УДК 621.391:519.2

А.Н. АЛЕКСЕЙЧУК, С.Н. КОНЮШОК, А.Ю. СТОРОЖУК

СТАТИСТИЧЕСКАЯ АТАКА НА ГЕНЕРАТОР ГАММЫ С ЛИНЕЙНЫМ ЗАКОНОМ РЕИНИЦИАЛИЗАЦИИ НАЧАЛЬНОГО СОСТОЯНИЯ И ФУНКЦИЕЙ УСЛОЖНЕНИЯ, БЛИЗКОЙ К АЛГЕБРАИЧЕСКИ ВЫРОЖДЕННОЙ

Введение

Одним из требований к современным синхронным поточным шифрам является условие их практической стойкости относительно атак на основе известных или подобранных векторов инициализации. Возможность осуществления таких атак на практике обусловлена особенностями функционирования синхронных поточных шифров (необходимостью синхронизации устройств зашифрования и расшифрования информации путем реинициализации начального состояния генератора гаммы (ГГ) поточного шифра) [1].

Одна из первых атак на основе известных векторов инициализации предложена в [2]. В этой работе показано, что если закон реинициализации (формирования начального состояния ГГ по ключу и вектору инициализации) является линейным, а функция усложнения зависит от s переменных, то на генератор можно провести алгебраическую атаку со сложностью $O(tsl_0^2 + t2^s)$ операций, где t – длина отрезка гаммы, вырабатываемого генератором при каждом запуске (новом значении вектора инициализации), l_0 – длина ключа; при этом требуется, чтобы число запусков было не меньше, чем 2^s.

Атака из [2] совершенствовалась и обобщалась в различных направлениях [3 – 6]. В [4] показано, что она применима к генератору гаммы с алгебраически вырожденной функцией усложнения порядка $n-s$ (то есть функцией от $n>s$ переменных, линейно эквивалентной функции от s переменных); рассмотрен также случай, в котором указанная функция может быть неизвестна криптоаналитику. В [5], наряду с другими, описана статистическая атака на ГГ с линейным законом реинициализации начального состояния и произвольной функцией усложнения, близкой к аффинной булевой функции. Отметим также работу [7], в которой предложен алгоритм восстановления начального состояния генератора гаммы по единственному отрезку выходной последовательности в предположении, что криптоаналику доступны знаки этой последовательности в определенных тактах, номера которых экспоненциально зависят от длины начального состояния ГГ.

В настоящей статье представлена атака на генератор гаммы на основе известных векторов инициализации, которая отличается от алгоритма из [7] и применима при менее жестких ограничениях относительно функции усложнения ГГ по сравнению с указанными выше атаками, описанными в [4, 5]. При общих естественных предположениях получена оценка трудоемкости предложенной атаки. Приведены результаты численных расчетов и вычислительных экспериментов.

Постановка задачи и основные теоретические результаты

Ниже используются следующие обозначения: V_n – множество двоичных векторов длины n, $F_{m\times n}$ – множество матриц размера $m\times n$ над полем $F=\mathbf{GF}(2)$, $\overline{a,b}=\{i\in \mathrm{Z}: a\le i\le b\}$, где $a,b\in \mathrm{Z}$.

Рассмотрим генератор гаммы, функционирование которого в режиме реинициализации начального состояния описывается следующей системой уравнений (СУ):

$$x^{(j)}=Ak\oplus Bc^{(j)},\ f(L^i(x^{(j)}))=\gamma_i^{(j)},\ i\in\overline{0,T-1},\ j\in\overline{1,r}. \qquad (1)$$

Здесь $x^{(j)}\in V_N$ – начальное состояние генератора при j-м запуске, соответствующее ключу

$k \in V_{l_0}$ и вектору инициализации $c^{(j)} \in V_{l_1}$; A и B – булевы матрицы; $f = f(x_1, \ldots, x_N)$ – функция усложнения генератора, существенно зависящая от n переменных $x_{\mu_1}, \ldots, x_{\mu_n}$, где $1 \le \mu_1 < \ldots < \mu_n \le N$; $L : V_N \to V_N$ – невырожденное линейное преобразование над полем F; $\gamma_i^{(j)}$ – знак шифрующей гамы в i-м такте при j-м запуске ГГ, $i \in \overline{0, T-1}$, $j \in \overline{1, r}$. Требуется восстановить ключ k по известным значениям f, L, A, B, $\gamma_i^{(j)}$, $c^{(j)}$, $i \in \overline{0, T-1}$, $j \in \overline{1, r}$.

Обозначим символом P $n \times N$-матрицу над полем F такую, что $Px^{\mathrm{T}} = (x_{\mu_1}, \ldots, x_{\mu_n})^{\mathrm{T}}$ для любого $x = (x_1, \ldots, x_N) \in V_N$, положим $A_i = PL^i A$, $B_i = PL^i B$, $i = 0, 1, \ldots$, и запишем СУ (1) в виде

$$f(A_i k \oplus B_i c^{(j)}) = \gamma_i^{(j)}, \; i \in \overline{0, T-1}, \; j \in \overline{1, r}. \tag{2}$$

Предположим, что выполнены следующие условия.

1. Существует функция $g(x) = \varphi(Mx)$, $x \in V_n$, где $\varphi : V_s \to \{0, 1\}$, $M \in F_{s \times n}$, такая, что

$$\mathrm{P}\{f(X) = g(X)\} = p \ge 1/2 \cdot (1 + \varepsilon), \; \varepsilon \in (0, 1), \tag{3}$$

где X – случайный равновероятный двоичный вектор длины n; другими словами, для функции f существует s-мерный статистический аналог g, находящийся от f на расстоянии не более $2^{n-1}(1 - \varepsilon)$, где $\varepsilon \in (0, 1)$;

2. Существует множество $I = \{i_1, i_2, \ldots, i_t\} \subseteq \overline{0, T-1}$ такое, что

$$\mathrm{rank}(B_{i_1}) = \mathrm{rank}(B_{i_2}) = \ldots = \mathrm{rank}(B_{i_t}) = n \le l_1 \tag{4}$$

и

$$\mathrm{rank} \begin{pmatrix} MA_{i_1} \\ MA_{i_2} \\ \ldots\ldots \\ MA_{i_t} \end{pmatrix} = l_0 \tag{5}$$

(напомним, что l_0 и l_1 обозначают длину ключа и вектора инициализации соответственно).

При выполнении указанных условий можно предложить следующий алгоритм восстановления ключа рассматриваемого ГГ.

Исходные данные: f, L, A, B, $\gamma_i^{(j)}$, $c^{(j)}$ ($i \in \overline{0, T-1}$, $j \in \overline{1, r}$), φ, M.

Этап 1 (*предварительные вычисления*). Построить множество I, удовлетворяющее условию 2; вычислить матрицы MA_i, MB_i, $i \in I$.

Этап 2 (*применение метода максимума правдоподобия*). Для каждого $i \in I$ вычислить значения

$$\nu_i(y) = \sum_{j=1}^{r} (\varphi(y \oplus MB_i c^{(j)}) \oplus \gamma_i^{(j)}), \; y \in V_s \tag{6}$$

и найти вектор $\hat{y}_i \in V_s$ такой, что $\nu_i(\hat{y}_i) = \min\limits_{y \in V_s} \nu_i(y)$.

Этап 3 (*восстановление ключа*). Составить систему линейных уравнений

$$MA_i k = \hat{y}_i, \; i \in I \tag{7}$$

относительно ключа k и, решая ее, найти этот ключ.

Замечание. Из равенства (5) следует, что СУ (7) имеет не более одного решения. Поэтому, если указанная система совместна, то ключ будет восстановлен однозначно.

Для того чтобы оценить эффективность описанного алгоритма, сделаем *два дополнительных предположения относительно функционирования ГГ.*

Прежде всего, предположим, что векторы инициализации $c^{(1)}, c^{(2)},\ldots,c^{(r)}$ независимы в совокупности, случайны и равномерно распределены на множестве V_{l_1}.

Для любых $i \in I$, $y \in V_s$ рассмотрим события $\Omega_i^{(j)}(y) = \{\varphi(y \oplus MB_i c^{(j)}) \oplus \gamma_i^{(j)} = 1\}$, $j \in \overline{1,r}$. Заметим, что эти события независимы в совокупности для каждой пары значений $i \in I$, $y \in V_s$. Кроме того, на основании условия (4) случайные векторы $B_i c^{(j)}$, $j \in \overline{1,r}$, равномерно распределены на множестве V_n. Отсюда в силу соотношений (2), (3) вытекает, что при $y = MA_i k$

$$\mathbf{P}\left(\Omega_i^{(j)}(MA_i k)\right) = \mathbf{P}\{\varphi(MA_i k \oplus MB_i c^{(j)}) \oplus \gamma_i^{(j)} = 1\} = \mathbf{P}\{g(A_i k \oplus B_i c^{(j)}) \oplus f(A_i k \oplus B_i c^{(j)}) = 1\} =$$

$$= \mathbf{P}\{g(X) \oplus f(X) = 1\} = 1 - p \le 1/2 \cdot (1 - \varepsilon).$$

Итак, для любых $i \in I$, $j \in \overline{1,r}$ справедливо следующее соотношение:

$$\mathbf{P}\left(\Omega_i^{(j)}(MA_i k)\right) \le 1/2 \cdot (1 - \varepsilon). \tag{8}$$

Примем в качестве второго предположения относительно функционирования ГГ, что

$$\mathbf{P}\left(\Omega_i^{(j)}(y)\right) = 1/2 \tag{9}$$

для любых $i \in I$, $j \in \overline{1,r}$ и $y \ne MA_i k$.

Обозначим $P_{\text{ід}}$ ошибки описанного алгоритма, то есть вероятность события, состоящего в том, что алгоритм не восстановит искомый ключ k.

Лемма. При указанных выше предположениях справедливо неравенство

$$P_{\text{ід}} \le 2^s t \exp\{-1/8 \cdot r\, \varepsilon^2\}. \tag{10}$$

Доказательство. Если алгоритм совершает ошибку, то нарушается хотя бы одно из равенств (7). Следовательно, $P_{\text{ід}} \le \sum\limits_{i \in I} \mathbf{P}\{MA_i k \ne \hat{y}_i\} \le t \max\limits_{i \in I} \mathbf{P}\{MA_i k \ne \hat{y}_i\}$ и для доказательства формулы (10) достаточно убедиться в справедливости следующих неравенств:

$$\mathbf{P}\{MA_i k \ne \hat{y}_i\} \le 2^s \exp\{-1/8 \cdot r\, \varepsilon^2\},\ i \in I. \tag{11}$$

Зафиксируем $i \in I$. Заметим, что в силу определения вектора $\hat{y}_i$ для любого $C > 0$ справедливы соотношения $\{MA_i k \ne \hat{y}_i\} \subseteq \{\nu_i(MA_i k) \ge C\} \cup \bigcup\limits_{y \in V_s : y \ne MA_i k} \{\nu_i(y) < C\}$, из которых следует, что

$$\mathbf{P}\{MA_i k \ne \hat{y}_i\} \le \mathbf{P}\{\nu_i(MA_i k) \ge C\} + (2^s - 1) \max_{y \in V_s : y \ne MA_i k} \mathbf{P}\{\nu_i(y) < C\}. \tag{12}$$

Далее, согласно равенству (6), $\nu_i(MA_i k)$ является суммой независимых случайных величин $\xi_j = \varphi(MA_i k \oplus MB_i c^{(j)}) \oplus \gamma_i^{(j)}$, $j \in \overline{1,r}$. Следовательно, полагая

$$C = 1/4 \cdot r(2 - \varepsilon), \tag{13}$$

на основании формулы (8) и неравенства для вероятностей больших уклонений (см. например, [8, с.31]) получим следующие соотношения:

$$\mathbf{P}\{\nu_i(MA_i k) \ge C\} = \mathbf{P}\{\sum_{i=1}^{r}\xi_i - \sum_{i=1}^{r}\mathbf{E}\xi_i \ge C - 1/2\cdot r(1-\varepsilon)\} \le \mathbf{P}\{\sum_{i=1}^{r}\xi_i - \sum_{i=1}^{r}\mathbf{E}\xi_i \ge 1/4\cdot r\varepsilon\} \le \exp\{-1/8\cdot r\varepsilon^2\} \quad (14)$$

Пусть теперь $y \in V_s$, $y \ne MA_i k$; тогда в силу равенств (6), (9) $\nu_i(y)$ является суммой независимых случайных величин $\eta_j = \varphi(y \oplus MB_i c^{(j)}) \oplus \gamma_i^{(j)}$, $j \in \overline{1,r}$, каждая из которых распределена равномерно на множестве $\{0,1\}$. Следовательно, на основании формулы (13) и неравенства для вероятностей больших уклонений

$$\mathbf{P}\{\nu_i(y) < C\} = \mathbf{P}\{\sum_{i=1}^{r}\eta_i - \sum_{i=1}^{r}\mathbf{E}\eta_i < C - 1/2\cdot r\} = \mathbf{P}\{\sum_{i=1}^{r}\eta_i - \sum_{i=1}^{r}\mathbf{E}\eta_i < -1/4\cdot r\varepsilon\} \le \exp\{-1/8\cdot r\varepsilon^2\} \quad (15)$$

Подставляя оценки (14), (15) в формулу (12), получим неравенство (11).

Лемма доказана.

Примем в качестве элементарной произвольную двоичную операцию (булеву функцию двух переменных), операцию вычисления значения функции φ, а также операцию вида $i \mapsto i+1$, где i – любое неотрицательное целое число.

Следующая теорема позволяет оценить эффективность описанного алгоритма.

Теорема. Пусть выполняются указанные выше предположения относительно генератора гаммы, $\delta \in (0,1)$ и

$$r = \left\lceil 8\cdot\varepsilon^{-2}\ln(2^s t\,\delta^{-1})\right\rceil. \quad (16)$$

Тогда описанный алгоритм восстанавливает ключ k с вероятностью не менее $1-\delta$, используя (без учета предвычислений на первом этапе):

$$\tau(s,\varepsilon) = O\left((2^s l_1 r + l_0^2)ts\right) \quad (17)$$

элементарных операций. При этом для выполнения алгоритма требуется

$$\lambda(s,\varepsilon) = ri_t \quad (18)$$

знаков гаммы, где i_t – наибольший элемент множества I.

Доказательство. Первое утверждение теоремы следует непосредственно из соотношений (10), (16), а последнее – из описания алгоритма. Наконец, поскольку для нахождения векторов $\hat{y}_i$ ($i \in I$) требуется $O(2^s ts l_1 r)$ элементарных операций, а для решения СЛУ (7) методом Гаусса – $O(l_0^2 ts)$ операций, то трудоемкость алгоритма составляет $O\left((2^s l_1 r + l_0^2)ts\right)$ элементарных операций.

Следствие. Пусть в условиях теоремы $l_0 = O(s)$, $l_1 = O(s)$ при $s \to \infty$,

$$t = \left\lceil (l_0 + C)s^{-1}\right\rceil \quad (19)$$

где $C \ge 0$. Тогда асимптотическая трудоемкость алгоритма при $s \to \infty$ и $\varepsilon \to 0$ составляет $O\left(2^s s^4 \varepsilon^{-2}\right)$ элементарных операций.

Остановимся подробнее на процедуре построения множества I, выполняемой на первом этапе алгоритма. Напомним, что это множество состоит из неотрицательных целых чисел $i_1, i_2, \ldots, i_t$, для которых выполняются соотношения (4) и (5), причем, согласно последнему из них, t должно быть не меньше чем $\lceil l_0 s^{-1} \rceil$.

Назовем число $i = 0, 1, \ldots$ *допустимым*, если $\mathrm{rank}(B_i) = n$, и *недопустимым* – в противном случае.

Из равенства $B_i = PL^i B$, $i = 0, 1, \ldots$, следует, что если $N \le l_1$ и $\mathrm{rank}(B) = N$, то каждое значение $i = 0, 1, \ldots$ является допустимым и можно положить $I = \{0, 1, \ldots, t-1\}$, выбирая в качестве t наименьшее натуральное число, для которого выполняется равенство (5). Если же $n \le l_1 < N$, то не все значения i допустимы, и процедура построения множества I может оказаться слишком трудоемкой. Вместе с тем, как показывает следующее утверждение, во многих практически важных случаях "удельный вес" недопустимых значений невелик.

Утверждение. Пусть L – полноцикловое линейное преобразование над полем F, $n < l_1 < N$ и $\mathrm{rank}(B) = l_1$. Тогда вероятность того, что выбранное случайно и равновероятно из множества $\overline{0, 2^N - 1}$ число i является недопустимым, меньше чем $2^{-(l_1 - n)}$

Доказательство. Обозначим $J = \{i \in \overline{0, 2^N - 1} : \mathrm{rank}(PL^i B) < n\}$ – совокупность всех недопустимых чисел из множества $\overline{0, 2^N - 1}$; U – подпространство векторного пространства V_n, порожденное строками матрицы P; W – подпространство, дуальное к векторному пространству, порожденному столбцами матрицы B. Из данных определений следует, что

$$i \in J \Leftrightarrow (\exists\, x \in V_n \setminus \{0\} : xPL^i B = 0) \Leftrightarrow L^i(U) \cap W \ne \{0\}.$$

Рассмотрим таблицу, состоящую из $2^n - 1$ строк, пронумерованных векторами $u \in U \setminus \{0\}$, и $2^{N - l_1} - 1$ столбцов, пронумерованных векторами $w \in W \setminus \{0\}$, содержащую на пересечении произвольной строки u и произвольного столбца w единственное число $i(u, w) \in \overline{0, 2^N - 1}$ такое, что $uL^{i(u,w)} = w$. Ясно, что эта таблица – латинский прямоугольник, а $|J|$ – число различных элементов в ней. Следовательно, $|J| \le (2^n - 1)(2^{N - l_1} - 1) < 2^{N - l_1 + n}$ и, значит, $2^N |J| < 2^{-(l_1 - n)}$.

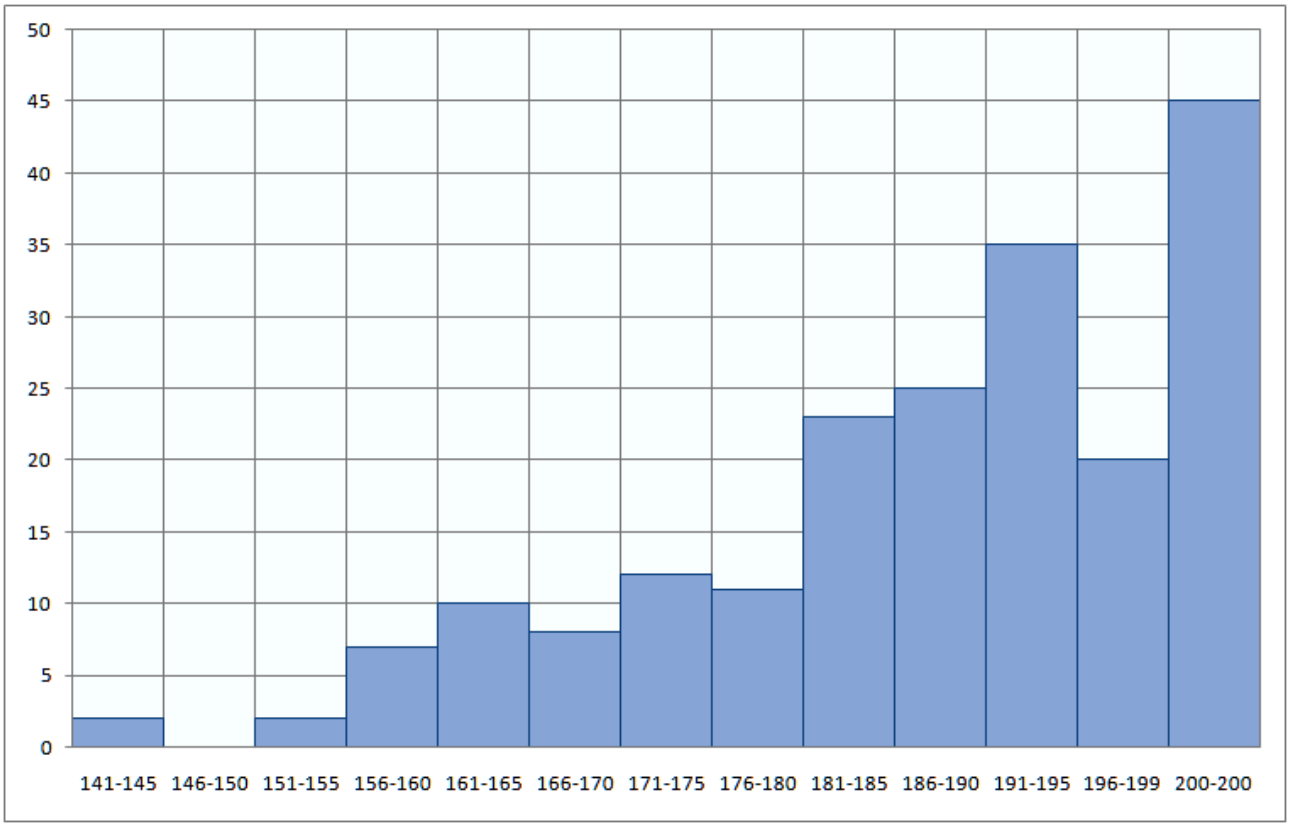
Утверждение доказано.

Численные расчеты и вычислительные эксперименты

Для того чтобы получить численные значения параметров, характеризующих эффективность предложенной атаки, и оценить возможность ее применения на практике, был проведен ряд вычислительных экспериментов. Ниже (рис. 1, табл. 1) приведены типичные результаты, полученные в ходе таких экспериментов при следующих значениях исходных параметров: длина начального состояния генератора $N = 128$; длина ключа $l_0 = 128$; число неизвестных функции усложнения $n = 64$. Для задания линейной функции переходов (матрицы L) использовался примитивный над полем F полином $x^{128} \oplus x^{95} \oplus x^{57} \oplus x^{45} \oplus x^{38} \oplus x^{36} + 1$, а для задания существенных переменных функции усложнения (матрицы P) – фиксированный набор чисел $1 \le \mu_1 < \ldots < \mu_n \le N$.

Данные на рисунке получены в результате 200 независимых испытаний, в j-м из которых генерировалась случайная равновероятная 128×64-матрица B и подсчитывалось значе-

ние случайной величины $\nu_j = \#\{i \in \overline{0,199} : \mathrm{rank}(B_i) = n\}$. Для каждого интервала $[u, v]$ на рисунке показано количество тех значений $j \in \overline{1,200}$, для которых $u \le \nu_j \le v$.



Эмпирическое распределение числа допустимых значений в интервале $[0,199]$

Полученные результаты свидетельствуют о том, что для случайно сгенерированных матриц B допустимые числа появляются достаточно часто. Например, в 35 из 200 проведенных испытаний количество допустимых чисел $i \in \overline{0,199}$ составляет от 191 до 195. Эффект "полного ранга" (когда все значения i допустимы или, что то же самое, все матрицы B_i имеют ранг n) наблюдается примерно в 25 % случаев (45 из 200).

В табл. 1 приведены результаты экспериментальной проверки условия 2 и оценки объема материала (количества знаков гаммы при фиксированных значениях ключа и вектора инициализации), необходимого для проведения атаки. Данные получены в результате 100 независимых испытаний, в каждом из которых генерировался случайный набор, состоящий из независимых равновероятных матриц A, B, M соответствующего размера, и формировалось множество I наименьшей мощности t, удовлетворяющее условию 2. В таблице указаны следующие параметры: t^* – значение числа t с наибольшей частотой встречаемости (среди 100 проведенных испытаний); $i_{\min}$, $i_{\max}$ и $i_{\text{ñð}}$ – соответственно наименьшее, наибольшее и среднее значение параметра i_t (наибольшего элемента множества I) при $t = t^*$. Отметим, что именно от последнего параметра зависит объем материала, необходимого для проведения атаки (см. формулу (18)).

Таблица 1

Результаты экспериментальной оценки необходимого объема материала при фиксированных значениях ключа и вектора инициализации

s	l_1	Параметр	Объем материала		
2	64	t^*	64	64	64
		$i_{\min}$	64	64	64
		$i_{\max}$	117	100	118
		$i_{\text{ñð}}$	76	74	76
10	80	t^*	13	13	13
		$i_{\min}$	13	13	13
		$i_{\max}$	33	32	38
		$i_{\text{ñð}}$	18	17	18
20	120	t^*	8	8	8
		$i_{\min}$	11	11	11
		$i_{\max}$	11	11	11
		$i_{\text{ñð}}$	11	11	11

Как видно из таблицы, при случайном независимом и равновероятном выборе матриц A, B, M среднее количество знаков гаммы при каждом запуске генератора, необходимое для проведения атаки, практически не зависит от длины вектора инициализации и колеблется от 11 до 76 в зависимости от числа s неизвестных функции φ (см. условие 1). При этом мощность множества I равна примерно $\lceil l_0 s^{-1} \rceil$.

В табл. 2, 3 показаны численные значения параметров (16) и (17), рассчитанные с использованием данных табл. 1 при $\delta = 0.01$ и $l_0 = 128$ соответственно. Как видно из таблиц, при $\varepsilon \geq 0{,}05$ и $s \leq 10$ предложенная атака позволяет восстанавливать ключ со сложностью 2^{38} (или менее) элементарных операций, используя не более 2^{15} отрезков гаммы (длины не более 117 знаков каждый) вместе с соответствующими им векторами инициализации.

Таблица 2

Количество векторов инициализации, достаточное для восстановления ключа с надежностью не менее 99 %

Параметры			r
ε	s	t^*	
0,05	2	64	2^{14}
	10	13	2^{15}
	20	8	2^{16}
0,10	2	64	2^{12}
	10	13	2^{13}
	20	8	2^{14}
0,30	2	64	2^{9}
	10	13	2^{10}
	20	8	2^{10}

Таблица 3

Численные оценки трудоемкости предложенной атаки

Параметры				$\tau(s,\varepsilon)$
l_1	s	t^*	r	
64	2	64	2^{14}	2^{29}
	10	13	2^{15}	2^{38}
	20	8	2^{16}	2^{49}
80	2	64	2^{12}	2^{28}
	10	13	2^{13}	2^{36}
	20	8	2^{14}	2^{47}
120	2	64	2^{9}	2^{25}
	10	13	2^{10}	2^{34}
	20	8	2^{10}	2^{45}

Выводы

Описана атака на генератор гаммы с линейным законом реинициализации начального состояния и функцией усложнения от n переменных, находящейся на расстоянии не более $2^{n-1}(1-\varepsilon)$ от множества s-мерных булевых функций ($\varepsilon \in (0,1)$, $1 \le s < n$). В отличие от ранее известных [2, 4, 5], предложенная атака применима к более широкому классу генераторов гаммы, при менее жестких ограничениях относительно их функций усложнения. Трудоемкость атаки зависит квадратично от параметра ε^{-1} и экспоненциально от параметра s (см. формулы (16), (17)).

Как показывают численные расчеты, при $\varepsilon \ge 0{,}05$ и $s \le 10$ предложенная атака позволяет восстанавливать ключ длины $l_0 = 128$ *бит* со сложностью не более 2^{38} элементарных операций, используя не более 2^{15} отрезков гаммы (длины не более 117 знаков каждый) вместе с соответствующими им векторами инициализации.

Моделирование атаки для проверки полученных теоретических выводов составляет задачу дальнейших исследований.

Список литературы: 1. *eStream* – the ECRYPT stream cipher project / http://www.ecrypt.eu.org/stream. 2. *Daemen J.* Resynchronization weaknesses in synchronous stream ciphers / J. Daemen, R. Govaerts, J. Vandewalle // Advances in Cryptology – EUROCRYPT'93, Proceedings. Berlin. Springer-Verlag, 1993. – P. 159–167. 3. *Borissov Y.* On a resynchronization weakness in a class of combiners with memmory / Y. Borissov, S. Nikova, B. Preneel, J. Vandewalle // The 3rd Conf. on Security in Communication Networks, Proceedings. Berlin. Springer-Verlag, 2003. – P. 165–177. 4. *Golić J.* On the resynchronization attack / J. Golić, G. Morgari // Fast Software Encryption. – FSE'03, Proceedings. Berlin. Springer-Verlag, 2003. – P. 100–110. 5. *Armknecht F.* Extending the resynchronization attack / F. Armknecht, J. Lano, B. Preneel // Selected Areas in Cryptography – SAC'04, Proceedings. Berlin. Springer-Verlag. 2004. – P. 19–38. 6. *Yang W.* A resynchronization attack on stream ciphers filtered by Maiorana-McFarland functions / W. yang, Y. Hu // Front. Comput. Sci. China, 2011. – Vol. 5(2). – P. 158 – 162. 7. *Алексеев Е.К.* Об атаке на фильтрующий генератор с функцией усложнения, близкой к алгебраически вырожденной / Е.К. Алексеев // Сборник статей молодых ученых факультета МВК МГУ, 2011. – Вып. 8. – С. 114–123. 8. *Ширяев А.Н.* Вероятность : учеб. пособие для вузов / А.Н. Ширяев. – М. : Наука, 1989. – 640 с.

Харьковский национальный университет радиоэлектроники

Поступила в редколлегию 20.12.2013