建構在可驗證匿名性機制上之安全電子投票系統

沈宥融、伍麗樵
國立雲林科技大學電子與資訊工程研究所
wuulc@yuntech.edu.tw

摘要

本論文提出一建構於可驗證匿名性機制上之電子投票系統，本系統共有四個主體：投票者、認證中心、電子佈告欄及 *N* 個管理中心。本文所提出之可驗證匿名性機制是要求投票者在進行投票之前必須先與認證中心共同合作產生一具有唯一性(*Collision-freeness*)及可驗證(*Verifiable*)之匿名身份證(*Anonymous Identity*)，之後投票者藉此身份證以證明其選票的合法性及杜絕重複投票之不法行為；該機制保證除了投票者，沒有人可知道投票者與其匿名身份證的關係，即無人可知道投票者與其已投遞選票的關聯性。在本系統中，我們還運用了(*t, N*)門檻式 *ElGamal* 密碼系統及盲目簽章方法來保證投票者投遞於電子佈告欄之選票的私密性(*Privacy*)及不可更改性(*Integrity*)，使得投票者所投遞之選票內容必須在計票階段藉由 *t* 個以上的管理中心一同解密後才能被公開。

關鍵詞：電子投票、可驗證之匿名性、盲目簽章、(*t,N*)門檻式 *ElGamal* 密碼系統

一、簡介

隨著網際網路的蓬勃發展及密碼技術的進步，電子投票系統有逐漸取代傳統投票機制的趨勢，電子投票是透過便利的線上投票方式讓投票者能在任何地方參與選舉，增加投票者投票的意願。早期提出的電子投票系統[1~7, 9~11, 14~17, 19~20, 22, 24~26]就是在公開的網路架構下利用密碼學技術(如盲目簽章技術、同構加密方法或匿名管道技術等)建構一安全的電子投票系統，其目標是藉由網路進行投票並公告最後結果，以簡化傳統投票系統費時費力的人工作業。然而，早期運用盲目簽章技術來建構一安全的電子投票系統[3, 7, 9, 11, 15~17, 19]可能衍生出下列的問題：

- [3, 7, 9, 11, 15, 17]為了保證投票者的匿名性，投票者在投票前需先至認證中心進行註冊以確認投票者身份的合格性，之後再對其已加密的選票執行認證中心的盲目簽章以確保加密選票的合法性，但無法防範投票者進行重複投票的不法行為。
- 另外有些作法[16]是由認證中心(*Authentication Center*)核發給具有選舉資格的投票者一代表其身份的唯一憑證或是投票者會透過認證中心將選票投遞至計票中心，即由認證中心代替投票者進行投票行為，以防止重複投票的不法行為，然而，認證中心可以知道投票者與其選票間的關聯性甚至得知投票者所投遞的選票內容，這樣的作法無法保證選票的私密性及投票者的匿名性。

本文改進上述缺點，代表投票者合法身份之唯一憑證將由認證中心與投票者共同產生，認證中心無法得知憑證與投票者的關聯性，以達到匿名性，但若有惡意之投票者任意自行產生憑證，而導致與一合法投票者所得到之憑證相同時，僅有合法投票者才能證明其憑證確實是與認證中心共同產生，我們稱上述方法為一可驗證匿名性機制(*Collision-free and Verifiable Anonymity Scheme*)。

本論文的目的就是在可驗證匿名性機制上建構一安全電子投票系統。該系統是由投票者、認證中心、電子佈告欄及 N 個管理中心四個主體所組成，投票者在投票之前必須先與認證中心共同合作產生一具有唯一性及可驗證之匿名身份證，之後投票者可藉此身份證以證明其選票的合法性及杜絕重複投票之不法行為，沒有人(除了投票者)可知道投票者與其匿名身份證的對應關係，當然也無人可知投票者與其已投遞選票間的關聯性，達到投票者的匿名性。

總之，本系統除了建構一可驗證匿名性機制外，還結合匿名管道(*Anonymous Channel*)技術、(*t, N*)門檻式 *ElGamal* 密碼系統及盲目簽章(*Blind Signature*)技術以達到電子投票系統所需要的安全性，其安全性如以下所示：

- 系統的健全性(*Robustness*)：為了防止參與者有意或無意的中斷選舉的進行或影響最後選舉的結果，我們通常會讓此投票系統容忍合理數目的參與者所產生的錯誤行為，使得整個系統能正常的運作。

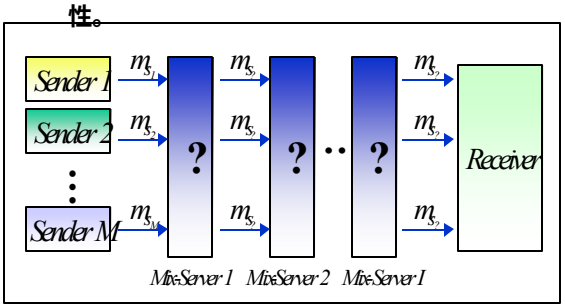
- **選票的私密性及不可更改性**(*Privacy & Integrity*)：**在整個系統未進行開票作業之前，除了投票者本身，沒有人可以事先知道或更改選票的內容，也就是說選票在整個選舉過程都會受到保護。**
- **選票的不可重複使用性**(*Un-reusability*)：**在投票流程中，每個合格的投票者都僅能投一張票，無任何投票者可投兩張以上的選票，而且沒有人可以複製別人已投遞的選票造成該選票無效或被重複計票。**
- **計票上的完整性**(*Completeness*)：**每一張選票在開票時都可以確實的被計算。**
- **投票者的合格性**(*Eligibility*)：**僅具有選舉資格的投票者才可進行投票。**
- **投票者的匿名性**(*Anonymity*)：**無任何人可得知任一具有選舉資格的投票者與其已投遞選票間的對應關係。**
- **全體可驗證性**(*Universal Verifiability*)：**每個人都可以驗證電子佈告欄上所投遞選票之合法性及正確性。**
- **投票位置的可移動性**(*Mobility*)：**投票者在任何地方都可進行投票行為。**

二、相關技術

以下介紹本系統所使用到的相關技術。

2.1 匿名管道(*Anonymous Channel*)

匿名管道[5，12，13]的目的是為了在傳送端及接收端之間建立一匿名的通道，使得傳送者於傳送訊息給予接收者時，接收者無法得知傳送者與訊息間的關聯性(如該訊息是由誰送出或該訊息送出的 *IP* 位置等)，匿名管道通常利用一混合網路(*Mix-net*)實現上述功能，如圖一所示。主要原理是藉由多個 *Mix Servers* 對多個傳送者送來的訊息進行重新排列的動作，再傳送給接收端，以達到傳送者的匿名性。



圖一：匿名管道

2.2 盲目簽章(*Blind Signature*)

Chaum[6]**於** 1982 **年提出，目的是讓簽章者無法得知他所簽署的訊息內容，但也無法否認此已簽章訊息的合法性。例如簽章者** *Bob* **其公開金匙及私人金匙分別為** $PK_{Bob}=(e_{Bob},n)$ **與** $SK_{Bob}=(d_{Bob},n)$ **，今** *Alice* **有一訊息** m **需** *Bob* **作** *RSA* **數位簽章但** m **的內容不能為** *Bob* **所得知，那麼** *Alice* **須遵循下列步驟以得到** *Bob* **的簽章：**

- ***Blinding phase:***
  Alice **選擇一數值** $k\in_R Z_n$(**符號** R **是指** k **為一隨機值，**$Z_n=\{0,1,\ldots,n\text{-}1\}$**)，此** k **為一盲目因子**(*blinding factor*)**且** $g.c.d(k,n)=1$ **；接著將** $m'=m\cdot k^{e_{Bob}}\pmod n$ **傳送給** *Bob*。
- ***Signing phase:***
  Bob **於收到訊息** m' **後，對此訊息作數位簽章可獲得** $Bs=(m')^{d_{Bob}}=(m\cdot k^{e_{Bob}})^{d_{Bob}}=m^{d_{Bob}}\cdot k\pmod n$ **，並將** *Bs* **值回傳給** *Alice*。**其中，因** *Bob* **不知道** k **，所以無法知道** m **的內容。**
- ***Unblinding phase:***
  只有知道 k **值的** *Alice* **在收到回傳值** *Bs* **後，經過** $Bs\cdot k^{-1}$ **的運算才可得到訊息** m **經過** *Bob* **的簽章** $Sig=Bs\cdot k^{-1}=m^{d_{Bob}}\pmod n$ **，然而為了防止** *Bob* **竄改訊息內容，** *Alice* **可計算** $Sig^{e_{Bob}}\bmod n$ **確認結果是否等於** m **，若** $m\equiv Sig^{e_{Bob}}\pmod n$ **則得證** *Bob* **並無竄改訊息。**

2.3 (*t*,*N*) 門檻式 *ElGamal* 密碼系統 (*Threshold ElGamal Cryptosystem*)

(*t*, *N*)**門檻式** *ElGamal*[25]**密碼系統**[4]**是由** N **個管理中心合力產生一加密金匙及解密金匙，其中解密金匙會被分享出** N **把次密金匙給所有管理中心保管。當以加密金匙對一訊息加密時，只需有** t **個以上擁有次密金匙的管理中心合作，就可對加密的訊息進行解密。與早期** (*t*, *N*)**門檻式密碼系統**[23]**的不同點在於**[4]**不需要一特別的金匙產生中心**(*Dealer*)**來產生加解密金匙及分配次密金匙的工作，**[4]**完全是由所有的管理中心共同合作產生加解密金匙及分享次密金匙，如此可防止金匙產生中心洩露各個次密金匙的可能性。**

下文將說明(*t*, *N*)**門檻式** *ElGamal* **密碼系統的金匙產生演算法及加解密演算法，下文中所使用的** p **及** q **是兩個很大的質數，** $q\mid(p-1)$ **而且有一** $g\in Z_p^*$**，** p**、** q **及** g **被公開於電子佈告欄**(*Bulletin Board*)**。**

- **金匙產生演算法[21]:**
  - **首先，每個管理中心** A_i **需各別產生一隨機值** $d_i\in_R Z_q$ **，** $i=1,\ldots,N$ **，計算** $h_{Ai}=g^{d_i}\pmod p$**，並公開** h_{Ai} **至電子佈告欄。當** N **個管理中心完成上述動作之後，任何人即可利用電子佈告欄上的資料計算出加密金匙**

$h=\prod_{i=1}^{N} h_{Ai}=g^{\sum_{i=1}^{N} d_i} \pmod{p}$；而解密金鑰 $s=\sum_{i=1}^{N} d_i \pmod{q}$，但沒有人(除了 t 個以上的管理中心合作)可求得 s，因為要從任一 h_{Ai} 求得相對應的 d_i 是一 *NP-Complete* 的問題[18]。

- 每個管理中心 A_i 接著產生一最高次方為 t-1 的多項式 $f_i(z)=f_{i0}+f_{i1}\cdot z+\ldots+f_{i,t-1}\cdot(z^{t-1}) \pmod{q}$，$f_i(0)=f_{i0}=d_i$，並計算 $F_{ij}=g^{f_{ij}} \bmod p$，$j=0, \ldots, t-1$，然後將 F_{ij} 公開在電子佈告欄。
- 每個管理中心 A_i 秘密的傳送 $s_{ij}=f_i(j)$ 給其它的管理中心 A_j，$j=1, \ldots, N$。
- 每個管理中心 A_i 由 $g^{s_{ji}} \equiv \prod_{l=0}^{t-1}(F_{jl})^{i^l} \pmod{p}$ 方法驗證每個 s_{ji} 的正確性，並於確認完成後，得到其次密金匙 $s_i=\sum_{j=1}^{N} s_{ji} \pmod{q}$ (即 $s_i=f(i)=\sum_{j=1}^{N} f_j(i)=s+\sum_{j=1}^{N}(f_{j1}\cdot i)+\ldots+\sum_{j=1}^{N}(f_{j,t-1}\cdot i^{t-1}) \pmod{q}$)，再計算 $h_i=g^{s_i} \pmod{p}$ 公佈至電子佈告欄。之後只要有 t 個以上擁有次密金匙 s_i 的管理中心合作(假設 t 個管理中心的集合為 Λ，$\Lambda=\{i \mid i$為t個管理中心的$ID,\ 1\le i\le N\}$)，便可利用下列 *Lagrange* 多項式插入法計算出解密金匙 s：$s=f(0)=\sum_{i\in\Lambda}(s_i\cdot\prod_{j\in\Lambda\setminus\{i\}}\frac{j}{j-i}) \pmod{q}$。

◆ 加解密演算法

- h 為系統公告之加密金匙，g 為公開參數，假設有一使用者對明文 m 加密可得到密文 $(c_1,c_2)=(g^b, h^b m)$，$b\in_R Z_q$ 為一亂數值。
- 當有 t 個以上的管理中心要合力對 (c_1,c_2) 進行解密時，每個管理中心 A_i 需計算 $D_i=c_1^{s_i}$ 並公開於電子佈告欄，之後此 t 個以上的管理中心(假設 t 個管理中心的集合為 Λ，$\Lambda=\{i \mid i$為t個管理中心的$ID,\ 1\le i\le N\}$)就可利用下列公式得到明文：

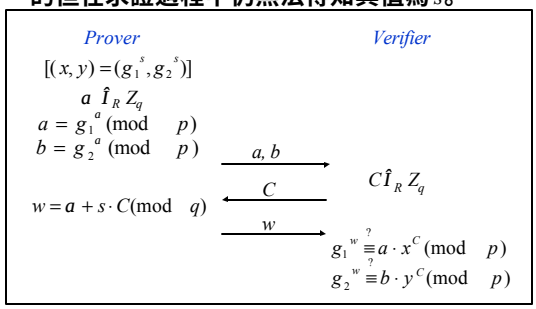
$$m=c_2/\prod_{i\in\Lambda}(D_i)^{l_{i,\Lambda}},\quad l_{i,\Lambda}=\prod_{j\in\Lambda\setminus\{i\}}\frac{j}{j-i}$$

。

- 在解密時，若有某個管理中心 A_i 故意不使用其次密金匙 s_i 去計算 D_i，則無法求出正確的明文 m，故每個管理中心在公開 D_i 於電子佈告欄時，還需產生一些驗證參數讓任何人都可利用 2.4 節所介紹的 *NI-PKE* 證明方法驗證管理中心 A_i 確實使用之前所公告 $h_i=g^{s_i}$ 之 s_i 去計算 D_i，所以每個管理中心公開 $D_i=c_1^{s_i}$ 時還需公開相對應的驗證參數 $(C,\ w)$，讓任何人驗證 h_i 與 D_i 是否都是用 A_i 擁有的次密金匙 s_i 所計算得到的結果，其中 $C=H(h_i \| D_i \| g^a \| (c_1)^a)$，$a\in_R Z_q$ 是管理中心 A_i 隨機產生的一亂數值，$w=a-s_i\cdot C \pmod{q}$。

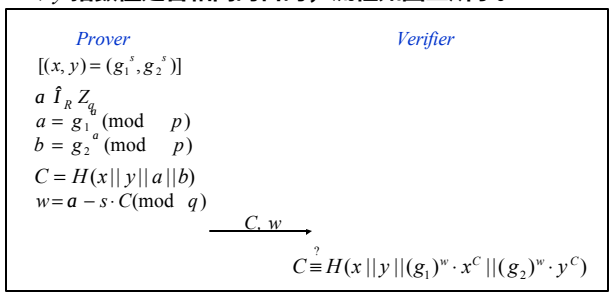
2.4 零知識離散對數等式證明法 (*Proof of knowledge for equality of discrete logs*，簡稱 *PKE*)

在[4, 8]中是假設一證明者(*Prover*)有一公開的數值組合 $(g_1,\ g_2,\ x,\ y)$，其中 $g_1,\ g_2\in Z_p$，$x=g_1^s \pmod{p}$ 及 $y=g_2^s \pmod{p}$，p 及 q 是兩個很大的質數而且 $q\,|\,(p-1)$，$r\in Z_q$ 不公開。只有知道 s 值的證明者可依循圖二的流程向求證者(*Verifier*)證明 $\log_{g_1} x\equiv\log_{g_2} y$，即任一求證者可利用圖二之 *PKE* 方法來求證 x，y 的指數值是相同的但在求證過程中仍無法得知其值為 s。



圖二：*PKE* 方法

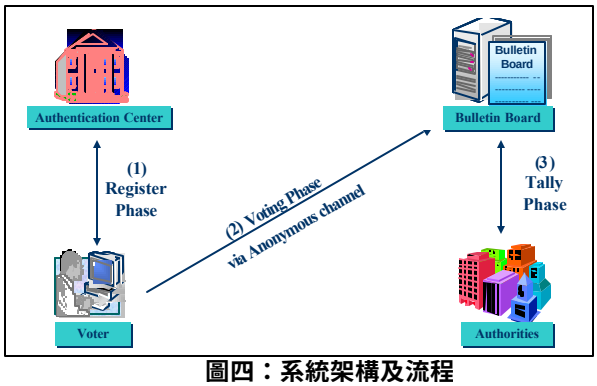
由圖二可知 *PKE* 需要三次的訊息交換後才可完成整個證明流程，在 [4, 8]中還提出了一非交互式(*Non-interactive*)的 *PKE* 方法，簡稱 *NI-PKE*，只需一次的訊息交換即可達到求證 x、y 指數值是否相同的目的，流程如圖三所示。



圖三：*NI-PKE* 方法

三、系統架構

本電子投票系統是由下列四個主體所組成：具有選舉資格的投票者、確認投票者身份的認證中心、公佈相關投票資訊的電子佈告欄以及在計票過程中負責驗證選票合法性及開票的 N 個管理中心。整個系統架構及流程如圖四所示。



圖四：系統架構及流程

3.1 系統主體

- **投票者**(*Voter*)：投票者是一具有選舉資格的主體，需先向認證中心註冊，取得一匿名身份證(*Anonymous Identity*，簡稱*AID*)，並將其已選擇候選人的加密選票經過認證中心的盲目簽章後，才可進行投票行為。
- **認證中心**(*Authentication Center*，簡稱*AC*)：認證中心猶如一政府機關，擁有投票者的相關身份資料。主要是負責投票者身份的識別，僅具有選舉資格的投票者才能與認證中心合力產生一代表合法投票者的匿名身份證(*AID*)，接著對此投票者所加密的選票盲目簽章，達到選票的不可更改性及唯一性。在本文中，我們假設認證中心是一誠實的主體。
- **電子佈告欄**(*Bulletin Board*)：電子佈告欄目的是收集選票及選舉過程中相關訊息的公佈，例如各個主體公開金匙的公佈、選票的驗證參數等等。一電子佈告欄具有以下特性：(*a*)所有的主體皆可傳送資料至電子佈告欄，但是當投票者投票時，該投票摘要(包括加密選票及匿名身份證)已附有認證中心的盲目簽章，所以電子佈告欄是以認證中心的 RSA 公開金匙確認加密選票的合法性；(*b*)所有人都可以閱讀電子佈告欄上的所有內容；(*c*)電子佈告欄上的資訊不可被任何人刪除、修改，甚至破壞，以達到公正、公開的特性。
- N **個管理中心**(*Authorities*)：N 個管理中心目的是負責對所有選票進行開票，也包括針對電子佈告欄上的相關投票訊息進行驗證，例如簽章訊息的合法性、選票的有效性、各個管理中心次解密金匙的正確性及計票的完整性等等。

3.2 系統流程

表一：符號說明

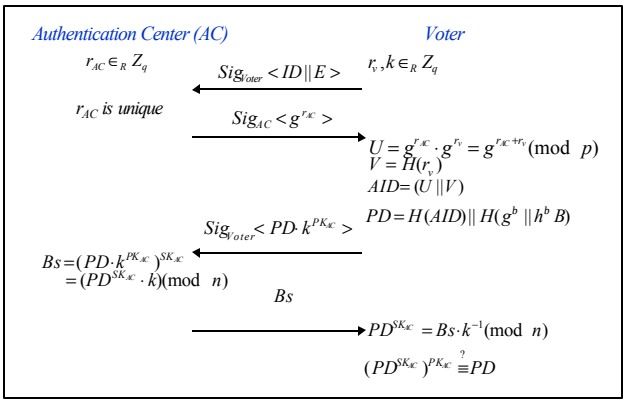
符號	說明
B	投票者所要投的選票，$B \in \{B_1, \ldots, B_l\}$，$l$為候選人人數。
p, q N	兩個很大的質數而且 $q \mid (p-1)$。 兩個很大質數(p_1 及 p_2)的乘積，而且 $n > p$。
g	一生成元(*generator*)，$g \in Z_p^*$，其序(*order*)為q。
h	所有管理中心共同產生的加密金匙 $h = g^s$，s 亦是所有管理中心共同產生的解密金匙。
s_i	次密金匙，是解密金匙s所秘密分享的金匙之一並交由A_i保管。
$H(Data)$	對$Data$作雜湊運算
PK_A, SK_A	使用者A的RSA公開金匙及私人金匙
$Data^{PKA}$	以使用者A的公開金匙對$Data$作非對稱式加密
$Sig_A<Data>$	使用者A對$Data$作數位簽章而且 $Sig_A < Data >= Data, < H(Data) >^{SK_A}$

我們的系統流程分成註冊流程(*Register Phase*)、投票流程(*Voting Phase*)及計票流程(*Tally Phase*)。在進行整個系統流程之前，假設每個主體都已擁有自己的 *RSA* 公開金匙及私密金匙，而且所有管理中心(*Authorities*)依循(*t, N*)門檻式 *ElGamal* 密碼系統方法已各別得到一把次密金匙s_i ($i = 1, \ldots, N$)並且將各個管理中心 A_i 所產生的 $h_{Ai} = g^{d_i}$ (A_i 各別產生的隨機值 $d_i \in_R Z_q$)及以該次密金匙s_i 所計算之 $h_i = g^{s_i}$ 都公開於電子佈告欄(*Bulletin Board*)，至於系統之加密金匙 $h = \prod_{i=1}^{N} h_{Ai}$ 則由電子佈告欄計算並公佈。表一是本文所會使用到的符號及其說明。

本文所提出之一可驗證匿名性機制即要求投票者於註冊流程中與認證中心合力產生一可代表投票者的匿名身份證(*AID*)，此 *AID* 將保證投票者的匿名性及不可重複投票的特性，而且該機制可遏止惡意投票者隨意自行產生 *AID* (於 3.2.2 節投票流程中說明)，因為惡意投票者若產生一與合法投票者相同之 *AID*，將會因無法向認證中心證明其 *AID* 的合法性而犧牲他可投票的權利。以下將針對各個流程作一詳細描述。

3.2.1 註冊流程(*Register Phase*)

註冊流程如圖五所示。



圖五：註冊流程

***Voter* ® *AC*: Sig_{Voter}<*ID*‖*E*>** **(1)**

首先，投票者以其 *RSA* 私人金匙對其身份資料(*ID*)及此次選舉代碼(*E*)作簽章，然後傳至認證中心。此時認證中心可由投票者的 *ID* 及 *RSA* 公開金匙(PK_{Voter})核對投票者身份，若是滿足此次選舉資格的投票者，便將此訊息儲存於註冊名單(*Register List*)中。

***AC* ® *Voter*: $Sig_{AC} < g^{r_{AC}} >$** **(2)**

認證中心於確認完投票者身份後，挑選一隨機值 $r_{AC} \in_R Z_q$，r_{AC} 必須具有唯一性，接著傳送 $Sig_{AC} < g^{r_{AC}} >$ 給投票者，並記錄 r_{AC} 與投票者 *ID* 的對應關係，其中認證中心對 $g^{r_{AC}}$ 簽章的目的是為了保證 $g^{r_{AC}}$ 完整性及合法性。此時投票者也隨機挑選一數值 $r_v \in_R Z_q$ 並計算 $U = g^{r_{AC}} \cdot g^{r_v} = g^{r_{AC}+r_v}$ 及 $V = H(r_v)$，而得到一代表此投票者的匿名身份證 $AID = (U \| V)$，由於 *AID* 最後是由投票者自行作出且認證中心並不知道 r_v，所以除了投票者外，無人可得知投票者與其 *AID* 的關係。

定理 1. 認證中心(*AC*)及投票者(*Voter*)所合力產生的 *AID* 具有唯一性。

證明： 利用矛盾證法，設有一 $AID = (U \| V)$，而且存在另一 $AID' = (U' \| V')$，$AID \equiv AID'$，則 $U \equiv U'$、$V \equiv V'$。然而，因為認證中心所產生的 r_{AC} 必不相同，即 $r_{AC} \neq r_{AC}'$，故當 $U \equiv U'$ 時 $\Rightarrow g^{r_{AC}+r_v} \equiv g^{r_{AC}'+r_v'} \Rightarrow r_v \neq r_v' \Rightarrow V \neq V'$，與假設矛盾，即得證 *AID* 具有唯一性。 Q.E.D.

***Voter* ® *AC*: Sig_{Voter}<*PD*‖ $k^{PK_{AC}}$>** **(3)**
***PD* = *H*(*AID*)‖*H*(g^b‖h^b*B*)**

投票者隨機產生一 $b \in_R Z_q$ 對已決定候選人的選票(*B*)用系統的加密金匙 *h* 加密，然後投票者會將 *AID* 及加密的選票 $g^b \| h^b B$ 各別作雜湊函數運算而得到投票摘要(*PD*)，再挑選一盲目因子 *k* 並以認證中心的 *RSA* 公開金匙加密後與 *PD* 相乘，並要求認證中心對此訊息 $PD \cdot k^{PK_{AC}} \pmod{n}$ 作盲目簽章。

AC* ® *Voter*: *Bs **(4)**
Bs* = (*PD*‖ $k^{PK_{AC}}$)$^{SK_{AC}}$ mod *n* = (*PD*$^{SK_{AC}}$‖ *k*) mod *n

認證中心將作過盲目簽章的 *Bs* 回傳給投票者並記錄 *Bs* 與投票者 *ID* 的對應關係。當投票者收到盲簽訊息 *Bs* 後，可以計算 $(Bs \cdot k^{-1})^{PK_{AC}}$，若其結果為 *PD*，則可確認 *PD* 並沒有被認證中心修改過，即得到具有認證中心的簽章 $PD^{SK_{AC}}$。

3.2.2 投票流程(*Voting Phase*)

***Voter* ® *Bulletin Board*: *AID*‖g^b‖h^b*B*‖*PD*^{SKAC}** **(5)**

在投票者得到認證中心對投票摘要的數位簽章 $PD^{SK_{AC}}$ 後，即以 $AID \| g^b \| h^b B \| PD^{SK_{AC}}$ 的訊息透過匿名管道(*Anonymous Channel*)傳遞至電子佈告欄(*Bulletin Board*)，也就是進行所謂的投票行為。電子佈告欄於收到上述訊息後，首先以認證中心的 *RSA* 公開金匙確認 *PD* 是否有認證中心的簽章，以確認 $AID \| g^b \| h^b B$ 的完整性及合法性，接著核對 *AID* 是否具有唯一性，以防止重複投票的情形，若上述程序都能通過驗證，則電子佈告欄會將此訊息放置於指定的公佈區域。之後任何人也可以上述的方式進行驗證電子佈告欄上任一加密選票的完整性、合法性及唯一性。

在本系統中，若具有選舉資格的惡意投票者在註冊的過程中蓄意自我產生 *AID* 進而導致與合法投票者的 *AID* 相同，而且此惡意投票者還讓包含此 *AID* 的投票摘要(*PD*)經過認證中心的盲目簽章並進行投票行為，會有下列兩種情況：

Case 1： 此蓄意自我產生 *AID* 的投票者先行投票，當合法投票者要進行投票時便會遭到電子佈告欄的否決，那麼此合法投票者需依循下述方式處理以達到 *AID* 的可驗證性：

Step1: 合法的投票者需傳送 $Sig_{Voter}(ID \| PD \| r_v \| k \| E)$ 給認證中心要求重新申請 *AID*，因認證中心之前已記錄相對應於投票者 *ID* 之 r_{AC}，所以認證中心先從上述傳送的訊息取得 r_v 及 $H(AID)$，接著計算 $H(AID') = H((g^{r_{AC}} \cdot g^{r_v}) \| H(r_v))$ 以驗證是否 $H(AID') \equiv H(AID)$，若等式成立，則認證中心確認此投票者遵循可驗證匿名性機制產生其匿名性身份證 *AID*，再繼續執行 Step 2，否則認證中心將拒絕此投票者重新申請 *AID*。

Step2: 認證中心從資料庫中取得該投票者之 *Bs* 及 Step 1 投票者傳送的訊息取得 *k* 以驗證

是否 $(Bs \cdot k^{-1})^{PK_{AC}} \stackrel{?}{\equiv} PD \pmod{n}$，若等式成立認證中心再繼續執行 Step 3，否則認證中心將拒絕此投票者重新申請 *AID*。

Step3: 認證中心驗證電子佈告欄上具有相同 *AID* 值的 *PD* 是否與 Step 1 上投票者所傳來的 *PD* 值相同，若不同則表示電子佈告欄上已加密的選票的確非此投票者所投遞，那麼認證中心將會撤銷此 *AID* 並讓該投票者重新執行註冊流程；撤銷的 *AID* 會被公佈於撤銷名單 (*Revoking List*)中。若二者的 *PD* 值相同，則表示投票者已成功的將加密選票連同 *AID* 投遞至電子佈告欄，認證中心將拒絕此投票者重新申請 *AID*。(注意：在 Case 1中，惡意投票者任意產生的 *AID* 將無法通過 Step 1的驗證，而 Step 2 及 Step 3 的目的是為了防止合法的投票者藉由通過 Step 1 的驗證方式而進行重複投票之不法行為。)

Case 2： 合法的投票者先完成投票流程，那麼與他有相同 *AID* 的惡意投票者在進行投票時將會遭到電子佈告欄的拒絕。(注意：惡意投票者的 *AID* 是自行產生，雖然已經過認證中心簽章，但他無法如上述的證明方式證明其 *AID* 是與認證中心合力產生。)

3.2.3 計票流程(*Tally Phase*)

$A_i \rightarrow$ ***Bulletin Board***: $(g^b)^{s_i} \| C_i \| w_i$ (i=1, …, N) (6)

在投票時間截止後，整個系統就會進入計票流程，認證中心會將註冊名單及撤銷名單公開於電子佈告欄，因為註冊名單上會列有每個投票者向認證中心註冊的資訊 $Sig_{Voter}(ID \| E)$，那麼任何人都可以以各個投票者的 *RSA* 公開金匙確定註冊名單上的正確性及確認名單上的人數應大於或等於投票的人數(有可能投票者於註冊後並未進行投票行為)。之後，每個管理中心 A_i 會從每個投票者所投遞的選票取得 g^b 並公告 $(g^b)^{s_i}$ 及證明 $\log_g h_i \equiv \log_{g^b} (g^b)^{s_i}$ 所需的驗證參數 (C_i, w_i) 於電子佈告欄，其中 h_i 已於各個管理中心得到其次密金匙後公開於電子佈告欄，而 $C_i = H(h_i \| (g^b)^{s_i} \| g^{a_i} \| (g^b)^{a_i})$，$a_i \in_R Z_q$ 是管理中心 A_i 隨機產生的一亂數值，$w_i = a_i - s_i \cdot C_i \pmod{q}$。

只需有 t 個以上的管理中心(假設 t 個管理中心的集合為 L)將其 $(g^b)^{s_i}$ 及 (C_i, w_i) 公開於電子佈告欄就可遵循下列 (t, N) 門檻式 *ElGamal* 密碼系統的解密方法對每張已加密選票進行解密而得到選票內容 $B \in \{B_1, \ldots, B_l\}$。

$$Y = h^b B \qquad \text{且} \qquad X = \prod_{i \in \Lambda} (g^b)^{s_i l_i} \quad ,$$

$$l_i = \prod_{j \in \Lambda \setminus \{i\}} \frac{j}{j-i} \quad \Rightarrow B = \frac{Y}{X} = \frac{h^b B}{(g^b)^s}$$

然而當 $B \notin \{B_1, \ldots, B_l\}$ 時可能有下述兩種情況：投票者原本所投遞的選票是一廢票或是 t 個管理中心有一個或多個管理中心未合法地使用他們所擁有的次密金匙計算 $(g^b)^{s_i}$ 而導致無法正確地求解出選票內容。後者的情況我們可利用各個管理中心所公開的驗證參數 (C_i, w_i) 以 2.4 節 *NI-PKE* 方法求證該次密金匙的正確性 (即驗證是否 $\log_g h_i \equiv \log_{g^b} (g^b)^{s_i}$)，故只要有 t 個以上的管理中心通過上述的驗證而 $B \notin \{B_1, \ldots, B_l\}$ 時即表示此選票原本就是一廢票。將每個投票者解密後的選票內容公佈於電子佈告欄後，即可由所有管理中心進行計票，並將最後選舉結果以其 *RSA* 私人金匙 SK_{A_i} 簽章後，公開於電子佈告欄上。此時每個人也可於電子佈告欄求證計票上的完整性，即所有合法的選票(*Valid Ballot*)都會被正確地計算。

四、討論與分析

在這一節中，我們將討論及分析本系統所具備的安全性：

4.1 投票者的合格性(*Eligibility*)

在(1)中，投票者在註冊時是以其所擁有的 *RSA* 私密金匙對身份資料(*ID*)作簽章，讓認證中心以投票者的公開金匙及 *ID* 確認投票者的選舉資格，若是一合格投票者，則對投票者的投票摘要進行盲目簽章；之後投票者在(5)中電子佈告欄是以認證中心的公開金匙確認此投票摘要上盲目簽章的合法性，間接的確認投票者身份的合格性。

4.2 投票者的匿名性(*Anonymity*)

每個合格的投票者與認證中心會依循本文所提出的可驗證匿名性機制的流程共同產生一具有唯一性及可驗證性的匿名身份證 (*AID*)，而且除了投票者外，無任何人可得知投票者與其 *AID* 間的關聯性，此外投票者是透過匿名管道(*Anonymous Channel*)投票至電子佈告欄，所以沒有人可得知選票及投票者間的關聯性(如投票者真正身份、*IP* 位址等)，而達到投票者的匿名性。

4.3 選票的私密性及不可更改性(*Privacy and Integrity*)

每張選票(B)首先會經由投票者本身產生的隨機值 b 加密，加密選票為 $(g^b, h^b B)$，因為在 N 個管理中心中需 t 個以上擁有此系統之次密金匙的管理中心才能對選票進行解

密，故除了投票者本身外，任何人除非能收集 t 把次密金匙，否則無法知道投票者選票的內容以保障選票的私密性。而且整個投票者的投票摘要 (PD) 會經過認證中心對其作盲目簽章，保證其不可更改性。

4.4 選票的不可重複使用性(*Un-reusability*)

投遞至電子佈告欄的投票內容包含了投票者的匿名身份證 (AID)、加密的選票 ($g^b,\ h^b B$) 及經過認證中心盲目簽章的投票摘要 ($PD^{SK_{AC}}$)，故投票者進行投票行為(如(5))時，電子佈告欄以認證中心的 RSA 公開金匙 PK_{AC} 驗證 $AID \| g^b \| h^b B \| PD^{SK_{AC}}$ 這段訊息的完整性及合法性後；接著檢查 AID 的唯一性，若有一相同的 AID 已存在於電子佈告欄，那麼此 AID 及其相關訊息將被拒絕公開於電子佈告欄上，以防止重複投票的情形。

假如此相同 AID 的擁有者是一合法的投票者(即完全遵循本系統的流程進行投票而遭到電子佈告欄的拒絕公佈該投票訊息時)，那麼該投票者可利用 3.2.2 節 AID 的可驗證性向認證中心證明電子佈告欄上相對應於同一 AID 的資訊並非他所投遞，而撤銷此 AID，並與認證中心重新合作產生一新 AID 再次進行投票，以保障此合法投票者的權利。然而，若有合法投票者想藉由 AID 的可驗證性進行重覆投票之不法行為將會被認證中心拒絕(如 3.2.2 節 Case 1 的 Step 2 及 Step 3)。

4.5 系統的健全性(*Robustness*)

在我們的電子投票系統中，為了防止參與者有意或無意的中斷選舉的進行或影響最後選舉的結果，我們使用了 (t, N) 門檻式 $ElGamal$ 密碼系統讓 N 個管理中心($Authorities$)中只需有 t 個以上的管理中心合作就可進行計票流程，即對所有的選票進行解密，所以當有 N-t 個管理中心有意、無意的發生錯誤行為時，本系統將不受影響。此外，每個擁有次密金匙的管理中心 A_i 在本系統進行前會先公開其相對應之公開金匙 $h_i = g^{s_i}$，故我們可由 2.4 節 NI-PKE 方法在計票流程中保證各個管理中心是以其所保管之次密金匙對每個選票進行解密，以排除惡意管理中心之不法行為。

當有惡意的合格投票者蓄意自行產生匿名身份證(AID)，令此匿名身份證與其他合法投票者相同時，合法投票者在無法投遞選票至電子佈告欄的情況下，可依本文提出之可驗證匿名性機制讓認證中心將此惡意產生的 AID 撤銷，即視同惡意投票者放棄投票權利，然後合法投票者再與認證中心合作產生一新 AID 並再次進行投票行為。若投票者故意投廢票或於註冊後不進行投票將不影響選舉的進行及結果，所以此系統具有健全性。

4.6 計票上的完整性(*Completeness*)

從(5)和(6)得證每一張選票都需要 t 個以上擁有次密金匙之管理中心的集合才能共同進行解密以得到選票的內容，並且每個管理中心在進行解密的同時為了證明其解密選票之金匙的正確性，每個管理中心會依 2.4 節 NI-PKE 方法於電子佈告欄公開其金匙的驗證參數，即驗證各個管理中心其擁有之次密金匙的正確性。此外，解密的流程及整個計算票數的作業都會公佈於電子佈告欄，所以每個人都可確認計票時的完整性。

4.7 全體可驗證性(*Universal Verifiability*)

本系統會將投票所須的相關資料公佈於電子佈告欄，如認證中心及各個投票者的 RSA 公開金匙、選舉註冊名單、選舉撤銷名單、每個投票者的投票資訊(包括唯一的匿名身份證、加密選票及經過認證中心盲目簽章的投票摘要)，還有在計票流程中，解密的程序、金匙的驗證及選舉結果都公佈於電子佈告欄上，所以任何人都可對佈告欄上的資訊進行驗證，而達到全體可驗證性。

4.8 投票位置的可移動性(*Mobility*)

本系統並不需要固定位置的投票站，投票者只需透過網際網路就可進行投票，消除了地理環境上的限制，這樣的特性可提高投票者的意願。

五、結論

在本電子投票系統中，我們提出一可驗證匿名性機制讓具有選舉資格的投票者可與認證中心共同合作產生一匿名身份證 (AID)，此匿名身份證將具有三個特性：唯一性、匿名性及可驗證性，即除了投票者外，無任何人可得知此匿名身份證與投票者間的關聯性，而且此匿名身份證將是唯一的，以杜絕重複投票之不法行為。當有惡意之投票者任意產生一匿名身份證，而導致與一合法投票者所得到的匿名身份證相同時，僅有合法投票者可向認證中心證明此匿名身份證是合法的與認證中心一同產生，以達到可驗證的特性。該機制可遏止惡意投票者隨意自行產生 AID，因為惡意投票者若產生一與合法投票者相同的 AID，將會因無法向認證中心證明其 AID 的合法性而犧牲他可投票的權利。

除此之外，我們還利用盲目簽章方法及 (t, N) 門檻式 $ElGamal$ 密碼系統來保障選票在整個選舉過程的私密性($Privacy$)、不可更改性($Integrity$)及系統的建全性($Robustness$)，並保證所有選票在計票過程中能確實的被計算及全體可驗證性($Universal\ Verifiability$)，以符合電子投票系統的安全特性。

參考文獻

[1] J. Benaloh, "Verifiable secret-ballot elections", PhD thesis, Computer Science, Yale University, New Haven, 1987.

[2] J. Benaloh, D. Tuinstra, "Receipt-free secret-ballot elections", Proc. of the 26th Symp. on Theory of Computing, ACM, pp. 544-553, 1994.

[3] L. F. Cranor, R. K. Cytron, "Sensus: a security-conscious electronic polling system for the Internet", System Sciences, 1997, Proc. of the Thirtieth Hwaii International Conference on, Vol. 3, pp. 561 –570, January 1997.

[4] R. Cramer, R. Gennaro, B. Schoenmakers, "A secure and optimally efficient multi-authority election scheme", Proc. of Advances in Cryptology-Eurocrypt '97, pp. 103-118, 1997.

[5] D. Chaum, "Untraceable electronic mail, return address, and digital pseudonyms", Communications of the ACM, Vol. 24, No. 2, pp. 84-88, 1981.

[6] D. Chaum, "Blind signatures for untraceable payments", In Advances in Cryptology-CRYPTO'82, Springer-Verlag, pp. 199-203, 1983.

[7] D. Chaum, "Elections with unconditionally-secret ballots and disruption equivalent to breaking RSA", Advances in Cryptology- Eurocrypt'88, LNCS Vol. 330, Springer-Verlag, pp. 177-182, 1988.

[8] D. Chaum, T. P. Pederson, "Wallet databases with observers", Proc. of Advances in Cryptology-Crypto'92, pp. 89-105, 1992.

[9] A. Fujioka, T. Okamoto, K. Ohta, "A practical secret voting scheme for large scale elections", Proc. of Advances in Cryptology-Auscrypt'92, pp. 244-251.

[10] M. Hirt, K. Sako, "Efficient receipt-free voting based on homomorphic encryption", Proc. of Advances in Cryptology-Eurocrypt 2000, pp. 539-556, 2000.

[11] J. K. Jan; Y. Y. Chen; Y. Lin, "The design of protocol for evoting on the Internet", Security Technology, 2001 IEEE 35th International Carnahan Conference on, pp. 180 –189, October 2001.

[12] M. Jakobsson, "A practical MIX", Proc. of Advances in Cryptology-Eurocrypt'98, pp. 448-461, 1998.

[13] M. Jakobsson, "Flash mixing", Proc. of ACM 18th Symp. on Principles of Distributed Computing, pp. 83-89, 1999.

[14] M. Jakobsson, A. Juels, R. Rivest. "Making mix nets robust for electronic voting by randomized partial checking", Proc. of the 11th USENIX Security Symposium, USENIX 2002, pp. 339-353, 2002.

[15] W. S. Juang, C. L. Lei. "A secure and practical electronic voting scheme for real world environments", IEICE Transaction on Fundamentals of Electronics, Communications and Computer Science, E80A (1), pp. 64-71, January 1997.

[16] J. Karro, J. Wang, "Towards a practical, secure and very large scale online election", Proc. 15th Annual Computer Security Applications Conference (ACSAC'99), pp. 161-169, 1999.

[17] W. C. Ku, S. D. Wang, "A secure and practical electronic voting scheme", Computer Communications, Vol. 22, Issue 3, pp. 279 –286, February 1999.

[18] A. Menezes, P. C. van Oorschot, and S. Vanstone. *Handbook of Applied Cryptography*, CRC Press, 1997.

[19] T. Okamoto, "Receipt-free electronic voting schemes for large scale elections", Proc. of Workshop on Security Protocols'97, LNCS Vol. 1361, Springer-Verlag, pp. 25-35, 1997.

[20] C. Park, K. Itoh, K. Kurosawa, "Efficient anonymous channel and all/nothing election scheme", Proc. of Advances in Cryptology-Eurocrypt'93, pp. 248-259, 1993.

[21] T. P. Pedersen, "A threshold cryptosystem without a trusted party", Proc. of Advances in Cryptology-Eurocrypt '91, pp. 522-526, 1991.

[22] A. Riera, J. Borrell, "Practical approach to anonymity in large scale electronic voting", Proc. of the 1999 Network and Distributed Systems Security Symposium (NDSS'99), pp. 69-82, 1999.

[23] A. Shamir, "How to share a secret", Communications of ACM, pp. 612-613, 1979.

[24] B. Schoenmakers, "A simple publicly verifiable secret sharing scheme and its application to electronic voting", Proc. of Advances in Cryptology-Crypto '99, pp. 148-164, 1999.

[25] D. R. Stinson, Cryptography: Theory and Practice, CRC Press, New York, NY, USA, 1995.

[26] K. Sako, J. Kilian, "Receipt-free mix-type voting scheme-a practical solution to the implementation of a voting booth", Proc. of Advances in Cryptology - Eurocrypt '95, pp. 393-403, 1995.