MỘT LƯỢC ĐỒ CHỮ KÝ XÂY DỰNG TRÊN TÍNH KHÓ CỦA VIỆC GIẢI ĐỒNG THỜI 2 BÀI TOÁN LOGARIT RỜI RẠC VÀ PHÂN TÍCH SỐ

Nguyễn Vĩnh Thái[1], Lưu Hồng Dũng[2*]

Tóm tắt: *Bài báo đề xuất một lược đồ chữ ký số xây dựng dựa trên tính khó của việc giải đồng thời 2 bài toán logarit rời rạc trên Z_p với phân tích một số nguyên lớn ra các thừa số nguyên tố. Vì thế, thuật toán chữ ký mới đề xuất ở đây có thể đáp ứng được các ứng dụng có yêu cầu cao về độ an toàn trong thực tế.*

Từ khóa: Logarit rời rạc; Phân tích số; Khai căn; Thuật toán khóa mật mã; Hệ thống mã khóa khóa công khai.

1. ĐẶT VẤN ĐỀ

Nâng cao độ an toàn cho các thuật toán mật mã khóa công khai và chữ ký số dựa trên tính khó của việc giải đồng thời 2 bài toán khó là một hướng tiếp cận đang nhận được nhiều sự quan tâm của các nhà nghiên cứu [1-8]. Trong bài báo này, cũng với mục đích nâng cao độ an toàn cho thuật toán trước một số dạng tấn công trong thực tế, nhóm tác giả đề xuất một lược đồ chữ ký số được xây dựng dựa trên tính khó của việc giải đồng thời 2 bài toán logarit rời rạc trên Zp (bài toán logarit rời rạc) và bài toán phân tích một số nguyên lớn ra các thừa số nguyên tố (bài toán phân tích số). Ngoài việc nâng cao độ an toàn cho thuật toán như [1-8], lược đồ chữ ký được đề xuất ở đây còn cho phép các thực thể cuối (người ký) trong cùng một hệ thống có thể sử dụng chung một bộ tham số (tham số miền) do nhà cung cấp dịch vụ tạo ra. Do đó, có thể sử dụng lược đồ mới đề xuất trong việc xây dựng các giao thức mật mã nhằm chống lại các dạng tấn công giả mạo rất hiệu quả.

2. MỘT SỐ BÀI TOÁN KHÓ ỨNG DỤNG TRONG MẬT MÃ

2.1. Bài toán phân tích số

Bài toán phân tích số được phát biểu như sau: Cho số $n \in \mathbb{N}$, hãy tìm biểu diễn:

$n = \Pi_{i=1}^{k} p_i^{e_i}$ với: $e_i \geq 1$ $(i = 1, \dots, k)$ nguyên dương;

$p_i \geq 1$ $(i = 1, \dots, k)$ nguyên tố.

Một trường hợp riêng của bài toán phân tích số được ứng dụng để xây dựng hệ mật RSA mà ở đó n là tích của hai số nguyên tố p và q. Khi đó, bài toán phân tích số hay còn gọi là bài toán $IFP_{(n)}$ được phát biểu như sau:

Với mỗi số nguyên dương n, hãy tìm số nguyên tố p hoặc q thỏa mãn phương trình sau: $p \times q = n$

Giải thuật cho bài toán $IFP_{(n)}$ có thể được viết như một thuật toán tính hàm $IFP_{(.)}$ với biến đầu vào là n, còn giá trị hàm là p hoặc q của phương trình sau: $p = IFP_{(n)}$ hoặc: $q = IFP_{(n)}$

Trong hệ mật RSA [10], bài toán phân tích số được sử dụng trong việc hình thành cặp khóa công khai/bí mật cho mỗi thực thể ký. Với việc giữ bí mật các tham số (p, q) thì việc tính được khóa bí mật (d) từ khóa công khai (e) và $modulo(n)$ là một bài toán khó nếu p, q được chọn đủ lớn và mạnh. Hiện tại bài toán trên vẫn

được coi là bài toán khó do chưa có giải thuật thời gian đa thức hay đa thức xác suất cho nó và hệ mật RSA là một minh chứng thực tế cho tính khó giải của bài toán này. Trong thực tế, các tham số p, q có thể chọn theo FIPS 186 - 4 [9] của Hoa Kỳ cho hệ mật RSA.

2.2. Bài toán logarit rời rạc trên Z_p

Cho cặp số nguyên dương (p, g) với p là số nguyên tố, còn g là một phần tử của nhóm Z_p^*. Khi đó, bài toán logarit rời rạc trên Z_p hay còn gọi là bài toán $DLP_{(p,g)}$ được phát biểu như sau:

Với mỗi số nguyên dương $y \in \mathbb{Z}_p^*$, hãy tìm x thỏa mãn phương trình sau:

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

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

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

Bài toán $DLP_{(p,g)}$ là cơ sở để xây dựng nên hệ mật ElGamal [11]. Hiện tại chưa có giải thuật hiệu quả (thời gian đa thức hay đa thức xác suất) cho $DLP_{(p,g)}$ và độ an toàn của thuật toán DSA trong chuẩn chữ ký số DSS của Hoa Kỳ là một minh chứng thực tế cho tính khó giải của bài toán này.

3. XÂY DỰNG LƯỢC ĐỒ CHỮ KÝ DỰA TRÊN TÍNH KHÓ CỦA VIỆC GIẢI ĐỒNG THỜI 2 BÀI TOÁN LOGARIT RỜI RẠC VÀ PHÂN TÍCH SỐ

3.1. Thuật toán hình thành tham số và khóa

Các tham số hệ thống hay tham số miền được nhà cung cấp dịch vụ chứng thực số hình thành bằng thuật toán như sau:

a) **Thuật toán 1.** Hình thành các tham số hệ thống

Input: lp, lq - độ dài (tính theo bit) của các số nguyên tố p, q.

Output: p, q, g.

Bước 1. Chọn cặp số p, q nguyên tố với:

$$len(p) = lp, len(q) = lq \text{ sao cho } q|(p-1)$$

Bước 2. Chọn g là phần tử sinh của nhóm Z_p^* theo:

$$g = \alpha^{\frac{p-1}{q}} \bmod p \text{ , với } \alpha \in (1, p)$$

<u>*Chú thích:*</u> $len(.)$: hàm tính độ dài (theo bit) của một số.

Mỗi thực thể cuối/người sử dụng trong hệ thống hình thành khóa của mình bằng thuật toán như sau:

b) **Thuật toán 2.** Hình thành khóa

Input: p, q, g, lp_1, lq_1 - độ dài (tính theo bit) của các số nguyên tố p_1, q_1.

Output: x_1, x_2, n, y.

Bước 1. Chọn cặp số p_1, q_1 là các nguyên tố với:

$$len(p_1) = lp_1, len(q_1) = lq_1$$

Bước 2. Tính $n = p_1.q_1$, nếu $n \leq p$ thì thực hiện lại Bước 1.

Bước 3. Tính $\varphi(n) = (p_1 - 1).(q_1 - 1)$

Bước 4. Chọn giá trị bí mật thứ nhất x_1 trong khoảng $(1, q)$

Bước 5. Tính giá trị *y* theo:

$$y = (g)^{(x_1)^{-1}} \, mod \, p \tag{1}$$

Kiểm tra nếu: $y \geq \varphi(n)$ hoặc: gcd $(y, \varphi(n)) \neq 1$ thì thực hiện lại từ Bước 4.

Bước 6. Tính giá trị bí mật thứ hai x_2 theo:

$$x_2 = y^{-1} \, mod \, \varphi(n) \tag{2}$$

Bước 7. Chọn hàm băm $H: \{0,1\}^* \rightarrow Z_h$ với $q < h < p$

Chú thích:

- *p, q, g*: Tham số hệ thống (tham số miền).
- x_1, x_2: Khóa bí mật.
- *y, n*: Khóa công khai.

3.2. Thuật toán ký

a) **Thuật toán 3:** Sinh chữ ký

Input: *p, q , g,* $\varphi(n)$, x_1, x_2 M - bản tin cần ký

Output: E, S- chữ ký

Bước 1. Chọn ngẫu nhiên giá trị k trong khoảng $(1, q)$

Bước 2. Tính giá trị:

$$R = g^k \; mod \, p \tag{3}$$

Bước 3. Tính thành phần thứ nhất E của chữ ký theo:

$$E = H(M \| R) \, mod \, q \tag{4}$$

Bước 4. Tính thành phần thứ hai S của chữ ký theo:

$$S = (x_1 \times (k + E) \, mod \, q)^{x_2} \, mod \, n \tag{5}$$

Chú thích: toán tử "||": phép nối 2 xâu bit.

b) **Thuật toán 4:** Kiểm tra chữ ký

Input: *p, q , g, y, n, y, M* - bản tin cần thẩm tra.

Output: $(E, S) = True/False$

Bước 1. Tính giá trị:

$$\bar{R} = ((Y)^{(S)^y mod \, n} \times (g)^{-E}) \, mod \, p \tag{6}$$

Bước 2. Tính giá trị:

$$\overline{E} = H(M \| \overline{R}) \, mod \, q \tag{7}$$

Bước 3. Nếu $\overline{E} = E$ thì (E, S) = true; nếu $\overline{E} \neq E$ thì (E, S) = false

Chú thích:

+ (E, S) = *true*: chữ ký hợp lệ, bản tin M được xác thực về nguồn gốc và tính toàn vẹn.

+ (E, S) = *false*: chữ ký hoặc/và bản tin bị giả mạo.

3.3. Tính đúng đắn của thuật toán mới đề xuất

Điều cần chứng minh ở đây là: Cho *p, q* , p_1, q_1 là các số nguyên tố thỏa mãn:

$q|(p-1),\ n = p_1 \times q_1,\ n > p,\ 1 < \alpha < p,\ g = \alpha^{\frac{p-1}{q}} mod\, p,$

$\varphi(n) = (p_1 - 1) \times (q_1 - 1), 1 < x_1 < q, y = g^{(x_1)^{-1}} mod\, p,$

$x_2 = (y)^{-1} mod\, \varphi(n), 1 < k < \varphi(n), R = g^k\ mod\, p,$

$H: \{0,1\}^* \rightarrow Z_h$ với $q < h < p, E = H(M\|S)\ mod\, q,$

$S = (x_1 \times (k + E)\ mod\, q)^{x_2}\ mod\, n.$

Nếu: $\bar{R} = \left((y)^{(S)^y mod\, n} \times (g)^{-E}\right) mod\, p, \bar{E} = H(M\|\bar{R})\ mod\, q$ thì $\bar{E} = E$.

Chứng minh:

Thật vậy, từ (1), (2), (3), (5) và (6) ta có:

$$\bar{R} = \left((y)^{(S)^y mod\, n} \times (g)^{-E}\ mod\, n\right) mod\, p$$

$$= \left(\left((g)^{(x_1)^{-1}} mod\, p\right)^{((x_1.(k+E)\ mod\, q)^{x_2}\ mod\, n)^y\ mod\, n} \times (g)^{-E}\right) mod\, p \qquad (8)$$

$$= \left(\left((g)^{(x_1)^{-1}} mod\, p\right)^{x_1.(k+E)} \times (g)^{-E}\right)\ mod\, p$$

$$= \left((g)^{(x_1)^{-1}.x_1.(k+E)} \times (g)^{-E}\right) mod\, p$$

$$= \left((g)^{(k+E)} \times (g)^{-E}\right) mod\, p = g^k\ mod\, p = R$$

Từ (4), (7) và (8) suy ra điều phải chứng minh:

$$\bar{E} = H(M\|\bar{R})\ mod\, q = H(M\|R)\ mod\, q = E$$

3.4. Mức độ an toàn của thuật toán mới đề xuất

+ Tấn công khóa bí mật

Ở thuật toán mới đề xuất, khóa bí mật là tích của cặp giá trị bí mật (x_1, x_2), tính an toàn của lược đồ sẽ bị phá vỡ khi cặp giá trị này có thể tính được bởi một hay các đối tượng không mong muốn. Từ Thuật toán 1 và 2 cho thấy, để tìm được x_2 theo (2) cần phải tính được tham số $\varphi(n)$, nghĩa là phải giải được $IFP_{(n)}$, còn để tính được x_1 theo (1) cần phải giải được $\mathrm{DLP}_{(p,g)}$. Chú ý rằng, để tính x_1 và x_2 thì kẻ tấn công cần phải giải được (4). Như vậy, để tìm được cặp khóa bí mật này kẻ tấn công cần phải giải được bài toán $IFP_{(n)}$ và $\mathrm{DLP}_{(p,g)}$. Nói cách khác, độ an toàn về khóa của thuật toán được đảm bảo bằng độ khó của việc giải đồng thời 2 bài toán $IFP_{(n)}$ và $\mathrm{DLP}_{(p,g)}$.

+ Tấn công giả mạo chữ ký

Từ điều kiện của Thuật toán 3, một cặp (E, S) bất kỳ sẽ được coi là chữ ký hợp lệ của đối tượng sở hữu các tham số công khai (n, y) lên bản tin M nếu thỏa mãn:

$$E = H(M \| ((Y)^S \times (g)^E \ mod\ n)\ mod\ p) \quad (9)$$

Từ (9) dễ thấy rằng, nếu H(.) được chọn là hàm băm có tính kháng va chạm cao (SHA 256/512,...) thì việc tạo ngẫu nhiên được cặp (E, S) thỏa mãn điều kiện của thuật toán kiểm tra là không khả thi trong các ứng dụng thực tế.

4. VÍ DỤ

a) Sinh tham số và khóa (Thuật toán 1)

Input: $l_p = 512\ bit, l_q = 160\ bit$.

Output: *p, q, g*.

- Giá trị của p:

```
685857363474414004386405106019671223703726526241414741884633600249391 7
702168060878926124580494470033000377606407165437177859447702147545372956 04
2876888251
```

- Giá trị của q:

```
1444125853144354424502004519548090639867409116997
```

- Giá trị của g:

```
34979939775230902729431607715147514744199810701561488505347029310823 72
535057909888460636521733626327437707355959782021818714882194962847489964 57
0361083060
```

b) Sinh tham số và khóa (Thuật toán 2)

Input: $p, q, g, l_{p_1} = 512\ bit, l_{q_1} = 512\ bit$.

Output: x_1, x_2, n, y.

- Giá trị của l_{p_1}:

```
7117013613810786406784266560984396928363531519896578037730893999461553 
5882763795090985273794905074755078531610867212321266780908118386131096512 7
3978117011
```

- Giá trị của l_{q_1}:

```
1334329757731294897401625580595445900545276917576694146992975210732330 
7720372454570171584587354934006853845871961088857301617361647084440199745 0
51845491769
```

- Giá trị của n:

```
9496443051086474210661085099332286031499892570755668623556339140829830 
6785725544463327137399409570166614587767493989408969030356864441430594551 2
4547764635304805551880885511167794769536592653141143016979268630532817281 0
7725844829574450391458091974397248807640947080066874310978450267709684418 5
5024379919382459
```

- Giá trị của x_1:

```
125154856969555720555873875538030172910716794854 2
```

- Giá trị của y:

```
2070674479402476292663411626561047511804694262936235504384953725137336 
6474942228693400041472580222090436155086813115743733707690204718177856166 5
6853358639
```

- Giá trị của x_2:

```
   708459455046727517956482593765545651959784361209640202273734848040395 1
0671302972894583153826495104655520772641782926144014977718225205392437938 4
1838374157183610398678007409026563022737745862708943921600252515466529554 9
9662433530239184728678795132531555617455037181870996619051361102380467068 7
2101153968183999
```

c) Sinh chữ ký (Thuật toán 3)

Input: *p, q , g, n,* x_1, x_2, M

Output: E, S

- M = "THIS IS A NEW DIGITAL SIGNATURE ALGRITHM !"

- Giá trị của *k*:

```
116920107649460341130725560154197382429289485007 9
```

- Giá trị của *R* tính được:

```
   505406879415007709961735066696142167250793316462442993021945228081870 4
1249845550301174825677479938402910095483367279968678281796304529359378102 2
3496441786
```

- Giá trị của *E* tính được:

```
627576451934184254727264502918899024375785781807
```

- Giá trị của *S* tính được:

```
   325325933815136956874479355244422881471413761849605924617522979998138 9
0387851547577596065788073216745215827840581735432180216570878918756396970 8
0039642623156297654735230161713130710638499431304097451217564578934377980 5
7167300045664340528587104511826768170271413732747929834475984500440736105 4
0621904481369519
```

d) Kiểm tra chữ ký (Thuật toán 4)

Input: *p, q, g, n, y, M, (E,S)*

+ Trường hợp 1:

- Bản tin cần kiểm tra:

M = "THIS IS A NEW DIGITAL SIGNATURE ALGRITHM !"

- Giá trị của E cần kiểm tra:

```
627576451934184254727264502918899024375785781807
```

- Giá trị của S cần kiểm tra:

```
   325325933815136956874479355244422881471413761849605924617522979998138 9
0387851547577596065788073216745215827840581735432180216570878918756396970 8
0039642623156297654735230161713130710638499431304097451217564578934377980 5
7167300045664340528587104511826768170271413732747929834475984500440736105 4
0621904481369519
```

- Giá trị của $\bar{R}$ tính được:

```
   505406879415007709961735066696142167250793316462442993021945228081870 4
1249845550301174825677479938402910095483367279968678281796304529359378102 2
3496441786
```

- Giá trị của $\bar{E}$ tính được:

```
627576451934184254727264502918899024375785781807
```

Output: (E,S) = *true*.

+ Trường hợp 2: Bản tin bị giả mạo.

- Bản tin cần kiểm tra:

M = "THIS IS A NEW DIGITAL SIGNATURE ALGRITHM "

- Giá trị của E cần kiểm tra:

627576451934184254727264502918899024375785781807

- Giá trị của S cần kiểm tra:

802165708789187563969708003964262315629765473523016171313071063849943130409745121756457893437798057167300045664340528587104511826768170271413732747929834475984500440736105406219044813695 19

- Giá trị của $\bar{R}$ tính được:

505406879415007709961735066696142167250793316462442993021945228081870412498455503011748256774799384029100954833672799686782817963045293593781022349644178 6

- Giá trị của $\bar{E}$ tính được:

950375168932516035853278712792326895469172097430

Output: (E,S) = *false*.

+ Trường hợp 3: Thành phần S của chữ ký bị giả mạo.

- Bản tin cần kiểm tra:

M = "THIS IS A NEW DIGITAL SIGNATURE ALGRITHM !"

- Giá trị của E cần kiểm tra:

627576451934184254727264502918899024375785781807

- Giá trị của S cần kiểm tra:

802165708789187563969708003964262315629765473523016171313071063849943130409745121756457893437798057167300045664340528587104511826768170271413732747929834475984500440736105406219044813695 10

- Giá trị của $\bar{R}$ tính được:

505406879415007709961735066696142167250793316462442993021945228081870412498455503011748256774799384029100954833672799686782817963045293593781022349644178 6

- Giá trị của $\bar{E}$ tính được:

950375168932516035853278712792326895469172097430

Output: (E,S) = *false*.

5. KẾT LUẬN

Bài báo đề xuất xây dựng một lược đồ chữ ký có độ an toàn được đảm bảo bằng mức độ khó của việc giải đồng thời 2 bài toán: bài toán phân tích một số nguyên lớn ra các thừa số nguyên tố và bài toán logarit rời rạc. Có thể khẳng định rằng không có bất kỳ kiểu tấn công nào vào lược đồ thành công được mà không phải giải được đồng thời 2 bài toán khó nêu trên, do đó lược đồ mới đề xuất có thể phù hợp với các ứng dụng yêu cầu cao về độ an toàn trong thực tế.

TÀI LIỆU THAM KHẢO

[1]. Q. X. WU, Y. X. Yang and Z. M. HU, "*New signature schemes based on discrete logarithms and factoring*", Journal of Beijing University of Posts and Telecommunications, vol. 24, pp. 61-65, January 2001.

[2]. Z. Y. Shen and X. Y. Yu, "*Digital signature scheme based on discrete logarithms and factoring*", Information Technology, vol. 28,pp. 21-22, June 2004.

[3]. Shimin Wei, "*Digital Signature Scheme Based on Two Hard Problems*", IJCSNS International Journal of Computer Science and Network Security, VOL.7 No.12, December 2007.
[4]. Eddie Shahrie Ismail, Tahat N.M.F., Rokiah. R. Ahmad, "*A New Digital Signature Scheme Based on Factoring and Discrete Logarithms*", Journal of Mathematics and Statistics, 04/2008; 12(3). DOI: 10.3844/jmssp.2008.222.225 Source:DOAJ.
[5]. Qin Yanlin , Wu Xiaoping,"*New Digital Signature Scheme Based on both ECDLP and IFP*", Computer Science and Information Technology, 2009. ICCSIT 2009. 2nd IEEE International Conference on, 8-11 Aug. 2009, E-ISBN : 978-1-4244-4520-2, pp 348 - 351.
[6]. Swati Verma1, Birendra Kumar Sharma, "*A New Digital Signature Scheme Based on Two Hard Problems*", International Journal of Pure and Applied Sciences and Technology, ISSN 2229 – 6107, Int. J. Pure Appl. Sci. Technol., 5(2) (2011), pp. 55-59.
[7]. Sushila Vishnoi , Vishal Shrivastava, "*A new Digital Signature Algorithm based on Factorization and Discrete Logarithm problem*", International Journal of Computer Trends and Technology, volume 3, Issue 4, 2012.
[8]. A.N. Berezin, N.A. Moldovyan, V.A. Shcherbacov, "*Cryptoschemes Based on Difficulty of Simultaneous Solving Two Different Difficult Problems*", Computer Science Journal of Moldova, vol.21, no.2(62), 2013.
[9]. National Institute of Standards and Technology, NIST FIPS PUB 186-4. Digital Signature Standard, U.S. Department of Commerce, 2013.
[10]. R. L. Rivest, A. Shamir, and L. M. Adleman, "*A Method for Obtaining Digital Signatures and Public Key Cryptosystems*", Commun. of the ACM, Vol. 21, No. 2, 1978, pp. 120-126.
[11]. T. ElGamal, "*A public key cryptosystem and a signature scheme based on discrete logarithms*", IEEE Transactions on Information Theory 1985, Vol. IT-31, No. 4. pp.469–472.

ABSTRACT

A NEW DIGITAL SIGNATURE SCHEME BASED ON FACTORING AND DISCRETE LOGARITHMS

The paper proposes a digital signature scheme based on the difficulty of simultaneous solving two discrete logarithm problems with integer factoring problems. Therefore, the new signature algorithm proposed here can meet applications with high security demands on actual security.

Keywords: Digital Signature Algorithm; Public - Key Cryptography Algorithm; Public - Key CryptoSystem; Discrete Logarithm Problem; Integer Factoring Problems.

Nhận bài ngày 21 tháng 12 năm 2018
Hoàn thiện ngày 12 tháng 3 năm 2019
Chấp nhận đăng ngày 25 tháng 3 năm 2019

Địa chỉ: [1]Viện CNTT, Viện KH và CNQS;
[2] Khoa CNTT, Học viện KTQS.
[*] Email: luuhongdung@gmail.com.