Исследование алгебро-геометрических кодов как кодов защиты от копирования

Загуменнов Денис Владимирович

Южный Федеральный университет
Институт математики, механики и компьютерных наук им. И. И. Воровича
Кафедра алгебры и дискретной математики

04.12.2015

ССШШ и их принципы

ССШШ - схемы специального широковещательного шифрования

- Свободное тиражирование данных в зашифрованном виде
- Уникальный набор ключей у легального пользователя
- Возможность коалиционной атаки
- Списочный декодер + "хороший"код

Списочное декодирование

- Возможность декодирования за пределами классического радиуса декодирования
- Результат в виде списка кодовых слов
- Кодовое слово, соответствующее исходному сообщению, находится в списке

Коалиции и её потомки

Пусть C — код. Коалицией размера c будем называть набор из c векторов кода, то есть $C_0 = \{u^{(1)}, u^{(2)}, \ldots, u^{(c)}\}, u^{(i)} \in C$.

Потомками коалиции C_0 назовём множество

$$\mathrm{desc}(C_0) = \{(x_1, x_2, , \ldots, x_n) \mid x_i \in \{u_i, u \in C_0\}\}.$$

Определение c-TA

Множество всех коалиций кода C размера не больше c обозначим $\mathrm{coal}_c(C)$
Код C называется $c-TA$ кодом, если выполнено следующее условие:

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

$$\forall \omega \in \mathrm{desc}(C_0)\ \exists y \in C_0 \to d(\omega, y) < d(v, y)$$

Достаточное условие наличия у кода c-TA - свойства

Теорема. (A. Silverberg, J. Staddon, J. L. Walker. Applications of List Decoding to Tracing Traitors. Theorem 5)

Пусть C — код, n — длина кода C, d — минимальное кодовое расстояние кода C. Если код C удовлетворяет условию $d > n - \frac{n}{c^2}$ $(c \in \mathbb{N}, c \geq 2)$, то код C является *c-TA* кодом.

Причём, если $C_0 \in \mathrm{coal}_c(C)$ $w \in \mathrm{desc}(\mathrm{C}_0)$, то

1) $\exists\, x \in C_0 : d(x, w) < n - \frac{n}{c}$,

2) $\forall\, x \in C : d(x, w) < n - \frac{n}{c} \to x \in C_0$

Код и декодер для ССШШ

Пусть C — код, n — его длина, d — минимальное кодовое расстояние. Пусть есть списочный декодер для C, исправляющий r ошибок. Для эффективного применения кода C и списочного декодера для кода C в ССШШ достаточно выполнения следующих условий:

1) $d > n - \frac{n}{c^2}$

2) $r > n - \frac{n}{c}$

Tom Høholdt, Jacobus H. van Lint and Ruud Pellikaan. Algebraic geometry codes.
Zhuo Zhia Dai. The Algebraic Geometric Coding Theory.
С.Г. Влэдуц, Д.Ю.Ногин, М.А.Цфасман. Алгеброгеометрические коды. Основные понятия.

Аффинное пространство

Пусть k — поле. Аффинное n-мерное пространство над полем k , точками которого являются наборы

$$P = \{x_1, x_2, \ldots, x_n\}, x_i \in k,$$

будем обозначать $\mathbb{A}^n(k)$.

Аффинное многообразие

Пусть $\overline{k}$ — алгебраическое замыкание поля k.

Пусть $I \in \overline{k}[x_1, x_2, \ldots, x_n]$ — простой собственный идеал.

Аффинным многообразием называется множество:

$$X = X(I) = \{P = (x_1, x_2, \ldots, x_n) \in \mathbb{A}^n(\overline{k}) : g(x_1, x_2, \ldots, x_n) = 0 \forall g \in I\}.$$

Наборы P называются точками многообразия.

Координатное кольцо и поле функций на многообразии

Факторкольцо $\overline{k}[X] = \overline{k}[x_1, x_2, \ldots, x_n]/I$ называется координатным кольцом многообразия X.

Поле частных координатного кольца называется полем функций многообразия X и обозначается $\overline{k}(X)$.

Плоская аффинная кривая

Пусть $f \in k[x, y]$ — **абсолютно неприводимый многочлен**, тогда $< f >= \{fh : h \in \overline{k}[x, y]\}$ — простой идеал в $\overline{k}[x_1, x_2]$.

Многообразие

$$C = C(f) = \{P = (x, y) \in \mathbb{A}^2(\overline{k}) : g(x, y) = 0 \ \forall g \in < f >\}$$

называется плоской аффиной кривой.

Как нам вернуться к рассмотрению поля k?

Рассматриваются только точки вида

$$P = (x, y) \in C : x, y \in k.$$

Такие точки называются рациональными. Множество рациональных над полем k точек на кривой C обозначается $C(k)$.

Понятия кооррдинатного кольца и поля функций сужаются.
Координатным кольцом плоской аффиной кривой C назовём

$$k[C] = k[x, y]/ < f >,$$

а полем функций $k(C)$ — поле частных $k[C]$.

Пример

$f = y - x^2, C = C(< f >), k = \mathbb{F}_2$
Точки (0,0), (1,1) — рациональные точки, а (α, α^2) и $(\alpha^2, 1)$ — нерациональные точки.

Проективное пространство

Проективное n-мерное пространство над k, точками которого являются наборы вида

$$Q = \{y_1 : y_2 : y_3 : \cdots : y_{n+1}\}, y_i \in k,$$

где

1) не все y_i равны нулю
2) наборы $\{\lambda y_1 : \lambda y_2 : \lambda y_3 : \cdots : \lambda y_n + 1\}, \lambda \in k, \lambda \neq 0$ определяют одну и ту же точку

будем обозначать $\mathbb{P}^n(k)$.

Плоская проективная кривая

Рассматриваются только однородные многочлены из $k[X : Y : Z]$.

Понятие кривой и многообразия вводятся аналогично:
абсолютно неприводимый однородный многочлен $\rightarrow$ простой однородный идеал $\rightarrow$ координатное кольцо $\rightarrow$ поле частных координатного кольца.

Замечание. Поле функций на проективной кривой задаётся как подкольцо поля частных с однородными числителем и знаменателем одинаковой степени.

Плоская проективная кривая

Любой неоднородный многочлен из $k[x, y]$ можно "проективизовать":
$f \in k[x, y]$ — неоднородный многолчен соответствует
$F(X : Y : Z) = Z^d f(\frac{X}{Z}, \frac{Y}{Z}) \in k[X : Y : Z]$, где $d = \deg(f)$.

Однородному многочлену из $k[X : Y : Z]$ поставим в соответствие многочлен из $k[x, y]$:
$F(X : Y : Z) = F(\frac{X}{Z} : \frac{Y}{Z} : 1)$, обозначим $x = \frac{X}{Z}, y = \frac{Y}{Z}$, тогда F соответсвует $F(x, y) \in k[x, y]$.

Пример

$f = y - x^2, C = C(< f >)$
$F = Z^2(Y/Z - X^2/Z^2) = YZ - X^2$
Рациональные точки над $\mathbb{F}_2$ — точки $(0 : 1 : 0)$, $(1 : 1 : 1)$, $(0 : 0 : 1)$.

Локальное кольцо точки

Напомнание: координатным кольцом плоской аффиной кривой C является $k[C] = k[x, y]/ < f >$, а полем функций $k(C)$ — поле частных $k[C]$.

Будем считать $g, h \in k(C)$ одинаковыми элементами поля рациональных функций, если из g обычными преобразованиями многочленов можно получить h, используя условие $f = 0$.

Пусть $\phi \in k(C), P \in C$. Говорят, что ϕ регулярна в точке P, если

$$\exists g, h \in k(C) : \phi = \frac{g}{h}, h(P) \neq 0.$$

$f = y - x^2, C = C(< f >)$

Функция $\frac{y}{x} = x = \frac{x}{1}$. Значит, $\frac{y}{x}$ регулярна в точке $(0, 0)$.

Локальное кольцо точки

Пусть $P \in X$. Локальным кольцом точки P называется кольцо $\mathfrak{O}_P$, состоящее из функций, регулярных в P, то есть:

$$\mathfrak{O}_P = \{\phi \in k(C) : \exists\, g, h \in k(C) : \phi = \frac{g}{h}, h(P) \neq 0\}.$$

Теорема

Локальное кольцо точки P имеет единственный максимальный идеал $\mathfrak{M}_P$. Он состоит из функций, принимающих на точке P значение 0: $\mathfrak{M}_P = \{\phi \in \mathfrak{O}_P : \phi(P) = 0\}$.

Неособые точки и гладкие кривые.

Точка P называется неособой, если $\forall \phi \in k(C) \phi \in \mathfrak{O}_P$ или $\phi^{-1} \in \mathfrak{O}_P$, в противном случае точка называется особой.

Аффинная кривая называется гладкой, если на ней нет особых точек. Далее будем рассматривать только гладкие кривые.

Локальный параметр.

Теорема.

Точка $P \in C$ неособа тогда и только тогда, когда максимальный идеал $\mathfrak{M}_P$ в локальном кольце точки P – главный, то есть $\exists t \in \mathfrak{M}_P : m = \{ta : a \in \mathfrak{O}_P\}$.

Если $P \in C$ – неособая точка, то такая функция $t \in \mathfrak{M}_P$, что $\mathfrak{M}_P = t\mathfrak{O}_P$, называется локальным параметром в точке P.

Локальный параметр.

Теорема.

Пусть C – гладкая кривая, $P \in C$, t – локальный параметр. Тогда любой элемент $\mathfrak{O}_P$ может быть представлен единственным образом в виде $ut^n, u \in \mathfrak{O}_P \setminus \mathfrak{M}_P, n \in \mathbb{N}$.

Дискретное нормирование.

Любой элемент $\phi \in \mathfrak{O}_P$ может быть представлен единственным образом в виде $ut^n, u \in \mathfrak{O}_P \setminus \mathfrak{M}_P, n \in \mathbb{N}$.
Рассмотрим функцию:

$$\mathrm{ord} : k(C) \to \mathbb{Z} \cup \infty,$$

заданную по правилу:
1) $\mathrm{ord}_P(0) = \infty \ \forall P \in C$
2) $\mathrm{ord}_P(\phi) = n, \phi \in \mathfrak{O}_P$
3) $\mathrm{ord}_P(\phi) = -n, \phi^{-1} \in \mathfrak{O}_P$.

Дифференциальный признак.

Пусть $f = \sum a_{i,j} x^i y^j$, тогда $f_x = \sum a_{i,j} i x^{i-1} y^j$, $f_y = \sum a_{i,j} j x^i y^{j-1}$.
Аналогично, пусть $F = \sum a_{i,j,k} X^i Y^j Z^k$, тогда $F_X = \sum a_{i,j,k} i X^{i-1} Y^j Z^k$, $F_Y = \sum a_{i,j} j X^i Y^{j-1} Z^k$, $F_Z = \sum a_{i,j} k X^i Y^j Z^{k-1}$.

Теорема — дифференциальный признак

Пусть C - аффинная кривая, $P = (a, b) \in C$, тогда если $f_y(P) \neq 0$, то $t = x - a$ является локальным параметром, а если $f_x(P) \neq 0$, то $t = y - b$ является локальным параметром. Если же $f_x = f_y = 0$, то P является особой точкой.

Дискретное нормирования поля функций на проективной кривой

Пусть C – плоская проективная кривая, заданная многочленом $F(X : Y : Z)$. Точка $P \in C$ называется особой, если

$$F_X(P) = F_Y(P) = F_Z(P),$$

иначе называется неособой.

Пусть $P = (a : b : c)$ – неособая точка на проективной кривой C, тогда:

$$\mathrm{ord}_{(a:b:c)}(G(X : Y : Z)) = \mathrm{ord}_{(\frac{a}{c}:\frac{b}{c}:1)}(G(\frac{X}{Z} : \frac{Y}{Z} : 1)) = \mathrm{ord}_{(\frac{a}{c},\frac{b}{c})}(G(x, y)).$$

Дивизоры

Пусть – гладкая проективная кривая. Дивизором D на C называется формальная конечная сумма вида $D = \sum a_P P$, где P – точки на C, $a_P \in \mathbb{Z}$.

Если для дивизора $D = \sum a_P P$ все $a_P \geq 0$, то D называют эффективным дивизором.

Степенью дивизора $\deg D$ называется число $\sum a_P$.

Главный дивизор функции

Пусть – гладкая проективная кривая, $\phi \in k(C), \phi \neq 0$. Главным дивизором функции ϕ называется дивизор

$$(\phi) = \sum_{P \in C} \mathrm{ord}_P(\phi) P.$$

Пространство Римана-Роха.

Пусть $D = \sum a_P P$ – дивизор на гладкой проективной кривой C, пространством функций Римана-Роха, ассоциированного с дивизором D называется

$$L(D) = \{\phi \in k(C) \setminus \{0\} : (\phi) + D \geq 0\} \cup \{0\}.$$

Оно является векторным пространством над полем k.

Род кривой

Формула Плюкера

Пусть C – гладкая **плоская** проективная кривая, заданная многочленом F, пусть $deg(F)$ – степень этого многочлена. Родом кривой C будем называть число

$$g = \frac{(\deg(F) - 1)(\deg(F) - 2)}{2}$$

.

Теорема Римана-Роха

Теорема

Пусть C – гладкая проективная кривая рода g, тогда $\forall D$ — дивизора на кривой C, такого, что $deg(D) \geq 2g - 1$ пространство Римана-Роха конечномерно, и

$$\dim(L(D)) = \deg(D) - g + 1$$

.

Алгеброгеометрический код (L-конструкция)

Пусть X - плоская гладкая кривая над произвольным полем, такая, что множество рациональных относительно поля Галуа $\mathbb{F}_q$ точек $X(\mathbb{F}_q)$ непусто.
Пусть $\mathfrak{P} \subset X(\mathbb{F}_q), \mathfrak{P} = \{P_1, \ldots, P_n\}$, $|\mathfrak{P}| = n$, D – выбранный на X дивизор.

Построим отображение $Ev_{\mathfrak{P}} : L(D) \to {\mathbb{F}_q}^n$ по правилу

$$Ev(\phi)_{\mathfrak{P}} = \{\phi(P_1), \ldots, \phi(P_n)\}.$$

Алгеброгеометрический код (L-конструкция)

Получаем код $C = \mathrm{Im}(L(D)) \subset {\mathbb{F}_q}^n$, будем его обозначать C.
Дивизор D будем называть дивизором кода C.

Пусть $\dim(L(D)) = m$. Если $\{\phi_1, \phi_2, \ldots, \phi_m\}$ – базис в $L(D)$, то матрица

$$\begin{pmatrix} \phi_1(P_1) & \phi_1(P_2) & \cdots & \phi_1(P_n) \\ \phi_2(P_1) & \phi_2(P_2) & \cdots & \phi_2(P_n) \\ \vdots & \vdots & \ddots & \vdots \\ \phi_m(P_1) & \phi_m(P_2) & \cdots & \phi_m(P_n) \end{pmatrix}$$

является порождающей матрицей кода.

Алгеброгеометрический код (L-конструкция)

Теорема о параметрах кода

Пусть X – кривая рода g, пусть $2g-1 \leq \deg D = \alpha < n = |\mathfrak{P}|$. Тогда соответствующй алгеброгеометрический код код C является $[n,k,d]_q$-кодом, где

$$k = \alpha - g + 1, d \geq d^* = n - \alpha.$$

Величина $d^* = n - \alpha$ называется конструктивным расстоянием кода. В дальнейшем рассматриваются только коды с конструктивным расстоянием.

Пример

$F = YZ - X^2, k = \mathbb{F}_7$.
$Q = (0 : 1 : 0) \in C$. Возьмём $D = mQ$.
Тогда получим алгеброгеометрический код с порождающей матрицей:

$$\begin{pmatrix} 1 & 1 & 1 & \cdots & 1 \\ 0 & 1 & 2 & \cdots & 6 \\ 0 & 1 & 2^2 & \cdots & 6^2 \\ \vdots & \vdots & \ddots & \vdots & \\ 0 & 1^m & 2^m & \cdots & 6^m \end{pmatrix}$$

Условие c-TA

Теорема (A. Silverberg, J. Staddon, J. L. Walker. Applications of List Decoding to Tracing Traitors. Theorem 6)

Пусть n - длина кода, k - размерность кода, g - род кривой, на котором определён код, D - дивизор кода C, $\deg(D) = \alpha \geq 2g - 1$. Алгеброгеометрический код C является *c-TA* кодом, если выполняется условие:

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

Списочный декодер Судана-Гурусвами.

Теорема о радиусе работы

Пусть C - алгебро-геометрический код длины n, D - дивизор кода C, $\deg(D) = \alpha \geq 2g - 1$. Тогда существует алгоритм декодирования (алгоритм декодирования Судана-Гурусвами) этого кода со сложностью, полиномиальной по n, исправляющий не более r ошибок, где $r < n - \sqrt{n(k + g - 1)}$.

Условие применения декодера. Случай 1.

Утверждение 1.1

Пусть $\sqrt{n(k+g-1)} \notin \mathbb{N}$, тогда максимальный возможный радиус декодера Судана-Гурусами равен $r_* = n - \lceil \sqrt{n(k+g-1)} \rceil$.

Утверждение 1.2

Пусть n - длина кода, k - размерность кода, g - род кривой, на которой определён код, r - радиус списочного декодера, D - дивизор кода C, $\deg(D) = \alpha \geq 2g-1$. Пусть $\sqrt{n\alpha} \notin \mathbb{N}$. Тогда списочный декодер Судана-Гурусвами для алгеброгеометрического кода C применим в ССШШ, если:

$$c < \frac{n}{\lceil \sqrt{n(k+g-1)} \rceil} \tag{2}$$

Причём при выполнении этого условия выполняется и условие (1) (C является $c - TA$-кодом).

Условие применения декодера. Случай 2.

Утверждение 2.1

Пусть $\sqrt{n(k+g-1)} \in \mathbb{N}$, тогда максимальный возможный радиус декодера Судана-Гурусами равен $r_* = n - \sqrt{n(k+g-1)} - 1$.

Утверждение 2.2

Пусть n - длина кода, k - размерность кода, g - род кривой, на котором определён код, r - радиус списочного декодера, D - дивизор кода C, $\deg(D) = \alpha \geq 2g-1$. Пусть $\sqrt{n\alpha} \in \mathbb{N}$. Тогда списочный декодер Судана-Гурусвами для алгебро-геометрического кода C применим в ССШШ, если:

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

Причём при выполнении этого условия выполняется и условие (1) (C является $c-TA$-кодом).

Двойственное условие на род кривой

Утверждение 3.1

Пусть C — алгеброгеометричсекий код, n — длина кода, k — размерность кода, g — род кривой, на котором определён код, D — дивизор кода C, $\deg(D) = \alpha \geq 2g - 1$.
Если

$$g < 1 - k + \frac{n}{c^2}, \tag{4}$$

то выполняется условие (1) (C является $c - TA$-кодом).

Двойственное условие на род кривой. Случай 1

Утверждение 3.2

Пусть C — алгеброгеометричсекий код, n — длина кода, k — размерность кода, g — род кривой, на котором определён код, D — дивизор кода C, $\deg(D) = \alpha \geq 2g - 1$. Пусть $\sqrt{n\alpha} \notin \mathbb{N}$. Обозначим $\epsilon = \lceil \sqrt{n\alpha} \rceil - \sqrt{n\alpha}$.

Если

$$g < 1 - k + \frac{n}{c^2} - \frac{2\epsilon}{c} + \frac{\epsilon^2}{n}, \tag{5}$$

то выполняется условие (2) (условие применение декодера Судана-Гурусвами).

Причём при выполнении (5) выполняется и (4).

Двойственное условие на род кривой. Случай 2

Утверждение 3.3

Пусть C — алгеброгеометричсекий код, n — длина кода, k — размерность кода, g — род кривой, на котором определён код, r — радиус списочного декодера, D — дивизор кода C, $\deg(D) = \alpha \geq 2g - 1$. Пусть $\sqrt{n\alpha} \in \mathbb{N}$. Если

$$g < 1 - k + \frac{n}{c^2} - \frac{2}{c} + \frac{1}{n}, \tag{6}$$

то выполняется (3) (условие применение декодера Судана-Гурусвами). Причём, если выполняется (6), то выполняется и (5), а значит, и (1) (C является $c - TA$-кодом).

Условие c-TA

Ω - конструкция алгеброгеометрических кодов — двойственные по отношению к L-конструкции коды. Будем обозначать алгеброгеометрический код Ω-конструкции C_Ω, его длину — n_Ω, размерность k_Ω.

Условие c-TA

Пусть C_Ω определён на кривой рода g, D — дивизор кода, $\deg(D) \geq 2g-1$, тогда C_Ω является c-TA кодом, если выполнено условие:

$$c < \sqrt{\frac{n_\Omega}{k_\Omega + g - 1}}.$$

Проблема использования в отсутствии списочного декодера.

Классические коды Гоппа

Классические коды Гоппа (в том числе бинарные коды Гоппа) — класс алгеброгеометрических кодов Ω-конструкции.
Бинарный код Гоппа g зависит от трёх параметров: $g = g(n, m, t)$.

Условие c-TA

Бинарный код Гоппа $g(n, m, t)$ является c-TA кодом, если выполнено условие:

$$c < \sqrt{\frac{n}{n - 2t - 1}}.$$

Списочный декодер Бернштейна

Списочный декодер Бернштейна — списочный декодер для бинарных кодов Гоппы.

Декодер исправляет $\lfloor n - \sqrt{n(n-2t-2)} \rfloor$ ошибок.

Условие применения декодера

Списочный декодер Бернштейна применим в ССШШ, если выполнено условие:

$$c < \frac{n}{\lceil \sqrt{n(n-2t-1)} \rceil}.$$

Спасибо за внимание!