УДК 621.391

РАЗРАБОТКА АЛГОРИТМА ДЕКОДИРОВАНИЯ КОДОГРАММ В КАСКАДНЫХ ТЕОРЕТИКО-КОДОВЫХ СХЕМАХ

Н.Н. Ляпа, канд. техн. наук, доцент;
В.Н. Лысенко, канд. техн. наук, доцент;
В.И. Грабчак
Военный институт РВиА Сумского государственного университета

Предлагается алгоритм декодирования кодограмм в каскадных теоретико-кодовых схемах, построенных на маскировании кодов внешней ступени обобщенного каскадного кода. Производится оценка временной и емкостной сложности разработанного алгоритма.

ВВЕДЕНИЕ

Перспективным направлением в развитии комплексных механизмов обеспечения информационной скрытности и достоверности передачи данных являются кодовые конструкции, функционирующие в режиме маскирования кодовых слов под случайную последовательность [1, 2]. Их практическое использование позволяет реализовать в одном устройстве методы канального кодирования и специального преобразования данных. В тоже время, как показывает проведенный анализ [1, 3], для реализации известных методов неприемлемо высоки временная и емкостная сложности алгоритмов формирования и декодирования кодограмм. Указанные недостатки сдерживают практическое использование указанных механизмов обеспечения требуемых показателей информационной скрытности и достоверности передачи данных.

Проведенный анализ [4] показал, что перспективным направлением в развитии методов помехоустойчивого кодирования являются 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 [5] показано, что наиболее эффективными по соотношениям длины ключа обеспечиваемой стойкости и сложности реализации являются каскадные теоретико-кодовые схемы (ТКС), построение которых базируется на маскировании кодов внешней ступени обобщенного каскадного кода.

Целью статьи является разработка алгоритма декодирования кодограмм в каскадных ТКС, оценка временной и емкостной сложности их реализации.

РАЗРАБОТКА АЛГОРИТМА ДЕКОДИРОВАНИЯ КОДОГРАММ В КАСКАДНЫХ ТКС

Для построения алгоритма декодирования кодограмм в каскадных ТКС воспользуемся алгебраическим описанием обобщенных каскадных кодов [6]. По определению алгебраически заданный обобщенный каскадный код 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 первой ступени) и $m+1$ групповыми над $GF(2^{a_i})$, $i=\overline{1,m+1}$ кодами второй ступени с параметрами (n_2,b_i,d_{2i}).

Для декодирования кодограммы в разработанной каскадной теоретико-кодовой схеме необходимо снять действие маскирования с кодов внешней ступени и воспользовавшись быстрыми (алгебраическими) алгоритмами декорировать кодовое слово обобщенного каскадного кода. В этом случае алгоритм декодирования кодограмм в общем виде можно представить последовательностью следующих шагов [7].

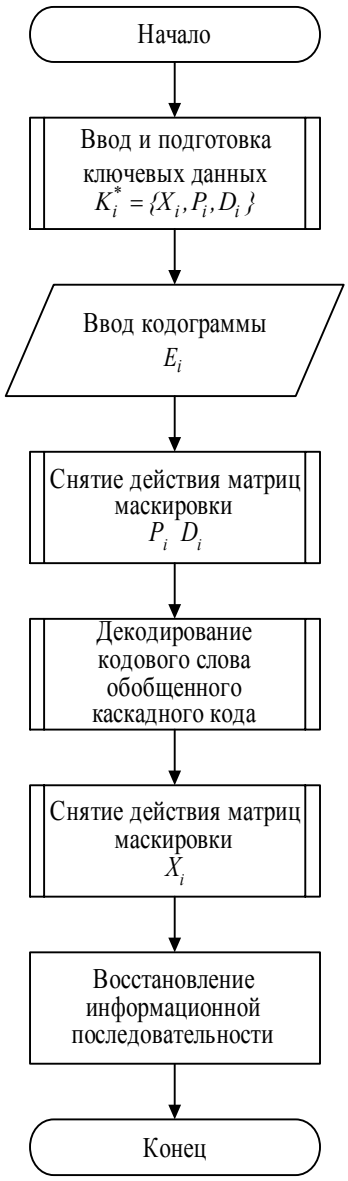

Рисунок 1 - Схема алгоритма декодирования кодограммы в каскадной теоретико-кодовой схеме на обобщенном каскадном коде

Шаг 1 Ввод и подготовка ключевых данных

$K^* = \{K_1^*, K_2^*, \ldots, K_s^*\} = \{\{X,P,D\}_1, \{X,P,D\}_2, \ldots, \{X,P,D\}_s\}$,

параметризирующих обратные отображения в каскадной теоретико-кодовой схеме.

Шаг 2. Ввод поступившей кодограммы

$$E_i = \{(\gamma^*_{1,1}, \gamma^*_{1,2}, \ldots, \gamma^*_{1,n_2}), (\gamma^*_{2,1}, \gamma^*_{2,2}, \ldots, \gamma^*_{2,n_2}), \ldots, (\gamma^*_{m+1,1}, \gamma^*_{m+1,2}, \ldots, \gamma^*_{m+1,n_2})\}$$

где $\gamma^*_{ij} = \gamma_{ij} + e_{ij}$, а γ_{ij} и e_{ij} – двоичные вектора длины a_i.

Шаг 3. Снятие действия матриц маскировки $P_i \cdot D_i$ с кодовых слов кодов второй ступени обобщенного каскадного кода.

Шаг 4 Декодирование кодового слова обобщенного каскадного кода, т.е. восстановление вектора

$$C_i = \{(\gamma_{1,1}, \gamma_{1,2}, \ldots, \gamma_{1,n_2}), (\gamma_{2,1}, \gamma_{2,2}, \ldots, \gamma_{2,n_2}), \ldots, (\gamma_{m+1,1}, \gamma_{m+1,2}, \ldots, \gamma_{m+1,n_2})\}.$$

Шаг 5 Снятие действия матриц маскировки X_i с кодовых слов кодов второй ступени обобщенного каскадного кода.

Шаг 6 Восстановление информационной последовательности

$$M_i = \{(I_{1,1}, I_{1,2}, \ldots, I_{1,a_1}), (I_{2,1}, I_{2,2}, \ldots, I_{2,a_1}), \ldots, (I_{b_1,1}, I_{b_1,2}, \ldots, I_{b_1,a_1}), (I_{1,1}, I_{1,2}, \ldots, I_{1,a_2}), (I_{2,1}, I_{2,2}, \ldots, I_{2,a_2}), \ldots, (I_{b_2,1}, I_{b_2,2}, \ldots, I_{b_2,a_2}), \ldots, (I_{1,1}, I_{1,2}, \ldots, I_{1,a_{m+1}}), (I_{2,1}, I_{2,2}, \ldots, I_{2,a_{m+1}}), \ldots, (I_{b_{m+1},1}, I_{b_{m+1},2}, \ldots, I_{b_{m+1},a_{m+1}})\}$$

путем выделения информационной части кодового слова обобщенного каскадного кода.

Схема алгоритма декодирования кодограммы представлена на рис. 1. Основными процедурами представленного алгоритма являются следующие:

- ввод и подготовка ключевых данных;
- снятие действия матриц маскировки;
- декодирование кодового слова обобщенного каскадного кода.

Рассмотрим эти процедуры подробнее.

Под вводом и подготовкой ключевых данных (шаг 1) понимается ввод $l_{K^*} = \sum_{j=1}^{m+1} b_j{}^2 \cdot a_j + n_2{}^2 \sum_{j=1}^{m+1} a_j$ данных, задающих ключ обратного отображения, и формирование на их основе набора порождающих матриц $\{X^1,P^1,D^1\},\{X^2,P^2,D^2\},\ldots,\{X^{m+1},P^{m+1},D^{m+1}\}$.

Каждая из матриц P^i и D^i, $i = 1,\ldots,m+1$ содержит $n_2 \times n_2$ символов из $GF(2^{a_i})$. Унипотентная матрица $\Lambda^i = P^i \cdot D^i$ содержит $n_2 \times n_2$ символов из $GF(2^{a_i})$, т.е. $n_2 \cdot n_2 \cdot a_i$ бит:

$$\Lambda^i = \begin{pmatrix} \lambda^i_{11} & \lambda^i_{12} & \ldots & \lambda^i_{1n_2} \\ \lambda^i_{21} & \lambda^i_{22} & \ldots & \lambda^i_{2n_2} \\ \ldots & \ldots & \ldots & \ldots \\ \lambda^i_{n_2 1} & \lambda^i_{n_2 2} & \ldots & \lambda^i_{n_2\, n_2} \end{pmatrix}.$$

Матрица X^i, $i = 1,\ldots,m+1$ содержит $k_{2i} \times k_{2i}$ символов из $GF(2^{a_i})$, т.е. $k_{2i} \cdot k_{2i} \cdot a_i$ бит:

$$X^i = \begin{pmatrix} x^i_{11} & x^i_{12} & \ldots & x^i_{1k_{2i}} \\ x^i_{21} & x^i_{22} & \ldots & x^i_{2k_{2i}} \\ \ldots & \ldots & \ldots & \ldots \\ x^i_{k_{2i}1} & x^i_{k_{2i}2} & \ldots & x^i_{n_2\, k_{2i}} \end{pmatrix}.$$

На третьем и пятом шагах алгоритма декодирования кодограмм каскадной кодовой схемы защиты информации производится снятие действия матриц маскирования. Эта процедура реализуется путем умножения на обратные матрицы маскирования и заключается в снятии действия унипотентных матриц $\Lambda^i = P^i \cdot D^i$, $i = 1,\ldots,m+1$ с кодовых слов $\{(\gamma^*_{1,1},\gamma^*_{1,2},\ldots,\gamma^*_{1,n_2}),(\gamma^*_{2,1},\gamma^*_{2,2},\ldots,\gamma^*_{2,n_2}),\ldots,(\gamma^*_{m+1,1},\gamma^*_{m+1,2},\ldots,\gamma^*_{m+1,n_2})\}$ кодов внешней ступени обобщенного каскадного кода и снятие действия матриц X^i, $i = 1,\ldots,m+1$.

На четвертом шаге алгоритма декодирования кодограмм в каскадных кодовых схемах защиты информации производится декодирование кодового слова обобщенного каскадного кода. После ввода кодограммы – кодового слова обобщенного каскадного кода с ошибками выполняется поочередное декодирование i-ми кодами внутренней и внешней ступени, $i = 1,\ldots,m+1$. Перед декодированием i-м кодом внутренней ступени производится формирование кодового слова с ошибками i-го кода внутренней ступени. После декодирования i-м кодом внутренней ступени производится формирование кодового слова с ошибками внутреннего кода i-й ступени. Подробно процедуры декодирования i-ыми кодами внутренней и внешней ступени и процессы декодирования кодового слова обобщенного каскадного кода изложены в монографии [6].

Таким образом, в ходе проведенных исследований разработан алгоритм декодирования кодограмм, который основан на последовательном выполнении процедуры демаскирования обобщенного каскадного кода и процедуры декодирования соответствующего кодового слова, что

позволяет за конечное число шагов декодировать кодограмму в каскадной теоретико-кодовой схеме.

ИССЛЕДОВАНИЕ СЛОЖНОСТИ РЕАЛИЗАЦИИ АЛГОРИТМА ДЕКОДИРОВАНИЯ КОДОГРАММ В КАСКАДНОЙ ТЕОРЕТИКО-КОДОВОЙ СХЕМЕ

При условии предварительного ввода и подготовки ключевых данных (шаг 1) декодирование кодограммы состоит в снятии действия матриц маскировки и декодировании кодового слова обобщенного каскадного кода.

При известных и хранимых в памяти элементах обратной матрицы маскирования сложность снятия действия маскирования определяется сложностью умножения на соответствующую матрицу. Так, сложность снятия действия матрицы маскирования $\Lambda^i = P^i \cdot D^i$ размером $n_2 \times n_2$ символов определяется сложностью умножения на матрицу $(\Lambda^i)^{-1}$ размером $n_2 \times n_2$ символов. Эта процедура потребует n_2^2 сложений и умножений над элементами из поля $GF(2^{a_i})$. Одна операция умножения двух элементов из $GF(2^{a_i})$ потребует a_i операций сложения и сдвига. Всего для снятия действия всех матриц $\Lambda^i = P^i \cdot D^i$ и X^i потребуется

$$n_2^2 \cdot \sum_{i=1}^{m+1} a_i + \sum_{i=1}^{m+1} b_i^2 \cdot a_i$$

временных интервалов. Емкостная сложность составит

$$n_2{}^2 + \sum_{i=1}^{m+1} b_i{}^2 \cdot a_i$$

двоичных ячеек памяти.

Сложность декодирования кодового слова обобщенного каскадного кода как функция размера задачи определяется суммой сложностей реализации алгоритмов декодирования кодами внешней и внутренней степеней обобщенного каскадного кода. Сложность декодирования циклических кодов исправляющих t ошибок определяется сложностью решения системы из t линейных уравнений и составляет порядка t^2 операций сложения и умножения элементов в конечном поле [8]. С учетом сложности реализации операций над элементами из $GF(2^{a_i})$ временная сложность декодирования кодового слова обобщенного каскадного кода составит

$$\sum_{i=1}^{m+1} (t_{1i}{}^2 + a_i \cdot t_{2i}^2)$$

временных интервалов, где t_{1i} и t_{2i} - исправляющая способность кодов первой и второй ступени соответственно. Емкостная сложность составит

$$\sum_{i=1}^{m+1} (t_{1i}{}^2 + a_i \cdot t_{2i}{}^2)$$

двоичных ячеек памяти.

С учетом сложности снятия действия матриц маскировки окончательные выражения по оценке временной и емкостной сложности алгоритмов декодирования запишутся в виде

$$S_B = n_2^2 \cdot \sum_{i=1}^{m+1} a_i + \sum_{i=1}^{m+1} \left(b_i{}^2 \cdot a_i + t_{1i}{}^2 + a_i \cdot t_{2i}{}^2 \right), \qquad (1)$$

$$S_E = n_2{}^2 + \sum_{i=1}^{m+1} \left(b_i{}^2 \cdot a_i + t_{1i}{}^2 + a_i \cdot t_{2i}{}^2 \right). \qquad (2)$$

Оценим асимптотическую временную и емкостную сложности алгоритма декодирования кодограмм. Для этого упростим полученное выражение. Положим, что $\forall a_i = \frac{n_1}{m+1}$, $\forall \mathrm{t}_{1i} = \frac{n_1}{4}$, $\forall \mathrm{t}_{2i} = \frac{n_2}{4}$, $\forall \mathrm{b}_i = \frac{n_2}{2}$, $n_2 = n_1 = \sqrt{n}$. Тогда после подстановки в (1) и (2) получим:

$$S_B = \frac{n \cdot (m+1)}{16} + \frac{21 \cdot n \cdot \sqrt{n}}{16},$$

$$S_E = n + \frac{n \cdot (m+1)}{16} + \frac{5 \cdot n \cdot \sqrt{n}}{16}.$$

В пределе при увеличении размера задачи асимптотическая сложность алгоритмов декодирования кодограммы в предложенных каскадных теоретико-кодовых схемах будет равна

$$S_B^* = n \cdot \left(\sqrt{n} + m \right), \qquad (3)$$

$$S_E = n \cdot \left(\sqrt{n} + m \right). \qquad (4)$$

Для реализации алгоритма декодирования кодограмм с использованием эквивалентного замаскированного двоичного линейного блокового *(n, k, d)* кода необходимо снять действие матрицы маскирования $\Lambda = P \cdot D$ размером $n \times n$ двоичных символов и действие матрицы X размером $k \times k$ двоичных символов. Для этого необходимо выполнить

$$S_{B_э} = S_{B_э}^* = \mathrm{n}^2 + k^2 \qquad (5)$$

операций сложения и умножения и хранить

$$S_{E_э} = S_{E_э}^* = \mathrm{n}^2 + k^2 \qquad (6)$$

двоичных элементов памяти.

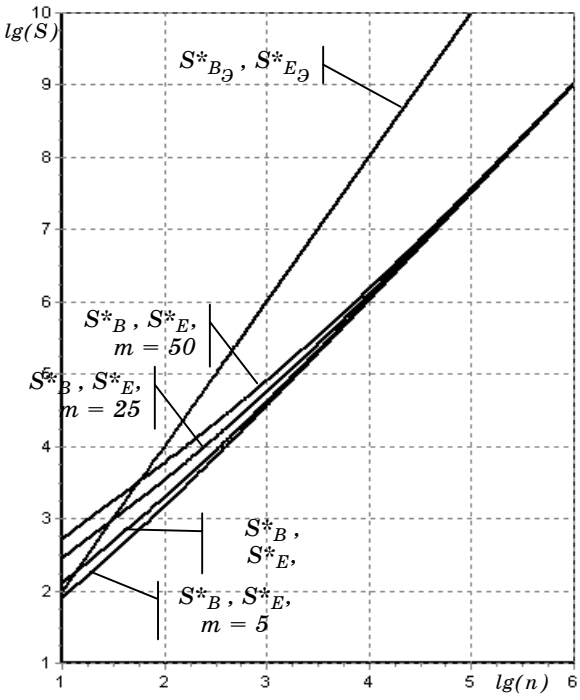

Рисунок 2 - Зависимости асимптотической сложности реализации алгоритмов декодирования кодограмм

Анализ выражений (1) – (6) показывает, что временная и емкостная асимптотическая сложность алгоритмов декодирования кодограммы в разработанных каскадных теоретико-кодовых схемах определяется суммарными временными затратами и затратами элементов памяти на снятие действия матриц маскирования и декодирования кодовых слов обобщенного каскадного кода.

При этом асимптотические временная и емкостная сложности алгоритмов декодирования кодограмм существенно ниже (примерно в $\sqrt{n}$ раз) по сравнению с декодированием кодограмм в

теоретико-кодовых схемах, построенных на эквивалентном двоичном линейном блоковом (n, k, d) коде.

На рис. 2 представлены зависимости асимптотической сложности реализации алгоритмов декодирования кодограмм в предлагаемых каскадных теоретико-кодовых схемах.

Анализ зависимостей, приведенных на рис. 2, показывает, что для кодограмм длиной в сотни символов выигрыш в сложности реализации алгоритмов декодирования составляет один - два порядка. При изменении порядка обобщенного каскадного кода сложность реализации алгоритмов декодирования изменяется слабо, что практически не оказывает существенного влияния на окончательный выбор параметров каскадной кодовой конструкции.

ВЫВОДЫ

Предложены алгоритмы декодирования кодограмм, которые основаны на последовательном выполнении процедуры демаскирования обобщенного каскадного кода и процедуры декодирования соответствующего кодового слова, что позволяет за конечное число шагов декодировать кодограмму в каскадных теоретико-кодовых схемах. При этом процедуры декодирования кодограмм в разработанных схемах выполняются по алгоритмам, сложность которых растет полиномиально от длины кода.

Исследование временной и емкостной сложности предложенного алгоритма показало, что его реализация для коротких кодограмм (несколько сотен бит) значительно (на один - два порядка) проще по сравнению с традиционными кодовыми конструкциями и сопоставима с широкоизвестными блочно-симметричными криптоалгоритмами. Показано, что рост этих сложностей в пределе при увеличении размера задачи (асимптотическая сложность) существенно ниже, чем в случае использования традиционных кодовых схем защиты информации.

SUMMARY

We offer an algorithm of decoding codegrams in cascade code theoretical schemes, based on camouflaging the codes of external level of summarized cascade code.

Time and capacity complexity of designed algorithm is produced out.

СПИСОК ЛИТЕРАТУРЫ

1. Сидельников В.М. Криптография и теория кодирования // Материалы конференции «Московский университет и развитие криптографии в России», МГУ. – 2002. – 22 с.
2. Кузнецов А.А., Грабчак В.И., Евсеев С.П. Каскадные кодовые схемы защиты информации // Системи обробки інформації. – Харків: ХУ ПС. –2005. – Вип. 9 (49). – С. 206 – 211.
3. Шнайер Б. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си. – М.: Издательство ТРИУМФ, 2003. – 816 с.
4. Стасев Ю.В., Кузнецов А.А., Евсеев С.П., Лысенко В.Н., Грабчак В.И. Теоретико-кодовые схемы с небольшим объемом ключа // Збірник наукових праць. – Севастополь: Севастопольський ВМІ ім. П.С. Нахімова. – 2005. – Вип. 2(8). – С. 110 – 114.
5. Стасев Ю.В., Кузнецов А.А., Грабчак В.И., Ковтун В.Ю. Разработка теоретико-кодовых схем на обобщенных каскадных кодах // Збірник наукових праць ХУПС. – Харків: ХУПС. – 2006. – Вип. 2 (8). – С. 79-81.
6. Блох Э.Л., Зяблов В.В. Обобщенные каскадные коды. – М.: Связь, 1976. – 240с.
7. Кузнецов А.А., Грабчак В.И. Алгоритмы формирования и декодирования кодограмм в каскадных теоретико-кодовых схемах // Проблеми інформатики і моделювання: Матеріали шостої міжнародної науково-технічної конференції. – Х.: НТУ „ХПІ”, 2006. – С. 15.
8. Блейхут Р. Теория и практика кодов, контролирующих ошибки / Пер. с англ. – М.: Мир, 1986. – 576 с.

Поступила в редакцию 28 декабря 2006 г.