

## СИММЕТРИЧНЫЕ ТЕОРЕТИКО-КODOVЫЕ СХЕМЫ НА АЛГЕБРОГЕОМЕТРИЧЕСКИХ КОДАХ

А.А. Кузнецов

(Харьковский университет Воздушных Сил)

*Исследуются симметричные криптосистемы на алгебраических блоковых кодах (теоретико-кодовые схемы) стойкость которых основана на трудноразрешимой задаче декодирования случайного кода. Предложены симметричные криптосхемы на алгеброгеометрических кодах.*

***криптосистема, алгеброгеометрический код, теоретико-кодовая схема***

**Постановка проблемы в общем виде, анализ литературы.** Перспективным направлением в развитии методов криптографической защиты информации является исследование и разработка криптосистем на алгебраических блоковых кодах (теоретико-кодовых схем) [1 – 5]. В работах [2, 3] показано, что их применение позволяет интегрировано (в один прием) обеспечивать безопасность информации и эффективно бороться с возникающими ошибками. В тоже время, как показано в [4, 5] существующие криптосистемы на обобщенных кодах Рида-Соломона могут быть взломаны алгоритмом полиномиальной сложности. Перспективным направлением является использование алгеброгеометрических кодов для построения криптографически стойких теоретико-кодовых схем.

**Симметричные криптосистемы на алгебраических блоковых кодах.** Симметричные криптосистемы на алгебраических блоковых кодах впервые предложены в работе Рао и Нама [1]. В их основе лежит использование теоретико-сложностной проблемы декодирования случайного кода: код с быстрым алгоритмом декодирования (полиномиальной сложности) маскируется под произвольный (случайный) линейный код, декодирование которого представляется как вычислительно сложная задача. Шифрованная информация (криптограмма) в виде вектора  $c^*$  длины  $n$  формируется как

$$c^* = I \cdot G + e, \quad (1)$$

где вектор  $c = I \cdot G$  принадлежит  $(n, k, d)$  коду с порождающей матрицей  $G$ ;  $I$  –  $k$ -разрядный информационный вектор; вектор  $e$  – секретный (случайный) вектор ошибок.

Параметры криптосистемы над  $GF(2^m)$  определяются выражениями:

– размерность секретного ключа (в битах)

$$l_{K+} = k \cdot n \cdot m; \quad (2)$$

– размерность информационного вектора (в битах)

$$l_I = k \cdot m; \quad (3)$$

– размерность криптограммы (в битах)

$$l_S = n \cdot m; \quad (4)$$

– относительная скорость передачи

$$R = l_I / l_S = k/n. \quad (5)$$

Основным недостатком схемы Рао-Нама является большой объем ключа. Действительно, для хранения секретной порождающей матрицы  $(n, k, d)$  блочного кода над  $GF(q)$  необходимо хранить, в общем случае,  $n \times k$   $q$ -ичных символов – выражение (2). Ниже рассматриваются теоретико-кодовые схемы, построенные на обширных классах алгеброгеометрических кодов, теоретически обосновывается построение симметричных криптосистем с небольшим объемом ключевых данных.

**Симметричные криптосистемы на алгеброгеометрических кодах.** Перспективным направлением в развитии алгебраической теории блочных кодов являются методы алгеброгеометрического кодирования [6–8]. Асимптотически эти коды лежат выше границы Варшавова-Гилберта [7].

Рассмотрим алгеброгеометрический код над  $GF(q)$ , построенный по алгебраической кривой рода  $g$ . Кодовые параметры связаны соотношениями [6–8]:  $k + d \geq n - g + 1$ , длина кода  $n$  меньше либо равна числу точек на кривой  $X$ . При  $2g < \alpha \leq n$  алгеброгеометрический код имеет параметры  $(n, \alpha - g + 1, d)$ ,  $d \geq n - \alpha$ , двойственный к нему код имеет параметры  $(n, n - \alpha + g - 1, d^\perp)$ ,  $d^\perp \geq \alpha - 2g + 2$ . Параметры симметричной криптосистемы по схеме Рао-Нама на алгеброгеометрических кодах задаются следующей теоремой.

*Теорема 1.* Алгеброгеометрический  $(n, k, d)$  код над  $GF(q)$ ,  $q = 2^m$  определяет симметричную криптосистему с параметрами (в битах):

$$l_{K+} = (\alpha - g + 1) \cdot (2g\sqrt{q} + q + 1) \cdot m; \quad l_I = (\alpha - g + 1) \cdot m; \quad (6)$$

$$l_S = (2g\sqrt{q} + q + 1) \cdot m; \quad R = (\alpha - g + 1) / (2g\sqrt{q} + q + 1). \quad (7)$$

*Доказательство.* Симметричная теоретико-кодовая схема, построенная с использованием порождающей матрицы алгебраического блочного  $(n, k, d)$  кода над  $GF(2^m)$ , обладает параметрами (2) – (5). Параметры алгеброгеометрического кода, заданного через порождающую матрицу определяются выражениями:

$$n \leq N; \quad k \geq \alpha - g + 1; \quad d \geq n - \alpha,$$

где  $N$  – число точек алгебраической кривой;  $\alpha$  – степень отображения;  $g$  – род кривой [6].

По теореме Хассе-Вейля  $N \leq 2g\sqrt{q} + q + 1$  [6–8], т.е.  $n \leq 2g\sqrt{q} + q + 1$ . При выполнении равенства в приведенных выражениях параметры сим-

метричной криптосистемы определяются соотношениями:

$$l_{K+} = k \cdot n \cdot m = (\alpha - g + 1) \cdot (2g\sqrt{q} + q + 1) \cdot m; \quad l_I = k \cdot m = (\alpha - g + 1) \cdot m;$$

$$l_S = n \cdot m = (2g\sqrt{q} + q + 1) \cdot m; \quad R = l_I / l_S = k / n = (\alpha - g + 1) / (2g\sqrt{q} + q + 1).$$

Как следует из выражений (6) – (7) криптосистемы обладают высокими конструктивными показателями. Так, например, длина криптограммы для рассмотренных случаев, превышает аналогичный показатель для кодов Рида-Соломона над тем же алфавитом символов. В то же время всем симметричным криптосистемам присущ существенный недостаток – большой объем секретных ключевых данных. Предлагается конструктивный способ устранения больших объемов ключа, состоящий в использовании в качестве секретных данных параметров алгебраической кривой. Длина ключа в заданных таким образом криптосистемах определяется следующей теоремой.

*Теорема 2.* Алгеброгеометрический код над  $GF(q)$  на алгебраической кривой  $X$ , заданной однородным многочленом степени  $\deg X$  задает симметричную криптосистему Рао-Нама с длиной секретного ключа:

$$l_{K+} \leq \frac{(\deg X + 1)(\deg X + 2)}{2} \cdot \log_2 q. \quad (8)$$

*Доказательство.* Действительно, значения генераторных функций  $F_j$  в точках  $P_i(X_i, Y_i, Z_i)$  алгебраической кривой  $X$  однозначно задают генераторную матрицу алгеброгеометрического кода [6 – 8]:

$$(F_i(P_j)), \text{ где } i = 0, \dots, k - 1; j = 0, \dots, n - 1.$$

Значения точек кривой однозначно задаются видом однородного многочлена кривой, т.е. его коэффициентами. Однородный многочлен степени  $\deg X$  состоит из суммы одночленов степени  $\deg X$ . Другими словами, число одночленов задает число коэффициентов, определяющих вид кривой. Всего в проективном пространстве  $P^n$  существует  $C_{\deg X + n}^n$  однородных одночленов, следовательно, в  $P^n$  однородный многочлен, задающий кривую  $X$ , состоит из  $\leq C_{\deg X + 2}^2$  одночленов. Практически это означает, что для определения генераторной матрицы алгеброгеометрического кода над  $GF(q)$  необходимо и достаточно задать

$$M \leq C_{\deg X + 2}^2 = \frac{(\deg X + 2)!}{(\deg X)! \cdot 2!} = \frac{(\deg X + 1)(\deg X + 2)}{2}$$

символов из  $GF(q)$ , или, что эквивалентно,  $M \cdot \log_2 q$  бит.

Теорема 2 задает симметричные криптосистемы на алгеброгеометрических кодах с небольшим объемом ключа. Действительно, выражение (8) задает объем секретных ключевых данных, который растет как квадрат степени соответствующей кривой. В теореме 1 размер ключа растет как произведение

длины кода на число информационных символов, что значительно превышает аналогичный показатель для теоретико-кодовых схем из теоремы 2.

Приведем *пример*. Зафиксируем конечное поле  $GF(2^6)$  и алгеброгеометрический код по кривой Эрмита,  $g = (q - \sqrt{q})/2$ ,  $R \approx 0,5$ . По теореме 1 объем секретных ключевых данных составит:  $l_{K+} = 789504$  бит. По выражению (8) объем ключа не превысит значения:  $l_{K+} = 330$  бит. Очевидно, что в рассмотренном примере результат теоремы 2 позволяет уменьшить объем ключа более чем на три порядка.

**Выводы.** Получили дальнейшее развитие симметричные криптосистемы, основанные на использовании теоретико-сложностной проблемы декодирования случайного кода. Впервые получено теоретическое обоснование симметричных криптосистем на алгеброгеометрических кодах, отличающееся от известных использованием в качестве секретного ключа параметров алгебраической кривой, что позволяет задавать теоретико-кодовые схемы с требуемыми параметрами и небольшим объемом служебных данных. **Перспективным направлением** дальнейших исследований является оценка эффективности криптосистем на алгеброгеометрических кодах.

## ЛИТЕРАТУРА

1. Rao T.R.N. and Nam K.H. *Private-key algebraic-coded cryptosystem. Advances in Cryptology – CRYPTO 86, New York. – NY: Springer. – 1986. – P. 35 – 48.*
2. Халимов Г.З., Буханцов А.Д. *Применение помехоустойчивого кодирования для обеспечения безопасности каналов передачи данных // Труды межд. НТК «Передача, обработка и отображение информации». – Х.: НАНУ, ПАНИ. – 1994. – С. 28.*
3. Халимов Г.З., Северинов А.В. *Обеспечение безопасности каналов передачи данных на основе помехоустойчивых кодов // Системы управления и связь. – Х.: ХВУ. – 1996. – С. 116 – 119.*
4. Сидельников В.М., Шестаков С.О. *О системе шифрования, построенной на основе обобщенных кодов Рида-Соломона // Дискретная математика. – 1992. – Т. 4, № 3. – С. 57 – 63.*
5. Сидельников В.М. *Криптография и теория кодирования. Материалы конференции «МГУ и развитие криптографии в России». – М.: МГУ. – 2002. – 22 с.*
6. Гоппа В.Д. *Коды на алгебраических кривых // Докл. АН СССР. – 1981. – Т. 259, № 6. – С. 1289 – 1290.*
7. Цфасман М.А. *Коды Гоппы, лежащие выше границы Варшавова-Гилберта // Проблемы передачи информации. – 1982. – № 3. – С. 3 – 6.*
8. Pellikaan Ruud. *Asymptotically good sequences of curves and codes // Proc. 34th Allerton Conf. on Communication, Control, and Computing, Urbana-Champaign, October 2 – 4, 1996. – P. 276 – 285.*

Поступила 1.03.2005

**Рецензент:** доктор технических наук, профессор Ю.В. Стасев,  
Харьковский университет Воздушных Сил.