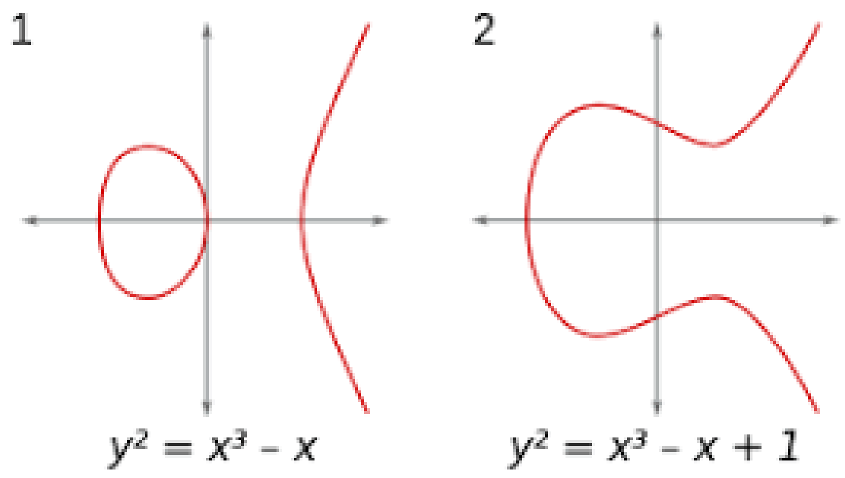
Elliptic Curve and Cryptography – ECC

Lesson 4

DECENTRALIZED

fit@hcmus.CRYPT

Elliptic curves



- An elliptic curve is the set of solution (x, y)

to an equation of the form (E): $Y^2 = X^3 + AX + B$

- Let P and Q be two points on E, $R = P \oplus Q$ is defined as the following:

(1) Let R' is intersection of E and the line L through P and Q.

(2) Then R is the reflection of R' by x-axis.

- $P \oplus P$ = ?. Take L to be the tangent line to E at P.
- $P \oplus Q$, where P = (a, b) and Q = (a, -b)? L is the vertical line x = a. There is no third point of intersection. The solution is to create an extra point O that lives "at infinity": $P \oplus Q = (a, b) \oplus (a, -b) = O$.

Elliptic Curve Addition Algorithm

Let (E): $Y^2 = X^3 + AX + B$ be an elliptic curve and

Let P1 = (x1, y1), P2 = (x2, y2) be points on E.

(1) If P1 = O, then P1 + P2 = P2.

(2) Else If P2 = O, then P1 + P2 = P1.

(3) Else If x1 = x2 and y1 = - y2, then P1 + P2 = O.

(4) Else P1 + P2 = (x3, y3), where

$$\alpha = \begin{cases} \dfrac{y2 - y1}{x2 - x1} & if\ P1 \neq P2, \\ \dfrac{3x1^2 + A}{2y1} & if\ P1 = P2 \end{cases}, x3 = \alpha^2 - x1 - x2, y3 = \alpha(x1 - x3) - y1$$

Elliptic curves over finite fields

Definition (elliptic curve). An elliptic curve E is the set of solutions to a Weierstrass equation (E): $Y^2 = X^3 + AX + B$, together an extra point O, where A, B satisfy $4A^3 + 27B \neq 0$.

Theorem. Let E be an elliptic curve over F_p, and P, Q $\in E(F_p)$. $(E(F_p), \oplus)$ is a finite group.

Theorem (Hasse). $\#E(F_p) = p + 1 - t_p$

with t_p satisfying $|t_p| \leq 2\sqrt{p}$.

The elliptic curve DLP - ECDLP

Definition (ECDLP). $P, Q \in E(F_p)$. The ECDLP is finding an integer n: $Q = nP$. We denote $n = \log_P(Q)$.

The Double-and-Add algorithm

- Input: $P \in E(F_p)$, $n \geq 1$
- Output: $R = nP$

(1) Set $Q = P$, $R = O$.

(2) While $n > 0$ {

  (1) If $n \equiv 1 \pmod 2$, set $R = R + Q$

  (2) Set $Q = 2Q$; $n = \lfloor n/2 \rfloor$

  }

(3) Return R

Elliptic Diffie-Hellman key exchange

Public Parameter Creation

A trusted party chooses and publishes a (large) prime, an elliptic curve $E(F_p)$, and a point P in $E(F_p)$

Private Computations

Alice	**Bob**
Chooses a secret integer n_A. Computes the point $Q_A = n_A P$.	Chooses a secret integer n_B. Computes the point $Q_B = n_B P$.

Public Exchange of Values

Alice sends Q_A to Bob $\longrightarrow Q_A$.

$Q_B \longleftarrow$ Bob sends Q_B to Alice

Furthure Private Computations

Computes the point $n_A Q_B$.	Computes the point $n_B Q_A$.

The shared secret value is $n_A Q_B = n_A(n_B P) = n_B(n_A P) = n_B Q_A$.

The Elliptic Curve Diffie-Hellman Problem

Definition (ECDP). Le $E(F_p)$ be an elliptic curve over a finite F_p and let $P \in E(F_p)$. The Elliptic Curve Diffie-Hellman Problem is the problem of computing the value $n_1 n_2 P$ from the known values $n_1 P$ and $n_2 P$.

Elliptic ElGamal public key cryptography

Public Parameter Creation

A trusted party chooses and publishes a (large) prime p, an elliptic curve $E(\mathbb{F}_p)$, and a point $P \in E(\mathbb{F}_p)$

Alice	**Bob**

Key Creation

Chooses a private key n_A.
Computes $Q_A = n_A P$.
Publishes the public key Q_A.

Encryption

Chooses plaintext $M \in E(\mathbb{F}_p)$.
Chooses an ephemeral key k.
Uses Alice's public key Q_A to

- Compute $C_1 = M + kP$ and
- Compute $C_2 = M + kQ_A$.

Sends ciphertext (C_1, C_2) to Alice

Decryption

Computes $C_2 - n_A C_1$.