МАТЕМАТИЧЕСКИЕ МЕТОДЫ КРИПТОГРАФИИ

УДК 512.64, 519.21, 519.72

ОПИСАНИЕ НЕЭНДОМОРФНЫХ МАКСИМАЛЬНЫХ СОВЕРШЕННЫХ ШИФРОВ С ДВУМЯ ШИФРВЕЛИЧИНАМИ

Н. В. Медведева, С. С. Титов

Уральский государственный университет путей сообщения, г. Екатеринбург, Россия

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 описано множество (полиэдр) матриц вероятностей ключей неэндоморфных совершенных шифров с двумя шифрвеличинами. Построено множество возможных значений априорных вероятностей шифробозначений данных шифров.

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

DOI 10.17223/20710410/30/4

DESCRIPTION OF NON-ENDOMORPHIC MAXIMUM PERFECT CIPHERS WITH TWO-VALUED PLAINTEXT ALPHABET

N. V. Medvedeva, S. S. Titov

Ural State University of Railway Transport, Ekaterinburg, Russia

E-mail: medvedeva_n_v@mail.ru; stitov@usaaa.ru

This paper deals with non-endomorphic perfect (according to Shannon) ciphers, which are absolutely immune against the ciphertext-only attacks in the case when plaintext alphabet consists of two elements. Matrices of probabilities of cipher keys are described in terms of linear algebra on the basis of Birkhoff's theorem (about the classification of doubly stochastic matrices). The set of possible values of a priori probabilities for elements in ciphertext alphabet of a perfect cipher is constructed.

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

Введение

К. Шеннон, разрабатывая теорию криптографической стойкости, ввел понятие совершенного шифра как шифра, абсолютно стойкого к атаке по шифртексту [1]. Такой шифр не даёт криптоаналитику никакой дополнительной информации об открытом тексте на основе изучения перехваченной криптограммы. Примерно в те же годы концепция совершенного шифра разрабатывалась в одной закрытой работе, выполненной

под руководством В. А. Котельникова [2, 3]. Впоследствии, в связи с изучением вопросов имитостойкости шифров, понятие совершенного шифра было обобщено для криптоатак на основе совокупностей шифртекстов, полученных на одном ключе, а также криптоатак на основе известного открытого текста [4 – 6].

В основе изучения совершенных шифров лежит математическая модель шифра. Впервые вероятностная модель шифра рассмотрена в фундаментальной работе К. Шеннона [1]. Имеются и другие подходы к построению таких моделей [7 – 10]. В [3] предлагается некоторая модификация модели, приведенной в [7]. Она использует понятия опорного шифра, ключевого потока; в ней введены два класса шифров — с ограниченным и неограниченным ключами.

Пусть X, Y — конечные множества соответственно шифрвеличин и шифробозначений, с которыми оперирует некоторый шифр замены; K — множество ключей; $|X| = \lambda$, $|Y| = \mu$, $|K| = \pi$, где $\lambda > 1$, $\mu \geqslant \lambda$. Это означает, что открытые и шифрованные тексты представляются словами в алфавитах X и Y соответственно. Согласно [3, 7], под *шифром* Σ_B будем понимать совокупность множеств правил зашифрования и 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*. В работе [1] полностью описаны *эндоморфные* ($|X| = |Y|$) совершенные шифры с минимально возможным числом ключей ($|K| = |Y|$). Согласно теореме К. Шеннона [1], эндоморфные совершеные шифры с минимально возможным числом ключей исчерпываются шифрами гаммирования со случайной равновероятной гаммой.

Изучение *неэндоморфных* ($|X| < |Y|$) шифров в общем виде предполагает знание распределения вероятностей на множестве открытых текстов. В качестве стандартного аппарата исследования распределения вероятностей на множестве открытых текстов используются дважды стохастические матрицы [11]. Шифры, содержащие все инъекции из X в Y, т. е. такие, что $|K| = \pi = \mu(\mu-1)\cdot\ldots\cdot(\mu-\lambda+1)$, называются *максимальными*. Для неэндоморфных максимальных совершенных шифров ключи могут быть неравновероятными [3, пример 2.2.10]. В [12] показано, что *неминимальный* ($|K| > |Y|$) совершенный шифр вкладывается в максимальный совершенный шифр.

Данная работа является продолжением [12, 13]. Здесь описано множество (полиэдр) матриц вероятностей ключей и множество вероятностей шифробозначений неэндоморфных совершенных шифров в случае, когда мощность множества шифрвеличин равна двум.

1. Постановка задачи

Рассмотрим неэндоморфный максимальный совершенный шифр в случае, когда мощность множества шифрвеличин равна двум. Пусть $X = \{x_1, x_2\}$ — множество шифрвеличин; $Y = \{y_1, y_2, \ldots, y_\mu\} = \{1, 2, \ldots, \mu\}$ — множество шифробозначений, с которыми оперирует некоторый шифр замены; $K = \{k_1, k_2, \ldots, k_\pi\}$ — множество ключей. 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

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

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 $e_k(x_1) = y_s = s$ 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}, т. е.

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

где $y_s \neq y_t$. Если $s = t$, то, в силу инъективности, $\mathsf{P}_{st} = 0$.

Отметим, что вероятности P_{st}, где $s, t = 1, \ldots, \mu$, задают распределение вероятностей ключей $P(K)$, которое не зависит от распределения $P(X)$ на множестве шифрвеличин [3].

Обозначим через $P = \| \mathsf{P}_{st} \|$ квадратную матрицу порядка μ, такую, что

$$\forall s \left(\sum_{t=1}^{\mu} \mathsf{P}_{st} = p_s \right), \ \forall t \left(\sum_{s=1}^{\mu} \mathsf{P}_{st} = p_t \right); \tag{1}$$

$$p_1 + \ldots + p_\mu = 1. \tag{2}$$

Заметим, что, как указано в [3], совершенный по Шеннону шифр является сильно совершенным, т. е. является совершенным при любом распределении на множестве шифрвеличин. Поэтому распределения вероятностей на множестве шифробозначений, индуцированные априорными распределениями вероятностей на множестве ключей, будем называть априорными.

Условие (1) задает равенство априорных $p_s = \mathsf{P}\{y = y_s\} = \mathsf{P}\{y = s\}$, $s = 1, \ldots, \mu$, и апостериорных (условных) $\mathsf{P}\{y = y_s |\ x = x_{i_j}\} = \mathsf{P}\{y = s |\ x = x_{i_j}\}$, $i_j \in \{1, 2\}$, вероятностей шифробозначений. Это, согласно [3, критерий (2.2.4)], означает, что условие (1) равносильно условию совершенности шифра.

Требуется описать множество возможных значений априорных вероятностей шифробозначений p_s, $s = 1, \ldots, \mu$, и найти общий вид матрицы P, удовлетворяющей условиям (1) и (2), в зависимости от значений вероятностей p_s. Согласно подходу [3, 7], 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]. 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 вид

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

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

$$p_1 = \mathsf{P}\{y = 1 \,|\, x = x_1\} = \mathsf{P}_{12} + \mathsf{P}_{13} = \frac{31}{80}; \quad p_1 = \mathsf{P}\{y = 1 \,|\, x = x_2\} = \mathsf{P}_{21} + \mathsf{P}_{31} = \frac{31}{80};$$

$$p_2 = \mathsf{P}\{y = 2 \,|\, x = x_1\} = \mathsf{P}_{21} + \mathsf{P}_{23} = \frac{29}{80}; \quad p_2 = \mathsf{P}\{y = 2 \,|\, x = x_2\} = \mathsf{P}_{12} + \mathsf{P}_{32} = \frac{29}{80};$$

$$p_3 = \mathsf{P}\{y = 3 \,|\, x = x_1\} = \mathsf{P}_{31} + \mathsf{P}_{32} = \frac{20}{80}; \quad p_3 = \mathsf{P}\{y = 3 \,|\, x = x_2\} = \mathsf{P}_{13} + \mathsf{P}_{23} = \frac{20}{80},$$

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

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

удовлетворяет условию (1) совершенности шифра.

2. Основные понятия

Аналогично подходу [11], введём

Определение 1. Нормальным циклом длины $d \geqslant 1$ матрицы P будем называть последовательность $(i_1, i_2, \ldots, i_d)$ различных элементов множества $\{1, 2, \ldots, \mu\}$, такую, что

$$P_{i_1 i_2} > 0,\ P_{i_2 i_3} > 0,\ \ldots,\ P_{i_{d-1} i_d} > 0,\ P_{i_d i_1} > 0.$$

Будем считать, что нормальные циклы $(i_1, i_2, \ldots, i_d)$, отличающиеся друг от друга циклической перестановкой элементов, совпадают. Справедлива

Лемма 1. Пусть неотрицательная матрица P удовлетворяет условию (1) и не имеет нормальных циклов. Тогда P — нулевая матрица.

Доказательство. Предположим, что матрица P ненулевая, т. е. имеет ненулевой положительный элемент $\mathsf{P}_{ij} > 0$. Тогда $p_i \geqslant \mathsf{P}_{ij} > 0$ и $p_j \geqslant \mathsf{P}_{ij} > 0$.

Обозначим $i_1 = i$ и $i_2 = j$, где $i_1 \neq i_2$ (при $i_1 = i_2$ матрица P имеет нормальный цикл длины $d = 1$, что противоречит условию). Так как $p_j = p_{i_2} > 0$ является суммой элементов j-го столбца, а также суммой элементов i-й строки, в силу справедливости равенств (1) в матрице P существует k-й столбец, содержащий элемент $\mathsf{P}_{jk} > 0$. Обозначим $i_3 = k$. В силу отсутствия в матрице P нормальных циклов длины 1 имеем $i_2 \neq i_3$, а в силу отсутствия нормальных циклов длины 2 получаем, что $i_3 \neq i_1$, т. е. числа i_1, i_2, i_3 различны.

Продолжим нахождение ненулевых элементов матрицы P. Пусть последовательность $(i_1, i_2, \ldots, i_m)$, где $3 \leqslant m \leqslant \mu$, различных элементов такая, что выполняются неравенства

$$\mathsf{P}_{i_1 i_2} > 0,\ \mathsf{P}_{i_2 i_3} > 0,\ \ldots,\ \mathsf{P}_{i_{m-1} i_m} > 0.$$

Тогда $p_{i_1} > 0$, $p_{i_2} > 0$, $\ldots$, $p_{i_m} > 0$. Поскольку сумма элементов i_m-й строки равна p_{i_m}, в матрице P существует элемент $\mathsf{P}_{i_m i_{m+1}} > 0$. В силу отсутствия нормальных циклов длины 1 имеем $i_{m+1} \neq i_m$, а в силу отсутствия нормальных циклов длины 2 получаем, что $i_{m+1} \neq i_{m-1}$. В силу отсутствия нормальных циклов длины 3 имеем $i_{m+1} \neq i_{m-2}$ и т. д.; а именно из-за отсутствия нормальных циклов длины $4, 5, \ldots, m$ выполняются условия $i_{m+1} \neq i_{m-3}$, $i_{m+1} \neq i_{m-4}$, $\ldots$, $i_{m+1} \neq i_1$, т. е. все числа $i_1, i_2, \ldots, i_{m+1}$ различны.

Однако в силу конечности множества строк (столбцов) матрицы P множество $\{i_1, i_2, \ldots, i_m\}$ является подмножеством множества $\{1, 2, \ldots, \mu\}$ всех номеров строк матрицы P. Максимальное значение m равно μ, при котором $i_{m+1} = i_{\mu+1} \in \{i_1, i_2, \ldots, i_\mu\}$, т. е. $i_{\mu+1} = i_n$ для некоторого $n \in \{i_1, i_2, \ldots, i_\mu\}$. Получаем противоречие с тем, что все числа $i_1, i_2, \ldots, i_{\mu+1}$ различны. Следовательно, предположение, что P — ненулевая матрица, неверно. ■

Определение 1. Пусть Z — непустое подмножество множества $\{1, 2, \ldots, \mu\}$ номеров строк и столбцов матрицы $P = ||P_{ij}||$. Главной подматрицей, соответствующей множеству Z, назовём квадратную матрицу $Q_Z = ||Q_{ij}||$ порядка μ, такую, что при

всех $i, j \in Z$ выполняются неравенства $0 \leqslant Q_{ij} \leqslant P_{ij}$, а при $i \notin Z$ или $j \notin Z$ — равенство $Q_{ij} = 0$.

Определение 2 [11]. Квадратную матрицу $T = ||t_{ij}||$ будем называть дважды стохастической, если $t_{ij} \geqslant 0$ и

$$\sum_{j=1}^{n} t_{ij} = 1,\ 1 \leqslant i \leqslant n; \quad \sum_{i=1}^{n} t_{ij} = 1,\ 1 \leqslant j \leqslant n.$$

В случае, когда мощность алфавита шифрвеличин равна двум, множество возможных значений априорных вероятностей шифробозначений $p_s = \mathsf{P}\{y = y_s\} = \mathsf{P}\{y = s\}$, где $s = 1, \ldots, \mu$, допускает описание на основе теоремы Биркгофа о классификации дважды стохастических матриц [11]. В [14] такие матрицы называются двояко стохастическими.

Замечание 1. Пусть $\tau = \min\{p_1, \ldots, p_\mu\}$. Тогда, если $\tau = 0$, то среди $p_1, \ldots, p_\mu$ есть нуль, и в матрице P есть (для некоторого i) столбец и строка с номером i, все элементы которых — нули, так что в этом случае матрица P определяется некоторой своей подматрицей размерами $\mu_1 \times \mu_1$ с $\mu_1 < \mu$, в которой нет ни нулевых строк, ни нулевых столбцов. Если $\tau > 0$, то при $\tau = \max\{p_1, \ldots, p_\mu\}$ матрица $\dfrac{1}{\tau}P$ — дважды стохастическая.

Замечание 2. Каждой дважды стохастической матрице размера $\mu \times \mu$ соответствует матрица равновероятных распределений, которая получается из данной матрицы делением каждого её элемента на μ. Здесь имеется в виду не равновероятность ключей, а равенство всех априорных вероятностей шифробозначений, т. е. $p_1 = p_2 = \ldots = p_\mu$.

Замечание 3. Главная подматрица равновероятных распределений — это главная подматрица матрицы P, такая, что если вычеркнуть в ней нулевые строки и столбцы, то получится матрица равновероятных распределений.

Определение 3. Пусть $(i_1, i_2, \ldots, i_d)$ — нормальный цикл длины $d \geqslant 1$ матрицы P. Матрицей $C^{(i_1,i_2,\ldots,i_d)} = ||C_{ij}||$ нормального цикла $(i_1, i_2, \ldots, i_d)$ назовём квадратную матрицу порядка μ, в которой

$$C_{i_1 i_2}^{(i_1,i_2,\ldots,i_d)} = C_{i_2 i_3}^{(i_1,i_2,\ldots,i_d)} = \ldots = C_{i_d i_1}^{(i_1,i_2,\ldots,i_d)} = 1,$$

а остальные элементы равны нулю.

Матрица $C^{(i_1,i_2,\ldots,i_d)}$ — это в точности матрица перестановки подматрицы, полученная из матрицы P вычеркиванием строк и столбцов, номера которых не лежат в Z. Отметим, что сумма элементов i-й строки (или j-го столбца) матрицы $C^{(i_1,i_2,\ldots,i_d)}$ равна нулю, если $i \notin (i_1, i_2, \ldots, i_d)$ $(j \notin (i_1, i_2, \ldots, i_d))$, и равна 1, если $i \in (i_1, i_2, \ldots, i_d)$ $(j \in (i_1, i_2, \ldots, i_d))$.

Пример 1. Пусть $\mu = 3$ и матрица P имеет нулевую диагональ. Нормальные наборы при $|Z| = 3$, $Z = \{1, 2, 3\}$ задаются матрицами перестановок

$$C^{(1,2,3)} = C^{(2,3,1)} = C^{(3,1,2)} = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}, \quad C^{(1,3,2)} = C^{(2,1,3)} = C^{(3,2,1)} = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix},$$

которым соответствует произвольная дважды стохастическая матрица 3×3 с нулевой диагональю

$$T_Z = \tau_1 \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix} + \tau_2 \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & \tau_1 & \tau_2 \\ \tau_2 & 0 & \tau_1 \\ \tau_1 & \tau_2 & 0 \end{pmatrix}, \quad \tau_1 \geqslant 0, \quad \tau_2 \geqslant 0, \quad \tau_1 + \tau_2 = 1,$$

и, тем самым, произвольная матрица P_Z равновероятного распределения (с равными априорными вероятностями)

$$P_{\{1,2,3\}} = \frac{1}{3} \begin{pmatrix} 0 & \tau_1 & \tau_2 \\ \tau_2 & 0 & \tau_1 \\ \tau_1 & \tau_2 & 0 \end{pmatrix}.$$

При $|Z| = 2$ нормальные циклы задаются матрицами

$$Z = \{1,2\} \Rightarrow C^{(1,2)} = C^{(2,1)} = T_Z = \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix},$$

$$Z = \{1,3\} \Rightarrow C^{(1,3)} = C^{(3,1)} = T_Z = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 0 & 0 \\ 1 & 0 & 0 \end{pmatrix},$$

$$Z = \{2,3\} \Rightarrow C^{(2,3)} = C^{(3,2)} = T_Z = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix},$$

которым соответствуют единственные матрицы равновероятных распределений

$$P_{\{1,2\}} = \frac{1}{2} \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}, \; P_{\{1,3\}} = \frac{1}{2} \begin{pmatrix} 0 & 0 & 1 \\ 0 & 0 & 0 \\ 1 & 0 & 0 \end{pmatrix}, \; P_{\{2,3\}} = \frac{1}{2} \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}.$$

Наконец, при $|Z| = 1$ нормальных циклов нет, так как диагональ матрицы P — нулевая.

3. Описание множества матриц вероятностей ключей

Пусть Z — непустое подмножество множества $\{1, 2, \ldots, \mu\}$ номеров строк и столбцов матрицы $P = ||\,\mathsf{P}_{ij}\,||$. Каждому множеству Z поставим в соответствие некоторое число $\rho_Z \geqslant 0$. Тогда можно составить матрицу

$$\sum_{\substack{Z \subset \{1,2,\ldots,\mu\}, \\ Z \neq \varnothing}} \rho_Z \cdot P_Z, \qquad \sum_{\substack{Z \subset \{1,2,\ldots,\mu\}, \\ Z \neq \varnothing}} \rho_Z = 1, \tag{3}$$

удовлетворяющую условиям (1) и (2). Справедлива

Теорема 1. Матрица P с неотрицательными элементами, удовлетворяющая условиям (1) и (2), лежит в выпуклой оболочке главных подматриц P_Z равновероятных распределений и определяется формулой (3), где суммирование проводится по всем непустым подмножествам Z множества номеров строк и $\rho_Z \geqslant 0$.

Доказательство. Согласно замечаниям 1–3, матрица, определяемая формулой (3), удовлетворяет условиям (1) и (2) совершенности шифра. Пусть неотрицательная матрица P удовлетворяет условиям (1) и (2), где $p_j \geqslant 0$, $\mathsf{P}_{st} \geqslant 0$ и $j, s, t = 1, \ldots, \mu$. Доказательство проведём в четыре этапа.

1. *Устранение нулевых априорных вероятностей.* Если $p_m = 0$, где $m \in \{1, \ldots, \mu\}$, то сумма элементов m-й строки (m-го столбца) матрицы P равна нулю. Поэтому, отбрасывая эти нулевые строку и столбец, придём к матрице P' порядка $\mu - 1$. Положим $P := P'$, $\mu := \mu - 1$. Продолжая исключать нулевые строки и столбцы, придём к матрице, для которой $p_i > 0$ для всех $i = 1, \ldots, \mu$ и в каждой строке и каждом столбце есть хотя бы один ненулевой элемент.

Пусть неотрицательная матрица P удовлетворяет условиям (1) и (2), где все $p_i > 0$, $i = 1, \ldots, \mu$, и в каждой строке и каждом столбце данной матрицы есть хотя бы один ненулевой элемент.

2. *Устранение нормальных циклов.* Обнулим некоторые элементы матрицы P с соответствующим уменьшением значений p_i и сохранением равенств (1), но без сохранения равенства (2).

Начнём с диагональных элементов. Если $\mathsf{P}_{ii} > 0$ для некоторого i, то построим новую матрицу P', в которой $\mathsf{P}'_{st} := \mathsf{P}_{st}$ для всех пар $\{s, t\}$, кроме случая $s = t = i$. Положим

$$Q_{(i)} := \mathsf{P}_{ii},\ \mathsf{P}'_{ii} := 0,\ p'_i := p_i - \mathsf{P}_{ii} = p_i - Q_{(i)}.$$

Поскольку $p_i = \mathsf{P}_{ii} + p'_i$, то $p_i \geqslant \mathsf{P}_{ii}$ и, следовательно, $p'_i \geqslant 0$. Переобозначая $\mathsf{P}_{st} := \mathsf{P}'_{st}$, $p_i := p'_i$, получим выполнение равенств (1). Перебирая таким образом все ненулевые диагональные элементы, придём к матрице P, которая удовлетворяет равенствам (1) и в которой все диагональные элементы равны нулю.

Далее будем обнулять элементы матрицы P, симметричные относительно главной диагонали, т. е. элементы P_{st} и P_{ts}, где $s \neq t$, $\mathsf{P}_{st} > 0$, $\mathsf{P}_{ts} > 0$. Положим

$$Q_{(s,t)} := \min\{\mathsf{P}_{st},\ \mathsf{P}_{ts}\},\ \mathsf{P}_{st} := \mathsf{P}_{st} - Q_{(s,t)},\ \mathsf{P}_{ts} := \mathsf{P}_{ts} - Q_{(s,t)},\ p_s := p_s - Q_{(s,t)},\ p_t := p_t - Q_{(s,t)}.$$

Перебирая таким образом все пары элементов P_{st} и P_{ts}, придём к матрице P, в которой нулевые не только диагональные элементы, но и для каждой пары $\{s, t\}$, где $s \neq t$, элемент $\mathsf{P}_{st} = 0$, или $\mathsf{P}_{ts} = 0$, или $\mathsf{P}_{st} = \mathsf{P}_{ts} = 0$.

Заметим, что, согласно определению 1, выше рассмотрены нормальные циклы длины $d = 1$ и $d = 2$ и из матрицы P вычитались главные подматрицы матрицы P, пропорциональные соответственно матрицам $C^{(i)}$ и $C^{(s,t)}$ нормальных циклов (i) и (s, t):

$$P := P - \sum_{(i)} \mathsf{P}_{ii} \cdot C^{(i)} = P - \sum_{(i)} Q_{(i)} \cdot C^{(i)}, \quad P := P - \sum_{(s,t)} Q_{(s,t)} \cdot C^{(s,t)}.$$

Отметим также, что при таком зануленении элементов матрицы P количество нулевых циклов возрастает, а количество нормальных циклов в матрице P убывает.

Аналогично будем действовать при $d \geqslant 3$. Пусть матрица P не имеет нормальных циклов длины $d = m - 1$, где $3 \leqslant m \leqslant \mu$. Будем устранять нормальные циклы $(i_1, i_2, \ldots, i_d)$ при $d = m$. Для этого положим

$$Q_{(i_1,i_2,\ldots,i_d)} := \min\{\mathsf{P}_{i_1i_2}, \mathsf{P}_{i_2i_3}, \ldots, \mathsf{P}_{i_{d-1}i_d}, \mathsf{P}_{i_di_1}\},$$
$$\mathsf{P}_{i_1i_2} := \mathsf{P}_{i_1i_2} - Q_{(i_1,i_2,\ldots,i_d)},\ \mathsf{P}_{i_2i_3} := \mathsf{P}_{i_2i_3} - Q_{(i_1,i_2,\ldots,i_d)}, \ldots, \mathsf{P}_{i_di_1} := \mathsf{P}_{i_di_1} - Q_{(i_1,i_2,\ldots,i_d)},$$
$$p_{i_1} := p_{i_1} - Q_{(i_1,i_2,\ldots,i_d)},\ p_{i_2} := p_{i_2} - Q_{(i_1,i_2,\ldots,i_d)}, \ldots, p_{i_d} := p_{i_d} - Q_{(i_1,i_2,\ldots,i_d)},$$

т. е. из матрицы P будем вычитать её главные подматрицы, пропорциональные матрицам $C^{(i_1,i_2,\ldots,i_d)}$ её нормальных циклов $(i_1,i_2,\ldots,i_d)$:

$$P' = P - \sum_{(i_1,i_2,\ldots,i_d)} Q_{(i_1,i_2,\ldots,i_d)} \cdot C^{(i_1,i_2,\ldots,i_d)}.$$

В силу конечности множества нормальных циклов за конечное число шагов придём к случаю, когда в матрице P отсутствуют нормальные циклы длины $d = m$.

Последовательно проводя данную процедуру, с увеличением длины d нормальных циклов на единицу придём к нормальным циклам длины $d = \mu$ и, после завершения процедуры, получим неотрицательную матрицу P, не имеющую нормальных циклов.

3. *Получение вида матрицы.* Согласно лемме 1, полученная неотрицательная матрица P — нулевая, а сумма всех отнятых матриц равна исходной матрице P. Следовательно, исходная матрица P удовлетворяет равенству

$$P = \sum_{d=1}^{\mu} \sum_{(i_1,i_2,\ldots,i_d)} Q_{(i_1,i_2,\ldots,i_d)} \cdot C^{(i_1,i_2,\ldots,i_d)}, \tag{4}$$

где $Q_{(i_1,i_2,\ldots,i_d)} \geqslant 0$. Матрица $Q^{(i_1,i_2,\ldots,i_d)} = Q_{(i_1,i_2,\ldots,i_d)} \cdot C^{(i_1,i_2,\ldots,i_d)}$ является главной подматрицей исходной матрицы P, согласно определению 2, со множеством $Z = \{i_1,i_2,\ldots,i_d\}$.

Для любой пары (i,j) имеем, в силу равенства (4), равенство $\mathsf{P}_{ij} = Q_{(i)}$ при $i = j$, а при $i \neq j$ и $d \geqslant 2$ имеем

$$\mathsf{P}_{ij} = \sum_{(i_1,i_2,\ldots,i_d)} Q_{(i_1,i_2,\ldots,i_d)},$$

где $i_1 = i$ и $i_2 = j$, так как нормальные циклы совпадают при циклической перестановке их элементов. Поскольку каждая такая пара (i,j) лежит в некотором цикле, а для элементов матрицы P имеем равенство $\sum\limits_{i=1}^{\mu}\sum\limits_{j=1}^{\mu} \mathsf{P}_{ij} = 1$, получаем, что

$$\sum_{(i_1,i_2,\ldots,i_d)} Q_{(i_1,i_2,\ldots,i_d)} = 1. \tag{5}$$

Следовательно, неотрицательная матрица P, удовлетворяющая условию (1), лежит в выпуклой оболочке матриц нормальных циклов — это аналог теоремы Биркгофа.

4. *Переход к равенству* (3). Далее для каждого $Z \subset \{1,2,\ldots,\mu\}$, где $d = |Z| \geqslant 2$, рассмотрим все нормальные циклы длины d, элементы которых берутся из Z. Это означает, что если $Z = \{j_1,j_2,\ldots,j_d\}$, то цикл $(i_1,i_2,\ldots,i_d)$ — это перестановка чисел $j_1,j_2,\ldots,j_d$. Положим

$$\tilde{P}_Z = \sum_{\{i_1,i_2,\ldots,i_d\}=Z} Q_{(i_1,i_2,\ldots,i_d)} \cdot C^{(i_1,i_2,\ldots,i_d)}, \quad \rho_Z = Q_Z = \sum_{\{i_1,i_2,\ldots,i_d\}=Z} Q_{(i_1,i_2,\ldots,i_d)},$$

где $\rho_Z = Q_Z \geqslant 0$ и, согласно (5), $\sum\limits_{\{i_1,i_2,\ldots,i_d\}=Z} \rho_Z = 1$. Тогда

$$\tilde{P}_Z = \left[\sum_{\{i_1,i_2,\ldots,i_d\}=Z} Q_{(i_1,i_2,\ldots,i_d)}\right] \cdot T_Z = \rho_Z \cdot T_Z,$$

где T_Z — дважды стохастическая матрица, номера строк и столбцов которой принадлежат множеству $\{i_1,i_2,\ldots,i_d\} = Z$.

Обозначим

$$P_Z = \frac{1}{d} \cdot T_Z$$

— главная подматрица равновероятных распределений, элементы которой $(\mathsf{P}_Z)_{ij} = 0$ при $i \notin Z$ или $j \notin Z$; $(\mathsf{P}_Z)_{ij} = (T_Z)_{ij}/d$ при $i, j \in Z$.

Таким образом, для неотрицательной матрицы P, удовлетворяющей условиям (1) и (2), выполняется равенство

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

т. е. матрица P лежит в выпуклой оболочке главных подматриц P_Z равновероятных распределений. ■

В обзоре [15] представлены некоторые работы, примыкающие к проблематике теоремы Биркгофа. В [16, 17] приведены результаты об экстремальных точках для полиэдра конечных симметрических матриц с заданными суммами по строкам. Для специального класса дважды стохастических матриц, определяемого границами для элементов матрицы, в [18] строятся экстремальные точки. В доказанной аналогичным образом выше теореме 1 описан соответствующий полиэдр указанием его вершин (экстремальных точек), которые представляют собой нормальные циклы.

Рассмотрим примеры, иллюстрирующие теорему 1.

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

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

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

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

$$a = \tau_1 \cdot \rho_{\{1,2,3\}} \geqslant 0, \quad b = \tau_2 \cdot \rho_{\{1,2,3\}} \geqslant 0, \quad c = \rho_{\{1,2\}} \geqslant 0, \quad d = \rho_{\{1,3\}} \geqslant 0, \quad e = \rho_{\{2,3\}} \geqslant 0,$$

где произвольные параметры τ_1, τ_2, ρ_Z таковы, что $\tau_1 \geqslant 0$, $\tau_2 \geqslant 0$, $\tau_1 + \tau_2 = 1$, $\rho_Z \geqslant 0$,

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

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

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

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

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

Отметим, что для любых $a \geqslant 0$, $e \geqslant 0$, 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 $a = 3/10$, $e = 0$.

4. Описание множества априорных вероятностей шифробозначений

Если для соблюдения условия инъективности операций зашифрования потребовать, чтобы диагональ в матрице P была нулевой, то не каждый набор априорных вероятностей элементов множества Y шифробозначений может быть реализован в совершенном по Шеннону шифре. Справедлива

Лемма 2. Точка $(p_1, \ldots, p_\mu)$ в $\mathbb{R}^\mu$ $(\mu \geqslant 2)$, координаты которой удовлетворяют условиям

$$p_1 + \ldots + p_\mu = 1, \quad 0 \leqslant p_i \leqslant \frac{1}{2}, \quad i = 1, \ldots, \mu, \tag{6}$$

лежит в выпуклой оболочке точек

$$V_{ij} = (0, \ldots, 0, v_i, 0, \ldots, 0, v_j, 0, \ldots, 0) = (0, \ldots, 0, \frac{1}{2}, 0, \ldots, 0, \frac{1}{2}, 0, \ldots, 0),$$

где $i, j = 1, \ldots, \mu,\ i \neq j$.

Доказательство. Пусть $p_1 + \ldots + p_\mu = 1$, $p_i \geqslant 0$ $(i = 1, \ldots, \mu)$. Эти условия определяют $(\mu - 1)$-мерный симплекс в μ-мерном пространстве $\mathbb{R}^\mu$. Полупространства $p_i \leqslant 1/2$, $i = 1, \ldots, \mu$, высекают в этом симплексе $(\mu-1)$-мерный выпуклый многогранник, на границе которого хотя бы одно из этих неравенств обращается в равенство. Найдём его вершины. На гиперпространстве $p_j = 1/2$, например, $p_1 = 1/2$ при $j = 1$, имеем наибольшее евклидово расстояние от начала координат

$$\sqrt{p_1^2 + p_2^2 + \ldots + p_\mu^2} = \sqrt{\frac{1}{4} + p_2^2 + \ldots + p_\mu^2} \leqslant \sqrt{\frac{1}{4} + (p_2 + \ldots + p_\mu)^2} = \sqrt{\frac{1}{4} + \left(\frac{1}{2}\right)^2} = \frac{\sqrt{2}}{2},$$

и оно достигается на вершинах в силу центральной симметричности этой гиперграни; однако неравенство обращается в равенство при $p_1^2 + p_2^2 + \ldots + p_\mu^2 = (p_1 + p_2 + \ldots + p_\mu)^2$, что может быть только если все p_i обращаются в нуль, кроме одного: $p_i = 0$ для $i = 2, \ldots, \mu$, $i \neq j$; $p_j = 1/2$. Итак, на этой грани имеется $\mu - 1$ вершин с двумя ненулевыми координатами $p_1 = 1/2$, $p_j = 1/2$, $j \in \{2, \ldots, \mu\}$. Ясно, что это верно для любой грани, поэтому описываемый многогранник имеет $\mu(\mu-1)/2$ вершин V_{ij} с двумя ненулевыми координатами $p_i = 1/2$, $p_j = 1/2$, $i, j \in \{1, 2, \ldots, \mu\}$, $i \neq j$. ■

В приложении к совершенным шифрам лемма 2 означает, что любой набор чисел p_i, $i = 1, \ldots, \mu$, с условиями (6) может быть набором априорных вероятностей шифробозначений совершенного шифра. Справедлива

Теорема 2. Набор чисел $p_1, \ldots, p_\mu$ при $\mu \geqslant 2$ является набором априорных вероятностей шифробозначений совершенного шифра в модели Σ_B с мощностью алфавита шифрвеличин, равной двум, тогда и только тогда, когда эти числа удовлетворяют условиям (6).

Доказательство. Необходимость. Пусть набор чисел $p_1, \ldots, p_\mu$ при $\mu \geqslant 2$ является набором априорных вероятностей шифробозначений совершенного шифра в модели Σ_B с мощностью алфавита шифрвеличин равной двум. Обозначим через $\sigma_Z^{(j)}$ сумму элементов j-й строки матрицы P_Z главной подматрицы со множеством строк Z. Так как $P_Z = T_Z/|Z|$, где T_Z соответствует дважды стохастической матрице, то

$$\sigma_Z^{(j)} = \begin{cases} 0, & j \notin Z, \\ 1, & j \in Z. \end{cases}$$

Имеем $\sigma_Z^{(j)} \leqslant 1/|Z| \leqslant 1/2$ при любом j, если диагональ нулевая и, стало быть, $|Z| \geqslant 2$. Суммируя все элементы j-й строки для определения p_j, из формулы (3) ввиду

$$P = \sum_{\substack{Z\subset\{1,2,\ldots,\mu\},\\ |Z|\geqslant 2}} \rho_Z P_Z$$

получаем формулу

$$p_j = \sum_{\substack{Z\subset\{1,2,\ldots,\mu\},\\ |Z|\geqslant 2}} \rho_Z \sigma_Z^{(j)} \leqslant \frac{1}{2}\sum_Z \rho_Z = \frac{1}{2},$$

поскольку из (2) сумма всех коэффициентов ρ_Z равна единице. Итак, априорные вероятности p_j $(j = 1, \ldots, \mu)$ совершенного шифра лежат в сегменте

$$0 \leqslant p_j \leqslant \frac{1}{2}.$$

Достаточность докажем путём построения симметричной матрицы. Пусть, в силу леммы 2, имеется разложение $P = \sum\limits_{i=1}^{\mu-1}\sum\limits_{j=i+1}^{\mu} r_{ij}V_{ij}$, в котором $\sum\limits_{i=1}^{\mu-1}\sum\limits_{j=i+1}^{\mu} r_{ij} = 1$, $r_{ij} \geqslant 0$, $1 \leqslant i < j \leqslant \mu$.

Сопоставляя каждой точке V_{ij} матрицу W_{ij}, у которой только два ненулевых элемента $w_{ij} = 1/2$ и $w_{ji} = 1/2$, построим симметричную матрицу P, лежащую в выпуклой оболочке этих матриц, как сумму $P = \sum\limits_{i=1}^{\mu-1}\sum\limits_{j=i+1}^{\mu} r_{ij}W_{ij}$. Для любого l, $1 \leqslant l \leqslant \mu$, выполняется равенство

$$p_l = \frac{1}{2}\sum\nolimits_{j=l+1}^{\mu} r_{ij} + \frac{1}{2}\sum_{i=1}^{l-1} r_{il},$$

и сумма элементов l-й строки (l-го столбца) матрицы P равна p_l, т. е. условия (1) и (2) выполнены. ■

Заключение

Таким образом, в работе описано множество (полиэдр) матриц вероятностей ключей и множество априорных вероятностей шифробозначений неэндоморфных максимальных совершенных шифров с двумя шифрвеличинами. Отметим, что в случае, когда мощность множества шифрвеличин строго больше двух, эта задача сильно усложняется по причине отсутствия аналога теоремы Биркгофа о дважды стохастических матрицах.

Получение обобщений теоремы Шеннона на неэндоморфные совершенные шифры с неравновероятными ключами и шифробозначениями оправдано изучением современных аналогов совершенных шифров [3], обладающих такими свойствами, как имитостойкость и помехоустойчивость, с более полным учётом свойств канала связи.

ЛИТЕРАТУРА

1. *Шеннон К.* Теория связи в секретных системах // Работы по теории информации и кибернетике. М.: Наука, 1963. С. 333–402.
2. *Андреев Н. Н., Петерсон А. П., Прянишников К. В., Старовойтов А. В.* Основоположник отечественной засекреченной телефонной связи // Радиотехника. 1998. № 8. С. 8–12.
3. *Зубов А. Ю.* Совершенные шифры. М.: Гелиос АРВ, 2003. 160 с.
4. *Stinson D. R.* A construction for authentication secrecy codes from certain combinatorial designs // Proc. Crypto'87. Advances in Cryptology. 1998. P. 355–366.

5. *De Soete M.* Some constructions for authentication-secrecy codes // Proc. Crypto'87. Advances in Cryptology. 1998. P. 57–75.
6. *Goldlewsky P. and Mitchell C.* Key-minimal cryptosystems for unconditional secrecy // J. Cryptology. 1990. No. 1. P. 1–25.
7. *Алферов А. П., Зубов А. Ю., Кузьмин А. С., Черемушкин А. В.* Основы криптографии. М.: Гелиос АРВ, 2001. 480 с.
8. *Бабаш А. В., Шанкин Г. П.* Криптография (аспекты защиты). М.: СОЛОН-Р, 2002. 512 с.
9. *Брассар Ж.* Современная криптология. М.: ПОЛИМЕД, 1999. 176 с.
10. *Stinson D. R.* Cryptography: Theory and Practice. N. Y.: CRC Press, 1995. 616 p.
11. *Birkhoff G. D* Tres observations sobre el algebra lineal // Revista Universidad Nacional Tucuman. 1946. Ser. A. V. 5. P. 147–151.
12. *Медведева Н. В., Титов С. С.* О неминимальных совершенных шифрах // Прикладная дискретная математика. Приложение. 2013. № 6. С. 42–44.
13. *Медведева Н. В., Титов С. С.* Неэндоморфные совершенные шифры с двумя шифрвеличинами // Прикладная дискретная математика. Приложение. 2015. № 8. С. 63–66.
14. *Гантмахер Ф. Р.* Теория матриц. М.: Наука, 1967. 576 с.
15. *Носов В. А., Сачков В. Н., Тараканов В. Е.* Комбинаторный анализ (неотрицательные матрицы, алгоритмические проблемы) // Итоги науки и техники. Сер. Теор. вероятн. Мат. стат. Теор. кибернет. Т. 21. М.: ВИНИТИ, 1983. С. 120–178.
16. *Converse G. and Katz M.* Symmetric matrices with given row sums // J. Combin. Theory. 1975. Ser. A. V. 18. No. 2. P. 171–176.
17. *Lewin M.* On the extreme points of the polytope of symmetric matrices with given row sums // J. Combin. Theory. 1977. Ser. A. V. 23. No. 2. P. 223–231.
18. *Koontz M.* Convex sets of some doubly stochastic matrices // J. Combin. Theory. 1978. Ser. A. V. 24. No. 1. P. 111–112.

REFERENCES

1. *Shennon K.* Teoriya svyazi v sekretnykh sistemakh [Communication theory of secrecy systems]. Raboty po Teorii Informatsii i ibernetike. Moscow, Nauka Publ., 1963, pp. 333–402. (in Russian)
2. *Andreev N. N., Peterson A. P., Pryanishnikov K. V., Starovoytov A. V.* Osnovopolozhnik otechestvennoy zasekrechennoy telefonnoy svyazi [The founder of the national classified telephone]. Radiotekhnika, 1998, no. 8, pp. 8–12. (in Russian)
3. *Zubov A. Yu.* Sovershennye shifry [Perfect Ciphers]. Moscow, Gelios ARV Publ., 2003. 160 p. (in Russian)
4. *Stinson D. R.* A construction for authentication secrecy codes from certain combinatorial designs. Proc. Crypto'87. Advances in Cryptology, 1998, pp. 355–366.
5. *De Soete M.* Some constructions for authentication-secrecy codes. Proc. Crypto'87. Advances in Cryptology, 1998, pp. 57–75.
6. *Goldlewsky P. and Mitchell C.* Key-minimal cryptosystems for unconditional secrecy. J. Cryptology, 1990, no. 1, pp. 1–25.
7. *Alferov A. P., Zubov A. Yu., Kuzmin A. S., Cheremushkin A. V.* Osnovy kriptografii [Basics of cryptography]. Moscow, Gelios ARV Publ., 2001. 480 p. (in Russian)
8. *Babash A. V., Shankin G. P.* Kriptografiya (aspekty zashchity) [Cryptography (protection aspects)]. Moscow, SOLON-R Publ., 2002. 512 p. (in Russian)
9. *Brassar Zh.* Sovremennaya kriptologiya [Modern Cryptology]. Moscow, POLIMED, 1999. 176 p. (in Russian)
10. *Stinson D. R.* Cryptography: Theory and Practice. N. Y., CRC Press, 1995. 616 p.

11. *Birkhoff G. D* Tres observations sobre el algebra lineal. Revista Universidad Nacional Tucuman, 1946, ser. A, vol. 5, pp. 147–151.
12. *Medvedeva N. V., Titov S. S.* O neminimal'nykh sovershennykh shifrakh [On non-minimal perfect ciphers]. Prikladnaya diskretnaya matematika. Prilozhenie, 2013, no. 6, pp. 42–44. (in Russian)
13. *Medvedeva N. V., Titov S. S.* Neendomorfnye sovershennye shifry s dvumya shifrvelichinami [Non-endomorphic perfect ciphers with two elements in plaintext alphabet]. Prikladnaya diskretnaya matematika. Prilozhenie, 2015, no. 8, pp. 63–66. (in Russian)
14. *Gantmacher F. R.* The Theory of Matrices. N. Y., Chelsea Publ. Company, 1959.
15. *Nosov V. A., Sachkov V. N., Tarakanov V. E.* Combinatorial analysis (nonnegative matrices, algorithmic problems). J. Soviet Math., 1985, vol. 29, no. 1, pp. 1051–1099.
16. *Converse G. and Katz M.* Symmetric matrices with given row sums. // J. Combin. Theory, 1975, ser. A, vol. 18, no. 2, pp. 171–176.
17. *Lewin M.* On the extreme points of the polytope of symmetric matrices with given row sums. J. Combin. Theory, 1977, ser. A, vol. 23, no. 2, pp. 223–231.
18. *Koontz M.* Convex sets of some doubly stochastic matrices. J. Combin. Theory, 1978, ser. A, vol. 24, no. 1, pp. 111–112.