МАТЕМАТИЧЕСКИЕ МЕТОДЫ КРИПТОГРАФИИ

DOI 10.17223/20710410/14/4

УДК 519.7

ПОЧТИ СОВЕРШЕННЫЕ ШИФРЫ И КОДЫ АУТЕНТИФИКАЦИИ

А. Ю. Зубов

Московский государственный университет им. М. В. Ломоносова, г. Москва, Россия

E-mail: Zubovanatoly@yandex.ru

Предлагаются конструкции почти совершенных шифров с экономным расходом ключа, совмещающие функции шифрования и аутентификации при равновероятном выборе ключей и открытых текстов.

Ключевые слова: *почти совершенный шифр, код аутентификации.*

Пусть $\Sigma = (S, K, M, E, D)$ — шифр[1], для которого S, M — множества открытых и шифрованных текстов; K — множество ключей; E — множество правил зашифрования, состоящие из инъективных отображений $E_k : S \to M$ для каждого $k \in K$; D — множество правил расшифрования, состоящее из отображений $D_k : M \to M \cup \{\varnothing\}$, таких, что

$$D_k(m) = \begin{cases} s, & \text{если } E_k(s) = m, \\ \varnothing, & \text{если } m \notin E_k(S). \end{cases}$$

Пусть на множествах S, K определены распределения вероятностей $\mathsf{P}(S)$, $\mathsf{P}(K)$, состоящие соответственно из вероятностей $p_S(s)$ и $p_K(k)$, строго больших нуля для каждого $s \in S$ и $k \in K$. Будем полагать, что при шифровании ключи и открытые тексты выбираются независимо друг от друга. Тогда $\mathsf{P}(S)$, $\mathsf{P}(K)$ естественным образом индуцируют распределение $\mathsf{P}(M)$ на множестве M, состоящее из вероятностей

$$p_M(m) = \sum_{k \in K(m)} p_K(k) \cdot p_S(D_k(m)), \quad m \in M, \tag{1}$$

где $K(m) = \{k \in K : D_k(m) \neq \varnothing\}$.

Так же естественно вводятся условные распределения $\mathsf{P}(S \,|\, M)$ и $\mathsf{P}(M \,|\, S)$. Для каждой пары (s, m) вероятности $p_{S\,|\,M}(s \,|\, m)$ и $p_{M\,|\,S}(m \,|\, s)$ определяются соответственно формулами

$$p_{M\,|\,S}(m \,|\, s) = \sum_{k \in K(s,m)} p_K(k); \tag{2}$$

$$p_{S\,|\,M}(s \,|\, m) = \frac{p_S(s) \cdot p_{M\,|\,S}(m \,|\, s)}{p_M(m)}, \tag{3}$$

где $K(s, m) = \{k \in K : E_k(s) = m\}$.

К. Шеннон назвал шифр Σ совершенным, если для любых $s \in S$, $m \in M$ имеет место равенство

$$p_{S\,|\,M}(s \,|\, m) = p_S(s). \tag{4}$$

[1]Пользуемся определением шифра, приведённым в [1, 2].

Интерес к таким шифрам связан с тем, что шифртекст не даёт вероятностной информации об открытом тексте. В этом смысле не менее интересны шифры Σ, для которых величина

$$\Delta(\Sigma) = \max_{(s,m)} \left| p_{S\,|\,M}(s\,|\,m) - p_S(s) \right|$$

не превосходит достаточно малого действительного числа $\varepsilon \geqslant 0$. Назовём такие шифры почти совершенными, или ε-совершенными. Совершенный шифр является ε-совершенным при $\varepsilon = 0$. Ясно, что такие шифры относятся (как и совершенные шифры) к классу теоретически стойких шифров, поскольку, независимо от используемых потенциальным противником вычислительных ресурсов, они не позволяют определить по шифртексту открытый текст с вероятностью, превосходящей ε. Как известно, недостатком совершенного шифра является большой расход ключа, поскольку для совершенного шифра должны выполняться неравенства $|S| \leqslant |M| \leqslant |K|$ (см. [1]). В связи с этим возникает вопрос о возможности сокращения расхода ключа при переходе от жёсткого условия (4) к менее жёсткому условию $\Delta(\Sigma) \leqslant \varepsilon$.

В работе предлагаются некоторые классы ε-совершенных шифров с равномерными распределениями $\mathsf{P}(S)$, $\mathsf{P}(K)$, допускающие эффективную реализацию, для которых $|K| \ll |S|$. Помимо стойкого шифрования, рассматриваемые шифры гарантируют также стойкую аутентификацию.

Заметим, что для равномерных распределений $\mathsf{P}(S)$, $\mathsf{P}(K)$ вероятность $p_{S\,|\,M}(s\,|\,m)$ представляется в виде

$$p_{S\,|\,M}(s\,|\,m) = \frac{|K(s,m)|}{|K(m)|}.$$

Это следует из формул (1)–(3). Таким образом, в рассматриваемых условиях величина

$$\Delta(s,m) = \left| p_{S\,|\,M}(s\,|\,m) - p_S(s) \right|$$

выражается формулой

$$\Delta(s,m) = \left| \frac{|K(s,m)|}{|K(m)|} - \frac{1}{|S|} \right|. \tag{5}$$

Приведём примеры почти совершенных шифров, построенных на основе кодов из [3].

Пример 1. Пусть F_q — поле характеристики 2, состоящее из q элементов, и r — произвольное натуральное число. Рассмотрим шифр Σ_1, для которого $S = (F_q)^r$, $K = (F_q)^2$ и $M = (F_q)^{r+1}$. Правило зашифрования строки $s = (s_1, \ldots, s_r)$ на ключе $k = (a, b)$ определим формулой

$$E_k(s) = \left(u_1, \ldots, u_r, a + u_1 \cdot b^1 + \ldots + u_r \cdot b^r\right),$$

где

$$u_i = s_i + c_i \cdot a + d_i \cdot b, \;\; i = 1, \ldots, r,$$

а $c_1, \ldots, c_r, d_1, \ldots, d_r$ — произвольные ненулевые константы из F_q, такие, что

$$c_i \cdot d_j \neq c_j \cdot d_i \tag{6}$$

при $i \neq j$.

Утверждение 1. Шифр Σ_1 с равномерными распределениями $\mathsf{P}(S)$, $\mathsf{P}(K)$ является ε-совершенным шифром для $\varepsilon < q^{-1}$.

Доказательство. Заметим, что для любого $m = (u_1, \ldots, u_r, w) \in M$ выполняется равенство $|K(m)| = q$. В самом деле, пусть $E_{(a,b)}(s_1, \ldots, s_r) = (u_1, \ldots, u_r, w)$. Тогда $s_i = u_i + c_i \cdot a + d_i \cdot b$, $i = 1, \ldots, r$, и $w = a + u_1 \cdot b + \ldots + u_r \cdot b^r$. Нужное утверждение следует из того, что для любого $b \in F_q$ однозначно определяется параметр a из последнего равенства.

Покажем теперь, что для любых $s \in S$ и $m \in M$ справедливо неравенство $|K(s, m)| \leqslant 1$. В самом деле, пусть для двух различных пар (a, b) и (a', b') выполняются равенства $u_i = s_i + c_i \cdot a + d_i \cdot b = s_i + c_i \cdot a' + d_i \cdot b'$, $i = 1, \ldots, r$. Из этих равенств получаем, в частности, следствия для любых различных $i, j = 1, \ldots, r$:

$$c_i \cdot (a + a') = d_i \cdot (b + b'),$$
$$c_j \cdot (a + a') = d_j \cdot (b + b').$$

Константы c_i, d_i ненулевые, поэтому $a + a' \neq 0$, так как в противном случае $b + b' = 0$, и тогда $(a, a') = (b, b')$, что противоречит условию. В таком случае из последних соотношений получаем равенства $c_i \cdot {d_i}^{-1} = (b + b')(a + a')^{-1} = c_j \cdot {d_j}^{-1}$, или $c_i \cdot d_j = c_j \cdot d_i$, что противоречит условию (6). Полученное противоречие доказывает требуемое свойство.

Теперь, используя (5), получаем неравенства $\Delta(s, m) \leqslant q^{-1} - q^{-r} < q^{-1}$, откуда $\Delta(\Sigma_1) = \max\limits_{(s,m)} \Delta(s, m) < q^{-1}$, что и требуется. ■

Рассмотрим вопрос об использовании шифра Σ_1 для обеспечения аутентификации данных. Формально речь идёт об оценке имитостойкости шифра Σ_1, то есть его стойкости к атакам типа имитации и подмены в случае, когда каждый ключ используется для передачи не более одного сообщения. Этот вопрос подробно рассмотрен в [2], где мерой стойкости служит вероятность успеха атаки. Тот же вопрос можно рассматривать и с других позиций. Шифр Σ_1 представляет собой код аутентификации с секретностью [4]. В случае, когда распределения $\mathsf{P}(S)$, $\mathsf{P}(K)$ равномерны, стойкость кода аутентификации к активным атакам определяется вероятностями p_0 и p_1, где (см., например, [5, 6])

$$p_0 = \max_{m \in M} \frac{|K(m)|}{|K|}; \tag{7}$$

$$p_1 = \max_{m \in M} \max_{n \in M \setminus \{m\}} \frac{|K(m, n)|}{|K(m)|}, \tag{8}$$

$$|K(m, n)| = |K(m)| \cap |K(n)|.$$

Как код аутентификации Σ_1 работает следующим образом. Получатель сообщения $m = (u_1, \ldots, u_r, w)$, владеющий секретным ключом $k = (a, b)$, восстанавливает передаваемое состояние источника $s = (s_1, \ldots, s_r)$, пользуясь соотношениями

$$s_i = u_i + c_i \cdot a + d_i \cdot b, \;\; i = 1, \ldots, r.$$

Критерием аутентичности сообщения служит равенство $w = a + u_1 \cdot b + \ldots + u_r \cdot b^r$.

Утверждение 2. Для кода аутентификации Σ_1 с равномерными распределениями $\mathsf{P}(S)$, $\mathsf{P}(K)$ выполняются соотношения

$$p_0 = q^{-1}, \;\; p_1 < r \cdot q^{-1}. \tag{9}$$

Доказательство. Как отмечалось в доказательстве утверждения 1, для любого $m \in M$ имеет место равенство $|K(m)| = q$. Пусть $(a, b) \in K(m, n)$, где $m = (u_1, \ldots, u_{r+1})$, $n = (v_1, \ldots, v_{r+1})$. Тогда a и b находятся из системы уравнений

$$\begin{cases} a + u_1 \cdot b + \ldots + u_r \cdot b^r = u_{r+1}, \\ a + v_1 \cdot b + \ldots + v_r \cdot b^r = v_{r+1}. \end{cases} \tag{10}$$

Поскольку уравнение $(u_1+v_1)\cdot b+\ldots+(u_r+v_r)\cdot b^r = u_{r+1}+v_{r+1}$ имеет в поле F_q не более r решений, системе (10) может удовлетворять не более r значений b. Для каждого из них из первого уравнения системы однозначно находится значение a. Это доказывает неравенство $|K(m)| \leqslant r$ для любых $m, n \in M$. Соотношения (9) следуют теперь из формул (7), (8). ■

Проиллюстрируем уровень стойкости шифра Σ_1 числовым примером. Пусть $q = 2^{64}$, $r = 2^{16}$. Тогда Σ_1 при использовании 128-битного ключа обеспечивает (2^{-64})-совершенное шифрование сообщений длины, не превосходящей $2^{16} \cdot 64 = 4194304$ бит, и их аутентификацию с уровнем стойкости, определяемым параметрами $p_0 = 2^{-64}$, $p_1 < 2^{-48}$.

Пример 2. Пусть $q = 2^r$, $Q = 2^{r+t}$, r, t — натуральные числа, такие, что $2t \geqslant r$. Рассмотрим шифр Σ_2, для которого $S = (F_Q)^{2^t+1}$, $K = F_Q \times F_Q \times F_q$, $M = (F_Q)^{2^t+2}$. Правило зашифрования строки $s = (s_{2^t}, \ldots s_1, s_0)$ на ключе $k = (a, b, c)$ определим формулой

$$E_k(s) = \left(u_{2^t}, \ldots, u_0, c + \left[b \cdot \left(u_{2^t} \cdot a^{2^t} + \ldots + u_1 \cdot a + u_0 \right) \right]_q \right), \tag{11}$$

где $u_i = s_i + h_i \cdot a + g_i \cdot b$, $i = 0, 1, \ldots, 2^t$, а $h_0, \ldots, h_{2^t}, g_0, \ldots, g_{2^t}$ — произвольные константы из F_Q, такие, что $h_i \cdot g_j \neq h_j \cdot g_i$ при $i \neq j$. Запись $[\alpha]_q$ означает приведение элемента α по модулю q, то есть вычёркивание t старших координат двоичного представления α.

Утверждение 3. Шифр Σ_2 с равномерными распределениями $\mathsf{P}(S)$, $\mathsf{P}(K)$ является ε-совершенным шифром для

$$\varepsilon = \left| \frac{1}{2^{r+2t}} - \frac{1}{2^{(r+1)\cdot(2^t+1)}} \right|.$$

Доказательство. Для любого $m = (u_{2^t}, \ldots, u_0, w) \in M$ выполняется равенство

$$|K(m)| = 2^{r+2t}. \tag{12}$$

В самом деле, пусть $E_{(a,b,c)}(s_{2^t}, \ldots, s_0) = (u_{2^t}, \ldots, u_0, w)$. Тогда $s_i = u_i + h_i \cdot a + g_i \cdot b$, $i = 0, 1, \ldots, 2^t$, и $w = c + \left[b \cdot \left(u_{2^t} \cdot a^{2^t} + \ldots + u_1 \cdot a + u_0 \right) \right]_q$. Для любых $a, b \in F_Q$ из последнего равенства однозначно определяется параметр $c \in F_q$. Равенство (12) следует теперь из того, что для любого $\gamma \in F_q$ число пар $(\alpha, \beta) \in F_Q \times F_Q$, таких, что $[\alpha, \beta]_q = \gamma$, равно Q^2/q.

Точно так же, как и в утверждении 1, доказывается, что для любых $s \in S$ и $m \in M$

$$|K(s, m)| \leqslant 1. \tag{13}$$

Теперь из (5), (12) и (13) получаем равенства

$$\Delta\left(\Sigma_2\right) = \max_{(s,m)} \Delta(s,m) = \max\left\{\frac{1}{2^{(r+1)\cdot(2^t+1)}}, \left|\frac{1}{2^{r+2t}} - \frac{1}{2^{(r+1)\cdot(2^t+1)}}\right|\right\} = \left|\frac{1}{2^{r+2t}} - \frac{1}{2^{(r+1)\cdot(2^t+1)}}\right|,$$

откуда следует (11). ■

Как и Σ_1, шифр Σ_2 можно рассматривать как код аутентификации с секретностью.

Утверждение 4. Для кода аутентификации Σ_2 с равномерными распределениями $\mathsf{P}(S)$, $\mathsf{P}(K)$ выполняются равенства

$$p_0 = 2^{-r}, \;\; p_1 = 2^{-(r-1)} - 2^{-2r}. \tag{14}$$

Доказательство. Вероятности p_0, p_1 можно вычислить непосредственно, как и в утверждении 2. Вместо этого воспользуемся известным утверждением. В [3] изучается код аутентификации Σ с теми же, что и у Σ_2, множествами S, K, M. Отличие состоит лишь в том, что правило кодирования кода Σ задаётся формулой

$$\overline{E}_{(a,b,c)}(s) = \left(s, c + \left[s(a)\cdot b\right]_q\right), \tag{15}$$

где $s = (s_{2^t}, \ldots, s_0)$ определяет коэффициенты многочлена $s(x) = s_{2^t}\cdot x^{2^t} + \ldots + s_0$. В [3] доказано, что для кода Σ вероятности успеха имитации и подмены определяются формулами (14). Покажем, что вероятности p_0, p_1 одинаковы для Σ и Σ_2. Для этого достаточно заметить, что одинаковы матрицы инцидентности кодов.

Напомним, что матрица инцидентности кода аутентификации — это матрица $(i(k,m))$ размера $|K|\times|M|$, состоящая из элементов

$$i(k,m) = \begin{cases} 1, & \text{если } E_k(s) = m \text{ для некоторого } s\in S,\\ 0 & \text{в противном случае.}\end{cases}$$

Заметим, что правила кодирования (11) и (15) связаны соотношением

$$E_k(s) = \overline{E}_k\left(\varphi_k(s)\right), \tag{16}$$

где $\varphi_k : S\to S$ — биекция для каждого $k\in K$. Очевидно, что матрицы инцидентности кодов, связанных соотношением (16), одинаковы. Это позволяет сделать вывод о том, что для любых сообщений $m, n \in M$ величины $|K(m)|$ и $|K(m,n)|$, определяющие вероятности p_0, p_1 по формулам (7), (8), одинаковы для Σ и Σ_2 при условии, что распределения $\mathsf{P}(S)$, $\mathsf{P}(K)$ равномерны. ■

Проиллюстрируем уровень стойкости шифра Σ_2 примером. Пусть $t = 32, r = 64$. Тогда Σ_2 при использовании 256-битного ключа обеспечивает (2^{-128})-совершенное шифрование сообщений длины, не превосходящей $(64+32)\cdot(2^{32}+1) = 412316860512$ бит, и их аутентификацию с уровнем стойкости, определяемым параметрами $p_0 = 2^{-64}$ и $p_1 < 2^{-63}$.

Шифры Σ_1 и Σ_2 допускают эффективную реализацию, поскольку операции сложения и умножения в полях характеристики 2 реализуются несложно. Выбор констант c_i, d_i (так же как и констант g_i, h_i), удовлетворяющих соотношениям (6), не представляет труда. Например, в качестве c_i можно выбрать элемент, двоичная запись которого представляет число 2^i, а в качестве d_i — элемент, двоичная запись которого представляет число $2^i + 1$.

Интересен вопрос об оценке стойкости рассмотренных шифров в случае, когда распределение $\mathsf{P}(S)$ неравномерно.

ЛИТЕРАТУРА

1. *Алфёров А. П., Зубов А. Ю., Кузьмин А. С., Черёмушкин 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. *Kabatianskii G. A., Johansson T., and Smeets B.* On the cardinality of systematic A-codes via error correcting codes // IEEE Trans. Inform. Theory. 1996. V. IT-42. No. 2. P. 566–578.
4. *Зубов А. Ю.* Математика кодов аутентификации. М.: Гелиос АРВ, 2007. 480 с.
5. *Зубов А. Ю.* Оценка стойкости кода аутентификации с двумя состояниями источника при случайном и равновероятном выборе ключей // Безопасность информационных технологий. 2008. № 2. С. 92–96.
6. *Зубов А. Ю.* О выборе оптимальной стратегии защиты для кода аутентификации с двумя состояниями источника // Дискретная математика. 2009. Т. 21. № 4. С. 136–147.