行政院國家科學委員會專題研究計畫　成果報告

具可匿名代理人的群體導向授權代理簽章法之設計

計畫類別：個別型計畫
計畫編號：NSC92-2213-E-032-019-
執行期間：92 年 08 月 01 日至 93 年 07 月 31 日
執行單位：淡江大學資訊工程學系

計畫主持人：黃心嘉

計畫參與人員：陳光熹　彭瑞珠

報告類型：精簡報告

處理方式：本計畫可公開查詢

中　華　民　國 93 年 9 月 24 日

行政院國家科學委員會補助專題研究計畫成果報告

※※※※※※※※※※※※※※※※※※※※※※※※※※※※

※ ※

※ 具可匿名代理人的群體導向授權代理簽章法之設計 ※

※ ※

※※※※※※※※※※※※※※※※※※※※※※※※※※※※

計畫類別：☑個別型計畫　　□整合型計畫

計畫編號：NSC 92-2213-E-032-019-

執行期間：　92 年 8 月 1 日至 93 年 7 月 31 日

計畫主持人：　黃心嘉　　淡江大學資工系　　副教授

計畫參與人員：　陳光熹　淡江大學資工系　　研究生

彭瑞珠　淡江大學資工系　　研究生

本成果報告包括以下應繳交之附件：

□赴國外出差或研習心得報告一份

□赴大陸地區出差或研習心得報告一份

□出席國際學術會議心得報告及發表之論文各一份

□國際合作研究計畫國外研究報告書一份

執行單位：淡江大學資工系

中　華　民　國　九十三 年八月三十一日

行政院國家科學委員會專題研究計畫成果報告

具可匿名代理人的群體導向授權代理簽章法之設計

Anonymous Proxy Group-oriented Signature Schemes with Undeniable Agents

計畫編號：NSC 92-2213-E-032-019
執行期限：92 年 8 月 1 日至 93 年 7 月 31 日
主持人：黃心嘉　淡江大學資工系　副教授
計畫參與人員：陳光熹　　淡江大學資工系　研究生
彭瑞珠　　淡江大學資工系　研究生
Email: sjhwang@mail.tku.edu.tw

一、中英文摘要

中文摘要

實務上，代理簽章者希望可以用匿名的方式代理，以免除不必要的困擾。在之前的計畫中，已提出一個匿名的代理簽章法，除了滿足 Mambo 等學者所提的七項要求外，也提供匿名的功能，當糾紛發生時，原始簽章者與公信的第三者合作，可以證實匿名代理簽章者的身份。因應群體導向的需求，植基於此一方法，本計畫提出一個匿名的多人授權代理簽章法，與一個匿名的(t, n) 門檻式授權代理簽章法。

英文摘要

Actually, in many situations, the proxy signer may want to be anonymous to avoid disturbance. In our previous project, an anonymous proxy signature scheme with undeniable agents has been proposed. Except satisfying the seven properties proposed by Mambo et al, the proxy signer in our scheme is anonymous. When any dispute occurs, the original signers and the trust third party can prove the identity of the proxy signer. Due to the group-oriented application, based on the prvious scheme, the anonymous proxy multi-signature scheme with undeniable agents and the anonymous proxy (t, n) threshold signature schemes with a mutually trusted party are proposed in this project.

關鍵字: proxy signature scheme, proxy multi-signature scheme, proxy threshold signature scheme, digital signature scheme.

二、緣由與目的

為了提供代理功能，日本學者 Mambo 等人[14, 15]題出代理簽章的觀念。但是過往的代理簽章法[9-12, 14, 15, 17, 18, 20-21, 23, 24]，為保護代理簽章者，必須公開代理簽章者的。然而為了保護代理簽章者隱私，代理簽章者卻希望匿名，因此在我們的計畫(NSC90-2213-Z-032-025)中，提出了一個匿名的代理簽章法，可以讓一位原始簽章者授權給一位匿名的代理簽章者，同時可以防禦匿名代理簽章者事後否認的攻擊。

在實際的應用中，匿名代理簽章存在群體導向的需求，因此在本年度計畫中，植基於匿名的代理簽章法，提出一個匿名的多人授權代理簽章法，讓一群原始簽章者授權給一位匿名的代理簽章者，而匿名代理簽章授權，必須在這一群原始簽章者的所有人共同合作下方才能產生，也可以防禦匿名代理簽章者事後否認的攻擊。另外參考許多門檻式授權代理簽章法[3-5, 19, 22, 25]的觀念，提出一個匿名的(t, n)

門檻式授權代理簽章法，讓 n 位原始簽章者授權給一位匿名的代理簽章者，而匿名代理簽章授權，必須在這一群原始簽章者中的其中 t 個人共同合作下方才能產生，同時能防禦匿名代理簽章者事後否認的攻擊。

三、結果與討論

(一) 匿名的代理簽章法回顧

首先回顧 Chaum 與 van Antwerpen [1]的不可否認簽章法中的否認協定。令 p 與 q 為兩個公開質數，滿足 $p= 2q+1$. 令$\omega \in Z_p^*$為一元素其秩為 q。使用者 Bob 秘密金鑰為 $a \in Z_q^*$ 與公開金鑰為 $\beta= \omega^a \bmod p$。此處 G 代表 Z_p^*中秩為 q 的乘法子群。對於任一個訊息 $M \in G$，使用者 Bob 的不可否認簽章是$\sigma= M^a \bmod p$。為了證明不可否認簽章σ為 Bob 的，Bob 須證明在 Z_P 中 $\log_\omega \beta= \log_M \sigma$。為了證明不可否認簽章σ不為 Bob 的，Bob 須向公信的單位證明在 Z_P 中 $\log_\omega \beta \neq \log_M \sigma$。假設驗證者為 Alice。否認協定如下：

步驟 1: Alice 在 Z_q^*中任選兩個亂數 e_1 與 e_2，計算且送 $c= \sigma^{e_1} \beta^{e_2} \bmod p$ 給 Bob。

步驟 2: Bob 計算且送 $d= c^{a^{-1}} \bmod p$ 給 Alice。

步驟 3: Alice 用 $d \neq M^{e1} \omega^{e2} \bmod p$ 驗證 d。

步驟 4: Alice 在 Z_q^*中任選另外兩個亂數 f_1 與 f_2，計算且送 $C= \sigma^{f_1} \beta^{f_2} \bmod p$ 給 Bob。

步驟 5: Bob 計算且送 $D= C^{a^{-1}} \bmod p$ 給 Alice。

步驟 6: Alice 用 $D \neq M^{f1} \omega^{f2} \bmod p$ 驗證 D。

步驟 7: Alice 得知σ是假的若且為若$(d\omega^{-e2})^{f1} \equiv (D\omega^{-f2})^{e1} \pmod p$.

因此當σ是假的，則在 Z_P 中 $\log_\omega \beta \neq \log_M$；不然 $\log_\omega \beta= \log_M$。

匿名的代理簽章法敘述如下。匿名的代理簽章法分成系統建置階段、代理授權階段、代理簽章產生與驗證階段、和代理簽章者識別階段。

系統建置階段

令 p 與 q 為兩個公開質數，滿足 $p= 2q+1$. 令 $g \in Z_p^*$為一元素其秩為 q。函數 h 為是單向雜湊函數。使用者 i 在 Z_q^*中任選他的秘密金鑰 x_i 且計算公開金鑰 $y_i= g^{x_i} \bmod p$。

代理授權階段

假設原始簽章者 A 欲授權給一位匿名代理簽章者 B。原始簽章者 A 隨機選一個整數 $k \in Z_q^*$，並且計算 $H= y_B^k \bmod p$ 與 $r= g^{-k}H \bmod p$。然後 A 計算 $s= k- rx_A h(m_W) \bmod q$，此處 m_w 代表代理授權書。代理授權書指出原始簽章者的公開金鑰、代理期間與其他的代理細節。原始簽章者 A 秘密地保管紀錄$(ID_B, (r, s), m_w)$。最終(r, s)與 m_w 透過秘密管道送給匿名代理簽章者 B。匿名代理簽章者 B 採用

$$g^s y_A^{rh(m_w)} r \equiv (g^s y_A^{rh(m_w)})^{x_B} \pmod p \qquad (1)$$

驗證(r, s)與 m_w。若等式(1)成立，匿名代理簽章者 B 儲存$((r, s), m_w, \alpha)$，此處$\alpha= g^s y_A^{rh(m_w)} \bmod p$。

代理簽章產生與驗證階段

假設匿名代理簽章者 B 欲對訊息 m 簽章。他首先選一個亂數 $t \in Z_q^*$，計算 $T= \alpha^t \bmod p$，然後找一個 U 滿足

$$h(m||r||s) \equiv Tx_B + tU \pmod q \qquad (2)$$

。最後(T, U)為訊息 m 的代理簽章。收到$((m_w, (r, s)), (m, (T, U)))$，驗證者首先計算$\alpha= g^s y_A^{rh(m_w)} \bmod p$ 與 $H= \alpha r \bmod p$。對於訊息 m 的代理簽章(T, U)，採用下列式子

$$\alpha^{h(m||r||s)} \equiv T^U H^T \pmod p \qquad (3)$$

。驗證(T, U)。

代理簽章者識別階段

當訊息 m 的代理簽章(T, U)產生糾紛時，必須確認匿名代理簽章者 B 的身分。假設原始簽章者 A 告訴公信單位 TTP，匿名代理簽章者

是 B 且秘密紀錄為(ID_B, (r, s), m_w)。公信單位 TTP 計算$\alpha = g^s y_A^{rh(m_w)} \bmod p$ 與 $H = \alpha r \bmod p$，並採用等式(3)驗證(T, U)。若代理簽章(T, U)合法，TTP 需要共同秘密指數驗證協定(common secret exponent validation protocol，簡稱 CSEV)，確定是否 $\log_g y_B = x_B = \log_\alpha H$。若 $\log_g y_B = x_B = \log_\alpha H$，則 B 是真正的匿名代理簽章者；若 $\log_g y_B \neq \log_\alpha H$，則 B 不是匿名代理簽章者。

共同秘密指數驗證協定

輸入：五項參數 g、y_B、α、H 與 x_B。

輸出：代表 $\log_g y_B = x_B = \log_\alpha H$ 的真假值。

步驟 1: 驗證者在 Z_q^*中任選兩個亂數 e_1 與 e_2，計算且送 $c = H^{e_1} y_B^{e_2} \bmod P$ 給辨護者。

步驟 2: 辨護者計算 $d = c^{x_B^{-1}} \bmod p$ 給驗證者。

步驟 3: 驗證者用 $d \equiv \alpha^{e_1} g^{e_2} \pmod P$驗證 d。若 $d \equiv \alpha^{e_1} g^{e_2} \pmod P$成立，則協定結束且 $\log_g y_B = x_B = \log_\alpha H$。

步驟 4: 驗證者在 Z_q^*中任選兩個亂數 f_1 與 f_2，計算且送 $c' = H^{f_1} y_B^{f_2} \bmod P$ 給辨護者。

步驟 5: 辨護者計算 $D = c'^{x_B^{-1}} \bmod p$ 給驗證者。

步驟 6: 驗證者用 $D \equiv \alpha^{f_1} g^{f_2} \pmod P$驗證 D。若 $D \equiv \alpha^{f_1} g^{f_2} \pmod P$成立，則協定結束且 $\log_g y_B = x_B = \log_\alpha H$。

步驟 7: 驗證者用$(dg^{-e_2})^{f_1} \equiv (Dg^{-f_2})^{e_1} \pmod p$驗證 D 與 d。若$(dg^{-e_2})^{f_1} \equiv (Dg^{-f_2})^{e_1} \pmod p$成立，則 $\log_g y_B \neq \log_\alpha H$；否則辨護者說謊。

一旦代理簽章與公開金鑰 H 被證明為代理簽章者 B 所擁有，為了保持匿名性，代理簽章者 B 需要被原始簽章者重新授權一把匿名的公開金鑰 H'。

(二) 匿名的多人授權代理簽章法

在匿名的多人授權代理簽章法中，匿名的代理簽章者為 U_B，必須在所有原始簽章者共同同意下，方能獲得匿名的代理簽章授權。

系統建置階段

令 p 與 q 為兩個公開質數，滿足 p= 2q+1。令 $g \in Z_p^*$為一元素其秩為 q。函數 h 為是單向雜湊函數。使用者 U_i 在 Z_q^*中任選他的秘密金鑰 x_i 且計算公開金鑰 $y_i = g^{x_i} \bmod p$。令原始簽章群為 $G_o = \{U_1, U_2, \ldots, U_n\}$，且匿名的代理簽章者為 U_B。原始簽章群的群公開金鑰為 $y_G = \prod_{i=1}^{n} y_i^{y_i} \bmod p$，群秘密金鑰為 $s_G = \sum_{i=1}^{n} x_i y_i \bmod q$。

代理授權階段

假設所有原始簽章群 G_o 中的成員，與匿名的代理簽章者 U_B 已經共同同意代理授權書內容。

步驟 1: G_o中的每一位成員 U_i在 Z_q^*中任選一個的亂數 k_i。

步驟 2: 每一位成員 U_i 計算 $H_i = y_B^{k_i} \bmod p$ 與$\alpha_i = g^{k_i} \bmod p$，然後以秘密的方式，將送$(H_i, \alpha_i)$給代理代理簽章者 U_B 與其它 G_o 中的成員 U_j，對 j= 1, 2, ..., n 且 $j \neq i$。

步驟 3: 收到(H_i, α_i)後，U_j 以驗證者身份和 U_i 以辨護者身份共同執行共同秘密指數驗證協定的前三個步驟，其協定使用的五個參數如下 g(=g)，$\alpha_i (= y_B)$，$y_B (= \alpha)$，H_i(= H)與秘密指數 k_i (= x_B)。然後 U_j 與 U_i 同意 $\log_g \alpha_i = k_i = \log_{y_B} H_i$。

步驟 4: 每位成員 U_i 計算$\alpha = \prod_{i=1}^{n} \alpha_i \bmod p = g^{\sum_{i=1}^{n} k_i} \bmod p$、$H = \prod_{i=1}^{n} H_i \bmod p = y_B^{\sum_{i=1}^{n} k_i} \bmod p$ 與 $R = \alpha^{-1} H \bmod p$。

然後 U_i 計算 $s_i = k_i - x_i y_i Rh(m_w) \bmod q$。以相同方式，$U_B$ 計算 R。

步驟 5: 每位成員 U_i 送 s_i 給 U_B 和其它成員。

步驟 6: U_B 和原始簽章群 G_o 中每位成員，利用$\alpha_i \equiv g^{s_i} y_i^{y_i Rh(m_W)} \pmod p$，驗證每一份個別的簽章 s_i。

步驟 7: 如果所有 s_i 都驗證通過，U_B 和原始簽章群 G_o 中每位成員計算 $S \equiv \sum_{i=1}^{n} s_i \equiv (\sum_{i=1}^{n} k_i) - Rh(m_w) \times (\sum_{i=1}^{n} x_i y_i) \pmod q$，然後每位成員 U_i 自己秘密保有紀錄 $(ID_B, (R, S), m_w)$。

代理簽章產生與驗證階段

此一階段與匿名的代理簽章法代理簽章產生與驗證階段相似。不同的是，匿名的代理簽章者 U_B 採取 $h(m||R||S) \equiv Tx_B + tU \pmod q$，取代 $h(m||r||s) \equiv Tx_B + tU \pmod q$，以對訊息 m 產生代理簽章(T, U)。而驗證者收到$((m_w, (R, S)), (m, (T, U)))$後，首先計算$\alpha \equiv g^S \times y_G^{Rh(m_W)} \pmod p$與 $H = \alpha R \bmod p$，再用$\alpha^{h(m||R||S)} \equiv T^U H^T \pmod p$驗證(T, U)。

代理簽章者識別階段

當訊息 m 的代理簽章(T, U)產生糾紛時，必須確認匿名代理簽章者 U_B 的身分。假設原始簽章群 G_o 告訴公信單位 TTP，匿名代理簽章者是 U_B 且秘密紀錄為$(ID_B, (R, S), m_w)$。公信單位 TTP 計算$\alpha = g^S \times y_G^{Rh(m_W)} \bmod p$ 與 $H = \alpha R \bmod p$，此處 $y_G = \prod_{i=1}^{n} y_i^{y_i} \bmod p$。公信單位 TTP 利用共同秘密指數驗證協定確認 $\log_g y_B = x_B = \log_\alpha H$。若 $\log_g y_B = x_B = \log_\alpha H$，則 U_B 是真正的匿名代理簽章者；若 $\log_g y_B \neq \log_\alpha H$，則 U_B 不是匿名代理簽章者。一旦代理簽章與公開金鑰 H 被證明為代理簽章者 U_B 所擁有，為了保持匿名性，代理簽章者 U_B 需要被原始簽章者重新授權一把匿名的公開金鑰 H'。

(三) 匿名的門檻式授權代理簽章法

匿名的門檻式授權代理簽章法中，匿名的代理簽章者為 U_B，必須獲得 n 位原始簽章者中任意 t 位或 t 位以上的原始簽章者共同授權，方能得到代理的權力。假設原始簽章群為 $G_o = \{U_1, U_2, ..., U_n\}$

系統建置階段

在此階段，原始簽章群 G_o 需要一個公信的金鑰授權中心(a trusted key authentication center，簡稱 KAC)協助。KAC 任選兩個公開的質數 p 與 q，滿足 $p = 2q+1$。KAC 公開一個秩為 q 的元素 $g \in Z_p^*$。對原始簽章群 G_o，KAC 在 Z_q^*上隨機造了一個 t-1 次方秘密多項式 $f(x) = a_0 + a_1 x + a_2 x^2 + \ldots + a_{t-1} x^{t-1}$，因此原始簽章群 G_o 的秘密金鑰為 f(0)且成員 U_i 秘密機密為 $f(ID_i)$，此處 ID_i 為成員 U_i 身分代號。然後 KAC 計算原始簽章群公開金鑰 $Y_G = g^{f(0)} \bmod p$ 與個別的公開金鑰 $y_{p_i} = g^{f(ID_i)} \bmod p$，給原始簽章群 G_o 中的成員 U_i。

代理授權階段

令原始簽章群 G_o 中的 t 位成員組成 $D = \{U_1, U_2, \ldots, U_t\}$，欲授權給匿名的代理簽章者 U_B。假設 D 群中 t 位成員，與匿名的代理簽章者 U_B 已經共同同意代理授權書 m_w，且代理授權書 m_w 也明列 t 位成員名單。

步驟 1: D 中的每一位成員 U_i 在 Z_q^*中任選一個的秘密隨機數 k_i，而且計算$\alpha_i = g^{k_i} \bmod p$ 與 $H_i = y_B^{k_i} \bmod p$，然後 U_i 以安全方式，廣播 (H_i, α_i)給 U_B 與 D 中的其他成員。

步驟 2: 收到(H_i, α_i)後，成員 U_j 以驗證者身份和 U_i 以辨護者身份共同執行共同秘密指數驗證協定的前三個步驟，其協定使用的五個參數如下 $g(=g)$，$\alpha_i(=y_B)$，$y_B(=\alpha)$，$H_i(=H)$ 與秘密指數 k_i $(=x_B)$。然後 U_j 與

U_i 同意 $\log_g \alpha_i = k_i = \log_{y_B} H_i$。

步驟 3: D 中的每位成員 U_i 計算 $\alpha = \prod_{i=1}^{t} \alpha_i \bmod p = g^{\sum_{i=1}^{t} k_i} \bmod p$、 $H = \prod_{i=1}^{t} H_i \bmod p = y_B^{\sum_{i=1}^{t} k_i} \bmod p$ 和 $R = \alpha^{-1} H \bmod p$。代理簽章者 U_B 也以相同方式計算。

步驟 4: D 中的每位成員 U_i 用自己的秘密機密 $f(ID_i)$與自己的秘密金鑰，對代理授權書 m_w，計算 $s_i = (f(ID_i)L_i + x_i y_i) \times R \times h(m_w) - k_i \bmod q$，此處

$$L_i = \prod_{j=1, j\neq i}^{t} \frac{-ID_j}{ID_i - ID_j} \bmod q$$。

步驟 5: 所有 D 中的每位成員 U_i，廣播自己的部分簽章 s_i，給其他成員與代理簽章者 U_B。

步驟 6: 當代理簽章者 U_B 與 D 中的 t 位成員收齊所有部分簽章 s_i，他們利用 $g^{s_i} \times \alpha_i \equiv ((y_{p_i}^{L_i}) \times (y_i^{y_i}))^{Rh(m_w)} \pmod p$，驗證每一份部分簽章 s_i，此處 $y_i = g^{x_i} \bmod p$ 且 $y_{p_i} = g^{f(ID_i)} \bmod p$。

步驟 7: 若所有部分簽章 s_i 合法，則代理簽章者 U_B 與 D 中的 t 位成員計算 $S \equiv \sum_{i=1}^{t} s_i \equiv R \times h(m_w) \times \sum_{i=1}^{t} (f(ID_i)L_i + x_i y_i) - \sum_{i=1}^{t} k_i \pmod q$。所以代理憑證為$(m_w, (R, S))$。D 中的 t 位成員秘密保有紀錄$(ID_B, (R, S), m_w)$。

代理簽章產生與驗證階段

此階段與匿名的代理簽章法代理簽章產生與驗證階段相似。匿名的代理簽章者 U_B 首先在 Z_q^*中任選一個隨機數 t，計算 $T = g^t \bmod p$，並找出一個 U 滿足 $h(m||R||S) \equiv Tx_B + tU \pmod q$。驗證者首先計算$\alpha = (Y_{G_s} \times y_D)^{Rh(m_w)} \times g^{-S} \bmod p$ 與 $H = \alpha R \bmod p$，此處 $Y_{G_s} = \prod_{i=1}^{t} y_{p_i}^{L_i} \bmod p$ 且 $y_D = \prod_{i=1}^{t} y_i^{y_i} \bmod p$。然後用$\alpha^{h(m||R||S)} = T^U H^T \bmod p$ 驗證(T, U)。

代理簽章者識別階段

當訊息 m 的代理簽章(T, U)產生糾紛時，必須確認匿名代理簽章者 U_B 的身分。假設 D 群告訴公信單位 TTP，匿名代理簽章者是 U_B 且秘密紀錄為$(ID_B, (R, S), m_w)$。公信單位 TTP 計算$\alpha = g^S \times y_G^{Rh(m_w)} \bmod p$ 與 $H = \alpha R \bmod p$，此處 $y_G = \prod_{i=1}^{n} y_i^{y_i} \bmod p$。公信單位 TTP 利用共同秘密指數驗證協定確認 $\log_g y_B = x_B = \log_\alpha H$。若 $\log_g y_B = x_B = \log_\alpha H$，則 U_B 是真正的匿名代理簽章者；若 $\log_g y_B \neq \log_\alpha H$，則 U_B 不是匿名代理簽章者。一旦代理簽章與公開金鑰 H 被證明為代理簽章者 U_B 所擁有，為了保持匿名性，代理簽章者 U_B 需要被原始簽章者重新授權一把匿名的公開金鑰 H'。

四、計畫成果自評

本計畫的結果分別提出了一個匿名的多人授權代理簽章法，讓一群原始簽章者，必須在所有成員共同同意下，方能授權給一位匿名的代理簽章者，此外也提出一個匿名的(t, n) 門檻式授權代理簽章法，讓 n 位原始簽章者授權給一位匿名的代理簽章者，而匿名代理簽章授權，必須在這一群原始簽章者中的其中 t 個人共同合作下方才能產生。兩個方法皆能防禦匿名代理簽章者事後否認的攻擊。因此達成本計畫的目標：具可匿名代理人的群體導向授權代理簽章法之設計。

五、參考文獻

[1] Chaum, D. and Van Heyst, E. V., “Group

signatures," *Pre-proceeding of Eurocrypt'91, Lecture Notes in Compute Science*, Vol. 547, Springer, Berlin, 1991, pp. 257-265.

[2] Harn, L., "Group-oriented (t, n) threshold digital signature scheme and digital multi-signature," *IEE Proceed Computer Digital Technicality*, Vol. 141, No. 5, 1994, pp. 307-313.

[3] Hsu, Chien-Lung, Wu, Tzong-Sun, and Wu, Tzong-Chen, "New nonrepudiable threshold proxy signature scheme with known signers," *The Journal of Systems and Software*, Vol. 58, 2001, pp. 119-124.

[4] Hwang, Min-Shiang, Lin, Iuon-Chang, and Lu, Jui-Lin Eric, "A secure nonrepudiable threshold proxy signature scheme with known signers," *INFORMATICA*, Vol. 11, No. 2, 2000, pp. 137-144.

[5] Hwang, Shin-Jia, and Chen, Chiu-Chin, "Cryptanalysis of Nonrepudiable Threshold Proxy Signature Schemes with Known Signers," *2002 Information Security Conference*, Taichung, Taiwan, R.O.C., May 16-17, 2002, pp. 243-246. Also appear in *Journal of Informatica*.

[6] Hwang, Shin-Jia, and Chen, Chiu-Chin, "A New Multi-Proxy Multi-Signature Scheme," *2001 National Computer Symposium: Information Security*, Taipei, Taiwan, R.O.C., Dec. 20-21, 2001, pp. F019-F026. Also appear in *Applied Mathematics and Computation.*

[7] Hwang, Shin-Jia, and Chen, Chiu-Chin, "A New Proxy Multi-Signature Scheme," *The 2001 International Workshop on Cryptology and Network Security*, Taipei, Taiwan, R.O.C., Sep. 26-28, 2001, pp. 199-204.

[8] Hwang, Shin-Jia and Shi, Chi-Hwai, "A simple multi-proxy signature scheme," *Proceedings of the Tenth National Conference on Information Security,* Taiwan, 2000, pp. 134-138.

[9] Hwang, Shin-Jia and Shi, Chi-Hwai, "A proxy signature scheme without using one-way hash functions," *2000 International Computer Symposium*, Chiayi, Taiwan, R.O.C., Dec. 6-8, 2000, pp. 60-64.

[10] Hwang, Shin-Jia and Shi, Chi-Hwai, "The specifiable proxy signature," *National Computer symposium 1999*, Vol. 1334, Taiwan, December 1999, pp. 190-197.

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

[12] Lee, Narn-Yih, Hwang, Tzonelih, and Wang, Chin Hung, "On Zhang's nonrepudiable proxy signature schemes," *Third Australasian Conference,* ACISP '98, 1998, pp. 415-422.

[13] Li, Z. C., Hui, L. C. K., Chow, K. P., Chong, C. F., Tsang, H. H., and Chan, H. W., "Cryptanalysis of Harn digital multi-signature scheme with distinguished signing authorities," *Electronics Letters,* Vol. 36, No. 4, 2000, pp. 314- 315.

[14] MAMBO, Masahiro, USUDA Keisuke, and OKAMOTO, Eiji, "Proxy signatures: Delegation of the power to sign message," *IEICE. Trans. Fundamentals*, E79-A, 9, 1996, pp. 1338-1354.

[15] MAMBO, Masahiro, USUDA, Keisuke, and OKAMOTO, Eiji, "Proxy signatures for

delegation signing operation," *Proc. 3nd ACM Conference on Computer and Communication Security,* 1996, pp. 48-57.

[16] Shum, K. and Wei, Victor K., "A strong proxy signature scheme with proxy signer privacy protection," *Proceedings of the IEEE International Workshops on Enabling Technologies*: Infrastructure for Collaborative Enterprises (WETICE'02), 2002, pp. 55-56.

[17] Sun, Hung-Min, "Design of time-stamped proxy signatures with traceable receivers," *IEE Proc.-Comput. Digit. Tech,* Vol. 147, No. 6, November 2000, pp. 462-466.

[18] Sun, Hung-Min, "On proxy (multi-) signature schemes," *2000 International Computer Symposium*, Chiayi, Taiwan, R.O.C., Dec. 6-8, 2000, pp. 65-72.

[19] Sun, Hung-Min, "An efficient nonrepudiable threshold proxy signature scheme with known signers," *Computer Communications,* Vol. 22, 1999, pp. 717-722.

[20] Sun, Hung-Min, Hsieh, and Bin-Tsan, "Time-stamp proxy signatures with traceable receivers," *Proceedings of the Ninth National Conference on Information Security,* Taiwan, 1999, pp. 247-253.

[21] Sun, Hung-Min, and Hsieh, Bin-Tsan, "Remark on two nonrepudiable proxy signature schemes," *Proceedings of the Ninth National Conference on Information Security,* Taiwan, 1999, pp. 241-246.

[22] Sun, Hung-Min, Lee N.-Y., and Hwang, T, "Threshold proxy signatures," *IEE Proceedings-computers & Digital Techniques,* Vol. 146, No. 5, September 1999, pp. 259-263.

[23] Yen, Sung-Ming, Hung, Chung-Pei, and Lee, Yi-Yuan, "Remarks on some proxy signature schemes," *2000 International Computer Symposium,* Chiayi, Taiwan, R.O.C., Dec. 6-8, 2000, pp. 54-59.

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

[25] Zhang, K., "Threshold proxy signature schemes," *1997 Information Security Workshop*, Japan, September 1997, pp. 191-197.