LƯỢC ĐỒ CHỮ KÝ TẬP THỂ XÂY DỰNG TRÊN BÀI TOÁN LOGARIT RỜI RẠC KẾT HỢP KHAI CĂN TRÊN Z_p

Nguyễn Đức Thụy*, Lưu Hồng Dũng+

* Khoa Công nghệ thông tin, Trường CĐ Kinh tế - Kỹ thuật Tp. HCM

+ Khoa Công nghệ thông tin, Học Viện Kỹ thuật Quân Sự

Tóm tắt: Bài báo đề xuất một lược đồ chữ ký tập thể xây dựng trên tính khó của bài toán logarit rời rạc kết hợp khai căn trên Z_p . Bài toán logarit rời rạc kết hợp khai căn được đề xuất ở đây là một dạng bài toán khó mới thuộc lớp các bài toán chưa có cách giải về mặt toán học. Do đó, việc xây dựng lược đồ chữ ký số dựa trên tính khó của bài toán logarit rời rạc kết hợp khai căn này cho khả năng nâng cao độ an toàn của thuật toán trong các ứng dụng thực tế.

Từ khóa: Chữ ký số; Chữ ký số tập thể; Bài toán logarit rời rạc; Bài toán logarit rời rạc kết hợp khai căn.

I. ĐẶT VẤN ĐỀ

Trong [1,2] nhóm tác giả đã đề xuất một phương pháp xây dựng lược đồ chữ ký số dựa trên tính khó của bài toán logarit kết hợp khai căn trên trường hữu hạn Z_p. Bài toán logarit kết hợp khai căn trên trường Z_p là một dạng bài toán khó mới mà trong toán học chưa có cách giải. Do đó, việc xây dựng lược đồ chữ ký dựa trên bài toán này cho phép nâng cao độ an toàn của thuật toán trước các dạng tấn công khóa bí mật và tấn công giả mạo chữ ký. Trong bài báo này, nhóm tác giả tiếp tục đề xuất xây dựng lược đồ ký tập thể dựa trên bài toán logarit kết hợp khai căn theo mô hình trong [3,4], đây là mô hình chữ ký được đề xuất ứng dụng cho các tổ chức có tư cách pháp nhân trong xã hội. Trong mô hình này, các thông điệp điện tử sẽ được chứng thực ở hai cấp độ khác nhau: thực thể tạo ra nó và tổ chức mà thực thể tạo ra nó là một thành viên hay bộ phận của tổ chức này.

Đã có nhiều kết quả nghiên cứu được công bố trên thế giới cũng như ở trong nước về đề tài chữ ký tập thể. Điều đáng nói là trong khi các lược đồ chữ ký tập thể đã được xây dựng trước đó đều dựa trên cơ sở là các bài toán khó kinh điển (như bài toán logarit rời rạc trên
trường hữu hạn cũng như trên đường cong ellipic hay dựa trên tính khó của việc giải đồng thời bài toán logarit rời rạc và bài toán phân tích số hoặc bài toán khai căn và bài toán phân tích số) thì lược đồ chữ ký tập thể đề xuất ở đây lại được xây dựng dựa trên bài toán khó mới như là một giải pháp nâng cao độ an toàn cho lược đồ chữ ký trong các ứng dụng thực tế.

Tác giả liên hệ: Nguyễn Đức Thụy
Email: thuyphulam2013@gmail.com
Đến tòa soạn: 17/7/2021, chỉnh sửa: 16/10/21, chấp nhận đăng: 26/10/2021

II. BÀI TOÁN LOGARIT KẾT HỢP KHAI CĂN TRÊN Z_p

Bài toán logarit kết hợp khai căn được phát biểu dưới 2 dạng như sau:

Dạng 1: Cho p là một số nguyên tố, với mỗi số nguyên dương y thuộc Z_p, hãy tìm số x thỏa mãn phương trình sau:

$$x^x \bmod p = y$$

Dạng 2: Cho p là một số nguyên tố, a và b là các số nguyên dương thuộc Z_p , hãy tìm số x thỏa mãn phương trình sau:

$$a^x \equiv x^b \bmod p$$

Dễ thấy rằng, cả 2 dạng của bài toán logarit kết hợp khai căn trên Z_p đều là các bài toán chưa có cách giải. Hiện tại không có cách giải nào khác cho bài toán này ngoài phương pháp "vét cạn" với độ phức tạp tính toán $\boldsymbol{O}(p)$.

Ở đây, dạng thứ nhất của bài toán logarit kết hợp khai căn được sử dụng để hình thành cặp khóa bí mật, công khai của các đối tượng ký, còn dạng thứ hai của bài toán này được sử dụng làm cơ sở xây dựng thuật toán kiểm tra của lược đồ chữ ký mới đề xuất.

III. XÂY DỰNG LƯỢC ĐỒ CHỮ KÝ SỐ TẬP THỂ DỰA TRÊN BÀI TOÁN LOGARIT KẾT HỢP KHAI CĂN

A. Lược đồ cơ sở

Lược đồ cơ sở ở đây là thuật toán chữ ký xây dựng trên tính khó của bài toán logarit kết hợp khai căn theo phương pháp đã được đề xuất trong [1,2] và được sử dụng để xây dựng lược đồ chữ ký tập thể ở mục tiếp theo. Lược đồ cơ sở bao gồm các thuật toán sinh tham số và khóa, thuật toán ký và thuật toán kiểm tra chữ ký như sau:

1. Thuật toán sinh tham số và khóa

Thuật toán 1.1:

input: Lp, Lq – độ dài (tính theo bit) của các số nguyên tố p,q.

output: p,q, x, y.

[1]. **generate** p,q: len(p) = Lp, len(q) = Lq, q|(p-1)

[2]. **select** α: $1<\alpha<p$

[3]. $x \leftarrow \alpha^{\frac{p-1}{q}} \bmod p$

[4]. **if** (x = 1 **OR** x = q) **then goto** [2]

[5]. $y \leftarrow x^x \bmod p$ (1.1)

[6]. **return** {p,q, x,y}

Chú thích:

- len(.) : Hàm tính độ dài (theo bit) của một số nguyên.
- p,q: Tham số hệ thống/tham số miền.
- x, y: Khóa bí mật và khóa công khai của đối tượng ký.

2. Thuật toán ký

Thuật toán 1.2:

input: p, q, x, y, M.
output: (r,s).

[1]. **select** k: $1<k<q$

[2]. $z \leftarrow (x)^k \bmod p$ (1.2)

[3]. $e_1 \leftarrow H(z \| M)$, $e_2 \leftarrow H(z \| y)$,
$e_3 \leftarrow H(z \| y \| M)$ (1.3)

[4]. $e_4 \leftarrow (k \times e_2 + x \times e_3) \times (e_1 + e_2)^{-1} \bmod q$ (1.4)

[5]. $e_5 \leftarrow (k - e_4) \bmod q$ (1.5)

[6]. $r \leftarrow (x)^{e_4} \bmod p$ (1.6)

[7]. $s \leftarrow (x)^{e_5} \bmod p$ (1.7)

[8]. **return** (r,s)

Chú thích:

- M: bản tin cần ký, với: $M \in \{0,1\}^\infty$.
- (r,s): chữ ký lên M.
- "||": toán tử ghép nối 2 xâu bit hoặc 2 xâu ký tự.
- mod : toán tử chia lấy phần dư.

3. Thuật toán kiểm tra chữ ký

Thuật toán 1.3:

input: p, q, y, M, (r,s).
output: TRUE / FALSE.

[1]. $\bar{z} \leftarrow r \times s \bmod p$ (1.8)

[2]. $\bar{e}_1 \leftarrow H(\bar{z} \| M)$, $\bar{e}_2 \leftarrow H(\bar{z} \| y)$,
$\bar{e}_3 \leftarrow H(\bar{z} \| y \| M)$ (1.9)

[3]. $A \leftarrow (r)^{\bar{e}_1} \bmod p$ (1.10)

[4]. $B \leftarrow (s)^{\bar{e}_2} \times (y)^{\bar{e}_3} \bmod p$ (1.11)

[5]. **if** (A = B) **then** {**return** (TRUE)}
else {**return** (FALSE)}

Chú thích:

- M, (r,s): bản tin, chữ ký cần thẩm tra.
- Nếu kết quả trả về là TRUE thì tính toàn vẹn và nguồn gốc của M được khẳng định. Ngược lại, nếu kết quả là FALSE thì M bị phủ nhận về nguồn gốc và tính toàn vẹn.

4. Tính đúng đắn của lược đồ cơ sở

Tính đúng đắn của lược đồ cơ sở được chứng minh dựa trên các bổ đề sau đây:

Bổ đề 1:

Cho p và q là 2 số nguyên tố với q là ước số của (p-1), α là một số nguyên dương trong khoảng (1,p). Nếu: $x = \alpha^{\frac{p-1}{q}} \bmod p$ thì: $x^q \bmod p = 1$.

Chứng minh:

Ta có:

$$(x)^q \bmod p = \left(\alpha^{\frac{p-1}{q}} \bmod p\right)^q \bmod p$$

$$= (\alpha)^{p-1} \bmod p$$

Theo định lý Fermat thì:

$$(\alpha)^{p-1} \bmod p = 1$$

Suy ra:

$$(x)^q \bmod p = 1$$

Bổ đề đã được chứng minh.

Bổ đề 2:

Cho p và q là 2 số nguyên tố với q là ước số của (p - 1), α là một số nguyên dương trong khoảng (1,p) và $x = \alpha^{\frac{p-1}{q}} \bmod p$. Nếu: $m \bmod q = n \bmod q$ thì: $x^m \equiv x^n \bmod p$.

Chứng minh:

Nếu: $m \bmod q = n \bmod q$ thì: $m = n + k \times q$ hoặc: $n = m + k \times q$, với k là một số nguyên. Không làm mất tính tổng quát, giả sử: $m = n + k \times q$.

Do đó:

$$x^m \bmod p = x^{n+k\times q} \bmod p = x^n \times x^{k\times q} \bmod p$$
$$= (x^n \bmod p) \times (x^{k\times q} \bmod p) \bmod p$$
$$= (x^n \bmod p) \times (x^q \bmod p)^k \bmod p$$

Theo Bổ đề 1 ta có:

$$(x)^q \bmod p = 1$$

Nên:

$$x^m \bmod p = (x^n \bmod p) \times (x^q \bmod p)^k \bmod p$$
$$= (x^n \bmod p) \times (1)^k \bmod p = x^n \bmod p$$

Bổ đề đã được chứng minh.

Bổ đề 3:

Cho p và q là 2 số nguyên tố với q là ước số của (p - 1), α là một số nguyên dương trong khoảng (1,p) và $x = \alpha^{\frac{p-1}{q}} \bmod p$. Nếu: $m \in (1, p)$ và $m \neq q$ thì: $(x)^m \equiv (x)^{m \bmod q} \bmod p$.

Chứng minh:

Do m nằm trong khoảng (1,p) và $m \neq q$ nên: $1 < m < q$ hoặc: $q < m < p$. Trường hợp thứ nhất: $1 < m < q$ thì: $m \bmod q = m$ nên: $(x)^m \equiv (x)^{m \bmod q} \bmod p$.

Trường hợp thứ hai: $q < m < p$ thì: $m = n + k \times q$, với k là một số nguyên và $n = m \bmod q$. Vì thế:

$$(x)^m \bmod p = (x)^{n+k\times q} \bmod p = (x)^n \times (x)^{k.q} \bmod p$$
$$= (x)^n \times ((x)^q \bmod p)^k \bmod p$$

Theo Bổ đề 1 ta có:

$$(x)^q \bmod p = 1$$

Nên:

$$(x)^m \bmod p = (x)^n \times (1)^k \bmod p = (x)^n \bmod p$$
$$= (x)^{m \bmod q} \bmod p$$

Như vậy, trong mọi trường hợp ta đều có:

$$(x)^m \bmod p = (x)^{m \bmod q} \bmod p$$

Bổ đề đã được chứng minh.

Tính đúng đắn của lược đồ cơ sở được chứng minh như sau:

Thật vậy, thay (1.6), (1.7) vào (1.8) và theo Bổ đề 3 ta có:

$$\begin{aligned} \bar{z} &= r \times s \bmod p \\ &= \left(x^{e_4} \bmod p\right) \times \left(x^{e_5} \bmod p\right) \bmod p \\ &= x^{e_4} \times x^{e_5} \bmod p = x^{e_4+e_5} \bmod p \\ &= x^{(e_4+e_5) \bmod q} \bmod p \end{aligned} \quad (1.12)$$

Mặt khác, từ (1.5) ta có:

$$(e_4 + e_5) \bmod q = k \quad (1.13)$$

Từ (1.12) và (1.13) dẫn đến:

$$\begin{aligned} \bar{z} &= (x)^{(e_4+e_5) \bmod q} \bmod p \\ &= (x)^k \bmod p \end{aligned} \quad (1.14)$$

Từ (1.14) và (1.2) suy ra:

$$\bar{z} = z \quad (1.15)$$

Thay (1.15) vào (1.9) ta được:

$$\begin{aligned} \bar{e}_1 &= H(\bar{z} \parallel M) \bmod q = H(z \parallel M) \bmod q, \\ \bar{e}_2 &= H(\bar{z} \parallel y) \bmod q = H(z \parallel y) \bmod q, \\ \bar{e}_3 &= H(\bar{z} \parallel y \parallel M) \bmod q \\ &= H(z \parallel y \parallel M) \bmod q \end{aligned} \quad (1.16)$$

Từ (1.16) và (1.3) suy ra:

$$\bar{e}_1 = e_1,\ \bar{e}_2 = e_2,\ \bar{e}_3 = e_3$$

Do đó:

$$A = (r)^{\bar{e}_1} \bmod p = (r)^{e_1} \bmod p \quad (1.17)$$

và:

$$B = (s)^{\bar{e}_2} \times (y)^{\bar{e}_3} \bmod p = (s)^{e_2} \times (y)^{e_3} \bmod p \quad (1.18)$$

Thay (1.1), (1.7) vào (1.18) ta được

$$\begin{aligned} B &= (s)^{e_2} \times (y)^{e_3} \bmod p \\ &= \left(x^{e_5} \bmod p\right)^{e_2} \times \left(x^{x} \bmod p\right)^{e_3} \bmod p \\ &= (x)^{(k-e_4) \times e_2} \times (x)^{x.e_3} \bmod p \\ &= (x)^{k \times e_2 + x \times e_3 - e_2 \times e_4} \bmod p \end{aligned} \quad (1.19)$$

Mặt khác, từ (1.4) suy ra :

$$e_4 \times (e_1 + e_2) \bmod q = (k \times e_2 + x \times e_3) \bmod q$$

Hay:

$$e_1 \times e_4 \bmod q = (k \times e_2 + x \times e_3 - e_2 \times e_4) \bmod q \quad (1.20)$$

Từ (1.6), (1.19), (1.20) và theo Bổ đề 2 ta được:

$$\begin{aligned} B &= (x)^{k.e_2 + x.e_3 - e_2.e_4} \bmod p = (x)^{e_1 \times e_4} \bmod p \\ &= \left(x^{e_4} \bmod p\right)^{e_1} \bmod p = (r)^{e_1} \bmod p \end{aligned} \quad (1.21)$$

Từ (1.17) và (1.21) suy ra: A = B.

Đây là điều cần phải chứng minh.

4. Mức độ an toàn của lược đồ cơ sở

Mức độ an toàn của lược đồ cơ sở có thể đánh giá qua khả năng chống lại một số dạng tấn công như:

a) Tấn công khóa bí mật

Tấn công khóa bí mật có thực hiện vào thuật toán sinh khóa (Thuật toán 1.1) và các bước [2], [4], [6] và [7] của thuật toán ký (Thuật toán 1.2) . Ơ các bước [2], [6] và [7], các tham số *r, s* và *z* là công khai, song các tham số *k, e_4* và *e_5* lại là bí mật. Vì vậy việc tìm *x* từ các bước [2], [6] và [7] của thuật toán ký là khó tương tự như tìm *x* từ thuật toán sinh khóa, là một dạng bài toán khó chưa có cách giải. Còn ở bước [4] của thuật toán ký, bản thân *e_4* cũng là 1 tham số bí mật nên việc tìm *x* từ bước [4] là không thể thực hiện được. Như vậy, để tính khóa bí mật thì kẻ tấn công buộc phải giải được bài toán logarit kết hợp khai căn trên Z_p.

b) Tấn công giả mạo chữ ký

Từ thuật toán kiểm tra (Thuật toán 1.3) của lược đồ cơ sở cho thấy, một cặp (r,s) sẽ được công nhận là chữ ký hợp lệ với một bản tin M nếu thỏa mãn điều kiện:

$$r^{e_1} \equiv (s)^{e_2} \times (y)^{e_3} \bmod p$$

hay:

$$(r)^{H(r \times s \bmod p \| M)} \equiv (s)^{H(r \times s \bmod p \| y)} \times (y)^{H(r \times s \bmod p \| y \| M)} \bmod p \quad (1.22)$$

Từ (1.22) cho thấy, việc lựa chọn ngẫu nhiên 1 cặp (r,s) với 1 bản tin M cho trước thỏa mãn được đẳng thức kiểm tra là hoàn toàn không khả thi. Ngoài ra, việc chọn trước 1 trong 2 giá trị r hoặc s rồi tính giá trị thứ 2 từ (1.22) là tương đương với việc giải bài toán logarit kết hợp khai căn ở dạng thứ 2, cũng là một dạng bài toán mà hiện tại còn chưa có cách giải.

B. Lược đồ chữ ký tập thể

Lược đồ chữ ký tập thể ở đây được phát triển từ lược đồ cơ sở theo mô hình đã được đề xuất trong [3,4] với các chức năng như sau:

- Chứng nhận và kiểm tra tính hợp pháp của thành viên nhóm ký.
- Hình thành chữ ký tập thể từ chữ ký một nhóm đối tượng ký. Kích thước của chữ ký tập thể được tạo ra không phụ thuộc vào số lượng thành viên nhóm ký.
- Kiểm tra chữ ký tập thể của một nhóm đối tượng được thực hiện tương tự như kiểm tra chữ ký do một đối tượng ký tạo ra.

Chú ý: Theo mô hình chữ ký tập thể trong [3,4], một tổ chức có thể hình thành nhiều nhóm ký với số lượng thành viên của mỗi nhóm ký khác nhau.

1. Thuật toán sinh tham số và khóa

Các tham số hệ thống (p, q) được lựa chọn theo phương pháp của DSA [5] hoặc GOST R34.10-94 [6]. Giả sử nhóm ký gồm N-thành viên: U = {U_i| i=1,2,...,N}. Các thành viên nhóm ký có khóa bí mật là: K_s = {x_i| i=1,2,...,N} và các khóa công khai tương ứng là: K_p = {y_i| i=1,2,...,N}. CA (Certificate Authority) là bộ phận chứng thực số của tổ chức mà U là thành viên, CA có cặp khóa bí mật, công khai là: (x_{ca},y_{ca}).

a) Thuật toán sinh tham số hệ thống và khóa của CA

Thuật toán 2.1: Sinh tham số hệ thống và khóa của CA.

input: L_p, L_q.
output: p,q, x_{ca},y_{ca}.

[1]. **generate** (p,q): len(p) = L_p, len(q) = L_q, q|(p-1)
[2]. **select** α: $1 < \alpha < p$
[3]. $x_{ca} \leftarrow \alpha^{\frac{p-1}{q}} \bmod p$
[4]. **if** (x_{ca} = 1 **OR** x_{ca} = q) **then goto** [2]
[5]. $y_{ca} \leftarrow (x_{ca})^{x_{ca}} \bmod p$ (2.1)
[6]. **return** (p, q, x_{ca},y_{ca})

Chú thích:

– L_p, L_q: kích thước tính theo bit của các số p, q.

b) Thuật toán sinh khóa của các đối tượng ký

Thuật toán 2.2: Sinh khóa của các đối tượng ký

input: p, q .
output: $\{(x_i,y_i)|\ i = 1,2,\ldots,N\}$.

[1]. **for** i = 1 **to** N **do**
[1.1]. **select** α_i: $1<\alpha_i<p$
[1.2]. $x_i \leftarrow (\alpha_i)^{\frac{p-1}{q}} \bmod p$
[1.3]. **if** ($x_i = 1$ **OR** $x_i = q$) **then goto** [1.1]
[1.4]. $y_i \leftarrow (x_i)^{x_i} \bmod p$ (2.2)
[2]. **return** $\{(x_i,y_i)|\ i = 1,2,\ldots,N\}$

2. Thuật toán chứng nhận và kiểm tra tính hợp pháp của đối tượng ký

Trong mô hình chữ ký tập thể, một tổ chức (có tư cách pháp nhân) công nhận các đối tượng (ký) là thành viên thuộc tổ chức này và có thẩm quyền ký (tùy thuộc vào vị trí, quyền hạn của đối tượng trong tổ chức) lên các văn bản do tổ chức này phát hành bằng cách tạo ra các *chứng chỉ khóa công khai*. Trong một chứng chỉ khóa công khai, các thông tin quan trọng nhất bao gồm: định danh (danh tính của đối tượng ký, danh tính của tổ chức mà đối tượng ký là thành viên, số hiệu chứng chỉ, trạng thái chứng chỉ…) và khóa công khai của đối tượng ký, cùng với *chữ ký xác nhận* của CA. Ở đây, chữ ký xác nhận hay *chứng nhận* của CA đối với định danh và khóa công khai của đối tượng ký được tạo ra bởi Thuật toán 6.9 với tham số đầu vào, bao gồm: định danh (ID_i) và khóa công khai của đối tượng ký (y_i) là các thông tin cần chứng thực; khóa bí mật của CA được dùng để tạo ra chữ ký/chứng nhận (u_i,v_i) lên các thông tin cần chứng thực. Có thể thấy, chứng nhận đối tượng ký trong mô hình chữ ký tập thể là hoàn toàn tương tự như việc một nhà cung cấp dịch vụ chứng thực số cấp chứng chỉ khóa công khai cho một khách hàng khi đăng ký sử dụng dịch vụ.

Việc kiểm tra tính hợp pháp của đối tượng ký được thực hiện khi có sự nghi ngờ về tư cách thành viên của đối tượng ký. Ví dụ: cần kiểm tra một đối tượng có phải/còn là thành viên của tổ chức và có thẩm quyền ký vào các bản tin do tổ chức này phát hành nữa hay không? Ngoài ra, kiểm tra tính hợp pháp của đối tượng ký còn đặc biệt quan trọng trong quá trình tạo chứng nhận của CA đối với chữ ký cá nhân của một hay một nhóm đối tượng ký lên bản tin cần ký nhằm ngăn chặn tấn công giả mạo từ bên ngoài hay bên trong nhóm ký. Kiểm tra tính hợp pháp của đối tượng ký được thực hiện bởi Thuật toán 6.10 với các tham số đầu vào bao gồm: khóa công khai (y_i) và định danh của đối tượng ký (ID_i) là các thông tin cần xác thực; khóa công khai (y_{ca}) của CA để kiểm tra tính hợp lệ của chữ ký (u_i,v_i). Nếu (u_i,v_i) được công nhận là hợp lệ thì danh tính (ID_i) và khóa công khai (y_i) đối tượng ký (U_i) được xác thực. Ngược lại, đối tượng này là giả mạo và không được phép tham gia vào nhóm ký.

a) CA chứng nhận đối tượng ký

Thuật toán 2.3: Tạo chứng nhận cho đối tượng ký
input: p, q, N, x_{ca}, $\{(ID_i, y_i)|i =1, 2,..,N\}$
output: $\{(u_i,v_i)|\ i = 1, 2,...,N\}$

[1]. **for** i = 1 **to** N **do**
[1.1]. $k_i \leftarrow H(x_{ca} \| y_i \| ID_i)$
[1.2]. $z_i \leftarrow (x_{ca})^{k_i} \bmod p$ (2.3)
[1.3]. $e_1 \leftarrow H(z_i \| y_i \| ID_i) \bmod q,$
$e_2 \leftarrow H(z_i \| y_{ca}) \bmod q,$
$e_3 \leftarrow H(z_i \| y_{ca} \| y_i \| ID_i) \bmod q$ (2.4)
[1.4]. $e_4 \leftarrow (k_i \times e_2 + x_{ca} \times e_3) \times (e_1 + e_2)^{-1} \bmod q$ (2.5)
[1.5]. $e_5 \leftarrow (k_i - e_4) \bmod q$ (2.6)
[1.6]. $u_i \leftarrow (x_{ca})^{e_4} \bmod p$ (2.7)
[1.7]. $v_i \leftarrow (x_{ca})^{e_5} \bmod p$ (2.8)
[2]. **return** $\{(u_i,v_i)|\ i = 1, 2,...N\}$

Chú thích:

– (u_i,v_i): chứng nhận của CA đối với U_i (i = 1,2,…,N) thực chất là chữ ký của CA đối với các thông tin cần chứng nhận bao gồm khóa công khai (y_i) và định danh của đối tượng ký (ID_i), ngoài ra còn có thể bao gồm các thông tin khác như: định danh của CA, thuật toán ký được sử dụng để tạo chứng nhận, định dạng của chứng chỉ,...

b) Kiểm tra tính hợp pháp của đối tượng ký

Thuật toán 2.4: Kiểm tra tính hợp pháp của đối tượng ký
input: p, q, y_i, ID_i, (u_i,v_i), y_{ca}.
output: TRUE / FALSE

[1]. $\bar{z}_i \leftarrow u_i \times v_i \bmod p$ (2.9)
[2]. $\bar{e}_1 \leftarrow H(\bar{z}_i \| y_i \| ID_i) \bmod q,$
$\bar{e}_2 \leftarrow H(\bar{z}_i \| y_{ca}) \bmod q,$
$\bar{e}_3 \leftarrow H(\bar{z}_i \| y_{ca} \| y_i \| ID_i) \bmod q$ (2.10)
[3]. $A_i \leftarrow (u_i)^{\bar{e}_1} \bmod p$ (2.11)
[4]. $B_i \leftarrow (v_i)^{\bar{e}_2} \times (y_{ca})^{\bar{e}_3} \bmod p$ (2.12)
[5]. **if** ($A_i = B_i$) **then** {**return** (TRUE)}
else {**return** (FALSE)}

Chú thích:

- Nếu kết quả trả về là TRUE thì đối tượng ký là thành viên thuộc tổ chức mà CA là cơ quan chứng thực của cơ quan này.
- Nếu kết quả trả về là FALSE thì đối tượng ký và/hoặc chứng nhận (u_i,v_i) là giả mạo.

3. Thuật toán ký và kiểm tra chữ ký tập thể

a) Thuật toán hình thành chữ ký tập thể của một nhóm đối tượng lên bản tin cần ký

Chữ ký tập thể được hình thành qua 4 bước:

– Hình thành chữ ký cá nhân của một nhóm đối tượng lên bản tin cần ký.

– Kiểm tra tính hợp pháp của các thành viên nhóm ký.

– Kiểm tra tính hợp lệ của chữ ký cá nhân.

– Tạo chứng nhận/chữ ký xác nhận của CA đối với chữ ký cá nhân và bản tin cần ký.

Chữ ký tập thể được tạo ra ở đây bao gồm chữ ký cá nhân của nhóm đối tượng lên bản tin cần ký và chứng nhận của CA đối với chữ ký cá nhân của nhóm đối tượng và bản tin cần ký.

Thuật toán 2.5: Sinh chữ ký tập thể
input: p, q, M, N, $\{(x_i|,y_i)|i = 1, 2,..,N\}$.
output: $\{(r,s),(u,v)\}$

[1]. **for** i = 1 **to** N **do**

[1.1]. $k_i \leftarrow H(x_i \| M)$

[1.2]. $z_i \leftarrow (x_i)^{k_i} \bmod p$ (2.13)

[1.3]. **send** z_i **to** CA

[2]. for i = 1 to N do

[2.1]. $\bar{z}_i \leftarrow u_i \times v_i \bmod p$

[2.2]. $\bar{e}_1 \leftarrow H(\bar{z}_i \| y_i \| ID_i) \bmod q$,

$\bar{e}_2 \leftarrow H(\bar{z}_i \| y_{ca}) \bmod q$,

$\bar{e}_3 \leftarrow H(\bar{z}_i \| y_{ca} \| y_i \| ID_i) \bmod q$

[2.3]. $A_i \leftarrow (u_i)^{\bar{e}_1} \bmod p$

[2.4]. $B_i \leftarrow (v_i)^{\bar{e}_2} \times (y_{ca})^{\bar{e}_3} \bmod p$

[2.5]. **if** ($A_i \neq B_i$) **then return** {(0,0),(0,0)}

[3]. $z \leftarrow \prod_{i=1}^{N} z_i \bmod p$ (2.14)

[4]. $y \leftarrow \prod_{i=1}^{N} y_i \bmod p$ (2.15)

[5]. $e_1 \leftarrow H(z \| M) \bmod q$,

$e_2 \leftarrow H(z \| y) \bmod q$,

$e_3 \leftarrow H(z \| y \| M) \bmod q$ (2.16)

[6]. **send** (e_1,e_2,e_3) **to** {U_1, U_2,...., U_i-,..., U_N};

[7]. **for** i = 1 **to** N **do**

[7.1]. $e_4 \leftarrow (k_i \times e_2 + x_i \times e_3) \times (e_1 + e_2)^{-1} \bmod q$ (2.17)

[7.2]. $e_5 \leftarrow (k_i - e_4) \bmod q$ (2.18)

[7.3]. $r_i \leftarrow (x_i)^{e_4} \bmod p$ (2.19)

[7.4]. $s_i \leftarrow (x_i)^{e_5} \bmod p$ (2.20)

[7.5] **send** (r_i,s_i) **to** CA

[8]. $r \leftarrow \prod_{i=1}^{N} r_i \bmod p$ (2.21)

[9]. $s \leftarrow \prod_{i=1}^{N} s_i \bmod p$ (2.22)

[10]. **if** (r = 0 **OR** s = 0) **then return** {(0,0),(0,0)} **else**

[10.1]. $\bar{z} \leftarrow r \times s \bmod p$ (2.23)

[10.2]. $\bar{e}_1 \leftarrow H(\bar{z} \| M) \bmod q$,

$\bar{e}_2 \leftarrow H(\bar{z} \| y) \bmod q$,

$\bar{e}_3 \leftarrow H(\bar{z} \| y \| M) \bmod q$ (2.24)

[10.3]. $A \leftarrow (r)^{\bar{e}_1} \bmod p$ (2.25)

[10.4]. $B \leftarrow (s)^{\bar{e}_2} \times (y)^{\bar{e}_3} \bmod p$ (2.26)

[10.5]. **if** ($A \neq B$) **then return** {(0,0),(0,0)}

[11]. $k_{ca} \leftarrow H(x_{ca} \| y \| M)$

[12]. $z_{ca} \leftarrow (x_{ca})^{k_{ca}} \bmod p$ (2.27)

[13]. $e_1 \leftarrow H(z_{ca} \| y \| M) \bmod q$,

$e_2 \leftarrow H(z_{ca} \| y_{ca}) \bmod q$,

$e_3 \leftarrow H(z_{ca} \| y_{ca} \| y \| M) \bmod q$ (2.28)

[14]. $e_4 \leftarrow (k_{ca} \times e_2 + x_{ca} \times e_3) \times (e_1 + e_2)^{-1} \bmod q$ (2.29)

[15]. $e_5 \leftarrow (k_{ca} - e_4) \bmod q$ (2.30)

[16]. $u \leftarrow (x_{ca})^{e_4} \bmod p$ (2.31)

[17]. $v \leftarrow (x_{ca})^{e_5} \bmod p$ (2.32)

[18]. **return** {(r,s),(u,v)}

Chú thích:

– {(e,s),(u,v)} là chữ ký tập thể của nhóm đối tượng {U_i| i=1,2,..,N} lên bản tin cần ký M. Trong đó, (e,s) là chữ ký cá nhân của nhóm ký, còn (u,v) là chứng nhận của CA đối với chữ ký cá nhân và bản tin cần ký.

– Các bước [1] và [7] do các thành viên nhóm ký thực hiện, các bước còn lại do CA thực hiện.

b) Thuật toán kiểm tra chữ ký tập thể

Việc kiểm tra tính hợp lệ của chữ ký tập thể để từ đó xác thực bản tin ở 2 cấp được thực hiện qua các bước:

- Kiểm tra tính hợp pháp của các đối tượng ký.

- Kiểm tra tính hợp lệ của chữ ký cá nhân của nhóm ký lên bản tin cần thẩm tra.

- Kiểm tra tính hợp lệ của chữ ký xác nhận của CA.

Việc kiểm tra chữ ký của CA chỉ thực hiện khi tính hợp pháp của các thành viên nhóm ký và tính hợp lệ của chữ ký cá nhân đã được khẳng định. Vì vậy, việc kiểm tra chữ ký CA ở bước cuối cùng của thuật toán kiểm tra chữ ký tập thể mà cho kết quả hợp lệ thì tính toàn vẹn và nguồn gốc bản tin cần thẩm tra đã được xác thực ở cả 2 cấp độ: cá nhân của thực thể ký (nhóm đối tượng ký) và tổ chức mà thực thể ký là thành viên trong tổ chức đó.

Thuật toán 2.6: Kiểm tra chữ ký tập thể

input: p,q,N, M,y_{ca},{y_i|i = 1,2,..,N},

{(u_i,v_i)|i=1,2,…N}, {(r,s), (u,v)}.

output: TRUE/FALSE.

[1]. **for** i = 1 **to** N **do**

[1.1]. $\bar{z}_i \leftarrow u_i \times v_i \bmod p$

[1.2]. $\bar{e}_1 \leftarrow H(\bar{z}_i \| y_i \| ID_i) \bmod q$,

$\bar{e}_2 \leftarrow H(\bar{z}_i \| y_{ca}) \bmod q$,

$\bar{e}_3 \leftarrow H(\bar{z}_i \| y_{ca} \| y_i \| ID_i) \bmod q$

[1.3]. $A_i \leftarrow (u_i)^{\bar{e}_1} \bmod p$

[1.4]. $B_i \leftarrow (v_i)^{\bar{e}_2} \times (y_{ca})^{\bar{e}_3} \bmod p$

[1.5]. if ($A_i \neq B_i$) then return (FALSE)

[2]. $y \leftarrow \prod_{i=1}^{N} y_i \bmod p$

[3]. **if** (r = 0 **OR** s = 0) **then** {**return** (FALSE)} **else**

[3.1]. $\bar{z} \leftarrow r \times s \bmod p$

[3.2]. $\bar{e}_1 \leftarrow H(\bar{z} \| M) \bmod q$,

$\bar{e}_2 \leftarrow H(\bar{z} \| y) \bmod q$,

$\bar{e}_3 \leftarrow H(\bar{z} \| y \| M) \bmod q$

[3.3]. $A \leftarrow (r)^{\bar{e}_1} \bmod p$

[3.4]. $B \leftarrow (s)^{\bar{e}_2} \times (y)^{\bar{e}_3} \bmod p$

[3.5]. if ($A \neq B$) then return (FALSE)

[4]. **if** (u = 0 **OR** v = 0) **then** {**return** (FALSE) } **else**

[4.1]. $\bar{z}_{ca} \leftarrow u \times v \bmod p$ (2.33)

[4.2]. $\bar{e}_1 \leftarrow H(\bar{z}_{ca} \| y \| M) \bmod q$,

$\bar{e}_2 \leftarrow H(\bar{z}_{ca} \| y_{ca}) \bmod q$,

$\bar{e}_3 \leftarrow H(\bar{z}_{ca} \| y_{ca} \| y \| M) \bmod q$ (2.34)

[4.3]. $A \leftarrow (u)^{\bar{e}_1} \bmod p$ (2.35)

[4.5]. $B \leftarrow (v)^{\bar{e}_2} \times (y_{ca})^{\bar{e}_3} \bmod p$ (2.36)

[4.6]. **if** ($A \neq B$) **then** {**return** (FALSE)}

else {**return** (TRUE) }

Chú thích:

- Nếu kết quả trả về là TRUE thì bản tin cần thẩm tra (M) được công nhận về tính toàn vẹn và nguồn gốc ở cả 2 cấp độ: cấp độ cá nhân của nhóm đối tượng ký (U = {U_i| I =1,2,…N}) và cấp độ tổ chức mà trong đó nhóm đối tượng ký là các thành viên và CA là bộ phận chứng thực thuộc tổ chức này.

- Nếu kết quả trả về là FALSE thì bản tin cần thẩm tra (M) và/hoặc chữ ký cá nhân (e,s) và/hoặc chứng nhận (u,v) của CA đã bị giả mạo.

4. Tính đúng đắn của lược đồ ký tập thể

Tính đúng đắn của lược đồ mới đề xuất bao gồm:

a) Tính đúng đắn của thuật toán chứng nhận và kiểm tra đối tượng ký

Thật vậy, thay (2.7), (2.8) vào (2.9) và theo Bổ đề 3 ta có:

$$\begin{aligned}\bar{z}_i &= u_i \times v_i \bmod p \\ &= \left((x_{ca})^{e_4} \bmod p\right) \times \left((x_{ca})^{e_5} \bmod p\right) \bmod p \\ &= (x_{ca})^{e_4} \times (x_{ca})^{e_5} \bmod p = (x_{ca})^{e_4+e_5} \bmod p \\ &= (x_{ca})^{e_4+e_5 \bmod q} \bmod p\end{aligned} \quad (2.37)$$

Mặt khác, từ (2.6) ta có:

$$e_4 + e_5 \bmod q = k_i \quad (2.38)$$

Từ (2.37) và (2.38) dẫn đến:

$$\begin{aligned}\bar{z}_i &= (x_{ca})^{(e_4+e_5) \bmod q} \bmod p \\ &= (x_{ca})^{k_i} \bmod p\end{aligned} \quad (2.39)$$

Từ (2.3) và (2.39) suy ra:

$$\bar{z}_i = z_i \quad (2.40)$$

Thay (2.40) vào (2.10) ta được:

$$\begin{aligned}\bar{e}_1 &= H(\bar{z}_i \| y_i \| ID_i) \bmod q = H(z_i \| y_i \| ID_i) \bmod q, \\ \bar{e}_2 &= H(\bar{z}_i \| y_{ca}) \bmod q = H(z_i \| y_{ca}) \bmod q \ , \\ \bar{e}_3 &= H(\bar{z}_i \| y_{ca} \| y_i \| ID_i) \bmod q \\ &= H(z_i \| y_{ca} \| y_i \| ID_i) \bmod q\end{aligned} \quad (2.41)$$

Từ (2.4) và (2.41) suy ra:

$$\bar{e}_1 = e_1, \ \bar{e}_2 = e_2, \ \bar{e}_3 = e_3$$

Do đó, từ (2.11) và (2.12) ta có:

$$A_i = (u_i)^{\bar{e}_1} \bmod p = (u_i)^{e_1} \bmod p \quad (2.42)$$

và:

$$\begin{aligned}B_i &= (v_i)^{\bar{e}_2} \times (y_{ca})^{\bar{e}_3} \bmod p \\ &= (v_i)^{e_2} \times (y_{ca})^{e_3} \bmod p\end{aligned} \quad (2.43)$$

Thay (2.1), (2.8) vào (2.43) ta được:

$$\begin{aligned}B_i &= (v_i)^{e_2} \times (y_{ca})^{e_3} \bmod p \\ &= \left((x_{ca})^{e_5} \bmod p\right)^{e_2} \times \left((x_{ca})^{x_{ca}} \bmod p\right)^{e_3} \bmod p \\ &= (x_{ca})^{(k_i - e_4) \times e_2} \times (x_{ca})^{x_{ca} \times e_3} \bmod p \\ &= (x_{ca})^{k_i \times e_2 + x_{ca} \times e_3 - e_2 \times e_4} \bmod p\end{aligned} \quad (2.44)$$

Mặt khác, từ (2.5) suy ra:

$$e_4 \times (e_1 + e_2) \bmod q = (k_i \times e_2 + x_{ca} \times e_3) \bmod q$$

Hay:

$$e_1 \times e_4 \bmod q = (k_i \times e_2 + x_{ca} \times e_3 - e_2 \times e_4) \bmod q \quad (2.45)$$

Từ (2.44), (2.45) và theo Bổ đề 2 ta được:

$$\begin{aligned}B_i &= (x_{ca})^{k_i \times e_2 + x_{ca} \times e_3 - e_2 \times e_4} \bmod p \\ &= (x_{ca})^{e_1 \times e_4} \bmod p \\ &= \left((x_{ca})^{e_4} \bmod p\right)^{e_1} \bmod p\end{aligned} \quad (2.46)$$

Thay (2.7) vào (2.46) ta được:

$$B_i = \left((x_{ca})^{e_4} \bmod p\right)^{e_1} \bmod p = (u_i)^{e_1} \bmod p \quad (2.47)$$

Từ (2.42) và (2.47) suy ra: $A_i = B_i$.

Đây là điều cần chứng minh.

b) Tính đúng đắn của thuật toán hình thành và kiểm tra chữ ký cá nhân của một nhóm đối tượng ký

Chứng minh:

Thật vậy, thay (2.19), (2.20), (2.21), (2.22) vào (2.23) và Bổ đề 3 ta có:

$$\begin{aligned}\bar{z} &= r \times s \bmod p \\ &= \left(\prod_{i=1}^{N} r_i \bmod p\right) \times \left(\prod_{i=1}^{N} s_i \bmod p\right) \bmod p \\ &= \left(\prod_{i=1}^{N} (x_i)^{e_4} \bmod p\right) \times \left(\prod_{i=1}^{N} (x_i)^{e_5} \bmod p\right) \bmod p \\ &= \prod_{i=1}^{N} (x_i)^{e_4} \times (x_i)^{e_5} \bmod p = \prod_{i=1}^{N} (x_i)^{e_4+e_5} \bmod p \\ &= \prod_{i=1}^{N} (x_i)^{(e_4+e_5) \bmod q} \bmod p\end{aligned} \quad (2.48)$$

Từ (2.19) suy ra:

$$(e_4 + e_5) \bmod q = k_i \quad (2.49)$$

Từ (2.48) và (2.49) ta được:

$$\begin{aligned}\bar{z} &= \prod_{i=1}^{N} (x_i)^{(e_4+e_5) \bmod q} \bmod p = \prod_{i=1}^{N} (x_i)^{k_i} \bmod p \\ &= \prod_{i=1}^{N} z_i \bmod p\end{aligned} \quad (2.50)$$

Từ (2.14) và (2.50) suy ra:

$$\bar{z} = z \quad (2.51)$$

Thay (2.51) vào (2.14) ta được:

$$\begin{aligned}\bar{e}_1 &= H(\bar{z} \| M) \bmod q = H(z \| M) \bmod q, \\ \bar{e}_2 &= H(\bar{z} \| y) \bmod q = H(z \| y) \bmod q, \\ \bar{e}_3 &= H(\bar{z} \| y \| M) \bmod q = H(z \| y \| M) \bmod q\end{aligned} \quad (2.52)$$

Từ (2.16) và (2.52) suy ra:

$$\bar{e}_1 = e_1,\ \bar{e}_2 = e_2,\ \bar{e}_3 = e_3$$

Nên từ (2.25) và (2.26) ta có:

$$A = (r)^{\bar{e}_1} \bmod p = (r)^{e_1} \bmod p \quad (2.53)$$

và:

$$B = (s)^{\bar{e}_2} \times (y)^{\bar{e}_3} \bmod p = (s)^{e_2} \times (y)^{e_3} \bmod p \quad (2.54)$$

Thay (2.2), (2.15), (2.20), (2.22) vào (2.54) ta được:

$$\begin{aligned} B &= (s)^{e_2} \times (y)^{e_3} \bmod p \\ &= \left(\prod_{i=1}^{N} s_i \bmod p\right)^{e_2} \times \left(\prod_{i=1}^{N} y_i \bmod p\right)^{e_3} \bmod p \\ &= \left(\prod_{i=1}^{N} (x_i)^{e_5} \bmod p\right)^{e_2} \times \left(\prod_{i=1}^{N} (x_i)^{x_i} \bmod p\right)^{e_3} \bmod p \\ &= \prod_{i=1}^{N} (x_i)^{e_2 \times e_5} \times (x_i)^{e_3 \times x_i} \bmod p = \prod_{i=1}^{N} (x_i)^{e_2 \times e_5 + e_3 \times x_i} \bmod p \\ &= \prod_{i=1}^{N} (x_i)^{e_2 \times (k_i - e_4) + e_3 \times x_i} \bmod p = \prod_{i=1}^{N} (x_i)^{e_2 \times k_i + e_3 \times x_i - e_2 \times e_4} \bmod p \end{aligned} \quad (2.55)$$

Mặt khác, từ (2.17) ta có:

$$e_4 \times (e_1 + e_2) \bmod q = (k_i \times e_2 + x_i \times e_3) \bmod q$$

Hay:

$$e_1 \times e_4 \bmod q = (k_i \times e_2 + x_i \times e_3 - e_2 \times e_4) \bmod q \quad (2.56)$$

Từ (2.55), (2.56) và theo Bổ đề 2 ta được:

$$\begin{aligned} B &= \prod_{i=1}^{N} (x_i)^{e_2 \times k_i + e_3 \times x_i - e_2 \times e_4} \bmod p \\ &= \prod_{i=1}^{N} (x_i)^{e_1 \times e_4} \bmod p \\ &= \left(\prod_{i=1}^{N} (x_i)^{e_4} \bmod p\right)^{e_1} \bmod p \end{aligned} \quad (2.57)$$

Thay (2.19), (2.21) vào (2.57) ta có:

$$\begin{aligned} B &= \left(\prod_{i=1}^{N} (x_i)^{e_4} \bmod p\right)^{e_1} \bmod p \\ &= \left(\prod_{i=1}^{N} r_i \bmod p\right)^{e_1} \bmod p = (r)^{e_1} \bmod p \end{aligned} \quad (2.58)$$

Từ (2.53) và (2.58) suy ra: A = B

Đây là điều cần phải chứng minh.

c) Tính đúng đắn của thuật toán hình thành và kiểm tra chứng nhận của CA đối với chữ ký cá nhân và bản tin cần ký

Thật vậy, thay (2.31), (2.32) vào (2.33) và theo Bổ đề 3 ta có:

$$\begin{aligned} \bar{z}_{ca} &= u \times v \bmod p \\ &= \left((x_{ca})^{e_4} \bmod p\right) \times \left((x_{ca})^{e_5} \bmod p\right) \bmod p \\ &= (x_{ca})^{e_4} \times (x_{ca})^{e_5} \bmod p = (x_{ca})^{e_4 + e_5} \bmod p \\ &= (x_{ca})^{(e_4 + e_5) \bmod q} \bmod p \end{aligned} \quad (2.59)$$

Mặt khác, từ (2.30) ta có:

$$e_4 + e_5 \bmod q = k_{ca} \quad (2.60)$$

Từ (2.59) và (2.60) dẫn đến:

$$\begin{aligned} \bar{z}_{ca} &= (x_{ca})^{(e_4 + e_5) \bmod q} \bmod p \\ &= (x_{ca})^{k_{ca}} \bmod p \end{aligned} \quad (2.61)$$

Từ (2.27) và (2.61) suy ra:

$$\bar{z}_{ca} = z_{ca} \quad (2.62)$$

Thay (2.62) vào (2.34) ta được:

$$\begin{aligned} &\bar{e}_1 = H(\bar{z}_{ca} \| y \| M) \bmod q = H(z_{ca} \| y \| M) \bmod q, \\ &\bar{e}_2 = H(\bar{z}_{ca} \| y_{ca}) \bmod q = H(z_{ca} \| y_{ca}) \bmod q, \\ &\bar{e}_3 = H(\bar{z}_{ca} \| y_{ca} \| y \| M) \bmod q \\ &\quad = H(z_{ca} \| y_{ca} \| y \| M) \bmod q \end{aligned} \quad (2.63)$$

Từ (2.28) và (2.63) suy ra:

$$\bar{e}_1 = e_1,\ \bar{e}_2 = e_2,\ \bar{e}_3 = e_3$$

Do đó, từ (2.35) và (2.36) ta có:

$$A = (u)^{\bar{e}_1} \bmod p = (u)^{e_1} \bmod p \quad (2.64)$$

và:

$$\begin{aligned} B &= (v)^{\bar{e}_2} \times (y_{ca})^{\bar{e}_3} \bmod p \\ &= (v)^{e_2} \times (y_{ca})^{e_3} \bmod p \end{aligned} \quad (2.65)$$

Thay (2.1) và (2.32) vào (2.65) ta được:

$$\begin{aligned} B &= (v)^{e_2} \times (y_{ca})^{e_3} \bmod p \\ &= \left((x_{ca})^{e_5} \bmod p\right)^{e_2} \times \left((x_{ca})^{x_{ca}} \bmod p\right)^{e_3} \bmod p \\ &= (x_{ca})^{(k_{ca} - e_4) \times e_2} \times (x_{ca})^{x_{ca} \times e_3} \bmod p \\ &= (x_{ca})^{k_{ca} \times e_2 + x_{ca} \times e_3 - e_4 \times e_2} \bmod p \end{aligned} \quad (2.66)$$

Mặt khác, từ (2.29) suy ra:

$$e_4 \times (e_1 + e_2) \bmod q = (k_{ca} \times e_2 + x_{ca} \times e_3) \bmod q$$

Hay:

$$e_1 \times e_4 \bmod q = (k_{ca} \times e_2 + x_{ca} \times e_3 - e_2 \times e_4) \bmod q \quad (2.67)$$

Từ (6.163), (6.164) và theo Bổ đề 6.2 ta được:

$$\begin{aligned} B &= (x_{ca})^{k_{ca} \times e_2 + x_{ca} \times e_3 - e_2 \times e_4} \bmod p \\ &= (x_{ca})^{e_1 \times e_4} \bmod p \\ &= \left((x_{ca})^{e_4} \bmod p\right)^{e_1} \bmod p \end{aligned} \quad (2.68)$$

Thay (2.31) vào (2.68) ta được:

$$\begin{aligned} B &= \left((x_{ca})^{e_4} \bmod p\right)^{e_1} \bmod p \\ &= (u)^{e_1} \bmod p \end{aligned} \quad (2.69)$$

Từ (2.64) và (2.69) suy ra: A = B.

Đây là điều cần chứng minh.

5. Một số kỹ thuật bảo đảm an toàn cho lược đồ ký tập thể

Về cơ bản, mức độ an toàn của lược đồ ký tập thể được thiết lập dựa trên độ an toàn của lược đồ cơ sở. Tuy nhiên, do lược đồ ký tập thể có *tính phân tán*, quá trình thực hiện thuật toán tạo chữ ký cá nhân của 1 nhóm đối tượng lên bản tin cần ký bao gồm một số bước trao đổi thông tin giữa các thành viên trong nhóm với CA, nên quá

trình tạo chữ ký của lược đồ ký tập thể sẽ tiềm ẩn nhiều nguy cơ tấn công giả mạo từ bên ngoài vào cũng như từ ngay nội bộ nhóm ký. Vì vậy, việc thực hiện một số kỹ thuật bảo đảm cho tính an toàn của lược đồ ký tập thể trước các dạng tấn công giả mạo như thế là vấn đề cần thiết phải được đặt ra. Các kỹ thuật được áp dụng ở đây bao gồm:

a) Kiểm tra tính hợp pháp của đối tượng ký

Một đối tượng là thành viên của tổ chức thì sẽ được một cấp chứng chỉ khóa công khai, chứng chỉ khóa công khai này được lưu trong một cơ sở dữ liệu khóa công khai cho phép mọi đối tượng sử dụng (thuộc hoặc không thuộc tổ chức) truy cập khi cần thiết. Khi một đối tượng không còn là thành viên của tổ chức hoặc bị tước bỏ thẩm quyền ký vào các văn bản của tổ chức thì chứng chỉ khóa công khai của đối tượng đó sẽ bị loại khỏi cơ sở dữ liệu khóa công khai của tổ chức này hoặc sẽ bị đưa vào trạng thái cấm truy cập. Trong mô hình ký tập thể, việc kiểm tra tính hợp pháp của đối tượng ký bằng Thuật toán 2.4 cho phép xác định được tư cách thành viên và thẩm quyền (ký) của một đối tượng ký ở mọi thời điểm, từ đó ngăn chặn các hành vi giả mạo tư cách thành viên của tổ chức. Hơn nữa, việc kiểm tra tính hợp pháp của đối tượng ký còn được thực hiện ở bước [2] của thuật toán hình thành chữ ký tập thể (Thuật toán 2.5) nhằm ngăn chặn các đối tượng giả mạo tham gia vào nhóm ký.

b) Kiểm tra tính hợp lệ của chữ ký cá nhân

Trong quá trình tạo chữ ký cá nhân của một nhóm đối tượng lên bản tin cần ký, ở các bước [1.3], [6], [7.5] của Thuật toán 2.5 có sự trao đổi thông tin qua lại giữa các thành viên trong nhóm ký với CA. Đây là điểm khác biệt giữa thuật toán ký tập thể với các thuật toán ký số thông thường (RSA, DSA,…) và cũng chính là yếu điểm mà kẻ tấn công giả mạo có thể lợi dụng. Do đó, việc kiểm tra tính hợp lệ của chữ ký cá nhân của nhóm ký ngay từ trong quá trình hình thành chữ ký tập thể là rất cần thiết để ngăn chặn các kiểu tấn công giả mạo từ bên ngoài vào hay từ chính bên trong nhóm ký. Việc kiểm tra tính hợp lệ của chữ ký cá nhân của nhóm ký được thực hiện ở bước [10] trong Thuật toán 2.5. Kết quả là chứng nhận của CA (và do đó chữ ký tập thể) chỉ được tạo ra khi chữ ký cá nhân của nhóm ký được xác nhận là hợp lệ.

c) Chứng nhận tính hợp pháp của đối tượng ký với từng bản tin được ký

Trong mô hình ký tập thể, một đối tượng là thành viên của một tổ chức không có nghĩa là sẽ được phép ký lên tất cả các văn bản của tổ chức này, thẩm quyền ký của mỗi đối tượng phụ thuộc vào vai trò của đối tượng đó trong tổ chức. CA là cơ quan/bộ phận chứng thực của một tổ chức sẽ thực hiện chức năng kiểm soát và chứng nhận việc ký của từng thành viên trong tổ chức đối với mỗi bản tin được ban hành từ tổ chức này. Trong thuật toán 2.5, việc kiểm tra thẩm quyền ký của một đối tượng được thực hiện ở bước [2] thông qua việc kiểm tra tính hợp pháp của đối tượng ký này, sau đó CA chứng nhận việc một nhóm đối tượng ký lên 1 bản tin cụ thể bằng cách tạo chữ ký của mình qua các bước từ [11] đến [17] với các tham số đầu vào là khóa công khai của nhóm đối tượng được phép ký, chữ ký cá nhân của nhóm ký và bản tin cần ký. Như thế, việc CA chỉ ký xác nhận lên khóa công khai của các đối tượng được phép ký và bản tin cần ký hoàn toàn có thể ngăn chặn một thành viên cố tình tham gia vào một nhóm ký (đã được xác định đối với một bản tin cần ký cụ thể) mà đối tượng này không được phép, điều đó cũng có nghĩa là một thành viên sẽ không thể ký vào một bản tin mà đối tượng đó không được phép.

IV. KẾT LUẬN

Bài báo đề xuất xây dựng lược đồ chữ ký (tập thể) có thể áp dụng cho đối tượng là các tổ chức có tư cách pháp nhân trong xã hội (cơ quan, đơn vị, doanh nghiệp,...) nhằm đảm bảo cho việc chứng thực các thông điệp dữ liệu trong các thủ tục hành chính điện tử hoàn toàn phù hợp với các thủ tục hành chính trong thực tế xã hội hiện nay. Với lược đồ chữ ký tập thể mới đề xuất, các thông điệp dữ liệu điện tử sẽ được chứng thực về nguồn gốc và tính toàn vẹn ở cả 2 cấp độ: thực thể tạo ra thông điệp dữ liệu và tổ chức (cơ quan, đơn vị,...) mà thực thể tạo ra nó là một thành viên hay bộ phận của tổ chức này. Hơn nữa, lược đồ mới đề xuất ở đây được xây dựng theo một phương pháp mới dựa trên tính khó giải của bài toán logarit rời rạc kết hợp khai căn trên Z_p, bài toán này là một dạng bài toán khó mới mà hiện thời chưa có cách giải về mặt toán học. Vì vậy, lược đồ được đề xuất có thể phù hợp với các ứng dụng yêu cầu cao về độ an toàn trong thực tế.

TÀI LIỆU THAM KHẢO

[1] Nguyễn Đức Thụy, Lưu Hồng Dũng, "Lược đồ chữ ký số xây dựng dựa trên tính khó của bài toán logarit rời rạc kết hợp khai căn trên Z_p", Tạp chí Nghiên cứu KH&CN quân sự, Số 66, 4 – 2020.

[2] Nguyen Duc Thuy, Bui The Truyen, Tong Minh Duc, Luu Hong Dung, "Constructing digital signature algorithm based on new key schemes", Journal of Science and Technique - Le Quy Don Technical University - No. 213 (12-2020).

[3] Lưu Hồng Dũng, Nguyễn Đức Thụy, "Chữ ký số tập thể - Mô hình và thuật toán", Hội thảo quốc gia lần thứ XVIII: Một số vấn đề chọn lọc của Công nghệ thông tin và truyền thông - TP HCM,05-06/11/2015..

[4] Phạm Văn Hiệp, Lưu Hồng Dũng, "Phát triển thuật toán chữ ký số tập thể", Tạp chí Nghiên cứu KH&CN quân sự, Số Đặc san CNTT, 11 – 2018.

[5] National Institute of Standards and Technology, NIST FIPS PUB 186-3. Digital Signature Standard, U.S. Department of Commerce,1994.

[6] GOST R 34.10-94. Russian Federation Standard. Information Technology. Cryptographic data Security. Produce and check procedures of Electronic Digital Signature based on Asymmetric Cryptographic Algorithm. Government Committee of the Russia for Standards, 1994 (in Russian).

A COLLECTIVE DIGITAL SIGNATURE SCHEME BASED ON THE DISCRETE LOGARIT COMBINING FINDING ROOT PROBLEM ON THE Z_p

Abstract: The paper proposes a collective digital signature schema based on the difficulty of the discrete logarithm combining finding the root problem on Z_p. This problem is a new difficult type of problems class without a mathematical solution. Therefore, the construction of a digital signature scheme based on the

difficulty of the discrete logarithm combining finding root problem has the ability to improve the security of the algorithm in practical applications.

Keywords: Collective digital signature; Collective digital signature; Discrete logarithm problem ; Discrete logarithm combining finding root problem.

Lưu Hồng Dũng Nhận học vị Tiến sỹ năm 2013. Hiện công tác tại khoa Công nghệ thông tin, Học viện Kỹ thuật Quân sự. Lĩnh vực nghiên cứu: Mật mã và An toàn thông tin.

Nguyễn Đức Thụy Nhận học vị Thạc sỹ năm 2013 Hiện công tác tại khoa Công nghệ thông tin, trường CĐ Kinh tế - Kỹ thuật Tp. Hồ Chí Minh. Lĩnh vực nghiên cứu: Mật mã và An toàn thông tin, Mạng và hệ thống thông tin.