國立政治大學資訊科學系
Department of Computer Science
National Chengchi University

碩士論文

Master's Thesis

基於模糊簽章之電子投票系統

An E-Voting System based on Oblivious Signatures

研 究 生：陳淵順

指導教授：左瑞麟 教授

中華民國一百年一月

January 2011

基於模糊簽章之電子投票系統

An E-Voting System based on Oblivious Signatures

研 究 生：陳淵順　　Student：YUAN SHUN CHEN

指導教授：左瑞麟　　Advisor：RAY LIN TSO

國立政治大學

資訊科學系

碩士論文

A Thesis

submitted to Department of Computer Science

National Chengchi University

in partial fulfillment of the Requirements

for the degree of

Master

in

Computer Science

中華民國一百年一月

January 2011

基於模糊簽章之電子投票系統

摘要

近期電子投票系統被廣泛討論，許多國家也開始實行電子投票系統來取代傳統紙本投票。而一套完整的電子投票系統欲取代傳統紙本投票，此系統就必須滿足傳統紙本投票的需求，有完善的機制用以保護投票者在進行投票時的隱私性，保證投票者的身分及選票內容不被其他人得知，並維持整個投票過程的完整性、可驗證性及公平性等等的需求，系統的穩定性也是必須要考量的因素。

本篇論文主要針對投票者的隱私性及如何減輕投票者的負擔進行討論，我們提出了參考愛沙尼亞國家的電子投票系統的優點做結合，設計出一個改良的基於模糊簽章的電子投票系統。

關鍵詞：盲簽章、密碼學、電子投票、資訊安全、模糊簽章

An E-Voting System based on Oblivious Signatures

Abstract

Electronic voting systems have been widely investigated in recent years since they are very convenient for voters. Many countries have begun to implement electronic voting system to replace the traditional voting system. In order to replace the traditional voting system, an e-voting system must satisfy all the security requirements of those in a traditional voting system. Those security requirements are, firstly, to have a sound mechanism to protect a voter's privacy, and to ensure that the identity of a voter or the content of a ballot will not be leaked to others. Moreover, it must maintain the integrity, verifiability and fairness during the entire voting process. To keep the system stable during the voting process is also an important factor that must be considered.

This thesis is a research on designing a secure electronic voting system. Based on some existing electronic voting systems, we design an improved system to enhance the privacy protection of voters on one hand and to reduce the loading of voters on the other hand. In detail, our scheme is modified from the existing e-voting system of Estonian state, and we proposed an improved e-voting system which uses the oblivious signatures as a building block.

Keywords: Blind Signature, Cryptography, Electronic Voting, Information Security, Oblivious Signatures.

誌謝

隨著碩士研究論文的完成，兩年多的碩士研究生活也將在此畫下句點。回想這兩年多的研究生活，我必須誠摯的感謝我的指導教授左瑞麟老師，從剛進入到政大資科時，老師就不辭辛勞的指導與照顧直到我完成論文。同學們以及學弟妹們在我的研究生活中對我的批評與指教，我們共同切磋討論研究並互相砥礪打氣，因為有你們對我的研究提供了寶貴的意見，使得我能夠順利的完成學業並拿到碩士學位。

在此我要特別感謝研究室的同學們詹省三、陳力瑋、王裕炫、詹毓君，在同樣沒有學長姐的研究室下，我們一起成長一起摸索，即使沒有學長姐提供寶貴的經驗，我們一樣能夠一步一步地完成我們的學業，儘管過程或許不順遂，但結果卻是美好的。還有陸續進來的學弟們邱士峰、朱致諺、陳奕愷、劉偉正，感謝你們對這間研究室帶來更多的歡樂也更加的熱鬧。

另外，我也要特別感謝學長林光德，讓我在研究之外，能得到額外的工讀經驗。還有學長邵育晟、曾仲瑋與其他的同學及學弟們楊泰榮、劉勇麟、陳界誠、郭惠翔、丁諭祺、周世剛、陳韋良、黃于育、江尚倫、蕭名宏、鄭迪嶸、郭建宏、劉恭良、李法賢、游詳閔、吳容瑜、蘇珮瑩、陳映似、陳家豪、鄭遠祥以及新進學弟妹與大學部的學弟妹，有你們大家在研究之餘陪我運動陪我休閒，讓我的研究生活更多采多姿。

也非常感謝我的朋友們allen、熊哥、哈比、少林、賤狗，在我的研究生活中不斷地鼓勵我支持我，讓我能堅持下去。

最後謝謝我的爸爸媽媽與家人們能夠包容我鼓勵我支持我，未來我將會繼續地努力，用更上進的心來面對未來的挑戰，來回報眾人對我的期望。

陳淵順 謹誌

2010/12

目錄

圖目錄

表目錄

第一章　　緒論

網際網路快速發展，從撥接、寬頻網路到近期的光纖網路還有無線網路普及化，網路技術逐漸成熟，使用網路的人口激增，人們透過網路將整個世界串聯在一起。網路的興起帶給人們便利，也因為網路的便利性使得人們對網路的依賴越來越大，隨之而來的，人們對於網路安全的問題日漸重視。由於網路發展快速，所衍生的網路安全問題越來越複雜，這些安全問題將是人們必須重視及解決的。

科技的進步與網路的普及，使得越來越多的傳統行為模式漸漸轉移到網路上來實作。截至目前為止，已經有很多的應用已經在網路上實行，透過網路沒有時間空間限制的優點，讓使用者隨時隨地都能利用電腦上網來完成以往只能到實體地點處理的事務，大大增加了使用者的便利性並提高處理事務的效率。

網路上的應用越來越多，舉凡利用電子信箱寄信代替紙本信件，讓發收信能即時快速節省時間；而一年一度的人民報稅也可以透過網路來執行節省相當多的時間，讓整個報稅的流程更為順暢，也減少人力資源；另外網路 ATM 與電子現金交易也逐漸盛行，透過網路銀行進行繳費匯款等動作，讓使用者不需親自到銀行 ATM 就能達成；其他像是關於醫療方面也有許多透過網路來完成的應用。由上述的應用來看，人們的生活可以說和網路息息相關。

在台灣這個民主的國家，由於目前大小型選舉過於頻繁，在每次傳統選舉中都需要投入大量的人力及物力，造成資源的浪費；甚至選民的選票在往後的保存工作也有

一定的難度。因此，有許多的專家及研究人員紛紛提出電子投票這個想法，將傳統紙本投票透過網路與投票機器搭配適當的投票機制轉變為電子投票，利用電腦快速的計算能力，讓人們能迅速的進行投票與投票結束後進行計票公開結果。而電子投票不受天候交通等影響,相對可以增加人民的投票率,促進國家人民積極參與政治選舉活動。

電子投票的好處除了讓投票者快速的進行投票，快速的進行計票公布結果，讓投票者更積極參與選舉活動外，在最後投票結果有爭議時，也能夠馬上調出儲存在電腦內的選票資料進行驗票的動作，增加選舉的正確及公正性，並減少相當多的人力與物力，在選票的保存方面也變得簡單而不易產生問題，而全世界也有越來越多的國家已經慢慢推動電子投票的實行，電子投票必為未來的趨勢。

而實行電子投票固然是好事，但其相對應的安全性問題方面也是每位專家及研究人員所必須要考慮的地方。除了要保護投票者的隱私、選票的秘密、投票過程與結果的正確性及公正性外，還要防止有心人士對於投票機制的破壞及干擾，甚至利用不當的方法竊取機密訊息。這些都是一個完整的電子投票所必須要考慮及防範的。如何設計出一個安全又完整的電子投票機制必須靠每位專家及研究人員的努力開發與眾人的配合及參與，使得電子投票能夠選賢與能，加強民主國家的發展。

1.1 研究動機與目的

目前對於電子投票已經有相當多的研究，雖然大多已可滿足投票選舉的需求或解決一般性的問題，但似乎還是有許多難解的問題必須處理，例如在傳統投票中常見的暴力脅迫、賄賂等等即使應用到電子投票上，這些問題仍然是不容易解決的。

由於網際網路的發達，現今有許多的駭客橫行於網路上，透過網路竊取個人隱私資料等等，嚴重影響網路上的資訊安全。也因為這些駭客，對於網路方面的應用也遭受重大的考驗，開發者必須考慮到更多的層面來抑制這些駭客們的入侵以保護這些使用者所使用的應用程式。在電子投票系統上面，開發者須考慮投票者的個人資料隱私方面是否會被竊取，投票者的選票內容是否被駭客們攻擊得知，也必須防範系統遭到有心人士故意影響選情而亂投票，如何判斷有效票無效票或是如何證明選票確實為選民所投，這些都是針對安全方面所要考量的。

除此之外，民主國家的選舉行之有年，而且往往可能一年就有好幾次的選舉，選民已經很習慣於傳統紙本投票，而且現場都有工作人員進行解說的動作，如果突然將傳統紙本投票轉換成電子投票，一時之間選民或許會懷疑其電子投票的完整及公正性，也會擔心其隱私是否會被竊取得知，又或許一些較年長的選民可能較少機會能接觸電子機器像是觸控螢幕，如此的數位落差也會造成選民的接受度不足。因此，如何讓選民們接受並支持電子投票這便是政府及研究人員所要考慮的因素之一。

近期已經有許多的研究人員已經提出很多的電子投票機制，許多的安全性也都有考慮到，但卻很少考慮到投票者的便利性，例如投票者投完票一直到投票結束後可能還必須配合投票中心來進行開票而增加投票者的負擔。而投票者以及選票的隱私性也是電子投票一個相當重要的安全性，這是實作電子投票必須要慎重考慮的地方。

因此，本篇論文將針對投票者的隱私性及如何減輕投票者的負擔進行討論，利用模糊簽章實作出一個更加完善的電子投票系統，考慮更多的安全性以及增加其實用性，也希望對於國內電子投票系統能夠提出一點貢獻。

1.2 章節架構

在本章介紹完現況及研究動機與目的後，為了有系統的介紹本篇論文，我們將分為七個章節。前兩章針對現行電子投票的發展趨勢作介紹，第三、四章為相關技術與文獻的介紹與探討，第五、六、七章將介紹我們提出的方法與架構並針對其安全性做一個簡單的分析，最後做一個總結以及未來的工作。各章節的說明如下：

第一章：緒論，介紹近期電子投票的現況與問題以及研究的動機與目的。

第二章：介紹電子投票的概論與各國實行狀況。

第三章：介紹相關技術，包括密碼系統、電子簽章與身分驗證方法。探討並介紹與論文相關的文獻。

第四章：詳細介紹並講解我們所提出的方法與架構。

第五章：針對安全性做一個簡單的分析與討論。

第六章：總結以及未來相關的工作。

第二章　　電子投票簡介

2.1　　電子投票概論

在一個民主的國家中，很多事情必須透過多數決的方式來決定，因此，投票便成為了民主國家中重要的一個活動。選舉投票代表著民意，參與投票也是人民的一項權利,投票的結果可以代表多數人民意見來決定最終結果,而選舉投票過程必須是公正、公平、公開的，任何人都無法打破這個規則。在一般傳統選舉投票中，每位有投票資格的選民都有權利到投開票所將選票投給心中理想的候選人，但由於選民有地域區域性的關係，因此，選民必須前往指定之戶籍所在的投開票所進行投票的動作，再加上可能因為天候的關係，而影響到選舉的投票率，使得選舉往往無法反應真正的民意。另外，當選舉結果出現而發生爭議時，則必須重新驗票，驗票的過程必須花非常多的時間也需要大量的人力。

而由於目前大小型選舉過於頻繁，在每次傳統選舉中不論是準備工作階段、投票階段、計票階段以及驗票階段等都需要投入大量的人力及物力，造成資源的浪費；甚至選民的選票在往後的保存工作也有一定的難度。而科技的進步，網際網路的發達，許多應用都轉而透過電腦來實作，於是許多研究人員便開始研究如何將投票電子化，如何讓選舉投票變得更方便、更有效率、更節省資源、更加正確的計票與驗票，再加上傳統投票的優點，這些都是研究人員在研究電子投票的過程中所必須考慮到的因素。

電子投票系統就是一個模擬現實生活中公民投票過程的線上系統，其應考慮的安全性以及性質也必須符合現實中投票的實況。簡單來說，就是把現實生活中的公民投票電子化和線上化，以節省時間及大量的人力、物力，並讓公民能更簡單輕鬆的投票。

現今電子投票系統大致分為兩種方式，電子投票(E-voting)系統與網路投票(I-voting)系統，以下將依序介紹這兩種投票方式有何不同[29]：

一、電子投票(Electronic voting)

這種投票方式較為接近傳統紙本投票的方式。投票者需到投開票所利用具有觸控螢幕的電子投票機進行投票的動作，而所有計票、驗票的動作都在此電子投票機進行，也有不少研究人員將此方法改良[25][26][27][28]，例如加入投票收據的動作，讓投票者可以有個憑證，證明他的選票有被系統計票，幫助投票者確認，使投票者對此投票方式更有信心而增加投票率。

二、網路投票(Internet voting)

此種投票方式不限定地區地點，只需要在有網路的地方就可以進行投票。投票者經由網路透過特定網站以及投票應用程式來進行投票的動作。透過這樣的方式，投票者就不需要前往投開票所即可投票，大大增加投票者的便利性。另外，近期也有像利用手機、PDA 等通訊器材經由手機網路、WIFI 或是 WLAN 透過簡訊或文字訊息進行投票的動作，也將其歸類在網路投票[10][17][21][22]。

當然還有其他不同的投票方式，但不管是哪種電子投票系統都必須詳細考慮其安全性，網路方面的安全、電子投票機的安全，甚至是網站及投票應用程式的安全，開發人員都應該針對這些安全考量來設計，如此才能保障投票者的隱私，使投票者對投票有信心。

不論是傳統紙本投票、電子投票或是網路投票，都是人們用來執行民主投票的一種方式，而在這些投票機制中，其投票程序大致分為三個步驟：

一、**註冊階段：**

在選舉前，投票中心會公布所有具投票權的選民名單，並寄發選舉通知及相關選舉的訊息給予合格的投票者，而投票者必須在特定的選舉日期進行相關的身分驗證後並領取選票，如此才算完成整個註冊階段。

二、**投票階段：**

當投票者領取到選票後，不論是到特定的投開票所或是利用網路透過網站及投票應用程式即可進行投票，選擇心中所屬的候選人後完成投票的動作，在投票程序中應避免投出廢票的可能性。

三、**開票階段：**

當選舉投票期限過後，任何人都無法再進行投票的動作，經由投票中心來完成計票及開票的程序，其過程必須是公正、公平、公開的，最後由投票中心將結果公布給選民以完成整個選舉投票的流程。

電子投票的產生就是用來改善傳統紙本投票的缺點。因為傳統紙本投票雖然實行已久，選民們也很習慣於現行投票方式，但由於國內大大小小的選舉相當多，造成紙張及人力資源的浪費、人工計票階段所花費的時間相當多、當最終結果出現爭議時重新驗票程序繁雜、選票的保存不易等等原因，所以研究人員積極研究開發出電子投票的方式來解決這些問題，使得選舉投票方式能讓投票者及整個程序更方便、處理選票更有效率、使投票結果更加準確。

雖然電子投票較傳統紙本投票多出很多優點，但也因為網際網路快速發展，科技的進步，使得網路上的病毒及駭客盛行，試圖對網路應用服務程式等進行破壞，再加

上資料在網路上傳送容易被攔截複製或修改傳送，這些都將嚴重的影響電子投票的發展。以下為電子投票所遇到的一些問題：

一、冒名投票:

如果電子投票機制無法對有效投票者進行身分驗證的話，就會遭到不明人士冒名進行投票，使其影響到最後選舉的結果，讓選舉失去了公正性。

二、重複投票：

假如投票系統沒有一個機制來限制投票者重複投票的話，攻擊者可能利用此弱點來做阻絕攻擊，長時間一直重複投票的動作，造成投票系統癱瘓。此外，一張選票憑證可以投給不同的候選人很多次，形成灌票的行為，這些會影響選舉的公平性的行為都是不應該被允許的。

三、暴力脅迫：

以金錢利益賄選或是以暴力脅迫控制投票者將選票投給特定的候選人，這種問題在傳統紙本投票層出不窮，即使是利用電子投票系統，如果沒有一個完善的機制，還是無法解決這類的問題而影響到選舉的公正性。

四、預先得知結果：

由於電子投票機制的設計不嚴謹，造成載投票期限還未截止前就被攻擊者從中預先得知選舉結果而進行買票或以暴力脅迫控制投票者投票，這將嚴重影響選舉的結果與公正性。

五、受制軟體廠商：

政府和廠商購買應用軟體或是電腦計票機，因對廠商規範不明，政府無法檢驗廠商在軟體內是否留有後門程式或是病毒，而可能會影響到整個選舉的結果。政府選舉機構如果無法證明廠商是值得信賴的，則對選民而言是缺乏公信力的。

六、**接受度不足與數位落差：**

傳統紙本投票行之有年，如突然改變為電子投票可能會使投票者不易接受，甚至懷疑其可行性與安全性。另外，電子投票系統必須利用電子投票機或是電腦等相關科技產品，而不一定所有選民都有使用這些機器的相關知識，造成了數位落差的情況。

七、**機器當機問題：**

在投票過程中，萬一機器發生了無法預期的問題或是當機的狀況，如果沒有替代方案來處理這類問題的話，將會影響到整個投票過程和投票結果。

八、**駭客入侵：**

網路的發達，駭客越來越多，如果電子投票機制沒有任何防範的措施來抵擋有心駭客的入侵，竊取投票者的個人資料甚至預先得知投票結果進而影響之後的選情，這對電子投票系統造成莫大的傷害。

雖然上面提到了許多電子投票所面臨的問題，但相信電子投票必是未來的趨勢，實行電子投票取代傳統紙本投票所帶來的好處是選民及研究開發人員樂意看到的。如何解決上述這些問題與未提及的問題都是未來研究與突破的課題。

而電子投票系統的安全性考量與現實中投票系統的需求及考量是大同小異，每位研究人員所提的項目也不盡相同，但大致上均包含以下七點：

一、**投票資格(Eligibility)：**只有具有投票資格者才能進行投票。

二、**不可重複性(Non-reusability)：**一個有資格投票的投票者只能投票一次，不能重複投給不同或是相同的候選人。

三、**合理性(Soundness)：**沒有人可以改變其他人的選票。

四、**完整性(Completeness)：**每個投票者都可以確認自己的選票有被計數。

五、**認證性(Verifiability)**：沒有人可以竄改投票後的結果，選舉結果是可以被公開驗證。

六、**公平性(Fairness)**：沒有人可以得知任何與投票內容相關的資訊，直到最後公開時才能得知，以免影響到尚未進行投票的投票者意願。

七、**隱私性(Privacy)**：沒有人可以確定誰投給誰，每個人對於自己所投的票都有隱私性，除非自己告訴別人，否則其他人應無法得知。

表 2-1 傳統投票與電子投票之優缺點比較

	現行投票	電子投票
優點	1. 符合直接、平等、無記名、秘密等選舉原則 2. 實體選票提高選民信心 3. 現有法制配合投票制度，如選罷法等	1. 改善人工計票費時的問題，增加行政效率 2. 降低廢票率 3. 減少人工作業可能引發的選務瑕疵 4. 降低傳統選票的印製與保留成本 5. 計票快速準確
缺點	1. 紙張、人力資源浪費 2. 有效票與無效票的認定容易產生爭議 3. 選票保存困難 4. 人工開票、計票曠日廢時 5. 出現爭議時，重新驗票手續繁雜 6. 投票流程複雜	1. 公民接受度不足，存有教育訓練宣導成本 2. 電子投票法制未健全 3. 數位落差 4. 選務機器存放空間問題 5. 選務人員的訓練成本 6. 投票機器有當機、讀取錯誤之可能，造成投票秩序混亂 7. 容易受制於軟體廠商

第三章　　相關技術研究

3.1　公開金鑰密碼系統

公開金鑰密碼系統[6]又稱為非對稱式密碼系統，每一對金鑰(Key Pair)包含兩把相互對應的金鑰，一把為可以公開的加密金鑰(Public Key)與一把只有本人才擁有的解密金鑰(Private Key)。雖然利用 Key Pair 改善了對稱金鑰密碼系統必須利用秘密通道傳送加解密金鑰的缺點，但是在運算速度上卻是比對稱金鑰密碼系統來的慢，這也是公開金鑰密碼系統的缺點。

在公開金鑰密碼系統中，任何人都可將加密金鑰公開(Public Key)，讓所有可能與其通信的人得到。當傳送者欲傳送訊息給該接收方時，可將訊息利用接收方的公鑰加密之後，再加以傳送。該加密後的訊息，只有接收方所擁有與此把公鑰相對應的私鑰(Private Key)可以將該訊息解密。所以公開金鑰密碼系統可以達到讓雙方，不需要事先交換金鑰即可從事秘密通訊的特性。

3.1.1　離散對數問題

p 為一個很大的質數，g 為對於有限場 GF(P)的生成元(generator)，則我們可以計算方程式如下：

$$y = g^x \bmod p$$

其中 mod 運算代表 y 為 g^x 除 p 之後的餘數。當我們有 g, p, x 則很容易算出 y，但當我們有 g, p, y 則要算出 x 是非常困難的。

如此我們可以利用離散對數問題來實作公開金鑰密碼系統。將 x 當作是自己的私鑰，而計算出 y 當作是公鑰公開給大家，雖然 g, p 也是公開的，但其他人卻很難算出私鑰 x，以此為概念，便可設計出許多實用的公開金鑰密碼系統[7][11][14]。

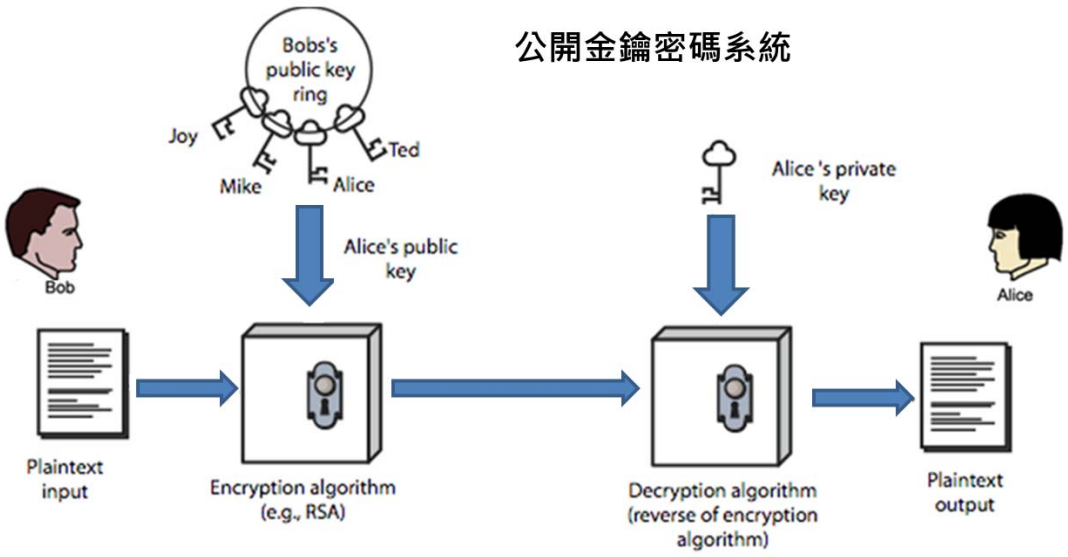

圖 3-1 公開金鑰密碼系統

3.2 電子簽章

電子簽章與公開金鑰密碼系統相似，當訊息擁有者利用私鑰進行加密當作此訊息的認證，任何擁有此私鑰所對應的公鑰的人都可以利用公鑰來進行驗證的動作，如此利用私鑰所加密的訊息即可視為是電子簽章。

電子簽章有很多不同的延伸及變化，在此簡單介紹兩種應用在電子投票系統上的

電子簽章系統，盲簽章(Blind Signature)是由 D. Chaum[2]在 1983 年所提出的一種電子簽章；而模糊簽章(Oblivious Signature)是由 L. Chen[5]在 1994 年所提出，2008 年由 R. Tso 等學者正式定義完整的 1-out-of-n Oblivious Signature[16]。

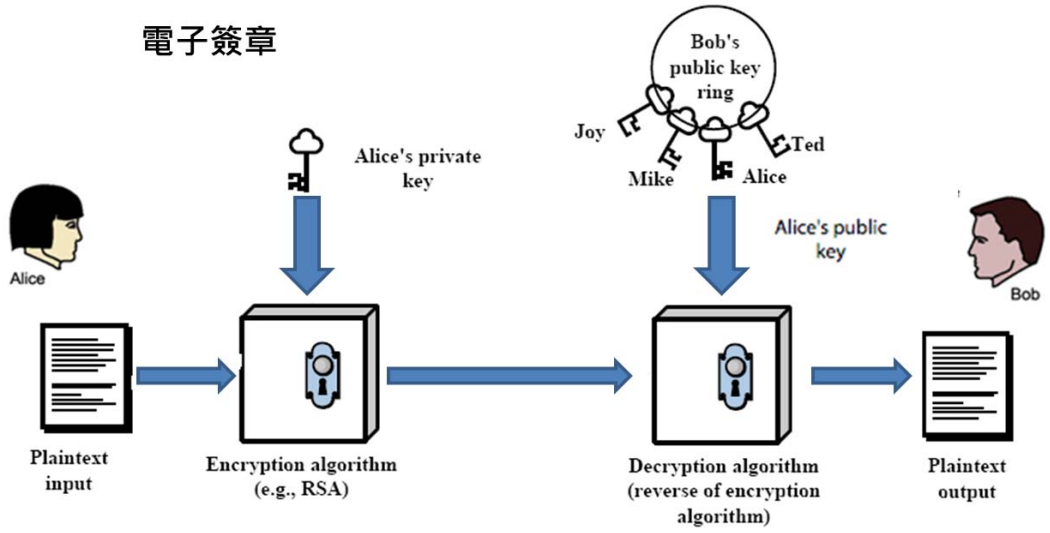

圖 3-2 電子簽章

3.2.1 電子盲簽章

在最近這幾年關於電子投票系統的研究中，很多都是以盲簽章(blind signature)為基礎來建構，進而對於盲簽章的安全性來做探討以及加以改進。盲簽章的概念最早是由學者 D. Chaum[2]於 1982 年所提出，隨後並引起相當多的相關研究[1][3][8][12][13][19][20]。在盲簽章的協定中，通常有使用者、簽章者及驗證者三個角色，其運作過程大致如下：使用者將要簽章的訊息用盲因子(亂數)盲化後，送交給簽章者進行簽名。由於簽章者收到的是盲化過的訊息，所以無從得知訊息的實際內容，簽章者只是盲目地進行簽名的動作，然後將盲簽章送回給使用者。使用者收到盲簽章

後，使用盲因子從中取出真正的簽章。而驗證者可以使用簽章者的公鑰(Public Key)驗證簽章的正確性。在電子投票的應用中，利用盲簽章的特性，使得簽章者無法得知投票者是將票投給哪位候選人，以達到隱密性的特性。

在 D. Chaum 所提的方法中有五個階段，分別為 Initializing phase、Blinding phase、Signing phase、Unblinding phase、Verifying phase：

一、**Initializing phase：**

簽章者隨機選取兩個很大的質數 p,q 並計算 $n = p \cdot q$ 及 $\phi(n) = (p-1)(q-1)$，簽章者選取兩個很大的數 e,d 其中 $ed \equiv 1(\mathrm{mod}\,\phi(n))$ 及 $\gcd(e,\phi(n)) = 1$。則 (e,n) 為簽章者的公鑰，而 d 為簽章者的私鑰。最後，簽章者將 (e,n) 公開，而自己留著 (p,q,d)。

二、**Blinding phase：**

需求者擁有一個訊息 m，他希望簽章者對這訊息作簽章的動作。首先需求者隨機選取一個亂數 r 當作是盲因子，用來將訊息 m 盲化成為 $m' = r^e \cdot h(m) \bmod n$， 並將 m' 傳送給簽章者。

三、**Signing phase：**

當簽章者收到 m' 後，計算 $s' = m'^{d} \bmod n$ 然後回傳給需求者。

四、**Unblinding phase：**

當需求者收到 s' 後，計算 $s = s' \cdot r^{-1} \bmod n$，則需求者得到盲簽章 s。

五、**Verifying phase：**

為 m 的簽章，任何人可以透過檢查 $s^e \equiv h(m) \bmod n$ 是否成立來驗證此簽章的正確性。

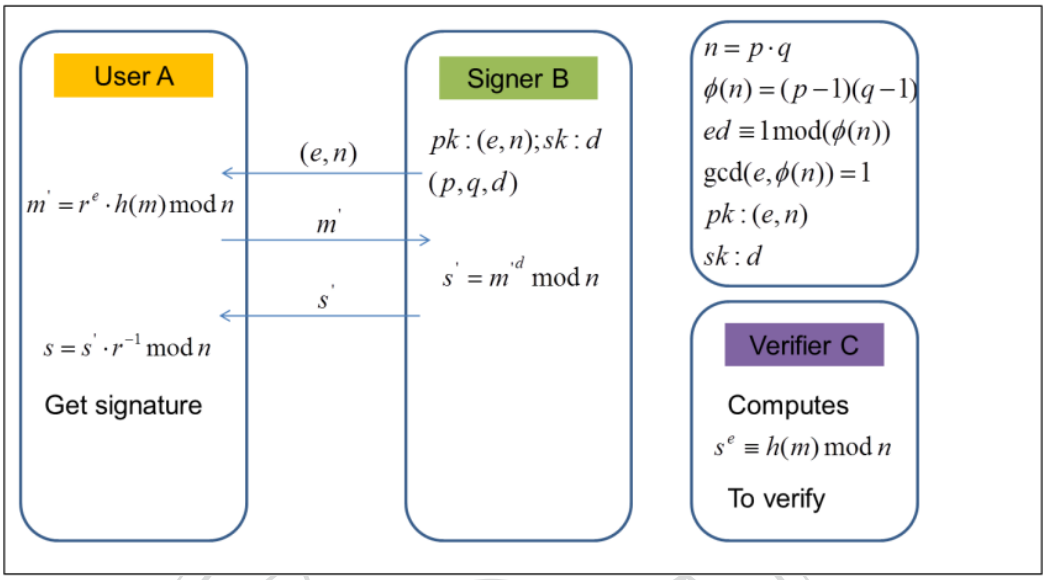

圖 3-3 電子盲簽章

3.2.2 電子模糊簽章

模糊簽章(oblivious signature)是電子簽章的一種類型，是由 L. Chen[5]在 1994 年所提出的。在[5]中，L. Chen 將模糊簽章分為兩種類型，第一種是利用 n 把金鑰（keys）來實作模糊簽章，第二種是利用 n 個訊息（messages）來實作模糊簽章。

第一種類型的協議(protocol)類似於群簽章(group signature)[4]的實作，其參與者有 n 個簽章者 Signer S1, S2, …, Sn (或是一個簽章者擁有 n 把不同的 key)與接受者 Recipient R。群簽章與第一種類型的模糊簽章不同的地方在於群簽章中的簽章者是匿名的，接受者 R 無法得知文件是由簽章者的哪一把 key 所簽章的；而此類型的模糊簽章則是接受者 R 可以知道文件是由簽章者的哪一把 key 簽章的。下面介紹此類型的模糊簽章有三點特色：

一、由 R 從 n 把 key 中挑選其中一把 key 來對 message 簽章，因此 R 可得到這個簽章。

二、所有可能的簽章者即使是此 key 的擁有者，也無法找出是哪一把 key 對

message 作簽章。

三、如果需要，R 可以公開他所得到的簽章，但不透露是由哪一把 key 所生成的簽章。

第二種 protocol 包含了簽章者 Signer S 和接受者 Recipient R。這類型的模糊簽章適合用在網路交易或是網路電子投票上，如何應用在網路電子投票上在之後的章節會提到。這類型的模糊簽章有三點特色：

一、接受者 R 只能選擇 n 個 messages 中的其中一個 message 得到簽章。

二、簽章者 S 無法得知 R 得到哪個 message 的簽章。

三、如果需要，R 可以公開他所得到的簽章，但不透露是對哪個 message 所生成的簽章。

2008 年，R. Tso 等學者認為先前的方法沒有很清楚的顯示出模糊簽章正規化的概念，而且方法的架構對於通訊和計算方面缺乏效率，因此 R. Tso 等學者發表了一篇 1-out-of-n oblivious signatures[18]來改善這些問題，與先前的方法相比較更有效率。

1-out-of-n oblivious signatures scheme with n messages 中有三個參與者：

一、**接受者 Recipient R**：R 可以從 n 個 messages 中選取任何一個 message 讓簽章者 S 進行簽章。

二、**模糊簽章者 Signer S**：S 可以對 R 所選的 message 簽章，但他不能得知是 n 個 messages 中的哪一個，只能確定 R 所選的 message 確實在 n 個 messages 中的其中一個。

三、**驗證者 Verifier V**：V 可以驗證 R 所得到的簽章的正確性而不需要任何的隱藏資訊輔助。

在 R. Tso 等人的方法中包含了四個步驟，分別為 System Setting、Key Generation、Signature Generation、Signature Verification：

一、**System Setting**：

1. p,q：兩個很大的質數，$q \mid (p-1)$。
2. g,h：屬於 Z_p^* 有相同的序(order) q。
3. $H:\{0,1\}^* \to Z_q^*$：是單向雜湊函數(one way hash function)。

二、**Key Generation**：

簽章者 S 選擇一亂數 $x \in Z_q^*$ 並計算 $y \leftarrow g^x \bmod p$，x 是 S 的私鑰而 y 則公開為 S 的公鑰。

三、**Signature Generation**：

假設接受者 R 想要得到簽章者 S 對 $m_l \in \{m_1,...,m_n\}$ 做的模糊簽章 σ：

1. 接受者 R 選擇一個亂數 $r \in Z_q^*$，計算 $c = g^r h^l \bmod p$，然後將 c 與 n 個 messages $m_1,...,m_n$ 一起傳給簽章者 S，$m_l \in \{m_1,...,m_n\}$。
2. $i = 1,...,n$，S 選擇一亂數 $k_i \in_R Z_q^*$，然後計算：
   - $K_i \leftarrow g^{k_i} \bmod p$
   - $\hat{e}_i \leftarrow H(m_i, K_i c/(gh)^i \bmod p)$
   - $\hat{s}_i \leftarrow k_i - x\hat{e}_i \bmod q$

   S 將 $(\hat{e}_i, \hat{s}_i), 1 \le i \le n$ 傳送給 R。

3. $1 \le i \le n$，R 計算 $\delta_i \leftarrow g^{(r-i)} h^{(l-i)} \bmod p$，並接受此模糊簽章，假如下列式子成立的話：

$$\hat{e}_i = H(m_i, g^{\hat{s}_i} y^{\hat{e}_i} \delta_i \bmod p) \qquad 1 \le i \le n$$

4. R 將模糊簽章轉換成一般的簽章：

- $e \leftarrow \hat{e}_l$, and
- $s \leftarrow r - l + \hat{s}_l \bmod q$,
- 則 R 得到對 m_l 所做的簽章 $\sigma \leftarrow (e, s)$.

四、**Signature Verification**：

最後任何驗證者 V 都可以去驗證此簽章 σ，假如下列式子成立的話：

$$e = H(m_l, g^s y^e \bmod p)$$

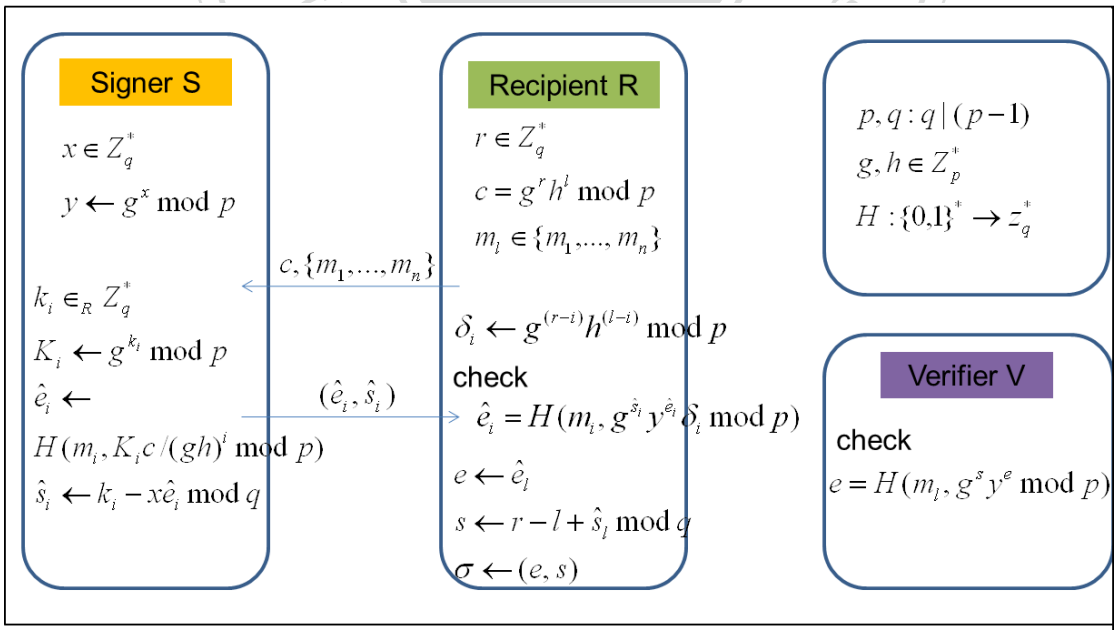

圖 3-4 1-out-of-n oblivious signature

完整的模糊簽章包括了三個參與者：一個簽章者(a signer S)，一個接受者(a recipient R)及一個認證者(a verifier V)。模糊簽章的特性就是接受者可以在 L 個訊息中選擇一個訊息給簽章者簽名，而簽章者不知道 L 個簽章中何者為接受者所需要的，只能確定接受者所選的訊息確實在 L 個訊息中的其中一個。因此，使用這個方法可以保障使用者的隱私而又能保護簽名者不會簽到任何他不願意簽署的文件(註：盲簽章不具保護簽名者的功能)。

模糊簽章除了可以應用在電子投票外，也可利用於其他方面如線上公平遊戲(on-line fair game) 。為了使讀者了解模糊簽章概念，以下以一個 Fair Game 的例子來做說明：

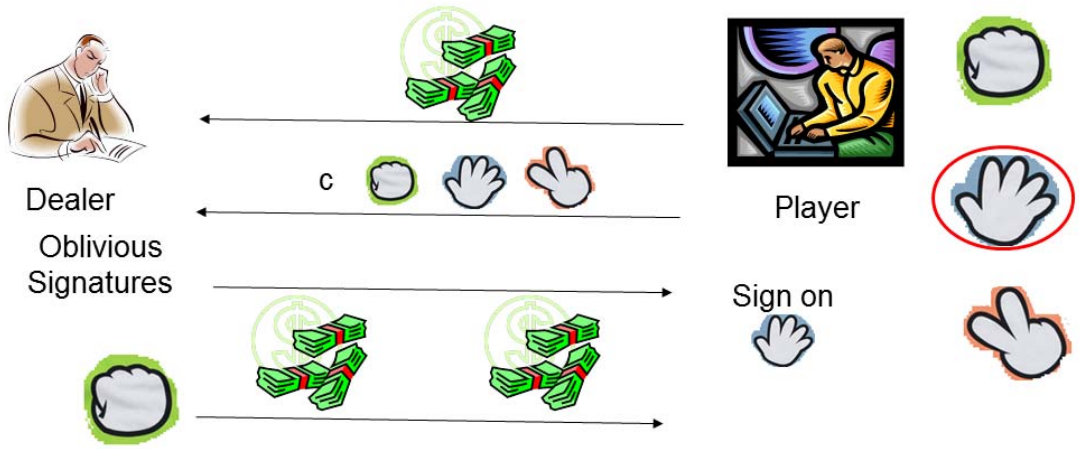

圖 3-5 模糊簽章應用於 Fair Game

這是一個網路猜拳的遊戲，首先 Player 從剪刀、石頭、布中選擇其一(例如選擇”布”)，將所選擇的參數經過計算(c)使得 Dealer 無法得知 Player 所選為何。Dealer 確認 Player 身分後利用 c 對訊息做模糊簽章後回傳給 Player，Player 透過計算得到”布”的簽章。最後 Player 與 Dealer 比較得知最後輸贏。以上為一種模糊簽章的應用。

3.3 身分驗證

使用者不論是在領取選票或是到銀行提領現金時都必須證明自己的身分，最常見用來證明身分的就是利用身分證。而在網路世界中就必須透過數位化的資訊來做身分的驗證，像是登入網頁使用 web service 時就必須有帳號密碼才能登入。

而認證的方法有很多種，像是利用 Kerberos 認證、基於身分的認證方法等等。以下將介紹一種基於身分的認證方法 Schnorr Identification Scheme。

3.3.1 Schnorr Identification Scheme

Schnorr Identification Scheme 是 1991 年由 C.P. Schnorr[15]所發表的一個基於離散對數問題的認證方法。這個方法需要一個可信賴的機構，Trusted Authority (TA)， 來選擇系統所需要的參數，其參數如下： p，q 是兩個很大的質數，其中 $q|p-1$，$q \geq 2^{140}, p \geq 2^{512}$， $\alpha \in_R Z_p^*$ 序(order)為 q。*TA* 的簽章及驗證演算法分別為 $Sign_{TA}$，Ver_{TA}。這個驗證方法的流程如下所示：

一、 *A* 選擇一個祕密的值 $a \in_R Z_q^*$，計算相對應的公鑰 $v = \alpha^a \pmod p$，接著傳送 (ID, v) 給 *TA*，其中 *ID* 為 *A* 的認證字串訊息。

二、 *TA* 驗證 *A* 的身分後，對 (ID, v) 簽章得 $s = Sign_{TA}(v)$，接著回傳一個憑證 $C(A)(=(v,s))$ 給 *A*。

三、 *A* 挑選一個亂數 $k \in_R Z_q^*$，接著計算 $\gamma = \alpha^k \pmod p$ 然後傳送 $(C(A), \gamma)$ 給驗證者 *B*。

四、B 藉由驗證 TA 的簽章來驗證 $C(A)$ 確實由 TA 簽署。驗證成功之後 B 傳送一個亂數 $r, 1 \le r \le 2^t$ 給 A ，t 為一秘密參數。

五、A 則傳送 $y = (k - ar) \bmod q$ 給 B 。

六、B 去驗證 $\gamma \equiv \alpha^y v^r \bmod p$ ，如果等式成立則接受 A 的身分證明。

Schnorr Identification Scheme 不管是在計算量或是訊息量來看，其優點是速度快且有效率。

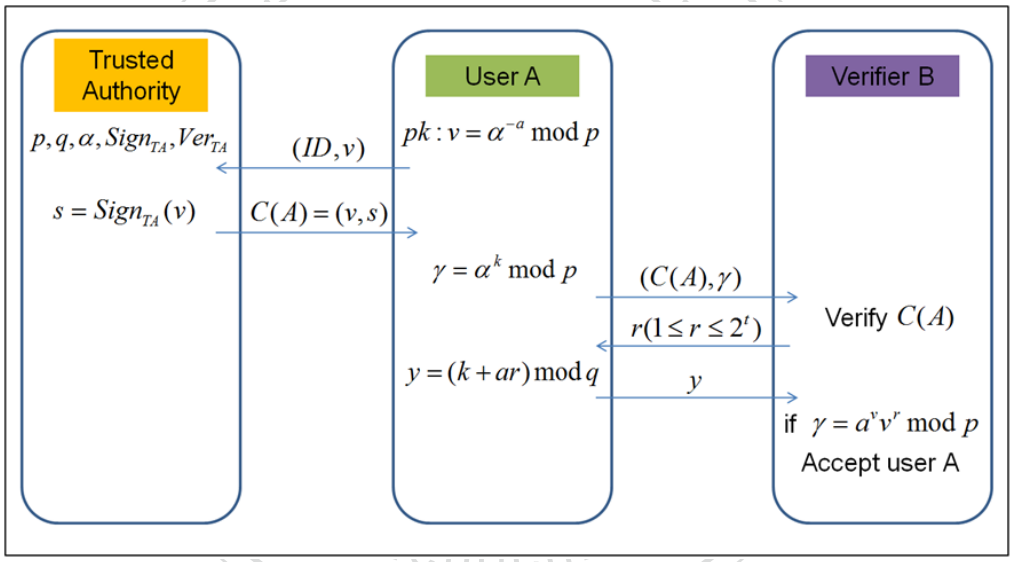

圖 3-6 Schnorr Identification Scheme

3.4 愛沙尼亞電子投票系統

2005 年在愛沙尼亞的 Tallinn 發表了一篇關於電子投票系統的介紹[22]，裡面詳細說明了愛沙尼亞電子投票系統的目標、系統架構、投票流程等等。下面是關於他們的電子投票系統的架構圖：

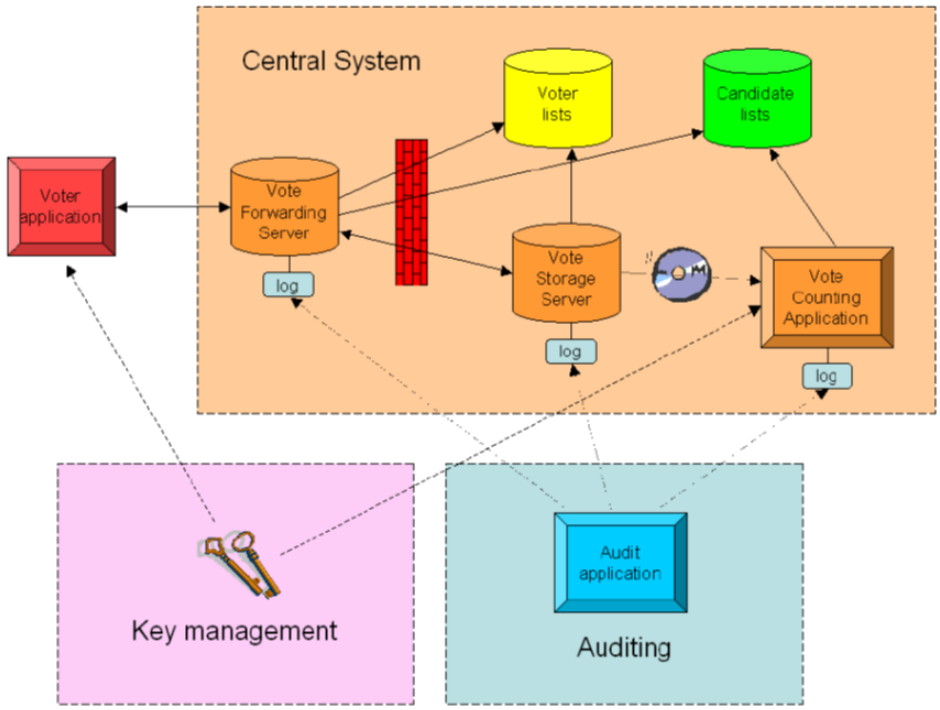

圖 3-7 愛沙尼亞的電子投票系統架構

其中包含 Voter、Central System、Key management、Auditing。而在 Central System 裡又包含了 Vote Forwarding Server(VFS)、Vote Storage Server(VSS)、Vote Counting Application(VCA)。

以下將介紹投票者將如何利用此系統來進行投票。

3.4.1 Key Management

此步驟系統將產生系統本身的 key pair，並且將一些 voter 的個人資訊及系統參數嵌入 ID-Card 中以便進行身分確認的動作。而系統參數及 key pair 等資訊都是非常秘密安全以防止外洩。

3.4.2 Voting and Vote Storing

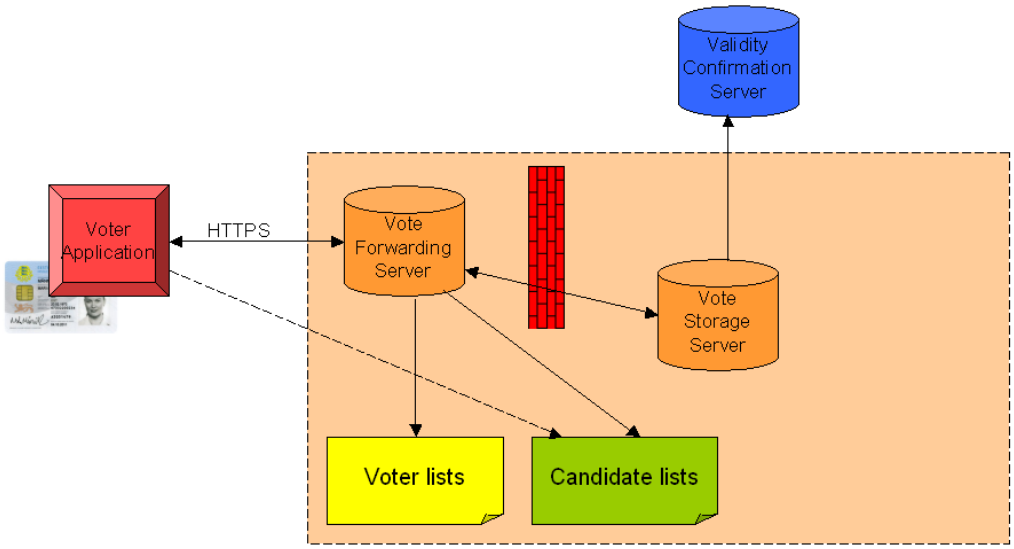

圖 3-8 Voting 架構

此步驟為投票者進行投票的步驟。投票者只需要備有一台可上網的電腦以及可讀取 ID-Card 之讀卡機，不論身處何處都能透過網路進行投票。

投票者利用讀卡機讀取 ID-Card 內的資訊並透過具 HTTPS-protocol 的網頁傳送資訊給 VFS 進行身分確認。一旦身分確認完畢後，投票者就可以選擇候選人並將選票送至系統並由系統儲存至 VSS 內。

3.4.3 Vote Cancellation and Sorting

當投票結束後，系統及開始分析投票名單，當有(a)多張重複選票、(b)提前投票、(c)重複投票三種情況的話則判定為不合格之選票，其餘則為合格的選票，之後將合格的投票者名單儲存下來並將選票 list 燒入 CD 中傳送到 Vote Counting Application (VCA)。

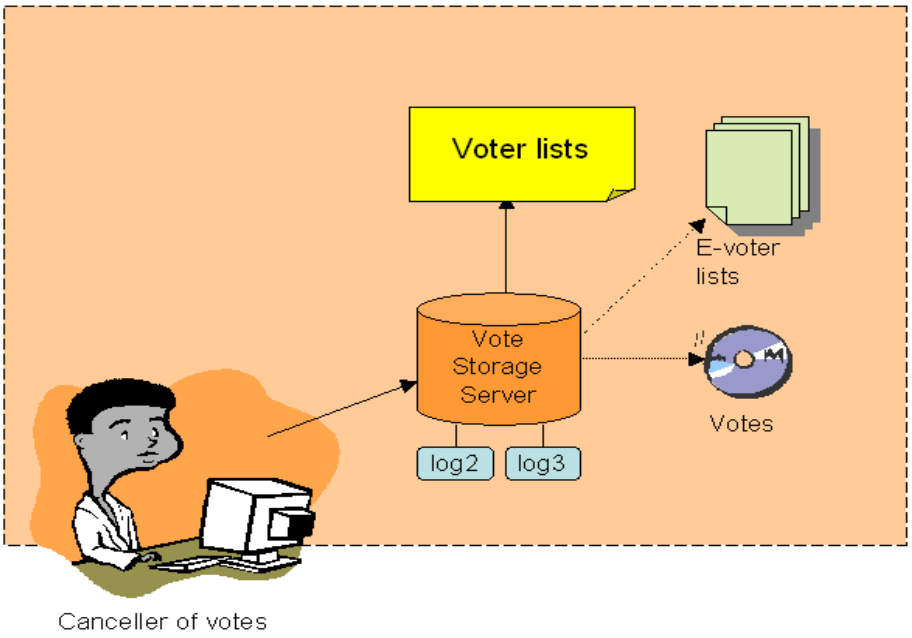

圖 3-9 Sorting and cancellation

3.4.4 Counting of votes

Vote Counting Application(VCA)收到 CD 後進行計票的動作並將最終結果公布。只有計票人員才有私鑰解開選票得到最後的結果。

3.4.5 Audit Application Possibilities

在此系統運作時會產生數個 log 檔在不同的步驟中，其中包括 LOG1: received votes、LOG2: cancelled votes、LOG3: votes to be counted、LOG4: invalid votes(invalid candidate number)、LOG5: accounted votes。

而當投票者對於結果或是過程有任何的疑慮而提出申請的話，系統將調出這 5 個 log 檔來進行查驗以得知對於結果是否有問題。

愛沙尼亞的電子投票系統的優點為 Voter 只需要面對一個窗口 Vote Forwarding Server (*VFS*)，透過 https 網頁來與 *VFS* 連絡並進行投票動作，而一些參數的傳送或是計算處理由 *VFS* 穿過防火牆來運作傳送，而 Auditing 則是有爭議出現時，必須透過 log 檔的檢視來排除並解決爭議。

3.5 基於盲簽章之電子投票系統

前面介紹了盲簽章的 protocol，有許多學者將盲簽章應用在電子投票上。在 Y-C. Lai 的 *A Study on Digital Blind Signature and Its Applications to Electronic Voting and Electronic Cash*[9]方法中就利用盲簽章來實做一個電子投票系統。在他的方法裡總共定義了有五個參與者分別是：voters、a certificate authority(*CA*)、an authentication center(*AC*) 、a tally center(*TC*)、a supervisor center(*SC*)，以及四個步驟：Registering phase、Authentication phase、Voting phase、Counting phase。

一、**Voters**：具有投票資格的投票者。

二、**Certificate Authority(*CA*)**：負責投票者的身分確認及註冊為具有投票資格的機構。

三、**Authentication Center(*AC*)**：類似傳統投票中選會的角色。負責檢查投票者是否有通過 CA 的註冊階段，如果有則傳送"voting certificate"給已註冊的投票者當作選票，投票者依此憑證進行投票。此外，要負責監督並防止投票者重複投票的情形。

四、**Supervisor Center(*SC*)**：類似傳統投票的投票站。負責監督所有選舉過程並驗證 Tally Center 在 Counting Phase 的計票是否正確。

五、**Tally Center(*TC*)**：類似傳統投票的投票站。負責最後的計票以及公布選舉結果。

3.5.1 Registering phase

在這個步驟中，CA 產生一組公私鑰 PK_{se}, SK_{se}，分別將公鑰傳給具投票資格的投票者用來加密選票 M'，私鑰傳給 tally center 在計票階段時解密選票進行計票動作。投票者用他的個人身分資訊 ID_i 向 CA 進行註冊，而 CA 確認投票者的身分後產生一組獨特的公私鑰 PK_i, SK_i 傳給已註冊通過之投票者，並將這些具投票資格的投票者記錄下來產生一組清單，在註冊階段結束後，將這組清單傳送給 AC 及 SC 用於 Authentication phase。

3.5.2 Authentication phase

投票者透過 SSL 網頁連上 AC 後作登入身分驗證的動作，接著下載一張空的選票 M，然後根據投票者的喜好選擇一位候選人將其標記在 M 上，此時選票為 M'，然後投票者利用 PK_{se} 將選票加密 $C = E_{PK_{se}}(M')$。接著投票者選擇一亂數當作盲因子 r_1，並將 C 盲化為 $X = B(C, r_1)$，利用投票者的私鑰 SK_i 將盲化的訊息 X 加密計算得到簽章 $X_1 = E_{SK_i}(X)$。

由於在下一個投票階段時，投票者必須要有帳號密碼對，也就是"voting certificate"，

因此投票者必須經由與AC傳遞參數而得到"voting certificate"。投票者計算$H(ID_i \| a)$，a為投票者隨機選擇的亂數，然後投票者再隨機選擇另一個盲因子r_2，並將$H(ID_i \| a)$盲化為$Y = B(H(ID_i \| a), r_2)$，利用投票者的私鑰SK_i將盲化的Y加密計算得到簽章$Y_1 = E_{SK_i}(Y)$。投票者利用AC的公鑰PK_{AC}將$(X,Y),(X_1,Y_1)$加密為$Z = E_{PK_{AC}}(X, X_1, Y, Y_1)$，然後投票者可以利用他的e-mail EM_i傳送密文Z給AC以請求" voting certificate "。

AC在收到密文Z後利用私鑰SK_{AC}解開得到$(X, X_1, Y, Y_1) = D_{SK_{AC}}(Z)$，然後AC根據投票者的e-mail帳號$EM_i$對照得知投票者的公鑰$PK_i$，然後去判斷簽章$X = ?D_{PK_i}(X_1)$和$Y = ?D_{PK_i}(Y_1)$，如果簽章$(X_1, Y_1)$是正確的，則AC利用自己的私鑰對盲化的訊息$(X,Y)$作簽章為$X_2 = E_{SK_{AC}}(X)$和$Y_2 = E_{SK_{AC}}(Y)$，然後將盲簽章$(X_2, Y_2)$利用投票者的功要加密計算為$W = E_{PK_i}(X_2, Y_2)$回傳給投票者，並將投票者的e-mail EM_i記錄下來，避免重複認證。

投票者收到AC傳來的W後利用私鑰解密得到(X_2, Y_2)，接著投票者利用盲因子r_1和r_2進行去盲化的動作得到真正的簽章$SG_1 = B^{-1}(X_2, r_1) = E_{SK_{AC}}(C)$和$SG_2 = B^{-1}(Y_2, r_2) = E_{SK_{AC}}(H(ID_i \| a))$。

在投票者通過AC認證後，還必須向SC認證，為了其他的簽章證明與確保選票

在計票階段是否被正確計算，提供 SC 一些認證的資訊來幫助 SC 監督 TC。所以投票者再一次的選擇另一個盲因子 r_3，並將 C 盲化為 $X_3 = B(C, r_3)$，接著將 $X_3, H(ID_i \| a), SG_2$ 利用 SC 的公鑰 PK_{SC} 加密為 $Z_1 = E_{PK_{SC}}(X_3, H(ID_i \| a), SG_2)$，透過 e-mail 傳送給 SC。SC 收到後解密得到 $X_3, H(ID_i \| a), SG_2$，然後 SC 去計算 $H(ID_i \| a) = ? D_{PK_{AC}}(SG_2)$ 確認 $H(ID_i \| a)$ 是否為 AC 所簽，然後 SC 利用自己的私鑰 SK_{SC} 對 X_3 作盲簽章得到 $X_4 = E_{SK_{SC}}(X_3)$。此外，SC 隨機選擇另一個亂數 b 加入 $H(ID_i \| a)$ 得到 $H(H(ID_i \| a) \| b)$，SC 利用私鑰 SK_{SC} 對 $H(H(ID_i \| a) \| b)$ 作簽章 $SG_3 = E_{SK_{SC}}(H(H(ID_i \| a) \| b))$，最後將 $H(H(ID_i \| a) \| b)$，SG_3 和 X_4 回傳給投票者。投票者收到後透過計算 $H(H(ID_i \| a) \| b) = D_{PK_{SC}}(SG_3)$ 確認 SG_3 為 SC 的簽章後，投票者利用盲因子 r_3 去盲化得到簽章 $SG_4 = B^{-1}(X_4, r_3) = E_{SK_{SC}}(C)$。

3.5.3 Voting phase

投票者在進行投票之前必須使用 voting certificate $(H(ID_i \| a), SG_2)$ 登入 TC。TC 藉由計算 $H(ID_i \| a) = ? D_{PK_{AC}}(SG_2)$ 來確認投票者的帳號密碼是否正確。在投票者成功登入 TC 後，他將選票及參數 $C, SG_1, SG_3, H(H(ID_i \| a) \| b), SG_4$ 透過 SSL 網頁傳給 TC。TC 收到這些資訊後，藉由計算 $M_1^{'} = D_{PK_{AC}}(SG_1), M_2^{'} = D_{PK_{SC}}(SG_3)$ 確認 $C = ? M_1^{'} = ? M_2^{'}$ 來驗證選票的正確性。此外 TC 為了驗證 $H(H(ID_i \| a) \| b)$ 是否為 SC 所簽章而計算 $H(H(ID_i \| a) \| b) = ? D_{PK_{SC}}(SG_4)$。

如果選票資訊通過認證程序的話，TC 將 $H(ID_i \| a)$ 紀錄當作為投過票的投票者以避免投票者重複投票。最後投票結束後 TC 將 $H(H(ID_i \| a) \| b), SG_4$ 和 M' 紀錄到計票結果選單內。

3.5.4 Tally phase

當投票結束後，TC 停止投票的流程，CA 將私鑰 SK_{se} 公開，TC 得到私鑰後將選票 C 解密得到 $M' = E_{SK_{se}}(C)$，然後將 $H(H(ID_i \| a) \| b), SG_4, C$ 和 M' 紀錄到選票 M 上，最後 TC 將計票結果選單公開，任何投票者和 SC 都可以去確認計票結果。

利用盲簽章來實作電子投票系統，由於簽章者沒辦法得知他所簽的文件到底是甚麼樣的文件，可能會有簽章者並不願意簽內容不明的文件，這也是盲簽章的一個問題所在。於是就有學者利用模糊簽章來取代盲簽章當做有效票的憑證來實作電子投票系統以解決盲簽章的問題。

3.6 基於模糊簽章之電子投票系統

2008 年 12 月，C. Song 等學者提出了基於模糊簽章[17]的技術來實作電子投票系統。在這篇文章中提出了投票者有可能傳送一些使簽章者無法簽章的訊息來影響干擾整個投票。所以 C. Song 等學者提出了一個新的電子投票方法，它可以確保已簽章的選票中所留的訊息確實是 L 位候選人的其中一個。

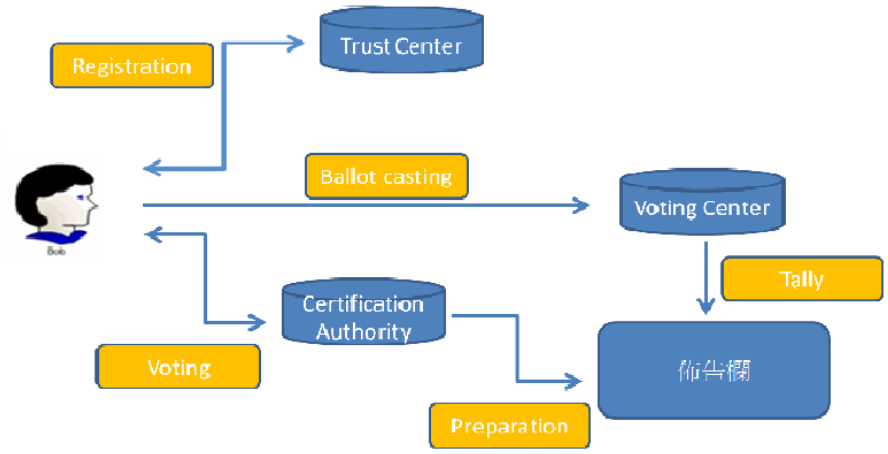

圖 3-10 C.Song 等學者的基於模糊簽章之電子投票系統架構

首先，他們定義了四個角色：

一、**Trusted Center(*TC*)**：用來驗證投票者的資格。

二、**Certification Authority(*CA*)**：確認投票者的資格，並負責對選票簽章，負責所有的投票相關事項。

三、**Voting Center(*VC*)**：負責收集所有選票，計算票數，並公布選舉的結果。

四、**Voter(*V*)**：具有投票資格的投票者。

此外，定義了一個公布欄可以公布相關資訊。在 Y-C. Lai 的 *A Study on Digital Blind Signature and Its Applications to Electronic Voting and Electronic Cash* 方法裡，*TC* 公布所有取得認證的投票者的 pseudo-name 在公布欄上，*CA* 公布它的公鑰，*VC* 則公布選票以及投票最後的結果。沒有任何一個機構能消除在公布欄上的任何資訊。

他們的方法總共有五個步驟：Preparation phase, Registration phase, Voting phase, Ballot casting phase, Tally phase。

3.6.1 Preparation phase

這個步驟首先定義參數，p，q 是很大的質數其中 $q|p-1$，$q \geq 2^{140}, p \geq 2^{512}$，$\alpha \in_R Z_p^*$ 序為 q，g, h 兩個元件屬於 Z_p^* 與 α 有相同序。$H:\{0,1\}^* \rightarrow Z_q^*$，$f:\{0,1\}^* \rightarrow Z_q^*$ 這兩個為 one way hash functions。

CA 選擇一個亂數 $x \in_R Z_q^*$，計算出投票系統的公鑰 $y = g^x \bmod p$ 然後公告給投票者。*CA* 也將 L 個候選人的列表公布 $\{CAN_1, CAN_2, ..., CAN_L\}$。所有參與者在此階段公布他們的公鑰在公布欄上。

3.6.2 Registration phase

想加入投票系統的投票者必須先向 *TC* 註冊，具有投票資格的人才能參與投票。

首先投票者 *V* 選擇 $a \in_R Z_p^*$，計算相對應的公鑰 $v = \alpha^{-a} (\bmod p)$，然後 *V* 將(*ID*,*v*)傳送給 *TC*，其中 *ID* 為 *V* 的認證字串，*v* 為 *V* 的 pseudo-name。

TC 收到訊息後驗證 *V* 的身分及投票資格，如果 *V* 具有投票資格則 *TC* 對 *v* 簽章 $s = Sign_{TC}(v)$，然後回傳認證 $C(V) = (v, s)$ 給 *V*。*TC* 將所有獲得認證的投票者的 pseudo-name 公布到公布欄上。

3.6.3 Voting phase

在這個階段中，假設投票者想得到 *CA* 對於訊息 $CAN_j \in \{CAN_1, CAN_2..., CAN_j\}$ 所簽的模糊簽章。

步驟 1：

V 由 *L* 個候選人中選擇心中所屬的候選人，假設選擇了第 *j* 個候選人 CAN_j，然後他計算出 $c = g^r h^j \bmod p$，$r \in Z_q^*$ 為 *V* 所選的一個亂數。接著將(*c*,*C(V)*)傳送給 *CA*，*CA* 利用 Schnorr identification 方法認證 *V* 的身分，假如是具資格的投票者，則 CA 選擇一亂數 $k_i \in_R Z_q^* (1 \le i \le L)$，$K_i = g^{k_i} \bmod p$，$\hat{e}_i = H(CAN_i, K_i c/(gh)^i \bmod p)$，$\hat{s}_i = k_i - x\hat{e}_i \bmod q$，接著傳送 $(\hat{e}_i, \hat{s}_i)\ (1 \le i \le L)$ 給投票者 *V*，並將 *C(V)*存進資料庫。

步驟 2：

V 計算 $\delta_i = g^{(r-i)} h^{(j-i)} \bmod p (1 \le i \le L)$，如果 $\hat{e}_i = (CAN_i, g^{\hat{s}_i} y^{\hat{e}_i} \delta_i \bmod p)$，則 *V* 得到了模糊簽章。接著 *V* 計算 $e = \hat{e}_j$，$s = r - j + \hat{s}_j \bmod q$，則 CAN_j 的簽章為 $\sigma = (e, s)$。

3.6.4 Ballot casting phase

投票階段將持續到投票截止。

步驟 1：

V 計算 $CAN' = f(CAN_j, \beta)$，f 為一個使用亂數金鑰 β 的 secure bit-commitment 方法。然後 *V* 將 (σ, CAN') 傳送給 *VC*。

步驟 2：

VC 收到 *V* 傳送的資料後，檢查 σ 是否存在資料庫內，如果沒有則 *VC* 將 σ 存進資料庫中並且將 (t,σ,CAN') 公布到公布欄上，t 為一序列數字；如果 σ 存在於資料庫中，則將訊息丟棄。

3.6.5 Tally phase

當投票截止後即進入計票階段。

步驟 1：

V 檢查他的選票是否在名單內，如果沒有則重新傳送 (σ,CAN') 給 *VC*。

步驟 2：

V 將金鑰 β 和序列數 t 經由匿名通道傳送給 *VC*。

步驟 3：

VC 將 $CAN' = f(CAN_j,\beta)$ 解開得到 CAN_j，然後 *VC* 檢查在選票 CAN_j 上 *CA* 的簽章，只有在 $e = H(CAN_j, g^s y^e \bmod p)$ 成立時 *VC* 才能確定是合法簽章。*VC* 將 $(t,\sigma,CAN',CAN_j,\beta)$ 公布到公布欄上。

步驟 4：

VC 開始計票並將投票結果公布。

第四章　　研究方法

基於模糊簽章來實作電子投票系統是很好的想法，但我們發現在 C. Song 等學者的實作中可能會產生幾個問題。首先，任何人都有可能在開票前就可以先得知投票者將選票投給了誰，而失去了投票者應有的隱私性。另外，在開票階段時需投票者的參與(傳送之前加密用的密鑰)，因此降低了實用性並增加了投票者的負擔。

一、投票者的負擔：

這個方法在最後 Tally phase 時，投票中心 *VC* 還是需要投票者 *V* 透過匿名通道傳送金鑰 β，如此 *VC* 才能夠解出 *V* 所投的候選人結果。本來投票者 *V* 投完票後，只需要等待開票結果就好，但是因為這道程序，使得投票者在投票結束後還必須多做一件事情(在開票時)，否則自己的票將無法被正確的計數。這無形中增加了投票者的負擔。

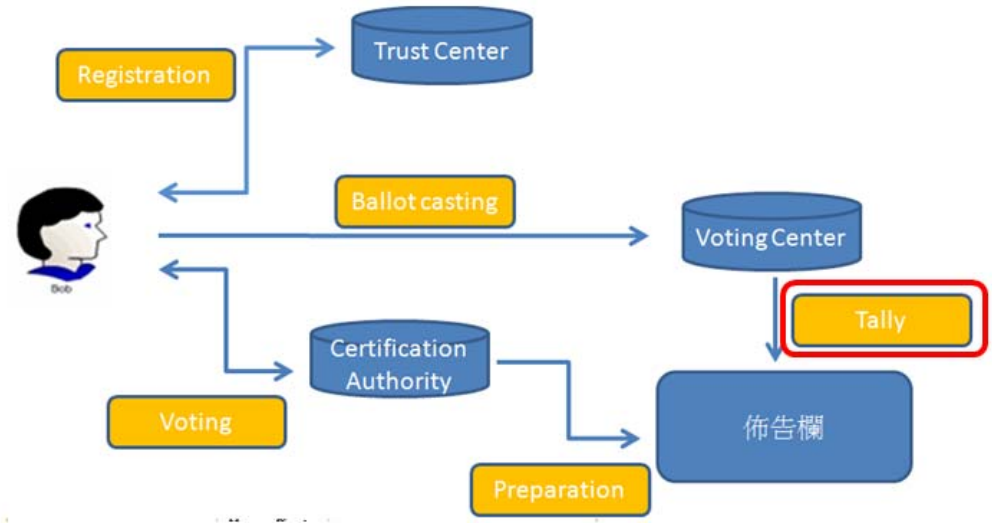

圖 4-11 Tally phase 造成投票者的負擔

二、可預測性：

在 Voting phase 中，任何一張有效的投票都會得到 CA 對訊息 $CAN_j \in \{CAN_1, CAN_2 ..., CAN_j\}$ 所簽的模糊簽章 $\sigma = (e, s)$。然後在 Ballot casting phase 中，投票者會將 σ 傳送給 VC。但為保障投票的公正性，此簽章 σ 的正確性應在 Tally phase，也就是記票階段才可被驗證。簽章的正確性是透過計算 e 是否等於 $H(CAN_j, g^s y^e \bmod p)$ 的值來驗證。然而，任何攻擊者其實在開票之前，就可事先知道每張有效票的投票的結果。因為 g, y, p 是公開的，而 e, s 攻擊者可以經由 Ballot casting phase 的步驟 2 擷取獲得 $\sigma = (e, s)$，所以驗證方程式只剩下 CAN_j 無法得知，但是因為候選人是有限個，因此攻擊者可以透過暴力攻擊法一個一個代入測試得知選票是投給哪位候選人，進而取得投票最後的結果，達到投票結果的可預測性。

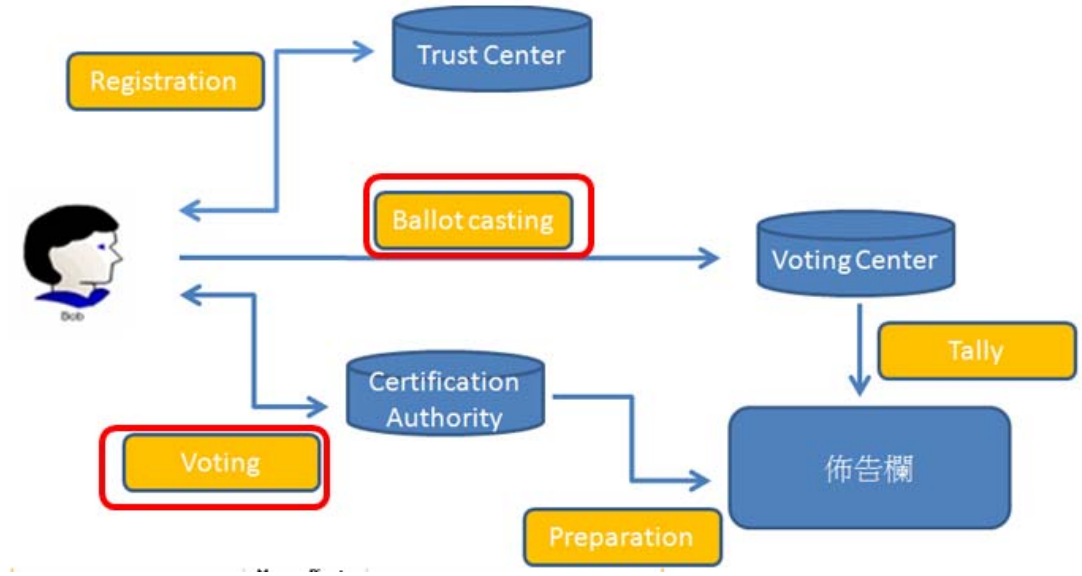

圖 4-12 Voting phase 與 Ballot casting phase 造成選票可預測性

上述的兩個問題，我們認為這是可以改進而且必須要改進的缺點。針對這些可改善的部份我們提出了改良的方案並參考愛沙尼亞國家的電子投票系統的優點做結合，設計出一個基於模糊簽章的電子投票系統。

本章接下來將在 4.1 節介紹系統架構，讓大家了解系統是如何的運作。接著 4.2 節將一一介紹系統所參與的單位及元素，還有一些系統的參數定義。然後在 4.3 節的部分，我們將介紹投票者開始投票的流程以及投票結束後的計開票流程，說明完我們的流程後，繼續的深入了解我們電子投票系統的方法與步驟。

4.1 系統架構

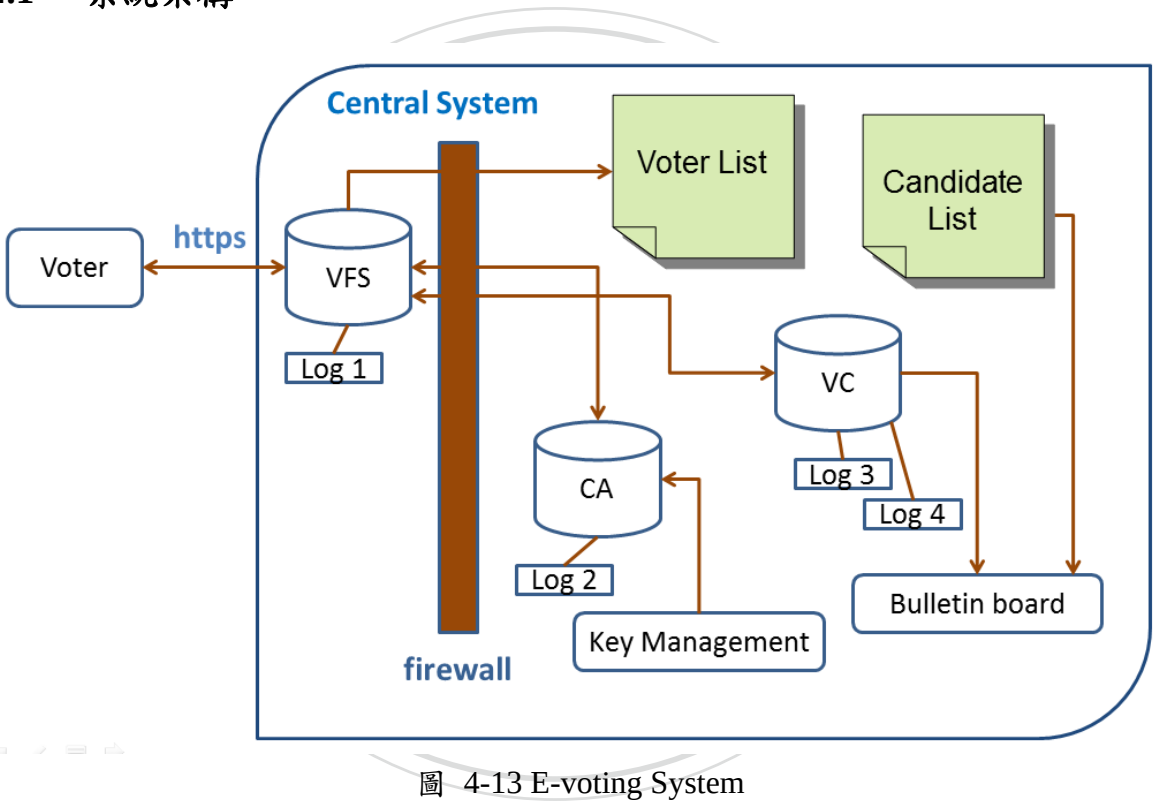

圖 4-13 E-voting System

上圖為我們提案方式的系統架構圖，由圖中可以清楚顯示我們的系統可分為兩個主要的角色：一個投票者 Voter 與系統的主機 Central System。每位投票者利用電腦透過網路連上系統的 https 網頁後與系統內的 Central System 進行一連串的投票動作，由於 https 網頁由 SSL 加密協定所保護，所以保證投票者與系統之間的溝通傳送不會遭到竊聽或是竄改。我們在下一節將一一介紹圖中系統架構內的角色以及系統操作步驟及流程。

4.2 系統定義

首先系統內定義有四個角色：

一、**Vote Forwarding Server(*VFS*)**：處理投票者V_l由 https 網頁與 Server System 的一切互動。其中包括驗證投票者身分、傳送$C(V_l)$認證給具投票資格的投票者V_l、負責傳送V_l與 *CA* 之間的參數並取得 *CA* 對有效票的憑證及最後傳送V_l的選票到 *VC* 儲存等待投票結束後做最後的統計。

二、**Certification Authority(*CA*)**：藉由驗證 *VFS* 所傳送給V_l的$C(V_l)$來確認投票者的資格，並負責對投票者所選的候選人名單做模糊簽章，在投票開始前負責所有的投票所需參數產生等相關事項。

三、**Voting Center(*VC*)**：投票結束前，負責收集所有投票者傳送的選票。投票結束後，解開選票並驗證 *CA* 的模糊簽章，然後計算票數，最後公布選舉的結果。

四、**Voter** V_l：V_l為具有投票資格的投票者。經由 *VFS* 確認身分後取得 *VFS* 所傳送的$C(V_l)$當作身分證明。在投票開始時，選擇候選人並取得 *CA* 所產生之模糊簽章後，將選票加密傳送給 *VC* 以完成投票。投票結束並開票完成後，仔細比對選票是否被計票，如有疑慮立即向選務中心提出並要求驗票。

以下將更進一步解釋整個電子投票架構的流程，在解釋的過程中也用到了許多我們自訂意義的符號，而所有的相關符號所代表的功用及意義，我們將在下面做簡單的整理描述：

一、PK_{CA}/SK_{CA}：*CA* 利用公開金鑰密碼系統(如 RSA、ElGamal 等方法)所生成的系統公/私鑰對。用於產生模糊簽章及 *VC* 驗證簽章時使用。

二、PK_{VFS}/SK_{VFS}：*VFS* 利用公開金鑰密碼系統(如 RSA、ElGamal 等方法)所生成的公/私鑰對。用於對V_l的身分認證產生簽章及驗證。

三、PK_{VC}/SK_{VC}：*CA* 利用公開金鑰密碼系統(如 RSA、ElGamal 等方法)所生成的系統公/私鑰對。V_l利用公鑰PK_{VC}加密選票，而 *VC* 利用私鑰SK_{VC}解密選票，SK_{VC}在投票期間結束開始計票時由 *CA* 秘密傳送給 *VC*。

四、PK_{V_l}/SK_{V_l}：V_l擁有的 ID-Card 利用公開金鑰密碼系統(如 RSA、ElGamal 等方法)所生成的系統公/私鑰對。用於V_l的身分認證。

五、$E_x(m)$：如金鑰 x 為公鑰(*PK*)則此為對 m 之加密演算法；如金鑰 x 為私鑰(*SK*)則此為對 m 之簽章演算法。

六、$D_y(m)$：如金鑰 y 為公鑰(*PK*)則此為對 m 之驗證演算法；如金鑰 y 為私鑰(*SK*)則此為對 m 之解密演算法。

七、$s_{VFS} \leftarrow E_{SK_{VFS}}(PK_{V_l})$：*VFS* 對於$V_l$的 pseudo-name 驗證$V_l$具有投票資格而利用私鑰$SK_{VFS}$所做的簽章，要驗證此簽章必須利用公鑰$PK_{VFS}$。

八、$C(V_l)$：$C(V_l)=(PK_{V_l}, s_{VFS})$，$V_l$經由 *VFS* 確認具投票資格後由 *VFS* 傳送給V_l的認證，以此證明V_l的身分及投票資格。

九、$H(m)$：單向雜湊函數(one way hash functions)。

十、$\sigma_{OB}=(e,s)$：*CA* 對於V_l所選候選人所產生的模糊簽章。

另外，我們定義了一個電子公布欄 Bulletin Board 可以公布相關資訊。在我們的方法裡，*VFS* 公布所有取得認證的投票者在公布欄上，*CA* 公布它的公鑰 PK_{CA}, PK_{vc}，*VC* 則公布選票以及投票最後的結果。沒有任何一個機構能消除在公布欄上的任何資訊。

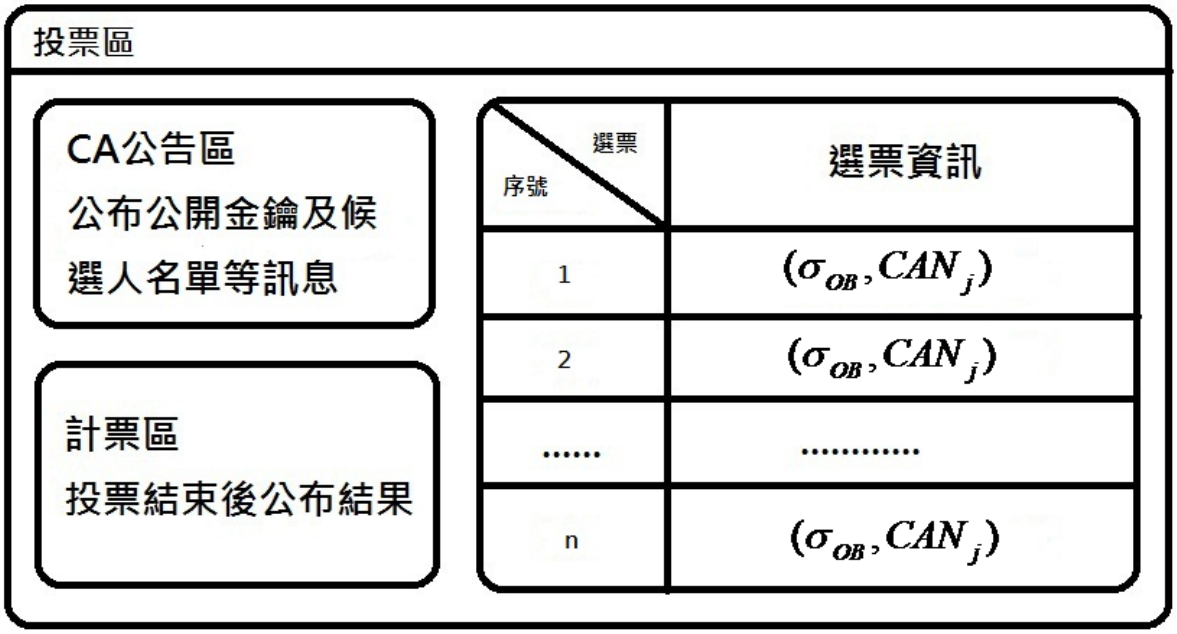

圖 4-14 投票系統中的電子公布欄

4.3 投票流程與方法步驟

我們所提出的方法在投票開始事前的準備、投票開始的流程以及投票結束後的計票流程幾乎與一般傳統投票或是與現有的電子投票如愛沙尼亞電子投票相同，一切都按標準程序進行。

下圖 4-5 及圖 4-6 為整個投票從開始投票到結束投票後開始計票的流程。而我們將投票的流程再細分為總共有六個階段：準備階段、註冊登入階段、驗證階段、投票階段、計票階段、爭議驗證階段。下面將針對此六個階段一一描述。

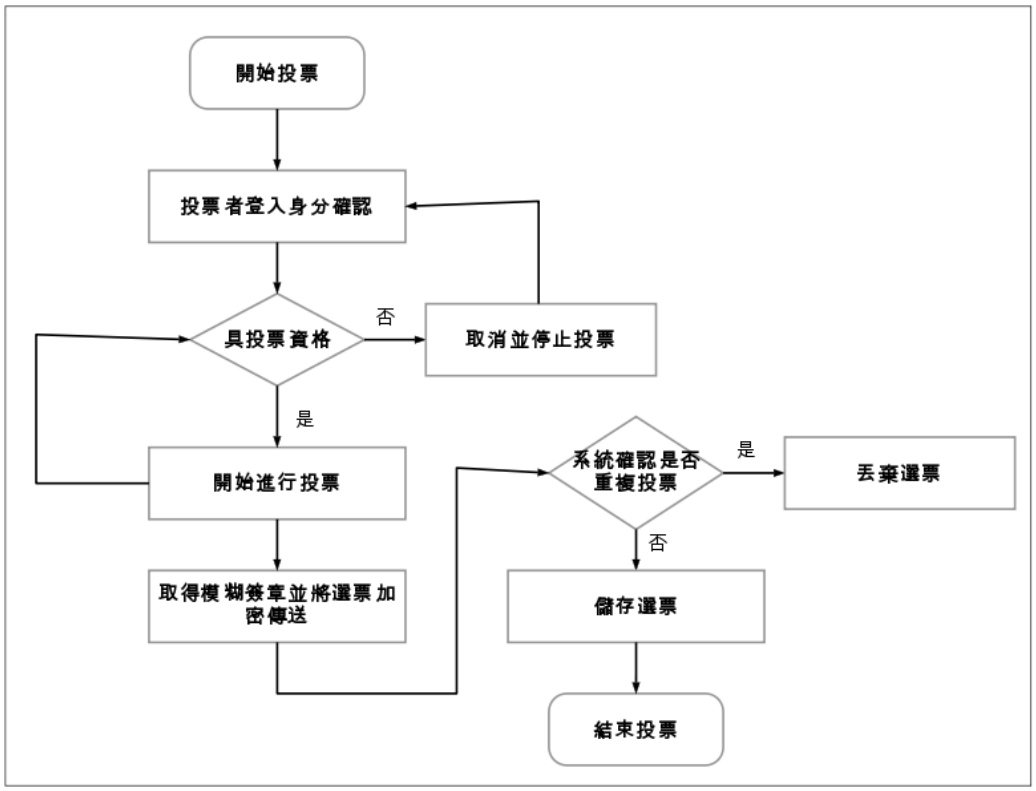

圖 4-15 投票者投票的流程

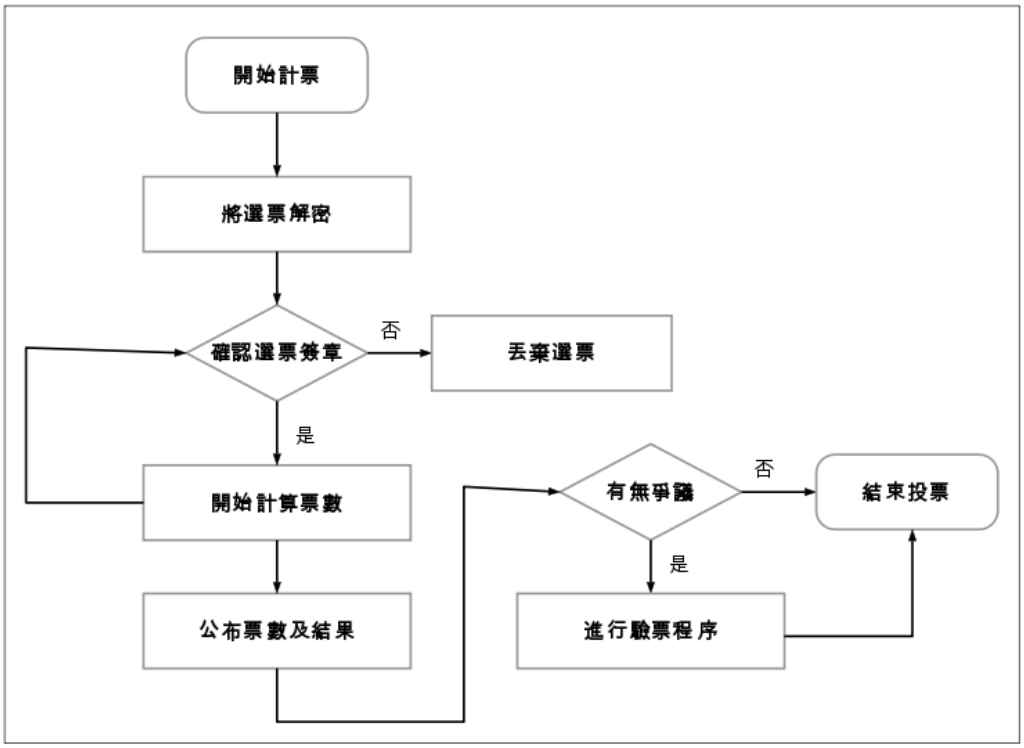

圖 4-16 投票結束後系統計票流程

4.3.1 準備階段

這個步驟首先定義參數，p，q 是很大的質數其中 $q|p-1$，$q \geq 2^{140}, p \geq 2^{512}$，$\alpha \in_R Z_p^*$ 序為 q，g, h 兩個元件屬於 Z_p^* 與 α 有相同序。$H:\{0,1\}^* \rightarrow Z_q^*$，為單向雜湊函數(one way hash functions)，可以利用如 MD5 及 SHA-1 來產生。

CA 選擇一個亂數 $SK_{CA} \in_R Z_q^*$，計算出投票系統的公鑰 $PK_{CA} = g^{SK_{CA}} \bmod p$，另外選擇一個亂數 $SK_{VC} \in_R Z_q^*$ 作為解開選票用的私鑰，其對應的加密選票用的公鑰為 $PK_{VC} = g^{SK_{VC}} \bmod p$，然後將兩把公鑰 PK_{CA}, PK_{VC} 公告給投票者。*CA* 也將公布 L 個候選人的列表 $\{CAN_1, CAN_2, ..., CAN_L\}$。

在投票期間之前，投票者必須親自利用身分證與印章到政府機構(投票中心)申請一張可以證明身分的 ID-Card，而 ID-Card 就代表著投票者的網路身分證，此 ID-Card 包含了投票中心的憑證 $CV_{\text{投票中心}}$ 與投票者的 ID_l 與公私鑰 PK_{V_l} / SK_{V_l}，其 ID-Card 的功能與目前已有的「自然人憑證」[24]功能相似，未來或許可以與「自然人憑證」做結合。投票者利用此 ID-Card 才能進入我們的投票網頁系統進行身分的認證與投票。

4.3.2 註冊登入階段

投票期間投票者 V_l 利用 ID-Card 登入系統時將 $CV_{\text{投票中心}}$ 與 $\mathrm{E}_{\mathrm{SK}_{V_l}}(ID_l, PK_{V_l})$ 傳送給 *VFS*，其中 ID_l 為 V_l 的認證身分，PK_{V_l} 為 V_l 的公鑰。*VFS* 收到訊息後確認 V_l 的身分及

投票資格，如果V_l具有投票資格則 *VFS* 對PK_{V_l}簽章$s_{VFS} \leftarrow E_{SK_{VFS}}(PK_{V_l})$，並且比對投票者$V_l$的戶籍地與選區來傳送相對應的候選人名單，然後回傳認證$C(V_l) = (PK_{V_l}, s_{VFS})$給$V_l$以供 CA 驗證。*VFS* 將獲得認證的投票者的PK_{V_l}公布到公布欄上並記錄在 log1 檔裡。

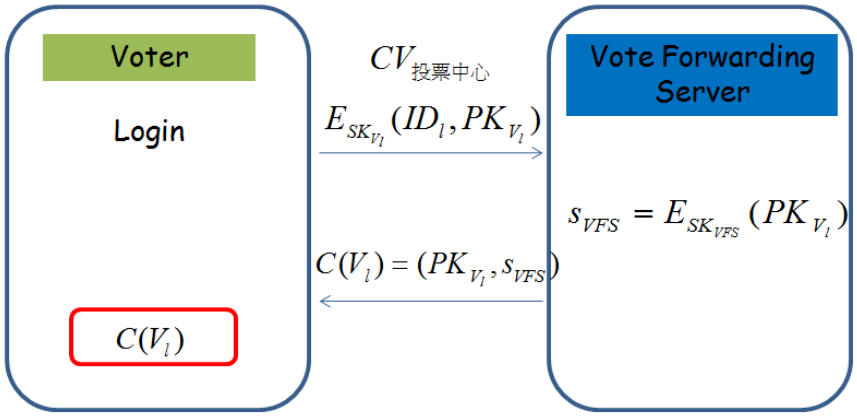

圖 4-17 註冊登入階段

4.3.3 驗證階段

步驟 1：

V_l由 *L* 個候選人中選擇心中所屬的候選人，假設選擇了第 *j* 個候選人CAN_j，然後他計算出$c = g^r h^j \bmod p, \gamma = \alpha^z \bmod p$，$r, z \in Z_q^*$為 *V* 所選的兩個亂數。接著將$(c, \gamma, C(V_l))$透過 *VFS* 傳送給 *CA*，*CA* 利用 Schnorr identification 方法驗證V_l的身分，首先 *CA* 利用 *VFS* 的公鑰來驗證$C(V_l) = (PK_{V_l}, s_{VFS})$中的$s_{VFS} = E_{SK_{VFS}}(PK_{V_l})$，證明$C(V_l)$確實由 *VFS* 所簽章的，*CA* 傳送一亂數 d,$1 \le d \le 2^t$給V_l，t 為一秘密參數，而V_l收到後則計算$u = (z - SK_{V_l} d) \bmod q$給 *CA*，*CA* 去驗證$\gamma \equiv \alpha^u PK_{V_l}^{\ d} \bmod p$，等式成立則

CA 接受了 V_l 的身分證明，則 CA 選擇亂數 $k_i \in_R Z_q^*(1 \le i \le L)$，$K_i = g^{k_i} \bmod p$，$\hat{e}_i = H(CAN_i, K_i c/(gh)^i \bmod p)$， $\hat{s}_i = k_i - SK_{CA}\hat{e}_i \bmod q$，接著透過 VFS 傳送 $(\hat{e}_i, \hat{s}_i)$,$1 \le i \le L$ 給 V_l ，並將 $C(V_l)$ 存進資料庫並記錄於 log2 檔裡。

步驟 2：

V_l 計算 $\delta_i = g^{(r-i)}h^{(j-i)} \bmod p(1 \le i \le L)$，如果 $\hat{e}_i = H(CAN_i, g^{\hat{s}_i} PK_{CA}^{\hat{e}_i} \delta_i \bmod p)$，則 V_l 得到了模糊簽章。接著 V_l 計算 $e = \hat{e}_j$， $s = r - j + \hat{s}_j \bmod q$ ，則對 CAN_j 的簽章為 $\sigma_{OB} = (e, s)$ 。

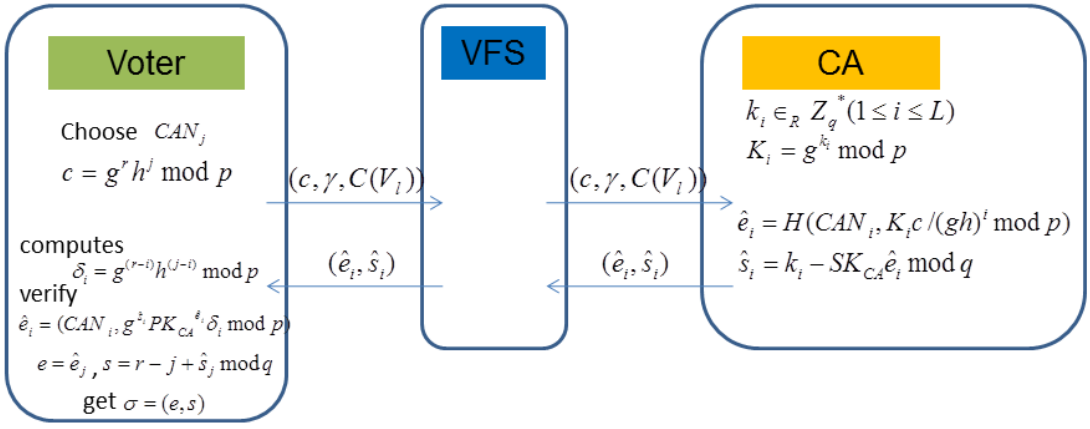

圖 4-18 驗證階段

4.3.4 投票階段

在這個階段中，共有兩個步驟來完成投票者 V_l 將選票經由 VFS 送至 VC。

步驟 1：

V_l 將 $(\sigma_{OB} \| CAN_j)$ 利用 CA 所公開的金鑰 PK_{VC} 透過公開金鑰加密系統加密得到一密文 $C_{V_l} = E_{PK_{VC}}((\sigma_{OB} \| CAN_j))$ 。

步驟 2：

V_l 將 $(C(V_l), C_{V_l})$ 透過 *VFS* 傳送至 *VC*，*VFS* 檢查 $C(V_l)$ 是否已存在資料庫中，如果沒有則將 $C(V_l)$ 存入，然後將 C_{V_l} 傳送給 *VC*，*VC* 將 C_{V_l} 儲存；如果 $C(V_l)$ 已存在資料庫中，則 *VFS* 將訊息丟棄。

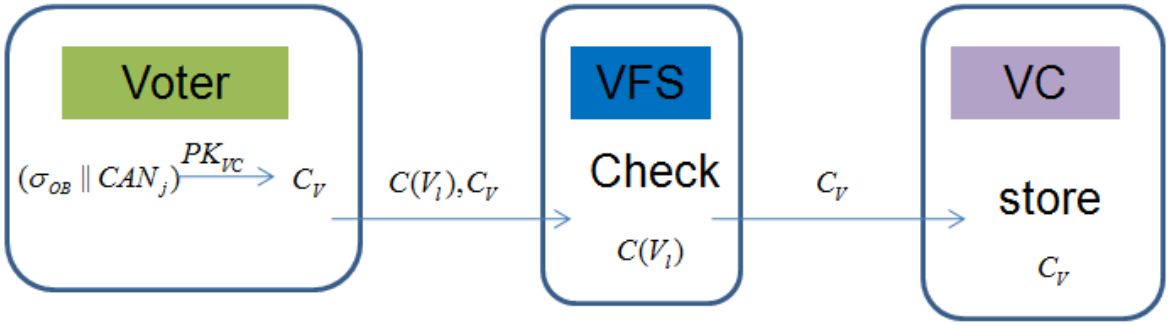

圖 4-19 投票階段

4.3.5 計票階段

當投票時間結束，*VC* 準備開始計票。

步驟 1：

CA 將解密私鑰 SK_{VC} 傳給 *VC*。*VC* 解密得到 $D_{SK_{VC}}(C_{V_l}) = (\sigma_{OB} \| CAN_j)$，然後 *VC* 檢查 *CA* 對於選票 CAN_j 上的簽章，只有在 $e = H(CAN_j, g^s PK_{CA}^{\ e} \bmod p)$ 成立 *VC* 才能確定是合法簽章。*VC* 將 (σ_{OB}, CAN_j) 公布於公布欄上，以便讓所有人可以驗證結果，並將合法的選票與不合法的選票分開紀錄於 log3 與 log4 檔裡。

步驟 2：

VC 計算候選人的得票數並且決定出當選者後將最終結果公布。

4.3.6 爭議驗證階段

在投票期間結束進行計票到最後的公開計票結果與宣布候選人當選之後，當發現選舉投票結果有任何爭議或疑似選舉不公時，就必須進入爭議驗證階段，經過檢驗相關投票紀錄與證據，以維持選舉的公正性。如發生下列之情況，投票者或候選人可以提出申請爭議驗證的程序。

一、候選人所獲得之選票差距過小：

根據公職人員選舉罷免法[23]第六十九條規定，得票數最高與次高之候選人得票數的差距在有效票數千分之三內時，於投票日結束七日內候選人可向相關機構申請重新計票的動作並冷靜等待驗票的結果，避免不必要的衝突及爭吵。驗票結束後，也必須尊重最後的結果。

二、選票的合法與否：

當最後的結果公布後，VC 將 (σ_{OB}, CAN_j) 公布於公布欄上，而所有人都可以去驗證結果，當發現簽章 $\sigma_{OB} = (e, s)$ 驗證出來的結果與選票內容不符，就代表著這並不是一張合法的選票，而造成 VC 在計票過程中出現了錯誤記票的情形，將不合法的選票當作是合法的選票進行計票，這也是令人爭議的部分。因此，如遇到此種狀況也必須進行爭議驗證階段。

第五章　安全性分析

針對第二章提到的電子投票系統的安全性分析與考量，以下對於我們的方法做投票系統安全性的簡單敘述及分析。

一、投票資格(Eligibility)

由於投票者V_l必須得到 *VFS* 的認證$C(V_l)$才算是有資格的投票者，而 *VFS* 會去判斷投票者V_l的ID_l，ID_l可視為投票者的身分證號，每個投票者的ID_l都不相同。如果投票者的ID_l不正確或是不在 *VFS* 的資料庫內，則投票者V_l不可能得到 *VFS* 的認證$C(V_l)$，換句話說就是沒有投票資格。因此，只有合法的投票者V_l才能得到 *VFS* 的認證$C(V_l)$並具有投票資格。

二、不可重複性(Non-reusability)

假設攻擊者V_l想要進行多次投票的動作，則V_l可從兩種情況著手。

1. 第一種情況是V_l從 *VFS* 得到兩個認證$C(V_1)=(v_1, E_{SK_{VFS}}(v_1))$及$C(V_2)=(v_2, E_{SK_{VFS}}(v_2))$。而$V_l$想得到兩個不同的 *VFS* 認證就必須傳送$(ID_1, v_1)$及$(ID_2, v_2)$給 *VFS* 驗證並成功，除非 *V* 擁有兩個 *ID* 也就是$ID_1 \neq ID_2$，但每個人所擁有的 *ID* 皆是獨一無二的，所以攻擊者 *V* 想得到兩個認證$C(V_1)$及$C(V_2)$在投票階段中傳送兩次選票進行多次投票的動作是不可行的。

2. 第二種情況則是使用同一個認證$C(V_l)$進行多次投票的動作，也就是直接重送$(C(V_l), C_{v_l})$給*VFS*，但*VFS*會檢查$C(V_l)$是否已經存在資料庫中，如果有就表示之前已經投過票了，而之後利用此$C(V_l)$來進行投票的選票則會被丟棄並且告知已經投過票了。如此，攻擊者V_l想進行多次投票其實是不可行的，而*VFS*的認證及檢查資料庫都因此避免了重複投票的情況。

三、**合理性(Soundness)**

因為攻擊者無法得知*CA*的私鑰SK_{CA}為何，因此無法偽造出與*CA*一樣的簽章，即使攻擊者自己偽造出一個簽章，也順利在投票階段中投出選票，但在最後計票階段中*VC*會去驗證等式$e = H(CAN_j, g^s PK_{CA}^{\ e} \bmod p)$是否成立，成立才算是擁有合法簽章的選票，然後公開給眾人驗證。而攻擊者所偽造的簽章將無法使判斷式成立，因而被判定為不合法的簽章，此選票也被認定為廢票不被採計，因此符合合理性。

四、**完整性(Completeness)**

投票結束後，*VC*將所有合法且有計票的資訊(σ_{OB}, CAN_j)公布於公布欄上，以利於所有人都可以驗證最後的結果，如果選舉結果有問題也可以此作為驗票的依據，加快作業速度。整個投票過程從註冊登入可以投票到最後開票計票與驗證階段都是一個完整的投票流程。

五、**可驗證性(Verifiability)**

透過 *VC* 公開的訊息(σ_{OB}, CAN_j)，所有選票的簽章是可以被任何人驗證的，而最後的投票結果也可以透過公開的訊息來計數並驗證最終結果，達到可驗證性。

六、**公平性(Fairness)**

假設攻擊者想事先得知其他投票者的投票結果，則必須先侵入由 SSL 防護的安全網頁並攔截投票者傳送給 *VFS* 的資訊$(C(V_l), C_{v_l})$，然後還要得知解開C_{v_l}的私鑰將訊息解密還原為投票資訊，經過重重關卡才可以事先得知選票是投給哪位候選人的，但在正常情況下，SSL 防護的網頁無法被竊聽或攔截，而加密C_{v_l}的私鑰是由公開金鑰密碼系統(如 RSA、ElGamal 等方法)所產生的，基於離散對數問題，私鑰是無法被得知的。所以任何參與者都無法在投票結束開始計票之前得知任何有關投票者的選票的訊息。

七、**隱私性(Privacy)**

當選票利用PK_{VC}加密傳送後，由於離散對數問題，任何人都無法解密得到訊息在投票結束之前，除了 *CA*。在我們的方法中，我們假設 *VFS*，*CA* 及 *VC* 皆是獨立可信任的機構，但皆隸屬於中央選舉委員會，所以私鑰的傳送可以在 off-line 中執行，例如，將私鑰存在 CD 並密封，開票時再將 CD 送至 *VC*。另外，因為皆為可信任的機構，所以我們假設三者之間沒有任何不法的密謀。實務上可利用立法及政策上的執行來達到。另外，技術上可利用秘密分享機制(Secret Sharing Schemes)[16]來增加密謀的困難度。如此，我們提出的電子投票系統具有隱私性。

下面表 5-1 我們將列出與本論文相關之電子投票機制之研究的比較表。由於愛沙尼亞電子投票系統提供投票者可以重複投票的功能，對於我們所提出的不可重複投票這個性質而言是不符合的。針對這個部分的比較，由於愛沙尼亞投票系統為了解決買票賄選的威脅，因此允許投票者多次投票，而取最後一次投出的選票來當作最後的結果，之前所投過的票皆會被刪除丟棄，因此，一位投票者還是只會有一張選票。而我們所考慮的因素是為了要符合傳統投票一位投票者只能行使一次的投票動作，也只能有一張選票，因此我們的系統不允許重複投票的動作。但對於一位投票者只能投出一張選票存在系統中的這個原則是都符合的。我們的系統與愛沙尼亞的系統所考慮到的因素不完全相同，但愛沙尼亞國家的電子投票系統行之有年，未來詳細了解並分析後，或許也可以在我們的系統上行使允許投票者重複投票的動作；而 C.Song 等學者的投票機制在投票尚未結束前可被預先知道投票結果，則是不符合公平性的部分；關於投票結束後的爭議驗證階段在本論文與愛沙尼亞電子投票系統皆有規劃以及描述狀況與處理方式。

表 5-1 各電子投票機制比較表

	Y-C Lai 2002[9]	C.Song et.al 2008[17]	Estonia 2005[22]	Our Scheme 2010
不可重複性	✓	✓	×	✓
可驗證性	✓	✓	✓	✓
合理性	✓	✓	✓	✓
完整性	✓	✓	✓	✓
公平性(可預測性)	✓	×	✓	✓
爭議驗證	×	×	✓	✓

下面表 5-2 為與本論文相關之電子投票機制的簽章次數與加解密次數的比較表，以一位投票者從登入系統後開始投票的動作直到傳送選票到投票中心完成投票的動作來計算過程中所需的簽章次數與加解密次數，其中 L 代表此次投票候選人名單中共有 L 位候選人($L \geq 1$)，N 代表為投票者在此次投票中共執行了 $N \geq 1$ 次的投票次數(在允許多次投票的系統中)。由表 3 中可以看出在簽章次數方面，如果候選人有三個以上的話，則我們的方法是比較多次的；在加解密次數方面，由於 C.Song 等學者的方法中使用對稱加密法來加解密選票，因此對稱加解密次數為 2 次，而在非對稱加解密次數則是 Lai 學者的方法較多次有 6 次。在愛沙尼亞投票系統方面，由於系統允許投票者多次投票的動作，因此在計算簽章次數及加解密次數上較為彈性，因此取 $N \geq 1$ 來表示。而執行越多次的數位簽章與加解密對於系統端來說必須花較多的時間來處理這些動作，次數越多對系統所造成的負擔也越大；對於投票者端來說必須花較多的時間來等待投票動作的完成。因此，減少的簽章次數與加解密次數對整個電子投票系統是有利的，簽章次數及加解密次數越少，系統的負擔會越小，所花的時間也越少。

表 5-2 投票者與系統在投票過程中簽章次數與加解密次數之比較表

	Y-C Lai 2002[9]	C.Song et.al 2008[17]	Estonia 2005[22]	Our Scheme 2010
簽章次數	5	1+L	N	2+L
對稱加解密次數	0	2	0	0
非對稱加解密次數	6	0	N	1

表 5-3 說明攻擊者由系統進行攻擊之情形，攻擊者藉由找尋系統上的漏洞而進行入侵攻擊的動作，其中分為兩種攻擊類型：預知結果、竊取資料。

表 5-3 攻擊者由系統進行攻擊之情形

由系統攻擊	
攻擊類型	**抵抗方法**
預知結果	SSL 防護的網頁無法被竊聽或攔截，而加密 C_{v_l} 的私鑰是由公開金鑰密碼系統所產生的，基於離散對數問題，私鑰是無法被得知的。所以任何參與者都無法在投票結束開始計票之前得知任何有關投票者的選票的訊息。
竊取資料	本系統是由 SSL 防護的網頁，在正常情況下無法被竊聽或是攔截，所以攻擊者想要經由系統竊取個人資料或是選票資訊就必須要破解 SSL 加密網頁，這是非常困難的。

表 5-4 說明攻擊者由投票過程進行攻擊之情形，攻擊者藉由投票過程中投票規則上的問題進行破壞投票的動作，分為三種攻擊類型：逾時投票、重複投票、偽造簽章。

表 5-4 攻擊者由投票過程進行攻擊之情形

由投票過程攻擊	
攻擊類型	**抵抗方法**
逾時投票	由於系統只會在該次投票所設定的期間內開放投票者進行投票，期間之外的時間皆不會開放，所以不論攻擊者想在投票規定的時間前或時間後進行逾時投票都無法順利完成攻擊。
重複投票	1. 任何投票者 V_l 皆只有一個特定的 ID 而一個 ID 只能得到一組 *VFS* 的憑證 $C(V_l)$，因此無法一個投票者無法利用兩個憑證來進行重複投票。 2. 任何投票者無法利用一個憑證 $C(V_l)$ 進行重複投票，*VFS* 會檢查有無重複，如有重複則將之後的選票丟棄。
偽造簽章	由於 *CA* 製造簽章之公私鑰對是由公開金鑰密碼系統所生成，基於離散對數問題，因此攻擊者無法得知 *CA* 製造簽章之私鑰為何而無法偽造有效票之簽章。

第六章　結論與未來展望

本論文中提出了一個基於模糊簽章之電子投票系統機制。一般投票率的高低決定於投票當天的氣候、投票者當天是否在戶籍地所在的縣市或是一些不可抗拒的因素，而考慮到投票者的方便性以及想提高投票率的原因，因此我們探討的選舉投票方式為網路電子投票 I-voting。我們參考了愛沙尼亞國家的電子投票系統架構，再搭配了模糊簽章的概念而建立出一個完整的電子投票系統。本方法利用模糊簽章的特性，使得 *CA* 在對選票簽章時，雖然無法得知V_l所選的候選人為何，但 *CA* 可以確定V_l所選為所有候選人的其中一位而進行簽章的動作，相較於以往利用盲簽章應用於電子投票的方法上面，簽章者無法得知必須簽章的內容為何而進行簽章，使得簽章者有不確定性的感覺，因此，我們認為利用模糊簽章應用在電子投票的方法上面是比利用盲簽章應用來的比較妥當。

在我們所提的方法中，我們利用具有一個公正憑證的 SSL 網站，利用 https 網頁來進行投票者與系統之間的參數傳遞，避免遭到監聽、竊取資料甚至是進行中間人攻擊等等。透過系統的身分認證，成功進行投票並取得 *CA* 對於選票的模糊簽章使得計票中心 *VC* 可以判斷是否為有效票，投票結果揭曉後，投票者可進行驗證投票的正確性，如有疑慮可進一步提出驗票的要求。我們所提的方法除了可以使得投票率增加，也解決了先前學者所提的方法的缺點：1.選舉結束後將解密的 key 傳送給 *VC* 進行解開選票的動作增加了投票者的負擔；以及 2.由於選舉的公平性，因此在選舉投票結束之前，任何人都無法得知選票內容及選舉結果，但由於公開驗證簽章的數學算式可能導致選票內容的洩漏造成選舉的可預測性。而我們提出的方法也符合投票的基本安全性，

像是：不可重複性、合理性、完整性、可驗證性、公平性、隱私性等等。

一個選舉投票的過程中，令人擔心且必須得解決的問題便是買票賄選甚至是進行暴力脅迫等方式控制投票者的選票，這些能算是人性的問題，也是選舉投票最難以控制的狀況。針對網路電子投票對不可脅迫性的解決方案，愛沙尼亞的作法為允許投票者重複投票，但我認為即使可以重複投票，有心人士依舊能以暴力脅迫的方式控制投票者到投票的最後一刻，如此也不能完全解決不可脅迫性。因此網路電子投票所帶來的便利性與不可脅迫性之間的拿捏，我想是未來必須要詳加考慮且值得研究的重點，如能改善買票賄選或暴力脅迫的情況，將使得網路電子投票更為完善。

參考文獻

[1] O. Cetinkaya, A. Doganaksoy. "*Pseudo-Voter Identity (PVID) Scheme for e-Voting Protocols*". ARES'07, IEEE, 2007, pp. 1190-1196.

[2] D. Chaum. "*Blind signatures for Untraceable Payments*". Advances in Cryptology-Crypto'82. Plenum Press, 1983, pp. 199-203.

[3] D. Chaum. "*Elections with Unconditionally-Secret Ballots and Disruption Equivalent to Breaking RSA*". Advances in Cryptology-EUROCRYPT'88, Springer-Verlag, 1989, pp. 177-182.

[4] D. Chaum, E. van Heijst. "*Group signatures*". IN: Davies, D.W.(ed.) EUROCRYPT 1991. Springer, LNCS, Vol. 547, 1991, pp. 257-265.

[5] L. Chen. "*Oblivious signatures*". IN: Gollmann, D.(ed.) ESORICS 1994. Springer, LNCS, Vol. 875, 1994, pp. 161-172.

[6] W. Diffie and M.E. Hellman. "*New Directions in Cryptography*". IEEE Transactions on Information Theory, Vol. IT-22, No. 6, 1976, pp. 644-654.

[7] T. ElGamal. "*A Public Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms*". CRYPTO '84, Springer, LNCS, 1985, pp. 10-18.

[8] J. Kim, K. Kim, and C. Lee. "*An Efficient and Provably Secure Threshold Blind Signature*", ICICS2001, Springer, LNCS 2288, springer-verlag, Berlin Heidelberg, 2001, pp. 318-327.

[9] Y-C. Lai. "*A Study on Digital Blind Signature and Its Applications to Electronic Voting and Electronic Cash*", 2002, available at http://ethesys.lib.cyut.edu.tw/ETD-db/ETD-search-c/view_etd?URN=etd-0715102-132859.

[10] Y-H. Li, S-Y. Wu. "*Research on a New E-voting Method based on the Cellular Phone*". ISECS2008, IEEE, 2008, pp.818-821.

[11] C. H. Lim and P. J. Lee. "*A key recovery attack on discrete log-based schemes using a prime order subgroup*". Springer, LNCS, CRYPTO '97, 1998, pp. 249-263.

[12] X. Lin, R. Lu, H. Zhu, P. Ho and X. Sherman. "*Provably Secure Self-certified Partially Blind Signature Scheme from Bilinear Pairings*". ICC2008, 2008, pp. 1530-1535.

[13] M. Mambo, K. Usuda, and E. Okamot. "*Proxy signature: delegation of the power to sign messages*". IEICE Trans, Fundamentals, Vol. E79-A, NO.9, 1996, pp. 1338-1353.

[14] D. Pointcheval. "*Practical Security in Public-Key Cryptography*". Springer, LNCS, ICISC 2001, 2001, pp. 223-241.

[15] C.P. Schnorr. "*Efficient signature generation for smart cards*". Journal of Cryptology, 1991,4(3). pp. 161- 174.

[16] A. Shamir. "*How to Share a Secret*". Communications of ACM, vol.22, no.11, 1979, pp.612-613.

[17] C. Song, X. Yin, Y. Liu. "*A Practical Electronic Voting Protocol Based upon Oblivious Signature Scheme*". CIS2008, IEEE, 2008, pp. 381-384.

[18] R. Tso, T. Okamoto and E. Okamoto. "*1-out-of-n oblivious signatures*". In Proceedings of the 4th Information Security Practice and Experience Conference (ISPEC2008), Springer, LNCS Vol. 4991, 2008, pp. 45-55.

[19] S. Wang, H. Fan, G. Cui. "*A proxy blind signature schemes based DLP and applying in e-voting*". ICEC '05, ACM, 2005, pp. 641-645.

[20] B-Y. Wang, F. Yang, Y-F. Hu. "*Online Voting Scheme Based on Blind Digital Signature*". MINIMICRO SYSTEM, 2002(3), pp. 588- 591.

[21] X. Yi, R. Tso. "*Mobile Electronic Election Using Smart Cards*". Communications of the CCISA Vol. 16 No. 1, 2010, pp. 26-40.

[22] http://www.vvk.ee/public/dok/Yldkirjeldus-eng.pdf, "E-Voting System", Tallinn 2005.

[23] http://www.6law.idv.tw/6law/law/公職人員選舉罷免法.htm, “公職人員選舉罷免法”, 2010 年修改。

[24] http://moica.nat.gov.tw/html/index.htm, “內政部憑證管理中心”。

[25] 王淳，NCKU 電子投票系統之安全性分析，國立成功大學工學院工程管理碩士在職專班論文，2008 年。

[26] 李秉禮,具選票驗證之匿名電子投票機制,佛光大學資訊學系碩士在職專班論文，2007 年。

[27] 吳正義、楊吳泉、金明浩，選民可即時檢驗之電子投票系統設計，資通安全通訊專論，2010 年。

[28] 范俊逸,抗暴力脅迫之匿名電子投票系統,國立中山大學資訊工程學系碩士論文，2006 年。

[29] 莊文勝、吳靖琳，電子投票，資通安全分析專論，T94008，2005 年。