

# Hệ mật mã dựa trên đường cong Elliptic

Version 0.1

# Nội dung

**1. Đường cong Elliptic (Elliptic Curve, EC)**

2. Bài toán Logarit rời rạc trên EC

3. Giao thức trao đổi khoá Diffie-Hellman trên EC

# Vấn đề: Tìm hệ mật với tham số ngắn hơn

| Algorithm Family      | Cryptosystems    | Security Level (bit) |          |          |           |
|-----------------------|------------------|----------------------|----------|----------|-----------|
|                       |                  | 80                   | 128      | 192      | 256       |
| Integer factorization | RSA              | 1024 bit             | 3072 bit | 7680 bit | 15360 bit |
| Discrete logarithm    | DH, DSA, Elgamal | 1024 bit             | 3072 bit | 7680 bit | 15360 bit |
| Elliptic curves       | ECDH, ECDSA      | 160 bit              | 256 bit  | 384 bit  | 512 bit   |
| Symmetric-key         | AES, 3DES        | 80 bit               | 128 bit  | 192 bit  | 256 bit   |

Kích thước theo bit của các hệ mật mã khoá công khai ở mức an toàn khác nhau

# Đường cong Elliptic

Đường cong Elliptic trên  $K$  là tập mọi cặp  $(x,y) \in K$  thoả mãn phương trình

$$y^2 = x^3 + a \cdot x + b$$

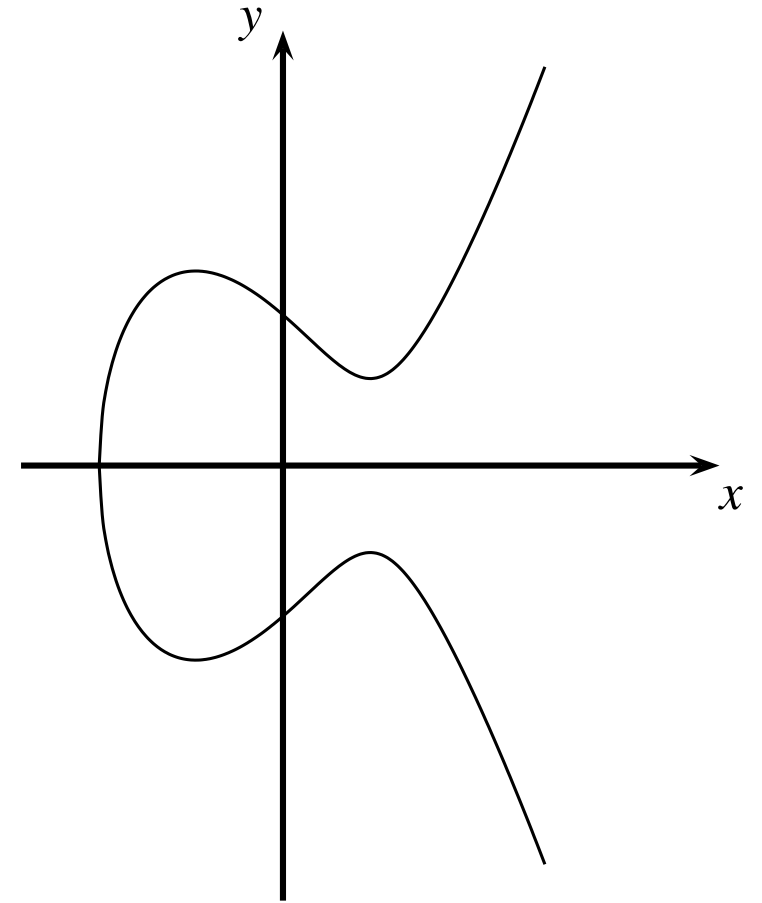
cùng với một điểm vô cực  $O$ ,

trong đó

$$a, b \in K$$

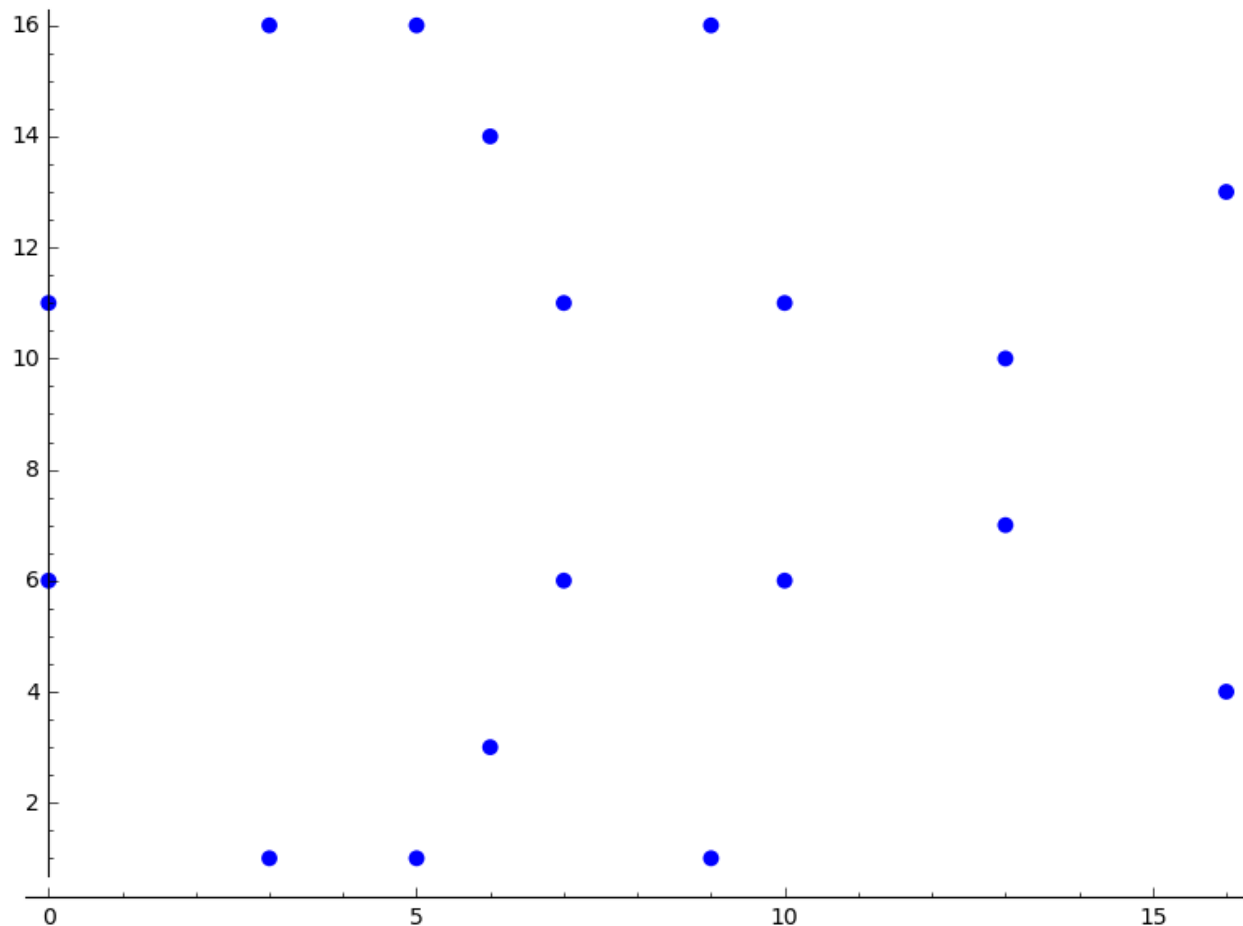
và thoả mãn  $4 \cdot a^3 + 27 \cdot b^2 \neq 0$ .

Đường cong không điểm kỳ dị



$$y^2 = x^3 - 3x + 3 \text{ trên } \mathbb{R}$$

# Đường cong $y^2 = x^3 + 2x + 2$ trên $Z_{17}$



Danh sách điểm

| $\mathcal{O}$ |          |
|---------------|----------|
| (0, 6)        | (7, 11)  |
| (0, 11)       | (9, 1)   |
| (3, 1)        | (9, 16)  |
| (3, 16)       | (10, 6)  |
| (5, 1)        | (10, 11) |
| (5, 16)       | (13, 7)  |
| (6, 3)        | (13, 10) |
| (6, 14)       | (16, 4)  |
| (7, 6)        | (16, 13) |

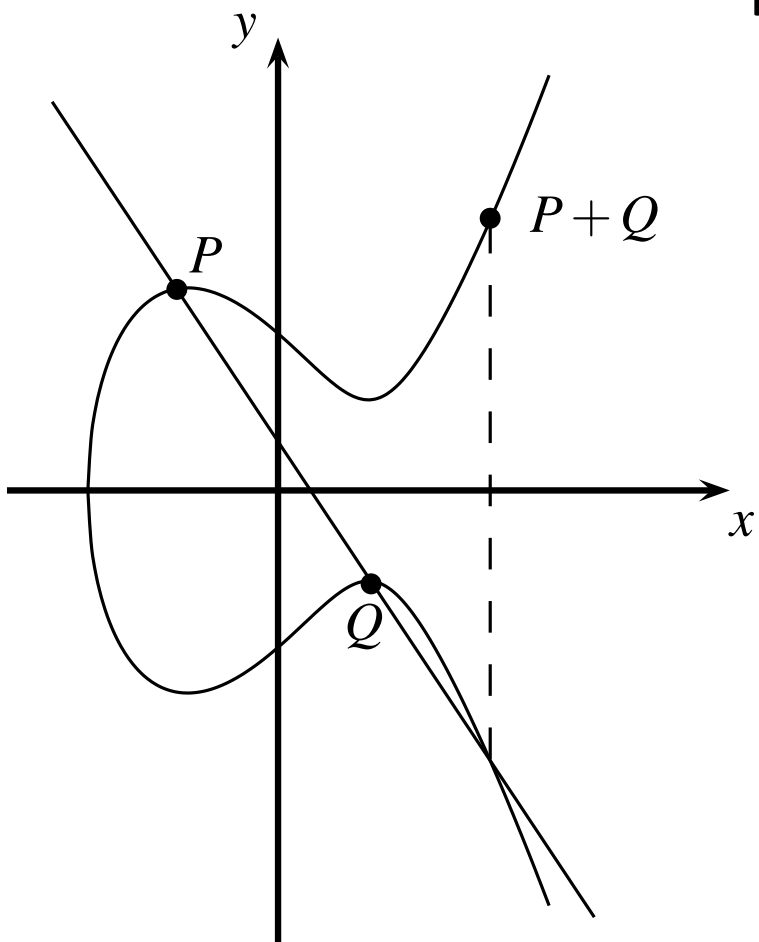
# Phép toán nhóm trên EC

- Ký hiệu phép toán nhóm bởi ký hiệu cộng “+”.
- Cho hai điểm  $P = (x_1, y_1)$  và  $Q = (x_2, y_2)$
- Ta phải tính tọa độ của điểm thứ ba R thoả mãn:

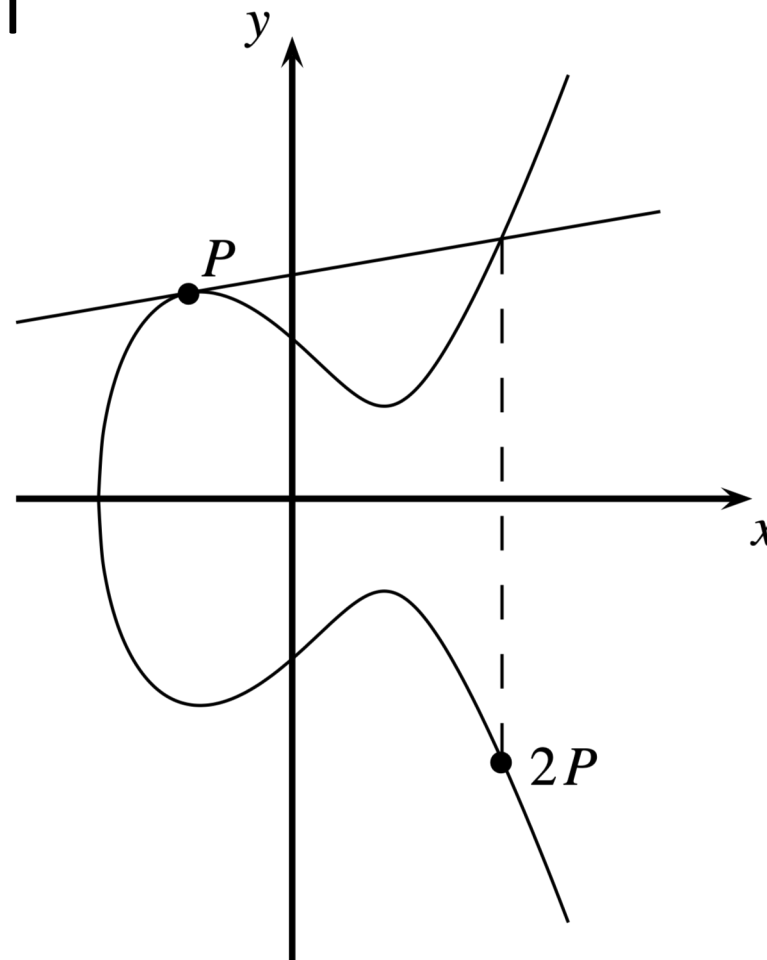
$$\begin{aligned} P + Q &= R \\ (x_1, y_1) + (x_2, y_2) &= (x_3, y_3) \end{aligned}$$

- **Phép cộng điểm  $P + Q$ :** Trường hợp  $R = P + Q$  và  $P \neq Q$
- **Nhân đôi điểm  $P + P$ :** Trường hợp  $P + Q$  nhưng  $P = Q$ .

# Phép toán nhóm



Cộng điểm  $P + Q$



Nhân đôi  $P + P = 2P$

# Phép toán cộng và nhân đôi các điểm

$$\begin{aligned}x_3 &= s^2 - x_1 - x_2 \mod p \\ y_3 &= s(x_1 - x_3) - y_1 \mod p\end{aligned}$$

với

$$s = \begin{cases} (y_2 - y_1)/(x_2 - x_1) \mod p & \text{if } P \neq Q \\ (3x_1^2 + a)/(2y_1) \mod p & \text{if } P = Q \end{cases}$$



Ví dụ

Xét đường cong

$$E: y^2 = x^3 + 2x + 2 \mod 17$$

Ta muốn nhân đôi điểm  $P = (5,1)$ .

$$2P = P + P = (5,1) + (5,1) = (x_3, y_3).$$

$$s = (3x_1^2 + a)/(2y_1) = (2 \cdot 1)^{-1}(3 \cdot 5^2 + 2) = 2^{-1} \cdot 9 = 13 \mod 17$$

$$x_3 = s^2 - x_1 - x_2 = 13^2 - 5 - 5 = 6 \mod 17.$$

$$y_3 = s(x_1 - x_3) - y_1 = 13(5 - 6) - 1 = -14 = 3 \mod 17$$

$$2P = (5,1) + (5,1) = (6,3)$$

# Tính toán với Sagemath

```
sage: E = EllipticCurve(GF(17),[2,2])
sage: E
Elliptic Curve defined by  $y^2 = x^3 + 2x + 2$  over
Finite Field of size 17
sage: P = E(5,1)
sage: Q = P + P
sage: print Q
(6 : 3 : 1)
sage: E.is_on_curve(6,3)
True
```

# Luật cộng đầy đủ cho EC

1.  $\mathcal{O} + \mathcal{O} = \mathcal{O}$ .

2.  $\mathcal{O} + (x_2, y_2) = (x_2, y_2)$ .

3.  $(x_1, y_1) + \mathcal{O} = (x_1, y_1)$ .

4.  $(x_1, y_1) + (x_1, -y_1) = \mathcal{O}$ .

5. cho  $y_1 \neq 0$ ,  $(x_1, y_1) + (x_1, y_1) = (\lambda^2 - 2x_1, \lambda(x_1 - x_3) - y_1)$   
với  $\lambda = (3x_1^2 + a)/2y_1$ .

6. cho  $x_1 \neq x_2$ ,  $(x_1, y_1) + (x_2, y_2) = (\lambda^2 - x_1 - x_2, \lambda(x_1 - x_3) - y_1)$   
với  $\lambda = (y_2 - y_1)/(x_2 - x_1)$ .

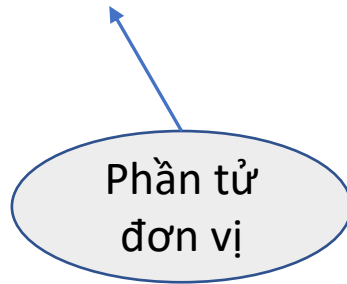
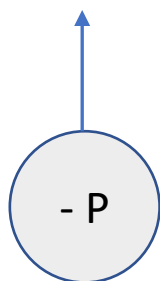
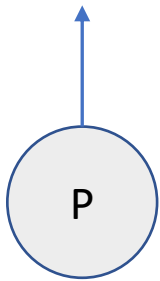
# Kiểm tra các tính chất với Sagemath

1.  $\mathcal{O} + \mathcal{O} = \mathcal{O}$ .

2.  $\mathcal{O} + (x_2, y_2) = (x_2, y_2)$ .

3.  $(x_1, y_1) + \mathcal{O} = (x_1, y_1)$ .

4.  $(x_1, y_1) + (x_1, -y_1) = \mathcal{O}$



```
sage: 0 = P + -P
```

```
sage: 0
```

```
(0 : 1 : 0)
```

```
sage: 0 + 0 == 0
```

```
True
```

```
sage: P + 0
```

```
(5 : 1 : 1)
```

```
sage: P + 0 == P
```

```
True
```

```
sage: 0 + P == P
```

```
True
```

# Hệ toạ độ chiếu

- Điểm chiếu  $(X : Y : Z)$ ,  $Z \neq 0$  tương ứng với điểm trên Affine  $(X/Z, Y/Z)$ .
- Phương trình chiếu của EC là
$$Y^2Z = X^3 + aXZ^2 + bZ^3.$$
- Điểm tại vô cực  $\mathcal{O}$  tương ứng với  $(0:1:0)$ , và phần tử nghịch đảo của  $(X: Y: Z)$  là  $(X: -Y: Z)$ .

# Lợi ích của hệ tọa độ chiếu

- Tính toán phép “+” hiệu quả hơn do tránh được phép nghịch đảo trên trường hữu hạn
- Phép toán cơ bản  $k P$  trở nên dễ dàng

$$(x', y') = 2(x, y)$$

$$s = \frac{3x^2 + a}{2y}$$
$$x' = s^2 - 2x$$
$$y' = s(x - x') - y$$

$$(X' : Y' : Z') = 2(X : Y : Z)$$

$$X' = 2XY(3X^2 + aZ^2)^2 - 8Y^2XZ$$
$$Y' = (3X^2 + aZ^2)(12Y^2XZ - (3X^2 + aZ^2)^2) - 8Y^4Z^2$$
$$Z' = 8Y^3Z^3$$

# Tính toán với Sagemath

```
sage: E = EllipticCurve(GF(17), [2, 2])
sage: E
Elliptic Curve defined by
 $y^2 = x^3 + 2x + 2$ 
over Finite Field of size 17
sage: for P in E:
.....:     print P
.....:
(0 : 1 : 0)
(0 : 6 : 1)
(0 : 11 : 1)
(3 : 1 : 1)
(3 : 16 : 1)
```

```
(5 : 1 : 1)
(5 : 16 : 1)
(6 : 3 : 1)
(6 : 14 : 1)
(7 : 6 : 1)
(7 : 11 : 1)
(9 : 1 : 1)
(9 : 16 : 1)
(10 : 6 : 1)
(10 : 11 : 1)
(13 : 7 : 1)
(13 : 10 : 1)
(16 : 4 : 1)
(16 : 13 : 1)
```

# Nội dung

1. Đường cong Elliptic (Elliptic Curve, EC)
- 2. Bài toán Logarit rời rạc trên EC**
3. Giao thức trao đổi khoá Diffie-Hellman trên EC



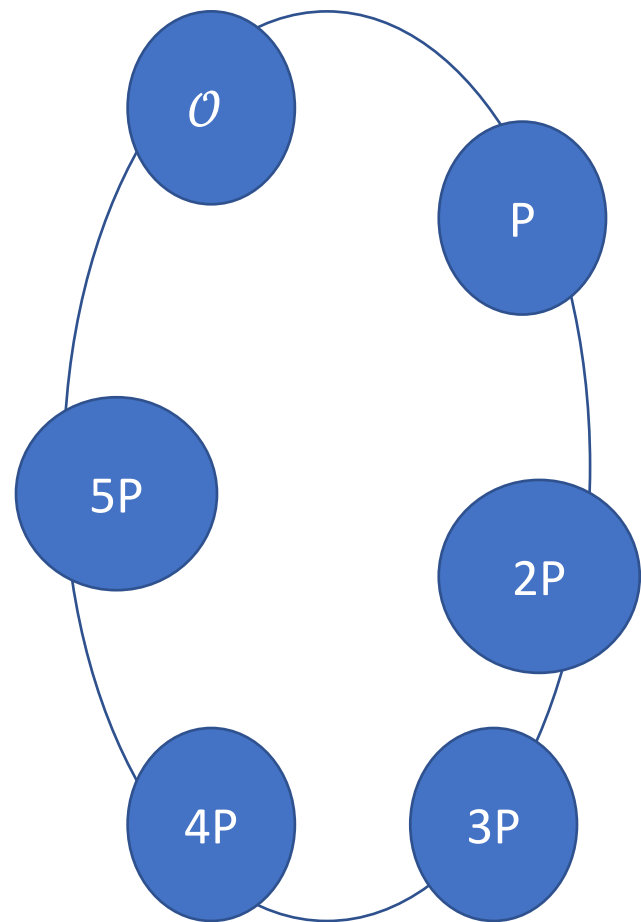
# Nhóm con vòng (cyclic)

## Định lý.

Các điểm trên đường cong Elliptic cùng với điểm  $\mathcal{O}$  có nhóm con vòng.

Dưới một số điều kiện các điểm trên EC lập thành một nhóm vòng.

|               |                |                 |                     |
|---------------|----------------|-----------------|---------------------|
| $P = (5,1)$   | $6P = (16,13)$ | $11P = (13,10)$ | $16P = (10,11)$     |
| $2P = (6,3)$  | $7P = (0,6)$   | $12P = (0,11)$  | $17P = (6,14)$      |
| $3P = (10,6)$ | $8P = (13,7)$  | $13P = (16,4)$  | $18P = (5,16)$      |
| $4P = (3,1)$  | $9P = (7,6)$   | $14P = (9,1)$   | $19P = \mathcal{O}$ |
| $5P = (9,16)$ | $10P = (7,11)$ | $15P = (3,16)$  |                     |

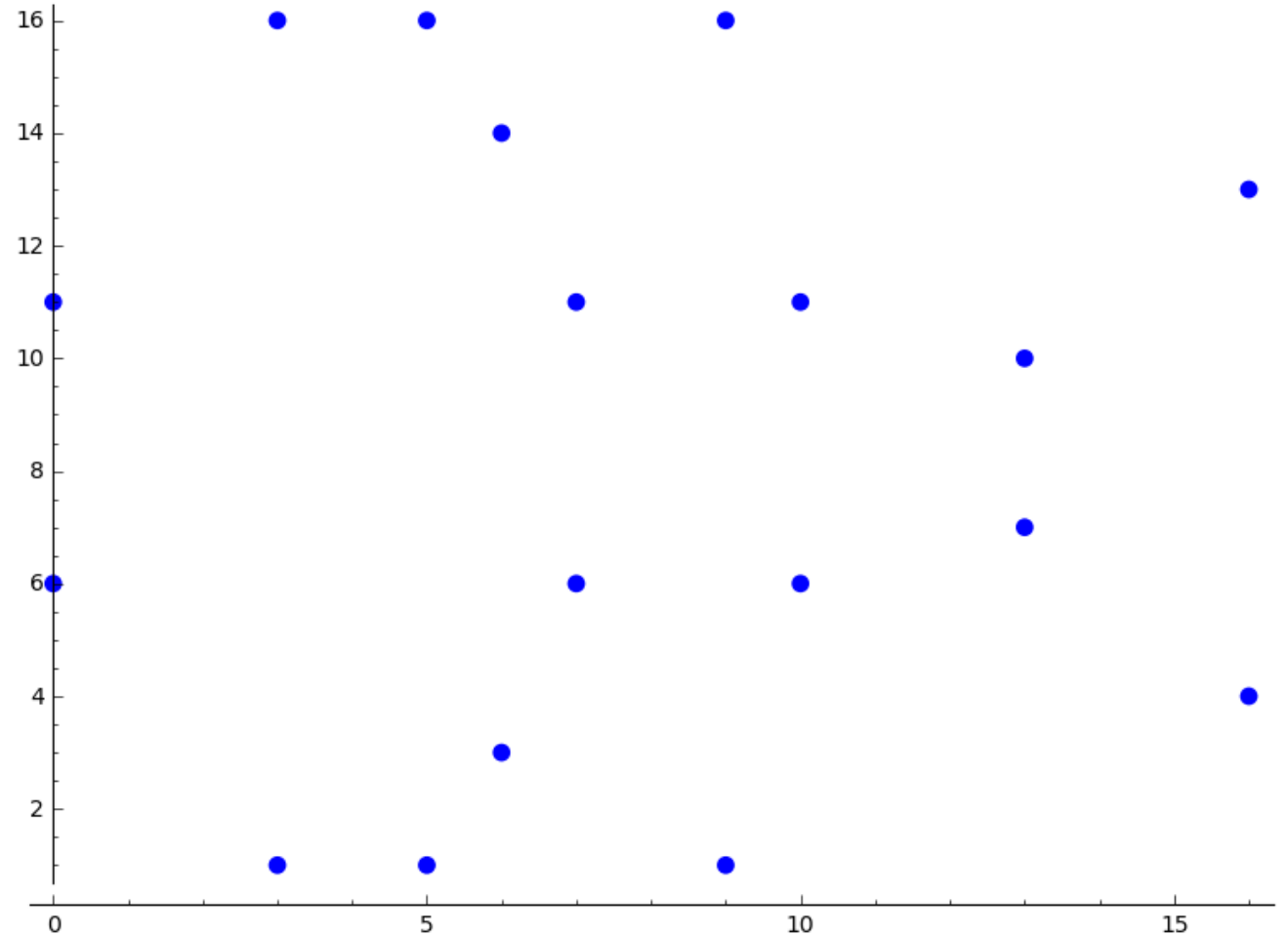


$$E: \quad y^2 = x^3 + 2x + 2 \pmod{17}$$

Tính  $\log_P(Q)$  với  $P = (5,1)$  và  $Q = (10,11)$

|                |                     |
|----------------|---------------------|
| $P = (5,1)$    | $11P = (13,10)$     |
| $2P = (6,3)$   | $12P = (0,11)$      |
| $3P = (10,6)$  | $13P = (16,4)$      |
| $4P = (3,1)$   | $14P = (9,1)$       |
| $5P = (9,16)$  | $15P = (3,16)$      |
| $6P = (16,13)$ | $16P = (10,11)$     |
| $7P = (0,6)$   | $17P = (6,14)$      |
| $8P = (13,7)$  | $18P = (5,16)$      |
| $9P = (7,6)$   | $19P = \mathcal{O}$ |
| $10P = (7,11)$ |                     |

$E: y^2 = x^3 + 2x + 2 \pmod{17}$

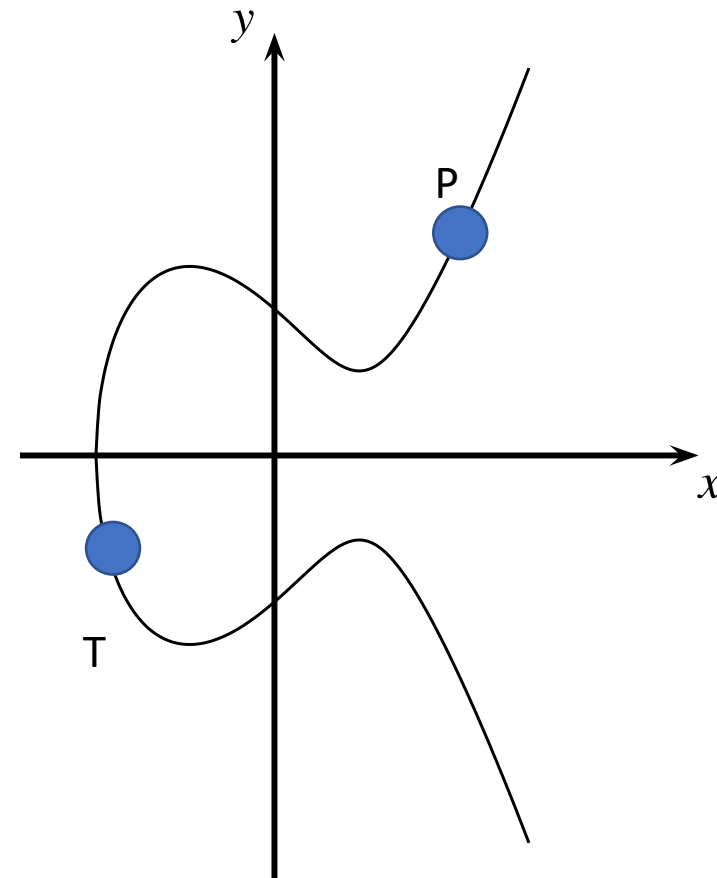


# Bài toán logarit rời rạc trên EC (ECDLP)

**ĐN.** Cho đường cong elliptic  $E$ . Ta xét một điểm  $P$  và điểm khác  $T$ .

Bài toán DL nhằm tìm số nguyên  $d$  thoả mãn

$$\underbrace{P + P + \cdots + P}_{d \text{ times}} = dP = T.$$



# Bài tập

Xét đường cong

$$E: y^2 = x^3 + 2x + 2 \pmod{17}$$

Ta đã tính các “mũ” của P.

|               |                |                 |                     |
|---------------|----------------|-----------------|---------------------|
| $P = (5,1)$   | $6P = (16,13)$ | $11P = (13,10)$ | $16P = (10,11)$     |
| $2P = (6,3)$  | $7P = (0,6)$   | $12P = (0,11)$  | $17P = (6,14)$      |
| $3P = (10,6)$ | $8P = (13,7)$  | $13P = (16,4)$  | $18P = (5,16)$      |
| $4P = (3,1)$  | $9P = (7,6)$   | $14P = (9,1)$   | $19P = \mathcal{O}$ |
| $5P = (9,16)$ | $10P = (7,11)$ | $15P = (3,16)$  |                     |

Với  $P = (5,1)$  và  $T = (16,4)$ , hãy tìm số nguyên  $d$  sao cho  $P = T$ .

# Số điểm của EC

## Hass's Theorem:

Cho đường cong  $E$  modun  $p$ , số điểm trên đường cong ký hiệu bởi  $\#E$  và bị chặn bởi:

$$p + 1 - \sqrt{p} \leq \#E \leq p + 1 + 2\sqrt{p}$$

- $\#E \approx p$
- Nếu ta cần một đường cong với số điểm  $2^{160}$  ta phải sử dụng số nguyên tố cỡ 160 bit

# Tính an toàn

- Mọi giao thức EC dựa trên tính khó giải của bài toán ECDLP
- Nếu EC được chọn cẩn thận, thuật toán tốt nhất để tính ECDLP cần  $\approx \sqrt{p}$  bước.
- VD:  $p \approx 2^{160}$

tấn công cần  $\approx \sqrt{2^{160}} = 2^{80}$  bước

# Nội dung

1. Đường cong Elliptic (Elliptic Curve, EC)
2. Bài toán Logarit rời rạc trên EC
3. **Giao thức trao đổi khoá Diffie-Hellman trên EC**

# Pha 1: Tham số miền cho ECDH

1. Chọn một số nguyên tố  $p$  và đường cong

$$E: \quad y^2 = x^3 + ax + b \pmod{p}$$

2. Chọn điểm  $P = (x_P, y_P)$



## Pha 2: Trao đổi khoá

Alice

Chọn  $\mathbf{a} \in \{2, \dots, \#E - 1\}$

$$A = aP$$

Bob

Chọn  $\mathbf{b} \in \{1, \dots, \#E - 1\}$

$$B = bP$$

$$a\mathbf{B} = a(bP) = \mathbf{k}_{AB} = abP = bA = b(aP)$$

# Phép nhân với hằng số

```
def scalarmult(n,P):  
    if n == 0: return 0  
    if n == 1: return P  
    R = scalarmult(n//2,P)  
    R=R+R  
    if n % 2: R = R + P  
    return R
```

Thời gian CPU bị chặn bởi

$\log_2(n)$

lần nhân đôi điểm

Trường hợp tồi nhất:

$$31P = 2(2(2(2P + P) + P) + P) + P.$$

4 phép nhân đôi; 4 phép cộng.

Trường hợp trung bình:

$$35P = 2(2(2(2(2P))) + P) + P.$$

5 phép nhân đôi; 2 phép cộng.

# Tính an toàn của giao thức trao đổi khoá Diffie Hellman

- Kẻ tấn công nhìn thấy giá trị  $aP$  và  $bP$
- Và phải tính giá trị  $K_{ab} = abP$
- Khó khăn của tính toán được dẫn từ hai bài toán được tin là khó

## **Bài toán quyết định (DDH):**

- Cho  $(P, aP, bP, cP)$ , hãy kiểm tra liệu  $ab == c$ .



## **Bài toán tính toán Diffie Hellman (CDH):**

- Cho  $(P, aP, bP)$ , hãy tính  $abP$ .

DLP  $\rightarrow$  DH

### Quyết định Diffie Hellman (DDH):

- Cho  $(P, aP, bP, cP)$ , kiểm tra liệu  $ab == c$



### Tính toán Diffie Hellman (CDH):

- Cho  $(P, aP, bP)$ , hãy tính  $abP$ .



Nhiều người tin là "đúng"

### Bài toán logarit rời rạc (DLP)

- Cho  $(P, aP)$ , hãy tính  $a$

# Giả sử tính toán Diffie Hellman

Giả sử tính toán DH đúng trong E nếu:  $P, aP, bP \not\Rightarrow abP$

với mọi thuật toán hiệu quả A:

$$\Pr[ A(P, aP, bP) = abP ] < \text{rất nhỏ}$$

với  $P \leftarrow \{\text{phần tử sinh của } E\}, \quad a, b \leftarrow \mathbb{Z}_n$

# Đường cong P256

Đường cong có dạng

$$y^2 = x^3 - 3x + b \pmod{p}$$

- Số nguyên tố  $p = 2^{256} - 2^{224} + 2^{192} + 2^{96} - 1$
- và b ở hexa là:

b := 5ac635d8 aa3a93e7 b3ebbd55 769886bc 651d06b0  
cc53b0f6 3bce3c3e

- Số nguyên tố gần bằng  $2^{256}$ , số điểm gần bằng  $2^{256}$ .
- Tính logarit rời rạc mất khoảng  $2^{128}$  bước
- Tham số b trong P256 được chọn thế nào?
- P256 được dung rộng rãi trong thực tế

# Bài tập

- Xét đường cong

$$E: y^2 = x^3 + 2x + 2 \bmod 17$$

- Và hai điểm  $P = (5,1)$  và  $Q=(10,6)$  trên  $E$ .
- Điểm  $R = P + Q$  là gì?

1.  $R = (15, 7)$
2.  $R = (3,1)$
3.  $R = \mathcal{O}$

# Bài tập

- Xét đường cong

$$E: y^2 = x^3 + 2x + 2 \pmod{17}$$

- Và hai điểm  $P = (5,1)$  và  $Q=(10,6)$  trên  $E$ .
- Hãy tìm số nguyên  $d$  mà  $1 \leq d \leq \#E$ , thoả mãn:  $dQ = P$ ?

1.  $d = 1$

2.  $d = 13$

3.  $d = 17$

4. Không có số  $d$  như vậy.