УДК 512.817 : 681.3.06

КРИПТОАНАЛИЗ ДВУХКАСКАДНОЙ СХЕМЫ АУТЕНТИФИКАЦИИ С КОДАМИ ЭРМИТА

А.Ю. Иохов
(Харьковский университет Воздушных Сил)

Получены выражения вероятности навязывания для двухкаскадной схемы аутентификации с кодами Эрмита. Исследованы зависимости вероятности навязывания универсальных схем хеширования с РС кодами и кодами Эрмита от числа попыток навязывания и параметров кодовых схем

двухкаскадная схема аутентификации, код Эрмита, криптоанализ

Введение. Семейства хеш-функций на основе длинных алгеброгеометрических кодов (АГК) относятся к классам хешей с большим коэффициентом сжатия [1, 2]. Для разрешения противоречия между длиной хешируемых данных, вероятностью коллизии и сложностью вычислений предложена двухкаскадная конструкция на основе АГ кодов [3]. В [3, 4] рассмотрены вопросы практической реализации MAC кодов с кодами Рида-Соломона и Эрмита со сложностью, которая эквивалентна вычислительной процедуре Горнера. Требования к параметрам двухкаскадной конструкции MAC с РС кодами и кодами Эрмита определяются оценками их стойкости к основным криптоаналитическим атакам.

Задачей статьи является криптоанализ MAC кодов с РС кодами и кодами Эрмита. С этой целью в разделе 1 приводятся определения двухкаскадной схемы аутентификации и универсальных схем хеширования с РС кодами (RS) и Эрмита (HC). В разделе 2 выполнен криптоанализ двухкаскадной схемы аутентификации с кодами Эрмита.

1. Определения двухкаскадной схемы аутентификации с РС кодами и кодами Эрмита. Двухкаскадная схема аутентификации предложена в [3]. Применение каскадной схемы хеширования на основе алгеброгеометрических кодов для универсальных классов хеш-функций обеспечивает наилучшие соотношения между размером хеш-значений, длинной данных, и вероятностью коллизии при вычислениях в конечных полях, а также минимизирует затраты по ключевым данным и затратам на вычисления. Соответствующее определение имеет следующее представление.

Определение 1 [3]. Пусть F_q – конечное поле и M – сообщение, $|M| \le q$ и $M = M_1 || M_2$. Алгоритм вычисления хеш-кода в каскадной конструкции определяется выражением

$$Ch_q(M) = HCh_q\,(RSh_q\,(M_1)\,||\,M_2\,), \qquad (1)$$

где $|M_1| \le \sqrt{q} + 1$; RSh_q, HCh_q – универсальные схемы хеширования на основе кодов Рида-Соломона и Эрмита.

Следующая теорема описывает коллизионные свойства $Ch_q(M)$ конструкции.

Теорема 1 [3]. Пусть F_q – конечное поле; $M = M_1||M_2$; $|M| \le q$; $|M_1| \le \sqrt{q} + 1$; $0 < k \le q + \sqrt{q}$. Тогда $Ch_q(M)$ определяет универсальное семейство хеш-функций $\varepsilon - U(q^2\sqrt{q}\,; q^k, q)$; $\varepsilon = \max(\varepsilon_{RS}, \varepsilon_{HC}) + 1 / |q\sqrt{q}$; ε_{RS}, ε_{HC} – вероятности коллизий для RSh_q и HCh_q хеширования соответственно.

Двухкаскадная схема включает последовательное включение универсальных схем хеширования с РС кодами (RS) и Эрмита (HC).

RSh_q семейство на основе РС кодов представляется следующей теоремой.

Теорема 2 [1]. Пусть q – степень простого числа и $1 \le k \le q$, тогда существует $\dfrac{k-1}{q}$ – U (q; q^k, q) хеш-семейство RSh_q.

РС коды имеют параметры

$$[q, k, q - k + 1]_q \qquad (2)$$

и вычисление МАС кодов определяется выражением $h_x(m) = \sum_{i=0}^{k} m_i x^i$, где $m = (m_1, m_2, \ldots, m_k)$ – сообщение; x – значение ключа, $x, m_i \in GF(q)$.

Эрмитовы коды (HC) определены над расширенным полем F_q, $q = p^2$ и имеют асимптотические параметры

$$[q\sqrt{q}\,, k, q\sqrt{q} - k + 1 - g]_q\,, \qquad (3)$$

где род кривой $g = \sqrt{q}\,(\sqrt{q} - 1) / 2$.

В [4] получено уточнение для кодового расстояния кода Эрмита.

Утверждение 1 [4]. Пусть $k \le g$. Уточненная граница кодового расстояние HC кода [n,k,d] определяется выражением

$$d = n - [(s - t - 1)\sqrt{q} + t(\sqrt{q} + 1)], \qquad (4)$$

где $t = k - s(s-1)/2 - 1$; $s = \lceil \sqrt{2k + 1/4} - 0{,}5 \rceil$; $\lceil x \rceil$ – округление числа x до большего целого.

При хешировании с кодами Эрмита (HCh_q), вычисление МАС кодов определяется выражением

$$h_{(x,y)}(m) = \sum_{i=0}^{k} m_i w_i(x, y), \quad (5)$$

где $m = (m_1, m_2, \dots, m_k)$ – сообщение; $m_i \in F_q$; $w_i(x, y)$ – значение рациональной функция на кривой Эрмита в точке (x, y) с порядком полюса u_i, $u_0 = 0 < u_1 < u_2 < \dots < u_k$; (x, y) – точка кривой Эрмита, значение которой определяют ключевые данные $x, y \in F_q$.

На основе кодов Эрмита, получим универсальное семейство хеш-функций HCh_q.

Теорема 3 [4]. Пусть F_q, $q = p^2$ – расширенное конечное поле и $1 \le k \le q\sqrt{q}$, тогда существует $\varepsilon -$ $U(q\sqrt{q}; q^k, q)$ семейство хеш-функций HCh_q, где

$$\varepsilon = [(s - t - 1)\sqrt{q} + t(\sqrt{q} + 1)] / (q\sqrt{q}), \quad 1 \le k \le g; \quad (6)$$

$$\varepsilon = \frac{1}{\sqrt{q}}\left(\frac{k-1}{q} + 1 - \frac{1}{\sqrt{q}}\right), \; k > g, \quad (7)$$

где $t = k - s(s - 1) / 2 - 1$; $s = \lceil \sqrt{2k + 1/4} - 0{,}5 \rceil$; $\lceil x \rceil$ – округление числа x до большего целого; g – род кривой.

Выражения для оценки вероятностей успеха прямой атаки на универсальные семейства хеш-функций с кодовыми схемами представлены в [5]. Ниже рассмотрим криптоанализ двухкаскадной схемы аутентификации.

2. Криптоанализ двухкаскадной схемы аутентификации с Эрмитовыми кодами. Коллизионная стойкость двухкаскадной схемы аутентификации зависит от длины хешируемых данных, определяется используемым каскадом хеширования и, как следствие, криптостойкость будет определяется криптостойкостью последнего каскада вычисления хеш значения. Выражения для вероятности успеха прямой атаки на RSh_q и HCh_q схемы хеширования с учетом приведенных оценок кодовых расстояний и результатов оценок для вероятности навязывания для универсальных классов хеш-функций с кодовыми схемами определяются следующим предложением.

Предложение 1.

1. Для MAC кодов на основе RSh_q универсального хеш-семейства $(k-1)/q - U(q;q^k,q)$, успех атаки угадывания MAC кода с помощью ключа определяется следующими соотношениями:

– при однократной попытке $P_{укRS} \le (k - 1) / q$;

– при t кратной попытке

$$P_{укRS}(t) \le \sum_{i=1}^{t} C^i_t C^i_k C^i_{q-k+1} / (C^i_q C^{t-i}_{q-i}); \quad (8)$$

– среднее число попыток прямой атаки

$$N_{RS} = \frac{k-1}{q} \sum_{i=1}^{q-k+2} iC^{i-1}_{q-k+1} / C^{i-1}_{q-1}. \quad (9)$$

2. Для МАС кодов на основе HCh_q универсального хеш-семейства $\varepsilon - U(q\sqrt{q}\,; q^k, q)$, где

$$\varepsilon = [(s - t - 1)\sqrt{q} + t(\sqrt{q} + 1)] / (q\sqrt{q}), \text{ при } 1 \le k \le g$$

и

$$\varepsilon = \frac{1}{\sqrt{q}}\left(\frac{k-1}{q} + 1 - \frac{1}{\sqrt{q}}\right), \text{ при } k > g;$$

$t = k - s(s - 1) / 2 - 1$; $s = \lceil \sqrt{2k + 1/4} - 0{,}5 \rceil$; $\lceil x \rceil$ – округление числа x до большего целого, g – род кривой, успех атаки угадывания МАС кода с помощью ключа определяется выражениями:

– при однократной попытке

$$P_{укНС} \le [(s - t - 1)\sqrt{q} + t(\sqrt{q} + 1)] / q\sqrt{q}, \quad 1 \le k \le g; \quad (10)$$

$$P_{укНС} \le (k - 1 + g) / q\sqrt{q}, \quad k > g; \quad (11)$$

– при t-кратной попытке

$$P_{укНС}(t) \le \sum_{i=1}^{t} C^i_t C^i_{(s-t-1)\sqrt{q}+t(\sqrt{q}+1)} C^i_{q\sqrt{q}-[(s-t-1)\sqrt{q}+t(\sqrt{q}+1)]} / (C^i_{q\sqrt{q}} C^{t-i}_{q\sqrt{q}-i}), \; k \le g; \quad (12)$$

$$P_{укНС}(t) \le \sum_{i=1}^{t} C^i_t C^i_{k-1+g} C^i_{q\sqrt{q}-k+1-g} / (C^i_{q\sqrt{q}} C^{t-i}_{q\sqrt{q}-i}), \; k > g; \quad (13)$$

– среднее число попыток прямой атаки

$$N_{НС} = \frac{(s-t-1)\sqrt{q} + t(\sqrt{q}+1)}{q\sqrt{q}};$$

$$\sum_{i=1}^{q\sqrt{q}+1-[(s-t-1)\sqrt{q}+t(\sqrt{q}+1)]} iC^{i-1}_{q\sqrt{q}-[(s-t-1)\sqrt{q}+t(\sqrt{q}+1)]} / C^{i-1}_{q\sqrt{q}-1}, \; k \le g; \quad (14)$$

$$N_{НС} = \frac{k-1+g}{q\sqrt{q}} \sum_{i=1}^{q\sqrt{q}-k+2-g} i\, C^{i-1}_{q\sqrt{q}-k+1-g} / C^{i-1}_{q\sqrt{q}-1}, \; k > g. \quad (15)$$

На рис. 1 представлены графики вероятности успешного угадывания МАС по ключу в зависимости от длины хешируемых данных и кратности попыток угадывания.

Анализ графиков показывает, что МАС с использованием HCh_q хеширования имеет большую защищенность от прямой атаки, чем RSh_q схема и с увеличением кратности попыток успех атаки возрастает. Из результатов табл. 1 следует, что зависимость вероятности навязывания с

угадыванием по ключу от числа попыток является почти линейной для практических длин данных.

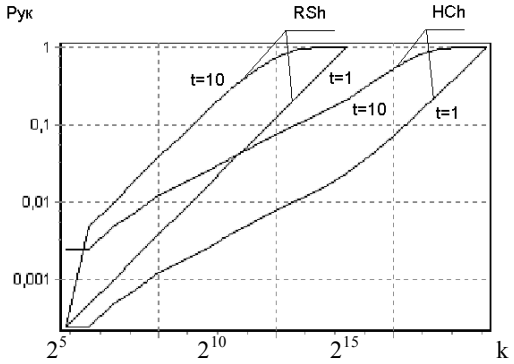

Рис. 1. Зависимости вероятности успешного угадывания MAC кода по ключу от длины хешируемых данных k и кратности попыток угадывания t, при q = 4096

Таблица 1

Значения вероятности угадывания MAC кода
по ключу для HCh_q хеширования при q = 4096

Lg k	t = 1	t = 10	t = 100
0	0,000244	0,002438	0,024125
1	0,000247	0,002476	0,024498
2	0,000492	0,004910	0,048038
3	0,000740	0,007376	0,071371
4	0,001224	0,012178	0,115338
5	0,001724	0,017109	0,158530
6	0,002475	0,024483	0,219583
7	0,003692	0,036319	0,309276
8	0,005382	0,052541	0,417140
9	0,007629	0,073728	0,535135
10	0,010871	0,103552	0,664907
11	0,015502	0,144651	0,790437
12	0,023315	0,210155	0,905542
13	0,038940	0,327797	0,981176
14	0,070190	0,517014	0,999310
15	0,132690	0,759159	0,999999
16	0,257690	0,949204	0,999999
17	0,507690	0,999163	1
18	0,999996	0,999996	0,999996

Успех прямой атаки на двухкаскадную схему вычисления MAC кода с угадыванием ключа определяется следующей теоремой.

Теорема 4. Пусть F_q – конечное поле и M – сообщение, и $M = M_1 || M_2$. Прямая атака с угадыванием ключа на MAC код с каскадным хешированием $Ch_q(M)$ эквивалентна прямой атаке на первый RSh_q каскад при $|M| \le \sqrt{q}$, и эквивалентна атаке на второй каскад с HCh_q хешированием, в случае если $|M| > \sqrt{q}$.

При вычислении MAC кода подключается один или два каскада хеширования в зависимости от длины хешируемых данных. Таким образом, первый результат теоремы следует сразу по определению. При $|M| > \sqrt{q}$ MAC код вычисляется последовательно в RSh_q схеме и затем в HCh_q схеме. Событие успешного угадывания является сложной группой событий и его вероятность определяется как

$$P_{укCh} = P_{укRS}\, P(укHC / укRS) + P_{нукRS}\, P(укHC / нукRS), \qquad (16)$$

где P(укHC / укRS) – вероятность успешного угадывания MAC кода по ключу в HCh_q каскаде, при условии, что в RSh_q каскаде произошло угадывание MAC результата; P(укHC / нукRS) – вероятность успешного угадывания MAC кода по ключу в HCh_q каскаде, при условии, что в RSh_q каскаде не был угадан MAC результат; $P_{нукRS}$ – вероятность того что не будет угадан MAC код по ключу в RSh_q каскаде.

Условная вероятность P(укHC/укRS) при однократной попытке угадывания ключа определяется вероятностью успеха для HCh_q схемы, выражением (10), (11). Условная вероятность P(укHC / нукRS) равна вероятности коллизии ε (6), (7) и как следует из сравнения соотношений (6) и (10), (7) и (11), равна P(укHC / укRS). Отсюда можно заключить, что вероятности являются безусловными и

$$P(укHC / укRS) = P(укHC / нукRS) = P_{укHC}.$$

При атаке с t попытками угадывания ключа формируются t различных ключа и вычисляются MAC значения. Используем оптимальную стратегию, когда ключи не повторяются на каждом каскаде хеширования. Мощность множества ключей будет определяться как $n_{RS} + n_{HC} = q + q\sqrt{q}$. Так как ключи не повторяются, тогда с каждой попыткой подделки размер множества ключей будет на единицу уменьшаться в каждом каскаде и вероятность успеха угадывания MAC кода будет определяться выражениями (12), (13) для $P_{укHC}(t)$, не зависимо от результата угадывания в RSh_q каскаде. Так как $P_{укRS} + P_{нукRS} = 1$ из выражения (16) получим $P_{укCh} = P_{укHC}$.

Из полученных результатов следует, что сложность прямой атаки до первого угадывания MAC кода путем подбора ключей определяется сложностью атак для схем RSh_q или HCh_q (9), (14), (15).

Атака с угадыванием MAC значений на алгоритм MAC кодов не зависит от свойств кодовых конструкций и полученные оценки могут быть перенесены непосредственно на каскадную схему.

Предложение 2. Для MAC кодов с каскадным хешированием Ch_q $\varepsilon - U(q^2\sqrt{q}; q^k, q)$, $\varepsilon = \max(\varepsilon_{RS}, \varepsilon_{HC}) + 1 / |q\sqrt{q}|$, успех атаки с угадыванием MAC значений определяется соотношениями:

– при однократной попытке $P_{yMACCh} = q^{-1}$;

– при t кратной попытке $P_{yMACCh} = tq^{-1}$;

– среднее число попыток прямой атаки $N_{MACCh} = (q+1) / 2$.

Выводы. Получены выражения для оценки сложности прямой атаки на MAC коды с универсальным хешированием для двухкаскадной схемы с РС кодами и кодами Эрмита.

Анализ оценок для вероятности навязывания показывает, что при универсальном хешировании с кодами Эрмита обеспечивается меньшая вероятность подделки MAC кода по сравнению с РС кодированием. Стойкость двухкаскадной схемы аутентификации при больших длинах данных определяется характеристиками каскада с универсальным хеш классом на основе кодов Эрмита.

ЛИТЕРАТУРА

1. *Bierbrauer J., Johansson T., Kabatianskii G., Smeets B. On families of hash functions via geometric codes and concatenation // Advances in Cryptology-CRYPTO '93 Proceedings, Springer-Verlag. – 1994. – P. 331 – 342.*
2. *Халимов Г.З., Кузнецов А.А. Аутентификация с применением алгеброгеометрических кодов // Радиотехника. Всеукр. межвед. науч.-техн. сб. – 2001. – Вып. 120. – С. 103 – 109.*
3. *Халимов Г.З., Иохов А.Ю. Двухкаскадное универсальное хеширование с использованием АГ кодов // Восточно-европейский журнал передовых технологий. – 2005. – Вып. 2(14). – С. 57 – 61.*
4. *Халимов Г.З., Иохов А.Ю. Аутентификация с применением Эрмитовых кодов. // Вестник национального технического университета «ХПИ». – Х.: НТУ «ХПИ». – 2005. – Вып. 47. – С. 118 – 122.*
5. *Халимов Г.З., Иохов А.Ю., Северинов А.В. Криптоанализ прямой атаки на универсальное семейство хеш-функций с алгебраическим кодированием // Системи обробки інформації. – Х.: ХВУ. – 2004. – Вип. 12(40). – С. 238 – 247.*

Поступила 31.01.2005

Рецензент: доктор физико-математических наук, профессор С.В. Смеляков, Харьковский университет Воздушных Сил.