GIẢI PHÁP NÂNG CAO ĐỘ AN TOÀN TRONG XÂY DỰNG LƯỢC ĐỒ CHỮ KÝ SỐ

A SOLUTION IMPROVES SAFETY IN BUILDING DIGITAL SIGNATURE SCHEME

Nguyễn Viết Cường[1*], Nguyễn Đức Thụy[2], Lưu Hồng Dũng[3]

[1]Trung tâm Công nghệ Thông tin, Học viện Kỹ thuật Quân sự
[2]Trường Cao đẳng Kinh tế - Kỹ thuật Tp. Hồ Chí Minh
[3]Học viện Kỹ thuật Quân sự

*Tác giả liên hệ: cuongnv@mta.edu.vn

(Nhận bài: 12/8/2021; Chấp nhận đăng: 17/01/2022)

Tóm tắt - Trong bài báo này, nhóm tác giả đề xuất một giải pháp nâng cao độ an toàn cho lược đồ chữ ký số dựa trên một dạng bài toán khó mới, bài toán này được phát triển từ bài toán logarit rời rạc và bài toán khai căn nên được gọi là bài toán logarit rời rạc kết hợp khai căn trên trường hữu hạn Z_p. Hiện tại, đây là một dạng bài toán khó thuộc lớp bài toán không giải được. Mặt khác, việc xây dựng lược đồ chữ ký ở đây được thực hiện theo một phương pháp hoàn toàn mới, đây cũng là một yếu tố quan trọng cho phép nâng cao độ an toàn của lược đồ chữ ký số theo giải pháp mới này. Lược đồ được đề xuất có thể phù hợp với các ứng dụng yêu cầu cao về độ an toàn trong thực tế.

Từ khóa - Lược đồ chữ ký số; thuật toán sinh tham số và khóa; thuật toán ký; thuật toán kiểm tra chữ ký

Abstract - This paper proposed a novel solution to improve the safety of the digital signature schema based on a new kind of thorny problem. It was built from the discrete logarithm and square root one in Galois field, which were named the discrete logarithm combined with square root extraction in Galois field. It is also one of unsolvable problems. In addition, the signature schema was implemented in a completely new way, which is also an important factor allowing to improve the security of this schema according to the new solution. The proposed scheme can be suitable for applications requiring high safety in practice.

Key words - Digital signature scheme; parameter and key generation algorithm; signaturing algorithm; signature testing algorithms.

1. Đặt vấn đề

Nâng cao độ an toàn cho thuật toán chữ ký số luôn là vấn đề cần thiết được đặt ra, khi mà năng lực tấn công các hệ mật khóa công khai nói chung và các hệ chữ ký số nói riêng liên tục được gia tăng nhờ các tiến bộ về khoa học công nghệ. Qua các kết quả nghiên cứu đã được công bố [1 - 8] có thể thấy, hướng tiếp cận cơ bản để nâng cao độ an toàn cho các lược đồ chữ ký chủ yếu dựa trên tính 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 trên trường hữu hạn nguyên tố Z_p. Tuy nhiên, một khi kẻ tấn công đã có đủ năng lực để giải được 1 bài toán thì về nguyên tắc cũng sẽ giải được bài toán còn lại, do đó cách tiếp cận như vậy là không có ý nghĩa thực tiễn.

Trong bài viết này, nhóm tác giả đề xuất phương pháp xây dựng lược đồ chữ ký số dựa trên một dạng bài toán khó mới mà hiện tại chưa có cách giải. Nhờ đó, lược đồ xây dựng theo giải pháp mới đề xuất có khả năng chống lại các dạng tấn công khóa bí mật cũng như tấn công giả mạo chữ ký đã được biết đến trong các ứng dụng thực tế.

2. Bài toán logarit kết hợp khai căn trên Z_p – một dạng bài toán khó mới

Bài toán khó làm cơ sở để xây dựng lược đồ chữ ký ở đây được gọi là bài toán logarit kết hợp khai căn trên trường hữu hạn Z_p [9]. Bài toán này được hình thành dựa trên cơ sở là bài toán logarit rời rạc có dạng:

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

Trong đó, p là một số nguyên tố; g là phần tử sinh của Z_p; x là giá trị cần tìm từ các tham số công khai g, p,y.

Từ bài toán logarit rời rạc trên Z_p ta thấy, nếu tham số g cũng được giữ bí mật thì bài toán logarit trên Z_p sẽ trở thành 1 dạng bài toán không giải được. Trường hợp đơn giản nhất, ta chọn chính khóa bí mật x cho vai trò của tham số g. Khi đó, bài toán có thể phát biểu dưới dạng: Cho p là số nguyên số và y thuộc Z_p, số tìm x thỏa mãn phương trình sau:

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

Cũng có thể xuất phát từ bài toán khai căn: Tìm giá trị x thỏa mãn phương trình:

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

Với p là một số nguyên tố và τ là giá trị trong khoảng (1, p-1). Ta cũng nhận được kết quả tương tự như trên, nếu tham số τ được giữ bí mật. Trường hợp đơn giản nhất, có thể chọn tham số bí mật x cho vai trò của τ. Khi đó, bài toán khai căn trên Z_p cũng trở thành 1 dạng bài toán không giải được, dạng:

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

Với cách tiếp cận như trên, bài toán này ở đây được gọi là *bài toán logarit rời rạc kết hợp khai căn trên Z_p* hay ngắn gọn là *bài toán logarit kết hợp khai căn*.

[1] Information Technology Center/ Le Quy Don Technical University (Nguyen Viet Cuong)
[2] HCM City Technical and Economic College (Nguyen Duc Thuy)
[3] Le Quy Don Technical University (Luu Hong Dung)

Có thể phát biểu bài toán khó mới này ở dạng thứ nhất như sau:

Dạng 1: Cho số nguyên tố p và số nguyên dương y thuộc Z_p, hãy tìm số x thỏa mãn phương trình sau:

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

Một cách tiếp cận khác cũng xuất phát từ 2 bài toán trên là:

Nếu vế trái của đẳng thức: $y = g^x \bmod p$ trong bài toán logarit rời rạc mà là một biến số dạng: $x^b \bmod p$ thì bài toán logarit sẽ trở thành bài toán không giải được, khi đó bài toán này có dạng: $g^x \bmod p = x^b \bmod p$.

Tương tự, nếu vế trái của đẳng thức: $y = x^\tau \bmod p$ trong bài toán khai căn mà là một biến số kiểu: $a^x \bmod p$ thì khi đó bài toán khai căn cũng trở thành bài toán không giải được: $a^x \bmod p = x^\tau \bmod p$.

Với cách tiếp cận này, ta có thể phát biểu dạng thứ 2 của bài toán khó mới như sau:

Dạng 2: Cho p là một số nguyên tố, a và b là các số thuộc Z_p, hãy tìm số x thỏa mãn phương trình sau:

$$a^x \equiv x^b \bmod p$$

Hiện tại, các giải thuật cho bài toán logarit rời rạc hay khai căn trên Z_p đều không thể áp dụng đối với bài toán này. Nghĩa là, không có cách giải nào khác cho bài toán này ngoài phương pháp "vét cạn" với độ phức tạp tính toán $O(2^n)$, ở đây: n = |p|.

3. Giải pháp nâng cao độ an toàn trong xây dựng lược đồ chữ ký số

Giải pháp nâng cao độ an toàn cho lược đồ chữ ký số đề xuất ở đây được trình bày thông qua cách thức xây dựng một lược đồ chữ ký dựa trên tính khó của bài toán logarit rời rạc kết hợp khai căn trên Z_p. Trong đó, dạng thứ nhất của bài toán được sử dụng để hình thành cặp khóa bí mật, công khai của các đối tượng ký trong thủ tục sinh khóa, các thành phần của chữ ký cũng được tạo ra bởi thủ tục ký từ dạng thứ nhất của bài toán này. Dạng thứ hai của bài toán được sử dụng làm cơ sở để xây dựng thủ tục kiểm tra chữ ký của lược đồ.

Lược đồ chữ ký mới đề xuất ở đây bao gồm các thủ tục sinh tham số và khóa, thủ tục ký và thủ tục kiểm tra chữ ký được xây dựng như sau:

3.1. Thủ tục sinh tham số và khóa

Các số nguyên tố p và q với vai trò là tham số hệ thống hay tham số miền, được lựa chọn tương tự như chuẩn DSS [11] của Hoa Kỳ, hay GOST R34-90.10 [12] của Liên bang Nga. Để tạo cặp khóa bí mật/ công khai, mỗi tượng ký cần chọn trước một giá trị $\alpha \in Z_p^*$, rồi tính khóa bí mật x theo:

$$x = \alpha^{\frac{p-1}{q}} \bmod p$$

Khóa công khai y được tạo ra từ x và p theo:

$$y = x^x \bmod p \quad (1)$$

Khi đó thủ tục sinh tham số và khóa được mô tả như sau:

Thuật toán 1:

input: Lp, Lq.

output: p, q, x, y.

[1]. **generate** p, q: len(p) = Lp, len(q) = Lq, q|(p-1)

[2]. **select** α: 1< α < p

[3]. $x \leftarrow \alpha^{\frac{p-1}{q}} \bmod p$

[4]. **if** (x = 1 **OR** x = q) **then goto** [2]

[5]. $y \leftarrow x^x \bmod p$

[6]. **return** {p, q, x, y}

3.2. Thủ tục ký

Giả sử với bản tin M cho trước, (r,s) là chữ ký tương ứng của một đối tượng ký U – người sở hữu cặp khóa (x,y) và điều kiện để (r,s) được công nhận hợp lệ là:

$$(s)^{e_1} \equiv (r)^{e_2} \times (y)^{e_3} \bmod p$$

Với, $1 < r, s < p$ và $1 < e_1, e_2, e_3 < q$.

Cũng giả thiết rằng, thành phần s của chữ ký được sinh ra từ một giá trị e_4 theo công thức:

$$s = (x)^{e_4} \bmod p \quad (3)$$

Với $1 < e_4 < q$. Tương tự, thành phần r được sinh ra từ một giá trị e_5 theo công thức:

$$r = (x)^{e_5} \bmod p \quad (4)$$

Ở đây, e_5 cũng có giá trị trong khoảng (1,q).

Từ (1), (2), (3) và (4) ta có:

$$(x)^{e_1 \times e_4} \equiv (x)^{e_2 \times e_5} \times (x)^{x \times e_3} \bmod p \quad (5)$$

Từ (5) suy ra:

$$e_1 \times e_4 \equiv (e_2 \times e_5 + x \times e_3) \bmod q \quad (6)$$

Mặt khác, từ (3), (4) ta có:

$$r \times s \bmod p = (x)^{e_4} \times (x)^{e_5} \bmod p = (x)^{e_4 + e_5} \bmod p \quad (7)$$

Đặt:

$$(e_4 + e_5) \bmod q = k \quad (8)$$

Suy ra:

$$e_5 = (k - e_4) \bmod q \quad (9)$$

Từ (6) và (9) ta có:

$$e_1 \times e_4 \bmod q = ((k - e_4) \times e_2 + x \times e_3) \bmod q$$

Suy ra:

$$e_4 = (e_1 + e_2)^{-1} \times (k \times e_2 + x \times e_3) \bmod q \quad (10)$$

Từ (10), giá trị s được tính theo (3):

$$s = (x)^{e_4} \bmod p$$

Từ (4) và (9), giá trị r được tính theo:

$$r = (x)^{k - e_4} \bmod p \quad (11)$$

Mặt khác, nếu đặt:

$$z = (x)^k \bmod p \quad (12)$$

Từ (7), (8) và (12), có thể tính r theo:

$$r = z \times s^{-1} \bmod p \quad (13)$$

Với lựa chọn:

$$e_1 = H(z \| M),\ e_2 = H(z \| y),$$
$$e_3 = H(z \| y \| M) \quad (14)$$

Khi đó thủ tục ký được mô tả như sau:

Thuật toán 2:

input: p, q, x, y, M.
output: (r, s).

[1]. **select** k: $1 < k < q$

[2]. $z \leftarrow x^k \bmod p$

[3]. $e_1 \leftarrow H(z \| M),\ e_2 \leftarrow H(z \| y),$
$e_3 \leftarrow H(z \| y \| M)$

[4]. $e_4 \leftarrow (e_1 + e_2)^{-1} \times (k \times e_2 + x \times e_3) \bmod q$

[5]. $s \leftarrow (x)^{e_4} \bmod p$

[6]. $r = z \times s^{-1} \bmod p$ (6)

[7]. **return** (r, s)

Chú thích:

- M: Bản tin cần ký, với: $M \in \{0,1\}^{\infty}$.

- (r,s): Chữ ký lên M.

3.3. Thủ tục kiểm tra chữ ký

Thủ tục kiểm tra của lược đồ được xây dựng dựa giả thiết là:

$$(s)^{e_1} \equiv (s)^{e_2} \times (y)^{e_3} \bmod p$$

Ở đây:

$$e_1 = H(z \| M),\ e_2 = H(z \| y),$$
$$e_3 = H(z \| y \| M) \text{ với: } z = (x)^k \bmod p.$$

Nghĩa là, nếu giả sử:

$$U = (s)^{e_1} \bmod p$$

và: $$V = (r)^{e_2} \times (y)^{e_3} \bmod p$$

thì: U = V là điều kiện để chữ ký (r,s) hợp lệ.

Vấn đề là khi cần thẩm tra bản tin M và chữ ký (r,s), do k là tham số bí mật nên giá trị z không thể tính theo: $z = (x)^k \bmod p$. Song, từ (7), (8) và (12) có thể tính z từ r và s theo: $z = r \times s \bmod p$. Tại thời điểm kiểm tra, tính hợp lệ của (r,s) chưa được xác thực nên ký hiệu $\bar{z}$ sẽ được sử dụng thay cho z:

$$\bar{z} = r \times s \bmod p \quad (15)$$

và do đó các ký hiệu $\bar{e}_1$, $\bar{e}_2$, $\bar{e}_3$ cũng được sử dụng thay cho e_1, e_2, e_3 trong thuật toán kiểm tra:

$$\bar{e}_1 = H(\bar{z} \| M), \bar{e}_2 = H(\bar{z} \| y), \bar{e}_3 = H(\bar{z} \| y \| M) \quad (16)$$

Khi đó, giá trị U được tính theo:

$$U = (s)^{\bar{e}_1} \bmod p \quad (17)$$

và giá trị V được tính theo:

$$V = (r)^{\bar{e}_2} \times (y)^{\bar{e}_3} \bmod p \quad (18)$$

Thủ tục kiểm tra của lược đồ khi đó sẽ được mô tả như sau:

Thuật toán 3:

input: p, q, y, M, (r,s).
output: TRUE / FALSE.

[1]. $\bar{z} \leftarrow r \times s \bmod p$

[2]. $\bar{e}_1 \leftarrow H(\bar{z} \| M),\ \bar{e}_2 \leftarrow H(\bar{z} \| y),$
$\bar{e}_3 \leftarrow H(\bar{z} \| y \| M)$

[3]. $A \leftarrow (s)^{\bar{e}_1} \bmod p$

[4]. $B \leftarrow (r)^{\bar{e}_2} \times (y)^{\bar{e}_3} \bmod p$

[5]. **if** (A = B) **then return** (TRUE)}
else return (FALSE)

3.4. Tính đúng đắn của lược đồ mới đề xuất

Tính đúng đắn của lược đồ mới đề xuất được chứng minh dựa trên các bổ đề sau đây:

Bổ đề 1:

Cho p và q là 2 số nguyên tố với q là ước số của (p-1), α là một số nguyên dương trong khoảng (1,p). Nếu $x = \alpha^{\frac{p-1}{q}} \bmod p$ thì $x^q \bmod p = 1$.

Chứng minh:

Ta có:

$$(x)^q \bmod p = \left(\alpha^{\frac{p-1}{q}} \bmod p \right)^q \bmod p = (\alpha)^{p-1} \bmod p$$

Theo định lý Fermat [9] thì: $(\alpha)^{p-1} \bmod p = 1$

Suy ra, điều cần chứng minh: $(x)^q \bmod p = 1$.

Bổ đề 2:

Cho p và q là 2 số nguyên tố với q là ước số của (p -1), α là một số nguyên dương trong khoảng (1, p) và $x = \alpha^{\frac{p-1}{q}} \bmod p$. Nếu: $m \bmod q = n \bmod q$ thì: $x^m \equiv x^n \bmod p$.

Chứng minh:

Nếu: $m \bmod q = n \bmod q$ thì: $m = n + k \times q$ hoặc: $n = m + k \times q$, với k là một số nguyên. Không làm mất tính tổng quát, giả sử: $m = n + k \times q$.

Do đó:

$$x^m \bmod p = x^{n+k\times q} \bmod p = x^n \times x^{k\times q} \bmod p$$
$$= \left(x^n \bmod p\right) \times \left(x^{k\times q} \bmod p\right) \bmod p$$
$$= \left(x^n \bmod p\right) \times \left(x^q \bmod p\right)^k \bmod p$$

Theo Bổ đề 1 ta có: $(x)^q \bmod p = 1$

Nên:

$$x^m \bmod p = \left(x^n \bmod p\right) \times \left(x^q \bmod p\right)^k \bmod p$$
$$= \left(x^n \bmod p\right) \times (1)^k \bmod p = x^n \bmod p$$

Bổ đề đã được chứng minh.

Từ đây, có thể chứng minh tính đúng đắn của lược đồ mới đề xuất như sau:

Thật vậy, từ (13) ta có:

$$z = r \times s \bmod p \quad (19)$$

Từ (15) và (19) suy ra: $\bar{z} = z$ (20)

Thay (20) vào (16) ta được:

$$\bar{e}_1 = H(\bar{z} \,\|\, M) = H(z \,\|\, M),$$
$$\bar{e}_2 = H(\bar{z} \,\|\, y) = H(z \,\|\, y),$$
$$\bar{e}_3 = H(\bar{z} \,\|\, y \,\|\, M) = H(z \,\|\, y \,\|\, M) \quad (21)$$

Từ (14) và (21) suy ra:

$$\bar{e}_1 = e_1,\ \bar{e}_2 = e_2,\ \bar{e}_3 = e_3$$

Do đó, từ (17) và (18) ta có:

$$U = (s)^{\bar{e}_1} \bmod p = (s)^{e_1} \bmod p \quad (22)$$

và: $V = (r)^{\bar{e}_2} \times (y)^{\bar{e}_3} \bmod p = (r)^{e_2} \times (y)^{e_3} \bmod p$ (23)

Thay (1), (11) vào (23) ta được

$$\begin{aligned} V &= (r)^{e_2} \times (y)^{e_3} \bmod p \\ &= \left(x^{k-e_4} \bmod p\right)^{e_2} \times \left(x^x \bmod p\right)^{e_3} \bmod p \\ &= (x)^{(k-e_4)\times e_2} \times (x)^{x \times e_3} \bmod p \\ &= (x)^{k\times e_2 + x\times e_3 - e_2 \times e_4} \bmod p \end{aligned} \quad (24)$$

Mặt khác, từ (6) và (9) suy ra:

$$e_1 \times e_4 \bmod q = (k \times e_2 + x \times e_3 - e_2 \times e_4) \bmod q \quad (25)$$

Từ (3), (23), (25) và theo Bổ đề 2 ta được:

$$\begin{aligned} V &= (x)^{k\times e_2 + x\times e_3 - e_2\times e_4} \bmod p = (x)^{e_1 \times e_4} \bmod p \\ &= \left(x^{e_4} \bmod p\right)^{e_1} \bmod p = (s)^{e_1} \bmod p \end{aligned} \quad (26)$$

Từ (22) và (26) suy ra điều cần chứng minh: U = V.

3.5. Một số đánh giá về tính an toàn của lược đồ chữ ký mới đề xuất

Tính an toàn của một lược đồ chữ ký số có thể đánh giá dựa trên một số cơ sở như sau:

3.5.1. Khả năng chống tấn công khóa bí mật

Tấn công khóa bí mật có thực hiện vào thuật toán sinh khóa (Thuật toán 1) và các bước [2], [4] và [5] của thuật toán ký (Thuật toán 2). Ở các bước [2] và [5], mặc dù các tham số *s* và *z* là công khai, song các tham số *k* và e_4 lại là bí mật. Vì vậy việc tìm *x* từ các bước [2] và [5] của thuật toán ký là khó, tương tự như tìm *x* từ thuật toán sinh khóa. Còn ở bước [4] của thuật toán ký, bản thân e_4 và *k* cũng đều là các tham số bí mật nên việc tìm *x* từ bước [4] là không thể thực hiện được. Như vậy, để tìm khóa bí mật thì kẻ tấn công buộc phải giải được bài toán khó trên đây bằng phương pháp "vét cạn" (brute force attack) với độ phức tạp tính toán là $O(2^n)$, với n = |p|.

3.5.2. Khả năng chống tấn công giả mạo chữ ký

Từ thủ tục kiểm tra (Thuật toán 3) của lược đồ mới đề xuất cho thấy, điều kiện cần phải thỏa mãn để (r,s) được công nhận hợp lệ với một bản tin M là:

$$(s)^{e_1} \equiv (r)^{e_2} \times (y)^{e_3} \bmod p$$

hay:

$$(r)^{H(r\times s \bmod p \| M)} \equiv (s)^{H(r\times s \bmod p \| y)} \times (y)^{H(r\times s \bmod p \| y \| M)} \bmod p \quad (27)$$

Từ (27) cho thấy, việc chọn trước 1 trong 2 giá trị r hoặc s rồi tính giá trị thứ 2 (s hoặc r) chính là dạng thứ 2 của bài toán đã nêu trong Mục 2, như đã biết đây là một dạng bài toán mà hiện tại trong toán học còn chưa có cách giải nào khác ngoài phương pháp "vét cạn". Hơn nữa, với việc sử dụng hàm băm ở đây thì giải (27) để tìm (r,s) thậm chí còn khó hơn dạng 2 của bài toán này.

Như vậy, để tạo chữ ký giả mạo tương ứng với 1 bản tin cho trước, kẻ tấn công không có cách nào khác ngoài việc chọn ngẫu nhiên 1 cặp (r,s) thỏa mãn (27), mà thực chất đây cũng là tấn công theo kiểu "vét cạn".

3.5.3. Tính hiệu quả của lược đồ mới đề xuất

Tính hiệu quả của lược đồ đề xuất được đánh giá thông qua việc so sánh chi phí thực hiện của lược đồ này với chi phí thực hiện lược đồ chữ ký số DSA [10] và GOST R34-10.94 [11].

Chi phí thực hiện hay chi phí tính toán là số các phép toán cần thực hiện của lược đồ, ở đây qui ước sử dụng các ký hiệu:

T_{exp}: Số phép toán lũy thừa modulo cần thực hiện.

T_h: Số phép băm cần thực hiện.

T_{mul}: Số phép nhân modulo cần thực hiện.

T_{inv}: Số phép nghịch đảo modulo cần thực hiện.

Chú ý:

Thủ tục sinh tham số và khóa chỉ cần thực hiện một lần duy nhất với mọi lược đồ. Vì thế, chi phí tính toán cho thuật toán sinh tham số và khóa có thể bỏ qua khi so sánh chi phí thực hiện của các lược đồ.

Chi phí thực hiện cho thủ tục ký và thủ tục kiểm tra chữ ký của lược đồ DSA và GOST R34-10.94 với lược đồ mới đề xuất được chỉ ra trong Bảng 1 và Bảng 2 như sau:

Bảng 1. *Chi phí thực hiện của các thuật toán ký*

	T_{exp}	T_{mul}	T_{inv}	T_h
DSA	1	2	1	1
GOST R34-10.94	1	2	0	1
MTA 21-07	2	3	2	3

Bảng 2. *Chi phí thực hiện của các thuật toán kiểm tra*

	T_{exp}	T_{mul}	T_{inv}	T_h
DSA	2	3	1	1
GOST R34-10.94	3	3	0	0
MTA 21-07	3	2	0	3

4. Kết luận

Trong bài báo này, nhóm tác giả đề xuất một một giải pháp nâng cao độ an toàn cho lược đồ chữ ký số dựa trên một dạng bài toán khó mới cùng với phương pháp xây dựng lược đồ chữ ký hoàn toàn mới. Tuy có nhược điểm là hiệu quả thực hiện không cao, song theo đánh giá chủ quan của nhóm tác giả thì hiện tại các dạng tấn công đã biết đối với lược đồ chữ ký số nói chung là không thực hiện được với lược đồ xây dựng theo giải pháp mới này. Ngoài ra, từ giải pháp mới đề xuất có thể triển khai một họ lược đồ chữ ký số có độ an toàn cao cho các lựa chọn khác nhau trong ứng dụng 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] Menezes A. J. Vanstone S.A, *Handbook of Applied Cryptography*, CRC Press, 1996.

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

[11] 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.

[12] Moldovyan, "Digital Signature Scheme Based on a new hard problem", *Computer Science Journal of Moldova*, vol. 16, no. 2, pp.163-182, 2008.