УДК 681.3.06

С.П. Евсеев

Харьковский университет Воздушных Сил им. И. Кожедуба, Харьков

КРИПТОГРАФИЧЕСКОЕ ПРЕОБРАЗОВАНИЕ ИНФОРМАЦИИ В КОДОВЫХ КРИПТОСИСТЕМАХ НА ЭЛЛИПТИЧЕСКИХ КОДАХ ДЛЯ КАНАЛОВ С АВТОМАТИЧЕСКИМ ПЕРЕСПРОСОМ

Исследуются кодовые криптосистемы на эллиптических кодах. Разработаны алгоритмы несимметричного криптографического преобразования информации для каналов с автоматическим переспросом.

кодовые криптосистемы, эллиптические коды

Введение

Эффективным механизмом комплексного повышения безопасности и достоверности информации в телекоммуникационных системах являются кодовые криптосистемы [1 – 5]. Их использование позволяет обеспечить защиту информации от несанкционированного доступа и воздействия случайных оши-

бок. В тоже время известные кодовые криптосистемы функционируют в режиме прямого исправления ошибок и не предполагают использование в каналах с автоматическим переспросом. Целью данной статьи является разработка алгоритмов криптографического преобразования информации для каналов с автоматическим переспросом с использованием кодовых криптосистем на эллиптических кодах.

Основная часть

В работе [6] предложена несимметричная криптосистема на эллиптических (n, k, d) кодах, построенных по эллиптическим кривым.

Пусть X – гладкая проективная алгебраическая кривая в P^n, т.е. совокупность решений однородного неприводимого алгебраического уравнения степени degX с коэффициентами из GF(q), F – однородные одночлены степени degF. Алгеброгеометрический код по кривой X над GF(q) – это линейный код, состоящий из всех слов $(c_1, c_2, \dots, c_n)$ длины $n \le N$, для которых выполняется равенство d + g – 1 уравнений

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

где $c_i \in GF(q)$, $d \ge \alpha - 2g + 2$, $\alpha = degX \cdot degF$.

Пусть H^{EC} – проверочная матрица эллиптического (n, k, d) кода над GF(q) вида

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

и размерности r×n, $r = \alpha$, $\alpha = 3 \cdot degF$. Пусть X – невырожденная k × k-матрица над GF(q), D – диагональная матрица с ненулевыми на диагонали элементами, P – перестановочная матрица размера n × n.

Формально кодовая криптосистема на эллиптических кодах задается совокупностью множеств:

– множество открытых текстов

$$M = \{M_1, M_2, \dots, M_\mu\},$$

где $M_i = (e_0, e_1, \dots, e_{n-1})$, $\forall e_j \in GF(q)$,

$$w(M_i) \le t = \left\lfloor \frac{(d-1)}{2} \right\rfloor;$$

– множество криптограмм

$$E = \{E_1, E_2, \dots, E_\mu\},$$

где $E_i = (S_{X_0}, S_{X_1}, \dots, S_{X_{n-k-1}})$, $\forall S_{X_j} \in GF(q)$;

– множество прямых отображений

$$\varphi = \{\varphi_1, \varphi_2, \dots, \varphi_s\},$$

где $\varphi_i: M \to E$, i = 1, 2 , …, s;

– множество обратных отображений

$$\varphi^{-1} = \{\varphi_1^{-1}, \varphi_2^{-1}, \dots, \varphi_s^{-1}\},$$

где $\varphi_i^{-1}: E \to M$, i = 1, 2 , …, s;

– множество ключей, параметризирующих прямые отображения

$$K = \{K_1, K_2, \dots, K_s\} = \{H_X^1, H_X^2, \dots, H_X^s\};$$

$$H_X^i = X_i \cdot H^{EC} \cdot P_i \cdot D_i;\ \varphi_i : M \xrightarrow{K_i} E;$$

– множество ключей, параметризирующих обратные отображения

$$K^* = \{K_1^*, K_2^*, \dots, K_s^*\} = \{\{X_1, P_1, D_1\}, \{X_2, P_2, D_2\}, \dots, \{X_s, P_s, D_s\}\};$$

$$\varphi_i^{-1} : E \xrightarrow{K_i^*} M,$$

таких, что сложность выполнения обратного отображения φ^{-1} без знания ключа $K_i^* \in K^*$ сопряжено с решением теоретико-сложностной задачи декодирования случайного кода (кода общего положения).

Криптограмма S_X представляет собой вектор длины *n* и формируется путем вычисления синдрома

$$S_X = e \cdot \left(H_X^i\right)^T,$$

соответствующего случайным образом сформированному вектору ошибок e, вес которого не превышает исправляющую способность эллиптического кода. Схема алгоритма формирования криптограммы представлена на рис. 1.

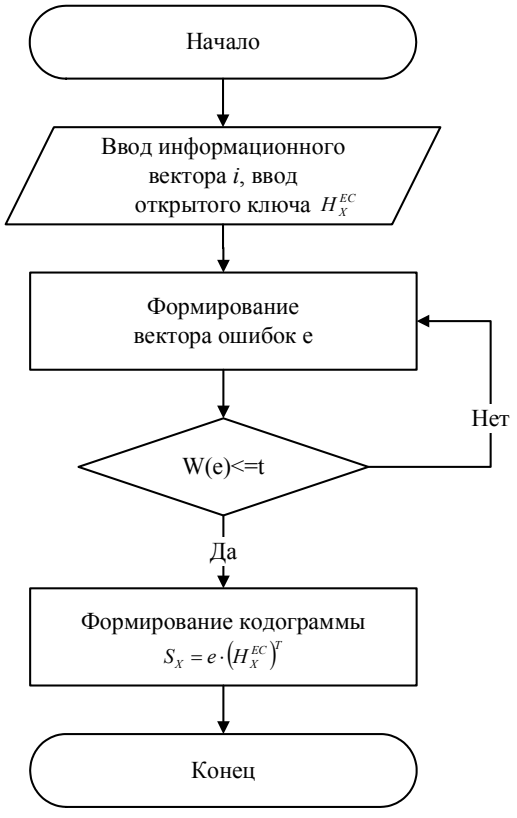

Рис. 1. Схема алгоритма формирования криптограммы

Алгоритм формирования криптограммы представим в виде последовательности следующих шагов:

ШАГ 1. Ввод информации, подлежащей шифрованию. Ввод открытого ключа H_X^{EC}.

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

ШАГ 4. Формирование криптограммы $S_X = e \cdot \left(H_X^{EC}\right)^T$.

Сложность предложенного алгоритма формирования криптограммы в кодовой криптосистеме с эллиптическими кодами составит $(r \times n)$ операций сложения и умножения над GF(q), что тождественно $(3 \cdot \deg F \times n)$ или $(d \times n)$.

Для расшифрования криптограммы в кодовой криптосистеме с эллиптическими кодами необходимо найти одно из возможных решений уравнения

$$S_X = c_X^* \cdot \left(H_X^{EC}\right)^T.$$

Затем следует снять действие диагональной D и перестановочной P матриц и декодировать полученный вектор. В результате декодирования нужно выделить вектор ошибок e’ преобразовав его получить искомую информацию в виде вектора e (рис. 2).

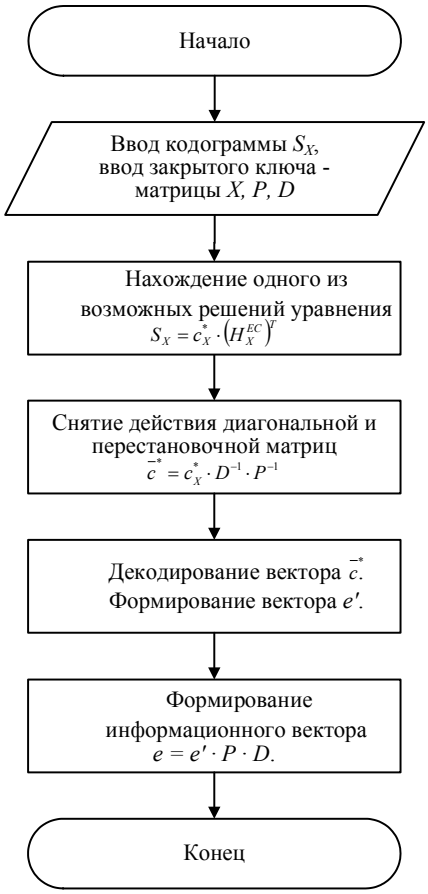

Рис. 2. Схема алгоритма расшифрования криптограммы

Алгоритм декодирования криптограммы представим в виде последовательности следующих шагов:

ШАГ 1. Ввод криптограммы S_X, подлежащей расшифрованияю. Ввод закрытого ключа – матрицы X, P, D.

ШАГ 2. Нахождение одного из возможных решений уравнения $S_X = c_X^* \cdot \left(H_X^{EC}\right)^T$.

ШАГ 3. Снятие действия диагональной и перестановочной матриц: $\bar{c}^* = c_X^* \cdot D^{-1} \cdot P^{-1}$.

ШАГ 4. Декодирование вектора $\bar{c}^*$. Формирование вектора *e’*.

ШАГ 5. Преобразование вектора e’: $e = e' \cdot P \cdot D$. Формирование искомого информационного вектора e.

Основным этапом разработанного алгоритма расшифрования криптограмм является декодирование вектора $\bar{c}^*$ (шаг 4). Сложность задачи декодирования эллиптического кода рассмотренным выше способом составляет $(4t^2 + (t^2 + t - 2)^2/4)$. Задача нахождения одного из возможных решений уравнения $S_X = c_X^* \cdot \left(H_X^{EC}\right)^T$ может быть решена, с помощью алгоритма, сложность которого не превышает $O(n^2)$. Сложность снятия и последующее наложение действия матриц P и D не превышает $O(n^2)$ операций (на каждую матрицу). Общая сложность расшифрования криптограмм в кодовой криптосистеме на эллиптических кодах составляет $(5 \cdot n^2 + 4t^2 + (t^2 + t - -2)^2/4)$ и является полиномиальной функцией от длины кода и его исправляющей способности.

Разработанные алгоритмы формирования и расшифрования криптограмм оперируют методами помехоустойчивого кодирования. Так, при формировании сообщения M_i участвуют алгоритмы равновесного кодирования, которые, в свою очередь являются алгоритмами избыточного (помехоустойчивого) кодирования. Положим, что контроль ошибок в режиме автоматического переспроса осуществляется на уровне равновесного кодирования. Тогда рассмотренная выше криптосистема позволяет осуществлять комплексную крипто-кодовую защиту информации. Злоумышленник, не зная секретного, не сможет вскрыть содержимое криптограммы (прочесть информационное сообщение), для него декодирование случайного кода – трудноразрешимая задача (экспоненциальной сложности). Напротив, уполномоченный абонент декодирует криптограмму по алгоритмам полиномиальной сложности. Декодер равновесного кода по принятому вектору *e* выдает решение о наличии или отсутствии ошибки в принятом информационном сообщении, по которому осуществляется управление процедурой автоматического переспроса.

Таким образом, использование разработанных алгоритмов позволяет выполнить задачу обмена секретными сообщениями между абонентами информационного обмена с использованием кодовых криптосистем на эллиптических кодах в каналах с автоматическим переспросом.

Выводы

В результате проведенных исследований кодовых криптосистем на эллиптических кодах разработаны алгоритмы несимметричного криптографического преобразования информации для каналов с автоматическим переспросом. Разработанные алгоритмы оперируют методами помехоустойчивого кодирования, в том числе, при формировании сообщения M_i участвуют алгоритмы равновесного кодирования. Декодер равновесного кода по принятой последовательности выдает решение о наличии или отсутствии ошибки в принятом информационном сообщении и осуществляет управление процедурой автоматического переспроса. **Перспективным направлением** дальнейших исследований является экспериментальная проверка полученных результатов, разработка и апробация имитационной модели крипто-кодовой защиты информации на эллиптических кодах в каналах с автоматическим переспросом.

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. H. Niederreiter. Knapsack-Type Cryptosystems and Algebraic Coding Theory. // Probl. Control and Inform. Theoty. – 1986. –V.15. – P. 19-34.

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

4. Стасев Ю.В., Кузнецов А.А. Несимметричные теоретико-кодовые схемы с использованием алгеброгеометрических кодов // Кибернетика и системный анализ: Международный научно-теоретический журнал. – К.: НАНУ. – 2005. – № 3. – С. 47-57.

5. Евсеев С.П. Несимметричный алгоритм шифрования с использованием эллиптических кодов. // Проблеми інформатики і моделювання. Матеріали четвертої міжнародної науково-технічної конференції. – Х.: НТУ „ХПІ". – 2004. – С.12.

6. Евсеев С.П. Несимметричные криптосистемы на эллиптических кодах для каналов с автоматическим переспросом. // Системи обробки інформації. – Х.: ХУ ПС, 2007. – Вип. 5(630. – С. 134-137.

Поступила в редколлегию 16.07.2007

Рецензент: д-р техн. наук, проф. С.В. Смеляков, Харьковский университет Воздушных Сил им. И. Кожедуба, Харьков.