УДК 512.817 : 621.391.25

СИММЕТРИЧНЫЕ ТЕОРЕТИКО-КОДОВЫЕ СХЕМЫ НА АЛЬТЕРНАНТНЫХ КОДАХ

А.А. Кузнецов
(Харьковский университет Воздушных Сил)

Установлена аналитическая зависимость между кодовыми характеристиками обширного класса альтернантных кодов и параметрами симметричных криптосистем на их основе по схеме Рао-Нама. Показано, что криптосистемы на ОРС кодах могут быть взломаны алгоритмом полиномиальной сложности и криптосистемы на альтернантных кодах (подкодах ОРС кодов) также недостаточно стойки.

симметричные криптосистемы, алгебраические блоковые коды, альтернантные коды, схема Рао-Нама, криптограмма

Постановка проблемы в общем виде, анализ литературы. Симметричные криптосистемы на алгебраических блоковых кодах (теоретико-кодовые схемы) впервые предложены в работе Рао и Нама [1]. В основе таких криптосистем лежит маскировка кода с быстрым алгоритмом декодирования (полиномиальной сложности) под произвольный (случайный) линейный код, декодирование которого представляется как вычислительно сложная задача. Шифрованная информация (криптограмма) в виде вектора c* длины n формируется по правилу

$$c^* = I \cdot G + e, \qquad (1)$$

где вектор $c = I \cdot G$ принадлежит (n, k, d) коду с порождающей матрицей G; I – k-разрядный информационный вектор; вектор e – секретный (случайный) вектор ошибок.

В работах [2 – 3] исследована возможность одновременного повышения безопасности и помехоустойчивости каналов передачи данных на основе использования симметричных криптосистем с алгебраическими блоковыми кодами. В тоже время основным недостатком схемы Рао-Нама является большой объем ключа. Действительно, для хранения секретной порождающей матрицы (n, k, d) блокового кода над GF(q) необходимо хранить, в общем случае, $n \times k$ q-ичных символов. Параметры криптосистемы над $GF(2^m)$ определяются следующими выражениями:

– размерность секретного ключа (в битах)

$$l_{K+} = k \cdot n \cdot m; \qquad (2)$$

© А.А. Кузнецов

– размерность информационного вектора (в битах):

$$l_I = k \cdot m; \tag{3}$$

– размерность криптограммы (в битах)

$$l_S = n \cdot m; \tag{4}$$

– относительная скорость передачи

$$R = l_I / l_S = k / n. \tag{5}$$

В статье рассматриваются теоретико-кодовые схемы, построенные на обширных классах альтернантных кодов, теоретически обосновывается построение симметричных криптосистем с небольшим объемом ключевых данных.

Симметричные криптосистемы на альтернантных кодах. Воспользуемся определением обобщенных кодов Рида-Соломона и их подкодов – альтернантных кодов [4 – 5].

***Определение* 1**. Пусть $X = (X_1, X_2, \ldots, X_n)$ вектор над $GF(q^m)$, причем все X_i – различные элементы $GF(q^m)$. Пусть также $h = (h_1, h_2, \ldots, h_n)$ – вектор над $GF(q^m)$ с необязательно различными h_i элементами $GF(q^m)$. Тогда (n, k, d) обобщенный код Рида-Соломона $ОРС_k(X, h)$ состоит из всех векторов вида

$$(h_1 \cdot F(X_1), h_2 \cdot F(X_2), \ldots, h_n \cdot F(X_n)),$$

где F(x) – любой многочлен с коэффициентами из $GF(q^m)$, степень которого не превосходит k. Код ОРС является кодом с максимально достижимым кодовым расстоянием, т.е. $d = r + 1$, $r = n - k$. Проверочная матрица $ОРС_k(X, h)$ равна:

$$H = \begin{pmatrix} 1 & 1 & \ldots & 1 \\ X_1 & X_2 & \ldots & X_n \\ X_1^2 & X_2^2 & \ldots & X_n^2 \\ \ldots & \ldots & \ldots & \ldots \\ X_1^{r-1} & X_2^{r-1} & \ldots & X_1^{r-1} \end{pmatrix} \cdot \begin{pmatrix} Y_1 & 0 & \ldots & 0 \\ 0 & Y_2 & \ldots & 0 \\ 0 & 0 & \ldots & 0 \\ \ldots & \ldots & \ldots & \ldots \\ 0 & 0 & \ldots & Y_n \end{pmatrix}, \tag{6}$$

где $\forall Y_i \in GF(q^m)$, $Y_i \neq 0$ и $ОРС^{\perp}_k(X, h) = ОРС_r(X, Y)$. Коды ОРС дают механизм построения обширного класса альтернантных кодов [4 – 5].

***Определение* 2**. Альтернантный (n, k, d) код A(X, h) состоит из всех слов кода $ОРС^{\perp}_k(X, h)$ таких, что их компоненты лежат в поле GF(q). Другими словами, A(X, h) равен ограничению кода $ОРС_k(X, h)$ на подполе GF(q) и состоит из всех векторов X над GF(q), удовлетворяющих равенству $H \cdot X^T = 0$, где H – проверочная матрица $ОРС_k(X, h)$, задавае-

мая выражением (6). Параметры альтернантного (n, k, d) кода A(X, h) связаны соотношением

$$n - mr \le k \le n - r;\ d \ge r + 1.$$

Альтернантные коды представляют собой обширный класс линейных блоковых кодов и обобщают (содержат как подкласс) все циклические коды, коды БЧХ и их обобщения, коды Гоппы, Сривэставы и др. [4 – 5]. Зададим симметричную теоретико-кодовую схему Рао-Нама на альтернантных кодах.

***Лемма* 1**. Альтернантный (n, k, d) код над GF(q) определяет симметричную теоретико-кодовую схему Рао-Нама с параметрами (в битах):

$$(n - (d - 1)\cdot m) \cdot \log_2(q) \le l_{K+} \le (n - d + 1) \cdot n \cdot \log_2(q); \quad (7)$$

$$(n - (d - 1)\cdot m) \cdot \log_2(q) \le l_I \le (n - d + 1) \cdot \log_2(q); \quad (8)$$

$$l_S = n \cdot \log_2(q); \quad (9)$$

$$(n - (d - 1)\cdot m) / n \le R \le (n - d + 1) / n. \quad (10)$$

Доказательство. Параметры криптосистемы на алгебраических блоковых кодах связаны соотношениями (2) – (5): $l_{K+} = k \cdot n \cdot m$; $l_I = k \cdot m$; $l_S = n \cdot m$; $R = k/n$. Параметры альтернантного (n, k, d) кода A(X, h) связаны соотношением: $n - mr \le k \le n - r$; $d \ge r + 1$, где A(X, h) задан через ограничение кода ОРС над $GF(q^m)$. После подстановки получим (7) – (10).

Результат леммы дает выражения по оценке параметров симметричных криптосистем на альтернантных кодах. В тоже время из определения альтернантных кодов следует, что для однозначного построения проверочной матрицы кода необходимо и достаточно определить символы вектора-шаблона $Y = (Y_1, Y_2, \ldots, Y_n)$. Практически это означает, что длина секретных ключевых данных в криптосистеме на альтернантных кодах будет определяться числом элементов вектора-шаблона Y, т.е. справедлива следующая теорема.

***Теорема* 1**. Длина секретных ключевых данных в криптосистеме на альтернантных (n, k, d) кодах над GF(q), заданных через ограничение ОРС кода над $GF(q^m)$, определяется выражением (в битах)

$$l_{K+} = n \cdot m \cdot \log_2(q). \quad (11)$$

Доказательство. Для определения всех коэффициентов проверочной матрицы альтернантного кода (6) необходимо и достаточно определить все элементы вектора $Y = (Y_1, Y_2, \ldots, Y_n)$. Размерность вектора $Y = (Y_1, Y_2, \ldots, Y_n)$ – n символов из $GF(q^m)$. Следовательно, для того, чтобы определить секретный ключ – проверочную матрицу кода потребуется n символов из $GF(q^m)$ или, что эквивалентно, $n \cdot m \cdot \log_2(q)$ бит.

Выражения (7 – 10) справедливы для криптосистем, построенных на всех кодах из обширного класса альтернантных кодов. Следующая лемма уточняет параметры криптосистем, построенных на кодах Гоппы.

Лемма 2. Альтернантный (n, k, d) код Гоппы Γ(L, G) над GF(q) определяет симметричную криптосистему с параметрами:

$$l_{K+} = n \cdot m \cdot \log_2(q); \quad (12)$$

$$l_I \geq (d - 1) \cdot m \cdot \log_2(q); \quad (13)$$

$$l_S = n \cdot \log_2(q); \quad (14)$$

$$R \geq (n - (d - 1) \cdot m) / n. \quad (15)$$

Доказательство. Альтернантный (n, k, d) код Гоппы Γ(L, G) над GF(q) состоит из всех векторов $c = (c_1, c_2, \ldots, c_n)$ таких, что

$$R_c(x) \equiv 0 \bmod G(x),$$

где

$$R_c(x) = \sum_{i=1}^{n} \frac{c_i}{x - \alpha_i},$$

G(x) – многочлен с коэффициентами из $GF(q^m)$ (многочлен Гоппы), $L = (\alpha_1, \alpha_2, \ldots, \alpha_n)$ – подмножество элементов из $GF(q^m)$ таких, что $G(\alpha_i) \neq 0 \ \forall \alpha_i \in L$ [6]. Параметры (n, k, d) кода Гоппы Γ(L, G) связаны соотношениями: $n = |L|$, $k \geq n - mr$, $r = \deg G(x)$, $d \geq r + 1$. Подставим эти значения в выражения (2) – (5), с учетом (7) – (10) и (11) получим соотношения (12) – (15).

Последняя лемма определяет криптосистему на альтернантых кодах Гоппы, заданных матричным способом. В тоже время, как показано в работах [2 – 3], выражение (12) можно существенно упростить. Для этого воспользуемся описанием кода Гоппы, через многочлен Гоппы G(x). Справедлива теорема.

Теорема 2. Альтернантный (n, k, d) код Гоппы Γ(L, G) над GF(q), заданный через многочлен Гоппы G(x), определяет симметричную теоретико-кодовую схему Рао-Нама с длиной ключа:

$$l_{K+} \leq d \cdot \log_2(q); \quad (16)$$

Доказательство. Многочлен Гоппы G(x) однозначно задает код Гоппы Γ(L, G) над GF(q). Действительно, как показано в [4 – 5] проверочную матрицу кода Гоппы можно записать в виде (6), где $Y_1 = G^{-1}(\alpha_1)$, $Y_2 = G^{-1}(\alpha_2)$, …, $Y_n = G^{-1}(\alpha_n)$, т.е. все элементы матрицы однозначно задаются значениями многочлена G(x) в элементах вектора $L = (\alpha_1, \alpha_2, \ldots, \alpha_n)$ – подмножества элементов из $GF(q^m)$. Этого достаточно, чтобы задать симметричную криптосистему Рао-Нама. Секретным ключом в этом случае будет выступать многочлен G(x), степень которого равна

deg G(x) = r ≤ d – 1 [4 – 5]. Практически это означает, что секретный ключ полностью определяется deg G(x) + 1= r + 1 ≤ d значениями коэффициентов многочлена G(x), т.е. выражение (12) перепишется в виде $l_{K+} \le d \log_2(q)$, что и завершает доказательство.

Выводы. Выражения (7) – (16) устанавливают аналитическую зависимость между кодовыми характеристиками обширного класса альтернантных кодов и параметрами симметричных криптосистем на их основе по схеме Рао-Нама. В тоже время в работе [5 – 7] показано, что криптосистемы на ОРС кодах могут быть взломаны алгоритмом полиномиальной сложности. Криптосистемы на альтернантных кодах (подкодах ОРС кодов) также считаются недостаточно стойкими.

Перспективным направлением в развитии теоретико-кодовых схем являются криптосистемы на алгеброгеометрических кодах.

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. Королева. – 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. *Мак–Вильямс Ф.Дж., Слоэн Н.Дж.А. Теория кодов, исправляющих ошибки.– М.: Связь. – 1979. – 744 с.*
5. *Блейхут Р. Теория и практика кодов, контролирующих ошибки. – М.: Мир, 1986. – 576 с.*
6. *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.*
7. *Сидельников В.М. Криптография и теория кодирования // Материалы конференции «Московский университет и развитие криптографии в России». – М.: МГУ. – 2002. – 22 с.*

Поступила 18.02.2005

Рецензент: доктор технических наук, профессор Ю.В. Стасев,
Харьковский университет Воздушных Сил.