Kỷ yếu Hội nghị Khoa học Quốc gia lần thứ IX "Nghiên cứu cơ bản và ứng dụng Công nghệ thông tin (FAIR'9)"; Cần Thơ, ngày 4-5/8/2016
DOI: 10.15625/vap.2016.00055

MỘT PHƯƠNG PHÁP XÂY DỰNG LƯỢC ĐỒ CHỮ KÝ SỐ DỰA TRÊN BÀI TOÁN LOGARIT RỜI RẠC

Lưu Hồng Dũng [1], Nguyễn Đức Thụy[2], Lê Đình Sơn[3], Nguyễn Thị Thu Thủy[4]

[1] Khoa Công nghệ thông tin, Học viện Kỹ thuật Quân sự
[2] Khoa Công nghệ thông tin, Cao đẳng Kinh tế - Kỹ thuật Tp. Hồ Chí Minh
[3] Phòng SĐH, Học viện Kỹ thuật Quân sự
[4] Khoa Cơ bản, Cao đẳng Kinh tế - Kỹ thuật Quảng Nam

luuhongdung@gmail.com, thuyphulam2013@gmail.com, sonld2004@gmail.com, thuytoankhcb@gmail.com

TÓM TẮT— *Bài báo đề xuất một phương pháp xây dựng lược đồ chữ ký số dựa trên tính khó của bài toán logarit rời rạc. Từ phương pháp được đề xuất có thể triển khai ra các lược đồ chữ ký khác nhau để lựa chọn phù hợp cho các ứng dụng trong thực tế.*

Từ khóa— *Chữ ký số, lược đồ chữ ký số, thuật toán chữ ký số, bài toán logarit rời rạc.*

I. ĐẶT VẤN ĐỀ

Lược đồ chữ ký số xây dựng trên bài toán logarit rời rạc lần đầu tiên được T. ElGamal [1] đề xuất vào năm 1985. Phương pháp xây dựng lược đồ chữ ký của ElGamal đã được sử dụng trong nhiều lược đồ chữ ký phát triển sau đó, mà quan trọng nhất là lược đồ chữ ký Schnorr [2] với việc cải tiến các tham số hệ thống nhằm cho phép rút gọn độ dài chữ ký và giảm độ phức tạp tính toán trong các thủ tục sinh và kiểm tra chữ ký. Các chuẩn chữ ký số của Hoa Kỳ [3], Nga [4], … đều được xây dựng trên cơ sở kết hợp phương pháp của ElGamal và Schnorr. Các lược đồ chữ ký này được gọi chung là họ chữ ký ElGamal. Trong [5] các tác giả đề xuất một phương pháp xây dựng lược đồ chữ ký số được phát triển từ phương pháp xây dựng của họ chữ ký ElGamal, ưu điểm của phương pháp đề xuất là có thể phát triển được nhiều lược đồ chữ ký khác nhau cho các ứng dụng thực tế.

Trong bài báo này, nhóm tác giả tiếp tục đề xuất một phương pháp xây dựng lược đồ chữ ký số dựa trên tính khó của bài toán logarit rời rạc, tuy nhiên phương pháp đề xuất ở đây có nguyên tắc thiết kế hoàn toàn khác với phương pháp xây dựng của họ chữ ký ElGamal. Tương tự [5], ưu điểm của phương pháp mới đề xuất ở đây là từ đó có thể phát triển được nhiều lược đồ chữ ký khác nhau để lựa chọn phù hợp với yêu cầu của các ứng dụng trong thực tế. Hiện tại, chưa có các kết quả nghiên cứu tương tự được công bố ở trong và ngoài nước.

II. XÂY DỰNG LƯỢC ĐỒ CHỮ KÝ SỐ TRÊN BÀI TOÁN LOGARIT RỜI RẠC

A. Phương pháp xây dựng lược đồ chữ ký trên bài toán logarit rời rạc

1. Bài toán logarit rời rạc

Cho p là số nguyên tố, g là phần tử sinh của nhóm $\mathbb{Z}_p^*$. Khi đó bài toán logarit rời rạc trên trường hữu hạn nguyên tố $DLP_{(p,g)}$ được phát biểu như sau:

Bài toán $DLP_{(g,p)}$: Với mỗi số nguyên dương $y \in \mathbb{Z}_p^*$, hãy tìm x thỏa mãn phương trình:

$$g^x \bmod p = y \tag{1.1}$$

Giải thuật cho bài toán $DLP_{(g,p)}$ có thể được viết như một thuật toán tính hàm $DLP_{(g,p)}(.)$ với biến đầu vào là y còn giá trị hàm là nghiệm x của phương trình (1.1):

$$x = DLP_{(g,p)}(y) \tag{1.2}$$

Dạng lược đồ chữ ký xây dựng theo phương pháp mới đề xuất ở đây cho phép các thực thể ký trong cùng một hệ thống có thể dùng chung bộ tham số $\{g, p\}$, trong đó mỗi thành viên **U** của hệ thống tự chọn cho mình khóa bí mật x thỏa mãn: $1 < x < (p-1)$, tính và công khai tham số:

$$y = g^x \bmod p \tag{1.3}$$

<u>*Chú ý*</u>:

(i) Mặc dù bài toán $DLP_{(g,p)}$ là khó, tuy nhiên không phải với mọi $y \in \mathbb{Z}_p^*$ thì việc tính $DLP_{(g,p)}(y)$ đều khó, chẳng hạn những $y = g^x \bmod p$, với x không đủ lớn thì bằng cách duyệt dần x = 1, 2, ... cho đến khi tìm được nghiệm của (1.2) ta sẽ tìm được khóa bí mật x, do đó các tham số mật x phải được lựa chọn sao cho việc tính $DLP_{(g,p)}(y)$ đều khó.

(ii) Với lựa chọn x nêu trên, chỉ có người ký U biết được giá trị x, vì vậy việc biết được x đủ để xác thực đó là U.

B. *Xây dựng lược đồ chữ ký số trên bài toán $DLP_{(p,g)}$*

Dạng lược đồ mới đề xuất ở đây xây dựng dựa trên tính khó giải của bài toán $DLP_{(g,p)}$ và được thiết kế theo dạng lược đồ sinh chữ ký 2 thành phần tương tự như DSA trong chuẩn chữ ký số DSS (Digital Signature Standard) của Hoa Kỳ [3] hay GOST R34.10-94 [4] của Liên bang Nga. Giả sử rằng khóa bí mật của người ký là *x* được chọn ngẫu nhiên trong khoảng $(1, p)$ và khóa công khai tương ứng *y* được hình thành từ *x* theo (1.3):

$$y = g^x \bmod p$$

Ở đây *p* là số nguyên tố được chọn sao cho việc giải bài toán $DLP_{(g,p)}(y)$ là khó, *g* là phần tử sinh của nhóm $\mathbb{Z}_p^*$ có bậc là *q*, với *q*|(*p-1*).

Giả sử (r,v) là chữ ký lên bản tin M, *u* là 1 giá trị: 1 < u < q và *r* được tính từ *u* theo công thức:

$$r = g^u \bmod p \tag{1.4}$$

và *v* là một giá trị được tính từ *s* theo công thức:

$$v = g^s \bmod p \tag{1.5}$$

Cũng giả thiết rằng phương trình kiểm tra của lược đồ có dạng:

$$v^{f_1(M,f(r,s))} \equiv r^{f_2(M,f(r,s))} \times y^{f_3(M,f(r,s))} \bmod p$$

Ở đây $f(r,s)$ là hàm của *r* và *s*. Do (1.5), nên $f(r,s)$ có thể biểu diễn dưới dạng hàm của *r* và *v*: $f(r,s) = F(r,v)$ và được lựa chọn khác nhau trong các trường hợp cụ thể, ví dụ như: $F(r,v) = r \times v^{-1}$, $F(r,v) = r^{-1} \times v$, $F(r,v) = r \times v^2$, $F(r,v) = r^2 \times v, \ldots$

Xét trường hợp: $f(r,s) = F(r,v) = r \times v \bmod p = r \times g^s \bmod p$ (1.6)

và: $f(r,s) = F(r,v) = g^k \bmod p$ (1.7)

với *k* được chọn ngẫu nhiên trong khoảng $(1,q)$. Đặt: $g^k \bmod p = Z$, khi đó ta có: $f(r,s) = F(r,v) = Z$, nên có thể đưa phương trình kiểm tra về dạng:

$$g^{s \cdot f_1(M,Z)} \equiv g^{u \cdot f_2(M,Z)} \times g^{x \cdot f_3(M,Z)} \bmod p \tag{1.8}$$

Từ (1.1), (1.3), (1.4) và (1.8) ta có:

$$s \times f_1(M,Z) \equiv \left(u \times f_2(M,Z) + x \times f_3(M,Z)\right) \bmod q \tag{1.9}$$

Từ (1.9) suy ra:

$$s = \left(u \times f_1(M,Z)^{-1} \times f_2(M,Z) + x \times f_1(M,Z)^{-1} \times f_3(M,Z)\right) \bmod q \tag{1.10}$$

Mặt khác, từ (1.6) và (1.7) ta có:

$$\left(s + u\right) \bmod q = k \tag{1.11}$$

Từ (1.10) và (1.11) ta có:

$$\left(u \times f_1(M,Z)^{-1} \times f_2(M,Z) + x \times f_1(M,Z)^{-1} \times f_3(M,Z) + u\right) \bmod q = k$$

hay:

$$\left(u \times (f_1(M,Z)^{-1} \times f_2(M,Z) + 1) + x \times f_1(M,Z)^{-1} \times f_3(M,Z)\right) \bmod q = k$$

suy ra:

$$u = \left(f_1(M,Z)^{-1} \times f_2(M,Z) + 1\right)^{-1} \times (k - x \times f_1(M,Z)^{-1} \times f_3(M,Z)) \bmod q \tag{1.12}$$

Từ (1.12), thành phần thứ nhất của chữ ký được tính theo (1.4):

$$r = g^u \bmod p$$

và thành phần thứ 2 được tính theo (1.10):

$$s = \left(u \times f_1(M,Z)^{-1} \times f_2(M,Z) + x \times f_1(M,Z)^{-1} \times f_3(M,Z)\right) \bmod q$$

Từ đây, một dạng lược đồ chữ ký tương ứng với trường hợp: $F(r,v) = r \times v \bmod p = g^k \bmod p$ được chỉ ra như các Bảng 1, Bảng 2 và Bảng 3 dưới đây.

Bảng 1. Thuật toán hình thành tham số và khóa

Input: *p, q, x*.
Output: *g, y*.

[1]. **select** *h*: $1 < h < p$
[2]. $g \leftarrow h^{(p-1)/q} \bmod p$
[3]. **if** (g = 1) **then goto** [1]
[4]. $y \leftarrow g^x \bmod p$
[5]. **return** {g,y}

Chú thích:

(i) p,q: các số nguyên tố thỏa mãn điều kiện: $p = N \times q + 1$, *N=1,2,3,....*

(ii) x,y: khóa bí mật, công khai của đối tượng ký **U**.

Bảng 2. Thuật toán hình thành chữ ký

Input: *p, q, g, x, M*.
Output: (*r,s*).

[1]. **select** *k*: $1 < k < q$
[2]. $Z \leftarrow g^k \bmod p$ (1.13)
[3]. $w_1 \leftarrow f_1(M, Z)$
[4]. $\overline{w}_1 \leftarrow (w_1)^{-1} \bmod q$
[5]. $w_2 \leftarrow f_2(M, Z)$
[6]. $w \leftarrow \overline{w}_1 \times w_2$
[7]. **if** $(\gcd(w+1, q) \neq 1)$ **goto** [1]
[8]. $w_3 \leftarrow f_3(M, Z)$
[9]. $u \leftarrow (w+1)^{-1} \times (k - x \times \overline{w}_1 \times w_3) \bmod q$ (1.14)
[10]. $r \leftarrow g^u \bmod p$ (1.15)
[11]. $s \leftarrow (u \times w + x \times \overline{w}_1 \times w_3) \bmod q$ (1.16)
[12]. **return** (*r,s*)

Chú thích:

(i) M: bản tin cần ký, với: $M \in \{0,1\}^{\infty}$.

(ii) (r,s): chữ ký của **U** lên M.

Bảng 3. Thuật toán kiểm tra chữ ký

Input: *p, q, g, y,* {*M,*(*r,s*)}.
Output: *true* / *false* .

[1]. $Z \leftarrow f(r, s)$
[2]. $w_1 \leftarrow f_1(M, Z)$
[3]. $w_2 \leftarrow f_2(M, Z)$
[4]. $w_3 \leftarrow f_3(M, Z)$
[5]. $A \leftarrow g^{s.w_1} \bmod p$ (1.17)
[6]. $B \leftarrow r^{w_2} \times y^{w_3} \bmod p$ (1.18)
[7]. **if** ($A = B$) **then** {**return** *true* }
else {**return** *false* }

Chú thích:

(i) M, (r,s): bản tin, chữ ký cần thẩm tra.

(ii) Nếu kết quả trả về là *true* thì tính toàn vẹn và nguồn gốc của M được khẳng định. Ngược lại, nếu kết quả là *false* thì M bị phủ nhận về nguồn gốc và tính toàn vẹn.

1. Tính đúng đắn của dạng lược đồ mới đề xuất

Điều cần chứng minh ở đây là: cho *p, q* là 2 số nguyên tố với $q|(p-1)$, $1<h<p$, $g=h^{(p-1)/q} \bmod p$, $1<k,x<q$, $y=g^x \bmod p$, $Z=f(r,s)=g^k \bmod p$, $w_1=f_1(M,Z)$, $\overline{w}_1=(w_1)^{-1} \bmod q$, $w_2=f_2(M,Z)$, $w=\overline{w}_1 \times w_2$, $\gcd(w+1,q)=1$, $w_3=f_3(M,Z)$, $u=(w+1)^{-1}\times(k-x\times\overline{w}_1\times w_3) \bmod q$, $r=g^u \bmod p$, $s=(u\times w+x\times\overline{w}_1\times w_3) \bmod q$. Nếu: $A=g^{s.w_1} \bmod p$, $B=r^{w_2}\times y^{w_3} \bmod p$ thì: $A=B$.

Tính đúng đắn của lược đồ dạng tổng quát có thể được chứng minh như sau:

Từ (1.17) và (1.18) ta có:

$$\begin{aligned} A &= g^{s.w_1} \bmod p = g^{s.f_1(M,Z)} \bmod p \\ &= g^{\left(u.f_1(M,Z)^{-1}.f_2(M,Z)+x.f_1(M,Z)^{-1}.f_3(M,Z)\right).f_1(M,Z)} \bmod p \\ &= g^{u.f_2(M,Z)+x.f_3(M,Z)} \bmod p \end{aligned} \quad (1.19)$$

Từ (1.14) và (1.19) ta lại có:

$$\begin{aligned} B &= r^{w_2}\times y^{w_3} \bmod p = g^{u.f_2(M,Z)}\times g^{x.f3(M,Z)} \bmod p \\ &= g^{u.f_2(M,Z)+x.f_3(M,Z)} \bmod p \end{aligned} \quad (1.20)$$

Từ (1.19) và (1.20) suy ra: $A=B$. Đây là điều cần chứng minh.

C. *Một lược đồ chữ ký phát triển theo phương pháp mới đề xuất*

Lược đồ chữ ký LD 16.5-01

Lược đồ chữ ký - ký hiệu LD 16.5-01, được phát triển từ dạng lược đồ mới đề xuất với các lựa chọn: $f_1(M,Z)=Z$, $f_2(M,Z)=H(M)$, $f_3(M,Z)=Z$, ở đây H(.) là hàm băm và H(M) là giá trị đại diện của bản tin M. Các thuật toán hình thành tham số và khóa, thuật toán ký và kiểm tra chữ ký của lược đồ được mô tả trong các Bảng 4, Bảng 5 và Bảng 6 dưới đây.

Bảng 4. Thuật toán hình thành tham số và khóa

Input: *p, q, x.* **Output**: *g, y, H(.).*	
[1]. **select** *h*: $1<h<p$	
[2]. $g \leftarrow h^{(p-1)/q} \bmod p$	
[3]. **if** (g = 1) **then goto** [1]	
[4]. $y \leftarrow g^x \bmod p$	(2.1)
[5]. **select** $H:\{0,1\}^* \mapsto Z_t$, $q<t<p$	
[6]. **return** {*g,y,H(.)*}	

Bảng 5. Thuật toán ký

Input: *p, q, g, x, M* – bản tin cần ký. **Output**: (*r,s*) – chữ ký của **U** lên M.	
[1]. $E=H(M)$	
[2]. **select** *k*: $1<k<q$	
[3]. $Z \leftarrow g^k \bmod p$	(2.2)
[4]. **if** ($(\gcd(Z,q)\neq 1)$ OR $(\gcd(Z^{-1}\times E+1,q)\neq 1)$) **then goto** [2]	
[5]. $u \leftarrow (Z^{-1}\times E+1)^{-1}\times(k-x) \bmod q$	
[6]. $r \leftarrow g^u \bmod p$	(2.3)
[7]. $s \leftarrow (u\times Z^{-1}\times E+x) \bmod q$	(2.4)
[8]. **return** (*r,s*)	

Bảng 6. Thuật toán kiểm tra

Input*: p, q, g, y, M, (r,s).* **Output**: *true* / *false* .	
[1]. $E=H(M)$	
[2]. $w \leftarrow r\times g^s \bmod p$	
[3]. $A \leftarrow g^{s.w} \bmod p$	(2.5)
[4]. $B \leftarrow r^E \times y^w \bmod p$	(2.6)
[5]. **if** ($A=B$) **then** {**return** *true* } **else** {**return** *false* }	

2. Tính đúng đắn của lược đồ LD 16.5 - 01

Điều cần chứng minh ở đây là: Cho *p, q* là 2 số nguyên tố với *q*|(*p-1*), $H:\{0,1\}^{*}\mapsto Z_n$, $q<n<p$, $1<k,x<q$, $y=g^x \bmod p$, $Z=g^k \bmod p$, $E=H(M)$, $u=\left(Z^{-1}\times E+1\right)^{-1}\times(k-x)\bmod q$, $r=g^u \bmod p$, $s=\left(u\times Z^{-1}\times E+x\right)\bmod q$. Nếu: $W = r\times g^s \bmod p$, $A=g^{s.W} \bmod p$, $B=r^E\times y^W \bmod p$ thì: $A=B$.

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

Từ (2.2), (2.3), (2.4) và (2.5) ta có:

$$\begin{aligned} A &= g^{s.W} \bmod p = g^{s.\left(g^s.r \bmod p\right)} \bmod p \\ &= g^{s.(r.v \bmod p)} \bmod p = g^{s.Z} \bmod p \\ &= g^{\left(u.Z^{-1}.E+x\right).Z} \bmod p = g^{u.E+x.Z} \bmod p \end{aligned} \tag{2.7}$$

Từ (2.1), (2.2), (2.3) và (2.6) ta lại có:

$$\begin{aligned} B &= r^E\times y^W \bmod p = g^{u.E}\times g^{x.\left(g^s.r \bmod p\right)} \bmod p \\ &= g^{u.E}\times g^{x.(r.v \bmod p)} \bmod p = g^{u.E+x.Z} \end{aligned} \tag{2.8}$$

Từ (2.7) và (2.8) suy ra: $A=B$

Đây là điều cần chứng minh.

3. Mức độ an toàn của lược đồ LD 16.5-01

Ở dạng lược đồ mới đề xuất, khóa công khai được hình thành từ khóa bí mật dựa trên tính khó giải của bài toán logarit rời rạc trên trường hữu hạn nguyên tố $DLP_{(g,p)}$. Vì vậy, nếu các tham số {*p,q,g*} được chọn để bài toán $DLP_{(g,p)}$ là khó thì mức độ an toàn của lược đồ mới đề xuất xét theo khả năng chống tấn công làm lộ khóa mật sẽ được đánh giá bằng mức độ khó của bài toán $DLP_{(g,p)}$. Cần chú ý rằng, để bài toán DLP là khó thì các tham số {*p,q,g,n*} cần phải được lựa chọn tương tự như DSA [3] hay GOST R34.10-94 [4], với: $|p|\geq 512bit$, $|q|\geq 160bit$, $|n|\geq 160bit$.

Từ *Thuật toán kiểm tra* (Bảng 6) của lược đồ LD 16.5-01 cho thấy, một cặp (*r,s*) bất kỳ sẽ được công nhận là chữ ký hợp lệ của U lên một bản tin M nếu thỏa mãn điều kiện:

$$g^{s.\left(g^s.r \bmod p\right)} \equiv r^E\times y^{\left(g^s.r \bmod p\right)} \bmod p \tag{2.9}$$

Ở đây: U là đối tượng ký sở hữu khóa công khai *y* và $E=H(M)$ là giá trị đại diện của bản tin cần thẩm tra M. Từ các kết quả nghiên cứu đã được công bố, có thể thấy rằng việc tìm được một cặp (*r,s*) giả mạo thỏa mãn (2.9) là một dạng bài toán khó chưa có lời giải nếu các tham số {*p,q,n*} 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 phương pháp thiết kế lược đồ chữ số mới dựa trên tính khó giải của bài toán logarit rời rạc và có thể được sử dụng để phát triển các lược đồ lược đồ chữ ký khác nhau cho các ứng dụng thực tế. Bài báo cũng đề xuất một lược đồ chữ ký xây dựng theo phương pháp này (lược đồ LD 16.5 – 01), đã cho thấy tính khả thi của phương pháp được đề xuất. Mức độ an toàn và hiệu quả thực hiện của các lược đồ chữ ký phát triển theo phương pháp đề xuất ở đây phụ thuộc vào việc lựa chọn các hàm $f(r,s)$, $F(r,v)$, $f_{1,2,3}(M,Z)$ và các tham số hệ thống, nếu việc lựa chọn nói trên là hợp lý thì khả năng ứng dụng của các lược đồ dạng này trong thực tế là rất khả quan. Tuy nhiên, mục tiêu của bài báo chỉ giới hạn ở việc đề xuất một phương pháp xây dựng lược đồ chữ ký mới, nên ở đây việc triển khai ứng dụng phương pháp mới đề xuất để tạo ra các lược đồ chữ ký có độ an toàn và hiệu quả thực hiện cao, ví dụ như việc lựa chọn các hàm $f(r,s)$, $F(r,v)$, $f_{1,2,3}(M,Z)$,... đã không được đặt ra, đây sẽ là những vấn đề cần được nghiên cứu tiếp theo.

TÀI LIỆU THAM KHẢO

[1] T. ElGamal (1985). "A public key cryptosystem and a signature scheme based on discrete logarithms", IEEE Transactions on Information Theory. Vol. IT-31, No. 4. pp.469–472.

[2] C. P. Schnorr (1991). "Efficient signature generation by smart cards". *J. Cryptol*., 4(3):161–174.

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

[4] GOST R 34.10-94. Russian Federation Standard. Information Technology. Cryptographic data Security. *Produce and check procedures of Electronic Digital Signature based on Asymmetric Cryptographic Algorithm*. Government Committee of the Russia for Standards, 1994 (in Russian).

[5] Luu Hong Dung, Le Dinh Son, Ho Nhat Quang, Nguyen Duc Thuy (2015). "DEVELOPING DIGITAL SIGNATURE SCHEMES BASED ON DISCRETE LOGARITHM PROBLEM". Hội nghị khoa học Quốc gia lần thứ VIII về Nghiên cứu cơ bản và ứng dụng Công nghệ thông tin (FAIR 2015). ISBN: 978-604-913-397-8.

A NEW CONSTRUCTION METHOD OF DIGITAL SIGNATURE SCHEME BASED ON DISCRETE LOGARITHM PROBLEM

Luu Hong Dung, Nguyen Duc Thuy, Le Dinh Son, Nguyen Thi Thu Thuy

ABSTRACT*—This paper proposes methods for developing digital signature scheme based on the difficulty of the discrete logarithm problem. With the new method proposed, can develop some signature schemes for practical applications.*

Keywords*— Digital Signature, Digital Signature Schema, Digital Signature Algorithm, Discrete Logarithm Problem.*

.