УДК 519.7

А.Н. АЛЕКСЕЙЧУК, С.Н. КОНЮШОК, М.В. ПОРЕМСКИЙ

ВЕРХНИЕ ОЦЕНКИ НЕСБАЛАНСИРОВАННОСТИ ДИСКРЕТНЫХ ФУНКЦИЙ, РЕАЛИЗУЕМЫХ ПОСЛЕДОВАТЕЛЬНОСТЯМИ КОНЕЧНЫХ АВТОМАТОВ

Аннотация. Получены матричное представление и верхние оценки несбалансированности произвольной дискретной функции, реализуемой последовательностью конечных автоматов. Приведенные результаты, обобщающие ряд известных ранее утверждений о матричных (линейных) представлениях несбалансированности функций специального вида, можно применять к решению задач обоснования стойкости поточных или блочных шифров относительно ряда статистических атак.

Ключевые слова: корреляционный криптоанализ, несбалансированность дискретной функции, конечный автомат, операция сложения по модулю 2^n, SNOW 2.0, «Струмок».

ВВЕДЕНИЕ

В конструкциях современных поточных и блочных шифров наряду с другими операциями широко используется операция сложения двоичных целых чисел по модулю 2^n. Исследованию корреляционных (а также некоторых других криптографических) свойств этой операции посвящено большое количество работ, среди которых отметим [1–7].

Методы нахождения верхних оценок параметров, характеризующих стойкость блочных шифров, содержащих сложение раундовых ключей по модулю 2^n, относительно дифференциального и линейного криптоанализа предложены в [8–11], а в [12–16] описаны корреляционные атаки на поточный шифр SNOW 2.0 [17], для оценки эффективности которых использованы методы вычисления распределений числа прообразов псевдолинейных [14] и обобщенно псевдолинейных [16] функций по модулю 2^n.

При распространении методов, описанных в [12–16], на произвольные SNOW 2.0-подобные шифры, в частности на шифр «Струмок» [18], который в будущем может использоваться как национальный стандарт поточного шифрования Украины, возникают трудности. Они связаны с тем, что в отличие от SNOW 2.0, построенного над полем порядка 2^{32}, «Струмок» задается над полем порядка 2^{64}. Это исключает возможность практического применения некоторых алгоритмов [13, 14, 16], сложность которых возрастает с $2^{32} \div 2^{37}$ до 2^{64} двоичных операций. Кроме того, методы из [12–16] ориентированы на построение конкретных атак, а не на обоснование стойкости (security proof) шифра, поэтому их применение для решения задач обоснования стойкости приводит к большому объему вычислений даже для шифра SNOW 2.0.

Для преодоления указанных трудностей в настоящей статье предлагается теоретико-автоматный подход к построению верхних оценок несбалансированности дискретных функций. Истоки этого подхода содержатся в [19], где получено матричное представление для числа прообразов выходной последовательности конечного автомата.

Основные приведенные далее результаты обобщают ряд известных утверждений о матричных (или линейных) представлениях несбалансированности

отображений специального вида [3, 8, 10, 13] и их можно применять для решения задач обоснования стойкости поточных или блочных шифров относительно статистических атак.

Авторы планируют посвятить отдельную статью применению полученных результатов для обоснования стойкости SNOW 2.0-подобных шифров относительно корреляционных атак.

ПОСТАНОВКА ЗАДАЧИ И ОСНОВНЫЕ РЕЗУЛЬТАТЫ

Пусть U, X_i — конечные множества, $h_i: U \times X_i \to U$, $f_i: U \times X_i \to V_{t_i}$ — отображения, где $V_{t_i} = \{0,1\}^{t_i}$, $i = 0, 1, \ldots$ Для любого натурального n зададим отображения $H_n: U \times X_0 \times \cdots \times X_{n-1} \to U$ и $F_n: U \times X_0 \times \cdots \times X_{n-1} \to V_{t_0} \times \cdots \times V_{t_{n-1}}$, полагая

$$H_n(u_0, x_0, \ldots, x_{n-1}) = u_n,$$

$$F_n(u_0, x_0, \ldots, x_{n-1}) = y_0, y_1, \ldots, y_{n-1}, \qquad (1)$$

где элементы $u_1, u_2, \ldots, y_0, y_1, \ldots$ вычисляются с помощью рекуррентных соотношений $u_{i+1} = h_i(u_i, x_i)$, $y_i = f_i(u_i, x_i)$, $i = 0, 1, \ldots$ Отметим, что если $X_i = X$, $V_{t_i} = V_t$, $h_i = h$, $f_i = f$ для любого $i = 0, 1, \ldots$, то $F_n(u_0, x_0, \ldots, x_{n-1})$ является выходной последовательностью автомата (X, U, V_t, h, f) (с входным алфавитом X, множеством состояний U и выходным алфавитом V_t), которая строится по его начальному состоянию u_0 и входной последовательности $x_0, \ldots, x_{n-1}$, а $H_n(u_0, x_0, \ldots, x_{n-1})$ — состояние этого автомата в n-м такте.

Определение 1. Функция $F: X_0 \times \cdots \times X_{n-1} \to V_{t_0} \times \cdots \times V_{t_{n-1}}$ реализуется последовательностью автоматов $(X_i, U, V_{t_i}, h_i, f_i)$, $i = \overline{0, n-1}$, если существует элемент $u_0 \in U$ такой, что $F(x_0, \ldots, x_{n-1}) = F_n(u_0, x_0, \ldots, x_{n-1})$ для всех $(x_0, \ldots, x_{n-1}) \in X_0 \times \cdots \times X_{n-1}$.

Пусть $\alpha = (\alpha_0, \alpha_1, \ldots)$ — последовательность двоичных векторов, $\alpha_i \in V_{t_i}$, $i = 0, 1, \ldots$ Для любого натурального n обозначим $\alpha^{(n)} = (\alpha_0, \alpha_1, \ldots, \alpha_{n-1})$ и зададим функцию $F_n\alpha^{(n)}$, значение которой в точке $(u_0, x_0, \ldots, x_{n-1})$ равно булевому скалярному произведению векторов $F_n(u_0, x_0, \ldots, x_{n-1})$ и $\alpha^{(n)}$.

Определение 2. Несбалансированностью функции $F_n\alpha^{(n)}$ при фиксированном значении $u_0 \in U$ называется число

$$l_\alpha^{(n)}(u_0) = \frac{1}{|X_0| \cdots |X_{n-1}|} \left| \sum_{(x_0, \ldots, x_{n-1}) \in X_0 \times \cdots \times X_{n-1}} (-1)^{F_n(u_0, x_0, \ldots, x_{n-1})\alpha^{(n)}} \right|. \qquad (2)$$

Задача, решаемая в статье, заключается в нахождении матричного представления и верхних оценок параметра (2) в терминах автоматов $(X_i, U, V_{t_i}, h_i, f_i)$, $i = \overline{0, n-1}$.

Для формулировки полученных результатов введем следующие обозначения. Для любых $u, u' \in U$ обозначим

$$l_\alpha^{(n)}(u, u') = \frac{1}{|X_0| \cdots |X_{n-1}|} \sum_{\substack{(x_0, \ldots, x_{n-1}) \in X_0 \times \cdots \times X_{n-1}: \\ H_n(u, x_0, \ldots, x_{n-1}) = u'}} (-1)^{F_n(u, x_0, \ldots, x_{n-1})\alpha^{(n)}}. \qquad (3)$$

Произвольно пронумеруем элементы множества U, полагая $U = \{u_0, u_1, \ldots, u_{M-1}\}$, где $M = |U|$, и зададим $M \times M$-матрицы $A_{\alpha_i}^{(i)}$ с элементами

$$A_{\alpha_i}^{(i)}(u,u') = \frac{1}{|X_i|} \sum_{x_i \in X_i:\, h_i(u,x_i)=u'} (-1)^{f_i(u,x_i)\alpha_i},\ u,u' \in U, \tag{4}$$

где $f_i(u,x_i)\alpha_i$ обозначает булево скалярное произведение указанных двоичных векторов длины t, $i = 0,1,\ldots$

Теорема 1. Для любого натурального n справедливо равенство

$$l_\alpha^{(n)}(u,u') = (A_{\alpha_0}^{(0)} A_{\alpha_1}^{(1)} \cdots A_{\alpha_{n-1}}^{(n-1)})(u,u'),\ u,u' \in U; \tag{5}$$

другими словами, параметр (3) совпадает с (u,u')-м элементом произведения матриц (4) по всем $i \in \overline{0,n-1}$. Кроме того, параметр (2) удовлетворяет следующему равенству:

$$l_\alpha^{(n)}(u_0) = |\,\mathbf{e}\, A_{\alpha_0}^{(0)} A_{\alpha_1}^{(1)} \cdots A_{\alpha_{n-1}}^{(n-1)}\, \mathbf{1}|, \tag{6}$$

где $\mathbf{e} = (1,0,\ldots,0)$, $\mathbf{1} = (1,1,\ldots,1)^{\mathrm{T}}$.

Доказательство. Формула (5) доказывается с помощью индукции по n. При $n = 1$ она следует непосредственно из данных определений. При $n \geq 2$ достаточно убедиться в справедливости такого равенства:

$$l_\alpha^{(n)}(u,u') = \sum_{u'' \in U} l_\alpha^{(n-1)}(u,u'')\, A_{\alpha_{n-1}}^{(n-1)}(u'',u'),\ u,u' \in U. \tag{7}$$

Действительно, на основании формул (3), (4) и определения отображений H_n, F_n имеют место следующие соотношения:

$$\sum_{u'' \in U} l_\alpha^{(n-1)}(u,u'')\, A_{\alpha_{n-1}}^{(n-1)}(u'',u') = \frac{1}{|X_0|\cdots|X_{n-1}|} \times$$

$$\times \sum_{u'' \in U} \sum_{\substack{(x_0,\ldots,x_{n-2}) \in X_0 \times \cdots \times X_{n-2}: \\ H_{n-1}(u,x_0,\ldots,x_{n-2}) = u''}} (-1)^{F_{n-1}(u,x_0,\ldots,x_{n-2})\alpha^{(n-1)}} \sum_{\substack{x_{n-1} \in X_{n-1}: \\ h_{n-1}(u'',x_{n-1}) = u'}} (-1)^{f_{n-1}(u'',x_{n-1})\alpha_{n-1}} =$$

$$= \frac{1}{|X_0|\cdots|X_{n-1}|} \sum_{(x_0,\ldots,x_{n-2}) \in X_0 \times \cdots \times X_{n-2}} (-1)^{F_{n-1}(u,x_0,\ldots,x_{n-2})\alpha^{(n-1)}} \times$$

$$\times \sum_{\substack{x_{n-1} \in X_{n-1}: \\ h_{n-1}(H_{n-1}(u,x_0,\ldots,x_{n-2}),x_{n-1}) = u'}} (-1)^{f_{n-1}(H_{n-1}(u,x_0,\ldots,x_{n-2}),x_{n-1})\alpha_{n-1}} = \frac{1}{|X_0|\cdots|X_{n-1}|} \times$$

$$\times \sum_{\substack{(x_0,\ldots,x_{n-2}) \in X_0 \times \cdots \times X_{n-2}, x_{n-1} \in X_{n-1}: \\ H_n(u,x_0,\ldots,x_{n-1}) = u'}} (-1)^{F_{n-1}(u,x_0,\ldots,x_{n-2})\alpha^{(n-1)} \oplus f_{n-1}(H_{n-1}(u,x_0,\ldots,x_{n-2}),x_{n-1})\alpha_{n-1}} =$$

$$= \frac{1}{|X_0|\cdots|X_{n-1}|} \sum_{\substack{(x_0,\ldots,x_{n-1}) \in X_0 \times \cdots \times X_{n-1}: \\ H_n(u,x_0,\ldots,x_{n-1}) = u'}} (-1)^{F_n(u,x_0,\ldots,x_{n-1})\alpha^{(n)}} = l_\alpha^{(n)}(u,u').$$

Итак, справедливо равенство (7), что и требовалось доказать.

Наконец, справедливость равенства (6) вытекает из формулы (5) и следующего равенства: $l_\alpha^{(n)}(u_0) = \left| \sum_{u' \in U} l_\alpha^{(n)}(u_0,u') \right|$.

Таким образом, теорема полностью доказана.

Отметим, что теорема 1 обобщает ряд известных утверждений о матричных (или линейных) представлениях параметров вида (2) для отображений, реализуемых конечными автоматами специального вида [3, 8, 10, 13]. Указанная теорема позволяет получить верхние оценки этого параметра, которые можно использовать для обоснования стойкости поточных или блочных шифров относительно ряда статистических атак.

Для того чтобы привести эти оценки, введем ряд дополнительных обозначений. Для любого вектора $x=(x_1,\dots,x_n)$ с действительными координатами обозначим $||x||_1=|x_1|+\dots+|x_n|$, $||x||_\infty=\max\{|x_i|: i\in\overline{1,n}\}$. Зададим обычным образом sup-норму действительной $n\times n$-матрицы A, полагая $||A||_\infty=$ $=\sup\{||Ax||_\infty : ||x||_\infty=1\}$, где супремум выбирается по всем действительным векторам $x=(x_1,\dots,x_n)^{\mathrm{T}}$ таким, что $||x||_\infty=1$. Нетрудно убедиться в том, что

$$||A||_\infty=\max\{||A_1||_1, ||A_2||_1,\dots,||A_n||_1\}, \tag{8}$$

где $A_1, A_2,\dots,A_n$ — строки матрицы A. Кроме того, для любых действительных $n\times n$-матриц A и B справедливо неравенство

$$||AB||_\infty\le||A||_\infty\,||B||_\infty. \tag{9}$$

Теорема 2. Параметр (2) удовлетворяет неравенству

$$l_\alpha^{(n)}(u_0)\le||A_{\alpha_0}^{(0)}||_\infty\,||A_{\alpha_1}^{(1)}||_\infty\cdots||A_{\alpha_{n-2}}^{(n-2)}||_\infty\,||A_{\alpha_{n-1}}^{(n-1)}\mathbf{1}||_\infty, \tag{10}$$

где

$$||A_{\alpha_i}^{(i)}||_\infty=\max_{u\in U}\left\{\frac{1}{|X|}\sum_{u'\in U}\left|\sum_{x_i\in X:\,h_i(u,x_i)=u'}(-1)^{f_i(u,x_i)\alpha_i}\right|\right\},\ i\in\overline{0,n-2},$$

$$||A_{\alpha_{n-1}}^{(n-1)}\mathbf{1}||_\infty=\max_{u\in U}\left\{\frac{1}{|X_{n-1}|}\left|\sum_{x_{n-1}\in X_{n-1}}(-1)^{f_{n-1}(u,x_{n-1})\alpha_{n-1}}\right|\right\}.$$

Кроме того, справедливо следующее неравенство:

$$\max_{(\alpha_0,\dots,\alpha_{n-1})\ne(0,\dots,0)}\{l_\alpha^{(n)}(u_0)\}\le\max_{i\in\overline{0,n-1}\ \alpha_i\ne0}\max\{||A_{\alpha_i}^{(i)}\mathbf{1}||_\infty\}. \tag{11}$$

Доказательство. Неравенство (10) следует непосредственно из равенства (6) и формул (8), (9).

Докажем неравенство (11). Обозначим i наибольшее целое число от 0 до $n-1$ такое, что $\alpha_i\ne0$. Поскольку $\alpha_{i+1}=\dots=\alpha_{n-1}=0$, то на основании формулы (4) $A_{\alpha_{i+1}}^{(i+1)}\cdots A_{\alpha_{n-1}}^{(n-1)}\mathbf{1}=\mathbf{1}$, откуда в силу формулы (6) вытекает, что $l_\alpha^{(n)}(u_0)=$ $=|\mathbf{e}\,A_{\alpha_0}^{(0)}A_{\alpha_1}^{(1)}\cdots A_{\alpha_i}^{(i)}\mathbf{1}|$. Следовательно, $l_\alpha^{(n)}(u_0)\le||A_{\alpha_0}^{(0)}||_\infty\cdots||A_{\alpha_{i-1}}^{(i-1)}||_\infty\times$ $\times||A_{\alpha_i}^{(i)}\mathbf{1}||_\infty\le||A_{\alpha_i}^{(i)}\mathbf{1}||_\infty$, что и требовалось доказать.

Теорема доказана.

НЕКОТОРЫЕ ПРИМЕНЕНИЯ

Пример 1. Рассмотрим произвольный набор подстановок $s=(s_0,\dots,s_{p-1})$, векторы $\alpha=(\alpha_0,\dots,\alpha_{p-1})$, $\beta=(\beta_0,\dots,\beta_{p-1})$, где $s_i:V_t\to V_t$, $\alpha_i,\beta_i\in V_t$, $i\in\overline{0,p-1}$, и применим теоремы 1 и 2 для нахождения верхней оценки параметра

$$l_{\alpha,\beta}(s)=2^{-2tp}\left|\sum_{x,y\in V_t^p}(-1)^{(\overset{pt}{(x+y)}\oplus x)\alpha\oplus s(y)\beta}\right|. \tag{12}$$

Здесь $x=(x_0,\dots,x_{p-1})$, $y=(y_0,\dots,y_{p-1})$, $s(y)=(s_0(y_0),\dots,s_{p-1}(y_{p-1}))$, $x_i, y_i \in V_t$, $i \in \overline{0, p-1}$, а $x \overset{pt}{+} y$ обозначает сумму по модулю 2^{pt} двоичных целых чисел, соответствующих векторам x, y (в данном случае и далее произвольный вектор $x=(x_0,\dots,x_{p-1}) \in V_t^p$ отождествляется с целым числом, младший разряд которого совпадает с самой левой координатой вектора x_0). Отметим, что к нахождению оценок параметра (12) приводит задача анализа стойкости шифра SNOW 2.0 относительно корреляционных атак [13].

Для любых $a, b \in V_t$, $i \in \overline{0, p-1}$, зададим 2×2-матрицу $A_{a,b}^{(i)}$ с элементами

$$A_{a,b}^{(i)}(u,u') = 2^{-2t} \sum_{\substack{x_i, y_i \in V_t: \\ \mathrm{msb}(x_i \overset{t}{+} y_i \overset{t}{+} u)=u'}} (-1)^{(x_i \overset{t}{+} y_i \overset{t}{+} u)a \oplus x_i a \oplus s_i(y_i)b}, \ u, u' \in \{0,1\},$$

где $\mathrm{msb}(x_i + y_i + u)$ — самый старший, т.е. t-й разряд суммы целых чисел, соответствующих указанным двоичным векторам длины t, а $x_i \overset{t}{+} y_i \overset{t}{+} u$ — сумма этих чисел по модулю 2^t.

Теорема 3. Параметр (12) удовлетворяет следующему равенству:

$$l_{\alpha,\beta}(s) = \left| (1,0)\, A_{\alpha_0,\beta_0}^{(0)} A_{\alpha_1,\beta_1}^{(1)} \cdots A_{\alpha_{p-1},\beta_{p-1}}^{(p-1)} \begin{pmatrix} 1 \\ 1 \end{pmatrix} \right|.$$

Кроме того, справедливо неравенство

$$l_{\alpha,\beta}(s) \le n_{\alpha_0,\beta_0}(s_0)\, n_{\alpha_1,\beta_1}(s_1) \ \cdots \ n_{\alpha_{p-1},\beta_{p-1}}(s_{p-1}),$$

где

$$n_{\alpha_i,\beta_i}(s_i) = || A_{\alpha_i,\beta_i}^{(i)} ||_\infty =$$

$$= \max\{ |A_{\alpha_i,\beta_i}^{(i)}(0,0)| + |A_{\alpha_i,\beta_i}^{(i)}(0,1)|, \ |A_{\alpha_i,\beta_i}^{(i)}(1,0)| + |A_{\alpha_i,\beta_i}^{(i)}(1,1)| \}, \ i \in \overline{0, p-1}.$$

Доказательство. На основании теорем 1 и 2 достаточно убедиться в том, что отображение $F(x,y) = ((x \overset{pt}{+} y) \oplus x, s(y))$, $x, y \in V_t^p$ (множества $V_t^p \times V_t^p$ в себя) реализуется последовательностью конечных автоматов $(X_i, U, V_{2t_i}, h_i, f_i)$, где $X_i = V_{2t_i} = V_{2t}, U = \{0,1\}$, а функции h_i, f_i для каждого $i \in \overline{0, p-1}$ определяются следующим образом:

$$h_i(u,(x_i,y_i)) = \mathrm{msb}(u + x_i + y_i), \ u \in U, \ (x_i, y_i) \in X_i,$$

$$f_i(u,(x_i,y_i)) = ((u \overset{t}{+} x_i \overset{t}{+} y_i) \oplus x_i, s_i(y_i)), \ u \in U, \ (x_i, y_i) \in X_i.$$

Действительно, обозначим $z = (z_0,\dots,z_{p-1}) = (x \overset{pt}{+} y) \oplus x$ и положим

$$u_0 = 0, \ u_{i+1} = h_i(u_i,(x_i,y_i)), \ z_i' = (u_i \overset{t}{+} x_i \overset{t}{+} y_i) \oplus x_i, \ i \in \overline{0, p-1}.$$

С помощью индукции по i нетрудно убедиться в том, что $z_i = z_i'$ для любого $i \in \overline{0, p-1}$. Отсюда следует, что отображение F совпадает с отображением (1) для указанных ранее функций h_i, f_i, фиксированного значения $u_0 = 0$ и $n = p$, что и требовалось доказать.

Таким образом, теорема полностью доказана.

Пример 2. Применим теорему 1 для получения верхней оценки параметра

$$L^{(s)}_{\alpha,\beta} = 2^{-tp} \sum_{k \in V_t^p} \left(2^{-tp} \sum_{x \in V_t^p} (-1)^{s(\overset{pt}{x+k})\beta \oplus x\alpha} \right)^2 \tag{13}$$

(здесь и далее используются обозначения, введенные в примере 1).

Для любых $\alpha_i, \beta_i, k_i \in V_t$, $i \in \overline{0, p-1}$, зададим 2×2-матрицу $A^{(i)}_{\alpha_i,\beta_i,k_i}$ с элементами

$$A^{(i)}_{\alpha_i,\beta_i,k_i}(u,u') = 2^{-t} \sum_{\substack{x_i \in V_t: \\ \mathrm{msb}(x_i+k_i+u)=u'}} (-1)^{s_i(x_i \overset{t}{+} k_i \overset{t}{+} u)\beta_i \oplus x_i\alpha_i}, \ u,u' \in \{0,1\}. \tag{14}$$

Теорема 4. Справедливо неравенство

$$L^{(s)}_{\alpha,\beta} \le \Lambda^{(s_0)}_{\alpha_0,\beta_0} \Lambda^{(s_1)}_{\alpha_1,\beta_1} \ \cdots \ \Lambda^{(s_{p-2})}_{\alpha_{p-2},\beta_{p-2}} L^{(s_{p-1})}_{\alpha_{p-1},\beta_{p-1}}, \tag{15}$$

где

$$\Lambda^{(s_i)}_{\alpha_i,\beta_i} = 2^{-t} \sum_{k_i \in V_t} \left(2^{-t} \sum_{v \in \{0,1\}} \left| \sum_{\substack{x_i \in V_t: \\ \mathrm{msb}(x_i+k_i)=v}} (-1)^{s_i(x_i \overset{t}{+} k_i)\beta_i \oplus x_i\alpha_i} \right| \right)^2, \ i \in \overline{0, p-2}. \tag{16}$$

$$L^{(s_{p-1})}_{\alpha_{p-1},\beta_{p-1}} = 2^{-t} \sum_{k_{p-1} \in V_t} \left(2^{-t} \sum_{x_{p-1} \in V_t} (-1)^{s_{p-1}(x_{p-1} \overset{t}{+} k_{p-1})\beta_{p-1} \oplus x_{p-1}\alpha_{p-1}} \right)^2.$$

Доказательство. Для заданных $s = (s_0, \ldots, s_{p-1})$, $\alpha = (\alpha_0, \ldots, \alpha_{p-1})$, $\beta = (\beta_0, \ldots, \beta_{p-1})$ обозначим $s' = (s_1, \ldots, s_{p-1})$, $\alpha' = (\alpha_1, \ldots, \alpha_{p-1})$, $\beta' = (\beta_1, \ldots, \beta_{p-1})$ и покажем, что

$$L^{(s)}_{\alpha,\beta} \le \Lambda^{(s_0)}_{\alpha_0,\beta_0} L^{(s')}_{\alpha',\beta'}. \tag{17}$$

Отсюда по индукции следует справедливость неравенства (15).

Для любого $k = (k_0, \ldots, k_{p-1}) \in V_t^p$ рассмотрим последовательность, состоящую из p автоматов с входным алфавитом $X_i = V_t$, множеством состояний $U = \{0,1\}$, выходным алфавитом $Y_i = V_t \times V_t$ и функциями переходов и выходов $h_i(u, x_i) = \mathrm{msb}(u + x_i + k_i)$, $u \in U$, $x_i \in X_i$, и $f_i(u, x_i) = (s_i(u \overset{t}{+} x_i \overset{t}{+} k_i), x_i)$, $u \in U$, $x_i \in X_i$, соответственно, $i \in \overline{0, p-1}$.

Из данных определений следует, что при $n = p$ и $u_0 = 0$ отображение (1) равно отображению $(s(\overset{pt}{x+k}), x)$, $x \in V_t^p$. Следовательно, на основании теоремы 1 выполняется равенство

$$2^{-tp} \sum_{x \in V_t^p} (-1)^{s(\overset{pt}{x+k})\beta \oplus x\alpha} = (1\,0)\, A^{(0)}_{\alpha_0,\beta_0,k_0} A^{(1)}_{\alpha_1,\beta_1,k_1} \cdots A^{(p-1)}_{\alpha_{p-1},\beta_{p-1},k_{p-1}} \begin{pmatrix} 1 \\ 1 \end{pmatrix}. \tag{18}$$

Кроме того, из теоремы 1 следует, что для любых $u, v \in \{0,1\}$ справедливо следующее равенство:

$$2^{-t(p-1)} \sum_{\substack{x' \in V_t^{p-1}: \\ \mathrm{msb}(x'+k'+u)=v}} (-1)^{s'(x' \overset{(p-1)t}{+} k' \overset{(p-1)t}{+} u)\beta' \oplus x'\alpha'} = (A^{(1)}_{\alpha_1,\beta_1,k_1} \cdots A^{(p-1)}_{\alpha_{p-1},\beta_{p-1},k_{p-1}})(u,v). \tag{19}$$

Обозначим

$$(a(k_0), b(k_0)) = (1\,0)\, A^{(0)}_{\alpha_0,\beta_0,k_0},\ \begin{pmatrix} c(k') \\ d(k') \end{pmatrix} = A^{(1)}_{\alpha_1,\beta_1,k_1} \cdots A^{(p-1)}_{\alpha_{p-1},\beta_{p-1},k_{p-1}} \begin{pmatrix} 1 \\ 1 \end{pmatrix}.$$

Из равенства (18) следует, что

$$\left| 2^{-tp} \sum_{x \in V_t^p} (-1)^{s(x \overset{pt}{+} k)\beta \oplus x\alpha} \right|^2 = |a(k_0)c(k') + b(k_0)d(k')|^2 \le$$

$$\le (|a(k_0)| + |b(k_0)|)^2 \left(\frac{|a(k_0)|}{|a(k_0)| + |b(k_0)|} |c(k')| + \frac{|b(k_0)|}{|a(k_0)| + |b(k_0)|} |d(k')| \right)^2 \le$$

$$\le (|a(k_0)| + |b(k_0)|)^2 \left(\frac{|a(k_0)|}{|a(k_0)| + |b(k_0)|} |c(k')|^2 + \frac{|b(k_0)|}{|a(k_0)| + |b(k_0)|} |d(k')|^2 \right). \quad (20)$$

При этом на основании формул (14), (16)

$$2^{-t} \sum_{k_0 \in V_t} (|a(k_0)| + |b(k_0)|)^2 = 2^{-t} \sum_{k_0 \in V_t} (|A^{(0)}_{\alpha_0,\beta_0,k_0}(0,0)| + |A^{(0)}_{\alpha_0,\beta_0,k_0}(0,1)|)^2 =$$

$$= 2^{-t} \sum_{k_0 \in V_t} \left(2^{-t} \sum_{v \in \{0,1\}} \left| \sum_{\substack{x_0 \in V_t: \\ \mathrm{msb}(x_0 + k_0) = v}} (-1)^{s_0(x_0 \overset{t}{+} k_0)\beta_0 \oplus x_0\alpha_0} \right| \right)^2 = \Lambda^{(s_0)}_{\alpha_0,\beta_0}. \quad (21)$$

Далее, согласно формуле (19)

$$2^{-t(p-1)} \sum_{k' \in V_t^{p-1}} |c(k')|^2 = 2^{-t(p-1)} \sum_{k' \in V_t^{p-1}} |d(k')|^2 =$$

$$= 2^{-t(p-1)} \sum_{k' \in V_t^{p-1}} \left(2^{-t(p-1)} \sum_{x' \in V_t^{p-1}:} (-1)^{s'(x' \overset{(p-1)t}{+} k')\beta' \oplus x'\alpha'} \right)^2 = L^{(s')}_{\alpha',\beta'}. \quad (22)$$

Из соотношений (20)–(22) непосредственно следует неравенство (17).

Теорема доказана.

Отметим, что неравенство (15) получено другим способом в [8]. Приведенное выше доказательство поясняет смысл параметра (16): он равен среднему значению квадратов l_1-норм первых строк матриц $A^{(i)}_{\alpha_i,\beta_i,k_i}$ по всем $k_i \in V_t$.

ЗАКЛЮЧЕНИЕ

Изложенные результаты показывают, что для нахождения верхних оценок несбалансированности дискретных функций можно применять общий метод, состоящий из следующих этапов:

— построить реализующую заданную функцию последовательность конечных автоматов с одним и тем же множеством состояний (при этом для практического применения желательно, чтобы мощность множества состояний была как можно меньшей);

— воспользоваться приведенным в теореме 1 матричным представлением для несбалансированности;

— перейти в этом представлении к матричным нормам для получения верхних оценок.

Изложенный метод обобщает и унифицирует ряд известных подходов к нахождению матричных (линейных) представлений или оценок несбалансированности функций специального вида [3, 8, 10, 13] и его можно применять для решения задач обоснования стойкости поточных или блочных шифров относительно ряда статистических атак.

СПИСОК ЛИТЕРАТУРЫ

1. Staffelbach O., Meier W. Cryptographic significance of the carry for ciphers based on integer addition. In: *Advances in Cryptology-CRYPTO'90. LNCS.* 1991. Vol. 537. P. 601–615.
2. Шерстнев В.И. Совместное распределение переносов при сложении целых чисел. *Теория вероятностей и ее применения*. 1996. Т. 91(2). С. 467–473.
3. Wallén J. Linear approximation of addition modulo 2^n. In: *Fast Software Encryption. FSE 2003. LNCS*. 2003. Vol. 2887. P. 261–273.
4. Lipmaa H., Moriai S. Efficient algorithms for computing differential properties of addition. In: *Fast Software Encryption*. *FSE 2001. LNCS*. 2002. Vol. 2355. P. 336–350.
5. Lipmaa H., Wallén J., Dumas P. On the additive differential probability of exlusive-or. In: *Fast Software Encryption*. *FSE 2004*. *LNCS*. 2004. Vol. 3017. P. 317–331.
6. Lipmaa H. On differential properties of pseudo-hadamard transform and related mappings. In: *Progress in Cryptology-INDOCRYPT 2002. LNCS*. 2002. Vol. 2551. P. 48–61.
7. Ковальчук Л.В., Сиренко О.А. Анализ перемешивающих свойств операций модульного и побитового сложения, определенных на одном носителе. *Кибернетика и системный анализ*. 2011. Т. 47, № 5. С. 83–97.
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 Stochastic Processes*. 2006. Vol. 12(28), N 1–2. P. 20–32.
9. Алексейчук А.Н., Ковальчук Л.В., Шевцов А.С., Яковлев С.В. О криптографических свойствах нового национального стандарта шифрования Украины. *Кибернетика и системный анализ*. 2016. Т. 52, № 3. С. 16–31.
10. Alekseychuk A.N., Kovalchuk L.V. Towards a theory of security evaluation for GOST-like ciphers against differential and linear cryptanalysis. Cryptology ePrint Archive, Report 2011/489. URL: http://eprint.iacr.org/2011/489.
11. Ковальчук Л.В., Бездетный В.Т. Верхние оценки средних вероятностей разностных характеристик блочных шифров с чередованием марковских и обобщенно марковских преобразований. *Кибернетика и системный анализ*. 2014. Т. 50, № 3. С. 71–78.
12. Watanabe D., Biryukov A., de Canniére C. A distinguishing attack of SNOW 2.0 with linear masking method. In: *Selected Arreas in Cryptography*. *SAC 2003*. *LNCS*. 2003. Vol. 3006. P. 222–233.
13. Nyberg K., Wallén J. Improved linear distinguishers for SNOW 2.0. In: *Fast Software Encryption. FSE 2006*. *LNCS*. 2006. Vol. 4047. P. 144–162.
14. Maximov A., Johansson Th. Fast computation for large distribution and and its cryptographic application. In: *Advanced in Cryptology-ASIACRYPT 2005*. *LNCS*. 2005. Vol. 3788. P. 313–332.
15. Lee J.-K., Lee D.H., Park S. Cryptanalysis of SOSEMANUC and SNOW 2.0 using linear masks. In: *Advanced in Cryptology-ASIACRYPT 2008*. *LNCS*. 2008. Vol. 5350. P. 524–538.
16. Zhang B., Xu C., Meier W. Fast correlation attacks over extension fields, large-unit linear approximation and cryptanalysis of SNOW 2.0. Cryptology ePrint Archive, Report 2016/311. URL: http://eprint.iacr.org/2016/311.
17. Ekdahl P., Johansson T. A new version of the stream cipher SNOW. In: *Selected Areas in Cryptography. SAC 2002. LNCS*. 2002. Vol. 2295. P. 47–61.

18. Gorbenko I., Kuznetsov A., Gorbenko Yu., Alekseychuk A., Timchenko V. Strumok Keystream Generator. *The 9th IEEE International Conference on Dependable Systems, Services and Technologies, DESSERT'2018*, 24–27 May, 2018, Kyiv, Ukraine. P. 292–299.

19. Жуков А.Е., Чистяков В.П. Матричный подход к исследованию прообразов выходной последовательности конечного автомата. *Обозрение прикл. промышл. матем*. 1994. Т. 1, вып. 1. С. 108–117.

Надійшла до редакції 27.11.2018

А.М. Олексійчук, С.М. Конюшок, М.В. Поремський

ВЕРХНІ ОЦІНКИ НЕЗБАЛАНСОВАНОСТІ ДИСКРЕТНИХ ФУНКЦІЙ, ЩО РЕАЛІЗУЮТЬСЯ ПОСЛІДОВНОСТЯМИ СКІНЧЕННИХ АВТОМАТІВ

Анотація. Отримано матричне представлення і верхні оцінки незбалансованості довільної дискретної функції, що реалізується послідовністю скінченних автоматів. Наведено результати, що узагальнюють низку відомих раніше тверджень про матричні (лінійні) представлення незбалансованості функцій спеціального вигляду, які можна застосувати для розв'язання задач обґрунтування стійкості потокових чи блокових шифрів відносно низки статистичних атак.

Ключові слова: кореляційний криптоаналіз, незбалансованість дискретної функції, скінченний автомат, операція додавання за модулем 2^n, SNOW 2.0, «Струмок».

A.N. Alekseychuk, S.M. Koniushok, M.V. Poremskyi

UPPER BOUNDS FOR IMBALANCE OF DISCRETE FUNCTIONS REALIZED BY SEQUENCES OF FINITE-STATE MACHINES

Abstact. A matrix representation and upper bounds of the imbalance of an arbitrary discrete function realized by a sequence of finite-state machines are obtained. The obtained results generalize a number of previously known assertions about matrix (linear) representations of the imbalance of the special form functions and can be used to solve the problems of security proofs of stream or block ciphers against a number of statistical attacks.

Keywords: correlation cryptanalysis, imbalance of discrete function, finite-state machine, addition modulo 2^n operation, SNOW 2.0, «Strumok».

Алексейчук Антон Николаевич,
доктор техн. наук, доцент, профессор кафедры Национального технического университета Украины «Киевский политехнический институт имени Игоря Сикорского», e-mail: alex-dtn@ukr.net.

Конюшок Сергей Николаевич,
кандидат техн. наук, доцент, заместитель начальника института по научной работе Института специальной связи и защиты информации Национального технического университета Украины «Киевский политехнический институт имени Игоря Сикорского», e-mail: 3tooth@iszzi.kpi.ua.

Поремский Михаил Васильевич,
аспирант Национального технического университета Украины «Киевский политехнический институт имени Игоря Сикорского», e-mail: undermyclouds@gmail.com.