Assymetrical cryptography

$y = f(x)$

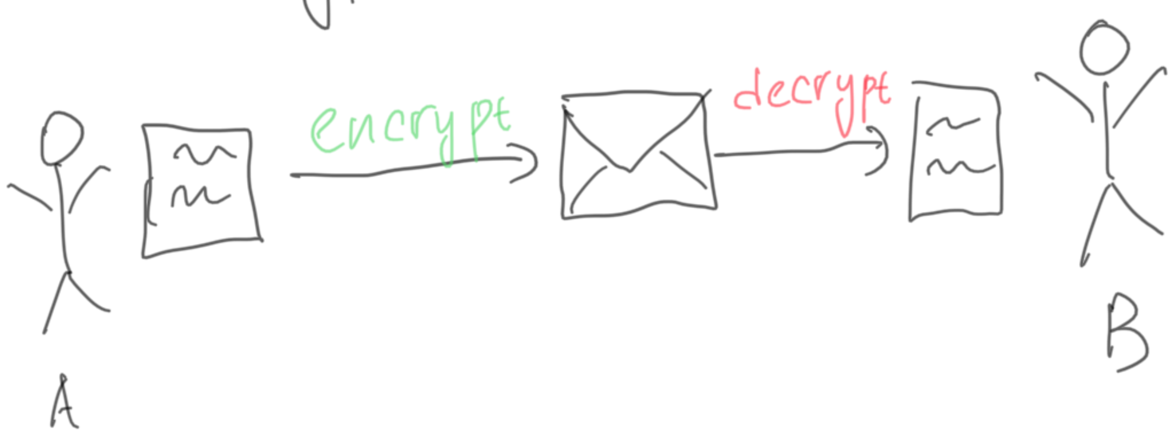
$x \longmapsto y$ ✓

$y \not\longmapsto x$ ✗

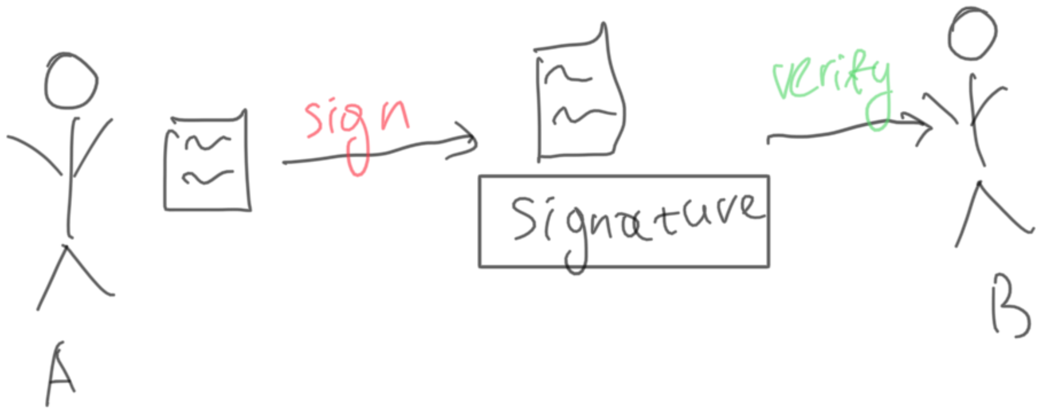
Public

Private

① Encryption



② Digital Signature



RSA

$a^{p-1} = 1 \pmod p$

- p - prime
- $(a, p) = 1$

$$a^{\varphi(n)} \equiv 1 \pmod{n}$$

- $(a, n) = 1$
- $\varphi(n) = |\{K : 1 \leq K \leq n, (K, n) = 1\}|$

$$n = p \cdot q$$

$$\varphi(n) = (p-1) \cdot (q-1)$$

$$1 < e < \varphi(n)$$

$$d \cdot e \equiv 1 \pmod{\varphi(n)}$$

(e, n) - public key

(d, n) - private key

1. Encryption

$\exists\, m$

$E(m)$ - encrypt

$D(c)$ - decrypt

$$E(m) = m^e \,\%\, n$$

$$D(c) = c^d \,\%\, n$$

$$D(E(m)) \equiv (m^e)^d = m^{ed} = m^{K \cdot \varphi(n) + 1} =$$

$$(\ldots\, \varphi(n))^K \cdot m \equiv m \pmod{n}$$

$= |m \quad /$

2 Digital Signature

$S(m)$ - sign $\qquad m = \text{hash(message)}$

$P(S)$ -

$P(S) == m$

$S(m) = m^d \% n$

$P(S) = S^e \% n$

$P(S) == m$

$m^{de} \equiv m \pmod n$

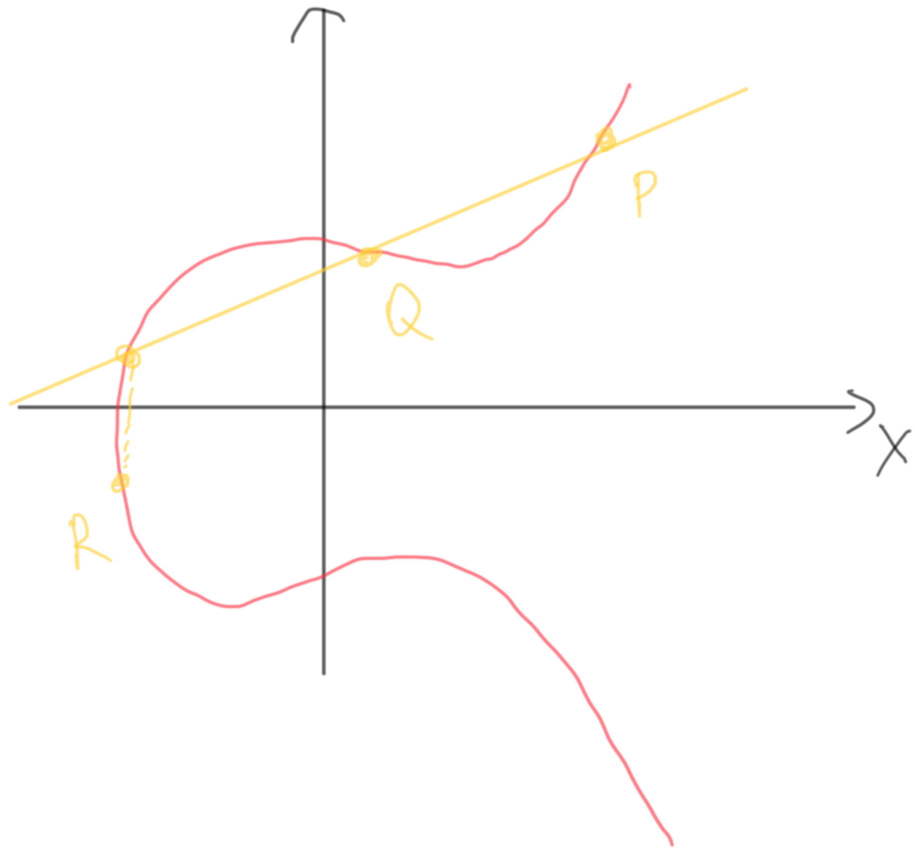
Elliptic curve

Security bits	RSA	ECC
80	1024	160
112	2048	224
128	3072	256

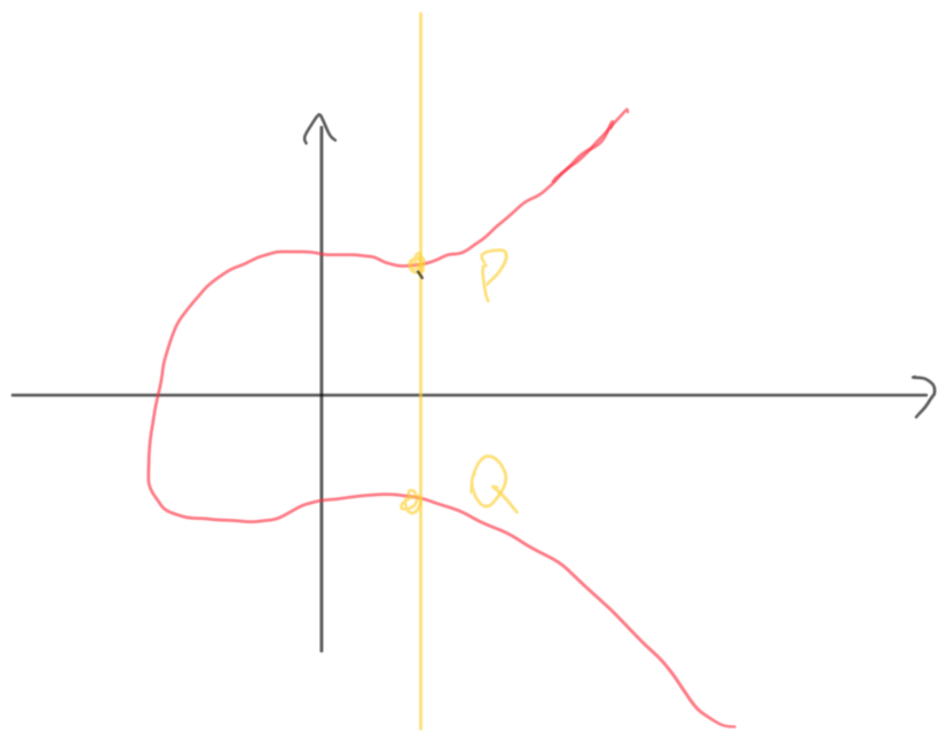
$\mathbb{R}$

$$y^2 = x^3 + ax + b$$

- $4a^3 + 27b^2 \neq 0$

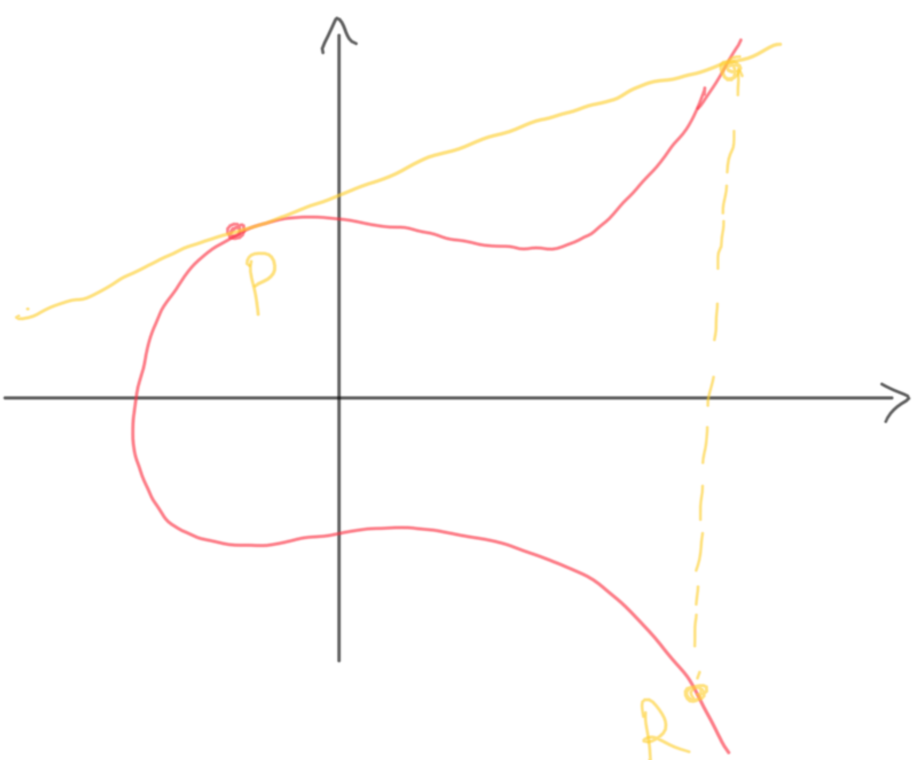


$P + Q = R$



$P + Q = \emptyset$

$P = -Q$



$P + P = 2P = R$

Group

- associativity

- associativity
$$(a+b)+c = a+(b+c)$$

- identity element
$$\exists \theta : a+\theta = a$$

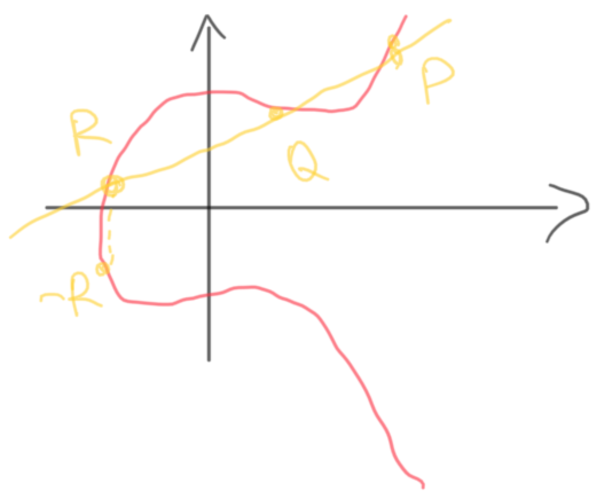
- inverse element
$$\forall a \in G \ \exists b : a+b = \theta$$

Abelian group

- commutative
$$a+b = b+a$$

Algebraic addition

$$P = (x_P, y_P)$$
$$Q = (x_Q, y_Q)$$



$P+Q = -R$

$$\lambda = \frac{y_P - y_Q}{x_P - x_Q}$$

$$\begin{cases} y = \lambda(x - x_P) + y_P \\ y^2 = x^3 + ax + b \end{cases}$$

P, Q, R

$$(\lambda(x-x_P)+y_P)^2 = x^3 + ax + b$$

$$\lambda^2(x-x_P)^2 + 2\lambda(x-x_P)y_P + y_P^2 = x^3 + ax + b$$

$$x^3 - \lambda^2 x^2 + \ldots x + \ldots = 0$$

$$x_P + x_Q + x_R = \lambda^2$$

$$\boxed{\begin{aligned} x_R &= \lambda^2 - x_P - x_Q \\ y_R &= \lambda(x_Q - x_P) + y_P \end{aligned}}$$

Logarithm

$$n \cdot P = \underbrace{P + P + \dots + P}_{n}$$

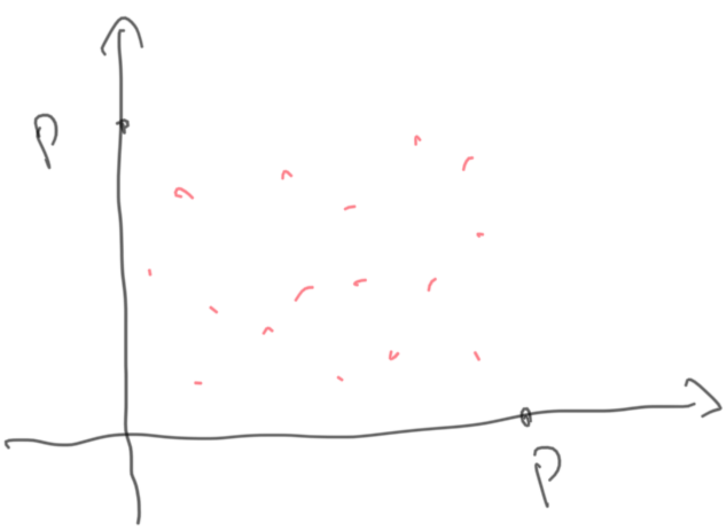
$n \longrightarrow n \cdot P$ ✓

$n \cdot P \not\longrightarrow n$ ✗

$\mathbb{F}_p$ $\quad 0, \dots, p-1$

$$y^2 \equiv x^3 + ax + b \pmod{p}$$

- $4a^3 + 27b^2 \not\equiv 0 \pmod{p}$



Addition

$$x_R = \lambda^2 - x_P - x_Q \pmod{p}$$

$$\lambda = (y_P - y_Q)(x_P - x_Q)^{-1} \pmod{p}$$

$$y_R = \lambda(x_P - x_R) + y_P \pmod{p}$$

$|E|$

Schoof $O(\log^5 p)$

P

$n \longrightarrow nP$ ✓

$nP \not\longrightarrow n$ ✗

$P+P+P+P+P=\mathcal{O}$

$\mathrm{ord}(P)=n: \quad nP=\mathcal{O}$

$E = \mathbb{Z}_{k_1} \oplus \dots \oplus \mathbb{Z}_{k_n}$

$N=|E|$

q^r

$\mathcal{O}, a, 2a, 3a, \dots, (k_1-1)a$

$nP=\mathcal{O}$

$N \vdots n$

$n=q$

$h=\frac{N}{n}$ – cofactor

$n(hP)=\mathcal{O}$

$hP = G$

$\exists n=q$

$nG=\mathcal{O}$

$\mathrm{ord}(G)=n$

G - generator

$\mathrm{ord}(G) = n$

$h = \frac{N}{n}$ - cofactor

$nG = \mathcal{O}$

rel. large

$k \longrightarrow kG$ ✓

$kG \not\longrightarrow k$ ✗

Encryption

ECDH

d_A

$H_A = d_A \cdot G$

A

d_B

$H_B = d_B G$

B

$$d_A H_B = d_A \cdot d_B G = d_B d_A G = d_B H_A$$

$$G, d_A G, d_B G \not\longrightarrow d_A d_B G$$

Signature

ECDSA

$z = \mathrm{hash}(m)$

1. $\exists\, k$ - random $\in \{1, \dots, n-1\}$

2. $P = kG$ — generator

3. $r = x_p \ \% \ n$

4. $r == 0$

5. $s = k^{-1}(z + r \cdot d_A) \ \% \ n$

6. $s == 0$

(r, s) — signature

Verifying

1. $u_1 = s^{-1} z \pmod n$

2. $u_2 = s^{-1} r \pmod n$

3. $P_1 = u_1 G + u_2 H_A$

4. $r == x_{P_1} \ \% \ n$

$$P_1 = u_1 G + u_2 H_A = u_1 G + u_2 d_A G =$$

$$= (u_1 + u_2 d_A) G = (s^{-1} z + s^{-1} r d_A) G =$$

$$= s^{-1}(z + r d_A) G = k (z + r d_A)^{-1} (z + r d_A) G =$$

$$= kG \ \blacksquare$$