УДК 621.391

ТЕОРЕТИКО-КОДОВЫЕ СХЕМЫ НА ЭЛЛИПТИЧЕСКИХ КОДАХ

В.И. Грабчак
Научный центр боевого применения РВиА Сумского государственного университета, г. Сумы

Рассматриваются теоретико-кодовые схемы, построенные с использованием эллиптических кодов. Предложены схемы, позволяющие эффективно противостоять "лобовым" атакам злоумышленника на коротких длинах кодов. Проведена сравнительная оценка объема ключевых данных для теоретико-кодовых схем, построенных по одной и двум эллиптическим кривым.

ВВЕДЕНИЕ

Одним из перспективных направлений в развитии теории помехоустойчивого кодирования являются методы алгебро-геометрического кодирования [1,2]. Недвоичные алгебраические блоковые коды, построенные по алгебраическим кривым (алгебро-геометрические коды), обладают хорошими асимптотическими свойствами [3]. Перспективным направлением в развитии методов защиты информации являются интегрированные механизмы, позволяющие совместить помехоустойчивое кодирование с маскировкой передаваемых данных под случайную последовательность, так называемые теоретико-кодовые схемы (ТКС)[4].

Известные ТКС обладают существенным недостатком – большим объемом ключевых данных [5-6]. Одним из перспективных направлений развития ТКС, направленных на повышение стойкости и снижение длины ключа, является использование алгебро-геометрических кодов. Применение кодов, построенных по алгебраическим кривым (алгебро-геометрических кодов), для формирования ТКС позволит получить дополнительный параметр маскировки кода – вид алгебраической кривой [7].

Предложенная в [8] конструкция позволяет снизить объем ключа, но стойкость к взлому такой схемы на коротких длинах кода, которые практически реализуются в системах передачи данных, считается недостаточной.

Актуальной научно-технической задачей является разработка и исследование ТКС, построенных на эллиптических кодах, позволяющих эффективно противостоять "лобовым" атакам противника на небольших длинах кода.

ОСНОВНАЯ ЧАСТЬ

ТКС на эллиптических кодах, заданных в проективном пространстве P^2. Эллиптической кривой в аффинном пространстве A^3 над полем $GF(2^m)$ называется гладкая кривая, заданная уравнением

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6\,, \qquad (1)$$

или в проективном пространстве P^2, заданная однородным уравнением

$$y^2z + a_1xyz + a_3yz^2 = x^3 + a_2x^2z + a_4xz + a_6z^3\,, \qquad (2)$$

где $a_i \in GF(2^m)$, род кривой $g = 1$.

Эллиптический (n, k, d) код над $GF(2^m)$ в P^2 задается с помощью генераторной матрицы G вида

$$G = \begin{pmatrix} F_0\left(p_0\left(x_0, x_1, x_2\right)\right) & F_0\left(p_1\left(x_0, x_1, x_2\right)\right) & \dots & F_0\left(p_{n-1}\left(x_0, x_1, x_2\right)\right) \\ F_1\left(p_0\left(x_0, x_1, x_2\right)\right) & F_1\left(p_1\left(x_0, x_1, x_2\right)\right) & \dots & F_1\left(p_{n-1}\left(x_0, x_1, x_2\right)\right) \\ \dots & \dots & \dots & \dots \\ F_m\left(p_0\left(x_0, x_1, x_2\right)\right) & F_m\left(p_1\left(x_0, x_1, x_2\right)\right) & \dots & F_N\left(p_{n-1}\left(x_0, x_1, x_2\right)\right) \end{pmatrix} \quad (3)$$

и размерности $M \times n$, $M = \alpha$, $\alpha = 3 \cdot degF$.

Каждый символ генераторной матрицы формируется путем вычисления значения генераторной функции F_j в точке p_i эллиптической кривой. Число M генераторных функций определяется конструктивными характеристиками эллиптического (n, k, d) кода. Вид функций F_j определяется степенью α отображения точек кривой и, следовательно, так же задается конструктивными параметрами кода.

Таким образом, если заданы конструктивные (n, k, d) характеристики эллиптического кода, то уникальность генераторной матрицы определяет набор точек $p_0, p_1, \dots, p_{n-1}$, в которых вычисляются значения генераторных функций.

Утверждение 1 Конкретный набор точек из пространства P^2 однозначно задается видом многочлена кривой, т.е. набором коэффициентов $a_1 \dots a_6$, где $\forall a_i \in GF(2^m)$.

Следствие. Объем секретного ключа (в битах) в ТКС, построенной по эллиптическим (n, k, d) кодам над $GF(2^m)$, которые задаются генераторной матрицей (3), определяется выражением [8]:

$$l_K = 5 \cdot m_i . \quad (4)$$

Выражение (4) позволяет оценить объем секретных ключевых данных в ТКС, построенной по эллиптическим кодам.

В табл. 1 представлены данные, характеризующие зависимости объемов ключевых данных от размерности поля $GF(2^m)$, над которым строится эллиптический код.

Таблица 1

$GF(2^m)$	2^4	2^8	2^{10}	2^{12}	2^{14}	2^{16}	2^{18}	2^{20}
l_K	20	40	50	60	70	80	90	100

Очевидно, что предложенный способ построения ТКС на эллиптических кодах позволяет существенно снизить объемы ключевой информации по сравнению с классическими схемами построения ТКС [5, 6].

В то же время потенциально стойкими считаются схемы с $l_K > 100$ бит [9]. Как следует из приведенных в табл. 1 значений, для построения такой теоретико-кодовой схемы необходимо использовать эллиптические коды с длиной кодового слова $> 2^{20}$ бит, что на сегодняшний день в системах передачи данных практически не реализуемо.

ТКС на эллиптических кодах, заданных в проективном пространстве P^3. Зафиксируем гладкую проективную алгебраическую кривую X в проективном пространстве P^3 над полем $GF(2^m)$ как совокупность

решений двух однородных неприводимых алгебраических уравнений от 4 переменных с коэффициентами из $GF(2^m)$:

$$\begin{cases} f_1(x_0, x_1, x_2, x_3) = 0, \\ f_2(x_0, x_1, x_2, x_3) = 0. \end{cases} \quad (5)$$

В качестве уравнений (5) используем уравнения эллиптической кривой (2).

Эллиптический (n, k, d) код над $GF(2^m)$ в пространстве P^3 задается с помощью генераторной матрицы G вида

$$G = \begin{pmatrix} F_0(p_0(x_0, x_1, x_2, x_3)) & F_0(p_1(x_0, x_1, x_2, x_3)) & \dots & F_0(p_{n-1}(x_0, x_1, x_2, x_3)) \\ F_1(p_0(x_0, x_1, x_2, x_3)) & F_1(p_1(x_0, x_1, x_2, x_3)) & \dots & F_1(p_{n-1}(x_0, x_1, x_2, x_3)) \\ \dots & \dots & \dots & \dots \\ F_m(p_0(x_0, x_1, x_2, x_3)) & F_m(p_1(x_0, x_1, x_2, x_3)) & \dots & F_N(p_{n-1}(x_0, x_1, x_2, x_3)) \end{pmatrix}. \quad (6)$$

Утверждение 2 Конкретный набор точек из пространства P^3 однозначно задается видом двух многочленов эллиптической кривой, т.е. набором коэффициентов $a_1 \dots a_6$, где $\forall a_i \in GF(2^m)$ первой и второй кривых.

Следствие Объем секретного ключа (в битах) в ТКС, построенной по эллиптическим (n, k, d) кодам над $GF(2^m)$, которые задаются генераторной матрицей (6), определяется выражением

$$l_K = 5 \cdot \sum_{i=1}^{2} m_i . \quad (7)$$

В табл. 2 представлены данные, характеризующие зависимости объемов ключевых данных от размерности поля $GF(2^m)$ для ТКС, построенной с использованием двух эллиптических кривых.

Таблица 2

$GF(2^m)$	2^4	2^8	2^{10}	2^{12}	2^{14}	2^{16}	2^{18}	2^{20}
l_{K^*}	40	80	100	120	140	160	180	200

На рис. 1 приведены зависимости объема ключевых данных соответственно для ТКС, построенной по одной (l_K) и двум (l_{K^*}) эллиптическим кривым.

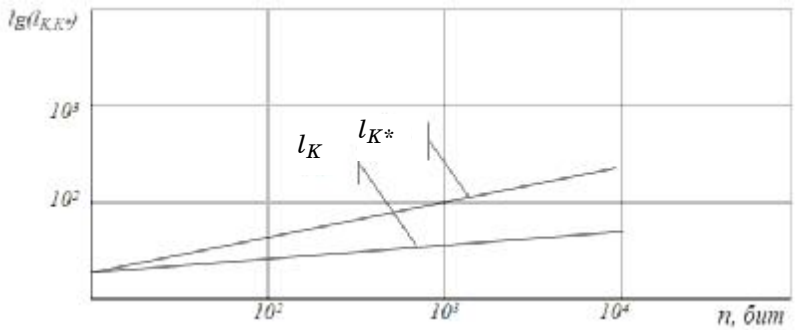

Рисунок 1 – Зависимости объема ключевых данных от длины кодограммы

Как видно из приведенных зависимостей, маскирование эллиптического кода путем сокрытия коэффициентов многочлена кривой в теоретико-кодовых схемах позволяет эффективно противодействовать "лобовой" атаке только для $n > 10^6$, что для практических приложений не реализуемо. Напротив, маскирование эллиптического кода путем сокрытия коэффициентов двух многочленов кривой в теоретико-кодовых схемах позволяют уже для $n > 1000$ эффективно противостоять "лобовым" атакам злоумышленника.

Таким образом, предложенные ТКС целесообразно использовать для защиты формализованных кодограмм в современных телекоммуникационных системах.

ВЫВОДЫ

Теоретико-кодовые схемы на эллиптических кодах позволяют значительно сократить объем ключевых данных по сравнению с классическими схемами их построения. Однако стойкость к взлому такой схемы на коротких длинах кода считается недостаточной.

В результате проведенных исследований предложены схемы, которые отличаются от известных применением в качестве служебных данных параметров двух эллиптических кривых, что позволяет эффективно защищать короткие формализованные кодограммы и обеспечить защиту данных от "лобовых" атак злоумышленника.

SUMMARY

THEORETICAL-CODE CHARTS ON ELLIPTIC KODAS

Grabchak V.I.

Theoretical-code charts built with the use of elliptic kodas are examined. Charts which allow effectively to resist the "frontal" attacks of opponent on short lengths of kodas are offered. The comparative estimation of volume of key information for theoretical-code charts, built on one and two elliptic curves, is conducted.

СПИСОК ЛИТЕРАТУРЫ

1. Гоппа В.Д. Коды и информация // Успехи математических наук. – 1984. –Т.30, Вып. 1(235). – С. 77-120.
2. Науменко М.І., Стасєв Ю.В., Кузнецов О.О. Теоретичні основи та методи побудови алгебраїчних блокових кодів: Монографія. – Харків.: ХУ ПС, 2005. – 267 с.
3. Цфасман М.А.Коды Гоппы, лежащие выше границы Варшамова - Гилберта //Проблемы передачи информации. – 1982. – №3 – С. 3-6.
4. Сидельников В.М. Криптография и теория кодирования // Материалы конференции «Московский университет и развитие криптографии в России». – МГУ, 2002. – 22 с.
5. R.J. McEliece. A Public-Key Criptosystem Based on Algebraic Theory. // DGN Progres Report 42-44, Jet Propulsi on Lab. Pasadena, CA. January – February, 1978. – P. 114-116.
6. H. Niederreiter. Knapsack-Type Cryptosystems and Algebraic Coding Theory. // Probl. Control and Inform. Theoty. – 1986. – V.15. – P. 19-34.
7. Кузнецов А.А., Евсеев С.П. Разработка теоретико-кодовых схем с использованием эллиптических кодов // Системи обробки інформації. – Харків: ХВУ. - 2004 - Вип.5. - С.127-132.
8. Стасев Ю.В., Кузнецов А.А., Евсеев С.П., Лисенко В.Н., Грабчак В.И. Теоретико-кодовые схемы с небольшим объемом ключа // Збірник наукових праць. – Севастополь: Севастопольський ВМІ ім. Нахімова. – 2005. – Вип. 2(8). – С. 110-114.
9. Шнайер Б. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си. – М.: Издательство ТРИУМФ, 2003. – 816 с.

Грабчак В.И., *канд. техн. наук*

Поступила в редакцию 11 апреля 2008 г.