PHÁT TRIỂN MỘT LƯỢC ĐỒ CHỮ KÝ SỐ MỚI CÓ ĐỘ AN TOÀN DỰA TRÊN BÀI TOÁN LOGARIT RỜI RẠC TRÊN VÀNH Z_N

Lê Văn Tuấn [+], Bùii Thế Truyền[+], Lều Đức Tân[+]
[*]Khoa công nghệ thông tin, Học viện Kỹ thuật Quân sự
[*]Viện mô phỏng, Học viện Kỹ thuật Quân sự
[* +]Học viện Kỹ thuật mật mã

***Tóm tắt*:** Năm 1985, ElGamal đề xuất một lược đồ chữ ký số dựa trên trên bài toán logarit rời rạc modulo nguyên tố. Cho đến nay, đã có nhiều kết quả nghiên cứu của các nhà khoa học trên thế giới chỉ ra rằng lược đồ chữ ký số này không an toàn trước các cuộc tấn công giả mạo chữ ký dựa trên tình huống khóa phiên lộ hoặc bị dùng trùng. Trong bài báo này, chúng tôi đề xuất một lược đồ chữ ký số dựa trên bài toán logarit rời rạc theo modulo hợp số, một biến thể của lược đồ chữ ký số Elgamal. Lược đồ đề xuất khắc phục được những nhược điểm của lược đồ chữ ký Elgamal và nó có thể áp dụng được vào thực tế.

Từ khóa: Digital Signature Scheme, Discrete logarithmic problem, order problem, Hash Function.

I. GIỚI THIỆU

Việc nghiên cứu và phát triển lược đồ chữ ký số dựa trên các lược đồ chữ ký đã có là hướng nghiên cứu của nhiều nhà khoa học mật mã trên thế giới. Kể từ khi ElGamal đề xuất một lược đồ chữ ký số vào năm 1985 [1] [2], cho đến nay đã có nhiều lược đồ chữ ký số là biến thể của nó được phát minh bởi các nhà khoa học trên thế giới, chẳng hạn như: lược đồ chữ ký số Schnorr năm 1990 [3] [4 [5], lược đồ chữ ký số DSA năm 1994 [6]. Nhìn chung, sự an toàn của các lược đồ này đều phụ thuộc vào độ khó giải của bài toán logarit rời rạc (DLP) trong các nhóm con của một nhóm nhân Z_p^*, trong đó p là một số nguyên tố. Một điều đáng quan tâm ở đây là các nhóm nhân trong trường hữu hạn Z_p thường để lộ ra bậc của nó. Chính vì thế mà các lược đồ chữ ký số có độ an toàn dựa trên các nhóm nhân mà bậc của nó được công khai đã khiến cho các lược đồ này không an toàn từ một số loại tấn công cơ bản như: tấn công giả mạo chữ ký, tấn công làm lộ bí mật… Cho đến nay có nhiều kết quả nghiên cứu chỉ ra các yếu điểm của các lược đồ lược đồ Elgamal và các biến thể như: lược đồ chữ ký số DSA, Schnorr, đồng thời cũng có nhiều đề xuất cải tiến các lược đồ này để khắc phục những nhược điểm của các lược đồ nguyên thủy [7] [8] [9] [10] [11] [12] [13] [14] [15] [16]. Tuy nhiên các cải tiến này thường xoay quanh vấn chống các tấn công làm lộ bí mật dựa vào khóa phiên bị lộ hoặc khóa phiên bị dùng hai lần cho một thông báo. Chẳng hạn như trong [10], để giải quyết vấn đề lược đồ Elgamal bị mất an toàn gây bởi việc dùng trùng khóa phiên. Các tác giả Li Xiao-fei, Shen Xuan-jing và Chen Hai-peng đã đề xuất một lược đồ sửa đổi giải quyết vấn đề này. Một nhược điểm chung ở các lược đồ này là để lộ bậc của phần tử sinh và một khi khóa bí mật bị lộ thì các lược đồ bị phá vỡ. Để giải quyết vấn đề lộ bậc phần tử sinh, người ta đã xây dựng các lược đồ chữ ký số có độ an toàn dựa trên tính khó giải của bài toán logarit rời rạc trên vành hữu hạn Z_n. Chúng ta biết rằng tập $Z_n$cùng với phép cộng và phép nhân theo modul n tạo nên một vành hữu hạn Z_n, trong đó n được cấu tạo từ hai đến 3 số nguyên tố, thông thường n=pq, trong đó p, q là các số nguyên tố phân biệt. Trường hợp n=pq thì nhóm nhân Z_n^* sẽ là nhóm có bậc lớn nhất là (p-1)(q-1) và việc tìm giá trị này được cho là khó khi không biết phân tích của n, tức là bậc của các nhóm con của nhóm nhân Z_n^* là được giữ bí mật. Khi đó, các kiểu tấn công chữ ký làm lộ khóa phiên hoặc làm lộ khóa bí mật đều phải đối mặt với việc giải của bài toán logarit rời rạc trên vành Z_n. Cho đến nay, ngoài thuật toán Baby step- giant step của Danied Shank có thể ứng dụng đề giải bài toán logarit rời rạc trên vành thì các thuật toán khác chẳng hạn như: thuật toán Rho của Pollard [17], thuật toán Pohlig-Hellman [18]... chỉ áp dụng để giải bài toán logarit rời rạc trên trường hữu hạn. Chính vì thế, trong thời gian qua các nhà khoa học đã phát triển các lược đồ chữ ký mà độ an toàn của nó dựa trên độ khó giải của bài toán logarithm rời rạc trên vành hữu hạn Zn. Chẳng hạn như: lược đồ Girault scheme [19] vào năm 1991; Chik How Tan [20] vào năm 2003; S. K. Tripathi và B. Gupta [21] vào năm 2017; E. Okamoto và K. Tanaka [22] vào năm 1989… ; Chik How Tan [20] chứng minh rằng sơ đồ chữ ký của ông đã được bảo vệ chống lại sự giả mạo hiện hữu dưới sự tấn công thông điệp được lựa chọn thích ứng liên quan đến độ

Tác giả liên hệ: Lê Văn Tuấn
Email: levantuan71@yahoo.com
Đến toàn soạn: 4/2018 , chỉnh sửa: 5/2018 , chấp nhận đăng: 6/2018

khó của bài toán logarithm rời rạc trong mô hình tiên tri ngẫu nhiên.Tuy nhiên, trong lược đồ của Chik How Tan, số modulo n được tạo bởi ba số nguyên tố, khi đó các phép toán sẽ nhanh hơn so với số mô đun được tạo bởi 02 số nguyên tố khi áp dụng Định lý Trung Quốc về đồng dư, nhưng nó chắc chắn sẽ phức tạp hơn trong việc tạo khóa và quản lý khóa. Trong lược đồ chữ ký của SK Tripathi và B. Gupta [21] đã chúng minh chống được những tấn công làm lộ bí mật mà lược đồ chữ ký số DSA mắc phải, chẳng hạn như: tấn công "adaptive chosen-message" Tuy nhiên, lược đồ chũ ký của ông tiêu tốn nhiều đến không gian và thời gian tính toán hơn so với lược đồ chữ ký số DSA.

Cùng với xu hướng phát triển chung của thế giới, chúng tôi đã nghiên cứu, phát triển lược đồ chữ ký số mới dựa trên lược đồ Elgamal và khắc phục được các kiểu tấn công giả mạo chữ ký dựa vào tình huống lộ khóa phiên hoặc trùng khóa phiên mà lược đồ Elgamal đã mắc phải. Một số đóng góp quan trọng trong bài báo này, đó là:

Thứ nhất, chúng tôi đã đề xuất một lược đồ chữ ký số kế thừa các ưu điểm của lược đồ chữ ký số Elgamal và khắc phục được các nhược điểm của lược đồ này.

Thứ hai, xét về độ phức tính toán, lược đồ của chúng tôi có độ phức tạp tính toán thấp hơn lược đồ chữ ký số Elgamal tương tự đương với lược đồ DSA (Hình 2, hình 3) và chi phí thấp hơn so với lược đồ Elgamal.

Thứ ba, xét về độ phức tạp không gian bộ nhớ, lược đồ của chúng tôi cũng tương tự như lược đồ DSA và chi phí thấp hơn so với lược đồ Elgamal.

Thứ tư, lược đồ chữ ký số của chúng tôi an toàn hơn so với lược đồ DSA và Elgamal, điều này được phân tích trong phần III của bài báo.

Bài báo được tổ chức như sau: Ngoài phần giới thiệu, trong phần II, chúng tôi đưa ra một số công việc liên quan. Phần III, chúng tôi trình bày lược đồ đề xuất. Cuối cùng, chúng tôi trình bày một số kết quả thử nghiệm, kết luận và các công việc tiếp theo trong tương lai.

II. MỘT SỐ VẤN ĐỀ LIÊN QUAN

MỘT SỐ ĐỊNH NGHĨA KHÁI NIỆM

Định nghĩa 1. Hàm Num() đổi một xâu nhị phân thành số nguyên không quá T bít, ký hiệu **Num**: $\mathbb{N}\times\{0, 1\}^H \rightarrow \mathbb{Z}$. Ứng cặp $(T, b_0b_1...b_{H-1})$ thành số $a = b_0 + b_12 + ... + b_{min(T,H)-1}2^{min(T,H)-1}$.

Định nghĩa 2. Hàm Str() có chức năng đổi số nguyên không âm thành xâu nhị phân có T+1 bít. Ký hiệu **Str:** $\mathbb{Z}_{\geq 0} \rightarrow \{0, 1\}^{T+1}$. Ứng số nguyên không âm $a = b_0 + b_12 + ... + b_{T-1}2^{T-1} + 2^T$ thành xâu $b_0b_1...b_{T-1}1$.

Định nghĩa 3. Hàm Random: Hàm random là hàm lấy ngẫu nhiên một số nguyên trong đoạn [a, b], ký hiệu **Random**(a, b).

Định nghĩa 1: Bậc của số g theo mô-đun n là số m, nếu như m là số nhỏ nhất thỏa mãn biểu thức:

$g^m = 1 \bmod n$ (1).

B. LƯỢC ĐỒ CHỮ KÝ SỐ ELGAMAL.

Tham số:

p là một số nguyên tố với độ dài bit, ký hiệu *Length*(p), là L.

g là phần tử sinh nhóm nhân Z_p^* cấp p-1 trên $\mathbb{Z}_p$ với $0 < g < p$.

x là khóa riêng phải được giữ bí mật; x được chọn một cách ngẫu nhiên hoặc giả ngẫu nhiên trong [1, p – 1].

y là khóa công khai với $y = g^x \bmod p$.

k là số bí mật dùng riêng cho mỗi thông báo, còn được gọi là khóa phiên; k được chọn một cách ngẫu nhiên hoặc giả ngẫu nhiên trong [1, p – 1].

Bộ (p, g, x) được gọi là khóa riêng còn (p,g,y) được gọi là khóa công khai của người ký.

Sinh chữ ký:

Thuật toán 1:

Input: (p, g, x), m∈ Z_p^*.

Output: (r, s).

1. while (k, p-1) ≠1 k ← **Random**(1, p-1).
2. $r \leftarrow g^k \bmod p$.
3. $s \leftarrow k^{-1}(m - x.r) \bmod p-1$.
4. if (r = 0) or (s = 0), then goto 1.
5. return (r, s).

Xác nhận chữ ký:

Thuật toán 2:

Input: (p, g, y), (r, s), m∈ Z_p^*.

Output: "*accept*" or "*reject*".

1. if (r = 0) or (s = 0), then return "*reject*".
3. $u_1 \leftarrow y^r \bmod p$.
4. $u_2 \leftarrow r^s \bmod p$.
5. $v \leftarrow u_1.u_2 \bmod p$.
6. if ($v = g^m$), then return "*accept*" else return "*reject*".

Phân tích tính an toàn:

Tuy nhiên với việc công khai cấp của g dẫn đến tình huống mất an toàn của hệ mã Elgamal đó là:

Thứ nhất. Nếu bị lộ khóa phiên k trong một lần thực hiện việc ký trên thông báo M nào đó thì từ công thức

$s = (k^{-1}(m - r.x)) \bmod p-1$

ta dễ dàng tính được

$x = ((m-s.k).r^{-1}) \bmod p-1$ (2)

Thứ hai. Nếu khóa phiên k được dùng trùng (hai thông báo có chung khóa phiên) khi đó ta có:

$s= (k^{-1}(m - r.x)) \bmod p-1 \leftrightarrow k= s^{-1}(m-r.x) \bmod p-1$(3)

$s'= (k^{-1}(m' - r.x)) \bmod q \leftrightarrow k= s'^{-1}(m'-r.x) \bmod p-1$(4)

Từ (3) và (4) ta có đẳng thức sau:

$s^{-1}(m-r.x) = s'^{-1}(m'-r.x) \bmod p-1$. Từ phương trình này dễ dàng tính được khoá bí mật x như sau:

$x= (s'^{-1}m' - s^{-1}m)(s'^{-1}r - s^{-1}r)^{-1} \bmod p-1$. (5)

Phân tích độ phức tạp tính toán:

Trong thuật toán 3 gồm hai phép lũy thừa và hai phép nhân trong Z_p. Giả sử ký hiệu M_L là độ phức tạp tính toán cho một phép nhân trên trường $\mathbb{Z}_p$ có Length(p)= L. Một phép lũy thừa trong modul p, g^k mod p, với Length(p)= L và độ phức tạp của phép toán g^k mod p xấp xỉ LM_L. Vậy độ phức tạp của thuật toán 1 được ước lượng như sau:

$C_G \approx (2L+2)M_L$ (6)

Độ phức tạp tính toán của thuật toán 4 tập trung vào câu lệnh ở bước 5 với hai phép luỹ thừa (($g^{u1}.y^{u2}$) mod p) mod q. Do Length(u_1)≈ N và Length(u_2)≈ N, nên tổng chi phí cho thuật toán 3.2 được ước lượng là:

$C_v \approx (3L+1)M_L$ (7)

Không gian lưu trữ: Đối với lược đồ DSA, mỗi chữ ký gồm hai thành phần và yêu cầu tối đa là 320 bít với Length(q)=160, cần đến 448 bít với Length(q)=224 và cần đến 512 bít nếu Length(q)=256. Trong trường hợp tổng quát lược đồ chữu ký DSA sẽ cần đến 2N bít để lưu trữ cho mỗi chữ ký với N= Length(q).

C. LƯỢC ĐỒ CHỮ KÝ SỐ DSA

Các tham số của DSA.

p là một số nguyên tố với độ dài bit, ký hiệu Length(p), là L.

q là ước nguyên tố của p – 1 với Length(q) = N.

g là phần tử sinh nhóm con cấp q trên Zp với 0 < g < p.

x là khóa riêng phải được giữ bí mật; x được chọn một cách ngẫu nhiên hoặc giả ngẫu nhiên trong [1, q – 1].

y là khóa công khai với $y = g^x$ mod p.

Số k là số bí mật dùng riêng cho mỗi thông báo, còn được gọi là khóa phiên; k được chọn một cách ngẫu nhiên hoặc giả ngẫu nhiên trong [1, q – 1].

Bộ (p, q, g, x) được gọi là khóa riêng của người ký, bộ (p, q, g, y) được gọi là khóa công khai của người ký.

Thuật toán sinh chữ ký.

Thuật toán 3:
Input: (p, q, g, x), k, M.
Output: (r,s).
1. z ← Num(N, Hash(M)).
2. k ← Random(1, q).
3. r ← (g^k mod p) mod q.
4. w ← (z + x.r) mod q.
5. if (r = 0) or (w = 0), then goto 2.
6. s ← (k^{-1}.(z + x.r)) mod q.
7. return (r, s).

Xác nhận chữ ký.

Thuật toán 4:
Input: (p, q, g, y), (r,s), M.
Output: "accept" or "reject".
1. w ← s^{-1} mod q.
2. z ←Num(N, Hash(M)).
3. u_1 ← (z.w) mod q.
4. u_2 ← (r.w) mod q.
5. v ← (($g^{u1}.y^{u2}$) mod p) mod q.
6. if (v = r) then return "accept". Else return "reject".

Độ phức tạp tính toán

Giả sử ký hiệu M_L là độ phức tạp tính toán cho một phép nhân hai số nguyên dương trên trường Z_P có Length(p)= L và trên trường trường Z_q có Length(q) = N, ký hiệu là M_N Độ phức tạp tính toán của thuật toán 3 tập trung ở phép (g^k mod p) mod q. Khi đó độ phức tạp của phép toán g^k mod p xấp xỉ O(logk. M_L). $_N$. Do đó chi phí cho thuật toán 3 ước lượng như sau:

$C_G \approx NM_L + (N+3)M_N)$ (8)

Độ phức tạp tính toán của thuật toán 4 tập trung vào câu lệnh ở bước 5 với hai phép luỹ thừa (($g^{u1}.y^{u2}$) mod p) mod q. Do Length(u_1)≈ N và Length(u_2)≈ N, nên tổng chi phí cho thuật toán 4 được ước lượng là:

$C_v \approx 2NM_L + (2+N)M_N$ (9)

Tính an toàn của lược đồ chữ ký số DSA.

Tính an toàn của một lược đồ chữ ký thể hiện ở tính "khó" tạo được chữ ký hợp lệ của người không sở hữu tham số x hay còn gọi là "giả mạo chữ ký" . Người ta đã chứng tỏ rằng mọi việc giả mạo chữ ký đều dẫn đến việc giải một bài toán logarit theo cơ số g trên Zp hoặc tìm được va chạm của hàm Hash cho nên trong FIPS_186-4[7] đã đưa ra yêu cầu về các kích thước L và N. Cụ thể các cặp (L, N) cho những ứng dụng cần an toàn đến năm 2030 là (L, N)= (2048, 224) hoặc (L, N)= (2048, 256) còn (L, N)= (3072, 256) an toàn cho đến sau năm 2030. Tuy nhiên với việc công khai cấp của g dẫn đến tình huống mất an toàn của DSA như sau:

Tình huống thứ nhất: Nếu khóa phiên k bị lộ trong một lần thực hiện việc ký trên thông báo M nào đó thì từ công thức sau:

s = (k–1(z + r.x)) mod q

ta dễ dàng tính được khoá bí mật x theo công thức sau:

x = ((s.k – z).r–1) mod q

Tình huống thứ hai: Nếu hai thông báo khác nhau được ký với cùng một khóa phiên k (dùng trùng khóa). Giả sử hai thông báo được ký trùng khóa phiên k là M và M' và hai chữ ký tương ứng với M và M’ lần lượt là (r,s) và (r,s'). Kẻ tấn công sẽ tìm được khóa bí mật x như sau: Đầu tiên hai giá trị z và z’ được tính từ công thức z = **Num**(N, **Hash**(M)) và z' = **Num**(N, **Hash**(M')), khi đó s và s’ được xác định như sau:

s= (k^{-1}(z + r.x)) mod q ↔ k= s^{-1}(z+r.x) mod q(10)

s'= (k^{-1}(z' + r.x)) mod q ↔ k= s'^{-1}(z’+r.x) mod (11)

Từ (10) và (11) ta có đẳng thức sau: s^{-1}(z+r.x)= s'^{-1}(z’+r.x) mod q ↔ s^{-1}z- s'^{-1}z’= (s'^{-1} – s^{-1}).r.x mod q. Từ kết quả này dễ dàng tính được khoá bí mật x như sau: x= r^{-1}(s^{-1}.z-s'^{-1}z’) (s'^{-1} – s^{-1})$^{-1}$ mod q.

Tác giả liên hệ: Lê Văn Tuấn
Email: levantuan71@yahoo.com
Đến toàn soạn: 4/2018 , chỉnh sửa: 5/2018 , chấp nhận đăng: 6/2018

III. LƯỢC ĐỒ CHỮ KÝ SỐ ELGAMAL TRÊN VÀNH $\mathbb{Z}_n$.

A. LƯỢC ĐỒ CHỮ KÝ SỐ ĐƯỢC ĐỀ XUẤT

Dựa trên kết quả phân tích, đưa ra những tình huống mất an toàn của lược đồ chữ ký số Elgamal và DSA trên trường, chúng tôi đề xuất một lược đồ chữ ký số mới trên vành khắc phục được một số nhược điểm đã chỉ ra trong hai lược đồ Elgamal và DSA, có độ phức tạp tính toán tương đương với DSA và có thể ứng dụng trên thực tế. Lược đồ chữ ký số mới được xây dựng dựa trên một số phân tích sau:

- Trong lược đồ đề xuất, độ an toàn của nó dựa trên tính khó giải của bài toán DLP trên nhóm nhân là $Z_m \subseteq Z_n^*$, m, n là hợp số. Trong khi lược đồ DSA, tính an toàn của nó dựa trên tính khó giải của bài toán DLP trên nhóm nhân là $Z_q \subseteq Z_p^*$, p, q là số nguyên tố.

- Thành phần r của chữ ký trong lược đồ đề xuất được cấu tạo tương tự trong lược đồ DSA.

- Điểm khác biệt quan trọng trong lược đồ đề xuất là thành phần thứ nhất của chữ ký là r được băm với thông báo cho đầu ra z tham gia vào tính thành phần thứ hai của chữ ký là s

$$z \leftarrow \text{Num}(N, H(T||\text{Str}(r))) \quad (12)$$

- Thành phần s của chữ ký trong lược đồ đề xuất được tính theo công thức sau:

$$s \leftarrow k^{-1}(z - x) \bmod m \quad (13)$$

được kế thừa từ thành phần s của lược đồ chữ ký Elgamal theo công thức

$$s \leftarrow k^{-1}(m - x.r) \bmod p\text{-}1. \quad (14)$$

Trong công thức (13), thành phần r trong lược đồ Elgamal được gỡ bỏ vì giá trị này đã tham gia vào tính tham số z, bởi công thức (12). Sự cải tiến này không ảnh hưởng đến độ an toàn của lược đồ và nó giảm cho thủ tục sinh chữ ký một phép nhân và giảm cho thủ tục xác nhận chữ ký một phép lũy thừa.

- Khóa bí mật trong lược đồ đề xuất là (n,m,g,x) và khóa công khai là (n,Length(m),g,y). Điểm khác biệt của khóa công khai trong lược đồ đề xuất so với hai lược đồ DSA và Elgamal là chỉ công khai cỡ của bậc phần tử sinh g(Length(m)) và giữ kín giá trị bậc của nó(giá trị m). Đây là đặc tính quan trọng nhất của lược đồ đề xuất, nhờ vào đặc tính này mà nó chống được các kiểu tấn công giả mạo khi tình huống lộ khóa phiên và trùng khóa phiên xảy ra. Tiếp cận với kết quả phân tích trên, lược đồ đề xuất được xây dựng như sau:

Tham số và khóa:

Cho n = p.q với p, q là các số nguyên tố thỏa mãn việc phân tích n ra thừa số là khó.

Giá trị m là khóa riêng phải được giữ bí mật; m = $p_1.q_1$ với p_1, q_1 là các nguyên tố thỏa mãn điều kiện sau:

$p_1 \mid (p-1)$, $q_1 \mid (q-1)$, $p_1 \nmid (q-1)$, $q_1 \nmid (p-1)$.

N là độ dài bít của m, *Length*(m), N= *Length*(m).

g là phần tử sinh của nhóm con cấp m mod n. m, g thỏa mãn việc tìm logarit cơ số g mod n là khó.

x là khóa riêng phải được giữ bí mật; x được chọn ngẫu nhiên trong đoạn [1, m−1].

y là khóa công khai, với $y = g^x \bmod n$.

k là số bí mật tương ứng duy nhất cho mỗi thông báo (còn được gọi là khóa phiên); k được chọn ngẫu nhiên trong đoạn [1, m−1].

Người ký lấy (n, m, g, x) làm khóa bí mật và công bố (n, N, g,y) là khóa công khai của mình.

Sinh chữ ký:

Thuật toán 5:

Input: (n, m, g, x), T∈ $\{0,1\}^*$.

Output: (r,s).

1. while (k, m) ≠1 k ← **Random**(1, m-1).
2. $r \leftarrow g^k \bmod n$.
3. z ← Num(N, H(T||Str(r)))
4. $s \leftarrow k^{-1}(z - x) \bmod m$.
5. if (r = 0) or (s = 0), then goto 1.
6. return (r, s).

Xác nhận chữ ký:

Thuật toán 6:

Input: M, (r, s), (n, N, g, y).

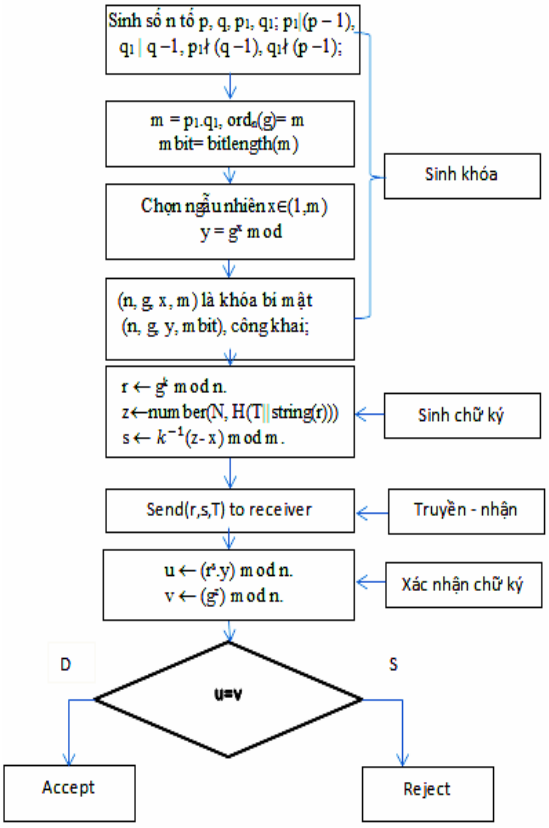
Output: "*accept*" hoặc "*reject*".

1. z ← ***Num***(N, ***H***(M||***Str***(r))).
2. $u \leftarrow (r^s.y) \bmod n$.
3. $v \leftarrow (g^z) \bmod n$.
4. if (u = v) return "*accept*" else return "*reject*".

Tính đúng đắn:

Dễ dàng thấy rằng

$(r^s.y) \bmod n = g^{k(k^{-1}(z-x))}\, g^x \bmod n = g^z \bmod n = v$



Hình 1. Lưu đồ mô tả quá trình sinh khóa, ký và xác nhận chữ ký

B. PHÂN TÍCH LƯỢC ĐỒ.

Phân tích an toàn:

Dưới đây xét một số tình huống gây đã mất an toàn cho lược đồ Elgamal cụ thể với lược đồ của chúng tôi:

Trường hợp thứ nhất: Khóa phiên bị lộ, khi đó khóa bí mật x sẽ được xác định bởi công thức sau đây:

$s \leftarrow k^{-1}.(z - x) \bmod m \rightarrow x \leftarrow (z - k.s) \bmod m$. Do m được giữ bí mật nên kẻ tấn công khó có thể xác định được khóa bí mật.

Trường hợp thứ hai: Khóa phiên bị dùng trùng lặp, giải sử thông báo T và T' dùng cùng một khóa phiên, khi đó khóa bí mật x sẽ được xác định bởi công thức sau:

$z \leftarrow Num(mbit, H(T||r))$

$z' \leftarrow Num(mbit, H(T'||r))$

$s \leftarrow k^{-1}.(z - x) \bmod m \leftrightarrow k = s^{-1}.(z-x) \bmod m$

$s' \leftarrow k^{-1}.(z' - x) \bmod m \leftrightarrow k = s'^{-1}.(z'-x) \bmod m$

$x=(s'^{-1} - s^{-1})^{-1} (s'^{-1}.z' - s^{-1}.z) \bmod m.$

Do m được giữ bí mật nên kẻ tấn công khó có thể xác định được khóa bí mật

Trường hợp thứ ba: Kẻ tấn công có được khóa bí mật x, khi đó để tạo một chữ ký giả của thông báo T nào đó, anh ta phải tính toán các thành phần của chữ ký (r,s) như sau:

$r = g^k \bmod n$

$z \leftarrow Num(mbit, H(T||r))$

$s \leftarrow k^{-1}.(z - x) \bmod m.$

Do m được giữ bí mật nên kẻ tấn công khó có thể xác định được thành phần s của chữ ký và không thể giả mạo.

Chi phí tính toán.

Giả sử ký hiệu C_G là tổng chi phí thời gian sinh chữ ký và C_V là tổng thời gian chi phí cho xác nhận chữ ký. Giả sử ký hiệu M_L là độ phức tạp tính toán của phép nhân hai số nguyên trên vành $\mathbb{Z}_n$ và M_N là độ phức tạp tính toán của một phép nhân trên vành $\mathbb{Z}_m$ có Length(m)= N. Dễ thấy có ít nhất một vòng lặp trong thuật toán 3. Độ phức tạp tính toán cho mỗi vòng lặp này là phép lũy thừa $g^k \bmod n$ trên vành $\mathbb{Z}_n$ và một phép tính phần tử nghịch đảo $k^{-1} \bmod m$. Theo [27] độ phức tạp phép toán $g^k \bmod n$ xấp xỉ $O(L.M_L)$ với L= Length(n). Để ước lượng độ phức tạp tính toán của phép nghịch đảo ta có $k^{-1} \bmod m$ có độ phức tạp tính toán của phép toán tìm $k^{-1} \bmod m$ xấp xỉ $O(N.M_N)$ với N= Length(m). Vậy độ phức tạp tính toán cho mỗi bước lặp sẽ là:

$LM_L + (N+1)M_N).$ (15)

Biết rằng điều kiện để thoát vòng lặp là gcd(k, m) = 1, tức là k phải có nghịch đảo và xác suất để k có nghịch đảo trong modulus m là:

$$Prob_{(gcd(k, m) = 1)} = \frac{\varphi(m)}{m} = \frac{(p_1 - 1)(q_1 - 1)}{m} \quad (16)$$

Với m đủ lớn thì $Prob_{(gcd(k, m) = 1)}$ xấp xỉ bằng 1. Vậy tổng chi phí cho thuật toán tạo chữ ký, ký hiệu là C_G xác định theo công thức sau

$C_G \approx LM_L + (N+1)M_N$ (17)

Độ phức tạp của thuật toán 4 tập trung ở phép toán $r^s.y \bmod n$ và $g^z \bmod n$. Giả sử M_L ký hiệu cho độ phức tạp tính toán của một phép nhân trên vành $\mathbb{Z}_n$ có *Length*(n) = L, thì tổng chi phí trung bình cho thuật toán này, ký hiệu là C_V xác định theo công thức sau:

$C_v \approx (2L+1)M_L$. (18)

Phân tích độ phức tạp về không gian đối với lược đồ đề xuất, mỗi chữ ký gồm hai thành phần và yêu cầu tối đa là 2N bít với Length(m)=N để lưu trữ cho mỗi chữ ký. Vậy kết quả phân tích hai lược đồ chữ ký số Elgamal và lược đồ đề xuất được thống kê trong bảng sau:

Bảng I. Kết quả phân tích

	Sinh chữ ký	Xác nhận chữ ký	Không gian lưu trữ
Elgamal scheme	$C_G \approx (2L+2)M_L$	$C_V \approx (3L+1)M_L$	2L, L= Length(p)
RSA	$C_G \approx LM_L$	$C_V \approx 128M_L$	L, L= Length(n)
DSA	$C_G \approx NM_L + (N+3)M_N$	$C_V \approx 2NM_L + (2+N)M_N$	2N, N= Length(q)
Lược đồ đề xuất	$C_G \approx LM_L + (N+1)M_N$	$C_V \approx (2L+1)M_L$	2N, N= Length(m)

C. THỬ NGHIỆM

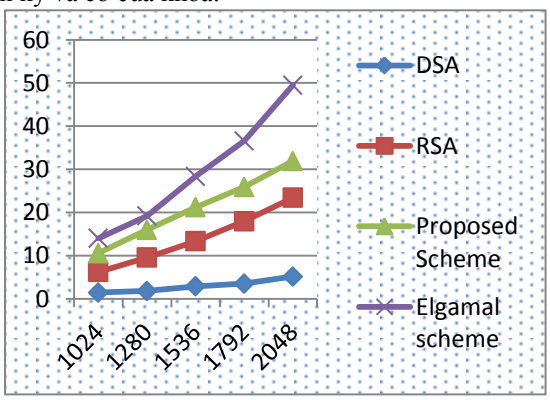
Trong phần thử nghiệm này, xét độ dài khóa lần lượt là: 1024, 1280, 1536, 1792, 2048 (bit) cho bốn lược đồ đó là lược đồ DSA, RSA, Elgamal và lược đồ đề xuất . Văn bản được sử dụng để thử nghiệm quá trình ký có dung lượng 18.87 MB. Số lần thử nghiệm cho mỗi bộ tham số là 10000 lần. Hàm băm SHA 512 được sử dụng trong thuật toán ký và xác nhận chữ ký của các lược đồ. Chương trình thử nghiệm viết bằng ngôn ngữ lập trình C++, được biên dịch bởi trình QT Creater và chạy trên hệ điều hành Window 7. Bộ vi xử lý Core2 Duo 2.2 GHz bộ nhớ 2GB. Tham số thử nghiệm của các lược đồ chữ ký số có kích thước và tiêu chuẩn gần với tham số trên thực tế và được sinh ra bằng thuật toán trong [28]. Kết quả thử nghiệm được chỉ ra trong bảng II.

Tác giả liên hệ: Lê Văn Tuấn
Email: levantuan71@yahoo.com
Đến toàn soạn: 4/2018 , chỉnh sửa: 5/2018 , chấp nhận đăng: 6/2018

Bảng II. Kết quả thử nghiệm

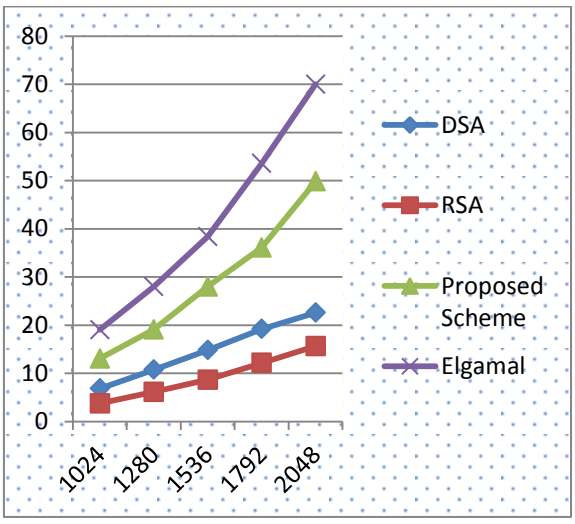
Modulus size (bit)	Sinh chữ ký (second)				Xác nhận chữ ký (second)			
	Elgamal	DSA	RSA	Proposed scheme	Elgamal	DSA	RSA	Proposed scheme
1024	14.017	1.416	6,216	10,056	19.017	6.836	3,743	13,027
1280	19,203	1.814	9,54	15,056	28,003	10.765	6,145	19,807
1536	28.356	2.89	13,317	21,076	38.356	14.813	8,656	26,001
1792	36,582	3.5	17,985	25,013	53,582	19.18	12,131	35,105
2048	46,981	5.138	23,419	31,057	69,981	22.59	15,646	46,820

Kết quả sinh chữ ký trong bảng II được minh họa bởi hình 2 dưới đây chỉ ra mối qua hệ giữa thời gian ký và cỡ của khóa:



Hình 2. Mối quan hệ giữa thời gian sinh chữ ký và cỡ của khóa

Kết quả xác nhận chữ ký trong bảng II được minh họa bởi hình 3 dưới đây chỉ ra mối qua hệ giữa thời gian xác nhận chữ ký và cỡ của khóa:



Hình 3. Mối quan hệ giữa thời gian xác nhận chữ ký và cỡ của khóa

IV. KẾT LUẬN

Cho đến nay, bài toán logarit rời rạc trên vành Z_n là bài toán khó giải với khả năng tính toán của máy tính. Dựa trren tính khó giải này mà nhiều lược đồ chữ ký số và các biến thể được phát triển trên bài toán này[20][21][22]. Góp phần vào sự phát triển chung trong lĩnh vực an toàn và bảo mật thông tin của nước ta nói chung và trong lĩnh vực quốc phòng-an ninh nói riêng, chúng tôi đã xây dựng một lược đồ chữ ký số mới có độ an toàn dựa trên tính khó giải của của bài toán logarit rời rạc trong vành các lớp thặng dư theo mô đun hợp số. Nhóm tác giả đã chứng minh tính đúng đắn, tính an toàn và tính hiệu quả của lược đồ đề xuất so với lược đồ DSA, Elgamal. Phần thử nghiệm, nhóm tác giả đã viết chương trình thử nghiệm trên ngôn ngữ C++. Kết quả thử nghiệm cho thấy giữa phân tích toán học về chi phí tính toán với kết quả thử nghiệm là tương đồng. 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, đây là vấn đề nghiên cứu mà nhóm tác giả sẽ giới thiệu trong bài báo tiếp theo.

TÀI LIỆU THAM KHẢO

[1] T. ElGamal. "A public key cryptosystem and signature scheme based on discrete logarithms," IEEE Transaction on Information Theory. 1985, IT-31(4): pp. 469 - 472.

[2] W. C. Kuo, "On ElGamal Signature Scheme," *Future Generation Communication and Networking (FGCN 2007)*, Jeju, 2007, pp. 151-153

[3] C. P. Schnorr, "Efficient signaturegeneration for smartcards," Journal of Cryptology Vol. 4, pp. 161-174, 1991.

[4] T. S. Ng, S. Y. Tan and J. J. Chin, "A variant of Schnorr signature scheme with tight security reduction," *2017 International Conference on Information and Communication Technology Convergence (ICTC)*, Jeju Island, Korea (South), 2017, pp. 411-415.

[5] H. Morita, J.C. Schuldt, T. Matsuda, G. Hanaoka, T. Iwata. "On the security of the schnorr signature scheme and DSA against related key attacks." International Conference on Information Security and Cryptology – CRYPTOLOGY '15, pp. 20—35, Springer, 2015.

[6] National Institute of Standards and Technology (NIST), FIPS Publication 186: Digital Signature Standards (DSS)(1994)

[7] Sung-Ming Yen and Chi-Sung Laih, "Improved digital signature algorithm," *in IEEE Transactions on Computers*, vol. 44, no. 5, pp. 729-730, May 1995.

[8] Z. M. Chen. "An inproved encryption algorithm on ELGamal algorithm," Computer Applications and Sostware, vol. 22. 2005, pp.82- 85.

[9] J.-m.Liu,X.-g.Cheng,andX.-m.Wang,"Methods to forge elgamal signatures and determine secret key,"in Advanced Information Networking and Applications, 2006. AINA 2006.20th International Conferenceon, vol.1.IEEE, 2006, pp. 859—862

[10] L. Xiao-fei, S. Xuan-jing and C. Hai-peng, "An Improved ElGamal Digital Signature Algorithm Based on Adding a Random Number" *2010 Second International Conference on Networks Security, Wireless Communications and Trusted Computing*, Wuhan, Hubei, 2010, pp. 236-240.

.

[11] Z. *Meng*, S. Wang and S. Nu, "A DSA Multi-Signature Protocol and Applying in E-Bank and E-Voting," 2010 2nd International Conference on E-business and Information System Security, Wuhan, 2010, pp.1-5.

[12] X.Li,X.Shen,andH.Chen,"Elgamal digital signature algorithm of adding a random number," Journal of Networks,vol.6, no.5, pp.774—782, 2011.

[13] C. Y. Lu, W. C. Yang and C. S. Laih, "Efficient Modular Exponentiation Resistant to Simple Power Analysis in DSA-Like Systems," 2010 International Conference on Broadband, Wireless Computing, communication and Applications, Fukuoka, 2010, pp. 401-406.

[14] Z. Ping, K. Yingzhan and J. Keke, "Instruction-Cache Attack on DSA Adopting Square-Multiply Method," 2012 Second International Conference on Instrumentation, Measurement, Computer, Communication and Control, Harbin, 2012, pp. 905-908 6-11.

[15] B. Yang, "A DSA-Based and Efficient Scheme for Preventing IP Prefix Hijacking," 2014 International Conference on Management of e-Commerce and e-Government, Shanghai, 2014, pp. 87-92.

[16] Z. Ping, W. Tao and C. Hao, "Research on L3 Cache Timing Attack against DSA Adopting Square-and-Multiply Algorithm," 2015 Fifth International Conference on Instrumentation and Measurement, Computer, Communication and Control (IMCCC), Qinhuangdao, 2015, pp. 1390-1393.

[17] J. M. Pollard, Monte carlo methods for index computation (mod p), Mathematics of Computation 32 (1978), no. 143, 918-924.

[18] Stephen C. Pohlig and Martin E. Hellman, "An improved algoritm for computing logarithms over GF(p) and its cryptographic significance , IEEE Transaction Theory IT-24 (1979), no. 1, 106-110.

[19] M. Girault, "An identity-based identification scheme based on discrete logarithms modulo a composite number" In Advances in Cryptology - Eumcrypt'SO, Lecture Notes in Computer Science 473, Springer-Verlag, pp.481-486, 1991.

[20] Chik How Tan, Xun Yi and Chee Kheong Siew, "Signature scheme based on composite discrete logarithm," Fourth International Conference on Information, Communications and Signal Processing, 2003 and the Fourth Pacific Rim Conference on Multimedia. Proceedings of the 2003 Joint, 2003, pp. 1702-1706

[21] S. K. Tripathi and B. Gupta, "An efficient digital signature scheme by using integer factorization and discrete logarithm problem," *2017 International Conference on Advances in Computing, Communications and Informatics (ICACCI),* Udupi, 2017, pp. 1261-1266.

[22] E. Okamoto and K. Tanaka, "Key distribution system based on identification information," in *IEEE Journal on Selected Areas in Communications*, vol. 7, no. 4, pp. 481-485, May 1989.

[23] Boyd, C.Digital signature and public key cryptosystem in a prime order subgroup of Z_n^*. First International Conference on Information and Communications Security, ICICS' 97 (LNCS1334), pages 346-355.Springer,1997.

[25] E. Okamoto and K. Tanaka, "Key distribution system based on identification information," in *IEEE Journal on* Selected *Areas in Communications*, vol. 7, no. 4, pp. 481-485, May 1989.

[26] Tuan Le Van, Truyen Bui The "Developping pollard algorithm to compute order of elements in $\mathbb{Z}_n^*$". The research journal of military science and technology, No.42, 04- 2016, ISSN 1859 — 1043

[27] D.R Stinson, "Cryptography Theory and Practice", CRC Press, pp 176, 2003

[28] Tuan Le Van, Truyen Bui The "Building a method for deterministic prime generation", The research journal of military science and technology, No.42, 04- 2016, ISSN 1859 — 1043.

[29] Richard Crandall, Carl Pomerance. "Prime Numbers, A Computational Perspective", Second Edition, Springer Science + Business Media, Inc, 2005.

[30] L. Harn, M. Mehta and Wen-Jung Hsin, "Integrating Diffie-Hellman key exchange into the digital signature algorithm (DSA)," in *IEEE Communications Letters*, vol. 8, no. 3, pp. 198-200, March 2004.

.

Tác giả liên hệ: Lê Văn Tuấn
Email: levantuan71@yahoo.com
Đến toàn soạn: 4/2018 , chỉnh sửa: 5/2018 , chấp nhận đăng: 6/2018

DEVELOPING A NEW SIGNATURE SCHEME ITS SECURITY BASED ON THE DISCRETE LOGARITHMIC PROBLEM ON RING Z_N

Abstract: In 1985, ElGamal proposed a digital signature scheme that based on prime discrete logarithm. Until now, there have been many research results that pointed out the two these scheme be insecure from some basic types of attacks, such as: forgy attacks base on session key revealing or session key coinciding. In this paper, we proposed a digital signature scheme in which the security is based on composite discrete problem. The proposed scheme overcame the disadvantages of two signature schemes above and it can be applied into practice.

Keywords: Digital Signature Scheme, Discrete logarithmic problem, order problem, Hash Function

Sinh năm 1972. Tốt nghiệp Khoa toán Đại học Thái Nguyên 1992; Năm 2000, nhận bằng kỹ sư CNTT tại Đại học Bách Khoa Hà Nội; Tốt nghiệp Thạc sỹ CNTT tại Học viện Kỹ thuật Quân sự năm 2007. Hiện là nghiên cứu sinh năm thứ 3 tại Học viện Kỹ thuật Quân sự.

Lĩnh vực nghiên cứu: An toàn và bảo mật thông tin.

Tel 0989394556

Email: levantuan71@yahoo.com

Tốt nghiệp Học viện Kỹ thuật Quân sự (HVKTQS) năm 2000. Nhận bằng Tiến sỹ tại LB Nga năm 2008. Hiện là Viện phó – Viện Công nghệ mô phỏng – HVKTQS. Hướng nghiên cứu: Mô phỏng - thực tại ảo, Công nghệ 3D, Mật mã và An toàn toàn thông tin.

Tel 0985245868

Email: Buithetruyen@gmai.co

Lều Đức Tân, Sinh năm 1948, tốt nghiệp Khoa toán Đại học Tổng hợp Hà Nội năm 1972; nhận bằng tiến sỹ toán học năm 1994, nguyên là Phó phân viện trưởng Phân viện Nghiên cứu Khoa học Mật mã thuộc Học viện KTMM Ban Cơ yếu Chính phủ nay đã nghỉ hưu. Lĩnh vực nghiên cứu toán học - an toàn và bảo mật thông tin.

Tel: 0978254363