02

아이소제니와 Velu 의 공식

목차

[1] 아이소제니

[2] Velu의 공식

1

아이소제니

Isogeny

Isogeny $\boldsymbol{\phi}: \boldsymbol{E_1 \rightarrow E_2}$

모든곳에서 정의되는 유리함수

- Non-constant morphism that maps the distinguish point of E_1 to the distinguished point of E_2

Isogeny

Standard form of ϕ

$$\boldsymbol{\phi(x,y) = \left(\frac{u(x)}{v(x)}, \frac{s(x)}{t(x)}y\right)}$$

- Where $\left(u(x), v(x)\right) = 1, \left(s(x), t(x)\right) = 1$
- $\deg \phi = \max\{\deg u, \deg v\}$

Isogeny

Example $\boldsymbol{F_{109}}$

- $E_0: y^2 = x^3 + 2x + 2 \xrightarrow{\boldsymbol{\phi}} E_1: y^2 = x^3 + 34x + 45$

$$\boldsymbol{\phi(x,y) = \left(\frac{x^3 + 20x^2 + 50x + 6}{x^2 + 20x + 100}, \frac{x^3 + 30x^2 + 23x + 52}{x^3 + 30x^2 + 82x + 19}y\right)}$$

Isogeny

Some facts

- Isogeny ≠ Isomorphism
  - E_0, E_1 is isomorphic if there exists an isogeny $\phi_1: E_0 \to E_1$ and $\phi_2: E_1 \to E_0$ such that $\phi_1 \circ \phi_2$=identity
  - Example by Cohen and Frey

$$\boldsymbol{\phi(x,y) = \left(\frac{x^2+301x+527}{x+301}, \frac{x^2+602x+1942}{x^2+602x\_466}y\right)}$$

$$\boxed{E_0}: y^2 = x^3 + 1132x + 278 \xrightarrow{\boldsymbol{\phi}} \boxed{E_1}: y^2 = x^3 + 500x + 1005$$

Cyclic group

Not a cyclic group

Isogeny

Separable isogeny

$$\phi\,(x, y\,) = \left(\frac{u(x)}{v(x)}, \frac{s(x)}{t(x)}y\right)$$

- Separable if $\left(\frac{u(x)}{v(x)}\right)' \neq 0$

Isogeny

Separable isogeny

- ϕ 가 d 차인 경우
  - $d = p_0^{e_0} p_1^{e_1} \cdots p_n^{e_n}$
  - $\phi = \underbrace{\phi_{p_0} \circ \cdots \circ \phi_{p_0}}_{e_0\text{-times}} \circ \cdots \circ \underbrace{\phi_{p_n} \circ \cdots \circ \phi_{p_n}}_{e_1\text{-times}}$

Isogeny

Separable isogeny

- ϕ 가 d 차인 경우
  - $d = p_0^{e_0} p_1^{e_1} \cdots p_n^{e_n}$
  - $\phi = \underbrace{\phi_{p_0} \circ \cdots \circ \phi_{p_0}}_{e_0\text{-times}} \circ \cdots \circ \underbrace{\phi_{p_n} \circ \cdots \circ \phi_{p_n}}_{e_1\text{-times}}$

- 주어진 타원곡선 $E(\bar{K})$ 의 유한 subgroup $G \subset E(\bar{K})$ 를 kernel로 하는 isogeny ϕ 를 만들 수 있다 (Velu)
- Order of such isogeny $\phi = ord\ G$

2

Velu의 공식

Velu's Formula

Velu Formula

- 주어진 타원곡선 $E(\overline{K})$의 유한 subgroup $G \subset E(\overline{K})$ 를 kernel로 하는 isogeny ϕ 를 만들 수 있다
- Order of such isogeny $\phi = ord\ G$
- Complexity: $O(n), n = ord\ G$

모든 커널의 원소와 연산해야 함

$$\phi(P) = \left(x_P + \sum_{Q \in F - \{\infty\}} (x_{P+Q} - x_Q), y_P + \sum_{Q \in F - \{\infty\}} (y_{P+Q} - y_Q) \right).$$

Kernel

Velu's Formula

Velu Formula : Algorithm

- Input : Curve of Weierstrass form E, and set of points of finite subgroup of $E(\overline{K})$
- Output : Codomain curve, coordinate map

$$\boldsymbol{E: y^2 + a_1 xy + a_3 y = x^3 + a_2 x^2 + a_4 x + a_6}$$

Velu's Formula

Velu Formula : Algorithm

- STEP 1 : Partition the set of points in C
  - 무한 원점 제거
  - C_2 : set of 2-torsion point , $R: C - C_2$
  - R 을 R_+ 와 R_- 로 분해
    - $P \in R_+$ then $-P \in R_-$
  - $S = R_+ \cup C_2$

Velu’s Formula

Velu Formula : Algorithm

- STEP 1 : Partition the set of points in C
  - 무한 원점 제거
  - C_2 : set of 2-torsion point , R: $C - C_2$
  - R 을 R_+ 와 R_- 로 분해
    - $P \in R_+$ then $-P \in R_-$
  - $S = R_+ \cup C_2$

- Example
  - $C = \{O, P\}, P$: 2-torsion point
  - $S = C_2 = \{P\}$

Velu's Formula

Velu Formula : Algorithm

- STEP 1 : Partition the set of points in C
  - 무한 원점 제거
  - C_2 : set of 2-torsion point , $R: C - C_2$
  - R 을 R_+ 와 R_- 로 분해
    - $P \in R_+$ then $-P \in R_-$
  - $S = R_+ \cup C_2$

- Example
  - $C = \{O, P, 2P\}, P$: 3-torsion point
  - NOTE : $3P = O$ so that $2P = -P$
  - $C_2 = \emptyset$
  - $R_+ = \{P\}, R_- = \{-P\}$

Velu's Formula

Velu Formula : Algorithm

- STEP 2 : Compute the following for $Q \in S$

$$g_Q^x = 3x_Q^2 + 2a_2x_Q + a_4 - a_1y_Q$$

$$g_Q^y = -2y_Q - a_1x_Q - a_3$$

$$v_Q = \begin{cases} g_Q^x & \text{if } 2Q = \infty \\ 2g_Q^x - a_1g_Q^y & \text{otherwise} \end{cases}$$

$$u_Q = (g_Q^y)^2$$

$$v = \sum_{Q \in S} v_Q, \quad w = \sum_{Q \in S} (u_Q + x_Qv_Q)$$

Velu's Formula

Velu Formula : Algorithm

- STEP 3 : Compute the image curve coefficient

$$A_1 = a_1,\ A_2 = a_2,\ A_3 = a_3,$$
$$A_4 = a_4 - 5v,\ A_6 = a_6 - (a_1^2 + 4a_2)v - 7w.$$

$$E': y^2 + A_1xy + A_3y = x^3 + A_2x^2 + A_4x + A_6$$

Velu's Formula

Velu Formula : Algorithm

- STEP 4 : Compute the coordinate maps

$$\begin{array}{ccc} E & \xrightarrow{\phi} & E' \\ (x, y) & & (\alpha, \beta) \end{array}$$

$$\alpha = x + \sum_{Q \in S} \left(\frac{v_Q}{x - x_Q} - \frac{u_Q}{(x - x_Q)^2} \right)$$

$$\beta = y - \sum_{Q \in S} \left(u_Q \frac{2y + a_1 x + a_3}{(x - x_Q)^3} + v_Q \frac{a_1 (x - x_Q) + y - y_Q}{(x - x_Q)^2} + \frac{a_1 u_Q = g_Q^x g_Q^y}{(x - x_Q)^2} \right)$$

Velu's Formula

Velu Formula : Example

- 2-isogeny on short Weierstrass curve

$$\boldsymbol{E: y^2 = x^3 + Ax + B}$$

$\boldsymbol{C = \{O, P\}}$ **($\boldsymbol{P = (x_0, 0)}$: 2-torsion point)**

- **STEP 1 : Partition the points**
  - $C = \{O, P\}, P$: 2-torsion point
  - $S = C_2 = \{P\}$

Velu's Formula

Velu Formula : Example

- 2−isogeny on short Weierstrass curve

$$\boldsymbol{E}: \boldsymbol{y}^2 = \boldsymbol{x}^3 + \boldsymbol{A}\boldsymbol{x} + \boldsymbol{B}$$

$\boldsymbol{C} = \{\boldsymbol{O}, \boldsymbol{P}\}$ ($\boldsymbol{P} = (\boldsymbol{x}_0, \boldsymbol{0})$: 2-torsion point)

- STEP 2 : Compute

$$g_Q^x = 3x_0^2 + A$$
$$g_Q^y = 0$$
$$v_Q = 3x_0^2 + A$$
$$u_Q = 0$$
$$v = 3x_0^2 + A$$
$$w = x_0(3x_0^2 + A)$$

Velu's Formula

Velu Formula : Example

- 2-isogeny on short Weierstrass curve

$$E: y^2 = x^3 + Ax + B$$

$$C = \{O, P\}$$ ($P = (x_0, 0)$: 2-torsion point)

- STEP 3 : Compute the image curve

$$E': y^2 = x^3 + \left(A - 5(3x_0^2 + A)\right)x - 7x_0(3x_0^2 + A)$$

Velu's Formula

Velu Formula : Example

- 2−isogeny on short Weierstrass curve

$$\boldsymbol{E: y^2 = x^3 + Ax + B}$$

$\boldsymbol{C = \{O, P\}}$ $(\boldsymbol{P = (x_0, 0)}$: 2-torsion point)

- STEP 4 : Compute the coordinate maps

$$\phi(x,y) = \left(x + \frac{3x_0^2 + A}{x - x_0}, y - (3x_0^2 + A)\frac{y}{(x - x_0)^2}\right)$$

Velu's Formula

Lessons learned

- Velu 공식에 의해 임의의 subgroup을 커널로 하는 아이소제니 생성 가능
- 함수값 연산하기 위해 커널의 모든 원소와 타원곡선 연산 수행해야함
- 커널 order 증가 ➔ 연산량 증가
- 효율성을 위해 암호에서는 cyclic subgroup 이용