01

타원곡선과
타원곡선 기반 암호

목차

1

타원곡선

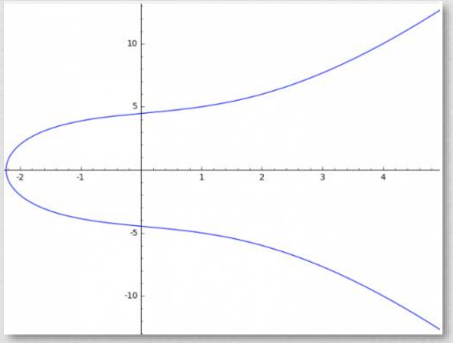
1) 타원곡선 정의
2) 타원곡선 연산

Elliptic Curve

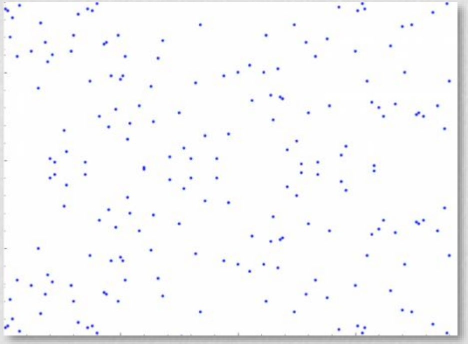
Elliptic Curve over K

- Smooth projective curve of genus 1 with a distinguished point
- 모든 타원곡선은 다음과 같은 형태로 나타낼 수 있음

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



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



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

Elliptic Curve

Forms of elliptic curve

- Weierstrass curve

$$E: y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

- Short Weierstrass curve

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

- Montgomery curve

$$E: By^2 = x^3 + Ax^2 + x$$

- (twisted) Edwards curves

$$E: ax^2 + y^2 = 1 + dx^2y^2$$

Elliptic Curve

Operations on Elliptic curves

- Point addition

$E/K : y^2 = x^3 + Ax + B \text{ , } char(K) \neq 2, 3$

Let $P = (x_1, y_1), Q = (x_2, y_2) \in E$

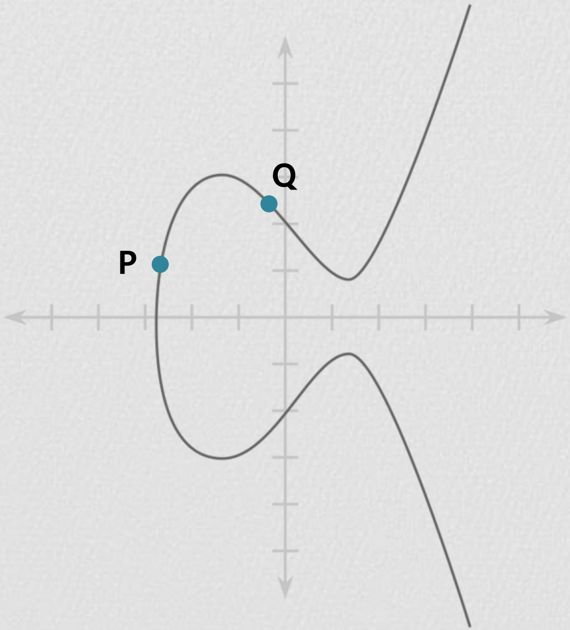
If $P \neq -Q = (x_2, -y_2)$ then

$$P + Q = \left(\lambda^2 - x_1 - x_2, \lambda(x_1 - x_3) - y_1\right) \text{ with } \lambda = \begin{cases} \frac{y_1 - y_2}{x_1 - x_2} & \text{If } P \neq Q \\ \frac{3x_1^2 + A}{2y_1} & \text{If } P = Q \end{cases}$$

Elliptic Curve

Operations on Elliptic curves

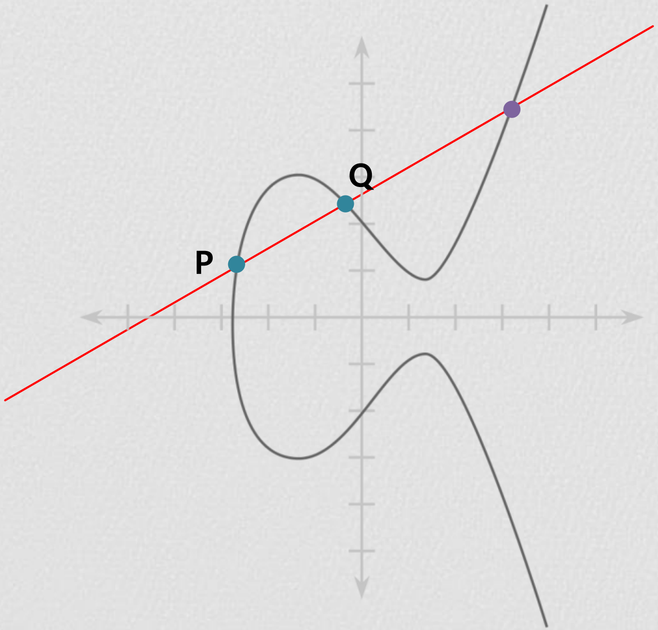
- Point addition $(P \neq Q)$



Elliptic Curve

Operations on Elliptic curves

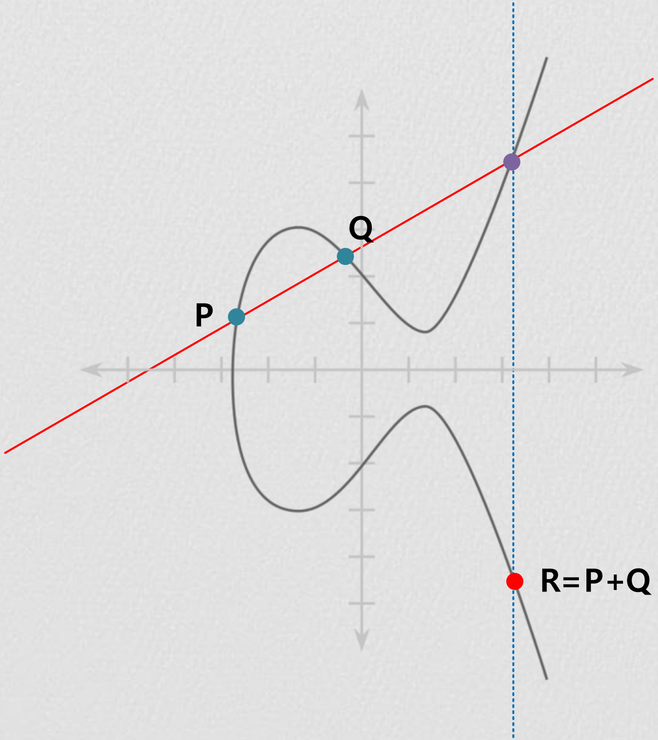
- Point addition $(P \neq Q)$



Elliptic Curve

Operations on Elliptic curves

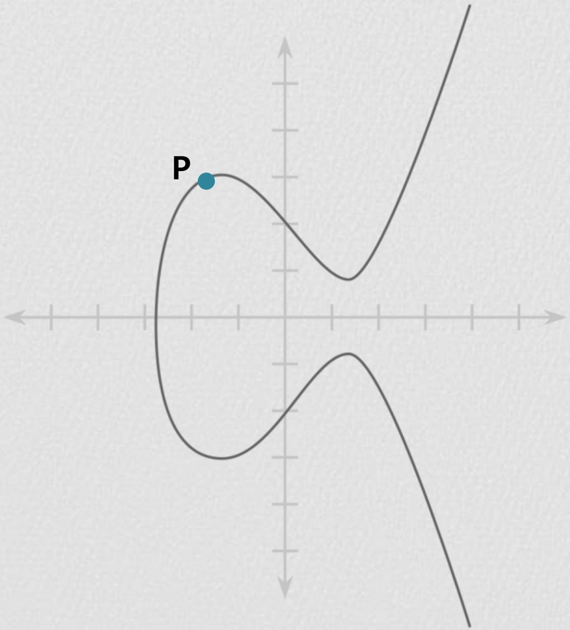
- Point addition $(P \neq Q)$



Elliptic Curve

Operations on Elliptic curves

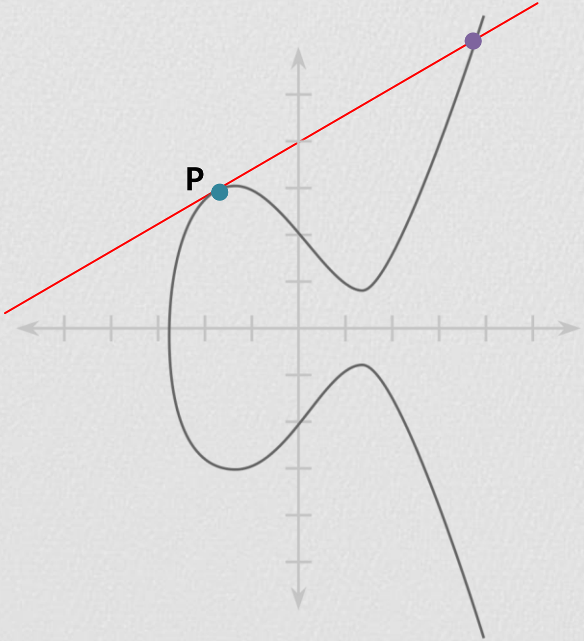
- Point doubling $(P = Q)$



Elliptic Curve

Operations on Elliptic curves

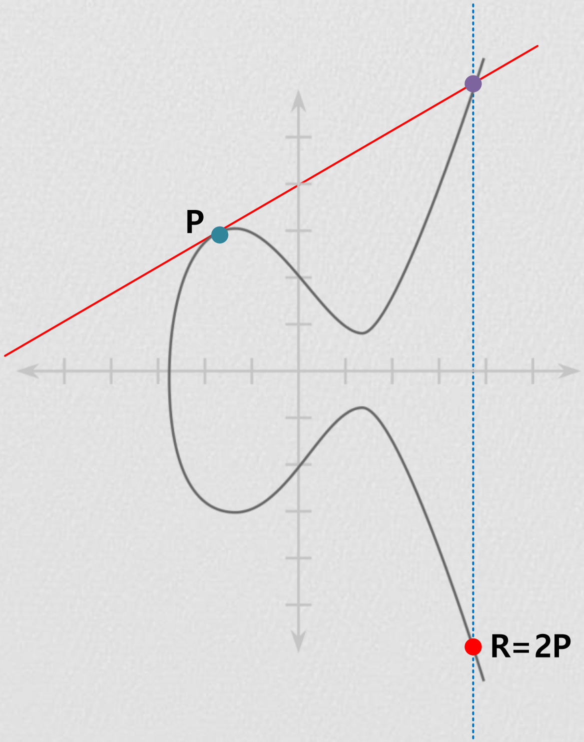
- Point doubling $(P = Q)$



Elliptic Curve

Operations on Elliptic curves

- Point doubling $(P = Q)$



Elliptic Curve

Elliptic curve group

- Theorem (Poincare)

Let K be a field and suppose that an elliptic curve E is given by the equation of the form

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

Let $E(K)$ denote the set of points of E with coordinates in K

$$E(K) = \{(x, y) \in E\} \mid x, y \in K\} \cup \{O\}$$

Then $E(K)$ is a **subgroup** of the group of all points of E

Elliptic Curve

Cyclic subgroups

- Let E be an elliptic curve defined over a field K
- Let $P \in E$ be a point on E with order n $([n]P = O)$
- Then $\langle P \rangle$ is a cyclic subgroup of E of order n

Elliptic Curve

Hasse's Bound

- 주어진 타원 곡선 E mod p 에 대해서, E 에 존재하는 점의 개수는 다음과 같이 제한된다

$$\boldsymbol{p + 1 - 2\sqrt{p} \leq \#E \leq p + 1 + 2\sqrt{p}}$$

Elliptic Curve

Discrete Logarithm Problem for Elliptic Curves

- 주어진 타원 곡선 E 와 타원곡선위의 점 P, Q 가 주어졌을 때, ECDLP는 다음을 만족하는 정수 d 를 찾는 것이다

$$\underbrace{\boldsymbol{P} + \boldsymbol{P} + \cdots + \boldsymbol{P}}_{\boldsymbol{d}\ \text{times}} = \boldsymbol{dP} = \boldsymbol{Q}$$

- 암호 시스템에서 d는 개인키, Q는 공개키로 여겨 사용한다

2

타원곡선 암호

Elliptic Curve Cryptography

Introduction to elliptic curve cryptography

- 1980년대 중반 Miller와 Koblitz가 각각 독립적으로 타원곡선을 암호에 적용
- 2000년도에 FIPS 186-2 에 ECC가 표준으로 채택
- 초반에는 RSA 암호보다 느렸으나 점차 속도가 향상
- ECDLP의 어려움에 기반

Elliptic Curve Cryptography

Elliptic Curve Diffie-Hellman (EC오)

- Parameter
  - Large prime power q
  - Elliptic curve $^{E}/_{F_q}$
  - $P \in E(F_q)$ with large prime order n

Elliptic Curve Cryptography

Elliptic Curve Diffie-Hellman (ECDH)

- Protocol

Alice	Bob
Choose a secret n_A	Choose a secret n_B
Compute $Q_A = [n_A]P$	Compute $Q_B = [n_B]P$

$$\xrightarrow{\quad \boldsymbol{Q_A} \quad}$$

$$\xleftarrow{\quad \boldsymbol{Q_B} \quad}$$

Compute $[n_A]Q_B$	Compute $[n_B]Q_A$

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

Elliptic Curve Cryptography

PKC and attack complexity

	Proposed	Security base	Complexity
RSA	1978	Hardness of factoring large integer	Sub-exponential (GNFS)
DSA	1977 (DH) 1985 (ElGamal) 1991 (DSA)	Hardness of solving discrete logarithm problem over finite field (DLP)	Sub-exponential (GNFS)
ECC	1985	Hardness of solving elliptic curve discrete logarithm problem over finite field (ECDLP)	Exponential (Summation Polynomial)

Elliptic Curve Cryptography

Recommended key sizes for a target security level

Security Level	Symmetric Key	FFC	IFC	ECC
112	3TDEA	L=2048 N=224	K=2048	F=224~255
128	AES-128	L=3072 N=256	K=3072	F=256~383
192	AES-192	L=7680 N=384	K=7680	F=384~511
256	AES-256	L=153600 N=512	K=15360	F=512+

3

아이소제니 기반 암호

Introduction to Isogeny-based Cryptography

(Elliptic) Curve-based cryptography

(Elliptic) Curve-based cryptography

Pre-quantum cryptography

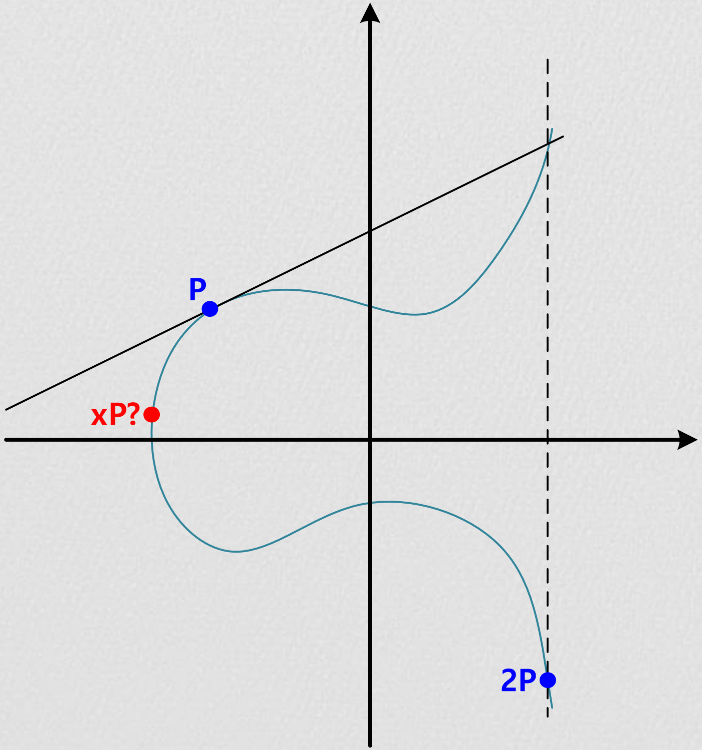
- ECC (ECDH/ECDSA)

Post-quantum cryptography

- Isogeny-based cryptography

Introduction to Isogeny-based Cryptography

Standard elliptic curve cryptography



Introduction to Isogeny-based Cryptography

Isogeny-based cryptography