Об аналогах теоремы Шеннона для совершенных шифров

Н.В. Медведева
medvedeva@usurt.ru

Уральский государственный университет путей сообщения (Екатеринбург)

Аннотация

Исследуется проблема описания совершенных по Шеннону (абсолютно стойких к атаке по шифртексту) шифров. В терминах комбинаторного анализа выпуклых множеств многомерного пространства сформулированы и доказаны некоторые обобщения (аналоги) теоремы Шеннона для совершенных по Шеннону неминимальных шифров. Построены примеры, подчеркивающие нетривиальность данной задачи.

Ключевые слова: совершенные шифры; неэндоморфные шифры; неминимальные шифры.

1 Введение

Разрабатывая теорию криптографической стойкости, К. Шеннон ввел понятие совершенного шифра как шифра, абсолютно стойкого к атаке по шифртексту [1]. Такой шифр не дает криптоаналитику никакой дополнительной информации об открытом тексте при изучении перехваченной криптограммы. Примерно в те же годы концепция совершенного шифра также разрабатывалась в одной закрытой работе под руководством В. А. Котельникова [2, 3].

В основе изучения совершенных шифров лежит математическая модель шифра. Впервые вероятностная модель шифра Σ_B рассмотрена в фундаментальной работе К. Шеннона [1]. Имеются и другие подходы к построению таких моделей [3]–[10]. В [3] предлагается некоторая модификация модели, приведенной в [9]. 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, причем $|X| = \lambda$, $|Y| = \mu$, $|K| = \pi$, где $\lambda > 1$, $\mu \geq \lambda$. Это означает, что открытые и шифрованные тексты представляются словами (ℓ-граммами, $\ell \geq 1$) в алфавитах X и Y соответственно. Согласно [3, 9], 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 табличного гаммирования со случайной равновероятной гаммой.

In: G.A. Timofeeva, A.V. Martynenko (eds.): Proceedings of 3rd Russian Conference "Mathematical Modeling and Information Technologies" (MMIT 2016), Yekaterinburg, Russia, 16-Nov-2016, published at http://ceur-ws.org

Существование *неэндоморфных* ($|X| < |Y|$) совершенных шифров [3, пример 2.2.10], а также шифров, минимальных не по числу ключей, а по включению (т. е. шифров, содержащих минимально возможное множество ключей зашифрования с ненулевыми вероятностями) оправдывает получение аналогов (обобщений) теоремы Шеннона для других совершенных шифров. К этому также приводит задача изучения минимальных (по включению) транзитивных шифров, так как совершенный шифр является транзитивным. Допускает обобщение и само понятие совершенного по Шеннону шифра, что подтверждается изучением современных аналогов совершенных шифров [3, 11].

Данная работа является продолжением исследования [12]–[15] проблемы описания совершенных по Шеннону шифров. Здесь в терминах комбинаторного анализа выпуклых множеств многомерного пространства сформулированы и доказаны некоторые обобщения (аналоги) теоремы Шеннона для совершенных по Шеннону *неминимальных* ($|K| > |Y|$) шифров. Нетривиальность задачи подчеркивают содержащиеся в работе примеры, показывающие, что даже для эндоморфных совершенных по Шеннону неминимальных шифров нет прямого аналога теоремы Шеннона.

2 Постановка задачи

Рассмотрим неэндоморфный неминимальный совершенный шифр. Пусть $X = \{x_1, x_2, \ldots, x_\lambda\} = \{1, 2, ..., \lambda\}$ — 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 $|X| = \lambda$, $|Y| = \mu \geq \lambda$, $|K| = \pi \geq \mu$.

Для обобщений теоремы Шеннона и построения примеров шифров будем использовать вероятностную модель Σ_B, в которой, согласно подходу [3, 9], шифр задается распределением вероятностей ключей при $\ell = 1$.

Как для эндоморфного шифра ($\lambda = \mu$), так и для неэндоморфного ($\lambda < \mu$), перечисляются в некотором порядке все возможные $\pi = \mu(\mu-1)...(\mu-\lambda+1)$ подстановки (инъекции) зашифрования, соответствующие ключам $k \in K$ и их вероятностям P_k. Получившийся π-мерный набор P вероятностей P_k ключей будем рассматривать как точку π-мерного пространства $\mathbf{R}^\pi$. Распределение биграмм, триграмм и т. д. может задаваться распределениями вероятностей и при $\ell = 2, 3, ...$

Задача описания шифров в вероятностной модели Σ_B приводит к описанию множества точек в π-мерном пространстве $\mathbf{R}^\pi$, которые являются распределениями вероятностей того или иного шифра. В работах [12]–[14] описано выпуклое множество (полиэдр [16]) матриц вероятностей ключей и множество вероятностей шифробозначений неэндоморфных совершенных шифров в случае, когда мощность λ множества шифрвеличин равна двум.

По теореме Шеннона, минимальные по числу ключей эндоморфные совершенные шифры соответствуют тем точкам пространства $\mathbf{R}^\pi$, у которых все координаты равны нулю, кроме λ ненулевых координат, равных $1/\lambda$, а сам набор координат соответствует набору ключей, подстановки которых образуют латинский квадрат. Поскольку множество точек π-мерного пространства $\mathbf{R}^\pi$, соответствующих совершенным шифрам, образует выпуклое множество (полиэдр), то и выпуклая оболочка точек, соответствующих латинским квадратам (шифрам Шеннона), также соответствует совершенным шифрам.

Требуется установить: будет ли полученный таким образом полиэдр множеством распределений всех эндоморфных совершенных шифров и сводится ли задача описания минимальных (по включению) совершенных шифров к задаче описания минимальных (по включению) транзитивных шифров.

3 Об описании эндоморфных совершенных шифров

Для $\lambda = \mu \in \{2, 3\}$ ответ на поставленный вопрос – положительный. При $\lambda = \mu = 2$ – это классический шифр Вернама с суммированием бита открытого текста и бита ключевого потока по модулю 2. При $\lambda = \mu = 3$ и $K = \{k_1, k_2, ..., k_6\}$ таблица зашифрования со всеми $\pi = 3! = 6$ подстановками из $X = \{x_1, x_2, x_3\}$ в $Y = \{1, 2, 3\}$ – это таблица 1, в которой точки $\mathsf{P}^{(1)}$ и $\mathsf{P}^{(2)}$ соответствуют латинским квадратам.

Утверждение 1. Любой эндоморфных совершенный шифр с мощностью множества шифрвеличин, равной трем, задается распределением вероятностей

$$\mathsf{P} = \alpha\,\mathsf{P}^{(1)} + \beta\,\mathsf{P}^{(2)} = \alpha\left(\frac{1}{3}, 0, 0, \frac{1}{3}, \frac{1}{3}, 0\right)^T + \beta\left(0, \frac{1}{3}, \frac{1}{3}, 0, 0, \frac{1}{3}\right)^T = \left(\frac{\alpha}{3}, \frac{\beta}{3}, \frac{\beta}{3}, \frac{\alpha}{3}, \frac{\alpha}{3}, \frac{\beta}{3}\right)^T,$$

$\alpha, \beta \geq 0,\ \alpha + \beta = 1$, лежащим в выпуклой оболочке точек $\mathsf{P}^{(1)}, \mathsf{P}^{(2)} \in \mathbf{R}^6$.

Таблица 1: Совершенный шифр при $\lambda = \mu = 3$

№	K	x_1	x_2	x_3	P_k	$\mathsf{P}_k^{(1)}$	$\mathsf{P}_k^{(2)}$
1	k_1	1	2	3	P_1	1/3	0
2	k_2	1	3	2	P_2	0	1/3
3	k_3	2	1	3	P_3	0	1/3
4	k_4	2	3	1	P_4	1/3	0
5	k_5	3	1	2	P_5	1/3	0
6	k_6	3	2	1	P_6	0	1/3

Согласно Утверждению 1, для $\lambda = \mu = 3$ искомое выпуклое множество (полиэдр) – отрезок в шестимерном пространстве.

Утверждение 2. Априорные вероятности шифробозначений эндоморфного совершенного шифра одинаковы и равны $\frac{1}{\lambda}$.

Доказательство. Для данного шифра условия совершенности по Шеннону в вероятностной модели шифра Σ_B (т. е. условие для ℓ-грамм при $\ell = 1$) [3] образуют однородную систему λ^2 линейных уравнений относительно $\lambda! + \lambda = \lambda(\lambda - 1)!$ неизвестных вероятностей ключей и априорных вероятностей $p_i, i = 1, 2, ..., \lambda$ шифробозначений. При этом первые λ уравнений данной системы, в которые входит p_1, содержат все вероятности ключей P_k, где $k \in K$. Действительно, вероятность $\mathsf{P}_k = \mathsf{P}_{y_1 y_2 \ldots y_\lambda}$ входит в m-ое уравнение, если в подстановке

$$e_k : \begin{pmatrix} 1 & 2 & ... & \lambda \\ y_1 & y_2 & ... & y_\lambda \end{pmatrix}$$

единица в нижней строке значений стоит на m-ом месте; а поскольку для каждой такой подстановки существует единственное такое $m \in \{1, 2, ..., \lambda\}$, то эта вероятность входит ровно один раз в первые λ уравнений. Ввиду того, что сумма всех вероятностей ключей равна единице, получаем, суммируя первые λ уравнений, что $1 = \lambda p_1$, откуда $p_1 = \frac{1}{\lambda}$. Повторяя это рассуждение для каждой априорной вероятности $p_i, i = 1, 2, ..., \lambda$ шифробозначений, находим

$$p_1 = p_2 = ... = p_\lambda = \frac{1}{\lambda},$$

что и требовалось доказать.

При $\lambda = \mu > 3$ выпуклая оболочка совершенных по Шеннону шифров с минимальным числом ключей является лишь частью множества точек, соответствующих совершенным шифрам, как показывает следующее

Утверждение 3. При $\lambda = \mu = 4$ существуют минимальные (по включению) совершенные шифры, не содержащие в себе наборов ключей (подстановок), образующих латинский квадрат.

Таблица 2: Совершенный шифр при $\lambda = \mu = 4$

№	K	x_1	x_2	x_3	x_4	P_k
1	k_1	1	2	3	4	1/4
2	k_2	2	4	1	3	1/8
3	k_3	3	1	4	2	1/8
4	k_4	4	3	1	2	1/8
5	k_5	3	4	2	1	1/8
6	k_6	2	3	4	1	1/8
7	k_7	4	1	2	3	1/8

Доказательство. Рассмотрим эндоморфный шифр в случае, когда мощность множества шифрвеличин равна четырем. Пусть $X = \{x_1, x_2, x_3, x_4\}$ – множество шифрвеличин; $Y = \{y_1, y_2, y_3, y_4\} = \{1, 2, 3, 4\}$ – множество шифробозначений, $K = \{k_1, k_2, \ldots, k_\pi\}$ – множество ключей. Таблица 2 – таблица зашифрования данного шифра, составленная из следующих подстановок – единичная и все шесть полноцикловых подстановок группы S_4, так что $\pi = 7$.

Легко проверяется, что это – совершенный эндоморфный шифр. Здесь полноцикловые подстановки f группы S_4 обладают свойством – для каждой подстановки f имеется ровно четыре различные другие полноцикловые подстановки g_i такие, что $f(i) = g_i(i), i = 1, 2, 3, 4$. Следовательно, максимальные четырехстолбцовые латинские прямоугольники в этой таблице состоят из трех строк вида e, f, f^{-1}, и латинских квадратов – нет.

Утверждение 4. Совершенный шифр – транзитивный [3]. Обратно неверно – не всякий транзитивный шифр является совершенным при некотором распределении вероятностей ключей.

Доказательство. Рассмотрим таблицы 3, 4 зашифрования эндоморфных шифров при $\lambda = \mu = 4$ с произвольными неизвестными вероятностями ключей. Это минимальные (по включению) транзитивные шифры, которые не могут быть совершенными ни при каких распределениях вероятностей ключей. Причем из их таблиц зашифрования невозможно извлечь латинский квадрат.

Таблица 3: Транзитивный шифр при $\lambda = \mu = 4$

№	K	x_1	x_2	x_3	x_4
1	k_1	1	4	3	2
2	k_2	1	3	2	4
3	k_3	2	1	3	4
4	k_4	3	2	4	1
5	k_5	4	2	1	3

Таблица 4: Транзитивный шифр при $\lambda = \mu = 4$

№	K	x_1	x_2	x_3	x_4
1	k_1	4	1	2	3
2	k_2	3	4	1	2
3	k_3	2	3	4	1
4	k_4	1	2	4	3
5	k_5	4	1	3	2
6	k_6	2	3	1	4

Действительно, в таблице 3 можно исключить только либо первую, либо только вторую строку. Если исключить первую, то в столбце для x_2 шифробозначение 2 встретится дважды, а шифробозначение 4 будет отсутствовать, а значит латинского квадрата не будет. Если же исключить вторую строку, то в столбце для x_2 шифробозначение 2 встретится дважды и не будет шифробозначения 3, т. е. снова останется не латинский квадрат. Аналогично проводятся рассуждения по исключению двух строк в таблице 4.

Таблица 5: Совершенный эндоморфный шифр при $\lambda = \mu = 4$

№	K	x_1	x_2	x_3	x_4	P_k
1	k_1	1	3	2	4	1/8
2	k_2	1	4	3	2	1/8
3	k_3	2	1	3	4	1/8
4	k_4	2	4	1	3	1/8
5	k_5	3	1	4	2	1/8
6	k_6	3	2	4	1	1/8
7	k_7	4	2	1	3	1/8
8	k_8	4	3	2	1	1/8

Утверждение 5. При $\lambda = \mu > 3$ существуют шифры с равновероятными ключами, не лежащие в выпуклой оболочке совершенных по Шеннону неминимальных по числу ключей шифров.

Доказательство. Рассмотрим совершенный эндоморфный шифр при $\lambda = \mu = 4$ с равновероятными

ключами и таблицей 5 зашифрования, не содержащей латинских квадратов и составленной из биекций (подстановок) группы S_4.

Действительно, в таблице 5 можно исключить или первую, или вторую строку. Если исключить первую, то вторая обязательно должна быть, а значит нужно исключить четвертую строку, чтобы шифробозначение 4 встречалось в столбце для x_2 один раз. Следовательно, нужно оставить третью строку, иначе в столбце для x_1 не будет шифробозначения 2. Вследствие этого получаем, что в столбце для x_3 шифробозначение 3 будет встречаться дважды, т. е. латинского квадрата не будет. Если же исключить вторую строку, то должна остаться первая, а значит нужно исключить восьмую строку, иначе шифробозначение 3 будет встречаться дважды в столбце для x_2. Следовательно, седьмая строка должна остаться, иначе в столбце для x_1 не будет шифробозначения 4. Вследствие этого нужно будет убрать шестую строку, иначе шифробозначение 2 в столбце для x_2 будет повторяться. Тогда получим, что в столбце для x_4 шифробозначения 1 не будет, т. е. останется не латинский квадрат. Это означает, что равновероятность ключей также не приводит к прямому обобщению теоремы Шеннона.

Согласно Утверждению 5, обобщение теоремы Шеннона в рассматриваемой постановке задачи неверно. Существуют шифры, выходящие за пределы рассматриваемой оболочки [16].

4 Об описании неэндоморфных совершенных шифров

Справедливо утверждение о дополнении неэндоморфного совершенного шифра до эндоморфного.

Утверждение 6. Латинский прямоугольник размерами $n \times (n-1)$, т. е. n строк, $(n-1)$ столбцов, заполненный величинами $1, 2, ..., n$, однозначно дополняется до латинского квадрата размерами $n \times n$.

Доказательство. Поскольку в строках латинского прямоугольника размера $n \times (n-1)$ величины $1, 2, ..., n$ не повторяются, то оставшуюся величину можно однозначно поместить в n-ый столбец. Получившийся квадрат не будет латинским, если в последнем столбце будут повторения.

Если на пересечении этого n-го столбца и каких либо двух строк находится одна и та же величина y, то некоторая величина $x \neq y$ из множества $\{1, 2, ..., n\}$ не встречается в этом столбце. Тогда эта величина x должна встретиться в каждой из n строк точно по одному разу в первых $(n-1)$-ой позициях. Следовательно, в исходном латинском прямоугольнике величина x входит n раз. Но так как столбцов в нём $n-1$, то x входит в какой-либо столбец два раза, что противоречит тому, что прямоугольник является латинским.

Утверждение 7. Любой неэндоморфный совершенный шифр с мощностью множества шифрвеличин, равной λ, мощностью множества шифробозначений, равной $\mu = \lambda + 1$, и одинаковыми априорными вероятностями шифробозначений, равными $1/\mu = 1/(\lambda+1)$, может быть расширен до эндоморфного совершенного шифра с мощностью множества шифрвеличин и шифробозначений, равными $\lambda + 1$.

Доказательство. Пусть дан неэндоморфный совершенный шифр с $|X| = \lambda$, $|Y| = \mu = \lambda + 1$ и $X = \{x_1, x_2, ..., x_\lambda\}$. Равенство $1/(\lambda+1)$ априорных вероятностей шифробозначений является необходимым условием, покажем, что оно является также и достаточным условием расширения данного шифра до совершенного эндоморфного шифра с $|\tilde{X}| = |Y| = \lambda + 1$.

Однозначно расширить данный шифр до эндоморфного шифра при $|\tilde{X}| = |Y| = \lambda+1$ можно добавлением биекции $\tilde{e}$ такой, что, если e – инъекция зашифрования исходного шифра, т. е.

$$e : X \to Y, \quad |X| = \lambda, \quad |Y| = \mu = \lambda + 1,$$

то $\tilde{e} : \tilde{X} = X \cup \{x_{\lambda+1}\} \to Y$ так, что

$$\tilde{e}(x) = \begin{cases} e(x) \text{ при } x \in X; \\ y, \text{ где } \{y\} = Y \backslash e(X) \text{ при } x = x_{\lambda+1}, \end{cases}$$

имеем $\tilde{e} : \tilde{X} \to Y$ (биекция), где $\tilde{X} = \{x_1, x_2, ..., x_\lambda, x_{\lambda+1}\}$.

Однозначно определенный таким образом шифр является совершенным, когда сумма вероятностей, соответствующих одному и тому же шифробозначению, равна $1/(\lambda+1)$ для каждого шифробозначения. Найдем

$$\mathsf{P}\{\tilde{e}(x_{\lambda+1}) = y\} = \mathsf{P}\{y \notin e(X)\} = \mathsf{P}\{e(x_1) \neq y \ \& \ e(x_2) \neq y \ \& \ ... \ \& \ e(x_\lambda) \neq y\} =$$

$$= 1 - [\mathsf{P}\{e(x_1) = y\} + \mathsf{P}\{e(x_2) = y\} + ... + \mathsf{P}\{e(x_\lambda) = y\}] = 1 - \left(\frac{1}{\lambda+1} + \frac{1}{\lambda+1} + ... + \frac{1}{\lambda+1}\right) = 1 - \frac{\lambda}{\lambda+1} = \frac{1}{\lambda+1},$$

т. е. расширенный единственным образом шифр будет совершенным.

5 Заключение

Таким образом, рассмотрена задача обобщения теоремы Шеннона для совершенных по Шеннону шифров, в том числе неэндоморфных. Нетривиальность задачи подчеркивают содержащиеся в работе контрпримеры, показывающие, что даже для эндоморфных совершенных по Шеннону неминимальных шифров нет прямого обобщения (аналога) теоремы Шеннона. Построенные в работе примеры также показывают, что минимальность по числу ключей и минимальность по включению приводят к разным постановкам задач, требующих проведения дополнительных исследований для формулировки соответствующих аналогов теоремы Шеннона.

Список литературы

[1] K. Shannon. The theory of secret communication systems. *Works on information theory and cybernetics. M.: Nauka*, 333–402, 1963.

[2] N. N. Andreev, A. P. Peterson, K. V. Pryanishnikov, A. V. Starovoytov. The founder of the national classified telephone. *Radiotechnics*, 8:8–12, 1998. (in Russian) = Н. Н. Андреев, А. П. Петерсон, К. В. Прянишников, А. В. Старовойтов. Основоположник отечественной засекреченной телефонной связи. *Радиотехника*, 8:8–12, 1998.

[3] A. Y. Zubov. *Perfect ciphers*. Moscow, Helios ART, 2003. (in Russian) = А. Ю. Зубов *Совершенные шифры*. Москва, Гелиос АРВ, 2003.

[4] P. Goldlewsky, C. Mitchell. Key-minimal cryptosystems for unconditional secrecy. *J. Cryptology*, 1:1–25, 1990.

[5] D. R. Stinson. *Cryptography: Theory and Practice*. N. Y., CRC Press, 1995.

[6] M. De Soete. Some constructions for authentication-secrecy codes. *Proc. Crypto'87. Advances in Cryptology*:57–75, 1998.

[7] D. R. Stinson. A construction for authentication secrecy codes from certain combinatorial designs. *Proc. Crypto'87. Advances in Cryptology*:355–366, 1998.

[8] J. Brassar. *Modern cryptology*. Moscow, POLYMEDIA, 1999. (in Russian) = Ж. Брассар. *Современная криптология*. Москва, ПОЛИМЕД, 1999.

[9] A. P. Alferov, A. Y. Zubov, A. S. Kuzmin, A. V. Cherëmushkin. *Basics of cryptography*. Moscow, Helios ART, 2001. (in Russian) = А. П. Алферов, А. Ю. Зубов, А. С. Кузьмин, А. В. Черемушкин. *Основы криптографии*. Москва, Гелиос АРВ, 2001.

[10] A. V. Babash, G. P. Shankin. *Cryptography (aspects of protection)*. Moscow, SOLON-P, 2002. (in Russian) = А. В. Бабаш, Г. П. Шанкин. *Криптография (аспекты защиты)*. Москваб СОЛОН-Р, 2002.

[11] D. S. Gutarin, S. S. Konovalova, V. I. Timin, E. S. Titov, S. S. Titov. Combinatorial problems of the existence of perfect ciphers. *Trudy Inst. Mat. i Mekh. UrO RAN*, 4:61–73, 2008. (in Russian) = Д. С. Гутарин, С. С. Коновалова, В. И. Тимин, Е. С. Титов, С. С. Титов. Комбинаторные проблемы существования совершенных шифров. *Труды ИММ УрО РАН*, 4:61–73, 2008.

[12] N. V. Medvedeva, S. S. Titov. On non-endomorphic perfect ciphers. *Applied discrete mathematics. Application*,6:42–44, 2013. (in Russian) = Н. В. Медведева, С. С. Титов. О неминимальных совершенных шифрах. *Прикладная дискретная математика. Приложение*, 6:42–44, 2013.

[13] N. V. Medvedeva, S. S. Titov. Non-endomorphic perfect ciphers with two plaintext value. *Applied discrete mathematics. Application*, 8:63–66, 2015. (in Russian) = Н. В. Медведева, С. С. Титов. Неэндоморфные совершенные шифры с двумя шифрвеличинами. *Прикладная дискретная математика. Приложение*, 8:63–66, 2015.

[14] N. V. Medvedeva, S. S. Titov. Description non-endomorphic maximum perfect ciphers with two plaintext value. *Applied discrete mathematics*, 4(30):43–55, 2015. = Н. В. Медведева, С. С. Титов. Описание неэндоморфных максимальных совершенных шифров с двумя шифрвеличинами. *Прикладная дискретная математика*, 4(30):43–55, 2015.

[15] N. V. Medvedeva, S. S. Titov. Analogues of the Shannon theorem for non-minimal endomorphic perfect ciphers. *Applied discrete mathematics. Application*, 9:62–65, 2016. (in Russian) = Н. В. Медведева, С. С. Титов. Аналоги теоремы Шеннона для эндоморфных неминимальных шифров. *Прикладная дискретная математика. Приложение*, 9:62–65, 2016.

[16] V. A. Nosov, V. N. Sachkov, V. E. Tarakanov. Combinatorial analysis (non-negative matrix, algorithmic problems). *The results of science and technology. Ser. Probability theory. Math statistics. Theor. Cybernetics., 18, M.: VINITI*, 21:120–178, 1983. (in Russian) = В. А. Носов, В. Н. Сачков, В. Е. Тараканов. Комбинаторный анализ (неотрицательные матрицы, алгоритмические проблемы). *Итоги науки и техн. Сер. Теор. вероятн. Мат. стат. Теор. кибернет. М.: ВИНИТИ*, 21:120–178, 1983.

On analogs of the Shannon's theorem for perfect ciphers

Natal'ya V. Medvedeva
Ural State University of Railway Transport (Yekaterinburg, Russia)

Abstract. The article is devoted to the problem of description of general perfect ciphers (which are absolutely immune against the attack on ciphertext, according to Shannon). In terms of combinatorial analysis of convex sets in multidimensional space some analogs of the theorem of Shannon for non-minimal ciphers are formulated and proved. The examples emphasizing non-triviality of this task are constructed.

Keywords: perfect ciphers, non-endomorphic ciphers, non-minimal ciphers.