東海大學應用數學研究所

碩士論文

# 電子投票系統

研究生：徐永憲

指導教授：沈淵源教授

中華民國九十六年一月

# 致謝

本篇論文得以順利完成，首先必須感謝我的指導教授沈淵源老師這兩年來辛勤的教誨與指導。 使我在疑惑的同時，能即使的找到方向，有如事半功倍、漸入佳境的效果。 感謝系上的所有老師們辛苦教誨。特此致謝！
此外，還要感謝這兩年來朝夕相處的同學們，謝謝你們的鼓勵及關懷，讓我一路走來，雖有艱辛，但所結的果實是甜美的。最後，我必須感謝我的兄姐， 能適時的鼓勵我關心我，讓我能無憂的唸書。因此，今後能在數學的領域裡能貢獻更多的心力以回饋大家。

# 摘要

本篇論文主要目的在探討電子投票系統。第二章我們介紹數位簽署演算法 且在第三章簡介橢圓曲線密碼系統以及橢圓曲線版的秘密分享。最後結合這些密碼術相關的演算法，發展一套不容易 被入侵以及能運用在各式各樣投票機制上的電子投票系統以供使用。

關鍵字： 電子投票系統、 橢圓曲線版的秘密分享。

# Abstract

In this thesis, we construction of our e-voting system. First, we discuss the security and verification of RSA, DSA, Blind signature, Shamir and Elliptic Curve Secret Sharing Algorithm. Finally, we try to use these technique to construct a security and fast e-voting system with keeping the privacy.



*Key Words :* E-voting system; Elliptic Curve Secret Sharing

# 目 錄

# 1 序論

在這個快速變遷講究效率的年代，傳統的投票、計票方式早已太過老舊 、浪費資源而且容易因人為因素造成選舉不公等等缺點。因此一個快速、有效率 、公正、透明、節省資源的電子投票系統是個不錯的選擇。然而想要 建立一個具安全性、隱密性及節省資源乾淨的電子投票系統也不是一件 容易的事。隨著電腦的快速發展以及密碼術的精進，我們嘗試結合密碼術中相關的演算法， 發展一套不容易被入侵以及能運用在各式各樣投票機制上的電子投票系統以供使用。 在這篇論文中我們的電子投票系統分成四大部分，分別為系統管理者、 監票中心、佈告欄以及佈告欄管理者。首先，選舉人先登入系統跟系統管理者註冊 以 DSA 數位簽署法註冊成合法的選舉人。其次，系統管理者再以盲簽法簽署選舉人的 數位身份 $\delta$ 為 $I$ 成為選票號碼。接著，選舉人以 $I$ 圈選選票 $c_i$ 以橢圓曲線秘密分享法加密分享 給佈告欄管理者、監票中心和自己，接著佈告欄管理者結合選票，最後監票中心再結合選票公佈在佈告欄，這樣便完成了選舉。

## 2 數位簽署

長久以來，人們使用各式各樣的簽名，作為簽名者本人與文件或作品之 間的一個連結或證明。在某些需要介紹信的場合，通常要求寫介紹信的人，將信放入 信封袋後彌封並在彌封接口處簽上大名，表示是此人親自做的。 譬如說，你要在一份電子文件上簽名，為何不能僅僅將你的簽字數位化後 然後附在文件上呢?任何人只要能接觸到你在某一份文件上的簽字，那只要將這份文件上的 簽字移除或加以拷貝，然後再貼入其他的地方，就可在電腦上造假這種文件則是相當容易而 且跟原版完全一樣難以區分。所以，我們要求數位簽署不可以跟它原來的訊息分離也不可以 附在原訊息上面，也就是說，簽名不僅僅要跟簽名者連結在一起，也要跟被簽署者的訊息 連結在一起。再者，數位簽署必須很容易被對方或其他的第三者來驗證。

下面我們介紹RSA簽署[6]及盲簽[1]，這是系統管理者 向登入者做位元承諾所需要使用的數位簽署，以達到合法選民的資格。接著，簡單介紹雜湊函數(Hash function)及利用雜湊函數的性質所發展出的MD5演算法，目的是為了對任意長度的的明文轉換成固定長度的字串， 這樣才符合實際上的應用，避免產生過大的資料造成的不實用性。最後，介紹ElGamal及DSA數位簽署演算法 ，這是投票者向統管理者登入所使用的數位簽署演算法。

## 2.1 RSA簽章及盲簽

西元1997，三位美國麻省理工學院學者李瓦士（Rivest）、夏米爾（Shamir） 、以及艾道曼（Adleman）率先公佈RSA[6]加密 演算法並取得專利權，此演算法是最先進及最方便的加密方法，它在電子商務交易中扮 演了相當重要的角色，目前有很多的數位消費性產品，都是利用了RSA加密來傳遞訊息。RSA加密 演算法是一種特殊的非對稱密碼法，利用兩個質數作為加密與解密的兩個鑰匙(key)。這 兩個鑰匙分別稱為公開鑰匙(public key) 和私人鑰匙 (private key 或是secret key)，鑰匙的長度約在40個位元到1024位元。公開鑰匙作為加密，只有使用私人鑰匙才能解密，解密者只要不洩露私人鑰匙，別 人就算有公開鑰匙，也是很難推演算出來私人鑰匙，就算是利用反向方式來解密也不是一件簡單的事，所以 RSA 算是一種十分安全的加密與解密演算法。 而在1982 年由Chaum 首先提出第一個盲簽章[1](Blind Signature) 的概念。 盲簽章不只達成了傳統數位簽章的需求，盲 簽章有著可以保護送簽者身份的特性，即所謂的匿名性，可以用來避免送簽者的身份 遭到追蹤。這種特性符合了無記名投票系統，電子競標的機制上對使用者身份保密的需求。

1. RSA簽署：甲擁有一份文件 $m$ ，乙同意在上面簽名，他們可如下進行。

- 乙選取兩個大質數 $p$ ， $q$ 並計算乘積 $n = pq$ 。他們同時又選取一介於1與 $\phi(n)$ 之間與 $\phi(n)$ 互質的整數 $e$ ，並計算在模 $\phi(n)$ 之下 $e$ 的乘法反元素 $d$ 。乙將 $(n, e)$ 公佈，如上網、印在名片上或放在電話簿內，但 $d, p, q$ 則保持私密。
- 乙的簽名為 $y = m^d \pmod{n}$，可將數對 $(n, e)$ 公開之。

甲可以驗證訊息的確是乙所簽名過的，步驟如下：

- 下載或查出乙的公開鑰匙 $(n, e)$ ，並計算 $z = y^e \pmod{n}$ 。
- 若 $z = m$ ，則甲接受此簽名為有效的，否則為無效。

假設丙要將乙的簽名附在另一份信息 $m'$ 上。丙不能僅僅使用數對 $(m', y)$ ，此乃因為 $y^e \neq m' \pmod{n}$ 。所以丙需要 $y'$ 滿足 $y'^e \equiv m \pmod{n}$ 。這就如同在解RSA的密文 $m$ 一樣，希望得到其對應的明文 $y'$ ；但這在計算上，是難於達成的任務。

2. 盲簽章： Chaum 說明要如何完成盲簽:假設甲有一份訊息$m$，希望透過乙來幫他完成簽署，但又不希望乙知道其內容 $m$ 。則 $(n, e)$ 為乙的 RSA 公開的鑰匙且 $d$ 為乙的 RSA 私密鑰匙。

- 甲隨機選取一個數 $r$ ， $\gcd(r, n) = 1$ ，計算 $x = (r^e \cdot m) \bmod n$ 並送 $x$ 給乙。
- $x$ 是由整數 $r$ 所矇蔽的結果，因此乙不可能在沒有任何資訊之下由 $x$ 衍生出 $m$。
- 乙對 $x$ 簽署 $t = x^d = (r^e m)^d \bmod n$ ，然後把 $t$ 回傳給甲。且 $x^d \equiv (r^e \cdot m)^d \equiv r \cdot m^d \pmod{n}$
- 甲在收到 $x$ 的簽署 $t$ 之後可以計算 $t' = r^{-1} \cdot t = x^d \cdot r^{-1} = m^d \pmod{n}$ ， $m = (t')^e \pmod{n}$ 則甲接受此簽名為有效的，否則為無效的。

## 2.2 ElGamal數位簽署

ElGamal密碼系統[8]是專門為簽名而設計的。不同於RSA的特色就是對任何的一個訊息有多種不同的簽署法。 假設甲要簽署一份文件，首先她先選擇一個大質數 $p$ 及一個原根 $\alpha$ ，然後選取一個介於1與 $p-2$ 之間的 整數 $a$ 並且計算 $\beta \equiv \alpha^a \pmod{p}$ 。公佈三個數為 $p, \alpha, \beta$ 。整個系統的安全性是建立在 $a$ 的私密性上。敵者想從 $(p, \alpha, \beta)$ 來決定 $a$ 是困難重重的，因為離散對數問題是困難的。

甲簽署一訊息 $m$ ，他可以進行如下：

1. 選取一秘密隨機整數 $k$ 使得 $\gcd(k, p-1) = 1$。
2. 計算 $r \equiv \alpha^k \pmod{p}$ 。
3. 計算 $s \equiv k^{-1}(m - ar) \pmod{p-1}$

簽署後的訊息為 $(m, r, s)$ 。

乙可以驗證此簽名的有效性，其步驟如下：

1. 下載甲公佈的鑰匙 $(p, \alpha, \beta)$ 。
2. 計算 $v_1 \equiv \beta^r r^s \pmod{p}$ 及 $v_2 \equiv \alpha^m \pmod{p}$ 。
3. 接受此為有效簽名 $\iff$ $v_1 \equiv v_2 \pmod{p}$ 。

   註：先假設此簽名是有效的。因為 $s \equiv k^{-1}(m-ar) \pmod{p-1}$ ，我們有 $ks \equiv m-ar \pmod{p-1}$ ，所以 $m \equiv ks+ar \pmod{p-1}$ 。因此 $v_2 \equiv \alpha^m \equiv \alpha^{ks+ar} \equiv (\alpha^a)^r(\alpha^k)^s \equiv \beta^r r^s \equiv v_1 \pmod{p}$ 。

## 2.3 雜湊函數(Hash function)

雜湊函數 (Hash function) $H$ 是將訊息 $m$ 轉換成固定長度的字串 $h$ ， $h = H(m)$ 。雜湊函數的性質常被用於各式各樣的計算用途, 但當使用在密碼學上，雜湊函數它的附加性質常被拿來使用。 在密碼學上雜湊函數的基本要求如下：

- 輸入的訊息長度是任意的。
- 輸出的長度是固定的。
- 對任意的訊息 $m$ ,可以很快地算出其對應的訊息 $H(m)$ ，且 $H(m)$ 是很容易計算的。
- 由訊息摘要 $H(m)$ ，來尋找一個 $m\prime$ 使得 $H(m\prime) = H(m)$ ，在計算上是不可行的(換句話說， $H$ 是一個單向函數)。注意，若 $H(m)$ 為某一訊息的訊息 摘要，我們並非試圖找出此一訊息。我們僅想找到一個 $m\prime$ 使得 $H(m\prime) = H(m)$ 而已。
- 尋找訊息 $m_1$ 及訊息 $m_2$ ，在計算上使得 $H(m_1) = H(m_2)$ 是不行的，我們稱為强勢免於碰撞的函數。

雜湊函數是單向不可逆的函數，也就是說由一個雜湊值 $h$ ,$(H(m_1) = h$ )推出 $m_1$ ，這是不可能辦的到的。如果給定訊息 $m_1$ ，在計算上 找不到一個訊息 $m_2$ ，使得 $H(m_1) = H(m_2)$ ，我們稱為强勢免於碰撞的函數。如果是任意找兩個不同的訊

息 $m_1,\ m_2$ ，且 $H(m_1) \neq H(m_2)$ ，我們稱為强勢免於碰撞的函數 $H$ 。

## 2.4 MD5演算法

MD5[6](Message Digest 5)為數位訊息加密演算法。 MD5是由Ron Rivest所設計的，他同時也是'RSA'的設計者之一的 一人，其中R就是他名子的R。它是以MD4的基礎下去做改變的，比MD4更加的安全 計算也比MD4多了一回合的運算。MD5 演算法是輸入任意長度的訊息，而輸出的訊息長度為128位元當做指印或訊息摘要。 它被臆想，計算上是不可能發生兩則不同的訊息有同樣訊息文摘。MD5 演算法欲為數位簽名之應用， 一個大文件必須是"壓縮的" 以安全方式以一把私有(秘密) 鑰匙及一把公衆鑰匙的加密系統之下，譬如RSA， 把它編成密碼。

- 輸入資料區分為四個暫存器：A, B, C, D。
- 區分為四個步驟，每步驟計算 16 次，合計 64 次。
- 加入 $sin(x)$ 非線性函數參數值。

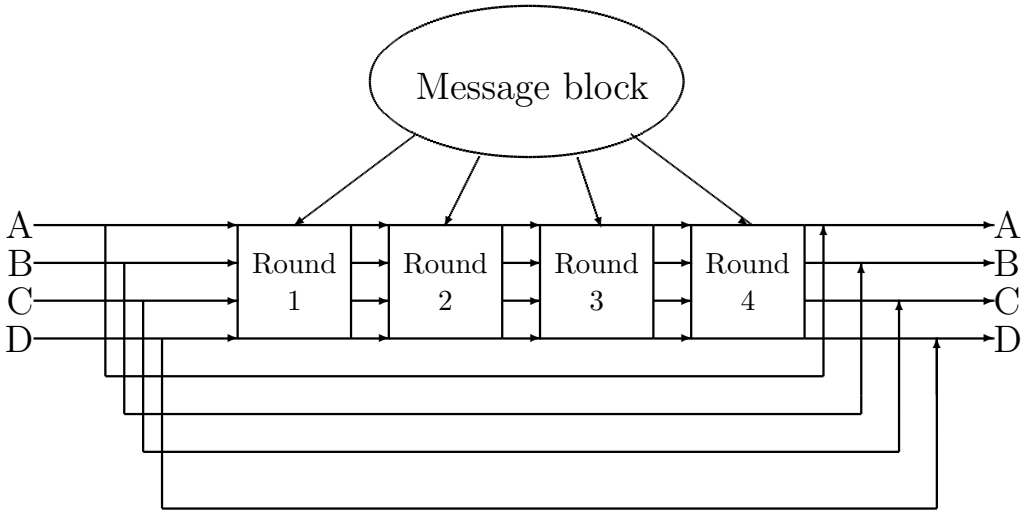


圖 2.1 MD5 主要迴路

- 每一回合16個運算步驟：

  首先給定四個函數做運算，每個函數以輸入32位元的字串當做起始 值，輸出32位元的字串為結果。

  以下為四個四個非線性函數，每一個函數接用在不同回合。(不同的函數用在不同的回合)

  1. $F(X,Y,Z) = (X \bigwedge Y) \bigvee ((\neg X) \bigwedge Z)$
  2. $G(X,Y,Z) = (X \bigwedge Z) \bigvee (Y \bigwedge (\neg Z))$
  3. $H(X,Y,Z) = X \bigoplus Y \bigoplus Z$
  4. $I(X,Y,Z) = Y \bigoplus (X \bigvee (\neg Z))$

  $\bigoplus$ 為 XOR, $\bigwedge$ 為 AND, $\bigvee$ 為 OR, $\neg$ 為 NOT $\Lambda$

$M_j$ 表示成第 $j$ 個子訊息(從 0 到 15 )，而 $\lll s$ 表示成往左平移 $s$ 位元，則此四個運算函數為：

在這個步驟中加入64個sine 函數值的運算 $T[i] = 2^{32} \cdot \text{abs}(sin(i)), i = 1 \ldots 64$ ， $i$ 為弧度。 輸出訊息摘要，執行 $SUM_{32}$ 計算。

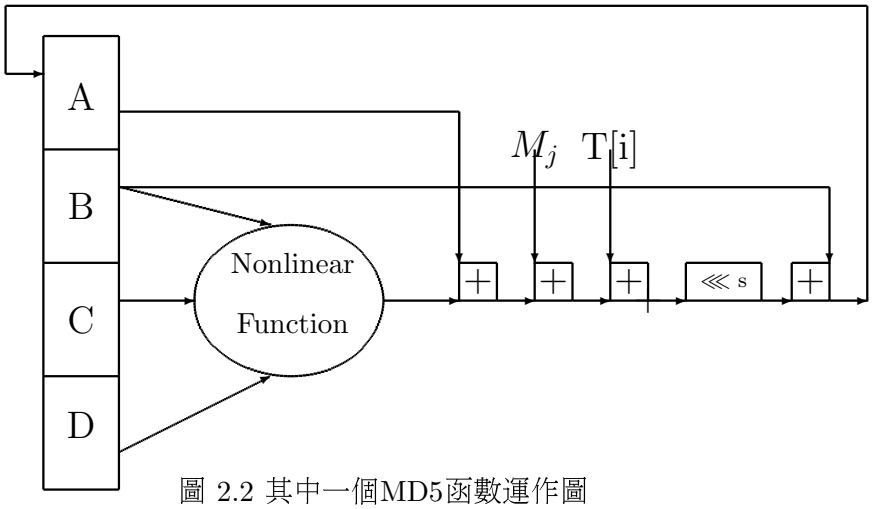


圖 2.2 其中一個MD5函數運作圖

- 總結

MD5訊息演算法提供"指印"或任意長度的訊息文摘。它被臆想，困難到二則消息有同 樣消息文摘是大約要操作 $2^{64}$ 次，並且困難到任一則消息有一本指定的消息文摘是大約要操 作 $2^{128}$ 次。MD5 算法仔細地被詳細檢查了為弱點。然而，相對地新算法和進一步安全分析當然這一點隨 著這個排序被被取代事情有可原的。

## 2.5 DSA 演算法

美國標準與工技院NIST於1991年時提出數位簽章演算法DSA(Digital Signature Algorithm)[11]，並於1994年採用DSA為其標準。又如同ElGamal簽署法，DSA是一種帶附錄的數位簽署法。又如同其它簽署 法，通常簽名在其信息摘要上。在此種情況下，其雜湊函數產生出一個160位元的信息摘要。下面我們假設資料信息 $m$ 已經被 雜湊函數處理過的。因此我們要在一個160位元的信息上簽名。

- 製做鑰匙:
  - 選擇一個160-bit 的質數 q.
  - 選擇一個 $L$-bit 質數 $p$, 對任意正整數 $z$ ,滿足 $p = qz + 1$ 且 $512 \leqq L \leqq 1024$ ,$L$ 可被64分解.
  - 選擇 $h$, $1 < h < p - 1$, 使得 $g = h^z (\text{mod } p) > 1$.
  - 隨機選取一個數 $a$,且 $0 < a < q$.
  - 計算 $y = g^a (\text{mod } p)$. $(p, q, g, y)$ 為公鑰 , $a$ 為私密鑰匙.

  Note:如果需要的話, $(p, q, g)$ 在這個系統裡可以分享給不同的使用者.

- 簽署:
  - 隨機選取一個整數 $k$ ,$0 < k < q$

– 計算 $r = (g^k \bmod p) (\bmod q)$.

– 計算 $s = (\text{MD5}(m) + a \cdot r)k^{-1} (\bmod q)$, 在這我們使用MD5($m$),把訊息 $m$ 加密.

– 如果 $r = 0$ or $s = 0$ 時,再重新計算.

– $(r, s)$ 為簽署.

- 驗證:

  – 計算 $w = s^{-1} (\bmod q)$.

  – 計算 $e_1 = ((\text{MD5}(m)) \cdot w) (\bmod q)$.

  – 計算 $e_2 = (r \cdot w) (\bmod q)$.

  – 計算 $v = ((g^{e_1} \cdot y^{e_2}) \bmod p) (\bmod q)$.

  – 如果 $v = r$ 則此簽署為真.

- 正確的演算法:

  驗證者都會接受經過辨別的正確簽署.這可由以下的費馬小定理來佐證:

  $g = h^z (\bmod p)$, $g^q \equiv h^{qz} \equiv h^{p-1} \equiv 1 \ (\bmod p)$, 因為 $g > 1$ 和 $q$ 為質數,且 $g$ 的週期為$q$.然後簽署者計算:

$$s \equiv k^{-1}((\text{MD5}(m)) + ar)$$

  則

$$k \equiv (\text{MD5}(m))s^{-1} + ars^{-1} \equiv (\text{MD5}(m))w + arw (\bmod q).$$

既然 $q$ 之週期為 $p$, 我們可得

$$g^k \equiv g^{(\mathrm{MD5}(m))w} g^{arw} \equiv g^{(\mathrm{MD5}(m))w} y^{rw} \equiv g^{e1} y^{e2} \pmod{p}.$$

最後,

$$r = (g^k \bmod p) \bmod q \equiv (g^{e1} y^{e2} \bmod p) \bmod q = v$$

DSA的簽署就正確無誤.

- DSA 例子:
  - 選取 $q = 101$, $p = 78q + 1 = 7879$, $g = 170$, $a = 75$; 則 $y = 4567$
  - 以MD5做簽署 $m$ =22, 簽署者選取 $k = 50$ ; 則

$$\gamma = (170^{50} \mathrm{mod} 7879) \mathrm{mod} 101 = 94$$

$$\delta = (22 + 75 \cdot 94) 50^{-1} \mathrm{mod} 101 = 97$$

    $(m, (94, 97))$ 為訊息的數位簽署。
  - $(94, 97)$ 的簽署訊息文摘為 22 ，在按照以下的步驟驗證。 計算：
  - $w = 97^{-1} \mathrm{mod} 101 = 25$
  - $e_1 = 22 \cdot 25 \mathrm{mod} 101 = 45$
  - $e_2 = 94 \cdot 25 \mathrm{mod} 101 = 27$
  - $(170^{45} \cdot 4567^{27} \mathrm{mod} 7879) \mathrm{mod} 101 = 94 = \gamma$

# 3 秘密分享

在這章節我們將介紹最受歡迎的兩個秘密分享系統，以及其推導過程。

## 3.1 沙密爾門檻秘密分享

在一九七九年由沙密爾(Shamir)[7]所提出，所以稱之為沙密爾門檻法或拉格蘭茲內插法(Lagrange Interpolation Scheme)。 其演算法如下：

定義：令 $t \leq w$ 為兩正整數。一個$(t, w)$-門檻法乃是將訊息 $M$ 分享給 $w$ 位參與者的一種方法。在此方法中， 只需其中任何 $t$ 位參與者就可重建訊息 $M$ ，若少於 $t$ 位便無法重建 $M$ 。

1. 選取一質數 $p$ ，大於所有的訊息也大於所有參與者的人數。此處所有的計算都在模 $p$ 的數系中進行。 若用合成數代替，那下面所得到的矩陣有可能沒有乘法反元素。

2. 將訊息 $M$ 表示成模 $p$ 數系中的一個數，而我們要將訊息 $M$ 分享給 $w$ 位參與者，但只需其中的 $t$ 位便可解出此一訊息。

3. 隨機選取 $t-1$ 個整數 $s_i$ $(i = 1, 2, \cdots, t-1)$ 作為多項式 $s(x)$ 中 $x^i$ 項的係數， 然後將 $M$ 放在此多項式的常數項位置。所以我們得到一多項式

$$s(x) = M + s_1 x + s_2 x^2 + s_3 x^3 + \cdots + s_{t-1} x^{t-1} \pmod{p}$$

其常數項就是原訊息 $M$ ，亦即 $s(0) \equiv M \pmod{p}$。

4. 對這 $w$ 位參與者，我們先選取相異的整數 $x_1, x_2, \cdots, x_w \pmod{p}$，然後再交給每個人一秘密數對 $(x_i, y_i)$，其中$y_i \equiv s(x_i) \pmod{p}$。例如：$1, 2, 3, \cdots, w$乃是這些 $x$ 值既合理而又自然的一個選擇。 所以我們就將數對$(1, s(1)), (2, s(2)), \cdots, (w, s(w))$交給這 $w$ 個人，一人一組。質數 $p$ 是公開的，但多項式 $s(x)$ 則保密。

5. 假設有 $t$ 個人聚在一起分享彼此間的數對。為了簡化符號，我們可假設這些數對為$(x_1, y_1), (x_2, y_2), \cdots, (x_t, y_t)$。 由此，我們要尋回原訊息 $M$ 。

6. 假設有一個 $t-1$ 次的多項式 $s(x)$ ，已知其中的 $t$ 個值為

$$y_k \equiv s(x_k) \pmod{p}$$

我們要從這些資訊來重建這多項式，所以對任意的 $k$ , $1 \leq k \leq t$ ,我們有

$$y_k(x_k) = M + s_1 x_k^1 + s_2 x_k^2 + s_3 x_k^3 + \cdots + s_{t-1} x_k^{t-1} \pmod{p}$$

此處 $s_i$ $(1 \leq i \leq t-1)$ 及 $M$ 均為未知數。

7. 將上面的 $t$ 個同餘式寫成矩陣形式

$$\begin{pmatrix} 1 & x_1 & x_1^2 & \cdots & x_1^{t-1} \\ 1 & x_2 & x_2^2 & \cdots & x_2^{t-1} \\ 1 & x_3 & x_3^2 & \cdots & x_3^{t-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & x_t & x_t^2 & \cdots & x_t^{t-1} \end{pmatrix} \begin{pmatrix} M \\ s_1 \\ s_2 \\ \vdots \\ s_{t-1} \end{pmatrix} \equiv \begin{pmatrix} y_1 \\ y_2 \\ y_3 \\ \vdots \\ y_t \end{pmatrix} \pmod{p}$$

此係數矩陣，暫且稱之為 $V$ ，是一個 Vandermonde 矩陣。我們知道，如果這個矩陣的行列式值在模 $p$ 下不等於零，則此矩陣有唯一的解。 此行列式值可被證明就是

$$\text{detV} = \prod_{1 \le j < k \le t} (x_k - x_j)$$

此值只有當兩個 $x_i$ 一樣時才是 $0 \pmod{p}$(此處的 $p$ 為質數)。所以只要 $x_i$ 相異，則此系統有唯一解。

8. 我們換一個角度來重建多項式 $s(x)$，由此引導我們得到這個多項式的一個公式從而可推得訊息 $M$ 的一個公式。 我們的目標是重建一多項式 $s(x)$，而其中的 $t$ 個值為 $(x_k, y_k), 1 \le k \le t$ ，很自然的 我們會想到 $t$ 次多項式

$$u(x) = (x - x_1)(x - x_2)(x - x_3) \cdots (x - x_t)$$

對每一個 $k = 1, 2, 3 \cdots, t$ ，將 $u(x)$ 除以 $x - x_k$ 得到一個 $t - 1$ 次多項式

$$u_k(x) = \prod_{\substack{j=1 \\ j\neq k}}^{t}(x - x_j)$$

此多項式滿足 $u_k(x_j) = 0, \forall j \neq k$ ；若這些 $x_i$ 兩兩相異，則 $u_k(x_k) \neq 0$ 。再將每一個 $u_k(x)$ 單位化，亦即除以 $u_k(x_k)$ ，稱之為 $l_k(x)$ 。因此得到

$$l_k(x) \equiv \frac{u_k(x)}{u_k(x_k)} \equiv \prod_{\substack{j=1 \\ j\neq k}}^{t}\frac{x-x_j}{x_k-x_j} \pmod{p}$$

顯而易見，我們有

$$l_k(x_j) \equiv \begin{cases} 1, & k = j \\ 0, & k \neq j \end{cases} \pmod{p}。$$

因此我們得到拉格蘭茲內插多項式

$$L(x) = \sum_{k=1}^{t} y_k l_k(x) = \sum_{k=1}^{t} y_k \prod_{\substack{j=1 \\ j\neq k}}^{t}\frac{x - x_j}{x_k - x_j} 。$$

這個多項式滿足所有的條件$L(x_j) = y_j, 1 \leq j \leq t$，因為

$$\begin{aligned} L(x_j) &\equiv \sum_{k=1}^{t} y_k l_k(x_j) \equiv y_j l_j(x_j) + \sum_{\substack{j=1 \\ j\neq k}}^{t} y_k l_k(x_j) \\ &\equiv y_j \cdot 1 + \sum_{\substack{j=1 \\ j\neq k}}^{t} y_k \cdot 0 \equiv y_j \pmod{p} \end{aligned}$$

因此，透過Vandermonde 矩陣的證明，我們知道 $s(x)$ 為經過這些點的唯一的 $t-1$ 次多項式，所以得到$L(x) = s(x)$。

9. 如果要重建秘密訊息 $M$ ，只需計算 $L(0)$ 之值。因此得到秘密訊息的公式為

$$M \equiv \sum_{k=1}^{t} y_k \prod_{\substack{j=1 \\ j \neq k}}^{t} \frac{-x_j}{x_k - x_j} \pmod{p}。$$

## 3.2 橢圓曲線版的秘密分享

我們利用橢圓曲線動態秘密分享[3, 7, 5]系統，强化其加密性。此方法改正了當分享者將自己手上的訊息傳送給分享者時，不需要經過安全秘密通道 ，假如 $t - 1$ 個成員想合謀還原秘密 $k$ ，他們無法知道其他人的訊息 也就無法求得秘密 $k$ 。另外，文中的合成者 $U_A$ ，有效避免以前方法中合成者本身也是參與秘密還原的分享者，而他在恢復秘密後不提供 或提供假的秘密給其他的參與秘密恢復的分享者的問題。

- 橢圓曲線版的秘密分享演算法：

  1. $U_D$ 是系統秘密的分發者， $U_D$ 選取一個大質數 $p$ 及模 $p$ 的一個原根 $g$ , $p$ 大於所有的訊息也大於所有參與者的人數。 $U_i$ 是第 $i$ 個參與者，其身份識別碼為 $\delta_i$ $(i = 1, \cdots, w)$。

  2. 將訊息 $k$ 表示成模 $p$ 數系中的一個數，而我們要將訊息 $k$ 分享給 $w$ 位參與者，但只需其中的 $t$ 位便可解出此一訊息。 $U_D$ 先計算 $K = g^k \pmod p$。

  3. 隨機選取 $t$ 個整數 $a_j$ $(j = 0, 1, 2, \cdots, t-1)$ 作為多項式 $f(x)$ 中 $x^j$ 項的係數 。所以我們得到一多項式

     $f(x) = a_0 + a_1 x + a_2 x^2 + a_3 x^3 + \cdots + a_{t-1} x^{t-1} \pmod{p-1}$,

     $U_D$ 計算 $s = k + a_0 \pmod{p-1}$,

     對 $j = 0, 1, 2, \cdots, t-1$, $U_D$ 算出 $A_j = g^{a_j} \pmod p$;

並對 $i = 1, 2, \cdots, w$ , $U_D$ 算出 $f(\delta_i) \pmod{p-1}$。

4. $U_D$ 選取一橢圓曲線 $E_p(a,b) : y^2 \equiv x^3 + ax + b \pmod{p}$ ,並公開之。

   每個 $U_i$ $(i = 1, 2, \cdots, w)$ 在 $E_p(a,b)$ 上選取一點 $\alpha_i$ ,再隨機選取一整數 $x_i$ 為私鑰，利用私鑰 $x_i$ 計算 $\beta_i = x_i \alpha_i$ 並將 $\alpha_i$ , $\beta_i$ 公佈，但 $x_i$ 保持私密。

5. $U_D$ 將其 $f(\delta_i)$ 轉換成 $E_p(a,b)$ 上的一點 $P_i$ ,

   並將 $s$ 轉換成 $E_p(a,b)$ 上的一點 $Q$ 。選取一隨機整數 $r$ ,

   並算出 $z_{1i} = r\alpha_i$ , $z_{2i} = P_i + r\beta_i$ 與 $z_{3i} = Q + r\beta_i$ ,

   將$(z_{1i}, z_{2i}, z_{3i})$傳給 $U_i$ , $i = 1, \cdots, w$ 。

6. $U_D$ 將 $p$ , $g$ , $K$ , $z_{1i}$ , $z_{2i}$ , $z_{3i}$ , $\delta_i$ ( $i = 1, \cdots, w$ );

   $A_j$ ( $j = 0, 1, \cdots, t-1$ ) 公開。

- 驗證:

1. 每一個 $U_i$ $(i = 1, 2, \cdots, w)$ 使用私鑰 $x_i$ 計算

   $b_i = z_{2i} - x_i \ z_{1i}$ ,

   $c_i = z_{3i} - x_i \ z_{1i}$

   再將 $b_i$ 及 $c_i$ 回復其原值分別為 $B_i$ 及 $B_i$

   (此 $b_i$ 即 $P_i$ , $c_i$ 即 $Q$ ,因而 $B_i$ 就是 $f(\delta_i)$ , $C_i$ 就是 $s$ )

2. $U_i$ 驗證下列各式是否呈立

   $g^{C_i} = K \cdot A_0 \pmod{p}$, $g^{B_i} = \prod_{j=1}^{t} {A_{j-1}}^{{\delta_i}^{j-1}} \pmod{p}$

   若等式成立，說明了 $U_D$ 沒有欺騙行為。

若等式不成立，則公開 $U_D$ 的欺騙行為。

驗證上二式成立之證明：

- **第一式:** $g^{C_i} = K \cdot A_0 \pmod{p}$

  證明: $\because\ s = k + a_0 \pmod{p-1}$

  $\therefore\ C_i = (k + a_0) + n \cdot (p-1)$

  且 $K = g^k \pmod{p-1},\ A_0 = g^{a_0} \pmod{p-1}$

  $\therefore\ g^{C_i} = g^{(k + a_0)+n\cdot(p-1)} = g^k \cdot g^{a_0} \cdot g^{n\cdot(p-1)} = K \cdot A_0 \cdot (g^{p-1})^n$

  $= K \cdot A_0 \pmod{p}$

- **第二式:** $g^{B_i} = \prod_{j=1}^{t} {A_{j-1}}^{{\delta_i}^{j-1}} \pmod{p}$

  證明: $B_i = f(\delta_i) \pmod{p}$

  $A_i = g^{a_i} \pmod{p}$

  把 $\delta_i$ 代入 $f(x) = a_0 + a_1x + a_2x^2 + a_3x^3 + \cdots + a_{t-1}x^{t-1} \pmod{p-1}$

  得到

  $f(\delta_i) = (a_0 + a_1\delta_i + a_2{\delta_i}^2 + a_3{\delta_i}^3 + \cdots + a_{t-1}{\delta_i}^{t-1}) + n \cdot (p-1)$

  $\therefore\ g^{B_i} = g^{f(\delta_i)} = g^{(a_0+a_1\delta_i+a_2{\delta_i}^2+a_3{\delta_i}^3+\cdots+a_{t-1}{\delta_i}^{t-1})+n\cdot(p-1)}$

  $= g^{(a_0+a_1\delta_i+a_2{\delta_i}^2+a_3{\delta_i}^3+\cdots+a_{t-1}{\delta_i}^{t-1})} \cdot (g^{p-1})^n$

  $= g^{(a_0+a_1\delta_i+a_2{\delta_i}^2+a_3{\delta_i}^3+\cdots+a_{t-1}{\delta_i}^{t-1})} \pmod{p}$

  $= g^{a_0} \cdot g^{a_1\delta_i} \cdot g^{a_2{\delta_i}^2} \cdot \cdots \cdot g^{a_{t-1}{\delta_i}^{t-1}}$

  $= (g^{a_0}) \cdot (g^{a_1})^{\delta_i} \cdot (g^{a_2})^{{\delta_i}^2} \cdot \cdots \cdot (g^{a_{t-1}})^{{\delta_i}^{t-1}}$

$$= A_0 \cdot {A_1}^{\delta_i} \cdot {A_2}^{{\delta_i}^2} \cdot \cdots \cdot {A_{t-1}}^{{\delta_i}^{t-1}}$$
$$= \prod_{j=1}^{t} {A_{j-1}}^{{\delta_i}^{j-1}} (\text{mod } p)$$

- 還原秘密:

假設有 $t$ 位說是 $U_1$ , $U_2$ , ... , $U_t$ 共同還原秘密。每個參與的成員 $U_i$ 將 $b_i$ 加密後傳送給合成者， 再由合成者將其秘密還原。

1. 已知合成者 $U_A$ 的 $\alpha_A$ 以及 $\beta_A$ , $U_i$ 將其手上的 $b_i$ 作運算得 $e_{1i} = x_i\alpha_A$以及 $e_{2i} = b_i + x_i\beta_A$,將 $(e_{1i}, e_{2i})$ 傳給 $U_A$ 。

2. 合成者 $U_A$ 得到一組 $(e_{1i}, e_{2i})$, $i = 1$ , $\cdots$ , $t$
   $U_A$ 利用自己的私鑰 $x_A$ 解出 $e_{2i} - x_A\ e_{1i}$, $i = 1, \cdots, t$,
   再回復其原值 $T_i$ 。

3. $U_A$ 首先驗證

$$g^{T_i} = \prod_{j=1}^{t} {A_{j-1}}^{{\delta_i}^{j-1}} (\text{mod } p),\ i = 1 , \cdots , t$$

   是否成立。若成立，說明分享者 $U_i$ 沒有欺騙行為；
   若不成立，則要求其重新發送自己手中的資訊。

4. 當 $U_A$ 獲得一組數據 ( $\delta_i$ , $T_i$), $i = 1$ , $\cdots$ , $t$,
   由 Lagrange 內插多項式求出 $L(T)$ ,並算出其常數項 $L(0)$ $(\text{mod } p-1)$, 將 $L(0)$ 表示為$E_p(a, b)$上的一點 $R$ ,

$U_A$ 再計算 $m_{1i} = x_A\alpha_i$以及 $m_{2i} = R+x_A\beta_i$, $i = 1, \cdots, t$ 並將 $(m_{1i}, m_{2i})$ 傳送給參與秘密還原的分享者 $U_i$ $(i = 1, 2, \cdots, t)$。

5. 分享者 $U_i$ 利用私鑰 $x_i$ 解出 $n_i = m_{2i} - x_i\, m_{1i}\,, i = 1, \cdots, t$ 再將 $n_i$ 回復其原值 $N_i$ ,( 此 $n_i$ 就是 $R$ ,因而 $N_i$ 就是 $L(0)$ ),

   分享者驗證 $A_0 = g^{N_i} \pmod p$ 是否成立，

   如果成立，則說明 $U_A$ 沒有欺騙行為，

   如果不成立，則要求 $U_A$ 重新發送計算之結果。

   最後，分享者計算 $k = C_i - N_i \pmod{p-1}$ 。

# 4 電子投票系統

## 4.1 傳統投票系統

以我國長久以來的投票系統做一個簡單的簡介。早在1950年，台灣當局舉辦 基層的競爭性選舉，而這些選舉當中常有一些選舉不公的爭議，我們就先從選舉的準備工作談起[11]。

1. 準備工作：

   - 候選人參選登記，並審查是否合乎資格成為候選人。
   - 印製候選人名冊供選舉人參考。
   - 統計合格選民人數並印製選票。(以一張選票5元作計算，根據中選會在上屆總統大選所統計的合 格選民16750867人，光是選票就要花上至少8千萬以上，這還不包括護送選票至各大投票所及保護 選票所需要的花費。)

2. 投票：

   在各大投票所派駐選務工作員及警察協助維護秩序及治安的工作。(在建制20人左右的投票所所需要的人事 費用至少要花台幣8萬左右，這當中當然也包括茶水及伙食費。)

3. 計票：

   選舉結束後的計票工作，以人為唱票的方式計票，若其中有選務人員不中立或因人為因素上的疏失容易造成選舉 不公而

引起社會上的對立。在各投票所計票完成後，統計回傳至選務中心。 (以上屆總統大選為例，產生了33萬多張的廢票引發落選者的質疑，造成台灣社會嚴重的對立。)

4. 公告：

   在投票所統計完成後回傳至選務中心做統整、計算，在透過各大媒體公告投票結果及當選人。 (在整個計票當中相當耗費人力、金錢與耗時以及不容易做監督的缺點，而選舉結果後也常常造成落選者的質疑，以為有舞弊的情形發生 而造成社會上的動盪，以至於對於中選會的中立產生質疑。)

以在*90*年代中期，雲林縣花費為例：

- 選村(里)長需要花費 50 至 100 萬元(新台幣)。
- 選鄉鎮(市)民意代表需要 100 至 200 萬元。
- 選鄉鎮(市)長需要 1,000 至 2,000 萬元。
- 選縣議員需要 3,000 至 8,000 萬元。
- 選立法委員需要 5,000萬到 1 億 2 千萬。
- 選縣長需要 1 億 5,000 萬。

  而台中市的選舉成本一般比上述的花費還要高出 500 至 2,000 萬不等。

## 4.2 如何改進

種種以上一些比較大的缺失作探討，傳統的選務工作需要花費龐大的人力、金錢及珍貴的地球資源，在環保意識抬頭 的今天，這樣似乎是個落後的作法，而且人為上的疏失也似乎不可避免，原因是這麼龐大的選舉工作光靠中選會跟警察單位 的力量想要掌握全國各大投票所似乎不是一件容易的事，有鑑於此此篇論文在提倡電子投票的好處。

然而在網路如此發達的社會建構一個可供合法選民投票而不造成網路塞車的電子投票系統也非難事，這樣既可避免 掉資源的浪費也可在自家的電腦(若家中沒電腦著可藉由鄉鎮市公所提供或是學校單位提供投票場所)登入選票中心投票。首先，中選會可 把選務的工作(含計票、公告)集中在中選會，這樣可避免過多不易管理的投票所。在選前，合乎資格的選民登入中選會註冊成合法選 民，在投票日當天以註冊完成之數位身份投票，事後選票還可儲存在一個小硬碟中保存供日後驗票使用，比起龐大的選票容易管理。在由 全國具威望的人士及檢察官、法官等人組成監票中心避免造成舞弊，這樣也可省去運送選票發生的意外及人力上的浪費，也可讓警力放 在更需要的地方。二來還可省去計票所需要花費的時間，以避免冗長的計票方式。諸多好處在這篇論文中可能有所缺漏，也歡迎各大家 能給予批評指教。

## 4.3 建構電子投票系統

此電子投票系統[2, 5, 9, 10] 是由四個部份所組成。分別為系統管理者(包含選舉人名單)、 監票中心、佈告欄管理者，這三大部份。

1. 準備

   (a) 系統管理者首先選取一個質數 $p$ 及一個小於 $p$ 的數 $g \in Z_p^*$ ,其週期為 $q$ ;並選取橢圓曲線 $E \pmod p$ 再選取RSA公鑰 $(n_1, e_1)$ ,其中 $n_1$ 為質數 $p_1, q_1$ 之乘積，並算出在模 $\phi(n_1)$ 下 $e_1$ 之乘法反元素 $d_1$ 。
   將 $(p, q, g, n_1, e_1, E \pmod p)$ 公開。

   (b) 候選人抽籤決定其號碼為 $c_1, c_2, \cdots, c_n$ ,並公告之。

   (c) 佈告欄管理者選取數位ID為Ta, 同時隨機選取私密鑰匙 $x_{\mathrm{Ta}}$ 及橢圓曲線 $E \pmod p$ 上的一點 $\alpha_{\mathrm{Ta}}$ 並算出 $\beta_{\mathrm{Ta}} = x_{\mathrm{Ta}}\alpha_{\mathrm{Ta}}$ , 將 Ta, $\alpha_{\mathrm{Ta}}, \beta_{\mathrm{Ta}}$ 公開。

   (d) 監票中心取數位ID為Ad, 同時隨機選取私密鑰匙 $x_{\mathrm{Ad}}$ 及橢圓曲線 $E \pmod p$ 上的一點 $\alpha_{\mathrm{Ad}}$ 並算出 $\beta_{\mathrm{Ad}} = x_{\mathrm{Ad}}\alpha_{\mathrm{Ad}}$ , 將 Ad, $\alpha_{\mathrm{Ad}}, \beta_{\mathrm{Ad}}$ 公開。

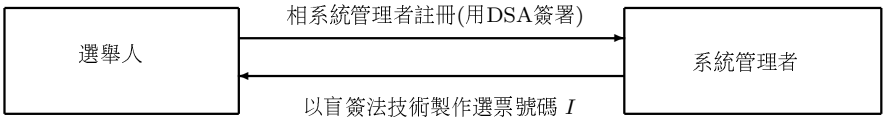


圖 4-1 選舉人註冊流程圖

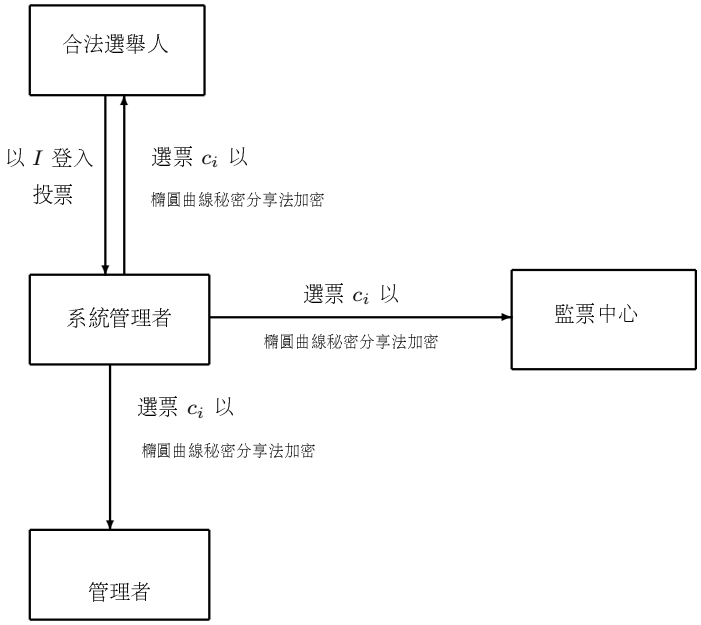


圖 4-2 投票步驟

2. 註冊

選舉人在投票之前先向系統管理者註冊成合法選舉人，其步驟如下：

(a) 選舉人首先隨機選取一個介於1和 $q-1$ 整數 $a$ 當作自己的私密鑰匙。

(b) 然後計算 $y = g^a (\mathrm{mod}\ p)$ 並公佈 $y$ 。

(c) 接著選舉人隨機選取整數 $k$ ( $0 < k < q$ )將其數位身份 $m$ 簽署為 $(\delta, \gamma)$, 其中

$$\gamma = (g^k \mathrm{mod}\ p)(\mathrm{mod}\ q),$$

$$\delta = (\mathrm{MD5}(m) + a \cdot \gamma)k^{-1} (\mathrm{mod}\ p).$$

(當 $\delta = 0$ ,選舉人必須重新選取 $k$ )

(d) 然後選舉人以 $(m, \gamma, \delta)$ ,登入系統。

(e) 系統管理者計算 $w, e_1, e_2$ ,其中

$$w = \delta^{-1} (\mathrm{mod}\ p),$$

$$e_1 = \mathrm{MD5}(m) \cdot w (\mathrm{mod}\ p),$$

$$e_2 = \gamma \cdot w (\mathrm{mod}\ p).$$

然後驗證 $(g^{e_1} y^{e_2} \mathrm{mod}\ p)(\mathrm{mod}\ q)$ 是否等於 $\gamma \pmod{p}$ 。若是 ，則接受其合法性，也就是選舉人已經完成註冊的手續。

3. 投票

(a) 已經註冊的合法選民隨機選取一與 $n_1$ 互質之整數 $r$ ,再計算 $x = r^{e_1}\delta \pmod{n_1}$ 並用 $x$ 登入系統取得選票號碼 $I$ , 此 $I$ 就是系統管理者對 $x$ 的簽署，亦即 $I = x^{d_1} = (r^{e_1}\delta)^{d_1} \pmod{n_1}$ 。

(b) 接著驗證 $I$ 是否為 $\delta$ 的簽署如下: 先算出 $I' = r^{-1}I \pmod{n_1}$ , 再算 $I'^{e_1} \pmod{n_1}$ 看看此數是否就是 $\delta$ 。

(c) 選舉人首先選取三個整數 $a_0, a_1, a_2$ 形成多項式 $f(x) = a_0 + a_1x + a_2x^2 (\mathrm{mod}\ p)$ , 再隨機選取私密鑰匙 $x$ 及橢圓曲線 $E \pmod{p}$ 上的一點 $\alpha$ ,接著圈選候選人 $c_i$ 並計算 $f(I), f(\mathrm{Ad}), f(\mathrm{Ta}), s, \beta$ 以及 $A_0, A_1, A_2$ , 其中

$$\beta = x\alpha$$

$$s = c_i + a_0 \pmod{p}$$

$$A_j = g^{a_j} \pmod{p}, j = 0, 1, 2$$

並將 $s, A_0, A_1, A_2, \alpha, \beta$ 公開，同時將 $f(I), f(\mathrm{Ad}), f(\mathrm{Ta})$ 傳送給系統管理者。

(d) 系統管理者將 $f(I), f(\mathrm{Ad}), \mathrm{f(Ta)}, \mathrm{s}$ 分別轉換成 $E \pmod{p}$ 上的點 ， $P, P_{\mathrm{Ad}}, P_{\mathrm{Ta}}, P_s$ 。 系統管理者隨機選取一整數 $r_1$ ，並計算 $R = g^{r_1} (\mathrm{mod}\ p-1)$

$z_1 = r_1\alpha,\ z_2 = P + r_1\beta,\ z_3 = P_s + r_1\beta$

$z_{1\mathrm{Ad}} = r_1\alpha_{\mathrm{Ad}},\ z_{2\mathrm{Ad}} = P_{\mathrm{Ad}} + r_1\beta_{\mathrm{Ad}},\ z_{3\mathrm{Ad}} = P_s + r_1\beta_{\mathrm{Ad}}$

$z_{1\mathrm{Ta}} = r_1\alpha_{\mathrm{Ta}},\ z_{2\mathrm{Ta}} = P_{\mathrm{Ta}} + r_1\beta_{\mathrm{Ta}},\ z_{3\mathrm{Ta}} = P_s + r_1\beta_{\mathrm{Ta}}$

公佈 $g, K, (z_1, z_2, z_3), I, A_j$ 再分別傳送給選舉人、佈告欄管理者及監票中心。

(e) 驗證

選舉人與佈告欄管理者及監票中心可驗證系統管理者所傳之資料是否有欺騙之行為。如選舉人驗證的步驟如下：

- 計算

$$b = z_2 - xz_1, c = z_3 - xz_1$$

$$R^x = D, B = b - D, C = c - D$$

- 驗證此簽署的是否成立，計算下列各式:

$g^C = K \cdot A_0 \pmod p$,

$g^B = \prod_{j=1}^{t} {A_{j-1}}^{I^{j-1}} \pmod p$

佈告欄管理者、監票中心及系統管理者之驗證方法類似，故省略之。

(f) 由佈告欄管理者結合監票中心及選舉人手上的資料，其步驟如下：

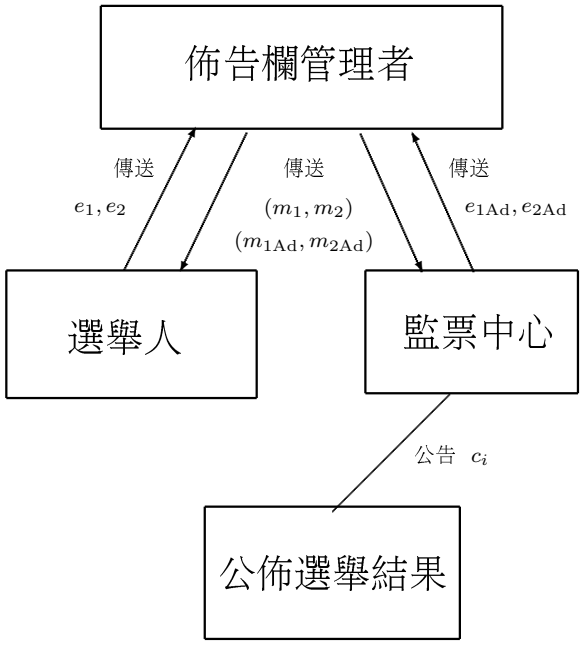


圖 4-3 祕密分享

- 選舉人算出 $e_1 = x\alpha_{\mathrm{Ta}}, e_2 = b + x\beta_{\mathrm{Ta}}$ 並傳送 $e_1, e_2$ 給佈告欄管理者。
- 監票中心算出 $e_{1\mathrm{Ad}} = x_{\mathrm{Ad}}\alpha_{\mathrm{Ta}}$, $e_{2\mathrm{Ad}} = b_{\mathrm{Ad}} + x_{\mathrm{Ta}}\beta_{\mathrm{Ta}}$ 並傳送 $e_{1\mathrm{Ad}}, e_{2\mathrm{Ad}}$ 給佈告欄管理者。
- 佈告欄管理者得到 $(e_1, e_2)$, $(e_{1\mathrm{Ad}}, e_{2\mathrm{Ad}})$使用自己的私鑰 $x_{\mathrm{Ta}}$ 解出 $b = e_2 - x_{\mathrm{Ta}}e_1, b_{\mathrm{Ad}} = e_{2\mathrm{Ad}} - x_{\mathrm{Ta}}e_{1\mathrm{Ad}}$ ,找回 $b, b_{\mathrm{Ad}}$ 原值 $T = f(I)$, $T_{\mathrm{Ta}} = f(\mathrm{Ta})$ 。
- 接著佈告欄管理者計算下列各式是否成立：

$$g^T = \prod_{j=1}^{t} {A_{j-1}}^{I^{j-1}} \pmod p,$$

$$g^{T_{\mathrm{Ta}}} = \prod_{j=1}^{t} {A_{j-1}}^{\mathrm{Ta}^{j-1}} \pmod p.$$

- 佈告欄管理者用 Lagrange 內插多項式找出 $L(x)$ 及 $L(0) \pmod p$ , 並將 $L(0)$ 表示成橢圓曲線 $E \pmod p$ 上的一個點 $R$ , 接著計算

$$m_1 = x_{\mathrm{Ta}}\alpha,\ m_2 = R + x_{\mathrm{Ta}}\beta$$

$$m_{1\mathrm{Ad}} = x_{\mathrm{Ta}}\alpha_{Ad},\ m_{2\mathrm{Ad}} = R + x_{\mathrm{Ta}}\beta_{\mathrm{Ad}}$$

在將計算結果 $(m_1,\ m_2)$, $(m_{1\mathrm{Ad}},\ m_{2\mathrm{Ad}})$ 傳送給選舉人與監票中心。

(g) 合法選舉人得到 $(m_1,\ m_2)$ 後，以自己的私鑰 $x$ 計算 $n = m_2 - xm_1$ 並恢復 $n$ 的原值 $N = L(0)$ , 合法選舉人驗證 $A_0 = g^N \pmod p$ 是否成立，如果成立，則說明佈告欄管理者沒有欺騙行為。

(h) 監票中心得到 $(m_{1\mathrm{Ad}},\ m_{2\mathrm{Ad}})$ 後，以自己的私鑰 $x_{\mathrm{Ad}}$ 計算 $n_{\mathrm{Ad}} = m_{2\mathrm{Ad}} - x_{\mathrm{Ad}}m_{1\mathrm{Ad}}$ 並恢復 $n_{\mathrm{Ad}}$ 的原值 $N_{\mathrm{Ad}} = L(0)$ , 合法選舉人驗證 $A_0 = g^{N_{\mathrm{Ad}}} \pmod p$ 是否成立，如果成立，則說明佈告欄管理者沒有欺騙行為。

(i) 最後監票中心計算 $c_i = s - N \pmod{p-1}$ , 並將 $c_i$ 公告，同時監票中心還可 檢驗合法票數是否有大於選舉人數，最後，公佈選舉結果。

## 4.4 結論

雖然此篇電子投票系統的投票過程略顯複雜及繁瑣，但這也是一件事情有利有弊的地方。然而 相較於過去傳統的投票系統，對於環保、節省資源、公正、公開性以及保密性上卻有相對的提升。我們可以花小錢 做到公正、公開及中立的選舉系統，並且可以做到有效率及更容易掌握的電子投票系統，在此還有許多地方可能有所缺漏 ，也希望大家能多多批評指教。

# 參 考 文 獻


[1] Chaum, D.: "Blind Signatures System" ,Advances in Cryptology Proceedings of Crypto 83, Pienum, p.153.

[2] Jan, J.K,/Tai, C.C.: "A Secure Electronic Voting Protocol with IC Cards, Journal of Systems and Software", U.S.A. Vol.39 Dec. 1997.

[3] Koblitz, N.: "Elliptic curve cryptosystems". *Mathematics of Computation*, 48(177) 203-209, 1987.

[4] Lin, Yih.: "The Design of Protocol for e-Voting on the Internet" ,2001.

[5] 林靜慧: 橢圓曲線版的動態秘密分享系統，私立東海大學，碩士論文，2006.

[6] Rivest, R.: "The MD5 Message Digest Algorithm", RFC 1321, MIT and RSA Data Security, Inc., April 1992.

[7] SHamir, Adi.: "How to share a secret", Communications of the ACM, Vo1.22,No.11,1979.

[8] 沈淵源： 密碼學之旅與MATHEMATICA同行全華科技圖書股份有限公司, 2006

[9] Yong-Sork HER,/Kouichi SAKURAI.: "Design of E-voting System with an Absentee voter Based on Cryptographic Techniques" Japan 2004

[10] http://www.votehere.com

[11] 中選會http://www.cec.gov.tw/