

A High-efficiency Discrete Logarithm-based Multi-proxy Blind Signature Scheme via Elliptic Curve and Bilinear Mapping

Lin Teng and Hang Li
(Corresponding author: Hang Li)

Software College, Shenyang Normal University
Shenyang 110034, China
(Email: 1451541@qq.com)

(Received July 14, 2017; revised and accepted Oct. 22, 2017)

Abstract

Generally, multi-proxy blind signature scheme has been proposed to provide privacy protection. However, multi-proxy blind signature scheme requires their signatures of all the proxy signers. So there are some drawbacks about proxy signature. Proxy knows all the information of signers, it will lead to information leakage. Therefore, we propose a discrete logarithm-based multi-proxy blind signature scheme in this paper. The new scheme combines Elliptic curve, bilinear mapping and blind signature. Elliptic curve can avoid that a proxy signer is absent or makes mistakes causing unsuccessful signature. It enhances the robustness and fault tolerance. Meanwhile, blind idea makes proxy signers have no information about sensitive message. Bilinear mapping can reduce the computation time. Finally, the security analysis shows that this new scheme is with more flexibility and fault tolerance than traditional multi-proxy signature schemes. And it can be widely used in many real engineering applications.

Keywords: Blind Signature; Bilinear Mapping; Discrete Logarithm; Elliptic Curve; Multi-proxy Blind Signature Scheme

1 Introduction

Proxy signature means that a designated proxy signer can generate valid signatures on behalf of the original signer in an agent signature scheme [12, 13, 18]. It allows the original signer to delegate the signature to the proxy signer and generate an effective proxy signature. Proxy signature contains initialization process, authorization process, proxy signature generation process and proxy signature verification process. Traditional proxy signature schemes are easily attacked and sensitive information is leaked [7, 10, 16]. Then in order to meet the actual de-

mand, some improved proxy signatures are proposed.

Xie *et al.* [26] proposed that in the system initialization phase, when each user's public key was certified by CA, the registering user must perform a challenge-response protocol or zero-knowledge protocol to convince CA that he knew the private key corresponding to his public key. Ma *et al.* [17] proposed a proxy signature-based re-authentication scheme for secure fast handoff in WMNs. To begin with, he designated the mesh portal (MPP) as the authenticator of the MH that initially accessed a certain mesh domain. After the successful initial association, the MH was authorized to obtain a temporal proxy delegation of the MPP for the preparation of handoff. Making use of the proxy delegation in handoff case, the MH could efficiently associate with a target MAP connecting to the MPP by performing the proposed re-authentication scheme, in which mutual authentication and pairwise master key (PMK) establishment were performed between the MH and the MAP in a three-way handshake procedure without involving any other parties.

A proxy signature scheme allowed a proxy signer to sign messages on behalf of an original signer within a given context. Most identity based proxy signature schemes currently known employ bilinear pairings. So an identity based proxy ring signature (IBPS) scheme from RSA without pairings was constructed, and the security was proved under the random oracle model [4]. Lan *et al.* [11] put forward a new security cloud storage data encryption scheme based on identity proxy re-encryption. This scheme could flexibility share data with other users security without fully trusted cloud. For the detailed structure, he used a strong unforgeable signature scheme to make the transmuted ciphertext had publicly verification combined identity-based encryption. Furthermore, the transformed ciphertext had chosen-ciphertext security under the standard model. Liu *et al.* [14] constructed the initial threshold proxy signature scheme independently, which is an improvement for proxy signature scheme.

In a (t, n) threshold proxy signature scheme, an original signer delegates his signature right to n proxy signers, in which cooperation of t proxy signers can produce a valid proxy signature. Then a lot of threshold proxy signature schemes are proposed [2, 8, 15, 22, 28, 29].

Through the above analysis, we make a summary on the type of proxy signature scheme.

- 1) Proxy multi-signature [27]. $m \rightarrow 1$, m original signers delegate the signature to one proxy signer.
- 2) Multi-proxy signature [19, 23]. $1 \rightarrow n$, an original signer delegates the signature authority to n proxy signers.
- 3) Multi-proxy multi-signature [3, 12]. $m \rightarrow n$, m original signers delegate the signature to n proxy signers. It is an extension of $m \rightarrow 1$ and $1 \rightarrow n$ applications and increases the flexibility of scheme.

The rest of this paper is organized as follows. Section 2 and Section 3 introduce Bilinear map and Elliptic curve respectively. the system model for wireless body area network. Section 3 outlines the proposed scheme to analyze detailed processes. Experience and security analysis are given in Section 4. Section 5 finally concludes the paper.

2 Bilinear Map

Supposing G_0 and G_1 are two p -order multiplicative cyclic groups [5]. g is a generator of G_0 and e is a bilinear map, namely $e : G_0 \times G_0 \rightarrow G_1$, then for any $i, j, k \in G_0$ and $a, b \in Z_p$, the map e has the following properties [21]:

- 1) Bilinear: $e(i^a, j^b) = e(i, j)^{ab}$.
- 2) Non-degenerative: $e(g, g) \neq 1$.
- 3) Polymerizability: $e(i \cdot j, k) = e(i, k) \times e(j, k)$.

If the group operation is highly computable in G_0 and the map $e : G_0 \times G_0 \rightarrow G_1$, then the group is called bilinear. So map e is commutative: $e(g^a, g^b) = e(g, g)^{ab} = e(g^b, g^a)$.

3 Elliptic Curve (ECC)

The elliptic curve crypto-system is currently known as the public key system, which provides the highest encryption intensity for each bit [1]. Assuming that q is a big prime number. F_q is the finite field of q . r is a prime number. Therefore, Elliptic curve EC of F_q is defined as,

$$y^2 = x^3 + ax + b.$$

Where $(4a^3 + 27b^2) \bmod q \neq 0$. Elliptic curve encryption algorithm is with small key length, high safety performance, little digital signature time. In the application of intelligent terminal, it has great potential development, such as PDA, mobile phones. In the network,

ECC algorithm also ensures its real-time collaborative work. Higher sensitivity level data encrypted by ECC algorithm, the speed can satisfy the large amount data, and the high security can well protect the safety of the system.

4 New Multi-proxy Blind Signature Scheme

First, we give the parameters used in this paper as shown in Table 1.

Assuming that the discrete logarithm problem in Z_p is difficult. And proxy signers, less than t , are dishonestly, that is, they unfaithfully execute the protocol.

4.1 Signature Scheme Based on Bilinear Map

Supposing that G_1 is the additive group with generator P and q order. G_2 is the multiplicative group with q order. Bilinear map is defined as $e : G_1 \times G_1 \rightarrow G_2$. $H_1 : 0, 1^* \rightarrow Z_q$ and $H_2 : 0, 1^* \rightarrow G_1$ are two Hash functions.

Detailed signature scheme based on bilinear map is as follows.

- 1) Key generation algorithm.
 - Private key generation. Randomly selecting $s \in Z_q^*$ as system private key.
 - Public key generation. P_{pub} as system public key, where $(G_1, G_2, q, P, P_{pub}, H_2)$ are public parameters.
- 2) Signature algorithm. For $M \in 0, 1^*$, signer computes $P_M = H_2(M) \in G_1$, $S_M = sP_M$. So the signature of information M is S_M .
- 3) Verification process. Verifying equation $e(S_M, P) = e(H_2(M), P_{pub})$. If it is correctness, then user accepts signature.

4.2 Generation Phase of Proxy Certificate

Assuming that m original signers and n proxy signers hold consultation the message range and the validity period of proxy for the proxy signature, and then it forms the Proxy Agent signature protocol W (including the public key of all original signers and proxy signers).

- 1) U_i randomly selects $k_{U_i} = Z_q^*$, calculates $L_{U_i} = g^{k_{U_i}} \bmod p$, and sends it to other $m - 1$ original signers and proxy signers. Each p_j randomly selects $k_{p_j} \in Z_q^*$, calculates $L_{p_j} = g^{k_{p_j}} \bmod p$, and sends it to other $n - 1$ proxy signers and m original signers. Finally, all original signers and proxy signers compute and save $K = \prod_{i=1}^m L_{U_i} \prod_{j=1}^n L_{p_j} \bmod p$.

Table 1: Parameter explanation

Symbol	Definition
p, q	Prime number. Where q is large prime factor of $p - 1$.
g	$g \in Z_p^*, g^q \equiv 1(mod p)$.
$h(\cdot)$	A secure one-way hash function.
\parallel	Concatenation of bit strings.
t	The threshold value.
x_{u_i}	Private key of original signer.
U_i	Original signer.
$y_{u_i} = g^{x_{u_i}} \bmod p$	Public key of original signer.
$x_{p_j} \in Z_q^*$	The private key of proxy signer.
$p_j = (1, 2, \dots, n)$	Proxy signer.
$y_{p_j} = g^{x_{p_j}} \bmod p$	Public key of proxy signer.
ID_j	The identity information.
U_I	The message owner.

2) U_i calculates $V_{U_i} = (h(W)x_{U_i} + k_{U_i}K) \bmod q$, sends it to other $m - 1$ original signers and n proxy signers. Personal delegation certificate of U_i is (L_{U_i}, V_{U_i}) . p_j calculates $V_{p_j} = (h(W)x_{p_j} + k_{p_j}K) \bmod q$, sends it to other $n - 1$ proxy signers and m original signers, then delegation certificate of p_j is (L_{p_j}, V_{p_j}) .

3) Each $\frac{U_i}{p_j}$ verifies the correctness of the $\frac{V_{U_i}}{V_{p_j}}$ by following formulas:

$$g^{V_{U_i}} = y_{U_i}^{h(W)} L_{U_i}^K \bmod p, i = 1, 2, \dots, m.$$

$$g^{V_{p_j}} = y_{p_j}^{h(W)} L_{p_j}^K \bmod p, j = 1, 2, \dots, n.$$

If V_{U_i} and V_{p_j} are correct, then each proxy signer p_j computes $V = (\sum_{i=1}^m V_{U_i} + \sum_{j=1}^n V_{p_j})$ to generate the delegation proxy certificate K, V .

4.3 Generation Phase of Proxy Signature Key

When signature enters into $i - th$ phase, U uses the signature private key $x_{U_{i-1}}$ of $(i - 1)th$ phase to calculate the signature private key x_{U_i} of $i - th$ phase.

$$x_{U_i} = x_{U_{i-1}} \bmod n.$$

Each p_j randomly selects $n_j \in Z_q^*$ and $a_{je} \in Z_q^*$, calculates and broadcasts $N_j = g^{n_j} \bmod p$ and $g^{a_{je}} \bmod p$ to other proxy signers. It requires that the product of any t N_j of the proxy signers is unequal. Meanwhile, It constructs a polynomial $f_j(x) = \sum_{e=0}^{t-1} a_{je}x^e \bmod q$, to satisfy $a_{j0} = (x_{p_j} + n_jV)$. p_j calculates and sends the sub-secret $f_j(ID_i) \bmod q$ for other $p_i (i = 1, 2, \dots, n, i \neq j)$, Calculate and save $f_j(ID_j) \bmod q$.

4.4 Generation Phase of Proxy Signature

Set the message m will be generated according to the will of the original signer. In this algorithm, each proxy

member D_i will produce a part proxy signature for m according to generated proxy key K_i . Then it appoints one agent member M to collect all the proxy signatures and get the final proxy signature scheme.

1) Each proxy member D_i randomly generates integer $k_{p_i} \in Z_q^*$, computes $r_{p_i} = e(p, p)^{k_{p_i}}$. And r_{p_i} is broadcast to other $l - 1$ proxy members.

2) Each proxy member D_i calculates $r_p = \prod_{i=1}^l r_{p_i}$ and $c_p = H_1(m || r_p)$, $U_{p_i} = c_p s_{p_i} + k_{p_i}p$. So the part proxy signature of each proxy member for m is binary array (c_p, U_{p_i}) .

3) Each proxy member D_i sends U_{p_i} to assigned member M .

4) M puts each proxy member's proxy signature into equation $c_p = H_1(m || \prod_{i=1}^l e(U_{p_i}, p)(eH_2(\xi), pK_0 + pK_i))^{-c_p}$.

When all the proxy signature verifications are passed. M calculates $U_p = \sum_{i=1}^l U_{p_i}$. So the proxy signature of each proxy member for m is quaternion array (m, c_p, U_{p_i}, ξ) .

4.5 Proxy Signature Verification Phase

Generated delegation proxy certificate (K, V) can verify the the validity of final signature. Due to $Y = \prod_{i=1}^n y_{p_i} \bmod p$ and $Q = \prod_{i=1}^n N_i \bmod p$ The verification is as follows:

$$g^V = K^K \left(\prod_{i=1}^m y_{U_i} \prod_{j=1}^n y_{p_j} \right)^{h(W)} \bmod p.$$

$$g^S = (YQ^V N^N)^{B+h(M)h(W)} \bmod p.$$

5 New Scheme Analysis

5.1 Security analysis

1) The security of the certificate.

Theorem 1. Under the discrete logarithmic problem (DLP) difficulty assumption, personal delegation certificate of $U_i(L_{U_i}, V_{U_i})$, personal proxy certificate (L_{p_j}, V_{p_j}) of p_j and delegation proxy certificate (K, V) are safe.

Proof. Assuming that the attacker A counterfeits a certificate (L'_{U_1}, V'_{U_1}) of U_1 , it needs to meet: $g^{V'_{U_1}} = y_{U_1}^{h(W)}(L'_{U_1})^{K'}$, $K' = L'_{U_1} \prod_{i=2}^m L_{U_i} \prod_{j=1}^n L_{p_j}$. Setting a known L'_{U_1} , through the above two formulas to solve V'_{U_1} , it needs to solve the discrete logarithm in Z_p , so personal delegation certificate of U_1 is safe. Similarly, certificate (L_{p_j}, V_{p_j}) of p_j is safe. \square

Let A counterfeits a delegation proxy certificate (K', V') , which needs to satisfy: $g^{V'} = K'^{K'} (\prod_{i=1}^m y_{U_i} \prod_{j=1}^n y_{p_j})^{h(W)} \text{mod} p$. Under the DLP difficulty assumption, (K, V) is security.

- 2) Unforgeability. There are two existence-unforgeabilities of proxy signature: existence authorization-unforgeability and proxy signature existence-unforgeability.

Theorem 2. Under the DLP difficulty assumption, the final proxy signature cannot be forged.

Proof. If A directly constructs B' and forges S , it needs to solve the discrete logarithm or first forge part signature S'_i . But we use the following explanation to verify that S'_i cannot be forged. If A randomly selects n_i and c_i . It uses $S'_i = (T_i c_i + n_i N)(B + \bar{M}h(W)) \text{mod} q$ to calculate S'_i , but when it computes $g^{S'_i}$, the process is very difficulty. It is also difficult to solve n_i and c_i by $N_i = g^{n_i} \text{mod} p$ and $C_i = g^{c_i}$ under the DLP difficulty assumption. To sum up, the new scheme satisfies unforgeability. \square

- 3) Non-repudiation. The original signature group cannot deny authorization to proxy signature group. The delegation proxy certificate (K, V) satisfies $C_i = g^{c_i}$. And $C_i = g^{c_i}$ refers to the private key information of all the original signers, so the original signature group cannot deny the authorization.

Proxy signature group cannot deny the signature of message M . In the proxy signature key generation phase, p_j only constructs the polynomial $f_j(x)$ satisfying $a_{j0} = (x_{p_j} + n_j V) \text{mod} q$ with its own private key, and verifies the public key y_{p_j} of p_j . And then it verifies the validity of the final signature. Therefore, the proxy signature group cannot deny its proxy signature.

- 4) Traceability. When a dispute occurring, the identity of the T proxy signers who actually participate in the signature can be identified according to the uniqueness of the N in the final signature, that is, the scheme is traceable for the actual identity of the signer involved.

- 5) Robustness. This new scheme adds a threshold proxy process in the proxy signature generation phase. Only t proxy signers can complete the signature. Therefore, when the several proxy signers cannot participate in the signature, it will not affect the implementation of this scheme. Namely, the scheme has good robustness and fault tolerance.

- 6) Blindness. U_I first uses the randomly number α and β to blind M as \bar{M} . Then it sends B and \bar{M} to the member p_i in E , and p_i wants to acquire message M through $\bar{M} = (\alpha^{-1}h(M||B') + \beta) \text{mod} q$, that is impossible. Therefore, each p_i in E cannot obtain the specific content of its signed message. So the scheme is with blindness.

- 7) Unlinkability. When U_I publishes the final signature of M , even if all p_i reserve intermediate variable B_i in each signature process and combine them to calculate B . By $B' = (\alpha B + \alpha\beta h(W)) \text{mod} q$ and $\bar{M} = (\alpha^{-1}h(M||B') + \beta) \text{mod} q$ to solve blind factor α and β . But α and β are randomly selected, p_i still does not know the final signature corresponding to which intermediate variables B_i , thereby p_i cannot combine the final signature with the detailed information of signature process. They are independent. So the scheme satisfies the unlinkability and effectively protect the privacy message.

- 8) Preventing the abuse of signature privilege. In W , it clearly stipulates the message range of proxy signature and the proxy valid period, this can prevent the proxy signer abuse of their proxy right. Because the proxy private key contains the original signer and proxy signer's private key, it only can be used for proxy signatures, which ensures that the proxy private key cannot be used for other purposes other than generating valid proxy signatures.

5.2 Proof of Correctness

Theorem 3. If the original signer and proxy signer strictly generate the correct parameters according to (1) and (2), the formula (1) and (2) can be verified.

Proof. $g^{V_{U_i}} = g^{h(W)x_{U_i} + k_{U_i}K} = y_{U_i}^{h(W)} L_{U_i}^K \text{mod} p$, that is, the formula (1) can be verified, and the same for formula (2). The original signer and proxy signer are established by verifying (1), (2) to confirm the security of their personal delegate certificate and personal proxy certificate. \square

6 Experiment And Analysis

We make comparison experiments to demonstrate the performance of our new scheme with MSBQ [6], EMRP [24], QPBW [25] and ECCB [20] with MATLAB 2014b platform. Supposing that bilinear pairings in this scheme is $e : G \times G \rightarrow G_T$. G_T is bilinear target group. Table 2

Table 2: Performance comparison with different schemes

Stage	MSBQ	EMRP	QPBW	ECCB	New scheme
Encryption	$p + 3e_T + 5h$	$2p + 2e_T + 4e + 2h$	$3p + 2e_T + 3e + 2h$	$4p + 3e + 2h$	$3e$
Derpytion	$3p + 2e_T + 4h$	$p + 3e_T + 3e + h$	$2p + 2e_T + 3h$	$3p + 4e_T + 3h$	$2e$

Table 3: Comparison results with different methods

Scheme	Blind signature scheme	Muilt-proxy mult-signature scheme	Security	Threshold signature scheme
MSBQ	NO	NO	YES	YES
EMRP	YES	NO	NO	NO
QPBW	YES	NO	NO	NO
ECCB	NO	YES	NO	YES
New scheme	YES	YES	YES	YES

is the computation complexity with different schemes. Where symbols p , e_T , e and h denote bilinear pairings operation, exponential operation in G_T , exponential operation in G and Hash operation. Their coefficients are operation numbers. From the table, we can know that our new scheme needs the least operation time. In addition, it has the optimal encryption results.

Table 3 is the comparison result with different methods in terms of qualitative analysis.

7 Conclusion

In this paper, we propose a discrete logarithm-based multi-proxy blind signature scheme in this paper. The new scheme combines Elliptic curve, bilinear mapping and blind signature. It can meet indistinguishable against adaptively chosen-ciphertext attacks in random oracle model. We also give security proof and efficiency analysis in this paper. And comparison with other proxy re-encryption schemes shows that our scheme is with high efficiency, more flexibility and fault tolerance. In the future, we will study more advanced re-encryption schemes taking communication cost between authorized user and proxy into consideration.

References

- [1] F. D. Aranha, R. Dahab, J. Pez, *et al.*, "Efficient implementation of elliptic curve cryptography in wireless sensors," *Advances in Mathematics of Communications*, vol. 4, no. 2, pp. 169-187, 2017.
- [2] W. C. Chang, H. F. Li and S. L. Yin, "Mixed symmetric key and elliptic curve encryption scheme used for password authentication and update under unstable network environment," *Journal of Information Hiding and Multimedia Signal Processing*, vol. 8, no. 3, pp. 632-639, May 2017.
- [3] H. Chen, Q. Xue, F. Li, *et al.*, "Multi-proxy multi-signature binding positioning protocol," *Security & Communication Networks*, vol. 9, no. 16, pp. 3868-3879, 2016.
- [4] L. Deng, H. Huang, Y. Qu, "Identity based proxy signature from RSA without pairings," *International Journal of Network Security*, vol. 19, no. 2, pp. 229-235, 2017.
- [5] X. Fu, X. Nie, F. Li, "Outsource the ciphertext decryption of inner product predicate encryption scheme based on prime order bilinear map," *International Journal of Network Security*, vol. 19, no. 2, pp. 313-322, 2017.
- [6] W. Guo, Z. J. Zhang, P. Y. Li, *et al.*, "Multi-proxy strong blind quantum signature scheme," *International Journal of Theoretical Physics*, vol. 55, no. 8, pp. 3524-3536, 2016.
- [7] M. S. Hwang, C. C. Lee, S. F. Tzeng, "A new proxy signature scheme for a specified group of verifiers," *Information Sciences*, vol. 227, pp. 102-115, 2013.
- [8] M. S. Hwang, Iuon-Chung Lin, Eric Jui-Lin Lu, "A secure nonrepudiable threshold proxy signature scheme with known signers", *Informatica*, vol. 11, no. 2, pp. 1-8, Apr. 2000.
- [9] M. S. Hwang, S. F. Tzeng and S. F. Chiou, "A non-repudiable multi-proxy multi-signature scheme", *Innovative Computing, Information and Control Express Letters*, vol. 3, no. 3, pp. 259-264, 2009.
- [10] M. S. Hwang, S. F. Tzeng, C. S. Tsai, "Generalization of proxy signature based on elliptic curves", *Computer Standards & Interfaces*, vol. 26, no. 2, pp. 73-84, 2004.
- [11] C. Lan, H. Li, S. Yin, *et al.*, "A new security cloud storage data encryption scheme based on identity proxy re-encryption," *International Journal of Network Security*, vol. 19, 2017.
- [12] C. C. Lee, T. C. Lin, S. F. Tzeng and M. S. Hwang, "Generalization of proxy signature based on factorization", *International Journal of Innovative Computing, Information and Control*, vol. 7, no. 3, pp. 1039-1054, 2011.
- [13] L. H. Li, S. F. Tzeng, M. S. Hwang, "Generalization of proxy signature based on discrete logarithms", *Computers & Security*, vol. 22, no. 3, pp. 245-255, 2003.
- [14] C. Y. Liu, A. H. Wen, L. C. Lin, *et al.*, "Proxy-protected signature secure against the undelegated

- proxy signature attack,” *Computers & Electrical Engineering*, vol. 33, no. 3, pp. 177-185, 2007.
- [15] J. Liu, S. L. Yin, H. Li and L. Teng, “A density-based clustering method for K-anonymity privacy protection,” *Journal of Information Hiding and Multimedia Signal Processing*, vol. 8, no. 1, pp. 12-18, Jan. 2017.
- [16] E. J. L. Lu, M. S. Hwang, and C. J. Huang, “A new proxy signature scheme with revocation”, *Applied Mathematics and Computation*, vol. 161, no. 3, PP. 799-806, Feb. 2005.
- [17] C. Ma, K. Xue, P. Hong, “A proxy signature-based re-authentication scheme for secure fast handoff in wireless mesh networks,” *International Journal of Network Security*, vol. 15, no. 2, pp. 122-132, 2013.
- [18] G. Pointcheval, “Anonymous proxy signatures,” *International Conference on Security and Cryptography for Networks, Springer Berlin Heidelberg*, pp. 201-217, 2008.
- [19] A. R. Sahu, S. Padhye, “Provable secure identity-based multi-proxy signature scheme,” *International Journal of Communication Systems*, vol. 28, no. 3, pp. 497-512, 2015.
- [20] N. Tahat, E. E. Abdallah, “A proxy partially blind signature approach using elliptic curve cryptosystem,” *International Journal of Mathematics in Operational Research*, vol. 8, no. 1, 87, 2017.
- [21] S. F. Tzeng, M. S. Hwang, “Digital signature with message recovery and its variants based on elliptic curve discrete logarithm problem”, *Computer Standards & Interfaces*, vol. 26, no. 2, pp. 61-71, Mar. 2004.
- [22] S. F. Tzeng, M. S. Hwang, C. Y. Yang, “An improvement of nonrepudiable threshold proxy signature scheme with known signers”, *Computers & Security*, vol. 23, no. 2, pp. 174-178, Apr. 2004.
- [23] S. F. Tzeng, C. C. Lee, and M. S. Hwang, “A batch verification for multiple proxy signature”, *Parallel Processing Letters*, vol. 21, no. 1, pp. 77-84, 2011.
- [24] K. G. Verma, B. B. Singh, “Efficient message recovery proxy blind signature scheme from pairings,” *Transactions on Emerging Telecommunications Technologies*, vol. 28, no. 11, 2017.
- [25] H. Wang, R. Shi, H. Zhong, *et al.*, “Quantum proxy blind signature based on W state,” *Chinese Journal of Quantum Electronics*, 2016.
- [26] Q. Xie, Y. X. Yu, “Cryptanalysis of two nonrepudiable threshold proxy signature schemes,” *International Journal of Network Security*, vol. 3, no. 1, pp. 18-22, 2006.
- [27] L. Yi, G. Bai, G. Xiao, “Proxy multi-signature scheme: A new type of proxy signature scheme,” *Electronics Letters*, vol. 36, no. 6, pp. 527-528, 2000.
- [28] S. Yin, L. Teng, J. Liu, “Distributed searchable asymmetric encryption,” *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 4, no. 3, pp. 684-694, 2016.
- [29] S. L. Yin, H. Li, J. Liu, “A new provable secure certificateless aggregate signcryption scheme,” *Journal of Information Hiding and Multimedia Signal Processing*, vol. 7, no. 6, pp. 1274-1281, 2016.

Biography

Hang Li obtained his Ph.D. degree in Information Science and Engineering from Northeastern University. Hang Li is a full professor of the Kexin software college at Shenyang Normal University. He is also a master's supervisor. He has research interests in wireless networks, mobile computing, cloud computing, social networks, network security and quantum cryptography. Prof. Li had published more than 30 international journal and international conference papers on the above research fields. Email:1451541@qq.com.

Lin Teng received the B.Eng. degree from Shenyang Normal University, Shenyang, Liaoning province, China in 2016. Now, she is a laboratory assistant in Software College, Shenyang Normal University. Her research interests include Multimedia Security, Network Security, Filter Algorithm and Data Mining. Email:yysl352720214@163.com.