Секция «Математическая логика, алгебра и теория чисел»

Об исследовании границ применения схемы широковещательного шифрования, основанной на некоторых АГ-кодах

Научный руководитель – Деундяк Владимир Михайлович

Загуменнов Денис Владимирович

Аспирант

Южный федеральный университет, Институт математики, механики и компьютерных наук им. И.И. Воровича, Ростов-на-Дону, Россия

E-mail: zagumionnov.denis@yandex.ru

В [1] рассмотрен перспективный способ применения помехоустойчивых кодов для защиты от несанкционированного копирования в системах широковещательного шифрования. Для использования в таких системах в настоящее время активно исследуются и применяются классы так называемых c-TA и c-FP-кодов (см., например, [2, 3]). Актуальной является задача определения, являются ли алгеброгеометрические коды (АГ-коды) L-конструкции (см. [4, 5]) применимыми для эффективного использования в системах широковещательного шифрования.

Пусть $\mathbb{F}_q$ — конечное поле мощности q, $C \subset \mathbb{F}_q$ — линейный код, n — длина, k — размерность, d — минимальное кодовое расстояние кода C. Введём следующие обозначения: $I(x,y) = \{i \in \mathbb{N} : 1 \le i \le n, x_i = y_i\}$, $d(x,y) = |\{i \in 1,\dots,n : x_i \neq y_i\}|$.

Пусть $c \in \mathbb{N} \setminus \{1\}$. Коалицией кода C назовём множество $C_0 = \{u^{(1)}, u^{(2)}, \dots, u^{(c)}\}$, где $u^{(i)} \in C$. Число c будем называть мощностью коалиции, а множество коалиций кода мощности не больше c будем обозначать как $\mathrm{coal}_c(C)$. Множеством потомков коалиции C_0 назовём множество

$$\mathrm{desc(C_0)} = \{(y_1, y_2, , \dots, y_n) \in \mathbb{F}_q^n \mid y_i = u_i^{(j)},\ j \in \{1,\dots,c\}\ \}.$$

Код C называется c-FP кодом, если

$$\forall\ v \in C\ \forall\ C_0 \in \mathrm{coal}_c(C \setminus \{v\}) : v \notin \mathrm{desc(C_0)} \setminus C_0,$$

код C называется c-TA кодом, если выполняется следующее условие:

$$\forall\ C_0 \in \mathrm{coal}_c(C)\ \ \forall\ v \in (C \setminus C_0)\ \ \forall\ y \in \mathrm{desc(C_0)}\ \ \exists\ \omega \in C_0 :\ d(w,y) < d(v,y)$$

[1]. Далее C – АГ-код L-конструкции над $\mathbb{F}_q$, g – род кривой, на которой определён код C, D – дивизор кода C, $\alpha = \deg(D) < n$.

Теорема 1. Код C является c-TA-кодом, если выполняется условие:

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

Рассмотрим $\Lambda_{FP} = \{R_{FP}, R_{FP}+1, \dots\} \subset \mathbb{N} \setminus \{1\}$ – множество таких натуральных чисел c, что для кода C не выполняется c-FP свойство, а также аналогично множество $\Lambda_{TA} = \{R_{TA}, R_{TA}+1, \dots\} \subset \mathbb{N} \setminus \{1\}$ – множество таких натуральных чисел c, что для кода C не выполняется c-TA свойство.

Лемма 1. Выполняется следующее утверждение:

$$\forall c \in \mathbb{N} \setminus \{1\}\ \forall v \in C\ \forall C_0 \in \mathrm{coal}_c(C \setminus \{v\})\ \forall \omega \in \mathrm{desc}(C_0) \setminus C_0 : |I(\omega, v)| \le \min\{\alpha c, n\}.$$

Лемма 2. Пусть кривая X задана многочленом F, Q – единственная точка на кривой X вида $(X : Y : 0)$, $D = \alpha Q$. Тогда:

$$\forall c \in \mathbb{N} \setminus \{1\}\ \forall v \in C\ \exists C_0 \in \mathrm{coal}_c(C \setminus \{v\})\ \exists \omega \in \mathrm{desc}(C_0) \setminus C_0 :$$

$$|I(\omega, v)| \geq \min\{c \left\lfloor \frac{\alpha}{\deg(F)} \right\rfloor, n\}$$

Теорема 2. Пусть выполняются условия леммы 2. Тогда:

$$R_{FP} \leq B_{FP} = \left\lceil \frac{n}{\lfloor \frac{\alpha}{\deg(F)} \rfloor} \right\rceil,\ R_{TA} \leq B_{TA} = \left\lceil \frac{n+\alpha}{2 \left\lfloor \frac{\alpha}{\deg(F)} \right\rfloor} \right\rceil.$$

Источники и литература

1) Staddon J. N., Stinson D. R., Wei R. Combinatorial properties of frameproof and traceability codes. // Information Theory, IEEE Transactions on. 2001. Т. 47. No. 3. С. 1042–1049.
2) Деундяк В. М., Мкртичян В. В. Исследование границ применения схемы защиты информации, основанной на РС-кодах. // Дискретный анализ и исследование операций. 2011. Т. 18. No 3. С. 21–38.
3) 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. No. 4. С. 99–111.
4) Hoholdt T., van Lint J. H., Pellikaan R. Algebraic geometry codes // Handbook of coding theory. 1998. Т. 1. No. 1. С. 871–961.
5) Влэдуц С. Г., Ногин Д. Ю., Цфасман М. А. Алгеброгеометрические коды. Основные понятия. // Москва: МЦНМО, 2003. 504 с.