TCVN TIÊU CHUẨN QUỐC GIA

TCVN 12854-4 : 2020

ISO/IEC 29192-4 : 2013

WITH AMENDMENT 1:2016

Xuất bản lần 1

CÔNG NGHỆ THÔNG TIN CÁC KỸ THUẬT AN TOÀN – MẬT MÃ HẠNG NHẸ – PHẦN 4: CÁC CƠ CHẾ SỬ DỤNG KỸ THUẬT PHI ĐỐI XỨNG

Information technology – Security techniques – Lightweight cryptography – Part 4: Mechanisms using asymmetric techniques

HÀ NỘI – 2020

Mục lục

Lời nói đầu

TCVN 12854-4: 2020 hoàn toàn tương đương với ISO/IEC 29192-4:2013 và sửa đổi 1:2016.

TCVN 12854-4: 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 12854 (ISO/IEC 29192) *Công nghệ thông tin – Các kỹ thuật an toàn – Mật mã hạng nhẹ* gồm các tiêu chuẩn sau:

- TCVN 12854-1: 2020 (ISO/IEC 29192-1:2012) Phần 1: Tổng quan

- TCVN 12854-2: 2020 (ISO/IEC 29192-2:2012) Phần 2: Mã khối

- TCVN 12854-3: 2020 (ISO/IEC 29192-3:2012) Phần 3: Mã dòng

- TCVN 12854-4: 2020 (ISO/IEC 29192-4:2013) Phần 4: Các cơ chế sử dụng kỹ thuật phi đối xứng.

TIÊU CHUẨN QUỐC GIA **TCVN 12854-4 : 2020**

Công nghệ thông tin - Các kỹ thuật an toàn – Mật mã hạng nhẹ - Phần 4: Các cơ chế sử dụng kỹ thuật phi đối xứng

Information technology – Security techniques – Lightweight cryptography – Part 4: Mechanisms using asymmetric techniques

1 Phạm vi áp dụng

Tiêu chuẩn này quy định bốn cơ chế hạng nhẹ sử dụng kỹ thuật phi đối xứng:

- Cơ chế xác thực một chiều dựa trên các logarit rời rạc trên đường cong elliptic;

- Cơ chế trao đổi khóa hạng nhẹ có xác thực (ALIKE) cho xác thực một chiều và thiết lập một khóa phiên;

- Cơ chế chữ ký dựa trên định danh;

- Một lược đồ xác thực một chiều (ELLI) dựa trên logarit rời rạc trên đường cong elliptic xác định trên các trường hữu hạn có đặc số hai.

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 (ISO/IEC 15946-1), Công nghệ thông tin – Các kỹ thuật an toàn – Kỹ thuật mật mã dựa trên đường cong elliptic – Phần 1: Tổng quan.

TCVN 12854-1 (SSO/IEC 29192-1), Công nghệ thông tin – Các kỹ thuật an toàn – Mật mã hạng nhẹ - Phần 1: Tổng quan.

3 Thuật ngữ và định nghĩa

Với mục đích của tiêu chuẩn này, các thuật ngữ và định nghĩa được đưa ra trong TCVN 12854-1 và dưới đây được áp dụng:

3.1

Kỹ thuật mật mã phi đối xứng (asymmetric cryptographic technique)

Kỹ thuật mật mã mà sử dụng hai phép toán liên quan đến nhau: Phép toán công khai được xác định bởi thành phần dữ liệu công khai và phép toán bí mật được xác định bởi thành phần dữ liệu bí mật.

CHÚ Ý Hai phép toán này có tính chất là, dựa trên phép toán công khai, để có được phép toán bí mật là không khả thi về mặt tính toán.

3.2

Cặp phi đối xứng (sysmmetric pair)

Hai thành phần dữ liệu có liên quan đến nhau trong đó thành phần dữ liệu bí mật xác định một phép toán bí mật và thành phần dữ liệu công khai xác định một phép toán công khai.

3.3

Thách thức (challenge)

Tham số thủ tục được sử dụng kết hợp với các tham số bí mật để đưa ra một phản hồi.

3.4

Bên được xác thực (claimant)

Thực thể với định danh có thể được xác thực, bao gồm các hàm và dữ liệu bí mật cần thiết để tham gia trao đổi xác thực thay mặt cho chủ thể.

3.5

Tham số bên được xác thực (claimant parameter)

Thành phần dữ liệu công khai, số hoặc xâu bit, đặc trưng cho bên được xác thực đã cho trong miền.

3.6

Hàm băm kháng va chạm (collision-resistant hash-fuction)

Hàm băm thỏa mãn tính chất sau: không khả thi về mặt tính toán để tìm ra hai đầu vào khác nhau mà ánh xạ tới cùng một đầu ra

CHÚ THÍCH Tính không khả thi về mặt tính toán phụ thuộc vào môi trường và các yêu cầu an toàn cụ thể.

[TCVN 11816-1, 3.2]

3.7

Coupon (coupon)

Cặp các số được tính toán trước chỉ sử dụng một lần

CHÚ THÍCH Một trong các số đó phải được giữ bí mật và một số khác phải được giữ bí mật trước khi sử dụng

3.8

Miền (domain)

Tập các thực thể hoạt động theo một chính sách bảo mật riêng.

3.9

Tham số miền (domain parameter)

Khóa công khai, hoặc hàm, được thống nhất và sử dụng bởi tất cả các thực thể trong miền

3.10

Xác thực thực thể (entity authentication)

Chứng thực rằng một thực thể chính là một thực thể đã khai báo

[TCVN 11817-1 (ISO/IEC 9798-1)]

3.11

Tham số số lượng trao đổi (exchange multiplicity parameter)

Số lượng quá trình trao đổi thông tin liên quan đến một trường hợp của cơ chế xác thực.

3.12

Hàm băm (hash-function)

Hàm mà ánh xạ một xâu bit tới một xâu bit có độ dài cố định thỏa mãn 2 tính chất sau:

- không khả thi về mặt tính toán để tìm được một giá trị đầu vào ứng với một giá trị đầu ra cho trước.

- không khả thi về mặt tính toán để thể tìm được một đầu vào thứ 2 khác với đầu vào cho trước mà có cùng đầu ra.

CHÚ THÍCH Tính khả thi về mặt tính toán phụ thuộc vào môi trường và các yêu cầu an toàn cụ thể.

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

3.13

Khóa chủ bí mật (master secret key)

Thành phần dữ liệu bí mật

CHÚ THÍCH Khóa chủ bí mật chỉ được sử dụng bởi máy chủ tin cậy phù hợp với quá trình sinh dữ liệu bí mật của người ký.

3.14

Khóa bí mật (private key)

Thành phần dữ liệu bí mật của một cặp phi đối xứng

CHÚ THÍCH Khóa bí mật phải được giữ bí mật và chỉ nên được sử dụng bởi bên được xác thực theo một cách thức phản hồi thích hợp, qua đó thiết lập định danh của nó.

3.15

Tham số thủ tục (produce parameter)

Thành phần dữ liệu công khai tạm thời được sử dụng trong một trường hợp của cơ chế xác thực, ví dụ như một bằng chứng, thách thức hoặc phản hồi.

3.16

Khóa công khai (public key)

Thành phần dữ liệu công khai của cặp phi đối xứng, có thể được công khai và được sử dụng bởi mỗi bên xác thực để xác thực định danh của bên được xác thực.

3.17

Số ngẫu nhiên (random number)

Tham số biến thiên theo thời gian có giá trị không thể đoán trước

[TCVN 11817-1 (ISO/IEC 9798-1)]

3.18

Phản hồi (response)

Tham số thủ tục được tạo ra bởi bên được xác thực, và được xử lý bởi bên xác thực để kiểm tra định danh của bên được xác thực

3.19

Tham số bí mật (secret parameter)

Số hoặc xâu bit không xuất hiện trong miền công khai và chỉ được sử dụng bởi bên được xác thực.

CHÚ THÍCH Ví dụ như một khóa bí mật

3.20

Ký (sign)

Quá trình sinh chữ ký, lấy một thông điệp và một khóa ký của người ký để tạo ra chữ ký.

3.21

Người ký (signer)

Thực thể với duy nhất một xâu bit đóng vai trò định danh, bao gồm các chức năng và dữ liệu riêng cần thiết để tham gia vào việc sinh một chữ ký

3.22

Khóa ký (signing key)

Thành phần dữ liệu bí mật được cho bởi máy chủ tin cậy.

CHÚ THÍCH Khóa ký chỉ nên được sử dụng bởi một người ký phù hợp với quá trình sinh một chữ ký.

3.23

Thẻ (token)

Thông điệp bao gồm các trường dữ liệu liên quan đến một phiên liên lạc cụ thể và chứa các thông tin đã được tạo ra bằng cách sử dụng kỹ thuật mật mã

3.24

Xác thực một chiều (unilateral authentication)

Xác thực thực thể cung cấp cho một thực thể sự đảm bảo về một định danh của một thực thể khác nhưng không xác thực chiều ngược lại

3.25

Bên xác thực (verifier)

Thực thể bao gồm các chức năng cần thiết để tham gia vào trao đổi xác thực thay mặt cho chủ thể yêu cầu xác thực thực thể hoặc tham gia xác minh chữ ký của một thông điệp và người ký đã cho.

3.26

Xác thực (verify)

Quá trình xác thực mà nhận đầu vào một thông điệp, một chữ ký và định danh của người ký để đưa ra kết quả *chấp nhận* nghĩa là chữ ký đã cho được sinh bởi người ký với khóa ký tương ứng hoặc ngược lại, đưa ra kết quả *từ chối.*

3.27

Bằng chứng (witness)

Tham số thủ tục mà cung cấp chứng cứ về định danh của bên được xác thực cho bên xác thực

3.28

Trường hữu hạn có đặc số hai (a finite field of characteristic two)

Trường hữu hạn mà có số lượng các phần tử là một lũy thừa của hai.

CHÚ THÍCH Mọi trường hữu hạn có đặc số hai mà có cùng số lượng phần tử đều đẳng cấu với nhau. Mô hình cụ thể để mô tả trường hữu hạn có đặc số hai sử dụng trong trong chuẩn này được cho ở Phụ lục C.

3.29

Đường cong elliptic thông thường trên một trường hữu hạn đặc số hai (ordinary elliptic curve over a finite field of characteristic two)

Đường cong elliptic trên trường hữu hạn đặc số hai *F* được xác định bởi một phương trình Weierstrass rút gọn (afine): $Y^2 + XY = X^3 + aX^2 + b$ với a, b ∈ F và $b \neq 0_F$

CHÚ THÍCH 1 Các tính chất của các đường cong elliptic được cho trong Phụ lục B - ISO/IEC 15946-1:2008.

CHÚ THÍCH 2 Tập các điểm trên E cùng với một điểm đặc biệt, ký hiệu 0_E tạo thành một nhóm giao hoán hữu hạn (nhóm abel hữu hạn).

4 Ký hiệu

Với mục đích của tiêu chuẩn này, các ký hiệu và thuật ngữ viết tắt sau được áp dụng.

$\|\Phi\|$	Kích thước theo bit của số Φ nếu Φ là một số nguyên không âm (tức là số nguyên i duy nhất thỏa mãn $2^{i-1} \leq \Phi \leq 2^i$ nếu Φ > 0, hoặc 0 nếu Φ = 0, ví dụ |65537| = $\|2^{16} + 1\|$= 17, hoặc độ dài bit của xâu bit Φ nếu Φ là một xâu bit. CHÚ THÍCH Để biểu diễn một số Φ như là một xâu α bit với $\alpha > \|\Phi\|, \alpha - \|\Phi\|$ bit 0 được thêm vào bên trái của |Φ| bit.
$\lfloor\Phi\rfloor$	Số nguyên lớn nhất mà nhỏ hơn hoặc bằng số thực Φ
$\Phi[i]$	bit thứ *i* của Φ, trong đó $\Phi[1]$ là bit bên phải nhất và $\Phi[\|\Phi\|]$ là bit bên trái nhất.
Ψ ‖ Γ	Xâu bit kết quả từ phép nối của các thành phần dữ liệu Ψ và Γ theo thứ tự đã được quy định.Trong trường hợp mà ở đó kết quả của phép nối hai hoặc nhiều thành phần dữ liệu là đầu vào của một thuật toán mật mã như là một phần của cơ chế xác thực, kết quả này sẽ được tạo ra sao cho nó có thể diễn giải ra thành các xâu dữ liệu cấu thành của nó, tức là không có sự mơ hồ trong việc diễn giải. Tính chất này có thể đạt được theo các cách khác nhau, tùy thuộc vào ứng dụng. Ví dụ, nó có thể được bảo đảm bởi: a) Cố định độ dài của mỗi xâu con xuyên suốt miền sử dụng của cơ chế, hoặc b) Mã hóa dãy các xâu được nối sử dụng một phương pháp mà đảm bảo việc giải mã là duy nhất, ví dụ như sử dụng các quy tắc mã hóa khác nhau được định nghĩa trong ISO/IEC 8825-1[18]
A	Bên được xác thực
B	Bên xác thực
D	Phản hồi (tham số thủ tục)
d	Thách thức (tham số thủ tục)
E	Đường cong elliptic (tham số miền)
E_K	Hàm mã hóa mã khối với khóa *K*

e	Số mũ công khai (tham số miền)
$E_{\{a,b\}}$	Đường cong elliptic thông thường trên trường $F(2^g)$ được cho bởi phương trình Weierstrass rút gọn $Y^2 + XY = X^3 + aX^2 + b$ cùng với điểm tại vô hạn 0_E với a, b $\in$ $F(2^g)$ và $b \neq 0_F$ (tham số miền)
E_{twist}	Đường cong elliptic xoắn đôi của đường cong elliptic E (tham số miền, được sử dụng nhưng không rõ ràng)
$\#(E_{\{a,b\}})$	Cấp (lực lượng) của $E_{\{a,b\}}$ (tham số miền)
$F(2^g)$	Trường hữu hạn chứa chính xác 2^g phần tử, g là một số nguyên dương
$f(X)$	Đa thức bất khả quy trên trường F(2) được sử dụng trong việc xây dựng trường $F(2^g)$
$f_0(u,x)$	$f_0(u,x) = 0 \parallel x \parallel \cdots \parallel 0 \parallel x \parallel 0 \parallel x^*$ trong đó x^* biểu diễn các bit có trọng số cao nhất của x (có thể là không có bit nào) với yêu cầu sao cho độ dài của $0 \parallel x \parallel \cdots \parallel 0 \parallel x \parallel 0 \parallel x^*$ bằng u.
$f_1(u,x)$	$f_1(u,x) = 1 \parallel x \parallel \cdots \parallel 1 \parallel x \parallel 1 \parallel x^*$ trong đó x^* biểu diễn các bit trọng số cao nhất của x (có thể là không có bit nào) với yêu cầu sao cho độ dài của $1 \parallel x \parallel \cdots \parallel 1 \parallel x \parallel 1 \parallel x^*$ bằng u.
h	Hàm băm
$\|h\|$	Độ dài bit của mã băm được sinh ra bởi hàm băm h
HE	Hàm đệm dựa trên mã khối E_K (tham số miền)
ID	Xâu nhị phân biểu diễn định danh hoặc thông tin về định danh
L	Độ dài bit của đoạn mã đệm được tạo ra bởi hàm HE (tham số miền)
m	Thông điệp
$MUL_{b,aff}(k,x_R)$	Hàm phụ thuộc vào phần tử trường $b \neq 0_F$, ánh xạ phần tử x_R từ $F(2^g)$ và số nguyên k vào x-tọa độ (affine) $X_S Z_S^{-1}$ của điểm $S = [k]R = (X_S : Y_S : Z_S)$ trên đường cong elliptic thông thường được xác định trên trường $F(2^g)$ với tham số b và một điểm R trên đường cong có x-toạ độ là x_R. CHÚ THÍCH Xem phụ lục F cho nền tảng toán học của $MUL_{b,aff}(k,x_R)$
$MUL_{b,proj}(k,x_R)$	Hàm phụ thuộc vào phần tử trường $b \neq 0_F$, ánh xạ phần tử x_R từ $F(2^g)$ và số nguyên k vào x-tọa độ xạ ảnh $(X_S : Z_S)$ của điểm $S = [k]R = (X_S : Y_S : Z_S)$ trên đường cong elliptic thông thường được xác định trên trường $F(2^g)$ với tham số b và một điểm R trên đường cong có x-toạ độ affine là x_R. CHÚ THÍCH Xem phụ lục F cho nền tảng toán học của $MUL_{b,proj}(k,x_R)$
N	Một hợp số đóng vai trò là giá trị modulo (tham số miền)

n	Cấp của điểm cơ sở P (tham số miền)
$[n]P$	Phép nhân lấy đầu vào là một số nguyên dương n và một điểm P trên đường cong E và đưa ra đầu ra là điểm Q trên đường cong E với $Q = [n]P = P + P + \ldots + P$ là tổng số lần xuất hiện của P. Phép toán thỏa mãn [0]P = 0_E (điểm tại vô hạn), và $[-n]P = [n](-P)$
P	Điểm cơ sở trên đường cong elliptic E (tham số miền)
$p_1, p_2, \ldots$	các thừa số nguyên tố theo thứ tự tăng dần của modulo, tức là $p_1 < p_2 < \cdots$ (tham số bí mật)
Q, Q_i	Khóa bí mật (tham số bí mật)
q	Kích thước trường (tham số miền)
r	Số ngẫu nhiên mới hoặc xâu mới gồm các bit ngẫu nhiên (tham số bí mật)
T	Điểm công khai (tham số miền)
t	Khóa chủ bí mật (tham số bí mật)
u	Độ dài bit của khóa K trong hàm mã hóa mã khối E_K (tham số miền)
v	Độ dài bit của khối thông điệp trong hàm mã hóa mã khối E_K (tham số miền)
W	Bằng chứng (tham số thủ tục)
w	Tham số an toàn (tham số miền)
$'X_1X_2 \ldots'$	Số biểu diễn dưới hệ thập lục phân là X_1X_2 ..., với mỗi X_i nhận giá trị trong đoạn 0-9 và các chữ cái A-F
α	Kích thước modulo theo bit, tức là $2^{\alpha-1} \leq$ modulo $< 2^{\alpha}$, được ký hiệu $\lvert modulo \rvert$ (tham số miền)
δ	Độ dài các xâu mới gồm các bit ngẫu nhiên biểu diễn các thách thức (tham số miền)
ρ	Độ dài các xâu mới gồm các bit ngẫu nhiên biểu diễn các số ngẫu nhiên (tham số miền)
$\{a, b, c, ..\}$	Tập chứa các phần tử a, b, c, ..
S, T, U	Các điểm trên đường cong E
$Tr(a)$	Tr(a) = $a^{2\wedge 0} + a^{2\wedge 1} + \cdots a^{2\wedge(g-1)}$ đối với một phần tử a tùy ý của trường F(2^g). Tr là "hàm vết" và Tr(a) là "vết của phần tử trường a". Hàm truy vấn chỉ nhận hai giá trị 1_F và 0_F

(X_R, Y_R)	Các tọa độ (affine) của điểm R, với X_R ký hiệu x-tọa độ và Y_R ký hiệu y-toạ độ của điểm R CHÚ THÍCH Điểm 0_E không có biểu diễn trong tọa độ affine
$(X_R : Y_R : Z_R)$	Tọa độ xạ ảnh của điểm R. $(X_R : Y_R : Z_R)$ là lớp tương đương của bộ ba phần tử (X_R, Y_R, Z_R) của trường F(2^g) mà thỏa mãn phương trình Weierstrass (xạ ảnh) tương ứng $Y^2Z + XYZ = X^3 + aX^2Z + bZ^3$, ở đây $(X_{R\prime}, Y_{R\prime}, Z_{R\prime})$ được gọi là tương đương với (X_R, Y_R, Z_R) nếu và chỉ nếu $X_{R\prime} = \lambda X_R$, $Y_{R\prime} = \lambda Y_R$, $Z_{R\prime} = \lambda Z_R$ với một phần tử $\lambda \neq 0_F$ nào đó CHÚ THÍCH Điểm 0_E có tọa độ xạ ảnh là $(0_F : 1_F : 0_F)$
$(X_R : Z_R)$	x-tọa độ xạ ảnh của điểm R CHÚ THÍCH 1 $Z_R \neq 0_F$ và $(X_R : Z_R)$ tương ứng với tọa độ affine $X_R Z_R^{-1} \in F(2^g)$ CHÚ THÍCH 2 Một điểm R với tọa độ affine (x_R, y_R) có tọa độ xạ ảnh là $(x_R : y_R : 1_F)$ CHÚ THÍCH 3 Một điểm R với tọa độ xạ ảnh $(X_R : Y_R : Z_R)$ có tọa độ affine là $(X_R Z_R^{-1}, Y_R Z_R^{-1})$

5 Cơ chế xác thực một chiều dựa trên logarit rời rạc trên đường cong elliptic

5.1 Tổng quan

Trong cơ chế này, cryptoGPS cũng được gọi là GPS trong tài liệu trước đó-, do Girault, Poupard, và Stern đề xuất. Tên thay đổi hiện được dùng để tránh nhầm lẫn với dịch vụ định vị vật lý GPS. cryptoGPS là một cơ chế xác thực tri thức không mà cung cấp xác thực thực thể một chiều. Các biến thể khác nhau của cryptoGPS được quy định trong TCVN 12854 (ISO/IEC 9798-5) và phiên bản phù hợp nhất với các thiết bị hạn chế, cùng với một số tối ưu hóa được trình bày bên dưới.

5.2 Các yêu cầu an toàn đối với môi trường

Cơ chế cryptoGPS cho phép bên xác thực kiểm tra rằng bên được xác thực có biết logarit rời rạc trên đường cong elliptic của một điểm công khai đã xác nhận đối với điểm cơ sở. Một khung tổng quát cho kỹ thuật mật mã dựa trên đường cong elliptic được đưa ra trong ISO/IEC 15946-1.

CHÚ THÍCH 1 Cơ chế này cài đặt biến thể đường cong elliptic của lược đồ cryptoGPS do Girault, Poupard, và Stern đề xuất. Nó cho phép sử dụng biến thể được gọi là LHW đặc biệt phù hợp cho các môi trường mà trong đó tài nguyên của bên được xác thực rất thấp.

Với một miền cho trước, các yêu cầu sau phải được thỏa mãn.

a) Các tham số miền có ảnh hưởng đến các hoạt động của cơ chế phải được lựa chọn. Các tham số đã lựa chọn phải được cung cấp một cách tin cậy cho tất cả các thực thể của miền.

b) Mỗi bên được xác thực phải được trang bị cùng một đường cong elliptic E và một tập các tham số miền, cụ thể là kích thước trường q, một điểm cơ sở P trên E, và cấp n của điểm P. Đường cong và tập các tham số hoặc là các tham số miền hoặc các tham số của bên được xác thực.

c) Mỗi điểm *P* sử dụng làm cơ số cho logarit rời rạc trên đường cong elliptic phải thỏa mãn với điểm *J* bất kỳ trên đường cong, việc tìm được số nguyên *k* trong khoảng [0, n-1] (nếu tồn tại) sao cho *J = [k]P* là không khả thi về mặt tính toán, trong đó tính khả thi được xác định bởi ngữ cảnh sử dụng của cơ chế.

d) Mỗi bên được xác thực phải được trang bị một khóa bí mật

e) Mỗi bên xác thực phải nhận được bản sao xác thực của khóa công khai tương ứng với khóa bí mật của bên được xác thực.

CHÚ THÍCH 2 Cách chính xác mà qua đó bên xác thực thu được bản sao tin cậy của điểm công khai cụ thể của bên được xác thực nằm ngoài phạm vi tiêu chuẩn này. Ví dụ, điều này có thể đạt được bằng cách sử dụng chứng chỉ khóa công khai hoặc bằng một số phương pháp khác phụ thuộc vào môi trường.

f) Bên xác thực phải có phương pháp để tạo ra các xâu mới gồm các bit ngẫu nhiên. Khi các coupon không được sử dụng, mỗi bên được xác thực cũng cần có phương pháp để tạo ra các xâu mới gồm các bit ngẫu nhiên.

g) Nếu cơ chế sử dụng một hàm băm, thì tất cả các thực thể trong miền phải thống nhất về hàm băm, ví dụ một trong các hàm băm được quy định trong TCVN 11817-3.

5.3 Tạo khóa

Với bên được xác thực A, một xâu mới phải được lựa chọn một cách ngẫu nhiên từ tập {2, 3, ..., n-2}. Xâu biểu diễn khóa khóa bí mật, được ký kiệu là Q.

Số $\sigma = |n|$ là số bit được sử dụng để biểu diễn các khóa bí mật.

Ký hiệu G(A) là điểm công khai của bên được xác thực A và được thiết lập bằng

a) Hoặc là điểm ngược của điểm nhận được qua phép nhân điểm cơ sở P với số Q.

$$G(A) = (x_G, y_G) = -[Q]P$$

CHÚ THÍCH 1 Phiên bản này là phù hợp nhất với các thiết bị hạn chế.

b) Hoặc là điểm nhận được qua phép nhân điểm cơ sở P với số Q.

$$G(A) = (x_G, y_G) = [Q]P$$

Các thách thức được lựa chọn từ một tập các số nguyên S có lực lượng Δ, với $2^{\delta-1} < \Delta \leq 2^{\delta}$. Độ dài theo bit của thách thức lớn nhất có thể được ký hiệu là β. Một giá trị của δ từ 8 đến 40 là phù hợp với hầu hết các ứng dụng. Trừ khi được quy định khác đi, giá trị của δ được lấy bằng 40. Nó là một tham số miền.

CHÚ THÍCH 2 Tổng số thách thức có thể nên được giới hạn đến 2^{40}. Nếu khuyến cáo này không được tuân thủ thì cần phải đặc biệt chú ý ngăn chặn bên xác thực coi bên được xác thực như một bộ tiên tri kỳ.

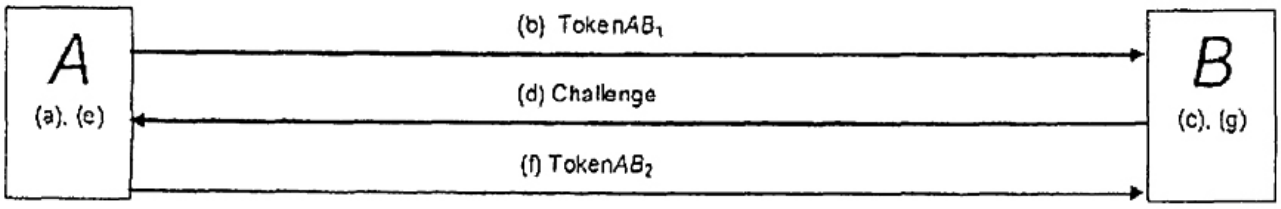
CHÚ THÍCH 3 Khi tập các thách thức là khoảng [0, Δ − 1] thì $\beta = \delta$.

CHÚ THÍCH 4 Một thách thức được gọi là LHW nếu tồn tại ít nhất $\sigma - 1$ bit 0 nằm giữa hai bit 1 liên tiếp trong biểu diễn nhị phân của nó.

CHÚ THÍCH 5 Định nghĩa điểm công khai G(A) hơi khác so với định nghĩa trong ISO/IEC 9798-5. Những thay đổi này cho phép các cài đặt nhỏ gọn và hiệu quả của việc tính toán kết quả trên thẻ vì lúc này công thức phản hồi là dễ dàng và đơn giản để thực hiện hơn so với phép trừ số nguyên.

5.4 Cơ chế xác thực một chiều

Các chữ cái trong ngoặc ở Hình 1 tương ứng với các bước của cơ chế xác thực một chiều, bao gồm các sự trao đổi thông tin, được miêu tả chi tiết bên dưới. Bên được xác thực được ký hiệu là A. Bên xác thực được ký hiệu là B.



Hình 1 – Cơ chế sử dụng logarit rời rạc trên đường cong elliptic

Bên được xác thực lưu một số δ, điểm cơ sở P, và một khóa bí mật Q (là một xâu σ bit). Trừ khi được quy định khác đi, $\delta = 40$.

Trong trường hợp sử dụng coupon, ngoài số δ và khóa bí mật Q, bên được xác thực chỉ cần lưu một tập các coupon và không yêu cầu có các phương thức để tạo ra các xâu mới gồm các bit ngẫu nhiên. Chỉ được sử dụng một lần, mỗi coupon bao gồm một xâu ρ bit (xâu này không cần được lưu trữ nếu nó có thể được tạo lại bằng một hàm giả ngẫu nhiên, ví dụ: một trong các hàm được đặc tả trong ISO/IEC 18031[25]) và một bằng chứng.

Ngoài một số δ và một số σ, bên xác thực phải được cung cấp một bản sao tin cậy của điểm công khai G(A) và đường cong E, điểm cơ sở P và các tham số q và n.

Với mỗi ứng dụng của cơ chế, thủ tục sau phải được thực hiện. Bên xác thực B sẽ chỉ xác nhận bên được xác thực là hợp lệ nếu hoàn thành thủ tục sau.

a) Với mỗi sự xác thực

1) Hoặc sử dụng một coupon (r, W)

2) hoặc một xâu mới ρ bit phải được chọn một cách ngẫu nhiên đều. Nó phải được giữ bí mật.

$$\rho = \sigma + \beta + 80$$

CHÚ THÍCH 1 Nếu xâu mới ρ bit được chọn ngẫu nhiên, thì xác suất để 80 bit bên trái nhất đều bằng nhau là không đáng kể.

Ký hiệu r là số được biểu diễn bởi xâu mới sẽ được chuyển đổi thành một bằng chứng, ký hiệu là *W*. Công thức bằng chứng: $W = EC2OSP_E([r]P, fmt)$

với $EC2OSP_E$ là hàm để chuyển đổi một điểm trên đường cong elliptic E thành các xâu bộ tám được xác định trong ISO/IEC 15946-1 và fmt là một kiểu định dạng mà nhận một trong các giá trị tượng trưng là `compressed`, `uncompressed`, hoặc `hybird`.

CHÚ THÍCH 2 Trong một số cài đặt nhất định, công thức bằng chứng dưới đây hay được sử dụng hơn:

W = $EC2OSP_E([r \bmod n]P, fmt)$.

b) A gửi $TokenAB_1$ cho B. $TokenAB_1$ có thể hoặc là bằng chứng W hoặc một mã băm của W và *Text*, một trong 4 biến thể băm dưới đây.

Bốn biến thể băm là $h(W \parallel Text), h(W \parallel h(Text)), h(h(W) \parallel Text)$ và $h(h(W) \parallel h(Text))$, với h là một hàm băm và *Text* là trường văn bản tùy chọn (nó có thể rỗng). Nếu trường văn bản là không rỗng, B phải có các cách để khôi phục lại giá trị của *Text*; điều này có thể yêu cầu *A* gửi tất cả hoặc một phần của trường văn bản kèm với thẻ. Cách trường văn bản được tạo sẵn để sử dụng trong các ứng dụng nằm ngoài phạm vi của tiêu chuẩn này. Phụ lục A của ISO/IEC 9798-1[20] đưa ra thông tin sử dụng của các trường văn bản. Biến thể băm là tham số miền.

c) Khi nhận $TokenAB_1$, một xâu mới phải được lựa chọn một cách ngẫu nhiên đều từ tập *S*.

d) *B* gửi xâu mới như một thách thức cho *A*. Xâu mới biểu diễn một số được ký hiệu là *d*.

CHÚ THÍCH 3 Nếu một thách thức LHW được sử dụng, nó có thể được truyền dưới dạng nén đến A, một thực thể phải có các phương pháp trích xuất được thách thức ban đầu trước bước e)1).

e) Khi đã nhận thách thức, các bước tính toán sau được thực hiện.

1) Nếu thách thức không phải là phần tử thuộc *S*, thì thủ tục thất bại.

2) Một phản hồi *D* được tính toán từ số ngẫu nhiên r và khóa bí mật *Q*.

Công thức phản hồi như sau:

i) $D = r + d \times Q$ nếu $G(A) = -[Q]P$

CHÚ THÍCH 4 Nếu thách thức nhận được là thách thức LHW, việc tính toán D được quy về thành một bổ sung tiếp nối của r với sự ghép nối các bản sao của Q, được phân tách bằng các bit 0.

hoặc

ii) $D = r - d \times Q$ nếu $G(A) = [Q]P$

f) *A* gửi $TokenAB_2$ cho *B*. $TokenAB_2$ là phản hồi D được tính toán từ bước e)2).

g) Khi đã nhận $TokenAB_2$ các bước tính toán sau được thực hiện.

1) Nếu phản hồi *D* không phải là một xâu ρ bit và/hoặc nếu 80 bit bên trái nhất của *D* đều bằng nhau, thì thủ tục thất bại.

2) Ký hiệu W^* là một bằng chứng được tính toán.

Công thức kiểm tra: $W^* = EC2OSP_E$([d]G(A) +[D]P, fmt)

CHÚ THÍCH 5 Trong một số cài đặt nhất định, công thức bằng chứng dưới đây hay được sử dụng hơn là:

W = $EC2OSP_E$([d]G(A) +[D mod n]P, fmt)

3) Nếu hoặc bằng chứng W^* hoặc một mã băm của W^* và *Text* (một trong bốn biến thể băm) bằng $TokenAB_1$ nhận được ở bước b), thì quá trình thành công. Ngược lại thủ tục thất bại.

CHÚ THÍCH 6 Thông tin khác có thể được gửi cùng trong quá trình trao đổi của thủ tục. B có thể sử dụng thông tin đó để tính toán giá trị của trường văn bản tùy chọn. Ví dụ, A có thể gửi cho B thông tin chẳng hạn như các chứng chỉ cùng với $TokenAB_1$.

6 Cơ chế trao đổi khóa có xác thực một chiều dựa trên mã hóa

6.1 Tổng quan

Cơ chế ALIKE được thiết kế cho các giao dịch không có sự tiếp xúc, tức là các giao dịch phải chịu hạn chế rất mạnh về thời gian. Trong giao thức này, bên xác thực (ví dụ như thiết bị đọc hoặc thiết bị đầu cuối) xác thực bên được xác thực (như thẻ không tiếp xúc) liên quan đến cơ quan cấp chứng nhận. Thêm nữa, bên được xác thực và bên xác thực thiết lập một khóa phiên để nhắn tin an toàn. Điểm đặc biệt của ALIKE là nó cho phép sử dụng thiết bị đọc có chi phí thấp (không có mô đun truy cập an toàn) trong khi đạt được giới hạn thời gian lớn. ALIKE dựa trên lược đồ mã hóa khóa công khai được gọi là RSA cho những người hoang tưởng - một biến thể của RSA – mà giải mã rất nhanh. Trong ALIKE, việc giải mã được thực hiện bởi bên được xác thực (ví dụ như thẻ không tiếp xúc) nơi mà thường có sẵn bộ xử lý mật mã.

CHÚ THÍCH ALIKE là viết tắt của Authenticated Lightweight Key Exchange (Trao đổi khóa hạng nhẹ có xác thực). Tên trước của ALIKE là SPAKE. Các chứng minh an toàn của ALIKE được cho trong [3].

6.2 Các yêu cầu an toàn đối với môi trường

Cơ chế ALIKE cho phép bên xác thực xác thực một bên được xác thực liên quan đến cơ quan cấp chứng nhận và cho phép thiết lập một khóa phiên để nhắn tin an toàn.

Với một miền đã cho, các yêu cầu sau phải được thỏa mãn.

a) Các tham số miền mà chi phối các hoạt động của cơ chế phải được lựa chọn. Các tham số đã lựa chọn phải được cung cấp một cách tin cậy cho tất cả các thực thể trong miền.

b) Mỗi bên được xác thực phải được cung cấp các thừa số nguyên tố khác nhau sao cho khi biết được tích của chúng, tức là giá trị mô đun(một tham số bên được xác thực), thì việc tính được chúng sẽ là không khả thi đối với bất kỳ thực thể nào, tính khả thi được xác định bởi bối cảnh sử dụng của cơ chế.

c) Tất cả các thực thể trong miền phải thống nhất sử dụng một mã khối E_K, ví dụ một trong các thuật toán được quy định trong TCVN 12854-2[27] hoặc TCVN 11367-3[26]. Kích thước khóa được ký hiệu là u và kích thước khối được ký hiệu là v. u và v phải lớn hơn hoặc bằng 128 bit và u phải lớn hơn hoặc bằng v. Entropy cực đại của khóa bí mật K của mã khối E_K được lấy là v-1. Độ dài u của khóa bí mật K được tính toán từ một khóa bí mật x có độ dài v-1 sử dụng các hàm $f_0(u,x)$ và $f_1(u,x)$.

CHÚ THÍCH Dựa vào định nghĩa của $f_0(u,x)$ và $f_1(u,x)$, bit khóa đầu tiên của mã khối được lấy là 0 hoặc 1. Điều này đảm bảo tính độc lập của hai lần sử dụng khác nhau của mã khối trong giao thức.

d) Mỗi bên được xác thực và bên xác thực sẽ có các phương pháp để tạo ra các số ngẫu nhiên.

6.3 Tạo khóa

Một số, ký hiệu là α, cố định độ dài bit của giá trị modulo (modulus) *N*, tức là $2^{\alpha-1} < modulo < 2^{\alpha}$, tùy thuộc vào ngữ cảnh sử dụng cơ chế. Nó là một tham số miền. Độ dài bit của modulo phải được lựa chọn sao cho ước lượng độ phức tạp của thuật toán phân tích ra thừa số nhanh nhất.[8],[16] – thuật toán mà có thời gian chạy phụ thuộc vào kích thước của modulo *N* – là lớn hơn mức an toàn được yêu cầu.

Một số nguyên không âm, ký hiệu là *w*, phải được chọn sao cho *w* >2.*v*. *w* là một tham số an toàn và nó là tham số miền. *w* có độ dài theo bit là p_1 và phải được chọn sao cho ước lượng độ phức tạp của thuật toán nhanh nhất đã biết[7] – với thời gian chạy phụ thuộc vào kích thước của $|p_1|$ – là lớn hơn mức an toàn được yêu cầu.

Bên được xác thực A phải giữ bí mật hai thừa số nguyên tố lớn khác nhau của modulo N, ký hiệu là p_1 và p_2. Hai thừa số nguyên tố p_1 và p_2 phải được lựa chọn sao cho modulo N là không cân bằng với $|p_1| \ll |p_2|$.

a) Sinh hai số nguyên tố p_1 và p_2 sao cho

1) $|p_1|$ = w và gcd(e, $p_1 - 1$) = 1 với e là số mũ công khai. e phải được chọn đủ lớn để tránh tấn công Coppersmith[2] và phù hợp với giới hạn dưới Shamir[15]. Giá trị e = 11 có một số lợi thế thực hành.

2) $|p_2| = \alpha - w$

3) $|p_1 \times p_2| = \alpha$

b) Tính $N = p_1 \times p_2$ và $t = e^{-1} \, mod \, (p_1 - 1)$. Khóa công khai là (N, e) và khóa bí mật là (p_1, t). Khóa công khai được chứng nhận bởi cơ quan cấp chứng nhận.

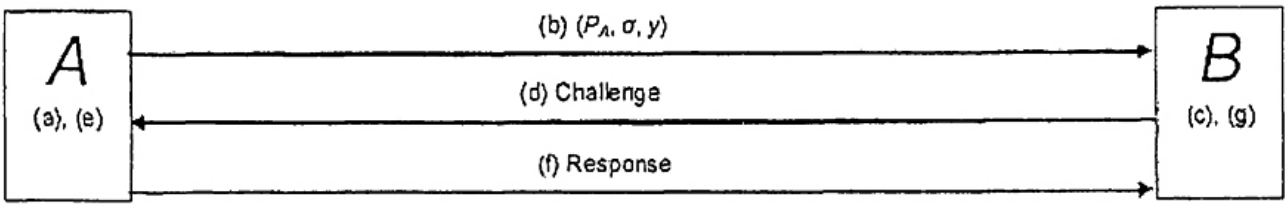
Bên được xác thực A phải được trang bị khóa bí mật $S_A = (p_1, t)$ và khóa công khai $P_A = (N, e)$ tương ứng với modulus N, xem [15].

Bên được xác thực A phải được trang bị một chứng chỉ khóa công khai P_A, ký hiệu là σ.

CHÚ THÍCH Cách chính xác mà bên được xác thực thu được bản sao khóa công khai tin cậy của nó nằm ngoài phạm vi tiêu chuẩn này. Ví dụ, nó có thể thu được bởi chứng chỉ khóa công khai hoặc bởi một số phương pháp khác phụ thuộc vào môi trường.

6.4 Trao đổi xác thực một chiều

Các chữ cái trong ngoặc ở Hình 2 tương ứng với các bước của cơ chế, bao gồm những sự trao đổi thông tin, được mô tả chi tiết bên dưới. Bên được xác thực ký hiệu là A. Bên xác thực ký hiệu là B.



Hình 2 – ALIKE

Thủ tục dưới đây phải được thực hiện. Bên xác thực B chỉ chấp nhận bên được xác thực A là hợp lệ nếu thủ tục hoàn thành thành công.

a) Một số k mới có độ dài v-1 phải được lựa chọn một cách ngẫu nhiên đều bởi bên được xác thực. Mã khối được sử dụng để tính cam kết y: y = $E_{f\_0(u,k)}(0)$

b) *A* gửi (P_A, σ, y) cho *B*

a) Một số mới r có độ dài v-1 được lựa chọn ngẫu nhiên đều bởi bên xác thực. Giá trị đệm thu được pad = $E_{f\_0(u,k)}(0)$ và thông điệp $(r \parallel pad)$ được mã hóa với P_A. Kết quả $d = (r \parallel pad)^e \bmod N$ là thách thức.

d) *B* gửi thách thức *d* cho *A*

e) Khi nhận được thách thức, các bước tính toán sau phải được thực hiện

1) Nếu kích thước của thách thức không bằng $|N|$, thủ tục thất bại.

2) A sử dụng khóa bí mật S_A để khôi phục lại bản rõ, $d^t \bmod p_1$, và xác thực tính thống nhất của phần đệm trong bản rõ:

i) Nếu phần đệm không đúng, thủ tục thất bại.

ii) Phần đệm được loại bỏ để khôi phục r

3) Một phản hồi D phải được tính toán bằng việc mã hóa số k sử dụng mã khối, tức là: $D = E_{f\_0(u,k)}(0 \parallel K)$

f) A gửi phản hồi D cho B

g) Khi nhận được phản hồi D, quá trình xác thực được thực hiện.

1) B xác thực rằng σ là bản sao tin cậy khóa công khai của bên được xác thực A

iii) Nếu xác thực ko thành công, và thủ tục thất bại.

iv) Ngược lại, B khôi phục k' từ phản hồi D.

2) Nếu $E_{f_{0(u,k')}}(0) = y$, thì thủ tục thành công. Ngược lại thủ tục thất bại.

6.5 Trích xuất khóa phiên

Một cách tùy chọn, khóa phiên có thể được thiết lập giữa bên được xác thực A và bên xác thực B để bảo mật thông điệp bằng cách sử dụng bí mật chung (r, k).

7 Cơ chế chữ ký dựa trên định danh

7.1 Tổng quan

Hệ thống mã hóa dựa trên định danh, là kỹ thuật mật mã phi đối xứng cho phép một khóa công khai được tính toán từ định danh và một tập các tham số toán học công khai và cho phép tính toán khóa bí mật tương ứng từ định danh, một tập các tham số toán học công khai, và giá trị bí mật trên toàn miền. Khóa công khai của người dùng có thể được tính toán bởi bất kỳ người nào mà có các tham số công khai cần thiết; trong khi bí mật mật mã là cần thiết để tính toán khóa bí mật của người dùng, và việc tính toán chỉ được thực hiện bởi máy chủ tin cậy có các bí mật đó.

Lược đồ chữ ký dựa trên định danh (IBS) có nền tảng là một lược đồ chữ ký trong đó việc xác thực chữ ký có thể được thực hiện mà không cần bên xác thực và người ký tương tác với nhau, hoặc trực tiếp hoặc qua proxy giống như một thư mục hoặc máy chủ chứng thực, trước khi xác minh các chữ ký. Các hệ thống khác có thể yêu cầu kết nối đến máy chủ cho mỗi lần xác thực.

Lược đồ[9] được mô tả dưới đây là lược đồ dựa trên định danh của Bellare, Namprepre và Neven[1], lươck đồ mà dựa trên lược đồ định danh Schnorr, nhưng tối ưu hơn. Bằng việc sử dụng các kỹ thuật được quy định trong Phụ lục B, Cơ chế chữ ký dựa trên định danh được nêu trong phần này có thể trở thành cơ chế rất hiệu quả cho các thiết bị hạng nhẹ.

CHÚ THÍCH Các chứng minh an toàn của cơ chế được mô tả dưới đây có trong [9].

7.2 Các yêu cầu an toàn đối với môi trường

Cơ chế IBS cho phép bên xác thực kiểm tra việc người ký sử dụng khóa ký của mình để tạo ra chữ ký cho một thông điệp cho trước.

Với một miền cho trước, các yêu cầu sau phải được thỏa mãn.

a) Các tham số miền mà chi phối hoạt động của cơ chế phải được lựa chọn. Các tham số đã lựa chọn phải được cung cấp một cách tin cậy cho tất cả các thực thể của miền.

b) Các tham số miền phải bao gồm đường cong elliptic E và một tập các tham số, cụ thể là điểm cơ sở P trên E, và cấp n của điểm P.

c) Mỗi điểm P được sử dụng như là cơ số cho logarit rời rạc trên đường cong elliptic phải thỏa mãn, với mỗi điểm J bất kỳ trên đường cong, việc tìm một số k trong khoảng [0, n-1] (nếu tồn tại), sao cho $J = [k]P$ là không khả thi về mặt tính toán, trong đó tính khả thi được xác định bởi ngữ cảnh sử dụng cơ chế.

d) Mỗi người ký và máy chủ tin cậy phải có các phương pháp để sinh ra các số ngẫu nhiên.

e) Tất cả các thực thể trong miền phải thống nhất sử dụng một hoàm băm kháng va chạm, ví dụ như một trong số các hàm băm được đặc tả trong TCVN 11816-3[23].

f) Máy chủ tin cậy phải lựa chọn ngẫu nhiên đều một số mới t , số này phải khác 0 và nhỏ hơn n, và việc tính toán điểm công khai T được thực hiện bằng cách lấy T là điểm nhận được qua phép nhân điểm cơ sở P với số t: $T = [t]P$.

g) Máy chủ tin cậy phải giữ số t như khóa chủ bí mật và khai báo đường cong E, điểm T, điểm cơ sở P, và số n như các tham số.

7.3 Tạo khóa

Người ký A phải hỏi máy chủ tin cậy để sinh khóa ký của mình. Với mỗi ứng dụng của cơ chế, các thủ tục sau phải được thực hiện bởi máy chủ tin cậy.

Máy chủ tin cậy phải lựa chọn ngẫu nhiên đều một số mới r khác 0 và nhỏ hơn n, và tính toán điểm $R = (x_R, y_R)$ với R được lấy là kết quả phép nhân của điển cơ sở P với số r.

$$R = [r]P$$

a) Một số s phải được tính toán từ số ngẫu nhiên r và khóa chủ bí mật của máy chủ tin cậy t.

$$s = r + h(x_R \parallel ID) \times t \bmod n$$

với h là hàm băm kháng va chạm và ID là xâu nhị phân biểu diễn định danh hoặc thông tin định danh của người ký A.

b) Khóa ký của người ký A là {R, S}

CHÚ THÍCH Khóa bí mật được sinh một cách đúng đắn sẽ thỏa mãn công thức sau: [s]P = R + [h($x_R \parallel ID$)]T

7.4 Ký

Để ký thông điệp có độ dài tùy ý m với khóa ký của người ký A, các thủ tục sau phải được thực hiện.

a) Người ký phải lựa chọn ngẫu nhiên đều một số mới y khác 0 và nhỏ hơn n.

b) Tính điểm $Y = (x_Y, y_Y)$ với Y là kết quả của phép nhân của điểm cơ sở P với số y.

$$Y = [y]P$$

c) Số z phải được tính toán từ khóa bí mật K và s.

$$z = y + h(x_Y \parallel x_R \parallel m) \times s \bmod n$$

d) Chữ ký của người ký A và thông điệp m là $\{Y, R, z\}$

7.5 Kiểm tra

Để kiểm tra chữ ký {Y, R, z} của người ký A với định danh ID đối với thông điệp m, bên xác thực phải tính:

$$c = h(x_Y \parallel x_R \parallel m)$$

và kiểm tra phương trình sau có đúng hay không:

$$[z]P = Y + [c]R + [\text{c x h}(x_R \parallel ID)]\text{T}$$

Bên xác thực sẽ đưa ra *đồng ý* nếu phương trình trên đúng hoặc *từ chối* nếu ngược lại.

8 Cơ chế xác thực một chiều dựa trên các logarit rời rạc trên đường cong elliptic trên trường hữu hạn có đặc số hai

8.1 Tổng quan

Cơ chế này, ELLI, được thiết kế để tạo ra mật mã phi đối xứng sử dụng được trên các thẻ RFID thụ động của các vùng lân cận (hoạt động với khoảng cách tới 1m) cho các ứng dụng chính được dự định bảo vệ thương hiệu/chống hàng giả trong các hệ thống phân tán lớn. Lược đồ ELLI và khái niệm để cài đặt nó trên thẻRFID thụ động được trình bày lần đầu tiên trong một bản đệ trình cho cuộc thi an toàn công nghệ thông tin của Đức được phát động bởi tổ chức Horst-Gortz năm 2006. Lược đồ này cũng được mô tả trong các tài liệu viện dẫn [30] và [31] (không sử dụng tên ELLI).

Khái niệm cơ bản ELLI có liên quan chặt chẽ với phiên bản Diffie-Hellman cho các đường cong elliptic trên trường F(2^g). Nhưng, do nó sử dụng một số giao thức đặc biệt và các bước tối ưu hóa tham số, nên nó được đặt tên riêng. Các tối ưu hóa bao gồm:

- Các y-tọa độ của các điểm trên đường cong elliptic không được sử dụng.

- Việc kiểm tra xem một phần tử trường cho trước có phải là x-tọa độ của một điểm trên đường cong elliptic đã khẳng định hay không được bỏ qua.

CHÚ THÍCH ELLI là viết tắt của ELLIPTIC LIGHT.

8.2 Các yêu cầu an toàn đối với môi trường

Lược đồ ELLI là cơ chế các thực một chiều dựa trên logarit rời rạc trên đường cong elliptic định nghĩa trên trường hữu hạn có đặc số hai. Nó cho phép bên xác thực kiểm tra rằng bên được xác thực biết logarit rời rạc trên đường cong elliptic của một điểm công khai được xác nhận gắn với điểm cơ sở.

Một nền tảng chung cho các kỹ thuật mật mã dựa trên đường cong elliptic được chỉ ra trong ISO/IEC 15946-1. Với cơ chế ELLI, một vài tính chất bổ sung của các đường cong elliptic xác định trên trường hữu hạn F(2^g) được sử dụng mà không được mô tả trong ISO/IC 15946-1. Các đặc điểm đó được trình bày bên dưới.

Với một miền cho trước, các yêu cầu sau phải được thỏa mãn. Các tham số miền chi phối hoạt động của cơ chế phải được lựa chọn.Các tham số đó bao gồm:

- Một trường hữu hạn có đặc số hai, F(2^g).

- Đường cong elliptic thông thường E xác định trên F(2^g). Đường cong E phải được cho bởi phương trình Weierstrass rút gọn: $Y^2 + XY = X^3 + aX^2 + b$ với $b \neq 0_F$, và phải được lựa chọn sao cho hai điều kiện sau được thỏa mãn:

  - # $(E) = 4q_1$ với q_1 là số nguyên tố;

  - # $(E_{twist}) = 2q_2$ với q_2 là số nguyên tố;

- Một điểm $P = (x_P, y_P)$ trên E sinh một nhóm con cấp q_1.

CHÚ THÍCH 1 Trong trường hợp này, điều kiện $q_1 < q_2$ tự động được thỏa mãn. Điều này là do thực tế rằng # (E) và # (E_{twist}) có cùng cấp độ lớn theo hệ quả của định lý Hasse-Weil (xem phụ lục F).

Kích thước của trường hữu hạn F(2^g) và các tham số của hai đường cong E và E_{twist} được lựa chọn theo cách mà sao cho việc giải quyết bài toán đường cong elliptic logarit rời rạc và bài toán Diffie-Hellman tĩnh trong cả E và E_{twist} là không khả thi về mặt tính toán.

Các tham số được lựa chọn phải được cung cấp, cho sự mở rộng cần thiết và theo cách đáng tin cậy tới tất cả các thực thể trong miền.

a) Mỗi bên được xác thực phải được cung cấp một khóa bí mật.

b) Mỗi bên được xác thực phải có khả năng thực hiện các phép toán cộng và phép toán nhân trong trường F(2^g).

c) Mỗi bên được xác thực phải có khả năng thực hiện hàm $MUL_{b,proj}$ được giới thiệu trong Mục 4, với mỗi giá trị b cụ thể có liên quan đến đường cong elliptic E.

d) Mỗi bên xác thực phải nhận được bản sao tin cậy của khóa công khai tương ứng với khóa bí mật của bên được xác thực

e) Mỗi bên xác thực phải được cung cấp một điểm cơ sở P trên đường cong elliptic E với q_1 là cấp của P.

f) Mỗi bên xác thực phải có khả năng thực hiện các phép toán cộng, phép nhân và phép chia trên trường F(2^g).

g) Mỗi bên xác thực phải có khả năng sinh một cách ngẫu nhiên các số nguyên dương < q_1.

h) Mỗi bên xác thực phải có khả năng thực hiện hàm $MUL_{b.aff}$ được giới thiệu trong Mục 4, với mỗi giá trị b cụ thể liên quan đến đường cong elliptic E.

CHÚ THÍCH 2 Có nhiều tùy chọn khác nhau để cung cấp cho các bên xác thực bản sao tin cậy khóa công khai của bên được xác thực. Điều này nằm ngoài phạm vi của tiêu chuẩn này.

8.3 Tạo khóa

Để tạo ra một cặp khóa, hai bước sau được thực hiện.

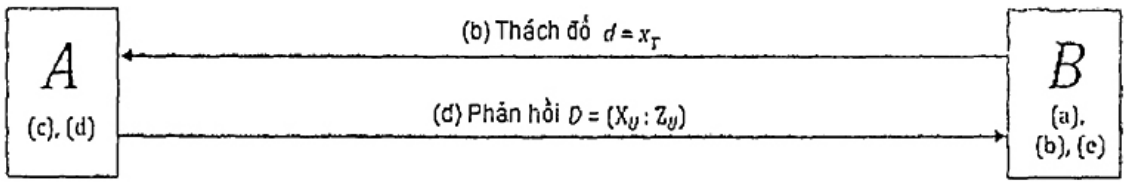
a) Bên được xác thực A phải lựa chọn ngẫu nhiên và đều một số nguyên Q từ tập {2, ...$q_1 - 1$}. Khóa bí mật của A là số nguyên Q.

b) Khóa công khai của A là $MUL_{b.aff}(Q, x_P)$, tức là x-tọa độ (affine) của điểm G = [Q]P = (x_G, y_G).

8.4 Cơ chế xác thực một chiều

Cơ chế này cho phép bên xác thực B xác thực bên được xác thực A, được tóm tắt trong Hình 3. Trong Hình 3, các chữ cái trong ngoặc từ a) đến e) tương ứng với các bước của cơ chế, bao gồm các trao đổi thông tin, được mô tả chi tiết bên dưới.

CHÚ THÍCH Cơ chế xác thực tuân theo cách tiếp cận "thách thức - phản hồi"



Hình 3 – ELLI

Các thủ tục dưới đây phải được thực hiện. Bên xác thực B chỉ chấp nhận bên được xác thực A là hợp lệ nếu thực hiện thành công thủ tục sau:

a) Bên xác thực lựa chọn ngẫu nhiên một số mới r với $0 < r < q_1$ và tính $MUL_{b.aff}(r, x_P)$ và $MUL_{b.aff}[r, G(A)]$, tức là x-toạ độ affine x_T của điểm $T = [r]P$ và x-tọa độ affine x_V của điểm $V = [r]([Q]P)$.

Thách thức d là phần tử trường $d = x_T$.

b) Bên xác thực gửi d cho bên được xác thực

c) Khi nhận được thách thức d, bên được xác thực A tính toán $D = MUL_{b,proj}(Q, d) = (X_U : Z_U)$, x-tọa độ xạ ảnh của điểm $U = [Q]T$, bao gồm hai phần tử trường X_U và Z_U trên trường F(2^g).

$D = (X_U : Z_U)$ là phản hồi

d) Bên được xác thực gửi D cho bên xác thực

e) Khi nhận được phản hồi D, bên xác thực B kiểm tra xem có xảy ra hoặc $X_U = 0_F$ hoặc $Z_U = 0_F$. Nếu một trong hai điều kiện xảy ra, bên được xác thực được xem là không hợp lệ.

Nếu $X_U \neq 0_F$ và $Z_U \neq 0_F$, bên được xác thực tính $x_V Z_U$ trên trường F(2^g) và kiểm tra xem phương trình $X_U = x_V Z_U$ có đúng trên trường F(2^g) hay không. Bên được xác thực được xem là hợp lệ nếu và chỉ nếu phương trình $X_U = x_V Z_U$ đúng.

Phụ lục A
(quy định)

Các định danh đối tượng

```
LightweightCryptography-4{
       iso(1) standard(0) lightweight-cryptography(29192)
       part4(4) asn1-module(0) algorithm-object-identifiers(0)}
       DEFINITIONS ::= BEGIN
EXPORTS ALL;

OID ::= OBJECT IDENTIFIER -- alias

-- Đồng bộ --

is29192-4 OID ::= {iso(1) standard(0) lightweight-cryptography(29192) part4(4)}

mechanism OID ::= {is29192-4 mechanisms(1)}

-- Cơ chế mật mã hạng nhẹ --

lw-discrete-logarithms-ecc-CryptoGPS OID ::= {mechanism
lw-discrete-logarithms-ecc-CryptoGPS(1)}
lw-authenticated-key-exchange-ALIKE OID ::= {mechanism
lw-authenticated-key-exchange-ALIKE(2)}
lw-identity-based-signature-IBS OID ::= {mechanism
lw-identity-based-signature-IBS(3)}
lw-unilateral-authentication-ecc-ELLI OID ::= {mechanism
lw-unilateral-authentication-ecc-ELLI (4)}

END
```

Phụ lục B
(quy định)

Kỹ thuật cân bằng tính toán bộ nhớ

Kỹ thuật sau có thể được sử dụng để đơn giản hóa việc tính toán lũy thừa hoặc phép nhân vô hướng. Các hoạt động này được sử dụng nhiều trong các cơ chế mật mã được quy định trong ISO/IEC, đặc biệt là dựa trên logarit rời rạc. Ví dụ, một vài cơ chế chữ ký quy định trong TCVN 12214-3[24] và ISO/IEC 9796-3[19], và các cơ chế xác thực thực thể trong TCVN 11817-5[21] có thể được thực hiện theo cách này. Bằng cách sử dụng kỹ thuật này, cơ chế chữ ký dựa trên định danh được trình bày trong phần 7 có thể trở thành cơ chế rất hiệu quả cho các thiết bị hạng nhẹ.

Kỹ thuật cân bằng của tính toán thuận tiện là sự gia tăng yêu cầu bộ nhớ.

Cho E là đường cong elliptic, P là điểm cơ sở trên đường cong E, và n là cấp của P.

Với mỗi i từ tập [0, |n| – 1], các điểm Y_i được đặt bằng phép nhân vô hướng của điểm cơ sở P với 2^i, tức là:

$Y_i = [2^i]$P

Để tính toán $Y = [y]P$ với một số y khác 0 mà nhỏ hơn n, thủ tục sau phải được thực hiện:

a) Đặt $Y = [0]P$

b) Với $i = 1$ đến |n| tính:

Nếu $y[i] = 1$ thì $Y = Y + Y_{i-1}$

c) Đưa ra Y.

Phụ lục C
(tham khảo)

Các ví dụ số

C.1 Cơ chế cryptoGPS

C.1.1 Tạo khóa

Đường cong elliptic *E* cho ví dụ này là đường cong *P*-192 xác định trên *FIBS PUB* 186-3[17]

$E: Y^2 = X^3 - 3X + b$ trên F_q

```
q =   FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFE FFFFFFFF FFFFFFFF

b =   64210519 E59C80E7 0FA7E9AB 72243049 FEB8DEEC C146B9B1
```

Điểm cơ sở *P* trên *E*

```
P =   (xP, yP)
  =   (188DA80E B03090F6 7CBF20EB 43A18800 F4FF0AFD 82FF1012,
       07192B95 FFC8DA78 631011ED 6B24CDD5 73F977A1 1E794811)
```

n là cấp của điểm cơ sở *P*

```
n =   FFFFFFFF FFFFFFFF FFFFFFFF 99DEF836 146BC9B1 B4D22831
```

Ví dụ này sử dụng hàm băm SHA-256, tức là hàm băm thứ tư đã quy định trong TCVN 11816-3[23].

Độ dài các thách thức theo bit $\delta = 40$ và $\sigma = |n| = 192$ bit.

C.1.2 Trao đổi xác thực

Khóa bí mật

```
Q =   4F1DF03A A32DCA02 652E83E7 E5FF5259 D61F5563 B3A0FA10
```

Điểm công khai

Ở biến thể đầu tiên, điểm công khai *G(A)* bằng với điểm ngược của điểm nhận được qua phép nhân điểm cơ sở *P* với số *Q*.

```
G(A) = – [Q]P
     = (xG, yG)
     = (D753BF14 9529BC23 B1850A37 57C4D34A 0D686A95 C3B03855,
        1656B8CB 2896BFD4 BC8F94A8 F3708741 B954CC44 4FC3951A)
```

Biến thể thứ hai, điểm công khai *G(A)* bằng điểm ngược của điểm nhận được qua phép nhân điểm cơ sở *P* với số *Q*.

```
G(A) = [Q]G
     = (xG, yG)
     = (D753BF14 9529BC23 B1850A37 57C4D34A 0D686A95 C3B03855,
        E9A94734 D769402B 43706B57 0C8F78BD 46AB33BB B03C6AE5)
```

Bước a

r là một xâu mới gồm các bit ngẫu nhiên có độ dài $\rho = \sigma + \beta + 80 = 192 + 40 + 80 = 312$ bit.

w là bằng chứng sao cho $W = EC2OSP_E([r]P, uncompressed)$

```
r =       05E8B1  E1121B08  FB9A0F58  FC1E932F  9CEFE94D  6298C223  40B5F04B
        554DCD2B  C812A76D  98F8BA3E

[h]P =  (DAD18D02  4B83E223  4C0F5FFF  B51C15B7  1D52CF92  B35358CF,
         FFE42756  843D0DF8  F3166971  E8AF6E22  6FD381B0  A816720F)

W =           04  DAD18D02  4B83E223  4C0F5FFF  B51C15B7  1D52CF92  B35358CF
        FFE42756  843D0DF8  F3166971  E8AF6E22  6FD381B0  A816720F
```

Bước b

$TokenAB_1 = h(W \parallel Text)$ với trường văn bản *Text* là rỗng. Từ đó, $TokenAB_1 = h(W)$.

```
h(W) =  0EB01E5E  32CA889D  099C8F6E  4CC3CB08  A3CD6008  C2849B43  0E07BCC7
        B5241843
```

Bước c, d

Thách thức của bên xác thực

```
d =           2D  F0F5B4F2
```

Bước e,f

Biến thể đầu tiên, phản hồi thách thức, $TokenAB_2$ là $D = r + d \times Q$.

```
D =       5E8B1  E1121B08  FB9A0F67  2ED9CE48  044BD618  3242087C  ADDDA392
        F2CA1F36  FDD94248  E8485D5E
```

Biến thể thứ hai, phản hồi thách thức $TokenAB_2$ là D = r - d x Q.

```
D =       5E8B1  E1121B08  FB9A0F4A  C9635817  3593FC82  92F578C9  D38E3D03
        B7D17B20  924C0C92  49A9171E
```

Bước g

Kiểm tra

```
W' =          04  DAD18D02  4B83E223  4C0F5FFF  B51C15B7  1D52CF92  B35358CF
        FFE42756  843D0DF8  F3166971  E8AF6E22  6FD381B0  A816720F

h(W') = 0EB01E5E  32CA889D  099C8F6E  4CC3CB08  A3CD6008  C2849B43  0E07BCC7
        B5241843
```

Xác thực là hợp lệ.

C.2 Cơ chế ALIKE

Các tham số của ALIKE được lựa chọn với 80 bit an toàn.

Kích thước bit cho modulus *N* là 1280 bit và 352 bit cho p_1.

Mã khối E_K được lựa chọn từ TCVN 12854-2[27] hoặc TCVN 11367-3[26]. Trong ví dụ này, nó là mã khối AES với kích thước khóa *u* là 128 bit.

CHÚ THÍCH Từ đó AES có kích thước khối là 128 bit, trong ví dụ này *u* và *v* bằng nhau .

C.2.1 Tạo khóa

e = 0000000B

p_1 = DD30D446 E32767CF E14885E7 44D077D0 89F82A87 37F53C4D 36AA9463
7C250E7D A516CA16 15C3B394 2B1CA791

p_2 = B544FE3B FB7D54D3 FA19B2E6 275CD79E B09CC643 44C03C6C 268F3624
5989FECC F44EC445 72A1F3C6 CD245A4D 4D17FDEC 0BF550D3 39C14EE8
4893CF1A 1E9BAF91 341AC6A9 E8B337B1 6B13B3A0 DF31E1A5 E5D63E70
0B93030D BDAF9D6B AFDBD696 6C1F09A0 95FA383C 32272D88 77A3F8FD

N = $p_1 \times p_2$
= 9C9F22B8 C7999ED9 54E7F600 63D134AB 6AF4BA29 046C2048 C7C0BC70
07686209 092D5B0B BE6E2D88 2E76E9B2 D2A43371 29490102 2401CCE7
A0143B96 13B1727B BC704892 F22B9EE6 A0C1F377 03229588 2EAC4879
3D88C4B3 800F5021 BAC0884C A05EA932 38FD8D35 50F227C6 8DB51EFE
A8051C08 8D475FC4 9A563C02 9616FDD0 650C5B66 ED2E1EFD 84732F70
F6F1A24A D5F88B5D 19864A5D 75F9124D

t = C9151E11 E5C6BB77 29E4D6D2 3E8EF88F 091026A9 78B0655D 7783CCB7
8821B015 21B7A071 2B0F0058 27315283

C.2.2 Trao đổi xác thực

Bước a, b

k là một xâu mới gồm các bit ngẫu nhiên có độ dài u-1 được sử dụng để tính toán cam kết y.

k = 6C64D272 0B770A23 D5700C0B EBC63E5E

y = $E_{f\_0(k)}(0)$
= E85D2E05 D4C6592B E571EE71 9BA636E7

Bước c, d

r là một xâu mới gồm các bit ngẫu nhiên có độ dài u -1.

r = 6E5707FA 1F9171C1 D802C92C 605A3FD1

$1 \| r$ = EE5707FA 1F9171C1 D802C92C 605A3FD1

$pad = HE(r)$ với $HE(r)$ bằng L = 128 bit bên trái nhất của $E_{f\_1(r)}(0)$.

pad = B8C940AE B22FDB93 7A1FE295 1584A26C

Thách thức của bên xác thực

$d = (r \| pad)^e \bmod N$

= 18240256 E10CFD25 725AD87B 7EBAFB43 81988968 B7D35E4F 6D75A201
6480DFA6 B5E4E78A EDE764E7 49CB5880 4BFA2A81 088ECFB3 3903AA0F
31E3CE42 C653CA28 4F418EED F76D6914 D6B40C9B 205A00E5 6C8008AC
13FFD2F1 CA57FB8A B6B57001 A5E3B04D BBE14BB5 D5200511 20F744E4
9B87B87E 7F411F3D 4657E4AF A26E6D0B F4414095 816D90CD 06CF6EE5
6C244F17 F30CDB58 C6226D80 AEDC70F4

Bước e, f

Phản hồi thách thức:

$D = E_{(z_{A,n})}(0 \| k)$

= 01203402 350C0611 F34C71BF 59F9CC3E

Bước g

Kiểm tra.

C.2.3 Trích xuất khóa phiên

Một cách tùy chọn, một khóa phiên s_k có thể được thiết lập.

$s_k = r \oplus k$

= 0233D588 14E67BE2 0D72C527 8B9C018F

C.3 Cơ chế chữ ký dựa trên định danh

C.3.1 Quá trình tạo khóa

Đường cong elliptic cho ví dụ này là:

$E: Y^2 = X^3 + aX + b$ trên F_q

với

a = FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF 7FFFFFFC

b = 1C97BEFC 54BD7A8B 65ACF89F 81D4D4AD C565FA45

q = FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF 7FFFFFFF

Điểm cơ sở P trên E.

$P = (x_P, y_P)$

= (4A96B568 8EF57328 46646989 68C38BB9 13CBFC82,
23A62855 3168947D 59DCC912 04235137 7AC5FB32)

n là cấp của điểm P

n = 1 00000000 00000000 0001F4C8 F927AED3 CA752257

t là khóa chủ bí mật.

t = D21DF3A7 5787F180 5F00792F 9D8C317C 23FDF91B

T là điểm công khai

$T = (x_T, y_T)$

= (1B2F7E1F 831DF943 F82CF8E2 FF753A4C 9DF8040A,
1FFE799A 563024AF 86652027 CEA9A60A 00E1FB73)

ID là thông tin định danh của người ký. $|ID| = 8$ bit.

ID = 01

r là số mới nhỏ hơn n

r = 8A29A77B 8826FC67 2ABEA882 FEAEE9C3 6E1A78C2

R = $[r]P$
= (x_R, y_R) with $|x_R| = |y_R|$ = 160 bits
= (1040E9BF 14546E1B 38FC74B5 31228C69 AF0BAED3,
8DC50619 E3B28AEC B8296F17 51466289 D32053F6)

Ví dụ này sử dụng hàm băm SHA-1, tức là hàm băm thứ ba được quy định trong TCVN 11816-3[23].

s = $r + h(x_R \| ID) \times t \bmod n$
= 49952E7E 4289DFA8 CE6ADB2F 55BA9C70 D89AA3C7

C.3.2 Ký

C.3.2.1 Ví dụ 1

m là một thông điệp 160 bit

m = 00000000 00000000 00000000 00000A73 199606B1

Bước a

y là nột số mới nhỏ hơn n

y = 00000000 00000000 00000000 00000000 00000007

Bước b

Y = $[y]P$
= (x_Y, y_Y) with $|x_Y| = |y_Y|$ = 160 bits

x_Y = 7A7F99D5 6472F619 577C4E8C 9B3A35E9 61472188

Bước c, d

z = $y + h(x_Y \| x_R \| m) \times s \bmod n$
= 92D28A45 FFDE887E C8D297A2 7FA02CB5 7DF2CBAF

C.3.2.2 Ví dụ 2

Thông điệp:

m = 00000000 00000000 00000000 00000A79 19B70693

Bước a

y là một số mới nhỏ hơn n.

y = 00000000 00000000 00000000 00000000 00000010

Bước b

Y = $[y]P$
= (x_Y, y_Y)

x_Y = B32F7DFA 2A82B99B 5CAC2772 AA6661BE 5F315034

Bước c

z = $y + h(x_Y \| x_R \| m) \times s \bmod n$
= BB7A0E5A 805F67A6 CF00FF5A 0BF8B782 0803751E

C.3.3 Kiểm tra

C.3.3.1 Ví dụ 1

$c = h(x_Y \| x_R \| m)$
$= 043969EF\ \ 9D9C6429\ \ 495139BD\ \ 8B37E086\ \ FAA78FF8$

$[z]P = (x_{[z]P}, y_{[z]P})$ với

$x_{[z]P} = 88913D78\ \ 4FD959FF\ \ 91E14157\ \ D44799FA\ \ 674B2717$

C.3.3.2 Ví dụ 2

$c = h(x_Y \| x_R \| m)$
$= F8228399\ \ 413773F9\ \ EB23CCA0\ \ DFD1D416\ \ D50941B7$

$[z]P = (x_{[z]P}, y_{[z]P})$

với

$x_{[z]P} = E0B100B3\ \ 1CA6F0E7\ \ 251275A7\ \ 8B5F0BFB\ \ C6207A29$

C.4 Cơ chế ELLI

C.4.1 Các ví dụ dựa trên ELLI_163.1

C.4.1.1 Các tính chất chung

Đường cong elliptic ELLI_163.2 và trường cơ bản $F(2^g)$ được xác định trong phụ lục E.1. Các ví dụ số dưới đây dành cho lược đồ xác thực ELLI, bao gồm các bước sinh khóa, sinh thách thức và sinh phản hồi.

Điểm cơ sở *P* được sử dụng chung trong tất cả các ví dụ của ELLI_163.1.

ĐIỂM CƠ SỞ P	
x_P	6 2DAE88E2 17BEFF09 F408E8F8 91EC8E51 05C9E8AB
y_P	0 5B29A42D C1EBEB2D 14AC1914 421FC4AC 2B61C7E5
CHÚ THÍCH Tọa độ-y y_P của điểm cơ sở P không cần thiết sử dụng trong cơ chế ELLI.	

C.4.1.2 Ví dụ 1

Một cặp khóa cho bên được xác thực được tạo ra.

SINHCẶP KHÓA	
KHÓA BÍ MẬT Q	DFCAC3BC 9A1E4B54 E03FAD6E E932F3BC 61170C51
KHÓA CÔNG KHAI G(A)	2 33C2A2B8 8BEE7DD9 1DB430F9 161B0A88 B7FEB527

Một thách thức *d* được sinhra bởi bên xác thực với đầu vào là số ngẫu nhiên *r* và tọa độ x_P của điểm cơ sở và sử dụng hàm $MUL_{b,aff}(r, x_P)$.

$$d = MUL_{b,aff}(r, x_P)$$

Phản hồi D được sinhra bởi bên được xác thực với đầu vào là thách thức d và khóa bí mật Q sử dụng hàm $MUL_{b,proj}$.

$$D = \left(X_v : Z_v\right) = MUL_{b,proj}(Q,d)$$

SINH THÁCH THỨC $d = MUL_{b,aff}(r, x_P)$	
SỐ NGẪU NHIÊN r	93D4625C 890DE3CD 8889225C 180E03C3 DF647545
THÁCH THỨC d	5 3735DD9D 700B0617 D6B0FE8E B0BA11D8 65D9532F
PHẢN HỒI CÓ KHẢ NĂNG $D = (X_U : Z_U)$	
GIÁ TRỊ-X X_U	3 F625D290 2FE3297F A177959A AD59AA0B 9D913C07
GIÁ TRỊ-Z Z_U	0 447352DD 05B0568B 191865A5 1FA0779C DD81258D
$x_V = X_U Z_U^{-1}$	4 531ADD58 617220E6 4A3915D5 6BCD69FD F434A2F2

CHÚ THÍCH Cặp $(X_U : Z_U)$ là "tọa độ xạ ảnh x", và từ đó không có một giá trị số cụ thể nào. Giá trị số duy nhất được thêm vào có liên quan đến thách thức là tọa độ affine x $x_V = X_U Z_U^{-1}$. Nó xảy ra cho tất các các ví dụ dưới đây.

C.4.1.3 Ví dụ 2

SINH CẶP KHÓA	
KHÓA BÍ MẬT Q	DE5A6D34 F3A8C4E1 6E132FD4 33F4B4BD 65E20CB9
KHÓA CÔNG KHAI $G(A)$	3 E8462A29 41BB3D71 433AEB2C 67877D4B 88D5529D
SINH THÁCH THỨC $d = MUL_{b,aff}(r, x_P)$	
SỐ NGẪU NHIÊN r	F9B6C01B CD3A85A8 99986F79 F4AFD289 056A3842
THÁCH THỨC d	61FE5AEC F245ECE4 B504CD65F E2D70C9C F28E6626
PHẢN HỒI CÓ KHẢ NĂNG $D = (X_U : Z_U)$	
GIÁ TRỊ-X X_U	3 8487B630 029D21C3 0768C095 B2AEF06B 63FE8143
GIÁ TRỊ-Z Z_U	0 19BF93D2 222E56E0 B8B50A7D B9C41150 B9E9F93C
$x_V = X_U Z_U^{-1}$	3 0DFD2997 2FD32C61 7356C895 D6912240 02752BFE

C.4.1.4 Ví dụ 3

SINH CẶP KHÓA

KHÓA BÍ MẬT Q	7E96501F 876C785B 1511893E 97F1E923 0967945E
KHÓA CÔNG KHAI *G(A)*	0 2F18219C DD1FEBA1 64FB2B1E 805CF6F7 D65C15F7
SINH THÁCH THỨC $d = MUL_{b,aff}(r, x_P)$	
SỐ NGẪU NHIÊN *r*	E3F72EA8 DF9A7E56 3039CBB3 745C14F9 759E40CF
THÁCH THỨC *d*	6 9EC45765 264CBA69 BBA3F698 789B06DF 26578B02
PHẢN HỒI CÓ KHẢ NĂNG $D = (X_U : Z_U)$	
GIÁ TRỊ-X X_U	0 5EE19683 164ABCDC F021A091 8046AA5B 56C6B128
GIÁ TRỊ-Z Z_U	2 15B2A8AB 8CFCF47D E173C38A A6BB8F0E 46B19463
$x_V = X_U Z_U^{-1}$	7 6F2BC182 34FDAD56 743C0387 90CEC425 54A5BD25

C.4.2 Các ví dụ dựa trên ELLI_193.1

C.4.2.1 Các thuộc tính chung

Đường cong lliptic ELLI_193.1 và trường cơ bản $F(2^g)$ được xác định trong phụ lục E.4. Các ví dụ số cho lược đồ xác thực ELLI được đưa ra bên dưới, bao gồm các bước sinh khóa, sinh thách thức và sinh phản hồi.

Điểm cơ sở *P* được sử dụng chung trong tất cả các ví dụ của ELLI_193.1.

ĐIỂM CƠ SỞ *P*	
x_P	1 C035F1CF E40C8BC6 B09F59E5 60953526 BB67E2A9 1CCD97B3
y_P	1 C848D5FF 00F24C02 63DB3036 3550F134 83769167 68EB72F5
CHÚ THÍCH Tọa độ y y_P của điểm cơ sở P không cần thiết được sử dụng trong cơ chế ELLI.	

C.4.2.2 Ví dụ 1

Một cặp khóa cho bên được xác thực được tạo ra.

SINH CẶP KHÓA	
KHÓA BÍ MẬT Q	12A4B91B 45E0E29E 54717EB7 3149B344 260DB6C5 85829BA1
KHÓA CÔNG KHAI *G(A)*	0 D74E3E63 ABECFFB7 4A57BC37 F0BBA4C2 A9436EF6 2C0C3331

Một thách thức *d* được sinh ra bởi bên xác thực với đầu vào là số ngẫu nhiên *r* và tọa độ x_P của điểm cơ sở và sử dụng hàm $MUL_{b,aff}(r, x_P)$.

$$d = MUL_{b,aff}(r, x_P)$$

Phản hồi D được sinh ra bởi bên được xác thực với đầu vào của hàm $MUL_{b,proj}$ là thách thức d và khóa bí mật Q.

$$D = \left(X_U : Z_U\right) = MUL_{b,proj}(Q,d)$$

SINH THÁCH THỨC $d = MUL_{b,aff}(r, x_P)$	
SỐ NGẪU NHIÊN r	3B5E7757 6B069EBC 757E6D99 366255E8 64EE6E64 BA8D4318
THÁCH THỨC d	1 342322E0 A5A77B74 92886779 09545939 E590A632 9FF797FD
PHẢN HỒI CÓ KHẢ NĂNG $D = (X_U : Z_U)$	
GIÁ TRỊ-X X_U	1 3FE539BC 35CAC440 9A30AAAC 9B416E09 44EBBEF8 ED42C259
GIÁ TRỊ-Z Z_U	1 8FA597E9 D28CA94D 98C2872B D31D1297 8DEE3580 CC66DFCE
$x_V = X_U Z_U^{-1}$	0 E1F66999 BE367042 C851A9E7 33B6A0CE 708C6165 1E6F0F7B

C.4.2.3 Ví dụ 2

SINH CẶP KHÓA	
KHÓA BÍ MẬT Q	610C5354 FADFB86E 2893DDC8 D864416F 8E85FFC3 EFC430B2
KHÓA CÔNG KHAI $G(A)$	1 7AF97A22 51AF656C 054D4F8F D29AAA31 DEF9148B D1B62940
SINH THÁCH THỨC $d = MUL_{b,aff}(r, x_P)$	
SỐ NGẪU NHIÊN r	47B631CF 510FE318 3D4CE47E 42A7F97B 70B3FD05 E9AEB4BE
THÁCH THỨC d	1 48BC609E ECE1EE7A 448900D6 5B2312A2 BB6928EC A7E21FC8
PHẢN HỒI CÓ KHẢ NĂNG $D = (X_U : Z_U)$	
GIÁ TRỊ-X X_U	1 21A6A15C 09345264 811AD857 6833CAEB 4D1AA265 AB8E3E94
GIÁ TRỊ-Z Z_U	0 9D64B2AF 1B5232E7 091B5D9A 9D3A7914 A28EA572 5B760D66
$x_V = X_U Z_U^{-1}$	1 0321B38B 4EEFC4B3 A08107E7 D1159CC2 965D3DEC F509A71F

C.4.2.4 Ví dụ 3

SINH CẶP KHÓA	
KHÓA BÍ MẬT Q	63825DA5 88BEDD37 3BFE2F2C 9E1E022D 32087314 4401AAD2
KHÓA CÔNG KHAI	1 D37D06DC 331EB141 03ABFBDD 4BACF334 10EDD836 F79CED32

G(A)	
SINH THÁCH THỨC $d = MUL_{b,aff}(r, x_P)$	
SỐ NGẪU NHIÊN *r*	69F78993 92558F1A D85A0D9B 853A7880 3F022000 4b28814C
THÁCH THỨC *d*	0 37D725B7 DB2A168E 9E52BE09 014A3AC3 8B2F802C B8808050
PHẢN HỒI CÓ KHẢ NĂNG $D = (X_U : Z_U)$	
GIÁ TRỊ-*X* X_U	1 94F6B90F D19DF28C A91FF7E0 B201F02E E0D4DC31 7BF187AF
GIÁ TRỊ-Z Z_U	1 756CEDB1 5052992A 4CD47C22 84487603 FD95FC75 A0BF197E
$x_V = X_U Z_U^{-1}$	0 74C9F956 B4E4E893 98A70D23 9C119D7A DE9D5D50 740CD1B7

Phụ lục D
(tham khảo)

Các điểm đặc trưng

Phụ lục này mô tả các đặc trưng hạng nhẹ của các thuật toán được đề cập trong tiêu chuẩn này và sự tuân thủ các yêu cầu trong TCVN XXX-1. Trong phụ lục này, cơ chế IBS là cơ chế đã mô tả ở Điều 7 được cài đặt với kỹ thuật đưa ra trong Phụ lục B.

Bảng D.1 – Sự tuân thủ các yêu cầu trong TCVN XXX-1 của các đặc trưng của các cơ chế

		Tên thuật toán				
		cryptoGPS[5]	ALIKE[3]	IBS[9]	ELLI_163.1	ELLI_193.1
Các ràng buộc	Diện tích chip	X			X	X
	Năng lượng tiêu thụ	X		X	X	X
	Kích thước chương trìnhvà kích thước RAM		X	X	X	X
	Băng thông liên lạc	X	X	X	X	X
	Thời gian thực thi	X	X		X	X

Bảng D.2 – Các đặc trưng cryptoGPS

	cryptoGPS[5]		
	Tính toán chính	Tính toán chính	Mô đun (Tính toán) đầy đủ
Độ an toàn [bit]	80	80	80
Diện tích chip [GE]	317	431	2876
Tiến trình xác thực [CLK]	1088	136	724
Năng lượng [GE*CLK]	344896	58616	2082224
Kỹ thuật [μm]	0,180	0,180	0,350
CHÚ THÍCH "Mô đun đầy đủ" bao gồm các quá trình sinh số giả ngẫu nhiên với việc tính toán trên thẻ cryptoGPS trong đó "tính toán chính" chỉ đề cập đến việc tính toán trên thẻ.			

Bảng D.3 - Các đặc trưng ALIKE

	ALIKE[3]	
	Tiến trình PICC[a]	Tiến trình PCD[b]
Độ an toàn [bit]	80	80
Hàm đồng bộ hóa mật mã	Yêu cầu phép nhân vô hướng	Không yêu cầu
Yêu cầu của các hàm	Một bộ sinh số ngẫu nhiên. Hai mã khối thực thi mà không cần kênh kề cụ thể và các phép đo chống lại các tấn công. Một lũy thừa mô đun với mudulo nhỏ ($\|p_1\| = 352$ bit)	Một bộ sinh số ngẫu nhiên. Hai mã khối thực thi. Một lũy thừa mô đun với số mũ nhỏ ($e \geq 11, \|N\| = 1248$ bit)
Bộ nhớ bất biến (bộ nhớ điện tĩnh)	Để lưu trữ các khóa RSA của ALIKE (88 byte để so sánh với 400 byte của RSA cổ điển) và các chứng chỉ	Để lưu trữ khóa công khai của CA
Kích thước chương trình	1.6 kbyte trên 8051 lõi	
Dữ liệu được truyền với tốc độ truyền 106.kb.s^{-1}	Dữ liệu đang truyền 160 byte ⇔ 15.40 ms	Dữ liệu đang truyền 192 byte ⇔ 18.8 ms
Tiến trình bên trong	Từ 4 đến 15 nhanh hơn RSA cổ điển tùy theo thành phần Ví dụ cho 8051 lõi: 80 ms là 31MHz cho CPU và 48 MHZ cho bộ đồng bộ hóa mật mã	

[a] PICC: Thẻ tích hợp vi mạch không tiếp xúc

[b] PCD: Thiết bị ghép đôi không tiếp xúc

Bảng D.4 – Các đặc trưng IBS

IBS[9]		
Mức an toàn [bit]		80
Kích thước chương trình và	Chỉ ký trực tuyến	flash = 54308

kích thước RAM [Byte] Nó dựa trên TinyOS 1.0.15 trên Micaz		RAM = 858
	Chỉ kiểm tra	flash = 55374 RAM = 922
Thời gian thực thi [ms]	Chữ ký	896
	Kiểm tra	5610
Năng lượng tiêu thụ [μJ] Nó dựa trên Micaz Atmel128L	Ký trực tuyến	12370
	Kiểm tra	77400
Băng thông liên lạc [bit]		480

Bảng D.5 – Các đặc trưng ELLI

		ELLI_163.1	ELLI_193.1
Độ an toàn [bit]		80	80
Diện tích chip [GE] dựa trên mẫu thử phần cứng my-d-ECC[30]	Tổng số mô đun ELLI	12876	xấp xỉ 15000
	Lưu trữ	5273	xấp xỉ 6243
	Đơn vị toán học + điều khiển lô gic	6171 + 1432 = 7003	xấp xỉ 8750
Tiến trình xác thực [CLK] dựa trên mẫu thử kiến trúc phần cứng my-d-ECC (163 bit)[30]		80645	xấp xỉ 95000
Năng lượng tiêu thụ [μJ]		7,5	xấp xỉ 10,5
Dữ liệu trên đường truyền [bit]		3 x 163	3 x 193

CHÚ THÍCH 1 Với đường cong ELLI_163.1, dữ liệu trong Bảng D.5 được dựa trên mẫu kiến trúc phần cứng được mô tả trong viện dẫn [30]. Các giá trị của ELLI_193.1 được ngoại suy một phần dựa trên các kết quả của viện dẫn [30] với giả định cách tiếp cận kiến trúc phần cứng là tương tự.

CHÚ THÍCH 2 Dựa trên thuật toán Pollard-Rho để tính logarit rời rạc, ta có thể lập luận rằng độ an toàn của các thực thể trên hai hàng nên được đặt tương ứng từ 81 đến 95. Nhưng, theo TCVN 12854, các thực thể được cho phép lại bị giới hạn bởi các giá trị 80, 112, 192, và 256.

CHÚ THÍCH 3 Với các thực thể trong hàng 2 của Bảng 5, các tấn công yêu cầu một số lượng lớn các truy vấn của thuật toán và một số lượng lớn bộ nhớ không được xem xét, ví dụ như vượt quá 2^{34} lượt truy vấn và kích thước lưu trữ 2^{64}. Nếu số các truy vấn tới các thiết bị được cho phép là $2^{34,3}$ và kích thước lưu trữ là 2^{34} được giả định là có sẵn cho các tấn công, thì mức an toàn bị giảm xuống đến 72 trong trường hợp ELLI_163.1. Xem mục G.3.

Phụ lục E
(quy định)

ELLI_163.1 và ELLI_193.1

E.1 Tổng quan

Phụ lục E quy định hai đường cong elliptic – ELLI_163.1 và ELLI_193.1 – mà được sử dụng trong cơ chế ELLI. Thêm đó, phụ lục này đưa ra các thông tin cần thiết cách tạo ra một tập đầy đủ các tham số miền.

Độ an toàn đường cong elliptic ELLI_163.1 là $\sim 2^{80}$ đối với bài toán ECDL. Giá trị trương ứng cho ELLI_193.1 là $>2^{95}$.

E.2 Mô tả của trường $F(2^g)$ và các phần tử của nó

Trường $F(2^g)$ được cho như $F(2)[X]/f(X)$, với $f(X)$ là đa thức bất khả quy bậc g trên trường F(2). Ở dạng này, các phần tử của $F(2^g)$ là các đa thức $b_{g-1}X^{g-1} + b_{g-2}X^{g-2} + \cdots + b_1X + b_0$, với $b_i \in \{0,1\}$.

Các phần tử $(b_{g-1}, b_{g-2}, \ldots, b_1, b_0)$ của trường $F(2^g)$ được biểu diễn dưới dạng các xâu thập lục phân, như trong ISO/IEC 15946-1.

E.3 ELLI_163.1 và các tham số có liên quan

Các tham số dưới đây sẽ được sử dụng với đường cong ELLI_163.1.

$f(X)$	=	$X^{163} + X^{17} + X^6 + X + 1$
	=	8 00000000 00000000 00000000 00000000 00020043
a	=	0_F
b	=	7 640BFEA7 CC3B22CD 51B4217C 25A70C81 E7A7260A
$\#(E)$	=	$4 \cdot q_1$
q_1	=	1 FFFFFFFF FFFFFFFF FFFEBD90 042B33A9 48E95823
$\#(E_{twist})$	=	$2 \cdot q_2$
q_2	=	4 00000000 00000000 000284DF F7A998AD 6E2D4F3B

CHÚ THÍCH 'a' không cần thiết được sử dụng trong cơ chế ELLI.

E.4 ELLI_193.1 và các tham số có liên quan

Các tham số dưới đây sẽ được sử dụng với đường cong ELLI_193.1.

$f(X)$	=	$X^{193} + X^{17} + X^{14} + X^{12} + 1$
	=	2 00000000 00000000 00000000 00000000 00000000 00025001
a	=	0_F
b	=	0 5BD20FC9 907A1E5F F4034D4A E883BDF7 5A8E05EA 5E41EC53
$\#(E)$	=	$4 \cdot q_1$
q_1	=	7FFFFFFF FFFFFFFF FFFFFFFF F38514E9 A5FB4D1E B499AF33
$\#(E_{twist})$	=	$2 \cdot q_2$
q_2	=	1 00000000 00000000 00000000 18F5D62C B40965C2 96CCA19B

CHÚ THÍCH 'a' không cần thiết được sử dụng trong cơ chế ELLI.

Phụ lục F
(tham khảo)

Một số điểm đặc trưng của đường cong elliptic trên trường $F(2^g)$

Phần lớn lược đồ ELLI dựa theo Diffie-Hellman tĩnh với các đường cong ellitic có các khóa của một trong hai thực thể giao tiếp được cố định. Cơ chế ELLI nằm ngoài hai các tiếp cận này.

- Lược đồ chỉ sử dụng tọa độ x của các điểm trên các đường cong elliptic trong đó toạ độ y hoàn toàn không được xem xét và không được sử dụng. (Điều này không bị nhầm lẫn với điểm nén).

- Không có việc kiểm tra xem có hay không việc đã gửi phần tử trường có chính xác là tọa độ x điểm nào đó trên đường cong đã sử dụng hay không.

Mục đích của Phụ lục này là mô tả nền tảng của hai đặc điểm đặc trưng của cơ chế ELLI. Nó được giả thiết rằng người đọc có đủ kiến thức cơ bản cần thiết về đường cong elliptic để hiểu việc sử dụng đường cong elliptic trên mật mã phi đối xứng.

Khẳng định 1: Cho E = $(E_{\{a,b\}})$ là đường cong elliptic thông thường trên $F(2^g)$. Tập điểm $(E_{\{a,b\}})$ là nhóm giao hoán hữu hạn có cấp $\#\left(E_{\{a,b\}}\right) = 2^g + 1 - t$, t là số nguyên lẻ với $|t| \leq 2\sqrt{2^g}$. Hơn nữa, tất cả các số lẻ t có thể nằm trong khoảng $-2\sqrt{2^g} \leq |t| \leq 2\sqrt{2^g}$ thực sự xuất hiện. (Tham số t được gọi là "vết của tự đồng cấu Frobenius").

Khẳng định 2: Cho E = $(E_{\{a,b\}})$ là đường cong elliptic thông thường trên $F(2^g)$ với $\#\left(E_{\{a,b\}}\right) = 2^g + 1 - t$. Tiếp đó, cấp của đường cong elliptic $E_{\{a',b\}}$ trên $F(2^g)$ với phần tử a' tùy ý thuộc $F(2^g)$, có chính xác hai khả năng:

Trường hợp (1): $\#\left(E_{\{a',b\}}\right) = \#\left(E_{\{a,b\}}\right) = 2^g + 1 - t$;

Trường hợp (2): $\#\left(E_{\{a',b\}}\right) = \#\left(E_{\{a,b\}}\right) + 2t = 2^g + 1 - t$.

Nền tảng toán học của luận cứ 2 có liên quan đến các khái niệm của đường cong elliptic đẳng cấu và các đường cong elliptic xoắn đôi, cụ thể là:

Cho $(E_{\{a,b\}})$ và $\left(E_{\{a',b\}}\right)$ là các đường cong elliptic thông thường trên trường hữu hạn $F(2^g)$ với phương trình Weierstrass $Y^2 + XY = X^3 + aX^2 + b$ và $Y^2 + XY = X^3 + a'X^2 + b'$ tương ứng. Các điều kiện sau thảo mãn:

- $(E_{\{a,b\}})$ và $\left(E_{\{a',b\}}\right)$ là đẳng cấu nếu và chỉ nếu $b' = b$ và $Tr(a') = Tr(a)$;

- $\left(E_{\{a',b\}}\right)$ và $(E_{\{a,b\}})$ là xoắn đôi nếu và chỉ nếu $b' \neq b$ và $Tr(a') \neq Tr(a)$;

- Trong trường hợp (1), đường cong $\left(E_{\{a',b\}}\right)$ là đẳng cấu với $(E_{\{a,b\}})$;

- Trong trường hợp (2), đường cong $\left(E_{\{a',b\}}\right)$ là xoắn đôi với $(E_{\{a,b\}})$.

CHÚ THÍCH 1 Chú ý của "đường cong elliptic đẳng cấu" ở đây được hiểu theo nghĩa phép đẳng cấu của các biến đại số, tức là không xem xét cấu trúc nhóm đã tạo ra trên đưuòng cong elliptic. Chú ý này của phép đẳng cấu là khác biệt và không nên nhầm lẫn với "các nhóm điểm của đường xong elliptic đẳng cấu như các nhóm hữu hạn".

CHÚ THÍCH 2 Kết quả đầu tiên của luận cứ 1 và luận cứ 2 là cấp của đường cong elliptic thông thường trên $F(2^g)$ luôn luôn là chẵn và nếu đường cong từ luận cứ 1 có cấp $\equiv 2\ modulo\ 4$, đường cong từ luận cứ (2) phải có cấp $\equiv 0\ modulo\ 4$, và ngược lại.

CHÚ THÍCH 3 Với lược đồ ELLI, đường cong elliptic được chọn sao cho cấp của cả hai kiểu đường cong có thừa số nguyên tố tốt nhất có thể: $\#\ (E) = 4 \cdot q_1$ và $\#\ (E_{twist}) = 2 \cdot q_2$ với q_1, q_2 là các số nguyên tố.

Khẳng định 3: Cho k là số nguyên dương tùy ý và cho *P* là một điểm trên đường cong elliptic thông thường ($E_{\{a,b\}}$). Sau đó, tọa độ *x* của k[P] là độc lập với tham số đường cong a và tọa độ y của điểm *P*. Nó chỉ phụ thuộc vào tham số đường cong *b* và tọa độ *x* của điểm *P*. (Xem chứng minh trong viện dẫn [28], trang 42).

Khẳng định 4: Cho *x* là phần tử tùy ý trên trường $F(2^g)$. b là một giá trị cố định trên trường $F(2^g)$, *x* luôn luôn là tọa độ x_R của điểm *P* trên đường cong elliptic thông thường nào đó trên trường $F(2^g)$ với tham số b, cụ thể:

- Hoặc *R* nằm trên đường cong đẳng cấu $E = (E_{\{a,b\}})$ hoặc

- *R* nằm trên đường cong xoắn đôi (E_{twist}) của E.

(Xem chứng minh trong tại liệu viện dẫn [28], trang 26 và 38).

Thông qua kết quả của các luận cứ trên, người ta có thể giới thiệu hai hàm $MUL_{b,proj}$ và $MUL_{b,aff}$ được sử dụng trong cơ chế ELLI.

$-\ MUL_{b,proj}\ (k, x_R) := (X_S : Z_S)$, nếu $S = [k]R = (X_S : Y_S : Z_S)$

- $MUL_{b,aff}\ (k, x_R) := X_S Z_S^{-1}$, nếu $S = [k]R = (X_S : Y_S : Z_S)$

Ở đây, k là số nguyên dương tùy ý; x_R là một phần tử trường và tọa độ afine x điểm R trên đường cong elliptic nào đó, cụ thể là hoặc trên $E = (E_{\{a,b\}}$ hoặc trên (E_{twist}) của E.

Phụ lục G
(Tham khảo)

ELLI - Các xem xét an toàn

G.1 Tổng quan

Trong phụ lục này, các tấn công khác nhau chống lại lược đồ ELLI được thảo luận và đánh giá. Việc đó dựa trên Diffie – Hellman tĩnh cho đường cong elliptic trên trường hữu hạn $F(2^g)$, Độ an toàn của cơ chế ELLI hoàn toàn phụ thuộc vào độ bền giả định của bài toán logarit rời rạc trên đường cong elliptic (ECDLP) cho các đường cong xác định trên trường $F(2^g)$. Bất cứ sự phát triển nào trong việc tấn công vấn đề này, và các vấn đề liên quan sẽ tự động ảnh hưởng đến độ an toàn của cơ chế ELLI.

G.2 Các tấn công dựa trên ECDLP

Tấn công rõ ràng nhất chống lại cơ chế ELLI là một nỗ lực để giải quyết bài toán ECDLP với khóa công khai cho trước G(A) với toạ độ x của một điểm nào đó trên nhóm cylic của số nguyên tố bậc q_1 sinh bởi điểm cơ sở P.

Tấn công tổng quát được biết đến nhiều nhất (thuật toán-ρ Pollard) yêu cầu $O(\sqrt{q_1})$ các phép toán trên nhóm điểm được sinh bởi điểm P. Với số nguyên tố q_1 trên đường cong elliptic ELLI_163.1 và ELLI_193.1 có độ dài 161 resp. 191 cuộc tấn công như vậy là không khả thi.

Tấn công MOV và tấn công Frey-Ruch biến đổi bài toán ECDL trên nhóm sinh bởi điểm P thành bài toán logarit rời rạc trên một trường mở rộng $F(2^{gj})$ của $F(2^g)$. Một điều kiện cần thiết cho tính khả thi của các tấn công này là bậc của nhóm điểm chia hết cho 2^{gj}-1, với j nhỏ. Đây không là trường hợp cho đường cong elliptic ELLI_163.1 và ELLI_193.1.

G.3 Các tấn công dựa trên bài toán Difie- Hellman tĩnh

Bên được xác thực A có thể đươợc xem xét như tiên tri Diffie – Hellman tĩnh. Nói đại khái, sau khi feed-in của một điểm R (trên đường cong E hoặc một đường cong xoắn đôi), nó cho ra bộ số [Q]R. Brown và Gallant biểu diễn trong tài liệu viện dẫn [29] thuật toán để tìm ra Q trong trường hợp này. Độ phức tạp của thuật toán phụ thuộc vào việc phân tích các số $q_1 - 1$ và $q_2 - 1$. Các tham số liên quan đến thuật toán ELLI_163.1 và ELLI_193.1, bao gồm cả các bậc của các đường cong xoắn đôi đều được lựa chọn theo một cách nào đó mà các tấn công dựa vào thuật toán Brown-Gallant hiện nay là không thể.

Cheon mô tả trong tài liệu viện dẫn [32] về mở rộng thuật toán Brown-Gallant mà cũng sử dụng việc phân tích hai số $q_1 + 1$ và $q_2 + 1$. Với đề xuất đường cho cong elliptic ELLI_163.1, thuật toán Cheon cần xấp xỉ 2^{32} câu truy vấn của thuật toán ELLI để xây dựng một cơ sở dữ liệu bao gồm 2^{64} các điểm trên đường cong elliptic. Với cơ sở dữ liệu này, khóa bí mật của thuật toán ELLI có thể được tính toán bằng xấp xỉ 2^{72} điểm bổ sung trên đường cong elliptic. Với ELLI_193.1, các dữ liệu tương ứng là: 2^{52} câu truy vấn của lược đồ ELLI, bộ nhớ để chứa 2^{71} các điểm trên đường cong elliptic, Độ phức tạp thời gian tính toán là 2^{79} các điểm bổ sung trên đường cong elliptic.

Dường như, kích thước bộ nhớ hiện tại là không cần thiết để cung cấp.

G.4 Các tấn công dựa trên đầu vào không hợp lệ hoặc yếu

Vì bên được xác thực không thực hiện bất kỳ đánh giá nào đối với các tham số đầu vào, nó có thể cung cấp cho bên được xác thực các tham số không hợp lệ hoặc yếu. Nếu thách thức không phải là tọa độ x của một điểm trên đường cong elliptic, thì nó là tọa độ x của một điểm trên một đường cong

xoắn đôi. Với đường cong elliptic ELLI_163.1 và ELLI_193.1, điều kiện $q_2 > q_1$ thảo mãn. Vì vậy, bài toán ECDL trên đường cong xoắn đôi khó hơn một chút so với bài toán ECDL trên E.

Nhóm điểm của E chứa một nhóm con bậc 4. Việc gửi tọa độ x của phần tử bậc 4 tới bên được xác thực đáp ứng ngay lập tức tiết lộ phần dư của Q modullo 4. Vì vậy, hai bit có trọng số thấp nhất của khóa bí mật Q phải được xem như là đã biết. Đây không phải là một tấn công liên quan nhưng là một tính năng thiết kế được chấp nhận.

Phụ lục H
(Tham khảo)

ELLI – Các tùy chọn cài đặt

H.1 Tổng quan

Trong phụ lục này, các tùy chọn khác nhau để cài đặt các hàm $MUL_{b,proj}$ và $MUL_{b,aff}$ được mô tả.

H.2 Thuật toán dựa trên Montgomery-ladder

Thuật toán này là một kết quả trực tiếp nên được gọi là "Montgomery-ladder". Thuật toán này sử dụng 5 biến X_S, Z_S, X_2, Z_2 và H (cho giá trị tạm thời).

Đầu vào:

- Một số nguyên dương k = $(k_g, \ldots, k_1)$, được biểu diễn dưới dạng nhị phân với $k_g = 1$;

- Tham số b;

- Phần tử trường x_R (thách thức).

Tính toán đầu ra:

a) $X_S \leftarrow 1_F, Z_S \leftarrow 0_F, X_2 \leftarrow x_R, Z_2 \leftarrow 1_F$;

b) với $i \leftarrow g$ giảm đến 1:

Nếu $k_i = 1$

$$H \leftarrow Z_S, Z_S \leftarrow (X_S Z_2 + X_2 Z_S)^2,$$

$$X_S \leftarrow x_R Z_S + X_S X_2 H Z_2, H \leftarrow X_2,$$

$$X_2 \leftarrow X_2^4 + b Z_2^4, Z_2 \leftarrow H^2 Z_2^2,$$

ngược lại

$$H \leftarrow Z_2, Z_2 \leftarrow (X_2 Z_S + X_S Z_2)^2,$$

$$X_2 \leftarrow x_R Z_2 + X_2 X_S H Z_S, H \leftarrow X_S,$$

$$X_S \leftarrow X_S^4 + b Z_S^4, Z_S \leftarrow H^2 Z_S^2,$$

$$(X_S : Z_S) := (X_S, Z_S).$$

Đầu ra:

— $MUL_{b,proj}(k, x_R) = (X_S : Z_S)$.

Nếu việc bảo vệ chống lại các tấn công kênh kề là một điểm đáng quan tâm, như bên được xác thực A, trong đó khóa bí mật có liên quan đến việc đánh giá $MUL_{b,proj}$, theo sau một phiên bản ngẫu nhiên hóa của thuật toán có thể được sử dụng để cài đặt $MUL_{b,proj}$. Trong trường hợp này, nhất thiết phải có các cách để tạo ra các phần tử trường ngẫu nhiên trên trường $F(2^g)$.

H.3 Thuật toán dựa trên Montgomery-ladder – Ngẫu nhiên hóa

Đầu vào:

- Một số nguyên dương k = $(k_g, \ldots, k_1)$, cho dưới dạng biểu diễn nhị phân với $k_g = 1$;

- Tham số b;

- Phần tử trường x_R (thách thức).

Tính toán đầu ra:

a) Chọn ngẫu nhiên một phần tử trường $\rho_1 \neq 0_F$

b) $X_S \leftarrow \rho_1, Z_S \leftarrow 0_F, X_2 \leftarrow \rho_1, Z_2 \leftarrow \rho_1$;

) với $i \leftarrow g$ giảm đến 1:

Nếu $k_i = 1$ thì

$$H \leftarrow Z_S, Z_S \leftarrow (X_S\ Z_2 + X_2\ Z_S)^2,$$

$$X_S \leftarrow x_R\ Z_S + X_S\ X_2 H Z_2, H \leftarrow X_2,$$

$$X_2 \leftarrow X_2^4 + b Z_2^4, Z_2 \leftarrow H^2\ Z_2^2,$$

ngược lại

$$H \leftarrow Z_2, Z_2 \leftarrow (X_2\ Z_S + X_S\ Z_2)^2,$$

$$X_2 \leftarrow x_R\ Z_2 + X_2\ X_S H Z_S, H \leftarrow X_S,$$

$$X_S \leftarrow X_S^4 + \mathrm{b} Z_S^4, Z_S \leftarrow H^2\ Z_S^2;$$

d) Chọn ngẫu nhiên một phần tử trường $\rho_2 \neq 0_F$

e) $X_S \leftarrow \rho_1 X_S,\ Z_S \leftarrow \rho_2 Z_S$

f) $(X_S : Z_S) := (X_S,\ Z_S)$

Đầu ra:

— $MUL_{b,proj}(k, x_R) = (X_S : Z_S)$.

CHÚ THÍCH Từ $MUL_{b,proj}(k, x_R) = (X_S : Z_S)$, ngay lập tức ta thu được $MUL_{b,aff}(k, x_R) = (X_S Z_S^{-1})$ sau khi thực hiện một phép chia trên trường $F(2^g)$.

H.4 Cách tiệm cận phép nhân điểm tiêu chuẩn

Thiết lập: Hai phần tử trường a và a' được lựa chọn sao cho Tr(a) ≠ $Tr(a')$. $E_{twist} = (E_{\{a',b\}})$ là đường cong xoắn với $E = (E_{\{a',b\}})$.

Đầu vào:

- Một số nguyên dương k;

- Tham số b;

- Phần tử trường x_R (thách thức).

Tính toán đầu ra:

1) Lựa chọn phương trình bậc 2: $y^2 + x_R y = x_R^3 + a x_R^3 + b$ và $y^2 + x_R y = x_R^3 + a' x_R^3 + b$ là có thể giải được và xác định một kết quả y_R.

CHÚ THÍCH Xem phụ lục F, luận cứ 4.

2) Đặt $R := (x_R, y_R)$.

CHÚ THÍCH R là một điểm hoặc trên E hoặc trên E_{twist}.

3) Lựa chọn $[k]R = (x_S, y_S)$ hoặc $[k]R = (X_S : Y_S : Z_S)$

CHÚ THÍCH Điều này có thể thực hiện bằng bất kỳ kỹ thuật nào để xác định kết quả của phép nhân điểm.

Đầu ra:

— $MUL_{b,proj}(k, x_R) = (X_s : Z_s) = (x_s : 1_F)$;

— $MUL_{b,aff}(k, x_R) = x_s = X_s (Z_s)^{-1}$.

Thư mục tài liệu tham khảo

[1] M. Bellare, C. Namprempre, and G. Neven, Security proofs for identity-based identification and signature schemes, in Proc. of Eurocrypt '04, Lecture Notes in Computer Science, Vol. 3027, pp 268-286, Springer-Verlag, 2004

[2] D. Coppersmith, Small solutions to polynomial equations, and low exponent RSA vulnerabilities, Journal of Cryptology, 10:233--260, 1997

[3] J-S. Coron, A. Gouget, P. Paillier and K. Villegas, SPAKE: a Single-party Public-key Authenticated Key Exchange Protocol for Contact-less Applications, in Proceedings of Financial Cryptography: Workshop on Real-Life Cryptographic Protocols and Standardization 2010, January 2010

[4] M. Girault and D. Lefranc, Public key authentication with one (online) single addition, in CHES'04, pp 413-427, 2004

[5] M. Girault, L. Juniot, and M.J.B. Robshaw, The feasibility of on-the-tag public key cryptography, in RFIDSEC 2007, 11-13 july 2007

[6] M. Girault, G. Poupard, and J. Stern, On the fly authentication and signature schemes based on groups of unknown order, Journal of Cryptology, 19(4):463-487, 2006

[7] H. W. Jr. Lenstra, Factoring Integers with Elliptic Curves, Ann. Math. 126, 649-673, 1987

[8] A. K. Lenstra and H. W. Lenstra, Jr, The development of the number field sieve, Lecture Notes in Math. (1993) 1554, Springer-Verlag

[9] J. Liu, J. Baek, J. Zhou, Y. Yang, and J.-W. Wong, Efficient Online/Offline Identity-Based Signature for Wireless Sensor Network, International Journal of Information Security, 9(4):287--296, Springer, August 2010

[10] M. McLoone and M.J.B. Robshaw, Public Key Cryptography and RFID, in M. Abe, editor, Proceedings of CT-RSA 07, volume 4377 of LNCS, pp 372-384, Springer, 2007

[11] M. McLoone and M.J.B. Robshaw, New Architectures for Low-Cost Public Key Cryptography on RFID Tags, in Proc. of IEEE International Conference on Security and Privacy of Emerging Areas in Communication Networks (SecureComm 2005), pp 1827-1830, IEEE, 2007

[12] A. Poschmann, M. Robshaw, F. Vater, and C.Paar, Lightweight Cryptography and RFID: Tackling the Hidden Overheads, in D. Lee and S. Hong, editors, Proc. of ICISC-2009, volume 5984 of LNCS, pp 129-145, Springer, 2010

[13] R.L Rivest, A. Shamir and L. Adleman, A method for obtaining digital signature and public-key cryptosystems, in technical report LCS!TM82, MIT Laboratory for Computer Science, Cambridge, Massachusetts, 4th April 1977

[14] C.P. Schnorr, Efficient identification and signatures for smart cards, in Proceedings of CRYPTO '89, volume 435 of Lecture Notes in Computer Science, pages 239-252. Springer, 1990 [15] A. Shamir, RSA for paranoids, in Cryptobytes, the technical newsletter from RSA Laboratories, Volume 1, Number 3 — Autumn 1995

[16] European Network of Excellence in Cryptology II, ECRYPT II Yearly Report on Algorithms and Key Lengths (2010), available on http://www.ecrypt.eu.orq/documents/D.SPA.13.pdf

[17] National Institute of Standards and Technology, Digital Signature Standard (DSS), FIPS Publication 186-3, available on http://csrc.nist.gov/publications/PubsFIPS.html

[18] ISO/IEC 8825-1:2002, Information technology — ASN.1 encoding rules: Specification of Basic Encoding Rules (BER), Canonical Encoding Rules (CER) and Distinguished Encoding Rules (DER)

[19] ISO/IEC 9796-3:2006, Information technology — Security techniques — Digital signature schemes giving message recovery — Part 3: Discrete logarithm based mechanisms

[20] ISO/IEC 9798-1:2010, Information technology — Security techniques — Entity authentication — Part 1: General

[21] ISO/IEC 9798-5:2009, Information technology — Security techniques — Entity authentication — Part 5: Mechanisms using zero-knowledge techniques

[22] ISO/IEC 10118-1:2000, Information technology — Security techniques — Hash-functions — Part 1: General

[23] ISO/IEC 10118-3:2004, Information technology — Security techniques — Hash-functions — Part 3: Dedicated hash-functions

[24] ISO/IEC 14888-3:2006, Information technology — Security techniques — Digital signature with appendix — Part 3: Discrete logarithm based mechanisms

[25] I SO/I EC 18031:2011, Information technology — Security techniques — Random bit generation
[26] ISO/IEC 18033-3:2010, Information technology — Security techniques — Encryption algorithms — Part 3: Block ciphers

[27] ISO/IEC 29192-2:2012, Information technology Security techniques — Lightweight Cryptography — Part 2: Block ciphers

[28] BLAKE I., SEROUSSI G., SMART N. Elliptic Curves in Cryptography, Cambridge University Press, 1999 [29] BROWN D. and GALLANT R. The Static Diffie-Hellman Problem, Cryptology ePrint Archive, Report 2004/306. Available via https://eprint.iacr.org/2004/306

[30] BOCK H., BRAUN M., DICHTL M., HESS E., HEYSZL J., KARGL W., KOROSCHETZ H., MEYER B., SEUSCHEK H. A Milestone towards RFID Products Offering Asymmetric Authentication based on Elliptic Curve Cryptography. In RFIDSEC-2008 - Proceedings of the 4th Workshop on RFID Security, July 9-11, 2008. Available via http://events.iaik.tugraz.at/RFIDSec08/Papers/index.htm

[31] BRAUN M., HESS E., MEYER B. Using Elliptic Curves on RFID Tags. IJCSNS International Journal of Computer and Network Security, 8(2), 1-9, February 2008

[32] CHEON J.H. Security Analysis of the Strong Diffie-Hellman Problem, Eurocrypt '06, LNCS 4004, Springer-Verlag, pp.1-11, 2006