東海大學應用數學系

碩士論文

指導教授：沈淵源 博士

電子彩券系統之研究

A Study of E-lottery System

研 究 生：李永霖

中華民國一百零一年十一月二十七日

摘 要

本文使用 RSA 演算法和數位簽章的技術提出具有匿名性且兼具安全性的彩券系統，且結合智慧卡高安全性和方便攜帶之特性，提供與銀行單位做認證功能，目的是為了此系統在各階段具有安全性，保障購買者、彩券服務商、銀行等在各階段中的相關資料。

關鍵詞：RSA 演算法、數位簽章、智慧卡。

誌 謝

首先要感謝我的指導教授沈淵源教授，在這兩年來對於我論文諄諄的指導與教誨，才使得此本論文得以完成。其次，要感謝在百忙之中前來參加我論文的口試委員，東海數學系曹景懿教授及彰師大數學系劉康滿教授，謝謝他們所提供的建設性見解。同時也要感謝數研所的同學們，對我的支持與鼓勵，並給予我寶貴的意見和指教，使我獲益良多。在校的這段期間，老師和同學們的扶持都將是我永難忘懷的回憶。最後，要感謝我的家人一直在背後默默支持著我，也要感謝大家對我的祝福。

目 錄

第一章 緒論

隨著社會的演化與進步，需求帶給人們的滿足與刺激感，已然成為人們不可或缺的一部分，愈來愈多人夢想著一夜致富，而樂透彩券、刮刮樂它正可以最小的代價，讓大家在做公益的同時，兼具有期待得獎的樂趣，與滿足人們最大的期望及好奇心。正因它有如此大的吸引力，且購買彩券為自願性參與之行為，所以才被大眾所接受。在國內我們稱之為「公益彩券」，是經由國家立法通過，賦予法制的規範，並從販售金額中抽取一定比例的銷售盈餘從事公益用途，因此，彩券正式的被合法化。

一般而言，政府發行公益彩券的最主要原因，是為了抑制及杜絕非法性賭博。由民國 38 年開始發行的「愛國獎券」，民國八十八年由台灣銀行發行的「公益彩券」，直至現今由台北銀行發行「電腦彩券」，其目的都是籌措中央及地方的經費，以帶動經濟景氣，照顧弱勢團體及創造就業機會，同時為政府帶來可觀的收入，充實社會福利的財源，也為社會財富的再分發提供了管道。

國內目前公益彩券的類別又分為「電腦型彩券」(樂透彩)、「立即型彩券」(吉時樂)、「傳統型彩券」(對對樂)，而購買彩券的方式，必須到彩券服務商(彩券投注站)購買紙張彩券居多，藉彩券上的號碼作為中獎的根據，所以彩券的保存儼然成為一大

問題。本文提出對電腦彩券具匿名及安全性之系統，且結合智慧卡之應用及密碼學技術，提供與銀行單位做認證功能，目的是為了此系統在各階段具有安全性，保障購買者、彩券服務商、銀行等在各階段中的相關資料。

第二章 預備知識

2.1 密碼系統

所謂的密碼系統是由明文、密文、鑰匙、加密法則和解密法則組合而成。明文為加密前的原始資料，密文為加密後的資料，而加密法則是利用鑰匙對明文進行加密的編碼動作的演算法，而解密法則是利用鑰匙對密文進行解密還原成明文的演算法。密碼系統又可分為對稱性密碼學(傳統加密系統)和非對稱性密碼學或公開鑰匙加密系統。

2.1.1 對稱性密碼學

此類型的加解密鑰匙是對稱的，首先發送方利用鑰匙進行加密，而接收方則利用鑰匙進行解密，其中解密鑰匙與加密鑰匙可能是相同，或解密鑰匙可輕易由加密鑰匙推導而出，所以此系統的鑰匙管理是一大問題。但其速度比非對稱性系統快速，常應用於資料加密，可確保資料的隱密性、來源性及完整性。常見之演算法有 DES、Triple-DES、AES、RC2/RC4/RC5 等。本研究未著重對稱性系統之演算法，故在此不多加討論。

圖 2-1 為對稱性密碼系統的示意圖，明文訊息經過加密函數處理後變成密文，而解密者將收到的密文經過解密函數處理還原

成原來的明文訊息，其中加密與解密所使用的是相同的鑰匙[1]。

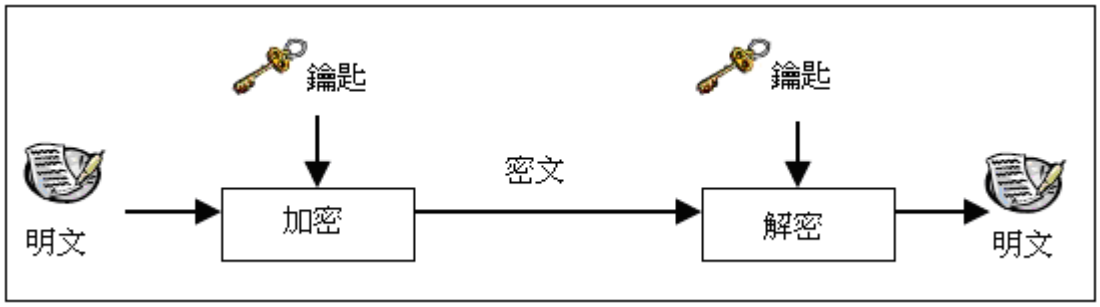


圖 2-1 對稱性密碼系統的示意圖

2.1.2 非對稱性密碼學

非對稱性密碼系統(Asymmetric Cryptosystem)又稱為公鑰密碼系統。加密鑰匙可以被公開，而解密鑰匙必須隱密的加以保存，只有該鑰匙的擁有者才知道其內容，因此在有效時間內，想由加密鑰匙推導出解密鑰匙是不可行的。此系統速度較慢、適合少量資料處理，大多用來傳送對稱演算法所需的密鑰或進行數位簽章。另外，在進行加密、解密之前，雙方都要先向一個公正的認證中心(Certificate Authority，CA)申請數位憑證，該憑證內記載了使用者的身分資訊以及該使用者的公鑰，由於憑證係由公信第三者所簽發，使用者從公開地方拿到憑證時，只要查驗憑證內容確實是由CA所簽發，即可確信憑證內的公鑰確實是憑證內使用者名稱所指之人所有，如圖2-2所示[10]。目前較有名的演算法有RSA等，其為本研究討論的重點。

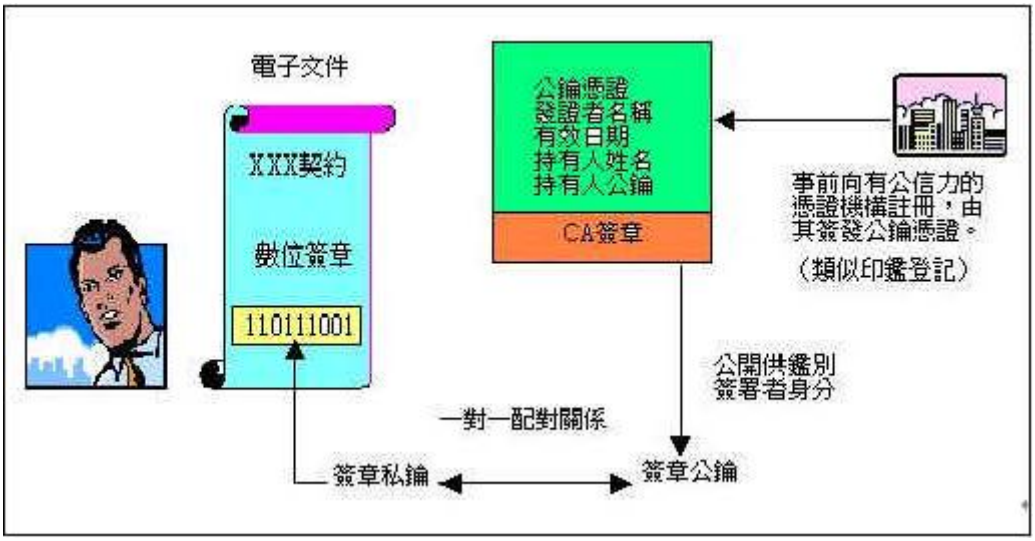


圖 2-2 身分辨識圖

圖 2-3 為非對稱性密碼系統的示意圖，首先發送者利用接收者的公鑰對文件訊息進行加密動作，使之成為密文，再將密文傳送給接收者。接收者使用只有本人知道的解密鑰匙進行解密，如此可將密文還原成明文[1]。

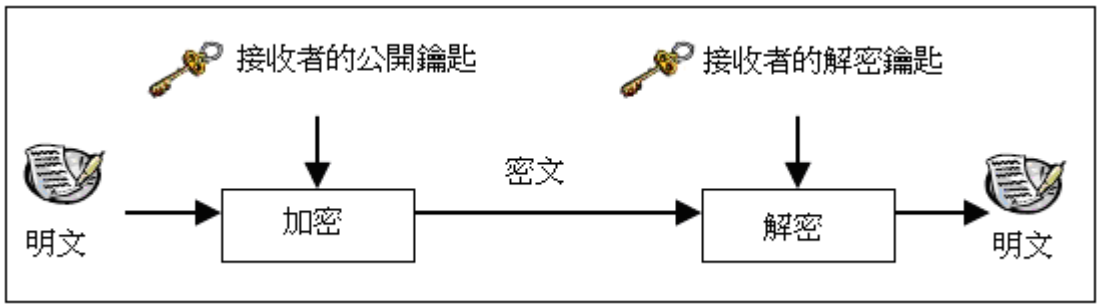


圖 2-3 非對稱性密碼系統的示意圖

2.2 RSA 演算法

RSA 演算法於 1977 年 5 月由 MIT 之 Rivest、Shamir 及 Adleman 三位學者所提出，是目前最為廣泛使用的公鑰密碼技術。RSA 演算法可作為加解密、數位簽章等作用，其安全性是建立於因數分解的困難度，而因數分解問題是指給定一合成數 n 為兩個大質數 p 與 q 的乘積，欲分解 n 為計算上不可行。以下我們將針對鑰匙產生、加解密步驟等方面說明。

張三欲將明文 M 加密成密文 C 傳給李四，李四則將密文 C 解密為明文 M 。

1、鑰匙產生

(i)李四選取 2 個相異大質數 p 和 q ，並將二數相乘計算 $n = p \cdot q$。

(ii)李四計算 $\phi(n) = (p-1)\cdot(q-1)$，並選取一個加密次冪 e，使得 $\gcd(e,\phi(n)) = 1$。

(iii)李四將加密鑰匙 (n,e) 公開。

2、加密步驟

張三將明文 M 加密為密文 $C \equiv M^e \pmod{n}$，並將密文 C 傳給李四。

3、解密步驟

（i）李四算出e在$\bmod \phi(n)$下的乘法反元素d（此為解密鑰匙）。

（ii）最後李四將密文C取d次冪，即可還原成明文M，即

$M \equiv C^d \pmod{n}$。

$< pf > C^d \equiv (M^e)^d \equiv M^{ed} \pmod{n}$

$\because ed \equiv 1 \pmod{\phi(n)} \ \therefore ed = 1 + k\phi(n), k \in Z$

則 $C^d \equiv M^{ed} \equiv M^{1+k\phi(n)} \equiv M \cdot (M^{\phi(n)})^k \pmod{n}$

根據歐拉定理，M與n互質，則$M^{\phi(n)} \equiv 1 \pmod{n}$

因此，$C^d \equiv M \pmod{n}$

例題：

1、鑰匙產生

（i）李四選取$p = 47$，$q = 71$，且算出$n = p \cdot q = 47 \cdot 71 = 3337$。

（ii）李四計算$\phi(n) = (p-1) \cdot (q-1) = (47-1) \cdot (71-1) = 3220$。

並選取$e \in Z^+$，且$\gcd(e, 3220) = 1$，$1 < e < 3220$，

$3220 = 2 \times 2 \times 5 \times 7 \times 23$ 須選擇不含因數 2、5、7、23 的數，

故選$e = 79$。

（iii）李四將加密鑰匙$(3337, 79)$公開。

2、加密步驟

張三將明文$M=668$加密為密文，然後將密文C傳給李四，即計算$C\equiv M^{e}\equiv 668^{79}(\mathrm{mod}\,3337)\equiv 1570\,(\mathrm{mod}\,3337)$。

3、解密步驟

(i)李四計算e的乘法反元素d，滿足$e\cdot d\equiv 1(\mathrm{mod}\,3220)$，即計算$79\cdot d\equiv 1(\mathrm{mod}\,3220)\Rightarrow 80501=79\times 1019\equiv 1(\mathrm{mod}\,3220)$。因此，$d=1019$為解密鑰匙。

(ii)李四計算$M\equiv C^{d}(\mathrm{mod}\,n)\equiv 1570^{1019}(\mathrm{mod}\,3337)\equiv 668$，即可得到明文。

2.2.1 RSA 數位簽章法

張三有一份文件M，李四同意在文件M上簽章。若李四的RSA 公開鑰匙為(n,e)，解密鑰匙為d，則以下我們將針對簽署、驗證和安全度分析等方面說明。

1、簽署

李四將文件M簽名為$s\equiv M^{d}\ (\mathrm{mod}\,n)$

2、驗證

張三得到李四回傳的s，並利用李四的公開鑰匙(n,e)，計算$t\equiv s^{e}\ (\mathrm{mod}\,n)$。比較$t$與$M$之值，若兩值相同，即為合法簽章。

3、安全度分析

RSA 的安全度建立於分解大合成數n的困難度。A.Lenstra(1994)已可成功分解出 RSA 129 位數。據學術界評估，目前應可有效地分解出 RSA 135 位數(約 400 位元)。因此，為確保至少五年內之安全度需求，建議 RSA 的鑰匙長度(即模數n的大小)要達到 1024 位元以上才算達到安全[11]。

2.3 單向雜湊函數

單向雜湊函數又可稱為單向赫序函數，通常用符號$h()$來表示，對於任何長度之明文M，經由雜湊函數$h()$可得一個固定長度的輸出資料$h(M)$，通常運用在明文鑑別或數位簽章方面，目前較知名的單向雜湊函數有 MD4、MD5，以及 SHA、SHA-1 等。而單向雜湊函數具有下列特性[5]：

1、單向性（one-way）

對任意長度的明文M，經過$h()$計算後，可以很容易計算出固定長度的雜湊值$h(M)$。相反的，若想藉由所給定的$h(M)$逆推出明文M，在有限資源內是不可行的。

2、抗碰撞性（collision-free）

抗碰撞性又稱為強勢免於碰撞，對任意兩個不同的明文M_1與M_2，在有限資源內不會得到相同雜湊函數值，即$h(M_1) \neq h(M_2)$。

2.3.1 MD5 演算法

MD5 是目前最為廣泛使用的一種單向雜湊函數演算法，它是由 MD2、MD3、MD4 演算法所改進而來，英文全名為「Message-Digest Algorithm 5」，由 Ron Rivest 所研發出來的。

它是一個 128 位元的雜湊函數，其處理流程如圖 2-4 所示[6]。運算時，輸入的原文會先被附加一些位元(padding bits)。再由其規則將訊息長度調整為 512 的整數倍，最後就可分割成好幾個 512 位元的區段($Y_0, Y_1, \cdots Y_q \cdots Y_{L-1}$)，再分別由四個壓縮函數(HMD5)處理。簡單的說，它的原理是將任意長度的數字，經由多次運算和調整長度，最後計算出一個 128 位元的結果。而其表示方法通常為一串 32 個字元的十六進位字串。

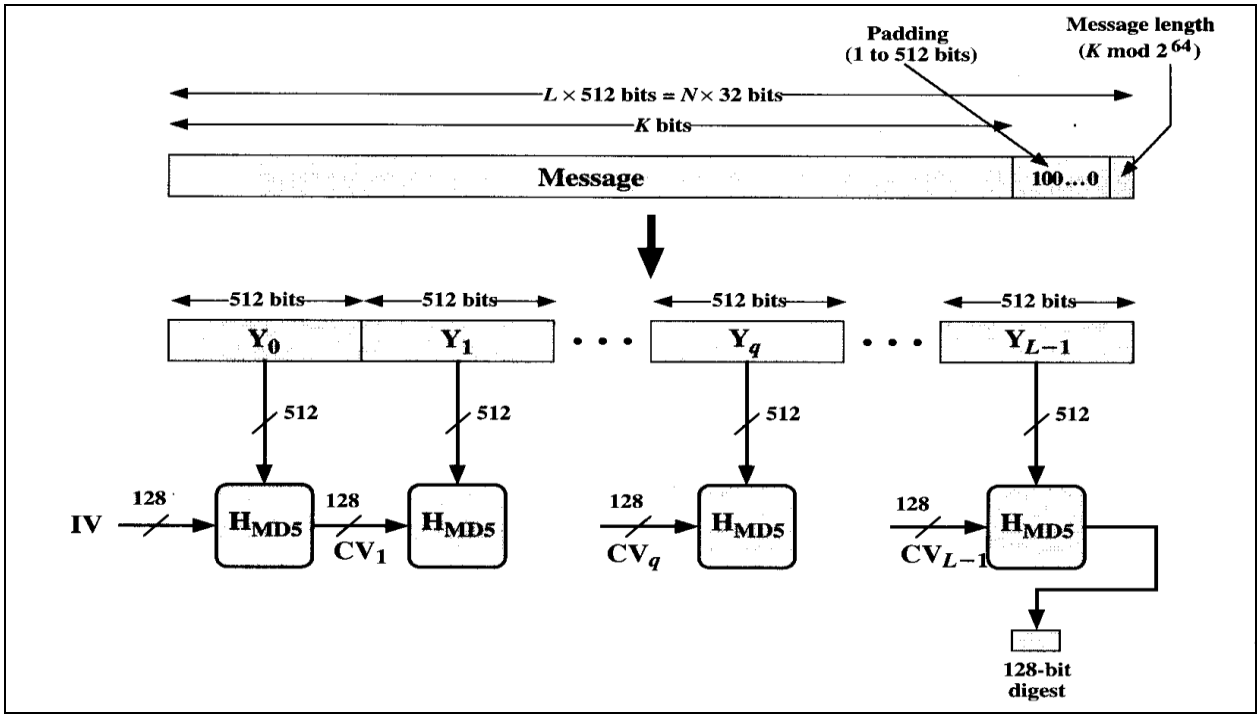


圖 2-4 MD5 運算處理流程

MD5 演算法具有以下特點：

1、固定的字串內容必定會得出一個固定的鍵值。

2、這是一個單向的雜湊演算，意味著，無法從鍵值反推算出原本的字串內容。

3、不同字串內容所演算出來的鍵值，雖有可能相同，但根據統計，重覆的機率小於百萬分之一，以重覆率來說，是相當好的演算法。

4、演算速度快，對硬體的要求很低。

5、它可演算任意長度的字串內容，而且能得出固定長度的鍵值。

6、若字串內容只相差一個字，它也能算出完全不同的鍵值。

7、鍵值長達 128 位元，而且可接受任何長度的字串，就密碼的安全性來說，比過去常用的 DES 還要好。DES 只能接受 8 個字元長度的字串，產生的鍵值只有 56 位元。

2.4 智慧卡

所謂的智慧卡又稱晶片卡或是 IC 卡，簡單地說就是在塑膠卡片內嵌入包括微處理器(MCU)及記憶體在內的 IC 晶片，使得這張卡片除了具有儲存的功能外，還能達到運算及資料處理等強大的功能。近年來因為磁卡的防偽性能不佳，容易被盜錄偽造使

用，使得許多原本採用磁卡的單位不堪損失而慢慢改用智慧卡。國內中華電信之公用電話已改採 IC 卡以取代卡式電話及投幣式電話，全民健康保險卡及規劃中的國民卡也將使用 IC 卡，而 Visa 及 Master 信用卡組織也將以台灣作為 IC 信用卡的試辦地區。相信智慧卡對大眾未來的生活將扮演舉足輕重的地位，尤其當全球電子商務陸續發展以後，智慧卡更將能夠深入日常生活中。

智慧卡具有以下特點：

1、安全性高：由於智慧卡具有防磁及防水的能力，比起一般磁卡更加安全。另外由於內含微處理器，可對資料進行加密及存取控制的功能，是一般磁卡所無法做到的。

2、卡片記憶容量大：一般的磁卡僅能儲存約 72 Byte 大小的資料；而智慧卡隨著應用的不同，可記憶的資料容量也不相同。以中央健康保險局所發行的「健保 IC 卡」為例，其 32K Byte 記憶容量即可儲存約 32000 字元的資料，且資料可重複寫入，可說是相當便利。

3、具運算能力：由於內含微處理器，隨著植入的程式不同，可做不同程度的資料運算，如：資料加密、雜湊運算或是數位簽章等。

4、可攜性高：智慧卡應用相當廣泛，因為其內可儲存加密演算法與個人私密資訊，使用者只要隨身攜帶此智慧卡，並搭配讀卡機，即可建置多種應用。

第三章 電子彩券之研究

3.1 我國購買彩券機制之流程

1、公佈階段

由主辦單位經各種公開管道，如：媒體、電視、網路、彩券投注站等，發佈彩券的相關訊息，如：彩券規則玩法、開獎日期、頭獎金額、兌獎時間等。一般民眾接獲訊息後，逕自到彩券服務商進行選購。

2、購買階段

購買者以匿名方式自行到彩券服務商選擇欲購買的彩券種類，並使用選號單或口頭方式進行投注，而投注內容包含彩券票號、投注期數等。

3、付款階段

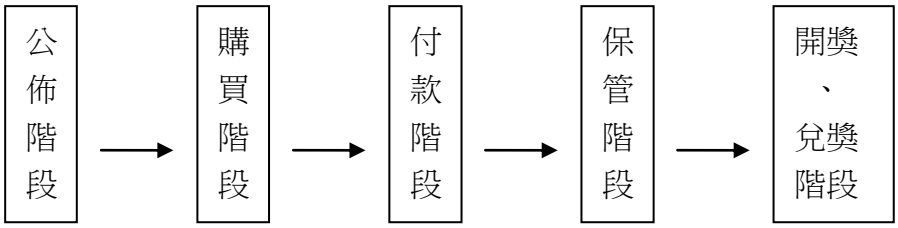
對欲選的彩券種類、彩券票號、投注期數等，進行確認無疑後，須支付相當的金額。

4、保管階段

在支付彩券的購買金額後，由彩券服務商的電腦印出紙張彩券，並交由購買者自行保管，凡彩券遺失、被盜或滅失者，不得掛失止付，中獎號碼的彩券亦同。

5、開獎及兌獎階段

主辦單位在開獎日期當天經由公平、公正、公開的方式公佈開獎號碼，由彩券持有人自行至公開管道核對是否中獎，若為中獎號碼之彩券，中獎人須憑中獎之彩券與本人身分證或其他身分證明文件依規定具領。



我國購買彩券流程圖

3.2 電子彩券系統之成員及設備

本文之彩券系統共分成四種角色，分別為彩券服務商、銀行、購買者及認證中心所組成，且加入了硬體設備：智慧卡。並導入前述預備知識及密碼學系統等作法，使得整個彩券機制具備安全及匿名性。角色及硬體設備說明如下：

1、彩券服務商(Lottery Service Provider)：提供彩券之銷售服務。

2、銀行(Bank)：為可信賴且提供彩券獎金之單位。

3、購買者(Purchaser)：為參與彩券活動的購買人。

4、認證中心(Certification Authority)：表公正客觀身分，查驗憑證申請人身分資料正確性及其與待驗證公開鑰匙間之關連性，並據以簽發電子憑證之單位，及負責統籌彩券發行等相關事宜，如有非法交易發生時，負責追蹤有問題的非法交易案件。

5、智慧卡（Smart Card)：具有計算能力和假設不可輕易被破壞性，且可儲存彩券資料和向銀行兌獎時的身分鑑別。

3.3 電子彩券系統之假設

本研究之彩券機制，須滿足以下的各點假設：

1、每個購買者在購買彩券時必須先申請智慧卡，並利用智慧卡可儲存彩券相關資料和向銀行兌獎時，可驗證其身分。

2、每個購買者、彩券服務商和銀行皆擁有智慧卡讀取設備。

3、其安全性是建立在 RSA 的系統上。

4、購買者、彩券服務商和銀行，都必須遵守本彩券機制，銀行和彩券服務商都是策略聯盟的組織。

5、各成員之間的傳輸皆基於一個安全且穩定的傳輸通道上。

3.4 本研究之彩券流程

本系統分為 4 個階段，分別是準備階段、申請註冊階段、下注付款階段、兌獎階段。流程說明如下：

1、準備階段：認證中心於準備階段公佈彩券規則及角色產生專屬所需要之公鑰及私鑰。

2、申請註冊階段：此階段目的在於欲購買彩券之購買者用真實身分向認證中心申請註冊為合法購買人，並核發智慧卡。

3、下注付款階段：此階段為合法購買人在完成投注後，在彩券上附上專屬的簽章，儲存於智慧卡中，並依投注數目付相當金額款項於彩券服務商。

4、兌獎階段：在認證中心公佈開獎號碼，並同時公佈相關資訊供購買者驗證後，得獎者則可以利用智慧卡提供中獎彩券資訊向銀行單位要求兌領獎金。

3.4.1 符號定義

- CA：表示認證中心。
- LSP：表示彩券服務商。
- B：表示銀行單位。
- P：表示購買者。
- SC：表示智慧卡。
- PIN：與智慧卡認證之 PIN Code。
- L：表示空白彩券。
- L_b：表示已下注之彩券。
- *CardID*：表示智慧卡的晶片唯一序號。
- X：表示認證中心的秘密參數。
- *ID*：表示購買者的唯一身分識別碼。
- *LID*：表示購買者的彩券身份。
- $h()$：表示做單向雜湊函數運算。
- d_P：表示購買者的私鑰。
- (n_P, e_P)：表示購買者之公鑰。
- d_{CA}：表示認證中心的私鑰。
- (n_{CA}, e_{CA})：表示認證中心的公鑰。

3.4.2 第一階段：準備階段

每個購買者、認證中心自行產生專屬的公鑰(n, e)，及秘鑰d，因此(n_p, e_p)為購買者之公鑰，d_p為購買者之私鑰，(n_{CA}, e_{CA})為認證中心之公鑰，d_{CA}為認證中心的私鑰。這些公鑰必須經由認證管道，使角色在需要時就可以取得。

認證中心是負責籌畫彩券之規則和相關事宜，如：開獎號碼、彩金之分配、開始購買與結束之時間、兌獎之開始和結束時間等。

3.4.3 第二階段：申請注冊階段

此階段主要是購買者必須先以真實身分向認證中心申請為合法購買人，將相關資訊存放於智慧卡中，再經由安全且秘密之通道核發給購買者。購買者只需註冊一次，往後購買彩券之交易，可不必再註冊，可減少每次需重新申請和註冊之不便利性。其步驟如下：

1、購買者先將自己的唯一身分識別碼ID利用認證中心的公鑰(n_{CA}, e_{CA})加密，即計算$C = ID^{e_{CA}} (\mathrm{mod}\, n_{CA})$，再傳給認證中心。

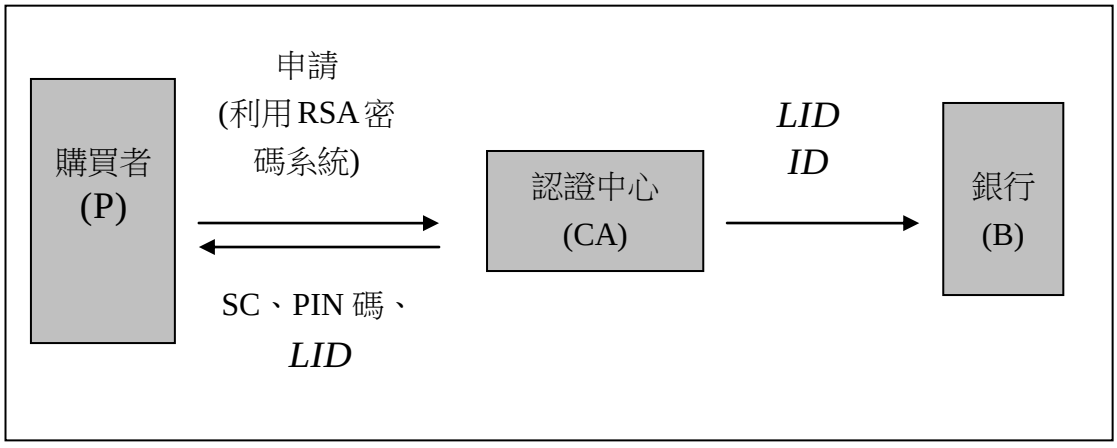
2、認證中心收到購買者註冊之請求與資訊後，會先利用自己的私鑰d_{CA}做解密的動作，即計算$M = C^{d_{CA}} (\mathrm{mod}\, n_{CA})$，將可轉換出購

買者的*ID*。

3、認證中心將購買者的*ID*、智慧卡晶片之唯一序號*CardID*和認證中心的秘密參數*X*做字串相連單向雜湊函數運算，產生：$LID = h(ID \| CardID \| X)$，$\|$ 表示連結符號。並將*LID*和各角色之公鑰，一起存放於智慧卡中，經由安全之秘密通道將智慧卡核發給購買者。而認證中心最後將購買者的*ID*與*LID*儲存於資料庫中。

4、認證中心須將購買者的唯一身分識別碼*ID*和彩券身分*LID*，經由安全之秘密通道傳送給銀行。銀行收到此筆資料後，將之儲存於資料庫中，以待中獎者持智慧卡和身分證件領取獎金時，驗證其身分之用。

5、認證中心將購買者之彩券身分*LID*，和與智慧卡認證之PIN碼，經由安全之秘密通道給購買者。



申請注冊流程圖

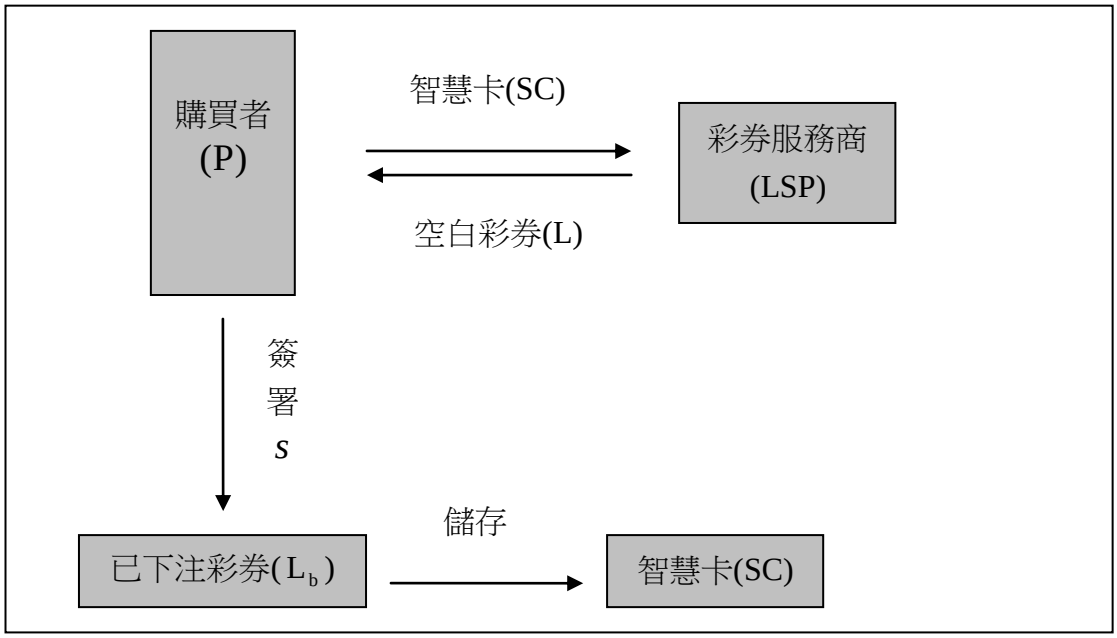
3.4.4 第三階段：下注付款階段

為購買者向彩券服務商下注及付款的流程，步驟如下：

1、 購買者先將智慧卡插入彩券服務商的讀卡機中，輸入 PIN 碼與智慧卡做認證之動作，若是輸入正確將可繼續下個步驟；若是輸入錯誤三次，此智慧卡將被鎖住，必須向認證中心申請解鎖，此部分本機制並不列入討論。

2、 彩券服務商提供空白彩券 L 給購買者，購買者在選擇投注號碼後，利用自己的私鑰 d_P，在已下注之彩券 L_b 上附上購買者之彩券身分 LID 簽署，即計算 $s \equiv LID^{d_P} \pmod{n_P}$，並將此下注彩券 L_b 及相對應之簽署 s 存放於智慧卡中。

3、 最後，購買者對此次購買彩券之交易完成付款動作即可。



下注付款流程圖

3.4.5 第四階段：兌獎階段

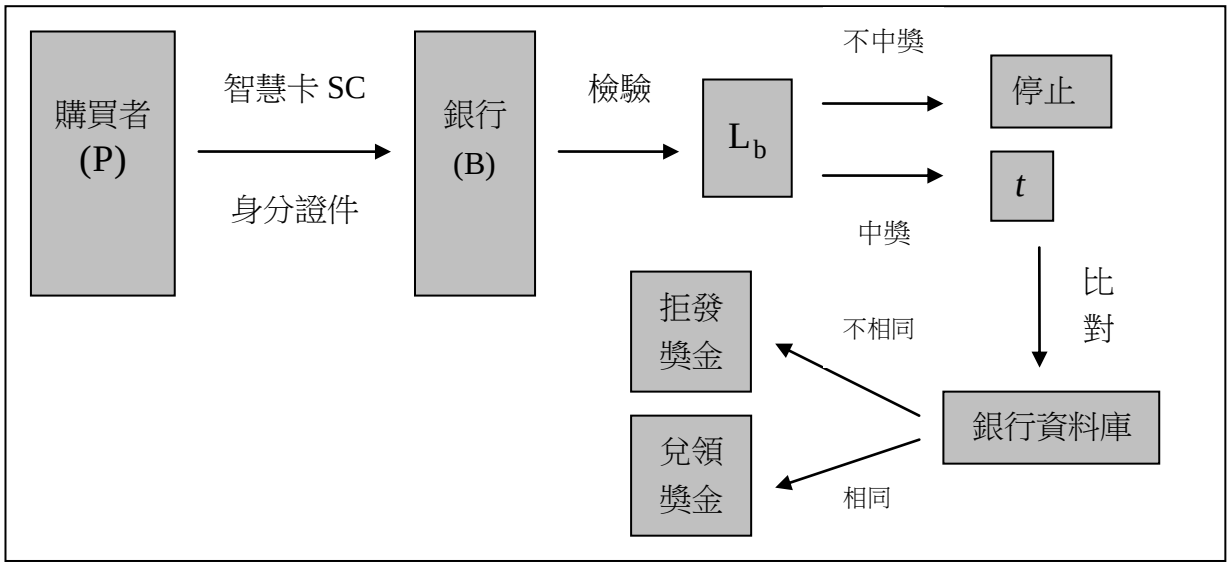
當進入開獎階段時，認證中心會公佈開獎號碼，彩券購買者則自行上網驗證自己是否為中獎人，若是中獎人，則持智慧卡和身分證件自行到銀行單位進行兌領獎金之動作。其步驟如下：

1、購買者先將智慧卡插入銀行的讀卡機中，輸入 PIN 碼與智慧卡做認證之動作，若是輸入正確將可繼續下個步驟；若是輸入錯誤三次，此智慧卡將被鎖住，必須向認證中心申請解鎖，此部分本機制並不列入討論。

2、銀行單位會先檢驗智慧卡內的彩券資訊L_b是否為中獎號碼，若為中獎號碼，則繼續下個步驟；反之，則停止。

3、此時，銀行單位利用購買者的公鑰(n_P, e_P)對中獎彩券上的簽署s進行驗證動作，即計算$t \equiv s^{e_P} \pmod{n_P} \equiv LID \pmod{n_P}$，而購買者還須附上代表其身分的身分證件，若與銀行資料庫中所儲存的*ID*和*LID*相同時，則代表此購買者為中獎彩券的合法購買人，銀行同意兌領獎金予此購買者；反之，則否。

4、最後，銀行將此次的兌領獎金紀錄於資料庫中，表示完成兌獎動作。



兌獎流程圖

第四章 分析與討論

4.1 安全性分析

以下針對本文所提出的彩券系統進行安全性分析，如下所述：

1、匿名性：除了購買者本人、認證中心和銀行外，其他任何人都無法找出彩券上的簽署*s*與購買者的關聯性，即無法得知此彩券是誰購買的。因此在本文的機制中是採用購買者的*ID*、智慧卡晶片之唯一序號*CardID*和認證中心的秘密參數*X* ，須同時有這三個數值，否則將無法查出購買者之真實身分。

2、公正性：是指在彩券中獎結果公佈之前都應保持秘密，任何人都無法從中得到額外的資訊，亦即無法預先計算出彩券開獎的結果。因為所有的開獎程序是由認證中心所進行，所以在開獎結果公佈之前，是無法取得相關資訊對智慧卡內的彩券進行篡改。

3、可靠性：本文是應用 RSA 的密碼學技術，使購買者在進行兌獎時，能驗證其簽署是否符合其身分，所以本機制達成可靠性需求。

4、不可否認性：由於購買者所購買的彩券資訊內附有本人的簽署*s* ，其簽署*s*是利用購買者的私鑰簽章，可用購買者的公鑰做驗證；因此，購買者無法否認曾買過該彩券。

5、可追蹤性：因為有上述不可否認之特性，若過程中有非法情事發生時，相關機構可利用此特點追蹤購買者的身分。

6、不能偽照性：本機制中購買者所購買的彩券是經由購買者的私鑰做簽章，而旁人無法得知其私鑰為何，故無法假造他人的簽章。

4.2 功能性分析

以下針對本文所提出的彩券系統進行功能性分析，如下所述：

1、可攜性：本機制是利用智慧卡來存取購買者購買彩券之資訊，所以購買者可攜帶智慧卡到任何彩券服務商都可進行安全性的交易。

2、鑑別性：購買者使用智慧卡時必須先輸入與智慧卡認證的 PIN 碼，因此當智慧卡遺失時，任何人將無法正常的使用智慧卡和輕易盜取裏面之資訊，故智慧卡可代表購買者之身分，銀行和彩券服務商可用它來鑑別是否為合法的購買人。

3、易存取性：本機制是利用購買者向認證中心申請後，擁有一張合法的智慧卡，利用智慧卡可方便的存取與彩券交易相關的資訊。因此，可不必擔心資料遺失和被竊取之困擾。

4、防竊取：本文中之智慧卡為安全性高的存取設備，無法從中得知他人的真實身分以及無法輕易讀取裏面的資料，即使智慧卡不小心遺失了，還是具有防竊取資料的保護性在。

5、雙重檢驗性：購買者在兌獎階段時，必須持智慧卡和身分證件向銀行做雙重檢驗的動作，若經由銀行資料庫比對無誤後，即確認為合法購買人，並同意兌領獎金。

4.3 可行性分析

本彩券系統所需的硬體設備皆為現有的設備，例如：電腦主機、顯示器、數字鍵盤、智慧卡和智慧卡讀取設備等。而上述的物品中，除了智慧卡外，就現有的環境而言，皆為相當普及的東西。

智慧卡所具有的高記憶體容量及邏輯運算能力，使得智慧卡被廣泛的應用於金融業、醫療、交通及人員管理上。例如：

1、電子錢包：有鑑於智慧卡所提供的安全性能，目前許多的電子付款系統中皆使用智慧卡來做為電子錢幣的載具，Visa Cash就是很好的例子。所謂電子錢包即為利用智慧卡上的晶片來儲存持卡人的可消費金額，而持卡人就可利用卡上的可消費金額進行消費。

2、IC 金融卡：所謂 IC 金融卡即在傳統磁條金融卡上，多加入一個積體電路晶片，以提供更多的加值服務。目前國內的 IC 金融卡所具有的功能頗多，除了具有預付電話卡、記憶八組電話號碼的功能之外，尚包含了轉帳、提款、電子錢等功能。

3、身分識別卡：所謂身分識別卡即為代表一個人的唯一身分的卡片。身分識別卡利用了智慧卡所具有的高儲存容量的特性，將持卡人的個人基本身分資料儲存於身分識別卡中，以取代原有的紙式身分證明文件。除此之外，智慧卡本身所具有的高安全存取控制功能也是它被用來開發身分識別卡的另一個主要因素。

雖然智慧卡產品在未來全球支付市場中的角色將會愈來愈重要，但由於對發卡機構而言，晶片卡的成本偏高、彩券服務商與銀行設置智慧卡系統的投資金額龐大等因素，為智慧卡的發展帶來阻力。不僅如此，消費者及彩券服務商未必認同晶片卡交易所帶來的利益。因此，若能從中獎彩金的稅收中，提取一定比率之金額來補助智慧卡的成本費用，則本彩券研究機制的落實性會更加提升。

4.4 結論

本文使用 RSA 演算法和數位簽章的技術提出具有匿名性且兼具安全性的彩券系統，購買者須和認證中心、銀行做身分的確認，同時也確保購買者身分須成年才能參與彩券活動，並假設銀行的角色是可信任的單位，在兌領獎金時對購買者進行身分確認。

本機制主要是利用智慧卡具有高安全性和方便攜帶之特性，來存取購買者購買彩券之資訊，可達到中獎者對於彩金領取之身分確認。就以現有的設備而言，我們提出的彩券機制方案若想實際運用在實務上是具體可行的。但其中仍有些許的關鍵因素，有待加強改善。如：設置智慧卡系統的投資金額龐大、智慧卡的普及率不足、多數消費者和彩券服務商對智慧卡機制仍存有不少的疑慮等。若能將上述的關鍵因素加以克服，相信未來的彩券市場將會愈來愈蓬勃發展。

參考文獻

[1] 陳怡璇，「具匿名及安全性之電子彩券系統」，世新大學資訊管理學系碩士論文，2005 年。

[2] 張莉庭，「兼具安全與效率的電子彩券系統」，世新大學資訊管理學系碩士論文，2006 年。

[3] 賴滄本，「電子投票系統的研究」，東海大學數學系碩士論文，2010 年。

[4] 許沁如，「結合智慧卡之通行碼認證機制研究」，世新大學資訊管理學系碩士論文，2005 年。

[5] 沈淵源，密碼學之旅與 MATHEMATICA 同行，全華科技圖書出版，2006。

[6] 巫坤品、曾志光，密碼學與網路安全——原理與實務第二版，碁峰資訊圖書出版，2001。

[7] 余致力，「我國彩券發行的理論探討與政策分析」，世新大學行政管理學系理論與政策期刊，15 卷 2 期，頁 25-44，1999 年。

[8] 郭玳質，密碼危機——MD5 演算法，http://www.shs.edu.tw/works/essay/2010/03/2010031221021597.pdf

［9］密碼學原理與技術(對稱式與非對稱式密碼技術)，

http://avp.toko.edu.tw/docs/class/3/%E5%AF%86%E7%A2%BC%E5%AD%B8%E5%8E%9F%E7%90%86%E8%88%87%E6%8A%80%E8%A1%93.pdf

［10］數位憑證技術應用，

http://bmeweb.niu.edu.tw/material/ec/%E6%95%B8%E4%BD%8D%E6%86%91%E8%AD%89%E6%8A%80%E8%A1%93%E6%87%89%E7%94%A8.htm

［11］密碼學與資訊安全，

http://ec2.ba.ntust.edu.tw/mic/download/security/%E5%AF%86%E7%A2%BC%E5%AD%B8%E8%88%87%E8%B3%87%E8%A8%8A%E5%AE%89%E5%85%A8ch5.doc

［12］中國信託-台灣彩券，

http://www.taiwanlottery.com.tw/index_new.aspx