INFORMATICA, 2003, Vol. 14, No. 3, 1–10

Improved Non-Repudiable Threshold Proxy Signature Scheme with Known Signers

Chwei-Shyong TSAI[b], Shiang-Feng TZENG[a], Min-Shiang HWANG[a,c]

[a]*Department of Information Management, Chaoyang University of Technology*
168, Gifeng E. Rd., Wufeng, Taichung County, Taiwan 413, ROC
e-mail: mshwang@mail.cyut.edu.tw

[b]*Department of Information Management, National Taichung Institute of Technology*
129 Sec. 3, San-min Rd., Taichung, Taiwan 404, ROC

[c]*Department of Management Information Systems, National Chung Hsing University*
250, Kuo Kuang Road, Taichung, Taiwan 402, ROC

Received: March 2003

Abstract. In 2001, Hsu *et al.* proposed a non-repudiable threshold proxy signature with known signers. In their scheme, the proxy group cannot deny having signed the proxy signature if they did. However, Hsu *et al.*'s scheme is vulnerable to some attacks. A malicious original signer or malicious proxy signer can impersonate some other proxy signers to generate proxy signatures. In this article, we shall present our cryptanalysis of the Hsu *et al.*'s scheme. After that, we shall propose a new threshold proxy signature that can overcome the weaknesses.

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

1. Introduction

The concept of a proxy signature (Mambo *et al.*, 1996a; Mambo *et al.*, 1996b) was first introduced in 1996. The proxy signature scheme allows the original signer to delegate her/his signing capability to a designated person, called a proxy signer. The proxy signer generates the proxy signature on a message on behalf of the original signer. After that, any verifier can check the validity of the proxy signature and can make sure of the original signer's agreement on the signed message.

Following the development of the proxy signature scheme, some threshold proxy signature schemes have been proposed and widely studied (Hsu *et al.*, 2001; Hwang *et al.*, 2000; Hwang *et al.*, 2002b; Kim *et al.*, 1997; Sun, 1999; Zhang, 1997). 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.

Sun (1999) proposed an efficient non-repudiable threshold proxy signature scheme with known signers based on Kim's scheme (Kim *et al.*, 1997). Sun's scheme is more

efficient than other threshold proxy signature schemes and has the non-repudiable property. The main advantage of Sun's scheme is that the verifier is able to identify the actual signers in the proxy group. However, Sun's scheme is vulnerable to the collusion attack (Hwang *et al.*, 2000) and the conspiracy attack (Hsu *et al.*, 2001).

Hsu *et al.* (2001) proposed a new and efficient non-repudiable proxy signature scheme that could withstand the above attacks. Furthermore, it also outperformed Sun's scheme in computational complexity and communication cost. However, we will show that Hsu *et al.'s* scheme is vulnerable to the public key substitution and the insider forgery attacks in this article. A malicious original signer can impersonate t or more legal proxy signers to generate proxy signatures. Besides, the malicious proxy signer can impersonate $t-1$ or more legal proxy signers to generate proxy signatures. Moreover, the real proxy signers cannot deny having signed the proxy signature before though they did not.

In this article, we shall show the weaknesses of Hsu *et al.'s* scheme and remedy the problems. In the next section, we shall review Hsu *et al.'s* scheme (the Hsu-Wu-Wu scheme). In Section 3, we shall show that the Hsu-Wu-Wu scheme is vulnerable to the public key substitution attack (Sun, 2000) and the insider forgery attack (Li *et al.*, 2000). In Section 4, our improved scheme and the security analysis of the improved scheme will be proposed and presented. Finally, the concluding remarks will be in the last section.

2. Review of the Hsu-Wu-Wu Scheme

The scheme includes four phases: secret share generation, proxy share generation, proxy signature generation, and proxy signature verification. There exists a system authority (SA) whose tasks are to initialize the system and to manage the public directory. In the secret share generation phase, initially, SA selects and publishes the following parameters:

- 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 signer and the proxy signers of the proxy group, parameters t and n, the valid delegation time, etc.,
- $ASID$: (Actual Signers' ID) the identities of the actual signers.

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

2.1. *Secret Share Generation Phase*

SA selects the group private key X_G and calculates the group public key $Y_G = g^{X_G} \bmod p$ which is certified by CA. Then, SA randomly creates a $(t-1)$-degree polynomial as

$$f(v) = X_G + a_1 v + a_2 v^2 + \cdots + a_{t-1} v^{t-1} \bmod q,$$

where the random integers $a_i \in Z_q$ $(i = 1, 2, \cdots, t-1)$.

For each $U_{P_i} \in G_P$, SA calculates the secret share $\gamma_i = f(v_i)$ and the corresponding public information $\tau_i = g^{\gamma_i} \bmod p$, where v_i is the public identifier for U_{P_i}. Then, SA separately sends γ_i to U_{P_i} via a secure channel and publishes all τ_i's.

2.2. *Proxy Share Generation Phase*

U_O performs the following steps to delegate the signing capability to G_P.

1. Select a random number $k \in Z_q^*$ and calculate $K = g^k \bmod p$.
2. Calculate the proxy signature key as $\sigma = k + x_O h(M_w \| K) \bmod q$, where "$\|$" denotes the concatenation operator.
3. Generate a polynomial $f_O(v) = \sigma + b_1 v + b_2 v^2 + \cdots + b_{t-1} v^{t-1} \bmod q$, where the random numbers $b_j \in Z_q$ $(j = 1, 2, \cdots, t-1)$.
4. Publish $B_j = g^{b_j} \bmod p$, for $j = 1, 2, \cdots, t-1$.
5. Send $\sigma_i = f_O(v_i)$ to $U_{P_i} \in G_P$ via a secure channel.
6. Broadcast (M_w, K).

Receiving σ_i, each $U_{P_i} \in G_P$ can validate it by checking the following equation

$$g^{\sigma_i} \stackrel{?}{=} y_O^{h(M_w \| K)} K \Big(\prod_{j=1}^{t-1} B_j^{v_i^j} \Big) \bmod p. \tag{1}$$

If it holds, U_{P_i} calculates $\sigma_i' = \sigma_i + \gamma_i h(M_w \| K) \bmod q$ as her/his proxy share.

2.3. *Proxy Signature Generation Phase*

Given a message M, any t or more proxy signers of G_P will be the proxies for U_O to sign M in this phase. Without loss of generality, let $D_P = \{U_{P_1}, U_{P_2}, \cdots, U_{P_t}\}$ be the actual proxy signers. D_P as a group performs the following steps to generate the proxy signature.

1. Each U_{P_i} selects a random number $k_i \in Z_q^*$ and then broadcasts $r_i = g^{k_i} \bmod p$.
2. Upon receiving all r_j's $(j = 1, 2, \cdots, t; j \neq i)$, each U_{P_i} calculates

$$\begin{aligned} R &= \prod_{j=1}^{t} r_j \bmod p, \\ s_i &= k_i R + (L_i \sigma_i' + x_{P_i}) h(R \| ASID \| M) \bmod q, \end{aligned}$$

where $L_i = \prod_{j=1, j\neq i}^{t}(-v_j)(v_i - v_j)^{-1} \bmod q$. Here, s_i is the individual proxy signature which is sent to the designated clerk.

3. Upon receiving s_i, the designated clerk validates it by checking

$$g^{s_i} \stackrel{?}{=} r_i^R \left(\left((y_O \tau_i)^{h(M_w \| K)} \Big(\prod_{j=1}^{t-1} B_j^{v_i^j} \Big) K \right)^{L_i} y_{P_i} \right)^{h(R \| ASID \| M)} \bmod p.$$

If it holds, (r_i, s_i) is the valid individual proxy signature of M. If all the individual proxy signatures of M are valid, the clerk calculates

$$S = \sum_{j=1}^{t} s_j \bmod q. \tag{2}$$

The proxy signature of M is $(R, S, K, M_w, ASID)$.

2.4. *Proxy Signature Verification Phase*

Receiving the proxy signature (R, S, K, M_w, $ASID$) of M, 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 can identify the original signer and the proxy signers, and obtain the necessary public keys from the CA. In addition, she/he can identify the actual proxy signers, too.
2. The verifier validates the proxy signature by checking

$$g^S \stackrel{?}{=} R^R \Big(K (y_O Y_G)^{h(M_w \| K)} \prod_{i=1}^{t} y_{P_i} \Big)^{h(R \| ASID \| M)} \bmod p. \tag{3}$$

If it holds, the proxy signature (R, S, K, M_w, $ASID$) for M is valid.

3. The Weaknesses of the Hsu-Wu-Wu Scheme

In this section, we show that the Hsu-Wu-Wu scheme is vulnerable to the public key substitution attack and the insider forgery attack. A malicious original signer (U_O) or a malicious proxy signer (U_{P_k}) can forge the valid proxy signature without the other signers' private keys.

3.1. *Public Key Substitution Attack*

In this subsection, we will show the Hsu-Wu-Wu scheme is vulnerable to the public key substitution attack. Suppose the malicious original signer, without any private keys of the other proxy signers, attempts to forge a valid proxy signature for a message. The steps of this attack are as follows:

1. U_O randomly selects a private key $x_O \in Z_q^*$.
2. U_O waits until she/he obtains any t or more proxy signers y_{P_i}. Then, instead of broadcasting $y_O = g^{x_O} \bmod p$, she/he calculates

$$y'_O = g^{x_O}(Y_G)^{-1} \prod_{i=1}^{t} y_{P_i}^{-h(M_w \| K)^{-1}} \bmod p,$$

   and reveals the value y'_O as her/his public key.
3. U_O selects two random numbers k and r, and calculates K and R as follows:

$$K = g^k \bmod p,$$
$$R = g^r \bmod p.$$

4. U_O chooses a message M at will and calculates S as

$$S = rR + (k + x_O h(M_w \| K)) h(R \| ASID \| M) \bmod q.$$

Then, the proxy signature for M is (R, S, K, M_w, $APSID$).

Theorem 1. *A forged proxy signature generated by U_O according to the above steps, namely (R, S, K, M_w, $ASID$), is a valid proxy signature for the message M.*

Proof. On receipt of (R, S, K, M_w, $ASID$), the verifier checks the validity of the proxy signature of the message M through (3) as follows.

$$\begin{aligned} g^S &= R^R \Big(K (y_O Y_G)^{h(M_w \| K)} \prod_{i=1}^{t} y_{P_i} \Big)^{h(R \| ASID \| M)}, \\ &= R^R \Bigg(K \Big(g^{x_O} (Y_G)^{-1} \prod_{i=1}^{t} y_{P_i}^{-h(M_w \| K)^{-1}} Y_G \Big)^{h(M_w \| K)} \prod_{i=1}^{t} y_{P_i} \Bigg)^{h(R \| ASID \| M)}, \\ &= R^R (K g^{x_O h(M_w \| K)})^{h(R \| ASID \| M)}, \\ &= g^{rR + (k + x_O h(M_w \| K)) h(R \| ASID \| M)} \bmod p. \end{aligned}$$

The above equation holds, and the forged proxy signature (R, S, K, M_w, $ASID$) is taken for the valid proxy signature for message M.

3.2. *Insider Forgery Attack*

In this subsection, we will show the Hsu-Wu-Wu scheme is vulnerable to the insider forgery attack feasible. Suppose a malicious proxy signer U_{P_k}, without any private key of the other proxy signers, attempts to forge a valid proxy signature for an arbitrary message. The attacker can take the steps as follows:

1. U_{P_k} randomly chooses a private key $x_{P_k} \in Z_q^*$.

2. U_{P_k} waits until she/he obtains any $t-1$ or more proxy signers y_{P_i}. Then, instead of broadcasting $y_{P_k} = g^{x_{P_k}} \bmod p$, she/he calculates

$$y'_{P_k} = g^{x_{P_k}} \Big(K(y_O Y_G)^{h(M_w \| K)} \prod_{i=1}^{t-1} y_{P_i} \Big)^{-1} \bmod p,$$

and reveals the quantity y'_{P_k} as her/his public key.

3. U_{P_k} chooses a random number r and calculates R as follows:

$$R = g^r \bmod p.$$

4. U_{P_k} chooses an arbitrary message M and calculates S as

$$S = rR + x_{P_k} h(R \| ASID \| M) \bmod q.$$

Then, the proxy signature for M is (R, S, K, M_w, $ASID$).

Theorem 2. *A forged proxy signature generated by U_{P_k} according to the above steps, namely (R, S, K, M_w, $ASID$), is a valid proxy signature for the message M.*

Proof. On receipt of (R, S, K, M_w, $ASID$), the verifier checks the validity of the proxy signature of the message M through (3) as follows.

$$\begin{aligned} g^S &= R^R \Big(K(y_O Y_G)^{h(M_w \| K)} \prod_{i=1}^{t} y_{P_i} \Big)^{h(R \| ASID \| M)}, \\ &= R^R \Bigg(K(y_O Y_G)^{h(m_w \| K)} g^{x_{P_k}} \Big(K(y_O Y_G)^{h(M_w \| K)} \prod_{i=1}^{t-1} y_{P_i} \Big)^{-1} \prod_{i=1}^{t-1} y_{P_i} x \Bigg)^{h(R \| ASID \| M)}, \\ &= R^R g^{x_{P_k} h(R \| ASID \| M)}, \\ &= g^{rR + x_{P_k} h(R \| ASID \| M)} \bmod p. \end{aligned}$$

The above equation holds, and the forged proxy signature (R, S, K, M_w, $ASID$) is taken for the valid proxy signature for the message M.

4. Improvement and Cryptanalysis

In this section, we shall modify the Hsu-Wu-Wu scheme to remedy the weaknesses described previously.

4.1. *The Improved Scheme*

In the Hsu-Wu-Wu scheme, the proxy signature can be forged by a malicious original signer or malicious proxy singer. To remedy this weakness, we have modified the Hsu-Wu-Wu scheme, and the revised scheme is as follows.

In the proxy share generation phase, we replace σ with

$$\sigma = k + x_O y_O h(M_w \| K) \bmod q.$$

Therefore, 1) becomes as follows.

$$g^{\sigma_i} \stackrel{?}{=} y_O^{y_O h(M_w \| K)} K \Big(\prod_{j=1}^{t-1} B_j^{v_i^j} \Big) \bmod p.$$

The other steps of the proxy share generation phase are the same as those of the Hsu-Wu-Wu scheme.

In the proxy signature generation phase, we replace s_i with

$$s_i = k_i R + (L_i \sigma_i' + x_{P_i} y_{P_i}) h(R \| ASID \| M) \bmod q.$$

The proxy signer U_{P_i} calculates s_i from the above equation and sends s_i to the designated clerk. The designated clerk can then verify the validity of s_i by the following equation:

$$g^{s_i} \stackrel{?}{=} r_i^R \Bigg(\Big((y_O^{y_O} \tau_i)^{h(M_w \| K)} \Big(\prod_{j=1}^{t-1} B_j^{v_i^j} \Big) K \Big)^{L_i} y_{P_i}^{y_{P_i}} \Bigg)^{h(R \| ASID \| M)} \bmod p,$$

where $L_i = \prod_{j=1, j \neq i}^{t} (-v_j)(v_i - v_j)^{-1} \bmod q$. Then, the designated clerk calculates S from (2), and the proxy signature on message M is (R, S, K, M_w, $ASID$).

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

$$g^S \stackrel{?}{=} R^R \Big(K (y_O^{y_O} Y_G)^{h(M_w \| K)} \prod_{i=1}^{t} y_{P_i}^{y_{P_i}} \Big)^{h(R \| ASID \| M)} \bmod p.$$

If it holds, the verifier can make sure of the validity of the proxy signature and identify the actual signers. Furthermore, the revised scheme can withstand the public key substitution attack and the insider forgery attack. Neither, the malicious original signer nor anyone malicious proxy signer can forge the proxy signatures.

4.2. *Security Analysis of the Improved Scheme*

The security of the improved scheme is examined as follows. As with the Hsu-Wu-Wu scheme, the level of security is quite desirable. The difference, however, is that our scheme can withstand the public key substitution attack and the insider forgery attack.

Attack 1: Consider the public key substitution attack. The malicious original signer U_O tries to impersonate any t or more proxy signers in G_P and to forge their proxy signature without the agreement of these proxy signers.

Analysis of attack 1: U_O has to change her/his public key after the public keys of the t or more proxy signers have been determined. Assume U_O waits until she/he receives any t proxy signers' public keys y_{P_i}. She/He substitutes her/his public key y_O.

Assume U_O selects a random number x_O as her/his private key. Then, U_O has to make her/his public key y'_O in satisfying the following equation:

$$y_O'^{y'_O} = g^{x_O}(Y_G)^{-1}\prod_{i=1}^{t} y_{P_i}^{-h(M_w\|K)^{-1}} \bmod p.$$

In the above equation, suppose U_O determines the value x_O first. She/He has to obtain the value y'_O by solving the difficult problem. On the other hand, suppose U_O wants to fix y'_O, she/he has to solve the discrete logarithms (ElGamal, 1985; Hwang *et al.*, 2002a; Hwang *et al.*, 2001; Lee *et al.*, 2002) to find her/his private key x_O. Therefore, the malicious original signer cannot successfully forge any proxy signature for any message by launching the public key substitution attack.

Attack 2: Consider the insider forgery attack. Suppose a malicious proxy signer U_{P_k} tries to impersonate any $t-1$ or more of the other proxy signers in G_P and to forge the proxy signature without the agreement of these proxy signers.

Analysis of attack 2: Similarly, G_P can also launch the insider forgery attack. Without losing generality, suppose that the malicious proxy signer U_{P_k} wants to update her/his public key y_{P_k}. Assume U_{P_k} waits until she/he obtains any $t-1$ proxy signers' public keys y_{P_i}. She/He changes her/his public key y_{P_k}. U_{P_k} chooses a random number x_{P_k} and makes her/his public key y'_{P_k} as follows:

$$y_{P_k}'^{y'_{P_k}} = g^{x_{P_k}}\left(K(y_O Y_G)^{h(M_w\|K)}\prod_{i=1}^{t-1} y_{P_i}\right)^{-1} \bmod p.$$

However, U_{P_k} cannot create a valid proxy signature. From the above equation, assume the value of x_{P_k} is determined first. Then, it is an extremely difficult thing to find a y'_{P_k} satisfying the equation. On the other hand, if U_{P_k} determines the integer y'_{P_k} first, she/he has to solve the discrete logarithms to find the value of x_{P_k}. Thus, the insider forgery attack here will not work.

5. Conclusions

In this article, we have presented the public key substitution attack and the insider forgery attack on the Hsu-Wu-Wu scheme. In these attacks, the malicious original signer or any malicious insider proxy signer in the proxy group, without any private keys of other proxy signers, can forge a valid proxy signature for any message. We have also proposed a secure improved scheme to remedy the weaknesses of the Hsu-Wu-Wu scheme. In our new scheme, neither the original signer nor any malicious proxy signer can forge the legal proxy signature.

Acknowledgements

The authors wish to thank many anonymous referees for their suggestions to improve this paper. Part of this research was supported by the National Science Council, Taiwan, ROC, under contract no. NSC91-2213-E-324-003.

References

ElGamal, T. (1985). A public-key cryptosystem and a signature scheme based on discrete logarithms. *IEEE Transactions on Information Theory*, **1**(5), 469–472.

Hsu, C.L., T.S. Wu and T.C. Wu (2001). New nonrepudiable threshold proxy signature scheme with known signers. *The Journal of Systems and Software*, **58**(5), 119–124.

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

Hwang, M.S., C.C. Chang and K.F. Hwang (2002a). An ElGamal-like cryptosystem for enciphering large messages. *IEEE Transactions on Knowledge and Data Engineering*, **14**(2), 445–446.

Hwang, M.S., C.C. Lee and E.J.L. Lu (2001). Cryptanalysis of the batch verifying multiple DSA-type digital signatures. *Pakistan Journal of Applied Sciences*, **1**(3), 287–288.

Hwang, M. S., E. J. L. Lu and Iuon-Chang Lin (2002b). A practical (*t, n*) threshold proxy signature scheme based on the RSA cryptosystem. *IEEE Transactions on Knowledge and Data Engineering* (to appear).

Kim, S., S. Park and D. Won (1997). Proxy signatures, revisited. In *Proc. of ICICS'97, LNCS*, **1334**. pp. 223–232.

Lee, C.C., M.S. Hwang and L.H. Li (2002). A new key authentication scheme based on discrete logarithms. *Applied Mathematics and Computation* (to appear).

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**, 1338–1353.

Mambo, M., K. Usuda and E. Okamoto (1996b). Proxy signatures for delegating signing operation. In *Proc. Third ACM Conf. on Computer and Communications Security*. pp. 48–57.

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

Sun, H.M. (2000). On proxy (multi-) signature schemes. In *2000 International Computer Symposium*, Chiayi, Taiwan. pp. 65–72.

Zhang, K. (1997). Threshold proxy signature schemes. In *1997 Information Security Workshop*. pp. 191–197.

C.-S. Tsai received the BS degree in applied mathematics in 1984 from National Chung Hsing University, Taichung, Taiwan. He received the MS degree in computer science and electronic engineer in 1986 from National Center University, Chungli, Taiwan. He received the PhD degree in computer science and information engineering in 2002 from National Chung Cheng University, Chiayi, Taiwan. Since August 2002, he has been an associate professor of the Department of Information Management at National Taichung Institute of Technology, Taichung, Taiwan. His research interests include image authentication, information hiding, and cryptography.

S.-F. Tzeng received the BS degree in information management from Chaoyang University of Technology (CYUT), Taichung, Taiwan, Republic of China, in 2001. He is currently pursuing his MS degree in information management from CYUT. His current research interests include applied cryptography and data security.

M.-S. Hwang received the BS in electronic engineering from National Taipei Institute of Technology, Taipei, Taiwan, Republic of China, in 1980; the MS in industrial engineering from National Tsing Hua University, Taiwan, in 1988; and the PhD in computer and information science from National Chiao Tung University, Taiwan, in 1995. He also studied applied mathematics at National Cheng Kung University, Taiwan, 1984–1986. Dr. Hwang passed the National Higher Examination in field "Electronic Engineer" in 1988. He also passed the National Telecommunication Special Examination in field "Information Engineering", qualified as advanced technician the first class in 1990. From 1988 to 1991, he was the leader of the Computer Center at Telecommunication Laboratories (TL), Ministry of Transportation and Communications, ROC. He was also a project leader for research in computer security at TL in July 1990. He obtained the 1997, 1998, and 1999 Distinguished Research Awards of the National Science Council of the Republic of China. He is currently a professor and chairman of the Department of Information Management, Chaoyang University of Technology, Taiwan, ROC. He is a member of IEEE, ACM, and Chinese Information Security Association. His current research interests include database and data security, cryptography, image compression, and mobile communications.