УДК 621.391

# РАЗРАБОТКА ТЕОРЕТИКО-КОДОВЫХ СХЕМ С ИСПОЛЬЗОВАНИЕМ ЭЛЛИПТИЧЕСКИХ КОДОВ

к.т.н. А.А. Кузнецов, С.П. Евсеев
(представил д.ф-м.н., проф. С.В. Смеляков)

*Разрабатываются несимметричный метод криптографического преобразования информации, основанный на использовании теоретико-кодовых схем с алгеброгеометрическими кодами на эллиптических кривых.*

**Постановка проблемы.** Одним из перспективных направлений развития современной криптографии считается использование несимметричных криптосистем, в которых для передачи ключевой информации не требуется организация закрытого канала связи. Среди известных примеров несимметричных криптосистем особое место занимают теоретико-кодовые схемы, основанные на использовании алгебраических кодов. Они обладают существенным достоинством – высокой скоростью криптографического преобразования информации. В тоже время существует ряд ограничений, затрудняющих их практическое использование. Это, прежде всего, большой объем ключа. Кроме того, как показано в [1 – 2], известные схемы, построенные на кодах Рида-Соломона, могут быть взломаны с полиномиальной сложностью. Там же намечены пути дальнейшего их развития, один из которых – использование алгеброгеометрических кодов.

**Анализ последних исследований и публикаций.** Теоретико-кодовые схемы для криптографической защиты информации впервые предложены в [3 – 4]. Известные примеры асимметричных криптосистем на основе теоретико-кодовых схем Мак-Элиса и Нидеррайтера рассмотрены для случаев использования кодов БЧХ и кодов Рида-Соломона (подкласс недвоичных кодов БЧХ) [1 – 4]. Стойкость таких криптосистем считается недостаточной [1 – 2].

**Цель статьи.** Разработка теоретико-кодовых схем с использованием эллиптических кодов, оценка их параметров.

**Изложение основного материала.** Одним из перспективных направлений в развитии теории помехоустойчивого кодирования являются методы алгеброгеометрического кодирования. Недвоичные алгебраические блоковые коды, построенные по алгебраическим кривым (алгеб-

рогеометрические коды) обладают хорошими асимптотическими свойствами [5]. Доказано, что при большой длине эти коды лежат выше границы Варшамова-Гилберта [6].

Зафиксируем конечное поле GF(q). Пусть X – гладкая проективная алгебраическая кривая в проективном пространстве $P^n$ над GF(q); g = g(X) – род кривой; X(GF(q)) – множество ее точек над конечным полем; N = X(GF(q)) – их число. Пусть C – класс дивизоров на X степени $\alpha > g - 1$. Тогда C определяет отображение $\varphi: X \to P^{k-1}$, где $k \geq \alpha - g + 1$. Набор $y_i = \varphi(x_i)$ задает код. Число точек в пересечении $\varphi(X)$ с гиперплоскостью равно $\alpha$, т.е. $n - d \leq \alpha$. Эта конструкция позволяет строить коды с параметрами $k + d \geq n - g + 1$, длина n которых 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 также является алгеброгеометрическим и имеет параметры $(n, n - \alpha + g - 1, d^{\perp})$, $d^{\perp} \geq \alpha - 2g + 2$ [5 – 6]. Дадим следующее определение алгеброгеометрического кода.

*Определение 1* [7]. Пусть X – гладкая проективная алгебраическая кривая в проективном пространстве $P^n$, т.е. совокупность решений однородного неприводимого алгебраического уравнения степени degX с коэффициентами из GF(q). Рассмотрим многообразия, соответствующие проективным гиперповерхностям, заданным в $P^n$ уравнениями F = 0, где F – однородные одночлены степени degF. Пусть I $(i_1, i_2, \dots, i_n)$ – информационная последовательность. *Алгеброгеометрический код* по кривой X над GF(q) – это линейный код длины $n \leq N$, кодовые слова C $(c_1, c_2, \dots, c_n)$ которого задаются равенством

$$\sum_{i=0}^{k-1} i_j F_j(P_i) = c_i,$$

где $P_i(X_i, Y_i, Z_i)$ – проективные точки кривой X, т.е. $(X_i, Y_i, Z_i)$ – решения однородного алгебраического уравнения, задающие кривую X, $i = \overline{1, n}$; $F_j(P_i)$ – значения генераторных функций в точках кривой.

*Определение 2* [8]. *Эллиптической кривой* (EC) в аффинном пространстве $A^2$ над полем GF(q) называется гладкая кривая, заданная уравнением

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6,$$

или в $P^2$ заданная однородным уравнением

$$y^2z + a_1xyz + a_3yz^2 = x^3 + a_2x^2z + a_4xz + a_6z^3,$$

$a_i \in GF(q)$, род кривой g = 1.

Пусть X(GF(q)) – множество точек гладкой проективной кривой X над конечным полем GF(q), $N = |X(GF(q))|$ – их число. Число N точек кривой X над GF(q) ограничено сверху выражением Хассе-Вейля [2]:

$$N \le 2\sqrt{q} \cdot g + q + 1,$$

где g – род кривой. Точные значения верхней границы числа точек эллиптической кривой над GF(q), $q = 2^m$, $m = \overline{2,10}$ приведены в табл. 1.

Таблица 1

Оценка верхней границы числа точек эллиптической проективной кривой

| $N = \lvert EC(GF(q)) \rvert$ | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| GF(4) | GF(8) | GF(16) | GF(32) | GF(64) | GF(128) | GF(256) | GF(512) | GF(1024) |
| 9 | 14 | 25 | 44 | 81 | 151 | 289 | 558 | 1089 |

*Утверждение 1*. Алгеброгеометрический (n, k, d) код по эллиптической кривой (эллиптический код) над GF(q), построенный через отображение вида $\varphi: EC \to P^{k-1}$, связан характеристиками $k + d \ge n$, причем:

$$n \le 2\sqrt{q} + q + 1,\ k \ge \alpha,\ d \ge n - \alpha,\ \alpha = 3 \cdot \deg F.$$

*Доказательство*. Пусть EC – гладкая проективная эллиптическая кривая в проективном пространстве $P^2$ над GF(q), g = g(EC) = 1, EC(GF(q)) – множество ее точек над GF(q), N = EC(GF(q)) – их число.

По теореме Хассе-Вейля число точек гладкой проективной кривой рода g в $P^2$ над GF(q) ограничено сверху выражением $N \le 2g\sqrt{q} + q + 1$. Для эллиптической кривой это выражение примет вид $N \le 2\sqrt{q} + q + 1$. По определению $n \le N$, следовательно $n \le 2\sqrt{q} + q + 1$.

Пусть C – класс дивизоров на EC степени $\alpha > 0$. Тогда C определяет отображение $\varphi: X \to P^{k-1}$, где $k \ge \alpha$. Набор $y_i = \varphi(x_i)$ задает код. Число точек в пересечении $\varphi(EC)$ с гиперплоскостью равно $\alpha$, т.е. $n - d \le \alpha$. Следовательно, параметры алгеброгеометрического кода по эллиптической кривой связаны соотношением $k + d \ge n$, причем $d \ge n - \alpha$. Степень deg EC = 3, следовательно, $\alpha = 3 \cdot \deg F$.

Конструктивные характеристики эллиптических кодов, построенных через отображение вида $\varphi: EC \to P^{k-1}$ над GF(q), $q = 2^m$, $m = \overline{2,6}$ приведены в табл. 2.

Таблица 2

Конструктивные кодовые характеристики эллиптических кодов, построенных через отображение $\varphi$: EC $\to P^{k-1}$ над GF(q), $q = 2^m$, $m = \overline{2,6}$

| degF | $\alpha$ | (n, k, d) | | | | |
|---|---|---|---|---|---|---|
| | | GF(4) | GF(8) | GF(16) | GF(32) | GF(64) |
| 1 | | 9, 3, 6 | 14, 3, 11 | 25, 3, 22 | 44, 3, 41 | 81, 3, 78 |
| 2 | | 9, 6, 3 | 14, 6, 8 | 25, 6, 19 | 44, 6, 38 | 81, 6, 75 |
| 3 | | – | 14, 9, 5 | 25, 9, 16 | 44, 9, 35 | 81, 9, 72 |
| 4 | 12 | – | 14, 12, 2 | 25, 12, 13 | 44, 12, 32 | 81, 12, 69 |
| 5 | 15 | – | – | 25, 15, 10 | 44, 15, 29 | 81, 15, 66 |
| 6 | 18 | – | – | 25, 18, 7 | 44, 18, 26 | 81, 18, 63 |
| 7 | 21 | – | – | 25, 21, 4 | 44, 21, 23 | 81, 21, 60 |
| 8 | 24 | – | – | – | 44, 24, 20 | 81, 24, 57 |
| 9 | 27 | – | – | – | 44, 27, 17 | 81, 27, 54 |
| 10 | 30 | – | – | – | 44, 30, 14 | 81, 30, 51 |
| 11 | 33 | – | – | – | 44, 33, 11 | 81, 33, 48 |
| 12 | 36 | – | – | – | 44, 36, 8 | 81, 36, 45 |
| 13 | 39 | – | – | – | 44, 39, 5 | 81, 39, 42 |
| 14 | 42 | – | – | – | 44, 42, 2 | 81, 42, 39 |

Определения 1 – 2 и результат утверждения 1 позволяют задать теоретико-кодовую схему Мак-Элиса на основе эллиптических кодов следующим образом. Пусть $G^{EC}$ – порождающая матрица эллиптического (n, k, d) кода над GF(q) вида

$$G^{EC} = \begin{pmatrix} F_0(P_0) & F_0(P_1) & \dots & F_0(P_{n-1}) \\ F_1(P_0) & F_1(P_1) & \dots & F_1(P_{n-1}) \\ \dots & \dots & \dots & \dots \\ F_{k-1}(P_0) & F_{k-1}(P_1) & \dots & F_{k-1}(P_{n-1}) \end{pmatrix} = \left\| F_j(P_i) \right\|_{n,k}$$

и размерности $k \times n$, $k = \alpha$, $\alpha = 3 \cdot \deg F$.

Пусть X – невырожденная $k \times k$-матрица над GF(q), D – диагональная матрица с ненулевыми на диагонали элементами, P – перестановочная матрица размера $n \times n$.

Определим несимметричную криптосистему по схеме Мак-Элиса с эллиптическим кодом:

– *открытый ключ* – матрица $G_X^{EC} = X \cdot G^{EC} \cdot P \cdot D$;

– *секретный (закрытый) ключ* – матрицы X, P, D.

Шифрованная информация (криптограмма) представляет собой вектор длины n и вычисляется по правилу

$$c_X^* = i \cdot G_X^{EC} + e,$$

где вектор $c_X = i \cdot G_X^{EC}$ принадлежит эллиптическому (n, k, d) коду с порождающей матрицей $G_X^{EC}$, i – k-разрядный информационный вектор, вектор e – секретный вектор ошибок веса ≤ t.

Схема передачи секретного сообщения от абонента А к абоненту Б в несимметричной криптосистеме Мак-Элиса с использованием эллиптических кодов представлена на рис. 1.

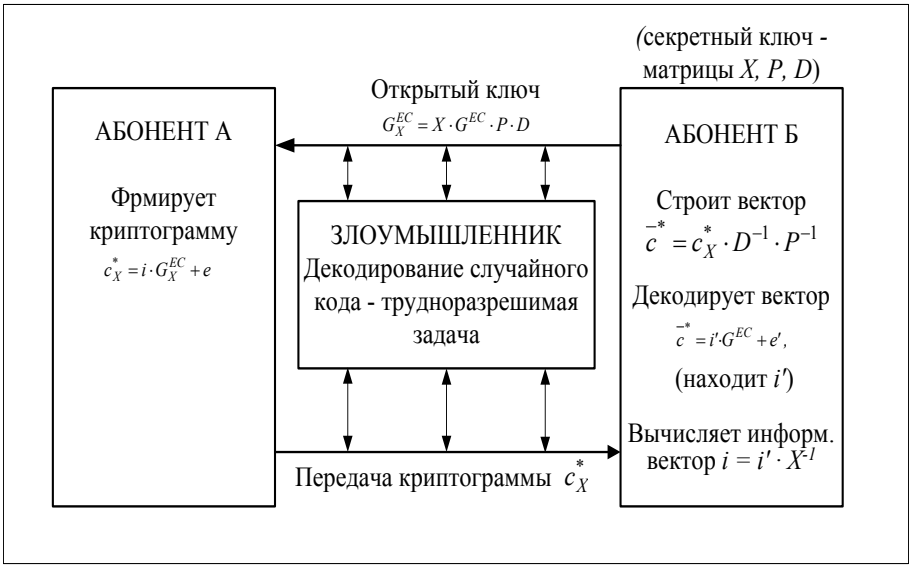


Рис. 1. Схема передачи криптограммы в криптосистеме Мак-Элиса при использовании эллиптических кодов

Передача криптограммы предваряется следующими операциями. Абонент Б случайно, равновероятно, независимо от других абонентов формирует матрицы X, P, D и хранит их в секрете (закрытый ключ). Вычисляет матрицу $G_X^{EC} = X \cdot G^{EC} \cdot P \cdot D$ и публикует ее как открытый (общедоступный) ключ. Абонент А для отправки секретного сообщения i формирует криптограмму $c_X^* = i \cdot G_X^{EC} + e$.

Ее может сформировать (зашифровать отправляемую информацию) любой пользователь, знающий публичный (общедоступный) ключ. Злоумышленник, не зная секретного ключа абонента Б, не сможет вскрыть содержимое криптограммы (прочесть информационное сообщение), для него декодирование – трудноразрешимая задача (экспоненциальной

сложности). Напротив, абонент Б декодирует криптограмму по алгоритмам полиномиальной сложности.

**Выводы.** В статье предложена теоретико-кодовая схема на основе использования алгеброгеометрических кодов по эллиптическим кривым, являющаяся дальнейшим развитием криптосхемы Мак-Элиса. Предложенная криптосистема обобщает теоретико-кодовые схемы на кодах Рида-Соломона и, потенциально, является более стойкой. Одним из **перспективных направлений дальнейших исследований** является исследование криптостойкости предложенных теоретико-кодовых схем, разработка и исследование методов оптимизации объема ключа.

## ЛИТЕРАТУРА


1. *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.*
2. *Сидельников В.М. Криптография и теория кодирования // Материалы конференции «Московский университет и развитие криптографии в России». – МГУ. – 2002. – 22 с.*
3. *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.*
4. *H. Niederreiter. Knapsack-Type Cryptosystems and Algebraic Coding Theory. // Probl. Control and Inform. Theoty. – 1986. – V. 15. – P. 19 – 34.*
5. *Гоппа В.Д. Коды на алгебраических кривых // Докл. АН СССР. – 1981. – Т. 259, № 6. – С. 1289 – 1290.*
6. *Влэдуц С. Г., Манин Ю. И. Линейные коды и модулярные кривые // Современные проблемы математики. – М.: ВИНИТИ. – 1984. – Т. 25. – С. 209 – 257.*
7. *Кузнецов А.А., Северинов А.В., Лысенко В.Н., Науменко И.В. Алгоритм помехоустойчивого кодирования с использованием кодов по кривым Эрмита // Системи обробки інформації. – Х.: ХВУ. – 2003. – Вип. 6(28).– С. 181 – 185.*
8. *Болотов А.А. и др. Алгоритмические основы эллиптической криптографии. – М.: МЭИ, 2000. – 100 с.*


*Поступила 2.03.2004*

***КУЗНЕЦОВ Александр Александрович**, канд. техн. наук, нач. научно-исследовательской лаборатории Харьковского военного университета. В 1996 году окончил Харьковский военный университет. Область научных интересов – криптографическое преобразование информации, алгебраическая теория кодов и их применение в системах передачи данных.*

***ЕВСЕЕВ Сергей Петрович**, адъюнкт Харьковского военного университета. В 2002 году окончил командно-штабной факультет Харьковского военного университета. Область научных интересов – криптографическое преобразование информации, алгебраическая теория кодов и их применение в системах передачи данных.*