5. *Courtois N.* The Security of Cryptographic Primitives based on Multivariate Algebraic Problems. Ph.D. Thesis, Paris, 2001.
6. *Bard G.* Algebraic Cryptanalysis. Springer, 2009. 356 p.
7. *Courtois N. and Bard G. V.* Algebraic cryptanalysis of the data encryption standard // LNCS. 2007. V. 4887. P. 152–169.
8. *Albrecht M., Brickenstein M., and Soos M.* An ANF to CNF Converter using a Dense/Sparse Strategy. `https://doc.sagemath.org/html/en/reference/sat/sage/sat/converters/polybori.html`.
9. *Soos M.* The CryptoMiniSat 5 set of solvers at SAT competition 2016 // Proc. SAT Competition. Helsinki, 2016. P. 28.
10. *Biere A.* CaDiCaL, Lingeling, Plingeling, Treengeling, YalSAT entering the SAT Competition 2017 // Proc. SAT Competition. Helsinki, 2017. P. 14–15.
11. *Raddum H. and Semaev I.* New Technique for Solving Sparse Equation Systems. IACR Cryptology ePrint Archive, 2006/475, 2006.
12. *Biere A.* New technique for solving sparse equation systems // Des. Codes Cryptogr. 2008. V. 49. No. 1–3. P. 47–60.

УДК 512.64, 519.21, 519.72 DOI 10.17223/2226308X/14/20

К ЗАДАЧЕ ОПИСАНИЯ МИНИМАЛЬНЫХ ПО ВКЛЮЧЕНИЮ СОВЕРШЕННЫХ ШИФРОВ

Н. В. Медведева, С. С. Титов

Исследуются совершенные по Шеннону (абсолютно стойкие к атаке по шифртексту) шифры. На множестве ключей шифра определён граф эквивалентности ключей. Для шифра доказано достаточное условие его минимальности по включению. Построены примеры.

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

Рассматривается вероятностная 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 $\lambda > 1$, $\mu \geqslant \lambda$. 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*.

Получение строгих доказуемых оценок стойкости для каждого конкретного шифра — это очень сложная, актуальная и до конца не решённая проблема криптоанализа. Различают теоретическую и практическую стойкость шифров (оцениваемую через ресурсы, требуемые на взлом), которую естественно описывать как вероятность успеха в противодействии атакам различного вида. Здесь впечатляющим результатом представляется теорема Шеннона [1] о совершенных (абсолютно стойких к атакам по шифртексту) шифрах, которую можно (нестрого) сформулировать так: атака по шифртексту на совершенный шифр бессмысленна, так как пассивный злоумышленник, перехватив зашифрованный текст, не получает никакой информации (кроме длины сообщения) об исходном открытом тексте. Но совершенный шифр не стоек к атакам

активного злоумышленника (который может подменить или модифицировать сообщение).

Перспективным является изучение шифров, близких к совершенным, в том числе «приближённо совершенных» [4, 5]. Для таких шифров теорему Шеннона можно переформулировать — в виде теоремы А. Ю. Зубова — следующим образом: атака по шифртексту на почти совершенный шифр почти бессмысленна. При этом такие шифры приобретают дополнительные полезные свойства. Современные аналоги совершенных шифров пытаются бороться с атаками имитации и подмены, отказываясь от эндоморфности ($\lambda = \mu$), внося информационную избыточность за счёт имитовставок и других приёмов, в том числе повышающих помехоустойчивость. Однако эта проблематика в данный момент не считается центральной — например, потому, что имеется много других более актуальных назревших нерешённых задач. Тем более что она признаётся достаточно сложной, но остающейся в поле зрения исследователей в связи с другими смежными комбинаторными задачами. Кроме этого, данные исследования могут быть применены для обобщений на почти совершенные шифры.

Описание эндоморфных с минимально возможным числом ключей ($|K| = |Y|$) совершенных шифров даётся теоремой 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 $\mu \times \lambda$ [6]. 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 [7]. Если $\lambda > 2$, то даже для равновероятных инъекций зашифрования неэндоморфный совершенный шифр может не содержать в своей таблице зашифрования латинских прямоугольников $\mu \times \lambda$ [8].

Описание минимальных по включению (т. е. шифров, содержащих минимально возможное множество ключей зашифрования с ненулевыми вероятностями) неэндоморфных совершенных шифров, не сводящихся к латинским прямоугольникам размера $\mu \times \lambda$, может быть осуществлено с помощью конструкций таблиц зашифрования, не содержащих латинских прямоугольников. Первый этап реализации данного подхода — это построение таких конструкций для шифробозначений, априорные вероятности которых считаются равными.

В работе [9] на основе отношения эквивалентности на множестве ключей получены достаточные условия того, что в таблице зашифрования неэндоморфных (эндоморфных) совершенных шифров отсутствуют латинские прямоугольники (квадраты). В частности, получены достаточные условия того, что таблицы зашифрования эндоморфных совершенных шифров не содержат латинских квадратов.

Определение 1 [9]. 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.

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

при этом в обозначении эквивалентности ключей используется биекция: $i \leftrightarrow x_i$.

Определение 2 [9]. 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 $i_2 \neq i_3$, $i_3 \neq i_4$, …, $i_{n-1} \neq i_n$, $i_n \neq i_1$.

Следующим за минимальными по Шеннону шифрами по количеству ключей идёт класс минимальных по включению шифров, в которых для каждой пары (x, y) шифрвеличины x и шифробозначения y имеется не более двух ключей k, на которых x зашифровывается в y. В каждом столбце таблицы зашифрования каждое шифробозначение y встречается, следовательно, не более двух раз.

При $\mu = 4$ такие таблицы построены для семи и восьми ключей [8]. При $\mu = 5$ такие таблицы тоже могут быть построены.

Пример 1. Рассмотрим эндоморфный шифр с множеством из пяти шифрвеличин. Пусть $X = \{x_1, x_2, x_3, x_4, x_5\} = \{1, 2, 3, 4, 5\}$ — 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.

Таблицы зашифрования (табл. 1 и 2) совершенного эндоморфного шифра с $\lambda = \mu = 5$ и вероятностями ключей $\mathsf{P}_1 = 0{,}2$ и $\mathsf{P}_2 = \ldots = \mathsf{P}_9 = 0{,}1$ не содержат латинских квадратов.

Таблица 1

№ п/п	K	x_1	x_2	x_3	x_4	x_5	P_k
1	k_1	1	2	3	4	5	0,2
2	k_2	2	3	4	5	1	0,1
3	k_3	2	5	1	3	4	0,1
4	k_4	3	4	5	1	2	0,1
5	k_5	3	1	2	5	4	0,1
6	k_6	4	5	2	3	1	0,1
7	k_7	4	3	5	1	2	0,1
8	k_8	5	1	4	2	3	0,1
9	k_9	5	4	1	2	3	0,1

Таблица 2

№ п/п	K	x_1	x_2	x_3	x_4	x_5	P_k
1	k_1	1	2	3	4	5	0,2
2	k_2	2	3	4	5	1	0,1
3	k_3	2	5	1	3	4	0,1
4	k_4	3	4	5	1	2	0,1
5	k_5	3	1	2	5	4	0,1
6	k_6	4	5	1	3	2	0,1
7	k_7	4	3	5	2	1	0,1
8	k_8	5	1	4	2	3	0,1
9	k_9	5	4	2	1	3	0,1

Для шифров, в которых для каждой пары (x, y) шифрвеличины x и шифробозначения y имеется не более двух ключей k, на которых x зашифровывается в y, естественно определить граф на множестве ключей, а именно: два различных ключа (соответствующих разным инъекциям зашифрования) соединим ребром, если существует такая пара (x, y), что на обоих этих ключах шифрвеличина x зашифровывается в y.

Пример 2. Рассмотрим графы, соответствующие шифрам с табл. 1 и 2. Ясно, что ключи k с вероятностью $\mathsf{P}_k = 0{,}2$ представляют собой изолированные вершины.

Шифру с табл. 1 соответствует граф эквивалентности ключей, изображённый на рис. 1. Из рис. 1 и табл. 1 видно, что ключи k_2, k_3, k_5 образуют цикл длины три:

$$k_2 \underset{2}{\equiv} k_3 \underset{4}{\equiv} k_5 \underset{5}{\equiv} k_2;$$

а ключи k_3, k_4, k_6, k_7, k_9 образуют цикл длины пять:

$$k_9 \underset{1}{\equiv} k_3 \underset{4}{\equiv} k_6 \underset{2}{\equiv} k_7 \underset{5,1,2}{\equiv} k_4 \underset{4}{\equiv} k_9.$$

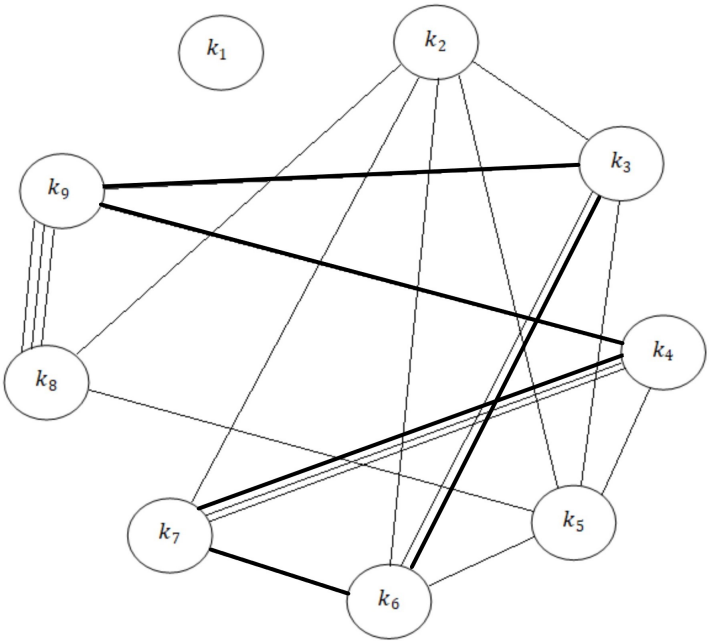

Рис. 1. Граф 1

Шифру с табл. 2 соответствует граф эквивалентности ключей, изображённый на рис. 2. Из рис. 2 и табл. 2 видно, что ключи k_2, k_3, k_5 образуют цикл длины три:

$$k_2 \underset{2}{\equiv} k_3 \underset{4}{\equiv} k_5 \underset{5}{\equiv} k_2;$$

а ключи k_2, k_4, k_5, k_8, k_9 образуют цикл длины пять:

$$k_2 \underset{5}{\equiv} k_5 \underset{3}{\equiv} k_4 \underset{4,1}{\equiv} k_9 \underset{5,3}{\equiv} k_8 \underset{4}{\equiv} k_2.$$

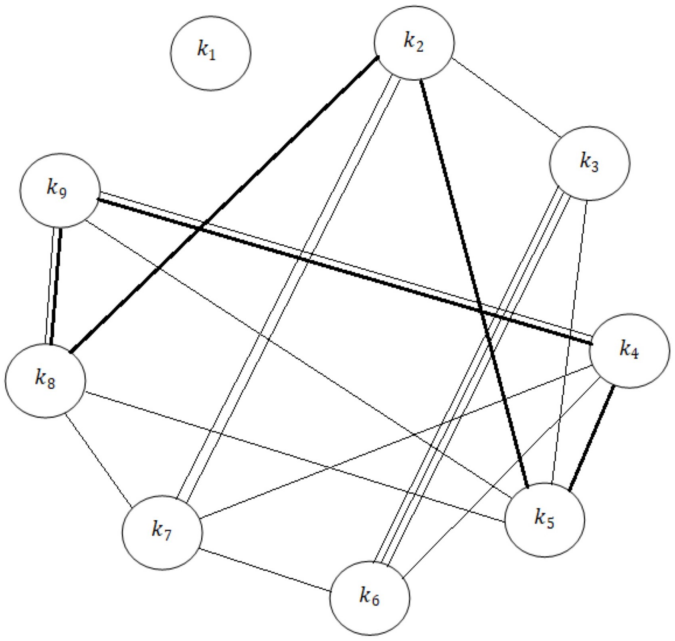

Рис. 2. Граф 2

Утверждение 1. Пусть в некоторой неодноэлементной связной компоненте графа эквивалентности ключей шифра существует цикл нечётной длины. Тогда данный шифр минимален по включению.

Таким образом, в работе предложен графовый подход к исследованию и описанию совершенных шифров, их аналогов и обобщений. В рамках предлагаемого подхода доказано утверждение (достаточное условие минимальности шифра по включению), которое может служить основой для дальнейших обобщений; приведены примеры, иллюстрирующие эффективность подхода. Полученные результаты могут быть применены и для изучения почти 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. *Зубов А. Ю.* Почти совершенные шифры и коды аутентификации // Прикладная дискретная математика. 2011. № 4(14). С. 28–33.
5. *Зубов А. Ю.* О понятии ε-совершенного шифра // Прикладная дискретная математика. 2016. № 3(33). С. 45–52.
6. *Медведева Н. В., Титов С. С.* Аналоги теоремы Шеннона для эндоморфных неминимальных шифров // Прикладная дискретная математика. Приложение. 2016. № 9. С. 62–65.
7. *Медведева Н. В., Титов С. С.* Описание неэндоморфных максимальных совершенных шифров с двумя шифрвеличинами // Прикладная дискретная математика. 2015. № 4 (30). С. 43–55.
8. *Медведева Н. В., Титов С. С.* Геометрическая модель совершенных шифров с тремя шифрвеличинами // Прикладная дискретная математика. Приложение. 2019. № 12. С. 113–116.
9. *Медведева Н. В., Титов С. С.* Конструкции неэндоморфных совершенных шифров // Прикладная дискретная математика. Приложение. 2020. № 13. С. 51–54.

УДК 512.55+003.26 DOI 10.17223/2226308X/14/21

ПОСТКВАНТОВОЕ ЭЛЕКТРОННОЕ ГОЛОСОВАНИЕ НА ОСНОВЕ РЕШЁТОК ПРИ УЧАСТИИ НЕСКОЛЬКИХ КАНДИДАТОВ

Д. А. Набоков

В последние годы появляется множество эффективных криптографических схем на основе решёток, среди которых стоит отметить (полностью) гомоморфное шифрование и протокол конфиденциального вычисления. Такие схемы на решётках интересны тем, что являются стойкими к атакам квантового компьютера. В работе реализована схема электронного голосования, эффективно поддерживающая нескольких кандидатов, за которых можно голосовать. Возможны два варианта голосования: голос за единственного кандидата или голоса для любого подмножества кандидатов. В схеме присутствует множество администраций, конфиденциальность голосов сохраняется в случае, когда хотя бы одна администрация остаётся честной. Схема направлена на соблюдение конфиденциальности голосов и проверямости результатов; для соблюдения других часто рассматриваемых свойств безопасности электронного голосования используются различные предположения,