INFORMATICA, 2000 Vol. 0, No. 0, 1–0

A SECURE NONREPUDIABLE THRESHOLD PROXY SIGNATURE SCHEME WITH KNOWN SIGNERS

Min-Shiang Hwang, Iuon-Chang Lin, Eric Jui-Lin Lu

Department of Information Management
Chaoyang University of Technology
168, Gifeng E. Rd., Wufeng,
Taichung County, TAIWAN 413, R.O.C.
Fax: 886-4-3742337 E-mail: mshwang@mail.cyut.edu.tw

Abstract.

In the (t, n) proxy signature scheme, the signature, originally signed by a signer, can be signed by t or more proxy signers out of a proxy group of n members. Recently, an efficient nonrepudiable threshold proxy signature scheme with known signers was proposed by H.-M. Sun. Sun's scheme has two advantages. One is nonrepudiation. The proxy group cannot deny that having signed the proxy signature. Any verifier can identify the proxy group as a real signer. The other is identifiable signers. The verifier is able to identify the actual signers in the proxy group. Also, the signers cannot deny that having generated the proxy signature. In this article, we present a cryptanalysis of the Sun's scheme. Further, we propose a secure, nonrepudiable and known signers threshold proxy signature scheme which remedies the weakness of the Sun's scheme.

Key words: Cryptography, Lagrange interpolating polynomial, Proxy signature, Threshold proxy signature.

1. Introduction A proxy signature scheme is a method which allows original signer delegates his works to a designated person with a proxy signature key (Mambo, 1996-a, Mambo, 1996-b, Usuda, 1996). In these schemes, the proxy signature key is created by the original signer's signature key which cannot be computed from the proxy signature key. The proxy signer can generate proxy signature on a message on behalf of the original signer.

To further expand the proxy signature scheme, the (t, n) threshold proxy signature schemes were proposed (Kim, 1997, Lee, 1998, Zhang, 1997). The original signer now shares the proxy signature key with an authorized proxy group. Any t or more proxy signers of the proxy group of n members can co-operately generate a proxy signature on a message. Some threshold proxy signature schemes, such as Zhang's scheme (Zhang, 1997), are not nonrepudiable. Although some threshold proxy signature schemes, such as the Kim's scheme (Kim, 1997), are nonrepudiable, they suffer a severe limitation; that the verifier cannot identity the actual signers in the proxy group.

Based on Kim's scheme, H.-M. Sun proposed an efficient nonrepudiable threshold proxy signature scheme with known signer (Sun, 1999). The Sun's scheme is more efficient than the other threshold proxy signature schemes, and has nonrepudiable property. The main advantage of Sun's scheme is that the verifier is able to identify the actual signers in the proxy group. The security of the Sun's scheme is based on Lagrange interpolating polynomial and the difficulty of calculating discrete logarithms. However, the weakness of the Sun's scheme is that, if an adversary can obtain the proxy signer's secret key. Then he can impersonate a legal proxy signer to generate a proxy signature and the real proxy signer cannot deny that having signed the proxy signature before.

In this article, we show the weakness of the Sun's scheme and remedy the Sun's scheme. In next section, we review the Sun's scheme and illustrate its weakness. In Section 3, we propose a new secure scheme based on the Sun's scheme. And the security of our proposed scheme is analyzed. Finally, we conclude this paper by listing the advantages of the proposed scheme.

2. Review of Sun's nonrepudiable threshold proxy signature scheme In this section, we first review the Sun's threshold proxy signature scheme (Sun, 1999) and then present a weakness of the Sun's scheme.

2.1. Sun's (t, n) threshold proxy signature scheme The Sun's proposed nonrepudiable (t, n) threshold proxy signature with known signer, which is based on the Kim's threshold scheme (Kim, 1997). The Sun's scheme uses the secret share technique (Blakley, 1979, Shamir, 1979) to share the proxy signature key. It is divided into three phases: proxy sharing generation, proxy signature issuing, and proxy signature verification. Initially, the system parameters are defined as follows:

- p be a large prime, q be a prime factor of $p-1$, g be an element of order q in Z_p^*;
- x_i is participant $p_i's$ private key and its corresponding public key is $y_i,\ y_i = g^{x_i}\ (mod\, p)$;

- h is an one-way function;
- m_w is a warrant that be minted by the original signer, and its records some information such as the identity of the original signer; the identities of proxy signers of the proxy group; etc. and
- $ASID$ (Actual Signers' ID) records the identities of the actual signers.

In the proxy sharing generation phase, the group shares a secret value from multiplicative sharing technique. The steps are described as follows:

1. (Group key generation) In a (t, n) threshold proxy signature scheme, let p_0 be the original signer, and $p_1, p_2, \cdots, p_n$ be the n proxy signers of the proxy group. Each member, $p_1, p_2, \cdots, p_n$, randomly generates a secret polynomial f_i of degree $t-1$, which $f_i(X) = x_i + a_{(i,1)}X + \cdots + a_{(i,t-1)}X^{t-1}$ $(mod\ q)$. Here, $a_{(i,1)}, a_{(i,2)}, \cdots, a_{(i,t-1)}$ are random number. Then, each proxy signer p_i can receive the shared value $f_j(i)$ from p_j, where $0 < i, j < n$, and $i \neq j$. Therefore, each proxy signer p_i can obtain a value s_i,

$$\begin{aligned} s_i &= f(i) \\ &= f_1(i) + f_2(i) + \cdots + f_n(i) \\ &= a_0 + a_1 i + \cdots + a_{t-1} i^{t-1} \pmod q, \end{aligned} \tag{1}$$

where $a_0 = \sum_{i=1}^{n} x_i$ $(mod\ p)$, $a_1 = \sum_{i=1}^{n} a_{(i,1)}$ $(mod\ p)$, $\cdots$, $a_{t-1} = \sum_{i=1}^{n} a_{(i,t-1)}$ $(mod\ p)$. And the public parameters of the proxy group (Pedersen, 1991-a, Pedersen, 1991-b) are $y_G = g^{a_0}$ $(mod\ p)$, and $A_j = g^{a_j}$ $(mod\ p)$,

$j = 1, \cdots, t-1$.

2. (Proxy generation) The original signer chooses a random number k and computes the parameter K, $K = g^k \ mod\, p$. Then the original signer can obtain the value σ,

$$\sigma = ex_0 + k \pmod q, \tag{2}$$

where $e = h(m_w, K)$.

3. (Proxy sharing) The original signer shares a proxy key σ in a (t, n) threshold scheme. He generates a secret degree $t-1$ polynomial f', and computes

$$\begin{aligned} \sigma_i &= f'(i), \text{ for } i = 1, 2, \cdots, n, \\ &= \sigma + b_1 i + \cdots + b_{t-1} i^{t-1}, \end{aligned} \tag{3}$$

where b_j is a random number, $j = 1, \cdots, t-1$. After the original signer sends σ_i to proxy signer p_i, $i = 1, \cdots, n$, over a secured channel, and publishes $B_j = g^{b_j} \ (mod\, p)$, $j = 1, \cdots, t-1$, and (m_w, K).

4. (Proxy share generation) After receiving the σ_i, each proxy signer p_i checks whether or not the following equation is hold,

$$g^{\sigma_i} = y_0^{h(m_w, K)} K \prod_{j=1}^{t-1} B_j^{i^j} \pmod p. \tag{4}$$

If the above equation is hold, each p_i computes

$$\sigma_i' = \sigma_i + s_i \cdot h(m_w, K) \pmod q, \tag{5}$$

the σ'_i as a proxy share of p_i. Otherwise, the proxy signer rejects σ_i.

Assume that the t proxy signers, $p_1, \cdots, p_t$, want to cooperately sign a message on behalf of the proxy group, the steps of the proxy signature issuing phase are listed below:

1. As the step 1 of the proxy share generation phase, the polynomial is using $f_i"(X) = (c_{(i,0)} + x_i) + c_{(i,1)}X + \cdots + c_{(i,t-1)}X^{t-1}\ (mod\, q)$. Each actual proxy signer p_i can obtain the value s'_i when they receive the values $f_j"(i)$ from each actual proxy signer p_j, as shown in following:

$$\begin{aligned} s'_i &= f"(i) \\ &= f_1"(i) + f_2"(i) + \cdots + f_t"(i) \\ &= \sum_{i=1}^{n} x_i + c_0 + c_1 i + \cdots + c_{t-1} i^{t-1}\ (\mathrm{mod}\ q), \end{aligned} \tag{6}$$

where $i = 1, \cdots, t$. The public parameters of this step are $Y = g^{c_0}\ (mod\, p)$, and $C_j = g^{c_j}\ (mod\, p)$, $j = 1, \cdots, t-1$.

2. Each proxy signer p_i, $i = 1, \cdots, t$, has two secret values σ'_i and s'_i. Therefore, each proxy signer p_i can computes

$$\gamma_i = s'_i Y + \sigma'_i h(ASID, m)\ (\mathrm{mod}\ q), \tag{7}$$

where m is the message. Then each proxy signer p_i sends γ_i to proxy signer p_j, $j = 1, \cdots, t$ and $j \neq i$.

3. For each received γ_j $(j = 1, \cdots, t; j \neq i)$, p_i can check whether the

following equation is hold

$$g^{\gamma_j} = [Y(\prod_{i=1}^{t-1} C_i^{j^i})(\prod_{i=1}^{t-1} y_i)]^Y \times$$
$$[(y_0^{h(m_w,K)} K \prod_{i=1}^{t-1} B_i^{j^i})(y_G \prod_{i=1}^{t-1} A_i^{j^i})^{h(m_w,K)}]^{h(ASID,m)} \mod p. \quad (8)$$

4. Each proxy signer p_i can apply Lagrange formula to $[\gamma_j]$ to compute(Denning, 1983)

$$T = f\text{"}(0)Y + [f(0) + f'(0)]h(ASID, m). \quad (9)$$

The proxy signature on m is $(m, T, K, m_w, ASID)$.

In the verification phase, 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 gets the public keys of the proxy signers from the CA, and knows who the original signer and the actual proxy signers are.

2. The verifier then checks the validity of the proxy signature on the message m from the following equation:

$$g^T = [y_0^{h(m_w,K)} K \prod_{t=1}^{n} y_i]^{h(ASID,m)} (Y \prod_{i=1}^{t} y_i)^Y \pmod p. \quad (10)$$

2.2. The weakness of Sun's scheme In Sun's (t, n) threshold proxy signature scheme, any verifier can verify the validity of the proxy signature and identify the actual signers. However, in this subsection we will show that the proxy signer's secret key is not kept in privacy. Any $(n-1)$ proxy signers in the group of n members can conspire the secret key of the remainder one. We call this attack as *collusion attack*. In this attack, any $(n-1)$ proxy signers in the group of n members can impersonate the remainder one.

For example, assume that a $(3,5)$ threshold proxy signature scheme. The proxy signer $p_1, \cdots, p_4$ intend to obtain the secret key of the proxy signer p_5. Then, they can impersonate a legal proxy signer p_5 to sign a message m. In Equations (1), any 3 proxy signers of $p_1, \cdots, p_4$ can compute a_0 using the Lagrange formula since $a_0 = \sum_{i=1}^{5} x_i \ (mod\, p)$. Thus the proxy signers $p_1, \cdots, p_4$ can present their secret keys to conspire the secret key x_5 of the proxy signer p_5 easily. Next, we can impersonate the proxy signer p_5 to generate a legal proxy signature.

In the same way, the s_5, σ_5, and σ_5' can be computed by using Lagrange formula from the Equations (1), (3), and (5), respectively. In proxy signature issuing phase, we can impersonate p_5 to share a random number as described in step 1, and we can get a secret s_5' from Equation (6). By having s_5' and σ_5', we can obtain γ_5 from Equation (7) and send it to other proxy signers of the proxy group. Then T can be computed from Equation (9) and, thus, the proxy group can generate a proxy signature $(m, T, K, m_w, ASID)$ for message m.

In the verification phase, the verifier can verify the validity of the proxy signature and identify the p_5 as actual signer of the proxy group. In fact, p_5 have never signed the message m, but p_5 cannot deny. Therefore, in Sun's scheme, the secret key x_i of the proxy signer p_i can be compromised by collusion attack and an adversary can impersonate a legal proxy signer p_i to sign a message.

3. Improvement of Sun's scheme In this section, we modify Sun's scheme to remedy the weakness as described in Section (2.2) and analyze the security of our scheme.

3.1. The improved scheme In Sun's scheme, the secret key x_i can be compromised by collusion attack. To remedy the weakness we modify Sun's scheme and the revised scheme is presented in details.

In the proxy share generation phase, we replace $f_i(X)$ with $f_i(X) = x_i + a_{(i,0)} + a_{(i,1)}X + \cdots + a_{(i,t-1)}X^{t-1}\ (mod\ q)$, where $a_{(i,0)}$ is a random number. Therefore, the Equation (1) becomes

$$\begin{aligned} s_i &= f(i), \\ &= \sum_{i=1}^{n} x_i + a_0 + a_1 i + \cdots + a_{t-1} i^{t-1} (\bmod\ q), \end{aligned} \tag{11}$$

where $a_i = \sum_{i=1}^{t-1} a_{(i,0)}\ (mod\ p)$. The proxy group then publishes y_g ($y_G = \prod_{i=1}^{n} g^{x_i} = \prod_{i=1}^{n} y_i\ (mod\ p)$), and A_j ($A_j = g^{a_j}\ (mod\ p);\ j = 0, \cdots, t-1$). The other steps of the proxy share generation phase are the same as that of the Sun's scheme.

In the proxy signature issuing phase, the proxy signer p_i computes γ_i from Equation (7) and sends γ_i to other proxy signers of the proxy group. Each proxy signer can verify the validity of γ_i from the following equation:

$$\begin{aligned} g^{\gamma_j} = {} & [Y(\prod_{i=1}^{t-1} C_i^{j^i})(\prod_{i=1}^{t-1} y_i)]^Y \times \\ & [(y_0^{h(m_w,K)} K \prod_{i=1}^{t-1} B_i^{j^i})(y_G A_0 \prod_{i=1}^{t-1} A_i^{j^i})^{h(m_w,K)}]^{h(ASID,m)} \pmod p. \end{aligned}$$

Then, each signer computes T from Equation (9) and the proxy signature on message m is $(m, T, K, m_w, ASID)$.

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

$$g^T = [y_0^{h(m_w,K)} K A_0 \prod_{t=1}^{n} y_i]^{h(ASID,m)} (Y \prod_{i=1}^{t} y_i)^Y \pmod p. \tag{12}$$

If the above equation is hold, the verifier can firmly believe the validity of the proxy signature and identify the actual signers.

Furthermore, the revised scheme can withstand the collusion attack. Any $n-1$ proxy signers cannot conspire the secret key of the remainder. Therefore, the secret key of any proxy signer can be kept in privacy. And any adversary cannot forge the legal proxy signature.

3.2. Security analysis of the improved scheme The security of the proposed threshold proxy signature scheme as described above is examined. As with Sun's scheme, the level of security is tightened. However, our scheme can withstand the collusion attack. Assume that we use the same example as described in Section (2.2). Any 3 proxy signers can obtain the $f(0) = \sum_{i=1}^{5}(x_i + c_{(i,0)})\ (mod\, p)$ by Lagrange formula. However, any 4 proxy signers, $p_1, \cdots, p_4$, can only obtain $x_5 + c_{(5,0)}$. They cannot conspire the secret key x_5 of proxy signer p_5. Therefore, collusion attack is impossible since it is difficult to compute the secret key x_5 from the addition of two unknown numbers x_5 and $c_{(5,0)}$.

The secret key of the proxy signer in the proposed scheme is kept in privacy. In addition, we can conspire to get the σ_5, and σ_5' from Equation (3), and (5). However, an adversary cannot obtain valid s_5 and S_5' without p_5' secret key. If an adversary tries to forge a proxy signature of p_5, the verify check in the Equation (10) is not hold. Therefore, it can withstand the collusion attack and the proxy signature cannot be forged.

4. Conclusions In this article, we presented a cryptanalysis of Sun's threshold proxy signature scheme. We have shown that the secret key can be compromised by collusion attack. And a secure threshold proxy signature scheme was proposed to remedy the weakness of Sun's scheme. The main advantages of our scheme are:

- it obtains the property of nonrepudiable,
- the verifier is able to identify the actual proxy signer of the proxy group, and

- anyone cannot 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, R.O.C., under contract no. NSC89-2213-E-324-025.

REFERENCES

Blakley, G.R. (1979). Safeguarding cryptographic keys. *Proc. of AFIPs 1979*, 313–317.

Denning, D.E.R. (1983). Cryptography and data security. *Addison-Wesley*.

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

Lee, N.Y., T. Hwang, and C.H. Wang (1998). On Zhang's nonrepudiable proxy signature schemes. *ACISP'98, LNCS 1438*, 415–422.

Mambo, M., K. Usuda, and E. Okamoto (1996-a). Proxy signatures: Delegation of the power to sign message. *IEICE Trans. Fundamentals*, textbfE79-A(9), 1338–1354.

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

Pedersen, T.P. (1991-a). Distributed provers with applications to undeniable signatures. *Proc. Eurocrypt'91, LNCS 547*, 221–238.

Pedersen, T.P. (1991-b). A threshold cryptosystem without a trusted party. *Proc. Eurocrypt'91, LNCS 547*, 522–526.

Shamir, A. (1979). How to share a secret. *Commun. of the ACM*, **22**(11), 612–613.

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

Usuda, K., M. Mambo, T. Uyematsu, and E. Okamoto (1996). Proposal of an automatic signature scheme using a compiler. *IEICE Trans. Fundamentals*, **E79-A**(1), 94–101.

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

Min-Shiang Hwang received the B.S. in Electronic Engineering from National Taipei Institute of Technology, Taipei, Taiwan, Republic of China, in 1980; the

M.S. in Industrial Engineering from National Tsing Hua University, Taiwan, in 1988; and the Ph.D. in Computer and Information Science from National Chiao Tung University, Taiwan, in 1995. He also studied Applied Mathematics at National Cheng Kung University, Taiwan, from 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.

Iuon-Chang Lin received the B.S. in Computer and Information Sciences from Tung Hai University, Taichung, Taiwan, Republic of China, in 1998. He is currently pursuing his master degree in Information Management from Chaoyang University of Technology. His current research interests include electronic commerce, information security, cryptography, and mobile communications.

Eric Jui-Lin Lu received his B.S. degree in Transportation Engineering and Management from National Chiao Tung University, Taiwan, R.O.C, in 1982; M.S. degree in Computer Information Systems from San Francisco State University, California, U.S.A, in 1990; and Ph.D. degree in Computer Science from University of Missouri-Rolla, Missouri, U.S.A, in 1996. He is currently an associate professor and vice chairman of the Department of Information Management, Chaoyang University of Technology, Taiwan, R.O.C. His current research interests include electronic commerce, distributed processing, and security.