2012 Математические методы криптографии №3(17)

DOI 10.17223/20710410/17/5

УДК 519.7

О СОВЕРШЕННЫХ ИМИТОСТОЙКИХ ШИФРАХ

С. М. Рацеев

Ульяновский государственный университет, г. Ульяновск, Россия

E-mail: RatseevSM@rambler.ru

В работе приводятся конструкции совершенных имитостойких шифров.

Ключевые слова: *шифр, совершенный шифр, имитация сообщения.*

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 [1], 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:

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

Обозначим через $K(x, y)$ множество таких ключей $k \in K$, для которых $E_k(x) = y$. Условная вероятность $P_{Y|X}(y|x)$ определяется естественным образом:

$$P_{Y|X}(y|x) = \begin{cases} \sum\limits_{k\in K(x,y)} P_K(k), & \text{если } K(x,y) \neq \varnothing, \\ 0, & \text{если } K(x,y) = \varnothing. \end{cases}$$

С помощью теоремы умножения вероятностей можно определить и условную вероятность $P_{Y|X}(y|x)$:

$$P_{X|Y}(x|y) = \frac{P_X(x)P_{Y|X}(y|x)}{P_Y(y)}.$$

Напомним, что шифр Σ_B называется совершенным по Шеннону, если для любых $x \in X$ и $y \in Y$ выполняется равенство $P_{X|Y}(x|y) = P_X(x)$. Для совершенного по Шеннону шифра можно дать и эквивалентные определения.

Утверждение 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 $P_{Y|X}(y|x_1) = P_{Y|X}(y|x_2)$.

Для удобства читателей сформулируем и докажем следующее несложное, но важное утверждение.

Теорема 1. Пусть для шифра Σ_B выполнены следующие условия:

(i) для любой пары $(x, y) \in X \times Y$ существует, и притом единственный, ключ $k \in K$, такой, что $E_k(x) = y$, где E_k — правило зашифрования на ключе k;

(ii) распределение вероятностей $P(K)$ является равномерным.

Тогда шифр Σ_B является совершенным по Шеннону, причём распределение вероятностей $P(Y)$ является равномерным и $|K| = |Y|$.

Доказательство. Пусть выполнены условия теоремы. Покажем, что в этом случае выполнен пункт (ii) утверждения 1.

Из условий теоремы и определения вероятности $P_{Y|X}(y|x)$ следует равенство $P_{Y|X}(y|x) = P_K(k) = 1/|K|$. Зафиксируем произвольное значение $y \in Y$. Применяя формулу полной вероятности, получаем

$$P_Y(y) = \sum_{x \in X} P_X(x) P_{Y|X}(y|x) = \sum_{x \in X} P_X(x) \cdot \frac{1}{|K|} = \frac{1}{|K|}.$$

Таким образом, для любых $x \in X$ и $y \in Y$ имеет место равенство $P_{Y|X}(y|x) = P_Y(y)$, распределение вероятностей на множестве Y является равномерным и $|K| = |Y|$. ■

Будем говорить, что матрица A порядка $m \times n$, $m \geqslant n$, над некоторым m-элементным множеством S является латинским прямоугольником относительно столбцов, если транспонированная матрица A является латинским прямоугольником над множеством S.

Пусть матрица A порядка $m \times n$, $m \geqslant n$, над множеством шифрованных текстов $Y = \{y_1, \ldots, y_m\}$ является латинским прямоугольником относительно столбцов. Пусть $|K| = m$, $|X| = n$. Занумеруем строки матрицы A элементами множества K, а столбцы — элементами множества X. Если матрица A является матрицей зашифрования для некоторого шифра Σ_B и распределение вероятностей $P(K)$ является равномерным, то из теоремы 1 следует, что шифр Σ_B является совершенным по Шеннону.

Рассмотрим вероятностное пространство $\Omega = (K, F_K, P_K)$. Зафиксируем $y \in Y$. Обозначим через $K(y)$ следующее множество: $K(y) = \{k \in K : y \in E_k(X)\}$. Под обозначением $K(y)$ будем также понимать событие $(K(y) \in F_K)$, заключающееся в том, что при случайном выборе ключа $k \in K$ шифртекст y можно расшифровать на ключе k, то есть $y \in E_k(X)$. Тогда событию $K(y)$ благоприятствуют все элементы из множества $K(y)$, и только они. Поэтому $P(K(y)) = \sum\limits_{k \in K(y)} P_K(k)$.

Если канал связи готов к работе и на приёме установлены действующие ключи, но в данный момент времени никакого сообщения не передаётся, то противником может быть предпринята попытка имитации сообщения. Вероятность успеха имитации определяется следующим образом:

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

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 рассчитывает 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

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

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

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

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

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

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

Утверждение 2. Пусть A — некоторая $(m \times n)$-матрица над множеством $Y = \{y_1, \ldots, y_m\}$, $m \geqslant n$, которая является латинским прямоугольником относительно столбцов. Тогда если распределение вероятностей $P(K)$ является равномерным, то для шифра Σ_B с матрицей зашифрования A выполнено равенство $P_{\text{im}} = n/m$.

Утверждение 3. Для любых натуральных чисел m и n, таких, что $m \geqslant n$ и $n \neq m-1$, существует латинский $(m \times n)$-прямоугольник относительно столбцов, в котором имеется ровно n строк, содержащих два различных фиксированных элемента.

Доказательство. Если $m = n$, то все очевидно. Поэтому пусть $m \geqslant n+2$. Построим латинский прямоугольник A над множеством $\{1, 2, \ldots, m\}$ следующим образом. Расположим число 1 в A на позициях с координатами $(1,1)$, $(2,2)$, …, (n,n), а число 2 — на позициях $(1,2)$, $(2,3)$, …, $(n-1,n)$, $(n,1)$.

Обозначим через T^i циклический сдвиг на i позиций влево. В матрице A в i-м столбце на свободные позиции поставим элементы $T^{i-1}(3, 4, \ldots, m)$, $i = 1, \ldots, n$. Тогда полученная матрица является латинским прямоугольником относительно столбцов с требуемым свойством. ■

Из данного утверждения следует, что для любых натуральных чисел m и n, $m \geqslant n$ и $n \neq m-1$, можно построить такой латинский прямоугольник A размера $m \times n$ над множеством $Y = \{y_1, \ldots, y_m\}$, что при равномерном распределении вероятностей $P(K)$ для шифра Σ_B с матрицей зашифрования A будет выполнено равенство $P_{\text{podm}} = 1$. Отдельно рассмотрим случай $n = m-1$.

Утверждение 4. Пусть $A = A(n+1, n)$ — некоторая матрица над множеством $Y = \{y_1, \ldots, y_{n+1}\}$, которая является латинским прямоугольником относительно столбцов. Тогда если распределение вероятностей $P(K)$ является равномерным, то для шифра Σ_B с матрицей зашифрования A выполнено равенство $P_{\text{podm}} = (n-1)/n$.

Доказательство. Заметим, что из равномерности распределения $P(K)$ следует, что для любых $\widetilde{y}, y \in Y$, $\widetilde{y} \neq y$, выполнено равенство

$$P(K(\widetilde{y} \mid K(y))) = \frac{|K(\widetilde{y}, y)|}{|K(y)|}.$$

Дополним матрицу A до латинского квадрата B размера $(n+1) \times (n+1)$ [3]. Зафиксируем произвольный элемент $y_0 \in Y$. Так как матрица B является латинским квадратом, то элемент y_0 присутствует в последнем столбце матрицы B. Пусть он находится на позиции $(i_0, n+1)$. Это означает, что в матрице A элемент y_0 встречается во всех строках, кроме строки с номером i_0, а в i_0-й строке матрицы A расположены все элементы множества $Y \setminus \{y_0\}$. Поэтому для любого $y \in Y \setminus \{y_0\}$ выполнено равенство $|K(y, y_0)| = n-1$. Очевидно также, что для любого $y \in Y$ выполнено равенство $|K(y)| = n$. В силу произвольности y_0, из теоремы 2 следует, что $P_{\text{podm}} = (n-1)/n$. ■

Несложно проверить также следующее

Утверждение 5. Пусть B — квадрат Виженера над множеством $Y = \{y_1, \ldots, y_m\}$. Составим из первых n столбцов матрицы B матрицу A, где $1 \leqslant n \leqslant m-1$. Пусть $|K| = m$, $|X| = n$, матрица A является матрицей зашифрования для шифра Σ_B и распределение вероятностей $P(K)$ является равномерным. Тогда для шифра Σ_B выполнено равенство $P_{\text{podm}} = (n-1)/n$.

Определённая 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 определённой константой. В работе [2] приводятся модели шифров замены с ограниченным и неограниченным ключом, для которых, в частности, на множество X такое ограничение не накладывается. Поскольку в общем случае шифр замены с ограниченным ключом совершенным не является [2], нас будет интересовать шифр замены с неограниченным ключом. Приведем модель данного шифра.

Пусть U — конечное множество возможных шифрвеличин, а V — конечное множество возможных шифробозначений. Пусть имеются $r > 1$ инъективных отображений (простых замен) из U в V. Пронумеруем данные отображения: E_1, E_2, …, E_r. Обозначим $\mathbb{N}_r = \{1, 2, \ldots, r\}$. Опорным шифром шифра замены назовём совокупность $\Sigma = (U, \mathbb{N}_r, V, E, D)$, для которой выполнены следующие свойства:

1) для любых $u \in U$ и $j \in \mathbb{N}_r$ выполнено равенство $D_j(E_j(u)) = u$;

2) $V = \bigcup\limits_{j \in \mathbb{N}_r} E_j(U)$.

При этом $E = \{E_1, \ldots, E_r\}$, $D = \{D_1, \ldots, D_r\}$, $D_j : E_j(U) \to U$, $j \in \mathbb{N}_r$.

Назовём l-й степенью опорного шифра Σ совокупность $\Sigma^l = \left(U^l, \mathbb{N}_r^l, V^l, E^{(l)}, D^{(l)}\right)$, где $U^l, \mathbb{N}_r^l, V^l$ — декартовы степени соответствующих множеств. Множество $E^{(l)}$ состоит из отображений $E_{\overline{j}} : U^l \to V^l$, $\overline{j} \in \mathbb{N}_r^l$, таких, что для любых $\overline{u} = u_1 \ldots u_l \in U^l$, $\overline{j} = j_1 \ldots j_l \in \mathbb{N}_r^l$ выполнено равенство

$$E_{\overline{j}}(\overline{u}) = E_{j_1}(u_1) \ldots E_{j_l}(u_l) = v_1 \ldots v_l \in V^l,$$

а множество $D^{(l)}$ состоит из отображений $D_{\overline{j}} : E_{\overline{j}}(U^l) \to U^l$, $\overline{j} \in \mathbb{N}_r^l$, таких, что для любых $\overline{v} = v_1 \ldots v_l \in V^l$, $\overline{j} = j_1 \ldots j_l \in \mathbb{N}_r^l$ выполнено равенство

$$D_{\overline{j}}(\overline{v}) = D_{j_1}(v_1) \ldots D_{j_l}(v_l) = u_1 \ldots u_l \in U^l.$$

Пусть ψ_c — случайный генератор ключевого потока, который для любого натурального числа l вырабатывает случайный ключевой поток $j_1 \ldots j_l$, $j_i \in \mathbb{N}_r$.

Обозначим через Σ_H^l следующую совокупность величин:

$$\Sigma_H^l = \left(U^l, \mathbb{N}_r^l, V^l, E^{(l)}, D^{(l)}, P(U^l), P(\mathbb{N}_r^l)\right).$$

Шифром замены с неограниченным ключом назовем семейство

$$\Sigma_H = \left(\Sigma_H^l, l \in \mathbb{N}; \psi_c\right).$$

При этом независимые и не содержащие нулевых вероятностей распределения $P(U^l)$ и $P(\mathbb{N}_r^l)$ индуцируют распределения вероятностей на множестве V^l:

$$P_{V^l}(\overline{v}) = \sum_{\substack{(\overline{u}, \overline{j}) \in U^l \times \mathbb{N}_r^l, \\ E_{\overline{j}}(\overline{u}) = \overline{v}}} P_{U^l}(\overline{u}) P_{\mathbb{N}_r^l}(\overline{j}).$$

Определим условные вероятности $P_{U^l|V^l}(\overline{u}|\overline{v})$ и $P_{V^l|U^l}(\overline{v}|\overline{u})$:

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

где $\mathbb{N}_r^l(\overline{u},\overline{v}) = \{\overline{\jmath}\in\mathbb{N}_r^l : E_{\overline{\jmath}}(\overline{u}) = \overline{v}\}$. Говорят, что шифр Σ_H является совершенным тогда и только тогда, когда для любого натурального l шифр Σ_H^l является совершенным по Шеннону.

Утверждение 6. 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

$$P_{V^l|U^l}(\overline{v}|\overline{u}_1) = P_{V^l|U^l}(\overline{v}|\overline{u}_2).$$

Теорема 3. Пусть для шифра замены Σ_H выполнены следующие условия:

(i) простые замены E_1, E_2,..., E_r шифра Σ_H обладают тем свойством, что для любого $u\in U$ и любого $v\in V$ найдется, и при том единственный, элемент $j = j(u,v)\in\mathbb{N}_r$, что $E_j(u) = v$;

(ii) распределение вероятностей $P(\mathbb{N}_r)$ для случайного генератора ψ_c является равномерным.

Тогда шифр Σ_H является совершенным, причём для любого $l\in\mathbb{N}$ выполнено равенство $|V^l| = r^l$ и распределение вероятностей $P(V^l)$ является равномерным.

Доказательство. Зафиксируем произвольное натуральное число l. Из условия (i) следует, что для любых $\overline{u} = u_1\dots u_l\in U^l$ и $\overline{v} = v_1\dots v_l\in V^l$ найдется, и причём единственный, ключевой поток $\overline{\jmath} = j_1\dots j_l\in\mathbb{N}_r^l$, зависящий от $\overline{u}$ и $\overline{v}$, что

$$E_{\overline{\jmath}}(\overline{u}) = E_{j_1}(u_1)\dots E_{j_l}(u_l) = v_1\dots v_l = \overline{v}.$$

Из данного свойства и того, что $P_{\mathbb{N}_r^l}(\overline{\jmath}) = P_{\mathbb{N}_r}(j_1)\cdot\ldots\cdot P_{\mathbb{N}_r}(j_l) = 1/r^l$ для любого $\overline{\jmath}\in\mathbb{N}_r^l$ (условие (ii) теоремы 1), следует справедливость данной теоремы. ■

Обозначим через P_{im}^l и P_{podm}^l соответственно вероятности успеха имитации и подмены сообщений для шифра Σ_H^l. Из теоремы 2 следует, что если для некоторого шифра Σ_H выполнено равенство $|U| = |V|$, где U, V — множества шифрвеличин и шифробозначений соответственно, то $P_{\text{im}}^l = P_{\text{podm}}^l = 1$ для любого натурального l, то есть такие шифры максимально уязвимы к угрозам имитации и подмены сообщения.

Утверждение 7. Пусть A — некоторая $(n+1,n)$-матрица над множеством шифробозначений $V = \{v_1,\dots,v_{n+1}\}$, которая является латинским прямоугольником относительно столбцов, и пусть матрица A является матрицей зашифрования для опорного шифра замены с неограниченным ключом Σ_H. Пусть также случайный генератор

ключевых последовательностей φ_c из конструкции шифра Σ_H имеет равномерное распределение. Тогда для любого натурального l шифр Σ_H^l является совершенным по Шеннону и выполнены следующие равенства:

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

то есть $P_{\text{im}}^l, P_{\text{podm}}^l \to 0$ при $l \to +\infty$.

Доказательство следует из теоремы 3 и предложений 2 и 4.

В вероятностной модели шифра Σ_B множества X и Y конечны, поэтому вероятности P_{im} и P_{podm} имеют достижимые нижние оценки (теорема 2). Так как для любого фиксированного натурального числа l множества U^l и V^l также конечны, то для шифра Σ_H^l вероятности P_{im}^l и P_{podm}^l также ограничены снизу. Но в модели шифра Σ_H ограничения на длины сообщений снимаются, поэтому с ростом числа l (длин сообщений) вероятности P_{im}^l и P_{podm}^l стремятся к 0 при выполнении условий предложения 7.

Таким образом, если в качестве матрицы зашифрования A для опорного шифра Σ использовать латинский квадрат (например, квадрат Виженера), то при равномерном распределении $P(\mathbb{N}_r)$ шифр Σ_H будет совершенным, но максимально уязвимым к угрозам имитации и подмены. Но стоит в данном квадрате Виженера вычеркнуть, например, последний столбец, как шифр Σ_H с полученной матрицей зашифрования для опорного шифра Σ приобретёт два дополнительных свойства.

ЛИТЕРАТУРА

1. *Алферов А. П., Зубов А. Ю., Кузьмин А. С., Черемушкин А. В.* Основы криптографии. М.: Гелиос АРВ, 2005. 480 с.
2. *Зубов А. Ю.* Криптографические методы защиты информации. Совершенные шифры. М.: Гелиос АРВ, 2005. 192 с.
3. *Холл М.* Комбинаторика. М.: Мир, 1970. 424 с.