Tìm hiểu về mật mã đường cong Elliptic và ứng dụng

Nguyễn Đức Huy* Lê Thị Thùy Dung† Lưu Hiểu Huy‡

Mục lục

Tóm tắt nội dung

Mật mã đường cong Elliptic là phương pháp tiếp cận mã hóa khóa công khai dựa trên cấu trúc đại số của đường cong Elliptic trên các trường hữu hạn. Đường cong elliptic bao gồm các điểm thỏa mãn phương trình $Y^2 = X^3 + AX + B$ cùng với một điểm O ở vô cực. Chúng tôi sẽ giới thiệu và phân tích hệ mật mã dựa trên đường cong elliptic bao gồm các bài toán Logarit rời rạc, trao đổi khóa, mã hóa - giải mã, chữ kí số, ... và một số ứng dụng của nó trong mật mã như thuật toán phân tích thành nhân tử của đường cong elliptic Lenstra, thuật toán kiểm tra tính nguyên tố Pocklington-Lehmer.

*Khoa Toán, Đại học Khoa học Tự Nhiên, `mtait@math.ucsd.edu`
†Khoa Toán, Đại học Khoa học Tự Nhiên, `craig.timmons@csus.edu`
‡Khoa Toán, Đại học Khoa học Tự Nhiên, `craig.timmons@csus.edu`

1 Giới thiệu

2 Đường cong Elliptic

Một *đường cong Elliptic* là tập nghiệm của một phương trình có dạng

$$Y^2 = X^3 + AX + B$$

Các phương trình thuộc loại này được gọi là *phương trình Weierstrass* sau khi ông đã nghiên cứu chúng trong suốt thế kỉ XIX. Hai ví dụ cho đường cong elliptic:

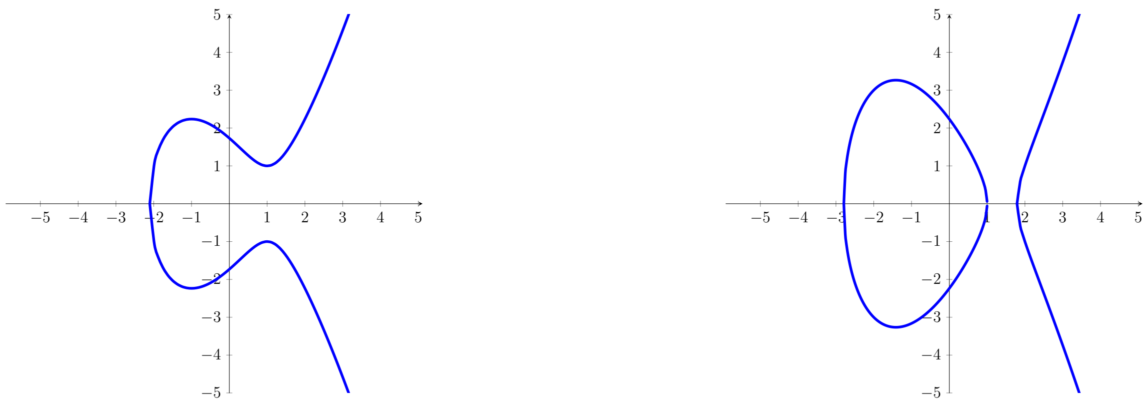
$$E_1 : Y^2 = X^3 - 3X + 3$$

và

$$E_2 : Y^2 = X^3 - 5X + 5$$

được minh họa ở Hình 1

Hình 1: Hình 1



Một điều tuyệt vời của đường cong elliptic là có một cách tự nhiên để chọn hai điểm trên đường cong và “cộng” chúng để tạo ra điểm thứ ba. Phép “cộng” được chúng tôi nhắc đến ở đây là một phép toán kết hợp hai điểm theo cách tương tự với phép cộng thông thường ở một vài khía cạnh (có tính chất giao hoán, kết hợp và có cách nhận dạng), nhưng rất khác ở những phần còn lại. Một trong những cách đơn giản để miêu tả "luật cộng"là sử dụng hình học.

Cho P và Q là hai điểm trên đường cong elliptic E, như minh họa ở Hình 2. Ta bắt đầu vẽ một đường thẳng L đi qua P và Q. Đường thẳng L sẽ cắt E tại ba điểm P, Q và một điểm R thứ ba. Ta lấy đối xứng điểm R qua trục Ox để được điểm R'. Điểm R' này gọi là *tổng của P và Q*, phép “cộng” này không giống phép cộng thông thường. Ta biểu thị phép “cộng” này bằng kí hiệu $\oplus$. Ta viết

$$P \oplus Q = R' \tag{1}$$

Example 1. Cho đường cong elliptic E:

$$Y^2 = X^3 - 15X + 18 \tag{2}$$

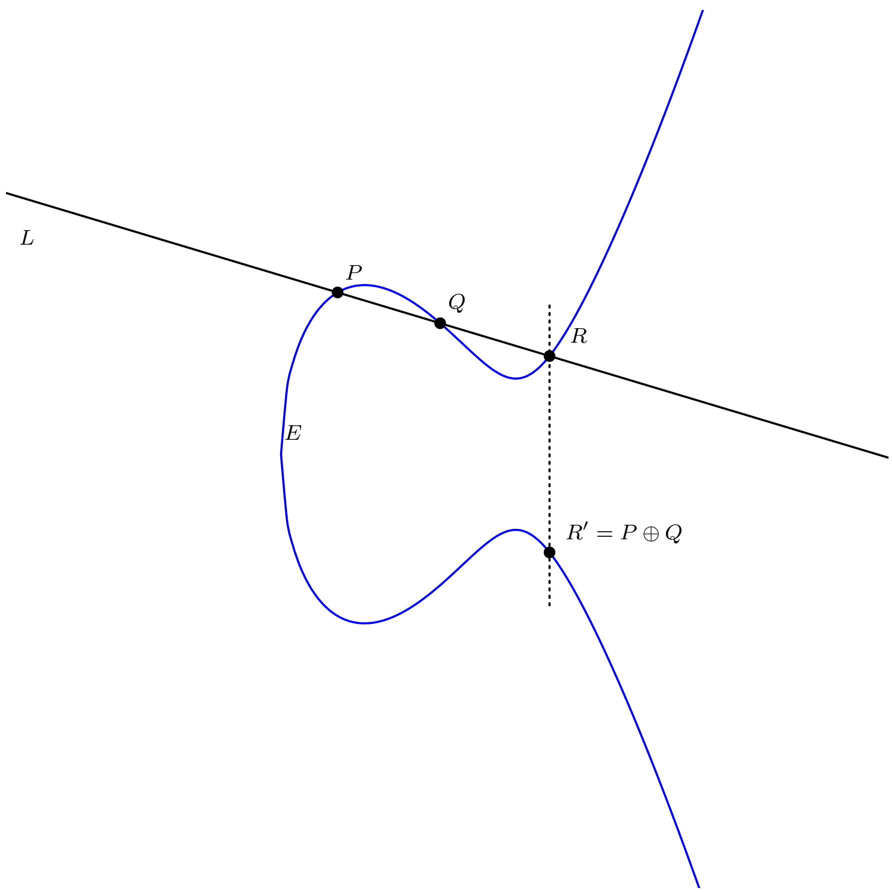
Điểm $P = (7, 16)$ và $Q = (1, 2)$ nằm trên E. Đường thẳng L nối P và Q có phương trình

$$L : Y = \frac{7}{3}X - \frac{1}{3} \tag{3}$$

Để tìm giao điểm của E và L, ta thay Y ở phương trình (3) vào phương trình (2) để tìm X. Ta có

$$\begin{aligned}
(\frac{7}{3}X - \frac{1}{3})^2 &= X^3 - 15X + 18 \\
\frac{49}{9}X^2 - \frac{14}{9}X + \frac{1}{9} &= X^3 - 15X + 18 \\
0 &= X^3 - \frac{49}{9}X^2 - \frac{121}{9}X + \frac{161}{9}
\end{aligned}$$

Hình 2: Hình 2



Thông thường, việc tìm nghiệm của phương trình bậc ba không đơn giản, nhưng ta đã biết trước 2 giao điểm của L và E là P và Q, nên rõ ràng phương trình trên có 2 nghiệm $X = 1$ và $X = 7$. Từ đó, ta dễ dàng tìm được nghiệm còn lại

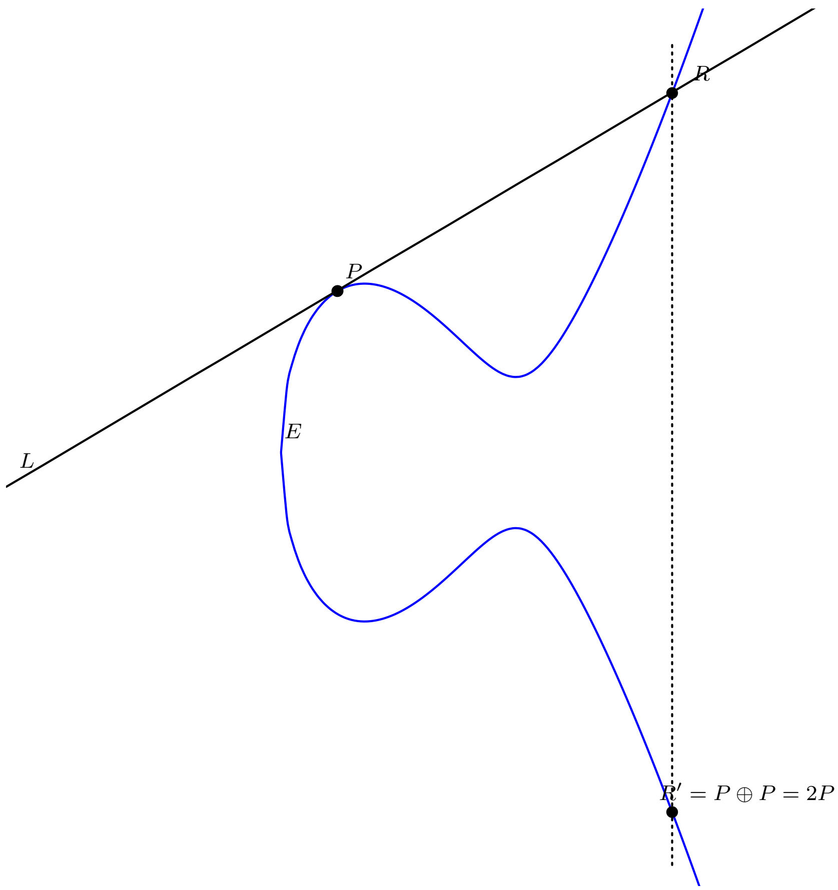
$$X^3 - \frac{49}{9}X^2 - \frac{121}{9}X + \frac{161}{9} = (X - 7) \cdot (X - 1) \cdot (X + \frac{23}{9})$$

Thay $X = -\dfrac{23}{9}$ vào phương trình (3) ta được điểm $R = (-\dfrac{23}{9}, -\dfrac{170}{27})$. Cuối cùng, lấy đối xứng qua trục Ox ta được

$$P \oplus Q = (-\frac{23}{9}, \frac{170}{27})$$

Điều gì xảy ra khi ta cộng điểm P với chính nó? Khi điểm Q tiến dần đến P, đường thẳng L sẽ trở thành tiếp tuyến của E tại P. Vậy, để cộng điểm P với chính nó, ta đơn giản chỉ cần lấy L là tiếp tuyến của E tại P, minh họa ở Hình 3. Khi đó L giao E tại P và một điểm R khác, điểm P được tính 2 lần.

Hình 3: Hình 3



Example 2. Tiếp tục với đường cong E và điểm P ở ví dụ 1, ta tính $P \oplus P$.

Ta tìm độ dốc tại P của E bằng cách đạo hàm 2 vế phương trình (2). Ta được

$$2\frac{dY}{dX} = 3X^2 - 15, \text{ suy ra } \frac{dY}{dX} = \frac{3X^2 - 15}{2Y}$$

Thay tọa độ điểm $P = (7, 16)$ ta được độ dốc $\lambda = \dfrac{33}{8}$, nên đường tiếp tuyến của E tại P có phương trình

$$L : Y = \frac{33}{8}X - \frac{103}{8} \tag{4}$$

Tiếp theo, thay Y ở phương trình (4) vào phương trình (2):

$$\begin{aligned}
(\frac{33}{8}X - \frac{103}{8})^2 &= X^3 - 15X + 18 \\
X^3 - \frac{1089}{64}X^2 + \frac{2919}{32}X - \frac{9457}{64} &= 0 \\
(X-7)^2 . (X - \frac{193}{64}) &= 0
\end{aligned}$$

Ta đã biết trước $X = 7$ là nghiệm bội 2 của phương trình bậc 3 nên dễ dàng phân tích thành nhân tử và tìm được nghiệm còn lại. Cuối cùng, thay $X = \frac{193}{64}$ vào phương trình (4) ta được $Y = -\frac{233}{512}$. Đổi dấu Y ta được

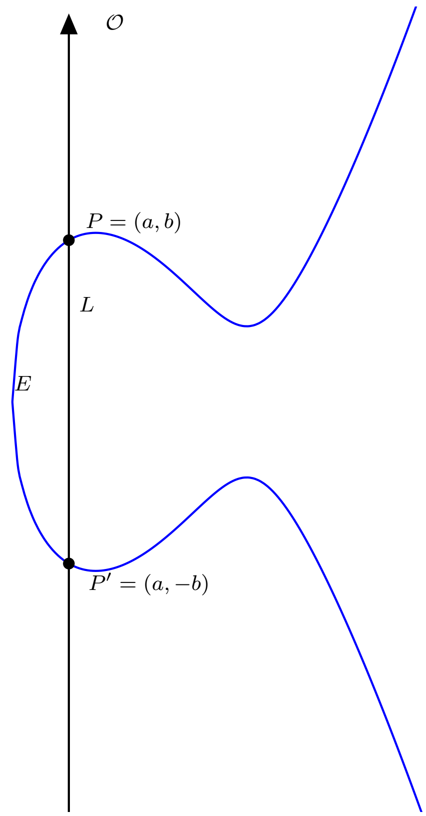
$$P \oplus P = (\frac{193}{64}, \frac{233}{512})$$

Vấn đề thứ hai là khi ta cố gắng cộng điểm $P = (a, b)$ với điểm đối xứng của nó qua trục Ox $P' = (a, -b)$. Đường thẳng L đi qua P và P' có phương trình $x = a$, chỉ cắt E tại 2 điểm P và P'. (Hình 4) Vậy nên không có giao điểm thứ ba. Giải pháp là tạo thêm một điểm $\mathcal{O}$ ở "vô cực". Chính xác hơn, điểm $\mathcal{O}$ không tồn tại trên mặt phẳng Oxy, nhưng ta giả định nó nằm trên mọi đường thẳng đứng. Ta có:

$$P \oplus P' = \mathcal{O}$$

Tiếp theo, ta cần tìm cách cộng điểm $\mathcal{O}$ với điểm $P = (a, b)$ thuộc E. Đường thẳng L nối P với $\mathcal{O}$ là đường thẳng đứng đi qua P và cắt E tại $P' = (a, -b)$. Để cộng P với $\mathcal{O}$, ta lấy điểm đối xứng với P' qua trục Ox, ta được điểm P. Nói cách khác $P \oplus \mathcal{O} = P$, vậy điểm $\mathcal{O}$ có vai trò như số 0 trong phép cộng elliptic.

Hình 4: Hình 4



Example 3. Tiếp tục với đường cong E ở ví dụ 1 và điểm $T = (3, 0)$.

Chú ý điểm T nằm trên E và tiếp tuyến tại T là đường thẳng đứng $X = 3$. Vậy nếu cộng điểm T với chính nó, ta được $T \oplus T = \mathcal{O}$.

Definition 1. Một đường cong elliptic E là tập nghiệm của một phương trình Weierstrass:

$$E : Y^2 = X^3 + AX + B$$

cùng với một điểm $\mathcal{O}$ ở vô cùng, trong đó hằng số A và B thỏa mãn

$$4A^3 + 27B^2 \neq 0$$

Luật cộng trên E được định nghĩa như sau. Cho 2 điểm P và Q là 2 điểm thuộc E. L là đường thẳng nối P và Q, hoặc là đường tiếp tuyến của E tại P nếu $P = Q$. Khi đó, giao điểm của E và L là ba điểm P, Q và R, với $\mathcal{O}$ được hiểu là điểm nằm trên mọi đường thẳng đứng. $R = (a, b)$, tổng của P và Q là điểm $R' = (a, -b)$. Tổng này được ký hiệu là $P \oplus Q$, có thể viết đơn giản $P + Q$.

Ta biểu diễn điểm đối xứng của P bởi $\ominus P = (a, -b)$, hoặc $-P$; ta định nghĩa $P \ominus P$ (hay $P - Q$) là $P \oplus (\ominus Q)$. Tương tự, lặp lại phép cộng nhiều lần là biểu diễn của phép nhân một điểm với một số nguyên,

$$nP = \underbrace{P + P + P + \ldots + P}_{n \text{ số hạng}}$$

Remark 1. Tại sao cần thỏa mãn điều kiện $4A^3 + 27B^2 \neq 0$?

Đại lượng $\Delta_E = 4A^3 + 27B^2$ được gọi là *phân thức của* E. $\Delta_E \neq 0$ là điều kiện để đa thức $X^3 + AX + B$ có 3 nghiệm phân biệt, nếu phân tích thành nhân tử $X^3 + AX + B$ ta được:

$$X^3 + AX + B = (X - e_1)(X - e_2)(X - e_3)$$

trong đó e_1, e_2, e_3 là các số phức, thì

$$4A^3 + 27B^2 \neq 0 \qquad \text{khi và chỉ khi} \qquad e_1, e_2, e_3 \text{ phân biệt}$$

Phép cộng không hoàn toàn đúng đối với đường cong có $\Delta_E = 0$ nên chúng tôi thêm điều kiện $\Delta_E \neq 0$ khi nêu khái niệm đường cong elliptic.

Theorem 2.1. Cho đường cong elliptic E. Luật cộng trên E thỏa mãn các tính chất sau:

(a)	$P + \mathcal{O}$	$=$	$\mathcal{O} + P = P$	$\forall P \in E$	[Cộng với điểm $\mathcal{O}$]
(b)	$P + (-P)$	$=$	$\mathcal{O}$	$\forall P \in E$	[Nghịch đảo]
(c)	$(P + Q) + R$	$=$	$P + (Q + R)$	$\forall P, Q, R \in E$	[Kết hợp]
(d)	$P + Q$	$=$	$Q + P$	$\forall P, Q \in E$	[Giao hoán]

Chứng minh. Như đã giải thích trước đó, dễ thấy tính cộng với điểm $\mathcal{O}$ và tính nghịch đảo là đúng vì $\mathcal{O}$ nằm trên mọi đường thẳng đứng. Tính giao hoán dễ dàng chứng minh vì đường thẳng qua P và Q cũng là đường thẳng qua Q và P.

Phần còn lại cần chứng minh của định lý 2.1 là tính kết hợp. Có nhiều cách để chứng minh tính kết hợp, nhưng không cách nào trong số chúng đơn giản. Sau khi có đủ các kiến thức cần thiết về luật cộng trên E (2.2), bạn đọc có thể sử dụng để tự chứng minh. Có thể tìm thấy những chứng minh rõ ràng hơn ở [1], [4] hoặc [5] và một vài quyển sách khác về đường cong elliptic. □

Tiếp theo, chúng ta sẽ chứng minh một vài công thức để dễ dàng cộng và trừ các điểm trên một đường cong elliptic. Những công thức này sử dụng hình học giải tích, tính toán vi phân và một vài thao tác đại số cơ bản. Chúng tôi đưa kết quả dưới dạng một định lý và đưa ra chứng minh sau đó.

Theorem 2.2 (Thuật toán cộng đường cong Elliptic)**.** Cho

$$E : Y^2 = X^3 + AX + B$$

là một đường cong elliptic và P_1 và P_2 là hai điểm trên E.

1. Nếu $P_1 = \mathcal{O}$ thì $P_1 + P_2 = P_2$.

2. Ngược lại, nếu $P_2 = \mathcal{O}$ thì $P_1 + P_2 = P_1$.

3. Ngược lại, viết $P_1 = (x_1, y_2)$ và $P_2 = (x_2, y_2)$.

4. Nếu $x_1 = x_2$ và $y_1 = -y_2$ thì $P_1 + P_2 = \mathcal{O}$.

5. Nếu không, định nghĩa λ bởi

$$\lambda = \begin{cases} \dfrac{y_2 - y_1}{x_2 - x_1} & \text{nếu } P_1 \neq P_2 \\ \dfrac{3x_1^2 + A}{2y_1} & \text{nếu } P_1 = P_2. \end{cases}$$

Và ta có $P_1 + P_2 = (x_3, y_3)$, trong đó:

$$x_3 = \lambda^2 - x_1 - x_2 \quad \text{và} \quad y_3 = \lambda(x_1 - x_3) - y_1.$$

Chứng minh. Phần (1) và (2) của định lý 2.2 là đúng, và (4) là trường hợp đường thẳng qua P_1 và P_2 là đường thẳng đứng, nên $P_1 + P_2 = \mathcal{O}$. (lưu ý, vẫn đúng với trường hợp $y_1 = y_2 = 0$.) Còn phần (5), ta để ý rằng λ là hệ số góc của đường thẳng đi qua P_1 và P_2, và cũng là hệ số góc của tiếp tuyến tại P_1 nếu $P_1 = P_2$. Trong cả 2 trường hợp, đường thẳng L đều có phương trình $Y = \lambda X + \nu$ với $\nu = y_1 - \lambda x_1$. Thế Y vào phương trình đường cong E ta được:

$$(\lambda X + \nu)^2 = X^3 + AX + B$$

nên

$$X^3 - \lambda^2 X^2 + (A - 2\lambda\nu)X + (B - \nu^2) = 0$$

Phương trình trên có 2 nghiệm đã biết trước là x_1 và x_2. Ta gọi nghiệm còn lại là x_3, phân tích thành nhân tử ta được

$$X^3 - \lambda^2 X^2 + (A - 2\lambda\nu)X + (B - \nu^2) = (X - x_1)(X - x_2)(X - x_3)$$

Đồng nhất hệ số 2 vế, ta được $x_3 = \lambda^2 - x_1 - x_2$. Cuối cùng, để tìm được $P_1 + P_2$, ta thay x_3 vào phương trình L để tìm giao điểm còn lại của L và E rồi lấy đối xứng qua Ox. $\square$

3 Đường cong elliptic trên trường hữu hạn

Trong phần trước, chúng ta đã phát triển lý thuyết về đường cong elip về mặt hình học. Tuy nhiên, để áp dụng lý thuyết về đường cong elliptic vào mật mã, chúng ta cần xem xét các đường cong elliptic mà các điểm của nó có tọa độ trong một trường hữu hạn F_p. Các ứng dụng về mật mã của đường cong Elliptic đa số chỉ sử dụng các đường cong trên trường hữu hạn.

3.1 Sơ bộ

Definition 2. Trường là một tập hợp K có nhiều hơn một phần tử, được định nghĩa hai phép toán cộng và nhân, ký hiệu bởi dấu (+) và dấu (.). Trường thỏa mãn các tính chất của số học.

Các tính chất số học: TODO:

1. Tính kết hợp

2. Tính giao hoán

3. Đơn vị cộng và đơn vị nhân

4. Nghịch đảo phép cộng

5. Nghịch đảo phép nhân

6. Tính phân phối

Definition 3. Trường hữu hạn (còn gọi là trường Galois) là những trường có hữu hạn số phần tử. Bậc của một trường hữu hạn là số phần tử của nó, là số nguyên tố hoặc lũy thừa nguyên tố.

Trường hữu hạn là cơ bản trong một số lĩnh vực toán học và khoa học máy tính, bao gồm lý thuyết số, hình học đại số, lý thuyết Galois, hình học hữu hạn, mật mã và lý thuyết mã hóa.

Definition 4 (Bình phương modulo)**.** Cho số nguyên dương $m \geq 2$. Số nguyên a được gọi là *bình phương modulo m* nếu $\gcd(a, m) = 1$ và phương trình

$$x^2 \equiv a(\mod m)$$

có nghiệm

Definition 5 (Nghịch đảo modulo)**.** Với một số nguyên a, ta gọi nghịch đảo modulo m của a là a^{-1} là số nguyên thỏa mãn:

$$a * a^{-1} \equiv 1(\mod m)$$

Chú ý rằng không phải lúc nào a^{-1} cũng tồn tại. Ví dụ với $m = 4, a = 2$, ta không thể tìm được a^{-1} thỏa mãn đẳng thức trên.

Definition 6 (Thặng dư bình phương)**.** Một số nguyên q gọi là thặng dư bình phương theo modulo m nếu nó đồng dư với một số chính phương theo modulo m. Nói cách khác, tồn tại số nguyên x thỏa mãn:

$$x^2 \equiv q(\mod m)$$

Ngược lại, q được gọi là *phi thặng dư bình phương*

Definition 7 (Modular square root)**.** Một Modular square root r của số nguyên a theo modulo m là một số nguyên thỏa mãn:

$$r^2 \equiv a(\mod m)$$

Xét F_p là một trường hữu hạn (hữu hạn số phần tử nguyên dương):

$$F_p = \{0, 1, 2, \ldots p - 1\}$$

Với p là một số nguyên tố. F_p giống như cách viết Z/mZ là vành các số nguyên modulo m.

3.2 Đường cong elliptic trên trường hữu hạn

Ta định nghĩa một đường cong elliptic E trên trường hữu hạn $\mathbb{F}_q$ là một phương trình có dạng:

$$E : Y^2 = X^3 + AX + B \text{ với các hằng số } A, B \in F_p \text{ thỏa mãn } 4A^3 + 27B^2 \neq 0$$

Tập hợp các điểm trên E có toạ độ thuộc $\mathbb{F}_p$ được kí hiệu bởi

$$E(F_p) = \{(x, y) : x, y \in \mathbb{F}_p \text{ thỏa mãn } y^2 = x^3 + Ax + B\} \cup \mathcal{O}$$

Remark 2. Vì một vài lí do mà chúng tôi sẽ giải thích ở phần sau, ở đây, chúng tôi thêm điều kiện $p \geq 3$. Những đường cong Elliptic trên trường $\mathbb{F}_2$ có vai trò quan trọng trong mật mã, nhưng chúng rất phức tạp, nên chúng ta sẽ thảo luận về chúng ở phần 7.

Example 4. Xem xét đường cong elliptic

$$E : Y^2 = X^3 + 3X + 8 \quad \text{ trên trường } F_{13}$$

Ta tìm các điểm thuộc $E(\mathbb{F}_{13})$ bằng cách thay tất cả giá trị của $X = 0, 1, 2, \ldots, 12$ và kiểm tra với mỗi giá trị của X, $X^3 + 3X + 8$ có là bình phương modulo của 13 hay không. Ví dụ, thay $X = 0$, ta có $X^3 + 3X + 8 = 8$ và 8 không phải bình phương modulo của 13. Tiếp theo, thay $X = 1$, ta được $X^3 + 3X + 8 = 12$ và 12 là bình phương modulo của 13. Nó có 2 nghiệm

$$5^2 \equiv 12 (\mod 13) \quad \text{ và } \quad 8^2 \equiv 12 (\mod 13)$$

.

Ta tìm được 2 điểm $(1, 5)$ và $(1, 8)$ thuộc $E(\mathbb{F}_{13})$. Tiếp tục theo cách này, ta kết thúc với tập hoàn chỉnh gồm 9 điểm:

$$E(\mathbb{F}_{13}) = \{\mathcal{O}, (1, 5), (1, 8), (2, 3), (2, 10), (9, 6), (9, 7), (12, 2), (12, 11)\}.$$

Cho $P_1 = (x_1, y_1)$ và $P_2 = (x_2, y_2)$ thuộc $E(\mathbb{F}_p)$. Ta định nghĩa tổng $P_1 + P_2$ có tọa độ (x_3, y_3) thu được bằng cách áp dụng thuật toán cộng (2.2). Vì tọa độ các độ các điểm đó nằm trong trường $\mathbb{F}_p$, ta thu được (x_3, y_3) có tọa độ trong trường $\mathbb{F}_p$. Nhưng điều này vẫn chưa đủ chỉ ra (x_3, y_3) có thể thuộc $E(\mathbb{F}_p)$ hay không.

Theorem 3.1. Cho E là đường cong elliptic trên $\mathbb{F}_p$ và P và Q là 2 điểm thuộc $E(\mathbb{F}_p)$.

- Thuật toán cộng đường cong elliptic áp dụng cho P và Q (2.2) đưa ra một điểm trong $E(\mathbb{F}_p)$. Điểm này được kí hiệu bởi $P + Q$.
- Luật cộng trên $E(\mathbb{F}_p)$ thỏa mãn tất cả các tính chất được liệt kê ở định lý 2.1. Nói cách khác, luật cộng này làm cho $E(\mathbb{F}_p)$ thành nhóm hữu hạn.

Chứng minh. □

Example 5. Tiếp tục với đường cong E từ ví dụ 4

$$E : Y^2 = X^3 + 3X + 8 \quad \text{ trên trường } \mathbb{F}_{13}$$

Áp dụng thuật toán cộng (2.2) để cộng $P(9,7)$ và $Q(1,8)$, trước hết, ta tính hệ số góc của L:

$$\lambda = \frac{y_2 - y_1}{x_2 - x_1} = \frac{8-7}{1-9} = \frac{1}{-8} = \frac{1}{5} = 8$$

vì các tính toán [1] đang được thực hiện trên trường $\mathbb{F}_{13}$ nên $-8 = 5$ và $\dfrac{1}{5} = 5^{-1} = 8$. Tiếp tục, ta tính

$$\nu = y_1 - \lambda x_1 = 7 - 8\,.\,9 = -65 = 0.$$

Cuối cùng:

$$\begin{aligned} x_3 &= \lambda^2 - x_1 - x_2 = 64 - 9 - 1 = 54 = 2, \\ y_3 &= -(\lambda x_3 + \nu) = -8\,.\,2 = -16 = 10. \end{aligned}$$

Và ta hoàn thành việc tính toán

$$P + Q = (1,8) + (9,7) = (2,10) \in E(\mathbb{F}_{13})$$

Tương tự, ta dùng thuật toán cộng để cộng điểm $P = (9,7)$ với chính nó. Lưu ý ta vẫn đang thực hiện tính toán trên trường $\mathbb{F}_{13}$, ta có:

$$\begin{aligned} \lambda &= \frac{3x_1^2 + A}{2y_1} = \frac{3\,.\,9^2 + 3}{2\,.\,7} = \frac{246}{14} = 1 \\ \nu &= y_1 - \lambda x_1 = 7 - 1\,.\,9 = 11. \end{aligned}$$

sau đó

$$\begin{aligned} x_3 &= \lambda^2 - x_1 - x_2 = 1 - 9 - 9 = 9 \\ y_3 &= -(\lambda x_3 + \nu) = -1\,.\,9 - 11 = 6. \end{aligned}$$

nên $P + P = (9,7) + (9,7) = (9,6) \in E(\mathbb{F}_{13})$. Theo cách đó, ta có thể cộng mọi cặp điểm trong $E(\mathbb{F}_{13})$, kết quả được thể hiện ở Bảng 1

Hình 5: Phép cộng $E : Y^2 = X^3 + 3X + *$ trên trường $\mathbb{F}_{13}$

	$\mathcal{O}$	$(1,5)$	$(1,8)$	$(2,3)$	$(2,10)$	$(9,6)$	$(9,7)$	$(12,2)$	$(12,11)$
$\mathcal{O}$	$\mathcal{O}$	$(1,5)$	$(1,8)$	$(2,3)$	$(2,10)$	$(9,6)$	$(9,7)$	$(12,2)$	$(12,11)$
$(1,5)$	$(1,5)$	$(2,10)$	$\mathcal{O}$	$(1,8)$	$(9,7)$	$(2,3)$	$(12,2)$	$(12,11)$	$(9,6)$
$(1,8)$	$(1,8)$	$\mathcal{O}$	$(2,3)$	$(9,6)$	$(1,5)$	$(12,11)$	$(2,10)$	$(9,7)$	$(12,2)$
$(2,3)$	$(2,3)$	$(1,8)$	$(9,6)$	$(12,11)$	$\mathcal{O}$	$(12,2)$	$(1,5)$	$(2,10)$	$(9,7)$
$(9,6)$	$(9,6)$	$(2,3)$	$(12,11)$	$(12,2)$	$(1,8)$	$(9,7)$	$\mathcal{O}$	$(1,5)$	$(2,10)$
$(9,7)$	$(9,7)$	$(12,2)$	$(2,10)$	$(1,5)$	$(12,11)$	$\mathcal{O}$	$(9,6)$	$(2,3)$	$(1,8)$
$(12,2)$	$(12,2)$	$(12,11)$	$(9,7)$	$(2,10)$	$(9,6)$	$(1,5)$	$(2,3)$	$(1,8)$	$\mathcal{O}$
$(12,11)$	$(12,11)$	$(9,6)$	$(12,2)$	$(9,7)$	$(2,3)$	$(2,10)$	$(1,8)$	$\mathcal{O}$	$(1,5)$

[1]Đây là lúc thích hợp để hiểu rằng, $\dfrac{1}{5}$ chỉ là *kí hiệu* cho một nghiệm của phương trình $5x = 1$. Để gán một giá trị cho $\dfrac{1}{5}$, bạn phải biết giá trị đang ở trường nào. Trong trường $\mathbb{Q}$, giá trị của $\dfrac{1}{5}$ là một số bình thường, nhưng ở trường $\mathbb{F}_{13}$ giá trị của $\dfrac{1}{5}$ là 8 ($\dfrac{1}{5} = 5^{-1}$ và nghịch đảo modulo 13 của 5 là 8).

Tập điểm trong $E(\mathbb{F}_p)$ là tập hữu hạn. Chính xác hơn, có p cách chọn X và mỗi cách chọn X, phương trình

$$Y^2 = X^3 + AX + B$$

cho nhiều nhất 2 nghiệm Y. Thêm điểm $\mathcal{O}$, $\#E(\mathbb{F}_p)$ có tối đa $2p+1$ điểm.

Khi gán giá trị cho X, có ba trường hợp xảy ra với đại lượng

$$X^3 + AX + B$$

Thứ nhất, nó là thặng dư bình phương và có hai Modular square root, ta được hai điểm thuộc $E(\mathbb{F}_p)$, trường hợp này xảy ra khoảng 50%. Thứ hai, nó không là thặng dư bình phương, ta bỏ qua X, trường hợp này cũng chiếm khoảng 50%. Thứ ba, $X^3+AX+B=0$, ta được một điểm thuộc $E(\mathbb{F}_p)$, trường hợp này rất hiếm xảy ra [2]. Theo đó, số phần tử của $E(\mathbb{F}_p)$ xấp xỉ

$$\#E(\mathbb{F}_p) \approx 50\% \cdot (2p+1) = p+1.$$

Một định lý nổi tiếng của Hasse, sau này được Weil và Deligne tổng quát hóa rộng rãi, nói rằng điều này đúng với các dao động ngẫu nhiên

Theorem 3.2 (Hasse)**.** Cho E là đường cong elliptic trên trường F_p. Thì

$$\#E(\mathbb{F}_p) = p + 1 - t_p \text{ với } t_p \text{ thỏa mãn } |t_p| \leq 2\sqrt{p}.$$

Definition 8. Đại lượng $t_p = p + 1 - \#E(\mathbb{F}_p)$ ở định lý 3.2 được gọi là *dấu vết của Frobenius* trên $E/\mathbb{F}_p$.

t_p xuất hiện dưới dạng dấu vết của một ma trận 2x2 có vai trò như phép biến đổi tuyến tính trên một không gian vector 2 chiều liên kết với $E/\mathbb{F}_p$.

Example 6. Cho phương trình E:

$$E : Y^2 = X^3 + 4X + 6$$

Chúng ta có thể coi E là đường cong elliptic trên trường F_p cho các trường hữu hạn $\mathbb{F}_p$ khác nhau và đếm số điểm thuộc $E(\mathbb{F}_p)$. Bảng 2 liệt kê các kết quả với những số nguyên tố đầu tiên, cùng giá trị của t_p để so sánh với giá trị của $2\sqrt{p}$.

Hình 6: Số điểm và dấu vết Frobenius của $E : Y^2 = X^3 + 4X + 6$

p	$\#E(\mathbb{F}_p)$	t_p	$2\sqrt{p}$
3	4	0	3.46
5	8	-2	4.47
7	11	-3	5.29
11	16	-4	6.63
13	14	0	7.21
17	15	3	8.25

[2] Phép đồng dư $X^3 + AX + B \equiv 0(\mod p)$ có nhiều nhất ba nghiệm, và nếu p lớn, tỉ lệ chọn ngẫu nhiên một trong số chúng là rất nhỏ.

Remark 3. Định lý Hasse cho ta một giới hạn của $\#E(\mathbb{F}_p)$, nhưng không cung cấp một phương pháp để tính giá trị này. Về nguyên tắc, để tìm $\#E(\mathbb{F}_p)$, ta có thể thay từng giá trị của X rồi kiểm tra giá trị của $X^3 + AX + B$ dựa vào bảng thặng dư bình phương p, nhưng độ phức tạp thời gian là $O(p)$, rất kém hiệu quả. Schoof [2] đã tìm ra một phương pháp tốt hơn để tính $\#E(\mathbb{F}_p)$ trong thời gian $O(\log^6(p))$. Nghĩa là ông ấy tìm được một thuật toán có thời gian đa thức. Thuật toán của Schoof được cải thiện bởi Elkies và Atkin, với tên gọi là *thuật toán SEA* [3].

4 Bài toán Logarit rời rạc đường cong elliptic

4.1 Bài toán Logarit rời rạc

Proposition 4.1. Cho số nguyên tố p, giả sử p là ước của tích ab của 2 số nguyên a và b. Thì p là ước của ít nhất 1 trong 2 số a hoặc b. Nói chung là, nếu p là ước của một tích các số nguyên, hay

$$p | a_1 a_2 \ldots a_n$$

thì p là ước của ít nhất một số a_i.

Theorem 4.2 (Căn nguyên thủy)**.** Cho số nguyên tố p. Tồn tại một phần tử $g \in \mathbb{F}_p^*$ mà lũy thừa của g sinh ra mọi phần tử của $\mathbb{F}_p^*$, hay

$$\mathbb{F}_p^* = \{1, g, g^2, g^3, \ldots, g^{p-2}\}.$$

Những phần tử thỏa mãn được gọi là căn nguyên thủy của $\mathbb{F}_p$ hoặc phần tử sinh của $\mathbb{F}_p^*$. Chúng là những phần tử của $\mathbb{F}_p^*$ có bậc $p - 1$

Theorem 4.3 (Fermat nhỏ)**.** Cho số nguyên tố p và số nguyên a. Ta có:

$$a \equiv \begin{cases} 1 \pmod{p} & \text{nếu } p \nmid a \\ 0 \pmod{p} & \text{nếu } p \mid a \end{cases}$$

Chứng minh. Nếu $p \mid a$ thì mọi lũy thừa của a chia hết cho p. Vậy ta chỉ cần xét trường hợp $p \nmid a$. Nhìn vào dãy các số:

$$a, 2a, 3a, \ldots, (p-1)a \pmod{p} \tag{5}$$

Có $p - 1$ số trong dãy. Ta khẳng định chúng đều khác nhau. Vì:

Ta lấy ra hai số bất kì trong $p - 1$ số, là $ja \pmod{p}$ và $ka \pmod{p}$. Giả sử $ja \equiv ka \pmod{p}$, thì $(j-k)a \equiv 0 \pmod{p}$. Mệnh đề 4.1 cho ta biết p là ước của $j-k$ hoặc a. Tuy nhiên, ta đã giả định p không là ước của a nên p là ước của $j-k$. Lại có $1 \le j, k \le p-1$, do đó $-(p-2) \le j - k \le p - 2$. Trong khoảng $-(p-2)$ đến $p-2$ chỉ có số 0 chia hết cho p. Điều này chỉ ra $j - k = 0$ hay $j = k$.

Do đó, $p - 1$ số trong (5) đều khác nhau và cũng khác 0. Danh sách (5) bao gồm $p - 1$ số phân biệt năm trong khoảng $(1; p - 1)$. Nhưng chỉ có $p - 1$ số phân biệt giữa 1 và $p - 1$, vì vậy danh sách các số (5) đơn giản là danh sách các số $1, 2, \ldots, p - 1$

Nhân tất cả các số trong (5) ta được đồng dư thức sau:

$$\begin{array}{rrcll} & a\cdot 2a\cdot 3a\dots(p-1)a & \equiv & 1\cdot 2\cdot 3\dots(p-1) & \pmod p\\ \Rightarrow & a^{p-1}\cdot(p-1)! & \equiv & (p-1)! & \pmod p\\ \Rightarrow & a^{p-1} & \equiv & 1 & \pmod p\end{array}$$

□

Cho p là một số nguyên tố lớn. Định lý 4.2 cho chúng ta biết rằng tồn tại một căn nguyên thủy g mà mọi phần tử khác 0 của F_p đều là lũy thừa của g. Cụ thể, $g^{p-1} = 1$ theo định lý nhỏ của Fermat (4.3), và không có lũy thừa nhỏ hơn nào của g bằng 1. Tương đương,

$$\mathbb{F}_p^* = \{1, g, g^2, g^3, \dots, g^{p-2}\}$$

Definition 9. Cho g là căn nguyên thủy của F_p, và h là một số khác 0 thuộc F_p. Bài toán Logarit rời rạc (DLP) là bài toán tìm một nghiệm x thỏa mãn

$$g^x \equiv h \pmod p$$

Số x được gọi là logarit của h theo cơ số g và được ký hiệu $\log_g(h)$.

Remark 4. Một thuật ngữ cũ hơn cho logarit rời rạc là *chỉ số*, được ký hiệu là $ind_g(h)$. Thuật ngữ chỉ số vẫn thường được sử dụng trong lý thuyết số. Nó cũng thuận tiện trong khi phân biệt giữa logarit thông thường và logarit rời rạc, ví dụ, đại lượng log_2 thường xuyên xuất hiện cả trong logarit thông thường và logarit rời rạc.

Remark 5. Bài toán logarit rời rạc là bài toán tìm x sao cho $g^x \equiv h$. Tuy nhiên nếu có một nghiệm thì sẽ có vô số nghiệm, vì theo định lý nhỏ của Fermat $g^{p-1} \equiv 1 (modp)$. Do đó nếu x là nghiệm thì $x + k(p-1)$ cũng là nghiệm với mọi giá trị k, vì

$$g^{x+k(p-1)} \equiv g^x \cdot (g^{p-1})^k \equiv h \cdot 1^k \equiv h \pmod p$$

Do đó, $\log_g(h)$ được định nghĩa khi ta cộng hoặc trừ một bội số của $(p-1)$. Nói cách khác, $log_g(h)$ được đụnh nghĩa bởi modulo $p-1$. Không khó để chứng minh rằng log_g được định nghĩa bởi hàm xác định:

$$log_g : \mathbb{F}_p^* \to \frac{\mathbb{Z}}{(p-1)\mathbb{Z}}$$

Đôi khi, để cụ thể hóa, ta có thể coi "logarit rời rạc" là số nguyên x nằm giữa 0 và $p-2$ thỏa mãn đồng dư thức $g^x \equiv h \pmod p$

Remark 6. Không khó để chứng minh rằng

$$\log_g(ab) = \log_g(a) + \log_g(b)\ \forall a, b \in \mathbb{F}_p^*$$

Hình 7: Lũy thừa và logarit rời rạc với $g = 627$ modulo $p = 941$

n	$g^n \mod p$
1	627
2	732
3	697
4	395
5	182
6	253
7	543
8	760
9	374
10	189

n	$g^n \mod p$
11	878
12	21
13	934
14	316
15	522
16	767
17	58
18	608
19	111
20	904

h	$\log_g(h)$
1	0
2	183
3	469
4	366
5	356
6	652
7	483
8	549
9	938
10	539

h	$\log_g(h)$
11	429
12	835
13	279
14	666
15	825
16	732
17	337
18	181
19	43
20	722

Definition 10. Cho G là một nhóm được trang bị phép toán hai ngôi, ký hiệu là $\star$. Bài toán logarit rời rạc trên G được định nghĩa như sau: Với hai phần tử cho trước g và h thuộc G, tìm một số nguyên x thỏa mãn

$$\underbrace{g \star g \star g \star \ldots \star g}_{x \text{ lần}} = h$$

4.2 Trao đổi khóa Diffie - Hellman

Thuật toán trao đổi khóa Diffie-Hellman giải quyết tình huống sau. Alice và Bob muốn chia sẻ một khóa bí mật để sử dụng trong mật mã đối xứng, nhưng phương tiện liên lạc duy nhất của họ không an toàn. Mọi thông tin mà họ trao đổi đều được quan sát bởi đối thủ của họ, Eve. Làm cách nào để Alice và Bob có thể chia sẻ khóa mà Eve không biết? Thoạt nhìn, có vẻ như Alice và Bob phải đối mặt với một nhiệm vụ bất khả thi. Tuy nhiên độ khó của bài toán logarit rời rạc trong $\mathbb{F}_p^*$ cung cấp một giải pháp khả thi.

Đầu tiên, Alice và Bob thống nhất sử dụng một số nguyên tố p và một số nguyên khác khoong g theo modulo p. Hai giá trị này là công khai nên Eve cũng có thể biết. Vì nhiều lý do sẽ được thảo luận ở phần sau, tốt nhất là họ nên chọn g sao cho thứ tự của nó trong $\mathbb{F}_p^*$ là một số nguyên tố lớn.

Tiếp theo, Alice bí mật chọn một số nguyên a và không cho ai biết. Cùng lúc đó, Bob cũng bí mật chọn một số nguyên b. Alice và Bob sử dụng những số bí mật của họ và tính

$$\underbrace{A \equiv g^a \pmod p}_{\text{Alice tính}} \text{ và } \underbrace{B \equiv g^b \pmod p}_{\text{Bob tính}}$$

.

Sau đó, họ trao đổi với nhau giá trị vừa tính được, Alice gửi A cho Bob và Bob gửi B cho Alice. Eve cũng có thể nhìn thấy được các giá trị này, vì họ đang giao tiếp trên một kênh không an toàn.

Cuối cùng, Bob và Alice tiếp tục sử dụng những số bí mật mà họ đã chọn ở bước trước đó, và tính

$$\underbrace{A' \equiv B^a \pmod p}_{\text{Alice tính}} \text{ và } \underbrace{B' \equiv A^b \pmod p}_{\text{Bob tính}}$$

.

Giá trị cả hai thu được, A' và B', là bằng nhau, vì:

$$A' \equiv B^a \equiv (g^a)^b \equiv g^{ab} \equiv (g^b)^a \equiv A^b \equiv B' \pmod p.$$

Giá trị này là khóa mà cả hai cùng chấp nhận sử dụng.

Example 7. Alice và Bob chọn số nguyên tố $p = 941$,và căn nguyên thủy $g = 627$. Alice bí mật chọn $a = 347$ và tính được $A = 390 \equiv 627^{347} \pmod{941}$. Bob chọn $b = 781$, tính được $B = 691 \equiv 627^{781} \pmod{941}$. Alice và Bob trao đổi 2 số A và B. Việc gửi của Alice và Bob được thực hiện qua một kênh không an toàn, vì vậy hai giá trị $A = 390$ và $B = 691$ được coi là công khai. Các số $a = 347$ và $b = 781$ không được truyền đi và được giữ bí mật. Sau đó, Alice và Bob đều có thể tính được số

$$470 \equiv 627^{347 \cdot 781} \equiv A^b \equiv B^a \pmod{941}.$$

Vậy 470 là khóa bí mật được dùng chung.

Giả sử Eve đã nhìn thấy toàn bộ quá trình trao đổi khóa, Eve có thể tìm được khóa chung của Alice và Bob nếu cô ấy giải được một trong hai phương trình

$$627^a \equiv 390 \pmod{941} \textit{ hoặc } 627^b \equiv 691 \pmod{941}.$$

Tất nhiên, ví dụ của chúng tôi sử dụng các số quá nhỏ để đủ khả năng bảo mật cho Alice và Bob, vì máy tính của Eve cần rất ít thời gian để kiểm tra tất cả các luỹ thừa của 627 modulo 941.

Như ta đã biết, đây là cách duy nhất để Eve tìm được khóa mà không cần trợ giúp của Alice và Bob. Nguyên tắc hiện tại đề xuất rằng Alice và Bob nên chọn một số nguyên tố p có khoảng 1000 bit (tức là $p \approx 2^{1000}$) và một phần tử g có bậc là số nguyên tố và xấp xỉ $\frac{p}{2}$. Khi đó, Eve sẽ phải đối mặt với một nhiệm vụ thực sự khó khăn.

Eve biết giá trị của A và B, cô ấy cũng biết g và p. Vì vậy nếu Eve có thể giải được DLP, thì cô ấy có thể tìm được a và b, sau đó có thể dễ dàng tính toán g^{ab} và khóa bí mật chung của Alice và Bob. Alice và Bob vẫn an toàn với điều kiện là Eve không thể giải được DLP.

Definition 11. Cho số nguyên tố p và số nguyên g. *Bài toán Diffie-Hellman* (DHP) là bài toán tìm giá trị của $g^{ab} \pmod p$ khi biết trước giá trị của $g^a \pmod p$ và $g^b \pmod p$.

4.3 Hệ thống mật mã khóa công khai ElGamal

Mặc dù thuật toán trao đổi khóa Diffie-Hellman cung cấp một phương pháp chia sẻ công khai một khóa bí mật ngẫu nhiên, nhưng nó không đạt được mục tiêu đầy đủ là trở thành một hệ thống mật mã khóa công khai, vì một hệ thống mật mã cho phép trao đổi thông tin cụ thể, không chỉ là một chuỗi bit ngẫu nhiên. Hệ thống mật mã khóa công khai ElGamal là ví dụ đầu tiên của chúng tôi về hệ thống mật mã khóa công khai, nên chúng tôi sẽ giải thích một cách chậm rãi và chi tiết. Alice bắt đầu bằng cách công khai một khóa công khai và một thuật toán. Khóa công khai đơn giản chỉ là một số, thuật toán là phương pháp Bob sử dụng để mã hóa thông điệp của anh ấy sử dụng khóa công khai của Alice. Alice không tiết lộ khóa riêng tư của mình. Khóa riêng tư cho phép Alice, chỉ Alice, giải mã thông điệp đã được mã hóa bằng khóa công khai của cô ấy.

đọc ở đâyyyyyyyyyyyy

Quá trình này áp dụng cho bất kỳ hệ thống mật mã khóa công khai nào. Đối với hệ mã hóa khóa công khai ElGamal, Alice cần một số nguyên tố p lớn để bài toán Logarit rời rạc trong $\mathbb{F}_p^*$ trờ nên đủ khó, và cô ấy cần một phần tử g ....

4.4 Bài toán Logarit rời rạc đường cong elliptic

Ở phần trước, ta đã thảo luận về bài toán Logarit rời rạc (DLP) trên trường hữu hạn $\mathbb{F}_p^*$. Để tạo ra một hệ mã hóa dựa trên DLP cho $\mathbb{F}_p^*$, Alice công khai 2 số g và h, cô ấy giữ bí mật một số mũ x là nghiệm của phương trình

$$h \equiv g \pmod{p}$$

Hãy xem xét Alice có thể làm gì tương tự với một đường cong elliptic trên trường $\mathbb{F}_p$. Nếu Alice xem g và h như 2 phần tử thuộc nhóm $\mathbb{F}_p$, thì bài toán logarit rời rạc yêu cầu Eve tìm một số x thỏa mãn

$$h \equiv \underbrace{g \cdot g \cdot g \ldots g}_{x \text{ số hạng}} \pmod{p}$$

Nói cách khác, Eve cần xác định phải nhân g bao nhiêu lần để có kết quả đồng dư với h theo modulo p.

Với thông tin này, Alice hoàn toàn có thể tìm được với một nhóm điểm $E(\mathbb{F}_p)$ của đường cong elliptic E trên trường $\mathbb{F}_p$. Cô ấy công khai 2 điểm P và Q thuộc $E(\mathbb{F}_p)$, và giữ bí mật một số n sao cho

$$Q = P + P + \ldots + P + P = nP$$

Eve cần tìm ra phải cộng P bao nhiêu lần để được Q. Phép cộng trên E là một phép toán phức tạp, xây dựng một bài toán logarit rời rạc trên đường cong này rất khó để giải.

Definition 12. Cho đường cong elliptic E trên trường $\mathbb{F}_p$ và 2 điểm P và Q thuộc $E(\mathbb{F}_p)$. *Bài toán logarit rời rạc trên đường cong elliptic* (ECDLP) là bài toán tìm số nguyên n thỏa mãn $Q = nP$. Tương tự với bài toán Logarit rời rạc cho $\mathbb{F}_p^*$, ta ký hiệu cho n bởi

$$n = \log_P(Q)$$

và ta gọi n là *Logarit rời rạc elliptic* của Q đối với P.

Tài liệu

[1] Halmos, F. G. P. Graduate texts in mathematics 84.

[2] Schoof, R. Elliptic curves over finite fields and the computation of square roots mod p. *Mathematics of computation 44*, 170 (1985), 483–494.

[3] Schoof, R. Counting points on elliptic curves over finite fields. *Journal de théorie des nombres de Bordeaux 7*, 1 (1995), 219–254.

[4] Silverman, J. H. *The arithmetic of elliptic curves*, vol. 106. Springer, 2009.

[5] Silverman, J. H., and Tate, J. T. *Rational points on elliptic curves*, vol. 9. Springer, 1992.