TCVN TIÊU CHUẨN QUỐC GIA

TCVN 12852-1 : 2020

ISO/IEC 15946-1 : 2016

Xuất bản lần 1

CÔNG NGHỆ THÔNG TIN – CÁC KỸ THUẬT AN TOÀN – KỸ THUẬT MẬT MÃ DỰA TRÊN ĐƯỜNG CONG ELLIPTIC – PHẦN 1: TỔNG QUAN

Information technology – Security techniques – Cryptography based on elliptic curves – Part 1: General

HÀ NỘI – 2020

Mục Lục

Lời nói đầu

TCVN 12852-1 : 2020 hoàn toàn tương đương với ISO/IEC 15946-1:2016.

TCVN 12852-1 : 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 – Mật mã hạng nhẹ* gồm các tiêu chuẩn sau:

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

- TCVN 12852-5 : 2020 (TCVN 12852-5:2017) Phần 5: Sinh đường cong elliptic

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

TIÊU CHUẨN QUỐC GIA **TCVN 12852-1 : 2020**

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

Information technology – Security techniques – Cryptography based on elliptic curves – Part 1: General

1 Phạm vi áp dụng

Tiêu chuẩn này mô tả nền tảng toán học và các kĩ thuật chung cần thiết để thực hiện các cơ chế mật mã trên đường cong elliptic được mô tả trong các tiêu chuẩn TCVN 12852-5, TCVN 12855-3, TCVN 7817-3, TCVN 12214-3, TCVN 11367-2 và các tiêu chuẩn có liên quan.

Tiêu chuẩn này không chỉ ra việc thực thi các kĩ thuật mà nó mô tả. Ví dụ, nó không mô tả phép biểu diễn cơ sở được sử dụng khi đường cong elliptic định nghĩa trên trường hữu hạn có đặc số hai. Do đó, các cơ chế bên trong của các sản phẩm tuân thủ theo tiêu chuẩn 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 12852-5:2020 (ISO/IEC 15946-5), Công nghệ thông tin - Các kỹ thuật an toàn - Kỹ thuật mật mã dựa trên đường cong elliptic - Phần 5: Sinh đường cong elliptic.

3 Thuật ngữ và định nghĩa

Tiêu chuẩn này áp dụng các thuật ngữ và định nghĩa sau:

3.1

Nhóm Abel (abelian group)

Nhóm $(S,*)$ sao cho $a*b=b*a$ với mọi $a,b\in S$

3.2

Đường cong bậc ba (cubic curve)

Tập hợp các nghiệm, tạo ra bởi các cặp phần tử của một trường xác định, được biết như là các điểm, của một phương trình bậc ba ở dạng đặc biệt.

3.3

Đường cong elliptic (elliptic curve)

Đường cong bậc ba *E* mà không có điểm kì dị

CHÚ THÍCH 1 Tập các điểm E cùng với một phép toán được định nghĩa một cách thích hợp (xem mục 6.2) tạo thành một nhóm abel. Trường bao gồm tất cả các hệ số của phương trình mô tả *E* được gọi là trường định nghĩa của *E*. Trong tiêu chuẩn này, chỉ các trường hữu hạn *F* được sử dụng làm trường xác định. Khi cần biểu thị trường định nghĩa *F* của *E* một cách rõ ràng, đường cong được ký hiệu là E/F.

CHÚ THÍCH 2 Dạng của một phương trình đường cong bậc ba sử dụng để định nghĩa một đường cong elliptic thay đổi phụ thuộc vào trường. Dạng tổng quát của một phương trình bậc ba phù hợp cho tất cả các trường hữu hạn được định nghĩa trong 6.1

CHÚ THÍCH 3 Định ghĩa của một đường cong bậc ba được đưa ra trong tài liệu viện dẫn [15].

3.4

Trường (field)

Tập các phần tử S và một cặp các phép toán (+, *) định nghĩa trên S sao cho: (i) a*(b + c) = a*b + a*c với mọi a, b, c thuộc S, (ii) S cùng với phép toán + tạo thành một nhóm albel (với phần tử trung hòa 0) và (iii) S loại bỏ phần tử 0 cùng với phép toán * tạo thành một nhóm abel.

3.5

Trường hữu hạn (finite field)

Trường bao gồm một số hữu hạn các phần tử

CHÚ THÍCH Với số nguyên dương *m* và số nguyên tố *p* tùy ý, tồn tại một trường hữu hạn chứa chính xác p^m phần tử. Trường này là duy nhất sai khác đẳng cấu và được kí hiệu là $F(p^m)$ với *p* được gọi là đặc số của $F(p^m)$.

3.6

Nhóm (group)

Tập hợp các phần tử S và một phép toán * xác định trên tập các phần tử sao cho (i) $a*(b*c)=(a*b)*c$ với mọi a, b, c thuộc S, (ii) tồn tại một phần tử trung hòa e thuộc S sao cho $a*e=e*a=a$ với mọi a thuộc S, và (iii) với mọi a thuộc S tồn tại phần tử nghịch đảo a^{-1} trong S sao cho $a*a^{-1}=a^{-1}*a=e$

3.7

Ánh xạ mật mã song tuyến tính (cryptographic bilinear map)

Ánh xạ thỏa mãn tính không suy biến, song tuyến tính và có thể tính toán được.

CHÚ THÍCH 1 Định nghĩa của tính không suy biến, song tuyến tính và có thể tính toán được được cho trong 6.4

3.8

Điểm kì dị (signular point)

Điểm mà tại đó một đối tượng toán học cho trước không được xác định.

4 Các ký hiệu

B	Số nguyên dương nhỏ nhất sao cho *n* chia hết $q^B - 1$
d	Khóa bí mật của người dùng (*d* là một số nguyên ngẫu nhiên trong tập [2, n-2])
E	Đường cong elliptic cho bởi phương trình có dạng $Y^2 = X^3 + aX + b$ trên trường $F(p^m)$ với $p > 3$, hoặc cho bởi một phương trình có dạng $Y^2 + XY = X^3 + aX^2 + b$ trên trường $F(2^m)$, hoặc cho bởi phương trình $Y^2 = X^3 + aX^2 + b$ trên trường $F(3^m)$, cùng với một điểm O_E được gọi là điểm tại vô hạn; đường cong được kí hiệu là $E/F(P^m)$, $E/F(2^m)$ và $E/F(3^m)$, tương ứng.
$E(F(q))$	Tập các điểm có tọa độ thuộc *F(q)* của *E* cùng với O_E
$\#E(F(q))$	Cấp hoặc lực lượng của $E(F(q))$
$E(n)$	Nhóm n-xoắn của *E*, tức là $\{Q \in E \mid nQ = O_E\}$
e_n	Ánh xạ mật mã song tuyến tính
$\|F\|$	Số phần tử trong *F*
F(q)	Trường hữu hạn gồm có chính xác *q* phần tử, bao gồm các trường hợp *F(p)*, $F(2^m)$ và $F(p^m)$
*F(q)**	$F(q)\backslash\{0_F\}$
G	Điểm cơ sở trên *E* với cấp nguyên tố *n*
<*G*>	Nhóm được sinh bởi *G* với cấp nguyên tố *n*
h	Đồng hệ số của *E(F(q))*
kQ	Bội thứ k của một điểm Q nào đó của *E*, tức là $kQ = Q + ... + Q$ (*k* lần phép cộng) nếu $k > 0$, $kQ = (-k)(-Q)$, nếu $k < 0$, và $kQ = O_E$ nếu $k = 0$
μ_n	Nhóm cyclic cấp n gồm các căn bậc n của phần tử đơn vị trong bao đóng đại số của *F(q)*
n	Ước nguyên tố của *#E(F(q))*
O_E	Điểm của đường cong elliptic tại vô hạn
p	Số nguyên tố
P	khóa công khai của người dùng (*P* là một điểm đường cong elliptic trong <*G*>)
q	Lũy thừa nguyên tố p^m của một số nguyên tố *p* và số nguyên $m \geq 1$ nào đó
Q	Điểm trên *E* với các tọa độ (x_Q, y_Q)
$Q_1 + Q_2$	Tổng của hai điểm Q_1 và Q_2 trên đường cong elliptic
x_Q	Tọa độ *x* của $Q \neq O_E$
y_Q	Tọa độ *y* của $Q \neq O_E$
[0,k]	Tập các số nguyên từ 0 đến *k*
0_F	Phần tử trung hòa của *F(q)* đối với phép cộng

1_F Phần tử trung hòa của *F(q)* đối với phép nhân

5 Quy ước cho các trường

5.1 Trường nguyên tố hữu hạn *F(p)*

Với số nguyên tố *p* bất kì, tồn tại một trường hữu hạn chứa chính xác *p* phần tử. Trường này được xác định duy nhất sai khác đẳng cấu và trong tiêu chuẩn này nó được gọi là trường nguyên tố hữu hạn F(p).

Các phần tử của trường nguyên tố hữu hạn *F(p)* có thể được đồng nhất với tập *[0, p-1]* gồm tất cả các số nguyên không âm nhỏ hơn *p*. *F(p)* được cung cấp 2 phép toán gọi là phép toán cộng và phép toán nhân sao cho các điều kiện sau được thỏa mãn:

- *F(p)* là một nhóm abel đối với phép toán cộng "+"

Với $a,b \in F(p)$ tổng $a+b$ được định nghĩa là $a+b := r$, trong đó $r \in F(p)$ là phần dư thu được khi lấy số nguyên tổng $a+b$ chia cho *p*.

- $F(p)\backslash\{0\}$, kí hiệu *F(p)** là một nhóm abel với phép toán nhân "x".

Với $a,b \in F(p)$ tích $a \times b$ được định nghĩa là $a \times b := r$, trong đó $r \in F(p)$ là phần dư thu được khi lấy số nguyên tích $a \times b$ chia cho *p*. Khi không sợ gây nhầm lẫn, thì dấu x được lược bỏ và kí hiệu thay thế là a.b hoặc ab được sử dụng.

5.2 Các trường hữu hạn $F(p^m)$

Với số nguyên dương *m* và số nguyên tố *p* bất kỳ, tồn tại một trường hữu hạn có chính xác p^m phần tử. Trường này là duy nhất sai khác đẳng cấu và trong tiêu chuẩn này nó được gọi là trường hữu hạn $F(p^m)$

CHÚ THÍCH 1 $F(p^m)$ là định nghĩa tổng quát bao gồm cả *F(p)* với *m = 1* và $F(2^m)$ với *p = 2*.

CHÚ THÍCH 2 Nếu *p = 2* thì các phần tử của trường có thể được đồng nhất với các xâu bit có độ dài *m* và tổng của hai phần tử trường là phép loại trừ *XOR* theo từng bit của hai xâu bit.

Trường hữu hạn $F(p^m)$ có thể được đồng nhất với tập các xâu *p*-phân với độ dài m theo cách sau đây.

Mỗi trường hữu hạn $F(p^m)$ chứa ít nhất một cơ sở $\{\xi_1, \xi_2, ..., \xi_m\}$ trên trường *F(p)* sao cho mọi phần tử $\alpha \in F(p^m)$ có một biểu diễn duy nhất dưới dạng $\alpha = a_1\xi_1 + a_2\xi_2 + ... + a_m\xi_m$, trong đó $a_i \in F(p)$ với *i = 1, 2..., m*. Khi đó phần tử α có thể được đồng nhất với xâu *p*-phân $(a_1, a_2, ..., a_m)$. Việc chọn cơ sở nằm ngoài phạm vi của tiêu chuẩn này. $F(p^m)$ được bổ xung hai phép toán gọi là phép toán cộng và phép toán nhân thỏa mãn các điều kiện sau:

- $F(p^m)$ là nhóm abel với Phép toán cộng "+"

Với $\alpha = (a_1, a_2, ..., a_m)$ và $\beta = (b_1, b_2, ..., b_m)$, tổng $\alpha + \beta$ được cho bởi $\alpha + \beta := \gamma = (c_1, c_2, ..., c_m)$, trong đó $c_i = a_i + b_i$ là tổng trong *F(p)*. Phần tử trung hòa của phép cộng là $0_F = (0, 0, ...0)$.

- $F(p^m)\backslash\{0\}$, kí hiệu bởi $F(p^m)^*$ là một nhóm abel với phép toán nhân "x".

Với $\alpha = (a_1, a_2, ..., a_m)$ và $\beta = (b_1, b_2, ..., b_m)$ tích $\alpha \times \beta$ được cho bởi một xâu p-phân $\alpha \times \beta := \gamma = (c_1, c_2, ..., c_m)$ trong đó $c_i = \sum_{1 \le j,k \le m} a_j b_k d_{i,j,k}$, với $\xi_j \xi_k = d_{1,j,k}\xi_1 + d_{2,j,k}\xi_2 + ... + d_{m,j,k}\xi_m (1 \le j, k \le m)$. Khi không sợ gây nhầm lẫn thì kí hiệu phép nhân "x" được bỏ

qua và kí hiệu *ab* được sử dụng. Cơ sở có thể chọn theo cách sao cho phần tử trung hòa của phép nhân là $1_F = (1,0,0,...,0)$.

CHÚ THÍCH 3 Việc chọn cơ sở được mô tả trong tài liệu viện dẫn [4].

6 Các quy ước trên đường cong elliptic

6.1 Định nghĩa các đường cong elliptic

6.1.1 Đường cong elliptic trên trường $F(p^m)$

Cho $F(p^m)$ là một trường hữu hạn với số nguyên *tố p* > 3 và một số nguyên dương *m*. Trong tiêu chuẩn này, ta giả sử rằng *E* được mô tả bằng một phương trình Weierstrass (dạng affine) rút gọn, tức là phương trình có dạng:

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

sao cho $4a^3 + 27b^2 \neq 0_F$ trong trường $F(p^m)$.

CHÚ THÍCH Đường cong trên với $4a^3 + 27b^2 = 0_F$ được gọi là đường cong kì dị và đó không phải là một đường cong elliptic.

Tập các điểm với tọa độ trong $F(p^m)$ (các điểm $F(p^m)$ –giá trị) của *E* được đưa ra bởi công thức (1):

$$E(F(p^m)) = \{Q = (x_Q, y_Q) \in F(p^m) \times F(p^m) \mid y_Q^2 = x_Q^3 + ax_Q + b\} \cup \{O_E\} \quad (1)$$

trong đó O_E là điểm đặc biệt được gọi là điểm tại vô hạn của *E*.

6.1.2 Các đường cong elliptic trên $F(2^m)$

Cho $F(2^m)$, với $m \geq 1$ nào đó, là một trường hữu hạn. Trong tiêu chuẩn này, ta giả sử *E* được mô tả bởi một phương trình có dạng:

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

sao cho $b \neq 0_F$ là đúng trong $F(2^m)$.

Để sử dụng trong lĩnh vực mật mã, *m* phải là một số nguyên tố để chống lại được các loại tấn công vào các hệ mật mã.

CHÚ THÍCH Đường cong trên với $b = 0_F$ được gọi là đường cong kì dị, không phải đường cong elliptic.

Tập các điểm với tọa độ trong $F(2^m)$ (các điểm $F(2^m)$ –giá trị) của *E* được cho bởi công thức (2)

$$E(F(2^m)) = \{Q = (x_Q, y_Q) \in F(2^m) \times F(2^m) \mid y_Q^2 + x_Q y_Q = x_Q^3 + ax_Q^2 + b\} \cup \{O_E\} \quad (2)$$

với O_E là điểm đặc biệt, được gọi là điểm tại vô hạn của *E*.

6.1.3 Các đường cong elliptic trên trường $F(3^m)$

Cho $F(3^m)$ là một trường hữu hạn với một số nguyên dương *m*. Trong tiêu chuẩn này, ta giả sử rằng *E* được mô tả bởi một phương trình có dạng:

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

sao cho $a,b \neq 0_F$ trong $F(3^m)$

CHÚ THÍCH Đường cong trên với a hoặc $b = 0_F$ được gọi là đường cong kì dị, không phải là đường cong elliptic.

Tập các điểm với tọa độ trong $F(3^m)$ (các điểm $F(3^m)$ –giá trị) của E được cho bởi công thức (3)

$$E(F(3^m)) = \{Q = (x_Q, y_Q) \in F(3^m) \times F(3^m) \mid y_Q^2 = x_Q^3 + ax_Q^2 + b\} \cup \{O_E\} \quad (3)$$

với O_E là điểm đặc biệt được gọi là điểm tại vô hạn của E.

6.2 Luật nhóm trên các đường cong elliptic

Đường cong elliptic được cung cấp phép toán cộng + : $E \times E \to E$, xác định đối với mỗi cặp $\{Q_1, Q_2\}$ các điểm trên E một điểm thứ 3 $Q_1 + Q_2$. Với phép toán cộng này, E là một nhóm abel với phần tử trung hòa O_E. Bội số k lần của Q được định nghĩa là kQ, trong đó $kQ = Q + ... + Q$ (tổng k lần) nếu $k > 0, kQ = (-k)(-Q)$ nếu $k < 0$, và $kQ = O_E$ nếu $k = 0$. Số dương nhỏ nhất k với $kQ = O_E$ được gọi là cấp của Q.

CHÚ THÍCH Công thức của luật nhóm và Q được đưa ra trong B.3, B.4 và B.5

6.3 Sinh các đường cong elliptic

Để sử dụng đường cong elliptic cho các hệ mật mã, việc sinh một đường cong elliptic thích hợp là cần thiết. TCVN 12852-5 là tài liệu tham chiếu cho các phương pháp sinh đường cong elliptic.

6.4 Ánh xạ song tuyến tính mật mã

Ánh xạ song tuyến tính mật mã e_n được sử dụng trong một số ứng dụng mật mã, chẳng hạn như các lược đồ kí số hoặc lược đồ thỏa thuận khóa. Một ánh xạ song tuyến tính mật mã e_n được xác định qua việc lấy hạn chế trên miền xác định của các phép ghép cặp Weil hoặc Tate như sau.

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

trong đó ánh xạ song tuyến tính mật mã e_n thỏa mãn các tính chất sau:

- Tính song tuyến tính: $e_n(aG_1, bG_2) = e(G_1, G_2)^{ab}$ ($\forall\, a, b \in [0, n-1]$);

- Không suy biến: $e_n(G_1, G_2) \neq 1$;

- Có thể tính toán được: Tồn tại một thuật toán hiệu quả đển tính toán e_n.

CHÚ THÍCH 1 Mối liên hệ giữa ánh xạ song tuyến tính mật mã với phép ghépcặp Weil hoặc Tate được chỉ ra trong B.7

CHÚ THÍCH 2 Công thức cho các phép ghép cặp Weil và Tate được chỉ ra trong C.6

CHÚ THÍCH 3 Có hai kiểu ghép cặp:

- Trường hợp $G_1 = G_2$;
- Trường hợp $G_1 \neq G_2$.

7 Các hàm chuyển đổi

7.1 Chuyển đổi xâu bộ tám/xâu bit: OS2BSP và BS2OSP

Các nguyên thủy OS2BSP và BS2OSP dùng để chuyển đổi giữa các xâu bộ tám và các xâu bit được định nghĩa như sau:

- Hàm OS2BSP(x) lấy đầu vào là xâu bộ tám x, biểu diễn nó thành một xâu bit y và đầu ra xâu bit y. Thiết lập bit đầu tiên của xâu bit là bit có trọng số cao nhất (bên trái nhất) của bộ tám đầu tiên, bit thứ hai là bit

có trọng số cao nhất tiếp theo của bộ tám đầu tiên, tiếp tục như vậy, và cuối cùng thiết lập bit cuối cùng là bit có trọng số thấp nhất (bên phải nhất) của bộ tám cuối cùng.

- Hàm BS2OSP(y) lấy đầu vào một xâu bit *y* với độ dài xâu là bội của 8 và đầu ra là một xâu bộ tám *x* duy nhất sao cho *y* = OS2BSP(x).

7.2 Chuyển đổi xâu bit/số nguyên: *BS2IP* và *I2BSP*

Các nguyên thủy *BS2IP* và *I2BSP* dùng để chuyển đổi giữa các xâu bit và các số nguyên được định nghĩa như sau:

- Hàm $BS2IP(x)$ ánh xạ một xâu bit x tới một giá trị nguyên x', như sau:

Nếu $x = \langle x_{l-1}, \dots, x_0 \rangle$ trong đó $x_0, \dots . x_{l-1}$ là các bit, thì x' được xác định $x' = \sum_{0 \le i < l, x_i = 1} 2^i$.

- Hàm $I2BSP(m, l)$ lấy hai số nguyên không âm m và l làm đầu vào và đầu ra duy nhất là một xâu bit x có độ dài l, sao cho $BS2IP(x) = m$, nếu một xâu x như vậy tồn tại. Ngược lại hàm cho đầu ra là một thông điệp lỗi.

Độ dài theo bit của một số nguyên không âm m là số bit của m trong phép biểu diễn nhị phân, tức là $[log_2(m + 1)]$. Để cho tiện $Oct(m)$ được xác định là $Oct(m) = I2BSP(m, 8)$.

CHÚ THÍCH $I2BSP(m, l)$ thất bại khi và chỉ khi độ dài theo bit của m lớn hơn l.

7.3 Chuyển đổi xâu bộ tám/số nguyên: *OS2IP* và *I2OSP*

Các nguyên thủy *OS2IP* và *I2OSP* dùng để chuyển đổi giữa các xâu bộ tám và các số nguyên được định nghĩa như sau:

- Hàm $OS2IP(x)$ lấy xâu bộ tám x làm đầu vào và đưa ra số nguyên $BS2IP[OS2BSP(x)]$.

- Hàm $I2OSP(m, l)$ lấy hai số nguyên không âm m và l làm đầu vào và đưa ra đầu ra duy nhất là một xâu bộ tám x có độ dài l, sao cho $OS2IP(x) = m$, nếu tồn tại xâu x như vậy. Trong các trường hợp khác hàm sẽ trả về một thông điệp lỗi.

Độ dài theo bộ tám của một số nguyên không âm m là số các chữ số trong phép biểu diễn theo cơ số 256, tức là $[log_{256}(m + 1)]$.

CHÚ THÍCH 1 $I2OSP(m, l)$ thất bại khi và chỉ khi độ dài theo bộ tám của m là lớn hơn l.

CHÚ THÍCH 2 Một bộ tám x thường được viết theo dạng thập lục phân với độ dài 2; khi $OS2IP(x) < 16$, "0" biểu diễn cho xâu bit 0000. Ví dụ số nguyên 15 được viết là là 0f trong hệ thập lục phân.

CHÚ THÍCH 3 Độ dài theo bộ tám của một số nguyên không âm m được kí hiệu là $L(m)$.

7.4 Chuyển đổi phần tử trên trường hữu hạn/số nguyên: $FE2IP_F$

Nguyên thủy $FE2IP_F$ dùng để chuyển đổi các phần tử của F thành các giá trị nguyên được định nghĩa như sau:

- Hàm $FE2IP_F$ ánh xạ một phần tử $a \in F$ thành một giá trị nguyên a' như sau:

Nếu một phần tử *a* của *F* được đồng nhất với một bộ gồm m thành phần $(a_1 \dots a_m)$ trong đó lực lượng của F là $q = p^m$ và $a_i \in [0, p - 1]$ với $1 \le i \le m$ thì giá trị a' được định nghĩa là $a' = \sum_{1 \le i < m} a_i p^{i-1}$.

7.5 Chuyển đổi xâu bộ tám/phần tử của trường hữu hạn: $OS2FEP_F$ và $FE2OSP_F$

Các nguyên thủy $OS2FEP_F$ và $FE2OSP_F$ dùng để chuyển đổi giữa các xâu bộ tám và phần tử của trường hữu hạn đã xác định rõ ràng F được định nghĩa như sau:

- Hàm $OS2FEP_F(a)$ lấy một phần tử a của trường F làm đầu vào và cho đầu ra là xâu bộ tám $I2OSP(a', l)$ trong đó $a' = FE2IP_F(a)$ và $l = L(|F| - 1)$. Như vậy đầu ra của $FE2OSP_F(a)$ luôn là một xâu bộ tám có độ dài chính xác là $[log_{256}|F|]$.

CHÚ THÍCH 1 $L(x)$ biểu diễn độ dài theo bộ tám của số nguyên x hoặc xâu bộ tám x (số nguyên không âm)

- Hàm $OS2FEP_F(x)$ lấy xâu bộ tám x làm đầu vào và đưa ra đầu ra (duy nhất) là phần tử trường $a \in F$ sao cho $FE2OSP_F(a) = x$, nếu a như vậy tồn tại, nếu không sẽ trả lại kết quả lỗi.

CHÚ THÍCH $OS2FEP_F(x)$ lỗi khi và chỉ khi x không có độ dài chính xác bằng $[log_{256}|F|]$ hoặc $OS2IP(x) \geq |F|$.

7.6 Chuyển đổi điểm đường cong elliptic/xâu bộ tám: $EC2OSP_E$ và $OS2ECP_E$

7.6.1 Các điểm đường cong elliptic dạng nén

Cho E là một đường cong elliptic trên một trường hữu hạn đã cho F, trong đó F có đặc số p. Một điểm $P \neq O_E$ có thể được biểu diễn dưới *dạng nén*, *không nén* hoặc *lai ghép*. Nếu $P = (x, y)$ thì (x, y) là dạng *không nén* của P. Dạng nén của P là cặp $(x, \tilde{y})$, với $\tilde{y} \in \{0,1\}$ và được xác định như sau:

- Nếu $p \neq 2$ và $y = 0_F$ thì $\tilde{y} = 0$;

- Nếu $p \neq 2$ và $y \neq 0_F$ thì $\tilde{y} = [(y'/p^f) \bmod p] \bmod 2$, với $y' = FE2IPF_F(y)$ và f là số nguyên không âm lớn nhất sao cho $p^f | y'$;

CHÚ THÍCH 1 Nếu $p \neq 2$ và $y = (y_1, \ldots y_m) \neq 0_F$ thì việc này tương đương với việc lấy j là chỉ số nhỏ nhất với $y_j \neq 0$ và định nghĩa $\tilde{y} = y_j \bmod 2$.

- Nếu $p = 2$ và $x = 0_F$ thì $\tilde{y} = 0$;

- Nếu $p = 2$ và $x \neq 0_F$ thì $\tilde{y} = [z'/2^f] \bmod 2$ trong đó $z = y/x$, với $z' = FE2IP_F(z)$ và f là số nguyên không âm lớn nhất sao cho 2^f chia hết $FE2IP_F(1_F)$.

CHÚ THÍCH 2 Nếu $p = 2$ và $x \neq 0_F$ thì điều này tương đương với việc lấy $y/x = (z_1, \ldots z_m)$ và định nghĩa $\tilde{y} = z_1$.

Dạng lai ghép của $P = (x, y)$ là bộ ba $(x, \tilde{y}, y)$ với $\tilde{y}$ được định nghĩa như trong đoạn trước.

7.6.2 Các thuật toán giải nén điểm

Tồn tại các thủ tục hiệu quả để giải nén điểm, tức là tính toán y từ $(x,\tilde{y})$. Các thủ tục đó được mô tả tóm tắt như sau:

- Nếu $p \neq 2$, cho $(x, \tilde{y})$ là dạng nén của (x, y) trong đó điểm (x, y) thỏa mãn phương trình Weierstrass $y^2 = f(x)$ định nghĩa trong 6.1.1 hoặc 6.1.3. Nếu $f(x) = 0_F$ thì chỉ có duy nhất một lựa chọn cho y, chính là $y = 0_F$. Ngược lại, nếu $f(x) \neq 0_F$ thì có hai lựa chọn cho y, hai lựa chọn này chỉ khác nhau về dấu và việc chọn đúng được xác định bởi $\tilde{y}$. Có một số thuật toán đã biết để tính căn bậc hai trong trường hữu hạn, do vậy hai lựa chọn cho y là dễ dàng tính toán được.

- Nếu $p = 2$, cho $(x, \tilde{y})$ là dạng nén của (x, y) trong đó điểm (x, y) thỏa mãn phương trình Weierstrass $y^2 + xy = x^3 + ax^2 + b$. Nếu $x = 0_F$ thì phương trình là $y^2 = b$, từ đó y được xác định một cách duy

nhất và dễ dàng tính toán được. Ngược lại, nếu $x \neq 0_F$, khi đó đặt $z = y/x$ thì phương trình trở thành $z^2 + z = g(x)$ với $g(x) = x + a + bx^{-2}$. Gía trị của y được xác định duy nhất, và dễ dàng tính toán được từ các giá trị z và x, và do vậy ta chỉ cần tính toán z là đủ. Để tính z, với x cố định, nếu z là một nghiệm của phương trình $z^2 + z = g(x)$, thì có chính xác một nghiệm khác, cụ thể là $z + 1_F$. Việc tính toán hai giá trị có thể của z là khá dễ dàng, và việc lựa chọn giá trị z đúng đắn là đơn giản với việc sử dụng $\tilde{y}$.

7.6.3 Các hàm chuyển đổi

Gọi E là một đường cong elliptic trên một trường hữu hạn đã cho F.

Các nguyên thủy $EC2OSP_E$ và $OS2ECP_E$ dùng để chuyển đổi giữa các điểm trên đường cong E và các xâu bộ tám được định nghĩa như sau:

- Hàm $EC2OSP_E(P, fmt)$ nhận đầu vào là một điểm P trên E và một kiểu định dạng cụ thể fmt - một trong các giá trị tượng trưng cho kiểu *nén*, *không nén*, hoặc *lai ghép*. Đầu ra là một xâu bộ tám, EP được tính như sau:

  - Nếu $P = O_E$ thì $EP = Oct(0)$;

  - Nếu $P = (x, y) \neq O_E$ với dạng nén $(x, \tilde{y})$ thì $EP = H||X||y$, trong đó:

    - H là một bộ tám đơn có dạng $Oct[4U + C(2 + \tilde{y})]$, trong đó

    - U = 1 nếu fmt hoặc là dạng *không nén* hoặc *lai ghép* và ngược lại U = 0;

    - C = 1 nếu fmt hoặc là dạng *nén* hoặc dạng *lai ghép*, và ngược lại C = 0

    - X là xâu bộ tám $FE2OSP_F(x)$;

    - Y là xâu bộ tám $FE2OSP_F(y)$ nếu fmt hoặc ở dạng *không nén* hoặc dạng *lai ghép*, và ngược lại Y là xâu bộ tám rỗng.

- Hàm $OS2ECP_E(CP)$ nhận đầu vào là xâu bộ tám EP. Nếu tồn tại một điểm P trên đường cong E và một kiểu định dạng fmt, sao cho $EC2OSP_E(P, fmt) = EP$ thì cho đầu ra là P (ở dạng *không nén*), và ngược lại, hàm thất bại. Chú ý rằng điểm P, nếu tồn tại, được xác định duy nhất và do đó hàm $OS2ECP_E(CP)$ được định nghĩa tốt.

CHÚ THÍCH Nếu kiểu định dạng fmt là *không nén*, thì cả x và y được sử dụng; và giá trị $\tilde{y}$ không cần phải tính toán.

7.7 Chuyển đổi số nguyên/đường cong elliptic: $I2ECP$

Cho E là một đường cong elliptic trên trường hữu hạn đã biết F. Nguyên thủy $I2ECP$ dùng để chuyển đổi các số nguyên thành các điểm trên đường cong elliptic được định nghĩa như sau:

a) Hàm $I2ECP(x)$ lấy đầu vào là một số nguyên x.

b) Chuyển đổi số nguyên x thành một xâu bộ tám $X = I2OSP[x, L(|F| - 1)]$.

c) Nếu tồn tại một điểm P trên đường cong E sao cho $EC2OSP_E(P, nén) = 03 || X$, thì đầu ra của hàm là P, và ngược lại, hàm lỗi.

CHÚ THÍCH 1 Điểm P đầu ra, nếu tồn tại thì được xác định duy nhất.

CHÚ THÍCH 2 Hàm I2ECP sẽ thất bại với đầu vào x nếu không tồn tại một điểm P trên đường cong E sao cho $EC2OSP_E(P, nén) = 03 \,||\, X$

CHÚ THÍCH 3 Miền giá trị của $I2ECP$ là xấp xỉ một nửa của $E(F)$. Tức là, $I2ECP$ luôn đưa ra các điểm $P = (x, y)$ trên đường cong elliptic với dạng nén $(x, 1)$. Hàm này sẽ không đưa ra hoặc điểm tại vô hạn hoặc điểm trên đường cong elliptic $P = (x, y)$ với dạng nén $(x, 0)$.

CHÚ THÍCH 4 Một vài ứng dụng dựa trên đường cong elliptic có thể cần một hàm, mà ánh xạ các xâu bộ tám tới các điểm trên đường cong elliptic. Hàm $I2ECP$ được sử dụng như một thành phần cùng với $OS2IP$ hoặc một hàm băm.

8 Các tham số miền đường cong Elliptic và khóa công khai

8.1 Các tham số miền đường cong elliptic trên $F(q)$

Các tham số miền đường cong elliptic trên $F(q)$ [bao gồm cả các trường hợp đặc biệt $F(p)$ và $F(2^m)$] sẽ bao gồm các thành phần sau:

Nếu $m > 1$ thì nên có một thỏa thuận về việc lựa chọn cơ sở giữa các bên tham gia liên lạc.

- Kích thước trường $q = p^m$ xác định trường hữu hạn cơ sở $F(q)$, với p là một số nguyên tố và một chỉ dẫn rõ ràng về cơ sở được sử dụng để biểu diễn các phần tử của trường trong trường hợp m > 1;

- Nếu $q = p^m$ với $p > 3$, hai phần tử a và b của trường $F(q)$ định nghĩa phương trình đường cong elliptic E: $y^2 + xy = x^3 + ax^2 + b$;

- Nếu $q = 2^m$, hai phần tử a và b của trường $F(2^m)$ định nghĩa phương trình đường cong elliptic E: $y^2 + xy = x^3 + ax^2 + b$;

- Nếu $q = 3^m$, hai phần tử a và b trong $F(3^m)$ định nghĩa phương trình đường cong elliptic E: $y^2 = x^3 + ax^2 + b$;

- Hai phần tử x_G và y_G của trường $F(q)$ xác định một điểm G = (x_G, y_G) cócấp nguyên tố trên E;

- Cấp n của điểm G;

- Đồng hệ số $h = \#E(F(q))/n$ (khi được yêu cầu bởi lược đồ cơ sở).

CHÚ THÍCH Việc tính toán $\#E(F(q))$ được mô tả trong tài liệu viện dẫn [4].

8.2 Sinh khóa đường cong elliptic

Cho một tập các tham số miền đường cong elliptic hợp lệ, một khóa bí mật và một khóa công khai tương ứng có thể được tạo ra như sau:

a) Chọn một số nguyên d trong tập $[2, n - 2]$ một cách ngẫu nhiên hoặc giả ngẫu nhiên. Số nguyên d phải được bảo vệ khỏi việc tiết lộ trái phép và không thể đoán trước được.

b) Tính điểm $P = (x_P, y_P) = dG$.

c) Cặp khóa là (P, d), với P sẽ được sử dụng như khóa công khai và d là khóa bí mật.

Trong một số ứng dụng, khóa công khai có thể là eG, với $de \equiv 1 \bmod n$.

Phụ lục A
(tham khảo)
Thông tin cơ bản về các trường hữu hạn

A.1 Giới thiệu chung

Phụ lục A trình bày các kiến thức về trường hữu hạn cần thiết cho các lược đồ khóa công khai dựa trên đường cong elliptic.

A.2 Các xâu bit

Một bit hoặc là '0' hoặc là '1'. Một xâu bit x là một dãy hữu hạn $(x_{l-1}, \ldots, x_0)$ của các bit $x_0, \ldots, x_{l-1}$. Độ dài của một xâu bit x là số lượng bit, ký hiệu l, có trong xâu x. Với một số nguyên không âm n cho trước, $\{0,1\}^n$ ký hiệu tập các xâu bit có độ dài n. $\{0,1\}^* = \cup_{n \geq 0} \{0,1\}^n$ ký hiệu tập các xâu bit, bao gồm cả xâu rỗng (xâu có độ dài bằng 0).

A.3 Các xâu bộ tám

Một bộ tám là một xâu bit có độ dài bằng 8. Một xâu bộ tám là một dãy hữu hạn các bộ tám. Độ dài của xâu bộ tám là số lượng bộ tám trong xâu. $\{0,1\}^{8*}$ ký hiệu tập các xâu bộ tám, bao gồm cả xâu rỗng (xâu có độ dài bằng 0). Một bộ tám thường được viết dưới dạng thập lục phân, sử dụng miền giá trị giữa 00 và FF.

A.4 Đặc số của một trường hữu hạn $F(p^m)$

Đặc số của một trường là số nguyên dương nhỏ nhất c sao cho việc cộng c phần tử 1_F với nhau cho kết quả là phần tử 0. Nếu không tồn tại c như vậy thì đặc số của trường là 0. Với số nguyên tố p bất kỳ, đặc số của trường $F(p^m)$ là p.

A.5 Việc tính nghịch đảo các phần tử của một trường hữu hạn $F(p^m)$

Cho a là phần tử của $F(p^m)$. Khi đó tồn tại duy nhất một phần tử $b \in F(p^m)$ sao cho $a \cdot b = b \cdot a = 1_F$, và b được gọi là nghịch đảo theo phép nhân của a, ký hiệu là a^{-1}. Nếu $a = \gamma^i$, thì a^{-1} có thể được tính là $a^{-1} = \gamma^{q-1-i}$.

CHÚ THÍCH Nếu $m = 1$, a^{-1} được cho như là x trong phương trình $ax + by = 1$, và phương trình có thể được giải nhờ sử dụng thuật toán Euclid mở rộng.

A.6 Chính phương và không chính phương trong trường hữu hạn $F(p^m)$

Một phần tử $a \in F(p^m)$ được gọi là chính phương trong trường $F(p^m)$, nếu tồn tại một phần tử $b \in F(p^m)$ sao cho $a = b^2$. Việc xác định $a \in F(p^m)$ có phải là chính phương hay không có thể được thực hiện bằng cách sử dụng công thức (A.1):

a là chính phương trong trường $F(p^m) \Leftrightarrow a^{(q-1)/2} = 1_F$ (A.1)

A.7 Việc tính căn bậc hai trong trường $F(p^m)$

Có nhiều phương pháp khác nhau để tính căn bậc hai trong trường $F(p^m)$. Cho trước $a \in F(p^m)$, với a là chính phương, tìm $b \in F(p^m)$ sao cho $a = b^2$.

CHÚ THÍCH Nếu $q = 3 \pmod 4$, thì căn bậc hai có thể được tính là $b = a^{(q+1)/4}$. Trường hợp khác được mô tả trong các Tài liệu viện dẫn [4] và [5].

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

B.1 Giới thiệu chung

Phụ lục B trình bày kiến thức về các đường cong elliptic cần thiết cho lược đồ khóa công khai dựa trên đường cong elliptic.

B.2 Các tính chất của đường cong elliptic

Một đường cong elliptic E trên $F(q)$ được cung cấp một phép toán hai ngôi "+": $E \times E \rightarrow E$ mà gán hai điểm bất kỳ Q_1, Q_2 trên E vào một điểm thứ ba $Q_1 + Q_2$ trên E. Đường cong elliptic E là một nhóm abel đối với phép "+".

Số lượng các điểm của E (bao gồm O_E) được gọi là cấp (hoặc lực lượng) của E và được ký hiệu là $\#E(F(q))$. Cấp thỏa mãn định lý của Hasse sau đây:

$$q + 1 - 2\sqrt{q} \leq \#E(F(q)) \leq q + 1 + 2\sqrt{q}.$$

Số nguyên t xác định bởi $t = q + 1 - \#E(F(q))$ được gọi là *vết*. Định lý Hasse cho biết giới hạn của vết. B.6 giới thiệu các điều kiện đủ để với một giá trị t cho trước trong $[-2\sqrt{q}, 2\sqrt{q}]$, tồn tại một đường cong elliptic E trên $F(q)$ có vết t.

Đường cong bất quy tắc và siêu kỳ dị

Một đường cong elliptic E xác định trên $F(q)$ với vết t chia hết cho p được gọi là siêu kỳ dị. Một đường cong elliptic E xác định trên $F(q)$ với $\#E(F(q)) = q$ được gọi là bất quy tắc. Các đường cong siêu kỳ dị là đối tượng của các thuật toán của Frey-Rück [7] và Menezes-Okamoto-Vanstone [10]. Các hệ mật sử dụng đường cong bất quy tắc dễ bị tấn công khi sử dụng thuật toán Araki-Satoh [12], Semaev [13] và Smart [14].

B.3 Luật nhóm cho đường cong elliptic E trên $F(q)$ với $p > 3$

B.3.1 Tổng quan về tọa độ

Một đường cong elliptic thường được định nghĩa theo các tọa độ affine. Do đó, điểm cơ sở hay khóa công khai của người dùng được cho dưới dạng tọa độ affine. Hạn chế chính của tọa độ affine là sử dụng nhiều phép chia trong $F(q)$ cho cả phép cộng điểm và nhân đôi điểm. Trong hầu hết các cài đặt số học trường hữu hạn, phép chia trong trường là một phép tính rất "tốn kém" và trong những trường hợp như vậy, cần thận trọng để tránh sử dụng các phép chia càng nhiều càng tốt. Điều này có thể đạt được bằng cách sử dụng các tọa độ khác cho các điểm đường cong elliptic như tọa độ xạ ảnh, Jacobi và Jacobi sửa đổi. Tất cả các hệ tọa độ cho một đường cong elliptic đều tương thích.

B.3.2 Luật nhóm theo tọa độ affine

Cho $F(q)$ là một trường hữu hạn với $p > 3$. Gọi E là một đường cong elliptic trên $F(q)$ cho bởi "phương trình Weierstrass dạng rút gọn":

(Aff) $y^2 = x^3 + ax + b$ với $a, b \in F(q)$

trong đó bất đẳng thức $4a^3 + 27b^2 \neq 0_F$ là đúng trong $F(q)$.

LƯU Ý: Chính xác hơn, (Aff) được gọi là phương trình Weierstrass affine.

Trong tọa độ affine, luật nhóm trên đường cong elliptic cho bởi (Aff) như sau:

- Điểm tại vô hạn là phần tử trung hòa O_E đối với phép "+";

- Cho $R = (x, y)$ là một điểm trên E, sao cho $R \neq O_E$, thì $-R = (x, -y)$;

- Cho $R_1 = (x_1, y_1)$ và $R_2 = (x_2, y_2)$ là hai điểm khác nhau trên E, sao cho $R_1 \neq \pm R_2$ và $R_1, R_2 \neq O_E$; tổng là điểm $R_3 = (x_3, y_3)$ trong đó:

$x_3 = r^2 - x_1 - x_2$;

$y_3 = r(x_1 - x_3) - y_1$;

với $r = (y_2 - y_1)/(x_2 - x_1)$;

- Cho $R = (x, y)$ là một điểm trên E, sao cho $R \neq O_E$ và $y \neq 0_F$; phép nhân đôi điểm là một điểm $2R = (x_3, y_3)$, trong đó :

$x_3 = r^2 - 2x$;

$y_3 = r(x - x_3) - y$;

với $r = (3x^2 + a)/(2y)$.

Trong trường hợp $R = (x, 0_F)$, thì phép nhân đôi điểm là $2R = O_E$.

B.3.3 Luật nhóm theo tọa độ xạ ảnh

LƯU Ý 1: Sử dụng tọa độ xạ ảnh sẽ dẫn đến nhiều phép nhân hơn trong quá trình tính toán các luật nhóm nhưng không cần tính toán phép nghịch đảo. [6]

LƯU Ý 2: Khi sử dụng các hệ mật đường cong elliptic, thông thường một phép chuyển đổi sang tọa độ affine được thực hiện vào lúc kết thúc phép nhân vô hướng. Khi chuyển đổi tọa độ xạ ảnh thành affine, cần thực hiện 1 phép chia.

Không gian xạ ảnh hai chiều trên $F(q)$, $\Pi_{\text{proj}}(F(q))$ được cho bởi các lớp bộ ba tương đương $(X, Y, Z) \in F(q) \times F(q) \times F(q) \backslash \{(0_F, 0_F, 0_F)\}$, trong đó hai bộ ba $(X, Y, Z), (X', Y', Z') \in F(q) \times F(q) \times F(q) \backslash \{(0_F, 0_F, 0_F)\}$ được gọi là tương đương, nếu tồn tại $\lambda \in F(q)^*$, sao cho $(X', Y', Z') = (\lambda X, \lambda Y, \lambda Z)$. Phiên bản xạ ảnh của phương trình Weierstrass affine rút gọn (Aff) định nghĩa trên $\Pi_{\text{proj}}(F(q))$ và cho bởi phương trình bậc ba thuần nhất

(Proj) $Y^2 Z = X^3 + aXZ^2 + bZ^3$ với $a, b \in F(q)$.

LƯU Ý 3: Tập hợp tất cả các bộ ba tương đương với (X, Y, Z) được ký hiệu là $(X, Y, Z)/\sim$.

Đường cong elliptic được cho dưới dạng tọa độ xạ ảnh bao gồm tất cả các điểm $R = (X, Y, Z)$ của $F(q) \times F(q) \times F(q) \backslash \{(0_F, 0_F, 0_F)\}$, sao cho bộ ba (X, Y, Z) là một nghiệm của phương trình (Proj), trong đó ký hiệu (X, Y, Z) được sử dụng đồng nhất với lớp tương đương $(X, Y, Z)/\sim$ chứa (X, Y, Z). Tồn tại một mối liên hệ giữa các điểm Q của E khi đường cong được cho ở dạng tọa độ affine và các điểm R ở dạng tọa độ xạ ảnh. Thật vậy, các điều kiện sau là đúng:

- Nếu $Q = (X_Q, Y_Q)$ là một điểm affine của E, thì $R = (X_Q, Y_Q, 1_F)$ là điểm tương ứng theo tọa độ xạ ảnh;

- Nếu $R = (X, Y, Z)$ (với $Z \neq 0_F$) là một nghiệm của (Proj), thì $Q = (X/Z, Y/Z)$ là điểm affine tương ứng của E.

- Chỉ có duy nhất một nghiệm của (Proj) với $Z = 0_F$, cụ thể là điểm $(0_F, 1_F, 0_F)$; điểm này tương ứng với O_E.

Trong tọa độ xạ ảnh, luật nhóm trên một đường cong elliptic cho bởi (Proj) như sau:

- Điểm $(0_F, 1_F, 0_F)$ là phần tử trung hòa O_E đối với phép "+";

- Cho $R = (X, Y, Z) \neq (0_F, 1_F, 0_F)$ là một điểm trên E được cho ở dạng tọa độ xạ ảnh; thì $-R = (X, -Y, Z)$.

- Cho $R_1 = (X_1, Y_1, Z_1)$ và $R_2 = (X_2, Y_2, Z_2)$ là hai điểm khác nhau trên E, sao cho $R_1 \neq R_2$ và $R_1, R_2 \neq (0_F, 1_F, 0_F)$ và ký hiệu tổng là $R_3 = (X_3, Y_3, Z_3)$. Các tọa độ X_3, Y_3 và Z_3 có thể được tính bằng cách sử dụng công thức sau:

$X_3 = -su;$
$Y_3 = t(u + s^2 X_1 Z_2) - s^3 Y_1 Z_2;$
$Z_3 = s^3 Z_1 Z_2;$

với $s = X_2 Z_1 - X_1 Z_2, t = Y_2 Z_1 - Y_1 Z_2$, và $u = s^2(X_1 Z_2 + X_2 Z_1) - t^2 Z_1 Z_2$.

- Cho $R = (X, Y, Z) \neq (0_F, 1_F, 0_F)$ là một điểm trên E và ký hiệu phép nhân đôi điểm là $2R = (X_3, Y_3, Z_3)$. Các tọa độ X_3, Y_3 và Z_3 có thể được tính bằng cách sử dụng công thức sau:

$X_3 = -su;$
$Y_3 = t(u + s^2 X) - s^3 Y;$
$Z_3 = s^3 Z;$

với $t = 3X^2 + aZ^2, s = 2YZ$ và $u = 2s^2 X - t^2 Z$.

B.3.4 Luật nhóm theo tọa độ Jacobi

LƯU Ý 1: Sử dụng tọa độ Jacobi sẽ dẫn đến nhiều phép nhân hơn trong quá trình tính toán nhưng không cần tính toán phép nghịch đảo. [6]

Không gian hai chiều trên $F(q)$, $\Pi_{\text{jac}}(F(q))$ được cho bởi các lớp bộ ba tương đương $(X, Y, Z) \in F(q) \times F(q) \times F(q) \backslash \{(0_F, 0_F, 0_F)\}$, trong đó hai bộ ba $(X, Y, Z), (X', Y', Z') \in F(q) \times F(q) \times F(q) \backslash \{(0_F, 0_F, 0_F)\}$ được gọi là tương đương, nếu tồn tại $\lambda \in F(q)^*$, sao cho $(X', Y', Z') = (\lambda^2 X, \lambda^3 Y, \lambda Z)$. Phiên bản Jacobi của phương trình Weierstrass affine rút gọn (Aff) định nghĩa trên $\Pi_{\text{jac}}(F(q))$ và được cho bởi phương trình bậc ba.

(Jac) $Y^2 = X^3 + aXZ^4 + bZ^6$ với $a, b \in F(q)$.

LƯU Ý 2: Tập hợp tất cả các bộ ba tương đương với (X, Y, Z) được ký hiệu là $(X, Y, Z)/\sim$.

Đường cong elliptic được cho ở dạng tọa độ Jacobi bao gồm tất cả các điểm $R = (X, Y, Z)$ của $F(q) \times F(q) \times F(q) \backslash \{(0_F, 0_F, 0_F)\}$, sao cho bộ ba (X, Y, Z) là một nghiệm của phương trình (Jac), trong đó ký hiệu (X, Y, Z) được sử dụng đồng nhất với lớp tương đương $(X, Y, Z)/\sim$ chứa (X, Y, Z). Tồn tại một mối liên hệ giữa các điểm Q của E khi đường cong được cho ở dạng tọa độ affine và các điểm R của dạng tọa độ Jacobi. Thật vậy, các điều kiện sau đây là đúng:

- Nếu $Q = (X_Q, Y_Q)$ là một điểm affine của E, thì $R = (X_Q, Y_Q, 1_F)$ là điểm tương ứng dạng tọa độ Jacobi;

- Nếu $R = (X, Y, Z)$ (với $Z \neq 0_F$) là một nghiệm của (Jac), thì $Q = (X/Z^2, Y/Z^3)$ là điểm affine tương ứng của E.

- Chỉ có duy nhất một nghiệm của (Jac) với $Z = 0_F$, cụ thể là điểm $(1_F, 1_F, 0_F)$; điểm này tương ứng với O_E.

Trong tọa độ Jacobi, luật nhóm trên một đường cong elliptic cho bởi (Jac) như sau:

- Điểm $(1_F, 1_F, 0_F)$ là phần tử trung hòa O_E đối với phép "+";

- Cho $R = (X, Y, Z) \neq (1_F, 1_F, 0_F)$ là một điểm trên E được cho ở dạng tọa độ Jacobi; thì $-R = (X, -Y, Z)$.

- Cho $R_1 = (X_1, Y_1, Z_1)$ và $R_2 = (X_2, Y_2, Z_2)$ là hai điểm khác nhau trên E, sao cho $R_1 \neq R_2$ và $R_1, R_2 \neq (1_F, 1_F, 0_F)$ và ký hiệu tổng là $R_3 = (X_3, Y_3, Z_3)$. Các tọa độ X_3, Y_3 và Z_3 có thể được tính bằng cách sử dụng công thức sau:

$X_3 = -h^3 - 2u_1h^2 + r^2;$
$Y_3 = -s_1h^3 + r(u_1h^2 - X_3);$
$Z_3 = Z_1Z_2h;$

với $u_1 = X_1Z_2^2, u_2 = X_2Z_1^2, s_1 = Y_1Z_2^3, s_2 = Y_2Z_1^3, h = u_2 - u_1$, và $r = s_2 - s_1$.

- Cho $R = (X, Y, Z) \neq (1_F, 1_F, 0_F)$ là một điểm trên E và ký hiệu phép nhân đôi điểm là $2R = (X_3, Y_3, Z_3)$. Các tọa độ X_3, Y_3 và Z_3 có thể được tính bằng cách sử dụng công thức sau:

$X_3 = t;$
$Y_3 = -8Y^4 + m(s - t);$
$Z_3 = 2YZ;$

với $s = 4XY^2, m = 3X^2 + aZ^4$ và $t = -2s + m^2$.

B.3.5 Luật nhóm theo tọa độ Jacobi sửa đổi

Cùng với phương trình bậc ba (Jac), luật nhóm trong Jacobi sửa đổi được cho bằng cách biểu diễn các tọa độ Jacobi như một bộ bốn (X, Y, Z, aZ^4), dạng biểu diễn mà cho phép thực hiện phép nhân đôi điểm nhanh nhất có thể trên $E(F(q))$.

Trong tọa độ Jacobi sửa đổi, luật nhóm trên một đường cong elliptic cho bởi (Jac) như sau :

- Cho $R_1 = (X_1, Y_1, Z_1, aZ_1^4)$ và $R_2 = (X_2, Y_2, Z_2, aZ_2^4)$ là hai điểm khác nhau trên E sao cho $R_1 \neq R_2$ và $R_1, R_2 \neq (1_F, 1_F, 0_F, 0_F)$ và ký hiệu tổng là $R_3 = (X_3, Y_3, Z_3, aZ_3^4)$. Các tọa độ X_3, Y_3 và Z_3 có thể được tính bằng cách sử dụng công thức sau:

$X_3 = -h^3 - 2u_1h^2 + r^2;$
$Y_3 = -s_1h^3 + r(u_1h^2 - X_3);$
$Z_3 = Z_1Z_2h;$
$aZ_3^4 = aZ_3^4;$

với $u_1 = X_1Z_2^2, u_2 = X_2Z_1^2, s_1 = Y_1Z_2^3, s_2 = Y_2Z_1^3, h = u_2 - u_1$, và $r = s_2 - s_1$.

- Cho $R = (X, Y, Z, aZ^4) \neq (1_F, 1_F, 0_F, 0_F)$ là một điểm trên E và ký hiệu phép nhân đôi điểm bằng $2R = (X_3, Y_3, Z_3, aZ_3^4)$. Các tọa độ X_3, Y_3 và Z_3 có thể được tính bằng cách sử dụng công thức sau:

$X_3 = t;$

$Y_3 = m(s - t) - u;$
$Z_3 = 2YZ;$
$aZ_3^4 = 2u(aZ^4);$

với $s = 4XY^2, u = 8Y^4, m = 3X^2 + (aZ^4)$, và $t = -2s + m^2$.

B.3.6 Tọa độ hỗn hợp

Có những ưu điểm và nhược điểm về mặt tính toán khi biểu diễn một điểm trên đường cong elliptic theo tọa độ affine, xạ ảnh, Jacobi và Jacobi sửa đổi trong tài liệu tham khảo [6]. Không có hệ tọa độ nào cung cấp cả phép cộng điểm nhanh và phép nhân đôi điểm nhanh. Có thể kết hợp các tọa độ khác nhau, tức là cộng hai điểm trong đó một điểm được biểu diễn ở một hệ tọa độ nào đó và điểm còn lại biểu diễn trong hệ tọa độ khác. Hệ tọa độ của kết quả có thể được chọn một trong số hệ tọa độ. Vì có bốn loại hệ tọa độ khác nhau, nên sẽ cung cấp một số lượng lớn khả năng. Các tọa độ hỗn hợp cho sự kết hợp tốt nhất của các hệ tọa độ đối với phép nhân điểm hoặc phép cộng điểm nhằm giảm thiểu thời gian của phép lũy thừa trên đường cong elliptic. Các tọa độ hỗn hợp chạy hiệu quả nhất trong thuật toán tiền tính toán mô tả trong C.3.2.

B.4 Luật nhóm cho các đường cong elliptic trên $F(2^m)$

B.4.1 Luật nhóm theo tọa độ affine

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

(Aff) $y^2 + xy = x^3 + ax^2 + b$

với $a, b \in F(2^m)$, sao cho $b \neq 0_F$.

Trong tọa độ affine, luật nhóm trên một đường cong elliptic cho bởi (Aff) xác định như sau:

- Điểm tại vô hạn là phần tử trung hòa O_E đối với phép "+";

- Cho $R = (x, y) \neq 0_E$ là một điểm trên E được cho dưới dạng ký hiệu affine. Khi đó $-R = (x, x + y)$.

- Cho $R_1 = (x_1, y_1)$ và $R_2 = (x_2, y_2)$ là hai điểm khác nhau trên E, sao cho $R_1 \neq \pm R_2$ và $R_1, R_2 \neq O_E$. Tổng là điểm $R_3 = (x_3, y_3)$, trong đó:

$x_3 = r^2 + r + x_1 + x_2 + a;$
$y_3 = r(x_1 + x_3) + x_3 + y_1;$

với $r = (y_2 + y_1)/(x_2 + x_1)$.

- Cho $R = (x, y)$ là một điểm trên E, sao cho $R \neq O_E$ và $x \neq 0_F$. Phép nhân đôi chính nó là điểm $2R = (x_3, y_3)$, trong đó:

$x_3 = r^2 + r + a;$
$y_3 = r(x + x_3) + x_3 + y;$
với $r = x + (y/x)$. Trong trường hợp $R = (0_F, y)$, phép nhân đôi điểm là $2R = O_E$.

Như với luật nhóm trong mô tả affine của một đường cong elliptic trên $F(p^m)$, luật nhóm được đưa ra ở trên sử dụng nhiều phép chia trong $F(2^m)$, khi tính toán phép nhân vô hướng. Tuy nhiên, mô tả xạ ảnh

của luật nhóm đường cong elliptic có thể được sử dụng, và với mô tả này ta chỉ sử dụng duy nhất một phép chia ở cuối phép nhân vô hướng. Cả hai mô tả của đường cong elliptic đều tương thích.

B.4.2 Luật nhóm theo tọa độ xạ ảnh

LƯU Ý 1: Sử dụng tọa độ xạ ảnh sẽ dẫn đến nhiều phép nhân hơn trong quá trình tính toán nhưng không cần tính toán phép nghịch đảo.

Không gian xạ ảnh hai chiều trên $F(2^m), \Pi_{\text{proj}}(F(2^m))$, cho bởi các lớp tương đương của các bộ ba $(X,Y,Z) \in F(2^m) \times F(2^m) \times F(2^m) \backslash \{(0_F, 0_F, 0_F)\}$, trong đó hai bộ ba $(X,Y,Z), (X',Y',Z') \in F(2^m) \times F(2^m) \times F(2^m) \backslash \{(0_F, 0_F, 0_F)\}$ được gọi là tương đương nếu tồn tại $\lambda \in F(2^m)^*$, sao cho $(X',Y',Z') = (\lambda X, \lambda Y, \lambda Z)$. Phiên bản xạ ảnh của phương trình affine (Aff) được xác định trên $\Pi_{\text{proj}}(F(2^m))$, và cho bởi phương trình bậc ba thuần nhất

(Proj) $Y^2Z + XYZ = X^3 + aX^2Z + bZ^3$ với $a, b \in F(2^m)$

LƯU Ý 2: Tập hợp tất cả các bộ ba tương đương với (X,Y,Z) được ký hiệu là $(X,Y,Z)/\sim$.

Đường cong elliptic được cho trong tọa độ xạ ảnh bao gồm tất cả các điểm $R = (X,Y,Z)$ của $F(2^m) \times F(2^m) \times F(2^m) \backslash \{(0_F, 0_F, 0_F)\}$ sao cho bộ ba (X,Y,Z) là một nghiệm của phương trình (Proj), trong đó ký hiệu (X,Y,Z) được sử dụng đồng nhất với lớp tương đương $(X,Y,Z)/\sim$ chứa (X,Y,Z). Rõ ràng tồn tại quan hệ 1:1 giữa các điểm Q của E khi đường cong được cho ở dạng tọa độ affine và các điểm R được cho ở dạng tọa độ xạ ảnh. Thật vậy, các điều kiện sau đây được thỏa mãn:

- Nếu $Q = (x_Q, y_Q)$ là một điểm affine của E, thì $R = (X_Q, Y_Q, 1_F)$ là điểm tương ứng theo tọa độ xạ ảnh;

- Nếu $R = (X,Y,Z)$ (với $Z \neq 0_F$) là một nghiệm của (Proj), thì $Q = (X/Z, Y/Z)$ là điểm affine tương ứng của E.

- Chỉ có duy nhất một nghiệm của (Proj) với $Z = 0_F$, cụ thể là điểm $(0_F, 1_F, 0_F)$; điểm này tương ứng với O_E.

Trong tọa độ xạ ảnh, luật nhóm trên một đường cong elliptic cho bởi (Proj) định nghĩa như sau:

- Điểm $(0_F, 1_F, 0_F)$ là phần tử trung hòa O_E đối với phép "+";

- Với $R = (X,Y,Z) \neq (0_F, 1_F, 0_F)$ là một điểm trên E đã cho ở dạng tọa độ xạ ảnh; thì $-R = (X, X+Y, Z)$.

- Cho $R_1 = (X_1, Y_1, Z_1)$ và $R_2 = (X_2, Y_2, Z_2)$ là hai điểm khác nhau trên E, sao cho $R_1 \neq R_2$ và $R_1, R_2 \neq (0_F, 1_F, 0_F)$ và ký hiệu tổng là $R_3 = (X_3, Y_3, Z_3)$. Các tọa độ X_3, Y_3 và Z_3 có thể được tính bằng cách sử dụng công thức sau:

$X_3 = su;$
$Y_3 = t(u + s^2X_1Z_2) + s^3Y_1Z_2 + su;$
$Z_3 = s^3Z_1Z_2;$

với $s = X_2Z_1 + X_1Z_2, t = Y_2Z_1 + Y_1Z_2$, và $u = (t^2 + ts + as^2)Z_1Z_2 + s^3$.

- Cho $R = (X,Y,Z) \neq (0_F, 1_F, 0_F)$ là một điểm trên E và ký hiệu phép nhân đôi điểm của nó là $2R = (X_3, Y_3, Z_3)$. Các tọa độ X_3, Y_3 và Z_3 có thể được tính bằng cách sử dụng công thức sau:

$X_3 = st;$
$Y_3 = X^4s + t(s + YZ + X^2);$

$Z_3 = s^3$;

với $s = XZ$ và $t = bZ^4 + X^4$.

B.5 Luật nhóm cho các đường cong elliptic trên $F(3^m)$

B.5.1 Luật nhóm theo tọa độ affine

Cho $F(3^m)$, với số $m \geq 1$ nào đó, là một trường hữu hạn. Gọi E là một đường cong elliptic trên $F(3^m)$ cho bởi công thức (B.2):

$$(Aff)\ y^2 = x^3 + ax^2 + b \qquad \text{(B.2)}$$

với $a, b \in F(3^m)$, sao cho $a, b \neq 0_F$.

Trong tọa độ affine, luật nhóm trên một đường cong elliptic cho bởi (Aff) định nghĩa như sau:

- Điểm tại vô hạn là phần tử trung hòa O_E đối với phép "+";

- Cho $R = (x, y) \neq 0_E$ là một điểm trên E được cho ở dạng ký hiệu affine. Khi đó $-R = (x, -y)$.

- Cho $R_1 = (x_1, y_1)$ và $R_2 = (x_2, y_2)$ là hai điểm khác nhau trên E, sao cho $R_1 \neq \pm R_2$ và $R_1, R_2 \neq O_E$. Tổng là điểm $R_3 = (x_3, y_3)$, trong đó:

$x_3 = r^2 - a - x_1 - x_2$;
$y_3 = r(x_1 - x_3) - y_1$;

với $r = (y_2 - y_1)/(x_2 - x_1)$.

- Cho $R = (x, y)$ là một điểm trên E, sao cho $R \neq O_E$ và $x \neq 0_F$. Phép nhân đôi điểm của nó là điểm $2R = (x_3, y_3)$, trong đó:

$x_3 = r^2 - a + x$;
$y_3 = r(x - x_3) - y$;
với $r = ax/y$.

Trong trường hợp $R = (x, 0_F)$, phép nhân đôi điểm của nó là $2R = O_E$.

Như với luật nhóm trong mô tả affine của một đường cong elliptic trên $F(p^m)$, luật nhóm được đưa ra ở trên sử dụng nhiều phép chia trong $F(3^m)$, khi tính toán phép nhân vô hướng. Tuy nhiên, mô tả xạ ảnh của luật nhóm đường cong elliptic có thể được sử dụng, và mô tả này chỉ sử dụng duy nhất một phép chia ở cuối phép nhân vô hướng. Cả hai mô tả của đường cong elliptic đều tương thích.

B.5.2 Luật nhóm theo tọa độ xạ ảnh

LƯU Ý 1: Sử dụng tọa độ xạ ảnh sẽ dẫn đến nhiều phép nhân hơn trong quá trình tính toán nhưng không cần tính toán phép nghịch đảo.

Không gian xạ ảnh hai chiều trên $F(3^m), \Pi_{\text{proj}}(F(3^m))$, cho bởi các lớp tương đương của các bộ ba $(X, Y, Z) \in F(3^m) \times F(3^m) \times F(3^m) \backslash \{(0_F, 0_F, 0_F)\}$, trong đó hai bộ ba $(X, Y, Z), (X', Y', Z') \in F(3^m) \times F(3^m) \times F(3^m) \backslash \{(0_F, 0_F, 0_F)\}$ được gọi là tương đương nếu tồn tại $\lambda \in F(3^m)^*$, sao cho $(X', Y', Z') = (\lambda X, \lambda Y, \lambda Z)$. Phiên bản xạ ảnh của phương trình affine (Aff) định nghĩa trên $\Pi_{\text{proj}}(F(3^m))$, và được cho bởi phương trình bậc ba thuần nhất

(Proj) $Y^2Z = X^3 + aX^2Z + bZ^3$ với $a, b \in F(3^m)$

LƯU Ý 2: Tập hợp tất cả các bộ ba tương đương với (X, Y, Z) được ký hiệu là $(X, Y, Z)/\sim$.

Đường cong elliptic cho trong tọa độ xạ ảnh bao gồm tất cả các điểm $R = (X, Y, Z)$ của $F(3^m) \times F(3^m) \times F(3^m) \backslash \{(0_F, 0_F, 0_F)\}$ sao cho bộ ba (X, Y, Z) là một nghiệm của phương trình (Proj), trong đó ký hiệu (X, Y, Z) được sử dụng đồng nhất với lớp tương đương $(X, Y, Z)/\sim$ chứa (X, Y, Z). Rõ ràng tồn tại quan hệ 1:1 giữa các điểm Q của E khi đường cong được cho ở dạng tọa độ affine và các điểm R được cho ở dạng tọa độ xạ ảnh. Thật vậy, các điều kiện sau đây được thỏa mãn:

- Nếu $Q = (x_Q, y_Q)$ là một điểm affine của E, thì $R = (X_Q, Y_Q, 1_F)$ là điểm tương ứng theo tọa độ xạ ảnh;

- Nếu $R = (X, Y, Z)$ (với $Z \neq 0_F$) là một nghiệm của (Proj), thì $Q = (X/Z, Y/Z)$ là điểm affine tương ứng của E.

- Chỉ có duy nhất một nghiệm của (Proj) với $Z = 0_F$, cụ thể là điểm $(0_F, 1_F, 0_F)$; điểm này tương ứng với O_E.

Trong tọa độ xạ ảnh, luật nhóm trên một đường cong elliptic cho bởi (Proj) như sau:

- Điểm $(0_F, 1_F, 0_F)$ là phần tử trung hòa O_E đối với phép "+";

- Cho $R = (X, Y, Z) \neq (0_F, 1_F, 0_F)$ là một điểm trên E cho trước ở dạng tọa độ xạ ảnh; khi đó $-R = (X, -Y, Z)$.

- Cho $R_1 = (X_1, Y_1, Z_1)$ và $R_2 = (X_2, Y_2, Z_2)$ là hai điểm khác nhau trên E, sao cho $R_1 \neq \pm R_2$ và $R_1, R_2 \neq (0_F, 1_F, 0_F)$ và ký hiệu tổng là $R_3 = (X_3, Y_3, Z_3)$. Các tọa độ X_3, Y_3 và Z_3 có thể được tính bằng cách sử dụng công thức sau:

$$X_3 = st^2Z_1Z_2 - s^3u;$$
$$Y_3 = t(s^2X_1Z_2 - t^2Z_1Z_2 + s^2u) - s^3Y_1Z_2;$$
$$Z_3 = s^3Z_1Z_2;$$

với $s = X_2Z_1 - X_1Z_2, t = Y_2Z_1 - Y_1Z_2$, và $u = aZ_1Z_2 + X_1Z_2 + X_2Z_1$.

- Cho $R = (X, Y, Z) \neq (0_F, 1_F, 0_F)$ là một điểm trên E và ký hiệu phép nhân đôi điểm của nó là $2R = (X_3, Y_3, Z_3)$. Các tọa độ X_3, Y_3 và Z_3 có thể được tính bằng cách sử dụng công thức sau:

$$X_3 = tY;$$
$$Y_3 = s(XY^2 - t) - Y^4;$$
$$Z_3 = Y^3Z;$$

với $s = aX$ và $t = s^2Z - aY^2Z + XY^2$.

B.6 Điều kiện tồn tại cho đường cong elliptic E

B.6.1 Cấp của một đường cong elliptic E xác định trên $F(p)$

Vết của E trên $F(p)$ được giới hạn trong $[-2\sqrt{p}, 2\sqrt{p}]$ theo định lý Hasse. Định lý Waterhouse [16] khẳng định rằng, cho trước t thuộc $[-2\sqrt{p}, 2\sqrt{p}]$, tồn tại một đường cong elliptic E trên $F(p)$ với vết t.

"Mỗi số nguyên n trong đoạn đã cho bởi định lý Hasse là cấp của một đường cong elliptic nào đó định nghĩa trên $F(p)$[16]

B.6.2 Cấp của một đường cong elliptic E định nghĩa trên $F(2^m)$

Vết của E trên $F(2^m)$ được giới hạn trong $[-2\sqrt{2^m}, 2\sqrt{2^m}]$ bởi định lý Hasse. Các điều kiện để với một giá trị t cho trước trong $[-2\sqrt{2^m}, 2\sqrt{2^m}]$, tồn tại một đường cong elliptic E trên $F(2^m)$ với vết t được cho bởi định lý Waterhouse:

Cho t là một số nguyên trong đó $|t| \leq 2\sqrt{2^m}$. Khi đó tồn tại một đường cong elliptic xác định trên $F(2^m)$ có cấp $2^m + 1 - t$ nếu và chỉ nếu một trong các điều kiện sau được thỏa mãn:

- t là số lẻ;

- $t = 0$;

- m là số lẻ và $t^2 = 2^{m+1}$;

- m là số chẵn và $t^2 = 2^{m+2}$ hoặc $t^2 = 2^m$.

B.6.3 Cấp của một đường cong elliptic E định nghĩa trên $F(p^m)$ với $p \geq 3$

Vết của E trên $F(p^m)$ được giới hạn trong $[-2\sqrt{p^m}, 2\sqrt{p^m}]$ bởi định lý Hasse. Các điều kiện để với một giá trị t cho trước trong đoạn $[-2\sqrt{p^m}, 2\sqrt{p^m}]$, tồn tại một đường cong elliptic E trên $F(p^m)$ với vết t được cho bởi định lý Waterhouse:

Cho t là một số nguyên trong đó $|t| \leq 2\sqrt{p^m}$. Khi đó tồn tại một đường cong elliptic xác định trên $F(p^m)$ có cấp $p^m + 1 - t$ khi và chỉ khi một trong các điều kiện sau được thỏa mãn:

- t không chia hết cho p;

- m là số lẻ và thỏa mãn một trong các điều kiện sau:

  - $t = 0$;

  - $t^2 = 3^{m+1}$ và $p = 3$;

- m là số chẵn và thỏa mãn một trong các điều kiện sau:

  - $t^2 = 4p^m$;

  - $t^2 = p^m$ và $p - 1$ không chia hết cho 3;

  - $t = 0$ và $p - 1$ không chia hết cho 4;

B.7 Các phép ghép cặp

B.7.1 Tổng quan về các phép ghép cặp

Cho E là một đường cong elliptic trên $F(q)$ trong đó $q = p^m$, và cho n là số nguyên tố cùng nhau với đặc số p của $F(q)$. Nhóm n-xoắn được sinh bởi hai điểm khi n nguyên tố cùng nhau với p. $E(F(q))$ bao gồm một điểm n-xoắn G_1 vì theo định nghĩa n là một ước số nguyên tố của $\#E(F(q))$ (xem mục 4). Lưu ý rằng khẳng định này không kéo theo $E(F(q)) \supset E[n]$. Các phép ghép cặp Weil và Tate là các ánh xạ song tuyến tính, không suy biến được định nghĩa từ một đường cong elliptic E đến μ_n. Phép ghép cặp Weil được xác định trong nhóm n-xoắn $E[n]$, do đó yêu cầu $E(F(q^B))$ thỏa mãn $E(F(q^B)) \supset E[n]$. Mặt khác, phép ghép cặp Tate có thể định nghĩa chỉ khi $E(F(q^B)) \ni G_1$ và $F(q^B) \supset \mu_n$. Do đó, việc tính toán phép ghép cặp Tate hiệu quả hơn so với phép ghép cặp Weil.

B.7.2 Định nghĩa về các phép ghép cặp Weil và Tate

Cho $\frac{E}{F}$ là một đường cong elliptic, n là một ước số nguyên tố của $\#E(F(q))$ và $E[n]$ là nhóm n-xoắn, trong đó n nguyên tố cùng nhau với q. Khi đó $E[n]$ chứa hai điểm G_1 và G_2 sao cho $E[n] = < G_1 > \mathrm{x} < G_2 >$

Gọi B là số nguyên nhỏ nhất sao cho $q^B - 1$ chia hết cho n. Khi đó $E[n] \subseteq E[F(q^B)]$.

Phép ghép cặp Weil là

$$e_n: E[n] \times E[n] \to \mu_n,$$

và phép ghép cặp Tate là

$$E\big(F(q^B)\big)[n] \times E(F(q^B))/nE(F(q^B)) \to \mu_n.$$

LƯU Ý: Thông tin chi tiết về phép ghép cặp Weil và Tate được mô tả trong tài liệu tham khảo [15].

B.7.3 Ánh xạ song tuyến tính mật mã

Một ánh xạ song tuyến tính mật mã e_n được thực hiện bằng cách hạn chế miền xác định của phép ghép cặp Weil hoặc Tate, đáp ứng các điều kiện không suy biến, song tuyến tính và có thể tính toán được. Trong các ứng dụng mật mã, ánh xạ song tuyến tính mật mã e_n được mô tả theo hai cách:

- $e_n: < G_1 > \times < G_2 > \to \mu_n$;
- $e_n: < G_1 > \times < G_1 > \to \mu_n$;

trong đó $< G_1 >$ và $< G_2 >$ là các nhóm cyclic cấp n và μ_n là nhóm cyclic có căn bậc n của phần tử đơn vị.

Phụ lục C
(tham khảo)
Thông tin cơ bản về các hệ mật trên đường cong elliptic

C.1 Giới thiệu chung

Phụ lục C giới thiệu một số thuật toán đối với các hệ mật trên đường cong elliptic cần thiết để có lược đồ khóa công khai dựa trên đường cong elliptic an toàn được mô tả trong TCVN 12852-5.

C.2 Định nghĩa các bài toán mật mã

C.2.1 Bài toán lôgarit rời rạc trên đường cong elliptic (ECDLP)

Cho 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 logarit rời rạc trên đường cong elliptic (đối với điểm cơ sở G) là tìm số nguyên $x \in [0, n-1]$ sao cho $P = xG$ nếu tồn tại giá trị x như vậy.

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

C.2.2 Bài toán Diffie-Hellman tính toán trên đường cong elliptic (ECDHP)

Cho 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 vào độ khó được tin tưởng của bài toán Diffie-Hellman tính toán trên đường cong elliptic.

C.2.3 Bài toán Diffie-Hellman quyết định trên đường cong elliptic (ECDDHP)

Cho 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 vào độ khó được tin tưởng của bài toán Diffie-Hellman quyết định trên đường cong elliptic.

C.2.4 Bài toán Diffie-Hellman song tuyến tính (BDH)

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 $e_n(G_1, G_1)^{abc}$.

C.2.5 Bài toán Gap Diffie-Hellman (GDH)

Bài toán Gap Diffie-Hellman là bài toán Diffie-Hellman tính toán được cho quyền truy cập vào một bộ tiên tri có thể giải bài toán Diffie-Hellman quyết định.

C.3 Các thuật toán xác định logarit rời rạc trên đường cong elliptic

C.3.1 Độ khó của ECDLP

Độ khó của ECDLP phụ thuộc vào đường cong elliptic $E/F(q)$ được chọn và độ lớn n của cấp điểm cơ sở G. C.3.1 trình bày tổng quan về các thuật toán giải ECDLP. Đường cong elliptic $E/F(q)$ phải được chọn sao cho đáp ứng các mục tiêu an toàn đã xác định nhằm chống lại các thuật toán sau đây để giải ECDLP. Độ lớn của n phải được thiết lập sao cho đáp ứng các mục tiêu an toàn đã xác định chống lại thuật toán bước nhỏ - bước lớn và các biến thể khác của thuật toán ρ của Pollard.

C.3.2 Tổng quan về các thuật toán

Các kỹ thuật sau đây cho phép tính logarit 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 xác định 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 (song song).
- Thuật toán của Frey-Rück [7] và thuật toán Menezes-Okamoto-Vanstone [10] 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 trên trường mở rộng nhỏ nhất $F(q^B)$ của $F(q)$ sao cho n chia hết $(q^B - 1)$. Thuật toán Frey-Rück chạy dưới các điều kiện yếu hơn so với thuật toán Menezes-Okamoto-Vanstone.
- Thuật toán của Araki-Satoh [12], Smart [13] và Semaev [14] giải bài toán lôgarit 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 logarit rời rạc trong nhóm nhân của một trường hữu hạn nào đó, không tồn tại thuật toán "tính toán chỉ số" mà có thể hoạt động được đối với trường hợp đường cong elliptic.

LƯU Ý 1: Các thuật toán Pohlig-Silver-Hellman và bước nhỏ - bước lớn hoạt động được 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 tính chất đặc biệt.

LƯU Ý 2: Độ an toàn của điểm G có độ lớn cấp n-bit chống lại thuật toán bước nhỏ - bước lớn và nhiều biến thể khác của thuật toán ρ của Pollard tương ứng với $2^{n/2}$.

C.3.3 Điều kiện MOV

Cho n như trong định nghĩa của tập hợp các tham số miền đường cong elliptic, trong đó n là một ước số nguyên tố của $\#E[F(q)]$. Một giá trị B đã cho là số nguyên nhỏ nhất sao cho n chia hết $p^B - 1$. Như lưu ý ở phần trên, các thuật toán Frey-Rück và Menezes-Okamoto-Vanstone biến đổi đưa bài toán lôgarit rời rạc trên một đường cong elliptic trên $F(q)$ về bài toán lôgarit rời rạc trong trường hữu hạn $F(p^B)$. Qua việc sử dụng tấn công, độ khó của bài toán lôgarit rời rạc trên một đường cong elliptic $E/F(q)$ được liên hệ với bài toán lôgarit rời rạc trên một trường hữu hạn $F(p^B)$. *Điều kiện MOV* mô tả bậc B đảm bảo cho độ an toàn của bài toán lôgarit rời rạc trên đường cong elliptic tương đương với 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 bằng 6 thường là thích hợp hơn cả.

C.4 Các thuật toán nhân vô hướng các điểm trên đường cong elliptic

C.4.1 Thuật toán cơ bản

Việc tính toán bội số của một điểm trên đường cong elliptic được gọi là phép nhân vô hướng của một điểm trên đường cong elliptic. Phép nhân vô hướng của một điểm đường cong elliptic dễ dàng được

thực hiện bằng cách sử dụng thuật toán "nhân đôi và cộng". Cho k là một số nguyên dương l bit tùy ý và cho $k = k_{l-1}2^{l-1} + \cdots + k_1 2 + k_0$ là biểu diễn nhị phân của k, trong đó $k_{l-1} = 1$.

Để tính $Q = kG$, thực hiện như sau:

a) Đặt $Q \coloneqq G$.
b) Với $i = l - 2$ giảm xuống $i = 0$, thực hiện:
   1) $Q \coloneqq 2Q$.
   2) Nếu $k_i = 1$ thì $Q \coloneqq Q + G$.

Do đó, đối với một k được chọn ngẫu nhiên có thể kỳ vọng rằng quá trình tính kG sẽ cần đến $(l - 1)$ phép nhân đôi điểm đường cong elliptic cộng với khoảng $l/2$ phép cộng điểm đường cong elliptic.

Phép nhân vô hướng của một điểm trên đường cong elliptic cũng có thể được thực hiện sử dụng thuật toán "cộng-trừ" dựa trên biểu diễn định dạng không liên tục (NAF). Cho k là một số nguyên dương l-bit tùy ý, và cho $k = k_{l-1}2^{l-1} + \cdots + k_1 2 + k_0$ là biểu diễn nhị phân có dấu của k, trong đó $k_i = 0, +1, -1$ và hai giá trị k_i và k_{i+1} không đồng thời khác không.

LƯU Ý: Biểu diễn NAF của k được xác định duy nhất [4]. Độ dài biểu diễn NAF của k là l hoặc $l + 1$.

Để tính $Q = kG$, thực hiện như sau:

a) Đặt $Q \coloneqq O_E$.
b) For $i = l$ down to $i = 0$, do:
   1) Đặt $Q \coloneqq 2Q$.
   2) Nếu $k_i = 1$ thì đặt $Q \coloneqq Q + G$.
   3) Nếu $k_i = -1$ thì đặt $Q \coloneqq Q - G$.

Đối với một k được chọn ngẫu nhiên có thể kỳ vọng rằng quá trình tính kG sẽ cần đến nhiều nhất l phép nhân đôi điểm đường cong elliptic và khoảng $l/3$ phép cộng điểm đường cong elliptic.

C.4.2 Thuật toán với bảng tính toán trước

Phép nhân vô hướng của một điểm đường cong elliptic dễ dàng được thực hiện sử dụng thuật toán "cửa sổ". Thuật toán bao gồm hai phần: phần tính toán trước và vòng lặp chính. Trong giai đoạn tính toán trước, các điểm $G_i = iG$ được tính toán với số lẻ $i \in [1, 2^w - 1]$ đối với một số $w > 0$ nào đó, trong đó w xác định độ lớn của bảng tính toán trước. Trong giai đoạn vòng lặp chính, kG được tính toán bằng cách sử dụng các điểm đã tính toán trước.

Cho k là một số nguyên dương tùy ý và cho $k = k_{l-1}2^{l-1} + \cdots + k_1 2 + k_0$ là biểu diễn nhị phân của k, trong đó $k_{l-1} = 1$. Để tính $Q = kG$, thực hiện như sau:

- Tính toán trước:

a) $G_1 \coloneqq G, G_2 \coloneqq 2G$.
b) Với $i = 1$ đến $2^{w-1} - 1$, thực hiện: $G_{2i+1} \coloneqq G_{2i-1} + G_2$.

- Vòng lặp chính:

c) $j \coloneqq l - 1, Q \coloneqq G$.
d) Vòng lặp $j \geq 0$, do:
1) Nếu $k_j = 0$, thì $Q \coloneqq 2Q$ và $j \coloneqq j - 1$.

2) Ngược lại, $h := \sum_{j \geq i \geq t} k_i 2^{i-t}, Q := 2^{j-t+1}Q + G_h$ đối với số nguyên nhỏ nhất t sao cho $j - t + 1 \leq w$ và $k_t = 1$, và $j := t - 1$.

Tính toán trước cần một phép nhân đôi điểm và $2^{w-1} - 1$ phép cộng. Vòng lặp chính cần (nhiều nhất) $l - 1$ phép nhân đổi điểm và khoảng $[l/(w + 1)]$ phép cộng. Do đó, đối với một k được chọn ngẫu nhiên, có thể mong đợi rằng quá trình tính kG sẽ yêu cầu $(l - 1)$ phép nhân đôi điểm đường cong elliptic cùng với khoảng $(l/(w + 1) + 2^{w-1} - 1)$ phép cộng điểm đường cong ellipitc.

C.5 Kháng lại phân tích kênh kề

C.5.1 Tổng quan về phân tích kênh kề

Tấn công kênh kề giám sát mức tiêu thụ năng lượng và thậm chí là khai thác thông tin rò rỉ liên quan đến tiêu thụ năng lượng để tìm các bit của một khóa bí mật. Có hai kiểu phân tích năng lượng chính, phân tích năng lượng đơn giản (SPA) và phân tích năng lượng vi sai (DPA). SPA sử dụng một lệnh như một chỉ thị được thực hiện trong thuật toán tính lũy thừa mà phụ thuộc vào dữ liệu đang được xử lý. DPA sử dụng mối tương quan giữa mức tiêu thụ năng lượng và các bit phụ thuộc khóa cụ thể.

Trong bất kỳ một hệ mật ECC, việc thực thi phép nhân vô hướng phải được cứng hóa chống lại tấn công kênh kề. Trong tấn công kênh kề, kẻ tấn công tìm cách khám phá các khóa bí mật hoặc dữ liệu bí mật bằng cách quan sát ảnh hưởng phụ của quá trình tính toán được thực hiện bởi thiết bị mật mã được đề cập. Ví dụ về các ảnh hưởng phụ của quá trình tính toán là trường hợp phát xạ điện từ, mức sử dụng năng lượng của thiết bị, phát xạ âm thanh hoặc thông báo lỗi do hệ thống tạo ra.

Một khuyến cáo mạnh được đưa ra là cần phải có một chuyên gia về cài đặt kháng tấn công kênh kề sớm tham gia vào quá trình thiết kế khi thực thi phần này của ISO/IEC 15946, ít nhất khi các hệ thống được triển khai không thể được bảo vệ một cách đáng tin cậy chống lại tấn công kênh kề bằng cách thực hiện phép đo các bước hoạt động; xem tài liệu tham khảo [8] và [17] để biết thông tin tổng quan.

C.5.2 Thuật toán cơ bản an toàn chống lại SPA

Một trong các thuật toán cơ bản an toàn chống lại SPA là thang Montgomery.[9] Cho k là một số nguyên dương tùy ý và cho $k = k_{l-1}2^{l-1} + \cdots + k_1 2 + k_0$ là biểu diễn nhị phân của k, trong đó $k_{l-1} = 1$. Để tính $Q = kG$, thực hiện như sau:

a) $Q_0 := O$.
b) $Q_1 := G$.
c) For $i = l - 1$ down to 0, do:
   1) $b := k_i$.
   2) $Q_{1-b} := Q_{1-b} + Q_b$.
   3) $Q_b := 2Q_b$.
d) Return Q_0.

C.5.3 Thuật toán cơ bản an toàn chống lại DPA

Một trong các thuật toán cơ bản an toàn chống lại DPA là ngẫu nhiên hóa điểm.[11] Cho k là một số nguyên dương tùy ý và cho $k = k_{l-1}2^{l-1} + \cdots + k_1 2 + k_0$ là biểu diễn nhị phân của k, trong đó $k_{l-1} = 1$. Cho R là một điểm ngẫu nhiên. Để tính $Q = kG$, thực hiện như sau:

a) $Q_2 := R, Q_0 := -Q_2, Q_1 := G - Q_2$.
b) For $i = l - 1$ down to 0, do:

1) $b := k_i$.
2) $Q_2 := 2Q_2$.
3) $Q_2 := Q_2 + Q_b$.

c) Return $Q_2 + Q_0$.

C.6 Các thuật toán tính phép ghép cặp

C.6.1 Hàm bổ trợ

Để tính các phép ghép cặp, hai hàm bổ trợ f và g được định nghĩa như sau: Hàm $f(P, Q, R)$ được định nghĩa đối với $E\left(F(q^B)\right) \ni P = (x_P, y_P), Q = \left(x_Q, y_Q\right), R = (x_R, y_R)$ như sau.

Đối với một đường cong elliptic E trên $F(p^m)(p > 3)$ có phương trình $Y^2 = X^3 + aX + b$:

- Nếu $P = O_E$ và $Q = O_E$, thì $f(P, Q, R) = 1_F$;
- ngược lại, nếu $P = O_E$, thì $f(P, Q, R) = x_R - x_Q$;
- ngược lại, nếu $Q = O_E$, thì $f(P, Q, R) = x_R - x_P$;
- ngược lại, nếu $x_P \neq x_Q$, thì $f(P, Q, R) = (x_Q - x_P)y_R - (y_Q - y_P)x_R - x_Q y_P + x_P y_Q$;
- ngược lại, nếu $y_P \neq y_Q$, thì $f(P, Q, R) = x_R - x_P$;
- ngược lại, nếu $b = 0_F$ và $x_P = y_P = x_Q = y_Q = 0_F$, thì $f(P, Q, R) = x_R$;
- ngược lại, thì $f(P, Q, R) = (-3xp^2 - a)(x_R - x_P) + 2y_P(y_R - y_P)$
$= -(y_R - y_P)^2 + (x_R - x_P)^2(2x_P + x_R)$.

Đối với một đường cong elliptic E trên $F(2^m)$ có phương trình $Y^2 + XY = X^3 + aX^2 + b$:

- Nếu $P = O_E$ và $Q = O_E$, thì $f(P, Q, R) = 1_F$;
- ngược lại, nếu $P = O_E$, thì $f(P, Q, R) = x_R + x_Q$;
- ngược lại, nếu $Q = O_E$, thì $f(P, Q, R) = x_R + x_P$;
- ngược lại, nếu $x_P \neq x_Q$, thì $f(P, Q, R) = (x_Q + x_P)y_R + \left(y_Q + y_P\right)x_R + x_Q y_P + x_P y_Q$;
- ngược lại, nếu $y_P \neq y_Q$, thì $f(P, Q, R) = x_R + x_P$;
- ngược lại, nếu $x_P = x_Q = 0_F$ và $y_P = y_Q = \sqrt{b}$ thì $f(P, Q, R) = x_R$;
- ngược lại, thì $f(P, Q, R) = (y_P + x_{P^2})(x_R + x_P) + x_P(y_R + y_P)$
$= (y_R + y_P)^2 + (x_R + x_P)[y_R + y_P + (x_R + x_P)(a + x_R)]$.

Đối với một đường cong elliptic E trên $F(3^m)$ có phương trình $Y^2 = X^3 + aX^2 + b$:

- Nếu $P = O_E$ và $Q = O_E$, thì $f(P,Q,R) = 1_F$;

- ngược lại, nếu $P = O_E$, thì $f(P,Q,R) = x_R - x_Q$;

- ngược lại, nếu $Q = O_E$, thì $f(P,Q,R) = x_R - x_P$;

- ngược lại, nếu $x_P \neq x_Q$, thì $f(P,Q,R) = (x_Q - x_P)y_R - (y_Q - y_P)x_R - x_Q y_P + x_P y_Q$;

- ngược lại, nếu $y_P \neq y_Q$, thì $f(P,Q,R) = x_R - x_P$;

- ngược lại, nếu $b = 0_F$ và $x_P = y_P = x_Q = y_Q = 0_F$, thì $f(P,Q,R) = x_R$;

- ngược lại, thì $f(P,Q,R) = -(y_R - y_P)^2 + (x_R - x_P)^2(2x_P + a + x_R)$.

Hàm $g(P,Q,R)$ định nghĩa với $P,Q,R \in E(F(q^B))$ là $g(P,Q,R) = f(P,Q,R)/f(P+Q,-P-Q,R)$.

Hàm $d_n(P,Q)$ cho hai điểm P và Q trên E với cấp $n > 2$ được tính toán sử dụng thuật toán sau đây.

a) Cho $n = n_{l-1}2^{l-1} + \cdots + n_1 2 + n_0$ ($n_{l-1} \neq 0$) là một biểu diễn nhị phân, trong đó $n_i = 0,1$.
b) Đặt $Y := P, h := 1$.
c) Với $i = l-2$ đến 0, thực hiện:
   1) $h := h^2 \cdot g(Y,Y,Q), Y := 2Y$;
   2) Nếu $n_i \neq 0$, thì

      $h := h \cdot g(Y,P,Q)$;
      $Y := Y + P$.
d) Đầu ra h là $d_n(P,Q)$.

C.6.2 Thuật toán để tính phép ghép cặp Weil

Cho G_1 và G_2 là hai điểm trên E với $nG_1 = nG_2 = O_E$. Phép ghép cặp Weil $e_n(G_1,G_2)$ được tính toán theo các bước sau:

a) Chọn ngẫu nhiên một điểm R trên E sao cho $O_E, G_2, R, G_1 + R$ đều khác nhau.

b) Tính $e_n(G_1,G_2) = [d_n(G_2,R)d_n(G_1,G_2 - R)]/[d_n(G_2,G_1+R)d_n(G_1,-R)]$.

c) Nếu xuất hiện phép chia cho 0 trong quá trình tính toán ở trên, thì bắt đầu lại với một điểm R mới.

C.6.3 Thuật toán để tính phép ghép cặp Tate

Cho G_1 và G_2 là hai điểm trên E với $nG_1 = nG_2 = O_E$. Cặp Tate $e_n(G_1,G_2)$ được tính toán theo các bước sau:

a) Chọn ngẫu nhiên một điểm R trên E.

b) Tính $e_n(G_1,G_2) = d_n(G_1,G_2 - R)/d_n(G_1,-R)$.

c) Nếu xuất hiện phép chia cho 0 trong quá trình tính toán ở trên, thì bắt đầu lại với một điểm R mới.

C.7 Phê chuẩn tham số miền đường cong elliptic và khóa công khai (tùy chọn)

C.7.1 Giới thiệu chung

Trong C.7.1 mô tả các tham số miền đường cong elliptic và cách thức kiểm tra các tham số này. Một tập hợp các tham số miền cụ thể có thể được các bên liên quan thỏa thuận để sử dụng cho một mục đích hoặc cho nhiều mục đích.

Nếu một tập hợp các tham số miền ứng viên là không hợp lệ, thì tất cả các giả thiết về độ an toàn sẽ được giả định là vô hiệu, bao gồm độ an toàn dự kiến cho mọi hoạt động mật mã tùy ý và tính bí mật của khóa riêng. Do đó, trước khi sử dụng một tập hợp các tham số miền ứng viên, người dùng phải đảm bảo rằng nó là hợp lệ. Đảm bảo này có thể đạt được vì:

- Các tham số miền được sinh bởi người dùng hoặc cho người dùng bởi bên thứ ba đáng tin cậy, hoặc

- Các tham số miền đã được người dùng hoặc bên thứ ba đáng tin cậy kiểm tra kỹ lưỡng.

C.7.2 Phê chuẩn tham số miền đường cong elliptic trên $F(q)$

Các điều kiện sau đây phải được người dùng các tham số đường cong elliptic kiểm tra.

a) Kiểm tra q là một lũy thừa của một số nguyên tố, p^m.

b) Kiểm tra a, b, x_G và y_G là các phần tử của trường cơ sở.

c) Kiểm tra $4a^3 + 27b^2 \neq 0$ nếu $q = p^m$ với $p > 3, b \neq 0$ nếu $q = 2^m$, và $a, b \neq 0$ nếu $q = 3^m$.

d) Nếu đường cong elliptic được sinh giả ngẫu nhiên, kiểm tra rằng a và b được dẫn xuất từ MẦM.

e) Nếu $q = p^m$ với $p > 3$, kiểm tra $y_G^2 = x_G^3 + ax_G + b$ trong $F(q)$. Nếu $q = 2^m$, kiểm tra $y_G^2 + x_G y_G = x_G^3 + ax_G^2 + b$ trong $F(2^m)$.

Nếu $q = 3^m$, kiểm tra $y_G^2 = x_G^3 + ax_G^2 + b$ trong $F(3^m)$.

f) Kiểm tra n là số nguyên tố và $n > 4\sqrt{q}$.

LƯU Ý: n là tham số an toàn chính. Các giới hạn cụ thể có trong mô tả của các thuật toán.

g) Kiểm tra $nG = O_E$.

h) Tính $h' = [(\sqrt{q} + 1)^2/n]$ và kiểm tra $h = h'$.

i) Kiểm tra danh sách để loại trừ các đường cong yếu đã biết:

- Kiểm tra xem có thỏa mãn điều kiện MOV, tức là bài toán lôgarit rời rạc trong $F(q^B)$ có mức an toàn đủ cao, trong đó ECDLP trên $E/F(q)$ được quy dẫn xuống DLP trên $F(q^B)$ bởi thuật toán Frey-Rück hoặc Menezes-Okamoto-Vanstone.

- Kiểm tra đường cong không phải là đường cong bất quy tắc, tức là $\#E(F(q)) \neq q$.

Nếu bất kỳ bước kiểm tra nào ở trên không thành công, thì tham số miền được coi là không hợp lệ.

C.7.3 Phê chuẩn khóa công khai (tùy chọn)

Cho trước một tập hợp các tham số miền đường cong elliptic hợp lệ và một khóa công khai được xác nhận có liên quan Q với các tọa độ nhất định và một cấp nhất định, khóa công khai được phê chuẩn như sau:

a) Kiểm tra Q không phải là điểm tại vô hạn O_E.

b) Kiểm tra x_Q và y_Q là các phần tử trong trường $F(q)$, trong đó x_Q và y_Q là tọa độ x và y của Q tương ứng.

c) Nếu $q = p^m$ với $p > 3$, kiểm tra $y_G^2 = x_G^3 + ax_G + b$ trong $F(q)$. Nếu $q = 2^m$, kiểm tra $y_G^2 + x_G y_G = x_G^3 + ax_G^2 + b$ hoặc $y_Q^2 + ay_Q = x_Q^3 + bx_Q + c$ trong $F(2^m)$. Nếu $q = 3^m$, kiểm tra $y_G^2 = x_G^3 + ax_G^2 + b$ hoặc $y_Q^2 = x_Q^3 + ax_Q + b$ trong $F(3^m)$.

d) Kiểm tra $nQ = O_E$.

Nếu bất kỳ bước kiểm tra nào ở trên không thành công, thì khóa công khai được coi là không hợp lệ.

Nếu một khóa công khai ứng viên không hợp lệ, thì tất cả các giả thiết về độ an toàn sẽ được giả định là vô hiệu, bao gồm độ an toàn dự kiến của bất kỳ hoạt động mật mã nào và tính bí mật của khóa riêng liên quan. Ngoài ra, việc sử dụng khóa công khai không hợp lệ trong một hoạt động mật mã, ví dụ như trong việc thiết lập khóa, với khóa riêng có thể tiết lộ thông tin về khóa riêng. Do đó, trước khi sử dụng khóa công khai ứng viên, người dùng phải đảm bảo rằng nó là hợp lệ. Điều này có thể giải quyết được vì:

- Khóa công khai được người dùng phê chuẩn một cách rõ ràng,

- Khóa công khai được phê chuẩn một cách rõ ràng bởi TTP cho người dùng,

- Người dùng chấp nhận rủi ro khi sử dụng khóa công khai không được phê chuẩn,

LƯU Ý 1: Điều này bao gồm một phân tích cho thấy tiềm năng an toàn bị hạn chế trong ứng dụng cụ thể. Việc chấp nhận rủi ro đó có thể phù hợp với khóa công khai tức thời hơn so với khóa công khai dài hạn. Lưu ý rằng việc thực hiện phê chuẩn khóa công khai EC là một mặc định an toàn, vì không có hậu quả an toàn tiêu cực tiềm ẩn nào khi thực hiện.

- Một khóa công khai không được kiểm tra có thể được sử dụng trong các điều kiện khóa được sinh hoặc xác nhận tính hợp lệ một cách rõ ràng bởi một thực thể được người dùng tin cậy trong suốt vòng đời của khóa.

LƯU Ý 2: Phê chuẩn khóa công khai không đảm bảo rằng chủ sở hữu đã xác nhận quyền sở hữu khóa riêng là chủ sở hữu thực sự của khóa.

Phụ lục D
(tham khảo)
Tổng hợp các hệ tọa độ

Các tính chất của các hệ tọa độ khác nhau được tổng hợp lại. Trong trường hợp $E(F(q))$ với $p > 3$, có năm hệ tọa độ, tọa độ affine, tọa độ xạ ảnh, tọa độ Jacobi, tọa độ Jacobi sửa đổi và tọa độ hỗn hợp. Trong các trường hợp của $E(F(2^m))$ và $E(F(3^m))$, có hai hệ tọa độ, tọa độ affine và tọa độ xạ ảnh.

Ký hiệu tọa độ affine, tọa độ xạ ảnh, tọa độ Jacobi và tọa độ Jacobi sửa đổi bằng A, P, J và J_m; thời gian cho phép cộng hai điểm theo tọa độ C_1 và C_2 cho kết quả trong tọa độ C_3 là $t(C_1 + C_2 = C_3)$; thời gian cho phép nhân đôi một điểm theo tọa độ C_1 cho kết quả trong tọa độ C_2 là $t(2C_1 = C_2)$; và phép nhân (tương ứng, nghịch đảo, tương ứng, bình phương) trong $F(q)$ bằng M(tương ứng, I, tương ứng, S_q). Bảng D.1 tổng hợp các tọa độ của $E(F(q))$ với $p > 3$. Bảng D.2 tổng hợp các tọa độ của $E(F(2^m))$. Bảng D.3 tổng hợp các tọa độ của $E(F(3^m))$.

Bảng D.1 – Tổng hợp các tọa độ của $E(F(q))$ với $p > 3$

Phép nhân đôi điểm		Phép cộng điểm	
Hoạt động	**Thời gian tính toán**	**Hoạt động**	**Thời gian tính toán**
$t(2P)$	$7M + 5S_q$	$t(J_m + J_m)$	$13M + 6S_q$
$t(2J)$	$4M + 6S_q$	$t(J + J)$	$12M + 4S_q$
$t(2J_m)$	$7M + 5S_q$	$t(P + P)$	$12M + 2S_q$
$t(2J_m = J)$	$7M + 5S_q$	$t(J + A = J_m)$	$9M + 5S_q$
$t(2A = J_m)$	$3M + 4S_q$	$t(J_m + A = J_m)$	$9M + 5S_q$
$t(2A = J)$	$2M + 4S_q$	$t(J + A = J)$	$8M + 3S_q$
–	–	$t(J_m + A = J)$	$8M + 3S_q$
–	–	$t(A + A = J_m)$	$5M + 4S_q$
$t(2A)$	$2M + 2S_q + I$	$t(A + A)$	$2M + S_q + I$

Bảng D.2 – Tổng hợp các tọa độ của $E(F(2^m))$

Phép nhân đôi điểm		Phép cộng điểm	
Hoạt động	**Thời gian tính toán**	**Hoạt động**	**Thời gian tính toán**
$t(2P)$	$7M + 5S_q$	$t(P + P)$	$16M + 2S_q$

$t(2A)$	$2M + S_q + I$	$t(A + A)$	$2M + S_q + I$

Bảng D.3 – Tổng hợp các tọa độ của $E(F(3^m))$

Phép nhân đôi điểm		Phép cộng điểm	
Hoạt động	Thời gian tính toán	Hoạt động	Thời gian tính toán
$t(2P)$	$9M + 3S_q$	$t(P + P)$	$15M + 2S_q$
$t(2A)$	$3M + S_q + I$	$t(A + A)$	$2M + S_q + I$

Thư mục tài liệu tham khảo

[1] ANSI X9.62-2005, *Public Key Cryptography for the Financial Services Industry: The Elliptic Curve Digital Signature Algorithm (ECDSA)*

[2] ANSI X9.63-2001, *Public Key Cryptography for the Financial Services Industry: Key Agreement and Key Transport Using Elliptic Curve Cryptography*

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

[4] AVANZI R., COHEN H., DOCHE C., FREY G., LANGE T., NGUYEN K. Handbook of Elliptic and Hyperelliptic Curve Cryptography. Chapman & Hall/CRC, 2005

[5] COHEN H. *"A course in computational algebraic number theory"*, Graduate Texts in Math. 138, Springer-Verlag, 1993, Fourth printing, 2000

[6] COHEN H., MIYAJI A., ONO T. *"Efficient elliptic curve exponentiation using mixed coordinates"*, Advances in Cryptology -Proceedings of ASIACRYPT'98, Lecture Notes in Computer Science, 1514 (1998), Springer-Verlag, 51-65

[7] 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

[8] KILLMANN W., LANGE T., LOCHTER M., THUMSER W., WICKE G. *"Minimum Requirements for Evaluating Side-Channel Attack Resistance of Elliptic Curve Implementations"*, version 1.0.4 Federal Office for Information Security, 2011

[9] PETER L. Montgomery, *"Speeding up the Pollard and elliptic curve methods of factorization"*, Mathematics of Computation. Fundamentals. 1987, **48** (177) pp. 243-264

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

[11] MAMIYA H., MIYAJI A., MORIMOTO H. *"Secure elliptic curve exponentiation against RPA, ZRA, DPA, and SPA"*, IEICE Trans. Fundamentals. 2006, **89-A** (8) pp. 2207-2215

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

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

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

[15] WASHINGTON L.C. Elliptic Curves: Number Theory and Cryptography. Chapman & Hall/CRC, 2003

[16] WATERHOUSE W. *"Abelian varieties over finite fields"*, Ann. scient. Éc. *Norm. Sup.* 1969, **2** pp. 521-560

[17] GOUNDAR R., JOYE M., MIYAJI A., RIVAIN M., VENELLI A. *"Scalar multiplication on weierstrass elliptic curves from Co-Z arithmetic"*, Journal of Cryptographic Engineering, vol. 1 (2011), Springer-Verlag, 161-176