УДК 621.391

ИССЛЕДОВАНИЕ ЭФФЕКТИВНОСТИ КРИПТОСИСТЕМ НА АЛГЕБРАИЧЕСКИХ БЛОКОВЫХ КОДАХ

А.А. Кузнецов
(Харьковский университет Воздушных Сил)

Рассматриваются криптосистемы, стойкость которых основана на трудноразрешимой задаче декодирования случайного кода. Исследована эффективность криптосистем, построенных на кодах Рида-Соломона, на алгеброгеометрических кодах по эллиптическим кривым, кривым Гурвица, Эрмита, Ферма, Сузуки.

кодирование, криптосистема, теоретико-сложностная задача

Постановка проблемы в общем виде, анализ литературы. Симметричные криптосистемы на алгебраических блоковых кодах (теоретико-кодовые схемы) впервые предложены в [1]. Их применение позволяет интегрировано (в один прием) обеспечивать безопасность информации и эффективно бороться с возникающими ошибками [2 – 5]. Целью статьи является исследование эффективности криптосистем на алгебраических блоковых кодах.

Показатели эффективности криптосистем на алгебраических блоковых кодах. Основными показателями эффективности криптосистем принято считать следующие: стойкость криптографического алгоритма, которую оценивают как сложность решения задачи криптоанализа наилучшим известным методом; объем ключевых данных, которые необходимо хранить в тайне от неавторизованного пользователя системы; сложность выполнения прямого и обратного криптографического преобразования, например, шифрование и дешифрование сообщений. Введем следующие обозначения: I_{K+} – сложность решения задачи криптоанализа (количество групповых операций); I_K – сложность формирования криптограммы (количество групповых операций); I_{SK} – сложность снятия криптограммы (количество групповых операций).

Проанализируем перечисленные показатели. Стойкость криптографического алгоритма лежащего в основе криптосистем на алгебраических блоковых кодах базируется на решении трудноразрешимой задачи декодирования случайного кода [1 – 5]. Следовательно, задача поиска хорошего (в смысле вычислительной сложности) алгоритма криптоана-

лиза сводится к задаче поиска хорошего алгоритма декодирования случайного кода. Декодирование произвольного линейного кода (кода общего положения) является сложной вычислительной задачей. Для корреляционного декодирования (n, k, d) кода над GF(q) необходимо, в общем случае, сравнить принятую последовательность со всеми разрешенными кодовыми словами и выбрать ближайшее (в метрике Хемминга), т.е. мощность множества слов-кандидатов составит $N_K = q^k$. Даже для небольших n, k, d и q задача корреляционного декодирования весьма трудоемка и, очевидно, методы криптоанализа на его основе малоэффективны.

Одним из наиболее эффективных подходов к декодированию линейного блокового кода с произвольной внутренней структурой является перестановочный метод [6 – 7]. Задача перестановочного декодера состоит в том, чтобы найти проверочное множество, которое покрывает неизвестную комбинацию ошибок. Наименьшее количество множеств, которые могут исправить все комбинации из t ошибок, ограничивается следующим выражением [7]:

$$N_{\text{покр}} \geq \frac{C_n^t}{C_{n-k}^t} = \frac{n(n-1)\ldots(n-t-1)}{(n-k)(n-k-1)\ldots(n-k-t-1)}.$$

Для вычисления синдромной последовательности для каждого слова-кандидата необходимо выполнить $n \cdot r$ операций (при матричном умножении слова-кандидата на проверочную матрицу).

Таким образом, сложность задачи криптоанализа как решение задачи декодирования случайного кода перестановочным декодером будет определяться выражением

$$I_{K+} = N_{\text{покр}} \cdot n \cdot r.$$

Формирование криптограммы соответствует вычислению кодового слова замаскированного кода с последующим добавлением случайного вектора ошибок [1 – 5].

Если код задан порождающей матрицей G, то для формирования кодового слова достаточно умножить информационный вектор длины k символов на матрицу G. Сложность реализации этой процедуры составит $k \cdot n$ операций сложения и умножения над конечным полем [6 – 7]. Сложность операции добавления случайного вектора ошибок к кодовому слову составит n операций сложения. Следовательно, запишем:

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

Сложность снятия криптограммы определяется сложностью алгебраического алгоритма декодирования алгебраического блокового кода. Для кодов БЧХ, кодов Рида-Соломона и их обобщений (ОРС), альтернантных кодов и их подклассов, локализация ошибок сводится к решению системы линейных уравнений от t неизвестных, где t – исправляющая способность соответствующего кода [6 – 7]. Для нахождения значений ошибок (для недвоичных кодов) необходимо дополнительно решить еще одну систему линейных уравнений от t неизвестных. Следовательно, для кодов ОРС запишем:

$$I_{SK} = 2 \cdot t^2.$$

Для алгеброгеометрических кодов сложность декодирования определяется следующим выражением [8]:

$$I_{SK} = 4t^2 + (t^2 - t)^2/4.$$

Оценка эффективности теоретико-кодовых схем. Зафиксируем конечное поле $GF(2^m)$ и блоковый (n, k, d) код с относительной скоростью кодирования R. Рассмотрим криптосистемы, построенные по кодам ОРС и по алгеброгеометрическим кодам, заданных на эллиптических кривых (EC), кривых Гурвица (HurC), Эрмита (HC), Ферма (FC), Сузуки (SC) [9]. Проведем оценку отношения сложности взлома к сложности дешифрования I_{K+} / I_{SK}.

На рис. 1 – 4 приведены зависимости I_{K+} / I_{SK} для случаев: 1) коды по SC, 2) коды по FC, 3) коды по HC, 4) коды по HurC, 5) коды по EC, 6) коды ОРС.

Приведенные на рис. 1 – 4 зависимости показывают, что криптосистемы на алгебраических блоковых кодах обладают высокой криптографической стойкостью при небольших вычислительных затратах на формирование/дешифрование криптограммы. Наибольшую стойкость к взлому криптосистемы методом перестановочного декодирования обладают теоретико-кодовые схемы на алгеброгеометрических кодах, заданных по кривым Сузуки, Ферма, Эрмита.

Выводы. Проведенные исследования показали, что криптосистемы на алгебраических блоковых кодах обладают высокими криптографическими свойствами. Их применение позволяет эффективно использовать теоретико-сложностную задачу декодирования случайного кода и получать большие значения I_{K+} / I_{SK}. Отношение I_{K+} / I_{SK} возрастает при переходе к кодам, построенным над полями бóльшей мощности. Для получения больших значений I_{K+} / I_{SK} наиболее предпочтительно использовать коды с $R \approx 0{,}5$.

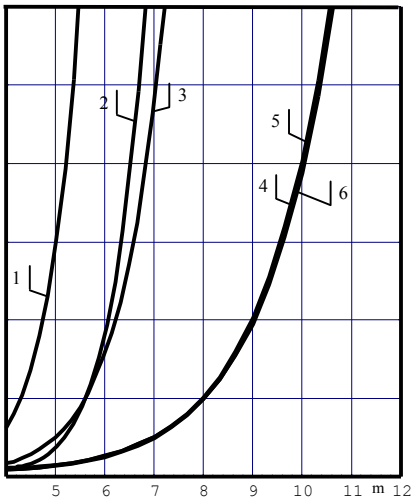

Рис. 1. Отношение I_{K+}/I_{SK} в криптосистеме на кодах с R = 0,1

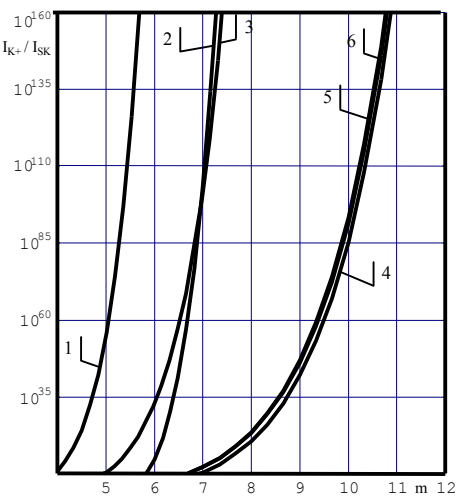

Рис. 2. Отношение I_{K+}/I_{SK} в криптосистеме на кодах с R = 0,25

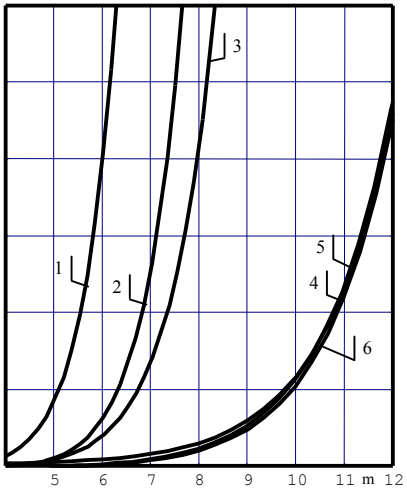

Рис. 3. Отношение I_{K+}/I_{SK} в криптосистеме на кодах с R = 0,5

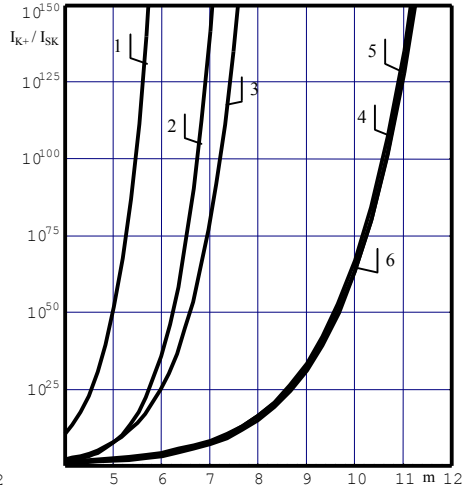

Рис. 4. Отношение I_{K+}/I_{SK} в криптосистеме на кодах с R = 0,75

Перспективным направлением является исследование возможностей теоретико-кодовых схем по интегрированному обеспечению безопасности и достоверности информации.

ЛИТЕРАТУРА

1. *Rao T.R.N. and Nam K. H.. Private-key algebraic-coded cryptosystem. Advances in Cryptology – CRYPTO 86, New York. – NY: Springer. – 1986. – P. 35 – 48.*
2. *Халимов Г.З., Буханцов А.Д. Применение помехоустойчивого кодирования для обеспечения безопасности каналов передачи данных // Труды международной НТК «Передача, обработка и отображение информации» / Под ред. А.В. Королёва. – Х.: НАНУ, ПАНИ. – 1994. – С. 28.*
3. *Халимов Г.З., Северинов А.В. Обеспечение безопасности каналов передачи данных на основе помехоустойчивых кодов // Системы управления и связь. – Х.: ХВУ. – 1996. – С. 116 – 119.*
4. *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.*
5. *Кузнецов А.А., Лысенко В.Н., Евсеев С.П. Метод повышения безопасности и помехоустойчивости каналов передачи данных // Материалы международной НТК 26-27 октября 2004 г. – Сумы: СМКЭС. – 2004. – С. 11 – 12.*
6. *Блейхут Р. Теория и практика кодов, контролирующих ошибки. – М.: Мир, 1986. – 576 с.*
7. *Кларк Дж.-мл., Кейн Дж. Кодирование с исправлением ошибок в системах цифровой связи: Пер. с англ. / Под ред. Б.С. Цыбакова. – М.: Радио и связь, 1987. – 392 с.*
8. *Кузнецов А.А., Северинов А.В., Задворный Д.А. Лысенко В.Н. Алгебраическое декодирование кодов по кривым Эрмита // Вісник ХПІ. – Х.: НТУ "ХПІ". – 2003. – № 26. – С. 95 – 102.*
9. *Кузнецов А.А. Несимметричные криптосистемы на алгеброгеометрических кодах // Системи обробки інформації. – Х.: ХВУ. – 2005. – Вип. 1 (41). – С. 65 – 71.*

Поступила 11.04.2005

Рецензент: доктор технических наук, профессор Ю.В. Стасев,
Харьковского университета Воздушных Сил.