Buletin Teknik Elektro dan Informatika
(Bulletin of Electrical Engineering and Informatics)
Vol.1, No.3, September 2012, pp. 185~190
ISSN: 2089-3191

New Proxy Blind Multi Signature based on Integer-Factorization and Discrete-Logarithm Problems

Swati Verma, Birendra Kumar Sharma
School of Studies in Mathematics, Pt. Ravishankar Shukla University, Raipur (C.G.), India.
e-mail: swativerma15@gmail.com, sharmabk07@gmail.com

Abstract

Digital proxy multi-signature and blind signature scheme are found very useful for the purpose of electronic voting and electronic cash transaction. In proxy multi-signature, many original signers can delegate their signing power to a proxy signer in such a way that the proxy signer can sign any message on behalf of original signers. In blind signature, the signer cannot make a linkage between the blind signature and the identity of the requester. Proxy blind multi-signature is the combination of proxy multi-signature and blind signature. In this paper, we propose a new proxy blind multi-signature scheme based on integer factorization problem (IFP) and discrete logarithm problem (DLP) to improve the security aspect. It satisfies the security properties of both the blind signature and the proxy multi-signature scheme.

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

1. Introduction

The notion of proxy signature was first introduced by Mambo et al. [8, 9] in 1996. In a proxy signature scheme, an original signer can delegate his signing capacity to a proxy signer who can sign any message on behalf of the original singer.

The notion of blind signature was firstly introduced by David Chaum [1] in 1983. Blind Signature is a signature on a message signed by another party without having any information about the message. Blind signatures are applicable where sender's privacy is important such as digital cash transaction, electronic voting systems etc. A proxy blind signature scheme combines the properties of proxy signature and blind signature schemes. In a proxy blind signature scheme, the proxy signer is allowed to generate a blind signature on behalf of the original signer.

The frist proxy blind signature scheme was introduced by Lin and Jan [5] in 2000. Later, two new schemes have been proposed: Tan et al.'s scheme [12] which is based on Schnorr blind signature scheme and Lal et al.'s scheme [4] which is based on Mambo et al.'s proxy signature scheme. These schemes need a secure channel to transmit a proxy secret key. To solve this problem, inspired by Yi et al.'s [13] proxy multi-signature and Okamoto-Schnorr blind signature [10], Lu, Cao and Zhou [7] proposed a new proxy blind multi-signature scheme which does not require a secure channel. They also proved the unforgeability of the scheme and concluded that only the designated proxy signer can generate a valid proxy blind multisignature, any other one, even the original signer, cannot do it. In 2010, Kang et al.'s [3] showthat Lu et al.'s [7] scheme does not satisfy the unforgeability property. Recently, Liu et al.'s [6] proposed Proxy blind multi-signature scheme based on ElGamal signature [2], their security is based on DLP.

The existing proxy blind multi signature schemes are based on only one hard mathematical problem, i.e., discrete logarithm problem (DLP). A digital signature scheme based on more than one hard mathematical problem is much more secure other than based on one hard mathematical problem because one mathematical problem is easy to solve as compare to two. With such notion we propose new proxy blind multi signature scheme based on two hard mathematical problems, i.e. integer factoring problem (IFP) and discrete logarithm problem (DLP). Its security also we discuss in this paper.

Received July 11, 2012; Revised August 25, 2012; Accepted September 17, 2012

Our Proxy blind multi signature satisfies the following security properties:

- Verifiability- The verifier is able to verify the proxy signature in the similar way to the verification of the original signature.
- Unlinkability- The proxy signer will be able to know neither the message nor the original signature associated with the proposed signature schemes after proxy blind signature is created.
- Unforgeability- Only the designated proxy signer can create a valid proxy signature, for the original signer (even the original signer can not do it).
- Non-repudiation- Neither the original signer nor the proxy signer can sign in place of the other party. In other words, they cannot deny their signatures against anyone.
- Prevention of misuse- It is well assumed that proxy key pair is used to create proxy signature, only to order confirm the delegation of information.This way the responsibility of proxy signer will be determined explicitly in case of any misuse of proxy key pair.

Remaining paper is organized as follows. In Section 2, new proxy blind multi signature scheme is proposed and we analyze the security properties of this scheme in section 3. Finally Section 4, describes the concluding remarks.

2. Proposed Proxy Blind Multi Signature Scheme

We divide our proxy blind multi-signature scheme into five phases: Initialization parameters, Generation of proxy sub secret key, Veriifcation of proxy sub secret key, Generation of proxy secret key, Signing phase and Validation phase.

2.1 Initialization Phase

For the convenience of describing our work, we define the parameters as follows:

* A: the original signer
* B: the proxy signer
* p, q : two large random prime numbers and product of two prime number is equal to n, i.e., n = pq.
* $\phi(n)$: it is equal to (p-1)(q-1).
* g: is an element of Zp^* , its order is q
* x_i : secret key of each original signer Ai(1 < i < n).
* y_i: corresponding public key of original signers defined by yi = g^{xB} mod p
* x_B: the secret key of proxy signer.
* y_B: the public key of proxy signer defined by $y_B = g^{xB}$ mod p
* H(), H1(), H2() : three universal secure hash function.
* m_w: authorized information.

2.2 Generation of proxy sub secret key

Every original signer Ai(1 < i < n) produces sub proxy secret si and makes signcryption on it, then sends it to proxy signer B in any manner.

1. Select $k_i \in Z_q^*$ at random and compute (r_i; s_i).

$$r_i = g^{k_i} \bmod p \quad (1)$$

$$s_i = x_i + H(m_w, r_i).k_i \bmod n \quad (2)$$

where m_w is the designated proxy warrant negotiated by all original signers, which records the delegation policy including limit of authority, valid period of delegation, proxy signature, all identities and the public keys of the original signers.

2. Again select $k'_i \in Z_q^*$ at at random and compute (r'_i, c_i, r''_i, s'_i).

$$r'_i = g^{k'_i} \bmod p \quad (3)$$

$$c_i = s_i.r'_i.y_B^{k_i} \bmod p \quad (4)$$

$$r''_i = H_1(c_i, r_i, r'_i), \quad (5)$$

$$s'_i = k'_i.(r''_i + x_i)^{-1} \bmod n. \quad (6)$$

3. Publish (r_i, m_w) and send (ci, r''$_i$, s'$_i$) to proxy signer B in any manner. Anyone can obtain (c_i, r''$_i$, s'$_i$) by wiretap, but this does not affect our scheme.

2.3 Verification of proxy sub secret key

Proxy signer B when received (ci, r''$_i$, s'$_i$) he validates it and recovers s_i by following steps.

1. First compute r'$_i$,

$$r''_i = (y_i.g^{r''_i})^{s'_i} = g^{(x_i + r''_i).s_i} = g^{(x_i + r''_i)(k'_i)(r''_i + x_i)^{-1}} = g^{k'_i} \bmod p \quad (7)$$

2. Then check the equation r''$_i$=H_1 (c_i,r_i,r'$_i$).
   If it holds, B can be convinced (c_i, r_i, s'$_i$) is indeed produced by the original signer A_i. Otherwise, it will be rejected.

3. Once (c_i, r_i, s'$_i$) is validated, B can use his private key x_B to recover s_i,

$$s_i = c_i r'^{-1}_i . r_i^{x_B} = s_i . r'_i . y_B^{k_i} . r'^{-1}_i . r_i^{-x_B} = s_i \bmod p \quad (8)$$

4. Finally, validate si by the following equation.

$$g^{s_i} = r_i . y_i^{H(m_w, r_i)} \bmod p. \quad (9)$$

2.4 Generation of proxy secret key

Proxy signer B when received n valid s_i (1≤i≤n), he can generate the proxy secret key β

$$\beta = \sum_{i=1}^{n} s_i + x_B \bmod n. \quad (10)$$

2.5 Signing phase

When proxy secret key β is generated, proxy signer B will be able to create blind signature on behalf of all original signer Ai (1≤ i ≤n). Let requester C requests proxy signer B to make a blind signature on message m. Then the process is as follows:

1. Proxy signer B randomly selects $w_1 = Z_q^*$ and computes $x = g^{w_1} \bmod p$ then sends x to requester C.
2. Requester C first computes α according with proxy signer and all original signer's public key and all r_i(1≤i ≤n) published by original signers.

$$g^{\beta} = y_B . \prod_{i=1}^{n} (y_i . r_i^{H(m_w, r_i)}) \bmod p. \quad (11)$$

then selects randomly $w_2, w_3 \in Z_q^*$ and computes x*, e* and e.

$$x^* = g^{w_2} . \alpha^{w_3} . x \bmod p, \quad (12)$$

$$e^* = H_2(x^*, m), \quad (13)$$

$$e = e^* + w_3 \bmod n \quad (14)$$

.

then, sends e sends to proxy signer B.

3. After receiving e, B computes y and sends it to requester C.

$$y = w_1 + e.\beta \bmod n \tag{15}$$

4. when C received e, he computes y*,

$$y^* = y + w_2 \bmod n. \tag{16}$$

and creates the proxy blind multi signature (e*, y*) of message m.

2.6 Validation phase

Any one can verify the validity of the proxy blind signature by checking that
-- Compute α in the same way of requester C.
-- Computes

$$\begin{aligned} x^* &= g^{y^*}.\alpha^{-e^*} \\ &= g^{y+w_2}.\alpha^{-e^*} \\ &= g^{w_1+w_2+e.\beta}.\alpha^{-e^*} \\ &= g^{w_1+w_2+w_3.\beta+e^*.sk}\alpha^{-e^*} \\ &= g^{w_1+w_2}.\alpha^{w_3}.\alpha^{-e^*} \\ &= g^{w_2}.\alpha^{w_3}.x \bmod p. \end{aligned} \tag{17}$$

-- Compute $e^*=H_2$ (x*, m) and check e'*=e* If it is hold, anyone can be convinced (e*, y*) is a valid proxy blind multi-signature on message m. Otherwise, it will be rejected.

3. Security Analyses

We analyze the security of our scheme as follows. In the Lu et al.'s [7] scheme, the proxy public key is

$$\alpha = y_B \prod_{i=1}^{n} y_i^{H(m_w, r_i)}.r_i \bmod p,$$

where r_i appears in a single r_i manner. A malicious original signer A1 can forge a proxy secret key by setting his random value r_1.

$$r_1 = g^t.y_B^{-1}(\prod_{i=2}^{n}(r_i.y_i^{H(m_w, r_i)}))^{-1} \bmod p.$$

However, in our proxy secret key generation phase,

$$g^{\beta} = y_B.\prod_{i=1}^{n}(y_i.r_i^{H(m_w, r_i)}) \bmod p.$$

where

$$\beta = \sum_{i=1}^{n} s_i + x_B \bmod n,$$

r_i appears in the proxy public key in $r_i^{H(m_w, r_i)}$ manner, which makes it hard for A_1 to set a particular r_1 to eliminate the proxy signer's public key y_B.

Therefore the new proxy secret key generation phase overcomes the weakness of the Lu et al.'s [7] scheme.

- Verifiability :
  Any one can verify the proxy blind multi signature when check whether the verification equation (11) and (17) holds or not.
- Unlinkability :
  To prove the scheme is unlinkability, we observe the scheme, the requester C randomly select two values $w_2, w_3 \in Z_q^*$ and blinds (e*,y*) in the following equation

$$e = e^* + w_3 \bmod n,$$

$$y^* = y + w_2 \bmod n.$$

  without knowing w_2 ,w_3 the proxy signer B cannot find (e*, y*) from (e, y). Therefore, the signer cannot make a linkage between the signature and the requester of signature. So the unlinkability property is satisfied.
- Non-repudiation:
  In the proposed proxy blind multi-signature scheme, the proxy secret key β is secure, if only the proxy signer B holds it. From equation (10) we can conclude that the proxy secret key β is secure.
- Prevention of misuse:
  The tuple (c_i, r''_i, s'_i, r'_i) is secure, only the proxy signer B with his private key x_B can recover s_i.

4. Conclusion

In this paper, we proposed a new proxy blind multi signature scheme based on integer factorization problem (IFP) and discrete logarithm problem (DLP). The proposed scheme satisfies the security requirements of both the blind signature and the proxy multi signature scheme.

References

[1] Chaum D., Blind signatures for untraceable payments", *Advances in Cryptology Crypto82*, (1983), 199-203.
[2] ElGamal T, A public-key cryptosystem and a signature scheme based on discrete logarithms", *IEEE Transactions on Information Theory IT-31*, (1985), 469-472.
[3] Kang B., Han J. and Wang, Q., "*On the security of proxy blind multi-signature scheme without a secure channel"*, Computer Engineering and Technology (IC-CET), 2010 2nd International Conference on Volume: 1, (2010), Page(s): V1-62-64.
[4] Lal S. and Awasthi A. K., "Proxy Blind Signature Scheme", *Journal of Information Science and Engineering. 2003*, Cryptology ePrint Archive, Report2003/072. Available at: http://eprint.iacr.org/.
[5] Lin W. D. and Jan J.K., "*A security personal learning tools using a proxy blind signature scheme*", Proc. of Intl Conference on Chinese Language Computing, (2000), 273-277.
[6] Liu W. and Zhang J., "Proxy blind multi-signature scheme based on ElGamal signature", Computer Engineering and Application, (2012), 48(10), 95-97.
[7] Lu R., Cao Z. and Zhou, Y., "Proxy blind multi-signature scheme without a secure channel", *Applied mathematics and computation,* (2005), 164, 179-187.

[8] Mambo M., Usuda K. and Okamoto E., "*Proxy signatures for delegating sign operation*", In: Proceeding of the 3rd ACM conference on compute and communications security (CCS96), ACM press, (1996), 48-57.
[9] Mambo M., Usuda K. and Okamoto E., "Proxy signatures: delegation of the power to sign messages", IEICE *Trans Fundam*, (1996), E79-A(9):1338-1354.
[10] Okamoto T., "Provable secure and practical identi_cation schemes and corresponding signature schemes" *Advances in Crypto-Crypto'92, Lecture Notes in Computer Science*, (1992), 740, 31-53.
[11] Pointcheval D. and Stern J., Security argument for digital signatures and blind signatures, Journal *of Cryptology*, (2000), 13(3), 361-396.
[12] Tan Z., Liu Z. and Tang C., "Digital proxy blind signature schemes based on DLP and ECDLP", *MM Research Preprints, No. 21, MMRC, AMSS, Academia, Sinica*, (2002), 212-217.
[13] Yi L., Bai G. and Xiao G., "Proxy multi-signature scheme" *Electronic Letters*, (2000), 6(36), 527-528.