XÂY DỰNG LƯỢC ĐỒ CHỮ KÝ SỐ DỰA TRÊN BÀI TOÁN LOGARIT RỜI RẠC KẾT HỢP KHAI CĂN TRÊN Z_p

A CONSTRUCTION METHOD OF DIGITAL SIGNATURE SCHEME BASED ON THE DISCRETE LOGARIT COMBINING FINDING ROOT PROBLEM ON Z_P

Nguyễn Đức Thụy[1], Bùi Tất Hiếu[2], Lưu Hồng Dũng[3]

[1]Trường Cao đẳng Kinh tế - Kỹ thuật Tp.HCM; thuyphulam2013@gmail.com
[2]Trường Cao đẳng Du lịch Hà Nội; buitathieu@yahoo.com
[3]Học viện Kỹ thuật Quân sự; luuhongdung@gmail.com

Tóm tắt - Các lược đồ chữ ký số thường được xây dựng dựa trên một số bài toán khó đã được nghiên cứu kỹ lưỡng. Các DSS được biết đến nhiều nhất dựa trên ba bài toán khó sau đây: 1). Bài toán phân tích một số nguyên lớn ra các thừa số nguyên tố: n = p.q, ở đây p và q là các số nguyên tố lớn; 2). Bài toán logarit rời rạc trên trường hữu hạn nguyên tố Z_p; 3). Bài toán logarit rời rạc trong một nhóm các điểm trên một số đường cong eliptic. Bài báo đề xuất xây dựng lược đồ chữ ký số dựa trên bài toán logarit rời rạc kết hợp khai căn trên Z_p, đây là một dạng bài toán khó mới, thuộc lớp các bài toán chưa có cách giải về mặt toán học. Việc xây dựng lược đồ chữ ký số dựa trên tính khó của bài toán logarit rời rạc kết hợp khai căn này cho phép nâng cao độ an toàn của thuật toán.

Từ khóa - Chữ ký số; thuật toán chữ ký số; lược đồ chữ ký số; bài toán Logarit rời rạc; bài toán khai căn

Abstract - The digital signature schemes (DSSes) are based on some well investigated hard computational problems. The most efficient known DSSes are based on the following three difficult problems: 1). Factorization of a composite number n = p.q, where p and q are two large primes; 2). Finding discrete logarithm modulo large prime number Z_p; 3). Finding discrete logarithm in a group of points of some elliptic curve. The paper proposes building a digital signature scheme based on the difficulty of the discrete logarithm combining finding root problem on Z_p,.This problem is a new difficult problem type, the problems class without mathematical solution. Building a digital signature scheme based on the difficulty of the discrete logarithm combining finding root problem allows us to improve the security of the algorithm.

Key words - Digital signature; Digital signature algorithm; Digital Signature Scheme (DSS); Discrete Logarithm Problem (DLP); Finding Root Problem (FRP)

1. Đặt vấn đề

Trong [9], đề xuất một phương pháp xây dựng thuật toán chữ ký số dựa trên tính khó của việc giải bài toán logarit rời rạc trên Zp. Ưu điểm của phương pháp mới đề xuất là từ đó có thể triển khai một lớp thuật toán chữ ký số cho các ứng dụng khác nhau. Tuy nhiên, độ an toàn của các thuật toán chữ ký được xây dựng theo phương pháp này chỉ được đảm bảo bởi độ khó của việc giải bài toán logarit rời rạc – DLP trên Zp. Do đó, nếu có một giải thuật thời gian đa thức cho bài toán này (DLP) thì tính an toàn của các thuật toán sẽ bị phá vỡ hoàn toàn. Nâng cao độ an toàn cho các thuật toán 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. Trong [10 – 17] các tác giả đã đề xuất một số thuật toán chữ ký xây dựng trên đồng thời hai bài toán phân tích số và logarit rời rạc. Trong bài báo này, cũng với mục đích nâng cao độ an toàn cho các thuật toán chữ ký số, nhóm tác giả tiếp tục phát triển phương pháp đề xuất trong [9] trên cơ sở tính khó giải của một bài toán mới, ở đây được gọi là bài toán logarit rời rạc kết hợp khai căn trên Zp, ký hiệu: DLRP (Discrete Logarithm combining Finding Root Problem). Đây là một dạng bài toán khó lần đầu được đề xuất và ứng dụng cho việc xây dựng thuật toán chữ ký số và có nhiều triển vọng cho phép xây dựng các thuật toán phù hợp với các ứng dụng thực tế đòi hỏi độ an toàn cao.

2. Bài toán khó mới và phương pháp xây dựng thuật toán chữ ký số

2.1. Bài toán logarit rời rạc - khai căn trên Zp

Bài toán logarit rời rạc kết hợp khai căn trên trường Zp được đề xuất ở đây có thể phát biểu như sau:

Với mỗi cặp số nguyên dương $(y_1, y_2) \in Z_p^*$, hãy tìm các số x_1 và x_2 thỏa mãn hệ phương trình sau:

$$\begin{cases} (x_1)^{x_1+x_2} \bmod p = y_1 \\ (x_1)^{(x_1)^{-1}.x_2} \bmod p = y_2 \end{cases}$$

Về mặt hình thức, nếu x_1 là hằng số, x_2 là biến cần tìm thì bài toán trên sẽ trở thành bài toán logarit rời rạc trên Z_p – DLP. Tuy nhiên, ở đây x_1 cũng là ẩn số như x_2, vì thế các giải thuật cho DLP không thể áp dụng với bài toán này. Tương tự, nếu x_2 là hằng số và x_1 là biến thì bài toán trên lại trở thành bài toán khai căn trên Z_p – FRP [18]. Song ở đây x_2 cũng là biến cần tìm, do vậy các giải thuật cho FRP cũng không áp dụng được đối với bài toán mới đề xuất. Trong toán học, bài toán trên thực chất là một hệ phương trình phi tuyến và thuộc lớp các bài toán chưa có cách giải, các giải thuật cho DLP và FRP hiện tại là không áp dụng được với bài toán này. Điều đó cho thấy, bài toán mới đề xuất ở đây có mức độ khó cao hơn DLP và FRP.

2.2. Xây dựng lược đồ chữ ký dựa trên tính khó của bài toán mới đề xuất

2.2.1. Thuật toán sinh khóa

Ở phương pháp xây dựng thuật toán chữ ký mới đề xuất, bài toán logarit rời rạc kết hợp khai căn trên *Zp* được sử dụng để hình thành cặp khóa bí mật và công khai của các đối tượng ký. Trong đó, p là tham số hệ thống (tham số miền) do nhà cung cấp dịch vụ tạo ra, ở đây p là số nguyên tố cần phải được chọn sao cho việc giải bài toán DLP là khó. Cặp (x_1, x_2) là khóa bí mật và (y_1,y_2) là các khóa công khai tương ứng của mỗi đối tượng ký trong hệ thống. Để tạo khóa x_1 mỗi thực thể ký cần tạo trước số nguyên tố q

thỏa mãn: q|(p – 1) và một số $\alpha \in Z_p^*$. Khóa x_1 được tạo theo: $x_1 = \alpha^{\frac{p-1}{q}} \bmod p$.

Khóa x_2 là một giá trị được chọn ngẫu nhiên trong khoảng (1, q). Sau đó, các khóa công khai được tạo ra từ (x_1, x_2) theo (1.1):

$$y_1 = (x_1)^{x_1+x_2} \bmod p\ ,\ y_2 = (x_1)^{(x_1)^{-1}.x_2} \bmod p \quad (1)$$

Chú ý rằng, tham số q cũng được sử dụng với vai trò của một khóa bí mật tương tự như x_1 và x_2 trong thuật toán ký.

Thuật toán sinh khóa có thể được mô tả lại như trên Bảng 1 sau đây:

Bảng 1. *Thuật toán sinh khóa*

Input: p – số nguyên tố, lq – độ dài (tính theo bit) của số nguyên tố q. Output: q, x_1, x_2, y_1, y_2.
1. generate q: len(q) = lq, q|(p-1) 2. select α: $1 < \alpha < p$ 3. $x_1 \leftarrow \alpha^{(p-1)/q} \bmod p$ 4. if (x1 = 1) then goto [2] 5. select x2: $1 < x_2 < q$ 6. $y_1 \leftarrow (x_1)^{x_1+x_2} \bmod p$, $y_2 \leftarrow (x_1)^{(x_1)^{-1}.x_2} \bmod p$ 7. return {q, x_1, x_2, y_1, y_2}

Chú thích:

- len(.): Hàm tính độ dài (theo bit) của một số nguyên.
- p: Tham số hệ thống/tham số miền.
- q, x_1, x_2: Khóa bí mật.
- y_1, y_2: Khóa công khai của đối tượng ký.

2.2.2. Thuật toán ký

Giả sử (R,S) là chữ ký lên bản tin M, u là 1 giá trị trong khoảng (1,q) và R được tính từ u theo công thức:

$$R = (x_1)^u \bmod p \quad (2)$$

và S được tính từ v theo công thức:

$$S = (x_1)^v \bmod p \quad (3)$$

Ở đây: v cũng là 1 giá trị trong khoảng (1,q).

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

$$(S)^{y_1} \equiv (R)^{y_2} \times (y_1)^E \times (y_2)^{R.S \bmod p} \bmod p$$

Với:

$$E = H(M) \text{ và: } R \times S \bmod p = (x_1)^k \bmod p \quad (4)$$

Trong đó: H(.) là hàm băm và $k \in Z_q^*$.

Đặt: $$(x_1)^k \bmod p = Z \quad (5)$$

Khi đó có thể đưa phương trình kiểm tra về dạng:

$$(S)^{y_1} \equiv (R)^{y_2} \times (y_1)^E \times (y_2)^Z \bmod p \quad (6)$$

Từ (1), (2), (3) và (6) ta có:

$$(x_1)^{v.y_1} \equiv (x_1)^{u.y_2} \times (x_1)^{(x_1+x_2).E} \times (x_1)^{((x_1)^{-1}.x_2).Z} \bmod p \quad (7)$$

Từ (7) suy ra:

$$v \times y_1 \equiv (u \times y_2 + (x_1 + x_2) \times E + (x_1)^{-1} \times x_2 \times Z) \bmod q$$

Nên:

$$v = \left(u \times (y_1)^{-1} \times y_2 + (x_1 + x_2) \times (y_1)^{-1} \times E + \right. \\ \left. + (y_1)^{-1} \times (x_1)^{-1} \times x_2 \times Z\right) \bmod q$$

Hay:

$$v = (y_1)^{-1} \times \left(u \times y_2 + x_1 \times E + \right. \\ \left. + x_2 \times \left(E + (x_1)^{-1} \times Z\right)\right) \bmod q \quad (8)$$

Mặt khác, từ (2), (3) và (4) ta có:

$$(v + u) \bmod q = k \quad (9)$$

Từ (8) và (9) ta có:

$$\left(\left(u \times (y_1)^{-1} \times y_2 + (x_1 + x_2) \times (y_1)^{-1} \times E + \right. \right. \\ \left. \left. + (x_1)^{-1} \times x_2 \times (y_1)^{-1} \times Z + u\right) \bmod q = k\right.$$

Hay:

$$\left(u \times \left((y_1)^{-1} \times y_2 + 1\right) + (x_1 + x_2) \times (y_1)^{-1} \times E + \right. \\ \left. + \left((x_1)^{-1} \times x_2\right) \times (y_1)^{-1} \times Z\right) \bmod q = k \quad (10)$$

Từ (10), suy ra:

$$u = \left((y_1)^{-1} \times y_2 + 1\right)^{-1} \times (k - (x_1 + x_2) \times (y_1)^{-1} \times E \\ - (x_1)^{-1} \times x_2 \times (y_1)^{-1} \times Z) \bmod q$$

Hay:

$$u = \left((y_1)^{-1} \times y_2 + 1\right)^{-1} \times (k - x_1 \times (y_1)^{-1} \times E \\ \left. - x_2 \times (y_1)^{-1} \times (E + (x_1)^{-1} \times Z)\right) \bmod q \quad (11)$$

Từ (11) và (8), có thể tính thành phần thứ nhất của chữ ký theo (2):

$$R = (x_1)^u \bmod p$$

và thành phần thứ 2 theo (3):

$$S = (x_1)^v \bmod p$$

Từ đây thuật toán ký được mô tả trên Bảng 2 như sau:

Bảng 2. *Thuật toán ký*

Input: p, q, x_1, x_2, y_1, y_2, M. Output: (R,S).
1. $E \leftarrow H(M)$ 2. select k: $1 < k < q$ 3. $Z \leftarrow (x_1)^k \bmod p$ 4. $u \leftarrow \left((y_1)^{-1} \times y_2 + 1\right)^{-1} \times (k - x_1 \times (y_1)^{-1} \times E -$ $- x_2 \times (y_1)^{-1} \times \left(E + (x_1)^{-1} \times Z\right)) \bmod q$ 5. $v \leftarrow (y_1)^{-1} \times (u \times y_2 + x_1 \times E +$ $+ x_2 \times \left(E + (x_1)^{-1} \times Z\right)) \bmod q$ 6. $R \leftarrow (x_1)^u \bmod p$ 7. $S \leftarrow (x_1)^v \bmod p$ 8. return (R,S)

Chú thích:

- M: bản tin cần ký, với: $M \in \{0,1\}^\infty$.
- (R,S): chữ ký của U lên M.

2.2.3. Thuật toán kiểm tra chữ ký

Thuật toán kiểm tra của lược đồ được giả thiết là:

$$(S)^{y_1} \equiv (R)^{y_2} \times (y_1)^E \times (y_2)^{R.S \bmod p} \bmod p$$

Ở đây, E là giá trị đại diện của bản tin cần thẩm tra: $E = H(M)$. Nếu M và chữ ký (R,S) thỏa mãn đẳng thức trên thì chữ ký được coi là hợp lệ và bản tin sẽ được xác thực về nguồn gốc và tính toàn vẹn. Ngược lại, thì chữ ký bị coi là giả mạo và bản tin bị phủ nhận về nguồn gốc và tính toàn vẹn. Do đó, nếu vế trái của đẳng thức kiểm tra được tính theo:

$$A = (S)^{y_1} \bmod p \quad (12)$$

và vế phải được tính theo:

$$B = (R)^{y_2} \times (y_1)^E \times (y_2)^{\bar{Z}} \bmod p \quad (13)$$

ở đây: $\bar{Z} = R \times S \bmod p \quad (14)$

thì điều kiện chữ ký hợp lệ là: A = B.

Khi đó, thuật toán kiểm tra của lược đồ mới đề xuất được mô tả trong Bảng 3 như sau:

Bảng 3. *Thuật toán kiểm tra*

Input: p, y_1, y_2, M, (R,S). Output: *true* / *false*.
1. $E \leftarrow H(M)$ 2. $A \leftarrow (S)^{y_1} \bmod p$ 3. $\bar{Z} \leftarrow R \times S \bmod p$ 4. $B \leftarrow (R)^{y_2} \times (y_1)^E \times (y_2)^{\bar{Z}} \bmod p$ 5. if ($A = B$) then {return *true* } else {return *false*}

Chú thích:

- M, (R,S): bản tin, chữ ký cần thẩm tra.

- 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.

2.2.4. Tính đúng đắn của lược đồ mới đề xuất

Điều cần chứng minh ở đây là: Cho p, q là 2 số nguyên tố với: $q \mid (p-1)$, $H: \{0,1\}^* \mapsto Z_n$, $|q| \leq n < |p|$, $1 < \alpha < p$, $x_1 = \alpha^{(p-1)/q} \bmod p$, $1 < x_2 < q$, $y_1 = (x_1)^{x_1 + x_2} \bmod p$, $y_2 = (x_1)^{(x_1)^{-1} \cdot x_2} \bmod p$, $E = H(M)$, $1 < k < q$, $Z = (x_1)^k \bmod p$, $u = \left((y_1)^{-1} \times y_2 + 1\right)^{-1} \times \left(k - x_1 \times (y_1)^{-1} \times E - x_2 \times (y_1)^{-1} \times \left(E + (x_1)^{-1} \times Z\right)\right) \bmod q$, $v = (y_1)^{-1} \times \left(u \times y_2 + x_1 \times E + x_2 \times \left(E + (x_1)^{-1} \times Z\right)\right) \bmod q$, $R = (x_1)^u \bmod p$, $S = (x_1)^v \bmod p$. Nếu: $\bar{Z} = R \times S \bmod p$, $A = (S)^{y_1} \bmod p$, $B = (R)^{y_2} \times (y_1)^E \times (y_2)^{\bar{Z}} \bmod p$ thì: $A = B$.

Tính đúng đắn của thuật toán mới đề xuất được chứng minh như sau:

Từ (3), (8) và (12) ta có:

$$\begin{aligned} A &= (S)^{y_1} \bmod p = (x_1)^{v.y_1} \bmod p \\ &= (x_1)^{(y_1)^{-1}.\left(u.y_2 + x_1.E + x_2.\left(E + (x_1)^{-1}.Z\right)\right).y_1} \bmod p \\ &= (x_1)^{\left(u.y_2 + x_1.E + x_2.\left(E + (x_1)^{-1}.Z\right)\right)} \bmod p \end{aligned} \quad (15)$$

Với: $u = \left((y_1)^{-1} \times y_2 + 1\right)^{-1} \times (k - x_1 \times (y_1)^{-1} \times E - x_2 \times (y_1)^{-1} \times \left(E + (x_1)^{-1} \times Z\right)) \bmod q$

Từ (2), (3), (5), (8), (11) và (14) ta lại có:

$$\begin{aligned} \bar{Z} &= R \times S \bmod p = (x_1)^u \times (x_1)^v \bmod p \\ &= (x_1)^{u + (y_1)^{-1}.\left(u.y_2 + x_1.E + x_2.\left(E + (x_1)^{-1}.Z\right)\right)} \bmod p \\ &= (x_1)^{u + u.(y_1)^{-1}.y_2 + (y_1)^{-1}.x_1.E + (y_1)^{-1}.x_2.\left(E + (x_1)^{-1}.Z\right)} \bmod p \\ &= (x_1)^{u\left((y_1)^{-1}.y_2 + 1\right) + (y_1)^{-1}.x_2.\left(E + (x_1)^{-1}.Z\right) + (y_1)^{-1}.x_1.E} \bmod p \\ &= (x_1)^{\left((y_1)^{-1}.y_2 + 1\right)^{-1}.\left(k - x_1.(y_1)^{-1}.E - x_2.(y_1)^{-1}.\left(E + (x_1)^{-1}.Z\right)\right)\left((y_1)^{-1}.y_2 + 1\right) + x_2.(y_1)^{-1}.\left(E + (x_1)^{-1}.Z\right) + (y_1)^{-1}.x_1.E} \\ &\bmod p = (x_1)^{k - x_2.(y_1)^{-1}.\left(E + (x_1)^{-1}.Z\right) - x_1.(y_1)^{-1}.E + x_2.(y_1)^{-1}.\left(E + (x_1)^{-1}.Z\right) + (y_1)^{-1}.x_1.E} \bmod p \\ &= (x_1)^k \bmod p = Z \end{aligned} \quad (16)$$

Thay (1), (2), (5) và (16) vào (13) ta được:

$$\begin{aligned} B &= (R)^{y_2} \times (y_1)^E \times (y_2)^{\bar{Z}} \bmod p \\ &= (x_1)^{u.y_2} \times (x_1)^{(x_1 + x_2).E} \times (x_1)^{(x_1)^{-1}.x_2.Z} \bmod p \\ &= (x_1)^{\left(u.y_2 + x_1.E + x_2.\left(E + (x_1)^{-1}.Z\right)\right)} \bmod p \end{aligned} \quad (17)$$

Từ (15) và (17) suy ra điều cần chứng minh: $A = B$

2.2.5. Ví dụ

Tính đúng đắn của lược đồ mới đề xuất được minh họa bằng một ví dụ số như sau:

a. Sinh tham số và khóa (Bảng 1)

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

Output: q, x_1, x_2, y_1, y_2.

- Giá trị của p:

11125047481941070585483791498765271363372319494651382867527128102052391566875979592156815652441744489180542674814431022681529221056687456481556094275955901

- Giá trị của q:

1396040063414249106233756715423506814076734227141

- Giá trị của x_1:

40583703186076810077555107626851782713652321929471000568735620774126567223984754965898162800508328979557287628021663946280519333840076222717260562084338 6

- Giá trị của x_2:

13364690171973798719196853150685406862722780355 77

- Giá trị của y_1:

41664145438537544774635134322725556214909941901511883506834222768226003954066407701818701173717255608834951932639814922269821356253574624278301142112113 97

- Giá trị của y_2:

34449004056916080126558125182750770281678173954520452155461712791247704263118008086208153111070041176951528716919095253650909954321250383097814987832983 31

b. Sinh chữ ký (Bảng 2)

Input: p, q, y_1, y_2, x_1, x_2, M.

Output: (R,S).

- Bản tin: M = "THIS IS A NEWDIGITAL SIGNATURE ALGRITHM !"

- Giá trị của k:

12552122068290233521328436559895699222669216936 76

- Giá trị của E tính được:

99479775789854978284331121961379715519810391936 0

- Giá trị của R tính được:

44499114087527776492440404662063073703454141929343934596076092067962791347983369564752943525594529514108745601474922131256912519202627375973263920431000 28

- Giá trị của S tính được:

87266621344195220360196944973599908111043941598406241186524326179846189573383626435667071635345061472098711179591610661485712194698845813374554223839816 55

c. Kiểm tra chữ ký (Bảng 3)

Input: p, y_1, y_2, (R,S), M.

+ Trường hợp 1:

- Bản tin: M = "THIS IS A NEWDIGITAL SIGNATURE ALGRITHM !"

- Giá trị của R cần kiểm tra:

44499114087527776492440404662063073703454141929343934596076092067962791347983369564752943525594529514108745601474922131256912519202627375973263920431000 28

- Giá trị của S cần kiểm tra:

87266621344195220360196944973599908111043941598406241186524326179846189573383626435667071635345061472098711179591610661485712194698845813374554223839816 55

- Giá trị của E tính được:

99479775789854978284331121961379715519810391936 0

- Giá trị của Z tính được:

69069719679636425136540788279236783210132354165420687120820589978943542468944086437422274320253098307019887418283540161248286954736391381696566805153939123

- Giá trị của A tính được:

46726245383885022668358537167105491063273030654205315339132641545609008093755946635143008531473628209680208251122603703288240974782483275437116743832096 14

- Giá trị của B tính được:

46726245383885022668358537167105491063273030654205315339132641545609008093755946635143008531473628209680208251122603703288240974782483275437116743832096 14

Output: (R,S) = true.

Chú thích:

Trường hợp này kết quả cho thấy chữ ký hợp lệ vì tính toàn vẹn của cả bản tin và chữ ký đều được đảm bảo.

+ Trường hợp 2:

- Bản tin: M = "THIS IS A NEWDIGITAL SIGNATURE ALGRITHM "

- Giá trị của R cần kiểm tra:

44499114087527776492440404662063073703454141929343934596076092067962791347983369564752943525594529514108745601474922131256912519202627375973263920431000 28

- Giá trị của S cần kiểm tra:

87266621344195220360196944973599908111043941598406241186524326179846189573383626435667071635345061472098711179591610661485712194698845813374554223839816 55

- Giá trị của E tính được:

45942812914655251101746677437733633894779435085

- Giá trị của Z tính được:

69069719679636425136540788279236783210132354165420687120820589978943542468944086437422274320253098307019887418283540161248286954736391381696566805153939123

- Giá trị của A tính được:

46726245383885022668358537167105491063273030654205315339132641545609008093755946635143008531473628209680208251122603703288240974782483275437116743832096 14

- Giá trị của B tính được:

20925305882558770584753460208619478492871619098055755472151142456277874491594998297359048178303634143232835349834149659470985087886392921555159467540424063

Output: (R,S) = false.

Chú thích:

Trường hợp này kết quả cho thấy chữ ký không hợp lệ vì ký tự cuối cùng của bản tin đã bị sửa đổi.

+ Trường hợp 3:

- Bản tin: M = "THIS IS A NEWDIGITAL SIGNATURE ALGRITHM !"

- Giá trị của R cần kiểm tra:

44499114087527776492440404662063073703454141929343934596076092067962791347983369564752943525594529514108745601474922131256912519202627375973263920431000 20

- Giá trị của S cần kiểm tra:

87266621344195220360196944973599908111043941598406241186524326179846189573383626435667071635345061472098711179591610661485712194698845813374554223839816 50

- Giá trị của E tính được:

99479775789854978284331121961379715519810391936 0

- Giá trị của Z tính được:

38444977043721426631466525081343858874295671303561714050415768364551394492036594500866235804859518094129883959330526027600364485667484513357402200742329 91

- Giá trị của A tính được:

14066778225978218020105260570759546932410856857650576352585936590763908843256504202090165

57856891805455841762922469963966774657916245247844607175313754533

- Giá trị của B tính được:

99393855515823105437384214469311928400151138197085285633813123513787042678692559553651709833987610345040124075262635052068926037631535010374772621806591752

Output: (R,S) = false.

Chú thích:

Trường hợp này kết quả cho thấy chữ ký không hợp lệ vì chữ số cuối cùng của R và S đã bị thay đổi.

2.2.6. Mức độ an toàn của lược đồ mới đề xuất

Mức độ an toàn của lược đồ mới đề xuất có thể đánh giá qua khả năng chống lại một số dạng tấn công như:

- Tấn công khóa bí mật

Ở lược đồ mới đề xuất, cặp tham số x_1, x_2 cùng được sử dụng làm khóa bí mật để hình thành chữ ký. Vì thế, lược đồ chỉ bị phá vỡ nếu cả 2 tham số này cùng bị lộ, nói cách khác là kẻ tấn công phải giải được bài toán logarit rời rạc kết hợp khai căn trên *Zp*. Do đó, mức độ an toàn của lược đồ mới đề xuất xét theo khả năng chống tấn công làm lộ khóa bí mật được đánh giá bằng mức độ khó của việc giải được DLRP. Cần chú ý, DLRP là một dạng bài toán khó mới, mà ngay cả khi có các giải thuật thời gian đa thức cho FRP và DLP cũng không có nghĩa là sẽ giải được bài toán này. Ngoài ra, tham số q cũng được sử dụng với vai trò khóa bí mật trong thuật toán ký. Như vậy, để phá vỡ tính an toàn của thuật toán, kẻ tấn công còn phải giải được bài toán tìm bậc của x_1. Tuy nhiên, việc tìm bậc của x_1 là không thể thực hiện được, vì x_1 ở đây là 1 tham số bí mật.

- Tấn công giả mạo chữ ký

Từ thuật toán kiểm tra (Bảng 3) của thuật toán mới đề xuất cho thấy, một cặp (R,S) giả mạo sẽ được công nhận là chữ ký hợp lệ với một bản tin M nếu thỏa mãn điều kiện:

$$(S)^{y_1} \equiv (R)^{y_2} \times (y_1)^{R.S \bmod p} \times (y_2)^{E} \bmod p \quad (18)$$

Từ (18), nếu chọn trước R rồi tính S thì khi đó điều kiện (18) sẽ có dạng:

$$(S)^{y_1} \equiv a \times (y_2)^{(R.S) \bmod p} \bmod p \quad (19)$$

Còn nếu chọn trước S rồi tính R thì khi đó điều kiện (18) sẽ trở thành:

$$(R)^{y_2} \equiv b \times (y_2)^{(R.S) \bmod p} \bmod p \quad (20)$$

Với a, b là hằng số, dễ thấy rằng (19) và (20) cũng là một dạng bài toán khó chưa có cách giải tương tự bài toán logarit rời rạc kết hợp khai căn trên *Zp*.

3. Kết luận

Bài báo đề xuất xây dựng thuật toán chữ ký số dựa trên tính khó giải của bài toán logarit rời rạc – khai căn trên *Zp*. Mức độ an toàn của các thuật toán xây dựng theo phương pháp này sẽ được đảm bảo bằng mức độ khó của việc giải bài toán trên. Ở đây, bài toán logarit rời rạc kết hợp khai căn trên *Zp* là một dạng bài toán khó mới, lần đầu được đề xuất và ứng dụng trong việc xây dựng thuật toán chữ ký số. Từ phương pháp mới đề xuất có thể xây dựng một lớp thuật toán chữ ký số có độ an toàn cao cho các ứng dụng trong thực tế.

TÀI LIỆU THAM KHẢO

[1] R.L. Rivest, A. Shamir, and L.M. Adleman. *A Method for Obtaining Digital Signatures and Public Key Cryptosystems.* Communications of the ACM, 1978, vol. 21, no 2, pp. 120–126.

[2] Rabin M.O. *Digitalized Signatures and Public Key Functions as Intractable as Factorization.* - Technical report MIT/LCS/TR-212, MIT Laboratory for Computer Science, 1979.

[3] ElGamal T. *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.

[4] Schnorr C.P. *Efficient signature generation by smart cards.* J. Cryptology. 1991. vol. 4. pp. 161–174.

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

[6] 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).

[7] ANSI X9.62 and FIPS 186-2. *Elliptic curve signature algorithm*, 1998.

[8] GOST R 34.10-2001. *Russian Federation Standard. Information Technology. Cryptographic data Security. Produce and check procedures of Electronic Digital Signature.* Government Committee of the Russia for Standards, 2001 (in Russian).

[9] Nguyen Duc Thuy and Luu Hong Dung, "A New Construction Method of Digital Signature Algorithms", IJCSNS International *Journal of Computer Science and Network Security.* Vol. 16 No. 12 pp. 53-57, December 2016. ISSN: 1738 - 7906.

[10] 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.

[11] 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.

[12] 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.

[13] 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.

[14] 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.

[15] 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.

[16] 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.

[17] 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.

[18] N.A. Moldovyan, "Digital Signature Scheme Based on a New Hard Problem", *Computer Science Journal of Moldova*, vol.16, no.2(47), 2008.

(BBT nhận bài: 03/3/2019, hoàn tất thủ tục phản biện: 04/7/2019)