УДК 519.7

С.М. Рацеев, В.М. Рацеев[1]

ПОСТРОЕНИЕ СОВЕРШЕННЫХ ИМИТОСТОЙКИХ ШИФРОВ НА ОСНОВЕ КОМБИНАТОРНЫХ ОБЪЕКТОВ

В статье исследуются совершенные шифры, стойкие к имитации и подмене шифрованных сообщений. Особо выделен случай, когда вероятности имитации и подмены достигают нижних границ. На основе математической модели шифра замены с неограниченным ключом, предложенной А.Ю. Зубовым, в статье приводится конструкция совершенного шифра на основе комбинаторных объектов, стойкого к имитации и подмене.

Ключевые слова: шифр, совершенный шифр, имитация сообщения.

Все необъясняемые понятия можно найти в [1]. Пусть $\Sigma_B = (X, K, Y, E, D, P_X, P_K)$ — вероятностная модель шифра. 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. В работе [2] приводится критерий совершенных шифров с фиксированным набором параметров. Пусть $x \in X$, $y \in Y$. Обозначим $K(x, y) = \{k \in K \mid E_k(x) = y\}$.

Нам понадобится следующий критерий совершенных шифров в классе шифров с равномерным распределением вероятностей на множестве K.

Теорема 1 [3]. 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 $|K(x_1, y)| = |K(x_2, y)|$.

Рассмотрим вероятностное пространство $(\Omega = K, F_K, P_K)$. Зафиксируем $y \in Y$. Обозначим $K(y) = \{k \in K \mid y \in E_k(X)\}$. 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

Рацеев Сергей Михайлович (RatseevSM@mail.ru), кафедра информационной безопасности и теории управления, Ульяновский государственный университет, 432017, Российская Федерация, г. Ульяновск, ул. Льва Толстого, 42.

Рацеев Владимир Михайлович, кафедра телекоммуникационных технологий и сетей, Ульяновский государственный университет, 432017, Российская Федерация, г. Ульяновск, ул. Льва Толстого, 42.

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 [1]. Для любого шифра Σ_B, $|X| = m$, $|Y| = n$, справедливы неравенства

$$P_{im} \geqslant \frac{m}{n}, \quad P_{podm} \geqslant \frac{m-1}{n-1}.$$

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

Будем говорить, что шифр Σ_B является имитостойким, если для него достигаются нижние границы для вероятностей успехов имитации и подмены шифрованных сообщений. В следующем утверждении приводится конструкция имитостойких шифров на основе сочетаний.

Утверждение 1. Пусть для шифра Σ_B выполнены следующие условия:

(i) $|X| = m$, $|Y| = n$, $1 < m < n$, $|K| = C_n^m$, C_n^m — число сочетаний из n по m, и все строки матрицы зашифрования являются сочетаниями из n элементов множества Y по m;

(ii) распределение вероятностей P_K равномерно.

Тогда $P_{im} = m/n$, $P_{podm} = (m-1)/(n-1)$.

Доказательство. Пусть $y, \widetilde{y} \in Y$, $y \neq \widetilde{y}$. Тогда

$$P(K(y)) = \frac{|K(y)|}{|K|} = \frac{C_{n-1}^{m-1}}{C_n^m} = \frac{m}{n}.$$

$$P(K(\widetilde{y}) \mid K(y)) = \frac{|K(\widetilde{y}, y)|}{|K(y)|} = \frac{C_{n-2}^{m-2}}{C_{n-1}^{m-1}} = \frac{m-1}{n-1}.$$

Поэтому из теоремы 2 следует, что

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

□

В следующей теореме приводится конструкция совершенных имитостойких шифров на основе размещений.

Теорема 3. Пусть для шифра Σ_B выполнены следующие условия:

(i) $|X| = m$, $|Y| = n$, $1 < m < n$, $|K| = A_n^m$, A_n^m — число размещений из n по m, и все строки матрицы зашифрования являются размещениями из n элементов множества Y по m;

(ii) распределение вероятностей P_K равномерно.

Тогда шифр Σ_B является совершенным, причем $P_{im} = m/n$, $P_{podm} = (m-1)/(n-1)$.

Доказательство. Пусть $x \in X$, $y \in Y$. Так как $|K(x, y)| = A_{n-1}^{m-1}$, то из теоремы 1 следует, что шифр Σ_B является совершенным.

Пусть $y, \widetilde{y} \in Y$, $y \neq \widetilde{y}$. Тогда

$$P(K(y)) = \frac{|K(y)|}{|K|} = \frac{mA_{n-1}^{m-1}}{A_n^m} = \frac{m}{n}.$$

$$P(K(\widetilde{y}) \mid K(y)) = \frac{|K(\widetilde{y}, y)|}{|K(y)|} = \frac{A_m^2 A_{n-2}^{m-2}}{mA_{n-1}^{m-1}} = \frac{m-1}{n-1}.$$

Поэтому из теоремы 2 следует, что

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

□

Определенная вероятностная модель шифра Σ_B позволяет рассматривать лишь конечные множества открытых текстов X. В работе [1] приводятся модели шифров замены с ограниченным и неограниченным ключом, для которых, в частности, на множество X такое ограничение не накладывается. Пусть

$$\Sigma^l = (U^l, \mathbb{N}_r^l, V^l, E^{(l)}, D^{(l)}), \quad \Sigma_H = (\Sigma_H^l, \ l \in \mathbb{N}; \ \psi_c)$$

— шифр замены с неограниченным ключом (подробнее см. [3]). В работе [4] приводятся различные конструкции совершенных имитостойких шифров Σ_H. Обозначим $\mathbb{N}_r^l(\overline{u}, \overline{v}) = \{\overline{\jmath} \in \mathbb{N}_r^l \mid E_{\overline{\jmath}}(\overline{u}) = \overline{v}\}$.

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

Теорема 4 [3]. 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 $|\mathbb{N}_r(u_1, v)| = |\mathbb{N}_r(u_2, v)|$.

Для шифра замены с неограниченным ключом Σ_H 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 $s \leqslant l$.

Утверждение 2. Пусть для шифра Σ_H выполнены следующие условия:
(i) $|U| = m$, $|V| = n$, $1 < m < n$, $r = C_n^m$, и все строки матрицы зашифрования опорного шифра Σ являются сочетаниями из n элементов множества V по m;
(ii) распределение вероятностей $P_{\mathbb{N}_r}$ равномерно.
Тогда

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

Доказательство следует из утверждения 1 и теоремы 4. □

Теорема 5. Пусть для шифра Σ_H выполнены следующие условия:
(i) $|U| = m$, $|V| = n$, $1 < m < n$, $r = A_n^m$ и все строки матрицы зашифрования опорного шифра Σ являются размещениями из n элементов множества V по m;
(ii) распределение вероятностей $P_{\mathbb{N}_r}$ равномерно.
Тогда шифр Σ_H является совершенным, причем

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

Доказательство следует из теорем 3 и 4. □

Заметим, что для шифров Σ_H из утверждения 2 и теоремы 5 выполнено условие $P_{im}^l \to 0$ при $l \to \infty$, $P_{podm}^l(s) \to 0$ при $s \to \infty$.

Литература

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

[2] Рацеев С.М. О построении совершенных шифров // Вестн. Сам. гос. техн. ун-та. Сер.: Физ.-мат. науки. 2014. № 1 (34). С. 192–199.

[3] Рацеев С.М. О совершенных имитостойких шифрах замены с неограниченным ключом // Вестник Самарского государственного университета. Естественнонаучная серия. 2013. № 9/1 (110). С. 42–48.

[4] Рацеев С.М. Некоторые обобщения теории Шеннона о совершенных шифрах // Вестн. ЮУрГУ. Сер.: Матем. моделирование и программирование. 2015. № 1 (8). С. 111–127.

References

[1] Zubov A.Yu. Kriptograficheskie metody zashchity informatsii. Sovershennye shifry [Cryptographic Methods of Information Security. Perfect ciphers]. M.: Gelios ARV, 2005 [in Russian].

[2] Ratseev S.M. O postroenii sovershennykh shifrov [On Construction of Perfect Ciphers]. *Vestn. Samar. Gos. Tekhn. Un-ta. Ser. Fiz.-Mat. Nauki* [Journal of Samara State Technical University, Ser. Physical and Mathematical Sciences], 2014, no. 1(34), pp. 192–199 [in Russian].

[3] Ratseev S.M. O sovershennykh imitostoikikh shifrakh zameny s neogranichennym kliuchom [On Perfect Imitation Resistant Ciphers with Unbounded Key]. *Vestnik Samarskogo Gosudarstvennogo Universiteta* [Vestnik of Samara State University], 2013, no. 9/1 (110), pp. 42–48 [in Russian].

[4] Ratseev S.M. Nekotorye obobshcheniia teorii Shennona o sovershennykh shifrakh [Some generalizations of Shannon's theory of perfect ciphers]. *Vestn. IuUrGU. Ser. Matem. modelirovanie i programmirovanie* [Bulletin of the South Ural State University. Series: "Mathematical Modelling, Programming & Computer Software"], 2015, no. 1(8), pp. 111–127 [in Russian].

S.M. Ratseev, V.M. Ratseev[2]

ON PERFECT IMITATION RESISTANT CIPHERS BASED ON COMBINATORIAL OBJECTS

We study perfect imitation resistant ciphers, highlighting particularly the case in which the probabilities of successful imitation and substitution attain their lower limits. On the basis of A.Yu. Zubov's mathematical model of substitution cipher with unbounded key model of perfect and imitation resistant cipher based on combinatorial objects is constructed.

Key words: cipher, perfect cipher, imitation resistant ciphers.

Статья поступила в редакцию 28/*I*/2016.
The article received 28/*I*/2016.

[2] *Ratseev Sergey Mihaylovich* (RatseevSM@mail.ru), Department of Information Security and Control Theory, Ulyanovsk State University, 42, Lev Tolstoy Street, Ulyanovsk, 432017, Russian Federation.

Ratseev Vladimir Mihaylovich, Department of Telecommunication Technologies and Networks, Ulyanovsk State University, 42, Lev Tolstoy Street, Ulyanovsk, 432017, Russian Federation.