May 2003, Vol.18, No.3, pp.399–402 J. Comput. Sci. & Technol.

Nonrepudiable Proxy Multi-Signature Scheme

LI JiGuo (李继国)[1], CAO ZhenFu (曹珍富)[2] and ZHANG YiChen (张亦辰)[3]

[1] *Department of Computer Science and Engineering, Harbin Institute of Technology, Harbin 150001, P.R. China*

[2] *Department of Computer Science and Engineering, Shanghai Jiao Tong University Shanghai 200030, P.R. China*

[3] *Department of Computer Science and Engineering, Qiqihar University, Qiqihar 161005, P.R. China*

E-mail: ljg1688@163.com; zfcao@cs.sjtu.edu.cn

Received May 28, 2001; revised February 5, 2002.

Abstract The concept of proxy signature introduced by Mambo, Usuda, and Okamoto allows a designated person, called a proxy signer, to sign on behalf of an original signer. However, most existing proxy signature schemes do not support nonrepudiation. In this paper, two secure nonrepudiable proxy multi-signature schemes are proposed that overcome disadvantages of the existing schemes. The proposed schemes can withstand public key substitution attack. In addition, the new schemes have some other advantages such as proxy signature key generation and updating using insecure channels. This approach can also be applied to other ElGamal-like proxy signature schemes.

Keywords nonrepudiable, digital signature, proxy signature, multi-signature

1 Introduction

The concept of proxy signature introduced by Mambo, Usuda, and Okamoto[1,2] allows a designated person, called a proxy signer, to sign on behalf of an original signer. Mambo[1,2] *et al.* showed proxy signature should have properties of proxy signer's deviation, unforgeability, verifiability, distinguishability, identifiablity, and undeniability. The proxy signature plays an important role in many applications and receives great attention after it was proposed. So far, three types of delegation, full delegation, partial delegation and delegation with warrant, have been proposed. Zhang[3] and Kim[4] *et al.* proposed a threshold proxy signature which is a variant of proxy signature, respectively. Sun[5] *et al.* showed that their threshold proxy signature suffered from some weaknesses and gave a modified scheme. Later, Sun[6] proposed an efficient nonrepudiable threshold proxy signature. But Hwang[7] *et al.* showed Sun's scheme had two disadvantages and proposed a modified scheme which remedied the weakness of Sun's scheme. Sun and Chen[8,9] proposed a time-stamped proxy signature scheme with traceable receivers which can ascertain whether a proxy signature is created at a certain time, and can trace the receivers who received the proxy signature from the proxy signer. Recently, Yi LiJiang[10] *et al.* proposed a proxy multi-signature scheme.

In some proxy signature schemes[1−4,10], it is possible for the original signer to generate a proxy signature instead of the proxy signer if the original signer can derive the proxy signature key from original signature key. Therefore, it is important and sometimes necessary to identify exactly who signs the proxy signature. This property is called nonrepudiation. Hence, a partial proxy with the property of nonrepudiation is ideal. Hwang and Shi[11] proposed a specifiable proxy signature scheme, which provides the fair security of protection for the proxy signer and the original signer.

The paper is organized as follows. In Section 2, two secure nonrepudiable proxy multi-signatures are proposed. The security analysis, performance analysis and advantages of our schemes are given in Section 3. Finally, we draw the conclusions in Section 4.

2 Proposed Nonrepudiable Proxy Multi-Signature Scheme

The proxy signature schemes of Mambo[1,2] *et al.*, Kim[4] *et al.* and Yi LiJiang[10] *et al.* do not provide nonrepudiation. It is impossible to decide

This work is supported by the National Natural Science Foundation of China (Grant No.60072018), the National Science Fund for Distinguished Young Scholars (Grant No.60225007) and the Special Fund of China for Ph.D. Instructors in Universities (Grant No.20020248024).

who is the actual signer of a proxy signature in their schemes. The original or the proxy signer cannot disavow a valid proxy signature. In practice, it is important and sometimes necessary to exactly identify who is the actual signer of a proxy signature for internal auditing purpose or when there is abusing of signing capability. We call this property nonrepudiation. Another drawback of their schemes[1,2,4,10] is that they require a secure channel to transmit the proxy signature key from the original signer to the proxy signer. Anyone who can intercept this proxy signature key can impersonate the proxy signer. In addition, their schemes are insecure against public key substitution attack. Next we will propose two modified schemes which overcome these shortcomings.

2.1 Nonrepudiable Proxy Multi-Signature Scheme 1

Let $A_1, \ldots, A_n$ be n original signers. They jointly ask a proxy signer to carry out signing a document m for them altogether. A_i $(i = 1, \ldots, n)$ selects $s_i \in_R Z_q$ as a secret key and corresponding public key is $V_i = g^{s_i} \bmod p$. Proxy signer selects $s_p \in_R Z_q$ as his secret key and corresponding public key is $V_p = g^{s_p} \bmod p$.

1) Original signer A_i $(i = 1, \ldots, n)$ selects $\tilde{k}_i \in Z_q$ and computes $\widetilde{K}_i = g^{\tilde{k}_i} \bmod p$ and then sends $\widetilde{K}_i$ to proxy signer.

2) Proxy signer selects $\alpha_i \in_R Z_q$ and computes $K_i = g^{\alpha_i}\widetilde{K}_i \bmod p \bmod q$. He sends K_i to original signer A_i.

3) Original signer A_i computes $\tilde{\sigma}_i = K_i V_i s_i + \tilde{k}_i K_i \bmod q$ and sends $\tilde{\sigma}_i$ to proxy signer.

4) Proxy signer computes $\sigma_i = \tilde{\sigma}_i + K_i \alpha_i \bmod q$, and checks if the following equality holds:

$$g^{\sigma_i} = V_i^{K_i V_i} K_i^{K_i} \bmod p.$$

If it holds, proxy signer accepts σ_i as a valid proxy signature key from original signer A_i. Otherwise, he rejects it and requests another one, or he stops the protocol.

5) Proxy key generation: if proxy signer confirms the validity of all (σ_i, K_i). Then he computes $\sigma = V_p s_p + \sum_{j=1}^{n} \sigma_i$.

6) Signing by proxy signer: when proxy signer signs a document m on behalf of $A_1, \ldots, A_n$, he uses σ as his signature key. Then the proxy signature is $(m, \mathrm{sign}_\sigma(m), K_1, \ldots, K_n)$, where $\mathrm{sign}_\sigma(m)$ is computed by using any existing signature scheme based on discrete logarithm[12].

7) Verification of proxy signature: the verifier firstly computes the verifying key

$$V' = V_p^{V_p} V_1^{K_1 V_1} \cdots V_n^{K_n V_n} K_1^{K_1} \cdots K_n^{K_n} \bmod p,$$

then checks the validity of the signature $\mathrm{sign}_\sigma(m)$ by using the same verification process as the ordinary signature scheme.

2.2 Nonrepudiable Proxy Multi-Signature Scheme 2

Let $h(\ )$ be a public collision resistant function. T is time-stamped, m_w is a warrant which contains the original signer's ID, the proxy signer's ID, the delegation period, etc. The other system parameters are the same as in Subsection 2.1.

1) Original signer A_i $(i = 1, \ldots, n)$ selects $\tilde{k}_i \in_R Z_{p-1}^*$ and computes $\widetilde{K}_i = g^{\tilde{k}_i} \bmod p$ and then sends $\widetilde{K}_i$ to proxy signer.

2) Proxy signer selects $\alpha_i \in_R Z_{p-1}^*$ and computes $K_i = g^{\alpha_i}\widetilde{K}_i \bmod p \bmod q$. He sends K_i to original signer A_i.

3) Original signer A_i computes $e_i = h(m_w, K_i, V_1, \ldots, V_n, V_p, T)$, $\tilde{\sigma}_i = e_i s_i + \tilde{k}_i \bmod (p-1)$ and sends $\tilde{\sigma}_i$ to proxy signer.

4) Proxy signer computes $\sigma_i = \tilde{\sigma}_i + \alpha_i \bmod (p-1)$ and checks if the following equality holds:

$$g^{\sigma_i} = V_i^{e_i} \cdot K_i \bmod p$$

If it holds, proxy signer accepts σ_i as a valid proxy signature key from original signer A_i. Otherwise, he rejects it and requests another one, or he can stop the protocol.

5) Proxy key generation: if proxy signer confirms the validity of all (σ_i, K_i). He computes $e_p = h(m_w, K_1, \ldots, K_n, V_1, \ldots, V_n, T)$ and $\sigma = e_p s_p + \sum_{j=1}^{n} \sigma_i$.

6) Signing by proxy signer: proxy signer uses σ as his signature key when he signs a document m on behalf of $A_1, \ldots, A_n$. The proxy signature is $(m, \mathrm{sign}_\sigma(m), K_1, \ldots, K_n, m_w, T)$, where $\mathrm{sign}_\sigma(m)$ is computed by using any existing signature scheme based on discrete logarithm[12].

7) Verification of proxy signature: the verifier first computes e_p, e_i $(i = 1, \ldots, n)$, the verifying key $V' = V_p^{e_p} V_1^{e_1} \ldots V_n^{e_n} K_1 \ldots K_n \bmod p$, then checks the validity of the signature $\mathrm{sign}_\sigma(m)$ by using the same verification process as the ordinary signature scheme.

3 Security Analysis and Performance Analysis

Clearly, security analysis and performance analysis of above two modified schemes are similar. In this section, we only analyze nonrepudiable proxy multi-signature Scheme 1 as follows.

3.1 Security Analysis

In the following, it will be shown that the nonrepudiable proxy multi-signature Scheme 1 is secure and nonrepudiable.

Attack 1. The difficulty in finding the corresponding proxy signature key σ from the equation $g^{\sigma} = V' = V_p^{V_p} V_1^{K_1 V_1} \cdots V_n^{K_n V_n} K_1^{K_1} \cdots K_n^{K_n} \bmod p$ for the attacker knowing $K_1, \ldots, K_n$ is equivalent to solving discrete logarithm hard problem. Hence, it is computationally infeasible for the attacker to derive proxy signer's signature key σ.

Attack 2. Without loss of generality, we assume that the original signer A_1 intends to forge a proxy signature key σ at the cost of having his secret key unknown by public key substitution attack in which A_1 can forge a valid proxy signature by updating his own public key. He firstly selects $\sigma, K_1, \ldots, K_n \in_R Z_p^*$, then solves

$$V_1 = \big(\big((V_p^{V_p} V_2^{K_2 V_2} \cdots V_n^{K_n V_n} K_1^{K_1} \cdots K_n^{K_n})^{-1} g^{\sigma}\big)^{K_1^{-1}}\big) V_1^{-1} \bmod p$$

such that

$$g^{\sigma} = V' = V_p^{V_p} V_1^{K_1 V_1} \cdots V_n^{K_n V_n} K_1^{K_1} \cdots K_n^{K_n} \bmod p.$$

But this problem is more difficult than discrete logarithm hard problem.

Attack 3. Without loss of generality, we assume $n = 2$. An attacker may try to forge proxy signature secret key σ by finding σ, K_1, K_2 such that the congruence

$$g^{\sigma} = V_p^{V_p} V_1^{K_1 V_1} V_2^{K_2 V_2} K_1^{K_1} K_2^{K_2} \bmod p$$

holds. Let

$$K_1 = V_p^a V_1^b V_2^c g^d \bmod p,$$
$$K_2 = V_p^e V_1^f V_2^h g^w \bmod p$$

then

$$g^{\sigma} = V_p^{V_p + K_1 a + K_2 e} V_1^{K_1 V_1 + K_1 b + K_2 f} V_2^{K_1 V_2 + K_1 c + K_2 h} g^{K_1 d + K_2 w} \bmod p.$$

Thus, the following four equations must hold:

$$V_p + K_1 a + K_2 e = 0 \bmod q,$$
$$K_1 V_1 + K_1 b + K_2 f = 0 \bmod q$$
$$K_2 V_2 + K_1 c + K_2 h = 0 \bmod q,$$
$$\sigma = K_1 d + K_2 w \bmod q$$

But the only way to determine K_1 and K_2 is to fix a, b, c, d, e, f, h, w. Thus, the first three equations will hold with a negligibly small probability. This attack fails to work.

Now let us consider the public key substitution attack. An attacker, taking the role of proxy signer, must compute σ, V_p, K_1, K_2 such that the congruence

$$g^{\sigma} = V_p^{V_p} V_1^{K_1 V_1} V_2^{K_2 V_2} K_1^{K_1} K_2^{K_2} \bmod p$$

holds. Let

$$V_p = V_1^a V_2^b g^c \bmod p,$$
$$K_1 = V_1^d V_2^e g^f \bmod p,$$
$$K_2 = V_1^h V_2^w g^q \bmod p,$$

such that

$$g^{\sigma} = V_1^{K_1 V_1 + V_p a + K_1 d + K_2 h} V_2^{K_2 V_2 + V_p b + K_1 e + K_2 w} g^{V_p c + K_1 f + K_2 q} \bmod p,$$

where $a, b, c, d, e, f, h, w, q$ are integers to be determined. Therefore, the following three equations must hold:

$$K_1 V_1 + V_p a + K_1 d + K_2 h = 0 \bmod q,$$
$$K_2 V_2 + V_p b + K_1 e + K_2 w = 0 \bmod q$$
$$V_p c + K_1 f + K_2 q = \sigma \bmod q$$

The attacker must first fix d, e, f, h, w, q to determine K_1, K_2. However, it is infeasible to solve a, b such that the first two equations hold. This is because V_p depends on a, b and hence any change of a, b will lead to the change of V_p. If the attacker fixes V_p such that it is independent of a, b, then he has to solve c from $V_p = V_1^a V_2^b g^c \bmod p$ such that $V_p c + K_1 f + K_2 q = \sigma \bmod q$ holds. It is discrete logarithm hard problem. Thus the first two equations will hold with a negligibly small probability. Finally, if the attacker lets $a, b, c, d, e, f, h, w, q \in_R Z_q$, then it is believed that above three equations will hold with a negligibly small probability.

3.2 Performance Analysis

We only analyze nonrepudiable proxy multi-signature Scheme 1. The performance of Scheme 1 is measured by the time complexity and the total communication cost. We analyze the performance of Scheme 1 as follows.

Let T_E, T_M and T_I be the times for computing modular exponentiation, multiplication and inverse, respectively. The time complexity required

by the original signer is $nT_E + 3nT_M$, which heavily depends on the computation of Steps 1), 3). The time complexity required by proxy signer is $(4n + 1)T_E + (4n + 3)T_M + T_I$, which contains the time complexity of $\text{sign}_\sigma(m)$, which heavily depends on the computation of Steps 2), 4)–6). The time complexity contributed by the verifier is $(2n + 4)T_E + (3n + 1)T_M$ which contains the time complexity of verification of $\text{sign}_\sigma(m)$, which heavily depends on the computation of Step 7).

Denoted by $|x|$ is the bit length of an integer x. In the proposed scheme, the size of proxy signature $(m, \text{sign}_\sigma(m), K_1, \ldots, K_n)$ for message m is $|p|+(n+1)|q|+|m|$ which contains the communication cost of $\text{sign}_\sigma(m)$ and the total communication cost is $(n + 1)|p| + (3n + 1)|q| + |m|$ which heavily depends on the communication cost of Steps 1)–6).

Remark 1. The time complexity and the total communication cost $\text{sign}_\sigma(m)$ are measured by ElGamal[12] signature scheme.

Remark 2. In Scheme 1, proxy signature key σ contains information of the original signer A_i's secret key s_i and verifying key $V' = V_p^{V_p} V_1^{K_1 V_1} \cdots V_n^{K_n V_n} K_1^{K_1} \cdots K_n^{K_n} \bmod p$ contains information of A_i's public key V_i. Hence, the verifier can be convinced that the proxy signature is authorized by the original signer A_i. On the other hand, since proxy signature key σ contains information of the proxy signer's secret key s_p and verifying key V' contains information of the proxy signer's public key V_p, so the proxy signer does not disavow his signature.

Remark 3. In Scheme 1, another merit of our protocol is that communications between an original signer and a proxy signer need not use secure channel, because an attacker does not know σ and the secret key s_p of the proxy signer. Even if an attacker knows all the messages transmitted between an original signer and a proxy signer, he does not obtain proxy signature key σ.

Remark 4. Since we use one-way hash function $h(\ )$, time-stamped T, warrant m_w in nonrepudiable proxy multi-signature Scheme 2, the security of this scheme is better than that of nonrepudiable proxy multi-signature Scheme 1. Security analysis is similar with nonrepudiable proxy multi-signature Scheme 1.

4 Conclusions

In this paper, we propose two secure nonrepudiable proxy multi-signature schemes that overcome the disadvantages of schemes proposed by Yi Li-Jiang *et al.*, Mambo *et al.* and Kim *et al.*, respectively. The proposed schemes can withstand public key substitution attack. In addition, our new schemes have some other advantages such as proxy signature key generation and updating using insecure channels. Our approach can also be applied to other ElGamal-like proxy signature schemes. The security analysis and performance analysis of the modified schemes are given.

Acknowledgement The authors would like to thank anonymous referees for their suggestions to improve this paper. The authors would also like to thank Professor Min-Shiang Hwang and Dr. Shin-Jia Hwang of the Department of Information Management, Chaoyang University of Technology for their valuable references.

References

[1] Mambo M, Usuda K, Okamoto E. Proxy signatures for delegating signing operation. In *Proc. 3rd ACM Conference on Computer and Communications Security,* ACM Press, 1996, pp.48–57.

[2] Mambo M, Usuda K, Okamoto E. Proxy signatures: Delegation of the power to sign messages. *IEICE Trans. Fundam.,* 1996, E79-A(9): 1338–1354.

[3] Zhang K. Threshold proxy signature schemes. In *1997 Information Security Workshop,* Japan, 1997, pp.191–197.

[4] Kim S, Park S, Won D. Proxy signatures, revisited. In *Proc. ICICS'97, Int. Conf. on Information and Communications Security, LNCS,* Springer-Verlag, 1997, 1334: 223–232.

[5] Sun H M, Lee N Y, Hwang T. Threshold proxy signatures. In *IEE Proc. Computers & Digital Techniques,* 1999, 146(5): 259–263.

[6] Sun H M. An efficient nonrepudiable threshold proxy signature scheme with known signers. *Computer Communications,* 1999, 22(8): 717–722.

[7] Hwang M S, Lin I C, Lu E J L. A secure nonrepudiable threshold proxy signature scheme with known signers. *International Journal of Informatica,* 2000, 11(2): 1–8.

[8] Sun H M, Chen B J. Time-stamped proxy signatures with traceable receivers. In *Proc. the Ninth National Conference on Information Security,* 1999, pp.247–253.

[9] Sun H M. Design of time-stamped proxy signatures with traceable receivers. In *IEE Proc. Computers & Digital Techniques,* 2000, 147(6): 462–466.

[10] Yi L J, Bai G Q, Xiao G Z. Proxy multi-signature scheme: A new type of proxy signature scheme. *Electron. Lett.,* 2000, 36: 527–528.

[11] Hwang S J, Shi C H. Specifiable proxy signature schemes. In *1999 Computer Symposium,* Taipei, 1999, pp.190–197.

[12] ElGamal T. A public key cryptosystem and signature scheme based on discrete logarithms. *IEEE Trans.,* 1985, IT-31(4): 469–472.