Aene?aoiia
eiaa?eoie?iaaiea
aeia?yeeeioe?aneeo e?eau

МОСКОВСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
имени М. В. ЛОМОНОСОВА
Механико—математический факультет
Кафедра теории чисел

Студент III курса
Милованов Алексей Сергеевич

Дискретное логарифмирование гиперэллиптических кривых
(Discrete logarithm on hyperelliptic curves)

Научный руководитель:
Черепнёв Михаил Алексеевич

Москва, 2011

Введение

Будем обозначать гиперэллиптическую кривую[1] C над полем K как C/K. Основное поле $K = GF(q), q = p^m$. Поле функций кривой C над полем K будем обозначать $K(C)$[1]. Группу всех дивизоров над кривой[1] будем обозначать $div(C)$. Фактор группу дивизоров по подгруппе главных дивизоров(дивизоров функций[1]) будем обозначать $Pic(C)$. Фактор группу дивизоров степени 0 по подгруппе главных дивизоров будем обозначать $Pic^0(C)$. Мы будем сводить задачу нахождения дискретного логарифмирования в группе $Pic^0(C)$ (или, в случае эллиптческой кривой, в группе точек кривой) к аддитивной группе в векторном пространстве или к мультикативной группе в конечном поле.

1.Дискретное логарифмирование в подруппе p-кручения гиперэллиптической кривой

Определение: пространством дифференциалов над кривой C называется векторное пространство Ω над $K(C)$ порожденное элементами

вида dx, где $x \in K(C)$ в котором выполняются следующие свойства:

$1)d(x + y) = dx + dy$

$2)d(xy) = xdy + ydx$

$3)d(const) = 0$.

Утверждение 1.1(доказательство в [7])

Ω есть одномерное векторное пространство над $K(C)$.

Пусть $\omega \in \Omega, P \in C$. Определим $ord_P(\omega)$, как $ord_P(f)$, $\omega = fdt$, где $f, t \in K(C), t$ - униформизатор в точке P.

Утверждение 1.2(доказательство в [1])

Значение $ord_P(\omega)$ не зависит от выбора униформизатора t.

Определение: $div(\omega) = \sum_P ord_P(w)(P)$.

Дивизор называется положительным, если все его члены ≥ 0. Дифференциал ω называется голоморфным, если $div(\omega)$ - положительный дивизор. Пространство голоморфных дифференциалов обозначается Ω^0.

Обозначим K_C - образ $div(\omega)$ в $Pic(C)$ всех ненулевых дифференциалов $\omega \in \Omega$. (то есть дивизоры вида $div(\omega) + div(f)$, где $\omega \in \Omega, f \in K(C)$)

Пусть $D \in div(C)$.

Рассмотрим множество:$\mathfrak{L}(D) = \{f \in K(C) : div(f) \geq -D\} \cup \{0\}$.

Это будет конечномерное векторное пространство. $l(D) = dim\mathfrak{L}(D)$

Утверждение 1.3(теорема Римана-Роха, доказательство в [2]).

$l(D) - l(K_C - D) = deg(D) - g + 1$. g называется родом кривой C.

Следствие 1:

1) $l(K_C) = g$.

Следствие 2:

2) $deg(K_C) = 2g - 2$.

Замечание:

Так как K_C состоит из дивизоров вида $div(\omega) + div(f)$, где $\omega \in \Omega, f \in K(C)$, то положив $f = 0$ получаем, что теоремой Римана-Роха можно пользоваться для любого ненулевого дифференциала.

Определим производную Δ на $K(C)$ как K-линейное отображение: $K(C) \to K(C)$, такое что: $\Delta(\mathrm{fg}) = \Delta(\mathrm{f})\mathrm{g} + \Delta(\mathrm{g})\mathrm{f}$.

Утверждение 1.4(доказательство в [3])

Если $x \in K(C)$ и $K(C)$ конечное расширение $K(x)$, то существует единственная производная D такая, что $D(x) = 1$. Образ $f \in K(C)$ этой производной D обозначается как $\partial f/\partial x$.

Утверждение 1.5(доказательство в [4])

Пусть $f \in K(C)$. Тогда $df = (\partial f/\partial x)dx$.

Утверждение 1.6(доказательство в [1])

Пусть t - униформизатор в некоторой не особой точке P. Тогда $K(C)$ есть конечное расширение $K(t)$

Утверждение 1.7(доказательство в [5])

Пусть $f \in K(C), f$ регулярна в точке P, t - униформизатор в точке P. Тогда $(\partial f/\partial t)$ также регулярна в точке P.

Обозначим подгруппу p-кручения в группе Pic^0_C как $Pic^0_C[p]$.

Рассмотрим $D \in Pic^0_C[p]$. Тогда $pD = div(f), f \in K(C)$

Утверждение 1.8

$df/f \in \Omega^0$.

Доказательство:

Запишем, в некоторой точке $P : f = t^n u$, где $ord_P(u) = 0$.

Так как $pD = div(f)$, то $p|n$.

$df/f = nt^{n-1}udt/t^n u + t^n du/t^n u = \frac{(\partial u/\partial t)dt}{u}$. Используя Утверждение 1.7 для u получаем, что $(\partial u/\partial t)$ регулярна в P, откуда $ord_P(df/f) \geq 0$.

Утверждение 1.9

$\exists$ мономорфизм(инъективный гомоморфизм) $Pic^0_C[p] \to K^{2g-1}$.

Доказательство:

Зафиксируем произвольную точку $P \in C$ и униформизатор t для неё. Для $D \in Pic^0_C[p]$ найдём $f \in K(C) : pD = div(f)$([8],стр.77, 389-403). $df/f \in \Omega^0$ в точке P записывается следующим образом:

$df/f = a_0 + a_1 t + ...$

Определим отображение $Pic^0_C[p] \to K^{2g-1} : D \to (a_0, ..., a_{2g-2})$.

Пусть различные D_1, D_2 которым соответсвуют функции f_1 и f_2 отобразились в одну точку $\in K^{2g-1}$. Используя утверждение 1.8 получаем, что $df_i/f_i \in \Omega^0$(i = 1, 2). Так как Ω^0 - векторное пространство получаем, что $df_1/f_1 - df_2/f_2 \in \Omega^0$. Тогда у ненулевого голоморфного дифференциала $df_1/f_1 - df_2/f_2$ в разложении по униформизатору t первые $2g-1$ координат будут нулевыми(т. к. df_1/f_1 и df_2/f_2 по предположению имеют одинаковые первые $2g-1$ координат). Но тогда степень этого дифференциала будет $> 2g-2$, т. к. любой ненулевой член в разложении будет иметь степень хотя бы $2g-1$. Таким образом мы получили голоморфный дифференциал у которого степень в точке $> 2g-2$. Так как у дивизора голоморфного дифференциала все члены ≥ 0 получам, что у дивизора этого дифференциала степень $> 2g-2$. Это противоречит следствию 2 теоремы Римана-Роха(этой теоремой можно воспользоваться по замечанию находящемуся после этого следствия).

2.Спаривание Вейля В этом и последующих разделах C - эллиптическая кривая.n - натуральное число взаимно простое с p. $C[n]$ - подгруппа n-кручения группы точек $C(\overline{GF}(q))$.

Спариванием Вейля называется отображение $e_n : C[n]\times C[n] \to \mu_n$(корни из единицы степени n) со следующими свойствами(здесь $P, Q, R \in C[n]$):

1) $e_n(P+Q, R) = e_n(P, R)e_n(Q, R)$, $e_n(P, Q+R) = e_n(P, Q)e_n(P, R)$

2) $e_n(P, P) = 1$

3) Если $P \neq O$, $\exists Q$ такое, что $e_n(P, Q) \neq 1$, если $Q \neq O$, $\exists P$ такое, что $e_n(P, Q) \neq 1$

Пусть $D = \sum n_P(P) \in Div(C)$.

Определение:носителем $D(support(D))$ называется множество точек кривой, таких что $n_P \neq 0$. Пусть $f \in K(C)$. Если $support(D) \cap support(div(f)) \in \{O\}$, то можно определить $f(D)$ следующим образом:

$f(D) = \prod_{P\in C} f(P)^{n_P}$

Утверждение 2.1(доказательство в [5])

Дивизор $D = \sum n_P(P)$ является дивизором функции $\Leftrightarrow \sum n_P = 0$ и $\sum(n_P P) = O$.

Пусть $P \in C[n]$. Обозначим через f_P такую функцию, что $div(f_P) = n(P)-n(O)$. Обозначим $D_P = (P)-(O)$. Определим $e_n(P, Q) = f_P(D_Q)/f_Q(D_P)$.

Утверждение 2.2(доказательство в [5])

Определенная таким образом $e_n(,)$ действительно является спариванием Вейля.

3.Вычисление спаривания Вейля Пусть P и $Q \in C[n]$. Для вычисления спаривания Вейля нужно вычислить функции f_P и f_Q.

Возьмём точку $R \in C$, такую, что $P, P+R \neq Q$.

Заметим, что $\forall$ натурального k $\exists f_k \in K(C)$, такое что: $div(f_k) = k(P+R) - k(R) - (kP) + (O)$. При $n = k : div(f_n) = n(P+R) - n(R)$.

Рассмотрим функцию r такую, что $div(r) = (P) + (R) - (P+R) - (O)$.

Мы можем определить f_P как $f_P = r^n f_n$(мы выбирали R специальным образом чтобы $support(r) \cap support(f_P) \in \{O\}$).

Осталось научиться эффективно вычислять f_n.

Рассмотрим следующие функции:

$g_{P,Q}$ - уравнение прямой проходящей через P и Q.

Утверждение 3.1(доказательство в [5])

$div(g_{P,Q}) = (P) + (Q) + (-(P+Q)) - 3(O)$

Обозначим g_P - уравнение прямой проходящей через P и $-P$.

Утверждение 3.2

$div(f_{k_1+k_2}) = div(f_{k_1} f_{k_2} g_{k_1 P, k_2 P} / g_{(k_1+k_2)P})\forall$ натуральных k_1 и k_2.

Доказательство:

$div(f_{k_1+k_2}) - div(f_{k_1}) - div(f_{k_2}) = (k_1+k_2)(P+R) - (k_1+k_2)(R) - ((k_1+k_2)P) + (O) - k_1(P+R) + k_1(R) + (k_1P) - (O) - k_2(P+R) + k_2(R) + (k_2P) - (O) = (k_1P) + (k_2P) - ((k_1+k_2)P) - (O) = div(g_{k_1P,k_2P}/g_{(k_1+k_2)P})$

Таким образом можно эффективно вычислить f_P и следовательно $e_n(P,Q)$.

Пусть есть точка$P \in C[n]$ порядка n и точка $Q = lP$. Для вычсления l применяется следующая атака:

Находится минимальное k, такое, что $n \mid q^k - 1$. В $C/GF(q^k)$ находится такая точка R, что $e_n(P,R) = \alpha$ имеет порядок n. Далее вычисляется $e_n(Q,R) = \beta$. В мультипликативной группе $GF(q^k)^*$ вычисляется такое t, что $\alpha^t = \beta$. В силу свойств спаривания Вейля, $t = l$.

4.Нахождение дискретного логарифма в группе точек суперсингулярной эллиптической кривой

Обозначим количество точек на кривой $C : \#C(GF(q)) = q + 1 - t$. C является суперсингулярной кривой если $p \mid t$.

Утверждение 4.1(доказательство в [6])

Кривая C является суперсингулярной если:

1) $t^2 = q$, $2q$ или $3q$. В этом случае группа $C(GF(q))$ циклическая.

2) $t^2 = 4q$. В этом случае $C(GF(q)) \cong Z_{\sqrt{q}-1} \oplus Z_{\sqrt{q}-1}$ при $t = 2\sqrt{q}$ или $C(GF(q)) \cong Z_{\sqrt{q}+1} \oplus Z_{\sqrt{q}+1}$ при $t = -2\sqrt{q}$.

3) $t = 0$. В этом случае $C(GF(q))$ циклическая или, что возможно только при $q \equiv 3 \pmod 4$, $C(GF(q)) \cong Z_{(q+1)/2} \oplus Z_2$.

Утверждение 4.2(доказательство в [1])

Пусть, как прежде $t = q + 1 - \#C(GF(q))$, $GF(q^k)$ - расширения поля $GF(q)$ степени k. Тогда $\#C(GF(q^k)) = q^k + 1 - \alpha^k - \beta^k$, где α и β комплексные корни многочлена $1 - tT + qT^2$.

Утверждение 4.3(доказательсво в [1])

Если n и q взаимно просты, то $C[n] \cong Z_n \oplus Z_n$.

Утверждение 4.4

Пусть $C(GF(q))$ эллиптическая кривая, такая, что $C[n] \subseteq C(GF(q))$. $e_n(,)$ - спаривание Вейля. Тогда $\forall P_1, P_2 \in C[n]$ равносильно:

1) $P_1 = P_2 + kP$

2) $e_n(P, P_1) = e_n(P, P_2)$

Доказательство:

1) $\Rightarrow$ 2)

$e_n(P, P_1) = e_n(P, P_2)e_n(P, P)^k = e_n(P, P_2)$

2) $\Rightarrow$ 1)

Пусть точки P и Q порождают группу $C[n]$. Тогда $P_1 - P_2 = aP + bQ$. Если $bQ \neq O$, то, из-за свойства невырожденности спаривания Вейля, $e_n(P, bQ) \neq 1$. Но тогда $e_n(P, P_1) = e_n(P, P_2)e_n(P, P)^a e_n(P, bQ) \neq e_n(P, P_2)$. Противоречие.

Утверждение 4.5

Пусть $P, P_1 \subseteq C[n]$. $P_1 = aP + bQ$(Q - тоже самое, что и в док-ве утверждения 4.4), тогда $e_n(P, P_1)$ имеет порядок $n \Leftrightarrow b$ взаимно просто с n.

Доказательство:

Пусть d - порядок $e_n(P, aP + bQ)$.

$e_n(P, aP + bQ)^d = 1 \Leftrightarrow e_n(P, daP + dbQ) = 1 \Leftrightarrow dbQ = O$(из утверждения 4.4 и определения точки Q). Так как Q имеет порядок n, то получаем, что $d = n \Leftrightarrow b$ взаимно просто с n.

Будем рассматривать суперсингулярные кривые над полем $GF(q)$ и над $GF(q^k)$, где k - такое минимальное число, что $\#C(GF(q)) \mid q^k - 1$. Применяя результаты утверждений 1 и 2 получаем 6 случаев:

1) $t = 0$,$C(GF(q)) \cong Z_{q+1}$. Тогда $k = 2$, $C(GF(q^2)) \cong Z_{q+1} \oplus Z_{q+1}$

2) $t = 0$,$C(GF(q)) \cong Z_{(q+1)/2} \oplus Z_2$.$k = 2$, $C(GF(q^2)) \cong Z_{q+1} \oplus Z_{q+1}$

3) $t = \pm\sqrt{q}$, $C(GF(q)) \cong Z_{q+1\mp\sqrt{q}}$. $k = 3$, $C(GF(q^3)) \cong Z_{\sqrt{q^3}\pm 1} \oplus Z_{\sqrt{q^3}\pm 1}$

4) $t = \pm\sqrt{2q}$, $C(GF(q)) \cong Z_{q+1\mp\sqrt{2q}}$. $k = 4$, $C(GF(q^4)) \cong Z_{q^2+1} \oplus Z_{q^2+1}$

5) $t = \pm\sqrt{3q}$, $C(GF(q)) \cong Z_{q+1\mp\sqrt{3q}}$. $k = 6$, $C(GF(q^6)) \cong Z_{q^3+1} \oplus Z_{q^3+1}$

6) $t = \pm 2\sqrt{q}$. $C(GF(q)) \cong Z_{\sqrt{q}\mp 1} \oplus Z_{\sqrt{q}\mp 1}$. $k = 1$.

Обозначим $n = \#C(GF(q))$. Тогда, заметим, что $C(GF(q^k)) \cong Z_{cn} \oplus Z_{cn}$. Пусть точка $P \in C$ имеет порядок n_1. Пусть также есть точка $R = lP$. Для сведения дискретного логарифмирования в этой группе к дискретному логарифмированию в конечном поле нужно найти такую точку Q, что $e_n(P, Q)$ имеет порядок n_1. Для нахождения такой точки возьмём случайную точку $Q' \in C(GF(q^k))$ и положим $Q = (cn/n_1)Q'$. Вероятность того, что $e_n(P, Q)$ будет иметь порядок $n_1 = \varphi(n_1)/n_1$

Список литературы:

1. J. Silverman, The Arithmetic of Elliptic Curves.
2. R. Hartshorne, Algebraic Geometry
3. O. Zariski & P. Samuel, Commutative algebra
4. H. Stichtenoth, Algebraic function fields and codes
5. V. S. Miller, Weil Pairing and Its Efficient Calculation
6. R. Schoof, Nonsingular plane cubic curves over finite fields.
7. H. Matsumura, Commutative Algebra.
8. Henri Cohen and Gerhard Frey, Handbook of Elliptic and Hyperelliptic curve cryptography.