國立交通大學

資訊科學系

碩 士 論 文

使 用 可 記 憶 密 碼 的 電 子 投 票 機 制

An Electronic Voting Scheme Using Memorable Password

研 究 生：張政偉

指導教授：曾文貴　博士

中 華 民 國　九 十 三　年 六 月

使用可記憶密碼的電子投票機制
An Electronic Voting Scheme Using Memorable Password

研 究 生：張政偉　　Student：Cheng-Wei Chang

指導教授：曾文貴 博士　　Advisor：Dr. Wen-Guey Tzeng

國 立 交 通 大 學

資 訊 科 學 系

碩 士 論 文

A Thesis

Submitted to Department of Computer and Information Science

College of Electrical Engineering and Computer Science

National Chiao Tung University

in partial Fulfillment of the Requirements

for the Degree of

Master

in

Computer and Information Science

June 2004

Hsinchu, Taiwan, Republic of China

中華民國九十三年六月

使用可記憶密碼的電子投票機制

學生：張 政 偉　　指導教授： 曾 文 貴　博士

國立交通大學資訊科學系

摘 要

一般的電子投票機制，合法的投票者都持有一私密值，用此私密值來投票，才能投出能通過驗證的合法選票。由於私密值是很複雜難記的，所以大多存在特定的可攜式裝置中，例如：磁片、光碟片、或是智慧卡等，然而，將私密值儲存在可攜式裝置中，卻必須承擔遺失的風險，只要可攜式裝置遺失或是儲存在裡面的私密值被攻擊者知道，則攻擊者可代替合法的投票者投出有效的選票。

有鑑於上述問題的存在，本篇論文將電子投票機制加上可記憶密碼，由投票者記憶長度短的密碼，在投票時除了必須擁有私密值外，還需要知道可記憶密碼，才能成功的完全投票，確保攻擊者即使偷到私密值，在缺乏該投票者密碼的情況下，仍然沒辦法仿冒投票者投出合法的選票。

關鍵詞：電子投票機制、可記憶密碼、以密碼為基礎

An Electronic Voting Scheme Using Memorable Password

Student: Cheng-Wei Chang Advisor: Dr. Wen-Guey Tzeng

Institute of Computer and Information Science

National Chiao Tung University

Abstract

In general electronic voting scheme, every qualified voter owns one secret value. Every voter must use this secret value to generate ballot that can be verified successfully. Since the length of secret value is long and the content of secret value is hard to memory, we often put our own secret value in some kind of portable device, such as magnetic disc, compact disk, and smart card. However, we must afford the risk of losing the device. If the device is stolen or the secret value is revealed , attacker can forge ballot which can be verified successfully.

To solve this problem, we combine electronic voting scheme and memorable password scheme. Even though attacker gets the secret value of some voter, he can't generate legal ballot without relatively password.

Keywords : Electronic Voting Scheme, memorable password, password-based

誌謝

這篇論文的完成必須感謝許多人的協助與支持。首先必須感謝我的指導教授，曾文貴老師，由於他的耐心指導和勉勵，讓我可以順利的完成此篇論文。此外，在這兩年中，除了學習應有的專業知識外，在與老師的相處及言談中，對於待人處世方面也啟發不少，對於研究以及做事情的態度上，讓我受益匪淺，真的十分感激。同時，也必須感謝我的口試委員，孫宏民教授、蔡錫鈞教授，他們對於這篇論文提供了不少寶貴的建議。

我也要感謝我父母和家人，在我求學的每個階段，都全力給我支持，尤其是我父母，沒有他們辛勞的工作以及從小對我的教導，我不可能一路堅持理想，完成碩士的學業。

另外，要感謝實驗室的學長和同學們，感謝成康學長、季穎學姐、以及惠龍學長，對於我論文有疑惑時，跟我討論與協助，也感謝實驗室的同學們，尚宸、佩琳、尚宸、坤衫、以及兆儀，和我共同走過這段忙碌又充實的碩士生涯。

要感謝的人很多，無法一一詳述，在此僅向所有幫助過我的人，致上我最深的謝意。

目錄

第一章 引言

電子投票機制(electronic voting system)是屬於密碼學領域裡”secure multi-party computations”的應用之一，也是我們在網路上比較常會接觸到的應用實例。所有的投票者都希望他們所投出去的選票(ballot)能保持祕密，也就是說即使是其他的參與者或旁觀的第三者，都無法得知關於該投票者選票內容的任何相關資訊。

然而，不管是在投票或者是在計票的過程中，電子投票系統都可能遭受不法的參與者或旁觀第三者的惡意破壞，以阻止投票的進行或改變最後的投票結果。因此，一個完整的投票系統必需要能防止此種情況的發生，同時也必須能夠讓所有人能夠驗證計票結果是否正確、合法以及驗證每一張由投票者投出的選票是否為有效票。

在本篇論文中，研究的重點在於將可記憶密碼加到電子投票機制中，使其不僅能達到電子投票機制所要求的安全性，並能夠在投票者遺失或洩露秘密參數時能夠依然保持系統的安全性。

第一節 研究動機

由於網路發展所帶來的便利性，許多在現實生活中所發生的行為也可以藉由網路來完成，電子投票機制就是一例，傳統投票的行為可能發生在公司、學校、或是一個國家等有特定範圍的團體，而投票電子化、網路化之後，投票者不須真正的到投票區投票，直接透過網

路完成投票、計票、驗證得票結果的目的，不但使得投票的便利性大大的增加，可以增加選民投票的意願，也使得計票的過程簡化了，參與投票的人不但不需要長久的等待，才能夠得知選舉最後的結果，而對於每張選票和最後計票結果的正確性，也能夠做驗證，讓選舉的公正性可以得到證明。

然而，以往的電子投票機制相關研究中，雖然都可以很有效率的達到投票機制的安全性需求，但是由於在這些機制中，投票者都必需持有一私密值，藉由這私密值來確認身份以及選票的合法性，而這一私密值由於不容易直接記憶，因此大都存在某種特定儲存裝置裡，例如：磁片、光碟、或是智慧卡，儲存在這些裝置雖然可以解決不易記的問題，但如果這個私密值被竊取或是儲存私密值的裝置被偷走，則得到這項私密值的第三者就可以代替原投票者投出合法的選票。

要怎樣才能避免一旦私密值被竊走，則竊走的第三者可以代替原投票者投出合法選票呢？最直覺的想法就是不要將所有的雞蛋放在同一個籃子中，也就是說不要將所有的私密值放在同一個儲存裝置裡，然而，放在不同的儲存裝置仍有同時遺失的危險，當分散儲存的裝置過多時，更可能造成投票者的不便，因此，在不另外增加儲存裝置的前提上，有一個方法可以達到分散私密值風險，那就是使用可記憶密碼機制，利用這個機制來保護私密值，而可記憶密碼則由投票者記在腦中，如此一來，即使存放私密值的儲存裝置被偷走，在不知道該名投票者的可記憶密碼的情況下，還是可以確保得到私密值的第三者，無法投出合法的選票。

因此，本篇論文的研究重點在於如何將可記憶的密碼的機制加到原本的投票機制中，只有同時知道該名投票者的可記憶密碼，以及其存放在智慧卡中的私密值，才能投出合法的選票，即使私密值被竊取

仍然可以保持系統的安全性，不會有冒名投票的問題。

第二節　研究重點與成果

本篇論文的研究重點在於將可記憶的密碼機制和電子投票系統結合在一起，利用智慧卡對資料的保護，將私密值放在智慧卡中，投票者在投票時必需將存有私密值的智慧卡放入投票機器中，而且輸入正確的密碼，才可以投出合法的選票，藉由這步驟來對整個投票機制的安全性增加多一層的保護。本篇論文所提出的使用可記憶密碼的電子投票機制具備了下列幾種特性：

1. **私密性(privacy)**

電子投票機制的私密性在於當投票者將選票(ballot)投出後，任意第三者都無法從中得到任何有關於投票者的投票內容(vote)的資訊。

2. **可公開驗證性(universal verifiability)**

電子投票機制的可公開驗證性是指任何人皆可以驗證此次的投票結果是否公正，此一特性包括可公開驗證所有投票者所投出的選票是否正確、有效，以及可公開驗證最後宣佈的計票結果是否公正(意即是否所有合法的選票都被加入計算，不合法的選票都未被列入)。

3. **強固性(robustness)**

電子投票機制的強固性是指當一個合理數目的投票者或是選務中心有錯誤行為發生時，整個投票的作業程序依然能夠繼續正常運作，此外，任何投票者如果有作弊的行為都可以被偵測出來並不予採計，也就是說任何數量的投票者作弊都不影響整個投票的進行以及最後的投票結果。

4. **合格性(eligibility)**

電子投票機制的合格性是指只有合格並經過認證的投票者才能參與投票，任何無法驗證通過的投票者都無法投出一張合法的選票，所以，一個電子投票系統必需能有效防止非法的第三者投出偽造的選票，以達到選舉的公平性。

5. **無選票重複性(no vote duplication)**

電子投票機制的無選票重複性是指任合投票者皆無法複製他人的選票來當成自己的選票，此一特性是為了防止有買票者要求某些投票者投出與他相同的選票。

6. **無投票收據性(receipt-freeness)**

電子投票機制的無投票收據性是指在整個投票過程中，投票者無法利用投票過程中所接收的資訊來向第三者證明該張選票中的選票內容為何，如此則可以避免有人利用此收據來進行買票(vote buying)和強迫投票等非法行為，使得投票變的不公平。

第三節　各章節簡介

在以下的各章節中，第二章介紹目前對於電子投票機制以及可記憶密碼機制所做的一些相關研究。第三章介紹在本篇論文中所會用到的相關理論與技術。而在第四章，則會提出本篇論文中使用可記憶密碼的電子投票機制的主要架構。在第五章，則針對本篇論文的安全性做分析，並且和其他電子投票機制做比較。最後，在第六章則是本篇論文的總結，以及提出未來可以努力的方向。

第二章 相關研究

本篇論文結合了可記憶的密碼機制以及電子投票機制，所以針對這兩個領域，我們將之前做的研究，在本章中做介紹和說明。

第一節 傳統與電子投票機制

在日常生活中，我們常會接觸到的是傳統的投票機制，這類的投票機制通常在特定時間，特定地點舉行，選票則為印有供圈選的選項的一張紙，傳統的投票機制大多是因為某種特定原因(例如：選舉民意代表，表決特定事項)而舉辦，大致上傳統的電子投票機制可以分成以下三種程序：

1. **註冊(registration)**：

具備投票資格的投票者，在限定的投票時間內，帶著自己的身份證明文件、印章、以及投票通知單等，到指定的投票所，在經過選務人員身份查核後，登記並領取選票，即完成投票者註冊的程序。

2. **投票(vote casting)**：

投票者通過註冊這項程序，領取到選票之後，進入投票所的投票亭(voting booth)內圈選自己的投票內容，最後，將這張簽選後的選票投入投票箱內，即完成整個投票的程序。

3. **計票(vote counting)**：

在投票時間截止之後，投票階段的作業即宣告結束，也就是說不再接受具備投票資格的投票者提出投票的要求，開始進行最後的計票階段。在計票的過程中，通常都會有一至二個唱票員負責唸出每張選票內容，數個監票人員負責監督投票和計票過程，以及數個計票人員負責加總統計得票數，最後，當所有的投票所都完成計票程序後，把每個投票所公佈的各候選人計票結果相加，即可得到最後每一位候選人的總得票數。

如上面所述，在傳統的投票機制中，投票者在投票時要到指定的投票所，開票時必須由唱票人員一張張的唱票，而每個投開票所都必須要有數名選務人員、監票人員，負責該投開票所的投開票業務，這樣的機制不但需要很長的時間才能完成開票及最後加總計票的工作，如果規模很大時，則動用到的人力也是相當的可觀，而最大的缺點則是，傳統的投票機制由於投票者必須到指定的投票所投票，天氣情況或是其他的外在因素會大大的影響選民到指定的投票所投票的意願，如此則投票的結果可能無法充份代表舉行投票的團體裡真政的意向，這些都是傳統投票系統的缺點。

因此，基於電腦普及與網路的發達，電子投票機制讓投票和開票可以透過網路進行，解決了上一段中提到的關於傳統投票機制的幾個問題，為投票者帶來了更佳的便利性，更大大提升了整個投票程序的時效性。而電子投票機制的目的和傳統的投票機制相同，程序則與傳統的投票機制無太大的差異，同樣也分成註冊、投票與計票三個階段。通常，一個電子投票機制都存在一個公開的電子佈告欄(bulletin board)，每個具有投票資格的投票者在這個佈告欄有自己專屬的區塊，投票者將圈選後的選票，藉由電子投票機制提供的加密功能將選票加密後，再將加密後的選票公佈在電子公佈欄中自己的區塊上，並

且另外產生額外的資訊做為認證之用，將這些資訊也公佈在電子佈告欄自己的區塊中，如此即完成註冊與投票的程序；而在投票時間截止後，選務中心會對電子佈告欄中的選票做驗證，並將所有合格的選票依電子投票機制所提供的計票功能，得到各候選人的總得票數，最後則公佈所有候選人的總得票數，完成計票的程序。

我們舉出並且說明一些電子投票機制相對於傳統投票機制的優點。

1. **不需到固定的投票所投票**

利用電子投票機制，不需要到指定的投票所投票，只要是合法的投票者，都可以在任何可以上網的地方，利用電腦或是投票機器(voting machine)來進行投票的作業，而不再受空間的限制，也可以避免排隊等候投票之苦。

2. **減少作業人員**

在傳統的投票機制中，每個投票所都需要好幾位選務人員負責登記註冊程序、輔助投票者投票、以及投票所秩序的維持，在開票時，還需要另外的監票人員，監督整個開票的過程，以確保整個開票過程的公平性與正確性；而使用電子投票機制，由於沒有投票所的存在，且開票也交由電腦來做，所以也不需要這些選務人員以及監票人員，只需少數幾位負責維持選務中心系統正常運作的人員即可。

3. **防止重複投票**

每個合法的投票者，在電子佈告欄上都有一欄自己專屬的區塊，在這個區塊中，該投票者只能做新增資料，而不能對在該欄位的資料做刪除或修改，也就是說投票者一投出自己的選票後，即不能對選票內容修改或刪除；如此便可有效防止重複投票的行為。

4. **有效並快速的驗證投票者的身份**

在電子投票機制中，由於使用密碼學的上的身份驗證技術，所以可以快速且正確的驗證每位投票者的身份。而每位投票者有一份投票的秘密參數存在，可以防止不法人士偽造合法投票者的選票，破壞選舉的公平性。

5. 節省投票所需花費的時間

由於不必到特定地點投票，也不需要排隊領票、投票，電子投票機制相較於傳統投票機制，在時間上的花費改善非常的多；而由於計票是由電腦計算出來，因此，不像傳統投票機制的計票，需要唱票、驗票等步驟，整個計票時間也會大幅的縮短，能夠儘快的公佈選舉結果。

6. 提供更簡單方便的投票方法

電子投票機制，所有的投票程序皆可在任何有網路的地方完成，投票者不必為了投票特地到投票所，另外，由於電子投票機制是透過電腦或投票機器來投票，因此，投票者只需選擇其選擇的投票內容，其餘的部份可全交由電腦或投票機器來處理，讓選舉變的更簡單與方便。

第二節　電子投票機制

電子投票機制最早是由 Chaum 在 1981 年[Cha81]提出，這篇的做法是建立在混合網路(mix-net)的觀念上， Cohen 和 Fischer 在 1985 年[CF85]以及 Benaloh 在 1987 年[Ben87]則分別提出了建立在同型加密函數上的電子投票機制，而基於盲簽章的電子投票機制則是由 Chaum 在 1989 年[Cha89]以及 Fujioka、Okamoto 和 Ohta 在 1992 年

[FOO92]提出，在這之後許多基於以上三種方法的電子投票機制相繼被發表。

無收據性的觀念是投票者無法藉由投票過程所獲得的資料來向攻擊者證明投票者所投出的選票內容為何，最早是由 Benaloh 和 Tuinstra 在 1994 年[BT94]提出，這也是第一篇建立在同型加密函數上的滿足無收據性的電子投票機制，不過，這篇論文後來被證實並不滿足無收據性，在同一年另外有 Niemi 和 Renvall[NR94]提出另一篇無收據性的電子投票機制，不過這篇論文是基於一般的密碼理論，在效率上非常不理想， Sako 和 Kilian 則在 1995 年[SK95]發表了基於混合網路的多計票中心機制，Okamoto 在 1997 年[Oka97]提出了基於盲簽章的無收據性的電子投票機制，藉由多計票中心來隱藏投票者投出的選票，另外，使用同型加密函數來使得計票工作變的比較簡易，Crammer[CGS97]等人在同一年也提出了使用同型加密函數的多計票中心(multi-authority)的電子投票機制，在 2000 年由 Lee 和 Kim[LK00]兩個人提出了使用隨機器(randomizer)來達到無收據性的方法，Magos 在等人則在 2001 年[MBC01]提出藉著能抵擋入侵的硬體(tamper-resistant hardware)的電子投票機制。

電子投票機制可以大致上分為三種方法：基於同型加密函數、基於混序網路、和基於盲簽章的機制，以下就這三種方法做說明：

同型加密函數(homomorphic encryption function)：

Crammer等人在1997年[CGS97]提出的機制就是基於同型加密函數，什麼是一個同型的加密函數呢？如果一個加密函數是同型的，則存在下列假設：假設$y_1 \in E(x_1)$且$y_2 \in E(x_2)$，以⊕表示函數的加法，則 $y = y_1 \oplus y_2$ 是代表y是屬於x_1與x_2相加後的加密結果，即$y \in E(x_1 +$

x_2)。基於同型加密函數可以使得電子投票機制能敢簡單的完成計票的工作。

混序網路(mix-nets)：

混序網路是由 Sako 和 Kilian 在 1995 年[SK95]提出，一個混序網路架構就是，對於輸入的一些值(input)，混序網路會輸出一個這些值經由重新排列與函數運算後的結果，而對於最後輸出的結果，我們無法得知輸出值與輸入值之間的關係為何。

盲簽章(blind signature)：

基於盲簽章的機制有 Fujioka、Okamoto 和 Ohta[Foo92]所提出的”A partial secret voting scheme for large scale elections”，以及 Okamoto [Oka97]所提出的”Receipt-free electronic voting scheme for large scale elections”等；所謂的盲簽章就是：有兩個參與者，一個是傳送者 A，另一個是要對傳送者 A 所送來的文件做簽章動作的簽章者 B，A 希望 B 能夠對於其所送出的文件做一個簽章的動作，但又不希望 B 知道文件的內容為何，最後傳送者 A 仍然能夠獲得簽章者 B 對於此一文件的簽章。

第三節　使用可記憶密碼的機制

在現今電腦與網路日益普及的社會，可記憶密碼的使用是越來越普遍，想像如果金融卡沒有可記憶密碼這一層保護，則只要金融卡遺失，帳戶裡的錢將被盜領一空，再想像如果電腦使用的作業系統沒有可記憶密碼的保護，則電腦裡的機密資料將輕易的被竊取，然而，雖然可記憶密碼的使用在現實生活中幾乎隨處可見，但是在密碼學的觀

點裡，因可記憶密碼長度不長的特性，的所以在使用上有其特有的限制，在安全性的要求上必須符合嚴謹的規範，在下面的兩個小節，將分別就可記憶密碼的特性及安全性做介紹。

可記憶密碼在密碼學各領域中，比較被廣泛的運用的是在身份認證與金鑰交換協定(Authenticated encryption key exchange protocol)這方面的論文，最早是在 Bellovin 等人在 1992 年[BM92]提出，在此之後許多以可記憶密碼為基礎的身份認證協定便被一一提出，而本篇則是第一篇將可記憶密碼機制套用在電子投票機制上的，由於可記憶密碼為了能夠符合可記憶的特性，所以其長度大都不長，而由於長度不長，所以可記憶密碼的範圍大都很小，藉由這個特性衍生出了許多種的攻擊方法，安全的使用可記憶密碼的機制，必需能抵擋這些攻擊方法，以下就針對這些攻擊方法做介紹：

1. **竊聽攻擊法**

本攻擊法是指攻擊者藉由竊聽投票者所傳送的投票內容，並分析這些內容得到有用的資訊。

2. **重送攻擊法**

本攻擊法是指攻擊者記錄之前投票者傳送的投票內容，並再稍後將這些內容重新傳送，用來仿冒成一次合法的投票。

3. **通行碼檔案的洩露連累**

本攻擊法是指在選務中心的隱藏密碼的檔案被攻擊者獲得，使得攻擊者藉由隱藏密碼的檔案可以得到投票者的通行碼或仿冒投票者的投票內容。

4. **字典攻擊法**

本攻擊法是指攻擊者藉由可記憶密碼長度短且投票者選擇的可記憶密碼通常都是有特殊意義的文字的特性，重複測試來尋找客戶所

可能選擇的可記憶密碼，本攻擊法有兩種攻擊模式，一為即時字典攻擊法，一為離線字典攻擊法，以下就這兩種攻擊模式做說明：

（一）即時字典攻擊法(On-line dictionary attack)：攻擊者直接仿冒投票者產生投票內容將其送到選務中心，並重複的猜測投票者的可記憶密碼，想要利用猜測的可記憶密碼來仿冒合法的投票者，如果失敗再重複猜測新的密碼，直到成功為止。

（二）離線字典攻擊法(Off-line dictionary attack)：攻擊者觀察並記錄之前投票者的投票內容，並且利用這個投票內容來驗證攻擊者所猜測的密碼的正確性。

第三章 相關理論與技術

在設計一個電子投票機制時，會利用到許多密碼學上的相關技術；在本章接下來的幾個小節中，將介紹在本篇論文中，主要會用到的技術。

第一節 私密分享機制

私密分享機制(secret sharing scheme)的概念是一個私密值(secret value)的持有者希望將這個私密值分散式的傳給一些分享者保管，又不希望他們能夠單獨的從接收到的私密資訊中得知該持有者的私密值，而當需要把其中的私密值求出來時，則需要經由一些特定群組的分享者合作計算，才能將此私密值求出。通常的做法是該私密值的持有者，將該私密值分割成取多的分享值(shares)，並將這些分享值分送給所有的分享者，持有者會設定一個門檻值(threshold) t，在超過該門檻值的分享者合作計算後，才可以求得該私密值。當分享者為 n 個人，而門檻值為 t 時，則稱此種私密分享機制為(t,n) – 門檻值私密分享機制。此種機制的做法如下：

1. 私密值的持有者將此私密值輸入到一個產生分享值的演算法中，並產生欲傳送給分享者U_i的分享值S_i。
2. 私密值的持有者將這些分享值S_i藉由安全通道送給對應的U_i，每

個分享者U_i無法得知其他分享者U_j的分享值S_j為何。

3. 當要算出這個私密值時，只要超過門檻值 t 的分享者共同合作計算，即可以利用他們收到的分享值將私密值算出。

以 Shamir 的(t, n) – 門檻值私密分享機制為例：

1. 私密值的持有者從Z_p^*中選擇一值當做私密值，p為安全質數。
2. 私密值的持有者隨機選擇t-1 個$a_i \in Z_p^*$，$1 \le i \le t-1$。
3. 私密值的持有者隨機選擇n個$u_i \in Z_p^*$，$1 \le i \le n$，且每一個u_i對應一個U_i(u_i可以公開)。
4. 私密值的持有者建立一多項式$F(X)=S+a_1x+a_2x^2+\ldots+a_{t-1}x^{t-1}$，計算$S_i=F(u_i)$ ，$1 \le i \le n$。
5. 私密持有者藉由安全通道將S_i送給U_i。

在此 n 個分享值 Si 中的 t 個分享值可以經由”拉格蘭矩內插法”(Lagrange interpolation Polynomial)計算出 F(X)：

$$F(x)=\sum_{i=1}^{t}\frac{S_i(x-x_1)\ldots(x-x_{i-1})(x-x_{i+1})\ldots(x-x_t)}{(x_i-x_1)\ldots(x_i-x_{i-1})(x_i-x_{i+1})\ldots(x_i-x_t)} \pmod p$$

而私密值為 S=F(0)：

$$S=F(0)=\sum_{i=1}^{t}\frac{S_i(x_1)\ldots(x_{i-1})(x_{i+1})\ldots(x_t)(-1)^t}{(x_i-x_1)\ldots(x_i-x_{i-1})(x_i-x_{i+1})\ldots(x_i-x_t)} \pmod p$$

由 Shamir 的(t, n) - 門檻值私密分享機制，我們接下來介紹在本篇論文中採用的 ElGamal 加密機制如何引入 Shamir 的(t, n) - 門檻值私密分享機制，這部份的機制是由 Pedersen 提出，其分享的是 ElGamal 加密機制中的私密金鑰，必須更動的部份有兩個，分別是金鑰產生和解密。

金鑰產生(Key generation)：

在這個階段時，使用Pedersen提出的金鑰分享方法，將私密金鑰(secret key) s分成n個等份，並將這n個等份的私密金鑰分享值交給n個私密分享中心，每個私密分享中心A_j用收到的私密金鑰分享值s_j算出$h_j = g^{s_j} \pmod p$，並公佈h_j，而私密金鑰 s則可以由t個以上私密金鑰分享值藉由拉格蘭矩內插法來算出，而其內容如表一：

假設 t 個私密金鑰分享值形成的集合為 Λ $s = \sum_{j\in\Lambda} s_j \lambda_{j,\Lambda} \pmod q, \quad \lambda_{j,\Lambda} = \prod_{l\in\Lambda\setminus\{j\}} \frac{l}{l-j}$

（表一）由私密金鑰分享值算私密值

如表一所示，這其實就是上一段所介紹的Shamir的(t, n) - 門檻值私密分享機制。公開金鑰$h = g^s$被公佈給所有參與者知道，而且私密金鑰 s無法被單獨算出。

解密(Decryption)：

假設要解密的ElGamal格式的密文是$(x, y) = (g^{\alpha}, h^{\alpha}m) \pmod p$，則解密時不需要先還原私密金鑰 s，我們可以依下列的步驟來做解密：

(1) 每個私密分享中心A_j 依自己所持有的私密金鑰分享值 s_j，算出 $w_j = x^{s_j} \pmod p$ 並且將w_j 公佈，然後用下一節會介紹到的互動式零知識證明系統來證明 $\log_g h_j = \log_x w_j \pmod q$，證明的過程請看表二。

(2) 令Λ為任意 t 個通過上一個步驟證明的私密金鑰分享中心，藉由表一的內容可以把明文還原：$m = y \Big/ \prod_{j\in\Lambda} w_j^{\lambda_{j,\Lambda}}$

Prover		Verifier
$[(x, y) = (g^{\alpha}, h^{\alpha})]$		
$w \in_R \mathbf{Z}_q$		
$(a, b) \leftarrow (g^w, h^w)$	$\xrightarrow{a.b}$	
	$\xleftarrow{c}$	$c \in_R \mathbf{Z}_q$
$r \leftarrow w + \alpha c$	$\xrightarrow{r}$	$g^r \stackrel{?}{=} ax^c$
		$h^r \stackrel{?}{=} by^c$

（表二）證明 $\log_g x = \log_h y \pmod q$

第二節　互動式零知識證明系統

互動式證明系統的觀念是當一個擁有私密資訊的證明者(Prover)想要讓另一個驗證者(verifier)相信證明者確實擁有此私密資訊時，所使用的證明方式。而如果這個系統有零知識的特性，也就是說在這個系統的驗證過程中，驗證者除了可以驗證證明者所擁有私密資訊的正確性之外，無法得到任何和證明者有關且無法由驗證者自行算出的額外資訊。

一個互動式證明系統分成藏密(commit)、挑戰(challenge)、和回應(response)三個階段，而其內容如下所述：

藏密：證明者任一選擇一個值，將這個值隱藏在其他的值中，得到一藏密值，並將此藏密值傳送給驗證者，這個值將會在後面介紹的回應部份，負責隱藏私密資訊。

挑戰：驗證者在收到藏密後的值之後，任意選一個挑戰值送給證明者。

回應：證明者在收到驗證者的挑戰值之後，依自己知道的私密資訊、之前送給驗證者的藏密值、以及驗證者送回的挑戰值，來產生回應值，由於只有證明者的確知道私密資訊，才可以產生能通過驗證的回應值，所以在驗證者接收回應值後，可以對於證明者是否擁有私密資料，做正確的驗證。

而零知識的互動系統則是在這三個階段的資訊傳遞之下，能夠擁有完全性、完美性、以及零知識性，接下來我們來說明這三項性質：

完全性(completeness)：如果證明者知道私密資訊，那麼他永遠可以說服驗證者相信他的確知道私密資訊。

完美性(soundness)：如果證明者有一個不可乎略的機率說服驗證者相信他知道私密資訊，那麼我們就有很大的機會與證明者合力算出私密資訊。也就是說存在一個提取者(extractor)，把證明者當做他的一個子程式(subroutine)，而提取者可以利用這個子程式求得證明者的私密資訊。

零知識性(zero-knowledge)：要證明一個互動式具有零知識，採用的是模擬器(simulator)的方法，首先觀察證明者P在互動證明程序中的輸出，產生有關證明者view的公佈：$View_p(C, E, R)$，其中C是證明者所傳送的訊息，E為互動證明程序中由驗證者V所選擇的隨機值， R則是證明者利用(C, E)所產生的回應值。接著嘗試建構一個模擬器 M*來模擬證明者P的行為，並產生模擬器：M*(C*, E*, R*)，其中C*、E*、R*皆由M*自行產生。如果可以成功的利用M*來取代證明者P來和驗證者V進行互動證明程序，則表示 $View_p(C, E, R)$ 和M*(C*, E*, R*)擁有相同的機率分佈，也就是說藉由觀察證明者的輸出所能得到的資訊，也能直接藉由模擬器M*模擬得到，不一樣的是模擬器M*是

在不知道證明者私密資訊的情形下建構出來的。換句話說，如果使 $View_p(C, E, R)$和$M^*(C^*, E^*, R^*)$擁有相同的機率分佈，我們就無法從 $View_p(C, E, R)$得到任何有關證明者P的私密資訊，而這就表示本系統具有零知識性。

第三節　ElGamal 加密機制

ElGamal 加密機制是由 ElGamal 在 1985 年所提出的一種基於離散對數的公開金鑰密碼系統，其精神在於解離散對數是很難的，這個機制分為金鑰產生(key generation)、加密(encryption)以及解密(decryption)三個部份，以下分別就這三個部份做詳細的說明：

1. 金鑰產生

（1）系統參數：系統隨機選擇一個n位元的質數p，並且從Z_p^*中選出一個生成元(generator) g

（2）個人密鑰：使用者A從Z_{p-1}中選出一個x_A，則個人密鑰為(p, g, x_A)

（3）公開金鑰：計算 $y_A = g^{x_A} \bmod p$，則公開金鑰為(p, g, y_A)

2. 加密

若A欲傳送明文$m(1 \le m \le p-1)$給B，則A先找出B的公開金鑰y_B，並且從Z_p中任選一個整數k，然後執行加密得密文$C=(C_1, C_2)$。

加密：$C_1 = g^k \bmod p$,　$C_2 = y_B^k \, m \bmod p$

3. 解密

A將密文C傳送給B，等B收到密文之後，利用其個人密鑰x_B，執行解密的動作。

解密：$\frac{C_2}{C_1^{x_B}} = \frac{y_B^k m}{\left(g^k\right)^{x_B}} = \frac{\left(g^{x_B}\right)^k m}{\left(g^k\right)^{x_B}} = m \pmod p$

4. 安全性分析

ElGamal 加密機制的安全性是建立在基於解離散對數之困難上。如果能由y_A及g求出A之密鑰x_A，則能解離散對數，而由於解離散對數是很難的問題，所以ElGamal加密機制是安全的。

第四節　有效率的證明有效性

在本篇論文中，每個投票者都會投出一張 ElGamal 加密格式的選票，而選票的內容只有兩種可能（贊成： +1 或反對： -1 ）的其中一種可能而無其他的可能性存在，為了確認選票的內容的確是合法的，也就是說只有+1 和-1 兩種可能，必須對投票者所送出的選票資訊加以驗證，以確定其有遵照正確的投票方法來進行投票程序；在本篇論文中，我們針對這個證明所採用的方法是“不可辨別證據的證明(witness indistinguishable proof，簡稱 W.I. Proof)”技術來證明該投票者所投出選票的有效性。

由於本篇論文採用的選票格式是ElGamal加密格式，當投票內容是贊成： +1，則選票的可能格式是$(x, y) = (g^{\alpha}, h^{\alpha}G^{+1})$ ，當投票內容是反對： -1，則選票的可能格式是$(x, y) = (g^{\alpha}, h^{\alpha}G^{-1})$ ，所以，W.I. Proof是明這張選票滿足$\log_g x = \log_h (y/G)$ 或是$\log_g x = \log_h (y/G^{-1})$。在表三中，將分別就投票內容是 +1 或是 -1 來介紹投票者產生驗證資料的步驟，以及描述驗證者(verifier)取得驗證資料後執行驗證的步

驟，由於驗證者不管投票者投票的內容為何，對於驗證資料的驗證步驟都相同，如此可以保證驗證者在驗證時，無法從驗證步驟得知該張選票中投票者的投票內容。

Voter			Verifier
v = +1	v = -1		
$\alpha, \omega, r_1, d_1 \in_R Z_q$	$\alpha, \omega, r_2, d_2 \in_R Z_q$		
$x \leftarrow g^{\alpha}$	$x \leftarrow g^{\alpha}$		
$y \leftarrow h^{\alpha} G$	$y \leftarrow h^{\alpha} / G$		
$a_1 \leftarrow g^{r_1} x^{d_1}$	$a_1 \leftarrow g^{\omega}$		
$b_1 \leftarrow h^{r_1} (yG)^{d_1}$	$b_1 \leftarrow h^{\omega}$		
$a_2 \leftarrow g^{\omega}$	$a_2 \leftarrow g^{r_2} x^{d_2}$		
$b_2 \leftarrow h^{\omega}$	$b_2 \leftarrow h^{r_2} (yG)^{d_2}$		
		$x, y, a_1, b_1, a_2, b_2 \longrightarrow$	
		$\longleftarrow c$	$c \in_R Z_q$
$d_2 \leftarrow c - d_1$	$d_1 \leftarrow c - d_2$		
$r_2 \leftarrow \omega - \alpha d_2$	$r_1 \leftarrow \omega - \alpha d_1$		
		$d_1, d_2, r_1, r_2 \longrightarrow$	
			$c \stackrel{?}{=} d_1 + d_2$
			$a_1 \stackrel{?}{=} g^{r_1} x^{d_1}$
			$b_1 \stackrel{?}{=} h^{r_1} (yG)^{d_1}$
			$a_2 \stackrel{?}{=} g^{r_2} x^{d_2}$
			$b_2 \stackrel{?}{=} h^{r_2} (y/G)^{d_2}$

(表三)有效率的驗證有效性

第四章 使用可記憶密碼的電子投票機制

本章將介紹本篇論文提出的改良後的電子投票機制，這個投票機制結合可記憶的密碼和無收據電子投票兩種功能。首先，對於本電子投票機制的架構做分析，接下來，對於本投票機制中所會用到的模組與定義做一個說明，接著會介紹本投票機制的每一個執行步驟。

第一節 架構分析

本篇論文是利用可記憶密碼簡短易記的特性，由投票者自行選擇密碼，並且記憶在腦海中，另外將長而不易記的私密值存放在智慧卡中，在投票時必須同時知道該投票者的可記憶密碼以及擁有該投票者存放私密值的智慧卡才能投出合法的選票。

本篇論文的架構可以分成投票者和選務中心這兩大部份，而選務中心底下則有投票電子佈告欄以及門檻式解密中心，投票的程序如圖一所示，以下分別就這幾個部份做說明：

投票者：

投票者在註冊階段選擇一個可記憶的密碼，並且將私密值存放在智慧卡中，另外將藏有可記憶密碼及私密值的驗證碼公佈在電子佈告欄中自己的區塊裡，在投票時，投票者將智慧卡插入投票機器，輸入自己記憶的密碼以及投票內容，由投票機器產生一個亂數，藉由這些

資料產生一張合法的選票，並且為了能夠有效率的驗證有效性，另外產生一組驗證資料，將產生的選票以及驗證資料公佈在電子佈告欄中自己的區塊裡。

選務中心：

選務中心在投票開始舉行前決定系統的參數，並且維持一個電子佈告欄，這個佈告欄的每個區塊只能提供一次的輸入，並不能做更改，另外，啟動私密分享機制，將私密金鑰分成 n 個等份，分別交給各門檻式解密中心。

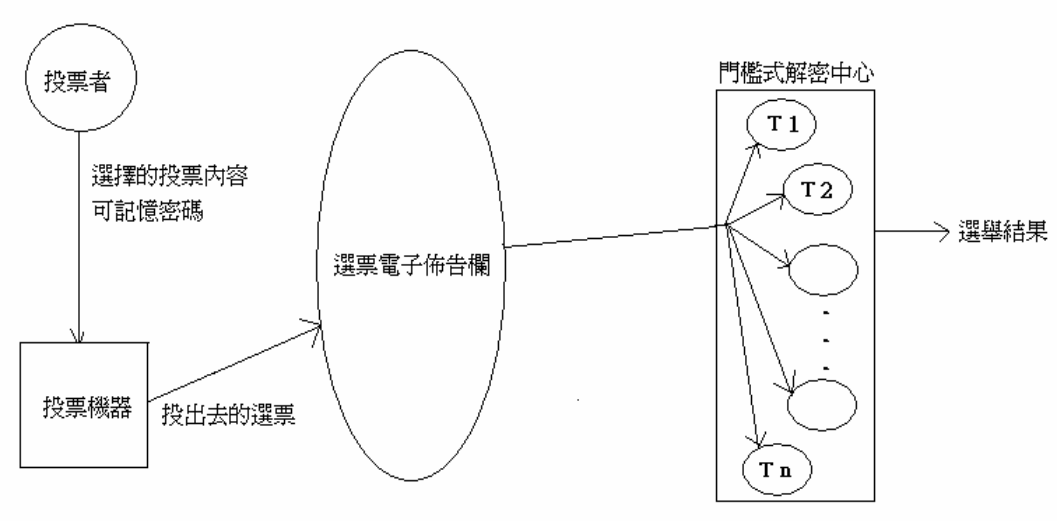
門檻式解密中心：

門檻式解密中心從電子佈告欄上得到各投票者投出的選票以及驗證資料，將各選票做驗證，判斷其是否正確後，將所有正確的選票連乘起來，得到尚未解密的計票結果，再依自己持有的私密金鑰分享值將尚未解密的計票結果做部份的解密，並且用非互動式零知識證明系統產生門檻式計票中心的驗證資料，讓所有人可以藉由驗證資料相信門檻式解密中心的確是正確的將尚未解密的計票結果做部份解密，最後，將可以通過驗證的門檻式解密中心所公佈的部份解密的計票結果，依拉格蘭矩內插法算出最後的計票結果。

投票電子佈告欄：

投票電子佈告欄是一個公開的頻道，每一位投票者在該電子佈告欄上都有屬於自己的區塊，當投票者要將選票或是其他投票資料放到投票電子佈告欄時，只可以放到屬於自己的區塊中，投票電子佈告欄擁有只能寫入資料一次，寫入的資料不可以修改，但是可以多次讀取，在本論文中，註冊時各投票者將選票驗證值放到投票電子佈告欄中，在投票時，投票者將選票以及選票驗證資料放到投票電子佈告欄中，在投票結束後，各門檻式解密中心到投票電子佈告欄有資料的區

塊讀取資料。



（圖一）

第二節　參數定義

1. n個門檻式解密中心：$T_0, T_1, \ldots T_n$，各自保管一部份的私密值，合作算出最後的投票結果。
2. 門檻值參數 t：在此電子投票機制中，必須有超過 t 個以上誠實的門檻式解密中心，才可以正確的計算出最後投票結果。另外，如果超過 t+1 個門檻式解密中心不誠實，則整個投票系統將不安全。
3. 兩個大質數 p,q：p=2q+1。
4. G_q：一個order為q的群
5. s：私密金鑰
6. g, h：兩個G_q的生成元，且$h = g^s \pmod p$。
7. $s_1, s_2, \ldots, s_n$：藉由私密分享機制產生的 n 份私密分享值
8. $w_1, w_2, \ldots, w_n$：各門檻式解密中心公佈的驗證值

第三節　提出的機制

我們在本節介紹本篇論文提出的使用可記憶密碼的電子投票機制的詳細內容，包括：註冊、投票、驗證和計票。

1. 註冊

註冊這個階段分成兩個方面，一個是系統對於投票環境的設定，另一面則是投票者選擇自己的可記憶密碼，並配合智慧卡存放的私密值產生驗證值。

(1) 選務中心選擇g_1,h_1,G為G_q的生成元，任意選擇一個值s當做私密金鑰，計算$g_2=g_1^s$、$h_2=h_1^s \pmod p$。

(2) 選務中心藉由 3.1 節介紹的私密分享機制將 s 分成 n 等份，並送給 n 個門檻式解密中心。

(3) 門檻式解密中心T_i得到屬於自己的s_i後，計算出並公佈該門檻式解密中心的驗證值 $h_i = g^{s_i} \pmod p$。

(4) 投票者選擇可記憶密碼π，任意選擇一個值α當做私密值，並將α存入智慧卡中。

(5) 投票者計算$g_1^{\alpha}h_1^{\pi} \pmod p$，將這個值送到選票電子佈告欄自己的區塊上當做選票驗證值。

2. 投票

在投票階段，投票者將所持的智慧卡插入投票機器中，並輸入自己的密碼以及投票內容，產生選票以及驗證選票正確性的選票驗證資料，並將這些驗證資料送到電子佈告欄上。

(1) 投票者將存有α的智慧卡插入投票機器中。

(2) 投票者將自己的選擇 v∈(+1, -1)，以及可記憶的密碼π輸入投票機器。

(3) 投票機器隨機選擇一個值β。

(4) 投票機器依投票者的輸入產生一張選票。

ballot (x, y)=($g_1^{\beta} \bmod p$, $g_2^{\alpha+\beta} h_2^{\pi} G^{v} \bmod p$)

(5) 投票機器任意選擇$r_1, r_2, r_3, r_4, r_5, d_1 \pmod q$

(6) 投票機器計算出藏密值(以 v=+1 為例)：

$a_1 = g_1^{r_1} \bmod p$

$a_2 = g_1^{r_2} h_1^{r_3} \bmod p$

$a_3 = g_2^{r_2} h_2^{r_3} \bmod p$

$a_4 = g_1^{r_4} h_1^{r_5} (x * g_1^{\alpha} h_1^{\pi})^{d_1} \bmod p$

$a_5 = g_2^{r_4} h_2^{r_5} (y * G)^{d_1} \bmod p$

(7) 投票機器模擬出挑戰值(以 v=+1 為例)：

$c = \boldsymbol{H}(x||y||g_1^{\alpha} h_1^{\pi}||a_1||a_2||a_3||a_4||a_5) \bmod q$

$d_2 = c - d_1 \bmod q$

(8) 投票機器計算出回覆值(以 v=+1 為例)：

$s_1 = r_1 - d_2 \beta \bmod q$

$s_2 = r_2 - d_2(\alpha+\beta) \bmod q$

$s_3 = r_3 - d_2 * \pi \bmod q$

$s_4 = r_4$

$s_5 = r_5$

(9) 投票機器將選票以及(6)、(7)、(8)得到的身份驗證資料送到投票電子佈告欄。

選票：(x, y)

身份驗證資料：$(a_1, a_2, a_3, a_4, a_5)$、$(d_1, d_2)$、$(s_1, s_2, s_3, s_4, s_5)$

3. 驗證

在註冊時，每個投票者都會送藏有自己密碼及私密值的身份驗證值到投票電子佈告欄上自己的區塊中，而在投票階段除了選票以外，還送出了身份驗證資訊，藉由身份驗證值及選票驗證資訊，任何人都可以用來驗證選票的合法性，也可以驗證投票者是否真的選擇指定的投票內容，也就是說，也可以驗證選票內容是否正確，驗證的方法請看表四：

(1) $c' = \boldsymbol{H}(x||y||g_1^{\alpha}h_1^{\pi}||a_1||a_2||a_3||a_4||a_5) \pmod q$

(2) 檢查是否$d_1+d_2=c' \pmod q$

(3) 檢查以下式子

$a_1 \stackrel{?}{=} g_1^{s_1}(g_1^{\beta})^{d_2} \bmod p$

$a_2 \stackrel{?}{=} g_1^{s_2}h_1^{s_3}(x*g_1^{\alpha}h_1^{\pi})^{d_2} \bmod p$

$a_3 \stackrel{?}{=} g_2^{s_2}h_2^{s_3}(y/G)^{d_2} \bmod p$

$a_4 \stackrel{?}{=} g_1^{s_4}h_1^{s_5}(x*g_1^{\alpha}h_1^{\pi})^{d_1} \bmod p$

$a_5 \stackrel{?}{=} g_2^{s_4}h_2^{s_5}(y*G)^{d_1} \bmod p$

(表四)選票驗證步驟

4. 計票

計票這個階段分成兩個部份，第一個部份是門檻式解密中心對每張選票做驗證，將合法的選票集合起來，得到尚未解密的計票結果，第二個部份是由門檻式解密中心合作解出最後的計票結果，每個門檻式解密中心必需證明自己有依自己持有的私密分享值做解密。

(1) 各門檻式解密中心利用驗證機制檢查每張在投票電子佈告欄上的選票，對於每張合法的選票做以下的處理：

投票者i：原選票(x_i, y_i)、驗證值$g_1^{\alpha_1}h_1^{\pi_1} \pmod p$、處理後的選票$(x_i', y_i')$

$x_i' = x_i * g_1^{\alpha_1} h_1^{\pi_1} \pmod p$、$y_i' = y_i$

（2） 各門檻式解密中心各自將所有選票處理後的值連乘起來，得到尚未解密的計票結果(X, Y)：

假設共有m個投票者通過驗證程序，則處理後的選票為

$(x_1', y_1'), (x_2', y_2'), \ldots, (x_m', y_m')$

而連乘起來的值則為

$$X = \prod_{i=1}^{m} x_i', \quad Y = \prod_{i=1}^{m} y_i'$$

（3） 各門檻式解密中心將驗證並處理後的尚未解密的計票結果，依其所持有的私密分享值，做以下的部份解密步驟：

a. 門檻式解密中心A_j依所持有的s_j算出 $w_j = X^{s_j} \pmod p$，並將w_j公佈，

b. 利用非互動式零知識證明系統產生驗證資料：

1. $(H_j, w_j) = (g^{s_j}, X^{s_j}) \pmod p$

2. 門檻式解密中心任選一個值 γ，並算出藏密值$(a, b)=(g^{\gamma}, X^{\gamma}) \pmod p$

3. 門檻式解密中心用郝序函數H模擬出挑戰$c = H(a||b||h_j||w_j)$

4. 門檻式解密中心計算回應值，$\beta = \gamma + s_j * c \pmod q$

c. 檢查以下兩等式以驗證門檻式解密中心是否確實依其所持有的私密分享值，做部份解密：

$g^{\beta} \stackrel{?}{=} a * h_j^{c}$ ， $h^{\beta} \stackrel{?}{=} b * w_j^{c} \pmod p$

（4） 將能通過步驟(3)驗證的門檻式解密中心A_j，所得到的(w_j, Y)集合起來，如果超過t個以上能夠通過，則利用 3.1 節Decryption的第

2 步驟，解出這次投票的結果。

5. 零知識證明

在產生選票驗證資料的部份，我們採用的是"有效率的證明有效性"的方法來證明，並將這個方法改成非互動性，我們要證明我們採用的證明步驟是符合零知識特性的，也就是說驗證資料滿足了完全性、完美性、和零知識性，也就是說此有效率證明有效性的方法是符合零知識性的。

完全性(completeness)：

由驗證步驟得知，只要投票者確實擁有可記憶密碼π和私密值α，則產生的驗證資料一定可以驗證通過，所以符合完全性的要求。

完美性(soundness)：

要證明有完美性，則必需證明有一個提取者存在，且這個提取者可以將私密值提取出來，以下是基於本篇論文架構所造出的存取者E：

Input: P', V, (x, y)

1. 執行 $P'(x, y) = a_1, a_2, a_3, a_4, a_5, d_1$
2. 設回復點
3. 執行 $V(x||y||g^{\alpha}h^{pwd}||a_1||a_2||a_3||a_4||a_5) = c$
4. 執行 $P'(x, y, a_1, a_2, a_3, a_4, a_5, d_1, c) = s_1, s_2, s_3, s_4, s_5, d_2$ $(d_1+d_2=c)$
5. 回到步驟 2 並且重新執行上述步驟

   (a)執行 $V(x||y||g^{\alpha}h^{pwd}||a_1||a_2||a_3||a_4||a_5) = c'$ (V使用新的隨機值)

   (b)執行 $P'(x, y, a_1, a_2, a_3, a_4, a_5, d_1, c') = s_1', s_2', s_3', s_4', s_5', d_2'$

   $(d_1+d_2'=c')$
6. $\beta = s_1-s_1'/d_2'-d_2$, $\alpha+\beta = s_2-s_2'/d_2'-d_2$, $pwd = s_3-s_3'/d_2'-d_2$

零知識性(zero-knowledge)：

如果可以造出一個模擬器(simulator) M*，在不知道私密資訊的前提下，M* 可以成功的取代證明者和驗證者做驗證的話，則滿足零知識性，以下是本篇論文架構下的模擬器：

1. 隨機選擇兩個位元值 d_1", d_2" 以及五個隨機值 r1', r2', r3', r4', r5'
2. 令 c"=d_1"+d_2"
3. 計算出以下的值 $a_1' = g_1^{r_1'}$， $a_2' = g_1^{r_2'} h_1^{r_3'}$， $a_3' = g_2^{r_2'} h_2^{r_3'}$，$a_4' = g_1^{r_4'} h_1^{r_5'} (x * g_1^{\alpha} h_1^{\pi})^{d_1''}$， $a_5' = g_2^{r_4'} h_2^{r_5'} (y * G)^{d_1} \pmod p$
4. 計算H(x||y||$g^{\alpha}h^{\pi}$||a_1'||a_2'||a_3'||a_4'||a_5')=c'
5. 如果 c'=c"，則表示模擬成功， M*將模擬結果輸出：

   (x, y), a_1', a_2', a_3', a_4', a_5', d_1", d_2", r_1', r_2', r_3', r_4', r_5'

   其他的狀況則表示失敗，輸出 ⊥

第五章 安全性分析與比較

一個電子投票機制有許多安全性的要求,而在加入可記憶的密碼機制後，對於可記憶密碼機制可能遭受的攻擊，也必須能夠抵擋，在以下的小節將討論本篇論文採用的機制，是否滿足這兩方面的安全性需求；另外，我們將本篇論文的架構和其他的電子投票機制的論文做安全性的比較。

第一節 在電子投票機制方面的安全性分析

我們對於電子投票機制中的所要求的安全性和攻擊做說明，並且分析本篇的機制如何能符合這些安全性，以及能否抵擋攻擊。

1. **正確性(correctness)**

在電子投票機制中，正確性是針對最後計票的結果，也就是說每個人都能被說服計票的結果是正確的，沒有偽造或是漏計任何選票。

而在本篇採用的機制中，每一個人可以依以下步驟來相信計票的結果是正確的。

1. 使用在第四章提過的驗證步驟，驗證每張在電子佈告欄上選票的合法性。
2. 將所有通過驗證的選票做連乘，得到(X”, Y”)。
3. 將所得到的 X”帶進第四章計票階段的第 c 步做檢驗，並將 Y”和

各門檻式解密中心公佈的 Y 做比對，看是否相等。

4. 若超過 t 個以上可以驗證通過，則表示誠實的門檻式解密中心有 t 個以上，如此則可以相信計票結果是正確的。

2. **完整性(completeness)**

在電子投票機制中，完整性的意義可以看做是一般投票時所強調的平等，也就是說是所有投票者投出的選票中，只要是合法的選票，在計票時都必須被列入計票結果中。

在本篇論文的架構中，請參考本章有關正確性的證明，假設有門檻式解密中心計票時漏計了部份的合法票，則驗證者得到的(X", Y") 在代入正確性的驗證步驟做驗證時，會產生所有門檻式解密中心都無法通過驗證的情形，使得計票結果不被信服，所以，只有在所有合法選票都被列入時，才能正確的公佈計票結果，因此符合完整性。

3. **強固性(robustness)**

在電子投票機制中，強固性的定義為整個投票機制並不會因為部份的錯誤或是破壞而使得整個電子投票機制不安全，在本篇論文所採用的架構中，最關鍵的私密值藉由私密分享機制分散由 n 個門檻式解密中心保管，所以只要不超過 t 個以上的門檻式解密中心被攻破，都可以確保本機制的安全。

在投票者方面，由於本篇的架構採用的是前面章節有說明的有效率的證明有效性的技術，所以，投票者無法在選票上做任何變動，來達到破壞本次投票的進行，由此可知，本篇論文的架構是符合強固性的要求的。

4. **所有人都可以驗證(universal verifiability)**

在電子投票機制中，所有人都可以驗證這項性質的定義為任何人都可以針為選票以及計票結果的合法性做檢查與確認。在本篇論文的

架構中，由第四章的選票驗證過程可以檢查每張選票的合法性，由計票的步驟以及本章正確性推導可以檢查最後計票結果的合法性，所以，本篇論文的架構是可以讓所有人都對每張選票以及最後計票結果的合法性做確認的。

5. 無收據性(receipt-freeness)

在電子投票機制中，無收據性的定義為所有的投票者都無法藉由投票過程所得到的資訊，來向其他人證明其投票內容，在本篇論文的架構中，由於投票的步驟是經由投票機器隨意產生一個值來配合智慧卡存的值以及投票者輸入的可記憶密碼和選擇的投票內容來產生合法選票，因此，投票者並沒有從投票的行為中得到任何資訊，而由於選票的產生有用到投票機器隨意產生的值，而這個值如果投票者想知道，則相當於解離散對數的問題，而在數論上，解離散對數的問題是很難的，由以上的分析知道，在本篇論文的架構底下，投票者無法向其他人證明其投票內容，所以，符合無收據性的要求。

6. 合格性(eligibility)

在電子投票機制中，合格性的定義為只有合法的投票者能投出合法的選票，也就是說，一個滿足合格性的電子投票機制，必須能掌握投票者的身份，並能夠在計票時判斷出是否是合法投票者所投出來的，在本篇論文的架構中，投票者在投票前必須先向選務中心登記屬於自己的驗證值，在這個階段，選務中心就已經確認了合格投票者的身份，就有如現實的投票程序中，必須查驗身份證一樣，因此，除非選務中心造假，否則，不合格的投票者無法產生合法的驗證值，並且藉由選務中心將驗證值放到投票電子佈告欄上，如此，則不合格的投票者即使送出自己的選票，也會因為無法通過檢查而成為無效票，因此，本篇論文的架構滿足合格性的要求。

7. 一人一票(unreusability)

在電子投票機制中，一人一票的定義為一個合法的投票者只能投出一張選票，而在本篇論文的架構中，每個經過註冊程序的合法投票者都會在投票電子佈告欄上有一欄屬於自己的欄位，在這個欄位會預先放著之前註冊時傳給選務中心的驗證值，而該投票者在完成投票程序後，也只能上傳到屬於他的欄位，因此，一個投票者只能在投票電子佈告欄上放一份自己的選票，藉此達到一人一票的要求，由以上所述可知，本篇論文的架構滿足一人一票的要求。

8. 隱私性(privacy)

在電子投票機制中，隱私性的定義為每張選票的圈選內容都是保密的、不會被其他人知道的。在本篇論文的架構中，要得到圈選內容的方法就只有分析選票，也就是說分析投票者v_i投出來的(x_i, y_i)，而圈選內容是藏在y_i中的，在不知道私密值的情況下，要解出藏在y_i中的圈選內容相當於解離散對數的問題，所以，本篇論文的架構滿足隱私性的要求。

9. 不可複製性(non-duplication)

在電子投票機制中，不可複製性的定義為惡意的投票者不可以拿其他投票者的選票當做是自己的選票投出去，或是要求其他投票者把惡意投票者的選票當做是自己的投出去，這個性質的意義在於避免惡意投票者控制其他投票者的圈選內容，或是讓惡意投票者窺得其他投票者的投票內容。在本篇論文的架構中，每個合法投票者在註冊時都有交給選務中心自己的驗證碼，這個驗證碼隱藏了投票者的可記憶密碼以及存放在智慧卡上的值，而在驗證時，只有投票者輸入自己的密碼，使用自己的智慧卡，才可以投出可以配合記錄在投票電子佈告欄上的驗證值成功通過驗證的選票，因此，在本篇論文的架構下，藉由

複製其他投票者的選票當做自己選票的方法，是無法通過驗證的，因此，本篇論文的架構滿足不可複製性的要求。

第二節　本機制抵擋攻擊分析

在電子投票機制中，攻擊的類別分成兩大部份，一個部份是投票者或是選務中心被攻陷(corrupted)，另一個部份是在整個投票機制的哪個時期被攻陷，不同時期以及不同角色被攻陷有不同效果，以下分別就這兩部份做介紹與討論，並且說明本篇論文的架構能否抵擋這些攻擊。

1. 投票者被攻陷

(a) 註冊前被攻陷

由於投票者在註冊前被攻陷，因此，入侵者(corrupter)可以指定投票者在註冊時使用由入侵者選定的α'以及π'，並將$g^{\alpha'}h^{\pi'}$交給選務中心當做驗證值，並且在投票時要求投票者投出由入侵者選擇的圈選內容，因此，只要投票者在註冊前被入侵，則本篇論文的架構就會不安全，也就是說，本篇論文的架構中，投票者無法抵抗在註冊前被攻擊。

(b) 註冊後投票前被攻陷

投票者在註冊後投票前被攻陷，則入侵者可以指定被入侵的投票者投出其圈選的內容，而投票者只能依入侵者的指示輸入正確的可記憶密碼以及插入正確的智慧卡完成投票，否則在選票投出後，入侵者在驗證時會發現無法驗證成功，因此，

在這時期被攻陷，本篇論文的架構是不安全的。

(c) 完成投票後被攻陷

在這個時期投票者被攻陷，則入侵者可以做的就只有要求投票者證明其圈選內容，然而，本篇論文的架構是滿足無收據性的，也就是說，投票者在投票過後，由於選票的內容是在投票機器隨機產生一個值之後配合投票者輸入的內容產生的，所以，投票者在無法知道投票機器產生的值的情況下，並沒有任何方法來向入侵者證明其圈選內容，所以在這個時期被攻陷時，本篇論文的架構是安全的。

2. 選務中心被攻陷

(a) 註冊前被攻陷

選務中心在註冊開始前被攻陷，則入侵者可以自行選擇生成元 g', h'，以及私密值 s'，並且可以執行私密分享機制，將私密分享值分送給所有的門檻式解密中心，整個投票機制都被入侵者掌控住了，所以，在註冊前被攻陷，則本篇論文的架構是不安全的。

(b) 註冊後所有投票完成前被攻陷

由於本篇論文的投票者在產生選票及合法性的證明資料時是採用非交互式的零知識證明機制，不需要和選務中心做溝通，所以，在這時期選務中心被入侵者攻陷，只要超過 t 個門檻式解密中心不被攻陷，則本篇論文的架構仍然是安全的，可以抵擋這樣的攻擊方法。

(c) 所有投票完成後開票前被攻陷

在這個時期，入侵者能做的就是攻陷門檻式解密中心，只要不超過 t 個私門檻式解密中心被攻陷，則入侵者無法製造出

假造的計票結果和證明，因此，在本時期中，本篇論文的架構的安全性，是建立在有多少門檻式解密中心被攻陷。

3. **投票者和選務中心都被攻陷**

(a) 註冊前被攻陷

由前面的說明得知，當投票者和選務中心都被攻陷時，則整個投票機制都不安全，本篇論文的架構無法抵擋這樣的攻擊方法。

(b) 註冊後投票完成前被攻陷

當投票者在投票完成前被攻陷，則入侵者可以要求該名投票者依入侵者的意志投票，或者是代替投票者投票，因此，在註冊後投票完成前，投票者和選務中心都被攻陷，本篇論文的架構無法抵擋攻擊。

(c) 投票完成後開票前被攻陷

投票完成後，即使投票者被攻陷，亦無法改變該名投票者投出的選票，而如果選務中心被攻陷，則只要 n 個私密分享中心，不要超過 t 個以上被入侵者攻陷，則本篇論文的架構在這樣的情況下，依然是安全的。

第三節　在可記憶密碼機制方面的安全性分析

在密碼學上，可記憶密碼機制大多被用在可認證金鑰交換系統(authenticated key exchange)上，而在本篇論文中，是首次將可記憶密碼機制應用在電子投票系統上，為了能讓使用者容易記得，可記憶密碼的長度大多不長，最多只有 8~10 個字元，由於長度短、範圍小，

攻擊者隨意亂猜，猜中的機率相對的就比較高，因此，可記憶密碼機制的安全性其實是很脆弱，最簡單的攻擊方法就是用所有可能的密碼去測，畢竟 8~10 個字元的組合並不多，以現在電腦運算的速度不需要很長的時間，另外，由於一般使用者為了方便好記，有可能將可記憶密碼取成某個有意義的字，所以，攻擊者可以使用字典攻擊法，利用特定長度有意義的字來試使用者的密碼。

在本節接下來的內容，將針對可記憶密碼機制可能的攻擊方法，對於本篇論文的架構做分析，來說明本篇論文可否抵擋這些攻擊。

1. 竊聽攻擊法

在可記憶密碼機制，竊聽功擊法的做法是在使用者傳遞資料時從旁竊聽，並從竊聽到的資料，得到有關這個使用者的可記憶密碼的相關資訊。表五的內容是用來證明，本論文的架構可以抵擋竊聽攻擊。

1. 在整個架構中和可記憶密碼有關的資料 ballot (x, y)=(g_1^{β} mod p, $g_2^{\alpha+\beta}h_2^{\pi}G^{v}$ mod p), $g_1^{\alpha}h_1^{\pi}$ mod p, $s_3=r_3-d_2*\pi$ mod q
2. 由s_3任何π' 都可以找到一組r_3'及d_2'滿足$r_3'-d_2'*\pi'=s_3$
3. 由$g_1^{\alpha}h_1^{\pi}$ mod p 相當於解discrete log的問題
4. 由選票，由於是 ElGamal 加密機制，ElGamal 是基於 Discrete log.，是很難的問題，所以很難由選票得到和使用者的可記憶密碼的有關資訊

（表五）阻擋竊聽攻擊法

2. 驗證碼的洩露連累

在可記憶密碼機制，”驗證碼的洩露連累”的意義是，在選務中心的驗證碼被攻擊者得到，而由於驗證碼隱藏了投票者的可記憶密碼，所以，攻擊者可能藉由驗證碼的洩露來得到有關該名投票者的可記憶密碼的資訊，或甚至得到該名投票者的可記憶密碼。表六的內容是用來證明，本論文的架構沒有”驗證碼的洩露”連累的問題存在。

驗證碼：$g^{\alpha}h^{\pi} \bmod p$ (1) 令$g = h^{a}$, 則$g^{\alpha}h^{\pi} = h^{a\alpha+\pi}$ (2) 攻擊者隨意猜一個值α'，都會有一個π'符合$h^{a\alpha+\pi} = h^{a\alpha'+\pi'}$。 (3)事實上, 要單獨從驗證碼得到投票者的可記憶密碼，相當於是解離散對數的問題，而解離散對數的問題是非常難的。

(表六)可避免驗證碼的洩露連累

3. 字典攻擊法(dictionary attack)

在可記憶密碼機制，字典功擊法的做法是攻擊者利用投票者取的可記憶密碼大多都是有特殊意義的文字的特性，將這些有意義的文字當做猜測的密碼，來尋找可能是投票者的可記憶密碼。

在字典攻擊法中，有兩種攻擊的模式，一種是即時字典攻擊法(online dictionary attack)，另一種則是離線字典攻擊法(offline dictionary attack)，在下面的內容，將分別就這兩種攻擊法做分析，以及針對本篇論文的架構能否抵擋這兩種攻擊法做說明：

(a) 即時字典攻擊法

即時字典攻擊法的做法是，猜測欲攻擊的投票者的可記憶密碼，代替該名投票者投出選票，在表七的內容中，用來證明本篇論文的架構可以抵擋即時字典攻擊法。

1. 每次選舉只能投一張選票，攻擊者猜對的機會只有 $1/2^{\lvert\pi\rvert}$， 2. 即使猜對通行碼，亦需解出$g_1^{\alpha}h_1^{\pi} \bmod p$ 的α， 此為解discrete log的問題，在理論上的認知是很難解的問題

(表七)

(b) 離線字典攻擊法

離線字典攻擊法的做法是，先得到投票者的投票內容，再離線猜測該名投票者可能的可記憶密碼，然後，再跟投票者的投票內容做比較，藉此得到部份或全部的該名投票者的可記憶密碼的資訊。

在表八的內容中，將分析攻擊者使用離線字典攻擊法，無法得到任何資訊，用來證明本篇論文的架構可以抵擋離線字典攻擊法。

1. 攻擊者從本篇的投票機制可以得到以下三個和投票者的可記憶密碼有關的數值。
   $g_1^{\alpha}h_1^{\pi} \bmod p$
   $r_3-d_2*\pi \bmod q$
   $g_2^{\alpha+\beta}h_2^{\pi}G^{v} \bmod p$
2. 攻擊者猜測該位投票者的可記憶密碼π'
3. 攻擊者將第一步的三個數值做以下的計算
   $g_1^{\alpha}h_1^{\pi-\pi'} \bmod p$
   $r_3-d_2*(\pi-\pi') \bmod q$
   $g_2^{\alpha+\beta}h_2^{\pi-\pi'}G^{v} \bmod p$
4. 因為α,β都是從範圍很大的一組數裡面隨機選的值，所以從步驟 3.得到的三個數值無法讓攻擊者藉由不斷猜測和比對，得到任何有關該名投票者的可記憶密碼的資訊。
5. 既然攻擊者無法直接用比對的方法來判斷猜測的π'是否正確，那攻擊者是否可以利用本篇論文的架構中，驗證合法性的式子，來判斷是否猜測的密碼是否正確呢?我由下列的式子來證明，攻擊者是沒辦法利用這方法來做猜測的密碼是否正確的判斷。
   $g_1^{s_2}h_1^{s_3}(x*g_1^{\alpha}h_1^{\pi-\pi'})^{d_2}$
   $=g_1^{r_2-d_2(\alpha+\beta)}h_1^{r_3-d_2*(\pi-\pi')}(g_1^{\beta}*g_1^{\alpha}h_1^{\pi-\pi'})^{d_2}$
   $=g_1^{r_2}h_1^{r_3}=a_2 \pmod p$

(表八)抵擋離線攻擊法

第四節　與其他電子投票系統安全性的比較

我們選了幾篇電子投票機制的論文，將本篇論文和其他數篇電子投票機制的論文做安全性上的比較，來顯示出各篇論文在安全性上的達成度，而本篇論文除了能符合全部的電子投票機制的安全性外，還加入可記憶密碼保護機制的論文，和其他篇論文比較的結果，整理

在表九。

√: 滿足 ×:不滿足

	正確性	完全性	完美性	強固性	隱私性	驗證性
[SK95]	√	√	√	√	√	每個人皆可
[CGS97]	√	√	√	√	√	每個人皆可
[HS00]	√	√	√	√	√	限特定人士
[LK00]	×	√	√	√	√	每個人皆可
[MBC01]	√	√	√	√	√	每個人皆可
[本篇論文]	√	√	√	√	√	每個人皆可

	無收據性	合格性	一人一票	密碼保護	untappable channel
[SK95]	×	√	√	×	**yes**
[CGS97]	×	√	√	×	**no**
[HS00]	√	√	√	×	**yes**
[LK00]	√	√	√	×	**yes**
[MBC01]	√	√	√	×	**yes**
[本篇論文]	√	√	√	√	**no**

(表九)安全性分析

第五節　與其他電子投票系統可抵擋攻擊的比較

每一個電子投票機制，在不同時期被攻擊，對於整個投票系統安全所造成的影響也有所不同，在本節中，我們將針對本篇論文和其他篇論文，在不同時期被攻擊時，對於整個投票系統安全的影響，做詳細的分析與說明，整個分析的內容在下面的表十、表十一中，這兩個表格中分別是分析只有投票者被攻陷，以及只有選務中心被攻陷的情況下，在不同時期被攻陷，對於整個投票系統的安全所造成的影響。

√: 可抵擋 ×:不可抵擋

	投票前	投票後
[SK95]	×	√
[CGS97]	×	×
[HS00]	×	√
[LK00]	×	√
[MBC01]	×	√
[本篇論文]	×	√

（表十）只有投票者被攻陷

投票前：

[SK95]

如果投票者在這時期被攻陷，則入侵者可以指定投票內容給該名投票者，如此，則該名投票者被入侵者掌握住，因此，這篇論文，如果投票者在這時期被攻陷，則不安全。

[CGS97]

如果投票者在這時期被攻陷，則入侵者可以指定所有在整個投票過程中必須用到的數值給該名投票者，如此，則該名投票者被入侵者掌握住，因此，這篇論文，如果投票者在這時期被攻陷，則不安全。

[HS00]

如果投票者在這時期被攻陷，則入侵者可以指定投票內容給該名投票者，如此，則該名投票者被入侵者掌握住，因此，這篇論文，如果投票者在這時期被攻陷，則不安全。

[LK00]

入侵者可以指定自己想投的內容，並且自行選擇其他必須的值，產生在一開始也就是這篇論文提到的 PV1 時期所需要的內容，並將這些值告訴投票者，投票者在和誠實的驗證者做完將選票再加密的步驟後，只能選擇由入侵者指定的並且經由誠實的驗證者再加密的選票，所以，這篇論文在這時期被攻破是不安全的。

[MBC01]

如果入侵者希望投票者投出的選票是 v，則入侵者可以自行選擇 a_2，並且產生屬於−v 的選票 $(g^{a_2}, h^{a_2}G^{-v}) \pmod p$，如此，則該明投票者必須產生另一張圈選內容為 v 的合法選票，不然，送出去的選票就不合法，因此，投票者在這個時期被攻陷是不安全的。

[本篇論文]

在這個機制中，和其他機制有相同的問題，當投票者在投票前被攻破，則攻擊者可以控制投票者的投票動作，因此，在這時期被攻破，則不安全。

投票後：

[SK95]

由於這篇論文採用混合網路(mix-net)的機制，而且使用不公開的管道來送各混網中心的排列順序給投票者，投票者無法像入侵者證明混網中心送來的排列順序為何，因此，投票者無法向入侵者證實其圈選內容，所以，本篇論文在這時期被攻陷是安全的。

[CGS97]

由於在這篇的機制中，投票者只單純送出選票(x, y)到選票電子公佈欄上，因此，入侵者可以要求投票者透露其選擇的私密值以及投票內容，並依這兩個值產生一組選票(x',y')，和(x, y)做比對看是否相同。而由於選票是採用 ElGamal 加密機制，投票者要找到另一組私密值和投票內容來滿足(x', y') = (x, y)是很難的，因此，這個機制在這時期還是不安全的。

[HS00]

由於這篇論文採用混合網路(mix-net)的機制，而且使用不公開的管道來送各混網中心的排列順序給投票者，投票者無法像入侵者證明混網中心送來的排列順序為何，因此，投票者無法向入侵者證實其圈選內容，所以，本篇論文在這時期被攻陷是安全的。

[LK00]

由於在投票者投出選票時，會經由一個誠實的驗證者將選票做再加密的動作，而誠實的驗證者向投票者證明其的確有正確的做再加密的步驟，無法轉移向任意第三者證實，所以，投票者無法向入侵者證明其投票內容。

[MBC01]

因為投票者會產生兩張選票，並且由智慧卡產生隨意值對選票做再加密的動作，在投完票之後，投票者無法向入侵者證明所投出去的選票內容為何，因此，可以確保在這時期，投票者被攻破的話，仍然可以維持其安全性。

[本篇論文]

由於本篇論文中，會由投票機器另外產生一個隨機值，將選票做再加密，並且由投票機器產生選票和驗證資料，在無法知道投票機器

產生的隨機值為何的情況下，投票者無法向入侵者證實其投票內容。

√: 可抵擋 ×:不可抵擋

	註冊	投票	計票
[SK95]	×	√	√
[CGS97]	×	√	√
[HS00]	×	√	√
[LK00]	×	√	√
[MBC01]	×	√	√
[本篇論文]	×	√	√

（表十一）只有選務中心被攻陷

註冊：

在註冊階段被攻破的話，所有的系統參數，還有私密金鑰都由入侵者決定，因此，所有的機制在這時期被攻破，都不安全。

投票：

[SK95]

在這篇論文的架構中，所有的混網中心(mix-net center)在做再加密的動作時，都必須要向所有人證明其所再加密的確實是投票者或是前個混網中心送出的選票，因此，攻擊者在這個階段是無法造假的。

[CGS97]

由於在投票階段，投票者只從投票中心接收挑戰值 c，而這個值被攻擊者知道，或由攻擊者決定，都不會讓選票內容被竊取，因此，不影響安全性。

[HS00]

只要不要超過門檻值 t 個以上的計票中心被攻破，則可以保證這

時期的安全性。

[LK00]

在投票的階段，投票中心扮演的角色是驗證者，所以即使在這時期被攻擊者攻破，由於攻擊者可以操作的只有挑戰值，而知道挑戰值並無法藉此解出投票內容，因此，對於整個投票過程並沒任何影響，所以仍然保持安全性。

[MBC01]

在這時期，投票者除了將選票放到電子佈告欄以外，並沒有跟投票中心有任何的互動，即使投票中心在這時期被攻破，依舊是安全的。

[本篇論文]

由於在本篇論文中，所採用的證明步驟都是非互動式的，投票者除了將選票放到電子佈告欄以外，並沒有跟投票中心有任何的互動，即使投票中心在這時期被攻破，依舊是安全的。

計票：

[SK95]

在這篇的機制中，選票和計票結果都有驗證資料，藉由這些資料每個人都可以驗證選票和計票結果是否正確，因此，攻擊者在計票階段無法假造計票結果，卻又能夠通過驗證，所以是安全的。

[CGS97]

由於本篇採用私密分享機制，將私密值分佈在私密分享中心，只要不超過門檻值 t 的私密分享中心被攻破，則可以確保計票的正確性，可以保證本階段的安全。

[HS00]

由這篇論文完全性的證明，任何人都可以驗證選票是否正確，並且套到計票結果的證明步驟做驗證，因此，入侵者無法假造計票結

果，並且通過驗證。

[LK00]

由於本篇採用私密分享機制，將私密值分佈在私密分享中心，只要不超過門檻值 t 的私密分享中心被攻破，則可以確保計票的正確性，可以保證本階段的安全。

[MBC01]

由於本篇採用私密分享機制，將私密值分佈在私密分享中心，只要不超過門檻值 t 的私密分享中心被攻破，則可以確保計票的正確性，可以保證本階段的安全。

[本篇論文]

由私密金鑰是被分佈在私密分享中心，而驗證者可以藉由投票者投票時產生的驗證資料，來驗證每張選票是否合法，因此，只要不超過門檻值的私密分享中心被攻破，則本篇論文是安全的。

第六章 結論與未來工作

在本篇論文中，我們提出了新的電子投票機制，這個電子投票機制除了保留原本以 ElGamal 加密機制為基礎的電子投票機制的安全性之外，還加上了可記憶密碼機制的保護，藉由可記憶密碼簡短易記的特性，保障即使代表自己身份的智慧卡遺失了，拾獲的人由於沒有和該張智慧卡相配合的可記憶密碼，所以沒有辦法代替智慧卡的所有者投出合法的選票。

因為使用了可記憶密碼的機制，在第四章有關安全性的說明中，除了證明本篇論文的架構符合電子投票的安全性外，還證實了本篇論文的架構能夠抵擋在使用可記憶密碼機制時最可能受到的幾種攻擊型態，因此，本篇論文在可記憶密碼機制和電子投票機制的安全性，都能夠滿足，不因使用可記憶密碼機制，而犧牲了任何有關電子投票機制安全性的要求

雖然本篇論文在電子投票機制中，加入了可記憶密碼的機制，是一個蠻特別的想法，也增加了電子投票機制的安全性，然而，本篇論文並不是盡善盡美的，在本篇論文中仍有幾個問題，在此提出來，期待各位對電子投票機制有興趣的人，能夠一起來思考這些問題，找到解決的方法。

(1) 目前無收據式的電子投票機制，都必須要經由一個投票盒或投票機器來投票，藉此來保證投票者無法向第三者證明自己圈選的內

容，是否有方法，可以不經由這樣的一個中介機制，直接由投票者做出選票，而且又能達到無收據性的要求？

(2) 在本篇有關可記憶密碼機制的安全性證明上，只能就個案去解釋本篇的機制符合安全性的需求，以往在身份認證與金鑰交換協定上，有許多學者提出了數種正規的驗證方法，但是這些方法，在本篇使用可記憶密碼的電子投票機制上，由於必須知道所有的私密資訊，包括投票內容以及密碼等，這樣子的證明方法反而就不合適了，期望在未來，有人能研究出適合可記憶密碼機制使用的正規驗證方法。。

(3) 本篇論文是將可記憶密碼機制，加在以 ElGamal 加密機制為基礎的電子投票機制，也就是說，本篇採用的機制不一定適合在其他的電子投票機制使用，在這方面有兩個研究方向可做，一個是針對其他電子投票機制，加入可記憶密碼機制，另外一個方向則是，是否能找到一個針對所有電子投票機制都合用的加入可記憶密碼機制的方法。

參考文獻

[Cha81] D. Chaum. “Untraceable electronic mail, return address, and digital pseudonyms.” Communications of the ACM, 24(2):84-88, 1981.

[CF85] D. Cohen and M.J.Fisher. “A robust and verifiable cryptographically secure election scheme.” In Proc. 26th IEEE Symposium on the Foundations of Computer Science(FOCS), pp.372-382. IEEE, 1985.

[Ben87] J.C.Benaloh. “Verifiable Secret-Ballot Elections.” PhD thesis, Yale University, Dec. 1987.

[Cha89] D.Chaum. “Elections with unconditionally-secret ballots and distribution equivalent to break RSA.” In Advances in Cryptology – EUROCRYPT ’89, volume 434 of Lecture Notes in Computer Science, pp.177-182, 1989.

[FOO92] A.Fujioka, T.Okamoto, and K.Ohta. “A practical secret voting scheme for large scale elections.” In Advances in Cryptology – AUSCRYPT ’92, pp.244-251, 1992.

[BT94] J.C.Benaloh, D.Tuinstra “Receipt-free Secret-ballot Elections (Extended Abstract)”, Proceedings of the 26th ACM symposium on the Theory of Computing, pp. 544-553, 1994.

[SK95] K.Sako, J.Kilian “Receipt-free mix-type voting scheme – A practical solution to the implementation of a voting booth -.” Proceedings of Advances in Cryptography: Eurpcrypt ’95, Lecture Notes in Computer Science 921, Springer-Verlag, pp. 393-403, 1995

[NR94] V.Niemi, A.Renvall. “How to prevent buying of votes in computer elections.”

In advances in Cryptology – ASIACRYPT ’94, volume 917 of Lecture Notes in Computer Science, pp.164-170, 1994.

[CGS97] R.Cramer, R.Gennaro and B.Schoenmakers “A Secure and Optimally Efficient Multi-authority Election Scheme.” Eurppean Transactions on Telecommunications, pp. 481-489, 1997. Preliminary version in Proceedings of Advances in Cryptography: Eurocrypt ’97.

[Oka97] T.Okamoto. “Receipt-free electronic voting schemes for large scale elections.” In Proc. of Workshop on Security Protocols ’97, volume 1361 of Lecture Notes in Computer Science, p.25-35, 1997.

[HS00] M.Hirt, K. Sako “Efficient receipt-free voting based on homomorphic encryption” Proceedings of Advances in Cryptography: Eurocrypt ’00, Lecture Notes in Computer Science 1807, Springer-Verlag, pp. 539-556, 2000.

[LK00] B.Lee, K.Kim “Receipt-free Electronic Voting through Collaboration of Voter and Honest verifier” In Japan-Korea Joint Workshop on Information Security and Cryptology (TW-ISC2000), pp.101-108, 2000.

[MBC01] E.Magkos, M.Burmester and V.Chrissikopoulos “Receipt-freeness in Large-Scale Elections without Untappable Channels” In B.Schmid et al., editor, First IFIP Conference on E-Commerce, E-Business, E-government(I3E), page 683-694, 2001

[BM92] S. Bellovin and M. Merritt, “Encrypted key exchange : password-based protocols secure against dictionary attacks”, In Proceedings of the IEEE Symposium on Research in Security and Privacy, pp. 72-84, 1992