無線射頻辨識（RFID）技術於有價票證防偽之應用（下）

曲文豪

摘要

目前，國際防僞產業逐漸興起了一股利用微電子防僞技術的潮流，尤其是 RFID 標籤的運用。未來歐元及日圓也都準備加上 RFID 做鈔券防僞的機制之一；美國及中國大陸正考慮在公民身分證上增加 RFID 作爲身分辨識之用，而日本也有學者研究將汽車駕駛執照上加入 RFID 技術；故本文針對國內研究學者所提出 RFID 有價票證的建構模式之研究成果加以摘錄整理，諸如土地所有權狀、金融票據、紙鈔、晶片護照等等，都是需要具備防僞機制的安全文件；因此，RFID 技術應用系統無非是一項可以審慎評估的裝置，其中，晶片護照由於美國及歐盟的支持正在全世界積極的推展與建置中，可見 RFID 的應用已經揭開了防僞技術史上的一個新頁，不能不加以重視。

關鍵詞：有價票證、防偽、RFID（無線射頻辨識）、EPCglobal、RBPS、電子憑證、數位簽章

七、無線射頻辨識（RFID）技術應用於有價票證防偽研究介紹

（一）世界各國推動「電子護照計劃」淺析：

自從 2001 年發生了 911 恐怖攻擊事件之後，全球各國無不開始對於國境安全及邊防控管措施重新思考更積極有效的邊境管理（Border Management）策略，便著手研究可以整合臉部等多重生物特徵辨識技術的「Electronic passport，ePassport」，其目的在於達成對護照僞造、變造，遺失冒用等預防性之安全功能，藉以保障國家安全。ePassport，有人稱之爲「RFID 護照」，也有人將其稱爲「生物特徵護照」，其最大特點是在護照本封面（底）裡或內頁內嵌入「Contactless Smartcard」。ePassport 的基本結構如上圖（七）所示：

圖（七）圖解 ePassport 基本結構

該非接觸式智慧卡晶片所使用的是 ISO/IEC 14443“Proximity cards”標準與 ISO/IEC 7816 系列的“Smartcard”標準；而我們現在所用的 RFID（Radio Frequency Identification）標準，如 ISO/IEC 15693“Vicinity cards”及 ISO/IEC 18000 等是有所差異的。雖然 ePassport 非接觸式晶片的無線連結技術與 RFID 類似，但 ePassport 所引用的標準卻擁有更高的安全等級與保障晶片護照持有人的資料隱私安全。因此 ePassport 應正名爲「晶片護照」。

全球晶片護照現況

歐、美、亞洲各國正如火如荼地開始，依國際民航組織（International Civil Aviation Organization，ICAO）的規範，陸續完成晶片護照的正式製發作業；ICAO 規範晶片護照的主要功能包括：

1. 對於護照的高度防僞
2. 通關自動化
3. 順暢的國際旅遊

表（三）已完成晶片護照製發國家統計表

全球實施晶片護照國家概況	
1998 年	1
2004 年	3
2005 年	9
2006 年	34
2007 年	49
2008 年	85
2009 年	99

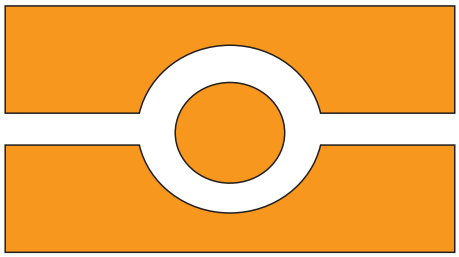
此外，美國要求全球 27 個免簽證計畫（Visa Waiver Program，VWP）會員國都必須在 2006 年 10 月 26 日起，所有受該計畫保護的旅客，必須出示可機器讀取的護照（Machine-Readable Passport，MRP）就是所謂的晶片護照，否則就會喪失免簽證待遇，因此更驅動世界各國積極投入晶片護照的製發作業。

上表（三）爲目前國際上已完成晶片護照製發的現況統計。

我國晶片護照導入現況

我國晶片護照的導入作業於 2007 年 12 月正式啓動；在未來，若民眾請領新的護照本，會發現在護照本的封面將多了如下圖（八）所示由 ICAO 所制定的晶片護照標記，而這也代表我國的 MRTD 業務又邁進了一個新的里程碑：

對於晶片護照的導入與應用，主要包含有下列四項特點：



圖（八）ICAO 所制定的晶片護照標記

1、非接觸式智慧卡晶片與現有護照的整合。

2、提供臉部相片影像生物辨識比對功能。

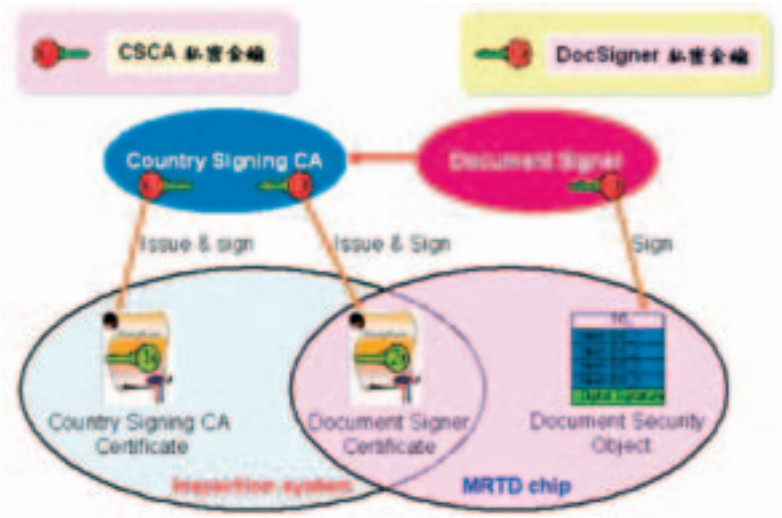
3、個人數位化資料以 LDS（Logical Data Structure）形式儲存於晶片中。

4、透過 PKI（Public Key Infrastructure）機制達成晶片資料安全。

爲確保晶片護照資料的「完整性」、「保密性」、「驗證性」與「不可否認性」ICAO 藉由 PKI 的數位憑證及金鑰管理架構達成了晶片資料安全的目的。如右圖（九）所示：

在此架構中，藉由 Country Signing CA 發行數位憑證並利用 Document Signer Certificate 對晶片內資料進行數位簽章，以確認該晶片的發行者及資料完整性；對護照查驗單位而言，即可利用相同的數位憑證與數位簽章機制進行該晶片內容的驗證，如此，對於晶片內之資料安全而言，也不用擔心晶片內之資料遭受篡改與不當之變更。同時該非接觸式晶片在所有資料寫入後就立即進行晶片鎖死的動作，也不會有資料再被寫入與篡改的可能，可確保晶片護照欲達成的安全應用目的。

在**美國**的新護照之底頁中含有一顆高度安全之整合性電路電腦晶片，其中安全的儲存了印在文件上的相同資料。電子護照之設計是採用多層次安全以保護持有人之隱私，其中包括基本存取控制 Basic Access Control（BAC），必須由入出境控制



圖（九）

檢驗員將護照通過一台掃瞄機，讀取編碼後之資料，然後再授權電子讀取機讀出存在晶片上的資料。實際的資料將傳輸至四吋（十公分）的距離。除了防護和基本存取控制之外，在晶片中還有超過 50 個獨立安全機制，包括精密的電腦資料加密方式，以保證個人資料的私密性。在晶片中的安全機制還包括晶片表面的主動保障防護以及感應器，以防止未經授權人士讀取晶片內容。

歐盟規定會員國必須在 2009 年 6 月 28 日以前完成與新一代電子護照的相容工作及系統轉移。德國是第一個轉移至新系統的國家（從 2007 年 11 月開始）。在電子護照上的兩個指紋的數位生物識別影像數據需要一個由 ICAO 製定的安全增強型程式（Extended Access Control，EAC）。EAC 可提供必要的加密技術來保護私人且敏感數據，並且防止複製。而新的 SmartMX 晶片建置在此基礎上，有助於生物識別數據安全地儲存於護照上，進而在檔案及其所有者之間建立更加密切的聯繫。

SmartMX 支援 EAC 規範的安全要求。藉由使用以橢圓曲線爲基礎的非對稱（asymmetric）加密技術，確保儲存在 IC 晶片上數據的安全。每個晶片的儲存量均達 80K Byte EEPROM，能容納持有人的照片、指紋、姓名、出生日和出生國家等生物識別數據，將護照與使用者永久性地鎖定在一起。此外，還可防止光線和鐳射進行的攻擊，並包含一個專用的硬體防火牆來保護晶片上的特定部分。

法國新型護照中的 SmartMX 晶片技術獲得 EAL5+ 認證，該晶片可符合國際民航

組織（ICAO）標準，並採用超低功耗通訊商議技術（ultra low power handshaking technology），符合 ISO/IEC14443 的標準能功耗範圍需求；此外該款高安全性晶片擁有 36K Byte EEPROM 記憶體，儲存能力可用於保存如指紋和面部特徵等生物辨識資訊。

韓國 Samsung SDI，宣佈和德國安全技術供應商 Bundesdruckerei 聯手開發出一款配備了顯示螢幕的電子護照。該種護照擁有一個能顯示護照全部內容（包含動態護照影像）的主動矩陣彩色有機發光二極體（AMOLED）顯示螢幕，其每個像素是由一個嵌入在薄膜材料中的對應電子電路來驅動。顯示螢幕厚度僅 300 微米（microns），配備顯示器、含保護膠膜的該頁面總厚度不到 700 微米。這款電子護照的顯示螢幕是透過非接觸式讀卡器來供電的。Bundesdruckerei 表示，透過該螢幕，可以檢索和顯示儲存在護照中的所有資訊，如護照持有人的動態影像，以及護照中通常包含的文字資訊，如護照持有人的個人資訊，姓名、地址以及出入境記錄。並採用了加密技術，對這款電子護照內容的讀取和更改權限進行保護。

新加坡政府在 2006 年 8 月開始全面啓用生物辨識護照，該新式電子護照將採用安全性非接觸式智慧卡晶片技術。這款晶片可以完全支援並甚至超越由國際民航組織（International Civil Aviation Organization；ICAO）所訂定的智慧型護照規格要求。所採用的 SmartMX 晶片技術，內含 72K Byte EEPROM 記憶體，擁有可以儲存指紋與臉部特徵等生物辨識資訊的高記憶體容量，並使用高度先進的加密硬體保護與駭客侵入防止措施，以降低旅行證件的僞造機會，並提升旅客的安全控管。除此之外，超低耗電訊息交換技術，在晶片感應距離上有優異表現，完全符合 ISO/IEC14443 標準電源範圍需求。並已通過德國資訊安全聯邦辦公室（German Federal Office for Information Security）的 Common Criteria EAL+ 5 安全認證。

（二）票據結合無線射頻辨識（RFID）標籤於金融防偽應用淺析

國立成功大學 碩士研究生張瑞益提出「票據結合無線射頻辨識（RFID）標籤於金融防僞應用」，所採用安全防僞機制理論說明：

1、加密及電子簽章之安全機制：

擬使用 PGP（Pretty Good Privacy），PGP 自 1991 年由 Philip Zimmermann 發表，他採用被全世界密碼學專家公認安全而且可信賴的幾種基本密碼演算法，如 IDEA、AES 對稱式文件加密演算法、RSA 或 Diffie-Hellman 的非對稱式加密演算法處理公開金鑰及私鑰之加解密、以及利用 SHA1

或 SHA2 單向雜湊函數應用於文件標註、電子簽章認證上。

其原理是利用 PGP 產生一對鑰匙，一把是私人金鑰，一把是公開金鑰。當要傳送一個保密訊息給對方時，首先必須先取得對方的公開金鑰，並將加入自己的公開金鑰環中，接下來利用對方的公開金鑰將檔案加密後再傳給對方。當對方收到加密的訊息後，對方必須利用其相對的私人金鑰來解密。 PGP 也提供 PGP 專屬電子簽章，其目的是當要公開傳送訊息時，希望讓別人知道這訊息確實是由發送者所發出，一旦加上專屬電子簽章後，任何人只要更改訊息本身或簽章的話，PGP 都能偵測出此訊息已被他人更動，並非是原來之訊息內容。另一方面 PGP 作者採用一切公開（包含其程式原始碼在內），而且是全球性的免費軟體方式發行，不致讓人懷疑會有所謂的程式暗門（Trapdoor）存在，因此更深獲全球廣大使用者的信任。

2、RFID 票據防偽構想如下：

（1）票據原磁性墨水字元識別（Magnetic Ink Character Recognition, MICR）作業相關鍵印流程不變。

（2）RFID 標籤需薄如紙張，以便於嵌入票據內；或是可以印刷方式植入票據中。

（3）設計並建置金鑰（公私金鑰）管理之驗證應用系統及 RFID 讀取器，供金融機構及發票人（客戶）使用；金鑰使用與管理採「封閉型」管理架構，信任方式採直接信任、完全信任模式。

（4）產生一把付款銀行（原存行）專門在票據簽章用的私鑰（Private Key）。

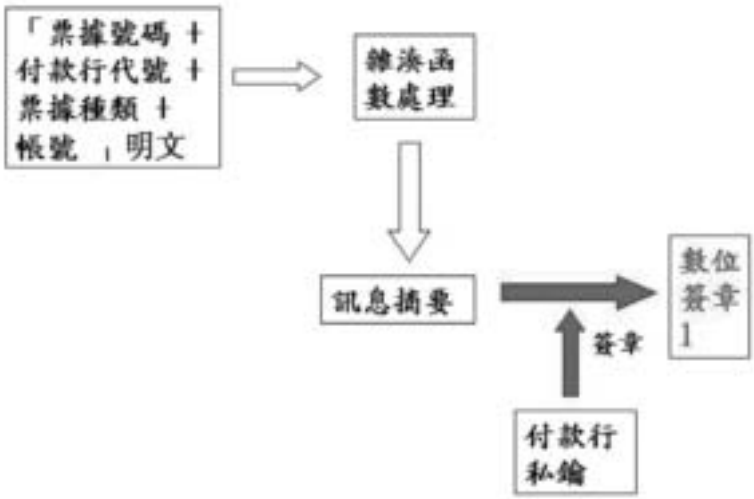
（5）每一客戶產生一把專門在票據簽章用的私鑰（Private Key）。

（6）付款銀行對每一張客戶領用之空白票據，根據它的「票據號碼、付款行代號、票據種類、帳號等資料」，使用雜湊函數處理後，用付款銀行私鑰產生一個付款銀行對該票據內容所做之數位簽章（「數位簽章 1」），如圖（十）所示。

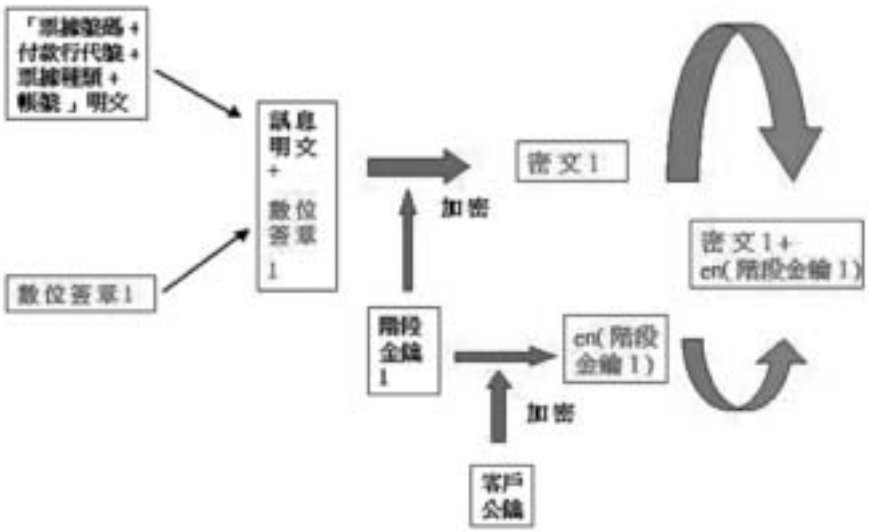
（7）付款銀行把每一張空白票據內「票據號碼、付款行代號、票據種類、帳號等資料」及「數位簽章 1」，以階段金鑰 1 加密產生「密文 1」；將階段金鑰 1 以客戶公鑰加密爲「en（階段金鑰 1）」，如圖（十一）所示；最後將「客戶金鑰 ID 明文」、「付款行金鑰 ID 明文」、「數位簽章 1」、「密文 1、en（階段金鑰 1）」寫入 RFID 標籤的記憶體內。

（8）客戶登錄領用之空白票據時，將 RFID 標籤的記憶體內資料讀出，先依據「客戶金鑰 ID」取出客戶私鑰將「en（階段金鑰 1）」解密後，再以階段金鑰 1 將「密文 1」解密，如圖（十二）所示；再依據付款行金鑰 ID 取出付款銀行公鑰，驗證「數位簽章 1」，比對空白票據原內容無誤。

（9）客戶開立票據時，將 RFID 標籤

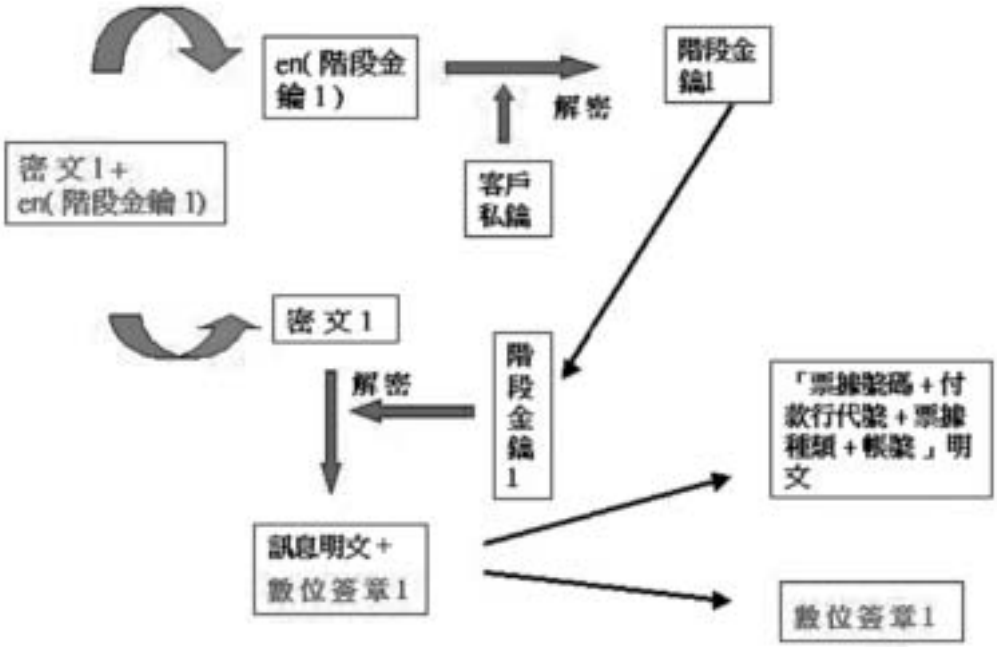


圖（十）數位簽章程序



圖（十一）加密程序

的記憶體內資料讀出，先依據「客戶金鑰 ID」取出客戶私鑰將「en（階段金鑰 1)」解密後，再以階段金鑰 1 將「密文 1」解密，再依據付款行金鑰 ID 取出付款銀行公鑰，驗證「數位簽章 1」，比對空白票據原內容無誤。再將「票據號碼、付款行代號、票據種類、帳號、發票日、開立票面金額等資料」，使用雜湊函數處理後用客戶私鑰產生一個客戶對該開立票據內容所做之數位簽章（「數位簽章 2」）。



圖（十二）解密程序

（10）客戶將每一張開立票據內「票據號碼、付款行代號、票據種類、帳號、發票日、開立票面金額等資料」及「數位簽章 2」，以階段金鑰 2 加密產生「密文 2」；將階段金鑰 2 以付款銀行公鑰加密爲「en（階段金鑰 2)」；最後將「客戶金鑰 ID 明文」、「付款行金鑰 ID 明文」、「數位簽章 1」、「密文 2、en（階段金鑰 2)」寫入 RFID 標籤的記憶體內。

（11）執票人向付款銀行提示時，付款銀行將 RFID 標籤的記憶體內資料讀出，先依據付款行金鑰 ID 取出付款銀行私鑰，將「en（階段金鑰 2)」解密後，再以階段金鑰 2 將「密文 2」解密；再依據客戶金鑰 ID 取出客戶公鑰，驗證「數位簽章 2」，比對驗證提示票據內容無誤。

（12）前項驗證提示票據內容如無法成功，則依據付款行金鑰 ID 取出付款銀行公鑰，驗證「數位簽章 1」，比對票據原內容無誤，驗證該票據確爲本付款銀行發行之票據。

（13）付款行以讀出 RFID 標籤之票據票據號碼、付款行代號、票據種類、帳號、發票日、開立票面金額等資料內容，進行票據存款應用系統資料核對、更新相關處理（連動印鑑核對及兌現）。

3. 由該研究架構經檢證歸納出以下結論：

（1）PGP 安全機制防僞運算後之安全資訊，因使用較高安全等級之金鑰長度及加密演算法，導致電子簽章及密文資訊儲存需使用之記憶體需求較大。

（2）防範票據上使用之 RFID 標籤被不當讀取、寫入、複製、追蹤，採用具有安全驗證功能之 RFID 標籤有其必要性。

（3）強制規範支票存款客戶，開立支票時一定要使用 RFID 機制，提供客戶必要之週邊設備及應用軟體系統，在推廣上有其必要性。

（4）以目前支票透過票據交換之每年流通量就高達 1 億 5 千萬張，在推廣建置 RFID 票據最大的挑戰，就是如何才能取得低價的或可重覆使用的 RFID 標籤。

（5）引進 RFID 的運用，結合票據上磁性墨水字元（MICR）的鍵印，對加強票據的防僞功能、防污辨識力，減少櫃員操作時的錯誤及負擔，加速支票核印、兌付程序，確有其可行性及便利性。

（6）爲了提高 RFID 標籤讀取率，建議選用近旁式讀取器，作近距離、逐張的讀取，如仍有發生 RFID 標籤無法讀取情事，可配合支票上鑑印之磁性墨水字元（MICR）的讀取，來執行支票兌付程序；並建議保留原支票人工簽章機制，備供 RFID 標籤無法讀取時驗印及對高面額支票雙重核驗之用。

（三）、鈔券結合無線射頻辨識技術應用淺析

在 2003 年由 Ari Juels 及 Ravikanth Pappu 兩位學者共同提出 RFID 辨識技術在歐元防僞與防洗錢之應用機制，對 RFID 鈔票提出幾點需求特性。不僅是歐洲，連日本和美國都有意使用 RFID 鈔票。RFID 鈔票最大的好處就是防僞鈔和防洗錢。當 RFID 嵌入鈔票後，鈔票就不能使用彩色列印機或複印機來進行僞造，如德國的 Bundesbank 銀行期望 RFID 應用在鈔票中。

表（四）Juels-Pappu 的 RFID 防僞鈔機制

RFID			
Cell β un-readable / keyed-writable	Cell γ universally-readable / un-writable	Cell δ keyed-readable / keyed-writable	Cell ε keyed-readable / un-writable
$Enc(PK_I, \sum \| S, r_1)$	$C = Enc(PK_I, \sum \| S, r_1) \oplus r_2$	r_1	r_2
Optical			
S		$\sum = Sign(SK_B, S \| den)$	

表（五）RFID data on the proposed banknote for Approach 1.

RFID	
Cell γ universally-readable/keyed-writable	Cell δ keyed-readable/keyed-writable
$C = Enc(PK_L, \sum \| S, r)$	r
Optical	
S	$\sum = Sign(SK_B, S \| den)$

此外，RFID 具有可追蹤性，可以達到防洗錢的功能。

國立東華大學研究生陳潔如改進了 Juels-Pappu 的 RFID 防僞鈔機制，設計了兩種不同的方法。方法一利用增加標籤的記憶體來提高整套機制的安全性，方法二中則是增加的記憶體的數量較少，但需要較多的運算次數。

方法一：增加兩個額外的記憶體 β & ε，記憶體 β 是不能讀取但可用金鑰 DM 開啓寫入；記憶體 ε 是不能寫入但可用金鑰 DM 或 DL 開啓讀取資料；在 Juels-Pappu 的 RBPS 中的記憶體 γ 是從（一般讀取 / 金鑰開啓寫入）調整爲（一般讀取 / 不能寫入），記憶體 δ 及光學資料則與 Juels-Pappu 的 RBPS 中功能相同。標籤本身在記憶體 β 被金鑰開啓寫入資料後，會自動執行將記憶體 β 和記憶體 ε 的邏輯運算結果儲存在記憶體 γ 中 "（β）⊕（ε）→（γ）"。當記憶體 γ 被詢答時，就會去執行兩個控制運算 "R（ε）→（ε）" 及 "（β）⊕（ε）→（γ）"，其中 "R（ε）→（ε）" 是表示在記憶體 ε 所儲存具有 80bit 的隨機亂數值的選擇。

方法二：只有增加一個記憶體，記憶體 ε 功能與方法一興同；記憶體 γ 、記憶體 δ 及光學資料則與 Juels-Pappu 的 RBPS 中功能相同。當記憶體 γ 被詢答時，標籤本身就會去執行三次的控制運算 "（γ）⊕（ε）→（γ）"、"R（ε）→（ε）" 及 "（γ）⊕（ε）→（γ）"；而標籤本身在記憶體 γ 被金鑰開啓寫入資料後，會自動執行 "（γ）⊕（ε）→（γ）" 的邏輯運算。

操作驗證步驟分爲四個階段來完成查核工作：

（1）紙鈔的生產製作階段

（2）紙鈔的發行查核階段

（3）紙鈔的匿名使用階段

（4）紙鈔的追蹤階段

兩種不同的方法中，主要差別在於方

表（六）RFID data on the proposed banknote for Approach 2.

RFID		
Cell γ universally-readable / keyed-writable	Cell δ keyed-readable / keyed-writable	Cell ε keyed-readable / un-writable
$C = Enc(PK_L, \sum \| S, r_1) \oplus r_2$	r_1	r_2
Optical		
S	$\sum = Sign(SK_s, S \| den)$	

表（八）Attack-prevention ability for the Juels-Pappu RBPS and our RBPS

系統種類 / 攻擊類型	J-P RBPS	方法一	方法二
扒手攻擊	X	X	X
資料恢復攻擊	X	O	O
密文追蹤	X	O	O
存取金鑰追蹤	X	O	O
Cookies 威脅	X	O	O
阻絕服務攻擊	X	O	O
睡眠與死亡鈔票	X	X	X

O：克服攻擊； X：被攻擊擊退

法一增加記憶體空間來減少運算次數，方法二則是以增加運算次數來維持較低的記憶體需求量。而原本 Juels-Pappu 的 RBPS 機制中所無法克服的多數攻擊也得到了解決。

此外，呂崇富、奚正德、張克章等多位學者都曾提出關於有價票證加上無線射頻辨識標籤建構假設，再配合銀行或金融機構的原有驗鈔機加裝可讀取無線射頻辨識的功能，則可以快速又大量的鑑別鈔票眞僞。

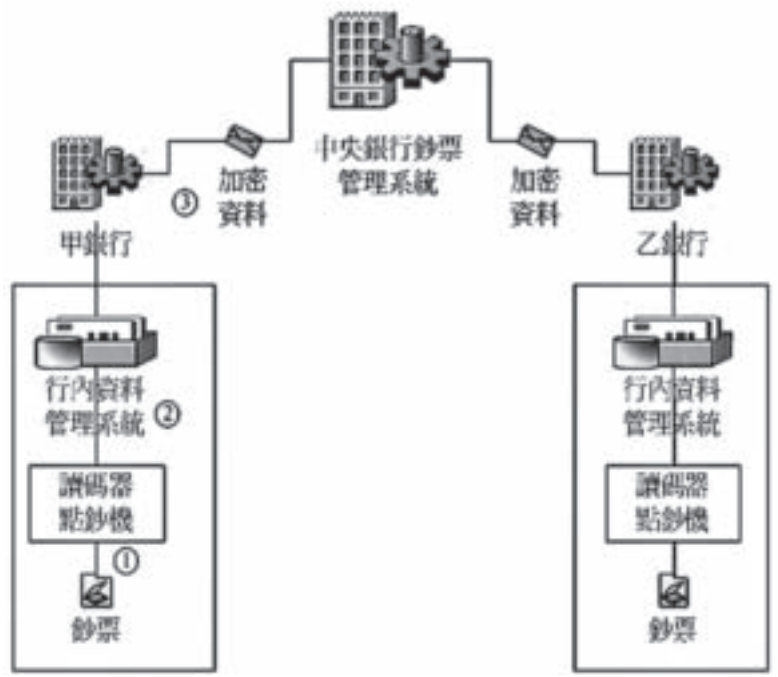
這個 RFID 鈔票防僞驗鈔流程可以簡述如下圖（十三）所示：

（1）經過具有無線射頻辨識讀取功能的點鈔機，暫名爲「讀碼驗鈔機」，先讀取所有鈔票號碼，並且與鈔票張數比對，若數量不符，則應有部分鈔票不具有無線射頻標籤，就研判可能是僞鈔，立即提出警告。

（2）將讀出鈔票號碼與行內資料庫比對，若有重複，亦判屬僞鈔。

（3）將讀出鈔票號碼經加密傳輸管道，送至中央銀行的鈔票管理系統，經資料比對後，若發現與他行號碼重複，亦判屬僞鈔。

另外，針對鈔票的序號、讀碼驗鈔機及無線射頻標籤等技術規劃一個簡易 RFID 新台幣防僞構想如下：



圖（十三）廠融防偽系統架構圖

（1）無線射頻標籤需薄如紙張，以便於嵌入鈔票內，並且嚴格控管所有標籤流向，使歹徒不能複製或取得相似標籤。

（2）產生一把中央銀行總裁專門在鈔票做簽章用的私鑰（Private Key）。

（3）對每一張鈔票根據它的序號、票面額、發行日期、發行地方等資料，用央行總裁的私鑰產生一個簽章。

（4）把每一張鈔票的獨特簽章，寫入無線射頻辨識標籤的記憶體內。

（5）把製成的無線射頻辨識標籤，在製鈔過程中嵌入鈔票內。

（6）設計並建置內含央行總裁公鑰及具備無線射頻辨識接受器功能的特製讀碼驗鈔機。

（7）讀碼驗鈔機係經根據 FIPS-140 的安全需求所設計的裝置，防止歹徒的仿製或經由逆向工程而加以破解。

（8）在無線射頻辨識標籤和驗鈔機裡設計一套簡單而適當的「交互認證（mutual authentication）」通訊規程，讓無線射頻辨識標籤辨識對方如果是合法授權的驗鈔機的話，就讓它讀取標籤內的鈔票簽章，否則就拒絕回應；而讓驗鈔機也可以用機內的央行總裁公鑰，驗出所持的鈔票是否爲眞鈔。

由於 RFID 標籤技術上的不易複製，再加上非法的驗鈔機無法讀取 RFID 標籤進而

得知標籤內容和其他秘密來仿造標籤，如果我們又提升驗鈔機的安全門檻，即使他們經由「倒轉工程（reverse engineering）」或其他類似方法都無法仿製。

（四）、無線射頻辨識（RFID）標籤結合所有權狀防偽機制淺析

楊淯婷提出 應用無線射頻辨識（RFID）技術於所有權狀防僞機制的構想；

1、防偽　證機制需求解析：

由 RFID 防僞分析可知「寫入型」作爲防僞驗證機制似乎是快速導入 RFID 的較佳方案。RFID 晶片從工廠生產出來後，即已被賦予一個 ID 編碼，基本上這個無法被修改的 ID 編碼就是使用權狀的最佳辨識機制。

而且 RFID 標籤其複製難度極高，若經由非法複製之 RFID 標籤，其除變爲需要外部電源才可將自身之 ID 與記憶體發射予讀卡機接收外，其外型亦將變得龐大，使得他人極易分辨出其爲非法複製品。

此外，爲了保證 IC 晶片不會被複製，可在晶片中預留一些欄位進行資訊加密作業，我們可以利用政府憑證管理中心（GCA）所發出之電子憑證，進行電子簽章加密機制，於簽發權狀時對其內嵌之 RFID Tag 作數位簽章，確保該 RFID 之內容不被竄改；另外，也可以利用雜湊函數（例如 MD5）對 RFID 的 ID 進行編碼，以求出防僞校對字組，並於地政單位使用者端應用系統提供數位簽章之查檢功能。

除此之外，目前各地政機關均已建置「土地登記複丈地價地用整合系統」，加上 RFID 中介應用軟體的需求僅止於對 RFID ID 進行加密、解密與電子簽章，因此，可直接於現行「土地登記複丈地價地用整合系統」中新增加密、解密與電子簽章功能，只要於「土地登記複丈地價地用整合系統」之地籍資料庫增加儲存 ID 之資料，即可直接將 RFID Tag 的資料與地籍資料庫結合。

總結上述之分析，應用 RFID 技術於所有權狀防僞的整體系統架構，可分成「權狀核發」與「權狀驗證」兩個程序，「權狀核發」程序係在權狀核發單位在現行權狀核發程序中加入 RFID 防僞機制；「權狀驗證」程序則爲接受民眾持具有 RFID 防僞機制之地政機關（本機關或上級機關），對權狀上之 RFID 進行防僞驗證。以上兩個程序分別說明如後：

2、「權狀核發」程序

（1）先完成現行程序之權狀製發作業，包含資料庫建檔與權狀印製。

（2）地政單位所核發之權狀，是透過「土地登記複丈地價地用整合系統」前端軟體新開發之「ID 加密／解密子系統」，將唯一性之 ID 編碼（例：A123456789）寫入「土地登記複丈地價地用整合系統」後端資

料庫新增之欄位，該 ID 編碼即可與原權狀記載之資料結合。

（3）透過「土地登記複丈地價地用整合系統」前端軟體新開發之「ID 加密／解密子系統」，利用 MD5 雜湊函數將該 ID 編碼運算得到一編碼後之數值（例：3Xy$wr&W9as），並同時以前端軟體新開發之「電子簽章子系統」，以權狀核發機關之 GCA 政府憑證（私鑰）製作核發權狀之地政單位的電子簽章。

（4）以上 2. 及 3. 步驟完成後，自動以 RFID 讀寫器（Reader/Writer）將編碼後之 ID（3Xy$wr&W9as）及核發權狀之地政單位的電子簽章寫入擁有可供一次編制、非易變性（non-volatile）記憶體之 RFID 唯讀 class 1 標籤。

（5）完成以上防偽步驟後，即可將 RFID 標籤貼於權狀上核發。

3、「權狀　證」程序

（1）地政單位承辦人員從民眾申辦業務所提送權狀上記載之地籍資料（如 xx 段 xx 地號與土地所有權人姓名），自「土地登記複丈地價地用整合系統」後端資料庫查出該權狀之電子資料錄，該資料錄上應包含權狀上之 RFID 標籤的「原始 ID」紀錄欄（例：A123456789）。

圖（十四）RFID 所有權狀核發流程圖

（2）地政單位承辦人員以 RFID 讀寫器，透過「土地登記複丈地價地用整合系統」前端軟體新開發之「ID 加密／解密子系統」讀取權狀上之 RFID 標籤，此時，「ID 加密／解密子系統」會自動將自後端資料庫查得之「原始 ID」進行 MD5 雜湊函數運算，並將運算後得到之數值與 RFID 標籤上紀錄之加密後的 ID 值比對（例：3Xy$wr&W9as），假如兩個值相符，即表

圖（十五）RFID 所有權狀　證流程圖

示通過第一道驗證。

（3）在進行前項 ID 驗證時，「土地登記複丈地價地用整合系統」前端軟體新開發之「電子簽章子系統」，會在 RFID 讀寫器讀取權狀上之 RFID 標籤的同時，亦以 GCA 憑證（公鑰）驗證該標籤上紀錄之電子簽章是否確爲原發狀單位所核發，假如驗證結果該電子簽章確爲原發狀單位所核發，即表示通過第二道驗證。

（4）以上驗證程序如果不計「土地登記複丈地價地用整合系統」後端資料庫搜尋時間，整個程序應可在一分鐘內完成，且由於技術成熟，準確率應可達百分之百。

（5）必要時仍可以權狀上之原始印刷防僞機制再進行雙重驗證。以上完整之「權狀驗證」程序詳圖。

4、無線射頻辨識（RFID）標籤結合所有權狀防偽機制之效益分析

在我國，由於工研院、資策會等研究單位，及微軟、惠普等軟硬體大廠相繼投入研發經費，全力發展 RFID 技術，因此，技術導入的門檻也相對甚低。

在硬體方面，有 RFID 標籤、RFID 讀寫機與驗證 GCA 電子憑證之讀卡機。就 RFID 標籤（Tag）而言，國產 RFID 標籤成本約新台幣 10 元以下。目前紙質權狀的成本約新台幣 8.7 元，塑膠權狀的成本約 14 元，但書狀核發的規費爲 80 元，因此，增加 RFID 防僞技術後，每張權狀製作成本的提高應尚在合理範圍；就讀寫機（Reader/Writer）而言，研究建議採低頻率、近距離規格的手持設備，其成本約在新台幣 20,000-30,000 元左右。另外，驗證 GCA 電子憑證之讀卡機市約 200-300 元。

就軟體而言，需配合透過「土地登記

複丈地價地用整合系統」前端軟體新開發之「ID 加密／解密子系統」與「電子簽章子系統」，均屬原有系統之功能擴充，且相關技術均爲成熟之應用技術。

總而言之，無線射頻辨識（RFID）標籤結合所有權狀防僞機制系統架構，對現行的政府財政將不會造成負擔，而且技術導入的門檻低，也不會產生研發期過長之問題。

八、未來展望

未來 RFID 的發展方向，應就各個產業的需求而朝向產業別甚至於是客製化發展；而在有價票證產業中的應用來看，目前多停留在學術領域的研發階段，在實際應用上也僅止於 epassport 的運用，至於金融票據、紙鈔、土地權狀及身分證或駕照等等，還有一些技術上的瓶頸及軟硬體之間的搭配都是有待克服的議題；因此，RFID 技術未來將朝向下列幾個方向發展：

（一）內嵌式標籤： 隨著 RFID 技術的發展，以及 RFID 標籤技術愈趨於成熟，且相對的生產成成本的大幅降低，內崁 RFID 標籤的包裝材料將是一個趨勢；內崁 RFID 標籤技術將有助於 RFID 的普遍性應用。

（二）RFID 標籤技術上的不易複製，以及即使被複製也可以用驗證的程序讓 RFID 系統把僞造的 RFID 標籤揪出來的特性；再加上採用 PKI 技術於 RFID 標籤中，來做到以「公共金鑰密碼系統」爲基礎類似「電子浮水印」的高階安全水準，使得僞鈔業者等仿冒集團難以得逞。

（三）Item level RFID： RFID 的技術成熟，會由大型物品的應用發展至小包裝的物品。應用層級由 Container、Pallet、Case level 逐漸發展至 Item-level RFID。而這些數以萬計 Item-level 的 RFID 資料會有跨企業、跨產業的交換需求，後端支援的系統架構與平台標準也會慢慢的成熟。

（四）智慧型 RFID 標籤： 未來會有愈來愈多結合 RFID 與感應器、嵌入式系統的創新產品出現。當 RFID 與溫度計、感應器、顯示器等物品結合，其中 RFID 扮演了一種可攜式的資料儲存媒體、以及與後端系統的溝通介面。

（五）發展與改善具有加密功能、對稱式加密、信息授權碼和隨機號碼產生器的硬件，將會增進 RFID 的安全性。如今，透過公開密碼匙技術，RFID 供應商也將其應用在協助改良機密性、使用者認證和 RFID 標籤及隱私相關的議題。

九、結論

由以上的探討可知，RFID 在有價票證防僞上的應用，可說是潛力無窮，因此，

希望藉由本篇文章的探討，可以提供金融機構及政府相關主管機關在有價票證的防僞技術上，多一種尖端科技的選擇；有人說消費者的需求是教育出來的；同樣的道理，在有價票證防僞的角度來看，防僞技術的複雜度再配合尖端科技的運用，才能夠眞正的達到有效阻卻仿冒、僞變造的機會；而 RFID 技術還具有防止洗錢的功能，更是現今貨幣體制中所極度缺乏的項目，而必須要靠人爲通報發現，往往緩不濟急甚至發生疏漏、吃案等弊端，如果能夠成功的將 RFID 技術建置在紙鈔上，那將會開啓有價證券防僞、防盜、防變造及防洗錢技術嶄新的史頁，也能夠間接的幫助金融產業及政府相關主管機關在管理制度方面更加健全與活絡。

參考資料

1. 鄭博仁、陳林福、陳品儀、謝德鑫，" 有價票證防僞架構 "，無線涉頻便是技術與資訊安全應用，資訊安全技術通訊，第 10 卷，第二期，頁 78 ～ 86，2004。
2. 鄭博仁，"RFID 無線射頻辨識在金融防僞之應用 "，財金資訊雙月刊，第 044 期，2006。
3. 張瑞益，" 票據結合 RFID 標籤於金融防僞之應用 "，國立成功大學工程科學系，碩士論文，2007。
4. 陳潔如，" 應用無線射頻認證技術之紙鈔防僞機制 "，國立東華大學資訊工程學系，碩士論文，2007。
5. 林致祥，" RFID 應用在服裝業的經營管理 "，私立亞東技術學院，碩士論文，2007。
6. 楊淯婷，" 應用「RFID（無線射頻辨識）」技術於所有權狀防僞之初探 "，台中市地政事務所，2005。
7. 周桂田，"RFID 的效益與風險 "，科學發展月刊，第 427 期，2008/7。
8. 鄭博仁、陳秋華、蝗崇哲、陳聖輝、何皇寬，" 已知 RFID 鈔票隱私保護機制的缺失與改善 "，財金資訊雙月刊，2008。
9. 呂崇富，“RFID 鈔票之隱私保護機制”，電子商務學報，第 9 卷，第 3 期，2007。
10. RFID 應用推動辦公室網站
11. 精聯電子網站
12. http://www.tu-braunschweig.de/Medien-DB/iff
13. www.twce.org.tw/twce/epaper/246/index.htm
14. www.teema.org.tw/default.asp
15. www.eettaiwan.com/

曲文豪／中央印製廠