ĐẠI HỌC QUỐC GIA HÀ NỘI
TRƯỜNG ĐẠI HỌC CÔNG NGHỆ

ĐÀO VIỆT ANH

NGHIÊN CỨU MỘT SỐ CHỮ KÝ ĐẶC BIỆT TRÊN ĐƯỜNG CONG ELLIPTIC

Ngành: CÔNG NGHỆ THÔNG TIN

Mã số:

TÓM TẮT LUẬN VĂN THẠC SĨ

HẢI PHÒNG – 2011

Chương 1. CÁC KHÁI NIỆM CƠ BẢN

1.1. MỘT SỐ KHÁI NIỆM TRONG SỐ HỌC

1.1.1. Số nguyên tố

Số nguyên $a > 1$ được gọi là *số nguyên tố,* nếu a chỉ có ước số là 1 và a.

Một số nguyên lớn hơn 1 không là số nguyên tố thì được gọi là hợp số.

Ví dụ các số 2, 3, 5, 7 là số nguyên tố; các số 6, 8, 10, 12, 14, 15 là hợp số.

Hai số a và b được gọi là *nguyên tố cùng nhau,* nếu chúng có ước số chung là 1, tức là nếu gcd $(a,b) = 1$.

Định lý 1.1 (Thuật toán Euclid tìm ước số chung lớn nhất)

Với mọi $a, b \in Z, b \neq 0$, tồn tại duy nhất $q, r \in Z$ để: $a = bq + r,\ 0 \leq r < |b|$

Nếu $r = 0$ thì $b|a$, nghĩa là b là ước số của a.

Ngược lại thì $b \nmid a$. Với $a_1, \ldots, a_k \in Z$, nếu $b|a_i$ $(i = 1, \ldots, k)$ thì b gọi là ước chung của $a_1, \ldots, a_k$. Ước chung lớn nhất của $a_1, \ldots, a_k$ ký hiệu là gcd$(a_1, \ldots, a_k)$.

Định lý 1.2

Nếu $a, b \in Z$ và khác 0 thì $d = \gcd(a, b)$ là phần tử nhỏ nhất trong tất cả các số nguyên dương có dạng $ax + by$ (x, $y \in Z$)

Hệ quả 1.3

Tồn tại $x, y \in Z$ thỏa mãn:

$$ax + by = c$$

khi và chỉ khi $d|c$ với $d = \gcd(a, b)$

Định lý 1.4

Với $a, m \in Z$, tồn tại $x \in Z$ thỏa mãn $ax \equiv 1 \bmod m$ khi và chỉ khi gcd$(a, m) = 1$.

Định lý 1.5 (Định lý phần dư Trung Quốc)

Giả sử $m_1, \ldots, m_r \in N$ đôi một nguyên tố cùng nhau, gcd$(m_i, m_j) = 1$ với mọi $i \neq j$. Có $a_1, \ldots, a_r \in Z$. Khi đó, hệ phương trình

$$x \equiv a_i \,(mod\ m_i)\ (1 \leq i \leq r)$$

có một nghiệm duy nhất theo modulo $M = m_1 x \ldots x m_r$ là

$$x = \sum_{i=1}^{r} a_i M_i y_i \bmod M$$

trong đó $M_i = M/m_i$ và $M_i y_i \equiv 1 \ mod \ m_i$

Định lý 1.7 (Euler)

Với $a, m \in Z$ thỏa mãn gcd(a, m) = 1,

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

Định lý 1.8 (Fermat)

Cho p là số nguyên tố và $a \in Z$. Khi đó, ta có:

(1) $a^{p-1} \equiv 1 \bmod p$, nếu $p \not| a$.

(2) $a^p \equiv a \bmod p$

1.2. MỘT SỐ KHÁI NIỆM TRONG ĐẠI SỐ

1.2.1. Khái niệm Nhóm, Vành, Trường

1/. Nhóm

Nhóm là cấu trúc bao gồm tập G và toán tử hai ngôi * trên G. Với $a, b \in G$, $a * b \in G$ được định nghĩa như sau:

1. $a * (b * c) = (a * b) * c$ với mọi $a, b, c \in G$
2. Tồn tại $e \in G$ thỏa mãn $e * a = a * e = a$ với mọi $a \in G$, (e được gọi là phần tử trung hòa).
3. Với mỗi $a \in G$, tồn tại một phần tử $b \in G$ thỏa mãn $b * a = a * b = e$

(b là duy nhất và được gọi là phần tử nghịch đảo của a)

Ký hiệu $\langle G,* \rangle$ là nhóm nhân và $\langle G,+ \rangle$ là nhóm cộng. Trong nhóm cộng, phần tử trung hòa là 0 và phần tử nghịch đảo của a là $-a$. Trong nhóm nhân, phần tử trung hòa là 1 và phần tử nghịch đảo của a là a^{-1}.

$\langle G,* \rangle$ được gọi là nhóm Abel nếu $a * b = b * a$ với mọi a, b thuộc G.

2/. Vành

Vành là tập R với 2 toán tử cộng (+) và nhân (.) với các điều kiện sau:

1. $\langle R,+ \rangle$ là nhóm Abel.
2. $a \ . \ (b \ . \ c) = (a \ . \ b) \ . \ c$ với mọi $a, b, c \in R$.

3. $a \,.\, (b + c) = a \,.\, b + a \,.\, c$ và $(a + b) \,.\, c = a \,.\, c + b \,.\, c$ với mọi $a, b, c \in R$.

3/. Trường

Trường F là vành với phần tử đơn vị $e \neq 0$ và $F^* = \{a \in F \mid a \neq 0\}$ là một nhóm nhân.

Định lý 1.11

Vành Z_p là một trường khi và chỉ khi p là số nguyên tố.

1.2.2. Trường hữu hạn

Trường hữu hạn là trường có hữu hạn các phần tử ký hiệu là F_q hoặc $GF(q)$ với q là số các phần tử.

Định lý 1.14

F là trường mở rộng bậc n trên trường hữu hạn K. Nếu K có q phần tử thì F có q^n phần tử.

Định lý 1.15

Trường hữu hạn $F = F_{p^n}$ là một trường mở rộng của Z_p bậc n và mọi phần tử của F_{p^n} là một nghiệm của đa thức $x^{p^n} - x$ trên Z_p.

1.3. KHÁI NIỆM VỀ ĐỘ PHỨC TẠP CỦA THUẬT TOÁN

1.3.1. Khái niệm thuật toán

Thuật toán là một dãy hữu hạn các thao tác được bố trí theo một trình tự xác định nhằm giải quyết một bài toán..

1.3.2. Độ phức tạp của thuật toán

Trước hết, hiểu *độ phức tạp tính toán* (về không gian hay về thời gian) của một tiến trình tính toán là số ô nhớ được dùng hay số các phép toán sơ cấp được thực hiện trong tiến trình tính toán đó.

1.3.3 Một số lớp bài toán

Ta ký hiệu lớp tất cả với các bài toán giải được bởi thuật toán không đơn định trong thời gian đa thức là *NP*.

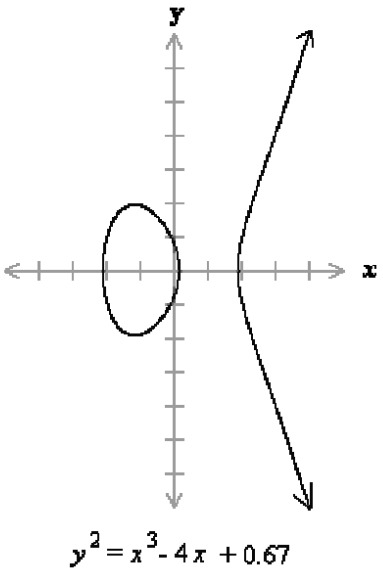
Người ta đã chứng tỏ được rằng tất cả những bài toán trong các ví dụ kể trên và rất nhiều các bài toán tổ hợp thường gặp khác đều thuộc lớp *NP*, dù rằng hầu hết chúng đều chưa được chứng tỏ là thuộc P. Một bài toán A được gọi là *NP*-đầy đủ, nếu $A \in NP$ và với mọi $B \in NP$ đều có $B \alpha A$.

Chương 2. **SƠ ĐỒ CHỮ KÝ TRÊN ĐƯỜNG CONG ELLIPTIC**

2.1. ĐƯỜNG CONG ELLIPTIC

2.1.1. Đường cong Elliptic theo công thức Weierstrass

Gọi K là trường hữu hạn hay vô hạn. Đường cong elliptic được định nghĩa trên trường K bằng công thức Weierstrass: $y^2+a_1xy+a_3y=x^3+a_2x^2+a_4x+a_6$, trong đó $a_i \in K$.



Hình 2.1. Một ví dụ về đường cong elliptic

2.1.2. Đường cong Elliptic trên trường Galois

Nhóm E trên trường Galois $E_p(a,b)$ nhận được bằng cách tính $x^3 + ax + b \bmod p$ với $0 \le x < p$.

Các hằng số a, b là các số nguyên không âm và nhỏ hơn số nguyên tố p và thỏa mãn điều kiện:

$4a^3 + 27b^2 \bmod p \neq 0$.

2.1.3. Đường cong Elliptic trên trường hữu hạn

Đường cong elliptic được xây dựng trên các trường hữu hạn. Có hai trường hữu hạn thường được sử dụng: trường hữu hạn Fq với q là số nguyên tố hoặc q là 2^m (m là số nguyên).

Tùy thuộc vào trường hữu hạn F_q, với mỗi bậc của q, tồn tại nhiều đường cong elliptic. Do đó, với một trường hữu hạn cố định có q phần tử và q lớn, có nhiều sự lựa chọn nhóm đường cong elliptic.

2.1.3.1 Đường cong elliptic trên trường F_P (p là số nguyên tố)

Cho p là số nguyên tố (p > 3), Cho a, b ∈ Fp sao cho $4a^3 + 27b^2 \neq 0$ trong trường F_p. Một đường cong elliptic $E(F_p)$ trên F_p (được định nghĩa bởi các tham số a và b) là một tập hợp các cặp giá trị (x, y) (x, y ∈ Fp) thỏa công thức: $y^2 = x^3 + ax + b$.

cùng với một điểm O – gọi là điểm tại vô cực. Số lượng điểm của E(Fp) là #E(Fp) thỏa định lý Hasse:

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

2.1.3.2 Đường cong elliptic trên trường F_2^m

Một đường cong elliptic $E(F_2^m)$ trên F_2^m được định nghĩa bởi các tham số a, b ∈ F_2^m (với b ≠ 0) là tập các điểm (x, y) với x ∈ F_2^m, y ∈ F_2^m thỏa công thức:

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

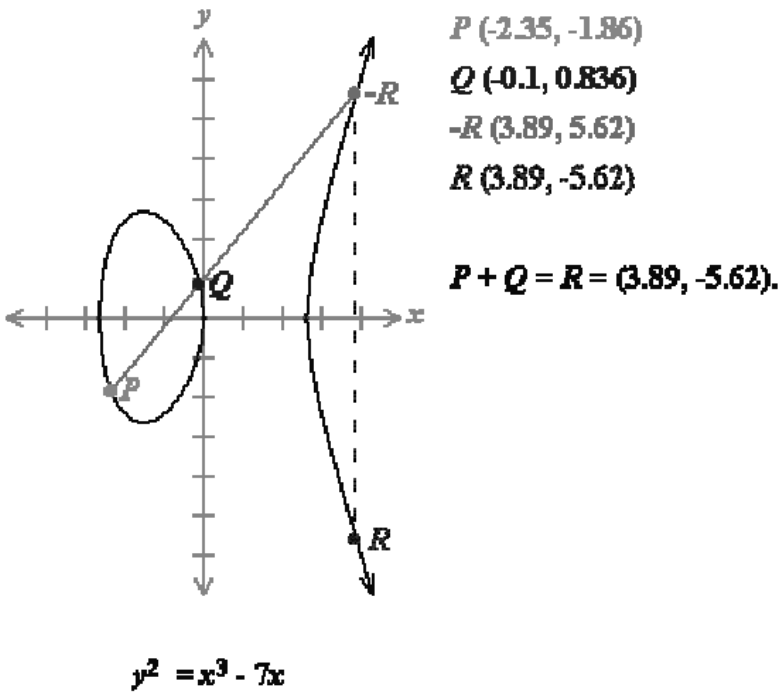
cùng với điểm O là điểm tại vô cực. Số lượng các điểm thuộc $E(F_2^m)$ ký hiệu $\#E(F_2^m)$ thoả định lý Hasse:

$$q + 1 - 2\sqrt{q} \leq \#E\left(F_{2^m}\right) \leq q + 1 + 2\sqrt{q}$$

trong đó $q = 2^m$. Ngoài ra, $\#E(F_2^m)$ là số chẵn.

2.1.4 CÁC PHÉP TOÁN TRÊN ĐƯỜNG CONG ELLIPTIC

2.1.4.1 Phép cộng

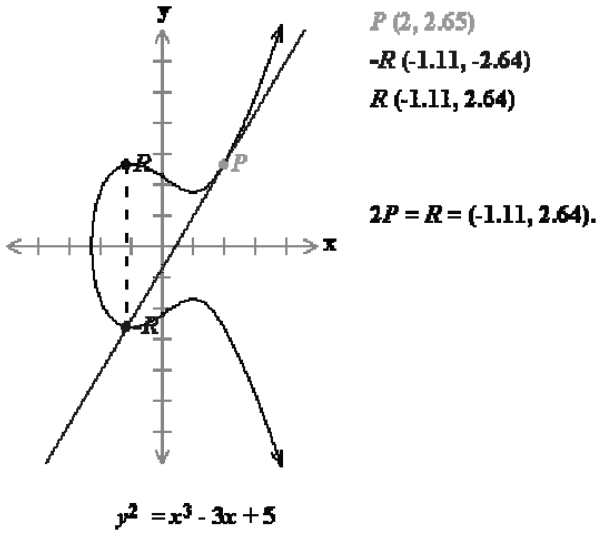


Hình 2.3. Phép cộng trên đường cong elliptic

Để tìm điểm R, ta nối P và Q bằng đường thẳng L. Đường thẳng L sẽ cắt E tại ba điểm P, Q và –R(x, y). Điểm R(x, –y) sẽ có tung độ là giá trị đối của y.

2.1.4.2 Phép nhân

Phép nhân đôi



Hình 2.4. Phép nhân đôi trên đường cong elliptic

Xét phép nhân đôi (EDBL): nếu cộng hai điểm P, Q ∈ E(R) với P = Q thì đường thẳng L sẽ là tiếp tuyến của đường cong elliptic tại điểm P. Trường hợp này điểm –R sẽ là giao điểm còn lại của L với E. Lúc đó R = 2P.

Phép nhân kP

Phép nhân kP nhận được bằng cách thực hiện lặp k lần phép cộng.

2.1.5 SỐ ĐIỂM TRÊN ĐƯỜNG CONG ELLIPTIC VỚI TRƯỜNG F_Q

Việc xây dựng các hệ mật mã trên đường cong elliptic bao gồm việc lựa chọn đường cong E thích hợp và một điểm G trên E gọi là điểm cơ sở. Xét trường K là F_q.

Định lý (Hasse)

N là số điểm của E trên trường F_q (trường hữu hạn q phần tử). Khi đó: $|N - (q + 1)| \leq 2\sqrt{q}$ Từ định lý Hasse suy ra $\#E(F_q) = q + 1 - t$ trong đó $|t| \leq 2\sqrt{q}$.

Định nghĩa Bậc của một đường cong elliptic là số điểm của đường cong đó.

Bậc của điểm G thuộc E là số k sao cho $kG = O$; khi $k = \#E(F_q)$ thì G là điểm cơ sở của E.

2.2. MỘT SỐ SƠ ĐỒ CHỮ KÝ TRÊN ĐƯỜNG CONG ELLIPTIC

2.2.1 NHÚNG BẢN RÕ VÀO ĐƯỜNG CONG ELLIPTIC

Nhúng bản rõ lên **E** là biểu diễn lại bản rõ đó như là các điểm trên **E**, nhờ đó có thể thực hiện được các tính toán trên **E**. Có một số phương pháp để thực hiện việc này. Trong đó có 2 phương pháp chính là "nhúng" (**imbeding**) và "mặt nạ" (**mask**).

2.2.1.1 Phép nhúng (Imbeding)

Cách 1

Để nhúng m lên $E(Z_p)$ với p là số nguyên tố, chẳng hạn $p \equiv 3 \pmod 4$. Giả sử $E(Z_p)$ được cho bởi phương trình $y^2 = x^3 + ax^2 + b$ và giả sử m là số nguyên thỏa mãn $0 \leq m \leq p/1000 - 1$.

Thêm 3 chữ số vào m được x thỏa mãn $1000m \leq x \leq 1000(m+1) < p$ Chúng ta sẽ bổ sung các chữ số khác nhau cho đến khi tìm được x sao cho $f(x) = x^3 + ax + b$ là một số chính phương trong Z_p và y (với $f(x) = y^2 \bmod p$) thỏa mãn $y \neq -1 \bmod p$.

Điểm P_m được tạo thành khi nhúng m lên E là:

$$P_m = (x, f(x))$$

Có thể dễ dàng khôi phục lại m từ $P_m \in E(Z_p)$ bằng cách loại bỏ 3 chữ số cuối của tọa độ x của điểm P_m.

Cách 2

Bước 1

Sử dụng bảng chữ cái gồm N ký tự. Chia bản rõ thành các khối có độ dài cố định l. Các ký tự được đánh số là $0,..., N-1$. Một khối văn bản w cùng với các số $0 \le x_w \le N^l$ tạo thành một ánh xạ:

$$w = (a_0 a_1 ... a_{l-1}) \mapsto x_w = a_0 N^{l-1} + a_1 N^{l-2} + \cdots + a_{l-2} N + a_{l-1}, \quad 0 \le x_w \le N^t$$

Bước 2 Chọn một giá trị k thích hợp sao cho $kN^l < q$. Với mỗi j là phần tử của F_q tính $kx_w + j$. Lấy điểm P_w đầu tiên mà tọa độ $x \ge kx_w$, $j \ge 0$, ví dụ $P_w = (kx_w + j, *) \in E(F_q)$

Bước 3 Khôi phục lại khối bản rõ từ P_w bằng cách tính $x_w = \left\lfloor \frac{x}{k} \right\rfloor$

2.2.1.2 Phép mặt nạ (Mask)

Để biểu diễn lại bản rõ dạng (m_1, m_2) thành các điểm P_m trên E có thể áp dụng phương pháp masking bằng cách nhân m_1 và m_2 với các tọa độ x, y của các điểm trên E. Giả sử có điểm $G \in E$ có tọa độ (x_G, y_G) thì $P_m = (m_1 x_G, m_2 y_G)$.

2.2.2 SƠ ĐỒ CHỮ KÝ TRÊN ĐƯỜNG CONG ELLIPTIC

2.2.2.1 Sơ đồ chữ ký ECDSA

Để thiết lập sơ đồ chữ ký ECDSA(Elliptic Curve Digital Signature Algorithm), cần xác định các tham số: lựa chọn đường cong E trên trường hữu hạn F_q với đặc số p sao cho phù hợp, điểm cơ sở $G \in E(F_q)$.

Sinh khóa

1. Chọn số ngẫu nhiên d trong khoảng $[2, n-1]$ làm khóa bí mật.
2. Tính $Q = dG$ làm khóa công khai.

Ký trên bản rõ *m*

1. Chọn một số ngẫu nhiên k, $2 \le k \le n-1$
2. Tính $kG = (x_1, y_1)$.
3. Tính $r = x_1 \bmod n$. Nếu $r = 0$, quay lại bước 1.
4. Tính $k^{-1} \bmod n$.
5. Tính $s = k^{-1}(m + dr) \bmod n$. Nếu $s = 0$, quay lại bước 1.
6. Chữ ký trên thông điệp m là (r, s)

Kiểm tra chữ ký

1. Kiểm tra r và s có là các số tự nhiên trong khoảng $[2, n-1]$ không.
2. Tính $w = s^{-1} \bmod n$.

3. Tính $u_1 = mw \bmod n$ và $u_2 = rw \bmod n$.

4. Tính $X = u_1G + u_2Q = (x_X, y_X)$

5. Nếu $X = O$ thì phủ nhận chữ ký. Ngược lại tính $v = x_X \bmod n$.

6. Chữ ký chỉ được chấp nhận nếu $v = r$.

Chứng minh

Nếu chữ ký (r, s) trên m là đúng thì $s = k^{-1}(m + dr) \bmod n$.

$$k \equiv s^{-1}(m + dr) \equiv s^{-1}m + s^{-1}rd \equiv wm + wrd \equiv u_1 + u_2d \pmod{n}.$$

Vì vậy, $u_1G + u_2Q = (u_1 + u_2d)G = kG$, và vì vậy $v = r$.

2.2.2.2 Sơ đồ chữ ký Nyberg - Rueppel

Giả sử E là một đường cong Elliptic trên trường Z_p (p>3 và nguyên tố) sao cho E chứa một nhóm con cyclic H trong đó bài toán logarith rời rạc là "khó".

Với $P = Z_p^* x Z_p^*$, $C = ExZ_p^* xZ_p^*$, ta định nghĩa: $K = \{(E,Q,a,R) : R = aQ\}$ với $Q \in E$. Các giá trị α và R là công khai, a là bí mật.

Với $K = (E,Q,a,R)$, chọn một số ngẫu nhiên $k \in Z_{|H|}$.Khi đó, với $x = (x_1, x_2) \in Z_p^* xZ_p^*$ ta định nghĩa $sig_K(x,k) = (c,d)$, trong đó:

1. $(y_1, y_2) = kQ$
2. $c = y_1 + hash(x) \bmod p$
3. $d = k - ac \bmod p$
4. $ver_K(x,c,d) = true \Leftrightarrow hash(x) = e$
5. $(y_1, y_2) = dQ + cR$
6. $e = c - y_1 \bmod p$

2.2.2.3 Sơ đồ chữ ký mù Harn trên EC

Năm 1994, Harn đã công bố một sơ đồ chữ ký mù tựa như sơ đồ ECDSA. Chữ ký mù là chữ ký thực hiện trên một văn bản mà người ký hoàn toàn không biết nội dung. Điều này thực hiện được vì người trình ký đã sử dụng một phương pháp nào đó để che dấu nội dung của văn bản gốc để người ký không biết. Để người ký yên tâm, người xin cấp chữ ký phải chứng minh tính hợp lệ của nội dung đã bị che dấu.

Sinh khóa

Chọn các tham số cho đường cong Elliptic

(1) Chọn số nguyên tố p và số nguyên n.

(2) Với 2 phần tử a_1, a_2 của $GF(p^n)$, xác định phương trình của E trên $GF(p^n)$ ($y^2 = x^3 + a_1x + a_2$ trong trường hợp $p>3$) với $4a_1^3 + 27a_2^2 \neq 0$

(3) Với 2 phần tử x_G và y_G trong $GF(p^n)$ xác định một điểm $G = (x_G, y_G)$ trên $E(GF(p^n))$ ($G \neq O$ với O là điểm gốc).

(4) Giả sử điểm G có bậc q

Việc sinh khóa bao gồm:

(1) Chọn một khóa bí mật d là số nguyên ngẫu nhiên trong $[2, q-1]$

(2) Tính khóa công khai Q, là một điểm trên E sao cho $Q = dG$.

Ký mù

Giả sử Bob yêu cầu Alice ký lên một văn bản m_0 mà m là đại diện của văn bản này ($m = H(m_0)$ với H là một hàm băm nào đó). Giao thức ký được thực hiện như sau:

(1) Alice sinh ra cặp khóa $(\bar{k}, \bar{R})$ theo cách sau: chọn ngẫu nhiên $\bar{k} \in [2, q-1]$ và tính $\bar{R} = \bar{k}G = (x_{\bar{k}}, y_{\bar{k}})$. Đặt $\bar{r} = x_{\bar{k}}$, rồi gửi $\bar{r}$ và $\bar{R}$ cho Bob

(2) Bob chọn các tham số làm mù $a, b \in [1, q-1]$, tính R trên E sao cho $R = a\bar{R} + bG = (x_k, y_k)$ và tính $r = c(x_k)$ và $\bar{m} = (m + r)a^{-1} - \bar{r}$. Sau đó gửi $\bar{m}$ cho Alice ($\bar{m}$ là m sau khi đã bị làm mù).

(3) Alice tính $\bar{s} = d(\bar{m} + \bar{r}) + \bar{k} \pmod q$, rồi gửi $\bar{s}$ cho Bob.

(4) Bob nhận được $\bar{s}$, xóa mù để có được chữ ký s trên m bằng cách tính

$$s = a\bar{s} + b$$

Cặp (r, s) là chữ ký trên m.

2.2.2.4 Sơ đồ chữ ký mù bội Harn trên EC

Đa chữ ký hiểu là chữ ký được tạo thành bởi nhiều người ký. Có văn bản cần được ký bởi một số người thay vì một người nhằm bảo đảm tính an toàn. Những người ký không biết về nội dung văn bản ký.

Sinh khóa

Việc chọn các tham số cho đường cong elliptic tương tự như sơ đồ chữ ký Harn. Giả sử rằng có *t* người ký là U_i, với $i = 1\ldots,t$. Việc sinh khóa được thực hiện qua các bước:

(1) Mỗi người ký U_i chọn ngẫu nhiên một khóa bí mật d_i là một số nguyên thuộc [2, q – 1].

(2) Khóa công khai của người ký U_i là điểm: $Q_i = d_iG = (x_{d_i}, y_{d_i})$, $i = 1\ldots,t$

(3) Khóa công khai cho tất cả người ký là: $Q = Q_1 + \ldots + Q_t = dG = (x_d, y_d)$ với $d = d_1 + \ldots + d_t \pmod q$.

Ký mù trên *m*

(1) Người ký U_i sinh một lần cặp $(\bar{k}_i, \bar{R}_i)$ bằng cách chọn ngẫu nhiên $\bar{k}_i \in [2, q-1]$ và tính $\bar{R}_i = \bar{k}_i G = (x_{k_i}, y_{k_i})$. U_i đặt $\bar{r}_i = x_{\bar{k}_i}$, $i = 1,\ldots, t$ rồi gửi $\bar{r}_i$ và $\bar{R}_i$ cho Ban thư ký.

(2) Ban thư ký chọn các tham số làm mù $a, b \in [1, q-1]$, tìm điểm R trên E sao cho $R = a\bar{R} + bQ = (x_k, y_k)$ trong đó $\bar{R} = \bar{R}_1 + \cdots \bar{R}_t$ và Q = Q_1 +…+ Q_t . Ban thư ký tính $r = c(x_k) \pmod q$ và $\bar{m} = (m + r + b)a^{-1} - \bar{r}$. Sau đó, gửi $\bar{m}$ và $\bar{r}$ đến cho từng người ký U_i.

(3) U_i tính chữ ký $\bar{s}_i = d_i(\bar{m} + \bar{r}) + \bar{k}_i \pmod q$, i=1,..., t , gửi $\bar{s}_i$ tới Ban thư ký.

(4) Ban thư ký tính $\bar{s}_i G - (\bar{m} + \bar{r})Q_i = (x_{e_i}, y_{e_i})$ và kiểm tra $\bar{r}_i \overset{?}{=} x_{e_i} \pmod q$, i=1,..., t. Chữ ký mù nhóm ECC là cặp (r, s) trong đó $s = \bar{s}a \pmod q$ và $\bar{s} = \bar{s}_1 + \ldots + \bar{s}_t \pmod q$.

2.3. MỘT SỐ PHƯƠNG PHÁP TẤN CÔNG CHỮ KÝ ECC

2.3.1. Phương pháp tấn công "baby-step giant - step"

Đây là phương pháp tấn công đầu tiên lên hệ mật mã ECC do Shanks đưa ra, và thực hiện với thời gian là hàm mũ. Nó giải bài toán DLP trong trường nguyên tố Z_p được mở rộng cho bài toán EDLP.

Bài toán Tìm k sao cho $kG = Q$ trên $E(F_q)$ với $\#E(F_q) = N$, giả sử k tồn tại thực sự.

Thuật toán

1. Chọn số nguyên $m > \sqrt{N}$.
2. Tính mG.
3. Với $i = 0$ đến $i = m-1$ tính (và lưu lại) iG.
4. Với $j = 0$ đến $j = m-1$ tính (và lưu lại) $Q - jmG$.
5. Sắp xếp danh sách trong bước 3 và 4 theo một thứ tự nhất định.
6. So sánh các danh sách ở các bước 3 và 4 cho đến khi tìm được cặp i, j thỏa mãn iG = Q – jmG.

7. Kết quả trả lại là $k \equiv i + jm \pmod{N}$.

2.3.2 Phương pháp tấn công MOV

Phương pháp tấn công MOV (Menezes, Okamoto, và Vanstone) làm yếu bài toán logarit rời rạc trên đường cong elliptic $E(F_q)$ thành bài toán logarith rời rạc trên trường F_{q^m} với m nào đó. Khi đó có thể tấn công bằng tấn công chỉ số, nhất là khi m nhỏ.

2.3.3. Các thuật toán tấn công khác

Nhiều thuật toán tấn công khác cũng đã được chứng minh là không hiệu quả với các hệ mật mã trên đường cong elliptic. Thuật toán tấn công chỉ số áp dụng hiệu quả để giải bài toán DLP nhưng không áp dụng được cho EDLP. Giao thức trao đổi khóa trên đường cong elliptic tương tự giao thức Diffie – Hellman cũng chống lại được tấn công của Western, Miller, và tấn công với thời gian là hàm mũ nhỏ của Adleman. Thuật toán tương tự RSA của Demytko cũng an toàn với các tấn công đẳng cấu.

2.4. LỰA CHỌN ĐƯỜNG CONG ELLIPTIC PHÙ HỢP

2.4.1. Trường K

Các đường cong elliptic trên trường nguyên tố F_p và trên trường F_{q^n} có các tính chất giúp chúng có thể thực thi được trên các thiết bị mà vẫn đảm bảo an toàn.

2.4.2. Dạng của đường cong elliptic

Trước hết, chúng ta cần xem các dạng đường cong elliptic. Trên trường F_q có hai lớp đường cong elliptic được dùng trong các hệ mã hóa là supersingular và non-supersingular (xem [22]). Xét F_q có đặc số là 2 ($g = 2^m$). Khi đó:

i) Tập tất cả các cặp nghiệm (x, y) của phương trình $y^2 + ax = x^3 + bx + c$ với $a, b, c \in F_q$ và $a = 0 \pmod{q}$ cùng với điểm trung hòa O tạo thành một đường cong elliptic dạng supersingular.

ii) Tập tất cả các cặp nghiệm (x, y) của phương trình $y^2 + ax = x^3 + bx + c$ với $a, b, c \in F_q$ và $b = 0 \pmod{q}$ cùng với điểm trung hòa O tạo thành một đường cong elliptic dạng non-supersingular.

Supersingular Curve:

Menezes và Vanstone đã tìm ra các ưu điểm của các đường cong elliptic supersingular cho các hệ mật mã, đặc biệt trên trường F_{2^r} . Tuy nhiên, các đường cong supersingular có thể bị tấn công bằng MOV.

Nonsupersingular:

Ưu điểm của các đường cong nonsupersingular là nó cung cấp độ bảo mật tương đương như các đường cong supersingular nhưng với các trường nhỏ hơn. Độ dài khóa ngắn giúp chúng có thể được triển khai trên các thiết bị như smart card. Hơn nữa, các đường cong nonsupersingular có thể chống lại tấn công MOV, ví dụ với nhóm con cyclic cỡ 2^{160}.

2.4.3 Phương pháp lựa chọn

Có một số phương pháp để lựa chọn các đường cong elliptic. Phương pháp tự nhiên nhất là chọn ngẫu nhiên. Chọn ngẫu nhiên một đường cong elliptic E trên trường K và một điểm cơ sở $P \in E$. K được chọn và cố định trước. Phương pháp chọn ngẫu nhiên Koblitz cho các đường cong elliptic trên trường F_q (với q lớn) như sau:

1. Chọn ngẫu nhiên 3 phần tử từ F_q là x, y, a
2. Tính $b = y^2 - (x^3 + ax)$
3. Kiểm tra $4a^3 + 27b^2 \neq 0$ để đảm bảo phương trình $x^3 + ax + b = 0$ không có nghiệm kép
4. Nếu điều kiện trên không thỏa mãn quay lại bước 1
5. Còn lại, đặt $P = (x, y)$ và đường cong $y^2 = x^3 + ax + b$ là đường cong cần chọn.

Sơ đồ 2.4. Phương pháp chọn ngẫu nhiên Koblitz

2.5. MỘT SỐ CHUẨN SỬ DỤNG HỆ MẬT ECC

Việc đưa ra một chuẩn chung cho các hệ thống mật mã, các giao thức, các giao diện là một việc quan trọng. Việc chuẩn hóa mang lại 3 lợi ích chính:

(1). Cho phép kết hợp phần cứng và phần mềm của nhiều nhà cung cấp khác nhau.

(2). Đưa ra chuẩn cho việc đảm bảo an toàn các hệ thống dưới khía cạnh mật mã học

(3). Cho phép có thiết kế chuẩn cho các môi trường ứng dụng khác nhau.

Các đường cong elliptic đã được xem xét và nghiên cứu kỹ lưỡng bởi các nhà toán học trong hơn 10 năm và đã được khảo sát kỹ bởi các tổ chức chuẩn hóa từ năm 1995. Điều này đảm bảo rằng tính tin cậy của nó đã được kiểm chứng như: **ANSI X9**, **ATM Forum**, **Certicom**, **FSTC**, **IEEE, P1363**, **IETF, ISO/IEC**, **NIST**, **OTP 0.9, SET, WAP**.

Chương 3. CHỮ KÝ ECC TRONG TIỀN ĐIỆN TỬ

3.1. THANH TOÁN BẰNG TIỀN ĐIỆN TỬ

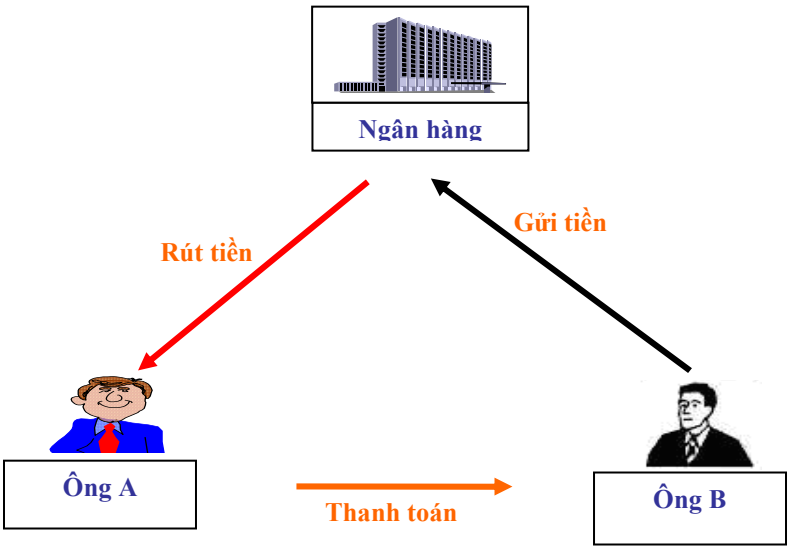
3.1.1. Khái niệm tiền điện tử

Tiền điện tử (e-money, digital money, digital cash, electronic money, electronic currency, digital currency hay internet money) là thuật từ vẫn còn mơ hồ và chưa định nghĩa đầy đủ. Tuy nhiên có thể hiểu Tiền điện tử là loại tiền trao đổi theo phương pháp "điện tử", liên quan đến mạng máy tính và những hệ thống chứa giá trị ở dạng số (digital stored value systems).

Tiền điện tử có loại ẩn danh và định danh. Hệ thống tiền ẩn danh không tiết lộ thông tin định danh của người sử dụng, và hệ thống này dựa vào Sơ đồ chữ ký "mù". Hệ thống tiền định danh tiết lộ thông tin định danh của người sử dụng, hệ thống dựa vào Sơ đồ chữ ký thông thường.

3.1.2. Lược đồ giao dịch

Lược đồ giao dịch của hệ thống tiền điện tử cơ bản, có 3 giao dịch chính sau:



Hình 3.1. Mô hình giao dịch cơ bản của hệ thống tiền điện tử.

- **Rút tiền**: A chuyển tiền của ông ta từ tài khoản ở ngân hàng vào 'Túi' của mình (Nó có thể là smart card hay là máy Pc).
- **Thanh toán**: A chuyển tiền từ 'Túi' của ông ta đến ông B.

- **Gửi tiền**: B chuyển tiền nhận được vào tài khoản của ông ta ở ngân hàng.

Trong lược đồ giao dịch này, có thể thực hiện 2 kiểu giao dịch: trực tuyến (online) và ngoại tuyến (offline).

Trực tuyến: ông B liên lạc với ngân hàng và kiểm tra tính hợp lệ của đồng tiền trước khi tiến hành thủ tục thanh toán và phân phối hàng. Quá trình thanh toán và quá trình trả tiền (ghi tiền vào tài khoản người bán) được tiến hành đồng thời.

Ngoại tuyến: quá trình giao dịch với ngân hàng và việc kiểm tra tính hợp lệ của đồng tiền được tiến hành sau quá trình thanh toán.

3.1.3. Phân loại

Hiện nay tiền điện tử có thể chia thành hai loại: **Tiền điện tử định danh** (identified e-money) và **Tiền điện tử ẩn danh** (anonymous identified e-money).

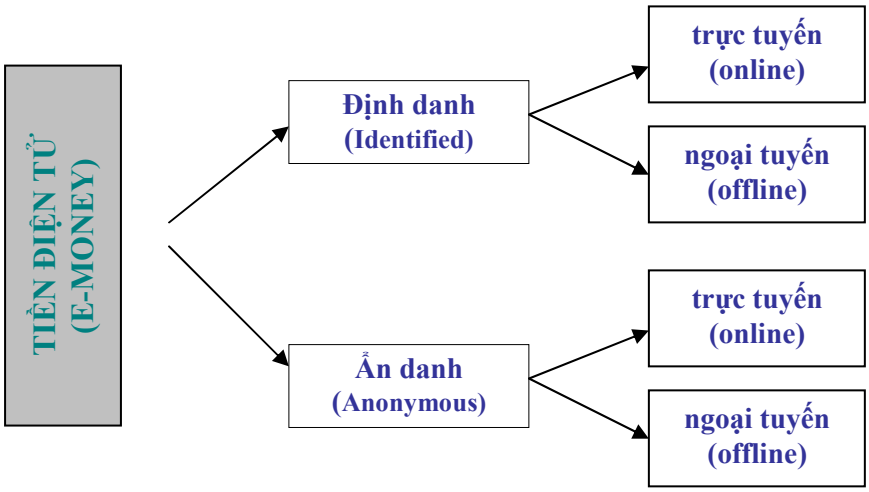
Tiền điện tử định danh chứa thông tin định danh của người sử dụng từ khi bắt đầu rút tiền từ ngân hàng. Kiểu lưu thông tin người dùng giống như trường hợp sử dụng thẻ tín dụng trong thanh toán, tiền điện tử định danh cũng cho phép ngân hàng lưu dấu vết của tiền khi luân chuyển.

Tiền điện tử ẩn danh giống như tiền giấy thực sự. Đồng tiền điện tử ẩn danh được rút từ một tài khoản, có thể được tiêu xài hay chuyển cho người khác mà không để lại dấu vết.

Trong 2 loại tiền điện tử trên, dựa vào phương pháp thực hiện, có thể chia mỗi loại trên thành 2 dạng: **trực tuyến** (online) và **ngoại tuyến** (offline).

Trực tuyến: nghĩa là cần phải tương tác với phía thứ ba để kiểm soát giao dịch.

Ngoại tuyến: nghĩa là có thể kiểm soát được giao dịch, mà không phải liên quan trực tiếp đến phía thứ ba (ngân hàng)



Hình 3.2. Phân loại tiền điện tử.

3.1.4. Những đặc điểm của tiền điện tử

3.1.4.1 Tính an toàn

Tiền điện tử phải không thể bị sao chép (sử dụng lại) hay giả mạo. Chính vì vậy khi phát triển hệ thống tiền điện tử, phải quan tâm đến vấn đề giảm thiểu rủi ro về sự giả mạo và xây dựng một hệ thống xác thực tốt.

3.1.4.2 Tính riêng tư

Quá trình thanh toán của người trả tiền phải được ẩn danh, không để lại dấu vết, nghĩa là ngân hàng không nói được tiền giao dịch là của ai.

3.1.4.3 Tính độc lập

Việc sử dụng tiền điện tử không phụ thuộc vào bất kỳ vị trí địa lý nào. Tiền có thể được chuyển qua mạng máy tính hay chứa trên những thiết bị nhớ khác nhau.

3.1.4.4 Tính chuyển nhượng

Cho phép hai bên có thể chuyển tiền cho nhau mà không phải liên hệ với bên thứ 3 (ngân hàng). Tính chuyển nhượng là đặc trưng của tiền mặt, nó cho phép người sở hữu tiền chuyển cho người khác, mà không cần liên hệ với ngân hàng.

3.1.4.5 Tính phân chia

Người dùng có thể phân chia đồng tiền số của mình thành những đồng tiền có giá trị nhỏ hơn, với điều kiện tổng giá trị của các đồng tiền này bằng giá trị của đồng tiền điện tử ban đầu.

3.1.4.6 Tính dể sử dụng

Tính dể sử dụng đồng tiền với người dùng là đặc tính rất quan trọng. Bởi vì tiền điện tử là một giải pháp mang tính phổ biến, nhắm đến nhiều đối tượng sử dụng.

3.2. MỘT SỐ VẤN ĐỀ VỀ TIỀN ĐIỆN TỬ

Hai vấn đề lớn nhất hiện nay đặt ra đối với tiền điện tử bao gồm: vấn đề **ẩn danh** người sử dụng và vấn đề ngăn chặn người sử dụng tiêu một đồng tiền điện tử nhiều lần (**double-spending**).

Tuỳ theo loại tiền điện tử, sẽ có những giải pháp khác nhau để giải quyết các vấn đề trên.

3.2.1. Vấn đề ẩn danh

Trong hệ thống tiền điện tử, để giải quyết vấn đề trên người ta đã sử dụng kỹ thuật "chữ ký số mù". Chữ ký số mù là một dạng đặc biệt của chữ ký điện tử, nó đòi hỏi người ký thực hiện ký vào một thông điệp mà không biết nội dung của nó. Thêm vào đó, người ký sau này có thể nhìn thấy cặp chữ ký/thông điệp, nhưng không thể biết được là mình đã ký thông điệp đó khi nào và ở đâu (mặc dù anh ta có thể kiểm tra được chữ ký đó là đúng đắn). Nó cũng giống như ký khi đang nhắm mắt vậy.

Chữ ký số mù đảm bảo ngân hàng không thể có được bất cứ mối liên hệ nào giữa đồng tiền điện tử và chủ sở hữu của nó.

3.2.2. Vấn đề khai man giá trị đồng tiền

Tuy nhiên giải pháp sử dụng chữ ký mù làm nảy sinh một vấn đề, đó là: Điều gì xảy ra nếu như ông A cố tình gian lận, gửi tới ngân hàng một đồng tiền điện tử ghi giá trị 50 $ để ký, nhưng báo với ngân hàng là 1$. Vì ngân hàng ký mù lên đồng tiền, nên rõ ràng là không thể biết được nội dung của nó. Để giải quyết trường hợp gian lận này, có hai giải pháp được đề ra:

1. Cách rõ ràng nhất là ngân hàng sử dụng một khoá công khai khác nhau cho mỗi loại tiền. Nghĩa là nếu có k đồng tiền khác biệt thì ngân hàng phải công khai k khoá công khai.

Giả sử với đơn vị tiền có giá trị là 1$ thì ngân hàng sử dụng khoá k_1 và 50$ thì sử dụng khoá k_{50}. Như vậy trường hợp gian lận của ông A sẽ tạo ra đồng tiền có giá trị 50$ với k_1, đây là đồng tiền không hợp lệ.

2. Phương pháp thứ hai là dùng giao thức "cắt và chọn" (Cut and choose).

Ý tưởng của giao thức này là: để có một đồng tiền có giá trị thì ông A phải tạo **k** đồng tiền, ký hiệu là $C_1,C_2,...,C_k$. Mỗi đồng tiền đều được gắn định danh, sự khác nhau duy nhất giữa chúng là số sê-ri.

Ông A làm mù những đồng tiền này và gửi chúng đến ngân hàng.

Ngân hàng yêu cầu ông A cung cấp các thông tin tương ứng để có thể khử mù **k-1** đồng tiền bất kỳ. Ngân hàng khử mù và kiểm tra chúng. Nếu tất cả đều hợp lệ, ngân hàng ký mù lên đồng tiền còn lại $\mathbf{C_i}$ (là đồng tiền mà ngân hàng không khử mù) và gửi lại cho ông A.

Ngân hàng có sự đảm bảo cao rằng đồng tiền còn lại cũng là hợp lệ vì nếu ông A gửi kèm đồng tiền không hợp pháp trong số **k** đồng tiền, thì xác suất bị phát hiện ít nhất là k-1/k. Xác suất này càng cao nếu **k** càng lớn. Tuy nhiên nếu k quá lớn thì hệ thống xử lý phải trao đổi nhiều dữ liệu.

3.2.3. Vấn đề tiêu xài một đồng tiền nhiều lần

- Đối với hệ thống **Tiền điện tử trực tuyến**:

Hệ thống yêu cầu người bán hàng liên lạc tới ngân hàng với mỗi lần bán. Ngân hàng lưu giữ thông tin tất cả những đồng tiền điện tử đã tiêu xài trước đấy và có thể dễ dàng cho người bán hàng biết đồng tiền nào còn khả năng tiêu xài được. Nếu ngân hàng báo rằng đồng tiền nào đó đã thực sự được tiêu xài rồi, thì người bán hàng lập tức từ chối bán hàng. Điều này giống như cách mà những nhà bán hàng hiện tại kiểm tra thẻ tín dụng tại những điểm bán hàng.

- Đối với hệ thống **Tiền điện tử ngoại tuyến**:

Phát hiện việc "tiêu xài hai lần" sẽ được thực hiện bằng hai cách khác nhau.

Cách thứ nhất là tạo **thẻ thông minh đặc biệt** (special smart card) chứa con chip chống trộm cắp. Trong những hệ thống khác, chip này còn được gọi là "người theo dõi". Chip theo dõi sẽ lưu một lượng nhỏ dữ liệu của tất cả những phần tiền tiền điện tử đã được tiêu xài qua smart card. Nếu người sở hữu smart card đó cố gắng sao chép tiền điện tử này và tiêu xài nó lần hai, thì chip theo dõi (được gắn vào smart card) sẽ phát hiện được hành động này, và không cho phép giao dịch "tiêu xài". Bởi vì chip theo dõi dùng để chống sự gian dối, người sở hữu smart card này không thể xoá được dữ liệu trừ khi họ phá huỷ smart card.

Cách thứ hai là dựa vào cấu trúc của tiền điện tử và những giao thức mật mã để có thể truy vết tìm ra kẻ gian lận (tiêu xài hai lần). Nếu như người sử dụng biết rằng họ sẽ bị bắt khi cố tính gian lận, về lý thuyết thì tỷ lệ hành động gian lận sẽ bị giảm đi. Điều thuận lợi của phương pháp là chúng không đòi hỏi những con chip đặc biệt. Hệ thống có thể được phát triển trên chương trình phần mềm (software) và có thể chạy trên máy tính cá nhân thông thường hay smart card.

- Tiền điện tử định danh-ngoại tuyến (Identified offline):

Dựa vào thông tin định danh để truy vết tìm ra kẻ gian lận. Trong quá trình giao dịch, định danh của người sử dụng được tích luỹ đầy đủ trên đường đi của đồng tiền và thông tin định danh sẽ "trưởng thành" ở mỗi lần nó được tiêu xài. Những chi tiết thông tin mỗi lần giao dịch được gắn vào phần tiền điện tử, và đi với nó khi nó được chuyển từ người này sang người khác.

Khi tiền điện tử chuyển tới ngân hàng, họ kiểm tra dữ liệu của nó, để xem tiền điện tử có bị tiêu xài hai lần không ?. Ngân hàng sử dụng những thông tin này để lần theo vết của những giao dịch, để phát hiện ra người nào tiêu xài hai lần.

- Tiền điện tử ẩn danh-ngoại tuyến (Anonymous Offline):

Đây là dạng phức tạp nhất, bởi vì hệ thống phải làm sao vừa đảm bảo tính ẩn danh của người dùng, vừa đảm bảo có thể truy vết được định danh người dùng trong trong hợp xảy ra vi phạm (tiêu xài hai lần).

Giải pháp cho hệ thống này là gắn thông tin lên đồng tiền ở mỗi lần giao dịch. Thông tin này sẽ 'trưởng thành' với mỗi giao dịch. Khi tiền điện tử đến ngân hàng, họ sẽ kiểm tra trong cơ sở dữ liệu xem tiền này đã được tiêu chưa. Nếu ngân hàng phát hiện tiền này đã được tiêu trước đây, thì họ sẽ sử dụng thông tin tích luỹ để xác định định danh của kẻ gian lận (người tiêu xài hai lần).

Tuy nhiên thông tin được tích luỹ trong trường hợp này chỉ có thể dùng để lần theo vết giao dịch nếu như tiền điện tử được tiêu hai lần, nghĩa là chỉ khi có gian lận thì ngân hàng mới có thể truy lại thông tin của người sử dụng.

Nếu tiền điện tử ẩn danh không bị tiêu hai lần, thì ngân hàng không thể phát hiện được định danh của người tiêu tiền, cũng như không thể xây dựng lại đường đi của tiền điện tử.

3.3. CHỮ KÝ ECC DÙNG TRONG TIỀN ĐIỆN TỬ

3.3.1. Sử dụng chữ ký "mù" nhằm ẩn danh người dùng tiền điện tử

Sơ đồ chữ ký mù nhằm chắc chắn rằng bên A (khách hàng) không muốn người ký B (ngân hàng) biết được định danh của mình.

Nội dung sơ đồ như sau:

Chuẩn bị:

- Ký hiệu chữ ký mù cho người ký B là $Sig_B(X)$. $Sig_B(X)$ là chữ ký của B trên X
- Hàm f và g (chỉ được biết bởi người gửi) trong đó: $g(Sig_B(f(m)))= Sig_B(m)$
- m là văn bản cần ký.
- H là hàm băm có thể là SHA-1 hoặc MD5.

f được gọi là hàm làm mù, g là hàm xóa mù và f(m) là thông điệp đã bị làm mù.

Đường cong Elliptic trên trường hữu hạn F_p với p là số nguyên tố và q là số nguyên tố nhỏ hơn p-1

Sinh khóa:

Chọn 2 điểm Q và R là 2 điểm trên đường cong $E(F_p)$. Khóa bí mật của ngân hàng (người ký) cho chữ ký mù là cặp (s_1,s_2) trong đó s_1,s_2 thuộc Z_q. Khóa công khai là (Q,R,V) trong đó $V= s_1Q+s_2R$.

Ký mù:

Lược đồ diễn ra theo các bước sau:

Bước 1: Ngân hàng chọn các số ngẫu nhiên k_1, k_2 thuộc Z_q.

Tính $X= k_1Q+k_2R$

Gửi X đến cho khách hàng.

Bước 2: Khách hàng chọn ngẫu nhiên số $\beta, \gamma, \delta \in Z_q$

Tính $L=X+\beta Q+\gamma R+\delta V$ và $e= H(m||L) - \delta$.

Khách hàng gửi e cho ngân hàng. m là thông điệp đã được ký.

Bước 3: Ngân hàng tính $\alpha_1=k_1-e. s_1 \bmod q$ và $\alpha_2=k_2-e.s_2 \bmod q$

Gửi cặp(α_1, α_2) cho khách hàng.

Bước 4: Khách hàng tính $\rho=\alpha_1+\beta \bmod q$, $\sigma=\alpha_2+\gamma \bmod q$.

(L, ρ, σ) là chữ ký của ngân hàng.

3.3.2. Sử dụng chữ ký "dùng một lần" nhằm tránh tiêu một đồng tiền hai lần

Sơ đồ chữ ký dùng một lần (one-time signature) là một khái niệm vẫn còn khá mới mẻ song rất quan trọng, đặc biệt là trong một số mô hình về tiền điện tử. Luận văn sẽ trình bày về *sơ đồ chữ ký dùng một lần của Schnorr*.

Nội dung sơ đồ như sau:

Chuẩn bị: Chọn P là một điểm trên đường cong Elliptic trên trường hữu hạn F_p với p là một số nguyên tố lớn, q là một số nguyên tố và q < p-1.

Sinh khóa:

- Người dùng, giả sử là Alice, chọn $S_k<p \in Z_q$ ngẫu nhiên làm khóa bí mật
- Tính $P_k= S_k.P$ làm khóa công khai

Ký:

Giả sử Alice cần ký lên thông điệp m

Alice lấy ngẫu nhiên $\delta \in Z_q^*$, $\delta < p$

- Tính $P'= \delta .P$
- Tính c'=H(P'||m)
- Tính $d=(\delta +c'.S_k) \bmod p$
- Chữ ký trên thông điệp *m* là cặp (c',d).

Nhận xét:

Số δ không được dùng quá một lần để tạo ra các chữ ký khác nhau.

Nếu Alice sử dụng δ quá một lần cho hai thông điệp khác nhau thì bất kỳ ai có hai thông điệp trên đều có thể giải mã được khóa bí mật S_k. Vì vậy, sơ đồ chữ ký loại này được gọi là sơ đồ chữ ký dùng một lần. Sơ đồ chữ ký dùng một lần được ứng dụng nhằm tránh trường hợp tiêu một đồng tiền 2 lần trong mô hình tiền điện tử

3.3.3. Sơ đồ tiền điện tử đề xuất

Sơ đồ được đề xuất bởi Jayaprakash Kar [1] và Banshidhar Majhi [2] là sự kết hợp dựa trên *sơ đồ chữ ký dùng một lần của Schnorr* và *Sơ đồ chữ ký mù Okamoto-Schnorr*. Vì là sự kết hợp giữa 2 sơ đồ trên nên lược đồ này có khả năng ẩn danh và tránh được tình huống tiêu một đồng tiền 2 lần.

Lược đồ bao gồm 3 bên: khách hàng, thương gia và ngân hàng. Ngân hàng và khách hàng có thể truy vết được khách hàng gian lận. Lược đồ sử dụng chữ ký một lần để tránh tình trạng tiêu một đồng tiền 2 lần trong bước thanh toán.

Có 3 giao thức là:

- ✓ Rút tiền với sự tham gia của khách hàng và ngân hàng
- ✓ Thanh toán với sự tham gia của khách hàng và thương gia. Quá trình này có thêm bên thứ 3 tin cậy (luật sư) và thêm 2 giao thức nữa xảy ra giữa ngân hàng và luật sư 3 nhằm truy vết sự gian lận hoặc tiêu một đồng tiền 2 lần nếu có.
- ✓ Gửi tiền với sự tham gia của thương gia và ngân hàng.

Chuẩn bị:

Mô tả đường cong Elliptic:

p>=3 là một số nguyên tố. Lấy a, b $\in F_p$ sao cho $4a^3+27b^2 \neq 0$. Một đường cong Elliptic trên trường hữu hạn F_p được định nghĩa bởi 2 tham số a và b là tập hợp của các điểm có tọa độ (x,y) sao cho $y^2=x^3+ax+b$. Điểm cơ sở G có bậc n.

Sinh khóa:

a. Ngân hàng:

Ngân hàng tính các tham số sau đây:

Chọn một số bí mật s_1,s_2 nằm trong khoảng từ [1, n-1] làm khóa bí mật để làm mù.

Khóa công khai của ngân hàng là (Q,R,V) trong đó: $V= s_1.Q+ s_2.R$

b. Khách hàng

Chọn một khóa bí mật ngẫu nhiên s_k trong khoảng [1, n-1]

Tính $P_k=s_k.P$

Khóa công khai của khách hàng là P_k.

Khóa bí mật là s_k.

c. Bên thứ 3 tin cậy.

Bên thứ 3 đáng tin thực hiện các công đoạn sau:

Chọn một khóa bí mật u_t nằm trong khoảng [1, n-1]

[1]. Jayaprakash Kar- Department of Information Technology- Al Musanna College of Technology- Sultanate of Oman

[2]. Banshidhar Majhi- Department of Computer Science of Engineering National Institute of Technology

Tính $P_t = u_t . P$

Khóa công khai của bên thứ 3 là P_t.

Khóa bí mật là u_t.

d. Hàm băm một chiều H có thể lấy là SHA-1 hoặc MD5

1./ Giao thức rút tiền:

Giao thức rút tiền với sự tham gia của khách hàng và ngân hàng trong đó khách hàng rút tiền từ ngân hàng.

Trong giao thức này khách hàng nhận lấy giá trị thời gian hết hạn T_v của tiền (mỗi đồng tiền có một thời hạn sử dụng) từ ngân hàng, tạo ra đồng tiền điện tử m' *và lấy chữ ký mù của ngân hàng*. Cuối cùng khách hàng nhận lấy tiền điện tử. Vì thế khách hàng thực hiện các giao thức sau với ngân hàng:

a. Ngân hàng chọn một số ngẫu nhiên r nằm trong khoảng [1, n-1], tính U=r.R và gửi nó tới khách hàng.

b. Cho mỗi đồng tiền, khách hàng chọn một số ngẫu nhiên δ nằm trong khoảng [1, n-1] và tính $U' = \delta . U$

c. Ngân hàng chọn số ngẫu nhiên k_1 và k_2 nằm trong khoảng [1, n-1] và tính $T = k_1.Q + k_2.U$. Sửa giá trị thời gian hết hạn T_v và ký vào nó. Rồi sau đó gửi T, T_v, $Sig_{bank}(T_v)$ cho khách hàng.

d. Khách hàng tạo tiền điện tử $m' = m || T_v || Sig_{bank}(T_v) || ID$ trong đó ID là số định danh của khách hàng. Chọn số ngẫu nhiên (β_1, β_2, γ) nằm trong khoảng [1, n-1].

Tính $T' = T + \beta_1.Q + \beta_2.U + \gamma.V$ và $c' = H(m', U', T')$ và $c = c' - \gamma$.

Sau đó khách hàng ký lên thành phần tiền điện tử c sừ dụng lược đồ ký một lần Schnorr.

Ký mù và ký một lần:

Khách hàng chọn khóa ngẫu nhiên $0 < \delta < p$

Tính $P' = \delta . P$

Tính $d = (\delta + c'.s_k) \bmod p$

Chữ ký lên thành phần tiền điện tử c là cặp (d, P'). Sau đó khách hàng gửi cặp chữ ký (d, P') cho ngân hàng. Ngân hàng kiểm tra dựa vào biểu thức sau:

$P' = d.P - c'.P_k$.

e. Sau đó ngân hàng tạo ra *chữ ký mù* sử dụng lược đồ chữ ký mù Okamoto-Schnorr. Giao thức con được thực hiện bởi ngân hàng và khách hàng theo các bước sau:

Ngân hàng tính $\alpha_1 = k_1 - c.s_1 \bmod p$, $\alpha_2 = k_2 - c.s_2.r^{-1} \bmod p$ và gửi cặp (α_1, α_2) tới khách hàng.

Khách hàng tính $\alpha_1' = \alpha_1 + \beta_1 \bmod p$ và $\alpha_2' = \delta^{-1}.\alpha_2 + \beta_2 \bmod p$

Ngân hàng tính $C_{ID}=x_1 \mod p$ trong đó $T=(x_1,y_1)$

Ngân hàng lưu trữ (ID, C_{ID}) trong cơ sở dữ liệu

Cuối cùng khởi tạo dòng dữ liệu (m',T', α_1', α_2', U')

Để kiểm tra ai cũng có thể kiểm tra bởi đẳng thức sau:

$T'=\alpha_1'.Q+\alpha_2'.U'+c'.V$

trong đó c' được tính theo công thức sau: c'=H(m',U',T').

Khách hàng thực hiện các giao thức con với bên thứ 3 tin cậy :

a. Khách hàng gửi dòng dữ liệu (m',T', α_1', α_2', U') và T cho bên thứ 3 tin cậy

b. Bên thứ 3 kiểm tra chữ ký của đồng tiền đã bị làm mù bằng đẳng thức $P'=d.P-c'.P_k$. Nếu sai thì các giao thức con này cũng thất bại. Nếu đúng bên thứ 3 sẽ chấp nhận chữ ký.

c. Bên thứ 3 tạo ra chữ ký theo các bước sau:

Chọn một số ngẫu nhiên làm khóa: $0<\eta<p$

Tính $P''=\eta.P$

Tính $s=(\eta+c'.u_1) \mod p$

d. Bên thứ 3 gửi chữ ký là cặp (P'',s) tới khách hàng.

e. Bên thứ 3 tính $C_{ID}=x_1 \mod p$ (trong đó $T=(x_1,y_1)$), lưu C_{ID} và

dòng dữ liệu (m',T', α_1', α_2', U'). Dòng dữ liệu hoặc tiền điện tử được đại diện bởi (m',T', α_1', α_2', U',P'',s)

2./ Giao thức thanh toán:

Giao thức thanh toán bao gồm khách hàng và thương gia trong đó khách hàng thanh toán tiền cho thương gia.

a. Khách hàng gửi (m',T', α_1', α_2', U',P'',s) cho thương gia .

b. Thương gia xác minh chữ ký mù bởi đẳng thức : $P'=d.P-c'.P_k$

c. Cuối cùng thương gia sẽ xác minh tính chân thực của chữ ký một lần ví dụ như cặp (P'',s) theo đẳng thức sau:

$P''=s.P-c'.P_t$

3./ Giao thức gửi tiền:

Giao thức bao gồm thương gia và ngân hàng. Tại đây thương gia sẽ gửi tiền điện tử tới ngân hàng. Nhưng có thêm sự tương tác cho việc truy vết và ngăn ngừa tiêu một đồng tiền 2 lần.

a. Thương gia gửi tiền (m',T', α_1', α_2', U',P",s) cho ngân hàng. b. Ngân hàng kiểm tra thời hạn T_v cho mỗi đồng tiền

c. Ngân hàng kiểm tra tính hợp lệ của các đồng tiền bằng cách kiểm tra chữ ký dùng một lần của bên thứ 3 bằng đẳng thức P"=s.P-c'.P_t và chữ ký mù của ngân hàng bằng đẳng thức T'= α_1'.Q+ α_2'.U'+c'.V

d. Ngân hàng xác minh xem đồng tiền đã được tiêu 2 lần hay chưa?. Nếu đồng tiền chưa bao giờ được gửi trước đó, ngân hàng sẽ chấp nhận đồng tiền.

4./ Giao thức truy vết sự gian lận:

Giao thức truy vết bao gồm ngân hàng và bên thứ 3. Giao thức này được sử dụng để tìm ra định danh của khách hàng trong trường hợp khách háng gian lận trong quá trình giao dịch. Tiền được luân chuyển có thể bị từ chối nếu như tính định danh của khách hàng là bất hợp pháp trong giao thức này. Các bước của quá trình này như sau:

Ngân hàng gửi tiền(m',T', α_1', α_2', U',P",s) và T=(x_1,y_1) cho bên thứ 3 tin cậy

Bên thứ 3 tin cậy xác minh tính hợp lệ của tiền bằng cách sử dụng đẳng thức : c'=H(m',U',T'). Tính C_{ID}=x_1 mod p và gửi C_{ID} tới ngân hàng. Chú ý là C_{ID} được liên kết tới định danh của khách hàng trong cơ sở dữ liệu của ngân hàng.

5./ Vấn đề tiêu một đồng tiền 2 lần:

Mỗi đồng tiền đều có thời hạn sử dụng. Do đó tiền phải được gửi vào ngân hàng trước thời hạn T_v. Trong hệ thống tiền điện tử khi một thương gia nhận được tiền, ông ta có thể yêu cầu ngân hàng xem đồng tiền đó đã từng được tiêu hay chưa. Nếu đồng tiền đã được tiêu, ngân hàng sẽ hủy giao dịch. Vì thế thương gia không cần phải yêu cầu chữ ký thứ một lần từ bên thứ 3 tin cậy. Trong hệ thống ngoại tuyến, quá trình tiêu một đồng tiền 2 lần không thể ngăn chặn nhưng phát hiện thì có thể. Chữ ký dùng một lần có thể là giải pháp cho vấn đề này. Trong bước trước khách hàng chọn số ngẫu nhiên duy nhất δ và nhận chữ ký mù của ngân hàng.. Vì thế nếu khách hàng sử dụng δ nhiều hơn một lần cho mỗi đại diện m' của từng dồng tiền, khóa bí mật của khách hàng có thể phát giác . Do đó khách hàng sẽ không cố sử dụng dồng tiền quá 1 lần. Nếu không trong bước cuối cùng quá trình tiêu đồng tiền 2 lần có thể bị phát hiện ra và ngân hàng có thể nhận ra được sự phạm pháp với sự giúp đỡ của bên thứ 3. Giao thức phát hiện việc tiêu 1 đồng tiền 2 lần như sau:

a. Khách hàng gửi định danh của mình cho ngân hàng

b. Ngân hàng gửi T=(x_1,y_1) cho bên thứ 3

c. Bên thứ 3 đáng tin tính C_{ID}= x_1 mod p và tìm sự phụ thuộc của dòng dữ liệu (m',T', α_1', α_2', U',P",s) và gửi tiền cho ngân hàng. Chú ý là C_{ID} liên kết tới đồng tiền trong cơ sở dữ liệu của bên thứ 3.

d. Ngân hàng có thể từ chối tiền hoặc kiểm tra việc tiêu một đồng tiền 2 lần.