УДК 621.391:519.2

Л.В. КОВАЛЬЧУК, В.Т. БЕЗДЕТНЫЙ

ВЕРХНИЕ ОЦЕНКИ СРЕДНИХ ВЕРОЯТНОСТЕЙ РАЗНОСТНЫХ ХАРАКТЕРИСТИК БЛОЧНОГО ШИФРА С ЧЕРЕДОВАНИЕМ МАРКОВСКИХ И ОБОБЩЕННО-МАРКОВСКИХ ПРЕОБРАЗОВАНИЙ

Аннотация. Предложен новый метод построения верхних оценок средних вероятностей разностных характеристик блоковых шифров, который позволяет использовать индекс ветвления даже для шифров, которые не являются марковскими и имеют разные операции в ключевом сумматоре. Получены верхние оценки средних вероятностей разностных характеристик для блочных шифров с чередованием марковских и обобщенно-марковских раундовых преобразований.

Ключевые слова: разностный криптоанализ, марковский шифр, немарковский шифр, обобщенно-марковский шифр.

ВВЕДЕНИЕ

Разностный и линейный методы криптоанализа [1, 2] в настоящее время являются одними из наиболее мощных статистических методов криптоанализа блоковых шифров (БШ). Впервые эти методы использовались для криптоанализа алгоритма DES [1–4] и с тех пор продолжают развиваться параллельно. Большое количество работ по данной тематике подтверждает их тесную взаимосвязь.

Существенным шагом в развитии разностного криптоанализа было введение понятия марковского шифра (МШ) [5]. Хотя само это понятие может быть определено с использованием любой операции на входных и выходных разностях, по умолчанию в определении марковского шифра использовалась операция побитового сложения. Шифры, являющиеся марковскими относительно побитового сложения, наиболее распространены: это DES [6], а также любая схема Фейстеля с побитовым сложением в ключевом сумматоре, Rijndael [7], CS-шифр [8] (а также любой SPN-шифр, у которого раундовая функция является композицией побитового сложения с ключом, блока подстановки и линейного оператора) и т.д. После появления понятия МШ теория оценивания практической стойкости таких шифров, а также теория построения шифров, заведомо стойких к указанным атакам, начали стремительно развиваться. Было сделано два существенных шага в этом направлении: 1) показано, что для МШ вероятность разностной характеристики равна произведению вероятностей раундовых дифференциалов; 2) введено понятие индекса ветвления линейного оператора и показано, какую роль индекс ветвления играет при синтезе БШ, стойких к указанным атакам. На данный момент разработаны мощные математические методы, позволяющие оценивать и обосновывать стойкость МШ к разностному и линейному криптоанализу, а также строить заведомо стойкие БШ (см. [5, 8–14] и библиографию к ним).

Однако помимо МШ достаточно широкое применение имеют и БШ, не являющиеся марковскими, например стандарт ГОСТ 28147-89 (далее — ГОСТ) [15], а также кандидат на новый стандарт БШ Украины — шифр «Калина» [16]. Для немарковских шифров развитие теории оценивания стойкости сталкивается с существенными трудностями. Это связано, в первую очередь, с тем, что для немарковского БШ вероятность разностной характеристики не равна произведению вероятностей раундовых дифференциалов. Во-вторых, одним из отличительных признаков современных немарковских БШ является операция модульного (как правило, по модулю 2^n) сложения в ключевом сумматоре, что вносит дополнительные аналитические трудности при построении оценок вероятностей раундовых дифференциалов вследствие наличия бита переноса между s-блоками. И, наконец, наличие этого бита переноса не позволяет так же просто, как это делается для БШ с побитовым сложением в ключевом сумматоре, использовать индекс ветвления линейного оператора, поскольку в этом случае количество ненулевых компонент разности на входе в ключевой сумматор, вообще говоря, не равно количеству ненулевых компонент разности на выходе из ключевого сумматора.

Следует заметить, что линейному и разностному криптоанализу шифра ГОСТ посвящено множество публикаций, основная цель которых — построение «высоковероятных» линейных или разностных характеристик данного шифра, выходя из некоторых предположений относительно ключевого сумматора (см., например, [17–19]). Но результаты этих работ не позволяют получать теоретически обоснованные оценки стойкости шифра ГОСТ относительно линейного или разностного криптоанализа.

Впервые общий метод получения математически обоснованных оценок стойкости для широкого класса так называемых ГОСТ-подобних БШ предложен в [20] и развит в [21, 22], а позже и в [23]. Также в [23] впервые введено понятие обобщенно-марковского шифра и показано, что алгоритм ГОСТ обобщенно-марковский. Полученные в этих работах результаты обобщены и усилены в [24, 25]. Однако полностью использовать все возможности, связанные с индексом ветвления линейного оператора, так и не удалось. В частности, до сих пор остается вопрос, улучшится ли оценка практической стойкости этого алгоритма к разностному криптоанализу, если линейный оператор сдвига в раундовой функции заменить на оператор с большим индексом ветвления (у оператора сдвига этот индекс минимальный и равен двум).

В работе [26] на примере БШ «Калина» впервые получены результаты, показывающие, как использовать индекс ветвления линейного оператора для немарковского шифра при построении оценок практической стойкости к линейному и разностному криптоанализу.

Цель данной работы — обобщить и усилить результаты, полученные в [26], а также предложить более простые и удобные методы построения оценок практической стойкости к разностному криптоанализу обобщенно-марковских шифров с чередованием различных операций в ключевом сумматоре.

ОПРЕДЕЛЕНИЯ И ОБОЗНАЧЕНИЯ

Пусть $V_m = \{0,1\}^m$ — множество m-битных векторов, $(V_m, *)$ — абелева группа, $*$ — групповая операция, 0 — нейтральный элемент группы. Пусть преобразование $f_k(x) = f(x, k): V_m \times V_n \to V_m$ такое, что при фиксированном значении k преобразование $f_k(\cdot)$ — биекция.

Положим

$$d^f(x; \alpha, \beta) = 2^{-n} \sum_{k \in V_n} \delta(f_k(x * \alpha), f_k(x) * \beta). \qquad (1)$$

Определение 1. Преобразование $f_k(x)$ называется марковским (МП) относительно операции $*$, если $\forall x \in V_m, \forall \alpha, \beta \in V_m$:

$$d^f(x; \alpha, \beta) = 2^{-n} \sum_{k \in V_n} \delta(f_k(x * \alpha), f_k(x) * \beta), \qquad (2)$$

т.е. значение $d^f(x; \alpha, \beta)$ не зависит от x.

Определение 2. Преобразование $f_k(x)$ называется обобщенно-марковским (ОМП) относительно операции $*$, если $\forall x \in V_m\ \exists \pi_x: V_m \to V_m$ — биекция такая, что $\forall \alpha, \beta \in V_m$:

$$d^f(x; \alpha, \beta) = d^f(0; \pi_x(\alpha), \beta). \qquad (3)$$

ВСПОМОГАТЕЛЬНЫЕ РЕЗУЛЬТАТЫ

Рассмотрим r-раундовый шифр $E_K(x): V_m \to V_m$, $K = (k_r, k_{r-1}, \ldots, k_2, k_1)$, $k_i \in V_n$, $i = \overline{1, r}$. Пусть $f^{(0)}, f^{(1)}$ — раундовые функции, причем $f^{(0)}$ — МП относительно операции *, а $f^{(1)}$ — ОМП относительно операции *, и

$$E_k(x) = f_{k_r}^{(r \bmod 2)} \circ f_{k_{r-1}}^{(r-1 \bmod 2)} \circ \ldots \circ f_{k_2}^{(0)} \circ f_{k_1}^{(1)}(x). \qquad (4)$$

Теорема 1. Пусть $\Omega = (\omega_0, \omega_1, \ldots, \omega_r)$ — разностная характеристика шифра E, $\omega_i \in V_m$, $i = \overline{0, r}$. Тогда

$$EDP(\Omega) \le \max_{\alpha \in V_m \setminus \{0\}} \{ d^{f^{(1)}}(0; \alpha, \omega_1) \} \times$$

$$\times d^{f^{(0)}}(0; \omega_1, \omega_2) \times \max_{\alpha \in V_m \setminus \{0\}} \{ d^{f^{(1)}}(0; \alpha, \omega_3) \} \times \ldots$$

Доказательство. Для удобства рассмотрим четырехраундовый шифр E. Тогда $r = 4$, $\Omega = (\omega_0, \omega_1, \omega_2, \omega_3, \omega_4)$ — разностная характеристика шифра E.

Замечание. Если $EDP(\Omega) \ne 0$ и $\exists\, i = \overline{0, r} : \omega_i = 0$, то $\forall i = \overline{0, r} : \omega_i = 0$. Действительно, если $i > 0$, то

$$f_{k_i}^{(i \bmod 2)}(x_{i-1} * \omega_{i-1}) = f_{k_i}^{(i \bmod 2)}(x_{i-1}) * \omega_i = f_{k_i}^{(i \bmod 2)}(x_{i-1}).$$

Поскольку $f^{(i \bmod 2)}$ — биекция, то $x_{i-1} * \omega_{i-1} = x_{i-1}$, т.е. $\omega_{i-1} = 0$ и т.д.

Если $i < r$, то

$$f_{k_{i+1}}^{(i+1 \bmod 2)}(x_i * \omega_i) = f_{k_{i+1}}^{(i+1 \bmod 2)}(x_i) * \omega_{i+1} = f_{k_{i+1}}^{(i+1 \bmod 2)}(x_i),$$

откуда $\omega_{i+1} = 0$ и т.д.

По определению имеем

$$EDP(\Omega) = 2^{-m} \sum_{x_0 \in V_m} 2^{-nr} \sum_{K \in (V_n)^r} \prod_{i=1}^{r} \delta(f_{k_i}^{(i \bmod 2)}(x_{i-1} * \omega_{i-1}), f_{k_i}^{(i \bmod 2)}(x_{i-1}) * \omega_i) =$$

$$= 2^{-m} \sum_{x_0 \in V_m} 2^{-4n} \sum_{K \in (V_n)^4} \{ \delta(f_{k_1}^{(1)}(x_0 * \omega_0), f_{k_1}^{(1)}(x_0) * \omega_1) \times$$

$$\times \delta(f_{k_2}^{(0)}(x_1 * \omega_1), f_{k_2}^{(0)}(x_1) * \omega_2) \times \delta(f_{k_3}^{(1)}(x_2 * \omega_2), f_{k_3}^{(1)}(x_2) * \omega_3) \times$$

$$\times \delta(f_{k_4}^{(0)}(x_3 * \omega_3), f_{k_4}^{(0)}(x_3) * \omega_4) \},$$

где $x_i = f_{k_i}^{(i \bmod 2)}(x_{i-1})$, $i = \overline{1, 4}$. Отметим, что x_1, x_2, x_3 зависят от x_0 и ключей k_1, k_2, k_3, k_4.

Далее будем учитывать что $f^{(0)}$ — МП относительно операции *, а $f^{(1)}$ — ОМП относительно операции *. Для $\forall x \in V_m$, $\forall \alpha, \beta \in V_m \setminus \{0\}$ справедливы следующие выражения:

$$d^{f^{(0)}}(x; \alpha, \beta) = d^{f^{(0)}}(0; \alpha, \beta),$$

$$d^{f^{(1)}}(x; \alpha, \beta) = d^{f^{(1)}}(0; \pi_x(\alpha), \beta) \le \max_{\alpha \in V_m \setminus \{0\}} \{ d^{f^{(1)}}(0; \alpha, \beta) \}.$$

Учитывая, что $K = (k_4, k_3, k_2, k_1)$, получаем:

$$EDP(\Omega) = 2^{-m} \sum_{x_0 \in V_m} 2^{-3n} \sum_{k_1 \in V_n,\, k_2 \in V_n,\, k_3 \in V_n} \Bigg\{ \delta(f_{k_1}^{(1)}(x_0 * \omega_0), f_{k_1}^{(1)}(x_0) * \omega_1) \times$$

$$\times \delta(f_{k_2}^{(0)}(x_1 * \omega_1), f_{k_2}^{(0)}(x_1) * \omega_2) \times \delta(f_{k_3}^{(1)}(x_2 * \omega_2), f_{k_3}^{(1)}(x_2) * \omega_3) \times$$

$$\times \left(2^{-n} \sum_{k_4 \in V_n} \delta(f_{k_4}^{(0)}(x_3 * \omega_3), f_{k_4}^{(0)}(x_3) * \omega_4) \right) \Bigg\} =$$

$$= 2^{-m} \sum_{x_0 \in V_m} 2^{-3n} \sum_{k_1 \in V_n,\, k_2 \in V_n,\, k_3 \in V_n} \{\delta(f_{k_1}^{(1)}(x_0 * \omega_0),\, f_{k_1}^{(1)}(x_0) * \omega_1) \times$$

$$\times\, \delta(f_{k_2}^{(0)}(x_1 * \omega_1),\, f_{k_2}^{(0)}(x_1) * \omega_2) \times \delta(f_{k_3}^{(1)}(x_2 * \omega_2),\, f_{k_3}^{(1)}(x_2) * \omega_3) \times$$

$$\times\, d^{f^{(0)}}(0; \omega_3, \omega_4)\}.$$

Последний множитель в фигурных скобках не зависит от x_0 и ключей k_1, k_2, k_3, поэтому его можно вынести за знаки суммирования и перейти к следующему множителю:

$$EDP(\Omega) = d^{f^{(0)}}(0; \omega_3, \omega_4) \cdot 2^{-m} \sum_{x_0 \in V_m} 2^{-2n} \sum_{k_1 \in V_n,\; k_2 \in V_n} \left\{ \delta(f_{k_1}^{(1)}(x_0 * \omega_0),\, f_{k_1}^{(1)}(x_0) * \omega_1) \times \right.$$

$$\left. \times\, \delta(f_{k_2}^{(0)}(x_1 * \omega_1),\, f_{k_2}^{(0)}(x_1) * \omega_2) \times \left(2^{-n} \sum_{k_3 \in V_n} \delta(f_{k_3}^{(1)}(x_2 * \omega_2),\, f_{k_3}^{(1)}(x_2) * \omega_3) \right) \right\} \le$$

$$\le d^{f^{(0)}}(0; \omega_3, \omega_4) \cdot 2^{-m} \sum_{x_0 \in V_m} 2^{-2n} \sum_{k_1 \in V_n,\, k_2 \in V_n} \{\delta(f_{k_1}^{(1)}(x_0 * \omega_0),\, f_{k_1}^{(1)}(x_0) * \omega_1) \times$$

$$\times\, \delta(f_{k_2}^{(0)}(x_1 * \omega_2),\, f_{k_2}^{(0)}(x_1) * \omega_2) \max_{\alpha \in V_m \setminus \{0\}} \{d^{f^{(1)}}(0; \alpha, \omega_3)\}\}.$$

Также следует, что последний множитель в фигурных скобках не зависит от x_0 и ключей k_1, k_2, поэтому его можно вынести за знаки суммирования:

$$EDP(\Omega) \le \max_{\alpha \in V_m \setminus \{0\}} \{d^{f^{(1)}}(0; \alpha, \omega_3)\} \cdot d^{f^{(0)}}(0; \omega_3, \omega_4) \times$$

$$\times\, 2^{-m} \sum_{x_0 \in V_m} 2^{-2n} \sum_{k_1 \in V_n} \left\{ \delta(f_{k_1}^{(1)}(x_0 * \omega_0),\, f_{k_1}^{(1)}(x_0) * \omega_1) \times \right.$$

$$\left. \times \left(2^{-n} \sum_{k_2 \in V_n} \delta(f_{k_2}^{(0)}(x_1 * \omega_1),\, f_{k_2}^{(0)}(x_1) * \omega_2) \right) \right\}.$$

Аналогично для оставшихся множителей окончательно получим

$$EDP(\Omega) \le \max_{\alpha \in V_m \setminus \{0\}} \{d^{f^{(1)}}(0; \alpha, \omega_1)\} \cdot d^{f^{(0)}}(0; \omega_1, \omega_2) \times$$

$$\times \max_{\alpha \in V_m \setminus \{0\}} \{d^{f^{(1)}}(0; \alpha, \omega_3)\} \cdot d^{f^{(0)}}(0; \omega_3, \omega_4).$$

Для других значений r доказательство аналогичное.

Лемма 1. Пусть $f_k(x) = f(x * k)$. Тогда $f_k(x)$ МП относительно операции *.

Доказательство. В данных обозначениях

$$d^f(x; \alpha, \beta) = 2^{-n} \sum_{k \in V_n} \delta(f((x * \alpha) * k),\, f(x * k) * \beta) =$$

$$= 2^{-n} \sum_{k \in V_n} \delta(f(\alpha * (x * k),\, f(x * k) * \beta).$$

Сделаем замену переменных: $t = x * k$, тогда

$$d^f(x; \alpha, \beta) = 2^{-n} \sum_{t \in V_n} \delta(f(\alpha * t),\, f(t) * \beta) = d^f(0; \alpha, \beta),$$

что завершает доказательство леммы.

Лемма 2. Пусть $f_k(x) = f(x \otimes k)$, где $(V_m, \otimes)$ — абелева группа, причем ее нейтральный элемент совпадает с нейтральным элементом абелевой группы $(V_m, *)$. Тогда $f_k(x)$ — ОМП относительно операции $\otimes$.

Доказательство. Пусть

$$d^f(x;\alpha,\beta)=2^{-n}\sum_{k\in V_n}\delta(f((x*\alpha)\otimes k),\, f(x\otimes k)*\beta)=$$

$$=2^{-n}\sum_{k\in V_n}\delta(f(((x*\alpha)\otimes x^{-1})\otimes(x\otimes k)),\, f(x\otimes k)*\beta),$$

где x^{-1} — обратный элемент в группе $(V_m,\otimes)$. Выполним замену переменных: $t=x\otimes k$, и положим $\pi_x(\alpha)=(x*\alpha)\otimes x^{-1}$, тогда

$$d^f(x;\alpha,\beta)=2^{-n}\sum_{t\in V_n}\delta(f(\pi_x(\alpha)\otimes t),\, f(t)*\beta)=d^f(0;\pi_x(\alpha),\beta),$$

что завершает доказательство леммы.

Замечание 1. В лемме 2 для $\forall x\in V_m$ отображение $\pi_x: V_m\to V_m$, $\pi_x(\alpha)=(x*\alpha)\otimes x^{-1}$, где $\alpha\in V_m$, является биекцией. Действительно, для $\forall\alpha_1,\alpha_2\in V_m$ таких, что $\pi_x(\alpha_1)=\pi_x(\alpha_2)$, выполняется $(x*\alpha_1)\otimes x^{-1}=$ $=(x*\alpha_2)\otimes x^{-1}$, что равносильно $\alpha_1=\alpha_2$, а для $\forall\beta\in V_m$ существует $\alpha=x_*^{-1}*(\beta\otimes x)\in V_m$, где x_*^{-1} — обратный элемент в группе $(V_m,*)$, такое, что

$$\pi_x(\alpha)=(x*(x_*^{-1}*(\beta\otimes x)))\otimes x^{-1}=((x*x_*^{-1})*(\beta\otimes x))\otimes x^{-1}=\beta.$$

Далее предположим, что $V_m=(V_t)^p$ $(m=p\cdot t)$, а операции * и $\otimes$ допускают представления соответствующими операциями на V_t следующим образом:

$$x*y=(x^{(p)}*_t y^{(p)},\ldots,x^{(2)}*_t y^{(2)},x^{(1)}*_t y^{(1)}),$$

$$x\otimes y=(x^{(p)}\otimes_t y^{(p)}\otimes_t \nu_{p-1},\ldots,x^{(2)}\otimes_t y^{(2)}\otimes_t \nu_1, x^{(1)}\otimes_t y^{(1)}),$$

где $\nu_j=\nu_j(x^{(j)},y^{(j)},\ldots,x^{(1)},y^{(1)})\in V_t$, $j=\overline{1,\,p-1}$.

Замечание 2. Примером операции $*$ может быть побитовое сложение, а примером операции $\otimes$ — сложение по модулю 2^m, тогда ν_j, $j=\overline{1,\,p-1}$, — это биты переноса:

$$\nu_j=\begin{cases}0, & 2^{(j-1)\cdot t}\cdot(x^{(j)}+y^{(j)})+\ldots+(x^{(1)}+y^{(1)})<2^{j\cdot t},\\ 1, & 2^{(j-1)\cdot t}\cdot(x^{(j)}+y^{(j)})+\ldots+(x^{(1)}+y^{(1)})\ge 2^{j\cdot t}.\end{cases}$$

Также предположим, что

$$f_k^{(0)}(x)=A(S(x*k)),\tag{5}$$

$$f_k^{(1)}(x)=A(S(x\otimes k)).\tag{6}$$

где $A:(V_t)^p\to(V_t)^p$ — невырожденное линейное преобразование относительно операции $*$, $S(x)=(s^{(p)}(x^{(p)}),s^{(p-1)}(x^{(p-1)}),\ldots,s^{(1)}(x^{(1)}))$, $s^{(j)}:V_t\to V_t$ — блок подстановки (биективный), $x^{(j)}\in V_t$, $j=\overline{1,\,p}$.

Согласно лемме 1 преобразование $f_k^{(0)}$ — МП относительно операции $*$, а согласно лемме 2 преобразование $f_k^{(1)}$ — ОМП относительно операции $*$.

Определение 3. Весом Хемминга вектора $x=(x^{(p)},x^{(p-1)},\ldots,x^{(1)})\in$ $\in(V_t)^p=V_m$ называется величина

$$w_h(x)=\#\{x^{(j)}\ne 0\mid j=\overline{1,\,p}\}.$$

Определение 4. Индексом ветвления линейного преобразования $A:(V_t)^p\to(V_t)^p$ называется величина

$$B(A)=\min_{x\in(V_t)^p\setminus\{0\}}\{w_h(x)+w_h(A^{-1}(x))\}.$$

Для $\alpha, \beta \in V_t$ введем обозначения:

$$d_{*}^{s^{(j)}}(\alpha, \beta) = 2^{-t} \sum_{k^{(j)} \in V_t} \delta(s^{(j)}(\alpha *_t k^{(j)}), \beta *_t s^{(j)}(k^{(j)})),$$

$$d_{\otimes}^{s^{(j)}}(\alpha, \beta) = 2^{-t} \sum_{k^{(j)} \in V_t} \delta(s^{(j)}(\alpha \otimes_t k^{(j)}), \beta *_t s^{(j)}(k^{(j)})).$$

$$\Delta_{*} = \max \{ d_{*}^{s^{(j)}}(\alpha, \beta) \mid \alpha, \beta \in V_t \setminus \{0\},\ j = \overline{1, p} \},$$

$$\Delta_{\otimes} = \max \{ d_{\otimes}^{s^{(j)}}(\alpha, \beta) \mid \alpha, \beta \in V_t \setminus \{0\},\ j = \overline{1, p} \},$$

$$\Delta = \max \{\Delta_{*}, \Delta_{\otimes}\}.$$

ОСНОВНЫЕ РЕЗУЛЬТАТЫ

Теорема 2. Рассмотрим блочный шифр вида (4) с раундовыми преобразованиями вида (5) и (6). Тогда $EDP(\Omega) \le \Delta^{\left[\frac{r}{2}\right] \cdot B(A)}$.

Доказательство. Рассмотрим двухраундовый шифр $D_K(x) = f_{k_2}^{(0)} \circ f_{k_1}^{(1)}(x)$, $K = (k_2, k_1)$ и двухраундовую разностную характеристику $\Omega_2 = (\omega_0, \omega_1, \omega_2)$. По теореме 1 справедлива оценка

$$EDP(\Omega_2) \le \max_{\alpha \in V_m \setminus \{0\}} \{ d^{f^{(1)}}(0; \alpha, \omega_1) \} \cdot d^{f^{(0)}}(0; \omega_1, \omega_2).$$

Далее,

$$d^{f^{(1)}}(0; \alpha, \omega_1) = 2^{-n} \sum_{k \in V_n} \delta(A(S(\alpha \otimes k)), \omega_1 * A(S(k))) =$$

$$= 2^{-n} \sum_{k \in V_n} \delta(S(\alpha \otimes k), A^{-1}(\omega_1) * S(k)).$$

Обозначим

$$k = (k^{(p)}, \ldots, k^{(1)}),\ \alpha = (\alpha^{(p)}, \ldots, \alpha^{(1)}),\ A^{-1}(\omega_1) = \gamma_1 = (\gamma_1^{(p)}, \ldots, \gamma_1^{(1)}).$$

$$d^{f^{(1)}}(0; \alpha, \omega_1) =$$

$$= 2^{-tp} \sum_{(k^{(p)}, \ldots, k^{(1)}) \in (V_t)^p} \delta(s^{(p)}(\alpha^{(p)} \otimes_t k^{(p)} \otimes_t \nu_{p-1}), \gamma_1^{(p)} *_t s^{(p)}(k^{(p)})) \times \ldots$$

$$\ldots \times \delta(s^{(1)}(\alpha^{(1)} \otimes_t k^{(1)}), \gamma_1^{(1)} *_t s^{(1)}(k^{(1)})) \le$$

$$\le \prod_{1 \le j \le p \,:\, \gamma_1^{(j)} \ne 0} d_{\otimes}^{s^{(j)}}(\tilde{\alpha}^{(j)}, \gamma_1^{(j)}) \le (\Delta_{\otimes})^l,$$

где $\tilde{\alpha}^{(j)} = \alpha^{(j)} \otimes_t \nu_{j-1}$, $j = \overline{1, p}$, $\nu_0 = 0$, l — количество ненулевых компонент в $\gamma_1 \in (V_t)^p$, т.е. $l = w_h(\gamma_1) = w_h(A^{-1}(\omega_1))$.

Аналогично для $d^{f^{(0)}}(0; \omega_1, \omega_2)$ справедливо равенство

$$d^{f^{(0)}}(0; \omega_1, \omega_2) = 2^{-n} \sum_{k \in V_n} \delta(A(S(\omega_1 * k)), \omega_2 * A(S(k))) =$$

$$= 2^{-n} \sum_{k \in V_n} \delta(S(\omega_1 * k), A^{-1}(\omega_2) * S(k)).$$

Положим $\omega_1 = (\omega_1^{(p)}, \ldots, \omega_1^{(1)})$, $A^{-1}(\omega_2) = \gamma_2 = (\gamma_2^{(p)}, \ldots, \gamma_2^{(1)})$. Тогда

$$d^{f^{(0)}}(0; \omega_1, \omega_2) = 2^{-tp} \sum_{(k^{(p)}, \ldots, k^{(1)}) \in (V_t)^p} \delta(s^{(p)}(\omega_1^{(p)} *_t k^{(p)}), \gamma_2^{(p)} *_t s^{(p)}(k^{(p)})) \times \ldots$$

$$\ldots \times \delta(s^{(1)}(\omega_1^{(1)} *_t k^{(1)}), \gamma_2^{(1)} *_t s^{(1)}(k^{(1)})) \le \prod_{1 \le j \le p:\, \gamma_1^{(j)} \ne 0} d_*^{s^{(j)}}(\omega_1^{(j)}, \gamma_2^{(j)}) \le (\Delta_*)^u,$$

где u — количество ненулевых компонент в $\gamma_2 \in (V_t)^p$, т.е. $l = w_h(\gamma_2) = w_h(A^{-1}(\omega_2))$. Отметим, что $w_h(A^{-1}(\omega_2)) = w_h(\omega_1)$, поскольку операция * и действие блока подстановки переводят ненулевые разности в ненулевые. Тогда

$$EDP(\Omega_2) \le \max_{\alpha \in V_m \setminus \{0\}} d^{f^{(1)}}(0; \alpha, \omega_1) \cdot d^{f^{(0)}}(0; \omega_1, \omega_2) \le (\max\{\Delta_*, \Delta_\otimes\})^{l+u} =$$

$$= \Delta^{w_h(A^{-1}(\omega_1)) + w_h(\omega_1)} \le \Delta^{B(A)}.$$

Таким образом, для двухраундового шифра $D_K(x)$ справедливо неравенство

$$EDP(\Omega_2) \le \Delta^{B(A)}. \qquad (7)$$

Теперь перейдем к r-раундовому шифру (4). Для каждой пары раундов можно воспользоваться оценкой (7), а поскольку шифр содержит $\left[\frac{r}{2}\right]$ соответствующих пар раундов, то получаем оценку

$$EDP(\Omega) \le \Delta^{\left[\frac{r}{2}\right] \cdot B(A)}.$$

Теорема доказана.

ПРАКТИЧЕСКОЕ ПРИМЕНЕНИЕ

Частным случаем применения результата теоремы 2 можно считать оценку практической стойкости блочного шифра «Калина» к разностному криптоанализу, полученную в работе [26]. В этом случае соответствующие параметры имеют такие значения:

$$m = 128, \ p = 16, \ t = 8, \ r = 10, \ B(A) = 9, \ \Delta = 2^{-5},$$

а операции * и $\otimes$ — это операции побитового сложения и сложения по модулю 2^{32} соответственно. Тогда получаем следующую оценку для средней вероятности разностной характеристики: $\Omega = (\omega_0, \omega_1, \ldots, \omega_{10}) \in (V_m \setminus \{0\})^{11}$: $EDP(\Omega) \le 2^{-230}$.

ЗАКЛЮЧЕНИЕ

В данной работе предложен метод, позволяющий использовать индекс ветвления линейного оператора при построении верхних оценок средних вероятностей разностных характеристик немарковских блочных шифров, в раундах которых чередуются марковские и обобщенно-марковские преобразования. Существенным также является то, что в раундах с марковским преобразованием операция, реализованная в ключевом сумматоре, сохраняет количество ненулевых компонент во входной и выходной разности (т.е. отсутствует бит переноса между отдельными компонентами входных и выходных векторов). Предметом дальнейших исследований может быть обобщение этих результатов на случай, когда преобразования во всех раундах являются обобщенно марковскими (или просто немарковскими), а операция в ключевом сумматоре не сохраняет количество ненулевых компонент.

СПИСОК ЛИТЕРАТУРЫ

1. Matsui M. Linear cryptanalysis methods for DES cipher // Advances in Cryptology. — EUROCRYPT'93, Proceedings. — Berlin: Springer-Verlag, 1994. — P. 386–397.
2. Biham E., Shamir A. Differential cryptanalysis of DES-like cryptosystems // J. of Cryptology. — 1991. — **4**, N 1. — P. 3–72.
3. Biham E., Shamir A. Differential cryptanalysis of the full 16-round DES // Advances in Cryptology — CRYPTO'92, Proceedings. — Berlin: Springer-Verlag, 1993. — P. 487–496.
4. Matsui M. The first experimental cryptanalysis of the data encryption standard // Advances in Cryptology — CRYPTO'94. — Berlin: Springer-Verlag, 1994. — P. 1–11.

5. Lai X., Massey J.L., Murphy S. Markov ciphers and differential cryptanalysis // Advances in Cryptology — EUROCRYPT'91, Proceedings. — Berlin: Springer-Verlag, 1991. — P. 17–38.
6. FIPS PUB 46-3. Data Encryption Standard (DES). Federal Information Processing Standard, National Institute of Standards and Technology, U.S. Dept. of Commerce, 1999 October 25.
7. FIPS-197. Advanced Encryption Standard (AES). Federal Information Processing Standard, National Institute of Standards and Technology, U.S. Dept. of Commerce, November 26, 2001.
8. Vaudenay S. On the security of CS-cipher // Fast Software Encryption. — FSE'99, Proceedings. — Berlin: Springer-Verlag, 1999. — P. 260–274.
9. Biryukov A. Block ciphers and stream ciphers: the state of the art. — http://eprint.iacr.org/2004/094.
10. Vaudenay S. Decorrelation: a theory for block cipher security // J. of Cryptology. — 2003. — **16**, N 4. — P. 249–286.
11. Daemen J. Cipher and hash function design strategies based on linear and differential cryptanalysis. — Doctoral Dissertation, 1995.
12. Daemen J., Rijmen V. Statistics of correlation and differentials in block ciphers. — http://eprint.iacr.org/2005/212.
13. A strategy for constructing fast raund functions with practical security against differential and linear cryptanalysis / M. Kanda, Y. Takashima, T. Matsumoto et al. // Selected Areas in Cryptography. — SAC 1998, Proceedings. — Berlin: Springer-Verlag, 1999. — P. 264–279.
14. Kanda M. Practical security evaluation against differential and linear cryptanalyses for Feistel ciphers with SPN round function // Selected Areas in Cryptography. — SAC 2000, Proceedings. — Berlin: Springer-Verlag, 2001. — P. 324–338.
15. Системы обработки информации. Защита криптографическая. Алгоритмы криптографического преобразования: ДСТУ ГОСТ 28147:2009. — Чинний від 2009-02-01. — К.: Держспоживстандарт України, 2008. — 28 с. — (Національний стандарт України).
16. Горбенко І.Д., Долгов В.І. та ін. Перспективний блоковий симетричний шифр «Калина» — основні положення та специфікація // Прикладная радиоэлектроника. — 2007. — **6**, № 2. — С. 195–208.
17. Seki H., Toshinobu K. Differential cryptanalysis of redused round of GOST // Selected Areas in Cryptography. — SAC 2000, Proceedings. — Berlin: Springer-Verlag, 2001. — P. 315–323.
18. 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.
19. Олейников Р.В. Дифференциальный криптоанализ алгоритма шифрования ГОСТ 28147-89 // Там же. — 2001. — Вып. 119. — С. 146–152.
20. 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. — **12** (28), N 1, 2. — P. 20–32.
21. Скрыпник Л.В., Ковальчук Л.В. Верхние границы средних вероятностей дифференциалов булевых отображений // Захист інформації. — 2006. — № 3. — С. 7–12.
22. Алексейчук А.Н. Верхние границы параметров, характеризующих стойкость немарковских блочных шифров относительно методов разностного и линейного криптоанализа // Там же. — 2006. — № 3. — С. 20–28.
23. Ковальчук Л.В. Обобщенные марковские шифры: построение оценки практической стойкости относительно дифференциального криптоанализа // Математика и безопасность информационных технологий. Материалы конф. в МГУ 25–27 октября 2006 г. — М.: МЦНМО, 2007. — С. 595–599.
24. Олексійчук А.Н., Ковальчук Л.В., Пальченко С.В. Криптографічні параметри вузлів заміни, що характеризують стійкість ГОСТ-подібних блокових шифрів відносно методів лінійного та різницевого криптоаналізу // Захист інформації. — 2007. — № 2. — С. 12–23.
25. Alekseychuk A.N., Kovalchuk L.V. Towards a theory of security evaluation for GOST-like ciphers against differential and linear cryptanalysis: Prepr. 9 Sep 2011. — http://eprint.iacr.org/2011/489.
26. Алексейчук А.Н., Ковальчук Л.В., Скрынник Е.В., Шевцов А.С. Оценки практической стойкости блочного шифра «Калина» относительно методов разностного, линейного криптоанализа и алгебраических атак, основанных на гомоморфизмах // Прикладная радиоэлектроника. — 2008. — **7**, № 3. — С. 203–209.

Поступила 02.07.2013