Cryptanalysis of Nonrepudiable Threshold Proxy Signature Schemes with Known Signers

Shin-Jia HWANG

Department of Computer Science and Information Engineering, TamKang University
Tamsui, Taipei Hsien, 251, Taiwan, ROC
e-mail: sjhwang@mail.tku.edu.tw

Chiu-Chin CHEN

Department of Information Management, Chaoyang University of Technology
Wufeng, Taichung Country, 413, Taiwan, ROC
e-mail: s8914604@mail.cyut.edu.tw

Received: November 2002

Abstract. Sun's nonrepudiation threshold proxy signature scheme is not secure against the collusion attack. In order to guard against the attack, Hwang *et al.* proposed another threshold proxy signature scheme. However, a new attack is proposed to work on both Hwang *et al.*'s and Sun's schemes. By executing this attack, one proxy signer and the original signer can forge any valid proxy signature. Therefore, both Hwang *et al.*'s scheme and Sun's scheme were insecure.

Key words: digital signature, proxy signature, threshold proxy signature.

1. Introduction

Mambo *et al.* (1996a; 1996b) first proposed the proxy signature schemes. In proxy signature schemes, a proxy signer can generate proxy signatures on behalf of an original signer. For the group-oriented applications, the threshold proxy signature scheme is proposed. In (t, n) threshold proxy signature schemes, the original signer authorizes a proxy signer group consisting of n proxy signers. Only any t or more members in the proxy signer group can generate the proxy signatures on behalf of the original signer. Sun (1999) proposed his efficient nonrepudiable threshold proxy signature scheme with known signers. However, Hwang *et al.* (2000) point out that Sun's scheme is vulnerable against their collusion attack. In the collusion attack, any $n-1$ proxy signers are able to cooperatively obtain the secret key of the remainder proxy signer. To overcome this secure problem, they also proposed their improved scheme (Hwang *et al.*, 2000).

However, a new attack is proposed to show that, both in Hwang *et al.*'s and Sun's schemes, valid proxy signatures can be forged successfully by the original signer and only one proxy signer. In the next section, the review of Hwang *et al.*'s and Sun's schemes is given. Our new attack is proposed in Section 3. Finally, Section 4 is our discussions and conclusion.

2. Review of Nonrepudiable Threshold Proxy Signature Schemes with Known Signers

In Hwang *et al.*'s scheme, there are three phases: Proxy share generation phase, proxy signature issuing without revealing proxy shares phase, and verification of the proxy signature phase. The system parameters of Hwang *et al.*'s scheme are given now. There are two prime numbers p and q such that $q \mid (p-1)$. The parameter g is the generator of order q in Z_p^*. The original signer P_0 has his secret key x_0 and his certificated public key $y_0 = g^{x_0} \bmod p$. The proxy signers $P_1, P_2, \ldots, P_n$ have their secret key x_i and their certificated public key $y_i = g^{x_i} \bmod p$, for $i = 1, 2, \ldots, n$. The h is one-way hash function. The m_w is a warrant that at least records the authorization details about the identities of the original signer and the proxy signers of the proxy group. The ASID (Actual Signer's ID) records the actual signers' identities of messages.

Proxy Share Generation Phase

In this phase, all of the proxy signers, $P_1, P_2, \ldots$, and P_n, generate their individual proxy secret keys, $\delta_1', \delta_2', \ldots, \delta_n'$, by the following steps.

Step 1: Each proxy signer P_i selects a secret $t-1$ degree polynomial $f_i(x) = x_i + a_{(i,0)} + a_{(i,1)}x + \cdots + a_{(i,t-1)}x^{t-1} \bmod q$, where $a_{(i,u)}$'s are random integers selected form Z_q^*. Then P_i sends $f_i(j)$ to P_j by secret channels for $j = 1, 2, \ldots, n$, and $j \neq i$, and then he broadcasts $A_{(i,u)} = g^{a_{(i,u)}} \bmod q$, for $u = 0, 1, \ldots, t-1$.

Step 2: Each proxy signer P_i verifies the received $f_j(i)$ by the equation $g^{f_j(i)} \equiv y_j \times A_{(j,0)} \times (A_{(j,1)})^i \times \ldots \times (A_{(j,t-1)})^{i^{t-1}} (\bmod p)$, for $j = 1, 2, \ldots, n$, and $j \neq i$. Once all of the equations hold, P_i computes $s_i \equiv f(i) \equiv f_1(i) + f_2(i) + \cdots + f_n(i) \equiv \sum_{j=1}^{n} x_j + a_0 + a_1 i + \cdots + a_{t-1} i^{t-1} (\bmod q)$, where $a_u = \sum_{j=1}^{n} a_{(j,u)} \bmod q$, for $u = 0, 1, \ldots, t-1$.

Step 3: The proxy group public parameters are $y_G \equiv \prod_{i=1}^{n} g^{x_i} \equiv \prod_{i=1}^{n} y_i (\bmod p)$ and $A_u = g^{a_u} \bmod p$ for $u = 0, 1, \ldots, t-1$.

Step 4: The original signer P_0 selects a random number k form Z_q^* and computes $K = g^k \bmod p$. Then he computes $e = h(m_w, K)$ and $\delta = x_0 e + k \bmod q$.

Step 5: To share the proxy key δ among the n proxy signers, the original signer P_0 constructs a secret polynomial $f'(z) = \delta + b_1 z + \cdots + b_{t-1} z^{t-1} \bmod q$, where b_u's are random integers selected form Z_q^*. P_0 computes $\delta_i \equiv f'(i) \equiv \delta + b_1 i + \cdots + b_{t-1} i^{t-1} (\bmod q)$ for $i = 1, 2, \ldots, n$. Then P_0 sends δ_i to the proxy signer P_i through secret channels, for $i = 1, 2, \ldots, n$. P_0 also broadcasts $B_u = g^{b_u} \bmod p$ for $u = 1, 2, \ldots, t-1$.

Step 6: Each P_i verifies δ_i by the equation $g^{\delta_i} \equiv y_0^{h(m_w,K)} K \prod_{j=1}^{t-1} B_j^{i^j} (\bmod p)$. Once the equation holds, P_i computes his proxy secret key δ_i' by $\delta_i' = \delta_i + s_i h(m_w, K) \bmod q$, for $i = 1, 2, \ldots, n$.

Proxy Signature Issuing without Revealing Proxy Shares Phase

Without losing generality, suppose that $P_1, P_2, \ldots, P_t$ want to sign a message m on behalf of the original signer P_0.

Step 7: Each proxy signer P_i selects a secret polynomial $f_i''(x) = (x_i + c_{(i;0)}) + c_{(i,1)}x + \cdots + c_{(i,t-1)}x^{t-1} (\operatorname{mod} q)$, where $c_{(i,u)}$'s are random integers from Z_q^*. Then P_i sends $f_i''(j) \operatorname{mod} q$ to P_j in a secret channel for $j = 1, 2, \ldots, t$, and $j \neq i$. He also broadcasts $C_{(i,u)} = g^{c_{(i,u)}}$ for $u = 0, 1, \ldots, t-1$.

Step 8: Each P_i verifies the received $f_j''(i)$ from the other $t-1$ proxy signers by the equation $g^{f_j''(i)} \equiv y_j \times C_{(j,0)} \times (C_{(j,1)})^i \times \ldots \times (C_{(j,t-1)})^{i^{t-1}} (\operatorname{mod} p)$ for $j \neq i$. If all of the equations hold, P_i computes $s_i' \equiv f''(i) \equiv f_1''(i) + f_2''(i) + \cdots + f_t''(i) \equiv \sum_{j=1}^{t} x_j + c_0 + c_1 i + \cdots + c_{t-1} i^{t-1} (\operatorname{mod} q)$, where $c_u = \sum_{j=1}^{t} c_{(j,u)} \operatorname{mod} q$ for $u = 0, 1, \ldots, t-1$.

Step 9: The proxy signers $P_1, P_2, \ldots, P_t$ publish parameters $Y = g^{c_0} \operatorname{mod} p$ and $C_u = g^{c_u} \operatorname{mod} p$ for $u = 1, 2, \ldots, t-1$.

Step 10: Each P_i computes $\gamma_i = s_i' Y + \delta_i' h(ASID, m) \operatorname{mod} q$ and sends γ_i to P_j for $j = 1, 2, \ldots, t$, and $j \neq i$.

Step 11: Each P_i verifies γ_i by $g^{\gamma_j} \equiv \Big[\big(\prod_{i=1}^{t} y_i\big) Y \big(\prod_{i=1}^{t-1} C_i^{j^i}\big)\Big]^Y \times \Big[\big(y_0^{h(m_w,K)} K \prod_{i=1}^{t-1} B_i^{j^i}\big)\big(y_G \prod_{i=0}^{t-1} A_i^{j^i}\big)^{h(m_w,K)}\Big]^{h(ASID,m)} (\operatorname{mod} p)$ for $j = 1, 2, \ldots, t$, and $j \neq i$. Once all of the equations hold, P_i applies the Lagrange formula to γ_i to compute $T = f''(0)Y + [f(0) + f'(0)]h(ASID, m) \operatorname{mod} q$. Finally, the threshold proxy signature on m is $(m, T, K, Y, A_0, m_w, ASID)$.

Verification of the Proxy Signature

To verify the threshold proxy signature $(m, T, K, Y, A_0, m_w, ASID)$, the verifier first obtained the certificated public keys of the proxy signers according to the warrant m_w and $ASID$. Then he checks the proxy signature by $g^T \equiv \big[y_0^{h(m_w,K)} \times K \times A_0 \times \prod_{i=1}^{n} y_i\big]^{h(ASID,m)} \big(Y \times \prod_{i=1}^{t} y_i\big)^Y (\operatorname{mod} p)$.

Since Hwang *et al.*'s scheme is the improvement on Sun's scheme, Sun's scheme is also a variant of Hwang *et al.*'s scheme with $A_0 = 1$ for $a_{(1,0)} = a_{(2,0)} = \ldots = a_{(n,0)} = 0$ and $a_0 \equiv \sum_{j=1}^{n} a_{(j,0)} \equiv 0 (\operatorname{mod} q)$. The signature generation equation is still $T = f''(0)Y + [f(0) + f'(0)]h(ASID, m) \operatorname{mod} q$. In Sun's scheme, the proxy signature is $(m, T, K, Y, A_0, m_w, ASID) = (m, T, K, Y, 1, m_w, ASID)$ while the verification equation is $g^T \equiv \big[y_0^{h(m_w,K)} \times K \times A_0 \times \prod_{i=1}^{n} y_i\big]^{h(ASID,m)} \big(Y \times \prod_{i=1}^{t} y_i\big)^Y \equiv \big[y_0^{h(m_w,K)} \times K \times 1 \times \prod_{i=1}^{n} y_i\big]^{h(ASID,m)} \big(Y \times \prod_{i=1}^{t} y_i\big)^Y (\operatorname{mod} p)$. In (Hwang *et al.*, 2000), the authors intended to use the n random integers $a_{(1,0)}, a_{(2,0)}, \ldots$, and $a_{(n,0)}$, to overcome the weakness of Sun's scheme. However, an attack is proposed to show that it is useless.

3. An Insider Attack on Hwang *et al.*'s Scheme

Being inspired of the insider attack in (Li *et al.*, 2000), a new attack is proposed on Hwang *et al.*'s scheme. This attack needs the cooperation of one malicious proxy signer and the original signer. They want to forge threshold proxy signatures without the agreement of the other proxy signers. Without losing generality, assume that the malicious proxy signer is P_1.

To perform this new attack, after the other $n-1$ proxy signers publishing their certificated public keys $y_2, y_3, \ldots, y_n$, the malicious proxy signer P_1 selects a random integer α form Z_q^* and computes $y_1' = g^\alpha \times (y_2 \times y_3 \times \ldots \times y_n)^{-1} (\bmod p)$ as his certificated public key. Then the original signer gives P_1 the proxy secret key $\delta = x_0 e + k \bmod q$ and $K = g^k \bmod p$, where k is a random integer chosen by the original signer.

Without losing generality, suppose that P_1 wants to forge a proxy signature on a message m without the cooperation of the other $t-1$ proxy signers P_2, $P_3, \ldots, P_t$. So ASID records the identifies of $P_1, P_2, \ldots, P_t$. Then P_1 first selects a random integer $\beta \in Z_q^*$ computes $A_0 = g^\beta \bmod p$. He also computes $Y = (y_{t+1} \times y_{t+2} \times \ldots \times y_n) \bmod p$ and $T = \alpha Y + (\alpha + \beta + \delta) h(ASID, m) \bmod q$. Finally, P_1 forges 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.

$$
\begin{aligned}
&\left[y_0^{h(m_w,K)} \times K \times A_0 \times \prod_{i=1}^{n} y_i \right]^{h(ASID,m)} \left(Y \times \prod_{i=1}^{t} y_i \right)^{Y} \\
&\equiv \left[y_0^{h(m_w,K)} \times g^k \times g^\beta \times \left(g^\alpha \times (y_2 \times y_3 \times \ldots \times y_n)^{-1} \right) \right. \\
&\qquad \left. \times y_2 \times y_3 \times \ldots \times y_n \right]^{h(ASID,m)} \times \left(Y \times \prod_{i=1}^{t} y_i \right)^{Y} \\
&\equiv \left[g^{x_0(m_w,K)+k} \times g^\beta \times g^\alpha \right]^{h(ASID,m)} \times \left(Y \times \prod_{i=1}^{t} y_i \right)^{Y} \\
&\equiv \left[g^\delta \times g^\beta \times g^\alpha \right]^{h(ASID,m)} \times \left(Y \times \prod_{i=1}^{t} y_i \right)^{Y} \\
&\equiv \left[g^\delta \times g^\beta \times g^\alpha \right]^{h(ASID,m)} \Big[(y_{t+1} \times y_{t+2} \times \ldots \times y_n) \\
&\qquad \times \left(g^\alpha \times (y_2 \times y_3 \times \ldots \times y_n)^{-1} \right) \times (y_2 \times y_3 \times \ldots \times y_t) \Big]^{Y} \\
&\equiv \left[g^\delta \times g^\beta \times g^\alpha \right]^{h(ASID,m)} \times (g^\alpha)^{Y} \\
&\equiv g^{(\alpha+\beta+\delta)h(ASID,m)+\alpha Y} \equiv g^{T} (\bmod p).
\end{aligned}
$$

The threshold proxy signature is forged successfully for Hwang *et al.*'s scheme. Further, by this attack with $\beta = 0$ and $A_0 = 1$, the threshold proxy signature $(m, T, K, Y, 1, m_w, ASID)$ is also forged for Sun's scheme (Sun, 1999).

In the following, an example illustrates our insider attack on Hwang *et al.*'s scheme below. Suppose that the proxy signers $(P_1, P_2, P_3, P_4, P_5)$ are authorized to act for the original signer P_0 while at least three proxy signers have to generate the proxy signatures. We assume that the malicious proxy signer P_1 and the original signer P_0 want to forge threshold proxy signatures without the agreement of the other proxy signers. The system parameters and secret and public keys of signers are show in Tables 1 and 2.

After the other 4 proxy signers publishing their certificated public key 18, 12, 16, 4, the malicious proxy signer P_1 selects a random integer $\alpha = 2$ and computes $y'_1 \equiv 3^2 \times (18 \times 12 \times 16 \times 4)^{-1} = 9 (\bmod 23)$ as his public key. The original signer P_0 gives P_1 the proxy secret key $\delta \equiv x_0 e + k \equiv 5 \times 10 + 8 \equiv 3 (\bmod 11)$ and $K \equiv 3^8 \equiv 6 (\bmod 23)$, where $k = 8$. Without losing generality, suppose that P_1 wants to forge a proxy signature on a message m without the cooperation of the other 2 proxy signers P_2, P_3. The ASID records the identities of the proxy signers: P_1, P_2, P_3. Then P_1 first selects a random integer $\beta = 5$ and computes $A_0 \equiv 3^5 \equiv 13 (\bmod 23)$. He also computes $Y \equiv (y_4 \times y_5) \equiv 16 \times 4 \equiv 18 (\bmod 23)$ and $T \equiv \alpha Y + (\alpha + \beta + \delta) h(ASID, m) \equiv 2 \times 18 + (2 + 5 + 3) \times 8 \equiv 6 (\bmod 11)$. Finally, P_1 forges a valid proxy signature $(m, T, K, Y, A_0, m_w, ASID) = (m, 6, 6, 18, 13, m_w, ASID)$. To verify the proxy signature $(m, 6, 6, 18, 13, m_w, ASID)$, the verifier first computes $e = h(m_w, K) = 10$ and $h(ASID, m) = 8$. Then $g^T \equiv 3^6 \equiv 16 (\bmod 23)$ and $\left[y_0^{h(m_w,K)} \times K \times A_0 \times \prod_{i=1}^{n} y_i\right]^{h(ASID,m)} (Y \times \prod_{i=1}^{t} y_i)^Y \equiv [13^{10} \times 6 \times 13 \times (9 \times 18 \times 12 \times 16 \times 4)]^8 \times (18 \times (9 \times 18 \times 12))^{18} \equiv 16 (\bmod 23)$. The both sides of the verification equation obtain the same value. Therefore, the proxy signature is forged.

Table 1

System public parameters and functions' values

Parameters	Values
p	23
q	11
g	3
$e = h(m_w, K)$	10
$h(ASID, m)$	8

Table 2

Public and secret keys of original and proxy signers

Key \ Signer	P_0	P_2	P_3	P_4	P_5
Secret key x	5	9	4	6	3
Public key y	13	18	12	16	4

4. Discussions and Conclusions

Between our insider attack and Hwang *et al.*'s collusion attack, there exists some differences. The goals of these attacks are different. The goal of the collusion attack is to obtain the secret key of some proxy signer. The goal of our insider attack is to forge valid threshold proxy signatures. The participators are also different. In the collusion attack, the participators are $(n-1)$ proxy signers who collude to perform the collusion attack. In our insider attack, the participators are only one proxy signer and original signer who cooperatively forge valid proxy signatures.

Besides these differences, our new attack can work on both Hwang *et al.*'s and Sun's schemes while the collusion attack only works on Sun's scheme. In 2000, Hwang *et al.* show Sun's scheme (Sun, 1999) is vulnerable against the collusion attack. They tried to propose an improvement to overcome the security problem. However, a new attack is proposed to show that not only Hwang *et al.*'s but also Sun's schemes are insecure. The new attack is more powerful than the collusion attack.

References

Hwang, M.-Sh., I.-C. Lin and E.J.-L. Lu (2000). A secure nonrepudiable threshold proxy signature scheme with known signers. *Informatica*, **11**(2), 137–144.

Li, Z.C., L.C.K. Hui, K.P. Chow, C.F. Chong, H.H. Tsang and H.W. Chan (2000). Cryptanalysis of harn digital multisignature scheme with distinguished signing authorities. *Electronics Letters*, **36**(4), 314–315.

Mambo, M., K. Usuda and E. Okamoto (1996a). Proxy signatures: delegation of the power to sign message. *IEICE. Trans. Fundamentals*, **E79-A**(9), 1338–1354.

Mambo, M., K. Usuda and E. Okamoto (1996b). Proxy signatures for delegation signing operation. In *Proc. 3nd ACM Conference on Computer and Communication Security*. pp. 48–57.

Sun, H.-M. (1999). An efficient nonrepudiable threshold proxy signature scheme with known signers. *Computer Communications*, 717–722.

Sh.-J. Hwang is an associate professor of Department of Computer Science and Information Engineering, Tankang University, Tamsui, Taipei, Taiwan. During the academic years of 1996–2001, he was on the faculty of the Department of Information Management at Chaoyang University of Technology, WuFeng, Taichung Country, Taiwan. He received his BS degree in information and computer engineering from Chung–Yuan Christian University, Chungli, Taiwan in 1987 and his MS degree in computer science and information engineering from National Chung Cheng University, Chiayi, Taiwan in 1992. He received his PhD degree in computer and information science form National Chaio Tung University, Hsinchu, Taiwan. His research interests include cryptography and computer security.

Ch.-Ch. Chen is working on Benq company in Taiwan. She received the BS degree in information management from Kun Shan University of Technology, Tainan, Taiwan, Republic of China, in 2000. She received her MS degree in information management from Chaoyang University of Technology, WuFeng, Taichung Country, Taiwan, in 2002. Her current research interests include cryptography and data security.

Neišsižadamo slenkstinio atstovaujančiojo asmens parašo schemos su žinomais pasirašančiaisiais asmenimis kriptoanalizė

Shin-Jia HWANG, Chiu-Chin CHEN

Sun neišsižadamo slenkstinio atstovaujančiojo asmens parašo schema yra nesaugi prieš suokalbio ataką. Kad apsisaugoti nuo šios atakos, Hwang *et al.* pasiūlė kitą slenkstinio atstovaujančiojo asmens parašo schemą. Mes siūlome naują ataką, kuri įveikia Hwang *et al.* ir Sun schemas. Vykdant šią ataką, vienas atstovaujantis pasirašantysis asmuo ir tikras pasirašantysis asmuo kartu gali padirbti bet kurį galiojantį atstovaujantį parašą. Todėl Hwang *et al.* schema ir Sun schema yra nesaugios.