УДК 621.391

АНАЛИЗ ПЕРСПЕКТИВНЫХ НАПРАВЛЕНИЙ В РАЗВИТИИ МЕТОДОВ ИНТЕГРИРОВАННОГО ОБЕСПЕЧЕНИЯ КОНФИДЕНЦИАЛЬНОСТИ И ДОСТОВЕРНОСТИ ПЕРЕДАЧИ ДАННЫХ

В.И. Грабчак, *канд. техн. наук;*
А.П. Мельник*
Львовский институт Сухопутных войск Национального университета "Львовская политехника", г. Львов;
**Научный центр БП РВ и А Сумского государственного университета, г. Сумы*

В статье исследуются методы маскирования алгебраических блоковых кодов с быстрым алгоритмом декодирования под случайный код (код общего положения), анализируются перспективные направления их развития.

Ключевые слова: *алгебраический, алгеброгеометрический код, блоковый код, процедура кодирования и декодирования.*

У статті досліджуються методи маскування алгебраїчних блокових кодів з швидким алгоритмом декодування під випадковий код (код загального положення), аналізуються перспективні напрямки їх розвитку.

Ключові слова: *алгебраїчний, алгеброгеометричний код, блоковий код, процедура кодування та декодування.*

ПОСТАНОВКА ПРОБЛЕМЫ В ОБЩЕМ ВИДЕ И АНАЛИЗ ЛИТЕРАТУРЫ

Одним из наиболее эффективных средств защиты передаваемых данных от возникающих ошибок являются методы помехоустойчивого кодирования, суть которого состоит во внесении по определенному алгоритму в передаваемые данные избыточности (проверочной части) [1, 2].

Первое направление в развитии теории кодов носит вероятностный характер и привело к появлению неблоковых кодов бесконечной длины, которые можно описать деревом и декодировать с помощью алгоритмов поиска по дереву. Наибольшее распространение среди древовидных методов получило сверточное кодирование. Эти коды, принадлежащие к подклассу линейных непрерывных кодов, можно генерировать с помощью цепей линейных регистров сдвига.

Второе направление базируется на алгебраических методах и преимущественно оперирует блоковыми кодами. Наибольшее распространение среди блоковых кодов нашли коды с проверкой на четность, с повторением символов, равновесные коды, коды Хемминга, коды Рида-Малера и наиболее обширный класс кодов – циклические коды. К последнему классу принадлежат коды Боуза-Чоудхури-Хоквингема (БЧХ) и коды Рида-Соломона (РС), получившие наибольшее распространение в технике связи. Наиболее полно основы алгебраической теории кодов изложены в [1, 2].

Одним из основных и наиболее эффективных средств обеспечения конфиденциальности являются методы криптографического (специального) преобразования данных [4, 5, 6]. Развитие методов обеспечения конфиденциальности также шло по нескольким направлениям (рис.1). Каждое направление тесно связано с категорией обеспечиваемой стойкости [5].

Первое направление, самое развитое и наиболее изученное, оперирует преимущественно статистическими параметрами оценки стойкости криптографической системы [4]. Это практически все симметричные криптографические системы, построение которых основано на комбинировании простых (элементарных, базовых) блоках преобразований (блоках подстановки и блоках перестановки) [4, 5, 6]. Шифрограмма (криптограмма) формируется путем многократного выполнения одинаковых групп преобразований, в результате чего удается обеспечить высокий уровень перемешивания и рассеивания информационных блоков данных, т.е. получить хорошие статистические показатели преобразования.

Оценка криптографической стойкости оценивается путем статистического тестирования, а сами криптографические системы такого рода получили общее название систем временной стойкости. Очевидным преимуществом систем временной стойкости является высокая скорость преобразования и простота их реализации.

Существенным недостатком является отсутствие строгого математического обоснования криптографической стойкости.

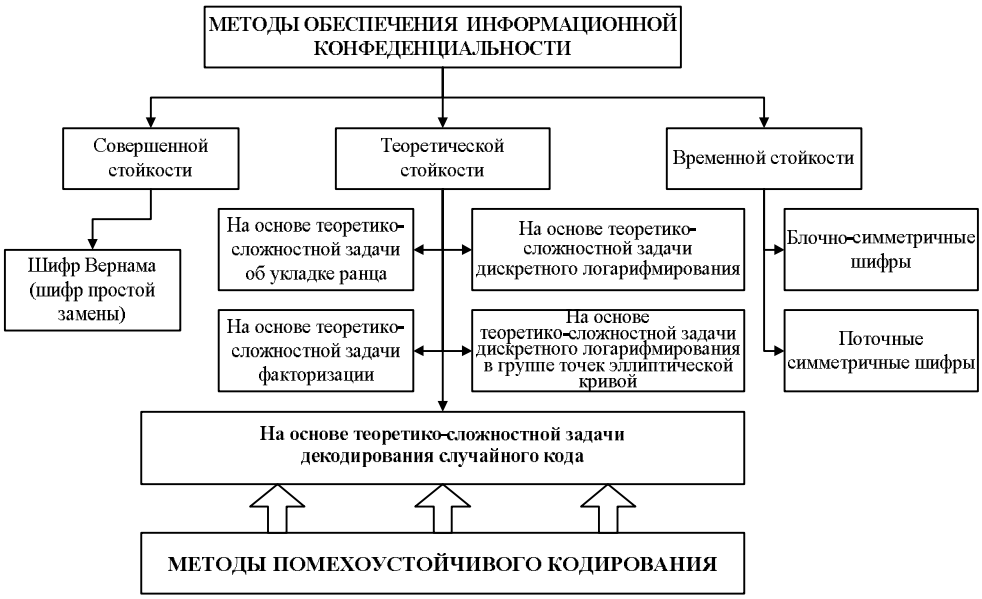

Рисунок 1 – Классификация методов обеспечения конфиденциальности по категориям стойкости

В отличие от криптографических систем временной стойкости шифр простой замены (шифр Вернама) обеспечивает совершенную стойкость [4, 5]. Это понятие введено в классических работах К. Шеннона и подразумевает равенство априорной и апостериорной вероятностей формирования криптограммы [4]. К сожалению, необходимыми условиями построения совершенной криптографической системы является большой объем ключевых данных, по крайней мере не меньший мощности множества сообщений и равновероятное формирование ключевых данных.

Третьим направлением являются криптографические системы теоретической стойкости, в которых задача взлома ключевых данных сводится к решению известной математической задачи [5]. Как правило, это несимметричные криптографические системы, сложность взлома которых сведена к решению одной из следующих задач:

– теоретико-сложностная задача об укладке ранца;
– теоретико-сложностная задача факторизации числа;
– теоретико-сложностная задача дискретного логарифмирования;
– теоретико-сложностная задача дискретного логарифмирования в группе точек эллиптической кривой;
– теоретико-сложностная задача декодирования случайного кода.

Очевидным преимуществом криптографических систем теоретической стойкости является строгое математическое обоснование криптографической стойкости и возможность, в некоторых случаях, построить криптографическую систему с открытым ключом [5]. К недостатком большинства криптографических систем теоретической стойкости следует отнести высокую сложность криптографического преобразования [5]. Исключением являются криптографические системы, основанные на сведении задачи взлома ключевых данных к решению теоретико-сложностной задачи декодирования случайного кода [5, 7]. В некоторых источниках они получи название теоретико-кодовых схем [7]. Их практическое использование позволяет реализовать в одном устройстве методы канального кодирования и специального преобразования данных.

Целью статьи является анализ методов маскирования алгебраических блоковых кодов с быстрым алгоритмом декодирования под случайный код (код общего положения), а также исследование перспективных направлений их развития.

АНАЛИЗ МЕТОДОВ ОБЕСПЕЧЕНИЯ КОНФИДЕНЦИАЛЬНОСТИ И ДОСТОВЕРНОСТИ ПЕРЕДАЧИ ДАННЫХ, ОСНОВАННЫХ НА ИСПОЛЬЗОВАНИИ АЛГЕБРАИЧЕСКИХ БЛОКОВЫХ КОДАХ

Общая классификация известных методов построения теоретико-кодовых схем приведена на рис. 2. Дадим общее определение теоретико-кодовой схемы [7,8].

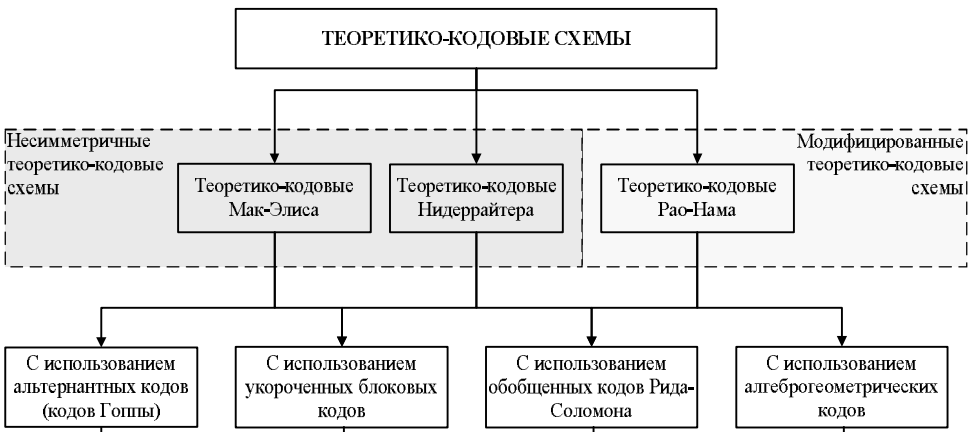

Рисунок 2 – Классификация методов построения теоретико-кодовых схем

Пусть G – порождающая матрица линейного (n, k, d) кода над $GF(q)$ с полиномиальной сложностью декодирования. Пусть X – невырожденная $k \times k$-матрица над $GF(q)$, D – диагональная матрица с ненулевыми на диагонали элементами, P – перестановочная матрица размера $n \times n$.

Перестановочная матрица реализует перестановку координат вектора в виде матричного умножения, а именно, элемент p_{ij} матрицы P равен 1

тогда и только тогда, когда координата с номером i переходит посредством перестановки в координату с номером j. В остальных случаях $p_{ij} = 0$. Таким образом, матрица P содержит в каждом столбце и в каждой строке только одну единицу. Произведение матриц $\Lambda = P \cdot D$ задает перестановочную матрицу Λ с ненулевыми элементами поля $GF(q)$. Перестановочная матрица Λ (унипотентная матрица) при перестановке координат вектора сохраняет расстояние по Хеммингу, т.е. $d(a, b) = d(a \cdot \Lambda, b \cdot \Lambda)$, где $d(x, y)$ – расстояние по Хеммингу между векторами x и y.

Открытым ключом в криптографической системе Мак-Элиса [8] является матрица $G_X = X \cdot G \cdot P \cdot D$, секретным (закрытым) ключом являются матрицы X, P, D.

Шифрованная информация (криптограмма) в теоретико-кодовой схеме представляет собой вектор длины n и вычисляется по правилу

$$c_X^* = I \cdot G_X + e\,, \qquad (1)$$

где $c_X = I \cdot G_X$ – вектор принадлежащий (n, k, d) коду с порождающей матрицей G_X;

I – k-разрядный информационный вектор, $I = \{I_1, I_2, ..., I_k\}$;

$e = \{e_1, e_2, ..., e_n\}$ – секретный (случайный) вектор ошибок веса $\le t$.

Противнику необходимо декодировать криптограмму c_X^* с известной порождающей матрицей $G_X^i \in K$. Не зная набор матриц $\{X, P, D\}_i \in K^*$ противник не может воспользоваться алгоритмом декодирования полиномиальной сложности. Декодирование случайного кода большой длины вычислительно недоступно (экспоненциальная сложность при корреляционном декодировании). Для уполномоченного пользователя (знающего секретный ключ) декодирование криптограммы – полиномиально разрешимая задача. Действительно, легитимный пользователь, получив вектор c_X^*, строит вектор $\bar{c}^* = c_X^* \cdot D^{-1} \cdot P^{-1}$.

Унипотентная матрица $\Lambda = P \cdot D$ сохраняет вес по Хеммингу вектора e. Практически, это означает, что вектор $\bar{c}^*$ является кодовым словом кода с порождающей матрицей G, искаженный не более чем в t разрядах. Далее уполномоченный пользователь, пользуясь алгоритмом полиномиальной сложности, декодирует вектор $\bar{c}^* = i' \cdot G + e'$, т.е. находит i'.

Достоинство схемы Мак-Элиса состоит в несимметричности протокола – ключ прямого преобразования открыт и может быть использован любым абонентом. Напротив, ключ обратного преобразования, который скрывает алгоритм быстрого декодирования, известен только уполномоченному пользователю. Следовательно, для организации обмена конфиденциальными сообщениями не требуется закрытого канала связи (канала фельдъегерской почты), обмен открытыми ключами может быть осуществлен по открытым каналам связи.

Основным недостатком схемы Мак-Элиса является большой объем ключевых данных. Действительно, для хранения и передачи открытого ключа необходим большой объем данных – $k \times n$ символов из $GF(q)$. Для рекомендованных параметров схемы объем ключа составляет ≈1 Мбит. Для хранения секретного ключа – матриц X, P, D требуется такой же объем памяти.

В работе [9] предложена схема Рао-Нама, в которой в качестве ключа прямого отображения используется матрица G_X, вычисленная по правилу $G_X = X \cdot G$ и хранящаяся в секрете. За счет сокращения числа матриц удается сократить объем ключа (в несколько раз), однако применение такой схемы не предполагает несимметричного протокола обмена данными. Кроме того, для декодирования (расшифрования) кодограммы требуется декодировать кодовое слово *(n, k, d)* кода. Для рекомендованных параметров сложность реализации этой схемы на несколько порядков выше, чем у блочных симметричных шифров (БСШ). Следовательно, применение схемы Рао-Нама менее эффективно по сравнению с БСШ.

В работах [10,11] предложены модифицированные схемы, в которых в качестве ключевых данных используется многочлен Гоппы и/или символы укорочения *(n, k, d)* кода. Достоинством таких схем является небольшой объем ключа (сравнимый с БСШ). Недостатком является высокая (по сравнению с БСШ) сложность реализации. Действительно, для рекомендованных параметров схемы сложность ее реализации на 1 – 2 порядка выше, чем для реализации БСШ.

Для обеспечения стойкости и снижения длины ключа в ТКС предлагается использовать алгеброгеометрические коды [12]. Применение кодов, построенных по алгебраическим кривым (алгеброгеометрических кодов), для формирования ТКС позволит получить дополнительный параметр маскировки кода – вид алгебраической кривой.

Для устранения основного недостатка теоретико-кодовых схем в работах [13,14] предлагается использовать каскадные кодовые конструкции. Их использование позволяет без значительного ухудшения кодовых параметров и снижения энергетического выигрыша от кодирования существенно (на несколько порядков) снизить сложность практической реализации. В работе [15] показано, что наибольший эффект каскадное кодирование позволяет получить при использовании на внешней ступени алгеброгеометрических кодов. Их применение позволяет эффективно бороться с ошибками в каналах передачи данных с независимыми и группирующимися ошибками.

ДИНАМИЧЕСКИЕ СХЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ НА АЛГЕБРАИЧЕСКИХ КОДАХ

Одним из перспективных направлений в развитии методов интегрированного обеспечения конфиденциальности и достоверности передачи данных являются динамические схемы защиты информации на алгебраических кодах.

Исследование методов кодирования совместно с динамическим режимом изменения (n, k, d) параметров кода, когда закон смены этих параметров непредсказуем, позволяет повысить конфиденциальность и имитозащищенность передаваемой информации на уровне контура динамического кодирования. Одновременно достигается значительный энергетический выигрыш в зависимости от вида канала связи и метода кодирования. В связи с этим повышаются требования к выбору метода кодирования, использование которого предполагается в КДК. Здесь важными характеристиками являются:

- ансамбль возможных параметров кода, смена которых приводит к изменению «тонкой» структуры кодового слова;
- спектр возможных длин N;
- основание алфавита кода q;
- вычислительная сложность алгоритма кодирования-декодирования;
- характер гарантированно исправляемых ошибок;

– корректирующие способности кода.

Важным фактором, влияющим на выбор помехоустойчивого кода, является характер распределения ошибок в канале связи. Исследование статистических свойств последовательностей ошибок в реальных каналах связи показало, что ошибки являются зависимыми и обладают тенденцией к группированию (пакетированию), т.е. между ними существует определенная зависимость – корреляция [16]. Большую часть времени информация проходит по каналам связи без искажений, а в отдельные моменты времени возникают сгущения ошибок, так называемые пакеты (пачки, группы) ошибок, внутри которых вероятность ошибки оказывается значительно выше средней вероятности ошибок, вычисленной для значительного времени передачи. Таким образом, предпочтение отдается тем кодам, которые помимо независимых ошибок позволяют обнаруживать и исправлять сложные пакеты ошибок. К их числу относятся недвоичные коды БЧХ, в том числе недвоичные коды Гоппы и коды Рида-Соломона.

В работе проведено исследование динамических схем защиты информации на кодах Рида-Соломона [17]. По определению [1], эти коды строятся на длинах N=q-1 в поле GF(q) по образующему полиному

$$G(x) = (x - \alpha^{j_0})(x - \alpha^{j_0+1})\ldots(x - \alpha^{j_0+d-2}), \qquad (2)$$

где α -примитивные элементы поля GF(q); $j_0 = \overline{1, N}$ -произвольные элементы поля; d - кодовое расстояние или величина избыточности кода.

Изменение любого из параметров (N, α, j_0, d) образующего полинома кода РС (2) приводит к образованию нового смежного класса кода. В этом случае, если на приемной стороне не известен закон смены параметров GF(x), то декодирование представляет собой сложную вычислительную задачу.

Кроме того, коды РС обладают хорошими ансамблевыми структурными свойствами, изменяя *q*-ное основание алфавита, исправляют как одиночные, так и пакеты ошибок.

ВЫВОДЫ

Проведенный анализ показал, что перспективным направлением в развитии теории защиты информации является построение секретных систем теоретической стойкости, основанных на сведении задачи взлома ключевых данных к решению теоретико-сложностной задачи декодирования случайного кода. Их применение позволяет получить строгое математическое обоснование криптографической стойкости и возможность, в некоторых случаях, построить секретную систему с открытым ключом. Кроме того, практическое использование секретных систем на основе кодов позволяет реализовать комплексную защиту информации и обеспечить помимо информационной скрытности эффективный контроль возникающих ошибок, т.е. выполнить требование достоверности передачи данных. Основным недостатком секретных систем, основанных на использовании помехоустойчивых кодов, является большие объемы ключевых данных и высокая, по сравнению с блочно-симметричными алгоритмами, сложность алгоритмов формирования и декодирования кодограмм.

Перспективным направлением их дальнейшего развития является исследование методов кодирования совместно с динамическим режимом изменения (n, k, d) параметров алгебраических кодов, где в качестве кодов целесообразно рассматривать недвоичные коды БЧХ, в том числе недвоичные коды, Гоппы, коды Рида-Соломона, а также

алгеброгеометрические коды, которые обобщают (содержат как подкласс) коды Рида-Соломона. Решение этой задачи позволит обеспечить требуемые показатели информационной скрытности и достоверности передачи данных в телекоммуникационных системах.

SUMMARY

ANALISIS OF PERSPECTIVE DIRECTIONS IN DEVELOPMENT OF METHODS OF INTEGRATED PROVIDING OF CONFIDENTIALITY AND AUTHENTICITY OF DATA COMMUNICATION

V.I. Grabchak, A.P. Melnyk*
Lviv National University "Lvivska Polytechnika", Lviv
**Sumy State University, Sumy*

The methods of disguise of algebraic block code with a rapid decoding algorithm under a casual code (code of general) are investigated, perspective directions of their development are analyses.

Key words: *algebraic, algebra-geometrical code, block code, coding and decoding procedure.*

СПИСОК ЛИТЕРАТУРЫ

1. Блейхут Р. Теория и практика кодов, контролирующих ошибки: пер. с англ. – М.: Мир, 1986. – 576 с.
2. 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.
3. Злотник Б.М. Помехоустойчивые коды в системах связи / Б.М. Злотник – М.: Радио и связь, 1989. – 232 с.
4. Шеннон К. Теория связи в секретных системах // Шеннон К. Работы по теории информации и кибернетике. – М.: Изд-во иностранной литературы, 1963. – С.333-402.
5. Шнайер Б. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си / Б. Шнайер. – М.: Издательство ТРИУМФ, 2003. – 816 с.
6. Молдовян Н.А. Криптография: от примитивов к синтезу алгоритмов / Н.А. Молдовян, А.А. Молдовян, М.А. Еремеев. – СПб.: БХВ-Петербург, 2004. – 448 с.
7. Сидельников В.М. Криптография и теория кодирования / В.М. Сидельников // Материалы конференции «Московский университет и развитие криптографии в России», МГУ. – 2002. – 22 с.
8. R.J. McEliece. 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.
9. T. R. N. Rao and K. H. Nam. Private-key algebraic-coded cryptosystem. Advances in Cryptology – CRYPTO 86, New York. – NY: Springer. – P. 35–48.
10. Северинов А.В. Алгоритм построения укороченных кодов Гоппы / А.В. Северинов // Обработка информации и обеспечение надежности систем управления. – Х.:ХВУ, 1997. – С.38-41.
11. Северинов А.В. Обеспечение имитозащищенности каналов передачи данных с укороченными кодами Гоппы / А.В. Северинов // Інформаційно-керуючі системи на залізничному транспорті. – Х.: ХарДАЗТ, 1997. – №3. – С.29-30.
12. Кузнецов А.А. Разработка теоретико-кодовых схем с использованием эллиптических кодов / А.А. Кузнецов, С.П. Евсеев // Системи обробки інформації. – Х.: ХВУ, 2004 – №5. – С.127-132.
13. Кузнецов А.А. Каскадные кодовые схемы защиты информации / А.А. Кузнецов, В.И. Грабчак, С.П. Евсеев // Системи обробки інформації. – Харків: ХУ ПС, 2005 – Вип. 9 (49). – С. 206 – 211.
14. Стасев Ю.В. Разработка теоретико-кодовых схем на обобщенных каскадных кодах / Ю.В. Стасев, А.А. Кузнецов, В.И. Грабчак, В.Ю. Ковтун // Збірник наукових праць ХУПС. – Харків: ХУПС, 2006. – Вип. 2 (8). – С. 79-81.
15. Стасев Ю.В. Каскадні схеми захисту інформації на алгеброгеометричних кодах / Ю.В. Стасев, А.А. Кузнецов, В.И. Грабчак, С.П. Евсеев // Системи озброєння і військова техніка. – Х.: ХУ ПС, 2006. – Вип. 1 (5). – С. 82-87.
16. Типикин А.П. Коррекция ошибок в оптических накопителях информации / А.П. Типикин, В.В. Петров, А.Г. Бабанин; отв. ред. А.Г. Додонов; АН УССР. Ин-т проблем регистрации информации. – К.: Наукова думка, 1990. – 172 с.
17. Грабчак В.І. Динамічні схеми захисту інформації на кодах Ріда-Соломона / В.І. Грабчак // Вісник Сумського державного університету. - 2008. – Вип. 4. – С. 38-44.

Поступила в редакцию 1 марта 2009 г.