KHẮC PHỤC LỖI VÀ NÂNG CAO TÍNH HIỆU QUẢ CHO CÁC LƯỢC ĐỒ CHỮ KÝ SỐ DỰA TRÊN HAI BÀI TOÁN KHÓ

Lều Đức Tân[1], **Hồ Kim Giàu**[2]

[1]Học viện Kỹ thuật Mật mã
[2]Học viện Kỹ thuật Quân sự;
[2]Trường Sĩ quan Thông tin

***Tóm tắt*—Các lược đồ chữ ký số dựa trên hai bài toán khó sẽ tăng tính an toàn hơn lược đồ dựa trên một bài toán khó trong trường hợp một trong hai bài toán khó có thể giải được. Những năm qua có nhiều nghiên cứu đề xuất lược đồ chữ ký số dựa trên hai bài toán khó là bài toán logarit rời rạc và phân tích số. Trong đó, có thể kể đến hai lược đồ đã công bố là Rabin-Schnorr và RSA-Schnorr [1]. Trong bài báo này, chúng tôi chỉ ra một số lỗi dẫn đến việc có thể giả mạo chữ ký hoặc lược đồ chỉ phụ thuộc vào một bài toán khó của hai lược đồ trên, đồng thời đưa ra nhược điểm dẫn đến tính không hiệu quả của các lược đồ này. Ngoài ra, bài báo cũng đề xuất một lược đồ chữ ký số mới dựa trên hai bài toán khó mà thuật toán ký hiệu quả hơn lược đồ Rabin-Schnorr.**

***Từ khóa*—Chữ ký số, logarit rời rạc, phân tích số, hai bài toán khó.**

I. GIỚI THIỆU

Chữ ký số được dùng để xác thực về nguồn gốc và tính toàn vẹn của thông tin. Các thuật toán chữ ký số thường dựa trên hai hệ mật phổ biến là RSA và Elgamal. Hệ mật RSA dựa trên độ khó của bài toán phân tích thừa số nguyên tố. Elgamal dựa trên độ khó của bài toán logarit rời rạc. Các lược đồ chữ ký số có độ an toàn dựa trên tính khó của hai bài toán khó được quan tâm từ năm 1994 do L. Harn đề xuất [2] và liên tục sau đó các công bố vào năm 2008 của ba tác giả E. S. Ismail, N. M. F. Tahat và R. R. Amad [3], của E. S. Dermova năm 2009 [4], của S. Vishnoi và Shrivastava năm 2012 [5], của Binh V. Do, Minh H. Nguyên, Nikolay A. Moldovyal, năm 2013 [1],... Cùng với chúng là những phân tích chỉ ra thực chất về độ an toàn của chúng như phân tích của N. Y. Lee và T. Hwang về lược đồ của Harn công bố năm 1996 [6], phân tích của Shin-Yan Chiou và Yi-Xuan He về giao thức của Vishnoi và Shrivastava công bố năm 2013 [7]... Tóm lại chỉ còn hai lược đồ đưa ra trong [1] là đúng nghĩa với việc có độ an toàn dựa trên tính khó của hai bài toán khó đó là lược đồ Rabin-Schnorr và RSA-Schnorr. Trong bài báo này chúng tôi trình bày hai nội dung đó là:

- Chỉ ra một số lỗi dẫn đến việc dễ giả mạo hoặc dẫn đến việc chỉ phụ thuộc vào một bài toán khó của hai lược đồ Rabin-Schnorr và RSA-Schnorr. Tiếp đến chỉ ra nhược điểm dẫn đến tính không hiệu quả của các lược đồ này.
- Công bố một lược đồ Williams-Rabin-Schnorr với thuật toán ký hiệu quả hơn hẳn thuật toán ký của lược đồ Rabin-Schnorr.

Phần còn lại của bài báo được tổ chức như sau: Trong phần 2, chúng tôi trình bày một số kết quả làm cơ sở cho việc đánh giá tính hiệu quả của các thuật toán chữ ký số. Phần 3 giới thiệu, phân tích các lỗi của hai lược đồ Rabin-Schnorr và RSA-Schnorr, và đưa ra các lược đồ sửa đổi tương ứng; phần 4 đề xuất lược đồ WR-Schnorr bằng cách thay thế lược đồ Rabin trong Rabin-Schnorr bằng lược đồ Williams-Rabin (WR); cuối cùng là kết luận và tài liệu tham khảo.

II. MỘT SỐ KẾT QUẢ LÀM CƠ SỞ CHO VIỆC ĐÁNH GIÁ TÍNH HIỆU QUẢ

Các kết quả trình bày trong mục này bạn đọc có thể tìm trong các tài liệu. [8], [9], [10].

A. Một số ký hiệu

- $len(a)$: Số bít tối thiểu để biểu diễn nhị phân số nguyên dương a, còn gọi là độ dài của a.
- $t_M(N)$: Chi phí trung bình cho một phép nhân hai số N-bít.

Tác giả liên hệ: Hồ Kim Giàu
Email: hkgiau@gmail.com
Đến tòa soạn: 2/2020, chỉnh sửa: 4/2020, chấp nhận đăng: 4/2020;

- $t_{Red}(N)$: Chi phí trung bình cho một phép rút gọn một số 2N-bít theo modulo N-bít.
- $t_m(N)$: Chi phí trung bình cho một phép nhân rút gọn theo modulo n với len(n) = N.
- $t_{exp}(N, L)$: Chi phí trung bình cho một phép tính a^e mod n với len(e) = N và len(n) = L.
- $t_{inv}(N)$: Chi phí trung bình cho một phép tính a^{-1} mod n với len(n) = N.
- t_H: Chi phí trung bình cho một phép tính hàm H: $\{0,1\}^\infty \to \{0,1\}^h$.
- $t_{gcd}(N)$: Chi phí trung bình cho một phép tính gcd(a, b) với len(a), len(b) $\leq$ N.
- $t_{Jacobi}(N)$: Chi phí trung bình cho một phép tính $(\frac{a}{n})$ với len(n) = N.

B. Một số kết quả

Theo phương pháp Karatsuba thì:

$t_M(N) = O(N^{ln3/ln2})$ (phép toán bit).

Theo phương pháp Mongomegy hoặc Barrett thì:

$t_{Red}(N) = 2.t_M(N)$.

$t_{inv}(N) = t_{gcd}(N) = t_{Jacobi}(N) = O(N^2)$ (phép toán bit).

C. Một số quy đổi

$$t_m(N) = 3.t_M(N).$$

$$t_m(L) = 3^{log_2(L/N)} \times t_m(N) \quad (1)$$

Đặc biệt

$$t_m(2N) \approx 3 \times t_m(N) \quad (2)$$

Theo phương pháp bình phương-nhân thì

$$t_{exp}(N, L) = 1.5 \times N \times t_m(L) \quad (3)$$

Theo phương pháp nhị phân thì

$$t_{inv}(N) = t_{gcd}(N) = t_{Jacobi}(N) \approx \sqrt{N}.t_M(N) \quad (4)$$

Công thức Garner

Cho $n = p.q$ là tích của hai số nguyên tố khác nhau. Khi đó với mỗi $a \in \mathbb{Z}_n$, ký hiệu $a_p = a$ mod $p, a_q = a$ mod q, thì:

$$a = (c(a_p - a_q) + a_q) \bmod n \quad (5)$$

$$\text{với } c = q.(q^{-1} \bmod p) \quad (6)$$

giá trị a được xác định từ (a_p, a_q) được ký hiệu là $CRT(a_p, a_q)$.

D. Bảng kích thước tương đương về độ an toàn của các tham số RSA và logarit rời rạc (DL)

Tham số L = len(p) đối với DL và L = len(n) đối với RSA.

Tham số N = len(q) đối với DL.

Bảng I
KÍCH THƯỚC TƯƠNG ĐƯƠNG VỀ ĐỘ AN TOÀN CỦA CÁC THAM SỐ RSA VÀ DL

N	160	224	256	384	512
L	1024	2048	3072	8192	15360

III. PHÂN TÍCH HAI LƯỢC ĐỒ RABIN-SCHNORR VÀ RSA-SCHNORR

A. Lược đồ Rabin-Schnorr và RSA-Schnorr [1]

1) Các tham số: Hai lược đồ Rabin-Schnorr và RSA-Schnorr có chung bộ tham số miền đó là:

- Kích thước modulo L.
- Tập các thông báo $M = \{0,1\}^\infty$.
- Tập các chữ ký $S = \mathbb{N} \times \mathbb{N}$.
- Hàm tóm lược H:$\{0,1\}^\infty \to \{0,1\}^h$. Giá trị h được gọi là độ dài tóm lược.

Mỗi thành viên tương ứng với bộ các tham số sau:

- Số nguyên tố p có dạng $p = 2.n + 1$ với len(p) = L.
- Hợp số n có dạng $n = q.q'$ là hai số nguyên tố lẻ khác nhau sao cho việc phân tích n ra thừa số là khó (với lược đồ Rabin-Schnorr thì $q, q' \equiv 3$ (mod 4)).
- Phần tử sinh g có cấp bằng n.
- Tham số mật $x \in \langle g \rangle$ (nhóm cyclic sinh bởi g trong GF(p)) và tham số công khai $y = g^x$ mod p (với lược đồ RSA-Schnorr thêm số mũ mật d, số mũ công khai e thỏa mãn $e.d$ mod $\phi(n)$ = 1 với ϕ là số Euler).

Khi này khóa ký và khóa kiểm tra chữ ký:

- Trong lược đồ Rabin-Schnorr lần lượt là: (p, n, q, q', x) và (p, n, y).
- Trong lược đồ RSA-Schnorr lần lượt là: (p, n, q, q', d, x) và (p, n, e, y).

2) Lược đồ Rabin-Schnorr: Thuật toán 1,2.

Thuật toán 1: Thuật toán tạo chữ ký của người có khóa ký là (p, n, q, q', x)

Input: $m \in M$
Output: $(r, s) \in S$
1 $k \in_R (0, n)$
2 $u \leftarrow g^k$ mod p
3 $r \leftarrow H(m||u)$
4 $a \leftarrow (k - x.r)$ mod n
5 if $((\frac{a}{q}) = -1)$ or $((\frac{a}{q'}) = -1)$ then goto 1
6 $s_q \leftarrow a^{(q+1)/4}$ mod q; $s'_q \leftarrow a^{(q'+1)/4}$ mod q'
7 $s \leftarrow CRT(s_q, s_{q'})$
8 **return** (r, s)

3) Lược đồ RSA-Schnorr: Thuật toán 3,4.

Thuật toán 2: Thuật toán kiểm tra chữ ký của người có khóa kiểm tra là (p, n, y)

Input: $(m, (r, s)) \in M \times S$
Output: *"Accept"* nếu chữ ký là hợp lệ và *"Reject"* trong trường hợp ngược lại

$a \leftarrow s^2 \bmod n$
$u \leftarrow g^a.y^r \bmod p$
$r' \leftarrow H(m||u)$
If $(r = r')$ then **return** *"Accept"*
Else **return** *"Reject"*

Thuật toán 3: Thuật toán tạo chữ ký của người có khóa ký là (p, n, q, q', d, x)

Input: $m \in M$
Output: $(r, s) \in S$

$k \in_R (0, n)$
$u \leftarrow g^k \bmod p$
$r \leftarrow H(m||u)$
$a \leftarrow (k - x.r) \bmod n$
$s \leftarrow a^d \bmod p$
return (r, s)

Thuật toán 4: Thuật toán kiểm tra chữ ký của người có khóa kiểm tra là (p, n, e, y)

Input: $(m, (r, s)) \in M \times S$
Output: *"Accept"* nếu chữ ký là hợp lệ và *"Reject"* trong trường hợp ngược lại

$a \leftarrow s^e \bmod n$
$u \leftarrow g^a.y^r \bmod p$
$r' \leftarrow H(m||u)$
If $(r = r')$ then **return** *"Accept"*
Else **return** *"Reject"*

B. Một số phân tích và đề nghị sửa đổi cho hai lược đồ Rabin-Schnorr và RSA-Schnorr

1) Các lỗi của lược đồ Rabin-Schnorr và RSA-Schnorr: Lược đồ Rabin-Schnorr có hai lỗi sau:

- Lỗi thứ nhất. Xuất phát từ "Nếu (r, s) được chấp nhận bởi thuật toán kiểm tra M thì $(r, -s)$ cũng được chấp nhận". Như vậy sơ đồ là dễ giả mạo.
- Lỗi thứ hai. Nếu $gcd(s, n) \neq 1$ thì đây chính là ước của n. Trong trường hợp này lược đồ sẽ chỉ còn dựa vào bài toán logarit rời rạc.

Để tránh các lỗi trên chúng tôi đề nghị bước 4 và bước 7 của thuật toán ký được sửa đổi như sau:

4. $a \leftarrow (k - x.r) \bmod n$; if $(gcd(a, n) \neq 1)$ then goto 1.

7. $s \leftarrow CRT(s_q, s_{q'})$; if $(s \geq n/2)$ then goto $s = n - s$.

Tương ứng với việc sửa bước 7 trong thuật toán ký thì thuật toán kiểm tra bổ thêm điều kiện $(s < n/2)$. Lược đồ RSA-Schnorr có lỗi gống hệt như lỗi thứ hai của lược đồ Rabin-Schnorr và theo chúng tôi cũng cần sửa đổi bước 4 trong thuật toán ký của lược đồ này giống như đã sửa đổi với lược đồ Rabin-Schnorr.

Chú ý 1. Với n là tích của hai số nguyên tố khác nhau q và q' ta có:

$(gcd(a, n) \neq 1) \Leftrightarrow (a \bmod q = 0)$ hoặc $(a \bmod q' = 0)$.

2) Nâng cao tính hiệu quả cho lược đồ Rabin-Schnorr và RSA-Schnorr: Xuất phát từ lược đồ ElGamal, các lược đồ phát triển của nó như DSA, GOST, Schnorr,... nhằm đạt được tính hiệu quả cao đều có chung một giải pháp đó là đưa thêm vào tham số miền N vừa đủ lớn sao cho bài toán tìm các logarit trong nhóm $\langle g \rangle$ có kích thước N-bít là "khó". Khi này các lược đồ cải biên đều có hai đặc điểm:

- Thứ nhất. Kích thước chữ ký chỉ là 2.N bít.
- Thứ hai. Các phép tính lũy thừa có số mũ N-bít.

Trong khi cả hai lược đồ được trình bày ở trên luôn có kích thước nhóm đúng bằng L - 1. Nếu như các phép lũy thừa trong các thuật toán kiểm tra thường có số mũ là (L - 1)-bít thì phép lũy thừa trong thuật toán ký có thể điều khiển được.

Chúng tôi có một số khuyến nghị như sau:

- *Thứ nhất*. Đưa vào tham số miền N giống như các cải biên nếu trên cụ thể nó được lấy tương ứng với L theo bảng I, khi này bước 1 của các thuật toán ký nên chỉ là $k \in_R (2^{N-1}, 2^N)$.
  Tương tự tham số mật x cũng chỉ cần là $x \in_R (2^{N-1}, 2^N)$.
  Tham số $h = N$.
- *Thứ hai*. Số mũ công khai e nên có dạng $2^t + 1$, thậm chí lấy cố định là $2^{16} + 1$ như khuyến cáo đối với lược đồ RSA.
- Thứ ba. Đối với lược đồ Rabin-Schnorr, người ký tính sẵn và lưu như một tham số mật giá trị $c = q.(q^{-1} \bmod p) \bmod n$. Khi này chi phí cho việc tính $CRT(x, y)$ chỉ còn là $t_m(L)$.

C. Các lược đồ sau khi sửa đổi

1) Các tham số: Các tham số cho lược đồ Rabin-Schnorr và RSA-Schnorr giống như nêu trong mục III-A1 với một số bổ sung sau:

- Hàm tóm lược H:$\{0,1\}^\infty \rightarrow \{0,1\}^N$.
- Tham số mật $x \in_R (2^{N-1}, 2^N)$.
- Số mũ công khai $e = 2^{16} + 1$ dùng cho RSA-Schnorr.
- Tham số mật của người ký $c = q.(q^{-1} \bmod p)$ dùng cho Rabin-Schnorr.

Khi này khóa ký và khóa kiểm tra chữ ký:

- Trong lược đồ Rabin-Schnorr lần lượt là: (p, n, q, q', x, c) và (p, n, y).

- Trong lược đồ RSA-Schnorr lần lượt là: (p, n, q, q', d, x) và (p, n, e, y).

2) Lược đồ Rabin-Schnorr sửa đổi: Thuật toán 5,6.

Thuật toán 5: Thuật toán tạo chữ ký của người có khóa ký là (p, n, q, q', x, c)

Input: $m \in M$
Output: $(r, s) \in S$
1 $k \in_R (2^{N-1}, 2^N)$
2 $u \leftarrow g^k \bmod p$
3 $r \leftarrow H(m||u)$
4 $a \leftarrow (k - x.r) \bmod n$
5 $a_q \leftarrow a \bmod q; a'_q \leftarrow a \bmod q'$
6 if $((a_q = 0)$ or $(a_{q'} = 0))$ then goto 1. (thay cho $\gcd(a, n) \neq 1$)
7 if $((\frac{a}{q}) = -1)$ or $((\frac{a}{q'}) = -1)$ then goto 1
8 $s_q \leftarrow (a_q)^{(q+1)/4} \bmod q$; $s'_q \leftarrow (a_{q'})^{(q'+1)/4} \bmod q'$
9 $s \leftarrow (c.(s_q - s_{q'}) + s_{q'}) \bmod n$
10 if $(s \geq n/2)$ then $s \leftarrow n - s$
11 **return** (r, s)

Thuật toán 6: Thuật toán kiểm tra chữ ký của người có khóa kiểm tra là (p, n, y)

Input: $(m, (r, s)) \in M \times S$
Output: *"Accept"* nếu chữ ký là hợp lệ và *"Reject"* trong trường hợp ngược lại
1 if $(s \geq n/2)$ then **return** *"Reject"*
2 $a \leftarrow s^2 \bmod n$
3 $u \leftarrow g^a.y^r \bmod p$
4 $r' \leftarrow H(m||u)$
5 If $(r = r')$ then **return** *"Accept"*
6 Else **return** *"Reject"*

3) Lược đồ RSA-Schnorr sửa đổi: Thuật toán 7,8.

Thuật toán 7: Thuật toán tạo chữ ký của người có khóa ký là (p, n, q, q', d, x)

Input: $m \in M$
Output: $(r, s) \in S$
1 $k \in_R (2^{N-1}, 2^N)$
2 $u \leftarrow g^k \bmod p$
3 $r \leftarrow H(m||u)$
4 $a \leftarrow (k - x.r) \bmod n$
5 $a_q \leftarrow a \bmod q$; $a_{q'} \leftarrow a \bmod q'$
6 if $((a_q = 0)$ or $(a_{q'} = 0))$ then goto 1. (thay cho $\gcd(a, n) \neq 1$)
7 $s_q \leftarrow (a_q)^{d \bmod q} \bmod q$; $s_{q'} \leftarrow (a_{q'})^{d \bmod q'} \bmod q'$
8 $s \leftarrow (c.(s_q - s_{q'}) + s_{q'} \bmod n$
9 **return** (r, s)

Thuật toán 8: Thuật toán kiểm tra chữ ký của người có khóa kiểm tra là (p, n, e, y)

Input: $(m, (r, s)) \in M \times S$
Output: *"Accept"* nếu chữ ký là hợp lệ và *"Reject"* trong trường hợp ngược lại
1 $a \leftarrow s^e \bmod n$
2 $u \leftarrow g^a.y^r \bmod p$
3 $r' \leftarrow H(m||u)$
4 If $(r = r')$ then **return** *"Accept"*
5 Else **return** *"Reject"*

D. So sánh chi phí giữa những cặp lược đồ gốc và sửa đổi

Do những sửa đổi nêu ra trong mục III-B2 nhằm tăng tính hiệu quả chủ yếu trong các thuật toán tạo chữ ký cho nên ở đây chúng tôi chỉ đánh giá trong từng cặp thuật toán này. Trong phân tích của chúng tôi luôn giả thiết các cặp thuật toán cùng sử dụng việc lưu giá trị c để tính CRT và dùng chung số mũ e.

Mệnh đề 1. *Chi phí thuật toán ký của lược đồ Rabin-Schnorr sửa đổi ít hơn của Rabin-Schnorr là:*

$$4.(1,5.(L-N)-1).t_m(L) \quad (7)$$

Chứng minh

Sự khác nhau giữa hai thuật toán là tham số k ở thuật toán 1 là số L-bít, còn ở thuật toán 5 là N-bít như vậy chi phí cho việc tính giá trị $g^k \bmod p$ của hai thuật toán theo công thức (3) lần lượt sẽ là $1,5.L.t_m(L)$ và $1,5.N.t_m(L)$. Đối với thuật toán sửa đổi có thêm việc kiểm tra $((a_q = 0)$ or $(a_{q'} = 0))$ có chi phí $2.t_{Red}(\frac{L}{2}) < t_m(L)$.

Biết rằng xác suất để $(\frac{a}{q}) = -1$ (hoặc tương tự $(\frac{a}{q'})$=-1) bằng 0,5 nên để qua được bước 5 của thuật toán 1 (tương tự bước 6 của thuật toán 5) trung bình cần thực hiện 4 lần kiểm tra $(\frac{a}{q}) = -1$ or $(\frac{a}{q'}) = -1$. Như vậy hiệu chi phí giữa thuật toán 1 và 5 sẽ là $4.(1,5.L-(1,5.N+1)).t_m(L) = 4.(1,5.(L-N)-1).t_m(L)$.

Và đây là điều cần chứng minh.

Lập luận hoàn toàn tương tự đối với cặp lược RSA-Schnorr ta có.

Mệnh đề 2. *Chi phí thuật toán ký của lược đồ RSA-Schnorr sửa đổi ít hơn của RSA-Schnorr là*

$$(1,5.(L-N)-1).t_m(L) \quad (8)$$

Từ (7) và (8) ta tính được chi phí (theo đơn vị $t_m(L)$) tiết kiệm được khi sử dụng các lược đồ sửa

đổi so với lược đồ ban đầu cho trong bảng 2 dưới đây.

Bảng II
CHI PHÍ TIẾT KIỆM ĐƯỢC KHI LƯỢC ĐỒ SỬA ĐỔI ỨNG VỚI CẶP (L, N) CHO TRONG BẢNG I

N	160	224	256	384	512
L	1024	2048	3072	8192	15360
Rabin-Schnorr	5180	10940	16892	46844	89084
RSA-Schnorr	1295	2735	4223	11711	22271

IV. LƯỢC ĐỒ WR-SCHNORR

Lược đồ WR-Schnorr mà chúng tôi đưa ra trong phần này là sự thay thế lược đồ Rabin trong Rabin-Schnorr bằng lược đồ Williams-Rabin (WR) do Williams công bố vào năm 1980 [11]. Cơ sở để lược đồ WR ưu việt hơn hẳn Rabin trong thuật toán tạo chữ ký cho trong bổ đề 1 trình bày trong mục IV-A dưới đây.

A. Kết quả bổ trợ

Bổ đề 1. *Cho $n = p.q$ với $p \equiv 3$ (mod 8), $q \equiv 7$ (mod 8) là hai số nguyên tố. Khi đó với mọi $a \in \mathbb{Z}_n^*$ thì giá trị b xác định theo công thức sau:*

$$b = \begin{cases} a \in QR(n) \ \ khi \ \ (\frac{a}{p}) = 1, (\frac{a}{q}) = 1 \\ -2a \in QR(n) \ \ khi \ \ (\frac{a}{p}) = 1, (\frac{a}{q}) = -1 \\ 2a \in QR(n) \ \ khi \ \ (\frac{a}{p}) = -1, (\frac{a}{q}) = 1 \\ -a \in QR(n) \ \ khi \ \ (\frac{a}{p}) = -1, (\frac{a}{q}) = -1 \end{cases} \quad (9)$$

Sẽ thoả mãn:

1)

$$(\frac{b}{p}) = (\frac{b}{q}) = 1.$$

2) Hơn nữa nếu ký hiệu:

$$r_p = b^{(p+1)/4}, r_q = b^{(q+1)/4} \text{ và } c = q.(q^{-1} \bmod p) \quad (10)$$

thì giá trị:

$$r = (c.(r_p - r_q) + r_q) \bmod n \quad (11)$$

Thỏa mãn $r^2 \equiv b \ (\text{mod } n)$. (12)

B. Lược đồ WR-Schnorr

Tham số miền. Tham số miền giống như của Rabin-Schnorr sửa đổi nhưng thêm:

- $q \equiv 3 \ (\text{mod } 8)$ và $q' \equiv 7 \ (\text{mod } 8)$.
- Tập chữ ký $S = \{\pm 1\} \times \{\pm 1\} \times \mathbb{N} \times \mathbb{N}$.

Lược đồ WR-Schnorr được trình bày trong thuật toán 9, 10.

Thuật toán 9: Thuật toán tạo chữ ký của người có khóa ký là (p, n, q, q', c, x)

Input: $m \in \{0,1\}^\infty$
Output: $(u, v, r, s) \in \{\pm 1\} \times \{\pm 1\} \times \mathbb{N} \times \mathbb{N}$

$k \in_R (2^{N-1}, 2^N)$
$w \leftarrow g^k \bmod p$
$r \leftarrow H(m||w)$
$a \leftarrow (k - x.r) \bmod n$
$a_q \leftarrow a \bmod q$; $a_{q'} \leftarrow a \bmod q'$
if $((a_q = 0)$ or $(a_{q'} = 0))$ then goto 1. (thay cho $gcd(a, n) \neq 1$)
$u \leftarrow (\frac{a_q}{q}); v \leftarrow (\frac{a_{q'}}{q'})$
if $(u \neq v)$ then $a \leftarrow 2.a \bmod n$
if $(v = -1)$ then $a \leftarrow n - a$
$s_q \leftarrow a^{(q+1)/4} \bmod q$; $s'_q \leftarrow a^{(q'+1)/4} \bmod q'$
$s \leftarrow (c.(s_q - s'_q) + s'_q) \bmod n$
if $(s \geq n/2)$ then $s \leftarrow n - s$
return (u, v, r, s)

Thuật toán 10: Thuật toán kiểm tra chữ ký của người có khóa kiểm tra là (p, n, q, q', x)

Input: $(m, (u, v, r, s)) \in M \times S$
Output: *"Accept"* nếu chữ ký là hợp lệ và *"Reject"* trong trường hợp ngược lại

if $(s \geq n/2)$ **return** *"Reject"*
$b \leftarrow s^2 \bmod n$
if $(u \neq v)$ then $b \leftarrow b/2 \bmod n$
if $(v = -1)$ then $b \leftarrow n - b$
$w \leftarrow g^b.y^r \bmod p$
$r' \leftarrow H(m||w)$
If $(r = r')$ then **return** *"Accept"*
Else **return** *"Reject"*

C. Tính đúng đắn của lược đồ WR-Schnorr

Tính đúng đắn của lược đồ WR-Schnorr được cho trong kết quả sau.

Mệnh đề 3. *Lược đồ WR-Schnorr là đúng đắn.*

Chứng minh

Giả sử (u, v, r, s) là chữ ký được tạo từ thuật toán 9 của người giữ tham số mật (p, n, q, q', c, x) lên thông báo m. Nếu ký hiệu $a = (k - x.r) \bmod n$ (giá trị

tính được ở bước 4 và qua được bước 6), còn b là giá trị a tính được sau bước 9. Với tác động của bước 8 và bước 9 ta có:

$$\begin{aligned} b = a \quad &\Leftrightarrow \quad u = v = 1. \\ b = -2.a \quad &\Leftrightarrow \quad u = 1 \text{ và } v = -1. \\ b = 2.a \quad &\Leftrightarrow \quad u = -1 \text{ và } v = 1. \\ b = -a \quad &\Leftrightarrow \quad u = -1 \text{ và } v = -1. \end{aligned}$$

Theo bổ đề 1 thì giá trị s tính được ở bước 11 sẽ thỏa mãn:

$s^2 \bmod n = b$.

Bây giờ ký hiệu ngược lại b là giá trị tính được ở bước 2 thuật toán 10 còn a là giá trị b tính được sau bước 4 của thuật toán này ta có:

$$\begin{aligned} a = b \quad &\Leftrightarrow \quad u = v = 1. \\ a = -b/2 \quad &\Leftrightarrow \quad u = 1 \text{ và } v = -1. \\ a = b/2 \quad &\Leftrightarrow \quad u = -1 \text{ và } v = 1. \\ a = -b \quad &\Leftrightarrow \quad u = -1 \text{ và } v = -1. \end{aligned}$$

Từ hai kết quả trên thì giá trị b tính được sau bước 4 của thuật toán 10 chính là giá trị a tính được ở bước 4 trong thuật toán 9 hay

$b = (k - x.r) \bmod n$.

Như vậy giá trị w tính được tại bước 5 trong thuật toán 10 là

$w \equiv g^b.y^r \equiv g^{(k-x.r)}.y^r \equiv g^k \pmod p$

đúng bằng giá trị w tính được ở bước 2 thuật toán 9. Điều này dẫn đến hai giá trị r tính ở bước 3 thuật toán 9 và r' tính ở bước 6 thuật toán 10 là trùng nhau, hay đầu ra của thuật toán 10 là *"Accept"*. Mệnh đề đã được chứng minh.

D. Tính hiệu quả của lược đồ Williams-Rabin

Biết rằng trong hai lược đồ chữ ký dựa trên hai bài toán khó Rabin-Schnorr sửa đổi và RSA-Schnorr sửa đổi thì thuật toán ký của lược đồ thứ hai hiệu quả hơn nhưng thuật toán kiểm tra chữ ký thì ngược lại. Để có những kết luận về tính hiệu quả của lược đồ mới thành lập chúng tôi sẽ thực hiện so sánh thuật toán ký của nó với lược đồ thứ hai và so sánh thuật toán kiểm tra với lược đồ thứ nhất. Kết quả chop trong mệnh đề sau.

Mệnh đề 4. *Chi phí cho thuật toán thứ j, ký hiệu là $T_j (j = 5, 6, 7, 8, 9$ và $10)$. Ta có:*

$$T_9 - T_7 = 2.t_{Jacobi}(L/2). \tag{13}$$

$$T_{10} = T_6. \tag{14}$$

Chú ý, do

$$b/2 \bmod n = \begin{cases} (b+n) \gg 1 \text{ khi } b \text{ lẻ} \\ b \gg 1 \text{ khi } b \text{ chẵn} \end{cases}$$

nên phép toán này được bỏ qua trong công thức.

E. Tính an toàn của lược đồ WR-Schnorr

Lặp lại việc chứng minh tính an toàn của lược đồ Rabin-Schnorr trong [1] ta có kết quả sau.

Mệnh đề 5. *Lược đồ WR-Schnorr có độ an toàn dựa vào tính khó giải của đồng thời hai bài toán phân tích số và bài toán logarit rời rạc.*

V. KẾT LUẬN

Trong bài báo này, chúng tôi đã phân tích một số lỗi có thể xảy ra đối với hai lược đồ chữ ký số Rabin-Schnorr và RSA-Schnorr, đồng thời đưa ra các khuyến nghị và sửa đổi cho hai lược đồ này để hạn chế lỗi. Ngoài ra, chúng tôi còn đề xuất một thuật toán chữ ký số mới bằng cách thay thế lược đồ Rabin trong Rabin-Schnorr bằng lược đồ Williams-Rabin. Lược đồ đề xuất có thuật toán tạo chữ ký hiệu quả hơn lược đồ Rabin-Schnorr mà vẫn đảm bảo được độ an toàn do vẫn dựa trên hai bài toán khó.

TÀI LIỆU THAM KHẢO

[1] B. V. Do, M. H. Nguyen, and N. A. Moldovyan, "Digital signature schemes from two hard problems," in *Multimedia and Ubiquitous Engineering*. Springer, 2013, pp. 817–825.

[2] L. Harn, "Public-key cryptosystem design based on factoring and discrete logarithms," *IEE Proceedings-Computers and Digital Techniques*, vol. 141, no. 3, pp. 193–195, 1994.

[3] E. S. Ismail, N. Tahat, and R. R. Ahmad, "A new digital signature scheme based on factoring and discrete logarithms," *Journal of mathematics and statistics*, vol. 4, no. 4, pp. 222–225, 2008.

[4] E. S. Dermova, "Information authentication protocols on two hard problems. ph. d. dissertation," Ph.D. dissertation, St. Petersburg State Electrotechnical University St. Petersburg, Russia, 2009.

[5] S. Vishnoi and V. Shrivastava, "A new digitalsignature algorithm based on factorization and discrete logarithm problem," 2012.

[6] N.-Y. Lee and T. Hwang, "Modified harn signature scheme based on factorising and discrete logarithms," *IEE Proceedings-Computers and Digital Techniques*, vol. 143, no. 3, pp. 196–198, 1996.

[7] S. Chiou and Y. He, "Remarks on new digital signature algorithm based on factorization and discrete logarithm problem," *International Journal of Computer Trends and Technology (IJCTT)*, vol. 4, pp. 3322–3324, 2013.

[8] J. Katz, A. J. Menezes, P. C. Van Oorschot, and S. A. Vanstone, *Handbook of applied cryptography*. CRC press, 1996.

[9] R. Crandall and C. B. Pomerance, *Prime numbers: a computational perspective*. Springer Science & Business Media, 2006, vol. 182.

[10] D. Hankerson, A. J. Menezes, and S. Vanstone, *Guide to elliptic curve cryptography*. Springer Science & Business Media, 2006.

[11] H. Williams, "A modification of the rsa public-key encryption procedure (corresp.)," *IEEE Transactions on Information Theory*, vol. 26, no. 6, pp. 726–729, 1980.

FIX BUGS AND ENHANCE EFFICIENCY FOR THE DIGITAL SIGNATURE SCHEME BASED ON TWO HARD PROBLEMS

Abstract: Digital signature schemes based on two hard problems will be higher security than the scheme based on a single hard problem in case one of the two hard problems was solved. In recent years, many researchers have proposed the digital signature scheme based on the discrete logarithm problem and integer factorization problem. In particular, two published schemes are Rabin-Schnorr and RSA-Schnorr [1]. In this paper, we point out some bugs that lead to the possibility of forging signatures or schemes depending only on a single hard problem of the two proposed schemes, and the disadvantages leading to inefficiency of these schemes. In addition, this paper proposes a new digital signature scheme based on two hard problems that it is more efficient than the Rabin-Schnorr scheme in the signing algorithm.

Keywords: Digital signature, discrete logarithm problem, integer factorization problem, two hard problems.

Lều Đức Tân là Tiến sĩ toán học, từng công tác tại Học viện Kỹ thuật Mật mã, hiện nay đã nghỉ hưu. Hướng nghiên cứu chính: toán học và mật mã.

Hồ Kim Giàu Tốt nghiệp Đại học Khoa học - Tự nhiên, TP. Hồ Chí Minh năm 2005. Nhận bằng Thạc sỹ tại Học viện Bưu chính Viễn thông TP. Hồ Chí Minh năm 2011. Đơn vị công tác: Trường Đại học Thông tin liên lạc, Khánh Hoà. Hiện đang làm nghiên cứu sinh tại Học viện Kỹ thuật Quân sự. Email: hkgiau@gmail.com. Hướng nghiên cứu hiện nay: An toàn và bảo mật thông tin.