私 立 東 海 大 學 資 訊 工 程 與
科 學 研 究 所

碩 士 論 文

指 導 教 授：林 祝 興 博士
(Dr. Chu-Hsing Lin)

可 防 止 盜 用 的 電 子 現 金 系 統 之 研 究

A Study of Electronic Cash Schemes Against Embezzling

研究生：楊 國 鴻
(Kuo-Hung Yang)

中 華 民 國 九 十 一 年 五 月

中文摘要

隨著網際網路的日益發展，有越來越多的網路服務被提出來，電子商務便是其中炙手可熱的一種。因為網際網路是一種新興的的工具，可以提供低成本的即時性與互動性，使得人們有越來越多的機會在網路上處理交易，電子給付系統便是在電子商務之中一個重要的部分。我們可以把電子給付系統分為三類，其中電子信用卡系統是最廣為人知的系統，電子信用卡系統在每次交易時都需要信用卡號碼，而電子支票與電子現金等服務，也有越來越多的研究被專家學者提出。

在本論文中我們提出了三個電子現金系統，第一個系統是以視覺式秘密分享和指紋辨識技術為基礎架構，利用指紋作為認證付款者與電子現金的申請者是否相同的依據，並且以視覺式秘密分享的技術保護指紋，使其得以在網路上安全的傳遞；第二個系統則是將通行碼認證架構整合智慧卡，利用通行碼認證的方式來驗證付款者與電子現金申請人的身分；第三個系統則在相同的安全性考量下，將原本的通行碼認證的方式，改良為橢圓曲線的架構來提昇系統運算的的效能，使其運算需求可以降到最低並且達到與第二個系統相同的安全度。

關鍵詞：電子給付系統、電子現金、電子支票、電子信用卡、指紋辨識、視覺式秘密分享、智慧卡、通行碼認證、數位簽章、單向雜湊函數、匿名性、安全性、電子商務、橢圓曲線。

英文摘要

With the development of Internet day by day, there are more and more services on Internet proposed. e-Commerce is one of burning to the touch issues. People have more and more chances to do business on the Internet, since Internet is a newly risen tool. It can provides real-time interactive without expensive cost. An important part of e-Commerce is electronic payment system. We can class electronic payment system among three types: electronic credit card system is the most popular one, which is based on credit card. The system requests a credit card number for each transaction. And the others are electronic cheque and electronic cash systems. There are also more and more researches published by scholars and professionals.

In the thesis, we proposed three electronic cash system. The first proposed system is based on visual secret sharing and fingerprint recognition technologies. We use biologic recognition to authenticate the identity of payer and claimer. The second one is integrated password authentication scheme with smart cards. We employ password authentication scheme to verify the status between payer and claimer. The third system improves the password authentication scheme using elliptic curve. Besides the same security consideration, and the time complexity will be decrease by the scheme.

Keywords: Electronic Payment System, Electronic Cash, Electronic Cheque, Electronic Credit card, Fingerprint Recognition, Visual Secret Sharing, Smart Card, Password Authentication Scheme, Digital Signature, One-Way Hash Function, Anonymity, Security, e-Commerce, Elliptic Curve.

致謝辭

本論文的完成，首先要感謝我的指導教授林祝興博士的細心指導；在專業能力上，教授孜孜不倦的帶領與指導，讓我在學術領域的鑽研如魚得水；在待人處事上，教授溫文爾雅的風度，更讓我在研究所期間如沐春風。

接下來要感謝我的口試委員：周志賢教授、葉義雄教授、詹進科教授及蕭如淵教授(依筆劃順序)的指導，口試時承蒙教授們提供的寶貴意見，得以讓我的碩士論文更加完善。

也要感謝系助理若瑩、春蘭，在平常為我們處理瑣碎的雜務，使我們得以專心課業，更為我們妥善安排了口試的時間與場所。

感謝助教錦菁細心的校稿，實驗室夥伴子杰、正隆、峰菖、國榮、及其他學弟們在平常的協助與指教，才能讓我在論文的研究上無後顧之憂。

當然更要感謝我的家人，提供我不虞匱乏的環境以及精神支柱，我才能順利的成長茁壯。

要感謝的人太多，不及一一備載；套用一句老掉牙的話 — 既然要感謝的人太多，那就謝天吧。

目錄

圖表目錄

第壹章　　導論

第一節　　研究背景與動機

隨著網路的日益發達，人們上網購物的機會也大大地增加，感覺上，似乎網路時代已然來臨。然而，目前的電子商務系統所採用的付款工具，仍然以傳統的電匯及信用卡為主，根據統計，在台灣，約有 6%的電子商務系統採用了由 VISA 等國際組織所發行的 SET 系統，也大約有 6%是採用了由網景公司發行的 SSL 系統，由比例上來看，現行的網路購物採用的仍是以傳統的付款方式為主。

至於一個系統即使採用了 SET 與 SSL 能不能稱得上是一個完全的電子商務系統呢？我們可以想想 SET 與 SSL 付款的方式。雖然 SET 與 SSL 都提供安全的交易環境，然而，SET 與 SSL 所使用的交易媒介卻是現行的信用卡，信用卡的使用固然方便，最終卻還是要消費者親自去清償信用卡的款項。SET 與 SSL 是完全的電子商務嗎？答案是顯而易見的。

那麼在電子商務裡頭，什麼樣子的付款工具才是最適當的呢？根據統計，雖然信用卡支票等金融工具已經相當普及，但是人們在一般商業行為中，最常使用的付款工具還是現金，如果說電子商務是把人們的交易行為搬上網路，那麼如果有一種可以在網路上交易

的現金，相信人們也更能接受電子商務才是。

第二節　研究目的及論文架構

在三類電子現金給付系統中，電子支票系統及電子信用卡系統都牽涉到使用者資訊曝光的問題，而電子現金系統為了達到傳統現金的功能，所必須具備的一些特性，相較於前面兩類電子給付系統，有更寬廣的應用空間。

施大偉[25]提出了一個理想電子現金系統所應具備的特性：獨立性、安全性、匿名性、離線付款、可傳輸性、可分性、條件稽核及災難復原。

我們希望可以提出一個安全方便的電子現金系統，可以避免偽造，避免重複使用的問題，更要做到防止盜用來保護使用者的財富及個人資訊被不當的使用。並且提供適當的匿名復原機制，以達到符合理想電子現金的特質。

本論文第壹章主要介紹一些電子現金的發展以及我們的研究動機及目的；在第貳章的內容之中，我們將分別探討一般電子現金的流程，理想電子現金所應具備的基本特性，並討論我們所應用的技術與架構；在第叁章中，我們首先提出一個應用視覺式秘密分享技術的電子現金架構，這個架構的重點是利用指紋辨識技術來達到辨

識使用者身份的目的[4]，而指紋是每一個人重要的一項生理特徵，倘若任其在網路上不加保護的傳送，對使用者而言，可能會招致難以想像的嚴重後果，所以我們也應用了視覺式秘密分享技術[2,7,13,14,15]來達到保護指紋的目的；在第肆章裡面，我們進一步將電子現金整合到智慧卡之中，除了原有系統架構的安全性等相關性都保存之外，並且結合了通行碼認證的演算法[3]，在電子現金之外，又加了一層保護傘，而智慧卡本身所提供的運算功能及儲存空間，也提供了本系統的便利性需求；在第伍章中，我們將第肆章所提出的架構進一步整合了運算速度比較快的橢圓曲線演算法，將原有的通行碼認證的方式以全新的面貌整合在我們的電子現金系統之中，除了可以提昇運算速度之外，更加強了原有系統的安全性；最後在第陸章，我們討論了一些電子現金系統所面臨的問題，並且提出一些電子現金未來可應用的研究方向，再對電子現金系統作個簡單的結論。

第三節　研究範圍及假設條件

本論文的討論主要在電子現金系統的技術，以及電子現金系統相關的研究，電子信用卡及電子支票系統，雖然同樣都是電子給付系統，但其架構與應用並不在本文的討論範圍之內。

本文假設政府當局有權管理國民的指紋，並且有責任保護國民的指紋不遭到非法濫用等問題，所以政府當局應有一個存放全民指紋的安全資料庫，而這個資料庫應與戶政機關所使用的資料一致。而此資料庫的保全及技術等安全措施均不在本文討論範圍之中，意即假設所使用的資料庫安全無虞。

在本論文之中，我們應用了許多的加密或簽章技術，我們只討論其對於電子現金的安全性，關於這些技術的安全性等相關問題，請參照參考文獻。

我們主要討論的是電子現金本身的安全問題及理想特性，關於網路本身的安全問題，流量控制等並不列入討論的範圍，這些網路相關問題請參照網路協定等文獻。

第貳章　　文獻探討

在本章中，我們將分節討論一般的電子現金系統概述、現行使用的電子現金系統介紹、理想的電子現金特性、視覺式秘密分享技術等等相關的文獻。

第一節　　電子現金概述

所謂的電子現金，是以電子的方式來處理交易的電子貨幣，而依據電子現金儲存的方式又可分為智慧卡型電子現金與網際網路空間型電子現金，智慧卡型電子現金是指將電子現金儲存在一個安全方便的智慧卡中，可由使用者隨身攜帶以取代傳統的貨幣方式，作為交易媒介之用；而網際網路空間型電子現金則是交易雙方設定電子給付系統，以達到付款收款的目的。而不論是哪一種電子現金，都是用電腦資料的方式來儲存及傳遞。而使用者在使用電子現金的時候，並不會暴露使用者的個人資訊，亦即電子現金與傳統現金所具備的匿名性質。

第二節　　現行的電子現金系統

我們可把現行的電子現金約略分為兩種模式：連線模式及離線模式。為了簡明介紹，我們將以系統流程來說明這兩種模式。

一、連線模式

在連線模式之中，是以 Chaum 的數位盲簽章[5]作為基本的架構，系統流程如下：

第一步—使用者首先隨機選取電子現金序號 x 和盲因子 r，利用銀行的公開金鑰 e，計算$r^e f(x)$並傳給銀行，f(x)是一個單向雜湊函數。

第二步—銀行將收到的$r^e f(x)$用秘密金鑰 d 簽章之後可得到$rf(x)^d \bmod n$，並將其傳回給使用者。

第三步—使用者收到$rf(x)^d \bmod n$後除以使用者選取的 r，便可得到$f(x)^d \bmod n$，(x, $f(x)^d \bmod n$)即為單位電子現金。

第四步—使用者拿到單位電子現金之後便可以付款給商店。

第五步—商店在收到使用者送來的單位電子現金之後，利用銀行的公開金鑰 e 驗證$(f(x)^d \bmod n)^e$是不是等於$f(x) \bmod n$，如果相等，表示這電子現金是合法的，並同時將這個電子現金傳給銀行，也就是把(x, $f(x)^d \bmod n$)傳給銀行。

第六步—銀行同樣檢查$(f(x)^d \bmod n)^e$是不是等於$f(x) \bmod n$，如果相等，再核對資料庫中有沒有同樣的序號，如果沒有，將金額存入商店的帳戶中，並把序號紀錄在資料庫裡，然後通知商店確認這筆交易，商店再通知使用者已經完成

交易；如果已有紀錄，則此電子現金是已經交易過的，此次交易無效。

在這個模式下，銀行只要建立一個資料庫來記錄使用過的電子現金序號，就可以檢查電子現金是否為重複使用，然而隨著發行越來越多的電子現金，銀行的資料庫將會越來越龐大，不易維護。

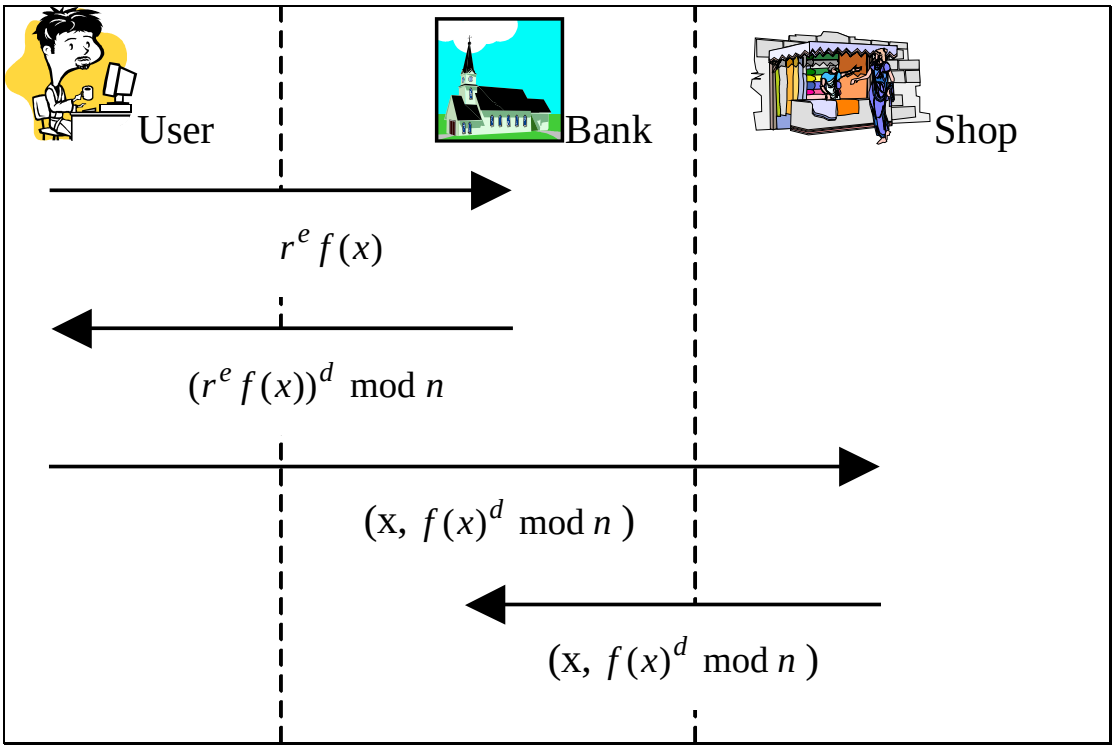


圖 2.1連線模式電子現金系統

二、離線模式

在離線模式之中，是以 Chaum 及 Finny[6,7]提出的挑戰與回應方式作為系統的基本架構，系統流程如下：

第一步—使用者隨機選擇 k 個電子現金序號 a_i 和 k 個盲因子 r_i，i 從 0 到 k-1，對每個 i 算出 $x_i \equiv f(a_i) \bmod n$、$y_i \equiv f(a_i \oplus <ID>) \bmod n$，<ID>是用來識別使用者的資訊，求得 $r_i^e \cdot g(x_i, y_i) \bmod n$ 並送給銀行，e 是銀行的公開金鑰。

第二步—銀行隨機選取 k/2 個 $r_i^e \cdot g(x_i, y_i) \bmod n$，要求使用者傳回相對應的 a_i、<id>、$g(x_i,y_i)$及相應的盲因子 r_i，以查驗使用者有沒有把<id>計算進來。

第三步—使用者把銀行要求的參數傳給銀行。

第四步—銀行驗證通過後，對剩下的 k/2 個 $r_i^e \cdot g(x_i, y_i) \bmod n$ 作數位簽章運算，也就是用秘密金鑰 d 計算 $(r_i^e \cdot g(x_i, y_i) \bmod n)^d$，得到 $r_i \cdot g(x_i, y_i)^d \bmod n$，並回傳給使用者。

第五步—使用者將銀行傳回的 k/2 個數除以相對應的盲因子 r_i 再相乘起來，便得到單位電子現金 $\prod_{i=1}^{k/2} g(x_i, y_i)^d \bmod n$。

第六步—付款時，使用者將 $\prod_{i=1}^{k/2} g(x_i, y_i)^d \bmod n$ 傳給商店。

第七步—商店送出 k/2 個位元的隨機挑戰字串給使用者。

第八步—對每個 i，如果對應的隨機挑戰是 1，使用者以 a_i、y_i 作為回應，如果隨機挑戰為 0，則使用者以 x_i、$a_i \oplus$<ID>作為回應。

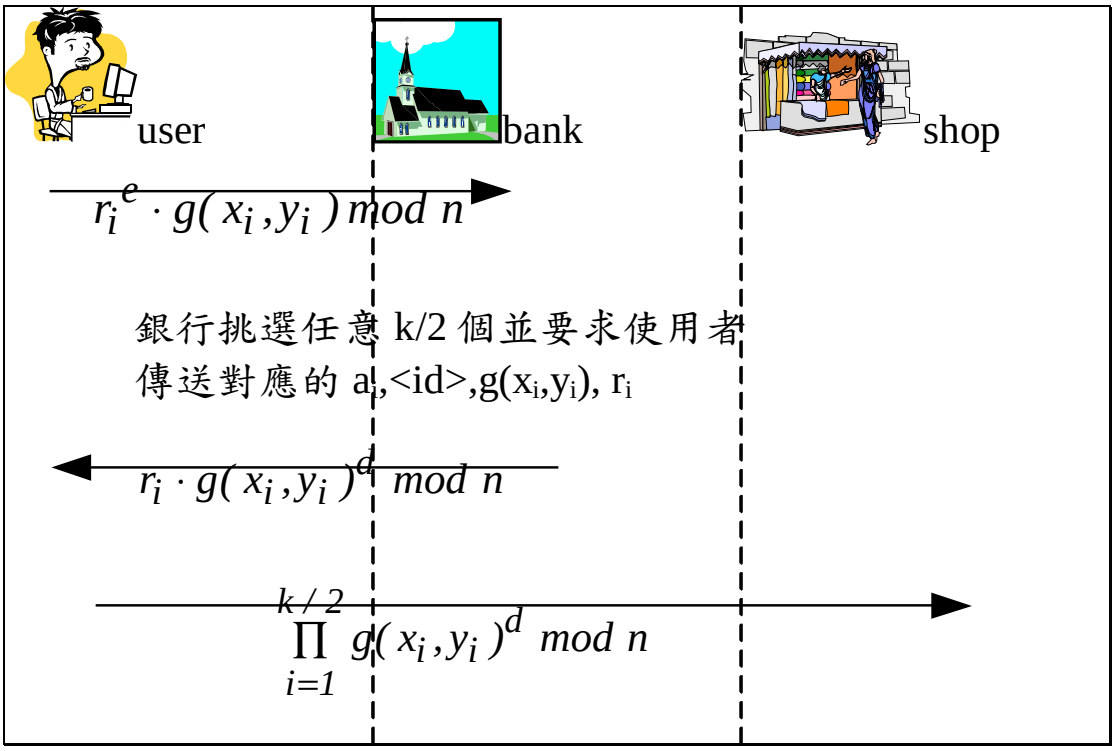
第九步—商店利用收到的各組回應可以求得 x_i 或 y_i 並進一步可求得 $\prod_{i=1}^{k/2} g(x_i, y_i)^d \bmod n$ ，檢查是不是跟使用者在付款時送來的 $\prod_{i=1}^{k/2} g(x_i, y_i)^d \bmod n$ 相等。至此使用者完成與商店之間的付款流程。

接下來，商店在累積了一定數量的電子現金之後，便以批次的方式將這些電子現金存到銀行，同樣的，銀行在收到許多商店送來的電子現金之後，也以批次的方式檢驗是否有重複使用的電子現金。

假設使用者用同樣的電子現金在不同的商店付款，使用者所收到商店的隨機挑戰幾乎不可能完全相同，所以銀行可以將同一組隨機挑戰的回應資料經過 XOR 運算，就可以得到使用者的身分資料<ID>。

這種模式的缺點是不能做到事前預防，只能事後驗證，所以只能應用在小額付費上。

離線模式的電子現金架構如圖 2.2 所示。



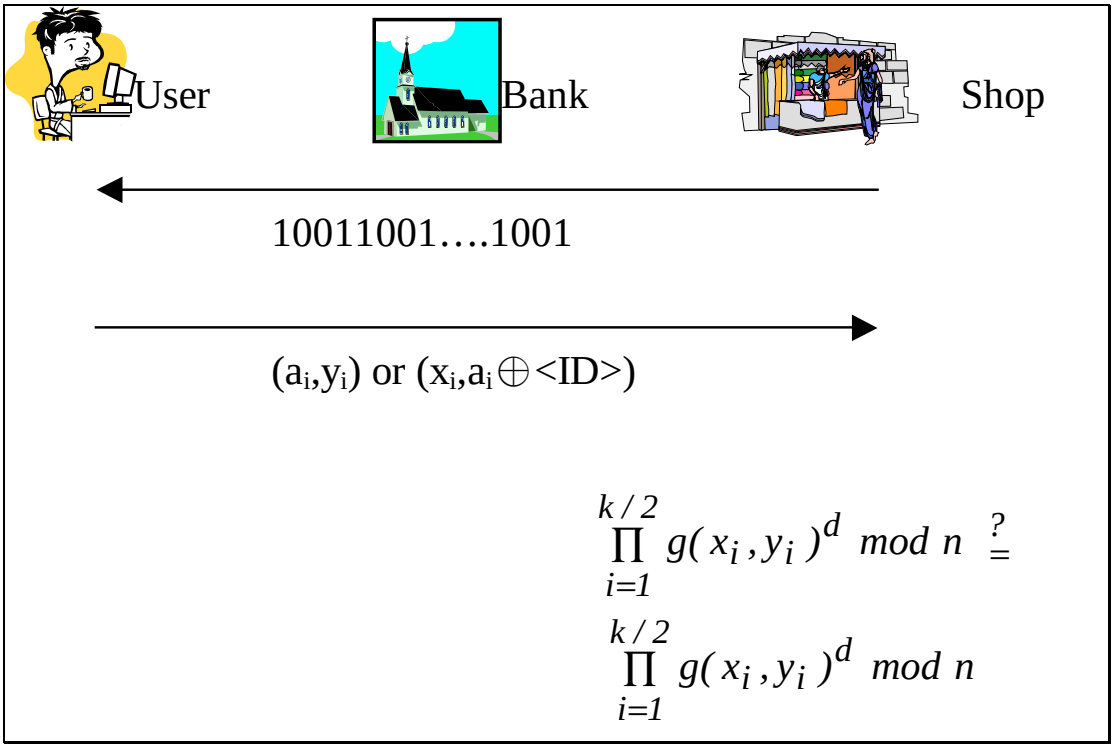


圖 2.2離線模式電子現金系統

第三節　　電子現金的理想特性

施大偉在 1988 年提出[25]八個電子現金的理想特性：獨立性、安全性、匿名性、離線付款、可傳輸性、可分性、條件稽核、災難復原。接下來我們針對每一個理想特性做個討論及介紹。

一、獨立性

電子現金不應該依賴任何實體的物理性質，而能夠在網路上傳輸。也就是電子現金的本質應該是一連串的電腦資料，可以透過網路連線在網際網路上流通；簡單的說，電子現金就是在網路世界裡所適用的貨幣。

二、安全性

眾所皆知，網際網路是一個開放式的環境，任何人只要有網路設備，就可以進入網路的世界中搜尋、接收資料，因此任何在網際網路中流通的資料，當然也包括電子現金，都有被竊取、被複製的可能，因此電子現金必須符合一定的安全性，才能有網路貨幣的功用。電子現金的安全性主要著重在如何避免偽造、避免重複使用以及不被盜用等問題。

三、匿名性

隱私權對於使用者而言，其重要程度不下於實質的財富，而網際網路的盛行，更使得隱私權的保護越來越受到重視。電子現金之所以比電子信用卡、電子支票系統更具優勢，就在於電子現金可以保障使用者的私密資訊不外流，一般電子現金對於保障匿名性的做法是採用數位盲簽章的技術，或者是採用可信賴的電子現金伺服器方式。

四、離線付款

離線付款指的是消費時，電子現金不需要透過與銀行主機的連線查驗，也能進行付款的動作。一般的電子現金離線付款主要有兩種作法，第一種是利用在電子現金的模組裡加上一個稱為觀察者的模組，用來記錄每筆電子現金交易的流程；另外一種則是比較常用的挑戰回應方式，由收款方送出挑戰，付款方傳回回應的過程，以揭露原先加密過的資訊，藉此驗證電子現金是否經過重複消費。

五、可傳輸性

電子現金的用途主要是在網路上取代傳統貨幣的地位，而在現實生活中，傳統貨幣是可以經過使用者之間的私相授受，

來轉移所有權及使用權，因此一個理想的電子現金也應該要具備這種理想特性，可以經由使用者之間的協議轉移所有權及使用權，而不會影響到電子現金的安全性與匿名性。為求立意明確，我們在以後章節改稱為所有權轉移性。

六、可分性

簡單的說可分性就是電子現金應該也具備有可找零的特性，電子現金應該要有各種面額的存在，而目前有關電子現金的研究之中，都把電子現金設計成單位貨幣，因此電子現金的總額都可以加成，而不需要有可找零的特性。

七、條件稽核

電子現金的設計，基於保護使用者的匿名性，因此除了交易雙方，沒有任何第三者可以得知電子現金的流向與用途，雖然保障了使用者的隱私權，卻也使得電子現金容易淪為販毒、洗錢等方便的犯罪工具，因此電子現金應該具備可以在有條件的法律管理情況下提供檢調單位得以追查某筆電子現金的流向。

八、災難復原

既然電子現金不需依賴任何實體的物理性質，而得以在網

路上傳輸，因此電子現金的儲存媒介，勢必容易受到破壞，而造成使用者的損失，因此電子現金應該要避免使用者的權益受到破壞，所以應該具備有匿名的災難復原機制，可以補足電子現金儲存媒介的先天缺失，將使用者的損失降到最低。

第四節　視覺式秘密分享技術

在 M. Naor 和 A. Shamir 在 EUROCRYPT'94 發表的"Visual Cryptography"[2]中，提出了視覺式秘密分享的概念，以下針對視覺式秘密分享作個簡單的介紹：

假設我們擁有一張以二進位編碼的黑白圖片，我們要對這張圖片做(2,2)視覺式秘密分享處理，首先分析這張圖片中的每一個圖素，因為圖片是以二進位編碼的，所以每一個圖素不是黑色就是白色，我們將原來的黑色圖素表示為 1111，白色圖素可表示為 1110、1101、1011、0111，如圖 2.3 所示。

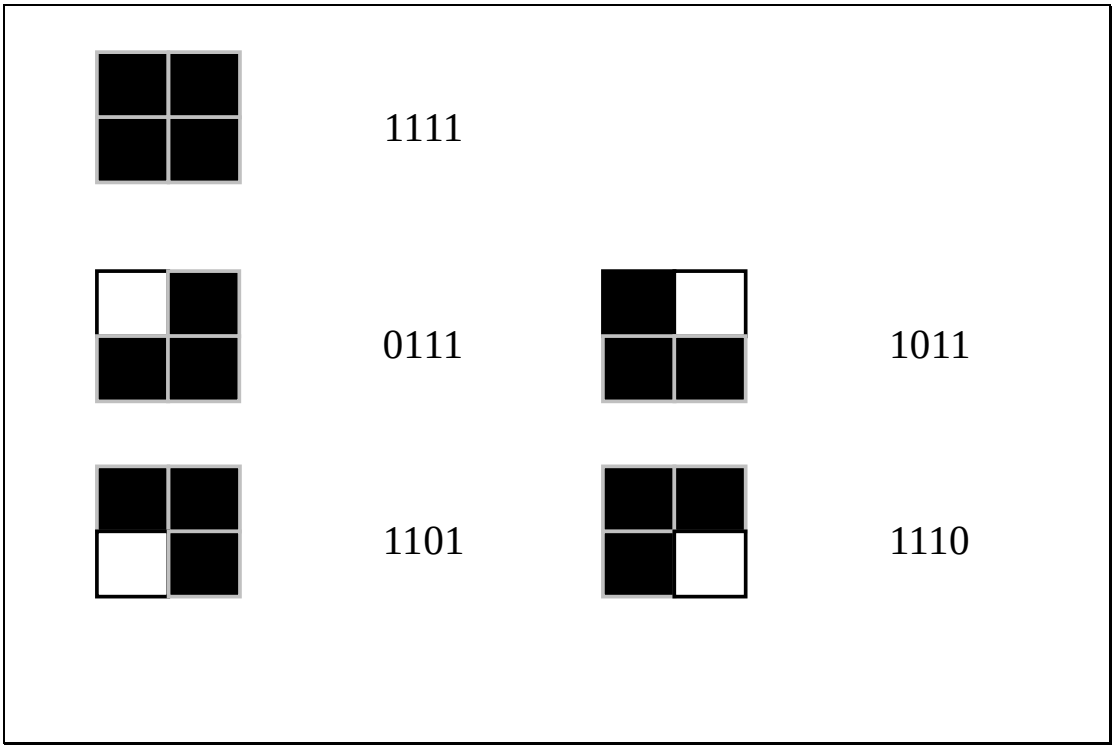


圖 2.3圖素編碼原則

接下來將每個圖素切割成 2 個子圖素，使得兩個子圖素經過互斥或(XOR)的運算之後可以得到原來的圖素；每個子圖素的表示法如圖 2.4 所示。

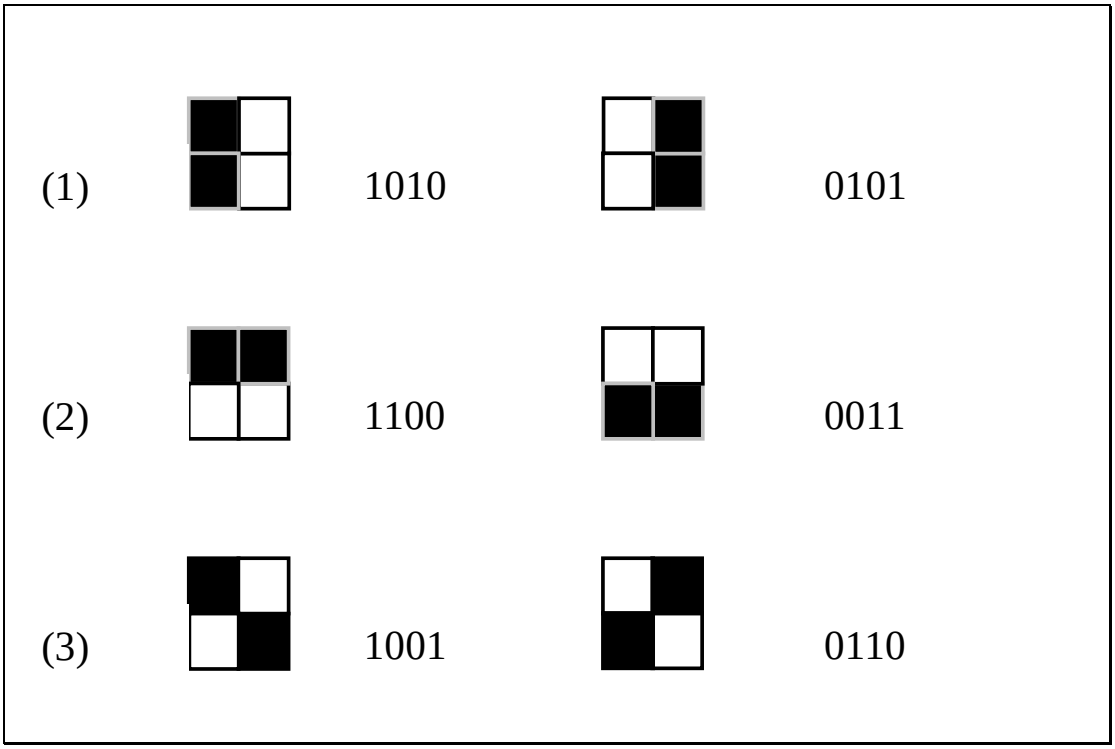


圖 2.4子圖素表示法

當所有的圖素都分成兩個子圖素之後，就可以得到兩張子圖。在兩張子圖疊合之後，會得到原來的母圖，這便是簡單的視覺式秘密分享概念。

第五節　通行碼認證 (Password Authentication)

在 W.H. Yang 和 S.P. Shieh 所提出的通行碼認證[3]中，是以 RSA 演算法作為基本的架構，並以 timestamp 及 nonce 作為抵擋重播攻擊的工具，本論文中引進一個公正的第三團體(Key Information Center)

作為發行智慧卡的機構，透過 KIC 的註冊程序，達到結合智慧卡的通行碼認證架構。我們將介紹其中 timestamp-based 的架構來說明通行碼認證的技術。

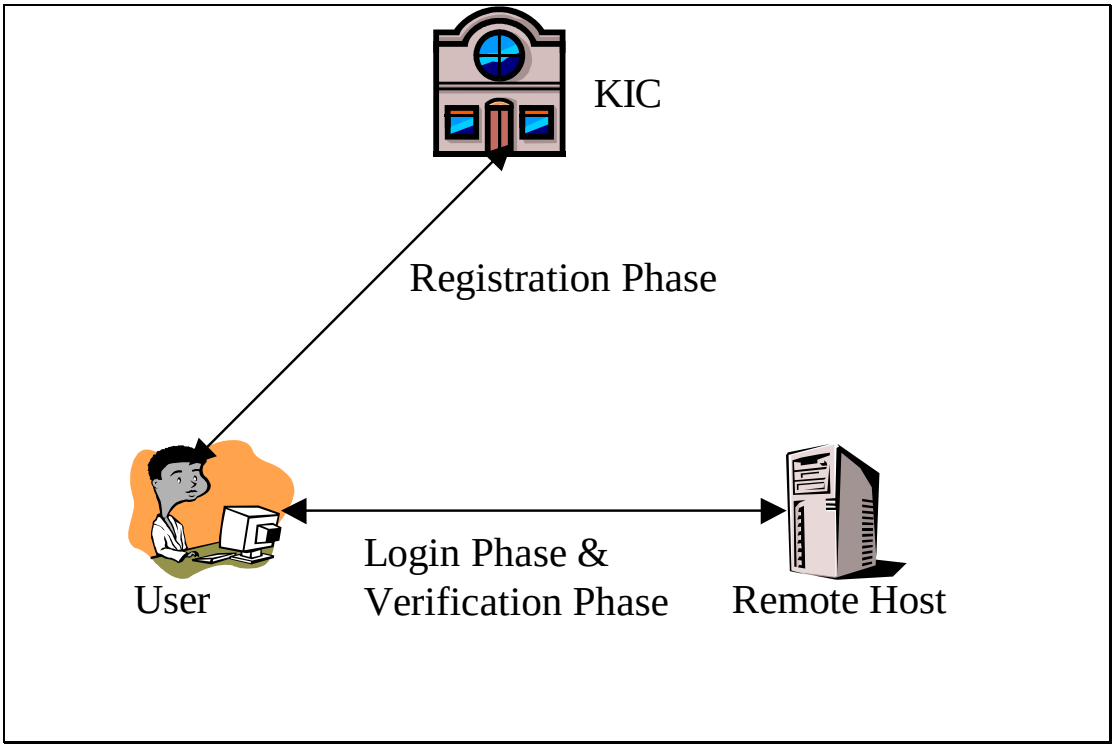


圖 2.5通行碼驗證架構

一、KIC 的基本設定

以下是說明 KIC 在製造智慧卡之前所必須準備的基本參數。

第一步—KIC 任選 p 和 q 兩個大質數，計算 $n = p \cdot q$。

第二步—KIC 任選一個整數 d 作為 KIC 的私密金鑰(private

key)，並找出與 d 互質的整數 e，滿足 $d \cdot e \pmod{(p-1)(q-1)} = 1$。e 即為相對應的公開金鑰(public key)。

第三步—KIC 找出一個整數 g，g 是 GF(p)和 GF(q)中的 primitive element，也是 KIC 的公開資訊。

二、註冊程序

以下是敘述使用者在向 KIC 申請智慧卡時的註冊程序。

第一步—使用者向 KIC 註冊，並輸入使用者自選的識別碼(ID_i)及通行碼(PW_i)。

第二步—當 KIC 收到使用者的註冊需求及使用者自選的 ID_i、PW_i 之後，計算 $S_i \equiv ID_i^{\,d} \bmod n$，根據 RSA 演算法，我們可以得到 $ID_i \equiv S_i^{\,e} \bmod n$。

第三步—KIC 產生智慧卡的識別碼(CID_i)，並計算 $h_i \equiv g^{PW_i \cdot d} \bmod n$。

第四步—KIC 將 n、e、g、ID_i、CID_i、S_i 及 h_i 寫入智慧卡，並把智慧卡交給使用者，完成註冊程序。

完整的註冊程序如圖 2.6 所示。

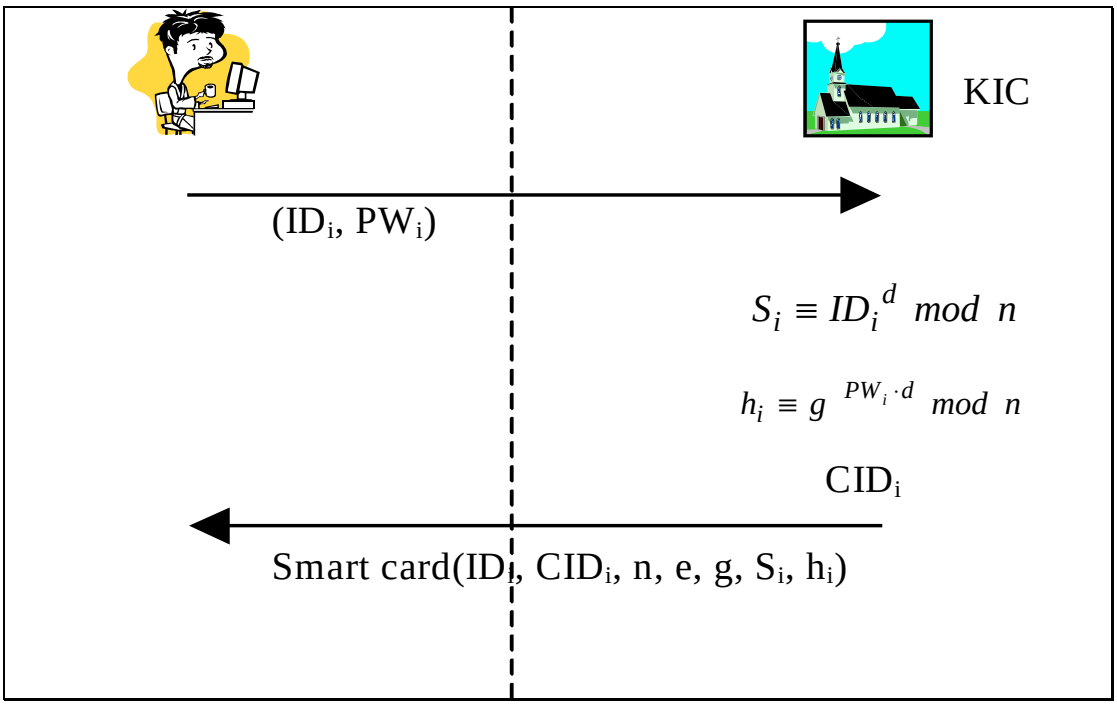


圖 2.6註冊程序

三、登入程序

以下是使用者在取得智慧卡之後，利用智慧卡登入遠端主機的步驟。

第一步—使用者將智慧卡插入讀卡機中，並輸入 ID_i'及 PW_i'。

第二步—智慧卡產生一個亂數 r_i，並計算下列參數，$X_i \equiv g^{r_i \cdot PW_i'} \bmod n$，$Y_i \equiv S_i \cdot h_i^{r_i \cdot f(CID_i, T)}$(T 是當時的時間)。

第三步—智慧卡將(ID_i、CID_i、X_i、Y_i、n、e、g、T)傳送給遠端系統作驗證。

完整的登入程序如圖 2.7 所示。

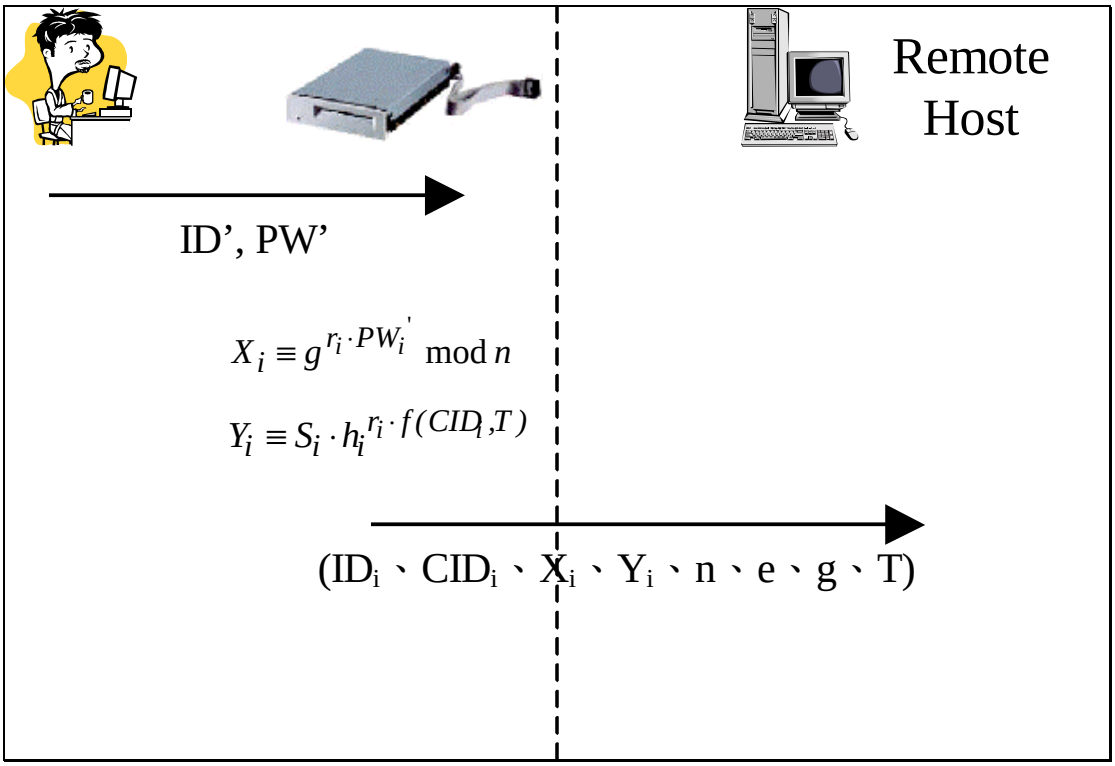


圖 2.7 登入遠端主機

四、驗證程序

以下敘述遠端主機驗證使用者資訊的步驟，以決定是否讓使用者登入。

第一步—遠端系統首先驗證 ID_i 與 CID_i 是不是合法的識別碼。

第二步—比較收到登入訊息的時間(T)與登入訊息中的時間(T')，是不是在規定的時距範圍內。

第三步—檢查 $Y_i^{e} \stackrel{?}{=} ID_i \cdot X_i^{f(CID_i,T)}$ 是否成立，若等式成立，則接受使用者登入。

完整的驗證程序如圖 2.8 所示。

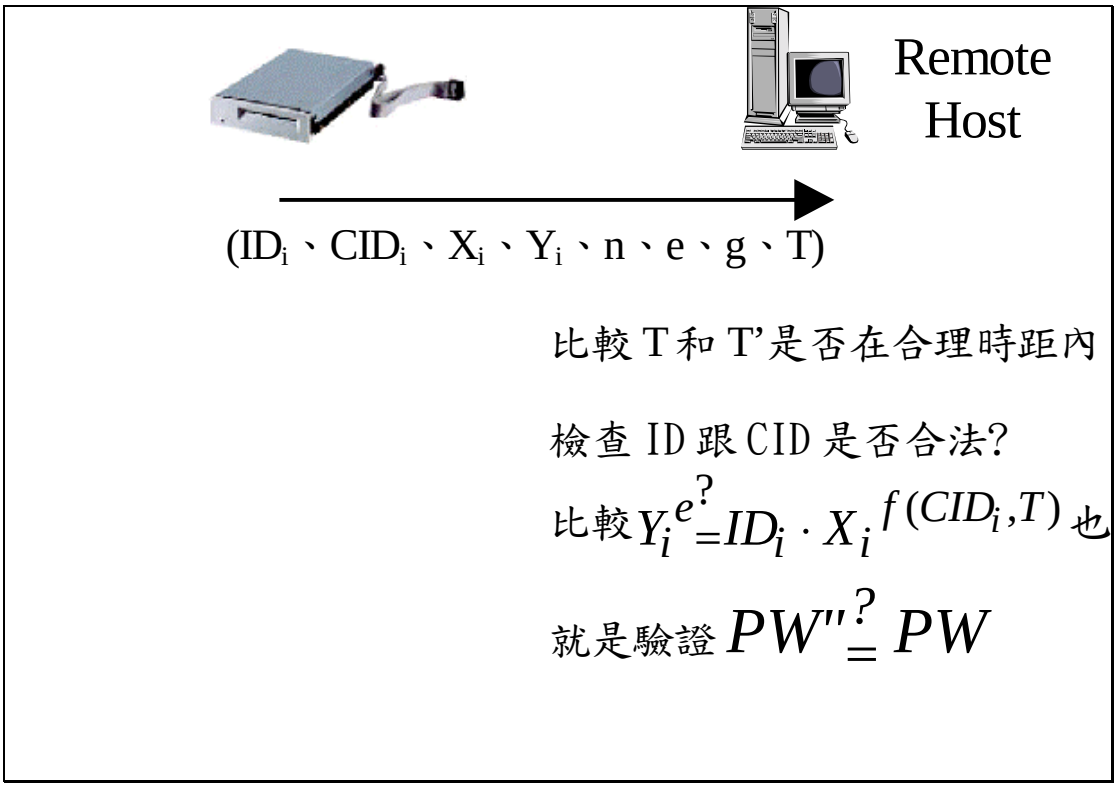


圖 2.8遠端主機驗證程序

第六節　有限場F_p（The Finite Field, F_p）

令 p 是一個質數，則 F_p 稱為一個質數場，包含了 $\{0,1,2,...,p-1\}$等整數所形成的集合，在這個有限場中包含了以下算數運算：

一、加法—若 $a,b \in F_p$，$a+b=r$，則 $r \equiv (a+b) \bmod p$，而且 $0 \le r \le p-1$；

二、乘法—若 $a,b \in F_p$ ，$a \cdot b = s$ ，則 $s \equiv (a \cdot b) \bmod p$ ，而且 $0 \le s \le p-1$；

三、反元素—若 a 是屬於 F_p 中的一個非零元素，則 a 的反元素，表示為 a^{-1}，是一個唯一的整數 c，並且滿足 $a \cdot c = 1$。

例如 F_{23} 的所有元素集合為 $\{0,1,2,...,22\}$，$12+21=10$，$6 \cdot 9 = 8$，$6^{-1} = 4$。

第七節　　橢圓曲線概論

橢圓曲線的功能，主要是用來減少在一般加解密演算法及數位簽章演算法上經常使用到的冪次方運算。在一般的加解密及數位簽章演算法中，通常是以離散對數或者是大數分解的數學難題作為主要的架構，進而衍生出許多複雜的演算法，以達到加解密以及數位簽章的需求。而這些演算法又經常需要運用到許多大數的冪次方運算，雖然近代的電子計算機在處理這些複雜的運算方面已經遊刃有餘，但是過多的複雜運算，使得這類型的系統實作仍然是曠日費時，因此仍然有許多學者專家致力於減少運算量的研究，橢圓曲線便是其中較為熱門的一種方式，本節將簡單介紹橢圓曲線的定義以及橢圓曲線上的運算。

一、有限場的橢圓曲線(Elliptic curves over F_p)

令 p 為大於 3 的質數，橢圓曲線定義為 $y^2 \equiv x^3 + ax + b$，其中 a ,b 屬於 F_p，且 $4a^3 + 27b^2 \neq 0 \,(mod\ p)$。

假設 $p = 19$，在有限場 F_{19} 的橢圓曲線為 $E: y^2 = x^3 + x + 4$，可以利用判別式 $4a^3 + 27b^2 = 4 + 432 = 436 \,(mod\ 19) = 18 \neq 0$ 得知 E 確實是一個橢圓曲線，這個橢圓曲線在 F_{19} 的所有點的集合為一個無限遠的點以及(0,2)、(1,11)、(1,12)、(4,7)、(4,16)、(7,3)、(7,20)、(8,8)、(8,15)、(9,11)、(9,12)、(10,5)、(10,18)、(11,9)、(11,14)、(13,11)、(13,12)、(14,5)、(14,18)、(15,6)、(15,17)、(17,9)、(17,14)、(18,9)、(18,14)。

二、橢圓曲線的點運算

在有限場 F_p 的橢圓曲線 $y^2 \equiv x^3 + ax + b$ 上的加法可描述為在橢圓上的兩點 P 及 Q，首先將 P 跟 Q 畫一條連接線，交到拋物線上得一點 R’，接著以 x 軸為中心，投影到拋物線的另一端得到一點 R，R 即為 P 跟 Q 的和。如圖 2.9 所示：

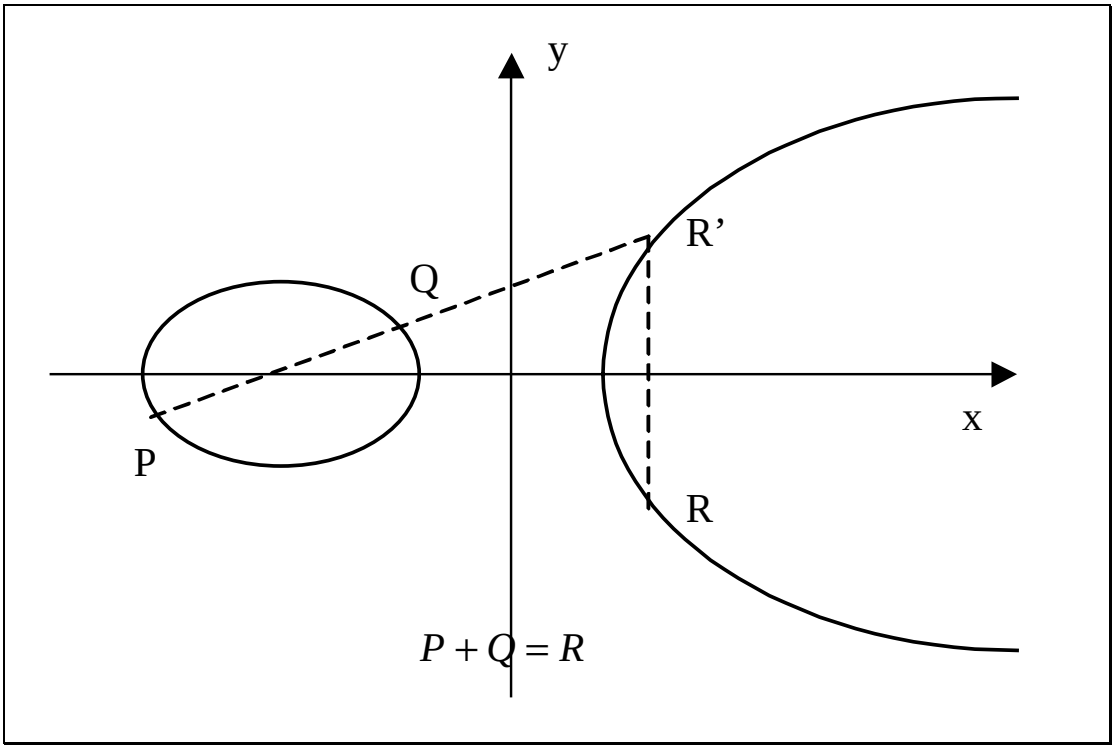


圖 2.9橢圓曲線的點運算 $P+Q=R$

令 $P=(x_1,y_1)$ ， $Q=(x_2,y_2)$ ， $R=P+Q=(x_3,y_3)$ ，$P\neq\pm Q$ ，則 $x_3=(\frac{y_2-y_1}{x_2-x_1})^2-x_1-x_2$ ，$y_3=(\frac{y_2-y_1}{x_2-x_1})(x_1-x_3)-y_1$ 。

令 $P=Q$ ，則 $P+Q=P+P=2P$ ，在幾何圖形上可以表示為在 P 點上畫一條切線，交到拋物線上的 R'，再以 x 軸為中心，投影到拋物線的另一點 R， $R=2P$ ，如圖 2.10 所示。

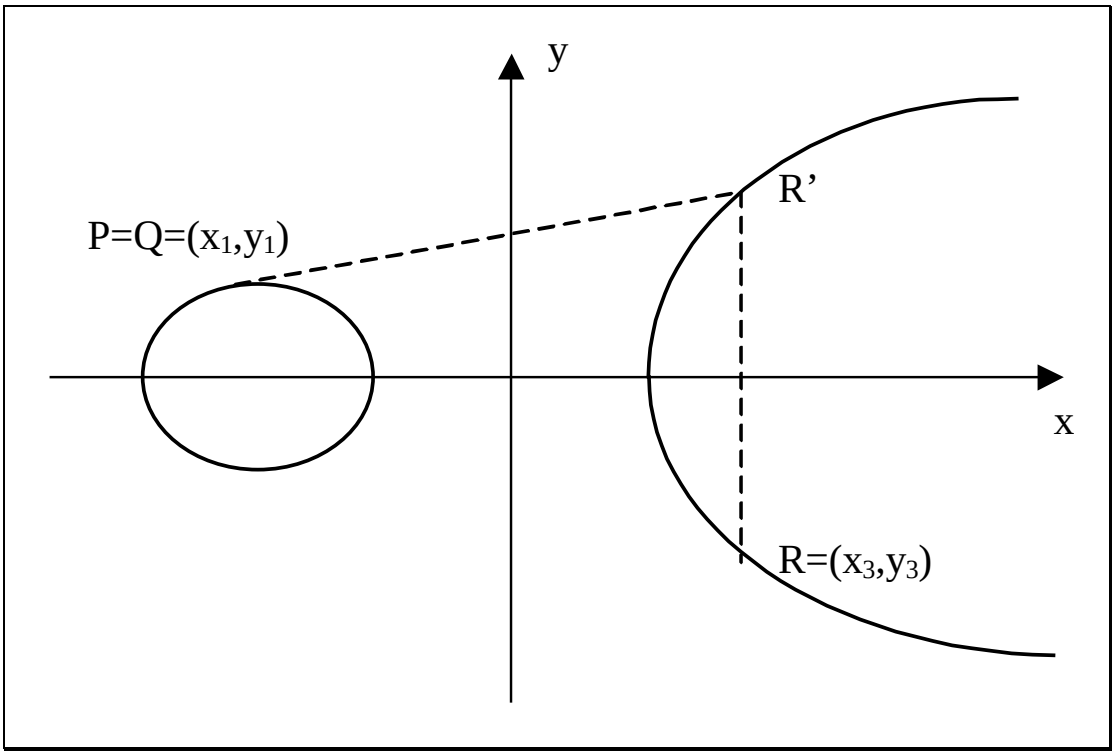


圖 2.10　　橢圓曲線的點運算 $2P = P + P = R$

$x_3 = (\frac{3x_1^2 + a}{2y_1})^2 - 2x_1$ ， $y_3 = (\frac{3x_1^2 + a}{2y_1})(x_1 - x_3) - y_1$ 。

舉個範例說明如下：令 $p = 23$ ， $E: y^2 = x^3 + x + 4$ ，$P = (4,7)$ ， $Q = (13,11)$ ， $P + Q = (x_3, y_3)$ ，

$$x_3 = (\frac{11-7}{13-4})^2 - 4 - 13 = 3^2 - 4 - 13 = -8 = 15 \pmod{23}$$

$$y_3 = 3(4 - 15) - 7 = -40 = 6 \pmod{23}$$

所以 $P + Q = (15,6)$ 。

$2P = P + P = (x_3, y_3)$ ，

$$x_3 = (\frac{3(4)^2+1}{14})^2 - 8 = 15^2 - 8 = 217 = 10 \,(mod\ 23)$$

$$y_3 = 15(4-10) - 7 = -97 = 18 \,(mod\ 23)$$

所以$2P = (10,18)$。

第八節　植基於橢圓曲線的類 RSA 演算法

本節將介紹如何以橢圓曲線的方式，完成一個類似 RSA 的演算法，以下將逐步說明，關於數學定義請參照參考文獻[16]。

第一步—選擇兩個大質數 p 跟 q，令$n = p \cdot q$。

第二步—選擇一個橢圓曲線方程式$E: y^2 = x^3 + ax + b \,(mod\ n)$，滿足$gcd(4a^3 + 27b^2, n) = 1$。

第三步—令橢圓曲線的序(order)為$\left|E_p(a,b)\right| = 1 + p + \alpha$，$\overline{\left|E_p(a,b)\right|} = 1 + p - \alpha$，$\left|E_q(a,b)\right| = 1 + q + \beta$，$\overline{\left|E_q(a,b)\right|} = 1 + q - \beta$。

若要對文件 x 加密，以得到密文 s，則計算$(s,t) = (x,y)\#e \,(mod\ n)$。

若要對密文 s 解密，以得到明文 x，則計算$(s,t) = (x,y)\#d_i \,(mod\ n)$。

其中$(x,y)\#e$表示將點(x, y)乘上 e 倍，(d_i, e)為私密金鑰與公開金鑰，滿足$e \cdot d_i \equiv 1 (mod\ N_i)$，$gcd(e, N_i) = 1$，$1 \le i \le 4$。

$N_1 = lcm(1+p+\alpha, 1+q+\beta)$，$(\frac{w}{p})=1$ 且 $(\frac{w}{q})=1$；

$N_2 = lcm(1+p+\alpha, 1+q-\beta)$，$(\frac{w}{p})=1$ 且 $(\frac{w}{q})\neq 1$；

$N_3 = lcm(1+p-\alpha, 1+q+\beta)$，$(\frac{w}{p})\neq 1$ 且 $(\frac{w}{q})=1$；

$N_4 = lcm(1+p-\alpha, 1+q-\beta)$，$(\frac{w}{p})\neq 1$ 且 $(\frac{w}{q})\neq 1$。

$z \equiv x^3 + ax + b \,(mod\ n)$，$y = \sqrt{z}$；

$w \equiv s^3 + as + b \,(mod\ n)$，$t = \sqrt{w}$。

若要對文件 x 計算數位簽章 s，則計算 $(s,t) = (x,y) \# d_i \,(mod\ n)$。

若要驗證數位簽章 s，則計算 $(x,y) = (s,t) \# e \,(mod\ n)$。

第叁章　　應用視覺式秘密分享技術的電子現金模型

在這一章裡，我們將介紹我們所提出的電子現金系統架構，我們主要運用了指紋作為使用者身分辨識的依據，並且應用了視覺式秘密分享的技術，以保護消費者的指紋不被擷取濫用。

第一節　　簡介

本系統是以視覺式秘密分享技術來改善由 W. T. Lin 與 G. B. Horng 所提出的電子現金[4]，利用指紋作為消費者身分認證的依據，並且利用視覺式秘密分享技術來保護指紋。因為指紋是一項不可改變的生理特徵，如果在網路上不加以保護的傳送，容易成為犯罪者所覬覦的目標，而且一旦被盜用，對指紋的主人而言，將會是永遠的傷害。

在本架構中，假設可以合法擁有指紋紀錄檔的機構，只有政府單位，而這個政府單位必須負責維護全民指紋資料庫，只有指紋所有者本人得以申請取得在指紋資料庫中的資料；而這個全民指紋資料庫除了存放人民的指紋圖片之外，也必須具備視覺式秘密分享運算的能力。在銀行部分，我們採用的仍是現存的架構[4]，利用盲簽章的技術來製作電子現金，並且加入了視覺式秘密分享的技術對指紋加以處理保護，以強化系統的安全性與維護使用者的匿名性，並

保有指紋辨識認證使用者的特性。

系統架構如圖 3.1 所示，本系統包括了四個單位，分別為指紋資料庫、銀行子系統、消費者及網路商店；交易的流程包括了銀行子系統初始程序，視覺式秘密分享處理程序，電子現金製發程序，付款程序，指紋驗證程序及存款程序。

以下各節將介紹本系統中的各個子系統以及交易的流程。

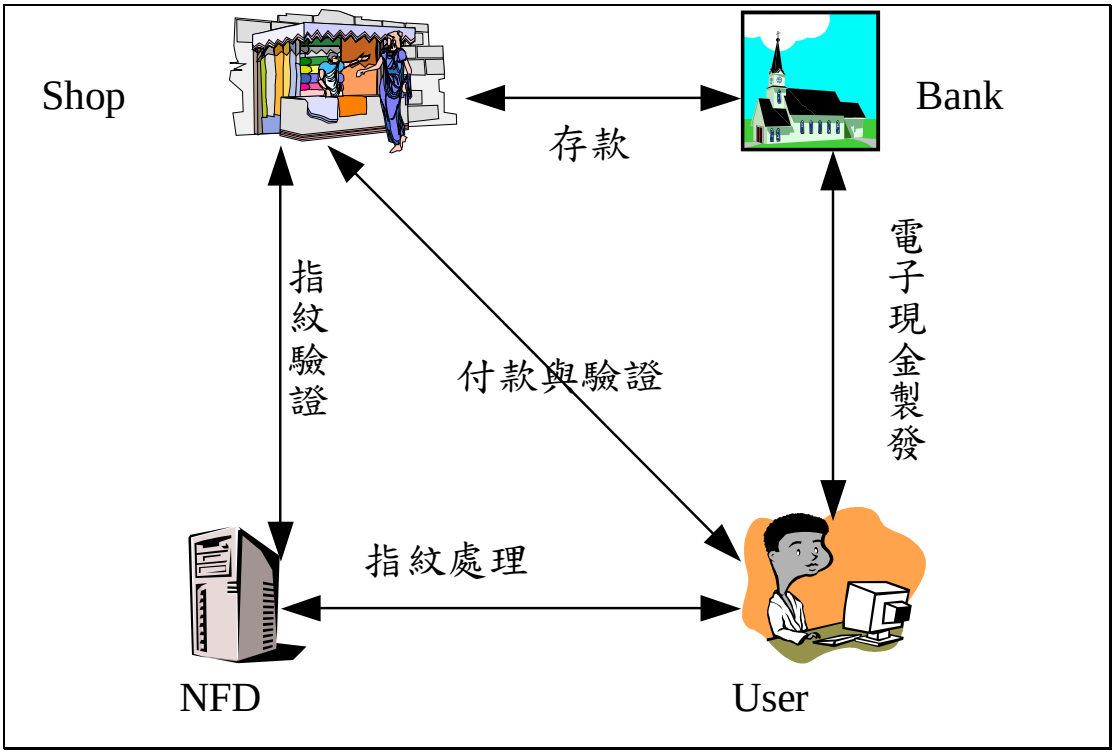


圖 3.1應用視覺式秘密分享技術的電子現金模型

第二節　　符號說明

一、NFD：由政府機關負責維護，儲存所有國民的指紋資料，並且根據使用者的請求，利用視覺式秘密分享的技術產生其指紋的子圖；

二、FPS#：經由視覺式秘密分享處理之後所產生的子圖，#表示 1 或 2；

三、EMSN：電子現金序號；

四、B(x,r)：表示將文件 x 利用盲因子 r 處理成為盲文件的過程，亦即表示$r^e H(x)$，e 是銀行的公開金鑰，H(x)為一單向雜湊函數；

五、S(x)：對文件 x 作數位簽章，亦即表示$s = H(x)^d \bmod n$，d 為銀行的秘密金鑰，n 為兩個大質數 p 和 q 的乘積；

六、V(S(x),e)：利用簽章者的公開金鑰 e 驗證數位簽章 S(x)，也就是計算$H(x) \stackrel{?}{=} S(x)^e \bmod n$；

七、U(x,r)：將盲文件 x 除以盲因子 r，得到一般的文件；

八、H(x)：單向雜湊函數；

第三節　視覺式秘密分享處理程序

針對使用者的指紋檔案作處理並加以保護，在本架構中我們僅需將指紋檔案經過視覺式秘密分享處理產生兩張子圖，一張藏在電

子現金內，另一張則與原來的指紋檔案一起存放在指紋資料庫中作為將來指紋比對之用。詳細的處理步驟列示如下：

第一步：將指紋檔案的每個圖素作編碼，編碼原則為黑色的圖素表示為(1111)，白色的圖素則可表示為(0111)、(1011)、(1101)、(1110)，(如圖 2.3)。

第二步：將每個圖素拆解為兩個子圖素，黑色圖素可以拆解成(1100)⊕(0011)、(1010)⊕(0101)或(1001)⊕(0110)，亦即圖 3.2 所示；白色圖素即可拆成任兩個不同群的子圖素組合，如圖 3.3 所示。

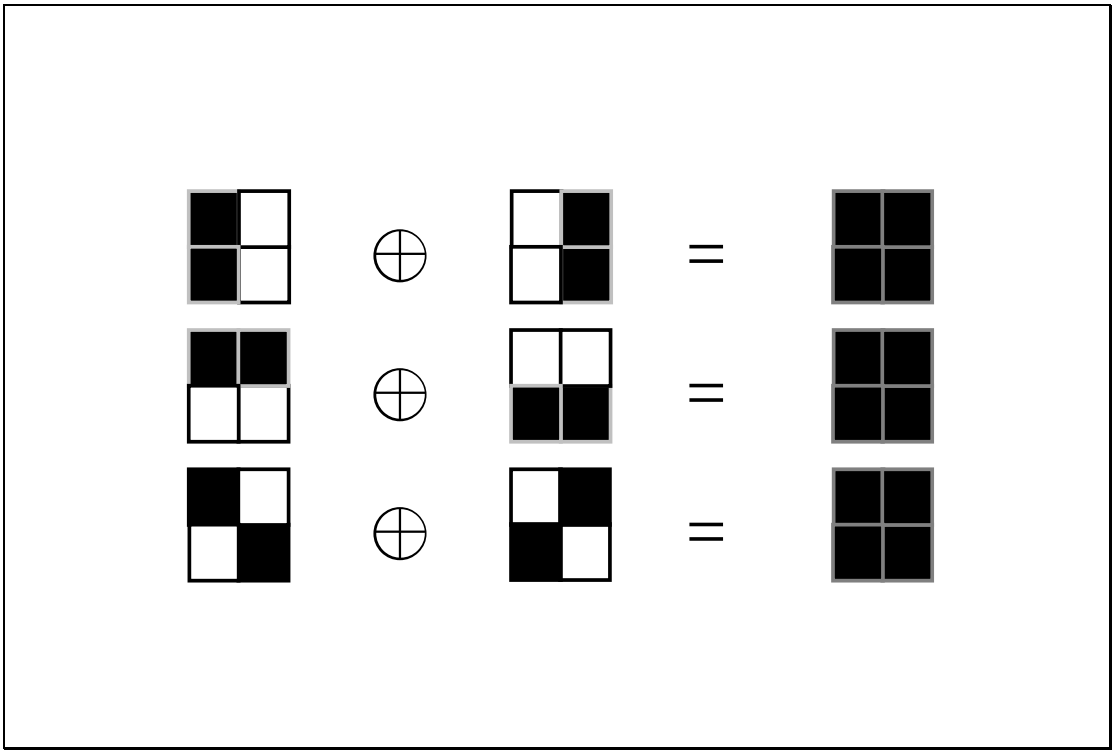


圖 3.2黑色圖素的拆解

如此一來，原來指紋圖檔中的每一個圖素分成了兩個子圖素，再儲存在兩個圖檔中的相對位置(FPS1 與 FPS2)，便完成了視覺式秘密分享的處理程序。

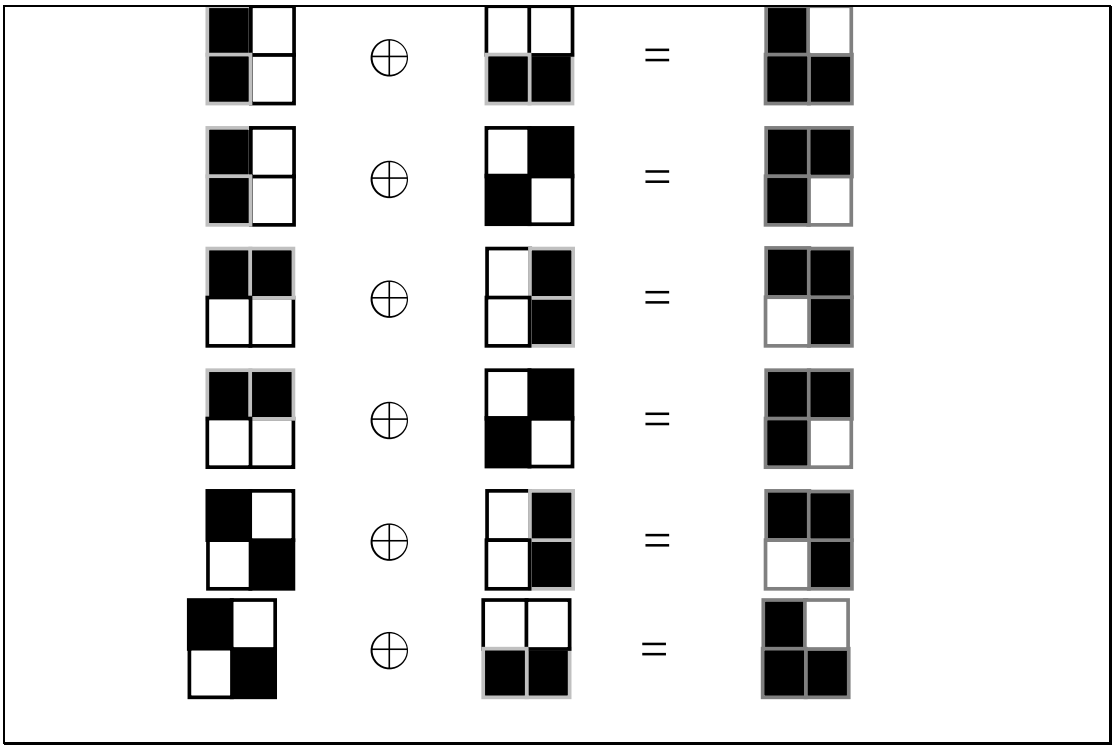


圖 3.3白色圖素的拆解

第四節　　銀行子系統

利用[12]提出的 RSA 加解密及簽章演算法作為銀行安全系統的架構，銀行產生專屬金鑰，(d，e)，作為電子現金數位簽章之用。

第五節　　電子現金製發過程

此節闡述使用者在申請電子現金之後，銀行產生電子現金的步驟，流程如圖 3.4 所示。

第一步—消費者必須先在銀行註冊一個帳號，由銀行產生一連串的電子現金序號，讓消費者隨機選取一個電子現金序號。

第二步—消費者隨機選取一個電子現金序號(EMSN)之後，再向 NFD 申請一份(2,2)的指紋視覺式秘密分享子圖，NFD 在認證消費者身分之後，根據消費者的請求，對消費者的指紋紀錄檔進行視覺式秘密分享處理程序，產生一份(兩張)視覺式秘密分享的子圖，把其中之一(FPS1)傳送給消費者，消費者將電子現金序號乘上一個盲因子 r 的 e 次方得到盲文件 $B(EMSN,r)=r^e \cdot EMSN$ ，跟指紋子圖 FPS1 一起傳送給銀行。

第三步—銀行收到消費者的指紋子圖及盲文件 B(EMSN, r)之後，對指紋子圖和盲文件 B(EMSN, r)做數位簽章並加上時戳 T，再將結果傳回給消費者。

第四步—消費者收到之後，將盲簽章除以 r，便得到可以使用的電子現金 S(EMSN, T, FPS1)。

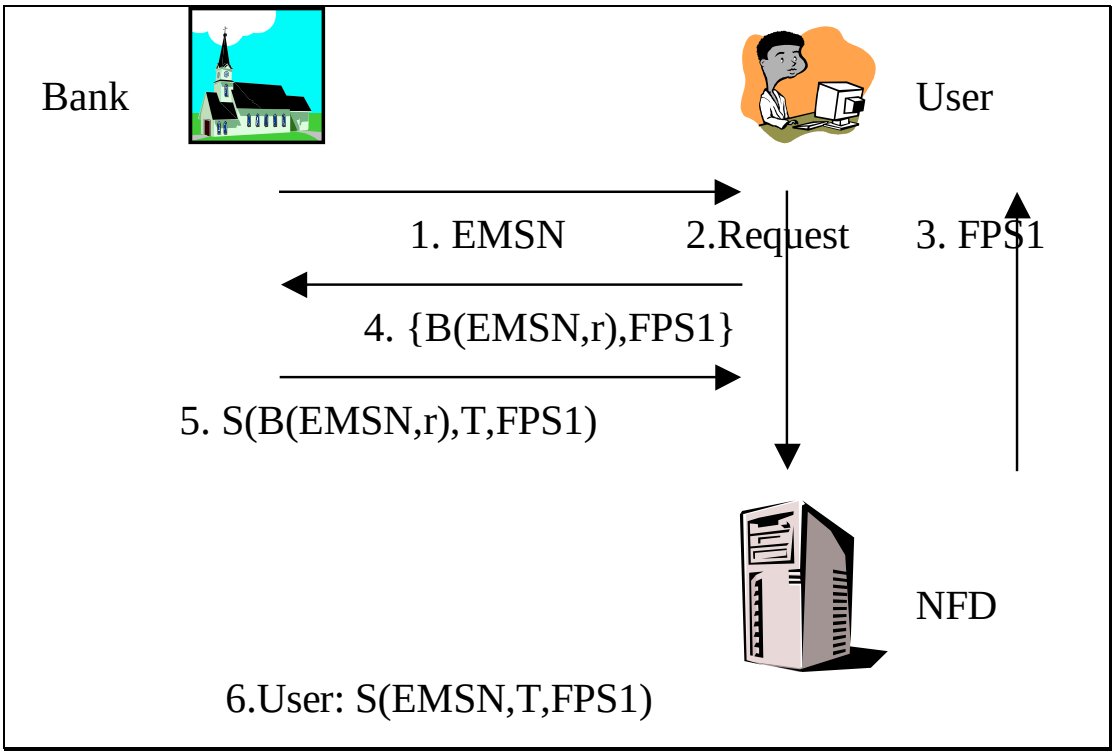


圖 3.4電子現金製發流程

第六節 付款過程

本節敘述消費者將電子現金付給商店與商店驗證電子現金的步驟。

第一步—消費者在認證過網路商店之後，以電子現金付款給網路商店，在傳送電子現金的同時，也把訂單(包括消費者的個人資訊)及消費者在付款時所按押的指紋以網路商店的公開金鑰加密之後一併傳送給網路商店。

第二步—網路商店在收到消費者送來的電子現金、訂單及加密

過的指紋之後，先驗證銀行的數位簽章及時戳，確定是合法的電子現金之後，再將指紋子圖 FPS1 從電子現金中取出來，加上解密之後所取得訂單中消費者的個人資訊(姓名、身分證號碼……)及使用者所按押的指紋，傳送到全民指紋資料庫中做疊合及比對等驗證程序。

第三步—全民指紋資料庫在收到網路商店要求認證的消費者資訊及指紋子片時，依據指紋子片中的序列號碼，取出相對應的另一張指紋子圖，將兩張指紋子圖疊合之後產生的新影像跟依據消費者資訊所搜尋到的指紋圖片做比對，如果符合，則回應網路商店符合的訊息；如果不符合，則回應不符合；比對完成之後，NFD 即把兩個指紋子圖銷毀。

第四步—網路商店在收到全民指紋資料庫的回應訊息之後，才通知消費者交易完成。

付款流程如圖 3.5 所示。

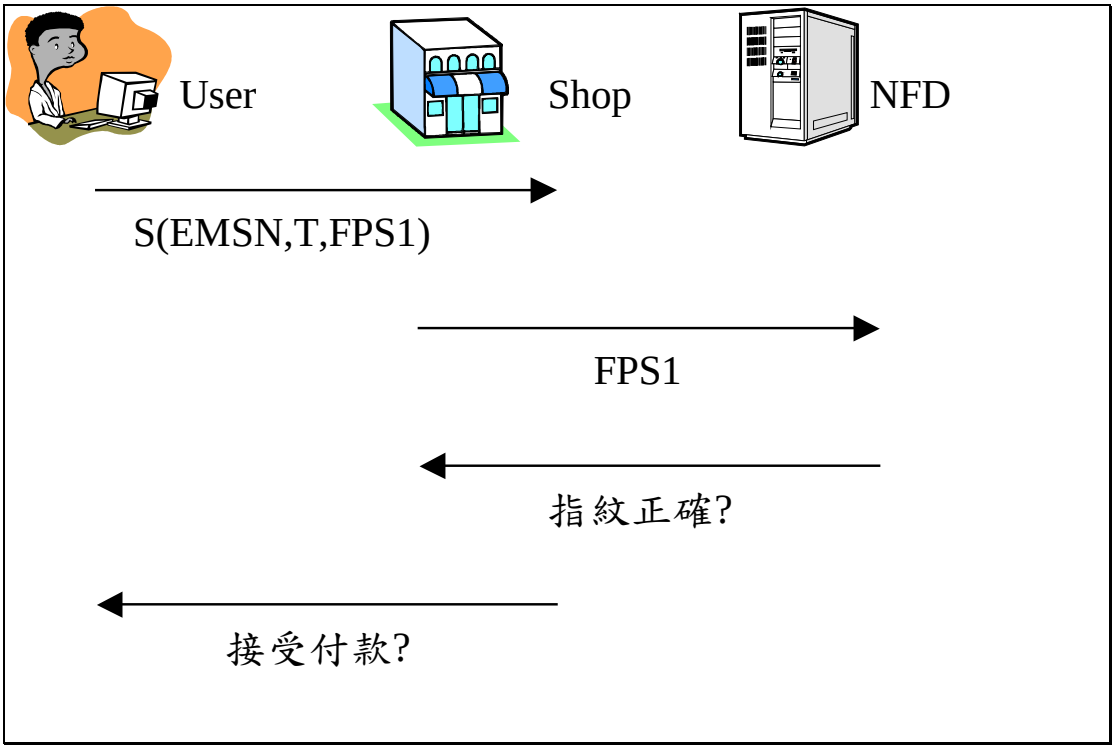


圖 3.5付款流程

第七節　　存款協定

本節敘述商店將電子現金存入銀行與銀行驗證的步驟。

第一步—網路商店只要將電子現金(S(EMSN,T,FPS1))及網路商店本身的帳號傳給銀行。

第二步—銀行在收到之後，驗證銀行本身的數位簽章，最後再驗證時戳，驗證通過之後即可將金額存入網路商店的帳號中，並通知商店存款已經完成。

存款流程如圖 3.6 所示。

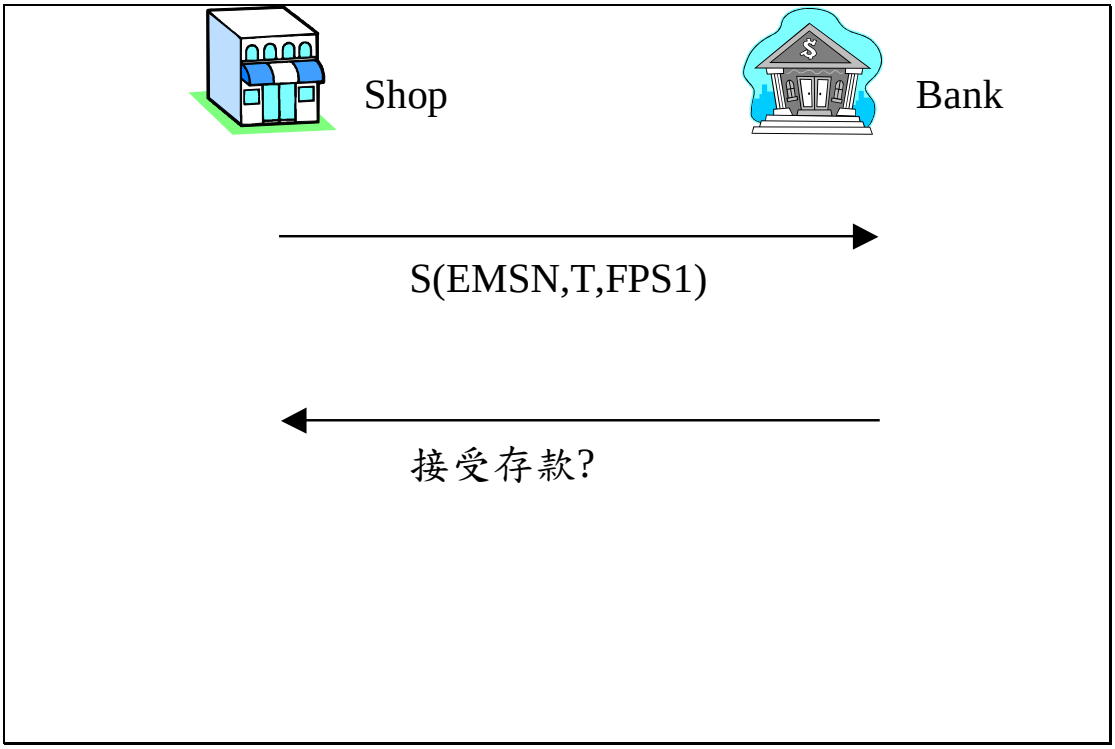


圖 3.6存款流程

第八節　　安全性分析

針對這個所提出的電子現金架構，我們以第貳章第三節所介紹的理想電子現金特性為基礎，做一個安全性的分析。

首先以獨立性而言，本架構所提出的電子現金不需要依賴任何其他的媒介，便能夠在網路上安全的傳輸，本架構所提出的電子現金便是一種可以在網路世界中流通的貨幣。

針對安全性而言，我們所提出的架構可以藉由數位簽章的保護而避免被偽造，更因為加上了指紋的部分資訊使得偽造的難度更加

提昇；在避免重複使用的問題上，我們套用了離線模式的驗證方式，可以避免銀行部分成為整個架構的瓶頸，在驗證的時候，也因為指紋的資訊在第一次使用時便遭刪除，因此也更提昇了重複使用的難度；在避免盜用的問題上面，我們藉由指紋的唯一性，達到消費者身分與申請者身份的比對，因此可以避免電子現金遭到申請者以外的其他人使用，簡單的說就是可以避免電子現金被其他人盜用。

在指紋的保護方面，我們顧慮到指紋對一個人而言，具有不可取代的特性，也就是說指紋可以代表一個人，因此在法律上，指紋也是一個判斷身份的依據，所以對於指紋，並不適合在未經任何保護處理的狀態下在網路世界中傳遞，因此我們應用了視覺式秘密分享的方式，將指紋做一番處理之後才在網路上傳遞，所傳遞的資訊，並不足以代表一個完整的指紋，因此有心人士並不能在網路上盜取任何人的指紋做任何用途，這也是本架構的精神所在。

以匿名性而言，本架構採取了一般電子現金架構最常應用的盲簽章技術，透過盲簽章的方式，銀行並無法得到電子現金序號與使用者之間的關係；在指紋驗證方面，雖然我們以指紋驗證作為使用者身分認證的依據，但銀行只能得到一份經過視覺式秘密分享處理過的子圖，這個部分的資訊並不足以代表使用者的指紋，所以可以

確保使用者的匿名性無虞。

至於離線付款方面，我們可以在電子現金上加入一個觀察者模組，專門用來記錄每筆電子現金交易的過程，以達到離線付款的要求。

在所有權轉移部分，我們提出的架構主要是避免電子現金遭到盜用的問題，為了解決盜用的問題，我們採用了指紋辨識技術作為使用者身分認證的方式，但是使用者無法自行變更藏在電子現金中的申請者指紋，所以我們的系統並無法達到理想電子現金中的可傳輸性要求，然而在一般的小額付款系統中，所有權轉移並非是一個必要的特性，所以我們以防止盜用的特性來替代所有權轉移。

在可分性部分，在現實世界中的貨幣是可以找零的，這可以找零的特性便是可分性，而在一些已提出的電子現金系統的架構中，都是把電子現金的面額設計成最小的單位電子現金，因此不需要考慮到可分性，本論文的主要精神是著眼於防止盜用的特性上，因此我們所提出的電子現金面額也是最小的單位，或稱為單位電子現金。

在條件稽核與災難復原這兩個特性上，本系統架構並沒有特殊的考量；以條件稽核來說，主要是以有條件的法律特權，使得電子現金得以破壞匿名性達到追蹤的目的，然而本系統是以使用者的權

利為出發點，因此並不提供條件稽核的特性。

以災難復原而言，是希望使用者能在匿名的狀態下，依據電子現金的殘餘部分，得以申請換發新的電子現金，然而本系統提出的電子現金是以電子檔案的形式存在於使用者的電腦系統之中，並不足以提供一個可靠的、可以衡量電子現金的完整性的系統架構，所以本系統並無法讓使用者有災難復原的功能，而且，本系統主要的用途是在小額付款，因此，災難復原的特性不是系統最主要的考量。

第肆章　　整合智慧卡與驗證技術的電子現金系統

在本章中，我們將電子現金整合了通行碼驗證與智慧卡[3]的技術，希望能夠加強原有系統的安全性，並且利用智慧卡的方便性，提昇電子現金系統的可用性，當然，防止電子現金被盜用，仍然是我們主要的目的；本章提出的現金架構，主要是以通行碼驗證的方式來達成這個目的。以下我們將從系統的流程作介紹。

第一節　　系統介紹

本章所提的架構主要是結合了通行碼驗證[3]的方式，以達到簡單的使用者驗證的目的。藉由銀行擔任發行智慧卡與電子現金的單位，發行使用者所需的電子現金，並且利用智慧卡的運算能力與儲存空間，使得電子現金可以達到防止盜用的目的。圖 4.1 為本系統的架構圖。

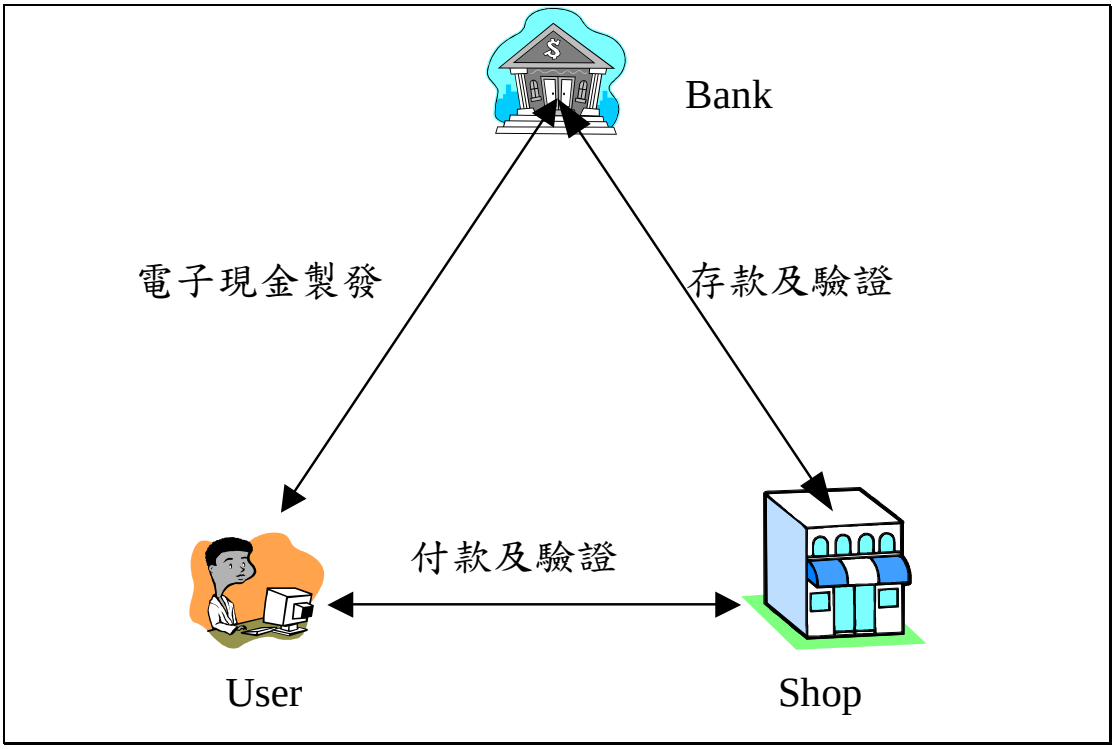


圖 4.1 系統架構圖

第二節　初始設定

本節敘述銀行在發行電子現金的過程中，必須事先準備的參數，在此主要是指銀行用來做數位簽章的金鑰對，在本架構中所使用的數位簽章演算法為 RSA。

一、銀行任選兩個大質數 p 和 q，並計算 $n = p \cdot q$；

二、在 GF(p)和 GF(q)的 primitive element 中找一個 g；

三、任選 d 為銀行的私密金鑰，並計算對應的公開金鑰 e，使滿足 $d \cdot e \bmod (p-1) \cdot (q-1) = 1$。

第三節　　電子現金發行程序

本節是在描述消費者向銀行申請電子現金的過程與銀行製造電子現金的步驟。當消費者向銀行提出電子現金的申請時，消費者必須先向銀行註冊專有的 ID 以及相對應的通行碼。主要步驟列示如下：

第一步—消費者向銀行註冊申請電子現金；

第二步—銀行產生多組序號傳送給消費者；

第三步—消費者任選一組序號 m，並計算 $B(m,r)=r^e \cdot m$，(r 為消費者任選的亂數，e 是銀行的公開金鑰)；

第四步—消費者任選認證碼 PW，並計算 $PW'=PW^e \bmod n$，將 B(m,r)及 PW’傳給銀行；

第五步—銀行計算 $BS=(B(m,r))^d \bmod n = r \cdot m^d \bmod n$，$PW=(PW')^d \bmod n$，接著計算 $h=g^{PW \cdot d} \bmod n$；

第六步—銀行將準電子現金(n, e, g, BS, h)傳送給消費者；

第七步—消費者計算 $S=BS/r$，得到電子現金(n, e, g, m, S, h)。

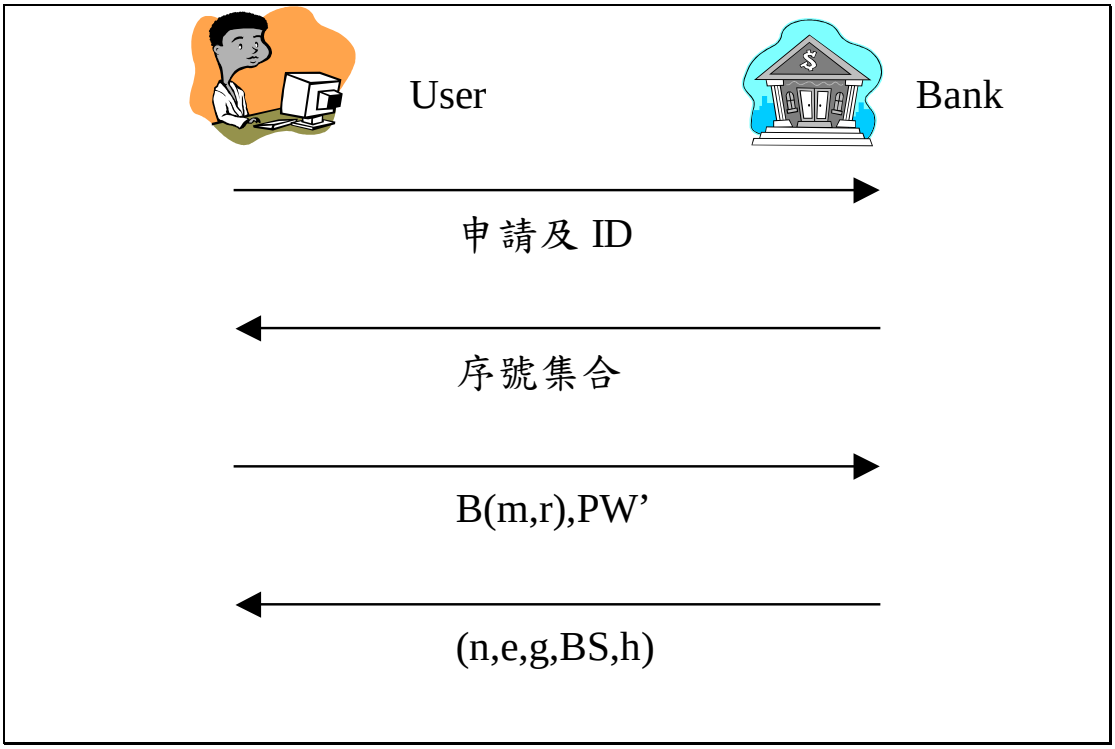


圖 4.2電子現金製發流程

第四節　　付款程序

本節是在敘述消費者在網路上購物之後，利用電子現金作為交易工具，並以電子現金支付帳款給網路商店，以下便是消費者將電子現金付給網路商店的步驟。

第一步—消費者計算 $X = g^{r' \cdot PW''} \bmod n$，PW”是消費者在付費時輸入的認證碼，r’是消費者任選的亂數；

第二步—消費者計算 $Y = S \cdot h^{r' \cdot T} \bmod n$，T 是當時的時戳；

第三步—消費者將(m, X, Y, n, e, g, T, S)傳給網路商店。

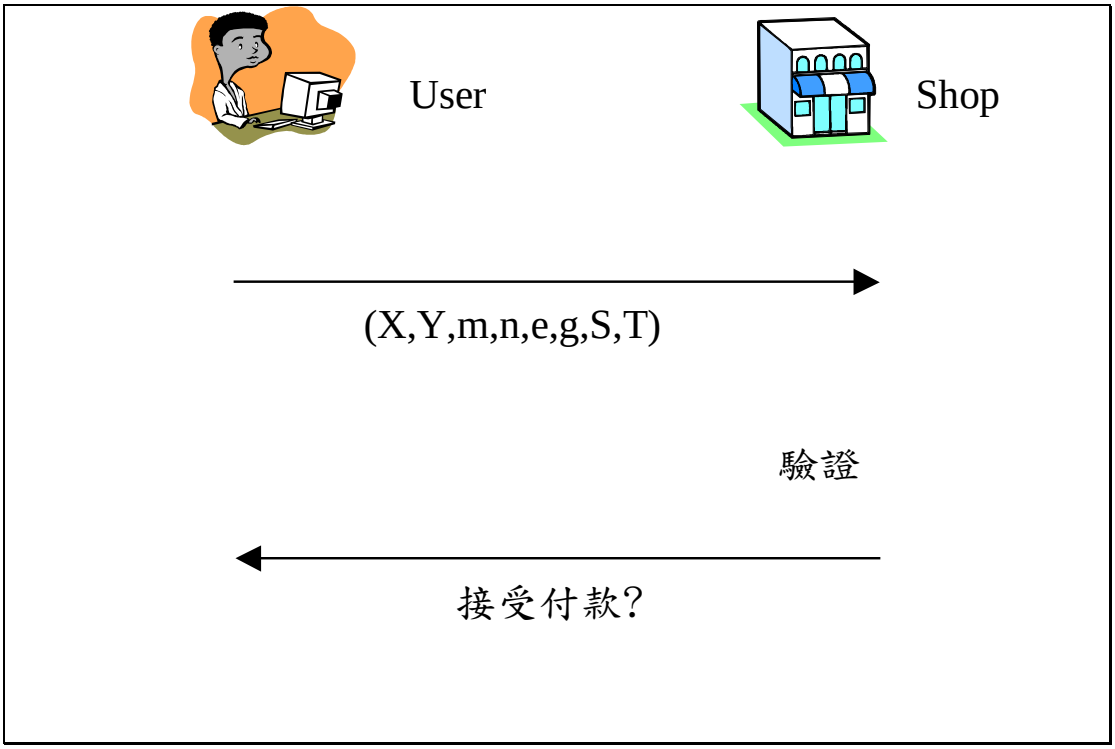


圖 4.3付款流程

第五節　　網路商店驗證程序

本節主要是介紹網路商店在收到電子現金之後，對電子現金及消費者進行的驗證步驟，主要目的是確保電子現金的可用性以及電子現金的申請者與消費者的身分，以下便是驗證的程序。

第一步—檢查 m 及 T 是不是正確的格式；

第二步—計算 $S^e \stackrel{?}{=} m \bmod n$ 等式是否成立；

第三步—比對收到電子現金的時間 T'與使用者傳送的 T 是不是在合理範圍內；

第四步—計算 $Y^e \stackrel{?}{=} m \cdot X^T$ 等式是否成立；

以上檢查通過後，商店便可以相信消費者送來的電子現金是合法的電子現金，並且消費者是電子現金合法的擁有者。

第六節　存款程序

網路商店在累積了許多電子現金現金之後，便必須把電子現金存入銀行帳戶，並轉換成其他形式的貨幣供網路商店做其他用途；本節即是在說明網路商店如何將電子現金存入銀行以及銀行驗證電子現金的步驟。

第一步—商店將(S, m)傳送給銀行；

第二步—銀行計算 $S^e \stackrel{?}{=} m \bmod n$ 等式是否成立；

第三步—銀行檢查資料庫中是否有 m 的紀錄；

以上檢查過後，銀行便可以相信電子現金是合法發行的，並且沒有重複使用的疑慮，最後把電子現金的款項存入網路商店的帳號中。

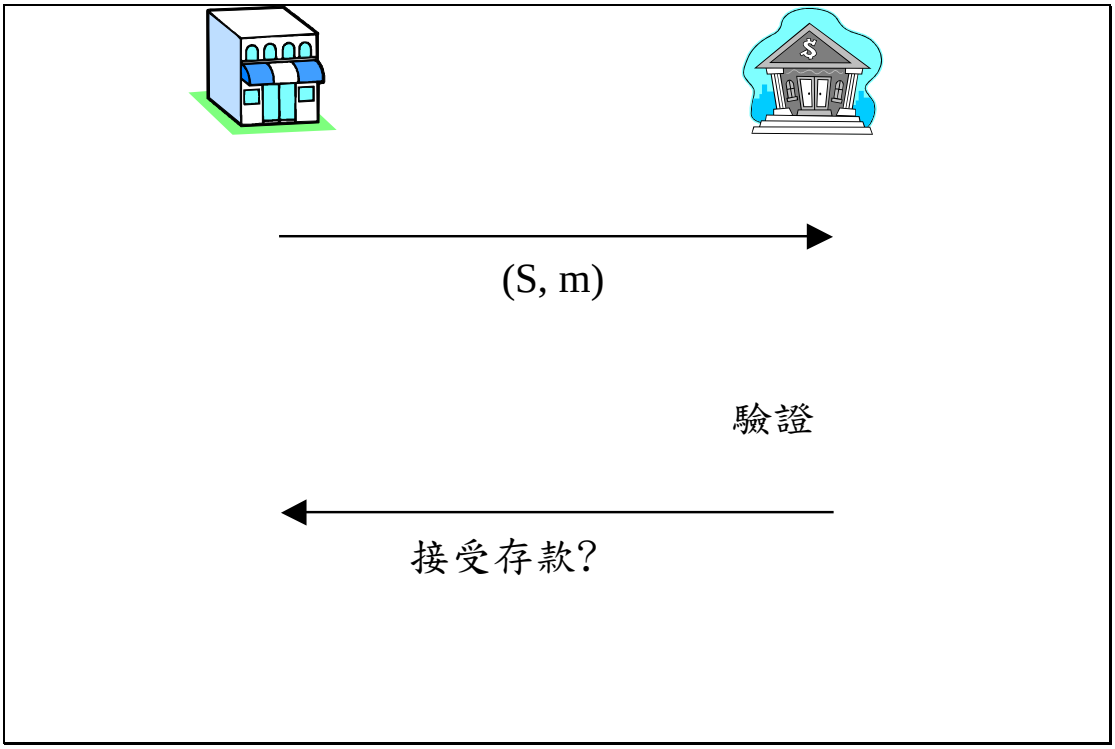


圖 4.4存款流程

第七節　　安全性分析

本節所做的安全性分析，主要是以第貳章介紹的理想電子現金特性為依據，並且加入了本論文所提出的主要精神—防止盜用的特性，以下我們便針對理想特性做安全性分析。

首先以獨立性而言，本章所提出的電子現金架構結合了智慧卡的物理特性，雖然獨立性不足，可是以智慧卡的便利及安全性，使我們對電子現金的使用及便利性得到提昇，因此我們仍然選擇了結合智慧卡的方式，讓電子現金的特性更加提昇；再者，本架構提出

的電子現金雖然是儲存在智慧卡上面，但是在消費者付款給商店及商店到銀行存款時，都是以網路資料的型態在做傳遞，因此我們還是可以說，本章所提出的架構仍然是保有獨立性的。

在安全性的考量方面，在理想的電子現金特性中提出了防止偽造及防止重複使用，我們另外將防止盜用也加入了安全性考量，以下我們將以本章所提出的電子現金架構，針對這些安全特性做一番討論。

在防止偽造方面，我們延續了一般電子現金所使用的數位簽章方式，確保銀行的數位簽章無法偽造，即可保障電子現金不會被偽造；在防止重複使用方面，藉由銀行維護紀錄已經使用的電子現金序號的資料庫，便可以避免電子現金被重複使用；在防止盜用部分，藉由使用者通行碼驗證的方式可以達到確認消費者身份的目的，藉以達到非註冊的使用者無法以該電子現金消費。

在匿名性部分，我們在電子現金的製發過程中，可以看出電子現金是由銀行產生許多序號再由使用者任意選擇其中一組，透過盲簽章的方式，使得銀行方面無法建立電子現金序號與使用者之間的連結，因此可以確保使用者的匿名性。

在離線付款方面，我們可以在電子現金上加入一個觀察者模組，專門用來記錄每筆電子現金交易的過程，以達到離線付款的要

求。

在所有權轉移部分，本章所提出的架構中，使用者雖然可以任意將通行碼洩漏給任何人，但是銀行只能確認通行碼是否正確，但無法得知註冊者與使用者是否為同一人，因此本架構並不支援理想電子現金中的所有權轉移。

本章所提電子現金架構，把發行的電子現金金額都定義為單位電子現金，因此不需要考慮理想電子現金中的可分性；至於災難復原與條件稽核都不是本論文的主要考量，因此本電子現金架構暫時不將這兩個理想特性列入考慮。

第伍章　　植基於橢圓曲線的電子現金系統

本章主要是以橢圓曲線的方式改良第肆章所提出的電子現金架構，透過橢圓曲線的運算可以有效改善原本的系統效率，改善的方式是以橢圓曲線的點運算取代原本系統所使用的 RSA 大數運算，橢圓曲線的加解密及數位簽章的方式已經被證明比原來的 RSA 演算法安全性還要好[16,17,18,19,20,21,22]。

第一節　　系統介紹

本章所提出的電子現金架構與第肆章所提出的架構相同，主要差異在第肆章所運用的計算方式是植基於 RSA 的大數運算，而本章所使用的是橢圓曲線的點運算，橢圓曲線的加解密及簽章方式不但可以達到比 RSA 演算法更好的安全性下，也大幅提昇運算的效能。

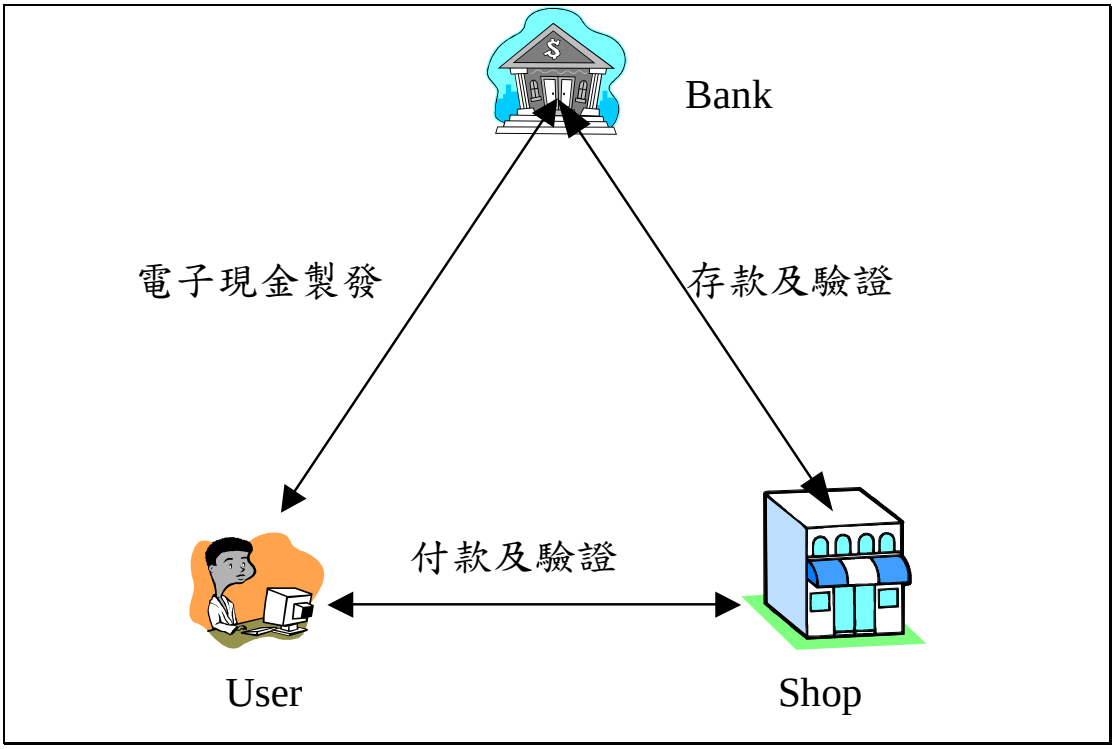


圖 5.1 系統架構圖

第二節　　初始設定

本節主要是介紹銀行在製發電子現金之前所必須準備的系統參數，主要包括了下列幾種：

一、銀行任選兩個大質數 p 跟 q，並計算 $n = p \cdot q$。

二、銀行選擇一個橢圓曲線 $E: y^2 = x^3 + ax + b \,(mod\ n)$，$4a^3 + 27b^2 \neq 0$。

三、銀行產生金鑰對(d,e)作為簽章之用。

四、銀行在橢圓曲線上任選一點 g 作為起始點。

第三節　　電子現金製發程序

本節是敘述當消費者向銀行申請電子現金時，銀行與消費者之間如何共同產生電子現金。

第一步—消費者向銀行申請電子現金。

第二步—銀行準備多個電子現金序號供消費者選擇，這些序號必須是橢圓曲線上的點集合。

第三步—消費者產生自己的金鑰對(d',e')，作為加解密之用。

第四步—消費者在銀行準備的電子現金序號之中任意選擇一個 m，並以消費者本身的公開金鑰 e'對 m 加密，得到 $m' = m \# e' \ (mod\ n)$。

第五步—消費者選擇一個通行碼 PW，並用銀行的公開金鑰 e 對 PW 加密，得到 $PW' = PW \# e \ (mod\ n)$。

第六步—消費者將 m'及 PW'傳送給銀行。

第七步—銀行用本身的私密金鑰 d 將 PW'解密，得到 PW；再用本身的私密金鑰 d 對 m'簽章，得到 $m'' = m' \# d \ (mod\ n)$；最後計算 $h = g \# (PW \cdot d) \ (mod\ n)$。

第八步—銀行將(n, e, g, E, m", h)寫入智慧卡，並將智慧卡交給使用者。

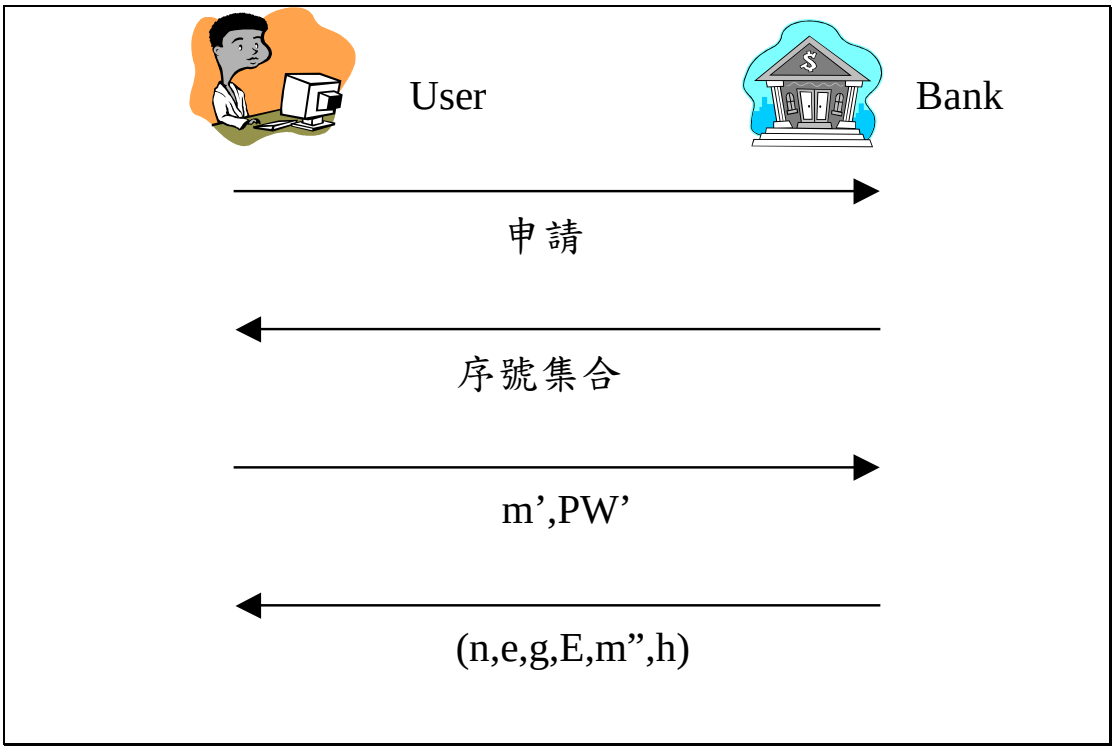


圖 5.2電子現金製發流程

第四節　　付款程序

接下來本節介紹消費者拿到隱含電子現金的智慧卡之後，如何與網路商店進行交易的過程。

第一步—消費者將智慧卡插入讀卡機，並且輸入通行碼 PW"。

第二步—智慧卡計算 $m''' = m'' \# d' \pmod{n} = m \# d \pmod{n}$，d'是消費者的私密金鑰。

第三步—智慧卡計算 $X \equiv g \# (r \cdot PW'') \pmod{n}$，r 是智慧卡產生

的亂數。

第四步—智慧卡計算 $Y \equiv m''' \cdot (h\#(r \cdot T))(mod\ n)$，T 是當時的時間點。

第五步—智慧卡將(n, e, g, E, X, Y, m’”, T)傳送給網路商店。

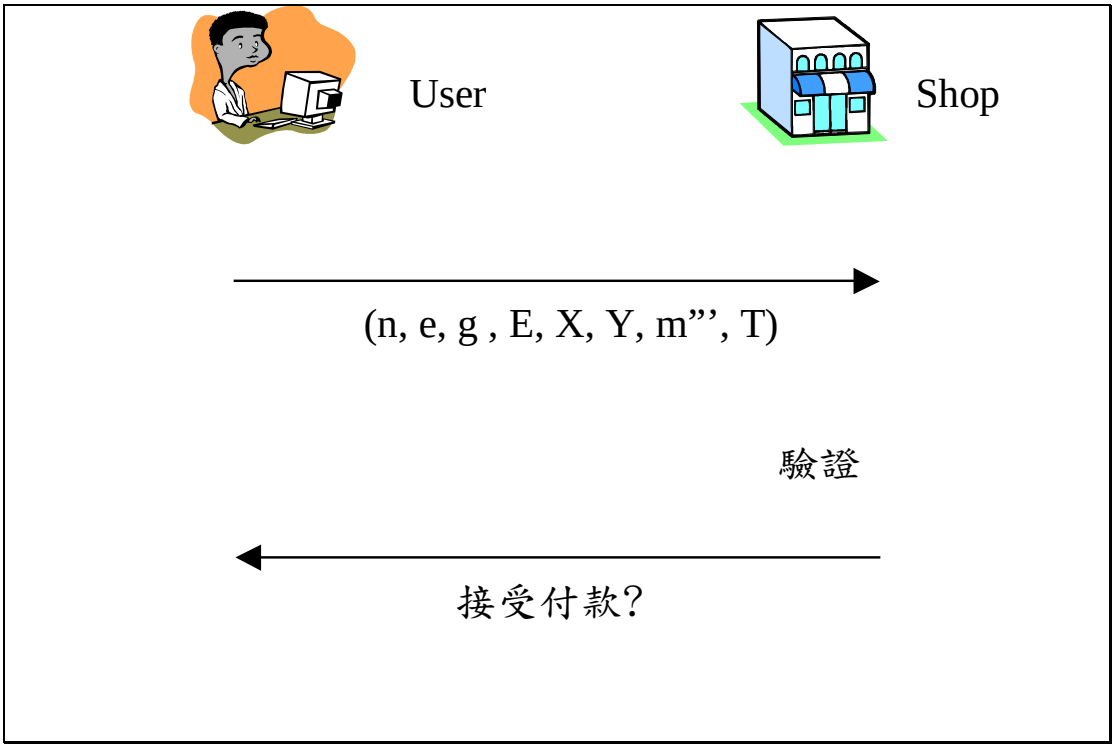


圖 5.3付款程序

第五節　網路商店驗證程序

這一節是說明網路商店如何驗證所收到的電子現金。

第一步—網路商店檢查收到(n, e, g, E, m’”, T)的時間點 T’與 T 是否在合理的時距內。

第二步—網路商店驗證 m”’是不是銀行發行的合法簽章。

第三步—網路銀行驗證$Y\#e\stackrel{?}{=}m\cdot(X\#T)(mod\ n)$。

第四步—以上驗證皆無誤後，網路商店通知消費者已經收到該筆電子現金，並結束交易。

第六節　存款程序

此節說明在網路商店累積一定數量的電子現金之後如何將電子現金存入銀行的步驟。

第一步—網路商店將把電子現金 m”’傳送給銀行。

第二步—銀行驗證 m”’是否為正確的數位簽章。

第三步—銀行檢查此筆電子現金是否為重複使用。

第四步—所有驗證無誤後，將此筆電子現金的金額存入網路商店的帳戶，並且紀錄此筆電子現金的序號，通知網路商店存款完成。

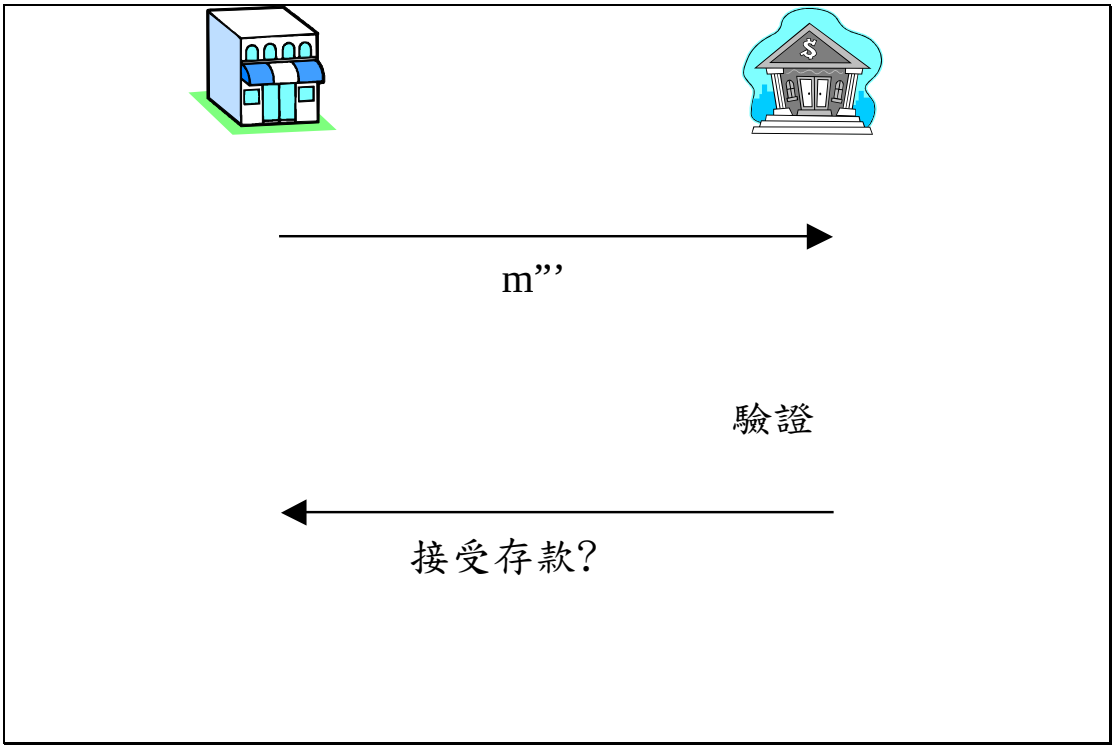


圖 5.4存款流程

第七節　　正確性分析

由於本章提出的電子現金架構跟第肆章所提的架構是一樣的，因此跟第肆章所提出的電子現金架構的安全性是一樣的，因此本章不再針對安全性做分析。

本章所使用的橢圓曲線方式已經大幅改變了原本第肆章中的驗證方式，為求正確起見，本節將簡單證明在本章所使用到的驗證方式，$m''' = m''\#d' \pmod n = m\#d \pmod n$ 與 $Y\#e \stackrel{?}{=} m\cdot(X\#T) \pmod n$。

首先證明 $m''' = m\#d \pmod n$：

因為 $m' = m\#e' \ (mod\ n)$，

並且 $m'' = m'\#d \ (mod\ n)$，

$\therefore m''' = m''\#d' \ (mod\ n)$

$= (m'\#d)\#d' \ (mod\ n)$

$= ((m\#e')\#d)d' \ (mod\ n)$

$= m\#d \ (mod\ n)$。

接下來證明 $Y\#e \stackrel{?}{=} m \cdot (X\#T) \ (mod\ n)$：

因為 $X \equiv g\#(r \cdot PW') \ (mod\ n)$，及 $Y \equiv m''' \cdot (h\#(r \cdot T)) \ (mod\ n)$，

並且 $h = g\#(PW \cdot d) \ (mod\ n)$，

$m''' = m\#d \ (mod\ n)$，

$\therefore Y\#e = ((m\#d) \cdot (h\#(r \cdot T)))\#e \ (mod\ n)$

$= m \cdot g\#(PW \cdot r \cdot T) \ (mod\ n)$

$= m \cdot X\#T \ (mod\ n)$。

第八節　效能分析

本章利用了橢圓曲線的點運算，將原本系統所使用的 RSA 大數冪次方運算，有效的將原有系統的冪次方運算的負擔減輕為點的運算，在新的系統中完全沒有使用到大數的冪次方運算，以下我們將列表檢視兩個系統間的效能差異。

	第肆章架構	第伍章架構
電子現金發行程序中消費者的計算量	$B(m)=r^{e}\cdot m$	$m'=m\#e'\ (mod\ n)$
	$PW'=PW^{e}\ mod\ n$	$PW'=PW\#e\ (mod\ n)$
電子現金發行程序中銀行的計算量	$BS=B(m)^{d}\ mod\ n$	$m''=m'\#d\ (mod\ n)$
	$PW=(PW')^{d}\ mod\ n$	$PW=PW'\#d\ (mod\ n)$
	$h=g^{PW\cdot d}\ mod\ n$	$h=g\#(PW\cdot d)(mod\ n)$
付款程序中智慧卡的計算量	$X=g^{r'\cdot PW''}\ mod\ n$	$X=g\#(r\cdot PW'')(mod\ n)$
	$Y=S\cdot h^{r'\cdot T}\ mod\ n$	$Y=m'''\cdot(h\#(r\cdot T))(mod\ n)$
網路商店驗證時的計算量	$S^{e}\stackrel{?}{=}m\ mod\ n$	$m'''\#e\stackrel{?}{=}m\ mod\ n$
	$Y^{e}\stackrel{?}{=}m\cdot X^{T}$	$Y\#e\stackrel{?}{=}m\cdot(X\cdot T)(mod\ n)$
存款時銀行的計算量	$S^{e}\stackrel{?}{=}m\ mod\ n$	$m'''\#e\stackrel{?}{=}m\ mod\ n$

表 5.1 系統效能比較

第陸章　　結論及未來發展

本章將對本論文所提出的三個電子現金架構：應用視覺式秘密分享的電子現金模型，整合智慧卡與驗證技術的電子現金系統，與植基於橢圓曲線的智慧卡與驗證技術的電子現金系統，做個簡單的比較與結論；並且對電子現金未來可能的應用與發展，做個簡單的介紹。

第一節　　結論

本論文提出的三個電子現金系統：應用視覺式秘密分享的電子現金模型，整合智慧卡與驗證技術的電子現金系統，與植基於橢圓曲線的智慧卡與驗證技術的電子現金系統，主要是針對電子現金能不能防止被擁有人之外的其他人盜用的特性做設計。

在第一個系統中，主要是透過指紋辨識的方式來驗證消費者的身分，除了申請者本人之外，任何人都無法使用這筆電子現金，雖然是違反了理想電子現金中的可傳輸性，但是基於對使用者財產的保護，使得電子現金在使用上的便利性受到限制，應該是可以被接受的。而指紋是屬於人類不可改變之生理特徵，如果指紋遭到其他人的竊取濫用，對於使用者而言，是一個無法挽回的錯誤，並且將對使用者的名譽及財富產生不可預期的破壞，因此在這個架構之中

我們整合了視覺式秘密分享的方式來保護使用者的指紋，使得使用者的指紋沒有遭竊之虞。

在第二個系統之中，則是利用常見的通行碼驗證技術來確保使用者是否有權使用這筆電子現金作為交易之用，比較特殊的是，這種通行碼驗證的方式，在不需要經過原註冊單位的協助之下，即可完成通行碼驗證的程序，對於網路交易來說是個相當重要的議題，因此我們應用這種方式，來達到我們所提出的電子現金系統的需求，但是這個通行碼驗證的架構在實際運算上，卻有太多的大數冪次方運算，對於智慧卡的運算能力是個不小的負擔，因此我們便試著利用橢圓曲線的方式，來改善系統的效能。

在第三個系統之中，我們成功的應用了橢圓曲線的方式完成了電子現金系統，利用橢圓曲線的點運算以及橢圓曲線的加解密和數位簽章演算法，取代了原來第二個系統中的 RSA 運算，加強了系統的效能，並且能保有原系統的安全性。

在本論文中，應用了不同的方式達到相同的需求，雖然目的一樣，卻是整合了多種資訊安全的理論與技術，在電子現金的研究上，也提供了許多研究的方向，應該是本論文最大的貢獻吧。

第二節　未來發展

對於本研究的相關發展，仍然有許多值得深入的課題可以繼續探討，在此提供幾點以供參考：

理想的電子現金應具備有八點要素，是不是還有其他傳統貨幣的特性與優點應該加入？

當大量的電子現金在網路上傳輸，如何減少電子現金的資料量以達到快速安全的目的？

電子現金除了在電子商務系統中充當交易的媒介，是不是可以取代傳統貨幣的地位，進而將貨幣的發展進一步邁向無現金社會？

電子現金的發行會對現有經濟體系造成什麼樣的影響？應該如何管制電子現金的發行量？應不應該對電子現金的交易課稅？

電子商務已經是今日網路發展的當紅課題，在電子商務之中，當下最重要的工作就是推廣網際網路商業行為及發展安全可靠的電子給付系統。目前在網路上的電子給付系統大致可分為三類，電子信用卡系統，電子支票系統，及電子現金。其中又以電子現金最為重要，因為只有電子現金可以保有匿名的特性。

一般來說，電子現金是經過加密、數位簽章等處理的數字或位元資料，利用這些密碼學的方法以期達到電子現金應具備的安全性及匿名性等特質，而依其付款形式可分為連線模式及離線模式。

本研究針對偽造、重複消費等安全性問題，以及考慮了電子現

金不應該被偷竊，而提出了一個具有防盜用特性的電子現金系統，這個系統可以在保有匿名性的情況下，也具備了驗證使用者身分的功能。

另外電子現金的技術又可以應用在無記名電子投票、電子競標系統等。

參考文獻

[1] C.H. Lin and K.H. Yang, “An Electronic Cash System Using Visual Secret Sharing Technology,” Journal of Internet Technology, Special Issue on TANET 2000 Conference, Vol.2, No.1, January 2001, pp. 75-80.

[2] M. Naor and A. Shamir, “Visual Cryptography,” Advances in Cryptology-EUROCRYPT ’94, Lecture Notes in Computer Science, Springer-Verlag, 1995, pp. 1-12.

[3] W.H. Yang and S.P. Shieh, “Password Authentication Schemes with Smart Cards,” Computers & Security, vol. 18, no. 8, 1999, pp. 727-733.

[4] W. T. Lin and G. B. Horng, “Using Biological Recognition Technology to Prevent Double Spending over Networks,” the 9th International Security conference, 1999, pp. 58-65.

[5] D. Chaum, ”Blind Signatures for Untraceable Payments,” Advances in Cryptology-CRYPTO 82, 1983, pp. 199-203.

[6] D. Chaum, A. Fiat and M. Naor, “Untraceable Electronic Cash,” Advances in Cryptography – CRYPTO 88-, Springer-Verlag, 1990, pp. 319-327.

[7] Hal Finny, “Digital Double-Spending,” http://www.portal.com/~hfinny/chcash2.html.

[8] N. Ferguson, “Single-Term Off-line Cash Coin,” Advances in Cryptology – EUROCRYPT 93, pp. 318-328.

[9] A. Shamir, “How to Share a Secret,” Communication of the ACM, Vol. 22, 1979, pp. 612-613.

[10] G. R. Blackly, “ Secure guarding Cryptographic Keys,” AFIPS Conference Proceedings, Vol. 48, 1979, pp. 313-317.

[11] Time Magazine, May 4, 1992, pp. 13.

[12] R. L. Rivest, A. Shamir, and L.M Adleman,”A Method for Obtaining Digital Signatures and Public-Key Cryptosystem,” Communications of the ACM, Vol. 21, No. 2, Feb 1978, pp. 120-126.

[13] R. L. Rivest, A. Shamir, and L.M Adleman, ”On Digital Signatures and Public Key Cryptosystems,” MIT Laboratory for Computer Science, Technical Report, MIT/LCS/TR-212, Jan 1979.

[14] R. Rivest, M.J.B. Robshaw, R. Sidney, Y.L. Yin, “The RC6 Block Cipher,” http://theory.lcs.mit.edu/~rivest/rc6.pdf

[15] M. Naor and B. Pinkas, “Visual Authentication and Identification,” Advanced in Cryptology-Crypto ’97, 1997, pp. 322-336.

[16] N. Demytko, “A New Elliptic Curve Based Analogue of RSA,” Advanced in Cryptology-EUROCRYPT 93, Vol. 765 of Lecture Notes in Computer Science, pp. 40-49.

[17] W. Diffie and M. Hellmen, “New Directory in Cryptography,” IEEE Transaction on Computer Theory, Vol. 22, pp. 644-654.

[18] V. S. Miller, “Use of Elliptic Curves in Cryptography,” Advances in Cryptology: Proceedings of CRYPTO ’85, Lecture Notes in Computer Science, Vol. 218, pp. 417-426, Springer-Verlag, 1986.

[19] N. Koblitz, A Course in Number Theory and Cryptography, Springer-Verlag, New York, 1987.

[20] K. Koyama, U.M. Maurer, T. Okamoto and S.A Vanstone, “New Public-Key Schemes Based on Elliptic Curves over the Ring Zn,” CRYPTO ’91 Abstracts, Santa Barbara, CA, pp. 6-1 to 6-7, August 11-15, 1991.

[21] R. Schoof, “Elliptic Curves over Finite Fields and the Computation of Square Roots mod p,” Mathematics of Computation, Vol. 44, No. 170, pp. 483-494, 1985.

[22] E. De Win, S. Mister, B. Preneel and M. Wiener, “On the performance of signature schemes based on the elliptic curves,” in

J.P. Buhler, editor, Algorithmic Number Theory, Proceedings Third Intern. Symp., ANTS-III, Lecture Notes in Computer Science, 1423 (1998), Springer-Verlag, pp. 252-266.

[23] 黃仁俊，「機密共享技術之設計與應用」，中正大學資訊工程研究所博士論文, 民國 87 年。

[24] 葉育斌，”On the Applications and Implementation of Network Security Based on Visual Secret Sharing,” 成功大學電機工程研究所碩士論文,Jun. 1998.