TELKOMNIKA, Vol.17, No.5, October 2019, pp.2327~2334
ISSN: 1693-6930, accredited First Grade by Kemenristekdikti, Decree No: 21/E/KPT/2018
DOI: 10.12928/TELKOMNIKA.v17i5.10525

Blind multi-signature scheme based on factoring and discrete logarithm problem

Duc Nguyen Tan*[1], Hai Nguyen Nam[2], Minh Nguyen Hieu[3]
[1]Posts and Telecommunication Institute of Technology, Vietnam
[2,3]Academy of Cryptography Techniques, Ha Noi, Vietnam
*Corresponding author, e-mail: tanducslc@gmail.com[1], nnthaivn61@gmail.com[2], hieuminhmta@gmail.com[3]

Abstract

One of the important objectives of information security systems is providing authentication of the electronic documents and messages. In that, blind signature schemes are an important solution to protect the privacy of users in security electronic transactions by highlighting the anonymity of participating parties. Many studies have focused on blind signature schemes, however, most of the studied schemes are based on single computationally difficult problem. Also, digital signature schemes from two difficult problems were proposed but the fact is that only finding solution to single hard problem then these digital signature schemes are breakable. In this paper, we propose a new signature schemes base on the combination of the RSA and Schnorr signature schemes which are based on two hard problems: IFP and DLP. Then expanding to propose a single blind signature scheme, a blind multi-signature scheme, which are based on new baseline schemes.

Keywords*: blind multi-signature, blind signature, digital signature, discrete logarithm problem, integer factorization problem*

1. Introduction

One of the important objectives of the information security systems is providing authentication of the electronic documents and messages. Usually digital signature schemes are considered the most important solutions to meeting these requirements [1]. There were many proposals for signature schemes published based on a single hard problem such as factoring (FAC), discrete logarithm (DL) or elliptic curve discrete logarithm (ECDL) problems [1]. Also digital signature schemes from two difficult problems were proposed but most of them have proved to be not as secure as claimed [2-4].

In various types of electronic transactions, including election systems and digital cash schemes, user anonymity and authentication are always required. To solve this problem the blind signature schemes are used [5-7]. The properties of the blind signatures are the signer can not to read the document during process of signature generation and the signer cannot correlate the signed document with the act of signing.

There were many proposals for blind signature schemes published based on a single hard problem such as FAC, DL or ECDL problems [8-12]. All of them remain secure and are resistant to attacks. However, if one finds a solution for the underlying hard problem hence break the corresponding signature schemes easily. In [6, 7] proposed blind signature schemes, which requires the simultaneous solving of two independent difficult problems. However, they have high complexity.

Blind multi-signatures are signatures in which the group of signers (*B*) do not know what they are signing, thus the term “blind”. Such signatures are possible because the content of the message *M* has been “blinded” to become *M′* before the message is provided to the collective to sign. Thus, the signing collective signed *M′* and not *M*. Specifically, the user *A* needs the collective *B* to sign message *M*; However, *A* does not provide *B* with *M* but rather blinds *M* to *M′* and then provides the blinded *M′* to *B* to sign. After receiving the signed *M′*, *A* unblinds the message to obtain the signature for *M*. Therefore, *A* has a signature for *M* without providing *B* with information on *M*.

Received July 8, 2018; Revised February 9, 2019; Accepted March 12, 2019

In 1999, Popescu [13] presented blind multi-signatures based on elliptic curves. In 2005, Chow et al. proposed two blind signature schemes partially based on Bilinear Pairings [14]. In 2011, Moldovyan [15] presented a blind signature scheme based on the GOST R34.10-2001 signature standard. In 2012, Nguyen and Dang [16] provided enhanced security for voting protocols on the Internet using blind signatures; Swati Verma et al. also presented New Proxy Blind Multi Signature based on Integer Factorization and Discrete-Logarithm Problems [17]. In 2013, Panda et al. researched blind signing authorizations in electronic voting processes [18]. In 2014, Hua Sun et al. proposed New Certificateless Blind Ring Signature Scheme [19]. In 2016, Shilbayeh et al. proposed security schemes for electronic voting processes [20]. In 2017, Minh et al. proposed New Blind Signature Protocols Based on a New Hard Problem [21]; Salome James et al. proposed Identity-Based Blind Signature Scheme with Message Recovery [22].

In this paper, we propose a new digital signature scheme from two difficult problems based on the RSA digital signature scheme [23] and the Schnorr digital signature scheme [24]. We expand our functionality to construct the blind signature scheme and the blind multi-signature scheme. This helps new blind digital signature schemes inherit some advantages of the security of the signature schemes that had been proven in practice. The organization of the paper is as follows: section 2 provides the related theories and schemes. In section 3, we shall design a new signature scheme, which requires the simultaneous breaking of the factorization and discrete logarithm. We expand our functionality to construct a new blind signature scheme and a new blind multi-signature scheme. In the last section, the conclusion of our research work will be presented.

2. Related Theories and Schemes

The following notations are used:

- p is a prime number, with structure $p=2n+1$, $n = q'q$ with q, q' are the strong prime numbers [25]
- H is a collision-resistant hash function
- α is a generator of order n over Z_p^*
- $q|p-1$: q is the divisor of $p-1$
- $\varphi(n)$ is the Euler function
- e is the public key and d is the secret key in RSA

2.1. Discrete Logarithm Problem (DLP) [26]

This problem is described as follows: Given an instance (y, p, q, α), where $y = \alpha^x \bmod p$ for some $x \in Z_q^*$, to derive x.

2.2. Integer Factorization Problem [26]

The integer factorization problem is the following: given a positive integer n, find its prime factorization, i.e., find pairwise distinct primes p_i and positive integers e_i such that $n = p_1^{e_1} p_2^{e_2} ... p_k^{e_k}$. The *eth* root problem is the following: Given a group G of unknown order, a positive integer $e < |G|$ and an element $a \in G$, find an element $b \in G$, such that $b^e = a$.

If $G = Z_n$, with n being the product two primes p and q, and the condition that $b \in G$, is replaced by $b \in Z_n$, we get the RSA problem. In this case the order of the group can be found by factoring n.

2.3. RSA Signature Scheme

2.3.1. Key Generation

- Choose large distinct primes p and q, and compute $n = pq$.
- Choose e such that $\gcd(e, \varphi(n)) = 1$. The pair (n, e) is published as the public key.
- Compute d such that $de = 1 \bmod \varphi(n)$. The pair (n, d) is used as the secret key.

- Let *H* and computed from the signed document *M*. It is proven that obtaining a private key from the public key is very difficult unless you know the factorization of *n* [1, 23].

2.3.2. Signature Generation Procedure

The signature pair can be computed easily by a signer who knows the message and secret key (*p*, *q*, *d*) as follows: $S = H^d \bmod n$. Then the (M, S) is the digital signature of *M*.

2.3.3. Signature Verification Procedure

It is easy to verify that (M, S) is valid by checking if the following equality holds: $S^e = H \bmod n$, where equality follows because $ed \equiv 1 \bmod \varphi(n)$. The hash function *H* is used to enhance security and efficiency.

2.4. Schnorr Signature Scheme

2.4.1. Key Generation

- Choose randomly a secret key x with $x \in Z_q^*$. Compute $y = \alpha^x \bmod p$.
- Let *H* and computed from the signed document *M*. The public key is (p, α, y). The secret key is x.

2.4.2. Signature Generation Procedure

To sign a message *M* the signer performs the following steps:

- Choose a random *k* such that $1 < k \le q-1$. Compute $R = \alpha^k \bmod p$.
- Compute $E = H(M \| R)$. Compute $S = k - xE \bmod q$. Then the pair (E, S) is the digital signature of *M*. The signer repeats these steps for every signature.

2.4.3. Signature Verification Procedure

A signature (E, S) of a message *M* is verified as follows:

- Compute $R^* = \alpha^S y^E \bmod p; E^* = H(M \| R^*)$.
- Compare the values E^* and E. If $E^* = E$ then signature is valid. The verifier accepts a signature if all conditions are satisfied and rejects it otherwise.

3. Blind Signature Scheme based on Difficulty of Solving Simultaneously Two Difficult Problems

3.1. New Signature Scheme based on Two Difficult Problems

To design the new blind signature scheme and blind multi-signature scheme, we first propose a new digital signature scheme as a basic structure of our developing blind signature schemes. Breaking the modified signature schemes described below requires simultaneous solving two different difficult problems, computing discrete logarithm in the ground field $GF(p)$ and factoring n. In this signature scheme, *p* is a prime number, with structure $p = 2n+1$.

The following modifications have been proposed to design the new basic signature scheme: α is used a value having order equal to *n* modulo *p*; additional element *e* of the public key; additional element *d* of the private key; instead of the value *S* in the signature verification equation it is introduced the value S^e. The values *e* and *d* are generated like in the RSA cryptosystem. As the value *e* it is selected a small number (having size from 16 to 32 bits) that is relatively prime to $\varphi(n) = (q-1)(q'-1)$. The value *d* is computed as follows $d = e^{-1} \bmod \varphi(n)$. The process of the basic structure is describe following:

3.1.1. Key generation

- Choose randomly an integer $e \in Z_n$ such that $\gcd(e, n) = 1$.
- Calculate a secret *d* such that $ed \equiv 1 \bmod \varphi(n)$.
- Choose randomly a secret key x with $x \in Z_p^*$. Compute $y = \alpha^x \bmod p$. The public key is (*e*, α, *y*). The secret key is (x, *d*).

3.1.2. Signature Generation Procedure

- Compute $R = \alpha^k \bmod p$, where *k* is a secret random number, $1 < k \le n-1$
- Compute $E = H(M \| R)$
- Calculate the value *S*, such that $S^e = k - xE \bmod n$, i.e. $S = (k - xE)^d \bmod n$ such that $R = \alpha^{S^e} y^E \bmod p$. The signature is the pair (E, S).

3.1.3. Signature Verification Procedure

- Compute $R^* = \alpha^{S^e} y^E \bmod p; E^* = H(M \| R^*)$.
- Compare the values E^* and E. If $E^* = E$, then signature is valid. Otherwise, the signature is rejected as invalid.

Solving the discrete logarithm problem in $GF(p)$ is not sufficient for breaking the modified scheme. Now to break the signature scheme it is required to know the factorization of *n*. The solution of the discrete logarithm problem leads to the computation of the secret key x and to the possibility to calculate the value $S^* = (k - xE) \bmod n$. However, to calculate the signature S is required to extract the *eth* root modulo *n* from the value S^*. This requires factoring the modulus *n*.

3.2. New Blind Signature Scheme

The proposed signature scheme using two difficult problems can be used as a basic algorithm for constructing blind signature scheme which is similar to the blind signature scheme based on the RSA [23] and Schnorr signature schemes [24]. This approach will be used to develop the following blind signature scheme, which requires the simultaneous solving of these two difficult problems. There are six rounds in the blind signature scheme.

- Round 1 (Signer B): Selects a random value $1 < k \le n-1$ and computes $R = \alpha^k \bmod p$. Then he sends *R* to the user A.
- Round 2 (User A): Selects two random values ε and τ and computes $R' = R\alpha^{\varepsilon} y^{\tau} \bmod p$. Then user *A* computes $E' = H(M \| R')$ and $E = E' - \tau$. Then he sends *E* to the signer *B*.
- Round 3 (Signer B): Computes the value $D = k - xE \bmod n$, such that $R = \alpha^D y^E \bmod p$. The value of *D* is sent to the user.
- Round 4 (User A): Selects a random value $\mu < n$ (masking factor), computes the value $D' = \mu^e (D + \varepsilon) \bmod n$ and sends D' to the signer *B*.
- Round 5 (Signer B): Computes the value $D'' = D'^d = \mu^{ed} (D + \varepsilon)^d = \mu (D + \varepsilon)^d \bmod n$ and sent to the user.
- Round 6 (User A): Computes the values (E', S') with $E' = E + \tau$ and $S' = D'' / \mu \bmod n$. The signature is the pair (E', S').

Verification of Blind signature scheme: The verification procedure described in the blind signature scheme is the same as in the previous basic digital signature scheme, i.e., using the verification equation is $R'^* = \alpha^{S'^e} y^{E'} \bmod p$.

3.3. New Blind Multi-signature Scheme

Assume that user *A* asks the entire group *B* who has the authority to include *n* signers to sign document *M*; however, this user does not want this authorized group to know the content of *M*. First, this user blinds the document *M*, which becomes document *M′*. Then, *M′* is sent to the authorized signing group. This group signs *M′* and sends it back to the requesting user. Then, the user unblinds *M′* to *M* and checks the received signature. If the signature is valid, then the user has a valid signature on document *M.* A blind multisignature scheme has three participants: User *A*, signers *B* and a trusted third party (TTP). The implementation process for blind signing the message *M* includes three schemes:

3.3.1. Key Generation

- Choose randomly an integer $e \in Z_n$ such that $\gcd(e,n)=1.$ Calculate a secret *d* such that $ed \equiv 1 \bmod \varphi(n)$.
- Choose randomly a secret key x_i with $x_i \in Z_p^*$. Compute $y_i = \alpha^{x_i} \bmod p$ and send it to TTP to compute *y* of signing group: $y = \prod_1^n y_i \bmod p, i = 1,2,...n.$ The public key is (*e*, α, *y*). The secret key is (x_i , *d*).

3.3.2. Signature Generation Procedure

- Round 1 (Signer group B): each user in the signing group selects a random value $1 < k_i \le n-1$ and computes $R_i = \alpha^{k_i} \bmod p.$ Then he sends R_i to TTP to compute $\bar{R}$ such as: $\bar{R} = \prod_1^n R_i \bmod p = \alpha^{\sum_{i=1}^{n} k_i \bmod p} \bmod p.$
- Round 2 (User A): Selects two random values ε and τ and computes $R' = \bar{R}\alpha^{\varepsilon} y^{\tau} \bmod p.$ Then computes $E' = H(M \| R')$ and $E = E' - \tau$ and sends to B.
- Round 3 (Signer group B): each user in the signing group computes the value $D_i = k_i - x_i E \bmod n,$ such that $R_i = \alpha^{D_i} y_i^{E} \bmod p.$ The value of D_i is sent to TTP to computes $\bar{D}$ such as: $\bar{D} = \sum_{i=1}^{n} D_i \bmod n$ and sends to A.
- Round 4 (User A): Selects a random value $\mu < n,$ computes the value $D' = \mu^e (\bar{D} + \varepsilon) \bmod n$ and sends to B.
- Round 5 (Signer group B): Computes $D'' = D'^d = \mu^{ed} (\bar{D} + \varepsilon)^d = \mu (\bar{D} + \varepsilon)^d \bmod n$ and sends to A.
- Round 6 (User A): Computes the values (E', S') with $E' = E - \tau$ and $S' = D'' / \mu \bmod n$
- The signature is the pair (E', S') .

3.3.3. Signature Verification Procedure

The verification procedure described in the blind signature scheme is the same as in the previous basic digital signature scheme, i.e., using the verification equation is $R'^{*} = \alpha^{S'^{e}} y^{E'} \bmod p.$

4. Analysis of the Proposed Blind Signature Security

4.1. Correctness

Theorem 1: The signature (E', S') is a valid blind signature scheme corresponding to the message *M*.

- Blind signature Scheme:
  Proof: In accordance with the rounds 4, 5 and 6 we have

$$S'^{e} \equiv \frac{D''^{e}}{\mu^{e}} \equiv \frac{D'^{de}}{\mu^{e}} \equiv \frac{\mu^{e}(D+\varepsilon)}{\mu^{e}} \equiv (D+\varepsilon) \bmod n.$$

  Using the condition $S'^{e} \equiv (D+\varepsilon) \bmod n,$ correctness of the scheme is proved as follows:

$$\begin{aligned} R'^{*} &\equiv \alpha^{S'^{e}} y^{E'} \equiv \alpha^{D+\varepsilon} y^{E+\tau} \equiv \alpha^{D} y^{E} \alpha^{\varepsilon} y^{\tau} \\ &\equiv R\alpha^{\varepsilon} y^{\tau} \ (\bmod p) \quad \Rightarrow \quad E'^{*} = E'. \end{aligned}$$

- Blind multi-signature Scheme: Instead of the value D and R in the proof equations in the blind signature scheme, it is replaced by the value $\bar{D}$ and $\bar{R}$. The result is like the blind signature scheme.

4.2. Unlinkability

In a blind signature scheme, the unlinkability property (or blindness property) makes it impossible for the signer to derive the link between a given signature and the instance of the signing scheme which produces the blinded form of that signature. Theorem 2: The scheme provides unlinkability property in the case when the message *M* and signature (E', S') will be presented to the signer.

- Blind signature scheme:
  Proof: With equal probability of each of the users, who participated in the blind signature scheme, they could provide a signature on a document *M*. This can lead to the following statement: from the fact that any triple (R, D, E) from the set of such triples formed by the signer may be associated with the signature (E', S') of this document *M*. Indeed, since $R = \alpha^D y^E \bmod p$ (see round 3 of the scheme) and $R' = \alpha^{S'^e} y^{E'} \bmod p$, then the relation: $\frac{R'}{R} \equiv \alpha^{S'^e - D} y^{E'-E} \equiv \alpha^{\varepsilon} y^{\tau} \pmod p$. So, when choosing random equiprobable values τ and ε, the signature (E', S') with equal probability could be generated with any user in the process of blind signing.
- Blind multi-signature scheme: Instead of the value D and R in the proof equations in the blind signature scheme, it is replaced by the value $\bar{D}$ and $\bar{R}$. The result is like the blind signature scheme.

4.3. Randomization

The signer had better inject one or more randomizing factors into the blinded message such that the attackers cannot predict the exact content of the message the signer signs. Theorem 3: The scheme provides randomization property.

- Blind signature scheme:
  Proof: In the proposed scheme, attackers are infeasible to sign a valid signature (E', S') on behalf of the original signer. The signer selects a random value $1 < k \le n-1$ and computes $R = \alpha^k \bmod p$ and sends *R* to the user *A*. To get a random value k from R is computationally infeasible (it is difficult to determine k because that the derivation is solving the discrete logarithm problem). Therefore, in the proposed scheme, attackers cannot remove the random k from the corresponding signature (E', S') of message *M*.
- Blind multi-signature scheme: Instead of the value *k* and *R* in the proof equations in the blind signature scheme, it is replaced by the value k_i and R_i. The result is like the blind signature scheme.

4.4. Unforgeability

It means that only the signer can generate the valid signature. The intruder may attack the proposed scheme by following way. Intruder tries to derive the signature (E', S') for a given message *M* by letting one integer fixed and finding the other one. For example, intruder selects E' and tries to figure out the value of S' satisfying $R' = \alpha^{S'^e} y^{E'} \bmod p$ and vise-versa. To do this, intruder first chooses at random an integer R'. He then computes $S'^e = \log_\alpha R' y^{-E'} \bmod p$ and only if two difficult problems is breakable.

4.5. Performance

The security of the new blind digital signature scheme has been proven to be equivalent to solving two independent difficult problems simultaneously including IFP and DLP. We investigate the performance of our schemes in the number of modular multiplication, number of hashing operation, number of random number generation, number of inverse computations, number of cube root and number of modular exponentiation.

Time for computing modular addition and subtraction are ignored, since it is much smaller than time for computing modular exponentiation, modular multiplication and modular inverse. The comparisons of computation costs performed by the user, signer and verifier between the proposed blind signature scheme and the scheme of [27] are summarized in Table 1 and Table 2.

Table 1. The Computation Costs of the Proposed Blind Multi-signature Scheme and the Scheme of [27]

Type of Operations	Performed by the user		Performed by the signer	
	Our scheme	[27]	Our scheme	[27]
Numbers of Exponentiations	3	2	2	1
Numbers of Inverses	1	1	0	0
Numbers of Hashings	1	1	0	0
Numbers of Multiplications	3	5	2	1
Numbers of cube root	0	0	0	1
Random number generation	3	3	1	1

Table 2. The Computation Costs of the Proposed Blind Multi-signature Scheme and the Scheme of [27]

Type of Operations	Performed by the verifier	
	Our scheme	[27]
Numbers of Exponentiations	3	2
Numbers of Hashings	1	1
Numbers of Multiplications	1	3

This section will compare the performance of our blind multi-signature scheme with the blind multi-signature scheme in [27] also design the blind multi-signature scheme, but the basic scheme is based on the Rabin and the Schnorr schemes and using S^3 instead S in the Signature verification procedure. Our blind multi-signature scheme is based on the RSA and the Schnorr schemes and using S^e instead S in the Signature verification procedure.

From the comparison Table 1 and Table 2, we realized that the time costs of the proposed blind multi-signature scheme has more the time cost than the scheme in [27] with performed by uer and with performed by the Verifier. However, with performed by the signer, it is easier to perform because it is not required to extract the square 3 root to calculate the D'' value (D'' is used to computing the blind signature S'). And therefore, they can be applied in practice.

5. Conclusion

In this paper, we proposed a new signature scheme from two difficult problems IFP and DLP. Then expanding to propose a single blind signature scheme and a blind multi-signature scheme, which requires the simultaneous breaking of two independent difficult problems, these are based on the RSA signature scheme and Schnorr signature scheme. It has been proved to be correct, blind, unforged, random and provides higher level security than schemes that based on a single hard problem. The results show that the proposed blind multi-signature signature scheme are safe and present high performance; therefore, they can be applied in practice such as the proposed schemes can be applied in election systems and digital cash schemes.

References

[1] Menezes AJ, Vanstone SA. Handbook of Applied Cryptography. CRC Press. 1996: 780.
[2] Z Shao. Security of a new digital signature scheme based on factoring and discrete logarithms. *International Journal of Computer Mathematics*. 2005; 82(10): 1215-1219.
[3] TH Chen, WB Lee, G Horng. Remarks on some signature schemes based on factoring and discrete logarithms. *Applied Mathematics and Computation*. 2005: 1070-1075.
[4] J Buchmann, A May, U Vollmer. Perspectives for cryptographic long term security. *Communications of the ACM.* 2006; 49(9): 50-55.

[5] D Chaum. *Blind signatures for untraceable payments*. Advances in Cryptology, CRYPTO'82. 1982: 199-203.
[6] NMF Tahat, SMA Shatnawi, ES Ismail. New Partially Blind Signature Based on Factoring and Discrete Logarithms. *Journal of Mathematics and Statistics*. 2008; 4(2): 124-129.
[7] NMF Tahat, ES Ismail, RR Ahmad. A New Blind Signature Scheme Based On Factoring and Discrete Logarithms. *International Journal of Cryptology Research*. 2009; 1(1): 1-9.
[8] HF Huang, CC. Chang. A new design of efficient blind signature scheme. *The Journal of Systems and Software*. 2004: 73: 397-403.
[9] JL Camenish, JM Priveteau, MA Stadler. *Blind signature based on the discrete logarithm problem.* Advances in Cryptology (Eurocrypt '94), LNCS 950, Springer-Verlag. 1994: 428-432.
[10] D Jena, SK Jena, B Majhi, SK Panigrahy. A novel ECDLP-based blind signature scheme with an illustration. *Web engineering and applications*. 2008: 59-68.
[11] D Zheng, K Chen, W Qiu. *New Rabin-like signature scheme.* Workshop Proceedings of the Seventh International Conference on Distributed Multimedia Systems, Knowledge Systems Institute. 2001: 185-188.
[12] FG Jeng, TL Chen, TS Chen. An ECC-Based Blind Signature Scheme. *Journal of networks*. 2010; 5(8): 921-928.
[13] C Popescu. Blind Signature and BMS Using Elliptic Curves. Studia univ. "babes–bolyai", Informatica. 1999: 43-49.
[14] SS Chow, et al. Two Improved Partially Blind Signature Schemes from Bilinear Pairings. *Information Security and Privacy.* 2005; 3547: 316-328.
[15] NA Moldovyan. Blind Signature Protocols from Digital Signature Standards. *International Journal of Network Security*. 2011: 13(1): 22-30.
[16] TAT Nguyen, TK Dang. Enhanced security in internet voting protocol using blind signature and dynamic ballots. *Electronic Commerce Research.* 2013; 13(3): 257-272.
[17] S Verma, BK Sharmal. New Proxy Blind Multi Signature based on Integer Factorization and Discrete-Logarithm Problems. 2012; 1(3): 185-190.
[18] S Panda, et al. An Application of time stamped proxy blind signature in e-voting. *International Journal on Computer Science and Engineering.* 2013; 5(6): 547-552.
[19] H Sun, Y Ge. New Certificateless Blind Ring Signature Scheme. *TELKOMNIKA Indonesian Journal of Electrical Engineering*. 2014; 12(1): 778-783.
[20] NF Shilbayeh, RA Al-Saidi, AH Alsswey. Evaluation and Analysis of the Secure E-Voting Authentication Preparation Scheme. *International Journal of Computer and Information Engineering*. 2016: 10(3): 560-568.
[21] H Minh, N Hai, N Moldovyan, T Giang. New Blind Signature Protocols Based on a New Hard Problem. *The International Arab Journal of Information Technology*. 2017; 14(3): 307-313.
[22] S James, T Gowri, GVR Babu, PV Reddy. Identity-Based Blind Signature Scheme with Message Recovery, *International Journal of Electrical and Computer Engineering (IJECE)*. 2017; 7(5): 2674-2682.
[23] R Rivest, A Shamir, L Adleman. A method for obtaining digital signatures and public key cryptosystems. *Communications of the ACM*. 1978; 21(2): 120-126.
[24] Schnorr CP. Efficient signature generation by smart cards. *Journal of Cryptology*. 1991; 4: 161-174.
[25] M Blum. CRYPTO. 1981: 11-15.
[26] Menezes AJ, Vanstone SA. Handbook of Applied Cryptography. CRC Press. 1996.
[27] DN Tan, HN Nam, MN Hieu. *Blind signature scheme and blind multi-signature scheme based on two hard problems*. The 20th National Conference on Electronics, Communications and Information Technology-REV-ECIT. 2017: 95-100.