МАТЕМАТИЧЕСКИЕ МЕТОДЫ КРИПТОГРАФИИ

УДК 519.1+519.719.2+519.712

КРИПТОСИСТЕМА ШИФРОВАНИЯ С АУТЕНТИФИКАЦИЕЙ НА ОСНОВЕ КОДА АУТЕНТИФИКАЦИИ С СЕКРЕТНОСТЬЮ

А. Ю. Зубов

ООО «Центр сертификационных исследований», г. Москва, Россия

Предлагается идея построения криптосистемы шифрования с аутентификацией, представляющей собой модификацию кода аутентификации с секретностью на основе кода Рида — Соломона. Модификация состоит в использовании неповторяющегося вектора инициализации и производного ключа для шифрования каждого сообщения. Получены оценки стойкости криптосистемы как кода аутентификации с секретностью: стойкость шифрования оценивается близостью к совершенному шифрованию, а стойкость аутентификации — вероятностями успеха имитации и подмены. Приводятся соображения по выбору параметров и оценке стойкости криптосистемы.

Ключевые слова: *код аутентификации с секретностью, криптосистема шифрования с аутентификацией.*

DOI 10.17223/20710410/43/4

AUTHENTICATION ENCRYPTION BASED ON AUTHENTICATION CODE WITH SECRECY

A. Yu. Zubov

Center for Certification Research, Moscow, Russia

E-mail: zubovanatoly@yandex.ru

The idea of authentication encryption cryptosystem is proposed. This cryptosystem is a modification of an authentication code with secrecy considered in previous papers of the author and based on Reed — Solomon error-correcting code. The essence of the modification is to use a non-repeating initialization vector and derivative key for encryption of each message. Estimations of cryptosystem security as an authentication code with secrecy at a one-time usage of the key are received: the encryption security is estimated by proximity to perfect encryption, and the authentication security — by probabilities of imitation and substitution success. Considerations for selection of parameters and estimation of cryptosystem security to chosen plaintext attacks at multiple usage of the key as well as distinction attacks are provided.

Keywords: *authentication code with secrecy, authentication encryption.*

Введение

В [1 – 4] изучались коды аутентификации на основе кодов Рида — Соломона. В данной работе предлагается идея конструкции криптосистемы шифрования с аутентификацией, представляющей собой модификацию кода аутентификации с секретностью — $\mathbb{AC}$, введённого в [2, 4].

Код аутентификации $\mathbb{AC}$ (далее A-код) строится следующим образом. Он определяется множествами

$$\mathcal{S} = (\mathbb{F}_q)^r, \quad \mathcal{K} = (\mathbb{F}_q)^2, \quad \mathcal{M} = (\mathbb{F}_q)^{r+1},$$

где $\mathbb{F}_q = \mathbb{GF}(q)$ — поле из $q = 2^n$ элементов; $r \geqslant 2$; $\mathcal{S}$ — множество состояний источника (открытых текстов); $\mathcal{K}$ — множество номеров правил кодирования (ключей); $\mathcal{M}$ — множество сообщений (шифртекстов), и правилом кодирования (функцией зашифрования) строки $s = (s_1, \dots s_r) \in \mathcal{S}$ на ключе $k = (a, b) \in \mathcal{K}$ по формуле

$$e_k(s) = (m_1, \dots, m_r, a \oplus m_1 \cdot b^r \oplus \dots \oplus m_r \cdot b^1),$$

где $\oplus, \cdot$ — операции поля $\mathbb{F}_q$; $m_i = s_i \oplus c_i \cdot a \oplus d_i \cdot b$, $i = 1, \dots, r$; $c_1, \dots, c_r$, $d_1, \dots, d_r$ — ненулевые константы из $\mathbb{F}_q$, такие, что

$$c_i \cdot d_j \neq c_j \cdot d_i \tag{1}$$

при $j \neq i$. Фактически строка $(m_1, \dots, m_r)$ является результатом зашифрования, а

$$m_{r+1} = a \oplus m_1 \cdot b^r \oplus \dots \oplus m_r \cdot b^1$$

— имитовставкой. Предполагается, что ключи и состояния источника выбираются случайно в соответствии с распределениями вероятностей $\mathcal{P}_K = (p_K(k),\ k \in \mathcal{K})$, $\mathcal{P}_S = (p_S(s), s \in \mathcal{S})$ и независимо друг от друга.

Интерес к A-коду $\mathbb{AC}$ вызван тем, что он допускает эффективную реализацию, обеспечивает ε-совершенное шифрование и высокий уровень имитозащиты при однократном использовании ключа. Понятие ε-совершенного шифрования введено в [2, 3]. Оно обобщает понятие совершенного шифрования, введённого К. Шенноном, и определяется следующим образом.

$\mathcal{P}_S$ и $\mathcal{P}_K$ индуцируют распределение вероятностей $\mathcal{P}_M = (p_M(m), m \in \mathcal{M})$ на множестве сообщений A-кода по формуле

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

где

$$\mathcal{K}(m) = \{k \in \mathcal{K} : \exists s \in \mathcal{S}\,(e_k(s) = m)\},$$

а для $k \in \mathcal{K}(m)$ по определению $e_k^{-1}(m) = s$, если $e_k(s) = m$. Пусть $\mathcal{P}_{S,M}, \mathcal{P}_{S|M}, \mathcal{P}_{M|S}$ — совместное и условные распределения вероятностей, определяемые формулами

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

$$\mathcal{K}(s, m) = \{k \in \mathcal{K} : e_k(s) = m\},$$

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

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

Тогда говорят, что А-код реализует *совершенное шифрование*, если равенство

$$p_{S|M}(s|m) = p_S(s)$$

выполняется для любых $s \in \mathcal{S}$ и $m \in \mathcal{M}$. Используя обозначение

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

это определение можно записать в виде равенства

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

В свою очередь, А-код с данными распределениями $\mathcal{P}_S$ и $\mathcal{P}_K$ реализует *ε-совершенное шифрование*, если

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

где $0 \leqslant \varepsilon < 1$.

Теорема 1 [3]. Пусть для А-кода $\mathbb{AC}$ распределение $\mathcal{P}_K$ равномерное, а $\mathcal{P}_S$ — любое такое распределение, что для действительных чисел α, β, σ, удовлетворяющих неравенствам $0 < \alpha, \beta < 1 \leqslant \sigma$, выполняются условия $\alpha \leqslant p_S(s) \leqslant \beta$, $\beta/\alpha \leqslant \sigma$ для каждого $s \in \mathcal{S}$. Тогда $\mathbb{AC}$ реализует ε-совершенное шифрование для $\varepsilon < \sigma q^{-1}$ и обеспечивает следующие значения вероятностей успеха имитации и подмены: $p_0 = q^{-1}$, $p_1 \leqslant r\sigma q^{-1}$.

1. Криптосистема $\mathbb{CS}$

Заметим, что А-код $\mathbb{AC}$ обеспечивает указанный в теореме 1 уровень стойкости лишь при однократном использовании ключа и при условии, что открытый текст неизвестен. При частично известном открытом тексте $\mathbb{AC}$ не обеспечивает стойкости. В самом деле, если известны две пары (s_i, m_i), (s_j, m_j), то ключ (a, b) можно определить из системы уравнений

$$\begin{cases} m_i \oplus s_i = c_i \cdot a \oplus d_i \cdot b, \\ m_j \oplus s_j = c_j \cdot a \oplus d_j \cdot b. \end{cases} \tag{2}$$

Константы c_i, d_i не являются секретными, кроме того, из условий (1) следует, что система (2) совместна, возможно, лишь за исключением случая, когда $a = b = 0$. Таким образом, $\mathbb{AC}$ нестоек к атаке на основе подобранного открытого текста.

Алгоритм шифрования, реализуемый $\mathbb{AC}$, можно трактовать как «одноразовый» алгоритм шифрования с аутентификацией. Он использует шифрсистему гаммирования и систему аутентификации полиномиального типа, известную под названием GMAC.

Модифицируем этот алгоритм таким образом, чтобы стало допустимо многократное использование ключа. Для этого введём зависимость констант c_i, d_i от основного ключа и будем использовать зависящие от вектора инициализации производные ключи для зашифрования каждого сообщения.

Введём обозначения $a, \overline{a}, \mathbf{a}$ соответственно для элемента поля $a \in \mathbb{F}_{2^n}$, строки $\overline{a} \in \{0,1\}^n$ коэффициентов многочлена, представляющего a как элемент фактор-кольца $\mathbb{F}_2[x]/(h(x)) \cong \mathbb{F}_{2^n}$, и числа $\mathbf{a} \in \mathbb{Z}_{2^n}$, двоичная запись которого совпадает с $\overline{a}$.

Определим криптосистему шифрования с аутентификацией $\mathbb{CS}$, которая использует основной ключ $k = (a, b) \in \left(\mathbb{F}_{2^n}\right)^2$, наборы констант

$$\mathcal{A} = \{w_i \in \mathbb{F}_{2^n} : \mathbf{w}_i = p(i)\},\ \mathcal{A}(k) = \{w_i(k) : w_i \in \mathcal{A}\},$$
$$c_i(k) = w_i(k),\ d_i(k) = \varphi(w_i(k)),\ i = 1, 2, \ldots, 2^n - 1,$$

и вектор инициализации

$$iv^{(\tau)} = \left(\gamma^{(\tau)}, \delta^{(\tau)}\right) \in (\mathbb{F}_{2^n})^2$$

для зашифрования текстов $s^{(\tau)}$, $\tau = 1, 2, \ldots, L$, $L \in \mathbb{N}$. Здесь p — биективное отображение $\mathbb{Z}_{2^n} \to \mathbb{Z}_{2^n}$; $w_i(k) = f_k(w_i)$ определяется с помощью отображения $f_x : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$, $x \in (\mathbb{F}_{2^n})^2$, а φ — отображение $\mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$. Вектор инициализации $iv^{(\tau)}$ должен содержать счётчик, который делает вектор неповторяющимся, метку времени и необходимые атрибуты передаваемого сообщения.

Текст $s^{(\tau)}$, представленный в виде последовательности $s^{(\tau)} = (s_1^{(\tau)}, \ldots, s_{r_\tau}^{(\tau)})$ элементов из $\mathbb{F}_{2^n}$, шифруется на производном ключе $k^{(\tau)} = (a^{(\tau)}, b^{(\tau)}) = g\left(k, iv^{(\tau)}\right)$, где g — отображение $(\mathbb{F}_{2^n})^4 \to (\mathbb{F}_{2^n})^2$. Результатом зашифрования $s^{(\tau)}$ служит $m^{(\tau)} = (m_1^{(\tau)}, \ldots, m_{r_\tau}^{(\tau)}, m_{r_\tau+1}^{(\tau)})$ — последовательность элементов из $\mathbb{F}_{2^n}$, где

$$m_i^{(\tau)} = s_i^{(\tau)} \oplus c_i(k)a^{(\tau)} \oplus d_i(k)b^{(\tau)},\ i = 1, \ldots, r_\tau,$$
$$m_{r_\tau+1}^{(\tau)} = a^{(\tau)} \oplus m_1^{(\tau)} \left(b^{(\tau)}\right)^{r_\tau} \oplus \ldots \oplus m_{r_\tau}^{(\tau)} \left(b^{(\tau)}\right)^1.$$

Отправитель посылает сообщение $(iv^{(\tau)}, m^{(\tau)})$. Получатель сообщения (iv, m), где $iv = (\gamma, \delta)$, $m = (m_1, \ldots, m_r, m_{r+1})$, вычисляет производный ключ $(a', b') = g(k, iv^{(\tau)})$. Критерий аутентичности сообщения — равенство

$$m_{r+1} = a' \oplus m_1 \cdot b'^r \oplus \ldots \oplus m_r \cdot b'^1.$$

Если оно выполнено, то получатель вычисляет константы $w_i' = f_k(w_i)$ и открытый текст $s = (s_1, \ldots, s_r)$, где

$$s_i = m_i \oplus w_i' \cdot a' \oplus \varphi(w_i')b',\ i = 1, 2, \ldots, r.$$

Уточним выбор отображений p, f_x, g и φ. Этот выбор должен обеспечить достаточный уровень стойкости, в частности достижимость оценок теоремы 1, а также возможность эффективной реализации криптосистемы. Далее мы остановимся на некоторых вариантах выбора указанных отображений. Подчеркнём, что предлагаемые варианты являются лишь примерами и не дают окончательного решения задачи синтеза криптосистемы. Заинтересованный читатель может предложить и свои варианты, возможно, более разумные и обоснованные.

Выбор отображения φ свяжем с необходимостью выполнения условия (1). Такими отображениями являются, например, $\varphi(c) = c^2$ или $\varphi(c) = c \oplus \alpha$, где α — любой фиксированный ненулевой элемент из $\mathbb{F}_{2^n}$. В самом деле, если, скажем, $\varphi(c) = c^2 = d$ и для ненулевых элементов поля c', c выполняется равенство $c \cdot d' = c' \cdot d$, то $c \cdot c'^2 = c' \cdot c^2$ и $c' = c$.

Набор констант $w_i \in \mathcal{A}$ играет роль «счётчика». Набор констант $w_i(k) = f_k(w_i) \in \in \mathcal{A}(k)$ делает «счётчик» зависимым от ключа. Естественно потребовать, чтобы отображение f_k было инъективным и, кроме того, делало зависимость констант $w_i(k)$ от ключа нелинейной. Это необходимо для того, чтобы нелинейной стала функция зашифрования. Один из вариантов такого f_k связан с использованием подходящих квазигрупповых операций $*$ на $\mathbb{F}_{2^n}$ (перемешивающие преобразования) и обратимых преобразований множества $\{0,1\}^n$ (рассеивающие преобразования).

Такое отображение можно определить, например, формулой

$$f_k(w) = L(w * a) *' b, \tag{3}$$

где $*, *'$ — квазигрупповые операции (возможно, одинаковые), а L — обратимое преобразование множества $\{0,1\}^n$, обладающее хорошими рассеивающими свойствами. Подходящие квазигрупповые операции предложены, например, в [6, 7]. Так, в [6] операция $x * y = z$ на $\mathbb{F}_{2^t}$ задаётся формулой

$$\mathbf{z} = P(\mathbf{x}, \mathbf{y}) = \sum_{i,j} a_{i,j}\mathbf{x}^i\mathbf{y}^j \bmod 2^t \tag{4}$$

при условии, что $P(u,0), P(0,v), P(u,1)$ и $P(1,v)$ определяют биекции. Критерий биективности отображения $\mathbb{Z}_{2^t} \to \mathbb{Z}_{2^t}$, задаваемого многочленом $a_0 + a_1x + \ldots + a_mx^m$, определяется следующими уловиями: a_1 — нечётное число, а числа $(a_2 + a_4 + a_6 + \ldots)$ и $(a_3 + a_5 + a_7 + \ldots)$ — чётные. В [7] операция $x * y = z$ на $\mathbb{F}_{2^t}$ задаётся формулой

$$\mathbf{z} = \theta\mathbf{x} + \vartheta\mathbf{y} + \pi\mathbf{x}^\lambda\mathbf{y}^\mu \bmod 2^t, \tag{5}$$

где θ, ϑ — нечётные числа; π — чётное число; $\lambda, \mu \in \mathbb{N}$.

В качестве L в (3) можно предложить, например, следующее отображение. Представим вектор $\overline{x} \in \{0,1\}^n$ в виде последовательности байтов $\overline{x} = \overline{x}_1||\ldots||\overline{x}_{n/8}$. Пусть $\widehat{L}$ — максимально рассеивающая матрица размеров $n/8 \times n/8$. Тогда $L(x) = y$, где $\overline{y} = \overline{y}_1||\ldots||\overline{y}_{n/8}$, а $\left(\mathbf{y}_1, \ldots, \mathbf{y}_{n/8}\right) = \left(\mathbf{x}_1, \ldots, \mathbf{x}_{n/8}\right)\widehat{L}$. Умножение выполняется в поле $\mathbb{F}_{256}$. Такое преобразование делает зависимым каждый байт вектора $\overline{y}$ от каждого байта вектора $\overline{x}$. Например, при $n = 128$ это преобразование, используемое в шифрсистеме «Кузнечик».

Отображение p, определяющее «счётчик», можно, например, задать перестановочным многочленом $p(x)$ над кольцом $\mathbb{Z}_{2^n}$. Критерий биективности такого многочлена сформулирован выше.

При выборе отображения g будем исходить из того, чтобы при случайном равновероятном выборе ключа $k = (a, b)$ ключ $k^{(\tau)} = (a^{(\tau)}, b^{(\tau)})$ также выбирался случайно равновероятно, разным значениям τ отвечали разные ключи $k^{(\tau)}$ и чтобы задача нахождения ключа k при известных $k^{(\tau)}$, $iv^{(\tau)}$ была вычислительно сложной. Один из вариантов такого отображения даёт использование введённых квазигрупповых операций

$$g\left(a, b, \gamma^{(\tau)}, \delta^{(\tau)}\right) = \left(L\left(a * \gamma^{(\tau)}\right) *' a, L\left(b * \delta^{(\tau)}\right) *' b\right), \tag{6}$$

где компоненты правой части равенства получены аналогично формуле (3).

2. Анализ криптосистемы $\mathbb{CS}$

Приведём некоторые общие соображения, которые качественно характеризуют стойкость криптосистемы $\mathbb{CS}$.

Заметим, что предложенный выбор отображений φ, f_k, p, g позволяет утверждать, что $w_i(k) \neq w_j(k)$ при $i \neq j$ и при неповторяющемся векторе инициализации $iv^{(\tau)}$ каждый производный ключ $k^{(\tau)}$ используется однократно, причём если k выбирается случайно равновероятно, то и $k^{(\tau)}$ выбирается случайно равновероятно. Эти замечания приводят к следующему утверждению.

Теорема 2. Пусть ключ k криптосистемы $\mathbb{CS}$ выбирается случайно равновероятно, а распределение $\mathcal{P}_S$ таково, что для действительных чисел α, β, σ, удовлетворяющих неравенствам $0 < \alpha, \beta < 1 \leqslant \sigma$, выполняются условия $\alpha \leqslant p_S(s) \leqslant \beta$, $\beta/\alpha \leqslant \sigma$ для каждого $s \in \mathcal{S}$. Тогда $\mathbb{CS}$ реализует ε-совершенное шифрование текста $s^{(\tau)}$, состоящего из $r^{(\tau)} > 1$ блоков, для $\varepsilon < \sigma 2^{-n}$. При этом для $\mathbb{CS}$ как A-кода с секретностью имеют место следующие оценки вероятностей успеха имитации и подмены: $p_0 = 2^{-n}$, $p_1 \leqslant r^{(\tau)}\sigma 2^{-n}$.

Доказательство. Заметим, что роль констант c_i, d_i для криптосистемы $\mathbb{CS}$ выполняют $f_k(w_i)$ и $\varphi(f_k(w_i))$. В нашем случае не исключается ситуация, когда $f_k(w_i) = L(w_i * a) *' b = 0$. В условиях теоремы 1 константы c_i, d_i ненулевые и удовлетворяют соотношению (1). Такой выбор констант позволял получить оценку величины ε. Для этого использовалась формула

$$\varepsilon = \max_{s,m} \left| \frac{|\mathcal{K}(s,m)|}{|\mathcal{K}(m)|} - \frac{1}{|\mathcal{S}|} \right|, \tag{7}$$

в которой величина $|\mathcal{K}(m)|$ равна q, а величина $|\mathcal{K}(s,m)|$ ограничена сверху единицей.

В условиях теоремы 2 величина $|\mathcal{K}(m)|$ не меняется, поскольку меняется лишь производный ключ $k^{(\tau)} = (a^{(\tau)}, b^{(\tau)})$, т. е., по сути дела, лишь вектор инициализации $iv^{(\tau)}$. Выясним, остается ли в силе ограничение для $|\mathcal{K}(s,m)|$.

Пусть для различных производных ключей $k' = (a', b')$ и $k'' = (a'', b'')$ выполняются равенства

$$m_i = s_i \oplus \widetilde{w}_i \cdot a' \oplus \widetilde{w}_i^2 \cdot b' = s_i \oplus \widetilde{w}_i \cdot a'' \oplus \widetilde{w}_i^2 \cdot b''.$$

Если $\widetilde{w}_i \neq 0$, то, как и в теореме 1, это невозможно. А если $\widetilde{w}_i = 0$, то это возможно лишь для одного значения i. Но по условию $r > 1$, поэтому либо $\widetilde{w}_{i-1} \neq 0$, либо $\widetilde{w}_{i+1} \neq 0$, и мы попадаем в условия предыдущего случая. Тем самым для различных k' и k'' при $r > 1$ невозможно равенство $E_{k'}(s) = E_{k''}(s)$. Следовательно, оценка величины ε по формуле (7) остаётся в силе, т. е. $\varepsilon < \sigma 2^{-n}$ в условиях теоремы 2. Вероятности успеха имитации и подмены оцениваются так же, как и в теореме 1. ■

Приведём числовой пример, характеризующий результаты теоремы 2. При $n = 128$, $\sigma = 2^{32}$, $r = 2^{32}$ криптосистема $\mathbb{CS}$ реализует ε-совершенное шифрование текста $s^{(\tau)}$ длины, не превосходящей 2^{32} блоков, для $\varepsilon < 2^{-96}$ и его аутентификацию, обеспечивая значения $p_0 = 2^{-128}$, $p_1 < 2^{-64}$.

Сделаем ряд замечаний по выбору параметров криптосистемы:

1) Выбор квазигрупповых операций в формулах (4) или (5) может быть достаточно произвольным. Он должен обеспечивать нелинейность преобразований в (3) и (6).
2) Задача определения ключа по открытому и шифрованному текстам для криптосистемы $\mathbb{CS}$ сводится к решению системы уравнений

$$\begin{cases} w_i(k)a^{(\tau)} \oplus w_i(k)^2 b^{(\tau)} = u_i^{(\tau)}, \\ a^{(\tau)} \oplus m_1^{(\tau)}(b^{(\tau)})^{r_\tau} \oplus \ldots \oplus m_{r_\tau}^{(\tau)}(b^{(\tau)})^1 = m_{r_\tau+1}^{(\tau)}, \\ i = 1, 2, \ldots, r_\tau,\ \tau = 1, 2, \ldots, L, \end{cases}$$

относительно ключа $k = (a, b)$, где $u_i^{(\tau)} = s_i^{(\tau)} \oplus m_i^{(\tau)}$. В этой системе можно считать известными лишь элементы $u_i^{(\tau)}$ и $m_j^{(\tau)}$, $j = 1, \ldots, r_{\tau+1}$. Для выбранных в (3) и (6) отображений f_k и g уравнения системы из первой строки приводят к нелинейным уравнениям относительно a, b, в записи которых используются как операции поля $\mathbb{F}_{2^n}$, так и операции кольца $\mathbb{Z}_{2^n}$.

Исключение $a^{(\tau)}$ из второй строки системы не даёт возможности исключить $a^{(\tau)}$ и из первой строки, поскольку $w_i(k)$ неизвестны. Остаётся возможность того, что при некотором τ шифртекст будет состоять из большого числа нулевых элементов поля, в результате чего получится уравнение невысокой степени в поле $\mathbb{F}_{2^n}$ относительно $a^{(\tau)}, b^{(\tau)}$. В худшем случае, когда $m_1^{(\tau)} = \ldots = m_{r_\tau}^{(\tau)} = 0$,

получается равенство $a^{(\tau)} = m^{(\tau)}_{r_\tau+1}$. Однако вероятность такого события сравнима с величиной 2^{-nr_τ}. При этом найти $b^{(\tau)}$ не представляется возможным.
Можно попытаться для нахождения производного ключа опробовать все варианты $b^{(\tau)}$ и вычислять из соотношения второй строки $a^{(\tau)}$. Но при этом для 2^n получившихся допустимых вариантов производного ключа необходимо проверить соотношение из первой строки. Для этого потребуется решить уравнения $a^{(\tau)} = L\left(a * \gamma^{(\tau)}\right) *' a$ и $b^{(\tau)} = L\left(b * \delta^{(\tau)}\right) *' b$ относительно неизвестных a и b. Ясно, что такая задача является вычислительно сложной. Это делает практически невозможной попытку нахождения производного ключа путём опробования. Тем самым задача определения ключа в атаке с подобранными открытыми текстами объективно сложна.

3) Выбор в определении (3) преобразования L с хорошими рассеивающими свойствами делает маловероятной возможность того, чтобы близким векторам $\overline{w}_i$ и $\overline{w}_j$ соответствовали близкие векторы $\overline{w}_i(k)$ и $\overline{w}_j(k)$. Поэтому даже для тривиального счётчика p, такого, что $p(x) = x$, маловероятна близость векторов $\overline{w}_i(k)$ и $\overline{w}_{i+1}(k)$, которую можно использовать для построения метода определения производного ключа. Использование нетривиального счётчика p, предложенного выше, ещё в большей степени защищает от указанной потенциальной слабости преобразования (3).
4) Оценка $\mathbb{CS}$ с позиций атак различения возможна по той же схеме, которая была использована при оценке стойкости криптосистемы GCM [5, 8]. В самом деле, $\mathbb{CS}$ отличается от GCM лишь тем, что использует в качестве базовой системы шифрования не систему подстановок $E = \{E_k : \{0,1\}^n \to \{0,1\}^n,\ k \in \mathcal{K}\}$, а систему функций $\Phi = \{\Phi_{k,iv} : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n} |\ k, iv \in (\mathbb{F}_{2^n})^2\}$, где
$$\Phi_{k,iv}(w) = f_k(w)a^{(\tau)} \oplus (f_k(w))^2 b^{(\tau)}, \tag{8}$$
и тем, что её система аутентификации основана на полиномах со свободным членом, тогда как GCM использует для аутентификации полиномы без свободного члена. Последнее, очевидно, не влияет на стойкость аутентификации. Значения функции $\Phi_{k,iv}$ — это блоки гаммы, используемые для шифрования блоков открытого текста. Так как при шифровании текста $a^{(\tau)}$ и $b^{(\tau)}$ не изменяются, мы имеем дело с семейством функций вида $\alpha w' \oplus \beta w'^2$ для некоторых $\alpha, \beta \in \mathbb{F}_{2^n}$, где $w' = L(w * a) *' b$. Поскольку многочлен $\alpha x \oplus \beta x^2$ может иметь более одного корня в $\mathbb{F}_{2^n}$, функции $\Phi_{k,iv}$ могут не быть биективными. В то же время, так как для любого $\rho \in \mathbb{F}_{2^n}$ и любых α, β, одновременно не равных нулю, уравнение $\alpha x \oplus \beta x^2 = \rho$ имеет не более двух решений, число образов $\Phi_{k,iv}$ (блоков гаммы) достаточно велико: $|\{\Phi_{k,iv}(w) | w \in \mathcal{A}\}| \geqslant 2^n/2 > 2^{n-1}$.
5) Биективная связь w' с w, зависящая от ключа, и зависимость от ключа $a^{(\tau)}$ и $b^{(\tau)}$ делают недоступными для атакующего ни w', ни α, β. Поэтому в атаке различения семейства функций Φ, получая от оракула значения $\Phi_{k,iv}(w)$, $i = 1, 2, \ldots$, различитель не может воспользоваться тем, что $\Phi_{k,iv}$ как функция от w'_i является многочленом. Если бы зависимость $w' = f(w)$ была известной, различитель воспользовался бы интерполяционной формулой Лагранжа и построил эффективную атаку, использующую всего лишь четыре запроса к оракулу.
6) Можно использовать криптосистему $\mathbb{CS}$ в режиме AEAD (режим шифрования с аутентификацией, использующий ассоциированные данные), добавив на этапе аутентификации блоки ассоциированных данных подобно тому, как это сделано в GCM.

7) При случайном выборе ключа не исключается случай, когда $k^{(\tau)} = (0,0)$. Этот случай нежелателен, поскольку все блоки гаммы становятся равными 0^n. Избавиться от этого можно следующим образом. При вычислении производного ключа $k^{(\tau)}$ можно ввести дополнительный шаг — проверку равенства $k^{(\tau)} = (0,0)$. Если оно выполняется, то нужно сменить $iv^{(\tau)}$. Для этого можно в $\overline{iv}^{(\tau)}$ выделить один бит, например старший, и в случае, когда $k^{(\tau)} = (0,0)$, инвертировать этот бит.
8) Схема алгоритма криптосистемы $\mathbb{CS}$ представлена на рис. 1.

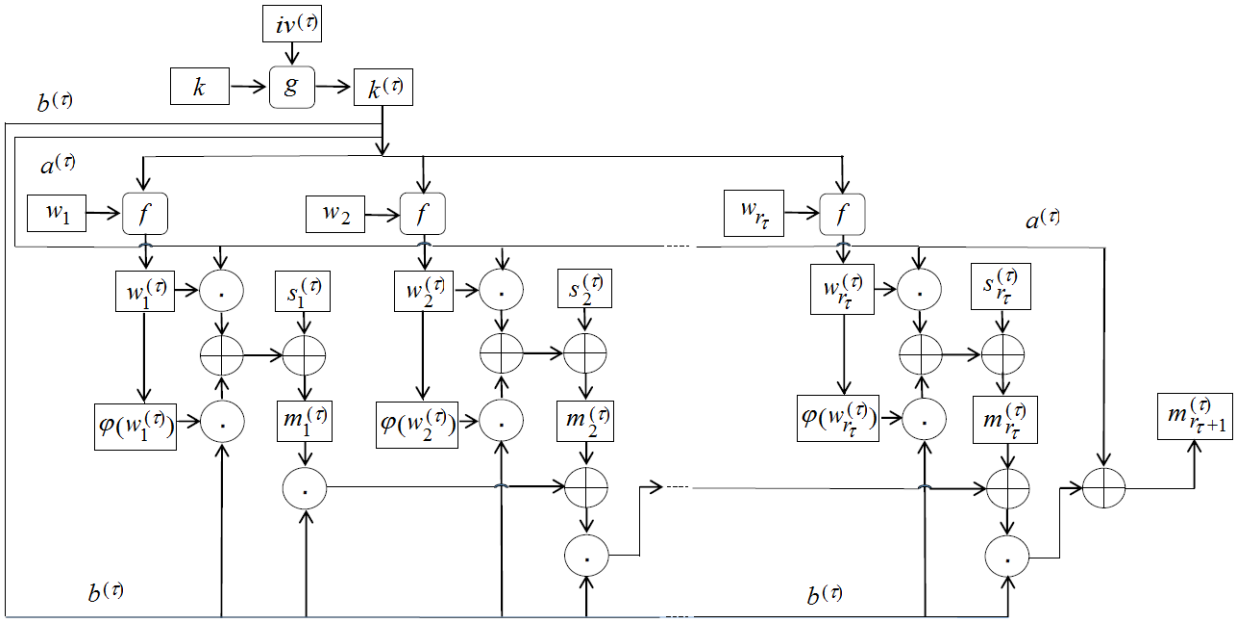

Рис. 1. Криптосистема $\mathbb{CS}$ (без дополнения последнего неполного блока)

Все шаги алгоритма эффективно реализуемы, об этом свидетельствует, например, то, что операции алгоритма реализуются стандартными средствами пакета «Математика». Наиболее трудоёмкими являются квазигрупповые операции $*$ и операции умножения элементов поля $\mathbb{F}_{2^n}$. Были бы интересны и другие варианты выбора квазигрупповых операций на множестве $\{0,1\}^n$, обладающие указанными выше свойствами и допускающие более эффективные реализации.
9) Заметим, что при использовании предложенного варианта отображения $\varphi(c) = c \oplus \alpha$, где α — любой фиксированный ненулевой элемент из $\mathbb{F}_{2^n}$, можно выиграть в трудоёмкости. Получим алгоритм, который при шифровании каждого блока использует не три, а лишь две операции умножения в поле. В таком варианте схемы вместо функций (8) используются функции вида $\Phi_{k,iv}(w) = f_k(w)a^{(\tau)} \oplus (f_k(w) \oplus \alpha)\, b^{(\tau)}$. Следует, однако, отметить недостаток такой схемы. В случае, если $a^{(\tau)} = b^{(\tau)}$, $\mathbb{CS}$ реализует шифр простой замены. Такой случай нежелателен. Он устраним таким же образом, как и в п. 7.
10) Выбор констант, используемых в алгоритме, позволяет параллельно вычислять блоки шифртекста и допускает возможность зашифрования текста вплоть до длины, сравнимой с числом элементов поля. Заметим, что предложенный алгоритм допускает этап предвычислений, который может дать существенный выигрыш в трудоёмкости при шифровании многих сообщений с помощью основного ключа k. В самом деле, при шифровании текстов $s^{(\tau)}$ используется один и тот

же набор констант $w_i(k)$, $i = 1, 2, \ldots$ Если в некотором приложении тексты $s^{(\tau)}$ имеют не слишком большие длины, то можно выделить память для записи этих констант и использовать их далее при шифровании многих текстов.

11) Схему дополнения последнего неполного блока для $\mathbb{CS}$ можно выбрать той же, что и в GCM.

Заключение

Представленная идея криптосистемы шифрования с аутентификацией допускает эффективную реализацию при широком спектре изменяемых параметров, прежде всего отображений φ, f_k, p, g, L. Конструкция криптосистемы позволяет в теореме 2 дать оценку её стойкости как кода аутентификации с секретностью и показать, что она реализует ε-совершенное шифрование сообщений с незначительными ограничениями на их частотные характеристики и обеспечивает стойкую аутентификацию. Подобная оценка для криптосистемы шифрования с аутентификацией получена впервые.

Приводятся соображения, указывающие на объективную сложность задачи определения ключа варианта криптосистемы в атаке с подобранными открытыми текстами. Выделяются некоторые «слабые» ключи и предлагаются пути обхождения этих слабостей. Вместе с тем задача определения ключа требует более детального анализа, как и задача оценки псевдослучайности семейства функций (8), определяющей оценку стойкости криптосистемы в атаках различения.

Некоторые детали алгоритма, реализуемого криптосистемой, такие, как выбор вектора инициализации, дополнение последнего неполного блока, способы реализации операций поля $\mathbb{F}_{2^n}$ и кольца $\mathbb{Z}_{2^n}$, организация и объём необходимой памяти, возможность использования ассоциированных данных, также требуют более тщательной проработки.

ЛИТЕРАТУРА

1. *Kabatianskii G. A., Johansson G., 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.
2. *Зубов А. Ю.* Почти совершенные шифры и коды аутентификации // Прикладная дискретная математика. 2011. № 4(14). С. 28–33.
3. *Зубов А. Ю.* О понятии ε-совершенного шифра // Прикладная дискретная математика. 2016. № 3(33). С. 45–52.
4. *Зубов А. Ю.* Коды аутентификации с секретностью // Математические вопросы криптографии. 2017. Т. 8. № 3. С. 5–40.
5. *Зубов А. Ю.* Об оценке стойкости AEAD-крипосистемы типа GCM // Прикладная дискретная математика. 2016. № 2(32). С. 49–62.
6. *Rivest R. R.* Permutation polynomials modulo 2^w // Finite Fields Their Appl. 2001. V. 7. No. 2. P. 287–292.
7. *Заец М. В.* Построение подстановок с использованием вариационно-координатно полиномиальных функций над примарным кольцом вычетов // Математические вопросы криптографии. 2015. Т. 6. № 1. С. 5–32.
8. *McGrew D. A. and Viega J.* The security and performance of Galois/Counter mode of operation // LNCS. 2004. V. 3348. P. 343–355.

REFERENCES

1. *Kabatianskii G. A., Johansson G., and Smeets B.* On the cardinality of systematic A-codes via error correcting codes. IEEE Trans. Inform. Theory, 1996, vol. IT-42, no. 2, pp. 566–578.

2. *Zubov A. Yu.* Pochti sovershennye shifry i kody authentifikatsii [Almost perfect ciphers and authentication codes]. Prikladnaya Diskretnaya Matematika, 2011, no. 4(14), pp. 28–33. (in Russian)
3. *Zubov A. Yu.* O ponyatii ε-sovershennogo shifra [About the concept of ε-perfect cipher]. Prikladnaya Diskretnaya Matematika, 2016, no. 3(33), pp. 45–52. (in Russian)
4. *Zubov A. Yu.* Kody authentifikatsii s sekretnostiu [Authentication codes with secrecy]. Matematicheskie Voprosy Kriptografii, 2017, vol. 8, no. 3, pp. 5–40. (in Russian)
5. *Zubov A. Yu.* Ob otcenke stoykosti AEAD-kriptosystemy tipa GCM [On the estimation of secrecy of the type GCM AEAD-cryptosystem]. Prikladnaya Diskretnaya Matematika, 2016, no. 2(32), pp. 49–62. (in Russian)
6. *Rivest R. R.* Permutation polynomials modulo 2^w. Finite Fields Their Appl., 2001, vol. 7, no. 2, pp. 287–292.
7. *Zaec M. V.* Postroenie podstanovok s ispolzovaniem variatcionno-koordinatno polinomialnykh funktciy nad primarnym koltcom vychetov [Build of permutations using variation-coordinate polynomiality functions over primary deduction ring]. Matematicheskie Voprosy Kriptografii, 2015, vol. 6, no. 1, pp. 5–32. (in Russian)
8. *McGrew D. A. and Viega J.* The security and performance of Galois/Counter mode of operation. LNCS, 2004, vol. 3348, pp. 343–355.