sum_{k\in V_l}\sum_{\nu(\alpha,k)=a}\delta\left(g(k+\alpha)\oplus g(k),\beta\right),\ a\in\{0,1\}, \tag{5}$$

$$\Delta^{(g)}(\alpha,\beta) = 2^{-l} \max_{\substack{x\in V_l,\\ (a_1,a_2)\in V_2}} \left\{ \sum_{k\in V_l} \delta\left(g_{k+a_1}(x\oplus\alpha)\oplus g_{k+a_2}(x),\beta\right)\right\}, \tag{6}$$

где $\delta(\cdot,\cdot)$ – символ Кронекера.

Рассмотрим r-раундовый шифр Фейстеля $\Im$ с множеством открытых (шифрованных) сообщений V_n, где $n = 2m$, $m \geq 2$, множеством раундовых ключей $K = V_m$ и функцией шифрования F: $V_n \times K^r \to V_n$. Преобразование $F^{(\kappa)}$ открытого текста $x \in V_n$ в шифрованный текст $y \in V_n$ на ключе $\kappa = (k(1), \ldots, k(r)) \in K^r$ представляет собой композицию r раундовых преобразований:

$$y = F^{(\kappa)}(x) = (f^{(k(r))} \circ \ldots \circ f^{(k(1))})(x),\ x \in V_n. \tag{7}$$

При этом преобразование $f^{(k)}$ ($k \in V_m$) в каждом раунде имеет вид

$$f^{(k)}(x) = f^{(k)}(u, v) = (v, u \oplus \varphi(v + k)), \tag{8}$$

где $x = (u, v)$, $u, v \in V_m$, $\varphi \in S^{V_m}$, а символ + обозначает операцию сложения m-разрядных чисел по модулю 2^m.

Предположим, далее, что $m = pt$, p, $t \in N$, и подстановка φ имеет следующий вид:

$$\varphi(z) = A(s(z)) = A(s^{(p-1)}(z^{(p-1)}), \ldots, s^{(0)}(z^{(0)}))^{\mathrm{T}},\ z = (z^{(p-1)}, \ldots, z^{(0)}) \in V_m, \tag{9}$$

где $z^{(j)} \in V_t$, $s^{(j)} \in S^{V_t}$, $j \in \overline{0, p-1}$, A – обратимая матрица порядка m над полем $\mathbf{GF}(2)$.

Шифр $\Im$, описываемый соотношениями (7) – (9), называется ГОСТ-подобным блочным шифром с раундовой функцией φ и узлами замены (s-блоками) $s^{(j)}$, $j \in \overline{0, p-1}$ [11].

Напомним, что (дифференциальная или линейная) характеристика шифра $\Im$ определяется как произвольная последовательность $\Omega = (\omega_0, \omega_1, \ldots, \omega_r)$ ненулевых булевых векторов $\omega_0, \omega_1, \ldots, \omega_r \in V_n$. Вероятность дифференциальной характеристики Ω при ключе шифрования $(k(1),\ldots,k(r))$ определяется по формуле [2, 7]

$$DP^{(k(r),\ \ldots,k(1))}(\Omega) = \mathbf{P}\left(\bigcap_{i=1}^{r}\{X_i \oplus X_i' = \omega_i\} \mid X \oplus X' = \omega_0\right), \tag{10}$$

где X, X' – случайные, независимые и равновероятные двоичные векторы длины n, $X_i = (f^{k(i)} \circ \ldots \circ f^{k(1)})(X)$, $X_i' = (f^{k(i)} \circ \ldots \circ f^{k(1)})(X')$, $i \in \overline{1,r}$. Среднее значение параметра (10) по всем $(k(1),\ldots,k(r)) \in K^r$ называется средней вероятностью дифференциальной характеристики Ω и обозначается $EDP(\Omega)$.

Таким образом,

$$EDP(\Omega) = |K|^{-r} \sum_{(k(1),\ \ldots,k(r))\in K^r} DP^{(k(r),\ \ldots,k(1))}(\Omega). \tag{11}$$

Средняя вероятность линейной характеристики Ω определяется формально как произведение [7]

$$ELP(\Omega) = \prod_{t=1}^{r}\left(2^{-m}\sum_{k\in V_m}\left(C_{f^{(k)}}(\omega_t,\omega_{t-1})\right)^2\right). \qquad (12)$$

Положим

$$MDP(\Omega) = \prod_{t=1}^{r}\left(2^{-m}\max_{x\in V_n}\{\sum_{k\in V_m}\delta(f^{(k)}(x\oplus\omega_{t-1})\oplus f^{(k)}(x),\omega_t)\}\right). \qquad (13)$$

Параметры (11) и (12) являются традиционными показателями практической стойкости марковских блочных шифров относительно методов разностного и, соответственно, линейного криптоанализа. Как показано в [13], в качестве аналогичных показателей стойкости произвольного блочного шифра $\mathfrak{Z}$, можно использовать числа (12) и (13). Отметим, что для любой характеристики Ω справедливо неравенство

$EDP(\Omega) \le MDP(\Omega)$.

В [11] и, соответственно, в [13] получены следующие верхние границы параметров

$$M_L(\mathfrak{Z}) = \max_{(\Omega)}\{ELP(\Omega)\},\ M_D(\mathfrak{Z}) = \max_{(\Omega)}\{MDP(\Omega)\},$$

где максимумы берутся по всем характеристикам Ω данного ГОСТ-подобного шифра $\mathfrak{Z}$:

$$M_L(\mathfrak{Z}) \le \Lambda(\mathfrak{Z})^{\left[\frac{2r}{3}\right]},\ M_D(\mathfrak{Z}) \le \Delta(\mathfrak{Z})^{\left[\frac{2r}{3}\right]}, \qquad (14)$$

где

$$\Lambda(\mathfrak{Z}) = \max\{\Lambda^{(s^{(j)})}(\alpha,\beta): \alpha,\beta\in V_t\setminus\{0\},\ j\in\overline{0,p-1}\}, \qquad (15)$$

$$\Delta(\mathfrak{Z}) = \max\{\Delta^{(s^{(j)})}(\alpha,\beta): \alpha,\beta\in V_t\setminus\{0\},\ j\in\overline{0,p-1}\} \qquad (16)$$

и числа $\Lambda^{(s^{(j)})}(\alpha,\beta)$, $\Delta^{(s^{(j)})}(\alpha,\beta)$ определяются по формулам (3), (6) соответственно. Неравенства (14) позволяют непосредственно оценивать или обосновывать практическую стойкость ГОСТ-подобных шифров, исходя из определенной информации об их s-блоках (значениях параметров (15), (16)) и количестве раундов шифрования. Вместе с тем, эти соотношения не учитывают свойств линейного преобразования (обратимой матрицы A) в конструкции раундовой функции данного шифра $\mathfrak{Z}$ (см. формулу (9)).

Ниже под весом вектора $z = (z^{(p-1)}, \ldots, z^{(0)}) \in V_m$, где $z^{(j)} \in V_t$, $j\in\overline{0,p-1}$, понимается число $wt(z) = |\{j\in\overline{0,p-1}: z^{(j)}\neq 0\}|$. Индекс ветвления (branch number) $m\times m$-матрицы A над полем $\mathbf{GF}(2)$ определяется по формуле [6]

$$B_A = \min\{wt(x) + wt(xA): x\in V_m\setminus\{0\}\}. \qquad (17)$$

Следующая теорема устанавливает верхние оценки параметра (12), зависящие от индекса ветвления матрицы A и числовых параметров s-блоков ГОСТ-подобного шифра $\mathfrak{Z}$.

Теорема 1. При выполнении соотношений (7) – (9), (17) справедливы неравенства

$$M_L(\mathfrak{I}) \le (\Lambda_{\mathfrak{I}})^{\left[\frac{2r}{3}\right]}, \text{ если } B_A = 2, \tag{18}$$

$$M_L(\mathfrak{I}) \le (\Lambda_{\mathfrak{I}})^{r}, \text{ если } B_A = 3, \tag{19}$$

$$M_L(\mathfrak{I}) \le (\Lambda_{\mathfrak{I}})^{\left[\frac{r}{4}\right]B_A}, \text{ если } B_A \ge 4, \tag{20}$$

где $\Lambda_{\mathfrak{I}} = \max\{\Lambda^{(s^{(j)})}(\alpha,\beta) : (\alpha, \beta) \in V_t \times V_t \setminus \{(0, 0)\}, j \in \overline{0, p-1}\}$.

Обозначим символом W подгруппу абелевой группы $(V_m, \oplus)$, состоящую из всех векторов $z = (z^{(p-1)}, \ldots, z^{(0)}) \in V_m$ (где $z^{(j)} \in V_t$, $j \in \overline{0, p-1}$), удовлетворяющих условию: $z^{(j)} = 0$ для любого $j \in \overline{0, p-2}$.

Следующая теорема устанавливает более точные, по сравнению с неравенствами (14), оценки параметров (12), (13).

Теорема 2. Пусть $\mathfrak{I}$ – ГОСТ-подобный шифр с раундовой функцией (9). Тогда справедливо неравенство

$$M_L(\mathfrak{I}) \le l(\mathfrak{I})^{\left[\frac{2r}{3}\right]}, \tag{21}$$

где

$$l(\mathfrak{I}) = \max\{l^{(s^{(j)})}(\alpha,\beta) : \alpha, \beta \in V_t \setminus \{0\}, \ j \in \overline{0, p-1}\}, \tag{22}$$

и числа $l^{(s^{(j)})}(\alpha,\beta)$ определяются в соответствии с формулой (2).

Кроме того, при выполнении условия

$$\{Az^{\mathrm{T}} : z^{\mathrm{T}} \in W\} \cap W = \{0\} \tag{23}$$

справедливо неравенство

$$M_D(\mathfrak{I}) \le \max\{d(\mathfrak{I})^{r-1}, \ d(\mathfrak{I})^{r+1-2\left[\frac{r}{3}\right]} d'(\mathfrak{I})^{\left[\frac{r}{3}\right]}\}, \tag{24}$$

где

$$d(\mathfrak{I}) = \max\{d^{(s^{(j)})}(\alpha,\beta) : \alpha, \beta \in V_t \setminus \{0\}, \ j \in \overline{0, p-1}\}, \tag{25}$$

$$d'(\mathfrak{I}) = \max\{d_a^{(s^{(j)})}(\alpha,\beta) : \alpha, \beta \in V_t \setminus \{0\}, \ j \in \overline{0, p-1}, \ a \in \{0,1\}\}, \tag{26}$$

а числа $d^{(s^{(j)})}(\alpha,\beta)$ и $d_a^{(s^{(j)})}(\alpha,\beta)$ определяются согласно формулам (4) и (5) соответственно.

Заметим, что условие (23) выполняется для линейного преобразования A, используемого в конструкции шифра ГОСТ.

Вычисления, проведенные для 10000 сгенерированных (случайно, равновероятно и независимо одна от другой) подстановок степени 16, показывают, что более 6500, 5700 и 4500 из них имеют значения параметров (2), (4) и (5) соответственно, содержащиеся в промежутке [0,250, 0,299).

Более того, существует немало долговременных ключевых элементов шифра ГОСТ, для которых значения параметров (22), (25), (26) малы одновременно. Например, если

$s^{(0)} = \ldots = s^{(7)} = (1\ 2\ 7\ 10\ 3\ 4\ 11\ 14\ 6\ 15\ 5\ 9\ 8\ 12\ 13\ 0)$,

то $l(\mathfrak{I}) = 0{,}2500$, $d(\mathfrak{I}) = 0{,}1875$, $d'(\mathfrak{I}) = 0{,}1250$. При этом, согласно формулам (21) и (24), справедливы следующие оценки:

$M_D(\mathfrak{I}) \le 2^{-56}$, $M_L(\mathfrak{I}) \le 2^{-42}$.

Литература

1. Matsui M. Linear cryptanalysis methods for DES cipher // Advances in Cryptology – EUROCRYPT'93, Proceedings. – Springer Verlag, 1994. – P. 386 – 397.

2. Biham E, Shamir A. Differential cryptanalysis of DES-like cryptosystems // Journal of Cryptology. – 1991. – V. 4. – № 1. – P. 3 – 72.

3. Lai X., Massey J.L., Murphy S. Markov ciphers and differential cryptanalysis // Advances in Cryptology – EUROCRYPT'91, Proceedings. – Springer Verlag, 1991. – P. 17 – 38.

4. Biryukov A. Block ciphers and stream ciphers: the state of the art // http://eprint.iacr.org/ 2004/094.

5. Vaudenay S. Decorrelation: a theory for block cipher security // J. of Cryptology. – 2003. – V. 16. – № 4. – P. 249 – 286.

6. Daemen J. Cipher and hash function design strategies based on linear and differential cryptanalysis. – Doctoral Dissertation, 1995.

7. Vaudenay S. On the security of CS-cipher // Fast Software Encryption. – FSE'99, Proceedings. – Springer Verlag, 1999. – P. 260 – 274.

8. Seki H., Toshinobu K. Differential cryptanalysis of redused round of GOST // Selected Areas in Cryptography. – SAC 2000, Proceedings. – Springer Verlag, 2001. – P. 315 – 323.

9. Долгов В.И., Лисицкая И.В., Олейников Р.В., Шумов А.И. "Слабые" ключи в алгоритме шифрования ГОСТ 28147-89 // Радиотехника. – 2000. – Вып. 114. – С. 63 – 68.

10. Олейников Р.В. Дифференциальный криптоанализ алгоритма шифрования ГОСТ 28147-89 // Радиотехника. – 2001. – Вып. 119. – С. 146 – 152.

11. Alekseychuk A.N., Kovalchuk L.V. Upper bounds of maximum values of average differential and linear characteristic probabilities of Feistel cipher with adder modulo 2^m // Theory of Stohastic Processes. – 2006. – Vol. 12(28). – № 1, 2. – P. 20 – 32.

12. Срыпник Л.В., Ковальчук Л.В. Верхние границы средних вероятностей дифференциалов булевых отображений // Захист інформації. – 2006. – № 3. – С. 7 – 12.

13. Алексейчук А.Н. Верхние границы параметров, характеризующих стойкость немарковских блочных шифров относительно методов разностного и линейного криптоанализа // Захист інформації. – 2006. – № 3. – С. 20 – 28.