УДК 621.391:519.2:519.7

А.Н. АЛЕКСЕЙЧУК, Л.В. КОВАЛЬЧУК, А.С. ШЕВЦОВ, С.В. ЯКОВЛЕВ

О КРИПТОГРАФИЧЕСКИХ СВОЙСТВАХ НОВОГО НАЦИОНАЛЬНОГО СТАНДАРТА ШИФРОВАНИЯ УКРАИНЫ

Аннотация. Исследован ряд криптографических свойств блочного шифра «Калина», принятого в качестве нового национального стандарта шифрования Украины. Проанализированы важнейшие свойства компонент этого шифра. Показано, что его раундовые преобразования порождают знакопеременную группу подстановок, а сам шифр является обоснованно стойким относительно разностного и линейного криптоанализа.

Ключевые слова: симметричная криптография, блочный шифр, конечная группа подстановок, разностный криптоанализ, линейный криптоанализ, национальный стандарт шифрования Украины, шифр «Калина».

ВВЕДЕНИЕ

В 2015 г. в Украине принят новый национальный стандарт шифрования — блочный шифр «Калина» [1]. Основные принципы, которыми руководствовались разработчики шифра, изложены в работе [2], а в [3] описана одна из первых атак на редуцированную версию «Калины». В настоящей статье представлены результаты исследования криптографических свойств шифра «Калина», отсутствующие в [2, 3].

Исследования проводились по следующим направлениям:

— анализ общей структуры блочного шифра (за исключением процедуры формирования раундовых ключей);

— исследования криптографических свойств отдельных компонент шифра (узлов замены и линейных преобразований);

— оценка и обоснование стойкости шифра относительно алгебраических и статистических методов криптоанализа (разностного, линейного и алгебраических атак, основанных на гомоморфизмах).

В разд. 1 описано SPN-представление шифра «Калина» (с точностью до процедуры формирования раундовых ключей [1, п. 7]), которое служит основой дальнейших исследований и позволяет применять для анализа шифра известные методы. В разд. 2 проанализированы криптографические свойства используемых в «Калине» узлов замены и линейных преобразований; приведены значения параметров, характеризирующих разностные, корреляционные (линейные) и комбинаторные свойства отдельных компонент шифра. Полученные результаты используются далее при анализе и обосновании стойкости шифра относительно ряда методов криптоанализа. В разд. 3 исследована группа подстановок, порожденная раундовыми преобразованиями «Калины». Базируясь на результатах работы [4], показано, что эта группа является знакопеременной для любой версии шифра. В разд. 4 сформулирована теорема, содержащая оценки теоретической стойкости (provable security) «Калина»-подобных блочных шифров относительно разностного и линейного криптоанализа. Доказательство теоремы представлено в разд. 5, а в заключении сформулированы краткие выводы.

1. SPN-ПРЕДСТАВЛЕНИЕ ШИФРА «КАЛИНА»

Рассмотрим общий класс блочных шифров, к которому относится «Калина». Предварительно введем ряд обозначений.

Для любого натурального m обозначим V_m множество двоичных векторов длины m. Зафиксируем натуральные числа t, q, c, r, при этом $t, q, c \geq 2$, $r \geq 4$,

$q < 2^{t-1}+1$, и положим $p = cq$, $n = pt$. Зададим на V_t структуру поля порядка 2^t, согласованную с операцией покоординатного булевого сложения двоичных векторов. Последнюю обозначим символом $\oplus$ (независимо от длины векторов-слагаемых x, $y \in V_m$). В дальнейшем будем отождествлять множество V_t с полем $\mathbf{GF}(2^t)$, а множество V_{mt} — с m-мерным векторным пространством над этим полем. Произвольный вектор $x \in V_n = \mathbf{GF}(2^t)^p$ будем записывать в виде $x = (x_1, \ldots, x_c)$, где $x_j = (x_{1,j}, \ldots, x_{q,j})$, $x_{i,j} \in V_t = \mathbf{GF}(2^t)$, $i \in \overline{1, q}$, $j \in \overline{1, c}$, и называть векторы $x_1, \ldots, x_c$ компонентами, а элементы $x_{1,1}, \ldots, x_{q,1}, \ldots$ $\ldots, x_{1,c}, \ldots, x_{q,c}$ — координатами вектора x.

Зафиксируем семейство подстановок $s_{i,j}\colon V_t \to V_t$, $i \in \overline{1, q}$, $j \in \overline{1, c}$. Зададим подстановки $s_j : V_{tq} \to V_{tq}$ и $s\colon V_n \to V_n$, полагая

$$s_j(x_{1,j}, \ldots, x_{q,j}) = (s_{1,j}(x_{1,j}), \ldots, s_{q,j}(x_{q,j})),\ x_{i,j} \in V_t,\ i \in \overline{1, q},\ j \in \overline{1, c}, \quad (1)$$

$$s(x) = (s_1(x_1), \ldots, s_c(x_c)),\ x \in V_n. \quad (2)$$

Далее, зафиксируем перестановку g на множестве $\overline{1, q} \times \overline{1, c}$ и положим для любого $x \in V_n = \mathbf{GF}(2^t)^p$

$$\hat{g}(x) = (x_{g(1,1)}, \ldots, x_{g(q,1)}, \ldots, x_{g(1,c)}, \ldots, x_{g(q,c)}). \quad (3)$$

Отображение $\hat{g}$ является линейным преобразованием векторного пространства $\mathbf{GF}(2^t)^p$, переставляющим координаты $x_{i,j}$ произвольного вектора x в соответствии с перестановкой g, и может быть записано в виде

$$\hat{g}(x) = xG_p,\ x \in \mathbf{GF}(2^t)^p, \quad (4)$$

где G_p — подстановочная $p \times p$-матрица над полем $\mathbf{GF}(2^t)$. Назовем матрицу G_p соответствующей перестановке g.

Зафиксируем МДР-матрицу D порядка q над полем $\mathbf{GF}(2^t)$, т.е. такую $q \times q$-матрицу над этим полем, все квадратные подматрицы которой являются невырожденными. Заметим, что на основании приведенного выше условия $q < 2^{t-1}+1$ указанная матрица заведомо существует (см. [5] и [6, с. 313]).

Наконец, зададим на множестве V_n бинарную операцию $\overset{\circ}{+}$, полагая для любых x, $y \in V_n$

$$x \overset{\circ}{+} y = (x_1 + y_1, \ldots, x_c + y_c),$$

где $x_j + y_j$ — сумма по модулю 2^{tq} двоичных целых чисел, соответствующих векторам x_j, $y_j \in V_{tq}$, $j \in \overline{1, c}$. Обозначим

$$M_p = G_p \cdot \mathrm{diag}\,(\underbrace{D, \ldots, D}_{c \text{ раз}}), \quad (5)$$

$$\varphi(x) = s(x) M_p,\ x \in \mathbf{GF}(2^t)^p, \quad (6)$$

и рассмотрим r-раундовый блочный шифр $\mathfrak{I}$ с множеством открытых (шифрованных) сообщений V_n, множеством раундовых ключей $K = V_n$ и семейством шифрующих преобразований

$$F_\lambda = f_{r,k_r} \circ \ldots \circ f_{1,k_1},\ \lambda = (k_1, \ldots, k_r) \in K^r, \quad (7)$$

где для любых $x \in V_n$, $k \in K$, $i \in \overline{1, r}$

$$f_{i,k}(x) = \varphi(x \overset{\circ}{+} k), \text{ если } i = 1; \tag{8.1}$$

$$f_{i,k}(x) = \varphi(x \oplus k), \text{ если } 2 \le i \le r-1, \tag{8.2}$$

$$f_{i,k}(x) = x \overset{\circ}{+} k, \text{ если } i = r. \tag{9}$$

Назовем отображение φ вида (6) раундовой функцией шифра $\Im$, а подстановки $s_{i,j}$ ($i \in \overline{1, q}$, $j \in \overline{1, c}$) — узлами замены (или s-блоками) этого шифра.

Алгоритм «Калина-l/k» (с точностью до процедуры формирования раундовых ключей) относится к классу блочных шифров указанного выше вида. В табл. 1 приведены значения параметров n, p, c и r для каждой пары исходных значений l, k, где l — длина блока, а k — длина ключа шифрования [1]. Заметим, что при этом $t = q = 8$, c совпадает с количеством столбцов матрицы состояния, а r на единицу больше количества раундов, указанных в табл. 1 из [1]. Кроме того, входное (выходное) сообщение $x \in V_n$ в каждом раунде отождествляется с матрицей состояния (см. [1, п. 4]), составленной из координат $x_{i,j}$ вектора x. Аналогичным образом представляются раундовые ключи.

Таблица 1

Исходные значения		Значения параметров			
l	k	n	p	c	r
128	128	128	16	2	11
128	256	128	16	2	15
256	256	256	32	4	15
256	512	256	32	4	19
512	512	512	64	8	19

Во всех версиях шифра «Калина» используются четыре различные подстановки $s_{i,j}$, которые обозначены в [1] символами π_0, π_1, π_2 и π_3; при этом $s_{i,j} = \pi_{(i-1) \bmod 4}$ для любых $i \in \overline{1, q}$, $j \in \overline{1, c}$. Перестановка g определяется по формуле $g(i, j) = \left(i, \left(j + \left\lfloor \frac{i \cdot n}{512} \right\rfloor \right) \bmod c + 1 \right)$, $i \in \overline{1, q}$, $j \in \overline{1, c}$ (см. [1, п. 6.4]). Отображение $\hat{g}$, используемое в шифре «Калина» с длиной блока n бит, имеет следующий вид:

а) при $n = 128$

$$\begin{pmatrix} x_{1,1} & x_{2,1} \\ x_{1,2} & x_{2,2} \\ x_{1,3} & x_{2,3} \\ x_{1,4} & x_{2,4} \\ x_{1,5} & x_{2,5} \\ x_{1,6} & x_{2,6} \\ x_{1,7} & x_{2,7} \\ x_{1,8} & x_{2,8} \end{pmatrix} \overset{\hat{g}}{\mapsto} \begin{pmatrix} x_{1,1} & x_{2,1} \\ x_{1,2} & x_{2,2} \\ x_{1,3} & x_{2,3} \\ x_{1,4} & x_{2,4} \\ x_{2,5} & x_{1,5} \\ x_{2,6} & x_{1,6} \\ x_{2,7} & x_{1,7} \\ x_{2,8} & x_{1,8} \end{pmatrix};$$

б) при $n = 256$

$$\begin{pmatrix} x_{1,1} & x_{2,1} & x_{3,1} & x_{4,1} \\ x_{1,2} & x_{2,2} & x_{3,2} & x_{4,2} \\ x_{1,3} & x_{2,3} & x_{3,3} & x_{4,3} \\ x_{1,4} & x_{2,4} & x_{3,4} & x_{4,4} \\ x_{1,5} & x_{2,5} & x_{3,5} & x_{4,5} \\ x_{1,6} & x_{2,6} & x_{3,6} & x_{4,6} \\ x_{1,7} & x_{2,7} & x_{3,7} & x_{4,7} \\ x_{1,8} & x_{2,8} & x_{3,8} & x_{4,8} \end{pmatrix} \overset{\hat{g}}{\mapsto} \begin{pmatrix} x_{1,1} & x_{2,1} & x_{3,1} & x_{4,1} \\ x_{1,2} & x_{2,2} & x_{3,2} & x_{4,2} \\ x_{4,3} & x_{1,3} & x_{2,3} & x_{3,3} \\ x_{4,4} & x_{1,4} & x_{2,4} & x_{3,4} \\ x_{3,5} & x_{4,5} & x_{1,5} & x_{2,5} \\ x_{3,6} & x_{4,6} & x_{1,6} & x_{2,6} \\ x_{2,7} & x_{3,7} & x_{4,7} & x_{1,7} \\ x_{2,8} & x_{3,8} & x_{4,8} & x_{1,8} \end{pmatrix};$$

в) $n = 512$

$$\begin{pmatrix} x_{1,1} & x_{2,1} & x_{3,1} & x_{4,1} & x_{5,1} & x_{6,1} & x_{7,1} & x_{8,1} \\ x_{1,2} & x_{2,2} & x_{3,2} & x_{4,2} & x_{5,2} & x_{6,2} & x_{7,2} & x_{8,2} \\ x_{1,3} & x_{2,3} & x_{3,3} & x_{4,3} & x_{5,3} & x_{6,3} & x_{7,3} & x_{8,3} \\ x_{1,4} & x_{2,4} & x_{3,4} & x_{4,4} & x_{5,4} & x_{6,4} & x_{7,4} & x_{8,4} \\ x_{1,5} & x_{2,5} & x_{3,5} & x_{4,5} & x_{5,5} & x_{6,5} & x_{7,5} & x_{8,5} \\ x_{1,6} & x_{2,6} & x_{3,6} & x_{4,6} & x_{5,6} & x_{6,6} & x_{7,6} & x_{8,6} \\ x_{1,7} & x_{2,7} & x_{3,7} & x_{4,7} & x_{5,7} & x_{6,7} & x_{7,7} & x_{8,7} \\ x_{1,8} & x_{2,8} & x_{3,8} & x_{4,8} & x_{5,8} & x_{6,8} & x_{7,8} & x_{8,8} \end{pmatrix} \overset{\hat{g}}{\mapsto}$$

$$\overset{\hat{g}}{\mapsto} \begin{pmatrix} x_{1,1} & x_{2,1} & x_{3,1} & x_{4,1} & x_{5,1} & x_{6,1} & x_{7,1} & x_{8,1} \\ x_{8,2} & x_{1,2} & x_{2,2} & x_{3,2} & x_{4,2} & x_{5,2} & x_{6,2} & x_{7,2} \\ x_{7,3} & x_{8,3} & x_{1,3} & x_{2,3} & x_{3,3} & x_{4,3} & x_{5,3} & x_{6,3} \\ x_{6,4} & x_{7,4} & x_{8,4} & x_{1,4} & x_{2,4} & x_{3,4} & x_{4,4} & x_{5,4} \\ x_{5,5} & x_{6,5} & x_{7,5} & x_{8,5} & x_{1,5} & x_{2,5} & x_{3,5} & x_{4,5} \\ x_{4,6} & x_{5,6} & x_{6,6} & x_{7,6} & x_{8,6} & x_{1,6} & x_{2,6} & x_{3,6} \\ x_{3,7} & x_{4,7} & x_{5,7} & x_{6,7} & x_{7,7} & x_{8,7} & x_{1,7} & x_{2,7} \\ x_{2,8} & x_{3,8} & x_{4,8} & x_{5,8} & x_{6,8} & x_{7,8} & x_{8,8} & x_{1,8} \end{pmatrix}.$$

Используя данную информацию, а также формулы (3), (4), нетрудно убедиться в том, что первой из трех перестановок ($n = 128$) соответствует матрица

$$G_{16} = \begin{pmatrix} I\,0\,0\,0 \\ 0\,0\,0\,I \\ 0\,0\,I\,0 \\ 0\,I\,0\,0 \end{pmatrix},$$

где I и 0 — соответственно единичная и нулевая матрицы четвертого порядка над полем $\mathbf{GF}(2^8)$.

Второй перестановке ($n = 256$) соответствует матрица

$$G_{32} = \begin{pmatrix}
I & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & I & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & I & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & I \\
0 & 0 & 0 & 0 & I & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & I & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & I & 0 \\
0 & 0 & 0 & I & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & I & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & I & 0 & 0 \\
0 & 0 & I & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & I & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & I & 0 & 0 & 0 \\
0 & I & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & I & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & I & 0 & 0 & 0 & 0
\end{pmatrix}.$$

Здесь I и 0 — соответственно единичная и нулевая матрицы второго порядка над полем $\mathbf{GF}(2^8)$.

Третьей перестановке ($n = 512$) соответствует циркулянтная матрица G_{64} порядка 64 над полем $\mathbf{GF}(2)$, первый столбец которой равен $(1, 0, \ldots, 0)^{\mathrm{T}}$, а каждый следующий столбец образуется при циклическом сдвиге предыдущего на семь позиций вверх.

Во всех версиях «Калины» используется одна и та же МДР-матрица D порядка 8 над полем $\mathbf{GF}(2^8)$, которая является транспонированной к матрице, приведенной в [1, п. 5.5].

Таким образом, шифр «Калина» относится к классу Rijndael-подобных блочных шифров, однако заметно отличается от шифра Rijndael. В частности, в шифре «Калина» применяются:

— оригинальная процедура формирования раундовых ключей [1, п. 7];

— процедура «отбеливания» с помощью алгебраической операции $\overset{\circ}{+}$;

— узлы замены $\pi_0, \pi_1, \pi_2, \pi_3$, выбранные в соответствии с определенными критериями [2].

2. КРИПТОГРАФИЧЕСКИЕ СВОЙСТВА И ПАРАМЕТРЫ ОТДЕЛЬНЫХ КОМПОНЕНТ ШИФРА «КАЛИНА»

Значения параметров, характеризующих разностные и корреляционные свойства узлов замены. Для любой подстановки π на множестве V_t обозначим

$$d_{\oplus}^{(\pi)} = \max\{d_{\oplus}^{(\pi)}(\alpha, \beta): \alpha, \beta \in V_t \setminus \{0\}\},\ d_{+}^{(\pi)} = \max\{d_{+}^{(\pi)}(\alpha, \beta): \alpha, \beta \in V_t \setminus \{0\}\}, \quad (10)$$

$$l_{\oplus}^{(\pi)} = \max\{l_{\oplus}^{(\pi)}(\alpha, \beta): \alpha, \beta \in V_t \setminus \{0\}\}, \quad (11)$$

$$l_{+}^{(\pi)} = \max\{l_{+}^{(\pi)}(\alpha, \beta): \alpha, \beta \in V_t \setminus \{0\}\},\ \Lambda^{(\pi)} = \max\{\Lambda^{(\pi)}(\alpha, \beta): \alpha, \beta \in V_t \setminus \{0\}\}, \quad (12)$$

где

$$d_{\oplus}^{(\pi)}(\alpha,\beta)=2^{-t}\sum_{k\in V_t}\delta(\pi(k\oplus\alpha)\oplus\pi(k),\beta), \tag{13}$$

$$d_{+}^{(\pi)}(\alpha,\beta)=2^{-t}\sum_{k\in V_t}\delta(\pi(k+\alpha)\oplus\pi(k),\beta), \tag{14}$$

$$l_{\oplus}^{(\pi)}(\alpha,\beta)=2^{-t}\sum_{k\in V_t}(2^{-t}\sum_{x\in V_t}(-1)^{\alpha x\oplus\beta\pi(x\oplus k)})^2, \tag{15}$$

$$l_{+}^{(\pi)}(\alpha,\beta)=2^{-t}\sum_{k\in V_t}(2^{-t}\sum_{x\in V_t}(-1)^{\alpha x\oplus\beta\pi(x+k)})^2, \tag{16}$$

$$\Lambda^{(\pi)}(\alpha,\beta)=2^{-t}\sum_{k\in V_t}\left(2^{-t}\sum_{a\in\{0,1\}}\left|\sum_{x\in V_t:\,\nu(x,k)=a}(-1)^{\alpha x\oplus\beta\pi(x+k)}\right|\right)^2. \tag{17}$$

Символы $\oplus$ и $+$ в формулах (10)–(17) обозначают операции покоординатного булевого сложения двоичных векторов длины t и сложения по модулю 2^t двоичных целых чисел, соответствующих этим векторам. Под обозначением $\nu(x,k)$ в формуле (17) понимаем бит переноса в t-й разряд при сложении (в кольце **Z**) целых чисел, соответствующих векторам $x, k\in V_t$.

Параметры (10) характеризуют разностные свойства подстановки π относительно операций $\oplus$, $+$, а параметры (11), (12) — ее корреляционные (линейные) свойства относительно этих операций. Матрицы размера $(2^t-1)\times(2^t-1)$, состоящие из элементов (13) и (15), где α и β пробегают все ненулевые элементы множества V_t, называются таблицей разностей и таблицей линейных аппроксимаций подстановки π соответственно. При этом расширенные таблица разностей и таблица линейных аппроксимаций подстановки π состоят соответственно из элементов (13) и (15) для всех $\alpha,\beta\in V_t$.

Отметим, что вектор $\alpha\in V_t$ называется линейным транслятором функции $f: V_t\to\{0,1\}$, если для любого $x\in V_t$ выполняется равенство $f(x\oplus\alpha)=f(x)$. Согласно определению [7] подстановка π имеет тривиальную линейную структуру, если для каждой ненулевой линейной комбинации ее координатных функций не существует ненулевых линейных трансляторов. Известно [8], что для тривиальности линейной структуры подстановки $\pi: V_t\to V_t$ достаточно выполнения условия $NW^{(\pi)}<2^{t-1}$, где $NW^{(\pi)}$ — максимальное количество нулевых элементов в столбцах таблицы линейных аппроксимаций этой подстановки.

В табл. 2 приведены значения параметров (10)–(12) для узлов замены шифра «Калина». При этом $NW^{(\pi_0)}=37$, $NW^{(\pi_1)}=33$, $NW^{(\pi_2)}=36$, $NW^{(\pi_3)}=35$.

Таблица 2

Подстановка π	Значения параметров				
	$d_{\oplus}^{(\pi)}$	$d_{+}^{(\pi)}$	$l_{\oplus}^{(\pi)}$	$l_{+}^{(\pi)}$	$\Lambda^{(\pi)}$
π_0	2^{-5}	$6\cdot2^{-8}$	$9\cdot2^{-8}$	$9\cdot2^{-8}$	0,035415
π_1	2^{-5}	$7\cdot2^{-8}$	$9\cdot2^{-8}$	$1936\cdot2^{-16}$	0,029541
π_2	2^{-5}	$7\cdot2^{-8}$	$9\cdot2^{-8}$	$1936\cdot2^{-16}$	0,029573
π_3	2^{-5}	$7\cdot2^{-8}$	$9\cdot2^{-8}$	$1600\cdot2^{-16}$	0,025883

Таким образом, все узлы замены имеют тривиальную линейную структуру и приемлемые разностные и линейные свойства. В частности, максимальные значения элементов таблиц разностей и таблиц линейных аппроксимаций узлов замены не превышают 2^{-5} и $9\cdot 2^{-8}$ соответственно.

Вполненеразложимость таблиц разностей узлов замены шифра «Калина». Напомним (см., например, [9, с. 353]), что неотрицательная матрица P порядка n называется неразложимой, если не существует подстановочной матрицы Π такой, что

$$\Pi P \Pi^{-1} = \begin{pmatrix} P_1 0 \\ P_2 P_3 \end{pmatrix},$$

где P_1 — квадратная матрица порядка, меньшего n. Матрица P называется вполне неразложимой, если не существует подстановочных матриц Π_1 и Π_2 таких, что

$$\Pi_1 P \Pi_2 = \begin{pmatrix} P_1 0 \\ P_2 P_3 \end{pmatrix},$$

где P_1 — квадратная матрица порядка, меньшего n. Известно [9], что дважды стохастическая матрица P вполне неразложима тогда и только тогда, когда неразложима матрица $P\cdot P^{\mathrm{T}}$. Кроме того, положительная квадратная матрица является вполне неразложимой.

Для каждой подстановки $\pi \in \{\pi_0, \pi_1, \pi_2, \pi_3\}$ обозначим $D^{(\pi)} = (d_{\oplus}^{(\pi)}(\alpha, \beta))_{\alpha,\, \beta \in V_t \setminus \{0\}}$ таблицу разностей подстановки π (см. формулу (13)). Следующее утверждение доказывается непосредственной проверкой.

Утверждение 1. Все матрицы $\widetilde{D}^{(\pi_i)} = D^{(\pi_i)} \cdot (D^{(\pi_i)})^{\mathrm{T}}$, $i \in \overline{0, 3}$, являются положительными. В частности, таблица разностей каждого узла замены шифра «Калина» является вполне неразложимой матрицей.

Заметим, что положительность матрицы $\widetilde{D}^{(\pi_i)}$ равносильна существованию для любых $u_1, u_2, v_1, v_2 \in V_t$, где $u_1 \neq u_2, v_1 \neq v_2$, таких $k, k', k'' \in V_t$, что $\pi_i(u_1 \oplus k) \oplus k' = \pi_i(v_1 \oplus k'')$, $\pi_i(u_2 \oplus k) \oplus k' = \pi_i(v_2 \oplus k'')$, $i \in \overline{0, 3}$. Этот факт свидетельствует о хороших перемешивающих свойствах узлов замены (в смысле работы [4]) и используется ниже при исследовании группы подстановок, порожденной раундовыми преобразованиями шифра «Калина».

Свойства линейных преобразований, используемых в шифре «Калина». Для любого натурального m и произвольного вектора $z = (z^{(1)}, \ldots, z^{(m)}) \in \mathbf{GF}(2^t)^m$ обозначим $wt(z)$ вес вектора z:

$$wt(z) = \#\{i \in \overline{1, m}\colon z^{(i)} \neq 0\}.$$

Индекс ветвления (branch number) $m \times m$-матрицы M над полем $\mathbf{GF}(2^t)$ определяется по формуле [5]

$$B_M = \min\{wt(z) + wt(zM)\colon\ z \in \mathbf{GF}(2^t)^m \setminus \{0\}\}.$$

Для любого вектора $x = (x_1, \ldots, x_c)$, где $x_j = (x_{1,j}, \ldots, x_{q,j})$, $x_{i,j} \in V_t$, $i \in \overline{1, q}$, $j \in \overline{1, c}$, и произвольной матрицы L порядка p над полем $\mathbf{GF}(2^t)$ обозначим

$$Wt(x) = \#\{j \in \overline{1, c}\colon x_j \neq 0\},\ B'_L = \min\{Wt(x) + Wt(xL)\colon\ x \in \mathbf{GF}(2^t)^p \setminus \{0\}\}.$$

Числа $Wt(x)$ и B'_L назовем расширенным весом вектора x и расширенным индексом ветвления матрицы L соответственно.

Рассмотрим линейное преобразование $\hat{g}$ и матрицу M_p над полем $\mathbf{GF}(2^t)$, определенные по формулам (3) и (5) соответственно, и положим $\Lambda(x) = \hat{g}(xM_p)$,

$x \in V_n$. Из (3)–(5) вытекает, что $\Lambda(x) = xL_p$, $x \in V_n$, где

$$L_p = G_p \cdot \mathrm{diag}\,(\underbrace{D, \ldots, D}_{c \text{ раз}}) \cdot G_p. \tag{18}$$

Отметим (см., например, [5]), что поскольку D является МДР-матрицей порядка q над полем $\mathbf{GF}(2^t)$, то

$$B_D = B_{D^{\mathrm{T}}} = q + 1. \tag{19}$$

Утверждение 2. Пусть $q = c\mu$, $g(i, j) = (i, (j + c_i) \bmod c + 1)$, $i \in \overline{1, q}$, $j \in \overline{1, c}$, причем в наборе $(c_1, \ldots, c_q)$ каждый элемент $0, 1, \ldots, c-1$ повторяется ровно μ раз. Тогда расширенный индекс ветвления каждой из матриц L_p, L_p^{T} равен $c+1$.

Доказательство. Из условия утверждения и определения функций wt и Wt вытекает, что для любых $x \in V_n$, $j \in \overline{1, c}$ справедливы следующие неравенства:

$$Wt(x) \geq wt(\hat{g}(x)_j)\mu^{-1}, \; Wt(\hat{g}(x)) \geq wt(x_j)\mu^{-1}. \tag{20}$$

Пусть $x \in V_n \setminus \{0\}$; тогда существует $j \in \overline{1, c}$ такое, что $\hat{g}(x)_j \neq 0$. Отсюда, последовательно используя формулы (20), (4), (5), (19), получаем

$$Wt(x) + Wt(xL_p) = Wt(x) + Wt(\hat{g}(xM_p)) \geq (wt(\hat{g}(x)_j) + wt((xM_p)_j))\mu^{-1} =$$

$$= (wt(\hat{g}(x)_j) + wt(\hat{g}(x)_j D))\mu^{-1} \geq B_D \mu^{-1} = (q+1)\mu^{-1}.$$

Итак,

$$B'_{L_p} \geq \lceil cq^{-1}(q+1) \rceil = c + 1. \tag{21}$$

Далее, по условию утверждения существует $i \in \overline{1, q}$ такое, что $c_i = 0$. Рассмотрим вектор $x \in V_n$ с единственной ненулевой координатой $x_{i,1}$. Тогда $\hat{g}(x) = x$ и согласно (19) $wt((xM_p)_1) = wt(\hat{g}(x)_1 D) = wt(x_1 D) = q$, т.е. все координаты вектора $(xM_p)_1$ являются ненулевыми. Отсюда с учетом определения перестановки g получим $Wt(\hat{g}(xM_p)) = c$. Итак, $Wt(x) + Wt(xL_p) = Wt(x) + Wt(\hat{g}(xM_p)) = c + 1$ и, следовательно, на основании (21) имеем $B'_{L_p} = c + 1$.

Равенство $B'_{L_p^{\mathrm{T}}} = c + 1$ доказывается аналогично. Утверждение доказано.

Заметим, что каждая из трех перестановок g, используемых в «Калине» (см. разд. 1), удовлетворяет условию утверждения 2. Отсюда вытекает следующий результат.

Следствие 1. Пусть L_p — матрица вида (18), используемая в шифре «Калина» с длиной блока n бит. Тогда

$$B'_{L_p} = B'_{L_p^{\mathrm{T}}} = \begin{cases} 3, & \text{если } p = 16 \;\; (n = 128); \\ 5, & \text{если } p = 32 \;\; (n = 256); \\ 9, & \text{если } p = 64 \;\; (n = 512). \end{cases}$$

Отметим также важное комбинаторное свойство матриц (5), используемых в шифре «Калина».

Напомним, что неотрицательная квадратная матрица P называется примитивной, если существует натуральное число l такое, что $P^{\,l} > 0$ (т.е. все элементы последней матрицы являются положительными числами). Наименьшее натуральное число l с указанным свойством называется экспонентой матрицы P [10, с. 392]. Носитель произвольной матрицы $M = (m_{ij})$ над произвольным полем

определяется как неотрицательная матрица $N(M)$ с элементами

$$n_{ij} = \begin{cases} 1, & \text{если } m_{ij} \neq 0; \\ 0 & \text{в противном случае.} \end{cases}$$

Справедливость следующего утверждения проверяется непосредственно.

Утверждение 3. Для любого $p \in \{16, 32, 64\}$ носитель матрицы M_p является примитивной матрицей, экспонента которой равна двум.

Последние два утверждения используются ниже при обосновании стойкости шифра «Калина» относительно ряда алгебраических и статистических атак.

3. ГРУППА, ПОРОЖДЕННАЯ РАУНДОВЫМИ ПРЕОБРАЗОВАНИЯМИ ШИФРА «КАЛИНА»

Рассмотрим произвольный блочный шифр $\mathfrak{I}$, заданный соотношениями (1)–(9), и обозначим $G_{\mathfrak{I}} = \langle f_{i,k} : i \in \overline{2, r-1}, k \in V_n \rangle$ группу подстановок, порожденную раундовыми преобразованиями этого шифра в раундах с номерами $2, 3, \ldots, r-1$.

В [4] получены достаточные условия, при которых $G_{\mathfrak{I}}$ является знакопеременной группой подстановок на множестве V_n.

Теорема 1 [4]. Пусть выполняются следующие условия:

а) носитель матрицы M_p является примитивной матрицей;

б) для любых $i \in \overline{1, q}$, $j \in \overline{1, c}$ группа подстановок

$$G(s_{i,j}) = \langle s_{i,j}^{\alpha,\beta} : \alpha, \beta \in V_t \rangle,$$

где $s_{i,j}^{\alpha,\beta}(x) = s_{i,j}^{-1}(s_{i,j}(x \oplus \alpha) \oplus \beta)$, $x \in V_t$, является 2-транзитивной и среди элементов этих групп есть подстановка π такая, что $\#\{k \in V_t : \pi(k) = k\} \notin \{0, 2^0, 2^1, \ldots, 2^t\}$;

в) справедливо неравенство $2^{pt} < (2^t - 1)^{p-1}(2^t + 2^{t-1} - 2)$.

Тогда группа $G_{\mathfrak{I}}$ состоит из всех четных подстановок на множестве V_n.

Утверждение 4. Каждая версия шифра «Калина» удовлетворяет условиям а)–в) теоремы 1.

Доказательство. Справедливость условия а) вытекает из утверждения 3, а выполнение условия в) проверяется непосредственно. Далее, согласно теореме 3 в [4] 2-транзитивность группы $G(s_{i,j})$ равносильна неразложимости матрицы $\widetilde{D}^{(s_{i,j})} = D^{(s_{i,j})} \cdot (D^{(s_{i,j})})^{\mathrm{T}}$, где $D^{(s_{i,j})}$ — таблица разностей подстановки $s_{i,j}$, $i \in \overline{1, q}$, $j \in \overline{1, c}$.

Следовательно, справедливость первой части условия б) вытекает из утверждения 1.

Наконец, в таблице разностей узла замены π_0 шифра «Калина» имеются элементы $d_{\oplus}^{(\pi_0)}(\alpha, \beta)$, равные $2^{-8} \cdot 6$. Следовательно, для подстановки $\pi = \pi_0^{\alpha,\beta}$ выполняются соотношения

$$6 = 2^8 d_{\oplus}^{(\pi_0)}(\alpha, \beta) = \sum_{k \in V_8} \delta(\pi_0(k \oplus \alpha) \oplus \pi_0(k), \beta) =$$

$$= \#\{k \in V_t : \pi(k) = k\} \notin \{0, 2^0, 2^1, \ldots, 2^8\},$$

из которых вытекает справедливость второй части условия б) теоремы 1.

Утверждение доказано.

Таким образом, группа подстановок, порожденная раундовыми преобразованиями шифра «Калина» с длиной блока $n \in \{128, 256, 512\}$, является знакопеременной на множестве V_n. Указанный факт свидетельствует о стойкости шифра относительно алгебраических атак, основанных на гомоморфизмах, а также о его асимптотической (с ростом числа раундов r) стойкости относительно ряда статистических атак [11–14].

4. ОЦЕНКИ СТОЙКОСТИ ШИРФА «КАЛИНА» ОТНОСИТЕЛЬНО РАЗНОСТНОГО И ЛИНЕЙНОГО КРИПТОАНАЛИЗА

Для любого конечного семейства подстановок $\Phi = (\varphi_k : k \in K)$ на множестве V_n, произвольных бинарных операций $\circ$, $\bullet$ на V_n и для векторов $\alpha, \beta \in V_n$ обозначим

$$d_{\circ,\bullet}^{(\Phi)}(\alpha, \beta) = 2^{-n} |K|^{-1} \sum_{k \in K} \sum_{x \in V_n} \delta(\varphi_k(x \circ \alpha), \varphi_k(x) \bullet \beta),$$

$$l^{(\Phi)}(\alpha, \beta) = |K|^{-1} \sum_{k \in K} \left(2^{-n} \sum_{x \in V_n} (-1)^{\alpha x \oplus \beta \varphi_k(x)} \right)^2.$$

Для заданного выше шифра $\Im$ положим

$$\Im_i = (f_{i,k} : k \in V_n),\ \Im_{[i,j]} = (f_{i,k_i} \circ \ldots \circ f_{j,k_j} : (k_i, \ldots, k_j) \in V_n^{j-i+1}),\ 1 \le i \le j \le r.$$

Из формулы (7) вытекает, что $\Im$ является произведением шифров $\Im_1, \ldots, \Im_r$, причем согласно формуле (8) $\Im_{[2,r-1]}$ является марковским (относительно операции $\oplus$) SPN-шифром.

Следующие утверждения доказываются непосредственной проверкой.

Утверждение 5. Пусть символ $\circ$ обозначает произвольную бинарную операцию на множестве V_n. Тогда для любых $\alpha, \beta \in V_n$ справедливо равенство

$$d_{\circ,\oplus}^{(\Im_{[1,r-1]})}(\alpha, \beta) = \sum_{\gamma \in V_n} d_{\circ,\oplus}^{(\Im_1)}(\alpha, \gamma)\, d_{\oplus,\oplus}^{(\Im_{[2,r-1]})}(\gamma, \beta).$$

В частности,

$$\max_{\alpha, \beta \in V_n \setminus \{0\}} \{d_{\circ,\oplus}^{(\Im_{[1,r-1]})}(\alpha, \beta)\} \le \max_{\alpha, \beta \in V_n \setminus \{0\}} \{d_{\oplus,\oplus}^{(\Im_{[2,r-1]})}(\alpha, \beta)\}. \qquad (22)$$

Утверждение 6. Для любых $\alpha, \beta \in V_n$ справедливо равенство

$$l^{(\Im)}(\alpha, \beta) = \sum_{\substack{\gamma_1 \in V_n, \\ \gamma_2 \in V_n}} l^{(\Im_1)}(\alpha, \gamma_1)\, l^{(\Im_{[2,r-2]})}(\gamma_1, \gamma_2)\, l^{(\Im_{[r-2,r]})}(\gamma_2, \beta).$$

В частности,

$$\max_{\alpha, \beta \in V_n \setminus \{0\}} \{l^{(\Im)}(\alpha, \beta)\} \le \max_{\alpha, \beta \in V_n \setminus \{0\}} \{l^{(\Im_{[2,r-2]})}(\alpha, \beta)\}. \qquad (23)$$

Отметим, что параметры в левых частях неравенств (22) и (23) совпадают соответственно с максимальными значениями вероятностей $(r-1)$-раундовых дифференциалов и r-раундовых линейных аппроксимаций шифра $\Im$ (обычно под операцией $\circ$ подразумевают операцию $\oplus$). Указанные параметры являются стандартными показателями теоретической стойкости (provable security) блочных шифров относительно разностного и соответственно линейного криптоанализа. Таким образом, соотношения (22), (23) позволяют применять для оценки стойкости шифра $\Im$ относительно указанных методов криптоанализа известные

результаты, полученные для марковских SPN-шифров. В частности, справедлива следующая теорема.

Теорема 2. Пусть $\Im$ — r-раундовый блочный шифр, заданный соотношениями (1)–(9), где перестановка g удовлетворяет условию утверждения 2. Обозначим

$$d_{\oplus} = \max\{d_{\oplus}^{(s_{i,j})} : i \in \overline{1, q},\ j \in \overline{1, c}\},\ l_{\oplus} = \max\{l_{\oplus}^{(s_{i,j})} : i \in \overline{1, q},\ j \in \overline{1, c}\}$$

соответственно максимальные значения элементов таблиц разностей и таблиц линейных аппроксимаций всех узлов замены шифра $\Im$ (см. (10), (11)). Тогда при $r \geq 6$ для любой бинарной операции $\circ$ на множестве V_n справедливо неравенство

$$\max_{\alpha, \beta \in V_n \setminus \{0\}} \{d_{\circ, \oplus}^{(\Im_{[1, r-1]})}(\alpha, \beta)\} \leq d_{\oplus}^{cq}\ . \tag{24}$$

Кроме того, при $r \geq 7$ справедливо неравенство

$$\max_{\alpha, \beta \in V_n \setminus \{0\}} \{l^{(\Im)}(\alpha, \beta)\} \leq l_{\oplus}^{cq}\ . \tag{25}$$

Доказательство теоремы приведено в разд. 5.

Непосредственно из теоремы 2 и данных табл. 2 получаем следующий результат.

Следствие 2. Пусть $\Im$ является шифром «Калина» с длиной блока n бит и r раундами шифрования. Тогда при $r \geq 6$ для любой бинарной операции $\circ$ на множестве V_n выполняется неравенство

$$\max_{\alpha, \beta \in V_n \setminus \{0\}} \{d_{\circ, \oplus}^{(\Im_{[1, r-1]})}(\alpha, \beta)\} \leq \begin{cases} 2^{-80}, & \text{если } n = 128; \\ 2^{-160}, & \text{если } n = 256; \\ 2^{-320}, & \text{если } n = 512. \end{cases} \tag{26}$$

Кроме того, при $r \geq 7$ выполняется неравенство

$$\max_{\alpha, \beta \in V_n \setminus \{0\}} \{l^{(\Im)}(\alpha, \beta)\} \leq \begin{cases} 9^{16} \cdot 2^{-128} \approx 1{,}65 \cdot 2^{-78}, & \text{если } n = 128; \\ 9^{32} \cdot 2^{-256} \approx 1{,}35 \cdot 2^{-155}, & \text{если } n = 256; \\ 9^{64} \cdot 2^{-512} \approx 1{,}83 \cdot 2^{-310}, & \text{если } n = 512. \end{cases} \tag{27}$$

Итак, на основании неравенств (26) и (27) для проведения классической разностной (линейной) атаки на любую версию «Калины» необходимо зашифровать не менее чем 2^{80} (2^{78}) открытых сообщений. Таким образом, успешное применение к этому шифру разностного или линейного криптоанализа практически нереализуемо.

5. ДОКАЗАТЕЛЬСТВО ТЕОРЕМЫ 2

Предварительные замечания. Из определения шифра $\Im$ и неравенств (22), (23) вытекает, что

$$\max_{\alpha, \beta \in V_n \setminus \{0\}} \{d_{\oplus, \oplus}^{(\Im_{[1, r-1]})}(\alpha, \beta)\} \leq \max_{\alpha, \beta \in V_n \setminus \{0\}} \{d_{\oplus, \oplus}^{(\Im_{[2, 5]})}(\alpha, \beta)\},\ \text{если } r \geq 6; \tag{28}$$

$$\max_{\alpha, \beta \in V_n \setminus \{0\}} \{l^{(\Im)}(\alpha, \beta)\} \leq \max_{\alpha, \beta \in V_n \setminus \{0\}} \{l^{(\Im_{[2,5]})}(\alpha, \beta)\},\ \text{если } r \geq 7. \tag{29}$$

Покажем, что для любых векторов $\alpha, \beta \in V_n \setminus \{0\}$ справедливы неравенства

$$d_{\oplus, \oplus}^{(\Im_{[2, 5]})}(\alpha, \beta) \leq d_{\oplus}^{(B_D - 1)(B_{L_p'} - 1)}, \tag{30}$$

$$l^{(\Im_{[2, 5]})}(\alpha, \beta) \leq l_{\oplus}^{(B_{D^{\mathrm{T}}} - 1)(B_{L_p^{\mathrm{T}}}' - 1)}, \tag{31}$$

где B_D ($B_{D^{\mathrm{T}}}$) — индекс ветвления матрицы D (D^{T}), B'_{L_p} ($B'_{L_p^{\mathrm{T}}}$) — расширенный индекс ветвления матрицы L_p (L_p^{T}). Тогда неравенства (24) и (25) вытекают непосредственно из формул (19), (28)–(31) и утверждения 2.

Убедимся в справедливости неравенств (30) (отметим, что в завершающей части доказательства не используется никаких дополнительных предположений относительно матрицы D и перестановки g). Неравенство (31) доказывается аналогично.

Вспомогательные утверждения. Сформулируем следующий общий результат.

Лемма 1. Пусть $P_i = (P_i(u, v))_{u, v \in V_l}$, $P'_i = (P'_i(u, v))_{u, v \in V_l}$ — дважды стохастические матрицы такие, что $P_i(0, 0) = P'_i(0, 0) = 1$, $i \in \overline{1, m}$; $L: V_l^m \to V_l^m$ — биективное отображение, удовлетворяющее условию

$$L(x \oplus y) = L(x) \oplus L(y), \ x, y \in V_l^m.$$

Для любого $x = (x^{(1)}, \ldots, x^{(m)}) \in V_l^m$ обозначим

$$wt_l(x) = \#\{i \in \overline{1, m}: x^{(i)} \neq 0\}, \qquad B_l(L) = \min\{wt_l(x) + wt_l(L(x)): x \in V_l^m\}.$$

Далее, для любых $\alpha = (\alpha^{(1)}, \ldots, \alpha^{(m)})$, $\beta = (\beta^{(1)}, \ldots, \beta^{(m)}) \in V_l^m$ положим

$$P(\alpha, \beta) = \prod_{i=1}^{m} P_i(\alpha^{(i)}, \beta^{(i)}), \ P'(\alpha, \beta) = \prod_{i=1}^{m} P'_i(\alpha^{(i)}, \beta^{(i)}), \tag{32}$$

$$(P \overset{L}{\cdot} P')(\alpha, \beta) = \sum_{x \in V_l^m} P(\alpha, x) P'(L(x), \beta). \tag{33}$$

Тогда справедливо неравенство

$$\max_{\alpha, \beta \in V_l^m \setminus \{0\}} \{(P \overset{L}{\cdot} P')(\alpha, \beta)\} \le \left(\max \left\{ \max_{\substack{i \in \overline{1, m}, \\ u, v \in V_l \setminus \{0\}}} \{P_i(u, v)\}, \max_{\substack{i \in \overline{1, m}, \\ u, v \in V_l \setminus \{0\}}} \{P'_i(u, v)\} \right\} \right)^{B_l(L)-1}.$$

Доказательство леммы почти дословно повторяет доказательство теоремы 1 и следствия из нее в работе [15]. Заметим, что в [15] рассматривается частный случай, в котором матрица $P_i = P'_i$ является расширенной таблицей разностей некоторой подстановки $S_i: V_l \to V_l$, $i \in \overline{1, m}$. В этом случае параметр (33) совпадает с вероятностью дифференциала 2-раундового SPN-шифра, раундовая функция которого является композицией набора узлов замены $(S_1, \ldots, S_m)$ и линейного преобразования L. Заметим также, что в случае, когда последнее задается с помощью $m \times m$-матрицы M над полем из 2^l элементов, значение $B_l(L)$ совпадает с индексом ветвления матрицы M (см. разд. 2).

Изложим еще одну (эквивалентную) формулировку леммы 1.

Назовем произвольную дважды стохастическую матрицу Q с элементами $Q(u, v)$, $u, v \in V_l$, специальной, если $Q(0, 0) = 1$. Обозначим P и P' соответственно матрицы с элементами $P(\alpha, \beta)$ и $P'(\alpha, \beta)$ вида (32) и зададим матрицу P'_L, полагая $P'_L(\alpha, \beta) = P'(L(\alpha), \beta)$, $\alpha, \beta \in V_n$. Тогда по определению матрицы P и P' являются тензорными произведениями матриц $P_1, \ldots, P_m$ и $P'_1, \ldots, P'_m$ соответ-

ственно: $P = P_1 \otimes \cdots \otimes P_m$, $P' = P_1' \otimes \cdots \otimes P_m'$, а формула (33) содержит выражение (α, β)-го элемента (обычного) произведения PP_L' , которое является специальной матрицей (поскольку таковыми являются P_i и P_i' , $i \in \overline{1, m}$). Наконец, зададим ∞-норму любой специальной матрицы $Q = (Q(u, v))_{u, v \in V_l}$, полагая $\|Q\|_\infty = \max\limits_{u, v \in V_l \setminus \{0\}} \{Q(u, v)\}$. Тогда утверждение леммы 1 можно записать в виде неравенства

$$\| P_1 \otimes \cdots \otimes P_m \overset{L}{\cdot} P_1' \otimes \cdots \otimes P_m' \|_\infty \le \left(\max \left\{ \max_{i \in \overline{1, m}} \| P_i \|_\infty , \max_{i \in \overline{1, m}} \| P_i' \|_\infty \right\} \right)^{B_l(L)-1}.$$

Для формулировки следующего результата введем несколько дополнительных обозначений.

Для любой подстановки $h: V_l \to V_l$ обозначим $P^{(h)} = (d^{(h)}(u, v))_{u, v \in V_l}$ ее расширенную таблицу разностей,

$$d^{(h)}(u, v) = 2^{-l} \sum_{x \in V_l} \delta(h(x \oplus u) \oplus h(x), v) , \ u, v \in V_l .$$

Для каждого $i \in \overline{1,4}$ обозначим $D_i^{(\overline{\Im})} = (d_i(\alpha, \beta))_{\alpha, \beta \in V_n}$ матрицу вероятностей i-раундовых дифференциалов шифра $\overline{\Im} = \Im[2, 5]$. Заметим, что поскольку $\overline{\Im}$ является 4-раундовым марковским SPN-шифром с раундовой функцией φ вида (6), то матрица $D_i^{(\overline{\Im})}$ является i-й степенью матрицы $P^{(\varphi)}$, $i \in \overline{1,4}$. Отсюда вытекают следующие равенства:

$$d_4(\alpha, \beta) = \sum_{\gamma \in V_n} d_2(\alpha, \gamma) d_2(\gamma, \beta) , \ \alpha, \beta \in V_n, \tag{34}$$

$$d_2(\alpha, \gamma M_p) = \sum_{x \in V_n} d^{(s)}(\alpha, x) d^{(s)}(x M_p, \gamma) , \ \alpha, \gamma \in V_n, \tag{35}$$

где подстановка s и матрица M_p определяются по формулам (2) и (5) соответственно.

Наконец, используя введенные выше обозначения (см. (1) и (3)), положим $s_j^{(g)} = (s_{g(1, j)}, \ldots, s_{g(q, j)})$, $x_j^{(g)} = \hat{g}(x)_j$, где $x \in V_n$, $j \in \overline{1, c}$.

Лемма 2. При выполнении соотношений (1)–(6) для любых $\alpha, \beta, \gamma \in V_n$ справедливы равенства

$$d_2(\alpha, \gamma M_p) = P(\hat{g}(\alpha), \gamma) , \tag{36}$$

$$d_4(\alpha, \beta) = (P \overset{\Lambda}{\cdot} P)(\hat{g}(\alpha), \beta (M_p)^{-1}) , \tag{37}$$

где P — специальная матрица с элементами

$$P(x, y) = \prod_{j=1}^{c} (P^{(s_j^{(g)})} \overset{\mathcal{D}}{\cdot} P^{(s_j)})(x_j, y_j), \quad x, y \in V_n, \tag{38}$$

$\mathcal{D}$ и Λ — отображения, определяемые по формулам

$$\mathcal{D}(x) = xD , \ \Lambda(x) = \hat{g}(x M_p) , \ x \in V_n .$$

Доказательство. Положим $I = \overline{1, q} \times \overline{1, c}$. Согласно равенствам (1), (2), (35)

$$d_2(\alpha, \gamma M_p) = \sum_{x \in V_n} \left(\prod_{(i, j) \in I} d^{(s_{i, j})}(\alpha_{i, j}, x_{i, j}) \right) \left(\prod_{j=1}^{c} d^{(s_j)}((x M_p)_j, \gamma_j) \right).$$

Используя введенные выше обозначения и принимая во внимание, что g является перестановкой на множестве I, получаем следующие равенства:

$$\prod_{(i,j)\in I} d^{(s_{i,j})}(\alpha_{i,j}, x_{i,j}) = \prod_{(i,j)\in I} d^{(s_{g(i,j)})}(\alpha_{g(i,j)}, x_{g(i,j)}) = \prod_{j=1}^{c} d^{(s_j^{(g)})}(\alpha_j^{(g)}, x_j^{(g)}).$$

Далее, используя равенство $(xM_p)_j = x_j^{(g)} D$, $x \in V_n$, которое вытекает из формул (4) и (5), получаем

$$\prod_{j=1}^{c} d^{(s_j)}((xM_p)_j, \gamma_j) = \prod_{j=1}^{c} d^{(s_j)}(x_j^{(g)} D, \gamma_j).$$

Итак,

$$d_2(\alpha, \gamma M_p) = \sum_{x\in V_n} \prod_{j=1}^{c} d^{(s_j^{(g)})}(\alpha_j^{(g)}, x_j^{(g)})\, d^{(s_j)}(x_j^{(g)} D, \gamma_j) =$$

$$= \sum_{x\in V_n} \prod_{j=1}^{c} d^{(s_j^{(g)})}(\alpha_j^{(g)}, x_j)\, d^{(s_j)}(x_j D, \gamma_j) =$$

$$= \prod_{j=1}^{c} \left(\sum_{x_j \in V_t^q} d^{(s_j^{(g)})}(\alpha_j^{(g)}, x_j)\, d^{(s_j)}(x_j D, \gamma_j) \right) = \prod_{j=1}^{m} (P^{(s_j^{(g)})} \overset{\mathcal{D}}{\cdot} P^{(s_j)})(\alpha_j^{(g)}, \gamma_j),$$

где последнее равенство вытекает непосредственно из определения параметра в его правой части (см. (33)). Отсюда на основании формулы (38) вытекает равенство (36).

Наконец, равенство (37) является следствием формул (34), (36) и определения отображения Λ:

$$d_4(\alpha, \beta) = \sum_{\gamma\in V_n} d_2(\alpha, \gamma M_p) d_2(\gamma M_p, \beta) = \sum_{\gamma\in V_n} P(\hat{g}(\alpha), \gamma) P(\hat{g}(\gamma M_p), \beta(M_p)^{-1}) =$$

$$= \sum_{\gamma\in V_n} P(\hat{g}(\alpha), \gamma) P(\Lambda(\gamma), \beta(M_p)^{-1}) = (P \overset{\Lambda}{\cdot} P)(\hat{g}(\alpha), \beta(M_p))^{-1}.$$

Лемма доказана.

Завершение доказательства неравенства (30). Зафиксируем векторы $\alpha, \beta \in V_n \setminus \{0\}$. Используя введенные выше обозначения, формулы (37), (38) и применяя лемму 1 к специальным матрицам $P_j = P'_j = P^{(s_j^{(g)})} \overset{\mathcal{D}}{\cdot} P^{(s_j)}$ порядка q, $j \in \overline{1, c}$, получаем

$$d_{\oplus,\oplus}^{(\Im_{[2,5]})}(\alpha, \beta) = d_4(\alpha, \beta) = (P \overset{\Lambda}{\cdot} P)(\hat{g}(\alpha), \beta(M_p))^{-1} \le$$

$$\le \| P \overset{\Lambda}{\cdot} P \|_\infty \le \left(\max_{j\in\overline{1,m}} \| P_j \|_\infty \right)^{B_q(\Lambda)-1}. \qquad (39)$$

Далее, используя равенства

$$P^{(s_j^{(g)})} = P^{(s_{g(1,j)})} \otimes \cdots \otimes P^{(s_{g(q,j)})}, \quad P^{(s_j)} = P^{(s_{1,j})} \otimes \cdots \otimes P^{(s_{q,j})},$$

которые вытекают непосредственно из определения подстановок $s_j^{(g)}$ и s_j, $j \in \overline{1, c}$, на основании леммы 1 и определения параметра $d_\oplus$ получаем соотношения

$$\| P_j \|_\infty = \| P^{(s_j^{(g)})} \overset{\mathcal{D}}{\cdot} P^{(s_j)} \|_\infty \le$$

$$\le \left(\max \left\{ \max_{i\in\overline{1,m}} \| P^{(s_j^{(g)})} \|_\infty, \max_{i\in\overline{1,m}} \| P^{(s_j)} \|_\infty \right\} \right)^{B_t(\mathcal{D})-1} \le d_\oplus^{B_t(\mathcal{D})-1}, \quad j \in \overline{1, c}. \qquad (40)$$

Неравенство (30) вытекает из формул (39), (40) и равенств $B_t(\mathcal{D}) = B_D$, $B_q(\Lambda) = B'_{L_p}$ (см. разд. 2).

Таким образом, теорема 2 полностью доказана.

ЗАКЛЮЧЕНИЕ

Шифр «Калина» относится к классу Rijndael-подобных блочных шифров, однако заметно отличается от шифра Rijndael. В частности, в шифре «Калина» применяются:

а) оригинальная процедура формирования раундовых ключей [1, п. 7];

б) процедура «отбеливания» с помощью алгебраической операции $\overset{\circ}{+}$ (см. (8), (9));

в) узлы замены $\pi_0, \pi_1\ \pi_2, \pi_3$, сформированные по определенным критериям [2].

Используемые в «Калине» узлы замены и линейные преобразования имеют приемлемые криптографические свойства (см. разд. 2). Не выявлено слабостей указанных компонент, которые могут быть использованы при построении известных атак на этот шифр.

Группа, порожденная раундовыми преобразованиями шифра «Калина» с длиной блока $n \in \{128, 256, 512\}$, является знакопеременной на множестве V_n. Это свидетельствует о стойкости шифра относительно алгебраических атак, основанных на гомоморфизмах, а также о его асимптотической (с ростом числа раундов r) стойкости относительно ряда статистических атак [11–14].

Полученные оценки максимальных значений вероятностей дифференциалов и линейных аппроксимаций шифра «Калина» (следствие 2) свидетельствуют о том, что успешное применение к этому шифру классического разностного или линейного криптоанализа практически невозможно.

СПИСОК ЛИТЕРАТУРЫ

1. Oliynykov R.V., Gorbenko I.D., Kazymyrov O.V. et. al. A new encryption standard of Ukraine: The Kalyna block cipher // Cryptology ePrint Archive. http://eprint.iacr.org/ 2015/650.
2. Олійников Р.В., Горбенко І.Д., Казимиров О.В. та ін. Принципи побудови і основні властивості нового національного стандарту блокового шифрування України // Захист інформації. — 2015. — **17**, № 2. — С. 142–157.
3. AlTawy R., Abdelkhalek A., Youssef A.M. A meet-in-the-middle attack on reduced-round Kalyna-b/2b // Cryptology ePrint Archive. http://eprint.iacr.org/2015/762.
4. Маслов А.С. Об условиях порождения SA-подстановками знакопеременной группы // Труды Ин-та математики. — 2007. — **15**, № 2. — С. 58–68.
5. Daemen J. Cipher and hash function design strategies based on linear and differential cryptanalysis. — Ph. D. Thesis. — Katholieke Univ. Leuven, 1995. — 224 p.
6. Мак-Вильямс Ф.Дж., Слоэн Н.Дж.А. Теория кодов, исправляющих ошибки: Пер. с англ. — М.: Связь, 1979. — 743 с.
7. Алексейчук А.Н. Критерий примитивности группы подстановок, порожденной раундовыми преобразованиями Rijndael-подобного блочного шифра // Реєстрація, зберігання і обробка даних. — 2004. — **6**, № 2. — С. 11–18.
8. Алексейчук А.Н., Скрынник Е.В. Классы отображений с тривиальной линейной структурой над конечным полем // Реєстрація, зберігання і обробка даних. — 2008. — **10**, № 3. — С. 80–88.
9. Сачков В.Н. Введение в комбинаторные методы дискретной математики. — М.: МНЦНМО, 2004. — 424 с.
10. Сачков В.Н., Тараканов В.Е. Комбинаторика неотрицательных матриц. — М.: ТВП, 2000. — 447 с.
11. Paterson K.G. Imprimitive permutation groups and trapdoors in iterated block ciphers // Fast Software Encryption. — FSE'99, Proceedings. — Springer Verlag, 1999. — P. 201–214.

12. Hornauer G., Stephan W., Wernsdorf R. Markov ciphers and alternating groups // Advances in Cryptology — EUROCRYPT'93, Proceedings. — Springer Verlag, 1994. — P. 453–460.

13. Wagner D. Towards a unifying view of block cipher cryptanalysis // Fast Software Encryption. — FSE'04, Proceedings. — Springer Verlag, 2004. — P. 116–135.

14. Vaudenay S. Decorrelation: A theory for block cipher security // J. of Cryptology. — 2003. — N 4. — P. 249–286.

15. Park S., Sung J., Lee S., Lim J. Improving the upper bound on the maximum differential and the maximum linear hull probability for the SPN structures and AES // Fast Software Encryption — FSE'03, Proceedings. — Springer Verlag, 2003. — P. 247–260.

Надійшла до редакції 05.10.2015

А.М. Олексійчук, Л.В. Ковальчук, А.С. Шевцов, С.В. Яковлєв

ПРО КРИПТОГРАФІЧНІ ВЛАСТИВОСТІ НОВОГО НАЦІОНАЛЬНОГО СТАНДАРТУ ШИФРУВАННЯ УКРАЇНИ

Анотація. Досліджено низку криптографічних властивостей блокового шифру «Калина», прийнятого як новий національний стандарт шифрування України. Проаналізовано найважливіші властивості компонент цього шифру. Показано, що його раундові перетворення породжують знакозмінну групу підстановок, що свідчить про стійкість до алгебраїчних атак, побудованих на гомоморфізмах, а сам шифр є обгрунтовано стійким відносно різницевого та лінійного криптоаналізу.

Ключові слова: симетрична криптографія, блоковий шифр, скінченна група підстановок, різницевий криптоаналіз, лінійний криптоаналіз, національний стандарт шифрування України, шифр «Калина».

A.N. Alekseychuk, L.V. Kovalchuk, A.S. Shevtsov, S.V. Yakovliev

CRYPTOGRAPHIC PROPERTIES OF THE NEW NATIONAL ENCRYPTION STANDARD OF UKRAINE

Abstract. Block cipher "Kalyna" has been recently accepted as a new national encryption standard of Ukraine. In the paper we analyze the most important properties of components of this cipher. We show that round transformations of "Kalyna" generate a sign-alternating group of substitutions. As a result, "Kalyna" is secure against algebraic attacks based on homomorphisms. Also we demonstrate that this cipher is reasonably secure against differential and linear cryptanalysis.

Keywords: symmetric cryptography, block cipher, finite permutation group, differential cryptanalysis, linear cryptanalysis, national encryption standard of Ukraine, cipher "Kalyna."

Алексейчук Антон Николаевич,
доктор техн. наук, доцент, профессор Института специальной связи и защиты информации Национального технического университета Украины «КПИ», Киев, e-mail: alex-dtn@ukr.net.

Ковальчук Людмила Васильевна,
доктор техн. наук, доцент Физико-технического института Национального технического университета Украины «КПИ», Киев, e-mail: lusi.kovalchuk@gmail.com.

Шевцов Артур Сергеевич,
кандидат техн. наук, доцент Института специальной связи и защиты информации Национального технического университета Украины «КПИ», Киев, e-mail: as.shevtsov@gmail.com.

Яковлев Сергей Владимирович, кандидат техн. наук, старший преподаватель Физико-технического института Национального технического университета Украины «КПИ», Киев, e-mail: yasv@rl.kiev.ua.