ОБОЗРЕНИЕ
ПРИКЛАДНОЙ И ПРОМЫШЛЕННОЙ
Том 23 МАТЕМАТИКИ Выпуск 5
2016

А. Ю. Нестеренко (Москва, НИУ ВШЭ)**. Об одном подходе к построению схем шифрования с возможностью аутентификации.**

В работе предлагается подход к построению режима работы произвольного блочного шифра, позволяющего одновременно зашифровыввать сообщения и вычислять их код аутентичности. Предлагаемый подход основан на использовании универсальных функций хеширования с заданными свойствами.

Пусть w, m натуральные числа, $\mathbb{V}^w$ — пространство двоичных векторов длины m и $\mathbb{V}^\infty \supset \mathbb{V}^w$ — пространство двоичных векторов произвольной длины.

Под режимом шифрования с возможностью аутентификации мы рассматриваем следующее отображение.

$$\begin{gathered}\mathrm{AEAD} : \mathbb{V}^m \times \mathbb{V}^m \times \mathbb{V}^\infty \times \mathbb{V}^\infty \times \mathbb{V}^{2w} \to \mathbb{V}^\infty \times \mathbb{V}^{2w},\\ \mathrm{AEAD}(K_1, K_2, X, M, iv) = \{C, a\},\end{gathered} \tag{1}$$

где $X \in \mathbb{V}^\infty$ открытый текст, $M \in \mathbb{V}^\infty$ — ассоциированные с открытым текстом X данные, $C \in \mathbb{V}^\infty$ зашифрованный текст, $K_1 \in \mathbb{V}^m$ — ключ шифрования, $K_2 \in V^m$ — ключ аутентификации, $iv \in \mathbb{V}^{2w}$ — случайный вектор (синхропосылка) и $a \in \mathbb{V}^{2w}$ — код аутентичности сообщения X.

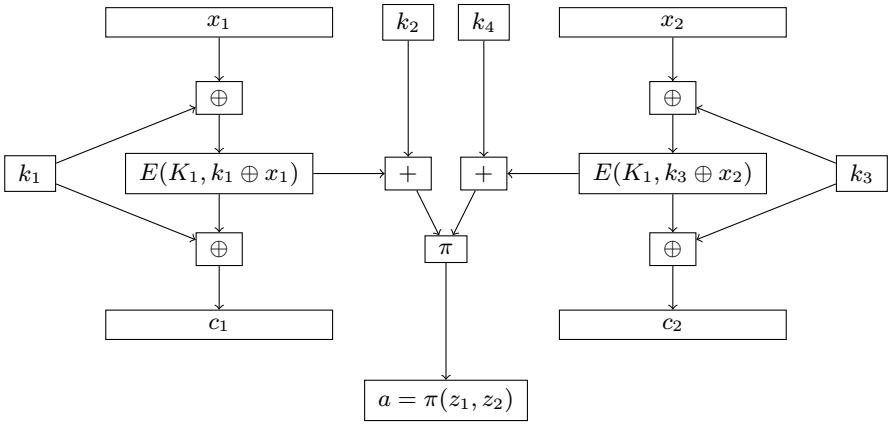
Для того, чтобы определить отображение (1) нам потребуется ряд вспомогательных определений. Обозначим $E(K, x) : \mathbb{V}^m \times \mathbb{V}^w \to \mathbb{V}^w$ произвольный блочный шифр и $\pi(z_1, z_2) : \mathbb{V}^w \times \mathbb{V}^w \to \mathbb{V}^{2w}$ нелинейное отображение, являющееся перестановкой на множестве $\mathbb{V}^{2w}$. Пример такой перестановки был приведен автором в работе [1]. Введем отображение

$$\begin{gathered}\Omega : \mathbb{K} \times \mathbb{V}^{2w} \times \mathbb{V}^{4w} \to \mathbb{V}^{2w} \times \mathbb{V}^{2w},\\ \Omega(K, x, \gamma) = \{c, a\},\end{gathered}$$

где $\gamma = (k_1, \ldots, k_4)$ вектор размерности четыре, $k_1, \ldots, k_4 \in \mathbb{V}^w$, и

$$\begin{gathered}\xi_1 = E(K, x_1 \oplus k_1), \quad \xi_2 = E(K, x_2 \oplus k_3), \quad x = x_1 || x_2,\\ c = k_1 \oplus \xi_1 || k_3 \oplus \xi_2, \quad a = \pi(\xi_1 + k_2, \xi_2 + k_4).\end{gathered}$$

Отображение Ω представляет собой процедуру зашифрования двух блоков открытого текста $x = x_1 || x_2$ с одновременным вычислением контрольной суммы a этих блоков. Схематично, отображение Ω можно изобразить следующим образом.



Опишем способ генерации ключевой последовательности k_n, используемой в преобразовании Ω и вырабатываемой с помощью исходной синхропосылки $iv \in \mathbb{V}^{2w}$ и ключа аутентификации $K_2 \in \mathbb{V}^m$. Определим $k_{-1} = E(K_2, \mathrm{lsb}_w(iv))$ и $k_0 = E(K_2, \mathrm{msb}_w(iv))$, тогда

$$\begin{aligned} k_{2n-1} &= k_{2n-3} + nC \pmod{2^w}, \\ k_{2n} &= k_{2n-2}\theta^n, \end{aligned}$$

где C фиксированная константа, а θ примитивный элемент поля $\mathbb{F}_{2^w}$.

Представим ассоциированные данные $M = (m_1, \ldots, m_u)$ и открытый текст $X = (x_1, \ldots, x_t)$ в виде последовательности блоков длины $2w$. Тогда мы можем определить режим шифрования с возможностью аутентификации следующей последовательностью шагов.

1. Для всех $n = 1, \ldots, u$ применим преобразование $\Omega(K_2, m_n, \gamma_n) = (\cdot, a_n)$, где $\gamma_n = (k_{4n-3}, \ldots, k_{4n})$, и определим значение a равенством $a \equiv \sum_{n=1}^{u} a_n \pmod{2^{2w}}$.
2. Если $0 < \mathrm{len}\,(x_t) < 2w$, то определим $t^* = t-1$. В противном случае, определим $t^* = t$.
3. Для всех $n = 1, \ldots, t^*$ применим преобразование $\Omega(K_1, x_n, \gamma_{u+n}) = (c_n, a_{u+n})$ и определим значение a равенством $a \equiv a + \sum_{n=1}^{t^*} a_{u+n} \pmod{2^{2w}}$.
4. Если $t^* = t - 1$, то определим $x_t^* = x_t || \mathrm{msb}(c_{t-1})$, применим преобразование $\Omega(K_1, x_t^*, \gamma_{u+t}) = (c_t^*, a_{u+t})$, определим значение a равенством $a \equiv a + a_{u+t} \pmod{2^{2w}}$ и положим $c_t = \mathrm{lsb}(c_{t-1})$, $c_{t-1} = c_t^*$.
5. Вычислим $\Omega(K_2, a, \gamma_{u+t+1}) = (A, \cdot)$ и определим код аутентичности сообщения X равным A. При этом, величины $c_1, \ldots, c_t$ образуют зашифрованный текст, соответствующий сообщению X.

Верна следующая теорема.

Теорема. *Пусть отображение $E(K, x)$ представляет собой перестановку на множестве $\mathbb{V}^w$ для любого фиксированного значения K. Тогда, для любого натурального числа t и любых фиксированных значений K_1, K_2, M, iv и A найдется в точности $2^{2w(t-1)}$ сообщений X таких, что $\mathrm{len}\,(X) = 2^{2wt}$ и* $\mathrm{AEAD}(K_1, K_2, M, X, iv) = A$.

СПИСОК ЛИТЕРАТУРЫ

1. *Нестеренко А. Ю.* Об одном семействе универсальных функций хеширования. — Математические вопросы криптографии, 2015, т. 6, в. 3, с. 135–151.