УДК 621.391

С.П. ЕВСЕЕВ (г. Харьков)

НЕСИММЕТРИЧНЫЙ АЛГОРИТМ ШИФРОВАНИЯ С ИСПОЛЬЗОВАНИЕМ ЭЛЛИПТИЧЕСКИХ КОДОВ

Розробляються несиметричні методи шифрування з використанням алгеброгеометричних кодів, побудованих по еліптичних кривих (еліптичних кодів). Досліджуються ефективні процедури кодування-декодування еліптичних кодів.

Asymmetrical methods of coding with the use of algebraic geometric codes built on the elliptic curves are developed (elliptic codes). Effective procedures of encoding-decoding elliptic codes are explored.

Постановка проблемы в общем виде, анализ литературы. Важной научно-технической проблемой является построение криптографически стойких несимметричных алгоритмов шифрования информации, обеспечивающих высокие показатели быстродействия. Перспективным направлением является разработка и исследование несимметричных методов шифрования, основанных на использовании алгебраических кодов.

Теоретико-кодовые схемы для криптографической защиты информации впервые предложены в [1 – 2]. Основное достоинство несимметричных криптосистем, построенных на их основе, состоит в высокой скорости криптографического преобразования информации [1 – 4]. Однако, как показано в [3 – 4], известные схемы, построенные с использованием обобщенных кодов Рида-Соломона, могут быть взломаны алгоритмом полиномиальной сложности. Перспективным направлением в их развитии считается применение алгеброгеометрических кодов [4].

Целью статьи является разработка несимметричных методов шифрования с использованием алгеброгеометрических кодов, построенных по эллиптическим кривым (эллиптических кодов), исследование эффективных процедур кодирования-декодирования эллиптических кодов.

Разработка алгоритмов шифрования-дешифрования в теоретико-кодовой схеме с эллиптическими кодами. В работах [5 – 6] предложен метод построения несимметричных теоретико-кодовых схем на эллиптических кодах. Он основывается на использовании теоретико-сложностной проблемы декодирования случайного кода. Случайный код получают маскированием эллиптического кода так, чтобы для неуполномоченного пользователя криптосистемы задача декодирования представлялась трудноразрешимой с экспоненциальным показателем сложности, а для уполномоченного пользователя существовала лазейка – алгоритм декодирования с полиномиальным показателем сложности.

Пусть X – невырожденная $k \times k$-матрица над $GF(q)$, D – диагональная матрица с ненулевыми элементами на диагонали, P – перестановочная матрица размера $n \times n$. Определим несимметричную криптосистему по *схеме Мак-Элиса с эллиптическим кодом* [5 – 6]: 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 $\le t$.

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.

Таким образом, криптограмма формируется путем кодирования исходной информации эллиптическим кодом с последующим добавлением случайного вектора ошибок, вес которого не превышает исправляющую способность эллиптического кода. *Алгоритм формирования криптограммы (шифрования)* представим в виде последовательности следующих шагов:

ШАГ 1. Ввод информации, подлежащей шифрованию, ввод открытого ключа шифрования G_X^{EC}.

ШАГ 2. Кодирование информации эллиптическим кодом. Формирование кодового слова c_X эллиптического кода, заданного матрицей G_X^{EC}.

ШАГ 3. Формирование вектора ошибок e, вес которого не превышает t – исправляющую способность эллиптического кода.

ШАГ 4. Формирование криптограммы $c_X^* = c_X + e$.

Основным этапом предложенного алгоритма является кодирование информационного вектора эллиптическим кодом (шаг 2). Пусть задан эллиптический код своей порождающей матрицей G_X^{EC}:

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

где $F_j(P_i)$ – значения генераторной функции F_j в точке P_i эллиптической кривой.

Кодовое слово в этом случае может быть сформировано по следующему правилу:

$$c_j = \sum_{i=1} I_i F_i(P_j), \ j = \overline{0,\ n-1},$$

или в матричной форме – как произведение информационного вектора-строки на порождающую матрицу

$$\left\| c_j \right\|_n = G \left\| I_i \right\|_k^T = \left\| F_i(P_j) \right\|_{n,k} \left\| I_i \right\|_k^T.$$

Таким образом, для реализации несистематического алгоритма кодирования необходимо хранить элементы матрицы $\left\| F_i(P_j) \right\|_{n,k}$, либо поочередно вычислять их как значения генераторных функций в точках кривой. Всего, при известном и хранимом в памяти массиве $\left\| F_i(P_j) \right\|_{n,k}$ необходимо выполнить $k \times n$ операций сложения и умножения. Формально, сложность алгоритма $O(k \times n)$. Если эллиптический код задан через проверочную матрицу H^{EC}, построенную через вычисления генераторных функций в точках кривой, то алгоритм кодирования будет следующим.

Пусть I – множество k информационных позиций кодового слова (т.е. множество номеров позиций, входящих в заданный информационный набор кода) и h – множество $r = n - k$ проверочных позиций. Объединение множеств $I \cup h$ содержит все целые числа (номера) от 0 до $n-1$. На информационных позициях разместим k символов сообщения, а на проверочных – нули. Вычислим суммы $S_j = \sum_{i \in I} c_i F_j(P_i), \quad j = \overline{0,\ r-1}$ или в матричной форме $\left\| S_j \right\|_r = \left\| F_j(P_i) \right\|_{k,r} \left\| c_i \right\|_k^T$, где $F_j(P_i)$ – значения генераторных функций в точках эллиптической кривой – элементы проверочной матрицы H^{EC}.

Задача состоит в том, чтобы вычислить и записать на проверочных позициях такие символы c_i, $i \in h$, которые удовлетворяют уравнению $cH^T = 0$.

Из определения эллиптического кода следует, что значения $r = n - k$ проверочных символов могут быть найдены из системы линейных уравнений

$$\sum_{i \in h} c_i F_j(P_i) = -S_j \ , \ \ j = \overline{0, r-1}.$$

В матричном представлении последняя запись эквивалентна выражению

$$\left\| F_j(P_i) \right\|_{r,r} \left\| c_i \right\|_r^T = \left\| - S_j \right\|_r .$$

Для нахождения значений $r = n - k$ проверочных символов используем методы обращения матриц [7]. Запишем в матричной форме

$$\left\| c_i \right\|_r = \left\| F_j(P_i) \right\|_{r,r}^{-1} \left\| - S_j \right\|_r^T ,$$

где $\left\| F_j(P_i) \right\|_{Y,Y}^{-1}$ – обратная матрица $\left\| F_j(P_i) \right\|_{Y,Y}$.

Поскольку размещение проверочных позиций обычно известно и фиксировано, то заранее можно найти обратную матрицу и получить все проверочные символы умножением вектора $(S_0, \ldots, S_{r-1})$ на матрицу $\left\| F_j(P_i) \right\|_{Y,Y}^{-1}$. В качестве информационных могут быть выбраны любые k позиций кодового слова. Следовательно, всегда можно выбрать такое множество проверочных (и информационных) позиций, для которого матрица $\left\| F_j(P_i) \right\|_{Y,Y}^{-1}$ наиболее удобна для вычислений.

Таким образом, для реализации такого алгоритма кодирования достаточно хранить элементы матрицы $\left\| F_j(P_i) \right\|_{k,Y}$ и $\left\| F_j(P_i) \right\|_{Y,Y}^{-1}$ либо поочередно вычислять $\left\| F_j(P_i) \right\|_{k,Y}$ как значения генераторных функций в точках кривой. Всего, при известных и хранимых в памяти массивах $\left\| F_j(P_i) \right\|_{k,Y}$ и $\left\| F_j(P_i) \right\|_{Y,Y}^{-1}$, необходимо выполнить $r \times n$ операций сложения и умножения. Формально, сложность алгоритма $O(r \times n)$.

Для дешифрования информации в теоретико-кодовой схеме Мак-Эллиса с эллиптическими кодами необходимо снять действие диагональной D и перестановочной P матриц. Затем, декодировав полученный вектор, необходимо снять действие матрицы X. *Алгоритм дешифрования* представим в виде последовательности следующих шагов.

ШАГ 1. Ввод криптограммы c_X^*, подлежащей дешифрованию. Ввод закрытого ключа – матриц X, P, D.

ШАГ 2. Снятие действия диагональной и перестановочной матриц: $\bar{c}^* = c_X^* D^{-1} p^{-1}$.

ШАГ 3. Декодирование вектора $\bar{c}^*$. Формирование вектора *i'*.

ШАГ 4. Снятие действия матрицы *X*: $i = i' \cdot X^{-1}$. Формирование искомого информационного вектора *i*.

Основным этапом разработанного алгоритма дешифрования криптограмм является декодирование вектора $\bar{c}^*$ (шаг 3), которое состоит в нахождении вектора ошибок $e = (e_0, e_1, \ldots, e_{n-1})$ по известной синдромной последовательности.

Рассмотрим в качестве генераторных функций однородные одночлены степени *degF*. Каждый такой одночлен запишем в виде $f_{lmp} = x^l y^m z^p$, $l + m + p = degF$. На множестве проективных точек кривой, представимых в однородных координатах в виде $P(X, Y, 1)$, значения генераторных функций примут вид $f_{lm} = X_i^l Y_i^m$, $i = 0, \ldots, n-1$, $l + m \le degF$. Проверочная матрица *H* запишется в виде

$$H^{EC} = \begin{pmatrix} 1 & 1 & \ldots & 1 \\ X_0 & X_1 & \ldots & X_{n-1} \\ \ldots & \ldots & \ldots & \ldots \\ Y_0^{\deg F} & Y_1^{\deg F} & \ldots & Y_{n-1}^{\deg F} \end{pmatrix}.$$

Элементы синдромной последовательности, как элементы вектора $\left\|S_{lm}\right\|_y$, вычислим по правилу

$$S_{lm} = \sum_{i=0}^{n-1} c_i^* X_i^l Y_i^m = \sum_{i=0}^{n-1} e_i X_i^l Y_i^m,\ l + m \le degF, \qquad (1)$$

или, в матричной форме,

$$\left\|S_{lm}\right\|_r = H \left\|c_n^*\right\|_n^T = \left\|X_i^l Y_i^m\right\|_{n,r} \left\|e_i\right\|_n^T.$$

Таким образом, задача декодирования алгеброгеометрического кода, построенного через отображение проективных точек $P(X, Y, 1)$ кривой однородными одночленами степени *degF* эквивалентна задаче решения системы из $r = d + g - 1$ нелинейных уравнений от $3t$ переменных. Для решения этой задачи воспользуемся искусственным приемом. Введем в рассмотрение *многочлен локаторов ошибок алгеброгеометрического кода*, решения которого однозначно локализуют (указывают местоположение) возникших ошибок – многочлен от двух переменных, степени $\le (t-1)$:

$$a_{00} + a_{10}x + \ldots + y^{t-1} = 0, \qquad (2)$$

где *t* – число ошибок, которое может исправить алгеброгеометрический код.

Умножив обе части многочлена (2) на e_i и просуммировав по всем $i = 0, \ldots, n-1$, значениям в точке $(x = X_i, y = Y_i)$, получим рекуррентное выражение

$$a_{00}S_{00} + a_{10}S_{10} + \ldots + S_{0\,t-1} = 0,$$

которое задает систему линейных уравнений относительно неизвестных коэффициентов многочлена локаторов ошибок. В матричном виде система линейных уравнений запишется в виде

$$\begin{pmatrix} S_{00} & S_{10} & \dots & S_{1\,t-2} \\ S_{10} & S_{20} & \dots & S_{2\,t-2} \\ \dots & \dots & \dots & \dots \\ S_{1\,t-2} & S_{0\,t-2} & \dots & S_{2\,2t-4} \end{pmatrix} \cdot \begin{pmatrix} a_{00} \\ a_{10} \\ \dots \\ a_{1\,t-2} \end{pmatrix} = \begin{pmatrix} -S_{0\,t-1} \\ -S_{1\,t-1} \\ \dots \\ -S_{1\,2t-3} \end{pmatrix}.$$

После нахождения коэффициентов многочлена локаторов ошибок локализуем ошибки. Подставим в известный многочлен локаторов ошибок локаторы и выберем те из них, которые обращают его в нуль. Т.е. в многочлен локаторов подставляются все пары (X, Y), отождествляющие все проективные точки кривой, заданные в однородных координатах $P(X, Y, 1)$. После нахождения локаторов ошибок, указывающих на расположение возникшей ошибки, процедура нахождения кратности ошибки (значение всех $e_i \neq 0$) состоит в подстановке локаторов в систему (1), которая вырождается в систему $\leq r$ линейных уравнений относительно $\leq t$ неизвестных. Сложность решения системы линейных уравнений методом Гаусса – $O(n^2)$, где n – число переменных. Общая сложность рассмотренного алгоритма декодирования – $O(4t^2 + (t^2 + t - 2)^2/4)$.

Выводы. Несимметричные методы шифрования с использованием эллиптических кодов обладают высокими показателями быстродействия. Алгоритмы кодирования и декодирования эллиптических кодов, лежащие в основе процедур шифрования и дешифрования криптограмм, имеют полиномиальный показатель сложности. Одним из **перспективных направлений дальнейших исследований** является оценка криптостойкости предложенных схем шифрования.

Список литературы. 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». – М.: МГУ, 2002. – 22 с. **5.** *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. **6.** *Кузнецов А.А., Лысенко В.Н., Евсеев С.П.* Метод повышения безопасности и помехоустойчивости каналов передачи данных // Современные методы кодирования в электронных системах. Материалы международной НТК 26–27 октября 2004. – Сумы: СМКЭС. – 2004. – С. 12 – 13. **7.** *Гантмахер Ф.Р.* Теория матриц. – М.: Наука, 1988. – 552 с.

Поступила в редакцию 01.10.2004