Cryptography

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

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

$K_{pub} = K_{priv}$

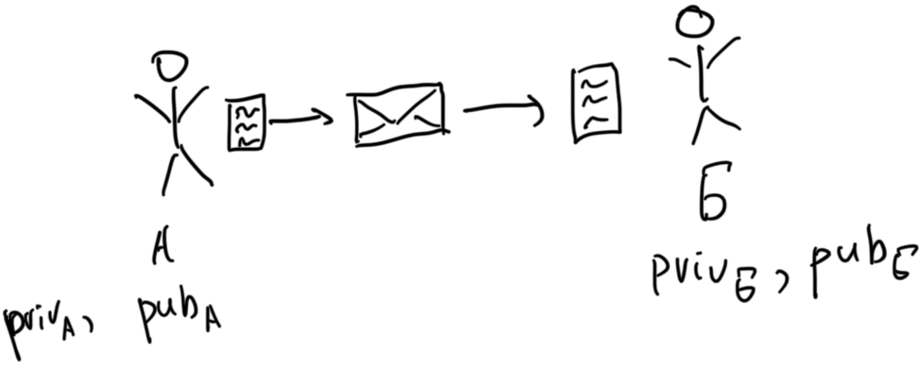
Assymetrical cryptography

$y = f(x)$

$x \longmapsto y$ ✓

$y \longmapsto x$ ✗

① Encryption



② Digital Signature

sign
verify

$priv_A$, pub_A

R SA

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

$n = p \cdot q$

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

$(e, n) \to$ public key

$d \cdot e \equiv 1 \ (\mathrm{mod}\ \underset{(p-1)(q-1)}{\underset{\shortparallel}{\varphi(n)}}))$

$(a, p) = 1$

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

$(a, n) = 1$

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

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

$\varphi(p) = p - 1$

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

① Encryption

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

$E(m) =$

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

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

② Signing

$m = hash(message)$

$s(m)$ - sign

$v(s, m, pub)$

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

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

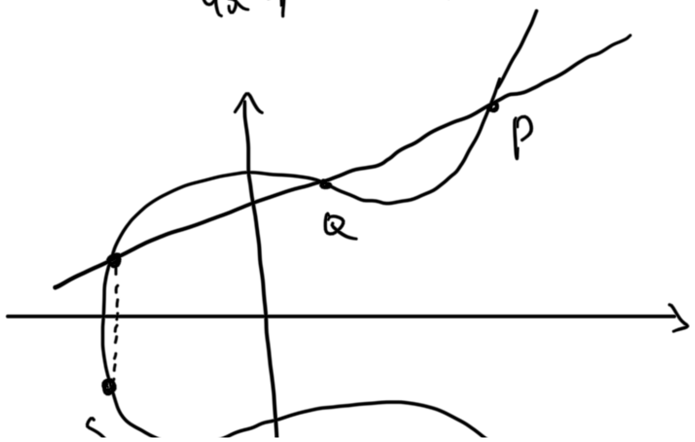
Elliptic Curves

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

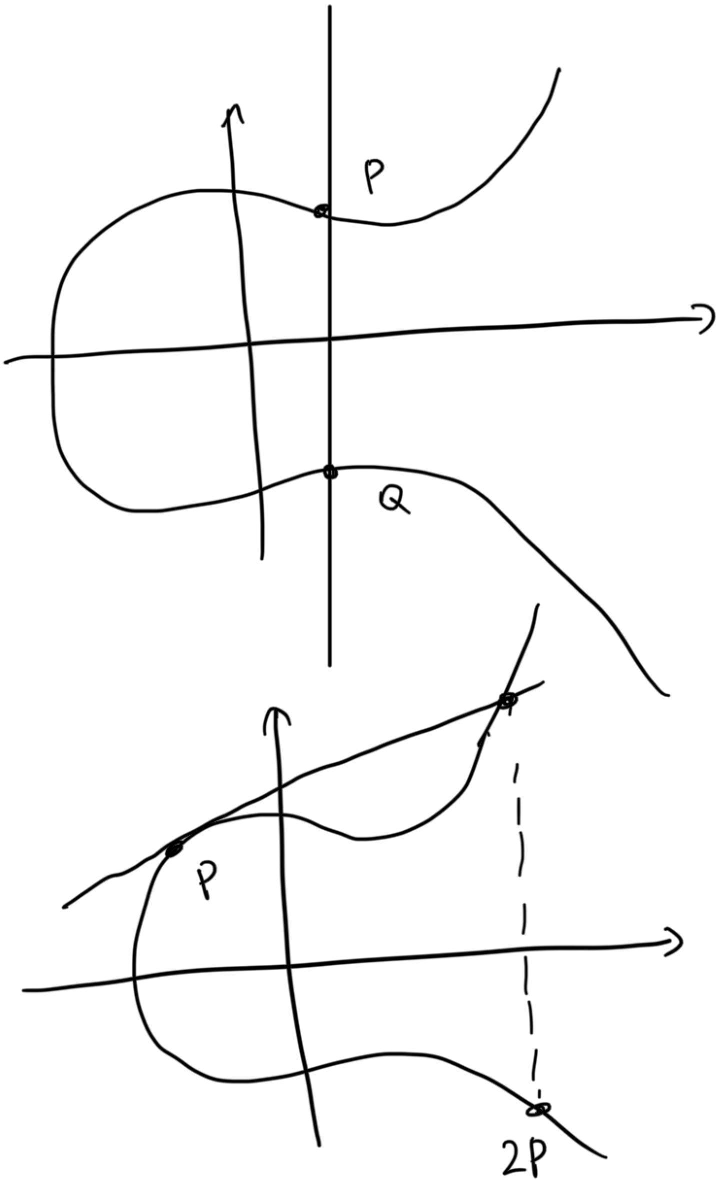
$\mathbb{R}$

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

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



$S = P + Q$



$P + Q = \Theta$

$Q = -P$

$P + P$

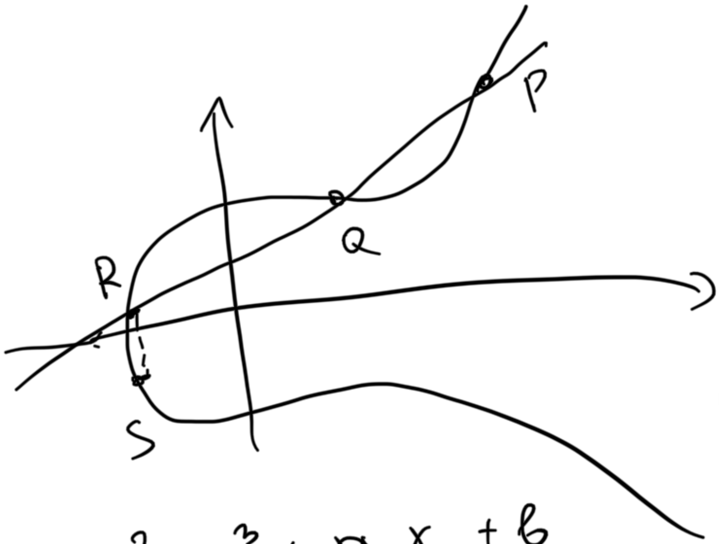
- $(a + b) + c = a + (b + c)$
- $\exists\ \Theta\ ;\ A + \Theta = A$!
- $\forall a\ \exists b\ ;\ a + b = \Theta$!

+ commutative
  $a + b = b + a$

$n, P \longmapsto n \cdot P$

addition

Algebraic



(x_p, y_p)

(x_Q, y_Q)

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

$$\boxed{\lambda = \frac{y_P - y_Q}{x_p - x_Q}}$$

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

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

$$(\lambda(x_r - x_p) + y_p)^2 = x_r^3 + ax_r + b$$

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

$$x_r^3 \underbrace{- \lambda^2}\, x_r^2 + \ldots\ldots = 0$$

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

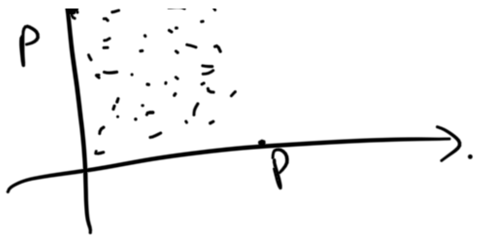
$$x_R = \lambda^2 - x_P - x_Q = \left(\frac{y_P - y_Q}{x_P - x_Q}\right)^2 - x_p - x_Q$$

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

$\mathbb{F}_p$

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

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



$f(x) = y$

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

$f(n, P) = n \cdot P$

$n \cdot P \not\rightarrow n$

G - generator (point)

$E = \underset{p_1^{d_1}}{\mathbb{Z}_{k_1}} \oplus \underset{p_2^{d_2}}{\mathbb{Z}_{k_2}} \oplus \dots \oplus \mathbb{Z}_{k_n}$

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

$n\, G = 0$

$G,\ 2G,\ 3G,\ \dots$

$\frac{|E|}{k}$ - cofactor

$x \longrightarrow x\,G$

$x\,G \longrightarrow x$

Encryption

ECDH

d_B

$H_B = d_B G$

d_A

$H_A = d_A G$

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

Signing

d_A - private

$H_A = d_A G$ - public

ECDSA

hash $(m) = z$

1. $\exists k \in \{1, \dots, n\}$
2. $P = kG$
3. $r = x_{\underline{P}} \% n$
4. $r == 0$
5. $s = k^{-1}(z + r \cdot d_A) \% n$
6. $s == 0$

$(r, \underline{s})$ - signature

verify

1. $u_1 = s^{-1} z \pmod n$
2. $u_2 = s^{-1} r \pmod n$
3. $P_1 = u_1 G + u_2 \underbrace{H_A}$

$r \% n$

4. $r == {}^{\wedge}P_1$ 10 ·

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

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

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

$$\shortparallel \; kG. \quad \shortparallel \; \smile$$

$$s^{-1} = k \, (z + r d_A')^{-1} \pmod{n}$$

$$aG = bG$$

$$\Updownarrow$$

$$a \equiv b \pmod{n}$$

$$a = b + t \cdot n$$