Список літератури

1.*Хогланд Г., Мак-Гроу Г.* Взлом программного обеспечения: анализ и использование кода. – М.: Издательский дом "Вильямс", 2005. – 400 с.

2.*Weapons* For The Hunt: Methods for Software Risk Assessment. – OunceLabs Inc., 2004. – 14 p.

3.CERT/CC Overview Incident and Vulnerability Trends. – Pittsburgh: CERT Coordination Center, Software Engineering Institute, Carnegie Mellon University, 2003. – 221 p.

4.*Bishop M., Bailey D.* A Critical Analysis of Vulnerability Taxonomies (CSE-96-11), 1996. – 15 p.

5.*Robert C. Seacord, Allen Householder.* A Structured Approach to Classifying Security Vulnerabilities. Technical Note. – Pittsburgh: Software Engineering Institute, Carnegie Mellon University, 2005. – 39 p.

6.*Ховард М., Лебланк Д.* Защищенный код. – 2-е изд., испр. – Москва: Издательско-торговый дом "Русская Редакция", 2005. – 704 с.

7.*Эриксон Дж.* Хакинг: искусство эксплойта. – СПб.: Символ-Плюс, 2005. – 240 с.

8.*Sverre Huseby.* Innocent Code: A Security Wake-Up Call for Web Programmers. – John Wiley & Sons, 2004. – 246 p.

9.*Мак-Клар С., Шах С., Шах Ш.* Хакинг в Web: атаки и защита. – М.: Издательский дом "Вильямс", 2003. – 384 с.

10. *Бабак В. П., Корченко О. Г.* Інформаційна безпека та сучасні мережеві технології: Англо-українсько-російський словник термінів. – К.: НАУ, 2003. – 670 с.

11. *Пройдаков Э. М., Теплицкий Л. А.* Англо-русский толковый словарь по вычислительной технике, Интернету и программированию. – 3-е изд., испр. и доп. – М.: Издательско-торговый дом "Русская Редакция", 2002. – 640 с.

12. *Корченко А. Г.* Построение систем защиты информации на нечетких множествах. Теория и практические решения. – К.: "МК-Пресс", 2006. – 320 с.

Надійшла 17.05.2006

УДК 621.391:519.2

Алексейчук А.Н.

ВЕРХНИЕ ГРАНИЦЫ ПАРАМЕТРОВ, ХАРАКТЕРИЗУЮЩИХ СТОЙКОСТЬ НЕМАРКОВСКИХ БЛОЧНЫХ ШИФРОВ ОТНОСИТЕЛЬНО МЕТОДОВ РАЗНОСТНОГО И ЛИНЕЙНОГО КРИПТОАНАЛИЗА

Введение

Разностный и линейный криптоанализ [1–3] относится к числу наиболее известных общих методов криптографического анализа блочных шифров (БШ). За последние пять – семь лет произошли качественные изменения в основаниях этих методов, результатом которых стало более глубокое понимание их сущности, роли и положения в общей теории статистических методов криптоанализа БШ. В настоящее время разностный и линейный криптоанализ рассматривается, скорее, как различающий атаки, призванный выявлять определенные потенциальные слабости в конструкциях шифров, а не как метод практического взлома данных конструкций [4–6].

С точки зрения современного разностного и линейного криптоанализа, все блочные шифры естественным образом разделяются на классы марковских и немарковских шифров. Марковские (относительно той или иной групповой операции на множестве блоков шифруемых сообщений) шифры [2], к числу которых относятся DES, IDEA, Rijndael и многие другие БШ, образуют широкий класс блочных шифров, для которых удается построить общую содержательную теорию оценки и обоснования их теоретической или

практической стойкости относительно разностного и линейного криптоанализа (см. работы [4, 5, 7] и приведенную в них библиографию).

Примером блочного шифра, не являющегося марковским (по крайней мере, относительно ряда "естественных" групповых операций), является ГОСТ 28147-89. Как правило, для оценки стойкости таких шифров приходится разрабатывать специальные методы, в значительной мере опирающиеся на конкретные особенности их построения [8, 9].

Обычно нахождение нетривиальных верхних границ параметров, характеризующих теоретическую стойкость данного блочного шифра $\Im$ относительно разностного или линейного криптоанализа (см. ниже формулы (11), (12)), сопряжено со значительными трудностями математического и вычислительного характера. В результате оценивают практическую стойкость шифра относительно специфических разностных или линейных атак, используя при этом различные ad hoc-показатели стойкости, обоснованию адекватности которых часто не уделяют должного внимания [8–11].

В настоящей статье предлагается один из возможных подходов к унифицированному обобщению понятия практической стойкости марковских БШ относительно разностного и линейного криптоанализа (определяемой в терминах средних вероятностей дифференциальных и, соответственно, линейных характеристик) [1, 3, 12 – 14] на произвольные блочные шифры. Показано, что адекватными, в определенном смысле, показателями практической стойкости немарковских БШ относительно разностного и линейного криптоанализа могут служить параметры, определяемые по формулам (20) и (21) соответственно. Для ГОСТ-подобного блочного шифра получено аналитическое выражение верхней границы параметра (20), зависящее только от s-блоков этого шифра и числа раундов шифрования. Отметим, что аналогичные выражения верхних границ параметров (15) и (21) получены ранее в [8].

Дальнейшее изложение в статье построено следующим образом. В п. 1 приведены необходимые сведения о блочных шифрах и связанных с ними понятиях. Точные постановки задач и формулировки основных результатов статьи (см. утверждения 1 – 4) изложены в п. 2. В п. 3 даны доказательства утверждений, а в последнем пункте сформулированы краткие выводы.

1. Основные понятия, обозначения и вспомогательные результаты

Обозначим S^{V_l} симметрическую группу подстановок на множестве $V_l = \{0,1\}^l$, $l \in \mathbf{N}$. Для любых $\alpha = (\alpha_1, \ldots, \alpha_l)$, $\beta = (\beta_1, \ldots, \beta_l) \in V_l$ положим
$\alpha\beta = \alpha_1\beta_1 \oplus \ldots \oplus \alpha_l\beta_l$, $\alpha \oplus \beta = (\alpha_1 \oplus \beta_1, \ldots, \alpha_l \oplus \beta_l)$.

Элементы корреляционной матрицы $C_f = (C_f(\alpha,\beta))_{\alpha,\beta\in V_l}$, таблицы разностей $D_f = (D_f(\alpha,\beta))_{\alpha,\beta\in V_l}$ и таблицы линейных аппроксимаций $L_f = (L_f(\alpha,\beta))_{\alpha,\beta\in V_l}$ подстановки $f \in S^{V_l}$ определяются соответственно по формулам [14, 15]

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

$$D_f(\alpha,\beta) = \mathbf{P}\{f(X\oplus\alpha)\oplus f(X) = \beta\},\ \alpha,\beta \in V_l, \tag{2}$$

$$L_f(\alpha,\beta) = (2\mathbf{P}\{\alpha X = \beta f(X)\} - 1)^2,\ \alpha,\beta \in V_l, \tag{3}$$

где в выражениях (2), (3) X обозначает случайный вектор с равномерным законом распределения на множестве V_l. Из формул (1) и (3) следует равенство

$$L_f(\alpha,\beta) = C_f(\beta,\alpha)^2,\ \alpha,\beta \in V_l. \tag{4}$$

Обозначим $H_l = ((-1)^{\alpha\beta})_{\alpha,\beta\in V_l}$ матрицу Адамара абелевой группы $(V_l, \oplus)$, $\Pi_f = (\delta(f(\alpha),\beta))_{\alpha,\beta\in V_l}$ – подстановочную матрицу, соответствующую подстановке $f \in S^{V_l}$

(здесь и далее δ обозначает символ Кронекера: $\delta(f(\alpha),\beta)=1$, если $f(\alpha)=\beta$; $\delta(f(\alpha),\beta)=0$ – в противном случае). Справедливы следующие равенства [15]:

$$C_f = 2^{-l} H_l \Pi_f{}^T H_l,\ D_f = 2^{-l} H_l L_f H_l. \tag{5}$$

Из первой формулы (5) вытекает, что матрица C_f является унитарной. Следовательно, в силу равенства (4) и второй формулы (5) матрицы L_f и D_f – дважды стохастические [14, 15].

Для любых подстановок $f, g \in S^{V_l}$ обозначим символом $f \circ g$ их композицию: $(f \circ g)(x) = f(g(x))$, $x \in V_l$. Заметим, что $\Pi_{f \circ g} = \Pi_g \Pi_f$ и, следовательно, на основании первого равенства (5)

$$C_{f \circ g} = C_f C_g,\ f, g \in S^{V_l}. \tag{6}$$

Рассмотрим r-раундовый блочный шифр $\Im$ со множеством открытых (шифрованных) сообщений $V_n = \{0,1\}^n$, множеством раундовых ключей K, семейством раундовых шифрующих преобразований $(f^{(k)} \in S^{V_n} : k \in K)$ и функцией шифрования F: $V_n \cdot K^r \to V_n$. Преобразование $F^{(\lambda)}$ открытого сообщения $x \in V_n$ в шифрованный текст $y \in V_n$ на ключе $\lambda = (k(1), \ldots, k(r)) \in K^r$ шифра $\Im$ является композицией r-раундовых шифрующих преобразований $f^{(k(1))}, \ldots, f^{(k(r))}$, определяемых ключом λ:

$$y = F^{(\lambda)}(x) = (f^{(k1)} \circ \ldots \circ f^{(k(1))})(x),\ x \in V_n. \tag{7}$$

Всюду далее предполагается, что ключ $\lambda = (k(1), \ldots, k®)$ является случайным элементом с равномерным законом распределения на множестве K^r.

Блочный шифр $\Im$ называется марковским [2, 14], если для любых x, α, $\beta \in V_n$ выполняется равенство

$$\sum_{k \in K} \delta(f^{(k)}(x \oplus \alpha) \oplus f^{(k)}(x), \beta) = \sum_{k \in K} D_{f^{(k)}}(\alpha, \beta) \tag{8}$$

(здесь и далее под марковским БШ понимается исключительно марковский шифр относительно операции $\oplus$ на множестве V_n).

Дифференциальной (линейной) характеристикой шифра $\Im$ называется произвольная последовательность $\Omega = (\omega_0, \omega_1, \ldots, \omega_r)$ ненулевых векторов $\omega_0, \omega_1, \ldots, \omega_r \in V_n$. Средняя вероятность дифференциальной характеристики Ω определяется по формуле

$$EDP(\Omega) = \prod_{i=1}^{r} \left(|K|^{-1} \sum_{k \in K} D_{f^{(k)}}(\omega_{i-1}, \omega_i) \right), \tag{9}$$

а средняя вероятность линейной характеристики Ω – по формуле

$$ELP(\Omega) = \prod_{i=1}^{r} \left(|K|^{-1} \sum_{k \in K} L_{f^{(k)}}(\omega_{i-1}, \omega_i) \right). \tag{10}$$

Показателями теоретической (или "обоснованной" – provable [5, 13]) стойкости БШ $\Im$ относительно классических методов разностного и линейного криптоанализа являются максимальные значения $D^{\Im}_{\max}(r)$, $L^{\Im}_{\max}(r)$ вероятностей r-раундовых дифференциалов и, соответственно, линейных аппроксимаций шифра $\Im$, определяемые по формулам

$$D^{\Im}_{\max}(r) = \max\{|K|^{-r} \sum_{\lambda \in K^r} D_{F^{(\lambda)}}(\alpha,\beta) : \alpha,\beta \in V_n \setminus \{0\}\}, \tag{11}$$

$$L^{\Im}_{\max}(r) = \max\{|K|^{-r} \sum_{\lambda \in K^r} L_{F^{(\lambda)}}(\alpha,\beta) : \alpha,\beta \in V_n \setminus \{0\}\}, \tag{12}$$

где $F^{(\lambda)}$ – отображение вида (7), и суммирование ведется по всем ключам $\lambda = (k(1), \ldots, k®)$ БШ $\Im$.

Как правило, нахождение точных значений или нетривиальных верхних оценок параметров (11), (12) для данного блочного шифра $\Im$ представляет собой сложную математическую задачу, получить удовлетворительное решение которой удается лишь в отдельных случаях (см. [16, 17]). Вследствие этого обоснование теоретической стойкости подавляющего большинства используемых на практике блочных шифров остается в настоящее время открытой проблемой.

Для марковских шифров известны соотношения, связывающие вероятности r-раундовых дифференциалов (линейных аппроксимаций) шифра со средними вероятностями его дифференциальных (линейных) характеристик [2, 18]:

$$|K|^{-r} \sum_{\lambda \in K^r} D_{F^{(\lambda)}}(\alpha, \beta) = \sum_{\substack{\Omega=(\omega_0,\ldots,\omega_r):\\ \omega_0=\alpha,\, \omega_r=\beta}} EDP(\Omega),\ \alpha, \beta \in V_n \setminus \{0\}, \tag{13}$$

$$|K|^{-r} \sum_{\lambda \in K^r} L_{F^{(\lambda)}}(\alpha, \beta) = \sum_{\substack{\Omega=(\omega_0,\ldots,\omega_r):\\ \omega_0=\alpha,\, \omega_r=\beta}} ELP(\Omega),\ \alpha, \beta \in V_n \setminus \{0\}, \tag{14}$$

где параметры $EDP(\Omega)$ и $ELP(\Omega)$ определяются по формулам (9) и (10) соответственно, а суммирование ведется по всем дифференциальным (линейным) характеристикам $\Omega = (\omega_0, \omega_1, \ldots, \omega_r)$, удовлетворяющим условию $\omega_0 = \alpha$, $\omega_r = \beta$.

Соотношения (13), (14) лежат в основе известных эвристических аргументов (см., например [12, 16–18]) в пользу выбора, в качестве показателей практической стойкости марковских БШ $\Im$ относительно разностного и линейного криптоанализа, соответственно максимальных значений средних вероятностей дифференциальных и линейных характеристик данного шифра $\Im$, которые определяются по формулам

$$M_D(\Im) = \max_{(\Omega)} \{EDP(\Omega)\}, \tag{15}$$

$$M_L(\Im) = \max_{(\Omega)} \{ELP(\Omega)\}. \tag{16}$$

Мотивацией для замены параметров (11), (12) соответственно параметрами (15), (16) служит эвристическое утверждение о том, что все слагаемые в выражении (13) (в выражении (14)), за исключением одного, как правило, пренебрежимо малы. Это единственное слагаемое вносит основной вклад в сумму (13) (соответственно, в (14)) и, следовательно, достаточно точно приближает значение указанной суммы. Другими словами, предполагается, что вероятность произвольного дифференциала (произвольной линейной аппроксимации) (α, β) марковских БШ $\Im$ по существу совпадает со средней вероятностью одной из дифференциальных (линейных) характеристик $\Omega = (\omega_0, \omega_1, \ldots, \omega_r)$, такой, что $\omega_0 = \alpha$, $\omega_r = \beta$ [16–18].

Отметим, что сформулированное предположение выполняется для DES и некоторых других блочных шифров [1, 3, 12]. Вместе с тем оно оказывается ложным для шифра Rijndael [16, 17]. Более весомым аргументом, свидетельствующим в пользу выбора параметров (15), (16) в качестве адекватных показателей практической стойкости марковских БШ, является отсутствие известных в практике криптоанализа случаев реального взлома блочных шифров, имеющих малые (порядка 2^{-n}) максимальные значения средних вероятностей дифференциальных или линейных характеристик [12, 13].

2. Постановка задачи и формулировка основных результатов

Пусть $\Im$ – произвольный блочный шифр с уравнением шифрования (7). Требуется определить параметры для оценки практической стойкости БШ $\Im$ относительно разностного и линейного криптоанализа, которые удовлетворяли бы следующим условиям:

- если $\Im$ является марковским шифром, то новые показатели его практической стойкости относительно разностного и линейного криптоанализа совпадают с традиционными показателями (15) и (16) соответственно;

- эвристические аргументы, используемые для обоснования адекватности показателей практической стойкости марковских БШ [12, 16, 17], сохраняют свою силу для новых показателей.

Справедливы следующие утверждения.

Утверждение 1. Вероятность линейной аппроксимации $(\alpha, \beta) \in V_n \cdot V_n$ произвольного БШ $\Im$ удовлетворяет неравенству

$$|K|^{-r} \sum_{\lambda \in K^r} L_{F^{(\lambda)}}(\alpha, \beta) \le \left(\sum_{\substack{\Omega=(\omega_0,\ldots,\omega_r):\\ \omega_0=\alpha,\, \omega_r=\beta}} ELP(\Omega)^{1/2} \right)^2. \tag{17}$$

Утверждение 2. Для вероятности дифференциала $(\alpha, \beta) \in V_n \cdot V_n$ произвольного БШ $\Im$ справедливо неравенство

$$|K|^{-r} \sum_{\lambda \in K^r} D_{F^{(\lambda)}}(\alpha, \beta) \le \sum_{\substack{\Omega=(\omega_0,\ldots,\omega_r):\\ \omega_0=\alpha,\, \omega_r=\beta}} MDP(\Omega), \tag{18}$$

где
$$MDP(\Omega) \stackrel{\text{def}}{=} \prod_{i=1}^{r} \left(|K|^{-1} \max_{x \in V_n} \{ \sum_{k \in K} \delta(f^{(k)}(x \oplus \omega_{i-1}) \oplus f^{(k)}(x), \omega_i) \} \right), \tag{19}$$

$\Omega = (\omega_0, \omega_1, \ldots, \omega_r)$. При этом неравенство (18) обращается в равенство (и параметр (19) совпадает с параметром (9)) в том и только в том случае, когда $\Im$ является марковским шифром.

Соотношения (17), (18) позволяют ввести (эвристически, по аналогии с марковскими БШ), в качестве показателей практической стойкости произвольного блочного шифра $\Im$ относительно разностного и линейного криптоанализа, соответственно следующие параметры:

$$\widetilde{M}_D(\Im) = \max_{(\Omega)} \{MDP(\Omega)\}, \tag{20}$$

$$\widetilde{M}_L(\Im) = \max_{(\Omega)} \{ELP(\Omega)\}. \tag{21}$$

Отметим, что для марковских шифров введенные показатели совпадают с традиционными (см. формулы (15), (16)). При этом если каждая из сумм в правых частях неравенств (17), (18) может быть аппроксимирована единственным слагаемым, то выражения в правых частях равенств (20) и (21) являются приближенными верхними границами параметров (11) и (12) соответственно.

В качестве конкретного примера немарковского блочного шифра рассмотрим ГОСТ-подобный шифр $\Im$ с длиной блока $n = 2m$ ($m \in \mathbf{N}$), шифрующие преобразования $f^{(k)}$ ($k \in K = V_m$) которого определяются по формуле

$$f^{(k)}(x) = f^{(k)}(u, v) = (v, u \oplus \varphi(v + k)), \tag{22}$$

где $x = (u, v)$ – открытое сообщение в данном раунде, $u, v \in V_m$, $\varphi \in S^{V_m}$, а символ + обозначает операцию сложения m-разрядных двоичных целых чисел, соответствующих булевым векторам, по модулю 2^m.

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

$$\varphi(z) = A(s^{(p-1)}(z^{(p-1)}), \ldots, s^{(0)}(z^{(0)}))^T, z = (z^{(p-1)}, \ldots, z^{(0)}) \in V_m, \tag{23}$$

где $z^{(j)} \in V_t$, $s^{(j)} \in S^{V_t}$ для любого $j \in \overline{0, p-1}$, A – обратимая матрица порядка m над полем $\mathbf{GF}(2)$. Отображение φ называется раундовой функцией шифра $\Im$, а подстановки $s^{(j)}$ ($j \in \overline{0, p-1}$) – s-блоками этого шифра [8].

Введем ряд дополнительных обозначений. Обозначим $x \overset{l}{+} y$ сумму по модулю 2^l двоичных целых чисел, соответствующих векторам $x, y \in V_l$, $l \in \mathbf{N}$. Для любых $g \in S^{V_l}$, $\alpha, \beta \in V_l$ положим $g_k(x) = g(x \overset{l}{+} k)$, $x, k \in V_l$,

$$M^{(g)}(\alpha,\beta) = \max_{x \in V_l}\{2^{-l}\sum_{k \in V_l}\delta(g_k(x \oplus \alpha) \oplus g_k(x), \beta)\}, \tag{24}$$

$$\mu^{(g)}(\alpha,\beta) = \max_{(a_1,a_2)\in\{0,1\}^2}\ \max_{x \in V_l}\{2^{-l}\sum_{k \in V_l}\delta(g_{k+a_1}(x \oplus \alpha) \oplus g_{k+a_2}(x), \beta)\}. \tag{25}$$

Непосредственно из формул (24), (25) следует, что

$$0 \le M^{(g)}(\alpha,\beta) \le \mu^{(g)}(\alpha,\beta) \le 1,\ \alpha,\beta \in V_l.$$

В работе [8] для рассматриваемого ГОСТ-подобного шифра $\Im$ получены аналитические выражения верхних границ параметров (15) и (21), зависящие только от s-блоков этого шифра и числа раундов шифрования. Следующие утверждения устанавливают аналогичную границу параметра (20).

Утверждение 3. Пусть $t, m \in N$, $t \le m-1$, $\psi^{(1)}$ и $\psi^{(2)}$ – подстановки на множествах V_t и V_{m-t} соответственно. Определим подстановку $\psi \in S^{V_m}$, полагая

$$\psi(x_2, x_1) = (\psi^{(2)}(x_2), \psi^{(1)}(x_1)),\ x_1 \in V_t,\ x_2 \in V_{m-t}. \tag{26}$$

Тогда для любых $\alpha = (\alpha_2, \alpha_1)$, $\beta = (\beta_2, \beta_1)$, где $\alpha_1, \beta_1 \in V_t$, $\alpha_2, \beta_2 \in V_{m-t}$, выполняются неравенства

$$M^{(\psi)}(\alpha,\beta) \le M^{(\psi^{(1)})}(\alpha_1,\beta_1)\,\mu^{(\psi^{(2)})}(\alpha_2,\beta_2). \tag{27}$$

Утверждение 4. Пусть $\Im$ – r-раундовый блочный шифр, описываемый соотношениями (7), (22), (23). Тогда

$$\tilde{M}_D(\Im) \le \mu(\Im)^{\left[\frac{2r}{3}\right]},$$

где $\tilde{M}_D(\Im)$ определяется по формуле (20) и

$$\mu(\Im) = \max\{\mu^{(s^{(j)})}(\alpha,\beta) : \alpha, \beta \in V_t \setminus \{0\},\ j \in \overline{0, p-1}\}.$$

3. Доказательства утверждений

3.1. Доказательство утверждения 1. Заметим, что в силу соотношений (6), (7) для любых $\alpha, \beta \in V_n$ выполняются равенства

$$C_{F^{(\lambda)}}(\beta,\alpha) = (C_{f^{(k(r))}\circ\ldots\circ f^{(k(1))}})(\beta,\alpha) = (C_{f^{(k(r))}}\ldots C_{f^{(k(1))}})(\beta,\alpha) = \sum_{\substack{\Omega=(\omega_0,\ldots,\omega_r):\\ \omega_0=\alpha,\ \omega_r=\beta}}\prod_{i=1}^{r} C_{f^{(k(i))}}(\omega_i,\omega_{i-1}).$$

Отсюда на основании равенств (10) и (4)

$$|K|^{-r}\sum_{\lambda\in K^r} L_{F^{(\lambda)}}(\alpha,\beta) = |K|^{-r}\sum_{(k_1,\ldots,k_r)\in K^r}\left(\sum_{\substack{\Omega=(\omega_0,\ldots,\omega_r):\\ \omega_0=\alpha,\ \omega_r=\beta}}\prod_{i=1}^{r} C_{f^{(k(i))}}(\omega_i,\omega_{i-1})\right)^2 =$$

$$= \sum_{\substack{(\omega_0,\ldots,\omega_r),\\ (\omega_0',\ldots,\omega_r'):\\ \omega_0=\omega_0'=\alpha,\ \omega_r=\omega_r'=\beta}}\ \prod_{i=1}^{r}\left(|K|^{-1}\sum_{k\in K} C_{f^{(k)}}(\omega_i,\omega_{i-1})C_{f^{(k)}}(\omega_i',\omega_{i-1}')\right). \tag{28}$$

Далее, согласно неравенству Коши-Буняковского,

$$\left|\,|K|^{-1}\sum_{k\in K} C_{f^{(k)}}(\omega_i,\omega_{i-1})C_{f^{(k)}}(\omega_i',\omega_{i-1}')\right| \le$$

$$\le \left(|K|^{-1} \sum_{k\in K} (C_{f^{(k)}}(\omega_i, \omega_{i-1}))^2 \right)^{1/2} \left(|K|^{-1} \sum_{k\in K} (C_{f^{(k)}}(\omega_i', \omega_{i-1}'))^2 \right)^{1/2}.$$

Следовательно, на основании равенств (28), (4) и (10)

$$|K|^{-r} \sum_{\lambda\in K^r} L_{F^{(\lambda)}}(\alpha,\beta) \le \left(\sum_{\substack{(\omega_0,\ldots,\omega_r):\\ \omega_0=\alpha,\ \omega_r=\beta}} \left(\prod_{i=1}^{r} |K|^{-1} \sum_{k\in K} (C_{f^{(k)}}(\omega_i, \omega_{i-1}))^2 \right)^{1/2} \right)^2 = \left(\sum_{\substack{\Omega=(\omega_0,\ldots,\omega_r):\\ \omega_0=\alpha,\ \omega_r=\beta}} ELP(\Omega)^{1/2} \right)^2,$$

что и требовалось доказать.

3.2. Доказательство утверждения 2. Обозначим для краткости $f_r = f^{(k(r))}$, $F_i = f^{(k(i))} \circ \ldots \circ f^{(k(1))}$, $i \in \overline{1,r}$. Справедливо равенство

$$ED_r(\alpha,\beta) \overset{\text{def}}{=} |K|^{-r} \sum_{\lambda\in K^r} D_{F^{(\lambda)}}(\alpha,\beta) = 2^{-n} \sum_{\substack{(x_1,x_2): x_1\oplus x_2=\alpha,\\ (y_1,y_2): y_1\oplus y_2=\beta}} \mathbf{P}_{F_r}\left({}^{y_1,y_2}/_{x_1,x_2} \right), \tag{29}$$

где $\mathbf{P}_{F_r}\left({}^{y_1,y_2}/_{x_1,x_2} \right) = |K|^{-r} \sum_{\lambda\in K^r} \delta(F^{(\lambda)}(x_1), y_1)\delta(F^{(\lambda)}(x_2), y_2)$ – элементы матрицы переходных вероятностей биграмм случайного отображения $F_r = F^{(\lambda)}$ [5].

В силу независимости раундовых ключей $k(1)$, …, k® выражение в правой части равенства (29) можно представить в виде

$$ED_r(\alpha,\beta) = \sum_{\gamma\in V_n} \sum_{\substack{(x_1,x_2):\\ x_1\oplus x_2=\alpha,}} 2^{-n} \sum_{\substack{(z_1,z_2):\\ z_1\oplus z_2=\gamma}} \mathbf{P}_{F_{r-1}}\left({}^{z_1,z_2}/_{x_1,x_2} \right) \sum_{\substack{(y_1,y_2):\\ y_1\oplus y_2=\beta}} \mathbf{P}_{f_r}\left({}^{y_1,y_2}/_{z_1,z_2} \right). \tag{30}$$

Заметим теперь, что для любых $z_1, z_2 \in V_n$, таких, что $z_1 \oplus z_2 = \gamma$,

$$\sum_{\substack{(y_1,y_2):\\ y_1\oplus y_2=\beta}} \mathbf{P}_{f_r}\left({}^{y_1,y_2}/_{z_1,z_2} \right) = |K|^{-1} \sum_{k\in K} \delta(f^{(k)}(z_1\oplus\gamma)\oplus f^{(k)}(z_1), \beta) \tag{31}$$

и, следовательно, в соответствии с формулой (19),

$$\max_{\substack{(z_1,z_2):\\ z_1\oplus z_2=\gamma}} \left\{ \sum_{\substack{(y_1,y_2):\\ y_1\oplus y_2=\beta}} \mathbf{P}_{f_r}\left({}^{y_1,y_2}/_{z_1,z_2} \right) \right\} = MDP(\gamma,\beta). \tag{32}$$

Из соотношений (29), (30) и (32) вытекает неравенство

$$ED_r(\alpha,\beta) \le \sum_{\gamma\in V_n} ED_{r-1}(\alpha,\gamma)\, MDP(\gamma,\beta), \tag{33}$$

из которого, в свою очередь, непосредственно следует формула (18).

Наконец, согласно соотношениям (9), (30) – (32), неравенство (33) обращается в равенство в том и только в том случае, когда $MDP(\gamma,\beta) = EDP(\gamma,\beta)$ для любых $\beta, \gamma \in V_n$. Последнее условие равносильно тому, что сумма в правой части равенства (31) не зависит от z_1, то есть $\mathfrak{I}$ является марковским шифром.

Утверждение доказано.

3.3. Доказательство утверждения 3. Для любого $z \in V_m$ обозначим z_1 и z_2 подвекторы вектора z, содержащиеся в его младших t и старших $m - t$ двоичных разрядах соответственно. Вектор z будем записывать в виде $z = (z_2, z_1)$.

Пусть $x = (x_2, x_1)$, $k = (k_2, k_1)$, где $x_1, k_1 \in V_t$, $x_2, k_2 \in V_{m-t}$. Рассмотрим числа $x = x_1 + 2^t x_2$ и $k = k_1 + 2^t k_2$, соответствующие указанным булевым векторам. Справедливо равенство

$$\overset{m}{x} + \overset{t}{k} = (x_1 + k_1) + 2^t(x_2 \overset{m-t}{+} k_2 \overset{m-t}{+} \nu(x_1, k_1)), \tag{34}$$

где $\nu(x_1, k_1)$ – бит переноса в самый старший (t-й) разряд суммы чисел x_1 и k_1 в кольце $\mathbf{Z}$.

Для доказательства неравенства (27) зафиксируем $x = (x_2, x_1) \in V_m$ и оценим сверху выражение

$$m_x^{(\psi)}(\alpha,\beta) \stackrel{\text{def}}{=} 2^{-m} \sum_{k \in V_m} \delta\big(\psi_k(x \oplus \alpha) \oplus \psi_k(x), \beta\big).$$

На основании формул (26) и (34) справедливы следующие соотношения:

$$m_x^{(\psi)}(\alpha,\beta) = 2^{-2m} \sum_{k_1 \in V_t} \delta\left(\psi^{(1)}((x_1 \oplus \alpha_1) \overset{t}{+} k_1) \oplus \psi^{(1)}(x_1 \overset{t}{+} k_1), \beta_1 \right) \times$$

$$\times \sum_{k_2 \in V_{m-t}} \delta\left(\psi^{(2)}((x_2 \oplus \alpha_2) \overset{m-t}{+} k_2 \overset{m-t}{+} \nu(x_1 \oplus \alpha_1, k_1)) \oplus \psi^{(2)}(x_2 \overset{m-t}{+} k_2 \overset{m-t}{+} \nu(x_1, k_1)), \beta_2 \right) =$$

$$= \sum_{(a_1,a_2) \in \{0,1\}^2} 2^{-t} \sum_{\substack{k_1 \in V_t: \\ \nu(x_1 \oplus \alpha_1, k_1) = a_1, \\ \nu(x_1, k_1) = a_2}} \delta\left(\psi^{(1)}((x_1 \oplus \alpha_1) \overset{t}{+} k_1) \oplus \psi^{(1)}(x_1 \overset{t}{+} k_1), \beta_1 \right) \times$$

$$\times 2^{-(m-t)} \sum_{k_2 \in V_{m-t}} \delta\left(\psi^{(2)}((x_2 \oplus \alpha_2) \overset{m-t}{+} k_2 \overset{m-t}{+} a_1) \oplus \psi^{(2)}(x_2 \overset{m-t}{+} k_2 \overset{m-t}{+} a_2), \beta_2 \right) \le$$

$$\le 2^{-t} \sum_{k_1 \in V_t} \delta\left(\psi^{(1)}((x_1 \oplus \alpha_1) \overset{t}{+} k_1) \oplus \psi^{(1)}(x_1 \overset{t}{+} k_1), \beta_1 \right) \times$$

$$\times 2^{-(m-t)} \max_{(a_1,a_2) \in \{0,1\}^2} \left\{ \delta\left(\psi^{(2)}((x_2 \oplus \alpha_2) \overset{m-t}{+} k_2 \overset{m-t}{+} a_1) \oplus \psi^{(2)}(x_2 \overset{m-t}{+} k_2 \overset{m-t}{+} a_2), \beta_2 \right) \right\}.$$

Сопоставляя последнее неравенство с формулами (24) и (25), получаем неравенство (27). Утверждение доказано.

3.4. Доказательство утверждения 4 по существу аналогично доказательству теоремы 2 из [8] и здесь не приводится.

Выводы

В данной статье получены верхние границы вероятностей дифференциалов и линейных аппроксимаций произвольного блочного шифра $\mathfrak{I}$ с уравнением шифрования (7), которые позволяют ввести показатели (20) и (21) практической стойкости такого шифра относительно разностного и линейного криптоанализа, по аналогии с параметрами (15), (16), традиционно используемыми для оценки практической стойкости марковских блочных шифров [1, 3, 12–14].

Согласно равенству (21), практическая стойкость немарковского БШ $\mathfrak{I}$ относительно линейного криптоанализа определяется (как и для марковских шифров) максимальным значением средних вероятностей линейных характеристик шифра $\mathfrak{I}$ (см. формулы (10), (16)). С другой стороны, предложенный показатель (20) практической стойкости БШ $\mathfrak{I}$ относительно разностного криптоанализа в общем случае отличается от параметра (15) (максимума средних вероятностей дифференциальных характеристик шифра $\mathfrak{I}$) и совпадает с этим параметром только для марковских шифров.

Следует подчеркнуть, что предложенные для оценки практической стойкости блочных шифров параметры (20), (21) не являются единственно возможными. Как и для марковских шифров, обоснованием их адекватности служат эвристические аргументы и практика современного криптоанализа.

Для ГОСТ-подобного шифра $\mathfrak{I}$, описываемого соотношениями (7), (22), (23), получено аналитическое выражение верхней границы параметра (20); см. утверждение 4. Этот результат представляет собой дополнение к теореме 2 [8], устанавливающей для шифра $\mathfrak{I}$ аналогичные выражения верхних границ параметров (15) и (21). Указанные утверждение и

теорема позволяют оценивать и обосновывать практическую стойкость ГОСТ-подобных шифров относительно разностного (линейного) криптоанализа непосредственно по определенным числовым параметрам их *s*-блоков. Одной из задач дальнейших исследований является построение более общих аналитических границ параметров (20) и (21), учитывающих свойства линейного преобразования в выражении раундовой функции ГОСТ-подобного блочного шифра.

Список литературы

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

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

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

4. *Wagner D.* Towards a unifying view of block cipher cryptanalysis // Fast Software Encryption. – FSE'04, Proceedings. – Springer Verlag, 2004. – P. 16 – 33.

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

6. *Junod P.* On the optimality of linear, differential and sequential distinguishers // Advances in Cryptology – EUROCRYPT'03, Proceedings. – Springer Verlag, 2003. – P. 17 – 32.

7. *Daemen J., Rijmen V.* Statistics of correlation and differentials in block ciphers // http://eprint.iacr.org/ 2005/212.

8. *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. 1-2 (to appear).

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

10. *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.

11. *Shorin V.V., Jelezniakov V.V., Gabidulin E.M.* Linear and differential cryptanalysis of GOST // Univ. Bielefeld, SFB 343 Diskrete Strukturen in der Mathematik. – 2001. – Preprint., available from ftp.uni-bielefeld.de

12. *Knudsen L.R.* Practically secure Feistel cipher // Fast Software Encryption. – FSE'94, Proceedings. – Springer Verlag, 1994. – P. 211 – 221.

13. *Kanda M.* Practical security evaluation against differential and linear cryptanalyses for Feistel ciphers with SPN round function // Selected Areas in Cryptography. – SAC 2000, Proceedings. – Springer Verlag, 2001. – P. 324 – 338.

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

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

16. *Keliher L., Meier H., Tavares S.* Improving the upper Bond on the maximum average linear hull probability for Rijndael // Selected Areas in Cryptography. – SAC 2001. – Proceedings. – Springer Verlag, 2001. – P. 112 – 128.

17. *Baigneres T., Vaudenay S.* Proving the security of AES substitution-permutation network // http://lasecwww.eptf.ch./php_code/publications.

18. *Nyberg K.* Linear approximations of blok ciphers // Advances in Cryptology. – EUROCRYPT'94, Proceedings. – Springer Verlag, 1994. – P. 139 – 144.

Поступила 22.03.2006