行政院國家科學委員會專題研究計畫　成果報告

可匿名代理簽章群的群體導向代理簽章法之設計

計畫類別：個別型計畫
計畫編號：NSC93-2213-E-032-020-
執行期間：93 年 08 月 01 日至 94 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　黃嘉濰

報告類型：精簡報告

處理方式：本計畫可公開查詢

中　華　民　國 94 年 9 月 15 日

行政院國家科學委員會補助專題研究計畫 ☑ 成 果 報 告 □期中進度報告

可匿名代理簽章群的群體導向代理簽章法之設計

計畫類別：☑ 個別型計畫　　□整合型計畫

計畫編號：NSC93－2213－E－032－020－

執行期間：　93 年 8 月 1 日至　94 年 7 月 31 日

計畫主持人：黃心嘉　淡江大學資工系　　副教授

共同主持人：

計畫參與人員：陳光熹 淡江大學資工系　　研究生

黃嘉濰 淡江大學資工系　　研究生

成果報告類型(依經費核定清單規定繳交)：☑精簡報告 □完整報告

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

處理方式：除產學合作研究計畫、提升產業技術及人才培育研究計畫、列管計畫及下列情形者外，得立即公開查詢

□涉及專利或其他智慧財產權，□一年□二年後可公開查詢

執行單位：淡江大學資工系

中　華　民　國　九十四 年八月三十一日

一、中英文摘要

中文摘要

所謂的具匿名性質的代理簽章法，即滿足代理簽章者身份是不對外公開的，而驗證者可以不需要知道代理簽章者的身份即可驗證代理簽章的代理簽章法。Shum 跟 Wei 兩位學者首先提出了相關的代理簽章法，但是 Shum 跟 Wei 的方法會遭受到代理簽章偽造攻擊，所以是不安全的方法。本計畫首先提出新的匿名代理簽章法。此外為了可以授權給匿名代理簽章群，提出匿名的多人代理簽章法，以及匿名的門檻式代理簽章法，在新的匿名多人與門檻式代理簽章法中，匿名代理簽章群中每一個匿名的代理簽章者都無法知道其他代理簽章者的身份，以達到對匿名代理簽章者最大的匿名保護。

英文摘要

In an anonymous proxy signature scheme, the identity of a proxy singer is publicly unknown and anonymous proxy signatures are validated without knowing proxy signers. Shum and Wei first proposed related proxy signature scheme. However, their scheme is not secure against the forgery attack of proxy signatures. So, in this project, a new anonymous proxy signature scheme is first proposed. For the group-oriented applications, our anonymous multi-proxy signature scheme and anonymous threshold proxy signature scheme are also proposed. Moreover, the anonymity of our anonymous multi-proxy signature scheme is so strong that any proxy signer cannot know the identity of anyone in the proxy group. Then the anonymity of each proxy signer has the strong protection.

關鍵字: Digital signature scheme, proxy signature scheme, multi-proxy signature scheme, threshold proxy signature scheme

二、前言與研究目的

為了在數位簽章法中提供代理的功能，日本學者 Mambo 等人[16, 17]提出代理簽章的觀念。但是過往的代理簽章法，為了保護代理簽章者受到原始簽章者的偽造代理簽章攻擊，就必須利用代理簽章者的公開金鑰驗證代理簽章，然而如此一來就無法隱匿代理簽章者的身份，保護代理簽章者的隱私。為了保護代理簽章者的隱私，代理簽章者必須是匿名，但是必須防止代理簽章者事後否認代理簽章的問題。因此本年度計畫將先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，也就是原始簽章者可以授權給一個由多人組成的匿名代理簽章群。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代理簽章法，讓一位原始簽章者授權給一群匿名的代理簽章者，而匿名多人代理簽章必須在代理簽章群所有人合作下才能產生。此外也提出匿名的門檻式代理簽章法，讓一位原始簽章者授權給一個匿名代理簽章群，而匿名門檻式代理簽章產生，必須在匿名代理簽章群中，超過門檻人數代理簽章者的合作下才能產生。在兩個方法中，匿名代理簽章授權，皆可以防範匿名代理簽章群，事後否認產生匿名代理簽章的安全顧慮。

三、文獻探討

Shum 跟 Wei 學者方法回顧

在 Shun 與 Wei 方法[20]中一共有四類的成員，公正的機構 T，原始簽章者 O，代理簽章者 P 和簽章驗證者 V。方法中使用的符號如下：p 和 q 為兩個大質數滿足 q|p-1，元素 g 為在 Z_p^*中 order 為 q 的生成子，h()為一個安全的單向賀序函數，m_w 為一個代理委任書，$x_u \in Z_q^*$為使用者 u 的私密金鑰，$y_u=g^{x_u} \bmod p$ 為使用者 u 的公開金鑰，sign()為簽章產生演算法，verify()為簽章驗證演算法。

別名發佈階段

假設公正的機構 T 傳送一個別名 h_p 給代理簽章者 P，發佈別名的程序如下:

步驟 1: 代理簽章者 P 傳送他的身份 ID_P 給公正的機構 T。

步驟 2: 公正的機構 T 選擇一個隨機數 $k_P \in Z_q^*$，T 計算 $h_P=h(k_P, ID_P)$，$r_T=g^{k_T} \bmod p$，和 $s_T= x_T h(h_P, r_T)+k_T \bmod q$。接著 T 傳送$(h_P, r_T, s_T)$給 P。

步驟 3: 代理簽章者 P 利用驗證式 $g^{s_T}=y_T^{h(h_P, r_T)}$測試$(h_P, r_T, s_T)$的正確性，如果驗證式通過則信任$(h_P, r_T, s_T)$為公正的機構 T 所發佈的別名 h_p。

代理授權階段

原始簽章者 O 產生代理授權參數(m_w, r_O, s_O)給代理簽章者 P。

步驟 1: 原始簽章者 O 選擇隨機數 $k_O \in Z_q^*$，然後計算 $r_O=g^{k_O} \bmod p$ 和 $s_O=x_O h(m_w, r_O)+k_O \bmod q$。接著他傳送$(m_w, r_O, s_O)$給 P。

步驟 2: 代理簽章者 P 接收到(m_w, r_O, s_O)後，利用驗證式 $g^{s_O} \equiv y_O^{h(m_w, r_O)} r_O \pmod p$ 驗證(m_w, r_O, s_O)是否合法正確。

簽章與驗證階段

代理簽章者 P 計算一把代理私密金鑰 $s= s_O+s_T \bmod q$，接著利用任何一種離散對數型的數位簽章法對明文 m 產生代理簽章α。P 把$(m, \alpha, r_O, m_w, ID_O, h_P, r_T)$傳送給驗證者 V。驗證者 V 計算出對應的代理公開金鑰 $y= y_O^{h(m_w, r_O)} r_O \, y_T^{h(h_P, r_T)} r_T \bmod p$ 接著用驗證者公開金鑰 y 以及驗證者簽章對應的簽章，驗證演算法驗證代理簽章α是否正確。

匿名撤銷階段

如果驗證者想知道代理簽章者的身份，他先傳送別名 h_P 給公正的機構 T，接著公正的機構 T 回傳 k_P 和 ID_P。最後驗證者利用驗證式 $h_P=h(k_P, ID_P)$來驗證 ID_P 和 h_P 是否正確。最後驗證者就知道別名 h_P 的代理簽章者身份 ID_P。

然而根據[15, 25]的研究成果發現，Shun 與 Wei 方法並無法抵抗代理簽章偽造的攻擊。

四、研究方法

本計畫首先針對我們所提出的匿名代理簽章法進行研究，重點在於如何讓代理簽章群可以真正匿名的授權法進行研究，尤其如何防止代理簽章群否認，與原始簽章者偽造代理簽章的兩種主要攻擊進行考量。再者對三種類型的代理簽章法進行詳細的研究，在第一種類型的代理簽章法－群體授權與群體的門檻式代理簽章法中，探討一個代理簽章群者如何在超過一定門檻數即可產生代理授權的機制，另外為了安全分析，也將探討Sun學者[21]所

提出具有指定代理簽署者功能的門檻式代理簽章法，為何易遭受共謀攻擊，以及Hwang等學者對所提出的改良方法如何克服共謀攻擊的問題。也將研究Hwang與Chen[6]指出Sun學者的方法及Hwang等學者[5]的方法為何不安全之處；更進一步地，我們也將探討Hsu等學者[4]所提出的方法為何不會遭受共謀攻擊，以及其方法的通訊量與計算量為何較Sun 學者的方法少的原因。第二種類型的代理簽章法，我們將探討多人授權代理簽章法，研究多位原始簽章者如何授權予一位代理簽章者的簽章機制，藉以了解Sun學者[23]的方法和Yi等學者[28]的方法為何同樣都會有當原始代理群的人數過於龐大時，授權書也會相對的成同比例成長的問題，並研究Hwang與Chen [7]的方法為何沒有此項缺點，更進一步地，我們將深入探討Hwang與Chen的方法為何能防禦multisignature 中強大的insider attack 的攻擊。第三種要探討的代理簽章法為多人授權予多人的代理簽章法，深入了解如何在兩個群體中進行授權及如何產生代理簽章的機制，並研究Hwang與Chen [7]的方法中兩個群體的架構，探討其中的計畫量，通訊量等問題，另外，也將研究此多人授權予多人的代理簽章法為何也能抵抗insider attack的攻擊。最後我們將設計可以讓代理簽章群如同單一位代理簽章者一般，彼此確認對方不作假的情況下，產生匿名的代理簽章者。再將之轉換到門檻式的代理簽章群在彼此確認對方不作假的情況下，產生匿名的代理簽章者。最後研究如何使代理簽章群無法在事後否認，我們預定從群體導向式的不可否認簽章法上下手。

五、結果與討論

本計畫的結果提出了匿名的代理簽章法、匿名的多人代理簽章法、匿名的門檻式代理簽章法。這些方法分別敘述如下。

匿名的代理簽章法

基於離散對數且利用委任書(warrant)的匿名代理簽章法描述如下。此方法一共有四種成員：原始簽章者 U_O，代理簽章者 U_P，驗證者 V 和公正的第三方 TTP。首先說明的是公開系統參數和函數部分。p 和 q 是兩個大質數且符合 $p = 2q+1$ 要求，元素 g 是一個在 Z_p^* 中且 order 為 q 的生成子，h()是一個賀序函數。每一個使用者 U_i 都有一個身份 ID_i，一把私密金鑰 $x_i \in Z_q^*$，和一把經過認證的公開金鑰 $y_i = g^{x_i} \bmod p$。在代理委任書 M_W 上，定義了原始簽章者 U_O，原始簽章者經過認證的公開金鑰 y_O，合法代理的授權期限和必要的代理細節。

該方法有下列的演算法，經由這些演算法，就可以構成匿名代理簽章法。這些演算法描述如下。

演算法 $\mathbf{Auth_{APDW}(U_O, U_P, M_W, b, Proxy\text{-}Certificate)}$

輸入: 使用者 U_O 和 U_P 的身份以及委任書 M_W

輸出: 秘密值 b 和 Proxy-Certificate

步驟 1: U_O 隨機在 Z_q^* 中選擇一個秘密值 $b \in Z_q^*$，接著計算 $y = y_P g^b \bmod p$

步驟 2: U_O 使用離散對數型的簽章產生法和私密金鑰 x_O 對 $h(M_W, y, h(bg^b \bmod p))$ 產生簽章(r, s)。Proxy-Certificate=$(M_W, y, h(bg^b \bmod p), (r, s))$。

步驟 3: U_O 透過安全通道傳送 Proxy-Certificate 和授權的秘密值 b 給 U_P。

演算法 $\mathbf{VerAuth_{APDW}(U_O, U_P, b', Proxy\text{-}Certificate)}$

輸入: U_O 和 U_P 的身份和秘密值 b'和 Proxy-Certificate

輸出: 由 VerCertAPDW(U_O, Proxy-Certificate)所回傳的布林值

步驟 1: U_P 計算代理公開金鑰 $y'= y_P g^{b'} \bmod p$ 和 $h'= h(b' g^{b'} \bmod p)$。接著確認 $h(M_W, y, h(bg^b \bmod p))= h(M_W, y', h(b'g^{b'} \bmod p))$。

步驟 2: 代理簽章者利用 $\text{VerCert}_{APDW}(U_O,$ Proxy-Certificate)確認 Proxy-Certificate 的正確性。

步驟 3: 若 $\text{VerCert}_{APDW}(U_O,$ Proxy-Certificate)回傳 true，則代理簽章者計算代理秘密金鑰 $x= x_P+b$ 並且回傳 true，否則結束程序並回傳 false。

演算法 $\text{VerCert}_{APDW}(U_O,$ Proxy-Certificate)

輸入: U_O 的身份和 Proxy-Certificate。

輸出: 布林數。如果 Proxy-Certificate 被驗證通過則回傳 true 否則回傳 false。

步驟 1: 驗證者計算 $H= h(M_W, y, h(bg^b \bmod p))$。

步驟 2: 驗證者用公開金鑰 y_O，離散對數型的簽章驗證演算法及 H 去驗證簽章(r, s)的正確性，若驗證通過則回傳 true, 否則回傳 false。

演算法 $\text{ID}_{APDW}(\text{TTP}, U_O, y_p,$ b', Proxy-Certificate)

輸入: 公正的第三方 TTP，U_O 的身份，經過認證的公開金鑰 y_P，由 U_O 提供的秘密值 b'和 Proxy-Certificate

輸出: 布林數。如果證明代理秘密金鑰 x 和代理公開金鑰的對應關係只會被知道 x_P 的人所產生則回傳 true，否則回傳 false。

步驟 1: TTP 利用函式 $\text{VerCert}_{APDW}(U_O,$ Proxy-Certificate)驗證 Proxy-Certificate，若通過驗證則 TTP 確信代理公開金鑰被原始簽章者所認證。

步驟 2: TTP 計算 $g^{b'} \bmod p$ 和 $y'= g^{b'} y_P \bmod p$ 並且檢查 $h(g^{b'} y_P \bmod p)= h(g^b y_P \bmod p)$和 $y'=y$ 兩個等式是否都成立，如果等式皆成立則回傳 true，否則回傳 false。

在新的匿名代理簽章法中共分為四個階段：系統初始階段、代理授權階段、代理簽章的產生與驗證階段、和代理簽章者的識別階段。

系統初始階段

系統的公開參數和函示如同上述，對於每一位使用者 U_i 都有一個身份 ID_i，一把私密金鑰 x_i 和對應的公開金鑰 $y_i=g^{x_i}$。M_W 則代表代理授權的委任書。

代理授權階段

原始簽章者 U_O 首先執行 $\text{Auth}_{APDW}(U_O, U_P, M_W,$ b, Proxy-Certificate)產生秘密值 b 和 Proxy-Certificate 並送給代理簽章者 U_P。代理簽章者 U_P 收到秘密值 b 和 Proxy-Certificate 後利用函式 $\text{VerAuth}_{APDW}(U_O, U_P,$ b', Proxy-Certificate)來做驗證。如果 $\text{VerAuth}_{APDW}(U_O, U_P,$ b', Proxy-Certificate)回傳 true 則代理簽章者計算代理私密金鑰 $x=x_P+b \bmod q$ 和對應的代理公開金鑰 $y=g^x \bmod p= y_P g^b \bmod p$。

代理簽章的產生與驗證階段

首先代理簽章者 U_P 利用代理秘密金鑰 x 及離散對數型的簽章法 $DLS_{(x, y)}(h(m||r||s))$對明文 m 產生代理簽章(R, S)。當驗證者收到(R, S)和 m 後利用 $VerAuth_{APDW}(U_O, U_P, b', Proxy\text{-}Certificate)$，驗證 Proxy-Certificate 和代理公開金鑰 y 是否為原始簽章者所合法授權的，若正確則利用代理公開金鑰及 DLS 使用的簽章驗證演算法來驗證代理簽章(R, S)。

代理簽章者的識別階段

若匿名的代理簽章(R, S)有任何爭議，原始簽章者必須使用執行 $ID_{APDW}(TTP, U_O, y_p, b', Proxy\text{-}Certificate)$來揭發匿名代理簽章者的身份並使公正的第三方信任只有知道秘密金鑰 x_P 的人才可產生代理秘密金鑰 x。

匿名的多人代理簽章法

基於離散對數型的數位簽章法，利用代理委任書(warrant)的匿名多人代理簽章法描述如下。此方法一共有四種成員：原始簽章者 U_O，匿名代理簽章群 $G_P(U_1, U_2, \ldots, U_n)$，驗證者 V 和公正的第三方 TTP。首先說明的是公開系統參數和函數部分。p 和 q 是兩個大質數必且符合 p= 2q+1，g 是一個在 Z_p^* 中且 order 為 q 的生成子，h()是一個賀序函數。每一個使用者 U_i 都有一個身份 ID_i，一把私密金鑰 $x_i \in Z_p^*$，合一把經過認證的公開金鑰 $y_i=g^{x_i} \bmod p$。在代理委任書裡面定義了原始簽章者 U_O，原始簽章者經過認證的公開金鑰 y_O，合法的授權期限和必要的代理細節描述。

演算法 $Auth_{AMPDW}(U_O, G_P, M_W, \{b_1, b_2, \ldots, b_n\}, Proxy\text{-}Certificate)$

輸入: U_O 和 G_P 的身份和代理委任書(M_W)

輸出: 秘密值($b_1, b_2, \ldots, b_n$)

步驟 1: 原始簽章者 U_O 為每一位代理簽章者 U_i 選擇一個秘密值 $b_i \in Z_q^*$ 並計算 $g^{b_i} \bmod p$ 和 $g^{\Sigma_{i=1}^{n} b_i} \bmod p$。接著 U_O 計算每一把獨立的代理公開金鑰 $y_{G_i}=y_i g^{b_i} \bmod p$ 和 $y_{G_P}=\Pi_{i=1}^{n} y_i g^{\Sigma_{i=1}^{n} b_i} \bmod p$。

步驟 2: 原始簽章者 U_O 利用私密金鑰 x_O 和離散對數型的簽章法對摘要 $h(M_W, y_{G_P}, \{(y_{G_1}, h(b_1 g^{b_1} \bmod p)), (y_{G_2}, h(b_2 g^{b_2} \bmod p)), \ldots, (y_{G_n}, h(b_n g^{b_n} \bmod p))\})$產生簽章(r, s)。則 $Proxy\text{-}Certificate=(M_W, y_{G_P}, \{(y_{G_1}, h(b_1 g^{b_1} \bmod p)), (y_{G_2}, h(b_2 g^{b_2} \bmod p)), \ldots, (y_{G_n}, h(b_n g^{b_n} \bmod p))\}, (r, s))$。

步驟 3: 原始簽章者送 Proxy-Certificate 和授權的秘密值 b_i 透過安全的方法傳送給匿名代理簽章群 G_P 中的每一位代理簽章者 U_i。

演算法 $VerAuth_{AMPDW}(U_O, G_P, \{b_1', b_2', \ldots, b_n'\}, Proxy\text{-}Certificate)$

輸入: U_O 和匿名代理簽章群 G_P 的身份，秘密值$\{b_1, b_2, \ldots, b_n\}$和 Proxy-Certificate。

輸出: 由函式 $VerCert_{AMPDW}(U_O, Proxy\text{-}Certificate)$所回傳的布林值。

步驟 1: 每一位在匿名代理簽章群 G_P 中的代理簽章者 U_i 首先計算自己的公開金鑰 $y_{G_i}'=y_i g^{b_i} \bmod p$ 和 $h'=h(b_i' g^{b_i'} \bmod p)$，接著檢查 $h(M_W, y_{G_P}, \{(y_{G_1}, h(b_1 g^{b_1} \bmod p)), (y_{G_2}, h(b_2 g^{b_2} \bmod p)), \ldots, (y_{G_i}, h(b_i g^{b_i} \bmod p)), \ldots, (y_{G_n}, h(b_n g^{b_n} \bmod p))\}) = h(M_W, y_{G_P}, \{(y_{G_1}, h(b_1 g^{b_1} \bmod p)), (y_{G_2}, h(b_2 g^{b_2} \bmod p)), \ldots, (y_{G_i}', h(b_i' g^{b_i'} \bmod p)), \ldots,$

$(y_{G_n}, h(b_n g^{b_n} \bmod p))\}$)是否成立。

步驟 2: G_P 中的代理簽章者 U_i 執行函式 $VerCert_{AMPDW}(U_O,$ Proxy-Certificate)檢查 Proxy-Certificate。

步驟 3: 若 $VerCert_{AMPDW}(U_O,$ Proxy-Certificate)回傳 true 而且 $y_{G_P}=\Pi_{i=1}{}^{n} y_{G_i} \bmod p$，代理簽章者 U_i 計算代理秘密金鑰 $x_{G_i}=x_i+b_i \bmod q$。若所有的代理簽章者接回傳 true 給原始簽章者，則原始簽章者回傳 true，否則回傳 false。

演算法 $VerCert_{AMPDW}(U_O,$ Proxy-Certificate)

輸入: U_O 的身份和 Proxy-Certificate

輸出: 如果 Proxy-Certificate 通故所有使用者 U_i 的驗證，則回傳布林數 true，否則回傳 false。

步驟 1: 驗證者計算 $H= h(M_W, y_{G_P}, \{(y_{G_1}, h(b_1 g^{b_1} \bmod p)), (y_{G_2}, h(b_2 g^{b_2} \bmod p)), \ldots, (y_{G_n}, h(b_n g^{b_n} \bmod p))\})$

步驟 2: 驗證者利用公開金鑰 y_O 和離散對數型的驗證式來驗證 Proxy-Certificate。如果簽章(r, s) 正確且 $y_{G_P}=\Pi_{i=1}{}^{n} y_{G_i} \bmod$ 則 Proxy-Certificate 驗證通過且回傳布林值 true，否則回傳 false。

演算法 $ID_{AMPDW}(TTP, U_O, \{y_1, y_2, \ldots, y_n\}, G_P, M_W, \{b_1, b_2, \ldots, b_n\},$ Proxy-Certificate)

輸入: 公正的第三方(TTP)，U_O 的身份，每一位代理簽章者經過認證的公開金鑰$\{y_1, y_2, \ldots, y_n\}$，$U_O$ 所提供的秘密值$\{b_1, b_2, \ldots, b_n\}$和 Proxy-Certificate

輸出: 如果確認了秘密金鑰 x_i 和公開金鑰 y_i 只能被知道 x_{G_i} 的使用者知道則回傳 true，否則回傳 false。

步驟 1: 公正的第三方 TTP 首先用 $VerCert_{AMPDW}(U_O,$ Proxy-Certificate) 驗證 Proxy-Certificate，則公正的第三方可以確認群代理公開金鑰 y_{G_P} 和個別的代理公開金鑰 y_{G_i} 是被原始簽章者 U_O 所認證。

步驟 2: 公正第三方計算每一個 $y_{G_i}'=y_i g^{b_i'} \bmod$ 和 $y_{G_P}'=\Pi_{i=1}{}^{n} y_i g^{\Sigma_{i=1}{}^{n} b_i'} \bmod$ 接著在檢查等式 $h(b_i g^{b_i} \bmod p)= h(b_i' g^{b_i'} \bmod p)$和 $y_{G_i}=y_{G_i}'$對於每一個 i=1, 2, …, n，如果兩等式皆成立則回傳 true，否則回傳 false。

在新的匿名多人代理簽章法中共分為四個階段：系統初始階段，代理授權階段，代理簽章的產生與驗證階段和代理簽章者的識別階段。

系統初始階段

如同上述匿名代理簽章的代理簽章法。

代理授權階段

原始簽章者 U_O 先執行 $Auth_{AMPDW}(U_O, G_P, M_W, \{b_1, b_2, \ldots, b_n\},$ Proxy-Certificate)來授權給一群代理簽章者。當代理簽章者收到 Proxy-Certificate 和秘密值 b_i 則利用 $VerAuth_{AMPDW}(U_O, G_P, \{b_1', b_2', \ldots, b_n'\},$ Proxy-Certificate)來驗證 Proxy-Certificate 和秘密值 b_i 的正確性，若驗證通過則信任代理簽章的授權並產生個別的代理秘密金鑰 $x_{G_i}=x_i+b_i \bmod q$ 及對應的代理公開金鑰 $y_{G_i}= g^{xG_i} \bmod p$。群代理公開金鑰為 $y_{G_P}=\Pi_{i=1}{}^{n} y_{G_i} \bmod p$。

代理簽章的產生與驗證階段

藉由在 G_P 中所有代理簽章者 U_i 的合作，每個代理簽章者提供他們的代理秘密金鑰 x_{G_i} 和一個離散對數型的多人簽章法(表示為 DLMS)，對於一個明文 m 產生一組簽章(R, S)=$DLMS_{(\Sigma_{i=1}{}^{n}x_{Gi},\ \Sigma_{i=1}{}^{n}y_{Gi})}(h(m||r||s))$。當驗證者收到對明文 m 的簽章(R, S)，首先利用 $VerCert_{AMPDW}(U_O, \text{Proxy-Certificate})$驗證 Proxy-Certificate 的正確性，接著則利用對應的離散對數驗證式(表示為 DLMV)和群代理公開金鑰 y_{G_P} 驗證簽章的正確性 $DLMV_{\Pi_{i=1}{}^{n}y_{Gi}}((R, S), h(m||t||s))$。若量個驗證式皆通過則驗證者信任 Proxy-Certificate 及代理簽章(R, S)耶為合法且為原始簽章者 U_O 所授權。

代理簽章者的識別階段

若簽章(R, S)出現爭議時，原始簽章者必須執行 $ID_{AMPDW}(TTP, U_O, \{y_1, y_2, \diamond, y_n\}, G_P, M_W, \{b_1, b_2, \ldots, b_n\}, \text{Proxy-Certificate})$證明代理群 G_P 就是使用者$\{U_1, U_2, \ldots, U_n\}$。

匿名的門檻式代理簽章法

在新的匿名門檻式代理簽章法中共分為四個階段：系統初始階段，代理授權階段，代理簽章的產生與驗證階段和代理簽章者的識別階段。系統初始階段與匿名的門檻式代理簽章法相同。

代理授權階段

原始簽章者 U_O 先執行 $Auth_{AMPDW}(U_O, G_P, M_W, \{b_1, b_2, \ldots, b_n\}, \text{Proxy-Certificate})$來授權給一群代理簽章者，不過此時 M_W 必須包含門檻值 t，此處 $1\le t\le n$。當代理簽章者收到 Proxy-Certificate 和秘密值 b_i 則利用 $VerAuth_{AMPDW}(U_O, G_P, \{b_1', b_2', \ldots, b_n'\}, \text{Proxy-Certificate})$來驗證 Proxy-Certificate 和秘密值 b_i 的正確性，若驗證通過則信任代理簽章的授權並產生個別的代理秘密金鑰 $x_{G_i}=x_i+b_i \bmod q$ 及對應的代理公開金鑰 $y_{G_i}=g^{xG_i} \bmod p$。群代理公開金鑰為 $y_{G_P}=\Pi_{i=1}{}^{n}y_{G_i} \bmod p$。

代理簽章的產生與驗證階段

在不失一般性，假設 G_P 中產生代理簽章者為$\{U_1, U_2, \ldots, U_{t'}\}$，此處 $t\le t'\le n$。藉由在 G_P 中 t 個代理簽章者 U_i 的合作，每個代理簽章者提供他們的代理秘密金鑰 x_{G_i} 和一個離散對數型的多人簽章法(表示為 DLMS)，對於一個明文 m 產生一組簽章(R, S)= $DLMS_{(\Sigma_{i=1}{}^{t'}x_{Gi},\ \Pi_{i=1}{}^{n}y_{Gi})}(h(m||r||s))$，此處 m 包含 t'個代理簽章者 U_i 的代理公開金鑰。當驗證者收到對明文 m 的簽章(R, S)，除了確任 $t\le t'$ 外，首先利用 $VerCert_{AMPDW}(U_O, \text{Proxy-Certificate})$驗證 Proxy-Certificate 的正確性，接著則利用對應的離散對數多人簽章驗證式(表示為 DLMV)，和群代理公開金鑰$\Pi_{i=1}{}^{t'}y_{G_i}$驗證簽章的正確性 $DLMV_{\Pi_{i=1}{}^{t'}y_{Gi}}((R, S), h(m||r||s))$。若兩個驗證式皆通過則驗證者信任 Proxy-Certificate 及代理簽章(R, S)為合法，且為原始簽章者 U_O 所授權。

代理簽章者的識別階段

若代理簽章(R, S)出現爭議時，原始簽章者必須執行 $ID_{AMPDW}(TTP, U_O, \{y_1, y_2, \ldots, y_{t'}\}, G_P, M_W, \{b_1, b_2, \ldots, b_{t'}\}, \text{Proxy-Certificate})$，證明代理群 G_P 中使用者$\{U_1, U_2, \ldots, U_{t'}\}$。

六、參考文獻

[1] Chan, C.-C., "Anonymous (multi-) proxy signature schemes with undeniable agents," Master Thesis, Tamkung University, Taiwan, R.O.C., 2005.

[2] ElGamal, T. "A public key cryptosystem and a signature scheme based on discrete logarithms," *IEEE Transactions on Information Theory*, Vol. 31, Issue: 4, pp. 469–472. July 1985.

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

[4] 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, pp. 119-124, 2001.

[5] 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, pp. 137-144, 2000.

[6] Hwang, Shin-Jia, and Chen, Chiu-Chin, "Cryptanalysis of Nonrepudiable Threshold Proxy Signature Schemes with Known Signers," Journal of Informatica, Vol. 14, No. 2, pp. 205-212, 2003.

[7] Hwang, Shin-Jia, and Chen, Chiu-Chin, "A New Multi-Proxy Multi-Signature Scheme," *Applied Mathematics and Computation*, Vol. 147, Issue 1, pp. 57-67, 2004.

[8] 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, pp. 199-204, 2001.

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

[10] 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, pp. 60-64, 2000.

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

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

[13] Li, Li-Hua, Tzeng, Shiang-Feng, and Hwang, Min-Shiang, "Generalization of proxy signature-based on discrete logarithms," *Computers & Security*, Vol. 22, No. 3, pp. 245-255, 2003.

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

[15] Lee, N.-Y. and Lee, M.-F., "The security of a strong proxy signature scheme with proxy signer privacy protection," *Applied Mathematics and Computation*, Vol. 161, 2005, pp.

807-812.

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

[17] MAMBO, Masahiro, USUDA, Keisuke, and OKAMOTO, Eiji, "Proxy signatures for delegation signing operation," *Proc. 3nd ACM Conference on Computer and Communication Security*, pp. 48-57, 1996.

[18] P. Horster, M. Michels, and H. Petersen, "Meta-multisignature schemes based on the discrete logarithm problem," *Proc. of IFIP/SEC '95*, pp. 128-141. Chapman & Hall, 1995.

[19] Shao, Z., "Signature schemes based on factoring and discrete logarithms," Computers and Digital Techniques, IEE Proceedings-, Vol. 145, Issue. 1, pp. 33-36, January 1998

[20] 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), pp. 55-56, 2002.

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

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

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

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

[25] Sun, H.-M. and Hsieh, B.-T., ""Cryptanalysis of a strong proxy signature scheme with proxy signer privacy protection", *2003 IEEE International Carnahan Conference on Security Technology*, 2003.

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

[27] 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, pp. 54-59, 2000.

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

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

七、計畫成果自評

本計畫的結果分別提出了一個匿名的代理簽章法、一個匿名的多人代理簽章法、以及

匿名的門檻式代理簽章法，讓原始簽章者能授權給一位或一群匿名的代理簽章者。在方法中，被授權代理簽章者是匿名的，且每一位代理簽章者亦無法知道代理簽章群中，其他代理簽章者的身份，另外和 Shum 跟 Wei 的方法比較，新的方法不需要發佈別名的公正機構，也減少了安全通道的使用。新的方法能防禦匿名代理簽章者事後否認的攻擊。因此基本上達到本計畫的目標：可匿名代理簽章群的群體導向代理簽章法之設計。本計畫的部份結果，匿名的代理簽章法與匿名的多人代理簽章法，為淡江碩士生詹景中的碩士論文[1]，也已經投稿到國際期刊，審查中。