Proxy Blind Signature Scheme Applying for Privacy Awareness e-Applications

Aung Nway Oo
University of Computer Studies, Yangon
aungnwayoo79@gmail.com

Abstract

Proxy blind signature, which combines the properties of both proxy signature and blind signature. In a proxy blind signature scheme, the proxy signer is allowed to generate a blind signature on behalf of the original signer. The proxy blind signature scheme is useful in several applications such as e-voting, e-payment and mobile agent environments. In this paper, we present proxy blind signature scheme based on discrete logarithm problem (DLP), which satisfy the security properties of both the blind signature scheme and the proxy signature scheme. Analysis shows that our scheme is secure and efficient.

Keywords—blind signature, proxy signature, proxy blind signature, DLP.

1. Introduction

With the growing importance of the mobile transaction, the proxy blind signature scheme has become a very active research area. In some applications, it is necessary to protect the privacy of participants. In 1982, David Chaum invented a blind signature [1], that scheme allows the sender to have a given message signed by the signers, without revealing any information about the message or its signature. In 1996, Mambo, Usudu and Okamoto [4] proposed a new concept, proxy signature. In a proxy signature scheme, the original signer delegates his signing capacity to a proxy signer who can sign a message submitted on behalf of the original singer. Mambo, Usudu and Okamoto [5] proposed complete proxy signature, partial proxy signature and signature with an entitlement certificate. Zhang [6], and Kim, Park, and Won [7] proposed threshold proxy signature.

The first proxy blind signature was proposed by Lin and Jan [2] in 2000. Later, Tan et al.[3] proposed a proxy blind signature scheme based on DLP and ECDLP. However, in 2003, Lal et al.[8] pointed out that Tan et al.'s scheme was insecure and proposed a new proxy blind signature scheme based on Mambo et al.'s scheme [6]. In 2004, Wang et al.[9] demonstrated that Tan's scheme was insecure and proposed two effective attacks. In 2005, Sun et al.[10] showed that Tan et al.'s schemes didn't satisfy the unforgeability and unlinkability properties and they also pointed out that Lal's scheme [8] didn't possess the unlinkability property either. In 2004, Xue and Cao [11] showed there exists one weakness in Tan et al.'s scheme [3] and Lal et al.'s scheme [8] since the proxy signer can get the link between the blind message and the signature or plaintext with great probability. Xue and Cao introduced concept of strong unlinkability and they also proposed a proxy blind signature scheme. Recently, Li et al.[12] proposed a proxy blind signature scheme using verifiable self-certified public key, and compared the efficiency with Tan et al.[3].

In this paper, we present proxy blind signature schemes on the basis of schnoor blind signature. Our proposed scheme satisfied all the security requirements of both the blind signature scheme and the proxy signature scheme. Compared with previous scheme[12], our scheme is more efficient and low-computation.

The rest of this paper is organized as follows. In Section 2, we list the security properties of the scheme. And then, our proposed proxy blind signature scheme based on DLP is presented in Section 3. In Section 4, we analyze the security properties and the efficiency of the proposed scheme and compared with previous schemes. Instance of application is describing in Section 5. In Section 6, we give the notations used throughout this paper. Finally Section 7 describes the concluding remarks.

2. Required Security Properties

Since proxy blind signatures are combination of the proxy signature and blind signature, they should have the security properties of the proxy signature and blind signature. In this section, we describe the require properties of the scheme as follows.

1) Distinguishability: The proxy signature must be distinguishable from the normal signature.

2) Nonrepudiation: Neither the original signer nor the proxy signer can sign a message instead of

other party. Both the proxy signer and original signer cannot deny their signatures against anyone.

3) Unforgeability: Only a designated proxy signer can create a valid proxy signature for the original signer (even the original signer cannot do it).

4) Identifiability: Anyone can determine the identity of the corresponding proxy signer from a proxy signature.

5) Verifiability: The receiver of the signature should be able to verify the proxy signature in a similar way to the verification of the original signature.

6) Prevention of misuse: It should be confident that proxy key pair should be used only for creating proxy signature, which conforms to delegation information. In case of any misuse of proxy key pair, the responsibility of proxy signer should be determined explicitly.

7) Unlinkability: When the signature is verified, the signer knows neither the message nor the signature associated with the signature scheme.

3. Proposed Proxy Blind Signature Scheme based on DLP

In the proposed scheme, the original signer delegates his signing capabilities to proxy signer. The proxy signer generates the signature to the requester without knowing the content of the message. The protocol consists of following phases:

- Proxy delegation phase
- BlindSigning phase
- Verification phase

Original signer delegates his signing capability to proxy signer in the delegation phase. To obtain a signature, the requester submits an encrypted version (blinds the message) of the message to the proxy signer in the signing phase, then the proxy signer computes the blind signature of the message, and then sends the result back to the requester. In the extraction phase, the requester extracts the signature from the result received form proxy signer. Lastly, anyone can verify the legitimacy of the digital signature in the verifying phase. The different phases of the signature scheme are explained below.

3.1 Proxy Delegation Phase

Original signer O selects random number $k_o \in_R Z^*_q$ and computes:

$$r_o = g^{k_o} \pmod p \quad (1)$$

$$s_o = x_o + k_o\ h(\ m_w // r_o)\ (mod\ q) \quad (2)$$

O sends (r_o, s_o) along with the warrant m_w to the proxy signer. And then proxy signer checks:

$$g^{s_o} = y_o\ r_o^{\ h(m_w//r_o)}\ (mod\ p) \quad (3)$$

If it is correct, proxy signer P accepts it and computes proxy signature secret key s_{pr} as follow:

$$s_{pr} = s_o + x_p \pmod q \quad (4)$$

Note: responding proxy public key $y_{pr} = y_o\ y_p\ r_o^{\ h(m_w//r_o)} = g^{\ s_{pr}} \pmod p$.

3.2 Blind Signing Phase

Proxy signer P selects random number $k \in_R Z^*_q$ and computes:

$$r = g^k\ (mod\ p) \quad (5)$$

and then sends (r_o, r) to signature asker A. To obtain the blind signature of message m, original signer A randomly choose two random numbers $u,v \in_R Z^*_q$ and computes:

$$r^* = r\ g^u\ (y_o\ y_p)^{-v} \pmod p \quad (6)$$

$$e^* = h(r^*//m) \pmod q \quad (7)$$

$$e = e^* - v \pmod q \quad (8)$$

If $r^* = 0$ then A has to select new tuple (u, v). Otherwise A sends e to P. After receiving e proxy signer P computes :

$$s^* = k + e\ s_{pr} \pmod q \quad (9)$$

and sends the sign message s^* to A.

After blind signing finish, *signature asker A extract the signature as follows* :

$$s = g^{\ s^*+u}\ r_o^{\ vh(m_w//r_o)} \quad (10)$$

Finally the signature of message m is (m, m_w, s, e^*, r_o) .

3.3 Verification Phase

The recipient of the signature can verify the proxy blind signature by checking whether

$$e^* = (\ h(\ s\ y_{pr}^{\ -e^*} \mod p\ //\ m)\ ) \pmod q \quad (11)$$

Where $y_{pr} = y_o y_p\ r_o^{\ h(m_w//r_o)}$

If it is true, the verifier accepts it as a validproxy blind signature, otherwise rejects. The comparison of computational cost with previous DLP based schemes is described in Table 1.

4. Proof of Security Properties of Scheme

In this section we discuss the correctness and some of the properties of our proposed DLP based proxy blind signature scheme, described in section 3.

Proxy Distinguishability: On the one hand, the proxy blind signature (m, m_w, s, e^*, r_o) *contains* the warrant m_w. On the other hand, anyone can verify the validity of the proxy blind signature, so he can easily distinguish the proxy blind signature from the normal signature.

Nonrepudiation: The original signer does not obtain the proxy signer's secret key x_p and proxy signer does not obtain original signer's secret key x_o . Thus, neither the original signer nor the proxy signer can sign in place of the other party. At the same time, through the valid proxy blind signature, the verifier can confirm that the signature of the message has been entitled by the original signer, because the verifier must use the original signer's public key during the verification. Likewise, the proxy signer cannot repudiate the signature. The scheme offers nonrepudiation property.

Unforgeability: An adversary (including the original signer and the receiver) wants to impersonate the proxy signer to sign the message m. He can intercept the delegation information (m_w, s_o ,r_o) but he cannot obtain the proxy signature secret key s_{pr} . From Equation (4), we know that only the proxy signer holds the proxy signature secret key x_p . Because of $x_p \in_R Z_q^*$, the adversary can obtain the proper proxy signature secret key by guessing it with at most a probability $1/q$ .That is, anyone else (even the original signer and the receiver) can forge the proxy blind signature successfully with a probability $1/q$.

Identifiability: The proxy blind signature (m, m_w, s, e^*, r_o) contains the warrant m_w. Moreover, in the verification equation $y_{pr} = y_o\, y_p\, r_o^{h(m_w // r_o)}$ which includes the original signer O' s public key y_o and the proxy signer P' s public key y_p . Hence, anyone can determine the identity of the corresponding proxy signer from a proxy signature.

Verifiability: The proposed scheme satisfies the property of verifiability. The verifier can verify the proxy blind signature by checking:

$$e^* \stackrel{?}{=} (h(s\, y_{pr}^{-e^*} \bmod p // m)) \pmod q$$

holds. This is because:

$$s\, y_{pr}^{-e^*} \bmod p$$

$$= g^{s^*+u\, r_o\, vh(m_w // r_o)}\, y_{pr}^{-e^*} \bmod p$$

$$= g^{k + es_{pr}+u\, r_o\, vh(m_w // r_o)}\, y_{pr}^{-e^*} \bmod p$$

$$= g^{k + e^*s_{pr} - vs_{pr}+u\, r_o\, vh(m_w // r_o)}\, y_{pr}^{-e^*} \bmod p$$

$$= g^{k + e^*s_{pr}+u}\, g^{-v\, s_o}\, g^{-v\, x_p}\, r_o^{vh(m_w // r_o)}\, y_{pr}^{-e^*} \bmod p$$

$$= g^{k + e^*s_{pr}+u\, y_o^{-v}\, r_o^{-vh(m_w // r_o)}\, g^{-v\, x_p}\, r_o^{vh(m_w // r_o)}\, y_{pr}^{-e^*}} \bmod p$$

$$= g^{k+u}\, g^{e^*s_{pr}}\, (y_o y_p)^{-v}\, y_{pr}^{-e^*} \bmod p$$

$$= g^{k+u}\, y_{pr}^{e^*}\, (y_o y_p)^{-v}\, y_{pr}^{-e^*} \bmod p$$

$$= r\, g^{u}\, (y_o y_p)^{-v} \bmod p$$

$$= r^*$$

Prevention of misuse: The proposed scheme can prevent proxy key pair misuse because the warrant m_w includes original signer and proxy signer identities information, message type to be signed by the proxy signer, delegation period, etc. With the proxy key, the proxy signer cannot sign messages that have not been authorized by the original signer.

Proxy unlinkability: During generation of the signature (m, m_w, s, e^*, r_o) , the proxy signer has the view of transcripts(r, m_w, s^*, e, r_o).Since (m_w, r_o) are specified by the original signer for all the signatures under the same delegation condition. The proxy unlinkability holds if and only if there is no conjunction between (r, s^*, e) and (m, m_w, s, e^*, r_o) . This is obvious from Equations (5)-(10). The value r is only included in Equation (6) and connected to e^* through Equation (7). For this, one must be able to compute r which is masked with two random numbers. Similarly, e and s^* may be associated with the signature through Equation (8) and (9) respectively. They fail again due to the random numbers. Even they are combined, the number of unknowns is still more than that of the equations. So, the proposed scheme provides indeed the proxy blindness property.

Efficiency: In Table 1, we can see that our scheme is more efficient and low computational cost than previous scheme . The detailed costs in each phase are compared with previous schemes. In this table, T_E and T_M denote the once running of modulo exponential and multiplication operations, respectively. T_H denotes the once running of hash operations. The modulo-additions are omitted due to its high performance. Also note that all the minus exponential operations can be transformed to positive exponential operations without losing almost any efficiency (modulo q).

Table 1: Comparison of computational cost with previous DLP based scheme

Schemes	Delegation	Blind signing	Verification	Total costs
Scheme [12]	$3T_E+2T_M+2T_H$	$5T_E+6T_M+2T_H$	$3T_E+3T_M+2T_H$	$11T_E+11T_M+6T_H$
Our Scheme	$3T_E+2T_M+2T_H$	$3T_E+4T_M+1T_H$	$2T_E+3T_M+2T_H$	$8T_E+9T_M+5T_H$

5. Instance of Application

As an instance, the applying of the schemes in electronic voting is describing. In the electronic vote, the vote managing center commission a vote branch to proxy voting. A voter can log on a vote branch and vote. It is request that the vote branch know nothing about the voting message during voting. So, the proxy blind signature scheme can be used in it. The proxy delegation process is to intrusting a vote branch. The proxy blind signature generation process is a voting process.

As another instance, in the production of e-coins, the user makes the bank blindly sign a coin using blind signature schemes. The user is in possession of a valid coin such that the bank itself cannot recognize nor link with the user. Whenever a user goes through a valid branch to withdraw a coin, he needs the branch to make proxy blind signature on behalf of the signee bank. This application leads to the need of proxy blind signature schemes.

6. System Parameters and Notations

Throughout this paper, we used the following notations and parameters to explain and analyze the scheme.

O	the original signer
P	the proxy signer
A	the signature asker
p, q	two large prime numbers with q|(p − 1)
x_u	secret key of user u
y_u	public key of user u, $y_u = g^{x_u} \bmod p$
m_w	the designated proxy warrant which contains the identities information of the original signer and the proxy signer, message type to be signed by the proxy signer, the delegation limits of authority, valid periods of delegation, etc.
g	generator of order q in Z^*_p
$h(.)$	a secure one-way hash function
//	the concatenation of strings
$O \rightarrow P$	O sends message to P

7. Conclusion

In this paper, we proposed proxy blind digital signature scheme based on DLP. The proposed scheme satisfies the given security requirements and our proposed scheme has less computational cost when comparing with previous schemes. The future work is to design more effective proxy blind signature schemes and proxy blind signature schemes which provably secure in the standard model.

References

[1] D. Chaum, "Blind Signature Systems", *Proceedings of Crypto'83*, Plenum, pp.153.

[2] W. D. Lin, and J. K. Jan, "A security personal learning tools using a proxy blind signature scheme", *Proc. of Int'l Conference on Chinese Language Computing*, 2000, pp.273-277.

[3] Z. W. Tan, Z. J. Liu, and C. M. Tang, "A proxy blind signature scheme based on DLP", *Journal of Software*, Vol14, No11, 2003, pp.1931-1935.

[4] M. Mambo& K. Usuda and E. Okamoto, "Proxy Signatures for delegating signing operation", *Proc. 3rd ACM Conference on Computer and communications Security* , ACM Press, 1996. pp.48-57.

[5] M. Mambo, K. Usuda and E. Okamoto, "Proxy signatures: Delegation of the power to sign messages", *IEICE Trans. Fundamentals*, 1996, Vol. E79-A, (9), pp.1338-1354.

[6] K. Zhang, "Threshold Proxy signature schemes", *1997 Information Security Workshop* , Janpan, 1997, pp.191-197.

[7] S. Kim, S. Park and D. Won, "Proxy signature. *Information and Communication Security"*, LNCS, Vol. 1334, Springer-Verlag, 1997, pp.223-232.

[8] S. Lal, and A. K. Awasthi, "Proxy blind signature scheme", http://eprint.iacr.org/2003/072.pdf.

[9] S. H. Wang, G. L. Wang, F. Bao, and J. Wang, "Cryptanalysis of a proxy blind signature scheme based on DLP", *Journal of Software*, Vol. 16, No. 5, 2005,pp. 911–915.

[10] H. M. Sun, B. T. Hsieh, and S. M. Tseng, "On the security of some proxy signature schemes", *Journal of System and Software*, Vol. 74, 2005, pp.297-302.

[11] Q. S. Xue, and Z. F. Cao, "A new proxy blind signature scheme with warrant", *IEEE Conference on Cybernetics and Intelligent Systems (CIS and RAM 2004)*, Singapore, 2004, pp.1385-1390.

[12] J.G. Li, and S. H. Wang, "New Efficient Proxy Blind Signature Scheme Using Verifiable Self-certified Public Key", *International Journal of Network Security*, Vol.4, No.2, 2007, pp.193–200.