УДК 519.7 **DOI: 10.14529/mmp150109**

НЕКОТОРЫЕ ОБОБЩЕНИЯ ТЕОРИИ ШЕННОНА О СОВЕРШЕННЫХ ШИФРАХ

С.М. Рацеев

К. Шеннон в 40-х годах XX века ввел понятие совершенного шифра, обеспечивающего наилучшую защиту открытых текстов. Такой шифр не дает криптоаналитику никакой дополнительной информации об открытом тексте на основе перехваченной криптограммы. При этом хорошо известный шифр гаммирования с равновероятной гаммой является совершенным, но максимально уязвимым к попыткам имитации и подмены. Это происходит потому, что в шифре гаммирования алфавиты для записи открытых и шифрованных текстов равномощны. Также в данном шифре должны использоваться равновероятные гаммы, что не всегда достигается на практике. В данной обзорной работе рассматриваются задачи построения совершенных и $(k|y)$-совершенных шифров по заданному набору параметров, приводятся необходимые и достаточные условия данных шифров, рассматриваются совершенные и $(k|y)$-совершенные шифры замены с неограниченным ключом, а также совершенные шифры, стойкие к имитации и подмене шифрованных сообщений с необязательно равномерным распределением на множестве ключей.

Ключевые слова: шифр; совершенный шифр; имитация сообщения.

Введение

Пусть X, K, Y — конечные множества открытых текстов, ключей и шифрованных текстов соответственно. Обозначим через $\Sigma_B = (X, K, Y, E, D, P_X, P_K)$ вероятностную модель шифра (см. [1, 2]), где E и D — множества правил зашифрования и расшифрования соответственно. При этом предполагается, что априорные распределения вероятностей P_X и P_K на соответствующих множествах X и K независимы и не содержат нулевых вероятностей. Распределения P_X и P_K естественным образом индуцируют распределение вероятностей P_Y следующим образом:

$$P_Y(y) = \sum_{\substack{(x,k)\in X\times K \\ E_k(x)=y}} P_X(x)\cdot P_K(k).$$

Пусть $x \in X$, $y \in Y$. Обозначим через $K(x, y)$ множество всех таких ключей $k \in K$, для которых $E_k(x) = y$. Условные вероятности $P_{Y|X}(y|x)$ и $P_{Y|X}(y|x)$ определяются естественным образом:

$$P_{Y|X}(y|x) = \sum_{k\in K(x,y)} P_K(k), \quad P_{X|Y}(x|y) = \frac{P_X(x)\cdot P_{Y|X}(y|x)}{P_Y(y)}.$$

Напомним, что шифр Σ_B называется совершенным (по Шеннону), если для любых $x \in X$, $y \in Y$ выполнено равенство $P_{X|Y}(x|y) = P_X(x)$. Другими словами, перехваченное шифрованное сообщение y не дает никакой дополнительной информации об открытом тексте x. Приведем эквивалентные условия совершенного шифра.

Предложение 1. *Для произвольного шифра Σ_B следующие условия эквивалентны:*
(i) для любых $x \in X$ и $y \in Y$ выполнено равенство $P_{X|Y}(x|y) = P_X(x)$;
(ii) для любых $x \in X$ и $y \in Y$ выполнено равенство $P_{Y|X}(y|x) = P_Y(y)$;
(iii) для любых $x_1, x_2 \in X$ и $y \in Y$ выполнено равенство $P_{Y|X}(y|x_1) = P_{Y|X}(y|x_2)$.

Естественным образом определяются следующие вероятности:

$$P_{Y|K}(y|k) = \sum_{x \in X(k,y)} P_X(x), \quad P_{K|Y}(k|y) = \frac{P_K(k) P_{Y|K}(y|k)}{P_Y(y)},$$

где $X(k,y) = \{x \in X \mid E_k(x) = y\}$. Заметим, что для любых $k \in K$, $y \in Y$ множество $X(k,y)$ либо пусто, либо одноэлементно.

Шифр Σ_B называется $(k|y)$-совершенным, если для любых $k \in K$, $y \in Y$ выполнено равенство $P_{K|Y}(k|y) = P_K(k)$. Приведем также эквивалентные условия $(k|y)$-совершенных шифров.

Предложение 2. *Для произвольного шифра Σ_B следующие условия эквивалентны:*
(i) для любых $k \in K$ и $y \in Y$ выполнено равенство $P_{K|Y}(k|y) = P_K(k)$;
(ii) для любых $k \in K$ и $y \in Y$ выполнено равенство $P_{Y|K}(y|k) = P_Y(y)$;
(iii) для любых $k_1, k_2 \in K$ и $y \in Y$ выполнено равенство $P_{Y|K}(y|k_1) = P_{Y|K}(y|k_2)$.

Далее используется понятие латинского квадрата, ортогональных матриц, ортогональной таблицы и латинского прямоугольника. Данные определения можно найти, например, в работе [3].

1. Построение совершенных шифров

Приведем некоторые свойства совершенных шифров.

Предложение 3. [1] *Пусть Σ_B — совершенный шифр. Тогда для шифра Σ_B будут выполнены следующие свойства:*
(i) для любых $x \in X$, $y \in Y$ найдется такой ключ $k \in K$, что $E_k(x) = y$;
(ii) для множеств X, Y и K справедливо двойное неравенство $|X| \le |Y| \le |K|$.

Заметим, что условие (i) предыдущего предложения эквивалентно тому, что каждый элемент множества Y должен присутствовать во всех столбцах матрицы зашифрования совершенного шифра.

Теорема 1. (достаточные условия совершенного шифра [4]) *Пусть для шифра Σ_B выполнены следующие условия:*
(i) $|K(x,y)| = 1$ для любых $x \in X$, $y \in Y$;
(ii) распределение вероятностей P_K является равномерным.
Тогда шифр Σ_B является совершенным, причем распределение вероятностей P_Y будет являться равномерным и $|K| = |Y|$.

Следствие 1. (теорема К. Шеннона) *Пусть Σ_B — некоторый шифр, для которого выполнены равенства $|X| = |K| = |Y|$. Шифр Σ_B является совершенным тогда и только тогда, когда выполнены следующие условия:*
(i) $|K(x,y)| = 1$ для любых $x \in X$, $y \in Y$;
(ii) распределение вероятностей P_K является равномерным.

Наряду с теоремой Шеннона приведем еще один критерий совершенных шифров в классе шифров с равномерным распределением вероятностей на множестве ключей K.

Теорема 2. [5] *Шифр Σ_B с равномерным распределением вероятностей P_K является совершенным тогда и только тогда, когда выполнены следующие условия:*

(i) для любых $x \in X$, $y \in Y$ найдется такой ключ $k \in K$, что $E_k(x) = y$;

(ii) для любых $x_1, x_2 \in X$, $y \in Y$ выполнено равенство $|K(x_1, y)| = |K(x_2, y)|$.

Следствие 2. *Пусть для шифра Σ_B выполнено равенство $|Y| = |K|$ и распределение вероятностей P_K является равномерным. Шифр Σ_B является совершенным тогда и только тогда, когда $|K(x, y)| = 1$ для любых $x \in X$, $y \in Y$.*

Данное следствие утверждает, что если $|Y| = |K|$ и P_K равномерно, то совершенность шифра Σ_B эквивалентно тому, что матрица зашифрования шифра Σ_B является латинским прямоугольником.

Рассмотрим следующую задачу: по заданному множеству открытых текстов X_0 и множеству ключей K_0 с распределением вероятностей P_{K_0} (независимо от P_{X_0}) однозначно определить, существует ли шифр $\Sigma_B = (X_0, K_0, Y, E, D, P_{X_0}, P_{K_0})$, являющийся совершенным. Таким образом, по заданным X_0, K_0, P_{K_0} требуется определить, найдутся ли такие Y, E, D, для которых шифр Σ_B являлся бы совершенным.

Теорема 3. [6] *Для заданных X, $|X| = n$, K, $|K| = m$, P_K существует совершенный шифр $\Sigma_B = (X, K, Y, E, D, P_X, P_K)$ тогда и только тогда, когда найдется такое натуральное число s и n разбиений множества K*

$$\begin{aligned} K &= K_{11} \cup K_{12} \cup \ldots \cup K_{1s}, \quad K_{1i} \cap K_{1j} = \emptyset, \quad 1 \le i < j \le s, \\ K &= K_{21} \cup K_{22} \cup \ldots \cup K_{2s}, \quad K_{2i} \cap K_{2j} = \emptyset, \quad 1 \le i < j \le s, \\ &\ldots \\ K &= K_{n1} \cup K_{n2} \cup \ldots \cup K_{ns}, \quad K_{ni} \cap K_{nj} = \emptyset, \quad 1 \le i < j \le s, \end{aligned} \tag{1}$$

для которых выполнены следующие условия:

1) $K_{it} \cap K_{jt} = \emptyset$, $1 \le i < j \le n$, $t = 1, \ldots, s$;

2) *для любых* $1 \le i < j \le n$, $t = 1, \ldots, s$ *выполнено равенство*

$$\sum_{k \in K_{it}} P_K(k) = \sum_{k \in K_{jt}} P_K(k).$$

Пусть для некоторого числа s выполнены равенства (1), для которых выполнены условия 1 и 2 данной теоремы. Тогда матрицу зашифрования A для (совершенного) шифра Σ_B можно построить следующим образом. Пусть $Y = \{y_1, \ldots, y_s\}$ — некоторое множество шифрованных текстов, где s — число частей разбиений из (1). Составим матрицу зашифрования размера $|K| \times |X|$, где строки пронумерованы элементами множества K, а столбцы — элементами множества X, следующим образом. В i-м столбце ($i = 1, \ldots, |X|$) данной матрицы в строках, пронумерованных элементами множества K_{ij}, ставится элемент y_j, $j = 1, \ldots, s$.

Следствие 3. *Пусть для заданных X, K, P_K существует совершенный шифр. Тогда для любого множества открытых текстов $\widetilde{X}$, $|\widetilde{X}| \le |X|$, и для заданных K, P_K существует совершенный шифр.*

Пример 1. Пусть $X = \{x_1, x_2\}$, $K = \{k_1, k_2, k_3, k_4\}$, и распределение вероятностей на множестве K имеет вид

K	k_1	k_2	k_3	k_4
P_K	1/8	1/4	3/8	1/4

.

В этом случае можно построить два разбиения множества K вида

$$K = \{k_1, k_2\} \cup \{k_3\} \cup \{k_4\},$$

$$K = \{k_3\} \cup \{k_1, k_4\} \cup \{k_2\},$$

где $\{k_1, k_2\} \cap \{k_3\} = \{k_3\} \cap \{k_1, k_4\} = \{k_4\} \cap \{k_2\} = \varnothing$. При этом будут выполнены равенства

$$P_K(k_1) + P_K(k_2) = P_K(k_3), \quad P_K(k_3) = P_K(k_1) + P_K(k_4), \quad P_K(k_4) = P_K(k_2).$$

По теореме 3 для данных X, K, P_K можно построить совершенный шифр. Пусть $Y = \{y_1, y_2, y_3\}$. Составим матрицу зашифрования следующим образом:

$K \diagdown X$	x_1	x_2
k_1	y_1	y_2
k_2	y_1	y_3
k_3	y_2	y_1
k_4	y_3	y_2

.

Тогда полученный шифр будет являться совершенным.

Предложение 4. [6] *Для заданных X и Y можно построить совершенный шифр Σ_B тогда и только тогда, когда $|X| \le |Y|$.*

2. Построение $(k|y)$-совершенных шифров

Приведем некоторые свойства $(k|y)$-совершенных шифров.

Предложение 5. *Пусть шифр Σ_B является $(k|y)$-совершенным. Тогда $|X| = |Y|$.*

Теорема 4. (достаточные условия $(k|y)$-совершенного шифра [7]) *Пусть для шифра Σ_B выполнены следующие условия:*

(i) $|X| = |Y|$;

(ii) распределение вероятностей P_X является равномерным.

Тогда шифр Σ_B является $(k|y)$-совершенным, причем распределение вероятностей P_Y будет являться равномерным.

Теорема 5. [7] *Пусть для шифра Σ_B выполнены равенства $|X| = |Y| = |K|$. Шифр Σ_B является одновременно совершенным и $(k|y)$-совершенным тогда и только тогда, когда выполнены следующие условия:*

(i) $|K(x, y)| = 1$ для любых $x \in X$ и $y \in Y$;

(ii) распределение вероятностей P_K является равномерным;

(iii) распределение вероятностей P_X является равномерным.

Предложение 6. *Пусть шифр Σ_B является одновременно совершенным и $(k|y)$-совершенным. Тогда для шифра Σ_B выполнены следующие условия:*

1) *для любых $x \in X$ и $y \in Y$ найдется такой ключ $k \in K$, что $E_k(x) = y$;*
2) *$|X| = |Y| \leq |K|$;*
3) *распределение вероятностей P_X равномерно;*
4) *распределение вероятностей P_Y равномерно.*

Доказательство. Условия 1 и 2 следуют из предложений 3 и 5.

Покажем справедливость условий 3 и 4. Зафиксируем произвольным образом $y \in Y$. Из условия 1 следует, что шифртекст y присутствует во всех столбцах матрицы зашифрования шифра Σ_B. Пронумеруем элементы множеств $K = \{k_1, ..., k_m\}$, $X = \{x_1, ..., x_n\}$, $n \leq m$, таким образом, чтобы выполнялось равенство $E_{k_i}(x_i) = y$, $i = 1, ..., n$. Тогда

$$P_X(x_i) = P_{Y|K}(y|k_i) = P_Y(y),\ i = 1, ..., n.$$

Поэтому P_X имеет равномерное распределение. При этом в силу произвольности выбора $y \in Y$, имеем $P_Y(y) = P_X(x) = \frac{1}{|X|} = \frac{1}{|Y|}$. □

Теорема 6. *Пусть для шифра Σ_B выполнено равенство $|X| = |Y|$, и распределения вероятностей P_X и P_K равномерны. Шифр Σ_B является совершенным и $(k|y)$-совершенным тогда и только тогда, когда выполнены следующие условия:*

(i) для любых $x \in X$, $y \in Y$ найдется такой ключ $k \in K$, что $E_k(x) = y$;
(ii) для любых $x_1, x_2 \in X$, $y \in Y$ выполнено равенство $|K(x_1, y)| = |K(x_2, y)|$.

Доказательство. Следует из теорем 2 и 4. □

Предложение 7. *Для заданных X, Y существует $(k|y)$-совершенный шифр*

$$\Sigma_B = (X, K, Y, E, D, P_X, P_K)$$

тогда и только тогда, когда выполнено равенство $|X| = |Y|$.

Доказательство. Необходимое условие $(k|y)$-совершенного шифра следует из предложения 5.

Достаточность. Пусть $X = \{x_1, ..., x_n\}$, $Y = \{y_1, ..., y_n\}$. Понятно, что в этом случае для любого натурального $m > 1$ найдутся такие перестановки σ_1,..., $\sigma_m \in S_n$, для которых выполнены следующие равенства:

$$P_X(x_{\sigma_i(s)}) = P_X(x_{\sigma_j(s)}), \quad 1 \leq i < j \leq m, \quad s = 1, ..., n. \tag{2}$$

Например, в качестве таких перестановок можно взять тождественные перестановки. Пусть для некоторого фиксированного m перестановки σ_1,..., $\sigma_m \in S_n$ обладают условием (2). Пусть $K = \{k_1, ..., k_m\}$ — некоторое множество ключей. Составим матрицу зашифрования размера $m \times n$, где строки пронумерованы элементами множества K, а столбцы — элементами множества X, следующим образом: на позицию $(i, \sigma_i(s))$ поставим шифртекст y_s, $i = 1, ..., m$, $s = 1, ..., n$. Пусть $1 \leq i < j \leq m$, $1 \leq s \leq n$. Так как $X(k_i, y_s) = \{x_{\sigma_i(s)}\}$, то

$$P_{Y|K}(y_s|k_i) = P_X(x_{\sigma_i(s)}) = P_X(x_{\sigma_j(s)}) = P_{Y|K}(y_s|k_j).$$

Поэтому из предложения 2 следует, что шифр Σ_B является $(k|y)$-совершенным. □

Рассмотрим следующую задачу (с учетом предложения 6): по заданному множеству шифрованных текстов Y_0, множеству открытых текстов X_0 с равномерным распределением вероятностей P_{X_0}, множеству ключей K_0 с распределением вероятностей P_{K_0} однозначно определить, существует ли шифр $\Sigma_B = (X_0, K_0, Y_0, E, D, P_{X_0}, P_{K_0})$, являющийся одновременно совершенным и $(k|y)$-совершенным.

Теорема 7. *Для заданных $Y = \{y_1, ..., y_n\}$, $X = \{x_1, ..., x_n\}$ с равномерным распределением P_X, K с распределением вероятностей P_K существует одновременно совершенный и $(k|y)$-совершенный шифр $\Sigma_B = (X, K, Y, E, D, P_X, P_K)$ тогда и только тогда, когда найдется такая матрица $A = A(K)$ порядка $n \times n$, каждый элемент которой является непустым подмножеством в K, для которой выполнены следующие условия:*

1) *каждая строка и каждый столбец матрицы A является разбиением множества K на непересекающиеся подмножества;*

2) *для любых $i = 1, ..., n$, $j = 1, ..., n$ выполнено равенство $\sum_{k \in A_{ij}} P_K(k) = \frac{1}{n}$.*

Доказательство. Достаточность. Пусть выполнены условия 1 и 2 для заданной матрицы $A = A(K)$. Составим матрицу зашифрования размера $n \times n$, где строки пронумерованы элементами множества K, а столбцы — элементами множества X, следующим образом: в i-м столбце $(i = 1, ..., n)$ данной матрицы в строках, пронумерованных элементами множества A_{ij}, поставим элемент y_j, $j = 1, ..., n$. Условие 1 в этом случае гарантирует, что все правила зашифрования полученного шифра являются биективными отображениями. А из условия 2 следует, что для любого $t = 1, ..., n$ и любых $1 \le i < j \le n$ будут выполнены равенства

$$P_{Y|X}(y_t|x_i) = \sum_{k \in A_{it}} P_K(k) = \frac{1}{n} = \sum_{k \in A_{jt}} P_K(k) = P_{Y|X}(y_t|x_j).$$

Поэтому, учитывая предложение 1 и теорему 4, полученный шифр будет являться совершенным и $(k|y)$-совершенным.

Необходимость. Пусть для заданных X, P_X, Y, K, P_K существует совершенный и $(k|y)$-совершенный шифр Σ_B. Обозначим для данного шифра

$$A_{ij} = \{k \in K \mid E_k(x_i) = y_j\}, \quad i = 1, ..., n, \quad j = 1, ..., n.$$

Понятно, что матрица $A = A(K)$ порядка $n \times n$, составленная из элементов A_{ij}, будет обладать условием 1. При этом $P_{Y|X}(y_j|x_i) = \sum_{k \in A_{ij}} P_K(k)$. С учетом предложения 1 получаем такие равенства:

$$1 = \sum_{i=1}^{n} P_{Y|X}(y_j|x_i) = \sum_{i=1}^{n} \sum_{k \in A_{ij}} P_K(k) = n \cdot \sum_{k \in A_{ij}} P_K(k).$$

Поэтому $\sum\limits_{k \in A_{ij}} P_K(k) = \frac{1}{n}$. □

Пример 2. Пусть $X = \{x_1, x_2, x_3\}$, распределение вероятностей P_X равномерно, $Y = \{y_1, y_2, y_3\}$, $K = \{k_1, k_2, k_3, k_4, k_5\}$, и распределение вероятностей на множестве K имеет вид

K	k_1	k_2	k_3	k_4	k_5
P_K	1/15	4/15	1/9	2/9	1/3

.

В этом случае матрицу A из теоремы 7 можно построить следующим образом:

$\{k_1, k_2\}$	$\{k_3, k_4\}$	$\{k_5\}$
$\{k_3, k_4\}$	$\{k_5\}$	$\{k_1, k_2\}$
$\{k_5\}$	$\{k_1, k_2\}$	$\{k_3, k_4\}$

.

Составим матрицу зашифрования следующим образом:

$K \diagdown X$	x_1	x_2	x_3
k_1	y_1	y_3	y_2
k_2	y_1	y_3	y_2
k_3	y_2	y_1	y_3
k_4	y_2	y_1	y_3
k_5	y_3	y_2	y_1

.

Тогда полученный шифр будет являться совершенным и $(k|y)$-совершенным.

3. Совершенные шифры замены с неограниченным ключом

Определенная вероятностная модель шифра Σ_B позволяет рассматривать в качестве множества открытых текстов X лишь последовательности в некотором конечном алфавите A, длины которых ограничены некоторой заранее определенной константой. В работе [2] приводятся модели шифров замены с ограниченным и неограниченным ключом, для которых, в частности, на множество X такое ограничение не накладывается. Пусть Σ_H — шифр замены с неограниченным ключом (подробнее см. [4]).

Говорят, что шифр Σ_H является совершенным тогда и только тогда, когда для любого натурального l шифр Σ_H^l является совершенным.

Предложение 8. *Для шифра Σ_H следующие условия эквивалентны:*

(i) для любого $l \in \mathbb{N}$ и любых $\overline{u} \in U^{(l)}$, $\overline{v} \in V^{(l)}$ выполнено равенство $P_{U^{(l)}|V^{(l)}}(\overline{u}|\overline{v}) = P_{U^{(l)}}(\overline{u})$;

(ii) для любого $l \in \mathbb{N}$ и любых $\overline{u} \in U^{(l)}$, $\overline{v} \in V^{(l)}$ выполнено равенство $P_{V^{(l)}|U^{(l)}}(\overline{v}|\overline{u}) = P_{V^{(l)}}(\overline{v})$;

(iii) для любого $l \in \mathbb{N}$ и любых $\overline{u}_1, \overline{u}_2 \in U^{(l)}$, $\overline{v} \in V^{(l)}$ выполнено равенство $P_{V^{(l)}|U^{(l)}}(\overline{v}|\overline{u}_1) = P_{V^{(l)}|U^{(l)}}(\overline{v}|\overline{u}_2)$.

Предложение 9. *Пусть шифр замены с неограниченным ключом Σ_H является совершенным. Тогда для данного шифра будут выполнены следующие свойства:*

(i) для любого натурального числа l и любых $\overline{u} \in U^{(l)}$, $\overline{v} \in V^{(l)}$ найдется такой ключевой поток $\overline{\jmath} \in \mathbb{N}_r^l$, что $E_{\overline{\jmath}}(\overline{u}) = \overline{v}$;

(ii) для любого натурального числа l справедливо двойное неравенство

$$|U^{(l)}| \leq |V^{(l)}| \leq |\mathbb{N}_r^l| = r^l.$$

Теорема 8. (достаточные условия совершенности шифра Σ_H [4]) *Пусть шифр замены Σ_H обладает следующими условиями:*

(i) правила зашифрования E_1, E_2,..., E_r шифра Σ_H обладают тем свойством, что для любых $u \in U$, $v \in V$ найдется, и притом единственный, элемент $j = j(u, v) \in \mathbb{N}_r$, такой что $E_j(u) = v$;

(*ii*) *распределение вероятностей* $P_{\mathbb{N}_r}$ *является равномерным.*
Тогда шифр Σ_H *является совершенным, причем для любого* $l \in \mathbb{N}$ *выполнено равенство* $|V^{(l)}| = r^l$, *и распределение вероятностей* $P_{V^{(l)}}$ *будет являться равномерным.*

Теорема 9. *Пусть для шифра* Σ_H *выполнены равенства* $|U| = |\mathbb{N}_r| = |V|$. *Шифр* Σ_H *является совершенным тогда и только тогда, когда выполнены следующие условия:*

(*i*) *правила зашифрования* E_1, E_2,..., E_r *шифра* Σ_H *обладают тем свойством, что для любых* $u \in U$, $v \in V$ *найдется, и притом единственный, элемент* $j = j(u, v) \in \mathbb{N}_r$, *такой что* $E_j(u) = v$;

(*ii*) *распределение вероятностей* $P_{\mathbb{N}_r}$ *является равномерным.*

Доказательство. Следует из теоремы Шеннона и теоремы 8. □

Пусть для шифра Σ_H выполнены равенства $|U| = |\mathbb{N}_r| = |V|$, и распределение вероятностей $P_{\mathbb{N}_r}$ является равномерным. Тогда из теоремы 9 следует, что шифр Σ_H является совершенным тогда и только тогда, когда матрица зашифрования опорного шифра для Σ_H

$\mathbb{N}_r \diagdown U$	u_1	...	u_r
1	$E_1(u_1)$	...	$E_1(u_r)$
...	...	...	...
r	$E_r(u_1)$	...	$E_r(u_r)$

является латинским квадратом (подробнее о латинских квадратах см. [8]). Поэтому шифры табличного и модульного гаммирования с равновероятной гаммой являются совершенными.

Рассмотрим еще один критерий совершенных шифров замены с неограниченным ключом в классе шифров с равномерным распределением вероятностей на множестве $\mathbb{N}_r$.

Теорема 10. [5] *Шифр* Σ_H *с равномерным распределеним вероятностей* $P_{\mathbb{N}_r}$ *является совершенным тогда и только тогда, когда выполнены следующие условия:*

(*i*) *для любых* $u \in U$ *и* $v \in V$ *найдется такое* $j \in \mathbb{N}_r$, *что* $E_j(u) = v$;

(*ii*) *для любых* $u_1, u_2 \in U$, $v \in V$ *выполнено равенство* $|\mathbb{N}_r(u_1, v)| = |\mathbb{N}_r(u_2, v)|$.

Следствие 4. *Пусть для шифра* Σ_H *выполнено равенство* $|V| = |\mathbb{N}_r|$, *и распределение вероятностей* $P_{\mathbb{N}_r}$ *является равномерным. Шифр* Σ_H *является совершенным тогда и только тогда, когда* $|\mathbb{N}_r(u, v)| = 1$ *для любых* $u \in U$ *и* $v \in V$.

Рассмотрим задачу построения совершенного шифра Σ_H по заданному множеству шифрвеличин U и множеству $\mathbb{N}_r$ с распределением вероятностей $P_{\mathbb{N}_r}$.

Теорема 11. [6] *Для заданных* U, $|U| = n$, $\mathbb{N}_r$, $P_{\mathbb{N}_r}$ *существует совершенный шифр* Σ_H *тогда и только тогда, когда найдется такое натуральное число* s *и* n *разбиений множества* $\mathbb{N}_r$

$$\begin{aligned}
&\mathbb{N}_r = K_{11} \cup K_{12} \cup ... \cup K_{1s}, \quad K_{1i} \cap K_{1j} = \emptyset, \quad 1 \le i < j \le s,\\
&\mathbb{N}_r = K_{21} \cup K_{22} \cup ... \cup K_{2s}, \quad K_{2i} \cap K_{2j} = \emptyset, \quad 1 \le i < j \le s,\\
&\qquad\qquad ...\\
&\mathbb{N}_r = K_{n1} \cup K_{n2} \cup ... \cup K_{ns}, \quad K_{ni} \cap K_{nj} = \emptyset, \quad 1 \le i < j \le s,
\end{aligned} \tag{3}$$

для которых выполнены следующие условия:

1) $K_{it} \cap K_{jt} = \emptyset$, $1 \le i < j \le n$, $t = 1, ..., s$;

2) *для любых* $1 \le i < j \le n$, $t = 1, ..., s$ *выполнено равенство*

$$\sum_{k \in K_{it}} P_{\mathbb{N}_r}(k) = \sum_{k \in K_{jt}} P_{\mathbb{N}_r}(k).$$

Следствие 5. *Пусть для заданных* U, $\mathbb{N}_r$, $P_{\mathbb{N}_r}$ *существует совершенный шифр. Тогда для любого множества шифрвеличин* $\widetilde{U}$, $|\widetilde{U}| \le |U|$, *и для заданных* $\mathbb{N}_r$, $P_{\mathbb{N}_r}$ *существует совершенный шифр* Σ_H.

4. $(k|y)$-совершенные шифры Σ_H

Далее везде предполагается, что для любого натурального l выполнены равенства $U^{(l)} = U^l$, $V^{(l)} = V^l$.

Определим условные вероятности $P_{V^l|\mathbb{N}_r^l}(\overline{v}|\overline{\jmath})$ и $P_{\mathbb{N}_r^l|V^l}(\overline{\jmath}|\overline{v})$:

$$P_{V^l|\mathbb{N}_r^l}(\overline{v}|\overline{\jmath}) = \sum_{\overline{u} \in U^l(\overline{\jmath},\overline{v})} P_{U^l}(\overline{u}), \quad P_{\mathbb{N}_r^l|V^l}(\overline{\jmath}|\overline{v}) = \frac{P_{\mathbb{N}_r^l}(\overline{\jmath}) \cdot P_{V^l|\mathbb{N}_r^l}(\overline{v}|\overline{\jmath})}{P_{V^l}(\overline{v})},$$

где $U^l(\overline{\jmath}, \overline{v}) = \{\overline{u} \in U^l \mid E_{\overline{\jmath}}(\overline{u}) = \overline{v}\}$.

Говорят, что шифр Σ_H является $(k|y)$-совершенным, если для любого натурального l шифр Σ_H^l является $(k|y)$-совершенным.

Предложение 10. *Для шифра* Σ_H *следующие условия эквивалентны:*

(i) для любого $l \in \mathbb{N}$ *и любых* $\overline{\jmath} \in \mathbb{N}_r^l$, $\overline{v} \in V^l$ *выполнено равенство* $P_{\mathbb{N}_r^l|V^l}(\overline{\jmath}|\overline{v}) = P_{\mathbb{N}_r^l}(\overline{\jmath})$;

(ii) для любого $l \in \mathbb{N}$ *и любых* $\overline{\jmath} \in \mathbb{N}_r^l$, $\overline{v} \in V^l$ *выполнено равенство* $P_{V^l|\mathbb{N}_r^l}(\overline{v}|\overline{\jmath}) = P_{V^l}(\overline{v})$;

(iii) для любого $l \in \mathbb{N}$ *и любых* $\overline{\jmath}_1, \overline{\jmath}_2 \in \mathbb{N}_r^l$, $\overline{v} \in V^l$ *выполнено равенство* $P_{V^l|\mathbb{N}_r^l}(\overline{v}|\overline{\jmath}_1) = P_{V^l|\mathbb{N}_r^l}(\overline{v}|\overline{\jmath}_2)$.

Теорема 12. *Пусть для шифра* Σ_H *выполнены следующие условия:*

(i) $|U| = |V|$;

(ii) для любого $l \in \mathbb{N}$ *распределение вероятностей* P_{U^l} *является равномерным. Тогда шифр* Σ_H *является* $(k|y)$*-совершенным.*

Доказательство. Зафиксируем $l \in \mathbb{N}$. Пусть $j_1...j_l \in \mathbb{N}_r^l$, $v_1...v_l \in V^l$. Тогда найдется, и притом единственный, открытый текст $u_1...u_l \in U^l$, такой что $E_{j_1...j_l}(u_1...u_l) = v_1...v_l$. Поэтому

$$P_{V^l|\mathbb{N}_r^l}(v_1...v_l|j_1...j_l) = P_{U^l}(u_1...u_l) = \frac{1}{|U|^l} = \frac{1}{|V|^l}.$$

Поэтому для любых $\overline{\jmath}_1, \overline{\jmath}_2 \in \mathbb{N}_r^l$, $\overline{v}_1, \overline{v}_2 \in V^l$ выполнены равенства

$$P_{V^l|\mathbb{N}_r^l}(\overline{v}_1|\overline{\jmath}_1) = \frac{1}{|V|^l} = P_{V^l|\mathbb{N}_r^l}(\overline{v}_2|\overline{\jmath}_2).$$

Таким образом, из предложения 10 следует, что шифр Σ_H^l является $(k|y)$-совершенным. □

Предложение 11. *Для заданных U, V существует $(k|y)$-совершенный шифр Σ_H с распределением вероятностей $P_{U^l}(u_1...u_l) = \prod_{i=1}^{l} P_U(u_i)$, $u_1...u_l \in U^l$, $l \in \mathbb{N}$ тогда и только тогда, когда $|U| = |V|$.*

Доказательство. Достаточность. Пусть для произвольного фиксированного $m > 1$ найдутся такие перестановки σ_1,..., $\sigma_m \in S_n$, где $n = |U| = |V|$, для которых выполнены условия

$$P_U(u_{\sigma_i(s)}) = P_U(u_{\sigma_j(s)}), \quad 1 \le i < j \le m, \quad s = 1, ..., n.$$

Составим матрицу зашифрования размера $m \times n$ для опорного шифра следующим образом: на позицию $(i, \sigma_i(s))$ поставим v_s, $i = 1, ..., m$, $s = 1, ..., n$. Так как $\mathbb{N}_m(i, v_s) = \{u_{\sigma_i(s)}\}$, то для любого $l \in \mathbb{N}$ и любых $v_{i_1}...v_{i_l} \in V^l$, $a_1...a_l \in \mathbb{N}_m^l$, $b_1...b_l \in \mathbb{N}_m^l$ выполнены равенства

$$P_{V^l|\mathbb{N}_m^l}(v_{i_1}...v_{i_l}|a_1...a_l) = P_{U^l}(u_{\sigma_{a_1}(i_1)}...u_{\sigma_{a_l}(i_l)}) = \prod_{t=1}^{l} P_U(u_{\sigma_{a_t}(i_t)}) =$$
$$= \prod_{t=1}^{l} P_U(u_{\sigma_{b_t}(i_t)}) = P_{U^l}(u_{\sigma_{b_1}(i_1)}...u_{\sigma_{b_l}(i_l)}) = P_{V^l|\mathbb{N}_m^l}(v_{i_1}...v_{i_l}|b_1...b_l).$$

Таким образом, из предложения 10 следует, что шифр Σ_H^l является $(k|y)$-совершенным. *Необходимое* условие следует из предложения 7. □

Теорема 13. *Для заданных $V = \{v_1, ..., v_n\}$, $U = \{u_1, ..., u_n\}$ с равномерным распределением P_{U^l} для любого $l \in \mathbb{N}$, $\mathbb{N}_r$ с распределением вероятностей $P_{\mathbb{N}_r}$ существует одновременно совершенный и $(k|y)$-совершенный шифр Σ_H тогда и только тогда, когда найдется такая матрица $A = A(\mathbb{N}_r)$ порядка $n \times n$, каждый элемент которой является непустым подмножеством в $\mathbb{N}_r$, для которой выполнены следующие условия:*

1) *каждая строка и каждый столбец матрицы A является разбиением множества $\mathbb{N}_r$ на непересекающиеся подмножества;*

2) *для любых $i = 1, ..., n$, $j = 1, ..., n$ выполнено равенство $\sum_{k \in A_{ij}} P_{\mathbb{N}_r}(k) = \frac{1}{n}$.*

Доказательство. Необходимое условие следует из теоремы 7. *Достаточность.* Составим матрицу зашифрования над элементами множества V для опорного шифра Σ так же, как и в теореме 7. Зафиксируем некоторое натуральное l. Пусть $\overline{a} = a_1...a_l \in U^l$, $\overline{b} = b_1...b_l \in U^l$, $\overline{v} = v_1...v_l \in V^l$. Тогда

$$P_{V^l|U^l}(\overline{v}|\overline{a}) = \prod_{i=1}^{l} P_{V|U}(v_i|a_i) = \prod_{i=1}^{l} P_{V|U}(v_i|b_i) = P_{V^l|U^l}(\overline{v}|\overline{b}),$$

где второе равенство следует из теоремы 7. Поэтому из предложения 8 и теоремы 12 следует, что шифр Σ_H^l является совершенным и $(k|y)$-совершенным. □

5. Совершенные имитостойкие шифры

Вернемся к вероятностной модели шифра Σ_B. Рассмотрим вероятностное пространство $(\Omega = K, F_K, P_K)$. Зафиксируем $y \in Y$. Обозначим через $K(y)$ следующее множество: $K(y) = \{k \in K \mid y \in E_k(X)\}$. Под обозначением $K(y)$ будем также понимать событие $(K(y) \in F_K)$, заключающееся в том, что при случайном выборе ключа

$k \in K$ шифрованный текст y можно расшифровать на ключе k, то есть $y \in E_k(X)$. Тогда событию $K(y)$ будут благоприятствовать все элементы из множества $K(y)$, и только они. Поэтому $P(K(y)) = \sum_{k \in K(y)} P_K(k)$. Если канал связи готов к работе, и на приеме установлены действующие ключи, но в данный момент времени никакого сообщения не передается, то в этом случае противником может быть предпринята попытка имитации сообщения. Тогда вероятность успеха имитации определяется следующим образом:

$$P_{im} = \max_{y \in Y} P(K(y)).$$

Если же в данный момент передается некоторое сообщение $y \in Y$ (которое получено из открытого текста $x \in X$ на ключе $k \in K$), то противник может заменить его на $\widetilde{y} \in Y$, отличный от y. При этом он будет рассчитывать на то, что на действующем ключе k криптограмма $\widetilde{y}$ будет воспринята как некий осмысленный открытый текст $\widetilde{x}$, отличный от x. Пусть "$K(\widetilde{y}) \mid K(y)$" — событие, заключающееся в попытке подмены сообщения y сообщением $\widetilde{y}$. Применяя теорему о произведении вероятностей, получаем, что

$$P(K(\widetilde{y}) \mid K(y)) = \frac{P(K(y) \cap K(\widetilde{y}))}{P(K(y))} = \frac{\sum_{k \in K(y,\widetilde{y})} P_K(k)}{\sum_{k \in K(y)} P_K(k)},$$

где $K(y, \widetilde{y}) = K(y) \cap K(\widetilde{y})$. Тогда вероятность успеха подмены сообщения будет вычисляться по следующей формуле:

$$P_{podm} = \max_{\substack{y, \widetilde{y} \in Y \\ y \neq \widetilde{y}}} P(K(\widetilde{y}) \mid K(y)).$$

Теорема 14. [2] *Для любого шифра Σ_B справедливы неравенства*

$$P_{im} \geq \frac{|X|}{|Y|}, \quad P_{podm} \geq \frac{|X| - 1}{|Y| - 1}.$$

При этом $P_{im} = |X|/|Y|$ тогда и только тогда, когда для любого $y \in Y$ выполнено равенство $P(K(y)) = |X|/|Y|$. Также $P_{podm} = (|X| - 1)/(|Y| - 1)$ тогда и только тогда, когда для любых $y, \widetilde{y} \in Y$, $y \neq \widetilde{y}$, выполнено равенство $P(K(\widetilde{y}) \mid K(y)) = (|X| - 1)/(|Y| - 1)$.

Далее везде предполагается, что для любого натурального l выполнены равенства $U^{(l)} = U^l$, $V^{(l)} = V^l$. Для шифра замены с неограниченным ключом Σ_H обозначим через P^l_{im} вероятность имитации сообщения для шифра Σ^l_H, а через $P^l_{podm}(s)$ — вероятность подмены в сообщении длины l ровно s символов для шифра Σ^l_H, где $s \leq l$. Из теоремы 14 следует, что если для некоторого шифра Σ_H выполнено равенство $|U| = |V|$, то $P^l_{im} = P^l_{podm}(s) = 1$ для любого натурального l и любого $s \leq l$, то есть такие шифры максимально уязвимы к угрозам имитации и подмены сообщения. Приведем некоторые конструкции шифра замены с неограниченным ключом, в котором одновременно обеспечивается стойкость и имитостойкость. При этом матрица зашифрования строится только для опорного шифра, поэтому ее размерность не зависит от длины открытого текста.

Предложение 12. [4] *Пусть $A = A(n+1, n)$ — некоторая матрица над множеством шифробозначений $V = \{v_1, ..., v_{n+1}\}$, которая является латинским прямоугольником, и пусть матрица A является матрицей зашифрования для опорного шифра замены с неограниченным ключом Σ_H. Пусть также случайный генератор ключевых последовательностей ψ_c из конструкции шифра Σ_H имеет равномерное распределение. Тогда для любого натурального l шифр Σ_H^l является совершенным, и выполнены следующие равенства:*

$$P_{im}^l = \left(\frac{n}{n+1}\right)^l, \quad P_{podm}^l(s) = \left(\frac{n-1}{n}\right)^s.$$

Пусть S_n — симметрическая группа степени n, $T^j \in S_n$ — циклическая перестановка на j позиций влево. Обозначим через $A_j = A_j(n, 2)$ матрицу размера $n \times 2$ над множеством $\mathbb{N}_n$, имеющую такой вид:

$$A_j = \begin{pmatrix} 1 & 2 & ... & n \\ T^j(1) & T^j(2) & ... & T^j(n) \end{pmatrix}^T, \quad j = 1, ..., n-1.$$

Из матриц A_j, $j = 1, ..., n-1$, составим матрицу $M = M(n^2-n, 2)$ размера $(n^2-n) \times 2$ путем последовательной графической записи матриц A_1,..., A_{n-1} одной под другой.

Предложение 13. [4] *Пусть $M = M(n^2 - n, 2)$ — матрица над множеством $V = \{v_1, ..., v_n\}$, построенная выше, $r = n^2-n$, $|U| = 2$ и пусть матрица M является матрицей зашифрования для опорного шифра замены с неограниченным ключом Σ_H. Пусть также случайный генератор ключевых последовательностей ψ_c из конструкции шифра Σ_H имеет равномерное распределение. Тогда для любого натурального l шифр Σ_H^l является совершенным, и выполнены следующие равенства:*

$$P_{im}^l = \left(\frac{2}{n}\right)^l, \quad P_{podm}^l(s) = \left(\frac{1}{n-1}\right)^s.$$

Заметим, что в предложениях 12 и 13 $P_{im}^l \to 0$ при $l \to \infty$, $P_{podm}^l(s) \to 0$ при $s \to \infty$.

Построим также совершенный имитостойкий шифр на базе ортогональных таблиц. Пусть для чисел s и n, $1 < n < s$, существует ортогональная таблица $OA(s, n)$ над множеством $V = \{v_1, ..., v_s\}$, в которой i-я строка содержит только элемент v_i, $i = 1, ..., s$. Из сказанного выше следует, что если, например, s является степенью простого числа, то $OA(s, n)$ существует для любого $n = 2, ..., s-1$. Вычеркнем из таблицы $OA(s, n)$ первые s строк и обозначим полученную таблицу через $A(s, n)$. Понятно, что таблица $A(s, n)$ имеет размерность $(s^2 - s) \times n$, в каждой строке нет повторяющихся элементов, а каждый столбец содержит ровно $s-1$ экземпляров элемента v_i, $i = 1, ..., s$.

Предложение 14. [3] *Пусть для шифра Σ_H выполнены следующие условия:*

(i) $|U| = n$, $|V| = s$, $1 < n < s$, $r = s^2 - s$;

(ii) матрица зашифрования опорного шифра представляет собой таблицу вида $A(s, n)$;

(iii) распределение вероятностей $P_{\mathbb{N}_r}$ является равномерным.

Тогда шифр Σ_H является совершенным, и для любого l выполнены следующие равенства:

$$P_{im}^{l} = \left(\frac{n}{s}\right)^{l}, \quad P_{podm}^{l}(t) = \left(\frac{n-1}{s-1}\right)^{t},$$

то есть $P_{im}^{l} \to 0$ при $l \to \infty$, $P_{podm}^{l}(t) \to 0$ при $t \to \infty$.

Предложение 15. *Пусть для шифра Σ_H (с матрицей зашифрования опорного шифра из теоремы 11) выполнены равенства (3) и условия 1 и 2 теоремы 11. Тогда*

$$P_{im}^{l} = \left(n \cdot \max_{1\le i\le s} \sum_{k\in K_{1i}} P_{\mathbb{N}_r}(k)\right)^{l},$$

$$P_{podm}^{l}(t) = \left(\frac{1}{n} \cdot \max_{\substack{1\le i,j\le s\\ i\ne j}} \frac{\sum_{k\in K_i\cap K_j} P_{\mathbb{N}_r}(k)}{\sum_{k\in K_{1i}} P_{\mathbb{N}_r}(k)}\right)^{t},$$

где

$$K_i = \bigcup_{j=1}^{n} K_{ji}, \quad i = 1, ..., s.$$

Доказательство. Пусть $V = \{v_1, ..., v_s\}$, $1 \le i \le s$. Тогда из условий 1 и 2 теоремы 11 следуют такие равенства:

$$P(\mathbb{N}_r(v_i)) = \sum_{k\in K_{1i}\cup ...\cup K_{ni}} P_{\mathbb{N}_r}(k) = n \cdot \left(\sum_{k\in K_{1i}} P_{\mathbb{N}_r}(k)\right),$$

поэтому

$$P_{im} = n \cdot \max_{1\le i\le s} \sum_{k\in K_{1i}} P_{\mathbb{N}_r}(k).$$

Далее, пусть $1 \le i, j \le s$, $i \ne j$. Тогда

$$P(\mathbb{N}_r(v_j) \mid \mathbb{N}_r(v_i)) = \frac{\sum_{k\in K_i\cap K_j} P_{\mathbb{N}_r}(k)}{\sum_{k\in K_i} P_{\mathbb{N}_r}(k)} = \frac{\sum_{k\in K_i\cap K_j} P_{\mathbb{N}_r}(k)}{n \cdot \left(\sum_{k\in K_{1i}} P_{\mathbb{N}_r}(k)\right)},$$

поэтому

$$P_{podm} = \frac{1}{n} \cdot \max_{\substack{1\le i,j\le s\\ i\ne j}} \frac{\sum_{k\in K_i\cap K_j} P_{\mathbb{N}_r}(k)}{\sum_{k\in K_{1i}} P_{\mathbb{N}_r}(k)}.$$

□

Предложение 16. *Пусть для шифра Σ_H выполнены равенства (3) и условия 1 и 2 теоремы 11. Для шифра Σ_H достигаются нижние границы для вероятностей имитации и подмены*

$$P_{im}^{l} = \left(\frac{n}{s}\right)^{l}, \quad P_{podm}^{l}(t) = \left(\frac{n-1}{s-1}\right)^{t},$$

где $n = |U|$, $s = |V|$, тогда и только тогда, когда для любых $1 \le i < j \le s$ выполнены следующие равенства:

$$\sum_{k\in K_{1i}} P_{\mathbb{N}_r}(k) = \frac{1}{s}, \qquad \sum_{k\in K_i\cap K_j} P_{\mathbb{N}_r}(k) = \frac{n(n-1)}{s(s-1)}.$$

Доказательство. Следует из теоремы 14 и предложения 15. □

Заметим, что совершенные имитостойкие шифры можно строить не только для случая, когда $P_{\mathbb{N}_r}$ равномерно.

Пусть Σ_H — некоторый шифр замены с неограниченным ключом с опорным шифром $\Sigma = (U, \mathbb{N}_r, V, E, D)$, $|U| = n$, $|V| = s$, распределением вероятностей $P_{\mathbb{N}_r}$ для случайного генератора ψ_c и матрицей зашифрования A размера $r \times n$ над множеством V для опорного шифра Σ. При этом строки матрицы A пронумерованы элементами множества $\mathbb{N}_r$, а столбцы — элементами множества U. Пусть также для некоторого $\widetilde{r} \geq r$ имеется случайный генератор $\widetilde{\psi}_c$ с распределением вероятностей $\widetilde{P}_{\mathbb{N}_{\widetilde{r}}}$ и условием, что найдется такое разбиение множества $\mathbb{N}_{\widetilde{r}}$ на r непустых непересекающиеся подмножеств

$$\mathbb{N}_{\widetilde{r}} = K_1 \cup K_2 \cup ... \cup K_r, \tag{4}$$

для которого выполнены равенства

$$\widetilde{P}_{\mathbb{N}_{\widetilde{r}}}(K_i) = \sum_{k \in K_i} P_{\mathbb{N}_{\widetilde{r}}}(k) = P_{\mathbb{N}_r}(j), \quad i = 1, ..., r. \tag{5}$$

Построим шифр замены с неограниченным ключом $\widetilde{\Sigma}_H$ со случайным генератором $\widetilde{\psi}_c$ и опорным шифром $\widetilde{\Sigma} = (U, \mathbb{N}_{\widetilde{r}}, V, \widetilde{E}, \widetilde{D})$ со значениями U и V, как в опорном шифре Σ. Для этого необходимо определить множество правил зашифрования $\widetilde{E}$ и множество правил расшифрования $\widetilde{D}$. $\widetilde{E}$ и $\widetilde{D}$ определим с помощью матрицы зашифрования B размера $\widetilde{r} \times n$ над множеством V, в которой строки пронумерованы элементами множества $\mathbb{N}_{\widetilde{r}}$, а столбцы — элементами множества U, следующим образом: j-ю строку матрицы A продублируем $|K_j|$ раз, $j = 1, ..., r$, и из всех полученных (продублированных) строк составим матрицу B.

Предложение 17. [3] *Если один из шифров Σ_H или $\widetilde{\Sigma}_H$ является совершенным, то другой также будет являться совершенным. Более того, вероятности успехов имитации и успехов подмены данных шифров соответственно равны.*

Пусть

$$\mathbb{N}_r = K_1 \cup K_2 \cup ... \cup K_s \tag{6}$$

— разбиение множества $\mathbb{N}_r$ на непустые непересекающиеся подмножества с условием, что

$$P_{\mathbb{N}_r}(K_i) = \sum_{k \in K_i} P_{\mathbb{N}_r}(k) = \frac{1}{s}, \quad i = 1, ..., s. \tag{7}$$

Пусть $U = \{u_1, ..., u_n\}$, A — матрица размера $s \times n$, $1 < n < s$, над множеством $V = \{v_1, ..., v_s\}$ вида

v_1	v_2	...	v_n
v_2	v_3	...	v_{n+1}
...	...	...	...
v_s	v_1	...	v_{n-1}

,

в которой каждый следующий столбец является циклическим сдвигом на одну позицию предыдущего столбца. Понятно, что данная матрица является латинским прямоугольником. Как и перед предложением 17, на основе матрицы A построим матрицу зашифрования B размера $r \times n$ над множеством V для опорного шифра Σ.

Предложение 18. [3] *Полученный шифр Σ_H будет являться совершенным, причем будут выполнены следующие равенства:*

$$P_{im}^{l} = \left(\frac{n}{s}\right)^{l}, \quad P_{podm}^{l}(t) = \left(\frac{n-1}{n}\right)^{t}.$$

Пример 3. Пусть $U = \{u_1, u_2\}$, $V = \{v_1, v_2, v_3\}$, $\mathbb{N}_5 = \{1, 2, 3, 4, 5\}$, и распределение вероятностей на множестве $\mathbb{N}_5$ имеет вид

$\mathbb{N}_5$	1	2	3	4	5
$P_{\mathbb{N}_5}$	1/15	4/15	1/12	1/4	1/3

.

В этом случае существует разбиение вида (6) с условием (7):

$$K_1 = \{1, 2\},\ K_2 = \{3, 4\},\ K_3 = \{5\},$$

$$P_{\mathbb{N}_5}(K_1) = P_{\mathbb{N}_5}(K_2) = P_{\mathbb{N}_5}(K_3) = \frac{1}{3}.$$

Сначала составим матрицу A

$\mathbb{N}_3 \diagdown U$	u_1	u_2
1	v_1	v_2
2	v_2	v_3
3	v_3	v_1

,

которая является латинским прямоугольником, а на ее основе составим матрицу B

$\mathbb{N}_5 \diagdown U$	u_1	u_2
1	v_1	v_2
2	v_1	v_2
3	v_2	v_3
4	v_2	v_3
5	v_3	v_1

.

По предложению 18 для данных U, V, $\mathbb{N}_5$, $P_{\mathbb{N}_5}$ и матрицы зашифрования B для опорного шифра полученный шифр Σ_H будет являться совершенным, причем

$$P_{im}^{l} = \left(\frac{2}{3}\right)^{l}, \quad P_{podm}^{l}(t) = \left(\frac{1}{2}\right)^{t}.$$

Пусть теперь

$$\mathbb{N}_r = K_1 \cup K_2 \cup ... \cup K_{s^2-s} \tag{8}$$

— разбиение множества $\mathbb{N}_r$ с условием, что

$$P_{\mathbb{N}_r}(K_i) = \sum_{k \in K_i} P_{\mathbb{N}_r}(k) = \frac{1}{s^2 - s}, \quad i = 1, ..., s^2 - s. \tag{9}$$

Пусть T^j — циклическая перестановка на j позиций влево s-го множества. Обозначим через $A_j = A_j(s,2)$ матрицу размера $s \times 2$ над множеством $V = \{v_1, ..., v_s\}$, имеющую такой вид:

$$A_j = \begin{pmatrix} v_1 & v_2 & ... & v_s \\ v_{T^j(1)} & v_{T^j(2)} & ... & v_{T^j(s)} \end{pmatrix}^T, \quad j = 1, ..., s-1.$$

Из матриц A_j, $j = 1, ..., s-1$, составим матрицу A размера $(s^2 - s) \times 2$ путем последовательной графической записи матриц A_1,..., A_{n-1} одной под другой. Теперь на основе матрицы A построим матрицу зашифрования B размера $r \times 2$ для опорного шифра указанным выше способом.

Предложение 19. [3] *Полученный шифр Σ_H будет являться совершенным, причем будут выполнены следующие равенства:*

$$P_{im}^l = \left(\frac{2}{s}\right)^l, \quad P_{podm}^l(t) = \left(\frac{1}{s-1}\right)^t.$$

Вернемся к ортогональным таблицам. Пусть имеется разбиение (8) с условием (9). Пусть также для чисел s и n существует ортогональная таблица $OA(s,n)$ над множеством $V = \{v_1, ..., v_s\}$, $1 < n < s$. Построим из данной таблицы (как и до предложения 14) матрицу A размера $(s^2 - s) \times n$. А на основе матрицы A, как и ранее, построим матрицу зашифрования B размера $r \times 2$ для опорного шифра.

Предложение 20. [3] *Полученный шифр Σ_H будет являться совершенным, причем будут выполнены следующие равенства:*

$$P_{im}^l = \left(\frac{n}{s}\right)^l, \quad P_{podm}^l(t) = \left(\frac{n-1}{s-1}\right)^t.$$

Литература

1. Основы криптографии / А.П. Алферов, А.Ю. Зубов, А.С. Кузьмин, А.В. Черемушкин. – М.: Гелиос АРВ, 2005.
2. Зубов, А.Ю. Криптографические методы защиты информации. Совершенные шифры / А.Ю. Зубов. – М.: Гелиос АРВ, 2005.
3. Рацеев, С.М. О совершенных шифрах на основе ортогональных таблиц / С.М. Рацеев, О.И. Череватенко // Вестник ЮУрГУ. Серия «Математическое моделирование и программирование». – 2014. Т. 7, № 2. – С. 66–73.
4. Рацеев, С.М. О совершенных имитостойких шифрах / С.М. Рацеев // Прикладная дискретная математика. – 2012. – Т. 17, № 3. – С. 41–47.
5. Рацеев, С.М. О совершенных имитостойких шифрах замены с неограниченным ключом / С.М. Рацеев // Вестник Самарского государственного университета. Естественнонаучная серия. – 2013. – Т. 110, № 9/1. – С. 42–48.
6. Рацеев, С.М. О построении совершенных шифров / С.М. Рацеев // Вестник Самарского государственного технического университета. Серия Физ.-мат. науки. – 2014. – Т. 34, № 1. – С. 192–199.
7. Рацеев, С.М. О теоретически стойких шифрах / С.М. Рацеев // Системы и средства информатики. – 2014. – Т. 24, № 1. – С. 61–72.
8. Холл, М. Комбинаторика: пер. с англ. / М. Холл. — М.: Мир, 1970.

Сергей Михайлович Рацеев, кандидат физико-математических наук, доцент, кафедра «Информационная безопасность и теория управления», Ульяновский государственный университет (г. Ульяновск, Российская Федерация), RatseevSM@mail.ru.

Поступила в редакцию 18 сентября 2014 г.

MSC 68P25, 94A60 **DOI: 10.14529/mmp150109**

Some Generalizations of Shannon's Theory of Perfect Ciphers

S.M. Ratseev, Ulyanovsk State University, Ulyanovsk, Russian Federation, RatseevSM@mail.ru.

K. Shannon in the 1940s introduced the concept of a perfect cipher, which provides the best protection of plaintexts. Perfect secrecy means that a cryptanalyst can obtain no information about the plaintext by observing the ciphertext. It is well known that the Vernam cipher with equiprobable gamma is a perfect cipher but it is not imitation resistant because it uses equipotent alphabets for plaintexts and ciphertexts. Also in this cipher should be used equiprobable key sequences that are not always reached. In this review paper discusses the problems of constructing perfect and $(k|y)$-perfect ciphers for a given set of parameters. We give necessary and sufficient conditions for these ciphers. We construct perfect and $(k|y)$-perfect substitution ciphers with unlimited key and imitation resistant perfect ciphers. We study the case when the random generator of key sequences does not necessarily have a uniform probability distribution.

Keywords: cipher; perfect cipher; imitation of message.

References

1. Alferov A.P., Zubov A.Yu., Kuz'min A.S., Cheremushkin A.V. Osnovy kriptografii [Foundations of Cryptography]. Moscow, Gelios ARV, 2005. 480 p.
2. Zubov A.Yu. Kriptograficheskie metody zashhity informacii. Sovershennye shifry [Cryptographic Methods of Information Security. Perfect ciphers]. Moscow, Gelios ARV, 2005. 192 p.
3. Ratseev S.M., Cherevatenko O.I. [On Perfect Ciphers Based on Orthogonal Tables]. *Bulletin of the South Ural State University. Series: Mathematical Modelling, Programming & Computer Software*, 2014, vol. 7, issue 2, pp. 66–73. (in Russian)
4. Ratseev S.M. [On Perfect Imitation Resistant Ciphers]. *Prikladnaya Diskretnaya Matematika* [Applied Discrete Mathematics], 2012, vol. 17, issue 3, pp. 41–47. (in Russian)
5. Ratseev S.M. [On Perfect Imitation Resistant Ciphers with Unbounded Key]. *Vestnik Samarskogo Gosudarstvennogo Universiteta* [*Vestnik Samara Proposition University*], 2013, vol. 110, issue 9/1, pp. 45–50. (in Russian)
6. Ratseev S.M. [On Construction of Perfect Ciphers]. *Vestn. Samar. Gos. Tekhn. Univ. Ser. Fiz.-Mat. Nauki* [Journal of Samara State Technical University. Ser. Physical and Mathematical Sciences], 2014, vol. 34, issue 1, pp. 192–199. (in Russian)
7. Ratseev S.M. [On Theoretically Perfect Ciphers]. *Sistemy i sredstva informatiki* [Systems and Means of Informatics], 2014, vol. 24, issue 1, pp. 61–72. (in Russian)
8. Holl M. Combinatorics. Waltham (Massachusetts), Blaisdell Publishing, 1967. 310 p.

Received September 18, 2014