# 具鑑別性之代理盲簽章設計

**蘇品長曾健豪***

國防大學資訊管理學系

## 摘要

數位簽章為網路世界中的重要設計，用以辨識及確認電子文件簽署人身分、資格及電子文件真偽者。其中代理盲簽章更是客製化的應用，結合代理簽章及盲簽章的概念，適合於電子商務上，例如：電子投票、電子交易...等。在電子商務的環境中，經常需在短時間內處理一筆電子交易的紀錄；因此，通訊安全及計算成本顯得格外重要。本研究提出可同時簽章和鑑別加密的代理盲簽章演算法，除了增加鑑別性外，又補強了不可否認性，並運用模擬實作方式驗證此演算法之可行性，且與先前演算法分析比較，證明此研究不僅能達到所有安全性要求，也能減少計算成本，提升運算效率，以利爾後實務上運用。

**關鍵詞：**鑑別性，代理盲簽章，鑑別加密法

# A Blind Proxy Signature Design with Authenticity

**Pin-Chang Su and Jian-Hao Zeng ***

*Department of Information Management, National Defense University*

## ABSTRACT

Digital signature is one of the important designs in the internet world.Its purpose is to confirm signer's identity, qualification level and authenticity. Blind proxy signature, the concept of combining proxy signature and blind signature, can be applied customized in e-business, such as digital voting, digital trade etc. Digital trading often needs to be processed in a short amount of time in E-business environment; thus, communication safety and calculation cost are especially important. This research proposed an authenticated encryption design that can process signature and encryption at the same time.Other than incorporating authenticated design, it also strengthens its non-repudiation. Through real life simulation, we're able to verify its feasibility and analyzing it compare with former calculation method; hence, demonstrating such research will not only reach all the safety requirements, but also increases calculation efficiency and minimize the cost in order to apply it in real life situation.

**Keywords:** Authenticity, Blind Proxy Signature, Authenticated Encryption.

文稿收件日期 104.8.12;文稿修正後接受日期 105.3.2;*通訊作者
Manuscript received August 12, 2015;revised March 2, 2016;* Corresponding author

# 一、前言

隨著網際網路的快速發展，資訊流通更為方便與快速，電子商務交易日漸頻繁，許多公司企業都希望利用此模式來創造商機，然而，「水能載舟，亦能覆舟」；利潤與安全往往是一體兩面的，安全機制越嚴謹，消費者就越放心的在網路上進行交易，如何讓消費者安心的在網路上交易和抵抗外來侵入者的攻擊，是一個值得探討的議題[1]。

1978 年，由 Rivest 等人[2]所提出的公開金鑰簽章方式，在網路世界中，我們則是利用數位簽章來確定是否為原始傳輸者，因為數位簽章具有機密性、完整性、鑑別性和不可否認性；其安全性基於分解兩個大質數上，是目前最著名的公開金鑰密碼系統之一，通常使用單向雜湊函數來減少簽章時所需的時間和傳送訊息。是現今商業上使用最為廣泛的數位簽章系統。

1982 年，Chaum[3]率先提出了盲簽章的概念，主要就是簽章者在不知道文件內容的情況下，就要得到簽章者的簽章，其具有兩種特性：一是簽章者對所簽署的文件內容是盲目的，也是就簽章者不知道自己所簽文件的內容；二是即使公佈文件內容和簽章，簽章者也無法追蹤文件與當時他所簽署文件的關係。應用層面為匿名投票或電子貨幣等，緊接著許多變化，例如：由 Abe 和 Fujisaki[4]提出基於 RSA 難解問題的部份盲簽章、Juang 和 Lei[5]也提出了門檻式盲簽章等。1996 年，Mambo[6]等人提出新的盲簽章機制，其概念大致如下，當原始簽章者無法親自簽署時，原始簽章者能指派他的簽章給另一位他所信任的簽章者，也就是所謂的代理簽章者，除了原始簽章者、代理簽章者之外，還有簽章驗證者，簽章驗證者能驗證該簽章的合法性、正確性，也能區別出簽章是由原始簽章者或是代理簽章者所簽署的。

2002 年，Tan 等人[7]整合代理簽章和盲簽章技術，成為代理盲簽章，並表示一個完整的代理盲簽章應俱備可區分性、不可否認性、可驗證性、不可偽造及不可追蹤性。而後 Xue 和 Cao[8]指出 Tan 等人[7]的協定不俱備匿名的特性，並提出一個新的協定，解決 Tan 等人[7]協定的問題。但是，Li 等人[9]也發現 Xue 和 Cao 的協定無法提供不可偽造性及不可連結性。2007 年，Li 和 Wang 提出了使用自我認證公開金鑰的代理盲簽章協定[10]，能抵擋公鑰替換攻擊，並且與 Tan 等人[7]的協定進行效能比較。2008 年，Yang 和 Yu 提出有效的代理盲簽章協定[11]，是基於離散對數問題上，並指出他們的協定在計算量上比 Li 和 Wang 的協定更有效率。在 2009 年，Oo 和 Thein 提出植基於離散對數問題的代理盲簽章協定[12]，並表示他們的協定不僅滿足代理盲簽章所需俱備之安全需求，也比其他協定更有效及低計算量；然而，2011 年，Alghazzawi 等人[13]指出此機制並無法提供簽章的完整性，提出了一套基於橢圓曲線離散對數難題的新型代理盲簽章機制，號稱能解決簽章完整性的問題，且運用此機制，能更節省效率。

2000 年，許建隆與吳宗成[14]等學者提出一套可以「真正同時」簽章和加密的鑑別加密法(Authenticated Encryption)。簽署者利用自己的私鑰和驗證者的公鑰要產生簽章，再將此簽章傳送給該特定驗證者進行驗證；此簽章限定只由特定驗證者驗證並回覆訊息，恰可補強「無對運算的隨機代理盲簽密」安全效益不足部份，另以計算成本而言，運用解橢圓曲線離散對數難題代替解離散對數難題，可大大增加計算效率[15]。後續學者對訊息本身簽密及「鑑別性」等問題卻鮮少探討，其用應用性值得存疑，有些機制也嘗試以先簽章後加密方式，然就效率分析而言，增加多餘的計算量及金鑰長度，不符成本；後續的研究，不斷的針對效益及安全之間做出權衡，到了近代，2013 年覃海生與張雷[16]等學者提出植基於離散對數難題的「無對運算的隨機代理盲簽密」，在簽密過程中運用了隨機因子，提高安全效益，實際分析其機制，針對訊息本身簽密部分並未特別強化，訊息鑑別之安全性仍略顯不足，且以計算成本而論，運用解離散對數難題特性，並非最佳的方法；2015 年，葉昱宗[17]「新型態之電子投票機制」論文中提出符合上述安全性需求的新型態應用設計，唯鑑別性為多文件的客製制化設計，是否適用於一般性的應用，尚待評估。

本文架構一共區分為六章，各章說明如下：第一章：說明研究背景、動機與目的；第二章：針對論文、期刊等文獻，整理歸納出「代理盲簽章」的相關資料，第三章：嘗試結合鑑別加密法與橢圓曲線密碼系統之架構，設計具「鑑別性」之代理盲簽密機制，第四章：配合

程式實作，驗證此系統之可行性；第五章：針對本研究方法與先前代理盲簽章機制進行安全與效益分析；第六章：針對本文做簡單的結論、探討其貢獻度及未來可研究方向，並為有興趣於此鑽研之研究學者提供目標。

## 二、文獻探討

本章整理出實驗相關的「代理盲簽章」文獻，包含 Tan 等人[7]、Alghazzawi 等人[13]、覃海生與張雷[16]及鑑別加密法[21]，概述如後：

### 2.1 基於離散對數及橢圓曲線離散對數的代理盲簽章

「Digital Proxy Blind Signature Schemes Based on DLP and ECDLP」是 2002 年由 Tan 等人[7]學者所提供新的簽章方式，顧名思義就是結合代理簽章和盲簽章的特性，經由原始簽章者授權給代理簽章者後，代理簽章者可以對欲簽署文件產生盲簽章，當然也就視同原始簽章者對該文件簽署的認可，其概述如下：

(1)系統初始階段：系統產生各種參數提供於簽章過程中使用。

- 任選兩個大質數 $p$ 和 $q$，計算 $n=pq$。
- 任選一整數 $e$，需滿足 GCD ($e$, $\varphi(n)$)=1；$1 < e < \varphi(n)$，並計算 $d = e^{-1} \bmod \varphi(n)$。
- 原始簽章者選擇私密金鑰 $X_O$，並計算相對應公開金鑰 $Y_O = g^{X_O}$。
- 代理簽章者選擇私密金鑰 $X_P$，並計算相對應公開金鑰 $Y_P = g^{X_P}$。

(2)代理簽章金鑰產生階段：原始簽章者將透過下列步驟產生代理簽章金鑰($R$, $S$)。

- 原始簽章者隨機產生一亂數 $k$。

$$R = g^k \bmod p;\ S = X_O R + k$$

- 將($R$, $S$)透過安全通道送給代理簽章者，收到之後利用 $g^S = Y_O{}^R R$ 來驗證($R$, $S$)是否正確。
- 若正確，代理簽章者計算代理簽章金鑰

$$\sigma = S + X_P$$

(3)代理盲簽章產生階段：簽章要求者將訊息做加盲的動作，再傳送給簽章者簽署，完畢後回傳給簽章要求者去盲。

- 代理簽章者任選一整數 $k_P$，計算 $t = g^{k_P}$，將($t$, $R$)透過安全通道送給簽章要求者。
- 盲化：簽章要求者選 $\alpha$, $\beta$ 為盲因子，計算

$$r = t g^{\beta} Y_P{}^{-\alpha-\beta} (Y_O{}^R)^{-\alpha}$$

$$e = h(r||m);$$

$$u = (Y_O{}^R R)^{-e+\beta} Y_O{}^{-e}$$

$$e' = e - \alpha - \beta$$

將 傳送給代理簽章者。

- 簽署：代理簽章者收到 後，計算 $s' = e'\sigma + k_P$，再將 傳送給簽章要求者。
- 去盲：簽章要求者收到 後，計算 $s = s' + \beta$，而 $(m, u, s, e)$ 為對的簽章。

(4)驗證階段：驗證者收到簽章之後驗證簽章的合法性。其安全效益仍明顯不足!

- 驗證者收到 後，驗證 $e = h(g^s Y_P{}^{-e} Y_O{}^e u \bmod p)$ 是否成立。
- 若成立則表示 ($u$為有效簽章。

### 2.2 基於橢圓曲線離散對數的新型態代理盲簽章

2011 年 Alghazzawi 等人[13]學者提出植基於 ECDLP 的演算法，此機制可以適用於智慧及 PDA 等小型處理器；相關敘述如下：

(1)代理階段

- 代理產生：原始簽章者在 [1, $n$區間任選一整數 ，計算 $I$， $P = (x_1$ 及 $r = x_1$，必須在 [0, $q$，接著計算 s $= (d + kr)$及 $Q_p$。
- 傳送盲因子：原始簽章者傳送 (給代理簽章者，並公布 。
- 代理者驗證：在接收 (後，代理簽章者利用 $Q_p = sP = Q$ 式子驗證。

(2)簽章階段

- 代理簽章者在 [1, n區間任選一整數 ，計算 $U$，傳送給驗證者。
- 驗證者隨機選擇 $\alpha, \beta \rightarrow [1, n$並計算 $\tilde{R} = U + \alpha P -$， $\tilde{e} = H(I$，$e = (\tilde{e} + \beta)$1；並將 傳送給代理簽章者。
- 代理簽章者接收 後，接著計算

  $\tilde{s} = (t - se)$1，在傳送給驗證者。
- 驗證者接收 後，接著計算

  $s_p = (\tilde{s} + \alpha)$1， $(M, s$為代理盲簽章對。

(3)驗證階段

- 驗證者利用下列式子

  $\gamma = H((s_p P + \tilde{e} Q_p$ 驗證代理盲簽章對 $(M, s$中， $\gamma$。

## 2.3 無對運算的隨機代理盲簽密

2013 年覃海生與張雷[16]提出植基於離散對數難題的「無對運算的隨機代理盲簽密」，在簽密過程中運用了隨機因子，提高安全效益，實際分析其機制，針對訊息本身簽密部分並未特別強化，其安全效益仍明顯不足，且以計算成本而論，運用解離散對數難題特性，並非最佳的方法；相關敘述如下：

(1)初始及密鑰生成階段

任選一亂數 $k$，得到兩個大質數 $p$ 和 $q$，其中 $p|q-1$，$k \in$ ， 是階為 $q$、生成元為 $g$ 的群。任選取安全的單向函數： ， 然後，KGC 隨機選取 $S_{\text{MASTER}}$，並計算系統公鑰，公開相關參數。

(2)密鑰生成階段

給定用戶身分 ，KGC 隨機選取 $S_u \in Z_q^*$，計算

$w_u \equiv g^{s_u}$1

$t_u = s_u + sH_2(ID_u, w_u)$1

給定用戶身分 ，部分公鑰 以及部分私鑰 ，由用戶隨機選擇 $r_u$作為自己的祕密值，計算 $u_u \equiv g^{r_u}$1

(3)委託階段

- 授權階段：原始簽名者 C 隨機選擇 $l$1，計算

  $h \equiv g^l$1； $y_p = u_D{}^{n_2}$1

  為簽証公鑰。
- 代理密鑰生成：產生( )作為代理簽名者的代理簽名密鑰。

(4)代理盲簽密階段

需要簽名者發送請求，並對之前與簽名者協商好的 M 處理，計算

$t_1 = r_A H_1(M)$1； $t_2 = g^{t_A}$1

將( $t$)與請求一起發送給簽名者，簽名者收到後並驗證；接著計算 $\alpha = ahr$；

$\beta = g^{t_D} \bmod p$； $b = \beta^{\alpha}$mc並將 $b$ 傳送給消息擁有者，實施盲化，計算

$u = g^{z_1} b^{z_2} \bmod p$ ； $r \equiv Mu$mc

$M' = rz_2{}^{-1}$1

接著用代理私鑰( )計算

$s' \equiv a\lambda + m'\sigma$1

並將 傳給消息擁有者 A，計算

$s \equiv s'z_2 + z_1$1，並將( )及 作為盲簽密通過安全通道傳給消息接收者 B 供解簽密使用。

(5)解簽密階段

消息接收者接收$(u, s)$和 $r$ 驗證並計算，得到

$M_1 \equiv rg^{-s} y_p^{u} \bmod p_1$，代表$M_1$為原本訊息。

(6)驗證階段

將接收到的簽章$(u, s)$和通過解密得到的訊息 M 代入$g^s \equiv u y_p{}^{mu}$若成立，則$(u, s)$就是原消息 M 的簽密。

## 2.4 鑑別加密法

簽章加密法(signcryption)在公開金鑰密碼學(public key cryptographic)中是一個新的術語，此術語最早由在 1997 年 Zheng[21]在密碼學會議中提出。目的是可以在單一的步驟中，同時達到數位簽章及加密的功能，而且成本遠遠比傳統的先簽後加密方法低得多。

2000 年，許建隆與吳宗成[14]等學者提出了「鑑別加密法」(Authenticated Encryption)是一套可以「真正同時」完成簽章和加密的機制。簽署者利用自己的私鑰和驗證者的公開金

鑰要來產生簽章，隨後再將此簽章送給該特定的驗證者來驗證；這個簽章只能由該特定的驗證者才能才能夠驗證並且回復訊息。敘述如下：

(1)使用者$U_A$選擇一個隨機參數值為$k \to Z_q^*$

(2)使用者$U_A$利用使用者$U_B$的公鑰$y_b$設計加密演算法$E = (y_b{}^k \bmod p) \bmod q$。

(3)使用者$U_A$利用私鑰$x_a$產生與訊息$m$結合，產生簽章$(r, s)$

$r = m \cdot E \bmod p;\ s = k - x_a \cdot r \bmod q$

(4)接著計算$E = (y_b{}^s \cdot y_{ab}{}^r \bmod p) \bmod q$;其中$y_{ab} = g^{x_a \cdot x_b} \bmod p$。

(5)使用者$U_B$利用私鑰$x_b$解密，獲得$m = r \cdot E^{-1} \bmod p$。

(6)使用者$U_B$檢查附加在訊息$m$之後的冗餘是否正確。如果正確則表示此簽章唯一合法正確的簽章。

## 三、研究方法

本研究除了運用「鑑別加密法」補足其安全特性外，也運用「橢圓曲線公開金鑰密碼系統」，其具有相同安全度下，使用的加密金鑰長度較其他系統小且處理速度快，使得具有更高的安全性；本章針對所提之運作流程及系統架構分別說明：

### 3.1 本系統整體運作流程架構及參數表

本研究系統設計之演算法區分為系統初始化及密鑰生成階段、委託階段、盲簽密階段、解盲化階段及驗證階段等五個階段，整體運作流程架構如圖 1，相關系統符號說明表如表 1 所示:

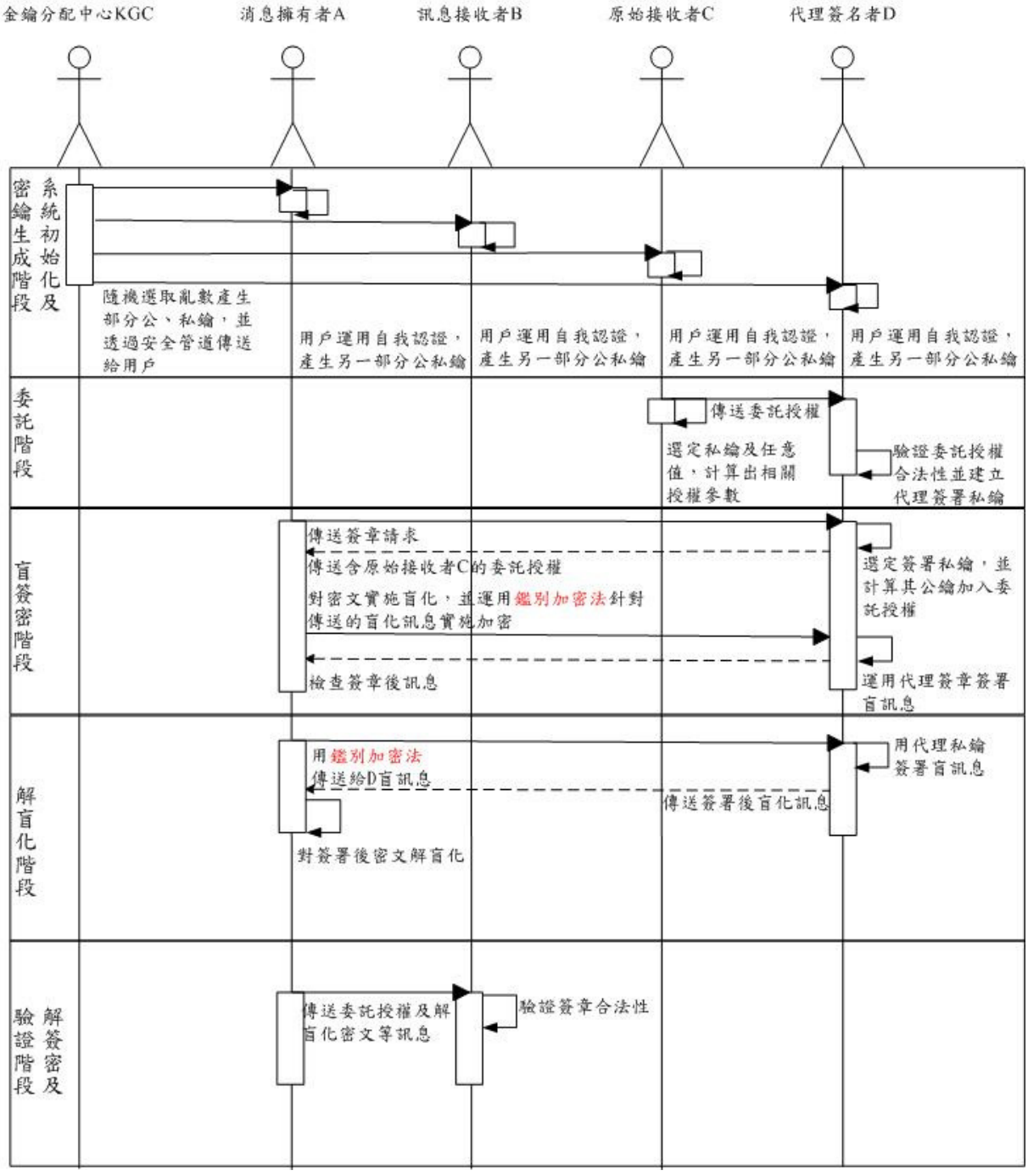


圖 1.整體運作流程圖。

表 1.系統符號說明表

| 項次 | 符號 | 說明 | 項次 | 符號 | 說明 |
|---|---|---|---|---|---|
| 1 | $E(F_q)$ | 有限域 $F_q$ 中的一條橢圓曲線 | 14 | $z_3$ | 鑑別加密法盲因子 |
| 2 | $G$ | 橢圓曲線中的基點 | 15 | $m_w$ | 原始接收者C授權給代理簽名者D範圍內的訊息值 |

| | | | | | |
|---|---|---|---|---|---|
| 3 | $n$ | 橢圓曲線上基點的秩(Order) | 16 | $h_1$ | 將用戶身份$id_u$與部份公鑰$W_u$轉換成值的雜湊函數 |
| 4 | $q$ | $q > 2^{224}$之質數 | 17 | $H_2$ | 將明文序列$m$轉換成點的雜湊函數 |
| 5 | $PK_{CA}$ | CA 系統主公鑰 | 18 | $Y_p$ | 簽証公鑰 |
| 6 | $sk_{CA}$ | CA 系統主私鑰 | 19 | $m_w$ | 是指C授權給D範圍內的訊息 |
| 7 | $sk_u$ | 自行選定之部份私鑰 | 20 | $k_o$ | 原始簽名者 C 隨選之任意值，計算授權公鑰$R_o$。 |
| 8 | $id_u$ | 用戶身分 | 21 | $R_o$ | 授權公鑰 |
| 9 | $W_u$ | 使用者由 CA 主密鑰計算所產生之部份私鑰 | 22 | $k_p$ | 代理簽章者 D 隨選之任意值，計算代理私鑰$R_p$。 |
| 10 | $t_u$ | 使用者由 CA 主密鑰計算所產生之部份私鑰 | 23 | $R_p$ | 代理私鑰$R_p$。 |
| 11 | $U_u$ | 使用者自行運算所產生之部份公鑰 | 24 | $z_1$, $z_2$ | 代理盲簽章盲因子 |
| 12 | $r_u$ | 使用者自行運算所產生之部份私鑰 | 25 | $(\lambda, \sigma)$ | 代理簽名者的代理簽署私鑰 |
| 13 | $U_E$ | 代理盲簽章隨機因子 | 26 | $S_{AD}$ | 消息擁有者A與代理簽名者D之間的傳送金鑰 |

### 3.2 鑑別加密法之隨機代理盲簽章

系統架構可分為系統初始化及密鑰生成階段、委託階段、盲簽密階段、解簽密及驗證階段等五個階段，各步驟分述如后：

#### 3.2.1 系統初始化及密鑰生成階段

(1)系統認證中心(CA)系統建置階段：系統在有限域上選取一條安全的橢圓曲線$E(F_q)$ ($q$ 為一個 224 bits 以上之大質數)並在$E(F_q)$上選一階數(Order)為$n$的基點$G$，使得$n \cdot G = O$，其中 $O$ 為此橢圓曲線之無窮遠點；並選擇一個單向雜湊函數$h_1()$，計算公開參數。

$$PK_{CA} = sk \quad (3\text{-}1)$$

給定用戶身分$id_u$，CA 隨機選取$sk_u \in (1 < k_u < n)$，計算：

$$W_u = sk \quad (3\text{-}2)$$

$$t_u = sk_u + sk_{CA} \cdot h_1(id_u \quad (3\text{-}3)$$

最後公開$\{G, q, n, PK_{CA}, h_1(), id_u\}$。

CA 分別替消息擁有者 A、訊息接收者 B、原始接收者 C 及代理簽章者 D 選擇$\{sk_A, sk_B, sk_C, sk_D \in Z_n^*\}$為系統主密鑰，並計算出由系統選定之部份公鑰$\{W_a, W_b, W_c, W_d\}$及私鑰$\{t_A, t_B, t_C, t_D\}$。

(2)由此可知，消息擁有者$id_A$的部分公鑰為

$$W_A \equiv sk_i \quad (3\text{-}4)$$

消息擁有者$id_A$部分私鑰為

$$t_A = sk_A + sk_{CA} \cdot h_1(id_A, \quad (3\text{-}5)$$

簽名接收者$id_B$的部分公鑰為

$$W_B \equiv sk_B \cdot G \quad (3\text{-}6)$$

簽名接收者$id_B$部分私鑰為

$$t_B = sk_B + sk_{CA} \cdot h_1(id_B, W_B) \quad (3\text{-}7)$$

原始接收者$id_C$的部分公鑰為

$$W_C \equiv sk_C \cdot G \quad (3\text{-}8)$$

原始接收者$id_C$部分私鑰為

$$t_C = sk_C + sk_{CA} \cdot h_1(id_C, W_C) \quad (3\text{-}9)$$

代理簽名者$id_D$的部分公鑰為

$$W_D \equiv sk_D \cdot G \quad (3\text{-}10)$$

代理簽名者$id_D$部分私鑰為

$$t_D = sk_D + sk_{CA} \cdot h_1(id_D, W_D) \quad (3\text{-}11)$$

(3)給定用戶身分$id_u$，部分公鑰$W_u$以及部分私鑰$t_u$，由用戶隨機選擇$r_u \in (1 < r_u < n)$作為自己的祕密值，計算

$$U_u \equiv r_u \cdot G \quad (3\text{-}12)$$

用戶公鑰為$PP_u = \{W_u, U_u\}$，私鑰為$PS_u = \{t_u, r_u\}$。消息擁有者$id_A$公鑰為$PP_A = \{W_A, U_A\}$，私鑰為$PS_A = \{t_A, r_A\}$，簽名接收者$id_B$公鑰為$PP_B = \{W_B, U_B\}$，私鑰為$PS_B = \{t_B, r_B\}$，原始簽名者$id_C$公鑰為$PP_C = \{W_C, U_C\}$，私鑰為$PS_C = \{t_C, r_C\}$，代理簽名者$id_D$公鑰為$PP_D = \{W_D, U_D\}$，私鑰為$PS_D = \{t_D, r_D\}$。

### 3.2.2 委託階段

(1)授權階段：原始簽名者 C 隨選一個任意值$k_o (1 < k_o < n)$隨，計算授權公鑰$R_o$。

$$R_o \equiv k_o \cdot G \equiv (R_{ox}, R_{oy}) \quad (3\text{-}13)$$

$$n_1 = t_C \cdot R_{ox} + r_C \quad (3\text{-}14)$$

$$N_2 = W_D + PK_{CA} \cdot h_1(id_D, W_D) \quad (3\text{-}15)$$

$$Y_p = n_1 \cdot U_D \quad (3\text{-}16)$$

$Y_p$為簽証公鑰，將$\{R_o, n_1, N_2, m_w\}$透過安全通道傳給代理簽名者 D，其中$m_w$是指 C 授權給 D 範圍內的訊息，代理簽名者 D 收到後再實施驗証。

(2)代理密鑰生成：計算$(\lambda, \sigma)$

$$\lambda = t_D \cdot R_o = (\lambda_x, \lambda_y) \quad (3\text{-}17)$$

$$\sigma = r_D \cdot n_1 \quad (3\text{-}18)$$

並將$(\lambda, \sigma)$作為代理簽名者的代理簽署私鑰。

### 3.2.3 代理盲簽密階段

(1)需要簽名的消息擁有者 A 發送簽名請求，並對之前與簽名者協商好的 $m$ 處理，計算

$$T_1 = r_A \cdot H_2(m) = r_A \cdot M \quad (3\text{-}19)$$

$$T_2 = t_A \cdot G \quad (3\text{-}20)$$

將$T_1, T_2$與請求一起發送給簽名者，簽名者收到後並驗證

$$\begin{aligned} & T_1 + T_2 \\ &= (r_A \cdot M) + \left(sk_A + sk_{CA} \cdot H_1(id_A, W_A)\right) \cdot G \\ &= (r_A \cdot M) + (W_A + PK_{CA} \cdot H_1(id_A, W_A)) \\ &= r_A \cdot M + h_1(id_A, W_A) \cdot PK_{CA} + W_A \end{aligned} \quad (3\text{-}21)$$

驗證$PK_{CA}$, $W_A$是否正確。

(2)若成立，代理簽章者 D 隨機選擇$k_p (1 < k_p < n)$，計算代理私鑰$R_p$

$$\alpha = k_p \cdot R_o = (\alpha_x \quad (3\text{-}22)$$

$$\beta = 1 \quad (3\text{-}23)$$

$$R_p = \alpha \cdot \beta = k_p \cdot R_{ox} \cdot \quad (3\text{-}24)$$

並將$R_p$傳送給消息擁有者，但消息擁有者 A 不希望簽名者看到訊息 $M$，對訊息實施盲化，任取$z_1$ 、$z_2 \in Z_n^*$，計算隨機因子$U_z$。

$$U_z \equiv z_1 \cdot G + z_2 \cdot R_p \equiv (U_x \quad (3\text{-}25)$$

$$R_z \equiv M + U_z \equiv (R_{zx}, \quad (3\text{-}26)$$

$$m' = R_{zx} \cdot \quad (3\text{-}27)$$

將$m'$用鑑別加密法加密，消息擁有者 A 隨機選擇$z_3 \in (1 < z_3 < n)$，消息擁有者 A 利用代理簽章者 D 的公鑰$U_D$設計加密演算法

$$E = z \quad (3\text{-}28)$$

消息擁有者 A 利用私鑰$r_A$產生與訊息$M'$結合，產生$R'$, $S'$

$$R' = m' \cdot G \quad (3\text{-}29)$$

$$S' = z_3 \cdot G - r \quad (3\text{-}30)$$

將$R'$, $S'$傳送給代理簽章者 D，代理簽章者 D 接著計算$E$。

$$E = z_3 \cdot U_D \quad (3\text{-}31)$$

(3)消息擁有者 A 運用祕密通道將$U_{AD}$傳送給代理簽章者 D；其中：

$$U_{AD} = r_A \cdot r \quad (3\text{-}32)$$

$$m' \cdot G = R' - E \quad (3\text{-}33)$$

檢查附加在訊息$m'$之後的冗餘是否正確。如果正確則表示此簽章唯一合法正確的簽章。

(4)接著代理簽名者 D 用代理私鑰$(\lambda, r_D)$計算

$$s_Z' \equiv k_p \cdot \lambda_x + m' \cdot \sigma \quad (3\text{-}34)$$

並將$s'$通過安全管道傳給消息擁有者 A，消息擁有者 A 收到後並計算

$$s_z \equiv s_Z' z_2 + z_1 \quad (3\text{-}35)$$

並將$(U_Z, s_Z)$作為盲簽密通過安全通道傳給消息接收者 B，同時將$R_z$透過秘密通道給消息接收者 B 供解簽密使用。

### 3.2.4 解簽密階段

(1)消息接收者接收$(U_Z, s_Z)$和$R_z$驗證並計算，得到$M_1$

$$M_1 \equiv R_Z - s_z \cdot G + R_{Z_X} \cdot Y_p \quad (3\text{-}36)$$

(2)求$R_1$，$R_1 \equiv M_1 + U$;接著驗證$R_z = R_1$，若成立，代表$M_1$為原本訊息。

### 3.2.5 驗證階段

將接收到的簽章$(U_Z, s_Z)$和通過解密得到的訊息 $M$ 代入

$$s_Z \cdot G \equiv U_Z + R_{Z_X} \cdot Y_p \quad (3\text{-}37)$$

若成立，則$(U_Z, s_Z)$就是原消息 $M$ 的簽密。

## 四、系統模擬

本章將針對所提方法之系統架構，實際帶入數據進行系統實作，說明如下：

### 4.1 系統初始化及密鑰生成階段

(1)系統在有限域上選取一條安全的橢圓曲線 $y^2=x^3+3x+60 \pmod{3001}$建立 $E(F_{3001})$，從 $E(F_{3001})$選一個基點 $G=(1,8)$，其階數 $n$ 為 2962，使得$2962 \cdot G=O$，其中 $O$ 為此橢圓曲線之無窮遠點，如圖 2。

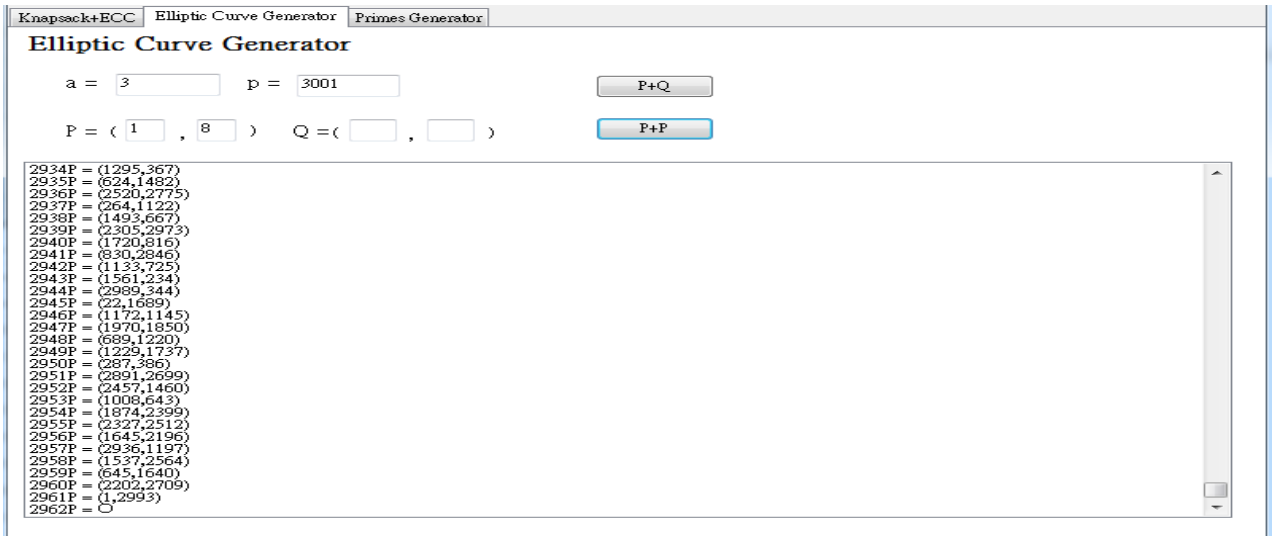


圖 2. 產生橢圓曲線。

$$PK_{CA} = sk_{CA} \cdot G$$
$$= 97 \cdot (1, 8) = (1520, 97) \quad (4\text{-}1)$$

(2)系統替消息擁有者 A、訊息接收者 B、原始接收者 C、代理簽名者 D 分別選擇 $sk_A = 3$、$sk_B$=5、$sk_C$=7、$sk_D$=11，$sk_A, sk_B, sk_C, sk_D \in Z_{2962}^*$當成系統私鑰，並計算出相應之公鑰$W_A, W_B, W_C, W_D$，及私鑰 $t_A, t_B, t_C, t_D$。

$$W_u = sk_u \cdot G \quad (4\text{-}2)$$

$$t_u = sk_u + sk_{CA} \cdot h_1(id_u, W_u) \quad (4\text{-}3)$$

$W_A = sk_A \cdot G$

消息擁有者 A 部分私鑰為

$$t_A = sk_A + sk_{CA} \cdot h_1(id_A, W_A) = 3 + 97 \cdot 2 = 197 \quad (4\text{-}5)$$

$$W_B = sk_B \cdot G = 5 \cdot (1,8) = (2936,1804) \quad (4\text{-}6)$$

訊息接收者 B 部分私鑰為

$$t_B = sk_B + sk_{CA} \cdot h_1(id_B, W_B) = 5 + 97 \cdot 4 = 393 \quad (4\text{-}7)$$

$$W_C = sk_C \cdot G = 7 \cdot (1,8) = (2327,489) \quad (4\text{-}8)$$

原始接收者 C 部分私鑰為

$$t_C = sk_C + sk_{CA} \cdot h_1(id_C, W_C) = 7 + 97 \cdot 6 = 589 \quad (4\text{-}9)$$

$$W_D = sk_D \cdot G = 11 \cdot (1,8) = (2891,302) \quad (4\text{-}10)$$

$$t_D = sk_D + sk_{CA} \cdot h_1(id_D, W_D) = 11 + 97 \cdot 8 = 787 \quad (4\text{-}11)$$

(3)給定用戶身分$id_u$，部分公鑰$W_u$以及部分私鑰$t_u$，由用戶隨機選擇$r_u \in (1 < r_u < n)$作為自己的祕密值，計算

$$U_u \equiv r_u \cdot G \quad (4\text{-}12)$$

$$U_A \equiv r_A \cdot G;\ r_A = 13 = 13 \cdot (1,8) = (1229,1264) \quad (4\text{-}12\text{-}1)$$

$$U_B \equiv r_B \cdot G\ ;\ r_B = 17 = 17 \cdot (1,8) = (22,1312) \quad (4\text{-}12\text{-}2)$$

$$U_C \equiv r_C \cdot G = 19 \cdot (1,8);\ r_C = 19 = (1561,2767) \quad (4\text{-}12\text{-}3)$$

$$U_D \equiv r_D \cdot G;\ r_D = 23 = 23 \cdot (1,8) = (2305,28) \quad (4\text{-}12\text{-}4)$$

消息擁有者 A 公鑰為

$PP_A = \{W_A, U_A\} = \{(645,1361), (1229,1264)\}$

私鑰為$PS_A = \{t_A, r_A\} = \{197, 13\}$

簽名接收者 B 公鑰為

$PP_B = \{W_B, U_B\} = \{(2936,1804), (22,1312)\}$

私鑰為$PS_B = \{t_B, r_B\} = \{393,17\}$

原始簽名者 C 公鑰為

$PP_C = \{W_C, U_C\} = \{(2327,489), (1561,2767)\}$

$= 3 \cdot (1,8) = (645, 1361)$ (4-4)

私鑰為$PS_C = \{t_C, r_C\} = \{589,19\}$

代理簽名者 D 公鑰為

$PP_D = \{W_D, U_D\} = \{(2891,302), (2305,28)\}$

私鑰為$PS_D = \{t_D, r_D\} = \{787,23\}$。

## 4.2 委託階段

(1)授權階段：原始簽名者 C 隨選一個任意值$k_\sigma = 29$，計算其公鑰$R_\sigma$、x 軸座標值、$n_1$、$N_2$、$m_w$，其中$m_w$是指 C 授權給 D 範圍內的訊息，透過安全通道傳給代理簽名者 D。

$$R_\sigma \equiv k_\sigma \cdot G \equiv (R_{\sigma x}, R_{\sigma y}) \equiv 29 \cdot (1,8) \equiv (2305,28) \quad (4\text{-}13)$$

$$n_1 = t_c \cdot R_{\sigma x} + r_C = 589 \cdot 2309 + 19 = 567 \quad (4\text{-}14)$$

$$N_2 = W_D + PK_{CA} \cdot h_1(id_D, W_D) = 205 \cdot (1,8) = (1830, 2981) \quad (4\text{-}15)$$

$$Y_p = n_1 \cdot U_D = (1877, 1502) \quad (4\text{-}16)$$

(2)代理密鑰生成：計算$(\lambda, \sigma)$

$$\lambda = t_D \cdot R_\sigma = (\lambda_x, \lambda_y) = (2335,1876) \quad (4\text{-}17)$$

$$\sigma = r_D \cdot n_1 = 23 \cdot 567 = 1037 \quad (4\text{-}18)$$

將$(\lambda, \sigma) = \{(2335,1876), 1037\}$作為代理簽名者的代理簽署私鑰。

## 4.3 代理盲簽密階段

(1)需要簽名的消息擁有者 A 發送簽名請求，並對之前與簽名者協商好的 $m$ 處理，計算

$$T_1 = r_A \cdot H_2(m) = r_A \cdot M = 481(1,8) = (2203, 2630) \quad (4\text{-}19)$$

$$T_2 = t_A \cdot G = 197(1,8) = (61, 1311) \quad (4\text{-}20)$$

將$T_1, T_2$簽名請求一起發送給代理簽章者 D，代理簽章者 D 收到後並驗證。

$$T_1 + T_2 = (r_A \cdot M) + (t_A \cdot G) = (r_A \cdot M) + \left(sk_A + sk_{CA} \cdot h_1(id_A, W_A)\right) \cdot G$$

$$= (r_A \cdot M) + h_1(id_A, W_A) \cdot PK_{CA} + W_A$$
$$= 678(1,6) \quad (4\text{-}21)$$

驗證$PK_{CA}$, $W_A$。

(2)若成立，代理簽章者 D 隨機選擇任意值$k_p = 41$，計算代理私鑰$R_p$

$$\alpha = k_p \cdot R_o = (\alpha_x, \quad \alpha_y)$$
$$= 1189(1,8) = (1823,1754) \quad (4\text{-}22)$$
$$\beta = t_D \cdot G$$
$$= 787(1,8) = (4,1022) \quad (4\text{-}23)$$
$$R_p = \alpha_x \cdot \beta$$
$$= 1093(1,8) = (2274,1635) \quad (4\text{-}24)$$

並將$R_p$傳送給消息擁有者 A。

(3)但消息擁有者 A 不希望簽名者看到訊息 $M$，對訊息實施盲‧化，任取$z_1 = 47$, $z_2 = 43$，計算隨機因子$U_s$。

$$U_s \equiv z_1 \cdot G + z_2 \cdot R_p \equiv (U_{s_x}, \quad U_{s_y})$$
$$\equiv 2616(1,8) \equiv (2833,2728) \quad (4\text{-}25)$$
$$R_s \equiv M + U_s \equiv (R_{s_x}, \quad R_{s_y})$$
$$\equiv 2653(1,8) \equiv (369, 1842) \quad (4\text{-}26)$$
$$m' = R_{s_x} \cdot z_2^{-1}$$
$$= 369 \cdot 43^{-1} = 2870 \quad (4\text{-}27)$$

將$M'$用鑑別加密法加密，消息擁有者 A 隨機選擇$z_3 = 23$，消息擁有者 A 利用代理簽章者D 的公鑰$U_D$設計加密演算法。

$$E = z_3 \cdot U_D$$
$$= 1219(1,8) = (762, 2 \quad (4\text{-}28)$$
$$R' = m' \cdot G + E$$
$$= 1127(1,8) = (2205,2952) \quad (4\text{-}29)$$
$$S' = z_3 \cdot G - r_A \cdot R'$$
$$= 407(1,8) = (2665,2474) \quad (4\text{-}30)$$

將$R'$, $S'$傳送給代理簽章者 D，代理簽章者 D 接著計算$E$

$$E = z_3 \cdot U_D$$
$$= 1219(1,8) = (762, 2222) \quad (4\text{-}31)$$

(4)消息擁有者 A 運用祕密通道將$U_{AD}$傳送給代理簽章者 D

$$U_{AD} = r_A \cdot r_D \cdot G$$
$$= 299(1,8) = (1753, 1562) \quad (4\text{-}32)$$
$$m' \cdot G = R' - E$$
$$= 2870(1,8) = (1068,651) \quad (4\text{-}33)$$

檢查附加在訊息$m'$之後的冗餘是否正確。如果正確則表示此簽章唯一合法正確的簽章。

(5)接著代理簽名者 D 用代理私鑰$(\lambda, r_D)$計算

$$s_s' \equiv k_p \cdot \lambda_x + m' \cdot \sigma$$
$$\equiv 1902 \quad (4\text{-}34)$$

並將$s'$通過安全管道傳給消息擁有者 A，消息擁有者 A 收到後並計算

$$s_s \equiv s_s' z_2 + z_1$$
$$\equiv 1902 \cdot 43 + 47 \equiv 806 \quad (4\text{-}35)$$

將$(U_Z, s_Z)$作為盲簽密通過安全通道傳給消息接收者 B，同時將$R_s$透過秘密通道給消息接收者 B 供解簽密使用。

### 4.4 解簽密階段

(1)消息接收者接收$(U_Z, s_Z)$和$R_s$驗證並計算，得到$M_1$

$$M_1 \equiv R_Z - s_s \cdot G + R_{Z_X} \cdot Y_p$$
$$\equiv 37(1,8) \quad (4\text{-}36)$$

(2)求$R_1$，$R_1 \equiv M_1 + U$；接著驗證$R_s = R_1$，若成立，代表$M_1$為原本訊息。

$$R_1 \equiv M + U_s \equiv (R_{s_x}, \quad R_{s_y})$$
$$\equiv 2653(1,8) \equiv (369,1842) \quad (4\text{-}26)$$

### 4.5 驗證階段

將接收到的簽章$(U_Z, s_Z)$和通過解密得到的訊息 $M$ 代入

$$s_Z \cdot G \equiv U_Z + R_{Z_X} \cdot Y_p$$
$$\equiv 806(1,8) \equiv (2490,224) \quad (4\text{-}37)$$

驗證成立，$(U_Z, s_Z)$就是原消息 $M$ 的簽密。

## 五、安全性及效益分析

本研究於應用上可滿足「代理盲簽章」所

需功能，安全性部分，符合 ISO 組織所提之機密性、完整性等資訊安全管理需求[22]，並滿足機密性、完整性、驗證性、隱匿性及可註銷性等基本特性，做安全分析比較。並參酌文獻[23]所提之運算量，時間複雜度運算關係表，做出分析比較，相關說明如後：

## 5.1 安全性分析

針對各項安全需求分析說明如下：

### 5.1.1 機密性(Confidentiality)

機密性是指資料不得被未經授權之個人、實體或程序所取得或揭露的特性。本系統中密文傳輸使用了橢圓曲線公開金鑰之加密方法，管理者以橢圓曲線點加法，編碼如(3-11)與(3-12)式，將使用者存取權限予以編碼。破譯者若想解開這些資訊，將面臨橢圓曲線離散對數難題，需先經由破解(3-17)與(3-18)式，再從(3-17)與(3-18)式中設法得知值$(t_D, r_D)$與取得雙方共享金鑰；儘管破譯者不管運用何種方法取得$(W_D, U_D)$，仍然會再面臨到橢圓曲線離散對數難題，攻擊者無法順利偽造，故達成保密需求。

### 5.1.2 完整性(Integrity)

完整性是指對資料之精確與完整安全保證的特性。假若破譯者想偽冒原始消息擁有者 A 發送訊息給代理簽名者 D 簽署，除非獲得代理簽名者 D 的代理簽署資訊，否則代理簽署私鑰$(\lambda, \sigma)$是無法被偽造的。編碼如(3-17)-(3-18)式將代理簽名的代理簽署私鑰$(\lambda, \sigma)$傳送給對方(消息擁有者 A)，對方也將須授權的訊息進行雜湊運算，再結合消息擁有者 A 的簽名檔透過(3-22)- (3-27)式，運算並回傳，若第三方想要竄改或偽冒代理簽名者 D 簽章而不被現，則他將面對破解單向雜湊函數(One-Way 發 Hash Function, OWHF)及橢圓曲線離散對數難題；假若破譯者想要偽冒代理簽名者 D，除非獲得代理簽名者 D 私鑰$(t_D, r_D)$，將面對破解橢圓曲線離散對數難題，否則傳送至消息擁有者 A 之代理簽署是無法被偽冒或更改的。

### 5.1.3 不可否認性(Non-repudiation)

不可否認性指的是對一已發生之行動或事件的證明，使該行動或事件往後不能被否認的能力。在(3-16)式除了$Y_p$簽証公鑰，(3-9)- (3-12)式中，$(t_C, r_c)$為原始接收者 C 的私鑰，因此$Y_p$除了鑑別代理簽名者 D 的身分外，原始接收者 C 也無法否認曾經授權給代理簽名者 D 簽章；另一方面，代理簽名者 D 無法否定提出服務請求或使用過該服務。

覃海生與張雷[16]的演算法針對原始接收者曾經授權的問題未深入探討，僅針對代理簽章者無法否認提出服務請求部分提出說明，對使用過該服務無法否認部分也無特別著墨，故此演算法不完全符合此特性。

### 5.1.4 驗證性(Verifiability)

驗證性指的是簽署文件能通過驗證者的驗證，證明文件為指定的簽署者所簽；在(3-16)-(3-17)式中，驗證簽密是由訊息接收者 B 接到訊息的簽密$(U_Z, S_Z)$，經過(3-12)、(3-14)與(3-16)式，經由參數計算，檢驗簽章的正確性，故滿足其特性。

### 5.1.5 隱匿性(Anonymity)

隱匿性是網際網路獨特的一種特性，又稱盲化；訊息擁有者不想讓代理簽章者知道訊息的詳細內容，必須讓訊息盲化，滿足隱匿性；在(3-25)-(3-27)式中，消息擁有者 A 在訊息發送前對訊息進行了盲化處理，由於$z_1, z_2 \in Z_n^*$為訊息擁有者 A 任意選取的，故代理簽章者 D 無從得知，故滿足其特性。

### 5.1.6 可註銷性(Log out)

可註銷性是授權者想回收之前釋放出去的權力；原始簽章者 C 想要收回代理簽章者 D 的代理簽章權，在(3-12)-(3-16)式中，於任意值$k_o(1 < k_o < n)$為原始接收者 C 隨機選擇的，原始接收者 C 只需要在整個系統內公布代理公鑰$Y_p$失效，之後代理簽名者 D 所生成的代理簽章均失效，故滿足其特性。

### 5.1.7 鑑別性(Authentication)

覃海生與張雷[16]提出植基於離散對數難題的「無對運算的隨機代理盲簽密」，在簽密過程中運用了隨機因子，以強化身分識別的安全機制，惟對訊息本身的簽密部分並未特別強化，安全性顯著不足，同時兼具身分及訊息的識別及保護即為鑑別性的定義；鑑別性適用於如使用者、程序、系統與資訊等實體確保一主體或資源之識別就是其所聲明者的特性。

(1)假設攻擊者偽冒代理簽章者 D 要獲得消息擁有者 A 訊息，他必須偽造$(R', s')$；在(3-29)-(3-31)式中，消息擁有者 A 隨機選擇$z_3 \in (1 < z_3 < n)$；$r_A$為消息擁有者 A 的私鑰，均無法得知，故符合其鑑別性。

(2)然而假設消息擁有者 A 想要偽造代理簽名者 D 的簽章，他必須偽造$(U_Z, S_Z)$；在(3-25)與(3-35)式中，也必須偽造$R_p, s'$;必須透過(3-22)- (3-24)與(3-34)，由於$k_p, \lambda_x, \sigma$僅掌握在代理簽名者 D 手中，故滿足其特性。

(3)將接收到的簽密$(U_Z, S_Z)$和通過解簽密得到的訊息$M$帶入(3-37)式，進行驗證，透過式(3-26)與(3-36)，若成功即為原訊息 $M$ 的簽密，符合其鑑別特性。

覃海生與張雷[16]的演算法主要是針對委託階段，原始接收者授權給代理簽名者實施盲簽章時，訊息傳送部分未深入探討有關鑑別部分，故安全性明顯不足，故本研究運用「鑑別加密法」以強化此特性，相關研究之彙整分析比較詳如表 2。

表 2. 本研究與其他演算法安全分析比較

| 演算法與安全性 | Tan 等人[7] | Alghazzawi 等人[13] | 覃海生與張雷[16] | 本研究方案 |
|---|---|---|---|---|
| 機密性 | X | X | V | V |
| 完整性 | △ | △ | V | V |
| 不可否認性 | X | V | △ | V |
| 鑑別性 | X | X | **X** | V |
| 可驗證性 | V | V | V | V |
| 隱匿性 | V | V | V | V |
| 可註銷性 | V | V | V | V |
| 註一：V 代表符合特性、△代表部分符合、X 代表不符合特性 | | | | |

## 5.2 效益分析

本研究參酌表 3 之運算量[17]分析比較，彙製時間複雜度運算關係表，如以整體效益而言，Alghazzawi 等人[13]的運算效益雖較高，分析其演算法，針對訊息加密、鑑別性全未考量，訊息完整性部分在盲簽章階段中也無相關機制，安全性顯著不足，相關分析表如表 4 所示：

表 3.時間複雜度運算之相互關係參考表

| 符號 | 定義 | 運算時間 |
|---|---|---|
| $T_{ECMUL}$ | 進行一次 ECC 乘法運算所需時間 | $\approx 29\ T_{MUL}$ |
| $T_{ECADD}$ | 進行一次 ECC 加法運算所需時間 | $\approx 5\ T_{MUL}$ |
| $T_{INVS}$ | 進行一次模式乘法反元素運算所需時間 | $\approx 240\ T_{MUL}$ |
| $T_{EXP}$ | 進行一次模式指數運算所需時間 | $\approx 240\ T_{MUL}$ |
| $T_{ADD}$ | 進行一次模式加法運算所需時間() | 可忽略不計 |

表 4.存取時間複雜度比較表

| 演算法 | | Tan 等人[7] | | Alghazzawi 等人[13] | | 覃海生與張雷[16] | | 本研究方案 | |
|---|---|---|---|---|---|---|---|---|---|
| 階段 | 比較 | 演算法 | 時間複雜度 | 演算法 | 時間複雜度 | 演算法 | 時間複雜度 | 演算法 | 時間複雜度 |

| | 項目 | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| 代理階段 | 代理運算 | $3T_{ECMUL}+1T_{ECADD}+1T_{MUL}+2T_{ADD}$ | $\approx 64 T_{MUL}$ | $3T_{ECMUL}+1T_{ECADD}+1T_{MUL}+2T_{ADD}$ | $\approx 64 T_{MUL}$ | $2T_{MUL}+4T_{EXP}+1T_{ADD}+1t_h$ | $\approx 962.4 T_{MUL}$ | $2T_{ECMUL}+1T_{ECADD}+1t_h$ | $\approx 63.4 T_{MUL}$ |
| 盲簽密階段 | 加密運算 | 無 | 無 | 無 | 無 | 無 | 無 | $3T_{ECMUL}+3T_{ECADD}$ | $\approx 102 T_{MUL}$ |
| | 盲簽運算 | $8T_{ECMUL}+6T_{ECADD}+3T_{MUL}+7T_{ADD}+1t_h$ | $\approx 265 T_{MUL}$ | $3T_{ECMUL}+2T_{ECADD}+2T_{MUL}+3T_{ADD}+1t_h$ | $\approx 99 T_{MUL}$ | $4T_{MUL}+4T_{EXP}+2T_{INVS}+1T_{ADD}$ | $\approx 1444 T_{MUL}$ | $2T_{ECMUL}+2T_{ECADD}$ | $\approx 68 T_{MUL}$ |
| 驗證階段 | 驗證運算 | $3T_{ECMUL}+3T_{ECADD}+1t_h$ | $\approx 68 T_{MUL}$ | $2T_{ECMUL}+1T_{ECADD}+1T_{MUL}+1t_h$ | $\approx 64 T_{MUL}$ | $2T_{MUL}+T_{EXP}$ | $\approx 242 T_{MUL}$ | $2T_{ECMUL}+2T_{ECADD}$ | $\approx 68 T_{MUL}$ |
| | 解密運算 | 無 | 無 | 無 | 無 | $2T_{MUL}+2T_{EXP}$ | $\approx 482 T_{MUL}$ | $2T_{ECMUL}+2T_{ECADD}$ | $\approx 68 T_{MUL}$ |
| 總和 | | $14T_{ECMUL}+10T_{ECADD}+4T_{MUL}+9T_{ADD}+2t_h$ | $\approx 397 T_{MUL}$ | $7T_{ECMUL}+4T_{ECADD}+4T_{MUL}+4T_{ADD}+2t_h$ | $\approx 277 T_{MUL}$ | $10T_{MUL}+11T_{EXP}+2T_{INVS}+2T_{ADD}+1t_h$ | $\approx 3130.4 T_{MUL}$ | $11T_{ECMUL}+10T_{ECADD}+1t_h$ | $\approx 369.4 T_{MUL}$ |

註：僅有本研究對盲簽密部份有加密運算，故運算成本較第二種演算法高

## 六、結論

本研究設計具同時簽章和加密的鑑別代理盲簽章演算法，除了增加鑑別性外，又補強了不可否認性，並運用橢圓曲線加密法改善效率，模擬實作方式驗證此演算法之可行性，且與先前演算法分析比較，證明此研究不僅能達到所有安全性要求，也能減少計算成本，提升運算效率，以利後續相關領域研究運用；預期貢獻如下：

(1)透過「鑑別加密法」，將被授權的訊息利用此方法從消息擁有者傳送給代理簽名者，符合其「鑑別性」。

(2)本機制除了滿足「鑑別性」外，在消息擁有者傳送給代理簽名者，因應用代理簽名者公鑰傳送訊息，故代理簽名者無法否認沒有接收此要求，故補足在訊息傳送時的「不可否認性」。

(3)以橢圓曲線密碼系統執行權限密文加密，在同樣的密鑰長度下，擁有更高安全性，更適用於電子行動商務。

(4)本研究以程式模擬實驗，以實作數據來證明其演算法之可行性，未來研究可導入門檻式系統，以提供爾後應用於日常實務上。

## 參考文獻

[1] 李南逸，王智弘，林峻立，張智超，溫翔安，葉禾田，“網路安全與密碼學概論”，滄海書局，第 15-18 頁，2008。

[2] Rivest, R.L., Shamir, A., andAdleman, L., “A Method for Obtaining Digital Signature and Public Key Cryptosystem,” Communications of the ACM, Vol. 21, No. 2, pp.120-126, 1978.

[3] Chaum, D.,“Blind Signatures for Untraceable Payments,” Advances in Cryptology-CRYPTO’82,pp.199-203,1982.
[4] Abe, M. and Fujisaki, E., “How to Fate Blind Signatures,”Advances in Cryptology- ASIACRYPT’96, pp.244-251, 1996.
[5] Juang, W.S. and Lei, C.L., “Blind Threshold Signatures Based on Discrete Logarithm,” Proceedings Second Asian Computing Science Conference on Networking and Security, Vol. 1179, pp.172-181, 1996.
[6] Mambo, M.,Usuda, K.,and Okamoto, E., “Proxy Signatures for Delegating Signing Operation,” Proceedings thirdACM Conference on Computer and Communications Security, pp.48-57, 1996.
[7] Tan, Z.,Liu,Z., and Tang, C., “Digital Proxy Blind Signature Schemes Based on DLP and ECDLP,” MM Research Preprints, MMRC, AMSS, Academia Sinica, Vol. 21, pp.212-217, 2002.
[8] Xu, Q., and Cao, Z., “A New Proxy Blind Signature Scheme with Warrant,”2004 IEEE Conference on Cybernetics and Intelligent Systems, pp.1386-1391, 2004.
[9] Li, J., and Wang, S., “New Efficient Proxy Blind Signature Scheme Using Verifiable Self-Certified Public Key,”International Journal of Network Security, Vol. 4, No. 2, pp.193-200, 2007.
[10] Li, J., and Wang, S., “New Efficient Proxy Blind Signature Scheme Using Verifiable Self-Certified Public Key,” International Journal of Network Security, Vol. 4, No. 2, pp.193-200, 2007.
[11] Yang, X., and Yu, Z.,“An Efficient Proxy Blind Signature Scheme Based on DLP,” The2008 International Conference on Embedded Software and Systems (ICESS2008), pp.163-166, 2008.
[12] Oros, H., andPopescu, C., “A Secure and Efficient Off-line Electronic Payment System for Wireless Networks,” International Journal of Computers, Communications and Control, Vol. 5, pp.551-557, 2010.
[13] Alghazzawi, D. M., Salim, T. M., and Hasan, S. H., “A new proxy blind signature scheme based on ECDLP,” International Journal of Computer Science Issues, Vol. 8, No. 1, pp.73-79, 2011.
[14]許建隆，吳宗成，“簽章加密法及其應用”，資訊安全通訊，第 6 卷，第 1 期，第 33-41 頁，2000。
[15]蘇品長，“植基於 LSK 和 ECC 技術之公開金鑰密碼系統”，長庚大學電機工程系研究所博士論文，2007。
[16]覃海生，張雷，“無對運算的代理盲簽章方案設計”，計算機應用研究，第 39 卷，第 4 期，第 169-173 頁，2013。
[17]葉昱宗，“新型態之電子投票機制”，國防大學資訊管理學系碩士班論文，2015。
[18] Koblitz, N., “Elliptic Curve Cryptosystems”, Mathematics of Computation American Mathematical Society, Vol. 48, pp.203-209. 1987.
[19] Wang, R. C., “A Web Metering Scheme for FairAdvertisement Transactions,” International Journal of Security and its Applications,Vol. 2, No. 4, pp.49-55,2008.
[20] Girault, M., “Self-Certified Public Keys,” Advances in Cryptology- Eurocrypt’91, Vol. 547, pp.490-497,1991.
[21] Nishoka,T.,Matsuura,K,. Tzeng,Y.,andImai,H., “A proposed for authenticated key recovery system,” in Proceedings of 1997 Joint Workshop on information Security and Cryptolography, pp.189-196,1997.
[22] ISO, Information technology-Security techniques-Code of practice for information security controls, ISO/IEC 27002, 2013.
[23] Wang, R. C., “A Web Metering Scheme for Fair Advertisement Transactions,” International Journal of Security and its Applications,Vol. 2, No. 4, pp.49-55, 2008.