PHÁT TRIỂN MỘT DẠNG LƯỢC ĐỒ CHỮ KÝ SỐ MỚI DỰA TRÊN BÀI TOÁN RSA

Pham Van Hiep*, Luu Hong Dung+

* Khoa Công nghệ thông tin, Trường Đại Học Công nghiệp Hà Nội

+ Khoa Công nghệ thông tin, Học Viện Kỹ thuật Quân Sự

***Abstract*:** Bài báo đề xuất một phương pháp xây dựng lược đồ chữ ký mới dựa trên bài toán khai căn trên vành Z_n hay còn gọi là bài toán RSA. Từ phương pháp được đề xuất có thể tạo ra một họ lược đồ chữ ký mới tương tự như họ chữ ký ElGamal xây dựng trên bài toán logarit rời rạc. Bài báo cũng đề xuất 2 lược đồ chữ ký cùng các đánh giá về mức độ an toàn của chúng với mục đích minh họa cho việc triển khai phương pháp đã đề xuất nhằm tạo ra các lược đồ chữ ký và khả năng ứng dụng chúng trong các ứng dụng thực tế. Các lược đồ sẽ an toàn trước các dạng tấn công làm lộ khóa mật và tấn công giả mạo chữ ký nếu tuân thủ các điều kiện an toàn đã được chỉ ra.

***Keywords*:** Bài toán khai căn, Chữ ký số, Hàm băm, Lược đồ, Lược đồ chữ ký số.

I. ĐẶT VẤN ĐỀ

Chữ ký số hiện nay đã được ứng dụng rộng rãi trong các lĩnh vực như Chính phủ điện tử, Thương mại điện tử,… hay trong các hệ thống viễn thông và mạng máy tính. Tuy nhiên, việc nghiên cứu, phát triển các lược đồ chữ ký số mới cho mục đích thiết kế - chế tạo các sản phẩm, thiết bị an toàn và bảo mật thông tin trong các quốc gia vẫn luôn là vấn đề cần thiết được đặt ra.

Bài báo này đề xuất phát triển một dạng lược đồ chữ ký số mới dựa trên các bài toán khó đã được biết đến như là cơ sở để xây dựng nên hệ mật RSA danh tiếng [1]. Tuy nhiên, việc sử dụng các bài toán này trong các thủ tục hình thành tham số và khóa, hình thành chữ ký ở lược đồ chữ ký RSA và các lược đồ chữ ký mới đề xuất là hoàn toàn khác nhau.

II. BÀI TOÁN RSA

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: $1<t<\varphi(n)$ và thỏa mãn: $\gcd(t,\varphi(n))=1$, ở đây: $\varphi(n)=(p-1)\times(q-1)$. Khi đó bài toán khai căn trên vành số nguyên Z_n 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:*

$$x^t \bmod n = y \qquad (1)$$

Thuật toán để giải 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):

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

Trong một hệ thống giao dịch điện tử với dịch vụ chứng thực số dùng chung bộ tham số {n,t}, bài toán **RSA**$_{(n,t)}$ là khó theo nghĩa không thể thực hiện được trong thời gian thực. Ở đó, 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:

$$y = x^t \bmod n \qquad (2)$$

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 (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.

Hiện tại, bài toán **RSA**$_{(n,t)}$ vẫn được coi là bài toán khó [4-6] 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 RSA

A. *Lược đồ dạng tổng quát*

Lược đồ dạng tổng quát 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 dạng tổng quát 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

input: p, q.

Tác giả liên lạc: Phạm Văn Hiệp,
Email: hiephic@gmail.com; hieppv@haui.edu.vn
Đến tòa soạn 2/2020, chỉnh sửa 4/2020, chấp nhận đăng 5/2020

output: n, t, x, y.
Các bước thực hiện:
1. Tính modulo n: $n = p \times q$
2. Tính $\phi(n)$: $\phi(n) = (p-1) \times (q-1)$
3. Chọn số mũ t có giá trị trong khoảng: $1 < t < \phi(n)$ và thỏa mãn điều kiện: $\gcd(t, \phi(n)) = 1$
4. Chọn khóa bí mật x trong khoảng (1,n) và tính khóa công khai y theo:
$y = x^t \bmod n$ (3a), hoặc: $y = x^{-t} \bmod n$ (3b)

Chú thích:
- p, q: là các số nguyên tố.
- Việc tính: $y = x^t \bmod n$ theo (3a) hay: $y = x^{-t} \bmod n$ theo (3b) là tùy thuộc vào từng lược đồ cụ thể. Trường hợp nếu y tính theo (3b) thì x cần phải thỏa mãn điều kiện: $\gcd(x, n) = 1$

2) *Phương pháp hình thành chữ ký*
input: n, t, x, M – thông điệp dữ liệu cần ký.
output: (R,S)/(E,S) – chữ ký của U lên M.
Các bước thực hiện:
1. Chọn ngẫu nhiên giá trị *k* trong khoảng (1,n), tính thành phần thứ nhất của chữ ký theo:
$R = k^t \bmod n$ (4)
hoặc:
$E = f_1(M, R^{f_2(M,R)} \bmod n)$ (5)
2. Tính thành phần thứ 2 của chữ ký theo:
$S = k^{f_2(M,R)} \times x^{f_3(M,R)} \bmod n$ (6)
hoặc:
$S = k^{f_2(M,R)} \times x^{f_3(M,E)} \bmod n$ (7)

Chú thích:
- $f_1(.)$: 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 $(1, \phi(n))$.
- (R,S): chữ ký được tạo theo (4) và (6).
- (E,S): chữ ký được tạo theo (5) và (7).

3) *Phương pháp kiểm tra chữ ký*
a. Trường hợp chữ ký là (R,S)
input: n, t, y, (R,S), M.
output: (R,S) = true hoặc (R,S) = false.
Các bước thực hiện:
1. Tính giá trị u theo:
$u = S^t \bmod n$ (8)
2. Tính giá trị v theo:
$v = R^{f_2(M,R)} \times y^{f_3(M,R)} \bmod n$ (9)
3. Nếu (u = v) thì (R,S) = true, ngược lại thì: (R,S) = false.

b. Trường hợp chữ ký là (E,S)
1. Tính giá trị u theo:
$u = S^t \times y^{f_3(M,E)} \bmod n$ (10)
2. Tính giá trị v theo:
$v = f_1(M, u)$ (11)
3. Nếu (v = E) thì (E,S) = true, ngược lại thì: (E,S) = false.

Chú thích:
- (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 hình thành và kiểm tra chữ ký*
Mệnh đề 1:
Cho p, q là 2 số nguyên tố, $n = p \times q$, $\phi(n) = (p-1) \times (q-1)$, $1 < a, b, c < \phi(n)$, $1 < x, k < n$. Nếu: $y = x^a \bmod n$, $R = k^a \bmod n$, $S = k^b \times x^c \bmod n$ thì: $S^a \equiv R^b \times y^c \bmod n$.

Chứng minh:
Thật vậy, ta có:
$$S^a \bmod n = \left(k^b \times x^c \bmod n\right)^a \bmod n = k^{a.b} \times x^{a.c} \bmod n$$
$$= \left(k^a \bmod n\right)^b \times \left(x^a \bmod n\right)^c \bmod n = R^b \times y^c \bmod n$$
Mệnh đề đã được chứng minh.

Tính đúng đắn của phương pháp hình thành và kiểm tra chữ ký theo (4), (6), (8) và (9) có thể chứng minh như sau:
Đặt: $t = a$, $f_2(M,R) = b$, $f_3(M,R) = c$ ta có:
$u = S^t \bmod n = S^a \bmod n$, với: $S = k^b \times x^c \bmod n$
Và:
$v = R^{f_2(M,R)} \times y^{f_3(M,R)} \bmod n = R^b \times y^c \bmod n$, với:
$y = x^a \bmod n$ và: $R = k^a \bmod n$
Theo Mệnh đề 1 suy ra điều cần chứng minh: $u = v$.

Mệnh đề 2:
Cho p, q là 2 số nguyên tố, $n = p \times q$, $\phi(n) = (p-1) \times (q-1)$, $1 < a, b, c < \phi(n)$, $1 < x, k < n$, $\gcd(x, n) = 1$. Nếu: $y = x^{-a} \bmod n$, $R = k^a \bmod n$, $S = k^b \times x^c \bmod n$ thì: $R^b \equiv S^a \times y^c \bmod n$.

Chứng minh:
Thật vậy, ta có:
$$S^a \times y^c \bmod n = \left(k^b \times x^c \bmod n\right)^a \times \left(x^{-a} \bmod n\right)^c \bmod n$$
$$= k^{a.b} \times x^{a.c} \times x^{-a.c} \bmod n$$
$$= k^{a.b} \bmod n = \left(k^a \bmod n\right)^b \bmod n = R^b \bmod n$$
Mệnh đề đã được chứng minh.

Tính đúng đắn của phương pháp hình thành và kiểm tra chữ ký theo (5), (7), (10) và (11) cũng được chứng minh tương tự như sau:
Đặt: $t = a$, $f_2(M,R) = b$, $f_3(M,E) = c$ ta có:
$u = S^t \times y^{f_3(M,E)} \bmod n = S^a \times y^c \bmod n$, với:
$S = k^b \times x^c \bmod n$ và: $y = x^{-a} \bmod n$.
Theo Mệnh đề 2 suy ra:
$u = R^b \bmod n$, với: $R = k^a \bmod n$.
Nên:
$$v = f_1(M,u) = f_1\left(M, R^b \bmod n\right) = f_1\left(M, R^{f_2(M,R)} \bmod n\right) \quad (12)$$
Từ (5) và (12) ta có điều cần chứng minh: v = E.

B. Lược đồ chữ ký LDH.01
Lược đồ thứ nhất - ký hiệu LDH.01, được hình thành từ lược đồ dạng tổng quát với lựa chọn: $f_2(M,R) = H(M)$, $f_3(M,R) = R$. Ở đây H(.) là hàm băm và H(M) là giá trị đại diện (giá trị băm) của bản tin cần ký (M).

1. Thuật toán sinh tham số và khóa

Thuật toán 1.1:

Input: lp, lq.
Output: n, t, x, y, H(.).

[1]. **generate** *p, q*: *len*(*p*) = *lp*, *len*(*q*) = *lq*
[2]. $n \leftarrow p \times q$
[3]. select $H: \{0,1\}^* \mapsto Z_m$, $m < n$;
[4]. **select** t: $\left[\frac{n}{2}\right] < t < \phi(n)$
[5]. **select** *x*: $1 < x < n$
[6]. $y \leftarrow x^t \bmod n$ (13)
[7]. **return** {n,t,x,y,H(.)};

Chú thích:

- *len(.):* hàm tính độ dài (theo bit) của một số nguyên.
- p,q: là các số nguyên tố.

2. Thuật toán ký

Thuật toán 1.2:

Input: n, t, x, M.
Output: (R,S).

[1]. **select** *k*: $1 < k < n$
[2]. $R \leftarrow k^t \bmod n$ (14)
[3]. $E \leftarrow H(M)$
[4]. $S \leftarrow k^E \times x^R \bmod n$ (15)
[5]. **return** (R,S)

3. Thuật toán kiểm tra chữ ký

Thuật toán 1.3:

Input: n, t, y, M, (R,S).
Output: (R,S) = $true$ / $false$.

[1]. $E \leftarrow H(M)$
[2]. $u \leftarrow S^t \bmod n$ (16)
[3]. $v \leftarrow R^E \times y^R \bmod n$ (17)
[4]. **if** ($u = v$) **then** {**return** $true$;}
else {**return** $false$;}

4. Tính đúng đắn của lược đồ LDH.01

Tính đúng đắn của lược đồ LDH.01 được chứng minh như sau:

Đặt: $t = a$, $E = b$, $R = c$. Từ (13), (14), (15), (16) và (17) ta có:

$u = S^t \bmod n = S^a \bmod n$

Và:

$v = R^E \times y^R \bmod n = R^b \times y^c \bmod n$

Theo Mệnh đề 1, suy ra: $u = v$.

Đây là điều cần chứng minh.

C. Lược đồ chữ ký LDH.02

Lược đồ thứ hai - ký hiệu LDH.02, được hình thành từ lược đồ dạng tổng quát với lựa chọn: $f_1(M,R) = f_3(M,E) = H(M||R)$, $f_2(M,R) = 1$. Toán tử "||" được sử dụng ở đây là phép nối 2 xâu bit.

1. Thuật toán sinh tham số và khóa

Thuật toán 1.4:

Input: lp, lq.
Output: n, t, x, y, H(.).

[1]. **generate** *p, q*: *len*(*p*) = *lp*, *len*(*q*) = *lq*
[2]. $n \leftarrow p \times q$
[3]. **select** $H: \{0,1\}^* \mapsto Z_m$, $m < n$;
[4]. **select** t: $\left[\frac{m}{2}\right] < t < \phi(n)$
[5]. **select** *x*: $1 < x < n$, $\gcd(x, n) = 1$;
[6]. $y \leftarrow x^{-t} \bmod n$ (18)
[7]. **return** {n,t,x,y,H(.)};

2. Thuật toán ký

Thuật toán 1.5:

Input: n, t, x, M.
Output: (E,S).

[1]. **select** *k*: $1 < k < n$
[2]. $R \leftarrow k^t \bmod n$ (19)
[3]. $E \leftarrow H(M \parallel R)$ (20)
[4]. $S \leftarrow k \times x^E \bmod n$ (21)
[5]. **return** (E,S)

3. Thuật toán kiểm tra chữ ký

Thuật toán 1.6:

Input: n, t, y, M, (E,S).
Output: (E,S) = $true$ / $false$.

[1]. $u \leftarrow S^t \times y^E \bmod n$ (22)
[2]. $v \leftarrow H(M \parallel u)$ (23)
[3]. **if** ($v = E$) **then** {**return** $true$;}
else {**return** $false$;}

4. Tính đúng đắn của lược đồ LDH.02

Tính đúng đắn của lược đồ LDH.02 được chứng minh như sau:

Đặt: $t = a$, $b = 1, E = c$. Từ (18), (19), (21), (22) và Mệnh đề 2 ta có:

$u = S^t \times y^E \bmod n = S^a \times y^c \bmod n = R^b \bmod n = R$ (24)

Từ (23) và (24) suy ra:

$v = H(M \parallel u) = H(M \parallel R)$ (25)

Từ (20) và (25) ta có điều cần chứng minh: v = E.

D. Mức độ an toàn của các lược đồ mới đề xuất

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.

Ở các lược đồ mới đề xuất, có thể thực hiện một số dạng tấn công làm lộ khóa mật (x) và giả mạo chữ ký, từ khả năng thành công của các dạng tấn công này có thể đánh giá về mức độ an toàn và thiết lập một số điều kiện an toàn cho các lược đồ mới đề xuất. Phân tích, đánh giá mức độ an toàn sau đây được thực hiện cho lược đồ chữ ký LDH.02, việc đánh giá cho lược đồ LDH.01 cũng có thể thực hiện theo cách tương tự.

1. Tấn công khóa mật bằng phương pháp "vét cạn".

Thuật toán 1.7:

Input: n, t, y.
Output: x - khóa bí mật của đối tượng ký.

[1]. **for** i = 1 **to** n **do**
[1.1]. $z \leftarrow (i)^{-t} \bmod n$;
[1.2]. **if** ($z = y$) **then** { $x \leftarrow i$; **break**;}
[2]. **return** (x)

Nhận xét: Nếu giá trị của *x* không đủ lớn thì việc tấn công làm lộ khóa mật bằng Thuật toán 1.7 là hoàn toàn có thể thực hiện được.

Điều kiện 1.1: *Khóa bí mật x phải được chọn để việc tính:* $x = \boldsymbol{RSA_{(n,t)}(y)}$ *là khó.*

2. Tấn công khóa mật khi giá trị của k bị lộ.

Thuật toán 1.8:

Input: n, t, (E,S), k, $\gcd(k,n)=1$, $\gcd(E,-t)=1$
Output: x – khóa bí mật của đối tượng ký

[1]. $w \leftarrow S \times k^{-1} \bmod n$;
[2]. **Euclid** (E,t; a,b): $a \times E + b \times (-t) = 1$
[3]. $z \leftarrow w^a \times y^b \bmod n$;
[4]. **return** (z)

Chú thích: là giải thuật Euclid mở rộng để giải phương trình: $a \times E + b \times (-t) = 1$ với *E*, *t* cho trước và *a*, *b* là nghiệm.

Nhận xét: Khi giá trị của k bị lộ hoặc do lựa chọn giá trị không hợp lý dẫn đến bị lộ, thì việc tấn công khóa mật bằng Thuật toán 1.8 là có thể thực hiện được. Thật vậy, với giả thiết: $\gcd(k_i,n)=1$ *và* $\gcd(E,-t)=1$, *khi đó:*

$$w = S \times k^{-1} \bmod n = k \times x^E \times k^{-1} \bmod n$$
$$= x^E \bmod n$$

Giải: $a \times E + b \times (-t) = 1$ bằng thuật toán Euclid mở rộng được a và b, ta có:

$$z = w^a \times y^b \bmod n = x^{a.E} \times x^{b.(-t)} \bmod n$$
$$= x^{a.E+b.(-t)} \bmod n = x$$

Như vậy, nếu giá trị của khóa k bị lộ và các giả thiết đặt ra: $\gcd(k,n)=1$ và $\gcd(E,-t)=1$ được thỏa mãn thì việc tính khóa mật (x) là hoàn toàn có thể thực hiện được.

Điều kiện 1.2: *Giá trị của k cần được chọn để việc tính:* $k = \boldsymbol{RSA_{(n,t)}(R)}$ *là khó.*

3. Tấn công khóa mật khi giá trị của k bị sử dụng lặp lại

Thuật toán 1.9:

Input: (E_1,S_1), (E_2,S_2), $k_1 = k_2$, $\gcd(S_2,n)=1$
$\gcd((E_1-E_2),-t)=1$
Output: x – khóa bí mật của người ký.

[1]. $w \leftarrow S_1 \times (S_2)^{-1} \bmod n$;
[2].**Euclid** (E_1,E_2,t; a,b): $a \times (E_1 - E_2) + b \times (-t) = 1$;
[3]. $z \leftarrow w^a \times y^b \bmod n$;
[4]. **return** (z)

Nhận xét: Khi giá trị của *k* bị sử dụng lại thì việc tấn công làm lộ khóa mật bằng Thuật toán 1.8 là có thể thực hiện được.

Thật vậy, giả sử: $R_1 = (k_1)^t \bmod n$, $E_1 = H(M_1 \| R_1)$, $S_1 = k_1 \times x^{E_1} \bmod n$ là chữ ký tương ứng với thông điệp M_1 và $R_2 = (k_2)^t \bmod n$, $E_2 = H(M_2 \| R_2)$, $S_2 = k_2 \times (x)^{E_2} \bmod n$ là chữ ký tương ứng với thông điệp M_2. Với giả thiết: $k_1 = k_2 = k$, $\gcd((E_1 - E_2),-t)=1$ và $\gcd(S_2,n)=1$, khi đó:

$$w = S_1 \times S_2^{-1} \bmod n$$
$$= (x)^{E_1} \times k \times (x)^{-E_2} \times k^{-1} \bmod n$$
$$= x^{(E_1-E_2)} \bmod n$$

Giải: $a \times (E_1 - E_2) + b \times (-t) = 1$ được *a* và *b*, ta có:

$$z = w^a \times (y)^b \bmod n$$
$$= x^{a.(E_1-E_2)+b.(-t)} \bmod n = x$$

Như vậy, việc tấn công khóa mật (*x*) có thể thành công nếu khóa *k* bị sử dụng lặp lại và các giả thiết đặt ra được thỏa mãn.

Điều kiện 1.3: *Giá trị của k không được phép lặp lại ở các lần ký khác nhau.*

4. Tấn công giả mạo chữ ký khi lựa chọn tham số t không hợp lý.

Thuật toán 1.10:

Input: n, t, M, y – khóa công khai của U.
Output: (E^*,S^*) – chữ ký của U do đối tượng giả mạo U* tạo ra.

[1]. **select** k^*: $1 < k^* < n$
[2]. $R^* \leftarrow (k^*)^t \bmod n$;
[3]. $E^* \leftarrow H(M \| R^*)$;
[4]. $S^* \leftarrow k^* \times y^{-\left(\frac{E^*}{t}\right)} \bmod n$; (26)
[5]. **return** (E^*,S^*);

Nhận xét: Nếu $\left(\frac{E^*}{t}\right)$ cho kết quả là một giá trị nguyên thì việc tính S* theo (26) và do đó việc tạo chữ ký giả mạo (E*,S*) bằng Thuật toán 1.9 là hoàn toàn có thể thực hiện được. Thật vậy:

$$u^* = (S^*)^t \times (y)^{E^*} \bmod n = (k^*)^t \times y^{-\left(\frac{E^*}{t}\right).t} \times y^{E^*} \bmod n$$
$$= R^* \times y^{-E^*} \times y^{E^*} \bmod n = R^*$$

Do đó:

$$v^* = H(M \| u^*) = H(M \| R^*) = E^*$$

Như vậy, chữ ký giả mạo (E^*,S^*) do U* tạo ra nhưng hoàn toàn thỏa mãn điều kiện của thuật toán kiểm tra chữ ký (Thuật toán 1.6) do đó sẽ được công nhận là chữ ký hợp lệ của đối tượng U (chủ thể của khóa công khai y).

Điều kiện 1.4: *Cần chọn* $t = \left\lfloor \frac{m}{2} \right\rfloor + 1$

5. Tấn công giả mạo chữ ký nếu biết {p, q}.

Thuật toán 1.11:

Input: n, p, q, t, M, y – khóa công khai của U.
Output: (E^*,S^*)– chữ ký của U do U* tạo ra.

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

[2]. $R^* \leftarrow (k^*)^t \bmod n$;

[3]. $E^* \leftarrow H(M \parallel R^*)$;

[4]. $S^* \leftarrow k^* \times y^{-(E^* t^{-1} \bmod \phi(n))} \bmod n$ (27)

[5]. **return** (E^*, S^*);

Nhận xét: Nếu từ n có thể biết {p,q} thì việc tính S* theo (27) và do đó việc tạo cặp chữ ký giả mạo (E^*, S^*) bằng Thuật toán 1.10 là có thể thực hiện. Trong trường hợp này, kẻ giả mạo (U*) có thể tính: $E^* . t^{-1} \bmod \phi(n)$ thay cho việc tính $\left(\frac{E^*}{t}\right)$ và kết quả (E^*, S^*) vẫn được công nhận là chữ ký hợp lệ của đối tượng U.

Điều kiện 1.5: *Cần chọn {p,q} để bài toán phân tích một số nguyên lớn ra các thừa số nguyên tố là khó giải.*

Trong ứng dụng thực tế, các tham số {p,q} có thể chọn theo Chuẩn X9.31 [2] hay FIPS 186-3 [3] 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 ≥ 0).
- $\sqrt{2} \times 2^{511+128s} \le p, q \le 2^{511+128s}$ (s ≥ 0).
- $|p - q| > 2^{412+128s}$ (s ≥ 0).
- Các ước nguyên tố của p±1 và q±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 dưới đây:

Bảng 1. 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 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:

- $\sqrt{2} \times 2^{511+128s} \le p, q \le 2^{511+128s}$ (s ≥ 0).
- $|p - q| > 2^{\left(\frac{nlen}{2}\right)-100}$.
- Các ước nguyên tố của p±1 và q±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 2 dưới đây:

Bảng 2. Tiêu chuẩn an toàn đối với các số nguyên tố bổ trợ (độ dài tối đa, tối thiểu của p1, p2, q1, q2)

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 suất	*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

Những phân tích trên đây cho thấy, mức độ an toàn của lược đồ mới đề xuất phụ thuộc vào mức độ khó của hai bài toán: Bài toán phân tích số nguyên lớn ra các thừa số nguyên tố và Bài toán khai căn trên vành số nguyên $Z_{n=p.q}$, ở đây p và q là các số nguyên tố phân biệt. Lược đồ sẽ an toàn trước các dạng tấn công làm lộ khóa mật và tấn công giả mạo chữ ký nếu tuân thủ các điều kiện an toàn đã được chỉ ra.

IV. KẾT LUẬN

Bài báo đề xuất một dạng lược đồ chữ ký số mới xây dựng dựa trên bài toán khai căn trên vành Z_n. Từ dạng lược đồ đã đề xuất có thể xây dựng được một họ lược đồ chữ ký số mới, trong đó các lược đồ LDH.01 và LDH.02 chỉ là hai trong số các lược đồ được xây dựng theo phương pháp được đề xuất ở đây. Việc đánh giá mức độ an toàn của lược đồ LDH.02 trước một số dạng tấn công cho thấy khả năng ứng dụng của các lược đồ dạng này là hoàn toàn thực tế nếu bảo đảm các điều kiện an toàn đã được phân tích, đánh giá đưa ra trong bài báo.

REFERENCES

[1] 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.

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

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

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

[5] D.R Stinson, Cryptography: Theory and Practice, CRC Press 1995.

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

DEVELOPING A NEW TYPE OF DIGITAL SIGNATURE SCHEME BASED ON RSA PROBLEM

Abstract: The paper proposes a new method for constructing a signature scheme based on the Z_n ring-rooted problem, also known as RSA problem. From the proposed method, it is possible to create a new family of signature schemes similar to ElGamal's signature family based on discrete logarithmic problem. The paper also proposes two signature schemes and assessments of their security for the purpose of illustrating the implementation of the proposed method to create signature schemes and their applicability in practical applications. The schemas will be safe against attacks that expose secret keys and forged signature attacks if the specified security conditions are followed.

Keywords: Root problem, Digital Signature Schema, Hash Function, Schema, Digital Signature.

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.

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.