УДК 512.817 : 621.391.25

НЕСИММЕТРИЧНЫЕ КРИПТОСИСТЕМЫ НА АЛГЕБРО-ГЕОМЕТРИЧЕСКИХ КОДАХ

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

Теоретически обосновывается построение несимметричных криптосистем на алгебро-геометрических кодах. Получены основные аналитические выражения, связывающие параметры теоретико-кодовых схем Мак-Элиса с кодовыми характеристиками алгебро-геометрических кодов.

Постановка проблемы в общем виде, анализ литературы. Перспективным направлением в развитии криптографии является разработка и исследование криптосистем, построенных на алгебраических блоковых кодах (т.н. несимметричных теоретико-кодовых схем) [1 – 4]. Их применение позволяет построить быстрый несимметричный криптоалгоритм, стойкость которого основана на теоретико-сложностной проблеме декодирования случайного кода. Маскируя код с быстрым алгоритмом декодирования (полиномиальной сложности) под произвольный (случайный) блоковый код, можно представить задачу декодирования для постороннего наблюдателя (возможного злоумышленника), как вычислительно сложную задачу (экспоненциальной сложности). Для уполномоченного пользователя криптосистемы (имеющего секретный ключ) декодирование – полиномиально разрешимая задача.

Пусть G – порождающая матрица линейного (n, k, d) кода над GF(q) с полиномиальной сложностью декодирования. Пусть X – невырожденная k × k-матрица над GF(q); D – диагональная матрица с ненулевыми на диагонали элементами; P – перестановочная матрица размера n × n. Перестановочная матрица реализует перестановку координат вектора в виде матричного умножения, а именно, элемент p_{ij} матрицы P равен 1 только тогда, когда координата с номером i переходит посредством перестановки в координату с номером j. В остальных случаях $p_{ij} = 0$. Таким образом, матрица P содержит в каждом столбце и в каждой строке только одну единицу. Произведение матриц $\Lambda = P \cdot D$ задает перестановочную матрицу Λ с ненулевыми элементами поля GF(q). Матрица Λ (унипотентная матрица) при перестановке координат вектора сохраняет расстояние по Хеммингу, т.е.

$$d(a, b) = d(a \cdot \Lambda, b \cdot \Lambda),$$

где d(x, y) – расстояние по Хеммингу между векторами x и y.

Открытым ключом в криптосхеме Мак-Элиса является матрица $G_X = X \cdot G \cdot P \cdot D$, секретным (закрытым) ключом являются матрицы X, P, D [1]. Шифрованная информация (криптограмма) представляет собой вектор длины n и вычисляется по правилу

$$c_X^* = I \cdot G_X + e, \qquad (1)$$

где вектор $c_X = I \cdot G_X$ принадлежит (n, k, d) коду с порождающей матрицей G_X, I – k-разрядный информационный вектор, вектор e – секретный (случайный) вектор ошибок веса меньше или равно t.

Злоумышленнику необходимо декодировать криптограмму c_X^* с известной порождающей матрицей G_X. Не зная матрицы X, P и D, он не может восстановить G и воспользоваться алгоритмом декодирования полиномиальной сложности. Для уполномоченного пользователя (знающего секретный ключ) декодирование криптограммы – полиномиально разрешимая задача. Действительно, легитимный пользователь, получив вектор c_X^*, строит вектор $\bar{c}^* = c_X^* \cdot D^{-1} \cdot P^{-1}$. Далее уполномоченный пользователь, пользуясь алгоритмом полиномиальной сложности, декодирует вектор $\bar{c}^* = I' \cdot G + e'$, т.е. находит I'. Затем вычисляет k-разрядный информационный вектор $I = I' \cdot X^{-1}$.

Известные несимметричные теоретико-кодовые схемы Мак-Элиса используют коды Гоппы, БЧХ, Рида-Соломона и обобщенные коды Рида-Соломона [1 – 4]. Для таких криптосистем в [3 – 4] предложен эффективный метод криптоанализа, сложность которого растет полиномиально. Перспективным направлением построения потенциально стойких теоретико-кодовых схем считается использование алгебро-геометрических кодов [4].

Целью статьи является разработка несимметричных криптосистем на алгебро-геометрических кодах, вывод основных аналитических выражений, связывающих параметры кодов с параметрами криптосхемы Мак-Элиса.

1. Общие положения алгебро-геометрического кодирования. Алгебро-геометрические коды впервые введены в работах Гоппы [5 – 6]. Асимптотически они лежат выше границы Варшамова-Гилберта.

Зафиксируем конечное поле GF(q). Пусть K – гладкая проективная алгебраическая кривая в проективном пространстве P^n над GF(q), т.е. совокупность решений однородного неприводимого алгебраического уравнения степени degK с коэффициентами из GF(q); g = g(K) – род кривой; K(GF(q)) – множество ее точек над конечным полем; N = K(GF(q)) – их число. Пусть C – класс дивизоров на K степени $\alpha > g - 1$. Тогда C определяет отображение $\varphi: K \to P^{k-1}$, где $k \geq \alpha - g + 1$. Набор $y_i = \varphi(x_i)$ задает

код. Число точек в пересечении $\varphi(K)$ с гиперплоскостью равно α, т.е. $n - d \le \alpha$. Эта конструкция позволяет строить коды с параметрами $k + d \ge n - g + 1$, длина n которых меньше либо равна числу точек на кривой K. При $2g < \alpha \le n$ алгебро-геометрический код имеет параметры $(n, \alpha - g + 1, d)$, $d \ge n - \alpha$. Двойственный к нему код также является алгебро-геометрическим и имеет параметры $(n, n - \alpha + g - 1, d^{\perp})$, $d^{\perp} \ge \alpha - 2g + 2$ [5 – 6].

Дадим следующее определение алгебро-геометрического кода.

Определение 1. Рассмотрим многообразия, соответствующие проективным гиперповерхностям, заданным в P^n уравнениями $F = 0$, где F – однородные одночлены степени degF. Пусть $I(I_0, I_1, \ldots, I_{k-1})$ – информационная последовательность. Алгебро-геометрический код над GF(q), построенный через отображение кривой X вида $\varphi: EC \to P^{k-1}$ – это линейный код длины $n \le N$, кодовые слова $C(c_0, c_1, \ldots, c_{n-1})$ которого задаются равенством

$$\sum_{i=0}^{k-1} I_j F_j(P_i) = c_i , \qquad (2)$$

где $P_i(X_i, Y_i, Z_i)$ – проективные точки кривой X, $i = 0,1,\ldots,n-1$; $F_j(P_i)$ – значение генераторной функции F_j в точке P_i, $j = 0, 1, \ldots, k-1$.

Это определение равносильно матричному представлению алгебро-геометрического кода: $G \cdot (I_0, I_1, \ldots, I_{k-1})^T = (c_0, c_1, \ldots, c_{n-1})$, где G – порождающая матрица размерности $k \times n$, $k = \alpha - g + 1$, $\alpha = \deg K \cdot \deg F$,

$$G = \begin{pmatrix} F_0(P_0) & F_0(P_1) & \ldots & F_0(P_{n-1}) \\ F_1(P_0) & F_1(P_1) & \ldots & F_1(P_{n-1}) \\ \ldots & \ldots & \ldots & \ldots \\ F_{k-1}(P_0) & F_{k-1}(P_1) & \ldots & F_{k-1}(P_{n-1}) \end{pmatrix} = \left\| F_j(P_i) \right\|_{n,k} . \qquad (3)$$

2. Несимметричные теоретико-кодовые схемы Мак-Элиса на алгебро-геометрических кодах. Определим несимметричную криптосистему по схеме Мак-Элиса с алгебро-геометрическим кодом. Справедлива следующая теорема.

Теорема 1. Пусть G – порождающая матрица (n, k, d) алгебро-геометрического кода над $GF(2^m)$, построенного по кривой K. Пусть X – невырожденная $k \times k$-матрица над $GF(2^m)$; D – диагональная матрица с ненулевыми на диагонали элементами над $GF(2^m)$; P – перестановочная матрица размера $n \times n$. Тогда несимметричная теоретико-кодовая схема Мак-Элиса на алгебро-геометрических кодах обладает следующими параметрами.

1. Длина информационной последовательности (в битах)

$$l_I = k \ge (\alpha - g + 1) \cdot m. \qquad (4)$$

2. Длина криптограммы (в битах)

$$l_S = n \le \left(\sqrt{q} \cdot g + q + 1\right) \cdot m . \qquad (5)$$

3. Относительная скорость передачи данных

$$R = (\alpha - g + 1)/(\sqrt{q} \cdot g + q + 1). \quad (6)$$

4. Длина открытого ключа (в битах)

$$l_K = (\alpha - g + 1) \cdot \left(\sqrt{q} \cdot g + q + 1\right) \cdot m. \quad (7)$$

5. Длина закрытого ключа (в битах)

$$l_{K+} = (\alpha - g + 1)^2 \cdot \left(\sqrt{q} \cdot g + q + 1\right)^2 \cdot m. \quad (8)$$

Доказательство. По определению 1 параметры алгебро-геометрического кода связаны соотношениями: $k + d \geq n - g + 1$, а при $2g < \alpha \leq n$ код имеет параметры ($n \leq N$, $k \geq \alpha - g + 1$, $d \geq n - \alpha$). Следовательно, длина информационной последовательности в теоретико-кодовой схеме Мак-Элиса с алгебро-геометрическим кодом равна $l_I = k \geq \alpha - g + 1$ символов над $GF(2^m)$ или $l_I = k \geq (\alpha - g + 1) \cdot m$ бит. Длина алгебро-геометрических кодов $n \leq N$, где N – число точек кривой K над GF(q) ограничено сверху выражением Хассе-Вейля [5-8]: $N \leq 2\sqrt{q} \cdot g + q + 1$, где g – род кривой. Следовательно, длина криптограммы в теоретико-кодовой схеме с алгебро-геометрическими кодами $l_S = n \leq N \leq 2\sqrt{q} \cdot g + q + 1$ символов над $GF(2^m)$ или $l_S = n \leq \left(\sqrt{q} \cdot g + q + 1\right) \cdot m$ бит. Используя равенства в выражениях (4) – (5), получим соотношение для относительной скорости передачи: $R = l_I / l_s = k / n = (\alpha - g + 1)/\left(\sqrt{q} \cdot g + q + 1\right)$. Открытым ключом в криптосистеме по схеме Мак-Элиса является матрица $G_X = X \cdot G \cdot P \cdot D$. Размерность порождающей матрицы линейного блокового кода составляет $k \times n$ символов над $GF(2^m)$. Следовательно, при выполнении равенства в выражениях (4) – (5) размерность открытого ключа (в битах): $l_K = (\alpha - g + 1) \cdot \left(\sqrt{q} \cdot g + q + 1\right) \cdot m$. Закрытым ключом в несимметричной теоретико-кодовой схеме являются, по определению, матрицы X, D, и P. Для их хранения в общем случае необходимо $k^2 \cdot n^2$ символов над $GF(2^m)$. Подставив параметры алгебро-геометрических кодов, получим искомое выражение для объема закрытого ключа (в битах): $l_{K+} = (\alpha - g + 1)^2 \cdot \left(\sqrt{q} \cdot g + q + 1\right)^2 \cdot m$, что и завершает доказательство.

Используя выражения (4) – (8) и определения эллиптических кривых [7], кривых Гурвица, Эрмита, Ферма, Сузуки [8 – 9], получим следующие следствия теоремы 1.

Следствие 1. Несимметричная теоретико-кодовая схема Мак-Элиса на алгебро-геометрических кодах, построенных по эллиптической кривой, обладает параметрами:

$$l_I = k \geq \alpha \cdot m;$$

$$l_S = n \leq \left(2\sqrt{q} + q + 1\right) \cdot m;$$

$$R = \alpha / (2\sqrt{q} + q + 1);$$

$$l_K = \alpha \cdot \left(2\sqrt{q} + q + 1\right) \cdot m;$$

$$l_{K+} = \left(2\sqrt{q} + q + 1\right)^2 \cdot \alpha^2 \cdot m.$$

Следствие 2. Несимметричная теоретико-кодовая схема Мак-Элиса на алгебро-геометрических кодах, построенных по кривой Гурвица, обладает параметрами:

$$l_I = k \geq \alpha \cdot m - \frac{\left(q^{\frac{1}{3}} + 1\right) \cdot q^{\frac{1}{3}} \cdot m}{2} + m;$$

$$l_s = n \leq q \cdot m + 2q^{\frac{2}{3}} \cdot m + 2q^{\frac{1}{3}} \cdot m + m;$$

$$R = \frac{l_I}{l_s} = \frac{\alpha + 1}{q + 2q^{\frac{2}{3}} + 2q^{\frac{1}{3}} + 1} - \frac{q^{\frac{2}{3}} + q^{\frac{1}{3}}}{2q + 4q^{\frac{2}{3}} + 4q^{\frac{1}{3}} + 2};$$

$$l_K = (\alpha - 1) \cdot q \cdot m + \left(2\alpha + \frac{3}{2}\right) q^{\frac{1}{3}} \cdot m + \left(2\alpha + \frac{1}{2}\right) \cdot q^{\frac{2}{3}} \cdot m +$$

$$+ \left(2\alpha - \frac{3}{2}\right) q^{\frac{4}{3}} \cdot m - \frac{1}{2} q^{\frac{5}{3}} \cdot m + \alpha \cdot m + m;$$

$$l_{K+} = \left(q + 2q^{\frac{2}{3}} + 2q^{\frac{1}{3}} + 1\right)^2 \cdot \left(\alpha - (q^{\frac{2}{3}} + q^{\frac{1}{3}})/2 + 1\right)^2 \cdot m.$$

Следствие 3. Несимметричная теоретико-кодовая схема Мак-Элиса на алгебро-геометрических кодах, построенных по кривой Эрмита, обладает параметрами:

$$l_I = k \geq \alpha \cdot m - \frac{q - \sqrt{q}}{2} \cdot m + m;$$

$$l_s = n \leq q\sqrt{q} \cdot m + m;$$

$$R = \frac{l_I}{l_s} = \frac{\alpha + 1}{q\sqrt{q} + 1} - \frac{q - \sqrt{q}}{2q\sqrt{q} + 2};$$

$$l_K = m\cdot(\alpha+1)\cdot q\sqrt{q} - \frac{m}{2}q^2\sqrt{q} + \frac{m}{2}q^2 - \frac{m}{2}q + \frac{m}{2}\sqrt{q} + m\cdot\alpha + m;$$

$$l_{K+} = \left(q\sqrt{q}+1\right)^2\cdot\left(\alpha-(q-\sqrt{q})/2+1\right)^2\cdot m.$$

Следствие 4. Несимметричная теоретико-кодовая схема Мак-Элиса на алгебро-геометрических кодах, построенных по кривой Ферма, обладает параметрами:

$$l_I = k \ge m\alpha - \frac{mq^{\frac{4}{3}} + 2mq - mq^{\frac{1}{3}}}{2} + m;$$

$$l_s = n \le mq^{\frac{5}{3}} - mq - mq^{\frac{2}{3}} + m;$$

$$R = \frac{l_I}{l_s} = \frac{\alpha+1}{q^{\frac{5}{3}} - q - q^{\frac{2}{3}} + 1} - \frac{q^{\frac{4}{3}} + 2q - q^{\frac{1}{3}}}{2q^{\frac{5}{3}} - 2q - 2q^{\frac{2}{3}} + 2};$$

$$l_K = m(\alpha+1)q^{\frac{5}{3}} - m(\alpha+1)q^{\frac{2}{3}} + \frac{m}{2}\left(q^2 - q^3\right) -$$

$$- m(\alpha+2)q + \frac{m}{2}q^{\frac{1}{3}} - mq^{\frac{8}{3}} - \frac{m}{2}q^{\frac{4}{3}} + m\alpha + m;$$

$$l_{K+} = \left(q^{\frac{5}{3}} - q - q^{\frac{2}{3}} + 1\right)^2\cdot\left(\alpha - \left(q^{\frac{4}{3}} + 2q - q^{\frac{1}{3}}\right)/2 + 1\right)^2\cdot m.$$

Следствие 5. Несимметричная теоретико-кодовая схема Мак-Элиса на алгебро-геометрических кодах, построенных по кривой Сузуки, обладает параметрами:

$$l_I = k \ge m\alpha - m\frac{q^2 - q}{\left\lfloor 2\sqrt{q}\right\rfloor} + m;$$

$$l_s = n \le mq^2 + m;$$

$$R = \frac{l_I}{l_s} = \frac{\alpha}{q^2+1} - \frac{q^2 - q}{\left\lfloor 2\sqrt{q}\right\rfloor\cdot\left(q^2+1\right)} + \frac{1}{q^2+1};$$

$$l_K = \left(\alpha - \frac{q^2 - q}{\left\lfloor 2\sqrt{q}\right\rfloor} + 1\right)\cdot\left(q^2+1\right)\cdot m;$$

$$l_{K+} = \left(q^2+1\right)^2 \cdot \left(\alpha - \frac{q^2-q}{\left\lfloor 2\sqrt{q} \right\rfloor} + 1\right)^2 \cdot m .$$

Выводы. Таким образом, результаты доказанных теорем позволяют определить несимметричную криптосистему на основе теоретико-кодовых схем с алгебро-геометрическими кодами. Полученные аналитические выражения (4) – (8) связывают параметры алгебро-геометрических кодов и построенных на их основе несимметричных теоретико-кодовых схем Мак-Элиса. Следствия доказанных теорем уточняют параметры теоретико-кодовых схем на алгебро-геометрических кодах, построенных по эллиптическим кривым, кривым Гурвица, Эрмита, Ферма и Сузуки. ***Перспективным направлением*** является исследование криптостойкости предложенных теоретико-кодовых схем.

ЛИТЕРАТУРА

1. *McEliece R.J. 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.*
2. *Niederreiter H. Knapsack-Type Cryptosystems and Algebraic Coding Theory // Probl. Control and Inform. Theoty. – 1986. – V. 15. – P. 19 – 34.*
3. *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.*
4. *Сидельников В.М. Криптография и теория кодирования. Материалы конференции «Московский университет и развитие криптографии в России», МГУ. – 2002. – 22 с.*
5. *Гоппа В.Д. Коды на алгебраических кривых // Докл. АН СССР. – 1981. – Т. 259, № 6. – С. 1289 – 1290.*
6. *Гоппа В.Д. Коды и информация // Успехи математических наук. – 1984. – Т. 30, вып. 1 (235). – С. 77 – 120.*
7. *Болотов А.А. Алгоритмические основы эллиптической криптографии. – М.: МЭИ, 2000. – 100 с.*
8. *Garcia G. Algebraic function fields over finite fields with many rational places // IEEE Trans. Info. Theory. – November 1995. – Vol. IT-41. – P. 1548 – 1563.*
9. *Pellikaan R. The Klein quartic, the Fano plane and curves representing designs, in Codes, Curves, and Signals: Common Threads in Communications, (A. Vardy, Ed.) // Kluwer Acad. Publ. – Dordrecht. – 1998. – P. 9 – 20,*

Поступила 12.01.2005

***КУЗНЕЦОВ Александр Александрович**, канд. техн. наук, начальник НИЛ Харьковского университета Воздушных Сил. В 1996 году окончил ХВУ. Область научных исследований – алгебраическая теория кодов и ее приложения в криптографии.*