TRƯỜNG ĐẠI HỌC BÁCH KHOA HÀ NỘI
HANOI UNIVERSITY OF SCIENCE AND TECHNOLOGY

Bảo mật và độ phức tạp tính toán

Mật mã trên đường cong Elliptic

Nội dung

- 1/ Đường cong elliptic
- 2/ Mật mã khóa công khai trên đường cong elliptic

Cơ sở toán

Cơ sở

- Nhóm
  - tập hợp G, phép toán 2 ngôi * thỏa
    - với mọi a,b thuộc G: a*b=c thuộc G
    - tính kết hợp (a*b)*c = a*(b*c)
    - phần tử đồng nhất (trung hòa) e: a*e=e*a=a
    - phần tử nghịch đảo: a*a-1=e
  - Nhóm G là nhóm giao hoán (nhóm Abel) nếu a*b=b*a
  - Nhóm G: có số lượng phần tử hữu hạn => nhóm hữu hạn. cấp/bậc của G = số lượng phần tử
  - nếu G là nhóm nhân hữu hạn, a thuộc G, bậc của a là n - nhỏ nhất thỏa a^n=1

- Nhóm cyclic
  - nhóm G,
  - mọi phần tử x được sinh từ phần tử g: x=g*g*g...
  - g là phần tử sinh, phần tử nguyên thủy

Trường hữu hạn Galois - GF

- Trường hữu hạn Galois GF là nhóm Abel trang bị thêm phép nhân và phần tử đơn vị 1:
  - phần tử đơn vị: a*1 = 1*a = a
  - Phần tử nghịch đảo a^{-1} : $a^{-1} . a = 1$
  - Phân phối phép cộng và phép nhân: a*(b+c)=a*b+a*c

- Ví dụ
  - trường Zp = {0,1,...,p-1}, p nguyên tố
  - phép +, * theo modulo p
- Nếu p - nguyên tố
  - Trường Fp = {0,1,...p-1}
- Nếu q = p^r, p nguyên tố
  - Trường F gồm các phần tử X thỏa Xq - X = 0 => là nghiệm của phương trình Xq-X=0

- Đặc số của một trường
  - cho trường K với phép nhân, phần tử đơn vị 1
  - đặc số của K: character K là số nguyên n nhỏ nhất sao cho
  - 1 + 1 + ... + 1 (n lần) = 0, nếu không tồn tại n => đặc số = 0
  - số nhỏ nhất đó - số nguyên tố p => trường đặc số p
  - Nếu F có đặc số p thì
  - $(a + b)^p = a^p + b^p$

  - Trường Fq (q=p^r)
    - phần tử a, bậc của a là số n>0 nhỏ nhất thỏa a^n = 1
    - bậc của a: là ước của q-1

- Đa thức trên trường GF(q)

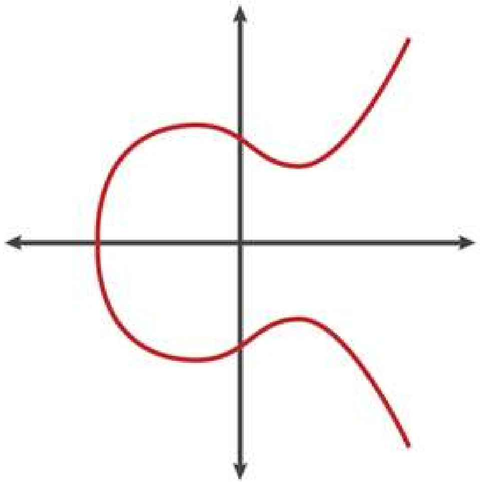
$$g(X) = g_0 + g_1X + g_2X^2 + \ldots + g_nX^n \text{ , hệ số } g_i \in GF(q), g_n <> 0$$

- Nếu g(x) phân tích thành tích 2 đa thức => gọi là rút gọn được
- Vd GF(2) = {0,1}, phép cộng là cộng modulo

  Đa thức $x^2 + 1$ rút gọn được

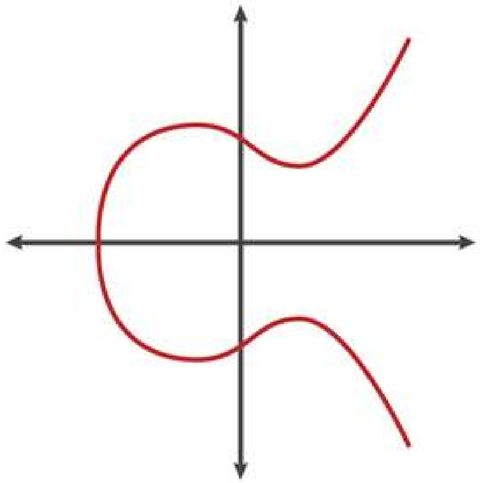
  Đa thức $x^2 + x + 1$ không rút gọn đc

1. Đường cong elliptic



Đường cong elliptic

- Đường cong elliptic trên trường số thực R
  - phương trình bậc 3
  - $y^2 + axy + by = x^3 + cx^2 + dx + e$, với a,b,c,d,e∈R
  - có thể đưa về dạng $y^2 = x^3 + dx + e$



- Đường cong elliptic trên trường hữu hạn F
  - Là tập điểm thỏa phương trình
    - $y^2 + axy + by = x^3 + cx^2 + dx + e$
  - Không kỳ dị - non singular
  - Với điểm O vô cực

  - Với trường F_p (p - nguyên tố)
    - Có thể biến đổi về dạng

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

    - điều kiện không kỳ dị: $4a^3 + 27b^2 \neq 0 \ mod \ p$

- Đường cong elliptic trên trường hữu hạn (Z_p hoặc F_q)
  - Đường cong EC trên F gồm các điểm thỏa phương trình $y^2 = x^3 + ax + b$ (1)
  - và điểm vô cực O
  - Số lượng các điểm nguyên là hữu hạn

  - Tìm các điểm của đường cong ED trên Z_p - $Z_p(a, b)$
    - với x: $x \in Z_p$, kiểm tra $x^3 + ax + b$ có phải là thặng dư bình phương

    sử dụng tiêu chuẩn Euler:

    p - nguyên tố lẻ, x là thặng dư bậc 2 mod p khi và chỉ khi $x^{(p-1)/2} \equiv 1 mod\ p$
    - tìm căn bậc 2:

    với p-nguyên tố p ≡3 mod 4

    Nếu z là thặng dư bình phương => căn bậc 2 của z là $z^{(p+1)/4} mod\ p$

- Đường cong elliptic trên trường hữu hạn Zp hoặc Fq
  - ví dụ: p=23, a=b=1
    - $4a^3 + 27b^2 \neq 0 \; mod \; 23$
    - với $x \in Z_p = \{0,1, \ldots, 22\}$ tính $z = x^3 + x + 1 \; mod \; 23$,

    kiểm tra z là thặng dư bình phương: $z^{(23-1)/2} = z^{11} \equiv 1 mod \; 23$?

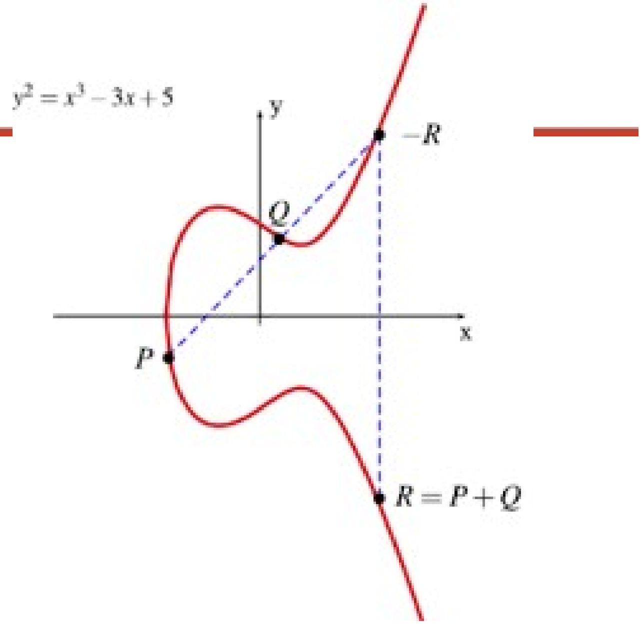
    tính căn của z: $z^{(23+1)/4} = z^6 \; mod \; 23$
    - x=1: z=3

      3^11 = 1 mod 23 => x=1 thuộc E(1,1)

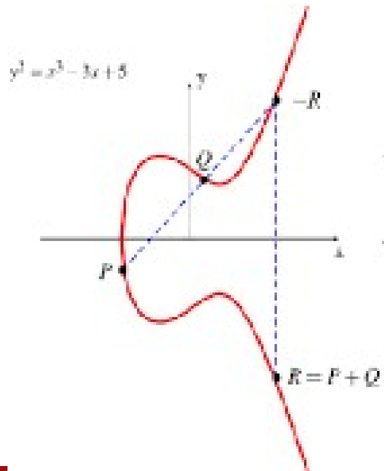
      3^6 = 16 mod 23 => nghiệm căn là 16 và 7

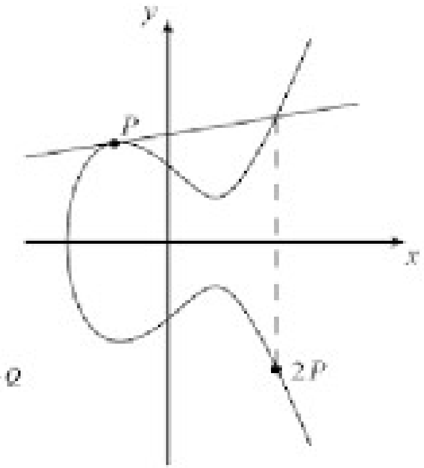
$$E_{23}(1,1) = \left\{ \begin{matrix} (0,1) & (0,22) & (1,7) & (1,16) & (3,10) & (3,13) & (4,0) \\ (5,4) & (5,19) & (6,4) & (6,19) & (7,11) & (7,12) & (9,7) \\ (9,16) & (11,3) & (11,20) & (12,4) & (12,19) & (13,7) & (13,16) \\ (17,3) & (17,20) & (18,3) & (18,20) & (19,5) & (19,18) & \end{matrix} \right\}$$

Phép toán trên EC



- Đường cong EC, các điểm trên đường cong E(a,b), điểm vô cực O
- Phép cộng
  - 2 điểm P ≠ Q trên EC, đường thẳng qua P, Q cắt tại 1 điểm -R, điểm đối xứng -R qua trục hoành => điểm R = P+Q
  - Nếu P, Q đối xứng qua Ox => Q = -P và đường nối P,-P cắt EC tại điểm vô cực O: P+(-P) = (-P) + P = O
  - Nếu P trùng Q - đường thẳng là tiếp tuyến tại P, cắt tại -R, điểm R = P + P





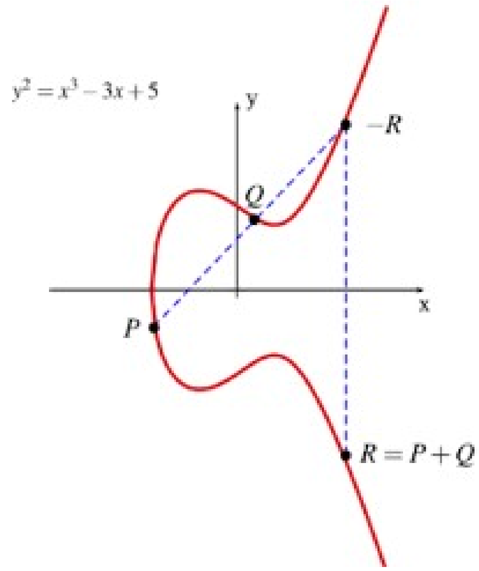
Phép toán trên EC

- Đường cong EC, các điểm trên đường cong E(a,b), điểm vô cực O
- Phép cộng P+Q
  - Biết tọa độ $P(x_1, y_1)$, $Q(x_2, y_2)$, Q ≠-P, có thể tính được tọa độ P+Q=$R(x_3, y_3)$:

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

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

    với
    - $\lambda = (y_2 - y_1)/(x_2 - x_1)$ khi P ≠ Q
    - và $\lambda = (3x_1^2 + a)/(2y_1)$ khi P=Q



- Phép cộng P+Q
  - ví dụ:
    - cho p=23, a=b=1: $y^2 = x^3 + x + 1\ (mod\ 23)$

    tập các điểm $E_{23}(1,1)$, cùng điểm vô cực O
    - xét 2 điểm: P(3,10), Q(5,19) thuộc E
      - P+Q=$R(x_3, y_3)$ => **R (18,3)** tính như sau

        $\lambda = (y_2 - y_1)/(x_2 - x_1)$ = (19-10)/(5-3) mod 23 = 9/2 mod 23 = 16

        $x_3 = \lambda^2 - x_1 - x_2$ = 16^2 - 3 - 5 = 248 mod 23 = 18

        $y_3 = \lambda(x_1 - x_3) - y_1$ = 16(3-18)-10 = 3 mod 23
      - P + P = $R(x_3, y_3)$ => **R (7,12)** tính như sau:

        $\lambda = (3x_1^2 + a)/(2y_1)$=(3*3^2+1)/2*10 mod 23 = 5/20 mod 23 = 6

        $x_3 = \lambda^2 - x_1 - x_2$ = 6^2 - 3 - 5 = 30 mod 23 = 7

        $y_3 = \lambda(x_1 - x_3) - y_1$ = 6(3-7)-10 = -34 mod 23 = 12 mod 23

Đường cong EC

- Ep(a,b) được trang bị phép + và điểm O => là nhóm Abel

Tính đóng: Nếu P, Q $\in E$ thì P + Q $\in E$.

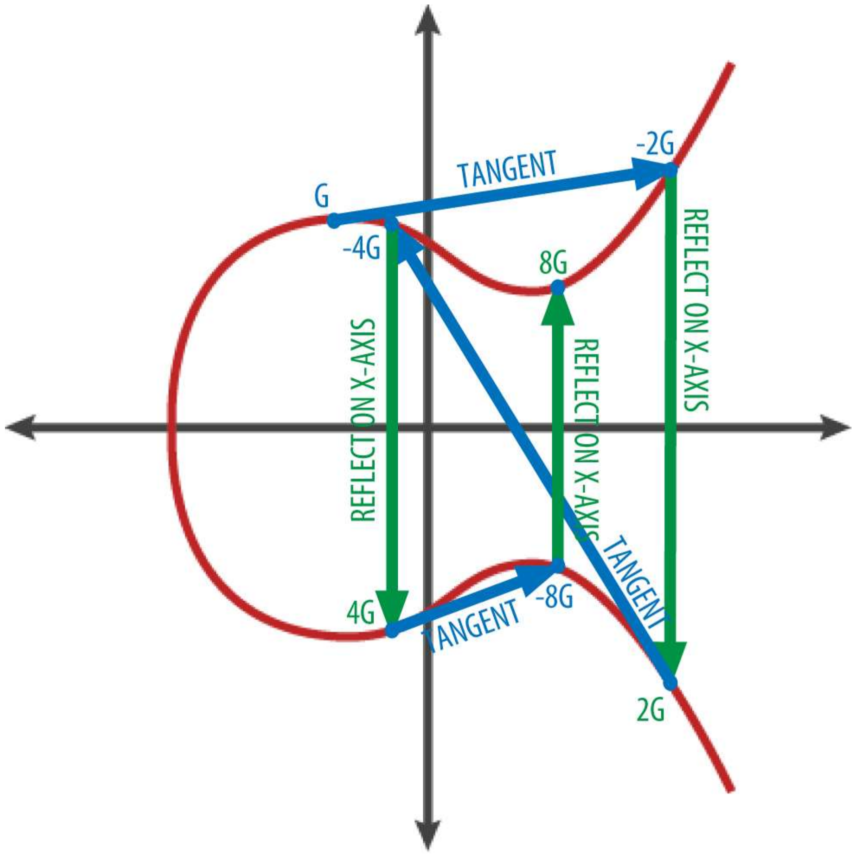
Tính kết hợp: Nếu P, Q, R $\in$ E thì P + (Q + R) = R + (Q + P).

Tồn tại phần tử trung hoà O: với mọi P $\in E$ thì P + O = O + P = P (theo định nghĩa).

Tồn tại phần tử nghịch đảo: với mỗi P(x, y) $\in E$ thì luôn tồn tạ phần tử -P(x, -y) $\in E$ để P + (-P) = O.

Tính chất giao hoán Nếu P, Q $\in E$ thì P + Q = Q + P.

- Phép nhân k*P
  - điểm P, số tự nhiên k
  - Phép cộng k lần: P + P +... + P = kP - tích k với P



2/ Mật mã đường cong elliptic

Mật mã đường cong elliptic

- Giới thiệu
  - Công bố 1991, đồng thời bởi Neals Koblitz, Victor Miller
  - Độ an toàn dựa trên bài toán logarithm rời rạc trên các điểm của đường cong EC (ECDLP - Elliptic Curve Discrete Logarithm Problem)

    hiện chưa tìm thấy thuật toán độ phức tạp dưới hàm mũ
  - Đã được nhiều nước đưa vào tiêu chuẩn (ANSI, IEEE, SECG, FIPS) như
    - GOST R34-10-2001
    - FIPS 186-3

- Bài toán ECDLP
  - Cho EC trên Zp

    Nhóm Ep(a,b)
  - xét phương trình Q = P+ P + .. + P = kP
    - Cho trước điểm P, số k => dễ tính Q
    - Cho trước điểm P và Q => khó tính k

  - vd n=100 = 1100100(2) = 2^6 + 2^5 + 2^2 => nP = 64P + 32P + 4P

- Cài đặt hệ mã
  - Thiết lập
    - Lựa chọn đường cong EC phù hợp - có tập các điểm $E_q(a,b)$
    - Điểm cơ sở G: sao cho bậc - số nhỏ nhất n để n*G = 0 là số nguyên tố lớn
  - Bản rõ M - mã hóa thành điểm P_M trên $E_p(a,b)$
  - Người dùng A
    - chọn $d_A < n$ nào đó, khóa bí mật (d_A) (và thông số hệ mã G, q,a,b)
    - tính $e_A = d_A * G$, khóa công khai (e_A , G, q,a,b)
  - Mã hóa dữ liệu gửi A
    - chọn số nguyên ngẫu nhiên *k*, bản mã là cặp điểm P_C :

    $P_C = [(k*G),(P_M + k*e_A)]$
  - Giải mã: lấy điểm (k*G) nhân với khóa bí mật nA, điểm thứ 2 trừ đi kết quả

    $(P_M + k*e_A) - d_A (k*G) = (P_M + k* d_A * G) - d_A (k*G) = P_M$ => tính được bản rõ

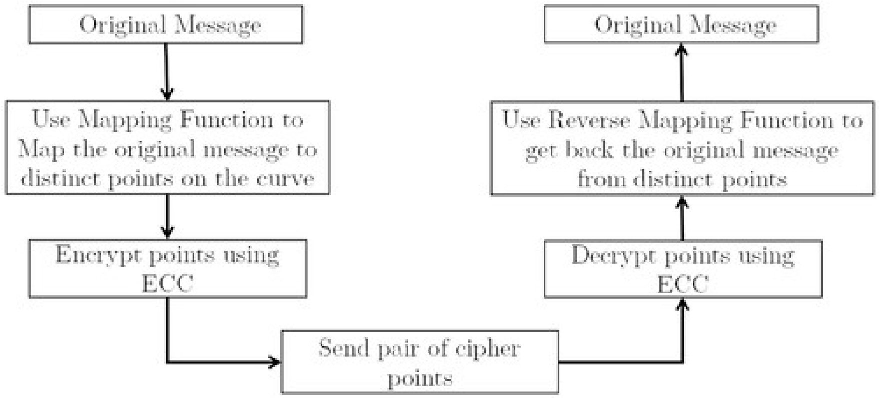
- Ưu điểm của hệ mã ECC
  - Độ an toàn tương đương với khóa nhỏ hơn RSA nhiều lần
  - dẫn đến có thể cài đặt trên các thiết bị tài nguyên tính toán giới hạn

Mã hóa RSA (bit của N)	Mã hóa ECC (bit của n)
512	112
1,024	160
2,048	224
3,072	256
7,680	384
15,360	512

- Trao đổi khóa
  - Diffie - Hellman

Alice				Bob		
Bí mật	Công khai	Tính	Gửi	Tính	Công khai	Bí mật
a	p, g		p,g$\rightarrow$			b
a	p, g, A	g^a mod p = A	A$\rightarrow$		p, g	b
a	p, g, A		$\leftarrow$ B	g^b mod p = B	p, g, A, B	b
a, **s**	p, g, A, B	B^a mod p = s		A^b mod p = s	p, g, A, B	b, **s**

- Ánh xạ bản rõ thành điểm trên EC:
  - thuật toán của Koblitz
  - Zp, trường Galois 2^q



Tham khảo: Cơ sở toán học liên quan

Cơ sở

- Nhóm
  - tập hợp G, phép toán 2 ngôi * thỏa
    - với mọi a,b thuộc G: a*b=c thuộc G
    - tính kết hợp (a*b)*c = a*(b*c)
    - phần tử đồng nhất (trung hòa) e: a*e=e*a=a
    - phần tử nghịch đảo: a*a-1=e
  - Nhóm G là nhóm giao hoán (nhóm Abel) nếu a*b=b*a
  - Nhóm G: có số lượng phần tử hữu hạn => nhóm hữu hạn. cấp/bậc của G = số lượng phần tử
  - nếu G là nhóm nhân hữu hạn, a thuộc G, bậc của a là n - nhỏ nhất thỏa a^n=1

- Nhóm cyclic
  - nhóm G,
  - mọi phần tử x được sinh từ phần tử g: x=g*g*g...
  - g là phần tử sinh, phần tử nguyên thủy

Trường hữu hạn Galois - GF

- Trường hữu hạn Galois GF là nhóm Abel trang bị thêm phép nhân và phần tử đơn vị 1:
  - phần tử đơn vị: a*1 = 1*a = a
  - Phần tử nghịch đảo a^{-1} : $a^{-1} . a = 1$
  - Phân phối phép cộng và phép nhân: a*(b+c)=a*b+a*c

- Ví dụ
  - trường Zp = {0,1,...,p-1}, p nguyên tố
  - phép +, * theo modulo p
- Nếu p - nguyên tố
  - Trường Fp = {0,1,...p-1}
- Nếu q = p^r, p nguyên tố
  - Trường F gồm các phần tử X thỏa Xq - X = 0 => là nghiệm của phương trình Xq-X=0

Đặc số của một trường

- cho trường K với phép nhân, phần tử đơn vị 1
- đặc số của K: character K là số nguyên n nhỏ nhất sao cho
- 1 + 1 + ... + 1 (n lần) = 0, nếu không tồn tại n => đặc số = 0
- số nhỏ nhất đó - số nguyên tố p => trường đặc số p
- Nếu F có đặc số p thì
- $(a + b)^p = a^p + b^p$

- Trường Fq (q=p^r)
  - phần tử a, bậc của a là số n>0 nhỏ nhất thỏa a^n = 1
  - bậc của a: là ước của q-1

- Đa thức trên trường GF(q)

$$g(X) = g_0 + g_1X + g_2X^2 + \ldots + g_nX^n \text{ , hệ số } g_i \in GF(q),\ g_n <> 0$$

- Nếu g(x) phân tích thành tích 2 đa thức => gọi là rút gọn được
- Vd GF(2) = {0,1}, phép cộng là cộng modulo

  Đa thức $x^2 + 1$ rút gọn được

  Đa thức $x^2 + x + 1$ không rút gọn đc