ОБОЗРЕНИЕ
ПРИКЛАДНОЙ И ПРОМЫШЛЕННОЙ
Том 24 МАТЕМАТИКИ Выпуск 5
2017

Д. В. Загуменнов, В. В. Мкртичян (Ростов-на-Дону, ЮФУ).
О достаточных условиях применимости алгеброгеометрических кодов L-конструкции как кодов защиты от копирования.

Рассматривается схема специального широковещательного шифрования — ССШШ [1]. В ССШШ допускаются атаки коалиций, состоящих из легальных пользователей схемы. Для борьбы с атаками коалиций мощности c в [2], [3] предложен метод обнаружения членов коалиций, являющийся эффективным при использовании некоторых классов кодов, например c-ТА кодов ([2], определение 1), а также быстрых алгоритмов списочного декодирования. В [4], [5] исследуется возможность эффективного применения в ССШШ кодов Рида–Соломона и Рида–Маллера соответственно. Интересной представляется задача определения, являются ли алгеброгеометрические коды (АГ-коды) L-конструкции ([6], 4.1.1) и списочный декодера Судана–Гурусвами (СДСГ) [7], пригодными для эффективного использования в ССШШ с $N(\in \mathbb{N})$ пользователями. Под эффективностью здесь понимается существование алгоритма определения пользователей из коалиции злоумышленников мощности c, работающий за полиномиальное время.

Далее будем использовать следующие обозначения: C — алгеброгеометрический $[n, k, d]_q$-код L-конструкции, g — род кривой, на которой построен код, D — дивизор кода C, $\deg(D) = \alpha$ — степень дивизора D.

Рассмотрим следующее неравенство:

$$\alpha > 2g - 2\,. \tag{1}$$

Утверждение 1. *Код C возможно использовать для построения* ССШШ *с N пользователями, если выполнено условие*:

$$\alpha \geqslant \log_q N + g - 1\,. \tag{2}$$

Утверждение 2. *Код C является c-*ТА*-кодом, если выполняется условие*:

$$c < \sqrt{\frac{n}{\alpha}}\,.$$

Если выполнено (1), *то это условие можно представить в виде*:

$$c < \sqrt{\frac{n}{k+g-1}}. \tag{3}$$

Утверждение 3. *Если* $\sqrt{n(k+g-1)} \notin \mathbb{N}$, *то* СДСГ *для кода C применим при построении* ССШШ, *если выполняются условия* (1) *и*

$$c \leqslant \frac{n}{\lceil \sqrt{n(k+g-1)}\ \rceil}\,. \tag{4}$$

Если $\sqrt{n(k+g-1)} \in \mathbb{N}$, *то* СДСГ *для кода* C *применим при построении* ССШШ, *если выполняются условия* (1) *и*

$$c \leqslant \frac{n}{\sqrt{n(k+g-1)}+1}\,. \tag{5}$$

Причем при выполнении условия (5) *выполняется и условие* (4), *а при выполнении* (4) *выполняется* (3).

Таким образом, для возможности эффективного применения АГ-кода C и СДСГ достаточно выполнения условий (4) или (5), а также (2).

Утверждение 4. *Пусть существует алгоритм построения кривой рода* g *с числом точек больше заданного числа* l, *работающий за полиномиальное время. Тогда существует алгоритм, работающий за полиномиальное время, принимающий на вход значения максимальной мощности коалиции злоумышленников* c, *числа пользователей* N *и мощности поля* q *и выдающий на выходе порождающую матрицу АГ-кода* C, *применимого в* ССШШ.

Данный алгоритм построен и публикуется отдельно.

Отметим, что полученные достаточные условия при некоторых параметрах ССШШ не гарантируют существования подходящих классических кодов. Например, для параметров $q = 8$, $N = 512$, $c = 2$ не гарантируется существование кода Рида–Соломона или кода на эллиптической кривой, применимого для построения ССШШ с такими параметрами, хотя это и не означает, что таковых не существует. Заметим, однако, что, используя только достаточные условия, можно построить код с более сложной структурой, применимый для построения ССШШ с указанными параметрами. Например, для этих параметров алгоритм строит порождающую матрицу $[22, 3, d \geqslant 17]_8$-кода на кривой рода 3, заданной уравнением $X^3Y + Y^3Z + Z^3X = 0$.

СПИСОК ЛИТЕРАТУРЫ

1. *Chor B.*, *Fiat A.*, *Naor M.* Tracing Traitors. Heidelberg etc.: Springer, 1994, p. 257–270.
2. *Staddon J. N.*, *Stinson D. R.*, *Wei R.* Combinatorial properties of frame proof and traceability codes. — IEEE Trans. Inform. Theory, 2001, v. IT-47, is. 3, p. 1042–1049.
3. *Silverberg A.*, *Staddon J.*, *Walker J.* Applications of list decoding to tracing traitors. — IEEE Trans. Inform. Theory, 2003, v. IT-49, is. 5, p. 1312–1318.
4. *Деундяк В. М.*, *Мкртичян В. В.* Исследование границ применения схемы защиты информации, основанной на РС-кодах. — Дискретный анализ и исследование операций, 2011, т. 18, № 3, с. 21–38.
5. *Деундяк В. М.*, *Евпак С. А.*, *Мкртичян В .В.* Исследование свойств q-ичных помехоустойчивых кодов Рида–Маллера как кодов для защиты от копирования. — Проблемы передачи информации, 2015, т. 51, № 4, с. 99–111.
6. *Влэдуц С. Г.*, *Ногин Д. Ю.* , *Цфасман М. А.* Алгеброгеометрические коды. Основные понятия. М.: МЦНМО, 2003, 504 с.
7. *Guruswami V.* , *Sudan M.* Improved decoding of Reed–Solomon and algebraic-geometric codes. In: 39rd Annual Symposium on Foundations of Computer Science. Proceedings. (Palo Alto, CA, November 8–11, 1998.) Piscataway, NJ: IEEE, 1998, p. 28–37.