FACULTY OF INFORMATION TECHNOLOGY

UNIVERSITY OF SCIENCE, HO CHI MINH CITY, VIET NAM

TRƯỜNG ĐẠI HỌC KHOA HỌC TỰ NHIÊN

KHOA CÔNG NGHỆ THÔNG TIN

BÁO CÁO LAB 1 MÔN CÔNG NGHỆ CHUỖI KHỐI – K31

THUẬT TOÁN ECC VÀ ỨNG DỤNG CHO CHỮ KÝ SỐ

A. THÔNG TIN CHUNG

Học viên thực hiện: Nguyễn Thị Ngọc Trâm

Mã số học viên: 21C11036

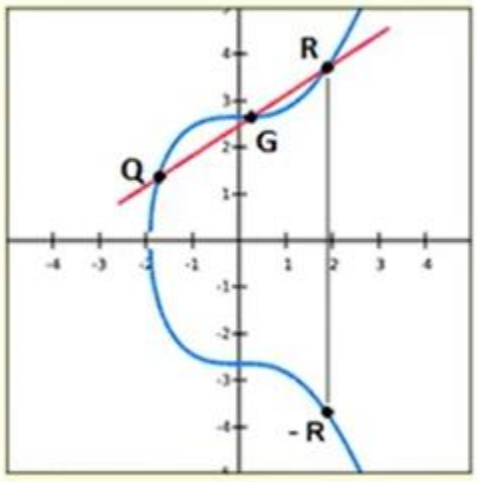
Khóa: 31 Ngành: Khoa học máy tính

B. NỘI DUNG BÁO CÁO

1. GIỚI THIỆU THUẬT TOÁN ECC

Phương trình đường cong elip có dạng $y^2 = x^3 + ax + b$

Trường hợp 1: Hai điểm phân biệt Q và G



Cho 2 điểm nằm trên đường cong elip G(x, y), Q(x1, y1)

Kẻ một đường thẳng từ Q đến G, đường thẳng cắt đường cong tại điểm thứ 3 là R(x2, y2)

Đối xứng điểm R qua trục x ta được điểm -R(x2, -y2)

Tìm tọa độ của -R

Tìm hệ số góc k của đường thẳng đi qua hai điểm

k = (y-y1)/(x-x1) (1)

k(x-x1) = (y-y1)

y = k(x-x1) + y1

y = kx-kx1+y1

y = kx + y1 - kx1

Đặt B = y1 - kx1

y = kx + B (phương trình đường thẳng)

$y^2 = (kx + B)^2$

Kết hợp với đường cong elip $y^2 = x^3 + ax + b$

$x^3 + ax + b = (kx + B)^2$

$x^3 + ax + b = (kx)^2 + 2kxB + B^2$

$x^3 + ax + b = (kx)^2 + 2kxB + B^2$

$x^3 + ax + b - (kx)^2 - 2kxB - B^2 = 0$

$x^3 - k^2x^2 + (a - 2kB)x + b - B^2 = 0$

=> Dạng đa thức monic, do có hệ số của nghiệm có lũy thừa cao nhất x^3 = 1.

Tính chất của đa thức monic: Tổng các nghiệm bằng **âm** hệ số của nghiệm có lũy thừa cao thứ hai.

Đặt x, x1, x2 lần lượt là 3 nghiệm của đa thức trên.

$x + x1 + x2 = k^2$

$x2 = k^2 - x - x1$ (2)

Điểm R nằm trên đường thẳng y = kx+B

$y2 = kx2 + B$

$y2 = kx2 + y1 - kx1$

$y2 = k(x2 - x1) + y1$

Đối xứng điểm R qua trục x ta được điểm -R(x2, -y2)

$y2 = k(-x2 + x1) - y1$

$y2 = k(x1 - x2) - y1$ (3)

(1)(2)(3)

k=(y-y1)/(x-x1)

$x2 = k^2 - x - x1$

$y2 = k(x1 - x2) - y1$

Công thức trên cho ra những số thực (số thập phân, số âm hoặc số dương)

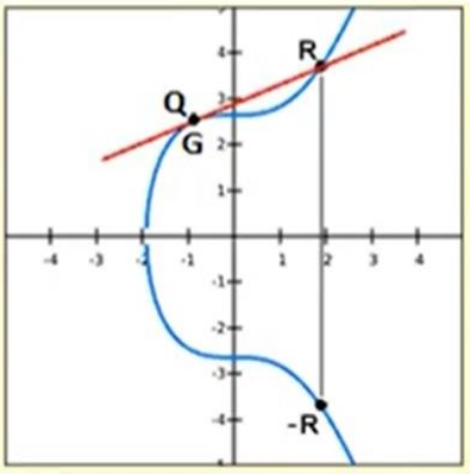
Trong ECC chỉ sử dụng số nguyên, nếu làm tròn số thập phân thành số nguyên sẽ có sai số. => mod P với P là số nguyên tố 32byte

k = (y-y1)/(x-x1)mod P hay k = (y-y1)*nghịch đảo modulo(x-x1)mod P

$x2 = k^2 - x - x1$ mod P

$y2 = k(x1 - x2) - y1$ mod P

Trường hợp 2: Hai điểmt Q và G trùng nhau



Phương trình đường cong elip

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

$2y = 3x^2 + a$ (lấy đạo hàm)

$2ydy = 3x^2dx + adx$ (lấy vi phân)

$2ydy = 3x^2dx$ (trong ECC a=0)

$\frac{dy}{dx} = \frac{3x^2}{2y}$ = k (1)

(Hệ số góc của đường thẳng tiếp tuyến đường cong tại 1 điểm)

Sử dụng cách làm như trên đến khi chuyển thành đa thức monic:

$x + x1 + x2 = k^2$

Do Q và G trùng nhau nên

$x + x + x2 = k^2$

$x2 = k^2 - 2x$ (2)

Điểm R nằm trên đường thẳng y=kx+B

$y2 = kx2 + B$

$y2 = kx2 + y1 - kx1$

$y2 = k(x2 - x1) + y1$

Đối xứng R qua trục x

$y2 = k(x1 - x2) - y1$ (3)

Modulo cho P:

$k = \frac{3x^2}{2y} mod\ P$

$$x2 = k^2 - 2x \bmod P$$

$$y2 = k(x1 - x2) - y1 \bmod P$$

Kết quả code thực nghiệm:

Input: G (random), Private Key (>0 và <=N)

Output: Public Key (Uncompress/compress)

```
(base) O:\POSTGRAD\HK5\Blockchain\Lab1>py ECC.py
Private Key:  03c256cc8d3796fb6702f79a4041d4146e5d308b769c3acc871a47d101f4107d
N:  115792089237316195423570985008687907852837564279074904382605163141518161494337
Prime: 115792089237316195423570985008687907853269984665640564039457584007908834671663
Uncompressed public key:  04f9308a019258c31049344f85f89d5229b531c845836f99b08601f113bce036f9388f7b0f632de8140fe337e62a37f3566500a99934c2231b6cb9fd7584b8e672
Compressed public key:  02f9308a019258c31049344f85f89d5229b531c845836f99b08601f113bce036f9
Total runtime of ECC:  0.0002872999999999973
```

Github: https://github.com/ntngoctram98/Blockchain

2. ỨNG DỤNG CHO CHỮ KÝ SỐ

2.1. Chữ ký số

Chữ ký số là một công cụ mã hóa để ký thông điệp và xác minh thông điệp bằng chữ ký cung cấp bằng chứng về tính xác thực của tin nhắn số và tài liệu điện tử.

Chữ ký số cung cấp:

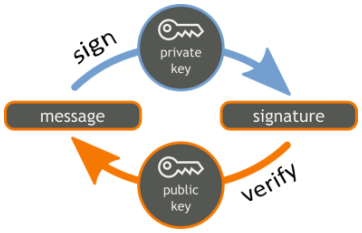
+ Thông điệp xác thực: người gửi đã biết, tạo và ký

+ Tính toàn vẹn của thông điệp: không bị thay đổi sau khi ký

+ Chống từ chối: không thể từ chối ký tài liệu sau khi chữ ký được tạo.

Ứng dụng: thanh toán ngân hàng (chuyển tiền); trao đổi các tài liệu đã ký, giao dịch blockchain (chuyển coins, mã thông báo);…

Digital signature schemes:



Thông điệp được ký bởi người gửi sử dụng private key, được hash và ký bằng thuật toán ký (RSA, ECC)

Chữ ký được verified bởi public key tương ứng trả về giá trị Boolean (valid/invalid).

Kết quả code:

```
Message: Message for ECDSA signing
Private key: 0xc374556584db050001c2c9265b546e66d3dbbe8239d17427c176d834a19638dc
Signature: r=0xd034c98af3274ad93f3c8ce944bbc17b11b6aa170c5f097ed98687fa0d93347c, s=0xa2318ceea2002caba38efbba3bf8ef8d43236a6edc33c040734d8eb2ed77f608

Message: Message for ECDSA signing
Public key: (0x10b5d9028ec828a0f9111e36f046afa5a0c677357351093426bcec10c663db7d, 0x271763c56fcd87b72d59ceaa5b9c3fd2122788fe344751a9bde373f903e5bb20)
Signature valid? True

Message: Tampered message
Signature (tampered msg) valid? False

Message: Message for ECDSA signing
Signature: r=0xd034c98af3274ad93f3c8ce944bbc17b11b6aa170c5f097ed98687fa0d93347c, s=0xa2318ceea2002caba38efbba3bf8ef8d43236a6edc33c040734d8eb2ed77f608
Recovered public key from signature: (0x1353fd26a6cb6110980cfd2bb5eca3b3cc3e08c930ad5991395dd826a250c79, 0xba6825142e230ee1fa2b406f3f9158a47ee49daca8ac47898c5fd92d805a101e)
Recovered public key from signature: (0x10b5d9028ec828a0f9111e36f046afa5a0c677357351093426bcec10c663db7d, 0x271763c56fcd87b72d59ceaa5b9c3fd2122788fe344751a9bde373f903e5bb20)
```

Github:

https://github.com/ntngoctram98/Blockchain

C. TÀI LIỆU THAM KHẢO

https://cryptobook.nakov.com/digital-signatures

https://github.com/tintinweb/ecdsa-private-key-recovery

https://github.com/nakov/Practical-Cryptography-for-Developers-Book/blob/master/digital-signatures/ecdsa-sign-verify-examples.md