On the security of some nonrepudiable threshold proxy signature schemes with known signers

Zuowen Tan, Zhuojun Liu *

Institute of Systems Science, Chinese Academy of Sciences,
State Key Laboratory of Information Security,
Graduate School of Chinese Academy of Sciences

tanzyw@163.com, zliu@mmrc.iss.ac.cn

Abstract

A (t, n) threshold proxy signature scheme enables an original signer to delegate the signature authority to a proxy group of n member such that t or more than t proxy signers can cooperatively sign messages on behalf of the original signer. In the paper, we review the security of some nonrepudiable threshold proxy signature schemes with known signers. We show that Sun's threshold proxy scheme, Yang et al.'s threshold proxy signature scheme and Tzeng et al.'s threshold proxy signature scheme are insecure against an original signer's forgery. We also show that Hsu et al.'s threshold proxy signature scheme suffers from the conspiracy of the original signer and the secret share dealer SA, and that Hwang et al.'s threshold proxy signature scheme is universally forgeable. In a word, none of the above-mentioned threshold proxy signature schemes can provide non-repudiation.
Key Words: Cryptography; Digital signature; Proxy signature; Threshold proxy signature

1 Introduction

In a proxy signature scheme, an original signer delegates a user which is called a proxy signer to sign message on its behalf. Since Mambo et al. introduced the concept of the proxy signature [12], many proxy signature schemes have been proposed [1,5,7,8,10,11,13]. According to the type of delegation, the proxy signatures are classified into three types: full delegation, partial delegation and delegation by warrant [12]. In full delegation, the original signer sends its private key as the proxy signature key to the proxy signer via a secure channel. The original signer's standard signature is indistinguishable from the proxy signature.

*Partially Supported by National Science Foundation of China(10371127)

In partial delegation, the proxy signer has a proxy signature key which is from the proxy signer's private key and a delegation key sent by the original. The delegation key is generated by the original through a trap-door permutation of the original signer's private key. The proxy signature is different from both the original's and the proxy's standard signature. In delegation by certificate, the original signer uses its standard signature algorithm to sign a warrant which records the type of the information delegated, the original signer's and the proxy signers' identities and the period of delegation, etc. The signature of the warrant is called certificate, which prevents the transfer of proxy power to a third party. Combined with delegation by certificate, the partial delegation can be changed into a partial delegation by warrant. The partial delegation by warrant can provide enough security and proper efficiency. Hereafter, for simplicity, we refer to the partial delegation by warrant as the proxy signature.

Mambo et al.'s proxy signature schemes [12] satisfy the following property: no one except the original signer and the proxy signer can create a valid proxy signature on behalf of the original signer. In 2001, J. Lee, H. Kim and K. Kim [10] improved the security property of the proxy signature: only the proxy signer can create a valid proxy signature and anyone else, even the original signer, can not generate a valid proxy signature. Thus, for a valid proxy signature, the actual proxy signer cannot deny that he/she has signed the message and the original signer cannot deny that he/she has delegated the signing authority to the actual proxy signer. That is, the proxy signature scheme holds the security property: non-repudiation.

Based on the secret sharing schemes [14,15,17] and threshold cryptosystemes [2], K. Zhang and Kim et al. independently proposed the threshold proxy signature schemes[21, 9], respectively. In a (t, n) threshold proxy signature scheme, a proxy signature key is shared among the subset of the n proxy signers such that at least t proxy signers can cooperatively sign messages on behalf of the original signer. To avoid dispute about who are the actual signers, Sun first proposed a nonrepudiable threshold proxy signature scheme with known signers (Sun's scheme [18]). Sun's scheme eliminates Kim et al.'s scheme's disadvantage that the verifier is unable to determine whether the proxy group key is generated by the legal proxy group. However, Hsu et al. [4] showed that Sun's scheme is vulnerable against the conspiracy attack: any t or more than t proxy signers can obtain the secret keys of other proxy signers. Hsu et al. still proposed a new nonrepudiable threshold proxy signature scheme with known signers (Hsu-Wu-Wu scheme [4]). In 2003, C.-Y. Yang et al. [19] made an improvement on Hsu-Wu-Wu scheme. Yang et al.'s scheme (Yang-Tzeng-Hwang scheme [20]) is

more efficient in terms of computational complexity and communication cost. In 2000, Hwang et al. proposed a nonrepudiable threshold proxy signature scheme with known signers (Hwang-Lin-Lu scheme [6]). Recently, S.-F Tzeng et al. [19] found that in Hwang-Lin-Lu scheme, a malicious original signer can forge the threshold proxy signatures without the agreement of the proxy signers. S.-F Tzeng et al. also constructed a nonrepudiable threshold proxy signature scheme with known signers (Tzeng-Hwang-Yang scheme [19]) and claimed the proposed scheme improved the security of Hwang-Lin-Lu scheme.

In this paper, we analyze the security of the above-mentioned nonrepudiable threshold proxy signature schemes with known signers. We show that Sun's scheme, Yang-Tzeng-Hwang scheme and Tzeng-Hwang-Yang scheme are all insecure against the original signer's forgery. Hsu-Wu-Wu scheme suffers from the conspiracy attack of the original signer and the secret share dealer SA. We still show that Hwang-Lin-Lu scheme is universally forgeable.

The rest of this paper is organized as follows. In Section 2, we will give some notations and recall Pedersen's threshold distributed key generation protocol [16]. In Section 3, we review the security of some threshold proxy signature schemes. Section 4 is dedicated to our conclusion.

2 Preliminaries

2.1 Notations

In the section, we give the notations which are used thorough this paper.

-p, q: two large prime numbers, $q \mid p-1$.

-g: an element of Z_p^*, its order is q.

-O: the original signer.

-$P_1, P_2, \cdots, P_n$: the n proxy signers.

-x_0: the secret key of the original signer O .

-y_0: the public key of the original signer O , $y_0 = g^{x_0} \pmod{p}$.

-x_i: the secret key of the proxy signer P_i , $i = 1, 2, \cdots, n$.

-y_i: the public key of the proxy signer P_i , $i = 1, 2, \cdots, n$, $y_i = g^{x_i} \pmod{p}$.

-$h(\cdot)$: a public cryptographically strong hash function.

-$\|$: the concatenation of strings.

-$ASID$: the actual signers' identities, sometimes we refer to it as the actual proxy signers.

-m_w: a warrant which records the type of the information delegated, the original signer's and the proxy signers' identities and the period of delegation, etc.

2.2 Pedersen's Threshold Distributed Key Generation Protocol

Pedersen's threshold distributed key generation protocol (PTDK protocol [16]) comprises n Feldman's (t, n) verifiable secret sharing schemes (Feldman VSS [3]). Assume $\{P_1, P_2, \cdots, P_n\}$ are n players. PTDK protocol contains the following three stages.

(1) Each player P_i randomly chooses a polynomial $f_i(z)$ over Z_q of degree $t-1$.

$$f_i(z) = a_{i0} + a_{i1}z + a_{i2}z^2 + \cdots + a_{i,t-1}z^{t-1}. \quad (1)$$

P_i broadcasts $g^{a_{i0}}, g^{a_{i1}}, \cdots, g^{a_{i,t-1}}$. Then P_i computes and sends $f_i(j) \pmod q$ to P_j $(j = 1, 2, \cdots, n,\ j \neq i)$ in a secure manner.

(2) Each P_j verifies the validity of the share $f_i(j) \pmod q$ by checking for $i = 1, 2, \cdots, n$:

$$g^{f_i(j)} = g^{a_{i0}}(g^{a_{i1}})^j(g^{a_{i2}})^{j^2} \cdots (g^{a_{i,t-1}})^{j^{t-1}} \pmod p.$$

If all $f_i(j)$ are verified to be legal, P_j computes $v_j = \sum_{i=1}^{n} f_i(j) \pmod q$ as his share.

(3) Let $f(z) = a_0 + a_1z + a_2z^2 + \cdots + a_{t-1}z^{t-1} \pmod q = \sum_{i=1}^{n} f_i(z) \pmod q$. In fact, $a_k = \sum_{i=1}^{n} a_{ik} \pmod q$ for $0 \leq k \leq t-1$, and $v_i = f(i) \pmod q$. So, $v = \sum_{i=1}^{n} v_i \pmod q$. If any t secret shares, say $v_1, v_2, \cdots, v_t$, are given, the shared secret key v can be reconstructed by the Lagrange interpolating polynomial:

$$v = f(0) = \sum_{i=1}^{i=t-1} s_i \cdot \prod_{j=1, j\neq i}^{t-1} \frac{(0-j)}{(i-j)} \pmod q. \quad (2)$$

The validity of the reconstructed secret key v can be verified by checking if the following equation holds:

$$g^v = \prod_{i=1}^{i=n} g^{a_{i0}} \pmod p. \quad (3)$$

3 On the Security of Some Threshold Proxy Signature Schemes

3.1 On the security of Sun's scheme

3.1.1 Sun's Scheme

We describe Sun's threshold proxy signature scheme (Sun's scheme [18]) as follows.

[**Secret Share Generation Phase**]

In the phase, the proxy group $\{P_1, P_2, \cdots, P_n\}$ needs to generate a group private/public key pair $(v, y_G) \in Z_q^* \times Z_p$. The proxy group run PTDK protocol as in Section 2. Here, each player P_i uses $f_i(z) = x_i + a_{i1}z + a_{i2}z^2 + \cdots + a_{i,t-1}z^{t-1}$. Therefore, the secret key shared by the proxy group is $v = \sum_{i=1}^{n} x_i$ and the corresponding public key is $y_G = \prod_{i=1}^{n} y_i \pmod p$. Each proxy signer P_i obtains a secret key share $v_i = f(i) = \sum_{j=1}^{n} f_j(i) \pmod q$. Let $A_j = g^{a_j} \pmod p, j = 1, 2, \cdots, t-1$.

[**Proxy Share Generation Phase**]

In the phase, the original signer O generates the proxy share as follows.

First, O randomly chooses $k \in Z_q$, and computes $K = g^k \pmod p$ and the proxy key $\sigma = x_0 h(m_w||K) + k \pmod q$. Next, O, as a dealer, distributes the proxy key σ among the proxy group by executing Feldman's VSS scheme [3]. In particular, O randomly chooses a polynomial of degree $t-1$:

$$f'(z) = \sigma + b_1 z + b_2 z^2 + \cdots + b_{t-1} z^{t-1} \pmod q.$$

O computes and secretly sends $\sigma_i = f'(i) \pmod q$ to the proxy signer P_i for $i = 1, 2, \cdots, n$. O publishes (m_w, K) and $B_j = g^{b_j}$ $(j = 1, 2, \cdots, t-1)$.

P_i accepts (σ_i, m_w, K) if the equation $g^{\sigma_i} = y_0^{h(m_w||K)} K \prod_{j=1}^{t-1} B_j^{ij} \bmod p$ holds. Then P_i computes $\sigma_i' = \sigma_i + v_i \cdot h(m_w||K) \bmod q$ as his proxy share.

[**Proxy Signature Generation Phase**]

Without loss of generality, we assume that $\{P_1, P_2, \cdots, P_t\}$ as the actual proxy group sign a message m.

First, the t proxy signers executes PTDK protocol [16] for sharing a random number $c_0 = \sum_{i=1}^{t} c_{i,0}$ by using $f_i''(z) = (c_{i,0} + x_i) + c_{i,1}z + c_{i,2}z^2 + \cdots + c_{i,t-1}z^{t-1} \pmod q$. Thus, each P_i for $i = 1, 2, \cdots, t$ obtains the public value $y = g^{c_0} \pmod p, C_j = g^{c_j} \pmod p$ and the secret random number share $v_i' = f''(i) = \sum_{i=1}^{t} x_i + c_0 + c_1 i + c_2 i^2 + \cdots + c_{t-1} i^{t-1} \pmod q$, where $c_j = \sum_{i=1}^{t} c_{ij}$ for $1 \le j \le t-1$.

Next, P_i computes his proxy signature share $s_i = v_i' y + \sigma_i' h(ASID||m) \pmod q$ and sends s_i to the proxy signers P_j $(j = 1, 2, \cdots, t, j \neq i)$ in a secure manner.

P_j can verify the validity of s_i by checking if the following equation holds:

$$g^{s_i} = \left[y \left(\prod_{j=1}^{t-1} C_j^{i^j} \right) \left(\prod_{j=1}^{t} y_j \right) \right]^y \left[\left(K y_0^{h(m_w||K)} \prod_{j=1}^{t-1} B_j^{i^j} \right) \cdot \left(y_G \prod_{j=1}^{t-1} A_j^{i^j} \right)^{h(m_w||K)} \right]^{h(ASID||m)} \mod p. \quad (4)$$

Each proxy signer in the actual proxy group can generate $s = f''(0)y + [f(0) + f'(0)]h(ASID||m)$ by the Lagrange interpolation formula to s_i. The proxy signature on m is $(m, m_w, K, ASID, y, s)$.

[Proxy Signature Verification Phase]

Any verifier can identify the original signer and the actual proxy signers from m_w and $ASID$, and validate the proxy signature by checking if

$$g^s = \left[K y_0^{h(m_w||K)} \prod_{i=1}^{n} y_i \right]^{h(ASID||m)} \left(y \prod_{i=1}^{t} y_i \right)^y \mod p. \quad (5)$$

3.1.2 Cryptanalysis of Sun's Threshold Proxy Signature Scheme

In the subsection, we show that Sun's scheme is vulnerable against the original signer's forgery. In Sun's scheme, a malicious original signer can generate a proxy signature on any message and claim that any t or more than t proxy signers are the actual proxy signers of the proxy signature. Given any message m, the original signer O randomly chooses a proxy group (thus, O chooses $ASID$). Here, we assume that O impersonates the proxy signers $\{P_1, P_2, \cdots, P_t\}$. O computes $K = (\prod_{i=1}^{n} y_i)^{-1} g^{\alpha} \mod p$, $y = (\prod_{i=1}^{t} y_i)^{-1} g^{\beta}$, where $\alpha \in_R Z_q, \beta \in_R Z_q$. Then O computes

$$s = (\alpha + x_0 h(m_w||K))h(ASID||m) + \beta y \pmod q. \quad (6)$$

Thus, $(m, m_w, K, ASID, y, s)$ is a valid proxy signature on message m. This is because:

$$\begin{aligned} g^s &= g^{(\alpha + x_0 h(m_w||K))h(ASID||m) + \beta y} \pmod p \\ &= (g^{\alpha} g^{x_0 h(m_w||K)})^{h(ASID||m)} (g^{\beta})^y \pmod p \\ &= [K y_0^{h(m_w||K)} \prod_{i=1}^{n} y_i]^{h(ASID||m)} (y \prod_{i=1}^{t} y_i)^y \pmod p. \end{aligned}$$

3.2 On the security of Hsu-Wu-Wu scheme

3.2.1 Hsu-Wu-Wu Scheme

We describe Hsu et al.'s threshold proxy signature scheme (Hsu-Wu-Wu scheme [4]) as follows.

[Secret Share Generation Phase]

In order to reduce the computation and communication cost, Hsu et al. introduce SA. SA is responsible for performing the secret share generation. SA first chooses a group private/public key pair $(v, y_G) \in Z_q^* \times Z_p$, where $y_G = g^v \pmod p$. Then, SA randomly generates a $(t-1)$-degree polynomial in $F_q[z]$:

$$f(z) = v + a_1 z + a_2 z^2 + \cdots + a_{t-1} z^{t-1} \pmod q. \tag{7}$$

SA computes and sends $v_i = f(i) \pmod q$ as P_i's secret share in a secure manner, and then publishes the corresponding value $g^{v_i} \pmod p$.

[Proxy Share Generation Phase]

The original signer O generates the proxy share in the same way as O does in Sun's scheme. O computes and sends $\sigma_i = f'(i) \pmod q$ in a secure manner to the proxy signer P_i for $i = 1, 2, \cdots, n$. Finally P_i computes $\sigma_i' = \sigma_i + v_i \cdot h(m_w||K) \pmod q$ as his proxy share.

[Proxy Signature Generation Phase]

Without loss of generality, we still assume that the actual proxy group is $\{P_1, P_2, \cdots, P_t\}$. Given any message m, the actual proxy group $\{P_1, P_2, \cdots, P_t\}$ cooperatively sign m as follows.

First, each proxy signer P_i randomly chooses $k_i \in Z_q^*$ and broadcasts $r_i = g^{k_i} \pmod p$. Then P_i computes

$$R = \prod_{j=1}^{t} r_j \pmod p, s_i = k_i R + (L_i \sigma_i' + x_i) h(R||ASID||m) \pmod q$$

where L_i is a Lagrange coefficient. P_i sends his individual proxy signature s_i to the designated clerk. If the following equation holds for $1 \le i \le t$,

$$g^{s_i} = r_i^R \left(\left((y_0 g^{v_i})^{h(m_w||K)} \left(\prod_{j=1}^{t-1} B_j^{i^j} \right) K \right)^{L_i} y_i \right)^{h(R||ASID||m)} \pmod p,$$

the designated clerk computes $s = \sum_{i=1}^{t} s_i \pmod q$. The proxy signature on m is $(m, m_w, K, ASID, R, s)$.

[Proxy Signature Verification Phase]

Any verifier can identify the original and the actual proxy signers from m_w and $ASID$, and validate the proxy signature by checking if

$$g^s = R^R \left(K(y_0 y_G)^{h(m_w||K)} \prod_{i=1}^{t} y_i \right)^{h(R||ASID||m)} \pmod p. \quad (8)$$

3.2.2 Cryptanalysis of Hsu-Wu-Wu Scheme

We show that Hsu-Wu-Wu is vulnerable against the conspiracy of the original signer and SA. A malicious original signer and SA can cooperatively generate a proxy signature on any message and claims that any t or more than t proxy signers are the actual proxy signers of the proxy signature. Given any message m, the original signer O randomly chooses $ASID$ with t or more than t proxy signers. Here, we still assume that O frames the proxy signers $\{P_1, P_2, \cdots, P_t\}$. The original signer computes $R = g^\beta$, $K = (\prod_{i=1}^{t} y_i)^{-1} g^\alpha \pmod p$, where $\alpha \in_R Z_q^*, \beta \in_R Z_q^*$. Then O computes

$$s = [\alpha + (x_0 + x_G)h(m_w||K)]h(R||ASID||m) + \beta R \pmod q. \quad (9)$$

Thus, $(m, m_w, K, ASID, R, s)$ is a valid proxy signature on message m. This is because:

$$\begin{aligned} g^s &= g^{[\alpha+(x_0+x_G)h(m_w||K)]h(R||ASID||m)+\beta R} \pmod p \\ &= (g^\beta)^R [g^\alpha (y_0 y_G)^{h(m_w||K)}]^{h(R||ASID||m)} \pmod p \\ &= R^R \left(K(y_0 y_G)^{h(m_w||K)} \prod_{i=1}^{t} y_i \right)^{h(R||ASID||m)} \pmod p. \end{aligned}$$

3.3 On the security of Yang-Tzeng-Hwang scheme

3.3.1 Yang-Tzeng-Hwang Scheme

Yang-Tzeng-Hwang scheme [20] is composed of three phases.

[Proxy Share Generation Phase]

O executes the following steps to delegate the signing capability. First, O randomly chooses $k \in Z_q$, and computes $K = g^k \pmod p$ and the proxy signature key $\sigma = x_0 h(m_w||K) + k \pmod q$. O broadcasts (σ, m_w, K) to $\{P_1, P_2, \cdots, P_n\}$.

P_i uses σ as his/her proxy share if the equation $g^{\sigma} = K y_0^{h(m_w||K)} \pmod{p}$ holds.

[Proxy Signature Generation Phase]

Without loss of generality, let $\{P_1, P_2, \cdots, P_t\}$ be the actual proxy signers.

First, each P_i randomly chooses $k_i \in Z_q^*$ and broadcasts $r_i = g^{k_i} \pmod{p}$. Then P_i computes

$$R = \prod_{j=1}^{t} r_j \pmod{p}, s_i = k_i R + (t^{-1}\sigma + x_i) h(R||ASID||m) \pmod{q}.$$

P_i sends the individual proxy signature s_i to the designated clerk. For each i, the clerk validates the individual proxy signature s_i:

$$g^{s_i} = r_i^R \left(((K y_0^{h(m_w||K)})^{t^{-1}} y_i \right)^h (R||ASID||m) \pmod{p}. \tag{10}$$

If all the individual proxy signatures s_i on message m is valid, the designated clerk computes $s = \sum_{i=1}^{t} s_i \pmod{q}$. The proxy signature on m is (m, m_w,K, $ASID$, R,s).

[Proxy Signature Verification Phase]

Any verifier can identify the original and the actual proxy signers from m_w and $ASID$, and check whether the number of the actual proxy signers is not less than the threshold value t. Finally, the verifier validates the proxy signature through the following equation.

$$g^s = R^R \left(K y_0^{h(m_w||K)} \prod_{i=1}^{t} y_i \right)^{h(R||ASID||m)} \pmod{p}. \tag{11}$$

3.3.2 Cryptanalysis of Yang-Tzeng-Hwang Scheme

In the subsection, we show that Yang-Tzeng-Hwang scheme is insecure against the original signer's forgery. Given any message m, a malicious original signer O randomly chooses a proxy group (thus, O chooses $ASID$) of not less than t proxy signers. Here, we assume that O frames the proxy signers $\{P_1, P_2, \cdots, P_t\}$. The original signer first randomly chooses $\alpha \in Z_q^*, \beta \in Z_q^*$ and computes $K = (\prod_{i=1}^{t} y_i)^{-1} \cdot g^{\alpha} \pmod{p}$, $R = g^{\beta} \pmod{p}$. Then O computes

$$s = (\alpha + x_0 h(m_w||K)) h(R||ASID||m) + \beta R \pmod{q}. \tag{12}$$

Thus, $(m, m_w, K, ASID, R, s)$ is a valid proxy signature on message m. This is because:

$$\begin{aligned} g^s &= g^{(\alpha+x_0h(m_w||K))h(R||ASID||m)+\beta R} \mod p \\ &= g^{\beta R}(g^{\alpha}g^{x_0h(m_w||K)})^{h(R||ASID||m)} \mod p \\ &= R^R(Ky_0^{h(m_w||K)}\prod_{i=1}^{t} y_i)^{h(R||ASID||m)} \mod p. \end{aligned}$$

3.4 On the security of Hwang-Lin-Lu scheme

3.4.1 Hwang-Lin-Lu Scheme

Hwang-Lin-Lu scheme [6] is nearly the same as Sun's threshold proxy signature scheme [18].

[Secret Share Generation Phase]

In the phase, the proxy group generates a group private/public key pair $(v, y_G) \in Z_q \times Z_p$ as the group does in Sun's scheme. Here, each P_i uses $f_i(z) = x_i + a_{i0} + a_{i1}z + a_{i2}z^2 + \cdots + a_{i,t-1}z^{t-1}$. The secret key shared by the proxy group is $v = \sum_{i=1}^{n} x_i$ and the corresponding public key is $y_G = \prod_{i=1}^{n} y_i \pmod p$. Each proxy signer P_i obtains a secret key share $v_i = f(i) = \sum_{j=1}^{n} f_j(i) \pmod q$. The group publishes $A_j = g^{a_j} \pmod p, j = 0, 1, 2, \cdots, t-1$.

[Proxy Share Generation Phase]

In the phase, the original signer O generates the proxy share as O does in Sun's scheme. O first generates the proxy key $\sigma = h(m_w||K)x_0 + k \pmod q$. Then O distributes the proxy key σ among the proxy group by executing Feldman's VSS scheme as follows. O randomly chooses a polynomial of degree $t-1$:

$$f'(z) = \sigma + b_1 z + b_2 z^2 + \cdots + b_{t-1}z^{t-1} \pmod q.$$

O computes and secretly sends $\sigma_i = f'(i) \pmod q$ to P_i for $i = 1, 2, \cdots, n$. O publishes (m_w, K) and $B_j = g^{b_j} \pmod p$ for $j = 1, 2, \cdots, t-1$.

P_i accepts (σ_i, m_w, K) if the equation holds.

$$g^{\sigma_i} = y_0^{h(m_w||K)} K \prod_{j=1}^{t-1} B_j^{i^j} \pmod p.$$

Then P_i computes $\sigma_i' = \sigma_i + v_i \cdot h(m_w||K) \pmod q$ as his proxy share.

[Proxy Signature Generation Phase]

We assume that $\{P_1, P_2, \cdots, P_t\}$ are the actual proxy group. P_i first generates the secret random share v_i' as P_i does in Sun's scheme. Then P_i computes the individual proxy signature $s_i = v_i' y + \sigma_i' h(ASID||m) \pmod q$ and sends s_i to the proxy signers P_j $(j = 1, 2, \cdots, t, j \neq i)$ in a secure manner. P_j can verify the validity of s_i by checking if the following equation holds:

$$\begin{aligned} g^{s_i} &= \left[y \left(\prod_{j=1}^{t-1} C_j^{i^j} \right) \left(\prod_{j=1}^{t} y_j \right) \right]^y \left[\left(K y_0^{h(m_w||K)} \prod_{j=1}^{t-1} B_j^{i^j} \right) \right. \\ &\quad \left. \cdot \left(y_G A_0 \prod_{j=1}^{t-1} A_j^{i^j} \right)^{h(m_w||K)} \right]^{h(ASID||m)} \quad \bmod p. \end{aligned} \tag{13}$$

By the Lagrange interpolation formula to s_i, each signer in the actual proxy group can generate

$$s = f''(0)y + [f(0) + f'(0)]h(ASID||m).$$

The proxy signature on m is $(m, m_w, K, ASID, y, A_0, s)$.

[Proxy Signature Verification Phase]

Any verifier can identify the original signer and the actual proxy signers from m_w and $ASID$, and check the validity of the proxy signature from the equation:

$$g^s = \left[K A_0 y_0^{h(m_w||K)} \prod_{i=1}^{n} y_i \right]^{h(ASID||m)} \left(y \prod_{i=1}^{t} y_i \right)^y \bmod p. \tag{14}$$

If the equation holds, the proxy signature $(m, m_w, K, ASID, y, A_0, s)$ is valid.

3.4.2 Cryptanalysis of Hwang-Lin-Lu Scheme

In the subsection, we show that Hwang-Lin-Lu scheme is insecure against universally forgery. Any adversary can impersonate any original signer and any t or more than t proxy signers to forge a proxy signature on any message. Given any message, any original signer, and any proxy group $\{P_1, P_2, \cdots, P_n\}$, the adversary chooses $\{P_1, P_2, \cdots, P_t\}$ as the actual proxy signers. The adversary chooses four random numbers $\alpha \in Z_q^*$, $\beta \in Z_q^*$, $\gamma \in Z_q^*$ and $y \in Z_p^*$. Then the adversary computes

$$K = (\prod_{i=1}^{n} y_i)^{-1} g^{\alpha} \pmod p, A_0 = (y_0^{h(m_{w||K})})^{-1} g^{\beta} \pmod p \tag{15}$$

$$s = (\alpha + \beta)h(ASID||m) + \gamma y \pmod q. \tag{16}$$

Thus, $(m, m_w, K, ASID, y, A_0, s)$ is a valid proxy signature on message m. This is because it satisfies the following verification equation:

$$\begin{aligned} g^s &= g^{(\alpha+\beta)h(ASID||m)+\gamma y} \pmod{p} \\ &= \left(g^{\alpha} g^{\beta}\right)^{h(ASID||m)} g^{\gamma y} \pmod{p} \\ &= \left[K A_0 y_0^{h(m_w||K)} \prod_{i=1}^{n} y_i\right]^{h(ASID||m)} \left(y \prod_{i=1}^{t} y_i\right)^{y} \pmod{p}. \end{aligned}$$

3.5 On the security of Tzeng-Hwang-Yang scheme

3.5.1 Tzeng-Hwang-Yang Scheme

Tzeng et al. [19] made some modifications on the Hwang-Lin-Lu scheme [6].

[Secret Share Generation Phase]

In the phase, Tzeng et al. replace $f_i(z)$ with $f_i(z) = x_i y_i + a_{i0} A_0 + a_{i1} z + a_{i2} z^2 + \cdots + a_{i,t-1} z^{t-1}$. Therefore, each proxy signer P_i obtains a secret key share $v_i = f(i) = \sum_{j=1}^{n} x_j y_j + a_0 A_0 + a_1 i + \cdots + a_{t-1} i^{t-1} \pmod{q}$, where $a_i = \sum_{j=1}^{n} a_{ji} \pmod{q}$. The proxy group publishes $y_G = \prod_{i=1}^{n} y_i^{y_i} \pmod{p}$ and $A_j = g^{a_j} \pmod{p}, (j = 0, 1, 2, \cdots, t-1)$. The other steps of the phase is the same as that of Hwang-Lin-Lu scheme.

Note: It seems complicated for each proxy signer to choose the proper $f_i(z)$ such that $a_0 = \sum_{j=1}^{n} a_{j0} \pmod{q}$ and $A_0 = g^{a_0} \pmod{p}$. It also seems complicated for each proxy signer to choose the proper $f_i''(z)$ during the following proxy signature generation phase.

[Proxy Share Generation Phase]

The proxy share phase is the same as that of Hwang-Lin-Lu scheme.

[Proxy Signature Generation Phase]

Without loss of generality, let $\{P_1, P_2, \cdots, P_t\}$ be the actual proxy group. First, P_i randomly chooses $f_i''(z) = x_i y_i + c_{i0} C_0 + c_{i1} z + \cdots + c_{i,t-1} z^{t-1} \pmod{q}$ instead of $f_i''(z) = x_i + c_{i0} + c_{i1} z + \cdots + c_{i,t-1} z^{t-1} \pmod{q}$. Thus, P_i's random number share is

$$v_i' = f''(i) = \sum_{j=1}^{t} x_i y_i + c_0 C_0 + c_1 i + \cdots + c_{t-1} i^{t-1} \pmod{q},$$

where $c_i = \sum_{j=1}^{t} c_{ji} \pmod q$. P_i then computes the individual proxy signature $s_i = v_i' y + \sigma_i' h(ASID||m) \pmod q$ and sends s_i to P_j $(j \neq i)$ in a secure manner. P_j can verify the validity of s_i from the following equation:

$$\begin{aligned} g^{s_i} &= \left[y^y \left(\prod_{i=1}^{t-1} C_i^{j^i} \right) \left(\prod_{i=1}^{t} y_i^{y_i} \right) \right]^y \left[\left(K y_0^{h(m_w||K)} \prod_{i=1}^{t-1} B_i^{j^i} \right) \right. \\ &\quad \left. \cdot \left(y_G A_0^{A_0} \prod_{i=1}^{t-1} A_i^{j^i} \right)^{h(m_w||K)} \right]^{h(ASID||m)} \quad \bmod p. \end{aligned} \tag{17}$$

Each proxy signer in the actual proxy group can generate $s = f''(0)y + [f(0) + f'(0)]h(ASID||m)$ by Lagrange formula. The proxy signature on m is $(m, m_w, K, ASID, y, A_0, s)$.

[Proxy Signature Verification Phase]

Any verifier can check the validity of the proxy signature $(m, m_w, K, ASID, y, A_0, s)$ from the equation:

$$g^s = \left[K A_0^{A_0} y_0^{h(m_w||K)} \prod_{i=1}^{n} y_i^{y_i} \right]^{h(ASID||m)} \left(y^y \prod_{i=1}^{t} y_i \right)^y \bmod p. \tag{18}$$

3.5.2 Cryptanalysis of Tzeng-Hwang-Yang Scheme

In the subsection, we show that Tzeng-Hwang-Yang scheme is insecure against the original signer's forgery. After a malicious original signer obtains the proxy signature $(m, m_w, K, ASID, y, A_0, s)$ on message m, O can generate another proxy signature $(m, m_w, K', ASID, y, A_0', s')$ without the agreement of the proxy group $ASID$. First, O randomly chooses A' in Z_p, and computes

$$K' = K A_0^{A_0} (A_0')^{-A_0'} \pmod p, \tag{19}$$

$$s' = s - x_0(h(m_w||K) - h(m_w||K'))h(ASID||m). \tag{20}$$

Then $(m, m_w, K', ASID, y, A_0', s')$ is a valid proxy signature on message m. This is because:

$$\begin{aligned} g^{s'} &= g^s y_0^{(h(m_w||K') - h(m_w||K))h(ASID||m)} \bmod p \\ &= \left[K A_0^{A_0} y_0^{h(m_w||K)} \prod_{i=1}^{n} y_i^{y_i} \right]^{h(ASID||m)} \left(y^y \prod_{i=1}^{t} y_i \right)^y \\ &\quad \cdot y_0^{(h(m_w||K') - h(m_w||K))h(ASID||m)} \bmod p \\ &= \left[K' (A_0')^{A_0'} y_0^{h(m_w||K')} \prod_{i=1}^{n} y_i^{y_i} \right]^{h(ASID||m)} \left(y^y \prod_{i=1}^{t} y_i \right)^y \bmod p. \end{aligned}$$

4 Conclusions

In the paper, we analyze the security of some nonrepudiable threshold proxy signature schemes with known signers. We find that in Sun's scheme and Yang-Tzeng-Hwang scheme, a malicious original signer can forge a valid proxy signature on any message without the agreement of the proxy group. Hsu-Wu-Wu scheme is insecure against the conspiracy of the original signer and the secret share dealer SA. In addition, we show that Hwang-Lin-Lu scheme is universally forgeable. As for Tzeng-Hwang-Yang scheme, a malicious original signer can generate another proxy signature on the same message without the same proxy group after the proxy group sign message on behalf of the original signer.

References

[1] A.Boldyreva, A. Palacio, B. Warinschi, "Secure Proxy Signature Schemes for Delegation of Signing Rights" Available at http://eprint.iacr.org/2003/096.

[2] Y. Desmedt and Y. Frankel, "Threshold Cryptosystems", *Proc. Advance in Cryptology CRYPTO'89*, LNCS 435, Springer-Verlag, pp. 307-315, 1989.

[3] P. Feldman, "A Practical Scheme for Non–Interactive Verifiable Secret Sharing", *Proc. 28th FOCS*, IEEE, pp. 427-437, 1987.

[4] C.-L. Hsu, T.-S. Wu, and T.-C. Wu, "New nonrepudiable threshold proxy signature schemem with known signers," The Journal of Systems and Software 58(2001), pp. 119-124, 2001.

[5] S. J. Hwang and C. C. Chen, "A new proxy multi-signature scheme," *International workshop on cryptology and network security*, Tamkang University, Taipei, Taiwan, Sep. 26-28, 2001.

[6] M.-S. Hwang, I.-C. Lin and K.-F. Lu, "A secure nonrepudiable threshold proxy signature scheme with known signers," International Journal of Informatica 11(2), pp.1-8, 2000.

[7] S. J. Hwang and C. H. Shi, "A simple multi-proxy signature scheme," *Proceedings of the Tenth National Conference on Information Security*, pp. 134-138, 2000.

[8] H. Kim, J. Baek, B. Lee, and K. Kim, "Secrets for mobile agent using one-time proxy signature," Cryptography and Information Security 2001, Vol 2/2, pp. 845-850, 2001.

[9] S. J. Kim, S. J. Park, D. H. Won, "Proxy Signatures, revisited." *ICICS'97*, LNCS 1334, Springer-Verlag pp. 223-232, 1997.

[10] B. Lee, H. Kim, and K. Kim, "Strong proxy signgture and its applications," *Proceedings of SCIS*, 2001, pp. 603-608, 2001.

[11] B. Lee, H. Kim, and K. Kim, "Secure mobile agent using strong non-designated proxy signature," *Proc. ACISP* 2001, pp. 474-486, 2001.

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

[13] H.-U. Park and L.-Y. Lee, "A digital nominative proxy signature scheme for mobile communications," ICICS 2001, LNCS 2229, Springer-Verlag, pp. 451-455, 2001.

[14] T. P. Pedersen, "Non-interactive and information-theoretic secure verifiable secret sharing," *Proc. Advance in Cryptology CRYPTO'91*, Springer-Verlag, pp. 129-140, 1991.

[15] T. P. Pedersen. "Distributed Provers with Applications to Undeniable Signatures". *Proc. Advance in Cryptology-EUROCRYPTO'91*, LNCS 547, Springer-Verlag, pp. 221-242, 1991.

[16] T. P. Pedersen. "A Threshold Cryptosystem without a Trusted Party," *Proc. Advance in Cryptology-EUROCRYPTO'91*, LNCS 547, Springer-Verlag, pp. 522-526, 1991.

[17] A. Shamir, "How to Share a Secret," *Communications of the ACM*, vol. 22, No. 11, pp. 612-613, 1979.

[18] H. M. Sun, "An efficient nonrepudiable threshold proxy signatures with known signers," *Computer Communications* 22(8),1999, pp. 717-722.

[19] S.-F. Tzeng, M.-S. Hwang, and C.-Y. Yang, "An improvement of nonrepudiable threshold proxy signature schemem with known signers," *Computers & Security* 23,2004, pp. 174-178.

[20] C.-Y. Yang, S.-F. Tzeng and M.-S. Hwang, " On the efficiency of nonrepudiable threshold proxy signatures with known signers," *The Journal of Systems and Software* 22(9),2003, pp. 1-8.

[21] K. Zhang, "Threshold proxy signature schemes," *Information Security Workshop* , Japan, 1997, pp. 191-197.