Security Analysis of a Threshold Proxy Signature Scheme

Kitae Kim and Dahun Nyang
ktkim,nyang@inha.ac.kr

July 16, 2010

Abstract

The t-out-of-n threshold proxy signatures allow an original signer to delegate his signing capability to a group of proxy signers, and t or more proxy signers can generate valid signatures by cooperating. Recently, Liu and Huang proposed a variant of threshold proxy signature scheme in which all proxy signers remain anonymous. The authors claimed their construction satisfies unforgeability, proxy signer's deviation, identifiability, undeniability and verifiability. In this paper, however, we show that their scheme does not provide the proxy signer's deviation and identifiability requirements.

Keyword : proxy signature, threshold proxy signature, anonymous, proxy signer's deviation, identifiability

1 Introduction

The concept of proxy signature was introduced by Mambo, Usuda and Okamoto in 1996 [8]. A proxy signature scheme allows a user, called original signer, to delegate his signing capability to one or more entities, called proxy signers. Then the proxy signers can sign messages, called proxy signature, on behalf of the original signer. Upon receiving a proxy signature, a verifier can check its validity to be convinced that the signature was generated by the authorized proxy of the original signer.

Following the first construction in [8], a number of proxy signature schemes have been proposed and, by combining other cryptographic primitives, some variants have been considered [1, 2, 6, 7, 11, 16, 17]. In particular, to remove single point of failure or decentralize the power of proxy signers, threshold cryptography was adapted in proxy signature scheme. The t-out-of-n threshold signature, introduced by Sharmir [10], is to distribute secret information and computation such as signature generation between n parties. Threshold proxy signature is the t-out-of-n threshold version in which t or more proxy signers can jointly generate publicly verifiable signatures but less proxy signers than t cannot.

In 2010, Liu and Huang proposed two variants of threshold proxy signature schemes, named for Scheme A and Scheme T [7]. In particular, the Scheme T was designed for enhancing privacy of proxy signers in the sense that identities of proxy signers are not revealed, except for an authority, from signatures. The authors used well known cryptographic primitives as building blocks and claimed that their scheme satisfies all security requirements, such as strong unforgeability, verifiability, proxy signer's deviation, distinguishability, undeniability and identifiability.

In this paper, we present a security analysis of Liu-Huang threshold proxy signature scheme with traceability (Scheme T). More specifically, we demonstrate that their scheme does not satisfy proxy signer's deviation and identifiability. Proxy signer's deviation means that, though t or more proxy signers may collude, they are not able to forge a valid signature that cannot be traced to themselves. Identifiability means that one can determine the signers from the trace tag in any valid signature.

2 Review of the Liu-Huang Scheme (Scheme T)

In this section, we briefly review the anonymous threshold proxy signature scheme based on pairing due to Liu and Huang.

- System Setup. PKG first generates two groups $\mathbb{G}_1$ and $\mathbb{G}_2$ of prime order p, for which there is a bilinear pairing $\hat{e} : \mathbb{G}_1 \times \mathbb{G}_1 \rightarrow \mathbb{G}_2$. PKG also selects three cryptographic hash functions $H_1 : \{0,1\} * \times \mathbb{G}_1 \rightarrow \mathbb{G}_1$, $H_2 : \{0,1\}* \rightarrow \mathbb{G}_1$, and $H_3 : \{0,1\}* \rightarrow \mathbb{Z}_p*$. Next, the authority selects a random $s \in \mathbb{Z}_p*$, a random $P \in \mathbb{G}_1$ and computes $P_{pub} = sP$. The system parameters $par = (\mathbb{G}_1, \mathbb{G}_2, \hat{e}, P, P_{pub}, H_1, H_2, H_3, p)$ are made public and the master secret key s is kept secret.

- User Key Extraction. On input identity ID, PKG computes $Q_{ID} = H_2(ID)$ as the public key and $d_{ID} = sQ_{ID}$ as the user's secret key.

- Proxy Certificate Generation. To delegate the signing capability to the proxy signer group $\mathcal{PS}$, an original signer A first generates a certificate for the proxy signer group by using Sakai *et al.*'s signature scheme

  1. Choose a random $x_a \in \mathbb{Z}_p^*$ and computes $U = x_a P$.
  2. Computes $V = x_a H_1(w, U) + d_A$ where w is a warrant, and broadcast U and V to all members in $\mathcal{PS}$.

- Proxy Shadow Generation. To generate secret shadows, the original signer A and each members B_i in $\mathcal{PS}$ perform the proxy shadow generation protocol as follows:

- Step1. The original signer A first choose a random polynomial $f(x) = x_a + \sum_{k=1}^{t-1} a_k x^k$ over $\mathbb{Z}_p[x]$ with $a_k \neq 0$ for each $k = 1, \dots, t-1$. Then he computes $A_k = a_k V, \hat{e}(P, A_k)$ for each $1 \leqslant k \leqslant t-1$, and $K_i = f(H_3(B_i))V + d_A$ for each $1 \leqslant i \leqslant n$, where n denotes the number of $\mathcal{PS}$. Finally, he publishes $\hat{e}(P, A_k)$'s to all members in $\mathcal{PS}$ and send K_i through a secure channel to B_i for each i.

  Each members B_i accepts K_i as a secret shadow if the following holds

  $$\hat{e}(P, K_i) \overset{?}{=} \hat{e}(U, V) \prod_{k=1}^{t-1} \hat{e}(P, A_k)^{H_3(B_i)^k}.$$

- Step2. To generate the other part of secret shadow, each proxy signer $B_j (1 \leqslant j \leqslant n)$ performs the following:
  1. Each B_j chooses a random $y_j \in \mathbb{Z}_p^*$, computes $W_j = y_j P$, and sends W_j to clerk B.
  2. After receiving all W_j's, clerk B computes $W = \sum_{j=1}^{n} W_j$, and broadcasts W to all members in $\mathcal{PS}$.
  3. Each B_j chooses a random polynomial $g_j(x) = y_j + \sum_{k=1}^{t-1} b_{j,k} x^k \in \mathbb{Z}_p[x]$ with $b_{j,k} \neq 0$ for all $k = 1, \dots, t-1$, computes $B_{j,k} = b_{j,k} V$ and $\hat{e}(P, B_{j,k})$, and publishes $\hat{e}(P, B_{j,k})$ to all members in $\mathcal{PS}$. With the polynomial $g_j(x)$, he computes $Y_{i,j} = g_j(H_3(B_i))V$ and sends it through a secure channel to B_i for each $1 \leqslant i \leqslant n$.
  4. After receiving $Y_{i,j} (1 \leqslant j \leqslant n)$, the member B_i accepts the $Y_{i,j}$ if the following equation holds:

     $$\hat{e}(P, Y_{i,j} = \hat{e}(P, y_j V) \prod_{k=1}^{t-1} \hat{e}(P, B_{j,k})^{H_3(B_i)^k}.$$

     Finally, he computes $Y_i = \sum_{j=1}^{n} Y_{i,j}$.

  Then (K_i, Y_i) is the secret shadow of the proxy signer B_i.

- Sign. To sign a message M, t members in the set $\mathcal{S}$ of proxy signers which are delegated by an original signer A perform the following protocol
  1. Each $C_i (1 \leqslant i \leqslant t)$ in $\mathcal{S}$ chooses a random $r_i \in \mathbb{Z}_p^*$, computes $R_i = r_i P, T_i = r_i d_{C_i}$, and broadcasts R_i and T_i to all other signers in $\mathcal{S}$
  2. After receiving all other $t-1$ R_j's and T_j's, each C_i computes $H = H_1(M, \sum_{i=1}^{t} R_i + \sum_{i=1}^{t} T_i), E_i = r_i P_{pub}$ and $S_i = r_i H + \ell_i (K_i + Y_i)$, where ℓ_i is the Lagrange coefficient $\prod_{j \neq i} \frac{-H_3(C_j)}{H_3(C_i) - H_3(C_j)}$, computes $\hat{e}(P, \ell_i(K_i + Y_i)$, and sends the partial signature (S_i, R_i, T_i, E_i) and $\hat{e}(P, \ell_i(K_i + Y_i)$ to clerk C.
  3. After receiving all partial signatures, clerk C generates the threshold signature on the message M as follows:
     (a) Compute $H = H_1(M, \sum_{i=1}^{t} R_i + \sum_{i=1}^{t} T_i)$.

(b) Verify whether each partial signature is valid

$$\begin{aligned}\hat{e}(P, S_i) &\overset{?}{=} \hat{e}(R_i, H)\hat{e}(P, \ell_i(K_i + Y_i), \\ \hat{e}(P, E_i + T_i) &\overset{?}{=} \hat{e}(R_i, P_{pub})\hat{e}(E_i, Q_{C_i}).\end{aligned}$$

(c) Compute $S = \sum_{i=1}^{t} S_i$.

The traceable threshold proxy signature on the message M is

$$\left(w, (U, V), \left(S, W, \{R_i\}_{i=1}^{t}, \{T_i\}_{i=1}^{t}\right)\right).$$

- Verify. Given a signature $(w, (U, V), (S, W, \{R_i\}_{i=1}^{t}, \{T_i\}_{i=1}^{t}))$ on message M, the verifier performs the following:

  1. Check if M conforms to the warrant w. If it does not conform then reject. Otherwise, continue on the next step.
  2. Verify the warrant w and the certificate (U, V) by

     $$\hat{e}(P, V) \overset{?}{=} \hat{e}(U, H_1(w, U))\hat{e}(P_{pub}, Q_A).$$

     If the above does not satisfied then reject. Otherwise, continue on the next step.
  3. Compute $R = \sum_{i=1}^{t} R_i, H = H_1(M, R + \sum_{i=1}^{t} T_i)$, and accept the signature if and only if the following equation holds:

     $$\hat{e}(P, S) = \hat{e}(R, H)\hat{e}(U, V)\hat{e}(P_{pub}, Q_A)\hat{e}(W, V).$$

- Trace. In case when a signature becomes controversial, the verifier sends the message M and the signature $(w, (U, V), (S, W, \{R_i\}_{i=1}^{t}, \{T_i\}_{i=1}^{t})$ to PKG, who is able to determine all the signers of the message by executing the following procedure:

  1. Verify the signature is valid.
  2. For each $i = 1, \ldots, t$, compute $O_i = (s^{-1} \bmod p)T_1$ and find C_i in $\mathcal{PS}$ such that $\hat{e}(H_2(C_i), R_i) = \hat{e}(O_i, P)$.
  3. Send $(O_1, \ldots, O_t)$ and $(C_1, \ldots, C_t)$ to the verifier as the proxy signers involved in the signature.

  Finally, the verifier can confirm the correctness of the signers by testing $\hat{e}(H_2(C_i), R_i) = \hat{e}(O_i, P)$

3 Analysis of the Liu-Huang scheme

In this section, we show that the anonymous threshold proxy signature scheme (scheme T) does not provide the *proxy signer's deviation* and *identifiability.* We first recall that, according to the paper [7], these are basic security requirements that their scheme satisfies: proxy signer's deviation means that, even if t or more poxy signers are colluding, they are not able to create a valid signature from which they are not traced, and identifiability is that one can determine the proxy signers from the trace tag in valid signatures (with the help of an authority). We also remark that, in the setting of the Liu-Huang scheme, a valid but untraceable signature will automatically violate both the requirements.

We assume that t members $B_1, \ldots, B_t$ collude as adversaries. First of all, we collect their proxy shadow K_i and compute $x_a V + d_A$ as follows:

$$\begin{aligned}
\sum_{i=1}^{t} \ell_i K_i &= \sum_{i=1}^{t} \prod_{j \neq i} \frac{-H_3(B_j)}{H_3(B_i) - H(B_j)} \left(f(H_3(B_i))V + d_A\right) \\
&= \sum_{i=1}^{t} \prod_{j \neq i} \frac{-H_3(B_j)}{H_3(B_i) - H(B_j)} f(H_3(B_i))V + \sum_{i=1}^{t} \prod_{j \neq i} \frac{-H_3(B_j)}{H_3(B_i) - H(B_j)} d_A \\
&= f(0)V + d_A = x_a V + d_A,
\end{aligned}$$

where we used the equation $\sum_{i=1}^{t} \ell_i = \sum_{i=1}^{t} \prod_{j \neq i} \frac{-H_3(B_j)}{H(B_i) - H(B_j)} = 1$.

Now, we can freely generate untraceable signatures on messages as follows:

1. Choose random values $\alpha \in \mathbb{Z}_p^*$, and $r_i, t_i \in \mathbb{Z}_p^*$ for each $i = 1, \ldots, t$.

2. Choose a message $\overline{M}$.

3. Compute

$$\begin{aligned}
\tilde{r} &= \sum_{i=1}^{t} r_i, \\
R_i &= r_i P, \quad R = \sum_{i=1}^{t} R_i = \sum_{i=1}^{t} r_i P = \tilde{r} P, \\
T_i &= t_i P, \quad T = \sum_{i=1}^{t} T_i = \sum_{i=1}^{t} t_i P, \\
W &= \alpha P, \\
S &= (x_a V + d_A) + \tilde{r} H_1(\overline{M}, R + T) + \alpha V.
\end{aligned}$$

4. Output $(w, (U, V)), (S, W, \{R_i\}_{i=1}^{t}, \{T_i\}_{i=1}^{t})$ as a signature for the message $\overline{M}$.

The correctness of the above attack can be verified directly: (w, U, V) is the legal certificate and the signature satisfies the following equation.

$$\begin{aligned}
\hat{e}(S, P) &= \hat{e}(x_a V + d_A, P) \hat{e}(\tilde{r} H_1(M, R + T), P) \hat{e}(dV, P) \\
&= \hat{e}(x_a V, P) \hat{e}(d_A, P) \hat{e}(H_1(\overline{M}, R + T), \tilde{r} P) \hat{e}(V, \alpha P) \\
&= \hat{e}(V, U) \hat{e}(Q_A, P_{pub}) \hat{e}(H_1(\overline{M}, R + T), R) \hat{e}(V, W).
\end{aligned}$$

Notice that no identity of the proxy signers is involved in the generation of the signature tags. Since we have selected random T_i's and R_i's that are irrelevant with the private keys d_{B_i}s of colluded proxy signers, the signature will avoid the trace procedure. This means that no one, as well as PKG, can detect the signers from the signature. Therefore, the Liu-Huang scheme does not satisfy proxy signer's deviation and identifiability.

4 Conclusion

Recently, Liu and Huang proposed an anonymous threshold proxy signature scheme, and claimed that their scheme has all the security requirements: unforgeability, verifiability, proxy signer's deviation, distinguishability, undeniability, and identifiability. In this paper, we have shown that their scheme does not provide the full security requirements such as proxy signer's deviation and identifiability.

References

[1] J. Baek and Y. Zheng, Identity-based threshold signature scheme from the bilinear pairings, Proceedings of the International Conference on Information Technology: Coding and Computing (IAS'04 track of ITCC'04), vol. 2, pp. 124-128, IEEE Computer Society, 2004.

[2] H. Bao, Z. Cao and S. Wang, Identity-based threshold proxy signature scheme with known signers, TAMC 2006, LNCS 3959, pp. 538-546, Springer-Verlag, 2006.

[3] Y.-F. Chang and C.-C. Chang, An RSA-based (t,n) threshold proxy signature scheme with freewill identities, Int. J. Information and Computer Security, vol. 1, no. 1/2, 2007.

[4] S. Guo, Z. Cao and R. Lu, An Efficient ID-Based Multi-proxy Multi-signature Scheme, In: Proceedings of the first International Multi-Symposiums on Computer and Computaional Sciences (IMSCCS 2006), vol. 2, pp. 81-88, IEEE Computer Society, 2006.

[5] H. Huang and C.C. Chang, An efficient and practical (t,n) threshold proxy signature scheme with known users, Fundamenta Informaticae, vol. 56, pp. 243-253, 2003.

[6] M.-S. Hwang, I.-C. Lin, and E. Lu, A secure nonrepudiable threshold proxy signarure scheme with known signers, Informatica, vol. 11. no. 2, pp. 137-144, 2000.

[7] J. Liu and S. Huang, Identity-Based Threshold Proxy Signature from Bilinear Pairings, Informatica, Inst. Math & Science, vol. 21, no. 1, pp. 41-56, IOS press, 2010.

[8] M. Mambo, K. Usuda and E. Okamoto, Proxy signature: delegation of the power to sign messages, IEICE Trans. Fundamentals E79-A(9), 1996, pp. 1338-1353.

[9] R. Sakai, K. Ohgishi, and M. Kasahara, Cryptosystems based on pairing, In: SCIS 2000, Okinawa, Japan, 2000, pp. 26-28.

[10] A. Shamir, How to share a secret, Communications of the ACM, vol. 22, no. 11, ACM Press, 1979, pp. 612-613.

[11] Q. Wang and Z. Cao, Indentity based proxy multi-signature, Journal of Systems and Software, vol. 80, no. 7, pp. 1023-1029, 2007.

[12] W. Wu, Y. Mu, W. Susilo, J. Seberry and X. Huang, Identity-based proxy signature from pairings, In: The 4th International Conference on Autonomic and Trusted Computing (ATC 2007), LNCS 4610, pp. 22-31, Springer-Verlag, 2007.

[13] J. Xu, Z. Zhang and D. Feng, Identity based threshold proxy signature, Cryptology ePrint Archive, Report 2004/250.

[14] J. Xu, Z. Zhang and D. Feng, ID-based Proxy Signature Using Bilinear Pairings, In: Parallel and Distributed Processing and Applications (ISPA 2005), LNCS 3759, pp. 359-367, Springer-Verlag, 2005.

[15] L. Yi, G. Bai and G. Xiao, Proxy multi-signature scheme: A new type of proxy signature scheme, Electronic Letters, vo. 36. no. 6, pp.527-528, 2000.

[16] K. Zhang, Threshold Proxy Signature Schemes, In Information Security Workwhop (ISW'97), pp. 191-197, 1997.

[17] F. Zhang and K. Kim, Efficient ID-based blind signature and proxy signature from bilinear pairings, ACISP 2003, LNCS 2727, pp. 312-323, Springer-Verlag, 2003.