資訊管理研究　Vol.14, 2014 第 73-94 頁

植基於橢圓曲線之多重盲簽密機制
- 具一次投領多重選票之設計

蘇品長
國防大學資訊管理學系

楊倫青
國防大學資訊管理學系

王博彥
國防大學資訊管理學系

摘要

在網路普及化的社會裡已有許多國家漸漸採取盲簽章技術來實現不可追蹤及不可偽造等特性的應用，電子投票及電子付款即為常見的例子；以電子投票為例，在整個電子投票過程裡，如何達到更有效率的執行速度與更安全的防護是值得省思的議題。陸續已有學者提出了局部盲簽章、公平盲簽章、橢機盲簽章、門檻式盲簽章等相關理論的論文，唯電子投票機制均採取單一盲簽章技術；本研究提出了多重盲簽密機制，以植基於橢圓曲線的快速運算為基礎，並能以多份電子選票執行一次盲簽章及加密的方法，以減少在傳遞過中的簽章及加密的次數，提升在運算過程中的效率及更安全的防護，可適用在多合一選舉電子投票及多筆電子付款一次支付的應用機制上。

關鍵字：橢圓曲線、盲簽章、電子投票、電子付款

Multiple Blind Signcryption Scheme Based on ECC Technology- Design of the E-voting at One Time for Multiple Polls

Pin-Chang Su
Department of Information Management, National Defense University

Lun-Qing Yang
Department of Information Management, National Defense University

Po- Yan Wang
Department of Information Management, National Defense University

Abstract

In the society of the Internet popularity that have many countries adopting the skills of the Blind Signature to fulfill unlinkability and unforgeability characteristics. Therefore, E-voting and E-payment that are usually used for them. For instance, in E-voting process, how to achieve more efficiency on the performing speed adds more safe protection that are worthy of considering issue in the future. Regarding to this, many scholars have submitted relative theories gradually such as the Partially Blind Signature, Fair Blinding Signature, Randomized Blind Signature, Threshold Blind Signature, etc. Viewing current E-voting systems on many countries is adopting the sole Blind Signature on the base of study skills. My professor and I have done research and submitted Multi-Blind Signcryption system. That is based on the fast calculation of the Elliptic Curve Cryptosystem and also can perform the Blind Signcryption and the method of encryption one time in the multitude copies of E-voting poll. Therefore, the system can reduce many times signatures and encryption on the transmitting process. Also, it can promote the efficiency in the calculating process and enhance more safe protection. That system is also applied for multiple elections of the E-voting changing into one kind type of the E-voting election in the future as well as multiple E-payments, which can be paid at one time.

Keywords: Elliptic Curve Cryptosystem, Blind Signature, E-voting, E-payment

壹、緒論

多合一選舉方式為近年來的新趨勢，2010 年 3 月 23 日台北市長郝龍斌表示(今日新聞網，民 99 年)，為了簡併選務，簡省選務經費，以及簡併選務工作等考量。北市府決定採三合一選舉：第 5 屆市長、11 屆市議員，以及 11 屆里長，將在同一天舉行「三合一」選舉。民政局長黃呂錦茹指出，「三合一」選舉會帶動整體投票率，雖然，市府補助里長每票新台幣 30 元支出將提高，但整體而言預估可省下經費約 800 萬元。另簡併選舉，選務工作分量加重，預估北市的投開票所將超過 1400 處以上，投入選務人員預估超過 2 萬人。此外，以往里長選舉投票率都不高，投票率大約在 30% 至 35% 之間，預估舉行「三合一」選舉，在五都選舉競爭激烈的氣氛下，官方也預期里長選舉的投票率，將跟著大幅提升。在選舉頻率很高的情況下，如總統，縣市長，立委、縣市議員、直轄市長及里長等選舉，每次所耗費的人力、物力、財力等有形與無形的資源難以計數。伴隨著網際網路的普及，研究以電子化方式在網路上運行，取代傳統以人工的方式來作業，是一個值得研究的課題。

Chaum (1982)率先提出盲簽章的觀念，在這個簽章方法裡面有兩個角色，一個是簽章者，另一個是簽章要求者，盲簽章能讓簽章要求者在不洩漏訊息的情形下，讓簽章者對該訊息加以簽名。因為盲簽章具有保護簽章要求者隱私的特性，所以可被應用於電子付款以及電子投票的機制中。此外，Chaum 認為將盲簽章應用到電子投票上，必須克服一些難題，諸如完整性、不可脅迫性及非欺騙性等問題。隨著學者們不斷改進，期許能將電子投票機制透過網際網路完成投票結果，滿足電子投票的最大特性與最小限制(Chang et al., 2006; Delaune et al., 2006; Liaw, 2004; Fan et al., 2008)。這些方法所提出：無論投票者身處何地，透過網際網路都可以進行投票，既可節省時間，又可不用特地返回戶籍地去投票而所受的舟車之勞，大大提升投票的便利性。但這些機制卻都僅考慮單一投票一次盲簽章之設計，且無加密機制的應用；如果我們能以多份選票來進行一次盲簽密並且導入加密的機制，勢必縮短了作業上的流程且強化資訊的安全性。本研究提出的多重盲簽密法適用於多合一選舉的電子投票機制，以多合一縣市議員選舉方案為例，將選票來選擇自己理想中的候選人，而一人可能有三張或三張以上選票來選擇不同類別的候選人，數以萬人可能就有數以萬張的選票，在執行上可減少多餘的簽章，提升運算上的時間，也能得到更佳的安全保護。

貳、文獻探討

一、橢圓曲線公開金鑰密碼系統

公開金鑰密碼學的理論在百年前就已經很完備，而橢圓曲線在代數學與幾何學上廣泛的研究也已超出百年之久，橢圓曲線系統第一次應用於密碼學上是由 Miller (1985)與 Koblitz (1987)分別提出，從此橢圓曲線在密碼學中就扮演重要的角色。茲將橢圓曲線密碼系統的定義及原理，分述如后(肖攸安，民 95 年)：

(一)橢圓曲線定義

令 P>3 為質數，在 $GF(P)$ 中的橢圓曲線 $E: y^2 = x^3 + ax + b \bmod p$ ，其中 $4a^3 + 27b^2 \neq 0 (\bmod p)$ 。曲線上另定義一個無窮遠點 O，對任一點 $A \in E$ ，$A + O = O + A = A$ 。

加法運算

令 $A = (x_1, y_1)$ 與 $B = (x_2, y_2)$ 為 E 上的點，則若 $x_2 = x_1$ 且 $y_2 = -y_1$ ，則 $A + B = O$ ；否則 $A + B = (x_3, y_3)$ ，其中 $x_3 = \lambda^2 - x_1 - x_2$ ， $y_3 = \lambda(x_1 - x_3) - y_1$

$$\lambda = \begin{cases} \dfrac{y_2 - y_1}{x_2 - x_1} & \text{if } A \neq B \\ \dfrac{3x_1^2 + a}{2y_1} & \text{if } A = B \end{cases}$$

橢圓曲線中的乘法運算是透過加法運算達成的。為了加快速度，可以用 doubling 的運算來達成。例如：計算時，由於 $4P = 2P + 2P$ ，再計算 $2P = P + P$ 即可。

反元素運算

點 $A = (x, y)$ 的反元素 $-A = -(x, y) = (x, -y)$ 。(因為 $A + (-A) = (-A) + A = O$，此時 O 稱為乘法單位元素)，例子：在橢圓曲線 $E: y^2 = x^3 + x + 6 (\bmod 11)$ 上的點有：(2, 4)(2, 7)(3, 5)(3, 6)(5, 2) (5, 9)(7,2)(7,9)(8, 3) (8,8) (10,2)(10,9) 再加上 O 共有 13 點。注意在計算點時，要檢驗 $x^3 + x + 6$ 之值是否屬於 QR_{11} 。除了 O 以外，任意點均可以視為 E 的始元素(primitive element)。

註：令定義於 Z_p 的橢圓曲線 E 的所有點的個數為 $\#E$ ，則 $p+1-2\sqrt{p} \leq \#E \leq p+1+2\sqrt{p}$ (蘇品長，民 96 年)。

假設一個橢圓曲線是屬於 Fq，而 P 是橢圓曲線 E 上的一個點，給定一個屬於橢圓曲線 E 上的一個點 Q，若要找出一整數 k 使得 Kp = Q，因為其特殊的點加法運算，破密者除了逐一的窮舉所有可能的點之外，別無他法。直至目前為止，這個問題仍無法於多項式時間內求出解答。橢圓曲線密碼系統的另一個優點是其加密的密鑰長度短，在同樣的安全度之下，橢圓曲線

密碼系統僅需要較小的密鑰長度，相同地，在同樣的密鑰長度下，橢圓曲線密碼系統卻擁有更高的安全性。表 1 為 RSA 與 ECC 在相同安全度下金鑰長度之比較表(蘇品長，民 96 年)：

表 1 RSA 與 ECC 相同安全度金鑰比較表

RSA 與 ECC 相同安全度金鑰長度比較					
RSA	512	1024	2048	3072	7680
ECC	112	163	224	256	384
Key	1:5	1:6	1:9	1:12	1:20

二、橢圓曲線簽密法

Zheng 等人(1998)提出以橢圓曲線為基礎之簽密法，以下為此簽密法的描述，假設送方 A 欲對明文 M 產生簽密文並將簽密文傳給收方 B 作解密與驗章。Zheng 的方法分成「系統初始階段」、「送方簽密階段」、「收方解密及驗簽階段」，分如後：

系統初始階段

系統在有限域 F_q 上選取一條安全的橢圓曲線 $E(F_q)$ (q 為一個 160bit 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 nG=O，其中 O 為此橢圓曲線之無窮遠點。選定一單向無碰撞雜湊函數 $H()$ 及一組對稱式加解密函數，令其加密函數為 $E()$ ，解密函數為 $D()$ ，系統公 $E(F_q), G, n, q, H(), E(), D()$ ，使用者 A、B 依系統參數分別選擇 $n_A, n_B \in Z_q^*$ 當成私鑰，並計算其相應之公鑰 $PK_A = n_A \cdot G$ ， $PK_B = n_B \cdot G$ 。

送方簽密階段

送方 A 使用以下步驟產生簽密文(C, h, s)以收方之憑證驗證其公鑰 PK_B 正確性，選取一亂數 $r \in Z_n^*$ ，計算 $B = H(r.PK_B) = (x_B, y_B)$ 計算密文 $C = E_{x_B}(M)$ ，計算 $h = H(M)$ ，計 $s = r/(h + n_A) \bmod q$ ，將簽密文(C, h, s)送出。

收方解密及驗簽階段

以送方之憑證驗證其公鑰正確性，計算 $u = s \cdot n_B \bmod q$ ，計算 B'=H(uPKA+u.k.G)，以 $x_{B'}$ 進行解密得到明文 $M' = D_{x_{B'}}(C)$ ，驗證 $h \stackrel{?}{=} H(M')$ ，若等式成立則收方接受送方訊息，並且表示簽密文確為送方所產製，反之，收方拒絕送方之簽密文。

三、盲簽章

Chaum(1982) 以 RSA 的方法提出盲簽章機制，運用密碼學中數位簽章之特性，使用公鑰與私鑰的特性對訊息做加密、解密，做為送簽者與需求者間確認之用，而電子匿名投票選舉即是利用這個方法確保投票者的身分達到隱匿效果。舉例來說，如同投票人「送簽者」請選委會「簽章者」在一封經彌封的選票信件上蓋鋼戳，鋼戳的戳記印痕會經由外層的信封複印至內層的選票，以證明此選票之合法性戳記，再將此封內含有選票信件回覆給具合法身分的投票人，投票人於收到蓋有戳

記的選票後，先檢查信封是否仍處於彌封狀態，再將選票自信封中取出，此選票帶有選務中心鋼戳的戳記，以證明此張選票之合法性。投票人在此選票上自行圈選後寄往開票中心，但該選票上不會記錄投票人身分或地址，寫上寄往開票中心的地址，如此完成匿名投票的步驟。圖 1 為盲簽章流程關係圖，運作流程概述茲分述如下：

Step1：假設(n,e)、d 分別為簽署者之公鑰與密鑰，使用者想要將訊息 M 送給簽署者簽章，但又不想讓簽署者知道訊息 M 的內容。使用者隨機挑選一整數 R 為盲因子，須滿足條件 GCD (R,n) = 1。

Step2： 計算 M'=Re x M mod n 後，將 M' 傳送給簽署者。

Step3：當簽署者收到 M'後，以密鑰 d 計算 $S'=M'^{d} \bmod n=M^{d}R^{ed} \bmod n$，將 S'回傳給使用者，在簽署過程中，簽署者完全不知道簽署資料的內容。

Step4：使用者利用之前所選擇的盲因子 R，對此簽章做除盲化的動作R-1，將收到的S'內之盲因子移除，計算 $S = S'R^{-1} \bmod n$ ，獲得S即為簽署者對訊息M的簽章。任何人均可以使用 $S^{e} = M \bmod n$ 來驗證(M,S)的有效性，若驗證成立，代表該簽章為簽署者對訊息M的簽章。

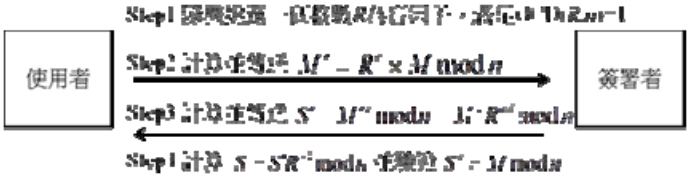

圖 1 盲簽章流程關係圖

參、多合一選舉電子投票的盲簽密機制之系統設計

隨著資訊科技快速的發展，講求是高效率及高安全的品質，如何使系統達到更快速及更安全防護，是非常重要的，而多合一選舉方式成為近年來的新趨勢，本研究提出一種植基於橢圓曲線離散對數的多重盲簽密法，可適用在多合一選舉的方案，本研究提出多張選票一次盲簽章及加密的概念，這項創新機制將縮短系統在作業處理時多餘程序進而提升執行時的效率。本系統中的盲簽密特性，可彈性選擇

要投票的張數及種類，所使用的加密機制具有雪崩效應，可增加密文破解的困難度。其次，橢圓曲線公開金鑰密碼系統在相同安全度下所使用的加密金鑰長度較其他公開金鑰密碼系統小且處理速度較快，使得橢圓曲線密碼系統具有更高的安全性。本章將針對所提方法之運作流程及系統架構進分別說明：

一、本系統整體運作流程

系統的整體運作流程如圖 2 所示。選舉人在開票中心進行註冊，再利用憑證中心把公鑰與簽章回傳，之後再透過選務中心做確認身分的動作，並且將多張選票進行一次盲化及加密，加密完以後利用私鑰做簽章，再來做一次確認身分動作，最後再由開票中心解開盲簽章，做開票動作。

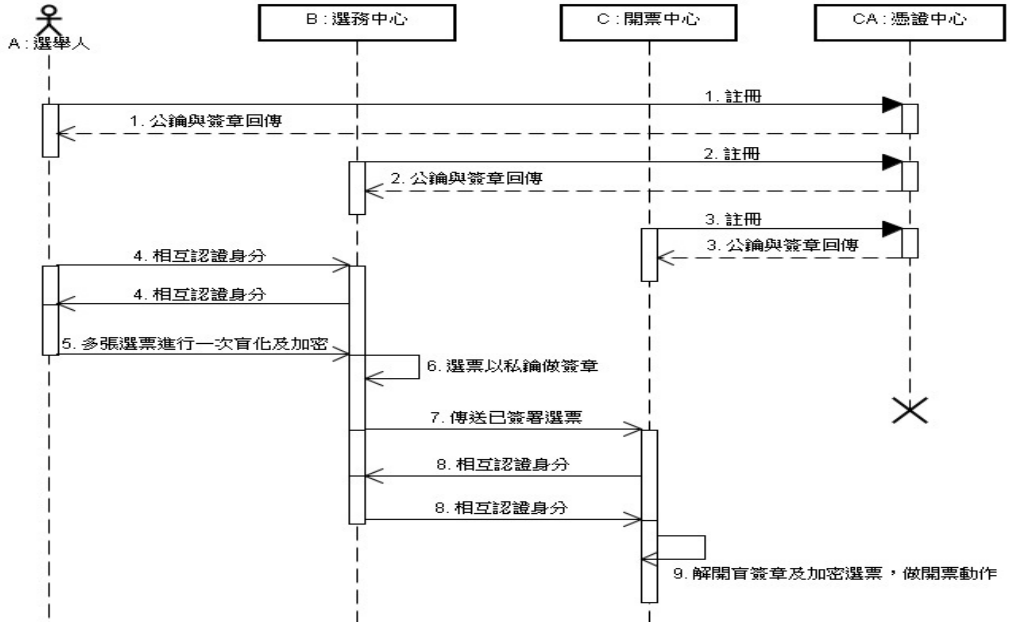

圖 2 本研究整體運作示意循序圖

二、系統架構

(一)系統參數設定

本研究採橢圓曲線演算法與 Chaum 的盲簽章機制，本系統架構可分為系統參數設定階段、系統初始階段、驗證身分階段、盲簽密階段、解盲簽密階段等五個階段，各階段分別說明如下：

系統初始時對密碼系統作一個參數設定選擇，以下針對本研究中各參數進行說明，如表 2 所示：

表 2 系統使用符號說明表

項目	符號	說明
1	$E(F_q)$	有限域 F_q 中的一條橢圓曲線
2	G	橢圓曲線中的基點
3	N	橢圓曲線上基點的秩(order)
4	q	$q > 2^{160}$ 之質數
5	id_A, id_B, id_C	選舉人 A、選務中心 B、開票中心 C 的 ID 資訊
6	PKAS, SKAS	CA 的公鑰與私鑰
7	PKA , PKB , PKC	選舉人 A、選務中心員 B 、開票中心 C 之公鑰
8	n_A, n_B, n_C	選舉人 A、選務中心 B 、開票中心 C 所選擇之私鑰
9	ca_A, ca_B, ca_C	選舉人 A、選務中心 B、開票中心 C 之憑證
10	h1( )	雜湊函數(值轉值)
11	h2( )	雜湊函數(點序列轉值)
12	fm2p( )	將訊息轉為橢圓曲線點之函數
13	fp2m( )	將橢圓曲線點轉為訊息之函數
14	w	明文之 0、1 背包值
15	b	盲因子
18	m	明文訊息
19	mi	明文之分解區塊

(二)系統初始(註冊階段)

系統在有限域 F_q 上選取一條安全的橢圓曲線 $E(F_q)$ (q 為一個 160bit 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 $NG=O$，其中 O 為此橢圓曲線之無窮遠點，令 $u \to N/\alpha$，$u \le 4$。選舉人 A、選務中心 B、開票中心 C 分別選擇 $n_A, n_B, n_C \in Z_q^*$ 當成私鑰，並計算出相應之公鑰 $PK_A = n_A \cdot G$、$PK_B = n_B \cdot G$、$PK_C = n_C \cdot G$，$PK_{AS} = n_{AS} G$，並透過一個絕對安全之通道將本身公鑰及身分 id_A, id_B, id_C 送至憑證中心計算出關聯值 $e_A = h_1(id_A, PK_A)$，$e_B = h_1(id_B, PK_B)$，$e_C = h_1(id_C, PK_C)$，並為選舉人 A、選務中心 B、開票中心 C，分別選擇 l_A, l_B, l_C，使 $Z_A = l_A G = (x_{Z_A}, y_{Z_A})$ $Z_B = l_B G = (x_{Z_B}, y_{Z_B})$，$Z_C = l_C G = (x_{Z_C}, y_{Z_C})$ 產生憑證 $ca_A = l_A(e_A + x_{Z_A} n_{AS}), ca_B = l_B(e_B + x_{Z_B} n_{AS}), ca_C = l_C(e_C + x_{Z_C} n_{AS})$，憑證中心將 ca_A, Z_A, PK_A, PK_{AS} 傳回選舉人 A，將 ca_B, Z_B, PK_B, PK_{AS} 傳回選務中心 B，將 ca_C, Z_C, PK_C, PK_{AS} 傳回開票中心 C，系統選擇的一個單向無碰撞雜湊函數 h1() 及 h2()，最後公開 $E(F_q), G, \alpha, q, PK_A, PK_B, PK_C, PK_{AS}, h_1(\,), h_2(\,)$。圖 3 為選舉人、選務中心及開票中心向憑證中心辦理註冊階段之循序圖：

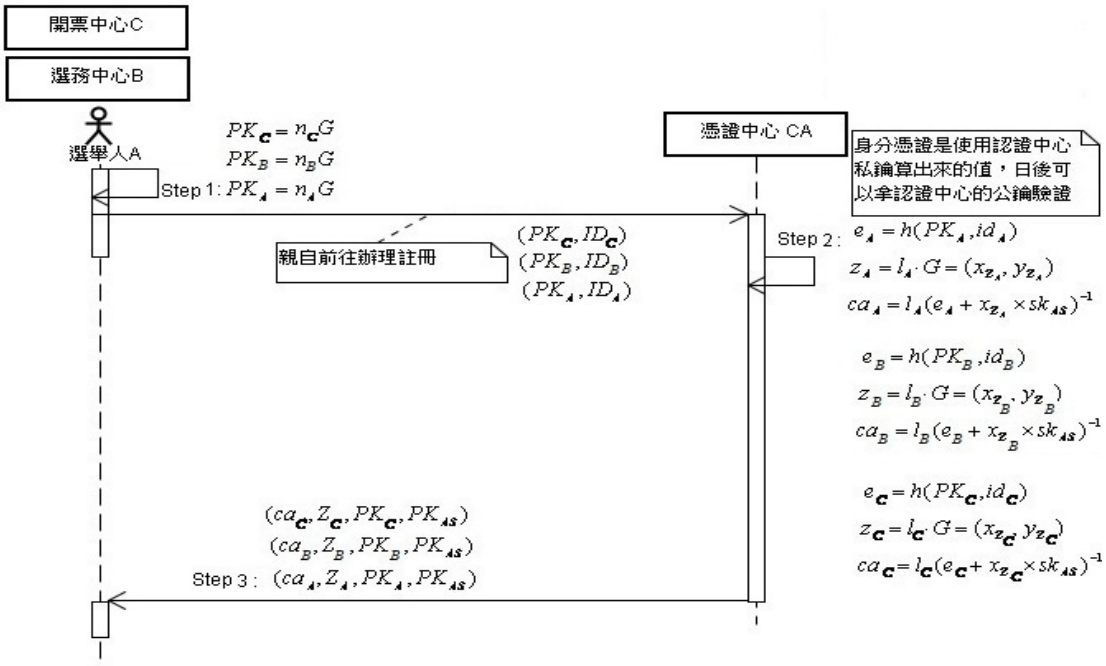

圖 3 選舉人、選務中心、開票中心辦理註冊階段循序圖

(三)選舉人與選務中心(相互驗證身分階段)

當選務中心 B 收到選舉人 A 所傳過來的 $\{ ca_A, Z_A, PK_A, PK_{AS} \}$ 之後，先行驗證身分，確認無誤後才能進行投票，計算如下：

$$u_1 = ca_A^{-1} \bmod \alpha \qquad (1)$$

$$u_2 = e_A \times u_1 \bmod \alpha \qquad (2)$$

$$u_3 = x_{Z_A} \times u_1 \bmod \alpha \qquad (3)$$

接著以憑證中心的公開金鑰來驗證身分之正確性，計算：

$$u_2 G + u_3 PK_{AS} = (v_x, v_y) \qquad (4)$$

$$\text{驗證：} \; x_{Z_A} \overset{?}{=} v_x \qquad (5)$$

雙方進行相互認證循序圖如圖 4 所示：

(2)

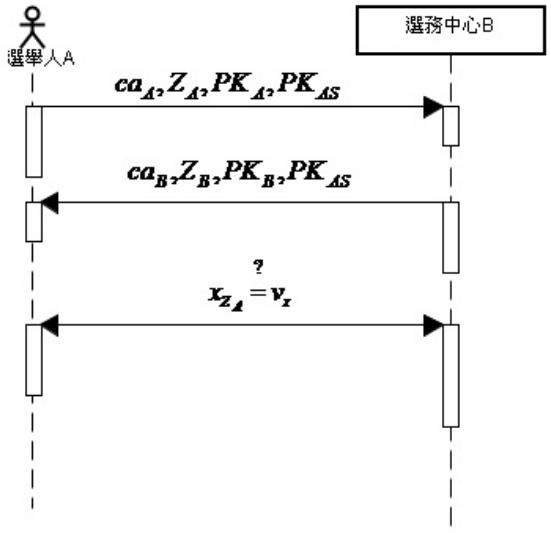

圖 4 選舉人與選務中心相互身分認證階段循序圖

(四)選舉人與選務中心(盲簽密階段)加密

(1) 選舉人 A 將多份選票明文分成數個區塊定義 $m_{ij} = m_{11}, m_{12}, ..., m_{n1}, m_{n2}$ ，$1 \le i \le n$ ，其中每份文件各切割為兩塊，並對明文 mij 實施雜湊值，利用明文轉點方式將明文轉為點座標，計算如式子(6)、(7)、(8)

$$\overline{m_{ij}} = \{m_{11}, m_{12}, ..., m_{n1}, m_{n2}\} \quad (6)$$

$$h_1(\overline{m_{ij}}) = m \quad (7)$$

$$f_{m2p}(m) = \{P_1, P_2, ..., P_n\} \quad (8)$$

(2) 定義 $\overline{x} = \{x_1, x_2, ..., x_i\} \in (0,1)$ 算出 w 如(9)，以二進位表達 w 值，假如對應 1 及右邊對應 0 則右移一個位元，對應 0 及右邊對應 1 則左移一個位元，其中每對應兩個相同數字 1 則右移三個位元，對應兩個相同數字 0 則左移三個位元。

$$\begin{aligned} &if \quad x_i = 1 \ ; \ x_{i+1} = 0 >> 1 \\ &\qquad x_i = 0 \ ; \ x_{i+1} = 1 << 1 \\ &if \quad x_i = 1 \ ; \ x_{i+1} = 1 >> 3 \\ &\qquad x_i = 0 \ ; \ x_{i+1} = 0 << 3 \end{aligned} \quad (7)(8)$$

$$w = \{x_1 2^{i-1}, x_2 2^{i-2}, ..., x_i 2^0\} \in (0,1) \quad (9)$$

(3) 加密運算，利用明文轉點的方式 fm2p(w,m)將 w 值以十進位表示轉成點座標 Pi，實施加密的動作，Ci 為加密後的訊息選票如式(10)(11)(12)

$$C_0 = [f_{m2p}(w,m) + n_A n_C G] \quad (10)$$

$$C_1 = [P_1 + x_1 C_0 + n_A n_C G]$$

$$C_2 = [P_2 + x_2 C_1 + n_A n_C G]$$

.

.

$$C_n = [P_i + x_i C_{i-1} + n_A n_C G]，2 \le i \quad (11)$$

$$\overline{C_i} = \{C_0, C_1, C_2, ..., C_n\} \quad (12)$$

$$h_2(\overline{C_i}) = M \quad (13)$$

- **盲化**

定義 $\overline{a} = \{a_1, a_2, ..., a_j\} \in (0,1)$ 算出 θ 如式子(14)， $j \ge n$ ，j 為總共有的選票張數，n 為只投了幾張選票，接著選舉人 A 以隨選盲因子 b 及參數 θ 與開票中心 C 的公開金鑰 nCG 算出 K 如式子(15)，目的是讓選務中心 B 在簽章過程中無法清楚知道選舉人 A 共投了多少張選票，但只有開票中心 C 才能解開知道。其次，將傳送過來的已加密訊息 M 進行盲化動作，選舉人 A 以隨選盲因子 b，及開票中心 C 的公鑰 nCG 進行盲化運算如式子(16)，之後將 $\{\overline{C_i}, K, B'\}$ 傳送給選務中心 B。

$$\theta = \{a_1 2^{j-1}, a_2 2^{j-2}, ... a_j 2^0\} \quad (14)$$

$$K = [f_{m2p}(b,\theta) + n_A n_C G] \quad (15)$$

$$B' = b \cdot M \cdot n_C G \quad (16)$$

- **簽章**

選務中心 B 收到選舉人 A 所傳送過來的 $\{\overline{C_i}, K, B'\}$ 後，選務中心 B 使用自己的私鑰 nB 對已盲化的訊息 B’執行簽章作業，以證明此選票為合法有效票，之後將盲簽密資訊 $\{\overline{C_i}, K, s_B'\}$ 傳送給開票中心 C，計算如下：

$$sB' = n_B \cdot B' \quad (17)$$

盲簽密階段循序圖如圖 5 所示：

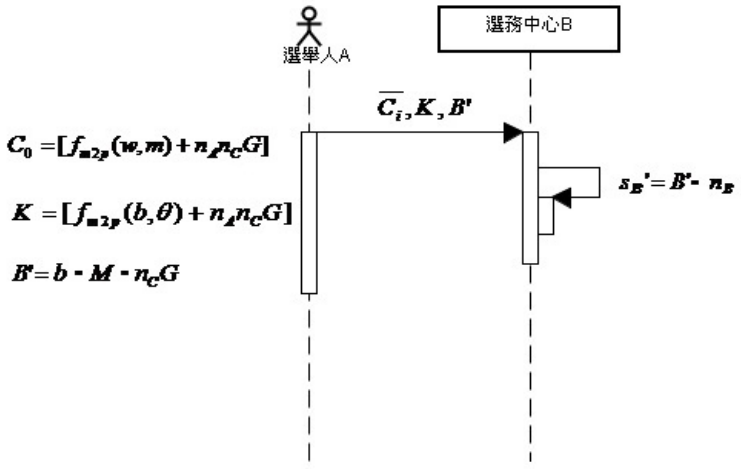

圖 5 選舉人與選務中心盲簽密階段循序圖

(五)選務中心與開票中心 (相互驗證身分階段)

解開選票前，開票中心 C 要先和選務中心 B 做一個驗證身分的動作，所以當開票中心 C 收到選務中心 B 所傳過來的 $\{ ca_B, Z_B, PK_B, PK_{AS} \}$ 後，先驗證身分，確認無誤後才能解開選票，計算如下：

$$u_1 = ca_B^{-1} \bmod \alpha \tag{18}$$

$$u_2 = e_B \times u_1 \bmod \alpha \tag{19}$$

$$u_3 = x_{Z_B} \times u_1 \bmod \alpha \tag{20}$$

接著以憑證中心的公開金鑰來驗證身分之正確性，計算：

$$u_2 G + u_3 PK_{AS} = (v_x, v_y) \tag{21}$$

驗證： $x_{Z_B} \overset{?}{=} v_x$ (27)

雙方進行相互認證循序圖如圖 6 所示：

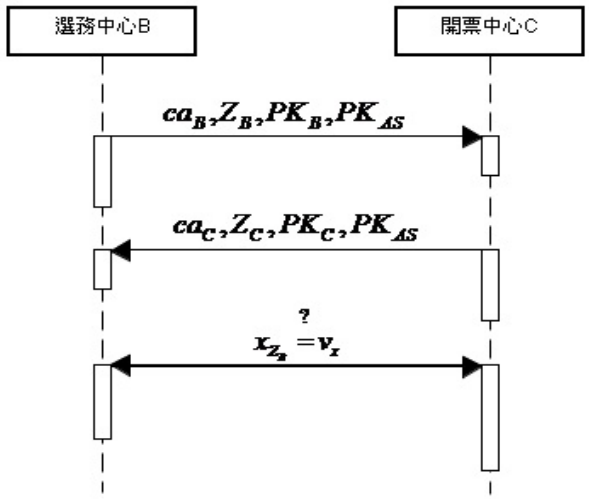

圖 6 選務中心與開票中心相互身分認證階段循序圖

(六)開票中心(解盲簽密階段)

- **解盲化**

以選務中心 B 所傳送過來的 $\{\overline{C_i}, K, s_B'\}$ 進行解盲簽密程序，開票中心 C 以自已的私密金鑰 nc 與選舉人的公開金鑰 nAG 進行解盲動作，之後對選票做一個簽章驗證動作，驗證簽章是否是選務人員 B 所簽署的，計算如下：

$$s_B' = b \cdot M \cdot n_B n_C G \quad (23)$$

$$h_2(\overline{C_i}) = M' \quad (24)$$

$$f_{m2p}(b,\theta) = K - n_A n_C G \quad (25)$$

$$(b,\theta) = f_{p2m}[f_{m2p}(b,\theta)] \quad (26)$$

$$s_B = b \cdot M' \cdot n_B n_C G \quad (28)$$

$$s_B \overset{?}{=} s_B' \quad (29)$$

- **解密**

(1) 接著將簽章過的加密選票進行解密動作，計算如下：

$$f_{m2p}(w,m) = C_0 - n_A n_C G \quad (30)$$

$$(w,m) = f_{p2m}[f_{m2p}(w,m)] \quad (31)$$

(2) 將 w 還原成 $\overline{x}$ 數列，將其二進位表示的 w 值，假如對應 1 及右邊對應 0 則左移一個位元，對應 0 及右邊對應 1 則右移

一個位元，其中每對應兩個相同數字 1 則左移三個位元，對應兩個相同數字 0 則右移三個位元，還原方式如式(31)：

$$if \quad x_i = 1 \ ; \ x_{i+1} = 0 << 1$$

$$x_i = 0 \ ; \ x_{i+1} = 1 >> 1$$

$$if \quad x_i = 1 \ ; \ x_{i+1} = 1 << 3$$

$$x_i = 0 \ ; \ x_{i+1} = 0 >> 3$$

$$w = \bar{x} = \{x_1 x_2 ... x_i\} \quad (32)$$

(3) 依序解開 $\overline{C}$ 可以取得 $\overline{P_i'}$ = { P1',P2',….,Pn'} 進行點序列 $\overline{P_i'}$ 解密，執行點轉成明文的動作，如式(32) - (35)，計算如下：

$$P_1' = C_1 - x_1 \cdot C_0 = n_A n_C G \quad (33)$$

$$\vdots$$

$$P_i' = C_i - x_i \cdot C_{i-1} = n_A n_C G \quad (34)$$

(4) 還原明文動作，將所有點資訊還原成訊息區塊，再將所有的訊息區塊組合成明文，計算如式(34)、(35)

$$\overline{P_i'} = \{P_1', P_2', ..., P_n'\} \quad (35)$$

$$f_{p2m}(\overline{P_i'}) = \overline{m_i'} \quad (36)$$

(5) $\overline{m_i'}$ 為解密後所得到的多重訊息選票集合，再將多重訊息選票集合實施一次雜湊如式(36)

$$h_1(\overline{m_i'}) = m' \quad (37)$$

驗證此選票的正確性，開票中心 C 計算如下：

$$m' \stackrel{?}{=} m \quad (38)$$

等式成立則收方所收之訊息選票正確無誤。解盲簽密階段循序圖如圖 7 所示：

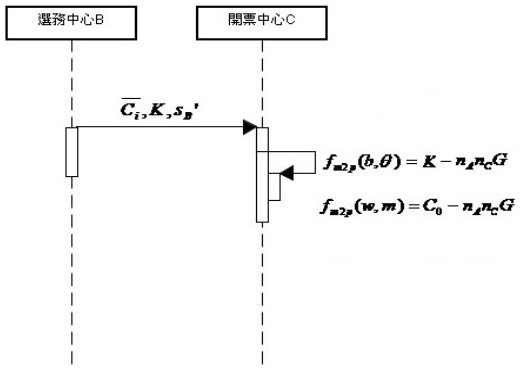

圖 7 開票中心解盲簽密階段循序圖

肆、安全性及效益分析

本章將針對所提方法之安全性及效益分析進行探討：

4.1 安全性分析

本研究所提盲簽密機制，其安全性植

基於橢圓曲線離散對數問題，將針對完整性、鑑別性、不可否認性、隱匿性、機密性、不可追蹤性、不可偽造性等安全需求進行探討：

- **完整性**

完整性是指選票在傳遞過程中不能被破壞或干擾，意旨在過程中不能被任意地加入、刪除或修改。在本方法式子(7)中 $h_1(\overline{m_{ij}}) = m$ 對明文進行雜湊運算得 m，並將 m 加入 $C_0 = [f_{m2p}(w,m) + n_A n_C G]$ (10) 中，若第三方想要竄改明文偽造 m 而不被發現，則必須對面破解單向雜湊函數的問題及面對橢圓曲線離散對數問題，使得本系統可以得到完整性的確保。

- **鑑別性**

公開金鑰密碼系統中，使用者的公鑰與密鑰有唯一的對應關係，只有使用者的密鑰才能對應使用者的公鑰，因此藉由金鑰對可達到鑑別使用者身分的功能。在簽章產生時必須使用簽署者的密鑰，驗證則要簽署者的公鑰，才能驗證該簽章的有效性。本方法如式子 $s_B' = b \cdot M \cdot n_B n_C G$ (23)

$h_2(\overline{C_i'}) = M'$ (24) $s_B = b \cdot M' \cdot n_B n_C G$

(27) $s_B \overset{?}{=} s_B'$ (28)，如果驗證者利用公鑰驗證所收到簽章為有效時，則表示此簽章與選票的確是由具有該公鑰的選務中心所簽署的。

- **不可否認性**

不可否認性指的是對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。在金鑰管理方面，使用者皆必須經過憑證中心 CA 的檢驗認證之後，就可獲取自已的公鑰和私鑰來進行加解密動作。所以本研究中之選舉人 A、選務人員 B、開票中心 C 在資料傳遞前，必定先進行使用者身份認證，以達到不可否認性。而本系統中如式子(17) $s_B' = B' \cdot n_B$，選務中心將選票簽署後以證明此選票為合法有效票，可防止選務中心是後否認經由他簽署的。

- **隱匿性**

簽署人對簽署的"選票內容"無法獲知該內容的訊息，本方法如式子(16) $B = b \cdot M \cdot n_C G$ 中有此功能，不必擔憂選務中心在簽章過程中知道選舉人所圈選的資料而所造成選票曝光。

- **機密性**

機密性指的是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，訊息(選票)在成功地送達目的地之後，所有的訊息(選票)交換都是保密的。本方法中的式子(9) $w=\{x_1 2^{i-1}, x_2 2^{i-2}, ... x_i 2^0\} \in (0,1)$，w 是隨機產生，假如對應 1 及右邊對應 0 則右移一個位元，對應 0 及右邊對應 1 則左移一個位元，其中每對應兩個相同數字 1 則右移三個位元，對應兩個相同數字 0 則左移三個位元，可達成加密區塊擬亂的效果，使得加密過後的密文選票具有雪崩效應，即便中途遭到第三方部分截獲，也無法求得任何資訊，可使本系統達到更安全的機密性，若攻擊者欲破解，則須面臨破解單向雜湊函數與橢圓曲線離散對數之難題。

- **不可追蹤性**

本系統中如式子(15)、(16) $K=[f_{m2p}(b,\theta)+n_A n_C G]$ ， $B'=b \cdot M \cdot n_C G$ ，經過加盲的訊息選票，簽章者無法知道選舉人共投了幾張選票及無法得知真正的選票內容，因為盲因子「b」是隨機的，簽章者僅知道這些資訊是經由自己簽署過的，此時選舉人與選票脫離了的關係(unlinkability)，使得簽章者無法追蹤出選舉人是誰，達到匿名的效果。

- **不可偽造性**

本方法中式子(13) $h_2(\overline{C_i}) = M$ ，由於 hash 單向雜湊函數有無法逆推的特性，無法正確的求得資訊或中途遭受第三方所偽造的可能，所以在 hash 的保護下，偽造有效選票是困難的。

4.2 效益分析

在分析前先定義各種運算符號及各種運算時的相互關係如表 3，而模數加法、模數減法運算時間低，予以忽略不計。參酌文獻(蘇品長，民 97 年)所提的各項運算量，表 4 及表 5 是植基於各系統 Blind signatures 之分析比較表，在表 4 中驗證階段本方法有使用到兩次驗證相對的在安全性上會比較嚴謹，所以所花的時間會比較多，利用表 4 的金鑰產生、盲化、簽章、解盲、驗證(取一次)的整體運算加總，以表 5 中的數量分析比較出本研究方法優於其他系統。

表 3 時間複雜度運算之相互關係參考表

符號	定義	相互關係
T_{MUL}	進行一次模式乘法運算所需時間	$= T_{MUL}$
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)
T_{INVS}	進行一次模式乘法反元素所需時間	$\approx 240\ T_{MUL}$
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	$\approx 0.12\ T_{MUL}$
T_h	進行一次點 hash 所需時間	$\approx 23\ T_{MUL}$
t_h	進行一次 hash 所需時間	$\approx 1T_{MUL}$

表 4 本研究與植基於各系統 Blind signatures 之時間複雜度比較表

演算法	RSA-Based Blind signatures (Chaum，1982)		ElGamal -Based Blind signatures (Jena，2007)		ECDLP-Based Blind signatures (Mohammed，2000)		本研究方法	
比較項目	時間複雜度	概估	時間複雜度	概估	時間複雜度	概估	時間複雜度	概估
金鑰產生	$2T_{MUL}+1T_{INVS}$	$\approx 242\ T_{MUL}$	$1T_{EXP}$	$\approx 240\ T_{MUL}$	$3T_{ECMUL}$	$\approx 87\ T_{MUL}$	$4T_{ECMUL}$	$\approx 116\ T_{MUL}$
加密運算	無	無	無	無	無	無	$5T_{ECMUL}+3T_{ECADD}+1t_h+1T_h$	$\approx 169.36\ T_{MUL}$
盲化運算	$1T_{EXP}+1T_{MUL}$	$\approx 241\ T_{MUL}$	$1T_{EXP}+1T_{MUL}$	$\approx 241\ T_{MUL}$	$+2T_{INVS}+6T_{MUL}$	$\approx 486\ T_{MUL}$	$4T_{ECMUL}+1T_{ECADD}$	$\approx 116.12\ T_{MUL}$
簽章運算	$1T_{EXP}$	$\approx 240\ T_{MUL}$	$2T_{MUL}+1T_{INVS}$	$\approx 242\ T_{MUL}$	$6T_{MUL}$	$\approx 6T_{MUL}$	$1T_{ECMUL}$	$\approx 29T_{MUL}$
解盲運算	$1T_{INVS}$	$\approx 240\ T_{MUL}$	$4T_{MUL}+3T_{INVS}$	$\approx 724\ T_{MUL}$	$+5T_{MUL}+2T_{ECADD}+1T_{INVS}$	$\approx 485.24\ T_{MUL}$	$10T_{ECMUL}+1T_h$	$\approx 313\ T_{MUL}$
解密運算	無	無	無	無	無	無	$5T_{ECMUL}+1t_h$	$\approx 146\ T_{MUL}$
驗證運算	$1T_{EXP}$	$\approx 240\ T_{MUL}$	$2T_{EXP}+1\ T_{MUL}$	$\approx 481\ T_{MUL}$	$2T_{ECMUL}+1T_{ECADD}$	$\approx 58.12\ T_{MUL}$	$8T_{ECMUL}+2T_{ECADD}+2T_{INVS}$	$\approx 712.24\ T_{MUL}$

表 5 本研究與植基於各系統 Blind signatures 之數量分析比較表

演算法 數量(份)	RSA-Based Blind signatures	ElGamal-Based Blind signatures	ECDLP-Based Blind signatures	本研究方法
1	$1203\,T_{MUL}$	$1928\,T_{MUL}$	$882.36\,T_{MUL}$	$930.24\,T_{MUL}$
2	$2406\,T_{MUL}$	$3856\,T_{MUL}$	$1764.72\,T_{MUL}$	$959.48\,T_{MUL}$
3	$3609\,T_{MUL}$	$5784\,T_{MUL}$	$2647.08\,T_{MUL}$	$988.72\,T_{MUL}$
4	$4812\,T_{MUL}$	$7712\,T_{MUL}$	$3529.44\,T_{MUL}$	$1017.96\,T_{MUL}$
5	$6015\,T_{MUL}$	$9640\,T_{MUL}$	$4411.8\,T_{MUL}$	$1047.2\,T_{MUL}$

伍、結論

一張選票做一次盲簽章及加密，如果以多合一的選舉方案來進行投票，每人就有多張選票而每張選票也都做一次的盲簽章及加密，數以萬人就有數以萬張選票，在時間複雜度計算量會耗費許多。本研究提出了多重盲簽密法適用在多合一選舉的電子投票機制。利用橢圓曲線密碼系統所具有金鑰長度較短與計算複雜度較低的特性，在執行效率上比現行 RSA 及 ElGamal 演算法來的好，且選票在運行過程中需透過選務人員來簽署選票，證明此選票為合法有效票，選票中所圈選之候選人是不能被選務人員所知道。本研究導入盲簽章及加密機制，滿足完整性、鑑別性、不可否認性、隱匿性、機密性、不可追蹤性及不可偽造性等安全需求，有別於以往學者以一次一張選票的盲簽章觀念，縮短了處理流程並提升執行效率，另強化加密設計使得選票在網路傳輸過程中更加安全。

參考文獻

1. 肖攸安，「橢圓曲線密碼體系研究」，華中科技大學出版，武漢，民國 95 年。
2. 蘇品長，「植基於 LSK 和 ECC 技術之公開金鑰密碼系統」，博士論文，長庚大學電機工程系，民國 96 年。
3. 蘇品長，"適用於 Ad Hoc 網路之快速交換金鑰機制設計", 中正嶺學報，第 37 卷第 1 期，民國 97 年，頁 219-228。

4. 今日新聞網，http://www.nownews.com/2010/03/23/301-2583410.htm，2010。
5. Chang, C.C., Lee, J.S., "An anonymous voting mechanism based on the key exchange protocol," Computers & Security, 25 (4), 2006, pp. 307-314
6. Chaum, D. "Blind signatures for untraceable payments," In Proceedings of Advances in Cryptology—CRYPTO , Plenum Press, 1982, pp. 199-203.
7. Delaune,S., Kremer, S., Ryan, M., "Coercion-resistance and receipt-freeness in electronic voting, " 19th Computer Security Foundations Workshop (CSFW), IEEE Comp. Soc. Press, 2006.
8. Fan, C.I., Sun, W.Z. , "An efficient multi-receipt mechanism for uncoercible anonymous electronic voting," Mathematical Modeling of Voting Systems andElections: Theoryand Applications, Mathematical and Computer Modelling (Special issue), 48 (9-10), 2008, pp. 1611-1627.
9. Jena, D., Jena, S.K., and Majhi, B., "A Novel Untraceable Blind Signature Based on Elliptic Curve Discrete Logarithm Problem," International Journal of Computer Science and Network Security, 7(6), 2007
10. Koblitz, N., "Elliptic Curve Cryptosystems," Mathematics of Computation American Mathematical Society, 48, 1987, pp. 203-209.
11. Liaw, H.T. , "A secure electronic voting protocol for general elections," Computers & Security, 23 (2), 2004, pp. 107-119.
12. Miller, V.S. "Use of Elliptic Curve in Cryptography," Advance in Cryptography-Crypto, New York: Spring-Verlag, 1985, pp. 417-426.
13. Mohammed, E., Emarah, A.E., and K.E. Shennawy, "A blind signatures scheme based on ElGamal signature," 17th National Radio Science Conference, 25, 2000.
14. Zheng, Y., and Imai, H., "How to construct Efficient Signcryption Schemes on Elliptic Curves," Information Processing Letters, 68, 1998, pp. 227-233.

作者簡介:

 蘇品長：長庚大學電機工程博士班畢業，現任於國防大學資訊管理學系助理教授。研究領域：國防安全及應用、資訊安全、應用密碼學、軟體工程、資訊系統管理。

 楊倫青：國防大學資訊管理學系碩士班第14期畢業。

 王博彥：中華大學資訊管理學系畢業，現為國防大學資訊管理學系第16期研究生。