С. П. ЕВСЕЕВ, Харьковский национальный экономический университет
О.Н. МИСЮРА, Научный центр Харьковского университета Воздушных Сил

КРИПТО-КОДОВЫЕ СИСТЕМЫ С ОТКРЫТЫМ КЛЮЧОМ НА АЛГЕБРАИЧЕСКИХ КОДАХ

Considered cryptosystems, built with use algebraic block codes, which stability is the casual code motivated by difficulty of the decoding. To set forth cryptosystems on elliptical code for channel with automatic negative acknowledgement. To develop algorithms of the asymmetrical cryptographic transformation to information for channel with automatic negative acknowledgement.

Обеспечение конфиденциальности и целостности передаваемых данных является одной из важнейших задач, стоящих при обмене информацией между пользователями. Для ее обеспечения наиболее эффективными являются криптографические методы.

Проведенный анализ [1-7] показал, что перспективным направлением в развитии несимметричных криптоалгоритмов для обеспечения конфиденциальности и целостности данных является применение криптосистем с быстрыми (алгебраическими) алгоритмами декодирования, функционирующими в режиме маскирования кодовых слов под случайную последовательность. При этом дешифрование информации для неуполномоченного пользователя (несанкционированный доступ к информационной части сообщения) является NP-полной задачей – декодирование случайного кода. Уполномоченный пользователь, владеющий секретным ключом, расшифровывает полученную последовательность быстрыми алгоритмами за полиномиальное время. Такие криптосистемы позволяют, интегрировано обеспечивать защиту и помехоустойчивость информационной части данных в каналах с прямым исправлением ошибок [3-7]. В то же время большая часть модемных протоколов коррекции ошибок функционирует в режиме автоматического переспроса. Для решения задачи обеспечения конфиденциальности и целостности данных предложена кодовая криптосистема Нидеррайтера, основанная на маскировании проверочной матрицы алгебраического блокового кода. Основное достоинство несимметричной криптосистемы состоит в высокой скорости преобразования информации (относительная скорость кодирования близка к 1). Для ее построения используются H – проверочная матрица линейного (n, k, d) кода над $GF(q)$ с полиномиальной сложностью декодирования; X – невырожденная r × r-матрица над $GF(q)$, D – диагональная матрица с ненулевыми элементами на диагонали, P – перестановочная матрица размера $n \times n$. Открытым ключом в криптосистеме Нидеррайтера является матрица $HX = X \cdot H \cdot P \cdot D$, 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 $\le t$, который несет конфиденциальную информацию (информационное сообщение, подлежащее закрытию).

В работах [1, 2] показано, что перспективным направлением считается использование криптосистемы на алгеброгеометрических кодах (АГК) [4-5]. Недвоичные алгебраические блоковые коды, построенные по алгебраическим кривым (алгеброгеометрические коды) обладают хорошими асимптотическими свойствами. Доказано, что при большой длине эти коды лежат выше границы Варшамова-Гилберта [2-5].

Разработаны алгоритмы шифрования и расшифрования информации, позволяющие уполномоченному пользователю производить криптографическую обработку информации за полиномиальное время. *Алгоритм формирования криптограммы* представим в виде последовательности следующих шагов:

шаг 1. Ввод информации, подлежащей шифрованию.

*шаг 2.*Ввод открытого ключа H_X^{EC} ;

шаг 3. Формирование вектора ошибок e, вес которого не превышает $\le t$ – 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 криптосистем с эллиптическими кодами составит ($r \times n$) операций сложения и умножения над $GF(q)$, что тождественно ($3 \cdot degF \times n$) или ($d \times n$). *Алгоритм декодирования криптограммы* представим в виде последовательности следующих шагов:

шаг 1. Ввод криптограммы S_X, подлежащей расшифрования. 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: $\overline{c}' = c'_X \cdot D^{-1} \cdot P^{-1}$;

шаг 4. Декодирование вектора $\overline{c}'$. Формирование вектора *e'*;

шаг 5. Преобразование вектора *e': e = e' · P · D*. Формирование искомого информационного вектора *e*. Основным этапом разработанного алгоритма расшифрования криптограмм является декодирование вектора $\overline{c}'$ (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.

Предложенные 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 для протоколов обмена секретными сообщениями с использованием предложенных криптосистем.

Литература:

1. H. Niederreiter. *Knapsack-Type Cryptosystems and Algebraic Coding Theory.* // Probl. Control and Inform. Theoty. – 1986. – V.15. – P. 19-34.
2. 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.
3. Кузнецов А.А., Евсеев С.П., Томашевский Б.П., Жмурко Ю.И. *Исследование протоколов и механизмов защиты информации в компьютерных системах и сетях*. // Збірник наукових праць ХУ ПС. – Харків: ХУПС. – 2007. – Вип. 2 (14). – С. 102-111.
4. Стасев Ю.В., Кузнецов А.А. *Несимметричные теоретико-кодовые схемы с использованием алгеброгеометрических кодов*. // Кибернетика и системный анализ: Международный научно-теоретический журнал. – Киев: НАНУ. – 2005. – № 3. – С. 47-57.
5. Евсеев С.П. *Несимметричные криптосистемы на эллиптических кодах для каналов с автоматическим переспросом*. // Збірник наукових праць ХУ ПС. – Харків: ХУПС. – 2007. – Вип. 5 (63). – С.134-137.
6. Евсеев С.П. *Несимметричные криптосистемы на ЭК для каналов с автоматическим переспросом*. // Збірник наукових праць ХУ ПС. – Харків: ХУПС. – 2007. – Вип. 5 (63). – С. 134-137.
7. Евсеев С.П. *Криптографическое преобразование информации в кодовых криптосистемах на эллиптических кодах для каналов с автоматическим переспросом*. // Збірник наукових праць ХУ ПС. – Харків: ХУПС. – 2007. – Вип. 8 (66). – С.29-32.