УДК 621.391:519.2:519.7

Л.В. КОВАЛЬЧУК

ПОСТРОЕНИЕ ВЕРХНИХ ОЦЕНОК СРЕДНИХ ВЕРОЯТНОСТЕЙ ЦЕЛОЧИСЛЕННЫХ ДИФФЕРЕНЦИАЛОВ КОМПОЗИЦИИ КЛЮЧЕВОГО СУММАТОРА, БЛОКА ПОДСТАНОВКИ И ОПЕРАТОРА СДВИГА

Ключевые слова: *немарковские блоковые шифры, целочисленный разностный криптоанализ*.

ВВЕДЕНИЕ

Большинство современных блоковых шифров (AES [1], ГОСТ 28147 [2], «Калина» [3], «Мухомор» [4]) содержат в структуре композицию ключевого сумматора, блока подстановки и оператора перестановки, линейного над полем F_2 или его некоторым расширением. Поэтому задача оценивания стойкости шифров к линейному, билинейному и различным модификациям разностного криптоанализа [5–11] или сводится к задаче построения верхних оценок средних вероятностей таких композиций, или содержит ее как подзадачу. Последняя полностью решена в следующих случаях:

— если в ключевом сумматоре реализована операция побитового сложения и при этом входные и выходные разности в раундовом дифференциале рассматриваются относительно этой же операции (см. библиографию, приведенную в работах [5, 7]);

— если в ключевом сумматоре реализована операция сложения по модулю 2^n, а входные и выходные разности в раундовом дифференциале рассматриваются относительно операции побитового сложения [5–10];

— если в ключевом сумматоре реализована операция сложения по модулю 2^n, входные и выходные разности рассматриваются относительно этой же операции (такой дифференциал называют целочисленным [12, 13]) и при этом либо отсутствует оператор перестановки [6], либо отсутствует блок подстановки и оператор перестановки является оператором циклического сдвига [14].

Вопрос о построении верхних оценок средних вероятностей целочисленных дифференциалов остается открытым в случае нетривиальных блока подстановки и оператора перестановки. Заметим, что аналитические сложности, возникающие в этом случае в связи с наличием бита переноса при модульном сложении, усиливаются тем, что оператор перестановки не является линейным относительно этой операции. Данная задача решена в настоящей работе для случая, когда в ключевом сумматоре реализована либо операция побитового сложения, либо операция сложения по модулю 2^n, блок подстановки произвольный, а оператор перестановки — оператор циклического сдвига.

В [12, 14], подобно данной работе, предлагается для построения высоковероятной характеристики хеш-функции MD5 использовать целочисленные дифференциалы, т.е. такие, в которых разностной операцией является операция сложения по модулю 2^n. Такой выбор операции объясняется тем, что хеш-функция MD5 содержит много преобразований, линейных относительно этой операции. В [14] удалось найти большое количество высоковероятных дифференциалов (вероятность которых не менее $1/4$) для отображений, являющихся композицией сумматора по модулю 2^n и оператора сдвига. Целочисленные дифференциалы использовались как для криптоанализа, так и для построения коллизий хеш-функций и во многих других работах; достаточно полный перечень ссылок, а также обоснование использования именно целочисленных дифференциалов можно найти в [12]. Настоящая работа, в которой рассматривается более сложная композиция преобразований, носит альтернативный характер: ее цель — построение верхних (а не нижних) оценок для средних вероятностей целочисленных дифференциалов отображений, являющихся

композициями ключевого сумматора, блока подстановки и оператора сдвига, а также определение параметров s-блоков, от которых зависят данные оценки, и условий, обеспечивающих как можно меньшее значение этих оценок.

ВСПОМОГАТЕЛЬНЫЕ РЕЗУЛЬТАТЫ

Введем следующие обозначения. Для любого $n \in N$ обозначим $V_n = \{0,1\}^n$ множество n-мерных битовых векторов. Здесь и далее векторам из V_n ставятся в соответствие целые числа от 0 до $2^n - 1$, $n \in N$.

Если $n = pu$, $p \geq 2$, то любой $x \in V_n$ можно представить в виде $x = (x^{(p)}, \ldots, x^{(1)})$, $x^{(i)} \in V_u$, $i = \overline{1, p}$.

На множестве V_n введем следующие операции и отображения. Для произвольных $a, b \in V_n$ обозначим $a \oplus b$ результат побитового сложения векторов a и b, а $a + b$ $(a - b)$ — соответственно результат сложения (вычитания) целых чисел по модулю 2^n.

Обозначим $L_m : V_n \to V_n$ отображение сдвига влево на m бит вектора из V_n. На множестве V_n определим подмножества:

$$\Gamma_m(\gamma) = \{\beta \in V_n \mid \exists\, k \in V_n : L_m(k + \gamma) - L_m(k) = \beta\};$$
$$\Gamma_m^{-1}(\beta) = \{\gamma \in V_n \mid \exists\, k \in V_n : L_m(k + \gamma) - L_m(k) = \beta\}.$$

Биективное отображение $S : V_n \to V_n$ зададим следующим образом:

$$\forall x \in V_n : S(x) = (s^{(p)}(x^{(p)}), \ldots, s^{(1)}(x^{(1)})), x^{(i)} \in V_u,\ i = \overline{1, p},$$

где $s^{(i)} : V_u \to V_u$, $i = \overline{1, p}$, — биективные отображения. Введенное отображение часто называют блоком подстановки, а отображения $s^{(i)}$ — s-блоками.

Для произвольной функции $F : V_n \times V_n \to V_n$ обозначим $F_k(x) := F(k, x)$, $k, x \in V_n$. В данной работе рассматриваются раундовые функции, которые являются композицией ключевого сумматора, блока подстановки и оператора сдвига:

$$F_k(x) = L_m(S(x + k)) \tag{1}$$

или

$$G_k(x) = L_m(S(x \oplus k)). \tag{2}$$

Согласно [7] средние вероятности целочисленных раундовых дифференциалов для функций (1), (2) имеют следующий вид:

$$d_+^F(x; \alpha, \beta) = 2^{-n} \sum_{k \in V_n} \delta(F_k(x + \alpha) - F_k(x), \beta) =$$
$$= 2^{-n} \sum_{k \in V_n} \delta(L_m(S(x + k + \alpha)) - L_m(S(x + k)), \beta) \tag{3}$$

— средняя (по ключам) вероятность дифференциала отображения F в точке x,

$$d_+^F(\alpha, \beta) = 2^{-2n} \sum_{x, k \in V_n} \delta(F_k(x + \alpha) - F_k(x), \beta) =$$
$$= 2^{-2n} \sum_{x, k \in V_n} \delta(L_m(S(x + k + \alpha)) - L_m(S(x + k)), \beta) \tag{4}$$

— средняя (по ключам) вероятность дифференциала отображения F, а также

$$d_+^G(x; \alpha, \beta) = 2^{-n} \sum_{k \in V_n} \delta(L_m(S((x + \alpha) \oplus k)) - L_m(S(x \oplus k)), \beta),$$
$$d_+^G(\alpha, \beta) = 2^{-2n} \sum_{x, k \in V_n} \delta(L_m(S((x + \alpha) \oplus k)) - L_m(S(x \oplus k)), \beta), \tag{5}$$

в зависимости от операции, реализованной в ключевом сумматоре. Заметим, что выражение (4) совпадает с выражением (3) при любом $x \in V_n$, в частности при $x = 0$, что доказывается путем тривиальной замены переменной.

Введем две величины, зависящие от первого s-блока в блоке подстановки:

$$\delta_{+}^{s^{(1)}} = \max_{a,b\in\{0,1\}} \max_{\alpha,\gamma\in V_u\setminus\{0\}} 2^{-u} \sum_{\substack{k\in V_u:\\ \nu(k,\alpha)=a,\\ \tau(k,\alpha)=b}} \delta(s^{(1)}(k+\alpha)-s^{(1)}(k),\gamma), \tag{6}$$

где

$$\nu(k,\alpha)=\begin{cases}0, \text{ если } 0\le k+\alpha<2^u,\\ 1 \text{ в противном случае;}\end{cases} \quad \tau(k,\alpha)=\begin{cases}0, \text{ если } s^{(1)}(k+\alpha)\ge s^{(1)}(k),\\ 1 \text{ в противном случае;}\end{cases} \tag{7}$$

$$\delta_{\oplus,+}^{s^{(1)}} = \max_{a\in\{0,1\}} \max_{\alpha,\gamma\in V_u\setminus\{0\}} 2^{-u} \sum_{\substack{k\in V_u:\\ \tau(k,\alpha)=a}} \delta(s^{(1)}(k\oplus\alpha)-s^{(1)}(k),\gamma). \tag{8}$$

Для произвольного $j=\overline{2,p}$ положим

$$d_{+}^{s^{(j)}} = \max_{\alpha,\beta\in V_u\setminus\{0\}} 2^{-u} \sum_{k\in V_u} \delta(s^{(j)}(k+\alpha)-s^{(j)}(k),\beta), \tag{9}$$

$$d_{\oplus,+}^{s^{(j)}} = \max_{\alpha,\beta\in V_u\setminus\{0\}} 2^{-u} \sum_{k\in V_u} \delta(s^{(j)}(k\oplus\alpha)-s^{(j)}(k),\beta), \tag{10}$$

$$\Delta_{+} = \max_{j=\overline{2,p}} d_{+}^{s^{(j)}}, \quad \Delta_{\oplus,+} = \max_{j=\overline{2,p}} d_{\oplus,+}^{s^{(j)}}.$$

Сформулируем вспомогательные результаты, которые будут использоваться при получении основного результата работы. Следующие леммы получены с применением теоремы 3 из [14] и результатов, представленных в [5–11].

Лемма 1. Для $\forall m\in N$, $\forall\beta\in V_n$, $\beta=q2^t+r$, где $0\le r<2^t-1$, $0\le q<2^m-1$, выполняется соотношение между множествами

$$\Gamma_m^{-1}(\beta)=\Gamma_{n-m}(\beta)\subset\{\gamma,\gamma+1,\gamma-2^t,\gamma-2^t+1\},$$

где $\gamma=\gamma(\beta)=q+r2^t=q+\beta 2^t$. В частности, $|\Gamma_m^{-1}(\beta)|\le 4$.

Доказательство леммы использует тот факт, что $L_m^{-1}(x)=L_{n-m}(x)$. Оно достаточно простое и здесь не приводится.

Лемма 2. Пусть функции F,G определены в соответствии с (1), (2). Тогда для произвольного $\beta\in V_n\setminus\{0\}$ справедливы неравенства

$$\forall\alpha\in V_n\setminus\{0\}\ d_{+}^{F}(\alpha,\beta)\le \sum_{\gamma\in\Gamma_m^{-1}(\beta)} d_{+}^{S}(0;\alpha,\gamma), \tag{11}$$

$$\max_{\alpha\in V_n\setminus\{0\}} d_{+}^{G}(\alpha,\beta)\le \max_{\alpha\in V_n\setminus\{0\}} \sum_{\gamma\in\Gamma_m^{-1}(\beta)} d_{\oplus,+}^{S}(0;\alpha,\gamma), \tag{12}$$

где

$$d_{+}^{S}(0;\alpha,\gamma)=2^{-n}\sum_{k\in V_n}\delta(S(k+\alpha)-S(k),\beta),$$

$$d_{\oplus,+}^{S}(0;\alpha,\gamma)=2^{-n}\sum_{k\in V_n}\delta(S(k\oplus\alpha)-S(k),\beta).$$

Доказательство. Сначала докажем неравенство (11). По определению

$$d_{+}^{F}(\alpha,\beta)=2^{-2n}\sum_{x,k\in V_n}\delta(F_k(x+\alpha)-F_k(x),\beta)=$$
$$=2^{-2n}\sum_{x,k\in V_n}\delta(L_m\circ S(x+k+\alpha)-L_m\circ S(x+k),\beta).$$

После выполнения замены переменной $x+k$ на k получаем

$$d_+^F(\alpha,\beta)=2^{-n}\sum_{k\in V_n}\delta(L_m\circ S(k+\alpha)-L_m\circ S(k),\beta)=$$

$$=2^{-n}\sum_{k\in V_n}\left\{\sum_{\gamma\in V_n}\delta(L_m(S(k)+\gamma)-L_m(S(k)),\beta)\delta(S(k+\alpha)-S(k),\gamma)\right\}=$$

$$=2^{-n}\sum_{k\in V_n}\left\{\sum_{\gamma\in\Gamma_m^{-1}(\beta)}\delta(L_m(S(k)+\gamma)-L_m(S(k)),\beta)\delta(S(k+\alpha)-S(k),\gamma)\right\}\le$$

$$\le 2^{-n}\sum_{k\in V_n}\sum_{\gamma\in\Gamma_m^{-1}(\beta)}\delta(S(k+\alpha)-S(k),\gamma)=\sum_{\gamma\in\Gamma_m^{-1}(\beta)}d_+^S(0;\alpha,\gamma),$$

поскольку $\delta(L_m(S(k)+\gamma)-L_m(S(k)),\beta)\le 1$. Неравенство (11) доказано.

Докажем неравенство (12). По определению

$$d_+^G(\alpha,\beta)=2^{-2n}\sum_{x,\,k\in V_n}\delta(L_m(S((x+\alpha)\oplus k))-L_m(S(x\oplus k)),\beta).$$

Зафиксируем произвольное $x\in V_m$ и выполним преобразования

$$d_+^G(x;\alpha,\beta)=2^{-n}\sum_{k\in V_n}\delta(L_m(S((x+\alpha)\oplus k))-L_m(S(x\oplus k)),\beta)=$$

$$=2^{-n}\sum_{k\in V_n}\delta(L_m(S(x\oplus\alpha\oplus\mu(x,\alpha)\oplus k))-L_m(S(x\oplus k)),\beta),\qquad(13)$$

где $\mu(x,\alpha)=(x+\alpha)\oplus x\oplus\alpha$. Выполним замены переменных: $x\oplus k=k'$, $\alpha\oplus\mu(x,\alpha)=$ $=\alpha'=\alpha'(x,\alpha)$ и опять заменим k' на k. Тогда выражение (13) примет вид

$$d_+^G(x;\alpha,\beta)=2^{-n}\sum_{k\in V_n}\delta(L_m(S(k\oplus\alpha'))-L_m(S(k)),\beta)=d_{\oplus,+}^G(0;\alpha',\beta).$$

Заметим, что отображение $\pi_x:V_n\to V_n$, $\pi_x(\alpha)=\alpha'$, является биекцией на V_n, причем $\pi(0)=0$. Действительно, если $\pi_x(\alpha_1)=\pi_x(\alpha_2)$, то $\alpha_1\oplus\mu(x,\alpha_1)=$ $=\alpha_2\oplus\mu(x,\alpha_2)$, т.е. $(x+\alpha_1)\oplus x=(x+\alpha_2)\oplus x$, откуда $\alpha_1=\alpha_2$. Поэтому для произвольных $x,\beta\in V_n$ выполняется равенство

$$\max_{\alpha\in V_n\setminus\{0\}}d_+^G(x;\alpha,\beta)=\max_{\alpha'\in V_n\setminus\{0\}}d_{\oplus,+}^G(0;\alpha',\beta).\qquad(14)$$

Далее,

$$d_{\oplus,+}^G(0;\alpha,\beta)=2^{-n}\sum_{k\in V_n}\left\{\sum_{\gamma\in V_n}\delta(L_m(S(k)+\gamma)-L_m(S(k)),\beta)\delta(S(k\oplus\alpha')-S(k),\gamma)\right\}=$$

$$=2^{-n}\sum_{k\in V_n}\left\{\sum_{\gamma\in\Gamma_\beta^{-1}}\delta(L_m(S(k)+\gamma)-L_m(S(k)),\beta)\delta(S(k\oplus\alpha')-S(k),\gamma)\right\}\le$$

$$\le 2^{-n}\sum_{\gamma\in\Gamma_\beta^{-1}}\sum_{k\in V_n}\delta(S(k\oplus\alpha')-S(k),\gamma)=\sum_{\gamma\in\Gamma_\beta^{-1}}d_{\oplus,+}^G(0;\alpha,\gamma),\qquad(15)$$

поскольку $\delta(L_m(S(k)+\gamma)-L_m(S(k)),\beta)\le 1$. Используя (14) и (15), получаем

$$\max_{\alpha\in V_n\setminus\{0\}}d_+^G(\alpha,\beta)\le 2^{-n}\sum_{x\in V_n}\max_{\alpha\in V_n\setminus\{0\}}d_{\oplus,+}^G(0;\alpha,\beta)=$$

$$=\max_{\alpha\in V_n\setminus\{0\}}d_{\oplus,+}^G(0;\alpha,\beta)\le\max_{\alpha\in V_n\setminus\{0\}}\sum_{\gamma\in\Gamma_m^{-1}(\beta)}d_{\oplus,+}^S(0;\alpha,\gamma).$$

Доказано неравенство (12), а также лемма.

Для произвольного $\beta \in V_n$ ($\beta = q2^m + r, 0 \le q < 2^t - 1, 0 \le r < 2^m - 1$) введем следующие обозначения для элементов множества $\Gamma_m^{-1}(\beta)$:

$$\gamma_1 = \gamma_1(\beta) = \beta 2^t + q,\ \gamma_2 = \gamma_2(\beta) = \gamma_1 + 1,$$

$$\gamma_3 = \gamma_3(\beta) = \gamma_1 - 2^t, \gamma_4 = \gamma_4(\beta) = \gamma_1 - 2^t + 1.$$

Тогда из лемм 1, 2 получаем следствие.

Следствие 1. При введенных обозначениях для произвольного $\beta \in V_n \setminus \{0\}$ справедливы неравенства:

$$\forall \alpha \in V_n \setminus \{0\} \quad d_+^F(\alpha, \beta) \le \sum_{i=1}^{4} d_+^S(0; \alpha, \gamma_i(\beta)), \tag{16}$$

$$\max_{\alpha \in V_n \setminus \{0\}} d_+^G(\alpha, \beta) \le \max_{\alpha \in V_n \setminus \{0\}} \sum_{i=1}^{4} d_{\oplus,+}^S(0; \alpha, \gamma_i(\beta)). \tag{17}$$

Используя полученные результаты, сформулируем и докажем основную теорему, в которой будут построены верхние оценки средних вероятностей целочисленных дифференциалов отображений (1), (2).

ПОСТРОЕНИЕ ВЕРХНИХ ОЦЕНОК ВЕРОЯТНОСТЕЙ ЦЕЛОЧИСЛЕННЫХ РАУНДОВЫХ ДИФФЕРЕНЦИАЛОВ

Приведем верхние оценки вероятностей целочисленных раундовых дифференциалов (4) и (5) в случае, когда раундовая функция имеет вид (1) или (2).

Теорема 1. Пусть $t \ge u$, $p \ge 2$.

1. Если раундовая функция имеет вид (1), то справедливо неравенство

$$\forall \alpha, \beta \in V_n \setminus \{0\}: d_+^F(\alpha, \beta) \le \max\{2\Delta_+, 8\delta_+^{s^{(1)}}\}, \tag{18}$$

при выполнении дополнительного условия

$$\forall a \in V_u: s^{(2)}(a+1) \ne s^{(2)}(a) + 1 \tag{19}$$

справедлива более сильная оценка

$$d_+^F(\alpha, \beta) \le \max\{2\Delta_+, 4\delta_+^{s^{(1)}}\}. \tag{20}$$

2. Если раундовая функция имеет вид (2), то справедливо неравенство

$$\forall \alpha, \beta \in V_n \setminus \{0\}: d_+^G(\alpha, \beta) \le \max\{2\Delta_{\oplus,+}; 4\delta_{\oplus,+}^{s^{(1)}}\}. \tag{21}$$

Доказательство. Докажем только неравенства (18), (20) (неравенство (21) доказывается почти аналогично). Для произвольного $\alpha \in V_n$ обозначим $i = \min\{j = \overline{1, p}: \alpha^{(j)} \ne 0\}$.

Согласно следствию 1

$$d_+^F(\alpha, \beta) \le \sum_{i=1}^{4} \left\{ 2^{-n} \sum_{k \in V_n} \delta(S(k+\alpha) - S(k), \gamma_i(\beta)) \right\} = \sum_{i=1}^{4} d_+^S(0; \alpha, \gamma_i(\beta)).$$

Для произвольного $x \in V_n$, $x = (x^{(p)}, \ldots, x^{(1)})$, $x^{(i)} \in V_u$, $i = \overline{1, p}$, и введенного ранее отображения $S: V_n \to V_n$ обозначим

$$\tilde{x} = (x^{(p)}, \ldots, x^{(2)}) \in V_{n-u};\ \tilde{S}: V_{n-u} \to V_{n-u},\ \tilde{S}(\tilde{x}) = (s^{(p)}(x^{(p)}), \ldots, s^{(2)}(x^{(2)})). \tag{22}$$

Рассмотрим два случая.

Случай 1: $i = 1$. Поскольку $p \ge 2$, используя обозначения (7), для произвольного $j = \overline{1, 4}$ дифференциал $d_+^S(0; \alpha, \gamma_j(\beta))$ можно представить в виде

$$d_+^S(0; \alpha, \gamma_j(\beta)) = 2^{-n} \sum_{k^{(1)} \in V_u} \delta(S^{(1)}(k^{(1)} + \alpha^{(1)}) - S^{(1)}(k^{(1)}), \gamma_j^{(1)}) \times$$

$$\times \sum_{\tilde{k} \in V_{n-u}} \delta(\tilde{S}(\tilde{k} + \tilde{\alpha} + \nu(k^{(1)}, \alpha^{(1)})) - \tilde{S}(\tilde{k}) - \tau(k^{(1)}, \alpha^{(1)}), \tilde{\gamma}_j), \tag{23}$$

где сложение и вычитание выполняются по mod 2^u и mod 2^{n-u} соответственно, в зависимости от вида слагаемых.

Равенство (23) можно переписать следующим образом:

$$d_+^S(0;\alpha,\gamma_j(\beta)) = 2^{-u} \sum_{\substack{k^{(1)}\in V_u:\\ \nu(k^{(1)},\alpha^{(1)})=1,\\ \tau(k^{(1)},\alpha^{(1)})=1}} \delta(s^{(1)}(k^{(1)}+\alpha^{(1)})-s^{(1)}(k^{(1)}),\gamma_j^{(1)})\times$$

$$\times 2^{-(n-u)} \sum_{\widetilde{k}\in V_{n-u}} \delta(\widetilde{S}(\widetilde{k}+\widetilde{\alpha}+1)-\widetilde{S}(\widetilde{k})-1,\widetilde{\gamma}_j)+$$

$$+ 2^{-u} \sum_{\substack{k^{(1)}\in V_u:\\ \nu(k^{(1)},\alpha^{(1)})=0,\\ \tau(k^{(1)},\alpha^{(1)})=1}} \delta(s^{(1)}(k^{(1)}+\alpha^{(1)})-s^{(1)}(k^{(1)}),\gamma_j^{(1)})\times$$

$$\times 2^{-(n-u)} \sum_{\widetilde{k}\in V_{n-u}} \delta(\widetilde{S}(\widetilde{k}+\widetilde{\alpha})-\widetilde{S}(\widetilde{k})-1,\widetilde{\gamma}_j)+$$

$$+ 2^{-u} \sum_{\substack{k^{(1)}\in V_u:\\ \nu(k^{(1)},\alpha^{(1)})=1,\\ \tau(k^{(1)},\alpha^{(1)})=0}} \delta(s^{(1)}(k^{(1)}+\alpha^{(1)})-s^{(1)}(k^{(1)}),\gamma_j^{(1)})\times$$

$$\times 2^{-(n-u)} \sum_{\widetilde{k}\in V_{n-u}} \delta(\widetilde{S}(\widetilde{k}+\widetilde{\alpha}+1)-\widetilde{S}(\widetilde{k}),\widetilde{\gamma}_j)+$$

$$+ 2^{-u} \sum_{\substack{k^{(1)}\in V_u:\\ \nu(k^{(1)},\alpha^{(1)})=0,\\ \tau(k^{(1)},\alpha^{(1)})=0}} \delta(s^{(1)}(k^{(1)}+\alpha^{(1)})-s^{(1)}(k^{(1)}),\gamma_j^{(1)})\times$$

$$\times 2^{-(n-u)} \sum_{\widetilde{k}\in V_{n-u}} \delta(\widetilde{S}(\widetilde{k}+\widetilde{\alpha})-\widetilde{S}(\widetilde{k}),\widetilde{\gamma}_j) \le 2\delta_+^{s^{(1)}},$$

поскольку величина $\delta_+^{s^{(1)}}$ является верхней оценкой для каждого из первых сомножителей в четырех слагаемых последнего выражения, а сумма вторых множителей не превосходит 2 вследствие биективности отображений $s^{(i)}$, $i=\overline{1,p}$. Если при этом выполняется условие (19), то сумма вторых сомножителей не превосходит 1. Следовательно, согласно следствию 1 при $i=1$ выполняется неравенство $d_+^F(\alpha,\beta)\le 8\delta_+^{S^{(1)}}$ или, при выполнении условия (19), неравенство $d_+^F(\alpha,\beta)\le 4\delta_+^{S^{(1)}}$.

Случай 2: $1<i\le p$ (т.е. $\alpha^{(1)}=0$). Очевидно, что $d_+^S(\alpha,\gamma)\le d_+^{S^{(1)}}(\alpha^{(1)},\gamma^{(1)})$ и при выполнении условия $\gamma^{(1)}\ne 0$ будет выполняться условие $d_+^{S^{(1)}}(\alpha^{(1)},\gamma^{(1)})=0$. В таком случае условие $d_+^S(\alpha,\gamma)\ne 0$ выполняется только при $\gamma^{(1)}=0$. Следовательно, в рассматриваемых условиях $d_+^S(\alpha,\gamma)\ne 0\Rightarrow\gamma^{(1)}=0$, поэтому

$$d_+^F(\alpha,\beta)=\sum_{\substack{\gamma\in\Gamma_m^{-1}(\beta):\\ \gamma^{(1)}=0}} d_+^S(0;\alpha,\gamma).$$

Поскольку $\Gamma_m^{-1}(\beta)=\{\gamma,\gamma+1,\gamma-2^t,\gamma-2^t+1\}=\{\gamma_1,\gamma_2,\gamma_3,\gamma_4\}$, где $\gamma=q+\beta 2^t$, и вследствие условия $m\le n-u$, легко видеть, что множество $\{\gamma\in\Gamma_m^{-1}(\beta):\gamma^{(1)}=0\}$ содержит не более двух элементов: либо $\gamma^{(1)}$ и $\gamma^{(3)}$, либо $\gamma^{(2)}$ и $\gamma^{(4)}$. Поэтому

справедливо неравенство

$$d_+^F(\alpha,\beta) \le 2 \max_{\alpha,\gamma \in V_m \setminus \{0\}} d_+^S(0;\alpha,\gamma) \le 2 \max_{i=\overline{2,p}} d_+^{S^{(i)}}(0;\alpha,\gamma) \le$$

$$\le 2 \max_{i=\overline{2,p}} \left\{ \max_{\alpha,\gamma \in V_m \setminus \{0\}} d_+^{S^{(i)}}(0;\alpha,\gamma) \right\} = 2 \max_{i=\overline{2,p}} d_+^{S^{(i)}} = 2\Delta_+ ,$$

так как при произвольном значении $i = \overline{2,p}$ для произвольных $\alpha,\gamma \in V_n$ выполняется $d_+^S(0;\alpha,\gamma) \le d_+^{S^{(i)}}(0;\alpha^{(i)},\gamma^{(i)})$ и соответственно $d_+^S \le d_+^{S^{(i)}}$.

Теорема доказана.

РЕЗУЛЬТАТЫ СТАТИСТИЧЕСКИХ ИССЛЕДОВАНИЙ РАСПРЕДЕЛЕНИЙ ЧИСЛОВЫХ ПАРАМЕТРОВ, ХАРАКТЕРИЗУЮЩИХ ЗНАЧЕНИЯ СРЕДНИХ ВЕРОЯТНОСТЕЙ ЦЕЛОЧИСЛЕННЫХ РАУНДОВЫХ ДИФФЕРЕНЦИАЛОВ

Приведем результаты статистических исследований распределений параметров (6) и (8)–(10) для 8-битовых s-блоков. Для исследований сгенерировано 10 000 независимых и равновероятных подстановок, для каждой из которых посчитаны значения соответствующих параметров. В табл. 1 для 8-битовых узлов замены приведено статистическое распределение параметра $d_{\oplus,+}^{s^{(j)}} = \max_{\alpha,\beta \in V_u \setminus \{0\}} 2^{-u} \sum_{k \in V_u} \delta(s^{(j)}(k \oplus \alpha) - s^{(j)}(k), \beta)$ (выборка из 10 000 подстановок), в табл. 2 — параметра $d_+^{s^{(j)}} = \max_{\alpha,\beta \in V_u \setminus \{0\}} 2^{-u} \sum_{k \in V_u} \delta(s^{(j)}(k+\alpha) - s^{(j)}(k), \beta)$, в табл. 3 — параметра $\delta_+^{s^{(1)}} = \max_{a,b \in \{0,1\}} \max_{\alpha,\gamma \in V_u \setminus \{0\}} 2^{-u} \sum_{\substack{k \in V_u: \\ \nu(k,\alpha)=a, \\ \tau(k,\alpha)=b}} \delta(s^{(1)}(k+\alpha) - s^{(1)}(k), \gamma)$, в табл. 4 — параметра $\delta_{\oplus,+}^{s^{(1)}} = \max_{a \in \{0,1\}} \max_{\alpha,\gamma \in V_u \setminus \{0\}} 2^{-u} \sum_{\substack{k \in V_u: \\ \tau(k,\alpha)=a}} \delta(s^{(1)}(k \oplus \alpha) - s^{(1)}(k), \gamma)$.

Таблица 1

Значение параметра	Количество подстановок
0,0234375	486
0,0273438	4111
0,03125	4640
0,0351563	281
0,0390625	439
0,0429688	6
0,046875	35
0,0546875	2

Таблица 2

Значение параметра	Количество подстановок
0,0234375	486
0,0273438	4111
0,03125	4640
0,0351563	281
0,0390625	439
0,0429688	6
0,046875	35

Таблица 3

Значение параметра	Количество подстановок
0,0195313	13
0,0234375	4744
0,0273438	4458
0,03125	724
0,0351563	57
0,0390625	3
0,0429688	1

Таблица 4

Значение параметра	Количество подстановок
0,0195313	28
0,0234375	4972
0,0273438	4313
0,03125	622
0,0351563	61
0,0390625	4

ЗАКЛЮЧЕНИЕ

В результате статистических исследований распределений параметров (12), (14)–(16) для 8-битовых s-блоков, в частности, найдены подстановки с наименьшими возможными значениями данных параметров. Исходя из полученных ре-

зультатов, верхние оценки средних вероятностей целочисленных раундовых дифференциалов отображений (1), (2), при надлежащем выборе *s*-блоков, могут принимать значения $d_+^G(\alpha,\beta) \le 0{,}08$, $d_+^F(\alpha,\beta) \le 0{,}08$.

Данные результаты позволяют строить верхние оценки средних вероятностей целочисленных разностных характеристик блоковых шифров, в структуру которых входят указанные отображения. При этом средняя вероятность разностной характеристики зависит как от количества раундов, так и от свойств блока подстановки и наличия дополнительных преобразований в раунде.

Следует заметить, что открытым остается вопрос о влиянии на величину вероятности дифференциала наличия дополнительных преобразований в раунде (например, сложения с левой половиной, как в схеме Фейстеля, или более сложных преобразований, как в различных ее обобщениях), а также использования в раундовом преобразовании управляемой операции [15]. Данные вопросы могут быть предложены как направление дальнейших исследований.

СПИСОК ЛИТЕРАТУРЫ

1. National Institute of Standards and Technology: The Advanced Encryption Standard (AES) (http://csrc.nist.gov/aes/)
2. ГОСТ 28147-89. Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования. — М.: Госстандарт СССР, 1989. — 28 с.
3. Горбенко І.Д., Тоцький О.С., Казьміна С.В. Перспективний блоковий шифр «Калина» — основні положення та специфікація // Прикл. радіоелектроніка. — 2007. — **6,** № 2. — С. 195–208.
4. Перспективний блоковий шифр «Мухомор» — основні положення та специфікація / І.Д. Горбенко, М.Ф. Бондаренко, В.І. Долгов та ін. // Там же. — 2007. — **6,** № 2. — С. 147–157.
5. Kovalchuk L., Alekseyshuk A. Upper bounds of maximum value of average differential and linear characteristic probabilities of Feistel Cipher with adder modulo 2^n // Theory Stoch. Processes. — 2006. — **12(28),** N 1, 2. — P. 20–32.
6. Ковальчук Л.В. Верхние оценки средних вероятностей дифференциальных аппроксимаций булевых отображений // Тр. Четвертой Общерос. науч. конф. «Математика и безопасность информационных технологий» (МаБИТ-05), 2–3 нояб. 2005. — М.: МГУ, 2005. — С. 163–167.
7. Ковальчук Л.В. Обобщенные марковские шифры: оценка практической стойкости к методу дифференциального криптоанализа // Тр. Пятой Общерос. науч. конф. «Математика и безопасность информационных технологий» (МаБИТ-06), 25–27 окт. 2006. — М.: МГУ, 2006. — С. 595–599.
8. Олексійчук А.М., 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.
9. Алексейчук А.Н., Ковальчук Л.В., Шевцов А.С., Скрыпник Л.В. Оценки практической стойкости блочного шифра «Калина» относительно разностного, линейного билинейного методов криптоанализа // Тр. Седьмой Общерос. науч. конф. «Математика и безопасность информационных технологий» (МаБИТ-08), 30 окт.–2 нояб. 2008. — М.: МГУ, 2008. — С. 15–20.
10. Алексейчук А.Н., Ковальчук Л.В., Скрынник Е.Н., Шевцов А.С. Оценки практической стойкости блочного шифра «Калина» относительно методов разностного, линейного криптоанализа и алгебраических атак, основанных на гомоморфизмах // Прикл. радиоэлектроника. — 2008. — № 1. — С. 203–210.
11. Алексейчук А.Н., Шевцов А.С. Верхние оценки несбалансированности билинейных аппроксимаций раундовых функций блочных шифров // Кибернетика и системный анализ. — 2010. — № 3. — С. 42–51.
12. Wang X., Yu H. How to break MD5 and other hash functions // Adv. Cryptology. EUROCRYPT'05; Lect. Notes Comput. Sci. — Berlin: Springer-Verlag, 2005. — **3494**. — P. 19–35.
13. Cotini S., Riverst R.L., Robshaw M.J.B., Lisa Yin Y. Security of the RC6TM block cipher (http//www.rsasecurity.com/rsalabs/rc6/).
14. Berson T.A. Differential cryptanalysis mod 2^{32} with applications to MD5 // Adv. Cryptology. CRYPTO'98; Lect. Notes Comput. Sci. — Berlin: Springer-Verlag, 1999. — **372.** — P. 95–103.
15. Изотов Б.В., Молдовян А.А., Молдовян Н.А. Алгоритмы преобразования информации на базе управляемых двухместных операций // Кибернетика и системный анализ. — 2003. — № 2. — С. 164–177.

Поступила 03.11.2009