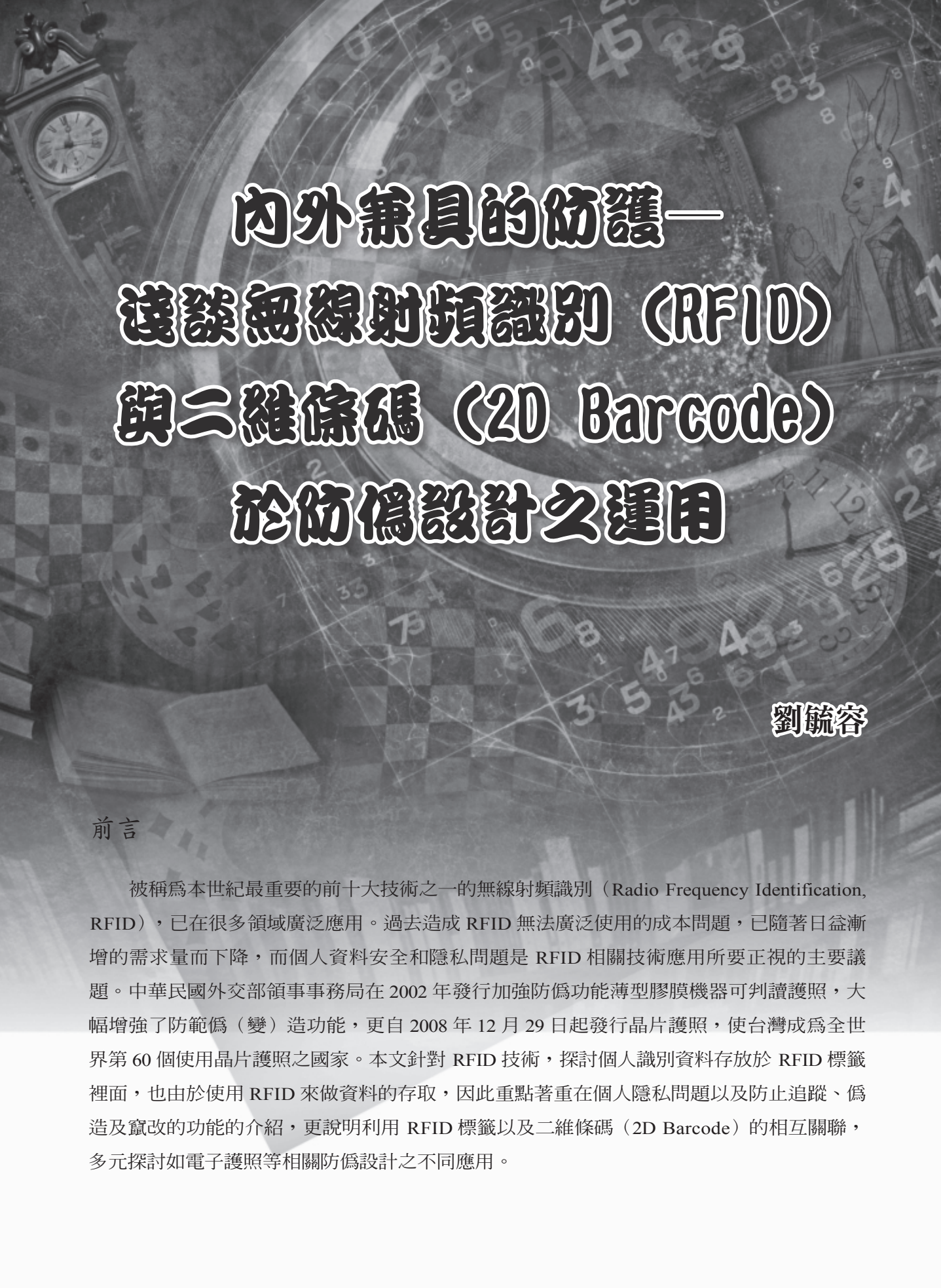




內外兼具的防護— 淺談無線射頻識別 (RFID) 與二維條碼 (2D Barcode) 於防偽設計之運用

劉毓容

前言

被稱為本世紀最重要的前十大技術之一的無線射頻識別 (Radio Frequency Identification, RFID)，已在很多領域廣泛應用。過去造成 RFID 無法廣泛使用的成本問題，已隨著日益漸增的需求量而下降，而個人資料安全和隱私問題是 RFID 相關技術應用所要正視的主要議題。中華民國外交部領事事務局在 2002 年發行加強防偽功能薄型膠膜機器可判讀護照，大幅增強了防範偽 (變) 造功能，更自 2008 年 12 月 29 日起發行晶片護照，使台灣成為全世界第 60 個使用晶片護照之國家。本文針對 RFID 技術，探討個人識別資料存放於 RFID 標籤裡面，也由於使用 RFID 來做資料的存取，因此重點著重在個人隱私問題以及防止追蹤、偽造及竄改的功能的介紹，更說明利用 RFID 標籤以及二維條碼 (2D Barcode) 的相互關聯，多元探討如電子護照等相關防偽設計之不同應用。

壹、緒論

被稱之為 21 世紀十大發明的無線射頻識別 (Radio Frequency Identification, RFID)，筆者在印刷科技第 32 卷 1 期中已介紹說明，RFID 的應用也早已環繞在我們生活之中，舉凡是購物、借書、坐公車、高速公路的 ETC 等等，均可知 RFID 正廣泛地被使用著。因此隨著 RFID 的使用量逐漸擴大，低價的 RFID 標籤 (Tag) 運用不再遙不可及，也讓 RFID 有機會擴大到其他領域來延伸，創造商品的附加價值，並且提高企業的競爭力。然而即使 RFID 看起來前程似錦，但事實上卻存在一些尚待解決的問題。RFID 應用的領域不同，所關注的焦點也有所不同，如物流業與身分識別方面，物流業相對關心讀取範圍以及降低成本，高於對身分識別方面的考量，相反的若針對個人資料相關安全考量，身分識別則需要將讀取範圍降低至安全的程度之內。

個人的重要證件，如：身分證、健保卡、駕照、護照等，近來常在傳媒看到遭非法分子偽 (變) 造，此類的社會問題層出不窮，讓政府不得不重視這樣的問題。自 2001 年美國發生 911 恐怖攻擊事件以來，全球各國都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，希望能降低不當與非法人士的滲透，避免再一次的悲劇

發生。近年來，陸續見到歐、美、亞洲各國均開始依國際民航組織 (International Civil Aviation Organization, ICAO) 的規範，生產晶片護照與正式製發晶片護照作業；國際民航組織定義了晶片護照的主要目的包括：

- A. 對於護照的高度防偽。
- B. 通關自動化。
- C. 順暢的國際旅遊。

回顧歷史，由於美國移民政策要求在 2006 年 10 月前，全球 27 個免簽證計畫 (Visa Waiver Program, VWP) 會員國都必須實施晶片護照，否則將失去其免簽證待遇，使得世界各國積極投入晶片護照的製發作業。然而，若是將個人識別身分資料放在 RFID 晶片上，將有可能被不法人士竊取、蒐集與使用，因此電子式護照最大的隱憂在於隱私權的議題。關於護照上的個人資料能被如何利用，除了出 (入) 境的查驗外，是否會有其它目的之蒐集與利用情況，可參照「電腦處理個人資料保護法」。本文彙整介紹採用二維條碼以及一次性密碼 (One Time password, OTP) 的方式，來保護在 RFID 標籤裡面的個人識別資料，避免遭到有心人士在 RFID 標籤與讀取器存取之間，利用監聽的方式，來竊取資料而造成個人隱私的外洩，甚至複製 RFID 標籤來進行非法行為，以進一步達到個人安全隱私的保護。

中華民國外交部於 2008 年 12 月 29 日發行晶片護照，使台灣成為全世界第 60 個使用晶片護照之國家。相較於傳統護照，新版晶片護照最大特色在於底頁植入一枚非接觸式晶片，用來儲存資料頁登載資料及持照人照片影像，資料一經寫入無法更改，更可大幅提升護照防偽功能。新版晶片護照外觀維持不變，僅於封面加印晶片護照標誌（），內頁之圖案全部更新，以台灣南北景點地標及風土民情為圖案主題。護照晶片儲存內容並無指紋、虹膜等項目，使個人隱私可獲保障。晶片有效讀取距離僅數釐米，在正常使用情形下，護照資料無遭竊之虞。晶片護照之發行，不僅符合國際趨勢，目前國內外各地機場晶片護照配套查驗設備陸續建置日漸完善，亦有效縮短通關時間。本文彙整相關論文研究資料並探討使用 RFID 技術，將個人識別資料放入 RFID 標籤裡面，除了改善護照變更資料不易，且著重個人隱私問題以及防止追蹤、偽造及竄改的功能，同時參考歐元導入 RFID 的做法，以其現行使用 RFID 的安全隱私問題解決方案，以保護個人隱私資料外露及防止個人遭到追蹤。並探討將二維條碼與 RFID 標籤產生關聯，若無法同時取得儲存其中的兩者資料，便無法得到持照人較為隱私之個人資料，以此達到互相牽制的功能。本文同時分析比較智慧卡與 RFID 在硬體安全機制、資料的安

全性、基本特性及成本各方面之差異，分析比較以在成本上較佔有優勢的 RFID 與普遍使用的智慧卡（Smart Card）之差異與不同運用。

貳、RFID 與二維條碼（2D Barcode）

針對防偽設計與其他國家導入的經驗，以下針對 RFID 與相關技術個別探討說明，期望讓閱讀者對 RFID 標籤與其相關技術，能有更完善的認識與了解。

一、RFID 簡介

RFID 是一種無線識別技術，透過在商品上的標籤，把商品資訊連至後端系統裡，用來追蹤、識別與確認商品的狀態。比起目前條碼系統具有更高的效率與彈性，其最大的好處就是提高整體物品管理效率及節省人力成本。

雖然 RFID 的功用與條碼相同，但 RFID 除了具有長距離讀取資料的特性，還可一次讀取數百筆資料，節省大量時間，並且可以無限擴充，功能遠遠強過二維條碼，下面就 RFID 與條碼（Bar code）的比較，如表 2-1 整理所示。

（一）RFID 系統架構

針對 RFID 系統架構，筆者已於本季刊第 32 卷 1 期中有關 RFID 的文章中詳細說

表 2-1：RFID 與條碼比較表

功能	條碼 (Bar code)	RFID
成本	低	高
讀取速度	限制移動速度	可高速讀取
耐污性	低	高
讀寫能力	資料不可更新	可反覆被覆寫
讀取方式	直視標籤	不須特定方向與光線
讀取距離	短 (0-50 公分)	長 (0.1~10 公尺)
讀取數量	一次一個	一次多個
資料容量	小	大
仿製	易	較難

資料來源：本文整理

明，於此彙整介紹 RFID 系統架構主要是由標籤 (Tag)、讀取器 (Reader)、後端應用系統 (Back-end Application System) 所組成，透過這三者之間的溝通，來達到無線辨識的功能。以下分別概述三者：

1. 標籤 (Tag)

RFID 標籤是一個可以儲存數位資料的小型裝置，可以透過無線電波與讀取器之間互相傳遞資訊，大部分的 RFID 標籤可分為三類：

(1) 被動式 (Passive)：被動式電子標籤其能源是由讀取器提供，所以標籤上不需附加電池，所以體積小、使用期限較長，但是讀取的距離較短。

(2) 半被動式 (Semi-Passive)：半被動式與被動式不同之處是多了一個電池，

電池的電力剛好可以驅動標籤，使得標籤處於工作的狀態，比起被動式，半主動式有更快的反應速度，更好的效率。

(3) 主動式 (Active)：主動式與被動式不同的部分是其標籤是附加電池的，系統另外增加所謂的喚醒裝置，平時標籤是處於休眠的狀態，當標籤進入喚醒裝置的範圍時，喚醒裝置利用無線電波或磁場來觸發或喚醒標籤，標籤這時才進入正常工作模式，開始傳送相關資訊，由於本身具備工作所需之電源所以傳輸距離較長，但是相對具有體積較大、需更換電池及成本較高等缺點。

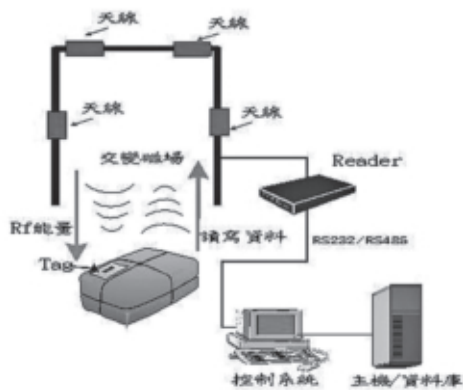
2. 讀取器 (Reader)

讀取器內含控制器及天線，大多數會與應用系統結合使用，來接收主機端的命

令，對於儲存在標籤的資料以有線或無線方式傳送回主機，電子標籤的識別速率每秒可達 50 個以上。有些 RFID 設備可以將資料寫入電子標籤中，稱為寫入器（Writer）；同時具備讀取和寫入功能的設備就稱為讀寫器（Reader/Writer）。

3. 後端應用系統（Back-end Application System）

RFID 系統結合資料庫管理系統、電腦網路與防火牆等技術，提供全自動安全便利的即時監控系統功能。相關整合應用包括航空行李監控、生產自動化管控、倉儲管理、運輸監控、保全管制以及醫療管理等。



RFID系統基本架構圖



資料來源：

（二）RFID 使用現況介紹

RFID 的運用早已圍繞在我們日常生活

當中，搭乘捷運會用到的「悠遊卡」，7-11 買東西用的「VISA WAVE」信用卡，寵物身上植入的「寵物晶片」，百貨公司或圖書館內的「防盜晶片」等，這些都是 RFID 在我們日常生活中的實際應用。而除了上述的應用之外，RFID 在其他領域中也相當頻繁地被使用，整合筆者在印刷科技第 32 卷 1 期中已介紹說明，將 RFID 使用現況介紹如下：

1. 身分識別

RFID 標籤可嵌入到身分證、護照、工作證的各種信任狀中，作為人員身分識別；也可植入動物皮下來追蹤，研究和保護動物。在 ISO-11784/5 規範裡已有對動物應用 RFID 做明確的說明，最大的特點在於使用低頻（Low Frequency, LF）頻段，乃因對動物的生理影響最小的電磁波在 125~135KHz 間，稍微高於動物可聽見的音頻範圍，同理，用在人身上的 RFID 也應該是低頻，若用於醫療處所，應避免使用高頻（High Frequency, HF）或超高頻（Ultrahigh Frequency, UHF），而低頻標籤的技術因穩定且成本低廉，目前許多歐美國家以及亞洲國家皆已開始把 RFID 標籤植入畜養動物的體內，加強管理以及避免因動物引起的疫情擴散，相關 RFID 標籤使用參考因素如表 2-2。

2. 防偽應用

RFID 自 2004 年被 Wal-Mart 炒熱後，

表 2-2：RFID 標籤選用因素參考

參考因素	LF（低頻）	HF（高頻）	NF-UHF（近距離超高頻）	FF-UHF（遠距離超高頻）
水與濕度	適用	適用	適用	不適用
抗金屬	適用	受挑戰	受挑戰	受挑戰
讀取距離	0.5M	1.5M	0.5M	7M
控制範圍	容易	容易	容易	不容易
商業應用	成熟	成熟	試用中	成熟
可靠性	穩定	穩定	具挑戰	具挑戰
頻率合法性	國家限制	國家限制	國家限制	國家限制

資料來源：本文整理

應用層出不窮，防偽的應用當然也是其一。RFID 在防偽應用的主要優勢包括編碼不僅為暗碼，而且可加密，正可解決過去條碼與雷射標籤容易複製的缺點，可望成為未來企業防偽解決方案的主流技術。日本近期計畫在大額紙鈔上建入的 RFID 標籤，體積僅有 $0.4\text{mm} \times 0.4\text{mm} \times 4\mu$ ，用實物來比擬，大約等於 1 顆芝麻的 $1/2$ ，而且之前造成體積無法縮小的最大障礙——天線，已被整合到晶片內，由於天線縮短，這種標籤無法長距離讀取，不過紙鈔、身分證件、精品類的真偽鑑定，本來就不需要長距離讀取，多半是以手持式裝置進行判讀即可。如此只要拿著手持式裝置，就可以輕鬆掃過一疊鈔票來辨識是否有偽鈔，減輕工作人員查驗的負擔。

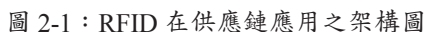
3. 供應鏈應用

目前在 RFID 的應用之中，就屬供應鏈

應用最為廣泛及深入，但同時他的技術難度也是最大的，基於 RFID 標籤成本的考量，也讓此部分成為是最難實現的應用，因為若是要在所有的商品上都貼上標籤，首先要面對的是標籤的成本，再來是龐大的資料需要複雜的後台管理軟體與流程，應用架構如圖 2-1。

4. 運動競技

國際足聯在 2006 年由德國主辦的世界盃全部 12 個會場中，均使用 RFID 電子門票系統，當時考量因球票黑市十分猖獗，很多人要花 2000 歐元購買一場球賽的入場券（如圖 2-2）。更嚴重的是，球票市場有大量的假票在市場上流通而引起混亂，由於 RFID 門票防偽性較高，並且可在近距離識別設備 10 釐米內進行快速方便的非接觸式驗證，從而確保觀眾安全並方便的進入賽場，根據報導指出，FIFA 與飛利浦電子



攜手合作提供的 MIFARE 票證技術，將 RFID 技術應用於全球性賽事的體育場管理，讓飛利浦不僅看到、更實際吃到世足賽商機。世界盃足球賽的共有三十二支國家代表隊出賽，比賽將在十二個球場輪番上陣。在整個賽期內，從慕尼黑的安聯體育場到萊比錫的中央體育場，都將採用飛利浦的票證技術，確保球迷能安全方便地進入球場，同時也證明 RFID 技術相當適合應用於全球性賽事的體育場管理，當球迷抵達球場入口處時，只需將具內建晶片的紙質門票通過掃描識別，便能快速安全的入場。此外，新的識別技術還可遏止黃牛行為以及偽造門票。三百二十萬張全部採用 RFID 技術的門票，將確保門票真正的持有人才可入場。飛利浦的 MIFARE 智慧卡

65



資料圖片來源

圖 2-2：2006 年德國世界盃門票（內有 RFID 外有數位列印資料與條碼）



資料圖片來源

圖 2-3：圖示 RFID 運動手環的量产應用

識別，同時，也可為其在運動員賽場內消費管理及藥檢的樣品進行標註。

5. 交通管理應用

交通管理的應用可說是 RFID 應用中最成功、也是最早被應用的實際例子之一，例如：台北市捷運公司所推行的悠遊卡（如圖 2-4），利用非接觸式 IC，使用 13.56MHz

頻率下的 ISO/IEC 14443 標準，悠遊卡採用晶片為 NXP 公司（前身為 Philips）的 Mifare S50 晶片，也稱 Mifare Std 1K；單程代幣採用晶片為 NXP 公司的 Mifare Ultra light 晶片；但由銀行發行的悠遊聯名卡又是另外一顆更高安全等級的晶片。感應距離一般為 1~5 公分，搭配較大的讀頭天線可到 10 公分。感應距離跟銅線繞線長度與面積都有關係，繞線長度是要調整 Q 值（品質因素）以達到最佳感應效果，品質因數 Q 值表示一個儲能器件（如電感線圈、電容等）、諧振電路所儲能量同每週損耗能量之比的一種質量指標，感測元件的 Q 值愈大，用該元件組成的電路或網絡的選擇性愈佳，感測元件的 Q 值越高，損耗越小而效率越高，諧振器的頻率穩定度就越高，也因此感應能夠更準確；總而言之，繞線面積愈大則感應距離愈遠，在此感應原理下得知悠遊卡 > 悠遊錶 & 單程代幣。也由於電子車票具有交易便捷，快速通過，可靠性高等優點，因此越來越多的城市也將採用電子



資料圖片來源

圖 2-4：台北市捷運公司悠遊卡示意圖



圖 2-5：亞洲 RFID 運輸應用



資料圖片來源

車票，並且擴大其使用的範圍，有關亞洲各國將 RFID 運用於交通管理卡片可參圖 2-5 所示。

6. 航空旅運及國土安全應用

有價票券的安全要求甚高，利用 RFID 可驗證紙鈔或支票等有價票證之真偽，以達到安全之需求，而在交通上如捷運、公

車等，使用 RFID 可進行儲值，達到安全方便的效果。目前航空公司透過「條碼標籤系統」來分辨將旅客的拖運行李運到何處，但在理想的狀況下，「條碼標籤系統」只能在 10 件拖運行李中正確讀取 8 至 9 件，這意味著航空公司必須投入大量的時間與人力以採用人工分辨行李並運送到正確的航班上，如此常會造成旅客的行李遺失。另外恐怖組織利用拖運裝有爆炸物的行李但人並未登機，以致造成飛機墜毀的悲劇，如 90 年代印度航空公司飛機在大西洋墜毀及美國 747 在蘇格蘭墜毀，所以現在航空公司為加強反恐，均強制執行已登機旅客與拖運行李的檢查比對，然而要人工從一架飛機所載運的所有行李或是由貨載裝置（ULD）準備裝機的行李當中找到目標行李，是件非常困難的事，還常會因此延誤飛機起飛時間，間接影響到航空公司聲譽。所以在恐怖主義盛行及航空市場需求的推動，「RFID 行李追蹤系統」已被應

用在行李檢查中。而國際航空運輸組織（International Air Transport Association；IATA）也早於 2004 年 6 月在所提出的業務簡化四大計畫中，將「無線辨識系統（RFID）行李標籤」此項 RFID 應用納入其中，計畫以 RFID 技術取代條碼。根據美國達美航空測試「RFID 行李追蹤系統」，在一次對 4 萬件行李的處理中，裝有 RFID Tag 的行李讀取準確率達到了 96.7%~99.8%，比起努力提昇現行的「條碼行李傳送系統」工作效能，行李讀取準確率最高仍只能達到 85%，準確度明顯強大許多。目前全世界航空公司每年需拖運大約 20 億件行李，平均錯領率（包括遺失率）為 1%，航空公司大約得為每件錯領的行李付出一百美元的花費，透過「RFID 行李追蹤系統」的較高讀取準確率，將會大大降低人工介入處理的狀況，如此將使行李遺失所造成的商譽損失及重運錯領行李的成本也隨之減少，同時也縮短登機旅客與拖運行李的檢查比對時間，讓飛機航班得以正確時間起飛，減少旅客久候的不耐，目前這項技術所有幾十家航空公司都參與這個 RFID 項目，在各自的乘客預辦登機服務櫃台，為行李打印條碼標籤，條碼標籤上有日期時間、航班編號及目的地機場代碼。這些資料就跟標籤中的 RFID 識別號連上，存放於機場行李處理系統中。

再則受到 911 事件與泰國爆炸事件的

影響，各國為保護自身國家的國土安全，形成全球民航最大的改變——大幅強化機場內的安檢措施，其中最重要的項目之一，便是推動旅客行李確認及安全系統。目前全球航空旅運保安已導入 RFID 應用與驗證的國家，已經有美國、澳洲、法國、英國、日本、韓國、新加坡及香港等，皆積極整合 RFID 技術與相關科技，推動國內航空旅運保安機制的發展與建置。如美國聯邦航空局（Federal Aviation Administration；FAA）推動旅客與行李管制（Positive Passenger Baggage Matching；PPBM）驗證計畫，及斯維加斯（Las Vegas）的 McCarran 國際機場規劃自 2004 年 4 月起實施將 RFID 技術導入行李管理系統的五年計畫。再如由日本國土交通省 2004 年 3 月於成田機場導入 RFID 技術執行『空手旅行』（SPT/Simplifying Passenger Travel）『E-Airport』的試驗計畫，旅客透過事先預約航空公司的貨運服務，貨運在指定時間到府收取已貼上 RFID Tag 的行李，直接運送至機場，然後送上正確班機，讓旅客得以空手直接登機，並可在抵達目的機場時領取行李；過程中，旅客甚至還可透過網際網路（Internet），追蹤自己行李的動態。目前的機場 RFID 應用為：若旅客因為停留在海關或免稅商店趕不上登機時間，也可以掌控旅客的所在位置和情況，用以判斷該如何處理旅客的行李。國際民航組織規劃「電

子護照」(e-Passport)的應用已於 2010 年起世界各國均採用「電子護照」。所謂的「電子護照」(又稱「生物護照」)是在護照內植入 RFID 電子晶片，其中將儲存照片影像及個人指紋、虹膜等生物辨識資料，並透過公鑰 (public key) 加密，加強其安全性，並在持有人出入境時，讀取及辨識這些電子資料。美國聯邦國土安全部早在 2006 年 3 月在美國舊金山國際機場、新加坡樟宜機場，和澳洲雪梨機場展開一場使用生物辨識科技的電子護照測試，新加坡、澳洲與紐西蘭政府均提供協助，顯示 RFID 電子護照是全球性的應用。在台灣方面，目前外交部已在桃園機場第二航廈施行使用，國人出入境台灣時，除了需向查驗員出示持有的護照，並可對著生物辨識的攝影鏡頭做「臉部特寫」，以將辨識資訊傳入電腦系統做比對，確認護照持有人的身分真偽。除了具備防偽功能，新護照用到 RFID 技術，類似使用悠遊卡搭捷運，在通關匣門通道上「嗶」一聲，利用電磁感應方式讀取資料，將有助於旅客快速通關。此外移民署也已發展「自動通關系統」，國人可快速通關不必經查驗員，第一道匣門先確認護照是否為本人，第二道匣門再確認是否遭限制出入境，全用生物辨識確認身分，不但節省排隊等待的時間，對於國人出入境的資料管理更可做全電腦系統的管控。有關各國電子護照的應用實

各國航空站之RFID應用

- 行李追蹤、航空電子票證、身份識別、後勤支援、貨品追蹤及倉儲管理、保安管理等，如被動式行李旅客確認系統 (PPBM)、飛行前旅客資訊 (API)、及智慧型護照 (Smart Passport) 等的相關應用計畫。
- 紐華克自由國際機場採用 RFID 追蹤作業車輛
 - 美國運輸安全管理局 (TSA, Newark Liberty International Airport) 推薦採用 RFID 追蹤機場地面車輛的運行，特別是加油卡車
 - 增強機場安全度，防止恐怖主義
- 德國漢莎航空技術公司使用 RFID 技術
 - 加快了從各大洲機場飛往法蘭克福機場的航班內切換座位的過程
- RFID 技術在 McCarran 國際機場中的應用
- 以色列要求入境航班飛行員配備身份識別卡防劫機
- 歐洲機場用 RFID 技術追蹤旅客在機場內的行蹤



資料圖片來源

例與介紹，將於第肆章節詳細說明之。

(三) RFID 與智慧卡之比較

RFID 的產品，大致上可分為 RFID 標籤與 RFID IC 卡。RFID 標籤著重於識別功能，RFID IC 卡也算是智慧卡的一種，它具有記憶功能及邏輯運算能力的 IC 卡片。RFID IC 卡依照是否有 CPU，區分為記憶卡 (無 CPU) 和智慧卡 (有 CPU)，而 RFID 與智慧卡的差異主要有三點：

1. 智慧卡記憶體較 RFID 容量大

目前智慧卡可達 128KB 的儲存容量，並且同樣可以重複讀寫資料，可用來儲存交易記錄和完整識別資料。

2. 智慧卡較 RFID 安全性高

智慧卡具有 3DES、RSA 等加密演算法，並且可以驗證 PIN 碼，也可以提供電子簽章且使用壽命長。

3. RFID 成本較智慧卡低

RFID 目前的成本約在三十美分，而智慧卡大約二元美金，因此 RFID 在成本上有絕對的優勢。

二、有關二維條碼（2D Barcode）簡介

條碼（Barcode）是將資料輸入電腦的一種方式，它簡化了可減少由傳統鍵盤輸入的麻煩及商易出錯，加快資料的讀取時間，配合應用系統軟體，將資料做更有效的處理和管理。台灣目前條碼的使用已相當普及，有 90% 以上的商品有使用條碼。但因為一維條碼的資料長度只能 15 個字元，因此已經有人提出儲存量較高的二維條碼，如圖 2-6 為一維條碼以及二維條碼的圖示範例。



圖 2-6：一維條碼與二維條碼範例

資料來源：本文整理

（一）二維條碼的特性

二維條碼（2D Barcode）與一般條碼之不同，在於文字資料也可以條碼化，資料不只可應用在英文數字、漢字、記號、各字型、甚至空白也可處理。印刷方面，不只在白紙上印黑字，也可以彩色印刷，受到污損或破損也可復原。其特性整理如下：

1. 儲存量大：可存 1100 個文數字，比起一維條碼的 15 個文數字，儲存量大增，並且可儲存中文。

2. 抗損性強：在二維條碼中使用錯誤修正（Error Correction）的技術，即使條碼受損程度高達 50%，仍可正確解讀出資訊。

3. 安全性高：在二維條碼中可以加上加密的技術，可使資料的安全性大幅提昇。

4. 可傳真和影印：經傳真和影印後仍可使用，一維條碼經傳真和影印後即無法判讀。

5. 資訊隨著產品走：關於產品的資訊可完全存於二維條碼，不須額外的資料庫而傳統維條碼經解碼後得到的只是一個索引（Index），需到資料庫（Database）中找尋對應的資料。

6. 資訊隱藏：因為二維條碼無法以肉眼直接讀出，所以有資訊隱藏之功能。

根據上述整理一維條碼與二維條碼的差異，整理如表 2-3 所示。

（二）二維條碼類型

二維條碼由於上述的優點及特性，在 1990 年代初期已逐漸被廣泛使用，它不僅能夠用來儲存表單、文字資料，更可以用來儲存影像資料，將整頁表單資料濃縮存放在一個條碼內，接收者可利用專屬掃描器自動地把表單資料輸入電腦，抗損性較高，不會有病毒、消磁、損壞、容量不足

表 2-3：一維條碼與二維條碼的差異

特性	一維條碼	二維條碼
儲存量	15 個文數字；不能儲存中文。	1100 個文數字；中英文皆可。
安全性	無，光憑肉眼即可讀出一維條碼粗細線的意義。	可在編碼及解碼時加上密碼。
效益性	因資訊仍在資料庫上，影印傳真仍無法直接傳遞資訊。	可影印及傳真，節省大量影印或傳真費用。
追蹤性	即使一維條碼跟著產品走，因無資料庫隨時連線，無追蹤性可言。	資訊跟著產品走，追蹤產品的流向。
抗磨損性	無，磨損即無法判讀。	使用錯誤糾正碼的技術，可將磨損率高達 50% 的條碼正確的讀出。
讀取率	讀取錯誤率 10^{-3} （光學辨識系統）。	讀取錯誤率 10^{-9} 。
圖像資料	無法儲存超過 15 個文字或數字。	可以將照片、指紋、掌紋、簽字、聲音、文字等凡可數字化的信息進行編碼，儲存至二維條碼中。

資料來源：本文整理

等問題，且具有高密度、大容量、抗磨損等特點，所以更拓展了條碼應用領域。二維條碼可區分為堆疊式（Stacked）以及矩陣式（Matrix），各類別之特性、技術與標準皆有所不同，詳述如下。

1. 堆疊式二維條碼

堆疊式二維條碼的編碼原理是建立在一維條碼的基礎上，一維條碼的高度變窄，再依需要堆成多行，其在編碼設計、檢查原理、識讀方式等方面都成了一維條碼的特點，但由於行數增加，對行的辨別、解碼算法及軟體則與一維條碼有所不同。較具代表性的堆疊式二維條碼有

PDF417、Code16K、Supercode、Code49 等，各種類條碼說明如圖 2-7 所示。

2. 矩陣式二維條碼

矩陣式二維條碼是以矩陣的形式組

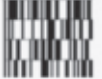
種類	說明	範例
Code 49	於1987年由Intermec Corporation公司提出，是第一個正式的二維條碼，主要是以Code 39一維條碼為基礎所發展，但缺乏錯誤糾正的機能，是一種多層次、連續型、可變長度的條碼系統，它可以表示全部128個ASCII字符，每個Code 49條碼符號由2~8層資料區組成，每層有18個垂直條線和17個空區，層與層間由一個垂直條線隔開，每層包含一個層標示符號，最後一層則包含了表示符號層數的信息。	
Code 16K	1989年由Laserlight 公司的Ted Williams提出，是一種多層次、連續型且長度可變的條碼，可以表示全ASCII字符集的128個字符及擴展ASCII字符，Code 16K通過唯一的起始符號禁止符號連續，通過字符由校驗及兩個107的校驗字符進行錯誤校驗，一個Code 16K通常有2~16層資料區，其中16層的Code 16K是可以表示77個ASCII字符或154個數字字符，是使用UPC與Code 128為基礎所發展而成，其編碼原理是建立在一維條碼基礎上，但需要連續二行或多行。	
PDF417	為目前最為人知的一個堆疊式二維條碼，於1992年由Symbol Technologies的主實君博士所發表；1993年時，由中山大學廖祥博士引進台灣推廣及研發相關軟體軟體。 一個PDF417碼包含3~90列的資料，儲存容量可達1,108位元，數字壓縮則可存放達2,729bytes，並具有錯誤糾正的機能，其錯誤復原率最高可達50%，亦可加入浮水印功能。另外，還有Micro PDF417格式，可應用在較小面積的印刷表面。	 條碼內容：彰化銀行 資訊處 資料處理科 台 北市八德路二段201號 2F

圖 2-7：各種類條碼簡易說明及圖示



資料圖片來源

成，在矩陣相應元素位置上，用點的出現表示二進制的“1”，不出現表示二進制的“0”，點的排列組合確定了矩陣碼所代表的意義。其中點可以是方點、圓點或其它形狀的點。矩陣碼是建立在電腦圖像處理技術、組合編碼原理等基礎上的圖形符號自動辨識的碼制，已較不適合用「條碼」稱之。較具代表性的矩陣式二維條碼有 Datamatrix、Maxicode、Vericode、Softstrip、Codel、Philips、Dot Code 等，各矩陣式二維條碼請參圖 2-8 及圖 2-9 所示。

(三) 二維條碼的主要應用

二維條碼具有儲存量大、保密性高、追蹤性高、抗損性強、備援性大、成本便宜等特性，而這些特性特別適用於表單、安全、證件、盤點等等。以下整理出相關應用：

種類	說明	範例
Dot Code	亦稱為 Philips Dot Code，由許多的小點所組成，其結構為 8×8 或 12×12 的四方陣，主要用於某些相對小領域中的物件標識或在印刷技術不夠精確的情形下使用。 用白色背景定標的條碼標識及決定店為次標識的標記。	
Maxi Code	1992 年由美國 UPS 公司所發明，也稱為 UPS Code；為了能快速辨識與解碼，其符號大小固定，且在中央有一個同心圓狀的公牛眼（bull-eye）可以用來定位二維條碼。 主要用途是郵包的快遞與追蹤。	
Data Matrix	DataMatrix 原名 DataCode，由美國國際資料公司（International Data Matrix, ID Matrix）於 1996 年發明。DataMatrix 二維條碼是一種矩陣式二維條碼，其發明的構思原是為了在較小的條碼標識上存入更多資料，它是一個正方形二維條碼，其大小可依儲存資料量多少而變動（最大儲存量為 2,000 bytes）。其上方與右邊界是由虛線組成；下方與左邊界則是由實線組成，這種特徵可用來判斷二維條碼的方向。 這種符號用來做小型物品或零件的標識，例如 IC 的終端標識，可以直接將其印製在物件實體上，且有錯誤糾正能力。	

圖 2-8：各矩陣式二維條碼 -1

種類	說明	範例
Aztec Code	在 1995 年由 Welch Allyn Inc 的 Andy Langacre 所提出，設計的主要目的是容易印刷及解碼。 Aztec Code 是一個方形的二維條碼，並且在條碼的正中央有著同心方形的特徵來做定位。 其大小可依儲存資料量多少而變動，最小的 Aztec Code 可儲存 6 位元的資料，最大的則可儲存 1,914 位元，使用有能自行校正其錯誤糾正能力，使解碼率達 50% 的條碼也能正確地讀出內容。	
QR Code	由 Nippondenso ID System 所發表，是一個方形的二維條碼，於左上角、右上角與正下方各有一個「回」字形的特徵來做定位二維條碼的辨識方向，可儲存大量的資料（最高可達 7,089 個數字元，或 4,296 個英文字元，亦可儲存最多 994 個用 UTF-8 格式表示的漢字），並具有錯誤糾正的機能。 右圖為個人名片用資料 QR Code，而且也能在其中加入自己的照片，只要不超過一定範圍都能解碼成功。	
GS1 DataBar 增強型	2002 年由 AIM 國際標準所發明，原名 RSS，於 2007 年更名為 DataBar，以符合其可結合二維之特性，可說是第二代的條碼系統；它是一種能以條形碼解碼，或結合二維 PDF417 或混合型條碼的第一代條碼，其高度比 GS1 條碼的小 0.6 倍，卻又能攜帶更多商品資訊的條碼，此種條碼類型可用於可變式量產品（GTIN）、更多資料，例如加諸如：厚度、合計重量、最後賣場與批發等的多資料，另外還有標準型、縮短型共七種不同類型。	
Quick Mark	由國內廠商金錫科技所開發之特殊格式，儲存量為 1,108 位元，特徵為條碼的頂部地直線條及左下方的小圈，容錯率級分 L、M、H、U 四級，且支援 Unicode。	
MagiCode (魔記)	由聯盛所研發使用，由電腦直接進行動科技引進國內推廣，特徵為條碼有四個直線，應為標準手機設計，體積小，存取資訊量卻比一般的一維條碼為多，辨識容易且迅速，平面、電子、戶外媒體都有可見對它的身影。	
Grid Matrix Code	由中國研發，經 AIM 認證為國際標準，GM 條碼是一種方形的二維條碼，其結構由正方形並帶橫線組成，將條碼可以儲存 1,143 位元的資料並提供快速解碼糾正功能。	
Microsoft Tag—HCCB (High Capacity Color BarCodes)	由微軟於微軟實驗室之工程師—Gavin Jandke 所開發，應用 CMYK 四原色及三角形排列的方式去對資料編碼，並非如 QR Code 等二維條碼的只是用黑色方格來儲存資料，但 HCCB 仍是可以允許使用在多種背景二色的條碼，優點是可以以在更少的方格中儲存更多的資料，在如條碼圖面所出現的誤差也可以減少，可廣泛用於系統未因應儲存容量增加的需求。	

圖 2-9：各矩陣式二維條碼 -2



資料圖片來源

1. 表單應用

公文表單、商業表單、進出口報單、艙單等資料之傳送交換，減少人工重複輸入表單資料，避免人為錯誤，降低人力成本。

2. 保密應用

商業情報、經濟情報、政治情報、軍事情報、私人情報等機密資料之加密及傳遞。

3. 追蹤應用

公文自動追蹤、生產線零件自動追蹤、客戶服務自動追蹤、郵購運送自動追蹤、維修記錄自動追蹤、危險物品自動追蹤、後勤補給自動追蹤、醫療體檢自動追蹤、生態研究自動追蹤等。

4. 證照應用

應用於護照、身分證、掛號證、駕照、會員證、識別證、連鎖店會員證等證照之資料登記及自動輸入，發揮使用者隨到隨讀、立即取用的資訊管理效果。

5. 盤點應用

物流中心、倉儲中心、聯勤中心之貨品及固定資產之自動盤點，發揮「立即盤點、立即決策」的效果。

6. 備援應用

電子檔表單的資料若不願或不能以磁碟、光碟等電子媒體儲存備援時，可利用二維條碼來儲存備援，攜帶方便又怕折疊，保存時間長，又可影印傳真，做更多備份。

參、RFID 應用於歐元之技術探討

本章節翻譯彙整探討的運用與計算方法，源自於 Gildas Avoine 於蘇黎世聯邦理工學院資訊安全與密碼演算實驗所發表的《PRIVACY ISSUES IN RFID BANKNOTE PROTECTION SCHEMES, RFID 在鈔票隱私問題保護建議方案》學術文章原文，

Gildas 於 2004 年提出把 RFID 加入歐元的構想，這項技術是基於光學和 RFID 所構成，主要目的在於防止偽鈔，同時可以追蹤偽鈔來源及去向。

原文文章中提到，歐洲中央銀行（簡稱歐洲央行）計畫將 RFID 導入歐元鈔票，雖然歐元鈔票已經包括物理安全特性，但歐洲央行相信加入 RFID 會使歐元提高其防偽性及安全性。除歐洲央行外，日本政府亦有計畫將 RFID 導入其 10,000 元紙幣，雖然類似這樣的計畫截至目前仍尚未現世，但相信在各國政府的努力下這樣的設計規劃將會被採用。

一、實驗系統角色說明

Gildas 將實驗系統角色區分為四個，歐洲央行（Central bank）、執法單位（Law Enforcement Agency）、商家（Merchants）、顧客（Consumers），詳述如下：

A. 歐洲央行：負責印製鈔票以及避免偽鈔，因此在鈔票上都有唯一的識別碼，並且使用電子簽章以保護秘密金鑰。

B. 執法單位：逮捕使用偽鈔使用者，因此必須要能追蹤，並且可以容易的發現偽鈔，即使是在擁擠的地方，如機場等。

C. 商家：處理大量的鈔票，必須保護顧客的隱私，並且向執法單位回報違法的鈔票。

D. 顧客：想要防護自己個人的隱私，

不被追蹤竊聽。不希望個人隱私被竊取。

二、系統概念

Gildas 設計的實驗方法主要是將資料分別存放於光學資料區 (Optical) 與電子資料區 (Electronic) 內。而光學資料區和電子資料區之間有一個關係，以致於遠端攻擊者即使知道電子資料區內的資料，少了光學資料區近距離的讀取，仍然無法解電子資料區內部資料，分述如下：

A. 光學資料區：資料可以被編譯為二維條碼，可由個人或商家讀取資料，條碼內包含有鈔票序號、面額及來源等。

B. 電子資料區：資料可透過無線傳輸來讀取，電子資料區的資料是由歐洲央行簽章和執法單位的公鑰及隨機亂數的加密。

電子資料儲存在 RFID 內，包含二個欄位，而存取時必須要有 Key 才能開啓，而 Key 是由光學資料區內的資料產生，這兩個欄位為 r 和 δ ， r 欄位的值一般為可讀取，但需要 Key 才可以寫入。 δ 欄位的值皆須要 Key 才可以讀取與寫入。 r 的值是歐洲央行簽章的鈔票序號並由執法單位的公鑰加密。如果加密後的值為固定的，則攻擊者仍可追蹤。故為了改善此弱點，由歐洲央行對鈔票序號與鈔票面額資料串聯簽章後，並由商家端的鈔票讀取器來解密。商家完成解密後，產生新的亂數後再經計算後寫入各欄位值。

三、符號說明

Sign (k,m)：以 k 為 Key，對訊息 m 簽章。

Enc (k,m,r)：以 k 為 Key，對加入 r 的訊息 m 做非對稱式加密。

$\parallel$ ：連接前後兩個字串。

PKB、SKB：歐洲央行之公私鑰。

PKL、SKL：執法單位之公私鑰。

S_i ：每一張鈔票之序號。

deni：每一張鈔票的資料，如面額等。

H (Hash)：防碰撞的雜湊函數。

Σi ：鈔票的簽章。

D_i ：存取鈔票的金鑰。

Dec (K, C)：以 K 對 C 做非對稱式解密。

r ：隨機產生之亂數。

四、系統說明

歐洲央行和執法單位分別擁有各自的公私鑰 (PKB、SKB) 和 (PKL、SKL)，其中 PKB 和 PKL 利用雜湊函數以避免公開碰撞。

(一) 鈔票製作

歐洲央行選擇唯一的識別號，並且計算簽章 $\Sigma i = \text{Sign}(\text{SKB}, S_i \parallel \text{deni})$ ，歐洲央行計算一個存取的金鑰 $D_i = h(\Sigma i)$ ，將 S_i 和 Σi 列印在鈔票上面，加密 $C_i = \text{Enc}(\text{PKL}, \Sigma i \parallel S_i, r_i)$ ，將 C_i 寫入 Cell r ，將 r_i 寫入 Cell δ ，表 3-1 整理出 RFID 以及光學資料欄位內容。

表 3-1：RFID 與 Optical 欄位內容

RFID	
Cell γ 通常可讀取， 寫入需要 Key	Cell δ 讀寫均需要 Key
$C_i = \text{Enc}(\text{PK}_L, \Sigma_i \parallel S_i, r_i)$	r_i
光學資料	
S_i	$\Sigma_i = \text{Sign}(\text{SK}_B, S_i \parallel \text{den}_i)$

資料來源：PRIVACY ISSUES IN RFID BANKNOTE PROTECTION SCHEMES

(二) 鈔票驗證

當商家（以下簡稱為 M）收到鈔票要做驗證的時候，M 將會根據下列步驟將鈔票做解密的動作。

1. M 讀取 Optical 資料 S_i 及 Σ_i ，並計算 $D_i = h(\Sigma_i)$ 。
2. M 讀取 C_i 的資料，利用 D_i 讀取 r_i 並且儲存至 Cell δ 。
3. M 確認 $C_i = \text{Enc}(\text{PK}_L, \Sigma_i \parallel S_i, r_i)$ 。
4. M 選擇一個變數 r_i ，並且將值寫入 Cell δ

M 計算 $C_i = \text{Enc}(\text{PK}_L, \Sigma_i \parallel S_i, r_i)$ ，並且將值寫入 Cell γ 。如果以上的步驟有錯誤，M 會將訊息告訴執法單位。

(三) 鈔票追蹤

若執法單位（以下簡寫執法單位代號為 L）想要確認或追蹤鈔票其做法為：

1. L 可以輕易的讀取 γ 欄位得到 C_i 。

2. 計算出明文 $\Sigma_i \parallel S_i = \text{Dec}(\text{SK}_L, C_i)$ 。

3. 確認 Σ_i 是否為有效的簽章，如果 Σ_i 是有效的簽章，L 就可以得到鈔票的識別碼 S_i 。

此學術實驗文章的最後結論，提及鈔券加入 RFID 將會提高其防偽和安全性的，然而針對鈔券使用者的隱私問題仍然無解，但期望拋磚引玉能帶動後續的研究，使鈔券加入 RFID 運用的防偽及安全性，可以在各國政府的肯定下，能有更多的貢獻。

肆、各國 RFID 電子護照介紹

電子護照，有人稱之為「RFID 護照」，也有人將其稱為「生物特徵護照」，除了傳統護照的列印資料頁 (Data Page) 之外，最大特點即是在護照本內嵌入非接觸式智慧卡晶片 (Contactless Smart-card)。

一、各國使用電子護照概況

2001 年 9 月 11 日美國本土遭受恐怖攻擊後，世界各國為了有效遏止恐怖份子在各地的破壞威脅，無不在其各個入出境海關加強安全查核的工作，然而，由於機器可判讀護照中的身分識別資料易被偽變造，使得各國海關在安檢作業上備受困擾，因此運用個人身體上所獨有的生物特徵，如指紋 (Fingerprint)、臉部 (Face)、虹膜 (Iris) 等經掃描後所轉化與分析的數據資

料來做為身分識別的標準，已是世界各國在文件安全檢查系統發展上不可或缺的標準。

國際民航組織為了使全球的通關檢查作業能達到一致的接受性與相互便利，建議世界各國均應發展新一代非接觸式內建生物辨識之 IC 晶片護照（Biometrics Passport，簡稱晶片護照），又稱電子護照（Electronic Passport, E-Passport），由於這種生物檢測係以個人獨特的生物特徵來辨識身分，因此較不易被偽冒變造，對查緝非法移民、外籍勞工及恐怖犯罪組織應極有成效，因此目前各國均加緊研發晶片護照改版工作，表 4-1 為目前已核發晶片護照國家及地區。

（一）中華民國電子護照

我國於 2008 年 12 月 29 日開始發行晶片護照，我國的晶片護照不涉及個人隱私，僅以臉部影像作為規劃方向，亦即所儲存之資料，以護照列印之持照人基本資料（如相片、中英文姓名、出生年月日等）為限，完全不涉及指紋、眼睛虹膜等敏感項目，可免除國人不必要的疑慮。中華民國電子護照由擁有嚴密安全防護設施及電腦科技化的晶片護照製作流程的中央印製廠製作，配合 ICAO(International Civil Aviation Organization，國際民航組織)的要求標準，從護照的防偽印刷開始，到護照的配頁、縫線、封皮裱合、燙金、軋切、



圖 4-1：中華民國電子護照



資料圖片來源

雷射穿孔及格式化等，均經由專人進行生產資料管控，均完全採自動控制的一貫作業模式，並有完善的安全措施，一旦印製過程中發生錯誤，機器即自動停止。以配頁線（Passport Assembly Line）為例，整條生產線上就有五十餘個偵測點，嚴密控管印製流程的精確度，而另一條將晶片個人化（Laser Personalization Line）的配置線更有六十餘個管制點，層層把關以確保品質無虞。

（二）美國電子護照

2006 年 8 月 14 日，美國國務院開始簽發生物識別護照（如圖 4-2），上面有一個 RFID 標籤，標籤內儲存了持照人的姓名、出生日期、性別、出生地點、日期、護照簽發及有效期限、護照號碼、數位照片。

核發晶片護照國家或地區 (依發行時間排列)

103.11.19 更新

國 名	國 名
1 馬來西亞 (1998.3.1) (2002 年起含指紋)	38 *義大利 (2006.10.26) (2010.1 起含指紋)
2 多明尼加 (2004.5.1)	39 列支敦士登 (2006.10.26)
3 巴基斯坦 (2004.10.25)	40 索馬利亞 (2007.1.21)
4 *比利時 (2004.11.24)	41 香港 (2007.2.5)
5 泰國 (2005.5.26)	42 埃及 (2007.2.5)
6 摩納哥 (2005.7.18)	43 汶萊 (2007.2.17)
7 *瑞典 (2005.10.3) (2012.1.1 起含指紋)	44 柬埔寨 (2007.3.6)
8 挪威 (2005.10.3)	45 馬其頓 (2007.4.2)
9 澳大利亞 (2005.10.24)	46 *愛沙尼亞 (2007.5.22)
10 *德國 (2005.11.1) (2007.11.1 起含指紋)	47 烏克蘭 (2007.6.1)
11 紐西蘭 (2005.11.4)	48 委內瑞拉 (2007.7.1)
12 直布羅陀 (2005)	49 馬爾地夫 (2007.7.26)
13 *英國 (2006.3.6)	50 奈及利亞 (2007.8.27)
14 日本 (2006.3.20)	51* 拉脫維亞 (2007.11.20) (2008.9.15 起含指紋)
15 *法國 (2006.4.12) (2009.6.16 起含指紋)	52 巴哈馬 (2007.12.5)
16 新加坡 (2006.4.29)	53 塞內加爾 (2007.12)
17 冰島 (2006.5.23)	54 摩多瓦 (2008.1.1)
18 *奧地利 (2006.6.16) (2009.3 起含指紋)	55 *斯洛伐克 (2008.1.15) (2009.6.22 起含指紋)
19 沙烏地阿拉伯 (2006.6.21)	56 南韓 (2008.3)
20 *葡萄牙 (2006.7.31)	57 卡達 (2008.4.20)
21 *丹麥 (2006.8.1) (2012.1.1 起含指紋)	58 蒙特尼格羅共和國 (2008.5)
22 美國 (2006.8.14)	59 印度 (2008.6.25)
23 *西班牙 (2006.8.14) (2009.10 起含指紋)	60 梵蒂岡市 (2008.6) (2012.12.1 起含指紋)
24 *芬蘭 (2006.8.21)	61 塞爾維亞 (2008.7.7)
25 *荷蘭 (2006.8.26) (2009.9.21 起含指紋)	62 土庫曼 (2008.7.10)
26 *希臘 (2006.8.26) (2009.6 起含指紋)	63 象牙海岸 (2008.7.30)
27 *立陶宛 (2006.8.28)	64 *馬爾它 (2008.10.8)
28 *盧森堡 (2006.8.28) (2009.6.29 起含指紋)	65 中華民國 (2008.12.29)
29 *波蘭 (2006.8.28) (2009.6.29 起含指紋)	66 *羅馬尼亞 (2009.1) (2010.1.19 起含指紋)
30 *斯洛伐尼亞(2006.8.28)(2009.6.29 起含指紋)	67 加彭 (2009.1)
31 *匈牙利 (2006.8.29) (2009.6.29 起含指紋)	68 哈薩克 (2009.1)
32 *捷克 (2006.9.1)	69 南非 (2009.4.8)
33 俄羅斯 (2006.9.1) (2013.7.1 起含指紋)	70 阿爾巴尼亞 (2009.5)
34 安道爾 (2006.9.1)	71 剛果 (2009.4)
35 瑞士 (2006.9.4) (2010.3.1 起含指紋)	72 蘇丹 (2009.5)
36 聖馬利諾 (2006.10.12)	73 菲律賓 (2009.8.11)
37 *愛爾蘭 (2006.10.16)	74 多哥 (2009.8)

P. 1/2

表 4-1：核發晶片護照國家及地區
(資料來源：監察院全球資訊網調查報告)

75	索羅門群島 (2009)	103	阿根廷 (2012.6.15) (基資頁)
76	波士尼亞赫塞哥維納 (2009.10.15)	104	亞美尼亞 (2012.7.1)
77	*克羅埃西亞 (2009.7.1)	105	亞塞拜然 (2012.7.17)
78	澳門 (2009.9.1)	106	阿富汗 (2012.10)
79	智利 (2009.12)	107	烏克蘭 (2013.1.1)
80	利比亞 (2009)	108	加拿大 (2013.7.1) (2009.1 公務護照)
81	巴西 (2010.1)	109	以色列 (2013.7)
82	迦納 (2010.1.25)	110	甘比亞 (2014.9.22)
83	塔吉克斯坦 (2010.2.1)		
84	*保加利亞 (2010.3.29)		
85	波紫那 (2010.3)		
86	土耳其 (2010.6.1)		
87	*塞浦路斯 (2010.12.13)		
88	摩洛哥 (2010)		
89	阿爾及利亞 (2010)		
90	喬治亞共和國 (2010.6)		
91	馬達加斯加 (2010)		
92	烏茲別克 (2010)		
93	印尼 (2011.1.26)		
94	伊朗 (2011.2.20) (2007.7 外交護照)		
95	茅利塔尼亞 (2011.5.6)		
96	科索沃 (2011.10.31)		
97	賴比瑞亞 (2011)		
98	莫三比克 (2011)		
99	阿拉伯聯合大公國 (2011.12.11)		
100	聖克里斯多福及尼維斯 (2012.1.5)		
101	南蘇丹 (2012.1)		
102	中國 (2012.5.15)		

備註：

1. 標註*者為歐盟會員國

2. 以上已核發晶片護照之 110 國家或地區均含臉部影像，其中黃色底色標示之 43 國家之晶片護照已採擷指紋。

表 4-1：核發晶片護照國家及地區（續）
（資料來源：監察院全球資訊網調查報告）

晶片還保留了空間來存儲一些額外的資料（如指紋、虹膜掃描記錄）。晶片數據可以由閱讀器掃描讀出，這有助於加快入境處理進程。但是因為晶片無須插入閱讀器也

可以被讀出數據，晶片數據可能被非法讀取，這引起了對隱私的擔心。類似收費公路上付費時使用的晶片，護照晶片可在接近閱讀器時被讀取。這一特性使得秘密讀取

晶片成為可能，例如政府可以藉此追蹤個人行蹤或是辨別一起罪案中的疑犯。雖然護照的封面有特別保護，封面合上時數據讀取變得很困難，而且晶片有接入控制和加密機制，但是當護照打開時這些特性都會失效，例如當護照放在旅館、銀行或者是一間網絡咖啡屋使用的時候。



資料圖片來源

圖 4-2：美國生物識別護照封面

美國國務院聲稱已於 2006 年底開始，所有新簽發的常規護照均包括這種晶片，但實際上是自 2007 年 8 月起實行的。所有簽發的非電子常規護照有效期限均至 2017 年 8 月 1 日為止。2017 年 8 月 1 日起，所有出境旅行均只承認電子護照，圖 4-3 為美國電子護照之內頁。

（三）香港特別行政區電子護照

2007 年 2 月 5 日起，香港特別行政區政府入境事務處簽發具生物特徵認證技術及符合國際民用航空組織標準的電子護



資料圖片來源

圖 4-3：美國電子護照內頁

照，封面設計與以往的護照基本相同，加入了電子晶片及 46 種防偽特徵（如圖 4-4）。本護照採用法國阿爾若公司（Arjo Systems）的防偽技術，將持有護照人的個人資料及容貌圖像等數位資料，儲存在證件封底的非接觸式晶片內。

香港特別行政區電子護照內嵌入的晶片包含兩部分資料：

1. 持照人個人資料：中英文姓名、國籍、性別、出生日期、出生地點、永久性居民身分證號碼、容貌影像。
2. 其他資料：護照號碼、簽發日期、有效日期、簽發機關。（如圖 4-5）

電子護照及電子簽證身分證已於 2007 年 2 月 5 日開始接受申請。申請手續及收費將維持不變。成人證件的處理申請時間，則由 15 個工作天縮減至 10 個工作天。未滿十一歲而並未持有香港永久性居民身



資料圖片來源

圖 4-4：香港特別行政區電子護照封面



電子護照封面

內藏資料包括：

- 持證人個人資料
 - 中英文姓名
 - 國籍
 - 性別
 - 出生日期
 - 出生地點
 - 永久性居民身份證號碼
 - 容貌影像
- 其他資料
 - 護照號碼
 - 簽發日期
 - 有效日期
 - 簽發機關

圖 4-5：香港特別行政區電子護照非接觸式晶片內所載資料簡介

分證的兒童，其申請的處理時間為十九個工作天，圖 4-6 為香港特別行政區電子護照個人資料頁。2019 年 2 月 1 日，香港入境事務處公布，今年第二季將分階段推出新一代電子特區護照，並加入最少 8 項新的防偽特徵，包括新背景設計，由原本的青馬大橋作背景圖樣，改為金紫荊廣場，突顯國旗及區旗的圖樣。另會加入浮凸防偽



圖 4-6：香港特別行政區現行電子護照個人資料頁



資料圖片來源

圖案、照片就刻蝕在透明視窗內，增加偽證的困難。至於備註頁，會載有彩色微縮字人像，以及增加全色螢光印刷個人資料頁，在紫外光燈下，可以見到維多利亞港夜景。

（四）日本電子護照

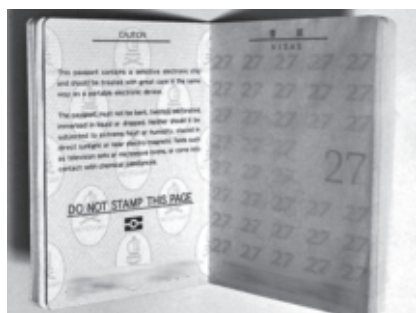
根據資料記載，日本在 2006 年 3 月 20 日開始接受電子護照（如圖 4-7）的申請，5 年有效的電子護照申請費用為 11,000 日圓，10 年有效的電子護照申請費用為 16,000 日圓；尚未更換電子護照的傳統護照仍可使用到護照有效期限終止。

日本電子護照內嵌的 RFID 標籤資料包含有持照人的姓名、國籍、出生日期、護照號碼以及個人相片，但並不包含指紋以及虹膜等相關生物特徵資料，圖 4-8 為日本電子護照內頁。



資料圖片來源

圖 4-7：日本電子護照封面



資料圖片來源

圖 4-8：日本電子護照內頁

(五) 馬來西亞電子護照

馬來西亞於 1998 年 3 月啓用晶片護照（如圖 4-9），是全世界第一個推出和使用這項技術的國家，而後國際民航組織對晶片護照標準化爲 Doc 9309 檔案「電子機讀旅行證件（eMRTD）」標準。目前世界各國簽發的晶片護照均依照此標準設計，此標準規定了生物特徵識別的標準，其中臉部辨識爲強制性要求，各國簽發部門還可選擇性對敏感資料進行加密，在此標準中包括了通訊方式、儲存格式等內容，如證件

持有人的容貌影像須以 JPEG 或 JPEG2000 格式儲存在晶片內、晶片的儲存容量至少 32 千位元組的 EEPROM，應符合 ISO/IEC 14443 通訊協定，保證與各地區的出入境口岸的護照閱讀器可與護照非接觸式互動內容，以在出入境口岸利用人臉識別、指紋和虹膜等生物特徵識別功能來驗證旅行證件持有人的身分。儲存在晶片內的生物特徵資訊帶有公開金鑰基礎建設數位簽章，以保證生物特徵資料的準確性。馬來西亞護照上的生物特徵數據包括了護照持有人面部的數碼照片，以及兩張其指紋的圖片。馬來西亞移民廳關卡是唯一具備可使用指紋掃描儀及面部識別技術讀取及驗證從 RFID 晶片讀取的數據之技術，但全球普遍採用之 ePassport 技術已有類似技術安裝在美國、英國等多個國家的國際機場。除了生物識別數據及存儲於信息頁面上的個人信息之外，該晶片還記錄了護照持有人最後十次馬來西亞邊境管制站的出、入境記錄。



資料圖片來源

圖 4-9：馬來西亞電子晶片護照封面及內頁

2010年2月2日，馬來西亞開始發行符合國際民航組織標準的e-護照。護照有效期為兩年或五年，取代現行護照，為全球第75個採用國際民航組織標準護照的國家。新護照發行的實施始於巴生谷，柔佛和彭亨之間的移民廳分行，隨後於2010年3月至5月期間擴大到全國範圍，並於2010年7月至8月期間延伸至國外使館。

（六）澳大利亞電子護照

澳大利亞外貿部自2002年起即和護照生產廠（Note Printing Australia, NAP）進行合作發展晶片護照（如圖4-10），其護照符合國際民用航空組織制定之標準，在2005年10月24日正式發行了第一本可使用的晶片護照，至同年12月5日為止已量產了116,000本的晶片護照可供發行。電子護照之晶片內儲存的資料與印製在護照上的資料相同，包含有持有人的數位照片、姓名、性別、出生日期、國籍、護照號碼以及護照的有效期限。



圖4-10：澳大利亞電子護照封面及個人資料頁

（七）德國電子護照

德國在2005年11月1日採用電子護照（如圖4-11），2007年11月1日起針對12歲含以上的發行，12歲以下如經父母要求下，也可以申請電子護照，但6歲以下孩童的護照是不包含指紋資料。一般成人申請電子護照的費用為59歐元，有效期限為10年。24歲以下的國民申請費用為37.5歐元，有效期限為六年。電子護照內的RFID標籤儲存資料包含有持有人的數位相片、姓名、出生日期、性別、國籍、護照號碼、發行國家、護照型式以及有效日期。2007年11月1日起更增加了兩個指紋資料在RFID標籤內。



圖4-11：德國電子護照封面及個人資料頁



資料圖片來源

（八）法國電子護照

法國政府在2006年4月12日啓用電子護照（如圖4-12），大約有二千個市政府在2009年6月份起即擁有免費記錄數位照片和指紋的機器，用在讀取電子護照的



圖 4-12：法國電子護照封面及個人資料頁

RFID 標籤。

據法新社報導，法國內政部發言人加歇說，根據 2004 年 12 月 13 日的歐盟協議，第一批法國生物護照應當在 2009 年 6 月 28 日之前使用。新的電子護照包含下列資料：姓名、出生年月、性別、眼睛顏色、身高、國籍、家庭住址、發放日期以及失效

日期、發放機構、護照號碼、持照人簽名和數位照片。除了簽名之外，其餘資料全部儲存在 RFID 標籤裡。

根據上述資料整理出各國電子護照使用概況，如表 4-2 所示。

二、電子護照的安全議題

由於電子護照使用 RFID 的技術，因此隱私權的保護議題勢必面臨考驗。在 RFID 晶片上的個人身分資料，是否會被不法份子蒐集與使用；若政府全面使用電子護照，那麼是否需要立法、修法限制電子護照所儲存的資料，只能在出（入）境的管理事項上使用。

依據護照條例施行細則第 2 條對於護

表 4-2：各國電子護照整理

國別	RFID 標籤內資料	發行日期
美國	姓名、出生日期、性別、出生地點、日期、護照簽發及有效期限、護照號碼、數位照片	2006.08.14
香港	中英文姓名、國籍、性別、出生日期、出生地點、永久性居民身分證號碼、容貌影像、護照號碼、簽發日期、有效日期、簽發機關	2007.02.05
日本	姓名、國籍、出生日期、護照號碼、個人相片	2006.03.20
馬來西亞	數位照片、兩個指紋、姓名、性別、出生日期、國籍、護照號碼、護照有效期限、前十次出、入境紀錄	1998.03.11
澳大利亞	數位照片、姓名、性別、出生日期、國籍、護照號碼、護照有效期限	2005.10.24
德國	數位相片、姓名、出生日期、性別、國籍、護照號碼、發行國家、護照型式、有效日期、兩個指紋	2005.11.01
法國	姓名、出生年月、性別、眼睛顏色、身高、國籍、家庭住址、發放日期、失效日期、發放機構、護照號碼、持照人簽名、數位照片	2006.04.12

照的定義：「所謂護照，指中華民國國民在國外旅行所使用之國籍身分證明文件。」護照為政府管理國民出（入）境製發之證明文件，其製作與記載之事項及方式，由相關主管機關定之（護照條例第3條、第13條與護照條例施行細則第3條）。除現行護照應記載事項外，如需額外加入個人生物特徵或者其他相關資訊，如：指紋、瞳孔、視網膜等，皆需要由主管機關加以制定（護照條例施行細則第28條第1項第13款）。

護照上的個人資料除了出（入）境的查驗外，是否會有其它蒐集與利用之可能。根據「電腦處理個人資料保護法」（以下稱個資法）第8條規定：「公務機關對個人資料之利用，應於法令職掌必要範圍內為之，並與蒐集之特定目的相符。但有左列情形之一者，得為特定目的外之利用：一、法令明文規定者；二、有正當理由而僅供內部使用者；三、為維護國家安全者；四、為增進公共利益者；五、為免除當事人之生命、身體、自由或財產上之急迫危險者；六、為防止他人權益之重大危害而有必要者；七、為學術研究而有必要且無害於當事人之重大利益者；八、有利於當事人權益者；九、當事人書面同意者。」。第1至第4項之規定過於籠統，將可能讓個人資料為政府所濫用；尤其是該條第1項僅僅規範「法令明文規定者」的情況

下，政府即可得為特定目的以外之利用。僅透過「法令」即可蒐集與利用，這樣的情況相當不利於個人資料的隱私保護，也可能違反了法律保留原則的精神。電子護照因嵌入了RFID晶片，因此可在一定距離透過讀取器讀取，往往在持照無預警的情況下所進行。如果政府機關透過讀取器在不同的場合蒐集個人資料，或是透過讀取器讀取到位置移動的隱私資訊，這樣的蒐集方式是否合理、合法，與所謂「公共安全利益」該做怎麼樣的衡量判斷，可能存在與現有憲法衝突之爭議。

根據個資法施行細則第19條第1項第4款：「政府機關為實施監督、管理、檢（調）查、取締對象之相關資料，其公開或提供將對實施目的造成困難或妨害者，得限制之或不予提供。」因此，公務機關對於電子護照所蒐集之個人資料，並不需要特定公告其資料檔案保有之依據及目的，也不需公告個人資料之類別、範圍及蒐集方法。政府沒有義務公告如何透過電子護照來蒐集個人資料，而民眾也無法得知政府對於個人資料的蒐集方式與其使用之目的。

電子護照與傳統護照最大的差別在，前者的資料是處於一種「主動發射」與「隨時可得接收」的狀態，如此個人資料可以輕易取得，但卻沒有相關公告讓人民得知，將可能造成公權力與個人隱私權間存在權利與義務上的不對等。

三、一次性密碼 (One Time Password, OTP)

隨著電腦網路的普及與廣泛運用，網路已經成為許多人不可或缺的生活工具，舉凡是金融交易、拍賣購物、線上遊戲……等。不過，伴隨著網路市場的高成長，資訊安全風險亦節節攀升，目前國內外普遍的網路犯罪行為，如：木馬程式、密碼破解、網路窺視、網路釣魚……等，這些犯罪行為不外乎就是要竊取個人機密，如：個人密碼、機密檔案等，如何避免個人密碼外洩，導致發生隱私問題就顯得格外的重要。



圖 4-13：目前 OTP 的解決方案



資料圖片來源

(一) 傳統 OTP

主要就是使用者會有一個像隨身碟大小一樣的 OTP Token，當使用者需要使用 OTP 的時候，使用者只要隨著時間的改變或按 OTP Token 上的按鈕，以產生一個 OTP 亂數來當做身分驗證的資料，如圖 4-14 為 RSA SecurID Token。



圖 4-14：RSA SecurID Token



資料圖片來源

(二) 簡訊 OTP

簡訊 OTP 運作流程就是當系統要進行使用者驗證的時候，使用者的手機會接收到一封由系統發出的簡訊，訊息內容就是一個 OTP 的驗證資料，輸入此密碼之後就可以進行驗證。簡訊 OTP 主要在於可以省掉硬體 OTP Token 的成本，取而代之的使用媒介是現代人手邊不可或缺的手機，因為現在幾乎都是人手一機，大家也都會隨

身攜帶手機，所以利用手機當做媒介，可以減少要多帶一個 OTP Token 的困擾，也降低忘記攜帶的可能性。

（三）行動裝置 OTP

所謂的行動 OTP，就是利用手機、PDA、隨身碟各式的行動裝置當作 OTP 使用者媒介，取代傳統的 OTP Token 來做 OTP 密碼資訊的產生。使用者可以根據自己手邊既有的行動裝置，選擇自己最常用的行動裝置，並將 OTP 程式安裝在行動裝置上，以便於日後做為身分驗證之用。行動裝置 OTP 使用的是離線 (Off-line) 產生驗證亂數，使用者不用擔心無法收到簡訊或簡訊被竊聽的問題，並且不需要簡訊傳送費用，可降低企業的建置成本。

經由上述的說明，整理各種身分驗證之比較如表 4-3。

伍、結論與建議

一、結論

隨著科技持續地發展，IC 智慧卡的技術不斷進步，應用的範圍也愈來愈廣泛。以台灣目前狀況來說，幾乎每個人至少都使用過兩張 IC 智慧卡，一為健保卡，一為行動電話的 SIM 卡，此外有關個人身分識別，如自然人憑證以及 IC 金融卡等，皆以智慧卡為主流，由於智慧卡內部有微處理器且具邏輯運算能力，因此安全性相當高，在身分識別的部分有相當不錯的成效，但目前智慧卡的成本相對 RFID 來的高，因此使用 RFID 技術的電子護照將可大幅降低利用智慧卡技術的電子護照成本。

筆者整理眾多資訊工程相關的論文與研究報告，若使用 RFID 的技術並結合二維

表 4-3：各種身分驗證方式比較表

	帳號 / 密碼	PKI	傳統 OTP	簡訊 OTP	行動 OTP
安全性	低	極高	高	中	高
攜帶性	高	低	低	中	中
成本考量	低	高	高	略高	中
適用情況	全部	多	多	少	多
整合性	易	難	難	中	易

資料來源：本文整理

條碼應用於護照上，可改善現行電子晶片護照修改資料之不便，日前中華民國傳統護照民眾如果要修改資料可利用加簽方式，但如果要修改持照人中文姓名、國民身分證統一編號等主要項目則需重新申請護照。使用 RFID 的電子護照，若是民眾欲修改資料時需至領務局或者領務局辦事處，修改標籤資料（中英文姓名、身分證字號、出生日期、性別）時，修改資料時持照人需先輸入個人密碼，再輸入 OTP 之後護照讀取器直接修改 RFID 標籤內部資料即可，修改資料之後將 RFID 標籤各欄位的資料重新計算後寫回 RFID 標籤內部，不需像傳統護照一般，需要重新換發護照，不僅浪費成本且浪費時間。若民眾修改資料時忘記個人密碼，則可進行修改個人密碼作業，修改個人密碼時預先按壓個人指紋，比對與二維條碼內所儲存之指紋是否相符，相符即可修改個人密碼。修改條碼資料（照片、出生地、指紋）時，僅需將更改後的資料重新轉譯為二維條碼，接著重製二維條碼，之後再將 RFID 標籤各欄位的資料重新計算後寫回 RFID 標籤內部。如此可改善傳統護照修改資料不易，不僅節省時間且節省成本。

二、建議

若依照上述設計方法，使用 RFID 的技術並結合二維條碼應用於護照上，可達到

一定的安全保護，但如果個人護照遺失，且個人密碼遭竊或者被破解，拾獲者只要易容成護照上的樣貌，就可以持該護照通過海關檢查，辦理出（入）境作業，如此將可能成為國家邊境安全風險漏洞。且對於護照防衛性，有關利用遠端 RFID 資料關聯近端二維條碼資料，對於 RFID 存取控制利用 OTP 做為寫入之 PIN，並將護照內部的資料分別利用領務局以及電子護照驗證中心做加解密運算以及簽章驗證，確保護照內部的個人隱私資料，但如何完整防範不法份子從其遠端攻擊（複製、竊聽、竄改、追蹤、偽造）以及近端攻擊（複製、竄改、偽造），在電子護照上可達成內外兼具的防護，以及維護個人安全及隱私之功效，除了軟硬體系統建置的規劃整合，單就 RFID 的技術層面來看，目前 RFID 標籤使用年限大約為 10 年左右，超過使用期限 RFID 標籤所儲存之資料將過期失效，且護照若因個人不慎保管、不當使用導致 RFID 標籤損壞，則護照內部之重要資料將可能消失，但個人之出（入）境資料是有必要永久儲存，未來研究與發展方向可將個人出（入）境資料設計儲存於電子護照驗證中心或者各國海關單位，以供日後相關法律事件查詢使用。此外有關二維條碼本身的容量限制性（1100 位元組），尚無法完整呈現目前中華民國海關要求之護照個人照片，大小為兩吋，解析度需為 300dpi，如

此照片之檔案大小約為 28,795 位元組，因此二維條碼無法放置，如果將調整解析度至 10dpi，檔案大小為 832 位元組，雖然可以放置於二維條碼鐘，但已經無法分辨照片中的人物，考量解析度的因素與狀況，照片等影像無法放置於二維條碼的解決辦法或許可使用多個二維條碼來儲存個人照片，利用二維條碼儲存照片以及領務局之簽章，避免護照上所顯示之照片被人更換的風險等，都是日後在影像解析度的呈現上，也需考量的設計方向。

參考文獻

1. 英文部分

- [1] Australian Government Department of Foreign Affairs and Trade, "The Australian ePassport," <http://www.dfat.gov.au/dept/passports/>, access on November 2018
- [2] Avoine, G., "Privacy Issues in RFID Banknote Protection Schemes," <http://lasecwww.epfl.ch/pub/lasec/doc/Avo04.pdf>, access on March 2018
- [3] Yeh, C.-T. and Chen, L.-H., "A System for a New two-dimensional Code: Secure 2D Code," *Machine Vision and Applications*, November 1998
- [4] Federal Ministry of the Interior, "The e-passport," <http://www.epass.de/>, access on

November 2018

- [5] GovHK, "Characteristics and Security Features of e-Passport," <http://www.gov.hk/en/residents/immigration/traveldoc/hksarpassport/characteristics.htm>, access on November 2018
- [6] Jules, A., "RFID Security and Privacy: A Research Survey," RSA Lab, September 2015
- [7] Juels, A. and Pappu, R., "Squealing Euros: Privacy Protection in RFID-Enabled Banknotes," RSA Laboratories Bedford, 2013
- [8] WIKIPEDIA, "European passport," http://en.wikipedia.org/wiki/European_passport, access on November 2008
- [9] WIKIPEDIA, "SecurID," <http://en.wikipedia.org/wiki/SecurID>, access on July 2018
- [10] WIKIPEDIA, "United States passport," http://en.wikipedia.org/wiki/United_States_passport, access on November 2018

2. 中文部分

- [11] 中央印製廠，「產品展示」，<http://www.cepp.gov.tw/internet/cn/pro/pro.aspx?uid=10&pid=8>，2019 年 2 月存取
- [12] 中華民國外交部領事事務局，「護照條例施行細則」，<https://www.boca.gov.tw/cp-211-4273-a354f-1.html>，2019 年 3 月存取
- [13] 中華民國外交部領事事務局，「請問補發（遺失）護照及污損換發申請說明」，<https://www.boca.gov.tw/cp-22-18-faf88-1.html>，

2019 年 3 月存取

- [14] 日本外務省日本國駐華大使館，「赴日签证（签证最新消息）」，[https://www.cn.emb-japan.go.jp/consular.htm /](https://www.cn.emb-japan.go.jp/consular.htm/)，2019 年 3 月存取（中文簡體）
- [15] 王明德，「真假之間的決斷，企業如何利用 RFID 進行防偽」，DIGITIMES 科技網，http://app.digitimes.com.tw/ShowNews.aspx?zCatId=117&zNotesDocId=0000040439_A361G5397T400908NQEWE6，2018 年 11 月存取
- [16] 外交部領事事務局，「晶片護照」，<https://www.boca.gov.tw/sp-gs-1.html?Query=%E6%99%B6%E7%89%87%E8%AD%B7%E7%85%A7/>，2019 年 3 月存取
- [17] 全景軟體，「當密碼不再是風險負擔」，<http://www.formosoft.com/sphinx/Formosoft-OTP.html>，2018 年 11 月存取
- [18] 李正明，「國內公領域推動 RFID 現況與未來發展」，<http://www.rfid.org.tw/content.php?sn=116>，2018 年 3 月存取
- [19] 金悅祖，謝和興，「提升動物 RFID 標籤辨識度之關鍵議題」，<http://www.rfid.org.tw/content.php?sn=227>，2018 年 12 月存取
- [20] 陳維美，「RFID 的應用現況」，台灣科技大學電資學院 <http://www.ccecs.ntust.edu.tw/front/bin/ptlist.phtml?Category=126>，2018 年 11 月存取
- [21] 新通國際，「法國 2009 年 6 月前開始使用電子護照」，<http://www.igo.cn/Guide/200803/633401379948208286.shtml>，2018 年 12 月存取
- [22] 楊建國，「交通行業成為目前中國 RFID 應用最成功行業」，RFID 世界網，http://news.rfidworld.com.cn/2007_10/200710261428391927.html，2018 年 12 月存取
- [23] 楊涓婷，「RFID（無線射頻識別）技術於所有權狀防偽之初探」，<http://www.tccg.gov.tw/site/3fd694a1/3fd6bc0f/40500f45/3ffe4358/3ffe755b/40ade19c/files/94.23.doc>，2019 年 3 月存取
- [24] 蘇志隆，「臺灣電子護照建置現況與未來進展」，經濟部 RFID 應用推動辦公室，<http://www.rfid.org.tw/content.php?sn=305>，2018 年 7 月存取
- [25] 騰訊科技，「RFID 賽事管理應用漸成主流」，RFID 世界網，<http://www.rfidworld.com.cn/news/2006718827574177.htm>，2018 年 12 月存取
- [26] 顧振豪，「RFID 電子式護照的應用與法律爭議」，經濟部技術處科技專案，2006 年 5 月

中央印製廠 / 劉毓容