

УДК 681.3.06

С.П. Евсеев

Харьковский университет Воздушных Сил им. И. Кожедуба, Харьков

НЕСИММЕТРИЧНЫЕ КРИПТОСИСТЕМЫ НА ЭЛЛИПТИЧЕСКИХ КОДАХ ДЛЯ КАНАЛОВ С АВТОМАТИЧЕСКИМ ПЕРЕСПРОСОМ

Рассматриваются криптосистемы, построенные с использованием алгебраических блочных кодов, стойкость которых обосновывается сложностью декодирования случайного кода. Предлагаются криптосистемы на эллиптических кодах для каналов с автоматическим переспросом.

несимметричные криптосистемы, эллиптические коды, автоматический переспрос

Постановка проблемы в общем виде и анализ литературы

Защита информации от несанкционированного доступа злоумышленником может реализовываться несколькими способами [1]. Основным и наиболее эффективным подходом является криптографическая защита [2, 3].

Проведенный анализ [4 – 8] показал, что перспективным направлением в развитии несимметричных криптоалгоритмов являются кодовые конструкции с быстрыми (алгебраическими) алгоритмами декодирования, функционирующие в режиме маскирования кодовых слов под случайную последовательность. Для неуполномоченного пользователя (злоумышленника) несанкционированный доступ к информационной части сообщения сопряжен с решением теоретико-сложностной задачи декодирования случайного кода. Уполномоченный пользователь, владеющий секретным ключом, декодирует полученную последовательность быстрыми (алгебраическими) алгоритмами. Этот подход позволяет стоять крипто-кодовые преобразования для комплексного повышения безопасности и достоверности передачи данных в каналах с прямым исправлением ошибок [8]. В тоже время большая часть современных модемных протоколов коррекции ошибок функционирует в режиме автоматического переспроса. Следовательно, актуальным направлением исследований является разработка несимметричных кодовых криптосистем для каналов с автоматическим переспросом.

Несимметричная кодовая криптосистема Нидеррайтера

В работе [5] впервые предложена кодовая криптосистема, основанная на маскировании проверочной матрицы алгебраического блочного кода. Рассмотрим особенности построения этой криптосистемы, исследуем возможные пути ее использования в каналах с автоматическим переспросом.

Пусть H – проверочная матрица линейного (n, k, d) кода над $GF(q)$ с полиномиальной сложностью

декодирования. Пусть X – невырожденная $r \times r$ -матрица над $GF(q)$, D – диагональная матрица с ненулевыми элементами на диагонали, P – перестановочная матрица размера $n \times n$. Открытым ключом в схеме Нидеррайтера является матрица $H_X = X \cdot H \cdot P \cdot D$, секретным (закрытым) ключом являются матрицы X, P, D . Закрытая информация (кодограмма) S_X представляет собой вектор длины $r = n - k$ и вычисляется по правилу $S_X = e \cdot H_X^T$, где вектор e – вектор длины n и веса $\leq t$, который несет конфиденциальную информацию (информационное сообщение, подлежащее закрытию).

Уполномоченный пользователь (имеющий секретный ключ) находит одно из q^k решений выражения $S_X = c_X^* \cdot H_X^T$. Найденное решение – суть кодовое слово c с ошибками $c_X^* = i \cdot G_X + e$. Далее, уполномоченный пользователь строит вектор $\bar{c}^* = c_X^* \cdot D^{-1} \cdot P^{-1}$, декодирует полученное слово и вычисляет кодовое слово $c' = i' \cdot G$, а затем и вектор ошибок $e' = \bar{c}^* - c'$. На последнем шаге производится вычисление вектора $e = e' \cdot P \cdot D$, который несет конфиденциальную информацию.

Таким образом, в теоретико-кодовой схеме Нидеррайтера основным средством маскировки линейного (n, k, d) кода с полиномиально разрешимой задачей декодирования также являются матрицы X, P, D . В работах [4 – 7] исследованы несимметричные криптосистемы, построенные по кодам Гоппы, Рида-Соломона, Рида-Маллера. В тоже время, в работе [7] показано, что криптосистемы на обобщенных кодах Рида-Соломона уязвимы быстрой атаке, основанной на особенных свойствах группы автоморфизмов кода. Перспективным направлением считается использование криптосистем на алгеброгеометрических кодах [7].

Несимметричная кодовая криптосистема на эллиптических кодах

Алгеброгеометрические коды – линейные системы на алгебраических кривых впервые предложены

ны в работе [9]. В работе [10] показано, что кодовые соотношения таких кодов асимптотически лежат выше нижней теоретической границы Варшамова-Гилберта.

Наиболее простой случай алгеброгеометрических кодов – линейные системы на эллиптических кривых (эллиптические коды).

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

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

где $c_i \in GF(q)$, $d \geq \alpha - 2g + 2$, $\alpha = \deg X \cdot \deg F$.

Это определение равносильно матричному представлению алгеброгеометрического кода:

$$H(c_0, c_1, \dots, c_{n-1})^T = 0,$$

где H – проверочная матрица кода размерности $r \times n$, $r = n - k = d + g - 2$

$$H = \begin{pmatrix} F_0(P_0) & F_0(P_1) & \dots & F_0(P_{n-1}) \\ F_1(P_0) & F_1(P_1) & \dots & F_1(P_{n-1}) \\ \dots & \dots & \dots & \dots \\ F_{r-1}(P_0) & F_{r-1}(P_1) & \dots & F_{r-1}(P_{n-1}) \end{pmatrix} = \|F_j(P_i)\|_{n,r}. \quad (2)$$

Утверждение. Эллиптический (n, k, d) код над $GF(q)$, построенный через проверочную матрицу связан характеристиками $k + d \geq n$, причем: $n \leq 2\sqrt{q} + q + 1$, $k \geq n - \alpha$, $d \geq \alpha$, $\alpha = 3 \cdot \deg F$.

Конструктивные характеристики эллиптических кодов, построенных через проверочную матрицу, приведены в табл. 1.

Таблица 1

Конструктивные кодовые характеристики эллиптических кодов

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

Определение и результат утверждения позволяют сформировать несимметричную кодовую криптосистему на основе эллиптических кодов следующим образом.

Пусть H^{EC} – проверочная матрица эллиптического (n, k, d) кода над $GF(q)$ вида (2) и размерности $g \times n$, $r = \alpha$, $\alpha = 3 \cdot \deg F$. Пусть X – невырожденная $k \times k$ -матрица над $GF(q)$, D – диагональная матрица с ненулевыми на диагонали элементами, P – перестановочная матрица размера $n \times n$. Тогда несимметричная кодовая криптосистема на эллиптических кодах задается совокупностью множеств:

- множество открытых текстов $M = \{M_1, M_2, \dots, M_\mu\}$, где $M_i = (e_0, e_1, \dots, e_{n-1})$,

$$\forall e_j \in GF(q), w(M_i) \leq t = \left\lfloor \frac{(d-1)}{2} \right\rfloor;$$

- 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 $\Phi = \{\phi_1, \phi_2, \dots, \phi_s\}$, где $\phi_i: M \rightarrow E$, $i = 1, 2, \dots, s$;

- множество обратных отображений $\Phi^{-1} = \{\phi_1^{-1}, \phi_2^{-1}, \dots, \phi_s^{-1}\}$, где $\phi_i^{-1}: E \rightarrow M$, $i = 1, 2, \dots, s$;

- множество ключей, параметризующих прямые отображения

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

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

– множество ключей, параметризующих 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). Схема передачи секретного сообщения от абонента А к абоненту Б в несимметричной схеме с использованием эллиптических кодов представлена на рис. 1.

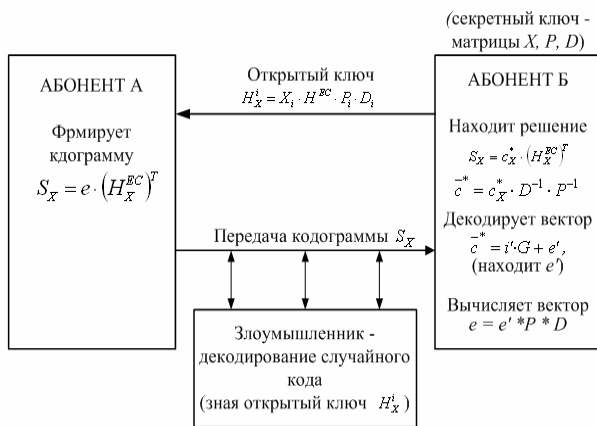


Рис. 1. Схема передачи кодограммы в несимметричной криптосистеме с эллиптическими кодами

Передача криптограммы в данной криптосистеме предваряется следующими операциями. Абонент Б случайно, равномерно, независимо от других абонентов формирует матрицы X, P, D и хранит их в секрете (закрытый ключ). Вычисляет матрицу $H_X^i = X_i \cdot H^{EC} \cdot P_i \cdot D_i$ и публикует ее как открытый (общедоступный) ключ.

Абонент А для отправки секретного сообщения формирует криптограмму.

$$E_j = (S_{X_0}, S_{X_1}, \dots, S_{X_{n-k-1}}) = M_j \cdot H_X^i =$$

$$= (e_0, e_1, \dots, e_{n-1}) \cdot \begin{pmatrix} h_{X_{0,0}} & h_{X_{0,1}} & \dots & h_{X_{0,n-1}} \\ h_{X_{1,0}} & h_{X_{1,1}} & \dots & h_{X_{1,n-1}} \\ \dots & \dots & \dots & \dots \\ h_{X_{k-1,0}} & h_{X_{k-1,1}} & \dots & h_{X_{k-1,n-1}} \end{pmatrix}.$$

Ее может сформировать (зашифровать отправляемую информацию) любой пользователь, знающий публичный (общедоступный) ключ.

Секретное сообщение M_i – суть специально подготовленный набор данных, удовлетворяющий следующему ограничению:

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

$$w(M_i) \leq t = \lfloor (d-1)/2 \rfloor.$$

Таким образом, в 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-кодую защиту информации. Злоумышленник, не зная секретного ключа абонента Б, не сможет вскрыть содержимое криптограммы (прочитать информационное сообщение), для него декодирование случайного кода – трудноразрешимая задача (экспоненциальной сложности). Напротив, абонент Б декодирует криптограмму по алгоритмам полиномиальной сложности. Действительно, уполномоченный пользователь (имеющий секретный ключ) находит одно из q^k решений выражения $S_X = c_X^* \cdot H_X^T$. Найденное решение – суть кодовое слово с ошибками $c_X^* = I \cdot G_X + e$. Далее уполномоченный пользователь строит вектор $\bar{c}^* = c_X^* \cdot D^{-1} \cdot P^{-1}$ и декодирует полученное слово. Однако, вместо восстановления информационного слова I' , он вычисляет кодовое слово $c' = I' \cdot G$, а затем и вектор ошибок $e' = \bar{c}^* - c'$. На последнем шаге производится вычисление вектора $e = e' \cdot P \cdot D$, который несет конфиденциальную информацию. 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, разработанный подход как совокупность установленных процедур и правил позволяет за конечное число определенных действий выполнить задачу обмена секретными сообщениями между абонентами информационного обмена с использованием кодовых криптосистем на эллиптических кодах в каналах с автоматическим переспросом.

Выводы

В ходе проведенных исследований рассмотрены криптосистемы, построенные с использованием алгебраических блочных кодов, стойкость которых обосновывается сложностью декодирования случайного кода. Предложены криптосистемы на эллиптических кодах, которые функционируют в режиме маскирования кодовых слов под случайную последовательность и позволяют обеспечить безопасность и достоверность передачи данных в каналах с автоматическим переспросом.

Перспективным направлением исследований является разработка алгоритмов шифрования и расшифрования, исследование протоколов обмена секретными сообщениями с использованием предложенных криптосистем.

Список літератури

1. *Захист інформації в комп'ютерних системах від несанкціонованого доступу / За ред. С.Г. Лаптева.* – К., 2001. – 321 с.
2. Шеннон К. Теория связи в секретных системах // Шеннон К. Работы по теории информации и кибернетике. – М.: Изд-во иностранной литературы. – 1963. – С. 333-402.
3. Horst Feistel. *Cryptography and Computer Privacy.* // *Scientific American.* – May 1973. – Vol. 228, No. 5. – P. 15-23.
4. McEliece R.J. *A Public-Key Cryptosystem Based on Algebraic Theory* // *DGN Progres Report 42-44, Jet Propulsi on Lab. Pasadena, CA. January- February, 1978.* – P. 114-116.
5. Niederreiter H. *Knapsack-Type Cryptosystems and Algebraic Coding Theory* // *Probl. Control and Inform. Theory.* – 1986. – V.15. – P. 19-34.
6. Rao T.R.N., Nam K.H. *Private-key algebraic-coded cryptosystem.* *Advances in Cryptology – CRYPTO 86, New York. – NY: Springer.* – P. 35-48.
7. Сидельников В.М. *Криптография и теория кодирования* // *Материалы конференции «Московский университет и развитие криптографии в России».* – М.: МГУ. – 2002. – 22 с.
8. 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.
9. Гоппа В.Д. *Коды на алгебраических кривых* // *Докл. АН СССР.* – 1981. – Т.259, № 6. – С. 1289-1290.
10. Влэдуц С.Г., Манин Ю.И. *Линейные коды и модулярные кривые* // *Современные проблемы математики.* – М.: ВИНТИ. – 1984. – Т. 25. – С. 209-257.

Поступила в редколлегию 10.04.2007

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