УДК 519.7

О ПОНЯТИИ ε-СОВЕРШЕННОГО ШИФРА

А. Ю. Зубов

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

Обсуждаются обобщения понятия совершенного шифра. Шифр называется ε-совершенным, если максимальное значение модуля разности апостериорной и априорной вероятностей открытого текста не превосходит ε. Изучаются две конструкции шифров, которые являются ε-совершенными для любого множества открытых текстов, частотные характеристики которых удовлетворяют незначительному ограничению. Понятие ε-совершенного шифра является одним из возможных приближений к понятию совершенного шифра. Приводятся результаты сравнения изучаемых конструкций шифров по степени близости различных таких приближений, свидетельствующие в пользу понятия ε-совершенности и её аналогов.

Ключевые слова: *совершенный шифр, ε-совершенный шифр.*

DOI 10.17223/20710410/33/3

ON THE CONCEPT OF A ε-PERFECT CIPHER

A. Yu. Zubov

Lomonosov Moscow State University, Moscow, Russia

E-mail: Zubovanatoly@yandex.ru

The generalizations of the perfect cipher concept are discussed. A cipher is called ε-perfect if the maximum absolute value of the difference between the posterior and prior probabilities of a plaintext does not exceed ε. Two constructions of ε-perfect ciphers for a multitude of plaintexts with a minor limitation of their frequency characteristics are studied. The notion of ε-perfect cipher is one of the possible approximations to the notion of a perfect cipher. For studied constructions of ciphers, it is shown that, in comparison with the other such approximations, ε-perfectness and its analogues have much better proximity to perfectness.

Keywords: *perfect cipher, ε-perfect cipher.*

Введение

В [1] введено понятие ε-совершенного шифра (который является совершенным шифром при $\varepsilon = 0$) и построены примеры таких шифров. Интерес к ним вызван следующими причинами. Основным недостатком совершенного шифра является чрезмерно большое число ключей, что делает такой шифр непрактичным. Замена жёсткого условия $\varepsilon = 0$ условием $\varepsilon > 0$ для достаточно малого ε незначительно понижает стойкость шифра (оставляя его в классе теоретически стойких шифров), но допускает возможность использования небольшого числа ключей, что делает шифр более практичным.

Вместе с тем свойство совершенности шифра не зависит от распределения вероятностей на множестве открытых текстов [2], тогда как примеры ε-совершенных шифров

из [1] построены лишь при условии, что открытые тексты выбираются случайно и равновероятно. Это ограничивает область применения таких шифров и делает их, в свою очередь, менее практичными, чем совершенные шифры. В данной работе показано, что на самом деле предложенные в [1] шифры остаются ε-совершенными и для любого распределения на множестве открытых текстов, удовлетворяющего некоторому ограничению. При этом параметр ε может принимать достаточно малые значения.

Помимо предложенного в [1] определения ε-совершенности известны и другие подобные определения. Так, в [3] введены шифры, «близкие» к совершенным, с позиции статистического расстояния между вероятностными распределениями. Интересен вопрос о сопоставлении мер «близости» к совершенным шифрам, а также их адекватности. Такой анализ проводится в данной работе на основе предложенной в [1] конструкции шифра.

1. Определения и конструкции

Пусть $\mathcal{S}, \mathcal{K}, \mathcal{M}$ — множества открытых текстов, ключей и шифрованных текстов шифра Σ и $\{E_k : k \in \mathcal{K}\}$ — множество функций зашифрования, представляющих собой инъективные отображения $\mathcal{S} \to \mathcal{M}$. Пусть S, K, M — случайные величины, принимающие значения из $\mathcal{S}, \mathcal{K}, \mathcal{M}$ в соответствии с распределениями вероятностей $\mathcal{P}_S = (p_S(s), s \in \mathcal{S})$, $\mathcal{P}_K = (p_K(k), k \in \mathcal{K})$, $\mathcal{P}_M = (p_M(m), m \in \mathcal{M})$, где

$$p_M(m) = \sum_{k \in \mathcal{K}(m)} p_K(k)\, p_S\left(E_k^{-1}(m)\right), \tag{1}$$

и $\mathcal{K}(m) = \{k \in \mathcal{K} : \exists s \in \mathcal{S}\,(E_k(s) = m)\}$. При этом случайные величины S, K полагаются независимыми.

Пусть $\mathcal{P}_{S,M}$, $\mathcal{P}_{S|M}$, $\mathcal{P}_{M|S}$ — совместное и условные распределения, для которых вероятность $p_{M|S}(m|s)$ вычисляется по формуле

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

где $\mathcal{K}(s,m) = \{k \in \mathcal{K} : E_k(s) = m\}$, а вероятность $p_{S|M}(s|m)$ — по формуле

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

Шифр Σ называется *совершенным*, если для любых $s \in \mathcal{S}$, $m \in \mathcal{M}$ выполняется равенство

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

Ослабим условие (4) и введём понятие ε-совершенного шифра.

Используя обозначения

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

запишем (4) в виде равенства

$$\max_{s,m} \Delta(s,m) = 0.$$

Заметим, что, согласно (3), величины $\Delta(s,m)$ и $\nabla(s,m)$ связаны соотношением

$$\begin{aligned} \Delta(s,m) &= \left|\frac{p_{M|S}(m|s)\, p_S(s)}{p_M(m)} - p_S(s)\right| = \\ &= \frac{p_S(s)}{p_M(m)}\left|p_{M|S}(m|s) - p_M(m)\right| = \frac{p_S(s)}{p_M(m)}\nabla(s,m). \end{aligned} \tag{5}$$

В [1] шифр Σ назван ε-совершенным, если для любых $s \in \mathcal{S}$, $m \in \mathcal{M}$

$$\max_{s,m} \Delta(s,m) \leqslant \varepsilon. \tag{6}$$

Там же предложены конструкции ε-совершенных шифров Σ_1 и Σ_2 с равномерными распределениями $\mathcal{P}_S$, $\mathcal{P}_K$. Для шифра Σ_1

$$\mathcal{S} = (F_q)^r\,,\ \mathcal{K} = (F_q)^2\,,\ \mathcal{M} = (F_q)^{r+1}\,,$$

где F_q — поле характеристики 2, состоящее из q элементов (этот случай удобен для эффективной реализации), и r — натуральное число. Функция зашифрования строки $s = (s_1, \ldots, s_r)$ на ключе $k = (a, b)$ определяется формулой

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

где

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

а $c_1, \ldots, c_r, d_1, \ldots, d_r$ — произвольные ненулевые константы из F_q, такие, что $c_i \cdot d_j \neq \neq c_j \cdot d_i$ при $i \neq j$. В [1] показано, что шифр Σ_1 является ε-совершенным для $\varepsilon < q^{-1}$.

Для шифра Σ_2

$$\mathcal{S} = (F_Q)^{2^t+1}\,,\ \mathcal{K} = (F_Q)^2 \times F_q,\ \mathcal{M} = (F_Q)^{2^t+2}\,,$$

где $q = 2^r$; $Q = 2^{r+t}$; r, t — натуральные числа, такие, что $2t \geqslant r$. Функция зашифрования строки $s = (s_{2^t}, \ldots, s_1, s_0)$ на ключе $k = (a, b, c)$ определяется формулой

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

где

$$u_i = s_i + h_i \cdot a + g_i \cdot b, \quad i = 0, 1, \ldots, 2^t,$$

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 $j \neq i$. Запись $[\alpha]_q$ означает приведение элемента $\alpha \in F_Q$ по модулю q. В [1] показано, что шифр Σ_2 является ε-совершенным для $\varepsilon = 2^{-(r+2t)} - 2^{-(r+1)\left(2^t+1\right)}$.

В следующем утверждении обобщаются результаты работы [1].

Теорема 1. Пусть для шифров Σ_1 и Σ_2 распределение $\mathcal{P}_K$ — равномерное, а $\mathcal{P}_S$ — любое такое распределение, что для некоторых действительных чисел α, β, δ, удовлетворяющих неравенствам $0 < \alpha,\ \beta < 1 \leqslant \delta$, выполняются условия

$$\alpha \leqslant p_S(s) \leqslant \beta, \quad \beta/\alpha \leqslant \delta \tag{7}$$

для каждого $s \in \mathcal{S}$. Тогда шифр Σ_1 является ε-совершенным для $\varepsilon < \delta q^{-1}$, а шифр Σ_2 — ε-совершенным для $\varepsilon < \delta \cdot 2^{-(r+2t)}$.

Доказательство. Согласно (1) и (2), для равномерного распределения $\mathcal{P}_K$ имеем

$$\nabla(s,m) = \left| \sum_{k \in \mathcal{K}(s,m)} p_K(k) - \sum_{k \in \mathcal{K}(m)} p_K(k)\, p_S\left(E_k^{-1}(m)\right) \right| = \frac{1}{|\mathcal{K}|} \left| |\mathcal{K}(s,m)| - \sum_{k \in \mathcal{K}(m)} p_S\left(E_k^{-1}(m)\right) \right|.$$

В [1] показано, что для шифра Σ_1 при любых $s \in \mathcal{S}$, $m \in \mathcal{M}$

$$|\mathcal{K}(m)| = q, \quad |\mathcal{K}(s,m)| \leqslant 1.$$

В частности, при $k \neq k'$ невозможно равенство $E_k^{-1}(m) = E_{k'}^{-1}(m)$. Поэтому сумма $\sigma = \sum\limits_{k \in \mathcal{K}(m)} p_S\left(E_k^{-1}(m)\right)$ заключена в пределах $0 < \sigma < 1$, откуда получаем неравенство

$$\nabla(s,m) \leqslant \frac{1}{|\mathcal{K}|} \max\{\sigma, |1-\sigma|\} < \frac{1}{|\mathcal{K}|}. \tag{8}$$

Теперь из (1), (5), (7), (8) следует искомое неравенство для шифра Σ_1:

$$\Delta(s,m) < \frac{p_S(s)}{p_M(m)\,|\mathcal{K}|} \leqslant \frac{\beta\,|\mathcal{K}|}{q\alpha\,|\mathcal{K}|} = \frac{\beta}{\alpha q} \leqslant \delta q^{-1}.$$

В [1] показано также, что для шифра Σ_2 при любых $s \in \mathcal{S}$, $m \in \mathcal{M}$

$$|\mathcal{K}(m)| = 2^{r+2t}, \quad |\mathcal{K}(s,m)| \leqslant 1. \tag{9}$$

Поэтому справедлива оценка (8) и, с учётом (9), отсюда следует искомое неравенство для шифра Σ_2: $\Delta(s,m) < \delta \cdot 2^{-(r+2t)}$. ■

Замечание 1. Условие (7) вводит ограничения, при которых шифры Σ_1 и Σ_2 являются ε-совершенными. Основное ограничение связано с величиной δ. Что можно о ней сказать? При достаточно больших q, например $q = 2^{128}$, частотные характеристики открытых текстов для шифра Σ_1 «распределяются» среди строк длины $128r$ битов. Возможна ли при этом ситуация, когда некоторые тексты встречаются, например, в $\delta = 2^{64}$ раз чаще, чем другие? Если это и возможно, то лишь для текстов с «экзотической» частотной характеристикой. Но даже и в этом случае из теоремы 1 мы получаем для шифра Σ_1 оценку $\varepsilon < 2^{64}$. Для шифра Σ_2 и значительно большие значения δ дают малые значения ε. Это даёт основание полагать, что ограничения (7) не являются слишком «стеснительными» в реальных условиях.

Замечание 2. Конструкция шифра Σ_1 использует константы c_i, d_i, удовлетворяющие соотношениям $c_i \cdot d_j \neq c_j \cdot d_i$ при $i \neq j$. Можно предложить следующий способ выбора таких констант в случае, когда $q = 2^n$, $r < n$. Элемент α поля F_{2^n} представляется многочленом $\alpha_{n-1}x^{n-1} + \ldots + \alpha_1 x^1 + \alpha_0$ с коэффициентами из F_2. Пусть константа c_i представлена многочленом $f_i(x) = c_{n-1}^{(i)}x^{n-1} + \ldots + c_1^{(i)}x$, а d_i — многочленом $g_i(x) = c_{n-1}^{(i)}x^{n-1} + \ldots + c_1^{(i)}x + 1$. Пусть $c_i \neq c_j$, тогда и $f_i(x) \neq f_j(x)$. Произведение $c_i \cdot d_j$ представляется многочленом $f_i(x)g_j(x) = f_i(x)\,(f_j(x)+1)$, а произведение $c_j \cdot d_i$ — многочленом $f_j(x)g_i(x) = f_j(x)\,(f_i(x)+1)$. Отсюда следует, что для выбранных вариантов констант $c_i \cdot d_j \neq c_j \cdot d_i$. Выбирая произвольно различные двоичные векторы $\left(c_{n-1}^{(i)}, \ldots, c_1^{(i)}\right)$, получаем искомый набор констант.

Замечание 3. В [1] шифры Σ_1 и Σ_2 рассматривались как коды аутентификации с секретностью. Нетрудно заметить, что в условиях теоремы 1 имеют место следующие оценки вероятностей p_0, p_1 успеха имитации и подмены для шифра Σ_1:

$$p_0 = q^{-1}, \quad p_1 < r\delta q^{-1}.$$

Например, при $q = 2^{128}$, $r = 2^{32}$, $\delta = 2^{32}$ имеем оценки

$$p_0 = 2^{-128}, \quad p_1 < 2^{-64}.$$

2. Другие определения «почти совершенного» шифра

Хорошо известно (см., например, [2]), что критерием совершенности шифра Σ является любое из равенств

$$p_{M|S}(m|s) = p_M(m),$$
$$p_{M|S}(m|s) = p_{M|S}(m|s'),$$
$$p_{S,M}(s,m) = p_S(s)\, p_M(m),$$

которые должны выполняться для любых $s, s' \in \mathcal{S}$, $m \in \mathcal{M}$. В связи с этим мы могли бы определить ε-совершенный шифр одним из соответствующих неравенств

$$\max_{s,m} \left| p_{M|S}(m|s) - p_M(m) \right| \leqslant \varepsilon; \tag{10}$$

$$\max_{s,s',m} \left| p_{M|S}(m|s) - p_{M|S}(m|s') \right| \leqslant \varepsilon; \tag{11}$$

$$\max_{s,m} \left| p_{S,M}(s,m) - p_S(s)\, p_M(m) \right| \leqslant \varepsilon. \tag{12}$$

Оценим правые части неравенств (10)–(12) для шифра Σ_1. Из (2) и (8) следует, что для определений (10) и (11) шифр Σ_1 является ε-совершенным для $\varepsilon = 1/|\mathcal{K}| = q^{-2}$, причём для любого распределения $\mathcal{P}_S$. Такой же вывод справедлив и для определения (12). В самом деле,

$$\max_{s,m} \left| p_{S,M}(s,m) - p_S(s)\, p_M(m) \right| = \max_{s,m} \left| p_S(s)\, p_{M|S}(m|s) - p_S(s)\, p_M(m) \right| =$$
$$= \max_{s,m} p_S(s) \left| p_{M|S}(m|s) - p_M(m) \right| = \max_{s,m} p_S(s) \cdot \nabla(s,m) < \max_{s,m} \nabla(s,m) < 1/|\mathcal{K}|\,.$$

Полученные оценки свидетельствуют о том, что определения (6) и (10)–(12) не эквивалентны.

Введённые определения не являются единственно возможными определениями «почти совершенного» шифра. В [3] предлагаются другие определения с позиции статистической неразличимости, а также соотношения между ними. Кратко изложим содержание этой работы и оценим стойкость шифра Σ_1 с этих позиций.

Для распределений вероятностей $\mathcal{P}_U$, $\mathcal{P}_V$ на конечном множестве $\mathcal{A}$ *статистическим расстоянием* (или *расстоянием по вариации*) называется величина

$$d\left(\mathcal{P}_U, \mathcal{P}_V\right) = 0{,}5 \sum_{a \in \mathcal{A}} \left| p_U(a) - p_V(a) \right|.$$

Известно, что эта величина представляется также в виде

$$d\left(\mathcal{P}_U, \mathcal{P}_V\right) = \max_{f:\mathcal{A}\to\{0,1\}} \left| \mathsf{P}\left[f(U) = 1\right] - \mathsf{P}\left[f(V) = 1\right] \right|,$$

где U и V в правой части равенства рассматриваются как случайные величины на множестве $\mathcal{A}$, имеющие распределения $\mathcal{P}_U, \mathcal{P}_V$, а максимум берётся по всем возможным отображениям $f : \mathcal{A} \to \{0,1\}$.

Пусть для шифра Σ распределение $\mathcal{P}_{\mathcal{S}}$ может выбираться из некоторого семейства распределений $\mathcal{P}\left[\mathcal{S}\right]$. Шифр Σ называется

— $\varepsilon(S|M)$-*стойким*, если для любого $m \in \mathcal{M}$ справедливо неравенство

$$d\left(\mathcal{P}_{S|M}\left(\cdot|m\right), \mathcal{P}_S\left(\cdot\right)\right) \leqslant \varepsilon;$$

— $\varepsilon(M|S)$-*стойким*, если для любого $s \in \mathcal{S}$ справедливо неравенство

$$d\left(\mathcal{P}_{M|S}\left(\cdot|s\right), \mathcal{P}_M\left(\cdot\right)\right) \leqslant \varepsilon;$$

— $\varepsilon(M|S^2)$-*стойким*, если для любых $s, s' \in \mathcal{S}$ справедливо неравенство

$$d\left(\mathcal{P}_{M|S}\left(\cdot|s\right), \mathcal{P}_{M|S}\left(\cdot|s'\right)\right) \leqslant \varepsilon;$$

— $\varepsilon(S, M)$-*стойким*, если

$$d\left(\mathcal{P}_{S,M}\left(\cdot,\cdot\right), \mathcal{P}_S\left(\cdot\right) \cdot \mathcal{P}_M\left(\cdot\right)\right) \leqslant \varepsilon.$$

Эти определения являются аналогами определений (5), (10)–(12) соответственно. Очевидно, что при $\varepsilon = 0$ введённые шифры являются совершенными.

В [3] приведены ещё два определения: $\varepsilon(M|S^2)$-стойкий шифр назван также $IND(\varepsilon)$-*стойким* (или *статистически* ε-*неразличимым*). Шифр Σ назван *статистически* ε-*семантически стойким* (кратко — $SS(\varepsilon)$-*стойким*), если для любого $\mathcal{P}_S \in \mathcal{P}[\mathcal{S}]$ и любого отображения $f : \mathcal{M} \to \{0,1\}$ существует случайная переменная G_f на $\{0,1\}$, зависящая от f, но не зависящая от M, такая, что для каждого отображения $h : \mathcal{M} \to \{0,1\}$ выполняется условие

$$\left|\mathsf{P}\left[f(M) = h(M)\right] - \mathsf{P}\left[G_f = h(M)\right]\right| \leqslant \varepsilon. \tag{13}$$

Качественно это определение означает, что шифртекст «почти бесполезен» для получения любого одного бита информации об открытом тексте M, поскольку из (13) следует, что при угадывании бита $h(M)$ «почти нет разницы» в том, что использовать — M и f или f и случайный бит G_f.

Результаты работы [3] сформулируем в виде следующего утверждения.

Теорема 2.

Шифр Σ является $\varepsilon(M|S)$-стойким тогда и только тогда, когда он является $IND(\varepsilon)$-стойким.

Шифр Σ является $\varepsilon(S, M)$-стойким, если он является $IND(\varepsilon)$-стойким. Обратно, шифр Σ является $IND(2\varepsilon)$-стойким, если он является $\varepsilon(S, M)$-стойким.

Шифр Σ является $SS(\varepsilon)$-стойким, если он является $IND(\varepsilon)$-стойким. Обратно, если шифр Σ является $SS(\varepsilon)$-стойким, то он является $IND(4\varepsilon)$-стойким.

Из теоремы 2 следует, что $\varepsilon(M|S)$, $\varepsilon(S, M)$, $IND(\varepsilon)$ и $SS(\varepsilon)$ — равносильные понятия стойкости. В то же время $\varepsilon(S|M)$ — более сильное понятие. В этом можно убедиться на примере шифра Σ, приведённого в [3], который для сколь угодно малого ε является $IND(\varepsilon)$-стойким, но при этом $\varepsilon'(S|M)$-стойким лишь для $\varepsilon' > 0{,}5$.

В свою очередь, введённые в [3] понятия стойкости сильнее их аналогов из [1]. Например, $\varepsilon(S|M)$-стойкий шифр является 2ε-совершенным в смысле определения (6), поскольку

$$\max_{a \in \mathcal{A}} |p_U(a) - p_V(a)| \leqslant \sum_{a \in \mathcal{A}} |p_U(a) - p_V(a)| \leqslant 2\varepsilon.$$

Для более точного сравнения подходов оценим стойкость шифра Σ_1 с позиции введённых понятий стойкости в случае, когда $\mathcal{P}_S$, $\mathcal{P}_K$ — равномерные распределения.

Используем определение $\varepsilon(M|S)$-стойкости. Вычислим расстояние

$$\sigma = d\left(\mathcal{P}_{M|S}\left(\cdot|s\right), \mathcal{P}_M\left(\cdot\right)\right) = 0{,}5 \sum_{m \in \mathcal{M}} \nabla(s, m). \tag{14}$$

Как показано в п. 1,

$$\nabla(s,m)=\frac{1}{|\mathcal{K}|}\left||\mathcal{K}(s,m)|-\frac{|\mathcal{K}(m)|}{|\mathcal{S}|}\right|. \tag{15}$$

Для каждого $s\in\mathcal{S}$ имеется q^2 элементов $m\in\mathcal{M}$, для которых $|\mathcal{K}(s,m)|=1$. Для остальных элементов m выполняется равенство $|\mathcal{K}(s,m)|=0$. Отсюда и из (14), (15) получаем

$$\sigma=0{,}5\frac{1}{q^2}\left[q^2\left(1-\frac{1}{q^{r-1}}\right)+\left(q^{r+1}-q^2\right)\frac{1}{q^{r-1}}\right]=\frac{q^{r-1}-1}{q^{r-1}}.$$

Таким образом, шифр Σ_1 является лишь $\dfrac{q^{r-1}-1}{q^{r-1}}$ $(M|S)$-стойким. Полученное значение ε неулучшаемо, поскольку мы точно вычислили $d\left(\mathcal{P}_{M|S}\left(\cdot|s\right),\mathcal{P}_M\left(\cdot\right)\right)$.

Используем определение $\varepsilon(S|M)$-стойкости. Вычислим расстояние

$$\sigma=d\left(\mathcal{P}_{S|M}\left(\cdot|m\right),\mathcal{P}_S\left(\cdot\right)\right)=0{,}5\sum_{s\in\mathcal{S}}\Delta(s,m). \tag{16}$$

Как показано в п. 1,

$$\sigma=0{,}5\sum_{s\in\mathcal{S}}\frac{p_S(s)}{p_M(m)}\left|p_{M|S}(m|s)-p_M(m)\right|=0{,}5\frac{1}{q}\sum_{s\in\mathcal{S}}\left||\mathcal{K}(s,m)|-\frac{1}{q^{r+1}}\right|. \tag{17}$$

Для каждого $m\in\mathcal{M}$ имеется q элементов $s\in\mathcal{S}$, для которых $|\mathcal{K}(s,m)|=1$. Для остальных элементов s выполняется равенство $|\mathcal{K}(s,m)|=0$. Отсюда и из (16), (17) получаем

$$\sigma=\frac{0{,}5}{q}\left[q\left(1-\frac{1}{q^{r-1}}\right)+\left(q^r-q\right)\frac{1}{q^{r-1}}\right]=\frac{q^{r-1}-1}{q^{r-1}}.$$

Таким образом, определения $\varepsilon(M|S)$- и $\varepsilon(S|M)$-стойкости дают для шифра Σ_1 одинаковые значения $\varepsilon=1-1/q^{r-1}$. Нетрудно проверить, что для $\varepsilon(S,M)$-стойкости значение ε точно такое же.

Используем определение $\varepsilon(M|S^2)$. Вычисляем расстояние

$$\sigma=d\left(\mathcal{P}_{M|S}\left(\cdot|s\right),\mathcal{P}_{M|S}\left(\cdot|s'\right)\right),$$

в результате имеем

$$\sigma=0{,}5q^{-2}\sum_{m\in\mathcal{M}}\left||\mathcal{K}(s,m)|-|\mathcal{K}(s',m)|\right|.$$

Пусть $s=(s_1,s_2,s_3,\ldots,s_r)$, $s'=(s_1,s_2,s'_3,\ldots,s'_r)$, тогда если $m=E_k(s)$, а $m'=E_{k'}(s')$ для некоторых ключей k,k', то равенство $m=m'$ невозможно. Поэтому множества из q^2 элементов m и m', таких, что $|\mathcal{K}(s,m)|=1$ и $|\mathcal{K}(s',m')|=1$, не пересекаются. Отсюда

$$\sigma=0{,}5q^{-2}\left[q^2+q^2\right]=1.$$

Таким образом, пользуясь определением $\varepsilon(M|S^2)$-стойкости, получаем $\varepsilon=1$. Следовательно, с позиции подхода к оценке стойкости, предложенного в [3], ни о какой «близости» шифра к совершенному шифру речи идти не может. Это и не удивительно, поскольку сумма вида $\sum\limits_{s\in\mathcal{S}}\Delta(s,m)$ накапливает большое количество «малых слагаемых», давая в результате «большую величину». В то же время определения (6) или

(10)–(12), на наш взгляд, более адекватны, поскольку отвечают классическому подходу «в худшем случае», который оценивает изучаемый параметр своим максимально возможным значением. Другой общепринятый подход — подход «в среднем» — оценивает изучаемый параметр своим средним значением, которое, очевидно, даёт не большее значение ε, чем определение (6).

Возвращаясь к исходной идее К. Шеннона о том, что шифртекст совершенного шифра не должен давать дополнительной вероятностной информации об открытом тексте (к известной априорной информации о нём), мы должны констатировать, что подход к определению «почти совершенного шифра» из [1] является более тонким, чем подход работы [3]. В самом деле, «почти совершенный» шифр должен быть таким, чтобы шифртекст «почти не давал» дополнительной информации об открытом тексте. Но если мера $\varepsilon(S|M)$-стойкости принимает для шифра Σ_1 значение, близкое к максимально возможному, то это свидетельствует о том, что шифртекст должен практически однозначно определять открытый текст. Получаем явное противоречие с тем, что для шифра Σ_1 (при равномерном распределении $\mathcal{P}_S$)

$$\max_{(s,m)} \bigl|p_{S|M}(s|m) - p_S(s)\bigr| \leqslant q^{-1}.$$

При $q = 2^{128}$, например, правая часть неравенства ($\approx 3 \cdot 10^{-39}$) практически равна 0, и нет никаких оснований полагать, что шифртекст сколь-нибудь значимо увеличивает априорную информацию об открытом тексте.

Заключение

На примере шифра, предложенного в [1], проведено сравнение различных определений «близости» шифра к совершенному шифру. На этом основании сделан вывод о том, что введённое в [1] определение ε-совершенного шифра и его аналоги соответствуют более адекватным мерам «близости» к совершенному шифру, нежели определения из [3]. Показано, что шифры из [1] остаются ε-совершенными для класса распределений на множестве открытых текстов, удовлетворяющих незначительному ограничению.

ЛИТЕРАТУРА

1. *Зубов А. Ю.* Почти совершенные шифры и коды аутентификации // Прикладная дискретная математика. 2011. № 4(14). С. 28–33.
2. *Зубов А. Ю.* Криптографические методы защиты информации. Совершенные шифры. М.: Гелиос АРВ, 2005.
3. *Iwamoto M. and Ohta K.* Security Notions for Information Theoretically Secure Encryptions. arXiv: 1106.1731 v2 [cs.CR], 4 Jan 2012. 6 p.

REFERENCES

1. *Zubov A. Yu.* Pochti sovershennye shifry i kody autentifikatsii [Almost perfect ciphers and authentication codes]. Prikladnaya Diskretnaya Matematika, 2011, no. 4(14), pp. 28–33.
2. *Zubov A. Yu.* Kriptograficheskie metody zashchity informatsii. Sovershennye shifry [Cryptographic Methods of Information Security. Perfect Ciphers]. Moscow, Gelios ARV Publ., 2005.
3. *Iwamoto M. and Ohta K.* Security Notions for Information Theoretically Secure Encryptions. arXiv: 1106.1731 v2 [cs.CR], 4 Jan 2012. 6 p.