TCVN TIÊU CHUẨN QUỐC GIA

TCVN 12852-5 : 2020

ISO/IEC 15946-5 : 2017

Xuất bản lần 1

CÔNG NGHỆ THÔNG TIN – CÁC KỸ THUẬT AN TOÀN – KỸ THUẬT MẬT MÃ DỰA TRÊN ĐƯỜNG CONG ELLIPTIC – PHẦN 5: SINH ĐƯỜNG CONG ELLIPTIC

Information technology – Security techniques – Cryptography based on elliptic curves – Part 5: Elliptic curve generation

HÀ NỘI – 2020

Mục Lục

Lời nói đầu

TCVN 12852-5 : 2020 hoàn toàn tương đương với ISO/IEC 15946-5:2017.

TCVN 12852-5 : 2020 do Cục Quản lý mật mã dân sự và Kiểm định sản phẩm mật mã biên soạn, Ban Cơ yếu Chính phủ đề nghị, Tổng cục Tiêu chuẩn Đo lường Chất lượng thẩm định, Bộ Khoa học và Công nghệ công bố.

Bộ tiêu chuẩn TCVN 12852 (ISO/IEC 15946) *Công nghệ thông tin – Các kỹ thuật an toàn – Kỹ thuật mật mã dựa trên đường cong elliptic* gồm các tiêu chuẩn sau:

- TCVN 12852-1 : 2020 (ISO/IEC 15946-1:2016) Phần 1: Tổng quan

- TCVN 12852-5 : 2020 (ISO/IEC 15946-5:2017) Phần 5: Sinh đường cong elliptic

Bộ tiêu chuẩn này có thể có thêm các phần tiếp theo.

TIÊU CHUẨN QUỐC GIA **TCVN 12852-5 : 2020**

Công nghệ thông tin – Các kỹ thuật an toàn – Kỹ thuật mật mã dựa trên đường cong elliptic – Phần 5: Sinh đường cong elliptic

Information technology – Security techniques – Cryptographic techniques based on elliptic curves – Part 5: Elliptic curve generation

1 Phạm vi áp dụng

Các tiêu chuẩn trong bộ tiêu chuẩn này quy định các kỹ thuật mật mã khóa công khai dựa trên các đường cong elliptic được mô tả trong TCVN 12852-1.

Tiêu chuẩn này quy định các kỹ thuật sinh đường cong elliptic hiệu quả cho việc thực thi các cơ chế dựa trên đường cong elliptic được mô tả trong TCVN 12854-4, TCVN 12855-3, TCVN 7817-3, TCVN 12214-3 và TVN 11367-2.

Tiêu chuẩn này được áp dụng cho các kỹ thuật mật mã dựa trên các đường cong elliptic định nghĩa trên trường hữu hạn có cấp là lũy thừa của một số nguyên tố (bao gồm cả các trường hợp đặc biệt của cấp nguyên tố và đặc số hai). Tiêu chuẩn này không áp dụng cho việc biểu diễn các phần tử của trường hữu hạn cơ sở (tức là cơ sở được sử dụng).

Bộ tiêu chuẩn này không quy định việc thực thi các kỹ thuật được định nghĩa. Khả năng tương thích của các sản phẩm phù hợp theo bộ tiêu chuẩn này sẽ không được đảm bảo.

2 Tài liệu viện dẫn

Các tài liệu viện dẫn sau rất cần thiết cho việc áp dụng tiêu chuẩn này. Đối với những tài liệu viện dẫn có năm công bố, thì áp dụng phiên bản được nêu. Đối với tài liệu viện dẫn không ghi năm công bố, thì áp dụng phiên bản mới nhất (bao gồm cả các sửa đổi, bổ sung).

TCVN 12852-1, Công nghệ thông tin - Các kỹ thuật an toàn - Kỹ thuật mật mã dựa trên đường cong elliptic - Phần 1: Tổng quan

3 Thuật ngữ và định nghĩa

Tiêu chuẩn này áp dụng các thuật ngữ và định nghĩa quy định trong TCVN 15946-1 và các thuật ngữ và định nghĩa dưới đây.

3.1

Trường xác định của một đường cong elliptic (definition field of an elliptic curve)

Trường bao gồm tất cả các hệ số của phương trình mô tả một đường cong elliptic.

3.2

Hàm băm (hash-function)

Hàm ánh xạ các xâu bit có độ dài tùy ý (nhưng thường có cận trên) thành các xâu bit có độ dài cố định thỏa mãn hai tính chất sau:

- Với một đầu ra cho trước thì rất khó có thể tìm được một đầu vào mà ánh xạ tới đầu ra đó;

- Với một đầu vào cho trước thì rất khó có thể tìm được một đầu vào thứ hai mà ánh xạ tới cùng một đầu ra.

CHÚ THÍCH 1 về đầu vào: Tính khả thi về mặt tính toán phụ thuộc vào các yêu cầu và môi trường an toàn cụ thể. Tham khảo phụ lục C, ISO/IEC 10118-1:2016.

[TCVN 11816-1 (ISO/IEC 10118-1), 3.4]

3.3

Số gần nguyên tố (nearly prime number)

Số nguyên dương, $n = m \cdot r$, trong đó m là một số nguyên tố lớn và r là một *số nguyên trơn* nhỏ (3.5).

CHÚ THÍCH 1 về đầu vào: Ý nghĩa của các thuật ngữ số nguyên tố nhỏ và lớn phụ thuộc vào ứng dụng và dựa trên các giới hạn do nhà thiết kế xác định.

3.4

Bậc của một đường cong elliptic (order of an elliptic curve)

$E(F)$

Số các điểm trên một đường cong elliptic E, định nghĩa trên một trường hữu hạn F.

3.5

Số nguyên trơn (smooth integer)

Số nguyên r, có tất cả các thừa số nguyên tố đều nhỏ (tức là nhỏ hơn giới hạn xác định).

4 Các Ký hiệu và hàm chuyển đổi

4.1 Ký hiệu

B Bậc nhúng, là giá trị B nhỏ nhất sao cho số $\#E[F(q)]|q^B - 1$.

E Đường cong elliptic, được cho bởi phương trình có dạng $Y^2 = X^3 + aX + b$ trên trường $F(p^m)$ với $p > 3$, hoặc phương trình có dạng $Y^2 + XY = X^3 + aX^2 + b$ trên trường $F(2^m)$, hoặc phương trình có dạng $Y^2 = X^3 + aX^2 + b$ trên trường $F(3^m)$, cùng với một điểm O_E được gọi là điểm tại vô hạn. Đường cong elliptic được ký hiệu là $E/F(p^m)$, $E/F(2^m)$, hoặc $E/F(3^m)$ tương ứng.

CHÚ THÍCH 1 Trong các ứng dụng không dựa trên một phép ghép cặp, $E/F(p)$ hoặc $E/F(2^m)$ thường được sử dụng do hiệu quả hơn. Trong các ứng dụng sử dụng một phép ghép cặp, thì $E/F(p)$ hoặc $E/F(3^m)$ lại hiệu quả hơn.

CHÚ THÍCH 2 Đường cong elliptic không chỉ là tập hợp các điểm trên đường cong, mà còn là một nhóm dưới phép toán được định nghĩa trên các điểm này.

N	Số lượng điểm trên một đường cong elliptic E trên $F(q)$, $\#E[F(q)]$.
n	Ước số nguyên tố của $\#E[F(q)]$.
O_E	Điểm tại vô hạn của đường cong elliptic.
p	Số nguyên tố
q	Lũy thừa nguyên tố, p^m đối với một số nguyên tố p và một số số nguyên $m \geq 1$.
r	Đồng hệ số, tức là $\#E[F(q)] = rn$.
$\#E[F(q)]$	Cấp (hoặc lực lượng) của $E[F(q)]$.
$\lceil x \rceil$	Số nguyên nhỏ nhất lớn hơn hoặc bằng số thực x.
$\lfloor x \rfloor$	Số nguyên lớn nhất nhỏ hơn hoặc bằng số thực x.

4.2 Các hàm chuyển đổi

BS2IP	Nguyên thủy chuyển đổi xâu bit thành số nguyên.
BS2OSP	Nguyên thủy chuyển đổi xâu bit thành xâu bộ tám.
EC2OSP$_E$	Nguyên thủy chuyển đổi điểm đường cong elliptic thành xâu bộ tám.
FE2IP$_F$	Nguyên thủy chuyển đổi phần tử trường hữu hạn thành số nguyên.
FE2OSP$_F$	Nguyên thủy chuyển đổi phần tử trường hữu hạn thành xâu bộ tám.
I2BSP	Nguyên thủy chuyển đổi số nguyên thành xâu bit.
I2OSP	Nguyên thủy chuyển đổi số nguyên thành xâu bộ tám.
I2ECP	Nguyên thủy chuyển đổi số nguyên thành đường cong elliptic.
OS2BSP	Nguyên thủy chuyển đổi xâu bộ tám thành xâu bit.
OS2FEP$_F$	Nguyên thủy chuyển đổi xâu bộ tám thành phần tử trường hữu hạn.
OS2ECP$_E$	Nguyên thủy chuyển đổi xâu bộ tám thành điểm trên đường cong elliptic.
OS2IP	Nguyên thủy chuyển đổi xâu bộ tám thành số nguyên.

5 Khuôn khổ cho việc sinh đường cong elliptic

5.1 Các kiểu đường cong elliptic tin cậy

Có một số cách người dùng có thể có được sự tin tưởng vào nguồn gốc của một đường cong elliptic, bao gồm:

- Đường cong có thể thu được từ một nguồn đáng tin cậy công bằng (ví dụ: tiêu chuẩn quốc tế hoặc quốc gia).

- Đường cong có thể được sinh và/hoặc kiểm tra bởi một bên thứ ba đáng tin cậy.

- Đường cong có thể được sinh và/hoặc kiểm tra bởi người dùng.

CHÚ THÍCH 1 Tham khảo Phụ lục A để biết thêm thông tin cơ bản về các đường cong elliptic.

CHÚ THÍCH 2 Tham khảo Phụ lục B để biết thêm thông tin cơ bản về các hệ mật trên đường cong elliptic.

5.2 Tổng quan về việc sinh đường cong elliptic

Có ba phương pháp chính để sinh các đường cong elliptic.

- Sinh một đường cong elliptic bằng cách áp dụng các thuật toán tính cấp (số điểm) đối với một đường cong elliptic được chọn (giả) ngẫu nhiên. Kỹ thuật này được đặc tả tại Mục 6.
- Sinh một đường cong elliptic bằng cách áp dụng phương pháp nhân phức. Kỹ thuật này được đặc tả tại Mục 7.
- Sinh một đường cong elliptic bằng cách nâng một đường cong elliptic trên một trường hữu hạn nhỏ lên trường có kích thước lớn hơn. Kỹ thuật này được đặc tả tại Điều 8.

CHÚ THÍCH 1 Tham khảo Phụ lục A để biết thêm thông tin cơ bản về các đường cong elliptic.

CHÚ THÍCH 2 Tham khảo Phụ lục B để biết thêm thông tin cơ bản về các hệ mật trên đường cong elliptic.

6 Sinh đường cong elliptic giả ngẫu nhiên kiểm tra được

6.1 Giới thiệu chung

Việc sinh các đường cong elliptic giả ngẫu nhiên kiểm tra được tập trung vào các đường cong trên trường nguyên tố và trường nhị phân (và do vậy không áp dụng với các đường cong trên các trường có đặc số 3).

6.2 Xây dựng đường cong elliptic giả ngẫu nhiên kiểm tra được (trường hợp trường nguyên tố)

6.2.1 Thuật toán xây dựng

Thuật toán sau đây tạo ra một tập hợp các tham số đường cong elliptic trên một trường $F(p)$ được lựa chọn (giả) ngẫu nhiên từ các đường cong có cấp thích hợp, cùng với thông tin đầy đủ để người dùng khác có thể kiểm tra xem đường cong có thực sự được chọn giả ngẫu nhiên hay không.

CHÚ THÍCH 1 Thuật toán phù hợp với tài liệu tham khảo [9].

CHÚ THÍCH 2 Các phương pháp lựa chọn (giả) ngẫu nhiên một số nguyên tố p được mô tả trong tài liệu tham khảo [5].

Giả thiết rằng các đại lượng sau đây đã được chọn:

- Cận dưới, n_{min}, cho cấp của điểm cơ sở;
- Hàm băm mật mã, H, với độ dài đầu ra L_{Hash} bit;
- Độ dài bit, L, của đầu vào của H, thỏa mãn $L \geq L_{Hash}$.

Ký hiệu sau được chấp nhận:

- $v = \lceil log_2 p \rceil$,
- $s = \lfloor (v-1)/L_{Hash} \rfloor$,
- $w = v - sL_{Hash} - 1$.

Đầu vào: một số nguyên tố p; cận dưới n_{min} cho n; giới hạn cho phép chia tầm thường l_{max}.

Đầu ra: một xâu bit X; các tham số EC a, b, n và G.

a) Chọn một xâu bit tùy ý X có độ dài bit L.

b) Tính $h = H(X)$.

c) Đặt W_0 là xâu bit thu được bằng cách lấy w bit ngoài cùng bên phải của h.

d) Đặt $Z = BS2IP(X)$.

e) Với i từ 1 đến s thực hiện:

1) Đặt $X_i = I2BSP(Z + i \bmod 2^L)$.

2) Tính $W_i = H(X_i)$.

f) Đặt $W = W_0 || W_1 || \dots || W_s$.

g) Đặt $c = OS2FEP[BS2OSP(W)]$.

h) Nếu $c = 0_F$ hoặc $4c + 27 = 0_F$, thì quay lại bước a).

i) Chọn các phần tử trường hữu hạn $a, b \in F(p)$ sao cho $b \neq 0_F$ và $cb^2 - a^3 = 0_F$. Chọn $a = b = c$ sẽ đảm bảo các điều kiện được thỏa mãn và lựa chọn này được đề xuất sử dụng.

CHÚ THÍCH 3 Việc chọn $a = b = c$ có thể không tối ưu về mặt hiệu suất.

CHÚ THÍCH 4 Nếu các giá trị mặc định được chọn như đề xuất, thì sẽ đảm bảo được tính ngẫu nhiên của đường cong đã sinh.

j) Tính cấp $\#E[F(p)]$ của đường cong elliptic E trên $F(p)$ cho bởi $y^2 = x^3 + ax + b$.

k) Kiểm tra xem $\#E[F(p)]$ có phải là một số gần nguyên tố hay không bằng cách sử dụng thuật toán được đặc tả trong 6.2.2. Nếu thỏa mãn, đầu ra của thuật toán được đặc tả trong 6.2.2 bao gồm các số nguyên r, n. Nếu không, thì quay lại bước a).

CHÚ THÍCH 5 Sự cần thiết của tính gần nguyên tố được quy định trong B.2.2.

l) Kiểm tra xem $E[F(p)]$ có thỏa mãn điều kiện MOV quy định trong B.2.3 hay không, tức là số nguyên nhỏ nhất B thỏa mãn n chia hết $q^B - 1$ đảm bảo mức an toàn mong đợi. Nếu không, thì quay lại bước a).

m) Nếu $\#E[F(p)] = p$, thì quay lại bước a).

CHÚ THÍCH 6 Việc kiểm tra này được thực hiện nhằm bảo vệ chống lại tấn công được mô tả trong B.2.2.

n) Kiểm tra xem ước số nguyên tố n có thỏa mãn điều kiện được quy định trong B.2.4 cho các hệ mật dựa trên ECDLP, ECDHP hoặc BDHP với các đầu vào phụ trợ trong B.1.5 hay không. Nếu không thỏa mãn, thì quay lại bước a).

o) Sinh một điểm G trên E có cấp n sử dụng thuật toán được mô tả trong 6.2.3.

p) Đầu ra là X, a, b, n, G.

CHÚ THÍCH 7 : Các phương pháp tính cấp $\#E[F(p)]$ được mô tả trong tài liệu tham khảo [11], [30] và [31].

6.2.2 Kiểm tra tính gần nguyên tố

Cho trước một cận dưới n_{min} và một giới hạn cho phép chia tầm thường l_{max}, quá trình sau đây kiểm tra tính gần nguyên tố của $N = \#E[F(p)]$.

Đầu vào: Các số nguyên dương N, l_{max} và n_{min}.

Đầu ra: Nếu N là số gần nguyên tố, đầu ra là một số nguyên tố n với $n_{min} \leq n$ và một số nguyên trơn r sao cho $N = rn$. Nếu N không phải là một số gần nguyên tố, thì đầu ra là thông báo "không gần nguyên tố".

a) Đặt $n = N, r = 1$.

b) For l from 2 to l_{max} do:

1) Nếu l là hợp số, thì chuyển sang bước 3).

2) While (l chia hết n)

i. Đặt $n = n/l$ và $r = rl$.

ii. Nếu $n < n_{min}$, thì đầu ra là "không gần nguyên tố" và dừng.

3) Next l.

c) Kiểm tra tính nguyên tố của n.

d) Nếu n là số nguyên tố, thì đầu ra là r và n và dừng.

e) Đầu ra "không gần nguyên tố".

CHÚ THÍCH Các phương pháp kiểm tra tính nguyên tố được mô tả trong tài liệu tham khảo [5] và [10].

6.2.3 Tìm một điểm có cấp nguyên tố lớn

Nếu cấp $\#E[F(q)]$ của một đường cong elliptic E là gần nguyên tố, thì thuật toán sau đây sinh hiệu quả một điểm ngẫu nhiên trên $E[F(q)]$ sao cho cấp của nó là một thừa số nguyên tố lớn n của $\#E[F(q)] = rn$.

Đầu vào: Một đường cong elliptic E trên trường $F(q)$, một số nguyên tố n và một số nguyên dương r không chia hết cho n.

Đầu ra: Nếu $\#E[F(q)] = rn$, một điểm G trên E có cấp n; nếu không, thông báo "cấp sai."

a) Sinh một điểm ngẫu nhiên P (khác O_E) trên E.

b) Đặt $G = rP$.

c) Nếu $G = O_E$, thì quay lại bước a).

d) Đặt $Q = nG$.

e) Nếu $Q \neq O_E$, thì đầu ra là "cấp sai" và dừng.

f) Đầu ra là G.

6.2.4 Kiểm tra tính giả ngẫu nhiên của đường cong elliptic

Thuật toán sau đây xác định một đường cong elliptic trên $F(p)$ có được sinh nhờ sử dụng phương pháp 6.2.1 hay không. Các đại lượng L_{Hash}, L, v, s và w và hàm băm H như trong 6.2.1.

Đầu vào: Một xâu bit X có độ dài L, các tham số EC $q = p, a, b, n$, và $G = (x_G, y_G)$, và một số nguyên dương n_{min}.

Đầu ra: "Đúng" hoặc "Sai".

a) Tính $h = H(X)$.

b) Đặt W_0 là xâu bit nhận được bằng cách lấy w bit ngoài cùng bên phải của h.

c) Đặt $Z = BS2IP(X)$.

d) For i from 1 to s do:

   1) Đặt $X_i = I2BSP(Z + i \bmod 2^L)$.

   2) Tính $W_i = H(X_i)$.

e) Đặt $W = W_0||W_1|| \dots ||W_s$.

f) Chuyển đổi W thành một phần tử trường hữu hạn $c = OS2FEP[BS2OSP(W)]$.

g) Kiểm tra các điều kiện sau đây:

   1) $n \geq n_{min}$.

   2) n là một số nguyên tố.

   3) $c \neq 0_F$.

   4) $4c + 27 \neq 0_F$.

   5) $b \neq 0_F$.

   6) $cb^2 - a^3 = 0_F$.

   7) $G \neq O_E$.

   8) $y_G^2 = x_G^3 + ax_G + b$.

   9) $nG = O_E$.

h) Nếu tất cả các điều kiện trong bước g) thỏa mãn, thì đầu ra là "Đúng"; ngược lại đầu ra là "Sai".

6.3 Xây dựng đường cong elliptic giả ngẫu nhiên kiểm tra được (trường hợp nhị phân)

6.3.1 Thuật toán xây dựng

Thuật toán sau đây sinh ra một tập hợp các tham số đường cong elliptic cho một đường cong giả ngẫu nhiên trên trường $F(2^m)$, cùng với thông tin đầy đủ để người dùng khác có thể kiểm tra xem đường cong có thực sự được chọn giả ngẫu nhiên hay không. Xem Phụ lục C để biết thêm thông tin.

CHÚ THÍCH 1 Thuật toán phù hợp với tài liệu tham khảo [9].

Giả thiết rằng các đại lượng sau đây đã được chọn:

- Trường $F(2^m)$;

- Cận dưới, n_{min}, cho cấp của điểm cơ sở;

- Hàm băm mật mã, H, với độ dài đầu ra L_{Hash} bit;

- Độ dài bit, L của đầu vào của H, thỏa mãn $L \geq L_{Hash}$.

Ký hiệu sau được chấp nhận:

- $s = \lfloor (m-1)/L_{Hash} \rfloor$,

- $w = m - sL_{Hash}$.

Đầu vào: một trường $F(2^m)$; cận dưới n_{min} cho n; giới hạn cho phép chia tầm thường l_{max}.

Đầu ra: một xâu bit X; các tham số EC a, b, n và G.

a) Chọn một xâu bit tùy ý X có độ dài bit L.

b) Tính $h = H(X)$.

c) Đặt W_0 là xâu bit nhận được bằng cách lấy w bit ngoài cùng bên phải của h.

d) Đặt $Z = BS2IP(x)$.

e) For i from 1 to s, do:

   1) Đặt $X_i = I2BSP(Z + i \bmod 2^L)$.

   2) Tính $W_i = H(X_i)$.

f) Đặt $W = W_0 || W_1 || \ldots || W_s$.

g) Đặt $b = \mathrm{OS2FEP}[\mathrm{BS2OSP}(W)]$.

h) Nếu $b = 0_F$, thì quay lại bước a).

i) Lấy a là một phần tử tùy ý trong $F(2^m)$. Chọn $a = 0_F$ sẽ thỏa mãn các điều kiện, và lựa chọn này được đề xuất sử dụng.

   CHÚ THÍCH 2 Các giá trị mặc định có thể không được lựa chọn vì các lý do hiệu suất.

   CHÚ THÍCH 3 Nếu các giá trị mặc định được lựa chọn theo đề xuất, tính ngẫu nhiên hoàn toàn được đảm bảo.

j) Tính cấp $\#E[F(2^m)]$ của đường cong E trên $F(2^m)$ được cho bởi $y^2 + xy = x^3 + ax^2 + b$.

   CHÚ THÍCH 4 Các phương pháp tính cấp $\#E[F(2^m)]$ được mô tả trong tài liệu tham khảo [11], [30] và [33].

k) Kiểm tra xem $\#E[F(2^m)]$ có phải là một số gần nguyên tố hay không bằng cách sử dụng thuật toán mô tả trong 6.2.2. Nếu đúng, thì đầu ra của thuật toán được mô tả trong 6.2.2 bao gồm các số nguyên r, n. Nếu sai, thì quay lại bước a).

l) Kiểm tra xem $E[F(2^m)]$ thỏa mãn điều kiện MOV quy định trong B.2.3. Nếu không thỏa mãn, thì quay lại bước a).

m) Kiểm tra xem ước số nguyên tố n có thỏa mãn điều kiện được quy định trong B.2.4 cho các hệ mật dựa trên ECDLP, ECDHP, hoặc BDHP với các đầu vào phụ trợ trong B.1.5 hay không. Nếu không thỏa mãn, thì quay lại bước a).

n) Sinh một điểm G trên E có cấp n sử dụng thuật toán được quy định trong 6.2.3.

o) Đầu ra là X, a, b, n, G.

CHÚ THÍCH 5 Sự cần thiết của tính gần nguyên tố được quy định trong B.2.2.

6.3.2 Kiểm tra tính giả ngẫu nhiên của đường cong elliptic

Thuật toán sau đây kiểm tra tính hợp lệ của một tập hợp các tham số đường cong elliptic. Ngoài ra, nó xác định xem đường cong elliptic trên $F(2^m)$ có được sinh bởi phương pháp trong 6.3.1 hay không.

Các đại lượng L_{Hash}, L, s, và w, và hàm băm H như trong 6.3.1.

Đầu vào: Một xâu bit X có độ dài L, các tham số EC $q = 2^m, a, b, n$ và $G = (x_G, y_G)$ và một số nguyên dương n_{min}.

Đầu ra: "Đúng" hoặc "Sai".

a) Tính $h = H(X)$.

b) Đặt W_0 là xâu bit nhận được bằng cách lấy w bit ngoài cùng bên phải của h.

c) Đặt $Z = BS2IP(x)$.

d) Với i từ 1 đến s thực hiện:

   1) Đặt $X_i = I2BSP(Z + i \bmod 2^L)$.

   2) Tính $W_i = H(X_i)$.

e) Đặt $W = W_0 || W_1 || \dots || W_s$.

f) Đặt $b' = OS2FEP[BS2OSP(W)]$.

g) Kiểm tra các điều kiện sau đây:

   1) $n \geq n_{min}$.

   2) n là một số nguyên tố.

   3) $b \neq 0_F$.

   4) $b = b'$.

   5) $G \neq O_E$.

   6) $y_G^2 + x_G y_G = x_G^3 + a x_G^2 + b$.

   7) $nG = O_E$.

h) Nếu tất cả các điều kiện trong bước g) thỏa mãn, thì đầu ra là "Đúng"; ngược lại đầu ra là "Sai".

7 Xây dựng đường cong elliptic bằng phép nhân phức

7.1 Cấu trúc chung (trường hợp trường nguyên tố)

Thuật toán sau đây sinh ra một đường cong E trên $F(p)$ với số các điểm hữu tỷ đã cho trước N.

CHÚ THÍCH 1 Thuật toán dựa trên tài liệu tham khảo [17] được áp dụng để chứng minh tính nguyên tố [10].

Đầu vào: Trường xác định $F(p)$ và số điểm $N = rn$, trong đó n là ước số nguyên tố lớn nhất của N và r là đồng hệ số.

Đầu ra: Các tham số đường cong của đường cong elliptic E với $\#E[F(p)] = N$ và điểm cơ sở G.

a) Kiểm tra xem ước số nguyên tố n có thỏa mãn điều kiện được quy định trong B.2.4 cho các hệ mật dựa trên ECDLP, ECDHP hoặc BDHP với các đầu vào phụ trợ như trong B.1.5 hay không. Nếu không thỏa mãn, thì thực thi với một đầu vào mới.

b) Đặt $t = p + 1 - N$.

c) Chọn một cặp số nguyên (D, V) sao cho $4p - t^2 = DV^2$.

d) Xây dựng đa thức lớp Hilbert $P_D(X)$.

e) Tìm một nghiệm j_0 trong $F(p)$ của $P_D(X) \equiv 0 \mod p$.

f) Chọn $c \in F(p)^*$ và xây dựng một đường cong elliptic trên $F(p)$ với j- bất biến j_0.

   1) $E_{D,j_0,c} : y^2 = x^3 + [3c^2 j_0/(1728 - j_0)]x + 2c^3 j_0/(1728 - j_0)$ (nếu $j_0 \neq 0_F, 1728$).

   2) $E_{D,j_0,c} : y^2 = x^3 + c$ (nếu $j_0 = 0_F$).

   3) $E_{D,j_0,c} : y^2 = x^3 + cx$ (nếu $j_0 = 1728$).

g) Xây dựng một điểm ngẫu nhiên G trên $E_{D,j_0,c}[F(p)]$ sao cho $G \neq O_E$ và $r \cdot G \neq O_E$.

h) Đặt $G = r \cdot G$.

i) Nếu $n \cdot G = O_E$, đưa ra các tham số đường cong của $E_{D,j_0,c}$ và điểm cơ sở G. Nếu $n \cdot G \neq O_E$, thì quay lại bước f) để lựa chọn giá trị c khác.

CHÚ THÍCH 2 Mọi cặp số nguyên (D, V) thỏa mãn $4p - t^2 = DV^2$ có thể được sử dụng trong bước c).

CHÚ THÍCH 3 Định nghĩa phương trình Diophantine được sử dụng trong bước c) có trong A.5.

CHÚ THÍCH 4 Định nghĩa đa thức lớp Hilbert $P_D(X)$ có trong A.2.

7.2 Đường cong Miyaji-Nakabayashi-Takano (MNT)

Thuật toán sau đây sinh một đường cong E trên $F(p)$ với bậc nhúng $B = 6$, phù hợp cho các hệ mật dựa trên phép ghép cặp song tuyến tính. Phép ghép cặp và bậc nhúng được mô tả lần lượt trong A.3 và B.2.2. Các ví dụ số và so sánh có trong Phụ lục C và Phụ lục D tương ứng.

CHÚ THÍCH 1 Một số thông tin và một thuật toán để sinh một đường cong MNT với $B = 3$ có trong tài liệu tham khảo [24].

CHÚ THÍCH 2 Có thể xây dựng các đường cong MNT không chỉ cho $B = 6$, mà còn cho $B = 3$ và 4.

Đầu vào: Cận dưới và trên (số nguyên lẻ) p_{min} và p_{max} cho trường xác định (tính bằng bit) và cận trên D_{max} cho độ lớn của D.

Đầu ra: Số nguyên tố p, các tham số đường cong của đường cong elliptic $E/F(p)$, cấp $n = \#E[F(p)]$ và điểm cơ sở G.

a) Chọn một số nguyên dương nhỏ $D < D_{max}$ sao cho $D \equiv 3(mod\ 8)$ và chuyển sang bước c).

b) Nếu không tồn tại giá trị D như vậy, thì dừng và cho đầu ra là "thất bại".

c) Tìm một cặp số nguyên (T, U) với $U > 0$ nhỏ nhất thỏa mãn $T^2 - 3DU^2 = 1$ bằng cách sử dụng thuật toán liên phân số.

d) Tìm một cặp số nguyên (x, y) thỏa mãn $x^2 - 3Dy^2 = -8$ và $0 \le x < 2U\sqrt{(2D)}, 2\sqrt{(2/D)} \le y < 2T\sqrt{(2/D)}$, nhờ sử dụng thuật toán Lagrange. Nếu không tìm được, quay lại bước a).

e) $i = 0$.

f) Tìm một cặp số nguyên tố (p, n) như sau:

1) Tính toán các số nguyên x_i và y_i sao cho $x_i + y_i\sqrt{(3D)} = [x + y\sqrt{(3D)}][T + U\sqrt{(3D)}]^i$.

CHÚ THÍCH 3 Không phải tất cả các nghiệm đều có thể được tìm ra bằng cách này.

2) Nếu $x_i \equiv 1(mod\ 6)$, thì $s = (x_i - 1)/6$ và $p = 4s^2 + 1$;

i) khác, nếu $x_i \equiv -1(mod\ 6)$, thì $s = (x_i + 1)/6$ và $p = 4s^2 + 1$;

ii) khác, $i = i + 1$ và quay lại bước 1).

3) Nếu $p < p_{min}$, thì $i = i + 1$ và quay lại bước 1).

4) Nếu $p > p_{max}$, thì quay lại bước a).

5) Nếu p là số nguyên tố, thì $n_1 = 4s^2 + 2s + 1$ và $n_2 = 4s^2 - 2s + 1$;

i) khác, $i = i + 1$ và quay lại bước 1).

6) Nếu $x_i \equiv 1(mod\ 6)$, thì $n = n_1$;

i) khác, $n = n_2$.

7) Nếu n là số nguyên tố, thì chuyển đến bước g);

i) khác, $i = i + 1$ và quay lại bước 1).

g) Kiểm tra xem ước số nguyên tố n có thỏa mãn điều kiện được mô tả trong B.2.4 cho các hệ mật dựa trên ECDLP, ECDHP hoặc BDHP với các đầu vào phụ trợ như trong B.1.5 hay không. Nếu không thỏa mãn, thì quay lại bước a).

h) Xây dựng đa thức lớp Hilbert $P_D(X)$.

i) Tìm một nghiệm j_0 trong $F(p)$ của $P_D(x) \equiv 0 \bmod p$.

j) Chọn $c \in F(p)^*$ và xây dựng một đường cong elliptic trên $F(p)$ với j- bất biến j_0.

1) $E_{D,j_0,c}: y^2 = x^3 + [3c^2 j_0/(1728 - j_0)]x + 2c^3 j_0/(1728 - j_0)$ (nếu $j_0 \ne 0_F, 1728$).

2) $E_{D,j_0,c}: y^2 = x^3 + c$ (nếu $j_0 = 0_F$).

3) $E_{D,j_0,c}: y^2 = x^3 + cx$ (nếu $j_0 = 1728$).

k) Xây dựng một điểm ngẫu nhiên G trên $E_{D,j_0,c}[F(p)]$, khác điểm tại vô hạn O_E.

l) Nếu $n \cdot G = O_E$, đầu ra là p, E, n và G.

m) Nếu $n \cdot G \neq O_E$, thì quay lại bước j) để chọn giá trị $c \in F(p)^*$ khác.

CHÚ THÍCH 4 Định nghĩa đa thức lớp Hilbert $P_D(X)$ có trong A.2.

CHÚ THÍCH 5 Thuật toán liên phân số trong bước c) có trong tài liệu tham khảo [27].

CHÚ THÍCH 6 Thuật toán Lagrange trong bước d) có trong tài liệu tham khảo [22] và [25].

CHÚ THÍCH 7 Kỹ thuật giúp tăng tốc độ một giao thức dựa trên phép ghép cặp song tuyến tính được mô tả trong tài liệu tham khảo [12].

7.3 Đường cong Barreto-Naehrig (BN)

Thuật toán sau đây sinh một đường cong elliptic E trên $F(p)$ với bậc nhúng $B = 12$, phù hợp cho các hệ mật dựa trên phép ghép cặp song tuyến tính. Bậc nhúng được mô tả trong B.2.2. Các ví dụ số và so sánh có trong Phụ lục C và Phụ lục D tương ứng.

CHÚ THÍCH 1 Thông tin chi tiết có trong tài liệu tham khảo [12].

CHÚ THÍCH 2 : Phương pháp này luôn luôn sinh ra nhiều nhất một đường cong với một giá trị cho trước m.

Đầu vào: Độ lớn xấp xỉ mong đợi m của cấp đường cong (tính bằng bit) và cận trên (số nguyên lẻ) p_{max} cho trường xác định.

Đầu ra: Số nguyên tố p, các tham số đường cong của đường cong elliptic $E/F(p)$, cấp $n = \#E[F(p)]$ và điểm cơ sở G.

a) Đặt $P(u) = 36u^4 + 36u^3 + 24u^2 + 6u + 1$.

b) Tính giá trị nhỏ nhất $u \approx 2^{m/4}$ sao cho $[log_2 P(-u)] = m$.

c) Lặp $p \leq p_{max}$

1) $t = 6u^2 + 1$.

2) $p = P(-u)$ và $n = p + 1 - t$.

3) Nếu p và n là số nguyên tố, thì chuyển sang bước e).

4) $p = P(u)$ và $n = p + 1 - t$.

5) Nếu p và n là số nguyên tố, thì chuyển sang bước e).

6) $u = u + 1$ và quay lại bước 1).

d) Dừng và cho đầu ra là "thất bại".

e) Kiểm tra xem ước số nguyên tố n có thỏa mãn điều kiện mô tả trong B.2.4 cho các hệ mật dựa trên ECDLP, ECDHP hoặc BDHP với các đầu vào phụ trợ như trong B.1.5 hay không. Nếu không thỏa mãn, thì quay lại bước a).

f) $b = 0$.

g) Nếu $b + 1$ không được biểu diễn dưới dạng $b + 1 = y_0^2 \bmod p$ đối với một số nguyên y_0, thì $b = b + 1$ và quay lại bước g).

h) Thiết lập một đường cong elliptic $E: y^2 = x^3 + b$.

i) Tính một căn bậc hai $y_0 \equiv \sqrt{(b+1)} \bmod p$.

j) Lấy điểm cơ sở $G = (1, y_0) \in E$.

k) Nếu $n \cdot G \neq O_E$, thì đặt $b = b + 1$ và quay lại bước g).

l) Đầu ra là p, E, n và G.

CHÚ THÍCH 3 Kỹ thuật giúp tăng tốc độ một giao thức dựa trên phép ghép cặp song tuyến tính được mô tả trong tài liệu tham khảo [12].

7.4 Đường cong Freeman (đường cong F)

Thuật toán sau đây sinh một đường cong elliptic E trên $F(p)$ với bậc nhúng $B = 10$, phù hợp cho các hệ mật dựa trên phép ghép cặp song tuyến tính. Bậc nhúng được mô tả trong B.2.2. Các ví dụ số và so sánh có trong Phụ lục C và Phụ lục D tương ứng.

CHÚ THÍCH 1 Thông tin chi tiết có trong tài liệu tham khảo [18].

Đầu vào: Cận dưới và trên p_{min} và p_{max} cho kích thước trường xác định (tính bằng bit) và cận trên D_{max} cho độ lớn của D.

Đầu ra: Số nguyên tố p, các tham số đường cong của đường cong elliptic $E/F(p)$, cấp $n = \#E[F(p)]$ và điểm cơ sở G.

a) Chọn một số nguyên dương nhỏ $D < D_{max}$ sao cho $D \equiv 43$ hoặc $67 \pmod{120}$ và $15D$ là số không có ước chính phương và chuyển sang bước c).

b) Nếu không tồn tại giá trị D như vậy, thì dừng và cho đầu ra là "thất bại".

c) Tìm một cặp số nguyên (T, U) với $U > 0$ nhỏ nhất thỏa mãn $T^2 - 15DU^2 = 1$ bằng cách sử dụng thuật toán liên phân số.

d) Đặt $g = T - U\sqrt{(15D)}$.

e) Tìm một cặp số nguyên (x, y) thỏa mãn $x^2 - 15Dy^2 = -20$ và $0 \leq x < 10U\sqrt{(3D)}, 2\sqrt{1/(3D)} \leq y < 2T\sqrt{1/(3D)}$ bằng cách sử dụng thuật toán Lagrange.

f) Đối với nghiệm hiện tại (x, y).

1) Nếu $x = \pm 5 (mod\ 15)$, thì:

i) Đặt $s = (-5 \pm x)/15$.

ii) Đặt $p = 25s^4 + 25s^3 + 25s^2 + 10s + 3$.

iii) Đặt $n = 25s^4 + 25s^3 + 15s^2 + 5s + 1$.

2) khác, chuyển sang bước 6).

3) Nếu $p > p_{max}$, quay lại bước a) để chọn một giá trị D mới.

4) khác nếu $p < p_{min}$, then chuyển sang bước 6).

5) Nếu p và n là các số nguyên tố, thì chuyển sang bước g).

6) Tìm một cặp số nguyên (x', y') sao cho $x' + y'\sqrt{15D} = (x + y\sqrt{15D}) \cdot g$.

CHÚ THÍCH 2 Không phải tất cả các nghiệm đều có thể được tìm ra bằng cách này.

7) Đặt $x = x'$ và $y = y'$ và quay lại bước 1).

g) Kiểm tra xem ước số nguyên tố n có thỏa mãn điều kiện mô tả trong B.2.4 cho các hệ mật dựa trên ECDLP, ECDHP hoặc BDHP với các đầu vào phụ trợ như trong B.1.5 hay không. Nếu không thỏa mãn, thì quay lại bước a).

h) Xây dựng đa thức lớp Hilbert $P_D(X)$.

i) Tìm một nghiệm j_0 trong $F(p)$ của $P_D(X) \equiv 0 \, mod \, p$.

j) Chọn $c \in F(p)^*$ và xây dựng một đường cong elliptic trên $F(p)$ với j- bất biến j_0.

1) $E_{D,j_0,c}: y^2 = x^3 + [3c^2 j_0/(1728 - j_0)]x + 2c^3 j_0/(1728 - j_0)$ (nếu $j_0 \neq 0_F, 1728$).

2) $E_{D,j_0,c}: y^2 = x^3 + c$ (nếu $j_0 = 0_F$).

3) $E_{D,j_0,c}: y^2 = x^3 + cx$ (nếu $j_0 = 1728$).

k) Xây dựng một điểm ngẫu nhiên G trên $E_{D,j_0,c}[F(p)]$ khác điểm tại vô hạn O_E.

l) Nếu $n \cdot G = O_E$, cho đầu ra là p, E, n và G.

m) Ngược lại, thì quay lại bước j) để chọn giá trị $c \in F(p)^*$ khác.

CHÚ THÍCH 3 Định nghĩa đa thức lớp Hilbert $P_D(X)$ trong bước i) có trong A.2.

CHÚ THÍCH 4 Thuật toán liên phân số trong bước c) có trong tài liệu tham khảo [27].

CHÚ THÍCH 5 Thuật toán Lagrange trong bước f) có trong tài liệu tham khảo [22] và [25].

CHÚ THÍCH 6 Kỹ thuật giúp tăng tốc độ một giao thức dựa trên phép ghép cặp song tuyến tính được mô tả trong tài liệu tham khảo [12].

7.5 Đường cong Cocks-Pinch (CP)

Thuật toán sau đây sinh một đường cong elliptic E trên $F(p)$ với bậc nhúng B tuỳ ý, phù hợp cho các hệ mật dựa trên phép ghép cặp song tuyến tính. Bậc nhúng được mô tả trong B.2.2.

CHÚ THÍCH 1 Thông tin chi tiết có trong tài liệu tham khảo [13].

Đầu vào: Một số nguyên dương B và một tập hợp R các số nguyên tố n ($n - 1$ chia hết cho B).

Đầu ra: Số nguyên tố p, các tham số đường cong của đường cong elliptic $E/F(p)$, cấp $n \cdot r = \#E[F(p)]$ và điểm cơ sở G.

a) Chọn một số nguyên dương không có ước chính phương, nhỏ D và n trong R sao cho $-D$ là số chính phương theo mô-đun n.

b) Tìm một căn nguyên thủy bậc B của phần tử đơn vị z trong $F(n)$.

c) $t' = z + 1$.

d) $y' = (t' - 2)/\sqrt{(-D)} (\mathrm{mod}\, n)$.

e) Lấy t là một số nguyên sao cho t bằng $t'\ mod\ n$ và lấy y là một số nguyên sao cho y bằng $y'\ mod\ n$.

f) $p = (t^2 + Dy^2)/4$.

CHÚ THÍCH 2 Có thể sử dụng $t = t'$ và $y = y'$.

g) Nếu p không phải là số nguyên tố, thì quay lại bước a).

h) Kiểm tra xem ước số nguyên tố n có thỏa mãn điều kiện mô tả trong B.2.4 cho các hệ mật dựa trên ECDLP, ECDHP hoặc BDHP với các đầu vào phụ trợ như trong B.1.5 hay không. Nếu không thỏa mãn, thì quay lại bước a).

i) Xây dựng đa thức lớp Hilbert $P_D(X)$.

j) Tìm một nghiệm j_0 trong $F(p)$ của $P_D(X) \equiv 0\ mod\ p$.

k) Chọn $c \in F(p)^*$ và xây dựng một đường cong elliptic trên $F(p)$ với j- bất biến j_0.

1) $E_{D,j_0,c}: y^2 = x^3 + [3c^2 j_0/(1728 - j_0)]x + 2c^3 j_0/(1728 - j_0)$ (nếu $j_0 \neq 0_F, 1728$).

2) $E_{D,j_0,c}: y^2 = x^3 + c$ (nếu $j_0 = 0_F$).

3) $E_{D,j_0,c}: y^2 = x^3 + cx$ (nếu $j_0 = 1728$).

l) Thiết lập đồng hệ số $r = (p + 1 - t)/n$.

m) Xây dựng một điểm ngẫu nhiên G trên $E_{D,j_0,c}[F(p)]$ sao cho $G \neq O_E$ và $r \cdot G \neq O_E$.

n) Đặt $G = r \cdot G$.

o) Nếu $n \cdot G = O_E$, đầu ra là n, G, và đường cong elliptic E.

p) Ngược lại, quay lại bước k) để chọn giá trị $c \in F(p)^*$ khác.

CHÚ THÍCH 3 Định nghĩa đa thức lớp Hilbert $P_D(X)$ trong bước c) có trong A.2.

CHÚ THÍCH 4 Kỹ thuật giúp tăng tốc độ một giao thức dựa trên phép ghép cặp song tuyến tính được mô tả trong tài liệu tham khảo [12].

8 Xây dựng đường cong elliptic bằng phép nâng

Thuật toán sau đây sinh một đường cong elliptic E trên $F(p^m)$ bằng cách nâng một đường cong elliptic E trên $F(p)$.

CHÚ THÍCH Thuật toán dựa trên tài liệu tham khảo [33].

Đầu vào: Trường hữu hạn nhỏ $F(p)$, đường cong elliptic E trên $F(p)$, cận dưới và cận trên N_{min} và N_{max} cho cấp của đường cong elliptic (tính bằng bit).

Đầu ra: Bậc mở rộng m, cấp $N_m = \#E[F(p^m)]$, điểm cơ sở G và cấp n của G.

a) Tính cấp $N = \#E[F(p)]$, điều này là dễ dàng thực hiện khi $F(p)$ nhỏ.

b) Đặt $t = p + 1 - N$ và tính các số nguyên đại số α và β thỏa mãn $t = \alpha + \beta$ và $p = \alpha\beta$.

c) Đặt $m = 1$.

d) Tìm một bộ ba (m, N_m, n) như sau:

1) Tính $N_m = pm + 1 - (\alpha^m + \beta^m)$ và $q = p^m$ là một số nguyên.

2) Nếu $N_m < N_{min}$, thì $m = m + 1$ và quay lại bước 1).

3) Nếu $N_m > N_{max}$, thì dừng và cho đầu ra là "thất bại".

4) Kiểm tra xem N_m có là một số gần nguyên tố hay không bằng cách sử dụng thuật toán được mô tả trong 6.2.2. Nếu thoản mãn, đầu ra của 6.2.2 bao gồm các số nguyên r và n. Nếu không thỏa mãn, thì $m = m + 1$ và quay lại bước 1).

5) Kiểm tra xem $E[F(q)]$ có thỏa mãn điều kiện MOV quy định trong B.2.3, tức là số nguyên B nhỏ nhất sao cho n chia hết $q^B - 1$ đảm bảo mức độ an toàn mong đợi hay không. Nếu không thỏa mãn, thì $m = m + 1$ và quay lại bước 1).

e) Sinh một điểm G trên $E[F(q)]$ có cấp n sử dụng thuật toán được mô tả trong 6.2.3.

f) Đầu ra là một bậc mở rộng m, cấp $N_m = \#E[F(q)]$, một điểm cơ sở G và cấp n.

Phụ lục A
(tham khảo)
Thông tin cơ bản về các đường cong elliptic

A.1 j-bất biến

Cho $F(q)$ là một trường hữu hạn với $q = p^m$, trong đó số nguyên tố $p > 3$. Cho E là một đường cong elliptic trên $F(q)$ xác định bởi phương trình Weierstrass dạng rút gọn:

$$Y^2 = X^3 + aX + b \text{ với } a, b \in F(q),$$

thỏa mãn bất đẳng thức $4a^3 + 27b^2 \neq 0_F$ trong $F(q)$. Khi đó, j- bất biến được định nghĩa như sau:

$$j = 1728 \cdot (4a^3)/(4a^3 + 27b^2).$$

Cho $F(2^m)$, với giá trị $m \geq 1$ nào đó, là một trường hữu hạn. Gọi E là một đường cong elliptic trên $F(2^m)$ xác định bởi công thức:

$$Y^2 + XY = X^3 + aX + b \text{ với } a, b \in F(2^m),$$

trong đó $b \neq 0_F$. Khi đó, j- bất biến được định nghĩa như sau:

$$j = 1/b.$$

Cho $F(3^m)$, với giá trị $m \geq 1$ nào đó, là một trường hữu hạn. Gọi E là một đường cong elliptic trên $F(3^m)$ xác định bởi công thức:

$$Y^2 = X^3 + aX^2 + b \text{ với } a, b \in F(3^m),$$

sao cho $a, b \neq 0_F$. Khi đó, j- bất biến được định nghĩa như sau:

$$j = -a^3/b.$$

A.2 Đa thức lớp Hilbert

Xây dựng đường cong elliptic bằng phép nhân phức sử dụng lý thuyết trường toàn phương ảo $Q(\sqrt{-D})$. Đối với trường toàn phương ảo $Q(\sqrt{-D})$, trường lớp Hilbert K là một trường mở rộng của $Q(\sqrt{-D})$, cũng chính là phần mở rộng abel không rẽ nhánh của $Q(\sqrt{-D})$. Đa thức lớp Hilbert $P_D(X)$ được xác định bằng đa thức tối tiểu của K trên $Q(\sqrt{-D})$. Trong việc xây dựng đường cong elliptic bằng phép nhân phức, j-bất biến của đường cong $E/F(p)$ được cho như một nghiệm của đa thức lớp Hilbert $P_D(X) \bmod p$.

CHÚ THÍCH 1 Những điều này được mô tả trong tài liệu tham khảo [13] và [16].

CHÚ THÍCH 2 Cơ sở dữ liệu trực tuyến của đa thức lớp Hilbert có trong tài liệu tham khảo [21].

A.3 Phép ghép cặp mật mã

Một phép ghép cặp mật mã e_n thỏa mãn các điều kiện không suy biến, song tuyến tính và tính toán được. Một phép ghép cặp e_n được định nghĩa trên $< G_1 > \times < G_2 >$ như sau:

$$e_n : < G_1 > \times < G_2 > \rightarrow \mu_n$$

trong đó $< G_1 >$ và $< G_2 >$ là các nhóm cyclic có cấp n và μ_n là nhóm cyclic gồm các căn bậc n của phần tử đơn vị. Một phép ghép cặp e_n nhận được bằng cách hạn chế miền xác định của các phép ghép cặp Weil hoặc Tate.

A.4 Phương trình Pell

Phương trình Pell là phương trình có dạng:

$$T^2 - dU^2 = \pm 1$$

trong đó d là một số nguyên cố định. Trong việc xây dựng các đường cong elliptic bằng phép nhân phức sử dụng phương trình Pell với một số nguyên dương d không phải là một số chính phương. Khi đó, tất cả các nghiệm nguyên dương (T, U) được tính bằng cách sử dụng nghiệm dương nhỏ nhất (T_0, U_0) với $U_0 > 0$ nhỏ nhất như sau:

$$T + U\sqrt{d} = (T_0 + U_0\sqrt{d})^k$$

với $k = 1,2, \ldots$

CHÚ THÍCH Những điều này được mô tả trong tài liệu tham khảo [28].

A.5 Phương trình Diophantine, $x^2 - dy^2 = n$

Trong việc xây dựng đường cong elliptic bằng phép nhân phức, phương trình Diophantine, $x^2 - dy^2 = n$ được sử dụng. Trong đó, n là một số nguyên và d là một số nguyên dương không phải là một số chính phương. Số lượng các nghiệm nguyên của công thức này bằng 0 hoặc vô hạn. Số lượng vô hạn các nghiệm nguyên (x, y) được cho bằng cách sử dụng nghiệm dương nhỏ nhất (T_0, U_0) với $U_0 > 0$ nhỏ nhất của phương trình Pell tương ứng $T^2 - dU^2 = 1$.

CHÚ THÍCH Thông tin chi tiết được mô tả trong tài liệu tham khảo [28].

Phụ lục B

(tham khảo)

Thông tin cơ bản về các hệ mật trên đường cong elliptic

B.1 Định nghĩa các bài toán mật mã

B.1.1 Bài toán lôgarit rời rạc trên đường cong elliptic (ECDLP)

Đối với một đường cong elliptic $E/F(q)$, điểm cơ sở $G \in E[F(q)]$ có cấp n và một điểm $P \in E[F(q)]$, bài toán lôgarit rời rạc trên đường cong elliptic (với điểm cơ sở G) là tìm số nguyên $x \in (0, n-1)$ sao cho $P = xG$ nếu tồn tại x như vậy.

Độ an toàn của các hệ mật trên đường cong elliptic là dựa trên độ khó được tin tưởng của bài toán lôgarit rời rạc trên đường cong elliptic.

B.1.2 Bài toán Diffie-Hellman tính toán trên đường cong elliptic (ECDHP)

Đối với một đường cong elliptic $E/F(q)$, điểm cơ sở $G \in E[F(q)]$ có cấp n và các điểm $aG, bG \in E[F(q)]$, bài toán Diffie-Hellman tính toán trên đường cong elliptic là tính abG.

Độ an toàn của một số hệ mật trên đường cong elliptic là dựa trên độ khó được tin tưởng của bài toán Diffie-Hellman tính toán trên đường cong elliptic.

B.1.3 Bài toán Diffie-Hellman quyết định trên đường cong elliptic (ECDDHP)

Đối với một đường cong elliptic $E/F(q)$, điểm cơ sở $G \in E[F(q)]$ có cấp n và các điểm $aG, bG, Y \in E[F(q)]$, bài toán Diffie-Hellman quyết định trên đường cong elliptic là quyết định xem liệu $Y = abG$ hay không.

Độ an toàn của một số hệ mật trên đường cong elliptic là dựa trên độ khó được tin tưởng của bài toán Diffie-Hellman quyết định trên đường cong elliptic.

B.1.4 Bài toán Diffie-Hellman song tuyến tính (BDHP)

Các bài toán Diffie-Hellman song tuyến tính được mô tả theo hai cách tùy thuộc vào các ánh xạ song tuyến tính mật mã tương ứng.

- Cho hai nhóm $< G_1 >$ và $< G_2 >$ có cấp n, một ánh xạ song tuyến tính mật mã $e_n: < G_1 > \times < G_2 > \rightarrow \mu_n, aG_1, bG_1 \in < G_1 >$, và $aG_2, bG_2 \in < G_2 >$, bài toán Diffie-Hellman song tuyến tính là tính toán $e_n(G_1, G_2)^{abc}$.

- Cho một nhóm $< G_1 >$ có cấp n, một ánh xạ song tuyến tính mật mã $e_n: < G_1 > \times < G_1 > \rightarrow \mu_n, aG_1, bG_1, cG_1 \in < G_1 >$, bài toán Diffie-Hellman song tuyến tính là tính toán $e_n(G_1, G_1)^{abc}$.

Độ an toàn của một số hệ mật trên đường cong elliptic là dựa trên độ khó được tin tưởng của bài toán Diffie-Hellman song tuyến tính trên đường cong elliptic.

B.1.5 Bài toán lôgarit rời rạc trên đường cong elliptic với các đầu vào phụ trợ (ECDLP với các đầu vào phụ trợ)

Độ an toàn của một số hệ mật dựa trên bài toán lôgarit rời rạc trên đường cong elliptic với các đầu vào phụ trợ.

- ECDLP với các đầu vào bổ sung $x^2G, x^3G, \ldots, x^kG$

- ECDHP với các đầu vào bổ sung $a^2G, a^3G, \ldots, a^kG$
- BDHP với các đầu vào bổ sung $a^2G_1, a^3G_1, \ldots, a^kG_1$

Ba ví dụ về các bài toán trên đường cong elliptic với các đầu vào phụ trợ được trình bày sau đây (tuân thủ ký hiệu từ phần định nghĩa chính thức của các bài toán trong B.1.1, B.1.2 và B.1.4).

B.2 Các thuật toán xác định lôgarit rời rạc trên đường cong elliptic

B.2.1 Độ khó của ECDLP

Độ khó của ECDLP phụ thuộc vào đường cong elliptic $E/F(q)$ được chọn và độ lớn của giá trị n là cấp của điểm cơ sở G. Độ lớn của n phải là lớn hơn hoặc bằng 160 bit để đảm bảo mức an toàn mong đợi trong các hệ mật dựa trên độ khó của ECDLP.

Đường cong elliptic $E/F(q)$ phải được chọn đáp ứng các mục tiêu an toàn xác định chống lại các thuật toán sau đây để giải ECDLP. Độ lớn của n phải được thiết lập đáp ứng các mục tiêu an toàn xác định chống lại thuật toán bước nhỏ - bước lớn và các biến thể khác của thuật toán ρ của Pollard.

B.2.2 Tổng quan về các thuật toán

Các kỹ thuật sau đây cho phép tính lôgarit rời rạc trên đường cong elliptic:

- Thuật toán Pohlig-Silver-Hellman. Đây là phương pháp "chia để trị" nhằm rút gọn bài toán lôgarit rời rạc trên một đường cong elliptic E định nghĩa trên $F(q)$ thành bài toán lôgarit rời rạc trong các nhóm con cyclic có cấp nguyên tố chia hết $\#E[F(q)]$.
- Thuật toán bước nhỏ - bước lớn và các biến thể khác của thuật toán ρ của Pollard.

CHÚ THÍCH 1 Các biến thể khác của thuật toán ρ của Pollard được mô tả trong tài liệu tham khảo [33].

- Thuật toán của Frey-Rück [19] và thuật toán Menezes-Okamoto-Vanstone [23] đều chuyển đổi bài toán lôgarit rời rạc trong một nhóm con cyclic của E với cấp nguyên tố n thành bài toán lôgarit rời rạc trong trường mở rộng nhỏ nhất $F(q^B)$ của $F(q)$ sao cho n chia hết $(q^B - 1)$, trong đó B được gọi là bậc nhúng. Thuật toán Frey-Rück chạy trong các điều kiện yếu hơn so với thuật toán được công bố bởi Menezes-Okamoto-Vanstone.
- Thuật toán của Araki-Satoh [29], Smart [32] và Semaev [31] giải quyết bài toán loogarit rời rạc đối với đường cong elliptic E xác định trên $F(p^m)$ trong trường hợp $\#E[F(p^m)] = p^m$.

Không giống với trường hợp lôgarit rời rạc trong nhóm nhân của một trường hữu hạn nào đó, không tồn tại thuật toán "tính toán chỉ số" đối với trường hợp đường cong elliptic. Về các tấn công sử dụng phép phủ đối với kiểu phủ đặc biệt, ví dụ: tấn công hạ bậc Weil, tấn công GHS,... xem chương 22 của tài liệu tham khảo [11].

CHÚ THÍCH 2 Các thuật toán Pohlig-Silver-Hellman và bước nhỏ - bước lớn làm việc trên tất cả các loại đường cong elliptic trong khi đó các thuật toán Frey-Rück, Menezes-Okamoto-Vanstone, Araki-Satoh, Smart, và Semaev chỉ làm việc trên các đường cong có các thuộc tính đặc biệt.

B.2.3 Điều kiện MOV

Cho n được định nghĩa như trong tập hợp các tham số miền đường cong elliptic, trong đó n là một ước số nguyên tố của $\#E[F(q)]$ và q là lũy thừa của một số nguyên tố p. Một giá trị B, được sử dụng cho điều kiện MOV, là số nguyên nhỏ nhất sao cho n chia hết $p^B - 1$. Như CHÚ THÍCH ở phần trên, các thuật toán Frey-Rück và Menezes-Okamoto-Vanstone biến đổi bài toán lôgarit rời rạc trên một đường cong elliptic trên $F(q)$ thành bài toán lôgarit rời rạc trong trường hữu hạn $F(p^B)$ với một số giá trị $B \geq 1$. Qua việc sử dụng tấn công, tính khó của bài toán lôgarit rời rạc trên một đường cong elliptic $E/F(q)$ liên quan

đến bài toán lôgarit rời rạc trên một trường hữu hạn $F(p^B)$. Điều kiện MOV đã điều chỉnh theo trường con mô tả bậc B mà đảm bảo mức an toàn của bài toán lôgarit rời rạc trên đường cong elliptic bằng bài toán lôgarit rời rạc trên trường hữu hạn. Đối với một số ứng dụng dựa trên phép ghép cặp Weil và Tate, một giá trị nhỏ hợp lý của B, chẳng hạn lớn hơn hoặc bằng 6, là thích hợp hơn cả.

CHÚ THÍCH Thông tin về bậc B được mô tả trong tài liệu tham khảo [20].

B.2.4 Điều kiện ước số nguyên tố, n

Đối với một số hệ mật dựa trên ECDLP, ECDHP hoặc BDHP với các đầu vào phụ trợ như trong B.1.5, ước số nguyên tố n phải thỏa mãn các điều kiện sau đây: không tồn tại ước số d của $n-1$ sao cho $(\log n)^2 < d < n^{1/2}$ và không tồn tại ước số e của $n+1$ sao cho $(\log n)^2 < e < n^{1/2}$. Các ước số d và e có thể là hợp số.

CHÚ THÍCH Độ lớn của d phụ thuộc vào k trong B.1.5, tức là giá trị lớn nhất của ước số lớn nhất của $n-1$ không vượt quá giá trị nhỏ nhất giữa k và $\sqrt{n}$. Thông tin chi tiết thêm về d và e có trong tài liệu tham khảo [14].

Phụ lục C
(tham khảo)
Các ví dụ số

C.1 Ví dụ số cho các đường cong elliptic giả ngẫu nhiên kiểm tra được

C.1.1 Giới thiệu chung

Tham chiếu tài liệu tham khảo [8] cho mục này. Các tham số được chọn từ một mầm sử dụng SHA-1.

C.1.2 Đường cong elliptic trên trường nguyên tố (192 bit)

p	ffffffff ffffffff ffffffff fffffffe ffffffff ffffffff
	$2^{192}-2^{64}-1$
a	ffffffff ffffffff ffffffff fffffffe ffffffff fffffffc
b	64210519 e59c80e7 0fa7e9ab 72243049 feb8deec c146b9b1
(mầm) X	3045ae6f c8422f64 ed579528 d38120ea e12196d5
(nén) G	03 188da80e b03090f6 7cbf20eb 43a18800 f4ff0afd 82ff1012
(không nén) G	04 188da80e b03090f6 7cbf20eb 43a18800 f4ff0afd 82ff1012 07192b95 ffc8da78 6310111ed 6b24cdd5 73f977a1 1e794811
n	ffffffff ffffffff ffffffff 99def836 146bc9b1 b4d22831
Đồng hệ số r	1

C.1.3 Đường cong elliptic trên trường nguyên tố (224 bit)

p	ffffffff ffffffff ffffffff ffffffff 00000000 00000000 00000001
	$2^{224}-2^{96}+1$
a	ffffffff ffffffff ffffffff fffffffe ffffffff ffffffff fffffffe
b	b4050a85 0c04b3ab f5413256 5044b0b7 d7bfd8ba 270b3943 2355ffb4
(mầm) X	bd713447 99d5c7fc dc45b59f a3b9ab8f 6a948bc5
(nén) G	02 b70e0cbd 6bb4bf7f 321390b9 4a03c1d3 56c21122 343280d6 115c1d21

(không nén) *G*

04 b70e0cbd 6bb4bf7f
321390b9 4a03c1d3 56c21122 343280d6 115c1d21 bd376388
b5f723fb 4c22dfe6 cd4375a0 5a074764 44d58199 85007e34

n

ffffffff
ffffffff ffffffff ffff16a2 e0b8f03e 13dd2945 5c5c2a3d

Đồng hệ số *r*

1

C.1.4 Đường cong elliptic trên trường nguyên tố (256 bit)

p

ffffffff 00000001
00000000 00000000 00000000 ffffffff ffffffff ffffffff

$2^{224}(2^{32}-1)+2^{192}+2^{96}-1$

a

ffffffff 00000001
00000000 00000000 00000000 ffffffff ffffffff fffffffc

b

5ac635d8 aa3a93e7
b3ebbd55 769886bc 651d06b0 cc53b0f6 3bce3c3e 27d2604b

(mầm) *X*

c49d3608 86e70493 6a6678e1 139d26b7 819f7e90

(nén) *G*

03 6b17d1f2 e12c4247
f8bce6e5 63a440f2 77037d81 2deb33a0 f4a13945 d898c296

(không nén) *G*

04 6b17d1f2 e12c4247 f8bce6e5 63a440f2
77037d81 2deb33a0 f4a13945 d898c296 4fe342e2 fe1a7f9b
8ee7eb4a 7c0f9e16 2bce3357 6b315ece cbb64068 37bf51f5

n

ffffffff 00000000
ffffffff ffffffff bce6faad a7179e84 f3b9cac2 fc632551

Đồng hệ số *r*

1

C.1.5 Đường cong elliptic trên trường nguyên tố (384 bit)

p	ffffffff ffffffff ffffffff ffffffff ffffffff ffffffff ffffffff fffffffe ffffffff 00000000 00000000 ffffffff $2^{384}-2^{128}-2^{96}+2^{32}-1$
a	ffffffff ffffffff ffffffff ffffffff ffffffff ffffffff ffffffff fffffffe ffffffff 00000000 00000000 fffffffc
b	b3312fa7 e23ee7e4 988e056b e3f82d19 181d9c6e fe814112 0314088f 5013875a c656398d 8a2ed19d 2a85c8ed d3ec2aef
(mầm) *X*	a335926a a319a27a 1d00896a 6773a482 7acdac73
(nén) *G*	03 aa87ca22 be8b0537 8eb1c71e f320ad74 6e1d3b62 8ba79b98 59f741e0 82542a38 5502f25d bf55296c 3a545e38 72760ab7
(không nén) *G*	04 aa87ca22 be8b0537 8eb1c71e f320ad74 6e1d3b62 8ba79b98 59f741e0 82542a38 5502f25d bf55296c 3a545e38 72760ab7 3617de4a 96262c6f 5d9e98bf 9292dc29 f8f41dbd 289a147c e9da3113 b5f0b8c0 0a60b1ce 1d7e819d 7a431d7c 90ea0e5f
n	ffffffff ffffffff ffffffff ffffffff ffffffff ffffffff c7634d81 f4372ddf 581a0db2 48b0a77a ecec196a ccc52973
Đồng hệ số *r*	1

C.1.6 Đường cong elliptic trên trường nguyên tố (521 bit)

p

01ff ffffffff ffffffff ffffffff ffffffff
ffffffff ffffffff ffffffff ffffffff ffffffff ffffffff
ffffffff ffffffff ffffffff ffffffff ffffffff ffffffff

$2^{521}-1$

a

01ff ffffffff ffffffff ffffffff ffffffff
ff1fffff ffffffff ffffffff ffffffff ffffffff ffffffff
ffiffffc ffffffff ffffffff ffffffff ffffffff fffffffc

b

0051 953eb961 8e1c9a1f 929a21a0 b68540ee
a2da725b 99b315f3 b8b48991 8ef109e1 56193951 ec7e937b
1652c0bd 3bb1bf07 3573df88 3d2c34f1 ef451fd4 6b503f00

(mầm) X

d09e8800 291cb853 96cc6717 393284aa a0da64ba

(nén) G

0200c6 858e06b7 0404e9cd 9e3ecb66 2395b442
9c648139 053fb521 f828af60 6b4d3dba a14b5e77 efe75928
fe1dc127 a2ffa8de 3348b3c1 856a429b f97e7e31 c2e5bd66

(không nén) G

04 00c6858e 06b70404 e9cd9e3e
cb662395 b4429c64 8139053f b521f828 af606b4d 3dbaa14b
5e77efe7 5928fe1d c127a2ff a8de3348 b3c1856a 429bf97e
7e31c2e5 bd660118 39296a78 9a3bc004 5c8a5fb4 2c7d1bd9
98f54449 579b4468 17afbd17 273e662c 97ee7299 5ef42640
c550b901 3fad0761 353c7086 a272c240 88be9476 9fd16650

n

01ff ffffffff ffffffff fffffffe 51868783 bf2f966b
7fcc0148 f709a5d0 3bb5c9b8 899c47ae bb6fb71e 91386409

Đồng hệ số r

1

C.2 Ví dụ số cho đường cong MNT

C.2.1 Giới thiệu chung

Thông tin cụ thể về các ví dụ cho đường cong Miyaji-Nakabayashi-Takano (MNT) trong 7.2 có trong tài liệu tham khảo [26].

C.2.2 Đường cong elliptic trên trường nguyên tố (160 bit)

p	8c72d321 e48aa141 9b22f914 cb43c112 b76d7ae5
a	8c72d321 e48aa141 9b22f914 cb43c112 b76d7ae2
b	299ce219 b7b01348 fc2b5007 b6ab1ee1 005676f7
(nén) G	03 00000000 00000000 00000000 00000000 00000002
(không nén) G	04 00000000 00000000 00000000 00000000 00000002 0be8f0d3 623edada ce4c2fac a541679b 002f1d07
n	8c72d321 e48aa141 9b23b6b2 e4a85a07 3822640f
Đồng hệ số r	1

C.2.3 Đường cong elliptic trên trường nguyên tố (256 bit)

p	f6529c2a 424a6332 b1d5054e 2f7b68aa ee7ef918 74dd140c 6919af9b 719ed905
a	f6529c2a 424a6332 b1d5054e 2f7b68aa ee7ef918 74dd140c 6919af9b 719ed902
b	6e974c68 ef44f266 ae3dd5d1 f97c497c 1d5452d1 b074a6c0 6a25a4e3 819ccd1c
(nén) G	02 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000003
(không nén) G	04 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000003 693d7af8 c4a29f8d e56e477f f569661c 4dcd2227 aac17b09 e4b4b0b7 03b978ce
n	f6529c2a 424a6332 b1d5054e 2f7b68ab e99c585a 8419ae9f b45c620e 5ef666c3
Đồng hệ số r	1

C.3 Ví dụ số cho đường cong BN

C.3.1 Giới thiệu chung

Tất cả các ví dụ sau đây được chọn sao cho p là số nguyên tố lớn nhất thỏa mãn $p = 3\ (mod\ 4)$ và $p = 4\ (mod\ 9)$ đối với tham số lớn nhất u có trọng số Hamming nhỏ nhất, cho phép trường mở rộng $F(p^2)$ được biểu diễn thành $F(p)[i]/(i^2 + 1)$ và trường mở rộng $F(p^{2m})$ được biểu diễn thành $F(p^2)[z]/(z^m - v)$ với $m = 2,3,6$ và $v = 1 + i$. Việc tính các căn bậc hai (hoặc bậc ba) cần thiết cho việc nén điểm và/hoặc phép ghép cặp cũng được đơn giản hóa trong cả $F(p)$ và $F(p^2)$. Ngoài ra, phương trình đường cong có dạng $E: y^2 = x^3 + 3$ với điểm cơ sở hiển nhiên $G = (1,2)$ và xoắn bậc sáu $E'/F(p^2)$ có dạng $E': y'^2 = x'^3 + 3v$ chứa một nhóm con có cấp n và đồng hệ số $h = 2p - n$, với điểm cơ sở $G' = hG'_0$, trong đó G'_0 là điểm với tọa độ x là $x'_0 = 1$. Cuối cùng, đẳng cấu $\Psi: E'/F(p^2) \rightarrow E/F(p^{12})$ có dạng $\Psi(x', y') =$

$(x'v^{-1}z^4, y'v^{-1}z^3)$, với $z^6 = v$. Những đặc tính này tạo điều kiện thuật lợi cho việc thực thi cặp Tate hoặc Weil (thuần túy hoặc nén) $e: E \times E' \rightarrow F(p^{2m})$, với các cặp tối ưu đặc biệt được hưởng ưu thế từ dạng thưa của u. Thông tin chi tiết cho những ví dụ này có trong tài liệu tham khảo [12].

C.3.2 Đường cong elliptic trên trường nguyên tố (160 bit)

p	ffffffda 48afd02c ccf4fe55 0dc1ddf3 f4046e43
a	0
b	3
(nén) G	02 00000000 00000000 00000000 00000000 00000001
(không nén) G	04 00000000 00000000 00000000 00000000 00000001 00000000 00000000 00000000 00000000 00000002
n	ffffffda 48afd02c ccf3fe55 0dd4bad5 95810cdd
Đồng hệ số r	1

C.3.3 Đường cong elliptic trên trường nguyên tố (192 bit)

p	ffffffff 26bac3d5 23661124 f38543e9 1f0186c1 f247719b
a	0
b	3
(nén) G	02 03000000 00000000 00000000 00000000 00000000 00000001
(không nén) G	04 00000000 00000000 00000000 00000000 00000000 00000001 00000000 00000000 00000000 00000000 00000000 00000002
n	ffffffff 26bac3d5 23661123 f38543ee 8ba2eb5d 35910e65
Đồng hệ số r	1

C.3.4 Đường cong elliptic trên trường nguyên tố (224 bit)

p	ffffffff fff10728 8ec29e60 2c4520db 42180823 bb907d12 87127833
a	0
b	3
(nén) G	02 00000000 00000000 00000000 00000000 00000000 00000001

(không nén) *G*

04 00000000 00000000
00000000 00000000 00000000 00000000 00000001 00000000
00000000 00000000 00000000 00000000 00000000 00000002

n

ffffffff
fff10728 8ec29e60 2c4420db 4218082b 36c2accf f76c58ed

Đồng hệ số *r*

1

C.3.5 Đường cong elliptic trên trường nguyên tố (256 bit)

p

ffffffff fffcf0cd
46e5f25e ee71a49f 0cdc65fb 12980a82 d3292ddb aed33013

a

0

b

3

(nén) *G*

02 00000000 00000000
00000000 00000000 00000000 00000000 00000000 00000001

(không nén) *G*

04 00000000 00000000 00000000 00000000
00000000 00000000 00000000 00000001 00000000 00000000
00000000 00000000 00000000 00000000 00000000 00000002

n

ffffffff fffcf0cd
46e5f25e ee71a49e 0cdc65fb 1299921a f62d536c d10b500d

Đồng hệ số *r*

1

C.3.6 Đường cong elliptic trên trường nguyên tố (384 bit)

p

ffffffff ffffffff fff2a968 23d5920d 2a127e3f 6fbca024
c8fbe295 31892c79 534f9d30 63282615 50a7cabd 7cccd10b

a

0

b

3

(nén) *G*

02

00000000 00000000 00000000 00000000 00000000 00000000
00000000 00000000 00000000 00000000 00000000 00000001

(không nén) *G*

04

00000000 00000000 00000000 00000000 00000000 00000000
00000000 00000000 00000000 00000000 00000000 00000001
00000000 00000000 00000000 00000000 00000000 00000000
00000000 00000000 00000000 00000000 00000000 00000002

n

ffffffff ffffffff fff2a968 23d5920d 2a127e3f 6fbca023
c8fbe295 31892c79 5356487d 8ac63e4f 4db17384 341a5775

Đồng hệ số *r*

1

C.3.7 Đường cong elliptic trên trường nguyên tố (512 bit)

p	ffffffff ffffffff ffffffff fff9ec7f 01c60ba1 d8cb5307 c0bbe3c1 11b0ef45 5146cf1e acbe98b8 e48c65de ab236fe1 916a55ce 5f4c6467 b4eb2809 22adef33
a	0
b	3
(nén) G	02 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000001
(không nén) G	04 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000001 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000002
n	ffffffff ffffffff ffffffff fff9ec7f 01c60ba1 d8cb5307 c0bbe3c1 11b0ef44 5146cf1e acbe98b8 e48c65dc ab2679a3 4a10313e 04f9a2b4 06a64a5f 519a09ed
Đồng hệ số r	1

C.4 Ví dụ số cho đường cong Freeman

C.4.1 Giới thiệu chung

Thông tin cụ thể về các ví dụ trong 7.4 có trong tài liệu tham khảo [18].

C.4.2 Đường cong elliptic trên trường nguyên tố (234 bit)

p	2a3 81f6c6d1 423bd477 5aa52e8b 38ffe9f2 36dfdd4a 4b6f5b03 8b3218db
a	2a3 81f6c6d1 423bd477 5aa52e8b 38ffe9f2 36dfdd4a 4b6f5b03 8b3218d8
b	248 268b780f a06cef9c 31295050 153fd4c6 f94dbbe6 21d5d68d a6487f2b
n	2a3 81f6c6d1 423bd477 5aa52e8b 38cbeecb 69176e35 bb5f3716 e4fe375b
D	492c7f03
j_0	22f 797b3651 920663fe 4bafb8ae 936a8e03 fae50ed6 91b32abc 806392dc

x	2232f3d6 535caaf9
y	1084 2631ac0b
Đồng hệ số r	1

C.4.3 Đường cong elliptic trên trường nguyên tố (252 bit)

p	e4989d4 fd7e87ff 6ff300ef d7e4393d 2c7ed585 2b0bf1c7 7b422e6f e4911f8b
a	e4989d4 fd7e87ff 6ff300ef d7e4393d 2c7ed585 2b0bf1c7 7b422e6f e4911f88
b	aefa431 ec51a8a3 7e999461 fe75b15b f85dd6e1 19ab1142 1b798e51 c565610d
n	e4989d4 fd7e87ff 6ff300ef d7e4393c b38a4f5e ceb8cc58 c00200ff c97e408d
D	3df4c893
j_0	a2f8ef5 6a4a1263 cd667d1a c0ddafd6 73fb2d4d d2acc85e 7d1879de ef60e305
x	3 42afc7c6 f6b26de7
y	1b615 02ae2383
Đồng hệ số r	1

Phụ lục D
(tham khảo)

Tóm tắt các thuộc tính của các đường cong elliptic được sinh bằng phương pháp nhân phức

Trong phụ lục này, các thuộc tính của bốn phương pháp sinh đường cong bằng phương pháp nhân phức cho các đường cong MNT, đường cong BN, đường cong F và đường cong CP được tổng hợp, trong đó sử dụng những ký hiệu sau đây.

- $E[F(p)], \#E[F(p)] = rn$ (r: đồng hệ số, n: ước số nguyên tố)
- B: bậc nhúng
- $4p - t^2 = Dy^2$ (t: vết, D: số nguyên không có ước chính phương)

Bảng D.1 là bảng tóm tắt các thuộc tính của các đường cong được sinh bởi bốn phương pháp.

Bảng D.1 – Tóm tắt các đường cong elliptic được sinh bởi phương pháp nhân phức tạp

	B	D	$log_2 p/log_2 n$	Đặc tính
Đường cong MNT	3, 4, 6	$D \equiv 3 (\mathrm{mod}\ 8)$	1	Có thể xây dựng tất cả các đường cong elliptic cấp nguyên tố với $B = 3,4,6$.
Đường cong BN	12	3	1	Xây dựng được một đường cong elliptic với $D = 3$ và $B = 12$ (không phải tất cả).
Đường cong F	10	$D \equiv$ 43 hoặc 47 (mod 1 và $15D$ là số không chính phương	1	Xây dựng được một đường cong elliptic với $B = 10$ (không phải tất cả).
Đường cong CP	Tùy chọn	Tùy chọn	> 2	$log_2 p > 2log_2 n$

Thư mục tài liệu tham khảo

[1] ISO/IEC 9796-3, *Information technology — Security techniques — Digital signature schemes giving message recovery — Part 3: Discrete logarithm based mechanisms*

[2] ISO/IEC 10118 (all parts), *Information technology — Security techniques — Hash-functions*

[3] ISO/IEC 11770-3, *Information technology — Security techniques — Key management — Part 3: Mechanisms using asymmetric techniques*

[4] ISO/IEC 14888-3, *Information technology — Security techniques — Digital signatures with appendix — Part 3: Discrete logarithm based mechanisms*

[5] ISO/IEC 18032, *Information technology — Security techniques — Prime number generation*

[6] ISO/IEC 18033-2, *Information technology — Security techniques — Encryption algorithms — Part 2: Asymmetric ciphers*

[7] ISO/IEC 29192-4, *Information technology — Security techniques — Lightweight cryptography — Part 4: Mechanisms using asymmetric techniques*

[8] FIPS. 186-2, *Digital Signature Standard. Federal Information Processing Standards Publication 186-2, 2000.* Available from: http://csrc.nist.gov/

[9] IEEE P1363-2000, *Standard Specifications for Public-Key Cryptography*

[10] ATKIN A.O.L., & MORAIN F. Elliptic curves and primality proving. *Math. Comput.* 1993, **61** pp. 29-68

[11] COHEN H., FREY G., AVANZI R., DOCHE C., LANGE T., NGUYEN K. *Handbook of Elliptic and Hyperelliptic Curve Cryptography.* Chapman & Hall/CRC, 2006

[12] BARRETO P.S.L.M., & NAEHRIG M. Pairing-friendly elliptic curves of prime order. In: *Selected Areas in Cryptography-SAC'2005, LNCS 3897.* Springer-Verlag, 2006, pp. 319-31.

[13] BLAKE I., SEROUSSI G., SMART N. *"Advances in elliptic curve cryptography",* London Mathematical Society Lecture Note Series 317

[14] CHEON J. Security Analysis of the Strong Diffie-Hellman Problem. In: *Eurocrypt 2006, LNCS 4004.* Springer-Verlag, 2006, pp. 1-11.

[15] COHEN H. *"A course in computational algebraic number theory",* Graduate Texts in Math. 138, Springer-Verlag, 1993, Third corrected printing, 1996.

[16] Cox D.A. *"Primes of the form $x^2 + ny^2$",* A Wiley-Interscience Publication, 1989

[17] DEURING M. Die Typen der Multiplikatorenringe elliptischer Funktionenkorper. *Abh. Math. Sem.Hamburg.* 1941, **14** pp. 197-272

[18] FREEMAN D. *"Constructing pairing-friendly elliptic curves with embedding degree 10",* In ANTS-V11, Springer- Verlag, LNCS 4076, Berlin, 2006, 452-465

[19] FREY G., & RUCK H.G. A remark concerning m-divisibility and the discrete logarithm in the divisor class group of curves. *Math. Comput.* 1994, **62** pp. 865-874

[20] HITT L. *"On the minimal embedding field"*, In Proceedings of the International Conference on Pairing-Based Cryptography 2007 (Pairing 2007), LNCS 4575 (2007), Springer-Verlag, 294-301

[21] KOHEL D.R. *"Algorithms for Algebra and Geometry Experimentation"* http://echidna.maths.usyd.edu.au/~kohel/dbs/

[22] MATTHEWS K. *The Diophantine equation $x^2Dy^2 = N$, $D > 1$. Expo. Math.* 2000, **18** pp. 323-331

[23] MENEZES A., OKAMOTO T., VANSTONE S. *"Reducing elliptic curve logarithms to logarithms in a finite field"*, Proceedings of the 22nd Annual ACM Symposium on the Theory of Computing (1991), 80-89

[24] MIYAJI A., NAKABAYASHI M., TAKANO S. *"New explicit conditions of Elliptic Curve Traces under FR reduction"*, IEICE Trans. Fundamentals. 2001, **E84-A** (5) pp. 1234-1243

[25] MOLLIN R. *Fundamental Number Theory with Applications.* CRC Press, Boca Raton, 1998

[26] PAGE D Smart N.P., Vercauteren F. *A comparison of MNT curves and supersingular curves"*, AAECC, 17. Springer-Verlag, 2006, pp. 379-392

[27] ROBERTSON J. *"Solving the generalized Pell equation"*, Unpublished manuscript (2004), available at http://www.jpr2718.org/pell.pdf

[28] ROSEN K.H. *Elementary number theory and its applications.* Addison Welsley Longman, 1999

[29] SATOH T., & ARAKI K. Fermat quotients and the polynomial time discrete logalgorithm for anomalous elliptic curves. *Comrnentarii Math. Univ. St. Pauli.* 1998, **47** pp. 81-92

[30] ScHooF R. Elliptic Curves Over Finite Fields and the Computation of Square Roots mod p. *Math.Comput.* 1985, **44** pp. 483-494

[31] SEMAEV I.A. Evaluation of discrete logarithms in a group of p-torsion points of an elliptic curve in characteristic p. *Math. Cornput.* 1998, **67** pp. 353-356

[32] SMART N.P. The discrete logarithm problem on elliptic curves of trace one./ *Cryptol.* 1999, **12** pp. 193-196

[33] WASHINGTON L.C. *Elliptic Curves-Number Theory and Cryptography.* Chapman & Hall/CRC, Second Edition, 2008