An Improvement of Nonrepudiable Threshold Proxy Signature Scheme with Known Signers*

Min-Shiang Hwang† Shiang-Feng Tzeng‡ Cheng-Ying Yang§

Department of Management Information System†
National Chung Hsing University
250 Kuo Kuang Road, 402 Taichung, Taiwan, R.O.C.
Email: mshwang@nchu.edu.tw

Department of Computer Science and Information Engineering‡
National Central University
No. 300, Jung-da Rd., Jung-li City, Taoyuan, Taiwan 320, R.O.C.

Graduate Institute of Networking and Communication Engineering§
Chaoyang University of Technology
168 Gifeng E. Rd., Wufeng,
Taichung County, Taiwan 413, R.O.C.

October 4, 2003

*This research was partially supported by the National Science Council, Taiwan, R.O.C., under contract no.: NSC90-2213-E-324-004.

An Improvement of Nonrepudiable Threshold Proxy Signature Scheme with Known Signers

Abstract

In a (t, n) threshold proxy signature scheme, which is a variant of the proxy signature scheme, the proxy signature key is shared among a group of n proxy signers delegated by the original signer. Any t or more proxy signers can cooperatively sign messages on behalf of the original signer. In 2000, Hwang et al. proposed a secure nonrepudiable threshold proxy signature scheme with known signers. In this paper, we point out a cryptanalysis of their scheme. Furthermore, we improve the security of the threshold proxy signature scheme which remedies the weakness of Hwang et al.'s scheme.

Keywords: Cryptography, digital signature, proxy signature, threshold proxy signature.

1 Introduction

The original signer delegates her/his signing capability to a designated person, called a proxy signer. The proxy signer can generate proxy signature on a message on behalf of the original signer. The concept of the proxy signature scheme was first introduced by Mambo et al. [8, 9] in 1996.

Following the development of the proxy signature, the (t, n) threshold proxy signature schemes were widely studied [3, 4, 6, 7, 10, 11, 12, 13]. The original signer delegates the proxy signature key to an authorized proxy group. Any t or more proxy signers of the proxy group of n members can cooperatively sign the message on behalf of the original signer.

Based on Kim's scheme [6], Hwang et al. [4] proposed a secure nonrepudiable threshold proxy signature scheme to improve Sun's scheme [10]. The main advantage of Hwang et al.'s scheme is that it has a property with non-repudiation, the verifier is able to identify the actual proxy signer in the proxy group, and anyone cannot forge the legal proxy signature. Recently, Hwang and Chen [5] present this scheme is vulnerable against their insider attack. This attack needs the cooperation of the original signer and one malicious proxy signer. They can be forged threshold proxy signatures without the agreement of the other proxy signers.

In this article, we show a forged attack of Hwang et al.'s scheme (Hwang-Lin-Lu Scheme) and remedy the attacking method of their scheme. In next section, we review Hwang-Lin-Lu scheme and point out its weakness. Then, in Section 3, our new secure scheme and the security of the proposed scheme will be proposed and analyzed. Finally, the concluding remarks will be in the last section.

2 Hwang-Lin-Lu Scheme and Its Weakness

In this section, we first review Hwang-Lin-Lu's threshold proxy signature scheme [4] and then present a weakness of their scheme.

2.1 Review of Hwang-Lin-Lu Scheme

There are three phases in Hwang-Lin-Lu scheme: proxy sharing generation, proxy signature issuing, and proxy signature verification. Initially, the system parameters are defined as follows:

- p: a large prime
- q: a large prime factor of $p-1$
- g: a generator of order q

- $h(\cdot)$: a one-way hash function

- m_w: a warrant in which records the identity of the original signer and proxy signers of the proxy group, the parameters t and n, and the valid delegation time, etc.

- $ASID$: (Actual Signers' ID) the identities of the actual signers

Each user P_i owns private key $x_i \in Z_q^*$ and a public key $y_i = g^{x_i} \bmod p$ which is certified by the certificate authority (CA). Let P_0 be the original signer and $G = \{P_1, P_2, \cdots, P_n\}$ be the proxy group of n proxy signers.

In the proxy sharing generation phase, the group shares a secret value from multiplicative sharing technique. The steps are described as follows:

1. Group Key Generation: Each $P_i \in G$ randomly generates a secret polynomial $f_i(x)$ of degree $t-1$, which $f_i(x) = x_i + a_{(i,0)} + a_{(i,1)}x + \cdots + a_{(i,t-1)}x^{t-1} \bmod q$. Here $a_{(i,0)}, a_{(i,1)}, \cdots, a_{(i,t-1)}$ are random numbers. Then, each P_i can receive the shared value $f_j(i)$ from P_j, where $0 < i, j < n$ and $i \neq j$. Therefore, each P_i can obtain a value s_i,

$$\begin{aligned} s_i &= f(i) \\ &= f_1(i) + f_2(i) + \cdots + f_n(i) \\ &= \sum_{i=1}^{n} x_i + a_0 + a_1 i + \cdots + a_{t-1} i^{t-1} \bmod q, \end{aligned}$$

   where $a_i = \sum_{i=1}^{t} a_{(i,0)} \bmod p$. The proxy group then publishes y_G ($y_G = \prod_{i=1}^{n} g^{x_i} = \prod_{i=1}^{n} y_i \bmod p$) and A_j ($A_j = g^{a_j} \bmod p; j = 0, 1, \cdots, t-1$).

2. Proxy Generation: The original signer chooses a random number k and computes the parameter K, $K = g^k \bmod p$. Then, the original signer can obtain the value σ,

$$\sigma = e x_0 + k \bmod q,$$

   where $e = h(m_w, K)$.

3. Proxy Sharing: The original signer shares a proxy key σ in a (t, n) threshold scheme. She/He generates a secret degree $t-1$ polynomial $f'(x)$, and computes

$$\begin{aligned} \sigma_i &= f'(i) \\ &= \sigma + b_1 i + \cdots + b_{t-1} i^{t-1}, \quad for \;\; j = 1, 2, \cdots, n, \end{aligned} \tag{1}$$

where b_j is a random number, $j = 1, 2, \cdots, t-1$. After the original signer sends σ_i to proxy signer P_i, $i = 1, 2, \cdots, n$, over a secured channel, and publishes $B_j = g^{b_j} \bmod p$, $j = 1, 2, \cdots, t-1$, and (m_w, K).

4. Proxy Sharing Generation: After receiving σ_i, each $P_i \in G$ checks whether or not the following equation is hold,

$$g^{\sigma_i} = y_0^{h(m_w, K)} K \prod_{j=1}^{t-1} B_j^{ij} \bmod p.$$

If the above equation holds, each P_i computes

$$\sigma_i' = \sigma_i + s_i h(m_w, K) \bmod q,$$

the σ_i' as a proxy sharing of P_i. Otherwise, the proxy signer rejects σ_i.

In proxy signature issuing phase, assume that t proxy signers want to cooperatively sign a message m on behalf of the proxy group. Let $D = \{P_1, P_2, \cdots, P_t\}$ be the proxy group of t proxy signers.

1. As Step 1 of the proxy sharing generation phase, the polynomial is using $f_i"(x) = (x_i + c_{(i,0)}) + c_{(i,1)}x + \cdots + c_{(i,t-1)}x^{t-1} \bmod q$. Each $P_i \in D$ can obtain the value s_i' when they receive the values $f_j"(i)$ from P_j, where $j \neq i$, as shown in following:

$$\begin{aligned} s_i' &= f"(i) \\ &= f_1"(i) + f_2"(i) + \cdots + f_t"(i) \\ &= \sum_{i=1}^{t} x_i + c_0 + c_1 i + \cdots + c_{t-1} i^{t-1} \bmod q. \end{aligned} \tag{2}$$

The public parameters of this step are $Y = g^{c_0} \bmod p$ and $C_j = g^{c_j} \bmod p, j = 1, 2, \cdots, t-1$.

2. Each $P_i \in D$ has two secret values σ'_i and s'_i. Therefore, P_i can computes

$$\gamma_i = s'_i Y + \sigma'_i h(ASID, m) \bmod q, \tag{3}$$

where m is the message. Then, P_i sends γ_i to proxy signer P_j, $j = 1, 2, \cdots, t$ and $j \neq i$.

3. For each received γ_j $(j = 1, 2, \cdots, t; j \neq i)$, P_i can check whether the following equation is hold.

$$g^{\gamma_j} \overset{?}{=} [Y(\prod_{i=1}^{t-1} C_i^{j^i})(\prod_{i=1}^{t-1} y_i)]^Y$$

$$\times[(y_0^{h(m_w,K)} K \prod_{i=1}^{t-1} B_i^{j^i})(y_G A_0 \prod_{i=1}^{t-1} A_i^{j^i})^{h(m_w,K)}]^{h(ASID,m)} \bmod p.$$

4. Each $P_i \in D$ can apply Lagrange formula [1] to γ_j to compute

$$T = f''(0)Y + [f(0) + f'(0)]h(ASID, m). \tag{4}$$

The proxy signature on m is $(m, T, K, Y, A_0, m_w, ASID)$.

In the proxy verification phase, any verifier can verify the validity of the proxy signature and identify the actual signers. The steps of this phase are described as follows:

1. According to m_w and $ASID$, the verifier gets the public keys of the proxy signers from the CA, and knows whom the original signer and the actual proxy signers are.

2. The verifier checks the validity of the proxy signature on the message m from the following equation:

$$g^T \overset{?}{=} [y_0^{h(m_w,K)} K A_0 \prod_{i=1}^{n} y_i]^{h(ASID,m)} (Y \prod_{i=1}^{t} y_i)^Y \bmod p.$$

If it holds, the proxy signature $(m, T, K, Y, A_0, m_w, ASID)$ for m is valid.

2.2 The Weakness of Hwang-Lin-Lu Scheme

In Hwang-Lin-Lu's (t, n) threshold proxy signature scheme, any verifier can verify the validity of the proxy signature and identity the actual signers. In this subsection, a forged attack will be proposed on Hwang-Lin-Lu scheme. In this attack, the malicious original signer can impersonate any t or more proxy signers in the group of n members. She/He can forge threshold proxy signatures without the agreement of the proxy signers.

Without losing generality, suppose that the malicious original signer wants to forge a proxy signature on a message m without t proxy signers $P_1, P_2, \cdots, P_t$. So $ASID$ records the identities of $P_1, P_2, \cdots, P_t$. The malicious original signer selects a random integer α from Z_q^* and computes

$$\begin{aligned} A_0 &= g^{\alpha}(y_1 y_2 \cdots y_n)^{-1} \bmod p, \\ Y &= g^{\alpha}(y_1 y_2 \cdots y_t)^{-1} \bmod p, \\ T &= (\alpha + \sigma)h(ASID, m) + \alpha Y \bmod q. \end{aligned}$$

Finally, the malicious original signer can forge a valid proxy signature $(m, T, K, Y, A_0, m_w, ASID)$. The following shows why the proxy signature $(m, T, K, Y, A_0, m_w, ASID)$ is valid.

$$(y_0^{h(m_w,K)} K A_0 \prod_{i=1}^{n} y_i)^{h(ASID,m)} (Y \prod_{i=1}^{t} y_i)^Y$$

$$\begin{aligned} &\equiv (y_0^{h(m_w,K)} g^k (g^{\alpha}(y_1 y_2 \cdots y_n)^{-1}) y_1 y_2 \cdots y_n)^{h(ASID,m)} (Y \prod_{i=1}^{t} y_i)^Y \\ &\equiv (g^{x_0 h(m_w,K)+k} g^{\alpha})^{h(ASID,m)} (Y \prod_{i=1}^{t} y_i)^Y \\ &\equiv (g^{\sigma} g^{\alpha})^{h(ASID,m)} (Y \prod_{i=1}^{t} y_i)^Y \\ &\equiv (g^{\sigma} g^{\alpha})^{h(ASID,m)} ((g^{\alpha}(y_1 y_2 \cdots y_t)^{-1}) y_1 y_2 \cdots y_t)^Y \\ &\equiv (g^{\sigma} g^{\alpha})^{h(ASID,m)} (g^{\alpha})^Y \\ &\equiv g^{(\alpha+\sigma)h(ASID,m)+\alpha Y} \\ &\equiv g^T \bmod p \end{aligned}$$

In the verification phase, any verifier can verify the validity of the proxy signature and $ASID$ records the identities as actual signers of the proxy group. In fact, $P_1, P_2, \cdots, P_t$ have never signed the message m, but they cannot deny. Therefore, the threshold proxy signature is forged successfully for Hwang-Lin-Lu scheme and the malicious original signer can impersonate any t legal proxy signers in the group of n members to sign a message.

3 Improvement of Hwang-Lin-Lu Scheme

In this section, we modify Hwang-Lin-Lu scheme to remedy the weakness as described in Section 2.2. In Hwang-Lin-Lu scheme, the threshold proxy signatures can be forged by the original signer. To remedy the weakness we modify Hwang-Lin-Lu scheme and the revised scheme is presented in details.

In the proxy sharing generation phase, we replace $f_i(x)$ with $f_i(x) = x_i y_i + a_{(i,0)}A_{(i,0)} + a_{(i,1)}x + \cdots + a_{(i,t-1)}x^{t-1} \bmod q$ where $a_{(i,0)}$ is a random number. Therefore, the Equation (1) becomes

$$\begin{aligned} s_i &= f(i), \\ &= \sum_{i=1}^{n} x_i y_i + a_0 A_0 + a_1 i + \cdots + a_{t-1} i^{t-1} \bmod q, \end{aligned}$$

where $a_i = \sum_{i=1}^{t-1} a_{(i,0)} \bmod p$. The proxy group publishes y_G ($y_G = \prod_{i=1}^{n} g^{x_i y_i} = \prod_{i=1}^{n} y_i^{y_i} \bmod p$) and A_j ($A_j = g^{a_j} \bmod p; j = 0, 1, \cdots, t-1$). The other steps of the proxy sharing generation phase are the same as that of Hwang-Lin-Lu scheme.

In the proxy signature issuing phase, we also replace $f_i^{"}(x)$ with $f_i^{"}(x) = x_i y_i + c_{(i,0)}C_{(i,0)} + c_{(i,1)}x + \cdots + c_{(i,t-1)}x^{t-1} \bmod q$ where $c_{(i,0)}$ is a random number. Therefore, the Equation (2) becomes

$$\begin{aligned} s_i' &= f^{"}(i) \\ &= \sum_{i=1}^{t} x_i y_i + c_0 C_0 + c_1 i + \cdots + c_{t-1} i^{t-1} \bmod q, \end{aligned}$$

where $c_i = \sum_{i=1}^{n} c_{(i,0)} \bmod p$. The public parameters are the same as that of Hwang-Lin-Lu scheme. The proxy signer P_i computes γ_i from Equation (3) and sends γ_i to other proxy signers of the proxy group. Each proxy signer can verify the validity of γ_i from the following equation:

$$g^{\gamma_j} \stackrel{?}{=} [Y^Y(\prod_{i=1}^{t-1} C_i^{j^i})(\prod_{i=1}^{t-1} y_i^{y_i})]^Y$$

$$\times[(y_0^{h(m_w,K)} K \prod_{i=1}^{t-1} B_i^{j^i})(y_G A_0^{A_0} \prod_{i=1}^{t-1} A_i^{j^i})^{h(m_w,K)}]^{h(ASID,m)} \bmod p.$$

Then, each signer computes T from Equation (4) and the proxy signature on message m is $(m, T, K, Y, A_0, m_w, ASID)$.

Finally, the verifier checks the validity of the proxy signature and identity the actual signers of the group from the following equation:

$$g^T \stackrel{?}{=} [y_0^{h(m_w,K)} K A_0^{A_0} \prod_{i=1}^{n} y_i^{y_i}]^{h(ASID,m)} (Y^Y \prod_{i=1}^{t} y_i^{y_i})^Y \bmod p. \qquad (5)$$

If the above equation holds, the verifier can firmly believe the validity of the proxy signature and identify the actual signers.

4 Cryptanalysis

The proposed scheme can withstand the insider attack and the forging attack. To achieve the insider attack, it needs to cooperation of the original signer and one malicious proxy signer. They could forge threshold proxy signatures without the agreement of the other proxy signers. The malicious proxy signer must to change his/her public key after the public keys of the other proxy signers have been determined. Suppose the signer P_1 is the malicious proxy signer. P_1 selects a random integer α and makes his/her public key as y_1' satisfying the following equation:

$$g^\alpha = y_1'^{y_1'}(y_2^{y_2} \cdots y_n^{y_n}) \bmod p.$$

P_1 has to compute the value of y_1' satisfying

$$y_1'^{y_1'} = g^{\alpha}(y_2^{y_2} \cdots y_n^{y_n})^{-1} \bmod p.$$

If P_1 fixed the integer y_1', she/he will find that who must to solve the discrete logarithm problem to find the value of α. If P_1 first determines the integer α, she/he has to obtain the value of y_1' by solving the difficult problem. Thus, the inside attacker cannot success to forge the threshold proxy signatures.

In the forging attack, the malicious original signer can impersonate any t or more proxy signers in the group of n members. She/He can forge threshold proxy signatures without the agreement of the proxy singers. The security analysis of the forging attack on our scheme is the same as that of the insider attack on our scheme. The threshold proxy signature cannot be forged by the forging attack using the following equations:

$$A_0^{A_0} = g^{\alpha}(y_1^{y_1} y_2^{y_2} \cdots y_n^{y_n})^{-1} \bmod p,$$
$$Y^{Y} = g^{\alpha}(y_1^{y_1} y_2^{y_2} \cdots y_t^{y_t})^{-1} \bmod p.$$

Any adversary cannot compute T to satisfy Equation (5). Therefore, those attacks on our scheme are impossible since it is difficult to obtain the proxy signature.

5 Conclusions

In this paper, we presented a cryptanalysis of Hwang-Lin-Lu scheme. We have shown that Hwang-Lin-Lu scheme is also vulnerable against the forge attack. By this attack, only the original signer can impersonate any t or more legal proxy signers in the group of n members to sign a message. And a new secure threshold proxy signature scheme was proposed to remedy the weakness of Hwang-Lin-Lu scheme. The revised scheme can withstand those attacks and anyone cannot forge the legal proxy signature.

References

[1] Dorothy E. R. Denning, *Cryptography and Data Security.* Massachusetts: Addison-Wesley, 1982.

[2] L. Harn, "Group-oriented (t, n) threshold digital signature scheme and digital multisignature," *IEE Proceedings - Computer and Digital Techniques*, vol. 141, no. 5, pp. 307–313, 1994.

[3] Chien-Lung Hsu, Tzong-Sun Wu, and Tzong-Chen Wu, "New nonrepudiable threshold proxy signature scheme with known signers," *The Journal of Systems and Software*, no. 58, pp. 119–124, 2001.

[4] M. S. Hwang, I. C. Lin, and Eric 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.

[5] Shin-Jia Hwang and Chiu-Chin Chen, "Cryptanalysis of nonrepudiable threshold proxy signature schemes with known signers," *Proceeding of* 12^{th} *National Conference on Information Security, R.O.C.*, pp. 243–246, 2002.

[6] S. Kim, S. Park, and D. Won, "Proxy signatures, revisited," *Proc. of ICICS'97, LNCS 1334*, pp. 223–232, 1997.

[7] N.Y. Lee, T. Hwang, and C.H. Wang, "On Zhang's nonrepudiable proxy signature schemes," *ACISP'98, LNCS 1438*, pp. 415–422, Jul. 1998.

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

[9] M. Mambo, K. Usuda, and E. Okamoto, "Proxy signatures for delegating signing operation," *Proc. Third ACM Conf. on Computer and Communications Security*, pp. 48–57, 1996.

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

[11] H. M. Sun, N. Y. Lee, and T. Hwang, "Threshold proxy signatures," *IEE Proc.-Computers Digital Techniques*, vol. 146, pp. 259–263, Sep. 1999.

[12] Shiang-Feng Tzeng, Chen-Ying Yang, and Min-Shiang Hwang, "A nonrepudiable threshold multi-proxy multi-signature scheme with shared verification," *Proceeding of* 12^{th} *National Conference on Information Security, R.O.C.*, pp. 285–292, 2002.

[13] K. Zhang, "Threshold proxy signature schemes," *1997 Information Security Workshop*, pp. 191–197, 1997.