Cryptography

$E(K_{pub}, m) = enc$

$D(K_{priv}, enc) = m$

$K_{pub} = K_{priv}$

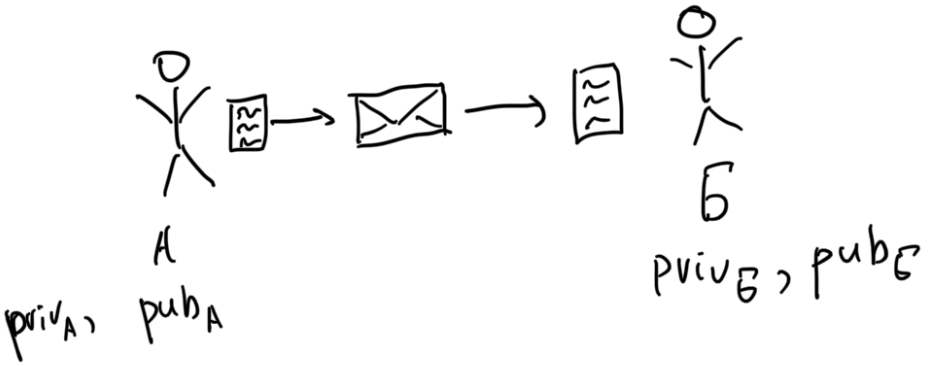
Assymetrical cryptography

$y = f(x)$

$x \longmapsto y$ ✓

$y \longmapsto x$ ✗

① Encryption



② Digital Signature

signature

A

$priv_A$, pub_A

RSA

$f(p_1, p_2) = p_1 \cdot p_2$

$n = p \cdot q$

$(d, n) \rightarrow$ private key, $d < n$

$(e, n) \rightarrow$ public key

$d \cdot e \equiv 1 \pmod{\varphi(n)}$
$\varphi(n) = (p-1)(q-1)$

$(a, p) = 1$

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

$(a, n) = 1$

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

$\varphi(n) = |\{k : k \in \{1, \dots n\}, (k, n) = 1\}|$

$\varphi(p) = p - 1$

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

1 Encryption

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

$E(m) =$

$D(enc) = enc^d \% n = m$

$(m^e)^d = m^{ed} = m^{k \cdot \varphi(n) + 1} = \left(m^{\varphi(n)}\right)^k \cdot m \equiv m \pmod{n}$

$\varphi(n) \equiv 1$

② Signing

$m = hash(message)$

$s(m)$ - sign

$v(s, m, pub)$

$s(m) = m^{priv_A} = s_A$

$v(s_A, m, pub_A) = s_A^{pub_A} == m$

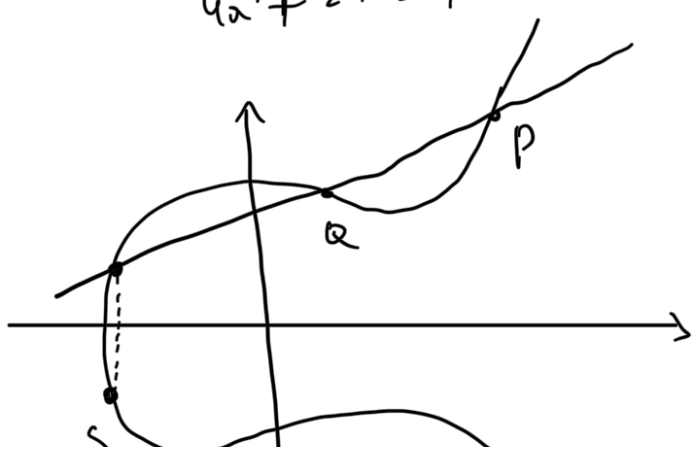
Elliptic Curves

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

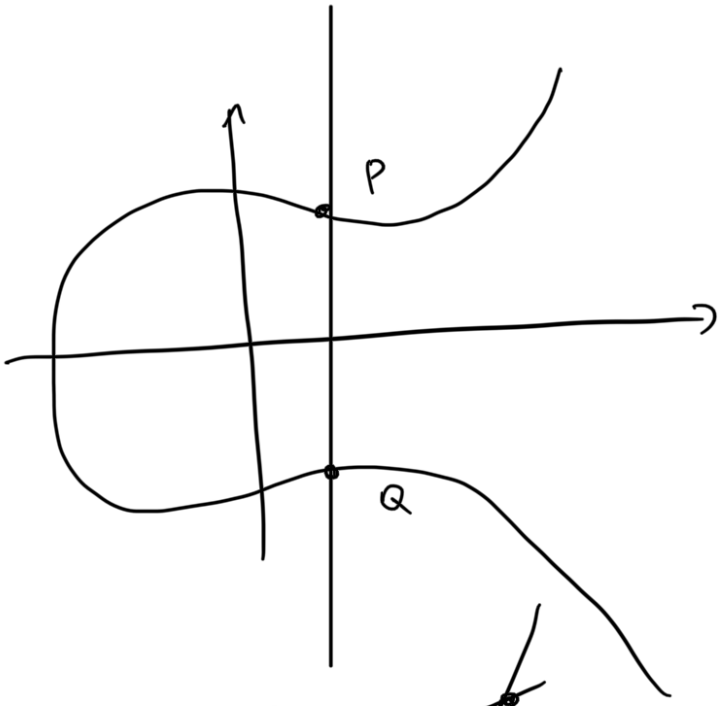
$\mathbb{R}$

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

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

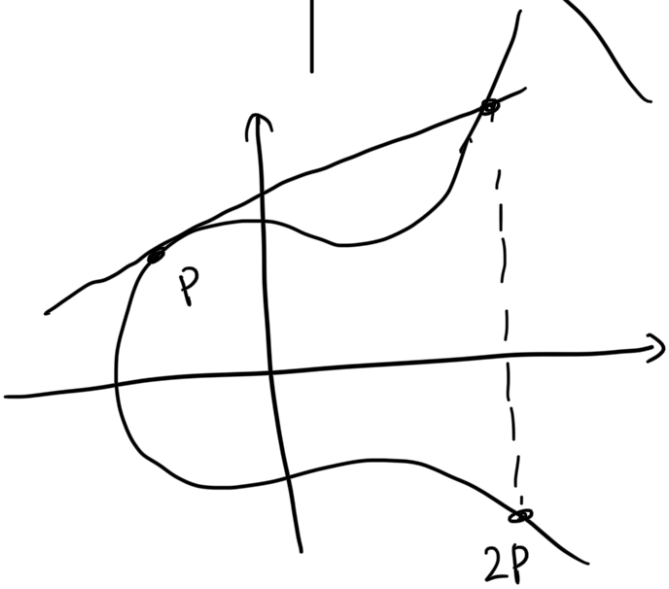


$S = P + Q$



$P + Q = \mathcal{O}$

$Q = -P$



$P + P$

- $(a+b)+c = a+(b+c)$
- $\exists\, 0 ;\ A + 0 = A$!
- $\forall a\ \exists b ;\ a + b = 0$!

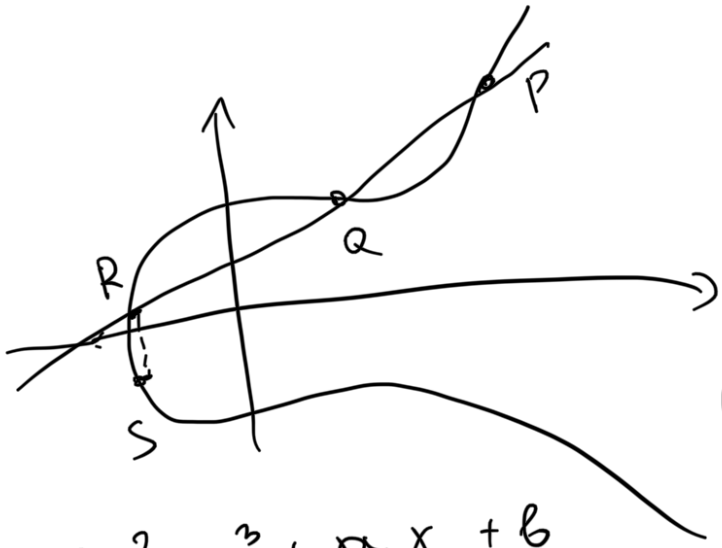
+ commutative

$a + b = b + a$

$n, P \longleftrightarrow n \cdot P$

addition

Algebraic



(x_P, y_P)

(x_Q, y_Q)

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

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

$$y = \lambda(x - x_P) + y_P$$

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

$$(\lambda(x_r - x_P) + y_P)^2 = x_r^3 + a x_r + b$$

$$\lambda^2 (x_r - x_P)^2 + 2\lambda(x_r - x_P) y_P + y_P^2 = x_r^3 + a x_r + b$$

$$x_r^3 - \lambda^2 x_r^2 + \dots\dots = 0$$

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

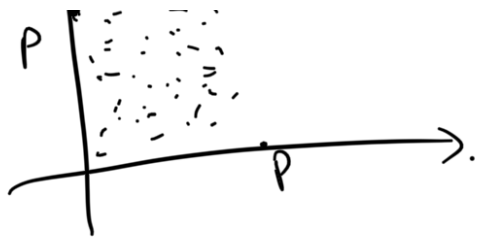
$$x_R = \lambda^2 - x_P - x_Q = \left(\frac{y_P - y_Q}{x_P - x_Q}\right)^2 - x_P - x_Q$$

$$y_R = \lambda(x_r - x_P) + y_P$$

$\mathbb{F}_p$

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

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



$f(x) = y$