УДК 512.64+ 519.21+ 519.72

Медведева Н. В., Титов С. С.

ОПИСАНИЕ НЕЭНДОМОРФНЫХ СОВЕРШЕННЫХ ШИФРОВ С ДВУМЯ ШИФРВЕЛИЧИНАМИ

В работе дано полное описание неэндоморфных совершенных по Шеннону (абсолютно стойких к атаке по шифртексту) шифров в случае, когда мощность алфавита шифрвеличин равна двум. Описание шифров приводится в терминах линейной алгебры на основе теоремы Биркгофа о классификации дважды стохастических матриц. Построено множество возможных значений априорных вероятностей шифробозначений совершенного шифра.

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

Medvedeva N. V., Titov S. S.

THE DESCRIPTION OF NON-ENDOMORPHIC PERFECT CIPHERS WITH TWO PLAINTEXT VALUE

In this work it is given full description for non-endomorphic perfect ciphers which are absolutely immune against the attack on ciphertext, according to Shannon in a case when plaintext alphabet contains two elements (but ciphertext alphabet contains more than two elements). The description of these ciphers is provided in terms of linear algebra on the basis of Birkhoff's theorem of classification of doubly stochastic matrices. The set of possible values for aprioristic probabilities of elements in ciphertext alphabet of a perfect cipher is constructed.

Keywords: *perfect ciphers, non-endomorphic ciphers, maximum ciphers, doubly stochastic matrices.*

Впервые вероятностная модель шифра рассмотрена в фундаментальной работе К. Шеннона [1]. Пусть X, Y – конечные множества соответственно открытых текстов и шифрованных (закрытых) текстов, с которыми оперирует некоторый шифр замены, K – множество ключей, причем $|X| = \lambda$, $|Y| = \mu$, $|K| = \pi$, где $\lambda > 1$, $\mu \geq \lambda$. Под шифром будем понимать совокупность множеств правил зашифрования и правил расшифрования с заданными распределениями вероятностей на множествах ℓ-грамм открытых текстов, шифрованных текстов и ключей [2, 3]. Шифры, для которых апостериорные вероятности открытых текстов совпадают с их априорными вероятностями, называются **совершенными**. Такие

шифры являются абсолютно стойкими к криптоатакам по шифртексту. В работе [1] полностью описаны **эндоморфные** ($|X|=|Y|$) совершенные шифры с минимально возможным числом ключей ($|K|=|Y|$). Согласно теореме К. Шеннона [1], эндоморфные совершенные шифры с минимально возможным числом ключей исчерпываются шифрами гаммирования со случайной равновероятной гаммой.

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]. В работе [5] рассматривались комбинаторные проблемы современных аналогов совершенных шифров, в том числе неэндоморфных **неминимальных** ($|K|>|Y|$) совершенных шифров. Шифры, содержащие все инъекции из X в Y, т. е. для которых $|K|=\pi=\mu\cdot(\mu-1)\cdot\ldots\cdot(\mu-\lambda+1)$, называются **максимальными**. В работе [6] рассмотрены свойства неминимальных совершенных шифров. В частности, показано, что неминимальный совершенный шифр вкладывается в максимальный совершенный шифр.

Продолжая исследования [6], в данной работе в терминах линейной алгебры дано полное описание неэндоморфных максимальных совершенных по Шеннону шифров с мощностью алфавита шифрвеличин, равной двум. Построено множество возможных значений априорных вероятностей шифробозначений совершенного шифра.

Рассмотрим неэндоморфный максимальный совершенный шифр в случае, когда мощность алфавита шифрвеличин равна двум. Пусть $X=\{x_1,x_2\}$ – алфавит открытых текстов; $Y=\{y_1,y_2,\ldots,y_\mu\}$ – алфавит шифрованных текстов, с которыми оперирует некоторый шифр замены; $K=\{k_1,k_2,\ldots,k_\pi\}$ – множество ключей. Здесь $|X|=\lambda=2, |Y|=\mu\geq 2, |K|=\pi=\mu\cdot(\mu-1)$.

Зашифрование открытого текста $x=x_{i_1}x_{i_2}\ldots x_{i_\ell}$, где $i_j\in\{1,2\}$, заключается в замене каждой шифрвеличины x_{i_j} на шифробозначение $y_{s_{ij}}\in Y$, где $s_{i_j}\in\{1,2,\ldots,\mu\}$, в соответствии с одним из

$$|K|=A_{|Y|}^{|X|}=A_\mu^2=\frac{\mu!}{(\mu-2)!}=\mu\cdot(\mu-1)=\pi$$

всех инъективных отображений $e_k: X\to Y$, индексированных ключами $k\in K=\{k_1,k_2,\ldots,k_\pi\}$, занумерованными числами $1,2,\ldots,\pi$. Инъективное отображение e_k, $k\in K$, при котором

$$e_k(x_1)=y_s=s \text{ и } e_k(x_2)=y_t=t,$$

будем также обозначать e_{st}, где $s,t=1,2,\ldots,\mu$.

Пусть P_{st} – вероятность того, что при зашифровании шифрвеличин X_1 и X_2 будет выбрано инъективное отображение e_{st}, т. е.

$$P_{st}=P\{e_{st}(x_1)=s \,\&\, e_{st}(x_2)=t\},$$

где $y_s\neq y_t$. 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

$$\forall s:\sum_{t=1}^{\mu}P_{st}=p_s,\quad \forall t:\sum_{s=1}^{\mu}P_{st}=p_t,\quad p_1+p_2+\ldots+p_\mu=1 \qquad (1)$$

Требуется описать множество возможных значений априорных вероятностей шифробозначений $p_s=P\{y=y_s\}=P\{y=s\}$, $s=1,2,\ldots,\mu$, и найти общий вид матрицы P, удовлетворяющей условию (1) совершенности шифра, в зависимости от значений вероятностей P_s.

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

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

Здесь априорные вероятности шифробозначений $p_s = P\{y = y_s\} = P\{y = s\}$, где s=1,2,3, равны:

$$p_1 = P\{y = 1\} = P\{k = k_1 \,\&\, x = x_1\} + P\{k = k_2 \,\&\, x = x_1\} + P\{k = k_3 \,\&\, x = x_2\} +$$
$$+ P\{k = k_5 \,\&\, x = x_2\} = \left(\frac{19}{80} + \frac{3}{20}\right)P\{x = x_1\} + \left(\frac{21}{80} + \frac{1}{8}\right)P\{x = x_2\} =$$
$$= \frac{31}{80}(P\{x = x_1\} + P\{x = x_2\}) = \frac{31}{80};$$

$$p_2 = P\{y = 2\} = P\{k = k_3 \,\&\, x = x_1\} + P\{k = k_4 \,\&\, x = x_1\} + P\{k = k_1 \,\&\, x = x_2\} +$$
$$+ P\{k = k_6 \,\&\, x = x_2\} = \left(\frac{21}{80} + \frac{1}{10}\right)P\{x = x_1\} + \left(\frac{19}{80} + \frac{1}{8}\right)P\{x = x_2\} =$$
$$= \frac{29}{80}(P\{x = x_1\} + P\{x = x_2\}) = \frac{29}{80};$$

$$p_3 = P\{y = 3\} = P\{k = k_5 \,\&\, x = x_1\} + P\{k = k_6 \,\&\, x = x_1\} + P\{k = k_2 \,\&\, x = x_2\} +$$
$$+ P\{k = k_4 \,\&\, x = x_2\} = \left(\frac{1}{8} + \frac{1}{8}\right)P\{x = x_1\} + \left(\frac{3}{20} + \frac{1}{10}\right)P\{x = x_2\} =$$
$$= \frac{20}{80}(P\{x = x_1\} + P\{x = x_2\}) = \frac{20}{80}.$$

Проверим, что $p_1 + p_2 + p_3 = \frac{31}{80} + \frac{29}{80} + \frac{20}{80} = 1.$

Апостериорные вероятности шифробозначений y_s, s=1,2,3, соответственно равны:

$$P\{y = 1 \mid x = x_1\} = P\{y = 1 \mid k = k_1\} + P\{y = 1 \mid k = k_2\} = \frac{19}{80} + \frac{3}{20} = \frac{31}{80};$$

$$P\{y = 1 \mid x = x_2\} = P\{y = 1 \mid k = k_3\} + P\{y = 1 \mid k = k_5\} = \frac{21}{80} + \frac{1}{8} = \frac{31}{80};$$

$$P\{y = 2 \mid x = x_1\} = P\{y = 2 \mid k = k_3\} + P\{y = 2 \mid k = k_4\} = \frac{21}{80} + \frac{1}{10} = \frac{29}{80};$$

$$P\{y = 2 \mid x = x_2\} = P\{y = 2 \mid k = k_1\} + P\{y = 2 \mid k = k_6\} = \frac{19}{80} + \frac{1}{8} = \frac{29}{80};$$

$$P\{y = 3 \mid x = x_1\} = P\{y = 3 \mid k = k_5\} + P\{y = 3 \mid k = k_6\} = \frac{1}{8} + \frac{1}{8} = \frac{20}{80};$$

$$P\{y = 3 \mid x = x_2\} = P\{y = 3 \mid k = k_2\} + P\{y = 3 \mid k = k_4\} = \frac{3}{20} + \frac{1}{10} = \frac{20}{80}.$$

При этом для вероятностей $P_{st} = P\{e_{st}(x_1) = s \,\&\, e_{st}(x_2) = t\}$, s=1,2,3, выполняются равенства:

$$P\{y = 1 \mid x = x_1\} = P_{12} + P_{13} = \frac{31}{80};\ P\{y = 1 \mid x = x_2\} = P_{21} + P_{31} = \frac{31}{80};$$

$$P\{y = 2 \mid x = x_1\} = P_{21} + P_{23} = \frac{29}{80};\ P\{y = 2 \mid x = x_2\} = P_{12} + P_{32} = \frac{29}{80};$$

$$P\{y = 3 \mid x = x_1\} = P_{31} + P_{32} = \frac{20}{80};\ P\{y = 3 \mid x = x_2\} = P_{13} + P_{23} = \frac{20}{80}.$$

Следовательно, для каждого шифробозначения y_s, $s=1,2,3$, априорные вероятности совпадают с апостериорными. Это, согласно [3], эквивалентно равенству априорных и апостериорных вероятностей шифрвеличин, т. е. матрица

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

удовлетворяет условию (1) совершенности шифра.

В работе [6] показано, что искомое распределение вероятностей на множествах ℓ-грамм шифрованных текстов и ключей, при котором максимальный неэндоморфный шифр будет совершенным, представляет собой некоторое выпуклое тело P^{ℓ} – многогранник в многомерном евклидовом пространстве.

В случае, когда мощность алфавита шифрвеличин равна двум, многогранник P^{ℓ} допускает полное описание на основе теоремы Биркгофа о классификации дважды стохастических матриц. В этом описании существенно используется тот факт, что матрица P с неотрицательными элементами, удовлетворяющая условию (1), есть линейная комбинация с неотрицательными коэффициентами δ_Z дважды стохастических главных подматриц T_Z, где Z – непустое множество номеров строк и столбцов, а именно

$$P = \sum_{\substack{Z \subset \{1,2,\ldots,\mu\} \\ Z \neq \varnothing}} \delta_Z T_Z.$$

Сумма всех элементов каждой матрицы T_Z равна $|Z|$. Для каждого $Z \subset \{1,2,\ldots,\mu\}$, $Z \neq \varnothing$ матрица P_Z равновероятных распределений определяется по формуле

$$P_Z = \frac{1}{|Z|} \cdot T_Z.$$

Сумма всех элементов каждой матрицы P_Z равна единице, как и для матрицы P. Следовательно,

$$1 = \sum_{\substack{Z \subset \{1,2,\ldots,\mu\} \\ Z \neq \varnothing}} \delta_Z \cdot |Z| = \sum_{\substack{Z \subset \{1,2,\ldots,\mu\} \\ Z \neq \varnothing}} \rho_Z,$$

где $\rho_Z = |Z| \cdot \delta_Z$ и $\rho_Z \geq 0$, т. е. для матрицы P выполняются условия

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

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

Рассмотрим примеры, иллюстрирующие теорему 1.

Пример 1. Пусть $\mu = 2$ и матрица P имеет нулевую диагональ. Тогда $p_{12} = p_{21} = p_1 = p_2 = \frac{1}{2}$ и матрица P единственна:

$$P = \begin{pmatrix} 0 & \frac{1}{2} \\ \frac{1}{2} & 0 \end{pmatrix} = \frac{1}{2} \cdot \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \frac{1}{2} \cdot T,$$

где T – дважды стохастическая матрица. Это частный случай теоремы Шеннона для эндоморфного минимального шифра.

Пример 2. Пусть $\mu = 3$, матрица P имеет нулевую диагональ и

$$a = \tau_1 \cdot \rho_{\{1,2,3\}} \geq 0,\ b = \tau_2 \cdot \rho_{\{1,2,3\}} \geq 0,$$

$$c = \rho_{\{1,2\}} \geq 0,\ d = \rho_{\{1,3\}} \geq 0,\ e = \rho_{\{2,3\}} \geq 0$$

где произвольные параметры τ_1, τ_2, ρ_Z таковы, что

$$\tau_1 \geq 0, \tau_2 \geq 0, \tau_1 + \tau_2 = 1, \rho_Z \geq 0,$$

$$\rho_{\{1,2,3\}} + \rho_{\{1,2\}} + \rho_{\{1,3\}} + \rho_{\{2,3\}} = a + b + c + d + e = 1$$

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

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

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

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

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

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

$$p_1 + \ldots + p_\mu = 1,\ 0 \leq p_i \leq \frac{1}{2},\ i = 1, 2, \ldots, \mu \qquad (3)$$

В приложении к совершенным шифрам это означает, что любой набор чисел $p_i, i = 1, 2, \ldots, \mu$ с условиями (3) может быть набором априорных вероятностей шифробозначений совершенного шифра.

Таким образом, в работе полностью описаны неэндоморфные совершенные шифры в случае, когда мощность алфавита шифрвеличин равна двум.

Примечания

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. – 480 с.

3. Зубов А. Ю. Совершенные шифры. – М.: Гелиос АРВ, 2003. – 160 с.

4. Birkhoff G. D. Tres observations sobre el algebra lineal // Revista Universidad Nacional Tucuman, 1946. – Ser. A. – V. 5. – С. 147–151.

5. Титов С. С., Гутарин Д. С., Коновалова С. С., Титов Е. С., Тимин В. И. Комбинаторные проблемы существования совершенных шифров // Труды ИММ УрО РАН. – 2008. – Т. 13. – № 4. – С. 61–73.

6. Медведева Н. В., Титов С. С. О неминимальных совершенных шифрах // Прикладная математика. Приложение. – 2013. – № 6. – С. 42–44.

Медведева Наталья Валерьевна, к. ф.-м. н., доцент, доцент кафедры «Высшая и прикладная математика» УрГУПС, г. Екатеринбург. E-mail: medvedeva_n_v@mail.ru.

Титов Сергей Сергеевич, д. ф.-м. н., профессор, профессор кафедры «Высшая и прикладная математика» УрГУПС, Екатеринбург. E-mail: stitov@usaaa.ru.

Natalia Valerievna Medvedeva, PhD Physics and Mathematics, associate professor of Ural State University of Railway Transport. E-mail: medvedeva_n_v@mail.ru.

Sergey Sergeevich Titov, DSc Physics and Mathematics, Professor of Ural State University of Railway Transport. E-mail: stitov@usaaa.ru.