MẬT MÃ ỨNG DỤNG TRONG AN TOÀN THÔNG TIN

(Applied Cryptography In Secure Information System)

ThS. Bùi Hữu Đông
buihuudong19@gmail.com
0903.82.36.46

Học viện Kỹ thuật Mật mã, khoa An toàn thông tin

Ngày 17 tháng 12 năm 2020

Buổi 09

MÃ HÓA TRÊN ĐƯỜNG CONG ELLIPTIC

Tổng quan

Các bài học trước ta đã nắm về:

- Mã hóa công khai với: RSA và trao đổi khóa Diffie-Hellman
  - Hệ RSA dùng hàm một chiều là phép tích hai thừa số nguyên tố lớn. Hai số nguyên tố p và q lớn cỡ 1024 bit => RSA thực hiện chậm
  - Diffie-Hellman dùng hàm một chiều là hàm logarit rời rạc

Ở bài học này, ta tiếp tục tìm hiểu một hàm một chiều khác dựa trên số học Elliptic => từ đó ta xây dựng một phương pháp mã hóa đường cong Elliptic (Elliptic Curve Cryptography - ECC)

Nhận xét ngay:

Mã hóa ECC giải quyết vấn đề này khi dùng các tham số có kích thước ngắn hơn (168 bít) tuy nhiên vẫn đảm bảo độ an toàn như RSA 1024 bít

Tổng quan

Nhận xét ngay về ECC:

- Mã hóa ECC giải quyết vấn đề của RSA khi dùng các tham số có kích thước ngắn hơn (168 bít) tuy nhiên vẫn đảm bảo độ an toàn như RSA 1024 bít
- ECC đảm bảo tính an toàn cao
- ECC giúp tiết kiệm chi phí tính toán
- Giá thành rẻ

Cơ sở toán học liên quan tới ECC

Ta sẽ tìm hiểu một số kiến thức cơ bản của toán học đó là đại số trừu tượng (abstract algebra). Theo đó, ta xét tới một tập các phần tử, cách thức kết hợp giữa các phần tử. (Giống với số học ta thường dùng phép cộng và nhân trên hai số cho ra số thứ ba). Các yếu tố đó gồm:

- Nhóm (Group)
- Vành (Ring)
- Trường (Field)

Nhóm - Group

- *Khái niệm:* Một nhóm, được ký hiệu là {G, $\circ$} là một tập G các phần tử và một phép kết hợp 2 ngôi $\circ$ thỏa các điều kiện:
  1. Tính bao đóng: $\forall a, b \in G$: $a \circ b \in G$
  2. Tính kết hợp: $\forall a, b, c \in G$: $(a \circ b) \circ c = a \circ (b \circ c)$
  3. Phần tử đơn vị: $\exists e \in G : a \circ e = e \circ a$, với $\forall a \in G$
  4. Phần tử nghịch đảo: $\forall a \in G$, $\exists a' \in G : a \circ a' = a' \circ a = e$
  5. Tính giao hoán: $\forall a, b \in G$: $a \circ b = b \circ a$

     Một nhóm mà thỏa tính chất giao hoán được gọi là *nhóm Abel*

- *Thí dụ 1:* Ta thấy, tập số nguyên $\mathbb{Z}$ và phép cộng số nguyên là một nhóm, phần tử đơn vị là 0, $\forall a \in \mathbb{Z}$ thì phần tử nghịch đảo của a là $-a$. Tập $\mathbb{Z}$ có vô hạn phần tử $=>$ nhóm vô hạn.

Nhóm - Group

- *Nhóm vòng - cyclic group:* cho nhóm $\{G, ^\circ\}$ ta định nghĩa phép lũy thừa như sau:
  - $a^k = a^\circ a^\circ a^\circ ... a^\circ$ (lặp k lần a với nguyên dương)
  - $a^{-k} = (a^{'})^k$
  - $a^0 = e$

    Thí dụ: $a^3 = a^\circ a^\circ a$

Ta gọi G là *nhóm vòng* nếu mọi phần tử đều biểu diễn dưới dạng a^k với $a \in G$ và k là số nguyên và a lúc này gọi là *phần tử sinh* của G

Thí dụ: Nhóm $(\mathbb{Z}^+, +)$ gồm các số nguyên dương với phần tử sinh là $g = 1$

Vành - Ring

- *Khái niệm:* Một vành R, kí hiệu $\{R, +, x\}$ là một tập các phần tử và hai phép kết hợp hai ngôi, gọi là phép cộng và phép nhân, nếu thỏa mãn các tính chất sau:
  - R là *nhóm Abel* theo phép cộng (tức thỏa 5 tính chất của *nhóm* ở trên)
  - Tính đóng với phép nhân: $\forall a, b \in R : ab \in R$ (Viết tắt cho phép x)
  - Tính kết hợp đối với phép nhân $\forall a, b, c \in R : (ab)c = a(bc)$
  - Tính phân phối giữa phép cộng và phép nhân $\forall a, b, c \in R : (a + b)c = ac + bc$
  - Tính giao hoán với phép nhân: $\forall a, b \in R : ab = ba$
  - Tồn tại phần tử đơn vị phép nhân: $a1 = 1a = a$
  - Liên quan giữa phép nhân và phần tử đơn vị phép cộng: $ab = 0; a = 0, b = 0$

Vành - Ring

- *Thí dụ 01:* Tập hợp các số nguyên $\mathbb{Z}$ với phép cộng và nhân thông thường là một vành
- *Thí dụ 02:* cho tập các ma trận vuông cấp n với số thực, các phép cộng và nhân ma trận tạo thành một vành
- *Thí dụ 03:* cho tập các số nguyên chẵn, với các phép cộng và nhân thông thường, tạo thành một vành giao hoán, tập ma trận vuông cấp n như trên không phải là vành giao hoán.
- Một vành được gọi là *miền nguyên* (integral domain) nếu đó là vành giao hoán và thỏa mãn tính chất tồn tại phần tử đơn vị của phép nhân và liên quan giữ a phép nhân và phân tử đơn vị.

Trường - Field

- *Khái niệm:* Một *trường* ký hiệu $\{F, +, x\}$ là một tập các phần tử và hai phép kết hợp 2 ngôi (phép cộng và nhân), nếu có các tính chất sau:
  - F là một miền nguyên (thỏa 5 tính chất của Nhóm và 6 tính chất của Vành)
  - Tồn tại phần tử nghịch đảo của phép nhân: $\forall a \in F, a \neq 0, \exists a^{-1} \in F : aa^{-1} = 1$ *Ngắn gọn:* trong trường, ta có thể thực hiện các phép +, -, *, / thuộc F. Phép chia: $\frac{a}{b} = ab^{-1}$

Trường - Field

- *Thí dụ:* Tập các số thực với phép cộng và nhân thông thường là một trường.

  Tập các số nguyên có phải là trường không? vì sao?

Số học modulo và trường hữu hạn GF(p)

- *Mô tả:*
  - Ta đã biết phép toán modulo. Cho một số nguyên n: $\mathbb{Z}_n = \{0, 1, 2, ..., n-1\}$
  - Như tập số nguyên $\mathbb{Z}$, trên tập $\mathbb{Z}_n$, ta định nghĩa phép cộng và phép nhân như sau: $\forall a, b, c \in \mathbb{Z}_n$
    - Phép cộng: $c = a + b$ nếu $c \equiv (a + b) mod\ n$
    - Phép nhân: $c = a.b$ nếu $c = a.b\ mod\ n$
- *Nhận xét:*
  - $\mathbb{Z}_n$ cùng phép cộng thỏa mãn các tính chất của *nhóm Abel* với phần tử đơn vị 0 (5 tính chất)
  - $\mathbb{Z}_n$ cùng với phép cộng và phép nhân thỏa các tính chất của miền nguyên với phần tử đơn vị là 1 (6 tính chất)

Số học modulo và trường hữu hạn GF(p)

- *Nhận xét <tiếp>:*
  - Không phải tập $\mathbb{Z}_n$ nào cũng tồn tại phần tử nghịch đảo. Tức là, mọi phần tử khác 0 của $\mathbb{Z}_n$ phải có phần tử nghịch đảo của phép nhân. Nói cách khác, chỉ với n là số nguyên tố thì mới thỏa mãn.
  - *Thí dụ:* với $n = 8$ - không tồn tại phần tử nghịch đảo, $n = 7$ thì tồn tại

a	$-a$	a^{-1}
0	0	-
1	7	1
2	6	-
3	5	3
4	4	-
5	3	5
6	2	-
7	1	7

a	$-a$	a^{-1}
0	0	-
1	6	1
2	5	4
3	4	5
4	3	2
5	2	3
6	1	6

Số học modulo và trường hữu hạn GF(p)

- *Nhận xét <tiếp>:*
  - Với n là số nguyên tố, thì tập $\mathbb{Z}_n$ trở thành một *trường hữu hạn* mà ta gọi là trường **Galois**
  - Vì vậy, ta đổi $\mathbb{Z}_n$ thành $\mathbb{Z}_p$ và kí hiệu trường hữu hạn trên là $GF(p)$

Số học đa thức và trường hữu hạn $GF(2^n)$

Phép toán đa thức bình thường

- *Mô tả:* Trong đại số, một đa thức bậc $n > 0$ có dạng:

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + ... + a_1 x + a_0 = \sum_{i=0}^{n} a_i x^i$$

  Với $a_i \in R, a_n \neq 0$ - gọi là hệ số

- *Phép toán đa thức:* Giả sử có hai đa thức $f(x) = \sum_{i=0}^{n} a_i x^i$ và $g(x) = \sum_{i=0}^{m} b_i x^i$
  - *Phép cộng:* $f(x) + g(x) = \sum_{i=0}^{max(m,n)} (a_i + b_i) x^i$
  - *Phép nhân:* $f(x)\ x\ g(x) = \sum_{i=0}^{(m+n)} (c_i) x^i$
  - *Phép trừ:* $f(x) - g(x) = \sum_{i=0}^{max(m,n)} (a_i - b_i) x^i$

Phép toán đa thức bình thường

- *Phép toán đa thức <tiếp>:*
  - *Phép chia:* $\frac{f(x)}{g(x)} = q(x) + \frac{r(x)}{g(x)}$
- *Thí dụ:* cho $f(x) = x^3 + x^2 + 2$ và $g(x) = x^2 - x + 1$
  - $f(x) + g(x) = x^3 + 2x^2 - x + 3$
  - $f(x) - g(x) = x^3 + x + 1$
  - $f(x)\ x\ g(x) = x^5 + 3x^2 - 2x + 2$
  - $f(x)/g(x)$: với $q(x) = x + 2; r(x) = x$
- *Nhận xét:* với các phép toán nhân và cộng như trên thì tập các đa thức (mỗi đa thức là một phần tử của tập) tạo thành một *vành*. Phần tử đơn vị của phép cộng là $e(x) = 0$, phần tử đơn vị của phép nhân là đa thức $d(x) = 1$

Phép toán đa thức bình thường

- *Câu hỏi:* tập các đa thức trên có tạo thành trường không? vì sao?

Đa thức định nghĩa trên tập $\mathbb{Z}_p$

- *Mô tả:* xét tập đa thức W_p có hệ số thuộc trường $\mathbb{Z}_p$

$$W_p = \left\{ f(x) = \sum_{i=0}^{n} (a_i) x^i \right\}$$

với $n \geq 0$, $a_i \in \mathbb{Z}_p, a_n \neq 0$

- *Các phép toán:* giả sử ta có hai đa thức:

$$f(x) = \sum_{i=0}^{n} a_i x^i; \; g(x) = \sum_{i=0}^{m} b_i x^i$$

Đa thức định nghĩa trên tập $\mathbb{Z}_p$

- *Các phép toán <tiếp>:*
  - Phép cộng: $f(x) + g(x) = \sum_{i=0}^{max(m,n)} (a_i + b_i)x^i$
  - Phép nhân: $f(x)\ x\ g(x) = \sum_{i=0}^{(m+n)} c_i x^i$
  - Phép trừ: $f(x) - g(x) = \sum_{i=0}^{max(m,n)} (a_i - b_i)x^i$
  - Phép chia: $f(x)/g(x)$: với $q(x)$ là thương, và $r(x)$ là phần dư.

    Trong đó: các phép toán $a_i + b_j$; $a_i b_j$; $a_i - b_j$ và a_i/b_j được định nghĩa trong tập $\mathbb{Z}_p$

Đa thức định nghĩa trên tập $\mathbb{Z}_p$

- *Thí dụ:* cho trường $\mathbb{Z}_2 = \{0, 1\}$, và đa thức $f(x) = x^7 + x^5 + x^4 + x^3 + x + 1$ và $g(x) = x^3 + x + 1$
  - $f(x) + g(x) = x^7 + x^5 + x^4$
  - $f(x) - g(x) = x^7 + x^5 + x^4$
  - $f(x)\ x\ g(x) = x^{10} + x^4 + x^2 + 1$
  - $f(x)/g(x)$: với $q(x) = x^4 + 1$ và $r(x) = 0$

Phép modulo đa thức

- *Mô tả:* giả sử ta có hai đa thức $f(x)$ và $m(x)$ được định nghĩa trên trường $\mathbb{Z}_p$, phép chia modulo được thực hiện như sau:

$$r(x) = f(x) \ mod \ m(x)$$

là phần dư của $f(x)/m(x)$

- *Thí dụ:* trong trường $\mathbb{Z}_2$ ta có:

$f(x) = x^{13} + x^{11} + x^9 + x^8 + x^6 + x^5 + x^4 + x^3 + 1$ và $m(x) = x^8 + x^4 + x^3 + x + 1$ ta có:

$f(x) \ mod \ m(x) = x^7 + x^6 + 1$

Trường hữu hạn GF(2^n)

- *Mô tả:* tương tự tập $\mathbb{Z}_p$ dùng phép modulo p với p là số nguyên tố, ta có một tập W_{pm} các đa thức dùng phép modulo đa thức.

  Chọn một đa thức $m(x)$ trên $\mathbb{Z}_p$ có bậc là n. Tập W_{pm} bao gồm các đa thức trên $\mathbb{Z}_p$ có bậc nhỏ hơn n, có dạng:

$$f(x) = \sum_{i=0}^{n-1} a_i x^i$$

  với $a_i \in \mathbb{Z}_p = \{0, 1, ..., p-1\}$; tập W_{pm} có p^n phần tử.

- *Thí dụ:* với $p = 2; n = 3$ thì W_{pm} có 8 phần tử:

$$\{0, 1, x, x+1, x^2, x^2+1, x^2+x, x^2+x+1\}$$

Trường hữu hạn GF(2^n)

- *Phần tử nghịch đảo:* Vì $m(x)$ là đa thức tối giản nên tương tự như số học modulo, các phần tử trong W_{pm} tồn tại phần tử nghịch đảo của phép nhân:

$$\forall f(x) \in W_{pm}, \exists f^{-1}(x) \in W_{pm} : f(x)f^{-1}(x) = 1$$

Do tồn tại phần tử nghịch đảo nên ta có thể tực hiện phép chia trong tập W_{pm}: $f(x)/g(x) = f(x)g^{-1}(x)$

Để tìm phần tử nghịch đảo của phép nhân đa thức ta cũng sử dụng thuật toán Euclid mở rộng tương tự như trong $\mathbb{Z}_p$

Ứng dụng GF(2^n) trong mã hóa

- Trong mã hóa đối xứng hoặc bất đối xứng việc mã hóa quy về phép cộng, trừ, nhân và chia với các con số. Do đó, bản rõ và mã phải thuộc một trường nào đó để tính toán không ra khỏi trường.
- Phép toán trên trường số thực không hiệu quả do tính toán nhiều thời gian. Máy tính chỉ hiệu quả trên số nguyên dạng byte hoặc bit $=>$ $\mathbb{Z}_p$ được tính tới, nhưng lại đòi hỏi p là nguyên tố. Trong khi, nếu bản rõ và mã biểu diễn dạng bit thì số lượng phần tử có dạng 2^n không phải là nguyên tố.

  Thí dụ: xét số nguyên 8 bit, có 256 phần tử. Nhưng Z_{256} không phải là một trường. Nếu chọn trường Z_{251} thì chỉ dùng được các số từ 0 đến 250, các số từ 251 đến 255 không tính toán được.

Ứng dụng GF(2^n) trong mã hóa

- Với hoàn cảnh này, ta dùng trường $GP(2^n)$ là phù hợp vì nó cũng gồm 2^n phần tử.
- Ta ánh xạ một hàm đa thức trong $GP(2^n)$ thành một số binary tương ứng bằng cách lấy các hệ số của đa thức tạo thành dãy bit $a_{n-1}a_{n-2}...a_1a_0$

Ứng dụng GF(2^n) trong mã hóa

- Thí dụ: xét trường $GF(2^3)$ với đa thức tối giản $m(x) = x^3 + x + 1$ ứng với số nguyên 3 bít như sau:

Đa thức trong GF(2^3)	*Số nguyên tương ứng*	*thập lục phân*
0	000	0
1	001	1
x	010	2
x+1	011	3
x^2	100	4
x^2+1	101	5
x^2+x	110	6
x^2+x+1	111	7

Ứng dụng GF(2^n) trong mã hóa

- Thí dụ <tiếp>: Bảng phép cộng và phép nhân tương ứng là:

+	0	1	2	3	4	5	6	7
0	0	1	2	3	4	5	6	7
1	1	0	3	2	5	4	7	6
2	2	3	0	1	6	7	4	5
3	3	2	1	0	7	6	5	4
4	4	5	6	7	0	1	2	3
5	5	4	7	6	1	0	3	2
6	6	7	4	5	2	3	0	1
7	7	6	5	4	3	2	1	0

x	0	1	2	3	4	5	6	7
0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7
2	0	2	4	6	3	1	7	5
3	0	3	6	5	7	4	1	2
4	0	4	3	7	6	2	5	1
5	0	5	1	4	2	7	3	6
6	0	6	7	1	5	3	2	4
7	0	7	5	2	1	6	4	3

Ứng dụng GF(2^n) trong mã hóa

- Thí dụ <tiếp>: Bảng nghịch đảo của phép cộng và nhân là:

a		$-a$		a^{-1}	
dạng đa thức	**dạng số**	**dạng đa thức**	**dạng số**	**dạng đa thức**	**dạng số**
0	0	0	0	-	-
1	1	1	1	1	1
x	2	x	2	x^2+1	5
x+1	3	x+1	3	x^2+x	6
x^2	4	x^2	4	x^2+x+1	7
x^2+1	5	x^2+1	5	x	2
x^2+x	6	x^2+x	6	x+1	3
x^2+x+1	7	x^2+x+1	7	x^2	4

ĐƯỜNG CONG ELLIPTIC

Đường cong Elliptic trên trường số thực

- *Giới thiệu:* Đường cong Elliptic có phương trình dạng tổng quát:

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_5$$

Sau biến đổi ta được:

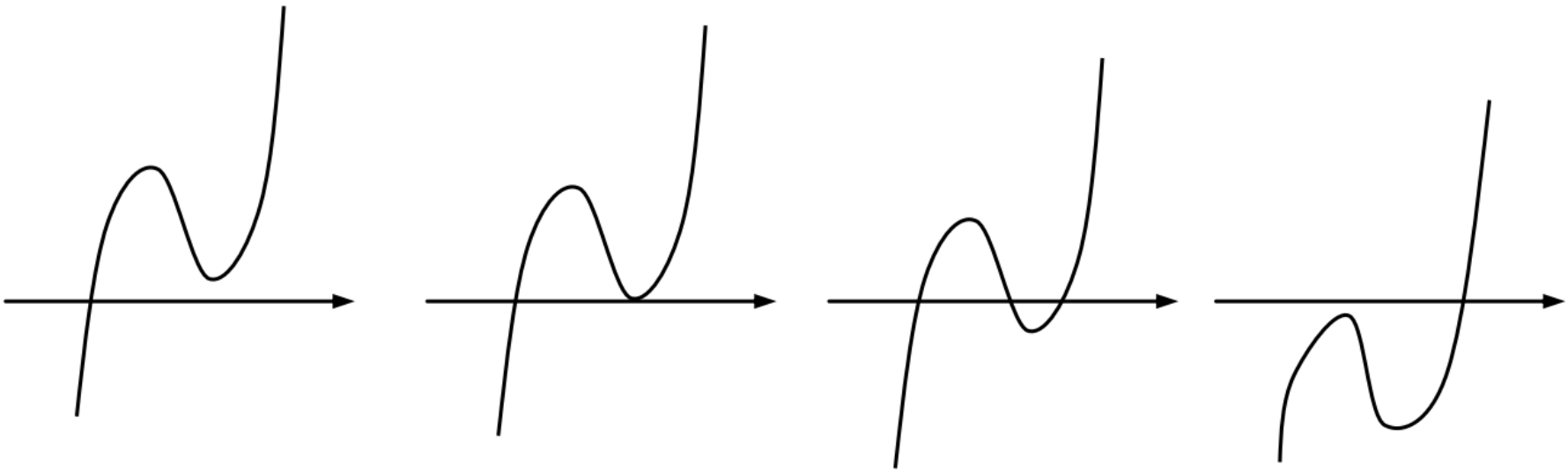
$$y^2 = x^3 + ax + b$$

với $a, b \in R$ Trước khi khảo sát đồ thị của đường cong Elliptic ta xét hàm bậc 3

- *Hàm bậc 3:* xét hàm $y = f(x) = x^3 + ax + b$

Đường cong Elliptic trên trường số thực

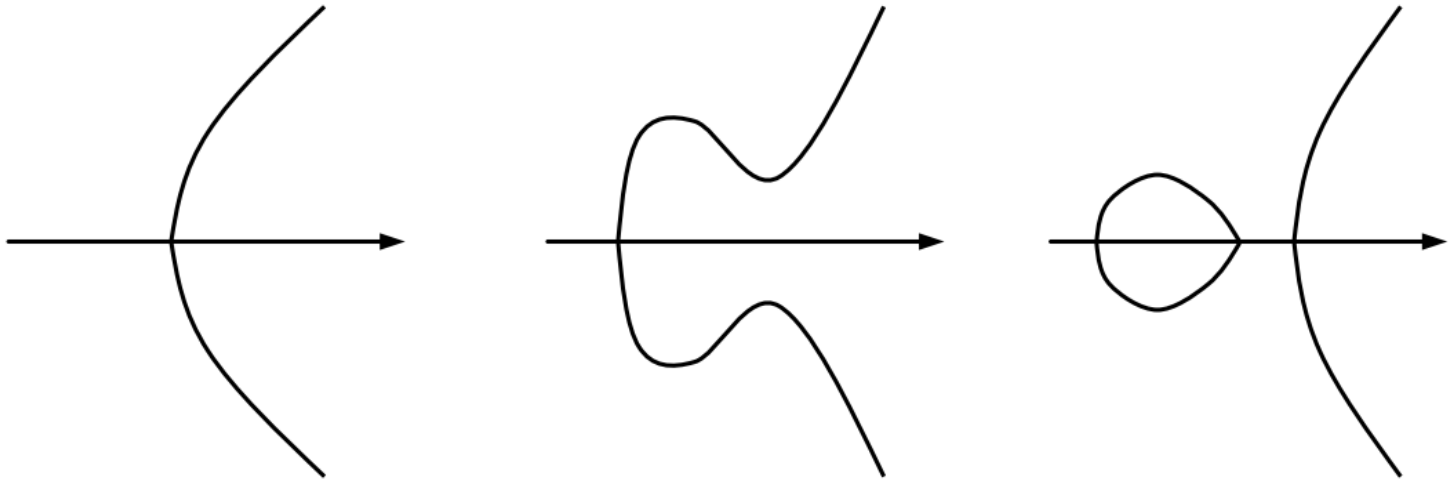
- *Hàm bậc 3:<tiếp>*
  - Nếu $a > 0$ thì $f(x)$ đơn điệu tăng.
  - Nếu $a \leq 0$, thì dạng đồ thị của $f(x)$ có 4 dạng sau: đặt $\lambda = 4a^3 + 27b^2$



$\lambda < 0$ $\lambda = 0$ $\lambda > 0$

Đường cong Elliptic trên trường số thực

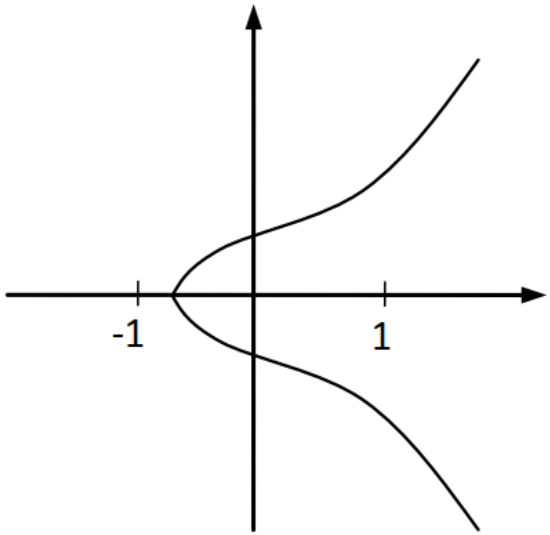
- *Đồ thị đường cong elliptic*: Ta có các dạng đường cong elliptic ứng với trường hợp $\lambda \neq 0$



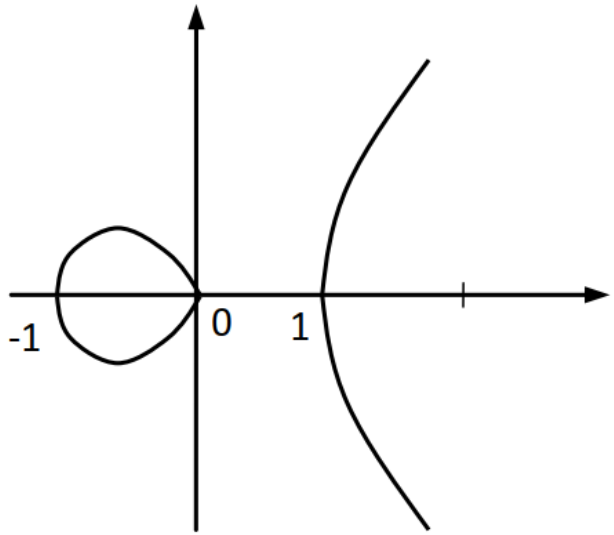
Lưu ý: *Đây chỉ là mặt cắt ngang, trong không gian 3D thì đường cong Elliptic trông như hình gif.*

Đường cong Elliptic trên trường số thực

- *Minh họa*: hai đường cong Elliptic $y^2 = x^3 - x$ và $y^2 = x^3 + x + 1$



$y^2 = x^3 + x + 1$



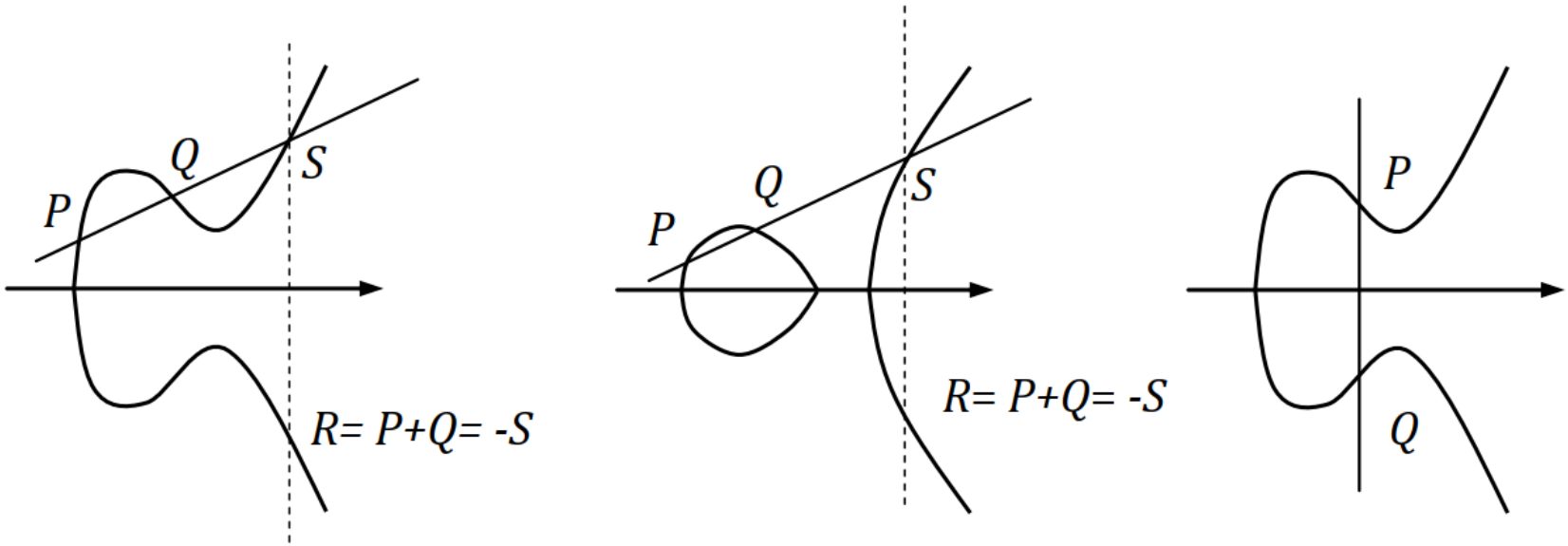
$y^2 = x^3 - x$

Đường cong Elliptic trên trường số thực

- *Các phép toán*: Trên đường cong Elliptic ta định nghĩa một điểm vô cực (O). Gọi $E(a, b)$ là tập các điểm thuộc đường cong $y^3 = x^2 + ax + b$ cùng với điểm O. Ta định nghĩa phép toán như sau:
  - *Phép cộng*:
    - Điểm O là phần tử đơn vị của phép cộng. Với $P \in E(a, b)$, với $P \neq O$ thì $P + O = O = P$
    - Phần tử nghịch đảo là $-P$ là điểm đối xứng với P qua trục hoành: $P + (-P) = O$
    - Với hai điểm P, Q bất kỳ ta kẻ đường thẳng đi qua P và Q sẽ cắt đường cong Elliptic ở điểm S phép $R = P + Q = -S$

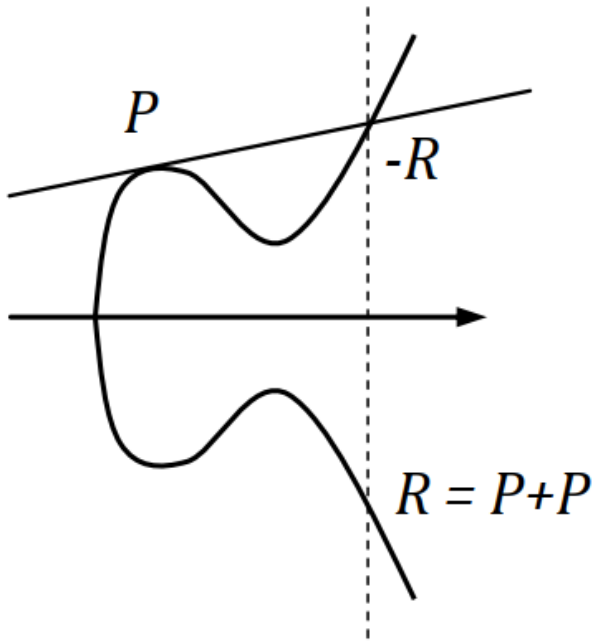
Đường cong Elliptic trên trường số thực

- *Các phép toán <tiếp>*:
  - *Phép cộng<tiếp>*:



Đường cong Elliptic trên trường số thực

- *Các phép toán <tiếp>*:
  - *Phép cộng<tiếp>*:
    - Để tính $P + P$, ta vẽ đường thẳng tiếp tuyến với đường cong Elliptic tại P, đường thẳng này cắt đường cong tại điểm S, lúc đó $R = P + P = -S$



Đường cong Elliptic trên trường số thực

- *Các phép toán <tiếp>*:
  - *Phép cộng<tiếp>*:
    - *Nhận xét:* Có thể thấy, tập $E(a, b)$ cùng với phép cộng định nghĩa như trên tạo thành một *nhóm Abel*
    - *Tính giá trị của phép cộng:* xét tọa độ $P(x_P, y_P)$ và của $Q(x_Q, y_Q)$ ta tính tọa độ điểm $R = P + Q = -S$ như sau:

      Đặt hệ số góc của đường thẳng là Δ, khi đó:

      $$\Delta = \frac{y_Q - y_P}{x_Q - x_P}$$

      Ta tính được:

      $$x_R = \Delta^2 - x_p - x_Q$$

      và

      $$y_R = \Delta(x_P - x_R) - y_P$$

Đường cong Elliptic trên trường số thực

- *Các phép toán <tiếp>*:
  - *Phép nhân*: Phép nhân thực chất là phép cộng nhiều lần.
    - Trước tiên ta cộng $2P = P + P$, sau đó tính $3P = 2P + P$
    - Việc tính nP thực hiện theo phương pháp *nhân đôi và cộng*. Bằng cách phân tích số n thành:

$$n = n_0 + 2n_1 + 2^2 n_2 + ... + 2^m n_m$$

với $[n_0 ... n_m] \in \{0, 1\}$

Đường cong Elliptic trên trường $\mathbb{Z}_p$

- *Mô tả*: Đường cong Elliptic trên trường $\mathbb{Z}_p$ là đường cong có các hệ số thuộc trường $\mathbb{Z}_p$ và đường cong này có dạng:

$$y^2 \ mod \ p = (a^3 + ax + b) \ mod \ p$$

với $a, b, x, y \in \mathbb{Z}_p$

- *Thí dụ*: trong trường $\mathbb{Z}_{23}$, chon $a = 1, b = 1, x = 9, y = 7$ ta có:

$$7^2 \ mod \ 23 = (9^3 + 9 + 1) \ mod \ 23$$

$$49 \ mod \ 23 = 739 \ mod \ 23$$

Đường cong Elliptic trên trường $\mathbb{Z}_p$

- *Nhận xét*:
  - Khác với đường cong Elliptic trên trường số thực, ta không thể biểu diễn đường cong Elliptic $\mathbb{Z}_p$ bằng đồ thị hàm số liên tục
  - *Thí dụ*: Các điểm (x, y) của đường cong trong $\mathbb{Z}_{23}$ với $a = 1, b = 1$ theo bảng 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)

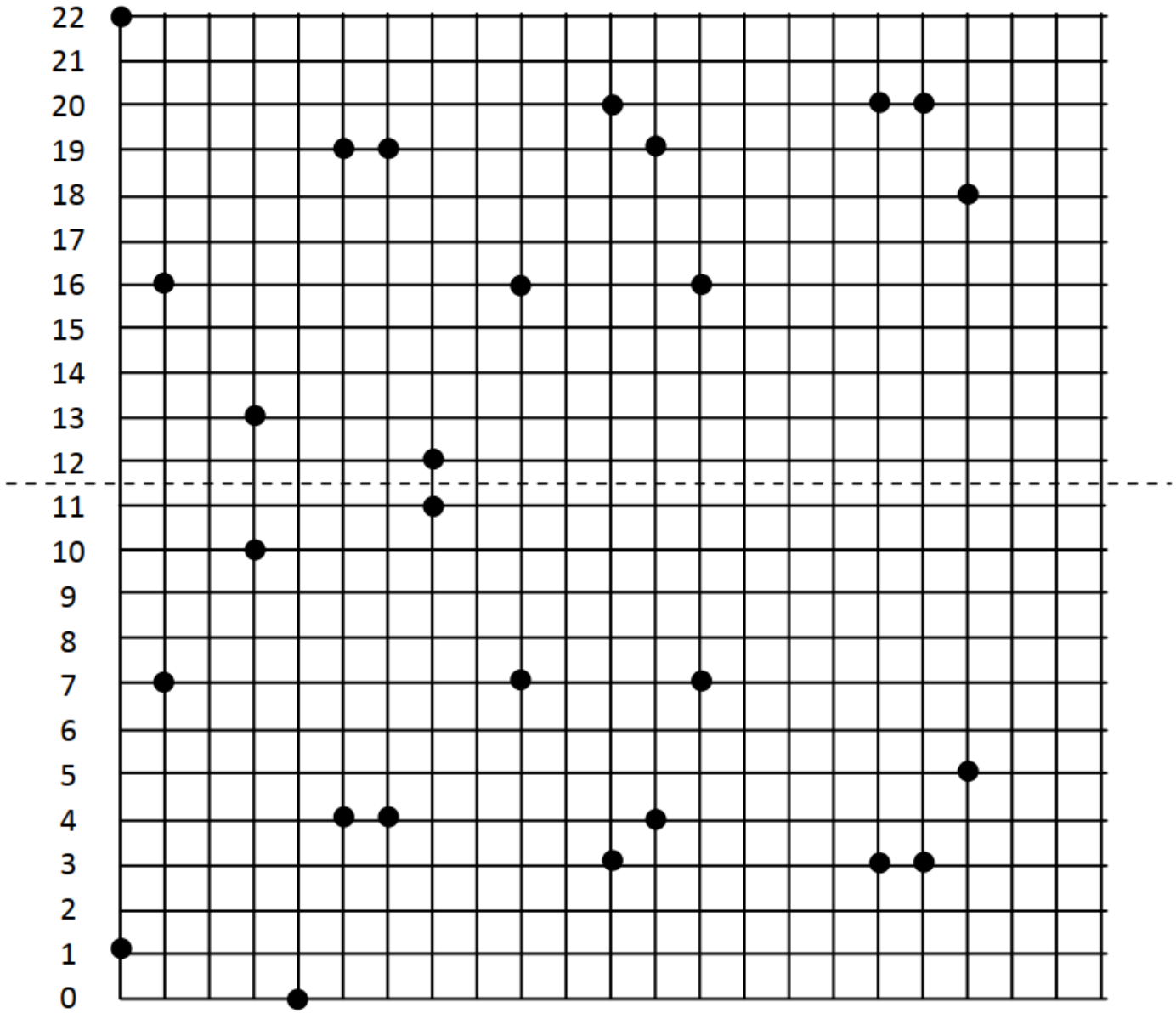
Đường cong Elliptic trên trường $\mathbb{Z}_p$

- *Nhận xét <tiếp>*:
  - Trên trường số thực ta lây đối xứng qua trục hoành, còn trong trường $\mathbb{Z}_p$ cũng đối xứng nhưng theo nghĩa modulo. Giả sử, điểm (x, y) thuộc đường cong $\mathbb{Z}_p$ thì trên điểm $(x, p - y)$ cũng thuộc đường cong này vì:

$$(p - y)^2 = p^2 - 2py + y^2 \equiv y^2 \, mod \, p$$

  - *Thí dụ:* điểm $(1, 7)$ đối xứng với $(1, 16)$ vì $7 + 16 = 0 \, mod \, 23$ cụ thể theo hình sau:

Đường cong Elliptic trên trường $\mathbb{Z}_p$



Đường cong Elliptic trên trường $\mathbb{Z}_p$

- *Nhận xét <tiếp>*:
  - Các điểm đối xứng với nhau qua đường $y = 11.5$. Riêng điểm $(4, 0)$ xem như là đối xứng với chính nó
  - Tương tự trên trường số thực, ta cũng định nghĩa một *nhóm Abel* $E_p(a, b)$ gồm các điểm của đường cong Elliptic $\mathbb{Z}_p$ cùng với điểm vô cực O
    - Với O là phần tử đơn vị của phép cộng: $P + O = O + P$
    - Phần tử nghịch đảo của điểm P trong phép cộng là $-P$, tức là: $P + (-P) = O$
    - Với hai điểm P và Q bất kỳ, phép $P + Q$ được xác định theo công thức:

$$x_R = \Delta^2 - x_P - x_Q \ mod\ p\ ;\ y_R = \Delta(x_P - x_R) - y_P \ mod\ p$$

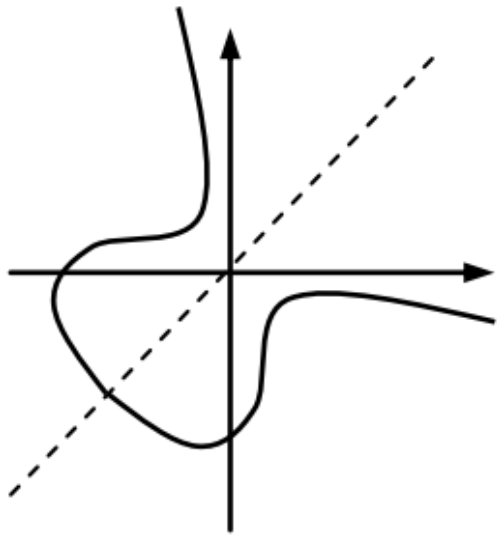
Trong đó:

$$\Delta = \begin{cases} \dfrac{y_Q - y_P}{x_Q - x_P} \ mod\ p & \text{nếu } P \neq Q; \\ \dfrac{(3{x_p}^2 + a)}{2y} \ mod\ p & \text{nếu } P = Q. \end{cases}$$

Đường cong Elliptic trên trường $GF(2^m)$

- *Mô tả*:
  - Đường cong Elliptic trên trường $GF(2^m)$ là đường cong có các hệ số thuộc trường $GF(2^m)$, dạng đường cong này hơi khác so với trên trường $\mathbb{Z}_p$:

$$y^2 + xy = x^3 + ax + b \quad a, b, x, y \in GF(2^m)$$



Đường cong Elliptic trên trường $GF(2^m)$

- *Thí dụ 01*: Xét trường $GF(2^4)$ với đa thức tối giản $m(x) = x^4 + x + 1$, phần tử sinh g của trường này có điều kiện $g^4 = g + 1$. Ta có bảng lũy thừa sau:

Biểu diễn lũy thừa	*Đa thức trong GF(2^3)*	*Số nhị phân*
0	0	0000
g^0	1	0001
g^1	g	0010
g^2	g^2	0100
g^3	g^3	1000
g^4	g+1	0011
g^5	g^2+ g	0110
g^6	$g^3 + g^2$	1100

Biểu diễn lũy thừa	*Đa thức trong GF(2^3)*	*Số nhị phân*
g^7	g^3+g+1	1011
g^8	g^2+ 1	0101
g^9	g^3 + g	1010
g^{10}	g^2+g+1	0111
g^{11}	g^3+ g^2+g	1110
g^{12}	g^3+ g^2+g+1	1111
g^{13}	g^3+ g^2+ 1	1101
g^{14}	g^3+ 1	1001

Đường cong Elliptic trên trường $GF(2^m)$

- *Thí dụ 02*: xét đường cong Elliptic trên $GF(2^4)$:

$$y^2 + xy = x^3 + g^4x + 1 \ \ (a = g^4, b = 1)$$

Bảng sau liệt kê các điểm thuộc đường cong này:

$(0, 1)$	(g^5, g^3)	(g^9, g^{13})
$(1, g^6)$	(g^5, g^{11})	(g^{10}, g)
$(1, g^{13})$	(g^6, g^8)	(g^{10}, g^8)
(g^3, g^8)	(g^6, g^{14})	$(g^{12}, 0)$
(g^3, g^{13})	(g^9, g^{10})	(g^{12}, g^{12})

Đường cong Elliptic trên trường $GF(2^m)$

- *Nhận xét*:
  - Giống như nhóm Abel $E_p(a, b)$, ta cũng xây dựng một nhóm Abel $E_{2^m}(a, b)$ gồm các điểm của đường cong Elliptic $GF(2^m)$ cùng với điểm vô cực (O)
    - Điểm O là phần tử đơn vị của phép cộng: $P + O = O + P$
    - Phần tử nghịch đảo của điểm P trong phép cộng là $-P$, là điểm đối xứng với P, ký hiệu $P = (x_P, y_P)$, và $-P = (x_P, x_P + y_P)$
    - Với hai điểm P, Q phân biệt và bất kỳ, phép cộng $R = P + Q$ được xác định:

$$x_R = \Delta^2 + \Delta + x_P + x_Q + a$$

$$y_R = \Delta(x_P + x_R) + x_R + y_P$$

Trong đó:

$$\Delta = \frac{y_Q + y_P}{x_Q + x_P}$$

Đường cong Elliptic trên trường $GF(2^m)$

- *Nhận xét <tiếp>*:
  - Phép cộng $R = P + P$ được xác định bằng công thức:

$$x_R = \Delta^2 + \Delta + a$$

$$y_R = x_P^2 + (\Delta + 1)x_R$$

Trong đó: $\Delta = x_P + \frac{y_P}{x_P}$

Ứng dụng đường cong Elliptic trong mã hóa

- *Mô tả*: Đối với mã hóa sử dụng đường cong Elliptic, ta xây dựng hàm một chiều (one-way) như sau:
  - Trong nhóm Abel $E_p(a, b)$ xây dựng từ đường cong Elliptic $\mathbb{Z}_p$, ta xét phương trình: $Q = P + P + P + ..P = kP \ \ (k < p)$
  - Cho trước k và P, việc tính Q được thực hiện dễ dàng, tuy nhiên nếu cho trước P và Q thì việc tìm ra k là việc khó khăn => đây là hàm logarit rời rạc của đường cong Elliptic
- *Thí dụ*: xét nhóm $E_{23}(9, 17)$ với phương trình:

$$y^2 \ mod \ (23 = x^3 + 9x + 7) \ mod \ 23 \ \ a, b, x, y \in \mathbb{Z}_{23}$$

Cho điểm $P = (16, 5)$, $Q = (4, 5)$ chúng ta chỉ có cách là vét cạn các giá trị của k từ 2 đến $p - 1$ để tìm ra k: $P = (16, 5)$; $2P = (20, 20)$; $3P = (14, 14)$; $4P = (19, 20)$; $5P = (13, 10)$; $6P = (7, 3)$; $7P = (8, 7)$; $8P = (12, 17)$; $9P = (4, 5)$

Ứng dụng đường cong Elliptic trong mã hóa

Từ thí dụ trên ta có nhận xét sau:

- Vì $9P = Q => k = 9$, trong thực tế ta sử dụng đường cong Elliptic $\mathbb{Z}_p$ với p lớn, sao cho việc vét cạn là bất khả thi.

Dựa vào hàm một chiều trên chúng ta có 2 cách sử dụng đường cong Elliptic trong lĩnh vực mã hóa là trao đổi khóa EC Diffie-Hellman và mã hóa EC.

Trao đổi khóa EC Diffie-Hellman

Ngoài phương pháp trao đổi khóa Diffie-Hellman dựa trên tính chất một chiều của hàm logrith rời rạc. Ta có thể dùng dạng một chiều của đường cong Elliptic.

- Trước tiên, ta chọn số nguyên q lớn. Nếu q là nguyên tố thì sử dụng đường cong Elliptic $\mathbb{Z}_p$ hoặc q có dạng 2^m thì sử dụng đường cong $GF(2^m)$
- Chọn hai tham số a, b tương ứng để tạo thành nhóm $E_q(a, b)$. Ta gọi G là điểm cơ sở của nhóm nếu tồn tại một số nguyên n sao cho $nG = O$. Số nguyên n nhỏ nhất như thế được gọi là *hạng* của G

Trao đổi khóa EC Diffie-Hellman

Trong trao đổi khóa EC Diffie-Hellman, ta chọn một điểm G có hạng n lớn, và cách thức trao đổi khóa giữa người A và người B như sau:

1. Người A chọn số $n_A < n$ và giữ bí mật n_A này, sau đó trong $E_q(a, b)$ người A tính $P_A = n_A G$ và gửi P_A cho người B
2. Tương tự B chọn một số bí mật n_B, tính P_B và gửi P_B cho người A
3. A tạo khóa phiên bí mật là $K = n_A P_B = n_A nBG$
4. B tạo khóa phiên bí mật là $K = n_B P_A = n_B n_A G = n_A n_B G$ (nhóm Abel có tính giao hoán) giống với khóa của người A

Trao đổi khóa EC Diffie-Hellman

- *Nhận xét:* Kẻ thám mã T có thể có được P_A và P_B, tuy vậy T chỉ có thể tính được:

$$P_A + P_B = n_A G + n_B G = (n_A + n_B)G$$

Để tính $K = n_A n_B G$, T phải tìm được n_A, n_B từ P_A, P_B và G $=>$ Bất khả thi

Chú ý: khóa phiên K là một điểm trên đường cong Elliptic, để sử dụng khóa này cho mã hóa đối xứng như *DES* hay *AES* thì ta cần chuyển K về số thường.

Mã hóa và giải mã EC

- Như vấn đề trao đổi khóa, trong mã và giải mã ta cũng chọn các tham số để tạo một nhóm Abel $E_q(a, b)$ và một điểm cơ sở G có hạng n lớn.
- Khóa riêng K_R và khóa công khai K_U được tính theo công thức sau:

$$K_R = (d, G, q, a, b)$$

$$K_U = (E, G, q, a, b)$$

Trong đó, $d < n$ và $E = dG$, với d là số bí mật do người sinh khóa chọn. Do tính chất hàm 1 chiều từ E và G ta không thể xác định được d

Mã hóa và giải mã EC - Phương pháp Elgamal

- Giả sử *An* muốn gửi thông điệp M cho *Bình*, trước hết *An* chuyển M từ dãy bít sang dạng điểm $P_M = (x, y)$. Bản mã C_M (dùng khóa public của *Bình*) được tính là cặp điểm như sau:

$$C_M = (kG, P_M + kE)$$

  với k là số ngẫu nhiên do *An* chọn

- Để giải mã dùng khóa riêng,*Bình* sẽ nhân điểm thứ nhất trong C_M với d, sau đó lấy điểm thứ hai trừ cho kết quả:

$$P_M + kE - dkM = P_M + kdG - kdG = P_M$$

Mã hóa và giải mã EC - Phương pháp Elgamal

- *Nhận xét*:
  - Trong phương thức mã hóa, *An* đã che dấu P_M bằng cách cộng P_M với kE, để giải mã *Bình* trừ lại kE
  - Thay vì gửi trực tiếp k cho *Bình* để *Bình* tính kE (thám mã T có thể chặn được), *An* gửi một *dấu hiệu* là kG. Dựa vào kG và d *Bình* có thể tính kE, còn thám mã T dù biết G và kG nhưng vẫn không thể tính được k $=>$ do tính chất của hàm môt chiều.

Mã hóa và giải mã EC - Phương pháp Elgamal

- *Thí dụ*: giả sử ta chọn $p = 751, a = 1, b = 188$, ta có phương trình đường cong Elliptic trên $\mathbb{Z}_{751}$ như sau:

$$y^2 \ mod \ 751 = (x^3 + x + 188) \ mod \ 751$$

Ta chọn điểm cơ sở $G = (0, 376)$

  - Giả sử *An* cần mã hóa bản rõ là điểm $P_M = (562, 201)$, dùng khóa công khai $E = (201, 5)$, *An* chọn $k = 386$. Ta có:

$$386(0, 376) = (676, 558)$$

$$(562, 201) + 386(201, 5) = (385, 328)$$

Vậy bãn mã là cặp điểm $\{(676, 558), (385, 328)\}$

Độ an toàn của ECC so với RSA

Hiện nay, phương pháp nhanh nhất để tính logarit đường cong Elliptic (tính k biết G và kG) là phương pháp **Pollar rho**, Cùng một độ an toàn thì mã hóa ECC chỉ dùng các phép tính có số bít nhỏ hơn nhiều lần so với mã hóa RSA.

Mã hóa đối xứng (số bít của khóa)	*Mã hóa ECC (số bít của n)*	*Mã hóa RSA (số bít của N)*
56	112	512
80	160	1024
112	224	2048
128	256	3072
192	384	7680
256	512	15360