УДК 621.391

Ю.В. Стасев, А.А. Кузнецов, В.И. Грабчак, В.Ю. Ковтун

РАЗРАБОТКА ТЕОРЕТИКО-КОДОВЫХ СХЕМ НА ОБОБЩЕННЫХ КАСКАДНЫХ КОДАХ

Исследуются секретные системы на алгебраических блоковых кодах (теоретико-кодовые схемы). Разрабатываются теоретико-кодовые схемы на обобщенных каскадных кодах, выводятся основные аналитические соотношения по оценке их параметров.

Постановка проблемы в общем виде и анализ литературы. Перспективным направлением в развитии теории секретных систем является разработка и исследование теоретико-кодовых схем – секретных систем доказуемой стойкости, задача взлома которых сводится к решению теоретико-сложностной задачи декодирования случайного кода [1 – 4]. Известные методы построения теоретико-кодовых схем обладают рядом недостатков: большим объемом ключевых данных и высокой, по сравнению с блочно-симметричными криптоалгоритмами, сложностью реализации [3 – 4]. Перспективным направлением их развития является разработка теоретико-кодовых схем на каскадных кодовых конструкциях. Их использование, как показано в данной работе, позволяет построить секретную систему, свободную от указанных недостатков.

Построение теоретико-кодовых схем. По определению [1 – 4], теоретико-кодовая схема – это секретная система, построенная с использованием трудноразрешимой задачи декодирования случайного (n, k, d) кода над GF(q). Формально она задается совокупностью следующих множеств:

– множество открытых текстов

$$M = \{M_1, M_2, \ldots, M_q k\},$$

где $M_i = \{I_1, I_2, \ldots, I_k\}$, $\forall I_j \in GF(q)$;

– множество криптограмм

$$E = \{E_1, E_2, \ldots, E_q k\},$$

где $E_i = \{C_1, C_2, \ldots, C_n\}$, $\forall C_j \in GF(q)$;

– множество прямых отображений

$$\varphi = \{\varphi_1, \varphi_2, \ldots, \varphi_s\},$$

где $\varphi_i: M \to E$, $i = 1, 2, \ldots, s$;

– множество обратных отображений

$$\varphi^{-1} = \{\varphi_1^{-1}, \varphi_2^{-1}, \ldots, \varphi_s^{-1}\},$$

где $\varphi_i^{-1}: E \to M$, $i = 1, 2, \ldots, s$;

– множество ключей, параметризирующих прямые отображения

$$K = \{K_1, K_2, \ldots, K_s\} = \{G_X^1, G_X^2, \ldots, G_X^s\},$$

т.е. $\varphi_i : M \xrightarrow{K_i} E$;

– множество ключей, параметризирующих обратные отображения

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

т.е. $\varphi_i^{-1} : E \xrightarrow{K_i^*} M$,

таких, что сложность выполнения обратного отображения φ^{-1} без знания ключа $K_i^* \in K^*$ сопряжена с решением теоретико-сложностной задачи декодирования случайного кода (кода общего положения).

Таким образом, алгебраический (n, k, d) код с быстрым алгоритмом декодирования маскируется под случайный (n, k, d) код посредством умножения генераторной матрицы G^i, $i = 1..s$, на хранящиеся в секрете маскирующие матрицы X^i, P^i и D^i:

$$G_X^i = X^i \cdot G^i \cdot P^i \cdot D^i.$$

Не зная правила маскировки, противник вынужден использовать сложный алгоритм декодирования случайного кода [3]. Напротив, уполномоченный пользователь, знающий правило маскировки, может воспользоваться быстрым алгоритмом декодирования алгебраического кода. Под прямым отображением (шифрованием) $\varphi_i : M \xrightarrow{K_i} E$ в классических теретико-кодовых схемах понимается процедура кодирования замаскированным алгебраическим кодом и добавлением к нему случайного вектора ошибки (с весом ошибки меньшей или равной исправляющей способности кода):

$$C_X^j = M_j \cdot G_X^i + e,$$

где $e = \{e_1, e_2, \ldots, e_n\}$, $w(e) \le t = (d - 1)/2$.

Под обратным отображением (расшифрованием) $\varphi_i^{-1} : E \xrightarrow{K_i^*} M$ понимается процесс декодирования кодового слова с ошибками замаскированного кода.

Построение каскадных теоретико-кодовых схем. Для построения каскадной теоретико-кодовой схемы зафиксируем обобщенный каскадный код порядка m. По определению [5] 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}). Величины $a_i > 0$ и $b_i \ge 0$, определяющие внутреннюю структуру обобщенного каскадного (n, k, d) кода, выбираются произвольно, при этом (n, k, d) параметры удовлетворяют следующим соотношениям:

$$n = n_1 n_2; \quad k = \sum_{i=1}^{m+1} a_i b_i;$$

$$d \ge \begin{cases} \min\left\{ d_{1i} d_{2i} : i = \overline{1,m} \right\} \text{при } b_{m+1} = 0, \\ \min\left\{ d_{2m+1}, d_{1i} d_{2i} : i = \overline{1,m} \right\} \text{при } b_{m+1} \neq 0. \end{cases}$$

Согласно сделанным в работе [6] выводам, наиболее эффективным (с точки зрения объемов ключевых данных) вариантом построения теоретико-кодовых схем на обобщенных каскадных кодах является маскирование всех кодов второй ступени. В этом случае под прямым отображением (шифрованием) $\varphi_i : M \xrightarrow{K_i} E$ будем понимать процедуру кодирования обобщенным каскадным кодом с замаскированными кодами внешней ступени и добавлением к нему случайного вектора ошибки (с весом ошибки меньшей или равной исправляющей способности кода). Под обратным отображением (расшифрованием) $\varphi_i^{-1} : E \xrightarrow{K_i^*} M$ будем понимать процесс декодирования кодового слова с ошибками обобщенного каскадного кода с замаскированным кодом внешней степени. Прямое отображение параметризируем ключом $K_i \in K$, который однозначно задает замаскированный код (например, в виде совокупности порождающих и/или проверочных матриц обобщенного кода). Обратное отображение параметризируем ключом $K_i^* \in K^*$, который позволяет восстановить правило быстрого декодирования (например с помощью матриц маскировки). Введем абстрактное определение каскадной теоретико-кодовой схемы построенной по обобщенному каскадному (n, k, d) коду порядка m как совокупность следующих множеств:

– множество открытых текстов

$$M = \{M_1, M_2, \ldots, M_q k\},$$

где каждое M_i представляет собой информационный блок вида

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

– множество криптограмм

$$E = \{E_1, E_2, \ldots, E_q k\},$$

где каждое E_i представляет собой кодовое слово вида $E_i = C_i + e_i$, т.е. сумму кодового слова обобщенного каскадного кода со случайным вектором ошибки e_i, причем

$$C_i = \{(C_{1,1}, C_{1,2}, ..., C_{1,a_1}), (C_{2,1}, C_{2,2}, ..., C_{2,a_1}), ..., (C_{n_2,1}, C_{n_2,2}, ..., C_{n_2,a_1}), (C_{1,1}, C_{1,2}, ..., C_{1,a_2}), (C_{2,1}, C_{2,2}, ..., C_{2,a_2}), ..., (C_{n_2,1}, C_{n_2,2}, ..., C_{n_2,a_2}), ..., (C_{1,1}, C_{1,2}, ..., I_{1,a_{m+1}}), (C_{2,1}, C_{2,2}, ..., C_{2,a_{m+1}}), ..., (C_{n_2,1}, C_{n_2,2}, ..., C_{n_2,a_{m+1}})\},$$

или

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

где $\gamma_{i,j} = (C_{j,1}, C_{j,2}, ..., C_{j,a_i})$.

Таким образом, кодограммой является вектор

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

где $\gamma^*_{ij} = \gamma_{ij} + e_{ij}$ – двоичный вектор длины a_i,

$$\sum_{i=1}^{m+1} a_i = n_1;$$

e_{ij} – элементы случайного вектора ошибок длины a_i (сеансовый ключ), который удовлетворяет системе ограничений

$$w(e_{i,1}, e_{i,2}, ..., e_{i,n_2}) \le t_{2i} = (d_{2i} - 1)/2;$$

– множество прямых отображений

$$\varphi = \{\varphi_1, \varphi_2, \ldots, \varphi_s\},$$

где $\varphi_i : M \to E$, i = 1, 2 , …, s;

– множество обратных отображений

$$\varphi^{-1} = \{\varphi_1^{-1}, \varphi_2^{-1}, \ldots, \varphi_s^{-1}\},$$

где $\varphi_i^{-1} : E \to M$, i = 1, 2 , …, s;

– множество ключей, параметризирующих прямые отображения

$$K = \{K_1, K_2, ..., K_s\}, \text{ т.е. } \varphi_i : M \xrightarrow{K_i} E,$$

где $K_i = \{G_X^1, G_X^2, ..., G_X^{m+1}\}$ – множество генераторных матриц, которые задают m+1 замаскированных кодов внешней ступени;

– множество ключей, параметризирующих обратные отображения

$$K^* = \{K_1^*, K_2^*, ..., K_s^*\}, \text{ т.е. } \varphi_i^{-1} : E \xrightarrow{K_i^*} M,$$

где

$K_i^* = \{\{X^1, P^1, D^1\}, \{X^2, P^2, D^2\}, ..., \{X^{m+1}, P^{m+1}, D^{m+1}\}\}$ – множество матриц, которые маскируют m+1 кодов внешней ступени.

Для оценки параметров каскадной теоретико-кодовой схемы сформулируем и докажем следующую теорему.

Теорема. Пусть задана каскадная теоретико-кодовая схема по обобщенному каскадному коду порядка *m* путем маскировки всех его кодов второй ступени. Тогда объем ключа (в битах) прямого отображения задается выражением

$$l_K = n_2 \sum_{j=1}^{m+1} b_j \cdot a_j, \qquad (1)$$

объем ключа (в битах) обратного отображения задается формулой

$$l_{K^*} = n_2{}^2 \sum_{i=1}^{m+1} b_i{}^2 \cdot a_j, \qquad (2)$$

длина информационного блока данных и длина ко-

дограммы (в битах) задаются, соответственно, выражениями:

$$l_M = \sum_{j=1}^{m+1} b_j \cdot a_j ; \quad (3) \qquad l_E = n_1 \cdot n_2 , \quad (4)$$

а относительная скорость передачи данных задается

$$R = \frac{1}{n_1 \cdot n_2} \sum_{j=1}^{m+1} b_j \cdot a_j . \quad (5)$$

Доказательство. Для маскировки всех кодов второй ступени обобщенного каскадного кода порядка m выполняется процедура умножения соответствующих порождающих матриц $G^1, G^2, ..., G^{m+1}$ на матрицы маскировки

$$\{X^1, P^1, D^1\}, \{X^2, P^2, D^2\}, ..., \{X^{m+1}, P^{m+1}, D^{m+1}\}:$$

$$G_X^1 = X^1 \cdot G^1 \cdot P^1 \cdot D^1 ,$$

$$\dots$$

$$G_X^{m+1} = X^{m+1} \cdot G^{m+1} \cdot P^{m+1} \cdot D^{m+1} .$$

Следовательно, для хранения ключа прямого отображения необходимо сберегать $m + 1$ матриц, размер каждой из которых задается параметрами соответствующего кода внешней ступени обобщенного каскадного кода. Так, например, матрица G_X^j задает замаскированный (n_2, b_j, d_{2j}) код внешней ступени, т.е. имеет размерность $n_2 \times b_j$ символов из $GF(2^{a_j})$. Практически это означает, что для хранения элементов матрицы G_X^j потребуется $n_2 \cdot b_j \cdot a_j$ бит. Всего для хранения ключа прямого отображения потребуется

$$l_K = \sum_{j=1}^{m+1} n_2 \cdot b_j \cdot a_j = n_2 \sum_{j=1}^{m+1} b_j \cdot a_j \text{ бит.}$$

Для хранения соответствующего ключа обратного отображения необходимо сохранять матрицы $\{X^j, P^j, D^j\}$, $j = 1,..,m + 1$. Матрица X^j имеет размерность $b_j \times b_j$ символов из $GF(2^{a_j})$, а матрица $\Lambda^j = P^j \cdot D^j$ имеет размерность $n_2 \times n_2$ символов из $GF(2^{a_j})$. Практически это означает, что для хранения ключа обратного отображения как совокупности маскирующих матриц

$$\{X^1, P^1, D^1\}, \{X^2, P^2, D^2\}, ..., \{X^{m+1}, P^{m+1}, D^{m+1}\}$$

необходимо сберегать

$$l_{K^*} = \sum_{j=1}^{m+1} \left(b_j \cdot b_j \cdot a_j + n_2 \cdot n_2 \cdot a_j \right) = {n_2}^2 \sum_{i=1}^{m+1} {b_i}^2 \cdot a_j \text{ бит.}$$

Длина информационного блока l_M, длина кодограммы l_E и относительная скорость передачи информации $R = l_M/l_E$ определяются соответствующими параметрами обобщенного каскадного кода:

$$l_M = k = \sum_{j=1}^{m+1} b_j \cdot a_j , \; l_E = n = n_1 \cdot n_2 , \; R = \frac{l_M}{l_E} = \frac{1}{n_1 \cdot n_2} \sum_{j=1}^{m+1} b_j \cdot a_j ,$$

что и завершает доказательство.

Сформулированная теорема устанавливает важную взаимосвязь между параметрами обобщенного каскадного кода и основными показателями каскадной теоретико-кодовой схемы. Выражения (1) – (5) раскрывают аналитическую зависимость между кодовыми характеристиками кодов внешней ступени обобщенного каскадного кода и характеристиками построенной на их основе криптосистемы.

Анализ полученных соотношений показывает, что применение обобщенных каскадных кодов позволяет строить кодовые схемы защиты информации с небольшими размерами ключевых данных. Сложность реализации операций шифрования и рас шифрования определяется сложностью операций кодирования и декодирования обобщенным каскадным кодом.

Выводы. В результате проведенных исследований разработаны каскадные теоретико-кодовые схемы, основанные на операции маскирования кодов внешней ступени обобщенного каскадного кода. Получены основные аналитические соотношения по оценке их параметров. Показано, что использование каскадных конструкций снимает основные практические ограничения по объему ключа и сложности реализации.

Перспективным направлением дальнейших исследований является разработка каскадных теоретико-кодовых схем с алгеброгеометрическими кодами на внешней ступени обобщенного каскадного кода, оценка их параметров.

ЛИТЕРАТУРА

1. 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.

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

3. Сидельников В.М. Криптография и теория кодирования // Материалы НТК «МГУ и развитие криптографии в России». – М.: МГУ. – 2002. – 22 с.

4. Стасев Ю.В., Кузнецов А.А. Несимметричные теоретико-кодовые схемы с использованием алгеброгеометрических кодов // Кибернетика и системный анализ. – 2005. – № 3. – С. 47-57.

5. Блох Э.Л., Зяблов В.В. Обобщенные каскадные коды (Алгебраическая теория и сложность реализации). – М.: Связь, 1976. – 240 с.

6. Кузнецов А.А., Грабчак В.И., Евсеев С.П. Каскадные кодовые схемы защиты информации // Системи обробки інформації. – Х.: ХУ ПС. – 2005. – Вип. 9 (49). – С. 206-211.

Поступила 19.01.2006

Рецензент: доктор технических наук, профессор И.Д. Горбенко, Харьковский национальный университет радиоэлектроники, Харьков.