ПРИКЛАДНАЯ ТЕОРИЯ КОДИРОВАНИЯ

УДК 519.7

О ГРАНИЦАХ МОЩНОСТИ ЗЛОУМЫШЛЕННИКОВ ДЛЯ ИДЕНТИФИЦИРУЮЩИХ АЛГЕБРОГЕОМЕТРИЧЕСКИХ КОДОВ НА СПЕЦИАЛЬНЫХ КРИВЫХ[1]

В. М. Деундяк*,**, Д. В. Загуменнов**

*ФГАНУ НИИ «Спецвузавтоматика», г. Ростов-на-Дону, Россия
**Южный федеральный университет, г. Ростов-на-Дону, Россия

Под схемами широковещательного шифрования понимают такие протоколы распространения легально тиражируемой цифровой продукции, которые способны предотвратить несанкционированный доступ к распространяемым данным. Эти схемы широко используются как для распределённого хранения данных, так и для защиты данных при передаче по каналам связи, и исследование таких схем представляется актуальной задачей. Для предотвращения коалиционных атак в схемах широковещательного шифрования используются классы помехоустойчивых кодов со специальными свойствами, в частности c-FP- и c-TA-свойствами. Рассматривается задача оценки нижней и верхней границ мощности коалиции злоумышленников, в пределах которых алгеброгеометрические коды обладают этими свойствами. Ранее были получены границы для одноточечных алгеброгеометрических кодов на кривых общего вида. В работе эти границы уточняются для одноточечных кодов на кривых специального вида; в частности, для кодов на кривых, на которых имеется достаточно много классов эквивалентности после факторизации множества точек кривой по отношению равенства соответствующих координат.

Ключевые слова: *помехоустойчивое кодирование, схемы специального широковещательного шифрования, алгеброгеометрические коды.*

DOI 10.17223/20710410/53/4

THE ATTACKERS POWER BOUNDARIES FOR TRACEABILITY OF ALGEBRAIC GEOMETRIC CODES ON SPECIAL CURVES[2]

V. M. Deundyak*,**, D. V. Zagumennov**

*FGANU NII "Specvuzavtomatika", Rostov-on-Don, Russia
**Southern Federal University, Rostov-on-Don, Russia

E-mail: zagumionnov.denis@yandex.ru, vl.deundyak@gmail.com

Broadcast encryption is a data distribution protocol which can prevent malefactor parties from unauthorized accessing or copying the distributed data. It is widely used in distributed storage and network data protection schemes. To block the so-called coalition attacks on the protocol, classes of error-correcting codes with special

[1]Исследование выполнено при финансовой поддержке РФФИ в рамках научного проекта № 20-31-90098.

[2]Funding: The reported study was funded by RFBR, project no. 20-31-90098.

properties are used, namely c-FP and c-TA properties. We study the problem of evaluating the lower and the upper boundaries on coalition power, within which the algebraic geometry codes possess these properties. Earlier, these boundaries were calculated for single-point algebraic-geometric codes on curves of the general form. Now, we clarified these boundaries for single-point codes on curves of a special form; in particular, for codes on curves on which there are many equivalence classes after factorization by equality of the corresponding points coordinates relation.

Keywords: *traceability codes, frameproof codes, algebraic geometry codes, broadcast encryption.*

Введение

В [1, 2] представлена криптографическая схема широковещательного шифрования, способная обеспечивать защиту легально тиражируемой цифровой продукции от несанкционированного доступа. В этой схеме дистрибьютор распространяет данные свободно в зашифрованном виде, а для обеспечения доступа к этим данным со стороны легальных пользователей он должен выдать каждому из них уникальный набор ключей. Далее пользователи применяют свои ключи для расшифрования и получения доступа к информации. В случае обнаружения нелегального использования ключей их владелец может быть идентифицирован контролёром. Тем не менее допускаются так называемые коалиционные атаки, при которых легальные пользователи объединяются в коалиции злоумышленников и, комбинируя свои ключи, генерируют «пиратские» наборы ключей, которые могут быть использованы с целью выполнения несанкционированного доступа к данным. Если в качестве «пиратского» набора коалиции удается реплицировать набор ключей законопослушного пользователя схемы, не входящего в коалицию, то говорят, что этот набор скомпрометирован.

Для борьбы с коалиционными атаками в [3] предложено усиление этих схем, найденное в использовании специальных классов помехоустойчивых кодов, называемых идентифицирующими кодами (в частности, c-FP- и c-TA-кодов [4, 5]), а также быстрых алгоритмов списочного декодирования для них. Векторы идентифицирующих кодов используются в алгоритме раздачи ключей легальным пользователям, а списочный декодер может использоваться в алгоритме определения злоумышленников из коалиции в случае, если это возможно [1–3; 6, разд. 1]. Так, использование c-TA-кодов гарантирует успешность определения злоумышленника из коалиции мощности максимум $c \in \mathbb{N}$ [7, п. 1.3]. Использование списочных декодеров позволяет делать это достаточно быстро [3, п. III]. Использование c-FP-кодов не гарантирует успешность нахождения злоумышленников, но c-FP-коды, наряду с c-TA-кодами, гарантируют невозможность компрометации наборов ключей законопослушных пользователей со стороны коалиций мощности максимум $c \in \mathbb{N}$ [7, п. 1.3], что также может являться важным преимуществом схемы.

Таким образом, для построения корректной и быстрой схемы широковещательного шифрования достаточно найти и рассмотреть классы линейных кодов, такие, чтобы, во-первых, они обладали идентифицирующими свойствами, и, во-вторых, для них существовали полиномиальные списочные декодеры. В [7, 8] рассмотрены коды Рида — Соломона и списочный декодер Судана — Гурусвами [9]; в [10] вместе с кодами Рида — Соломона исследуются циклические коды; в [11] исследуются коды Рида — Маллера, для которых также разработаны методы списочного декодирования, например [12]; в [6, 13] рассматриваются алгеброгеометрические коды, для списочного декодирова-

ния которых применим списочный декодер из [9]. В [14] построены коды, обладающие идентифицирующим c-IPP-свойством, для которых существует алгоритм определения злоумышленника из коалиции мощности c, основанный на списочном декодере из [9].

Говоря об иных исследованиях идентифицирующих свойств линейных кодов и их приложениях в широковещательном шифровании, отметим следующие работы. В [15] вместе с постановкой задачи, представленной выше, приведён краткий обзор применений широковещательного шифрования в конкретных телекоммуникационных сетях и распределённых хранилищах. Описание и анализ эффективности схем широковещательного шифрования, основанных на применении идентифицирующих кодов, даны в [16]. В [3, п. IV, Question 11, 12] поставлены вопросы об эквивалентности идентифицирующих c-TA- и c-IPP-свойств, обсуждение которых ведётся в [17, 18]. Отметим, что зачастую в литературе рассматривается задача, отличная от предложенной авторами: сначала фиксируется мощность коалиции злоумышленников, а оценки для длины, размерности или мощности кода получают через значение мощности коалиции, не рассматривая возможности списочного декодирования [19 – 22]. Наконец, схемы широковещательного шифрования могут рассматриваться и без явного использования линейных кодов [23].

В настоящей работе уточняются условия наличия идентифицирующих свойств c-FP и c-TA для алгеброгеометрических кодов на кривых специального вида; в частности, для алгеброгеометрических кодов на кривых, на которых найдётся достаточно много классов эквивалентности после факторизации множества точек кривой по отношению равенства соответствующих координат. Заметим, что доказательство теоремы о границах основано на ключевой конструктивной технической лемме, которая фактически анализирует действия злоумышленников.

Структура статьи организована следующим образом: в п. 1 приводятся необходимые сведения об идентифицирующих кодах, а в п. 2 — об алгеброгеометрических кодах. В п. 3 формулируются основные результаты о границах и приводятся иллюстративные примеры, а в п. 4 доказываются основные результаты.

1. Идентифицирующие коды

Пусть $q = p^r$, где p — простое число; $r \in \mathbb{N}$. Рассмотрим линейное подпространство C размерности k в линейном пространстве $\mathbb{F}_q^n$, которое будем называть линейным кодом, k — размерностью кода, n — длиной кода.

Рассмотрим отображение $\rho : \mathbb{F}_q^n \times \mathbb{F}_q^n \to \mathbb{N} \cup \{0\}$, определяемое следующим образом:

$$\rho(x, y) = |\{i \in \mathbb{N} : 1 \leqslant i \leqslant n,\ x_i \neq y_i\}|.$$

Через d обозначим величину

$$d = \min\{\rho(x, y) : x, y \in C,\ x \neq y\};$$

будем называть её минимальным кодовым расстоянием кода C. Код C над полем $\mathbb{F}_q$ длины n, размерности k и с минимальным кодовым расстоянием d будем называть $[n, k, d]_q$-кодом, или просто $[n, k, d]$-кодом.

Пусть C — линейный $[n, k, d]_q$ код, $x, y \in C$,

$$I(x, y) = \{i \in \mathbb{N} : i \in \{1, \ldots, n\},\ x_i = y_i\};$$

ясно, что $|I(x, y)| = n - \rho(x, y)$.

Пусть $c \in \mathbb{N} \setminus \{1\}$. *Коалицией* кода C называется множество

$$C_0 = \{(u_1, u_2, \ldots, u_c) : u_i \in C,\ u_i = (u_{i,1}, u_{i,2}, \ldots, u_{i,n})\}.$$

Число c называется мощностью коалиции, а множество коалиций мощности не более c обозначается как $\mathrm{coal}_c(C)$. Множеством потомков коалиции C_0 называется множество

$$\mathrm{desc}(C_0) = \{(y_1, y_2, \ldots, y_n) \in \mathbb{F}_q^n : \exists i \in \{1, \ldots, c\}\, \exists j \in \{1, \ldots, n\}\, (y_j = u_{i,j})\}.$$

Линейный код C будем называть c-FP-кодом [5, определение 1.1.1], если выполняется следующее условие:

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

Множеством FP-компрометации для кода C [11, с. 101] называется множество

$$\Omega_{\mathrm{FP}}(C) = \{c \in \mathbb{N} \setminus \{1\} : \exists C_0 \in \mathrm{coal}_c(C)\ \exists z \in C \setminus C_0\ \big(z \in \mathrm{desc}(C_0) \setminus C_0)\}.$$

Линейный код C называется c-TA-кодом [5, определение 1.1.4], если

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

Множеством TA-компрометации для кода C [11, с. 101] называется множество

$$\Omega_{\mathrm{TA}}(C) = \{c \in \mathbb{N} \setminus \{1\} : \exists v \in C\ \exists C_0 \in \mathrm{coal}_c(C \setminus \{v\})\ \exists \omega \in \mathrm{desc}(C_0) \setminus C_0\ \forall u \in C_0\ \big(\rho(v, \omega) \leqslant \rho(u, \omega)\big)\}.$$

Множества $\Omega_{\mathrm{TA}}(C)$ и $\Omega_{\mathrm{FP}}(C)$ есть целочисленные лучи:

$$\Omega_{\mathrm{TA}}(C) = \{R_{\mathrm{TA}}(C), R_{\mathrm{TA}}(C) + 1, \ldots\}, \quad \Omega_{\mathrm{FP}}(C) = \{R_{\mathrm{FP}}(C), R_{\mathrm{FP}}(C) + 1, \ldots\}.$$

Величины $R_{\mathrm{TA}}(C)$ и $R_{\mathrm{FP}}(C)$ называются рубежами множеств компрометации. Из определений вытекает, что

$$\Omega_{\mathrm{FP}}(C) \subseteq \Omega_{\mathrm{TA}}(C), \quad R_{\mathrm{TA}}(C) \leqslant R_{\mathrm{FP}}(C).$$

2. Алгеброгеометрические коды

Рассмотрим конечное поле $\mathbb{F}_q$. Пусть $\mathbb{F}_q[x_1, x_2]$ и $\mathbb{F}_q[X_1, X_2, X_3]$ — кольца многочленов от двух и трёх переменных над $\mathbb{F}_q$ соответственно; $\mathbb{F}_q^{\mathrm{hom}}[X_1, X_2, X_3]$ — множество однородных многочленов из $\mathbb{F}_q[X_1, X_2, X_3]$.

Отметим, что между многочленами f из $\mathbb{F}_q[x_1, x_2]$ и однородными многочленами F из $\mathbb{F}_q^{\mathrm{hom}}[X_1, X_2, X_3]$ существует взаимно-однозначное соответствие [24, с. 106–107], определяемое по следующему правилу: если d — максимальная степень одночлена в многочлене $f \in \mathbb{F}_q[x_1, x_2]$, то F получается из f заменой каждого одночлена вида $x_1^i x_2^j$ на одночлен вида $X_1^i X_2^j X_3^{d-i-j}$. Это соответствие называется проективизацией.

Далее будем рассматривать аффинное $\mathbb{A}^3$ и проективное $\mathbb{P}^2$ пространства, а также естественное вложение аффинного пространства в проективное [24, с. 106]. В частности, если точка P имеет аффинные координаты (a_1, a_2), то проективные координаты соответствующей точки из $\mathbb{P}^2$ будем записывать $(a_1 : a_2 : 1)$; в случае так называемых точек на бесконечности третья проективная координата равна нулю [25, с. 7–8].

Пусть $F \in \mathbb{F}_q^{\hom}[X_1, X_2, X_3]$ — неприводимый однородный многочлен, а $\mathcal{X} = \mathcal{X}(F, \mathbb{F}_q)$ — плоская гладкая проективная кривая над $\mathbb{F}_q$, заданная корнями $F \in \mathbb{F}_q^{\hom}[X_1, X_2, X_3]$ [24, п. 2.1.2]. Каждая такая кривая имеет неотрицательный целочисленный параметр g, который называется родом. В случае плоской гладкой кривой он может быть легко вычислен [24, следствие 2.2.8].

Рассмотрим поле рациональных функций над $\mathcal{X}$; обозначим его $\mathbb{F}_q(\mathcal{X})$. Это поле содержит рациональные функции, где числитель и знаменатель — однородные многочлены из $\mathbb{F}_q^{\hom}[X_1, X_2, X_3]$ одной степени. Две такие функции определяют один и тот же элемент поля $\mathbb{F}_q(\mathcal{X})$, если они аддитивно отличаются на рациональную функцию, делящуюся на F [24, п. 2.5.4].

Согласно [24, п. 2.5.2], для любой функции $H \in \mathbb{F}_q(\mathcal{X})$ и любой точки $M \in \mathcal{X}$ можно задать целочисленный параметр, называемый порядком и обозначаемый $\mathrm{ord}_M(H)$.

Дивизором D на кривой $\mathcal{X}$ называют формальную взвешенную сумму точек:

$$D = \sum_{M \in \mathcal{X}} a_M M, \quad a_M \in \mathbb{Z}.$$

Множество $\mathrm{supp}(D) = \{M \in \mathcal{X} : a_M \neq 0\}$ называется носителем D; $\deg(D) = \sum a_M$ — степенью D. Иногда, если $\deg(D) = \alpha$, вместо D будем писать D_α. Говорят, что D эффективен, если все $a_M \geqslant 0$. Если D эффективен, то пишут $D \geqslant 0$.

Для $H \in \mathbb{F}_q(\mathcal{X})$ определим дивизор функции (H) следующим образом:

$$(H) = \sum_{M \in \mathcal{X}} \mathrm{ord}_M(H) M.$$

Для любой точки $M \in \mathcal{X}$ рассмотрим произвольный линейный однородный многочлен $L \in \mathbb{F}_q^{\hom}[X_1, X_2, X_3]$, такой, что $L(M) \neq 0$, и многочлен $G \in \mathbb{F}_q^{\hom}[X_1, X_2, X_3]$, у которого $\deg(G) = r$. Пусть $\mathcal{I}(M; \mathcal{X}; G) = \mathrm{ord}_M(G/L^r)$ [25, определение 2.22]. Дивизором пересечения G и $\mathcal{X}$ называется дивизор вида

$$\mathcal{X} \cdot G = \sum_{M \in \mathcal{X}} \mathcal{I}(M; \mathcal{X}; G) M.$$

Пусть D — дивизор на плоской гладкой проективной кривой $\mathcal{X}(F, \mathbb{F}_q)$. Тогда множество

$$L(D) = \{H \in \mathbb{F}_q(\mathcal{X}) : (H) + D \geqslant 0\}$$

называется пространством Римана — Роха, ассоциированным с D. Известно, что $L(D)$ является конечномерным векторным пространством [25, теорема 2.37].

Пусть $P = \{P_1, \ldots, P_n\} \subset \mathcal{X}$, $\deg(D) = \alpha$ и $\mathrm{supp}(D) \cap P = \varnothing$. Определим алгебро-геометрический код L-конструкции как образ отображения

$$Ev_P : L(D) \to \mathbb{F}_q^n, \quad Ev_P(H) = (H(P_1), H(P_2), \ldots, H(P_n)),$$

и обозначим его как $C(\mathcal{X}, P, D)$. Дивизор $D = D_\alpha$ называется дивизором кода C.

Утверждение 1 [24, теорема 4.1.1]. Пусть $\mathcal{X}(F, \mathbb{F}_q)$ — плоская гладкая проективная кривая рода g, $0 < \alpha < n$. Тогда $C(\mathcal{X}, P, D_\alpha)$ является $[n, k, d]_q$-кодом, где

$$k \geqslant \alpha - g + 1, \; d \geqslant n - \alpha.$$

Если $\alpha > 2g - 2$, то $k = \alpha - g + 1$.

Отметим, что если $g = 0$, $\deg(F) = 1$, P — множество всех конечных точек кривой, то $C(\mathcal{X}, P, D_\alpha)$ является $[q, \alpha + 1, q - \alpha]_q$-кодом Рида — Соломона [24, с. 60, с. 263–264].

3. Формулировка основных результатов об улучшении границ для кодов на алгебраических кривых со специальными свойствами

3.1. Алгебраические кривые со специальными свойствами

Пусть $\mathcal{X} = \mathcal{X}(F, \mathbb{F}_q)$ — плоская гладкая проективная кривая; $P = \{P_1, \dots, P_n\}$ — множество всех точек вида $P_i = (P_{i,1} : P_{i,2} : 1)$ на кривой. Назовём это множество множеством конечных точек кривой.

Введём на нём два отношения эквивалентности:

$$P_i \sim_1 P_j \Leftrightarrow P_{i,1} = P_{j,1}, \quad P_i \sim_2 P_j \Leftrightarrow P_{i,2} = P_{j,2}.$$

Отношение $\sim_1$ разбивает P на классы эквивалентности

$$P/_{\sim_1} = \{R^1, \dots, R^{k_1}\}, \quad R^i = \{R^i_j = (R^i_{j,1} : R^i_{j,2} : 1) \in P,\ j = 1, \dots, l_i\}, \tag{1}$$

отношение $\sim_2$ разбивает P на классы эквивалентности

$$P/_{\sim_2} = \{S^1, \dots, S^{k_2}\}, \quad S^i = \{S^i_j = (S^i_{j,1} : S^i_{j,2} : 1) \in P,\ i = 1, \dots, m_i\}, \tag{2}$$

где l_i, m_i — мощности смежных классов R^i и S^i соответственно.

Значение k_1 назовём индексом множества P по первой координате; k_2 — индексом множества P по второй координате. Очевидно, что $k_1 \leqslant n$, $k_2 \leqslant n$. Легко проверить, что если оба индекса равны 1, то множество P состоит из одной точки. Таким образом, если $|P| > 1$, то один из индексов k_1, k_2 также больше 1.

Рассмотрим некоторые примеры.

Пример 1. Рассмотрим в качестве $\mathcal{X}$ проективную прямую, имеющую род 0 и заданную многочленом $F = X_2 - X_3$ над произвольным полем $\mathbb{F}_q$. Множество P (см. (1), (2)) для такой кривой состоит из точек вида $(\alpha_j : 1 : 1)$, $\alpha_j \in \mathbb{F}_q$. Таким образом, на этой кривой есть q классов R^i мощности $\deg(F) = 1$.

Пример 2. Рассмотрим в качестве $\mathcal{X}$ проективную прямую, имеющую род 1 и заданную многочленом

$$F(X_1, X_2, X_3) = X_2^2 X_3 + X_1 X_2 X_3 + X_2 X_3^2 - X_1^3 - X_3^3$$

над полем $\mathbb{F}_8 = \mathbb{F}_2[\xi]/(\xi^3 + \xi + 1)$. Выпишем все точки кривой:

$$Q = (0 : 1 : 0),\ P_1 = (1 : 0 : 1),\ P_2 = (\xi : \xi : 1),\ P_3 = (\xi^2 : \xi^2 : 1),$$
$$P_4 = (\xi^3 : \xi^4 : 1),\ P_5 = (\xi^4 : \xi^4 : 1),\ P_6 = (\xi^5 : \xi : 1),\ P_7 = (\xi^6 : \xi : 1),\ P_8 = (\xi^4 : 1 : 1),$$
$$P_9 = (\xi^5 : \xi^2 : 1),\ P_{10} = (\xi^6 : \xi^4 : 1),\ P_{11} = (\xi^2 : 1 : 1),\ P_{12} = (\xi^3 : \xi^2 : 1),\ P_{13} = (\xi : 1 : 1).$$

Построим классы S^i:

$$S^0 = \{(1 : 0 : 1)\},$$
$$S^1 = \{(\xi^4 : 1 : 1), (\xi^2 : 1 : 1), (\xi : 1 : 1)\},$$
$$S^2 = \{(\xi : \xi : 1), (\xi^5 : \xi : 1), (\xi^6 : \xi : 1)\},$$
$$S^3 = \{(\xi^2 : \xi^2 : 1), (\xi^5 : \xi^2 : 1), (\xi^3 : \xi^2 : 1)\},$$
$$S^4 = \{(\xi^3 : \xi^4 : 1), (\xi^4 : \xi^4 : 1), (\xi^6 : \xi^4 : 1)\}.$$

Пример 3. Рассмотрим кривую, имеющую род 6 и заданную многочленом

$$X^5 + Y^4 Z + Y Z^4 = 0$$

над полем $\mathbb{F}_{16}$. Можно проверить, что это максимальная кривая, содержащая 65 точек и 12 классов S^i мощности $\deg(F) = 5$.

3.2. Улучшение границ

Теорема 1. Пусть $\mathcal{X}(F, \mathbb{F}_q)$ — плоская гладкая проективная кривая, Q — её единственная точка на бесконечности. Рассмотрим код $C = C(\mathcal{X}(F, \mathbb{F}_q), P, D_\alpha)$, где $D = \alpha Q$. Пусть $|P| = n > 1$, $\varkappa$ — меньший из индексов k_1, k_2, $\varkappa > 1$, $\delta = \lfloor \alpha / \deg(F) \rfloor$. Предположим, что на кривой $\mathcal{X}$ существует $\delta \cdot \max\{2, \lfloor \varkappa/\delta \rfloor\}$ классов эквивалентности мощности $\deg(F)$, соответствующих индексу $\varkappa$ (если $\varkappa = k_1$, то классов R^i, иначе — S^i). Тогда

$$\begin{aligned}\sqrt{n/\alpha} \leqslant R_{\mathrm{TA}}(C) \leqslant \tilde{B}_{\mathrm{TA}}(C) = \min\left\{\left\lceil \frac{n+\alpha}{2\delta \deg(F)} \right\rceil, \left\lceil \frac{\varkappa}{\delta} \right\rceil\right\} \leqslant \left\lceil \frac{n}{\alpha} \right\rceil \leqslant R_{\mathrm{FP}}(C) \leqslant \\ \leqslant \tilde{B}_{\mathrm{FP}}(C) = \min\left\{\left\lceil \frac{n}{\lfloor \alpha/\deg(F) \rfloor \deg(F)} \right\rceil, \left\lceil \frac{\varkappa}{\delta} \right\rceil\right\}.\end{aligned} \tag{3}$$

Замечание 1. Ранее в [13, теоремы 3 и 4] получены оценки для рубежей R_{TA} и R_{FP} для более широкого класса кривых. Для кривых с рассматриваемыми специальными свойствами эти оценки усилены, при этом новая верхняя оценка для R_{TA} не превосходит новой нижней оценки для R_{FP}.

Замечание 2. Рассмотрим код $C = (\mathcal{X}(F, \mathbb{F}_q), P, D_\alpha)$. Если род g кривой $\mathcal{X}$ равен нулю, $\deg(F) = 1$ и $D = \alpha Q$, где Q — единственная точка на бесконечности, то код C является кодом Рида — Соломона, а его размерность k в силу утверждения 1 равна $\alpha + 1$. В таком случае неравенства (3) имеют вид

$$\sqrt{\frac{n}{k-1}} \leqslant R_{\mathrm{TA}} \leqslant \tilde{B}_{\mathrm{TA}}(C) = \left\lceil \frac{n+k-1}{2(k-1)} \right\rceil \leqslant R_{\mathrm{FP}} = \tilde{B}_{\mathrm{FP}}(C) = \left\lceil \frac{n}{k-1} \right\rceil$$

и совпадают по существу с оценками, полученными для кодов Рида — Соломона в [7].

3.3. Примеры вычисления параметров кодов

Пример 4. На каждой из рассмотренных в примерах 1–3 кривых находится одна и только одна точка на бесконечности. На первой кривой имеется q классов эквивалентности мощности, равной степени задающего её многочлена, на второй — 4 таких класса, а на третьей — 12. Поэтому эти кривые удовлетворяют условиям теоремы 1 при $\delta \leqslant \lfloor q/2 \rfloor$, $\delta \leqslant 2$ и $\delta \leqslant 6$ соответственно.

Пример 5. Рассмотрим кривую из примера 1 над полем $\mathbb{F}_{16}$ и дивизор $D = 2 \cdot (0 : 1 : 0)$ на ней. Выше отмечено, что эта кривая удовлетворяет условиям теоремы 1 при $\delta \leqslant 8$. В качестве множества P возьмём всё множество конечных точек кривой. Согласно утверждению 1, на рассмотренной кривой можно построить алгеброгеометрический $[16, 3, d]_{16}$-код L-конструкции C, где $d \geqslant 14$; в силу неравенства Синглтона $d = 14$. Известно, что этот код является кодом Рида — Соломона. В этом случае $\varkappa = n = 16$, $\alpha = 2$, $\delta = \lfloor 2/1 \rfloor = 2$. Для кода C выполняются все условия теоремы 1, следовательно

$$3 \leqslant R_{\mathrm{TA}}(C) \leqslant 5 \leqslant R_{\mathrm{FP}}(C) = 8$$

(см. также замечание 2).

Пример 6. Рассмотрим кривую над полем $\mathbb{F}_8$ из примера 2 и дивизор $D = 3Q$ на ней. В примере 4 отмечено, что эта кривая удовлетворяет условиям теоремы 1 при $\delta \leqslant 2$. В качестве множества P возьмём всё множество конечных точек кривой. Согласно утверждению 1, на этой кривой можно построить алгеброгеометрический $[13, 3, d]_8$-код L-конструкции C, где $d \geqslant 10$. В этом случае $n = 13$, $\varkappa = 5$, $\alpha = 3$, $\delta = \lfloor 3/3 \rfloor = 1$. Для кода C выполняются все условия теоремы 1, следовательно

$$R_{\mathrm{TA}}(C) = 3, \quad R_{\mathrm{FP}}(C) = 5.$$

Пример 7. Рассмотрим кривую над полем $\mathbb{F}_{16}$ из примера 3 и дивизор $D = 9 \cdot (0 : 1 : 0)$ на ней. В примере 4 показано, что эта кривая удовлетворяет условиям теоремы 1 при $\delta \leqslant 6$. В качестве множества P возьмём всё множество конечных точек кривой, общее количество которых, как показано в примере 3, равно 64. Тогда, согласно утверждению 1, на этой кривой можно построить алгеброгеометрический $[64, k, d]_{16}$-код L-конструкции C, где $k \geqslant 4$, $d \geqslant 55$ и, как следует из неравенства Синглтона, $k + d \leqslant 65$. В этом случае $n = 64$, $\varkappa = 12$, $\alpha = 9$, $\delta = \lfloor 9/5 \rfloor = 1$. Таким образом, для кода C выполняются все условия теоремы 1, значит,

$$3 \leqslant R_{\mathrm{TA}}(C) \leqslant 8 \leqslant R_{\mathrm{FP}}(C) \leqslant 12.$$

3.4. Применимость к схемам широковещательного шифрования

В работе рассмотрены идентифицирующие свойства алгеброгеометрических кодов в следующей постановке. Пусть выбран алгеброгеометрический код, для которого выполнены условия теоремы 1, и зафиксированы его основные параметры. Возникает вопрос, какое значение может принимать c, чтобы код сохранял c-FP- или c-TA-свойства? Ответ на этот вопрос дан в теореме 1. Таким образом, можно выбрать алгеброгеометрический код C со специальными свойствами (теорема 1), списочный декодер Судана — Гурусвами [9] и, проверив условия применимости этого списочного декодера к C [3, теорема 5; 6, следствие 1], построить:

1) устойчивую схему широковещательного шифрования, способную гарантировать невозможность прямой компрометации ключей законопослушных пользователей со стороны коалиций мощности вплоть до $c_1 = \lceil n/\alpha \rceil - 1 < \lceil n/\alpha \rceil \leqslant R_{\mathrm{FP}}(C)$;
2) отслеживающую схему широковещательного шифрования, способную находить участников коалиций мощности вплоть до $c_2 = \lceil \sqrt{n/\alpha} - 1 \rceil < \sqrt{n/\alpha} \leqslant R_{\mathrm{TA}}(C)$;
3) устойчивую и отслеживающую схему широковещательного шифрования, способную гарантировать как невозможность прямой компрометации ключей законопослушных пользователей со стороны коалиций мощности вплоть до $c_1 = \lceil n/\alpha \rceil - 1 < \lceil n/\alpha \rceil \leqslant R_{\mathrm{FP}}(C)$, так и находить при этом злоумышленников из коалиций мощности вплоть до $c_2 = \lceil \sqrt{n/\alpha} - 1 \rceil < \sqrt{n/\alpha} \leqslant R_{\mathrm{TA}}(C)$.

Возможность построения схем с такими свойствами обоснована в [7, п. 1.3]. Максимальное число пользователей такой схемы ограничено сверху мощностью кода [6, утверждение 2]. Сформулируем и докажем следующее утверждение:

Теорема 2. Пусть выполняются условия теоремы 1, $c \in \mathbb{N} \setminus \{1\}$. Тогда

1) если $c < \sqrt{n/\alpha}$, то
$$\max_{\alpha} |C| = q^{\lceil n/c^2 - 1 \rceil - g + 1};$$
2) если $c < \lceil n/\alpha \rceil$, то
$$\max_{\alpha} |C| = q^{\lceil n/(c-\varepsilon) - 1 \rceil - g + 1},$$
где $\varepsilon = \lceil n/\alpha \rceil - n/\alpha$.

Доказательство. Если C — линейный $[n, k, d]_q$-код, то $|C| = q^k$.

1) Если $c < \sqrt{n/\alpha}$, то $\alpha < n/c^2$, тогда
$$\max_{\alpha} \{\alpha : \alpha < n/c^2\} = \lceil n/c^2 - 1 \rceil.$$

Из утверждения 1 получим, что $\max\limits_{\alpha} k = \lceil n/c^2 - 1 \rceil - g + 1$. Следовательно, $\max\limits_{\alpha} |C| = q^{\lceil n/c^2 - 1 \rceil - g + 1}$.

2) Аналогично, так как $c < \lceil n/\alpha \rceil = n/\alpha + \varepsilon$, то $\alpha < n/(c-\varepsilon)$. Тогда

$$\max_{\alpha}\{\alpha : \alpha < n/(c-\varepsilon)\} = \lceil n/(c-\varepsilon) - 1 \rceil,$$

значит, $\max\limits_{\alpha} k = \lceil n/(c-\varepsilon) - 1 \rceil - g + 1$ и $\max\limits_{\alpha} |C| = q^{\lceil n/(c-\varepsilon) - 1 \rceil - g + 1}$. ■

Справедливость утверждения означает, что максимальное число пользователей устойчивой схемы равно $q^{\lceil n/(c_1-\varepsilon)-1 \rceil - g + 1}$, так как $c_1 < \lceil n/\alpha \rceil$, а для отслеживающей $q^{\lceil n/c_2^2 - 1 \rceil - g + 1}$, так как $c_2 < \sqrt{n/\alpha}$. Для усточивой и одновременно отслеживающей схемы число пользователей равно $\min\{q^{\lceil n/c_1^2 - 1 \rceil - g + 1}, q^{\lceil n/(c_2-\varepsilon) - 1 \rceil - g + 1}\}$, так как в такой схеме $c_1 < \lceil n/\alpha \rceil$ и $c_2 < \sqrt{n/\alpha}$ одновременно.

Пример 8. Используя код из примера 5, можно построить устойчивую схему для $c_1 = 4$, отслеживающую схему для $c_2 = 2$ или устойчивую и отслеживающую для $c_1 = 4$, $c_2 = 2$. Для устойчивой схемы максимальное число пользователей равно $16^{\lceil 16/(4-0) - 1 \rceil + 1} = 16^4 = 2^{16}$, так как $\varepsilon = \lceil 16/4 \rceil - 16/4 = 0$; для отслеживающей схемы максимальное число пользователей также равно $16^{\lceil 16/4 - 1 \rceil + 1} = 16^4 = 2^{16}$; для устойчивой и отслеживающей схемы максимальное число пользователей равно $\min\{2^{16}, 2^{16}\} = 2^{16}$.

Пример 9. Используя код из примера 6, можно построить устойчивую схему для $c_1 = 4$, отслеживающую схему для $c_2 = 2$, устойчивую и одновременно отслеживающую схему для $c_1 = 4$, $c_2 = 2$. Для устойчивой схемы максимальное число пользователей равно $8^{\lceil 13/(4-2/3) - 1 \rceil - 1 + 1} = 8^3 = 2^9$, так как $\varepsilon = \lceil 13/3 \rceil - 13/3 = 2/3$; для отслеживающей схемы также равно $8^{\lceil 13/4 - 1 \rceil - 1 + 1} = 8^3 = 2^9$; для усточивой и отслеживающей схемы равно $\min\{2^9, 2^9\} = 2^9$.

Пример 10. Используя код из примера 7, можно построить устойчивую схему для $c_1 = 7$, отслеживающую схему для $c_2 = 2$, устойчивую и одновременно отслеживающую для $c_1 = 7$, $c_2 = 2$. Максимальное число пользователей для устойчивой схемы равно $16^{\lceil 64/(7-8/9) - 1 \rceil - 6 + 1} = 16^5 = 2^{20}$, так как $\varepsilon = 8 - 7\frac{1}{9} = \frac{8}{9}$; для отслеживающей схемы максимальное число пользователей равно $16^{\lceil 64/4 - 1 \rceil - 6 + 1} = 16^{10} = 2^{40}$; для устойчивой и отслеживающей — $\min\{2^{40}, 2^{20}\} = 2^{20}$.

Рассмотрим иную постановку задачи. Предположим, что известна максимально возможная мощность коалиции злоумышленников c. Возникает вопрос, какой код (в частности, какой алгеброгеометрический код) выбрать, чтобы построить схему широковещательного шифрования при заданном c? Возможно ли использование списочного декодирования в этом случае? Эти задачи выходят за рамки данной работы и представляются темой отдельного исследования. При их решении может возникать необходимость перебора кодов; формализация такого перебора для одноточечных алгеброгеометрических кодов общего вида рассмотрена в [6, алгоритм 1].

4. Доказательство основного результата

4.1. Вспомогательные леммы

Следующая конструктивная техническая лемма является ключевой для доказательства теоремы 1. В её доказательстве, фактически имитирующем действия злоумышленников, явно показан способ построения коалиции и её потомка, на которых достигаются представленные в утверждении леммы оценки и равенства.

Лемма 1. Пусть $\mathcal{X}(F, \mathbb{F}_q)$ — плоская гладкая проективная кривая, Q — её единственная точка на бесконечности. Рассмотрим код $C = (\mathcal{X}(F, \mathbb{F}_q), P, D_\alpha)$, где $D = \alpha Q$. Пусть $|P| > 1$, $\varkappa$ — меньший из индексов k_1, k_2, $\varkappa > 1$, $\delta = \lfloor \alpha / \deg(F) \rfloor$. Предположим, что на кривой $\mathcal{X}$ существует $\delta \cdot \max\{2, \lfloor \varkappa/\delta \rfloor\}$ классов эквивалентности мощности $\deg(F)$, соответствующих индексу $\varkappa$ (если $\varkappa = k_1$, то классов R^i, иначе — S^i). Тогда

— для всех c, таких, что $2 \leqslant c \leqslant \varkappa/\delta$

$$\forall v \in C \; \exists C_0 \in \mathrm{coal}_c(C \setminus \{v\}) \; \exists \omega \in \mathrm{desc}(C_0) \setminus C_0 \; \big(|I(\omega, v)| \geqslant \min\{c\delta \deg(F), n\}\big), \quad (4)$$

— для всех c, таких, что $c > \varkappa/\delta$

$$\forall v \in C \; \exists C_0 \in \mathrm{coal}_c(C \setminus \{v\}) \; \exists \omega \in \mathrm{desc}(C_0) \setminus C_0 \; \big(|I(\omega, v)| = n\big). \quad (5)$$

Доказательство. Предположим, что лемма доказана для $v = 0$, т. е. можно построить коалицию $\hat{C}_0 = \{\hat{u}_1, \ldots, \hat{u}_c\}$, такую, что при $v = 0$ выполняются (4) и (5). Рассмотрим произвольный вектор $v \in C$, коалицию $C_0 = \{\hat{u}_1 + v, \ldots, \hat{u}_c + v\}$ и вектор $\omega = \hat{\omega} + v$. Так как C — линейный код, $C_0 \in \mathrm{coal}_c(C \setminus \{v\})$, $\omega \in \mathrm{desc}(C_0) \setminus C_0$, и (4), (5) выполняются для произвольного v. Таким образом, если лемма справедлива для $v = 0$, то она справедлива и для любых других $v \in C$.

Докажем теперь лемму в предположении, что $v = 0$.

Рассмотрим сначала случай, когда $c\delta < n$, и разобьём доказательство на несколько шагов.

I. Рассмотрим множество $P \subset \mathcal{X}$. Так как по построению АГ-кода $\mathrm{supp}(D) \cap P = \varnothing$, $\mathrm{supp}(D) = \{Q\}$ и Q — единственная бесконечная точка на кривой $\mathcal{X}$, то в P нет бесконечных точек, т. е. точек вида $(X_1 : X_2 : 0)$. Значит, множество P является подмножеством множества конечных точек кривой, причём, так как $|P| > 1$, один из индексов P больше единицы (см. (1), (2)). Не нарушая общности, будем считать, что $\varkappa = k_2 > 1$, и рассмотрим классы эквивалентности S^i. Перенумеруем множество P так, чтобы для первых $\varkappa$ точек из P выполнялось условие $P_i \in S^i$, $i \in \{1, \ldots, \varkappa\}$.

II. Так как коалиция является набором кодовых векторов, каждый из которых является образом некоторой рациональной функции из пространства Римана — Роха $L(D)$ при кодирующем отображении, для построения искомой коалиции необходимо сначала предъявить соответствующий набор рациональных функций.

Для искомых функций построим вспомогательные многочлены. Рассмотрим несколько случаев:

а) Пусть $c\delta \leqslant \varkappa$. Предположим, что F является проективизацией некоторого многочлена $f \in \mathbb{F}_q[x_1, x_2]$. По условию существует $\max\{2\delta, \lfloor \varkappa/\delta \rfloor \delta\}$ классов S^i, мощность которых равна $\deg(F)$. Так как $2 \leqslant c \leqslant \varkappa/\delta$, это означает, что существует как минимум $c\delta$ классов S^i, каждый из которых имеет мощность $\deg(F)$. Следовательно, существуют $\beta_1, \ldots, \beta_{c\delta}$, $\beta_i \in \mathbb{F}_q$ (β_i соответствует классу S^i), такие, что $f(x_1, \beta_i)$ имеет $\deg(F)$ различных корней. Обозначим корни $f(x_1, \beta_i)$ как α_{lj}, $l = 1, \ldots, \deg(F)$, $j = 1, \ldots, c\delta$. Каждому такому корню соответствует точка $(\alpha_{li} : \beta_i : 1) \in S^i$.

Тогда многочлены r_i будем строить следующим образом:

$$r_i(x_1, x_2) = (x_2 - \beta_{(i-1)\delta+1}) \ldots (x_2 - \beta_{i\delta}), \; i = 1, \ldots, c. \quad (6)$$

Каждый одночлен в $r_i(x_1, x_2)$ имеет $\deg(F)$ корней вида

$$(\alpha_{lj}, \beta_j), \; l = 1, \ldots, \deg(F), \; j \in \{(i-1)\delta + 1, \ldots, i\delta\},$$

значит, у $r_i(x_1, x_2)$ всего $\delta \deg(F)$ корней вида

$$(\alpha_{lj}, \beta_j),\ l = 1, \ldots, \deg(F),\ j = (i-1)\delta + 1, \ldots, i\delta.$$

Для каждого r_i и точки $P_l = R_1^{i\delta+1} = (P_{l,1} : P_{l,2} : 1)$ выполняется: $r_i(P_{l,1}, P_{l,2}) \neq 0$. Степень каждого r_i равна δ.

б) Пусть теперь $c\delta > \varkappa$, причём $\varkappa \leqslant \delta$ и $\varkappa < c$. Тогда в кольце $\mathbb{F}_q[x_1, x_2]$ рассмотрим следующие многочлены:

$$r_i(x_1, x_2) = (x_2 - S_{1,1}^i),\ i \in \{1, \ldots, \varkappa\}. \tag{7}$$

Для каждого r_i и точки $P_l = S_1^{i+1} = (P_{l,1} : P_{l,2} : 1)$ выполняется: $r_i(P_{l,1}, P_{l,2}) \neq 0$. Степень каждого r_i не превышает δ. Рассмотрим множество ненулевых многочленов степени не выше δ, не совпадающих с r_i, $i \in \{1, \ldots, \varkappa\}$. Таких многочленов $q^{\delta+1} - \varkappa - 1$ штук. Тогда в качестве r_j, $j \in \{\varkappa+1, \ldots, c\}$, возьмём многочлены из этого множества, такие, что $r_j(P_{l,1}, P_{l,2}) \neq 0$ для некоторой $P_l = (P_{l,1} : P_{l,2} : 1) \in P$.

в) Пусть теперь $c\delta > \varkappa$, причём $\varkappa \leqslant \delta$, но $\varkappa \geqslant c$. Тогда в кольце $\mathbb{F}_q[x_1, x_2]$ можно рассмотреть следующие многочлены:

$$r_i(x_1, x_2) = (x_2 - S_{1,1}^i),\ i \in \{1, \ldots, c-1\},\quad r_c(x_1, x_2) = (x_2 - S_{1,1}^c) \ldots (x_1 - S_{1,1}^{\varkappa}). \tag{8}$$

Для каждого такого r_i найдётся точка $P_l = (P_{l,1} : P_{l,2} : 1)$, для которой $r_i(P_{l,1}, P_{l,2}) \neq 0$. Для $i < c$ такой точкой, например, является S_1^{i+1}, а для $i = c$ — точка S_1^{c-1}. Так как $\varkappa - c + 1 \leqslant \delta - c + 1 \leqslant \delta$, степень каждого r_i не превышает δ.

г) Пусть $c\delta > \varkappa$ и $\varkappa > \delta$. Тогда в кольце $\mathbb{F}_q[x_1, x_2]$ можно рассмотреть следующие многочлены:

$$\begin{gathered} r_i = (x_1 - S_{1,1}^{(i-1)\delta+1}) \ldots (x_1 - S_{1,1}^{i\delta}),\quad i \in \{1, \ldots, \lceil \varkappa/\delta \rceil - 1\}, \\ r_{\lceil \varkappa/\delta \rceil} = (x_2 - S_{1,1}^{(\lceil \varkappa/\delta \rceil - 1)\delta+1}) \ldots (x_2 - S_{1,1}^{\varkappa}). \end{gathered} \tag{9}$$

Для каждого такого r_i найдётся точка $P_l = (P_{l1} : P_{l2} : 1)$, такая, что $r_i(P_{l1}, P_{l2}) \neq 0$. Для $i \leqslant \lceil \varkappa/\delta \rceil - 1$ такой точкой, например, является $S_1^{i\delta+1}$, а для $i = \lceil \varkappa/\delta \rceil$ — точка $S_1^{(\lceil \varkappa/\delta \rceil - 1)\delta}$. Так как

$$\varkappa - ((\lceil \varkappa/\delta \rceil - 1)\delta + 1) + 1 < c\delta - (\lceil c\delta/\delta \rceil - 1)\delta \leqslant c\delta - (c-1)\delta \leqslant \delta,$$

то степень каждого r_i не превышает δ. В качестве r_j, $j \in \{\lceil \varkappa/\delta \rceil + 1, \ldots, c\}$, возьмём произвольные ненулевые многочлены степени не выше δ, не совпадающие с r_i, $i \in \{1, \ldots, \lceil \varkappa/\delta \rceil\}$, такие, что для них существует точка $(P_{l,1} : P_{l,2} : 1) \in P$, такая, что $r_i(P_{l,1}, P_{l,2}) \neq 0$.

Во всех случаях *а–г* степень каждого из многочленов r_i не превышает δ, все многочлены различны и для каждого r_i найдётся такая точка $P_l = (P_{l,1} : P_{l,2} : 1) \in P$, что $r_i(P_{l,1}, P_{l,2}) \neq 0$.

Рассмотрим проективизацию многочленов $r_i(x_1, x_2)$ и получим однородные многочлены $R_i(X_1, X_2, X_3)$ степени не выше δ.

В случае II, *а* однородные многочлены $R_i(X_1, X_2, X_3)$, являющиеся проективизацией $r_i(x_1, x_2)$, обращаются в нуль на точках проективного пространства вида

$$P_{j,\beta_i} = (\alpha_{lj} : \beta_l : 1),\ j = 1, \ldots, \deg(F),\ l = (i-1)\delta + 1, \ldots, i\delta.$$

Легко проверить, что эти точки лежат на кривой $\mathcal{X}$, так как $f(\alpha_{lj}, \beta_l) = 0$, а значит, $F(\alpha_{lj}, \beta_l, 1) = 0$. Таким образом, в случае II, a $R_i(X_1, X_2, X_3)$ обращаются в нуль на $\delta \deg(F)$ точках кривой $\mathcal{X}$, причём для разных R_i наборы таких точек не пересекаются.

Построим рациональные функции:

$$H_i = \frac{R_i(X_1, X_2, X_3)}{X_3^{\deg(R_i)}}, \tag{10}$$

являющиеся элементами поля $\mathbb{F}_q(\mathcal{X})$. Покажем, что H_i принадлежит пространству Римана — Роха $L(D)$, ассоциированному с дивизором D. Действительно, согласно [6, замечание 2], дивизор построенной функции H_i имеет вид

$$(H_i) = \mathcal{X} \cdot R_i(X_1, X_2, X_3) - \mathcal{X} \cdot X_3^{\deg(R_i)}.$$

В силу замечания к теореме 2.23 [25],

$$\sum_{M \in \mathcal{X}(F, \mathbb{F}_q)} \mathcal{I}(M; \mathcal{X}(F, \mathbb{F}_q); G) \leqslant \deg(G) \deg(F),$$

поэтому

$$\mathcal{X} \cdot X_3^{\deg(R_i)} = \sum_{M \in \mathcal{X}(F, \mathbb{F}_q)} \mathcal{I}\left(M; \mathcal{X}(F, \mathbb{F}_q); X_3^{\deg(R_i)}\right) M = \mathcal{I}(Q; \mathcal{X}(F, \mathbb{F}_q); X_3^{\deg(R_i)}) Q \leqslant$$
$$\leqslant \deg\left(X_3^{\deg(R_i)}\right) \deg(F) Q = \deg(R_i) \deg(F) Q.$$

Тогда

$$(H_i) = \mathcal{X} \cdot R_i(X_1, X_2, X_3) - \mathcal{X} \cdot X_3^{\deg(R_i)} \geqslant \sum_{P_j \in P} \mathcal{I}(P_j, X, R_i) P_j - \deg(R_i) \deg(F) Q,$$
$$(H_i) + D \geqslant \sum_{P_j \in P} \mathcal{I}(P_j, \mathcal{X}, R_i) P_j - \deg(R_i) \deg(F) Q + \alpha Q =$$
$$= \sum_{P_j \in P}^{\delta i} \mathcal{I}(P_j, \mathcal{X}, \mathcal{P}) P_j + (\alpha - \deg(R_i) \deg(F)) Q.$$

Так как $\deg(R_i) \leqslant \delta = \lfloor \alpha / \deg(F) \rfloor$, то

$$(H_i) + D \geqslant \sum_{P_j \in P} \mathcal{I}(P_j, \mathcal{X}, \mathcal{P}) P_j + (\alpha - \lfloor \alpha / \deg(F) \rfloor \deg(F)) Q \geqslant 0,$$

значит, $H_i \in L(D)$.

III. Построим теперь искомую коалицию $C_0 = \{u_1; \ldots; u_c\}$ следующим образом:

$$u_i = Ev_P(H_i) = (H_i(P_1), \ldots, H_i(P_n)). \tag{11}$$

Все многочлены r_i различны, поэтому и все R_i, а также H_i тоже различны. Для каждого r_i существует точка $P_l = (P_{l,1} : P_{l,2} : 1) \in P$, такая, что $r_i(P_{l,1}, P_{l,2}) \neq 0$, следовательно, и $H_i(P_{l,1} : P_{l,2} : 1) \neq 0$. Таким образом, в коалиции ровно c различных ненулевых векторов.

IV. Теперь для каждого из рассмотренных на шаге II случаев *а–г* построим искомого потомка ω.

В случае *а* коалиция C_0 (см. (11)) в силу (6) и (10) выглядит следующим образом:

$$\begin{cases} u_1 = (0, \dots, 0, H(P_{\delta \deg(F)+1}), \dots, H(P_n)), \\ \dots \\ u_i = (H(P_1), \dots, H(P_{\delta \deg(F)(i-1)}), 0, \dots, 0, H(P_{\delta \deg(F)i+1}), \dots, H(P_n)), \\ \dots \\ u_c = (H(P_1), \dots, H(P_{\delta \deg(F)(c-1)}), 0, \dots, 0, H(P_{\delta \deg(F)c+1}), \dots, H(P_n)). \end{cases}$$

Рассмотрим потомка коалиции C_0

$$\omega = (0, \dots, 0, \omega_{\delta \deg(F)c+1}, \dots, \omega_n),$$

где для каждого $j \in \{\delta c + 1, \dots, n\}$ значение ω_j задаётся как произвольный элемент из $\{u_{1,j}, \dots, u_{c,j}\}$. Ясно, что $\omega \in \operatorname{desc}(C_0) \setminus C_0$. По построению

$$|I(\omega, 0)| \geqslant c\delta \deg(F) = c \lfloor \alpha / \deg(F) \rfloor \deg(F).$$

В случае *б* коалиция в силу (7) и (10) выглядит следующим образом:

$$\begin{cases} u_1 = (0, \dots, H(P_i), \dots, H(P_n)), \\ \dots \\ u_i = (H(P_1), \dots, H(P_{i-1}), 0, H(P_{i+1}), \dots, H(P_n)), \\ \dots \\ u_\varkappa = (H(P_1), \dots, H(P_{\varkappa-1}), 0, H(P_{\varkappa+1}), \dots, H(P_n)), \\ \dots \\ u_j = (H(P_1), \dots, H(P_{j-1}), H(P_j), H(P_{j+1}), \dots, H(P_n)), \\ \dots \\ u_c = (H(P_1), \dots, H(P_{c-1}), H(P_{c+1}), \dots, H(P_n)). \end{cases}$$

Построим потомка ω следующим образом. В качестве ω_i, где $1 \leqslant i \leqslant \varkappa$, из вектора u_i возьмём нуль, стоящий там на i-й позиции. Заметим, что для любой позиции j, такой, что $j > \varkappa$, точка P_j лежит в каком-либо классе эквивалентности S^m. Тогда $u_{m,j} = 0$, так как по построению значение H_m равно нулю на любой точке из S^m, в том числе на P_j. Значит, для любой такой позиции j мы можем выбрать $\omega_j = u_{m,j} = 0$. Таким образом, комбинированием только первых $\varkappa$ векторов можно выбрать потомка ω, совпадающего с нулевым вектором. Тогда

$$|I(\omega, 0)| = n.$$

В случае *в* коалиция в силу (8) и (10) выглядит следующим образом:

$$\begin{cases} u_1 = (0, \dots, H(P_i), \dots, H(P_n)), \\ \dots \\ u_i = (H(P_1), \dots, H(P_{i-1}), 0, H(P_{i+1}), \dots, H(P_n)), \\ \dots \\ u_c = (H(P_1), \dots, H(P_{c-1}), 0, \dots, 0, H(P_{\varkappa+1}), \dots, H(P_n)). \end{cases}$$

Построим потомка ω. В качестве ω_i, где $1 \leqslant i \leqslant c$, из вектора u_i возьмём нуль, стоящий там на i-й позиции. Если $c \leqslant i \leqslant \varkappa$, то в качестве элемента на позиции i возьмём нуль из вектора u_c, также стоящий там на i-й позиции. Аналогично предыдущему случаю, для любой позиции j, такой, что $j > \varkappa$, точка P_j лежит в одном из классов эквивалентности S^m. Тогда $u_{m,j} = 0$, так как значение H_m равно нулю на любой точке из S^m. Значит, для любой такой позиции j мы можем выбрать $\omega_j = u_{m,j} = 0$. Комбинированием всех c векторов можно выбрать потомка ω, совпадающего с нулевым вектором:

$$|I(\omega, 0)| = n.$$

В случае *г* коалиция в силу (9) и (10) выглядит следующим образом:

$$\begin{cases} u_1 = (0, \ldots, 0, H(P_{\delta+1}), \ldots, H(P_n)), \\ \ldots \\ u_i = (H(P_1), \ldots, H(P_{\delta(i-1)}), 0, \ldots, 0, H(P_{\delta i+1}), \ldots, H(P_n)), \\ \ldots \\ u_{\lceil k/\delta \rceil} = (H(P_1), \ldots, H(P_{(\lceil \varkappa/\delta \rceil - 1)\delta,1}), 0, \ldots, 0, H(P_\varkappa), \ldots, H(P_n)), \\ \ldots \\ u_c = (H(P_1), \ldots, H(P_{c-1}), H(P_{c+1}), \ldots, H(P_n)). \end{cases}$$

Построим потомка ω в этом случае. В качестве ω_i, где $1 \leqslant i \leqslant \lceil \varkappa/\delta \rceil$, из вектора u_i возьмём нуль, стоящий там на i-й позиции. Если $\lceil \varkappa/\delta \rceil \leqslant i \leqslant \varkappa$, то в качестве элемента на позиции i возьмём нуль из вектора $u_{\lceil \varkappa/\delta \rceil}$, также стоящий там на i-й позиции. Аналогично предыдущему случаю, для любой позиции j, такой, что $j > \varkappa$, существует номер m, такой, что $u_{m,j} = 0$. Значит, для любой такой позиции j мы можем выбрать $\omega_j = u_{m,j} = 0$. Тогда комбинированием первых $\lceil \varkappa/\delta \rceil$ векторов можно выбрать потомка ω, совпадающего с нулевым вектором:

$$|I(\omega, 0)| = n.$$

Итак, при $c\delta < n$, если $c\delta \leqslant \varkappa$, найдётся такой потомок ω коалиции C_0, что $|I(\omega, 0)| \geqslant c\delta \deg(F)$, а если $c\delta > \varkappa$, то найдется потомок ω, такой, что $|I(\omega, 0)| = n$.

Таким образом, лемма в случае $c\delta < n$ доказана. Теперь рассмотрим случай, когда $c\delta \geqslant n$. Для доказательства необходимо показать, что при условиях леммы можно построить коалицию, способную породить нулевого потомка.

Построим коалицию C_0 в этом случае. Пусть $\hat{c} = \lfloor n/\delta \rfloor$, тогда $\hat{c}\delta < n$. Набор многочленов r_i, $i \in \{1, \ldots, \hat{c}\}$, и первые $\hat{c}$ элементов коалиции построим так же, как для случая $c\delta < n$ на шагах II и III. Теперь нужно достроить коалицию до необходимой мощности c.

Если на шаге II для $\hat{c}$ реализовались случаи *б*, *в* или *г*, то, как показано на шаге IV, в качестве потомка построенной коалиции мощности $\hat{c}$ уже может быть выбран нулевой вектор. Поэтому в качестве остальных $c - \hat{c}$ членов коалиции можно взять любые из оставшихся ненулевых кодовых векторов.

Предположим, что на шаге II для $\hat{c}$ реализовался случай *а*. Тогда мы можем построить потомка ω с $\hat{c}\delta \deg(F)$ нулями. Если $\hat{c}\delta \deg(F) \geqslant n$, то дополнительных построений проводить не нужно, так как в качестве потомка коалиции мощности $\hat{c}$ уже может быть выбран нулевой вектор, а в качестве остальных членов коалиции можно взять любые из оставшихся ненулевых кодовых векторов. Иначе, если $\hat{c}\delta \deg(F) < n$, то существуют $\varkappa - \hat{c}\delta > 0$ классов S^j, таких, что ни один из многочленов R_i не имеет

корней ни на одной точке — представителе каждого из этих классов. Тогда построим элемент коалиции с номером $\lceil n/\delta \rceil$ следующим образом. Возьмём проективизацию $R_{\lceil n/\delta \rceil}$ многочлена $r_{\lceil n/\delta \rceil} = (x_2 - S_{1,2}^{(\lceil n/\delta \rceil - 1)\delta + 1}) \dots (x_2 - S_{1,2}^{\varkappa})$ и поделим на X_3^{δ}, получив рациональную функцию $H_{\lceil n/\delta \rceil}$. Степень $R_{\lceil n/\delta \rceil}$ не превышает δ, так как

$$\varkappa - (\lceil n/\delta \rceil - 1)\delta - 1 + 1 \leqslant n - (\lceil n/\delta \rceil - 1)\delta \leqslant n - \lceil n/\delta \rceil \delta + \delta \leqslant \delta.$$

Очевидно, что значение $H_{\lceil n/\delta \rceil}$ на всех точках из классов $S^{(\lceil n/\delta \rceil - 1)\delta + 1}, \dots, S^k$ равно нулю. Аналогично показанному на шаге II в случае $c\delta < n$ проверяется, что $H_{\lceil n/\delta \rceil} \in L(D)$. Тогда можно построить очередной член коалиции $u_{\lceil n/\delta \rceil}$, являющийся образом функции $H_{\lceil n/\delta \rceil}$. На позициях $(\lceil n/\delta \rceil - 1)\delta + 1, \dots, n$ в $u_{\lceil n/\delta \rceil}$ находятся нули. В этом случае оставшиеся $c - \lceil n/\delta \rceil$ членов коалиции выберем как произвольные кодовые ненулевые слова, не совпадающие с построенными ранее членами коалиции. В качестве потомка построенной коалиции может быть выбран нулевой вектор. Действительно, первые $\hat{c}\delta \deg(F)$ позиций могут быть заполнены нулями согласно построению из пункта II, a, а остальные $n - \hat{c}\delta \deg(F)$ позиций можно заполнить нулями, стоящими на соответствующих позициях в векторе $u_{\lceil n/\delta \rceil}$.

Таким образом, построена коалиция $C_0 \in \mathrm{coal}_c(C \setminus \{0\})$. В качестве $\omega \in \mathrm{desc}(C_0) \setminus C_0$ можно выбрать нулевой вектор. ■

Лемма 2.

$$\left\lceil \frac{n+\alpha}{2\lfloor \alpha/\deg(F) \rfloor \deg}(F) \right\rceil \leqslant \left\lceil \frac{n}{\alpha} \right\rceil.$$

Доказательство. Действительно,

$$\frac{n+\alpha}{2\,\lfloor \alpha/\deg(F) \rfloor \deg(F)} < \frac{2n}{2\,\lfloor \alpha/\deg(F) \rfloor \deg(F)} = \frac{n}{\lfloor \alpha/\deg(F) \rfloor \deg(F)},$$

так как $\alpha < n$, и, далее, так как $\lfloor \alpha/\deg(F) \rfloor \deg(F) \leqslant \alpha$, то

$$\frac{n}{\lfloor \alpha/\deg(F) \rfloor \deg(F)} \leqslant \frac{n}{\alpha},$$

значит, и

$$\left\lceil \frac{n+\alpha}{2\,\lfloor \alpha/\deg(F) \rfloor \deg(F)} \right\rceil \leqslant \left\lceil \frac{n}{\alpha} \right\rceil.$$

Лемма доказана. ■

4.2. Доказательство теоремы 1

1. Докажем сначала справедливость неравенства

$$R_{\mathrm{FP}}(C) \leqslant \tilde{B}_{\mathrm{FP}}(C) = \min\left\{ \left\lceil \frac{n}{\lfloor \alpha/\deg(F) \rfloor \deg(F)} \right\rceil, \left\lceil \frac{\varkappa}{\delta} \right\rceil \right\}. \tag{12}$$

Пусть $\hat{c}$ — произвольное целое, такое, что $\hat{c} \geqslant \tilde{B}_{FP}$. Чтобы доказать (12), достаточно показать, что при числе злоумышленников, равном как минимум $\hat{c}$, FP-свойство не выполнено.

Сначала пусть

$$\tilde{B}_{\mathrm{FP}} = \min\left\{ \left\lceil \frac{n}{\delta \deg(F)} \right\rceil, \left\lceil \frac{\varkappa}{\delta} \right\rceil \right\} = \left\lceil \frac{n}{\delta \deg(F)} \right\rceil.$$

Тогда в силу (4) из леммы 1

$$\forall v \in C\ \exists C_0 \in \mathrm{coal}_{\hat{c}}(C \setminus \{v\})\ \exists \omega \in \mathrm{desc}(C_0) \setminus C_0 \left(|I(\omega, v)| \geqslant \min\{\hat{c}\delta \deg(F), n\}\right).$$

По предположению $\hat{c} \geqslant B_{\mathrm{FP}}$, поэтому

$$|I(\omega, v)| \geqslant \min\{\hat{c}\delta \deg(F), n\} = n,$$

т. е. $|I(\omega, v)| = n$. Значит, $\omega = v \in \mathrm{desc}(C_0) \setminus C_0$. Следовательно, FP-свойство не выполняется, и $R_{\mathrm{FP}}(C) \leqslant B_{\mathrm{FP}}(C)$.

Пусть теперь

$$\tilde{B}_{\mathrm{FP}} = \min\left\{\left\lceil \frac{n}{\delta \deg(F)} \right\rceil, \left\lceil \frac{\varkappa}{\delta} \right\rceil\right\} = \left\lceil \frac{\varkappa}{\delta} \right\rceil.$$

Тогда в силу (5) из леммы 1

$$\forall v \in C\ \exists C_0 \in \mathrm{coal}_{\hat{c}}(C \setminus \{v\})\ \exists \omega \in \mathrm{desc}(C_0) \setminus C_0 \left(|I(\omega, v)| = n\right),$$

что также означает, что FP-свойство не выполняется.

Итак, неравенство (12) доказано.

2. Докажем неравенство

$$R_{\mathrm{TA}}(C) \leqslant \tilde{B}_{\mathrm{TA}}(C) = \min\left\{\left\lceil \frac{n+\alpha}{2\delta \deg(F)} \right\rceil, \left\lceil \frac{\varkappa}{\delta} \right\rceil\right\}. \tag{13}$$

Для этого достаточно показать, что если $\hat{c}$ — произвольное целое число, такое, что $\hat{c} \geqslant \tilde{B}_{\mathrm{TA}}(C)$, то C не является c-TA-кодом.

Пусть сначала

$$\tilde{B}_{\mathrm{TA}} = \min\left\{\left\lceil \frac{n+\alpha}{2\delta \deg(F)} \right\rceil, \left\lceil \frac{\varkappa}{\delta} \right\rceil\right\} = \left\lceil \frac{n+\alpha}{2\delta \deg(F)} \right\rceil.$$

Тогда, так как $\hat{c} \geqslant B_{\mathrm{TA}}(C)$, получаем

$$c\delta \deg(F) \geqslant (n+\alpha)/2. \tag{14}$$

Пусть $v \in C$ — произвольное кодовое слово. Согласно определению свойства c-TA, для того чтобы показать, что оно не выполнено при $c = \hat{c}$, достаточно доказать следующее:

$$\exists C_0 \in \mathrm{coal}_{\hat{c}}(C)\ \exists \omega \in \mathrm{desc}(C_0)\ \forall i \in \{1, \ldots, \hat{c}\} \left(|I(\omega, u_i)| \leqslant |I(\omega, v)|\right).$$

В качестве C_0 и ω рассмотрим построенные в лемме 1 для случая II, *а* коалицию C_0 и её потомка ω и докажем, что выполняются искомые условия.

Если $\hat{c}\delta \geqslant \varkappa$, то из (4) в лемме 1 легко показать, что C не является $\hat{c}$-FP, а значит, и $\hat{c}$-TA кодом, и (13) доказано.

Пусть $\hat{c}\delta \leqslant \varkappa$. Тогда в силу (4) из леммы 1

$$|I(\omega, v)| \geqslant \min\{\hat{c}\delta \deg(F), n\}. \tag{15}$$

Если $|I(\omega, v)| \geqslant \min\{\hat{c}\delta \deg(F), n\} = n$, то легко показать, что C не является $\hat{c}$-FP-, а значит, и $\hat{c}$-TA-кодом, и (13) доказано. Поэтому далее $|I(\omega, v)| \geqslant \hat{c}\delta \deg(F)$.

Для произвольного $S \subset \{1, \ldots, n\}$ определим $I_S(u, v) = \{i \in S : u_i = v_i\}$. Пусть $A = \{1, \ldots, \hat{c}\delta \deg(F)\}$. Докажем, что

$$\forall i \in \{1, \ldots, \hat{c}\} \left(|I_A(\omega, u_i)| \leqslant \alpha\right). \tag{16}$$

Предположим противное: найдётся такой номер i_0, что $|I_A(\omega, u_{i_0})| > \alpha$. Тогда существует $r > \alpha$ позиций из A, таких, что в каждой позиции k выполняется $u_{i_0,k} = \omega_k$. Согласно построению коалиции из леммы 1, $\omega_j = v_j$ для всех $j \in A$, поэтому $u_{i_0,k} = v_k$. Значит, $|I(v, u_{i_0})| = r > \alpha$. Тогда

$$\rho(v, u_{i_0}) = n - |I(v, u_{i_0})| < n - \alpha,$$

чего в силу утверждения 1 быть не может, значит, (16) выполнено.

Докажем неравенство

$$|I(\omega, u_i)| \leqslant n - \hat{c}\delta \deg(F) + \alpha.$$

Ввиду того, что

$$I(\omega, u_i) = I_A(\omega, u_i) \cup I_{\{1,\ldots,n\}\setminus A}(\omega, u_i),$$

и неравенства (16) получаем

$$|I(\omega, u_i)| = |I_A(\omega, u_i)| + |I_{\{1,\ldots,n\}\setminus A}(\omega, u_i)| \leqslant \alpha + n - \hat{c}\delta \deg(F). \tag{17}$$

Из (14) следует, что

$$n - \hat{c}\delta \deg(F) + \alpha \leqslant \hat{c}\delta \deg(F).$$

Тогда, учитывая (15) и (17), получаем

$$|I(\omega, u_i)| \leqslant n - \hat{c}\delta + \alpha \leqslant \hat{c}\delta \leqslant |I(\omega, v)|.$$

Это означает, что C не является $\hat{c}$-ТА-кодом.

Пусть теперь

$$\tilde{B}_{\mathrm{TA}} = \min\left\{\left\lceil \frac{n+\alpha}{2\delta \deg(F)} \right\rceil, \left\lceil \frac{\varkappa}{\delta} \right\rceil\right\} = \left\lceil \frac{\varkappa}{\delta} \right\rceil.$$

В этом случае, если $\hat{c} \geqslant \tilde{B}_{\mathrm{TA}}$, то с помощью (4) из леммы 1 легко показать, что C не является $\hat{c}$-FP-, а значит, и $\hat{c}$-ТА-кодом.

Неравенство (13) доказано.

3. Теперь, согласно лемме 2, получаем, что

$$\tilde{B}_{\mathrm{TA}}(C) = \left\lceil \frac{n+\alpha}{2\lfloor \alpha/\deg(F) \rfloor \deg(F)} \right\rceil \leqslant \left\lceil \frac{n}{\alpha} \right\rceil.$$

Справедливость неравенства

$$R_{\mathrm{TA}}(C) \geqslant \sqrt{n/\alpha}$$

доказана в [6, теорема 1], а справедливость

$$R_{\mathrm{FP}}(C) \geqslant \left\lceil \frac{n}{\alpha} \right\rceil$$

показана в [13, теорема 3].

Таким образом, доказана вся цепочка неравенств (3), а вместе с тем и теорема 1.

Заключение

В работе представлен специальный класс алгебраических кривых, на которых возможно уточнение рубежей множеств компрометации для идентифицирующих c-TA- и c-FP-свойств применительно к одноточечным алгеброгеометрическим кодам. Полученные для этих рубежей оценки даны в основной теореме; приведены примеры таких кривых и вычисления рубежей. Результаты работы представляют самостоятельный теоретичекий интерес, а также могут быть использованы в практических реализациях протоколов широковещательного шифрования.

ЛИТЕРАТУРА

1. *Fiat A. and Naor M.* Broadcast encryption // LNCS. 1994. V. 773. P. 480–491.
2. *Chor B., Fiat A., and Naor M.* Tracing traitors // LNCS. 1994. V. 839. P. 257–270.
3. *Silverberg A., Staddon J., and Walker J.* Applications of list decoding to tracing traitors // IEEE Trans. Inform. Theory. 2003. V. 49. No. 5. P. 1312–1318.
4. *Stinson D. R. and Wei R.* Combinatorial properties and constructions of traceability schemes and frameproof codes // SIAM J. Discr. Math. 1998. V. 11. Iss. 1. P. 41–53.
5. *Staddon J. N., Stinson D. R., and Wei R.* Combinatorial properties of frameproof and traceability codes // IEEE Trans. Inform. Theory. 2001. V. 47. No. 3. P. 1042–1049.
6. *Загуменнов Д. В., Мкртичян В. В.* О применимости алгеброгеометрических кодов L-конструкции как кодов защиты от копирования // Прикладная дискретная математика. 2019. № 44. С. 67–93.
7. *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.
8. *Ma Y. and Ding Y.* Reed — Solomon codes as traceability codes with an efficient tracing algorithm // 8th Intern. Conf. Signal Processing. Guilin, China, 2006. V. 4. `https://ieeexplore.ieee.org/document/4129649`.
9. *Guruswami V. and Sudan M.* Improved decoding of Reed-Solomon and algebraic-geometric codes // Foundations of Computer Science. Palo Alto: IEEE, 1998. P. 28–37.
10. *Fernandez M., Cotrina J., Soriano M., and Domingo N.* A note about the traceability properties of linear codes // LNCS. 2007. V. 4817. P. 251–258.
11. *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.
12. *Pellikaan R. and Wu X-W.* List decoding of q-ary Reed — Muller codes // IEEE Trans. Inform. Theory. 2004. V. 50. No. 4. P. 679–682.
13. *Деундяк В. М., Загуменнов Д. В.* Исследование свойств АГ-кодов как кодов для защиты от копирования // Моделирование и анализ информационных систем. 2020. Т. 27. № 1. С. 22–38.
14. *Barg A. and Kabatiansky G.* A class of I.P.P. codes with efficient identification // J. Complexity. 2004. V. 20. Iss. 2–3. P. 137–147.
15. *Zagumennov D., Deundyak V., Gufan A., and Mkrtichan V.* Algebraic geometry codes for special broadcast encryption schemes in telecommunication nets // Proc. MWENT. Moscow, Russia, 2020. P. 1–6.
16. *Кабатянский Г. А.* Идентифицирующие коды и их обобщения // Проблемы передачи информации. 2019. Т. 55. № 3. С. 93–105.
17. *Moreira J., Fernandez M., and Soriano M.* On the relationship between the traceability properties of Reed — Solomon codes // Adv. Math. Commun. 2012. V. 6. No. 4. P. 467–478.

18. *Fernandez M.* Codes with traceability properties and the Silverberg — Staddon — Walker conjecture // XVI Intern. Symp. "Problems of Redundancy in Information and Control Systems". Moscow, Russia, 2019. Plenary lecture.
19. *Safavi-Naini R. and Wang Y.* New results on frame-proof codes and traceability schemes // IEEE Trans. Inform. Theory. 2001. V. 47. No. 7. P. 3029–3033.
20. *Ge G. and Shangguan Ch.* Good traceability codes do exist. `https://arxiv.org/abs/1601.04810v1`.
21. *Ge G., Ma J., and Shangguan Ch.* New results for traitor tracing schemes. `https://arxiv.org/abs/1610.07719`.
22. *Chee Y. M. and Zhang X.* Improved constructions of frameproof codes // IEEE Trans. Inform. Theory. 2012. V. 58. No. 8. P. 5449–5453.
23. *Noskov I. and Bezzateev S.* Traceability schemes usings finite geometry // 10th Intern. Congress ICUMT. Moscow, Russia, 2018. P. 1–5.
24. *Цфасман М. А, Влэдуц С. Г., Ногин Д. Ю.* Алгеброгеометрические коды. Основные понятия. М.: МЦНМО, 2003.
25. *Hoholdt T., van Lint J. H., and Pellikaan R.* Algebraic geometry codes // Handbook of Coding Theory / V. S. Pless, W. C. Huffman, and R. A. Brualdi (eds.). V. 1. Amsterdam: Elsevier, 1998. P. 871–961.

REFERENCES

1. *Fiat A. and Naor M.* Broadcast encryption. LNCS, 1994, vol. 773, pp. 480–491.
2. *Chor B., Fiat A., and Naor M.* Tracing traitors. LNCS, 1994, vol. 839, pp. 257–270.
3. *Silverberg A., Staddon J., and Walker J.* Applications of list decoding to tracing traitors. IEEE Trans. Inform. Theory, 2003, vol. 49, no. 5, pp. 1312–1318.
4. *Stinson D. R. and Wei R.* Combinatorial properties and constructions of traceability schemes and frameproof codes. SIAM J. Discr. Math., 1998, vol. 11, iss. 1, pp. 41–53
5. *Staddon J. N., Stinson D. R., and Wei R.* Combinatorial properties of frameproof and traceability codes. IEEE Trans. Inform. Theory, 2001, vol. 47, no. 3, pp. 1042–1049
6. *Zagumennov D. V. and Mkrtichyan V. V.* O primenimosti algebrogeometricheskikh kodov L-konstruktsii kak kodov zashchity ot kopirovaniya [On application of algebraic geometry codes of L-construction in copy protection]. Prikladnaya Diskretnaya Matematika, 2019, no. 44, pp. 67–93. (in Russian)
7. *Deundyak V. M. and Mkrtichyan V. V.* Issledovaniye granits primeneniya skhemy zashchity informatsii, osnovannoy na RS-kodakh [Research of applying bounds of the information protection scheme based on PS-codes]. Diskretn. Anal. Issled. Oper., 2011, vol. 18, iss. 3, pp. 21–38 (in Russian)
8. *Ma Y. and Ding Y.* Reed — Solomon codes as traceability codes with an efficient tracing algorithm. 8th Intern. Conf. Signal Processing, Guilin, China, 2006, vol. 4. `https://ieeexplore.ieee.org/document/4129649`.
9. *Guruswami V. and Sudan M.* Improved decoding of Reed — Solomon and algebraic-geometric codes. Foundations of Computer Science. Palo Alto, IEEE, 1998, pp. 28–37.
10. *Fernandez M., Cotrina J., Soriano M., and Domingo N.* A note about the traceability properties of linear codes. LNCS, 2007, vol. 4817, pp. 251–258.
11. *Deundyak V. M., Evpak S. A., and Mkrtichyan V. V.* Analysis of properties of q-ary Reed — Muller error-correcting codes viewed as codes for copyright protection. Problems Inform. Transmission, 2015, vol. 51, no. 4, pp. 398–408.
12. *Pellikaan R. and Wu X-W.* List decoding of q-ary Reed — Muller codes. IEEE Trans. Inform. Theory, 2004, vol. 50, no. 4, pp. 679–682.

13. *Deundyak V. M. and Zagumennov D. V.* Issledovanie svoystv AG-kodov kak kodov dlya zashchity ot kopirovaniya [On the properties of algebraic geometric codes as copy protection codes]. Modelirovanie i Analiz Informatsionnykh Sistem, 2020, vol. 27, no. 1, pp. 22–38. (in Russian)
14. *Barg A. and Kabatiansky G.* A class of I.P.P. codes with efficient identification. J. Complexity, 2004, vol. 20, iss. 2–3, pp. 137–147.
15. *Zagumennov D., Deundyak V., Gufan A., and Mkrtichan V.* Algebraic geometry codes for special broadcast encryption schemes in telecommunication nets. Proc. MWENT, Moscow, Russia, 2020, pp. 1–6.
16. *Kabatyansky G. A.* Traceability codes and their generalizations. Problems Inform. Transmission, 2019, vol. 55, no. 3, pp. 283–294.
17. *Moreira J., Fernandez M., and Soriano M.* On the relationship between the traceability properties of Reed — Solomon codes. Adv. Math. Commun., 2012, vol. 6, no. 4, pp. 467–478.
18. *Fernandez M.* Codes with traceability properties and the Silverberg — Staddon — Walker conjecture. XVI Intern. Symp. "Problems of Redundancy in Information and Control Systems", Moscow, Russia, 2019, Plenary lecture.
19. *Safavi-Naini R. and Wang Y.* New results on frame-proof codes and traceability schemes. IEEE Trans. Inform. Theory, 2001, vol. 47, no. 7, pp. 3029–3033.
20. *Ge G. and Shangguan Ch.* Good traceability codes do exist. `https://arxiv.org/abs/1601.04810v1`.
21. *Ge G., Ma J., and Shangguan Ch.* New results for traitor tracing schemes. `https://arxiv.org/abs/1610.07719`.
22. *Chee Y. M. and Zhang X.* Improved constructions of frameproof codes. IEEE Trans. Inform. Theory, 2012, vol. 58, no. 8, pp. 5449–5453.
23. *Noskov I. and Bezzateev S.* Traceability schemes usings finite geometry. 10th Intern. Congress ICUMT, Moscow, Russia, 2018, pp. 1–5.
24. *Tsfasman M. A, Vleduts S. G., and Nogin D. Yu.* Algebrogeometricheskie kody. Osnovnye ponyatiya [Algebraic Geometric Codes. Basic Notions]. Moscow, MCCME Publ., 2003. (in Russian)
25. *Hoholdt T., van Lint J. H., and Pellikaan R.* Algebraic geometry codes. Handbook of Coding Theory, V. S. Pless, W. C. Huffman, and R. A. Brualdi (eds.), vol. 1, Amsterdam, Elsevier, 1998, pp. 871–961.