以橢圓曲線密碼學改良之多人授權予多人的代理簽章法

Improvement of A Multi-Proxy Multi-Signature Scheme Based on Elliptic Curve Cryptography

洪國寶 劉兆樑 劉容禎

Gwoboa Horng Chao-Liang Liu Jung-Chen Liu

中興大學資科所 中興大學資科所 中興大學資科所

Institute of Computer Science, National Chung Hsing University

E-mail : {gbhorng, s9056001, s9156010}@cs.nchu.edu.tw

摘要

2001 年，Hwang、Chen 等人提出一個植基於離散對數難題的多人授權予多人的代理簽章法。在這個方法中，原始簽章群體的所有人可以合作產生授權給一個代理簽章群體，且只有當代理簽章群體的所有人共同合作時，才能產生合法的代理簽章。但在 2002 年在 Sun 等人所提出的文章中，指出 Hwang-Chen 的方法中，攻擊者可偽造出通過驗證式的簽章。本文中，我們改進 Hwang-Chen 的方法，並將橢圓曲線密碼系統應用於此多人授權予多人的代理簽章法。

關鍵詞：代理簽章，多重代理多重簽章，多重代理簽章，橢圓曲線密碼學

Abstract

In 2001, Hwang and Chen proposed a new multi-proxy multi-signature scheme based on Discrete Logarithm Problem. In their scheme, an original group of signers can authorize a group of proxy signers. Then only the cooperation of all signers in proxy group can generate valid multi-proxy multi-signatures. But in 2002, Sun et al. pointed out that attacker can forge a valid signature for an arbitrary message. In this paper, we improve Hwang-Chen's method and propose a new scheme based on elliptic curve discrete logarithm problem.

Keywords: proxy signature, multi-proxy multi-signature, multi-proxy signature, elliptic curve cryptography

一、簡介

數位簽章的技術可以提供我們一份電子文件的完整性與確認性，而為了避免簽章者負擔過重，所以在現實生活中我們希望能以授權的方式，經由代理人來代理簽章，但傳統的數位簽章並不能達到這種要求，因此有代理簽章法的出現。

而代理簽章法(proxy signature)的概念在 1996 年由 Mambo 等人首先提出[10][11]，它允許任何一個原始簽章者委任給一個代理簽章者來代表他簽章。在 Mambo 的方法中，限制只有代理簽章者可以產生合法的代理簽章，因此任何人都可以辨認出簽章是經由原始簽章者或是代理簽章者所產生。這種做法提供原始簽章者及代理簽章者一種公平性的保護。

之後，又有各種變化的代理簽章法被提出

[2-5, 7-19]。其中在(t, n)門檻代理簽章法中[12][13][20]，原始簽章者可以授權給一個包含 n 人的代理簽章群體，只有當 n 個被授權的代理簽章者中任 t 人以上合作才可以產生出合法的代理簽章。而在 2000 年由 Hwang、Shi 等人所提出[3]多重代理簽章（multi-proxy signature）則是門檻代理簽章法的一種特例（t = n）。

2001 年，Hwang、Chen 等人提出一個植基於離散對數難題(discrete logarithm problem)的多人授權予多人的代理簽章法（multi-proxy multi-signature）[6]，由原始簽章群體中的所有人，合作授權給一個代理簽章群體，而只有代理簽章群體中的所有人共同合作，才能產生出合法的代理簽章。

但在 2002 年時，由 Sun 等人所提出的文章中[1]，指出了 Hwang-Chen 的方法有安全上的漏洞，也就是說偽造者可對任意文件，偽造出通過驗證式的簽章。因此我們修正原文中有問題的簽章式，並以橢圓曲線數位簽章法(elliptic curve digital signature algorithm 簡稱為 ECDSA)[7][21][22]應用於此多人授權予多人的代理簽章法。如此可以有效的降低金鑰的長度，以及減少廣播訊息時所需的頻寬，來提高系統的運作效率。

二、 Hwang-Chen 的新多人授權予多人的代理簽章法[6]

在本節中，我們將簡述 Hwang-Chen 的多重代理人的多重簽章方法。在此系統中的參與者共有三類：n 個原始簽章者(以下簡稱 $U_1, U_2, \ldots, U_n$)、m 個代理簽章者(以下簡稱 $P_1, P_2, \ldots, P_m$)及多重代理簽章合成者(以下簡稱 C)。接著介紹本系統的參數：p, q 為兩個大質數且 q|p-1； $g \in Z_p$ 為序是 q 的生成子； $h(\cdot)$ 為一公開的單向赫序函數； x_i 為參與者的秘密金鑰而 y_i 為對應之公開金鑰且 $y_i = g^{x_i} \bmod p$； w 為代理憑證； M 則為所要簽署的文件。而在這個方法中包含三個不同的階段，分別是代理憑證產生階段(proxy certificate generation phase)、多重代理多重簽章產生階段(multi-proxy multi-signature generation phase)以及多重代理多重簽章驗證階段(multi-proxy multi-signature verification phase)。茲將每一階段分別說明如下：

A、代理憑證產生階段

1. 每一個原始簽章者 U_i 選擇一個亂數 $k_{ui} \in Z_q^*$，計算

$$K_{ui} = g^{k_{ui}} \bmod p \qquad (2.1)$$

，並將 K_{ui} 廣播給群組中其餘成員(包括原始簽章者與代理簽章者)，其中 $i \in \{1, 2, \ldots, n\}$。

每一個代理簽章者 P_j 選擇一個亂數 $k_{pj} \in Z_q^*$，計算

$$K_{pj} = g^{k_{pj}} \bmod p \qquad (2.2)$$

，並將 K_{pj} 廣播給群組中其餘成員，而 $j \in \{1, 2, \ldots, m\}$。

2. 群組中每一個成員計算

$$K = \left(\prod_{i=1}^{n} K_{ui}\right)\left(\prod_{j=1}^{m} K_{pj}\right) \bmod p \qquad (2.3)$$

3. 群組中每一個成員計算

$$v_t = (h(w)x_t y_t + k_t K) \bmod q \qquad (2.4)$$

，其中 $t \in \{ u_1, \ldots, u_n, p_1, \ldots, p_m\}$，並將 v_t 廣播給群組中其餘成員。

4. 群組中每一個成員以(2.5)驗證所得到的 v_t。

$$g^{v_t} \equiv (y_t)^{y_t h(w)} (K_t)^K \bmod p \qquad (2.5)$$

其中 $t \in \{u_1, \ldots, u_n, p_1, \ldots, p_m\}$。

5. 若 v_t 驗證無誤，則代理簽章者計算

$$V = \sum_{i=1}^{n} v_{ui} + \sum_{j=1}^{m} v_{pj} \mod q \quad (2.6)$$

其中 $t \in \{u_1, \ldots, u_n, p_1, \ldots, p_m\}$。

B、多重代理多重簽章產生階段

1. 每一個代理簽章者 P_i 選擇一個亂數 $t_i \in Z_q^*$ 計算

$$r_i = g^{t_i} \mod p \quad (2.7)$$

並將 r_i 廣播給其它的代理簽章者，

$i \in \{1, 2, \ldots, m\}$。

2. 當每個代理簽章者 P_j 收到所有的 r_i 後，計算個別的代理簽章(r_j, s_j)

$$R = \prod_{i=1}^{m} r_i \mod p \quad (2.8)$$

及

$$s_j = (Vt_j + x_{p_j} y_{p_j} R)h(M)^{-1} \mod q \quad (2.9)$$

，最後將$(w, (K,V), M, (r_j, s_j))$送交 C，而 $i, j \in \{1, 2, \ldots, m\}$。

3. C 以

$$g^V \equiv K^K [\prod_{i=1}^{n} (y_{ui}^{y_{ui}}) \prod_{j=1}^{m} (y_{pj}^{y_{pj}})]^{h(w)} \mod p \quad (2.10)$$

驗證憑證(K, V)之合法性。

4. C 計算

$$R = \prod_{j=1}^{m} r_j \mod p \quad (2.11)$$

並以

$$g^{h(M)*s_j} \equiv (r_j)^V (y_{pj})^{R*y_{pj}} \mod p \quad (2.12)$$

驗證個別代理簽章(r_j, s_j)之合法性，若都合法則計算

$$S = \sum_{j=1}^{m} s_j \mod q \quad (2.13)$$

，並將$(w, (K, V), M, (R, S))$傳送給驗證者。

C、多重代理多重簽章驗證階段

1. 驗證 w 及(K, V)之合法性

$$g^V \equiv K^K [\prod_{i=1}^{n} y_{ui}^{y_{ui}} \prod_{j=1}^{m} y_{p_j}^{y_{pj}}]^{h(w)} \mod p \quad (2.14)$$

2. 驗證 M 及(R, S)之合法性

$$g^{h(M)*S} \equiv R^V [\prod_{j=1}^{m} y_{pj}^{y_{pj}}]^R \mod p \quad (2.15)$$

三、Sun 等人的攻擊方式[1]

在 2002 年時，Sun 等人針對 Hwang-Chen 的新多人授權予多人的代理簽章法，提出一個偽造簽章的方式。而這也說明了 Hwang-Chen 的方法存在安全上的漏洞，在本節中我們將簡述 Sun 等人偽造的方式。

偽造者利用先前取得的合法簽章$(w, (K, V), M, (R, S))$，再以下面的方法計算出對任意文件 M'的偽造簽章$(w, (K, V), M', (R, S'))$。

以偽造者想要取代 M 的文件 M'計算出 S'

$$S' = h(M) * h(M')^{-1} * S \mod q \quad (3.1)$$

，而偽造的簽章$(w, (K, V), M', (R, S'))$可通過驗證式：

$$g^{h(M')*S'} \equiv g^{h(M')*h(M)*h(M')^{-1}*S}$$

$$\equiv g^{h(M)*S}$$

$$\equiv R^V [\prod_{j=1}^{m} y_{pj}^{y_{pj}}]^R \mod p \quad (3.2)$$

四、我們的改進方法

在本節中我們將修改原先簽章式中不安全的部分(2.9)(2.15)，並以橢圓曲線數位簽章法(ECDSA)，應用於此多重代理人的多重簽章方法。參與者仍然有三類：n 個原始簽章者(以下簡稱 $U_1, U_2, \ldots, U_n$)、m 個代理簽章者(以下簡稱 $P_1, P_2, \ldots, P_m$)及簽章合成者(以下簡稱 C)。而在這個方法中也是三個不同的階段，分別是代理憑證產生階段、多重代理多重簽章產生階段以及多重代理多重簽章驗證階段。茲將每一階段分別說明如下。

首先介紹本系統的參數：

1. E：為在有限體 Z_p 之下的橢圓曲線方程式。
2. G：在 $E(Z_p)$上序為 q 的生成點。
3. *：定義於 Z_q*上的乘法運算。
4. ×：定義於 $E(Z_p)$上的乘法運算，如 $d\times G = G + G + \ldots + G$ 共 d 個 G。
5. ⊕：互斥運算(exclusive-or operation)。
6. h(·)：公開的單向赫序函數(如 SHA-1)。
7. x_i：參與者的秘密金鑰而 Y_i 為對應之公開金鑰且 $Y_i = x_i \times G$。
8. w：代理憑證。
9. M：欲簽署之文件。

A、代理憑證產生階段

1. 每一個原始簽章者 U_i 選擇一個亂數 $k_{ui} \in Z_q$*，計算

$$K_{ui} = k_{ui} \times G \qquad (4.1)$$

，並將 K_{ui} 廣播給群組中其餘成員(包括原始簽章者與代理簽章者)。

每一個代理簽章者 P_j 選擇一個亂數 $k_{pj} \in Z_q$*，並計算

$$K_{pj} = k_{pj} \times G \qquad (4.2)$$

，並廣播給群組中其餘成員，其中 $i \in \{1, 2, \ldots, n\}$，$j \in \{1, 2, \ldots, m\}$。

2. 群組中每一個成員計算

$$K = (K_x, K_y) = \sum_{i=1}^{n} K_{ui} + \sum_{j=1}^{m} K_{pj} \qquad (4.3)$$

$$\boldsymbol{\kappa} = (K_x \oplus K_y) \bmod q$$

$$(\text{If } \boldsymbol{\kappa} = 0 \text{ then } \boldsymbol{\kappa} = K_x \bmod q) \qquad (4.4)$$

3. 群組中每一個成員計算

$$v_{ui} = h(w)*x_{ui} + k_{ui}*\boldsymbol{\kappa} \mod q \qquad (4.5)$$

或

$$v_{pj} = h(w)*x_{pj} + k_{pj}*\boldsymbol{\kappa} \mod q \qquad (4.6)$$

並廣播給群組中其餘成員，其中 $i \in \{1, 2, \ldots, n\}$，$j \in \{1, 2, \ldots, m\}$。

4. 群組中每一個成員以

$$v_{ui} \times G \stackrel{?}{=} (h(w) \times Y_{ui}) + (\boldsymbol{\kappa} \times K_{ui}) \qquad (4.7)$$

或

$$v_{pj} \times G \stackrel{?}{=} (h(w) \times Y_{pj}) + (\boldsymbol{\kappa} \times K_{pj}) \qquad (4.8)$$

驗證所得到的 v_{ui}, v_{pj}，其中 $i \in \{1, 2, \ldots, n\}$，$j \in \{1, 2, \ldots, m\}$。

5. 若 v_{ui}, v_{pj} 驗證無誤，則每一個代理簽章者計算

$$\boldsymbol{\nu} = (\sum_{i=1}^{n} v_{ui}) + (\sum_{j=1}^{m} v_{pj}) \mod q \qquad (4.9)$$

B、多重代理多重簽章產生階段

1. 每一個代理簽章者 P_j 選擇一個亂數

$r_j \in Z_q^*$,計算

$$R_j = r_j \times G \qquad (4.10)$$

並將 R_j 廣播給其他的代理簽章者，其中 $j \in \{1, 2, \ldots, m\}$。

2. 每個代理簽章者 P_i 收到所有的 R_j 後，計算個別代理簽章(R_i, s_i)

$$R = (R_x, R_y) = \sum_{j=1}^{m} R_j \qquad (4.11)$$

$$\acute{r} = (R_x \oplus R_y \oplus \boldsymbol{\nu}) \mod q$$

$$(\text{If } \acute{r} = 0 \text{ then } \acute{r} = (R_x \oplus \boldsymbol{\nu}) \mod q) \qquad (4.12)$$

及

$$s_i = r_i * \acute{r} + x_i * h(M) \bmod q \qquad (4.13)$$

再將$(w, (K, \boldsymbol{\nu}), M, (R_i, s_i))$送交 C，其中 $i, j \in \{1, 2, \ldots, m\}$。

3. C 以下式驗證憑證$(K, \boldsymbol{\nu})$之合法性。

$$\boldsymbol{\nu} \times G \stackrel{?}{=} h(w) \times (\sum_{i=1}^{n} Y_{ui} + \sum_{j=1}^{m} Y_{pj}) + (\boldsymbol{\kappa} \times K) \qquad (4.14)$$

而 $\boldsymbol{\kappa}$ 的計算方式同(4.4)。

4. 若$(K, \boldsymbol{\nu})$通過驗證，則 C 計算 R 及 $\acute{r}$，而計算方式與(4.11)及(4.12)相同。

再以下式驗證每一對個別代理簽章(R_i, s_i)的合法性，而 $i \in \{1, 2, \ldots, m\}$。

$$s_i \times G \stackrel{?}{=} (\acute{r} \times R_i) + (h(M) \times Y_i) \qquad (4.15)$$

，若都合法則 C 合成多重代理多重簽章

$(R, \hat{s})$

$$\hat{s} = (\sum_{j=1}^{m} s_j) \bmod q \qquad (4.16)$$

，並將$(w, (K, \boldsymbol{\nu}), M, (R, \hat{s}))$傳送給驗證者。

C、多重代理多重簽章驗證階段

1. 以下式驗證 w 及$(K, \boldsymbol{\nu})$之合法性，而 $\boldsymbol{\kappa}$ 的計算方式同(4.4)

$$\boldsymbol{\nu} \times G \stackrel{?}{=} h(w) \times (\sum_{i=1}^{n} Y_{ui} + \sum_{j=1}^{m} Y_{pj}) + (\boldsymbol{\kappa} \times K) \qquad (4.17)$$

2. 以下式驗證 M 及$(R, \hat{s})$之合法性，而 $\acute{r}$ 的計算方式同(4.12)

$$\hat{s} \times G \stackrel{?}{=} (\acute{r} \times R) + (h(M) \times (\sum_{j=1}^{m} Y_j)) \qquad (4.18)$$

五、正確性分析

在本單元中我們針對上一單元中出現的驗證式，說明合法產生的參數必定可以滿足相關的驗證式。而以下將一一推導各相關之驗證式。

(1) v_{ui} , v_{pj} 之驗證式(4.7), (4.8)

$$v_{ui} \times G = (h(w) * x_{ui} + k_{ui} * \boldsymbol{\kappa}) \times G$$

$$= (h(w) * x_{ui}) \times G + (k_{ui} * \boldsymbol{\kappa}) \times G$$

$$= h(w) \times Y_{ui} + \boldsymbol{\kappa} \times K_{ui} \qquad (5.1)$$

而 $v_{pj} \times G = h(w) \times Y_{pj} + \boldsymbol{\kappa} \times K_{pj}$ (同理可得)

(2) $(K, \boldsymbol{\nu})$ 之驗證式(4.14), (4.17)

$\boldsymbol{\nu} \times G$

$$= (\sum_{i=1}^{n} v_{ui} + \sum_{j=1}^{m} v_{pj}) \times G$$

$$= (\sum_{i=1}^{n} v_{ui}) \times G + (\sum_{j=1}^{m} v_{pj}) \times G$$

$$= \sum_{i=1}^{n} (h(w) \times Y_{ui} + \boldsymbol{\kappa} \times K_{ui}) + \sum_{j=1}^{m} (h(w) \times Y_{pj} + \boldsymbol{\kappa} \times K_{pj})$$

$$= h(w) \times (\sum_{i=1}^{n} Y_{ui} + \sum_{j=1}^{m} Y_{pj}) + \boldsymbol{\kappa} \times (\sum_{i=1}^{n} K_{ui} + \sum_{j=1}^{m} K_{pj})$$

$$= h(w)\times(\sum_{i=1}^{n} Y_{ui} + \sum_{j=1}^{m} Y_{pj}) + \boldsymbol{\kappa}\times K \qquad (5.2)$$

(3) (R_i, s_i)之驗證式(4.15)

$$s_i\times G = (r_i * \acute{r} + x_i * h(M))\times G$$

$$= (r_i * \acute{r})\times G + (x_i * h(M))\times G$$

$$= \acute{r}\times R_i + h(M)\times Y_i \qquad (5.3)$$

(4) $(R, \hat{s})$之驗證式(4.18)

$$\hat{s}\times G = (\sum_{j=1}^{m} s_j)\times G$$

$$= \sum_{j=1}^{m} (\acute{r}\times R_j + h(M)\times Y_j)$$

$$= \acute{r}\times(\sum_{j=1}^{m} R_j) + (h(M)\times(\sum_{j=1}^{m} Y_j))$$

$$= (\acute{r}\times R) + (h(M)\times(\sum_{j=1}^{m} Y_j)) \qquad (5.4)$$

六、安全性分析

在第四節中我們介紹了另一種實現多重代理人的多重簽章之方式。在此方法中，我們將原先植基於離散對數問題的方法，改植於橢圓曲線離散對數問題。並修正原來文章中不安全的簽章(2.9)與驗證式(2.15)，以阻止 Sun 等人的偽造攻擊。由於我們修改的簽章方式，基本上是橢圓曲線數位簽章法[7]的一種變形。因此我們針對偽造者的攻擊模式，提供一個簡略的分析，並由此說明修改過後的簽章式是安全的。但在此之前我們先介紹本系統的安全基礎。

定義：

橢圓曲線離散對數問題(ECDLP)

令 E 為在有限體 Z_p 之下的橢圓曲線方程式，而 G 為在 $E(Z_p)$上序為 q 的生成點。在給定 G 及 s×G 的情況下求未知數 s，(其中 $s\in Z_q^*$)。

在安全分析之前，我們先釐清偽造者的目標，就是要偽造出新的多重代理多重簽章(w, (K, **ν**), M', (R', ŝ'))，而且能滿足驗證式(6.1)。

$$\hat{s}'\times G = (\acute{r}'\times R') + (h(M')\times(\sum_{j=1}^{m} Y_j)) \qquad (6.1)$$

因此我們將偽造者可行的偽造方式分析如後。

由於本系統為不可恢復式的簽章，因此偽造者必須先選擇有意義的文件 M'。

而由(6.1)可知，當偽造者選擇 M'後，$(h(M')\times(\sum_{j=1}^{m} Y_j))$即為橢圓曲線上之一固定點。

因此我們以偽造者對 R 的偽造方式，分為以下兩種狀況討論之。

Case 1. 偽造者先求α，使得 $\acute{r}'\times R' = \alpha\times G$

則由(6.1)可得

$$\hat{s}'\times G = \alpha\times G + (h(M')\times(\sum_{j=1}^{m} Y_j)) \qquad (6.2)$$

$$\Rightarrow \quad \hat{s}'\times G = Q$$

(Q 為橢圓曲線上的某一點) (6.3)

由此可知，偽造者必須求解橢圓曲線離散對數問題，才能求出 ŝ'的值。

Case 2. 偽造者先決定出 $\hat{s}'\times G$，並由此得到 R'。

則由(6.1)可得

$$(\acute{r}'\times R') = \hat{s}'\times G + (-h(M'))\times(\sum_{j=1}^{m} Y_j) \qquad (6.4)$$

也就是說，偽造者必須求出 R'，使得 R' 具有以下的特性。

$$((R_x' \oplus R_y' \oplus \boldsymbol{\nu}) \bmod q)\times R'$$

$$= \hat{s}'\times G + (-h(M'))\times(\sum_{j=1}^{m} Y_j) \qquad (6.5)$$

$\Rightarrow$ $((R_x' \oplus R_y' \oplus \mathbf{v}) \bmod q) \times R' = \beta \times G$ (6.6)

偽造者至少須求解橢圓曲線離散對數問題，以解出β的值後，才有可能求出 R' 的值。

由以上的分析得知，若偽造者具有解出橢圓曲線離散對數問題的能力，則多重代理多重簽章(w, (K, **v**), M, (R, ŝ))是可以被偽造的。但求解橢圓曲線離散對數問題，是大家所共同認知的難題。

七、結論

在本文中，我們針對 Hwang-Chen 的多重代理多重簽章法提出改進的方法。而此改進方法，除了可以有效的抵抗 Sun 等人的偽造攻擊外，更可以有效的降低金鑰的長度，以及減少廣播訊息時所需的頻寬，提高系統運作的效率。不過，在此方法中每一參與者的計算負擔仍不小，雖然可透過預先計算(pre-compute)的技巧來降低計算所需的時間，但如何簡化此系統，使其更有效率的運作，將是我們未來努力的方向。

致謝

本研究由經濟部委託（補助）財團法人資訊工業策進會通訊軟體關鍵技術開發五年計畫分包辦理。

九、參考文獻

[1] 孫宏民, 謝濱燦, 林宸堂, "Cryptanalysis of A New Multi-Proxy Multi-Signature Scheme," *第十二屆全國資訊安全會議*, pp. 151-154, 2002.

[2] S.J.Hwang and C.H.Shi, , "The Specifiable Proxy Signature," *National Computer Symposium*, vol. 1334, Taiwan, pp. 190-197, 1999.

[3] S.J.Hwang and C.H.Shi, "A Simple Multi-Proxy Signature Scheme," *Proceedings of the 10th National Conference on Information Security*, Taiwan, pp. 134-138, 2000.

[4] S.J.Hwang and C.H.Shi, "A Proxy Signature Scheme without Using One-Way Hash Functions," *International Computer Symposium*, Chiayi, Taiwan, R.O.C., Dec. 6-8, pp. 60-64, 2000.

[5] S.J.Hwang and C.H.Shi, "A New Proxy Multi-Signature Scheme," to appear in *International Workshop on Cryptology and Network Security*, Tamkang University, Taipei, Taiwan, pp. 26-28, 2001.

[6] S.J.Hwang and C.C.Chen, "A New Multi-Proxy Multi-Signature Scheme," *National Computer Symposium*, vol. F, Taiwan, pp. 19-26, 2001.

[7] Don B. Johnson and Alfred J. Menezes, "Elliptic Curve DSA (ECDSA): An Enhanced DSA," www.certicom.com/research/white.html , 1999.

[8] S.Kim, S.Park and D.won, "Proxy Signatures, revisited," *ICICS'97, Lecture Notes in Computer Science*, vol.1334, Springer, Berlin, pp. 223-232, 1997.

[9] N.Y.Lee, T.Hwang and C.H. Wang, "On Zhang's Nonrepudiable Proxy Signature Schemes," *Third Australasian Conference*, ASISP'98, pp. 415-422, 1998.

[10] M.Mambo, K.Usuda, and E.Okamoto, "Proxy Signatures：Delegation of the Power to Sign Message," *IEICE. Transaction Fundamentals*, E79-A, 9, pp. 1338-1354, 1996.

[11] M.Mambo, K.Usuda, and E.Okamoto, "Proxy Signatures for Delegation Signing Operation," *Proc. 3nd ACM Conference on Computer and Communication Security*, pp. 48-57, 1996.

[12] H.M.Sun, "An Efficient Nonrepudiable Threshold Proxy Signature Scheme with Known Signers," *Computer Communication*, vol. 22, pp. 717-722, 1999.

[13] H.M.Sun, N.Y.Lee and T.hwang, "Threshold Proxy Signature," *IEE Proceedings-computers & Digital Techniques*, vol. 146,No. 5, September, pp. 259-263, 1999.

[14] H.M.Sun and B.J.Chen, "Unforgeable Time-Stamped Proxy Signatures with Traceable Receivers," *Proceedings of the Ninth National Conference on Information Security*, Taiwan, pp. 247-253, 1999.

[15] H.M.Sun and B.T Hsieh, "Remark on Two Nonrepudiate Proxy Signature Schemes," *Proceedings of the Ninth National Conference on Information Security*, Taiwan, pp. 241-246, 1999.

[16] H.M.Sun, "Design of Time-Stamped proxy Signatures with Traceable Receivers," *IEE Proceedings of Computers and Digital Techniques*, vol.147, No. 6. pp. 462-466, 2000.

[17] H.M.Sun, "On Proxy (Multi-) Signature Schemes," *2000 International Computer Symposium*, Chiayi, Taiwan, R.O.C., pp. 65-72, 2000.

[18] S.M.Yen, C.P.Hung and Y.Y.Lee, "Remarks on Some Proxy Signature Schemes," *2000 International Computer Symposium*, Chiayi, Taiwan, R.O.C., pp. 54-59, 2000.

[19] L.B.Yi and G.Xiao, "Proxy Multi-Signature Scheme：A New Type of Proxy Signature Scheme," *Electronic Letters*, vol. 36, No. 5, pp. 527-528, 2000.

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

[21] William Stallings, *Cryptography and Network Security Principle and Practice (third edition)*. New Jersey: Person Education International, 2003.

[22] Menezes, A. *Elliptic Curve Public Key Cryptosystem*. Boston: Kluwer Academic Publishers, 1993.