MỘT DẠNG LƯỢC ĐỒ CHỮ KÝ XÂY DỰNG TRÊN BÀI TOÁN PHÂN TÍCH SỐ VÀ BÀI TOÁN KHAI CĂN

Developing a new type of digital signature scheme based on integer factorization and finding root problem

Hoàng Thị Mai [*], Lưu Hồng Dũng [**]

Bài báo đề xuất một dạng lược đồ chữ ký số mới được xây dựng trên tính khó giải của bài toán phân tích một số nguyên lớn ra các thừa số nguyên tố và bài toán khai căn trên vành $Z_{n=p.q}$, ở đây: p, q là các số nguyên tố lớn. Từ dạng lược đồ mới đề xuất có thể phát triển các lược đồ chữ ký có mức độ an toàn cao cho các ứng dụng trong thực tế.

Từ khoá: Digital Signature, Digital Signature Schema, Integer Factorization Problem.

1. Đặt vấn đề

Phát triển các lược đồ chữ ký số với mục đích nâng cao mức độ an toàn cho thuật toán là một hướng nghiên cứu được nhiều người quan tâm. Trong [1-7] các tác giả đã đề xuất một số lược đồ chữ ký xây dựng trên đồng thời 2 bài toán khó. Những phân tích, đánh giá trong [8,9] cho thấy hướng nghiên cứu này đã phần nào giải quyết được yêu cầu đặt ra về độ an toàn cho các lược đồ chữ ký số.

Trong bài báo này, nhóm tác giả tiếp tục đề xuất xây dựng một dạng lược đồ chữ ký số mới dựa trên tính khó của 2 bài toán phân tích một số nguyên lớn ra các thừa số nguyên tố (*Bài toán phân tích số*) và bài toán khai căn trên vành $Z_{n=p.q}$, ở đây: p, q là các số nguyên tố lớn (*Bài toán khai căn*). Ưu điểm của dạng lược đồ mới đề xuất là từ đó có thể phát triển được nhiều lược đồ chữ ký có mức độ an toàn cao cho các ứng dụng trong thực tế.

2. Xây dựng lược đồ chữ ký dựa trên bài toán phân tích số và bài toán khai căn

2.1 Bài toán phân tích số

Bài toán phân tích số được phát biểu như sau: *Cho số* $n \in N$, *hãy tìm biểu diễn:* $n = p_1^{e_1}.p_2^{e_2}...p_k^{e_k}$, *với* $e_i \geq 1$ *và* p_i *là các số nguyên tố.*

Một trường hợp riêng của Bài toán phân tích số được ứng dụng trong xây dựng hệ mật RSA được phát biểu như sau:

- Cho p, q là 2 số nguyên tố lớn và mạnh;

[*] Đại học Thủ đô
[**] Học viện KTQS

- Từ p và q dễ dàng tính được: $n = p \times q$;

- Từ n rất khó tìm được p và q.

Trong hệ mật RSA [10], bài toán phân tích số được sử dụng làm cơ sở để hình thành cặp khóa công khai (e)/bí mật (d) cho mỗi thực thể ký. Với việc giữ bí mật các tham số $\{p,q\}$ thì khả năng tính được khóa mật (d) từ khóa công khai (e) và *modulo n* là rất khó thực hiện, nếu $\{p,q\}$ được chọn đủ lớn và mạnh [11,12]. Hiện tại, bài toán trên vẫn được coi là bài toán khó [13-15] do chưa có giải thuật thời gian đa thức cho nó và hệ mật RSA là một chứng minh thực tế cho tính khó giải của bài toán này. Ở dạng lược đồ mới đề xuất, tham số: $\phi(n) = (p-1) \times (q-1)$ được sử dụng như khóa bí mật thứ nhất trong việc hình thành chữ ký. Việc giữ bí mật cho tham số này cũng hoàn toàn phụ thuộc vào mức độ khó giải của bài toán nêu trên. Trong ứng dụng thực tế, các tham số $\{p,q\}$ có thể chọn theo Chuẩn X9.31 [11] hay FIPS 186-3 [12] của Hoa Kỳ cho hệ mật RSA như sau:

Chuẩn X9.31.

Theo X9.31, tiêu chuẩn đối với các tham số $\{p,q\}$ của hệ mật RSA bao gồm:

- Độ dài modulo n (*nlen*) là: 1024+256s ($s \geq 0$).
- $\sqrt{2} \times 2^{511+128s} \leq p, q \leq 2^{511+128s}$ ($s \geq 0$).
- $|p - q| > 2^{412+128s}$ ($s \geq 0$).
- Các ước nguyên tố của $p \pm 1$ và $q \pm 1$ (các số nguyên tố bổ trợ), ký hiệu là: p_1, p_2 và: q_1, q_2 phải thỏa mãn các thông số kỹ thuật được cho trong Bảng 1.1 dưới đây:

Bảng 1.1: Tiêu chuẩn an toàn đối với các số nguyên tố bổ trợ.

nlen	*Độ dài tối thiểu của p_1, p_2 và q_1, q_2*	*Độ dài tối đa của p_1, p_2 và q_1, q_2*
1024 + 256.s	> 100 bit	≤ 120 bit

Chuẩn FIPS 186-3.

Theo FIPS 186-3, tiêu chuẩn đối với các tham số $\{p,q\}$ của hệ mật RSA bao gồm:

- $\sqrt{2} \times 2^{511+128s} \leq p, q \leq 2^{511+128s}$ ($s \geq 0$).
- $|p - q| > 2^{\left(\frac{nlen}{2}\right)-100}$.
- Các ước nguyên tố của $p \pm 1$ và $q \pm 1$ (các số nguyên tố bổ trợ), ký hiệu là: p_1, p_2 và: q_1, q_2 phải thỏa mãn các thông số kỹ thuật được cho trong Bảng 1.2 dưới đây:

Bảng 1.2: Tiêu chuẩn an toàn đối với các số nguyên tố bổ trợ.

Độ dài của modulo n (nlen)	*Độ dài tối thiểu của p_1, p_2, q_1, q_2*	*Độ dài tối đa của len(p_1) + len(p_2) và len(q_1) + len(q_2)*	
		Các số nguyên tố xác xuất	*Các số nguyên tố chứng minh được*
1024 bit	> 100 bit	< 496 bit	< 239 bit
2048 bit	> 140 bit	< 1007 bit	< 494 bit
3072 bit	> 170 bit	< 1518 bit	< 750 bit

2.2 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 $RSA_{(n,t)}$ (1.1) 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 (1.2) như sau:

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

Ở dạng lược đồ chữ ký mới đề xuất, mỗi thành viên U của hệ thống tự chọn cho mình bộ tham số $\{n,t\}$ và khóa bí mật x thỏa mãn: $1 < x < n$, theo (1.3) tính và công khai tham số:

$$y = x^t \bmod n \tag{1.3}$$

Tương tự như *Bài toán phân tích số*, bài toán $RSA_{(n,t)}$ cũng được sử dụng để xây dựng nên hệ mật RSA và nó là yếu tố quyết định tới độ an toàn xét theo khả chống giả mạo chữ ký của hệ RSA. Cụ thể, với công thức hình thành chữ ký S từ khóa bí mật d của đối tượng ký và bản tin cần ký M: $S = m^d \bmod n$, ở đây m là giá trị đại diện của bản tin M và H(.) là hàm băm, có thể suy ra: $m = S^e \bmod n$, dẫn đến: $S = \sqrt[e]{m} \bmod n$. Như vậy, có thể thấy rằng nếu việc tính: $\sqrt[e]{m} \bmod n$ là khả thi trong các ứng dụng thực tế thì một đối tượng bất kỳ hoàn toàn có thể tạo được chữ ký S tương ứng với bản tin M bằng cách tính căn bậc e giá trị đại diện (m) của bản tin này mà không cần biết khóa bí mật

của đối tượng ký. Tuy nhiên, việc thuật toán chữ ký số RSA vẫn được sử dụng rộng rãi trong thực tế như hiện nay là một minh chứng cho tính khó giải của bài toán $RSA_{(n,t)}$.

2.3 Xây dựng lược đồ dạng tổng quát

Dạng lược đồ mới đề xuất ở đây xây dựng trên cơ sở tính khó giải của 2 bài toán phân tích số và bài toán khai căn nói trên, và được thiết kế theo dạng lược đồ sinh chữ ký 2 thành phần tương tự như DSA trong chuẩn chữ ký số của Mỹ (DSS) hay GOST R34.10-94 của Liên bang Nga, như sau:

Giả sử khóa bí mật của người ký là x và khóa công khai tương ứng là: $y = x^t \bmod n$, thành phần thứ nhất của chữ ký lên bản tin M là S và S được tính từ một giá trị u theo công thức:

$$S = u^t \bmod n \tag{2.1}$$

ở đây: $n = p \times q$, với p, q là 2 số nguyên tố phân biệt và số mũ t được chọn thỏa mãn:

$$1 < t < \phi(n)$$

Giả sử thành phần thứ hai của chữ ký là Z và Z được tính từ một giá trị v theo công thức:

$$Z = v^t \bmod n \tag{2.2}$$

Giả thiết rằng:

$$f(S,Z) \equiv k^t \bmod n \tag{2.3}$$

với $f(S,Z)$ là hàm của S, Z và k được chọn ngẫu nhiên trong khoảng $(1,\phi(n))$.

Ta cũng giả thiết phương trình kiểm tra của lược đồ có dạng:

$$Z^{f_1(M,f(S,Z))} \equiv S^{f_2(M,f(S,Z))} \times y^{f_3(M,f(S,Z))} \bmod n$$

Hàm $f(S,Z)$ có thể được lựa chọn khác nhau trong các trường hợp cụ thể, như: $f(S,Z) = S \times Z^{-1}$, $f(S,Z) = S^{-1} \times Z$, $f(S,Z) = S \times Z^2$, $f(S,Z) = S^2 \times Z$,... Xét cho trường hợp: $f(S,Z) = S \times Z \bmod n$ và $k^t \bmod n = R$. Khi đó từ (2.1), (2.2) và (2.3) ta có: $f(S,Z) = R$, nên có thể đưa phương trình kiểm tra về dạng:

$$Z^{f_1(M,R)} \equiv S^{f_2(M,R)} \times y^{f_3(M,R)} \bmod n \tag{2.4}$$

ở đây: $f_1(M,R)$, $f_2(M,R)$, $f_3(M,R)$ là hàm của M và R. Với: $R = k^t \bmod n$

Vấn đề đặt ra ở đây là cần tìm $\{u,v\}$ sao cho $\{S,Z\}$ thỏa mãn (2.3) và (2.4).

Từ (2.1), (2.2) và (2.3) ta có:

$$u \times v \bmod n = k \tag{2.5}$$

Từ (2.1), (2.2) và (2.4) ta có:

$$v^{f_1(M,R)} \equiv u^{f_2(M,R)} \times x^{f_3(M,R)} \bmod n \tag{2.6}$$

Từ (2.6) suy ra:

$$v = u^{f_1(M,R)^{-1}.f_2(M,R)} \times x^{f_1(M,R)^{-1}.f_3(M,R)} \bmod n \tag{2.7}$$

Từ (2.5) và (2.7) ta có:

$$u \times u^{f_1(M,R)^{-1}.f_2(M,R)} \times x^{f_1(M,R)^{-1}.f_3(M,R)} \bmod n = k$$

hay:

$$u^{f_1(M,R)^{-1}.f_2(M,R)+1} \times x^{f_1(M,R)^{-1}.f_3(M,R)} \bmod n = k$$

dẫn đến:

$$u = \left(k \times x^{-f_1(M,R)^{-1}.f_3(M,R)}\right)^{[f_1(M,R)^{-1}.f_2(M,R)+1]^{-1}} \bmod n \qquad (2.8)$$

và:

$$v = \left(k \times x^{-f_1(M,R)^{-1}.f_3(M,R)}\right)^{[f_1(M,R)^{-1}.f_2(M,R)+1]^{-1}.f_1(M,R)^{-1}.f_2(M,R)} \times x^{f_1(M,R)^{-1}.f_3(M,R)} \bmod n \qquad (2.9)$$

Từ (2.1) và (2.8) ta có công thức tính thành phần thứ nhất của chữ ký:

$$S = \left(k \times x^{-f_1(M,R)^{-1}.f_3(M,R)}\right)^{[f_1(M,R)^{-1}.f_2(M,R)+1]^{-1}.t} \bmod n \qquad (2.10)$$

Từ (2.2) và (2.9), công thức tính thành phần thứ hai của chữ ký sẽ có dạng:

$$Z = \left(k \times x^{-f_1(M,R)^{-1}.f_3(M,R)}\right)^{[f_1(M,R)^{-1}.f_2(M,R)+1]^{-1}.f_1(M,R)^{-1}.f_2(M,R).t} \times x^{f_1(M,R)^{-1}.f_3(M,R).t} \bmod n$$

Cũng có thể chọn v làm thành phần thứ hai của chữ ký, khi đó cặp (v,S) sẽ là chữ ký lên bản tin M và phương trình kiểm tra khi đó sẽ có dạng:

$$v^{f_1(M,f^*(v,S)).t} \equiv S^{f_2(M,f^*(v,S))} \times y^{f_3(M,f^*(v,S))} \bmod n$$

Ở đây: $f^*(v,S)$ là hàm của v, S và: $f^*(v,S) = f(S,Z) = R$.

Từ những phân tích thiết kế trên đây, có thể khái quát các thuật toán hình thành tham số, thuật toán hình thành và kiểm tra chữ ký của lược đồ dạng tổng quát tương ứng với trường hợp $f(S,Z) = S \times Z \bmod n$ như được chỉ ra ở các Bảng 2.1, Bảng 2.2 và Bảng 2.3 dưới đây.

a) Phương pháp hình thành tham số

Bảng 2.1:

Input: p, q – các số nguyên tố lớn, x – khóa bí mật

Output: n, t, y, $\phi(n)$.

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

[2]. $\phi(n) \leftarrow (p-1) \times (q-1)$

[3]. **select** t: $1 < t < \phi(n)$

[4]. **select** x: $1 < x < n$ và $\gcd(x,n) = 1$

[5]. $y \leftarrow x^t \bmod n$ (2.11)

[6]. **return** $\{n, t, y, \phi(n)\}$

Chú thích:

i) $\{n, t, y\}$: các tham số công khai.

ii) $\{x, \phi(n)\}$: các tham số bí mật.

b) Phương pháp hình thành chữ ký

Bảng 2.2:

Input: n, t, x, $\phi(n)$, M – Bản tin được ký bởi đối tượng **U**.

Output: (v,S).

[1]. **select** k: $1 < k < n$

[2]. $R \leftarrow k^t \bmod n$

[3]. **if** $(\gcd((f_1(M,R),\phi(n)) \neq 1$ **OR**

$\gcd((f_1(M,R)^{-1} \times f_2(M,R)+1),\phi(n)) \neq 1)$ **then goto** [1].

[4]. $u \leftarrow \left(k \times x^{-f_1(M,R)^{-1}.f_3(M,R)}\right)^{[f_1(M,R)^{-1}.f_2(M,R)+1]^{-1}} \bmod n$

[5]. $v \leftarrow u^{f_1(M,R)^{-1}.f_2(M,R)} \times x^{f_1(M,R)^{-1}.f_3(M,R)} \bmod n$

[6]. $S \leftarrow u^t \bmod n$

[7]. **return** (v,S)

Chú thích:

U: đối tượng ký và là chủ thể của các tham số $\{n,t,x,y,\phi(n)\}$.

Nhận xét:

Trong các bước [4] và [5] của *Phương pháp hình thành chữ ký* (Bảng 1.2), theo định lý Euler thì việc tính: $f_1(M,R)^{-1}$ và: $[f_1(M,R)^{-1}.f2(M,R)+1]^{-1}$ thực chất là tính: $f_1(M,R)^{-1} \bmod \phi(n)$ và: $[f_1(M,R)^{-1}.f2(M,R)+1]^{-1} \bmod \phi(n)$. Như vậy, ở đây $\phi(n)$ có vai trò tương tự như khóa bí mật x trong việc hình thành chữ ký. Từ đó cho thấy lược đồ dạng tổng quát được xây dựng trên đồng thời 2 bài toán khai căn và phân tích số. Hơn nữa, cả 2 tham số x và $\phi(n)$ đều được sử dụng như khóa bí mật trong thuật toán hình thành chữ ký.

c) Phương pháp kiểm tra chữ ký

Bảng 2.3:

Input: n, t, y, M – Bản tin cần thẩm tra, (v,S) – Chữ ký của **U** lên M.

Output: (v,S) = *true* / *false*.

[1]. $A \leftarrow v^{f_1(M,f^*(v,S)).t} \bmod n$ (2.12)

---

[2]. $B \leftarrow S^{f_2(M,f^*(v,S))} \times y^{f_3(M,f^*(v,S))} \bmod n$ (2.13)

[3]. **if** ($A = B$) **then** {**return** *true* ;}

else {**return** *false* ;}

Chú thích:

i) **U**: đối tượng là chủ thể của cặp tham số $\{n,t\}$.

ii) (v,s) = *true*: chữ ký hợp lệ, M được khẳng định về nguồn gốc và tính toàn vẹn.

iii) (v,s) = *false*: chữ ký không hợp lệ, M không được công nhận về nguồn gốc và tính toàn vẹn.

d) Tính đúng đắn của lược đồ dạng tổng quát

Tính đúng đắn của lược đồ dạng tổng quát là sự phù hợp của phương pháp kiểm tra chữ ký với phương pháp hình thành các tham số hệ thống và phương pháp hình thành chữ ký. Điều cần chứng minh ở đây là: cho p, q là số nguyên tố, $n = p \times q$, $\phi(n) = (p-1) \times (q-1)$, $1 < t < \phi(n)$, $1 < k, x < n$, $\gcd(x,n) = 1$, $R = k^t \bmod n$, $y = x^t \bmod n$, $\gcd((f_1(M,R), \phi(n)) = 1$, $\gcd((f_1(M,R)^{-1}.f_2(M,R)+1), \phi(n)) = 1$, $u = \left(k \times x^{-f_1(M,R)^{-1}.f_3(M,R)}\right)^{[f_1(M,R)^{-1}.f_2(M,R)+1]^{-1}} \bmod n$, $v = u^{f_1(M,R)^{-1}.f_2(M,R)} \times x^{f_1(M,R)^{-1}.f_3(M,R)} \bmod n$, $S = u^t \bmod n$. Nếu: $A = v^{f_1(M,f^*(v,S)).t} \bmod n$, $B = S^{f_2(M,f^*(v,S))} \times y^{f_3(M,f^*(v,S))} \bmod n$ với: $f^*(v,S) = R$ thì: $A = B$.

Có thể chứng minh tính đúng đắn của dạng lược đồ này như sau:

Từ (2.9) và (2.12) ta có:

$$\begin{aligned} A &= v^{f_1(M,f^*(v,S)).t} \bmod n = v^{f_1(M,R).t} \bmod n \\ &= \left(k \times x^{-f_1(M,R)^{-1}.f_3(M,R)}\right)^{[f_1(M,R)^{-1}.f_2(M,R)+1]^{-1}.f_1(M,R)^{-1}.f_2(M,R).f_1(M,R).t} \times \\ &\times x^{f_1(M,R)^{-1}.f_3(M,R).f_1(M,R).t} \bmod n \\ &= \left(k \times x^{-f_1(M,R).f_3(M,R)}\right)^{[f_1(M,R)^{-1}.f_2(M,R)+1]^{-1}.f_2(M,R).t} \times x^{f_3(M,R).t} \bmod n \end{aligned} \quad (2.14)$$

Từ (2.10) và (2.13) ta lại có:

$$\begin{aligned} B &= S^{f_2(M,f^*(v,S))} \times y^{f_3(M,f^*(v,S))} \bmod n = S^{f_2(M,R)} \times Y^{f_3(M,R)} \bmod n \\ &= \left(u^t \bmod n\right)^{f_2(M,R)} \times \left(x^t \bmod n\right)^{f_3(M,R)} \bmod n \\ &= \left(k \times x^{-f_1(M,R)^{-1}.f_3(M,R)}\right)^{[f_1(M,R)^{-1}.f_2(M,R)+1]^{-1}.f_2(M,R).t} \times x^{f_3(M,R).t} \bmod n \end{aligned} \quad (2.15)$$

Từ (2.14) và (2.15) suy ra: $A = B$

Đây là điều cần chứng minh.

3. Một lược đồ chữ ký phát triển từ lược đồ dạng tổng quát

3.1 Lược đồ LD 15.9-01

Lược đồ chữ ký, ký hiệu LD 15.9-01, được phát triển từ dạng tổng quát với các lựa chọn: $f_1(M,R)=1$, $f_2(M,R)=R$ và $f_3(M,R)=H(M)$, ở đây *H(.)* là hàm băm và H(M) là giá trị đại diện của bản tin M. Các thuật toán hình thành và kiểm tra chữ ký của lược đồ được mô tả trong các Bảng 3.1 và Bảng 3.2 dưới đây, còn thuật toán hình thành tham số và khóa là như ở lược đồ dạng tổng quát.

a) Thuật toán hình thành chữ ký

Bảng 3.1:

Input: *n*, *t*, *x*, *ϕ(n), M* – Bản tin được ký bởi đối tượng **U**.
Output: (*v*,S) – chữ ký của **U** lên M.

[1]. $E \leftarrow H(M)$
[2]. **select** k: $1 < k < n$
[3]. $R \leftarrow k^t \bmod n$ (3.1)
[4]. **if** $\gcd((R+1),\phi(n)) \neq 1$ **then goto** [2]
[5]. $z \leftarrow (R+1)^{-1} \bmod \phi(n)$
[6]. $u \leftarrow \left(k \times x^{-E}\right)^z \bmod n$ (3.2)
[7]. $v \leftarrow u^R \times x^E \bmod n$ (3.3)
[8]. $S \leftarrow u^t \bmod n$ (3.4)
[9]. **return** (*v*,*S*)

b) Thuật toán kiểm tra chữ ký

Bảng 3.2:

Input: *n*, *t*, *y*, *M* – Bản tin cần thẩm tra, (*v*,*S*) – Chữ ký của **U** lên M.
Output: (*v*,*S*) = *true* / *false*.

[1]. $E \leftarrow H(M)$ (3.5)
[2]. $A \leftarrow v^t \bmod n$ (3.6)
[3]. $B \leftarrow S^{A.S \bmod n} \times y^E \bmod n$ (3.7)
[4]. **if** ($A = B$) **then** {**return** *true* }
else {**return** *false* }

3.2 Tính đúng đắn của lược đồ LD 15.9-01

Điều cần chứng minh ở đây là: Cho *p*, *q* là 2 số nguyên tố phân biệt, $n = p \times q$, $\phi(n) = (p-1) \times (q-1)$, $H: \{0,1\}^* \mapsto Z_m$, $m < n$, $1 < t < \phi(n)$, $1 < k, x < n$, $\gcd(x,n) = 1$, $y = x^t \bmod n$, $R = k^t \bmod n$, $E = H(M)$, $z = (R+1)^{-1} \bmod \phi(n)$, $u = \left(k \times x^{-E}\right)^z \bmod n$, $v = u^R \times x^E \bmod n$, $S = u^t \bmod n$. Nếu: $A = v^t \bmod n$, $B = S^{A.S \bmod n} \times y^E \bmod n$ thì: $A = B$.

Tính đúng đắn của lược đồ mới đề xuất được chứng minh như sau:

Từ (3.2), (3.3) và (3.6) ta có:

$$\begin{aligned} A &= v^t \bmod n = \left(u^R \times x^E \bmod n\right)^t \bmod n = u^{R.t} \times x^{E.t} \bmod n \\ &= \left(\left(k \times x^{-E}\right)^Z \bmod n\right)^{R.t} \times x^{E.t} \bmod n = \left(k \times x^{-E}\right)^{[R+1]^{-1}.R.t} \times x^{E.t} \bmod n \end{aligned} \quad (3.8)$$

Từ (2.11), (3.2), (3.4), (3.5) và (3.7) ta lại có:

$$\begin{aligned} B &= S^{A.S \bmod n} \times y^E \bmod n = \left(u^t \bmod n\right)^{A.S \bmod n} \times \left(x^t \bmod n\right)^E \bmod n \\ &= u^{(A.S \bmod n).t} \times x^{E.t} \bmod n = u^{\left(\left(v^t \bmod n\right).\left(u^t \bmod n\right) \bmod n\right).t} \times x^{E.t} \bmod n \\ &= u^{\left(v^t.u^t \bmod n\right).t} \times x^{E.t} \bmod n = u^{R.t} \times e^{E.t} \bmod n \\ &= \left(\left(k \times x^{-E}\right)^z \bmod n\right)^{R.t} \times x^{E.t} \bmod n = \left(k \times x^{-E}\right)^{[R+1]^{-1}.R.t} \times x^{E.t} \bmod n \end{aligned} \quad (3.9)$$

Từ (3.8) và (3.9) suy ra: $A = B$

Đây là điều cần chứng minh.

3.2 Mức độ an toàn của lược đồ LD 15.9-01

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

a) Chống tấn công làm lộ khóa mật

Ở dạng lược đồ mới đề xuất, 2 tham số *x* và $\phi(n)$ cùng được sử dụng làm khóa bí mật để hình thành chữ ký. Vì thế, lược đồ LD 15.9-01 chỉ bị phá vỡ nếu cả *x* và $\phi(n)$ cùng bị lộ, nói cách khác là kẻ tấn công phải giải được đồng thời 2 bài toán phân tích số và khai căn. Do đó, mức độ an toàn của lược đồ mới đề xuất xét theo khả năng chống tấn công làm lộ khóa mật được đánh giá bằng mức độ khó của hai bài toán phân tích số và khai căn. Từ đó cho thấy điều kiện tiên quyết để các lược đồ dạng này an toàn là cặp {*p*,*q*} phải được chọn đủ lớn và mạnh các bài toán nêu trên là khó giải.

b) Chống tấn công giả mạo chữ ký

Từ thuật toán kiểm tra (Bảng 3.2) của lược đồ LD 15.9-01 cho thấy, một cặp chữ ký (v,S) giả mạo sẽ được công nhận là hợp lệ với một bản tin M nếu thỏa mãn điều kiện:

$v^t \equiv S^{(v^t.S) \bmod n} \times y^E \bmod n$, ở đây: $E = H(M)$

Từ các kết quả nghiên cứu đã được công bố, có thể thấy rằng đây là một dạng bài toán khó chưa có lời giải nếu {*p*,*q*} được chọn đủ lớn để phương pháp vét cạn là không khả thi trong các ứng dụng thực tế.

4. Kết luận

Bài báo đề xuất một dạng lược đồ chữ ký số mới được xây dựng dựa trên bài toán phân tích số và bài toán khai căn kết hợp nhằm nâng cao mức độ an toàn cho các thuật toán phát triển từ dạng lược đồ chữ ký này. Có thể thấy rằng, mức độ an toàn của dạng lược đồ mới đề xuất được đánh giá bằng mức độ khó của việc giải đồng thời 2 bài toán nói trên. Từ đó cho thấy dạng lược đồ mới này có thể sử dụng cho các ứng

dụng thực tế nếu các tham số hệ thống $\{p,q\}$, các hàm $f(S,Z)$, $f_1(M,R)$, $f_2(M,R)$, $f_3(M,R)$ và các phương trình kiểm tra tính hợp lệ của chữ ký được lựa chọn hợp lý.

TÀI LIỆU THAM KHẢO

[1] Eddie Shahrie Ismail, Tahat N.M.F., Rokiah. R. Ahmad, "*A New Digital Signature Scheme Based on Factoring and Discrete Logarithms"*, Journal of Mathematics and Statistics 04/2008; 12(3). DOI: 10.3844/jmssp.2008.222.225 Source: DOAJ.

[2] Swati Verma1, Birendra Kumar Sharma, "*A New Digital Signature Scheme Based on Two Hard Problems"*, International Journal of Pure and Applied Sciences and Technology ISSN 2229 – 6107, Int. J. Pure Appl. Sci. Technol., 5(2) (2011), pp. 55-59

[3] Sushila Vishnoi , Vishal Shrivastava, "*A new Digital Signature Algorithm based on Factorization and Discrete Logarithm problem"*, International Journal of Computer Trends and Technology- volume3Issue4-2012.

[4] Shimin Wei, "*Digital Signature Scheme Based on Two Hard Problems"*, IJCSNS International Journal of Computer Science and Network Security, VOL.7 No.12, December 2007.

[5] Qin Yanlin , Wu Xiaoping, " *New Digital Signature Scheme Based on both ECDLP and IFP"*, Computer Science and Information Technology, 2009. ICCSIT 2009. 2nd IEEE International Conference on, 8-11 Aug. 2009, E-ISBN : 978-1-4244-4520-2, pp 348 - 351

[6] Q. X. WU, Y. X. Yang and Z. M. HU, "*New signature schemes based on discrete logarithms and factoring*," Journal of Beijing University of Posts and Telecommunications.Beijing, vol. 24, pp. 61-65, January 2001.

[7] Z. Y. Shen and X. Y. Yu, "*Digital signature scheme based on discrete logarithms and factoring*," Information Technology.Harbin, vol. 28,pp. 21-22,June 2004.

[8] J. W. Ren and D. D. Lin, "*Analysis and Improvement of a Digital Signature Scheme Based on Factoring and Discrete Logarithm*," Computer Engineering and Applications.vol 41,pp. 132-133,July 2005.

[9] X. L. Dong, Z. F. Cao and X. H. Li, "*Cryptanalysis of Two Signature Schemes Based on Two Hard Problems*," Journal of Shanghai Jiao Tong University.Shanghai,vol. 40,pp. 1174-1177,July 2006.

[10] R.L. Rivest, A. Shamir, and L. Adleman, *"A method for Obtaining digital signatures and public key cryptosystems*", Commun. of the ACM, 21:120-126,1978.

[11] Burt Kaliski, *"RSA Digital Signature Standards",* RSA Laboratories 23rd National Information Systems Security Conference, October 16-19,2000.

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

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

[14] D.R Stinson, "*Cryptography: Theory and Practice"*, CRC Press 1995.

[15] Wenbo Mao, "*Modern Cryptography: Theory and Practice"*, Prentice Hall PTR, 2003.