AEAD режимы на основе полиномиальных хэш–функций: существующие решения, их криптографические свойства и возможные модификации

Кислякова Анастасия

ВМК МГУ им. М.В. Ломоносова

РусКрипто — 2018

22 марта 2018 г.

Содержание

Существущие походы

Классические решения

- Два независимых примитива и их реализации
- Два различных ключа
- Низкая скорость

Существущие походы

Классические решения

- Два независимых примитива и их реализации
- Два различных ключа
- Низкая скорость

AEAD режимы

Аутентифицированное шифрование [ISO/EIC 19772:2009] — это преобразование данных с помощью криптографического алгоритма для создания шифр–текста, который не может быть незаметно изменен третьим лицом.

Содержание

Полиномиальные хэш–функции

Общий вид

$$f_H(x_1||\ldots||x_m) = \sum_{i=0}^{m} x_i H^i$$

Полиномиальные хэш–функции

Общий вид

$$f_H(x_1||\dots||x_m) = \sum_{i=0}^{m} x_i H^i$$

Хэш–функция GHASH

$$\mathrm{GHASH}_H(x_1||\dots||x_m) = \bigoplus_{i=0}^{m} x_i \cdot H^{m-i}$$

Полиномиальные хэш–функции

Общий вид

$$f_H(x_1||\dots||x_m) = \sum_{i=0}^{m} x_i H^i$$

Хэш–функция GHASH

$$\mathrm{GHASH}_H(x_1||\dots||x_m) = \bigoplus_{i=0}^{m} x_i \cdot H^{m-i}$$

Хэш–функция СТБ 34.101.31-2011

$$T_H(x_1||\dots||x_m) = const \cdot H^m \oplus \bigoplus_{i=1}^{m} x_i \cdot H^{m+1-i}$$

Полиномиальные хэш–функции

Общий вид

$$f_H(x_1||\ldots||x_m) = \sum_{i=0}^{m} x_i H^i$$

Хэш–функция GHASH

$$\mathrm{GHASH}_H(x_1||\ldots||x_m) = \bigoplus_{i=0}^{m} x_i \cdot H^{m-i}$$

Хэш–функция СТБ 34.101.31-2011

$$T_H(x_1||\ldots||x_m) = const \cdot H^m \oplus \bigoplus_{i=1}^{m} x_i \cdot H^{m+1-i}$$

Хэш–функция режима PD

$$T_H(A_1||\ldots||A_h||C_1||\ldots||C_q) =$$
$$= \sum_{i=1}^{h} H_i \cdot A_i \oplus \sum_{j=1}^{q} H_{h+j} \cdot C_j \oplus H_{h+q+1} \cdot (|A| \mid\mid |C|)$$

Содержание

Известные атаки на GCM

- **N.Ferguson**
  "Authentication Weaknesses in GCM"
- **M.-J. O. Saarinen**
  "Cycling Attacks on GCM, GHASH and other polynomial MACs and hashes"
- **C.Cid, G.Procter**
  "On Weak Keys and Forgery Attacks against Polynomial–based MAC Schemes"
- **J. Mattsson, M.Westerlund**
  "Authentication Key Recovery on GCM"

Атаки на GCM

N.Ferguson “Authentication Weaknesses in GCM”

В $\mathcal{GF}(2^{128})$ $\exists$ матрицы M_c и M_s над $\mathcal{GF}(2)$ такие, что

$$\overline{c \cdot x} = M_c \overline{x} \text{ и } \overline{x^2} = M_s \overline{x} \qquad \forall x.$$

Для успешной подмены блока необходимо:

$$0 = \sum_{i=1}^{t} (C_{2^i} - C'_{2^i}) H^{2^i} = \sum_{j=2^i} D_j H^j = \sum_j M_{D_j}^j \overline{H} = A_D \overline{H},$$

где A_D — матрица размера 128×128 над $\mathcal{GF}(2)$, M_s — фиксированное значение, а элемент M_D — линейная комбинация соответствующих бит D_j. Следовательно, коэффициенты $M_{D_j}(M_s)^j$ — линейная комбинация бит D_j.

Атаки на GCM

M.-J. O. Saarinen «Cycling Attacks on GCM, GHASH and other polynomial MACs and hashes»

В GCM используется группа порядка $(2^{128} - 1 = 2^{2^7} - 1)$.

$$2^{2^n} - 1 = \prod_{i=1}^{n} 2^{2^{i-1}} + 1.$$

Значит, можно получить полное разложение порядка группы на простые множители:

$$\underbrace{3 * 5 * 17 * 257 * 641 * 65537 * 274177 * 6700417 * 67280421310721}_{9}$$

Таким образом, находим циклы длины $n = 1,\ 3,\ 5,\ 15,\ 17,\ 51, \ldots$ — порядки $2^9 = 512$ различных мультипликативных подгрупп исходной группы $\mathcal{GF}(2^{128})$.

Содержание

Полиномиальная функция хэширования с модульным умножением

Полиномиальная функция хэширования с модульным умножением

$$\mathrm{Hash}_H(x_1||\ldots||x_m) = \circledcirc_{i=0}^{m} x_i \cdot H^i,$$

где $\circledcirc \in \{\oplus, \boxplus\}$ и "$\cdot$" — умножение в целых числах по модулю 2^{128},

Полиномиальная функция хэширования с модульным умножением

Полиномиальная функция хэширования с модульным умножением

$$\mathrm{Hash}_H(x_1 || \dots || x_m) = \circledcirc_{i=0}^{m} x_i \cdot H^i,$$

где $\circledcirc \in \{\oplus, \boxplus\}$ и "$\cdot$" — умножение в целых числах по модулю 2^{128},

$\mathbb{Z}_{2^{128}} = \{0, \dots, 2^{128} - 1\}$ — кольцо вычетов по модулю 2^{128}.
$\mathbb{Z}_{2^n} = \{0, \dots, 2^n - 1\}$ — кольцо вычетов по модулю 2^n.

Полиномиальная функция хэширования с модульным умножением

Полиномиальная функция хэширования с модульным умножением

$$\mathrm{Hash}_H(x_1 || \ldots || x_m) = \circledcirc_{i=0}^{m} x_i \cdot H^i,$$

где $\circledcirc \in \{\oplus, \boxplus\}$ и "$\cdot$" — умножение в целых числах по модулю 2^{128},

$\mathbb{Z}_{2^{128}} = \{0, \ldots, 2^{128} - 1\}$ — кольцо вычетов по модулю 2^{128}.
$\mathbb{Z}_{2^n} = \{0, \ldots, 2^n - 1\}$ — кольцо вычетов по модулю 2^n.

$$(A + B)^2 = A^2 + 2AB + B^2 = A^2 + B^2 \iff 2AB \equiv 0 \pmod{2^n}$$

Некоторые определения

Порядок группы G — число элементов в этой группе. $|G| = n$.

Порядком элемента g группы G называется наименьшее число k такое, что $g^k \equiv 1$ в G, т.е. $\mathrm{ord}(g) = k$.

Индекс нильпотентности элемента a кольца $\mathbb{K}$ — наименьшее число k такое, что $a^k \equiv 0 \pmod{|\mathbb{K}|}$.

Элемент a называется **обратимым элементом** кольца $\mathbb{K}$, если для него существует обратный в кольце $\mathbb{K}$, т.е. $\exists b \in \mathbb{K}$, т.ч. $ab \equiv 1$ в $\mathbb{K}$.

Мультипликативная группа $\mathbb{K}^*$ кольца $\mathbb{K}$ — множество всех обратимых элементов этого кольца.

Структура кольца $\mathbb{Z}_{2^n}$

$$\mathbb{Z}_{2^n} = \mathbb{Z}^*_{2^n} \ \cup \ \mathbb{Z}^{even}_{2^n}$$

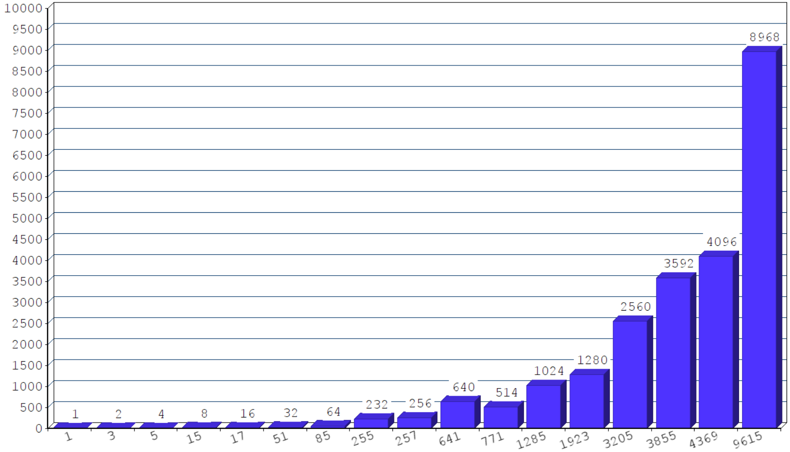
Кольцо $\mathbb{Z}_{2^n}$ будет содержать элементы следущих порядков:

Порядок/Индекс нильпотентности элемента	**Вероятность**
1	2^{1-n}
2	2^{2-n}
$2^k, \ \ k \in \{2, \dots, \ \lfloor \log_2 n \rfloor\}$	$(1 + 2^{-2})2^{k-n}$
$2^k, \ \ k \in \{\lfloor \log_2 n \rfloor + 1, \dots, n-2\}$	2^{k-n}
$m, \ \ m \in \{3, \dots n\}, \ \ m \neq 2^i$	2^{m-2-n}

Сравнение с GCM

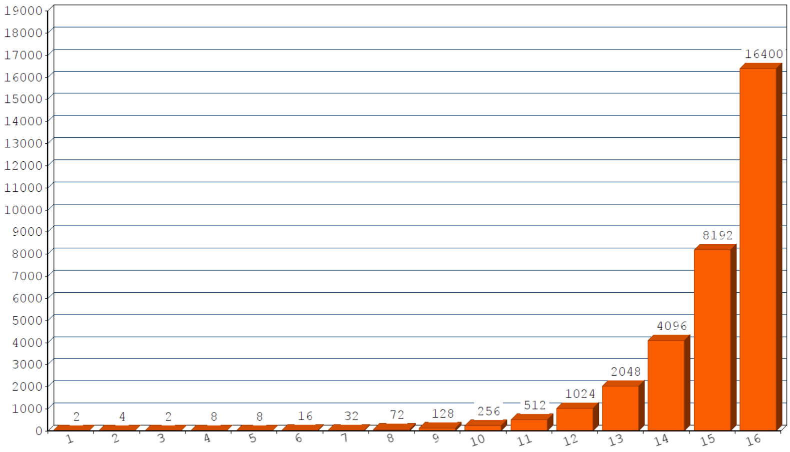
- **Число различных подгрупп**
  GCM — 512 подгрупп
  Хэш–функция с модульным умножением — 246 подгрупп
- **Максимальный порядок**
  GCM — 2^{128}
  Хэш–функция с модульным умножением — 2^{126}
- **Число элементов максимального порядка**
  GCM — $2^{126} + 2^{123} + \ldots$ элементов
  Хэш–функция с модульным умножением — 2^{126} элементов

Сравнение с GCM
Слабые ключи GCM



Сравнение с GCM

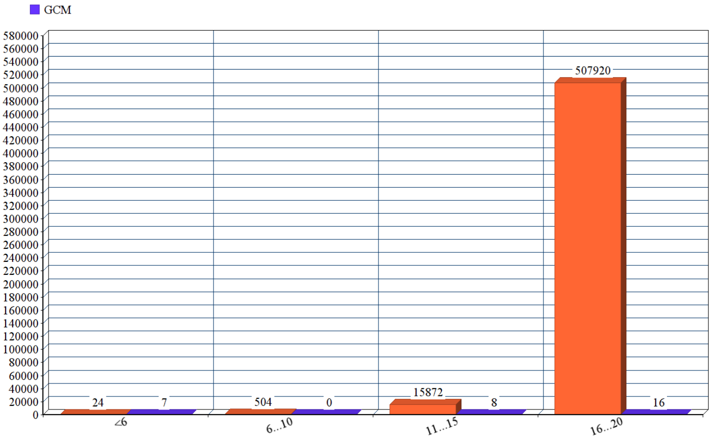
Слабые ключи хэш–функции с модульным умножением



Сравнение с GCM

Слабые ключи

Половина ключей хэш-функции с модульным умножением — слабые!



Спасибо за внимание!
Вопросы?

Алгоритм GCM (Galois Counter Mode)

Авторы: David A. McGrew, John Viega
Автор стандарта NIST: Morris Dworkin

Общий вид алгоритма шифрования

$E_K(P,\ A,\ IV) = C$

Общий вид алгоритма расшифрования

$D_K(C,\ A,\ IV) = P$ or FAIL

Ограничения на параметры:

- $\mathrm{len}(K) = 128$ бит;
- длина блока — 128 бит;
- $\mathrm{len}(P) \leq 2^{39} - 256$ бит;
- $\mathrm{len}(A) \leq 2^{64} - 1$ бит;
- $1 \leq \mathrm{len}(IV) \leq 2^{64} - 1$ бит, рекомендуемая длина: $\mathrm{len}(IV) =$ 96 бит;

Алгоритм GCM (Galois Counter Mode)

Универсальная хэш–функция GHASH

$$\mathrm{GHASH}_H(\mathrm{x}) = \bigoplus_{i=0}^{m} x_i \cdot H^{m-i},$$

Функция шифрования GCTR

$\mathrm{GCTR}_K(\mathrm{ICB}, \mathrm{x}) = \mathrm{Y}$

1. $CB_1 = ICB$
2. $CB_i = \mathrm{inc}_{32}(CB_{i-1}), \quad i = \overline{2, n}$
3. $Y_i = x_i \oplus \mathrm{CIPH}_K(CB_i), \quad i = \overline{1, n-1}$
4. $Y_n^* = X_n^* \oplus \mathrm{MSB}_{\mathrm{len}(X_n^*)}(\mathrm{CIPH}_K(CB_n))$
5. $Y = Y_1 || Y_2 || \dots || Y_n^*$.

где $H = \mathrm{CIPH}_K(0^{128})$ — ключ аутентификации,
K — ключ шифрования,
x — аутентифицируемое сообщение.

Алгоритм GCM (Galois Counter Mode)

Аутентифицированное шифрование GCM-AE

$\text{GCM-AE}_K(IV,\ P,\ A) = (C\ ,T)$

1. $H = \text{CIPH}_K(0^{128})$
2. $$\begin{cases} J_0 = IV||0^{31}||1, & \text{len}(IV) = 96, \\ \begin{cases} s = 128\lceil \text{len}(IV)/128 \rceil - \text{len}(IV), \\ J_0 = \mathrm{GHASH}_H(IV||0^{s+64}||[\text{len}(IV)]_{64}), \end{cases} & \text{len}(IV) \neq 96 \end{cases}$$
3. $C = \text{GCTR}_k(\text{inc}_{32}(J_0),\ P)$
4. $u = 128\lceil \text{len}(C)/128 \rceil - \text{len}(C)$
   $v = 128\lceil \text{len}(A)/128 \rceil - \text{len}(A)$
5. $S = \mathrm{GHASH}_H(A||0^v||C||0^u||[\text{len}(A)]_{64}||[\text{len}(\mathrm{C})]_{64})$
6. $T = \text{MSB}_t(\text{GCTR}_K(J_0, S))$

Алгоритм GCM (Galois Counter Mode)

Аутентифицированное расшифрование GCM-AD

$\text{GCM-AD}_K(IV,\ C,\ A,\ T) = P$ or FAIL

1. if ($\text{len}(IV)$, $\text{len}(A)$, $\text{len}(C)$ не соответствуют условиям) или ($\text{len}(T) \neq t$), то возвращаем *FAIL*.
2. $H = \text{CIPH}_K(0^{128})$
3. $J_0 = \begin{cases} IV \| 0^{31} \| 1, & \text{len}(IV) = 96 \\ \text{GHASH}_H(IV \| 0^{s+64} \| [\text{len}(IV)]_{64}), & \text{len}(IV) \neq 96 \\ \quad \text{где } s = 128\lceil \text{len}(IV)/128 \rceil - \text{len}(IV) & \end{cases}$
4. $P = \text{GCTR}_K(\text{inc}_{32}(J_0),\ C)$
5. $u = 128[\text{len}(C)/128] - \text{len}(C)$
   $v = 128[\text{len}(A)/128] - \text{len}(A)$
6. $S = \text{GHASH}_H(A \| 0^v \| C \| 0^u \| [\text{len}(A)]_{64} \| [\text{len}(C)]_{64})$
7. $T' = \text{MSB}_t(\text{GCTR}_K(J_0, S))$
8. Если $T = T'$, то возвращаем P, иначе — *FAIL*.

СТБ 34.101.31–2011

Используемые определения и операции

Синхропосылка — «Открытые входные данные криптографического алгоритма, которые обеспечивают уникальность результатов криптографического преобразования на фиксированном ключе.»

$\overline{u}$: а) для $u = u_1 u_2 \ldots u_8 \in \{0,\ 1\}^8$ число $2^7 u_1 + 2^6 u_2 + \cdots + u_8$;

б) для $u = u_1 || u_2 || \ldots || u_n,\ u_i \in \{0,\ 1\}^8,$ число $\overline{u}_1 + 2^8 \overline{u}_2 + \cdots + 2^{8(n-1)} \overline{u}_n$

$\langle U \rangle_{8n}$ — для целого U слово $u \in \{0,\ 1\}^{8n}$ такое, что $\overline{u} = U \pmod{2^{8n}}$

$u \boxplus v$ — для $u,\ v \in \{0,\ 1\}^{8n}$ слово $\langle \overline{u} + \overline{v} \rangle_{8n}$;

$u * v$ — для $u,\ v \in \{0,\ 1\}^{128}$ слово $w \in \{0,\ 1\}^{128}$ такое, что

$$w(x) = u(x)v(x) \pmod{x^{128} + x^7 + x^2 + x + 1}.$$

СТБ 34.101.31–2011

Шифрование и имитозащита данных

Ограничения на параметры

- Сообщение $X \in \{0,\ 1\}^*$, $\mathrm{len}(X) \leq 2^{64}$
- Ассоциированные данные $I \in \{0,\ 1\}^*$, $\mathrm{len}(I) \leq 2^{64}$
- Ключ $\theta \in \{0,\ 1\}^{256}$
- Синхропсылка $S \in \{0,\ 1\}^{128}$
- Тег аутентификации $T \in \{0,\ 1\}^{64}$.

СТБ 34.101.31–2011

Шифрование и имитозащита данных

Защита пары (X, I) на ключе θ при использовании синхропосылки S состоит в выполнении следующих шагов:

1 Установить $r \leftarrow F_\theta(S)$, $s \leftarrow r$.

2 Для $i = 1, 2, \ldots, n$ выполнить:

1) $s \leftarrow s \boxplus \langle 1 \rangle_{128}$;

2) $Y_i \leftarrow X_i \oplus L_{|X_i|}(F_\theta(s))$.

3 Установить $r \leftarrow F_\theta(r)$, $s \leftarrow \mathtt{B194BAC80A08F53B366D008E584A5DE4}_{16}$, где последнее присваиваемое значение определяется последовательными элементами первой строки таблицы 2.

4 Для $i = 1, 2, \ldots, m$ выполнить:

1) $s \leftarrow s \oplus (I_i \parallel 0^{128-|I_i|})$;

2) $s \leftarrow s * r$.

5 Для $i = 1, 2, \ldots, n$ выполнить:

1) $s \leftarrow s \oplus (Y_i \parallel 0^{128-|Y_i|})$;

2) $s \leftarrow s * r$.

6 Установить $s \leftarrow s \oplus (\langle |I| \rangle_{64} \parallel \langle |X| \rangle_{64})$;

7 Установить $s \leftarrow F_\theta(s * r)$.

8 Установить $T \leftarrow L_{64}(s)$.

9 Возвратить (Y, T).

СТБ 34.101.31–2011

Шифрование и имитозащита данных

Пункты 4-6 можно переписать в виде:

$$t = H \cdot r^p \oplus \bigoplus_{i=1}^{p} x_i \cdot r^{p+1-i},$$

где $x = (I||0^{128-|I_m|}||Y||0^{128-|Y_n|}||[len(I)]_{64}||[len(Y)]_{64})$
и $p = n + m + 1$ — число блоков длины 128 бит в строке x.

СТБ 34.101.31–2011

Шифрование и имитозащита данных

Пункты 4-6 можно переписать в виде:

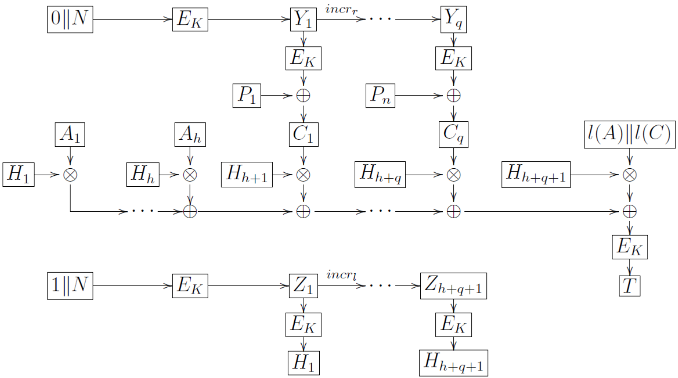
$$t = H \cdot r^p \oplus \bigoplus_{i=1}^{p} x_i \cdot r^{p+1-i},$$

где $x = (I||0^{128-|I_m|}||Y||0^{128-|Y_n|}||[len(I)]_{64}||[len(Y)]_{64})$
и $p = n + m + 1$ — число блоков длины 128 бит в строке x.

Сравним с функцией хеширования GCM:

$$\mathrm{GHASH}_H(\mathrm{x}) = \bigoplus_{i=0}^{m} x_i \cdot H^{m-i},$$

Parallel and Double (PD)



Таким образом:

$$T = E_K\left(\sum_{i=1}^{h} H_i \cdot A_i \oplus \sum_{j=1}^{q} H_{h+j} \cdot C_j \oplus H_{h+q+1} \cdot (|A| \mid\mid |C|)\right)$$

Конечное поле

Определение

Конечное множество $\mathbb{F}_q$ *из* q *элементов с введёнными на нём алгебраическими операциями сложения* $+$ *и умножения* $*$, *т. е.* $\forall a,\ b \in \mathbb{F}_q \quad (a+b) \in \mathbb{F}_q,\quad a * b \in \mathbb{F}_q$ *называется конечным полем* $\mathbb{F}_q$ *(или полем Галуа* $\mathcal{GF}(q)$*) порядка* q*, если выполнены следующие аксиомы:*

Конечное поле (продолжение)

Аксиомы:

1. Коммутативность сложения
2. Ассоциативность сложения
3. Существование нулевого элемента
4. Существование противоположного элемента
5. Коммутативность умножения
6. Ассоциативность умножения
7. Существование единичного элемента
8. Существование обратного элемента для ненулевых элементов
9. Дистрибутивность умножения относительно сложения

Атаки на GCM

N. Ferguson «Authentication Weaknesses in GCM»

Вычисление тега аутентификации можно записать следующим образом:

$$T = K_0 \oplus \sum_{i=1}^{n} C_i H^i,$$

где $K_0 = \mathrm{GCTR}_k(J_0,\ S)$, а $\sum_{i=1}^{n} C_i H^i = \mathrm{GHASH}_H(C)$.

Тогда для незаметной подмены блока C_i на C_i' необходимо $\sum_{i=0}^{n} C_i H^i = \sum_{i=0}^{n} C_i' H^i$ или равенство полинома ошибки нулю хотя бы для первых t бит:

$$\sum_{i=0}^{t} (C_i - C_i') H^i = 0.$$

Атаки на GCM

N. Ferguson «Authentication Weaknesses in GCM»

$$\sum_{i=0}^{t}(C_i - C_i')H^i = 0$$

Обозначим $E_i = C_i - C_i'$. Тогда полином ошибок можно записать как

$$\sum_{i=1}^{t} E_i H^i = 0.$$

Будем рассматривать только $D_i = E_{2^i} \neq 0$ такие, что

$$\sum_{i=1}^{t} D_i H_i = 0 = \overline{E}.$$

Атаки на GCM

N. Ferguson «Authentication Weaknesses in GCM»

Так как умножение на константу и возведение в квадрат в $\mathcal{GF}(2^{128})$ линейны:

$$\overline{E} = A_D\overline{H},$$

где A_D — матрица размера 128×128 над $\mathcal{GF}(2)$, коэффициенты которой — линейная комбинация бит D_i. Для установки нулевого значения в один бит необходимо 128 уравнений. Для n различных коэффициентов D_i есть $128 \cdot n$ свободных переменных и можно обнулить $n-1$ бит.

Атаки на GCM

M.-J. O. Saarinen «Cycling Attacks on GCM, GHASH and other polynomial MACs and hashes»

Если $\exists H^{m-i+1} = H^{m-j+1}, \ i \neq j$, можно получить коллизию на хэш–функцию, поменяв местами два соответствующих блока сообщения.
Период повтора степеней H равен $n = ord(H)$. То есть $\forall i, m$ можно поменять местами блоки X_i и $X_{i+n \cdot m}$.

Атаки на GCM

M.-J. O. Saarinen «Cycling Attacks on GCM, GHASH and other polynomial MACs and hashes»

В GCM используется группа порядка $(2^{128} - 1 = 2^{2^7} - 1)$.

$$2^{2^n} - 1 = \prod_{i=1}^{n} 2^{2^{i-1}} + 1.$$

Значит, можно получить полное разложение порядка группы на простые множители:

$$\underbrace{3 * 5 * 17 * 257 * 641 * 65537 * \ldots}_{9} \tag{1}$$

Таким образом, находим циклы длины $n = 1,\ 3,\ 5,\ 15,\ 17,\ 51, \ldots$ — порядки $2^9 = 512$ различных мультипликативных подгрупп исходной группы $\mathcal{GF}(2^{128})$.

Атаки на GCM

M.-J. O. Saarinen «Cycling Attacks on GCM, GHASH and other polynomial MACs and hashes»

Если $ord(H)|(i-j)$, то тег аутентификации будет верным, пока выполняется равенство:

$$X_i \cdot H^{m-i+1} \oplus X_j \cdot H^{m-j+1} = c.$$

Так как $ord(H)|(i-j)$, то $H^{m-i+1} = H^{m-j+1} = H_c$, следовательно, можно переписать условие в виде:

$$X_i + X_j = c \cdot H_c^{-1},$$

где $c \cdot H_c^{-1}$ — не меняется.

Идея атаки Saarinen и Cid & Procter

- Степени H будут повторяться с периодом $n = ord(H)$. Следовательно, $\forall i$ и m можно поменять местами блоки X_i и $X_{i+n\cdot m}$.
- Если $ord(H)|(i-j)$, то тег аутентификации будет верным, пока выполняется равенство:

$$X_i \cdot H^{m-i+1} \oplus X_j \cdot H^{m-j+1} = c.$$

Заметим, что порядок группы делит расстояние между переставленными элементами. Так как каждая подгруппа размера n имеет ровно n элементов, то:

- если НОД$(2^{128}-1,\ n) = n$, то вероятность успешной атаки будет $\geq \frac{n+1}{2^{128}}\ \forall H$;
- если НОД$(2^{128}-1,\ n) \neq n$, то причин ожидать вероятность $\neq \frac{1}{2^{128}}$ нет.

Список литературы

David A. McGrew, John Viega. *The Galois/Counter Mode of Operation (GCM).*
http://csrc.nist.gov/groups/ST/toolkit/BCM/documents/proposedmodes/gcm/gcm-spec.pdf

Государственный стандарт Республики Беларусь.
СТБ 34.101.31–2011. Информационные технологии и безопасность. Защита информации. Криптографические алгоритмы шифрования и контроля целостности. Минск, Госстандарт, 2011.

Vladislav Nozdrunov
Parallel and double block cipher mode of operation (PD–mode) for authenticated encryption.
Принят к опубликованию.

Niels Ferguson.
Authentication weaknesses in GCM. 2005
http://csrc.nist.gov/groups/ST/toolkit/BCM/documents/comments/CWC-GCM/Ferguson2.pdf

Markku-Juhani O. Saarinen.
Cycling Attacks on GCM, GHASH and Other Polynomial MACs and Hashes.
IACR Cryptology ePrint Archive, 2011, 202.

Gordon Procter, Carlos Cid.
On Weak Keys and Forgery Attacks against Polynomial-based MAC Schemes IACR Cryptology ePrint Archive, 2013, 144.

John Mattsson and Magnus Westerlund.
Authentication Key Recovery on Galois/Counter Mode (GCM).
IACR Cryptology ePrint Archive, 2015, 477.