УДК 519.7

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

МЕТОД ОЦЕНИВАНИЯ СТОЙКОСТИ SNOW 2.0-ПОДОБНЫХ ШИФРОВ ОТНОСИТЕЛЬНО КОРРЕЛЯЦИОННЫХ АТАК НАД КОНЕЧНЫМИ РАСШИРЕНИЯМИ ПОЛЯ ИЗ ДВУХ ЭЛЕМЕНТОВ

Аннотация. Предложен метод оценивания стойкости SNOW 2.0-подобных шифров относительно корреляционных атак, которые строятся по аналогии с известными атаками на шифр SNOW 2.0. В отличие от ранее известных предложенный метод ориентирован на обоснование стойкости и позволяет получать нижние оценки эффективности атак из рассматриваемого класса непосредственно по параметрам компонент поточных шифров аналогично тому, как обосновывают стойкость блочных шифров относительно линейного криптоанализа. Применение метода к шифрам SNOW 2.0 и «Струмок» показывает, что любая из рассмотренных корреляционных атак на них над полем порядка 256 имеет среднюю временную сложность не менее $2^{146,20}$ и $2^{249,40}$ соответственно и требует не менее $2^{142,77}$ и $2^{249,38}$ соответственно знаков гаммы.

Ключевые слова: корреляционный криптоанализ, конечный автомат, дискретное преобразование Фурье, обоснование стойкости, шифр SNOW 2.0, шифр «Струмок».

ВВЕДЕНИЕ

Поточный шифр SNOW 2.0 [1] предложен в 2002 г. в качестве альтернативы более ранней (и более слабой) версии — SNOW. В настоящее время этот шифр стандартизирован [2] и является одним из наиболее быстрых программно-ориентированных поточных шифров.

Наиболее мощными из известных атак на шифр SNOW 2.0 являются корреляционные атаки, суть которых заключается в составлении и решении систем линейных уравнений с искаженными правыми частями, в частности систем уравнений (СУ) над полями порядка 2^r [3–7]. Несмотря на определенный прогресс в этом направлении, остаются нерешенными задачи, связанные с разработкой методов оценивания и обоснования стойкости SNOW 2.0-подобных шифров относительно корреляционных атак. В настоящее время отсутствуют методы, позволяющие обосновывать стойкость указанных шифров относительно известных корреляционных атак непосредственно по их компонентам. Кроме того, при попытке распространения известных методов оценивания стойкости SNOW 2.0 относительно корреляционных атак на некоторые другие поточные шифры (например, шифр «Струмок» [8], который является национальным стандартом поточного шифрования Украины) возникают трудности, связанные с размером решаемых задач. В отличие от SNOW 2.0, построенного над полем порядка 2^{32}, шифр «Струмок» задается над полем порядка 2^{64}, что приводит к невозможности практического применения известных алгоритмов [4, 5, 7], сложность которых возрастает с $2^{32} \div 2^{37}$ до 2^{64} двоичных операций.

В настоящей статье предложен метод, позволяющий на практике оценивать и обосновывать стойкость SNOW 2.0-подобных шифров относительно широкого класса корреляционных атак. Показано, что задача получения нижних оценок эффективности корреляционных атак (из рассматриваемого класса) сводится к построению верхних оценок максимума модулей коэффициентов Фурье распределения искажений в правых частях некоторой системы линейных уравнений, которая не зависит от конкретной атаки. Исследована также взаимосвязь между эффективностью атак над полями порядка $2^{r'}$, где $r' > 1$, и обычных, двоичных атак, которые строятся над полем F_2 . Показано, что переход от булевых корре-

ляционных атак к атакам над полями порядка $2^{r'}$ может повысить эффективность первых не более чем в $2^{r'}$ раз. Наконец, базируясь на результатах работы [9], получено соотношение, позволяющее оценивать стойкость SNOW 2.0-подобных шифров относительно корреляционных атак над полем порядка $2^{r'}$ непосредственно по параметрам их компонент. Рассмотрены применения предложенного метода к шифрам SNOW 2.0 и «Струмок».

Отметим, что отдельные результаты, изложенные в статье (в частности, теоремы 1 и 2), могут применяться не только к SNOW 2.0-подобным шифрам, но и использоваться для решения других задач корреляционного криптоанализа симметричных шифрсистем.

SNOW 2.0-ПОДОБНЫЕ ШИФРЫ

Для любого натурального числа r обозначим V_r множество двоичных векторов длины r. Зададим на этом множестве структуру поля F_{2^r} (порядка 2^r), согласованную с операцией $\oplus$ покоординатного булевого сложения двоичных векторов. Отождествим элементы множества V_r с r-разрядными целыми числами, предполагая, что вектору $x = (x_1, x_2, \dots, x_r) \in V_r$ соответствует число $x_1 + 2x_2 + \dots + 2^{r-1}x_r$, и обозначим символом $\overset{r}{+}$ операцию сложения этих чисел по модулю 2^r. Для любых $a, b \in Z$ обозначим $\overline{a, b} = \{x \in Z: a \le x \le b\}$.

Согласно определению [10] исходными данными для построения генератора гаммы (keystream generator) SNOW 2.0-подобного поточного шифра являются следующие объекты (рис. 1): примитивный многочлен $g(z) = z^n \oplus c_{n-1}z^{n-1} \oplus \dots \dots \oplus c_0$ над полем F_{2^r}; подстановка $\sigma: V_r \to V_r$; число $\mu \in \overline{1, n-2}$. Генератор гаммы представляет собой конечный автономный автомат с множеством внутренних состояний $V_r^n \times V_r^2$, функцией переходов $h((x_{n-1}, x_{n-2}, \dots, x_0), u, v) = ((x_n, x_{n-1}, \dots, x_1), x_\mu \overset{r}{+} v, \sigma(u))$ и функцией выходов $f((x_{n-1}, x_{n-2}, \dots \dots, x_0), u, v) = x_0 \oplus (x_{n-1} \overset{r}{+} u) \oplus v$, где $x_0, \dots, x_{n-1}, u, v \in V_r$, $x_n = c_{n-1}x_{n-1} \oplus \dots \dots \oplus c_0 x_0$. Знак гаммы в i-м такте определяется по начальному состоянию $((x_{n-1}, x_{n-2}, \dots, x_0), u_0, v_0)$ генератора с помощью рекуррентных соотношений

$$\gamma_i = x_i \oplus (x_{i+n-1} \overset{r}{+} u_i) \oplus v_i, \tag{1}$$

$$u_{i+1} = x_{i+\mu} \overset{r}{+} v_i, \; v_{i+1} = \sigma(u_i), \tag{2}$$

справедливых для всех $i = 0, 1, \dots$

В дальнейшем рассматриваются SNOW 2.0-подобные шифры, удовлетворяющие следующим условиям: существуют целые числа $p, t \ge 2$ такие, что $r = pt$, базис B поля F_{2^r} над подполем F_{2^t}, подстановки $s_i: F_{2^t} \to F_{2^t}$, $i \in \overline{0, p-1}$, и обратимая $p \times p$-матрица D над полем F_{2^t} такие, что при отождествлении произвольного элемента a поля F_{2^r} с набором $(a_0, \dots, a_{p-1})$ его координат в базисе B выполняется равенство

$$\sigma(z) = (s_0(z_0), \dots, s_{p-1}(z_{p-1}))D, \; z = (z_0, \dots, z_{p-1}) \in F_{2^t}^p. \tag{3}$$

Подстановки $s_i: F_{2^t} \to F_{2^t}$, $i \in \overline{0, p-1}$, называются s-блоками (s-boxes) рассматриваемого шифра.

Замечание 1. В SNOW 2.0 [1] используются следующие параметры: $t = 8$, $p = 4$ ($r = 32$). При этом $n = 16$, $\mu = 5$, а подстановки s_i, $i \in \overline{0, p-1}$, и матрица D задаются так же, как в раундовом преобразовании блочного шифра Rijndael.

Замечание 2. Поточный шифр «Струмок» [8] является SNOW 2.0-подобным шифром с параметрами $t=8,\ p=8$ ($r=64$). При этом $n=16,\ \mu=13$, а подстановки s_i, $i\in\overline{0,\ p-1}$, и матрица D задаются так же, как в блочном шифре «Калина» [11, 12].

ПОСТРОЕНИЕ СИСТЕМ ЛИНЕЙНЫХ УРАВНЕНИЙ С ИСКАЖЕННЫМИ ПРАВЫМИ ЧАСТЯМИ ДЛЯ КОРРЕЛЯЦИОННЫХ АТАК НА SNOW 2.0-ПОДОБНЫЕ ШИФРЫ

Практически все известные корреляционные атаки на шифр SNOW 2.0 [3–7] основаны на том, что сумма знаков шифрующей гаммы в любых двух соседних тактах является результатом искажения знака линейной рекурренты над полем F_{2^r}, по которой можно непосредственно восстановить начальное состояние регистра сдвига с линейной обратной связью (см. рис. 1). Для произвольного SNOW 2.0-подобного шифра на основании соотношений (1), (2) справедливы равенства

$$\gamma_i \oplus \gamma_{i+1} = x_i \oplus x_{i+1} \oplus x_{i+\mu} \oplus x_{i+n-1} \oplus x_{i+n} \oplus \xi_i\ ,\ i=0,1,\dots\ , \tag{4}$$

где

$$\xi_i = ((x_{i+n-1} \overset{r}{+} u_i) \oplus x_{i+n-1} \oplus \sigma(u_i)) \oplus$$
$$\oplus\ ((x_{i+n} \overset{r}{+} x_{i+\mu} \overset{r}{+} v_i) \oplus (x_{i+n} \oplus x_{i+\mu} \oplus v_i))\ ,\ i=0,1,\dots \tag{5}$$

Предполагая, что переменные $x_{i+\mu}, x_{i+n-1}, x_{i+n}, u_i, v_i$ в формуле (5) являются независимыми случайными величинами с равномерным распределением на множестве V_r, и выражая знаки $x_i, x_{i+1}, x_{i+\mu}, x_{i+n-1}, x_{i+n}$ линейной рекурренты через начальное состояние регистра сдвига (см. рис. 1), получаем систему (4) линейных уравнений с искаженными правыми частями над полем F_{2^r}, где искажения имеют вид (5).

Опишем метод построения следствий системы (4), которые используются далее для построения корреляционных атак на SNOW 2.0-подобные шифры.

Запишем первые N уравнений системы (4) в виде

$$b_i = A_i a \oplus \xi_i,\ i\in\overline{0,\ N-1}, \tag{6}$$

где $b_i = \gamma_i \oplus \gamma_{i+1}$, $A_i a = x_i \oplus x_{i+1} \oplus x_{i+\mu} \oplus x_{i+n-1} \oplus x_{i+n}$, A_i — известная вектор-строка длины n над полем F_{2^r}, $a=(x_0,\dots,x_{n-1})^{\mathrm{T}}$ — неизвестный вектор-столбец, равный начальному состоянию регистра сдвига на рис. 1.

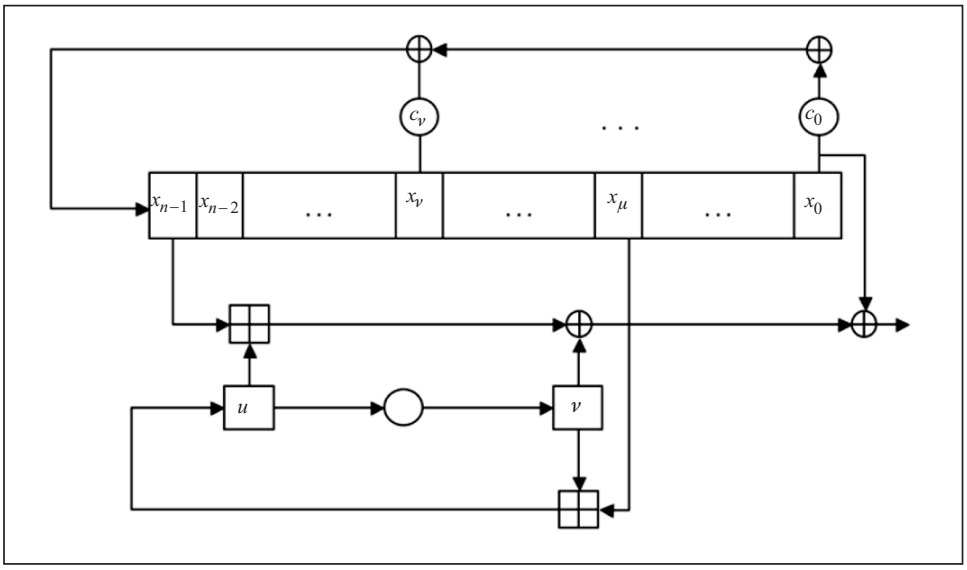

Рис. 1. Схема генератора гаммы SNOW 2.0-подобного поточного шифра

Зафиксируем произвольный делитель r' числа r и обозначим $\mathrm{Tr}_{2^{r'}}^{2^r}(z) = z \oplus z^{2^{r'}} \oplus \cdots \oplus z^{2^{r'(r''-1)}}$ след элемента $z \in F_{2^r}$ в поле $F_{2^{r'}}$, где $r'r'' = r$.

Отметим (см., например, [13, определение 2.30]), что базисы $B = \{b_1, \ldots, b_{r''}\}$ и $\hat{B} = \{\hat{b}_1, \ldots, \hat{b}_{r''}\}$ поля F_{2^r} над подполем $F_{2^{r'}}$ называются дуальными, если $\mathrm{Tr}_{2^{r'}}^{2^r}(b_i \hat{b}_j) = 1$ при $i = j$, и $\mathrm{Tr}_{2^{r'}}^{2^r}(b_i \hat{b}_j) = 0$ — в противном случае. Из данного определения вытекает, что след произведения элементов поля F_{2^r} совпадает со скалярным произведением векторов их координат в (произвольных) дуальных базисах.

Для построения системы-следствия СУ (6) зафиксируем элемент $c \in F_{2^r} \setminus \{0\}$ и пару дуальных базисов B и $\hat{B}$ поля F_{2^r} над подполем $F_{2^{r'}}$. Заметим, что из (6) вытекают равенства $\mathrm{Tr}_{2^{r'}}^{2^r}(cb_i) = \mathrm{Tr}_{2^{r'}}^{2^r}(A_i(ca)) \oplus \mathrm{Tr}_{2^{r'}}^{2^r}(c\xi_i)$, $i \in \overline{0, N-1}$, причем $\mathrm{Tr}_{2^{r'}}^{2^r}(A_i(ca))$ является скалярным произведением векторов A'_i и a' над полем $F_{2^{r'}}$, которые получены в результате замены каждой координаты вектора A_i (соответственно вектора ca) ее представлением в базисе B (соответственно в базисе $\hat{B}$). Отсюда следует, что вектор $a' \in F_{2^{r'}}^{nr''}$ совпадает с истинным решением системы уравнений с искаженными правыми частями

$$A'_i x = b'_i = A'_i a' \oplus \eta_i, \quad i \in \overline{0, N-1}, \tag{7}$$

где $b'_i = \mathrm{Tr}_{2^{r'}}^{2^r}(cb_i)$, $\eta_i = \mathrm{Tr}_{2^{r'}}^{2^r}(c\xi_i)$ для любого $i \in \overline{0, N-1}$.

Таким образом, для восстановления вектора a из СУ (4) достаточно построить для заранее выбранных делителя r' числа r и элемента $c \in F_{2^r} \setminus \{0\}$ систему уравнений (7) над полем $F_{2^{r'}}$ и найти ее истинное решение a' одним из известных методов. Зная вектор a' и базис $\hat{B}$, можно получить вектор ca, а следовательно, и искомый вектор a.

Отметим, что все известные корреляционные атаки на SNOW 2.0 базируются на решении систем уравнений указанного вида (однако без явного применения функции следа) или следствий таких СУ, состоящих из линейных комбинаций их уравнений. В частности, в [3, 4, 6] рассматриваются булевы системы линейных уравнений с искаженными правыми частями ($r' = 1$), получаемые из СУ (4) с помощью определенных линейных преобразований над полем F_2, а в [7] представлены аналогичные системы уравнений над полем порядка 2^8 ($r' = 8$). Кроме того, в [5] предлагается использовать непосредственно СУ (4) над полем порядка 2^{32} для построения различающей атаки на SNOW 2.0.

АЛГОРИТМ РЕШЕНИЯ ПОЛУЧЕННЫХ СИСТЕМ ЛИНЕЙНЫХ УРАВНЕНИЙ С ИСКАЖЕННЫМИ ПРАВЫМИ ЧАСТЯМИ

В настоящее время известно достаточно много быстрых (субэкспоненциальных) алгоритмов решения систем линейных уравнений с искаженными правыми частями над полем, состоящим из двух элементов (см., например, [14–16]). Некоторые из них допускают естественные обобщения на случаи СУ над конечными полями характеристики 2 [7] и даже над произвольными конечными кольцами [17]. Предполагается, что при проведении корреляционной атаки на SNOW 2.0-подобные шифры для решения СУ (7) используется алгоритм, предложенный в [7]. Этот алгоритм включает два этапа и зависит от чисел $k \geq 2$ и $l' \in \overline{1, l}$, при этом k является степенью двойки, а $l = nr''$.

На первом этапе с помощью алгоритма Вагнера (Wagner's k-tree algorithm) [18] проводится исключение из исходной СУ (7) последних $l - l'$ неизвестных. В результате получается новая СУ с искаженными правыми частями от l' неизвестных над полем $F_{2^{r'}}$, каждое уравнение которой является суммой некоторых k уравнений исходной СУ. На втором этапе полученная СУ решается методом максимума правдоподобия с использованием быстрого преобразования Адамара. Таким образом, указанный алгоритм позволяет восстановить первые l' неизвестных системы уравнений (7). Применяя его $\lceil l / l' \rceil$ раз к непересекающимся наборам неизвестных, можно найти искомый вектор a'.

Отметим, что распределение искажений η_i в правых частях уравнений системы (7) имеет следующий вид:

$$\mathbf{P}\{\eta_i = z\} = \sum_{x \in F_{2^r}:\ \mathrm{Tr}_{2^{r'}}^{2^r}(cx) = z} \mathbf{P}\{\xi_i = x\},\ z \in F_{2^{r'}}, \tag{8}$$

где случайная величина ξ_i определяется по формуле (5), $i \in \overline{0, N-1}$. Кроме того, искажение в правой части каждого уравнения системы, получаемой в результате выполнения первого этапа алгоритма, является суммой k независимых случайных величин, распределенных по закону (8). Следовательно, распределение искажений в правых частях уравнений системы, полученной после первого этапа алгоритма, имеет вид

$$p_{c, r', k}(z) = \mathbf{P}\{\eta_1 \oplus \cdots \oplus \eta_k = z\},\ z \in F_{2^{r'}}. \tag{9}$$

Отметим также, что эти искажения являются зависимыми случайными величинами, однако в [7] (неявно) используется эвристическое допущение об их независимости. Известно [17, 19], что при таком допущении для восстановления истинного решения СУ (7) с вероятностью ошибки не более $\delta \in (0, 1/2)$ на втором этапе алгоритма необходимо иметь не менее $m_{c, r'}(k, l') = \Delta_{c, r'}(k)^{-1}((1-\delta)l'r' - h(\delta))\ln 2$ уравнений, где $h(\delta) = -\delta \log_2 \delta - (1-\delta)\log_2(1-\delta)$,

$$\Delta_{c, r'}(k) = 2^{-r'} \sum_{z \in F_{2^{r'}}} (2^{r'} p_{c, r', k}(z) - 1)^2\ . \tag{10}$$

В [7] для оценки числа уравнений, необходимых для надежного решения СУ на втором этапе алгоритма, используется эвристическая формула

$$m_{c, r'}(k, l') = 2\Delta_{c, r'}(k)^{-1} l'r' \ln 2\,. \tag{11}$$

При этом согласно [7] средняя временная сложность алгоритма решения СУ (7) (при условии независимого случайного равновероятного выбора строк A_i', $i \in \overline{0, N-1}$) определяется по формуле

$$T_{c, r'}(k, l') = (m_{c, r'}(k, l'))^{1/\theta} k 2^{(r'(l-l'))/\theta} + r'(m_{c, r'}(k, l') + r'\, l' 2^{r'l'}) + 2^{r'(l'+1)}, \tag{12}$$

а объем материала (количество знаков гаммы), необходимого для успешного решения этой СУ, находится по формуле

$$N = N_{c, r'}(k, l') = k 2^{(r'(l-l'))/\theta} (2l'r' \ln 2)^{1/\theta} \Delta_{c, r'}(k)^{-1/\theta}, \tag{13}$$

где $\theta = 1 + \log k$ и $m_{c, r'}(k, l')$ имеет вид (11). Очевидно, что для повышения эффективности алгоритма параметры k и l' следует выбирать, исходя из условия минимальности значения (12).

Здесь и далее термин «корреляционная атака» означает одну из атак, описанных в предыдущих разделах. Отметим, что каждая такая атака определяется делителем r' числа r и ненулевым элементом c поля F_{2^r}. Она состоит в построении СУ (7) и последующем ее решении с помощью алгоритма из [7], который зависит от параметра $k \geq 2$ и является степенью двойки, и числа $l' \in \overline{1, l}$, где $l = nr''$, $r' r'' = r$. При этом средняя временная сложность атаки определяется по формуле (12), а объем материала, необходимого для реализации атаки, — по формуле (13). Обе формулы содержат параметр $\Delta_{c, r'}(k)$, который на основании равенств (9), (10) имеет вид

$$\Delta_{c, r'}(k) = 2^{-r'} \sum_{z \in F_{2^{r'}}} (2^{r'} \mathbf{P}\{\eta_1 \oplus \cdots \oplus \eta_k = z\} - 1)^2, \tag{14}$$

где $\eta_i = \mathrm{Tr}_{2^{r'}}^{2^r}(c\xi_i)$, а случайная величина ξ_i определяется по формуле (5), $i \in \overline{1, k}$. Таким образом, оценивание эффективности корреляционных атак на SNOW 2.0-подобные шифры или обоснование стойкости этих шифров относительно указанных атак возможно при вычислении (или оценивании) значения параметра (14) непосредственно по криптосхеме шифра.

Получим выражение этого параметра в терминах коэффициентов Фурье распределения вероятностей случайных величин (5). Отметим, что преобразование Фурье произвольного распределения ($p(z)$: $z \in F_{2^m}$) на поле F_{2^m} определяется по формуле

$$\hat{p}(u) = \sum_{z \in F_{2^m}} p(z)(-1)^{\mathrm{Tr}_2^{2^m}(uz)}, \ u \in F_{2^m},$$

где $\mathrm{Tr}_2^{2^m}(x) = x \oplus x^2 \oplus \cdots \oplus x^{2^{m-1}}$ — абсолютный след произвольного элемента $x \in F_{2^m}$. На основании равенства Парсеваля (см., например, [20, с. 27]) справедлива формула

$$2^{-m} \sum_{z \in F_{2^m}} (2^m p(z) - 1)^2 = \sum_{u \in F_{2^m} \setminus \{0\}} |\hat{p}(u)|^2. \tag{15}$$

Далее, согласно теореме о свертке [20, с. 26] преобразование Фурье распределения суммы независимых случайных величин равно произведению преобразований Фурье распределений слагаемых. Отсюда на основании (14), (15) при $m = r'$, $p(z) = \mathbf{P}\{\eta_1 \oplus \cdots \oplus \eta_k = z\}$, $z \in F_{2^{r'}}$, получаем равенство

$$\Delta_{c, r'}(k) = \sum_{u \in F_{2^{r'}} \setminus \{0\}} |\varphi_c(u)|^{2k}, \tag{16}$$

где

$$\varphi_c(u) = \sum_{z \in F_{2^{r'}}} \mathbf{P}\{\eta_i = z\}(-1)^{\mathrm{Tr}_2^{2^{r'}}(uz)}, \ u \in F_{2^{r'}} \tag{17}$$

есть преобразование Фурье распределения вероятностей случайной величины $\eta_i = \mathrm{Tr}_{2^{r'}}^{2^r}(c\xi_i)$.

Убедимся в справедливости равенства

$$\varphi_c(u) = \hat{\pi}(uc), \ u \in F_{2^{r'}}, \tag{18}$$

где

$$\hat{\pi}(\alpha) = \sum_{x \in F_{2^r}} \mathbf{P}\{\xi_i = x\}(-1)^{\mathrm{Tr}_2^{2^r}(\alpha x)}, \ \alpha \in F_{2^r}. \tag{19}$$

Действительно, используя формулу (17), условие $u \in F_{2^{r'}}$ и транзитивность функции следа (см., например, [13, теорема 2.26]), получаем

$$\varphi_c(u) = \sum_{z \in F_{2^{r'}}} \mathbf{P}\{\mathrm{Tr}_{2^{r'}}^{2^r}(c\xi_i) = z\}(-1)^{\mathrm{Tr}_2^{2^{r'}}(uz)} = \sum_{z \in F_{2^{r'}}} \sum_{\substack{x \in F_{2^r}: \\ \mathrm{Tr}_{2^{r'}}^{2^r}(cx) = z}} \mathbf{P}\{\xi_i = x\}(-1)^{\mathrm{Tr}_2^{2^{r'}}(uz)} =$$

$$= \sum_{x \in F_{2^r}} \mathbf{P}\{\xi_i = x\}(-1)^{\mathrm{Tr}_2^{2^{r'}}(u\mathrm{Tr}_{2^{r'}}^{2^r}(cx))} = \sum_{x \in F_{2^r}} \mathbf{P}\{\xi_i = x\}(-1)^{\mathrm{Tr}_2^{2^{r'}}(\mathrm{Tr}_{2^{r'}}^{2^r}(ucx))} =$$

$$= \sum_{x \in F_{2^r}} \mathbf{P}\{\xi_i = x\}(-1)^{\mathrm{Tr}_2^{2^r}(ucx)} = \hat{\pi}(uc).$$

Таким образом, справедливо равенство (18), из которого на основании (16) вытекает следующая теорема.

Теорема 1. Параметр (14) удовлетворяет равенству

$$\Delta_{c,r'}(k) = \sum_{u \in F_{2^{r'}} \setminus \{0\}} |\hat{\pi}(uc)|^{2k}, \tag{20}$$

где $\hat{\pi}(uc)$ определяется по формуле (19) при $\alpha = uc$.

Полученная теорема позволяет оценивать эффективность корреляционных атак на SNOW 2.0-подобные шифры непосредственно по коэффициентам Фурье распределения случайных величин (5) и является основой для результатов, изложенных далее в статье.

СРАВНЕНИЕ ЭФФЕКТИВНОСТИ КОРРЕЛЯЦИОННЫХ АТАК НАД ПОЛЯМИ РАЗЛИЧНЫХ ПОРЯДКОВ

С помощью теоремы 1 можно определить, насколько эффективнее (с точки зрения средней временной сложности и объема необходимого материала) могут быть корреляционные атаки над полями порядка $2^{r'}$, где $r' \geq 2$, по сравнению с традиционными двоичными атаками на SNOW 2.0-подобные шифры.

Справедлива следующая теорема.

Теорема 2. Пусть $r'r'' = r$, где $r', r'' \in \mathbf{N}$, $c \in F_{2^r} \setminus \{0\}$, $k = 2^s$, где $s \in \mathbf{N}$, $l = nr''$ и $l' \in \overline{1, l}$. Обозначим α^* ненулевой элемент поля F_{2^r} такой, что

$$|\hat{\pi}(\alpha^*)| = \max_{\alpha \in F^r \setminus \{0\}} |\hat{\pi}(\alpha)|, \tag{21}$$

где $\hat{\pi}(\alpha)$ определяется по формуле (19). Тогда для параметров (12) и (13) справедливы следующие неравенства:

$$T_{c,r'}(k, l') \geq (2^{r'} - 1)^{-1} T_{\alpha^*,1}(k, r'l'), \tag{22}$$

$$N_{c,r'}(k, l') \geq (2^{r'} - 1)^{-1} N_{\alpha^*,1}(k, r'l'). \tag{23}$$

Таким образом, любая корреляционная атака (из рассматриваемого класса атак) над полем $F_{2^{r'}}$ является не более чем в $2^{r'}$ раз эффективнее (с точки зрения как средней временной сложности, так и объема материала) по сравнению с наилучшей корреляционной атакой над полем F_2.

Доказательство. На основании формул (20) и (21) справедливы соотношения $\Delta_{c,r'}(k) = \sum\limits_{u \in F_{2^{r'}} \setminus \{0\}} |\hat{\pi}(uc)|^{2k} \le (2^{r'}-1)|\hat{\pi}(\alpha^*)|^{2k} = (2^{r'}-1)\,\Delta_{\alpha^*,1}(k)$. Используя формулы (11), (12), получаем

$$T_{c,r'}(k, l') = (2\Delta_{c,r'}(k)^{-1} l' r' \ln 2)^{1/\theta} k 2^{(r'(l-l'))/\theta} +$$

$$+ r' (2\Delta_{c,r'}(k)^{-1} l' r' \ln 2 + r' l' 2^{r'l'}) + 2^{r'(l'+1)} \ge$$

$$\ge (2^{r'}-1)^{-1/\theta} (2\Delta_{\alpha^*,1}(k)^{-1} l' r' \ln 2)^{1/\theta} k 2^{(r'(l-l'))/\theta} +$$

$$+ r' (2^{r'}-1)^{-1} (2\Delta_{\alpha^*,1}(k)^{-1} l' r' \ln 2 + r' l' 2^{r'l'}) + 2^{t'(l'+1)}.$$

Далее, полагая $l'' = r' l'$ и используя равенства $r'l = r' nr'' = nr$, $r' \ge 1$, получаем следующие соотношения:

$$T_{c,r'}(k, l') \ge (2^{r'}-1)^{-1} (2\Delta_{\alpha^*,1}(k)^{-1} l'' \ln 2)^{1/\theta} k 2^{(nr-l'')/\theta} +$$

$$+ (2^{r'}-1)^{-1} (2\Delta_{\alpha^*,1}(k)^{-1} l'' \ln 2 + l'' 2^{l''}) + 2^{l''+1} = (2^{r'}-1)^{-1} T_{\alpha^*,1}(k, l'').$$

Итак, справедливо неравенство (22). Неравенство (23) доказывается аналогично. Теорема доказана.

Пример 1. В работе [7] описана корреляционная атака на SNOW 2.0 над полем F_{2^8}, которая имеет среднюю временную сложность $2^{164,15}$ и требует приблизительно $2^{163,59}$ знаков гаммы. Эта атака намного быстрее по сравнению с ранее известной двоичной атакой, сложность которой составляет $2^{212,38}$ [6]. Однако на основании теоремы 2 существует двоичная корреляционная атака на SNOW 2.0, которая имеет среднюю временную сложность не более $2^8 \cdot 2^{164,15} = 2^{172,15}$ и требует не более $2^8 \cdot 2^{163,59} = 2^{171,59}$ знаков гаммы, причем параметры этой атаки (вектор α^* и числа k, l') определяются непосредственно по параметрам исходной атаки над полем F_{2^8} (см. (21), (22)).

Данный пример показывает, что выигрыш в сложности атаки из [7] по сравнению с атакой из [6] достигается не столько за счет увеличения порядка поля (с двух до 256), сколько в результате удачного выбора системы уравнений с искаженными правыми частями и применения более эффективного алгоритма ее решения при проведении атаки.

Итак, согласно теореме 2 переход от двоичных корреляционных атак к атакам над полями порядка $2^{r'}$ может повысить эффективность первых не более чем в $2^{r'}$ раз.

ОЦЕНКИ СТОЙКОСТИ SNOW 2.0-ПОДОБНЫХ ШИФРОВ ОТНОСИТЕЛЬНО КОРРЕЛЯЦИОНЫХ АТАК

Рассмотрим произвольный SNOW 2.0-подобный шифр (см. рис. 1). Отметим, что согласно его определению выполняется равенство $r = pt$, где $p, t \in \mathbf{N}$, $p, t \ge 2$, и существуют базис B поля F_{2^r} над подполем F_{2^t}, подстановки $s_j : F_{2^t} \to F_{2^t}$, $j \in \overline{0, p-1}$, и обратимая $p \times p$-матрица D над полем F_{2^t} такие, что (при отождествлении произвольного элемента поля F_{2^r} с набором его координат в базисе B) выполняется равенство (3).

Обозначим $\hat{B}$ базис, дуальный к базису B. Как и выше, отождествим произвольный элемент $z \in F_{2^r}$ с набором $(z_0, \dots, z_{p-1})$ его координат в базисе B и обозначим этот набор тем же символом: $z = (z_0, \dots, z_{p-1})$. Обозначим $\hat{z} = (\hat{z}_0, \dots, \hat{z}_{p-1})$ набор координат элемента $z \in F_{2^r}$ в базисе $\hat{B}$. Далее будем опускать символ транспонирования в формулах вида Dz^T, предполагая (как обычно), что вектор z является столбцом, если он записан справа от матрицы D.

Для любого $z = (z_0, \dots, z_{p-1}) \in F_{2^t}^p$ обозначим $\operatorname{supp}(z) = \{j \in \overline{0, p-1} : z_j \neq 0\}$, $wt(z) = |\operatorname{supp}(z)|$. Согласно определению в [21] число ветвления (branch number) матрицы D^T определяется по формуле

$$B(D^T) = \min\{wt(z) + wt(zD^T) : z \in F_{2^t}^p \setminus \{0\}\}. \tag{24}$$

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

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

где $\operatorname{msb}(x_i + y_i + u)$ — самый старший (т.е. t-й) разряд суммы целых чисел, соответствующих указанным двоичным векторам длины t; $x_i \overset{t}{+} y_i \overset{t}{+} u$ — сумма этих чисел по модулю 2^t, а выражение в показателе числа (-1) представляет собой булево скалярное произведение указанных двоичных векторов. Наконец, для любого $i \in \overline{0, p-1}$ обозначим

$$n_{a,b}(s_i) = \max\{|A_{a,b}^{(i)}(0,0)| + |A_{a,b}^{(i)}(0,1)|, |A_{a,b}^{(i)}(1,0)| + |A_{a,b}^{(i)}(1,1)|\}. \tag{25}$$

На основании соотношений (12), (13) стойкость рассматриваемого шифра относительно корреляционных атак над полем порядка $2^{r'}$ зависит от параметра (14). Следующая теорема устанавливает верхнюю оценку этого параметра.

Теорема 3. Справедливо неравенство

$$\Delta_{c, r'}(k) \leq (2^{r'} - 1)(n_{\max})^{2k\lceil (B(D^T))/2 \rceil}, \tag{26}$$

где $n_{\max} = \max\{n_{a,b}(s_i) : (a, b) \in V_t \times V_t \setminus \{(0,0)\},\ i \in \overline{0, p-1}\}$; $n_{a,b}(s_i)$ определяется по формуле (25), а $B(D^T)$ — по формуле (24).

Доказательство. Из теоремы 1 следует, что

$$\Delta_{c, r'}(k) \leq (2^{r'} - 1)\left(\max_{\alpha \in F_{2^r} \setminus \{0\}} |\hat{\pi}(\alpha)|\right)^{2k}, \tag{27}$$

где $\hat{\pi}(\alpha) = \sum_{x \in F_{2^r}} \mathbf{P}\{\xi_i = x\}(-1)^{\operatorname{Tr}_2^{2^r}(\alpha x)}$, $\alpha \in F_{2^r} \setminus \{0\}$. При этом согласно формуле (5) случайная величина ξ_i является суммой двух независимых случайных величин:

$$\xi_{1,i} = (x_{i+n-1} \overset{r}{+} u_i) \oplus x_{i+n-1} \oplus \sigma(u_i)$$

и

$$\xi_{2,i} = (x_{i+n} \overset{r}{+} x_{i+\mu} \overset{r}{+} v_i) \oplus (x_{i+n} \oplus x_{i+\mu} \oplus v_i),$$

где $x_{i+\mu}, x_{i+n-1}, x_{i+n}, u_i, v_i$ — независимые случайные величины с равномерным распределением на множестве V_r. Следовательно, по теореме о свертке коэффициенты Фурье распределения ξ_i являются произведениями коэффициентов Фурье распределений $\xi_{1,i}$ и $\xi_{2,i}$, т.е. $\hat{\pi}(\alpha) = \hat{\pi}_1(\alpha)\hat{\pi}_2(\alpha)$, где $\hat{\pi}_1(\alpha) = \sum\limits_{z \in F_{2^r}} \mathbf{P}\{\xi_{1,i} = z\}(-1)^{\mathrm{Tr}_2^{2^r}(\alpha z)}$, $\hat{\pi}_2(\alpha) = \sum\limits_{z \in F_{2^r}} \mathbf{P}\{\xi_{2,i} = z\}(-1)^{\mathrm{Tr}_2^{2^r}(\alpha z)}$. Отсюда следует, что

$$|\hat{\pi}(\alpha)| \le |\hat{\pi}_2(\alpha)| = \left| \sum_{z \in F_{2^r}} \mathbf{P}\{\xi_{2,i} = z\}(-1)^{\mathrm{Tr}_2^{2^r}(\alpha z)} \right| =$$

$$= 2^{-2r} \left| \sum_{x,\, y \in F_{2^r}} (-1)^{\mathrm{Tr}_2^{2^r}(((x \overset{r}{+} y) \oplus x \oplus \sigma(y))\alpha)} \right|.$$

Далее, используя формулу (3) и дуальные базисы B, $\hat{B}$ поля F_{2^r} над подполем F_{2^t}, получаем

$$\mathrm{Tr}_2^{2^r}(((x \overset{r}{+} y) \oplus x \oplus \sigma(y))\alpha) = \mathrm{Tr}_2^{2^t}(((x \overset{r}{+} y) \oplus x) \cdot \hat{\alpha} \oplus s(y) \cdot \hat{\beta}), \qquad (28)$$

где элементы $(x \overset{r}{+} y) \oplus x$ и $s(y) = (s_0(y_0), \ldots, s_{p-1}(y_{p-1}))$ поля F_{2^r} отождествляются с наборами их координат в базисе B; $\hat{\alpha} = (\hat{\alpha}_0, \ldots, \hat{\alpha}_{p-1})$ — набор координат элемента α в базисе $\hat{B}$; $\hat{\beta} = \hat{\alpha} D^T$, а символ $\cdot$ обозначает скалярное произведение векторов над полем F_{2^t}. Выражение в правой части равенства (28) совпадает с булевым скалярным произведением $((x \overset{r}{+} y) \oplus x)\hat{\alpha} \oplus s(y)\hat{\beta}$, если отождествить координаты векторов $(x \overset{r}{+} y) \oplus x$ и $s(y)$ над полем F_{2^t} с наборами их координат в любом фиксированном базисе этого поля над подполем F_2, а координаты векторов $\hat{\alpha}$ и $\hat{\beta}$ — с наборами их координат в соответствующем дуальном базисе. Таким образом, справедливо следующее неравенство:

$$|\hat{\pi}(\alpha)| \le 2^{-2tp} \left| \sum_{x,\, y \in F_{2^t}^p} (-1)^{((x \overset{pt}{+} y) \oplus x)\hat{\alpha} \oplus s(y)\hat{\beta}} \right|, \qquad (29)$$

где $\hat{\alpha} = (\hat{\alpha}_0, \ldots, \hat{\alpha}_{p-1}) \in F_{2^t}^p$, $\hat{\beta} = \hat{\alpha} D^T$, а $((x \overset{r}{+} y) \oplus x)\hat{\alpha}$ и $s(y)\hat{\beta}$ обозначают булевы скалярные произведения указанных двоичных векторов.

Из формулы (29) и теоремы 3 из [9] следует оценка $|\hat{\pi}(\alpha)| \le$ $\le n_{\hat{\alpha}_0, \hat{\beta}_0}(s_0)\, n_{\hat{\alpha}_1, \hat{\beta}_1}(s_1) \cdots n_{\hat{\alpha}_{p-1}, \hat{\beta}_{p-1}}(s_{p-1})$, которая, в свою очередь, влечет неравенство $|\hat{\pi}(\alpha)| \le (n_{\max})^l$, где $l = |\{i \in \overline{0,\, p-1} : (\hat{\alpha}_i, \hat{\beta}_i) \ne (0,0)\}|$.

Далее, используя равенство $\hat{\beta} = \hat{\alpha} D^T$ и формулу (24), получаем $B(D^T) \le wt(\hat{\alpha}) + wt(\hat{\beta}) \le l + l = 2l$. Следовательно, для любого $\alpha \in F_{2^r} \setminus \{0\}$ спра-

ведливо неравенство $|\hat{\pi}(\alpha)| \le (n_{\max})^{\lceil (B(D^T))/2 \rceil}$, из которого ввиду формулы (27) вытекает неравенство (26).

Теорема доказана.

Полученная теорема наряду с соотношениями (11)–(13) определяет возможность оценивания стойкости SNOW 2.0-подобных шифров относительно корреляционных атак над полем порядка $2^{r'}$ непосредственно по параметрам их компонент (см. (24), (25)). При этом использование вместо параметра $\Delta_{c, r'}(k)$ его верхней оценки (26) в формулах (11)–(13) позволяет получить нижние оценки эффективности рассмотренных корреляционных атак с помощью следующего алгоритма.

Алгоритм 1

Исходные данные: натуральные числа n, p, t; подстановки $s_j : F_{2^t} \to F_{2^t}$, $j \in \overline{0, p-1}$; обратимая $p \times p$-матрица D над полем F_{2^t}; число $k \ge 2$, являющееся степенью двойки; делитель r' числа $r = pt$.

Шаг 1. Вычислить значение $\Delta_{r'}(k) = (2^{r'} - 1)(n_{\max})^{2k\lceil (B(D^T))/2 \rceil}$, используя формулы (24), (25).

Шаг 2. Положить $r'' = r / r'$, $l = nr''$, $\theta = 1 + \log k$.

Шаг 3. Для каждого $l' = 1, 2, \ldots, l-1$ вычислить

$$m_{r'}(k) = 2(\Delta_{r'}(k))^{-1} l' r' \ln 2,$$

$$T_{r'}(k, l') = (m_{r'}(k))^{1/\theta} k 2^{(r'(l-l'))/\theta} + r' (m_{r'}(k) + r' l' 2^{r'l'}) + 2^{r'(l'+1)}.$$

Шаг 4. Выбрать $l^* \in \overline{1, l-1}$ такое, что $T_{r'}(k, l^*) = \min\{T_{r'}(k, l') : l' \in \overline{1, l-1}\}$.

Результат:

— число l^* фрагментов (каждый длиной r' бит) начального состояния генератора, которые восстанавливаются с помощью атаки;

— средняя временная сложность атаки $T_{r'}(k, l^*)$;

— объем материала $N_{r'}(k, l^*) = k 2^{(r'(l-l^*))/\theta} (2 l^* r' \ln 2)^{1/\theta} (\Delta_{r'}(k))^{-1/\theta}$, необходимого для успешной реализации атаки.

Для вычисления параметра $n_{\max}$ на шаге 1 алгоритма 1 можно использовать алгоритм 2, корректность которого следует из формулы (25).

Алгоритм 2

Исходные данные: подстановки $s_i : V_t \to V_t$, $i \in \overline{0, p-1}$.

Для каждого $i \in \overline{0, p-1}$ выполнить следующие вычисления.

Шаг 1. Для всех $a \in V_t$, $u, u' \in \{0, 1\}$ вычислить значения функции

$$f^{(i)}_{a, u, u'}(z) = \sum_{x \in V_t : \operatorname{msb}(x + s_i^{-1}(z) + u) = u'} (-1)^{(x + s_i^{-1}(z) + u)a \oplus xa}, \quad z \in V_t.$$

Шаг 2. Вычислить значения

$$A^{(i)}_{a, b}(u, u') = 2^{-2t} \sum_{z \in V_t} f^{(i)}_{a, u, u'}(z) (-1)^{zb}, \quad b \in V_t,$$

с помощью алгоритма быстрого преобразования Адамара.

Шаг 3. Для каждой пары $(a, b) \in V_t \times V_t \setminus \{(0, 0)\}$ вычислить

$$n_{a, b}(s_i) = \max\{|A^{(i)}_{a, b}(0, 0)| + |A^{(i)}_{a, b}(0, 1)|, |A^{(i)}_{a, b}(1, 0)| + |A^{(i)}_{a, b}(1, 1)|\}.$$

Шаг 4. Положить $n_{\max}(s_i) = \max\{n_{a,b}(s_i) : (a, b) \in V_t \times V_t \setminus \{(0, 0)\}\}$.

Результат: $n_{\max} = \max\limits_{i \in \overline{0, p-1}} \{n_{\max}(s_i)\}$.

Отметим, что применение алгоритма быстрого преобразования Адамара (см., например, [22, с. 217]) на шаге 2 алгоритма 2 позволяет сократить временную сложность вычисления значения параметра $n_{\max}$ до $O(pt2^{3t})$ операций вместо $O(p2^{4t})$ операций, используемых при обычном алгоритме, основанном на определении этого параметра.

Пример 2. Получим нижние оценки параметров, характеризующих эффективность корреляционных атак над полем $F_{2^t} = F_{256}$ на шифр SNOW 2.0 (замечание 1). В рассматриваемом случае $t = 8$, $p = 4$, $n = 16$, а подстановка σ имеет вид (3), где подстановки $s_i : F_{2^t} \to F_{2^t}$, $i \in \overline{0, p-1}$, и матрица D задаются так же, как в раундовом преобразовании шифра Rijndael, в частности $B(D^T) = p + 1 = 5$.

С использованием алгоритма 2 находим $n_{\max} = 2^{-3}$. Отсюда с помощью алгоритма 1 получим значения, приведенные в табл. 1.

Из полученных результатов следует, что любая (рассмотренная выше) корреляционная атака над полем порядка 256 на SNOW 2.0 имеет среднюю временную сложность не менее $2^{146,20}$ и требует не менее $2^{142,77}$ знаков гаммы. Отметим, что наилучшая из известных корреляционных атак на этот шифр требует порядка $2^{163,59}$ знаков гаммы и имеет среднюю временную сложность $2^{164,15}$ [7]. Дальнейшее увеличение параметра k в алгоритме 1 приводит к увеличению значений параметров $T_{r'}(k, l^*)$, $N_{r'}(k, l^*)$.

Пример 3. Рассмотрим шифр «Струмок» (замечание 2), в котором используются следующие параметры: $t = 8$, $p = 8$, $n = 16$. При этом подстановка σ имеет вид (3), где s-блоки и матрица D задаются так же, как в блочном шифре «Калина». В частности, в шифре «Струмок» применяются четыре разные подстановки: π_0, π_1, π_2, π_3, каждая из которых используется дважды; при этом $B(D^T) = p + 1 = 9$.

В табл. 2 приведены значения параметра $n_{\max}(\pi_i)$, $i \in \overline{0, 3}$, а также векторов a, b, на которых достигается максимум в выражении этого параметра (см. шаг 4

Таблица 1

k	Результаты выполнения алгоритма 1 для шифра SNOW 2.0 ($r' = 8$)		
	l^*	$\log T_{r'}(k, l^*)$	$\log N_{r'}(k, l^*)$
2	22	187,84	186,97
4	17	151,24	151,19
8	12	146,20	142,77
16	1	292,45	161,50

Таблица 2

Подстановка π, используемая в шифре «Калина»	Результаты применения алгоритма 2 для s-блоков шифра «Струмок»		
	Значения $n_{\max}(\pi)$	a	b
π_0	$3 \cdot 2^{-4}$	1 = (0000 0001)	212 = (1101 0100)
π_1	$11 \cdot 2^{-6}$	1 = (0000 0001)	244 = (1111 0100)
π_2	$5 \cdot 2^{-5}$	1 = (0000 0001)	20 = (0001 0100)
π_3	$5 \cdot 2^{-5}$	1 = (0000 0001)	190 = (1011 1110)

Таблица 3

k	Результаты выполнения алгоритма 1 для шифра «Струмок» ($r' = 8$)		
	l^*	$\log T_{r'}(k, l^*)$	$\log N_{r'}(k, l^*)$
2	44	363,91	361,62
4	34	285,42	285,06
8	29	249,40	249,38
16	1	384,88	283,58

алгоритма 2). Используя данные табл. 2 и алгоритм 1, получаем значения параметров, характеризующих эффективность корреляционных атак над полем $F_{2^t} = F_{256}$ на шифр «Струмок».

Дальнейшее увеличение параметра k в алгоритме 1 приводит к увеличению значений параметров $T_{r'}(k, l^*)$, $N_{r'}(k, l^*)$ в табл. 3. Таким образом, любая рассмотренная выше корреляционная атака над полем порядка 256 на «Струмок» имеет среднюю временную сложность не менее $2^{249,40}$ и требует не менее $2^{249,38}$ знаков гаммы.

ЗАКЛЮЧЕНИЕ

Предложен метод оценивания стойкости SNOW 2.0-подобных шифров относительно корреляционных атак, которые строятся по аналогии с известными атаками на SNOW 2.0 [3–7]. Каждая такая атака определяется делителем r' степени r поля, над которым задается регистр сдвига с линейной обратной связью (см. рис. 1), а также ненулевым элементом этого поля и заключается в составлении и решении системы линейных уравнений с искаженными правыми частями (7) с помощью алгоритма из [7].

Теорема 1 сводит задачу получения нижних оценок временной сложности атак из указанного класса и объема материала, необходимого для их успешной реализации, к построению верхних оценок максимума модулей коэффициентов Фурье распределения искажений в правых частях уравнений системы (4), которая не зависит от конкретной атаки. Таким образом, эффективность корреляционных атак на SNOW 2.0-подобные шифры можно оценить непосредственно по коэффициентам Фурье распределения случайных величин (5), что и составляет основу предложенного метода.

Любая корреляционная атака над полем $F_{2^{r'}}$ (из рассматриваемого класса атак) не более чем в $2^{r'}$ раз эффективнее (относительно как средней временной сложности, так и объема материала) по сравнению с наилучшей корреляционной атакой над полем F_2.

Теорема 3 позволяет оценить стойкость SNOW 2.0-подобных шифров относительно корреляционных атак над полем порядка $2^{r'}$ непосредственно по параметрам (24), (25) их компонент. При этом использование вместо параметра $\Delta_{c, r'}(k)$ его верхней оценки (26) в формулах (11)–(13) позволяет получать нижние оценки средней временной сложности и объема материала, необходимого для проведения на шифр любой описанной корреляционной атаки.

Применение теоремы 3 к шифрам SNOW 2.0 и «Струмок» показывает, что любая описанная корреляционная атака на них над полем порядка 256 имеет среднюю временную сложность не менее $2^{146,20}$ и $2^{249,40}$ соответственно и требует не менее $2^{142,77}$ и $2^{249,38}$ соответственно знаков гаммы.

СПИСОК ЛИТЕРАТУРЫ

1. Ekdahl P., Johansson T. A new version of the stream cipher SNOW. *Selected Areas in Cryptography — SAC 2002*. LNCS 2295. Springer-Verlag. P. 47–61.
2. ISO/IEC 18033-4: 2011(E). Information technology — Security techniques — Encryption algorithm. Part 4: Stream ciphers, 2011. 92 p.
3. Watanabe D., Biryukov A., de Cannière C. A distinguishing attack of SNOW 2.0 with linear masking method. *Selected Arreas in Cryptography — SAC 2003.* LNCS 3006. Springer-Verlag. P. 222–233.
4. Nyberg K., Wallén J. Improved linear distinguishers for SNOW 2.0. *Fast Software Encryption — FSE 2006*. LNCS 4047. Springer-Verlag, 2006. P. 144–162.
5. Maximov A., Johansson Th. Fast computation for large distribution and its cryptographic application. *Advanced in Cryptology — ASIACRYPT 2005.* LNCS 3788. Springer-Verlag, 2005. P. 313–332.
6. Lee J.-K., Lee D.H., Park S. Cryptanalysis of SOSEMANUC and SNOW 2.0 using linear masks. *Advanced in Cryptology — ASIACRYPT 2008*. LNCS 5350. Springer-Verlag, 2008. P. 524–538.
7. 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.
8. 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.
9. Алексейчук А.Н., Конюшок С.Н., Поремский М.В. Верхние оценки несбалансированности дискретных функций, реализуемых последовательностями конечных автоматов. *Кибернетика и системный анализ.* 2019. Т. 55, № 5. С. 58–66.
10. Олексійчук А.М. Достатня умова стійкості SNOW 2.0-подібних потокових шифрів відносно певних атак зі зв'язаними ключами. *Захист інформації*. 2016. Т. 18, № 3. С. 261–268.
11. Oliynykov R.V., Gorbenko I.D., Kazymyrov O.V. et. al. A new encryption standard of Ukraine: The Kalyna block cipher. *Cryptology ePrint Archive*. URL: http://eprint.iacr.org/2015/650.
12. 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.
13. Лидл Р., Нидеррайтер Г. Конечные поля: В 2 т. Пер. с англ. Москва: Мир, 1988. 818 с.
14. Blum A., Kalai A., Wasserman H. Noise-tolerant learning, the parity problem, and the statistical query model. *J. ACM.* 2003. Vol. 50, N 3. P. 506–519.
15. Олексійчук А.М. Субекспоненційні алгоритми розв'язання систем лінійних булевих рівнянь зі спотвореними правими частинами. *Прикладная радиоэлектроника*. 2012. Т. 11, № 2. С. 3–11.
16. Bogos S., Tramér F., Vaudenay S. On solving LPN using BKW and variants. Implementation and analysis. *Cryptology ePrint Archive*, Report 2015/049. URL: http://eprint.iacr.org/2015/049.
17. Олексійчук А.М, Ігнатенко С.М., Поремський М.В. Системи лінійних рівнянь зі спотвореними правими частинами над скінченними кільцями. *Математичне та комп'ютерне моделювання.* Серія: Технічні науки. 2017. Вип. 15. С. 150–155.
18. Wagner D. A generalized birthday problem. Advances in Cryptology — CRYPTO'02, Proceedings. Springer-Verlag, 2002. P. 288–303.
19. Олексійчук А.М., Поремський М.В. Нижні межі інформаційної складності кореляційних атак на потокові шифри над полями порядку 2^r. *Захист інформації.* 2017. Т. 19, № 2. С. 119–124.
20. Carlet C. Boolean functions for cryptography and error correcting codes. In: *Boolean Methods and Models*. Cambridge, U.K.: Cambridge Univ. Press, 2006.
21. Daemen J. Cipher and hash function design strategies based on linear and differential cryptanalysis. *Doctoral Dissertation,* 1995.
22. Логачев О.А., Сальников А.А., Ященко В.В. Булевы функции в теории кодирования и криптологии. Москва: МЦНМО, 2004. 470 с.

Надійшла до редакції 27.11.2018

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

МЕТОД ОЦІНЮВАННЯ СТІЙКОСТІ SNOW 2.0-ПОДІБНИХ ШИФРІВ ВІДНОСНО КОРЕЛЯЦІЙНИХ АТАК НАД СКІНЧЕННИМИ РОЗШИРЕННЯМИ ПОЛЯ З ДВОХ ЕЛЕМЕНТІВ

Анотація. Запропоновано метод оцінювання стійкості SNOW 2.0-подібних шифрів відносно кореляційних атак, які будуються за аналогією до відомих атак на шифр SNOW 2.0. На відміну від раніше відомих запропонований метод орієнтований на обґрунтування стійкості і дозволяє отримувати нижні оцінки ефективності атак з розглянутого класу безпосередньо за параметрами компонент поточних шифрів аналогічно тому, як це робиться при обґрунтуванні стійкості блокових шифрів відносно лінійного криптоаналізу. Застосування методу до шифрів SNOW 2.0 і «Струмок» показує, що будь-яка з розглянутих кореляційних атак на них над полем порядку 256 має середню часову складність не менше $2^{146,20}$ і $2^{249,40}$ відповідно і вимагає не менше $2^{142,77}$ і $2^{249,38}$ відповідно знаків гами.

Ключові слова: кореляційний криптоаналіз, скінченний автомат, дискретне перетворення Фур'є, обґрунтування стійкості, шифр SNOW 2.0, шифр «Струмок».

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

A METHOD FOR SECURITY EVALUATION OF SNOW 2.0-LIKE CIPHERS AGAINST CORRELATION ATTACKS OVER FINITE EXTENSIONS OF THE FIELD OF TWO ELEMENTS

Abstract. A method is proposed for security evaluation of SNOW 2.0-like ciphers against correlation attacks, which are generated by analogy with well-known attacks against SNOW 2. Unlike the available methods, the proposed one is oriented to the proof of security and allows us to obtain lower estimates of the efficiency of attacks from the considered class directly using the stream cipher components in the same way as it is done to prove the security of block ciphers against linear cryptanalysis. Application of the method to SNOW 2.0 and "Strumok" ciphers shows that any of the considered correlational attacks against them over the field of order 256 has an average time complexity no less than $2^{146,20}$ and $2^{249,40}$, respectively, and requires no less than $2^{142,77}$ and $2^{249,38}$ respectively, keysteam symbols.

Keywords: correlation cryptanalysis, finite-state machine, discrete Fourier transform, proof of security, SNOW 2.0, "Strumok".

Алексейчук Антон Николаевич,
доктор техн. наук, доцент, профессор кафедры Национального технического университета Украины «Київський політехнічний інститут імені Ігоря Сікорського», e-mail: alex-dtn@ukr.net.

Конюшок Сергей Николаевич,
кандидат техн. наук, доцент, заместитель начальника Национального технического университета Украины «Київський політехнічний інститут імені Ігоря Сікорського», e-mail: 3tooth@iszzi.kpi.ua.

Поремский Михаил Васильевич,
аспирант Национального технического университета Украины «Київський політехнічний інститут імені Ігоря Сікорського», e-mail: undermyclouds@gmail.com.