Cryptanalysis of Lu *et al.*'s Proxy Blind Multi Signature Scheme

Swati Verma and Birendra Kumar Sharma

***Abstract*—As a variation of ordinary digital signature scheme, a proxy signature scheme able a proxy signer to sign messages on behalf of the original signer. Proxy multi-signature is an extension of the basic proxy signature primitive and permits two or more entities to delegate their signing capabilities to the same other entity. 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. Recently, Lu *et al.* presented a proxy blind multi-signature scheme which did not need a secure channel. However, in this paper, we show that Lu *et al.'s* scheme does not satisfy the unforgeability and also shown that their scheme is not secure against the original signer's forgery attack and the proxy signer's forgery attacks.**

***Index Terms*—Blind signature, proxy-multi signature, proxy blind multi signature, security.**

I. Introduction

The notion of proxy signature was first introduced by Mambo *et al*. [1], [2] 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. Blind signature was firstly introduced by David Chaum [3] 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 first proxy blind signature scheme was introduced by Lin and Jan [4] in 2000. Later, two new schemes have been proposed: Tan *et al*.'s scheme [5] which is based on Schnorr blind signature scheme and Lal *et al*.'s scheme [6] 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 [7] proxy multi-signature and Okamoto-Schnorr blind signature [8], Lu, Cao and Zhou [9] proposed a new proxy blind multi-signature scheme which does not require a secure channel.

Manuscript received December 15, 2012; revised March 10, 2013.
The authors are with the School of Studies in Mathematics Pt. Ravishankar Shukla University, Raipur (C.G.), India (e-mail: swativerma15@gmail.com, sharmabk07@gmail.com).

They also proved the unforgeability of the scheme and concluded that only the designated proxy signer can generate a valid proxy blind multi-signature, any other one, even the original signer, cannot do it.

However, in this paper, we show that Lu *et al.*'s [9] scheme does not satisfy the unforgeability. We show that their scheme is not secure against the original signer's forgery attack and the proxy signer's forgery attacks. Using the forgery attack, a dishonest original signer can forge a proxy signing key on behalf of all the original signers without their agreements and produce valid proxy blind multi-signatures, which does harm to the benefits of the proxy signer and other original signers.

Organization: Remaining paper is organized as follows. In Section II, we review Lu *et al.*'s. proxy blind multi signature scheme. In Section III, we show that Lu *et al.*'s scheme is insecure against the original signer's forgery and the proxy signer's forgery. Finally Section IV describes the concluding remarks.

II. Brief Review of Lu *et al.*'s Signature Scheme

In this section, Lu *et al.*'s proxy blind multi-signature scheme is divided into six phases.

A. Initialization Phase

Randomly select two large prime integers p and q such that q/p-1, as well as a generator g of Z^*_p with order q. Let A_1, $A_2 \ldots A$ be the original signers and B be the designated proxy signer. Every original signer A_i ($1\leq i\leq n$) has a private key x_i and the corresponding public key y_i, where $x_i \in_R Z^*_q$ and $y_i = g^{x_i} \bmod p$. Proxy signer B also holds his own key pair (x_B; y_B), where $x_B \in_R Z^*_q$ is the private one and $y_B = g^{x_B} \bmod p$ the public one. Furthermore, three universal secure hash functions H (), H_1 (), and H_2 () are also published.

B. Generation of Proxy Sub Secret Key

Every original signer A_i ($1\leq i \leq n$) produces sub proxy secret s_i 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).

$$r_i = g^{k_i} \pmod g$$

$$s_i = x_i H(m_w, r_i) + k_i \pmod q$$

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.

DOI: 10.7763/IJCTE.2013.V5.804

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

$$r'_i = g^{k'_i} \bmod p,$$
$$c_i = s_i.r'_i.y_B^{k_i} \bmod p,$$
$$r''_i = H_1(c_i, r_i, r'_i),$$
$$s'_i = k'_i.(r''_i + x_i)^{-1} \bmod n$$

3) Publish (r_i, m_w) and send (c_i, r''_i, s'_i) to proxy signer B in any manner.

C. Verification of Proxy Sub Secret Key

After Proxy signer B received (c_i, r'', s'_i), he validates it and recovers s_i. Anyone can obtain (c_i, r'', s'_i), by wiretap, but this does not affect our scheme.

1) First compute r_i

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

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'', s'_i), is indeed produced by the original signer Ai. Otherwise, it will be rejected.
3) Once (c_i, r'', s'_i) is validatd, B can use his private key x_B to recover s_i,

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

4) Finally, validate s_i by the following equation.

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

If it holds, s_i will be accepted, otherwise, it will be rejected.

D. Generation of Proxy Secret Key

After proxy signer B received n valid s_i ($1 \le i \le n$), he can generate the proxy secret key s_k

$$sk = \sum_{i=1}^{n} s_i + x_B \bmod q$$

E. Signing Phase

Assume requester C asks proxy signer B to make a blind signature on message m. They will run the following interactive course.

1) Proxy signer B randomly selects $w_1 \in_R Z_q^*$ 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 ($1 \le i \le n$) published by original signers.

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

Then selects randomly $w_2, w_3 \in_R Z^*_q$ and computes x^*, e^* and e.

$$x^* = g^{w_2}.\alpha^{w_3}.x \bmod p,$$
$$e^* = H_2(x^*, m),$$
$$e = e^* + w_3 \bmod q$$

at last, sends e sends to proxy signer B.

3) After proxy signer B received e, he computes y and sends it to requester C.

$$y = w_1 + e.sk \bmod q$$

4) When requester C received y, he can compute y^* and form the proxy blind signature (e^*, y^*) of message m, where

$$y^* = y + w_2 \bmod q$$

F. Validation Phase

1) Compute α in the same way of requester C.
2) Computes

$$x^* = g^{y^*}.\alpha^{-e^*}$$

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

III. Cryptanalysis of Lu *et al.*'s Proxy Blind Multi Signature Scheme

In this section, we demonstrate two kinds of forgery attacks on Lu *et al.*'s [9] scheme.

A. The Original Signer's Forgery

We show that Lu *et al.*'s proxy blind multi-signature scheme is insecure against the original signers' forgery. In order to forge a proxy blind multi-signature, the n dishonest original signers can compute

$$\overline{r_1} = g^{\alpha_1} \bmod p,$$
$$\overline{r_2} = g^{\alpha_2} \bmod p,$$
$$---------$$
$$\overline{r_{n-1}} = g^{\alpha_{1n-1}} \bmod p,$$
$$\overline{r_n} = y_B^{-1} g^{\alpha_{1n}} \bmod p$$

$$\overline{s_i} = x_i H(m_w, \overline{r_i}) + \alpha_i \bmod q, i = 1, 2, ..., n.$$

where $\alpha_1, \alpha_2, ..., \alpha_n$ are random numbers. Thus

$$\overline{sk} = \sum_{i=1}^{n} \overline{s_i} \bmod q$$

is a valid proxy signature signing key.

This is proved by below equation

$$g^{\overline{sk}} = g^{\sum_{i=1}^{n}\overline{s_i}}$$
$$= g^{\sum_{i=1}^{n-1}\overline{s_i} + \overline{s_n}}$$
$$= \sum_{i=1}^{n-1}(\overline{r_i} y_i^{H(m_w, \overline{r_i})}.\overline{r_n} y_B.y_n^{H(m_w, \overline{r_n})})$$
$$= y_B \sum_{i=1}^{n}(\overline{r_i} y_i^{H(m_w, \overline{r_i})})$$
$$= a$$

So,

$$\begin{aligned}\overline{x*} &= g^{\overline{y*}}.\alpha^{-\overline{e*}}\\ &= g^{w_1+w_2}.g^{(w_3+\overline{e*})\overline{sk}}.\alpha^{-e*}\\ &= g^{w_1+w_2}\alpha^{w_3}.\alpha^{\overline{e*}}.\alpha^{-e*}\\ &= g^{w_2}.\alpha^{w_3}.x\end{aligned}$$

Anyone can be convinced that $(\overline{e*}, \overline{y*})$ is a valid proxy blind multi-signature, thus the original signers succeed to forge a proxy signature.

IV. The Proxy Signer's Forgery

Here, we show that the proxy signer can perform the universal forgery for any selected message. Assume that the proxy signer wants to generate a signature for message m, he can select $w_1 \in Z_q*$ at random and compute $\overline{e*} = H_2(g^w, m)$, $\overline{y*} = w + sk\overline{e*}$. Then $(\overline{e*}, \overline{y*})$ is a valid proxy blind multi-signature for message m.
This is because

$$\begin{aligned}\overline{x*} &= g^{y*}.\alpha^{-e*}\\ &= g^{w+sk\overline{e*}}.\alpha^{-\overline{e*}}\\ &= g^{w}.\overline{e*}.-\overline{e*}\\ &= g^{w}\end{aligned}$$

So, $H_2(x*; m) = H_2(g^w, m) = e*$ the proxy signer can forge a valid proxy blind multi-signature for any message m selected by himself without following the steps in Lu *et al.*'s scheme.

V. Conclusion

In this paper, we have reviewed Lu *et al*.'s proxy blind multi-signature scheme which did not need a secure channel. We show that Lu *et al*.'s scheme does not satisfy the unforgeability and also shown that their scheme is insecure against the original signers' forgery attacks and the proxy signers' forgery attacks.

Acknowledgment

The author wishes to thank the anonymous referees for their very useful comments and suggestions.

References

[1] M. Mambo, K. Usuda, and E. Okamoto, "Proxy signatures for delegating sign operation," in *Proceeding of the 3rd ACM conference on compute and communications security (CCS96),* ACM press, pp. 48-57, 1996.

[2] M. Mambo, K. Usuda, and E. Okamoto, "Proxy signatures: delegation of the power to sign messages," *IEICE Trans Fundam*, E79-A, vol. 9, pp.1338-1354, 1996.

[3] D. Chaum, "Blind signatures for untraceable payments," *Advances in Cryptology Crypto82*, pp. 199-203, 1983.

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

[5] Z. Tan, Z. Liu, and C. Tang, "Digital proxy blind signature schemes based on DLP and ECDLP," *MM Research Preprints, No. 21, MMRC, AMSS, Academia, Sinica, Beijing.* pp. 212-217, 2002.

[6] S. Lal and A. K. Awasthi. (2003). Proxy Blind Signature Scheme to Appear in Journal of Information Science and Engineering. Cryptology ePrint Archive, Report2003/072. [Online]. Available: http://eprint.iacr.org/.

[7] L. Yi, G. Bai, and G. Xiao, "Proxy multi-signature scheme," *Electronic Letters*, vol. 6, no. 36, pp. 527-528, 2000.

[8] T. Okamoto, "Provable secure and practical identification schemes and corresponding signature schemes," *Advances in Crypto'92, Lecture Notes in Computer Science*, Springer-Verlag, vol. 740, pp. 31-53, 1992.

[9] R. Lu, Z. Cao and Y. Zhou, "Proxy blind multi-signature scheme without a secure channel," *Applied Mathematics and Computation*, no. 164, pp. 179-187, 2005.

Swati Verma received the B.Sc. and M.Sc. degree in Mathematics from Pt. Ravishankar Shukla University, Raipur. Chhattisgarh, India in 2005 and 2007. She joined School of Studies in Mathematics, Pt. Ravishankar Shukla University, Raipur, India for her research work. She is a life member of Cryptology Research Society of India (CRSI). Her area of interest is Public Key Cryptography and Digital Signature.

Birendra Kumar Sharma is a professor, School of Studies in Mathematics, Pt. Ravishankar Shukla University Raipur (C. G.) India. He has been working for long time in the field of Non Linear Operator Theory and currently in Cryptography. He and his research scholars work on many branches of public key cryptography. He is a life member of Indian Mathematical Society and the Ramanujan Mathematical Society.