Kỷ yếu Hội nghị KHCN Quốc gia lần thứ XI về Nghiên cứu cơ bản và ứng dụng Công nghệ thông tin (FAIR); Hà Nội, ngày 09-10/8/2018
DOI: 10.15625/vap.2018.00012

CHỮ KÝ SỐ - MÔ HÌNH ỨNG DỤNG VÀ THUẬT TOÁN

Phạm Văn Hiệp[1], Lưu Hồng Dũng[2]

[1] Khoa CNTT, Đại học Công nghiệp Hà Nội
[2] Khoa CNTT, Học viện KTQS

hieppv@haui.edu.vn, luuhongdung@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 hai cấp độ: thực thể ký và tổ chức (cơ quan, đơn vị, ...) mà thực thể ký là thành viên của nó. Đồng thời bài báo cũng đề xuất lược đồ chữ ký số phù hợp theo mô hình ứng dụng này. Lược đồ mới đề xuất ở đây được phát triển từ một dạng lược đồ chữ ký số được xây dựng dựa trên tính khó của việc giải đồng thời hai bài toán phân tích số và logarit rời rạc trên vành* Z_n.

Từ khóa: *Chữ ký số, chữ ký số tập thể, lược đồ chữ ký số, thuật toán chữ ký số.*

I. ĐẶT VẤN ĐỀ

Trong các giao dịch 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 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 bởi những thực thể có tính độc lập. Tuy nhiên, trong các mô hình hiện tại khi mà các thực thể tạo ra thông tin là thành viên hay bộ phận của một tổ chức (đơn vị hành chính, hệ thống kỹ thuật, ...) thì nguồn gốc và tính toàn vẹn của thông tin ở cấp độ tổ chức mà thực thể tạo ra nó là một thành viên hay bộ phận lại không được chứng thực. Nói cách khác, yêu cầu về việc chứng thực đồng thời về nguồn gốc và tính toàn vẹn của thông tin ở cấp độ thực thể tạo ra nó và cấp độ tổ chức mà thực thể tạo ra thông tin là một thành viên hay bộ phận của nó không được đáp ứng trong các mô hình ứng dụng chữ ký số hiện tại. Trong khi đó, các yêu cầu như thế ngày càng trở nên cần thiết để bảo đảm cho việc chứng thực thông tin trong các thủ tục hành chính điện tử phù hợp với các thủ tục hành chính trong thực tế.

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 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. 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 CHỮ KÝ SỐ TẬP THỂ

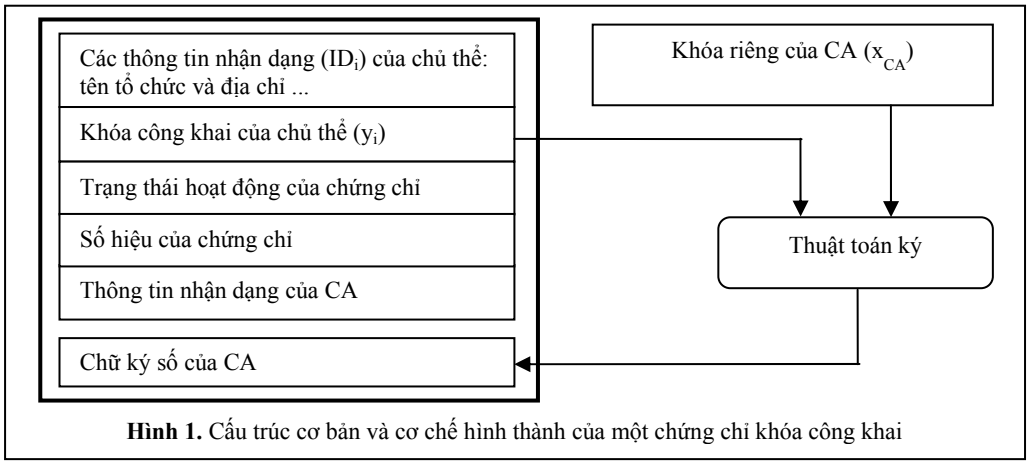
Mô hình chữ ký số tập thể được đề xuất cơ bản dựa trên cấu trúc của một PKI truyền thống [1] nhằm bảo đảm các chức năng về chứng thực số [3] cho đối tượng áp dụng là các tổ chức có tư cách pháp nhân trong xã hội (đơn vị hành chính, cơ quan nhà nước, doanh nghiệp...). Trong mô hình này, đối tượng ký là một hay một nhóm thành viên của một tổ chức và được phép ký lên các thông điệp dữ liệu với danh nghĩa thành viên của tổ chức này. Cũng trong mô hình này, CA là bộ phận có chức năng bảo đảm các dịch vụ chứng thực số như: chứng nhận một thực thể là thành viên của tổ chức, chứng thực các thông điệp dữ liệu được ký bởi các thực thể là 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, việc chứng thực được thực hiện bằng chữ ký của CA tương tự như việc CA chứng thực khóa công khai cho các thực thể cuối trong các mô hình PKI truyền thống. Trong mô hình này, chữ ký của CA cùng với chữ ký cá nhân của các thực thể ký hình thành nên *chữ ký tập thể* cho một thông điệp dữ liệu. Nói cách khác, chữ ký tập thể trong mô hình này bao hàm chữ ký với tư cách cá nhân của thực thể ký và chữ ký của CA với tư cách của tổ chức mà đối tượng ký là thành viên thuộc tổ chức này. Nói chung, một CA trong mô hình được đề xuất có những chức năng cơ bản như sau:

- *Chứng nhận tính hợp pháp của các thành viên trong một tổ chức*: thực chất là chứng nhận khóa công khai và danh tính (các thông tin nhận dạng) của các thành viên trong tổ chức bằng việc phát hành *Chứng chỉ khóa công khai* (PKC - Public Key Certificate). Ngoài ra, CA còn có trách nhiệm thu hồi PKC hết hạn lưu hành hoặc vi phạm chính sách an toàn của tổ chức.
- *Chứng thực nguồn gốc và tính toàn vẹn của các thông điệp dữ liệu*: được ký bởi các đối tượng là thành viên của tổ chức mà CA là cơ quan chứng thực của tổ chức này.

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:

- *Phát hành, quản lý chứng chỉ khóa công khai*

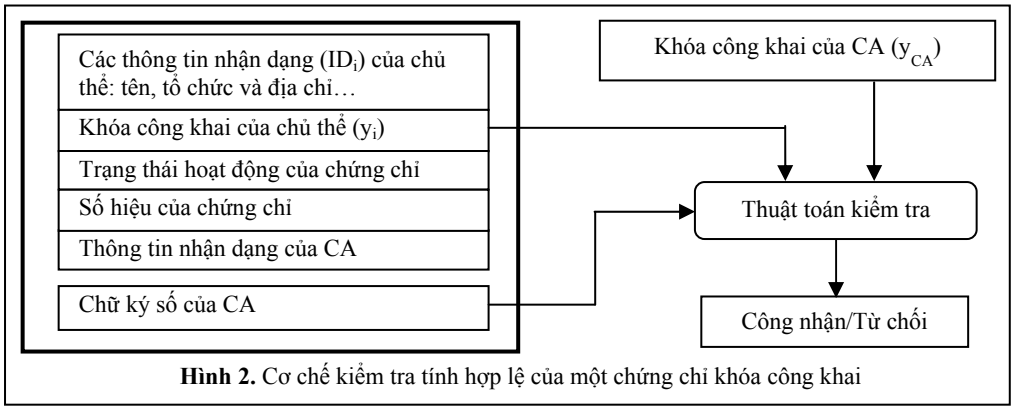
Trong mô hình chữ ký tập thể, chứng chỉ khóa công khai được sử dụng để một tổ chức chứng nhận các đối tượng ký là thành viên của nó. Một chứng chỉ khóa công khai bao gồm những thông tin cơ bản và cơ chế hình thành được chỉ ra trên Hình 1.



Hình 1. Cấu trúc cơ bản và cơ chế hình thành của một chứng chỉ khóa công khai

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 mới đề xuất.

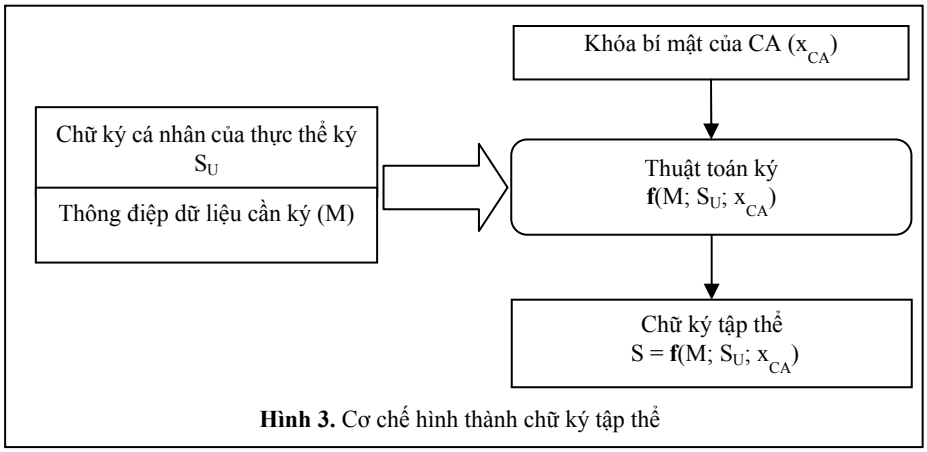
Cơ chế kiểm tra tính hợp lệ của một chứng chỉ khóa công khai được chỉ ra trên Hình 2 như sau:



Hình 2. Cơ chế kiểm tra tính hợp lệ của một chứng chỉ khóa công khai

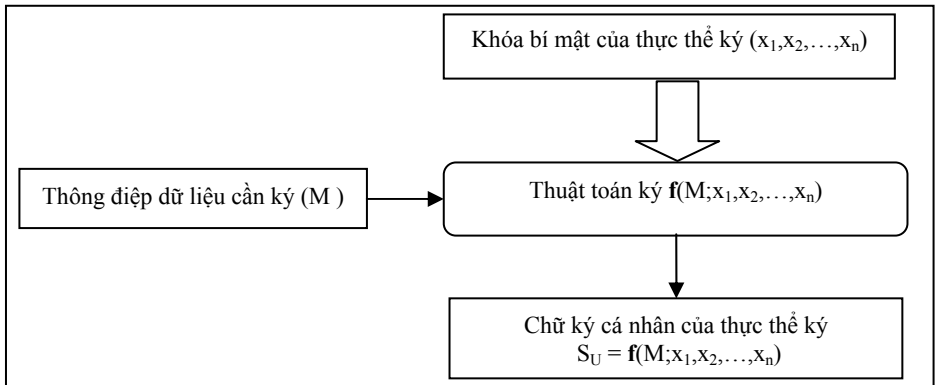
- *Hình thành và kiểm tra chữ ký số tập thể*

Trong mô hình được đề xuất, 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. Cơ chế hình thành chữ ký tập thể được chỉ ra trên Hình 3.



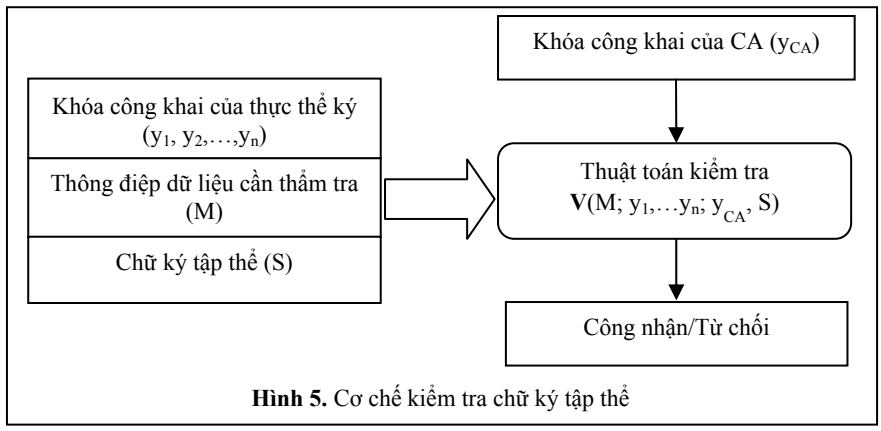
Hình 3. Cơ chế hình thành chữ ký tập thể

Chữ ký cá nhân hình thành từ khóa bí mật của thực thể ký (một hoặc một số đối tượng ký) và thông điệp dữ liệu cần ký theo cơ chế được chỉ ra trên Hình 4 như sau:



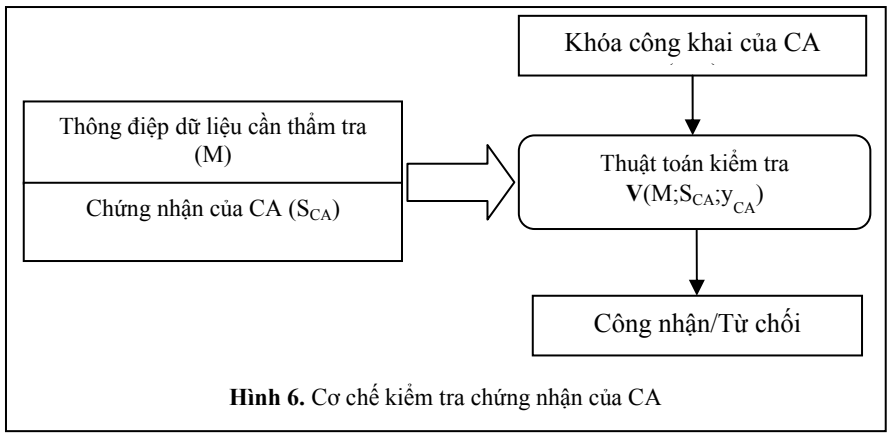
Hình 4. Cơ chế hình thành chữ ký cá nhân

Cơ chế kiểm tra tính hợp lệ của chữ ký tập thể được chỉ ra trên Hình 5 như sau:



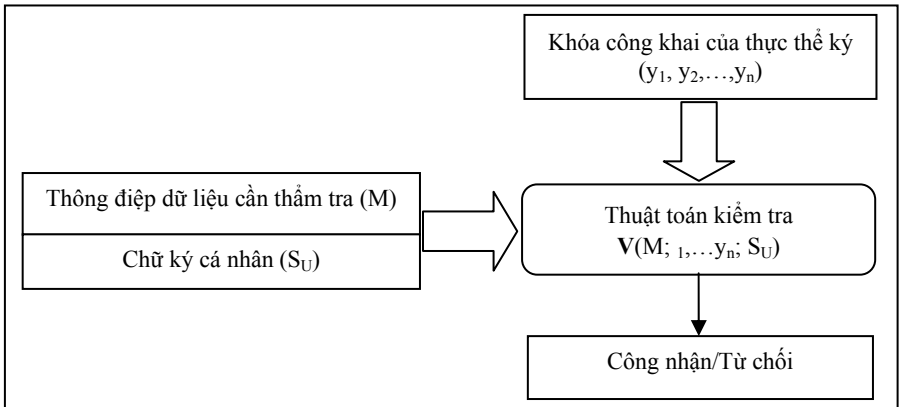
Hình 5. Cơ chế kiểm tra chữ ký tập thể

Cơ chế kiểm tra chứng nhận của CA về việc một hay một nhóm đối tượng ký lên một thông điệp dữ liệu (M) được chỉ ra trên Hình 6, kết quả kiểm tra là cơ sở để khẳng định thông điệp dữ liệu được ký bởi các đối tượng là thành viên của tổ chức và tính toàn vẹn của thông điệp dữ liệu được đảm bảo.



Hình 6. Cơ chế kiểm tra chứng nhận của CA

Cơ chế kiểm tra chữ ký cá nhân được chỉ ra trên Hình 7. 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 nguồn gốc và tính toàn vẹn của thông điệp dữ liệu cần thẩm tra được khẳng định.



Hình 7. Cơ chế kiểm tra tính hợp lệ của chữ ký cá nhân

Ở các lược đồ chữ ký tập thể mới đề xuất, thuật toán kiểm tra chữ ký cá nhân cũng là một bộ phận quan trọng của thuật toán hình thành chữ ký tập thể nhằm chống lại một số dạng tấn công giả mạo từ bên trong hệ thống.

Mục tiếp theo sẽ xây dựng một lược đồ chữ ký phù hợp theo mô hình chữ ký tập thể đã đề xuất.

III. THUẬT TOÁN CHỮ KÝ SỐ TẬP THỂ

1. Lược đồ cơ sở

Lược đồ mới đề xuất ở đây được phát triển dựa trên tính khó của việc giải đồng thời hai bài toán phân tích số [4] và bài toán logarit rời rạc [5] trên $\mathbb{Z}_n$, nhằm nâng cao độ an toàn của thuật toán chữ ký số, đồng thời có thể rút ngắn kích thước của chữ ký do lược đồ này sinh ra. Lược đồ mới đề xuất bao gồm: các thuật toán hình thành tham số và khóa, thuật toán ký và kiểm tra chữ ký như sau:

1.1. Thuật toán hình thành tham số và khóa

Mỗi đối tượng ký trong hệ thống hình thành các tham số và khóa theo các bước như sau:

Thuật toán 1.1: Hình thành tham số và khóa.

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

Output: n, m, g, y, x_1, x_2.

[1]. Chọn 1 cặp số p, q nguyên tố với: *len*(p) = *lp*, *len*(q) = *lq* sao cho bài toán phân tích số trên $\mathbb{Z}_n$ là khó giải.

[2]. Tính: $n = p.\ q$ và: $\varphi(n) = (p - 1).(q - 1)$

[3]. Chọn p_1, q_1 là các số nguyên tố thỏa mãn: $p_1|(p-1)$, $q_1|(q-1)$ và: $p_1 \nmid (q-1)$, $q_1 \nmid (p-1)$

[4]. Tính: $m = p_1.\ q_1$

[5]. Chọn g là phần tử sinh của nhóm $\mathbb{Z}_n^*$ có bậc là m ($\text{ord}_g = m$), được tính theo:

$g = \alpha^{\frac{\varphi(n)}{m}} \bmod n$ và thỏa mãn: $\gcd(g, n) = 1$, với: $\alpha \in (1, n)$

[6]. Chọn khóa bí mật thứ nhất x_1 trong khoảng (1, m)

[7]. Tính khóa công khai theo: $y = (g)^{-x_1} \bmod n$ (1)

Kiểm tra nếu: $y \geq \varphi(n)$ hoặc: $\gcd(y, \varphi(n)) \neq 1$ thì thực hiện lại từ bước [6]

[8]. Tính khóa bí mật thứ hai theo: $x_2 = y^{-1} \bmod \varphi(n)$ (2)

[9]. Chọn hash function H: $\{0,1\}^* \to Z_h$, với: h < n

Chú thích:

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

+ Khóa công khai là y, khóa bí mật là (x_1, x_2).

+ Các tham số công khai là n, g; các tham số bí mật là: p, q, p_1, q_1, m và $\varphi(n)$.

1.2. Thuật toán ký

Thuật toán 1.2: Sinh chữ ký.

Input: n, g, m, x_1, x_2, M - bản tin cần ký.

Output: (E,S) - chữ ký.

[1]. Chọn ngẫu nhiên giá trị k trong khoảng $(1, m)$

[2]. Tính giá trị: $R = g^k \bmod n$

[3]. Tính thành phần thứ nhất của chữ ký theo: $E = H(M \,||\, R)$

[4]. Tính thành phần thứ 2 của chữ ký theo: $S = x_2 \times \left(k + x_1 \times E\right) \bmod m$ (3)

Chú thích: Toán tử "||" là phép nối 2 xâu bit.

1.3. Thuật toán kiểm tra

Thuật toán 1.3: Kiểm tra chữ ký.

Input: n, g, y, M - bản tin cần thẩm tra.

Output: (E,S) = true/false.

[1]. Tính giá trị: $\overline{R} = \left(g^S\right)^y \times \left(y\right)^E \bmod n$

[2]. Tính giá trị: $\overline{E} = H(M \,||\, \overline{R})$

[3]. Nếu: $\overline{E} = E$ thì: (E,S) = *true*, ngược lại: (E,S) = *false*

Chú thích:

+ (E,S) = *true*: chữ ký hợp lệ, bản tin M được xác thực về nguồn gốc và tính toàn vẹn.

+ (E,S) = *false*: chữ ký hoặc/và bản tin bị giả mạo.

1.4. Tính đúng đắn của lược đồ mới đề xuất

Với các tham số và khóa được hình thành bởi thuật toán 1.1, chữ ký (E,S) được sinh bởi thuật toán 1.2, giá trị $\overline{E}$ được tạo bởi thuật toán 1.3 thì điều cần chứng minh ở đây là: $\overline{E} = E$.

Thật vậy, do:

$$\begin{aligned}\overline{R} &= \left(g^S\right)^y \times \left(y\right)^E \bmod n \\ &= \left(g^{x_2.(k+x_1.E)} \bmod n\right)^y + \left(g^{-x_1} \bmod n\right)^E \bmod n \\ &= g^{(k+x_1.E).x_2.y} \times g^{-x_1.E} \bmod n = g^k \bmod n \\ &= R\end{aligned}$$

Suy ra điều cần chứng minh:

$$\overline{E} = H(M \,||\, \overline{R}) = H(M \,||\, R) = E$$

1.5. Mức độ an toàn của lược đồ mới đề xuất

a) Tấn công khóa bí mật

Ở lược đồ mới đề xuất, khóa bí mật của một đối tượng ký là cặp (x_1,x_2), tính an toàn của lược đồ sẽ bị phá vỡ hoàn toàn khi cặp khóa này có thể tính được bởi một hay các đối tượng không mong muốn. Từ thuật toán 1.1 cho thấy, để tìm được x_2 cần phải tính được tham số $\varphi(n)$, nghĩa là phải giải được bài toán phân tích số (IFP), còn để tính được x_1 cần phải giải được logarit rời rạc bài toán (DLP). Như vậy, để tìm được cặp khóa bí mật này kẻ tấn công cần phải giải được đồng thời hai bài toán IFP và DLP.

b) Tấn công giả mạo chữ ký

Từ điều kiện của thuật toán 1.3, một cặp (E,S) bất kỳ sẽ được coi là chữ ký hợp lệ của đối tượng sở hữu các tham số công khai (n, g, y) lên bản tin M nếu thỏa mãn:

$$E = H\left(M \,||\, \left(\left(g^S\right)^y \times \left(y\right)^E \bmod n\right)\right) \quad (4)$$

Từ (4) cho thấy, việc tìm cặp (E, S) bằng cách chọn trước 1 trong 2 giá trị rồi tính giá trị còn lại đều khó hơn việc giải DLP. Hơn nữa, nếu H(.) được chọn là hàm băm có độ an toàn cao (SHA 256/512,...) thì việc chọn ngẫu nhiên cặp (E, S) thỏa mãn (4) hoàn toàn không khả thi trong các ứng dụng thực tế.

2. Lược đồ chữ ký tập thể

Lược đồ chữ ký tập thể ở đây được phát triển từ lược đồ cơ sở được đề xuất ở mục 1 với các chức năng như sau:

- 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 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 chữ ký do một đối tượng ký tạo ra.

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}}.

2.1. Thuật toán hình thành tham số và khóa của CA

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

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

Output: n, m, g, x_{ca}, y_{ca}.

[1]. Chọn 1 cặp số p, q nguyên tố với: *len*(p) = lp, *len*(q)= lq sao cho bài toán phân tích số trên $\mathbb{Z}_{n=p.q}$ là khó giải.

[2]. Tính: n = p. q và: φ(n) = (p - 1).(q - 1)

[3]. Chọn p_1, q_1 là các số nguyên tố thỏa mãn: p_1|(p-1), q_1|(q-1) và: $p_1 \nmid$(q-1), $q_1 \nmid$(p-1)

[4]. Tính: m = p_1. q_1

[5]. Chọn *g* là phần tử sinh của nhóm $\mathbb{Z}_n^*$ có bậc là *m* ($ord_g = m$), được tính theo:

$g = \alpha^{\frac{\varphi(n)}{m}} \bmod n$ và thỏa mãn: $\gcd(g,n)=1$, với: $\alpha \in (1,n)$

[6]. Chọn khóa công khai y_{ca} trong khoảng (1, φ(n)) và gcd (y_{ca} , φ(n)) = 1

[7]. Tính khóa bí mật x_{ca} theo: $x_{ca} = (y_{ca})^{-1} \bmod \varphi(n)$

[8]. Chọn hash function H: $\{0,1\}^* \to Z_h$, với: h < n

2.2. Thuật toán hình thành khóa của các đối tượng ký

Thuật toán 2.2: Hình thành khóa của U = {U_i| i=1,2,.,N}.

Input: n, g, 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]. $y_i \leftarrow g^{-x_i} \bmod n$

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

[2]. return K_P

2.3. Thuật toán hình thành chữ ký

Thuật toán 2.3: Hình thành chữ ký tập thể.

Input: M, n, m, K_S = {x_i| i = 1, 2,..,N}, K_P = {y_i| i = 1, 2,..,N}.

Output: (E,S) - chữ ký của U lên M.

[1]. for i = 1 to N do

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

[1.2]. $r_i \leftarrow g^{k_i} \bmod n$

[1.3]. send r_i to CA

[2]. r ← 1; for i = 1 to N do

$r \leftarrow r \times r_i \bmod n$

[3]. $k_{ca} \leftarrow H(x_{ca} \| M)$, $r_{ca} \leftarrow g^{k_{ca}} \bmod n$

[4]. $r \leftarrow r \times r_{ca} \bmod n$

[5]. $E \leftarrow H(M \| r)$, send E to {U_1, U_2,...., U_i,..., U_N};

[6]. for i = 1 to N do

[6.1]. $S_i \leftarrow (k_i + x_i \times E) \bmod n$

[6.2]. send S_i to CA

[7]. $S_u \leftarrow 0$; for i = 1 to N do

[7.1]. if ($r_i \neq g^{s_i} \times (y_i)^E \bmod n$) then {return (0,0)}

[7.2]. $S_u \leftarrow (S_u + S_i)$

[8]. $S \leftarrow x_{ca} \times (k_{ca} + S_u) \bmod m$

[9]. return (E,S);

Chú thích:

+ Các bước [1], [6] được thực hiện bởi các đối tượng ký.

+ Các bước [2], [3], [4], [5], [7], [8] và [9] được thực hiện bởi CA.

2.4. Thuật toán kiểm tra chữ ký

Thuật toán 2.4: Kiểm tra chữ ký tập thể

Input: g, n, y_{ca}, K_P={y_i| i =1,2,..,N}, M, (E,S).

Output: (E,S) = true / false.

[1]. if (E = 0 or S = 0) then {return *false*}

[2]. y ← 1; for i = 1 to N do

$y \leftarrow y \times y_i \bmod p$

[3]. $v \leftarrow (g^{S \cdot y_{ca}} \times y^E) \bmod n$

[4]. $\overline{E} \leftarrow H(M \| v)$

[5]. if ($\overline{E} = E$) then {return *true*}

else {return *false*}

2.5. Tính đúng đắn của lược đồ chữ ký tập thể

Với các tham số và khóa được hình thành bởi thuật toán 2.1 và 2.2, chữ ký tập thể (E, S) được sinh bởi thuật toán ký 2.3, giá trị $\overline{E}$ được tạo bởi thuật toán kiểm tra 2.4 thì điều cần chứng minh ở đây là $\overline{E} = E$.

Thật vậy, theo các thuật toán 2.1, 2.2 và 2.3 ta có:

$$y = \prod_{i=1}^{N} y_i \bmod n\text{, } r = \left(\prod_{i=1}^{N} r_i \bmod n\right) \bmod n \text{ và: } s = \sum_{i=1}^{N} s_i \bmod m$$

Nên:

$$u = (S)^{y_{ca}} \bmod n = \left(s^{x_{ca}} \bmod n\right)^{y_{ca}} \bmod n$$

$$= s^{x_{ca} \cdot y_{ca}} \bmod n = s = \sum_{i=1}^{N} s_i \bmod m$$

Và:

$$v = \left(g^{S.y_{ca}} \times y^{E}\right) \bmod n == \left(g^{x_2.\left(k_{ca}+\sum_{i=1}^{N}(k_i+x_i.E \bmod m)\right).y_{ca}} \times \left(\prod_{i=1}^{N} y_i \bmod n\right)^{E}\right) \bmod n$$

$$= \left(g^{k_{ca}} \times g^{\sum_{i=1}^{N} k_i} \times g^{E.\sum_{i=1}^{N} x_i} \times g^{-E.\sum_{i=1}^{N} x_i}\right) \bmod n = g^{k_{ca}} \times \left(g^{\sum_{i=1}^{N} k_i}\right) \bmod n = g^{k_{ca}} \times \left(\prod_{i=1}^{N}\left(g^{k_i} \bmod n\right)\right) \bmod n$$

$$= r_{ca} \times \left(\prod_{i=1}^{N} r_i \bmod n\right) \bmod n = r$$

Từ đây suy ra: $\overline{E} = H(M \parallel v) \bmod m = H(M \parallel r) \bmod m = E$

2.6. Tính an toàn của lược đồ chữ ký tập thể

Mức độ an toàn của lược đồ chữ ký tập thể ở đây được thiết lập dựa trên mức độ an toàn của lược đồ cơ sở đã đề xuất ở mục 1. Do vậy, về cơ bản mức độ an toàn của nó cũng được quyết định bởi mức độ khó của bài toán IFP và DLP tương tự như lược đồ đã đề xuất. Điều cần chú ý là ở lược đồ chữ ký tập thể còn tiềm ẩn nguy cơ tấn công giả mạo chữ ký của các thành viên nhóm ký trong quá trình hình thành chữ ký tập thể. Do vậy, việc CA kiểm tra tính xác thực của các thành viên nhóm ký ở bước [7.1] trong thuật toán 2.3 là rất cần thiết.

IV. KẾT LUẬN

Bài báo đề xuất một mô hình ứng dụng chữ ký số được gọi là *mô hình chữ ký số tập thể* 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. 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 hai cấp độ khác nhau: thực thể tạo ra thông điệp dữ liệu cần chứng thực và tổ chức mà thực thể tạo ra nó là một thành viên hay bộ phận của tổ chức này. Bài báo cũng đề xuất xây dựng lược đồ chữ ký số theo mô hình ứng dụng mới. Lược đồ mới đề xuất ở đây được phát triển từ một *dạng lược đồ chữ ký số* xây dựng dựa trên tính khó của việc giải đồng thời hai bài toán phân tích số và logarit rời rạc trên vành Z_n. Tính đúng đắn và mức độ an toàn của lược đồ mới đề xuất đã được chứng minh cho thấy khả năng ứng dụng của nó trong thực tế.

V. TÀI LIỆU THAM KHẢO

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

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

[3] Fegghi, J. (1999), Digital Certificates and Applied Internet Security, Addison-Wesley Longman Inc.

[4] Rivest R., Shamir A., Adleman L. (1978), "A Method for Obtaining Digital Signatures and Public Key Cryptosystems", Communications of the ACM, Vol. 21, No. 2, pp. 120-126.

[5] ElGamal T. (1985), "A public key cryptosystem and a signature scheme based on discrete logarithms", IEEE Transactions on Information Theory, Vol. IT-31, No. 4, pp. 469-472.

DIGITAL SIGNATURE - MODEL AND ALGORITHM

Pham Van Hiep, Luu Hong Dung

ABSTRACT: *This paper proposes a suitable digital signature application model for government agencies, administrative units, enterprises, etc., where data messages need to be authenticated. Origin and integrity at two levels: entity sign and organization (agency, unit, ...) that the entity signing is its member. At the same time, the paper also suggests digital signature schemes based on this application model. The proposed new scheme was developed from a digital signature scheme formulated based on the difficulty of simultaneous solving integer factorization and discrete logarithm problem.*

Keywords: *Digital signature; Collective signature; Digital signature schemes; Digital signature algorithm.*