ICIC International ©2009 ISSN 1881-803X
pp. **1–EL08-062**

A NON-REPUDIABLE MULTI-PROXY MULTI-SIGNATURE SCHEME

Min-Shiang Hwang[1], Shiang-Feng Tzeng[2] and Shu-Fen Chiou[3]

[1]Department of Management Information Systems
[3]Department of Computer Science and Engineering
National Chung Hsing University
250 Kuo Kuang Road, 402 Taichung, Taiwan
mshwang@nchu.edu.tw

[2]Department of Computer Science and Information Engineering
National Central University
no.300, Jung-da Rd., Jung-li City, 320 Taoyuan, Taiwan

Received October 2008; accepted January 2009

Abstract. *In this paper, we shall propose a multi-proxy multi-signature scheme which allows any u or more proxy signers from a designated group of v proxy signers to sign messages on behalf of any t or more original signers from a group of n original signers in total. The multi-proxy multi-signature scheme with the non-repudiation property is a new scheme that the proxy group cannot deny the signed messages and any verifier can identify the responsible proxy group for a proxy signature.*

Keywords: Cryptosystem, Digital signature, Proxy signature, Threshold proxy signature

1. **Introduction.** Proxy signature as embodied in Mambo et al. [12, 13] allows the original signer to delegate her/his signing capability to a proxy signer on behalf of the original signer. So far, proxy signature schemes have been widely discussed [1, 2, 3, 4, 6, 7, 10, 11, 8, 9, 14, 15, 17, 18]. Several articles about proxy multi-signature schemes [17] and threshold proxy signature schemes [5, 8, 9, 16, 18] have also been released. However, there still exists a dispute in the proxy signature schemes when the signer can repudiate the signatures that she/he signed. Several threshold proxy signature schemes adding non-repudiated property with known signers have been proposed consequently [6, 7, 14, 16].

These proxy signature schemes did not satisfy the following case. Suppose there are many employers in a company. When the company is facing economic difficulties, the manager might try to reduce the cost by laying off some of the employers. It causes conflicts between the employers and the manager. In this case, the company employers may authorize some lawyers to negotiate with the manager. For another example, the residents in the building may authorized some lawyers to sue the builder. Then, how can the two or more lawyers digitally sign the message on behalf of the group of employers or residents?

In this paper, a new non-repudiated multi-proxy multi-signature scheme, which can be applied to the above situations, will be examined. The new non-repudiated multi-proxy multi-signature scheme allows the group of the original signers to delegate the signing capability to the designated group of proxy signers. We shall introduce the new scheme in Section 2. In Section 3, we will analyze the security of the new scheme. Finally, the conclusion is given in Section 4.

2. **The Proposed Scheme.** The scheme can be divided into three phases: proxy share generation, proxy signature generation and proxy signature verification. Initially, the system parameters are defined as:

- *p:* a large prime.
- *q:* a large prime factor of $p-1$.
- *g:* a generator in $GF(p)$ of order q.
- *$h(\cdot)$:* a one-way hash function.
- *m_w:* a warrant which records the identities of the original signers of the original group and the proxy signers of the proxy group, the parameters (t,n) and (u,v), and the valid delegation time, etc.
- *$AOSID$:* (Actual Original Signers' ID) the identities of the actual original signers.
- *$APSID$:* (Actual Proxy Signers' ID) the identities of the actual proxy signers.

Each original signer has a randomly selected private key $x_{O_i} \in Z_q^*$ and a public key $y_{O_i} = g^{x_{O_i}} \bmod p$ certified by CA. Each proxy signer P_i owns a secret key $x_{P_i} \in Z_q^*$ and a public key $y_{P_i} = g^{x_{P_i}} \bmod p$ which is also certified by CA. Let $G_O = \{O_1, O_2, \cdots, O_n\}$ be the group of n original signers and $G_P = \{P_1, P_2, \cdots, P_v\}$ be the proxy group of v proxy signers.

2.1. **Proxy share generation phase.** Assume that any t or more original signers delegate their signing capability to the designated proxy group. Let $D_O = \{O_1, O_2, \cdots, O_t\}$ be the actual original signers. D_O as a group executes the following steps to delegate the signing capability to G_P.

1. Choose a random number $a_i \in Z_q^*$ and broadcast k_i,

$$k_i = g^{a_i} \bmod p.$$

2. For each received k_j, $j = 1, 2, \cdots, t$, and $j \neq i$, each $O_i \in D_O$ calculates

$$\begin{aligned} K &= \prod_{j=1}^{t} k_j \bmod p, \\ \sigma_i &= a_i K + x_{O_i} h(K \parallel m_w \parallel AOSID) \bmod q. \end{aligned}$$

3. Send σ_i to the designated clerk via a public channel.
4. After receiving σ_i, the designated clerk checks whether the following equation holds

$$g^{\sigma_i} \overset{?}{=} k_i^K y_{O_i}^{h(K \| m_w \| AOSID)} \bmod p.$$

If it does, the designated clerk calculates

$$\sigma = u^{-1} \sum_{i=1}^{t} \sigma_i \bmod q.$$

5. Broadcast $(\sigma, m_w, K, AOSID)$ to G_P.

After receiving $(\sigma, m_w, K, AOSID)$, each $P_i \in G_P$ checks whether or not the following equation holds

$$g^{\sigma} \overset{?}{=} (K^K \prod_{i=1}^{t} y_{O_i}^{h(K \| m_w \| AOSID)})^{u^{-1}} \bmod p. \tag{1}$$

If it does, each P_i uses σ as her/his proxy share.

2.2. **Proxy signature generation phase.** Without loss of generality, we assume that any u or more proxy signers want to sign a message m cooperatively on behalf of the proxy group. Let $D_P = \{P_1, P_2, \cdots, P_u\}$ be the actual proxy signers.

1. Each $P_i \in D_P$ chooses a random number $b_i \in Z_q^*$ and broadcasts r_i.

$$r_i = g^{b_i} \bmod p$$

2. For each received r_j $(j = 1, 2, \cdots, u; j \neq i)$, each $P_i \in D_P$ calculates

$$\begin{aligned} R &= \prod_{j=1}^{u} r_j \bmod p, \\ s_i &= b_i R + (\sigma + x_{P_i}) h(R \parallel APSID \parallel m) \bmod q. \end{aligned}$$

   Here, s_i is the individual proxy signature which is sent to the designated clerk.
3. For each received s_i, the designated clerk checks whether the following equation holds

$$g^{s_i} \overset{?}{=} r_i^R((K^K \prod_{i=1}^{t} y_{O_i}^{h(K \| m_w \| AOSID)})^{u^{-1}} y_{P_i})^{h(R \| APSID \| m)} \bmod p.$$

   If it does, (r_i, s_i) is a valid individual proxy signature of m. If all the individual proxy signatures of m are valid, the designated clerk calculates

$$S = \sum_{j=1}^{u} s_j \bmod q.$$

The proxy signature of m is $(m_w, K, AOSID, R, S, APSID)$.

2.3. **Proxy signature verification phase.** Any verifier can verify the proxy signature and identify the actual signers. The steps are described as following:

1. According to m_w, $AOSID$ and $APSID$, the verifier gets the public keys of the original signers and proxy signers from CA and knows who the actual original signers and the actual proxy signers are.
2. The verifier checks the validity of the proxy signature of message m through the following equation:

$$g^S \overset{?}{=} R^R(K^K \prod_{i=1}^{t} y_{O_i}^{h(K \| m_w \| AOSID)} \prod_{j=1}^{u} y_{P_j})^{h(R \| APSID \| m)} \bmod p.$$

If it holds, the proxy signature $(m_w, K, AOSID, R, S, APSID)$ of m is valid.

3. **Security Analysis of the Proposed Scheme.** In the proposed scheme, all the actual original signers' secret keys are used in the proxy share generation phase to create a proxy share. Thus, it is necessary for the group of proxy signers to verify the proxy share by using all of the actual original signers' public keys. It is also necessary for any verifier to verify the proxy signature verification equation by using all the actual original signers' public keys. These actual original signers' public keys are certified by CA. Without the knowledge of the original signers' secret keys, any malicious original signer(s), malicious proxy signer(s) or outsider(s) are unable to generate the proxy share in the proposed scheme. As the result, the original group cannot deny that they have delegated the signing capability to the group of proxy signers because of the existence of the proxy share.

In the proxy signature generation phase, all the actual proxy signers' secret keys are used to generate a proxy signature. Thus, it is also necessary for any verifier to verify the proxy signature verification equation by using all the actual proxy signers' public keys. These actual proxy signers' public keys are certified by CA. Without knowing the proxy signers' secret keys, any malicious original signer(s), malicious proxy signer(s) or outsider(s) are also unable to execute the proposed scheme. As the result, the proxy group cannot deny creating the proxy signature on behalf of the original group.

To combat the forgery attack, we consider the security of the proxy signature verification equation:

$$g^S = R^R(K^K \prod_{i=1}^{t} y_{O_i}^{h(K\|m_w\|AOSID)} \prod_{j=1}^{u} y_{P_j})^{h(R\|APSID\|m)} \bmod p.$$

In the case, an outsider tries to forge a valid proxy signature to pass the proxy signature verification. Let

$$\begin{aligned} V_O &= K^K \prod_{i=1}^{t} y_{O_i}^{h(K\|m_w\|AOSID)} \bmod p, \\ V_P &= \prod_{j=1}^{u} y_{P_j} \bmod p. \end{aligned}$$

Rewrite the proxy signature verification equation as

$$g^S = R^R(V_O V_P)^{h(R\|APSID\|m)} \bmod p.$$

V_O depends on the parameters K, m_w and $AOSID$. V_P is a fixed value. It works as the proxy signers' public keys which are certified by CA. Under the condition of given m', $APSID'$ and V_O', it is difficult to determine R' and S' based on the discrete logarithm problem and one-way hash inverse function. Again, given m', $APSID'$, R' and S', a V_O' is to be computed so that the equation holds. However, it is difficult to find m_w', $AOSID'$ and K' such that the equation

$$V_O = K^K \prod_{i=1}^{t} y_{O_i}^{h(K\|m_w\|AOSID)} \bmod p$$

holds. Also, it requires to solve the discrete logarithm problem and one-way hash inverse function. Therefore, the proxy signature verification equation is secure against the forgery attack.

4. **Conclusions.** Proxy mono-signature schemes, proxy multi-signature schemes and threshold proxy signature schemes are popular research topics these days. The proxy signature is useful for a group of proxy signers to sign a message on behalf of a group of the original signers. In this paper, we propose a new type of proxy signature scheme which allows (t, n) original signers to jointly make (u, v) proxy signers to sign messages on behalf of them. This new proxy signature scheme can be widely used in practice.

REFERENCES

[1] A. K. Awasthi and S. Lal, ID-based ring signature and proxy ring signature schemes from bilinear pairings, *International Journal of Network Security*, vol.4, no.2, pp.187-192, 2007.

[2] T. Cao and X. Mao, Original signer's forgery attacks on discrete logarithm based proxy signature schemes, *International Journal of Network Security*, vol.4, no.3, pp.355-360, 2007.

[3] Y. F. Chang and C. C. Chang, Robust t-out-of-n proxy signature based on RSA cryptosystems, *International Journal of Innovative Computing, Information and Control*, vol.4, no.2, 425-431, 2008.

[4] M. L. Das, A. Saxena, D. B. Phatak, Proxy signature scheme with effective revocation using bilinear pairings, *International Journal of Network Security*, vol.4, no.3, pp.312-317, 2007.

[5] L. Guo and Y. Liu, Security analysis and improvement of Hsu et al. threshold proxy signature scheme, *International Journal of Network Security*, vol.2, no.1, pp.69-72, 2006.

[6] C. L. Hsu, T. S. Wu, and T. C. Wu, New nonrepudiable threshold proxy signature scheme with known signers, *The Journal of Systems and Software*, no.58, pp.119-124, 2001.

[7] M. S. Hwang, I. C. Lin, and E. J. L. Lu, A secure nonrepudiable threshold proxy signature scheme with known signers, *International Journal of Informatica*, vol.11, no.2, pp.1-8, 2000.

[8] S. Kim, S. Park, and D. Won, Proxy signatures, revisited, *Proc. of the ICICS'97, LNCS*, vol.1334, pp.223-232, 1997.

[9] N. Y. Lee, T. Hwang, and C. H. Wang, 'n Zhang's nonrepudiable proxy signature schemes, *Proc. of the ACISP'98, LNCS*, vol.1438, pp.415-422, 1998.

[10] J. Li and S. Wang, New efficient proxy blind signature scheme using verifiable self-certified public key, *International Journal of Network Security*, vol.4, no.2, pp.193-200, 2007.

[11] R. Lu, Z. Cao, and J. Shao, On security of two nonrepudiable threshold multi-proxy multi-signature schemes with shared verification, *International Journal of Network Security,* vol.4, no.3, pp.248-253, 2007.

[12] M. Mambo, K. Usuda, and E. Okamoto, Proxy signatures: Delegation of the power to sign message, *IEICE Transactions on Fundamentals*, vol.E79-A, pp.1338-1353, Sep. 1996.

[13] M. Mambo, K. Usuda, and E. Okamoto, Proxy signatures for delegating signing operation, *Proc. of the Third ACM Conference on Computer and Communications Security*, pp.48-57, 1996.

[14] H. M. Sun, An efficient nonrepudiable threshold proxy signature scheme with known signers, *Computer Communications*, vol.22, no.8, pp.717-722, 1999.

[15] Z. W. Tan, Improvement on nominative proxy signature schemes, *International Journal of Network Security*, vol.7, no.2, pp.175-180, 2008.

[16] Q. Xie and X. Y. Yu, Cryptanalysis of two nonrepudiable threshold proxy signature schemes, *International Journal of Network Security*, vol.3, no.1, pp.18-22, 2006.

[17] L. Yi, G. Bai, and G. Xiao, Proxy multi-signature scheme: A new type of proxy signature scheme, *Electronics Letters*, vol.36, no.6, pp.527-528, 2000.

[18] K. Zhang, Threshold proxy signature schemes, *Proc. of the 1997 Information Security Workshop*, pp.191-197, 1997.