УДК 519.7

О СОВЕРШЕННЫХ ИМИТОСТОЙКИХ ШИФРАХ ЗАМЕНЫ С НЕОГРАНИЧЕННЫМ КЛЮЧОМ

© 2013 С.М. Рацеев[1]

В работе исследуются совершенные шифры, стойкие к имитации и подмене сообщений. Хорошо известно, что 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. На основе математической модели шифра замены с неограниченным ключом, предложенной А.Ю. Зубовым, в работе приводится конструкция шифра, который обладает указанными тремя свойствами. При этом опорный шифр данной модели является совершенным и достигает нижних границ для вероятностей успеха имитации и подмены сообщений.

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 (см. [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:

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

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

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

[1]Рацеев Сергей Михайлович (RatseevSM@mail.ru), кафедра информационной безопасности и теории управления Ульяновского государственного университета, 432017, Российская Федерация, г. Ульяновск, ул. Льва Толстого, 42.

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.

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

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

Приведем критерий совершенных шифров в классе шифров с равномерным распределением вероятностей на множестве ключей K.

Теорема 1. Пусть для шифра Σ_B выполнено двойное неравенство $|X| \leqslant |Y| \leqslant |K|$, и распределение вероятностей $P(K)$ является равномерным. Тогда шифр Σ_B является совершенным по Шеннону тогда и только тогда, когда выполнены следующие условия:

(i) для любых $x \in X$ и $y \in Y$ 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. Пусть шифр Σ_B является совершенным по Шеннону. Тогда пункт (i) следует из предложения 1 и того факта, что распределения вероятностей $P(X)$, $P(K)$ и $P(Y)$ не содержат нулевых вероятностей. Далее из предложения 1 следует, что для любых $x_1, x_2 \in X$ и $y \in Y$ выполнено равенство $P_{Y|X}(y|x_1) = P_{Y|X}(y|x_2)$. Так как распределение вероятностей на $P(K)$ является равномерным, то

$$\frac{|K(x_1, y)|}{|K|} = P_{Y|X}(y|x_1) = P_{Y|X}(y|x_2) = \frac{|K(x_2, y)|}{|K|}.$$

Поэтому следует равенство $|K(x_1, y)| = |K(x_2, y)|$ для любых $x_1, x_2 \in X$ и $y \in Y$, что показывает справедливость пункта (ii).

Обратно, пусть выполнены пункты (i) и (ii). Из (i) следует, что $|K(x, y)| > 0$ для любых $x \in X$, $y \in Y$, а из (ii) следует такое равенство для любых $x_1, x_2 \in X$, $y \in Y$:

$$P_{Y|X}(y|x_1) = \frac{|K(x_1, y)|}{|K|} = \frac{|K(x_2, y)|}{|K|} = P_{Y|X}(y|x_2).$$

Поэтому из предложения 1 следует, что шифр Σ_B является совершенным по Шеннону. Теорема доказана.

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 $k \in K$ шифртекст 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 2 ([2]). Для любого шифра Σ_B справедливы неравенства

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

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 $P(K(\widetilde{y}) \mid K(y)) = (|X|-1)/(|Y|-1)$.

Пусть $Y = \{y_1, ..., y_n\}$, 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 Y, 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 2. Пусть $|K| = n^2 - n$, $|X| = 2$. Занумеруем строки матрицы M элементами множества K, а столбцы — элементами множества X. Пусть

матрица M является матрицей зашифрования для некоторого шифра Σ_B и распределение вероятностей $P(K)$ является равномерным. Тогда шифр Σ_B является совершенным по Шеннону, и для шифра Σ_B одновременно достигаются нижние границы для вероятностей P_{im} и P_{podm}:

$$P_{im} = \frac{2}{n}, \quad P_{podm} = \frac{1}{n-1}.$$

Доказательство следует из теорем 1 и 2.

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. Поскольку в общем случае шифр замены с ограниченным ключом совершенным не является (см. [2]), нас будет интересовать шифр замены с неограниченным ключом. Такая математическая модель имеет ряд полезных свойств, например, она позволяет строить модели совершенных шифров, стойких к имитации и подмене (см. [3]). Приведем модель данного шифра.

Пусть U — конечное множество возможных шифрвеличин, а V — конечное множество возможных шифробозначений. Пусть также имеются r $(r > 1)$ инъективных отображений из U в V. Пронумеруем данные отображения: E_1, E_2,..., E_r. Они называются простыми заменами. Обозначим $\mathbb{N}_r = \{1, 2, ..., r\}$. Опорным шифром шифра замены назовем 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) $V = \bigcup_{j \in \mathbb{N}_r} E_j(U)$.

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

l-й степенью опорного шифра Σ назовем совокупность

$$\Sigma^l = (U^l, \mathbb{N}_r^l, V^l, E^{(l)}, D^{(l)}),$$

где $U^l, \mathbb{N}_r^l, V^l$ — декартовы степени соответствующих множеств U, $\mathbb{N}_r$, V. 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 $\overline{u} = u_1...u_l \in U^l$, $\overline{j} = j_1...j_l \in \mathbb{N}_r^l$ выполнено равенство

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

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 $\overline{v} = v_1...v_l \in V^l$, $\overline{j} = j_1...j_l \in \mathbb{N}_r^l$ выполнено равенство

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

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

Обозначим через Σ_H^l следующую совокупность величин:

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

Шифром замены с неограниченным ключом назовем семейство

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

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:

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

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

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

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

Предложение 3. 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 Σ_H выполнены неравенства

$$|U|\leqslant|V|\leqslant r,$$

и распределение вероятностей $P(\mathbb{N}_r)$ является равномерным. Тогда шифр Σ_H 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

$$|\mathbb{N}_r(u_1,v)| = |\mathbb{N}_r(u_2,v)|.$$

Доказательство. Пусть шифр Σ_H является совершенным. Тогда, в частности, опорный шифр шифра Σ_H будет являться совершенным по Шеннону. Поэтому условия (i) и (ii) следуют из теоремы 1.

Обратно, пусть выполнены условия (i) и (ii) для шифра Σ_H. Зафиксируем произвольное значение $l\in\mathbb{N}$. Из пункта (i) следует, что для любых $\overline{u} = u_1...u_l\in\in U^l$ и $\overline{v} = v_1...v_l\in V^l$ найдется такой ключевой поток $\overline{\jmath} = j_1...j_l\in\mathbb{N}_r^l$, зависящий от $\overline{u}$ и $\overline{v}$, что

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

Далее, зафиксируем произвольным образом некоторые значения $\overline{a} = a_1...a_l\in U^l$, $\overline{b} = b_1...b_l\in U^l$, $\overline{v} = v_1...v_l\in V^l$. Тогда

$$|\mathbb{N}_r(\overline{a},\overline{v})| = \prod_{i=1}^{l}|\mathbb{N}_r(a_i,v_i)| \overset{(ii)}{=} \prod_{i=1}^{l}|\mathbb{N}_r(b_i,v_i)| = |\mathbb{N}_r(\overline{b},\overline{v})|.$$

Таким образом, из теоремы 1 следует, что шифр Σ_H^l является совершенным по Шеннону. В силу произвольности значения l следует совершенность шифра Σ_H. Теорема доказана.

Обозначим через P_{im}^{l} вероятность успеха имитации сообщения для шифра Σ_H^l, а через $P_{podm}^{l}(s)$ — вероятность успеха подмены в сообщении длины l ровно s символов для шифра Σ_H^l, где $s \leqslant l$. Из теоремы 2 следует, что если для некоторого шифра Σ_H выполнено равенство $|U| = |V|$, где U, V — множества шифрвеличин и шифробозначений соответственно, то $P_{im}^{l} = P_{podm}^{l}(s) = 1$ для любых натуральных l и $s \leqslant l$, то есть такие шифры максимально уязвимы к угрозам имитации и подмены сообщения. В следующем предложении приводится шифр замены с неограниченным ключом, опорный шифр которого является совершенным и достигает нижних границ для вероятностей успеха имитации и подмены сообщений.

Предложение 4. Пусть $M = M(n^2 - n, 2)$ — матрица над множеством $V = \{v_1, ..., v_n\}$, построенная перед предложением 2, $r = n^2 - n$, $|U| = 2$, 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 по Шеннону и выполнены следующие равенства:

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

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

Доказательство следует из предложения 2 и теоремы 3.

Литература

[1] Основы криптографии / А.П. Алферов [и др.]. М.: Гелиос АРВ, 2005.

[2] Зубов А.Ю. Криптографические методы защиты информации. Совершенные шифры. М.: Гелиос АРВ, 2005.

[3] Рацеев С.М. О совершенных имитостойких шифрах // Прикладная дискретная математика. 2012. № 3(17). С. 41–47.

Поступила в редакцию 23/*IX*/2013;
в окончательном варианте — 23/*IX*/2013.

ON PERFECT IMITATION RESISTANT CIPHERS OF SUBSTITUTION WITH UNBOUNDED KEY

© 2013 S.M. Ratseev[2]

Constructions of perfect imitation resistant ciphers are investigated in the work. It is well known that Vernam cipher with equiprobable gamma is a perfect cipher but it is not imitation resistant. It is because in Vernam cipher equipotent alphabets for plaintexts and ciphertexts are used. On the basis of A.Yu. Zubov's mathematical model of substitution cipher with unbounded key a model of perfect and imitation resistant cipher is constructed. At that reference cypher of the given model is perfect and reaches lower boundaries for success probability of imitation and substitution of communication.

key words: cipher, perfect cipher, imitation of communication.

Paper received 23/*IX*/2010.
Paper accepted 23/*IX*/2010.

[2]Ratseev Sergey Mihailovich (RatseevSM@mail.ru), the Dept. of Information Security and Control Theory, Ulyanovsk State University, Ulyanovsk, 432017, Russian Federation.