VẤN ĐỀ VÀ SỰ KIỆN

PHÁT TRIỂN THUẬT TOÁN CHỮ KÝ SỐ TẬP THỂ ĐẢM BẢO AN TOÀN VÀ BẢO MẬT HỆ THỐNG THÔNG TIN CHO SINH VIÊN ĐẠI HỌC

NGUYỄN THANH HUYỀN
Trường Đại học Lao động - Xã hội

Ngày nhận bài: 10/05/2021; Ngày phản biện, biên tập và sửa chữa: 28/05/2021; Ngày duyệt đăng: 04/06/2021

ABSTRACT

According to the application model, the article proposes a collective digital signature scheme to ensure the authentication requirements of origin and integrity for data messages at two different levels: the entity that created it and the organization of the entity that made it a member division of this organization. The scheme is built based on the difficulty of simultaneously solving two discrete logarithmic and numerical analysis problems on Zn to improve the algorithm's safety and performance.

Key words: *Digital signature scheme, digital signature algorithm, digital signatures, Collective digital signature.*

I. ĐẶT VẤN ĐỀ

Hiện tại, các mô hình ứng dụng chữ ký số đáp ứng tốt 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, đối với các yêu cầu 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 (các tổ chức có tư cách pháp nhân trong xã hội) mà thực thể tạo ra thông tin là một thành viên hay bộ phận của nó thì các mô hình/thuật toán này - bao gồm các mô hình hiện tại với các thuật toán chữ ký đơn RSA [1], DSA [2], GOST R34.10-94 [3], ... hay các mô hình với các thuật toán chữ ký bội (digital multisignature scheme), chữ ký nhóm (group signature schemes) [4-8] đều không thể đáp ứng yêu cầu đặt ra. 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 thủ tục hành chính trong thực tế xã hội.

Trong bài báo này, tác giả đề xuất một lược đồ chữ ký xây dựng theo mô hình cho phép bảo đảm các yêu cầu chứng thực về nguồn gốc và tính toàn vẹn cho các thông điệp dữ liệu trong giao dịch điện tử, mà ở đó các thực thể ký là thành viên hay bộ phận của tổ chức có tư cách pháp nhân trong xã hội. Trong mô hình/thuật toán 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.

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

1. Mô hình chữ ký số tập thể

Mô hình chữ ký số tập thể được đề xuất ở đây cơ bản dựa trên cấu trúc của một PKI (Public Key Infrastructure) truyền thống 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 [9], 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 đó, CA (Certificate Authority) là bộ phận có chức năng bảo đảm các dịch vụ chứng thực số. 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 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.

- Chứng thực nguồn gốc và tính toàn vẹn của các 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:

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

Trong mô hình chữ ký tập thể, chứng chỉ khóa công khai (PKC) 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.

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

Trong mô hình được đề xuất, chữ ký tập thể hình thành trên cơ sở *chữ ký của 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.

Mục tiếp theo sẽ đề xuất một lược đồ chữ ký phù hợp theo mô hình chữ ký tập thể trên đây.

2. Xây dựng thuật toán theo mô hình chữ ký số tập thể

Việc xây dựng thuật toán theo mô hình chữ ký tập thể được thực hiện qua 2 bước: xây dựng lược đồ chữ ký cơ sở [10] và xây dựng lược đồ chữ ký tập thể.

2.1. Lược đồ cơ sở

Lược đồ cơ sở đề xuất ở đây được xây dựng dựa trên tính khó của việc giải đồng thời hai bài toán phân tích số (IFP) và bài toán logarit rời rạc (DLP) trên Z_n nhằm nâng cao độ an toàn của thuật toán, đây là các bài toán khó được sử dụng làm cơ sở xây dựng hệ mật RSA.

Lược đồ cơ sở bao gồm các thuật toán hình thành tham số và khóa, thuật toán ký và kiểm tra chữ ký như sau:

2.1.1. Thuật toán hình thành tham số và khóa

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 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, trong đó: p_1 là ước của (p-1) và không là ước của (q-1), còn q_1 là ước của (q-1) và không là ước của (p-1).

[4]. Tính: $m = p_1.\ q_1$

[5]. Chọn g là phần tử sinh của nhóm Z_n^*, 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: $y \geq \phi(n)$ hoặc: $\gcd(y, \phi(n)) \neq 1$ thì thực hiện lại từ bước [6]

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

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

2.1.2. 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 các 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:

$S = x_2 \times (k + x_1 \times E) \bmod m$.

2.1.3. 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: $\overline{R} = (g^S)^y \times (y)^E \bmod n$

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

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

2.1.4. Tính đúng đắn của lược đồ cơ sở

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: $\overline{E} = E$.

Bổ đề:

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

$$= g^{(k + x_1 E) x_2 - x_1 E} \bmod n = g^k \bmod n = R$$

Suy ra điều cần chứng minh: $\overline{E} = H(M \| \overline{R}) = H(M \| R) = E$

2.1.5. Mức độ an toàn của lược đồ cơ sở

- 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 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 IFP, còn để tính được x_1 cần phải giải được DLP. Như vậy, để tìm được cặp khóa bí mật này kẻ tấn công cần phải giải được đồng thời 2 bài toán IFP và DLP. Ngoài ra, tham số *m* cũng được sử dụng với vai trò khóa bí mật trong thuật toán ký. Như vậy, để phá vỡ tính an toàn của thuật toán, kẻ tấn công còn phải giải được bài toán tìm bậc của *g*.

- Tấn công giả mạo chữ ký

Mệnh đề 4: 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:

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

Từ (4) cho thấy, nếu H(.) được chọn là hàm băm có độ an toàn cao (SHA 256/512,...) thì việc tạo ngẫu nhiên được cặp (E,S) thỏa mãn (4) là không khả thi trong các ứng dụng thực tế.

2.2. 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 2.1 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:{xca, yca}.

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

Mệnh đề 1: Chọn một cặp số p, q nguyên tố với: *len*(p) = lp, *len*(q)= lq, n = p. q và: φ(n) = (p - 1).(q - 1). Chọn p_1, q_1 là các số nguyên tố, trong đó: p_1 là ước của (p-1) và không là ước của (q-1), còn q_1 là ước của (q-1) và không là ước của (p-1) khi đó m = p_1. q_1 , $g = \alpha^{\frac{\varphi(n)}{m}} \bmod n$, chọn khóa bí mật thứ nhất x_{ca1} trong khoảng $(1, m)$ khi đó khóa công khai y_{ca}: $y = (g)^{-x_{ca1}} \bmod n$. Khóa bí mật x_{ca2} được tính: $x_{ca} = (y_{ca})^{-1} \bmod \phi(n)$.

Mệnh đề 2:

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

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 một cặp số p, q nguyên tố với: *len*(p) = lp, *len*(q)= lq sao cho bài toán phân tích số trên 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, trong đó: p_1 là ước của (p-1) và không là ước của (q-1), còn q_1 là ước của (q-1) và không là ước của (p-1).

[4]. Tính: m = p_1. q_1

[5]. Chọn g là phần tử sinh của nhóm Z_n^*, được tính theo:

$g = \alpha^{\frac{\varphi(n)}{m}} \bmod n$ và thỏa mãn:

$\gcd(g,n) = 1$, với: $\alpha \in (1,n)$.

[6]. CA chọn khóa bí mật thứ nhất x_{ca1} trong khoảng $(1, m)$

[7]. CA tính khóa công khai y_{ca} theo:

$$y = (g)^{-x_{ca1}} \bmod n.$$

Kiểm tra nếu: $y_{ca} \geq \phi(n)$ hoặc: $\gcd(y_{ca}, \phi(n)) \neq 1$ thì thực hiện lại từ bước [6].

[8]. Tính khóa bí mật x_{ca2} theo: $x_{ca} = (y_{ca})^{-1} \bmod \phi(n)$.

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

2.2.2. 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

2.2.3. Thuật toán chứng thực các đối tượng ký U_i

Thuật toán này được sử dụng để hình thành chứng nhận (chứng chỉ số) của CA cho các đối tượng ký U_i (i=1,2,..,N)

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

Input: $ID_i, y_i, x_{ca1}, x_{ca2}$..

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

[1]. $k_i \leftarrow H(x_{ca1} \| y_i \| x_{ca2} \| ID_i)$

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

[3]. $u_i \leftarrow H(y_i \| ID_i \| r_i)$

[4]. $v_i \leftarrow x_{ca2} \times (k_i + x_{ca1} \times u_i) \bmod m$

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

2.2.4. 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: $ID_i, y_i, y_{ca}, , (u_i, v_i)$.

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

[1]. $\overline{r_i} \leftarrow (g^{v_i})^{y_{ca}} \times (y_{ca})^{u_i} \bmod n.$

[2]. $\overline{u_i} \leftarrow H(\overline{r_i} \| y_i \| ID_i)$.

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

2.2.5. Thuật toán ký tập thể

Thuật toán 2.5: 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]. $r \leftarrow 1$; for i = 1 to N do $r \leftarrow r \times r_i \bmod n$.

[3]. $k_{ca} \leftarrow H(x_{ca1} \| M)$, $r_{ca} \leftarrow g^{k_{ca}} \bmod n$

[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]. $S \leftarrow x_{ca2} \times (k_{ca} + S_u) \bmod m$

[9]. return (E,S);

2.2.6. Thuật toán kiểm tra chữ ký tập thể

Thuật toán 2.6: Kiểm tra chữ ký tập thể

Input: *g, n,* y_{ca}, K_P = {y_i| i =1,2,..,N}, *M*.

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

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

[2]. y ← 1; for i = 1 to N do $y \leftarrow y \times y_i \bmod n$

[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*}

2.2.7. 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 2.2.1. Do vậy, về cơ bản mức độ an toàn của lược đồ chữ ký tập thể cũng được quyết định bởi mức độ khó của việc giải đồng thời hai bài toán IFP và DLP..

III. KẾT LUẬN

Việc áp dụng chữ ký số phù hợp với hoạt động thực tế tại các cơ quan, đơn vị, doanh nghiệp,… hiện nay là rất cần thiết. Các mô hình đang được triển khai vẫn chưa đáp ứng được việc chứng thực về nguồn gốc và tính toàn vẹn của thông tin ở cấp độ tổ chức mà thực thể ký là một thành viên hay bộ phận của tổ chức đó. Bài báo đã đề xuất một thuật toán phù hợp với mô hình ứng dụng chữ ký số giải quyết được vấn đề đã nêu trên và đề xuất phát triển một lược đồ kỹ thuật số tập thể dựa trên mô hình ứng dụng mới nhằm đảm bảo các yêu cầu xác thực về nguồn gốc và tính toàn vẹn của thông điệp dữ liệu trong các giao dịch điện. Trong mô hình này, thông điệp điện tử sẽ được xác thực ở hai cấp độ khác nhau: thực thể tạo ra nó và tổ chức tạo ra nó là thành viên hoặc một phần của tổ chức. Lược đồ dựa trên độ khó của việc giải hai logarit số và rời rạc đồng thời trên Zn để cải thiện tính bảo mật của thuật toán và đảm bảo tính đúng đắn của lược đồ

TÀI LIỆU THAM KHẢO

1. R.L. Rivest, A. Shamir, L. Adleman (1078), *A method for obtaining digital signatures and public-key cryptosystems*, Communications of the ACM, No 21, pp. 120-126.

2. National Institute of Standards and Technology (2013), NIST FIPS PUB 186-4. *Digital Signature Standard*, U.S. Department of Commerce.

3. GOST R34.10-94 (1994), 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, in Russian.

4.S. J. Hwang, M. S. Hwang, S. F. Tzeng (2003), *"A new digital multisignature scheme with distinguished signing authorities"*, Journal of Information Science and Engineering, No 19, pp. 881-887.