Journal of e-Business
第十九卷　第一期　2017 年 6 月（pp.29～50）

新型態之電子投票機制設計

蘇品長 *　葉昱宗
國防大學資訊管理學系

摘要

網際網路的普及，改變了傳統的生活方式與行為模式，便利的同時也帶出了許多網路安全的課題。以應用於電子投票為例，已有許多國家致力於在電子投票發展，以降低傳統選舉所耗費之社會資源。安全評估一直是無法滿足的議題，因此，如何達到更具有效率且安全的防護設計，同時擁有代理的即時性與合乎匿名投票原則的機制為研究重點。本研究以植基於橢圓曲線密碼系統的快速運算為基礎，利用代理盲簽章的盲化特性與代理特性，提出多份電子選票執行一次簽密的方法，可增加密文破解難度，提升整體運算過程中的效率及安全的防護，此新型態設計更適用於未來多合一選舉之電子化投票機制參考。

關鍵詞：電子投票、代理盲簽章、多文件簽密法

New E-Voting Mechanism Design

Pin-Chang Su*　Yui-Chong Yeh
Department of Information Management, National Defense University

Abstract

The popularity of Internet has altered the traditional way of life and behavioral patterns. Indeed, while the Internet has brought great convenience, it has also highlighted numerous issues for network security. Many countries are committed to the development of e-voting, which would help societies reduce the amount of resources allocated for traditional elections. However, most literatures exploring the signature mechanisms of electronic elections only address research and technology pertaining to the single voting scheme and single blind signature mechanism. Further, these electoral processes typically exploit only blind signature rather than encryption. This research focuses on the implementation of the Elliptic Curve Cryptosystem and its capacity to generate

* 通訊作者　電子郵件：spc.cg@msa.hinet.net
DOI:10.6188/JEB.2017.19(1).02

computations rapidly as its foundation. The properties of blind signature and proxy signature in proxy blind signature are engaged to facilitate the signcyrption of multiple ballots simultaneously. It further harnessed the avalanche effect in the design of encryption to increase the difficulty of deciphering ciphertext. In all, these designs, which enhance the overall efficiency and security of the e-voting system, would be applicable to an e-voting mechanism that features multiple and varied polls in the future.

Keywords: E-voting, proxy blind signature, multi-document signcryption.

1. 緒論

隨著網際網路的蓬勃發展，資訊流通速度更加的便利與快速，擴大企業間的獲利商機，第三方支付、網路購物、電子投票（E-voting）等新興的應用模式在此背景的推波助瀾下迅速融入生活中，企業亦賺進為數可觀的全球財。然而，網際網路所帶來的便利性，卻也夾雜著安全的疑慮，如何確保資料在網路上傳輸是安全無虞，並達到來源的證明及不可否認性，值得深思及討論。許多國家已在網路普及化下推動電子投票，愛沙尼亞更曾於 2007 年舉行世界首次國會電子投票選舉。然而，探討電子投票過程中，如何確保選票安全，有效隱藏投票者票券內容，避免有心人士逆推得知票與投票者關係，本研究將針對數位簽章之代理盲簽章技術實施探討，以達到隱藏投票者所傳遞的選票內容以及保證簽署的及時性。

針對應用於電子投票及行動商務的簽章（Signature）及加密（Encryption）技術，有許多的文獻探討及研究，首先 Chaum（1982）提出盲簽章（Blind signature）的觀念，盲簽章要求簽章者在不知道待簽文件內容的前提下對文件進行簽名；Mambo et al.（1996）提出代理簽章（Proxy signature）概念，主要是指原始簽章者視情況需要將自己的簽名權授給代理人，由代理人代表原始簽章者實施簽署；Lin and Jan（2000）結合盲簽章與代理簽章各自的優點提出代理盲簽章（Proxy blind signature）架構，隨後 Tan et al.（2002）提出植基於離散對數難題（Discrete logarithm problem, DLP）及橢圓曲線離散對數難題（Elliptic curve discrete logarithm problem, ECDLP）下之代理盲簽章，Lal and Awasthi（2003）指出 Tan et al.（2002）架構可能承受簽章接收者偽冒攻擊，Sun et al.（2005）則提出 Tan et al.（2002）架構無法滿足不可偽造性與不可鏈結性等特性，並指出 Lal and Awasthi（2003）亦無法滿足不可鏈結性特性，惟 Sun et al.（2005）並未提出解決之道。Zhang et al.（2003）提出基於雙線

性曲線對數（Bilinear pairings）之代理盲簽章、Fan et al.（2012）提出基於前推安全（Forward secrecy）之代理盲簽章、Wang et al.（2005）則提出基於 ECDLP 之代理盲簽章，隨後 Yang et al.（2008）證明上述方法無法滿足強不可否認、強不可偽造性和不可鏈結性，並提出改善。而 Hu et al.（2009）指出 Yang et al.（2008）仍存在原始簽章者偽冒及通用偽冒等弱點，進而提出基於 ECDLP 改進式代理盲簽章；Pradhan and Mohapatra（2011）和 Alghazzawi et al.（2011）相繼提出植基於 ECDLP 之新代理盲簽章，隨後，Wang and Liao（2014）攻擊 Pradhan and Mohapatra（2011）和 Alghazzawi et al.（2011）均無法達成不可鏈結性，進而提出強化結構之 ECDLP 演算法；針對代理盲簽章方法，另有文獻曾提出多重簽章（Lu et al., 2005; 蘇品長等人，2014）方法，同樣存在無法滿足強不可鏈結性等問題；此外，Tian et al.（2013）提出植基於量子密碼學的簽章演算法，雖然量子技術具更快速及安全之特性，惟量子密碼技術尚屬實驗階段，要走向實用，必須結合一些其他技術，如：保密增強、糾錯及認證技術等，阻礙量子密碼術走向實用。另一個很重要的非技術問題則是經濟因素，因為量子金鑰分配技術需投資高成本的設備及設備相容性問題，且無實際應用案例，無法投入市場競爭；此外，在長距離傳輸及量子密碼的金鑰分配技術均劣於傳統的方法（曾貴華，2010），故本研究未導入量子技術。

Zheng（1997）提出簽密（Signcryption）概念，主要是指在一個邏輯步驟內同時完成訊息的簽名及加密，其計算量低於傳統的先簽名後加密方式，儘管仍有學者質疑其並非同一步驟內完成，而進一步提出鑑別加密法（Authenticated encryption）（許建隆、吳宗成，1999），宣稱可以真正同時簽章和加密的方法，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。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，覃海生等人（2013）提出植基於 DLP 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 DLP 特性，並非最佳的方法。

隨著學者們不斷改進，期許透過網際網路完成電子投票，滿足電子投票的最大特性與最小限制（Delaune et al., 2006），如何達到更具有效率且安全的防護設計，同時擁有代理的即時性與合乎匿名投票原則的機制，啟發研究動機。傳統電子投票可區分為混合型、同態理貨和盲簽章等投票模式；安全評估一直是無法滿足的議題，因此，如何達到更具有效率且安全的防護設計，同時擁有代理的即時性與合乎匿名投票

原則的機制是研究重點。本研究提出新型態之電子投票機制，多份電子選票執行一次簽密的方法（如將電子選票改為多個 Boolean 值或數字，亦可成為單一文件的選票處理），具高彈性設計，滿足不同選區不同選票、不同選區混合相同選票和不同選票、不同選票的特殊需求（加載資料等）、選票存取控管彈性及與實務上的選票分類保管等選務工作運作流程。本論文將針對先前文獻所提機制加以補強並改善先前文獻僅考慮單一投票機制且選票機密性設計之不足，透過擬亂設計及雪崩效應增加系統安全，同時利用代理盲簽章來補足原機制實用性不足之缺點，提出更適用的電子化投票機制。

2. 文獻探討

本研究相關電子投票的發展及代理盲簽章、簽密法的演算說明，分述如後。

2.1 電子投票

邁向民主道路的根本機制就是選舉，在過去十來年，選舉程序引起全世界的極大關注，許多國家無論貧富和發達與否，都在利用新技術與方法來選出領導人。儘管，仍有專家學者認為電子投票存在某些安全上的疑慮，然而，綜觀過去，各國無不努力朝向這個趨勢發展。表 1 即為傳統投票與電子投票之比較表（丘昌泰，2004）。過去幾十年來，安全的電子投票設計已吸引資訊安全學者的注意，最廣為探討的電子投票安全技術可區分為三類，分別為混合型的投票（Mix-type voting）、同態理貨（Homomorphic tallying）和盲簽章，然而，混合型及同態理貨等機制需牽涉複雜的零知識證明（Zero-knowledge proof），以提供完整性和公開驗證。除此之外，Homomorphic tallying 用來證明所花費的成本，已大大限制並說明其僅能用於小規模地方選舉（Mateu et al., 2014）。因此，本研究提出新型態之電子投票機制，以盲簽章方法為主，利用代理盲簽章來補足原盲簽章機制之實用性不足；同時以代理簽章改善盲簽章之實用性的缺點，探討應用於電子投票之可能。

▼ 表 1　傳統投票與電子投票比較表

構面	傳統投票	電子投票
身分確認	持身分證至所屬選區，核對選舉人名冊，蓋章領取選票。	至任意投票所核對名冊，再與卡片進行認證即可領取電子投票卡。
投票方法	於選票上印上記號，若蓋錯位置或有汙損，即無法塗改，形成廢票。	採用觸碰式螢幕等電子儀器，在未作最後確認前，都還能進行修改。

構面	傳統投票	電子投票
秘密投票	可從投票蓋章位置判斷，妨礙秘密原則，且視覺障礙及行動不便者，可代理投票，有違秘密投票原則。	電子投票卡不會留下任何記錄，且採用觸碰式螢幕搭配語音，視障或行動不便者，也可獨立完成投票。
開票程序	開票程序除唱票、計票、確認無效票，還需統計，常發生誤判爭議。	完全不需要唱票、計票、與確認無效票，可交由電腦中心統一處理。
票數統計	可能不準確；可能因計票、書寫而導致票數錯誤。	完全交由電子投票機器處理，完全正確，較無失誤可能。
選票保存	太佔空間，無法永久保存。	不受空間影響，可永久保存。

2.2　代理盲簽章

代理盲簽章其概念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，代理簽章者即可對簽署文件實施盲簽章，也就視同原始簽章者對該文件簽署的認可。完整之代理盲簽章架構應滿足鑑別性、不可偽造性、不可否認性、可驗證性、可識別性、防止不當使用等特性（Pradhan and Mohapatra, 2011），Wang and Liao（2014）提出強化結構基於橢圓曲線離散對數之代理盲簽章，補足先前學者無法達成之不可鏈結性，系統概分三階段，演算法步驟如下：

(1) 代理委託階段：簽章者隨選擇 $k_0(1<k_0<n)$，計算 $R_0=k_0\cdot P=(x_1, y_1)$，$r_0=x_1 \ modn$，$s_0=x_0+k_0H\ (m_w||r_0)modn$，並傳送 (R_0, s_0, m_w) 給代理簽章者。當代理簽章者收到後驗證 $s_0\cdot P=R_0\cdot H(m_w||r_0)+y_0$，若成立，則計算 $S_{pr}=x_p+s_0\ modn$ 作為代理簽署私鑰，$Y_{pr}=y_0+y_p+R_0\cdot H(m_w||r_0)=P\cdot S_{pr}$。

(2) 簽署階段：代理簽章者選擇 $k_p(1<k_p<n)$，計算 $R_p=k_p\cdot P=(x_2, y_2)$，$r_p=x_2 \ modn$，再將 (R_0, R_p, m_w) 傳給訊息擁有者。隨後，訊息擁有者隨選盲因子 a, b, c，計算 $R=a\times R_p+c\cdot P-b\cdot Y_{pr}$，若 R 為 0 則重新選擇，$e=h(R||m)mode$，$e^*=a^{-1}(e-b)modn$，並將 e^* 轉回。代理簽章者接收後，計算 $s"=e^*S_{pr}+k_p \ modn$ 回傳給訊息擁有者。當訊息擁有者收到 $s"$，解盲化計算計算 $s=as" + c \ modn$。最後，簽章文件為 (m, m_w, r_0, e, s)。

(3) 驗證階段：驗證者 $e=?h((s\cdot P-e\cdot Y_{pr})||m)$。

2.3　簽密法

簽密法為公開金鑰密碼學中新的應用，以許建隆、吳宗成（1999）所提的方法為例，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) 簽密階段：使用者 U_A 選擇一個隨機參數值為 $k \rightarrow Z_q^*$，使用者 U_A 利用使

用者 U_B 的公鑰 y_b 設計加密演算法 $E=(y_b^k \bmod p) \bmod q$。利用私鑰 x_a 產生與訊息 m 結合，產生簽章 (r, s)；$r=m \cdot E \bmod p$；$s=k-x_a \cdot r \bmod q$，接著計算 $E=(y_b^s \cdot y_{ab}^r \bmod p) \bmod q$；其中 $y_{ab}=g^{x_a \cdot x_b} \bmod p$。

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

(3) 驗證階段：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。

3. 研究方法

本研究提出的改良 Wang and Liao（2014）的方法並導入多文件簽密機制，將縮短系統在作業處理時多餘程序進而提升執行時效率，本章將分別說明運作流程、系統架構及系統模擬。

3.1 系統流程及符號說明

系統設計之演算法共分成四個階段，初始註冊階段、代理階段、盲簽密階段、驗證階段；本方法所使用的符號詳如表 2。

▼ 表 2 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	$q > 2^{224}$ 之質數
5	Y_a, Y_o, Y_p, Y_c	投票者 A、管理中心 O、投票所 P、開票中心 C 之公鑰
6	x_a, x_o, x_p, x_c	投票者 A、管理中心 O、投票所 P、開票中心 C 之私鑰
7	$h_1( )$	將授權書與原始簽章者公鑰 x 軸轉換成值的雜湊函數
8	$h_2( )$	將明文序列 $\bar{v}$ 轉換成值的雜湊函數
9	$h_3( )$	將密文點序列 $\bar{C}$ 轉換成密文摘要的雜湊函數
10	$h_4( )$	盲化值與密文摘要轉換成值的雜湊函數
11	$f_{m2p}( )$	將訊息轉為橢圓曲線點之函數
12	$f_{p2m}( )$	將橢圓曲線點轉為訊息之函數
13	*	位移運算
14	V	明文選票

項目	符號	說明
15	C	密文選票
16	w	明文之 0、1 背包值
17	t	明文序列雜湊值
18	m	密文摘要
19	m_w	委託授權書
20	k	投票者 A 的隨選值

3.2　多文件代理盲簽密機制設計

3.2.1　初始註冊階段

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），表示式為 $y^2=x^3+ax+b(\text{mod } q)$ 且 $4a^3+27b^2\neq 0$，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，系統公開 $E(F_q)$、G、n 等選定參數。

投票者 A、選票管理中心 O、投票所 P、開票中心 C 分別選擇 $x_a, x_o, x_p, x_c \in Z_n^*$ 當成私鑰，並計算出相應之公鑰 Y_a, Y_o, Y_p, Y_c。

投票者 A、投票所 P、開票中心 C 向管理中心 O 完成註冊並取得認證。

3.2.2　代理委託階段

選票管理中心 O 隨選一個值 $k_0(1<k_0<n)$，計算其公鑰 R_0 及 x 軸座標值，如式 (1)、(2)。並計算委託書相關參數如式 (3)，並將 (R_0, s_0, m_w) 傳送給投票所 P。

$$R_0=k_0\cdot G=(x_1, y_1) \tag{1}$$

$$r_0=x_1 \bmod n \tag{2}$$

$$s_0=x_0+k_0h_1(m_w||r_0) \bmod n \tag{3}$$

當投票所 P 收到委託書及相關參數，驗證是否為合法選票管理中心 O，如式 (4)。

$$s_0\cdot G=R_0\cdot h_1(m_w||r_0)+Y_0 \tag{4}$$

若驗證成立，則投票所計算代理簽署私鑰 s_{pr} 及其公鑰 Y_{pr}，如式 (5)、(6)。

$$s_{pr}=x_p+s_0 \bmod n \tag{5}$$

$$Y_{pr}=Y_0+Y_p+R_0\cdot h_1(m_w||r_0)=G\cdot s_{pr} \tag{6}$$

3.2.3 盲簽密階段

投票所 P 隨選一個值 $k_p(1<k_p<n)$，計算其公鑰 R_p 及 x 軸座標值，如式 (7)、(8)。最後，由投票所 P 直接將 (R_0, R_p, m_w) 傳送給投票者 A，可防止投票者重複領票。

$$R_p=k_p\cdot G=(x_2, y_2) \tag{7}$$

$$r_p=x_2 \bmod n \tag{8}$$

投票者 A 將要傳送的多份文件定義為 $\bar{v}=\{v_1, v_2, ..., v_n\}$，$1\le n$，對明文序列 $\bar{v}$ 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 (9)、(10)、(11)。

$$\bar{v}=\{v_1, v_2, ..., v_n\} \tag{9}$$

$$h_2(\bar{v})=t \tag{10}$$

$$f_{m2p}(\bar{v})=(V_1, V_2, ..., V_n) \tag{11}$$

定義 $\bar{x}=\{x_1, x_2, ..., x_n\}\in(0, 1)$ 算出 w 如式 (12)，以二進位表達 w 值，其循環位移關係為，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。

$$\begin{gathered}\text{if } x_i=1;\ x_{i+1}=0 \gg 1;\ x_i=0;\ x_{i+1}=1 \ll 1\\ \text{if } x_i=1;\ x_{i+1}=0 \gg 3;\ x_i=0;\ x_{i+1}=1 \ll 3\\ w=\{x_1\cdot 2^{i-1}+x_2\cdot 2^{i-2}+\cdots+x_n\cdot 2^0\}\end{gathered} \tag{12}$$

加密運算，利用明文轉點的方式將 (w, t) 轉成點座標 V_0，投票者 A 隨選一個值 k，k 屬於 Z_n^*，計算 $K=k\cdot G$，如式 (13)。實施加密的動作，C_i 為加密後的文件訊息如式 (14)、(15)、(16)、(17)。

$$K=k\cdot G \tag{13}$$

$$C_0=[f_{m2p}(w, t)+k\cdot Y_c] \tag{14}$$

$$C_i=[C_{i-1}+x_i * V_i],\ 1\le i\le n \tag{15}$$

$$\overline{C}=\{C_0, C_1, C_2, ..., C_n\} \tag{16}$$

$$h_3(\overline{C})=m \tag{17}$$

投票者 A 隨選盲因子 a, b, c，對密文摘要 m 進行盲化計算如式 (18)、(19)、(20)，若其結果為無窮遠點 O，則須重新選定盲因子。

$$R=a\cdot R_p+c\cdot G-b\cdot Y_{pr},\ R\neq O \tag{18}$$

$$e=h_4(R||m)\bmod n \tag{19}$$

$$e''=a^{-1}(e-b)\bmod n \tag{20}$$

投票所紀錄訊息有 (e''、s''、R_p)，在簽章文件 (m_w, r_o, m, e, s, $\overline{C}$, K) 揭露後，投票所亦無法從式 (19)、(20) 推導出盲因子 a, b, c，滿足代理簽署者所簽文件與文件本身的不可鏈結性。運算後將 e'' 投票所 P。投票所接收後，以代理私鑰 s_{pr} 實施簽署，並加上私鑰，運算產生 s'' 如式 (21)。

$$s''=e''s_{pr}+k_p\bmod n \tag{21}$$

投票所 P 將簽署後訊息 s'' 回傳給投票者，並解盲化，計算 s 如式 (22)。

$$s=as''+c\bmod n \tag{22}$$

最後，簽章文件為 (m_w, r_o, m, e, s, $\overline{C}$, K)。

3.2.4　驗證階段

以投票者 A 所傳送過來的 (m_w, r_o, m, e, s, $\overline{C}$, K) 進行簽章驗證程序，開票中心 C 驗證式 (23) 等號是否成立。

$$e=?h_4((s\cdot G-e\cdot Y_{pr})||m) \tag{23}$$

開票中心 C 接著將加密文件進行解密動作，計算如下：

$$f_{m2p}(w,\ t)=C_0-x_c\cdot K \tag{24}$$

$$(w,\ t)=f_{p2m}[f_{m2p}(w,\ t)] \tag{25}$$

將 w 還原成 x 數列，將其二進位表示的 w 值，其循環位移關係為，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 (26)：

$$\begin{gathered} w=\{x_1\cdot 2^{i-1}+x_2\cdot 2^{i-2}+\cdots+x_n\cdot 2^0\} \\ \text{if } x_i=1;\ x_{i+1}=0\gg 1;\ x_i=0;\ x_{i+1}=1\ll 1 \\ \text{if } x_i=1;\ x_{i+1}=1\gg 3;\ x_i=0;\ x_{i+1}=0\ll 3 \\ \overline{x}=\{x_1,\ x_2,\ \ldots,\ x_n\} \end{gathered} \tag{26}$$

執行解密的計算，依序對 $\overline{C}$ 進行解密，還原成點序列。解密運算如式 (27)：

$$V_i=[(C_i-C_{i-1}) * x_i],\ 1 \le i \le n \tag{27}$$

還原明文動作，將所有點資訊還原成明文訊息，計算如式 (28)、(29)。

$$\overline{V}=\{V_1, V_2, ..., V_n\} \tag{28}$$

$$f_{p2m}(\overline{V})=\bar{v} \tag{29}$$

3.3 系統模擬

本節將依本研究所提出之方法，驗證系統運作的可行性。

3.3.1 初始階段

系統選取橢圓曲線 $y^2=x^3+9x+26(\text{mod } 4229)$ 建立 $E(F_{4229})$ 選基點 $G=(1, 6)$，其階數 n 為 4254，使得 $4254 \cdot G=0$，其中 O 為無窮遠點。

$$n \cdot G=4254 \cdot (1, 6)=O$$

投票者 A、選票管理中心 O、投票所 P、開票中心 C 分別選擇 $x_a=9$、$x_o=5$、$x_p=22$、$x_c=13$，$x_a, x_o, x_p, x_c \in Z^*_{4254}$ 當成私鑰，並計算出相應之公鑰。

$$Y_a=x_a \cdot G=9 \cdot (1, 6)=(2213, 439)$$

$$Y_d=x_o \cdot G=5 \cdot (1, 6)=(3151, 4059)$$

$$Y_c=x_p \cdot G=22 \cdot (1, 6)=(320, 2015)$$

$$Y_c=x_a \cdot G=13 \cdot (1, 6)=(1844, 2742)$$

3.3.2 代理委託階段

選票管理中心 O 選擇一個值 $k_0=17$，計算其公鑰 R_0、x 軸座標值、委託書 m_w，並將 (R_0, s_0, m_w) 傳送給投票所 P。

$$R_0=k_0 \cdot G=17 \cdot (1, 6)=(911, 826)=(x_1, y_1) \tag{30}$$

$$r_0=x_1 \bmod n=911 \tag{31}$$

$$s_0=x_0+k_0h_1(m_w||r_0) \bmod n=5+17\times 5 \bmod 4254=90 \tag{32}$$

當投票所 P 收到委託書及相關參數，驗證是否為合法選票管理中心 O。

$$s_0 \cdot G=R_0 \cdot h_1(m_w||r_0)+Y_0$$

$$90 \cdot (1, 6)=17 \cdot (1, 6) \cdot 5+5 \cdot (1, 6)=(1309, 265) \tag{33}$$

若驗證成立，則投票所計算代理簽署私鑰 s_{pr} 及其公鑰 Y_{pr}。

$$s_{pr}=x_p+s_0 \bmod n=22+90 \bmod 4254=112 \tag{34}$$

$$\begin{aligned} Y_{pr}&=Y_0+Y_p+R_0\cdot h_1(m_w\|r_0)\\ &=5\cdot(1,6)+22\cdot(1,6)+17\cdot(1,6)\cdot 5\\ &=5\cdot(1,6)+22\cdot(1,6)+85\cdot(1,6)\\ &=112\times(1,6)=G\cdot s_{pr} \end{aligned} \tag{35}$$

3.3.3　盲簽密階段

投票所 P 選擇一個值 $k_p=28$，計算其公鑰 R_p、x 軸座標值。最後，投票所 P 將（$R_0=(911, 826)$, $R_p=(1480, 1946)$ 及 m_w）傳送給投票者 A。

$$R_p=k_p\cdot G=28\cdot(1,6)=(1480,1946)=(x_2,y_2) \tag{36}$$

$$r_p=x_2 \bmod n=1480 \tag{37}$$

投票者 A 將要傳送的多份文件定義為 $\bar{v}=\{1, 2, 3\}$，對明文實施雜湊值，利用明文轉點方式將明文轉為點座標，計算如下。

$$\bar{v}=\{v_1, v_2, v_3\}=\{1, 2, 3\} \tag{38}$$

$$h_2(\bar{v})=t=758 \tag{39}$$

$$f_{m2p}(\bar{v})=\{V_1, V_2, ..., V_n\}=\{12\cdot(1,6), 31\cdot(1,6), 20\cdot(1,6)\} \tag{40}$$

定義 $\bar{x}=\{1, 0, 1\}\in(0, 1)$ 算出 w 值，且以二進位表示 w。

$$\begin{aligned} &\text{if } x_i=1;\ x_{i+1}=0\gg 1;\ x_i=0;\ x_{i+1}=1\ll 1\\ &\text{if } x_i=1;\ x_{i+1}=1\gg 3;\ x_i=0;\ x_{i+1}=0\ll 3\\ &w=\{1\cdot 2^{3-1}+0\cdot 2^{3-2}+1\cdot 2^{3-3}\}=5=\{101\}_2 \end{aligned} \tag{41}$$

點序列循環位移前：{12·(1, 6), 31·(1, 6), 20·(1, 6)}
點序列循環位移後：{31·(1, 6), 12·(1, 6), 20·(1, 6)}
加密運算，利用明文轉點的方式將 (w, t) 轉成點座標 V_0，投票者 A 隨選一個值 $k=7$，k 屬於 Z^*_{4254}，計算 $K=k\cdot G$，實施加密的動作，C_i 為加密後的文件訊息。

$$K=k\cdot G=7\cdot(1,6)=(37, 2040) \tag{42}$$

$$\begin{aligned} C_0&=[f_{m2p}(w, t)+k\cdot Y_c]=f_{m2p}(5, 758)+7\cdot 13\cdot(1,6)\\ &=115\cdot(1,6)+91\cdot(1,6)=206\cdot(1,6)=(2085, 3513) \end{aligned} \tag{43}$$

$$C_1=[C_{1-1}+x_1 * V_1]=206\cdot(1,6)+31\cdot(1,6)=237\cdot(1,6) \quad (44)$$
$$C_2=[C_{2-1}+x_2 * V_2]=237\cdot(1,6)+12\cdot(1,6)=249\cdot(1,6)$$
$$C_3=[C_{3-1}+x_3 * V_3]=249\cdot(1,6)+20\cdot(1,6)=269\cdot(1,6)$$

$$\overline{C}=\{C_0, C_1, C_2, C_3\}=\{206\cdot(1,6), 237\cdot(1,6), 249\cdot(1,6), 269\cdot(1,6)\} \quad (45)$$

$$h_3(\overline{C})=m=39 \quad (46)$$

投票者 A 隨選盲因子 a=7, b=5, c=11，計算盲化運算式 $R=a\cdot R_p+c\cdot G-b\cdot Y_{pr}$，並對密文摘要 m 進行盲化計算。

$$R=a\cdot R_p+c\cdot G-b\cdot Y_{pr}=7\cdot 28\cdot(1,6)+11\cdot(1,6)-5\cdot 112\cdot(1,6)$$
$$=196\cdot(1,6)+11\cdot(1,6)-560\cdot(1,6)=3901\cdot(1,6) \quad (47)$$

$$e=h_4(R||m) \bmod n=11 \quad (48)$$

$$e''=a^{-1}(e-b) \bmod n=7^{-1}(11-5) \bmod 4254=1824 \quad (49)$$

運算後將 e'' 投票所 P。投票所接收後，以代理私鑰 s_{pr} 實施簽署，並加上私鑰。

$$s''=e''s_{pr}+k_p \bmod n=1824\times 112+24 \bmod 4254=120 \quad (50)$$

投票所 P 將簽署後訊息 s'' 回傳給投票者，由投票者實施解盲化。

$$s=as''+c \bmod n=7\times 720+11=851 \quad (51)$$

最後，簽章文件為 $(m_w, r_o, m, e, s, \overline{C}, K)$。

3.3.4 驗證階段

以投票者 A 所傳送過來的 $(m_w, r_o, m, e, s, \overline{C}, K)$ 進行簽章驗證程序，開票中心 C 驗證下述之左右兩式是否成立。

$$e=?h_4((s\cdot G-e\cdot Y_{pr})||m)$$

$$11=?h_4((851\cdot(1,6)-11\cdot 112\cdot(1,6)||39) \quad (52)$$

開票中心 C 接著將加密文件進行解密動作。

$$f_{m2p}(w,t)=206\cdot(1,6)-13\cdot 7\cdot(1,6)=115\cdot(1,6) \quad (53)$$

$$(w,t)=f_{p2m}[f_{m2p}(w,t)]=(5,758) \quad (54)$$

將 w 還原成 x 數列，將其二進位表示的 w 值，其循環位移關係為，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，還原方式如下：

$$w=\{1\cdot 2^{3-1}+0_2\cdot 2^{3-2}+1\cdot 2^{3-3}\}$$
$$\text{if } x_i=1;\ x_{i+1}=0 \ll 1;\ x_i=0;\ x_{i+1}=1 \gg 1$$
$$\text{if } x_i=1;\ x_{i+1}=1 \ll 3;\ x_i=0;\ x_{i+1}=0 \gg 3$$
$$\bar{x}=\{1,\ 0,\ ...,\ 1\} \tag{55}$$

執行解密的計算，依序對 $\overline{C}$ 進行解密，還原成點序列 $\overline{V}$。

$$V_3=[(C_3-C_{3-1})*x_3]=(269\cdot(1,\ 6)-249\cdot(1,\ 6))*1=20\cdot(1,\ 6)*1$$
$$V_2=[(C_2-C_{2-1})*x_2]=(249\cdot(1,\ 6)-237\cdot(1,\ 6))*0=12\cdot(1,\ 6)*0$$
$$V_1=[(C_1-C_{1-1})*x_1]=(237\cdot(1,\ 6)-206\cdot(1,\ 6))*1=31\cdot(1,\ 6)*1 \tag{56}$$

點序列循環位移前：$\{31\cdot(1,\ 6),\ 12\cdot(1,\ 6),\ 20\cdot(1,\ 6)\}$
點序列循環位移後：$\{12\cdot(1,\ 6),\ 31\cdot(1,\ 6),\ 20\cdot(1,\ 6)\}$
還原明文動作，將所有點資訊還原成明文訊息。

$$\overline{V}=\{V_1,\ V_2,\ V_3\}=\{12\cdot(1,\ 6),\ 31\cdot(1,\ 6),\ 20\cdot(1,\ 6)\} \tag{57}$$

$$f_{p2m}(\overline{V})=\bar{v}=\{1,\ 2,\ 3\} \tag{58}$$

4. 安全性及效益分析

本研究所提架構，其安全性主要植基於 ECDLP、單向雜湊函數，相關針對「安全性分析」及「效益分析」等內容分述如下：

4.1　安全性分析

(1) 驗證性（Verifiability）：驗證性指的是簽章文件能通過驗證者的驗證，證明文件為指定的簽署者所簽。本方法中的驗證式 (23) $e=?h_4((s\cdot G-e\cdot Y_{pr})\|m)$，由開票中心驗證簽署文件，證明此文件是由合法投票所簽署，並非假他人之手。驗證過程如下：

$$\begin{aligned} s\cdot G-e\cdot Y_{pr}&=(as''+c)\cdot G-e\cdot Y_{pr}=(e''s_{pr}+k_p)a\cdot G+c\cdot G-e\cdot Y_{pr}\\ &=a\cdot Y_{pr}\cdot a^{-1}(e-b)+a\cdot R_p+c\cdot G-e\cdot Y_{pr}\\ &=e\cdot Y_{pr}-b\cdot Y_{pr}+a\cdot R_p+c\cdot G-e\cdot Y_{pr}\\ &=a\cdot R_p+c\cdot G-b\cdot Y_{pr}=R \end{aligned}$$

(2) 不可否認性（Non-repudiation）：不可否認性指的是對已發生之行動或事件

的證明，使該行動或事件具有往後不能被否認的能力。在簽署過程中，本方法中式 (21) $s''=e''s_{pr}+k_p \bmod n$，投票所簽署選票後以證明此選票為合法有效票，同時防止投票所事後否認選票經由他簽署的。

(3) 隱匿性（Anonymity）：隱匿性是指為了維持投票的公平性，有著「無記名」的一項原則。在此原則下，人人都必須匿名投票。簽署人對簽署的「選票內容」無法獲知該內容的訊息，本方法透過盲化過程如式 (18) $R=a\cdot R_p+c\cdot G-b\cdot Y_{pr}$、式 (19) $e=h_4(R||m) \bmod n$、式 (20) $e''=a^{-1}(e-b) \bmod n$，不必擔憂投票所在簽署過程中知道投票者所圈選的資料而所造成選票曝光，可達到投票者選票資訊隱匿之特性。

(4) 不可偽造性（Unforgeability）：不可偽造性指的是在資料傳遞的過程中，不會遭到惡意的第三者竄改並偽造資料的內容。本方法中式 (17) $h_3(\overline{C})=m$，由於雜湊函數具有不可逆推的特性，若攻擊者欲偽造有效選票，則須面臨破解單向雜湊函數，且即使破解成功，但文件 m 已透過明文轉點及擬亂等加密過程，如式 (15) $C_i=[C_{i-1}+x_i * V_i]$，將大幅增加偽造難度；再者，若攻擊者欲偽造一個有效簽章文件 (m_w, r_o, m', e', s', $\overline{C}$, K)，使其可以通過驗證式 (23) $e=?h_4((s\cdot G-e\cdot Y_{pr})||m)$，則同樣亦須面臨單向雜湊函數與 ECDLP。

(5) 機密性（Confidentiality）：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，選票在成功送達目的地之前，所有內容均是保密。本方法中的式 (12) $w=\{x_1\cdot 2^{i-1}+x_2\cdot 2^{i-2}+\cdots+x_n\cdot 2^0\} \in (0, 1)$，$w$ 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，即便遭到截獲，也無法求得任何資訊。本研究代理盲簽密文件之訊息為加密過之訊息，並非明文訊息，可避免遭不相關人士攔截，得知訊息內容，倘若攻擊者欲破解，則須面臨破解單向雜湊函數與 ECDLP。

(6) 完整性（Integrity）：完整性指的是確保選票處理與傳遞是完整正確，過程中確認沒被任意地加入、刪除或修改選票。在本方法式 (10) $h_2(\bar{v})=t$ 對明文序列進行雜湊運算得 t，並將 t 加入式 (14) $C_0=[f_{m2p}(w, t)+k\cdot Y_c]$ 中，若第三方想要竄改明文偽造 t 而不被發現，則必須對面破解單向雜湊函數的問題及面對 ECDLP，使得本系統可以得到完整性的確保。

(7) 不可鏈結性（Unlinkability）：不可鏈結性是指在簽章文件揭露出來後，代理簽章者無法從文件中追蹤所簽文件與簽章要求者的關係，也沒有辦法追蹤文件與當時所簽署文件之間的關聯性。本研究投票所紀錄訊息有 (e''、s''、R_p)，在簽章文件 (m_w, r_o, m, e, s, $\overline{C}$, K) 揭露後，投票所亦無法從式 (19) $e=h_4(R||m)$

mod n、式 (20) $e''=a^{-1}(e-b)$ mod n 推導出盲因子 a, b, c，因而無法判斷式 (18) $R=a\cdot R_p+c\cdot G-b\cdot Y_{pr}$, $R \neq O$ 是否成立。因此，滿足代理簽署者所簽之文件與文件本身的不可鏈結性。

(8) 區別性（Distinguishability）：區別性指的是代理盲簽章必須與一般簽章有所區別。本方法簽章文件 (m_w, r_o, m, e, s, $\overline{C}$, K) 中的委託授權書 m_w，即能從一般簽章中辨別出代理盲簽章。

(9) 識別性（Identifiability）：識別性是指能確認原始簽章者與代理簽章者身分。根據委託授權書 m_w 及驗證式 (23) $e=?h_4((s\cdot G-e\cdot Y_{pr})\|m)$，代理簽署公鑰 Y_{pr} 包含原始簽章者（選票管理中心）與代理簽章者（投票所）之公鑰，如式 (6) $Y_{pr}=Y_0+Y_p+R_0\cdot h_1(m_w\|r_0)$，驗證者即可得知相對的簽署者身分。

(10) 避免不當使用（Prevention of misuse）：代理金鑰僅能用來產製代理使用的簽章，且委託授權中應明定代理責任，避免濫用。本架構中委託授權書 m_w，包含原始簽署者與代理簽署者身分、代理簽署者簽署之資料型態及授權期限等，因此代理金鑰無法任意產製代理簽署私鑰，亦無法任意簽署未經授權之資料。

本研究與相關文獻之安全性分析比較，詳如表 3。

▼ 表 3　本研究與植基於各系統代理盲簽章之安全性比較表

演算法與安全性	Tan et al.（2002）	Wang and Wang（2005）	Yang and Yu（2008）	Alghazzawi et al.（2011）	Pradhan and Mohapatra（2011）	Qin et al.（2013）	Wang and Liao（2014）	本研究方法
驗證性	V	V	V	V	V	V	V	V
不可否認性	V	V	V	V	V	V	V	V
隱匿性	V	V	V	V	V	V	V	V
不可偽造性	X	X	X	V	V	V	V	V
機密性	X	X	X	X	X	X	X	V
完整性	△	△	△	△	△	△	△	V
不可鏈結性	X	X	V	X	X	V	V	V
區別性	V	V	V	V	V	X	V	V
避免不當使用性	X	V	V	V	V	V	V	V

演算法與安全性	Tan et al.（2002）	Wang and Wang（2005）	Yang and Yu（2008）	Alghazzawi et al.（2011）	Pradhan and Mohapatra（2011）	Qin et al.（2013）	Wang and Liao（2014）	本研究方法
識別性	V	V	V	V	V	V	V	V
避免不當使用性	X	V	V	V	V	V	V	V

註一：本研究另含多文件之特性
註二：V 代表符合特性、Δ 代表部分符合、X 代表不符合特性

4.2 效益分析

運算符號及運算時的相互關係如表 4，模數加法、模數減法運算時間低，予以忽略不計（Wang, 2008）。表 5 是各系統之代理盲簽章一份文件所需運算成本比較表，當比較的文件份數愈來愈多時，可明顯發揮本研究所提之多文件效益。此外，由於 Qin et al.（2013）之機制為植基於離散對數難題，計算量遠超過其他植基於橢圓曲線離散對數難題之系統，因此扣除其機制後，可更明顯看出各系統之差異。

▼ 表 4　運算成本（Computation cost）參考表

運算成本（Computation cost）計算量分析	
符號	定義
T_{ECMUL}	進行一次 ECC 乘法運算所需時間 ≈ 29 T_{MUL}
T_{ECADD}	進行一次 ECC 加法運算所需時間 ≈ 5 T_{MUL}
T_{INVS}	進行一次模式乘法反元素運算所需時間 ≈ 240 T_{MUL}
T_{EXP}	進行一次模式指數運算所需時間 ≈ 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_{MUL}	進行一次模式乘法運算所需時間
t_h	進行一次 hash（SHA-1）所需時間 ≈ 0.4 T_{MUL}
T_h	進行一次點 hash 所需時間 ≈ 23 T_{MUL}

▼ 表 5　本研究與植基於各系統代理盲簽章機制一份文件所需運算成本比較表

演算法		Tan et al.（2002）		Wang and Wang（2005）		Yang and Yu（2008）		Alghazzawi et al.（2011）	
各階段	比較項目	運算成本	概估	運算成本	概估	運算成本	概估	運算成本	概估
代理階段	代理運算	$3T_{ECMUL}+1T_{ECADD}+1T_{MUL}+2T_{ADD}$	$\approx 93\ T_{MUL}$	$3T_{ECMUL}+1T_{ECADD}+1T_{MUL}+2T_{ADD}$	$\approx 93\ T_{MUL}$	$2T_{ECMUL}+1T_{ECADD}+1T_{MUL}+2T_{ADD}$	$\approx 64\ T_{MUL}$	$2T_{ECMUL}+1T_{ECADD}+1T_{MUL}+1T_{ADD}$	$\approx 64\ T_{MUL}$
盲簽密階段	加密運算	無	無	無	無	無	無	無	無
	盲簽運算	$8T_{ECMUL}+6T_{ECADD}+3T_{MUL}+7T_{ADD}+1t_h$	$\approx 265\ T_{MUL}$	$8T_{ECMUL}+6T_{ECADD}+3T_{MUL}+7T_{ADD}+1t_h$	$\approx 265\ T_{MUL}$	$5T_{ECMUL}+3T_{ECADD}+4T_{MUL}+2T_{ADD}+1t_h+1T_{INVS}$	$\approx 404\ T_{MUL}$	$3T_{ECMUL}+2T_{ECADD}+2T_{MUL}+3T_{ADD}+1t_h$	$\approx 99\ T_{MUL}$
驗證階段	驗證運算	$3T_{ECMUL}+3T_{ECADD}+1t_h$	$\approx 102\ T_{MUL}$	$3T_{ECMUL}+3T_{ECADD}+1t_h$	$\approx 102\ T_{MUL}$	$2T_{ECMUL}+3T_{ECADD}+1t_h$	$\approx 73\ T_{MUL}$	$2T_{ECMUL}+1T_{ECADD}+1T_{MUL}+1t_h$	$\approx 64\ T_{MUL}$
	解密運算	無	無	無	無	無	無	無	無

演算法		Tan et al.（2002）		Wang and Wang（2005）		Yang and Yu（2008）		Alghazzawi et al.（2011）	
各階段	比較項目	運算成本	概估	運算成本	概估	運算成本	概估	運算成本	概估
總和		$14T_{ECMUL}+10T_{ECADD}+4T_{MUL}+9T_{ADD}+2t_h$	$\approx 460\ T_{MUL}$	$14T_{ECMUL}+10T_{ECADD}+4T_{MUL}+9T_{ADD}+2t_h$	$\approx 460\ T_{MUL}$	$9T_{ECMUL}+7T_{ECADD}+5T_{MUL}+4T_{ADD}+2t_h+1T_{INVS}$	$\approx 541\ T_{MUL}$	$7T_{ECMUL}+4T_{ECADD}+4T_{MUL}+4T_{ADD}+2t_h$	$\approx 227\ T_{MUL}$

▼ 表 5　本研究與植基於各系統代理盲簽章機制一份文件所需運算成本比較表（續）

演算法		Pradhan and Mohapatra（2011）		Qin et al.（2013）		Wang and Liao（2014）		本研究方法	
各階段	比較項目	運算成本	概估	運算成本	概估	運算成本	概估	運算成本	概估
代理階段	代理運算	$3T_{ECMUL}+3T_{ECADD}+2T_{MUL}+1T_{ADD}+3t_h$	$\approx 105\ T_{MUL}$	$7T_{EXP}+7T_{MUL}+1T_{ADD}+2t_h$	$\approx 1687\ T_{MUL}$	$3T_{ECMUL}+3T_{ECADD}+1T_{MUL}+2T_{ADD}+3t_h$	$\approx 104\ T_{MUL}$	$3T_{ECMUL}+3T_{ECADD}+1T_{MUL}+2T_{ADD}+3t_h$	$\approx 104\ T_{MUL}$

演算法		Pradhan and Mohapatra（2011）		Qin et al.（2013）		Wang and Liao（2014）		本研究方法	
各階段	比較項目	運算成本	概估	運算成本	概估	運算成本	概估	運算成本	概估
盲簽密階段	加密運算	無	無	無	無	無	無	$2T_{ECMUL}$ + $1T_{ECADD}$ + $1t_h$ + $1T_h$	≈ 86 T_{MUL}
	盲簽運算	$3T_{ECMUL}$ + $2T_{ECADD}$ + $1T_{MUL}$ + $5T_{ADD}$ + $1t_h$	≈ 98 T_{MUL}	$8T_{EXP}$ + $12T_{MUL}$ + $2T_{ADD}$ + $3t_h$ + $1T_{INVS}$	≈ 2173 T_{MUL}	$4T_{ECMUL}$ + $2T_{ECADD}$ + $3T_{MUL}$ + $3T_{ADD}$ + $1t_h$ + $1T_{INVS}$	≈ 369 T_{MUL}	$4T_{ECMUL}$ + $2T_{ECADD}$ + $3T_{MUL}$ + $3T_{ADD}$ + $1t_h$ + $1T_{INVS}$	≈ 369 T_{MUL}
驗證階段	驗證運算	$2T_{ECMUL}$ + $1T_{ECADD}$ + $1t_h$	≈ 63 T_{MUL}	$4T_{EXP}$ + $5T_{MUL}$ + $1T_{INVS}$	≈ 1205 T_{MUL}	$2T_{ECMUL}$ + $1T_{ECADD}$ + $1t_h$	≈ 63 T_{MUL}	$2T_{ECMUL}$ + $1T_{ECADD}$ + $1t_h$	≈ 63 T_{MUL}
	解密運算	無	無	無	無	無	無	$2T_{ECMUL}$ + $2T_{ECADD}$	≈ 68 T_{MUL}
總和		$8T_{ECMUL}$ + $6T_{ECADD}$ + $3T_{MUL}$ + $6T_{ADD}$ + $5t_h$	≈ 266 T_{MUL}	$19T_{EXP}$ + $24T_{MUL}$ + $3T_{ADD}$ + $5t_h$ + $2T_{INVS}$	≈ 5065 T_{MUL}	$9T_{ECMUL}$ + $6T_{ECADD}$ + $4T_{MUL}$ + $5T_{ADD}$ + $5t_h$ + $1T_{INVS}$	≈ 536 T_{MUL}	$13T_{ECMUL}$ + $9T_{ECADD}$ + $4T_{MUL}$ + $5T_{ADD}$ + $6t_h$ + $1T_h$ + $1T_{INVS}$	≈ 690 T_{MUL}

5. 結論

我國因民情因素尚未將大選全面投入電子投票，然而，電子投票已是各國民主法治化所共同追求的方向及趨勢，政府可從公司股東代表遴選延伸至全國性選舉，使選務工作系統化，減少整體經費，避免不必要的人為錯誤與爭議。本研究提出新型態之電子投票機制，多份電子選票執行一次簽密的方法，具高彈性設計，滿足不同選區不同選票、不同選區混合相同選票和不同選票、不同選票的特殊需求（加載資料等）、選票存取控管彈性及與實務上的選票分類保管等選務工作運作流程；此外，本論文使用盲化特性保護投票者身分，運用代理機制強化資訊的即時性及多文件簽密設計，滿足未來複雜化的多合一選舉趨勢，同時強化選票之安全設計，避免遭第三者攔截，進而得知選票內容。藉由本研究所提架構之安全性及效益分析驗證，本研究兼顧效率及安全，可補強以往學者所提方法的缺陷，有助於國內客製化的電子投票推動與實行。

參考文獻

丘昌泰（2004）。從各國電子投票經驗看我國選務的改革方向。*研考雙月刊，28*（4），25-35。

許建隆、吳宗成（1999）。簽章加密法及其應用。*資訊安全通訊，6*（1），33-41。

曾貴華（2010）。*量子保密通信*。台北市：高等教育出版社。

覃海生、張雷、馮燕強、吳文俊、何傳波（2013）。無對運算的隨機代理盲簽章方案設計。*計算機工程，39*（4），169-173。

蘇品長、楊倫青、王博彥（2014）。植基於橢圓曲線之多重盲簽密機制。*資訊管理研究，14*，73-94。

Alghazzawi, D. M., Salim, T. M., & Hasan, S. H. (2011). A new proxy blind signature scheme based on ECDLP. *International Journal of Computer Science Issues*, *8*(3), 73-79.

Chaum, D. (1982). Blind signatures for untraceable payments. *Advances in Cryptology* (3rd ed.). New York: Springer Science + Business.

Delaune, S., Kremer, S., & Ryan, M. (2006). Coercion-resistance and receipt-freeness in electronic voting. *Proceedings of the 2006 IEEE 19th Computer Security Foundations Workshop (CSFW)*, Los Alamitos, California.

Fan, K., Wang, Y., & Li, H. (2012). A new proxy blind signature scheme. *International Journal of Grid and Utility Computing*, *3*(1), 38-42.

Hu, L., Zheng, K., Hu, Z., & Yang, Y. (2009). A secure proxy blind signature scheme based

on ECDLP. *International Conference on Multimedia Information Networking and Security*, DOI 10.1109/MINES.2009.220.

Lal, S., & Awasthi, A. (2003). Proxy blind signature scheme. *Journal of Information Science and Engineering*, Cryptology ePrint Archive, Report 2003/072. Available at http://eprint.iacr.org/.

Lin, W., & Jan, J. (2000). A security personal learning tools using a proxy blind signature scheme. *International Conference on Chinese Language Computing*, Illinois, USA.

Lu, R., Cao, Z., & Zhou, C. (2005). Proxy blind multi-signature scheme without a secure channel. *Applied Mathematics and Computation*, *164*(1), 179-187.

Mambo, M., Usuda, K., & Okamoto, E. (1996). Proxy signatures for delegating sign operation. *Proceeding of the 3rd ACM conference on computer and communications security (CCS96)*, New York, NY, USA.

Mateu, V., Sebe, F., & Valls, M. (2014). Constructing credential-based E-voting systems from offline E-coin protocols. *Journal of Network and Computer Applications*, *42*, 39-44.

Pradhan, S., & Mohapatra, R. (2011). Proxy blind signature scheme based on ECDLP. *International Journal of Engineering Science & Technology*, *3*(3), 2244-2248.

Qin, H. S., Zhang, L., Feng, Y., Wu, W., & He, C. (2013). Design of randomized proxy blind signcryption scheme without pairing computing. *Computer Engineering*, *39*(4), 169-173.

Sun, H., Hsieh, B., & Tseng, S. (2005). On the security of some proxy blind signature schemes. *The Journal of Systems and Software*, *74*(3), 297-302.

Tan, Z., Liu, Z., & Tang, C. (2002). Digital proxy blind signature schemes based on DLP and ECDLP. *MM Research Preprints, MMRC, AMSS, Academia, Sinica*, Beijing, *21*, 212-217.

Tian, Y., Chen, H., Yan, G., Tian, J., & Wen, X. (2013). A proxy blind signature scheme based on quantum entanglement. *Optical and Quantum Electronics*, *45*(12), 1297-1305.

Wang, C., & Liao, M. (2014). Security Analysis and Enhanced Construction on ECDLP-Based Proxy Blind Signature Scheme. *International Journal of e-Education, e-Business, e-Management and e-Learning*, *4*(1), 47-51.

Wang, H., & Wang, R. (2005). A proxy blind signature scheme based on ECDLP. *Chinese Journal of Electronics*, *14*(2), 281-284.

Wang, R., Juang, W., & Lei, C. (2008). A Web Metering Scheme for Fair Advertisement

Transactions. *International Journal of Security and its Applications*, *2*(4), 49-55.

Yang, X., & Yu, Z. (2008). Security analysis of a proxy blind signature scheme based on ECDLP. *Proceedings of 4th International Conference on Wireless Communications, Networking and Mobile Computing,* Dalian, China.

Zhang, F., & Kim, K. (2003). Efficient ID-based blind signature and proxy signature from bilinear pairings. *Proceedings of ACISP*, Wollongong, Australia.

Zheng, Y. (1997). Digital signcryption or How to achieve cost (Signature & Encryption) << Cost (Signature) + Cost (Encryption). In Kaliski, B. (Ed.), *Advances in Cryptology-Crypto*. Berlin: Springer.