Таким образом, доказано

Утверждение 1. Разделяющий матроид является однородным матроидом с трёхэлементными когиперплоскостями тогда и только тогда, когда его когиперплоскости образуют систему троек Штейнера, т. е. $k = 3$ и $\lambda = 1$.

Итак, в работе показана связь однородных матроидов с тройками Штейнера. Описанный метод может быть применён к решению более сложных задач обобщения связи матроидов с блок-схемами с $\lambda = 1$, согласно выдвинутой ранее гипотезе.

ЛИТЕРАТУРА

1. Введение в криптографию / под общ. ред. В. В. Ященко. СПб.: Питер, 2001.
2. *Блейкли Г. Р., Кабатянский Г. А.* Обобщенные идеальные схемы, разделяющие секрет, и матроиды // Проблемы передачи информации. 1997. Т. 33. № 3. С. 102–110.
3. *Парватов Н. Г.* Совершенные схемы разделения секрета // Прикладная дискретная математика. 2008. №2 (2). С. 50–57.
4. *Welsh D. J. A.* Matroid Theory. Academic Press, 1976.
5. *Marti-Farre J. and Padro C.* Secret sharing schemes on sparse homogeneous access structures with rank three // Electronic J. Combinatorics. 2004. No. 1 (1). Research Paper 72. 16 p.
6. *Алексейчук А. Н.* Совершенные схемы разделения секрета и конечные универсальные алгебры // Реєстрація, зберігання і оброб. даних. 2005. Т. 7. № 2. С. 55–65.
7. *Alekseychuk A. N.* Lattice-Theoretic Characterization of Secret Sharing Representable Connected Matroids. Cryptology ePrint Archive: Report 2010/348.
8. *Холл М.* Комбинаторика. М.: Мир, 1970.
9. *Медведев Н. В., Титов С. С.* Об однородных матроидах и блок-схемах // Прикладная дискретная математика. Приложение. 2017. № 10. С. 21–23.

УДК 512.64, 519.21, 519.72 DOI 10.17223/2226308X/12/35

ГЕОМЕТРИЧЕСКАЯ МОДЕЛЬ СОВЕРШЕННЫХ ШИФРОВ С ТРЕМЯ ШИФРВЕЛИЧИНАМИ

Н. В. Медведева, С. С. Титов

Рассматривается проблема описания совершенных по Шеннону (абсолютно стойких к атаке по шифртексту) шифров с мощностью шифрвеличин равной трём. Показано, что не существует минимальных по включению совершенных шифров с четырьмя шифробозначениями и пятью или шестью ключами зашифрования. Определено количество минимальных по включению совершенных шифров, содержащих семь ключей зашифрования, а также количество совершенных шифров с числом ключей равным восьми. Построены примеры минимальных по включению совершенных шифров.

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

Рассмотрим вероятностную модель Σ_B шифра [1 – 3]. 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*. 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 табличного гаммирования со случайной равновероятной гаммой.

Данная работа является продолжением исследования [4] проблемы описания совершенных по Шеннону шифров. Здесь для обобщений теоремы Шеннона и построения примеров используется вероятностная модель Σ_B шифра, в которой, согласно подходу [2, 3], шифр задаётся распределением вероятностей ключей при $\ell = 1$.

Для эндоморфного ($X = Y$) и неэндоморфного ($|X| < |Y|$) шифров перечисляются в некотором порядке все возможные $\pi_{\max} = \mu(\mu - 1) \cdot \ldots \cdot (\mu - \lambda + 1)$ инъекций зашифрования, соответствующие ключам $k \in K$ и их вероятностям P_k. При этом допускается, что некоторые вероятности P_k могут быть равны нулю. Это означает, что соответствующая инъекция не используется в данном шифре. Получившийся $\pi_{\max}$-мерный набор P вероятностей P_k ключей будем рассматривать как точку $\pi_{\max}$-мерного пространства $\mathbb{R}^{\pi_{\max}}$. Распределение биграмм, триграмм и т. д. может задаваться распределениями вероятностей при $\ell = 2, 3, \ldots$, что приводит к усложнению геометрической модели.

Задача описания шифров в вероятностной модели Σ_B приводит к описанию множества точек в пространстве $\mathbb{R}^{\pi_{\max}}$, которые являются распределениями вероятностей ключей того или иного шифра.

По теореме Шеннона, минимальные по числу ключей эндоморфные совершенные шифры соответствуют тем точкам пространства $\mathbb{R}^{\pi_{\max}}$, у которых все координаты равны нулю, кроме λ ненулевых координат, равных $1/\lambda$, а сам набор координат соответствует набору ключей (инъекций), образующих латинский квадрат. Поскольку множество точек пространства $\mathbb{R}^{\pi_{\max}}$, соответствующих совершенным шифрам, образует выпуклое множество (полиэдр [5]), то и выпуклая оболочка этих точек также соответствует совершенным шифрам. Однако могут быть совершенные шифры, соответствующие точкам вне этой выпуклой оболочки.

В работе [4] показано, что 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 [6]. В [4] описано выпуклое множество (полиэдр) матриц вероятностей ключей и множество вероятностей шифробозначений неэндоморфных совершенных шифров в случае, когда мощность множества шифрвеличин равна двум. Полиэдр описан через указание его вершин (экстремальных точек), которые представляют собой так называемые нормальные циклы.

В [7] в терминах комбинаторного анализа выпуклых множеств многомерного пространства сформулированы и доказаны некоторые обобщения (аналоги) теоремы Шеннона для совершенных по Шеннону эндоморфных неминимальных ($|K| > |Y|$) шифров. В частности, показано, что для любого эндоморфного совершенного шифра с мощностью множества шифрвеличин $\lambda = \mu = 3$ искомый полиэдр — это отрезок в шестимерном пространстве. Построены примеры, показывающие, что минимальность шифра по числу ключей и минимальность по включению (т. е. шифры, содержащие минимально возможное множество ключей зашифрования с ненулевыми вероятностями) приводят к разным постановкам задач обобщения теоремы Шеннона. Неэндоморфные совершенные шифры с $\lambda = 3$ и $\mu = 4$ дополняются до эндоморфных, и притом единственным образом.

Утверждение 1. При $\pi = 5$ или 6 не существует минимальных по включению совершенных шифров.

Утверждение 2. При $\pi = 7$ существует $4! = 24$ минимальных по включению совершенных шифров.

Все такие шифры получены перестановкой столбцов в таблице зашифрования эндоморфного совершенного шифра, составленной из единичной подстановки и всех шести полноцикловых подстановок группы S_4 [7] (табл. 1).

Утверждение 3. При $\pi = 8$ существует $4 \cdot 4! = 96$ минимальных по включению совершенных шифров.

Рассмотрим восемь подстановок (табл. 2), где $\{a, b, c, d\} = \{1, 2, 3, 4\}$. Данное множество подстановок не содержит латинских квадратов. Перестановкой столбцов и переименованием элементов a, b, c, d снова получаются восемь подстановок ключей с вероятностями 1/8.

Таблица 1

№	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

Таблица 2

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

В случае равновероятных шифробозначений совершенный шифр с мощностью множества шифрвеличин, равной трём, и $\mu > 4$ может быть дополнен до эндоморфного, но не едиственным способом.

Пример 1. Рассмотрим неэндоморфный шифр с множеством из трёх шифрвеличин. Пусть $X = \{x_1, x_2, x_3\} = \{1, 2, 3\}$ — множество шифрвеличин; $Y = \{y_1, y_2, y_3, y_4, y_5\} = \{1, 2, 3, 4, 5\}$ — множество шифробозначений; $K = \{k_1, k_2, \ldots, k_\pi\}$ — множество ключей. Таблица зашифрования данного шифра (табл. 3) не содержит латинских прямоугольников размера 5×3.

Таблица 3

№	K	x_1	x_2	x_3	P_k
1	k_1	1	2	3	1/5
2	k_2	2	3	4	1/10
3	k_3	2	1	5	1/10
4	k_4	3	4	5	1/10
5	k_5	3	5	1	1/10
6	k_6	4	5	2	1/10
7	k_7	4	3	1	1/10
8	k_8	5	1	4	1/10
9	k_9	5	4	2	1/10

Это совершенный эндоморфный шифр, дополняемый двумя способами (при фиксировании первой строки) до эндоморфного совершенного шифра с $\lambda = \mu = 5$ без латинских квадратов (табл. 4 и 5).

Таблица 4

№	K	x_1	x_2	x_3	x_4	x_5	P_k
1	k_1	1	2	3	4	5	1/5
2	k_2	2	3	4	5	1	1/10
3	k_3	2	1	5	3	4	1/10
4	k_4	3	4	5	1	2	1/10
5	k_5	3	5	1	2	4	1/10
6	k_6	4	5	2	1	3	1/10
7	k_7	4	3	1	5	2	1/10
8	k_8	5	1	4	2	3	1/10
9	k_9	5	4	2	3	1	1/10

Таблица 5

№	K	x_1	x_2	x_3	x_4	x_5	P_k
1	k_1	1	2	3	4	5	1/5
2	k_2	2	3	4	5	1	1/10
3	k_3	2	1	5	3	4	1/10
4	k_4	3	4	5	1	2	1/10
5	k_5	3	5	1	2	4	1/10
6	k_6	4	5	2	3	1	1/10
7	k_7	4	3	1	5	2	1/10
8	k_8	5	1	4	3	2	1/10
9	k_9	5	4	2	1	3	1/10

Таким образом, в работе рассмотрена задача построения геометрической модели совершенных по Шеннону шифров с мощностью множества шифрвеличин равной трём. Показано, что не существует минимальных по включению совершенных шифров с четырьмя шифробозначениями и пятью или шестью ключами зашифрования. Определено количество минимальных по включению совершенных шифров, содержащих семь ключей зашифрования, а также количество совершенных шифров с числом ключей равным восьми. Построены примеры минимальных по включению совершенных шифров.

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.* Описание неэндоморфных максимальных совершенных шифров с двумя шифрвеличинами // Прикладная дискретная математика. 2015. № 4 (30). С. 43–55.
5. *Носов В. А., Сачков В. Н., Тараканов В. Е.* Комбинаторный анализ (неотрицательные матрицы, алгоритмические проблемы) // Итоги науки и техн. Сер. Теор. вероятн. Мат. стат. Теор. Кибернет. Т. 21. М.: ВИНИТИ, 1977. С. 120–178.
6. *Birkhoff G. D.* Tres observations sobre el algebra lineal // Revista Universidad Nacional Tucuman. 1946. Ser. A. V. 5. P. 147–151.
7. *Медведева Н. В., Титов С. С.* Аналоги теоремы Шеннона для эндоморфных неминимальных шифров // Прикладная дискретная математика. Приложение. 2016. № 9. С. 62–65.