Chữ ký số tập thể - Mô hình và thuật toán

Lưu Hồng Dũng
Khoa CNTT
Học viện Kỹ thuật Quân sự
Hà Nội, Việt Nam
Email: luuhongdung@gmail.com

Nguyễn Đức Thụy
Bộ môn Tin Học Ứng Dụng
Cao đẳng Kinh tế Kỹ thuật Thành phố Hồ Chí Minh
Hồ Chí Minh, Việt Nam
Email: thuyphulam2013@gmail.com

Tóm tắt—Bài báo đề xuất một mô hình ứng dụng chữ ký số phù hợp cho đối tượng là các cơ quan nhà nước, đơn vị hành chính, doanh nghiệp,... mà ở đó các thông điệp dữ liệu cần phải được chứng thực về nguồn gốc và tính toàn vẹn ở 2 cấp độ: thực thể ký và tổ chức (cơ quan, đơn vị, ...) mà thực thể ký là thành viên của nó. Bài báo cũng đề xuất xây dựng lược đồ chữ ký số theo mô hình ứng dụng mới này

Từ khoá: Digital Signature, Collective Digital Signature, Digital Signature Schema

I. ĐẶT VẤN ĐỀ

Trong các lĩnh vực như Chính phủ điện tử, Thương mại điện tử,… chữ ký số được sử dụng nhằm đáp ứng yêu cầu chứng thực về nguồn gốc và tính toàn vẹn của thông tin (các bản tin, thông điệp dữ liệu điện tử,…) trong giao dịch điện tử. Các mô hình ứng dụng chữ ký số hiện tại cho phép đáp ứng tốt các yêu cầu về chứng thực nguồn gốc và tính toàn vẹn của các thông điệp dữ liệu được tạo ra hay ký bởi những thực thể có tính độc lập. Tuy nhiên, khi các thực thể ký là thành viên hay bộ phận của một tổ chức (đơn vị hành chính, cơ quan nhà nước, doanh nghiệp...) thì yêu cầu về việc chứng thực nguồn gốc và tính toàn vẹn của thông tin ở cấp độ thực thể ký và cấp độ tổ chức mà thực thể ký là một thành viên hay bộ phận của nó không được đáp ứng trong các mô hình ứng dụng chữ ký số hiện tại.

Bài báo đề xuất phát triển lược đồ chữ ký số theo mô hình ứng dụng mới nhằm bảo đảm các yêu cầu chứng thực về nguồn gốc và tính toàn vẹn cho các thông điệp dữ liệu trong các giao dịch điện tử mà ở đó các thực thể ký là thành viên hay bộ phận của 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 cả 2 cấp độ: 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. Ở đây, mô hình ứng dụng chữ ký số với các yêu cầu đặt ra như trên được gọi là *mô hình chữ ký số tập thể* (Collective Signature Model) và lược đồ/thuật toán chữ ký số xây dựng theo mô hình như thế được gọi là *lược đồ/thuật toán chữ ký số tập thể* (Collective Signature Schema/Algorithm).

II. MÔ HÌNH VÀ THUẬT TOÁN CHỮ KÝ SỐ TẬP THỂ

A. *Mô hình chữ ký số tập thể*

Mô hình chữ ký số tập thể được đề xuất cơ bản dựa trên cấu trúc của một *Hạ tầng cơ sở khóa công khai* - PKI (Public Key Infrastructures) [1] nhằm bảo đảm các chức năng về *chứng thực số* cho đối tượng áp dụng là các tổ chức có tư cách pháp nhân trong xã hội (đơn vị hành chính, cơ quan nhà nước, doanh nghiệp...). Trong mô hình này, đối tượng ký là một hay một nhóm thành viên của một tổ chức, chữ ký của các thành viên ở đây được gọi là *chữ ký cá nhân*. Cũng trong mô hình này, *Cơ quan chứng thực* - CA (Certificate Authority) là bộ phận có chức năng bảo đảm các dịch vụ chứng thực số, như: chứng nhận một đối tượng ký là thành viên của tổ chức, chứng thực các thông điệp dữ liệu được ký bởi các thành viên trong một tổ chức, mà CA là cơ quan chứng thực thuộc tổ chức này. Tính hợp lệ về nguồn gốc và tính toàn vẹn của một thông điệp dữ liệu ở cấp độ của một tổ chức chỉ có giá trị khi nó đã được CA thuộc tổ chức này chứng thực. Trong mô hình này, chữ ký của CA cùng với chữ ký cá nhân của các đối tượng ký hình thành nên chữ ký tập thể cho một thông điệp dữ liệu. Một hệ thống cung cấp dịch vụ chứng thực số xây dựng theo mô hình mới đề xuất sẽ bao gồm các hoạt động cơ bản như sau:

1) Phát hành, quản lý Chứng chỉ khóa công khai.

Trong mô hình chữ ký tập thể, *chứng chỉ khóa công khai* - PKC (Public Key Certificate) hay chứng chỉ số được sử dụng để một tổ chức chứng nhận các đối tượng ký là thành viên của nó.

Cấu trúc cơ bản của một PKC bao gồm khóa công khai của chủ thể chứng chỉ và các thông tin khác như: Thông tin nhận dạng của chủ thể, Trạng thái hoạt động của chứng chỉ, Số hiệu chứng chỉ, Thông tin nhận dạng của CA,... Không làm mất tính tổng quát, ở đây sử dụng thuật ngữ Thông tin nhận dạng (ID_i) của đối tượng ký để đại diện cho các thành phần thông tin nói trên. Trong thực tế, có thể sử dụng khuôn dạng chứng chỉ X.509 [2] cho chứng

chỉ khóa công khai trong mô hình chữ ký tập thể được đề xuất.

2) Hình thành và kiểm tra chữ ký số tập thể.

Chữ ký tập thể được hình thành trên cơ sở chữ ký cá nhân của thực thể ký (một hoặc một nhóm đối tượng ký) và chứng nhận của CA với vai trò chứng thực của tổ chức đối với thông điệp dữ liệu cần ký. Có thể hình thành chữ ký tập thể ở 2 dạng như sau:

- *Chữ ký tập thể dạng kết hợp*: ở dạng này CA ký trực tiếp lên thông điệp dữ liệu như các thành viên khác, chữ ký của CA và chữ ký cá nhân của các đối tượng ký được kết hợp với nhau theo một qui tắc nhất định để hình thành chữ ký tập thể.
- *Chữ ký tập thể dạng phân biệt*: ở dạng này chữ ký tập thể bao gồm chữ ký cá nhân của thực thể ký và chữ ký của CA là 2 thành phần phân biệt hay tách biệt nhau.

Trong bài báo, chữ ký tập thể dạng phân biệt được sử dụng do có khả năng chống lại hiệu quả các kiểu tấn công tập thể từ bên trong hệ thống.

Ở lược đồ chữ ký tập thể mới đề xuất, chứng nhận của CA về việc một hay một nhóm đối tượng ký lên một thông điệp dữ liệu 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.
- CA chứng thực tính hợp lệ của chữ ký cá nhân với thông điệp dữ liệu bằng cách ký lên bản tin được tạo ra từ thông điệp dữ liệu cần ký và khóa công khai của các đối tượng ký.

Bằng cách đó, lược đồ chữ ký tập thể mới đề xuất có khả năng ngăn chặn hiệu quả các dạng tấn công tập thể từ bên trong hệ thống do các đối tượng ký là thành viên của chính tổ chức đó liên kết với nhau gây ra. Kiểm tra tính hợp lệ của chữ ký tập thể được thực hiện qua các bước:

- Kiểm tra chứng nhận của CA.
- Kiểm tra tính hợp lệ của chữ ký cá nhân.

<u>*Chú ý*</u>:

Kiểm tra chữ ký cá nhân cần phải được thực hiện sau khi kiểm tra chứng nhận của CA, nếu chứng nhận của CA và chữ ký cá nhân được công nhận hợp lệ thì tính toàn vẹn của thông điệp dữ liệu cần thẩm tra được bảo đảm, đồng thời khẳng định thông điệp dữ liệu này được ký bởi các đối tượng là thành viên của tổ chức.

B. Xây dựng lược đồ chữ ký số tập thể

1) Lược đồ cơ sở

Lược đồ cơ sở ở đây được xây dựng theo [5] và được sử dụng để xây dựng lược đồ chữ ký tập thể ở mục tiếp theo, bao gồm các thuật toán hình thành tham số và khóa, thuật toán hình thành và kiểm tra chữ ký được chỉ ra sau đây:

a) Thuật toán hình thành tham số và khóa

Thuật toán 1.1a: Hình thành các tham số hệ thống.

Input: lp, lq - độ dài (tính theo bit) của số nguyên tố p, q.

Output: p, q, g, H(.).

[1]. **select** p, q: *len*(p) = lp, *len*(q)= lq, q|(p-1)

[2]. **select**: h ∈ $\mathbb{Z}_p^*$

[3]. $g \leftarrow h^{(p-1)/q} \bmod p$ (1.1)

[4]. **if** (g = 1) **then goto** [2]

[5]. **select** H: $\{0,1\}^* \rightarrow Z_q$

[6]. **return** {p, q, g, H(.)}

<u>*Chú thích:*</u>

- *len*(.) là hàm tính độ dài (theo bit) của một số.

Thuật toán 1.1b: Hình thành khóa.

Input: p, q, g, x – khóa bí mật của đối tượng ký U.

Output: y – khóa công khai của đối tượng ký U.

[1]. $y \leftarrow g^{-x} \bmod p$ (1.2)

[2]. return (y)

b) Thuật toán hình thành chữ ký

Thuật toán 1.2: Hình thành chữ ký.

Input: p, q, g, H(.), k, x, M – thông điệp dữ liệu cần ký.

Output: (r,s) – chữ ký của U lên M.

[1]. $e \leftarrow H(M)$ (1.3)

[2]. $r \leftarrow \left(g^k \bmod\right) p \bmod q$ (1.4)

[3]. $s \leftarrow k \times e^{-1} + x \times r \bmod q$ (1.5)

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

c) Thuật toán kiểm tra chữ ký

Thuật toán 1.3: Kiểm tra chữ ký.

Input: p, q, g, y, H(.), M, (r,s).

Output: (r,s) = true / false.

[1]. $e \leftarrow H(M)$ (1.6)

[2]. $u \leftarrow \left(g^{s.e} \times y^{r.e} \bmod p\right) \bmod q$ (1.7)

[3]. **if** (u = r) **then** {**return** *true*} (1.8)
else {**return** *false*}

d) Tính đúng đắn của lược đồ cơ sở

Chứng minh tính đúng đắn của lược đồ cơ sở được thực hiện dựa trên các cơ sở như sau:

Bổ đề 1.1:

Cho p và q là 2 số nguyên tố với q là ước số của (p-1), h là một số nguyên dương nhỏ hơn p. Nếu: $g = h^{(p-1)/q} \bmod p$ thì: $g^q \bmod p = 1$.

<u>*Chứng minh*</u>:

Ta có:

$$g^q \bmod p = \left(h^{(p-1)/q} \bmod p\right)^q \bmod p = h^{(p-1)} \bmod p$$

Theo định lý Fermat thì: $h^{(p-1)} \bmod p = 1$

Vì vậy: $g^q \bmod p = 1$. Bổ đề được chứng minh.

Bổ đề 1.2:

Cho p và q là 2 số nguyên tố với q là ước số của (p -1), h là một số nguyên dương nhỏ hơn p và $g = h^{(p-1)/q} \bmod p$. Nếu: $m \bmod q = n \bmod q$ thì: $g^m \bmod p = g^n \bmod p$.

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:

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

Theo Bổ đề 1.1 ta có: $g^q \bmod p = 1$. Nên:

$$g^m \bmod p = \left(g^n \bmod p\right) \times 1^k \bmod p = g^n \bmod p$$

Bổ đề đã được chứng minh.

Mệnh đề 1.1:

Cho p và q là 2 số nguyên tố với q là ước số của (p-1), h là một số nguyên dương nhỏ hơn p và $g = h^{(p-1)/q} \bmod p$, $1 < x, k < p$, $1 < e_1, e_2 < q$. Nếu: $y = g^{-x} \bmod p$, $r = \left(g^k \bmod p\right) \bmod q$, $s = k \times e_1^{-1} + x \times e_2 \bmod q$ thì: $\left(g^{e_1.s} \times y^{e_1.e_2} \bmod p\right) \bmod q = r$.

Chứng minh:

Thật vậy, ta có:

$$s = k \times e_1^{-1} + x \times e_2 \bmod q$$
$$= e_1^{-1} \times \left(k + x \times e_1 \times e_2\right) \bmod q$$

Nên: $s \times e_1 \bmod q = k + x \times e_1 \times e_2 \bmod q$

Theo Bổ đề 1.2 ta có:

$$g^{e_1.s} \bmod p = g^{k+x.e_1.e_2} \bmod p$$

Suy ra: $g^{e_1.s} \times g^{-x.e_1.e_2} \bmod p = g^k \bmod p$

Hay: $g^{e_1.s} \times y^{e_1.e_2} \bmod p = g^k \bmod p$

Nên ta có:

$$\left(g^{e_1.s} \times y^{e_1.e_2} \bmod p\right) \bmod q = \left(g^k \bmod p\right) \bmod q$$

Do: $r = \left(g^k \bmod p\right) \bmod q$

Dẫn đến: $\left(g^{e_1.s} \times y^{e_1.e_2} \bmod p\right) \bmod q = r$

Đây là điều cần chứng minh.

Chứng minh tính đúng đắn của lược đồ cơ sở là chứng minh chữ ký được tạo ra bởi thuật toán hình thành chữ ký (*Thuật toán 1.2*) sẽ thỏa mãn điều kiện (1.8) của thuật toán kiểm tra chữ ký (*Thuật toán 1.3*). Tính đúng đắn của lược đồ cơ sở được chứng minh như sau:

Đặt: $e_1 = e$, $e_2 = r$. Theo (1.1), (1.2), (1.3), (1.4), (1.5) và Mệnh đề 1.1 ta có:

$$\left(g^{s.e} \times y^{r.e} \bmod p\right) \bmod q = r \qquad (1.9)$$

Từ (1.6), (1.7) và (1.9) suy ra: u = r.

Mệnh đề đã được chứng minh.

e) Mức độ an toàn của lược đồ cơ sở

Lược đồ cơ sở là một lược đồ chữ ký số xây dựng dựa trên tính khó của bài toán logarit rời rạc – DLP (Discrete Logarithm Problem) tương tự như các lược đồ chữ ký thuộc họ ElGamal như DSA [3] hay GOST R34.10-94 [4]. Do vậy, mức độ an toàn của lược đồ cơ sở xét theo khả năng chống tấn công làm lộ khóa mật hoàn toàn phụ thuộc vào mức độ khó của bài toán DLP như ở DSA hay GOST R34.10-94.

Về khả năng chống giả mạo chữ ký của lược đồ cơ sở, từ (1.6), (1.7) và (1.8) cho thấy 1 cặp (r,s) bất kỳ sẽ được coi là chữ ký hợp lệ với M nếu thỏa mãn điều kiện: $r = \left(g^{s.e} \times y^{r.e} \bmod p\right) \bmod q$ (1.10)

Ở đây: $e = H(M)$ là giá trị đại diện của thông điệp dữ liệu cần thẩm tra (M). Dễ dàng thấy rằng việc giải (1.10) để để tạo được chữ ký giả mạo thỏa mãn điều kiện hợp lệ của lược đồ cơ sở thực chất cũng là việc giải bài toán DLP.

2) Lược đồ chữ ký tập thể

Lược đồ chữ ký tập thể ở đây được phát triển từ lược đồ cơ sở với các chức năng như sau:

- Chứng nhận tính hợp pháp của các đối tượng ký.
- Hình thành chữ ký tập thể từ chữ ký cá nhân của một hay một nhóm đối tượng ký và chữ ký của CA. 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.

Các tham số hệ thống {p, q} được lựa chọn theo phương pháp của DSA hoặc GOST R34.10-94. 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}. Còn CA có cặp khóa bí mật/công khai tương ứng là: {x_{ca}, y_{ca}}.

a) Thuật toán hình thành khóa của các đối tượng ký

Thuật toán 2.1: Hình thành khóa của các đối tượng ký **U** = {U_i| i=1,2,..,n}.

Input: p, g, n, K_S = {x_i| i = 1,2,…,n}.

Output: K_P = {y_i| i = 1, 2,..,n}.

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

[1.1]. $y_i \leftarrow g^{-x_i} \bmod p$ (2.1)

[1.2]. $K_p[i] \leftarrow y_i$

[2]. **return** K_P

b) Thuật toán hình thành khóa của CA

Thuật toán 2.2: Hình thành khóa của CA.

Input: p, g, x_{ca}.

Output: y_{ca}.

[1]. $y_{ca} \leftarrow g^{-x_{ca}} \bmod p$ (2.2)

[2]. **return** y_{ca}

c) Thuật toán hình thành chứng nhận (chứng chỉ số) của CA cho các đối tượng ký U_i

Thuật toán 2.3: CA chứng nhận tính hợp pháp của đối tượng ký U_i.

Input: ID_i, y_i, x_{ca}.

Output: (u_i,v_i) – chứng nhận của CA đối với U_i.

[1]. $k_i \leftarrow H(x_{ca} \| y_i \| ID_i)$

[2]. $u_i \leftarrow \left(g^{k_i} \bmod p\right) \bmod q$ (2.3)

[3]. $e \leftarrow H(y_i \| ID_i)$ (2.4)

[4]. $v_i \leftarrow k_i \times e^{-1} + x_{ca} \times u_i \bmod q$ (2.5)

[5]. **return** (u_i,v_i);

d) Thuật toán kiểm tra tính hợp pháp của các đối tượng ký U_i (i=1,2,..,n)

Thuật toán 2.4: Kiểm tra tính hợp pháp các đối tượng ký.

Input: y_i, y_{ca}, IDi, (u_i, v_i).

Output: (u_i,v_i) = true / false.

[1]. $e \leftarrow H(y_i \| ID_i)$ (2.6)

[2]. $u \leftarrow \left(g^{v_i \cdot e} \times \left(y_{ca}\right)^{u_i \cdot e} \bmod p\right) \bmod q$ (2.7)

[3]. **if** $(u = u_i)$ **then** {**return** *true*}
else {**return** *false*}

e) Thuật toán hình thành chữ ký cá nhân của một hay một nhóm đối tượng ký lên thông điệp dữ liệu M

Thuật toán 2.5: Hình thành chữ ký cá nhân.

Input: M, n, $KS = \{x_i | i = 1, 2,..,n\}$,
$KP = \{y_i | i = 1, 2,..,n\}$.

Output: (r,s) – chữ ký của U_i (i = 1, 2,..) lên M.

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

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

[1.2]. $r_i \leftarrow g^{k_i} \bmod p$ (2.8)

[1.3]. U_i **send** r_i **to** CA

[2]. $r \leftarrow 1$;

[2.1]. **for** i = 1 **to** n **do**

$r \leftarrow r \times r_i \bmod p$ (2.9)

[2.2]. CA **send** r **to** U_i (i = 1, 2,.., n)

[3]. **for** i = 1 **to** n **do**

[3.1]. $e \leftarrow H(M)$ (2.10)

[3.2]. $s_i \leftarrow k_i \times e^{-1} + x_i \times r \bmod q$ (2.11)

[3.3]. U_i **send** s_i **to** CA

[4]. $s \leftarrow 1$; **for** i = 1 **to** n **do**

[4.1]. **if** $\left(r_i \neq g^{s_i \cdot e} \times \left(y_i\right)^{r_i \cdot e} \bmod p\right)$ **then** **return** (0,0)

[4.2]. $s \leftarrow s \times s_i \bmod q$ (2.12)

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

<u>*Chú thích*</u>:

- Bước [1] và [3] được thực hiện bởi U_i (i = 1, 2,.., n).
- Bước [2] và [4] được CA thực hiện.

f) Thuật toán hình thành chứng nhận của CA đối với chữ ký cá nhân của một hay một nhóm đối tượng ký lên M

Thuật toán 2.6: Hình thành chứng nhận của CA cho chữ ký cá nhân với thông điệp dữ liệu M.

Input: p, q, g, x_{ca}, n, $KP = \{y_i | i = 1, 2,..,n\}$,
$(u_i,v_i),\{M, (r,s)\}$.

Output: (u_M,v_M) – chứng nhận của CA đối với $\{M, (r,s)\}$.

[1]. y ← 1; **for** i = 1 **to** n **do**

[1.1]. $e \leftarrow H(y_i \| ID_i)$

[1.2]. $u \leftarrow \left(g^{v_i \cdot e} \times \left(y_{ca}\right)^{u_i \cdot e} \bmod p\right) \bmod q$

[1.3]. **if** $(u \neq u_i)$ **then return** (0,0)

[1.4]. $y \leftarrow y \times y_i \bmod p$

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

[2.1]. $e \leftarrow H(M)$

[2.2]. $u \leftarrow \left(g^{s \cdot e} \times y^{r \cdot e} \bmod p\right) \bmod q$

[2.3]. **if** $(u \neq r)$ **then** {**return** (0,0)}

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

[4]. $u_M \leftarrow \left(g^k \bmod p\right) \bmod q$ (2.13)

[5]. $e \leftarrow H(y \| M)$ (2.14)

[6]. $v_M \leftarrow k \times e^{-1} + x_{ca} \times u_M \bmod q$ (2.15)

[7]. **return** (u_M,v_M)

g) Thuật toán kiểm tra chữ ký tập thể của một hay một nhóm đối tượng ký lên thông điệp dữ liệu M

Thuật toán 2.7: Kiểm tra chữ ký tập thể.

Input: p, q, g, n, y_{ca}, $KP=\{y_i | i = 1, 2,.., n\}$,
$M,\{(r,s), (u_M,v_M)\}$.

Output: $\{(r,s), (u_M,v_M)\}$ = true / false.

[1]. y ← 1; **for** i = 1 **to** n **do**

$y \leftarrow y \times y_i \bmod p$ (2.16)

[2]. **if** $(u_M = 0$ **or** $v_M = 0)$ **then return** *false*

[2.1]. $e \leftarrow H(y \| M)$ (2.17)

[2.2]. $u \leftarrow \left(g^{v_M \cdot e} \times \left(y_{ca}\right)^{u_M \cdot e} \bmod p\right) \bmod q$ (2.18)

[2.3]. **if** $(u \neq u_M)$ **then return** *false*

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

[3.1]. $e \leftarrow H(M)$ (2.19)

[3.2]. $u \leftarrow \left(g^{s \cdot e} \times y^{r \cdot e} \bmod p\right) \bmod q$ (2.20)

[3.3]. **if** $(u = r)$ **then** {**return** *true*}
else {**return** *false*}

3) Tính đúng đắn của lược đồ chữ 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.

Đặt: $e_1 = e$, $e_2 = u_i$, $s = v_i$, $x = x_{ca}$, $y = y_{ca}$. Theo (2.2), (2.3), (2.5) và Mệnh đề 1.1 ta có:

$$\left(g^{v_i \cdot e} \times \left(y_{ca}\right)^{u_i \cdot e} \bmod p\right) \bmod q = u_i \quad (2.21)$$

Từ (2.21) và (2.7) suy ra: $u = u_i$

Đây là điều cần chứng minh.

b) Tính đúng đắn của thuật toán hình thành và kiểm tra chứng nhận của CA đối với chữ ký cá nhân của một đối tượng ký.

Đặt: $e_1 = e$, $e_2 = u_M$, $s = v_M$, $y = y_{ca}$. Theo (2.2), (2.13), (2.14), (2.15) và Mệnh đề 1.1, ta có:

$$\left(g^{v_M \cdot e} \times \left(y_{ca}\right)^{u_M \cdot e} \bmod p\right) \bmod q = u_M \qquad (2.22)$$

Từ (2.16), (2.17), (2.18) và (2.22) suy ra:

$u = u_M$

Đây là điều cần chứng minh.

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

Mệnh đề 1.2:

Cho p và q là 2 số nguyên tố với q là ước số của (p -1), h là một số nguyên dương nhỏ hơn p và $g = h^{(p-1)/q} \bmod p$, $1 < x_i, k_i < q$, $1 < e_1, e_2 < q$. Nếu: $y_i = g^{-x_i} \bmod p$, $r_i = g^{k_i} \bmod p$, $s_i = k_i \times e_1^{-1} + x_i \times e_2 \bmod q$ với: $i = \overline{1,n}$, $y = \prod_{i=1}^{n} y_i \bmod p$, $r = \left(\prod_{i=1}^{n} r_i \bmod p\right) \bmod q$, $s = \sum_{i=1}^{n} s_i \bmod q$ thì: $\left(g^{e_1 \cdot s} \times y^{e_1 \cdot e_2} \bmod p\right) \bmod q = r$.

<u>*Chứng minh*</u>:

Thật vậy, ta có:

$$\left(g^{e_1 \cdot s} \times y^{e_1 \cdot e_2} \bmod p\right) \bmod q =$$

$$= \left(g^{e_1 \cdot \sum_{i=1}^{n} k_i \cdot e_1^{-1} + x_i \cdot e_2 \bmod q} \times \left(\prod_{i=1}^{n} y_i \bmod p\right)^{e_1 \cdot e_2} \bmod p \right) \bmod q$$

$$= \left(g^{e_1 \cdot \sum_{i=1}^{n} k_i \cdot e_1^{-1}} \times g^{e_1 \cdot \sum_{i=1}^{n} x_i \cdot e_2} \times g^{-\sum_{i=1}^{n} x_i e_1 \cdot e_2 \cdot} \bmod p \right) \bmod q$$

$$= \left(g^{\sum_{i=1}^{n} k_i} \bmod p \right) \bmod q = \left(\prod_{i=1}^{n} \left(g^{k_i} \bmod p\right) \bmod p \right) \bmod q$$

$$= \left(\prod_{i=1}^{n} r_i \bmod p \right) \bmod q = r$$

Từ đó tính đúng đắn của thuật toán hình thành và kiểm tra chữ ký của một hoặc một nhóm đối tượng ký lên một thông điệp dữ liệu M được chứng minh như sau:

Đặt: $e_1 = e$, $e_2 = r$. Theo (2.9), (2.10), (2.12), (2.16) và Mệnh đề 1.2, ta có:

$$\left(g^{s \cdot e} \times y^{r \cdot e} \bmod p\right) \bmod q = r \qquad (2.23)$$

Từ (2.23) và (2.20) suy ra: $u = r$

Mệnh đề đã được chứng minh.

4) Mức độ an toàn của lược đồ chữ ký tập thể

Mức độ an toàn của lược đồ chữ ký tập thể mới đề xuất được thiết lập dựa trên mức độ an toàn của lược đồ cơ sở. Do vậy, về cơ bản mức độ an toàn của nó được quyết định bởi mức độ khó của bài toán DLP. Ngoài ra, ở lược đồ chữ ký tập thể còn tiềm ẩn các nguy cơ tấn công giả mạo chữ ký từ ngay bên trong hệ thống do một nhóm đối tượng ký liên kết với nhau thực hiện. Vấn đề này được xem xét dưới góc độ *Bài toán giả mạo chữ ký nhóm* như sau:

a) Bài toán giả mạo chữ ký nhóm

Cho U và U* với $U \not\subset U^*$ là hai nhóm các đối tượng trong hệ thống có các tham số {*p, q, g*}.

Giả thiết: $U^* = \{U^*_i | \ i=1...m^*\}$, $U' = \{U'_i | \ i=1...m'\}$, $U^* \cap U' = \varnothing$ và $U^* \cup U' = U$. (3.1)

Khi này Bài toán giả mạo chữ ký nhóm có thể được mô tả như sau:

Bài toán LD$_{(U,U^*)}$: *Cho các tham số bí mật của các thành viên trong U*. Khi đó với mỗi thông báo M, hãy tìm cặp {r,s} được chấp nhận theo điều kiện của thuật toán kiểm tra chữ ký (Thuật toán 2.7) với đầu vào là bộ tham số công khai của U.*

Bài toán LD$_{(U',U^*)}$: *Cho các tham số bí mật của các thành viên trong U*. Khi đó với mỗi thông báo M, hãy tìm cặp {r',s'} được chấp nhận theo điều kiện của thuật toán kiểm tra chữ ký (Thuật toán 2.7) với đầu vào là bộ tham số công khai của U'.*

Giải thuật cho bài toán LD$_{(U,U^*)}$ được gọi là "*thuật toán giả mạo chữ ký của U lên M do U* thực hiện*". Còn giải thuật cho bài toán LD$_{(U',U^*)}$ được gọi là "*thuật toán giả mạo chữ ký của U' lên M do U* thực hiện*".

b) Giải thuật cho bài toán LD$_{(U,U^*)}$

Thuật toán 3.1 Giải thuật cho bài toán LD$_{(U,U^*)}$.

Input: p, q, g, M, (r',s') – chữ ký của U' lên M.

Output: (r,s) – chữ ký của U lên M do U* tạo ra.

[1]. $s^* \leftarrow 0$

[2]. **for** i = 1 **to** m* **do**

$$s^* \leftarrow s^* + x_i^* \times r' \bmod q \qquad (3.2)$$

[3]. $s \leftarrow s' + s^* \bmod q$ (3.3)

[4]. $r \leftarrow r'$ (3.4)

[5]. **return** (r,s);

Tính đúng đắn của *Thuật toán 3.1* được chứng minh như sau:

Từ (3.2) với mọi: $i = 1,2,..,m^*$, ta có:

$$g^{s_i^* \cdot e} \times \left(y_i^*\right)^{r' \cdot e} \bmod p = g^{x_i^* \cdot r' \cdot e} \times g^{-x_i^* \cdot r' \cdot e} \bmod p = 1 \qquad (3.5)$$

Với điều kiện (3.1), dễ dàng kiểm tra được rằng:

$$y = y' \times \left(\prod_{i=1}^{m^*} y_i^* \bmod p \right) \bmod q \qquad (3.6)$$

Từ (3.5) và (3.6) ta có:

$$\left(g^{s.e}\times y^{r.e} \bmod p\right)\bmod q =$$
$$=\left(g^{\left(s'+\sum_{i=1}^{m^*}s_i^*\right).e}\times\left(y'\times\left(\prod_{i=1}^{m^*}y_i^* \bmod p\right)\bmod p\right)^{r.e} \bmod p\right)\bmod q$$
$$=\left(g^{s'.e}\times(y')^{r.e}\times g^{\left(\sum_{i=1}^{m^*}s_i^*\right).e}\times\left(\prod_{i=1}^{m^*}y_i^*\right)^{r.e} \bmod p\right)\bmod q$$
$$=\left(g^{s'.e}\times(y')^{r'.e}\times\prod_{i=1}^{m^*}\left(g^{s_i^*.e}\times\left(y_i^*\right)^{r'.e} \bmod p\right)\bmod p\right)\bmod q$$
$$=\left(g^{s'.e}\times(y')^{r'.e} \bmod p\right)\bmod q = r' \qquad (3.7)$$

Từ (2.20), (3.4) và (3.7) suy ra:

$$u = r \qquad (3.8)$$

Từ (3.8) cho thấy, mặc dù (*r,s*) do U* tạo ra nhưng vẫn được công nhận là chữ ký hợp lệ của U lên M.

c) Giải thuật cho bài toán $LD_{(U',U^*)}$

Thuật toán 3. 2 Giải thuật cho bài toán $LD_{(U',U^*)}$.

Input: p, q, g, M, (r,s) - chữ ký của U lên M.

Output: (r',s') - chữ ký của U' lên M do U* tạo ra.

[1]. $s^* \leftarrow 0$

[2]. **for** i = 1 **to** m* **do**

$$s^* \leftarrow s^* + x_i^* \times r \bmod q \qquad (3.9)$$

[3]. $s' \leftarrow s - s^* \bmod q$ (3.10)

[4]. $r' \leftarrow r$ (3.11)

[5]. **return** (r',s');

Tính đúng đắn của *Thuật toán 3.2* được chứng minh như sau:

Từ (3.9) với mọi: i = 1,2,..,m*, ta có:

$$g^{-s_i^*.e}\times\left(y_i^*\right)^{-r.e} \bmod p = g^{-x_i^*.r.e}\times g^{x_i^*.r.e} \bmod p = 1 \qquad (3.12)$$

Với điều kiện (3.1), dễ dàng kiểm tra được rằng:

$$y' = y\times\left(\prod_{i=1}^{m^*}\left(y_i^*\right)^{-1} \bmod p\right)\bmod p \qquad (3.13)$$

Từ (2.12) và (2.13) ta có:

$$\left(g^{s'.e}\times(y')^{r'.e} \bmod p\right)\bmod q = \left(g^{(s-s^*).e}\times(y')^{r.e} \bmod p\right)\bmod q$$
$$=\left(g^{\left(s-\sum_{i=1}^{m^*}s_i^*\right).e}\times\left(y\times\left(\prod_{i=1}^{m^*}\left(y_i^*\right)^{-1} \bmod p\right)\bmod p\right)^{r.e} \bmod p\right)\bmod q$$
$$=\left(g^{s.e}\times y^{r.e}\times g^{\left(-\sum_{i=1}^{m^*}s_i^*\right).e}\times\left(\prod_{i=1}^{m^*}y_i^*\right)^{-r.e} \bmod p\right)\bmod q$$
$$=\left(g^{s.e}\times y^{r.e}\times\prod_{i=1}^{m^*}\left(g^{-s_i^*.e}\times\left(y_i^*\right)^{-r.e} \bmod p\right)\bmod p\right)\bmod q$$
$$=\left(g^{s.e}\times y^{r.e} \bmod p\right)\bmod q = r \qquad (3.14)$$

Từ (2.20), (3.11) và (3.14) suy ra:

$$u = r' \qquad (3.15)$$

Từ (3.15) cho thấy, mặc dù (*r',s'*) do U* tạo ra nhưng vẫn được công nhận là chữ ký hợp lệ của U' lên M, nói cách khác *Thuật toán 3.2* đã được chứng minh là đúng.

d) Mức độ an toàn của lược đồ chữ ký tập thể trước các tấn công giả mạo chữ ký nhóm.

Từ việc xem xét *Bài toán $LD_{(U,U^*)}$* và $LD_{(U',U^*)}$ cho thấy việc xây dựng theo mô hình chữ ký tập thể dạng phân biệt, mà ở đó CA tạo chứng nhận về tính hợp lệ của chữ ký cá nhân của một đối tượng ký hay của một nhóm đối tượng ký lên một thông điệp dữ liệu bằng cách ký lên bản tin được tạo ra từ thông điệp dữ liệu cần ký và khóa công khai chung của nhóm đối tượng ký, vì thế lược đồ chữ ký tập thể mới đề xuất có khả năng ngăn chặn hoàn toàn các dạng tấn công giả mạo từ bên trong hệ thống đã biết trong thực tế.

III. KẾT LUẬN

Bài báo đề xuất một mô hình ứng dụng chữ ký số gọi là mô hình chữ ký tập thể và lược đồ chữ ký số theo mô hình ứng dụng này có thể áp dụng cho đối tượng là các 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. Theo mô hình 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.

TÀI LIỆU THAM KHẢO

[1] C. Adams, "Understanding Public Key Infrastructures", New Riders Publishing, Indianapolis, 1999.

[2] R. Housley, W. Polk, W. Ford, D. Solo, "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile", RFC 3280, 2002.

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

[4] 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).

[5] Lưu Hồng Dũng, Lê Đình Sơn, Hồ Nhật Quang, Nguyễn Đức Thụy, Developing Digital Signature Schemes Base on Discrete Logarithm Problem, Kỷ yếu Hội nghị Khoa học Quốc gia lần thứ 8 về Nghiên cứu Cơ bản và Ứng dụng Công nghệ Thông tin (FAIR 2015 – Fundamental and Applied IT Reseach) 9-10/7/2015.