A Nonrepudiable Threshold Multi-Proxy Multi-Signature Scheme with Shared Verification*

Shiang-Feng Tzeng† Cheng-Ying Yang‡ Min-Shiang Hwang†

Department of Information Management†
Chaoyang University of Technology
168 Gifeng E. Rd., Wufeng,
Taichung County, Taiwan 413, R.O.C.
Email: mshwang@mail.cyut.edu.tw
Fax: 886-4-23742337

Department of Information and Communications Engineering‡
Chaoyang University of Technology
168 Gifeng E. Rd., Wufeng,
Taichung County, Taiwan 413, R.O.C.

March 6, 2008

*This research was partially supported by the National Science Council, Taiwan, R.O.C., under contract no.: NSC90-2213-E-324-004.

†Responsible for correspondence.

A Nonrepudiable Threshold Multi-Proxy Multi-Signature Scheme with Shared Verification

Abstract

In this paper, we shall propose a threshold multi-proxy multi-signature scheme with shared verification. In the scheme allows the group of original signers to delegate the signing capability to the designated group of proxy signers. Furthermore, a subset of verifiers in the designated verifier group can authenticate the proxy signature. A threshold multi-proxy multi-signature scheme with the non-repudiation property is a scheme where the proxy group cannot deny signing for the message and the verifier group can identify the proxy group for a proxy signature.

Keywords: Digital signature, Proxy signature, Threshold proxy signature, Proxy multi-signature scheme, Multi-proxy multi-signature scheme, Threshold Multi-proxy multi-signature scheme.

1 Introduction

A new type of digital signature, proxy signature, was first proposed in 1996 [6, 7]. The proxy signature allows a designated person, called a proxy signer, to sign on behalf of an original signer. So far, many proxy signature schemes were discussed [1, 3, 4, 5, 8, 9, 11, 12, 13, 14].

They distinguish into several kinds of proxy signature schemes. The proxy multi-signature schemes were proposed in [13]. In the proxy multi-signature schemes, a proxy signer is allowed to generate a proxy multi-signature on behalf of two or more original signers. The threshold proxy signature schemes were also widely proposed [1, 3, 4, 5, 8, 11, 12, 14]. In the (t, n) threshold proxy signature scheme, any t or more of the proxy singers can cooperatively sign messages on behalf of an original signer. Recently, a kind of proxy signature scheme, multi-proxy multi-signature scheme, was proposed [9]. The scheme allows the group of original signers to delegate the signing capability to the designated group of proxy signers.

In the schemes mentioned above, outsiders are allowed to play the role of verifiers. However, in most existing signature schemes, there can be only one legal signer and one legal verifier. To bridge this gap, Hsu and Wu [2] used the concept of (t, n) threshold signature to extend the capability of verification which is addressed to one signer and a group of verifiers. Wang et al. [10] also extended the existing schemes to the group-oriented (t, n) threshold signature with a (k, l) shared verification scheme among groups. Similarly, in all existing proxy signature schemes, there can be only one legal verifier. In practical applications, there is usually a need to have some specified verifiers verify the proxy signature. Assume that several directors represent a directorate to delegate their signing capability to a group of managers. Then, several of these managers represent the company to sign a contract with another company through computer network. By using the proposed scheme, the validity of the business between the two companies can be guaranteed.

According to the above statement, the group of verifiers to verify the message has to be specified, and the message should also be able to be authenticated by the specified group of verifiers. In this paper, we shall propose a new scheme in which the original signer group, proxy signer group and verifier group are specified under the predefined proxy warrant.

In Section 2, we shall use the concept of proxy signature and predefine the proxy warrant to propose a threshold multi-proxy multi-signature scheme for multi-groups.

The security of the proposed scheme will be discussed in Section 3. Finally, the conclusion will be given in Section 4.

2 The Proposed Scheme

In this section, a threshold proxy signature scheme among groups will be proposed. According to the proxy warrant, a subset of original signers allows a designated proxy group to sign on behalf of the original group. A message m has to be signed by a subset of proxy signers who can represent the proxy group. Then, the proxy signature is sent to the verifier group. A subset of verifiers in the verifier group can also represent the group to authenticate the proxy signature.

In other words, some threshold values will be given to indicate the number of persons to represent a group to authorize the signing capability or to sign a message or to verify the proxy signature. The proposed scheme requires a share distribution center (SDC for short) which is responsible for setting some parameters and initializing the scheme. Therefore, the proposed scheme involves four parties: the share distribution center, the original group, the proxy group and the verifier group. The procedure of the proposed scheme contains four phases: the secret share generation phase, the proxy share generation phase, the proxy signature generation phase and the proxy signature verification phase. The reference configurations and flow are illustrated in Figure 1. For the initial step, SDC first selects and publishes the following parameters:

- *p:* a large prime.
- *q:* a large prime factor of $p-1$.
- *g:* a generator in Galois field $GF(p)$ of order q.

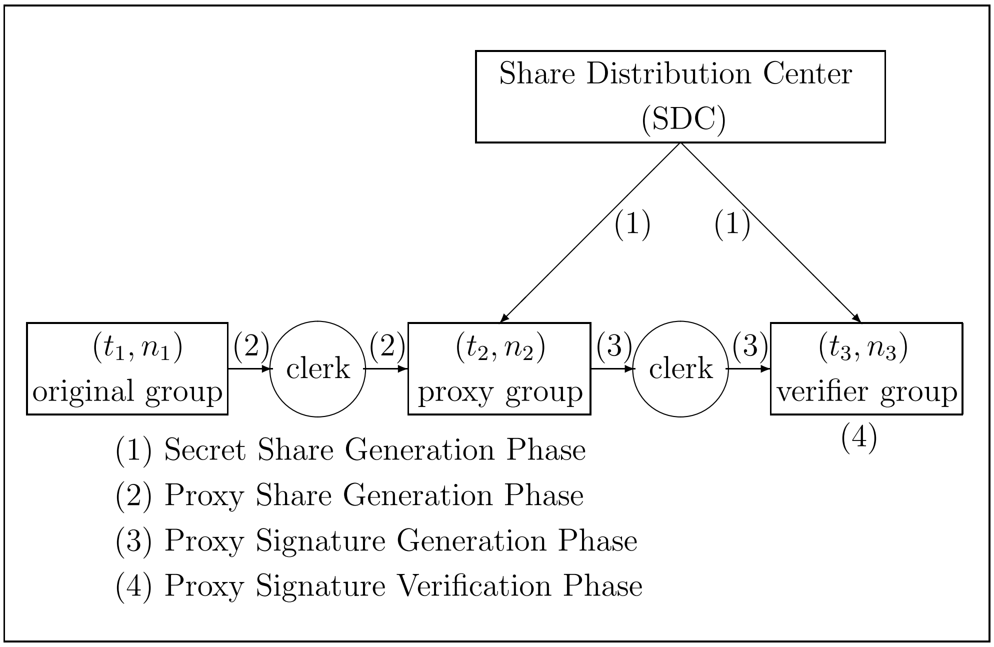

Figure 1: Threshold Multi-Proxy Multi-Signature Scheme

- $h(\cdot)$*:* a one-way hash function.
- m_w*:* a warrant which records the identities of the original signers in the original group, the proxy signers in the proxy group and the verifiers in the verifier group, the parameters $(t_1,\ n_1)$, $(t_2,\ n_2)$ and $(t_3,\ n_3)$ and the valid delegation time, etc.
- $AOSID$*:* (Actual Original Signers' ID) the identities of the actual original signers.
- $APSID$*:* (Actual Proxy Signers' ID) the identities of the actual proxy signers.

Each original signer U_{O_i} owns a secret key $x_{O_i} \in Z_q^*$ and a public key $y_{O_i} = g^{x_{O_i}} \bmod p$ which is certified by a certificate authority (CA). Similarly, each proxy signer U_{P_i} or verifier U_{V_i} also owns a secret key $x_{P_i} \in Z_q^*$ or $x_{V_i} \in Z_q^*$ and a public key $y_{P_i} = g^{x_{P_i}} \bmod p$ or $y_{V_i} = g^{x_{V_i}} \bmod p$ which is also certified by that CA.

Then, SDC accepts the registration of a group of proxy signers or a group of verifiers. For notations, the parameters will be expressed by a subscript G_O, G_S or G_V which is used by the original signer group, the proxy signer group or the verifier group. Let $G_O = \{U_{O_1}, U_{O_2}, \cdots, U_{O_{n_1}}\}$, $G_P = \{U_{P_1}, U_{P_2}, \cdots, U_{P_{n_2}}\}$ and $G_V = \{U_{V_1}, U_{V_2}, \cdots, U_{P_{n_3}}\}$ be groups of n_1 original signers, n_2 proxy signers and n_3 verifiers, respectively. According to the definition of a threshold multi-proxy multi-signature scheme, any t_1 out of n_1 original signers ($1 \leq t_1 \leq n_1$) can represent the original signer group to delegate signing capability. Any t_2 out of n_2 proxy signers ($1 \leq t_2 \leq n_2$) can represent the proxy group to sign a message on behalf of the original group. Similarly, any t_3 out of n_3 verifiers ($1 \leq t_3 \leq n_3$) can represent the verifier group to verify the proxy signature.

2.1 Secret Share Generation Phase

In this phase, three parties are involved, including the share distribution center, the proxy group and the verifier group. SDC first chooses the proxy group secret key $X_P \in Z_q^*$ and computes the proxy group public key $Y_P = g^{X_P} \bmod p$ which is certified by CA. Similarly, SDC also selects a verifier group secret key $X_V \in Z_q^*$ and computes the verifier group public key $Y_V = g^{X_V} \bmod p$ which is also certified by CA. For the proxy group G_P and the verifier group G_V, SDC randomly generates two secret polynomial functions

$$f_P(x) = X_P + P_1 x + \cdots + P_{t_2-1} x^{t_2-1} \bmod q$$

and

$$f_V(x) = X_V + V_1 x + \cdots + V_{t_3-1} x^{t_3-1} \bmod q,$$

and the degrees are $t_2 - 1$ and $t_3 - 1$, respectively.

Furthermore, SDC obtains a public key y_{P_i} for each proxy signer in the proxy signer group and computes her/his secret shadow $f_P(y_{P_i})$, for $i = 1, 2, \cdots, n_2$. The corresponding public key is also determined by $y_{fP_i} = g^{f_P(y_{P_i})} \bmod p$, for $i = 1, 2, \cdots, n_2$. Similarly, each verifier's secret shadow is $f_V(y_{V_i})$, and the corresponding public key is determined by $y_{fV_i} = g^{f_V(y_{V_i})} \bmod p$, for $i = 1, 2, \cdots, n_3$. In summary, the proposed scheme parameters are listed as follows:

- Public information of center: p, q, g, $h(\cdot)$
- Secret information of center: $f_P(x)$, $f_V(x)$
- Public information of original signer: y_{O_i}
- Secret information of original signer: x_{O_i}
- Public information of proxy signer: y_{P_i}, y_{fP_i}
- Secret information of proxy signer: x_{P_i}, $f_P(y_{P_i})$
- Public information of verifier: y_{V_i}, y_{fV_i}
- Secret information of verifier: x_{V_i}, $f_V(y_{V_i})$
- Public information of group: Y_P, Y_V
- Secret information of group: X_P, X_V

2.2 Proxy Share Generation Phase

The proposed scheme allows any t_1 original signers to represent the group to delegate the signing capability to the proxy group to sign on behalf of the original group. So, two parties, namely the original group and proxy group, are involved in this phase. Without loss of generality, assume that the t_1 original signers to delegate the signing capability are indicated as $D_O = \{U_{O_1}, U_{O_2}, \cdots, U_{O_{t_1}}\}$. Let D_O be the actual original signers. D_O is a group executes the following steps to delegate the signing capability to G_P.

1. Choose a random number $a_i \in Z_q^*$ and broadcast k_i.

$$k_i = g^{a_i} \bmod p$$

2. For each received k_j $(j = 1, 2, \cdots, t_1; j \neq i)$, each $U_{O_i} \in D_O$ computes

$$\begin{aligned} K &= \prod_{i=1}^{t_1} k_i \bmod p, \\ \sigma_{O_i} &= a_i K + x_{O_i} h(K \parallel m_w \parallel AOSID) \bmod q. \end{aligned}$$

3. Send σ_{O_i} to the designated clerk via a public channel.

4. After receiving σ_{O_i}, the designated clerk first computes

$$\sigma_O = \sum_{i=1}^{t_1} \sigma_{O_i} \bmod q.$$

   Then, the designated clerk checks whether the following equation holds

$$g^{\sigma_O} \stackrel{?}{=} K^K \prod_{i=1}^{t_1} y_{O_i}^{h(K \| m_w \| AOSID)} \bmod p.$$

   If it does, the designated clerk computes

$$\sigma = t_2^{-1} \sigma_O \bmod q.$$

   If it does not, the designated clerk checks whether the following equation holds

$$g^{\sigma_{O_i}} \stackrel{?}{=} k_i^K y_{O_i}^{h(K \| m_w \| AOSID)} \bmod p.$$

5. Broadcast $(\sigma, m_w, K, AOSID)$ to G_P.

After receiving $(\sigma, m_w, K, AOSID)$, each $P_i \in G_P$ checks whether or not the following equation holds

$$g^{\sigma} \stackrel{?}{=} (K^K \prod_{i=1}^{t_1} y_{O_i}^{h(K \| m_w \| AOSID)})^{t_2^{-1}} \bmod p.$$

If it does, each P_i uses σ as her/his proxy share.

2.3 Proxy Signature Generation Phase

This phase has to do with the proxy group and verifier group as well. Without loss of generality, the proposed scheme allows any t_2 proxy signers to represent the proxy group to sign a message m. Let $D_P = \{U_{P_1}, U_{P_2}, \cdots, U_{P_{t_2}}\}$ be the actual proxy signers. D_P is a group executes the following steps to generate the proxy signature.

1. Each $U_{P_i} \in D_P$ chooses a random number $b_i \in Z_q^*$ and broadcasts r_{P_i}.

$$r_{P_i} = g^{b_i} \bmod p$$

2. Each $U_{P_i} \in D_P$ uses a secret shadow $f_P(y_{P_i})$ and a group public key Y_V of the verifiers to compute and broadcast r'_{P_i}.

$$r'_{P_i} = (Y_V)^{f_P(y_{P_i}) \prod_{j=1, j\neq i}^{t_2} \frac{0 - y_{P_j}}{y_{P_i} - y_{P_j}}} \bmod p$$

3. For each received r_{P_j} and r'_{P_j} $(j = 1, 2, \cdots, t_2; j \neq i)$, each $U_{P_i} \in D_P$ computes

$$\begin{aligned} R &= \prod_{i=1}^{t_2} r_{P_i} \bmod p, \\ R' &= \prod_{i=1}^{t_2} r'_{P_i} \bmod p, \end{aligned}$$

$$s_i = R' f_P(y_{P_i}) \prod_{j=1, j\neq i}^{t_2} \frac{0 - y_{P_j}}{y_{P_i} - y_{P_j}} + b_i R + (\sigma + x_{P_i}) h(R \parallel APSID \parallel m) \bmod q. \quad (1)$$

Here, s_i is the individual proxy signature which is sent to the designated clerk.

4. After receiving s_i, the designated clerk first computes

$$S = \sum_{i=1}^{t_2} s_i \bmod q.$$

Then, the designated clerk checks whether the following equation holds

$$g^S \overset{?}{=} Y_P^{R'} R^R (K^K \prod_{i=1}^{t_1} y_{O_i}^{h(K \| m_w \| AOSID)} \prod_{j=1}^{t_2} y_{P_j})^{h(R \| APSID \| m)} \bmod p.$$

If it does, all (r_i, s_i) are valid individual proxy signatures of message m. If it does not, the designated clerk checks whether the following equation holds

$$g^{s_i} \stackrel{?}{=} y_{fP_i}^{R' \prod_{j=1, j\neq i}^{t_2} \frac{0-y_{P_j}}{y_{P_i}-y_{P_j}}} r_{P_i}^{R}((K^K \prod_{i=1}^{t_1} y_{O_i}^{h(K\|m_w\|AOSID)})^{t_2^{-1}} y_{P_i})^{h(R\|APSID\|m)} \bmod p.$$

The proxy signature of m is $(m_w, K, AOSID, R, S, APSID)$.

2.4 Proxy Signature Verification Phase

Any t_3 out of n_3 verifiers in the group G_V can cooperate to verify the validity of the proxy signature. Let $D_V = \{U_{V_1}, U_{V_2}, \cdots, U_{V_{t_3}}\}$ be the actual verifiers. The steps of this phase are described as follows:

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

2. Each $U_{V_i} \in D_V$ uses her/his secret shadow $f_V(y_{V_i})$ and the group public key Y_P of the proxy signers to compute and broadcast r'_{V_i}.

$$r'_{V_i} = (Y_P)^{f_V(y_{V_i}) \prod_{j=1, j\neq i}^{t_3} \frac{0-y_{V_j}}{y_{V_i}-y_{V_j}}} \bmod p$$

3. For each received r'_{V_j} $(j = 1, 2, \cdots, t_3; j \neq i)$, each $U_{V_i} \in D_V$ computes

$$R' = \prod_{i=1}^{t_3} r'_{V_i} \bmod p,$$

4. Then, each verifier $U_{V_i} \in D_V$ can check the validity of the proxy signature of the message m through the following equation:

$$g^S \stackrel{?}{=} Y_P^{R'} R^R (K^K \prod_{i=1}^{t_1} y_{O_i}^{h(K\|m_w\|AOSID)} \prod_{j=1}^{t_2} y_{P_j})^{h(R\|APSID\|m)} \bmod p. \quad (2)$$

If the equation holds, the message m is authenticated and the proxy signature $(m_w, K, AOSID, R, S, APSID)$ is valid.

3 Security Analysis of the Proposed Scheme

The security of the proposed scheme is based on the well-known difficulty of computing one-way hash function and the discrete logarithm problem cryptographic assumptions. In the following paragraphs, several possible attacks will be considered, and we shall also prove that none of them can successfully break the proposed scheme.

In proposed scheme, all of the actual original signer's secret keys x_{O_i}, $i = 1, 2, \cdots, t_1$, are used in the proxy share generation phase to create a proxy share σ. Thus, it is necessary for the proxy group to verify the proxy share and the verifier group to verify the proxy signature verification Equation (2) by using all of the actual original signer's public keys. These actual original signer's public keys are certified by CA. Without knowing the original signer's secret keys, an opponent is unable to generate the proxy share σ in the proposed scheme. Assume that an opponent wants to derive the original signers' secret key x_{O_i} from the public keys $y_{O_i} = g^{x_{O_i}} \bmod p$. It means this attacker has to face the difficulty of solving the discrete logarithm problem. At the same time, because of the proof of the proxy share, the original group cannot deny delegating their signing capability to a proxy group.

Similarly, all of the actual proxy signers' secret keys x_{P_i}, $i = 1, 2, \cdots, t_2$ are used to generate the proxy signature in the proxy signature generation phase. Thus, it is necessary for the verifier group to verify the proxy signature verification Equation (2) by using all of the actual proxy signers' secret keys. These actual proxy signers' public keys are certified by CA. Assume that an opponent wants to reveal the proxy signers' secret key x_{P_i} from the public keys $y_{P_i} = g^{x_{P_i}} \bmod p$. The equation is as difficult to meet as solving the discrete logarithm problem. Therefore, the proxy group cannot deny generating the proxy signature on behalf of the proxy group and the original signer group.

Without loss of generality, if the opponent tries to derive the proxy group secret key X_P and verifier group secret key X_V from their corresponding public keys $Y_P = g^{X_P} \bmod p$ and $Y_V = g^{X_V} \bmod p$, she/he also has to solve the same problem. As to the forgery attack, we consider the security of the proxy signature verification equation:

$$g^S \overset{?}{=} Y_P^{R'} R^R (K^K \prod_{i=1}^{t_1} y_{O_i}^{h(K\|m_w\|AOSID)} \prod_{j=1}^{t_2} y_{P_j})^{h(R\|APSID\|m)} \bmod p.$$

In this case, an outsider may try to forge a valid proxy signature to pass the proxy signature verification. Suppose

$$\begin{aligned} V_O &= K^K \prod_{i=1}^{t_1} y_{O_i}^{h(K\|m_w\|AOSID)} \bmod p, \\ V_P &= \prod_{j=1}^{t_2} y_{P_j} \bmod p. \end{aligned}$$

We rewrite the proxy signature verification equation as

$$g^S = Y_P^{R'} R^R (V_O V_P)^{h(R\|APSID\|m)} \bmod p.$$

The value of V_O depends on the parameters K, m_w and $AOSID$, while V_P is a fixed value as the proxy signers' public keys are certified by CA. Similarly, Y_P is a fixed value as the proxy signer group public key is certified by CA. Given m^*, $APSID^*$, V_O^* and R'^*, it is hard to determine R^* and S^* because of the difficulty of solving the discrete logarithm problem and the one-way hash function cryptographic assumptions. Again, given m^*, $APSID^*$, R'^*, R^* and S^*, one can compute a V_O^* such that this equation holds. However, it is difficult to find m_w^*, $AOSID^*$ and K^* such that the equation

$$V_O = K^K \prod_{i=1}^{t_1} y_{O_i}^{h(K\|m_w\|AOSID)} \bmod p$$

holds. The difficulty here is also based on the discrete logarithm problem and the one-way hash function cryptographic assumptions. Therefore, the proxy signature verification equation is secure to against forgery attack.

Consider the conspiracy attack. Assume that $t_2 - 1$ proxy signers of the group G_P conspire to derive some other proxy signers' secret keys and the proxy group secret key. They will have to first reconstruct the polynomial function $f_P(x)$ and compute the other proxy signers' secret shadows $f_P(y_{Pi})$ for some $U_{P_i} \in G_P$ and also obtain the proxy group secret key $f_P(0)$ for G_P. However, the secret polynomial function $f_P(x)$ can be reconstructed only by obtaining at least t_2 proxy signers' secret shadows $f_P(y_{P_i})$'s of G_P. Thus, any $t_2 - 1$ conspirators or less cannot reveal any other proxy signers' secret shadows and the proxy group secret key, even though they release their secret shadows to each other. Similarly, any $t_3 - 1$ verifiers or less in the verifier group G_v cannot obtain any other verifiers' secret shadows. Therefore, neither proxy signers' conspiracy attack nor verifiers' conspiracy attack can be successful.

Assume any t_2 or more proxy signers in G_P work together to reconstruct the secret polynomial function $f_P(x)$ and proxy group secret key. Thus, they can easily derive any other proxy signer U_{P_j}'s secret shadow. However, they cannot derive $P_j's$ secret key from x_{P_i} via Equation (1) with the given s_j because to obtain b_j means to solve the discrete logarithm problem.

4 Conclusions

A new threshold multi-proxy multi-signature scheme with (t_3, n_3) shared verification is proposed in this paper. In the proposed scheme, a subset of original signers can authenticate a designated proxy group to sign on behalf of the original group. A message m has to be signed by a subset of proxy signers who can represent the proxy group. Then, the proxy signature is sent to the verifier group. A subset of verifiers in the verifier group can also represent the group to authenticate the proxy signature. Furthermore, these actual proxy signers cannot deny the fact that they have signed the proxy signature. Based on the difficulty of the one-way hash function and the discrete logarithm problem, the security of the proposed scheme is confirmed. Some possible attacks are considered, and none of them can successfully break the proposed scheme.

References

[1] Chien-Lung Hsu, Tzong-Sun Wu, and Tzong-Chen Wu, "New nonrepudiable threshold proxy signature scheme with known signers," *The Journal of Systems and Software*, no. 58, pp. 119–124, 2001.

[2] C.L. Hsu and T.C. Wu, "Authenticated encryption scheme with (t, n) shared verification," *IEE Proc.-Comput. Digit. Tech.*, vol. 145, no. 2, pp. 117–120, 1998.

[3] M. S. Hwang, I. C. Lin, and Eric J. L. Lu, "A secure nonrepudiable threshold proxy signature scheme with known signers," *International Journal of Informatica*, vol. 11, no. 2, pp. 1–8, 2000.

[4] S. Kim, S. Park, and D. Won, "Proxy signatures, revisited," *Proc. of ICICS'97, LNCS 1334*, pp. 223–232, 1997.

[5] N.Y. Lee, T. Hwang, and C.H. Wang, "On Zhang's nonrepudiable proxy signature schemes," *ACISP'98, LNCS 1438*, pp. 415–422, Jul. 1998.

[6] M. Mambo, K. Usuda, and E. Okamoto, "Proxy signatures: Delegation of the power to sign message," *IEICE Trans. Fundamentals*, vol. E79-A, pp. 1338–1353, Sep. 1996.

[7] M. Mambo, K. Usuda, and E. Okamoto, "Proxy signatures for delegating signing operation," *Proc. Third ACM Conf. on Computer and Communications Security*, pp. 48–57, 1996.

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

[9] Shiang-Feng Tzeng, Cheng-Ying Yang, and Min-Shiang Hwang. "A new multi-proxy multi-signature scheme,". Technical Report CYUT-IM-TR-2002-004, CYUT, 2002.

[10] Ching-Te Wang, Chin-Chen Cheng, and Chu-Hsing Lin, "Generalization of threshold signature and authenticated encryption for group communications," *IEICE Trans. Fundamentals*, vol. E83-A, no. 6, pp. 1228–1237, 2000.

[11] Cheng-Ying Yang, Shiang-Feng Tzeng, and Min-Shiang Hwang. "A new nonrepudiable threshold proxy signature scheme with valid delegation period,". Technical Report CYUT-IM-TR-2002-005, CYUT, 2002.

[12] Cheng-Ying Yang, Shiang-Feng Tzeng, and Min-Shiang Hwang. "A nonrepudiable threshold proxy signature scheme with known signers,". Technical Report CYUT-IM-TR-2002-003, CYUT, 2002.

[13] L. Yi, G. Bai, and G. Xiao, "Proxy multi-signature scheme: A new type of proxy signature scheme," *Electronics Letters*, vol. 36, no. 6, pp. 527–528, 2000.

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