Криптосистеми на еліптичних кривих

Lecture 3: $E(F_q)$

Грубіян Євген Олександрович

Структура групи $E(\mathbb{F}_q)$

Структура групи

Нехай E/F_q — еліптична крива, визначена над скінченним полем $\mathbb{F}_q$, $\mathrm{char}(F_q) = p$. Тоді група $\mathbb{F}_q$-раціональних точок $E(\mathbb{F}_q)$ є скінченною абелевою групою, що ізоморфна:

$$E(\mathbb{F}_q) \cong \mathbb{Z}/n_1\mathbb{Z} \oplus \mathbb{Z}/n_2\mathbb{Z}, \quad n_2 \mid n_1.$$

- У випадку, коли одна з циклічних компонент групи тривіальна, група кривої є циклічною.
- Структура залежить від властивостей кривої та характеристики поля.

Підгрупа $E[n]$ (точок порядку n)

Підгрупа $E[n]$

Для цілого числа $n \geq 1$ підгрупа точок порядку n:

$$E[n] = \{P \in E(\overline{F_q}) \mid nP = \mathcal{O}\},$$

- Якщо $p \nmid n$, тоді існує канонічний ізоморфізм:

$$E[n] \cong \mathbb{Z}/n\mathbb{Z} \oplus \mathbb{Z}/n\mathbb{Z}.$$

- Якщо ж $n = p^k$, $\mathrm{char}(F_q) = p$: $E[n] \cong \mathbb{Z}/n\mathbb{Z}$ або $\{\mathcal{O}\}$.

Ординарні та суперсингулярні еліптичні криві

Визначення

- E називається ординарною, якщо $E[p] \cong \mathbb{Z}/p\mathbb{Z}$.
- E називається суперсингулярною, якщо $E[p] = \{\mathcal{O}\}$

- Ординарні криві застосовують в класичних криптосистемах на еліптичних кривих.
- Суперсингулярні криві мають особливу структуру кільця ендоморфізмів, тому їх часто застосовують в криптосистемах на базі ізогеній та білінійних спарювань.

Ендоморфізми на еліптичній кривій

Визначення

Ендоморфізм φ на еліптичній кривій E/K — це раціональне відображення:

$$\varphi : E \to E,$$

яке є груповим гомоморфізмом, тобто
$\forall P, Q \in E : \varphi(P + Q) = \varphi(P) + \varphi(Q)$. При цьому $\varphi(\mathcal{O}) = \mathcal{O}$.

- Ендоморфізми формують кільце $\mathsf{End}(E)$ за операцією додавання $(\varphi + \psi)(P) = \varphi(P) + \psi(P)$ та композиції $(\varphi \circ \psi)(P) = \varphi(\psi(P))$ ендоморфізмів.
- Серед них особливо важливим є ендоморфізм Фробеніуса.

Ендоморфізм Фробеніуса

Визначення Фробеніуса

Нехай E/F_q — еліптична крива, визначена над $\mathbb{F}_q$. Ендоморфізм Фробеніуса визначається як:

$$\pi : E \to E, \quad (x, y) \mapsto (x^q, y^q).$$

- π є ендоморфізмом E і елементом кільця $\mathsf{End}(E)$.
- Якщо $x, y \in F_q$ тоді π має тривіальну дію: $\pi(x, y) = (x, y)$
- Всі F_q-раціональні точки кривої лежать в ядрі ендоморфізму Фробеніуса: $E(F_q) = \ker(1 - \pi)$
- Ендоморфізм Фробеніуса відіграє ключову роль у визначенні кількості F_q-раціональних точок на кривій: $\#E(F_q) = \#\ker(1 - \pi) = \deg(1 - \pi)$.

Характеристичне рівняння Фробеніуса

Характеристичне рівняння

Ендоморфізм Фробеніуса π задовольняє характеристичному рівнянню:

$$T^2 - tT + q = 0,$$

де $t = \mathrm{tr}(\pi) = q + 1 - \#E(\mathbb{F}_q)$ - слід ендоморфізму Фробеніуса,
$q = \deg(\pi)$

- Будь який ендоморфізм на $E[n]$ діє як матриця із $GL_2(\mathbb{Z}/n\mathbb{Z})$
- За теоремою Келі (Cayley–Hamilton) кожен оператор(матриця) задовольняє своєму характеристичному многочлену.

Власні значення ендоморфізму Фробеніуса

Нехай α та β — корені характеристичного рівняння (власні значення оператора):

$$T^2 - tT + q = 0.$$

Тоді:

$$\alpha + \beta = t \quad \text{і} \quad \alpha\beta = q.$$

За теоремою Вейля (для ендоморфізмів еліптичних кривих) маємо:

$$|\alpha| = |\beta| = \sqrt{q}.$$

Тому, за нерівністю трикутника:

$$|t| = |\alpha + \beta| \leq |\alpha| + |\beta| = 2\sqrt{q}.$$

Теорема Хассе

Теорема Хассе

Нехай E — еліптична крива, визначена над $\mathbb{F}_q$. Тоді:

$$\left|\#E(\mathbb{F}_q) - (q+1)\right| \leq 2\sqrt{q}.$$

Оскільки $t = q + 1 - \#E(\mathbb{F}_q)$, отримуємо:

$$|t| \leq 2\sqrt{q} \quad \Longrightarrow \quad \left|\#E(\mathbb{F}_q) - (q+1)\right| \leq 2\sqrt{q}.$$

Наслідок: сума квадратичних характерів (1 якщо $f(x)$ є квадратом в F_q, інакше -1) рівняння $y^2 = f(x)$: $\sum \chi(f(x)) = t \leq 2\sqrt{q}$

Поліноми подільності

Нехай $E/K : y^2 = x^3 + ax + b$ — еліптична крива. Для кожного цілого числа $n \geq 0$ визначаються поліноми подільності $\psi_n(x, y)$:

$$\forall P \in E : \psi_n(P) = 0 \quad \Longleftrightarrow \quad [n]P = \mathcal{O},$$

Поліноми подільності визначаються рекурсивно:

$$\psi_0(x, y) = 0, \psi_1(x, y) = 1,$$

$$\psi_2(x, y) = 2y,$$

$$\psi_3(x, y) = 3x^4 + 6ax^2 + 12bx - a^2,$$

$$\psi_4(x, y) = 4y\left(x^6 + 5ax^4 + 20bx^3 - 5a^2x^2 - 4abx - 8b^2 - a^3\right).$$

$$\psi_{2n+1}(x, y) = \psi_{n+2}(x, y)\,\psi_n(x, y)^3 - \psi_{n-1}(x, y)\,\psi_{n+1}(x, y)^3.$$

$$\psi_{2n}(x, y) = \frac{\psi_n(x, y)}{2y}\left(\psi_{n+2}(x, y)\,\psi_{n-1}(x, y)^2 - \psi_{n-2}(x, y)\,\psi_{n+1}(x, y)^2\right).$$

При цьому зазначимо, що $\deg(\psi_n) = (n^2 - 1)/2$

Кількість точок на еліптичній кривій

З характеристичного рівняння Фробеніуса маємо:

$$\#E(\mathbb{F}_q) = q + 1 - t.$$

- Теорема Хассе гарантує, що $|t| \leq 2\sqrt{q}$.
- Отже, $\#E(\mathbb{F}_q)$ знаходиться в інтервалі:

$$q + 1 - 2\sqrt{q} \leq \#E(\mathbb{F}_q) \leq q + 1 + 2\sqrt{q}.$$

- Ідея обчислення кількості точок:
  $\forall P \in E(F_q) : \pi^2(P) + [q]P = \pi([t]P)$ з характеристичного рівняння Фробеніуса.

Алгоритм Скуфа для обчислення $\#E(\mathbb{F}_q)$

Мета: Обчислити $t = q + 1 - \#E(\mathbb{F}_q)$ для кривої $y^2 = f(x) = x^3 + ax + b$.
Основні кроки:

1. Вибір малих простих чисел ℓ (так, щоб $\ell \neq \mathsf{char}(\mathbb{F}_q)$ та добуток вибраних ℓ перевищував $4\sqrt{q}$).
2. Якщо $\ell = 2$ тоді слід перевірити чи існують точки другого порядку:

$$t_2 = \begin{cases} 1, \deg(\gcd(f(x), x^q - x)) \\ 0, \text{інакше} \end{cases}$$

3. Обчислення $t \mod \ell$: Перебираємо $t = 0..\ell - 1$ допоки не виконається
   $\forall P \in E[l] : \pi_l^2(P) + [q]P = \pi_l([t]P) \bmod (\psi_l(x), y^2 - f(x))$, це і буде шукане значення $t_l = t \mod \ell$
4. Відновлення t: Застосовуючи Китайську теорему залишків, відновлюють t (оскільки $|t| \leq 2\sqrt{q}$, достатньо знайти t за модулем великого числа).

Кількість точок на кривій

- Обчислення $\#E(\mathbb{F}_q)$: Нарешті, визначають

$$\#E(\mathbb{F}_q) = q + 1 - t.$$

- Алгоритм Скуфа працює за поліноміальний час: $O(\log(q)^8)$ від розміру скінченого поля
- Також є покращений алгоритм SEA(Schoof-Elkies-Atkin, 1990) що має складність $O(\log(q)^6)$