Досліджуються механізми комплексного забезпечення безпеки і достовірності передачі даних в комп'ютерних системах і мережах, засновані на інтеграції криптографічних засобів захисту інформації і канального (завадостійкого) кодування. Вводиться формальне математичне визначення крипто-кодових засобів захисту інформації з використанням недвійкових рівновагових кодів, розробляються схеми перетворення інформації запропонованими засобами захисту.

Ключові слова: криптографічні засобі, кодування, крипто-кодові засоби захисту.

Исследуются механизмы комплексного обеспечения безопасности и достоверности передачи данных в компьютерных системах и сетях, основанные на интеграции криптографических средств защиты информации и канального (помехоустойчивого) кодирования. Вводится формальное математическое определения крипто-кодовых средств защиты информации с использованием недвоичных равновесных кодов, разрабатываются схемы преобразования информации предложенными средствами защиты.

Ключевые слова: криптографические средства, кодирование, крипто-кодовые средства защиты.

The article explores the mechanisms of complex safeguarding of security and the trustworthiness of the datas' transmitting in the computer systems and resources that are based on the integration of cryptographic means of information protection and channel (antijamming) of encoding. The research defines mathematical definition of the cryptocoded means of information protection with non binary egnilibrium codes utihzation and also the schenes of the information transformation are worked out with the proposed means of protection.

Key words: cryptomaterial, coding, crypto-code security facilities.

Надійшла 24.12.2009

УДК 621.391:519.2

д.т.н., проф. Алексейчук А. Н., Шевцов А. С. (НТУУ «КПИ»)

ВЕРХНИЕ ОЦЕНКИ НЕСБАЛАНСИРОВАННОСТИ БИЛИНЕЙНЫХ АППРОКСИМАЦИЙ РАУНДОВЫХ ФУНКЦИЙ БЛОЧНЫХ ШИФРОВ ГОСТ 28147-89 И "КАЛИНА"

Введение

Одной из важнейших задач современного криптоанализа является разработка общих методов оценки и обоснования стойкости блочных шифров относительно статистических атак (разностых, линейных, билинейных и др. [1 – 6]). Как правило, решение этой задачи приводит к необходимости построения оценок параметров, вычисление точных значений которых практически не осуществимо.

Основным параметром, характеризующим обоснованную стойкость блочного шифра относительно линейного (билинейного) метода криптоанализа, является максимальное значение несбалансированности его линейных (билинейных) аппроксимаций [3, 4, 6]. При этом нахождение приемлемых (по точности и сложности вычислений) верхних оценок указанного параметра, как правило, представляет собой нетривиальную задачу, которая, за редким исключением [7], не поддается решению известными методами. В этой связи при исследовании стойкости блочных шифров относительно линейного (билинейного) метода криптоанализа обычно ограничиваются построением оценок вероятностей линейных характеристик (билинейных аппроксимаций раундовой функции) данного блочного шифра. Отметим, что последняя задача также является нетривиальной и, в ряде случаев, требует развития известных и применения новых математических методов [7 – 14].

В настоящей статье решается задача построения верхних оценок параметров, характризующих способность раундовых функций шифров ГОСТ 28147-89 (далее – ГОСТ) [15], и "Калина" [16] противостоять билинейному методу криптоанализа. (Напомним, что ГОСТ является действующим в настоящее время стандартом, а "Калина" – кандидатом на Национальный стандарт шифрования Украины). С использованием общих теорем, доказанных в [14], получены численные оценки несбалансированности ряда билинейных

аппроксимаций указанных шифров, свидетельствующие об отсутствии в их конструкциях ярко выраженных слабостей относительно известных билинейных атак [3, 6].

Определения основных понятий и вспомогательные результаты

Обозначим V_m множество булевых векторов длины m, S^{V_m} – симметрическую группу подстановок на множестве V_m, F_m – кольцо матриц размера $m \times m$ над полем $F = \mathbf{GF}(2)$. Будем отождествлять произвольный вектор $x = (x_1, \dots, x_m) \in V_m$ с целым числом $x = 2^{m-1}x_1 + \dots + 2^0 x_m$ 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 $x = (x_1, \dots, x_m)$ и $y = (y_1, \dots, y_m)$: $xy = x_1 y_1 \oplus \dots \oplus x_m y_m$. 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

$$l_*^{(\psi)}(A, \alpha, \beta) = 2^{-m} \sum_{k \in V_m} (2^{-m} \sum_{x \in V_m} \chi(x A \psi(x * k) \oplus \alpha x \oplus \beta \psi(x * k)))^2, \qquad (1)$$

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

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

где для любых $m \in \mathbf{N}$, $x, k \in V_m$ символ $\nu(x,k)$ обозначает бит переноса в m-й разряд суммы чисел x и k в кольце $\mathbf{Z}$, если $* = +$; $\nu(x,k) = 0$, если $* = \oplus$.

Заметим, что подстановке ψ и операции $*$ соответствует булево отображение

$$x \mapsto \psi(x * k), \; x \in V_m, \qquad (3)$$

используемое в конструкциях раундовых функций блочных шифров. Параметр (1) характеризует способность отображения (3) противостоять билинейному методу криптоанализа [3, 6] и называется несбалансированностью билинейной аппроксимации $f(x, y) = xAy \oplus \alpha x \oplus \beta y$, $x, y \in V_m$ (между входами и выходами) указанного отображения.

При исследовании стойкости блочных шифров относительно билинейного метода криптоанализа требуется, в частности, оценивать сверху значения (1) для данных $\psi \in S^{V_m}$, $*$ и произвольных $A \in F_m$, $\alpha, \beta \in V_m$. Нетривиальность этой задачи связана с тем, что m является достаточно большим числом (например, m равно 64 или 128). В [12 – 14] получены верхние оценки параметра (1) при различных дополнительных предположениях относительно подстановки $\psi \in S^{V_m}$, операции $*$ и матрицы $A \in F_m$. Наиболее общие на сегодняшний день результаты представлены в статье [14], где доказаны следующие теоремы.

Теорема 1. Пусть

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

где $\psi_1 \in S^{V_t}$, $\psi_2 \in S^{V_{m-t}}$, $1 \le t \le m-1$, и операция $*$ на множестве V_m определяется по формуле $(x_2, x_1) * (k_2, k_1) = (x_2 \overset{(2)}{*} k_2, \; x_1 \overset{(1)}{*} k_1)$, $x_1, k_1 \in V_t$, $x_2, k_2 \in V_{m-t}$, где $\overset{(1)}{*}$ и $\overset{(2)}{*}$ –

произвольные бинарные алгебраические операции на множествах V_t и V_{m-t} соответственно. Тогда для любой матрицы

$$A = \begin{pmatrix} A_2 & U \\ V & A_1 \end{pmatrix}$$

и произвольных векторов $\alpha = (\alpha_2, \alpha_1)$, $\beta = (\beta_2, \beta_1)$, где $A_1 \in F_t$, $A_2 \in F_{m-t}$, $\alpha_1, \beta_1 \in V_t$, $\alpha_2, \beta_2 \in V_{m-t}$, справедливы следующие неравенства:

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

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

Теорема 2. Пусть подстановка ψ представляет собой набор s-блоков:

$$\psi = (s_0, \ldots, s_{p-1}), \tag{4}$$

где $s_i \in S^{V_t}$, $i = \overline{0, p-1}$, $pt = m$. Тогда для любой матрицы $A = (A_{ij})_{i,j=\overline{0,p-1}}$ и векторов $\alpha = (\alpha_0, \ldots, \alpha_{p-1})$, $\beta = (\beta_0, \ldots, \beta_{p-1})$, где $A_{ij} \in F_t$, $\alpha_j, \beta_j \in V_t$, $i, j = \overline{0, p-1}$, справедливы следующие неравенства:

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

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

где $C_i(A)$ и $S_i(A)$ – подпространства векторного пространства V_t, порожденные столбцами матриц A_{ij} и, соответственно, строками матриц A_{ji} по всем $j \ne i$, $i = \overline{0, p-1}$. Кроме того, если A является блочно-треугольной матрицей (то есть $A_{ij} = 0$ для любых $0 \le i < j \le p-1$ или $A_{ji} = 0$ для любых $0 \le i < j \le p-1$), то справедливо неравенство

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

Сформулированные теоремы применимы к широкому классу билинейных аппроксимаций булевых отображений (3), соответствующих раундовым функциям современных блочных шифров. В частности, они позволяют оценивать сверху значения (1) для любой подстановки ψ вида (4), произвольной матрицы $A \in F_m$ и операции $*$ вида $(x_1, \ldots, x_n) * (k_1, \ldots, k_n) = (\overset{m_1}{x_1 + k_1}, \ldots, \overset{m_n}{x_n + k_n})$, $x_i, k_i \in V_{m_i}$, $i = \overline{1, n}$, где числа $m_1, \ldots, m_n$ делятся на t, $m_1 + \ldots + m_n = m$. Ниже изложены результаты исследования “билинейных свойств” раундовых функций шифров ГОСТ и “Калина”, полученные с использованием указанных теорем.

Численные оценки несбалансированности билинейных аппроксимаций раудовых функций шифров ГОСТ 28147-89 и "Калина"

Приведем необходимые для дальнейшего сведения об алгоритмах шифрования ГОСТ и “Калина”.

Напомним [15], что ГОСТ является 32-раундовым шифром Фейстеля с длиной блока $n = 64$ бит. Шифрующее преобразование $f_k : V_{64} \to V_{64}$, $k \in V_{32}$, в каждом из раундов определяется по формуле

$$f_k(x) = f_k(u, v) = (v, u \oplus \varphi(v \overset{32}{+} k)),\ x = (u, v),\ u, v \in V_{32}, \tag{5}$$

где

$$\varphi(z) = \psi(z)L,\ z \in V_{32}, \tag{6}$$

$$\psi(z) = (s_0(z_0), \ldots, s_7(z_7)),\ z = (z_0, \ldots, z_7),\ z_j \in V_4,\ j = \overline{0,7}, \tag{7}$$

$s_j \in S^{V_4}$, $j = \overline{0,7}$, а L – обратимая матрица над полем F, соответствующая операции циклического сдвига на 11 разрядов влево на множестве V_{32}. Подстановки s_j, $j = \overline{0,7}$, используются в качестве долговременного ключа шифрования и называются узлами замены (или s-блоками) шифра ГОСТ, а отображение φ вида (6) – раундовой функцией этого шифра.

Блочный шифр “Калина” имеет структуру SPN (substitution-permutation network) и допускает зашифрование блоков длины $n \in \{128, 256, 512\}$ бит с использованием n'-битовых ключей, где $n' \in \{128, 256, 512\}$, $n' \geq n$ [16]. Ниже рассматривается 128-битовая версия этого шифра ($n = n' = 128$). В этом случае число раундов шифрования $r = 11$, и шифрующее преобразование $f_{i,k} : V_{128} \to V_{128}$, $k \in V_{128}$, в i-м раунде имеет следующий вид:

$$f_{i,k}(x) = \psi(x \oplus k)M, \text{ если } i \equiv 1 (\mathrm{mod}\, 2),\ i = \overline{1,10};\ f_{11,k}(x) = \psi(x \oplus k); \tag{8}$$

$$f_{i,k}(x) = \psi(x \overset{\circ}{+} k)M, \text{ если } i \equiv 0 (\mathrm{mod}\, 2),\ i = \overline{1,10}. \tag{9}$$

В выражениях (8), (9)

$$\psi(z) = (s^{(0)}(z_0), \ldots, s^{(15)}(z_{15})),\ z = (z_0, \ldots, z_{15}),\ z_j \in V_8,\ j = \overline{0,15}, \tag{10}$$

где $s^{(j)} \in S^{V_8}$, $j = \overline{0,15}$, M – обратимая матрица определенного вида над полем $\mathbf{GF}(2^8)$, причем умножение произвольной вектор-строки $z = (z_0, \ldots, z_{15}) \in V_{128}$ на матрицу M осуществляется над этим полем (при естественном отождествлении двоичных векторов z_j, $j = \overline{0,15}$, с его элементами). Символ $\overset{\circ}{+}$ в выражении (9) обозначает алгебраическую операцию вида

$$x \overset{\circ}{+} k = (x^{(1)} \overset{32}{+} k^{(1)}, \ldots, x^{(4)} \overset{32}{+} k^{(4)}),$$

где $x = (x^{(1)}, \ldots, x^{(4)})$, $k = (k^{(1)}, \ldots, k^{(4)})$, $x^{(l)}, k^{(l)} \in V_{32}$, $l \in \overline{1,4}$. Отметим, что s-блоки $s^{(0)}, \ldots, s^{(15)}$ шифра “Калина” являются фиксированными подстановками на множестве V_8, выбранными в соответствии с рядом условий; при этом среди указанных 16 подстановок имеется ровно 8 попарно различных [16].

Получим численные оценки значений параметра (1) для подстановки (7), используемой в конструкции шифра ГОСТ, и операции $* = +$. С этой целью рассмотрим конкретный набор s-блоков $s_0, \ldots, s_7$, приведенных в табл. 1, 2. Эти s-блоки характеризуются наименьшими значениями параметров

$$d(s) = \max\left\{ 2^{-4} \mid \{x \in V_4 : s(x \oplus a) \oplus s(x) = b\} \mid : a, b \in V_4 \setminus \{0\} \right\}$$

и

$$l(s) = \max\left\{\left(2^{-4}\sum_{x\in V_4}(-1)^{ax\oplus bs(x)}\right)^2 : a,b \in V_4 \setminus \{0\}\right\}$$

среди всех подстановок $s \in S^{V_4}$ ($d(s_i) = l(s_i) = 0{,}25$ для любого $i = \overline{0,7}$) и рекомендуются в [17] для применения в качестве узлов замены шифра ГОСТ.

В табл. 1 указаны значения параметра

$$\Lambda_{+,0}^{(s_i)} = \max\{\Lambda_{+}^{(s_i)}(0,\alpha_i,\beta_i) :\ \alpha_i,\beta_i \in V_4 \setminus \{0\}\},$$

а в табл. 2 – значения параметра

$$\Lambda_{+,1}^{(s_i)} = \max\{\Lambda_{+}^{(s_i)}(A_{ii},\alpha_i,\beta_i) :\ A_{ii} \in F_4, \operatorname{rank} A_{ii} = 1, \alpha_i,\beta_i \in V_4\},$$

где для любых $A_{ii} \in F_4$, $\alpha_i,\beta_i \in V_4$ величина $\Lambda_{+}^{(s_i)}(A_{ii},\alpha_i,\beta_i)$ определяется в соответствии с формулой (2), $i = \overline{0,7}$. Используя теорему 2 и данные, приведенные в таблицах, нетрудно получить оценки параметра $l_{+}^{(\psi)}(A,\alpha,\beta)$ для широкого класса наборов (A,α,β), где $A \in F_{32}$, $\alpha,\beta \in V_{32}$.

Таблица 1

i	Подстановка s_i	$\Lambda_{+,0}^{(s_i)}$
0	[0, 1, 11, 13, 9, 14, 6, 7, 12, 5, 8, 3, 15, 2, 4, 10]	0,250000
1	[0, 1, 2, 4, 3, 5, 8, 10, 7, 9, 6, 13, 11, 14, 12, 15]	0,279297
2	[0, 1, 11, 2, 8, 6, 15, 3, 14, 10, 4, 9, 13, 5, 7, 12]	0,324219
3	[0, 1, 11, 2, 8, 3, 15, 6, 14, 10, 4, 9, 13, 5, 7, 12]	0,324219
4	[0, 4, 11, 2, 8, 6, 10, 1, 14, 15, 3, 9, 13, 5, 7, 12]	0,267578
5	[0, 4, 11, 2, 8, 3, 15, 1, 14, 10, 6, 9, 13, 5, 7, 12]	0,258789
6	[0, 11, 15, 9, 1, 5, 6, 8, 3, 10, 4, 12, 14, 13, 7, 2]	0,258789
7	[0, 7, 10, 14, 9, 1, 13, 8, 12, 2, 11, 15, 3, 5, 4, 6]	0,258789

Таблица 2

i	Подстановка s_i	$\Lambda_{+,1}^{(s_i)}$
0	[0, 1, 11, 13, 9, 14, 6, 7, 12, 5, 8, 3, 15, 2, 4, 10]	0,382812
1	[0, 1, 2, 4, 3, 5, 8, 10, 7, 9, 6, 13, 11, 14, 12, 15]	0,616211
2	[0, 1, 11, 2, 8, 6, 15, 3, 14, 10, 4, 9, 13, 5, 7, 12]	0,538086
3	[0, 1, 11, 2, 8, 3, 15, 6, 14, 10, 4, 9, 13, 5, 7, 12]	0,586914
4	[0, 4, 11, 2, 8, 6, 10, 1, 14, 15, 3, 9, 13, 5, 7, 12]	0,513672
5	[0, 4, 11, 2, 8, 3, 15, 1, 14, 10, 6, 9, 13, 5, 7, 12]	0,502930
6	[0, 11, 15, 9, 1, 5, 6, 8, 3, 10, 4, 12, 14, 13, 7, 2]	0,419922
7	[0, 7, 10, 14, 9, 1, 13, 8, 12, 2, 11, 15, 3, 5, 4, 6]	0,437500

Пусть, например, $A = (A_{ij})_{i,j=\overline{0,7}}$ – блочно-треугольная матрица, содержащая хотя бы одну подматрицу A_{ii} ранга 1 на главной диагонали. Согласно теореме 2, для любых $\alpha,\ \beta \in V_{32}$ справедливо неравенство $l_{+}^{(\psi)}(A,\alpha,\beta) \le \Lambda_{+,1}^{(s_i)}$; в частности, при $i = 0$ $l_{+}^{(\psi)}(A,\alpha,\beta) \le 0{,}382812$ (см. табл. 2).

Пусть теперь блочно-треугольная матрица $A \in F_{32}$ и векторы $\alpha = (\alpha_0,...,\alpha_7)$, $\beta = (\beta_0,...,\beta_7) \in V_{32}$ удовлетворяют условию:

$$\exists\, i \in \{0,1,...,7\} : A_{ii} = 0,\ \alpha_i \notin C_i(A),\ \beta_i \notin S_i(A).$$

Тогда по теореме 2 $l_{+}^{(\psi)}(A,\alpha,\beta) \le \Lambda_{+,0}^{(s_i)}$; в частности, при $i=0$ $l_{+}^{(\psi)}(A,\alpha,\beta) \le 0{,}250000$ (см. табл 1). Аналогично, используя неравенство

$$l_{+}^{(\psi)}(A,\alpha,\beta) \le \max\{\Lambda_{+}^{(s_i)}(A_{ii},\alpha_i,\beta_i) : \alpha_i,\beta_i \in V_4\},\ i=\overline{0,7}, \qquad (11)$$

вытекающее из последнего утверждения теоремы 2, можно оценить значение (1) для произвольных блочно-треугольной матрицы $A \in F_{32}$ и векторов $\alpha,\beta \in V_{32}$. Отметим, что в результате вычислений, проведенных для ряда случайно сгенерированных матриц $A_{ii} \ne 0$, не удалось обнаружить ни одной такой матрицы, для которой значение параметра в правой части неравенства (11) превосходит значение $\Lambda_{+,1}^{(s_i)}$, указанное в табл. 2, $i=\overline{0,7}$.

Приведем оценки параметра (1), полученные для подстановки (10) и операций $\oplus$, $\overset{\circ}{+}$, используемых в раундовых преобразованиях шифра “Калина” (см. формулы (8), (9)). В табл. 3, взятой из статьи [16], показан один из s-блоков этого шифра: подстановка $s = s^{(0)} = s^{(8)}$ в формуле (10). При этом значение, находящееся в i-й строке и j-м столбце табл. 3, является шестнадцатиричной записью числа $s(16i+j)$, $i,j=\overline{0,15}$.

Таблица 3

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	F9	CA	14	61	E4	1C	43	20	4E	54	58	A0	FC	DB	C0	72
1	22	74	FE	B5	65	A8	25	ED	69	33	F1	B1	36	9	6	9A
2	8E	90	CF	F6	EA	27	BC	7	7F	D7	3C	7C	44	45	21	6B
3	1A	52	62	29	13	9B	CC	99	4B	42	B6	1D	C7	91	76	16
4	92	4F	47	70	98	66	C2	48	96	B	2F	C9	C6	38	8C	63
5	10	F2	A9	37	A7	D3	55	3D	2C	7A	AF	EE	3E	F5	67	C
6	77	84	C1	C5	DE	A4	DD	B4	E3	B3	EF	49	E2	71	4C	AD
7	DF	3	12	19	9C	D9	D2	78	50	DC	AA	15	4	39	9D	D1
8	2D	11	24	2E	F7	59	FA	1E	68	3A	7E	CB	AE	D6	A5	FD
9	5F	5	F	6A	A6	E7	EC	30	5C	6F	83	CD	B2	BB	EB	2
A	28	73	4D	18	A3	86	9F	5B	3F	81	AB	75	1B	6C	E	53
B	64	FB	26	40	7D	E1	95	34	BF	A	BD	31	2B	B0	F4	8D
C	E0	1	87	56	CE	FF	5D	6D	A2	6E	88	9E	94	89	46	35
D	4A	B9	DA	C3	F3	5E	8F	97	B7	D4	51	60	D5	23	57	D0
E	79	3B	17	C4	B8	C8	7B	2A	D	8B	D8	0	E8	BA	E6	F8
F	41	85	32	F0	80	93	8	E5	82	BE	E9	1F	A1	8A	AC	5A

Для указанной подстановки s и произвольной матрицы $B \in F_8$ обозначим

$$l_{\oplus}^{(s)}(B) = \max\{l_{\oplus}^{(s)}(B,a,b) : a,b \in V_8\}, \qquad (12)$$

$$\Lambda_{+}^{(s)}(B) = \max\{\Lambda_{+}^{(s)}(B,a,b) : a,b \in V_8\}. \qquad (13)$$

Заметим, что на основании теорем 1 и 2 для любых $A=(A_{ij})_{i,j=\overline{0,15}} \in F_{128}$, $\alpha,\beta \in V_{128}$ справедливы следующие неравенства:

$$l_{\oplus}^{(\psi)}(A,\alpha,\beta) \le \min\{l_{\oplus}^{(s)}(A_{00}), l_{\oplus}^{(s)}(A_{88})\}, \qquad (14)$$

$$l_{\overset{\circ}{+}}^{(\psi)}(A,\alpha,\beta) \le \gamma_A \min\{\Lambda_{+}^{(s)}(A_{00}), \Lambda_{+}^{(s)}(A_{88})\}, \qquad (15)$$

где $\gamma_A = 1$, если A – блочно-треугольная матрица; $\gamma_A = 4$ – в противном случае. Используя соотношения (12) – (15), нетрудно получить численные оценки параметров $l_{\oplus}^{(\psi)}(A,\alpha,\beta)$, $l_{\overset{\circ}{+}}^{(\psi)}(A,\alpha,\beta)$ для широкого класса наборов (A,α,β).

Рассмотрим, например, сгенерированные случайно матрицу B и матрицу B' ранга 1, которые приведены в табл. 4. Для первой из них значения параметров (12) и (13) равны соответственно $l_{\oplus}^{(s)}(B) = 0{,}001068$, $\Lambda_{+}^{(s)}(B) = 0{,}007869$. Для второй матрицы $l_{\oplus}^{(s)}(B') = 0{,}002045$, $\Lambda_{+}^{(s)}(B') = 0{,}258865$. Отсюда на основании формул (14), (15) вытекает, что для любых векторов $\alpha, \beta \in V_{128}$ и матрицы $A \in F_{128}$ такой, что $B \in \{A_{00}, A_{88}\}$, выполняются неравенства $l_{\oplus}^{(\psi)}(A, \alpha, \beta) \le 0{,}001068$, $l_{\underset{+}{\circ}}^{(\psi)}(A, \alpha, \beta) \le 0{,}032076$.

Аналогично, при выполнении условия $B' \in \{A_{00}, A_{88}\}$ справедливо неравенство $l_{\oplus}^{(\psi)}(A, \alpha, \beta) \le 0{,}002045$, и если A является блочно-треугольной матрицей, то $l_{\underset{+}{\circ}}^{(\psi)}(A, \alpha, \beta) \le 0{,}258865$. Вычисление значений (12), (13) для ряда других случайно сгенерированных матриц B приводит к сравнимым с указанными выше оценкам параметров в левых частях неравенств (14) и (15).

Таблица 4

Матрица B	Матрица B'
$\begin{bmatrix} 0 & 1 & 1 & 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 & 1 & 0 & 0 & 1 \end{bmatrix}$	$\begin{bmatrix} 0 & 0 & 1 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}$

В целом, результаты проведенных исследований свидетельствуют в пользу предположения о практической стойкости шифров ГОСТ и “Калина” к известным в настоящее время билинейным атакам [3, 6].

Список литературы

1.*Matsui M.* Linear cryptanalysis methods for DES cipher // Advances in Cryptology – EUROCRYPT’93, Proceedings. – 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, Proceedings. – Springer Verlag, 1995. – P. 24 – 38.

3.*Courtois N.T.* Feistel schemes and bi-linear cryptanalysis // Advances in Cryptology – CRYPTO’04, Proceedings. – Springer Verlag, 2004. – P. 23 – 40.

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

5.*Wagner D.* Towards a unifying view of block cipher cryptanalysis // Fast Software Encryption. – FSE’04, Proceedings. – 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. – Т. 8 – Вип. 4. – С. 53 – 63.

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

8.*Alekseychuk A.N.*, *Kovalchuk L.V.* Upper bounds of maximum values of average differential and linear characteristic probabilities of Feistel cipher with adder modulo 2^m // Theory of Stohastic Processes. – 2006. – Vol. 12(28). – № 1, 2. – P. 20 – 32.

9.*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.

10. *Алексейчук А.Н.*, *Ковальчук Л.В.*, *Скрынник Е.В.*, *Шевцов А.С.* Оценки практической стойкости блочного шифра "Калина" относительно методов разностного, линейного криптоанализа и алгебраических атак, основанных на гомоморфизмах // Прикладная радиоэлектроника. – 2008. – Т. 7. – № 3. – С. 203 – 209.

11. *Шевцов А.С.* Оцінки ймовірностей узагальнених лінійних апроксимацій раундової функції ГОСТ-подібного блокового шифру // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. – Вип. 2(15). – Київ, 2007. – С. 76 – 81.

12. *Олексійчук А.М.*, *Шевцов А.С.* Аналітична оцінка ймовірності білінійної апроксимації композиції перетворень заміни та зсуву за модулем 2^m // Вісник ДУІКТ. – 2008. – № 1. – С. 5 – 11.

13. *Алексейчук А.Н.*, *Ковальчук Л.В.*, *Скрыпник Л.В.*, *Шевцов А.С.* Оценки практической стойкости блочного шифра "Калина" относительного разностного, линейного и билинейного методов криптоанализа // Материалы Четвертой международной конференции по проблемам безопасности и противодействию терроризму. МГУ им. М.В. Ломоносова. 30 – 31 октября 2008 г. Том. 2. Материалы Седьмой общероссийской научной конференции "Математика и безопасность информационных технологий" (МаБИТ-2008). – М.: МЦНМО, 2009. – С. 15 – 20.

14. *Алексейчук А.Н.*, *Шевцов А.С.* Верхние оценки несбалансированности билинейных аппроксимаций раундовых функций блочных шифров // Кибернетика и системный анализ. – 2010. – № 3 (в печати).

15. ГОСТ 28147-89. Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования. – М.: Госстандарт СССР, 1989.

16. *Горбенко І.Д.*, *Долгов В.І.*, *Олійников Р.В.*, *Руженцев В.І.*, *Михайленко М.С.*, *Горбенко Ю.І.*, *Тоцький О.С.*, *Казьміна С.В.* Перспективний блоковий симетричний шифр "Калина" – основні положення та специфікації // Прикладная радиоэлектроника. – 2007. – Т. 6. – № 2. – С. 195 – 208.

17. *Шевцов А.С.* Оцінки ймовірностей узагальнених лінійних апроксимацій раундової функції ГОСТ-подібного блокового шифру // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. – Вип. 2(15). – Київ, 2007. – С. 76 – 81.

18. *Растовцев А.Г., Маховенко Е.Б.* Введение в теорию итерированых шифров. – Спб.: НПО "Мир и Семья", 2003. – 302 с.

Получены верхние оценки параметров, характеризующих способность раундовых функций шифров ГОСТ 28147-89 и "Калина" противостоять билинейному методу криптоанализа. Результаты проведенных исследований свидетельствуют в пользу предположения о практической стойкости указанных шифров к известным в настоящее время билинейным атакам.

Ключевые слова: криптоанализ, билинейный метод, шифры, противостояние криптоанализу.

Отримані верхні оцінки параметрів, що характеризують здатність раундових функцій шифрів ГОСТ 28147-89 та "Калина" протистояти білінійному методу криптоаналізу. Результати проведених досліджень свідчать на користь припущення про практичну стійкість вказаних шифрів відносно відомих в наступний час білінійних атак.

Ключові слова: критоаналіз, білінійний метод, шифри, протистояння криптоаналізу.

In the article upper bounds of parameters that define the capability of round functions of State Standard 28147-89 and "Kalyna" ciphers to resist a bilinear method of cryptoanalysis.

Key words: cryptoanalysis, bilinear method, ciphers, resistance to cryptoanalysis.

Поступила 11.01.2010

УДК 681.3.07

д.т.н., проф. Белецкий А.Я., Аксентий Е.А.
(Национальный авиационный университет)

ПРОГРАММНЫЙ КОМПЛЕКС ДЛЯ ИССЛЕДОВАНИЯ СТАТИСТИЧЕСКИХ ХАРАКТЕРИСТИК КРИПТОГРАФИЧЕСКИХ ПРИМИТИВОВ ТИПА НЕЛИНЕЙНОЙ ПОДСТАНОВКИ

Введение и постановка задачи

Современные методы защиты информации (*шифрование*) в компьютерных сетях представляют собой математические преобразования (алгоритмы), в которых сообщения рассматриваются как числа или алгебраические элементы в некотором пространстве [1]. С позиций теории сигналов и процессов *зашифрование* исходного (коррелированного,