具不可追蹤之多重文件盲簽章機制設計
Design Multi-Document Blind Signature Schemes with Untraceable Protocol

蘇品長
國防大學資訊管理學系
Pin-Chang Su
Department of Information Management, NDU
Email: spc.cg@msa.hinet.net

李瑋豪
國防大學資訊管理學系
Wei-Hao Li
Department of Information Management, NDU
Email: lex010129@gmail.com

摘　要

網際網路的普及化，衍生了許多新的行為模式，例如電子商務以及電子投票等。但是，網際網路是一個開放的空間，在網路上進行很多活動都有其風險，特別是在電子商務及電子投票方面，使用者的身分隱私的保護為整個電子化行為成功與否的關鍵因素，而如何證明使用者在網路上的行為資料為有效資料而不是被惡意假造的呢？於是數位簽章這個機制就應運而生了。數位簽章能夠達到確認行為雙方的身份，但是要如何隱藏行為者所傳遞的資料內容以及隱藏行為者的身份又是另一個難題。國內外多位學者為了達到可應用於電子投票及電子商務的簽章及加密技術做了相當多的研究。從 Chaum 於 1982 年提出盲簽章的觀念後，隨著學者們不斷改進，如何達到更有效率的執行速度與更安全的防護設計是值得省思的議題。本研究透過蒐集彙整相關文獻，整理出現行的電子投票與電子商務機制在運算處理及身份隱藏上的缺漏。透過以植基於橢圓曲線密碼系統的快速運算為基礎，結合隨機背包密碼系統，提出多份電子文件執行一次盲簽章的方法，減少在傳遞過中的簽章次數，提升運算過程中的效率及安全的防護，並透過盲簽章技術確實隱藏使用者與其文件之間的關係，以保障使用者電子投票或是電子商務行為的隱私。未來可適用於多合一選舉的電子化、股東會電子投票及網路上多筆電子付款一次支付的應用機制上。

一、緒論

自從網際網路問世以來，人類的生活模式也起了莫大的改變，網路已經不僅僅是張貼文字、交流意見的一個平台，其更改進了人類在食、衣、住、行、育、樂等方面的行為模式。舉例來說，以往商業活動、買賣交易皆是以人與人之間互動，來達成交易的進行，並確保銀貨兩訖後整個商業行為才算結束。但是在網際網路下，商業行為模式已經不在侷限於人與人之間，電子商務、網路購物等新興的交易模式在網路快速發展的推波助瀾下迅速的融入人類的生活，帶給了人們不出門也可以買到貨品及所需物資的便利性。但是，網際網路是一個開放的空間，在網路上進行很多活動都有其風險，特別是在電子商務及電子投票方面，因為其涉及的除了金錢的流動外，更與使用者資料的隱私息息相關。以電子商務為例，對於使用者所購買的物品資訊需要保密；而在電子投票方面，如果無法隱藏投票者票卷內容，就可能讓有心人士藉由逆推方式得知票卷與投票者關係，將會造成電子投票失去公信力。而如何證明使用者在網路上的行為資料為有效資料而不是被惡意假造的呢？於是數位簽章這個機制就應運而生了。

數位簽章能夠達到確認行為雙方的身份，但是要如何隱藏行為者所傳遞的資料內容以及隱藏行為者的身份又是另一個難題。國內外多位學者為了達到可應用於電子投票及行動商務的簽章及加密技術做了相當多的研究，首先 Chaum 於 1982 年提出盲簽章的觀念[6]，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投票內容隱私的特性，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 [3]以及達成使用者身分不可追蹤性的盲簽章[12][13][14]。這些方法所提出：無論選舉者身處何地，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；而楊倫青[1]提出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又有無法有效隱藏選舉者身分。為因應本國未來多合一選舉以降低舉辦選舉所耗費的社會資源及有效保護選舉者，本研究提出適用於多合一選舉電子投票機制的多重盲簽章法，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，提升運算上的時間外，亦能有效達到選舉者身分之不可追蹤性，提供更佳的安全保護。

二、文獻探討

本章歸納整理與本研究相關的盲簽章文獻，並介紹基於各種演算法之盲簽章機制與演算架構。

2-1 基於 RSA 的盲簽章

Chaum[6]所提出的盲簽章是以 RSA 為基底的數位簽章演算法，*(n,e)*是簽章者的公鑰對，*d* 是簽章者的私鑰，*m* 為訊息，Chaum 的盲簽章可分為五階段，簡述如下：

Step1：初始階段

選擇 *p* 與 *q* 兩個質數，並計算 *n =p* q* 、計算 $\phi(n)=(p-1)*(q-1)$。選擇兩個亂數 *e* 和 *d*，使其滿足 $gcd(\phi(n), e)=1;1<e<\phi(n)$，

計算：$d=e^{-1} \bmod \phi(n)$。

公開金鑰：{*e, n*}

私密金鑰：{*d*}

Step2：盲化階段

送簽者先在 *0 ~ n* 之間隨機選取一數 *r*，並計算 $m' = mr^e \bmod n$，再將 m' 傳送給簽章者。而在此步驟中已經先將訊息盲化成 m'，當簽章者收到 m' 時則不知道該內容為何。

Step3：簽章階段

簽章者收到訊息 m' 後，用本身的私鑰 *d* 計算出 $s' = m'^d \bmod n$，再將 s' 回傳給送簽者；此步驟已完成簽章者對盲訊息的簽署。

Step4：解盲階段

當送簽者收到 s' 後，計算 $s=s'/r \bmod n$，此時已完成去盲的動作，回覆原本訊息 *m*，而 *s* 即為簽章者對於訊息 *m* 的簽章。

Step5：驗證階段

在驗證階段中，任何人皆可以用 $s = m^e \bmod n$ 來驗證(m, s)的有效性，若驗證成立，則代表該簽章為簽章者對訊息 *m* 的有效簽章。

2-2 基於 ECDLP 的盲簽章

由 Jeng 等三位學者[8]，利用橢圓曲線離散對數的難題以及橢圓曲線金鑰長度短，處理速度快且安全性高等特性提出基於橢圓曲線的盲簽章，也因此他們的演算法會比 RSA 及 ElGamal 運算更快，演算法步驟如下：

Step1：初始階段

$y^2 = x^3 + ax + b(mod\ p), 4a^3 + 27b^2 \neq 0$，建立 $E_p(a, b)$，選一個 order 為極大數 n 的基點 $G=(x,y)$ 在 $E_p(a, b)$ 上 $n*G=0$，$\{R_i \mid 1 \le i \le n, n \in N\}$，送簽者選擇 $n_t \in Z_p$ 當私鑰，產生他之公鑰 $P_t = n_t * G$，簽章者選擇一個隨機 $n_v \in Z_p$ 當作他之私鑰，而公鑰是 $P_v = n_v * G$。

Step2：盲化階段

假設訊息 m 要被簽章，送簽者產生一個盲因子$(r_t * p_t)$，接著將盲訊息 α 傳給簽章者，$\alpha \equiv m * (r_t * p_t)(mod\ p)$。

Step3：簽章階段

簽章者選擇一個元素 $n_v \in Z_p$ 當作第二個盲因子和產生一對盲簽章(r, s) $r = n_v * \alpha$、$s = (n_v + n_s) * \alpha$，n_s 是簽章者之私鑰，將簽章對$(\alpha,(r, s))$ 寄給送簽者，簽章者必須保留$(\alpha,\ n_v)$。

Step4：解盲階段

當送簽者接收到簽章對$(\alpha,(r, s))$，用他自己的私鑰 n_t 解出簽章(r, s)。接著送簽者用簽章者的公鑰 P_s 計算 s'，

$s' = s - m * n_t * P_s \ (mod\ p)$，然後請求者計算 m'，$m' = n_t * (n_t - 1) * m$，最後送簽者送出三個值(m', s', r)。

Step5：驗證階段

任何人都可以使用簽章者的公鑰 P_s 去計算 $r = s' - m' * P_s \ (mod\ p)$ 來驗證簽章值(m', s', r)。

三、具不可追蹤之多重文件盲簽章機制設計

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，而多合一選舉以及電子商務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[1][2]的多重盲簽章法，可適用在多合一選舉及行動商務方面的簽章認證，並有效隱藏使用者身份。本研究以電子投票為例，提出多張文件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。本系統中的盲簽章特性，可彈性選擇要加密的文件張數及種類，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。[5]本章將針對所提方法之運作流程及系統架構進分別說明：

3-1 本系統整體運作流程架構及參數表

系統的整體運作流程如圖 1 所示。

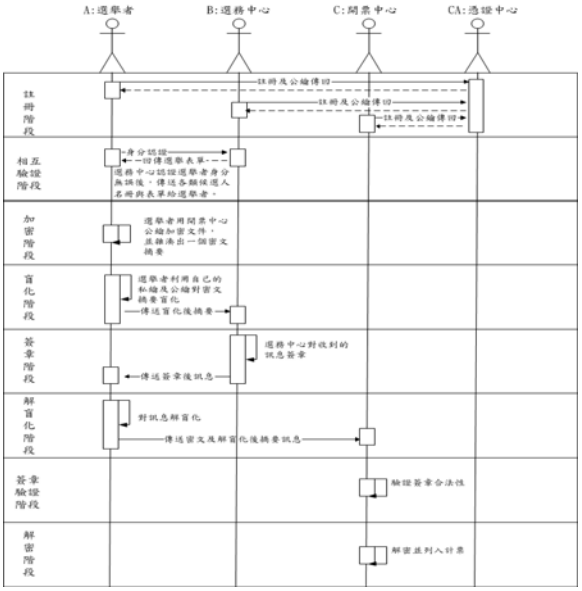

圖 1 運作流程

本系統架構可分為系統初始註冊階段、相互驗證身分階段、加密階段、盲化階段、簽章階段、解盲化階段、簽章驗證階段及解密階段等八個階段，各階段分別說明如下：

3-2 系統各階段流程

以下就本研究設計機制的各階段分別敘述。

3-2-1 系統初始註冊階段

- 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 $u \rightarrow n/\alpha$ ， $u \leq 4$ 。
- 選舉人 A、選務中心 B、開票中心 C、憑證中心 CA 分別選擇 n_A 、 n_B 、 n_C 、 n_{AS} ， n_A 、 n_B 、 n_C 、 $n_{AS} \in Z_q^*$ 當成私鑰，並計算出相應之公鑰

$$PK_A = n_A * G, PK_B = n_B * G,$$

$$PK_C = n_C * G, PK_{AS} = n_{AS} * G \quad (1)$$

- 並透過一個絕對安全之通道將本身公鑰及身分 送至憑證中心計算出關聯值

$$e_A=h_1(id_A,PK_A), e_B=h_1(id_B,PK_B), e_C=h_1(id_C,PK_C) \quad (2)$$

- 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

$$Z_A = l_A * G = (x_{Z_A}, y_{Z_A}),$$

$$Z_B = l_B * G = (x_{Z_B}, y_{Z_B}),$$

$$Z_C = l_C * G = (x_{Z_C}, y_{Z_C}) \cdot \quad (3)$$

- 產生憑證 $ca_A = l_A(e_A + x_{Z_A} * n_{AS})$,

$$ca_B = l_B(e_B + x_{Z_B} * n_{AS}),$$

$$ca_C = l_C(e_C + x_{Z_C} * n_{AS}) \text{。} \quad (4)$$

- 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 $h_1(\ )$ 及 $h_2(\ )$ ，最後公開

$$E(F_q), G, \alpha, q, PK_A, PK_B, PK_C, PK_{AS}, h_1(\ ), h_2(\ )$$

3-2-2 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：

$$u_1 = ca_A^{-1} \bmod \alpha \quad (5)$$

$$u_2 = e_A \cdot u_1 \bmod \alpha \quad (6)$$

$$u_3 = x_{Z_A} \cdot u_1 \bmod \alpha \quad (7)$$

- 著以憑證中心的公開金鑰來驗證身分之正確性，計算：

$$u_2 \cdot G + u_3 \cdot PK_{AS} = (v_x, v_y) \quad (8)$$

驗證： $Z_{A_x} \overset{?}{=} v_x$ (9)

3-2-3 加密階段

- 選舉人 A 將多份選票明文定義 $\bar{v} = \{v_1, v_2, \ldots, v_n\}$，$1 \leq n$，對明文 $\bar{v}$ 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(10)、(11)、(12)。

$$\bar{v} = \{v_1, v_2, ..., v_n\} \quad (10)$$

$$h_1(\bar{v}) = t \quad (11)$$

$$f_{m2p}(\bar{v}) = \{V_1, V_2, ..., V_n\} \quad (12)$$

- 定義 $\bar{x} = \{x_1, x_2, ..., x_i\} \in (0,1)$ 算出 w 如(13)，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。

$$w = \{x_1 2^{i-1}, x_2 2^{i-2}, ..., x_i 2^0\} \in (0,1) \quad (13)$$

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

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

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

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

- 密運算，利用明文轉點的方式 $f_{m2p}(w,t)$ 將 w 值以十進位表示轉成點座標 V_0，選舉人 A 隨選一個值 q，q 屬於 Z_p^* 且 $n_A \neq q$，計算 $T = q \cdot G$，如式(14)。實施加密的動作，C_i 為加密後的訊息選票如式(15)(16)(17)(18)。

$$T = q * G \quad (14)$$

$$C_0 = [f_{m2p}(w,t) + q * PK_c] \quad (15)$$

$$C_i = [V_i + x_i * C_{i-1}] \ , 1 \le i \le n \quad (16)$$

$$\vec{C} = \{C_0, C_1, C_2, \ldots C_n\} \quad (17)$$

$$h_2(\vec{C}) = m \quad (18)$$

3-2-4 盲化階段

- 選舉人 A 用自己的私鑰n_A對自己的公鑰PK_A做盲化後，再對密文摘要 m 進行運算產生β如式(19)。

$$\beta = m \cdot n_A \cdot PK_A \quad (19)$$

- 運算後將β傳給選務中心 B。

3-2-5 簽章階段

- 選務中心 B 收到選舉人 A 所傳送過來的β後，選務中心 B 隨選一個值e，e屬於Z_p^*，對β做運算產生r如式(20)。

$$r = e \cdot \beta \quad (20)$$

- 再利用選務中心 B 的私鑰n_B與隨選值e對β做運算產生簽章S如式(21)。

$$S = (r_B + e) \cdot \beta \quad (21)$$

- 後傳送$(\beta, (r, S))$給選舉人 A。

3-2-6 解盲化階段

- 選舉人 A 收到選務中心 B 傳來之$(\beta,(r, S))$後，對簽章 S 解盲化，計算S'如式(22) 。

$$S' = S - m \cdot n_A \cdot PK_B \quad (22)$$

- 並計算m'如式(23)。

$$m' = n_A \cdot (n_A - 1) \cdot m + m \quad (23)$$

- 算完成後選舉人 A 將$(S', m', r, \vec{C}, T)$傳給開票中心 C。

3-2-7 簽章驗證階段

- 以選舉人A所傳送過來的$(S', m', r, \vec{C}, T)$進行簽章驗證程序，開票中心 C 驗證式(24)等號是否成立。

$$r + m' S' = m' \cdot PK_B \quad (24)$$

- 如成立利用自己的私鑰對$\vec{C}$做解密後完成計票。

3-2-8 解密階段

- 開票中心 C 接著將加密選票進行解密動作，計算如下：

$$f_{m2p}(w,t) = C_0 - n_C \cdot T \quad (25)$$

$$(w,t) = f_{p2m}[f_{m2p}(w,t)] \quad (26)$$

- 將 w 還原成 $\bar{x}$ 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(27)：

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

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

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

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

$$w = \vec{x} = \{x_1, x_2, \ldots x_l\} \quad (27)$$

- 依序解開$\vec{C}$可以取得$\vec{V}$= { $V_1, V_2, \ldots, V_n$}進行點序列$\vec{V}$解密。

- 執行點轉成明文的動作，如式(28)，計算如下：

$$V_i = C_i - x_i \cdot C_{i-1} \quad , 1 \le i \le n \quad (28)$$

- 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(29)(30)，並列入開票計算。

$$\bar{V} = \{V_1, V_2, \ldots, V_n\} \quad (29)$$

$$f_{p2m}(\bar{V}) = \bar{v} \quad (30)$$

四、安全性分析

本研究所提盲簽章機制，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(Integrity)

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(11) $h_1(\bar{v}) = t$ 對明文進行雜湊運算得 v，並將 v 加入式 (15) $C_0 = [f_{m2p}(w,t) + q \cdot PK_c]$ 中，若第三方想要竄改明文偽造 v 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(Authenticity)

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(21) $S = (n_B + e) * \beta$與

(24) $r + m = S^r - m^r \cdot PK_B$，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(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，就可獲取自己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(21) $S = (n_B + e) * \beta$，選務中心將選票簽署後以證明此選票為合法有效票，可防止選務中心事後否認經由他簽署的。

- 隱匿性(Anonymity)

隱匿性是網際網路獨特的一種特性，在多數政治性的投票中，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；通常違反此原則是犯法的。如亮票行為。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(19)$\beta = m * r_A * PK_A$ 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，可達到選舉人選票資訊隱匿之特性。

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

本系統中如式子(19)$\beta = m * r_A * PK_A$、(20) $r = e * \beta$、(21) $S = (n_B + e) * \beta$，經過盲化且加密後的選票摘要，簽章者無法知道選舉人共投了幾張選票及開票中心無法得知真正的選舉者為何人，因為選舉者的公鑰透過選舉者的私鑰運算後無法追蹤適何人投的票，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(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資料的內容，以保證資料可以完整無誤的傳送至接收端。且不論收集到多少的傳輸封包，皆無法破解還原成原本的密文或是明文資料來逕行竄改偽造。本方法中式子(18) $h_2(\overline{C}) = m$，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。

綜整本研究與主要盲簽章法之安全性分析比較如表 1 所示。

表 1 本研究與植基於各系統盲簽章之安全性比較

演算法與安全性	RSA-Based Blind signatures (Chaum, 1982)	An ECC-Based Blind Signature Scheme (Jeng et.al., 2010)	本研究方法
完整性	V	V	V
不可否認性	V	V	V
隱匿性	X	V	V
不可偽造性	V	V	V
機密性	X	X	V
鑑別性	V	V	V
不可追蹤性	X	V	V

五、結論

明年(2014)本國將舉行地方首長七合一選舉[4]，屆時每個人手中將有三張以上的選票。若採取電子化投票，選舉一個類別需要簽章一次，一個投票者至少簽章三次；一千個投票者則須簽章三千次以上，將考驗選務中心的伺服器處理速度與網路傳輸速度。如果採用多文件一次盲簽章的方式處理，將大大減少簽章次數，在時間複雜度的計算上將會降低許多。本研究的盲簽章方式，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 演算法來的快速[5]，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，且可有效地隱匿選舉人身分，合乎現實中的不記名投票原則。

本研究所導入盲簽章及加密機制，滿足整性、不可否認性、隱匿性、不可偽造性、機密性、鑑別性及不可追蹤性等安全需求，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。未來更可應用於行動裝置上，提供利用行動裝置所進行的電子商務一個處理更加迅速與資料傳輸更加安全保密的一個解決方法。

參考文獻

中文部分

[1] 肖攸安，2006，橢圓曲線密碼體系研究，台北市：華中科技大學出版。

[2] 高嘉言，2009，植基於背包型態之橢圓曲線數位簽章系統設計，國防大學資訊管理學系研究所碩士論文。

[3] 楊倫青，2011，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，國防大學資訊管理學系研究所碩士論文。

[4] 東森新聞雲，政治中心，參見東森新聞雲網 http://www.ettoday.net/news/20120319/32827.htm. [visited in 2013/09/6]

[5] 蘇品長，2007，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。

英文部分

[6] D. Chaum, “Blind signatures for untraceable payments,” *In Proceedings of Advances in Cryptology—CRYPTO*, pp. 199-203, 1982.

[7] Chun-I, Fan, “An efficient multi-receipt mechanism for uncoercible anonymous electronic voting,” *Mathematical and Computer Modelling*, Volume 48, Issues 9–10, , pp. 1611–1627, 2008.

[8] F. G. Jeng, T. L. Chen, T. S. Chen, “An ECC-Based Blind Signature Scheme,” *journal of networks*, vol. 5, no. 8, pp. 921-928, 2010.

[9] N. Koblitz, “Elliptic Curve Cryptosystems,” *Mathematics of Computation American Mathematical Society*, vol. 48, pp. 203-209, 1987.

[10] V. S. Miller, “Use of Elliptic Curve in Cryptography,” *Advance in Cryptography-Crypto, New York: Spring-Verlag* , pp. 417-426, 1986.

[11] E. Mohammed, A. E. Emarah, and K. E. Shennawy, , “A blind signatures scheme based on ElGamal signature,” *IEEE/AFCEA EUROCOMM 2000 Information Systems for Enhanced Public Safety and Security*, pp. 51-53, 2000.

[12] T. Nakanishi, and Y. Sugiyama, “Unlinkable Divisible Electronic Cash,” *Information Security Lecture Notes in Computer Science*, vol. 1975, pp. 121-134, 2000.

[13] T. Nakanishi, M. Shiota, and Y. Sugiyama, “An Efficient on-line Electronic Cash with Unlinkable Exact Payments,” *Proceedings of the 7th Information Security Conference*, pp. 367-378, 2004.

[14] L. Wang, J. Guo, and M. Luo, “A More Effective Voting Scheme based on Blind Signature,” *Proceedings of International Conference on Computation Intelligence and Security*, vol. 2, pp. 1507-1510, 2006.

[15] S. H. Yun, and S. J. Lee, “An Electronic Voting Scheme based on Undeniable Blind Signature Scheme,” *Proceedings of IEEE 37th Annual International Carnahan Conference on Security Technology*, pp. 163-167, 2003.