УДК 621.391:519.2

А.Н. АЛЕКСЕЙЧУК, А.С. ШЕВЦОВ

ВЕРХНИЕ ОЦЕНКИ НЕСБАЛАНСИРОВАННОСТИ БИЛИНЕЙНЫХ АППРОКСИМАЦИЙ РАУНДОВЫХ ФУНКЦИЙ БЛОЧНЫХ ШИФРОВ

Ключевые слова: *блочный шифр, статистическая атака, билинейный криптоанализ, билинейная аппроксимация булевой функции, ГОСТ 28147-89, «Калина».*

ВВЕДЕНИЕ

При исследовании стойкости блочных шифров относительно статистических методов криптоанализа требуется вычислять или оценивать значения параметров вида

$$l_*^{(\psi)}(f) = 2^{-m} \sum_{k \in V_m} \left(2^{-m} \sum_{x \in V_m} (-1)^{f(x, \psi(x * k))} \right)^2, \tag{1}$$

где $\psi = (s_0, \ldots, s_{p-1})$ — подстановка на множестве $V_m = \{0, 1\}^m$, заданная с помощью набора подстановок (s-блоков) $s_i : V_t \to V_t$, $i = \overline{0, p-1}$, $pt = m$, $*$ — коммутативная групповая операция на множестве V_m, а f — функция, принадлежащая некоторому классу Ф булевых функций $2m$ переменных. Обычно функцию f называют аппроксимацией (между входами и выходами) булева отображения $x \mapsto \psi(x * k)$, $x \in V_m$, которое используется в конструкции раундовой функции данного блочного шифра, а значение (1) — (средней) несбалансированностью указанной аппроксимации. При этом класс Ф аппроксимирующих функций, как правило, определяется конкретным методом криптоанализа. Так, в случае линейного криптоанализа [1] $f = f(x, y)$ является линейной булевой функцией, существенно зависящей от каждого аргумента $x, y \in V_m$; для обобщенного линейного криптоанализа [2] $f(x, y) = g(x) \oplus h(y)$, $x, y \in V_m$, где g и h — уравновешенные булевы функции m переменных; билинейный метод криптоанализа [3] связан с классом билинейных булевых функций и т.д. Отметим работы [4, 5], в которых предложены общие подходы к построению перечисленных (и других) статистических методов криптоанализа блочных шифров. Верхние оценки надежности статистических атак на блочные шифры получены в [4] и усилены в [6] для случая атак первого порядка.

Заметим, что на практике нахождение нетривиальных оценок параметра (1), за исключением отдельных специальных случаев, представляет собой непростую задачу, поскольку m является достаточно большим числом (например, m равно 64 или 128). В [7] получены верхние оценки параметра (1), явно зависящие от числовых характеристик s-блоков s_i, $i = \overline{0, p-1}$, в случае, когда $*$ — операция сложения по модулю 2^m на множестве двоичных целых чисел, соответствующих векторам из V_m, а f — линейная булева функция. Эти оценки использованы в [7–9] для нахождения верхних границ вероятностей линейных характеристик широкого класса блочных шифров, построенных с использованием ключевого сумматора по модулю 2^m, подобных алгоритмам шифрования ГОСТ [10] и «Калина» [11] (отметим, что последний из них является кандидатом на Национальный стандарт шифрования Украины). В частности, применение указанных границ к шифру «Калина» [9] позволило обосновать его практическую стойкость относительно линейного метода криптоанализа без использования каких-либо упрощающих предположений. Верхние оценки параметра (1) для более широкого класса «обобщенно-линейных» функций ($f(x, y) = g_0(x_0) \oplus \ldots \oplus g_{p-1}(x_{p-1}) \oplus h_0(y_0) \oplus \ldots \oplus h_{p-1}(y_{p-1})$, где

$x=(x_0,\ldots,x_{p-1})$, $y=(y_0,\ldots,y_{p-1})$, $x_i, y_i \in V_t$, $g_i, h_i: V_t \to \{0,1\}$, $i=\overline{0, p-1}$) и указанной выше операции $*$ получены в [12].

В настоящей статье решается задача построения верхних границ параметра (1) для билинейных булевых фунций f. Полученные результаты обобщают ранее известные оценки [7] несбалансированности линейных аппроксимаций отображений рассматриваемого вида и позволяют оценивать значения (1) при достаточно слабых ограничениях на аппроксимирущую функцию f или операцию $*$.

Результаты применения полученных оценок к исследованию свойств раундовых функций шифров ГОСТ и «Калина» авторы предполагают изложить в отдельной статье. Актуальной задачей дальнейших исследований является обобщение представленных ниже теорем на более широкий класс криптографических преобразований, построенных на основе ряда управляемых двухместных подстановочных операций [13].

ПОСТАНОВКА ЗАДАЧИ И ФОРМУЛИРОВКИ ОСНОВНЫХ РЕЗУЛЬТАТОВ

Далее используются следующие обозначения: V_m — множество булевых векторов длины m; S^{V_m} — симметрическая группа подстановок на множестве V_m; F_m — кольцо матриц размера $m\times m$ над полем $F=\mathbf{GF}(2)$. Будем отождествлять произвольный вектор $x=(x_1,\ldots,x_m)\in V_m$ с целым числом $x=2^{m-1}x_1+\ldots+2^0 x_m$ и обозначать $x\overset{m}{+}y$ (или $x+y$, если значение m однозначно определено контекстом) сумму по модулю 2^m двоичных чисел, соответствующих векторам $x, y\in V_m$. Символом xy обозначим скалярное произведение над полем F векторов $x=(x_1,\ldots,x_m)$ и $y=(y_1,\ldots,y_m)$: $xy=x_1y_1\oplus\ldots\oplus x_m y_m$. Наконец, для любой двоичной $m\times n$-матрицы U обозначим $S(U)$ и $C(U)$ подпространства векторных пространств V_n и V_m, порожденные соответственно строками и столбцами матрицы U.

Для любых $m\in\mathbf{N}$, $\psi\in S^{V_m}$, $A\in F_m$, $\alpha,\beta\in V_m$ и произвольной бинарной алгебраической операции $*$ на множестве V_m положим

$$l_*^{(\psi)}(A,\alpha,\beta)=2^{-m}\sum_{k\in V_m}\left((2^{-m}\sum_{x\in V_m}\chi(xA\psi(x*k)\oplus\alpha x\oplus\beta\psi(x*k))\right)^2, \tag{2}$$

где $\chi(u)=(-1)^u$, $u\in\{0,1\}$; в случае, когда $*\in\{+,\oplus\}$, обозначим

$$\Lambda_*^{(\psi)}(A,\alpha,\beta)=2^{-m}\sum_{k\in V_m}\left(2^{-m}\sum_{a\in\{0,1\}}\left|\sum_{\substack{x\in V_m:\\ \nu(x,k)=a}}\chi(xA\psi(x*k)\oplus\alpha x\oplus\beta\psi(x*k))\right|\right)^2, \tag{3}$$

где для любых $m\in\mathbf{N}$, $x,k\in V_m$

$$\nu(x,k)=\begin{cases}\text{бит переноса в } m\text{-й разряд суммы чисел } x \text{ и } k\\ \text{в кольце } \mathbf{Z}, \text{ если } *=+;\\ 0, \text{ если } *=\oplus.\end{cases} \tag{4}$$

Отметим, что параметр (1) совпадает с параметром (2), если f является билинейной функцией: $f(x,y)=xAy\oplus\alpha x\oplus\beta y$, $x,y\in V_m$. Кроме того, если $*=\oplus$, то параметры (2) и (3) совпадают.

Предположим, что подстановка ψ имеет вид

$$\psi(x)=\psi(x_2,x_1)=(\psi_2(x_2),\psi_1(x_1)),\ x_1\in V_t,\ x_2\in V_{m-t}, \tag{5}$$

где $\psi_1\in S^{V_t}$, $\psi_2\in S^{V_{m-t}}$, $1\le t\le m-1$. Требуется получить верхние оценки параметра (2), зависящие непосредственно от подстановок ψ_1 и ψ_2.

Для решения поставленной задачи представим матрицу $A \in F_m$ в блочном виде:

$$A = \begin{pmatrix} A_2 & U \\ V & A_1 \end{pmatrix}, \; A_1 \in F_t, \; A_2 \in F_{m-t}; \tag{6}$$

аналогично запишем векторы α и β: $\alpha = (\alpha_2, \alpha_1)$, $\beta = (\beta_2, \beta_1)$, где $\alpha_1, \beta_1 \in V_t$, $\alpha_2, \beta_2 \in V_{m-t}$. В [7] показано, что в частном случае при $A = 0$ выполняется неравенство

$$l_+^{(\psi)}(0, \alpha, \beta) \le \Lambda_+^{(\psi_1)}(0, \alpha_1, \beta_1) l_+^{(\psi_2)}(0, \alpha_2, \beta_2). \tag{7}$$

Следующая теорема обобщает этот результат.

Теорема 1. Для любых векторов $\alpha, \beta \in V_m$, подстановки ψ вида (5), матрицы A вида (6) и операции $* \in \{+, \oplus\}$ справедливы неравенства

$$l_*^{(\psi)}(A, \alpha, \beta) \le \Lambda_*^{(1)} \max_{\substack{u \in C(U), \\ v \in S(V)}} l_*^{(\psi_2)}(A_2, \alpha_2 \oplus u, \beta_2 \oplus v), \tag{8}$$

$$l_*^{(\psi)}(A, \alpha, \beta) \le \Lambda_*^{(2)} \max_{\substack{u' \in S(U), \\ v' \in C(V)}} \Lambda_*^{(\psi_1)}(A_1, \alpha_1 \oplus v', \beta_1 \oplus u'), \tag{9}$$

где

$$\Lambda_*^{(1)} = 2^{-t} \sum_{k_1 \in V_t} \left(\sum_{\substack{b_2 \in S(V), \\ c_2 \in C(U)}} (|u_{k_1}(0, b_2, c_2)| + |u_{k_1}(1, b_2, c_2)|) \right)^2 \tag{10}$$

и для любых $a \in \{0, 1\}$, $k_1 \in V_t$, $b_2 \in S(V)$, $c_2 \in C(U)$

$$u_{k_1}(a, b_2, c_2) = 2^{-t} \sum_{x_1 \in S_{k_1}(a, b_2, c_2)} \chi(x_1 A_1 \psi_1(x_1 * k_1) \oplus \alpha_1 x_1 \oplus \beta_1 \psi_1(x_1 * k_1)), \tag{11}$$

$$S_{k_1}(a, b_2, c_2) = \{x_1 \in V_t : \nu(x_1, k_1) = a, \; x_1 V = b_2, \; U\psi_1(x_1 * k_1) = c_2\}; \tag{12}$$

$$\Lambda_*^{(2)} = 2^{-(m-t)} \sum_{k_1 \in V_{m-t}} \left(\sum_{\substack{b_1 \in C(V), \\ c_1 \in S(U)}} \max\{|v_{k_2}(0, b_1, c_1)|, |v_{k_2}(1, b_1, c_1)|\} \right)^2 \tag{13}$$

и для любых $a \in \{0, 1\}$, $k_2 \in V_{m-t}$, $b_1 \in C(V)$, $c_1 \in S(U)$

$$v_{k_2}(a, b_1, c_1) = 2^{-(m-t)} \sum_{x_2 \in S'_{k_2}(a, b_1, c_1)} \chi(x_2 A_2 \psi_2(x_2 * k_2 * \nu(a, 1)) \oplus$$

$$\oplus \alpha_2 x_2 \oplus \beta_2 \psi_2(x_2 * k_2 * \nu(a, 1))), \tag{14}$$

$$S'_{k_2}(a, b_1, c_1) = \{x_2 \in V_{m-t} : V\psi_2(x_2 * k_2 * \nu(a, 1)) = b_1, x_2 U = c_1\}. \tag{15}$$

Приведем ряд следствий, вытекающих из этой теоремы. Прежде всего, отметим, что в случае, когда $* = +$ и $A = 0$, параметр (10) совпадает с параметром $\Lambda_+^{(\psi_1)}(0, \alpha_1, \beta_1)$, который определяется в соответствии с формулой (3). Следовательно, в этом случае неравенство (8) сводится к неравенству (7), которое получено в [7]. Далее, на основании (10)–(12) справедливо неравенство $\Lambda_*^{(1)} \le 1$, $* \in \{+, \oplus\}$, из которого следует, что значение параметра (2) не превосходит значения второго сомножителя в правой части неравенства (8). Таким образом, справедливо следующее утверждение.

Следствие 1. В условиях теоремы 1 имеет место неравенство

$$l_*^{(\psi)}(A,\alpha,\beta) \le \max_{\substack{u \in C(U),\\ v \in S(V)}} l_*^{(\psi_2)}(A_2,\alpha_2 \oplus u, \beta_2 \oplus v). \tag{16}$$

Рассмотрим неравенство (9) и оценим первый сомножитель в его правой части. Пусть $* = \oplus$; тогда на основании (4), (14) для любых $k_2 \in V_{m-t}$, $b_1 \in C(V)$, $c_1 \in S(U)$ выполняется равенство $v_{k_2}(0,b_1,c_1) = v_{k_2}(1,b_1,c_1)$, из которого следует, что $\Lambda_\oplus^{(2)} \le 1$. Пусть $* = +$; тогда в силу неравенства

$$\max\{|v_{k_2}(0,b_1,c_1)|, |v_{k_2}(1,b_1,c_1)|\} \le |v_{k_2}(0,b_1,c_1)| + |v_{k_2}(1,b_1,c_1)|$$

и формул (13)–(15) справедлива оценка $\Lambda_+^{(2)} \le 4$. При этом в случае, когда хотя бы одна из матриц, U или V, в формуле (6) нулевая, имеет место более сильная оценка

$$\Lambda_+^{(2)} \le 1. \tag{17}$$

Действительно, если $U = 0$, то на основании формул (14), (15) для любых $a \in \{0,1\}$, $k_2 \in V_{m-t}$, $b_1 \in C(V)$, $c_1 \in S(U)$ справедливо соотношение

$$|v_{k_2}(a,b_1,c_1)| \le 2^{-(m-t)} |S'_{k_2}(a,b_1,c_1)| = 2^{-\operatorname{rank}(V)}.$$

Если $V = 0$, то, согласно тем же формулам,

$$|v_{k_2}(a,b_1,c_1)| \le 2^{-\operatorname{rank}(U)},\ a \in \{0,1\},\ k_2 \in V_{m-t},\ b_1 \in C(V),\ c_1 \in S(U).$$

Отсюда на основании (10) следует справедливость (17).

Суммируя изложенное выше, получаем следующий результат.

Следствие 2. В условиях теоремы 1 справедливы неравенства

$$l_\oplus^{(\psi)}(A,\alpha,\beta) \le \max_{\substack{u' \in S(U),\\ v' \in C(V)}} l_\oplus^{(\psi_1)}(A_1,\alpha_1 \oplus v', \beta_1 \oplus u'), \tag{18}$$

$$l_+^{(\psi)}(A,\alpha,\beta) \le 4 \max_{\substack{u' \in S(U),\\ v' \in C(V)}} \Lambda_+^{(\psi_1)}(A_1,\alpha_1 \oplus v', \beta_1 \oplus u'). \tag{19}$$

Кроме того, если в формуле (6) $U = 0$ или $V = 0$, то

$$l_+^{(\psi)}(A,\alpha,\beta) \le \max_{\substack{u' \in S(U),\\ v' \in C(V)}} \Lambda_+^{(\psi_1)}(A_1,\alpha_1 \oplus v', \beta_1 \oplus u'). \tag{20}$$

Отметим, что теорема 1 и следствия из нее сводят задачу нахождения верхних оценок параметра (2) для произвольной матрицы A порядка m и векторов $\alpha, \beta \in V_m$ к построению аналогичных оценок параметров (2), (3), (10), (13), зависящих от подматриц матрицы A меньшего размера и соответствующих «частей» векторов α и β. В ряде случаев оценки (16), (18)–(20) можно использовать многократно, применяя их последовательно к подматрицам, расположенным на главной диагонали матрицы A.

Пусть подстановка ψ представляет собой набор s-блоков:

$$\psi = (s_0, \ldots, s_{p-1}), \tag{21}$$

где $s_i \in S^{V_t}$, $i = \overline{0, p-1}$, $pt = m$. Запишем матрицу A в виде $A = (A_{ij})_{i,j=\overline{0,p-1}}$, где $A_{ij} \in F_t$; аналогично представим векторы α и β: $\alpha = (\alpha_0, \ldots, \alpha_{p-1})$, $\beta = (\beta_0, \ldots, \beta_{p-1})$, где $\alpha_j, \beta_j \in V_t$, $j = \overline{0, p-1}$. Для любого $i = \overline{0, p-1}$ обозначим $C_i(A)$ и $S_i(A)$ подпространства векторного пространства V_t, порожденные столбцами матриц A_{ij} и соответственно строками матриц A_{ji} по всем $j \ne i$.

Предположим вначале, что A является блочно-диагональной матрицей:

$$A = \mathrm{diag}(A_{00}, \dots, A_{p-1p-1}), \; A_{ii} \in F_t, \; i = \overline{0, p-1}. \tag{22}$$

Применяя последовательно неравенство (16) и $p-2$ раз неравенство (20) к соответствующим подматрицам матрицы (22), получаем следующий результат.

Следствие 3. При выполнении соотношений (21), (22) справедливо неравенство

$$l_{+}^{(\psi)}(A, \alpha, \beta) \le l_{+}^{(s_0)}(A_{00}, \alpha_0, \beta_0) \prod_{i=1}^{p-1} \Lambda_{+}^{(s_i)}(A_{ii}, \alpha_i, \beta_i),$$

которое обращается в равенство, если $A_{ii} = 0$, $\alpha_i = \beta_i = 0$ для всех $i = \overline{1, p-1}$.

В общем случае справедлива следующая теорема, устанавливающая верхние границы параметра (2) в терминах числовых параметров подстановок $s_0, \dots, s_{p-1}$.

Теорема 2. Пусть подстановка ψ имеет вид (21). Тогда для любых $A \in F_m$, $\alpha, \beta \in V_m$ справедливы неравенства

$$l_{\oplus}^{(\psi)}(A, \alpha, \beta) \le \min_{i = \overline{0, p-1}} \max_{\substack{u \in C_i(A), \\ v \in S_i(A)}} l_{\oplus}^{(s_i)}(A_{ii}, \alpha_i \oplus u, \beta_i \oplus v), \tag{23}$$

$$l_{+}^{(\psi)}(A, \alpha, \beta) \le 4 \min_{i = \overline{0, p-1}} \max_{\substack{u \in C_i(A), \\ v \in S_i(A)}} \Lambda_{+}^{(s_i)}(A_{ii}, \alpha_i \oplus u, \beta_i \oplus v). \tag{24}$$

Кроме того, если A — блочно-треугольная матрица (т.е. $A_{ij} = 0$ для любых $0 \le i < j \le p-1$ или $A_{ji} = 0$ для любых $0 \le i < j \le p-1$), то

$$l_{+}^{(\psi)}(A, \alpha, \beta) \le \min_{i = \overline{0, p-1}} \max_{\substack{u \in C_i(A), \\ v \in S_i(A)}} \Lambda_{+}^{(s_i)}(A_{ii}, \alpha_i \oplus u, \beta_i \oplus v). \tag{25}$$

Рассмотрим задачу нахождения оценок параметра (2) в несколько более общей постановке. Предположим, что операция $*$ на множестве V_m определяется по формуле

$$(x_2, x_1) * (k_2, k_1) = (x_2 \overset{(2)}{*} k_2, \; x_1 \overset{(1)}{*} k_1), \; x_1, k_1 \in V_t, \; x_2, k_2 \in V_{m-t}, \tag{26}$$

где $\overset{(1)}{*}$ и $\overset{(2)}{*}$ — произвольные бинарные алгебраические операции на множествах V_t и V_{m-t} соответственно, $1 \le t \le m-1$. Справедлива следующая теорема.

Теорема 3. При выполнении равенств (5), (6), (26) параметр (2) удовлетворяет соотношениям

$$l_{*}^{(\psi)}(A, \alpha, \beta) \le \max_{\substack{u \in C(U), \\ v \in S(V)}} l_{\overset{(2)}{*}}^{(\psi_2)}(A_2, \alpha_2 \oplus u, \beta_2 \oplus v),$$

$$l_{*}^{(\psi)}(A, \alpha, \beta) \le \max_{\substack{u' \in S(U), \\ v' \in C(V)}} l_{\overset{(1)}{*}}^{(\psi_1)}(A_1, \alpha_1 \oplus v', \beta_1 \oplus u').$$

Отметим, что последние две теоремы позволяют оценивать сверху значения (2) для любой подстановки ψ вида (21), произвольной матрицы $A \in F_m$ и операции $*$ вида

$$(x_1, \dots, x_n) * (k_1, \dots, k_n) = (x_1 \overset{m_1}{+} k_1, \dots, x_n \overset{m_n}{+} k_n), \; x_i, k_i \in V_{m_i}, \; i = \overline{1, n},$$

где числа $m_1, \dots, m_n$ делятся на t, $m_1 + \dots + m_n = m$.

ДОКАЗАТЕЛЬСТВА ТЕОРЕМ

Доказательство теоремы 1. Получим вспомогательное соотношение для внутренней суммы в правой части равенства (2), используя которое докажем неравенства (8), (9).

Пусть $x = x_1 + 2^t x_2$ и $k = k_1 + 2^t k_2$ — целые числа, соответствующие булевым векторам (x_2, x_1) и (k_2, k_1) соответственно, $x_1, k_1 \in V_t$, $x_2, k_2 \in V_{m-t}$. Справедливы равенства

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

которые с учетом формулы (4) можно записать в виде

$$x * k = (x_2 * k_2 * \nu(x_1, k_1), x_1 * k_1), \; * \in \{+, \oplus\}.$$

Отсюда на основании формулы (5) вытекает равенство

$$\psi(x * k) = (\psi_2(x_2 * k_2 * \nu(x_1, k_1)), \psi_1(x_1 * k_1)), \; x, k \in V_m. \tag{27}$$

Для любых $A \in F_m$, $\alpha, \beta \in V_m$, $k = (k_2, k_1)$, где $k_1 \in V_t$, $k_2 \in V_{m-t}$, обозначим

$$l_{k_1, k_2}^{(\psi)}(A, \alpha, \beta) = 2^{-m} \sum_{x \in V_m} \chi(xA\psi(x * k) \oplus \alpha x \oplus \beta\psi(x * k)) \tag{28}$$

внутреннюю сумму в правой части равенства (2). Используя формулы (6), (27), получаем следующее выражение параметра (28):

$$l_{k_1, k_2}^{(\psi)}(A, \alpha, \beta) = 2^{-m} \sum_{x_1 \in V_t, x_2 \in V_{m-t}} \chi(x_2 A_2 \psi_2(x_2 * k_2 * \nu(x_1, k_1))) \chi(x_1 A_1 \psi_1(x_1 * k_1)) \times$$

$$\times \chi(\beta_2 \psi_2(x_2 * k_2 * \nu(x_1, k_1)) \oplus \alpha_2 x_2) \chi(\beta_1 \psi_1(x_1 * k_1) \oplus \alpha_1 x_1) \times$$

$$\times \chi(x_1 V \psi_2(x_2 * k_2 * \nu(x_1, k_1)) \oplus x_2 U \psi_1(x_1 * k_1)). \tag{29}$$

Докажем неравенство (8). Обозначим в формуле (29) $a = \nu(x_1, k_1)$, $b_2 = x_1 V$, $c_2 = U\psi_1(x_1 * k_1)$ и запишем ее таким образом:

$$l_{k_1, k_2}^{(\psi)}(A, \alpha, \beta) = \sum_{\substack{a \in \{0,1\}, \\ b_2 \in S(V), \\ c_2 \in C(U)}} 2^{-t} \sum_{x_1 \in S_{k_1}(a, b_2, c_2)} \chi(x_1 A_1 \psi_1(x_1 * k_1) \oplus \alpha_1 x_1 \oplus \beta_1 \psi_1(x_1 * k_1)) \times$$

$$\times 2^{-(m-t)} \sum_{x_2 \in V_{m-t}} \chi(x_2 A_2 \psi_2(x_2 * k_2 * a) \oplus (\alpha_2 \oplus c_2) x_2 \oplus (\beta_2 \oplus b_2) \psi_2(x_2 * k_2 * a)) =$$

$$= \sum_{\substack{a \in \{0, 1\}, \\ b_2 \in S(V), \\ c_2 \in C(U)}} u_{k_1}(a, b_2, c_2) u'_{k_2}(a, b_2, c_2). \tag{30}$$

Здесь для любых $a \in \{0, 1\}$, $k_2 \in V_{m-t}$, $b_2 \in S(V)$, $c_2 \in C(U)$ имеем

$$u'_{k_2}(a, b_2, c_2) = 2^{-(m-t)} \sum_{x_2 \in V_{m-t}} \chi(x_2 A_2 \psi_2(x_2 * k_2 * a) \oplus$$

$$\oplus (\alpha_2 \oplus c_2) x_2 \oplus (\beta_2 \oplus b_2) \psi_2(x_2 * k_2 * a)), \tag{31}$$

а значения $u_{k_1}(a, b_2, c_2)$ и $S_{k_1}(a, b_2, c_2)$ определяются по формулам (11) и (12) соответственно.

Положим $u_{k_1} = \sum_{\substack{b_2 \in S(V), \\ c_2 \in C(U)}} (|u_{k_1}(0, b_2, c_2)| + |u_{k_1}(1, b_2, c_2)|)$, $k_1 \in V_t$. На основании равенства (30) и выпуклости вниз функции $x \mapsto x^2$, $x \in \mathbf{R}$, справедливы следующие неравенства:

$$(l_{k_1,k_2}^{(\psi)}(A,\alpha,\beta))^2 \le \left(\sum_{\substack{a\in\{0,1\},\\ b_2\in S(V),\\ c_2\in C(U)}} |u_{k_1}(a,b_2,c_2)|\,|u'_{k_1}(a,b_2,c_2)| \right)^2 \le$$

$$\le u_{k_1} \sum_{\substack{a\in\{0,1\},\\ b_2\in S(V),\\ c_2\in C(U)}} |u_{k_1}(a,b_2,c_2)|(u'_{k_2}(a,b_2,c_2))^2,\ k_1\in V_t,\ k_2\in V_{m-t}.$$

Отсюда на основании (2) и (28) вытекает

$$l_*^{(\psi)}(A,\alpha,\beta)\le$$

$$\le 2^{-t}\sum_{k_1\in V_t} u_{k_1}\left(\sum_{\substack{a\in\{0,1\},\\ b_2\in S(V),\\ c_2\in C(U)}} |u_{k_1}(a,b_2,c_2)|\,2^{-(m-t)} \sum_{k_2\in V_{m-t}} (u'_{k_2}(a,b_2,c_2))^2 \right). \quad (32)$$

Далее, согласно (31) для любых $a\in\{0,1\}$, $b_2\in S(V)$, $c_2\in C(U)$ выполняются соотношения

$$2^{-(m-t)}\sum_{k_2\in V_{m-t}} (u'_{k_2}(a,b_2,c_2))^2 = 2^{-(m-t)}\sum_{k_2\in V_{m-t}} (2^{-(m-t)}\sum_{x_2\in V_{m-t}} \chi(x_2A_2\psi_2(x_2*k_2)\oplus$$

$$\oplus(\alpha_2\oplus c_2)x_2\oplus(\beta_2\oplus b_2)\psi_2(x_2*k_2)))^2 \le \max_{\substack{u\in C(U),\\ v\in S(V)}} l_*^{(\psi_2)}(A_2,\alpha_2\oplus u,\beta_2\oplus v).$$

Следовательно, на основании (32) получаем

$$l_*^{(\psi)}(A,\alpha,\beta)\le 2^{-t}\sum_{k_1\in V_t}\left(\sum_{\substack{a\in\{0,1\},\\ b_2\in S(V),\\ c_2\in C(U)}} |u_{k_1}(a,b,c)| \right)^2 \max_{\substack{u\in C(U),\\ v\in S(V)}} l_*^{(\psi_2)}(A_2,\alpha_2\oplus u,\beta_2\oplus v).$$

Из последнего неравенства и формулы (10) следует неравенство (8), что и требовалось доказать.

Убедимся в справедливости неравенства (9). Обозначим в формуле (29) $a=\nu(x_1,k_1)$, $b_1=V\psi_2(x_2*k_2*\nu(x_1,k_1))$, $c_1=x_2U$ и запишем ее следующим образом:

$$l_{k_1,k_2}^{(\psi)}(A,\alpha,\beta)=\sum_{\substack{a\in\{0,1\},\\ b_1\in C(V),\\ c_1\in S(U)}} 2^{-t}\sum_{\substack{x_1\in V_t:\\ \nu(x_1,k_1)=a}} \chi(x_1A_1\psi_1(x_1*k_1)\oplus$$

$$\oplus(\alpha_1\oplus b_1)x_1\oplus(\beta_1\oplus c_1)\psi_1(x_1*k_1))\times$$

$$\times 2^{-(m-t)}\sum_{x_2\in\widetilde{S}_{k_2}(a,b_1,c_1)} \chi(x_2A_2\psi_2(x_2*k_2*a)\oplus\alpha_2x_2\oplus\beta_2\psi_2(x_2*k_2*a)). \quad (33)$$

Здесь для любых $a\in\{0,1\}$, $k_2\in V_{m-t}$, $b_1\in C(V)$, $c_1\in S(U)$ множество $\widetilde{S}_{k_2}(a,b_1,c_1)$ состоит из всех векторов $x_2\in V_{m-t}$, которые удовлетворяют условиям $V\psi_2(x_2*k_2*a)=b_1$, $x_2U=c_1$.

Заметим, что на основании (4), (33) выполняется равенство

$$l_{k_1,k_2}^{(\psi)}(A,\alpha,\beta)=\sum_{\substack{b_1\in C(V),\\ c_1\in S(U)}}(v'_{k_1}(0,b_1,c_1)v_{k_2}(0,b_1,c_1)+v'_{k_1}(1,b_1,c_1)v_{k_2}(1,b_1,c_1)), \quad (34)$$

где для любых $a\in\{0,1\}$, $k_1\in V_t$, $b_1\in C(V)$, $c_1\in S(U)$

$$v'_{k_1}(a,b_1,c_1)=2^{-t}\sum_{\substack{x_1\in V_t:\\ \nu(x_1,k_1)=a}}\chi(x_1A_1\psi_1(x_1*k_1)\oplus$$

$$\oplus(\alpha_1\oplus b_1)x_1\oplus(\beta_1\oplus c_1)\psi_1(x_1*k_1)), \quad (35)$$

а $v_{k_2}(a,b_1,c_1)$ определяется по формуле (14). Действительно, если $*=+$, то $\nu(a,1)=a$ для любого $a\in\{0,1\}$, множество $\widetilde{S}_{k_2}(a,b_1,c_1)$ совпадает с множеством (15) и формула (34) вытекает из равенства (33). Если $*=\oplus$, то $\nu(a,1)=$ $=\nu(x_1,k_1)=0$ для любых $a\in\{0,1\}$, x_1, $k_1\in V_t$. Следовательно, в этом случае

$$l_{k_1,k_2}^{(\psi)}(A,\alpha,\beta)=$$

$$=\sum_{\substack{b_1\in C(V),\\ c_1\in S(U)}}2^{-t}\sum_{x_1\in V_t}\chi(x_1A_1\psi_1(x_1*k_1)\oplus(\alpha_1\oplus b_1)x_1\oplus(\beta_1\oplus c_1)\psi_1(x_1*k_1))\times$$

$$\times 2^{-(m-t)}\sum_{x_2\in\widetilde{S}_{k_2}(0,b_1,c_1)}\chi(x_2A_2\psi_2(x_2*k_2)\oplus\alpha_2x_2\oplus\beta_2\psi_2(x_2*k_2)),$$

что вследствие (14), (15) и (35) совпадает с выражением в правой части равенства (34).

Для любых $k_1\in V_t$, $k_2\in V_{m-t}$, $b_1\in C(V)$, $c_1\in S(U)$ положим

$$v'_{k_1}(b_1,c_1)=\left|v'_{k_1}(0,b_1,c_1)\right|+\left|v'_{k_1}(1,b_1,c_1)\right|, \quad (36)$$

$$v_{k_2}(b_1,c_1)=\max\left\{\left|v_{k_2}(0,b_1,c_1)\right|,\ \left|v_{k_2}(1,b_1,c_1)\right|\right\}. \quad (37)$$

На основании (34) и выпуклости вниз квадратичной функции справедливы неравенства

$$(l_{k_1,k_2}^{(\psi)}(A,\alpha,\beta))^2\le\left(\sum_{\substack{b_1\in C(V),\\ c_1\in S(U)}}v'_{k_1}(b_1,c_1)v_{k_2}(b_1,c_1)\right)^2\le$$

$$\le\left(\sum_{\substack{b_1\in C(V),\\ c_1\in S(U)}}(v'_{k_1}(b_1,c_1))^2v_{k_2}(b_1,c_1)\right)\left(\sum_{\substack{\widetilde{b}_1\in C(V),\\ \widetilde{c}_1\in S(U)}}v_{k_2}(\widetilde{b}_1,\widetilde{c}_1)\right).$$

Отсюда согласно формулам (2), (13), (28) и (35)–(37) имеем следующие соотношения:

$$l_*^{(\psi)}(A,\alpha,\beta)=2^{-m}\sum_{\substack{k_1\in V_t,\\ k_2\in V_{m-t}}}(l_{k_1,k_2}^{(\psi)}(A,\alpha,\beta))^2\le$$

$$\le\sum_{\substack{b_1\in C(V),\\ c_1\in S(U)}}\left(2^{-t}\sum_{k_1\in V_t}(v'_{k_1}(b_1,c_1))^2\right)\left(2^{-(m-t)}\sum_{k_2\in V_{m-t}}\sum_{\substack{\widetilde{b}_1\in C(V),\\ \widetilde{c}_1\in S(U)}}v_{k_2}(\widetilde{b}_1,\widetilde{c}_1)v_{k_2}(b_1,c_1)\right)\le$$

$$\leq 2^{-(m-t)} \sum_{k_2 \in V_{m-t}} \left(\sum_{\substack{\widetilde{b}_1 \in C(V), \\ \widetilde{c}_1 \in S(U)}} v_{k_2}(\widetilde{b}_1, \widetilde{c}_1) \sum_{\substack{b_1 \in C(V), \\ c_1 \in S(U)}} v_{k_2}(b_1, c_1) \right) \max_{\substack{u' \in S(U), \\ v' \in C(V)}} \left\{ 2^{-t} \sum_{k_1 \in V_t} (v'_{k_1}(v', u'))^2 \right\} =$$

$$= 2^{-(m-t)} \sum_{k_2 \in V_{m-t}} \left(\sum_{\substack{b_1 \in C(V), \\ c_1 \in S(U)}} v_{k_2}(b_1, c_1) \right)^2 \max_{\substack{u' \in S(U), \\ v' \in C(V)}} \Lambda_*^{(\psi_1)}(A_1, \alpha_1 \oplus v', \beta_1 \oplus u') =$$

$$= \Lambda_*^{(2)} \max_{\substack{u' \in S(U), \\ v' \in C(V)}} \Lambda_*^{(\psi_1)}(A_1, \alpha_1 \oplus v', \beta_1 \oplus u').$$

Итак, справедливо неравенство (9), что и требовалось доказать.

Теорема доказана.

Доказательство теоремы 2. Обозначим T_m множество блочно-треугольных матриц порядка m над полем F; для любых $A \in F_m$, $* \in \{+, \oplus\}$ положим

$$\gamma_{A,*} = \begin{cases} 4, & \text{если } * = + \text{ и } A \notin T_m, \\ 1 & \text{в противном случае.} \end{cases}$$

Зафиксируем число $i \in \{0, 1, \ldots, p-1\}$ и покажем, что в условиях теоремы для любых $A \in F_m$, $\alpha, \beta \in V_m$ справедливо неравенство

$$l_*^{(\psi)}(A, \alpha, \beta) \leq \gamma_{A,*} \max_{\substack{u \in C_i(A), \\ v \in S_i(A)}} \Lambda_*^{s_i}(A_{ii}, \alpha_i \oplus u, \beta_i \oplus v). \tag{38}$$

Пусть $i = 0$; тогда, полагая в формуле (6) $A_2 = A_{00}$, на основании следствия 1 и равенств (2), (3) получаем неравенства

$$l_*^{(\psi)}(A, \alpha, \beta) \leq \max_{\substack{u \in C_0(A), \\ v \in S_0(A)}} l_*^{(s_0)}(A_{00}, \alpha_0 \oplus u, \beta_0 \oplus v) \leq$$

$$\leq \max_{\substack{u \in C_0(A), \\ v \in S_0(A)}} \Lambda_*^{(s_0)}(A_{00}, \alpha_0 \oplus u, \beta_0 \oplus v),$$

из которых следует оценка (38). Если $i = p-1$, то формула (38) вытекает непосредственно из неравенств (18)–(20) и формулы (6), в которой нужно положить $A_1 = A_{p-1p-1}$.

Рассмотрим теперь случай, когда $1 \leq i \leq p-2$. Полагая в формуле (6) $A_2 = (A_{kl})_{k,l=\overline{0,i}}$ и применяя к матрице A следствие 1, получаем неравенство

$$l_*^{(\psi)}(A, \alpha, \beta) \leq \max_{\substack{\widetilde{\alpha} \in C(U), \\ \widetilde{\beta} \in S(V)}} l_*^{(\psi_2)}(A_2, \alpha_2 \oplus \widetilde{\alpha}, \beta_2 \oplus \widetilde{\beta}), \tag{39}$$

где $\psi_2 = (s_0, \ldots, s_i)$, $\alpha_2 = (\alpha_0, \ldots, \alpha_i)$, $\beta_2 = (\beta_0, \ldots, \beta_i)$, а блочные матрицы U и V имеют следующий вид:

$$U = (A_{kl})_{k=\overline{0,i},\, l=\overline{i+1,p-1}}, \; V = (A_{kl})_{k=\overline{i+1,p-1},\, l=\overline{0,i}}. \tag{40}$$

Для оценки выражения в правой части неравенства (39) воспользуемся следствием 2, полагая в формуле (6) $A = A_2$, $A_1 = A_{ii}$. В результате для любых векторов $\widetilde{\alpha} = (\widetilde{\alpha}_0, \ldots, \widetilde{\alpha}_i) \in C(U)$, $\widetilde{\beta} = (\widetilde{\beta}_0, \ldots, \widetilde{\beta}_i) \in S(V)$, где $\widetilde{\alpha}_j, \widetilde{\beta}_j \in V_t$, $j = \overline{0,i}$, получим неравенство

$$l_*^{(\psi_2)}(A_2, \alpha_2 \oplus \widetilde{\alpha}, \beta_2 \oplus \widetilde{\beta}) \le \gamma_{A,*} \max_{(u_i, v_i)} \Lambda_*^{(s_i)}(A_{ii}, \alpha_i \oplus \widetilde{\alpha}_i \oplus v_i, \beta_i \oplus \widetilde{\beta}_i \oplus u_i), \quad (41)$$

где максимум берется по всем упорядоченным парам $(u_i, v_i) \in V_t \times V_t$ таким, что вектор u_i является линейной комбинацией строк матриц A_{ji}, $j = \overline{0, i-1}$, а вектор v_i — линейной комбинацией столбцов матриц A_{ij}, $j = \overline{0, i-1}$. Заметим теперь, что согласно равенствам (40) для любых указанных выше векторов $u_i, v_i, \widetilde{\alpha}, \widetilde{\beta}$ справедливы соотношения $\widetilde{\alpha}_i \oplus v_i \in C_i(A)$, $\widetilde{\beta}_i \oplus u_i \in S_i(A)$, из которых на основании формул (39), (41) вытекает неравенство (38).

Таким образом, формула (38) и теорема доказаны.

Доказательство теоремы 3 почти дословно повторяет доказательство теоремы 1 для случая $* = \oplus$ и поэтому не приводится.

СПИСОК ЛИТЕРАТУРЫ

1. Matsui M. Linear cryptanalysis methods for DES cipher // Advances in Cryptology – EUROCRYPT'93: Proc. — Berlin; Heidelberg: Springer-Verlag, 1994. — P. 386–397.
2. Harpes C., Kramer G.G., Massey J.L. A generalization of linear cryptanalysis and the applicability of Matsui's piling-up lemma // Advances in Cryptology – EUROCRYPT'95: Proc. — Berlin; Heidelberg: Springer-Verlag, 1995. — P. 24–38.
3. Courtois N.T. Feistel schemes and bi-linear cryptanalysis // Advances in Cryptology – CRYPTO'04: Proc. — Berlin; Heidelberg: Springer-Verlag, 2004. — P. 23–40.
4. Vaudenay S. Decorrelation: a theory for block cipher security // J. Cryptology. — 2003. — **16,** N 4. — P. 249–286.
5. Wagner D. Towards a unifying view of block cipher cryptanalysis // Fast Software Encryption. – FSE'04: Proc. — Berlin; Heidelberg: Springer-Verlag, 2004. — P. 116–135.
6. Алексейчук А.Н., Шевцов А.С. Показатели и оценки стойкости блочных шифров относительно статистических атак первого порядка // Реєстрація, зберігання і обробка даних. — 2006. — **8**, вип. 4. — С. 53–63.
7. 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 Stoh. Processes. — 2006. — **12(28)**, N 1, 2. — P. 20–32.
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., Скрынник Е.В., Шевцов А.С. Оценки практической стойкости блочного шифра «Калина» относительно методов разностного, линейного криптоанализа и алгебраических атак, основанных на гомоморфизмах // Прикл. радиоэлектроника. — 2008. — **7**, № 3. — С. 203–209.
10. ГОСТ 28147-89. Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования. — М.: Госстандарт СССР, 1989.
11. Перспективний блоковий симетричний шифр «Калина» — основні положення та специфікації / І.Д. Горбенко, В.І. Долгов, Р.В. Олійников та ін. // Прикл. радиоэлектроника. — 2007. — **6**, № 2. — С. 195–208.
12. Шевцов А.С. Оцінки ймовірностей узагальнених лінійних апроксимацій раундової функції ГОСТ-подібного блокового шифру // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. — Київ, 2007. — Вип. 2(15). — С. 76–81.
13. Изотов В.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 23.10.2009