Одарченко Роман Сергійович, кандидат технічних наук, доцент кафедри телекомунікаційних систем, Національний авіаційний університет.
E-mail: odarchenko.r.s@mail.ru.
Одарченко Роман Сергеевич, кандидат технических наук, доцент, доцент кафедры телекоммуникационных систем, Национальный авиационный университет.
Odarchenko Roman, PhD, Associate Professor of Telecommunications systems Academic Department, National Aviation University.

Гнатюк Сергій Олександрович, кандидат технічних наук, доцень, доцент кафедри безпеки інформаційних технологій, Національний авіаційний університет.
E-mail: s.gnatyuk@nau.edu.ua.
Гнатюк Сергей Александрович, кандидат технических наук, доцент, доцент кафедры безопасности информационных технологий, Национальный авиационный университет.
Gnatyuk Sergiy, PhD, Associate Professor of IT-Security Academic Department, National Aviation University.

УДК 621.391:519.2

ОБОБЩЕННАЯ СТАТИСТИЧЕСКАЯ АТАКА НА СИНХРОННЫЕ ПОТОЧНЫЕ ШИФРЫ

Антон Алексейчук, Сергей Конюшок, Артем Сторожук

В настоящее время наиболее мощными атаками на синхронные поточные шифры являются атаки на основе подобранных векторов инициализации. К ним относятся кубическая атака Динура-Шамира, статистическая атака Фишера-Хазаи-Майера (FKM), а также их различные модификации и усовершенствования. Атака FKM строится на основе статистических приближений булевых функций, связанных с алгоритмами шифрования, функциями, зависящими лишь от некоторых разрядов ключа. Разработчиками атаки предложен способ нахождения указанных приближений, однако не дано теоретического обоснования эффективности этого способа. Кроме того, остается открытым вопрос о том, можно ли повысить эффективность атаки FKM, выбирая приближения из более широкого класса булевых функций. В настоящей статье предлагается атака на синхронные поточные шифры, обобщающая как кубическую атаку, так и атаку FKM. Эта атака базируется на алгебраически вырожденных приближениях булевых функций, что предоставляет больше возможностей для реализации основной идеи атаки FKM. Предложен полиномиальный вероятностный алгоритм построения указанных приближений по известным подпространствам, допустимым для заданной булевой функции. Показано, что, выбирая определенным образом параметры этого алгоритма, можно строить атаки на синхронные поточные шифры, заметно более эффективные по сравнению с полным перебором ключей.

Ключевые слова: *поточный шифр, нелинейный криптоанализ, атака на основе подобранных векторов инициализации, алгебраически вырожденная булева функция, нахождение приближений булевых функций.*

Введение. В настоящее время наиболее мощными атаками на синхронные поточные шифры (СПШ) являются атаки на основе подобранных векторов инциализации (ВИ). К ним относятся кубическая атака [10], статистическая атака FKM [13], а также их различные модификации и усовершенствования [6–9, 11, 12]. В принципе, подобные атаки применимы к любому криптографическому алгоритму, который может быть описан с помощью булевой функции $F:\{0,1\}^{l_0}\times\{0,1\}^{l_1}\to\{0,1\}$, один из аргументов которой является секретным, а другой – общедоступным параметром. В случае СПШ в качестве F можно взять (рассматриваемый как функция ключа $k\in\{0,1\}^{l_0}$ и вектора инициализации $c\in\{0,1\}^{l_1}$) знак выходной последовательности генератора гаммы шифра в некотором такте. Предполагается, что функция F доступна противнику в виде оракула («черного ящика»), в частности, алгоритм, реализующий эту функцию, может быть не известен.

На этапе предвычислений противник может подавать на вход оракула любые пары векторов $(x,y)\in\{0,1\}^{l_0}\times\{0,1\}^{l_1}$, вычисляя значения $F(x,y)$, чтобы собрать нужную информацию о свойствах функциии F. Затем противник получает доступ к оракулу $F_k(c)=F(k,c)$, $c\in\{0,1\}^{l_1}$, где значение ключа $k\in\{0,1\}^{l_0}$ не известно. Противник может выбирать любые векторы $c\in\{0,1\}^{l_1}$ и вычислять значения $F_k(c)$ при фиксированном ключе k, стремясь восстановить этот ключ (или получить о нем некоторую информацию). Другой возможной стратегией противника является построение различающей атаки, направленной на то, чтобы статистически отличить (за приемлемое время с достаточно

высокой надежностью) отображение F_k от случайного равновероятного отображения $\Phi : \{0,1\}^{l_1} \to \{0,1\}$ [6, 7].

Атака FKM [13] строится на основе статистического приближения функции F булевой функцией g, зависящей лишь от некоторых разрядов ключа. Это позволяет сначала восстановить указанные разряды методом максимума правдоподобия, а затем найти оставшуюся часть ключа путем полного перебора. В [13] указаны способы выбора функций F и g для построения атаки, однако не дано теоретического обоснования эффективности этих способов. Кроме того, остается открытым вопрос о том, можно ли повысить эффективность атаки, описанной в [13], выбирая приближения функции F из более широкого класса булевых функций.

В настоящей статье предлагается статистическая атака на СПШ, обобщающая атаку FKM, а также кубическую атаку. Эта атака базируется на прибжении булевых функций алгебраически вырожденными функциями [1]. В п. 1 приведены подробное описание и оценка трудоемкости предложенной атаки; получен также ряд результатов, дополняющих и уточняющих отдельные результаты статьи [13]. В п. 2 описан полиномиальный вероятностный алгоритм построения (в некотором смысле сколь угодно близких к наилучшим возможным) приближений функции F по известному допустимому для F подпространству. Показано, что выбирая определенным образом параметры этого алгоритма, можно строить атаки на СПШ, заметно более эффективные по сравнению с полным перебором ключей. Наконец, в п. 3 сформулированы краткие выводы.

1. Статистическая атака на СПШ на основе алгебраически вырожденных приближений булевых функций

Ниже используются следующие обозначения: V_n – множество двоичных векторов длины n, $\mathbf{F}_2^{m\times n}$ – множество матриц размера $m\times n$ над полем $\mathbf{F}_2 = \{0,1\}$.

Рассмотрим синхронный поточный шифр, состоящий из генератора гаммы и алгоритма формирования начального состояния генератора по ключу и вектору инициализации. Генератор гаммы представляет собой конечный автономный автомат с множеством состояний V_N, функцией переходов $h : V_N \to V_N$ и функцией выходов $f : V_N \to \{0,1\}$, а алгоритм формирования начального состояния задается отображением $H : V_{l_0} \times V_{l_1} \to V_N$, где l_0 – длина ключа, l_1 – длина ВИ. Знак гаммы в i-м такте, соответствующий ключу $k \in V_{l_0}$ и ВИ $c \in V_{l_1}$, определяется по формуле

$$\gamma_i(k,c) = f(h^i(H(k,c))), \qquad (1)$$

где h^i – i-я степень отображения h относительно операции композиции, $i = 0, 1, \ldots$.

Предлагаемая атака на СПШ относится к классу атак на основе подобранных ВИ: предполагается, что противник может по своему усмотрению выбирать векторы инициализации и вычислять при фиксированном, но неизвестном ему ключе соответствующие им знаки гаммы, стремясь при этом восстановить искомый ключ. Предполагается также, что противник обладает алгоритмом $\mathcal{A}$ опробования ключей, позволяющим безошибочно находить истинный ключ, если он содержится среди перебираемых ключей (другими словами, алгоритм полного перебора ключей характеризуется стопроцентной надежностью).

Для проведения атаки противник выбирает тем или иным способом функции-оракулы $F : V_{l_0} \times V_{l_1} \to \{0,1\}$, $\varphi : V_{s+l_1} \to \{0,1\}$ и матрицу $M_0 \in \mathbf{F}_2^{l_0\times s}$ ранга $s < l_0$, удовлетворяющие следующим условиям:

а) существует эффективный алгоритм вычисления значений $F_k(c) = F(k,c)$, $c \in V_{l_1}$, каким бы ни был неизвестный фиксированный ключ $k \in V_{l_0}$;

б) справедливо неравенство

$$\mathbf{P}_{k,c}\{F(k,c) = \varphi(kM_0, c)\} \geq 1 - \vartheta, \qquad (2)$$

где k и c – независимые случайные векторы, первый из которых распределен равномерно на множестве V_{l_0}, а второй – в соответствии с некоторым (не обязательно равномерным) законом $\mathbf{P}_c$ на множестве V_{l_1}, $\vartheta \in (0, 1/2)$.

Отметим, что в качестве функции F, удовлетворяющей условию а), можно взять отображение γ_i, ставящее в соотвествие паре $(k,c) \in V_{l_0} \times V_{l_1}$ знак гаммы (1) в некотором фиксированном такте $i = 0, 1, \ldots$. Можно также положить $F_k(c)$ равным значению производной отображения γ_i по направлению некоторого подпространства $L \subseteq V_{l_1}$ (небольшой размерности):

$$F_k(c) = \bigoplus_{u \in L} \gamma_i(k, c \oplus u),\ (k,c) \in V_{l_0} \times V_{l_1}. \quad (3)$$

Если $u_1, \dots, u_l$ – произвольный базис подпространства L, то значение в правой части равенства (3) равно $D_{u_l} \cdots D_{u_1} \gamma_i(k, c)$, где $D_u g(x) = g(x \oplus u) \oplus g(x)$, $x \in V_m$ – производная функции $g : V_m \to \{0,1\}$ по направлению u (см., например, [4], с. 89). В частности, выбирая в качестве L подпространство, порожденное векторами $e_{j_1}, \dots, e_{j_l}$, где $1 \le j_1 < \dots < j_l \le l_1$ (а e_j обозначает двоичный вектор длины l_1, все координаты которого, за исключением j-й, равны нулю, $j \in \overline{1, l_1}$), можно задать функцию F_k по формуле:

$$F_k(c) = D_{j_1} \cdots D_{j_l} \gamma_i(k, c),\ (k,c) \in V_{l_0} \times V_{l_1}. \quad (4)$$

Именно такой способ задания указанных функций используется в [13], причем параметр l, характеризующий сложность вычисления их значений, обычно не превосходит 20.

Опишем теперь алгоритм восстановления ключа рассматриваемого СПШ при выполнении условий а) и б), который базируется на идеях работ [13] и [2].

Алгоритм 1.

Исходные данные:

– алгоритм $\mathcal{A}$ опробования ключей, обладающий стопроцентной надежностью;

– функции F_k и φ, заданные с помощью оракулов (где k – неизвестный ключ);

– матрица M_0.

Параметр: $r \in \mathbf{N}$.

Этап 1 (*восстановление вектора kM_0 методом максимума правдоподобия*):

– сгенерировать независимые случайные ВИ $c^{(1)}, \dots, c^{(r)}$, распределенные на множестве V_{l_1} по закону $\mathbf{P}_c$;

– для каждого $y \in V_s$ вычислить значение $\nu(y) = \sum_{j=1}^{r} (\varphi(y, c^{(j)}) \oplus F_k(c^{(j)}))$ и найти вектор $\hat{y} \in V_s$ такой, что $\nu(\hat{y}) = \min_{y \in V_s} \nu(y)$.

Этап 2 (*восстановление ключа*). Перебирая все решения $\tilde{k} \in V_{l_0}$ системы линейных уравнений

$$\tilde{k} M_0 = \hat{y}, \quad (5)$$

найти искомый ключ с помощью алгоритма $\mathcal{A}$.

Обозначим $T_{\mathcal{A}}$ временную сложность алгоритма $\mathcal{A}$, T_F и T_φ – временные сложности вычисления значений функций F и φ соответственно. Тогда временная сложность первого этапа алгоритма 1 составляет $O\left(2^s r (T_F + T_\phi)\right)$ операций. Далее, поскольку $rank(M_0) = s$, то система уравнений (5) имеет $2^{l_0 - s}$ решений, перебор которых с целью нахождения ключа k потребует $O\left(s(l_0 - s) 2^{l_0 - s} T_{\mathcal{A}}\right)$ операций. Таким образом, временная сложность алгоритма 1 составляет

$$T(l_0, s, r) = O\left(2^s r (T_F + T_\varphi) + s(l_0 - s) 2^{l_0 - s} T_{\mathcal{A}}\right) \quad (6)$$

операций.

Для того, чтобы оценить объем материала r, при котором алгоритм 1 позволяет находить ключи с заданной достоверностью, сделаем одно дополнительное предположение.

Зафиксируем число $\varepsilon \in (0,1)$. Назовем ключ $k \in V_{l_0}$ ε*-слабым* (*относительно описанной атаки*), если $\mathbf{P}_c\{F_k(c) = \varphi(kM_0, c)\} \ge 1/2(1+\varepsilon)$ и предположим, что, наряду с условиями а), б), выполняется следующее условие:

в) для любого ε-слабого ключа $k \in V_{l_0}$ и произвольного вектора $y \in V_s \setminus \{kM_0\}$ справедливо равенство

$$\mathbf{P}_c\{F_k(c) = \varphi(y, c)\} = 1/2. \quad (7)$$

Следующая лемма доказывается аналогично лемме в статье [2].

Лемма 1. Пусть k – ε-слабый ключ, $\varepsilon \in (0,1)$. Тогда при выполнении условий б), в) вероятность правильного восстановления вектора kM_0 на первом этапе алгоритма 1 ограничена снизу величиной $1 - 2^s \exp\{-1/8 \cdot r\, \varepsilon^2\}$.

Лемма 2. При выполнении условия б) для любого $\varepsilon \in (0,1)$ существует не менее $2^{l_0}\left(1 - \frac{2\vartheta}{1-\varepsilon}\right)$ ε-слабых ключей.

Доказательство. Обозначим $p_k = \mathbf{P}_c\{F_k(c) = \varphi(kM_0, c)\}$, $k \in V_{l_0}$. Тогда вероятность в левой части равенства (2) равна $2^{-l_0} \sum_{k \in V_{l_0}} p_k \ge 1 - \vartheta$. При этом ключ k не является ε-слабым тогда и только тогда, когда $p_k < 1/2(1+\varepsilon)$. Следовательно, вероятность того,

что случайно равновероятно выбранный ключ не окажется ε-слабым равна

$$\mathrm{P}_k\{p_k < 1/2(1+\varepsilon)\} = \mathrm{P}_k\{1-p_k > 1/2(1-\varepsilon)\} \le \frac{2}{1-\varepsilon} 2^{-l_0} \sum_{k \in V_{l_0}} (1-p_k) \le \frac{2\vartheta}{1-\varepsilon}.$$

Отсюда находим оценку числа ε-слабых ключей:

$$2^{l_0}(1-\mathbf{P}_k\{p_k < 1/2(1+\varepsilon)\}) \ge 2^{l_0}\left(1-\frac{2\vartheta}{1-\varepsilon}\right).$$

Лемма доказана.

На основании лемм 1 и 2 справедлива следующая теорема, позволяющая оценить эффективность алгоритма 1.

Теорема 1. Пусть выполняются условия а), б), в) при $\vartheta = 1/2 - 2^{-\mu}$, $\varepsilon = (2^{\mu}-1)^{-1}$, где $\mu \ge 2$. Положим $r = \left\lceil 2^{2\mu+3} \ln (2^s \delta^{-1}) \right\rceil$, $\delta \in (0,1)$. Тогда существует не менее $2^{l_0-\mu}$ ε-слабых ключей, каждый из которых может быть восстановлен с помощью алгоритма 1 с вероятностью не менее $1-\delta$ за время, определяемое по формуле (6).

Изложенные выше результаты допускают естественное обобщение на случай, когда φ является случайной булевой функцией, удовлетворяющей условию б) с некоторой положительной вероятностью, например, задается с помощью вероятностного алгоритма (см. ниже п. 2). В этом случае имеет место следующая теорема.

Теорема 2. Пусть $\vartheta = 1/2 - 2^{-\mu}$, $\varepsilon = (2^{\mu}-1)^{-1}$, где $\mu \ge 2$, и функция φ выбирается случайно (независимо от векторов k и c) в соответствии с некоторым распределением вероятностей $\mathbf{P}_{\varphi}$ на множестве булевых функций от $s+l_1$ переменных. Обозначим Φ_{ϑ} множество всех функций $\varphi : V_{s+l_1} \to \{0,1\}$, удовлетворяющих условию б), и предположим, что $\mathrm{P}_{\phi}(\Phi_{\vartheta}) \ge 1-\delta/2$, где $\delta \in (0,1)$. Предположим также, что для любой функции $\varphi \in \Phi_{\vartheta}$ выполняется условие в). Положим, наконец, $r = \left\lceil 2^{2\mu+3} \ln (2^{s+1} \delta^{-1}) \right\rceil$, $\delta \in (0,1)$. Тогда существует не менее $2^{l_0-\mu}$ ε-слабых ключей, каждый из которых может быть восстановлен с помощью алгоритма 1 с вероятностью не менее $1-\delta$ за время, определяемое по формуле (6).

Доказательство. Если некоторый ε-слабый ключ восстановлен неверно, то либо $\varphi \notin \Phi_{\vartheta}$, либо алгоритм 1 совершает ошибку при применении к входным данным с фиксированной функцией $\varphi \in \Phi_{\vartheta}$. Согласно сделанным предположениям и теореме 1, вероятность каждого из указанных событий не превосходит $\delta/2$. Следовательно, вероятность ошибки при восстановлении любого ε-слабого ключа не превосходит δ. Теорема доказана.

Отметим следующие отличия изложенных выше результатов от результатов работы [13]:

– предложена статистическая атака на СПШ, основанная на применении существенно более широкого класса приближений функции F (а именно, алгебраически вырожденных функций вида $\varphi(kM_0, c)$, $k \in V_{l_0}$, $c \in V_{l_1}$);

– охарактеризован класс ключей (ε-слабые ключи), которые могут быть восстановлены с помощью описанной атаки, и получена нижняя оценка количества ключей в этом классе;

– приведено явное выражение трудоемкости атаки как функции ее надежности, сложности вычисления значений функций-оракулов и алгоритма опробования ключей.

Отметим также, что в случае, когда функция F_k определяется по формуле (4), функция φ является аффинной, а параметр ϑ в формуле (2) равен нулю, описанная статистическая атака сводится к алгебраической (кубической) атаке, предложенной в [10].

2. Вероятностный алгоритм построения алгебраически вырожденных приближений булевой функции по известному допустимому подпространству

Пусть $F : V_n \to \{0,1\}$ – булева функция, заданная с помощью оракула, H – m-мерное подпространство векторного пространства V_n, $1 \le m \le n-1$, M – $n \times m$-матрица, столбцы которой образуют канонический базис пространства H (см., например, [5], с. 219).

Обозначим $B_{n,m}(H)$ множество всех функций вида $g(x) = \psi(xM)$, $x \in V_n$, где $\psi : V_m \to \{0,1\}$. Для любого $g \in B_{n,m}(H)$ обозначим $d(F,g) = 2^{-n} |\{x \in V_n : F(x) \ne g(x)\}|$ относительное расстояние между функциями F и g.

Предположим, что H является θ-*допустимым подпространством* для функции F, $\theta \in (0,1)$, то есть удовлетворяет следующему условию [1]:

$$d_F(B_{n,m}(H)) \stackrel{\text{def}}{=} \min_{g \in B_{n,m}(H)} d(F,g) \le 1/2 \cdot (1-\theta). \quad (8)$$

Требуется разработать вероятностный алгоритм, позволяющий для любого достаточно малого $\tau > 0$ эффективно вычислять значения функции $\psi : V_m \to \{0,1\}$, для которой относительное расстояние между функциями $g(x) = \psi(xM)$, $x \in V_n$ и F не превосходит $1/2 \cdot (1-\theta) + \tau$. Ниже показано как применить этот алгоритм для задания функции $\phi : V_{s+l_1} \to \{0,1\}$ и матрицы $M_0 \in \mathrm{F}_2^{l_0 \times s}$, необходимых для выполнения атаки, описанной в п. 1.

Предлагаемый алгоритм имеет следующий вид.

Алгоритм 2.

Исходные данные:

– функция $F : V_n \to \{0,1\}$, заданная с помощью оракула;

– $n \times m$-матрица M, столбцы которой образуют канонический базис θ-допустимого для функции F подпространства H, $1 \le m \le n-1$;

– число $\tau \in (0, 4\theta)$.

1. Положить $t = \left\lceil 32\tau^{-2} \ln(8\tau^{-1}) \right\rceil$.

2. Для вычисления значения функции ψ в точке $y \in V_m$ сгенерировать независимые случайные векторы $\xi_{1,y}, \ldots, \xi_{t,y}$ с равномерным распределением на множестве $L_y = \{x \in V_n : xM = y\}$ и положить

$$\psi(y) = \operatorname{sgn}\left(\sum_{i=1}^{t} (-1)^{F(\xi_{i,y})} \right), \qquad (9)$$

где $\operatorname{sgn}(x) = 0$, если $x \ge 0$, $\operatorname{sgn}(x) = 1$ – в противном случае, $x \in \mathbf{R}$.

Подчеркнем, что случайные векторы $\xi_{i,y}$, $i \in \overline{1,t}$, $y \in V_m$, используемые для вычисления значений функции ψ во всех точках ее области определения, являются независимыми в совокупности.

Для оценки эффективности алгоритма 2 воспользуемся следующей леммой.

Лемма 3 [14]**.** Пусть $\zeta_1, \ldots, \zeta_t$ – независимые случайные величины такие, что $\alpha_j \le \zeta_j \le \beta_j$, $\alpha_j, \beta_j \in \mathbf{R}$, $j \in \overline{1,t}$. Тогда для любого $x > 0$

$$\mathrm{P}\left\{ t^{-1} \sum_{l=1}^{t} \zeta_l - \mathrm{E}\left(t^{-1} \sum_{l=1}^{t} \zeta_l \right) \ge x \right\} \le \exp\left\{ - \frac{2t^2 x^2}{\sum_{l=1}^{t} (\beta_l - \alpha_l)^2} \right\}.$$

Обозначим $\mathbf{P}$ совместное распределение вероятностей случайных векторов $\xi_{i,y}$, $i \in \overline{1,t}$, $y \in V_m$.

Теорема 3. Случайная функция $g(x) = \psi(xM)$, $x \in V_n$ удовлетворяет следующему неравенству:

$$\mathbf{P}\{ d(F,g) \le 1/2 \cdot (1-\theta) + \tau \} \ge 1 - \exp\{ -2^{m-1} \tau^2 \}. \qquad (10)$$

При этом временная сложность вычисления значения (9) составляет

$$T_\psi = O(T_F m (n-m) t) \qquad (11)$$

операций, где T_F – временная сложность вычисления значения функции F.

Доказательство. Прежде всего, убедимся в справедливости неравенства

$$\mathbf{E}\, d(F,g) \le 1/2 \cdot (1-\theta) + 1/2 \cdot \tau. \qquad (12)$$

Обозначим $g^*(x) = \psi^*(xM)$, $x \in V_n$ функцию, ближайшую во множестве $B_{n,m}(H)$ к функции F. На основании леммы 3 в [1] справедливы следующие соотношения:

$$1 - 2d(F,g) = 2^{-m} \sum_{y \in V_m} (-1)^{\psi(y) \oplus \psi^*(y)} u_y,$$

$$1 - 2d(F,g^*) = 2^{-m} \sum_{z \in V_y} u_y,$$

$$(-1)^{\psi^*(y)} u_y = 2^{-(n-m)} \sum_{x \in L_y} (-1)^{f(x)}, \; y \in V_m,$$

где

$$u_y = 2^{-(n-m)} \left| \sum_{x \in L_y} (-1)^{f(x)} \right|, \; y \in V_m.$$

Отсюда вытекает, что

$$d(F,g) - d(F,g^*) = 2^{-m} \sum_{y \in V_m} u_y I\{ \psi(y) \ne \psi^*(y) \}, \qquad (13)$$

$$\mathbf{E}\left(t^{-1} \sum_{i=1}^{t} (-1)^{F(\xi_{i,y})} \right) = (-1)^{\psi^*(y)} u_y, \; y \in V_m. \qquad (14)$$

Положим $\delta = \tau/4$. Из формулы (13) следует, что

$$\mathbf{E}\left(d(F,g) - d(F,g^*) \right) = 2^{-m} \sum_{y \in V_m} u_y \mathbf{P}\{ \psi(y) \ne \psi^*(y) \} \le 2^{-m} \sum_{\substack{y \in V_m: \\ u_y < \delta}} u_y + 2^{-m} \sum_{\substack{y \in V_m: \\ u_y \ge \delta}} \mathbf{P}\{ \psi(y) \ne \psi^*(y) \}. \qquad (15)$$

Пусть теперь $u_y \ge \delta$ и $\psi(y) \ne \psi^*(y)$. Тогда на основании равенства (9) имеет место один из двух случаев:

1) $(-1)^{\psi^*(y)} u_y \ge \delta$, $\psi^*(y) = 0$, $t^{-1} \sum_{i=1}^{t} (-1)^{F(\xi_{i,y})} < 0$;

2) $(-1)^{\psi^*(y)} u_y \le -\delta$, $\psi^*(y) = 1$, $t^{-1} \sum_{i=1}^{t} (-1)^{F(\xi_{i,y})} \ge 0$,

причем в обоих случаях, согласно формуле (14), справедливо следующее неравенство:

$$\left| t^{-1} \sum_{i=1}^{t} (-1)^{F(\xi_{i,y})} - (-1)^{\psi^*(y)} u_y \right| = \left| t^{-1} \sum_{i=1}^{t} (-1)^{F(\xi_{i,y})} - \mathbf{E}\left(t^{-1} \sum_{i=1}^{t} (-1)^{F(\xi_{i,y})} \right) \right| \ge \delta .$$

Отсюда вытекает, что

$$2^{-m} \sum_{\substack{y \in V_m: \\ u_y \ge \delta}} \mathbf{P}\{\psi(y) \ne \psi^*(y)\} \le \mathbf{P}\left\{ \left| t^{-1} \sum_{i=1}^{t} (-1)^{F(\xi_{i,y})} - \mathbf{E}\left(t^{-1} \sum_{i=1}^{t} (-1)^{F(\xi_{i,y})} \right) \right| \ge \delta \right\} \le 2\exp\left\{-1/2 \cdot \delta^2 t\right\}, \qquad (17)$$

где последнее неравенство следует из условия независимости случайных векторов $\xi_{1,y}, \ldots, \xi_{t,y}$ и леммы 3.

Подставляя оценки (16), (17) в формулу (15) и используя соотношения $\delta = \tau/4$, $\tau \in (0, 4\theta)$, $t = \left\lceil 32\tau^{-2} \ln(8\tau^{-1}) \right\rceil$, после очевидных преобразований получим неравенство (12).

Заметим теперь, что согласно равенству (13) случайная величина $2^m (d(F,g) - d(F,g^*))$ является суммой 2^m независимых случайных величин, принимающих значения в промежутке $[0,1]$. Следовательно, на основании формулы (12) и леммы 3 справеливы соотношения

$$\mathbf{P}\{d(F,g) > 1/2 \cdot (1-\theta) + \tau\} = \mathbf{P}\{d(F,g) - \mathbf{E}\, d(F,g) > (1/2 \cdot (1-\theta) + \tau/2 - \mathbf{E}\, d(F,g)) + \tau/2\} \le$$

$$\le \mathbf{P}\{d(F,g) - \mathbf{E}\, d(F,g) > \tau/2\} = \mathbf{P}\{d(F,g) - d(F,g^*) - \mathbf{E}\,(d(F,g) - d(F,g^*)) > \tau/2\} \le$$

$$\le \exp\{-2 \cdot 2^m \cdot (\tau/2)^2\} = \exp\{-2^{m-1}\tau^2\},$$

из которых вытекает неравенство (10).

Наконец, справедливость формулы (11) следует непосредственно из описания алгоритма 2.

Теорема доказана.

Отметим, что для генерации независимых случайных векторов $\xi_{1,y}, \ldots, \xi_{t,y}$ с равномерным распределением на множестве $L_y = \{x \in V_n : xM = y\}$ на первом шаге алгоритма 2 целесообразно использовать особенности строения матрицы M (напомним, что ее столбцы образуют канонический базис порожденного ими подпространства). Пусть для простоты обозначений $M = \begin{pmatrix} I_m \\ B \end{pmatrix}$, где I_m – единичная матрица порядка m, $B \in \mathbf{F}_2^{(n-m)\times m}$. Тогда $L_y = \{(zB \oplus y, z) : z \in V_{n-m}\}$ и можно положить $\xi_{i,y} = (\eta_i B \oplus y, \eta_i)$, $i \in \overline{1,t}$, где $\eta_1, \ldots, \eta_t$ – независимые случайные равновероятные двоичные векторы длины $n-m$.

Вернемся к рассмотрению атаки на СПШ, описанной в п. 1. Напомним, что для успешного проведения этой атаки противнику необходимо задать функции $F : V_{l_0} \times V_{l_1} \to \{0,1\}$, $\phi : V_{s+l_1} \to \{0,1\}$ и матрицу $M_0 \in \mathbf{F}_2^{l_0 \times s}$ ранга $s < l_0$, удовлетворяющие условиям а), б) и в). Предположим, что противник выбрал функцию F (например, одним из способов, указанных в п. 1). Тогда, как показывает следующая теорема, для задания двух оставшихся объектов ему достаточно найти некоторое допустимое для F подпространство и воспользоваться алгоритмом 2.

Теорема 4. Пусть $F : V_n \to \{0,1\}$ – булева функция, удовлетворяющая условию а), где $n = l_0 + l_1$; $\delta, \theta \in (0,1)$, H – θ-допустимое для F подпространство, порожденное столбцами матрицы

$$M = \begin{pmatrix} M_0 & 0 \\ M_1 & M_2 \end{pmatrix}, \qquad (18)$$

где $M_0 \in \mathbf{F}_2^{l_0 \times s}$, $M_1 \in \mathbf{F}_2^{l_1 \times s}$, $M_2 \in \mathbf{F}_2^{l_1 \times (m-s)}$, $\operatorname{rank}(M_0) = s$, $\operatorname{rank}(M_2) = m - s$, $1 \le s < l_0$, $s \le m \le s + l_1$ и

$$m \ge \log(\theta^{-2} \ln(2\delta^{-1})) + 5. \qquad (19)$$

Предположим, что распределение вероятностей $\mathbf{P}_c$ случайного вектора c является равномерным на множестве V_{l_1}. Положим

$$\tau = \theta/4,\ \vartheta = 1/2 - \tau,\ \varepsilon = \theta(4-\theta)^{-1}, \qquad (20)$$

$$\varphi(z,c) = \psi(z \oplus cM_1, cM_2),\ z \in V_s,\ c \in V_{l_1}, \qquad (21)$$

где ψ – случайная функция, заданная с помощью алгоритма 2. Тогда случайная функция (21) удовлетворяет условию б) с вероятностью не менее $1-\delta/2$.

Предположим, наконец, что для указанного выше ε и любой реализации случайной функции (21), удовлетворяющей условию б), выполняется также условие в) и рассмотрим атаку на СПШ, состоящую в применении алгоритма 1 к входным данным $\mathcal{A}$, F_k, φ, M_0 с параметром

$$r = \left\lceil 128\,\theta^{-2} \ln\left(2^{s+1}\,\delta^{-1}\right) \right\rceil. \qquad (22)$$

Тогда существует по крайней мере $2^{l_0-2}\theta$ ε-слабых ключей СПШ, каждый из которых может быть восстановлен с помощью указанной атаки с вероятностью не менее $1-\delta$ за время

$$T(l_0, s, r) = O\left(2^s r T_F m(n-m)t + s(l_0 - s)2^{l_0 - s} T_{\mathcal{A}}\right). \qquad (23)$$

Доказательство. Справедливость теоремы следует непосредственно из теорем 2, 3 и соотношений (19) – (22).

В табл. 1 приведены численные значения параметра (23), рассчитанные для шифра Grain-128 ($l_0 = 128$, $l_1 = 96$) при $\delta = 0{,}1$, $T_F = 128$, $T_{\mathcal{A}} = 3 \cdot 128$ и различных значениях s, m и θ.

Как видно из таблицы, трудоемкость предложенной атаки практически не зависит от размерности m используемого подпространства (при условии, что $s \le m \le s + l_1$) и медленно растет с уменьшением параметра θ (то есть с увеличением расстояния между функцией F и множеством ее используемых приближений). Наименьшее значение трудоемкости достигается при $s = 52$ (напомним, что s обозначает длину вектора kM_0, который восстанавливается на первом этапе атаки) и составляет от 2^{99} до 2^{104} операций в зависимости от значения θ. При этом полный перебор ключей требует не менее $2^{l_0} = 2^{128}$ операций.

Подчеркнем, что для успешного применения предложенной атаки (со сложностью, указанной в табл. 1) необходимо предварительно найти θ-допустимое для функции F подпространство размерности m, порожденное столбцами матрицы вида (18). Для редуцированной версии шифра Grain-128, рассмотренной в [13], можно построить такое подпространство при $\theta = 0{,}586$, $s = 52$, $m = s + l_1$. Таким образом, при выполнении условия теоремы 4 существует атака на эту версию шифра со сложностью не более 2^{99} (отметим, что сложность атаки FKM на указанную версию Grain-128 составляет 2^{124} [13], пример 9).

Таблица 1

Оценка трудоемкости предложенной атаки

θ	s	$T(l_0, s, r)$	
		при $m = s + l_1$	при $m = s$
0,99	30	2^{119}	2^{119}
	40	2^{109}	2^{109}
	50	2^{99}	2^{99}
	60	2^{104}	2^{104}
	70	2^{114}	2^{114}
0,95	30	2^{119}	2^{119}
	40	2^{109}	2^{108}
	50	2^{99}	2^{99}
	60	2^{104}	2^{104}
	70	2^{115}	2^{115}
0,80	30	2^{119}	2^{119}
	40	2^{109}	2^{109}
	50	2^{99}	2^{99}
	60	2^{106}	2^{105}
	70	2^{116}	2^{116}
0,60	30	2^{119}	2^{119}
	40	2^{109}	2^{109}
	50	2^{99}	2^{99}
	60	2^{107}	2^{107}
	70	2^{117}	2^{118}
0,40	30	2^{119}	2^{119}
	40	2^{109}	2^{109}
	50	2^{100}	2^{100}
	60	2^{110}	2^{110}
	70	2^{120}	2^{120}
0,20	30	2^{119}	2^{119}
	40	2^{109}	2^{109}
	50	2^{104}	2^{104}
	60	2^{114}	2^{114}
	70	2^{124}	2^{124}

3. Заключительные замечания

Предложенная статистическая атака на СПШ обобщает известные ранее атаки [10, 13], предоставляя больше возможностей для выбора как функций-оракулов, так и их приближений. Согласно равенству (23), асимптотическая временная сложность атаки (с точностью до логарифмов от $2^{l_0+l_1}$ и θ^{-1}) определяется по формуле $T(l_0, s, r) = \tilde{O}\left(T_F 2^s \theta^{-4} + T_{\mathcal{A}} 2^{l_0-s}\right)$, где параметры s и θ зависят от подходящего допустимого для функции F подпространства H векторного пространства V_n, $n = l_0 + l_1$. Отметим, что на практике нахождение таких подпространств в общем случае представляет собой непростую задачу.

В [13] предложен метод «вероятностно нейтральных бит», по существу состоящий в проверке допустимости подпространств, порожденных векторами, каждый из которых имеет ровно одну ненулевую координату (используя введенные выше обозначения, можно сказать, что каждое такое подпространство порождается столбцами матрицы (18), где $m = s + l_1$, M_1 – нулевая, M_2 – единичная матрицы, а в каждом столбце и в каждой строке матрицы M_0 содержится не более одной единицы). В [1] предложен метод пречисления всех θ-допустимых подпространств для заданной функции F, обобщающий идею «вероятностно нейтральных бит» на случай произвольных направлений (ненулевых векторов в пространстве V_n), однако при отсутствии дополнительной информации о функции F этот метод оказывается малоэффективным ввиду огромного количества перебираемых подпространств. Отметим также, что при малых m и больших θ для нахождения всех θ-допустимых подпространств размерности m можно использовать алгоритм, описанный в [3]. По-видимому, аналогичный алгоритм можно применять и для поиска некоторых θ-допустимых подпространств большей размерности при меньших значениях θ.

Результаты экспериментального исследования эффективности предложенной атаки, в частности, ее сравнения с атакой FKM [13] авторы планируют опубликовать в отдельной статье.

ЛИТЕРАТУРА

[1]. Алексейчук А.Н. Алгебраически вырожденные приближения булевых функций / А. Н. Алексейчук, С. Н. Конюшок // Кибернетика и системный анализ. 2014. Т. 50. № 6. С. 3-14.

[2]. Алексейчук А.Н. Статистическая атака на генератор гаммы с линейным законом реинициализации начального состояния и функцией усложнения, близкой к алгебраически вырожденной / А.Н. Алексейчук, С.Н. Конюшок, А.Ю. Сторожук // Радиотехника. 2014. Вып. 176. С. 13-21.

[3]. Олексійчук А.М. Швидкі алгоритми побудови k-вимірних наближень наближень булевих функцій // А.М. Олексійчук, С.М. Конюшок, А.Ю. Сторожук // Захист інформації. 2015. Т. 17. № 1. С. 43-52.

[4]. Логачев О.А. Булевы функции в теории кодирования и криптологии / О.А. Логачев, А.А. Сальников, В.В. Ященко. М. : МЦНМО, 2004. 470 с.

[5]. Эндрюс Г. Теория разбиений / Г. Эндрюс. Пер. с англ. М.: Наука, 1982, 255 с.

[6]. Aumasson J.-Ph. Efficient FPGA implementations of high-dimensional cube testers on the stream cipher Grain-128 / J.-Ph. Aumasson, I. Dinur, L. Hensen, W. Meier, A. Shamir // http://eprint.iacr.org/2009/218.

[7]. Aumasson J.-Ph. Cube testers and key recovery attacks on reduced-raund MD6 and Trivium / J.-Ph. Aumasson, I. Dinur, W. Meier, A. Shamir // Fast Software Encryption – FSE'09. Proceedings. Springer-Verlag. 2009. P. 1-22.

[8]. Aumasson J.-Ph. New features of latin dances: analysis of Salsa, ChaCha, and Rumba / J.-Ph. Aumasson, S. Fischer, S. Khazaei, W. Meier, C. Rechberger // Fast Softvare Encryption – FSE 2008, Proceedings. Springer-Verlag. 2008, P. 470-488.

[9]. Dinur I. An experimentally verified attack on full Grain-128 using dedicated reconfigurable hardware / I. Dinur, T. Gueysu, C. Paar, A. Shamir, R. Zimmermann // http://eprint.iacr.org/2011/282.

[10]. Dinur I. Cube attacks on tweakable black box polynomials / I. Dinur, A. Shamir // Advances in Cryptology – EUROCRYPT'09. Proceedings. Springer-Verlag. 2009. P. 278-299.

[11]. Dinur I. Breaking Grain-128 with dynamic cube attacks / I. Dinur, A. Shamir // Fast Software Encryption – FSE'11. Proceedings. Springer-Verlag. 2011. P. 167-187.

[12]. Faisal Sh. Extended cubes: enhancing cube attacks by low-degree non-linear equations / Sh. Faisal, M. Resa, W. Susilo, J. Seberry // Proc. of the 6-th ACM Symp. on Information, Comput. and Communication Security (AIACCS'11). 2011. P. 296-305.

[13]. Fischer S. Chosen IV statistical analysis for key recovery attacks on stream ciphers / S. Fischer, S. Khazaei, W. Meier // AFRICACRYPT 2008. Proceedings. Springer-Verlag. 2008. P. 236-245.

[14]. Hoeffding W. Probability inequalities for sums of bounded random variables / W. Hoeffding // J. Amer. Statist. Assoc. 1963. Vol. 58. № 301. P. 13-30.

REFERENCES

[1]. Alekseychuk A. N., Konyushok S.N. (2014), «Algebraically degenerate approximation of Boolean functions» (in Russian), Kibernetika i Sistemnyi Analiz, Vol. 50, No. 6. pp. 3-14.

[2]. Alekseychuk A. N., Konyushok S. N., Storozhuk A. Y. (2014), «Statistical attack on gamma generator with linear law re-initialization of the initial state and complicating function at short distance from the algebraic degenerate function», Radiotehnika, No. 176, pp. 13-21.

[3]. Alekseychuk A. N., Konyushok S. N., Storozhuk A. Y. (2015), «Fast algorithms for constructing k-dimensional approximation of Boolean functions» Zahist Informatsii, Vol. 17. № 1. pp. 43–52.

[4]. Logachev O. A., Sal`nikov A. A, Yashchenko V. V. (2004), «Boolean functions in coding theory and cryptology» (in Russian), Moscow, MCCME, 470 p.

[5]. Andrews G.E (1976), «The Theory of partitions», Addison-Wesley Publishing Company, Inc.

[6]. Aumasson J.-Ph. Efficient FPGA implementations of high-dimensional cube testers on the stream cipher Grain-128 / J.-Ph. Aumasson, I. Dinur, L. Hensen, W. Meier, A. Shamir // http://eprint.iacr.org/2009/218.

[7]. Aumasson J.-Ph. Cube testers and key recovery attacks on reduced-raund MD6 and Trivium / J.-Ph. Aumasson, I. Dinur, W. Meier, A. Shamir // Fast Software Encryption – FSE'09. Proceedings. Springer-Verlag. 2009. P. 1–22.

[8]. Aumasson J.-Ph. New features of latin dances: analysis of Salsa, ChaCha, and Rumba / J.-Ph. Aumasson, S. Fischer, S. Khazaei, W. Meier, C. Rechberger // Fast Softvare Encryption – FSE 2008, Proceedings. Springer-Verlag. 2008, P. 470-488.

[9]. Dinur I. An experimentally verified attack on full Grain-128 using dedicated reconfigurable hardware / I. Dinur, T. Gueysu, C. Paar, A. Shamir, R. Zimmermann // http://eprint.iacr.org/2011/282.

[10]. Dinur I. Cube attacks on tweakable black box polynomials / I. Dinur, A. Shamir // Advances in Cryptology – EUROCRYPT'09. Proceedings. Springer-Verlag. 2009. P.278–299.

[11]. Dinur I. Breaking Grain-128 with dynamic cube attacks / I. Dinur, A. Shamir // Fast Software Encryption – FSE'11. Proceedings. Springer-Verlag. 2011. P. 167-187.

[12]. Faisal Sh. Extended cubes: enhancing cube attacks by low-degree non-linear equations / Sh. Faisal, M. Resa, W. Susilo, J. Seberry // Proc. of the 6-th ACM Symp. on Information, Comput. and Communication Security (AIACCS'11). 2011. P. 296-305.

[13]. Fischer S. Chosen IV statistical analysis for key recovery attacks on stream ciphers / S. Fischer, S. Khazaei, W. Meier // AFRICACRYPT 2008. Proceedings. Springer-Verlag. 2008. P. 236-245.

[14]. Hoeffding W. Probability inequalities for sums of bounded random variables / W. Hoeffding // J. Amer. Statist. Assoc. 1963. Vol. 58. № 301. P. 13-30.

УЗАГАЛЬНЕНА СТАТИСТИЧНА АТАКА НА СИНХРОННІ ПОТОКОВІ ШИФРИ

На сьогодні найбільш потужними атаками на синхронні потокові шифри є атаки на основі підібраних векторів ініціалізації. До них відносяться кубічна атака Дінура-Шаміра, статистична атака Фішера-Хазаї-Майєра (FKM), а також їх різні модифікації та вдосконалення. Атака FKM будується на основі статистичних наближень булевих функцій, пов'язаних з алгоритмами шифрування, функціями, які залежать лише від деяких розрядів ключа. Розробниками атаки запропоновано спосіб знаходження зазначених наближень, але не надано теоретичного обґрунтування ефективності цього способу. Крім того, залишається відкритим питання про те, чи можливо підвищити ефективність атаки FKM, вибираючи наближення з більш широкого класу булевих функцій. В даній статті пропонується атака на синхронні потокові шифри, яка узагальнює як кубічну атаку, так і атаку FKM. Ця атака базується на алгебраїчно вироджених наближеннях булевих функцій, що надає більше можливостей для реалізації основної ідеї атаки FKM. Запропоновано поліноміальний ймовірнісний алгоритм побудови зазначених наближень за відомими підпросторами, що є допустимими для заданої булевої функції. Показано, що вибираючи певним чином параметри цього алгоритму, можна будувати атаки на синхронні потокові шифри, значно більш ефективні в порівнянні з повним перебором ключів.

Ключові слова: потоковий шифр, нелінійний криптоаналіз, атака на основі підібраних векторів ініціалізації, алгебраїчно вироджена функція, знаходження наближень булевих функцій**.**

GENERALIZED STATISTICAL ATTACK ON SYNCRONOUS STREAM CIPHERS

Nowadays chosen IV attacks on synchronous stream ciphers are the most powerful. These include Dinur-Shamir cube attack, statistical Fisher-Khazaei-Meier (FKM) attack, and their different modifications and improvements. The FKM attack is based on statistical approximations (depended only on some key bits) of Boolean functions associated with encryption algorithms. Attack' developers suggested a method for finding these approximations but didn't provide a theoretical justification of such method' efficiency. Also there is an open question: is it possible to increase attack' efficiency by choosing approximations from a wider class of Boolean functions. We propose a generalization of cube attack and statistical attack FKM on synchronous stream ciphers. This attack is based on algebraic degenerate approximations of Boolean functions that provides more opportunities for implementation of FKM attack' basic idea. We also propose a polynomial probabilistic algorithm for

construction of such approximations from known subspaces acceptable for defined Boolean function. We show that the proposed algorithm allows us to construct much more efficient attacks on synchronous stream ciphers compared with exhaustive search.
Index Terms: stream cipher, non-linear cryptanalysis, chosen IV attack, algebraic degenerate function, finding approximations of Boolean functions.

Олексійчук Антон Миколайович, доктор технічних наук, професор Інституту спеціального зв'язку та захисту інформації НТУУ «КПІ».
E-mail: alex-dtn@ukr.net.
Алексейчук Антон Николаевич, доктор технических наук, профессор Института специальной связи и защиты информации НТУУ «КПИ».
Alekseychuk Anton, Doctor of Technical Science, Professor of Institute of Special Communication and Information Security of NTUU «KPI».

Конюшок Сергій Миколайович, кандидат технічних наук, доцент, заступник начальника Інституту спеціального зв'язку та захисту інформації НТУУ «КПІ».
E-mail: 3tooth@mail.ru.
Конюшок Сергей Николаевич, кандидат технических наук, доцент, заместитель начальника Института специальной связи и защиты информации НТУУ «КПИ».
Konyushok Sergey, Candidate of Technical Science, docent, vice-head of Institute of Special Communication and Information Security of NTUU «KPI».

Сторожук Артем Юрійович, аспірант Інституту спеціального зв'язку та захисту інформації НТУУ «КПІ».
E-mail: storojs72@gmail.com.
Сторожук Артем Юрьевич, аспирант Института специальной связи и защиты информации НТУУ «КПИ».
Storozhuk Artem, post-graduate student of Institute of Special Communication and Information Security of NTUU «KPI».

УДК 004.056.53:004.492.3 (045)

ЗАЩИТА АВИАЦИОННЫХ БОРТОВЫХ СЕТЕЙ ОТ АТАК МЕТОДАМИ ТЕОРИИ КОНФЛИКТА С ПРИМЕНЕНИЕМ МЕДОВЫХ ЛОВУШЕК

Сергей Водопьянов, Владимир Дрововозов, Елена Толстикова

Проблема защиты авиационных бортовых сетей от несанкционированных вторжений стоит особенно остро в связи с необходимостью безусловного обеспечения безопасности полетов, исключения летных происшествий и предпосылок к ним. Для защиты сети от внешних и внутренних атак необходимо не просто повышать энергетические и информационные ресурсы, а применять оптимальные методы борьбы с разумным противником. В работе предложены математические модели конфликтного взаимодействия с применением "медовых ловушек" – псевдосервисов, затягивающих противника в эскалацию атаки, вынуждающую его расходовать свои энергетические и информационные ресурсы. Разработана концептуальная модель построения комбинированной системы защиты с внедренным дополнительным уровнем защиты – сетевой медовой ловушки. Проведено компьютерное моделирование, результаты которого свидетельствуют о высокой эффективности разработанного метода защиты сети.
***Ключевые слова**: авиационная бортовая сеть, теория конфликта, медовая ловушка, марковский процесс, альтернирующий процесс восстановления.*

Введение. Мобильные коммуникации и организация доступа к Интернету для доступа к данным становятся все более востребованными в современных и тем более в будущих авиационных системах *CNS/ATM*. На первых этапах развития авиационных бортовых сетевых структур основное внимание уделялось использованию спутниковых коммуникационных систем и глобальных компьютерных сетей на их базе [1]. При выполнении полетов большой протяженности, включая трансконтинентальные полеты, а также полеты над пустынями, в полярных регионах, спутниковые коммуникационные системы играют основную роль в организации и развертывании глобальной авиационной сетевой инфраструктуры.

В настоящее время активно внедряются локальные компьютерные сети разного масштаба типа сотовых информационно-коммуникационных и вычислительных систем с самоорганизацией. Они имеют смешанную структуру "борт – борт" или "борт – земля". Благодаря таким системам обеспечиваются быстрый и экономичный