ОБОЗРЕНИЕ
ПРИКЛАДНОЙ И ПРОМЫШЛЕННОЙ
Том 25 МАТЕМАТИКИ Выпуск 4
2018

А. П. Науменко (Москва, ОАО «ИнфоТеКС»). **О подходах к анализу некоторых криптографических схем.**

В данном докладе рассмотрены две криптографические схемы.

1. Схема аутентифицированного шифрования «НЕФРИТ». Краткое описание (см. также [1])**.**

Входные данные алгоритма:

— уникальный вектор инициализации IV длиной 72 бита;

— ассоциированные данные $A = A_1 \parallel \ldots \parallel A_r \in V^*$; $|A_i| = 128$; $1 \leqslant i \leqslant r-1$; $|A_r| = s$; $0 < s \leqslant 128$; $1 \leqslant r \leqslant 256$;

— открытый текст $P = P_1 \parallel \ldots \parallel P_m \in V^*$, $0 \leqslant m \leqslant 2^{32} - 1$;

— базовый ключ шифрования $K \in V_{256}$, базовый ключ финализации $K_1 \in V_{256}$ (ключи K и K_1 предполагаются различными), ключ имитозащиты $H = E_K(0^{128})$;

— $len(A)$ — 16-разрядное двоичное представление количества байт $A \in V^*$ (старшие 4 бита равны нулю);

— $len(P)$ — 40-разрядное двоичное представление количества байт $P \in V^*$ (старшие 4 бита равны нулю).

— E — базовый алгоритм шифрования «Кузнечик» (ГОСТ Р 34.12.2015, 128 бит).

Выходные данные алгоритма:

— ассоциированные данные $A = A_1 \parallel \ldots \parallel A_r \in V^*$; $1 \leqslant r \leqslant 256$;

— шифртекст $C = C_1 \parallel \ldots \parallel C_m \in V^*$; $|C_i| = 128, 1 \leqslant i \leqslant m-1$; $|C_m| = |P_m| = s_1 \leqslant 128$; $0 \leqslant m \leqslant 2^{32}-1$;

— имитовставка сообщения $T_t \in V^t$, $t \leqslant 128$.

Процедура зашифрования:

— открытый текст $P = P_1 \parallel \ldots \parallel P_m \in V^*$ зашифровывается в режиме гаммирования;

— начальное значение счетчика: $CTR_1 = IV_1 = 0^{24} \parallel IV \parallel 0^{31}1$;

— каждое следующее значение счетчика CTR_j получается прибавлением единицы по модулю 2^{32} к правым 32 битам предыдущего значения счетчика CTR_{j-1};

— результатом зашифрования является шифртекст $C = C_1 \parallel \ldots \parallel C_m \in V^*$, $len(C)$ при передаче в канал связи совпадает с $len(P)$;

— ассоциированные данные при передаче в канал связи остаются неизменными.

Дополнение сообщения:

— $A = A_1 \parallel \ldots \parallel A_r$. Пусть $|A_r| = s$ бит. При $s < 128$ формируют вектор $A_r^* = A_r \parallel 1 \parallel 0^{128-s-1}$. При $s = 128$ полагают $A_r^* = A_r$.

— $C = C_1 \parallel \ldots \parallel C_m$. Пусть $m \neq 0$, $|C_m| = s_1$ бит. При $s_1 < 128$ формируют вектор $C_m^* = C_m \parallel 1 \parallel 0^{128-s_1-1}$. При $s_1 = 128$ полагают $C_m^* = C_m$.

В процессе вычисления имитовставки используются

$$A^* = A_1 \parallel \ldots \parallel A_r^* \in V^{128r}, \quad C^* = C_1 \parallel \ldots \parallel C_m^* \in V^{128m}.$$

Процедура выработки имитовставки. Вычисляется последовательность $T = E_{K_1}(\gamma_{m+r} \oplus E_{K_1}(IV_2))$, где

$$\begin{cases} \gamma_1 = A_1 \otimes H, & \\ \gamma_j = (\gamma_{j-1} \oplus A_j) \otimes H, & j = 2, \ldots, r-1, \\ \gamma_r = (\gamma_{r-1} \oplus A_r^*) \otimes H, & \text{при} \quad r > 1, \\ \gamma_{r+i} = (\gamma_{r+i-1} \oplus C_i) \otimes H, & i = 1, \ldots, m-1, \\ \gamma_{m+r} = (\gamma_{m+r-1} \oplus C_m^*) \otimes H & \text{при} \quad m > 0. \end{cases}$$

$$IV_2 = IV \parallel len(A) \parallel len(P).$$

В качестве имитовставки T_t берутся младшие $1 \leqslant t \leqslant 128$ бит последовательности T.

Атака на ключ имитозащиты H, основанная на циклической структуре многочлена.

Утверждение 1. *Вероятность того, что случайно выбранный из мультипликативной группы $GF(2^{128})$ элемент H имеет порядок, меньший n_0, может быть оценена следующим образом*:

$$\mathbf{P}\{ord(H) \leqslant n_0\} = \frac{\sum_{D|N,\ D \leqslant n_0} \varphi(D)}{N} = \min\left(\frac{8n_0}{N}, \frac{2n_0 \ln\ln n_0}{N}\right),$$

где $\varphi(x) = \sum_{s:gcd(s,x)=1} 1$ — *функция Эйлера,* $N = 2^{128} - 1$.

Атака на ключ имитозащиты H, основанная на использовании многочленов специального вида.

Утверждение 2. *Существует алгоритм вскрытия ключа имитозащиты H, имеющий сложность*

$$\frac{2^{128}}{m-1} + m - 1$$

попыток навязывания имитовставки. При этом предполагается, что все шифртексты имеют одинаковую длину m блоков. Для реализации алгоритма нарушителю требуется одна валидная пара (A, C, T_t).

Утверждение 3. *Имитовставка T_t принимает не менее $u = 2^t/m$ различных значений.*

2. Алгоритм выработки ключа «CryptoPro Key Meshing». Описание.

Пусть задана константа $C = (C_0||C_1||C_2||C_3)$, $C_i \in V_{64}$, $C_i \neq C_j$, $0 \leqslant i \neq j < 4$.

После зашифрования i-го блока данных (длиной 1024 байт) ключ K_i меняется в соответствии со следующим правилом:

$$K_{i+1}(K_0) = E^{-1}_{K_{K_i(K_0)}}(C), \quad i = 0, 1, \ldots,$$

где E^{-1} — расшифрование в режиме простой замены.

Результаты В. О. Миронкина [2]**.**

Пусть $K_1(K_0) = k_1^0 \| k_1^1 \| k_1^2 \| k_1^3$, $k_1^i \in V_{64}$. Тогда $k_1^i \neq k_1^j$, $0 \leqslant i \neq j < 4$.

Следовательно, мощность множество ключей $K_1(K_0)$, получаемых после первой итерации мешинга ограничена величиной $2^{64} \cdot (2^{64} - 1) \cdot (2^{64} - 2) \cdot (2^{64} - 3)$.

Обозначим B_i множество ключей, получаемых после i итераций мешинга. Тогда справедлива рекуррентная формула (см. также [3]):

$$M(|B_i|) = (1 - \tau_i)\,|B|, \quad \text{где} \quad \tau_0 = 0,\ \tau_{i+1} = e^{-1+\tau_i}.$$

Основные результаты.

Утверждение 4. *Справедливы соотношения*

$$\forall i \geqslant 1 \quad \alpha_i = 1 - \tau_i \leqslant \frac{3}{i};$$

$$\forall i \geqslant 10^8 \quad \alpha_i = 1 - \tau_i = \frac{2}{i} + \frac{\theta}{i^3},$$

где $|\theta| \leqslant 2/3$.

Утверждение 5. *Пусть* $c_{k,r}$ *— число ключей из множества* B_r, *в которые перешло ровно* k *ключей из множества* V_{256} *после* r *итераций мешинга. Справедлива рекурретная формула*

$$\frac{c_{k,r}}{c_{0,r}} = \sum_{t_1+2t_2+\ldots+kt_k=k} \prod_{s=1}^{k} \frac{c_{s,r-1}}{t_s!}.$$

Утверждение 6 (условное). *Пусть* Ψ_i *— распределение вероятностей* p_i *ключей из множества* B_i. *Тогда*

$$H(\Psi_i) = -\sum_{t=1}^{|B_i|} p_t \log_2 p_t \approx 256 - 2\ln 2 \cdot \log_2 T - \text{const}\,.$$

СПИСОК ЛИТЕРАТУРЫ

1. *Бабуева А. А.*, *Науменко А. П.* О подходах к анализу схем аутентифицированного шифрования, построенных с использованием умножения в конечных полях. — В сб.: Материалы XX научно-практической конференции «РусКрипто'2018» (Солнечногорск, 20–23 марта 2018 г.). https://www.ruscrypto.ru/resource/archive/rc2018/files/02_Babueva_Naumenko.pdf
2. *Миронкин В. О.* О некоторых вероятностных характеристиках алгоритма выработки ключа «CryptoPro Key Meshing». — В сб.: Материалы XVII научно-практической конференции «РусКрипто'2015» (Солнечногорск, 17–20 марта 2015 г.). https://www.ruscrypto.ru/resource/archive/rc2015/files/02_mironkin.pdf
3. *Flajolet P.*, *Odlyzko A. M.* Random mapping statistics.In: Advances in Cryptology–EUROCRYPT'89. Workshop on the Theory and Application of Cryptographic Techniques. (Houthalen, April 10–13, 1989.) Proceedings. Ed. by J.-J. Quisquater, J. Vandewalle. Heidelberg etc.: Springer, 1990, p. 329–354. (Ser. Lect. Notes Comput. Sci. V. 434.)