Bài 4.3 Hệ mật trên đường cong Elliptic (Elliptic Curves Cryptography – ECC)

I. Tổng quan về đường cong Elliptic:

Chúng ta tiến hành giới thiệu nhanh về lý thuyết hấp dẫn của các đường cong elliptic. Để đơn giản, chúng ta chỉ đề cập đến các đường cong elliptic trên $Z_p$trong đó p là 1 số nguyên tố lớn hơn 3.

Một đường Elliptic (E) trên Z_p được xác định bởi phương trình dạng:

(E) $y^2 = x^3 + ax + b$ (modp) (1)

ở đây a, b thuộc Z_p, với $4a^3 + 27b^2 \neq 0 (\text{mod } p)$, và một điểm đặc biệt O, gọi là điểm vô cực. Tập E(Z_p) bao gồm tất cả các điểm (x, y), với x thuộc Z_p và y thuộc Z_p, thỏa mãn phương trình (1), cùng với điểm vô cực O.

Ví dụ 1.

Cho p = 23 và xét đường cong Elliptic E: $y^2 = x^3 + x + 1$ (mod23) . Chú ý rằng

$4a^3 + 27b^2 \neq 4 + 27 (\text{mod}\, 23) = 8 \neq 0$.

Vậy E là một đường cong Elliptic trên Z_{23}.

Bây giờ ta xét các phần tử thặng dư bậc hai Q_{23} trong

$$Z_{23} = \{0, 1, 2, \ \ldots \ , 22\} :$$

$x^2 \bmod p$	$(p-x)^2 \bmod p$	$=$
$1^2 \bmod 23$	$22^2 \bmod 23$	1
$2^2 \bmod 23$	$21^2 \bmod 23$	4
$3^2 \bmod 23$	$20^2 \bmod 23$	9
$4^2 \bmod 23$	$19^2 \bmod 23$	16
$5^2 \bmod 23$	$18^2 \bmod 23$	2
$6^2 \bmod 23$	$17^2 \bmod 23$	13
$7^2 \bmod 23$	$16^2 \bmod 23$	3
$8^2 \bmod 23$	$15^2 \bmod 23$	18
$9^2 \bmod 23$	$14^2 \bmod 23$	12
$10^2 \bmod 23$	$13^2 \bmod 23$	8
$11^2 \bmod 23$	$12^2 \bmod 23$	6

Do đó, tập bao gồm $\frac{p-1}{2}=11$ phần tử thẳng dư bậc hai trong Q_{23} là:

$$\mathbf{Q}_{23} = \{1, 2, 3, 4, 6, 8, 9, 12, 13, 16, 18\}.$$

Bây giờ, với $0 \leq x < p = 23$, ta tính $y^2 = x^3 + x + 1 \pmod{23}$ và xác định được điểm thuộc $E_{23}(1, 1)$ nếu y^2 thuộc tập thặng dư bậc 2 Q_{23}:

x	0	1	2	3	4	5	6	7	8	9	10	11
y^2	1	3	11	8	0	16	16	6	15	3	22	9
$y^2 \in \mathbf{Q}_{23}$?	yes	yes	no	yes	no	yes	yes	yes	no	yes	no	yes
y_1	1	7		10	0	4	4	11		7		3
y_2	22	16		13	0	19	19	12		16		20

x	12	13	14	15	16	17	18	19	20	21	22
y^2	16	3	22	10	19	9	9	2	17	14	22
$y^2 \in \mathbf{Q}_{23}$?	yes	yes	no	no	no	yes	yes	yes	no	no	no
y_1	4	7				3	3	5			
y_2	19	16				20	20	18			

Do đó, ta có các điểm trên $E_{23}(1, 1)$ là điểm vô cực O và các điểm sau:

(0, 1)	(6, 4)	(12, 19)
(0, 22)	(6, 19)	(13, 7)
(1, 7)	(7, 11)	(13, 16)
(1, 16)	(7, 12)	(17, 3)
(3, 10)	(9, 7)	(17, 20)
(3, 13)	(9, 16)	(18, 3)
(4, 0)	(11, 3)	(18, 20)
(5, 4)	(11, 20)	(19, 5)
(5, 19)	(12, 4)	(19, 18)

k	$\lambda = \frac{y_2 - y_1}{x_2 - x_1}$ (if $P \neq Q$) or $\lambda = \frac{3x_1^2 + a}{2y_1}$ if $P = Q$	x_3 $\lambda^2 - x_1 - x_2 \bmod 23$	y_3 $\lambda(x_1 - x_3) - y_1 \bmod 23$	kP (x_3, y_3)
1				(3,10)
2	6	7	12	(7,12)
3	12	19	5	(19,5)
4	4	17	3	(17,3)
5	11	9	19	(9,16)
6	1	12	4	(12,4)
7	7	11	3	(11,3)
8	2	13	16	(13,16)
9	19	0	1	(0,1)
10	3	6	4	(6,4)
11	21	18	20	(18,20)
12	16	5	4	(5,4)
13	20	1	7	(1,7)
14	13	4	0	(4,0)
15	13	1	16	(1,16)
16	20	5	19	(5,19)
17	16	18	3	(18,3)
18	21	6	19	(6,19)
19	3	0	22	(0,22)
20	19	13	7	(13,7)
21	2	11	20	(11,20)
22	7	12	19	(12,19)
23	1	9	7	(9,7)
24	11	17	20	(17,20)
25	4	19	18	(19,18)
26	12	7	11	(7,11)
27	6	3	13	(3,13)

Đồ thị của $E = E_p(a, b) = E_{23}(1, 1)$ như sau:

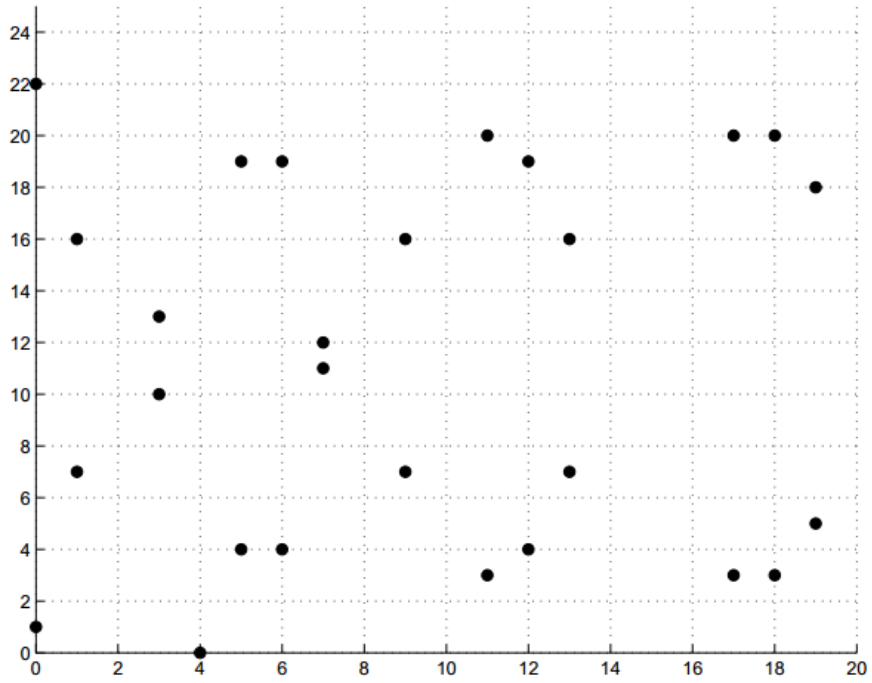


Figure 2: Scatterplot of elliptic group $E_p(a, b) = E_{23}(1, 1)$.

I.2 Quy tắc cộng và nhân trên các điểm thuộc đường cong Elliptic $E_p(a, b)$:

Trên các điểm thuôc $E_p(a, b)$ ta đưa vào phép cộng hai điểm

thuộc $E_p(a, b)$. Với phép toán cộng này, $E_p(a, b)$ trở thành một nhóm cộng. phép toán được xác định như sau:

a) Các tính chất của phép cộng điểm:

(i) P + O = P với mọi P thuộc $E_p(a, b)$;

(ii) Nếu P=(x, y) thuộc $E_p(a, b)$, thì (x, y) + (x, - y) = O. Điểm (x, - y) ký hiệu là – P, nó được gọi là điểm đối của P, nghĩa là nó cũng thuộc $E_p(a, b)$.

(iii)Cho P = (x_1, y_1) thuộc $E_p(a, b)$ và Q = (x_2, y_2) thuộc $E_p(a, b)$, ở đây, P≠-Q. Khi đó, P + Q = (x_3, y_3), ở đây:

$$x_3 = \lambda^2 - x_1 - x_2$$

$$y_3 = \lambda(x_1 - x_3) - y_1$$

Trong đó:

$$\lambda = \begin{cases} \dfrac{y_2 - y_1}{x_2 - x_1}, khi\ P \neq Q \\ \dfrac{3x_1^2 + a}{2y_1}, khi\ P = Q \end{cases}$$

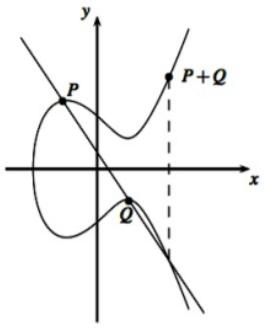
Adding Points

Let $P = (x_P, y_P)$, $Q = (x_Q, y_Q)$ and $R = (x_R, y_R)$ be points on E.

1. Add the point at infinity to itself.
   $\mathcal{O} + \mathcal{O} = \mathcal{O}$
2. Add the point at infinity to any other point.
   $P + \mathcal{O} = \mathcal{O} + P = P$
3. Add two points with the same x-coordinates and different (or equal to 0) y-coordinates: $x_Q = x_P$ and $y_Q = -y_P$.
   $P + Q = \mathcal{O}$

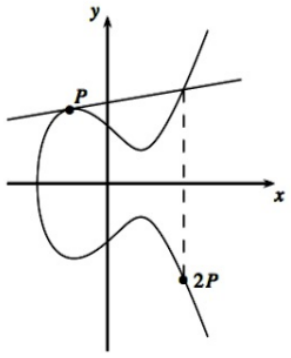
Adding Points

4. Add two points with different x-coordinates.
   $P + Q = R$
   $x_R = \lambda^2 - x_P - x_Q$
   $y_R = \lambda(x_P - x_R) - y_P$
   $\lambda = (y_Q - y_P)(x_Q - x_P)^{-1}$



Adding Points

5. Add a point to itself (*point doubling*).
   $P + P = R$
   $x_R = \lambda^2 - 2x_P$, $y_R = \lambda(x_P - x_R) - y_P$
   $\lambda = (3x_P^2 + a)(2y_P)^{-1}$



EC Groups

As noted before, elliptic curves mod p are finite sets of points.

The set of points on E forms a group given the $+$ operator. The group operator is defined using the addition law.

The group is abelian since $P + Q = Q + P$.

Notation:
$E(\mathbb{F}_p)$ denotes an elliptic curve group over $\mathbb{F}_p$.
$\#E(\mathbb{F}_p)$ denotes the order (cardinality) of $E(\mathbb{F}_p)$.

Ví dụ phép cộng điểm trên đường cong Elliptic

Chúng ta xét đường cong Elliptic trong ví dụ trên:

1. Giả sử P = (3, 10) và Q = (9, 7). Khi đó, P + Q = (x_3, y_3) được tính như sau:

$$\lambda = \frac{7-10}{9-3} = \frac{-3}{6} = \frac{-1}{2} = 11 \in Z_{23}$$

$$x_3 = 11^2 - 3 - 9 = -6 = 17 (\mathrm{mod}\, 23)$$

$$y_3 = 11(3-(-6)) - 10 = 11(9) - 10 = 89 = 20 (\mathrm{mod}\, 23)$$

Vậy, P + Q = (17, 20).

2. Giả sử P = (3, 10). Khi đó, 2P=P+ P = (x_3, y_3) được tính như sau:

$$\lambda = \frac{3(3^2)+1}{20} = \frac{5}{20} = \frac{1}{4} = 6 \in Z_{23}$$

$$x_3 = 6^2 - 6 = 30 = 7 (\mathrm{mod}\, 23)$$

$$y_3 = 6(3-7) - 10 = -24 - 10 = -11 = 12 (\mathrm{mod}\, 23)$$

Vậy, 2P = (7, 12).

Why points over an EC form a group?

Definition

A group $(G, \circ)$ is a set G with a binary operation $\circ : G \times G \to G$ such that the following three axioms are satisfied:

Associativity: For all $a, b, c \in G$ the equation $(a \circ b) \circ c = a \circ (b \circ c)$ holds.

Identity element: There is an element $e \in G$ s.t. for all $a \in G$ the equation $e \circ a = a \circ e = a$ holds.

Inverse element: For each $a \in G$ there exists an element $b \in G$ s.t. $a \circ b = b \circ a = e$.

Why points over an EC form a group?

Q: Does it really work?

Associativity: $(P + Q) + Z \stackrel{?}{=} P + (Q + Z)$

Identity element: What is it?

Inverse element: What is it?

Why points over an EC form a group?

Associativity: Points can be added in any order.

Identity element: $\mathcal{O}$ is an identity with respect to addition.

Inverse element: Every point on E has an inverse with respect to addition: $P + (-P) = \mathcal{O}$ where $P = (x_P, y_p)$ and $-P = (x_P, -y_P)$.

Therefore, $(E, +)$ is a group.

Additionally, the group operator $+$ is commutative since $P + Q = Q + P$. Hence, $(E, +)$ in an abelian group.

Do lịch sử để lại, phép toán nhóm trên đường cong elliptic $E_p(a, b)$ được gọi là phép cộng. Ngược lại, phép toán nhóm trong Z_p^* được gọi là phép nhân. Sự khác biệt trong ký hiệu phép công và ký hiệu nhân đôi khi có thể gây nhầm lẫn.
Bảng 1
cho thấy sự tương ứng giữa các ký hiệu được sử dụng cho hai nhóm trên Z_p^* và trên $E_p(a, b)$:

Group	$\mathbf{Z}_p^*$	$E(\mathbf{Z}_p)$
Group elements	Integers $\{ 1, 2, \ldots, p - 1 \}$	Points (x, y) on E plus O
Group operation	multiplication modulo p	addition of points
Notation	Elements: g, h	Elements: P, Q
	Multiplication: $g \bullet h$	Addition: $P + Q$
	Inverse: g^{-1}	Negative: $-P$
	Division: g / h	Subtraction: $P - Q$
	Exponentiation: g^a	Multiple: aP
Discrete Logarithm Problem	Given $g \in \mathbf{Z}_p^*$ and $h = g^a \bmod p$, find a	Given $P \in E(\mathbf{Z}_p)$ and $Q = aP$, find a.

Table 1: Correspondence between $\mathbf{Z}_p^*$ and $E(\mathbf{Z}_p)$ notation.

Phép nhân kP với k thuộc Z_p nhận được bằng cách lặp lại phép cộng điểm trên $E_p(a, b)$ và ta có bảng kết quả sau:

k	$\lambda = \frac{y_2 - y_1}{x_2 - x_1}$ (if $P \neq Q$) or $\lambda = \frac{3x_1^2 + a}{2y_1}$ if $P = Q$	x_3 $\lambda^2 - x_1 - x_2 \bmod 23$	y_3 $\lambda(x_1 - x_3) - y_1 \bmod 23$	kP (x_3, y_3)
1				(3,10)
2	6	7	12	(7,12)
3	12	19	5	(19,5)
4	4	17	3	(17,3)
5	11	9	19	(9,16)
6	1	12	4	(12,4)
7	7	11	3	(11,3)
8	2	13	16	(13,16)
9	19	0	1	(0,1)
10	3	6	4	(6,4)
11	21	18	20	(18,20)
12	16	5	4	(5,4)
13	20	1	7	(1,7)
14	13	4	0	(4,0)
15	13	1	16	(1,16)
16	20	5	19	(5,19)
17	16	18	3	(18,3)
18	21	6	19	(6,19)
19	3	0	22	(0,22)
20	19	13	7	(13,7)
21	2	11	20	(11,20)
22	7	12	19	(12,19)
23	1	9	7	(9,7)
24	11	17	20	(17,20)
25	4	19	18	(19,18)
26	12	7	11	(7,11)
27	6	3	13	(3,13)

Computations on Elliptic Curves – Example 3

- Example: Given $E: y^2 = x^3+2x+2 \bmod 17$ and point $P=(5,1)$
  Goal: Compute $2P = P+P = (5,1)+(5,1)= (x_3, y_3)$

$$s = \frac{3x_1^2 + a}{2y_1} \bmod p = (2\cdot 1)^{-1}(3\cdot 5^2+2) = 2^{-1}\cdot 9 \equiv 9\cdot 9 \equiv 13 \bmod 17$$

$$x_3 = s^2 - x_1 - x_2 = 13^2 - 5 - 5 = 159 \equiv 6 \bmod 17$$
$$y_3 = s(x_1-x_3) - y_1 = 13(5 - 6) - 1 = -14 \equiv 3 \bmod 17$$

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

Verify that $(6,3)$ is a point on the curve:

$3^2 = 9$, $6^3 + 12 + 2 = 36\cdot 6 + 14 \equiv 2\cdot 6 + 14 = 26 \equiv 9 \bmod 17$

$P+2P=(5,1)+(6,3)=(10,6)$ since

$$s = \frac{y_2 - y_1}{x_2 - x_1} \bmod p = (3-1)/(6-5) = 2\,(1)^{-1} \equiv 2 \bmod 17$$

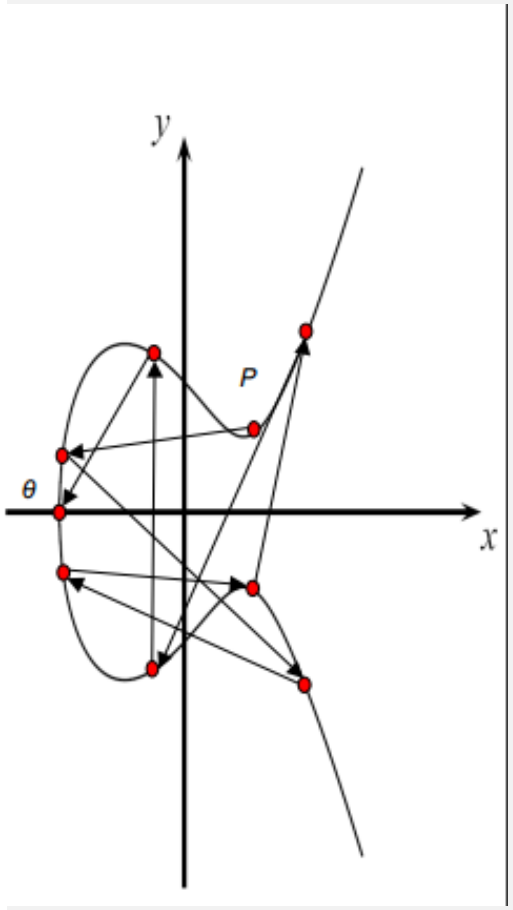
$x_3 = s^2 - x_1 - x_2 = 4 - 11 = -7 \equiv 10 \bmod 17$;

$y_3 = s(x_1 - x_3) - y_1 = -10 - 1 = -11 \equiv 6 \bmod 17$

- The points on an elliptic curve and the point θ form cyclic subgroups

$2P = (5,1)+(5,1) = (6,3)$;	$11P = (13,10)$
$3P = 2P+P = (10,6)$	$12P = (0,11)$
$4P = (3,1)$	$13P = (16,4)$
$5P = (9,16)$	$14P = (9,1)$
$6P = (16,13)$	$15P = (3,16)$
$7P = (0,6)$	$16P = (10,11)$
$8P = (13,7)$	$17P = (6,14)$
$9P = (7,6)$	$18P = (5,16)$
$10P = (7,11)$	$19P = \theta$

This elliptic curve has order $\#E = |E| = 19$ since it contains 19 points in its cyclic group.



Example 4

- Given $E: y^2 = x^3+x+3 \bmod 7$
- There are 6 points on this curve: Θ, (4,1), (6,6), (5,0), (6,1), (4,6)
- Addition table:

+	$\mathcal{O}$	(4, 1)	(6, 6)	(5, 0)	(6, 1)	(4, 6)
$\mathcal{O}$	$\mathcal{O}$	(4, 1)	(6, 6)	(5, 0)	(6, 1)	(4, 6)
(4, 1)	(4, 1)	(6, 6)	(5, 0)	(6, 1)	(4, 6)	$\mathcal{O}$
(6, 6)	(6, 6)	(5, 0)	(6, 1)	(4, 6)	$\mathcal{O}$	(4, 1)
(5, 0)	(5, 0)	(6, 1)	(4, 6)	$\mathcal{O}$	(4, 1)	(6, 6)
(6, 1)	(6, 1)	(4, 6)	$\mathcal{O}$	(4, 1)	(6, 6)	(5, 0)
(4, 6)	(4, 6)	$\mathcal{O}$	(4, 1)	(6, 6)	(5, 0)	(6, 1)

- P=(4,1): 2P=(6,6),3P=(5,0),4P=(6,1),5P=(4,6);6P=Θ
- P=(4,6): 2P=(6,1),3P=(5,0),4P=(6,6),5P=(4,1);6P=Θ
- P=(5,0): 2P= Θ; P=(6,1): 2P=(6,6),3P=Θ

Number of Points on an Elliptic Curve

- How many points can be on an arbitrary elliptic curve?
  - Example 1, $E: y^2 = x^3+2x+2 \bmod 17$ has 19 points
  - However, determining the point count on elliptic curves in general is hard
- But Hasse's theorem bounds the number of points to a restricted interval

Hasse's Theorem:

Given an elliptic curve module p, the number of points on the curve is denoted by #E and is bounded by

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

- Interpretation: The number of points is „close to" the prime p
- Example: To generate a curve with about 2^{160} points, a prime with a length of about 160 bits is required

Elliptic Curve Discrete Logarithm Problem

- Cryptosystems rely on the hardness of the Elliptic Curve Discrete Logarithm Problem (ECDLP)

Definition: Elliptic Curve Discrete Logarithm Problem (ECDLP)

Given a primitive element P and another element T on an elliptic curve E.
The ECDL problem is finding the integer d, where $1 \le d \le \#E$ *such that*

$$\underbrace{P + P + \ldots + P}_{d \text{ times}} = dxP = T$$

- Cryptosystems are based on the idea that *d* is large and kept secret and attackers cannot compute it easily
- If *d* is known, an efficient method to compute the point multiplication *dxP* is required to create a reasonable cryptosystem
  - Known Square-and-Multiply Method can be adapted to Elliptic Curves
  - The method for efficient point multiplication on elliptic curves: Double-and-Add Algorithm

Double-and-Add Algorithm for Point Multiplication

- Double-and-Add Algorithm

  Input: Elliptic curve E, an elliptic curve point P and a scalar d with bits d_i

Output: $T = dP$

Initialization:

$T = P$

Algorithm:

FOR $i = t-1$ DOWNTO 0

  $T = T + T \bmod n$

  IF $d_i = 1$

    $T = T + P \bmod n$

RETURN (T)

Example: $26P = (11010_2)P = (d_4d_3d_2d_1d_0)_2\ P$.

Step		
#0	$P = 1_2P$	inital setting
#1a	$P+P = 2P = 10_2P$	DOUBLE (bit d_3)
#1b	$2P+P = 3P = 10^2\ P+1_2P = 11_2P$	ADD (bit d_3=1)
#2a	$3P+3P = 6P = 2(11_2P) = 110_2P$	DOUBLE (bit d_2)
#2b		no ADD ($d_2 = 0$)
#3a	$6P+6P = 12P = 2(110_2P) = 1100_2P$	DOUBLE (bit d_1)
#3b	$12P+P = 13P = 1100_2P+1_2\ P = 1101_2P$	ADD (bit d_1=1)
#4a	$13P+13P = 26P = 2(1101_2P) = 11010_2P$	DOUBLE (bit d_0)
#4b		no ADD ($d_0 = 0$)

Bài tập về nhà

Hãy xác định các điểm trên đường cong Elliptic $E_{29}(1, 1)$:

$$y^2 = x^3 + x + 1 \pmod{29}$$

Bước 1. Xác định

Q_{29} = 0, 1, 4, 5, 6, 7, 9, 13, 16, 20, 22, 23, 24, 25, 28

II. Một số hệ mật trên đường cong Elliptic”

II.1 Hệ mã khóa công khai EC ElGamal:

Cũng như trong các sơ đồ mã hóa khác, trong hệ mật khóa công khai EC ElGamal, Alice cần gửi tin nhắn cho Bob để Eve không đọc nó được. Để làm như vậy, cả hai sử dụng thuật toán sau:

1. Bob thiết lập khóa công khai của mình bằng cách chọn đường

cong Elliptic E trên trường hữu hạn F_p sao cho bài toán logarithm rời rạc là khó giải trong $E(F_p)$, Bob cũng chọn một số nguyên s làm khóa riêng của Bob. Bob khi đó tính B = sP và công khai E, F_p, P và B. Alice để gửi bản tin của mình sẽ làm như sau:

3. Downloads khóa công khai của Bob E, F_p, P và B.
4. Biểu diễn bản tin của cô ta như như điểm $M \in E(F_p)$.

5. Chọn ngẫu nhiên số nguyên k một cách bí mật và tính $M_1 = kP$.
6. Tính $M_2 = M + kB$.
7. Gửi M_1 và M_2 cho Bob.
8. Bob giải mã bản tin M bằng cách tính $M = M_2 – sM_1$.

Bob có thể nhận được M bởi vì:

$M_2 – sM_1 = (M + kB) – s(kP) = M + k(sP) – skP = M$.

Do Eve không có khóa riêng của Bob nên anh ta không thể tính M. Eve chỉ có cách là tìm s

để giải bài toán logarithm rời rạc, nhận được B và P và biết rằng B = sP, tìm ra s.

Ví dụ 1.

Example *(Elliptic curve encryption):*

Consider the following elliptic curve:

$$\begin{aligned} y^2 &= x^3 + ax + b \bmod p \\ y^2 &= x^3 - x + 188 \bmod 751 \end{aligned}$$

that is: $a = -1$, $b = 188$, and $p = 751$. The elliptic curve group generated by the above elliptic curve is $E_p(a, b) = E_{751}(-1, 188)$.

Let the generator point $G = (0, 376)$. Then the multiples kG of the generator point G are (for $1 \leq k \leq 751$):

$G = (0, 376)$	$2G = (1, 376)$	$3G = (750, 375)$	$4G = (2, 373)$
$5G = (188, 657)$	$6G = (6, 390)$	$7G = (667, 571)$	$8G = (121, 39)$
$9G = (582, 736)$	$10G = (57, 332)$	...	$761G = (565, 312)$
$762G = (328, 569)$	$763G = (677, 185)$	$764G = (196, 681)$	$765G = (417, 320)$
$766G = (3, 370)$	$767G = (1, 377)$	$768G = (0, 375)$	$769G = O$(point at infinity)

If Alice wants to send to Bob the message M which is encoded as the plaintext point $P_M = (443, 253) \in E_{751}(-1, 188)$. She must use Bob public key to encrypt it. Suppose that Bob secret key is $n_B = 85$, then his public key will be:

$$\begin{aligned} P_B &= n_B G = 85(0, 376) \\ P_B &= (671, 558) \end{aligned}$$

Alice selects a random number $k = 113$ and uses Bob's public key $P_B = (671, 558)$ to encrypt the message point into the ciphertext pair of points:

$$\begin{aligned} P_C &= [(kG), (P_M + kP_B)] \\ P_C &= [113 \times (0, 376), (443, 253) + 113 \times (671, 558)] \\ P_C &= [(34, 633), (443, 253) + (47, 416)] \\ P_C &= [(34, 633), (217, 606)] \end{aligned}$$

Upon receiving the ciphertext pair of points, $P_C = [(34, 633), (217, 606)]$, Bob uses his private key, $n_B = 85$, to compute the plaintext point, P_M, as follows

$$\begin{aligned} (P_M + kP_B) - [n_B(kG)] &= (217, 606) - [85(34, 633)] \\ (P_M + kP_B) - [n_B(kG)] &= (217, 606) - [(47, 416)] \\ (P_M + kP_B) - [n_B(kG)] &= (217, 606) + [(47, -416)] \quad (\text{since } -P = (x_1, -y_1)) \\ (P_M + kP_B) - [n_B(kG)] &= (217, 606) + [(47, 335)] \quad (\text{since } -416 \equiv 335 \pmod{751}) \\ (P_M + kP_B) - [n_B(kG)] &= (443, 253) \end{aligned}$$

and then maps the plaintext point $P_M = (443, 253)$ back into the original plaintext message M.

Ví dụ 2. Sau đây là ví dụ đầu ra của hệ mật khóa công khai EC Elgamal trên đường cong E: $y^2 = x^3 + x + 1$ trong trường $F_{14734520141266665763}$.

ElGamal Public Key Encryption

Program represents exchange between two users, Alice and Bob, to exchange a secret message represented by a point M on E. First Bob publishes the public keys E, a finite field Fp, and two points P and B. B = sP, where s is Bob's private key. Alice then inputs her message M, and her secret integer k. This

program will
compute M1 = kP and M2 = M + kB. It will then find the original message
M = M2 - sM1
Bob, enter an elliptic curve E of the form y^2 = x^3 + Ax^2 + Bx + c
A = ?
0B
= ?
1C
= ?
1O
ver what field Fp?

p = ?
14734520141266665763
Bob, enter your point P = (x,y)
x = ?
72
y = ?
611
Bob, enter your integer s
947
Alice, enter the message you would like to send in the form of point M
= (x,y)
x = ?

3683630035316666441
y = ?
5525445052974999660
Alice enter your secret integer k
97742
Public:
E: y^2 = x^3 + 0x^2 + 1x + 1
P = (72,611), B = (10787375521999759655,1301544751114099523), M1 = (132492021744274304581433881143440817), M2 = (2191766698351684658 2,2267

771891450618491)
Alice Knows:
M = (3683630035316666441,552544505297499966 0), k = 97742
Bob Knows:
s = 947, M = M2 - sM1 = (3683630035316666441,552544505297499966 0)

Ví dụ 3

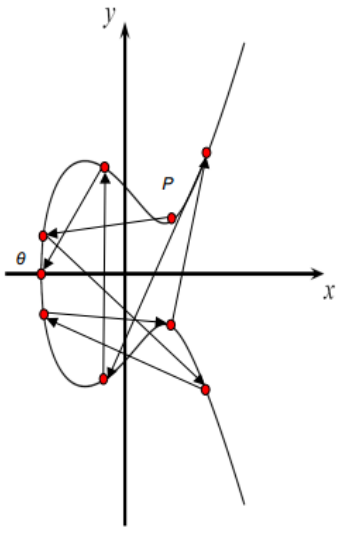
Giả sử ta có đường cong Elliptic

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

- The points on an elliptic curve and the point θ form cyclic subgroups

2P = (5,1)+(5,1) = (6,3);	11P = (13,10)
3P = 2P+P = (10,6)	12P = (0,11)
4P = (3,1)	13P = (16,4)
5P = (9,16)	14P = (9,1)
6P = (16,13)	15P = (3,16)
7P = (0,6)	16P = (10,11)
8P = (13,7)	17P = (6,14)
9P = (7,6)	18P = (5,16)
10P = (7,11)	19P = θ

This elliptic curve has order #E = |E| = 19 since it contains 19 points in its cyclic group.



Bước 1. Khóa công khai của Bob:

$E_{17}(2, 2)$, p=17, P= (9, 16), s=6.

Tính B=6P= (13, 10).

Bước 2. Alice muốn gửi bản tin m, khi đó gắn m với điểm M= (7, 11).

Để mã hóa Alice lấy bí mật 1 số k=9 tính kP=9P=(0,6)=M_1, rồi tính M_2=M+kB=(9,1).

Bản mã (M_1,M_2)=((0,6), (9,1)).

Bước 3. Giải mã

M=M_2 – sM_1 = (9,1) – 6*(0,6)

= ((14 – 6*7)mod19)(5,1)

= 10(5,1)=(7, 11) = M.

Commented [PDL1]:

II.2 Hệ mã hóa Massey - Omura:

Hệ mã Massey-Omura có thể được dùng để gửi khóa riêng hoặc bản tin được mã hóa. Ý tưởng đằng sau hệ mã hóa Massey-Omura như sau: Alice đặt bản tin của mình vào một chiếc hộp và khóa lại bằng khóa riêng của mình, sau đó gửi hộp này tới Bob. Sau đó Bob đặt khóa của mình vào hộp và trả lại hộp cho Alice. Sau đó, Alice tháo khóa của mình và gửi lại cho Bob. Nhận được hộp, Bob

tháo khóa của mình và lấy lại tin nhắn. Quy trình này có thể thực hiện bằng cách dung đường cong elliptic như sau:

Hệ mã hóa Massey-Omura:

1. Alice và Bob thống nhất với nhau đường elliptic E trên trường hữu hạn F_p sao cho bài toán logarithm rời rạc là khó giải trên $E(F_p)$. Giả sử $N = \#E(\mathrm{F})$
2. Alice biểu diễn bản tin của mình bằng điểm $M \in E(F_p)$.

3.Alice chọn số nguyên bí mật m_A với gcd(m_A, N) = 1, tính $M_1 = m_A M$, và gửi M_1 tới Bob.

4.Bob chọn số nguyên bí mật m_B thỏa mãn gcd(m_B, N) = 1, tính $M_2 = m_B M_1$, và gửi M_2 tới Alice.

5.Alice tính $m_A^{-1} \in Z_N$, sau đó tính $M_3 = m_A^{-1} M_2$ và gửi M_3 cho Bob.

6.Bob tính $m_B^{-1} \in Z_N$, sau đó tính $M_4 = m_B^{-1} M_3$. Khi đó M_4 = M.

Chú ý rằng, các khóa riêng của Alice và Bob không liên quan đến nhau, đây là hệ mật khóa không đối xứng.

Massey-Omura Encryption Program represents exchange between two users, Alice and Bob, to exchange a secret message. This program allows the user to input an elliptic curve E over a finite field Fp. A point M on E represents a message

communicated from Alice to Bob is input by Alice.Let N represent the order of the torsion subgroup on E. Then Alice and Bob input secret integers mA and mB, such that (mA,N)=1 and (mB,N)=1. This program will allow the secret exchange of M by computing M1 = mA*M, M2 = mB*M1, M3 = mA^-1*M2, and M4 = mB^-1*M3 = mA*mA^-1*mB*mB^-1*M = M, where

mA^-1 and mB^-1 are the respective multiplicative inverses of mA and mB over Z/NZ.
Enter an elliptic curve of the form y^2 = x^3 + Ax^2 + Bx + C
A = ?
4B
= ?
230
C = ?
-219
Over what field Fp?
p = ?

223
Enter a point (x,y)
x = ?
200
y = ?
148
Enter Alice's secret integer mA
179
Enter Bob's secret integer mB
71
Private
M = (200,148)
mA = 179, mB = 71
mA^-1 = 19, mB^-1 = 31

Public:
E: y^2 = x^3 + 4x^2 + 230x + -219
Fp = Z(mod 223), N = 200
M1 = (174,70) M2 = (73,159)
M3 = (174,153) M4 = M = (200,148)

III. Những ưu điểm của

So với các hệ mật khóa công khai RSA, ElGamal thì với cùng độ mật, hệ mật ECC có độ dài khóa ngắn hơn nhiều lần. Ví dụ, ta có bảng so sánh sau:

Comparison of Key Lengths

Symmetric Key Size (bits)	RSA and Diffie-Hellman Key Size (bits)	Elliptic Curve Key Size (bits)
80	1024	160
112	2048	224
128	3072	256
192	7680	384
256	15360	521

Image retrieved from http://www.nsa.gov/business/programs/elliptic_curve.shtml

Note: The above URL no longer works, and I have been unable to find a replacement URL. See Elliptic curve cryptography: The serpentine course of a paradigm shift for a historical account for how elliptic curve cryptography gained acceptance over many years.