東海大學應用數學系

碩士論文

指導教授：沈淵源

電子支票的行動化研究

The Research of Mobile Electronic Check

研究生：廖元宏

中華民國一百零二年六月十一日

論文名稱：電子支票的行動化研究

校所名稱：東海大學應用數學系研究所

研究生：廖元宏　　指導教授：沈淵源 博士

論文摘要：此篇論文旨在研究改善開立電子支票不便的缺點，進而提升國內支票使用者對電子票據的接受度，過程方法是以使用者自身的 SmartPhone 作為開票工具來替代以往所必需的電腦，並加入 ElGamal 簽署機制來為電子簽章的有效性把關，最後再探討此種方法所帶來的優缺點及安全性漏洞。

關鍵詞：密碼學、電子票據系統、電子支票、金融電子憑證、ElGamal 演算法

序　言

想想到了今天我的研究所學業還真念了段不短的日子，雖然中途為了工作休學而無心集中精力把它完成，總算在今年如願地把它交出去了，卡在心中的一顆石頭終於得以放下，這是件長期拖欠的舊有工作結束，之後就是全心全意投入到工作的另一個開始。

這篇論文並非什麼樣的曠世巨作，然而也是有下了功夫的去找尋靈感及資料撰寫的，俗話說萬事起頭難，確實花了我最多時間的就是在尋找論文的題材，一旦題材目標確定之後就順利很多，至少不再迷茫無方向，這也是我從中學習到的一個寶貴經驗。

這段時間很感謝指導教授沈淵源老師以及陳淑珍老師對我的耐心指導，求學期間給他們添了不少麻煩，尤其是對這篇論文的拖欠真是過意不去，在我休學那麼久後還願意等我繼續完成，讓他們擔當指導老師我覺得很幸運也覺得很愧疚，沒有他們的鼓勵就沒有這篇論文，真的非常感謝你們兩位老師對我的恩情。

最後也要謝謝家裡的父母他們體諒支持我繼續完成，反省我過去對自己學業的態度真的太任性了，才讓這論文遲遲生不出來，之後做任何事情都要一鼓作氣、全力以赴。

目　錄

第一章　緒論.....1
　第一節　研究動機.....1
　第二節　支票結構.....4
　第三節　研究方法.....7
第二章　預備知識.....8
　第一節　初等數論.....8
　第二節　ElGamal 密碼簽署系統.....10
第三章　電子支票行動化.....13
　第一節　一般電子支票開立流程.....13
　第二節　行動電子支票開立流程.....20
第四章　結論.....29
　第一節　可行性探討.....29
　第二節　總結.....30
附錄 2013 年第一季全球手機銷售市佔率.....32
參考文獻.....35

第一章 緒論

人只要一天活在世上就要用錢，錢要賺才有得花，雖然賺錢往往沒有花錢來的快，我們花錢即別人賺錢，別人賺了又花在其他地方，金錢的流動就是如此生生不息，而賺錢與花錢的行為都建立在「交易」上，交易順利才有錢賺，不需交易的金錢流動，不是中獎撿到，就是偷和搶了。

第一節 研究動機

交易是指利用支付「代價」來與對方達成以物易物的共識，在誕生「貨幣」之後，交易有了更明確的標準，規模也更龐大，出現了專司貿易的商人，經濟繁榮與商業貿易彼此息息相關，我們說「貨幣交流」是帶動了人類歷史，推動文明的進化的一份子也不為過。

貨幣本身存在著「演變」，從牲畜、貝殼、稀有石頭、礦物...等物質，都曾被拿來當作「貨幣工具」，為了讓交易能更公平、更容易，人們鑄造了金屬貨幣來取代過去的付款工具。隨著時間不斷推移，貨幣工具至今仍在演變，現在我們所用的錢幣、紙幣、現金卡、信用卡、以及近年來發展的電子錢包等...無一

不是貨幣演變下的產物，其中當然也包含著「支票」與「本票」。

支票與本票可以歸類為一種紙幣，開立人在票據上簽發一定金額後，交託給合法的銀行、信用合作社、農會、漁會等金融機構，於見票時無條件支付受款人票據上所註明的金額，本票與支票不同的地方在於它有指定到期日。支票付款廣泛作為企業之間大筆金額的流動方式，它的本質建立在「信用」與「安全」上，依據就是開立人的「簽名印章」，在國外，即使是小筆金額也常常使用支票來付款，不僅便利也可以降低出門意外遺失錢財危險性。

古往今來，貨幣工具存在著一個生存法則：貨幣即代表族群、國家，弱勢即淘汰，強者生存也適用於貨幣之間的競爭上。在環保意識抬頭，各方業務積極減少紙張浪費及時間成本的現在，電子付費系統因應潮流而生，「電子支票」便是其中一項產物。國外電子支票已經使用十幾年了，在 2003 年至 2011 年間，台灣也曾推行電子支票然而並沒有廣被國人所接受，當時有臺灣銀行、華南商業銀行、彰化商業銀行、第一商業銀行、臺灣土地銀行、臺灣中小企業銀行、合作金庫商業銀行、國泰世華商業銀行及兆豐國際商業銀行，這九家受理電子票據的業務。

其中一項不能普及的原因在於：一般開票者不願意為了開張支票而隨身帶著電腦，比起一台笨重的電腦或筆電，當下需要開支票時,還是紙本發票便利的多。但是科技每天都在進步，現在我們手邊在用的行動設備越來越好，智慧型手機、平板電腦已經形成一股趨勢，進入了人們的生活中而占有一席之地，若能以這些行動設備來替代以往開立電子支票所必要的電腦，藉以彌補攜帶不便的這項缺點，如此國內對電子支票的接受度將會隨之提高，再次推廣時會更加順利。

第二節　支票結構

實體支票結構：(以紙本形式存在)

每張支票內容包含：

1. 印有表明此為支票之文字
2. 受款人之姓名或商號
3. 有大寫支付金額與小寫支付金額
4. 發票人之商號、帳號
5. 付款行名稱、代號與地點
6. 支票流水號
7. 發票年、月、日
8. 若禁止背書轉讓則加上蓋印
9. 發票人銀行帳戶用印

電子支票結構：(以檔案形式存在)

1. 印有表明此為支票之文字

2. 受款人之識別碼、帳號

3. 受款人之電子信箱

4. 小寫支付金額

5. 發票人之商號、帳號

6. 付款行名稱、代號與地點

7. 支票流水號

8. 發票年、月、日

9. 若禁止背書轉讓則加上蓋印

10. 發票人數位簽章

兩種支票結構比較之下，實體支票會指定受款人帳戶名稱但不指定帳號，而電子支票則是指定受款人的憑證號碼或帳號，以及附上電子信箱作為通知受款人用途，而重點在於電子發票的簽章(印章)儲存在金融憑證 IC 卡中，它是由憑證中心所發的(可以申請多張做不同用途)，電子支票做簽章動作需要使用晶片讀卡機，所以開立電子支票有三個必要工具：

1. 金融電子憑證 IC 卡
2. 晶片讀卡機或其他能讀取憑證的設備
3. 可連上網路之電腦

第三節 研究方法

隨著 3C 行動設備性能越來越成熟，APP(Application)軟體應用功能與 WiFi、3G(第三代無線網路)上網，現在已經成為每隻智慧型手機的基本，傳統型手機的發展已經到了極限，開發如日當中的智慧型手機即將取代它原本的地位，就像當年傳統型手機取代 B.B,Call 一樣。我們現在既然希望能以行動設備來開立電子支票，就必須尋找上一節所提到的三項必要工具的取代方案。目前行動裝置系統的主流三大廠牌為 Android、iOS 以及 Windows Phone，在 2013 年第一季度，三個系統市場佔有率總和就達到了 95.5%(Android 74.4%, iOS 18.2%, Windows Phone 2.9%)，不管哪一個作業系統，發展成熟度都不輸給目前的一般電腦，因此行動裝置本身就可以達到第 3 項條件：功能類似電腦、能上網，而為了讓它具有第 1 及第 2 項的功能，我們考慮將申請的電子憑證簽章以檔案形式存於行動設備中，當用行動裝置開票時載入簽章，以密碼系統簽署支票後再將訊息發給銀行去驗證有效性，這些要求 APP 是可以辦到的，因此 APP 便是滿足這兩個條件不可或缺的角色。既然行動設備能一次滿足 3 項必要條件，想要將電子支票行動化自然不是那麼遙不可及。

第二章 預備知識

在提供簽章給銀行驗證有效性的過程中，使用了 ElGamal 演算法來簽署電子支票，因此在這裡對一些初等數論與 ElGamal 密碼簽署系統作介紹。

第一節 初等數論

1. 費馬小定理：若 p 為質數且 $\gcd(a,p)=1$，則 $a^{p-1}\equiv 1 \pmod{p}$

2. 歐拉函數：對正整數 n，所有小於或等於 n 且與 n 互質的正整數個數，以函數 $\varphi(n)$ 表示。

3. 歐拉定理：若 $\gcd(a,n)=1$，則 $a^{\varphi(n)}\equiv 1 \pmod{n}$

4. 原根(Primitive Roots)：

   對兩正整數 a,n，$\gcd(a,n)=1$

   由歐拉定理得知，存在正整數 $\varphi(n)\le n-1$

   使得 $a^{\varphi(n)}\equiv 1 \pmod{n}$

   令 x 為使 $a^{\varphi(n)}\equiv 1 \pmod{n}$ 成立的最小 $\varphi(n)$

   $\Rightarrow x\le\varphi(n)$

   若 $x=\varphi(n)$，則稱 a 是模 n 的原根

例：模11之下7的次冪

j	1	2	3	4	5	6	7	8	9	10
7^j	7	5	2	3	10	4	6	9	8	1

$7^{10} \equiv 1 \pmod{11}$，$10 = \varphi(11)$

$\Rightarrow$ 7是模11的原根

第二節 ElGamal 密碼簽署系統

由 Taher ElGamal 於 1985 年所提出的密碼系統，可作為加密、解密、數位簽章用，其演算法如下：

1. 產生公鑰：

   a. 任選一個大質數 p，使得 $p-1$ 有大質因數

   b. 任選一個 $(\text{mod } p)$ 之原根 α

   c. 任選一個介於 1 與 $p-2$ 之間的整數 a 為私鑰，計算

   $$\beta \equiv \alpha^a (\text{mod } p)$$

   d. 公佈 (p, α, β)

2. 加密程序(欲加密訊息為 x)

   a. 加密者隨機選一與 $p-1$ 互質的整數 k

   並算出 y_1， y_2

   $$y_1 \equiv \alpha^k \ (\text{mod } p)$$

   $$y_2 \equiv x\beta^k \ (\text{mod } p)$$

   b. 密文為 (y_1, y_2)

   解密程序： $x \equiv y_2 y_1^{-a} \ (\text{mod } p)$

例：三毛將訊息 x 加密為 (y_1, y_2) 傳遞給四郎，四郎則將密文 (y_1, y_2) 解密為 x

(1) 四郎選取一個大質數 p 及一個整數 $\alpha \pmod p$

(2) 四郎再選取一私密整數 a 且計算 $\beta \equiv \alpha^a \pmod p$

(3) 四郎公開 (p, α, β)，但 a 保持私密

(4) 三毛則根據四郎所公開的鑰匙，選取一個隨機整數 k 並算出 $y_1 \equiv \alpha^k$ 與 $y_2 \equiv x\beta^k \pmod p$

(5) 然後送出 (y_1, y_2) 給四郎，然後四郎根據此解密：

$y_2 \equiv x\beta^k \pmod p$，$\beta \equiv \alpha^a \pmod p$

$\Rightarrow y_2 \equiv x\alpha^{ak} \pmod p$

$\Rightarrow y_2 \equiv x(\alpha^k)^a \pmod p$

$\Rightarrow y_2 \equiv xy_1^a \pmod p$

$\Rightarrow x \equiv y_2 y_1^{-a} \pmod p$

3. 簽署程序(欲簽署訊息為 m)

a. 簽署者隨機選一與 $p-1$ 互質的整數 k

並算出 r，s

$r \equiv \alpha^k \pmod p$

$s \equiv k^{-1}(m - ar) \pmod{(p-1)}$

b. 簽章為(m,r,s)

簽章驗證：$\beta^r r^s \equiv \alpha^m \pmod{p}$

例：三毛簽署一份信息m，四郎欲驗證此簽名是否有效

(1) 三毛選取一個大質數p及一原根$\alpha \pmod{p}$

(2) 三毛再選取一私密整數a且計算$\beta \equiv \alpha^a \pmod{p}$

(3) 三毛公開(p,α,β)，但a保持私密

(4) 三毛選取一秘密隨機整數k，$\gcd(k, p-1)=1$，算出

$r \equiv \alpha^k \pmod{p}$

$s \equiv k^{-1}(m-ar) \pmod{(p-1)}$

將簽署過的信息(m,r,s)傳給四郎驗證

(5) 四郎下載三毛公開的(p,α,β)

(6) 計算$v_1 \equiv \beta^r r^s \pmod{p}$及$v_2 \equiv \alpha^m \pmod{p}$

(7) $v_1 \equiv v_2 \pmod{p} \Leftrightarrow$此為有效簽名

第三章 電子支票行動化

敘述一般電子支票與行動化後的開立流程，比較兩者之間的不同點，並舉一行動電子支票的開立範例。

第一節 一般電子支票開立流程

電子票據系統屬於個人網路銀行的其中一種功能，因此使用前要先向開戶銀行啟用個人網路銀行，設定登入網頁的帳號密碼與簽署相關規章條款，要注意網路銀行功能必須額外向銀行申請，並非只要在該銀行有帳戶就能進入的。

1. 登錄電子憑證：

   (1) 開戶人透過開戶銀行向憑證中心申請金融憑證IC卡。(憑證及簽章儲存於IC晶片卡內)

   (2) 登入個人網路銀行，開啟電子票據頁面並向票據交換所設定憑證登錄。

電子票據管理頁面(票交所)

憑證號碼	憑證使用者	憑證有效期限	憑證狀態			
011C226209878000001	廖小三	2014/08/17	登錄	設定	停用	憑證恢復
011C226209878000006	廖小三	2014/11/13	未登錄	設定	停用	憑證恢復

2. 加入往來帳戶：

交易前受票人或受讓人必須先新增為往來帳戶，帳戶資訊包含：

(1) 銀行代號

(2) 分行代號

(3) 帳號

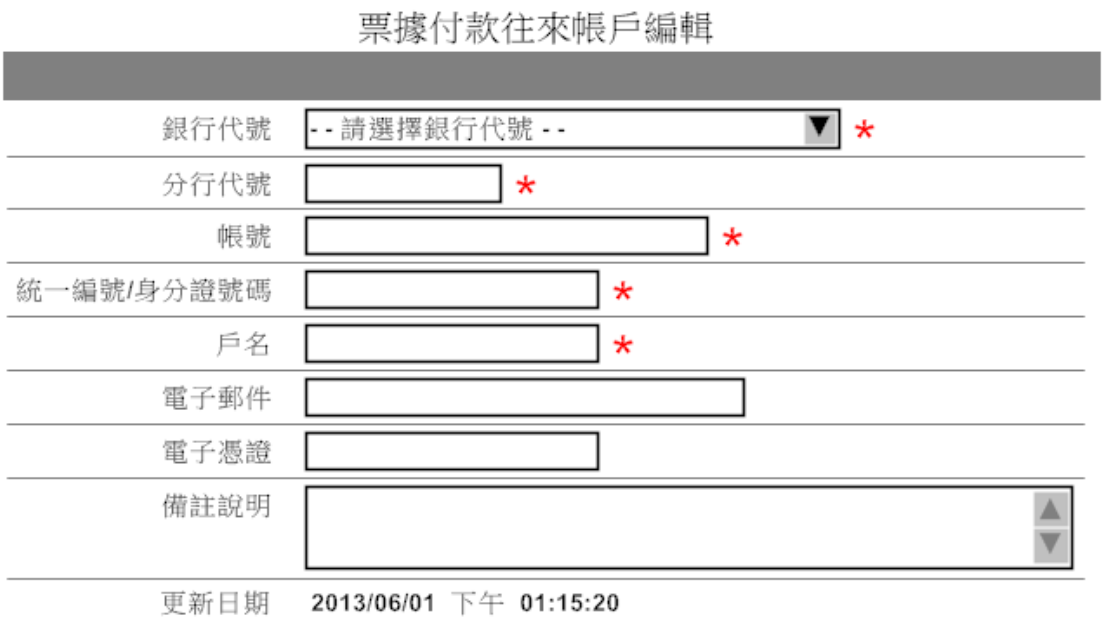
(4) 公司統一編號或身分證號碼

(5) 帳戶名稱或公司行號

(6) 有效電子郵件信箱，作為通知票據資訊用(如填寫錯誤或未填入將無法收到票據交換所的通知)

(7) 有效電子憑證(未填入則受票人僅能以指定帳號受票而無法使用憑證方式受票，受讓人也無法接受他人讓予)

(8) 相關備註說明(非必要)



3. 申領有效空白票據：

用戶想要開立電子支票必須先在電子票據系統功能中申領空白票據，填入申請張數，申領完方可開立。

4. 開立電子支票：(會要求插入電子憑證)

進入開立頁面輸入各項簽發所需的資料，「憑票支付」欄只能點選事先新增的那些來往帳號。

要求再度確定交易

交易完成

完成後電子支票會送到票據交易所，交易所再以 E-mail 通知收票人。

5. 票據託收、作廢、退回、背書轉讓：(會要求插入電子憑證)

以託收為例，在功能頁面點選票據託收，然後輸入所需要之各個欄位資訊，由於可能也會有收票對象沒有使用電子憑證的情形，因此開票時要註明受款人及收款行帳號，收票的一方，不需再跑一趟銀行，銀行會主動通知、交換、入帳，如果收票人持有電子憑證，也可以進行融資或背書轉讓。

要求再度確定交易

票據託收

存入帳號	057-051-45713-1
託收分行	土地銀行仁愛分行
發票人帳號	058-051-45724-1
付款行代碼	005058
票據種類	電子支票
票據號碼	9002155
票據發票日	民國93年 9月10日
金額	$400,000.00
調票使用憑證	005C223209478000001
請確認交易資料	確定交易

已完成調票，請再次確認才能完成交易

交易完成

電子票據

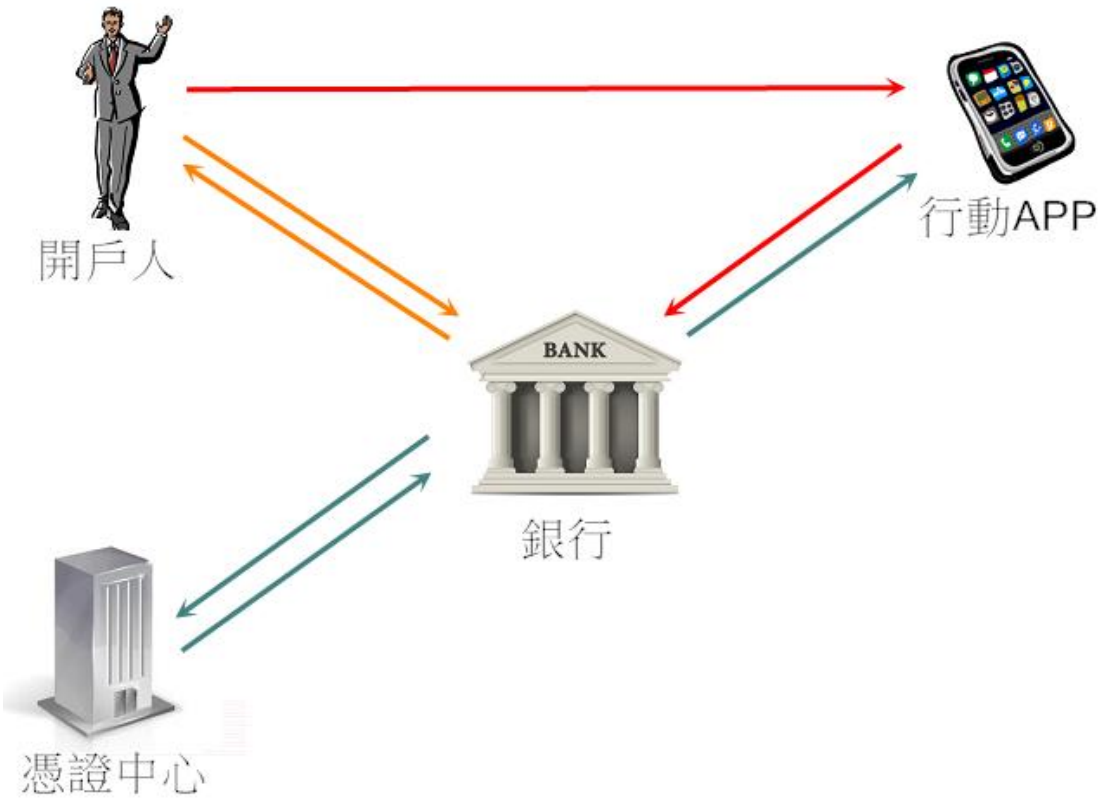
作業序號	632385362294193720
交易名稱	電子票據託收
作業時間	民國93年 9月9日 下午 02:17:19
存入帳號	057-051-45713-1
託收分行	土地銀行仁愛分行
發票人帳號	058-051-45724-1
付款行代碼	005058
票據種類	電子支票
票據號碼	9002155
票據發票日	民國93年 9月10日
金額	$400,000.00

交易完成

第二節　行動電子支票開立流程

在一般電子支票系統中，用戶需要帳號密碼登入個人網路銀行，同樣使用行動電子支票也必須向開戶銀行申請登入APP的帳號密碼。

1. 登錄電子憑證



(1) 開戶人向銀行申請電子支票 APP 帳戶

(2) 銀行給予申請人初始登入密碼

(3) 開戶人使用初始密碼登入行動 APP

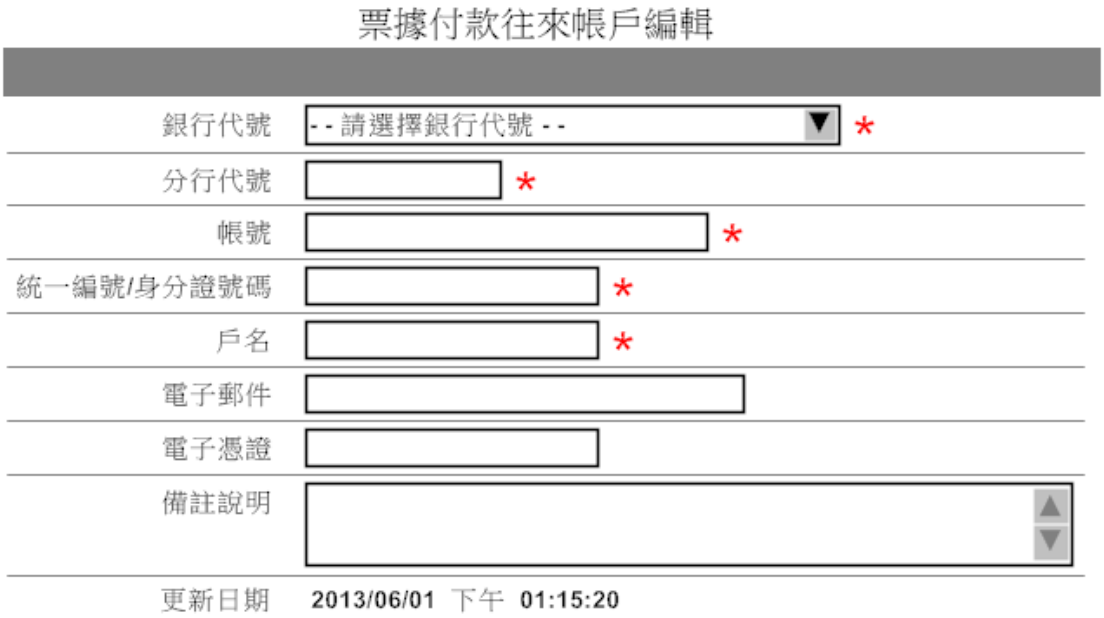
(4) 開戶人於 APP 上完善註冊資料，再傳送給銀行

(5) 銀行將註冊資料傳送憑證中心申請電子憑證

(6) 認證中心核發電子憑證，行動設備以檔案形式儲存

(7) 開戶人使用 APP 對銀行設定憑證登錄

2. 加入往來帳號



登入APP，使用來往帳號新增功能，帳戶資訊包含：

(1) 銀行代號

(2) 分行代號

(3) 帳號

(4) 公司統一編號或身分證號碼

(5) 帳戶名稱或公司行號

(6) 有效電子郵件信箱，作為通知票據資訊用

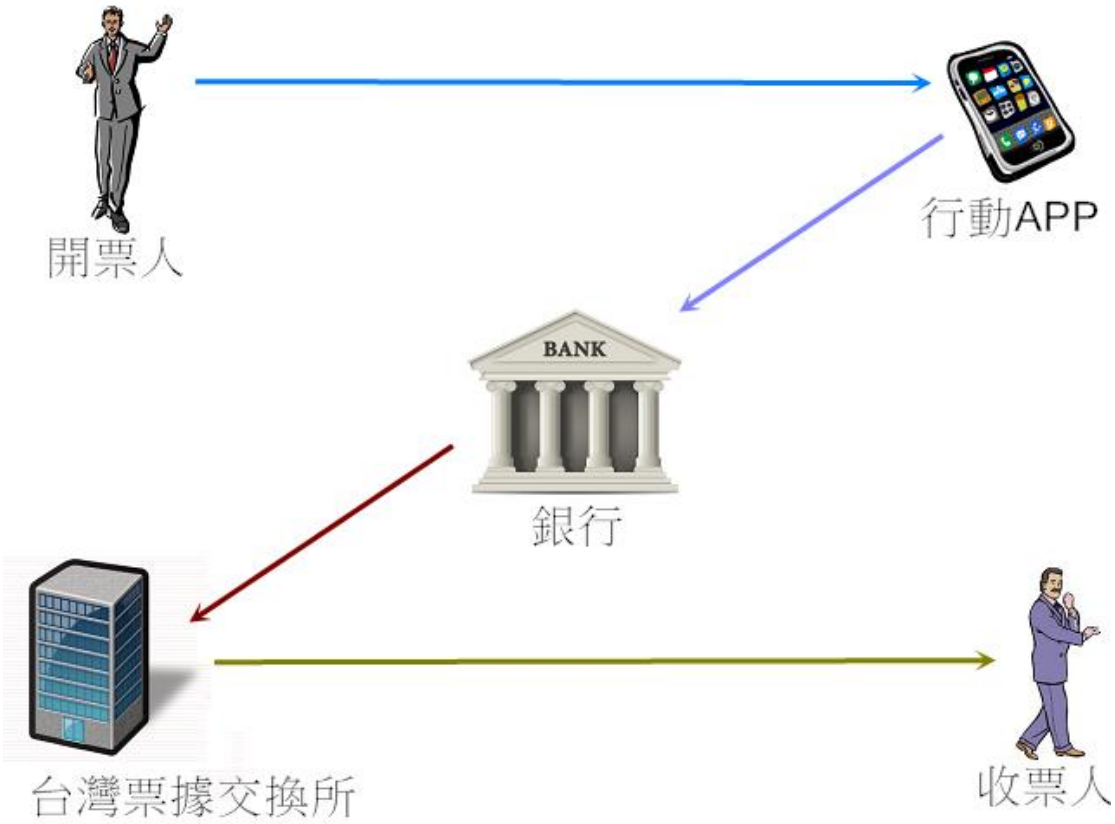
(7) 有效電子憑證

(8) 相關備註說明

3. 申領有效空白票據

登入 APP，使用申請空白票據功能，填入申請張數，申領完成方可開立。

4. 開立電子支票



(1) 開票人登入 APP，填入票據各項內容

(2) 載入電子憑證完成交易

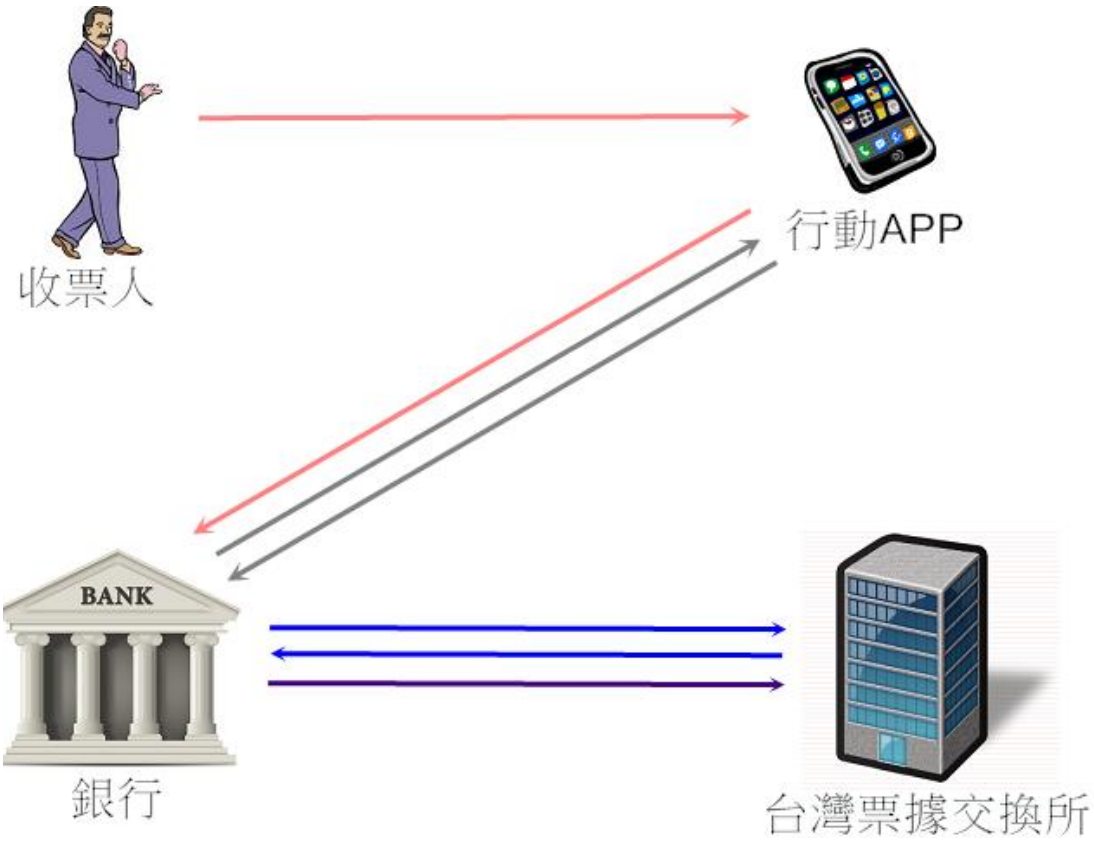
(3) APP 將票據資訊與簽章傳至銀行

(4) 銀行檢核票據內容與開票人簽章是否有效

(5) 票據檢核無誤後銀行將電子票據送票據交換所登錄保管

(6) 票據交換所以 E-mail(或 APP 即時訊息)通知收票人

5. 票據託收、作廢、退回、背書轉讓(以託收為例)：



(1) 收票人使用 APP 申請票據存入託收

(2) 銀行確認收票人存戶身分

(3) 銀行向票據交換所申請調出該張票據

(4) 票據交換所檢核申請人是否為權利人

(5) 確認後調出該票據傳給銀行

(6) 銀行將票據給收票人

(7) 收票人於 APP 上完成存入託收操作後載入電子憑證

(8) APP 將票據資訊與簽章傳送至銀行

(9) 銀行檢核票據內容與收票人簽章是否有效

(10)銀行將票據傳送交換所申請存入託收之登錄

(11)票據交換所檢核票據後，登錄系統資料庫註記存入託收

符號說明：

a：開票人的數位電子憑證

p：APP 所產生的大質數

α：模 p 之原根

β：APP 載入開票人的數位憑證後運算 $\alpha^a \pmod{p}$

(p,α,β) 為 APP 所產生給銀行的公鑰

m_i：銀行所給予支票的有效流水編號

r：由 APP 運算 $\alpha^k \pmod{p}$

k：APP 隨機產生的秘密整數

s：由 APP 用運算 $k^{-1}(m_i - ar) \pmod{p}$

(m_i,r,s) 為 APP 將支票 m_i 以 ElGamal 簽署過的信息

APP 與銀行都需要用到 ElGamal 演算法：

(1) 填完票據內容，APP 要求載入電子憑證 a 確認為本人所發

(2) APP 計算公鑰 (p,α,β)，將票據 m_i 簽署為 (r,s)

(3) APP 將公鑰 (p,α,β) 與簽章 (m_i,r,s) 傳給銀行驗證

(4) 銀行利用 $\beta^r r^s \equiv \alpha^m \pmod{p}$ 驗證用戶簽章有效性

(5) 驗證有效即送票據交換所

例：廖老二欲開立一張10000元的支票給廖小三，於是廖老二操作手機登入電子支票 APP，填入票據資訊後載入電子憑證，此時 APP 檢查廖老二的電子簽章$a_1=141421$且此張支票的有效流水號為$m_1=151405$，然後 APP 選擇一比a_1大之質數$p_1=225119$以及一與$p-1$ 互質的隨機整數$k_1=239$，算出

$$\alpha_1=11$$
$$\beta_1=11^{141421}\equiv 18191 \pmod{225119}$$

將流水號$m_1=151405$簽署

$$r_1=11^{239}$$
$$\equiv 164130 \pmod{225119}$$
$$s_1=239^{-1}(151405-141421\times 164130)$$
$$\equiv 130777 \pmod{225119}$$

然後將

$$(p_1,\alpha_1,\beta_1)=(225119,11,18191)$$

$$(m_1,r_1,s_1)=(151405,164130,130777)$$

傳送給銀行

銀行收到的廖老二手機 APP 所傳的(p_1,α_1,β_1)與(m_1,r_1,s_1)後驗算是否$\beta_1^{r_1}r_1^{s_1}\equiv\alpha_1^{m_1} \pmod{p_1}$

$$v_1=\beta_1^{r_1}r_1^{s_1}$$
$$\equiv 18191^{164130}\times 164130^{130777}$$
$$\equiv 128841\times 193273$$
$$\equiv 173527 \pmod{225119}$$

$$v_2 = \alpha_1^{m_1}$$
$$\equiv 11^{151405}$$
$$\equiv 173527 \pmod{225119}$$

$$\Rightarrow v_1 = v_2$$

因此銀行判定廖老二此張電子支票的簽章有效，將此支票傳至票據交換所，票據交換所再以 APP 的即時訊息和 E-mail 和通知廖小三。

後續廖小三收到通知後，登入 APP 委託銀行託收此張票據，完成操作後，APP 選出 p_2、k_2 並計算出 (α_2, β_2) 與簽章 (r_2, s_2) 給銀行，此張支票流水號依然是 $m_1 = 151405$，銀行收到 (p_2, α_2, β_2) 與 (m_1, r_2, s_2) 後，同樣驗證是否 $v_1' = v_2'$，$v_1' \equiv \beta_2^{r_2} r_2^{s_2} \pmod{p_2}$，$v_2' \equiv \alpha_2^{m_1} \pmod{p_2}$，確定有效就將支票送到票據交換所登錄資料庫，廖小三此時可以繼續將這張支票入帳或做轉讓動作。

第四章 結論

最後章節闡述此篇研究方法的可行性與優缺點，並分析目前行動設備的普及率與將來發展的可能性。

第一節 可行性探討

電子支票的開立流程與實體支票差異不大，在減少資源浪費方面則更勝一籌，按理來說應該很適合推廣使用，但是要融入一件新事物本來就有某些瓶頸，一般人在習慣舊方法後，對於要再重新學習新方法往往會興趣缺缺，縱使新的比舊的方便依然是如此。相比國外，國內使用支票的場合偏向於公司與公司之間，個人使用的情形則較少見，由於對電子支票操作不熟悉，覺得還可能需要添增新設備，因此經營者們最後還是習慣用紙本方式開票。就這樣，台灣的「電子票據系統」就在 2011 年落幕了，原因在於使用量太少。現在 3C 行動設備效能一台比一台好，智慧型手機普及率正逐年上升，電腦筆電可能沒辦法人手一台，但是手機卻幾乎是人手一機並且隨身攜帶，而且第四代無線網路(4G)即將上路，行動上網越來越方便，APP 的使用也越來越多樣性，這些新事物都逐漸滲入我們的日常生活中。在過去，我們可能不想為了開立電子發票而帶電腦，但現

在只要身邊的手機就可以代勞，如此一來，不便攜帶就不再構成難以推廣的理由。

第二節　總結

電子支票的安全性比傳統實體票據高，原因在於實體票據開完票後，持票人必須要等到票據到期才能入帳、轉讓，在這時才會知道此張票據有沒有效、印鑑有沒有符合，所以萬一有人隨便蓋個印章欺瞞收票人來個惡性倒帳，俗稱「芭樂票」，收票人屆時有可能欲追無門。但是電子支票在有效性的檢核上具有優勢，收票人可透過票據查詢系統知道收到的電子支票有沒有效，只要開票人有問題，銀行會立即將他列為拒往戶並停止其使用電子票據，大大降低惡性倒帳的機率，對收票人而言比較有保障。

此篇研究是在電子支票的使用方法上添增新途徑，對其系統結構安全性本質並無重大改變，若要考慮這項新方法所帶來的安全性漏洞，應該就在於 APP 是否容易被不當分子破解，以及當想要更換手機或是手機遺失時的處理情形，後者如果沒有好好將遺留在手機內的私密憑證適當處理，如刪除或暫停使用，一旦被懂得分析手機資料的人拿到，就會有憑證簽章外洩的可

能。所以這種情況的保險做法就是向憑證中心申請暫停此份憑證的交易功能,待確定後續沒問題才繼續使用或重新申請一份,這點就如同證件卡片遺失找管理機構作廢一樣。

手機的普及率增長，遺失率也隨著提高，工具可以帶來便利，也有可能帶來風險，各項安全系統的作用無非就是為了降低這些風險的存在，倘若自己不加以重視，再完善的保護程序也會形同虛設，小心駛得萬年船，保護私鑰密碼最重要的還是要靠自己的細心。

附錄

表一、 2013 年第一季全球手機終端銷售量（單位：千支）

廠商	2013Q1	2013Q1	2012Q1	2012Q1
	銷售量	市占率(%)	銷售量	市占率(%)
三星 Samsung	100,657.70	23.6	89,284.60	21.1
諾基亞 Nokia	63,215.20	14.8	83,162.50	19.7
蘋果 Apple	38,331.80	9	33,120.50	7.8
LG	15,615.80	3.7	14,720.40	3.5
中興 ZTE	14,606.60	3.4	17,379.70	4.1
華為 Huawei	11,114.80	2.6	10,796.10	2.6
TCL 通訊	8,515.90	2	7,396.60	1.7
索尼行動通訊 Sony Mobile	7,955.50	1.9	7,898.40	1.9
聯想 Lenovo	7,778.90	1.8	5,820.60	1.4
宇龍 Yulong	7,478.80	1.8	3,146.60	0.7
其他	120,550.60	35.4	120,229.40	35.5
總計	**425,821.60**	**100**	**422,955.40**	**100**

表二、 2013 年第一季全球智慧型手機終端銷售量（單位：千支）

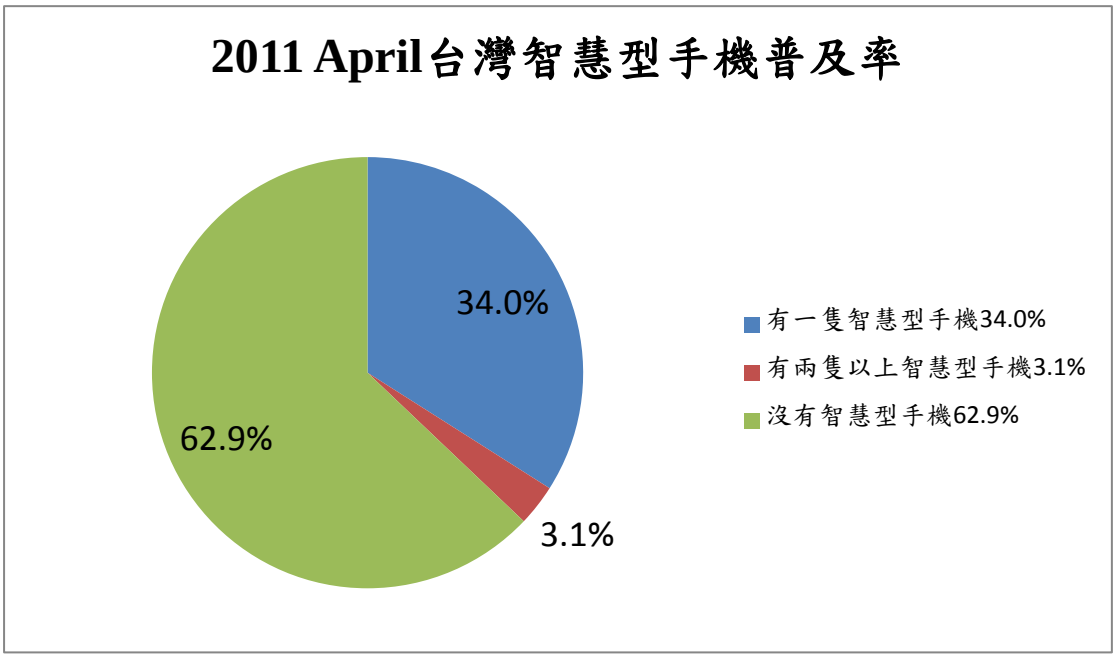
廠商	2013Q1	2013Q1	2012Q1	2012Q1
	銷售量	市占率(%)	銷售量	市占率(%)
三星 Samsung	64,740.00	30.8	40,612.80	27.6
蘋果 Apple	38,331.80	18.2	33,120.50	22.5
LG	10,080.40	4.8	4,961.40	3.4
華為 Huawei	9,334.20	4.4	5,269.60	3.6
中興 ZTE	7,883.30	3.8	4,518.90	3.1
其他	79,676.40	37.9	58,537.00	39.8
總計	**210,046.10**	**100**	**147,020.20**	**100**

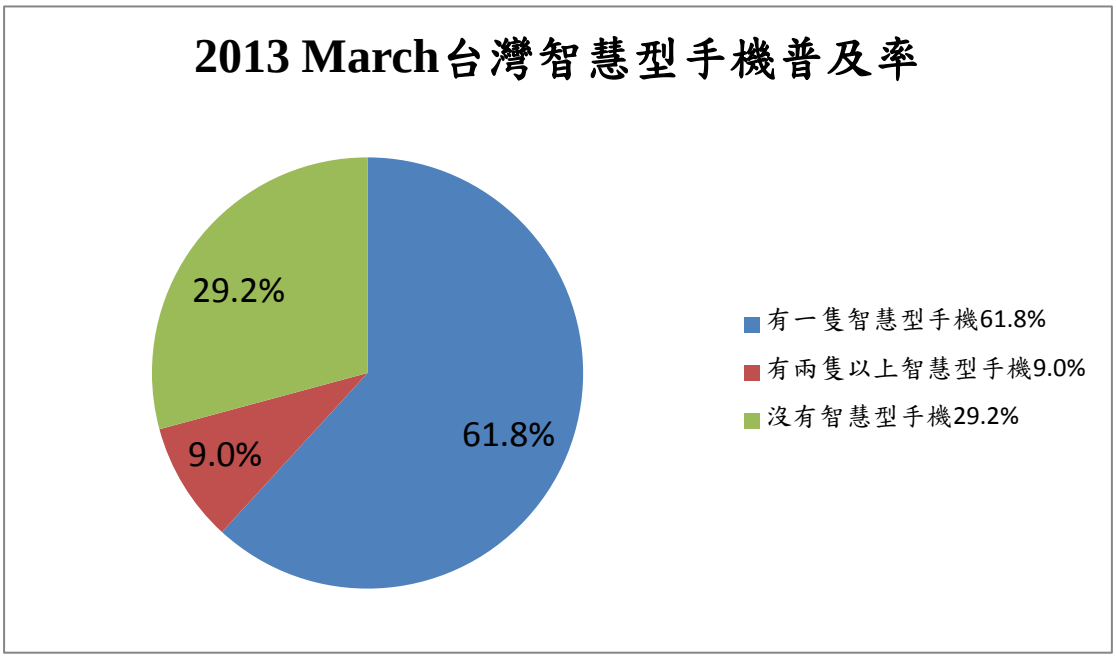
表三、2013 年第一季全球智慧型手機作業系統終端銷售量（單位：千支）

作業系統	2013Q1	2013Q1	2012Q1	2012Q1
	銷售量	市占率(%)	銷售量	市占率(%)
Android	156,186.00	74.4	83,684.40	56.9
iOS	38,331.80	18.2	33,120.50	22.5
Research In Motion	6,218.60	3	9,939.30	6.8
Windows Phone	5,989.20	2.9	2,722.50	1.9
Bada	1,370.80	0.7	3,843.70	2.6
Symbian	1,349.40	0.6	12,466.90	8.5
其他	600.3	0.3	1,242.90	0.8
總計	**210,046.10**	**100**	**147,020.20**	**100**

資料來源：Gartner 國際研究顧問機構（2013 年 5 月）

表四、2011 April 與 2013 March 台灣智慧型手機普及率市調





資料來源：創世紀市場研究顧問（2011.04）、104 市調（2013.03）

參考文獻

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

[2] 洪維恩，數學運算大師 MATHEMATICA 4，碁峯資訊股份有限公司，2001

[3] 劉尊全，數位時代密碼技術的現狀與未來，松崗電腦圖書資料股份有限公司，2001

[4] William Stallings，巫坤品、曾志光譯，密碼學與網路安全：原理與實務，碁峯資訊股份有限公司，2001

[5] 劉逸成，網路電子交易付款系統之民事法律關係研究，成功大學法律學系碩士論文，2004

[6] 章煒文，基於離散對數的 ELGamal 公鑰密碼系統，中國石油大學碩士論文，2006

[7] 賴滄本，電子投票系統的研究，東海大學應用數學系碩士論文，2010

[8] 中文維基百科，支票功能概述
http://zh.wikipedia.org/wiki/%E6%94%AF%E7%A5%A8

[9] MBAlib 智庫百科，電子支票系統說明
http://wiki.mbalib.com/zh-tw/%E7%94%B5%E5%AD%90%E6%94%AF%E7%A5%A8%E7%B3%BB%E7%BB%9F

[10]臺灣票據交換所，電子票據業務 FAQ、電子票據處理流程，
http://www.twnch.org.tw/echeck/FAQ.html
http://www.twnch.org.tw/echeck/echeckprocess.htm

[11]臺灣土地銀行，e-BANK 個人銀行使用手冊 第六章：電子票據

[12]Janessa Rivera & Rob van der Meulen (Gartner)，Asia/Pacific Led Worldwide Mobile Phone Sales to Growth in First Quarter of 2013 http://www.gartner.com/newsroom/id/2482816，2013 Gartner Research

[13]創世紀市場研究顧問，2011 四月台灣智慧型手機普及率市調

[14]104 人力銀行市調，2013 三月台灣智慧型手機普及率市調