3. Генератор с перемежающимся шагом

Генератор с перемежающимся шагом построен на базе двоичных ЛРС: управляющего ЛРС длины m и двух генерирующих ЛРС длины n и r с функциями обратной связи $f_{\text{у}}(x_1,\dots,x_m)$, $f_1(x_{m+1},\dots,x_{m+n})$ и $f_2(x_{m+n+1},\dots,x_{m+n+r})$ соответственно. В зависимости от знака управления сдвигается информация либо в первом, либо во втором генерирующем ЛРС, в силу чего преобразование h генератора нелинейное.

Пусть $J_1=\{m+1,\dots,m+n\}$, $J_2=\{m+n+1,\dots,m+n+r\}$, $S(f_{\text{у}})=\{b_1,\dots,b_\nu\}$, $S(f_1)=\{c_1,\dots,c_\mu\}$, $S(f_2)=\{d_1,\dots,d_\sigma\}$, где $1\leqslant b_1<\ldots<b_\nu=m$, $m+1\leqslant c_1<\ldots<c_\mu=m+n$ и $m+n+1\leqslant d_1<\ldots<d_\sigma=m+n+r$.

Уравнения гаммообразования имеют вид:

$$\gamma_t=h^t_{m+n}(x1,\dots,xm+n)\oplus h^t_{m+n+r}(x_1,\dots,x_m,x_{m+n+1},\dots,x_{m+n+r}).$$

Таким образом, для анализа свойств гаммы генератора представляют интерес величины $N_{m+n+r}\times\{m+n,m+n+r\}$-$\exp\Gamma(h)$ и $N_{m+n+r}\times\{m+n,m+n+r\}$-$\operatorname{qexp}\Gamma(h)$.

Утверждение 4. Граф $\Gamma(h)$ является:

а) $N_m\times\{m+n,m+n+r\}$-, $(N_m\cup J_1)\times\{m+n\}$- и $(N_m\cup J_2)\times\{m+n+r\}$-примитивным, при этом

$$\begin{gathered}N_m\times\{m+n,m+n+r\}\text{-}\exp\Gamma(h)=m+\max\{n,r\}-1,\\ N_m\times\{m+n,m+n+r\}\text{-}\operatorname{qexp}\Gamma(h)=m+\min\{n,r\}-1,\\ \delta_1=(N_m\cup J_1)\times\{m+n\}\text{-}\exp\Gamma(h)=m+n-1,\\ \delta_2=(N_m\cup J_2)\times\{m+n+r\}\text{-}\exp\Gamma(h)=m+r-1;\end{gathered}$$

б) не $N_{m+n+r}\times\{m+n,m+n+r\}$-примитивным, но $N_{m+n+r}\times\{m+n,m+n+r\}$-квазипримитивным, и

$$N_{m+n+r}\times\{m+n,m+n+r\}\text{-}\operatorname{qexp}\Gamma(h)=\max\{\min\{\delta_1,\delta_2\},n-1,r-1\}.$$

ЛИТЕРАТУРА

1. *Сачков В. Н., Тараканов В. Е.* Комбинаторика неотрицательных матриц. М.: ТВП, 2000.
2. *Кяжин С. Н., Фомичев В. М.* Локальная примитивность графов и неотрицательных матриц // Прикладная дискретная математика. 2014. № 3(25). С. 68–80.

УДК 512.64, 519.21, 519.72 DOI 10.17223/2226308X/9/25

АНАЛОГИ ТЕОРЕМЫ ШЕННОНА ДЛЯ ЭНДОМОРФНЫХ НЕМИНИМАЛЬНЫХ ШИФРОВ

Н. В. Медведева, С. С. Титов

Рассматриваются некоторые аналоги теоремы Шеннона для эндоморфных совершенных по Шеннону (абсолютно стойких к атаке по шифртексту) шифров. Построены примеры минимальных по включению совершенных и транзитивных шифров.

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

В основе изучения совершенных шифров лежит математическая модель шифра. Впервые вероятностная модель шифра рассмотрена в фундаментальной работе

К. Шеннона [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 $\lambda > 1$, $\mu \geqslant \lambda$. 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.

Существование неэндоморфных ($|X| < |Y|$) 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 и 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].

В данной работе для обобщений теоремы Шеннона и построения примеров шифров используется вероятностная модель Σ_B, в которой, согласно подходу [2, 3], шифр задаётся распределением вероятностей ключей при $\ell = 1$.

Для эндоморфного ($\lambda = \mu$) шифра перечисляются в некотором порядке все возможные $\pi = \lambda!$ подстановок зашифрования, соответствующих ключам $k \in K$ и определённым им вероятностям P_k ключей. При этом допускается, что некоторые вероятности P_k могут быть равны нулю — это означает, что соответствующая подстановка не используется в данном шифре. Получившийся π-мерный набор P вероятностей P_k ключей будем рассматривать как точку π-мерного пространства $\mathbb{R}^\pi$. Распределение биграмм, триграмм и т. д. может задаваться распределениями вероятностей при $\ell = 2, 3, \ldots$

Задача описания шифров в вероятностной модели Σ_B приводит к описанию множества точек в пространстве $\mathbb{R}^\pi$, которые являются распределениями вероятностей ключей того или иного шифра. В работах [4–6] описано множество (полиэдр) 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 $\mathbb{R}^\pi$, у которых все координаты равны нулю, кроме λ ненулевых координат, равных $1/\lambda$, а сам набор координат соответствует набору ключей (подстановок), образующих латинский квадрат. Поскольку множество точек пространства $\mathbb{R}^\pi$, соответствующих совершенным шифрам, образует выпуклое множество (полиэдр), то и выпуклая оболочка этих точек также соответствует совершенным шифрам. Возникает вопрос: будет ли полученный таким образом полиэдр множеством распределений всех эндоморфных совершенных шифров?

Для $\lambda = \mu \in \{2, 3\}$ ответ положительный. При $\lambda = \mu = 2$ — это классический шифр Вернама со сложением по модулю 2. При $\lambda = \mu = 3$ и $K = \{k_1, k_2, \ldots, k_6\}$ имеем следующую таблицу зашифрования со всеми $\pi = 3! = 6$ подстановками из

$X = \{x_1, x_2, x_3\}$ в $Y = \{1, 2, 3\}$, в которой точки $\mathsf{P}^{(1)}$ и $\mathsf{P}^{(2)}$ соответствуют латинским квадратам (табл. 1).

Таблица 1

№	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

Утверждение 1. Любой эндоморфных совершенный шифр с мощностью множества шифрвеличин, равной трём, задаётся распределением вероятностей

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

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

Это утверждение означает, что искомое выпуклое множество (полиэдр) — отрезок в шестимерном пространстве.

При $\lambda = \mu > 3$ выпуклая оболочка совершенных по Шеннону шифров с минимальным числом ключей является лишь частью множества точек, соответствующих совершенным шифрам. Например, при $\lambda = \mu = 4$ существуют минимальные (по включению) совершенные шифры, не содержащие в себе наборов ключей (подстановок), образующих латинский квадрат.

Пример 1. Рассмотрим эндоморфный шифр в случае, когда мощность множества шифрвеличин равна четырём. Пусть $X = \{x_1, x_2, x_3, x_4\}$ — множество шифрвеличин; $Y = \{1, 2, 3, 4\}$ — множество шифробозначений, $K = \{k_1, k_2, \ldots, k_\pi\}$ — множество ключей. Таблица зашифрования данного шифра, составленная из единичной и всех шести одноцикловых подстановок группы S_4, приведена в табл. 2.

Таблица 2

№	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

Это совершенный эндоморфный шифр. Здесь одноцикловые подстановки f группы S_4 обладают свойством: для каждой подстановки f имеется ровно четыре различных других одноцикловых подстановок g, таких, что $f(i) = g(i)$, $i = 1, 2, 3, 4$. Следовательно, максимальные четырехстолбцовые латинские прямоугольники в этой таблице состоят из трёх строк вида e, f, f^{-1} и латинских квадратов нет.

Пример 2. Рассмотрим таблицы зашифрования эндоморфных шифров при $\lambda = \mu = 4$ с произвольными вероятностями ключей (табл. 3 и 4).

Таблица 3

№	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

№	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

Это минимальные (по включению) транзитивные шифры, которые не могут быть совершенными ни при каких распределениях вероятностей ключей, причём из их таблиц зашифрования невозможно извлечь латинский квадрат.

Таким образом, в работе рассмотрена задача обобщения теоремы Шеннона для эндоморфных совершенных шифров. Построены примеры, показывающие, что минимальность шифра по числу ключей и минимальность по включению приводят к разным постановкам задач.

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.* О неминимальных совершенных шифрах // Прикладная дискретная математика. Приложение. 2013. № 6. С. 42–44.
5. *Медведева Н. В., Титов С. С.* Неэндоморфные совершенные шифры с двумя шифрвеличинами // Прикладная дискретная математика. Приложение. 2015. № 8. С. 63–66.
6. *Медведева Н. В., Титов С. С.* Описание неэндоморфных максимальных совершенных шифров с двумя шифрвеличинами // Прикладная дискретная математика. 2015. № 4 (30). С. 43–55.

УДК 519.1 DOI 10.17223/2226308X/9/26

О СПОСОБАХ ПОСТРОЕНИЯ КРИПТОГРАФИЧЕСКИХ ГЕНЕРАТОРОВ С ЗАДАННЫМ ПОКАЗАТЕЛЕМ БЕСПОВТОРНОСТИ ВЫХОДНЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ

Д. А. Романько, В. М. Фомичев

В связи с понятием слабого ключа итеративного симметричного блочного шифра исследованы некоторые способы построения ключевого расписания, обеспечивающего отсутствие повторений в последовательности раундовых ключей. На основе генератора «1-2 шага», использующего линейные регистры сдвига длины n и m с максимальной длиной периода, построен автономный автомат с выходным алфавитом V_m, у которого при любом начальном состоянии отрезок длины 2^{m-1} выходной последовательности не содержит повторяющихся векторов.