УДК 621.391

ИССЛЕДОВАНИЕ СВОЙСТВ НЕСИММЕТРИЧНЫХ ТЕОРЕТИКО-КОДОВЫХ СХЕМ С ЭЛЛИПТИЧЕСКИМИ КОДАМИ

к.т.н. А.А. Кузнецов, к.т.н. В.Н. Лысенко, С.П. Евсеев
(представил д.т.н., проф. О.Н. Фоменко)

Рассматриваются несимметричные криптосистемы, построенные с использованием теоретико-кодовых схем на эллиптических кодах. Проводится оценка параметров и исследование криптографических свойств несимметричных теоретико-кодовых схем с эллиптическими кодами.

Введение. Перспективным направлением современной криптографии является развитие несимметричных криптосистем, в которых для передачи ключевой информации не требуется организация закрытого канала связи. Особое место среди них занимают теоретико-кодовые схемы, основанные на использовании алгебраических кодов и обладающие существенным достоинством – высокой скоростью криптографического преобразования информации [1 – 6]. В работах [5 – 6] предложены несимметричные теоретико-кодовые схемы, основанные на использовании эллиптических кодов. **Актуальным** направлением их дальнейшего развития является исследование криптографических свойств.

1. Основные параметры теоретико-кодовых схем. Определим несимметричную криптосистему по схеме Мак-Элиса с эллиптическим кодом. Пусть X – невырожденная k × k-матрица над GF(2^m), D – диагональная матрица с ненулевыми на диогонали элементами, P – перестановочная матрица размера n × n. Тогда имеем [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 ≤ t.

Определим несимметричную криптосистему по схеме Нидеррайтера с эллиптическим кодом. Пусть X – невырожденная k × k-матрица над

$GF(2^m)$, D – диагональная матрица с ненулевыми на диагонали элементами, P – перестановочная матрица размера $n \times n$. Тогда имеем [5 – 6]: открытый ключ – матрица $H_X^{EC} = X \cdot H^{EC} \cdot P \cdot D$, секретный (закрытый) ключ – матрицы X, P, D. Шифрованная информация (криптограмма) представляет собой вектор длины n и вычисляется по правилу:

$$S_X = e \cdot \left(H_X^{EC}\right)^T,$$

где вектор e – вектор длины n и веса $\leq t$, который несет конфиденциальную информацию (информационное сообщение, подлежащее закрытию).

Проведем оценку параметров несимметричных криптосистем, построенных на основе теоретико-кодовых схем с использованием эллиптических кодов. Введем следующие обозначения: l_I – длина информационной последовательности, поступающей на вход теоретико-кодовой схемы (в битах); l_K – длина открытого ключа несимметричной криптосистемы (в битах); l_{K+} – длина закрытого ключа несимметричной криптосистемы (в битах); l_s – длина криптограммы (в битах); I_K – сложность формирования криптограммы (в групповых операциях); I_{SK} – сложность снятия криптограммы (в групповых операциях); I_{K+} – сложность решения задачи криптоанализа (в групповых операциях). Для несимметричных теоретико-кодовых схем введем также дополнительный параметр R – относительная скорость передачи.

Оценим параметры несимметричных криптосистем на основе теоретико-кодовых схем Мак-Эллиса с использованием эллиптических кодов. Длина информационной последовательности (в битах), поступающей на вход теоретико-кодовой схемы с алгебраическим (n, k, d) кодом над $GF(2^m)$ определяется следующим выражением:

$$l_I = k \cdot m. \quad (1)$$

Длина криптограммы (в битах) определяется выражением

$$l_s = n \cdot m. \quad (2)$$

Длина открытого ключа несимметричной криптосистемы (в битах) определяется суммой элементов матрицы G_X^{EC} и задается выражением

$$l_K = k \cdot n \cdot m. \quad (3)$$

Длина закрытого ключа несимметричной криптосистемы (в битах) на основе теоретико-кодовых схем определяется суммой элементов матриц X, P, D (в битах) и задается выражением

$$l_{K+} = n^2 \cdot k^2 \cdot m. \quad (4)$$

Сложность формирования криптограммы (количество групповых операций) при реализации систематического кодирования определяется как

$$I_K = (r + 1) \cdot n \quad (5)$$

и для несистематического кодирования

$$I_K = (k + 1) \cdot n. \quad (6)$$

Сложность снятия криптограммы определяется выражением

$$I_{SK} = 2 \cdot n^2 + k^2 + 4t^2 + (t^2 + t - 2)^2/4, \quad (7)$$

где t – исправляющая способность (n, k, d) кода.

Сложность решения задачи криптоанализа определяется наилучшим (самым простым по сложности реализации) алгоритмом декодирования случайного кода. Перестановочное декодирование представляет собой алгоритм последовательного преобразования кодового слова и перестановки символов, инвариантной относительно кода. Этот способ позволяет за конечное число шагов декодировать линейный блоковый код с произвольной структурой. Сложность задачи криптоанализа, как решение задачи декодирования случайного кода перестановочным декодером, будет определяться как

$$I_{K+} = N_{\text{покр}} \cdot n \cdot r. \quad (8)$$

Относительная скорость передачи в несимметричных криптосистемах Мак-Эллиса всегда меньше единицы:

$$R = l_I / l_s < 1.$$

Оценим параметры несимметричных криптосистем на основе теоретико-кодовых схем Нидеррайтера с использованием эллиптических кодов. Длина информационной последовательности определяется выражением

$$l_I \le m \cdot \log_{2^m} \left(\sum_{i=0}^{t} \left(C_n^t \right) \right), \quad t = \lfloor d - 1/2 \rfloor. \quad (9)$$

Длина криптограммы определяется выражением

$$l_s = r \cdot m. \quad (10)$$

Длина закрытого ключа несимметричной криптосистемы Нидеррайтера определяется выражением (4). Длина открытого ключа определяется суммой элементов матрицы H_X^{EC} и задается выражением:

$$l_K = r \cdot n \cdot m. \quad (11)$$

Сложность формирования криптограммы определяется выражением

$$I_K = r \cdot n. \quad (12)$$

Сложность снятия криптограммы определяется выражением (7). Сложность задачи криптоанализа, как решение задачи декодирования случайного кода перестановочным декодером, будет определяться выражением (9).

Проведем исследование свойств теоретико-кодовых схем на эллиптических кодах. Оценим сложность формирования криптограммы, сложность дешифрования, сложность взлома с помощью перестановочного декодирования случайного кода и объем открытого ключа по выражениям (1) – (12).

2. Исследование свойств теоретико-кодовых схем на эллиптических кодах. Зафиксируем относительную скорость передачи. Проведем исследование сложности формирования криптограммы в количестве груп-

повых операций от размерности поля и сложности дешифрования в теоретико-кодовой схеме с эллиптическими кодами. На рис. 1 представлены зависимости $I_K(m)$ для различных R в теоретико-кодовых схемах с эллиптическими кодами. На рис. 2 представлены зависимости $I_S(m)$ для различных R. Зависимости соответствуют значениям: $R_1 = 0{,}9$; $R_2 = 0{,}75$; $R_3 = 0{,}5$; $R_4 = 0{,}25$; $R_5 = 0{,}1$.

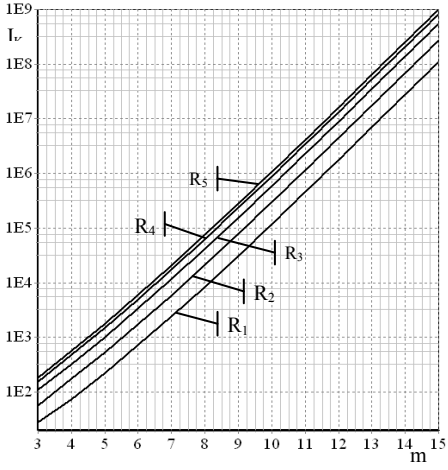

Рис.1. Зависимость сложности шифрования над $GF(2^m)$

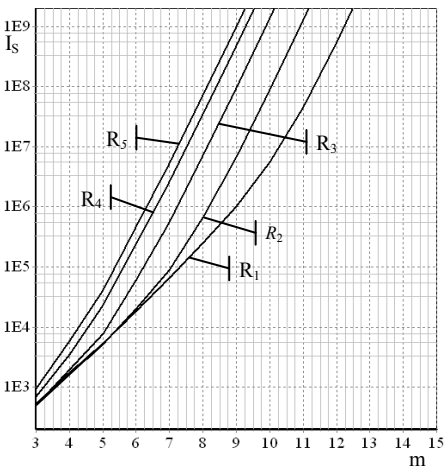

Рис. 2. Зависимость сложности дешифрования над $GF(2^m)$

Проведем исследование потенциальной стойкости теоретико-кодовых схем с эллиптическими кодами. На рис. 3 представлены зависимости $I_{K+}(m)$ для различных R. Наиболее стойкие к взлому методом перестановочного декодирования являются схемы использующие эллиптические коды с относительной скоростью $R \approx 0{,}5 - 0{,}75$. Зафиксируем конечное поле $GF(2^m)$, исследуем зависимость $I_{K+}(R)$. На рис. 4 представлены зависимости сложности взлома теоретико-кодовых схем от скорости эллиптических кодов над различными полями $GF(2^m)$, $m = 5, \ldots, 11$. На рис. 5 представлена сводная диаграмма сложности взлома и сложности шифрования теоретико-кодовых схем для различных скоростей эллиптических кодов. Расчеты производились над конечными полями $GF(2^m)$, $m = 2 - 15$; $R_1 = 0{,}9$; $R_2 = 0{,}75$; $R_3 = 0{,}5$; $R_4 = 0{,}25$; $R_5 = 0{,}1$. Проведем исследование зависимостей объема ключевых данных теоретико-кодовых схем. На рис. 6. представлены зависимости объема открытых ключевых данных теоретико-кодовых схем на эллиптических кодах для различных показателей стойкости.

Проанализируем зависимости, представленные на рис. 1 – 6. Теоретико-кодовые схемы, построенные по эллиптическим кодам, обладают высоким

быстродействием при формировании криптограмм (скорость шифрования) и их дешифрования (рис. 1 – 2). Несимметричные криптосистемы, построенные с использованием теоретико-кодовых схем на эллиптических кодах, потенциально являются криптографически стойкими (рис. 2 – 3). Однако они имеют недостаток – большой объем открытых ключевых данных (рис. 6).

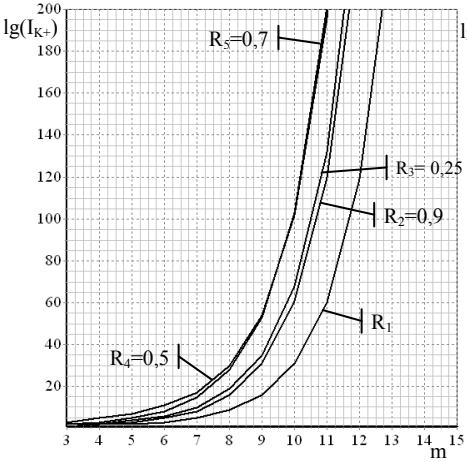

Рис. 3. Зависимость сложности взлома над GF(2^m) (R = const)

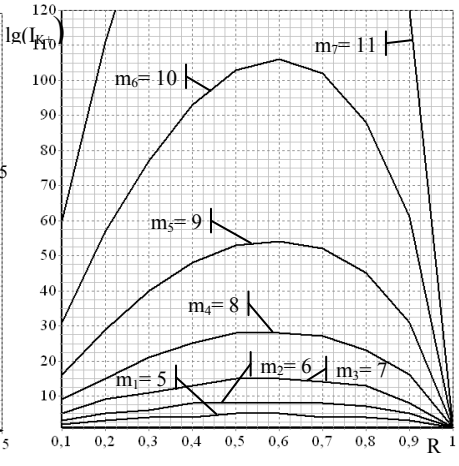

Рис. 4. Зависимость сложности взлома над GF(2^m) (m = const)

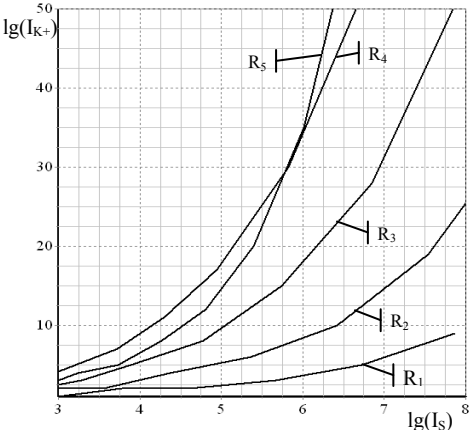

Рис. 5. Сводная диаграмма сложности взлома и сложности шифрования

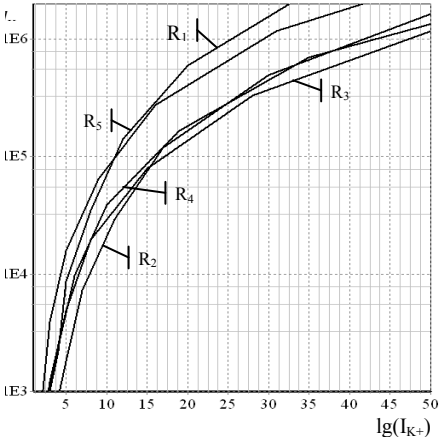

Рис. 6. Зависимости объема открытого ключа от показателя стойкости

Наименьшей затратностью ключевых данных обладают теоретико-кодовые схемы, построенные на эллиптических кодах с R ≈ 0,5.

Выводы. Как показали проведенные исследования, теоретико-кодовые схемы обладают высокими показателями быстродействия и потенциальной стойкости. Так, используя эллиптические коды с R = 0,5 над $GF(2^{10})$, можно построить несимметричную теоретико-кодовую схему со сложностью шифрования $< 10^{10}$ групповых операций. Для взлома такой криптосистемы злоумышленнику необходимо декодировать случайный код – выполнить $> 10^{100}$ операций (при перестановочном декодировании). Платой за такие параметры несимметричной теоретико-кодовой схемы являются большие объемы ключевых данных (в рассмотренном примере десятки мегабит). Таким образом, основным недостатком несимметричных криптосистем, построенных с использованием теоретико-кодовых схем, является большой объем ключевых данных.

Перспективным направлением дальнейших исследований является разработка методов снижения объема ключевых данных, разработка и исследование симметричных теоретико-кодовых схем на эллиптических кодах.

ЛИТЕРАТУРА

1. *McEliece R.J. A Public-Key Criptosystem Based on Algebraic Theory // DGN Progres Report 42 – 44, Jet Propulsi on Lab. Pasadena, CA. – 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 НТК «Московский ун-т и развитие криптографии в России». – 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 // Материалы межд. НТК 26 – 27 октября 2004 г. – Сумы: СМКЭС. – 2004. – С. 11 – 12.*

Поступила 16.08.2004

***КУЗНЕЦОВ Александр Александрович**, канд. техн. наук, ст. научн. сотр., начальник НДЛ ХУ ВС. В 1996 году окончил ХВУ. Область научных интересов – криптографическое преобразование информации, алгебраическая теория кодов и их применение в системах ПД.*

***ЛЫСЕНКО Валерий Николаевич**, канд. техн. наук, ст. научн. сотр. НЦ РВиА. В 1985 году окончил ХВВКИУРВ. Область научных интересов – криптографическое преобразование информации, алгебраическая теория кодов и их применение в системах ПД.*

***ЕВСЕЕВ Сергей Петрович**, адъюнкт ХУ ВС. В 2001 году окончил командно-штабной факультет ХВУ. Область научных интересов – криптографическое преобразование информации, алгебраическая теория кодов и их применение в системах ПД.*