아이소제니 기반 암호와 SIDH

IT정보공학과 신명수

2022 암호분석경진대회
7번 문제

양자 내성 암호 중 isogeny 기반 암호는 유한체 위의 두 타원곡선 E, E' 사이의 isogeny를 연산하는 어려움에 기반을 두어, isogeny $\phi : E \to E'$에 대해 ϕ를 비밀값으로 한다. 한편, Velu의 공식을 이용해 $\ker\phi$를 이용해 isogeny를 연산할 수 있으므로 $\ker\phi$ 도 비밀로 하며, 일반적인 구현에서는 isogeny를 저장하는 대신 $\ker\phi$를 저장한다.

한편, n차 isogeny ϕ에 대해서 dual isogeny는 차수가 같고 $\hat{\phi} \circ \phi = [n]$ 를 만족하는 isogeny $\hat{\phi}: E' \to E$ 이다. 여기에서 $[n]$은 multiplication-by-n map을 의미한다. 마찬가지로 dual isogeny를 알면 해당 isogeny를 복원할 수 있으므로 dual isogeny도 isogeny와 동일하게 비밀 값으로 한다.

목차

1. 군 (Group)
2. 타원곡선암호 (ECC)
3. Isogeny
4. Velu 공식
5. SIDH

1. 군 (Group)

- (1). Modular Arithmetic
- (2). Group
- (3). Cyclic Group

1-(1). Modular Arithmetic

정수 m, a, b $(m \geq 2)$ 가 존재한다.

a 와 b 의 차가 m으로 나누어 떨어지면, a와 b는 modular m으로 합동이다.

$$m \mid (a - b) <=> a \equiv b \ (mod\ m)$$

Modular m ($\equiv$ $(mod\ m)$) 이 정수범위에서 갖는 성질.

1. Reflexivity : $a \equiv a \ (mod\ m)$
2. Symmetry : $a \equiv b \ (mod\ m) \Rightarrow b \equiv a(mod\ m)$
3. Transitivity : $a \equiv b \ (mod\ m)$ and b $\equiv c \ (mod\ m) \Rightarrow a \equiv c \ (mod\ m)$

1-(2). Group

- 이항 연산이 하나 정의된 집합.

1. Closure $a + b = c \quad a, b, c \in G$
2. Associativity $(a + b) + c = a + (b + c) \quad a, b, c \in G$
3. Identity element $a + I = a \quad a, I \in G$
4. Inverse element $a + a^{-1} = I \quad a, a^{-1} \in G$

Commutativity를 만족하면 -> Abelian group $a + b = b + a \quad a, b \in G$

1-(3). Cyclic Group

- 한 원소(generator)로 생성될 수 있는 군을 말한다.

덧셈연산으로 정의된 군

$$< g > = \{ng : n \in \mathbb{Z}\}$$
$$= \{0, g, 2g, 3g, \dots (n-1)g\}, g \in G$$

곱셈연산으로 정의된 군

$$< g > = \{g^n : n \in \mathbb{Z}\}$$
$$= \{1, g^1, g^2, g^3, \dots, g^{n-1}\}, g \in G$$

군의 차수는 원소의 개수를 말한다.

2. 타원곡선암호(ECC)

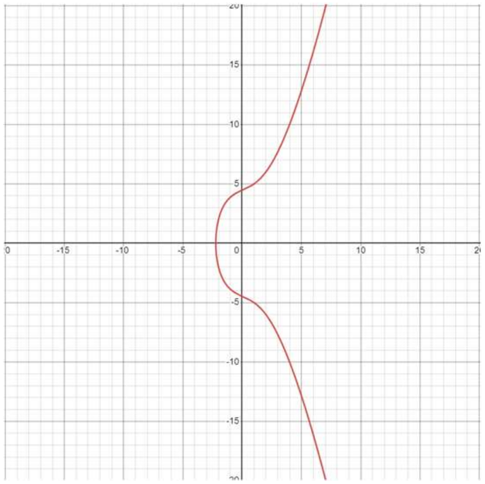
- (1). 타원곡선 (Elliptic Curve)
- (2). operations on Elliptic Curve
- (3). 타원곡선 암호

2-(1). 타원곡선(Elliptic Curve)

- 유한체 k상에서 정의된 타원곡선 E 는 다음과 같이 정의할 수 있다.

$$E = \{(x, y) \in k : y^2 = x^3 + Ax + B\} \cup \{\infty\}$$

$$E(k) = \{(x, y) \in E : x, y \in k\}$$

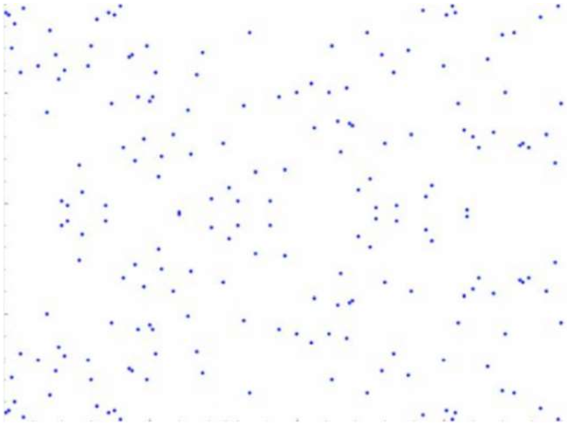


Example. $y^2 = x^3 + 4x + 20$

2-(1). 타원곡선(Elliptic Curve)

- 유한체 k상에서 정의된 타원곡선 E 는 다음과 같이 정의할 수 있다.

$$E = \{(x, y) \in k : y^2 = x^3 + Ax + B\} \cup \{\infty\}$$



$$E(k) = \{(x, y) \in E : x, y \in k\}$$

Example. $y^2 = x^3 + 4x + 20 \ over \ F(191)$

2-(1). 타원곡선(Elliptic Curve)

- Forms of Elliptic Curve
  - 타원곡선의 종류는 여러가지가 있다.
  - 타원곡선의 종류를 판가름하는 것은 식의 형태이다.
  - 곡선이 달라지면 타원 곡선 위에서 정의되는 연산 또한 달라진다.

2-(1). 타원곡선(Elliptic Curve)

- Forms of Elliptic Curve
  - Weierstrass Curve $\mathrm{E}: y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$
  - Short Weierstrass Curve $\mathrm{E}: y^2 = x^3 + Ax + B$
  - Montgomery Curve $\mathrm{E}: By^2 = x^3 + Ax + x$
  - (twisted) Edwards Curve $\mathrm{E}: ax^2 + y^2 = 1 + dx^2y^2$

2-(1). 타원곡선(Elliptic Curve)

- 암호에서 사용되는 타원곡선 E는 미분가능한 사영 평면 곡선이다.

Singularity Form

$$4a^3 + 27b^2 = 0$$

$4a^3 + 27b^2 = 0$ 을 만족하는 singularity form은 첨점으로 인해 미분이 불가능함.

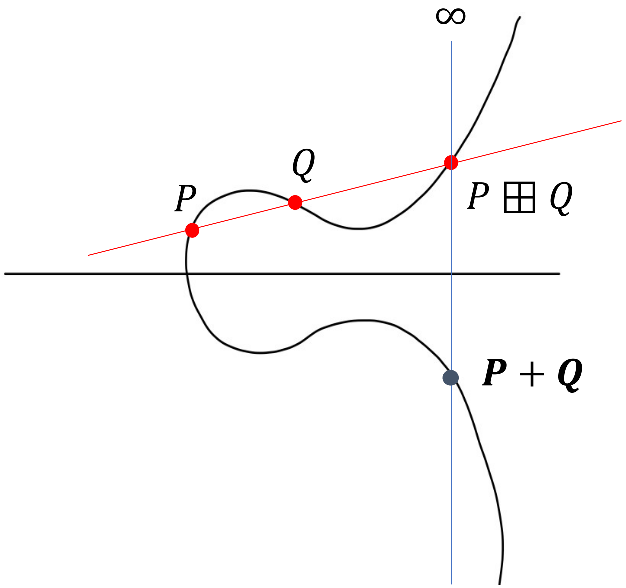
2-(2). Operations on Elliptic Curve

- Point Addition

- 무한원점 ∞은 E에서 접선이 삼중근을 가지는 점이다. (inflection point)
- E 위의 점 P, Q지나는 직선 l을 그었을 때,
  나머지 한 점을 $P \boxplus Q$라 하자.

$$\boldsymbol{P + Q = \infty \boxplus (P \boxplus Q)}$$

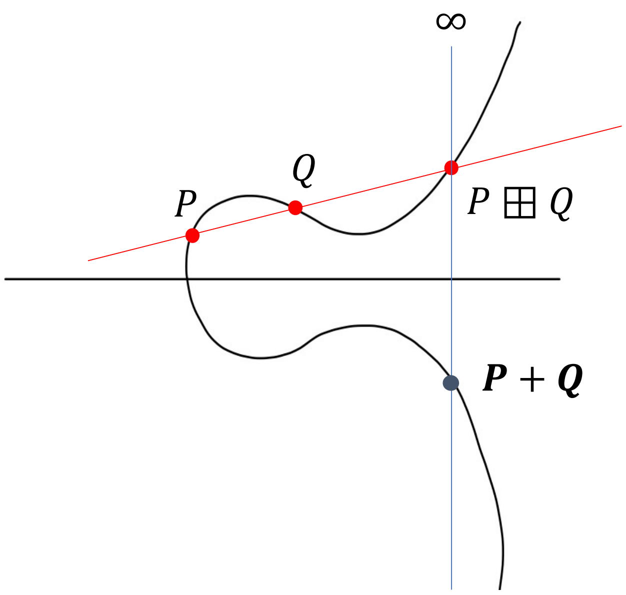
- 무한원점은 해당 연산에서 항등원이다.



2-(2). Operations on Elliptic Curve

- 타원곡선 E는 이 연산에서 abelian group 이다.

1. $P + Q \in E \ (closed)$
2. $(P + Q) + R = P + (Q + R)$
3. $\infty + P = P + \infty = P(Identity\ element\ \infty)$
4. $P + (-p) = \infty$
5. $P + Q = Q + P$



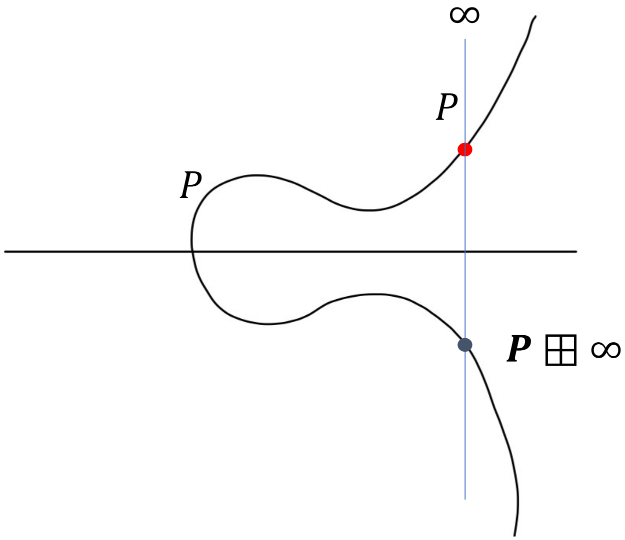
2-(2). Operations on Elliptic Curve

- 타원곡선 E는 이 연산에서 abelian group 이다.

3. $\infty + P = P + \infty = P(Identity\ element\ \infty)$

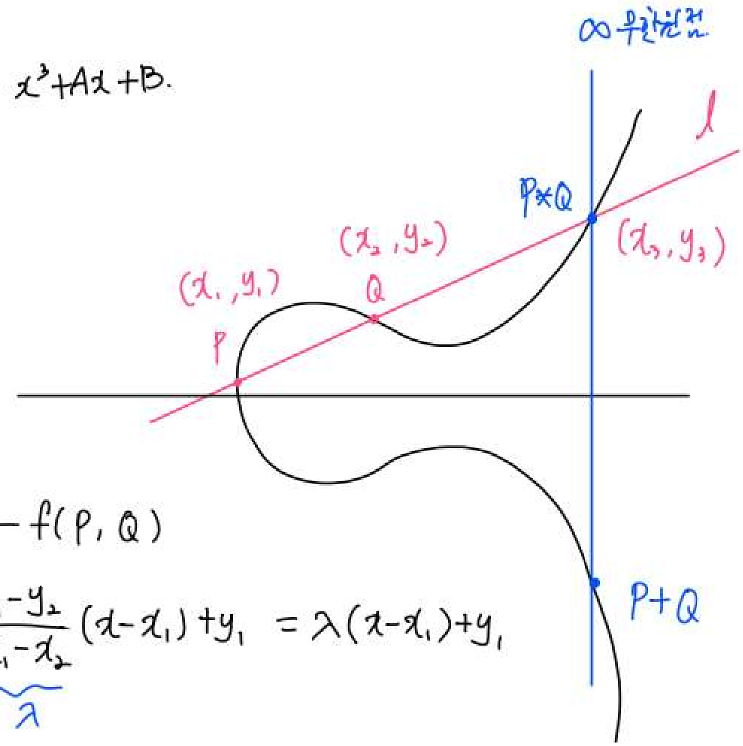
-> $\infty + P = \infty \boxplus (\infty \boxplus P)$

4. $P + (-p) = \infty$



2-(2). Operations on Elliptic Curve

$y^2 = x^3 + Ax + B.$



$P+Q \leftarrow f(P, Q)$

$$y = \underbrace{\frac{y_1 - y_2}{x_1 - x_2}}_{\lambda}(x - x_1) + y_1 = \lambda(x - x_1) + y_1$$

2-(2). Operations on Elliptic Curve

$$y^2 = x^3 + Ax + B$$
$$y = \lambda(x - x_1) + y_1$$

두 식을 연립하면,

$$(\lambda(x - x_1) + y_1)^2 = x^3 + Ax + B$$
$$\rightarrow x^3 - \lambda^2 x + \cdots = 0$$

근과 계수와의 관계에 따라 $x_1 + x_2 + x_3 = \lambda^2$ 을 만족한다.

$$x_3 = \lambda^2 - x_1 - x_2$$

2-(2). Operations on Elliptic Curve

$$y = \lambda(x - x_1) + y_1$$

식에 $x_3 = \lambda^2 - x_1 - x_2$ 을 대입하면,

$$y_3 = \lambda(x_3 - x_1) + y_1$$

$$\therefore P \boxplus Q = (\lambda^2 - x_1 - x_2, \lambda(x_3 - x_1) + y_1)$$

2-(2). Operations on Elliptic Curve

- Point Addition을 통해,
  어떤 점 P를 generator로 하는 타원곡선 group을 만들 수 있다.

- 이 group은 Cyclic subgroup 중 하나이다.

- $< P > = \{O, P, 2P, 3P, \dots \dots, (n-1)P\}, order\ of < P > is\ n$
- Order는 P를 더했을 때 무한원점이 나오는 최소 횟수를 말한다.

2-(3). 타원곡선암호(ECC)

- Discrete Logarithm Problem for Elliptic Curves (ECDLP)

주어진 타원곡선 E와 타원곡선 위의 점 P, Q가 주어졌을 때,
다음을 만족하는 정수 d를 찾는 문제.

$$dP = Q$$

2-(3). 타원곡선암호(ECC)

1980년대 중반 Miller와 Koblitz가 각각 독립적으로 타원곡선을 암호에 적용.

2000년도에 FIPS 186-2에 ECC가 표준으로 채택됨.

초반에는 RSA 암호보다 느렸으나, 점차 속도가 향상되었음.

ECDLP의 어려움에 기반함.

- 현재 타원곡선암호는 RSA보다 키 사이즈도 작고, 속도도 빠르기 때문에 IoT 환경에 적합한 암호로 평가받는다.

2-(3). 타원곡선암호(ECC)

- ECDH (Elliptic Curve Diffie-Hellman)

Alice		Bob
Choose a secret n_A		Choose a secret n_B
Compute $Q_A = [n_A]P$	$\xrightarrow{Q_A}$	Compute $Q_B = [n_B]P$
	$\xleftarrow{Q_B}$	
Compute $[n_A]Q_B$		Compute $[n_B]Q_A$

Shared Secret $\boldsymbol{[n_A]Q_B = [n_A n_B]P = [n_B]Q_A}$

3. Isogeny

3. Isogeny

- Isogeny : 두 타원곡선 사이를 연결하는 함수.
  Non-constant morphism that maps the distinguish point of E_1 to the distinguished point of E_2

- 일반적인 Isogeny 함수의 형태는 다음과 같다.

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

$$where\ gcd\big(u(x), v(x)\big) = 1, \qquad gcd\big(s(x), t(x)\big) = 1$$

3. Isogeny

- Example of F_{109}.

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

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

3. Isogeny

- Isogeny ≠ Isomorphism
- E_0에서 E_1 로 Isomorphism이 존재하면, Isogeny가 존재한다.($\phi: E_0 \to E_1$)
  하지만 Isogeny가 존재한다고 해서 Isomorphism이 존재하지 않는다.
  (A에서 B로 Isomorphism이 존재한다 -> A의 구조를 동일하게 B로 가져갈 수 있다.)

- Example.

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

$$\phi(x,y) = \left(\frac{x^3 + 301x + 527}{x + 301}, \frac{x^2 + 602x + 1942}{x^2 + 602x + 466} y\right)$$

3. Isogeny

- Separable Isogeny : $\left(\frac{u(x)}{v(x)}\right)' \neq 0$인 Isogeny 함수.

$$\phi(x,y) = \left(\frac{u(x)}{v(x)}, \frac{s(x)}{t(x)}y\right), separable\ if \left(\frac{u(x)}{v(x)}\right)' \neq 0$$

구현을 할 때는 Separable Isogeny를 사용한다.

$\phi(x,y)$가 d차일 때(d는 합성수), d를 쪼개서 Isogeny연산을 사용할 수 있기 때문.

3. Isogeny

- 구현을 할 때는 Separable Isogeny를 사용한다.

$\phi(x, y)$가 d차일 때(d는 합성수), d를 쪼개서 Isogeny연산을 사용할 수 있기 때문.

- Example.

$\phi(x, y)$가 6차일 때, 2차 Isogeny와 3차 Isogeny의 합성으로 6차 Isogeny를 연산할 수 있다.

4. Velu 공식

4. Velu 공식

- 주어진 타원곡선 $E(\bar{K})$의 유한 subgroup $\mathrm{G} \subset E(\bar{K})$를 **kernel**로 하는 Isogeny ϕ를 만들 수 있다.
- Order of such Isogeny $\phi = ord\ \mathrm{G}$
- Complexity: $O(n), n = ord\ G$
- Kernel $G : \phi(g) = 0, g \in G$
  커널 내의 원소와 연산을 했을 때, 무한원점(항등원)으로 보내게 되는 원소의 집합.

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

커널 G의 모든 원소와 연산해야 한다.

4. Velu 공식

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

subgroup C는 커널로 하고싶은 타원곡선의 유한부분군을 말한다.

$$\mathrm{E}: y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

4. Velu 공식 - algorithm

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

- Example1
  - $C = \{0, P\}, P$:2-torsion point
  - $S = C_2 = \{P\}$

- Example2
  - $C = \{0, P, 2P\}, P$: 3-torsion point
  - Note : $3P = 0$ *so that* $2P = -P$
  - $C_2 = \emptyset$
  - $R_+ = \{P\}, R_- = \{-P\}$
  - $S = \{P\}$

4. Velu 공식 - algorithm

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

$$g_Q^x = 3x_Q^2 + 2a_2 x_Q + a_4 - a_1 y_Q$$
$$g_Q^y = -2y_Q - a_1 x_Q - a_3$$
$$v_Q = \begin{cases} g_Q^x, & if\ 2Q = \infty \\ 2g_Q^x - a_1 g_Q^y, & otherwise \end{cases}$$
$$u_Q = (g_Q^y)^2$$
$$v = \sum_{Q \in S} v_Q, \qquad \omega = \sum_{Q \in S} (u_Q + x_Q v_Q)$$

4. Velu 공식 - algorithm

- Step 3 : Compute the image curve coefficient

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

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

4. Velu 공식 - algorithm

- Step 4 : Compute the coordinate maps

$$\boldsymbol{E} \xrightarrow{\boldsymbol{\phi}} \boldsymbol{E'}$$

$$(x, y) \quad (\alpha, \beta)$$

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

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

4. Velu 공식

- Velu 공식에 의해 임의의 subgroup을 커널로 하는 Isogeny 생성 가능
- 함수값 연산하기 위해 커널의 모든 원소와 타원곡선 연산 수행해야함.
- 커널의 order가 증가하면 연산량도 증가한다.
- 효율성을 위해 암호에서는 cyclic subgroup를 이용한다.
  Generator P만 잡으면 점 연산을 통해 모든 원소를 알 수 있다.
  커널의 order가 작은 것을 사용한다.

5. SIDH

(1). 아이소제니 기반 암호 소개

(2). SIDH

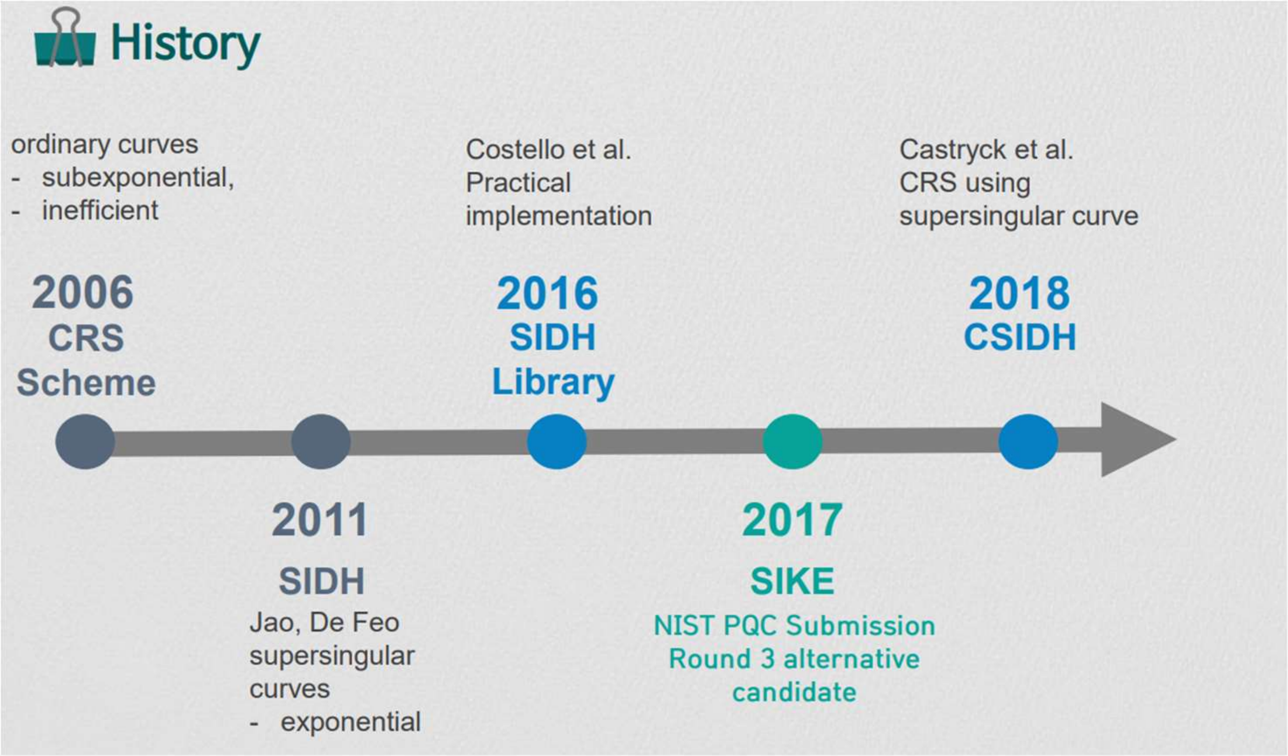
5-(1). 아이소제니 기반 암호 소개

- 아이소제니 기반 암호는 2006년 Conveignes, Rostovtsev, Stolbunov에 의해 처음으로 제안(CRS).
- 초반에 제안된 Isogeny 기반 암호는 Ordinary Curve를 사용한 DH기반 암호.

5-(1). 아이소제니 기반 암호 소개

- Ordinary curve의 endomorphism ring의 commutative(가환성) 성질을 활용한 Child등의 공격으로 sub-exponential complexity를 가지게 됨.
- endomorphism ring : 타원곡선이 존재할 때, 자기자신으로 가는 Isogeny집합.
- 매우 느린 속도로 효율성이 낮음. -> 처음에는 별로 주목받지 못했다.

5-(1). 아이소제니 기반 암호 소개



5-(1). 아이소제니 기반 암호 소개

- Isogeny Problem
  - Let E_1, E_2 be elliptic curves over F_q
  - Find an isogeny ϕ such that $\phi: E_1 \to E_2$

- Ramanujan Graph
  - Spectral gap 이 최대인 regular graph
  - Regular graph : 그래프의 모든 vertex가 동일한 degree를 갖는다.

5-(1). 아이소제니 기반 암호 소개

- Ramanujan Graph
  - Spectral gap 이 최대인 regular graph
  - Regular graph : 그래프의 모든 vertex가 동일한 degree를 갖는다.
  - Isogeny graph는 Ramanujan graph의 한 종류로, 가장 많이 퍼지는 그래프이다.
  - 연속된 $l - isojeny$ $\rightarrow (l+1)$가지 neighbor 존재함.

5-(1). 아이소제니 기반 암호 소개

- 특징
  - Velu formula : 타원곡선과 subgroup 이 주어지면 isogeny 연산이 가능하다.
  - 공개정보 : 두 타원곡선
  - 비밀정보 : Kernel (subgroup) -> (isogeny)
  - 비밀정보를 가진 사용자는 Velu 공식으로 isogeny 연산 가능.

5-(1). 아이소제니 기반 암호 소개

	SIDH	ECC
Prime	$p = 2^{e_A}3^{e_B} - 1$	$p = 2^{256} - 2^{224} + 2^{192} + 2^{96} + 1$
Field	F_{p^2}	F_p
Curve	Supersingular elliptic curve	Ordinary curve
Order of a curve		Near prime
Security	Hardness of finding isogeny	Hardness of solving ECDLP
Private key	Isogeny (kernel)	d

5-(2). SIDH

- Singularity Isogeny Diffie-Helman

Singularity Form

$4a^3 + 27b^2 = 0$

5-(2). SIDH

1. 타원곡선을 정의할 유한체를 정의한다.

$$p = l_A^{e_A} l_B^{e_B} f \pm 1, \qquad E \in F_{p^2}$$

- $l_A^{e_A}$와$l_B^{e_B}$는 서로소이고 아이소제니 차수와 연관있기 때문에 2와 3일 사용.

2. 타원곡선을 정의한다.

Alice $\quad E[l_A^{e_A}] =< P_A, Q_A >$

Bob $\quad E[l_B^{e_B}] =< P_B, Q_B >$

5-(2). SIDH

3. Generator를 이용해서 비밀정보인 커널을 생성한다.

$$ker\phi_A = < P_A + s_A Q_A >$$

$$ker\phi_B = < P_B + s_B Q_B >$$

4. 커널이 정해지면 Velu 공식을 통해 아이소제니를 결정할 수 있다.

5-(2). SIDH

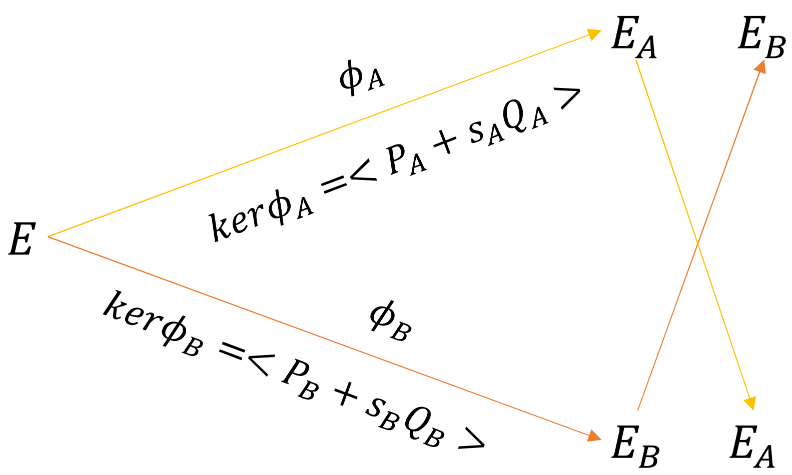
Alice : $E[l_A^{e_A}] =< P_A, Q_A >$

$$\begin{array}{ccc} & & E_A \\ & \nearrow^{\phi_A}_{ker\phi_A =< P_A + s_A Q_A >} & \\ E & & \\ & \searrow^{\phi_B}_{ker\phi_B =< P_B + s_B Q_B >} & \\ & & E_B \end{array}$$

Bob : $E[l_B^{e_B}] =< P_B, Q_B >$

5-(2). SIDH

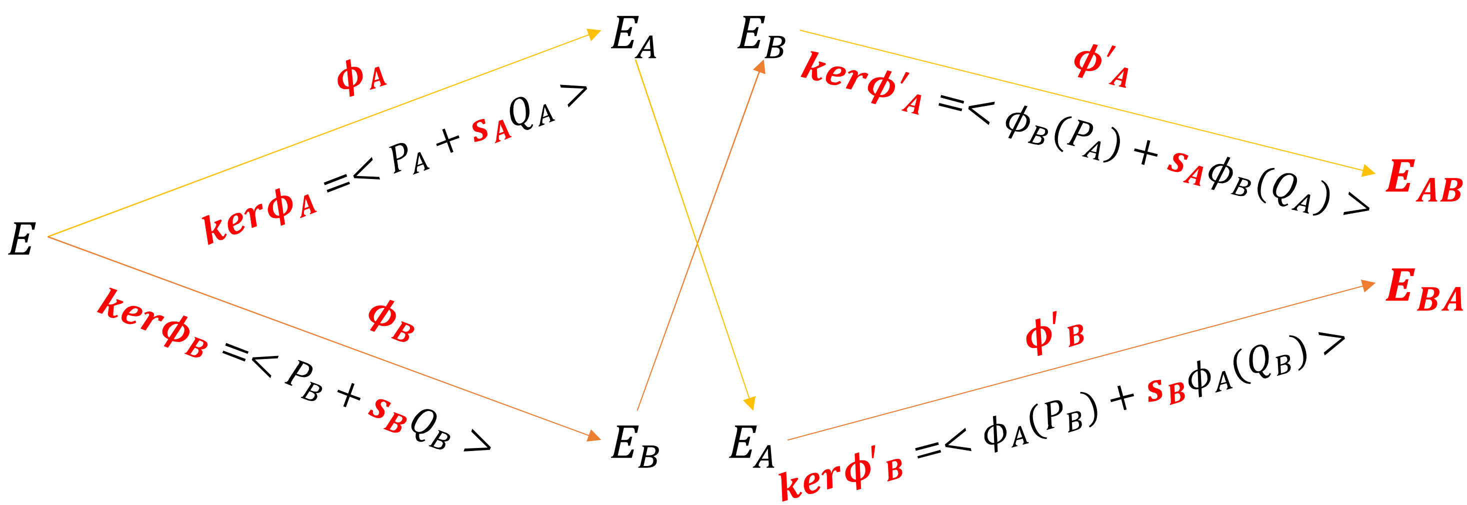
Alice : $E[l_A^{e_A}] =< P_A, Q_A >$



Bob : $E[l_B^{e_B}] =< P_B, Q_B >$

5-(2). SIDH

Alice : $E[l_A^{e_A}] =< P_A, Q_A >$



Bob : $E[l_B^{e_B}] =< P_B, Q_B >$

$j\_invarient(E_{AB}) = j\_invarient(E_{BA})$

5-(2). SIDH

Alice | **Bob**

Public curve : E

Alice	Bob
Choose a secret : m_A, n_A	Choose a secret : m_B, n_B
$R_A = m_A P_A + n_A Q_A$	$R_B = m_B P_B + n_B Q_B$
Compute $\phi_A(P_B), \phi_A(Q_B)$	Compute $\phi_B(P_A), \phi_B(Q_A)$
Compute $\phi_A(E) = E_A$	Compute $\phi_B(E) = E_B$

$$\xrightarrow{E_A,\ \phi_A(P_B),\ \phi_A(Q_B)}$$

$$\xleftarrow{E_B,\ \phi_B(P_A),\ \phi_B(Q_A)}$$

Alice	Bob
Compute: $m_A \phi_B(P_A) + n_A \phi_B(Q_A)$	Compute: $m_B \phi_A(P_B) + n_B \phi_A(Q_B)$
Compute: $\phi'_A(E_B) = E_{AB}$	Compute: $\phi'_B(E_A) = E_{BA}$

Shared Secret $j(E_{AB}) = j(E_{BA})$

5-(2). SIDH

- 장점
  - 다른 PQC에 비해 키 사이즈가 작다.
  - 개인키는 커널에 대한 난수 값을 개인키로 하기 때문에 키 사이즈가 상당히 작다.
  - 다른 PQC 암호는 새로운 기반 문제 또는 구조를 가지고 암호를 설계되었지만 SIDH는 상대적으로 익숙한 타원곡선을 사용한다.

- 단점
  - 다른 PQC에 비해 느리다.
  - P의 형태가 400bit~700bit 정도이다.