УДК 621.391

Е.Л. Онанченко[1], А.А. Кузнецов[2]; В.Н. Лысенко[3], В.И. Грабчак[3], Р.В. Королёв[2]

[1]*Сумской государственный университет*
[2]*Харьковский университет Воздушных Сил им. И. Кожедуба*
[3]*Военный институт РВ и А Сумского государственного университета*

ИССЛЕДОВАНИЕ МЕТОДОВ ЗАЩИТЫ ИНФОРМАЦИИ, ОСНОВАННЫХ НА ИСПОЛЬЗОВАНИИ АЛГЕБРАИЧЕСКИХ БЛОКОВЫХ КОДОВ

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

теоретико-кодовые схемы, контур динамического кодирования, схемы Мак–Эллиса и Нидеррайтера, модифицированные схемы, каскадные кодовые конструкции

Введение

Постановка проблемы в общем виде и анализ литературы. Перспективным направлением в развитии методов защиты информации, являются криптосистемы теоретической стойкости, в которых задача взлома ключевых данных сводится к решению известной математической задачи [1, 2]. Как правило, это несимметричные криптосистемы, сложность взлома которых сведена к решению одной из следующих теоретико-сложностных задач (ТСЗ):

– ТСЗ об укладке ранца;
– ТСЗ факторизации числа;
– ТСЗ дискретного логарифмирования;
– ТСЗ дискретного логарифмирования в группе точек эллиптической кривой;
– ТСЗ декодирования случайного кода.

Очевидным преимуществом криптосистем теоретической стойкости является строгое математическое обоснование криптографической стойкости и возможность, в некоторых случаях, построить криптосистему с открытым ключом. К недостаткам большинства криптосистем теоретической стойкости следует отнести высокую сложность криптографического преобразования. Исключением являются криптосистемы, основанные на сведении задачи взлома ключевых данных к решению ТСЗ декодирования случайного кода. В некоторых источниках они получи название теоретико-кодовых схем (ТКС) [1]. Различные подходы по применению методов помехоустойчивого кодирования для защиты информации рассматривались в работах [3 – 5]. Основная цель проводимых исследований состоит в поиске эффективных методов сокрытия (маскирования) быстрого правила декодирования алгебраических блоковых кодов, в результате чего криптоаналитик вынужден использовать сложные алгоритмы декодирования случайного кода. В общем случае, для декодирования случайного линейного блокового кода криптоаналитик вынужден использовать корреляционный декодер, сложность которого растет экспоненциально от длины кода и его корректирующей способности. Сложность декодирования уполномоченным пользователем растет полиномиально от параметров кода, в результате чего удается определить одностороннюю криптографическую функцию, используемую при построении криптосистемы [1, 2].

Целью статьи является исследование методов построения теоретико-кодовых схем, анализ перспективных направлений их развития.

Основная часть

Исследование методов маскирования алгебраических блоковых кодов. Основная идея, которая используется при построении ТКС, состоит в “маскировке” алгебраических блоковых кодов под коды общего положения (случайные коды). В этих схемах для реализации односторонней функции специального преобразования данных использована трудноразрешимая задача декодирования случайного кода (кода общего положения). Общая классификация известных методов построения ТКС представлена на рис. 1.

Задача декодирования может быть эффективно решена (с полиномиальной сложностью алгоритма) для узкого класса кодов, например, кодов Боуза-Чоудхури-Хоквигнема (БЧХ), кодов Рида-Соломона (РС) и др. Одним из наиболее эффек тивных алгоритмов алгебраического декодирования кодов БЧХ и РС является алгоритм Берлекэмпа-Месси и его модификации (улучшения). Известно [6], что алгоритм Берлекэмпа-Месси содержит число реализации умножений, порядка t^2, или, формально, сложность алгоритма $O(t^2)$, где t – исправляющая способность кода, $t = [(d – 1)/2]$.

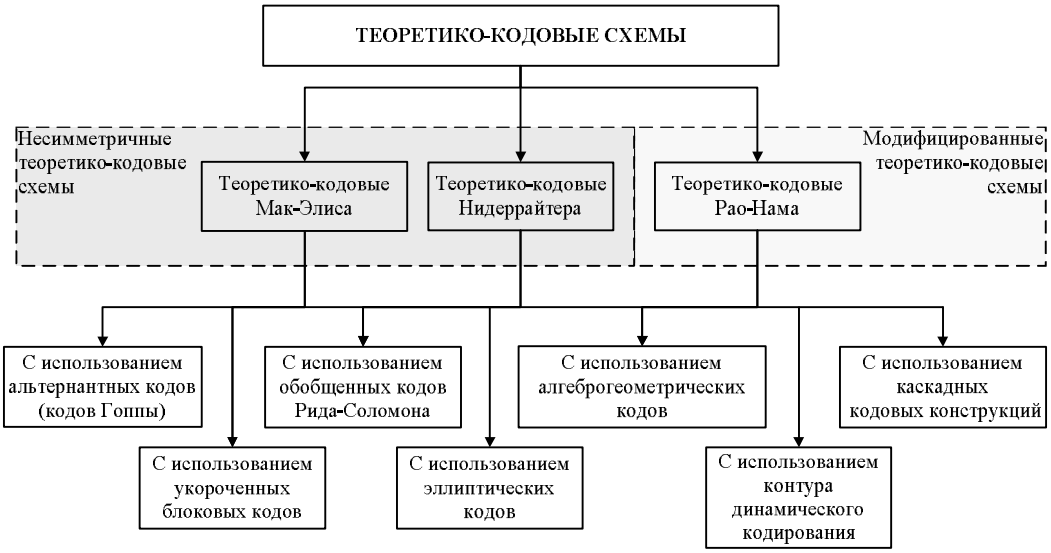

Рис. 1. Классификация известных методов построения теоретико-кодовых схем

Для большого t используют ускоренный алгоритм Берлекэмпа-Месси, позволяющий уменьшить вычислительную сложность алгоритма. Еще более эффективным, с точки зрения вычислительной сложности, является рекуррентный алгоритм Берлекэмпа-Месси. Асимптотическая сложность декодирования кодов Рида-Соломона в этом случае не превосходит величины $O(n\log^2 n)$, причем очень близка к величине $O(n\log n)$.

Декодирование произвольного линейного кода (кода общего положения) является весьма сложной вычислительной задачей, сложность ее решения растет экспоненциально. Так, для корреляционного декодирования произвольного (n, k, d) кода над GF(q) необходимо, в общем случае, сравнить принятую последовательность со всеми q^k кодовыми словами и выбрать ближайшее (в метрике Хемминга). Даже для небольших n, k, d и q задача корреляционного декодирования весьма трудоемка. Это положение лежит в основе всех несимметричных ТКС. Маскируя код с быстрым алгоритмом декодирования (полиномиальной сложности) под произвольный (случайный) линейный код можно представить задачу декодирования для постороннего наблюдателя (возможного злоумышленника) как вычислительно сложную задачу (экспоненциальной сложности). Для уполномоченного пользователя (имеющего секретный ключ) декодирование – полиномиально разрешимая задача.

Контур динамического кодирования. 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.

Целесообразно применение в КДК, кодов с высокой исправляющей способностью, в частности кодов РС. По определению эти коды строятся на длинах N = q – 1 в поле GF(q) по образующему полиному

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

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 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*-ичное основание алфавита, можно исправляют как одиночные, так и пакеты ошибок.

Схема Мак–Элиса. Пусть G – порождающая матрица линейного (n, k, d) кода над GF(q) с полиномиальной сложностью декодирования. Пусть X – невырожденная k × k-матрица над GF(q), D – диаго-

нальная матрица с ненулевыми на диагонали элементами, P – перестановочная матрица размера n × 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 схеме Мак-Элиса является матрица $G_X = X \cdot G \cdot P \cdot D$, секретным (закрытым) ключом являются матрицы X, P, D [3]. Закрытая информация (кодограмма) представляет собой вектор длины n и вычисляется по правилу

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

где вектор $c_X = i \cdot G_X$ принадлежит (n, k, d) коду с порождающей матрицей G_X, i – k-разрядный информационный вектор, вектор e – секретный вектор ошибок веса ≤ t. На рис. 2 представлена схема передачи кодограммы в ТКС Мак-Элиса.

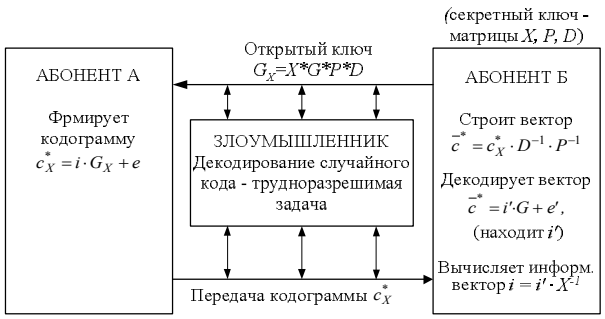

Рис. 2. Схема передачи кодограммы
в теоретико-кодовой схеме Мак–Элиса

Злоумышленнику необходимо декодировать кодограмму c_X^* с известной порождающей матрицей G_X. Не зная матрицы X, P и D злоумышленник не может восстановить G и воспользоваться алгоритмом декодирования полиномиальной сложности. Декодирование случайного кода большой длины вычислительно недоступно (экспоненциальная сложность при корреляционном декодировании). Для уполномоченного пользователя (знающего секретный ключ) декодирование кодограммы - 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'. Затем вычисляет k-разрядный информационный вектор $i = i' \cdot X^{-1}$.

Таким образом, в ТКС Мак-Элиса основным средством маскировки линейного (n, k, d) кода с полиномиально разрешимой задачей декодирования являются матрицы X, P, D.

Схема Нидеррайтера. Схема Нидеррайтера, впервые предложена в [4]. Пусть H – проверочная матрица линейного (n, k, d) кода над GF(q) с полиномиальной сложностью декодирования. Пусть X – невырожденная r × r-матрица над GF(q), D – диагональная матрица с ненулевыми элементами на диагонали, P – перестановочная матрица размера n × 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

$$S_X = e \cdot H_X^T, \qquad (2)$$

где вектор e – вектор длины n и веса ≤ t, который несет конфиденциальную информацию (информационное сообщение, подлежащее закрытию). На рис. 3 представлена схема передачи кодограммы в ТКС Нидеррайтера.

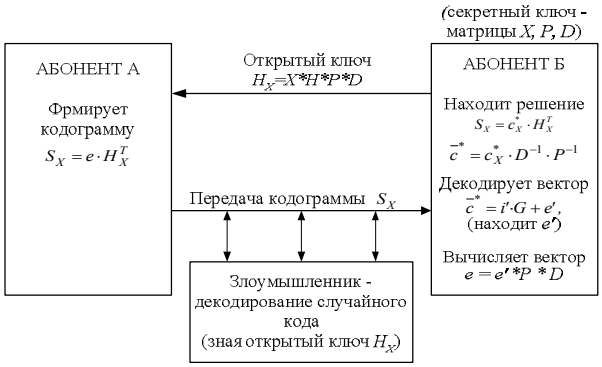

Рис. 3. Схема передачи кодограммы
в теоретико-кодовой схеме Нидеррайтера.

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, как и в схеме Мак-Элиса, 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.

Таким образом, в ТКС Нидеррайтера основным средством маскировки линейного (n, k, d) кода с полиномиально разрешимой задачей декодирования также являются матрицы X, P, D.

Известные примеры ТКС Мак-Элиса и Нидеррайтера рассмотрены для случая использования кодов БЧХ и кодов РС (подкласс недвоичных кодов БЧХ). По соображениям, изложенным в [1, 7], процедуры взлома схем Мак-Элиса могут быть легко трансформированы на схемы Нидеррайтера. Стойкость ТКС, построенных на кодах РС и кодах БЧХ, считается недостаточной.

Достоинство схемы Мак-Элиса и Нидеррайтера 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 этих схем является большой объем ключевых данных – k×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.

Модифицированные схемы. *Схема Рао-Нама.* В работе [5] 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.

Схема передачи кодограммы ТКС Рао-Нама приведена на рис. 4.

Теоретико-кодовые схемы на альтернантных кодах Гоппы. ТКС, построенная с использованием альтернантных кодов, заданных через многочлен Гоппы впервые предложена в работе [8]. Основная идея состоит в построении схемы Рао-Нама на (n, k, d) кодах Гоппы, заданных с помощью многочлена Гоппы степени t, $d = 2 \cdot t + 1$. При этом, если (n, k, d) код Гоппы над GF(q) позволяет исправить t ошибок, то все кодовые слова могут быть однозначно заданы многочленом Гоппы степени t над GF(q), где число неприводимых кодов Гоппы растет экспоненциально с ростом t. Следовательно, если вместо порождающей матрицы кода в качестве секретного ключа использовать многочлен Гоппы, то, как показано в работах [8,9], получим стойкую схему. При этом удается существенно сократить объем ключа. В общем случае, для однозначного определения многочлена Гоппы необходимо хранить t +1 q-ичных символов.

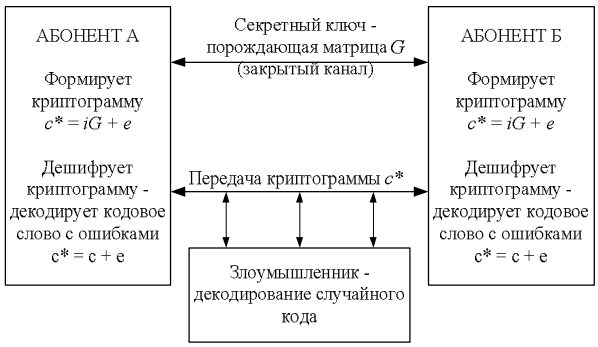

Рис. 4. Схема передачи кодограммы втеоретико-кодовой схеме Рао-Нама

Основное отличие от классической схемы Рао-Нама состоит в использовании многочлена Гоппы в качестве секретного симметричного ключа. В работах [8,9] исследованы возможности ТКС Рао-Нама, построенных с использованием заданных через многочлен Гоппы альтернантных кодов по обеспечению имитозащищенности и помехоустойчивости. Действительно, если при формировании кодограммы использовать случайный вектор ошибки e, такой, что $w(e) < t$, то появляется возможность на приемной стороне контролировать ошибки в пределах конструктивной величины t. Это позволяет, с одной стороны, решать задачу повышения имитозащищенности, а с другой, – повышать помехоустойчивость.

В работе [8] исследованы зависимости между уровнями обеспечиваемой помехоустойчивости и имитозащищенности при использовании ТКС на альтернантных кодах Гоппы. Однако, при повышенных требованиях к имитозащищенности, решить в полной мере задачу повышения помехоустойчивости не удается, помехоустойчивость такой схемы не велика. Она уступает возможностям большинства хороших алгебраических кодов и является критически низкой при построении специальных каналов передачи данных. Свободными от этих недостатков являются ТКС, построенные на укороченных алгебраических блоковых кодах.

Теоретико-кодовые схемы на укороченных алгебраических блоковых (n, k, d) кодов. В работах [10, 11] снято основное ограничение по низкой величине обеспечиваемой помехоустойчивости. Основная идея таких схем состоит в использовании укороченных алгебраических блоковых (n, k, d) кодов (в оригинальной схеме используются укороченные коды Гоппы). Символы укорочения выбираются случайно, независимо и хранятся в секрете (являются секретным симметричным ключом). Показано, что даже при небольшом числе символов укорочения удается построить стойкую схему.

Кодограммой в такой системе является кодовое слово укороченного алгебраического блокового кода (например, кода Гоппы), а всю конструктивную величину t предлагается использовать для исправления ошибок.

Таким образом, помехоустойчивость ТКС определяется полной конструктивной величиной t блокового (n, k, d) кода, $d = 2 \cdot t + 1$. Все возникшие в канале связи ошибки e веса $w(e) \le t$ исправляются в пределах сферы упаковки кода.

Основное преимущество этой ТКС состоит в высоких показателях помехоустойчивости. В то же время ей присущ существенный недостаток – линейность схемы. Каждая кодограмма представляет собой кодовое слово линейного укороченного блокового кода. Следовательно, сумма двух кодограмм даст третью разрешенную кодограмму.

Для устранения указанного недостатка предлагается использовать искусственные приемы внесения нелинейности (контрольные метки времени, использование режима сцепления блоков и др.). Эти меры усложняют анализ для криптоаналитика и потенциально повышают стойкость ТКС. Однако их использование усложняет процесс формирования/снятия кодограммы и, очевидно, снижает помехоустойчивость (например, за счет внесения дополнительной служебной информации).

Теоретико-кодовые схемы на эллиптических кодах. Одним из перспективных направлений развития ТКС, направленных на повышение стойкости и снижение длины ключа, является использование алгеброгеометрических кодов. Применение кодов, построенных по алгебраическим кривым (алгеброгеометрических кодов), для формирования ТКС позволит получить дополнительный параметр маскировки кода – вид алгебраической кривой [12].

Эллиптический (n, k, d) код над GF(q), задается с помощью генераторной матрицы A вида:

$$A = \begin{pmatrix} F_0(P_0) & F_0(P_1) & \dots & F_0(P_{n-1}) \\ F_1(P_0) & F_1(P_1) & \dots & F_1(P_{n-1}) \\ \dots & \dots & \dots & \dots \\ F_{M-1}(P_0) & F_{M-1}(P_1) & \dots & F_{M-1}(P_{n-1}) \end{pmatrix} = \left\| F_j(P_i) \right\|_{n,M}$$

и размерности $M \times n$, $M = \alpha$, $\alpha = 3 \cdot \deg F$.

Для снижения объема ключевых данных в ТКС на эллиптических кодах воспользуется следующая особенность построения матрицы *A*.

Генераторная матрица *A* формируется в результате отображения точек эллиптической кривой базисом генераторных функций. Для построения эллиптического кода используется генераторная матрица, построенная по кривой

$$y^2z + a_1xyz + a_3yz^2 = x^3 + a_2x^2z + a_4xz + a_6z^3,$$

где $a_i \in GF(q)$. Коэффициенты этого многочлена однозначно задают вид кривой и, соответственно, набор проективных точек по которым строится эллиптический код (его генераторная матрица).

Каждый символ генераторной матрицы формируется путем вычисления значения генераторной функции F_j в точке P_i эллиптической кривой. Число M генераторных функций определяется конструктивными характеристиками эллиптического (n, k, d) кода. Вид функций F_j определяется степенью α отображения точек кривой и, следовательно, так же задается конструктивными параметрами кода. Таким образом, если заданы конструктивные (n, k, d) характеристики эллиптического кода, то уникальность генераторной матрицы определяет набор точек $P_1, P_2, \dots, P_n$, в которых вычисляются значения генераторных функций. Конкретный набор точек из пространства P^2 однозначно задается видом многочлена кривой, т.е. набором коэффициентов $a_1 \dots a_6$, где $\forall a_i \in GF(q)$.

Объем секретного ключа (в битах) в модифицированной ТКС Рао-Нама, построенной по эллиптическим (n, k, d) кодам над $GF(2^m)$ определяется выражением $l_{K+} = 5 \cdot m$. Очевидно, что предложенный способ построения модифицированных ТКС на эллиптических кодах позволяет существенно снизить объемы ключевой информации по сравнению с классической схемой Рао-Нама.

Каскадные кодовые конструкции. Использование каскадных кодовых конструкций позволяет без значительного ухудшения кодовых параметров и снижения энергетического выигрыша от кодирования существенно (на несколько порядков) снизить сложность практической реализации. В работах [13] 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.

Наиболее общим классом каскадных кодовых конструкций являются обобщенные каскадные коды (ОКК). По определению [14] алгебраически заданный ОКК порядка m однозначно определяется n_2 квадратными двоичными матрицами H_0^j, $j = \overline{1, n_2}$ порядка n_1 (задающих (n_1, k_i, d_{1i}) коды внутренней сту-

пени) и $m+1$ групповыми над $GF(2^{a_i})$, $i=\overline{1,m+1}$ кодами внешней ступени с параметрами (n_2, b_i, d_{2i}). На рис. 5 представлена геометрическая трактовка ОКК.

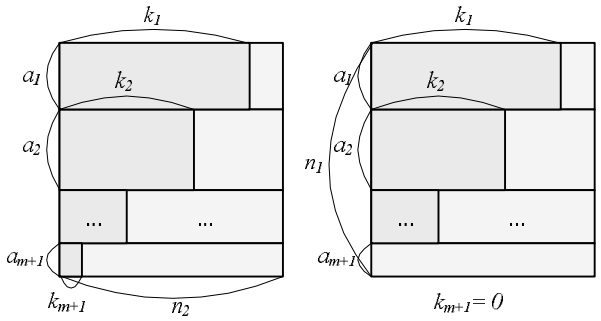

Рис. 5. Геометрическая трактовка ОКК

Формирование каскадной ТКС осуществляется путем маскировки кодов внешней ступени $(m+1)$ ОКК, а процесс формирования кодограмм соответствует формированию кодового слова замаскированного каскадного кода с добавлением к нему случайного вектора ошибки e_i, что позволяет получить высокие конструктивные показатели кодовых схем защиты информации при низкой сложности их реализации.

В работах [13, 14] показано, что практическое использование каскадных кодовых конструкций позволяет при сравнимых показателях стойкости на 2 – 3 порядка снизить сложность формирования и декодирования кодограмм, а также на 2 – 3 порядка уменьшить объемы необходимых ключевых данных по сравнению с эквивалентными некаскадными ТКС.

Выводы

Проведенные исследования показали, что перспективным направлением в развитии теории криптографии являются методы защиты информации, основанные на использовании алгебраических блоковых кодах. Их применение позволяет, во-первых, строить несимметричные алгоритмы преобразования информации, в которых не накладываются ограничения по секретности ключевых данных, во-вторых, совмещать помехоустойчивое кодирование со специальным преобразованием информации. Это дает возможность интегрировано (одним приемом) повышать достоверность и конфиденциальность передачи информации.

Перспективным направлением дальнейших исследований является поиск путей снижения вычислительной сложности алгоритмов формирования и декодирования кодограмм в ТКС, сокращение объема ключевых данных, выработка рекомендаций их по практическому использованию.

Список литературы

1. Сидельников В.М. Криптография и теория кодирования // Материалы конференции «Московский университет и развитие криптографии в России». – М.: МГУ, 2002. – 22 с.

2. Шнайер Б. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си. – М.: Издательство ТРИУМФ, 2003. – 816 с.

3. McEliece R.J. 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.

4. H. Niederreiter. Knapsack-Type Cryptosystems and Algebraic Coding Theory // Probl. Control and Inform. Theoty. – 1986. – V. 15. – P. 19-34.

5. Rao T. R. N. and Nam K. H. Private-key algebraic-coded cryptosystem. Advances in Cryptology – CRYPTO 86, New York. – NY: Springer. – P. 35-48.

6. Блейхут Р. Теория и практика кодов, контролирующих ошибки: Пер. с англ. – М.: Мир, 1986. – 576 с.

7. 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.

8. 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. Королева. – Х.: НАНУ, ПАНИ. – 1994. – С. 28.

9. 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.

10. Северинов А.В. Алгоритм построения укороченных кодов Гоппы // 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 // Інформаційно-керуючі системи на залізничному транспорті. – Х.: ХарДАЗТ. – 1997. – № 3.– С. 29-30.

12. Кузнецов А.А., Евсеев С.П. Разработка теоретико-кодовых схем с использованием эллиптических кодов // Системи обробки інформації. – Х.: ХВУ, 2004 – № 5. – С. 127-132.

13. Стасев Ю.В., Кузнецов А.А., Грабчак В.И., Евсеев С.П. Каскадні схеми захисту інформації на алгеброгеометричних кодах // Системи озброєння і військова техніка. – Х.: ХУ ПС. – 2006. – Вип. 1 (5). – С. 82-87.

14. Стасев Ю.В., Кузнецов А.А., Грабчак В.И., Ковтун В.Ю. Разработка теоретико-кодовых схем на обобщенных каскадных кодах // Збірник наукових праць ХУ ПС. – Х.: ХУ ПС. – 2006. – Вип. 2 (8). – С. 79-81.

Поступила в редколлегию 22.05.2007

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