PHƯƠNG PHÁP XÂY DỰNG LƯỢC ĐỒ CHỮ KÝ SỐ DỰA TRÊN TÍNH KHÓ CỦA BÀI TOÁN LOGARIT RỜI RẠC TRÊN VÀNH Z_n

Pham Van Hiep[*], Đoan Thi Bich Ngoc[+], Luu Hong Dung[+]
[*] Khoa Công nghệ thông tin, Trường đại học Công nghiệp Hà Nội
[+] Khoa CNTT, Trường đại học CNTT & TT - ĐH Thái Nguyên
[+] Khoa Công nghệ thông tin, Học Viện Kỹ thuật Quân Sự

Tóm tắt: Phát triển các lược đồ chữ ký số nhằm đáp ứng các nhu cầu giao dịch, hoạt động trong xã hội luôn là vấn đề được quan tâm. Tuy nhiên, mức độ an toàn của các lược đồ này luôn phải được bảo đảm. Trong bài báo này, chúng tôi đề xuất một phương pháp xây dựng lược đồ chữ ký tổng quát dựa trên bài toán logarit rời rạc trên vành Z_n. Từ phương pháp được đề xuất có thể tạo ra một họ lược đồ chữ ký mới tương tự như họ chữ ký ElGamal. Tuy nhiên, khi thực hiện lựa chọn các tham số phù hợp thì các lược đồ chữ ký xây dựng theo phương pháp mới đề xuất có độ an toàn cao hơn các lược đồ họ ElGamal. Dựa trên lược đồ chữ ký tổng quát, chúng tôi đã đề xuất được ba lược đồ chữ ký mới. Độ an toàn của các lược đồ này được bảo đảm bởi tính khó của việc giải đồng thời hai bài toán phân tích một số nguyên lớn ra các thừa số nguyên tố (Bài toán phân tích số) và bài toán logarit rời rạc trên *Zp* (DLP). Các lược đồ mới đề xuất phù hợp với các ứng dụng đòi hỏi tính an toàn cao trong thực tế.

Từ khóa: Bài toán logarit rời rạc; Bài toán phân tích số; Chữ ký số; Lược đồ chữ ký số; Số nguyên.

I. ĐẶT VẤN ĐỀ

Trong [1] đã đề xuất một lược đồ chữ ký số xây dựng dựa trên tính khó của việc giải đồng thời hai bài toán phân tích số và bài toán logarit rời rạc trên trường Z_p [2]. Ưu điểm của lược đồ này [1] là có độ an toàn cao hơn các lược đồ xây dựng chỉ trên một bài toán khó như các lược đồ họ ElGamal [3] hay lược đồ RSA [4] xây dựng trên ba bài toán nhưng chỉ cần giải được một trong ba bài toán này thì tính an toàn của lược đồ sẽ bị phá vỡ.

Phân tích trong [1] cũng đã chỉ ra tính khó của việc giải đồng thời hai bài toán phân tích số và bài toán logarit rời rạc trên trường Z_p là tương đương với tính khó của việc giải bài toán logarit rời rạc trên vành Z_n. Trên cơ sở đó, bài báo đề xuất một phương pháp xây dựng lược đồ chữ ký có tính tổng quát dựa trên bài toán logarit rời rạc trên vành Z_n. Ưu điểm của phương pháp được đề xuất ở đây là cho phép tạo ra một họ lược đồ chữ ký có độ an toàn cao, từ đó mở rộng khả năng lựa chọn được thuật toán phù hợp với các ứng dụng thực tế.

Tác giả liên hệ: Phạm Văn Hiệp
Email: hiephic@gmail.com; hieppv@haui.edu.vn
Đến tòa soạn: 17/2/2021, chỉnh sửa: 15/5/2021, chấp nhận đăng: 7/6/2021

II. BÀI TOÁN LOGARIT RỜI RẠC TRÊN VÀNH Z_n

Cho cặp các số nguyên dương $\{n,g\}$ với n là tích hai số nguyên tố p và q sao cho bài toán phân tích số là khó giải trên Z_n, còn g là một phần tử của nhóm Z_n*. Khi đó, bài toán logarit rời rạc trên Z_n hay còn gọi là bài toán $DLP_{(n,g)}$ được phát biểu như sau:

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

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

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

$$x = DLP_{(n,g)}(y)$$

Ở dạng lược đồ chữ ký mới được đề xuất, mỗi thành viên của hệ thống tự chọn cho mình bộ tham số (n,g), khóa bí mật x được chọn thỏa mãn: $1 < x < \varphi(n)$ và tính khóa công khai theo: $y = g^x \bmod n$

Bài toán $DLP_{(n,g)}$ là một trong ba bài toán cơ sở xây dựng nên hệ mật RSA. Hiện tại, bài toán $DLP_{(n,g)}$ vẫn được coi là bài toán khó [2] do chưa có giải thuật thời gian đa thức cho bài toán này và cũng như chưa có một công bố nào cho thấy hệ mật RSA bị phá vỡ trong các ứng dụng thực tế bằng việc giải bài toán này khi các tham số của nó được chọn hợp lý.

III. XÂY DỰNG LƯỢC ĐỒ CHỮ KÝ SỐ DỰA TRÊN BÀI TOÁN $DLP_{(N,G)}$

A. Phương pháp xây dựng

Phương pháp xây dựng lược đồ chữ ký đề xuất ở đây bao gồm các phương pháp hình thành các tham số hệ thống và khóa, phương pháp hình thành chữ ký và phương pháp kiểm tra tính hợp lệ của chữ ký. Từ phương pháp này, bằng cách lựa chọn các tham số cụ thể sẽ cho phép tạo ra các lược đồ chữ ký số khác nhau cho các ứng dụng thực tế.

1. Phương pháp 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: *p, q* và *lp, lq* - độ dài (tính theo bit) của số nguyên tố.
Output: *n, m, g, y, x_1, x_2*.
Bước 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.
Bước 2: Tính $n = p.q$ và $\varphi(n) = (p-1).(q-1)$
Bước 3: Chọn p_1, q_1 là các số nguyên tố thỏa mãn:
$p_1|(p-1), q_1|(q-1)$ và: $p_1 \nmid (q-1), q_1 \nmid (p-1)$
Bước 4: Tính: $m = p_1.\ q_1$
Bước 5: Chọn *g* là phần tử sinh của nhóm 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: $\alpha \in (1,n)$.
Bước 6: Chọn khóa bí mật thứ nhất x_1 trong khoảng (1,*m*).
Bước 7: Tính khóa công khai theo:
$$y = g^{\pm x_1} \bmod n \quad (1)$$
Kiểm tra nếu: $y \geq \varphi(n)$ hoặc: $\gcd(y, \phi(n)) \neq 1$ thì thực hiện lại từ Bước 6.
Bước 8: Tính khóa bí mật thứ hai theo:
$$x_2 = y^{-1} \bmod \varphi(n) \quad (2)$$
Bước 9: Chọn hash function H: $\{0,1\}^* \to Z_h$, với: h < n.

<u>*Chú thích:*</u>
+ *len(.)* là hàm tính độ dài (theo bit) của một số.
+ Khóa công khai là *y*, khóa bí mật là (*m*, x_1, x_2).
+ Các tham số công khai là *n, g*; các tham số bí mật là: *p, q,* p_1, q_1 và $\varphi(n)$.

2. Phương pháp hình thành chữ ký
Thuật toán 1.2: Sinh chữ ký.
Input: *n, g,* x_1,x_2, *M*.
Output: (*e,s*).
Bước 1: Chọn k: $1 < k < m$. Tính:
$$r = g^k \bmod n \quad (3)$$
Bước 2: Tính thành phần thứ nhất *e*:
$$e = f_1(M,r) \quad (4)$$
Bước 3: Thành phần thứ hai được tính theo một trong ba dạng sau:
$$s = x_2 \times \left(k \times f_2(M,e)^{-1} + x_1 \times f_3(M,e)\right) \bmod m \quad (5)$$
nếu $\gcd(f_2(M,e), m) \neq 1$ thì quay lại Bước 1.
Hoặc:
$$s = x_2 \times k \times \left(f_2(M,e) + x_1 \times f_3(M,e)\right)^{-1} \bmod m \quad (6)$$
nếu $\gcd(f_2(M,e) + x_1 \times f3(M,e), m) \neq 1$ thì quay lại Bước 1;
Hoặc:
$$s = (x_1)^{-1} \times x_2 \times \left(k \times f_2(M,e)^{-1} - f_3(M,e)\right) \bmod m \quad (7)$$
nếu $\gcd(f_2(M,e), m) \neq 1$ thì quay lại Bước 1.

<u>*Chú thích*</u>:
+ $f_1(.)$: hàm của *M* và *r* có giá trị trong khoảng (1,*n*).
+ $f_2(.)$, $f_3(.)$: các hàm của *M* và *r* hoặc *e* có giá trị trong khoảng $(1, \varphi(n))$.

3. Phương pháp kiểm tra chữ ký
Thuật toán 1.3: Kiểm tra chữ ký
Input: *n, g, y, M,* (*e,s*).
Output: true/ false
Bước 1: Tính giá trị *u*:
$$u = g^{s.f_2(M,e).y} \times y^{f_2(M,e).f_3(M,e)} \bmod n \quad (8)$$
nếu *s* được tính theo (5).
Hoặc:
$$u = g^{s.f_2(M,e).y} \times y^{s.f_3(M,e).y} \bmod n \quad (9)$$
nếu *s* được tính theo (6).
Hoặc:
$$u = y^{s.f_2(M,e)^{-1}.y} \times g^{f_2(M,e)^{-1}.f_3(M,e)} \bmod n \quad (10)$$
nếu s được tính theo (7).
Bước 2: Tính giá trị *v*:
$$v = f_1(M,u) \quad (11)$$
Bước 3: Kiểm tra nếu: *v = e* thì: (*e,s*) = true, ngược lại: (*e,s*) = false.

<u>*Chú thích*</u>:
+ (*r,s*)/(*e,s*) = true: chữ ký hợp lệ, bản tin *M* được công nhận về nguồn gốc và tính toàn vẹn.
+ (*r,s*)/(*e,s*) = false: chữ ký giả mạo và/hoặc *M* không còn toàn vẹn.

4. Tính đúng đắn của phương pháp mới đề xuất
Tính đúng đắn của phương pháp mới đề xuất được chứng minh qua các mệnh đề sau đây:
Mệnh đề 1:
Với các tham số và khóa được hình thành bởi **Thuật toán 1.1** với $y = g^{-x_1} \bmod n$, chữ ký (*e,s*) được sinh bởi (4) và (5) của **Thuật toán 1.2**, giá trị *u, v* được tạo bởi (8) và (11) của **Thuật toán 1.3** thì $v = e$.
Chứng minh:
Thật vậy, ta có:
$$\begin{aligned} u &= g^{s.f_2(M,e).y} \times y^{f_2(M,e).f_3(M,e)} \bmod n \\ &= g^{s.y.f_2(M,e)} \times g^{-x_1.f_2(M,e).f_3(M,e)} \bmod n \\ &= g^{f_2(M,e).x_2.\left(k.f_2(M,e)^{-1} + x_1.f_3(M,e)\right).y} \times g^{-x_1.f_2(M,e).f_3(M,e)} \bmod n \\ &= g^{k + x_1.f_2(M,e).f_3(M,e) - x_1.f_2(M,e).f_3(M,e)} \bmod n \\ &= g^k \bmod n \end{aligned}$$
Suy ra: $u = g^k \bmod n$ (12)
Từ (3) và (12) suy ra: *u = r*.
Do đó:
$$v = f_1(M,u) = f_1(M,r) \quad (13)$$
Từ (4) và (13) suy ra điều cần chứng minh: *v = e*.
Mệnh đề 2:
Với các tham số và khóa được hình thành bởi **Thuật toán 1.1** với $y = g^{x_1} \bmod n$, chữ ký (*e,s*) được sinh bởi (4) và (6) của **Thuật toán 1.2**, giá trị *u, v* được tạo bởi (9) và (11) của **Thuật toán 1.3** thì $v = e$.
Chứng minh:
Thật vậy, ta có:
$$\begin{aligned} u &= g^{s.f_2(M,e).y} \times y^{s.f_3(M,e).y} \bmod n \\ &= g^{f_2(M,e).x_2.k.\left(f_2(M,e)+x_1.f_3(M,e)\right)^{-1}.y} \times g^{x_1.f_3(M,e).x_2.k.\left(f_2(M,e)+x_1.f_3(M,e)\right)^{-1}.y} \bmod n \\ &= g^{f_2(M,e).k.\left(f_2(M,e)+x_1.f_3(M,e)\right)^{-1}} \times g^{x_1.f_3(M,e).k.\left(f_2(M,e)+x_1.f_3(M,e)\right)^{-1}} \bmod n \\ &= g^{k.\left(f_2(M,e)+x_1.f_3(M,e)\right)\left(f_2(M,e)+x_1.f_3(M,e)\right)^{-1}} \bmod n \\ &= g^k \bmod n \end{aligned}$$
Suy ra: $u = g^k \bmod n$ (14)
Từ (3) và (14) suy ra: *u = r*.

Do đó:

$$v = f_1(M,u) = f_1(M,r) \quad (15)$$

Từ (4) và (15) ta có điều cần chứng minh: $v = e$.

Mệnh đề 3:

Với các tham số và khóa được hình thành bởi **Thuật toán 1.1** với $y = g^{x_1} \bmod n$, chữ ký (e,s) được sinh bởi (4) và (7) của **Thuật toán 1.2**, giá trị u, v được tạo bởi (10) và (11) của **Thuật toán 1.3** thì $v = e$.

Chứng minh:

Thật vậy, ta có:

$$u = y^{s.f_2(M,e)^{-1}.y} \times g^{-f_2(M,e)^{-1}.f_3(M,e)} \bmod n$$

$$= g^{x_1.f_2(M,e)^{-1}.x_2.x^{-1}.(k.f_2(M,e)+f_3(M,e)).y} \times g^{-f_2(M,e)^{-1}.f_3(M,e)} \bmod n$$

$$= g^{f_2(M,e)^{-1}.(k.f_2(M,e)+f_3(M,e))} \times g^{-f_2(M,e)^{-1}.f_3(M,e)} \bmod n$$

$$= g^{k+f_2(M,e)^{-1}.f_3(M,e)-f_2(M,e)^{-1}.f_3(M,e)} \bmod n$$

$$= g^k \bmod n$$

Suy ra: $u = g^k \bmod n \quad (16)$

Từ (3) và (16) suy ra: $u = r$.

Do đó:

$$v = f_1(M,u) = f_1(M,r) \quad (17)$$

Từ (4) và (17) suy ra điều cần chứng minh: $v = e$.

B. Một số lược đồ chữ ký xây dựng theo phương pháp mới đề xuất

1. Lược đồ chữ ký LDH.Z – 01

Lược đồ thứ nhất - Ký hiệu LDH.Z – 01, được xây dựng theo phương pháp đề xuất với các lựa chọn:

- Khóa công khai: $y = g^{-x_1} \bmod n$
- Thành phần thứ nhất e của chữ ký được tính theo: $e = f_1(M,e) = r$
- Thành phần thứ hai s của chữ ký tính theo (5) với: $f_2(M,e) = r$ và $f_3(M,e) = H(M)$
- Giá trị u trong thuật toán kiểm tra được tính theo (8).

**) Thuật toán ký*

Input: n, g, x_1, x_2, M.
Output: (r,s).

[1]. **select** k: $1 < k < m$
[2]. $r \leftarrow g^k \bmod n$
if $\gcd(r,m) \neq 1$ **goto** [1]
[3]. $s \leftarrow x_2 \times \left(k \times r^{-1} + x_1 \times H(M)\right) \bmod m$
[4]. **return** (r,s)

**) Thuật toán kiểm tra*

Input: $n, g, y, M, (r,s)$.
Output: *(r,s) = true / false* .

[1]. $u \leftarrow g^{s.r.y} \times y^{r.H(M)} \bmod n$
[2]. **if** $(u = r)$ **then** {return *true*}
else {return *false*}

**) Tính đúng đắn của LDH.Z – 01*

Với: $y = g^{-x_1} \bmod n$, thay: $e = f_1(M,e) = r$, $f_2(M,e) = r$, $f_3(M,e) = H(M)$ vào (1), (4), (5), (8), theo **Mệnh đề 1** ta có điều cần chứng minh: $u = r$.

2. Lược đồ chữ ký LDH.Z – 02

Lược đồ thứ hai - Ký hiệu LDH.Z – 02, được xây dựng theo phương pháp đề xuất với các lựa chọn:

- Khóa công khai: $y = g^{x_1} \bmod n$
- Thành phần thứ nhất e của chữ ký được tính theo: $e = f_1(M,e) = r$
- Thành phần thứ hai s của chữ ký tính theo (9) với: $f_2(M,e) = r$ và $f_3(M,e) = H(M)$
- Giá trị u trong thuật toán kiểm tra được tính theo (9).

**) Thuật toán ký*

Input: n, g, x_1, x_2, M.
Output: (r,s)

[1]. **select** k: $1 < k < m$
[2]. $r \leftarrow g^k \bmod n$
[3]. $s \leftarrow x_2 \times k \times \left(r + x_1 \times H(M)\right)^{-1} \bmod m$
if $\gcd\left(r + x_1 \times H(M)\right) \neq 1$ **goto** [1]
[4]. **return** (r,s)

**) Thuật toán kiểm tra*

Input: $n, g, y, M, (r,s)$
Output: *(r,s) = true / false* .

[1]. $u \leftarrow g^{s.r.y} \times y^{s.H(M)} \bmod n$
[2]. **if** $(u = r)$ **then** {return *true* }
else {return *false* }

**) Tính đúng đắn của LDH.Z – 02*

Với: $y = g^{x_1} \bmod n$, thay: $e = f_1(M,e) = r$, $f_2(M,e) = r$ và $f_3(M,e) = H(M)$ vào (1), (4), (6), (9) theo **Mệnh đề 2** ta có điều cần chứng minh: $u = r$.

3. Lược đồ chữ ký LDH.Z – 03

Lược đồ thứ 3 - Ký hiệu LDH.Z – 03, được xây dựng theo phương pháp đề xuất với các lựa chọn:

- Khóa công khai: $y = g^{x_1} \bmod n$
- Thành phần thứ nhất e của chữ ký được tính theo: $e = f_1(M,e) = H(M \| r)$
- Thành phần thứ hai s của chữ ký được tính theo (7) với: $f_2(M,e) = 1$ và $f_3(M,e) = e$
- Giá trị u trong thuật toán kiểm tra được tính theo (10).

**) Thuật toán ký*

Input: n, g, x_1, x_2, M.
Output: (e,s).

[1]. **select** k: $1 < k < m$
[2]. $r \leftarrow g^k \bmod n$
[3]. $e \leftarrow H(M \| r)$
[4]. $s \leftarrow (x_1)^{-1} \times x_2 \times (k - e) \bmod m$
[5]. **return** *(e,s)*

**) Thuật toán kiểm tra*

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

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

**) Tính đúng đắn của LDH.Z – 03*

Với: $y = g^{x_1} \bmod n$, thay: $e = f_1(M,e) = H(M \| r)$, $f_2(M,e) = 1$ và $f_3(M,e) = e$ vào (1), (4), (7), (10), theo **Mệnh đề 3** ta có điều cần chứng minh: $v = e$.

C. Một số đánh giá về các lược đồ chữ ký xây dựng theo phương pháp mới đề xuất

1. Mức độ an toàn

Mức độ an toàn của một lược đồ chữ ký số được đánh giá qua các khả năng sau:

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

1.1. Tấn công khóa bí mật

Ở phương pháp mới đề xuất, khóa bí mật của một đối tượng ký là cặp (m, 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, còn để tính được x_1 cần phải giải được $DLP_{(n,g)}$. Như đã chỉ ra trong [1], việc giải được $DLP_{(n,g)}$ là khó tương đương với việc giải đồng thời hai bài toán phân tích số và logarit rời rạc trên Z_p. Vì thế, tính an toàn về khóa của các lược đồ xây dựng theo phương pháp mới đề xuất được đảm bảo bởi tính khó của việc giải đồng thời hai bài toán phân tích số và logarit rời rạc trên Z_p.

Ngoài ra, tham số m - bậc của phần tử sinh g, cũng được sử dụng với vai trò khóa bí mật trong thuật toán ký. Như vậy, để phá vỡ tính an toàn của lược đồ, kẻ tấn công còn phải giải được bài toán tìm bậc của g.

1.2. Tấn công giả mạo chữ ký

Khả năng chống tấn công giả mạo phụ thuộc vào từng lược đồ chữ ký cụ thể. Ở đây sẽ phân tích ba lược đồ LDH.Z – 01, LDH.Z – 02 và LDH.Z – 03 có tính chất đại diện cho ba dạng lược đồ khác nhau xây dựng theo phương pháp đề xuất.

Với lược đồ thứ nhất, một cặp (r,s) bất kỳ sẽ được công nhận là chữ ký hợp lệ tương ứng với bản tin M do lược đồ sinh ra nếu thỏa mãn:

$$r = g^{s.r.y} \times y^{r.H(M)} \bmod n \quad (18)$$

Khi kẻ tấn công không biết khóa bí mật thì cách tốt nhất là chọn trước r rồi tính s. Khi đó (18) sẽ có dạng:

$$A = g^{s} \bmod n \quad (19)$$

Với A là hằng số, thì việc tìm s từ (19) thực chất là giải bài toán $DLP_{(n,g)}$.

Hoàn toàn tương tự, một cặp (r,s) bất kỳ cũng sẽ được công nhận là chữ ký hợp lệ tương ứng với bản tin M do lược đồ thứ hai sinh ra nếu thỏa mãn điều kiện:

$$r = g^{s.r.y} \times y^{s.H(M)} \bmod n \quad (20)$$

Để tìm cặp (r,s) thỏa mãn (20) khi không biết khóa bí mật thì kẻ tấn công cũng chỉ có cách chọn trước r rồi tính s. Khi đó (20) sẽ trở thành:

$$B = g^{s} \bmod n \quad (21)$$

Rõ ràng là để tìm s từ (21), kẻ tấn công không có cách nào khác là phải giải được bài toán $DLP_{(n,g)}$.

Ở lược đồ thứ ba, một cặp (e,s) sẽ là chữ ký hợp lệ với bản tin M nếu thỏa mãn:

$$e = H\left(M \| \left(g^{e} \times y^{s.y} \bmod n\right)\right) \quad (22)$$

Nếu H(.) được chọn là hàm băm kháng va chạm mạnh (như SHA-256/512,…) thì việc chọn ngẫu nhiên (e,s) để thỏa mãn (22) là bất khả thi. Trường hợp này, kẻ tấn công có thể chọn trước giá trị u rồi tính thành phần thứ nhất của chữ ký: $e = H(M||u)$, rồi tính thành phần thứ hai của chữ ký dựa vào điều kiện:

$$u = g^{e} \times y^{s.y} \bmod n \quad (23)$$

Tìm s từ (23) thực chất cũng là giải bài toán $DLP_{(n,g)}$ khi đó có dạng:

$$C = g^{s} \bmod n \quad (24)$$

Như vậy, ở cả ba dạng lược đồ xây dựng theo phương pháp mới đề xuất, để giả mạo thành công thì kẻ tấn công buộc phải giải được bài toán $DLP_{(n,g)}$. Nói cách khác, khả năng chống tấn công giả mạo của các lược đồ xây dựng theo phương pháp đề xuất ở đây được bảo đảm bằng tính khó của việc giải đồng thời bài toán phân tích số và bài toán logarit rời rạc trên Z_p.

2. Hiệu quả thực hiện thuật toán

Tính hiệu quả của lược đồ chữ ký có thể đánh giá qua chi phí thực hiện của các thuật toán ký, kiểm tra chữ ký và kích thước chữ ký mà lược đồ sinh ra. Có thể thấy rằng, để nâng cao độ an toàn cho các lược đồ xây dựng theo phương pháp mới đề xuất thì các thuật toán hình thành tham số và khóa, thuật toán ký và thuật toán kiểm tra có độ phức tạp cao hơn các lược đồ DSA, RSA trong chuẩn chữ ký DSS [5] khi kích thước các bộ tham số được lựa chọn tương đương nhau, từ đó chi phí thực hiện các lược đồ theo phương pháp mới đề xuất sẽ cao hơn (đồng nghĩa với hiệu quả thực hiện thuật toán thấp hơn) so với các lược đồ trong DSS.

IV. KẾT LUẬN

Bài báo đề xuất một phương pháp xây dựng lược đồ chữ ký số dựa trên tính khó của việc giải bài toán logarit rời rạc trên vành Z_n. Từ phương pháp đã đề xuất có thể xây dựng được một họ lược đồ chữ ký số mới, mà độ an toàn của các lược đồ xây dựng theo phương pháp này được bảo đảm bằng tính khó của việc giải đồng thời hai bài toán phân tích số và logarit rời rạc trên Z_p phù hợp với các ứng dụng đòi hỏi có tính an toàn cao trong thực tế.

REFERENCES

[1] P. V. Hiep, N. H. Mong, and L. H. Dung, “A signature algorithm based on difficulty of simultaneous solving integer factorization and discrete logarithm problem,” Journal of Science and Technology - The University of Danang, vol. 128, no. 7, pp. 75-79, 2018.

[2] A. Menezes, P. van Oorschot, and S. Vanstone, Handbook of Applied Cryptography. CRC Press, 1996.

[3] T. ElGamal, “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, 1985.

[4] R. L. Rivest, A. Shamir, and L. Adleman, “A method for Obtaining digital signatures and public key cryptosystems,” Communications of the ACM, vol. 21, pp. 120-126, 1978.

[5] National Institute of Standards and Technology, NIST FIPS PUB 186-4. Digital Signature Standard, U.S. Department of Commerce, 2013.

THE METHOD OF CONSTRUCTING THE DIGITAL SIGNATURE SCHEME BASED ON THE DIFFICULTY OF THE DISCRETE LOGARITHMIC PROBLEM ON THE RING Z_n

Abstract: Developing digital signature schemes to meet the needs of transactions and activities in society is always a matter of concern. However, the security of these schemes must always be guaranteed. In this paper, we propose a method to build a general signature scheme based on the discrete logarithmic problem on Z_n rings. From the proposed method, it is possible to create a new signature schema family similar to the ElGamal signature family. However, when making the selection of the appropriate parameters, the proposed new method signature schemas have a higher degree of security than the ElGamal family schemas. Based on the general signature scheme, we have proposed three new signature schemes. The safety of these schemas is ensured by the difficulty of solving two problems simultaneously analyzing a large integer to prime factors (the numerical analysis problem) and the discrete logarithm problem on Z_p (DLP). The proposed new schemas are suitable for practical applications requiring high security.

Keywords: Dicrete logarithm problem; factorization problem; digital signature; digital signature schema; integer factoring problem.

Phạm Văn Hiệp Nhận học vị Thạc sỹ năm 2007. Hiện công tác tại khoa Công nghệ thông tin, trường đại học Công nghiệp Hà Nội. Lĩnh vực nghiên cứu: Mật mã và An toàn thông tin, Mạng và hệ thống thông tin.

Đoàn Thị Bích Ngọc học vị Thạc sỹ. Hiện công tác tại khoa Công nghệ thông tin, trường Đại học Công nghệ thông tin & Truyền thông - Đại học Thái Nguyên. Lĩnh vực nghiên cứu: An toàn thông tin, hệ thống thông tin.

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.