14. *Kiltz E., Lyubashevsky V., and Schaffner C.,* A concrete treatment of Fiat — Shamir signatures in the quantum random-oracle model // Adv. Cryptology — EUROCRYPT 2018. Springer, 2018. P. 552–586.
15. *Albrecht M. R., Göpfert F., Virdia F., and Wunderer T.* Revisiting the expected cost of solving uSVP and applications to LWE // ASIACRYPT 2017. LNCS. 2017. V. 10624. P. 297–322.
16. *Albrecht M. R., Curtis B. R., Deo A., et al.* Estimate all the {LWE, NTRU} schemes! // SCN 2018. LNCS. 2018. V. 11035. P. 351–367.

УДК 512.64, 519.21, 519.72 DOI 10.17223/2226308X/13/15

КОНСТРУКЦИИ НЕЭНДОМОРФНЫХ СОВЕРШЕННЫХ ШИФРОВ

Н. В. Медведева, С. С. Титов

Исследуются совершенные по Шеннону (абсолютно стойкие к атаке по шифртексту) шифры. Получены достаточные условия того, что таблицы зашифрования неэндоморфных (эндоморфных) совершенных шифров не содержат латинских прямоугольников (квадратов). Приведён пример таких конструкций.

Ключевые слова: *совершенные шифры, эндоморфные шифры, неэндоморфные шифры.*

Рассмотрим вероятностную модель Σ_B шифра [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 $\lambda > 1$, $\mu \geqslant \lambda$. Это означает, что открытые и шифрованные тексты представляются словами (ℓ-граммами, $\ell \geqslant 1$) в алфавитах X и Y соответственно. Согласно [2, 3], под *шифром* Σ_B будем понимать совокупность множеств правил зашифрования и правил расшифрования с заданными распределениями вероятностей на множествах открытых текстов и ключей. Шифры, для которых апостериорные вероятности открытых текстов совпадают с их априорными вероятностями, называются *совершенными*.

Описание эндоморфных ($\lambda = \mu$) с минимально возможным числом ключей ($|K| = |Y|$) совершенных шифров даёт теорема Шеннона, таблица зашифрования таких шифров — это латинский квадрат из равновероятных подстановок зашифрования [1].

Для неэндоморфных ($\lambda < \mu$) минимальных совершенных шифров характерно большое многообразие таблиц зашифрования: они не сводятся только к латинским прямоугольникам размера $\mu \times \lambda$ [4]. Для $\lambda = 2$, например, таблицы зашифрования могут быть составлены и из неравновероятных инъекций. Однако если все ключи равновероятны, то данный совершенный шифр является выпуклой оболочкой латинских прямоугольников, содержащихся в его таблице зашифрования, согласно аналогу теоремы Биркгофа [5]. Если $\lambda > 2$, то, даже для равновероятных инъекций зашифрования, неэндоморфный совершенный шифр может не содержать в своей таблице зашифрования латинских прямоугольников $\mu \times \lambda$ [6].

Таким образом, при $\mu > \lambda$ возникает естественная задача описания минимальных по включению (т. е. шифров, содержащих минимально возможное множество ключей зашифрования с ненулевыми вероятностями) совершенных шифров, не сводящихся к латинским прямоугольникам размера $\mu \times \lambda$, которые можно рассматривать как непосредственное обобщение теоремы Шеннона. Данную задачу можно трактовать как задачу описания выпуклого полиэдра, соответствующего совершенным шифрам, через нахождение его вершин [5].

Подходом к решению такой задачи могут быть конструкции таблиц зашифрования, не содержащих латинских прямоугольников. Первым этапом решения задачи описания минимальных (по включению) совершенных шифров является построение таких конструкций для равновероятных ключей. При этом полезны достаточные условия отсутствия в таких таблицах латинских прямоугольников, тем более что в некоторых случаях эти условия оказываются необходимыми и достаточными.

Более того, эти условия могут быть частью общей конструкции искомых таблиц зашифрования, так как любые два её столбца можно рассматривать как шифр с $\lambda = 2$, к которому применим аналог теоремы Биркгофа [5, 7]. Тем самым построение таблицы зашифрования при $\lambda > 2$ можно трактовать как расширение таблицы с $\lambda = 2$. Для равновероятных ключей латинские прямоугольники $\mu \times 2$ всегда содержатся в таблице зашифрования с $\lambda \geqslant 3$ и поэтому достаточные условия должны включать в себя не менее трёх столбцов таблицы.

Пример 1. Пусть таблица зашифрования с $\lambda = 3 = |X|$, где $X = \{x_1, x_2, x_3\}$ — множество (алфавит) шифрвеличин, содержит строки с ключами k_i, k_j, k_m с вероятностями p_i, p_j, p_m соответственно и с шифробозначениями $a, b, c, u, v, w \in Y$, где Y — множество шифробозначений, $|Y| = \mu$:

k	x_1	x_2	x_3	P
$\dots$	$\dots$	$\dots$	$\dots$	$\dots$
k_i	a	b	u	p_i
k_j	v	b	c	p_j
k_m	a	w	c	p_m
$\dots$	$\dots$	$\dots$	$\dots$	$\dots$

Здесь шифробозначения a, b и c не входят в другие строки этой таблицы. Тогда данная таблица не может содержать латинских прямоугольников размеров $\mu \times 3$.

Действительно, если такой прямоугольник имеется, то он содержит либо строку ключа k_i, либо строку ключа k_m, так как в столбце для шифрвеличины x_1 шифробозначение a больше не встречается. Если он содержит строку k_i, то строка ключа k_m в него не входит, поэтому он должен содержать строку k_j, так как в столбце x_3 шифробозначение c больше не встречается. Тогда в столбце x_2 шифробозначение b будет встречаться дважды, что невозможно в латинском прямоугольнике.

Если же латинский прямоугольник содержит строку ключа ключа k_m, то строка ключа k_i в него не входит из-за шифробозначения a в столбце x_1. Тогда в нём содержится строка k_j из-за шифробозначения b в столбце x_2. Следовательно, в столбце x_3 шифробозначение c будет встречаться дважды, что также невозможно в латинском прямоугольнике.

Пример 1 иллюстрирует утверждение 1.

Утверждение 1. Пусть a, b, c — различные шифробозначения, $X = \{x_1, x_2, x_3\}$ — множество шифрвеличин. При этом:

1) множество K ключей разбито на два непересекающихся подмножества K_1 и K_2, т. е. $K = K_1 \cup K_2$ и $K_1 \cap K_2 = \varnothing$;
2) для любого ключа $k \in K_1$ шифрвеличина x_2 на ключе k зашифровывается в шифробозначение b, т. е. $e_k(x_2) = b$;
3) существует такой ключ $k \in K_1$, что шифрвеличина x_1 на ключе k зашифровывается в шифробозначение a, т. е. $e_k(x_1) = a$;
4) для любого ключа $k \in K_2$ шифрвеличина x_2 на ключе k зашифровывается в шифробозначение, отличное от шифробозначения b, т. е. $e_k(x_2) \neq b$;

5) существует единственный ключ k из K_2, на котором шифрвеличина x_1 зашифровывается шифробозначением a, а шифрвеличина x_3 — шифробозначением c, т. е. $e_k(x_1) = a$ и $e_k(x_3) = c$.

Тогда таблица зашифрования не содержит латинских прямоугольников $\mu \times 3$.

Определение 1. Ключи k' и k'' эквивалентны по шифрвеличине x_i, если x_i на ключах k' и k'' зашифровывается в одно и то же шифробозначение, т. е.

$$k' \underset{i}{\equiv} k'' \;\Leftrightarrow\; e_{k'}(x_i) = e_{k''}(x_i).$$

Определение 2. Попарно различные ключи $k_1, k_2, k_3, \ldots, k_{n-1}, k_n$ образуют цикл длины n, если выполняются условия

$$k_1 \underset{i_2}{\equiv} k_2 \underset{i_3}{\equiv} k_3 \underset{i_4}{\equiv} \ldots \underset{i_{n-1}}{\equiv} k_{n-1} \underset{i_n}{\equiv} k_n \underset{i_1}{\equiv} k_1,$$

где $i_2 \neq i_3$, $i_3 \neq i_4$, $\ldots$, $i_{n-1} \neq i_n$, $i_n \neq i_1$.

Обозначим через $[k]_i$ смежный класс ключа k по отношению эквивалентности $\underset{i}{\equiv}$:

$$[k]_i = \{k' \in K : e_{k'}(x_i) = e_k(x_i)\}.$$

Утверждение 2. Пусть в таблице зашифрования с $\lambda = 3 = |X|$ ключи k_1, k_2, k_3 образуют цикл длины три:

$$k_1 \underset{i_2}{\equiv} k_2 \underset{i_3}{\equiv} k_3 \underset{i_1}{\equiv} k_1,$$

где i_1, i_2, i_3 — попарно различны, и при этом $[k_3]_{i_3} \setminus [k_1]_{i_2} = \{k_3\}$. Тогда инъекция ключа k_1 не может быть строкой никакого латинского прямоугольника. Кроме того, если

$$[k_3]_{i_1} \subset \left([k_1]_{i_2} \cup [k_2]_{i_2}\right),$$

то таблица зашифрования не содержит латинских прямоугольников.

Из утверждения 2 следует достаточное условие отсутствия латинских квадратов в таблице зашифрования эндоморфного совершенного шифра с $\lambda \geqslant 3$.

Утверждение 3. Если в таблице зашифрования ключи $k_1, k_2, \ldots, k_n$ образуют цикл нечётной длины, то данная таблица не содержит латинских прямоугольников.

Таким образом, на основе отношения эквивалентности на множестве ключей получены достаточные условия того, что в таблице зашифрования неэндоморфных совершенных шифров отсутствуют латинские прямоугольники. В частности, получены достаточные условия того, что таблицы зашифрования эндоморфных совершенных шифров не содержат латинских квадратов.

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. *Медведева Н. В., Титов С. С.* Аналоги теоремы Шеннона для эндоморфных неминимальных шифров // Прикладная дискретная математика. Приложение. 2016. № 9. С. 62–65.

5. *Медведева Н. В., Титов С. С.* Описание неэндоморфных максимальных совершенных шифров с двумя шифрвеличинами // Прикладная дискретная математика. 2015. № 4 (30). С. 43–55.
6. *Медведева Н. В., Титов С. С.* Геометрическая модель совершенных шифров с тремя шифрвеличинами // Прикладная дискретная математика. Приложение. 2019. № 12. С. 113–116.
7. *Birkhoff G. D.* Tres observations sobre el algebra lineal // Revista Universidad Nacional Tucuman. 1946. Ser. A. V. 5. P. 147–151.

УДК 519.7 DOI 10.17223/2226308X/13/16

ПОСТРОЕНИЕ РАЗЛИЧИТЕЛЕЙ ДЛЯ ИТЕРАТИВНЫХ БЛОЧНЫХ ШИФРОВ НА ОСНОВЕ НЕЙРОННЫХ СЕТЕЙ

А. А. Перов, А. И. Пестунов

Предлагается новый универсальный подход к построению атак-различителей на итеративные блочные шифры, подразумевающий использование нейронных сетей, предназначенных для классификации растровых изображений. Описываются два метода, основанных на идее представления шифртекстов после разного числа раундов шифрования в виде растровых изображений с последующим обучением нейронной сети распознавать эти изображения. Показано, что для ряда современных блочных шифров предлагаемый подход более эффективен, чем универсальные различители, основанные на статистических тестах.

Ключевые слова: *блочный шифр, машинное обучение, нейронная сеть, статистический анализ, атака-различитель.*

В работе предлагается новый универсальный подход к построению атак-различителей на итеративные блочные шифры, где используются нейронные сети, предназначенные для классификации растровых изображений. Идея данного подхода возникла в результате наблюдения того, что преобразованный в растровое изображение (графический эквивалент) шифртекст имеет различную текстуру (паттерн) в зависимости от числа раундов. При этом с ростом числа раундов такая текстура становится менее выраженной и приближается к случайной.

В рамках этого подхода предлагаются два метода: «эталонный» и метод соседних раундов. В первом нейронная сеть используется для выявления различий в текстурах графических эквивалентов шифртекста при различном числе раундов и эталонной последовательности, неотличимой от случайных чисел. Второй метод предполагает выявление различий в текстурах графических эквивалентов соседних раундов и, что является его достоинством, не требует наличия эталонной последовательности, однако, забегая вперед, отметим, что «эталонный» метод оказался немного более эффективен. В экспериментах в качестве эталонной последовательности использован шифртекст полнораундового шифра AES256.

Для реализации предлагаемых методов необходимо выполнить процесс обучения свёрточной нейронной сети на графических эквивалентах шифртекстов (алгоритм 1).

Для формирования выборки выполняется шифрование на разном числе раундов, что даёт выборку выходных последовательностей блочных шифров с разными статистическими свойствами. На шагах 2–3 алгоритма 1 с помощью криптографической программной библиотеки «УНИБЛОКС-2015» выполняется шифрование в режиме