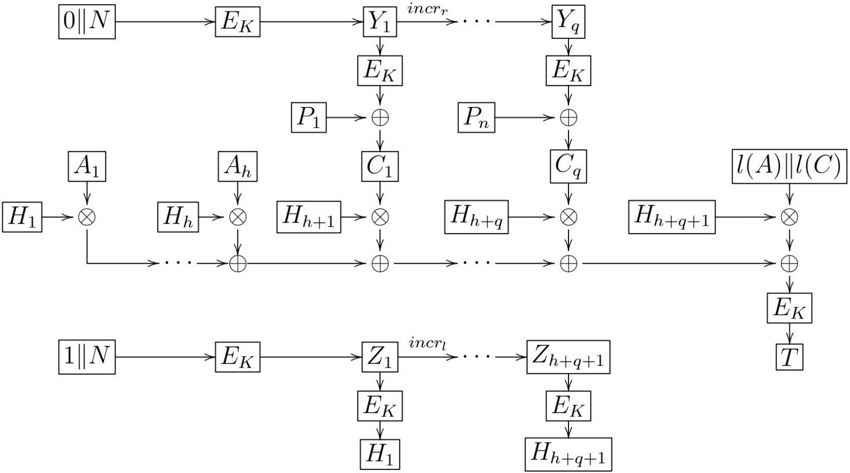
О подходах к анализу схем аутентифицированного шифрования, построенных с использованием умножения в конечных полях

Бабуева А. А., Науменко А.П.

ОАО «ИнфоТеКС»

22 марта 2018 г.

MGM



$0\|N$
E_K
Y_1
$incr_r$
Y_q
E_K
E_K
P_1
P_n
A_1
A_h
C_1
C_q
$l(A)\|l(C)$
H_1
H_h
H_{h+1}
H_{h+q}
H_{h+q+1}
E_K
T
$1\|N$
E_K
Z_1
$incr_l$
Z_{h+q+1}
E_K
E_K
H_1
H_{h+q+1}

MGM. Совпадение счетчиков.

Потенциально опасное событие для шифрования:

$$Y_{i_1}^{j_1} = Y_{i_2}^{j_2},\ 1 \leq i_1, i_2 \leq q,\ 1 \leq j_1, j_2 \leq N_{\text{сообщ}}.$$

В этом случае:

$$P_{i_1}^{j_1} \oplus C_{i_1}^{j_1} = P_{i_2}^{j_2} \oplus C_{i_2}^{j_2}.$$

$$P_{i_2}^{j_2} = P_{i_1}^{j_1} \oplus C_{i_1}^{j_1} \oplus C_{i_2}^{j_2}.$$

MGM. Совпадение счетчиков.

Пусть $\mu_v(N, 2^{n/2})$ — количество точек на отрезке длины $2^{n/2}$, в которые попадут левые части Y_l ровно v сообщений при общем числе сообщений N. Тогда справедлива формула:

$$Pr(Y_{i_1}^{j_1} \neq Y_{i_2}^{j_2}) = \prod_{v=2}^{N} p(v)^{\mu_v(N, 2^{n/2})},$$

где $p(v)$ — вероятность несовпадения правых частей счечиков Y_r в v произвольных сообщениях.

Для $p(v)$ справедлива оценка:

$$p(v) \geq e^{-\frac{v(v-1)(q-1)}{2^{n/2}}(1+\varepsilon)},$$

где $\varepsilon < 1/2$.

MGM. Совпадение счетчиков.

Для матожидания $M(v)$ величины $\mu_v(N, 2^{n/2})$ справедлива формула:

$$M(v) \approx 2^{n/2} \left(\frac{N}{2^{n/2}} \right)^v \frac{1}{v!}.$$

Разобьем промежуток изменения $1 \leq N < 2^{n/2}$ на области, в которых максимальное заполнение равно $r = 2, 3, 4, \ldots, N$, и оценим с использованием предельных теорем для $\mu_v(N, 2^{n/2})$ произведение

$$\prod_{v=2}^{r} p(v)^{\mu_v(N, 2^{n/2})}$$

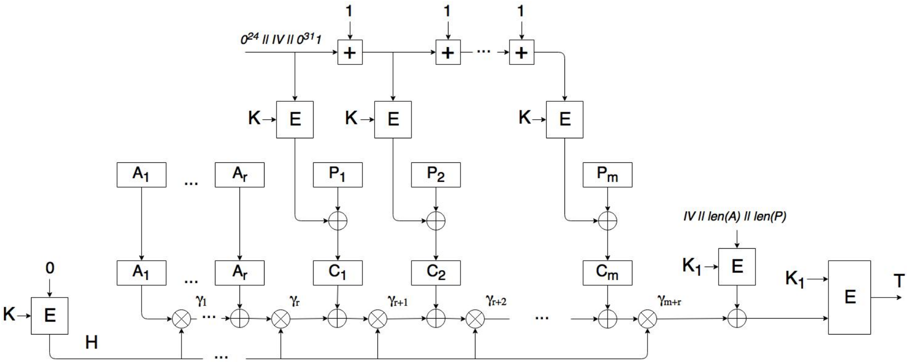
.

MGM. Совпадение счетчиков.

Получаем

$$Pr(Y_{i_1}^{j_1} = Y_{i_2}^{j_2}) \leq \frac{N^2(q-1)}{2^{n-1}},$$

N — количество переданных сообщений;
q — количество блоков открытого текста в одном сообщении (подразумеваем, что все сообщения имеют одинаковую длину);
n — длина блока.


1
1
1
0²⁴ II IV II 0³¹1
+
+
+
K
E
K
E
K
E
A1
Ar
P1
P2
Pm
IV II len(A) II len(P)
0
K
E
A1
Ar
C1
C2
Cm
K1
E
K1
E
T
γ1
γr
γr+1
γr+2
γm+r
H

«НЕФРИТ». Входные данные.

Входные данные алгоритма:

- уникальный вектор инициализации IV длиной 72 бита;
- ассоциированные данные
  $A = A_1 \parallel \ldots \parallel A_r \in V^*$; $|A_i| = 128$; $1 \le i \le r - 1$;
  $|A_r| = s$; $0 < s \le 128$; $1 \le r \le 256$;
  ассоциированные данные должны иметь в своем составе хотя бы один ненулевой блок;
- открытый текст $P = P_1 \parallel \ldots \parallel P_m \in V^*$, $0 \le m \le 2^{32} - r - 1$;
- базовый ключ шифрования $K \in V_{256}$;
- базовый ключ финализации $K_1 \in V_{256}$.

$len(A)$ – 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).

Выходные данные алгоритма:

- ассоциированные данные $A = A_1 \parallel \ldots \parallel A_r \in V^*$; $1 \leq r \leq 256$;
- шифртекст $C = C_1 \parallel \ldots \parallel C_m \in V^*$; $|C_i| = 128$, $1 \leq i \leq m-1$; $|C_m| = |P_m| = s_1 \leq 128$; $0 \leq m \leq 2^{32} - r - 1$;
- имитовставка сообщения $T_t \in V^t$, $t \leq 128$.

«НЕФРИТ». Ключевая система.

В процессе вычисления значения имитовставки используется базовый ключ шифрования K и базовый ключ финализации K_1. Ключи K и K_1 статистически независимы. Они могут быть выработаны в соответствии с любым из алгоритмов, описанных в проекте рекомендаций по стандартизации «Функции выработки производного ключа».

С использованием базового ключа шифрования K вырабатывается ключ имитозащиты:

$$H = E_K(0^{128}).$$

«НЕФРИТ». Процедура зашифрования.

- открытый текст $P = P_1 \| \ldots \| P_m \in V^*$ зашифровывается в режиме гаммирования;
- начальное значение счетчика:

$$CTR_1 = IV_1 = 0^{24} \| IV \| 0^{31}1;$$

- 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 $C = C_1 \| \ldots \| C_m \in V^*$, $len(C)$ при передаче в канал связи совпадает с $len(P)$;
- ассоциированные данные при передаче в канал связи остаются неизменными.

«НЕФРИТ». Дополнение сообщения.

- $A = A_1 \parallel \ldots \parallel A_r$. Пусть $|A_r| = s$ бит.
  При $s < 128$ $\quad A_r^* = A_r \parallel 1 \parallel 0^{128-s-1}$.
  При $s = 128$ $\quad A_r^* = A_r$.
- $C = C_1 \parallel \ldots \parallel C_m$. Пусть $m \neq 0$, $|C_m| = s_1$ бит.
  При $s_1 < 128$ $\quad C_m^* = C_m \parallel 1 \parallel 0^{128-s_1-1}$.
  При $s_1 = 128$ $\quad C_m^* = C_m$.

В процессе вычисления имитовставки используются

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

«НЕФРИТ». Процедура выработки имитовставки.

$$T = E_{K_1}(\gamma_{m+r} \oplus E_{K_1}(IV_2)),$$

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

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

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

«НЕФРИТ». Проверка имитовставки и расшифрование сообщения.

- К ассоциированным данным и шифртексту, полученным из канала связи, применяется процедура дополнения. Вычисляется значение имитовставки T_t согласно предыдущему слайду.
- Вычисленное значение имитовставки сравнивается с полученным из канала связи. Проверка считается успешно пройденной в случае, если указанные значения совпали. В противном случае проверка имитовставки считается *не пройденной*.
- Процедура расшифрования в режиме гаммирования шифртекста C, полученного из канала связи, может происходить независимо от процедуры вычисления имитовставки.

«НЕФРИТ». Проверка имитовставки и расшифрование сообщения.

- Полученный в результате расшифрования открытый текст P и ассоциированные данные подаются на выход режима *только в случае успешной проверки имитовставки.*
- В случае, если проверка оказалась *не пройденной* на выход режима поступает только *отрицательный результат проверки имитовставки* (например, сообщение об ошибке).
- Использование расшифрованного открытого текста P и ассоциированных данных A *не допустимо.*

«НЕФРИТ». Достоинства схемы.

- Возможность использования режима только для аутентификации.
- Возможность параллельной обработки блоков одного сообщения при шифровании и выработке/проверке имитовставки.
- Возможность шифрования без предварительного знания длины данных.
- Возможность выявления ложного сообщения без его расшифрования.
- Использование уникального (а не случайного) вектора инициализации упрощает реализацию схемы.

«НЕФРИТ». Особенности схемы.

- Использование двух разных ключей для шифрования и аутентификации.
- Возможность использования только базового блочного шифра с длиной блока 128 бит.
- Длина ассоциированных данных и открытого текста должна быть кратна 8 битам.
- Ограничение на суммарное количество блоков ассоциированных данных и открытого текста: $2^{32} - 1$.

«НЕФРИТ». Атака на ключ имитозащиты H, основанная на циклической структуре многочлена.

Пусть $H^{m-i+1} = H^{m-j+1}, i \neq j$. Тогда, меняя в исходном сообщении блоки C_i и C_j местами, получаем:

$$T' = E_{K_1}(\ldots \oplus C_i H^{m-j+1} \oplus \ldots \oplus C_j H^{m-i+1} \oplus E_{K_1}(IV_2)) =$$

$$= E_{K_1}(\ldots \oplus C_i H^{m-i+1} \oplus \ldots \oplus C_j H^{m-j+1} \oplus E_{K_1}(IV_2)) = T.$$

Если $H^{m-i+1} = H^{m-j+1}, i \neq j$, то $\exists\, \alpha = ord(H), 0 < \alpha < m$ и $H^{\alpha} = 1$ ($ord(H)$ – порядок элемента H в мультипликативной группе $GF(2^{128})$).

«НЕФРИТ». Атака на ключ имитозащиты H, основанная на циклической структуре многочлена.

Лемма

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

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

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

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

Фиксируем $k \in \{0, 1, \ldots, \frac{2^{128}}{m-1} - 1\}$ и строим многочлен относительно переменной H:

$$f_{mod}^{(k)}(H) = H \cdot (H \oplus g^{(k(m+1))}) \ldots (H \oplus g^{(m-2+k(m+1))}) =$$

$$= \sum_{j=1}^{m} b_j^{(k)} H^{m-j+1}, \quad b_j^{(k)} \in GF(2^n),\ j \in \{1, \ldots, m\}.$$

Построим последовательность шифртекстов:

$$C_1^{(k)} = C_1 \oplus b_1^{(k)}, \ldots, C_m^{(k)} = C_m \oplus b_m^{(k)}.$$

При подстановке этих шифртекстов в рассматриваемую схему имеем:

$$\gamma_m^{(k)} = \sum_{j=1}^{m} C_j^{(k)} H^{m-j+1} = \sum_{j=1}^{m} \left(C_j H^{m-j+1} \oplus b_j^{(k)} H^{m-j+1} \right).$$

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

Обозначим

$$\Omega^{(k)} = \{g^{(k(m-1))}, g^{(1+k(m-1))}, \ldots, g^{(m-2+k(m-1))}\}.$$

Пусть ключ имитозащиты $H \in \Omega^{(k)}$, тогда

$$\sum_{j=1}^{m} b_j^{(k)} H^{m-j+1} = 0,$$

и следовательно,

$$\gamma_m^{(k)} = \sum_{j=1}^{m} C_j H^{m-j+1} = \gamma_m \quad \Rightarrow \quad T^{(k)} = T.$$

А значит, произошло навязывание информации $(C_1^{(k)}, \ldots, C_m^{(k)}, T^{(k)})$.

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

Лемма

Существует алгоритм вскрытия ключа имитозащиты H, имеющий сложность

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

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

Дополнительно показано, что имитовставка T_t принимает не менее $u = \frac{2^t}{m}$ значений.

Вопросы?