УДК 621.391:519.2

Л.В. КОВАЛЬЧУК, Н.В. КУЧИНСКАЯ

ПОСТРОЕНИЕ ВЕРХНИХ ОЦЕНОК СРЕДНИХ ВЕРОЯТНОСТЕЙ ЦЕЛОЧИСЛЕННЫХ ДИФФЕРЕНЦИАЛОВ РАУНДОВЫХ ФУНКЦИЙ БЛОЧНЫХ ШИФРОВ ОПРЕДЕЛЕННОЙ СТРУКТУРЫ

Ключевые слова: *блочный шифр, разностный криптоанализ, целочисленные дифференциалы.*

ВВЕДЕНИЕ

Для построения оценок стойкости блочного алгоритма шифрования к разностному криптоанализу и различным его модификациям [1–6], как правило, необходимо оценить сверху среднюю вероятность раундового дифференциала. Раундовые функции большинства из современных блочных алгоритмов шифрования (AES [7], ГОСТ 28147 [8], «Калина» [9], «Мухомор» [10]) содержат композицию ключевого сумматора, блока подстановки и оператора перестановки, линейного над полем F_2 или его некоторым расширениям. Поэтому задача оценивания стойкости блочных шифров или сводится к задаче построения верхних оценок средних вероятностей таких композиций, или содержит ее как подзадачу. Последняя полностью решена в следующих случаях:

1) 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 в [1, 3]);

2) если в ключевом сумматоре реализована операция сложения по модулю 2^n, а входные и выходные разности в раундовом дифференциале рассматриваются относительно операции побитового сложения [1–6];

3) если в ключевом сумматоре реализована операция сложения по модулю 2^n, входные и выходные разности рассматриваются относительно этой же операции (такой дифференциал называют целочисленным [11, 12]) и при этом либо отсутствует оператор перестановки [2], либо отсутствует блок подстановки и оператор перестановки является оператором циклического сдвига [13];

4) если в ключевом сумматоре реализована либо операция побитового сложения, либо операция сложения по модулю 2^n, блок подстановки произвольный, а оператор перестановки является оператором циклического сдвига (величина сдвига взаимно проста с длиной входа s-блока [14].

В связи с возрастающими требованиями к быстродействию блочных алгоритмов многие современные алгоритмы строятся байт-ориентированными (например, AES). Поэтому актуальной является задача оценивания вероятности целочисленного дифференциала для композиции ключевого сумматора, блока подстановок и оператора байтовой перестановки, в том числе байтового сдвига. В частности, раундовая функция такого вида возможна при модификации алгоритма ГОСТ 28147, заключающейся в удлинении блока (до 128, 256 или 512 бит) и перевода его на байтовую основу. В данной работе решается задача построения верхних оценок средних вероятностей целочисленных дифференциалов отображений, которые являются композициями сумматора, блока подстановки и оператора циклического сдвига в случае, когда величина сдвига пропорциональна длине входа s-блока. В ходе ее решения также показывается, что верхние оценки вероятности целочисленного дифференциала уменьшатся, если величина циклического сдвига пропорциональна длине входа s-блока, т.е. описанная модификация приводит не только к увеличению скорости шифрования, но и к стойкости алгоритма к целочисленному разностному криптоанализу.

ВСПОМОГАТЕЛЬНЫЕ ОБОЗНАЧЕНИЯ И РЕЗУЛЬТАТЫ

Введем следующие обозначения: $\forall n \in N : V_n = \{0, 1\}^n$ — множество n-мерных битовых векторов. Векторы из V_n однозначно соответствуют целым числам от 0 до $2^n - 1$, $n \in N$.

Пусть $n = pu,\ p \geq 2$, тогда $\forall x \in V_n : x = (x^{(p)}, \ldots, x^{(1)}),\ x^{(i)} \in V_u,\ i = \overline{1, p}$.

Отображение $S : V_n \to V_n$ биективное, $\forall x \in V_n$: $S(x) = (S^{(p)}(x^{(p)}), \ldots$ $\ldots, S^{(1)}(x^{(1)}))$, $x^{(i)} \in V_u,\ i = \overline{1, p}$, где $S^{(i)} : V_u \to V_u,\ i = \overline{1, p}$, — биективные отображения. Такое отображение часто называют блоком подстановки, а отображения $S^{(i)}$ — s-блоками.

Обозначим L_{tu}: $V_n \to V_n$ отображение сдвига влево на tu бит вектора из V_n, $1 \leq t \leq p - 1$. В настоящей работе рассматриваются только такие операторы сдвига L_{tu}, в которых величина сдвига кратна длине s-блока.

На множестве V_n определим следующие подмножества [14]:

$$\Gamma_{tu}(\gamma) = \{\beta \in V_n \mid \exists\, k \in V_n : L_{tu}(k + \gamma) - L_{tu}(k) = \beta\};$$

$$\Gamma_{tu}^{-1}(\beta) = \{\gamma \in V_n \mid \exists k \in V_n : L_{tu}(k + \gamma) - L_{tu}(k) = \beta\}.$$

Для произвольной функции $F : V_n \times V_n \to V_n$ обозначим $F_k(x) := F(k, x)$, $k, x \in V_n$.

Согласно определению (например, [3]) средняя (по ключам) вероятность целочисленного дифференциала $d_+^F(\alpha, \beta)$, где $\alpha, \beta \in V_n \setminus \{0\}$, для произвольного отображения $F_k(x)$ имеет вид

$$d_+^F(\alpha, \beta) = 2^{-2n} \sum_{x, k \in V_n} \delta(F_k(x + \alpha) - F_k(x), \beta). \tag{1}$$

В данной работе рассматриваются отображения, которые являются композицией ключевого сумматора, блока подстановки и оператора циклического сдвига:

$$F_k(x) = L_{tu}(S(x + k)). \tag{2}$$

Согласно лемме 1 из [14] и результатам, представленным в [13], $\forall tu \in N$, $\forall \beta \in V_n,\ \beta = q2^{n-tu} + r$, где $0 \leq r \leq 2^{n-tu} - 1,\ 0 \leq q \leq 2^{tu} - 1$, выполняется следующее соотношение между множествами:

$$\Gamma_{tu}^{-1}(\beta) = \Gamma_{n-tu}(\beta) \subset \{\gamma, \gamma + 1, \gamma - 2^{n-tu}, \gamma - 2^{n-tu} + 1\} = \{\gamma_1, \gamma_2, \gamma_3, \gamma_4\},$$

где $\gamma = \gamma(\beta) = q + r2^{tu} = q + \beta 2^{tu}$. В частности, $|\Gamma_{tu}^{-1}(\beta)| \leq 4$ и $\gamma_1 = q + \beta 2^{tu} =$ $= q + r2^{tu}$, $\gamma_2 = q + 1 + r2^{tu}$, $\gamma_3 = q + r2^{tu} - 2^{n-tu}$, $\gamma_4 = q + 1 + r2^{tu} - 2^{n-tu}$.

Обозначим

$$D^S(\alpha, \beta) = 2^{-n} \sum_{k \in V_n} \sum_{\gamma \in \Gamma_{tu}^{-1}(\beta)} \delta(S(k + \alpha) - S(k), \gamma) = 2^{-n} \sum_{k \in V_n} \sum_{i=1}^{4} \delta(S(k + \alpha) - S(k), \gamma).$$

Лемма 1. В принятых обозначениях для отображения (2) выполняется следующая оценка:

$$d_+^F(\alpha, \beta) \leq D^S(\alpha, \beta),\ \alpha, \beta \in V_n \setminus \{0\}. \tag{3}$$

Доказательство. Согласно (1) и (2) имеем

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

$$= 2^{-2n} \sum_{x, k \in V_n} \delta(L_{tu}(S(x + k + \alpha)) - L_{tu}(S(x + k)), \beta).$$

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

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

Последнее выражение преобразуем следующим образом:

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

$$=2^{-n}\sum_{k\in V_n}\left\{\sum_{\gamma\in\Gamma_{tu}^{-1}(\beta)}\delta(L_{tu}(S(k)+\gamma)-L_{tu}(S(k),\beta)\times\delta(S(k+\alpha)-S(k),\gamma)\right\}.$$

Поскольку $\delta(L_m(S(k)+\gamma)-L_m(S(k)),\beta)\le 1,$ имеем

$$d_+^F(\alpha,\beta)\le 2^{-n}\sum_{k\in V_n}\sum_{\gamma\in\Gamma_{tu}^{-1}(\beta)}\delta(S(k+\alpha)-S(k),\gamma)=D^S(\alpha,\beta)\ ,$$

что и требовалось доказать.

ПОСТРОЕНИЕ ВЕРХНИХ ОЦЕНОК ВЕРОЯТНОСТЕЙ ЦЕЛОЧИСЛЕННЫХ РАУНДОВЫХ ДИФФЕРЕНЦИАЛОВ

Для дальнейшего изложения понадобятся следующие обозначения.

Для произвольного $x\in V_n$, $x=(x^{(p)},\ldots,x^{(1)}), x^{(i)}\in V_u, i=\overline{1,p},$ обозначим $\tilde{x}=(x^{(p)},\ldots,x^{(t+1)})\in V_{n-tu}$ и $\tilde{\tilde{x}}=(x^{(t)},\ldots,x^{(1)})\in V_{tu}$ (тогда $x=(\tilde{x},\tilde{\tilde{x}})$).

Для введенного ранее отображения $S:V_n\to V_n$ также обозначим $\tilde{S}:V_{n-tu}\to V_{n-tu}$, где $\tilde{S}(\tilde{x})=(S^{(p)}(x^{(p)}),\ldots,S^{(t+1)}(x^{(t+1)}))$, и $\tilde{\tilde{S}}:V_u\to V_{tu}$, где $\tilde{\tilde{S}}(\tilde{\tilde{x}})=(S^{(t)}(x^{(t)}),\ldots,S^{(1)}(x^{(1)}))$.

Введем следующие величины:

$$\delta^{S^{(i)}}=\max_{\substack{\alpha\in V_u\setminus\{0\}\\ q\in V_u}}2^{-u}\sum_{k\in V_u}\{\delta(S^{(i)}(k+\alpha)-S^{(i)}(k),q)+\delta(S^{(i)}(k+\alpha)-S^{(i)}(k),q+1)\},\quad i=\overline{1,p}; \tag{4}$$

$$d^{S^{(j)}}=\max_{\alpha,\beta\in V_u\setminus\{0\}}2^{-u}\sum_{k\in V_u}\delta(S^{(j)}(k+\alpha)-S^{(j)}(k),\beta),\ j=\overline{1,p},\ \Delta_{k,l}=\max_{j=\overline{k,l}}d^{S^{(j)}}. \tag{5}$$

Обозначим

$$\upsilon=\upsilon(\tilde{\tilde{k}}+\tilde{\tilde{\alpha}})=\begin{cases}0, & \text{если } \tilde{\tilde{k}}+\tilde{\tilde{\alpha}}\le 2^{tu}-1,\\ 1 & \text{в противном случае,}\end{cases}$$

$$\tau=\tau(\tilde{\tilde{k}}+\tilde{\tilde{\alpha}})=\begin{cases}0, & \text{если } \tilde{\tilde{S}}(\tilde{\tilde{k}}+\tilde{\tilde{\alpha}})>\tilde{\tilde{S}}(\tilde{\tilde{k}}),\\ 1 & \text{в противном случае.}\end{cases}$$

Следующие теоремы определяют верхние оценки для величины (1) отображения (2).

Теорема 1. Пусть $1\le t\le\left\lfloor\frac{p}{2}\right\rfloor, p\ge 4, p\in N$. Тогда

$$d_+^F(\alpha,\beta)\le\max\{\delta^{S^{(1)}},\Delta_{1,t},2\Delta_{(t+1),p}\}.$$

Доказательство. Пусть $1\le t\le\left\lfloor\frac{p}{2}\right\rfloor, p\ge 4, p\in N$ (величина сдвига влево не превосходит половины общего количества s-блоков), $0\le r\le 2^{n-tu}-1, 0\le q\le$ $\le 2^{tu}-1$. Рассмотрим для $\tilde{\tilde{\alpha}}\ne 0$ возможные случаи.

Случай 1. Пусть $0 \le q < 2^{tu} - 1$. Тогда $x = (\widetilde{x}, \widetilde{\widetilde{x}})$, $\alpha = (\widetilde{\alpha}, \widetilde{\widetilde{\alpha}})$ и соответственно $\gamma_1 = (\widetilde{\gamma}_1, \widetilde{\widetilde{\gamma}}_1) = (r, q)$, $\gamma_2 = (r, q+1)$, $\gamma_3 = (r - 2^{n-2tu}, q)$, $\gamma_4 = (r - 2^{n-2tu}, q+1)$.

В принятых обозначениях

$$D^S(\alpha, \beta) = 2^{-n} \sum_{k \in V_n} \sum_{i=1}^{4} \delta(S(k+\alpha) - S(k), \gamma_i) =$$

$$= 2^{-tu} \sum_{\widetilde{\widetilde{k}} \in V_{tu}} \delta(\widetilde{\widetilde{S}}(\widetilde{\widetilde{k}} + \widetilde{\widetilde{\alpha}}) - \widetilde{\widetilde{S}}(\widetilde{\widetilde{k}}), q) \times 2^{-(n-tu)} \sum_{\widetilde{k} \in V_{n-tu}} \delta(\widetilde{S}(\widetilde{k} + \widetilde{\alpha} + \upsilon) - \widetilde{S}(\widetilde{k}) - \tau), r) +$$

$$+ 2^{-tu} \sum_{\widetilde{\widetilde{k}} \in V_{tu}} \delta(\widetilde{\widetilde{S}}(\widetilde{\widetilde{k}} + \widetilde{\widetilde{\alpha}}) - \widetilde{\widetilde{S}}(\widetilde{\widetilde{k}}), q+1) \times 2^{-(n-tu)} \sum_{\widetilde{k} \in V_{n-tu}} \delta(\widetilde{S}(\widetilde{k} + \widetilde{\alpha} + \upsilon) - \widetilde{S}(\widetilde{k}) - \tau, r) +$$

$$+ 2^{-tu} \sum_{\widetilde{\widetilde{k}} \in V_{tu}} \delta(\widetilde{\widetilde{S}}(\widetilde{\widetilde{k}} + \widetilde{\widetilde{\alpha}}) - \widetilde{\widetilde{S}}(\widetilde{\widetilde{k}}), q) \times 2^{-(n-tu)} \sum_{\widetilde{k} \in V_{n-tu}} \delta(\widetilde{S}(\widetilde{k} + \widetilde{\alpha} + \upsilon) - \widetilde{S}(\widetilde{k}) - \tau, r - 2^{n-2tu}) +$$

$$+ 2^{-tu} \sum_{\widetilde{\widetilde{k}} \in V_{tu}} \delta(\widetilde{\widetilde{S}}(\widetilde{\widetilde{k}} + \widetilde{\widetilde{\alpha}}) - \widetilde{\widetilde{S}}(\widetilde{\widetilde{k}}), q+1) \times$$

$$\times 2^{-(n-tu)} \sum_{\widetilde{k} \in V_{n-tu}} \delta(\widetilde{S}(\widetilde{k} + \widetilde{\alpha} + \upsilon) - \widetilde{S}(\widetilde{k}) - \tau, r - 2^{n-2tu}) =$$

$$= 2^{-tu} \sum_{\widetilde{\widetilde{k}} \in V_{tu}} (\delta(\widetilde{\widetilde{S}}(\widetilde{\widetilde{k}} + \widetilde{\widetilde{\alpha}}) - \widetilde{\widetilde{S}}(\widetilde{\widetilde{k}}), q) + \delta(\widetilde{\widetilde{S}}(\widetilde{\widetilde{k}} + \widetilde{\widetilde{\alpha}}) - \widetilde{\widetilde{S}}(\widetilde{\widetilde{k}}), q+1)) \times$$

$$\times 2^{-(n-tu)} \sum_{\widetilde{k} \in V_{n-tu}} (\delta(\widetilde{S}(\widetilde{k} + \widetilde{\alpha} + \upsilon) - \widetilde{S}(\widetilde{k}) - \tau, r) + \delta(\widetilde{S}(\widetilde{k} + \widetilde{\alpha} + \upsilon) - \widetilde{S}(\widetilde{k}) - \tau, r - 2^{n-2tu}).$$

Обозначим

$$f_1(k, \alpha) = \delta(\widetilde{S}(\widetilde{k} + \widetilde{\alpha} + \upsilon) - \widetilde{S}(\widetilde{k}) - \tau, r),$$

$$f_2(k, \alpha) = \delta(\widetilde{S}(\widetilde{k} + \widetilde{\alpha} + \upsilon) - \widetilde{S}(\widetilde{k}) - \tau, r - 2^{n-2u}).$$

Тогда в силу однозначности операции сложения, если для некоторых $\widetilde{k}$ выполняется $f_1(k, \alpha) = 1$, то $f_2(k, \alpha) = 0$, и наоборот. Таким образом, $\forall \widetilde{k} : f_1(k, \alpha) + f_2(k, \alpha) \le 1$, следовательно,

$$2^{-(n-tu)} \sum_{\widetilde{k} \in V_{n-tu}} (\delta(\widetilde{S}(\widetilde{k} + \widetilde{\alpha} + \upsilon) - \widetilde{S}(\widetilde{k}) - \tau, r) + \delta(\widetilde{S}(\widetilde{k} + \widetilde{\alpha} + \upsilon) - \widetilde{S}(\widetilde{k}) - \tau, r - 2^{n-2tu}) \le 1.$$

Отсюда

$$D^S(\alpha, \beta) \le 2^{-tu} \sum_{\widetilde{\widetilde{k}} \in V_{tu}} (\delta(\widetilde{\widetilde{S}}(\widetilde{\widetilde{k}} + \widetilde{\widetilde{\alpha}}) - \widetilde{\widetilde{S}}(\widetilde{\widetilde{k}}), q) + \delta(\widetilde{\widetilde{S}}(\widetilde{\widetilde{k}} + \widetilde{\widetilde{\alpha}}) - \widetilde{\widetilde{S}}(\widetilde{\widetilde{k}}), q+1)).$$

Рассмотрим два возможных варианта для $\widetilde{\widetilde{\alpha}} = (\alpha^{(t)}, \ldots, \alpha^{(1)}) : \alpha^{(1)} \ne 0$ и $\alpha^{(1)} = 0$.

1. Если $\alpha^{(1)} \ne 0$, то

$$D^S(\alpha, \beta) \le 2^{-u} \sum_{k^{(1)} \in V_u} (\delta(S^{(1)}(k^{(1)} + \alpha^{(1)}) - S^{(1)}(k^{(1)}), q^{(1)}) +$$

$$+ \delta(S^{(1)}(k^{(1)} + \alpha^{(1)}) - S^{(1)}(k^{(1)}), q^{(1)} + 1)) \le$$

$$\le \max_{\substack{\alpha^{(1)} \in V_u \setminus \{0\} \\ q^{(1)} \in V_u}} 2^{-u} \sum_{k \in V_u} \{\delta(S^{(1)}(k^{(1)} + \alpha^{(1)}) - S^{(1)}(k^{(1)}), q^{(1)}) +$$

$$+ \delta(S^{(1)}(k^{(1)} + \alpha^{(1)}) - S^{(1)}(k^{(1)}), q^{(1)} + 1)\}.$$

Таким образом, $D^S(\alpha, \beta) \le \delta^{S^{(1)}}$.

2. Если $\alpha^{(1)}=0$, то равенство $\tilde{\tilde{S}}(\tilde{\tilde{k}}+\tilde{\tilde{\alpha}})-\tilde{\tilde{S}}(\tilde{\tilde{k}})=\tilde{\tilde{\varepsilon}}$ возможно лишь в случае $\varepsilon^{(1)}=0$. Поскольку только один из векторов, q или $q+1$, может иметь первую правую нулевую компоненту, то $D^S(\alpha,\beta)\le \max\limits_{\substack{\tilde{\tilde{\alpha}}\in V_{tu}\setminus\{0\}\\ \tilde{\tilde{q}}\in V_{tu}}} 2^{-tu}\sum\limits_{\tilde{\tilde{k}}\in V_{tu}}\delta(\tilde{\tilde{S}}(\tilde{\tilde{k}}+\tilde{\tilde{\alpha}})-\tilde{\tilde{S}}(\tilde{\tilde{k}}),\tilde{\tilde{q}})$.

Обозначим для произвольного $\tilde{\tilde{\alpha}}\in V_{tu}: i=\min\limits_{j=\overline{2,t}}\{\alpha^{(j)}\ne 0\}$. Тогда для $2\le i\le t$ имеем

$$D^S(\alpha,\beta)\le \max_{\substack{\alpha^{(i)}\in V_u\setminus\{0\}\\ q^{(i)}\in V_{tu}}} 2^{-u}\sum_{k^{(i)}\in V_u}(\delta(S^{(i)}(k^{(i)}+\alpha^{(i)})-S^{(i)}(k^{(i)}),q^{(i)}))=$$

$$=d^{S^{(i)}}\le \max_{i=\overline{2,t}} d^{S^{(i)}}=\Delta_{2,t}\le\Delta_{1,t}.$$

Случай 2. Пусть $q=2^{tu}-1$. Тогда

$$\gamma_1=(\tilde{\gamma}_1,\tilde{\tilde{\gamma}}_1)=(r,2^{tu}-1),\ \gamma_2=(r+1,0),$$

$$\gamma_3=(r-2^{n-2tu},2^{tu}-1),\ \gamma_4=(r-2^{n-2tu}+1,0),$$

$$D^S(\alpha,\beta)=2^{-tu}\sum_{\tilde{\tilde{k}}\in V_{tu}}\delta(\tilde{\tilde{S}}(\tilde{\tilde{k}}+\tilde{\tilde{\alpha}})-\tilde{\tilde{S}}(\tilde{\tilde{k}}),0)\times$$

$$\times 2^{-(n-tu)}\sum_{\tilde{k}\in V_{n-tu}}\{\delta(\tilde{S}(\tilde{k}+\tilde{\alpha})-\tilde{S}(\tilde{k}),r+1)+\delta(\tilde{S}(\tilde{k}+\tilde{\alpha})-\tilde{S}(\tilde{k}),r-2^{n-2tu}+1)\}+$$

$$+2^{-tu}\sum_{\tilde{\tilde{k}}\in V_{tu}}\delta(\tilde{\tilde{S}}(\tilde{\tilde{k}}+\tilde{\tilde{\alpha}})-\tilde{\tilde{S}}(\tilde{\tilde{k}}),2^{tu}-1)\times$$

$$\times 2^{-(n-tu)}\sum_{\tilde{k}\in V_{n-tu}}\{\delta(\tilde{S}(\tilde{k}+\tilde{\alpha})-\tilde{S}(\tilde{k}),r)+\delta(\tilde{S}(\tilde{k}+\tilde{\alpha})-\tilde{S}(\tilde{k}),r-2^{n-2tu})\}.$$

Очевидно, что в силу биективности отображения $\tilde{\tilde{S}}$ имеем $\tilde{\tilde{S}}(\tilde{\tilde{k}}+\tilde{\tilde{\alpha}})-\tilde{\tilde{S}}(\tilde{\tilde{k}})=0$ только при $\tilde{\tilde{\alpha}}=0$, что противоречит условию $\tilde{\tilde{\alpha}}\ne 0$.

1. При $\tilde{\tilde{\alpha}}\ne 0$ имеем

$$D^S(\alpha,\beta)=2^{-tu}\sum_{\tilde{\tilde{k}}\in V_{tu}}\delta(\tilde{\tilde{S}}(\tilde{\tilde{k}}+\tilde{\tilde{\alpha}})-\tilde{\tilde{S}}(\tilde{\tilde{k}}),2^{tu}-1)\times$$

$$\times 2^{-(n-tu)}\sum_{\tilde{k}\in V_{n-tu}}\{\delta(\tilde{S}(\tilde{k}+\tilde{\alpha})-\tilde{S}(\tilde{k}),r+1)+\delta(\tilde{S}(\tilde{k}+\tilde{\alpha})-\tilde{S}(\tilde{k}),r-2^{n-2tu}+1)\}.$$

Поскольку

$$2^{-(n-tu)}\sum_{\tilde{k}\in V_{n-tu}}\{\delta(\tilde{S}(\tilde{k}+\tilde{\alpha})-\tilde{S}(\tilde{k}),r+1)+\delta(\tilde{S}(\tilde{k}+\tilde{\alpha})-\tilde{S}(\tilde{k}),r-2^{n-2tu}+1)\}\le 1,$$

получим

$$D^S(\alpha,\beta)=2^{-tu}\sum_{\tilde{\tilde{k}}\in V_{tu}}\delta(\tilde{\tilde{S}}(\tilde{\tilde{k}}+\tilde{\tilde{\alpha}})-\tilde{\tilde{S}}(\tilde{\tilde{k}}),2^{tu}-1)\le 2^{-tu}\sum_{\tilde{\tilde{k}}\in V_{tu}}\delta(\tilde{\tilde{S}}(\tilde{\tilde{k}}+\tilde{\tilde{\alpha}})-\tilde{\tilde{S}}(\tilde{\tilde{k}}),q).$$

Обозначим для произвольного $\tilde{\tilde{\alpha}}\in V_{tu}: i=\min\limits_{j=\overline{1,t}}\{\alpha^{(j)}\ne 0\}$. Тогда

$$D^S(\alpha,\beta)\le \max_{\substack{\alpha^{(i)}\in V_u\setminus\{0\}\\ q^{(i)}\in V_u}} 2^{-u}\sum_{k^{(i)}\in V_{tu}}\delta(S^{(i)}(k^{(i)}+\alpha^{(i)})-S^{(i)}(k^{(i)}),q^{(i)})=d^{S^{(i)}}.$$

2. Рассмотрим случай $\tilde{\tilde{\alpha}} = 0$. Тогда аналогично [14] справедливо неравенство

$$\forall \alpha \in V_n,\ \forall \beta \in V_n \setminus \{0\}: d_+^F(\alpha, \beta) \le 2^{-n} \sum_{k \in V_n} \sum_{\substack{\gamma \in \Gamma_{tu}^{-1}(\beta) \\ \tilde{\tilde{\gamma}} = 0}} \delta(S(k+\alpha) - S(k), \gamma).$$

Поскольку $\Gamma_{tu}^{-1}(\beta) = \{\gamma, \gamma+1, \gamma - 2^{n-tu}, \gamma - 2^{n-tu}+1\} = \{\gamma_1, \gamma_2, \gamma_3, \gamma_4\}$, где $\gamma_1 = = \gamma(\beta) = q + \beta 2^{tu} = q + r2^{tu}$, множество $\{\gamma \in \Gamma_{tu}^{-1}(\beta) : \tilde{\tilde{\gamma}} = 0\}$ содержит не более двух элементов: либо γ_1 и γ_3, либо γ_2 и γ_4. Поэтому справедлива оценка

$$d_+^F(\alpha, \beta) \le 2 \max_{\underline{i = (t+1), p}} \max_{\alpha, \beta \in V_u \setminus \{0\}} 2^{-u} \sum_{k \in V_u} \delta(S^{(i)}(k+\alpha) - S^{(i)}(k), \beta) = 2\Delta_{(t+1), p}.$$

Теорема 2. Пусть $\frac{p}{2} < t \le p-1,\ p \ge 4,\ p \in N$. Тогда

$$d_+^F(\alpha, \beta) \le \max\{2d^{S^{(1)}}, 2\Delta_{2,t}, \Delta_{1,p}\}.$$

Доказательство. Пусть $\frac{p}{2} < t \le p-1,\ p \ge 4,\ p \in N$ (величина сдвига влево не меньше половины общего количества s-блоков).

В принятых обозначениях $\gamma_1 = q + \beta 2^{tu} = q + r2^{tu}$, $\gamma_2 = q + 1 + r2^{tu}$, $\gamma_3 = = q + r2^{tu} - 2^{n-tu}$, $\gamma_4 = q + 1 + r2^{tu} - 2^{n-tu}$; $0 \le r \le 2^{n-tu} - 1$, $0 \le q \le 2^{tu} - 1$.

Рассмотрим подробно возможные варианты.

Случай 1. Если $q = 2^{tu} - 1$, то $\gamma_1 = (\tilde{\gamma}_1, \tilde{\tilde{\gamma}}_1) = (r, 2^{tu} - 1)$, $\gamma_2 = (r+1, 0)$, $\gamma_3 = (r, 2^{tu} - 2^{n-tu} - 1)$, $\gamma_4 = (r, 2^{tu} - 2^{n-tu})$. Тогда

$$D^S(\alpha, \beta) = 2^{-n} \sum_{k \in V_n} \sum_{i=1}^{4} \delta(S(k+\alpha) - S(k), \gamma_i) =$$

$$= 2^{-(n-tu)} \sum_{\tilde{k} \in V_{(n-tu)}} \delta(\tilde{S}(\tilde{k} + \tilde{\alpha} + \upsilon) - \tilde{S}(\tilde{k}) - \tau, r) \times$$

$$\times 2^{-tu} \sum_{\tilde{\tilde{k}} \in V_{tu}} \{\delta(\tilde{\tilde{S}}(\tilde{\tilde{k}} + \tilde{\tilde{\alpha}}) - \tilde{\tilde{S}}(\tilde{\tilde{k}}), 2^{tu} - 1) + \delta(\tilde{\tilde{S}}(\tilde{\tilde{k}} + \tilde{\tilde{\alpha}}) - \tilde{\tilde{S}}(\tilde{\tilde{k}}), 2^{tu} - 2^{n-tu} - 1) +$$

$$+ \delta(\tilde{\tilde{S}}(\tilde{\tilde{k}} + \tilde{\tilde{\alpha}}) - \tilde{\tilde{S}}(\tilde{\tilde{k}}), 2^{tu} - 2^{n-tu})\} +$$

$$+ 2^{-n-tu} \sum_{\tilde{k} \in V_{(n-tu)}} \delta(\tilde{S}(\tilde{k} + \tilde{\alpha} + \upsilon)) - \tilde{S}(\tilde{k}) - \tau(\tilde{\tilde{k}} + \tilde{\tilde{\alpha}}), r+1) \times$$

$$\times 2^{-tu} \sum_{\tilde{\tilde{k}} \in V_{tu}} (\delta(\tilde{\tilde{S}}(\tilde{\tilde{k}} + \tilde{\tilde{\alpha}}) - \tilde{\tilde{S}}(\tilde{\tilde{k}}), 0).$$

1. Если $\tilde{\tilde{\alpha}} = 0$ (при этом $\tilde{\alpha} \ne 0$), то $\upsilon = 0$, $\tau = 0$ и $2^{-tu} \sum_{\tilde{\tilde{k}} \in V_{tu}} (\delta(\tilde{\tilde{S}}(\tilde{\tilde{k}}) - \tilde{\tilde{S}}(\tilde{\tilde{k}}), \xi) \ne 0$

только при $\xi = 0$. Тогда

$$D^S(\alpha, \beta) = 2^{-(n-tu)} \sum_{\tilde{k} \in V_{(n-tu)}} \delta(\tilde{S}(\tilde{k} + \tilde{\alpha}) - \tilde{S}(\tilde{k}), r+1) \times 2^{-tu} \sum_{\tilde{\tilde{k}} \in V_{tu}} \delta(\tilde{\tilde{S}}(\tilde{\tilde{k}}) - \tilde{\tilde{S}}(\tilde{\tilde{k}}), 0) =$$

$$= 2^{-(n-tu)} \sum_{\tilde{k} \in V_{(n-tu)}} \delta(\tilde{S}(\tilde{k} + \tilde{\alpha}) - \tilde{S}(\tilde{k}), r+1).$$

Обозначим для произвольного $\tilde{\alpha} \in V_{n-tu}$, $\tilde{\alpha} = (\alpha^{(p)}, \ldots, \alpha^{(t+1)})$: $i = \min\limits_{\overline{j=(t+1), p}} \{\alpha^{(j)} \neq 0\}$. Тогда для $t < i \leq p$ имеем

$$D^S(\alpha, \beta) \leq \max_{r^{(i)}, \alpha^{(i)} \in V_u \setminus \{0\}} 2^{-u} \sum_{k^{(i)} \in V_u} \delta(S^{(i)}(k^{(i)} + \alpha^{(i)}) - S(k^{(i)}), r^{(i)}) = d^{S^{(i)}} \leq$$

$$\leq \max_{t<i\leq p} d^{S^{(i)}} = \Delta_{(t+1), p}.$$

2. Если $\tilde{\tilde{\alpha}} \neq 0$, то $2^{-tu} \sum\limits_{\tilde{\tilde{k}} \in V_{tu}} (\delta(\tilde{\tilde{S}}(\tilde{\tilde{k}} + \tilde{\tilde{\alpha}}) - \tilde{\tilde{S}}(\tilde{\tilde{k}}), 0) = 0$,

$$D^S(\alpha, \beta) = 2^{-(n-tu)} \sum_{\tilde{k} \in V_{n-tu}} \delta(\tilde{S}(\tilde{k} + \tilde{\alpha} + \upsilon) - \tilde{S}(\tilde{k}) - \tau, r) \times$$

$$\times 2^{-tu} \sum_{\tilde{\tilde{k}} \in V_{tu}} \{\delta(\tilde{\tilde{S}}(\tilde{\tilde{k}} + \tilde{\tilde{\alpha}}) - \tilde{\tilde{S}}(\tilde{\tilde{k}}), 2^{tu} - 1) + \delta(\tilde{\tilde{S}}(\tilde{\tilde{k}} + \tilde{\tilde{\alpha}}) - \tilde{\tilde{S}}(\tilde{\tilde{k}}), 2^{tu} - 2^{n-tu} - 1) +$$

$$+ \delta(\tilde{\tilde{S}}(\tilde{\tilde{k}} + \tilde{\tilde{\alpha}}) - \tilde{\tilde{S}}(\tilde{\tilde{k}}), 2^{tu} - 2^{n-tu})\}.$$

Поскольку $2^{-(n-tu)} \sum\limits_{\tilde{k} \in V_{n-tu}} \delta(\tilde{S}(\tilde{k} + \tilde{\alpha} + \upsilon) - \tilde{S}(\tilde{k}) - \tau, r) \leq 1$, имеем

$$D^S(\alpha, \beta) \leq 2^{-tu} \sum_{\tilde{\tilde{k}} \in V_{tu}} \{\delta(\tilde{\tilde{S}}(\tilde{\tilde{k}} + \tilde{\tilde{\alpha}}) - \tilde{\tilde{S}}(\tilde{\tilde{k}}), 2^{tu} - 1) +$$

$$+ \delta(\tilde{\tilde{S}}(\tilde{\tilde{k}} + \tilde{\tilde{\alpha}}) - \tilde{\tilde{S}}(\tilde{\tilde{k}}), 2^{tu} - 2^{n-tu} - 1) + \delta(\tilde{\tilde{S}}(\tilde{\tilde{k}} + \tilde{\tilde{\alpha}}) - \tilde{\tilde{S}}(\tilde{\tilde{k}}), 2^{tu} - 2^{n-tu})\}.$$

Рассмотрим два возможных варианта: $\alpha^{(1)} = 0$ и $\alpha^{(1)} \neq 0$.

• Если $\alpha^{(1)} = 0$, то

$\delta(\tilde{\tilde{S}}(\tilde{\tilde{k}} + \tilde{\tilde{\alpha}}) - \tilde{\tilde{S}}(\tilde{\tilde{k}}), 2^{tu} - 1) = 0$, $\delta(\tilde{\tilde{S}}(\tilde{\tilde{k}} + \tilde{\tilde{\alpha}}) - \tilde{\tilde{S}}(\tilde{\tilde{k}}), 2^{tu} - 2^{n-tu} - 1) = 0$.

Обозначим для произвольного $\tilde{\tilde{\alpha}} \in V_n$: $i = \min\limits_{\overline{j=2, t}} \{\alpha^{(j)} \neq 0\}$. Тогда для $2 \leq i \leq t$ имеем

$$D^S(\alpha, \beta) \leq 2^{-tu} \sum_{\tilde{\tilde{k}} \in V_{tu}} \delta(\tilde{\tilde{S}}(\tilde{\tilde{k}} + \tilde{\tilde{\alpha}}) - \tilde{\tilde{S}}(\tilde{\tilde{k}}), 2^{tu} - 2^{n-tu}) \leq$$

$$\leq \max_{\overline{i=2, t}} \max_{\alpha^{(i)} \in V_u \setminus \{0\}} 2^{-u} \sum_{k \in V_u} \delta(S^{(i)}(k^{(i)} + \alpha^{(i)}) - S^{(i)}(k^{(i)}), q^{(i)}) = \Delta_{2, t}.$$

• Если $\alpha^{(1)} \neq 0$, то

$$D^S(\alpha, \beta) \leq 2^{-tu} \sum_{\tilde{\tilde{k}} \in V_{tu}} \delta(\tilde{\tilde{S}}(\tilde{\tilde{k}} + \tilde{\tilde{\alpha}}) - \tilde{\tilde{S}}(\tilde{\tilde{k}}), 2^{tu} - 1) + \delta(\tilde{\tilde{S}}(\tilde{\tilde{k}} + \tilde{\tilde{\alpha}}) - \tilde{\tilde{S}}(\tilde{\tilde{k}}), 2^{tu} - 2^{n-tu} - 1) \leq$$

$$\leq 2 \max_{\alpha^{(1)} \in V_u \setminus \{0\}} 2^{-u} \sum_{k \in V_u} \delta(S^{(1)}(k^{(1)} + \alpha^{(1)}) - S^{(1)}(k^{(1)}), 2^u - 1) \leq 2d^{S^{(1)}}.$$

Случай 2. Если $2^{n-tu} \leq q < 2^{tu} - 1$, то $\gamma_1 = (\tilde{\gamma}_1, \tilde{\tilde{\gamma}}_1) = (r, q)$, $\gamma_2 = (r, q+1)$, $\gamma_3 = (r, q - 2^{n-tu})$, $\gamma_4 = (r, q + 1 - 2^{n-tu})$. Тогда

$$D^S(\alpha, \beta) = 2^{-(n-tu)} \sum_{\tilde{k} \in V_{n-tu}} \delta(\tilde{S}(\tilde{k} + \tilde{\alpha} + \upsilon) - \tilde{S}(\tilde{k}) - \tau, r) \times$$

$$\times 2^{-tu} \sum_{\tilde{\tilde{k}} \in V_{tu}} \{\delta(\tilde{\tilde{S}}(\tilde{\tilde{k}} + \tilde{\tilde{\alpha}}) - \tilde{\tilde{S}}(\tilde{\tilde{k}}), q) + \delta(\tilde{\tilde{S}}(\tilde{\tilde{k}} + \tilde{\tilde{\alpha}}) - \tilde{\tilde{S}}(\tilde{\tilde{k}}), q+1) +$$

$$+ \delta(\tilde{\tilde{S}}(\tilde{\tilde{k}} + \tilde{\tilde{\alpha}}) - \tilde{\tilde{S}}(\tilde{\tilde{k}}), q - 2^{n-tu}) + \delta(\tilde{\tilde{S}}(\tilde{\tilde{k}} + \tilde{\tilde{\alpha}}) - \tilde{\tilde{S}}(\tilde{\tilde{k}}), q+1-2^{n-tu})\}.$$

Очевидно, что $2^{-(n-tu)} \sum_{\tilde{k} \in V_{n-tu}} \delta(\tilde{S}(\tilde{k} + \tilde{\alpha} + \upsilon) - \tilde{S}(\tilde{k}) - \tau, r) \le 1$,

$$D^S(\alpha, \beta) \le 2^{-tu} \sum_{\tilde{\tilde{k}} \in V_{tu}} \{\delta(\tilde{\tilde{S}}(\tilde{\tilde{k}} + \tilde{\tilde{\alpha}}) - \tilde{\tilde{S}}(\tilde{\tilde{k}}), q) + \delta(\tilde{\tilde{S}}(\tilde{\tilde{k}} + \tilde{\tilde{\alpha}}) - \tilde{\tilde{S}}(\tilde{\tilde{k}}), q+1) +$$

$$+ \delta(\tilde{\tilde{S}}(\tilde{\tilde{k}} + \tilde{\tilde{\alpha}}) - \tilde{\tilde{S}}(\tilde{\tilde{k}}), q - 2^{n-tu}) + \delta(\tilde{\tilde{S}}(\tilde{\tilde{k}} + \tilde{\tilde{\alpha}}) - \tilde{\tilde{S}}(\tilde{\tilde{k}}), q+1-2^{n-tu})\}. \qquad (6)$$

1. Пусть $\tilde{\tilde{\alpha}} \ne 0$. Обозначим: $\varepsilon_1 = q$, $\varepsilon_2 = q+1$, $\varepsilon_3 = q - 2^{n-tu}$, $\varepsilon_4 = q + 1 - 2^{n-tu}$, $\varepsilon_i = (\varepsilon_i^{(t)}, \ldots, \varepsilon_i^{(1)})$.

- Если $\alpha^{(1)} \ne 0$, то аналогично приведенным выше преобразованиям получим

$$D^S(\alpha, \beta) \le 2^{-(n-u)} \sum_{\tilde{k} \in V_{n-u}} \{\delta(\tilde{\tilde{S}}(\tilde{\tilde{k}} + \tilde{\tilde{\alpha}}) - \tilde{\tilde{S}}(\tilde{\tilde{k}}), \varepsilon_1) + \delta(\tilde{\tilde{S}}(\tilde{\tilde{k}} + \tilde{\tilde{\alpha}}) - \tilde{\tilde{S}}(\tilde{\tilde{k}}), \varepsilon_2) +$$

$$+ \delta(\tilde{\tilde{S}}(\tilde{\tilde{k}} + \tilde{\tilde{\alpha}}) - \tilde{\tilde{S}}(\tilde{\tilde{k}}), \varepsilon_3) + \delta(\tilde{\tilde{S}}(\tilde{\tilde{k}} + \tilde{\tilde{\alpha}}) - \tilde{\tilde{S}}(\tilde{\tilde{k}}), \varepsilon_4)\} \le$$

$$\le 2^{-u} \sum_{k \in V_u} \{\delta(S^{(1)}(k^{(1)} + \alpha^{(1)}) - S^{(1)}(k^{(1)}), \varepsilon_1^{(1)}) +$$

$$+ \delta(S^{(1)}(k^{(1)} + \alpha^{(1)}) - S^{(1)}(k^{(1)}), \varepsilon_2^{(1)}) +$$

$$+ \delta(S^{(1)}(k^{(1)} + \alpha^{(1)}) - S^{(1)}(k^{(1)}), \varepsilon_3^{(1)}) + \delta(S^{(1)}(k^{(1)} + \alpha^{(1)}) - S^{(1)}(k^{(1)}), \varepsilon_4^{(1)})\}.$$

Из определения дельта-функции очевидно, что из четырех слагаемых в фигурных скобках одновременно ненулевыми могут быть либо первое и третье, либо второе и четвертое.

Таким образом, справедлива следующая оценка:

$$D^S(\alpha, \beta) \le 2 \max_{\alpha^{(1)}, \varepsilon^{(1)} \in V_u \setminus \{0\}} 2^{-u} \sum_{k^{(1)} \in V_u} \delta(S^{(1)}(k^{(1)} + \alpha^{(1)}) - S^{(1)}(k^{(1)}), \varepsilon^{(1)}) \le 2d^{S^{(1)}}.$$

- Если $\alpha^{(1)} = 0$, то для $\alpha \in V_n$ выберем $\alpha^{(i)} \ne 0$: $i = \min_{j=\overline{2,t}} \{\alpha^{(j)} \ne 0\}$.

Заметим, что при $\alpha^{(1)} = 0$ имеем $\delta(\tilde{\tilde{S}}(\tilde{\tilde{k}} + \tilde{\tilde{\alpha}}) - \tilde{\tilde{S}}(\tilde{\tilde{k}}), \tilde{\tilde{\beta}}) \ne 0$ тогда и только тогда, когда $\beta^{(1)} = 0$.

Рассмотрим $\varepsilon_j^{(i)}$ — i-й справа блок в ε_j, $j = \overline{1, 4}$. Очевидно, в оценке (6) ненулевыми слагаемыми будут те, которые содержат либо $\varepsilon_1, \varepsilon_3$, либо $\varepsilon_2, \varepsilon_4$.

Предположим, что

$$2^{-u} \sum_{k \in V_u} \{\delta(S^{(i)}(k^{(i)} + \alpha^{(i)}) - S^{(i)}(k^{(i)}), \varepsilon_1^{(i)}) +$$

$$+ \delta(S^{(i)}(k^{(i)} + \alpha^{(i)}) - S^{(i)}(k^{(i)}), \varepsilon_3^{(i)})\} \ne 0$$

(в случае, если
$$2^{-u} \sum_{k \in V_u} \{\delta(S^{(i)}(k^{(i)} + \alpha^{(i)}) - S^{(i)}(k^{(i)}), \varepsilon_2^{(i)}) +$$

$$+ \delta(S^{(i)}(k^{(i)} + \alpha^{(i)}) - S^{(i)}(k^{(i)}), \varepsilon_4^{(i)})\} \ne 0,$$

оценка может быть построена аналогично). Тогда

$$2^{-u}\sum_{k^{(i)}\in V_u}\{\delta(S^{(i)}(k^{(i)}+\alpha^{(i)})-S^{(i)}(k^{(i)}),\varepsilon_1^{(i)})+$$

$$+\delta(S^{(i)}(k^{(i)}+\alpha^{(i)})-S^{(i)}(k^{(i)}),\varepsilon_3^{(i)})\}\le$$

$$\le 2^{-u}\left(\max_{\alpha^{(i)},\varepsilon_1^{(i)}\in V_u\setminus\{0\}}\sum_{k^{(i)}\in V_u}\delta(S^{(i)}(k^{(i)}+\alpha^{(i)})-S^{(i)}(k^{(i)}),\varepsilon_1^{(i)})+\right.$$

$$\left.+\max_{\alpha^{(i)},\varepsilon_3^{(i)}\in V_u\setminus\{0\}}\sum_{k^{(i)}\in V_u}\delta(S^{(i)}(k^{(i)}+\alpha^{(i)})-S^{(i)}(k^{(i)}),\varepsilon_3^{(i)})\right)\le$$

$$\le 2\max_{\alpha^{(i)},\varepsilon^{(i)}\in V_u\setminus\{0\}}2^{-u}\sum_{k^{(i)}\in V_u}\delta(S^{(i)}(k^{(i)}+\alpha^{(i)})-S^{(i)}(k^{(i)}),\varepsilon^{(i)})\le 2d^{S^{(i)}},$$

следовательно, $D^S(\alpha,\beta)\le \max_{i=\overline{2,t}}2d^{S^{(i)}}=2\Delta_{2,t}$.

2. Если $\tilde{\tilde{\alpha}}=0$, то при этом $\tilde{\alpha}\ne 0$. Тогда $\upsilon=0$, $\tau=0$ и $2^{-tu}\sum_{\tilde{\tilde{k}}\in V_{tu}}(\delta(\tilde{\tilde{S}}(\tilde{\tilde{k}})-\tilde{\tilde{S}}(\tilde{\tilde{k}}),\xi)\ne 0$ только при $\xi=0$. Для $\alpha\in V_n$ выберем $\alpha^{(i)}\ne 0$: $i=\min_{j=\overline{t+1,p}}\{\alpha^{(j)}\ne 0\}$. Тогда

$$D^S(\alpha,\beta)\le 2^{-n-tu}\max_{r,\alpha^{(p)}\in V_{n-tu}\setminus\{0\}}\sum_{k\in V_{n-tu}}\delta(\tilde{S}(\tilde{k}+\tilde{\alpha})-\tilde{S}(\tilde{k})),r)\le$$

$$\le\max_{i=\overline{t+1,p}}\max_{\alpha^{(i)}\in V_u\setminus\{0\}}2^{-u}\sum_{k\in V_u}\delta(S^{(i)}(k^{(i)}+\alpha^{(i)})-S^{(i)}(k^{(i)}),q^{(i)})=\Delta_{t+1,p}.$$

Случай 3. Если $0\le q<2^{n-tu}-1$, то $\gamma_1=(\tilde{\gamma}_1,\tilde{\tilde{\gamma}}_1)=(r,q)$, $\gamma_2=(r,q+1)$, $\gamma_3=(r-1,2^{tu}-2^{n-tu}+q)$, $\gamma_4=(r-1,2^{tu}-2^{n-tu}+q+1)$. Тогда

$$D^S(\alpha,\beta)=2^{-n-tu}\sum_{\tilde{k}\in V_{n-tu}}\{\delta(\tilde{S}(\tilde{k}+\tilde{\alpha}+\upsilon)-\tilde{S}(\tilde{k})-\tau,r)\}\times$$

$$\times 2^{-tu}\sum_{\tilde{\tilde{k}}\in V_{tu}}\{\delta(\tilde{\tilde{S}}(\tilde{\tilde{k}}+\tilde{\tilde{\alpha}})-\tilde{\tilde{S}}(\tilde{\tilde{k}}),q)+\delta(\tilde{\tilde{S}}(\tilde{\tilde{k}}+\tilde{\tilde{\alpha}})-\tilde{\tilde{S}}(\tilde{\tilde{k}}),q+1)\}+$$

$$+2^{-n-tu}\sum_{\tilde{k}\in V_u}\{\delta(\tilde{S}(\tilde{k}+\tilde{\alpha}+\upsilon)-\tilde{S}(\tilde{k})-\tau,r-1)\}\times$$

$$\times 2^{-tu}\sum_{\tilde{\tilde{k}}}\{\delta(\tilde{\tilde{S}}(\tilde{\tilde{k}}+\tilde{\tilde{\alpha}})-\tilde{\tilde{S}}(\tilde{\tilde{k}}),2^{tu}-2^{n-tu}+q)+$$

$$+\delta(\tilde{\tilde{S}}(\tilde{\tilde{k}}+\tilde{\tilde{\alpha}})-\tilde{\tilde{S}}(\tilde{\tilde{k}}),2^{tu}-2^{n-tu}+q+1)\}.\tag{7}$$

Легко заметить, что в данном случае одновременно либо $\delta(\tilde{S}(\tilde{k}+\tilde{\alpha}+\upsilon)-\tilde{S}(\tilde{k})-\tau,r)\ne 0$, либо $\delta(\tilde{S}(\tilde{k}+\tilde{\alpha}+\upsilon)-\tilde{S}(\tilde{k})-\tau,r-1)\ne 0$.

Если $\delta(\tilde{S}(\tilde{k}+\tilde{\alpha}+\upsilon)-\tilde{S}(\tilde{k})-\tau,r)\ne 0$ (во втором случае все оценки могут быть построены аналогично), либо $\delta(\tilde{\tilde{S}}(\tilde{\tilde{k}}+\tilde{\tilde{\alpha}})-\tilde{\tilde{S}}(\tilde{\tilde{k}}),q)\ne 0$, либо $\delta(\tilde{\tilde{S}}(\tilde{\tilde{k}}+\tilde{\tilde{\alpha}})-\tilde{\tilde{S}}(\tilde{\tilde{k}}),q+1)\ne 0$. Таким образом, выражение (7) содержит не более одного слагаемого и $\forall\alpha\in V_n\setminus\{0\}$, выбрав $\alpha^{(i)}\ne 0$: $i=\min_{j=\overline{1,p}}\{\alpha^{(j)}\ne 0\}$, получим

$$D^S(\alpha,\beta)\le\max_{j=\overline{1,p}}\max_{\alpha,\beta\in V_u\setminus\{0\}}2^{-u}\sum_{k\in V_u}\delta(S^{(j)}(k+\alpha)-S^{(j)}(k),\beta)\le\Delta_{1,p}.$$

Случай 4. Если $q = 2^{n-tu} - 1$, то $\gamma_1 = (\widetilde{\gamma}_1, \widetilde{\widetilde{\gamma}}_1) = (r, q)$, $\gamma_2 = (r, q+1)$, $\gamma_3 = (r-1, 2^{tu}-1)$, $\gamma_4 = (r, 0)$. Может быть построена оценка, аналогичная случаю 3:

$$D^S(\alpha, \beta) \le \max_{j=\overline{1,p}} \max_{\alpha, \beta \in V_u \setminus \{0\}} 2^{-u} \sum_{k \in V_u} \delta(S^{(j)}(k+\alpha) - S^{(j)}(k), \beta) \le \Delta_{1,p}.$$

Теорема доказана.

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

В табл. 1, 2 представлены результаты статистических распределений параметров (4), (5) для 8-битовых *s*-блоков. Для исследований сгенерировано 10 000 независимых равновероятных подстановок, для каждой из которых посчитаны значения соответствующих параметров. В табл. 1 приведено статистическое распределение параметра

$$\delta^{S^{(i)}} = \max_{\substack{\alpha \in V_u \setminus \{0\} \\ q \in V_u}} 2^{-u} \sum_{k \in V_u} \{\delta(S^{(i)}(k+\alpha) - S^{(i)}(k), q) + \delta(S^{(i)}(k+\alpha) - S^{(i)}(k), q+1)\},$$

в табл. 2 — статистическое распределение параметра

$$d^{S^{(j)}} = \max_{\alpha, \beta \in V_u \setminus \{0\}} 2^{-u} \sum_{k \in V_u} \delta(S^{(j)}(k+\alpha) - S^{(j)}(k), \beta).$$

Таблица 1

Значение параметра	Количество подстановок
0,03125	11
0,03515625	2415
0,0390625	5333
0,04296875	1847
0,046875	328
0,05078125	60
0,0546875	4
0,05859375	2

Таблица 2

Значение параметра	Количество подстановок
0,0195315	13
0,0234375	4744
0,0273438	4458
0,03125	724
0,0351563	57
0,0390625	3
0,0429688	1

ЗАКЛЮЧЕНИЕ

В результате статистических исследований распределений параметров (4), (5), в частности, для 8-битовых *s*-блоков найдены подстановки с наименьшими возможными значениями этих параметров. На основании полученных данных верхняя оценка средней вероятности целочисленного раундового дифференциала для отображения (2) при надлежащем выборе *s*-блоков может принимать значения, не превосходящие 0,04.

Отметим, что для отображения (2) достигается меньшее значение верхней оценки средней вероятности целочисленного раундового дифференциала, чем в случае, когда оператор перестановки является оператором циклического сдвига, величина которого взаимно проста с длиной входа *s*-блока, и при надлежащем выборе *s*-блоков будет выполняться неравенство $d_+^F(\alpha, \beta) \le 0{,}08$ (см. [14]).

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

СПИСОК ЛИТЕРАТУРЫ

1. 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.
2. 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. — С. 163–167.
3. 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. — С. 595–599.
4. 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.
5. 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. — С. 15–20.
6. 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.
7. National Institute of Standards and Technology: The Advanced Encryption Standard (AES). — http://csrc.nist.gov/aes/
8. ГОСТ 28147-89. Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования. — М.: Госстандарт СССР, 1989. — 28 с.
9. 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.
10. Горбенко І.Д., Бондаренко М.Ф., Долгов В.І. та ін. Перспективний блоковий шифр «Мухомор» — основні положення та специфікація // Там же. — 2007. — **6**, № 2. — С. 147–157.
11. Wang X., Yu H. How to break MD5 and other hash functions // Adv. Cryptology. EUROCRYPT'05; Lect. Notes in Computer Sci. — 2005. — **3494**. — P. 19–35.
12. Cotini S., Riverst R.L., Robshaw M.J.B., Yin Y.L. Security of the RC6TM block cipher. — http://www.rsasecurity.com/rsalabs/rc6/
13. Berson T.A. Differential cryptanalysis mod 2^{32} with applications to MD5 // Adv. Cryptology. CRYPTO'98 (LNCS). — 1999. — **372**. — P. 95–103.
14. Ковальчук Л.В. Построение верхних оценок средних вероятностей целочисленных дифференциалов композиции ключевого сумматора, блока подстановки и оператора сдвига // Кибернетика и системный анализ. — 2010. — № 6. — С. 89–96.

Поступила 07.12.2011