「non-smooth な次数の同種写像計算とその暗号応用」　中川さん　⑥

§1 導入.

1.1 楕円曲線暗号

k : 有限体, $\mathrm{char}(k) = p$.

E/k : 楕円曲線

$E \supset G$: 位数 n の巡回部分群. (P_0 : Gの生成元)

・離散対数問題 (DLP)

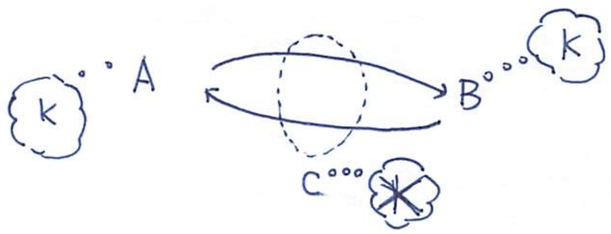
$P, Q \in G$, $P = dQ$ となる $d \in \mathbb{Z}/n\mathbb{Z}$ を求めよ. ← 多項式時間で解けない.

量子コンピュータでは poly で解ける

⟶ 新しい暗号が必要.

⟶ 同種写像暗号.

・鍵共有.



Step1 (sk と pk の生成)

A (sk_A, pk_A)　　　B (sk_B, pk_B)

Step2 (pk を送る)

(sk_A) A $\xrightarrow{pk_A}$ B (sk_B)

A $\xleftarrow{pk_B}$ B

Step3 (K を計算)

A $(sk_A, pk_B) \longmapsto K_A$　　　B $(sk_B, pk_A) \longmapsto K_B$

・正当性: $K_A = K_B$

・安全性: $(pk_A, pk_B) \underset{\text{poly}}{\longmapsto} K = K_A = K_B$

ECDH

Step1

A

$sk_A = d_A \in \mathbb{Z}/n\mathbb{Z}$.

$pk_A = d_A P_0$

Step2

$$A \underset{pk_B}{\overset{pk_A}{\rightleftarrows}} B$$

B

$sk_B = d_B$

$pk_B = d_B P_0$

Step3

$A : (d_A, d_A P_0) \longmapsto K_A = d_A d_B P_0$

$B : (d_B, d_B P_0) \longmapsto K_B = d_A d_B P_0$.

1.2 同種写像暗号.

isogeny E.C(楕円曲線)の間のよい射.

・IP.

EC. E, Fが与えられたとき, isogeny $\phi : E \longrightarrow F$を求めよ. 量子でもpolyで解けない.

・Isogenyの性質

① 準同型 : $\phi : E \longrightarrow F$ は $\phi(P+Q) = \phi(P) + \phi(Q)$

② $\ker(\phi)$ は Eの有限部分群

③ ϕ : separable ならば, $\deg(\phi) = |\ker(\phi)|$.

$\deg(\phi) = d$ のときに, ϕを d-isogeny という.

deg(φ)倍

④ $\phi : E \to F$ に対して, $\exists 1 \psi : F \longrightarrow E$ (s.t.) $\psi \circ \phi = [\deg\phi]_E$

$\phi \circ \psi = [\deg\phi]_F$

このようなψを $\psi = \hat{\phi}$ とかく.

⑤ G : E affine subgroup.

$\exists 1\ \phi : E \longrightarrow \exists 1 F$ (s.t.) $\ker(\phi) = G$

Veln's formulas

$$\boxed{\begin{array}{c}(E, G) \longmapsto (F, \phi) \\ O(|G|) \\ \shortparallel \\ O(\deg\phi)\end{array}}$$

⑧

⑥ Push forward.

$$\begin{tikzcd} E \arrow[r, "\phi_1"] \arrow[d, "\phi_2"'] \arrow[dr, phantom, "\circlearrowleft"] & E_1 \arrow[d, dashed, "{}^{\exists}\phi_2'"] \\ E_2 \arrow[r, dashed, "{}^{\exists}\phi_1'"'] & {}^{\exists}F \end{tikzcd}$$

(S.T.) $\cdot \deg \phi_i' = \deg \phi_i \quad (i=1,2)$

$$\left(\begin{array}{l} \phi_1' : E_1 \to F \\ \phi_2' : E_2 \to F \end{array} \right)$$

- SIDH (super singular isogeny DH)

Definition

E/K に対して,

E : super singular $\Leftrightarrow$ $|E(K)| \equiv 1 \mod p$

Proposition

E/K : super singular ならば, E は $\mathbb{F}_{p^2}$ 上で 定義できる.

E_0 : fix, d_A, d_B : fix.

SIDH

Step 1.2

A

$sk_A = \phi_A : E_0 \to E_A$

(d_A : isogeny)

$pk_A = E_A$

$\xrightarrow{pk_A}$

$\xleftarrow{pk_B}$

B

$sk_B = \phi_B : E_0 \to E_B$

(d_B- isogeny)

$pk_B = E_B$

Step 3

$$\begin{tikzcd} E_0 \arrow[r, "\phi_A"] \arrow[d, dashed, "(\phi_B)"'] & E_A \\ E_B \arrow[r, "\phi_A'"'] & E_{AB} \end{tikzcd}$$

$$\begin{tikzcd} E_0 \arrow[r, dashed] \arrow[d, "\phi_B"'] & E_A \arrow[d, "\phi_B'"] \\ E_B & E_{BA} \end{tikzcd}$$

1.3 共通点.

E $\begin{cases} \text{ob}: E\text{の点} \\ \text{mor}: \text{スカラー倍} \end{cases}$

DLP

2つの対象 P, Q の対

射: $f: P \to Q$ を求めよ.

$$\begin{tikzcd} P \arrow[r, "{[3]}"] \arrow[d, "{[2]}"'] \arrow[dr, phantom, "\circlearrowright"] & 3P \arrow[d, dashed, "{[2]}"] \\ 2P \arrow[r, dashed, "{[3]}"'] & 6P \end{tikzcd}$$

$\mathcal{E}ll$: obj: 楕E

mor: Isogeny

$$\begin{tikzcd} E \arrow[r, "\phi_1"] \arrow[d, "\phi_2"'] \arrow[dr, phantom, "\circlearrowright"] & E_1 \arrow[d, "\phi_2'"] \\ E_2 \arrow[r, "\phi_1'"'] & E_{12} \end{tikzcd}$$

IP

2つの対象 E, F : given

射: $\phi: E \to F$ ..

1.4 相違点

Note

射 f の effective representation

$$(\mathrm{dom}(f), \alpha_f) \xmapsto{\text{poly}} \mathrm{cod}(f)$$

は情報 α_f.

Example 1

$[d]: P \longrightarrow dP$ の ef. rep.

整数 d のバイナリ

$(P, d) \xmapsto[\text{poly}]{} dP$.

Example 2

d-iso $\phi: E \longrightarrow F$ の ef. rep.

$G = \ker(\phi) \leq E[d]$ (の生成元)

$(E, G) \longmapsto F$

Vélu's formula により, $O(d)$ 時間かかり, 多項式では解けない.

d: smooth （つまり，$d = 2^a$ などのとき）

$$E_0 \underset{\substack{\phi_1 \\ \text{2-isog.}}}{\overset{O(2)}{\longrightarrow}} E_1 \underset{\phi_2}{\overset{O(2)}{\longrightarrow}} \cdots\cdots \underset{\substack{\phi_n \\ \text{2-isog}}}{\overset{O(2)}{\longrightarrow}} E_a \qquad \text{total で } O(a) = O(\log_2 d)$$

⇝ Non-smooth な degree の isogeny を計算したい!!!

§2 本題

Rand Isog Imgs.

2.1 アルゴリズムの概要

$E_0 / \mathbb{F}_{p^2}$: $y^2 = x^3 + x$ (super singular)
($p \equiv 3 \bmod 4$)

Input : $d \in \mathbb{Z}_{>0}$ (s.t.) $d < B$; $P_1, \cdots, P_k \in E_0$

Output : ランダムな d-isogeny $\phi : E_0 \longrightarrow F$ の codmain F ; $\phi(P_1), \cdots, \phi(P_k)$

2.2 Endomorphism

$E \longrightarrow E$ の isogeny or 0 射を E の Endomorphism という．その全体を $\mathrm{End}(E)$ とかく．
$\mathrm{End}(E)$ は和と合成で環．

Proposition

E : super singular ならば，$\mathrm{End}(E)$ は四元数代数の maximal order と同型．

$$\mathrm{End}(E_0) \simeq \underbrace{\mathbb{Z} \oplus \mathbb{Z}i \oplus \mathbb{Z}\frac{i+j}{2} \oplus \mathbb{Z}\frac{1+k}{2}}_{=: \mathcal{O}_0}, \text{ where } i^2 = -1,\ j^2 = -p,\ ij = -ji = k$$

$$\begin{aligned} \varepsilon : \mathrm{End}(E_0) &\longrightarrow \mathcal{O}_0 \\ [n] &\longmapsto n \\ [\eta : (x, y) \mapsto (-x, \sqrt{-1}y)] &\mapsto i \\ [\pi : (x, y) \mapsto (x^p, y^p)] &\mapsto j \end{aligned}$$

$\mathrm{Alg}: \mathrm{RepInt}(M) \longrightarrow \alpha$

Input : $M > p$

Output : $\alpha \in \mathrm{End}(E_0)$, $\deg(\alpha) = M$

Step1 : $z, w \in \mathbb{Z}$ を $z^2 + w^2 < \frac{M}{p}$ をみたすもの.

Step2 : $x^2 + y^2 = M' := M - p(z^2 + w^2)$ となる x, y をとる.

Step3 : $x + yi + zj + wk$ を返す.

$([x] + [y]\iota + [z]\pi + [w]\iota\circ\pi)$

$x^2 + y^2 + p(z^2 + w^2) = M$ が成立.

⟶ 好きな次数の $\alpha : E_0 \longrightarrow E_0$ が得られる.

2.3 高次元 isogeny の利用

Theorem [Kani '97]

$d_1, d_2 \in \mathbb{Z}_{>0}$ を互いに素とし, $D := d_1 + d_2$ とする.

$$\begin{tikzcd}
E \arrow[r, "\phi_1"] \arrow[d, "\phi_2"'] \arrow[dr, "\psi"] & E_1 \arrow[d, "\phi_2'"] \\
E_2 \arrow[r, "\phi_1'"'] & F
\end{tikzcd}$$

$\deg(\phi_1) = \deg(\phi_1') = d_1$

$\deg(\phi_2) = \deg(\phi_2') = d_2$

このとき,

$$\Phi := \begin{bmatrix} \phi_1 & -\hat{\phi}_2' \\ \phi_2 & \hat{\phi}_1' \end{bmatrix} : E \times F \longrightarrow E_1 \times E_2$$

は 2-dim principally polarized abelian varieties 間の D-isogeny である.

また,

$\ker(\Phi) = \{ (d_2 P, \psi(P)) \mid P \in E[D] \} \subseteq E \times F$.

で与えられる.

利用法

Note

2-dimでも, $\ker(\Phi)$ から Φ が一意的に定まる.

また, $\deg(\Phi) = D$ が smooth なら

$$(E \times F, \ker(\Phi)) \xmapsto{\text{poly}} (\Phi \text{ と } E_1 \times F_2)$$

特に $D = 2^{a}$ について高速.

d_1, d_2, E, F : given

$d_1 d_2$ - isog $\psi: E \longrightarrow F$ の $E[D]$ 上の表現 (2つの生成元の像とする) とする.

① $G = \{ (d_2 P, \psi(P)) \mid P \in E[D] \} \subseteq E \times F$ を求める.

② $(E \times F, G) \xmapsto{\text{poly.}} (\Phi, E_1 \times E_2)$

Φ から $\phi_1, \phi_2, \hat{\phi}_1, \hat{\phi}_2$, $E_1 \times E_2$ から E_1, E_2 が得られる.

2.4 アルゴリズムの構成

Setting :

$p = Df - 1$ (f : small, $D = 2^{a}$ で $Df - 1$ が素数)

$E_0 / \mathbb{F}_{p^2}$: $y^2 = x^3 + x$ より

$$|E_0(\mathbb{F}_{p^2})| = (p+1)^2 = (2^a f)^2$$

より, $E_0[2^a] \subseteq E_0(\mathbb{F}_{p^2})$.

Rand Isog Img :

Input : $d \in \mathbb{Z}$, $f < d = 2^a - f$, d : odd

Output : random d-isogeny $\phi: E_0 \to F$ の F.

$$\begin{tikzcd} E_0 \arrow[r, "\phi"] \arrow[d] \arrow[dr, "\alpha"] & F \arrow[d] \\ F' \arrow[r] & E_0 \end{tikzcd}$$

① $\alpha \longleftarrow \mathrm{RepInt}(d(2^a - d))$

② $G \longleftarrow \{ ((2^a - d)P, \alpha(P)) \mid P \in E_0[2^a] \} \subseteq E_0 \times E_0$

③ $\ker(\Phi) = G$ なる $\Phi: E_0 \times E_0 \longrightarrow F \times F'$ を計算 (2-dim, 2^a-isogeny)

④ Φ の (1,1) 成分 $\phi: E_0 \to F$ を返す.