電子支票的行動化研究

廖元宏 Yuan-Hung Liao 沈淵源 Yuan-Yuan Shen

摘要

以往電子支票有開立工具攜帶不便的缺點，為了提升國內支票使用者對電子票據的接受度，在這裡假設以使用者自身的 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安全性把關，最後再探討此種方法所帶來的優缺點及部分漏洞。

1 支票結構

實體支票結構：(以紙本形式存在)

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)

內容包含：
(1) 印有表明此為支票之文字
(2) 受款人之識別碼、帳號
(3) 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) 發票人數位簽章
(10) 受款人之電子信箱

兩種結構比較下的差異，實體支票指定受款人帳戶名稱，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，而且電子發票需要金融憑證 IC 卡，它由憑證中心所管理，在簽章時當然也會用到晶片讀卡機，所以開立電子發票的必備工具有三項：
(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

2 替代開立支票工具的想法

現在 3C 行動設備性能越來越成熟，APP 軟體的應用與 WiFi、3G 行動上網已經成為每隻 Smart Phone 的基本，而傳統型手機的發展差不多已經到了極限，如同昔日傳統型手機取代 B. B. Call 的趨勢一樣，如日當中的智慧型手機即將取代它原本的地位，我們現在想以 Smart Phone 來開立電子支票，就必須解決上節所提到的三項必要工具替代方案。目前 Smart Phone 的作業系統，不管速度、效能都不輸給一般電腦，因此 Smart Phone 本身就可充當第 3 項條件：功能類似電腦、可上網，而為了讓它也滿足第 1 及第 2 項，我們考慮將申請的電子憑證簽章以檔案形式存於 Smart Phone 中，提供 Smart Phone 開票時載入簽章檔案，再加入密碼系統簽署支票給銀行驗證有效性，這些要求都能以 APP 辦到，即是在撰寫 APP 時加以調整就可以，如此 Smart Phone 就能滿足所有的開立條件。

3　一般電子支票開立流程

(1) 登錄電子憑證：

(a) 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)

(b) 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：

(a) 銀行代號

(b) 分行代號

(c) 帳號

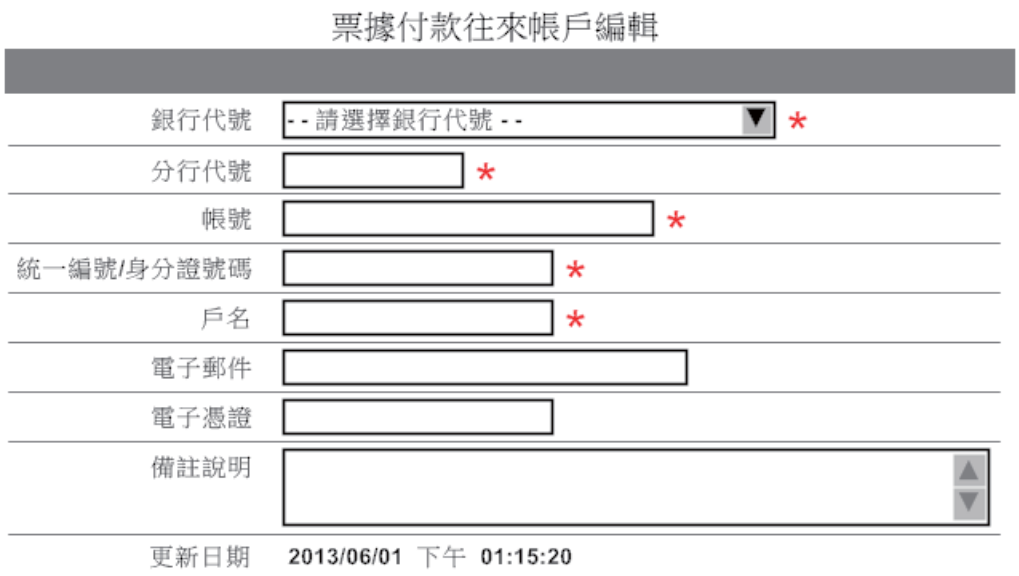
(d) 公司統一編號或身分證號碼

(e) 帳戶名稱或公司行號

(f) 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)

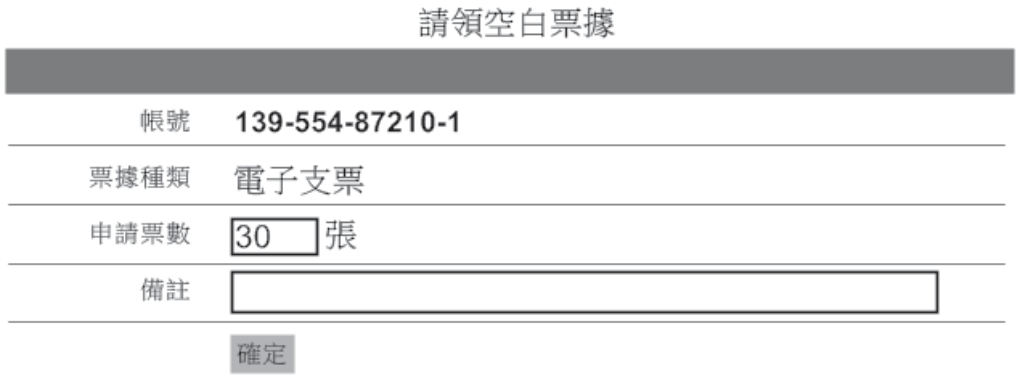
(g) 有效電子憑證(未填入則受票人僅能以指定帳號受票而無法使用憑證方式受票，受讓人也無法接受他人讓予)

(h) 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。

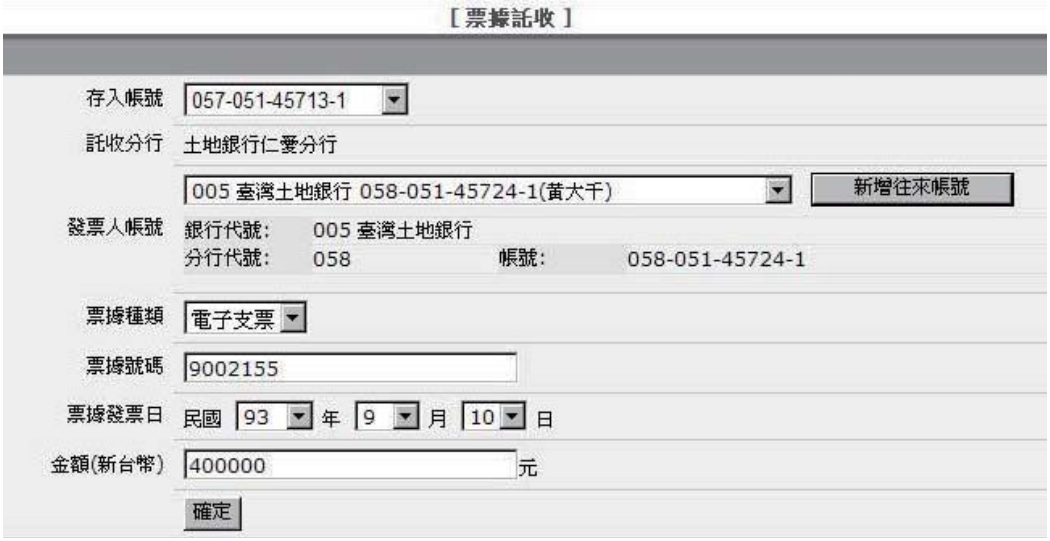
要求再度確定交易

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

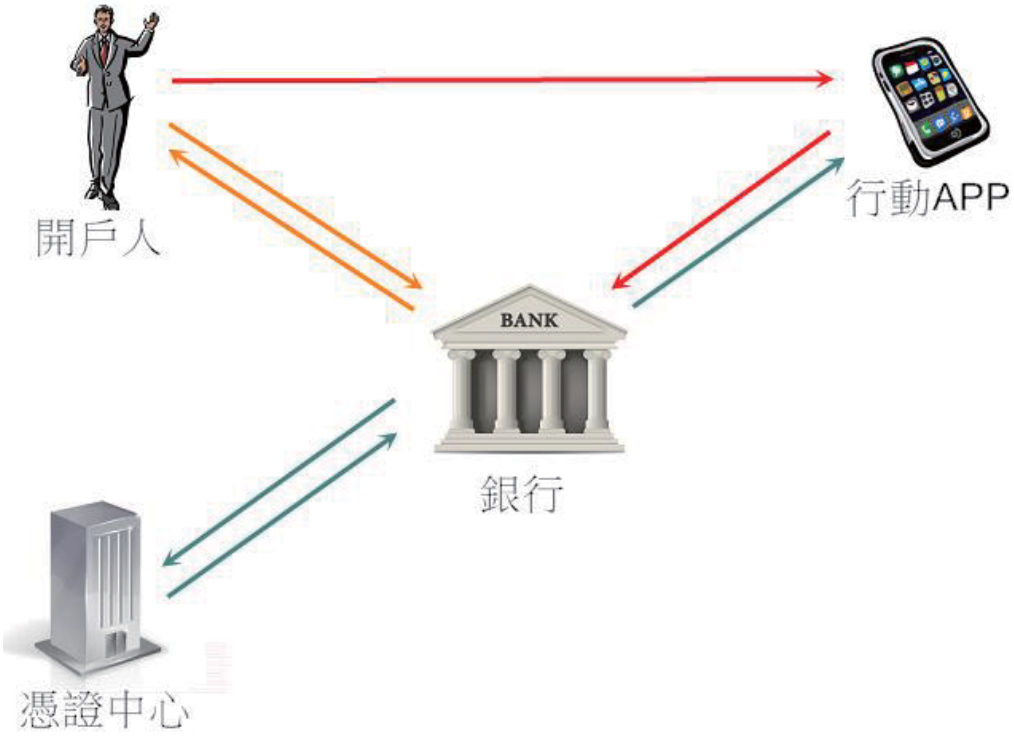
電子票據

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

4　行動電子支票開立流程

(1)　登錄電子憑證



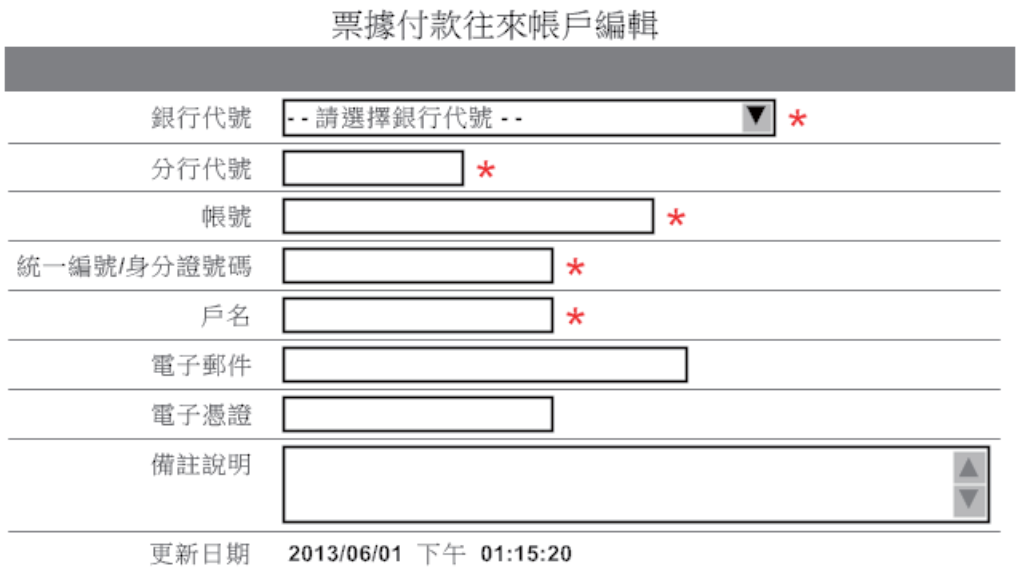
(a)　開戶人向銀行申請電子支票 APP 帳戶

(b)　銀行給予申請人初始登入密碼

(c)　開戶人使用初始密碼登入行動 APP

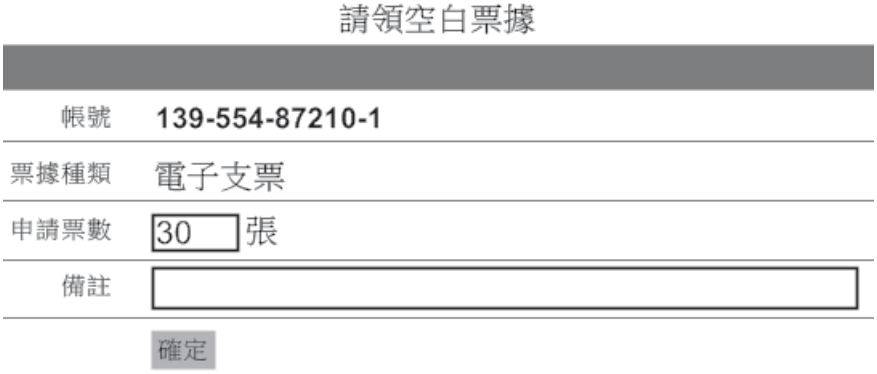
(d) 開戶人於 APP 上完善註冊資料，再傳送給銀行
(e) 銀行將註冊資料傳送憑證中心申請電子憑證
(f) 認證中心核發電子憑證，行動設備以檔案形式儲存
(g) 開戶人使用 APP 對銀行設定憑證登錄

(2) 加入往來帳號



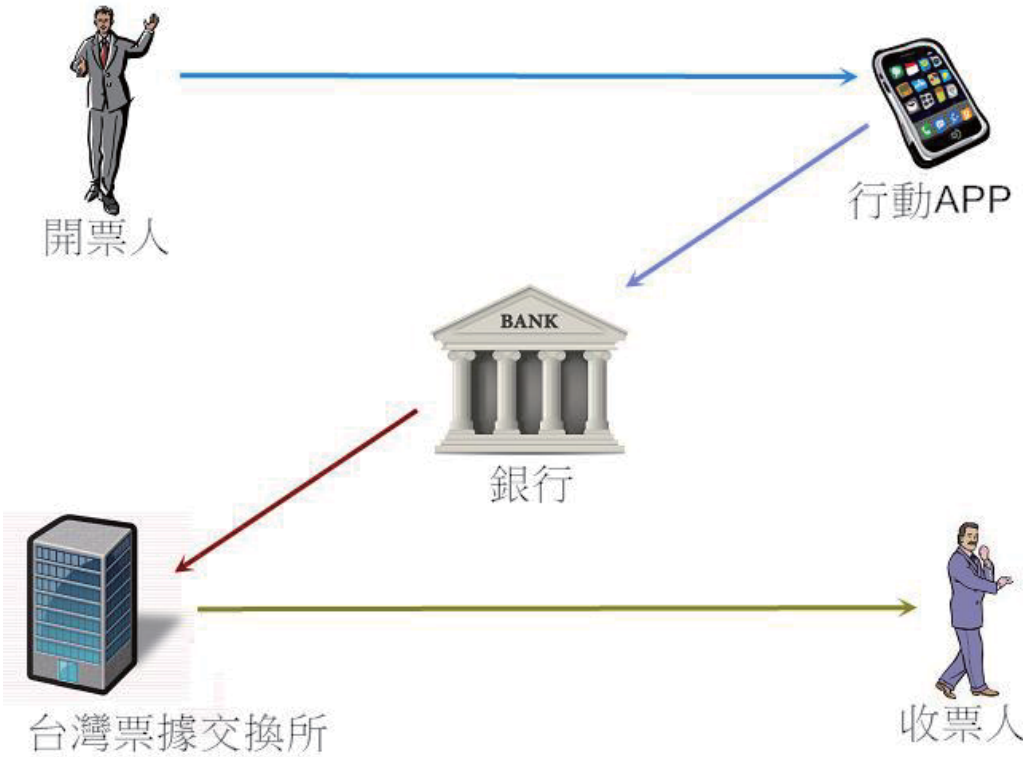
登入APP，使用來往帳號新增功能，帳戶資訊包含：
(a) 銀行代號
(b) 分行代號
(c) 帳號
(d) 公司統一編號或身分證號碼
(e) 帳戶名稱或公司行號
(f) 有效電子郵件信箱，作為通知票據資訊用
(g) 有效電子憑證
(h) 相關備註說明

(3) 申領有效空白票據



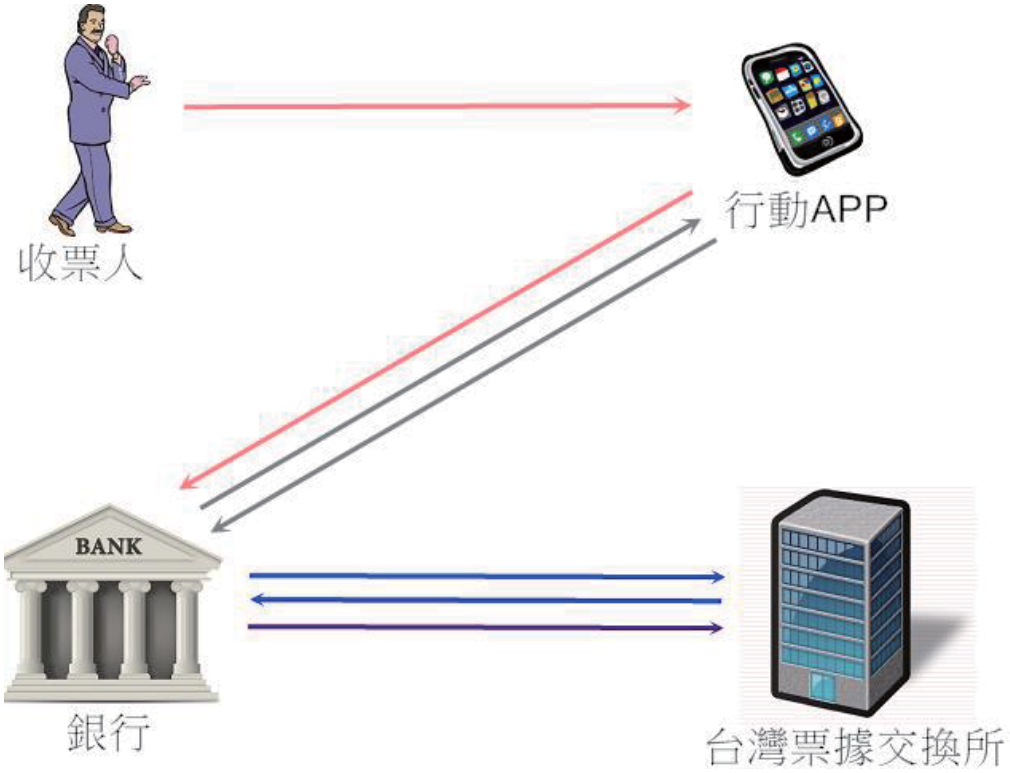
登入 APP，使用申請空白票據功能，填入申請張數，申領完成方可開立。

(4) 開立電子支票



(a) 開票人登入 APP，填入票據各項內容
(b) 載入電子憑證完成交易
(c) APP 將票據資訊與簽章傳至銀行
(d) 銀行檢核票據內容與開票人簽章是否有效
(e) 票據檢核無誤後銀行將電子票據送票據交換所登錄保管
(f) 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)：



(a) 收票人使用 APP 申請票據存入託收
(b) 銀行確認收票人存戶身分
(c) 銀行向票據交換所申請調出該張票據
(d) 票據交換所檢核申請人是否為權利人
(e) 確認後調出該票據傳給銀行
(f) 銀行將票據給收票人
(g) 收票人於 APP 上完成存入託收操作後載入電子憑證
(h) APP 將票據資訊與簽章傳送至銀行
(i) 銀行檢核票據內容與收票人簽章是否有效
(j) 銀行將票據傳送交換所申請存入託收之登錄
(k) 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)	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)	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。

5　可行性探討與總結

電子支票開立過程的想法邏輯與傳統實體支票很類似，因此並不難上手，況且減少紙張浪費也非常符合環保，再者實體支票持票人若是遇到「芭樂票」，往往要等到支票到期入帳時才會得知此張為空頭票據，屆時有可能欲追無門，相較於這一點，電子支票持票人只需透過電子票據查詢系統，就可以知道開票人的電子憑證是否有效，因為只要開票人信用安全有問題，銀行會立即將他列為拒往戶並停止其憑證權益，這樣可以大大降低惡性倒帳的機率，對收票人較有保障。

雖然這裡將開立電子支票的方式行動化了，但對其系統、結構及安全性本質並無重大改變，不過卻可能帶來的新的漏洞危險，例如 APP 是否容易被不肖分子破解、想要更換手機或是手機遺失時是否有適當處理，後者如果沒有妥善將遺

留在手機內的私密憑證刪除或暫停使用，一旦被懂得分析手機內資料的人拿到，就會有憑證簽章被濫用的可能。遇到此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。

手機的普及率增長，遺失率也隨著提高，工具可帶來便利，也可帶來風險，凡事都是一體兩面，各項安全措施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。

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

On the Mobil Electronic Checks

Yuan-Hung Liao & Yuan-Yuan Shen

Abstract

Due to the inconvenience of carrying notebook computers, electronic checks are not so popularly accepted by most business people of our country in the past. Instead of notebook computers, we use smart phones to make it more accessible. In addition, we adopt ElGamal signature scheme to increase the level of security concern. Finally, we discuss the strength and weakness of our system.