УДК 621.391

А.А. КУЗНЕЦОВ[1], В.Н. ЛЫСЕНКО[2], С.П. ЕВСЕЕВ[1]

[1]*Харьковский университет Воздушных Сил, Украина*
[2]*Сумской государственный университет, Украина*

СИММЕТРИЧНЫЕ КРИПТОСИСТЕМЫ С ИСПОЛЬЗОВАНИЕМ ЭЛЛИПТИЧЕСКИХ КОДОВ

Рассматриваются криптосистемы с использованием алгебраических кодов. Предложены симметричные теоретико-кодовые схемы на эллиптических кодах, получены аналитические выражения, связывающие параметры эллиптических кодов и симметричных криптосхем на их основе.

симметричные криптосистемы, эллиптические коды, теоретико-кодовые схемы

Постановка проблемы в общем виде, анализ литературы

Перспективным направлением в развитии криптографических методов обработки информации является разработка и исследование теоретико-кодовых схем с использованием алгебраических кодов [1 – 8]. Известные симметричные схемы Рао-Нама обладают существенным недостатком – большим объемом ключевых данных [1]. Предложенные в [2 – 4] модификации криптосхемы Рао-Нама позволяют снизить объем ключа, но криптостойкость таких схем считается недостаточной [5 – 6].

Актуальной научно-технической задачей является разработка и исследование симметричных теоретико-кодовых схем с небольшим объемом ключа и обеспечивающих высокие показатели криптостойкости.

1. Симметричные теоретико-кодовые схемы Рао-Нама и их модификации

Первым успешным результатом в разработке симметричных теоретико-кодовых схем является криптосистема Рао-Нама [1]. Основная идея, заложенная в эту конструкцию, состоит в использовании алгебраического блокового (n, k, d) кода, замаскированного под случайный код (код общего положения). Стойкость криптосистемы базируется на использовании теоретико-сложностной проблемы декодирования случайного кода.

Действительно, порождающую матрицу G алгебраического блокового (n, k, d) кода замаскируем матицей X:

$$G_X = G \cdot X.$$

Сформируем криптограмму – вектор c^* длины n, вычисляемый по правилу

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

т.е. криптограмма формируется кодированием информационной последовательности I длиной k информационных символов в кодовое слово длиной n кодовых символов и добавлении к нему случайного вектора ошибки e. Вес вектора e удовлетворяет ограничению $w(e) \le t$, где t – число ошибок, которое может исправить (n, k, d) блоковый код, $d = 2 \cdot t + 1$.

На приемной стороне уполномоченный пользователь (знающий секретный ключ – матрицу X) дешифрует полученную криптограмму – декодирует кодовое слово с ошибками (n, k, d) алгебраического блокового кода. Задача декодирования алгебраического блокового кода (например, кода БЧХ, Рида-Соломона, и др.) – полиномиально разрешимая задача. Декодирование произвольного линейного кода (кода общего положения) является весьма сложной вычислительной задачей, сложность ее решения растет экспоненциально. Это положение лежит в основе симметричных криптосистем по схеме

Рао-Нама: код с быстрым алгоритмом декодирования (полиномиальной сложности) маскируется под произвольный (случайный) линейный код, декодирование которого представляется как вычислительно сложная задача (без знания ключа – матрицы X). Для уполномоченного пользователя криптосистемы (имеющего секретный ключ) декодирование – полиномиально разрешимая задача.

Оценим параметрі симметричной теоретико-кодовой схемы, построенной с использованием алгебраических (n, k, d) блоковых кодов над $GF(2^m)$: размерность секретного ключа (в битах) $l_{K+} = k \cdot n \cdot m$; размерность информационного вектора (в битах) $l_I = k \cdot m$; размерность криптограммы (в битах) $l_S = n \cdot m$; относительная скорость передачи $R = k / n$.

Основным недостатком схемы Рао-Нама является большой объем ключа [1]. 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.

Модифицированная симметричная теоретико-кодовая схема Рао-Нама, построенная с использованием альтернантных кодов, заданных через многочлен Гоппы, впервые предложена в [2]. Основная идея состоит в построении схемы Рао-Нама на (n, k, d) кодах Гоппы, заданных с помощью многочлена Гоппы степени t, $d = 2 \cdot t + 1$. При этом если (n, k, d) код Гоппы над $GF(q)$ позволяет исправить t ошибок, то все кодовые слова могут быть однозначно заданы многочленом Гоппы степени t над $GF(q)$. Следовательно, если вместо порождающей матрицы кода и матрицы X в качестве секретного ключа использовать многочлен Гоппы, то удается существенно сократить его объем. В общем случае, для однозначного определения многочлена Гоппы необходимо хранить $t+1$ q-ичных символов.

Другой подход к сокращению объема ключевых данных состоит в использовании укороченных алгебраических кодов. Так в источниках [3 – 4] для построения симметричных теоретико-кодовых схем предложено использовать укороченные коды Гоппы, а символы укорочения хранить в секрете. При соответствующем выборе символов укорочения можно построить потенциально стойкую криптосхему. Однако, как показано в работах [5 – 6], криптосхему с обобщенными кодами Рида-Соломона можно взломать алгоритмом полиномиальной сложности. Альтернантные коды (коды Гоппы в том числе) строятся с использованием проверочной матрицы обобщенных кодов Рида-Соломона и, следовательно, криптосистемы на их основе также потенциально уязвимы.

2. Симметричные теоретико-кодовые схемы с использованием эллиптических кодов

Воспользуемся определением эллиптических кодов [7 – 8]. Справедливы следующие свойства.

Свойство 1. Эллиптический (n, k, d) код над $GF(q)$, построенный через отображение вида $\varphi : EC \to P^{k-1}$, связан характеристиками $k + d \geq n$, причем:

$$n \leq 2\sqrt{q} + q + 1;\ k \geq \alpha;\ d \geq n - \alpha;\ \alpha = 3 \cdot degF.$$

Свойство 2. Эллиптический (n, k, d) код над $GF(q)$, построенный через отображение вида $\varphi : EC \to P^{r-1}$, связан характеристиками $k + d \geq n$, причем:

$$n \leq 2\sqrt{q} + q + 1;\ k \geq n - \alpha;\ d \geq \alpha;\ \alpha = 3 \cdot degF.$$

Пусть A – генераторная матрица эллиптического (n, k, d) кода над $GF(q)$ вида

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

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

Зададим симметричную теоретико-кодовую схему Рао-Нама на эллиптических кодах, построенных через порождающую матрицу $G^{EC} = A$ (свойство 1). Справедливо следующее утверждение.

Утверждение 1. Эллиптический (*n, k, d*) код над $GF(2^m)$, заданный через порождающую матрицу $G^{EC} = A$, определяет симметричную теоретико-кодовую схему Рао-Нама с параметрами:

– размерность секретного ключа (в битах):

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

– размерность информационного вектора (в битах):

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

– размерность криптограммы (в битах):

$$l_S = \left(2\sqrt{q} + q + 1\right) \cdot m; \quad (4)$$

– относительная скорость передачи:

$$R = \alpha / \left(2\sqrt{q} + q + 1\right). \quad (5)$$

Доказательство. Действительно, симметричная теоретико-кодовая схема Рао-Нама, построенная с использованием порождающей матрицы алгебраического блокового (*n, k, d*) кода над $GF(2^m)$, обладает параметрами: размер секретного ключа $k \times n$ символов из $GF(2^m)$; информационный вектор длины k символов из $GF(2^m)$; длина криптограммы – n символов из $GF(2^m)$; относительная скорость передачи – $R = k / n$. Подставим параметры эллиптического (*n, k, d*) кода над $GF(q)$, построенного через отображение $\varphi : EC \to P^{k-1}$: $n \le 2\sqrt{q} + q + 1$; $k \ge \alpha$; $d \ge n - \alpha$; $\alpha = 3 \cdot degF$. С учетом степени m расширения двоичного поля получим выражения (2 – 5).

Зададим симметричную теоретико-кодовую схему Рао-Нама на эллиптических кодах, построенных через проверочную матрицу $H^{EC} = A$ (свойство 2). Справедливо следующее утверждение.

Утверждение 2. Эллиптический (*n, k, d*) код над $GF(2^m)$, заданный через проверочную матрицу $H^{EC} = A$, определяет симметричную теоретико-кодовую схему Рао-Нама с параметрами:

– размерность секретного ключа определяется выражением (2);

– размерность информационного вектора (в битах):

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

– размерность криптограммы определяется выражением (4);

– относительная скорость передачи:

$$R = \left(2\sqrt{q} + q + 1 - \alpha\right) / \left(2\sqrt{q} + q + 1\right). \quad (7)$$

Доказательство. Симметричная теоретико-кодовая схема Рао-Нама, построенная с использованием проверочной матрицы алгебраического блокового (*n, k, d*) кода над $GF(2^m)$, обладает параметрами: размер секретного ключа $r \times n$ символов из $GF(2^m)$; информационный вектор длины k символов из $GF(2^m)$; длина криптограммы – n символов из $GF(2^m)$; относительная скорость передачи – $R = k / n$. Подставим параметры эллиптического (*n, k, d*) кода над $GF(q)$, построенного через отображение вида $\varphi : EC \to P^{r-1}$: $n \le 2\sqrt{q} + q + 1$; $k \ge n - \alpha$; $d \ge \alpha$; $\alpha = 3 \cdot degF$. С учетом степени m расширения двоичного поля получим выражения (6 – 7).

Передача криптограмм в симметричной теоретико-кодовой схеме Рао-Нама на эллиптических кодах (по утверждению 1) представлена на рис. 1.

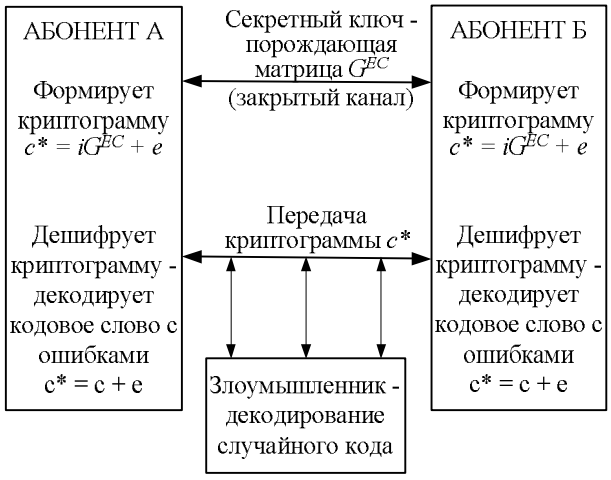

Рис. 1. Схема передачи криптограммы в теоретико-кодовой схеме с эллиптическими кодами

Для передачи криптограмм в симметричной криптосхеме, построенной с использованием результата утверждения 2, необходимо предварительно вычислить матрицу B, такую, что $A \cdot B^T = 0$. Далее,

формирование и передача криптограммы соответствует рис. 1 при $G^{EC} = B$.

Для снижения объема ключевых данных в симметричной теоретико-кодовой схеме на эллиптических кодах воспользуемся следующими особенностями построения матрицы A.

Генераторная матрица A формируется отображением точек $\{P_0, P_1, ..., P_{n-1}\}$ эллиптической кривой с помощью генераторных функций $\{F_0, F_1, ..., F_{M-1}\}$. В утверждениях 1 – 2 используется генераторная матрица эллиптического кода, построенного по кривой

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

$a_i \in GF(q)$. Коэффициенты этого многочлена однозначно задают вид кривой и, соответственно, набор проективных точек $\{P_0, P_1, ..., P_{n-1}\}$, по которым строится эллиптический код (его генераторная матрица A). Справедливо следующее утверждение.

Утверждение 3. Эллиптический (n, k, d) код над $GF(q)$ однозначно задается набором a_1 ... a_6, $\forall a_i \in GF(q)$.

Доказательство. Рассмотрим генераторную матрицу эллиптического (n, k, d) кода над $GF(q)$:

$$A = \begin{pmatrix} F_0(P_0) & F_0(P_1) & ... & F_0(P_{n-1}) \\ F_1(P_0) & F_1(P_1) & ... & F_1(P_{n-1}) \\ ... & ... & ... & ... \\ F_{M-1}(P_0) & F_{M-1}(P_1) & ... & F_{M-1}(P_{n-1}) \end{pmatrix}.$$

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 кривой и, следовательно, также задается конструктивными параметрами кода.

Таким образом, если заданы конструктивные (n, k, d) характеристики эллиптического кода, то уникальность генераторной матрицы определяет набор точек $P_1, P_2, ..., P_n$, в которых вычисляются значения генераторных функций. Конкретный набор точек однозначно задается видом многочлена кривой, т.е. набором коэффициентов a_1 ... a_6, $\forall a_i \in GF(q)$.

Следствие. Объем секретного ключа (в битах) в симметричной теоретико-кодовой схеме Рао-Нама, построенной по эллиптическим (n, k, d) кодам над $GF(2^m)$ определяется выражением

$$l_{K+} = 5 \cdot m. \qquad (8)$$

Доказательство. Действительно, секретный ключ в схеме Рао-Нама – генераторная матрица A (проверочная или порождающая матрица кода). Для определения генераторной матрицы A эллиптического (n, k, d) кода над $GF(2^m)$, по утверждению 3, достаточно определить набор коэффициентов a_1 ... a_6, $\forall a_i \in GF(2^m)$, всего 5 коэффициентов, на каждый по m бит над $GF(2^m)$, т.е. всего необходимо хранить $l_{K+} = 5 \cdot m$ бит секретной ключевой информации.

Выражение (8) позволяет оценить объем секретных ключевых данных в симметричной теоретико-кодовой схеме Рао-Нама с эллиптическими кодами. На рис. 2 представлены зависимости объемов ключевых данных от размерности поля $GF(q^m)$ для различных q = 2, 4, 16, 32.

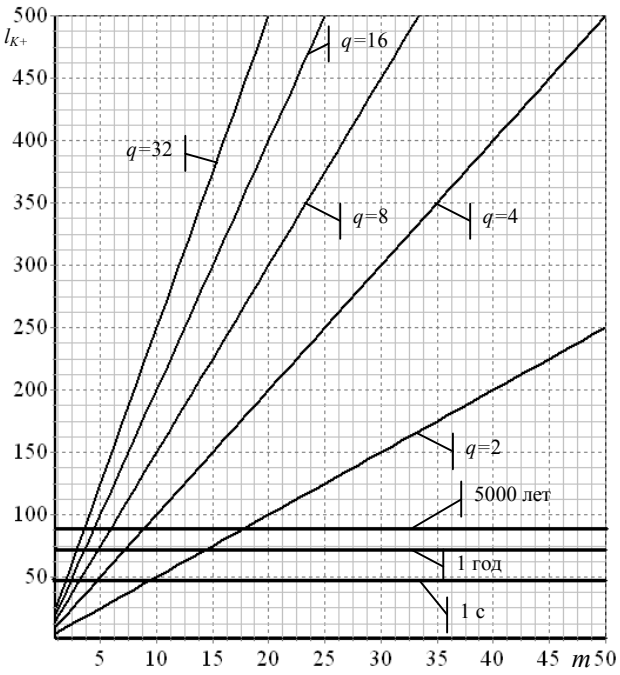

Рис. 2. Зависимости объема секретных ключевых данных симметричной теоретико-кодовой схемы на эллиптических кодах

На рис. 2 приведены также временные затраты, необходимые для полного перебора ключевых данных при выполнении 10^{15} переборов в секунду. Очевидно, что предложенный способ построения симметричных теоретико-кодовых схем на эллиптических кодах позволяет существенно снизить объемы ключевой информации по сравнению с классической схемой Рао-Нама. В то же время, потенциально стойкими считаются криптосистемы *с* $l_{K+} > 80$ бит. Как следует из приведенных на рис. 2 зависимостей, для построения такой криптосистемы необходимо использовать эллиптические коды с длиной кодового слова $> 2^{20}$ бит.

Выводы

Разработаны симметричные теоретико-кодовые схемы, отличающиеся от известных применением алгеброгеометрических кодов на эллиптических кривых (эллиптических кодов), что позволяет построить криптографически стойкую симметричную криптосистему. Получены аналитические выражения, связывающие параметры эллиптических кодов и построенных на их основе симметричных криптосхем. За счет использования параметров эллиптической кривой предложен эффективный способ снижения объемов ключевых данных теоретико-кодовых схем на эллиптических кодах.

Перспективным направлением дальнейших исследований является оценка криптостойкости предложенных теоретико-кодовых схем и сложности их практической реализации.

Литература

1. T. R. N. Rao and K. H. Nam. 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 международной НТК «Передача, обработка и отображение информации»: Под ред. А.В. Королева. – Х.: НАНУ, ПАНИ. – 1994. – С. 28.

3. Халимов Г.З., Северинов А.В. Обеспечение безопасности каналов передачи данных на основе помехоустойчивого кодирования // Системы управления и связь. – Х.: ХВУ. – 1996. – С. 116 – 119.

4. Северинов А.В. Оценка имитозащищенности каналов передачи данных с укороченными кодами Гоппы // Информационно-управляющие системы на железнодорожном транспорте. – 1997. – № 3. – С. 29 – 30.

5. 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.

6. Сидельников В.М. Криптография и теория кодирования // Материалы конференции «Московский университет и развитие криптографии в России». – МГУ. – 2002. – 22 с.

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.: НАНУ, ПАНМ, ХВУ. – 2003. – Вип. 6 (28). – С. 181 – 185.

8. Кузнецов А.А., Евсеев С.П. Разработка теоретико-кодовых схем с использованием эллиптических кодов // Системи обробки інформації. – Х.: ХВУ. – 2004. – Вип. 5. – С. 127 – 132.

Поступила в редакцию 18.10.2004

Рецензент: д-р техн. наук, проф. В.С. Харченко, Национальный аэрокосмический университет «ХАИ», Харьков.