Cryptanalysis of Two Nonrepudiable Threshold Proxy Signature Schemes

Qi Xie[1] and Xiu-Yuan Yu[2,3]
(Corresponding author: Qi Xie)

School of Information and Engineering, Hangzhou Teachers College[1]
No. 222, WenYi Load, Hangzhou 310012, P.R. China (Email: qixie68@yahoo.com.cn;qixie@hztc.edu.cn)
School of Science, Hangzhou Teachers College[2]
No. 222, WenYi Load, Hangzhou 310012, P.R. China
Department of Mathematics and Physics, Quzhou College[3]
Quzhou 324000, P.R. China

(Received June 30, 2005; revised and accepted July 25 & Aug. 15, 2005)

Abstract

This paper will show that Hsu and Wu's efficient nonrepudiable threshold proxy signature scheme with known signers and Yang, Tzeng and Hwang's efficient nonrepudiable threshold proxy signature scheme with known signers are insecure. The malicious original signer can forge a valid threshold proxy signature for any message and any warrant after getting a valid proxy signature. In addition, since Yang et al.'s scheme is more efficient than Hsu and Wu's scheme in terms of computational complexities and communication costs, this paper only presents a simple countermeasure to improve Yang et al.'s scheme.

Keywords: Cryptography, digital signature, forgery attack, proxy signature, threshold proxy signature

1 Introduction

The concept of proxy signature was first proposed by Mambo et al. [5] in 1996. A proxy signature scheme allows a signer to delegate the signing capability to a designated person, called the proxy signer, the proxy signer can generate proxy signature of a message on behalf of the original signer. In 1997, Kim et al. [4] and Zhang [8] proposed a new concept of proxy signature, called (t, n) threshold proxy signature. 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, but $t-1$ or fewer proxy signers cannot.

In some applications, it is important that the threshold proxy signature scheme has the nonrepudiable property, which the verifier is able to identify the actual signer in the proxy group. In 1999, Sun [6] pointed out the disadvantage of Kim et al.'s scheme [4] that the verifier of the proxy signature cannot authenticate the group key generated by the legal proxy group. Furthermore, based on the scheme of Kim et al., Sun proposed a nonrepudiable threshold proxy signature scheme with known signers to eliminate the disadvantage of [4]. Hwang et al. [3] and Hsu et al. [1] pointed out that Sun's scheme cannot resist the conspiracy attack, and they proposed a new scheme that can withstand the conspiracy attack, and that is more efficient than Sun's scheme, respectively. Recently, Hsu and Wu [2] presented a collusion attack to show that Hwang et al.'s scheme [3] was still vulnerable to the conspiracy attack, and proposed an improvement scheme not only to eliminate the security leaks but also to be more efficient than Hwang et al.'s scheme in terms of computational complexities and communication costs. On the other hand, Yang et al. [7] proposed an improvement of Hsu et al.'s scheme in terms of computational complexities and communication costs.

In this paper, we will show that Hsu and Wu's efficient nonrepudiable threshold proxy signature scheme with known signers and Yang et al.'s efficient nonrepudiable threshold proxy signature scheme with known signers are insecure. The malicious original signer can forge a valid threshold proxy signature for any message and any warrant with knowing a previously valid threshold proxy signature. Furthermore, in terms of computational complexities and communication costs, Yang et al.'s scheme is more efficient than Hsu and Wu's scheme, we present a simple countermeasure to improve Yang et al.'s scheme.

2 Brief Review of Hsu and Wu's Scheme

There exists a system authority (SA) to initialize the system and manage the public directory. Let p be a large prime, q a prime divisor of $p-1$; g a generator of a multiplicative subgroup of Z_p with order q; $h(\cdot)$ a one-way hash function; m_w is a warrant 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; $ASID$ denotes 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 $G = \{P_1, P_2, \ldots, P_n\}$ be the proxy group of n proxy signers. Hsu and Wu's scheme can be divided into four stages: secret share generation stage, proxy share generation stage, proxy signature generation stage and proxy signature verification stage.

2.1 Secret Share Generation

Each $P_i \in G$ randomly generates a secret polynomial $f_i(v)$ of degree $t-1$, which $f_i(v) = \sum_{l=1}^{t-1} a_{il}v^l + (x_i) + a_{i0}(\text{mod}q)$, where $a_{il} \in Z_q$ are random numbers and publishes $A_{il} = g^{a_{il}} \bmod p$ for $l = 0, 1, 2, \ldots, t-1$. Then, P_i computes and transmits $f_i(v_j)$ to other proxy signer P_j via a secure channel for $i \neq j$, and P_j can verify the validity of $f_i(v_j)$ by checking the equality $g^{f_i(v_j)} = y_i \prod_{l=0}^{t-1} A_{il}^{v_j^l}(\text{mod } p)$. If all $f_j(v_i)$ are vilified, P_i computes the public information $A_l = \prod_{i=1}^{n} A_{il} \bmod p$ for $l = 0, 1, 2, \ldots, t-1$, and his secret share $\gamma_i = \sum_{l=1}^{n} f_l(v_i) \bmod q$.

2.2 Proxy Share Generation

The original signer chooses a random integer $k \in Z_q^*$, computes $K = g^k \bmod p$ and $\sigma = x_0 h(m_w, K) + k(\text{mod } q)$. Then, he shares a proxy key σ in a (t, n) threshold scheme to the proxy group G, P_0 generates a secret $(t-1)$-degree polynomial $f_0(v)$, and computes $\sigma_i = f_0(v_i) = \sigma + \sum_{j=1}^{t-1} b_j v_i^j (\text{ mod } q)$, where $b_j$are random numbers. Finally, the original signer sends σ_i to each P_i via a secure channel, broadcasts (m_w, K) to G and publishes $B_j = g^{b_j} \bmod p(j = 1, 2, \ldots, t-1)$.

After receiving σ_i, each $P_i \in G$ checks whether the equation $g^{\sigma_i} = y_0^{h(m_w,K)} K \prod_{j=1}^{t-1} B_j^{v_i^j} \bmod p$ holds or not. If the equation holds, each P_i computes his proxy share $\sigma_i' = \sigma_i + \gamma_i h(m_w, K) \bmod q$.

2.3 Proxy Signature Generation

Let $D = \{P_1, P_2, \ldots, P_t\}$ be t proxy signers who want to cooperatively sign a message m on behalf of the original signer, they perform the following steps:

1) Each $P_i \in D$ chooses a random integer $k_i \in Z_q^*$, computes $r_i = g^{k_i} \bmod p$, and sends r_i to all signers in D.

2) Each $P_i \in D$ computes $R = \prod_{j=1}^{t} r_j \bmod p$, and

$$s_i = k_i R + (L_i \sigma_i' + x_i)h(A_0, R, ASID, m)(\text{mod } q)$$

where $L_i = \prod_{j=1, j\neq i}^{t} (-v_j)(v_i - v_j)^{-1}$. Then he sends his individual proxy signature (r_i, s_i) to the designated clerk.

3) On receiving all (r_i, s_i), the clerk can verify the validity by checking:

$$\begin{aligned} g^{s_i} &= r_i^R(((T))^{h(m_w,K)}K(\prod_{j=1}^{t-1} B_j^{v_i^j}))^{L_i} y_i)^X \bmod p \\ T &= y_0 Y_G A_0 (\prod_{j=1}^{t-1} A_j^{v_i^j}) \\ X &= h(A_0, R, ASID, m). \end{aligned}$$

If above equation holds, he computes $S = \sum_{i=1}^{t} s_i \bmod q$, the proxy signature on m is $(R, S, K, A_0, m_w, ASID)$.

2.4 Proxy Signature Verification

On receiving the proxy signature $(R, S, K, A_0, m_w, ASID$ $)$ of m, the verifier can identify the original signer and the proxy group from the m_w. Then he knows the actual signers from $ASID$ and obtains the necessary public keys from CA. The verifier can validate the proxy signature by checking:

$$g^S = R^R((y_0 Y_G A_0)^{h(m_w,K)} K (\prod_{i=1}^{t} y_i)^{h(A_0,R,ASID,m)} \bmod p$$

If it holds, the proxy signature $(R, S, K, A_0, m_w, ASID$ $)$ of m is valid.

3 Brief Review of Yang et al.'s Scheme

The system parameters are the same as those of Hsu and Wu's scheme. Yang et al.'s scheme can be divided into three stages: proxy share generation stage, proxy signature generation stage and proxy signature verification stage.

3.1 Proxy Share Generation

The original signer chooses a random number $k \in Z_q^*$, computes $K = g^k \bmod p$ and $\sigma = x_0 h(m_w, K) + k \bmod q$. Then, he sends (σ, m_w, K) to each P_i in G.

After receiving (σ, m_w, K), each $P_i \in G$ checks whether the equation $g^\sigma = y_0^{h(m_w,K)} K \bmod p$ holds or not. If the equation holds, each P_i obtains his proxy share σ.

3.2 Proxy Signature Generation

Let $D = \{P_1, P_2, \ldots, P_t\}$ be t proxy signers who want to cooperatively sign a message on behalf of the original signer, they perform the following steps:

1) Each $P_i \in D$ chooses a random number $k_i \in Z_q^*$, computes $r_i = g^{k_i} \bmod p$, and sends r_i to all signers in D.

2) Each $P_i \in D$ computes $R = \prod_{j=1}^{t} r_j \bmod p$, and
$$s_i = k_i R + (t^{-1}\sigma + x_i)h(R, ASID, m) (\bmod\ q).$$
Then he sends his individual proxy signature (r_i, s_i) to the designated clerk.

3) On receiving all (r_i, s_i) , the clerk can verify the validity by the equation:
$$g^{s_i} = r_i^R((Ky_0^{h(m_w,K)})^{t^{-1}}y_i)^{h(R,ASID,m)} \bmod p.$$
If above equation holds, he/she computes $S = \sum_{i=1}^{t} s_i \bmod q$, the proxy signature of m is $(R, S, K, m_w, ASID)$.

3.3 Proxy Signature Verification

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

The verifier checks the validity of the proxy signature through the following equation:
$$g^S = R^R(Ky_0^{h(m_w,K)}\prod_{i=1}^{t} y_i)^{h(R,ASID,m)} \bmod p.$$

4 Cryptanalysis of Hsu and Wu's Scheme

In this section, we will show that Hsu and Wu's scheme is insecure. The malicious original signer can forge a valid threshold proxy signature for any message and any warrant with knowing a previously valid threshold proxy signature. Assume that the threshold proxy signature $(R, S, K, A_0, m_w, ASID)$ of message m is a valid proxy signature, the malicious original signer can forge a valid threshold proxy signature for any message m' as follows:

1) Compute $A_0' = Y_G^{-1}g^{\alpha} \bmod p$, for $\forall\alpha \in Z_q$.

2) Compute $d = (h(A_0', R, ASID, m'))^{-1}h(A_0, R, ASID, m) \bmod q$.

3) Compute $K' = (Y_G A_0)^{dh(m_w,K)}K^d(\prod_{i=1}^{t} y_i)^{d-1} \bmod p$.

4) For $\forall m_w'$, compute
$$\begin{aligned} S' &= S - x_0 h(m_w, K)h(A_0, R, ASID, m) + (x_0 + \\ &\quad \alpha)h(m_w', K')h(A_0', R, ASID, m') \bmod q. \end{aligned}$$

The following shows that the threshold proxy signature $(R, S', K', A_0', m_w', ASID)$ for message m' is valid.
$$\begin{aligned} g^{S'} &= g^S g^{-x_0H_1H_2} g^{(x_0+\alpha)H_3H_4} \\ &= R^R((y_0Y_GA_0)^{H_1}K(\prod_{i=1}^{t} y_i))^{H_2} \times y_0^{-H_1H_2}(y_0g^{\alpha})^{H_3H_4} \\ &= R^R(Y_GA_0)^{H_1}K(\prod_{i=1}^{t} y_i))^{dH_4} \times (y_0Y_GA_0')^{H_3H_4} \\ &= R^R(K'\prod_{i=1}^{t} y_i)^{H_4}(y_0Y_GA_0')^{H_3H_4} \\ &= R^R((y_0Y_GA_0')^{H_3}K'(\prod_{i=1}^{t} y_i))^{H_4} \bmod p \\ H_1 &= h(m_w, K) \\ H_2 &= h(A_0, R, ASID, m) \\ H_3 &= h(m_w', K') \\ H_4 &= h(A_0', R, ASID, m') \end{aligned}$$

Therefore, the Hsu and Wu's scheme is insecure.

5 Cryptanalysis of Yang et al.'s Scheme

In this section, an attack will be proposed on Yang et al.'s scheme. The malicious original signer can forge a valid threshold proxy signature for any message and any warrant with knowing a previously valid threshold proxy signature. Assume that the threshold proxy signature $(R, S, K, m_w, ASID)$ of message m is a valid proxy signature, the malicious original signer can forge a valid threshold proxy signature $(R, S', K', m_w', ASID)$ for any message m' as follows:

1) Compute $d = (h(R, ASID, m'))^{-1}h(R, ASID, m) \bmod q$.

2) Compute $K' = y_0^{dh(m_w,K)}K^d(\prod_{i=1}^{t} y_i)^{d-1} \bmod p$.

3) For $\forall m_w'$, compute $S' = S + x_0 h(m_w', K')h(R, ASID, m') \bmod q$.

The following shows that the threshold proxy signature $(R, S', K', m_w', ASID)$ for message m' is valid.
$$\begin{aligned} &R^R(y_0^{H_3}K'\prod_{i=1}^{t} y_i)^{H_4} \\ = &R^R g^{x_0H_3H_4}((y_0^{dH_1}K^d(\prod_{i=1}^{t} y_i)^{d-1})\prod_{i=1}^{t} y_i)^{H_4} \\ = &g^{x_0H_3H_4}(R^R(y_0^{H_1}K(\prod_{i=1}^{t} y_i))^{dH_4}) \\ = &g^{x_0H_3H_4}(R^R(y_0^{H_1}K(\prod_{i=1}^{t} y_i))^{H_2}) \\ = &g^{x_0H_3H_4}g^S = g^{S'} \ (\bmod\ p). \end{aligned}$$

$$\begin{aligned} H_1 &= h(m_w, K) \\ H_2 &= h(R, ASID, m) \\ H_3 &= h(m'_w, K') \\ H_4 &= h(R, ASID, m') \end{aligned}$$

In the verification stage, any verifier can verify the validity of the proxy signature and $ASID$ records the identities as actual signers of the proxy group. In fact, $P_1, P_2, \ldots, P_t$ have never signed the message m', but they cannot deny.

Therefore, Yang et al.'s scheme is insecure.

6 Improvement of Yang et al.'s Scheme

In this section, we only modify the Yang et al.'s scheme to remedy the weakness as described in Section 5. The reason is that the Yang et al.'s scheme is more efficient than Hsu and Wu's scheme in terms of computational complexities and communication costs, the reader is encouraged to refer to [2] and [7].

The improvement threshold proxy signature scheme is similar to that of Yang et al.'s scheme, we only describe the differences below.

In the system initialization phase, when each user's public key is certified by CA, the registering user must perform a challenge-response protocol or zero-knowledge protocol to convince CA that he knows the private key corresponding to his public key.

In the proxy signature generation stage, we replace each P_i's proxy signature s_i with

$$s_i = k_i R + (t^{-1}\sigma + x_i) h(R, K, ASID, m_w, m) (\bmod\ q),$$

The verification equation is:

$$g^{s_i} = r_i^R ((K y_0^{h(m_w, K)})^{t^{-1}} y_i)^{h(R, K, ASID, m_w, m)} \bmod p.$$

Therefore, the threshold proxy signature of m is $(R, S, K, m_w, ASID)$.

In the proxy signature verification stage, according to m_w and $ASID$, the verifier gets the public keys of the original and the proxy signers from CA. Then he checks the validity of the proxy signature through the following equation:

$$g^S = R^R ((K y_0^{h(m_w, K)}) \prod_{i=1}^{t} y_i)^{h(R, K, ASID, m_w, m)} \bmod p.$$

7 Security Discussion

The security analysis of the proposed improvement is similar to that of Yang et al.'s scheme based on the well-known one-way hash function and the discrete logarithm problem cryptographic assumptions. In this subsection, we only discuss the pointed out weaknesses against the proposed improvement.

If the malicious original signer wants to find (S', K', m'_w) to forge a valid threshold proxy signature for the chosen message without knowing the secret key $x_i (i = 1, 2, \ldots, t)$, such that

$$g^{S'} = (R)^R (K' (y_0)^{h(m'_w, K')} \prod_{i=1}^{t} y_i)^{h(R, K', ASID, m'_w, m')} \bmod p.$$

Because the parameters $(R, ASID, K', m'_w, m')$ are protected by hush function, he must fix $(R, ASID, K', m'_w, m')$, and compute

$$\begin{aligned} d &= (h(R, K', ASID, m'_w, m'))^{-1} \\ &\quad h(R, K, ASID, m_w, m) \bmod q. \end{aligned}$$

However, the malicious original signer cannot obtain x, such as $g^x = (\prod_{i=1}^{t} y_i)^{d-1} \bmod p$, unless he can solve discrete logarithm problem.

That is, our improvement scheme can against the proposed attack.

8 Conclusions

In this paper, we demonstrate forgery attack to show that Hsu and Wu's scheme and Yang et al.'s scheme are insecure. It is noted that Yang et al.'s scheme is more efficient than Hsu and Wu's scheme in terms of computational complexities and communication costs. We present an improvement scheme of Yang et al.'s scheme.

Acknowledgements

This research was supported by National Natural Science Foundation of China under Grant No.10271037.

References

[1] C. L. Hsu, T. S. Wu, and T. C. Wu, "New nonrepudiable threshold proxy signature scheme with known signers," *The Journal of Systems and Software*, vol. 58, pp. 119–124, 2001.

[2] C. L. Hsu and T. S. Wu, "Efficient nonrepudiable threshold proxy signature scheme with known signers against the collusion attack," *Applied Mathematics and Computation*, In Press.

[3] M. S. Hwang, I. C. Lin, and E. J. L. Lu, "A secure nonrepudiable threshold proxy signature scheme with known signers," *Informatica*, vol. 11, no. 2, pp. 137–144, 2000.

[4] S. Kim, S. Park, and D. Won, "Proxy signatures, revisited," in *Proc of ICICS'97*, Springer-Verlag, pp. 223–232, 1997.

[5] M. Mambo, K. Usuda, and E.Okamoto, "Proxy signatures: delegation of the power to sign messages", *IEICE Transactions on Fundamentals*, vol. E79-A, no. 9, pp. 1338–1354, 1996.

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

[7] C. Y. Yang, S. F. Tzeng, and M. S. Hwang, "On the efficiency of nonrepudiable threshold proxy signature scheme with known signers", *The Journal of Systems and Software*, vol. 73, pp. 507–514, 2004.

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

Qi Xie was born on December 26, 1968 in Zhejiang, People's Republic of China. He received the B.S. in Department of Mathematics from Hangzhou Teachers College, Hangzhou, Zhejiang, in 1990; the M.S.in Operational Research from Shanghai University, Shanghai, in 1997; and a Ph.D. in Applied Mathematics from Zhejiang University, Hangzhou, Zhejiang, in 2005. Now he is an associate professor at Hangzhou Teachers College. His current research interests include cryptography and information security.

Xiu-Yuan Yu was born in February 1942 in Shandong, People's Republic of China. He received the B.S. in Department of Mathematics from Shandong University, Jinan, Shangdong, in 1964; the M.S.in Department of Mathematics from Hangzhou University, Hangzhou, Zhejiang, in 1967; and a Ph.D. in Department of Mathematics from Shandong University, Jinan, Shangdong, in 1983. Now he is a professor at Hangzhou Teachers College and Quzhou College; a Ph.D. supervisor at Shandong University and Zhejiang University. His current research interests include number theory and its applications, cryptography and information security.