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

Lưu Hồng Dũng[1], Hoàng Thị Mai[2], Nguyễn Hữu Mộng[3]

[1]Khoa Công nghệ Thông tin, Học viện Kỹ thuật Quân sự

[2] Khoa Công nghệ Thông tin, Đại học Thủ đô Hà Nội

[3] Khoa Công nghệ Thông tin, Học viện Kỹ thuật Quân sự

luuhongdung@hotmail.com, htmai@cdsphanoi.edu.vn, nghm06@yahoo.com

TÓM TẮT— *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. Từ dạng lược đồ mới đề xuất có thể phát triển các lược đồ chữ ký có khả năng ứng dụng trong thực tế*

Từ khóa— *Digital Signature, Digital Signature Schema, Integer Factorization Problem, Prime Factorization*

I. ĐẶT VẤN ĐỀ

Nghiên cứu phát triển các lược đồ chữ ký số là một trong những nội dung nghiên cứu khoa học quan trọng, mang tính thời sự của an toàn thông tin. Hầu hết các lược đồ chữ ký số hiện nay đều dựa trên tính khó của bài toán: phân tích một số nguyên lớn ra các thừa số nguyên tố, bài toán khai căn và bài toán logarit rời rạc trong modulo hợp số. Thuật toán chữ ký số đầu tiên (RSA) được đề xuất và công bố bởi Ron Rivest, Adi Shamir và Len Adleman [1] vào năm 1977 tại Viện Công nghệ Massachusetts (MIT) Hoa Kỳ. Thuật toán chữ ký số này được xây dựng dựa trên tính khó của bài toán phân tích một số nguyên lớn ra các thừa số nguyên tố. Lược đồ Elgamal [17] gồm cả hệ mã và chữ ký số có độ an toàn dựa trên bài toán logarit rời rạc.

Trên nền tảng của bài toán phân tích số, có nhiều hướng nghiên cứu phát triển thuật toán chữ ký số RSA. [2] và [5] nghiên cứu việc sinh các tham số đầu vào cho thuật toán nhằm tăng mức độ an toàn của thuật toán, [6] nghiên cứu xác thực bản tin bằng chữ ký số RSA-PSS theo cách sử dụng hai thuật toán nền tảng là thuật toán mã hóa và kiểm tra EMSA-PSS cho bản tin và thuật toán tạo chữ ký RSA để xác thực bản tin.

Nhằm tăng độ an toàn cho các lược đồ chữ ký số, có một mạch nghiên cứu khác là xây dựng lược đồ chữ ký dựa trên nền tảng của hai bài toán: phân tích số và logarit rời rạc. Năm 1998, Shao [8] và Li-Xiao [9] đã đề xuất các lược đồ chữ ký số dạng này. Sau đó Lee [10] năm 2000 chứng minh rằng lược đồ chữ ký của Shao là không an toàn như báo cáo. Để khắc phục những nhược điểm của lược đồ chữ ký Shao, He [11] năm 2001 đề xuất một sơ đồ chữ ký số cũng dựa vào bài toán phân tích số nguyên và bài toán logarit rời rạc; sử dụng cùng modulo và một tập số mũ và các khóa bí mật. Vào năm 2002 Hung Min Sun [12] chỉ ra rằng các lược đồ đó chỉ dựa trên bài toán logarit rời rạc. Năm 2003, Wang, Lin và Chang [14] đề xuất một lược đồ chữ ký dựa trên cả hai bài toán khó và lược đồ này vẫn chưa bị đánh bại. Năm 2007, Wei [15] đưa ra hai lược đồ cải tiến từ hai lược đồ của Shao và Li-Xiao nhằm chống lại những tấn công vào hai lược đồ này. Năm 2009, Lin, Gun và Chen [16] cho rằng các lược đồ của Wei vẫn không an toàn do có thể giả mạo chữ ký hợp lệ của một thông điệp bằng cách sử dụng phương pháp của Pollard và Schnorr.

Theo một hướng nghiên cứu khác, [3] đề cập đến việc xây dựng một lược đồ chữ ký số trên cơ sở bài toán phân tích một số nguyên lớn ra các thừa số nguyên tố (bài toán phân tích số) kết hợp với bài toán khai căn trong modulo hợp số (bài toán khai căn). Tuy nhiên, do bài toán khai căn không có vai trò quyết định đến mức độ an toàn của lược đồ nên đã không được đề cập đến trong [3]. Bài báo này đề xuất một phương pháp xây dựng lược đồ chữ ký số theo cùng nguyên tắc đã được chỉ ra trong [3], nhưng phương pháp đề xuất ở đây được mô tả dưới dạng một lược đồ tổng quát từ đó cho phép triển khai ra các lược đồ chữ ký số khác nhau cho các ứng dụng thực tế. Hơn nữa, phương pháp đề xuất ở đây được xây dựng trên cơ sở bài toán phân tích số kết hợp với bài toán logarit rời rạc trong modulo hợp số nên cho phép tạo ra các lược đồ chữ ký có hiệu quả thực hiện (tốc độ, tài nguyên hệ thống) cao hơn lược đồ chữ ký được xây dựng trong [3]. Cũng tương tự như bài toán khai căn đối với lược đồ trong [3], bài toán logarit rời rạc ở đây cũng không có vai trò quyết định tới độ an toàn của các lược đồ xây dựng theo phương pháp mới đề xuất nên cũng sẽ không được đề cập ở đây.

II. XÂY DỰNG LƯỢC ĐỒ CHỮ KÝ DỰA TRÊN BÀI TOÁN PHÂN TÍCH SỐ

A. Bài toán phân tích một số nguyên lớn ra các thừa số nguyên tố

Bài toán phân tích số về cơ bản có thể 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 ei ≥1 và pi là các số nguyên tố.

Trong hệ mật RSA [1], 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 và có thể phát biểu như sau:

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

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

- Từ n rất khó tìm được p và q.

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 [4,7] .

Hiện tại, bài toán trên vẫn được coi là bài toán khó 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.

B. Xây dựng lược đồ dạng tổng quát

Dạng lược đồ mới đề xuất ở đây xây dựng trên cơ sở tính khó giải của bài toán phân tích số 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, bao gồm 2 dạng tổng quát như sau.

2.1 Dạng lược đồ thứ nhất

Giả sử có một văn bản cần ký là M và chữ ký số chứa hai thành phần là S và Z. Để hình thành chữ ký số ta chọn hai số nguyên tố lớn khác nhau, đủ mạnh là p, q và đặt $n = p \times q$, đồng thời chọn một số nguyên t bất kỳ thỏa mãn $1 < t < \phi(n)$ với $\phi(n)$ là hàm Ơle của n, tức là $\phi(n) = (p-1)\times(q-1)$

Giả sử thành phần thứ nhất S của chữ ký được tính từ một giá trị u trong khoảng $(1,n)$ theo công thức:

$$S = u^t \bmod n \qquad (1.1)$$

Thành phần thứ hai Z của chữ ký được tính từ một giá trị v trong khoảng $(1,n)$ theo công thức:

$$Z = v^t \bmod n \qquad (1.2)$$

Giả thiết rằng $f(S,Z) \equiv k^t \bmod n$ (1.3) với $f(S,Z)$ là hàm của S và Z với k được chọn ngẫu nhiên sao cho $1 < k < n$. Cũng giả thiết rằng phương trình kiểm tra của lược đồ có dạng: $Z^{f_1(M,f(S,Z))} \equiv S^{f_2(M,f(S,Z))} \bmod n$.

Xét cho một trường hợp cụ thể: $f(S,Z) = S \times R \bmod n$ và đặt $R = k^t \bmod n$. Khi đó từ (1.1), (1.2) và (1.3) ta có $f(S,Z) = R$, nên có thể đưa phương trình kiểm tra về dạng:

$$Z^{f_1(M,R)} \equiv S^{f_2(M,R)} \bmod n \qquad (1.4)$$

ở đây: $f_1(M,R)$, $f_2(M,R)$ là các hàm của M và R.

Vấn đề đặt ra ở đây là cần tìm {u,v} sao cho {S,Z} thỏa mãn (1.3) và (1.4).

Từ (1.1), (1.2) và (1.3) ta có:

$$u \times v \bmod n = k \qquad (1.5)$$

Từ (1.1), (1.2) và (1.4) ta có:

$$v^{f_1(M,R)} \equiv u^{f_2(M,R)} \bmod n \qquad (1.6)$$

Từ (1.6) suy ra:

$$v = u^{f_1(M,R)^{-1}.f_2(M,R)} \bmod n \qquad (1.7)$$

Từ (1.5) và (1.7) ta có:

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

hay:

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

dẫn đến:

$$u = k^{[f_1(M,R)^{-1}.f_2(M,R)+1]^{-1}} \bmod n \qquad (1.8)$$

và:

$$v = k^{[f_1(M,R)^{-1}.f_2(M,R)+1]^{-1}.f_1(M,R)^{-1}.f_2(M,R)} \bmod n \qquad (1.9)$$

Từ (1.1) và (1.8) ta có công thức tính thành phần thứ nhất của chữ ký:

$$S = k^{[f_1(M,R)^{-1}.f_2(M,R)+1]^{-1}.t} \bmod n \qquad (1.10)$$

Từ (1.2) và (1.9), công thức tính thành phần thứ hai của chữ ký sẽ có dạng:

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

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:

$$v^{f_1(M,R).t} \equiv S^{f_2(M,R)} \bmod n$$

Từ những phân tích thiết kế trên đây, có thể khái quát các phương pháp hình thành tham số, phương pháp hình thành và kiểm tra chữ ký của dạng lược đồ thứ nhất như được chỉ ra ở các Bảng 1.1, Bảng 1.2 và Bảng 1.3 dưới đây.

a) Phương pháp hình thành tham số

Bảng 1.1:

Input: p, q – các số nguyên tố lớn.

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

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

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

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

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

Chú ý:

i) $\{n, t\}$: các tham số công khai.

ii) $\phi(n)$: tham số bí mật.

Nhận xét:

Ở lược đồ mới đề xuất không sử dụng cặp khóa bí mật/công khai như ở các lược đồ chữ ký RSA, DSA,...

b) Phương pháp hình thành chữ ký

Bảng 1.2:

Input: n, t, $\phi(n)$, 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]. $u \leftarrow k^{[f_1(M,R)^{-1}.f_2(M,R)+1]^{-1}} \bmod n$

[6]. $v \leftarrow k^{[f_1(M,R)^{-1}.f_2(M,R)+1]^{-1}.f_1(M,R)^{-1}.f_2(M,R)} \bmod n$

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

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

Chú ý:

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

Nhận xét:

i) Thuật toán không sử dụng khóa bí mật trong việc hình thành chữ ký như ở các lược đồ chữ ký RSA, DSA,...

ii) Tham số $\phi(n)$ được sử dụng như khóa bí mật để hình thành chữ ký (v,s) của đối tượng **U** lên bản tin M.

c) Phương pháp kiểm tra chữ ký

Bảng 1.3:

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

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

[1]. $A \leftarrow v^{f_1(M,R).t} \bmod n$ (1.11)

[2]. $B \leftarrow S^{f_2(M,R)} \bmod n$ (1.12)

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

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

Chú ý:

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.

Nhận xét:

Tham số {n,t} được sử dụng như khóa công khai của đối tượng U để kiểm tra tính hợp lệ của chữ ký (v,s).

d) Tính đúng đắn của dạng lược đồ thứ nhất

Tính đúng đắn của dạng lược đồ thứ nhất 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, $n = p \times q$, $\phi(n) = (p-1) \times (q-1)$, $1 < t < \phi(n)$, $1 < k < n$, $R = k^t \bmod n$, $\gcd((f_1(M,R), \phi(n)) = 1$, $\gcd((f_1(M,R)^{-1}.f_2(M,R)+1), \phi(n)) = 1$, $u = k^{[f_1(M,R)^{-1}.f_2(M,R)+1]^{-1}} \bmod n$, $v = k^{[f_1(M,R)^{-1}.f_2(M,R)+1]^{-1}.f_1(M,R)^{-1}.f_2(M,R)} \bmod n$, $S = u^t \bmod n$. Nếu: $A = v^{f_1(M,R).t} \bmod n$, $B = S^{f_2(M,R)} \bmod n$ thì: $A = B$.

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

Từ (1.9) và (1.11) ta có:

$$A = v^{f_1(M,R).t} \bmod n = k^{[f_1(M,R)^{-1}.f_2(M,R)+1]^{-1}.f_2(M,R).t} \bmod n \quad (1.13)$$

Từ (1.10) và (1.12) ta lại có:

$$B = S^{f_2(M,R)} \bmod n = k^{[f_1(M,R)^{-1}.f_2(M,R)+1]^{-1}.f_2(M,R).t} \bmod n \quad (1.14)$$

Từ (1.13) và (1.14) suy ra:

$A = B$

Đây là điều cần chứng minh.

2.2 Dạng lược đồ thứ hai

Phương pháp phân tích thiết kế áp dụng đối với dạng lược đồ thứ hai về cơ bản cũng tương tự như dạng lược đồ thứ nhất. Cũng giả sử rằng S là thành phần thứ nhất của chữ ký lên bản tin M và S được tính từ một giá trị u trong khoảng $(1, \phi(n))$ theo công thức:

$$S = g^u \bmod n \quad (2.1)$$

ở đây: $n = p \times q$, với p, q là 2 số nguyên tố phân biệt và: $1 < g < n$.

Thành phần thứ hai của chữ ký giả sử là Z được tính từ một giá trị v trong khoảng $(1, \phi(n))$ theo công thức:

$$Z = g^v \bmod n \quad (2.2)$$

Giả thiết rằng $f(S,Z) \equiv g^k \bmod n$ (2.3) với $f(S,Z)$ là hàm của S và Z với k được chọn ngẫu nhiên sao cho $1 < k < \phi(n)$. Cũng giả thiết rằng phương trình kiểm tra của lược đồ có dạng: $Z^{f_1(M,f(S,Z))} \equiv S^{f_2(M,f(S,Z))} \bmod n$.

Xét cho một trường hợp cụ thể: $f(S,Z) = S \times R \bmod n$ và đặt $R = g^k \bmod n$. 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:

$$Z^{f_1(M,R)} \equiv S^{f_2(M,R)} \bmod n \quad (2.4)$$

ở đây: $f_1(M,R)$, $f_2(M,R)$ là các hàm của M và R.

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:

$$(u+v) \bmod \phi(n) = k \quad (2.5)$$

Từ (2.1), (2.2) và (2.4) ta có:

$$v \times f_1(M,R) \equiv u \times f_2(M,R) \bmod \phi(n) \quad (2.6)$$

Từ (2.6) suy ra:

$$v = u \times f_1(M,R)^{-1} \times f_2(M,R) \bmod \phi(n) \quad (2.7)$$

Từ (2.5) và (2.7) ta có:

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

hay:

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

dẫn đến:

$$u = k \times [f_1(M,R)^{-1} \times f_2(M,R) + 1]^{-1} \bmod \phi(n) \quad (2.8)$$

và:

$$v = k \times [f_1(M,R)^{-1} \times f_2(M,R) + 1]^{-1} \times f_1(M,R)^{-1} \times f_2(M,R) \bmod \phi(n) \quad (2.9)$$

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

$$S = g^{k.[f_1(M,R)^{-1}.f_2(M,R)+1]^{-1} \bmod \phi(n)} \bmod n \quad (2.10)$$

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

$$Z = g^{k.[f_1(M,R)^{-1}.f_2(M,R)+1]^{-1}.f_1(M,R)^{-1}.f_2(M,R) \bmod \phi(n)} \bmod n$$

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:

$$g^{v.f_1(M,R)} \equiv S^{f_2(M,R)} \bmod n$$

Từ những phân tích thiết kế trên đây, có thể khái quát các phương pháp hình thành tham số, phương pháp hình thành và kiểm tra chữ ký của dạng lược đồ thứ hai 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.
Output: *n*, *g*, *ϕ(n)*.
[1]. $n \leftarrow p \times q$

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

[3]. **select** g: $1 < g < n$

[4]. **return** $\{n, g, \phi(n)\}$

Chú ý:

i) $\{n, g\}$: các tham số công khai.

ii) $\phi(n)$: tham số bí mật.

Nhận xét:

Ở lược đồ mới đề xuất không sử dụng cặp khóa bí mật/công khai như ở các lược đồ chữ ký RSA, DSA,...

b) Phương pháp hình thành chữ ký

Bảng 2.2:

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

Output: (v,s).

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

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

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

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

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

[5]. $v \leftarrow k.[f_1(M,R)^{-1}.f_2(M,R)+1]^{-1}.f_1(M,R)^{-1}.f_2(M,R) \bmod \phi(n)$

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

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

Chú ý:

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

Nhận xét:

i) Thuật toán không sử dụng khóa bí mật trong việc hình thành chữ ký như ở các lược đồ chữ ký RSA, DSA,...

ii) Tham số $\phi(n)$ được sử dụng như khóa bí mật để hình thành chữ ký (v,s) của đối tượng **U** lên bản tin M.

c) Phương pháp kiểm tra chữ ký

Bảng 2.3:

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

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

[1]. $A \leftarrow g^{v.f_1(M,R)} \bmod n$ (2.11)

[2]. $B \leftarrow S^{f_2(M,R)} \bmod n$ (2.12)

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

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

Chú ý:

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

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.

Nhận xét:

Tham số {n,g} được sử dụng như khóa công khai của đối tượng U để kiểm tra tính hợp lệ của chữ ký (v,s).

d) Tính đúng đắn của dạng lược đồ thứ hai

Điều cần chứng minh ở đây là: cho p, q là 2 số nguyên tố, $n = p \times q$, $\phi(n) = (p-1)\times(q-1)$, $1 < g < n$, $1 < k < \phi(n)$, $R = g^k \bmod n$, $\gcd((f_1(M,R),\phi(n)) = 1$, $\gcd((f_1(M,R)^{-1}.f_2(M,R)+1),\phi(n)) = 1$, $u = k.[f_1(M,R)^{-1}.f_2(M,R)+1]^{-1} \bmod \phi(n)$, $v = k.[f_1(M,R)^{-1}.f_2(M,R)+1]^{-1}.f_1(M,R)^{-1}.f_2(M,R) \bmod \phi(n)$, $S = g^u \bmod n$. Nếu: $A = g^{v.f_1(M,R)} \bmod n$, $B = S^{f_2(M,R)} \bmod n$ thì: $A = B$.

Tính đúng đắn của dạng lược đồ thứ hai có thể được chứng minh như sau:

Từ (2.9) và (2.11) ta có:

$$\begin{aligned} A &= g^{v.f_1(M,R)} \bmod n \\ &= g^{k.[f_1(M,R)^{-1}.f_2(M,R)+1]^{-1}.f_1(M,R)^{-1}.f_2(M,R).f_1(M,R)} \bmod n \\ &= g^{k.[f_1(M,R)^{-1}.f_2(M,R)+1]^{-1}.f_2(M,R)} \bmod n \end{aligned} \qquad (2.13)$$

Từ (2.10) và (2.12) ta lại có:

$$\begin{aligned} B &= S^{f_2(M,R)} \bmod n = g^{u.f_2(M,R)} \bmod n \\ &= g^{k.[f_1(M,R)^{-1}.f_2(M,R)+1]^{-1}.f_2(M,R)} \bmod n \end{aligned} \qquad (2.14)$$

Từ (2.13) và (2.14) suy ra:

$A = B$

Đây là điều cần chứng minh

2.3 Một số lược đồ chữ ký số được phát triển từ 2 lược đồ dạng tổng quát

Bằng việc lựa chọn các hàm $f_1(M,R)$ và $f_2(M,R)$ khác nhau, từ 2 dạng tổng quát đề xuất trên đây, có thể triển khai được một số lược đồ chữ ký số như sau.

a) Lược đồ thứ nhất LD-01

Lược đồ LD-01 được phát triển từ dạng tổng quát thứ nhất với các lựa chọn: $f_1(M,R) = 1$ và $f_2(M,R) = H(M)\times R$, ở đây H(.) là hàm băm và H(M) là giá trị đại diện của bản tin được ký M. Các thuật toán hình thành tham số, hình thành và kiểm tra chữ ký được mô tả trong các Bảng 3.1, Bảng 3.2 và Bảng 3.3 dưới đây.

a) Thuật toán hình thành tham số

Bảng 3.1:
Input: *p*, *q* – các số nguyên tố lớn.
Output: *n*, *t*, *H(.),ϕ(n)*.
[1]. $n \leftarrow p \times q$
[2]. $\phi(n) \leftarrow (p-1)\times(q-1)$
[3]. **select** $H: \{0,1\}^* \mapsto Z_m$, $m < n$
[4]. **select** t: $1 < t < \phi(n)$
[5]. **return** {*n*, *t*, *H(.),ϕ(n)*}

Chú ý:

i) *n*, *t*, *H(.)*: các tham số công khai.

ii) $\phi(n)$: tham số bí mật.

b) Thuật toán hình thành chữ ký

Bảng 3.2:

Input: n, t, $\phi(n)$, 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** $\gcd((E \times R + 1), \phi(n)) \neq 1$ **then goto** [2]

[5]. $w_1 \leftarrow (E \times R + 1)^{-1} \bmod \phi(n)$ (3.2)

[6]. $u \leftarrow k^{w_1} \bmod n$ (3.3)

[7]. $w_2 \leftarrow E \times R \bmod \phi(n)$ (3.4)

[8]. $v \leftarrow u^{w_2} \bmod n$ (3.5)

[9]. $S \leftarrow u^t \bmod n$ (3.6)

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

Chú ý:

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

Nhận xét:

Tham số $\phi(n)$ được sử dụng như khóa bí mật để hình thành chữ ký (v,S) của đối tượng **U** lên bản tin M.

c) Thuật toán kiểm tra chữ ký

Bảng 3.3:

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

[1]. $E \leftarrow H(M)$ (3.7)

[2]. $A \leftarrow v^t \bmod n$ (3.8)

[3]. $Z \leftarrow S \times A \bmod n$ (3.9)

[4]. $w \leftarrow E \times Z$ (3.10)

[5]. $B \leftarrow S^w \bmod n$ (3.11)

[6]. **if** ($A = B$) **then** {**return** *true* }
else {**return** *false* }

Chú ý:

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.

Nhận xét:

Tham số {n,t} được sử dụng như khóa công khai của U để kiểm tra tính hợp lệ của chữ ký (v,S).

d) Tính đúng đắn của lược đồ LD-01

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

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

Từ (3.6), (3.7), (3.8), (3.9) và (3.10) ta có:

$$w = E \times Z = E \times (S \times A \bmod n) = E \times \left(\left(u^t \bmod n\right) \times \left(v^t \bmod n\right) \bmod n \right)$$
$$= E \times \left(u^t \times v^t \bmod n\right) = E \times \left((u \times v)^t \bmod n\right) \quad (3.11)$$

Từ (3.1), (3.2), (3.3), (3.4), (3.5) và (3.11) ta có:

$$w = E\times\left((u\times v)^t \bmod n\right) = E\times\left(\left(k^{(E.R+1)^{-1}}\times k^{(E.R+1)^{-1}.E.R}\right)^t \bmod n\right)$$
$$= E\times\left(k^{(E.R+1)^{-1}.(E.R+1).t} \bmod n\right) = E\times\left(k^t \bmod n\right) = E\times R \qquad (3.12)$$

Từ (3.6) và (3.12), suy ra:

$$B = S^w \bmod n = \left(u^t \bmod n\right)^{E.R} \bmod n = u^{E.R.t} \bmod n \qquad (3.13)$$

Mặt khác, từ (3.4), (3.5) và (3.8) ta lại có :

$$A = v^t \bmod n = \left(u^{E.R} \bmod n\right)^t \bmod n = u^{E.R.t} \bmod n \qquad (3.14)$$

Từ (3.13) và (3.14), suy ra: $A = B$

Đây là điều cần chứng minh.

2.3.2 Lược đồ thứ hai LD-02

Lược đồ LD-02 được phát triển từ dạng lược đồ thứ hai với các lựa chọn: $f_1(M,R) = R$ và $f_2(M,R) = H(M)$. Các thuật toán hình thành tham số, hình thành và kiểm tra chữ ký được mô tả trong các Bảng 4.1, Bảng 4.2 và Bảng 4.3 dưới đây.

a) Phương pháp hình thành tham số

Bảng 4.1:

Input: p, q – các số nguyên tố lớn.

Output: n, g, $H(.)$,$\phi(n)$.

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

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

[3]. **select** g: $1 < g < n$

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

[5]. **return** $\{n, g, H(.),\phi(n)\}$

Chú ý:

i) $\{n, g\}$: các tham số công khai.

ii) $\phi(n)$: tham số bí mật.

b) Thuật toán hình thành chữ ký

Bảng 4.2:

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

Output: (v,S) – Chữ ký của **U** lên M.

[1]. $E = H(M)$

[2]. **select** k: $1 < k < \phi(n)$

[3]. $R \leftarrow g^k \bmod n$ (4.1)

[4]. **if** $(\gcd(R,\phi(n)) \neq 1$ **OR** $\gcd((R^{-1}\times E+1),\phi(n)) \neq 1)$ **then goto** [2]

[5]. $u \leftarrow k\times(R^{-1}\times E+1)^{-1} \bmod \phi(n)$ (4.2)

[6]. $v \leftarrow k\times(R^{-1}\times E+1)^{-1}\times R^{-1}\times E \bmod \phi(n)$ (4.3)

[7]. $S \leftarrow g^u \bmod n$ (4.4)

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

Chú ý:

U: đối tượng ký và là chủ thể của các tham số {n,g,ø(n)}.

Nhận xét:

Đối tượng U sử dụng tham số ø(n) như khóa bí mật để hình thành chữ ký (v,S) lên bản tin M.

c) Thuật toán kiểm tra chữ ký

Bảng 4.3:

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

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

[1]. $Z \leftarrow g^v \bmod n$ (4.5)

[2]. $w \leftarrow S \times Z \bmod n$ (4.6)

[3]. $A \leftarrow Z^w \bmod n$ (4.7)

[4]. $E = H(M)$ (4.8)

[5]. $B \leftarrow S^E \bmod n$ (4.9)

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

else {**return** *false* }

Chú ý:

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

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.

Nhận xét:

Tham số $\{n,g\}$ được sử dụng như khóa công khai của **U** để kiểm tra tính hợp lệ của chữ ký (v,S).

d) Tính đúng đắn của lược đồ LD-02

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

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

Từ (4.1), (4.2), (4.3), (4.4), (4.5) và (4.6) ta có:

$$\begin{aligned} w &= S \times Z \bmod n = (g^u \bmod n \times g^v \bmod n) \bmod n = g^{u+v} \bmod n \\ &= g^{k.[R^{-1}.E+1]^{-1} + k.[R^{-1}.E+1]^{-1}.R^{-1}.E} \bmod n = g^{k.[R^{-1}.E+1]^{-1}.(R^{-1}.E+1)} \bmod n \\ &= g^k \bmod n = R \end{aligned} \quad (4.10)$$

Từ (4.3), (4.5), (4.7) và (4.10) ta có:

$$\begin{aligned} A &= Z^w \bmod n = g^{v.R} \bmod n = g^{k.[R^{-1}.E+1]^{-1}.R^{-1}.E.R} \bmod n \\ &= g^{k.(R^{-1}.E+1)^{-1}.E} \bmod n \end{aligned} \quad (4.11)$$

Từ (4.4) và (4.9) ta lại có:

$$B = S^E \bmod n = g^{u.E} \bmod n$$
$$= g^{k.(R^{-1}.E+1)^{-1}.E} \bmod n \quad (4.12)$$

Từ (4.11) và (4.12) suy ra:

$$A = B$$

Đây là điều cần chứng minh.

2.4 Mức độ an toàn của các lược đồ mới đề xuất

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, tham số ø(n) được sử dụng làm khóa bí mật để hình thành chữ ký. Do đó, các lược đồ chữ ký được xây dựng theo phương pháp này sẽ bị phá vỡ nếu kẻ tấn công tìm được ø(n), tức là tìm được (p-1) và (q-1). Điều này cũng có nghĩa là muốn phá vỡ được các lược đồ theo dạng mới đề xuất, kẻ tấn công phải tìm được hai số nguyên tố p và q sao cho n= p×q với n cho trước. Đây là bài toán phân tích số đã được trình bày trong phần A. Như vậy, 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 bài toán phân tích số. 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 để bài toán phân tích số là khó giải..

b) Chống tấn công giả mạo chữ ký

Từ thuật toán kiểm tra (Bảng 3.3) của lược đồ LD-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:

$$A = S^{E.(S.A \bmod n)} \bmod n \text{, ở đây: } A = v^t \bmod n \text{ và } E = H(M) \quad (5.1)$$

Tương tự, ở lược đồ LD-02 nếu có thể chọn được một cặp (v,S) thỏa mãn điều kiện:

$$Z^{S.Z \bmod n} \bmod n = S^E \bmod n \text{, ở đây: } Z = g^v \bmod n \text{ và } E = H(M) \quad (5.2)$$

thì (v,S) sẽ được công nhận là chữ ký hợp lệ với bản tin M cần thẩm tra.

Bản chất của việc tìm các (v,S) thỏa mãn (5.1) và (5.2) là như nhau. 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.

III. KẾT LUẬN

Bài báo đề xuất một dạng lược đồ chữ ký số mới được xây dựng dựa trên bài toán phân tích số. Mức độ an toàn của dạng lược đồ mới đề xuất được đánh giá bằng mức độ khó giải của bài toán phân tích số. 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 $f_1(M,R)$, $f_2(M,R)$ và các phương trình kiểm tra tính hợp lệ của chữ ký được lựa chọn hợp lý. Tuy nhiên cũng cần phải thấy rằng, để sử dụng trong thực tế, các lược đồ này cần được đánh giá kỹ càng cả về mức độ an toàn cũng như khía cạnh hiệu quả thực hiện.

IV. TÀI LIỆU THAM KHẢO

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

[2] Lều Đức Tân, Hoàng Văn Thức,"Một thuật toán sinh cặp số nguyên tố RSA mạnh p, q thoả mãn điều kiện |p - q| có ước nguyên tố lớn," Tạp chí Nghiên cứu khoa học kỹ thuật và công nghệ quân sự số 14, 03 – 2006, trang 63-67.

[3] Lê Văn Tuấn, Lưu Hồng Dũng, Nguyễn Tiền Giang, "Phát triển lược đồ chữ ký trên bài toán phân tích số," Tạp chí Nghiên cứu khoa học và công nghệ quân sự - Đặc san CNTT, 04 – 2014, ISSN 1859 – 1043.

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

[5] Hoàng Văn Thức, "Thuật toán sinh tham số RSA an toàn," Tạp chí nghiên cứu khoa học và công nghệ quân sự, 02-2010, trang 40-45

[6] Bùi Việt Hồng, "Xây dựng thuật toán xác thực bản tin bằng chữ ký số theo hệ ký RSA-PSS,". Tạp chí Nghiên cứu khoa học kỹ thuật và công nghệ quân sự số 19, 06 – 2007, trang 59-64.

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

[8] Z. Shao, "Signature Schemes Based on Factoring and Discrete Logarithms," Computers and Digital Techniques, IEE Proceeding, 145(1):33-36, 1998.

[9] J. Li and G. Xiao, "Remarks on New Signature Scheme Based on Two Hard Problems," Electronics Letters, 34(25):2401, 1998.

[10] N. Y. Lee, "Security of Shao's Signature Schemes Based on Factoring and Discrete Logarithms," IEE Proceeding, 146(2):119-121, 1999.

[11] W. H. He, "Digital Signature Scheme Based on Factoring and Discrete Logarithms," Electronics Letters, 37(4):220-222, 2001

[12] Hung Min Sun, "Cryptanalysis of a Digital Signature Scheme Based on Factoring and Discrete Logarithms," NCS, 2002

[13] L. Ding and C. S. Laih, "Comment: Digital Signature Scheme Based on Factoring and Discrete Logarithms," IEEE, 49(12):2374-2391, 2002

[14] C. T. Wang, C. H. Lin, and C. C. Chang, "Signature Scheme Based on Two Hard Problems Simultaneously," Proceedings of the 17th International Conference on Advanced Information Networking and Application, Mar. 27-29, IEEE Computer Society, Washington, DC, USA, pp. 557-561, 2003

[15] S. Wei, "Digital Signature Scheme Based on Two Hard Problems," International Journal of Computer Science and Network Security, 7(12):207-209, December 2007.

[16] H. Lin, C. Gun, and C. Chen, "Comments on Wei's Digital Signature Scheme Based on Two Hard Problems," IJCSNS International Journal of Computer Science and Network Security, 9(2):1-3, February 2009.

[17] T. ElGamal, "A Public Key Cryptosystems and a Signature Scheme Based on Discrete Logarithms," IEE Transactions on Information Theory, IT-31(4):469-472, 1985.

DEVELOPING A NEW TYPE OF DIGITAL SIGNATURE SCHEME BASED ON INTEGER FACTORIZATION PROBLEM

Luu Hong Dung, Hoang Thi Mai, Nguyen Huu Mong

ABSTRACT- In this paper, we propose a new type of digital signature scheme based on a hard problem - the prime factorization of a large integer number. The result of this research can be applied to develop signature schemes in many applications in reality.