Предложено новое решение — нелинейные соотношения, выполняющиеся с преобладанием не меньше 0,25 для любого фиксированного ключа. Точнее, доказано:

$$\forall i > 0\ \forall K\ \exists z\ (\mathbf{P}\{y_i = x_i \oplus z x_{i-1}\} = 1/2 + \varepsilon,\ |\varepsilon| \geqslant 1/4; \tag{3}$$

$$\forall i > 0\ \forall K\ \exists z\ (\mathbf{P}\{y_i \oplus y_{i-1} = x_i \oplus z x_{i-1}\} = 1/2 + \varepsilon,\ |\varepsilon| \geqslant 1/4. \tag{4}$$

Изучена возможность применения соотношений (3), (4) для анализа блочных шифров, использующих операцию $+ \bmod 2^n$. Предложена модификация линейного метода криптоанализа, которая в ряде случаев позволяет провести более эффективные атаки.

В частности, аппроксимации (3), (4) использованы для проведения атаки с известным открытым текстом на конкретный шифр, имеющий структуру SP-сети, в котором для смешения с ключом используется операция $+ \bmod 2^n$. Эта атака позволяет восстановить ключ быстрее полного перебора, что подтверждено моделированием на ЭВМ. Далее был проанализирован шифр, имеющий аналогичное строение, но использующий для смешения с ключом операцию XOR. Сравнительный анализ показал, что замена операции XOR на $+ \bmod 2^n$ приводит к существенному увеличению стойкости шифра. При проведении атаки на шифр, использующий $+ \bmod 2^n$ вместо XOR, помимо S-блоков необходимо аппроксимировать блок смешения с ключом, поэтому в большинстве случаев абсолютная величина преобладания итогового соотношения, связывающего некоторые биты открытого текста, шифртекста и ключа, становится гораздо ниже, из-за чего для проведения атаки требуется существенно больше материала.

Проведена атака с известным открытым текстом на алгоритм ГОСТ 28147-89 с сокращённым числом раундов и S-блоками специального вида. В [2] доказана стойкость алгоритма ГОСТ 28147-89 с не менее чем пятью раундами шифрования относительно линейного метода криптоанализа. Предложенный метод позволил провести атаку на алгоритм ГОСТ 28147-89 с восемью раундами шифрования.

ЛИТЕРАТУРА

1. *Matsui M.* Linear cryptanalysis method for DES cipher // LNCS. 1993. V. 765. P. 386–397.
2. *Shorin V. V., Jelezniakov V. V., and Gabidulin E. M.* Linear and differential cryptanalysis of Russian GOST // Proc. Int. Workshop Coding and Cryptography (Paris, France, January 8–12, 2001). P. 467–476.

УДК 519.723 DOI 10.17223/2226308X/8/23

НЕЭНДОМОРФНЫЕ СОВЕРШЕННЫЕ ШИФРЫ С ДВУМЯ ШИФРВЕЛИЧИНАМИ

Н. В. Медведева, С. С. Титов

Исследуются неэндоморфные совершенные по Шеннону (абсолютно стойкие к атаке по шифртексту) шифры в случае, когда мощность множества шифрвеличин равна двум. В терминах линейной алгебры на основе теоремы Биркгофа о классификации дважды стохастических матриц описаны матрицы вероятностей ключей данных шифров. Построено множество возможных значений априорных вероятностей шифробозначений совершенного шифра.

Ключевые слова: *совершенные шифры, неэндоморфные шифры, максимальные шифры, дважды стохастические матрицы.*

Впервые вероятностная модель шифра рассмотрена в фундаментальной работе К. Шеннона [1]. Пусть X, Y — конечные множества соответственно шифрвеличин и

шифробозначений, с которыми оперирует некоторый шифр замены, K — множество ключей, причём $|X| = \lambda$, $|Y| = \mu$, $|K| = \pi$, где $\mu \geqslant \lambda > 1$. Согласно [2, 3], под *шифром* Σ_B будем понимать совокупность множеств правил зашифрования и расшифрования с заданными распределениями вероятностей на множествах ℓ-грамм открытых текстов, шифрованных текстов и ключей. Шифры, для которых апостериорные вероятности открытых текстов совпадают с их априорными вероятностями, называются *совершенными*. Изучение неэндоморфных ($|X| < |Y|$) совершенных шифров в общем виде предполагает знание распределения вероятностей на множестве ℓ-грамм алфавита открытых текстов. В качестве стандартного аппарата исследования распределения вероятностей на ℓ-граммах используются дважды стохастические матрицы [4]. Шифры, содержащие все инъекции из X в Y, называются *максимальными*. В [5] показано, что неминимальный ($|K| > |Y|$) совершенный шифр вкладывается в максимальный совершенный шифр.

Данная работа является продолжением [5]. Здесь описаны матрицы вероятностей ключей неэндоморфных совершенных шифров и множества вероятностей шифробозначений в случае, когда мощность множества шифрвеличин равна двум.

Рассмотрим неэндоморфный максимальный совершенный шифр в случае, когда мощность множества шифрвеличин равна двум. Пусть $X = \{x_1, x_2\}$; $Y = \{y_1, y_2, \ldots, y_\mu\} = \{1, 2, \ldots, \mu\}$; $K = \{k_1, k_2, \ldots, k_\pi\}$. Здесь $|X| = \lambda = 2$, $|Y| = \mu \geqslant 2$, $|K| = \pi = \mu(\mu - 1)$.

Зашифрование открытого текста $x = x_{i_1} x_{i_2} \ldots x_{i_\ell}$, где $x_{i_j} \in X$, т. е. $i_j \in \{1, 2\}$, заключается в замене каждой шифрвеличины x_{i_j} некоторым шифробозначением y_{i_j} в соответствии со случайно выбранным одним из $|K| = A_{|Y|}^{|X|} = A_\mu^2 = \mu!/(\mu - 2)! = \mu(\mu-1) = \pi$ всех инъективных отображений $e_k : X \to Y$, индексированных ключами $k \in K$. Инъективное отображение e_k, $k \in K$, при котором $e_k(x_1) = y_s = s$ и $e_k(x_2) = y_t = t$, будем также обозначать e_{st}, где $s, t = 1, \ldots, \mu$.

Пусть P_{st} — вероятность того, что при зашифровании шифрвеличины x_{i_j}, $i_j \in \{1, 2\}$, будет выбрано инъективное отображение e_{st}: $P_{st} = \mathbf{P}\{e_{st}(x_1) = s \,\&\, e_{st}(x_2) = t\}$, где $s \neq t$. Если $s = t$, то, в силу инъективности, $P_{st} = 0$.

Обозначим через $P = ||P_{st}||_{s,t=1}^{\mu}$ квадратную матрицу порядка μ, такую, что

$$\forall s \ \left(\sum_{t=1}^{\mu} P_{st} = p_s\right), \ \forall t \ \left(\sum_{s=1}^{\mu} P_{st} = p_t\right), \ p_1 + \ldots + p_\mu = 1. \tag{1}$$

Отметим, что, как указано в [3], совершенный по Шеннону шифр является сильно совершенным, т. е. не зависит от распределения на множестве шифрвеличин. Поэтому распределения вероятностей на множестве шифробозначений, индуцированные априорными распределениями вероятностей на множестве ключей, будем называть априорными.

Требуется описать множество возможных значений априорных вероятностей шифробозначений $p_s = \mathbf{P}\{y = s\}$, $s = 1, \ldots, \mu$, и найти общий вид матрицы P, удовлетворяющей условию (1) совершенности шифра, в зависимости от значений вероятностей p_s. Согласно подходу [2, 3], для вероятностной модели Σ_B шифра это достаточно сделать при $\ell = 1$. Для решения поставленной задачи будем использовать критерий совершенности шифра (2.2.4) из [3], который равносилен условию (1).

В частности, в примере 2.2.10 из [3] $X = \{x_1, x_2\}$, $Y = \{y_1, y_2, y_3\} = \{1, 2, 3\}$, $K = \{k_1, k_2, \ldots, k_6\}$, т. е. при $\lambda = 2$, $\mu = 3$, $\pi = 6$ таблица зашифрования имеет следующий вид:

$K\backslash X$	x_1	x_2	$P_{st} = \mathbf{P}\{e_{st}(x_1) = s \ \& \ e_{st}(x_2) = t\}$
k_1	1	2	$P_{12} = \mathbf{P}\{k = k_1\} = 19/80$
k_2	1	3	$P_{13} = \mathbf{P}\{k = k_2\} = 3/20$
k_3	2	1	$P_{21} = \mathbf{P}\{k = k_3\} = 21/80$
k_4	2	3	$P_{23} = \mathbf{P}\{k = k_4\} = 1/10$
k_5	3	1	$P_{31} = \mathbf{P}\{k = k_5\} = 1/8$
k_6	3	2	$P_{32} = \mathbf{P}\{k = k_6\} = 1/8$

При этом выполняются равенства:

$$p_1 = \mathbf{P}\{y = 1|x = x_1\} = P_{12} + P_{13} = 31/80; \quad p_1 = \mathbf{P}\{y = 1|x = x_2\} = P_{21} + P_{31} = 31/80;$$
$$p_2 = \mathbf{P}\{y = 2|x = x_1\} = P_{21} + P_{23} = 29/80; \quad p_2 = \mathbf{P}\{y = 2|x = x_2\} = P_{12} + P_{32} = 29/80;$$
$$p_3 = \mathbf{P}\{y = 3|x = x_1\} = P_{31} + P_{32} = 1/4; \qquad p_3 = \mathbf{P}\{y = 3|x = x_2\} = P_{13} + P_{23} = 1/4,$$

т. е. априорные и апостериорные (условные) вероятности шифробозначений y_i, $i = 1, 2, 3$, равны. Это, согласно критерию (2.2.4) из [3], означает, что матрица

$$P = ||P_{st}||_{s,t=1}^{3} = \begin{pmatrix} P_{11} & P_{12} & P_{13} \\ P_{21} & P_{22} & P_{23} \\ P_{31} & P_{32} & P_{33} \end{pmatrix} = \begin{pmatrix} 0 & 19/80 & 3/20 \\ 21/80 & 0 & 1/10 \\ 1/8 & 1/8 & 0 \end{pmatrix}$$

удовлетворяет условию (1) совершенности шифра.

Для матрицы P с неотрицательными элементами, удовлетворяющей условию (1), в силу теоремы Биркгофа [4] справедливы равенства

$$P = \sum_{\substack{Z\subset\{1,2,\ldots,\mu\},\\ Z\neq\varnothing}} \rho_Z P_Z, \qquad \sum_{\substack{Z\subset\{1,2,\ldots,\mu\},\\ Z\neq\varnothing}} \rho_Z = 1, \tag{2}$$

где Z — непустое множество номеров строк и столбцов; $\rho_Z \geqslant 0$ и P_Z — главные подматрицы равновероятных распределений.

Теорема 1. Матрица P с неотрицательными элементами, удовлетворяющая условию (1), лежит в выпуклой оболочке главных подматриц P_Z равновероятных распределений и определяется формулой (2).

При $\lambda = 2$ и $\mu = 3$ матрица P в общем случае определяется формулой

$$P = \frac{a}{3}\begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix} + \frac{b}{3}\begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix} + \frac{c}{2}\begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} +$$
$$+\frac{d}{2}\begin{pmatrix} 0 & 0 & 1 \\ 0 & 0 & 0 \\ 1 & 0 & 0 \end{pmatrix} + \frac{e}{2}\begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & a/3 + c/2c & b/3 + d/2 \\ b/3 + c/2 & 0 & a/3 + e/2 \\ a/3 + d/2 & b/3 + e/2 & 0 \end{pmatrix},$$

где $a, b, c, d, e \geqslant 0$ — произвольные параметры, такие, что $a + b + c + d + e = 1$.

Отметим, что для любых $a, e \geqslant 0$, где $2a + 3e = 3/5$, и однозначно по ним определённым параметрам $b = a + 3/40$, $c = e + 11/40$, $d = e + 1/20$, получаются числовые значения примера 2.2.10 из [3]. В частности, они получаются при крайних значениях параметров: $a = 0$, $e = 1/5$ и $a = 3/10$, $e = 0$.

Теорема 2. Набор чисел $p_1, \ldots, p_\mu$ при $\mu \geqslant 2$ может быть набором априорных вероятностей шифробозначений совершенного шифра в модели Σ_B с мощностью множества шифрвеличин, равной двум, тогда и только тогда, когда эти числа удовлетворяют условиям

$$p_1 + \ldots + p_\mu = 1, \quad 0 \leqslant p_i \leqslant \frac{1}{2} \quad (i = 1, \ldots, \mu).$$

Таким образом, описаны матрицы вероятностей ключей неэндоморфных совершенных шифров и множества вероятностей шифробозначений в случае, когда мощность множества шифрвеличин равна двум. Отметим, что при $\lambda > 2$ эта задача сильно усложняется ввиду отсутствия аналога теоремы Биркгофа о дважды стохастических матрицах.

ЛИТЕРАТУРА

1. *Шеннон К.* Теория связи в секретных системах // Работы по теории информации и кибернетике. М.: Наука, 1963. С. 333–402.
2. *Алферов А. П., Зубов А. Ю., Кузьмин А. С., Черемушкин А. В.* Основы криптографии. М.: Гелиос АРВ, 2001.
3. *Зубов А. Ю.* Совершенные шифры. М.: Гелиос АРВ, 2003.
4. *Birkhoff G. D.* Tres observations sobre el algebra lineal // Revista Universidad Nacional Tucuman. 1946. Ser. A. V. 5. P. 147–151.
5. *Медведева Н. В., Титов С. С.* О неминимальных совершенных шифрах // Прикладная дискретная математика. Приложение. 2013. № 6. С. 42–44.

УДК 519.7 DOI 10.17223/2226308X/8/24

ПРЕДВАРИТЕЛЬНАЯ ОЦЕНКА МИНИМАЛЬНОГО ЧИСЛА РАУНДОВ ЛЕГКОВЕСНЫХ ШИФРОВ ДЛЯ ОБЕСПЕЧЕНИЯ ИХ УДОВЛЕТВОРИТЕЛЬНЫХ СТАТИСТИЧЕСКИХ СВОЙСТВ[1]

А. И. Пестунов

Для новых легковесных блочных шифров (и нескольких известных шифров) проведена экспериментальная оценка минимального числа раундов, при котором в режиме CTR эти шифры обеспечивают удовлетворительные статистические свойства выходной псевдослучайной последовательности. Эксперименты проводились с помощью статистического теста «стопка книг» при длине выборки 2^{26} байт. В зависимости от шифра блоки представлялись в виде двух, трёх или четырёх 32-битовых слов и в качестве элементов тестируемой выборки брались первые слова каждого выходного блока. На вход шифра подавались блоки, где все слова, кроме второго, равны нулю, а второе слово менялось от 0 до $2^{24} - 1$.

Ключевые слова: *блочный шифр, легковесный шифр, статистический анализ, статистический тест, число раундов, псевдослучайные числа.*

Одно из применений итеративных блочных шифров — это генерация псевдослучайных чисел. Для этой цели часто используется режим CTR, подразумевающий последовательное шифрование значений некоторого счётчика и формирование псевдослучайной последовательности из выходных блоков или их частей. При этом удовлетворительные статистические свойства выходной последовательности могут быть обеспечены значительно меньшим числом раундов (обозначим его $R_{\min}$), чем полное число раундов шифра (обозначим его R). Очевидно, что сокращение числа раундов увеличит производительность шифров и позволит генерировать псевдослучайные числа быстрее. Причём даже если такой усечённый шифр имеет высоковероятные характеристики (линейные, дифференциальные, интегральные и пр.), он сможет генерировать псевдослучайные последовательности с удовлетворительными статистическими свой-

[1]Работа поддержана грантом РФФИ, проект № 14-01-31484 (мол_а).