MẬT MÃ ỨNG DỤNG TRONG ATTT

Bài 05. Mật mã trên đường cong elliptic

1. Nhóm hữu hạn trên đường cong elliptic
2. Mật mã trên đường cong elliptic
3. Nhúng số vào điểm trên đường cong elliptic

1. Nhóm hữu hạn trên đường cong elliptic
2. Mật mã trên đường cong elliptic
3. Nhúng số vào điểm trên đường cong elliptic

Đường cong elliptic

- p là số nguyên tố
- Fp là trường hữu hạn các số nguyên theo modulo p
- Đường cong elliptic E trên trường Fp được xác định bởi phương trình

$$y^2 = x^3 + ax + b \qquad (1)$$

- Với điều kiện: $\begin{cases} a,b \in F_p \\ 4a^3 + 27b^2 \neq 0 \pmod p \end{cases}$

4

Đường cong elliptic

$$y^2 = x^3 + ax + b \qquad (1)$$

- Một cặp (x, y) trong đó $x, y \in F_p$ được gọi là một điểm thuộc đường cong nếu chúng thỏa mãn (1)
- Ngoài ra có «điểm ở vô cùng»,ký hiệu là O, (∞)

5

Đường cong elliptic

- Ví dụ, xét đường cong E trên F_7

$$E : y^2 = x^3 + 2x + 4 \qquad (2)$$

- Tập hợp các điểm thuộc đường cong là:

$$E(F_7) = \{\infty, (0,2), (0,5), (1,0), (2,3), (2,4), (3,3), (3,4), (6,1), (6,6)\}$$

- Có thể tìm tất cả các điểm thuộc E bằng cách duyệt mọi giá trị x, nhưng không thể áp dụng khi p lớn ➔ có thuật toán hiệu quả hơn.

6

Luật nhóm các điểm trên đường cong elliptic

❑**Luật nhóm:**

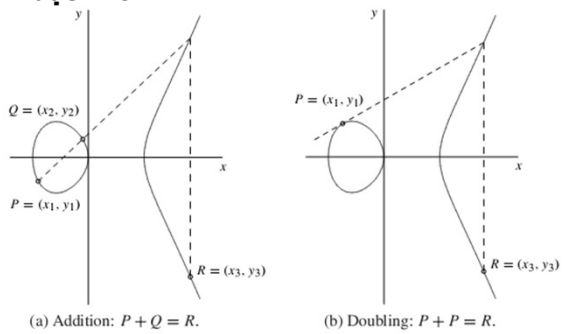
– Xét tập tất cả các điểm của một đường cong E

– Định nghĩa phép cộng điểm trên tập E sao cho (E,+) là một nhóm hữu hạn

7

Luật nhóm các điểm trên đường cong elliptic

❑**Luật nhóm:**



8

Luật nhóm các điểm trên đường cong elliptic

❑**Luật nhóm:**

"Điểm ở vô cùng", kí hiệu là ∞: đường thẳng đi qua hai điểm có thể không cắt đường cong ở điểm thứ ba. Khi đó, coi rằng nó cắt đường cong ở vô cùng!

9

Luật nhóm các điểm trên đường cong elliptic

❑**Luật nhóm:**

$E: y^2 = x^3 + ax + b; \quad P_1, P_2 \in E, \quad P_1 \neq \infty, \quad P_2 \neq \infty$

$P_1 = (x_1, y_1); \quad P_2 = (x_2, y_2); \quad P_1 + P_2 = P_3 = (x_3, y_3)$

1. Nếu $x_2 = x_1, y_2 = -y_1$ thì $P_1 + P_2 = \infty$,

2. Ngược lại $P_1 + P_2 = (x_3, y_3)$ trong đó:

- $x_3 = \lambda^2 - x_1 - x_2$
- $y_3 = \lambda(x_1 - x_3) - y_1$ và

$$\lambda = \begin{cases} \frac{y_2 - y_1}{x_2 - x_1}, \text{if } P_1 \neq P_2 \\ \frac{3x_1^2 + a}{2y_1}, \text{if } P_1 = P_2 \end{cases}$$

10

Luật nhóm các điểm trên đường cong elliptic

❑**Luật nhóm:**

$E: y^2 = x^3 + ax + b; \quad P_1, P_2 \in E, \quad P_1 \neq \infty, \quad P_2 \neq \infty$

$P_1 = (x_1, y_1); \quad P_2 = (x_2, y_2); \quad P_1 + P_2 = P_3 = (x_3, y_3)$

3. $P + \infty = \infty + P = P, \forall P \in E$

4. Phép lấy nghịch đảo được tính toán khá dễ dàng, nghịch đảo của (x, y) là $-(x, y)$ và $= (x, -y)$

11

Luật nhóm các điểm trên đường cong elliptic

❑**Ví dụ:** $E: y^2 = x^3 + 2x + 4; \quad p = 7$

$E(F_7) = \{\infty, (0,2), (0,5), (1,0), (2,3),$
$(2,4), (3,3), (3,4), (6,1), (6,6)\}$

VD1:

$P_1 = (x_1, y_1) = (0,2); \quad P_2 = (x_2, y_2) = (0,5)$

$Obviously: \quad (x_1 = x_2) \; and \; (y_2 = -y_1)$

$\Rightarrow P_1 + P_2 = \infty \quad \Rightarrow P_1 = -P_2$

12

Luật nhóm các điểm trên đường cong elliptic

❑**Ví dụ:** $E: y^2 = x^3 + 2x + 4; \quad p = 7$

$E(F_7) = \{\infty, (0,2), (0,5), (1,0), (2,3), (2,4), (3,3), (3,4), (6,1), (6,6)\}$

$VD2: P_1 = (x_1, y_1) = (0,2); \quad P_2 = (x_2, y_2) = (2,3)$

$Obviously: \quad (x_1 \neq x_2)$

$$\lambda = \frac{y_2 - y_1}{x_2 - x_1} = \frac{3-2}{2-0} = \frac{1}{2} = 2^{-1} = 4 \pmod 7$$

$$x_3 = \lambda^2 - x_1 - x_2 = 4^2 - 0 - 2 = 0 \pmod 7$$

$$y_3 = \lambda(x_1 - x_3) - y_1 = 4(0-0) - 2 = -2 = 5 \pmod 7$$

$$\Rightarrow P_3 = (x_3, y_3) = (0,5)$$

13

Luật nhóm các điểm trên đường cong elliptic

❑**Tính chất phép cộng điểm**

- Tính chất giao hoán
  $P_1 + P_2 = P_2 + P_1 \quad \forall P_1, P_2 \in E$
- Tính chất kết hợp
  $(P_1 + P_2) + P_3 = P_1 + (P_2 + P_3) \quad \forall P_1, P_2, P_3 \in E$
- Tồn tại phần tử trung hòa
  $P + \infty = \infty + P = P \quad \forall P \in E$
- Tồn tại phần tử đối
  $\exists P' \in E: P' + P = P + P' = \infty \quad \forall P \in E$
- Tính đóng

14

Luật nhóm các điểm trên đường cong elliptic

❑**Phần tử đối:**

- $P = \infty \quad \Rightarrow \quad -P = \infty$
- $P = P(x,0) \quad \Rightarrow \quad -P = P$
- $P = P(x,y) \quad \Rightarrow \quad -P = P'(x,-y)$

❑**Ghi chú**

$P(x,y) \in E \quad \Rightarrow \quad P'(x,-y) \in E$

❑**Ví dụ**

- $P = (2,3) \quad \Rightarrow \quad -P = (2,-3) = (2,4)$
- $P = (1,0) \quad \Rightarrow \quad -P = (1,0)$

15

Luật nhóm các điểm trên đường cong elliptic

❑**Bậc của điểm P**: Cho đường cong $E(F_p)$ và P là một điểm thuộc đường cong. Bậc của P là số nguyên n nhỏ nhất thỏa mãn $n \cdot P = \infty$

❑**Nhóm con cyclic sinh bởi P**: Cho đường cong $E(F_p)$ và P là một điểm thuộc đường cong. Giả sử P có bậc là n. Khi đó, nhóm con cyclic sinh bởi P được kí hiệu là <P> và:

$$\langle P \rangle = \{\infty, P, 2P, 3P, \ldots, (n-1)P\}$$

16

1. Nhóm hữu hạn trên đường cong elliptic
2. Mật mã trên đường cong elliptic
3. Nhúng số vào điểm trên đường cong elliptic

Mật mã trên đường cong elliptic

❑**Bài toán logarit rời rạc trên Z^*_p**

Cho p, a
- Biết x. Tính $y = a^x \pmod p$ DỄ
- Biết y. Tìm x: $y = a^x \pmod p$ KHÓ

❑**Bài toán logarit rời rạc trên E(Fp)**

Cho p, $P \in E(F_p)$
- Biết k. Tính Q = kP DỄ
- Biết Q. Tìm k: Q = kP KHÓ

18

Mật mã trên đường cong elliptic

❑**Sinh cặp khóa**

IN: Tham số hệ thống <p, $E(a,b)$, P, n>
OUT: Khóa công khai $\boldsymbol{Q}$ và khóa bí mật $\boldsymbol{d}$
1. Chọn ngẫu $\boldsymbol{d} \in [1, n-1]$
2. Tính $\boldsymbol{Q = dP}$
3. Kết quả là:
   + **KCK:** $\boldsymbol{Q}$
   + **KBM:** $\boldsymbol{d}$

19

Mật mã trên đường cong elliptic

❑**Mã hóa**

IN: Tham số hệ thống (p, $E_{(a,b)}$, P, n)
Khóa công khai Q
Thông điệp m
OUT: Bản mã (C_1, C_2)
1. Biểu diễn m thành điểm $M \in E$
2. Chọn ngẫu $k \in [1, n-1]$
3. Tính $C_1 = kP$
4. Tính $C_2 = M + kQ$
5. Kết quả là $C = (C_1, C_2)$

20

Mật mã trên đường cong elliptic

❑**Giải mã**

IN: Tham số hệ thống (p, $E_{(a,b)}$, P, n)
Khóa bí mật d
Bản mã $C = (C_1, C_2)$
OUT: Thông điệp ban đầu m
1. Tính $M = C_2 - dC_1$
2. Trích xuất m từ M
3. Kết quả là m

21

1. Nhóm hữu hạn trên đường cong elliptic
2. Mật mã trên đường cong elliptic
3. Nhúng số vào điểm trên đường cong elliptic

Nhúng số vào điểm thuộc đường cong elliptic

1. Cho đường cong $E(F_p)$: $y^2 = f(x) = x^3 + ax + b$
2. Cho m là số nguyên. Muốn mã hóa m bằng ECC thì cần chuyển m thành điểm $M=(x,y)$ nào đó.
3. Ý tưởng nhúng:
   1. Coi m là hoành độ của M, tức $M = (m, y)$
   2. Thay $x = m$ vào phương trình của E và giải phương trình $y^2 = f(m)$ đối với y, tìm được nghiệm u
   3. Điểm cần tìm là $M = (m, u)$
4. Trở ngại: Chỉ có khoảng ½ số phần tử của F_p là thặng dư bậc 2 → xác suất tìm được u là ½ → xác suất nhúng thành công là ½.

23

Nhúng số vào điểm thuộc đường cong elliptic

1. Xác định giới hạn $m_{max} << p$ đối với m
2. Tính hệ số nhúng $l = \lfloor p / (m_{max} + 1) \rfloor$
3. Đối với mỗi số m cần nhúng, ánh xạ m thành $m' \in [lm, lm+l-1]$ sao cho $f(m')$ là thặng dư bậc 2. Xác suất thất bại là 2^{-l}.
4. Nhúng m' thành điểm M bằng phương pháp đã biết
5. Từ m' tìm lại m bằng công thức $m = \lfloor m' / l \rfloor$

24

Nhúng số vào điểm thuộc đường cong elliptic

❑Ví dụ $E(F_{67}): y^2 = x^3 + 3x + 2$

$m \in \{0,1,2,3,4,5\} \Rightarrow m_{max} = 5 << p = 67$

❑Khi không dùng hệ số nhúng

m	f(m)	$\sqrt{f(m)}$
0	2	không tồn tại
1	6	26, 41
2	16	4, 63
3	38	không tồn tại
4	11	không tồn tại
5	8	không tồn tại

25

Nhúng số vào điểm thuộc đường cong elliptic

❑Ví dụ $E(F_{67}): y^2 = x^3 + 3x + 2$

$m \in \{0,1,2,3,4,5\} \Rightarrow m_{max} = 5 << p = 67$

❑Khi dùng hệ số nhúng (l = 11)

m	lm	$lm+l-1$	m'	f(m')	$\sqrt{f(m')}$	M	$m = \left\lfloor \frac{m'}{l} \right\rfloor$
0	0	10	1	6	26	(1, 26)	0
1	11	21	11	26	19	(11, 19)	1
2	22	32	24	29	37	(24, 37)	2
3	33	43	33	59	40	(33, 40)	3
4	44	54	47	49	60	(47, 60)	4
5	55	65	55	47	39	(55, 39)	5

26

Nhúng số vào điểm thuộc đường cong elliptic

❑**Bài tập về nhà (có trong đề thi)**

1. Thuật toán Euclid mở rộng
2. Kí hiệu Legendre
3. Thuật toán Tonelli-Shank
4. Nhúng số vào điểm thuộc đường cong elliptic xác định trên F_p

27