LƯỢC ĐỒ CHỮ KÝ SỐ MÙ XÂY DỰNG TRÊN BÀI TOÁN KHAI CĂN

THE BLIND SIGNATURE BASED ON FINDING ROOT PROBLEM

Nguyễn Tiền Giang[*], *Nguyễn Vĩnh Thái*[**], *Lưu Hồng Dũng* [***]

Bài báo đề xuất một lược đồ chữ ký số mù phát triển từ một dạng lược đồ chữ ký số được xây dựng dựa trên tính khó của bài toán khai căn trên vành $Z_{n=p.q}$, ở đây p, q là các số nguyên tố phân biệt. Lược đồ chữ ký mới đề xuất có mức độ an toàn cao hơn so với các lược đồ đã được công bố trước đó về khả năng giữ bí mật nguồn gốc bản tin được ký.

1. Đặt vấn đề

Khái niệm chữ ký số mù lần đầu được đề xuất bởi D. Chaum vào năm 1983 [1], đây là một loại chữ ký số được sử dụng để xác thực tính toàn vẹn của một bản tin điện tử và danh tính của người ký, nhưng không cho phép xác thực nguồn gốc thực sự của bản tin được ký. Với các loại chữ ký số thông thường thì người ký cũng chính là người tạo ra bản tin được ký, còn ở đây người ký và người tạo ra bản tin được ký là 2 đối tượng hoàn toàn khác nhau. Che giấu nguồn gốc của bản tin được ký thực chất là che dấu danh tính của người đã tạo ra bản tin đó, đây là tính chất đặc trưng của chữ ký số mù và cũng là một tiêu chí quan trọng để đánh giá mức độ an toàn của loại chữ ký số này.

Trong [1-5] các tác giả đã đề xuất một số lược đồ chữ ký số mù ứng dụng khi cần bảo vệ tính riêng tư của các khách hàng trong các hệ thống thanh toán điện tử hay vấn đề ẩn danh của cử tri trong việc tổ chức bầu cử trực tuyến. Tuy nhiên, điểm yếu chung của các lược đồ trên là không có khả năng chống lại kiểu tấn công làm lộ nguồn gốc của bản tin được ký, vì thế khả năng ứng dụng của các lược đồ này trong thực tế là rất hạn chế.

Trên cơ sở phân tích điểm yếu có thể tấn công của các lược đồ đã biết, bài báo đề xuất việc phát triển lược đồ chữ ký số mù từ một dạng lược đồ chữ ký số mới [10] được xây dựng dựa trên tính khó của bài toán khai căn trên vành $Z_{n=p.q}$, với p, q là các số nguyên tố lớn. Ưu điểm của lược đồ chữ ký số mù này là khả năng chống lại kiểu tấn công làm lộ nguồn gốc bản tin được ký so với các lược đồ chữ ký số mù đã được biết đến trước đó.

2. Tấn công làm lộ nguồn gốc bản tin đối với một số lược đồ chữ ký số mù

2.1. Tấn công lược đồ chữ ký số mù RSA

[*] Cục CNTT – Bộ QP.
[**] Viện CNTT – Viện KH & CNQS.
[***] Học viện KTQS.

2.1.1. Lược đồ chữ ký số mù RSA

Lược đồ chữ ký số mù RSA do D. Chaum đề xuất phát triển từ lược đồ chữ ký số RSA [6]. Lược đồ chữ ký số mù RSA có thể mô tả như sau: Giả sử A là người có thẩm quyền ký (người ký), cặp khóa bí mật và công khai (*d*,*e*) của A cùng với *modulo n* được hình thành theo lược đồ chữ ký RSA. B là người tạo ra bản tin M và yêu cầu A ký lên M (người yêu cầu ký). Để che dấu danh tính của B sau khi bản tin M đã được ký, thủ tục hình thành chữ ký ("ký mù") được thực hiện qua các bước như sau:

Bước 1: B làm "mù" bản tin M bằng cách chọn ngẫu nhiên một giá trị k thỏa mãn: $1 < k < n$ và k nguyên tố cùng nhau với n ($gcd(k,n) = 1$), sau đó B tính: $m' = m \times k^e \bmod n$, ở đây: $m = H(M)$ là giá trị đại diện của bản tin cần ký M và $H(.)$ là hàm băm kháng va chạm. B gửi bản tin đã được làm mù (m') cho A.

Bước 2: A sẽ ký lên m' bằng thuật toán ký của lược đồ RSA: $s' = (m')^d \bmod n$ rồi gửi lại s' cho B.

Bước 3: B "xóa mù" s' và nhận được chữ ký s như sau: $s = s' \times k^{-1} \bmod n$.

Việc kiểm tra tính hợp lệ của s và do đó là tính toàn vẹn của M được thực hiện như ở lược đồ RSA. Vấn đề cần giải quyết ở đây là, một đối tượng bất kỳ có thể khẳng định tính toàn vẹn của M và s là chữ ký của A, nhưng không ai có thể biết được bản tin M là do B hay một đối tượng nào khác tạo ra và yêu cầu A ký đó.

2.1.2. Tấn công làm lộ nguồn gốc bản tin được ký

Với lược đồ chữ ký số mù RSA như đã mô tả ở trên, việc xác định danh tính của người tạo ra bản tin được ký M là hoàn toàn có thể thực hiện được. Bởi vì tại thời điểm ký, người ký (A) chỉ không biết nội dung của bản tin được ký (M), còn danh tính của người yêu cầu ký (B) thì A hoàn toàn biết rõ. Giả sử có N người đã yêu cầu A ký lên các bản tin do họ tạo ra và $\{ID_{Bi} | i=1,2,\ldots N\}$ là danh tính tương ứng với những người đó, nói cách khác B ở đây là 1 tập N người: $B = \{B_i | i=1,2,\ldots N\}$ mà: $ID_B = \{ID_{Bi} | i=1,2,\ldots N\}$ là tập danh tính tương ứng của họ. Để xác định danh tính của 1 người yêu cầu ký từ bản tin M và chữ ký s tương ứng, với mỗi lần ký vào một bản tin, người ký A cần lưu trữ giá trị s_i' cùng danh tính của người yêu cầu ký ID_{Bi} trong một cơ sở dữ liệu. Có thể xác định danh tính của người yêu cầu ký (ID_{Bi}) từ một bản tin được ký M và chữ ký s tương ứng với nó (M) bằng thuật toán như sau:

Thuật toán 1.1:

Input: (M,s), $\{(s_i', ID_{Bi}) | i=1,2,\ldots N\}$.
Output: ID_B.

[1]. $m \leftarrow H(M)$, i = 0
[2]. **select**: (s_i', ID_{Bi})
[3]. $k^* \leftarrow s_i' \times m^{-d} \bmod n$
[4]. **if** $\gcd(k^*, n) \neq 1$ **then**
  [4.1]. $i \leftarrow i + 1$
  [4.2]. **goto** [2]
[5]. $s^* \leftarrow s_i' \times (k^*)^{-1} \bmod n$
[6]. **if** $(s^* \neq s)$ **then**

[6.1]. $i \leftarrow i+1$
[6.2]. **goto** [2]
[7]. **return** ID_{Bi}

Nhận xét: Từ Thuật toán 1.1 cho thấy, nếu N – số bản tin đã được A ký không đủ lớn thì việc xác định được danh tính của B (người yêu cầu ký/người tạo ra bản tin được ký) là hoàn toàn có thể thực hiện được. Nói cách khác, lược đồ chữ ký số mù RSA là không an toàn xét theo khả năng che giấu nguồn gốc của bản tin được ký, nếu số lượng bản tin được ký không đủ lớn.

2.2. Tấn công lược đồ chữ ký số mù DSA

2.2.1. Lược đồ chữ ký số DSA cải tiến

Lược đồ chữ ký số DSA cải tiến [7] có tham số hệ thống bao gồm một số nguyên tố p, một số nguyên tố q là ước của (p-1) và phần tử sinh $g \in Z_p^*$ có bậc là q. Người ký có khóa bí mật $x \in Z_q$ và khóa công khai tương ứng là $y = g^x \bmod p$. Để ký lên bản tin M có giá trị đại diện $m \in Z_q$ ($m = H(M)$, với H(.) là hàm băm), người ký chọn ngẫu nhiên một giá trị $k \in Z_q$ và tính:

$$R = g^k \bmod p$$
$$r = R \bmod q$$
$$s = (k \times m + x \times r) \bmod q$$

Chữ ký lên bản tin M ở đây là cặp (r,s).

Kiểm tra tính hợp lệ của chữ ký (r,s) với bản tin cần tính:

$$T = \left(g^s \times y^{-r}\right)^{m^{-1}} \bmod p$$

Ở đây m là giá trị đại diện của bản tin cần thẩm tra M.

Chữ ký được coi là hợp lệ nếu thỏa mãn:

$$r = T \bmod q$$

2.2.2. Lược đồ chữ ký số mù DSA

Từ lược đồ chữ ký số DSA cải tiến, nhóm tác giả Jan L. Camenisch, Jean-Marc Piveteau, Markus A. Stadler [9] đề xuất một lược đồ chữ ký số mù với thủ tục hình thành chữ ký bao gồm các bước như sau:

1. a) Người ký (A) chọn một giá trị $k \in Z_q$ và tính $R' = g^k \bmod p$
   b) A kiểm tra nếu $\gcd(R', q) \neq 1$ thì thực hiện lại bước a). Ngược lại, A gửi R cho người yêu cầu ký (B).
2. a) Người yêu cầu ký B chọn 2 giá trị $\alpha, \beta \in Z_q$ và tính $R = (R')^\alpha \times g^\beta \bmod p$.
   b) B kiểm tra nếu $\gcd(R', q) = 1$ thì tính tiếp giá trị $m' = \alpha \times m \times R' \times R^{-1} \bmod q$ rồi gửi m' cho A. Nếu điều kiện chỉ ra không thỏa mãn, B thực hiện lại bước a).
3. Người ký A tính giá trị $s' = (k \times m' + x \times R') \bmod q$ rồi gửi cho B.
4. Người yêu cầu ký B tính các thành phần (r,s) của chữ ký: $r = R \bmod q$, $s = (s' \times R \times (R')^{-1} + \beta \times m) \bmod q$.

Thủ tục kiểm tra tính hợp lệ của chữ ký hoàn toàn tương tự như ở lược đồ chữ ký DSA cải tiến.

2.2.3. Tấn công làm lộ nguồn gốc bản tin được ký

Để tấn công làm lộ nguồn gốc bản tin được ký M, người ký A cần lưu trữ giá trị các tham số $\{R_i', m_i', s_i'\}$ và ID_{Bi} ở mỗi lần ký. A có thể xác định được danh tính của B bằng thuật toán như sau:

Thuật toán 1.2:

Input: (M,r,s), $\{(R_i', m_i', s_i', ID_{Bi}) | i=1,2,\ldots N\}$.

Output: ID_B.

[1]. $m \leftarrow H(M)$, i = 0

[2]. **select**: $(R_i', m_i', s_i', ID_{Bi})$

[3]. $\alpha \leftarrow m_i' \times m \times r \times (R')^{-1} \bmod q$

[4]. $\beta \leftarrow m^{-1} \times (s - s_i' \times r \times (R')^{-1}) \bmod q$

[5]. $R \leftarrow (R_i')^{\alpha} \times g^{\beta} \bmod p$

[6]. $r^* \leftarrow R \bmod q$

[7]. **if** $(r^* \neq r)$ **then**

[7.1]. $i \leftarrow i + 1$

[7.2]. **goto** [2]

[8]. **return** ID_{Bi}

Nhận xét: Từ Thuật toán 1.2 cho thấy, nếu N không đủ lớn thì việc xác định được danh tính của người yêu cầu ký (người tạo ra bản tin được ký) là hoàn toàn có thể thực hiện được. Nói cách khác, lược đồ chữ ký số mù DSA là không an toàn nếu số lượng bản tin được ký không đủ lớn.

2.3. Tấn công lược đồ chữ ký số mù Nyberg-Rueppel

2.3.1. Lược đồ chữ ký số Nyberg-Rueppel

Tham số hệ thống của lược đồ chữ ký số do K. Nyberg và R. A. Rueppel đề xuất [8] được lựa chọn tương tự như ở lược đồ DSA cải tiến. Để ký lên một bản tin M có giá trị đại diện $m \in Z_p$, người ký chọn ngẫu nhiên một giá trị $k \in Z_q$ và tính:

$$r = m \times g^k \bmod p$$
$$s = k + x.r \bmod q$$

Chữ ký lên bản tin M ở đây là cặp (r,s). Chữ ký được coi là hợp lệ nếu thỏa mãn phương trình kiểm tra:

$$m = y^{-s} \times g^r \times r \bmod p$$

Ở đây m là giá trị đại diện của bản tin cần thẩm tra M.

2.3.2. Lược đồ chữ ký số mù Nyberg-Rueppel

Trên cơ sở lược đồ chữ ký Nyberg-Rueppel, cũng nhóm tác giả Jan L. Camenisch, Jean-Marc Piveteau, Markus A. Stadler [9] đã đề xuất một lược đồ chữ ký số mù với thủ tục hình thành chữ ký bao gồm các bước như sau:

1. Người ký (A) chọn một giá trị $k \in Z_q$ và tính $r' = g^k \bmod p$ rồi gửi cho người yêu cầu ký (B).

2. a) B chọn ngẫu nhiên giá trị $\alpha \in Z_q$, $\beta \in Z_q^*$ và tính $r = m \times g^{\alpha} \times (r')^{\beta} \bmod p$, $m' = r \times \beta^{-1} \bmod q$.

b) B kiểm tra nếu $m' \in Z_q^*$ thì gửi m' cho người ký A. Ngược lại, B thực hiện lại bước a).

3. A tính giá trị $s' = (k + x \times m') \bmod q$ rồi gửi cho B.

4. B tính $s = (s' \times \beta + \alpha) \bmod q$

Chữ ký của A lên M là cặp (r,s).

Thủ tục kiểm tra tính hợp lệ của chữ ký hoàn toàn tương tự như ở lược đồ chữ ký Nyberg-Rueppel. Nghĩa là: chữ ký (r,s) được coi là hợp lệ nếu thỏa mãn phương trình kiểm tra:

$m = y^{-s} \times g^{r} \times r \bmod p$

Ở đây m là giá trị đại diện của bản tin cần thẩm tra M.

2.3.3. Tấn công làm lộ nguồn gốc bản tin được ký

Đối với lược đồ chữ ký mù Nyberg-Rueppel, có thể tấn công làm lộ nguồn gốc bản tin được ký M nếu người ký A lưu trữ giá trị các tham số $\{r_i', m_i', s_i'\}$ và ID_{Bi} ở mỗi lần ký. Khi đó, A có thể xác định được danh tính của B bằng thuật toán như sau:

Thuật toán 1.3:

Input: (M,r,s), $\{(r_i', m_i', s_i', ID_{Bi}) | i=1,2,\ldots N\}$.

Output: ID_{Bi}.

[1]. $m \leftarrow H(M)$, i = 0

[2]. **select**: $(r_i', m_i', s_i', ID_{Bi})$

[3]. $\beta \leftarrow r \times (m_i')^{-1} \bmod q$

[4]. $\alpha \leftarrow (s - s_i' \times \beta) \bmod q$

[5]. $r^* = m \times g^{\alpha} \times (r_i')^{\beta} \bmod p$

[6]. **if** $(r^* \neq r)$ **then**

[6.1]. $i \leftarrow i + 1$

[6.2]. **goto** [2]

[7]. **return** ID_{Bi}

Nhận xét: Thuật toán 1.3 cho thấy, lược đồ chữ ký số mù Nyberg-Rueppel là không an toàn xét theo khả năng chống tấn công làm lộ nguồn gốc bản tin, nếu số lượng bản tin được ký không đủ lớn.

3. Xây dựng lược đồ chữ ký số mù

Phân tích các lược đồ chữ ký số mù trên đây cho thấy việc làm "mù" bản tin với một tham số bí mật như ở lược đồ chữ ký số mù RSA, hay với 2 tham số như ở các lược đồ mù DSA và Nyberg-Rueppal thì người ký vẫn có thể tìm được nguồn gốc thực sự của bản tin được ký, nói cách khác là các lược đồ này không có khả năng che giấu danh tính của người tạo ra bản tin được ký. Mục này đề xuất việc phát triển lược đồ chữ ký số mù từ một lược đồ chữ ký cơ sở được xây dựng dựa trên tính khó của bài toán khai căn trên vành $Z_{n=p.q}$, với p, q là các số nguyên tố lớn. Ưu điểm của lược đồ mới này là cũng chỉ sử dụng 2 tham số bí mật như ở các lược đồ mù DSA và Nyberg-Rueppal nhưng không

cho phép người ký hay bất kỳ một đối tượng nào khác có thể xác định được nguồn gốc thực sự của bản tin được ký.

3.1. Xây dựng lược đồ chữ ký cơ sở

3.1.1. Bài toán khai căn trên vành Z_n

Cho cặp các số nguyên dương $\{n,t\}$ với n là tích của hai số nguyên tố p và q, còn t được chọn trong khoảng: $1 < t < (p-1).(q-1)$. Khi này bài toán khai căn trên vành $Z_{n=p.q}$ hay còn gọi là bài toán $RSA_{(n,t)}$ được phát biểu như sau:

Bài toán $RSA_{(n,t)}$: *Với mỗi số nguyên dương $y \in \mathbb{Z}_n^*$, hãy tìm x thỏa mãn phương trình sau:*

$$x^t \bmod n = y \tag{1.1}$$

Giải thuật cho bài toán $RSA_{(n,t)}$ có thể được viết như một thuật toán tính hàm $RSA_{(n,t)}(.)$ với biến đầu vào là y còn giá trị hàm là nghiệm x của phương trình (1.1):

$$x = RSA_{(n,t)}(y) \tag{1.2}$$

Dạng lược đồ chữ ký mới đề xuất cho phép các thực thể ký trong cùng một hệ thống có thể dùng chung bộ tham số $\{n,t\}$, ở đây mỗi thành viên U của hệ thống tự chọn cho mình khóa bí mật x thỏa mãn: $1 < x < n$, tính và công khai tham số:

$$y = x^t \bmod n$$

Chú ý:

(i) Mặc dù bài toán $RSA_{(n,t)}$ là khó, tuy nhiên không phải với mọi $y \in \mathbb{Z}_n^*$ thì việc tính $RSA_{(n,t)}(y)$ đều khó, chẳng hạn những $y = x^t \bmod n$ với x không đủ lớn thì bằng cách duyệt dần $x = 1, 2, ...$ cho đến khi tìm được nghiệm của (1.2) ta sẽ tìm được khóa bí mật x, do đó các tham số mật x phải được lựa chọn sao cho việc tính $RSA_{(n,t)}(y)$ đều khó.

(ii) Với lựa chọn x nêu trên thì rõ ràng không có ai ngoài U biết được giá trị x, vì vậy việc biết được x đủ để xác thực đó là U.

3.1.2. Xây dựng lược đồ chữ ký cơ sở dựa trên bài toán khai căn

Lược đồ chữ ký cơ sở đề xuất ở đây, ký hiệu LD-01, được xây dựng dựa trên tính khó của bài toán $RSA_{(n,t)}$ và được sử dụng để phát triển lược đồ chữ ký số mù trong phần tiếp theo. Tính đúng đắn và mức độ an toàn của lược đồ cơ sở LD-01 được chỉ ra trong [10].

a) Thuật toán hình thành tham số và khóa

Thuật toán 2.1:

Input: p, q, x.

Output: n, t, y, H(.).

[1]. $n \leftarrow p \times q$;

[2]. **select** $H : \{0,1\}^* \mapsto Z_m$, $m < n$;

[3]. $t \leftarrow \left\lfloor \frac{m}{2} \right\rfloor + 1$;

[4]. $y \leftarrow (x)^{-t} \bmod n$; (1.3)

[5]. **return** {n,t,y,H(.)}

b) Thuật toán ký

Thuật toán 2.2:

Input: n, t, x, k, M.
Output: (e,s).

[1]. $r \leftarrow k^t \bmod n$; (1.4)
[2]. $e \leftarrow H(r \| M)$; (1.5)
[3]. $s \leftarrow k \times x^e \bmod n$; (1.6)
[4]. **return** (e,s)

Chú thích:
- Toán tử "||" là phép nối 2 xâu bit/ký tự.

c) Thuật toán kiểm tra

Thuật toán 2.3:

Input: n, t, y, M, (e,s).
Output: (e,s) = *true* / *false* .

[1]. $u \leftarrow s^t \times y^e \bmod n$; (1.7)
[2]. $v \leftarrow H(u \| M)$; (1.8)
[3]. **if** $(v = e)$ **then** {**return** *true* }
else {**return** *false* }

Chú thích:
- Nếu kết quả trả về *true* thì chữ ký (e,s) hợp lệ, do đó nguồn gốc và tính toàn vẹn của bản tin cần thẩm tra M được công nhận.
- Nếu kết quả trả về là *false* thì chữ ký (e,s) là giả mạo, hoặc nội dung bản tin M đã bị sửa đổi.

3.2. Xây dựng lược đồ chữ ký số mù

Lược đồ chữ ký số mù, ký hiệu LD-02, được phát triển từ lược đồ cơ sở LD-01. Giả sử A là người người ký có khóa công khai được hình thành theo Thuật toán 2.1 của lược đồ cơ sở và B là người tạo ra bản tin M được ký.

3.2.1. Thuật toán ký

Thuật toán 2.4:

Input: n, t, x, k, α, β, M.
Output: (e,s).

[1]. $r_a \leftarrow k^t \bmod n$; (2.1)
[2]. $r_b \leftarrow (r_a)^\alpha \times y^\beta \times \beta^t \bmod n$; (2.2)
[3]. $e \leftarrow H(r_b \| M)$; (2.3)
[4]. $e_b \leftarrow \alpha^{-1} \times (e - \beta) \bmod n$; (2.4)
[5]. $s_a \leftarrow k \times x^{e_b} \bmod n$; (2.5)

[6]. $s \leftarrow (s_a)^{\alpha} \times \beta \bmod n$; (2.6b)

[7]. **return** (e,s)

Chú thích:

- Các bước [1], [5] do người ký A thực hiện.
- Các bước [2], [3], [4], [6] và [7] do người có bản tin cần ký B thực hiện.
- Tham số k do A lựa chọn thỏa mãn: 1< k < n.
- Các tham số α, β do B lựa chọn thỏa mãn: 1< α, β < t.

3.2.2. Thuật toán kiểm tra

Thuật toán 2.5:

Input: n, t, y, M, (e,s).

Output: (e,s) = *true* / *false* .

[1]. $u \leftarrow (s)^t \times y^e \bmod n$; (2.7)

[2]. $v \leftarrow H(u \| M)$; (2.8)

[3]. **if** ($v = e$) **then** {**return** *true* }

else {**return** *false* }

Chú thích:

- Nếu kết quả trả về *true* thì tính hợp lệ của chữ ký (e,s) được công nhận, do đó nguồn gốc và tính toàn vẹn của bản tin cần thẩm tra M được khẳng định.
- Nếu kết quả trả về là *false* thì chữ ký (e,s) là giả mạo, hoặc nội dung bản tin M đã bị sửa đổi.

3.2.3. Tính đúng đắn của lược đồ LD-02

Nếu chữ ký được hình thành bằng Thuật toán 2.4a, điều cần chứng minh ở đây là: cho p, q là 2 số nguyên tố phân biệt, $n = p \times q$, $H : \{0,1\}^* \mapsto Z_m$ với: $m < n$, $t = \left[\frac{m}{2}\right] + 1$, $1 < x, k < n$, $1 < \alpha, \beta < t$, $y = (x)^{-t} \bmod n$, $r_a = k^t \bmod n$, $r_b = (r_a)^{\alpha} \times y^{\beta} \times \beta^t \bmod n$, $e_b = H(r_b \| M)$, $e = (e_b \times \alpha + \beta) \bmod n$, $s_a = k \times x^{e_b} \bmod n$, $s = (s_a)^{\alpha} \times \beta \bmod n$. Nếu: $u = (s)^t \times (y)^e \bmod n$ và $v = H(u \| M)$ thì: $v = e$.

Thật vậy, từ (1.1), (2.1a), (2.4a), (2.5a), (2.6a) và (2.7) ta có:

$$\begin{aligned} u &= s^t \times y^e \bmod n \\ &= \left((s_a)^{\alpha} \times \beta \bmod n\right)^t \times \left(x^{-t} \bmod n\right)^{(e_b.\alpha+\beta)} \bmod n \\ &= (s_a)^{\alpha.t} \times \beta^t \times x^{-t.(\alpha.e_b+\beta)} \bmod n \\ &= \left(k \times x^{e_b} \bmod n\right)^{\alpha.t} \times \beta^t \times x^{-\alpha.e_b.t} \times x^{-t.\beta} \bmod n \\ &= \left(k^t\right)^{\alpha} \times x^{\alpha.e_b.t} \times \beta^t \times x^{-\alpha.e_b.t} \times \left(x^{-t}\right)^{\beta} \bmod n \\ &= (r_a)^{\alpha} \times \beta^t \times y^{\beta} \bmod n \end{aligned} \quad (2.9)$$

Từ (2.2a) và (2.9), suy ra: $u = r_b$ (2.10)

Thay (2.10) vào (2.8) ta có: $v = H(u \| M) = H(r_b \| M)$ (2.11)

Từ (2.3a) và (2.11), suy ra: $v = e$. Đây là điều cần chứng minh.

Trường hợp chữ ký được hình thành bằng Thuật toán 2.4b, khi đó điều cần chứng minh ở đây là: cho p, q là 2 số nguyên tố phân biệt, $n = p \times q$, $H : \{0,1\}^* \mapsto Z_m$ với: $m < n$, $t = \left[\frac{m}{2}\right] + 1$, $1 < x, k < n$, $1 < \alpha, \beta < t$, $y = (x)^{-t} \bmod n$, $r_a = k^t \bmod n$, $r_b = (r_a)^{\alpha} \times y^{\beta} \times \beta^t \bmod n$, $e = H(r_b \| M)$, $e_b \leftarrow \alpha^{-1} \times (e - \beta) \bmod n$, $s_a = k \times x^{e_b} \bmod n$, $s = (s_a)^{\alpha} \times \beta \bmod n$. Nếu: $u = (s)^t \times (y)^e \bmod n$ và $v = H(u \| M)$ thì: $v = e$.

Có thể thấy rằng trong cả 2 thuật toán ký: Thuật toán 2.4a và Thuật toán 2.4b, ta đều có: $e = (e_b \times \alpha + \beta) \bmod n$, nên việc chứng minh tính đúng đắn của lược đồ trong trường hợp sử dụng Thuật toán 2.4b để hình thành chữ ký là hoàn toàn tương tự như trường hợp chữ ký được hình thành bằng Thuật toán 2.4a trên đây.

3.2.4. Mức độ an toàn của lược đồ LD-02

Tương tự như với lược đồ cơ sở LD-01, mức độ an toàn của lược đồ LD-02 cũng được đánh giá qua các khả năng:

- Chống tấn công làm lộ khóa mật.
- Chống giả mạo chữ ký.

Ngoài ra, với một lược đồ chữ ký số mù, mức độ an toàn của nó còn được đánh giá qua khả năng chống tấn công làm lộ nguồn gốc bản tin sau khi được ký. Yêu cầu đặt ra ở đây là, sau khi bản tin M đã được ký thì người ký A cũng như bất kỳ một đối tượng sử dụng nào khác hoàn toàn không thể biết được bản tin M được tạo ra từ người yêu cầu ký B.

a) Khả năng chống tấn công làm lộ khóa mật và giả mạo chữ ký

Mức độ an toàn của lược đồ LD-02 được thiết lập dựa trên mức độ an toàn của lược đồ cơ sở LD-01. Xét theo khả năng chống tấn công làm lộ khóa mật và khả năng chống giả mạo chữ ký, có thể thấy rằng mức độ an toàn của 2 lược đồ này (LD-01, LD-02) là tương đương như nhau.

b) Khả năng chống tấn công làm lộ nguồn gốc của bản tin sau khi ký

Thuật toán ký của lược đồ LD-02 cho thấy, với việc lưu trữ các tham số $\{r_a, e_b\}$ cùng với định danh của người yêu cầu ký (ID_B), người ký A có thể xác định được mối quan hệ giữa $\{M,(e,s)\}$ với ID_B, nghĩa là có thể xác định được người yêu cầu ký B từ bản tin M và chữ ký tương ứng (e,s), nếu từ (2.4) và (2.6) người ký A có thể xác định được các tham số (α,β). Thật vậy, khi biết (α,β) người ký A hoàn toàn có thể xác định được ID_B bằng thuật toán như sau:

Thuật toán 2.6:

Input: $\{(r_{ai}, e_{bi}, ID_{Bi}) | \ i=1,2,\ldots N\}$, M, α, β.

Output: ID_{Bi}.

[1]. $m \leftarrow H(M)$, i = 0;

[2]. **select**: $(r_{ai}, e_{bi}, ID_{Bi})$;

[3]. $r_{bi}^* \leftarrow (r_{ai})^{\alpha} \times y^{\beta} \times \beta^t \bmod n$;

[4]. $e_{bi}^* \leftarrow H(r_{bi}^* \| M)$

[5]. **if** $e_{bi}^{*} \neq e_{bi}$ **then**
  [5.1]. $i \leftarrow i+1$;
  [5.2]. **goto** [2];
[6]. **return** ID_{Bi}

Nhận xét: Thuật toán 2.6 cho thấy mức độ an toàn của lược đồ LD-02 xét theo khả năng giữ bí mật nguồn gốc của bản tin phụ thuộc vào mức độ khó của việc tìm được các tham số bí mật (α,β) từ việc giải (2.4) hoặc (2.6).

3. Kết luận

Trên cơ sở phát triển một dạng lược đồ chữ ký số xây dựng dựa trên tính khó của bài toán khai căn, bài báo đề xuất một lược đồ chữ ký số mù có độ an toàn cao hơn các lược đồ chữ ký số mù đã được công bố trước đó xét theo khả năng chống tấn công làm lộ nguồn gốc của bản tin được ký. Đây là yếu tố hết sức quan trọng để cho phép một lược đồ chữ ký số mù có thể ứng dụng được trong thực tế.

Tài liệu tham khảo

1. D. Chaum, *Blind signature systems*, Advances in Cryptology-CRYPTO'83, Plenum Press, 1984, pp. 153-156.
2. D. Chaum, *Blind signature for untraceable payments*, Advances in Cryptology-CRYPTO 1982, Plenum Press, NY, 1983, pp. 199-203.
3. D. Chaum, *Privacy Protected Payment*, *SMART CARD 2000*, Elsevier Science Publishers B.V., 1989, pp. 69-93.
4. N. Ferguson, *Single Term Off-line Coins*, Advances in Cryptology-EUROCRYPT'93, Lecture Notes in Computer Sciences, Vol. 765/1994, 1994, pp. 318-328.
5. D. Chaum, B. den Boer, E. van Heyst, S. Mjolsnes, A. Steenbeek, "*Efficient Offline Electronic Checks*", Advances in Cryptology, Eurocrypt'89, LNCS 434, Springer Verlag, pp. 294-301.
6. R. Rivest, A. Shamir, L. Adleman, *A Method for Obtaining Digital Signatures and Public Key Cryptosystems,* Communications of the ACM, Vol. 21, No. 2, 1978, pp. 120 – 126.
7. National Institute of Standards and Technology, NIST FIPS PUB 186-3. *Digital Signature Standard,* U.S. Department of Commerce, 1994.
8. K. Nyberg, R. A. Rueppel, *A New Signature Scheme Base on the DSA Giving Message Recovery*, 1st ACM conference on Computer and Communications Security, November 3 – 5, Fairfax, Virginia.
9. Jan L. Camenisch, Jean-Marc Piveteau, Markus A. Stadler, *Blind Signatures Base on Discrete Logarithm Problem*, Swiss KWF Foundation, grant no. 2724.1.
10. Lưu Hồng Dũng, Nguyễn Tiền Giang,…, *Phát triển một dạng lược đồ chữ ký số mới*, Kỷ yếu Hội thảo quốc gia lần thứ XVI: Một số vấn đề chọn lọc của Công nghệ thông tin và truyền thông- Đà Nẵng, 2013.

Lưu Hồng Dũng.
Sinh năm 1966.Tốt nghiệp đại học ngành Vô tuyến Điện tử tại Học viện Kỹ thuật Quân sự năm 1989. Hiện đang công tác tại khoa CNTT - Học viện KTQS. Hướng nghiên cứu: An toàn và bảo mật thông tin.
Email: luuhongdung@gmail.com.