EFFICIENT UNDENIABLE THRESHOLD PROXY SIGNATURE SCHEME

Sattar J Aboud and Sufian Yousef

Telecommunications Engineering Research Group
Anglia Ruskin University, UK
sattar_aboud@yahoo.com

Abstract

The threshold proxy signature scheme allows the original signer to delegate a signature authority to the proxy group member to cooperatively sign message on behalf of an original signer. In this paper, we also propose a new scheme which includes the features and benefits of the RSA scheme which is a popular security technique. Also, we will evaluate a security of undeniable threshold proxy signature scheme with known signers. We find that the existing threshold proxy scheme is insecure versus the original signer forgery. We also demonstrate that a threshold proxy signature suffers from a conspiracy of an original signer and a secret share dealer, and that the scheme is commonly forgeable, and cannot offer undeniable. We claim that the proposed scheme offers the undeniable characteristic.

Key Words - Cryptography; digital signature; proxy signature; threshold proxy signature.

1 INTRODUCTION

In the proxy signature scheme, the original signer delegates the user entitled the proxy signer to sign message on its behalf. Since Mambo et al. presented a thought of a proxy signature [1], various proxy signature schemes are suggested [2]. According to a type of delegation, a proxy signature is categorized as full delegation, partial delegation and delegation by warrant. In full delegation, an original signer passes its private key as a proxy signature key to a proxy signer by the secure channel.

In partial delegation, a proxy signer has the proxy signature key from a proxy signer secret key and the delegation key passed by an original. A delegation key is created by an original with the trap-door permutation of an original signer secret key. A proxy signature is dissimilar of an original and a proxy typical signature. In delegation by certificate, an original signer employs its typical signature scheme to sign the warrant that records a kind of information delegated, an original signer and a proxy signer identities and a period of delegation. The signature of a warrant is entitled certificate that stops a passing of proxy power to the trusted authority.

Combined with delegation by certificate, a partial delegation can be altered into the partial delegation by warrant. A partial delegation by warrant can offer sufficient security and efficiency. For simplicity, we denote that a partial delegation by warrant a proxy signature. Mambo et al. proxy signature scheme satisfy a characteristic of no one except an original signer and a proxy signer can generate the valid proxy signature on behalf of an original signer. In 2001, Lee et al. [3] enhanced a security characteristic of a proxy signature by generate the valid proxy signature and someone else, even an original signer, cannot create the valid proxy signature. So, for the valid proxy signature, a proxy signer cannot repudiate signed a message and an original signer cannot repudiate delegated a signing authority to a proxy signer. Namely, a proxy signature scheme has a security characteristic undeniable.

2 RELATED WORKS

Based on a secret sharing scheme and threshold algorithm [4], Zhang et al. suggested a threshold proxy signature scheme [5]. In (t, n) threshold proxy signature scheme, the proxy signature key is shared among a subset of n proxy signers where at least t proxy signers can cooperatively sign documents on behalf of an original signer. To avoid argument regarding who is a proxy signer, Sun [6] suggested the undeniable threshold proxy signature scheme with known signers. Sun scheme reduces Kim et al. scheme drawbacks that a verifier is incapable to verify if a proxy group key is created by an authorized proxy group. But, Hsu et al. [7] illustrated that Sun scheme is weak since any t or more than t proxy signers can get the private keys of other proxy signers. In 2003, Yang et al. [8] proposed an enhancement on Hsu et al. scheme. Yang et al. scheme is more efficient regarding the communication cost and timing complexity. In 2004, Tzeng et al. [9] obtained that in Hwang et al. scheme, a malicious original signer can forge a threshold proxy signature without an agreement of the proxy signers. Tzeng et al. also built the undeniable threshold proxy signature scheme with known signers and claimed the suggested scheme enhanced a security of Hwang et al. scheme. In 2006, Yuan Yumin [10] introduced a threshold proxy signature scheme with non-repudiation and anonymity. Yuan Yumin claims that the scheme with any verifier can check whether the authors of the proxy signature belong to the designated proxy group by the original signer, while outsiders cannot find the actual signers. In 2007, Qi Xie et al., [11] claims that their scheme made an improvement of undeniable_threshold multi-proxy threshold scheme with shared verification. In 2009, Hu and Zhang [12] presented a cryptanalysis and improvement of a threshold proxy signature scheme with undeniable.

The remainder of this paper is organized as follows. In Section 3, we will provide some notations and reconsider Pedersen threshold distributed key generation protocol [13]. In Section 4, we will analysis a security of Sun et al. threshold proxy signature scheme. In Section 5 we will describe the proposed scheme. Finally, conclusions are in Section 6.

3 PRELIMINARIES

In this Section, we will provide some notations used thorough the paper and also reconsider Pedersen threshold distributed key generation scheme.

3.1 Notations Used

In this section, we provide the notations which are used thorough this paper.

p, q: Two large prime numbers where $q / p-1$.

g: Generator of Z_p^* its order is q

O: Original signer

$P_1, P_2, ..., P_n$:The n proxy signer

d_O : Private Key of an original singer O

e_O : Public key of an original signer O

d_i : Private Key of a proxy signer P_i

e_i : Public key of a proxy signer P_i

$h(.)$: Secure hash function.

$\|$: Concatenation operation

id : The identity of the proxy signer

m_w :a warrant which records information delegated, an original signer and a proxy signer identities with a period of delegation.

3.2 Pedersen Threshold Distributed Key Generation Protocol

Pedersen threshold distributed key generation scheme contains n Feldman (t, n) verifiable secret sharing schemes [14]. Suppose $(P_1, P_2, ..., P_n)$ are n players. Pedersen scheme includes the following three stages.

1. Every player P_i arbitrarily selects a polynomial $f_i(z)$ over Z_q of degree $t-1$.

$$f_i(z) = a_{i0} + a_{i1}z + a_{i2}z^2 + ... + a_{i,t-1}z^{t-1} \quad (1)$$

P_i Transmit $b^{a_{i0}}, b^{a_{i1}}, ..., b^{a_{i,t-1}}$. Then P_i finds and passes $f_i(j) \bmod q$ to P_j such that $j = 1,2,...,n$ where $j \neq i$ in the secure channel.

2. Every P_j check a validity of a share $f_i(j) \bmod q$ by verifying for $i = 1,2,...,n$,
$b^{f_i(j)} = b^{a_{i0}} (b^{a_{i1}})^j (b^{a_{i2}})^{j^2} ... (b^{a_{i,t-1}})^{j^{t-1}} \bmod p$

When all $f_i(j)$ are checked to be certified, P_j finds $x_j = \sum_{i=1}^{n} f_i(j) \bmod q$ as his share.

3. Assume that $f(z) = a_0 + a_1 z + a_2 z^2 + ... a_{t-1} z^{t-1} \bmod q = \sum_{i=1}^{n} f_i(z) \bmod q$. Where, $a_r = \sum_{i=1}^{n} a_{ir} \bmod q$

for $0 \le r \le t-1$, and $x_i = f(i) \bmod q$. So $w = \sum_{i=1}^{n} x_i \bmod q$ when any t secret shares, say

$w_1, w_2, ..., w_t$ are Lagrange interpolating polynomial: $w = f(0) = \sum_{i=1}^{i=t-1} s_i \prod_{j=1, j \ne i}^{t-1} \frac{0-j}{i-j} \bmod q$ (2)

The validity of the reconstructed private key w can be checked by the following formula

holds: $b^w = \prod_{i=1}^{i=n} b^{a_{i0}} \bmod p$ (3)

4 SECURITY OF THRESHOLD PROXY SIGNATURE SCHEME

We will describe some threshold proxy signature schemes which are follows:

4.1 Sun et al. Scheme

The first scheme we will describe the Sun scheme as follows:

A. Description of Sun Scheme

First, we will describe Sun threshold proxy signature scheme as follows:

Secret Share Generation Phase

In this phase, a proxy group $(P_1, P_2, ..., P_n)$ wants to create a group of private and public key pair $(w, e_1) \in Z_q^* \times Z_p$. A proxy group run Pedersen threshold distributed key generation protocol as described in Section 2. Every player P_i uses $f_i(z) = d_i + a_{i1} z + a_{i2} z^2 + ... + a_{i,t-1} z^{t-1}$

So, a private key shared by a proxy group is $w = \sum_{i=1}^{n} d_i$ and a related public key is

$e_i = \prod_{i=1}^{n} e_i \bmod p$. Every proxy signer P_i gets a secret key share $x_i = f(i) = \sum_{j=1}^{n} f_j(i) \bmod q$.

Suppose $u_j = b^{a_j} \bmod p, j = 1,2,...,t-1$.

Proxy Share Generation Phase

In this phase, an original signer O creates a proxy share as follows.

Step 1: Original Signer O

1. arbitrarily selects $r \in Z_q$
2. find $l = b^r \bmod p$
3. Compute proxy $k = d_O h(m_w \| l) + r \bmod q$.
4. Allocate a proxy key k between a proxy groups by implementing Feldman scheme.
5. arbitrarily selects polynomial of degree $t-1$: $f^-(z) = k + g_1 z + g_2 z^2 + ..., + g_{t-1} z^{t-1} \bmod q$
6. finds and privately passes $k_i = f^-(i) \bmod q$ to a proxy signer P_i for $i = 1,2,...,n$
7. declares (m_w, l) and $v_j = b^{g_j} (j = 1,2,...,t-1)$

Step 2: Proxy Signer P_i

1. accepts (k_i, m_w, l) when a formula $b^{k_i} = e_O^{h(m_w\|l)} l \prod_{j=1}^{t-1} v_j^{i^j} \bmod p$ correct
2. Find $k_i^{-} = k_i + x_i h(m_w \| l) \bmod q$ as a proxy share.

Proxy Signature Generation Phase

Suppose that $(P_1, P_2, ..., P_t)$ as an actual proxy group signs a document m as follows:

1. The t proxy signer runs Pedersen threshold distributed key generation protocol for sharing value $c_O = \sum_{i=1}^{t} c_{i,O}$ using $f_i^{=}(z) = (c_{i,O} + d_i) + c_{i,1} z + c_{i,2} z^2 + ..., + c_{i,t-1} z^{t-1} \bmod q$.
2. Each P_i for $i = 1,2,...,t$ gets the public key $y = b^{c_O} \bmod p$ and a private arbitrary value share $x_i^{-} = f^{=}(i) = \sum_{i=1}^{t} d_i + c_O + c_1 i + c_2 i^2 + ... + c_{t-1} i^{t-1} \bmod q$ such that $c_j = \sum_{i=1}^{t} c_{ij}$ for $1 \le j \le t-1$
3. Each, P_i finds proxy signature share $s_i = x_i^{-} y + k_i^{-} h(id \| m) \bmod q$
4. Pass s_i to proxy signers $P_j = (j = 1,2,...,t, j \ne i)$ in the secure channel.
5. Each P_j can check a validity of s_i by verifying when the following formula correct:
6. $$b^{s_i} = \left[y \left(\prod_{j=1}^{t-1} c_j^{i^j} \right) \left(\prod_{j=1}^{t} e_j \right) \right]^{y} \left[(l_{e_O}^{h(m_w\|l)} \prod_{j=1}^{t-1} v_j^{i^j}) \left(e_1 \prod_{j=1}^{t-1} u_j^{i^j} \right)^{h(m_w\|l)} \right]^{h(id\|m)} \bmod p$$
7. Every proxy signer in actual proxy group can creates $s = f^{=}(0) y + (f(0) + f^{-}(0)) h(id \| m)$ by a Lagrange interpolation formula to s_i.
8. The proxy signature on m is (m, m_w, l, id, y, s).

Proxy Signature Verification Phase

The verifier can identify an original signer and an actual proxy signers from m_w, and id, and validate a proxy signature by verifying when

$$b^{s} = \left[l_{e_O}^{h(m_w\|l)} \prod_{i=1}^{n} e_i \right]^{h(id\|m)} \left(y \prod_{i=1}^{t} e_i \right)^{y} \bmod p \qquad (4)$$

B. *Cryptanalysis of Sun Threshold Proxy Signature Scheme*

In this subsection, we illustrate that Sun scheme is weak against an original signer forgery. Since the malicious original signer can create the proxy signature on every document and claim that any t proxy signers can be actual proxy signers of a proxy signature. Assume a message m, an original signer O arbitrarily selects the proxy group (thus, O selects id).

1. Suppose that O imitates proxy signers $(P_1, P_2, ..., P_t)$.
2. Then O finds $l = (\prod_{i=1}^{n} e_i)^{-1} g^{a} \bmod p$ where $y = (\prod_{i=1}^{t} e_i)^{-1} b^{v}$, such that $a \in Z_q, v \in Z_q$.
3. Then, O finds: $s = (a + d_O h(m_w \| l)) h(id \| m) + vy \bmod q$ (5)
4. So (m, m_w, l, id, y, s) is the valid proxy signature on message m since

$$b^{s} = b^{(a + d_O h(m_w\|l)) h(id\|m) + vy} \bmod p$$
$$= b^{a} b^{d_O h(m_w\|l) h(id\|m)} (b^{v})^{y} \bmod p$$

$$= \left(l_{e_O}^{h(m_w\|l)} \prod_{i=1}^{n} e_i \right)^{h(id\|m)} (y \prod_{i=1}^{t} e_i)^y \bmod p$$

5. THE PROPOSED SCHEME

The suggested scheme combines theta $\theta(n)$ and an elimination of a computation of inverse in RSA scheme if we calculate a value of Lagrange coefficient. Also, we suggest an equation to find a result of message warrant m_w. Suppose that $N_O < N_i \, (i = 1,2,...,n)$.

5.1 The Proxy Sharing Phase

The steps of the proxy sharing phase are as follows:

Step 1: Proxy Generation

The original signer O must do the following:

1. Find a group proxy signing key $d_1 = d_O^{m_w} \bmod \theta(N_O)$
2. Find the proxy verification key $e_1 = e_O^{m_w} \bmod \theta(N_O)$
3. Compute $m_w = (P + T + r)^T \bmod \theta(N_O)$ such that P is a validity period of proxy signature and T is a sum of identities of $P_O = P_1, P_2, ..., P_n$
4. Declare $(m_w, e_1, (m_w, e_1)^{d_O} \bmod N_O$

Step 2: Proxy Sharing

The original signer O must do the following:

1. Choose $t-1$ degree polynomial $f(x) = d_1 + a_1 x + ... a_{t-1} x \bmod N_O$, such that $a_1, a_2, ..., a_{t-1}$, are an arbitrary integers.
2. Compute a proxy singer P_i partial proxy signing key $k_i = f(i)$
3. Pass $((k_i)^{d_O} \bmod N_O, k_i)^{e_i} \bmod N_i$ to a proxy signer P_i .

Step3: Proxy Share Generation.

The proxy signer P_i must do the following:

1. Receive $((k_i)^{d_O} \bmod N_O, k_i)^{e_i} \bmod N_i$
2. Obtain $((k_i)^{d_O} \bmod N_O, k_i)$ by his secret key d_i
3. Verify a validity of k_i and keeps it secret.

5.2 The Proxy Signature Issuing Phase

Suppose that T indicate the group members including any t proxy signers who desire to create the proxy signature on a message m on behalf of P_O cooperatively.

Step 1: Proxy Signer P_i

Every proxy signer P_i uses a partial proxy signing key k_i to do the following:

1. Create a partial signature $s_i = m^{k_i} \bmod N_O$
2. Pass $((s_i, i)^{d_i} \bmod N_i, s_i$ to a combiner.

Step 2: The Combiner

The combiner must do the following:

1. Receive partial signature s_i from P_i
2. Check the validity of a partial proxy signature by verifying if $(s_i, i)^{d_i e_i} \bmod N_i = (s_i, i)$.
3. Find $v = \prod_{id_a, id_b \in T} id_a - id_b$ such that $a > b$

4. Find $L_i = \prod_{id_a,id_b \in T}(id_a - id_b)\prod_{j=1, j\neq i}^{t}\frac{-id_j}{id_i - id_j}$ where $\prod_{j=1, j\neq i}^{t}(id_i - id_j)$ a factor of $\prod_{id_a,id_b \in T}(id_a - id_b)$.

   Thus, L_i is integer and a combiner require not calculating inverse of $\prod_{j=1, j\neq i}^{t}(id_i - id_j)$.
5. Create a signature $s = \prod_{i \in T} s_i^{L_i} \bmod N_O$
6. The result of proxy signature is (v, s).

5.3 The Proxy Signature Verification Phase

The steps of this phase are as follows:

1. A verifier can check a signature signed on behalf of an original signer by a formula $s^{e_1} = m^v \bmod N_O$
2. An original signer can distinguish a proxy signer from a signature by $s_i^{d_i e_i} \bmod N_i = s_i$
3. An original signer can trace proxy signers by e_i.

6 CONCLUSION

In this paper, Sun threshold proxy signature scheme has been analysis. The scheme is based on discrete logarithm assumption. The security of Sun is undeniable threshold proxy signature scheme with known signers. We find that in Sun scheme, a malicious original signer can forge a valid proxy signature on any message without the agreement of the proxy group. We also suggest an efficient scheme which involves the characteristics and gains of the RSA cryptosystem which is a popular security scheme.

7 REFERENCES

[1] Mambo M., Usuda K., and Okamoto E., “Proxy Signatures for Delegating Signing Operation,” Proceeding of 3rd ACM Conference on Computer and Communications Security, ACM Press, pp. 48-57, 1996.

[2] Kim H., Baek J., Lee B., and. Kim K, “Secrets for Mobile Agent Using Onetime Proxy Signature,” Cryptography and Information Security 2001, Volume 2/2, pp. 845-850, 2001.

[3] Lee B., Kim H., and Kim K., “Secure Mobile Agent Using Strong Non-designated Proxy Signature,” Proceeding of ACISP 2001, pp. 474-486, 2001.

[4] Shamir A., “How to Share a Secret,” Communications of the ACM, Volume 22, No. 11, pp. 612-613, 1979.

[5] Zhang K, “Threshold Proxy Signature Schemes, "Information Security Workshop", Japan, pp. 191-197, 1997.

[6] Sun H., “An Efficient Nonrepudiable Threshold Proxy Signatures with Known Signers”, Computer Communications 22(8), pp. 717-722, 1999.

[7] Hsu C., and T. Wu, “New Nonrepudiable Threshold Proxy Signature Scheme with Known Signers,” The Journal of Systems and Software 58(2001), pp. 119-124, 2001.

[8] Yang C., Tzeng S. and M. Hwang, “On the Efficiency of Nonrepudiable Threshold Proxy Signatures with Known Signers”, Journal of Systems & Software 22(9), pp. 1-8, 2003.

[9] Tzeng S., Hwang M., and Yang C., “An Improvement of Nonrepudiable Threshold Proxy Signature Scheme with Known Signers”, Computers & Security 23, pp. 174-178, 2004.

[10] Yuan Yumin, "A Threshold Proxy Signature Scheme with Non-repudiation and Anonymity", Computer and Information Sciences – Proceedings of ISCIS 2006, 21th International Symposium, Istanbul, Turkey, November 1-3, 2006.

[11] Qi Xie, Jilin Wang and Xiuyuan Yu, "Improvement of Nonrepudiable Threshold Multi-proxy Threshold Multi-Signature Scheme with Shared Verification", Journal of Electronics (China), Volume 24, Number 6 (2007),

[12] Hu, J., Zhang, J., "Cryptanalysis & Improvement of a Threshold Proxy Signature Scheme", Computer Standards & Interfaces, (2009)

[13] Pedersen T., “A Threshold Cryptosystem without Trusted Party”, Proceeding of Advance in Cryptology-EUROCRYPTO’91, LNCS 547, Springer-Verlag, pp. 522-526, 1991.

[14] Feldman P., “A Practical Scheme for Non–Interactive Veriable Secret Sharing”, Proceeding of 28th FOCS, IEEE, pp. 427-437, 1987.