簽章者具名之門檻式代理鑑別加密
Threshold proxy authentication encryption with known signers

吳宗杉
佛光人文社會學院資訊學研究所
tswu@mail.fgu.edu.tw

陳益森
佛光人文社會學院資訊學研究所
j1010958@trts.dorts.gov.tw

摘要

在數位化的時代，數位簽章經常被用於簽署各種電子文件。為使數位簽章具有效性及不可否認性，簽章者必須利用自己所擁有之秘密金鑰簽署，而驗證時則利用簽章者之公開金鑰驗證，以驗證簽章的合法性。一旦簽章者無法自己簽署文件，但又必須為某些文件簽署時，則可找代理人 (例如秘書) 替他完成此項工作，所產生的數位簽章即稱為代理簽章。鑑別加密法 (authentication encryption) 是一種能滿足不可偽造性、不可否認性及機密性三大特性的訊息回復數位簽章法。本論文所提出的簽章者具名之門檻式代理鑑別加密法，結合代理簽章法與鑑別加密的觀念，允許原始簽章者可將其簽署權限授權給代理群體，代為行使職權。當糾紛發生或被簽署訊息不再具機密性時，鑑別加密訊息可以轉換成一般具訊息回復的數位簽章，作為數位證據 (digital evidence)。

關鍵詞：鑑別加密 (authentication encryption)、門檻策略 (threshold policy)、數位簽章 (digital signature)、訊息回復 (message recovery)

一、前言

數位簽章的技術在網路中可以達成身份確認，並確保資料完整及正確之目的，然而眾所周知，數位化資訊是非常容易遭到複製而且成本也很低廉，發生偽造或欺騙的情形應會較實體物質更頻繁，故必須要有一套機制來解決此類的爭議。目前大多利用數位簽章的技術來作為確保對數位化資料的一種認可與保證，而在多種不同數位簽章的發展與研發不斷創新下，例如 RSA 與 ElGamal，這些方法都能提供鑑別性 (authentication)、完整性 (integrity) 及不可否認性 (non-repudiation)，藉由它所具有的不可否認性質來取得使用者雙方對交易的信賴。

電子商務成功的關鍵在於是否有個公平競爭且安全的交易環境，因此電子商務目前所面臨的最大問題便是資料傳輸的安全性。如何在開放自主的網際網路中，防止資料在傳輸時遭到不法人士的竄改、竊取或不當使用，進而建立安全可信賴的電子商務環境，以取得使用者的信任，是目前電子商務的第一要務。

在兼顧方便、安全及效率的前提之下，進行傳輸或儲存資料的保護，並達到資料機密性（confidentiality）、完整性（integrity）、鑑別性(authenticity)、不可否認性(non-repudiation)的安全需求。以電子商務或電子交易的應用為例：

(1) 機密性：保護資訊內容的秘密性，防制不法人士在未授權的情況下揭露其內容，確保資料在傳輸或儲存狀態的祕密性。

(2) 完整性：在於能防制資料在傳輸或儲存過程遭受到刻意或無意的竄改或偽造，用以確保資訊內容完整不變，一旦遭到竄改將可偵測出來。

(3) 鑑別性：在於能讓通信雙方識別彼此身分，並可確認資料的來源(傳送端)與目的地(接收端)，資訊的接收者可以利用傳送者的公開資訊，來驗證資訊來源的合法性，以確認傳送者的身分。

(4) 不可否認性：在於提供可驗證的證據，使得傳送端無法否認曾經傳送某資料，接收端無法否認已接收到該資料或知道資料內容，防範傳送者/接收者否認他曾傳送/接收過的資訊。

Diffie 和 Hellman [4] 1976 年提出公開金鑰密碼系統以來，使得人們可以在未見面的情況下，利用開放和不安全的通路 (例如：網際網路 Internet) 來進行安全及可鑑別的溝通或訊息傳遞。為確保傳遞資訊的安全，需同時達

到資料的機密性、完整性、鑑別性以及不可否認性四項要求，傳統作法是採用二階段作法 (two-step approach) 如圖一所示，所謂二階段作法是指傳送者先利用數位簽章技術中的簽章產生機制 (signature generation mechanism) 來產生欲傳送之交易訊息的數位簽章，再利用加密技術來針對交易訊息及其數位簽章進行加密以產生密文，最後將此密文傳送給接收者。對接收者而言，則是先利用解密機制 (decryption mechanism) 對該密文進行解密，再利用簽章驗證機制對交易內容的數位簽章進行驗證，以確認該交易的有效性。私鑰加密機制所使用的任選訊息加密金鑰可以利用接收者的公開金鑰來加密，如此確保此密文只能由擁有該把公開金鑰的接收者才能解開此密文。這種作法的傳輸與計算成本為數位簽章與加解密技術之各別成本的總和。這種二階段的作法也稱為先簽後加密法 (sign then encrypt)。

代理簽章最早是由 Mambo [17] 等學者於 1996 年所提出，將代理的觀念應用於數位簽章中。該方法允許簽章者指派代理簽章者代表其負責簽署的動作。代理簽章者所簽署的文件就如同原始簽章者一樣具有效力。一般而言，代理簽章具有二個特性，一為不可偽造性，另一為可驗證性。前者是指除了簽章者或代理簽章者外，沒有任何人能產生有效之代理簽章。後者則是當驗證者驗證代理簽章無誤時，則就可相信此簽章是合法的代理簽章。而代理簽章有以下幾點特性：

(1) 可區別性 (distinguishability)：由代理簽章者所簽署的代理簽章與原始簽章者所產生的簽章是可分別的。

(2) 不可偽造性 (unforgeability)：唯有原始簽章者及指派的代理簽章者可產生有效的代理簽章。除此之外，沒有任何人能夠偽造代理簽章

(3) 可驗證性 (verifiability)：從代理簽章中，驗證者可以相信原始簽章者同意此份簽署文件。

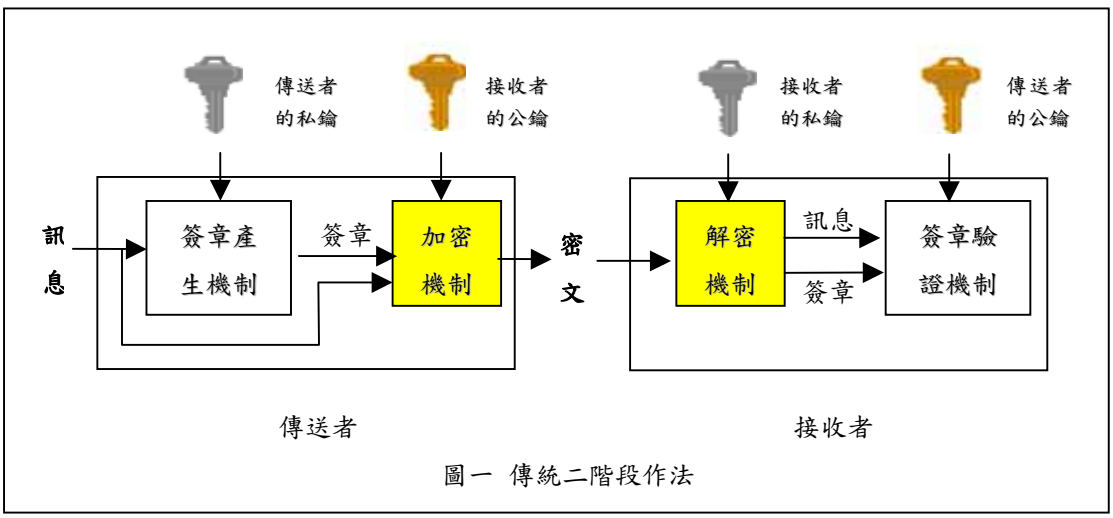
(4) 識別性 (identifiability)：從代理簽章中，原始簽章者可知道代理簽章者的身份。

(5) 不可否認性 (undeniability)：代理簽章者不可否認自己所簽署過的代理簽章。

代理簽章中原始簽章者授予代理簽章者簽章權力，其授權方式可分為以下四種 [15]：

(1) 完全授權 (full delegation)：簽章者將其所擁有之秘密金鑰完全秘密交付予代理簽章者，代理簽章者可依此秘密金鑰簽章必須簽章的文件。然而，此種授權方式將完全破壞簽章者的私密性。因為代理簽章者得知原始簽章者之秘密金鑰後，便可任意簽署文件，而所產生之簽章則無法分辨是由原始簽章者亦或是代理簽章者所簽署。

(2) 部分授權 (partial delegation)：基於上述授權方式之缺點，原始簽章者授予代理簽章者簽署權力時，並不是直接傳送其秘密金鑰給代理簽章者，而是利用此秘密金鑰計算出代理金鑰，將此代理金鑰傳送給代理簽章者。代理簽章者則可用代理金鑰簽署文件產生代理簽章。所產生的代理簽章與原始簽章者利用秘密金鑰所產生的簽章是不同的，因此驗證者可分辨出簽章是否為代理簽章。此外，此種授權方式可依「代理的保護」細分為兩類。一為非保護代理 (proxy unprotected) 之代理簽章，即除了代理簽者可產生代理簽章外，原始簽章者亦握有代理金鑰產生代理簽章。因此，所產生出之代理簽章無法分辨是否真正由代理簽章者所產生。這對代理簽章者而言



圖一 傳統二階段作法

是不公平的，倘若原始簽章者產生代理簽章，代理簽章者就被認定為是此簽章的簽署者，因而必須對此簽名負責。為解決這個問題，讓原始簽章者與代理簽章者保有獨立的簽署權力，另一種授權方式則為保護代理 (proxy protected) 之代理簽章。當原始簽章者欲授予代理簽章者簽署權力時，首先，依據其秘密金鑰產生數值，將此數值秘密傳送給代理簽章者，代理簽章者再利用自己所擁有之秘密金鑰與所接收的數值計算之後，得到代理金鑰。此代理金鑰即可產生代理簽章。由於代理金鑰是由代理簽章者的秘密金鑰所計算出的，唯有擁有此金鑰的人方可得知代理金鑰之後產生代理簽章。因此，除了代理簽章者，沒有任何人 (包括原始簽章者) 可以產生代理簽章。這種方式所產生的代理簽章使得簽章具有可追蹤性及不可否認性，讓簽署者必須為其所簽署的文件負責。

(3) 授權書授權 (delegation by warrant)：此種授權方式即由原始簽章者產生授權書給代理簽章者，此授權書是利用原始簽章者的秘密金鑰所簽署產生，除了宣告某代理簽章者可代理其行使簽署的權力外，尚可包含一些特殊的宣告，如代理的權限、可簽署文件的類型等皆可包括在此授權書中。代理簽章者得到此授權書後，即可利用自己的秘密金鑰簽署所代簽的文件，並將此授權書包含於簽章之中。而驗證者必須驗證二個步驟，首先針對簽章本身驗證其正確性，如果正確則進一步檢查其授權書，並由此授權書判斷此代理簽章者所簽署的代理簽章是否合法。

(4) 結合授權書之部分授權 (partial delegation with warrant)：在 1997 年，Kim [10] 等人提出新的代理簽章方法，即結合以上 (2) 及 (3) 的授權類型。原始簽章者先設定好該代理簽章者之簽署權力，如簽署期限、簽署文件類型等，之後利用其秘密金鑰連同所規範的簽署權力計算之後所得的結果，將之交付給代理簽章者，代理簽章者再依據所接收到的訊息，利用自己的秘密金鑰，計算而得到代理金鑰。之後，代理簽章者即可利用此代理金鑰簽署文件產生代理簽章。而所產生的代理簽章亦包含原始簽章者所規定的簽署權力，唯有完全符合此簽署權力的代理簽章方可認定為合法的代理簽章。

在不同的環境中，將會遇到不同的情形，因此就衍生出幾種不同的代理簽章方法，其中門檻式數位簽章 (threshold signature) 又稱為群體導向簽章 (group-oriented signature) [15]。而門檻式數位簽章之簽署方式也是由群體內的成員簽署同一文件，但是門檻式數位簽章並不需要群體內的所有成員皆參與，只要成員人數超過門檻值即可。另外它有一個特性是驗證者並不知道有那些成員參與簽署。由於門檻式數位簽章並不需要群體內的所有成員皆參與，且驗證者並不知道有那些成員參與簽署，因此造成發生爭議時，無法得知是群體中那些成員實際參與簽署文件。為提供不同之應用，故有所謂可追蹤簽署者 (traceable signer) 之門檻式數位簽章法 [23] 的提出。也就是說，驗證者在驗證門檻式群體簽章時，亦可同時知道有那些成員實際參與簽署文件。Sun 亦於 1999 年提出可追蹤接收者 (traceable receivers) 的代理簽章，用以追蹤代理簽章的接收者，確認代理簽章是否於有效的代理期間內產生，防止代理簽章者與驗證者於合法授權期間外，共謀產生有效的代理簽章。陸續有許多學者提出不同型態與用途的代理簽章方法。在群體導向應用的門檻代理簽章法中，實際參與簽署的簽署者對驗證者而言皆是匿名的，有鑑於簽章安全稽核之需要，Sun 於 1999 年提出可知道實際參與簽署者的門檻代理簽章法。然而，Sun 方法會面臨共謀攻擊 (conspiracy attack)，以致原始簽署的私鑰會被推導出來。

所謂的鑑別加密法 [3] (authenticated encryption scheme)，是一種能提供安全性的訊息回復數位簽章法。簽章者利用自己的私鑰和驗證者的公開金鑰來產生簽章，隨後再將此簽章送給該特定的驗證者來驗證 (如圖二所示)。這個簽章只能由該特定的驗證者才能夠驗證並且回復訊息。此鑑別加密法可以達到鑑別性、完整性及安全性。另外，此方法乃是「真正同時」完成簽章及加密動作，亦即在簽署訊息的同時，也完成訊息的加密；另一面在驗證簽章的過程中也同時完成解密的動作。因此鑑別加密法在簽章之簽署及驗證過程中，不需額外的加密及解密動作。既可符合上述四項安全需求，其所需要的傳輸與計算成本也較傳統二階段作法的成本低。

傳統的數位簽章，如 RSA 的數位簽章方法，其安全性是植基於分解二個大質數上之數學問題上，為了減少簽章時之計算時間及傳送訊息，常配合 One-way hash function 來使用。ElGamal 提出一種機率式的簽章方法，其簽章之安全性係植基在解離散對數之困難度上。對大多數的數位簽章方法的安全性而言，不是植基在分解二個大質數上之數學問題，就是植基於解離散對數之困難度上。而橢圓曲線密碼系統 (elliptic curve cryptosystem; ECC) 是在有

限體 (finite fileds) 下和橢圓曲線的整數點所構成的群 (group) 而發展出來。

一般的群體導向數位簽章法，並無法同時對群體導向系統提供機密性、完整性、鑑別性以及不可否認性保護，也無法有效率地應用於各種不同的應用需求。本論文結合鑑別加密法的特性及群體導向的觀念，提出門檻式的鑑別加密機制。

針對群體導向的應用環境，設計兼具效率與安全性的門檻式鑑別加密法，以昇企業或組織運作的安全防護能力，提供機密性、完整性、鑑別性以及不可否認性之保護，並且對組織活動提供安全控管與代理機制。

本論文的內容安排說明如下：在下一章中我們介紹本論文的相關文獻，在第三章中提出簽章者具名之門檻式代理鑑別加密法，第四章分析本論文所提方法的安全性，第五章為所提方法的效率評估，最後一章做一個簡單的結論。

二、文獻探討

本章中將介紹與本論文相關的知識背景，包括簽章者具名之門檻式代理簽章及鑑別加密的文獻。在群體簽章中，將會面臨如何將秘密金鑰分享的問題。Shamir 於 1979 年時，所提出 (t, n) 門檻秘密分享方法 (threshold secret sharing scheme)，其方法首先將要分享的秘密金鑰分成 n 把次金鑰，然後送給每位參與者一把次金鑰，當 t 個以上的參與者出示其保管之次金鑰時，就能利用這些次金鑰重建出秘密金鑰，如此就能兼具安全性與彈性。

Shamir 的 (t, n) 門檻秘密分享方法，其方法滿足以下兩個條件：

(1)當獲得大於或等於 t 把次金鑰，則能重建秘密金鑰。

(2)當獲得少於 t 把次金鑰，如同沒有獲得任何資訊一樣，無法重建秘密金鑰。

可分為秘密金鑰分派與秘密金鑰重建兩個階段，分別說明如下：

[秘密金鑰分派階段]

原始簽章者要分享的秘密金鑰 K，任選一個 $(t-1)$ 次方的多項式

$$f(x) = K + a_1 x + a_2 x^2 + \ldots + a_{t-1} x^{t-1} \bmod p$$

其中 p 為質數，$a_i \in Z_p$ $(i = 1, 2, \ldots, t-1)$ 且 $a_{t-1} \neq 0$。根據秘密多項式，並計算參與者 U_i $(i = 1, 2, \ldots, n)$ 的次金鑰 K_i

$$K_i = f(i) \bmod p$$

然後將次金鑰 K_i 經由安全通道傳送給參與者 U_i。

[秘密金鑰重建階段]

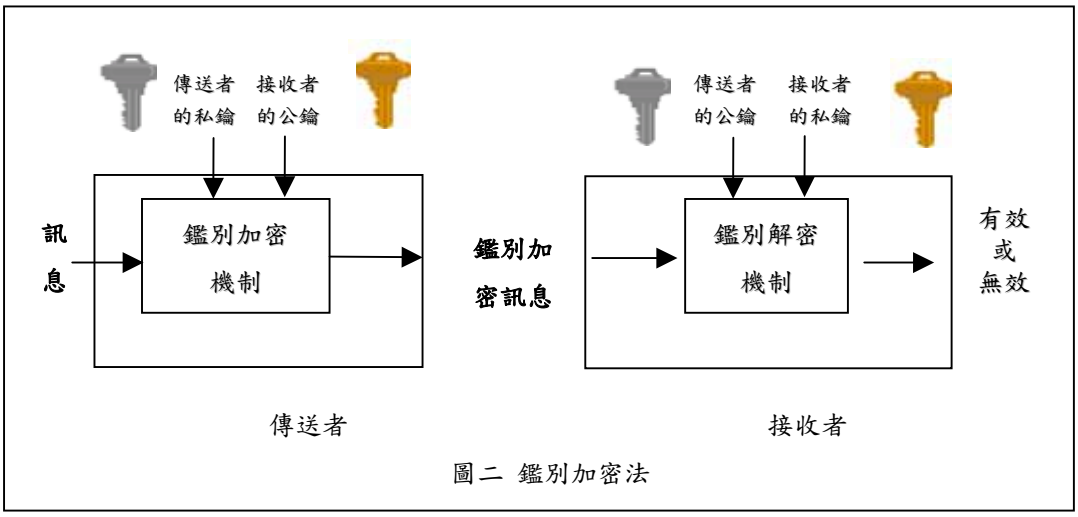
當參與者要重建秘密金鑰時，必須集合 t 把（以上）的次金鑰 K_i，採用 Lagrange 內插多項式的方式，重建秘密多項式：

$$f(x) = \sum_{i=1}^{t} K_i \prod_{j=1, j\neq i}^{t} \frac{x-j}{i-j} \bmod p$$

根據重建的秘密多項式 $f(x)$，計算出分享的秘密金鑰 K

$$K = f(0) \bmod p$$

如此，利用以上方式，原始簽章者就可將秘密金鑰 K 分享給代理群體，利用 (t, n) 門



圖二 鑑別加密法

檻策略，集合 t 位以上的實際參與者，便可重建秘密交鑰 K。

以往的授權的代理簽章者對驗證者都是匿名的，因應不同的業務需要，陸續有許多學者提出不同型態與用途的代理簽章方法。在群體導向應用的門檻代理簽章法中，有所謂簽章者具名門檻代理簽章，也就是說，驗證者在驗證門檻值群體簽章時，亦同時知道有那些成員實際參與簽署文件。Sun [18] 有鑑於簽章安全稽核之需要，於 1999 年提出可知道實際參與簽署者的門檻代理簽章法。

(一) Sun's 簽章者具名的門檻代理簽章方法

Sun 所提的方法是以 Kim [10] 簽章者匿名的門檻代理簽章方法為基礎，提出具不可否認性特性的簽章者具名門檻代理簽章方法，實際代理簽章者代表代理簽章群體或原始簽章者來簽署訊息，驗證者在簽章驗證階段，代理群體裡的實際代理簽章者的身分是可以被識別。其方法可分為系統初始階段、秘密分享階段、代理分享階段、代理簽章產生階段、代理簽章驗證階段等五個階段，詳細說明如下：

[系統初始階段]

系統管理者 (system authority, *SA*) 定義並公布以下的參數：

p, q：二大質數，其中 $q \mid (p-1)$；

g：在 GF(p) 下秩 (order) 為 q 的生成數 (generator)；

$h(.)$：單向雜湊函數 (one-way hash function)，該函數的輸入值為任意長度，而其輸出值為固定長度。

m_w：為代理授權書，內含有原始簽章者及代理簽章群體資訊，代理期限及門檻值 t 等相關資訊。

ASID (actual signers' ID)：實際參與者的身分識別。

P_0：為原始簽章者。

$G = \{P_1, P_2, \ldots, P_n\}$：代理簽章群體裡的 n 個代理簽章者的集合群體。

$D = \{P_1, P_2, \ldots, P_t\}$：代理簽章群體裡的 t 個參與代理簽章者的集合群體。

每位使用者 P_i，其身分識別為 $v_i \in Z_q$，擁有私密金鑰 $x_i \in Z_q^*$，其相對應的公開金鑰為 $y_i = g^{x_i} \bmod p$，並且為認證中心 (certificate authority, *CA*) 所認證。

[秘密分享階段]

步驟一：

每位代理簽章者 $P_i \in \mathrm{G}$，選擇 $(t-1)$ 次方的多項式

$$f_i(x) = s_i + a_{i,1}x + \cdots + a_{i,t-1}x^{t-1} (\bmod q)$$

因此，$a_0 = \sum_{i=1}^{n} x_i (\bmod q)$，且 x_i 為 P_i 的私鑰 (secret key)，其對應的公鑰為 y_i 。

代理群體的公鑰為 $y_G = g^{a_0} (\bmod p)$ ，

且 $A_j = g^{a_j} (\bmod p), j = 1, 2, \ldots, t-1$，

代理群體的私鑰為 s_i，

$$s_i = f(i) = a_0 + a_1 i + \ldots + a_{t-1} i^{t-1}$$ ，

因此，$y_G = \prod_{i=1}^{n} y_i \bmod p$，$y_i$ 是 p_i 的公開金鑰。

[代理分享階段]

步驟一：

原始簽章者任選 $k \in Z_q$，計算

$K = g^k \bmod p$，

原始簽章者結合 K 和授權書 m_w，產生

$e = h(m_w, K)$，之後，

原始簽章者計算代理金鑰

$$\sigma = ex_0 + k (\bmod q)$$

步驟二：

原始簽章者任選 $(t-1)$ 次方的多項式

$f'(x) = \sigma + b_1 x + \cdots + b_{t-1} x^{t-1} (\bmod q)$ ，且

$b_j \in Z_q, j = 1, 2, \ldots, t-1$，公佈

$B_j = g^{b_j} (\bmod p), j = 1, 2, \ldots, t-1$，計算

$$\sigma_i = f'(i) = \sigma + b_1 i + \ldots + b_{t-1} i^{t-1}, i = 1, \ldots, n$$

然後，將 σ_i 以秘密的方式傳給每位代理簽章者 P_i ($i = 1, 2, \ldots, n$)，並將 (m_w, K) 以廣播的方式傳播出去。

步驟三：

每位代理簽章者 P_i，收到 (σ_i, m_w, K)，必須確認是否合法，利用下列式子來驗證：

$$g^{\sigma_i} \stackrel{?}{=} y_0^{h(m_w,k)} K \prod_{j=1}^{t-1} B_j^{i^j} (\bmod p)$$

驗證上式正確，則每位代理簽章者 P_i 計

算

$\sigma'_i = \sigma_i + s_i \cdot h(m_w, K) \bmod q$ ，

實際參與者 P_i，將 σ'_i 當成自己的代理子金鑰。

[代理簽章產生階段]

步驟一：

$D = \{P_1, P_2, \ldots, P_t\}$，是 t 個代理簽章者的集合，*ASID* (actual proxy signers) 是其實際參與代理簽章的代理簽章者身分識別，每位實際代理簽章者 $P_i \in D$，選擇 $(t-1)$ 次方的多項式，

$f_i''(x) = (c_{i,0} + x_i) + c_{i,1}x + \ldots + c_{i,t-1}x^{t-1} (\bmod q)$ ，

令 $c_0 = \sum_{i=1}^{n} c_{i,0} (\bmod q)$，且將其公開金鑰

$$Y = g^{c_0} \bmod p,\ C_j = g^{c_j} (\bmod p),$$

$j = 1, 2, \ldots, t-1$，廣播出去，

而其秘密金鑰

$s_i' = f''(i)$

$= \sum_{i=1}^{n} x_i + c_0 + c_1 i + \ldots + c_{t-1} i^{t-1} (\bmod q)$ ，

則以秘密的方式傳送給每位實際代理簽章者。

步驟二：

每位代理簽章者 P_i , $i = 1, 2, \ldots, t$ ，計算

$\gamma_i = s'_i Y + \sigma'_i h(ASID, m) (\bmod q)$ ，

並將 γ_i 以秘密的方式傳送給其他代理簽章者 P_j ，$(j = 1, 2, \ldots, n, j \neq i)$ 。

步驟三：

接收者收到 $\gamma_j (j = 1, 2, \ldots, t, j \neq i)$，$P_i$ 必須以下列式子檢查是否正確，

$$g^{\gamma_j} \stackrel{?}{=} [Y(\prod_{i=1}^{t-1} C_i^{j^i})(\prod_{i=1}^{t-1} y_i)]^Y \times [(y_0^{h(m_w,K)} K \prod_{i=1}^{t-1} B_i^{j^i}) \times (y_G \prod_{i=1}^{t-1} A_i^{j^i})^{h(mw,K)}]^{h(ASID,m)} (\bmod p)$$

步驟四：

上式驗證正確，則每位代理簽章者 P_i，使用 Lagrange 內插多項式，計算

$T = f''(0)Y + [f(0) + f'(0)]h(ASID, m)$ ，

所產生的 $(m, T, K, m_w, ASID)$ 為其代理簽章。

[代理簽章驗證階段]

任何驗證者可以驗證代理簽章 $(m, T, K, m_w, ASID)$ 的合法性

步驟一：

從授權書 m_w 中，驗證者可以知道原始簽章者及代理簽章群體並且可以從 *CA* 得到代理簽章者的公開金鑰。

步驟二：

驗證者可以從 *ASID* 知道實際簽章者是誰，如果 $P_1, P_2, \ldots, P_t$ 是實際簽章者，就可以從 *CA* 得到其公開金鑰。

步驟三：

驗證者利用下列式子

$$g^T \stackrel{?}{=} [y_0^{h(m_w,K)} K \prod_{i=1}^{n} y_i]^{h(ASID,m)} \times (y \prod_{i=1}^{t} y_i)^Y \bmod p$$

y_0：是原始簽章者的公開金鑰。

y_i：是代理簽章者的公開金鑰。

上述式子驗證無誤，$(m, T, K, m_w, ASID)$ 就是由代理簽章群體所產生的合法簽章。

Wu 與 Hsu [25] 於 2002 年提出可公開驗證鑑別加密訊息的方法，當訊息需要公開時，可以將鑑別加密訊息，轉換成一般的簽章及 Hsu 與 Wu [6] 於 2005 年所提的自我驗證公開金鑰特性的門檻式代理簽章，證明公開金鑰可以在不需要憑證的情況下，可同一時間完成代理簽章的驗證及簽章訊息的回復。本論文利用可轉換的鑑別加密方法及可自我驗證的門檻式代理簽章的觀念，做為我們提出簽章者具名之門檻式鑑別加密機制的基礎。上述兩論文內容概述如下：

(二) Wu 與 Hsu 的可轉換的鑑別加密方法

Wu 與 Hsu [25] 於 2002 年提出可公開驗證鑑別加密訊息的方法，當鑑別加密訊息發生爭議時，該方法仲裁糾紛不必透過零知識證明協定，很容易將鑑別加密訊息轉換成一般數位簽章，讓公正第三者 (trust third party, TTP) 公開驗證，且此方法可以有效率地轉換簽章，

故本論文所設計之金鑰分配協定即是採用此觀念來達到降低成本的目的，其方法分為系統初始、鑑別加密、鑑別解密及公開驗證四個階段，詳細說明如下：

[系統初始階段]

p, q, g, $h(.)$ 等參數之定義與前一節相同。每位使用者 U_i 擁有私密金鑰 $x_i \in Z_q^*$, 其相對應的公開金鑰為 $y_i = g^{x_i} \bmod p$。

[鑑別加密階段]

簽署者 U_A 必須在安全且可鑑別的方式下傳送具有冗餘的訊息 $M \in Z_q$ 給驗證者 U_B。 U_A 選擇隨機亂數 $k \in Z_q^*$ ，並計算

$$r_1 = M \cdot (h(y_B^k))^{-1} \bmod p$$
$$r_2 = h(M \,\|\, h(g^k \bmod p)) \bmod q$$
$$s = k - x_A \cdot r_2 \bmod q$$

(r_1, r_2, s) 為 U_A 對訊息 M 產生的鑑別加密訊息。之後，U_A 將鑑別加密訊息 (r_1, r_2, s) 傳送給 U_B。

[鑑別解密階段]

U_B 接收到 U_A 傳送的鑑別加密訊息 (r_1, r_2, s) 之後，U_B 要從鑑別加密訊息回復原本的訊息 M 必須計算

$$M = h((g^s \cdot y_A^{r_2})^{x_B} \bmod p) \cdot r_1 \bmod p$$

檢查 M 是否符合所定義的冗餘。如果冗餘正確，再檢查下列等式：

$$r_2 = h(M \,\|\, h(g^s \cdot y_A^{r_2} \bmod p)) \bmod q$$

假使上述式子正確無誤，則 U_B 確認 (r_1, r_2, s) 為 U_A 對訊息 M 的簽章。

[公開驗證階段]

當 U_A 否認其傳送的鑑別加密訊息時，U_B 可以將其解密的訊息 M 與 (r_2, s) 交給 TTP 驗證，證明鑑別加密訊息確實是由 U_A 所產生的，TTP 檢查下列等式：

$$r_2 \stackrel{?}{=} h(M \,\|\, g^s \cdot y_A^{r_2} \bmod p)) \bmod q$$

假使上述式子正確無誤，則可確認 (r_2, s) 為 U_A 對訊息 M 的簽章。

(三) Hsu 與 Wu 具自我驗證公開金鑰特性的門檻式代理簽章方法

Hsu 與 Wu [6] 於 2005 年提出一種具訊息回復、不可否認性、可追蹤性及自我驗證公開金鑰特性的門檻式代理簽章，證明公開金鑰可以在不需要憑證的情況下，可同一時間完成代理簽章的驗證及簽章訊息的回復。其方法分可為系統初始、系統註冊、代理子金鑰產生、代理簽章產生及簽章驗證五個階段，詳細說明如下：

[系統初始階段]

p, q, g, $h(.)$ 等參數之定義與前一節相同，另外，SA 任選 $\gamma \in Z_q^*$ 當其私鑰，並計算其相對應的公鑰，$\beta = g^{\gamma} \bmod p$。

[註冊階段]

每位使用者 U_i 隨機選擇 $t_i \in Z_q^*$，計算

$$v_i = g^{h(t_i \| ID_i)} \bmod p$$

並將 (v_i, ID_i) 傳送給 SA，其中，ID_i 是 U_i 的身分。

當 SA 收到從U_i 的 (v_i, ID_i)，SA 隨機選擇 $k_i \in Z_q^*$，計算

$$y_i = v_i h(ID_i)^{-1} g^{k_i} \bmod p$$
$$e_i = k_i + h(y_i \,\|\, ID_i)\gamma \bmod p$$

並將回傳 (y_i, e_i) 給 U_i。

當每位使用者U_i 收到 (y_i, e_i) 後，計算

$$x_i = e_i + h(t_i \,\|\, ID_i) \bmod q$$

並驗證以下列式子是否有效

$$\beta^{h(y_i \| ID_i)} h(ID_i) y_i \stackrel{?}{=} g^{x_i} \pmod p$$

假使上述式子正確無誤，(x_i, y_i) 即是 U_i 的私鑰及公鑰。

[代理子金鑰產生階段]

令U_o 是原始簽章者，而$G = \{U_1, U_2, ..., U_n\}$為代理簽章群體中 n 個代理者。

步驟一

原始簽章者 U_o 選擇亂數 $k \in Z_q^*$，並計算

$$K = g^k \left(\beta^{\sum_{i=1}^{n} h(y_i \| ID_i)} \left(\prod_{i=1}^{n} h(ID_i) y_i \right) \right)^{-1} \bmod p$$

$$\sigma = h(m_w \,\|\, K \,\|\, PID) x_0 + k \bmod q$$

m_w 為代理授權書，內含有原始簽章者及代理簽章群體資訊，代理期限及門檻值 t 等相關資訊。

PID 為代理簽章群體中所有簽章者身分的集合。

步驟二

原始簽章者任選一個 $(t-1)$ 次方的多項式

$$f(x)=\sigma+a_1x+a_2x^2+...+a_{t-1}x^{t-1} \bmod q$$

並且公佈 $A_i=g^{a_i} \bmod p$，

其中 $a_i \in Z_q^*$, $i = 1, 2, \ldots, t-1$

步驟三：

原始簽章者計算代理次金鑰 (proxy share key)

$$\sigma_i = f(ID_i) \bmod p$$

然後傳送將 σ_i 給代理群體的每位代理者 P_i $(i = 1, 2, \ldots, n)$。

步驟四：

每位代理者必須檢驗個別的代理次金鑰是否有效。

$$g^{\sigma_i} \stackrel{?}{=} (\beta^{h(y_0\|ID_0)} \cdot h(ID_0) \cdot y_0)^{h(m_w\|K\|PID)} \cdot K \cdot \beta^{\sum_{i=1}^{n} h(y_i\|ID_i)} \cdot (\prod_{j=1}^{n} h(ID_j) \cdot y_j) \cdot (\prod_{j=1}^{t-1} A_j^{ID_i^j}) \pmod p$$

[代理簽章產生階段]

$D = \{U_1, U_2, \ldots, U_t\}$ 是實際參與者的集合，而 $ASID$ 是實際參與者身分的集合 (actual signers' ID)

步驟一：

實際代理簽章者 U_i 選擇亂數 $Z_i \in Z_q^*$，並計算

$$r_i = g^{Z_i} \bmod p \ ,$$

然後廣播給其他參與者。

步驟二：

每位實際代理簽章者 U_i $(i = 1, 2, \ldots, t)$ 計算

$$R = (m \| h(m)) \prod_{i=1}^{t} r_i^{r_i} \bmod p$$

$$s_i = z_i r_i + L_i \sigma_i h(PID \| R \| K) + x_i h(ASID \| R \| K) \bmod q$$

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

每位實際代理簽章者 U_i 選擇一個 CLK，然後將個別代理簽章 s_i 傳給 CLK。

步驟三：

CLK 驗證每個個別代理簽章 s_i 是否有效

$$g^{s_i} \stackrel{?}{=} r_i^{r_i} \cdot ((\beta^{h(y_0\|ID_0)} \cdot h(ID_0) \cdot y_0)^{h(m_w\|K\|PID)} \cdot K \cdot (\beta^{\sum_{i=1}^{n} h(y_j\|ID_j)} \cdot (\prod_{j=1}^{n} h(ID_j) \cdot y_j) \cdot (\prod_{j=1}^{t-1} A_j^{ID_i^j}))^{L_i \cdot h(PID\|R\|K)} \cdot (\beta^{h(y_i\|ID_i)} \cdot h(ID_i) \cdot y_i)^{h(ASID\|R\|PID)} \pmod p$$

驗證上式成立，則 (r_i, s_i) 是有效的 U_i 個別簽章；CLK 計算

$S = \sum_{i=1}^{t} s_i \bmod p$，最後將代理簽章 $(K, R, S, m_w, PID, ASID)$ 傳給驗證者。

[代理簽章驗證階段]

驗證者可以從授權書 m_w 得知原始簽章者，代理簽章群體及實際參與簽章者及 SA 的公鑰，來驗證代理簽章是否有效。

$$m \| h(m) = Rg^{-s} \cdot ((\beta^{h(y_0\|ID_0)} \cdot h(ID_0) y_0)^{h(m_w\|K\|PID)}) \cdot K \cdot (\beta^{\sum_{i=1}^{n} h(y_i\|ID_i)} \prod_{i=1}^{n} h(ID_i) y_i)^{h(PID\|R\|K)} \cdot (\beta^{\sum_{i=1}^{t} h(y_i\|ID_i)} \cdot \prod_{i=1}^{t} h(ID_i) \cdot y_i)^{h(ASID\|R\|K)} \pmod p$$

驗證上式成立，$(K, R, S, m_w, PID, ASID)$ 即是訊息 m 的有效代理簽章。

三、簽章者具名之門檻式鑑別加密

本模型的角色有原始簽章者、代理簽章群體及驗證者 (特定驗證者)，其中代理簽章群體的門檻策略為 (t, n)。透過本模型的授權代理簽章程序，原始簽章者可以將其簽署權限授權給代理簽章群體，而代理簽章群體中任意 t 位代理者便可代表代理簽章群體與原始簽章者，產生有效的代理鑑別加密訊息給特定驗證者。特定驗證者可以鑑別解密代理簽章群體所

產生的代理鑑別加密訊息，以回復出代理簽章群體的群體代理簽章與被簽署訊息。當發生糾紛或被簽署訊息不再具機密性時，驗證者可以將代理簽章群體的群體代理簽章傳送給仲裁者或任意驗證者，以證明代理簽章群體確實代理原始簽章者簽署過所回復的訊息。系統模型如圖三。

我們將這方法分為系統初始、授權代理簽章、代理鑑別加密、鑑別解密以及簽章驗證五個階段。在授權代理簽章階段，原始簽章者將其簽章權限授權給代理簽章群體。使得代理簽章群體可以取得合法的授權資訊，並且在代理鑑別加密階段中代理原始簽章者，產生有效的鑑別加密訊息。以下我們將描述簽章者具名之門檻式代理鑑別加密法：

[系統初始階段]

SA 產生之系統參數 p, q, g 及 $h(.)$ 與第二章所述相同：

系統使用者 U_i 任選一把個人私鑰 $x_i \in Z_q^*$，並計算相對應的個人公鑰 $y = g^{x_i} \bmod p$，使用者U_i 將 (x_i, y_i) 視為它的私鑰及公鑰，並將公鑰送給 *SA* 認證。*SA* 將參數 (p, q, g, h) 及 y_i 對外公佈。

[授權代理簽章階段]

原始簽章者和代理簽章群體中的代理者 $P_i (i = 1, 2, \ldots, n)$ 可以透過下列步驟來授權代理簽章：

步驟一：

原始簽章者任選亂數 $e \in Z_q^*$，計算

$$K = g^e \bmod p \qquad (1)$$

$$\sigma = h(m_w \| K) x_o + e \bmod q \qquad (2)$$

m_w：授權書，內含有原始簽章者及代理簽章群體資訊，代理期限等相關資訊。

步驟二：

原始簽章者分享自己的代理金鑰 (proxy key)，任選一個 $(t-1)$ 次方的多項式

$$f(x) = \sigma + a_1 x + a_2 x^2 + \ldots + a_{t-1} x^{t-1} \bmod q$$

並且公佈 $A_i = g^{a_i} \bmod p$，

其中 $a_i \in Z_q^*, i = 1, 2, \ldots, t-1$

步驟三：

原始簽章者，計算代理次金鑰

$$\sigma_i = f(ID_i) \bmod p \qquad (3)$$

然後透過安全通道傳送將 σ_i 給代理群體的所有代理者 $P_i (i = 1, 2, \ldots, n)$，且將 (m_w, K) 傳給驗證者。

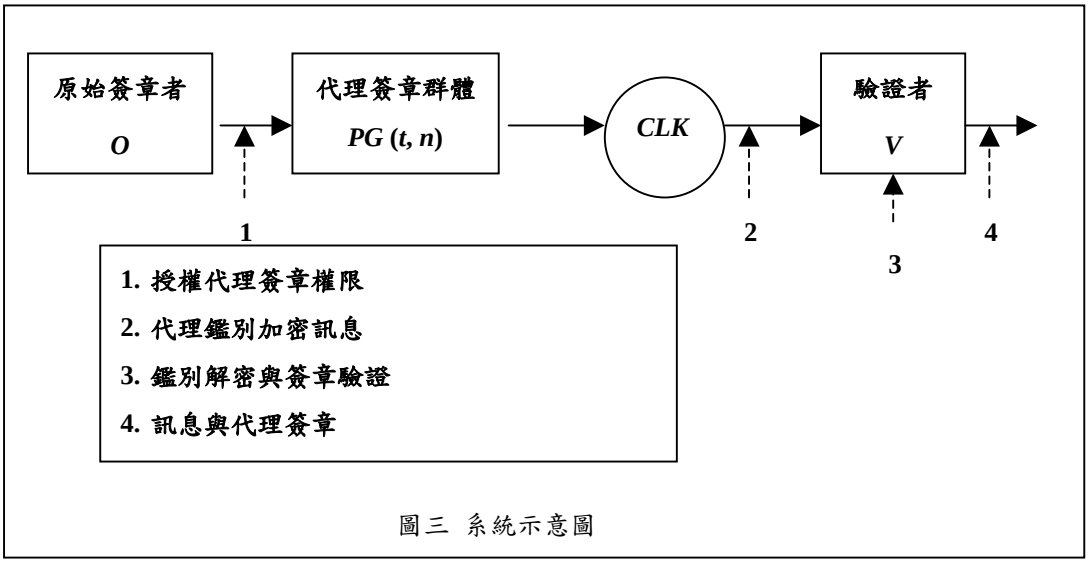
步驟四：

當代理群體的所有代理簽章者 $P_i (i = 1, 2, \ldots, n)$ 收到 σ_i，必須先驗證其正確性

$$g^{\sigma_i} \stackrel{?}{=} y_u^{h(m_w \| K)} \cdot K \cdot \prod_{j=1}^{t-1} A_j^{ID_i^j} \bmod p$$

若是上式成立，則表示他已取得原始簽章者的代理簽章授權，每位代理簽章者 P_i $(i = 1, 2, \ldots, n)$ 進一步計算個人代理簽章私鑰。

每位代理簽章者 $P_i (i = 1, 2, \ldots, n)$，任選一個 $(t-1)$ 次方的多項式



圖三 系統示意圖

$$f'(x) = x_i + b_1 x + b_2 x^2 + ... + b_{t-1} x^{t-1}$$

令 $s_i = f'(i)$ ，計算

$$\sigma'_i = \sigma_i + s_i \cdot h(m_w \| K) \bmod q \qquad (4)$$

並公佈 $B_i = g^{b_i} \bmod p$

其中 $b_i \in Z_q^*$, $i = 1, 2, \ldots, t$ -1

將 σ'_i 以安全通道傳送給每位代理者簽章者 P_i $(i = 1, 2, \ldots, n)$ ，並將 σ'_i 視為個人代理簽章私鑰。

[代理鑑別加密階段]

代理簽章群體可以代理原始簽章者簽署訊息 $M \in Z_q^*$ 給特定驗證者，其中 M 內附加特定冗餘。代理簽章群體中參與代理簽章的任意 t 位代理者共同合作來執行下列步驟，參與代理者共同選一個 CLK 驗證個人代理簽章的有效性及產生參與代理簽章者的代理簽章並建構出有效的代理鑑別加密訊息：

步驟一：

每位代理者 P_i 任選亂數 $k_i \in Z_q^*$，計算

$$r_i = g^{k_i} \bmod p \qquad (5)$$

並透過廣播的方式將 r_i 傳送給其他參與者。

步驟二：

代理簽章群體中每位代理者 P_i $(i = 1, 2, \ldots, n)$ 計算

$$R = M \prod_{i=1}^{t} r_i \bmod p \qquad (6)$$

$$\alpha_i = k_i + (L_i \sigma'_i + x_i) h(R \| ASID \| K) \bmod q \qquad (7)$$

並透過安全通道傳送 α_i 給 CLK

其中， $L_i = \prod_{j=1, j \neq i}^{t} \frac{0 - v_j}{v_i - v_j} \bmod q$

步驟三：

當 CLK 收到 t 個個人代理簽章之後，CLK 先行以下式驗證個人代理簽章 (r_i, α_i) 的有效性：

$$g^{\alpha_i} \stackrel{?}{=} [(y_u{}^{H(m_w \| K)} \cdot K \cdot \prod_j^{t-1} A_j^{ID_i{}^j})^{L_i} \cdot (y_i \cdot \prod_j^{t-1} B_j{}^{i^j})^{h(m_w \| K) \cdot L_i} \cdot y_i]^{h(R \| ASID \| K)} \cdot r_i \pmod p$$

驗證無誤後，計算

$$\alpha = \sum_{i=1}^{t} \alpha_i \pmod q$$
$$= \sum_{i=1}^{t} k_i + [h(m_w \| K) x_o + e + x_i \cdot h(m_w \| K)] \cdot h(R \| ASID \| K) + \sum_{i=1}^{t} x_i \cdot h(R \| ASID \| K) \qquad (8)$$

步驟四：

CLK 任選亂數 $d \in Z_q^*$，並計算代理群體的鑑別加密訊息 (C_1, C_2)

$$C_1 = g^d \bmod p \qquad (9)$$

$$C_2 = R \oplus (y_v{}^d \bmod p) \qquad (10)$$

並將 $(K, C_1, C_2, \alpha, m_w, ASID)$ 傳給特定驗證者。

[鑑別解密階段]

當驗證者收到 $(K, C_1, C_2, \alpha, m_w, ASID)$ 之後，必須先驗證 m_w 的有效性再利用自己的私鑰 x_v 從 (C_1, C_2) 回復出 R：

$$R = C_2 \oplus (C_1^{x_v} \bmod p) \qquad (11)$$

接著利用 (R, α) 回復出被簽署的訊息 M：

$$M = R g^{-\alpha} \cdot [(y_o)^{h(m_w \| K)} \cdot K \cdot (y_i)^{h(m_w \| K)} \cdot (\prod_{i=1}^{t} y_i)]^{h(R \| ASID \| K)} \qquad (12)$$

透過檢查附加於 M 之後的冗餘，驗證者可以確認其有效性。 (R, α) 可以視為代理群體代理原始簽章者簽署訊息 M 所產生的群體代理簽章。

[簽章驗證階段]

當發生糾紛或被簽署訊息不再具備機密性時，驗證者可以將 $(K, R, \alpha, m_w, ASID)$ 傳送給仲裁者或任意驗證者，而該驗證者可以利用式子 (12)證明，回復訊息 M 並檢查其附加冗餘。若是驗證成功，則表示 (R, α) 為代理群體代理原始簽章者簽署訊息 M 所產生的群體代理簽章。

四、安全分析

鑑別加密法需要滿足三個安全上的要求：

(1) 不可偽造性：指攻擊者不能偽造簽章者的簽章。

(2) 不可否認性：指 TTP 能利用 (R, α) 等資

訊以解決簽章者與驗證者之間的爭端，且不會洩露驗證者的私鑰和訊息。

(3) 機密性：指利用單向赫序函數保護訊息不被攻擊者得知。

我們所提出的門檻式代理鑑別加密法，是植基於 DLP 與 OWHF 的密碼假設下，為證明門檻式代理鑑別加密法可以達到鑑別加密法之機密性、不可偽造性與不可否認性三項安全要求。我們將從被簽署的訊息、原始簽章者之私鑰、代理簽章私鑰、代理簽章者之私鑰以及驗證者之私鑰來一一探討。由於我們所提的代理鑑別加密屬保護代理之代理簽章，所以亦滿足鑑別性的特性。

首先，我們先探討本論文植基於 DLP 與 OWHF 的兩個密碼假設：

[離散對數問題假設]

令 p, q為二大質數，其中 $q \mid (p-1)$， g 為在 GF(p) 下秩為 q 的生成數。從給定整數 y 滿足 $y = g^x \bmod p$，如果想從已知的 y 值求出未知的 x 值為計算上不可行的。

[單向雜湊函數假設]

$h(.)$ 為單向雜湊函數，該函數可接受任意長度的輸入值，輸出固定長度的雜湊值。應用在數位簽章的單向雜湊函數其安全性必須滿足以下幾點：

1 從給定的雜湊值 y，要找到其對應的 x 值滿足 $y = h(x)$ 為計算上的不可行。

2 從給定的一個輸入值 x_1，其雜湊值為 $y = h(x_1)$，要找到另一個輸入值 x_2，使其滿足 $h(x_1) = h(x_2) = y$ 為計算上的不可行。

3 從給定的一對相異輸入值 x_1 與 x_2，使其滿足 $h(x_1) = h(x_2)$ 為計算上的不可行。

(一) 機密性

(1) 簽署訊息的機密性

若攻擊者欲從所竊聽的鑑別加密訊息推導出被簽署的訊息，他必須要先回復出R。我們從 (9)及 (10) 式子得知，除非攻擊者知道秘密亂數 d，否則無法獲得 R。

植基於 DLP 假設，攻擊者將 $C_1 = g^d \bmod p$ 推導出 d，因此攻擊者無法回復出 R 以推導出被簽署的訊息。

(2) 原始簽章者私鑰的機密性

惡意的授權代理簽章群體，企圖從原始簽章者所給定的代理資訊 (σ_i, K) 中去推導出原始簽章者的私鑰 x_o。若此攻擊者欲從 (1) 至 (3) 式子去推導出 x_o，則必須先找到 σ 與 e。然而，攻擊者欲推導出 e 將面臨 DLP。此外，攻擊者如欲去推導出 σ 亦將面臨 DLP 假設，為計算上的不可行。

(二) 不可偽造性

(1) 代理資訊的不可偽造性

攻擊者在不知道原始簽章者私鑰的情況下，欲偽造有效的代理資訊，以假冒原始簽章者授權簽署權限給代理簽章群體。我們根據

$$g^{\sigma_i} \stackrel{?}{=} y_u^{h(m_w \| K)} \cdot K \cdot \prod_{j=1}^{t-1} A_j^{ID_i{}^j} \bmod p$$

上式式子，攻擊者欲偽造有效的代理資訊 (K, σ_i, m_w)，將面臨 DLP 與 OWHF 密碼假設。

(2) 個人代理簽章的不可偽造性

攻擊者企圖假冒參與簽署者與其他參與代理簽章者共同合作產生代理鑑別加密訊息。在鑑別加密階段中，攻擊者不知道參與代理簽章者 P_i 之個人代理簽章私鑰 σ_i，攻擊者利用

$$k_i \in_R Z_q^*, r_i = g^{k_i} \bmod p$$

來產生 $\overline{r_i}$，並廣播給其他代理者，然而他欲找到 $\overline{\alpha_i}$ 來滿足個人代理簽章驗證式

$$g^{\alpha_i} = [(y_u^{H(m_w \| K)} \cdot K \cdot \prod_j^{t-1} A_j^{ID_i{}^j})^{L_i} \cdot (y_i \cdot \prod_j^{t-1} B_j{}^{i^j})^{h(m_w \| K) \cdot L_i} \cdot y_i]^{h(R \| ASID \| K)} \cdot r_i (\bmod p)$$

基於 DLP 的密碼假設，為計算上的不可行。

(三) 不可否認性

代理鑑別加密訊息因為只有特定的驗證者可以鑑別解密其訊息及回復出被簽署訊息與群體代理簽章，但是當發生糾紛時，此特定驗證者可以將所回復的群體代理簽章交給仲裁者或 TTP，來證明該簽章是經過原始簽章者的授權，或者是代理簽章群體確實簽署過該訊息。根據上述的分析，惡意攻擊者無法在不知道原始簽章者之私鑰，以及代理簽章群體之私鑰與代理簽章私鑰的情況下，偽造出合法的鑑別加密訊息與群體代理簽章，因此原始簽章者無法否認曾經授權簽署，而代理簽章群體也將無法否認產生過代理鑑別加密訊息或群體代理簽章。

(四) 鑑別性

代理鑑別加密的授權方式為保護代理之

代理簽章。當原始簽章者欲授予代理簽章者簽署權力時，首先，依據其秘密金鑰產生數值，將此數值秘密傳送給代理簽章者，代理簽章者再利用自己所擁有之秘密金鑰與所接收的數值計算之後，得到代理金鑰。此代理金鑰即可產生代理簽章。由於代理金鑰是由代理簽章者的秘密金鑰所計算出的，唯有擁有此金鑰的人方可得知代理金鑰之後產生代理簽章。因此，除了代理簽章者，沒有任何人 (包括原始簽章者) 可以產生代理簽章。所以滿足鑑別性及不可否認性的特性。

伍、效率評估

簽章者具名之門檻式代理鑑別加密法的計算成本包括原始簽章者的授權、代理鑑別加密、特定驗證者鑑別解密、任意驗證者驗證代理簽章所需花費的計算成本，如表一所示。而通訊成本包含公開代理資訊、鑑別加密訊息以及數位簽章的位元長度，如表二所示。由於模加法與模減法所需的運算時間相對於複雜的模乘法或模指數等所需的運算時間較低，因此評估計算成本時可以忽略不計，為方便本章節的效率評估各階段之計算成本及位元長度，茲將符號定義如下：

T_E：計算一次模指數運算所需時間。

T_M：計算一次模乘法運算所需時間。

T_I：計算一次模反元素運算所需時間。

T_H：計算一次單向雜湊函數運算所需時間。

t：代理群體的門檻值。

n：代理群體的參與者總數。

$|k|$：變數 k 的位元長度。

表一 所提方法的計算成本

階段	計算成本
原始簽章者的授權代理	$2T_H+(2nt-n+2)\,T_M$ $+(2t-1)\,T_E$
代理鑑別加密	$(t+3)\,T_H+(4t+2)\,T_M+3\,T_E$ $+1\,T_I$
特定驗證者鑑別解密	$2T_H+(\,t+4\,)\,T_M+4\,T_E+T_I$
任意驗證者鑑別解密	$2\,T_H+(t+4)\,T_M+3\,T_E+T_I$

表二 所提方法的通訊成本

階段	通訊成本
公開代理資訊	$\|p\|+\|q\|+\|mw\|$
鑑別加密訊息	$3\|p\|+\|q\|+\|m_w\|+\|ASID\|$
數位簽章	$2\|p\|+\|q\|+\|m_w\|+\|ASID\|$

六、結論

我們有鑑於群體導向應用的安全控管機制會隨著網路科技與資訊技術的發展越來越重要，本論文從應用密碼學理論與技術面提出門檻式代理鑑別加密的議題，提出安全且具效率之適用於群體導向應用的門檻式代理鑑別加密法，以確保群體運作之機密性、完整性、鑑別性以及不可否認性等安全特性。

一般鑑別加密法只能交由特定驗證者來鑑別解密所收到的鑑別加密訊息，但本論文所提的方法允許驗證者可以在不需要花費額外計算成本的情況下，可將鑑別加密訊息轉換成一般的數位簽章，讓 TTP 或是任意的仲裁者也可以確認原始簽章者確實簽署過訊息，以達到不可否認安全需求。此外，所提的方法也考量群體運作所可能面臨的使用者欺騙行為，而且提供多種方法來偵測原始簽章者及驗證者來確保群體簽章驗證的公平性及正確性。

簽章者具名之門檻式代理鑑別加密法允許原始簽章者將其簽章權限，授權給特定的代理群體，並且可以針對代理群體設定不同的代理門檻策略。本論文所提的方法只能利用授權書的規定，將原始簽章者、代理群體以具名方式，加以限制其授權、代理的範疇與期限等，一旦發生代理群體與驗證者共謀的情形，還是會發生欺騙的行為，因此未來可以利用密碼機制來強制限定代理群體的代理權限或利用其他機制來改善原始簽章者、代理群體及驗證者之間的授權關係。

參考文獻

[1] 吳宗成, 許建隆, 蔡國裕, “適用於群體導向之匿名代理鑑別加密”, 第十三屆全國安全會議, pp. 74-82, 2003

[2] 賴溪松, 韓亮, 張真誠, “近代密碼學及其應用”, 旗標, 2004

[3] T.S. Chen, K.H Huang and Y.F. Chung, “A practical authenticated encryption scheme based on the elliptic curve cryptosystem”, Computer Standards and Interfaces, Vol. 26, pp. 461-469, 2004

[4] W. Diffie and M.E. Hellman, “New directions in cryptography”, IEEE Transactions on Information Theory, Vol. IT-22, pp. 644-654, 1976

[5] P. Horster, M. Michels and H. Petersen, “Authenticated encryption schemes with low communication costs”, Electronics Letters, 30, Vol.15, pp. 1212-1213, 1994

[6] C.L. Hsu and T.S. Wu, “Self-certified threshold proxy signature schemes with message recovery, nonrepudiation, and traceability”, Applied Mathematics and Computation Vol. 164, pp. 201-225, 2005

[7] C.L. Hsu, T.S. Wu and T.C. Wu, “New nonrepudiable threshold proxy signature scheme with known signer”, Journal of Systems and Software, Vol. 58, pp. 119-124, 2001

[8] C.L Hsu, T.S. Wu and W-H He, “New proxy multi-signature scheme”, Applied Mathematics and Computation, Vol. 162, pp. 1201-1206, 2005

[9] S.J Hwang and C.C Chen, “New threshold proxy threshold signature schemes”, Computers and Electrical Engineering, Vol. 31, pp. 69-80, 2005

[10] S Kim, S Park and D Won, “Proxy signature, revisited” Proceedings of International Conference on Information and Communications Security ICIS’97, Springer-Verlag, pp. 223-232, 1997

[11] N.Y. Lee and M.F. Lee, “The security of a strong proxy signature scheme with proxy signer privacy protection”, Applied Mathematics and Computation, Vol. 161, pp. 807-812, 2005

[12] E.J. Lu, M.S. Hwang and C.J. Huang, “A new proxy signature scheme with revocation”, Applied Mathematics and Computation, Vol. 161, pp. 799-806, 2005

[13] M. Mambo, E. Okamoto and K. Usuda, “Proxy signatures for delegating signing operation”, 3rd ACM Conf. On computer and Communication Security, pp. 48-57, 1996

[14] M. Mambo, K. Usuda and E. Okamoto, “Proxy signatures: Delegation of the power to sign messages”, IEICE Trans. Fundamentals, Vol. E-79-A, pp. 1338-1354, 1996

[15] K. Miyazaki and K. Takaragi, “A threshold digital signature scheme for a smart card based system”, IEICE Trans. Fundamentals, Vol. E-84-A, pp. 205-213, 2001.

[16] H.M. Sun, “On proxy (multi-) signature schemes”, Proceedings of the International Computer Symposium, pp. 65-72, 2000

[17] H.M. Sun, “Convertible proxy signature scheme”, 第十一屆全國計算機會議, pp. 186-189, 1999

[18] H.M. Sun, “An efficient nonrepudiable threshold proxy signature scheme with known signers”,Computer Communications, Vol. 22, no. 8, pp. 717-722, 1999

[19] S.F. Tzeng, M.S. Hwang and C.Y Yang, “An improvement of nonrepudiable threshold proxy signature scheme with known signers”, Computers and Security, Vol. 23, pp. 174-178, 2004

[20] S.F. Tzeng, C.Y. Yang and M.S. Hwang, “A nonrepudiable threshold multi-proxy multi-signature scheme with shared verification”, Future Generation Computer Systems, Vol. 20, pp. 887-893, 2004

[21] Y.M. Tseng, J.K. Jan and H.Y Chien, “Authenticated encryption schemes with message linkages for message flows”, Computers and Electrical Engineering, Vol. 29, pp. 101-109, 2003

[22] Y.M. Tseng and J.K. Jan, “Attacks on threshold signature scheme with traceable signers”, Information Processing Letters, vol.71, pp. 1-4, 1999.

[23] C.T. Wang, C.H. Lin and C.C. Chang, “Threshold signature schemes with traceable signers in group communications”, Computer Communications, Vol. 21, pp. 771-776, 1998

[24] T.S. Wu and C.L. Hsu, “Cryptanalysis of group-oriented (t, n) threshold digital signature schemes with traceable signers”, Computer Standards and Interfaces, Vol. 26, pp. 477-481, 2004

[25] T.S. Wu and C.L. Hsu, “Convertible authenticated encryption scheme”, The Journal of System and Software, Vol. 62, pp. 205-209, 2002

[26] C.Y. Yang, S.F Tzeng and M.S. Hwang, “On the efficiency of nonrepudiable threshold proxy signature scheme with known signers”, Journal of Systems and Software, Vol. 73, pp. 507-514, 2004