國立台灣科技大學
資訊工程系

碩士學位論文

無線射頻辨識防偽機制研究

The Study of RFID Anti-Counterfeiting Mechanism

余敬虔
M9015909

指導教授：林彥君 博士
鄭博仁 博士

中華民國九十五年一月十七日

中文摘要

無線射頻辨識(RFID)技術結合無線射頻(RF)和 IC 晶片技術。無線射頻辨識將會在幾年之後逐漸取代條碼功能，給零售、物流業乃至全球供應鏈帶來革命性改變。無線射頻辨識有極大的應用空間以及運作彈性，但是在防偽領域的應用上才剛起步。本論文對無線射頻辨識的防偽機制做了一個全面而深入的考察與研究，以加強無線射頻辨識防偽安全服務為目的，從全面的防偽架構觀點切入，提出點（電子標籤或讀取器本身）、線（電子標籤和讀取器之間）及面（全面網路系統架構）的整體防偽機制，研究如何利用無線射頻辨識解決生活周遭的偽造及仿冒問題。首先，就「點」而論：就是強化每個 RFID 物件（無線射頻標籤或讀取器）本身的防偽能力，使仿冒者必需花很高的代價才能進行偽造，以致知難而退，達到防偽目的。其次，就「線」而論：就是加強兩個 RFID 物件之間的防偽傳輸機制，也就是加強無線射頻標籤與讀取器之間的安全傳輸機制，並做好彼此身分認證，使得偽造的標籤或讀取器難以冒充合法的 RFID 物件來介入正常的資料傳輸過程，而達到防偽的目的。再根據面的防偽需求，提出四個防偽架構，並分析其應用範疇、配套措施、系統架構及優缺點等課題。接著，應用前述這四個架構於有價證券的防偽機制上。然後，再應用這四個架構解決生活中所面臨的諸多偽造問題，藉此幫助企業思考如何利用無線射頻辨識解決週遭所面臨的問題，更幫助企業在導入相關應用時做最佳選擇。

Abstract

Radio frequency identification (RFID) technology is a combination of RF and IC chip technology. RFID technology is expected to replace the “bar code” functions and will bring revolutionary changes to the retailers, the logistics and the global supply chains. Currently, RFID has a lot of applications potential and operational flexibility. However, its application in the field of anti-counterfeiting is just beginning. This paper has made a comprehensive survey and research in the anti-counterfeiting mechanism using RFID. The goal of this paper is to enhance the anti-counterfeiting capability of the RFID technology. It takes three perspective approaches to address this problem. At the “isolated component” level, we try to enhance the anti-counterfeiting capability of each major RFID component (e.g., RFID tag and RFID reader), such that the counterfeiter has to pay a high premium to counterfeit the authentic target object. At the “component interaction” level, we introduce the authentication mechanism between the data transmission of two RFID objects, such that there is no way for any fake object to participate in the transmission process. At the “overall system” level, we propose four anti-counterfeit architecture models to enhance the overall RFID system anti-counterfeiting mechanism, and apply these four models to the banking and financial anti-counterfeiting applications. Finally, we apply these four architecture models to solve many counterfeit problems surrounding us. We hope that our research will help the enterprise to solve many of their counterfeiting problems using RFID technology, and at the same time assist them to make wise and proper decisions when they need to deploy RFID technology in their companies.

誌　謝

感謝　神美好的安排，兩位恩師：林老師彥君及鄭老師博仁在我資質、時間皆不足下，耐心教我治學、處事及解決問題的方法，不只在學問上獲益良多，並在信仰上也得著許多幫助。感謝二位口試委員：雷老師欽隆及李老師育杰在百忙之中，對我論文提出許多指導方向，由衷感謝他們。

感謝實驗室的同學：黃建中、郭至恩、蕭恩奇、游景翔、王祥安、黃志榮、郭令斌、林泰安等所給予的協助及鼓勵，謝謝你們。

感謝公司的主管、同仁們諸多協助及支持，並且不斷給予關懷和加油打氣，才能在公務繁忙之中，讓我順利完成學業和論文。

感謝先父幫助我完成答應你的最後一件事，也感謝親愛的媽媽不斷為我禱告和鼓勵，使我一直能有往前的力量。感謝愛妻藍瑜背後最大的支持；沒有妳在旁陪伴，真不知清晨的第一聲鳥叫蟲鳴竟是那麼悅耳動聽。潔心、承恩盼你們將來都比老爸更有出息，在我一半年齡就能完成學業。感謝召會諸多弟兄姊妹的代禱和扶持，並不斷幫補我這一分缺少的力量。

感謝　神那「巧匠的手」為我安排的每一個細節，使我在年近半百得到碩士學位，求您祝福過程中幫助過我的每一個人，願他們都認識您的恩典。

目次

中文摘要 II

ABSTRACT II

誌　謝 III

目次 IV

圖表目錄 VII

第 1 章 緒論 1

1.1. 研究動機 1

1.2. 文獻回顧與研究目的 2

1.3. 論文組織 5

第 2 章 無線射頻辨識與EPC系統介紹 6

2.1. 無線射頻辨識系統 6

2.1.1. 射頻電路工作原理 9

2.1.2. 讀取器工作原理 12

2.2. EPC全球網路系統 13

2.2.1. EPC全球網路的由來 13

2.2.2. EPC系統主要元件 14

2.2.3. EPC系統之運作 18

第 3 章 無線射頻辨識防偽機制的安全問題 21

3.1. 現有的防偽機制介紹 21

3.2. 無線射頻辨識標籤在防偽上的缺失 24

3.3. 提昇無線射頻辨識的防偽功能 25

3.4. 數位簽章機制理論 28

3.4.1. 橢圓曲線密碼理論 30

3.4.2. SHA-1 演算法 31

3.4.3. 橢圓曲線數位簽章演算法 32

第 4 章 無線射頻辨識防偽架構探討 34

4.1. 防偽系統架構 34

4.2. 第一型：基本型（BASIC TYPE）系統架構 34

4.3. 第二型：開放型（OPEN TYPE）系統架構 36

4.4. 第三型：封閉型（CLOSED TYPE）系統架構 38

4.5. 第四型：混合型（HYBRID TYPE）系統架構 40

4.6. 防偽架構綜合說明 42

第 5 章 有價票證的防偽機制研究 44

5.1. 有價票證的防偽需求 44

5.2. 有價票證的防偽措施 46

5.2.1. 有價票證的V1 型防偽架構 47

5.2.2. 有價票證的V2 型防偽架構 48

5.2.3. 有價票證的V3 型防偽架構 49

5.2.4. 有價票證的V4 型防偽架構 50

5.3. 有價票證的防偽分析 52

第 6 章 無線射頻辨識的防偽機制應用 54

6.1. 無線射頻辨識應用於藥品的防偽機制 54

6.2. 無線射頻辨識應用於食品防偽機制 56

6.2.1. 防止「病死豬肉」流入市面 56

6.2.2. 防止飲料中毒事件再發生 58

6.3. 無線射頻辨識應用於護照的防偽機制 59

6.4. 無線射頻辨識應用於文書的管理機制 60

6.4.1. 一般圖書及文書管理系統 60

6.4.2. 機密文書管理系統 61

6.5. 應用上所遭遇的問題 62

第 7 章 結論與未來研究方向 66

7.1. 結論 66

7.2. 未來研究方向 67

參考資料 69

圖表目錄

圖 2.1. 無線射頻辨識系統架構圖 7

圖 2.2. 讀取器之天線對電子標籤充電 9

圖 2.3. 當電子標籤側開路時，讀取器側並無感應電流 10

圖 2.4. 當電子標籤側閉路時，讀取器側便有感應電流 10

圖 2.5. 無線射頻辨識標籤將資訊傳遞至讀取器之原理圖 11

圖 2.6. 13.56 MHz讀取器動作方塊圖 12

圖 2.7. EPC 網路系統架構圖 15

圖 2.8. EPC 網路系統運作流程 18

圖 4.1. 基本型架構 35

圖 4.2. 開放型架構 37

圖 4.3. 封閉型架構 39

圖 4.4. 混合型架構 42

表 2.1. 主、被動式標籤特性 8

表 2.2. 無線射頻辨識系統工作頻率特性 8

表 2.3. EPC-96 編碼結構 15

表 2.4. EPC無線射頻辨識標籤分類 16

表 3.1. 各種防偽技術的特性比較 23

表 3.2. 四種公鑰密碼的工作條件評比 27

表 4.1. 四種防偽架構歸納表 42

表 5.1. 有價票證的發行單位及票證內容 44

表 5.2. 無線射頻辨識在票證上的應用分類 46

第 1 章 緒論

1.1. 研究動機

2003 年 11 月全球銷售額最高的量販店 Wal-Mart 提出一道強制令（Wal-Mart's mandate），要求其一百家大供應商從 2005 年 1 月起，所有輸往德州三個分銷中心的棧板及貨箱上都必需貼上符合標準的「無線射頻辨識」(Radio Frequency Identification，簡稱 RFID)標籤（tag）。無線射頻辨識乃是一種非接觸式的自動辨識技術，它透過射頻信號自動識別目標物件並獲取相關資料，辨識過程無須人工干預，且可工作於各種惡劣環境。

從 Wal-Mart 發佈了這道強制令之後，無線射頻辨識這個還不太被人瞭解的電子元件，已經悄悄地從幕後走向臺前，成為近兩年來很熱門的話題。業者預期無線射頻辨識將會在幾年之後逐漸取代條碼功能，給零售、物流業乃至全球供應鏈（supply chain）帶來革命性改變。

但是，無線射頻辨識用在防偽技術領域，卻早已先於物流、零售業一步。例如：美國食品與藥物管理局（Food and Drug Administration, 簡稱 FDA）在 2003 年就已強烈建議：藥廠應採用無線射頻辨識加上「產品電子編碼」（Electronic Product Code，簡稱 EPC）作為防止偽藥的最佳手段。也就是在每罐藥品出廠時，都賦予一個全世界獨一的編碼，然後，運用全球網路機制，將每個藥品的運送流程都詳細記錄下來，以建立一套完整的電子履歷(E-pedigree)

系統。其間只要有任何一個仿冒藥品進入運送流程，就會立即被發現。所以 FDA 已要求全美的製藥業及藥局在 2007 年將都導入該項防偽計畫，以扼止攸關人命的藥品仿冒歪風[1]。

2004 年起，世界大藥廠 Pfizer 及 Purdue Pharma 率先在仿冒最嚴重的「威而剛」及止痛藥 OxyContin 的包裝都加上無線射頻辨識標籤，並結合 EPC 機制，以防止偽造[2]。另外盛傳歐元及日元也都準備加上無線射頻辨識做防止偽造的機制之一[34]；美國也考慮在公民護照上加無線射頻辨識作為身分辨識之用[13]，可見無線射頻辨識的應用已經揭開了防偽技術史上的另一個新頁。

目前，國際防偽領域已逐漸興起一股利用微電子技術防偽的潮流，尤其是無線射頻辨識的運用，具有唯一性、獨特性、難以仿造及快速、自動及大量讀取等優勢，已經引起了各方廣泛的關注，本論文也在「無線射頻辨識之防偽機制」相關課題上加以研究。

1.2. 文獻回顧與研究目的

無線射頻辨識有極大的運用空間以及運作彈性，本論文以無線射頻辨識在防偽機制上的運用為目的，提出全面性的解決方案。在此之前，Staake 等人的論文[25]，探討無線射頻辨識應用於防偽機制上的潛力，而且為了達到防偽機制的有效運作，必需配合唯一的產品編碼及運用現有網際網路架構，將產品的運送流程建立一套完整的管理系統。但是由於無線射頻標籤本身的安全度不足，必須加上密碼學的身分鑑別機制，以防止偽造的標籤或讀取器進入正常運

作流程，造成交易或商品損失。

另外，鄭博仁等人的「無線射頻辨識技術與資訊安全應用」論文[38]，從資訊安全的角度探討無線射頻辨識的應用問題。說明無線射頻辨識具有免於接觸、自動識別的諸多優點，但是從資訊安全的應用需求，諸如：身分鑑別（authentication）、存取控制（access control）、資料保密（confidentiality）、資料完整性（integrity）、不可否認性（non-repudiation）及可獲得性（availability）等功能是不足而且有缺陷的，因此，如何提昇無線射頻辨識的隱密性和安全性等課題，文中都分別提出解決方案。

鑒於無線射頻辨識系統的特性，無線射頻辨識在資訊安全應用侷限於提供身分證明與鑑別（identification and authentication）、存取控制（access control）、防盜（anti-theft）、防偽（anti-counterfeit）等方面的安全服務。本論文於是以加強無線射頻辨識防偽安全服為目的，提出以「點」、「線」和「面」的整體觀點，研究如何利用無線射頻辨識解決生活周遭的偽造及仿冒問題。

首先，就「點」而論：就是強化每個物體（無線射頻標籤或讀取器）本身的防偽能力，使仿冒者必需花很高的代價才能進行偽造，以致知難而退，達到防偽目的。但是，無線射頻標籤本來就不是為安全而設計的，並且它的運算能力非常有限，所以安全功能是不足而有缺陷的。本論文在 3.3 節，參考論文[4, 30]所述硬體的攻擊和防護之道，並以美國國家標準與技術研究院（National Institute of Standards and Technology, NIST）的「密碼模組產品安全需求標準」FIPS-140-2

[6]為藍本，提出設計無線射頻辨識標籤及讀取器的安全考量。

其次，就「線」而論：就是加強兩個物體之間的防偽傳輸機制，也就是加強無線射頻標籤與讀取器之間的安全傳輸機制，並做好彼此身分認證，使得偽造的標籤或讀取器難以介入正常的資料傳輸過程，達到防偽的目的。目前探討加強傳輸機制的論文較多，本論文在 3.4 節將其歸納為三個研究方向，並參考論文[15, 33]，採用較安全的「橢圓曲線數位簽章演算法」做為兩者的認證方式。

最後，從「面」而論：就是建立一個無線射頻辨識系統全面的防偽機制，使任何偽造的物品，一進入這個防偽機制，就會立刻被偵測出來，達到防偽的目的。目前可行的方法是：以無線射頻辨識具有快速且自動讀取的特性，加上網際網路全球互通功能，並且為每個無線射頻辨識標籤都賦予全世界獨一無二的產品電子編碼，以建構起全球獨一的產品管理系統，使每個產品從生產、出貨到售出都自動記錄其流程，並彙集成一個完整的電子履歷（E-Pedigrees）。只要任何一項仿冒商品，雖然也仿製相同標籤編號，一旦混進配售流程，就會與正常記錄產生衝突，而被原製造廠商發現，且該仿冒商品的位置也已清楚標示出來，可立即採取適當的法律行動，解決該項仿冒問題。

目前提出無線射頻辨識的全球網路架構有日本的 Ubiquitous ID Center 及歐、美的 EPCglobal 機構。本論文以 EPCglobal 的網路機制為主，因為其參與國及主導性都比較強，將在 2.2 節詳述其架構。目前無線射頻辨識在防偽領域的應用上才剛起步，許多企業嘗試要導入這項技術時，往往不知從何起步，且

事先若無良好的規劃，可能未蒙其利反受其害。本論文在第 4 章提出四個防偽架構，並分析其應用範疇、配套措施、系統架構及優缺點等課題。接著，第 5 章再討論前述四個架構應用在有價證券上的防偽機制；然後，又以專章研究生活中所面臨的諸多困擾問題，以及如何使用無線射頻辨識及運用四個防偽架構加以解決，藉此幫助企業思考如何利用無線射頻辨識解決周遭所面臨的問題，更幫助企業在導入相關應用時做最佳選擇。

研究過程中參考最多網站為：http://lasecwww.epfl.ch/~gavoine/rfid/（Security and Privacy in RFID Systems），係由Gildas Avoine將近年來有關無線射頻辨識安全防護的論文整理於網頁上，對相關研究獲益良多。

1.3. 論文組織

第 2 章討論無線射頻辨識基本原理，並且為要建立防偽機制，而導入一個國際性的無線射頻辨識網路架構。第 3 章討論無線射頻辨識應用在防偽機制上所牽涉的安全問題，以及運用 IC 製程、微電子防偽技術和密碼機制的解決方法。第 4 章根據防偽應用上的需求，提出防偽機制的四個架構，作為企業導入該項應用的參考依據；第 5 章則將上述四個防偽架構實際應用於有價票證的防偽機制。第 6 章更將這四個架構擴大應用於解決生活週遭所面臨的防偽問題。第 7 章為結論。

第 2 章 無線射頻辨識與 EPC 系統介紹

本章 2.1 節先從基本原理介紹無線射頻辨識系統的硬體架構及其組成元件；並從電子理論，探討無線射頻標籤與讀取器之間的動作原理。2.2 節開始運用這些基本元件結合現有的網際網路系統，形成 EPC 無線射頻辨識的全球網路架構，提供無線射頻辨識用於「面」的防偽機制簡介。

2.1. 無線射頻辨識系統

一般將無線射頻辨識系統分成四個主要成份[9, 38]：

1. 電子標籤（Tag）：由耦合元件及晶片組成，每個標籤內記錄著一串特別數字或資料，用來表示電子標籤所附著的物體。
2. 天線（Antenna）：在電子標籤和讀取器之間傳遞射頻信號。
3. 讀取器（Reader）：讀取(有些可以寫入)電子標籤資訊的設備，一般設計為掌上型或固定式。
4. 資料管理系統：主要是將讀取器所得到的電子標籤訊息經過篩選及過濾後，由資料管理系統取得標籤的相關資訊，並且進行資料的處理、儲存及管理。

圖 2.1 說明讀取器經由天線發送出一定頻率的射頻信號，當電子標籤進入磁場範圍時，產生感應電流並獲得工作能量，然後利用工作能量發送出自身編

碼等資訊，再經由讀取器讀取及解碼後送至電腦主機進行相關處理。

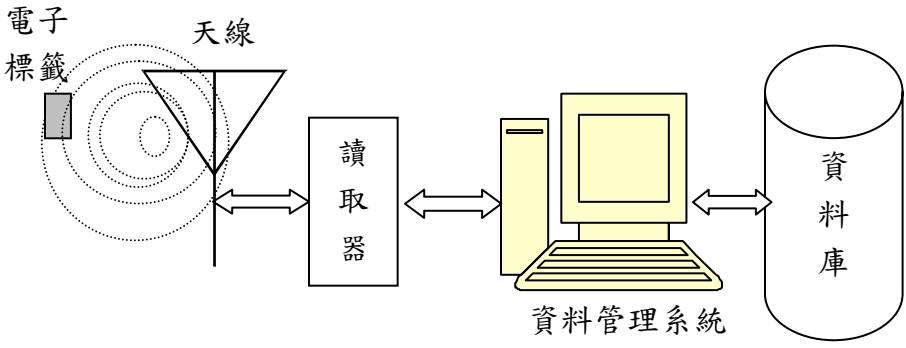


圖 2.1. 無線射頻辨識系統架構圖

電子標籤也稱為詢答器（transponder），可分為被動標籤（passive tag）和主動標籤（active tag）兩種。主動標籤自身帶有電池供電，讀/寫距離比較遠，體積也比較大，與被動標籤相比成本也比較高，另有人稱其為有源標籤。被動標籤則由天線產生的磁場中獲得工作所需的能量，成本很低並具有很長的使用壽命，比主動標籤小且輕，讀寫距離比較近，另有人稱其為無源標籤，其特性如表 2.1。

通常讀取器發送時所使用的頻率被稱為無線射頻辨識系統的工作頻率，常見的工作頻率在低頻有 125kHz、134.2kHz，高頻有 13.56MHz，超高頻的有 868~915MHz 及微波的 2.45~5.8GHz 等，其特性如表 2.2。但是，不同的國家和地區對頻率分配和最大發射功率的規定各有不同，所以，在某些地區，有些頻

段的無線射頻辨識產品可能是被禁止使用的。

表 2.1. 主、被動式標籤特性

	主動式	被動式
電源	由電池供電	由天線發送磁場取得能量
讀寫距離(公尺)	5~100	< 5
記憶體(byte)	64K~228K	64~8K
重量(g)	50~200	0.5~5
成本 (US$)	20~70	0.5~10
壽命(年)	2~7	>10

表 2.2. 無線射頻辨識系統工作頻率特性

	低頻	高頻	超高頻	微波
常用頻率	30KHz～300KHz	13.56MHz	868MHz～915MHz	2.45~5.8GHz
讀取方式	感應線圈	感應線圈	電容式電場效應	電容式電場效應
最大距離	< 0.5m	> 0.5m	>3m	>1.5m
應用範圍	1. 畜牧或寵物的管理。 2. 門禁管理、防盜系統。	1. 圖書館管理 2. 貨版追蹤 3. 大樓識別証 4. 航空行李標籤或電子機票	1. 工廠的物料清點系統 2. 卡車與拖車的追蹤	高速公路收費系統

2.1.1. 射頻電路工作原理

在無線射頻辨識系統中，射頻電路主要擔負兩大功能。1. 利用射頻訊號充電，取得工作能量；2. 利用工作能量將射頻訊號以負載調變方式進行資料收發[35]，分述如下：

- **射頻充電功能**

讀取器與電子標籤間是以交流磁場方式相互耦合。藉由此種耦合方式可以使電子標籤的天線產生感應電動勢，並經由二極體、電容做整流、濾波動作後，產生足夠讓電子標籤工作所需的電源，然後與讀取器做雙向資料的傳遞，如圖2.2 所示。由於目前 IC 設計的技術相當成熟， 因此射頻充電所需要的二極體、電容等元件皆設計在 IC 內部。電子標籤上只要保留天線(印刷電路或漆包線繞線皆可)以及一顆晶片(儲存標籤資訊及運算功能)，無需外加電源或任何的元件即可動作，因此在成本上相當的低。

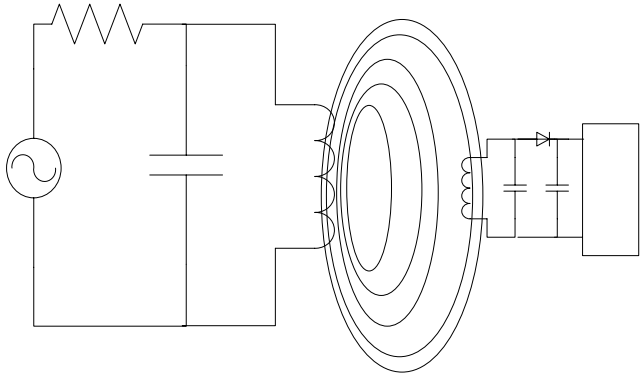


圖 2.2. 讀取器之天線對電子標籤充電

- **負載調變**

在電路行為模式上，電子標籤裝置的感應線圈與讀取器的天線可被視為一個耦合量極小的空心變壓器。假設此變壓器為理想變壓器，如圖 2.3，當開關 S1 為開路時，電子標籤側之變壓器並無電流流過，所以在讀取器側之變壓器亦無感應電流流過。當開關 S1 閉合時，如圖 2.4，電子標籤側之變壓器因串聯一電組 R1，將會造成在電子標籤側之變壓器有電流 I1(t)流過。並且在讀取器側之變壓器也會有感應電流 I2(t)流過。

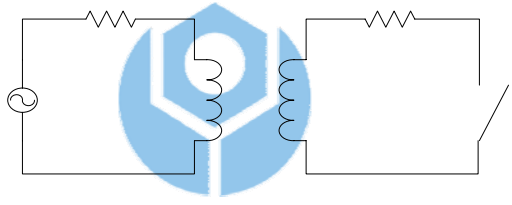


圖 2.3. 當電子標籤側開路時，讀取器側並無感應電流

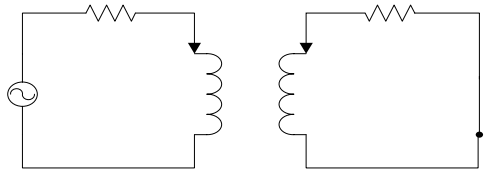


圖 2.4. 當電子標籤側閉路時，讀取器側便有感應電流

晶片會將內存的資料位元，依序操控 S1 的 ON/OFF 而傳送出去，如圖 2.5 所示。當資料為 1 時，開關為開路，當資料為 0 時，開關閉合。由於開關閉合時， I2(t)會感應 I1(t) 的電流變化，並使 R2 電阻上的電壓 V2(t)也產生變化；因此，只要在讀取器的 R2 電阻端加上訊號處理線路，便可正確還原標籤端所傳送的資料內容。

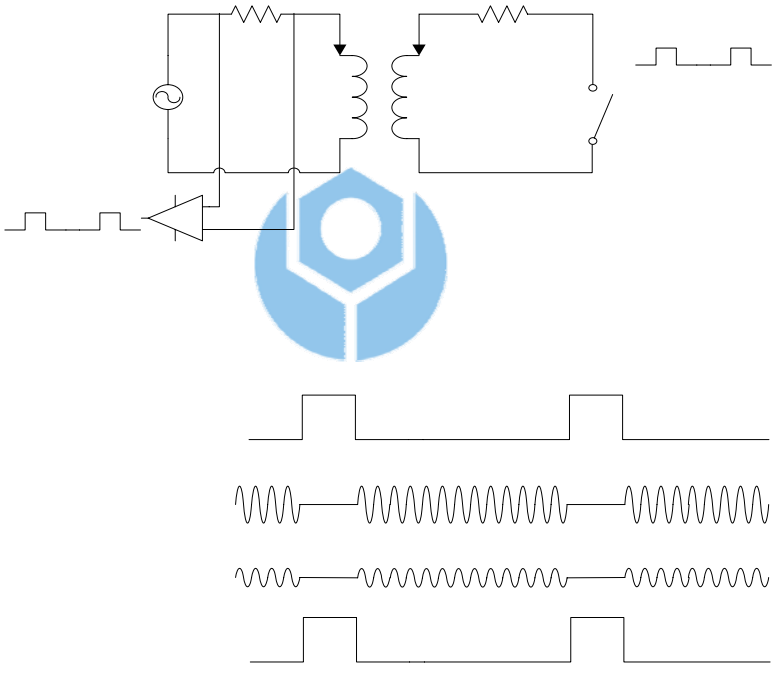


圖 2.5. 無線射頻辨識標籤將資訊傳遞至讀取器之原理圖

2.1.2. 讀取器工作原理

綜合以上原理，可知無線射頻辨識系統中，讀取器的主要功用為：

1. 提供穩定的交流訊號，讓電子標籤能感應此訊號，並充電以利晶片之動作。此交流訊號，即為系統之工作頻率，也稱為系統載波頻率。
2. 接受電子標籤所回傳的微弱資料訊息，過濾載波後，取出資料訊息，再加以放大。
3. 微處理器處理放大後的資料訊息，以判別電子標籤的資料內容。

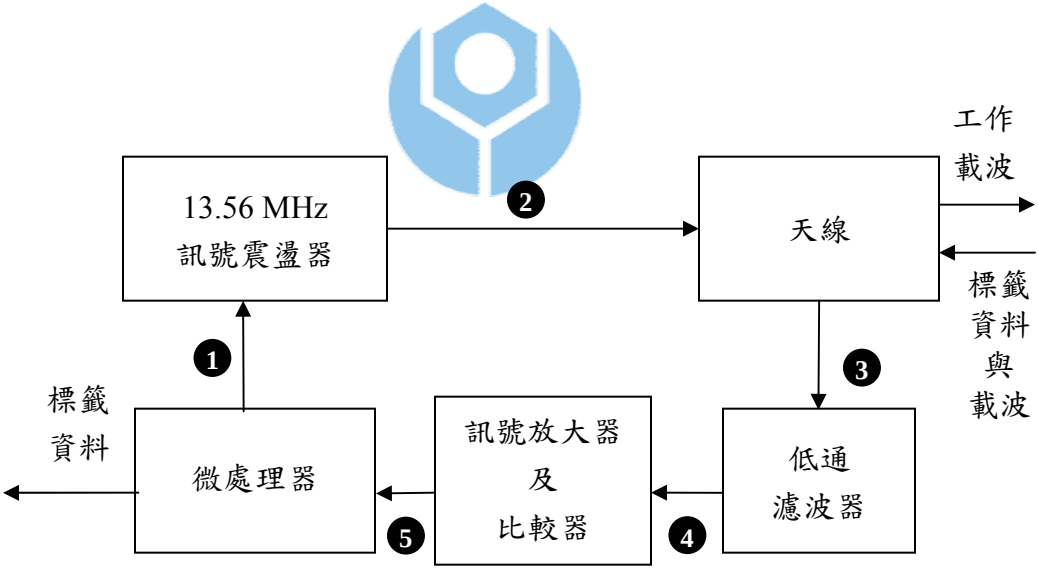


圖 2.6. 13.56 MHz 讀取器動作方塊圖

圖 2.6 以 13.56MHz 為載波系統的讀取器為例說明其動作原理：

1. 微處理器可以控制 13.56MHz 振盪器的開或關，以達到不工作時省電。
2. 13.56MHz 的交流訊號藉電晶體將訊號放大，並透過天線將訊號發射出去。
3. 電子標籤在取得能量之後，藉其晶片控制圖 2.5 的 S1 開關，將標籤資料回傳，天線就會感應到相對的訊號。
4. 由圖 2.5 可知，資料訊號 V2(t) 是重疊在載波上的，所以需先將 13.56MHz 的載波濾除，才能得到微弱的資料訊號，
5. 將資料訊號放大以供微處理器做辨識之用，然後，將辨識結果（即標籤資料）傳送給後端的處理系統。

2.2. EPC 全球網路系統

2.2.1. EPC 全球網路的由來

1999 年美國麻省理工學院（MIT）為無線射頻辨識的應用，提出了全球網路架構及為每一物品賦予唯一「產品電子碼」（Electronic Product Code, EPC）的概念後，就與世界上六所知名大學（英國劍橋大學、澳洲 Adelaide 大學、日本慶應大學、中國復旦大學、瑞士 St. Gallen 大學及韓國資訊和通訊大學等）共同成立了自動辨識技術中心（Auto-ID Center）。各大學皆有其專精領域，其中以瑞士的 St. Gallen 從事與本論文相關之防偽研究。

2003 年 10 月 31 日，又由 EAN （European Article Numbering）與 UCC（Uniform Code Council）共同創建了另一個非營利性國際組織 EPCglobal，負責管理和推廣 EPC 工作，並且與 Auto-ID Center 保持密切合作，使研究機構與使用者之間架起一座溝通的橋樑。EPCglobal 成立的目的是為了推動無線射頻辨識加上 EPC 的全球網路機制，並且訂定一套標準規範，使這個機制能在全球廣泛地應用。

有人稱 EPCglobal 的全球網路機制為「物聯網」（The Internet of things），主要是因為它準備利用現有的 Internet 網路架構，在全球建立起一個龐大的物品資訊交換平台，並且使所有參與流通的物品都具有唯一的產品電子編碼。藉由這個網路架構配合相關運作機制，將使具有 EPC 編碼的物品在網路上能夠準確的定位與追蹤（track and trace），並且為每項物品建立一套完整的電子履歷，使偽造商品（無電子履歷）不能流通。

2.2.2. EPC 系統主要元件

EPCglobal 自 2003 年起，已陸續發表其網路架構的軟硬體標準文件共九篇[3]，其中有關 EPC 網路架構規範（EPCglobal Architecture Framework Version 1.0）[28]甫於 2005 年 7 月 1 日公布，系統架構簡要如圖 2.7 所示，主要構成元件為：產品電子碼、電子標籤、讀取器、EPC 中介軟體（EPC middleware）、EPC 資訊服務（EPC Information Service，EPC-IS）、物件名稱服務（Object Name Service，ONS）、EPC 可信賴服務（EPC Trust Service）等所組成，功能說明如下：

1. **產品電子碼：**它就像條碼一樣，以一串數字代表產品製造商和產品類別，只是這每一個產品的編碼範圍必須向 EPCglobal 提出申請，以取得全世界唯一的代碼。根據「EPC 編碼標準資料格式」所定義的資料長度有：EPC-64 位元、EPC-96 位元及 EPC-128 位元等三種，目前大多數採用的是 EPC-96 規格，其編碼結構如表 2.3 所示。

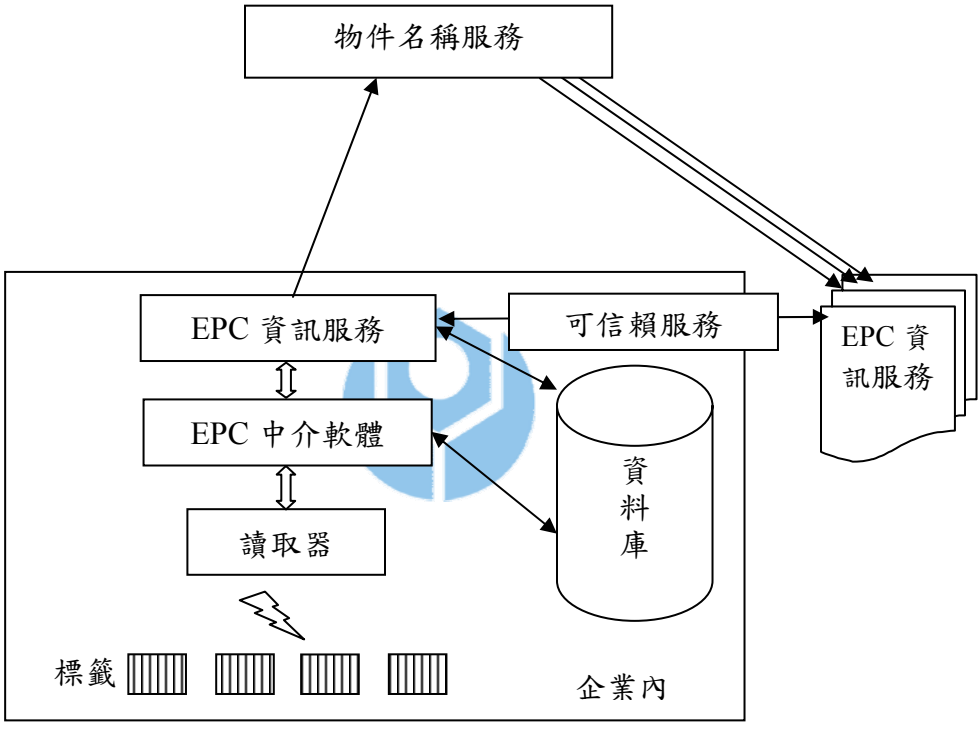


圖 2.7. EPC 網路系統架構圖

表 2.3. EPC-96 編碼結構

代碼意義	標頭	公司代碼	產品代碼	序號
位元長度	8	28	24	36

存儲在 EPC 電子標籤中的最重要資訊就是產品編碼，藉此可以與資料庫裏的大量存儲記錄相聯繫，用以建立包括產品的生產地點、製造日期、有效期限以及應該運往何地等重要資訊。

2. **電子標籤**：可以發送產品電子碼的電子標籤，其基本原理已見於 2.1 節。目前 EPC 規範將標籤歸納為六個等級，如表 2.4 所示。

表 2.4. EPC 無線射頻辨識標籤分類

Class	記憶體	電源	功能
0	無	被動	防止物品被竊
1	僅讀	被動	一般辨識功用
2	讀/寫一次	被動	可存放其他資訊
3	讀/寫	半被動	環境溫度偵測
4	讀/寫	主動	在無線網路傳遞資訊元件
5	讀/寫	主動	能與其它標籤直接傳遞資訊

3. **讀取器**：發送電磁波為電子標籤提供電源，使其能夠將儲存在微型晶片上的數據傳回，並將資料連結於管理機制，其基本原理也已見於 2.1.2 節。

4. **EPC 中介軟體（EPC middleware）**：又名為 ALE（Application Level Event），（2003 年前版本曾名為 Savant），主要功能為：

- 處理讀取器的資料讀取，和企業現有應用系統間的資料交換，並

依照設定好的商業邏輯來處理資料的讀取，以及進階的分析運用。

- 負責在讀取過程中，發現資料不吻合時，立即產生提醒功能。
- 管理讀取後的資料和 EPC 資訊服務的溝通，以及和現有企業應用系統間的溝通介面。

5. **EPC 資訊服務 （EPC Information Service, EPC-IS）**：EPC 資訊服務可說是提供 EPC 資訊的檔案櫃，主要提供合作夥伴間交換 EPC 相關資料的服務，也扮演著 EPC 網路資訊閘道的角色。因為每件商品出廠後，會經過許多轉運及儲存的過程，每一個轉運點都必需有 EPC-IS，記錄該商品的進出貨時間，運送地點等資訊，所以 EPC-IS 可比擬網際網路架構當中，提供訊息的網頁伺服器（Web server）。

6. **物件名稱服務（Object Naming Service, ONS）**：可查詢網域內某一 EPC 碼的資料存放於那些 EPC-IS 中。依照 EPCglobal 的規劃，有一個非常重要的要求，就是產品製造商必需在企業附近架設 Local ONS，以應付不時前來查詢它所生產之物品的製造日期、生產地點、保存期限等資訊。至於一般企業只需要安裝 EPC 資訊服務，以應付查詢某項物品的進、出貨時間、地點等資訊。而一般企業是藉由讀取器得到某一產品的特定電子編碼，然後，向 VeriSign 公司所管理的大型 Root ONS 查詢，找到該產品製造廠商的 Local ONS，以及具有該產品編碼的 EPC-IS，再向各 EPC-IS 讀取資料，以完成查詢作業。

7. **EPC 可信賴服務（EPC Trust Service）**：因為 EPC-IS 的資料庫包含許多廠商及產品的機密資訊，應該只能讓具有特定權限的合作夥伴才可以查詢。所以 EPCglobal 正在制訂一套安全管理規範，讓不同權限層級的使用者取得相對存取權限的資料，稱為 EPC 可信賴服務。同時，該標準架構將會規範消費者隱私、資料鑑別、資料傳輸過程的完整性等內容。

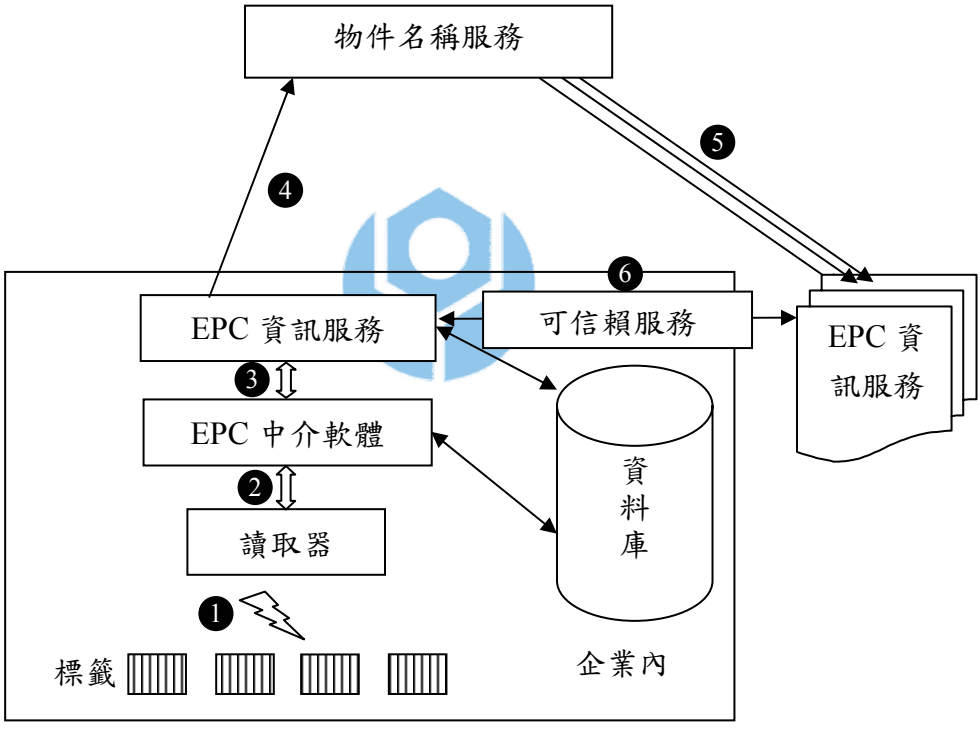


圖 2.8. EPC 網路系統運作流程

2.2.3. EPC 系統之運作

將圖 2.7 的系統架構依其工作流程重新標示於圖 2.8，以便說明整個系統的

運作流程如下：

1. 讀取器讀取電子標籤內的 EPC 碼，將編碼傳給中介軟體。
2. 經由 EPC 中介軟體（或 ALE）依據企業本身之需求，先進行資訊的初步篩選，過濾掉重複或沒有意義的資訊；再向企業內部的 EPC-IS 查詢該組 EPC 碼所代表的詳細資訊。
3. 如果是自己企業所生產的產品，或是不久前才查詢過其他企業的產品，則 EPC 資訊服務已經留有先前記錄，就會立刻以目前狀態更新先前的資料記錄。
4. 如果是其他企業製造的產品且最近未查詢過，則需要藉由全球「物件名稱服務」的基礎建設，查詢該產品之供應商為何，然後再查出該產品存放資訊的各 EPC-IS 位址（在 2.2.2 的物件名稱服務已詳述）。
5. 從存有該產品資訊的各 EPC-IS 取得完整的商品資訊。
6. 如果某些 EPC-IS 需要相互信任的安全服務，則必需經由可信賴服務建立合法使用者的讀取機制，完成資料存取功能。

從以上流程可以看出：商品的詳細資訊都是儲存在 EPC-IS 內，標籤本身僅有商品的 EPC 代碼，ONS 則是記錄並提供該組 EPC 碼可以在何處取得詳細資料的 URL 路徑，亦即 EPC-IS 的位址，只要讀取各 EPC-IS 的資訊後，就可以得到產品的完整歷史記錄。

藉由 EPC 網路架構，使用者將可以在 Internet 搜尋、分享每組 EPC 碼所代

表之唯一商品的不變資訊，例如商品的名稱、規格、製造商、製造日期、保存期限等資料。還可以查詢到商品的變動資訊，例如這個商品經過那些配送中心、經銷商、以及將運往何地等資料，這些資訊為商品提供詳細的流程記錄。但是，偽造商品即使也能複製同組 EPC 編號，卻不可能與正常商品同時進入相同流程，也就無法複製出完全相同的歷史記錄，藉此，就能提供全「面」防偽的最重要參考資料。

第 3 章 無線射頻辨識防偽機制的安全問題

本章進一步從資訊安全角度，探討無線射頻辨識防偽機制的安全問題。3.1 節先介紹現有的各種防偽機制，評比結果以採用無線射頻辨識為最佳選擇。但 3.2 節則列舉無線射頻標籤未達安全要求的一些缺失。於是，3.3 節先從「點」的角度，加強無線射頻標籤和讀取器的硬體防偽措施；接著，3.4 節再從「線」的角度，以「橢圓曲線數位簽章演算法」加強無線射頻標籤和讀取器之間的認證機制，以達到防偽目的。

3.1. 現有的防偽機制介紹

根據國際商業總會（The International Chamber of Commerce, ICC）的估計，2004 年仿冒品的總金額佔全球貿易總額的 7%，總值約 5,000 億美元。其中，仿冒名牌精品銷售的金額，每年就超過 2,000 億美元[22]。很明顯的，仿冒品對企業造成無以估計的損失，而企業及政府執法單位也越來越體認到偽造及仿冒問題的嚴重性。防止偽造問題必須從四個方面著手，即立法單位、執法單位、反仿冒政策及科技手段等。本論文只從科技手段為出發點，根據 Staake 等[25]將現有的防偽方法大略區分為：光學、生物、化工及微電子等四類科技。

- 光學科技：應用最廣泛的首推「全像術」（hologram）。就是利用全像科技在標籤、信用卡、貼紙、證件等物品上，製作很漂亮的立體影像。

過去仿製這樣的圖像需要花費很高的代價，但是現在的印刷科技已經可以很容易加以複製，而且因為大量使用，已經很少有人會去注意它的存在，所以它的防偽的效果已經非常有限。至於在鈔票上所製作的特殊反光影像，則是高難度的技術，偽造的門檻很高，至今仍被大多數國家用在有價票證的防偽手段上。

- 生物科技：最為大家所熟知的就是指紋辨識技術，更進一步還有瞳孔辨識技術。但是，這些技術都需要高成本，而且不是針對物品，所以不太適用於物品的防偽技術上。另外，尚有 DNA 防偽技術，是利用 DNA 防偽辨識棒，在 DNA 防偽標籤上來回塗抹，使標籤瞬間改變顏色，以辨識標籤的真偽。但是成本偏高且辨識過程需要人工介入，無法成為自動辨識的應用方案。
- 化工科技：最常用的是具有防偽功能的油墨，主要是利用油墨中特殊功能的色料和連結料來達到防偽的目的。在防偽印刷的領域，防偽印刷油墨的使用非常廣泛，如在各種票證、單據、商標及 標識等的防偽印刷上，都使用防偽印刷油墨。由於防偽印刷油墨具有防偽技術實施方便、成本低廉、隱蔽性較好、色彩鮮艷等特點。但是防偽油墨的技術門檻低，複製容易，很難達到防偽的功能。
- 微電子科技：目前正快速應用在防偽科技上，解決方案從簡單的辨識功能到複雜的數位驗證機制都有；製作上有看得見的也有隱藏的；一

般都具有不易磨損及自動辨識的特性。無線射頻辨識就是這類防偽領域的主要產品，目前成本高是其缺點，不過專家預期不久將會達到經濟可接受的價格。如果要將無線射頻辨識應用於防偽功能上，應該具有以下特點[9]：每個標籤都可以有一個全球唯一的編碼（例如：產品電子碼〔EPC〕）。這唯一的編碼可以在製作標籤時就放在其內的 ROM 中，既無法修改、也無機械磨損、更有防污損等特性。無線射頻辨識系統具有不需接觸（contactless）、不需直線視野（line of sight）的特性，所以可以遠距離識讀。

上述 4 項防偽技術（另加上條碼）比較後如表 3.1，如果考慮大量自動檢核的特性，則以採用電子防偽技術最好，也就是以無線射頻辨識為最佳選擇。

表 3.1. 各種防偽技術的特性比較

	可見	不可見	可觸摸	不可觸摸	破壞性	非破壞性	包裝上	產品上	大量檢核	安全性	價格
光學	○	○	○	○	○		○	○		低－中	低－中
生物	○		△	○	○	△		○		中－高	中－高
化學	○	△	△	○	○	△		○		中－高	中－高
條碼	○		△			○	○	△	△	低	低
電子	○	○	△	○		○	○	△	○	中－高	中－高

○：指完全具備該項特性　　△：指具備該項部分特性

3.2. 無線射頻辨識標籤在防偽上的缺失

雖然無線射頻辨識適合應用於大量且自動的辨識工作上，但是應用於防偽科技上，就無線射頻辨識標籤本身而言，論文[38]提出 4 項缺失，檢討它有某些特性不能符合資訊安全的應用需求，例如：

一、因為標籤的電源是靠讀取器在一定讀取時間內所提供，也就是說它只有在很短的時間內具有很小的電力可以執行運算功能。並且，標籤在被讀取時間之前，因為沒有電力，想做先行計算也是不可能的，所以要在標籤上做較複雜的密碼運算或鑑別機制，似乎是不可行的。

二、目前標籤上硬體製造能力所具有的數位邏輯閘約為 500 至 5000 個[31]，其中大部分用來做儲存和傳輸功能，剩下做安全機制的數量將非常有限，不可能會有複雜的運算能力。

三、如果用無線射頻辨識來做商品的防盜措施，對付順手牽羊的商店業餘小偷固然綽綽有餘，然而對付那些詭詐、智慧型的竊賊而言，可能一點用處都沒有。因為無線射頻辨識標籤很可能被錫箔紙加以包裹，也可能遭受非法讀取器強迫使其失效，使得竊賊偷取的商品離開現場時不至於觸動警鈴或被無線射頻辨識接受器追蹤到。

四、無線射頻辨識在防偽方面的功能仍待加強，因為複製或仿造無線射頻辨識標籤的技術門檻雖高，僅靠無線射頻辨識本身的特性仍不足夠保護應用無線射頻辨識標籤的高價值有價票證（像美金千元或五百元大

鈔)不被仿製;必須採納諸如「公開密鑰機制」(Public Key Infrastructure, PKI)等方法，並且將其建置於無線射頻辨識標籤中，才能使得歹徒複製或仿造高價證券或鈔票來獲利變得極端的困難。

3.3. 提昇無線射頻辨識的防偽功能

針對3.2節提出無線射頻辨識標籤的四項安全缺失,本論文提出:「點」、「線」及「面」的防偽功能加強機制。就「點」而論：以提昇無線射頻辨識 IC 晶片安全保護機能；增強無線射頻辨識標籤載體(例如非接觸式智慧卡)的防偽機制；及使用簡化且有效率的密碼技術來補強無線射頻辨識在防偽功能的先天限制等方法加以提昇。

提出的想法包括：採用 IC 產業對 IC 晶片製程上一般生產層級(Production Grade)的保護措施。並且，採用具有晶片層級保護機能的 IC 晶片，足以抵抗目前最常見的下列“Side Channel”攻擊方式：

- 電力分析（Power Analysis）
- 簡易電力分析 (SPA)
- 差異電力分析 (DPA)
- 時間分析（Timing Analysis）
- 錯誤歸納（Fault Induction）
- 瞬間的電磁脈衝放射標準 (TEMPEST)

至於，有關「線」的補強機制，主要為 3.2 節第一、二項密碼運算功能不

足的強化研究，歸納起來大約已有三個方向正在進行[25]：

1. **雜湊函數架構**（Hash based）：文獻[10, 20, 24, 31]都是在標籤上進行雜湊函數的計算，並且傳送加密後的資料，使非法截取者不知道真實資料為何，但合法讀取者會經由後端資料庫加以比對，取得正確的標籤資訊。但 Avion[25]也指出他們的安全漏洞。
2. **對稱式密碼架構**：Feldhofer 等人嘗試將 AES 密碼演算法放入無線射頻辨識中，但尚未達到實用階段[7]。另有一個很小的加密演算法稱為 TEA（Tiny Encryption Algorithm）[32]目前也還無法放進無線射頻辨識晶片內[31]。但是根據 Moore 的「單位矽晶片的電晶體數目每 18 個月將會增加一倍」推論[18]觀點來看，日後在晶片的製程上必定會有更精進的技術，上述方法應該都有實用價值。
3. **非對稱式密碼架構**：Juels 等人提出歐元模擬防偽機制[14]，以及 Wolkerstorfer [33]利用橢圓曲線簽章機制進行安全鑑別，都屬於非對稱式架構。另 NTRU 的演算法[11]也屬於非對稱式架構，但 Shamir 等人[12, 19, 27]指出 NTRU 的安全漏洞。

因為對稱式密碼架構會面臨金鑰保存上的困難，而且在諸多標籤同時讀取時，如何得到各標籤的正確金鑰，將會成為很大的問題。歸納起來，應該以運用非對稱式密碼加上雜湊函數的簽章驗證機制，然後在標籤和讀取器之間加上鑑別協定（authentication protocol），最適合用以防止偽造的標籤及非法的讀取

器，並且也能解決 3.2 節的第三、四項缺失。

表 3.2 比較四種非對稱密碼演算法的工作性能[15]，以採用橢圓曲線密碼演算法（Elliptic Curve Cryptography，ECC）的條件最好，因為它的公鑰長度是所有演算法中最短的，能符合標籤容量有限的需求。如果再加上簽章驗證機制，則以選用橢圓曲線數位簽章演算法（Elliptic Curve Digital Signature Algorithm，ECDSA）最為可行。Wolkerstorfer [33]也指出，橢圓曲線的密碼簽章機制運用在無線射頻辨識標籤上已經可行，只是需要儲存密鑰的資訊量仍大，目前的 EPC-96 的標籤容量尚不敷使用；還需等待 EPC-256 編碼架構普遍採用，以及晶片製程的容量大幅提昇之後，才有可能大量使用。現在只能考量較高價位商品，願意採用較高價位的特製防偽標籤為主；但是也正如 Moore 的推論，不久晶片的技術必定能夠突破上述限制，達到量產的地步。

表 3.2. 四種公鑰密碼的工作條件評比

密碼工作條件	RSA 1024	ECC 168	NTRU 263	Braid
明文長度 （bits）	1024	160	416	1088
公鑰長度 （bits）	1024	169	1841	1000
密鑰產生速度 （ms）	1432	65	19.8	8.5
加密速度 （ms）	4.28	140	1.9	29.8
解密速度 （ms）	48.5	67	3.5	14.9

（在 Pentium 500 MHz 的機器上）

3.4. 數位簽章機制理論

利用對稱密碼機制，要達到通信雙方的身分鑑別（authentication）是十分困難的；但是利用非對稱密碼機制（或稱公鑰密碼機制）卻可以輕易達成這項需求。

當通信或交易時，為了保證資訊的接收方和發送方都是正確的傳送對象，並且也能讓通信雙方都能夠知道資訊從那裡來或者到那裡去，我們就必需進行一項身分鑑別的安全認證。一般做法是：發送方除了傳送訊息外，還要利用雜湊函數（hash function）製作訊息摘要（message digest），並用自己的私鑰（private key）將訊息摘要加密後一起傳給接收方；接收方則透過公正的第三者取得發送端的公鑰（public key），並用公鑰將加密資料解密後，同時自己也用相同方法製作訊息摘要，兩者比對後，如果相同則可以確認是正確發送端所傳送的正確內容。茲以數位簽章演算法（Digital Signature Algorithm）說明之：

例如：Alice 欲將資訊 m 簽署成數位簽章 s 傳送給 Bob，讓 Bob 驗證 Alice 之數位簽章是否正確。

- 產生金鑰

  1. Alice 選擇 160 位元大小之質數 q。
  2. 選擇另一質數 p 介於 512 至 2048 位元之間，且 $q \mid p-1$。
  3. 取任一小於 p 之整數 h，並計算

$$g = h^{(p-1)/q}$$

4. 如果 $g = 1$，則繼續步驟 3

5. 取任一值 x，使得 $0 < x < q$，此為 Alice 之私鑰。

6. 計算 Alice 之公鑰 y 為

$$y = g^x \pmod{p}$$

7. Alice 將（p,q,g,y）公開之，並保留 x 為私鑰。

- 數位簽章

1. 計算 Hash 值 $h = H(m)$

2. 選任一整數 k，其中 $0 < k < q - 1$

計算

$$r = (g^k \pmod{p}) \pmod{q}$$

$$s = (h + xr)/k \pmod{q}$$

3. 將數位簽章 $s =$ （m, r, s） 傳送給 Bob

- 驗證

1. Bob 取得 Alice 之公鑰 （p,q,g,y）。

2. 計算 Hash 值 $h = H(m)$

3. 計算

$$a = h/s \quad (\bmod q)$$

$$b = r/s \quad (\bmod q)$$

$$v = (g^a y^b \pmod{p}) \pmod{q}$$

4. 如果 $v=r$，則驗證成功，否則驗證失敗。

3.4.1. 橢圓曲線密碼理論

Miller[17]和 Koblitz[16]同時提出橢圓曲線的基本理論，一般而言，密碼學中所採用的橢圓曲線主要分為兩大類：

- 定義在有限體Z_p （p為大質數）上的橢圓曲線，稱為質數橢圓曲線（Prime Curve），
- 定義在有限體F_{2^m}（m 為大整數）的橢圓曲線，稱為二元橢圓曲線（Binary Curve）。

如果要實作橢圓曲線密碼機制，根據 Fernandes 論文[8]指出：對於軟體應用程式而言，質數曲線應是最好的選擇，因為不需要二元曲線的擴充位元運算。至於對硬體應用而言，二元曲線則是最好的選擇，因為它只需要很少的邏輯閘，就可以完成強固的加解密系統，而無線射頻辨識標籤正符合這項需求，其步驟為：

1. 雙方先約定所欲計算之橢圓曲線。

$$E = E(p;a,b): y^2 \equiv x^3 + ax + b \pmod{p}$$

p 為質數

2. 計算值 g = #E（Fq）
3. 選擇在 E（Fq）上之某點 P，使得

- n = ord（P） 有大質數因數

- $h = \frac{g}{ord(P)}$ 很小

4. 曲線的參數值（E/Fq,P）為（q,l（x）,a,b,g,x（P）,y（P）,ord（P）,h）

3.4.2. SHA-1 演算法

SHA係安全雜湊演算法（Secure Hash Algorithm）的簡稱，由美國國家標準與技術協會（NIST）所開發，並於 1995 年定為 FIPS PUB 180-1，一般稱此版本為SHA-1。其設計原理與Ron Rivest提出的MD2、MD4 等雜湊函數類似。輸入的訊息長度必需小於 2^{64} 個位元，產生輸出為 160 位元的訊息摘要（digest），其簡要之演算法分為 5 個步驟：

1. 填充附加位元：在訊息之後附加一些位元，使其長度為 512 的倍數減去 64，填充的方法是添一個 1 在訊息之後，然後添加 0 直至達到要求的長度，要求至少 1 個，至多 512 個填充位元。
2. 加上長度值：完成第 1 步後，在新得到的訊息後附加上 64 位元填充前的訊息長度值；
3. 設定 MD 暫存區：SHA-1 使用 160 位元的暫存區存放這個雜湊函數的中間值，以及最後結果。
4. 處理每 512 位元的訊息區塊：進入訊息處理主迴圈，一次迴圈處理 512 位元，主迴圈有 4 回合，每回合進行 20 個動作。
5. 輸出：迴圈結束後，得到的輸出值即為所求。

給定一個資訊，可以很容易算出雜湊碼；但是反過來，如果給定一個雜湊

碼，我們應該無法找出其對應訊息，稱為雜湊函數的單向性。這個特性可以用做訊息確認的功能。

3.4.3. 橢圓曲線數位簽章演算法

將橢圓曲線實作於數位簽章機制，則為橢圓曲線數位簽章演算法（Elliptic Curve Digital Signature Algorithm，簡稱 ECDSA），已於 2000 年由 NIST 公布為 FIPS 186-2，其演算法為：

當 Alice 欲將訊息 m 數位簽章成 s 傳給 Bob，其中 m 為整數且 $0 \le m \le n$ ，則以 ECDSA 演算法密鑰對的產生成過程為：

- 產生金鑰

  1. Alice找出$g = \#E/（\mathrm{F}_q）$之大質因數n （假設$0 \le m \le n$ ）。
  2. 找出點$P_A \neq O$
  3. Alice選取一整數A，計算$P_B=[A]P_A$
  4. Alice公佈公鑰（$E/Fq,P,n,P_A,P_B$），私鑰為值A。

- 數位簽章

  1. Alice 隨機選取一整數 k 使得$1 \le k \le n$。
  2. 計算$R=[k]P_A=$ （x（R）,y（R））。
  3. 計算 $s^* = k^{-1}(h(m) + Ax(R)) \pmod n$ ，其中 x（R）為點 R 之 x 座標，h（ ）表 Hash 函數 SHA-1。
  4. 將數位簽章 $s =$ （m,R,s^*） 傳送給 Bob

- 驗證

1. Bob 收到數位簽章 $s = (m,R,s^*)$ 並取得 Alice 之公鑰 $(E/Fq,P,n,P_A,P_B)$。

2. 計算

$$v_1 = s^{*-1}\, h(m) \pmod{n}$$

$$v_2 = s^{*-1}\, x(R) \pmod{n}$$

$$P_V = [v_1]P_A + [v_2]P_B$$

3. 若 $P_V = R$ 則接受簽章，否則拒絕。

第 4 章 無線射頻辨識防偽架構探討

本章加強研究第 2 章的無線射頻辨識全球網路架構，再從「面」的角度，深入探討無線射頻辨識系統的應用層面。從 4.2 節起，本論文提出四種防偽系統架構，並分析其應用範疇、配套措施、系統架構及優缺點分析等課題。4.6 節則將前述四種防偽系統架構做綜整說明。

4.1. 防偽系統架構

EPCglobal 組織所發表的「The EPCglobal Architecture Framework 1.0」[28] 基本架構，已說明於 2.2.2 節。但是企業初導入該項應用時，仍無一些可茲遵循的應用架構，為減少摸索時間和投資上的浪費，本論文從防偽應用面的角度提出四種架構，為企業作不同應用時的參考依據，分述如下。

4.2. 第一型：基本型（Basic type）系統架構

一、適用環境

- 一個企業只需要管理自己內部的產品資料，並無必要與其他企業進行資料交換或資料查詢功能。
- 一個企業剛開始導入無線射頻辨識的應用，準備先以公司內部進行試用計畫。

二、配套措施

- 只要採購無線射頻辨識相關軟硬體設備，甚至不需要加入 EPC 組織，也無需遵循 EPC 相關技術規範。
- 但是為了長遠打算，建議仍以遵循標準所採購的設備才具有後續擴充的能力。

三、系統架構

根據圖 2.2 的 EPC 網路基本架構圖，如果採用「基本型架構」，其系統架構如圖 4.1 所示

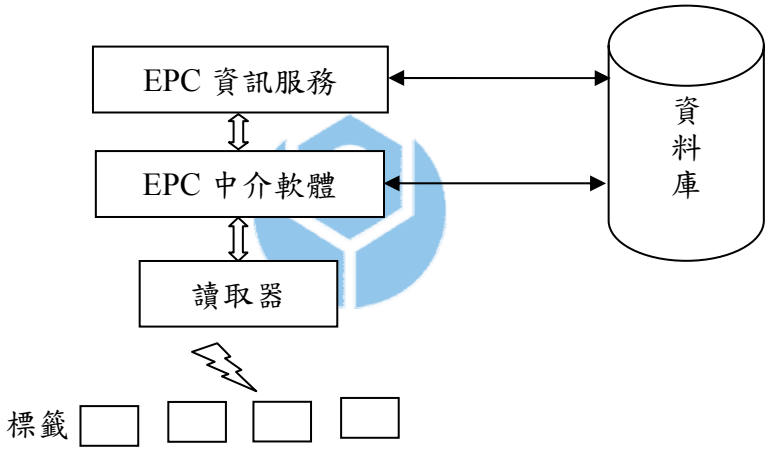


圖 4.1. 基本型架構

四、優缺點分析

本架構是各種應用架構的「基本架構」，因為所有資料都只在內部流通，易於測試及掌控，是一個企業初期導入無線射頻辨識的試用架構，配合應用程式，可以加強內部庫存管理功能，但以投資效益而

言，並無法發揮 EPC 網路的真正效益。

4.3. 第二型：開放型（Open type）系統架構

一、適用環境

- 公司的產品及進貨、銷售、庫存等狀況都可以完全公開。
- 一個企業剛導入 EPC 網路系統時，尚在試行各項軟硬體系統的運作環境，可先行採用本系統架構，待熟悉整個系統運作之後，再加強其他控管功能。

二、配套措施

- 加入 EPC 組織，取得產品的特定編碼範圍，並將產品依規定編碼。
- 遵循 EPC 組織規範採購相關無線射頻辨識軟硬體設備。

三、系統架構

根據圖 2.2 的EPC網路基本架構圖，如果採用「開放型架構」，其系統架構如圖 4.2所示

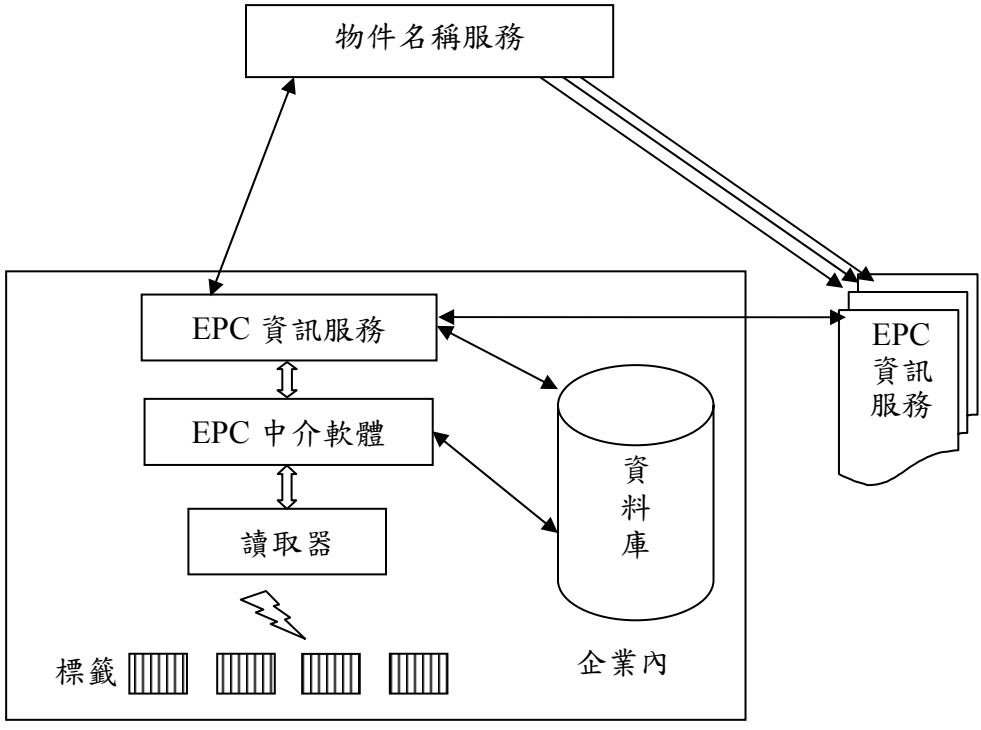


圖 4.2. 開放型架構

四、優缺點分析

本架構的資料內容完全公開，所以在 EPC-IS 間沒有架設可信賴服務，但是仍必須考量資料不能被任意修改，以維持資料的正確性及完整性。

本架構可以完全掌握 EPC 網路的運作情形，並且讓其他企業充分運用你所提供的資訊，做產品追蹤及流程式控制管的功能。但是所有資料公開，無法防止機密資料外洩，也無法防止不該取得資料的人進入系統讀取。

4.4. 第三型：封閉型（Closed type）系統架構

一、適用環境

- 公司的產品或營業具有特殊性、機密性或敏感性。例如：國防工業、飛機特殊零件等。
- 大型企業或一個專屬的應用領域，只限於這個群體之間進行資料交換。例如：輝瑞（Pfizer）製藥公司對威而剛（Viagra）產品的控管，農委會對豬肉來源的控管等。

二、配套措施

可以有兩種不同的做法：

- 加入 EPC 組織，取得產品的特定編碼範圍，並將產品依規定編碼。遵循 EPC 組織相關規格採購無線射頻辨識軟硬體設備，並加上安全控管功能，只允許組織內成員存取資料內容。
- 採用專屬網路架構，訂定自我運作的標準規範，採購或開發專屬的軟硬體設備，完全獨立運作，與其他企業或網路無法進行溝通。

三、系統架構

根據圖 2.2 的EPC網路基本架構圖，如果採用「封閉型架構」，其系統架構如圖 4.3所示。

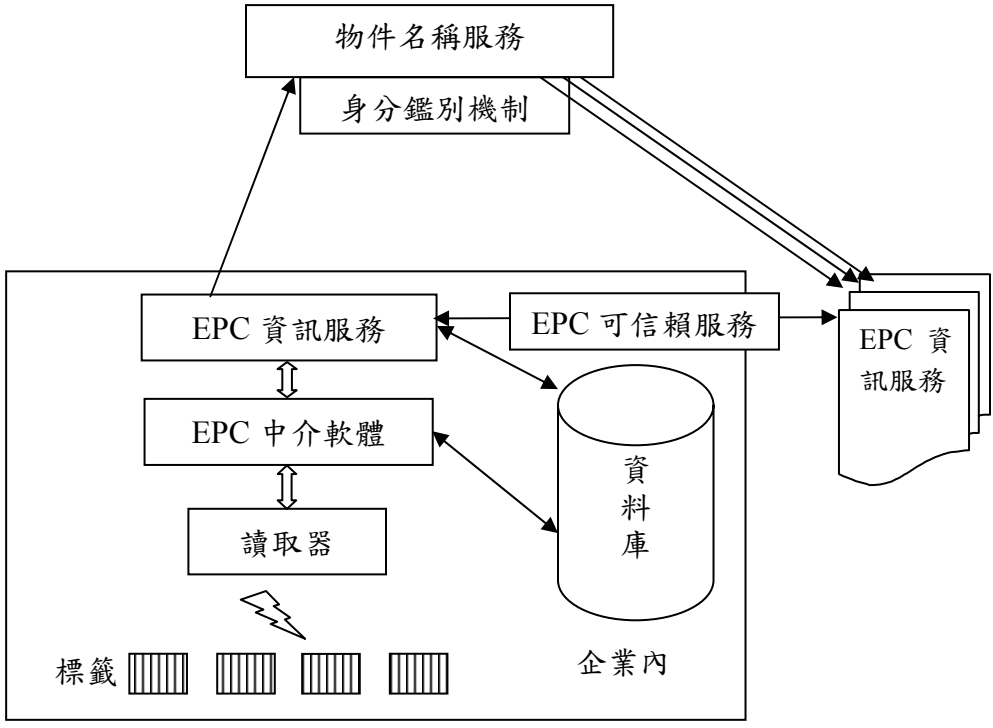


圖 4.3. 封閉型架構

本系統架構如果採用 EPC 標準規範將有三種選擇：

1. 運用 ONS 內建的身分鑑別機制，依照 EPC 規定提出申請，並限定資料存取的範圍或對象，不需增加額外配備。(中度安全)
2. 從 EPC 申請一個大範圍的產品編碼，並擁有自行的 ONS 系統。所有專屬於這系統的產品都在這範圍內編碼，且該系統內的 EPC-IS 也會指向這個專屬的 ONS 系統進行查詢及修改功能。(中高度安全)
3. 在 EPC-IS 上增加可信賴服務功能，讓所有存取本系統的對象都必須通過安全控管機制後，才能夠取得資料。安全控管機制可以

採用軟體或硬體達成。(高度安全)

四、優缺點分析

採用本系統架構可能有兩種考量：

1. 所屬產業具有私密性或安全性的顧慮，必需在安全條件完善的情況下，所有資料傳遞都只能在特定群體之間進行，而完全控管資料流程，不被非法竊取。

2. 認為所屬產品、企業或應用領域為專屬架構，不需與外界其他產業溝通，所以自行訂定封閉式架構，以簡化系統設計。其實這個觀念是錯誤的，實施後，不但不會簡化系統設計，反而可能會因為規格訂定不夠嚴謹，日後將因硬體系統之間的相容性，及軟體設計上不夠週延等問題而衍生諸多困擾，只會造成不斷增加投入的人力、物力等成本，甚至可能導致整個計畫失敗。其實，若無特殊安全需求，則採用前述之「開放型架構」即可；若有部分安全需求，則以採用下述之「混合型架構」為佳。

4.5. 第四型：混合型（Hybrid type）系統架構

一、適用環境

- 一個公司的部分產品或營業具有特殊性、機密性或敏感性。例如：公開招標之軍用物品、飛機的一般零件等。
- 一個大型企業或一個專屬的應用領域，需要交換部分機密資料(例

如公司內部資料)；還要與其他公司進行正常資料交換(例如產品的進出貨情況等)。

二、配套措施

- 加入 EPC 組織，取得產品的特定編碼範圍，並限定部分範圍內的編碼必需接受安全控管，將產品依規定編碼。
- 遵循 EPC 組織相關規格採購無線射頻辨識軟硬體設備。
- 加上適當安全控管功能，允許特定對象存取某些機敏性資料內容。

三、系統架構

根據圖 2.2 的EPC網路基本架構圖，如果採用「混合型架構」，其系統架構如圖 4.4所示

本系統架構與「封閉型架構」幾乎相同，只是存取物件名稱服務的對象沒有控管（沒有身分鑑別機制），但 EPC 資訊服務需要藉由可信賴服務進行更精細的控管，包括資料安全等級區隔，使不同權限的使用者，只能取得其允許讀取的資料，達到安全控管的功能。

四、優缺點分析

採用本系統架構應是大部分企業最終的選擇，就是允許將資料設定權限，讓存取資料的 EPC-IS 具有權限管制。因此，機敏性資料將只供特定對象存取，其餘資料則公開給其他系統存取使用。

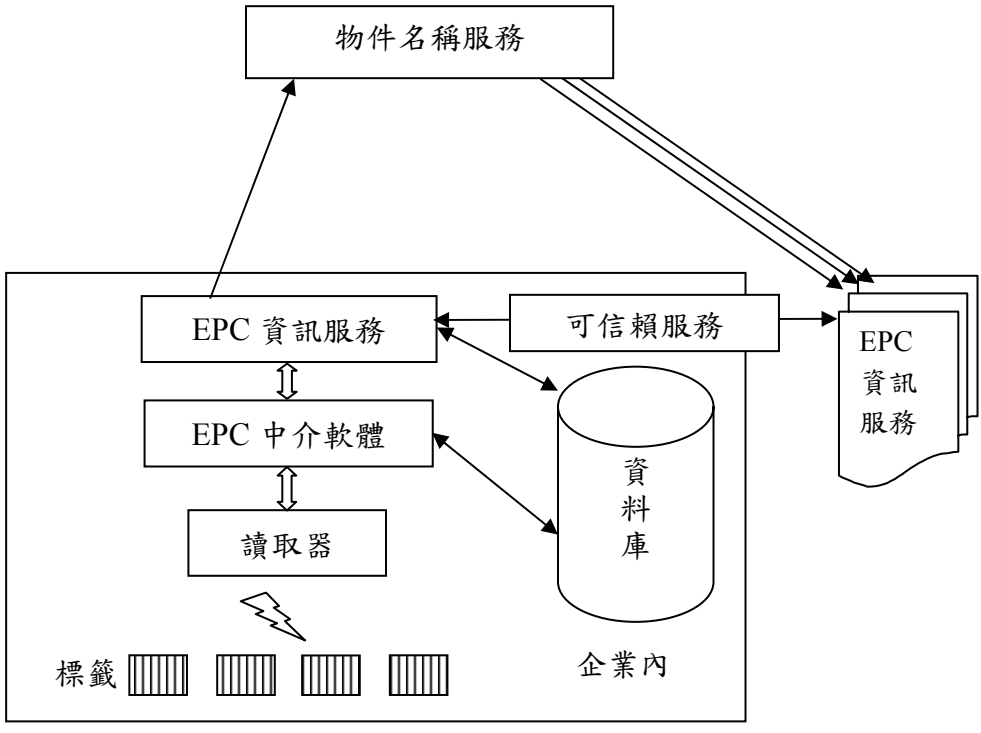


圖 4.4. 混合型架構

4.6. 防偽架構綜合說明

表 4.1. 四種防偽架構歸納表

	基本型	開放型	封閉型	混合型
應用環境	企業內部	企業之間	專屬社群	企業之間
資訊管制	無	無	完全	部分
可信賴服務	無	無	有	有
ONS 身分認證	無	無	有	無
適用於	資料只在企業內部，不與外界溝通	資訊完全公開的企業	資訊只供專屬社群間使用及流通	管制部分敏感資訊，供特定權限的使用者讀取

前述四種防偽架構綜整如表 4.1。其中基本型為最簡單的架構，可用於企業初步採納的依據。但是經過一段時間的運作之後，應該考慮昇級成開放型或混合型。如果資料完全具有機密性，則應考慮封閉型架構。

此四種架構是在無線射頻辨識防偽面的考量下，再根據企業的應用型態及資料流通特性加以分類，使企業準備採用無線射頻辨識系統時，可以衡量現有狀況，再評估其使用特性及參考架構，訂定出良好的規劃原則，而避免失敗。

第 5 章 有價票證的防偽機制研究

所謂的有價票證指在特選的紙張上印製出特種文字，圖案或紋路，而形成有價值，有面額的印刷物，此種印刷物可以通行於市面，並且能代表可交易的價值，合法的擁有權及正式官方承認的資格等稱之[36]。

因為是具有某種價值的票證，就會面臨到偽造的問題，本章先將票證以使用特性歸類後，運用第 4 章所提出的四種無線射頻辨識防偽架構，分別解決在實務上所遭遇的問題，並說明運用無線射頻辨識後，對使用者所帶來的好處。

5.1. 有價票證的防偽需求

有價票證的發行單位及其發行內容整理如表 5.1。

表 5.1. 有價票證的發行單位及票證內容

發行單位	票證內容
金融業	鈔票、支票、股票、銀行存、提款單、存摺等
政府	債券、發票、福利彩券、證書、證件等
郵政	郵票、匯票、印花、明信片等。
其他	門票憑證、車、船、機票、禮券、購物票證、企業證券等。

既然這些票證是有價，就會有人想利用不法手段來達到自己的慾望，市面上也就會出現複製、仿造及偽造等問題；尤其是目前各種新式的彩色影印機、雷射印表機、電子掃描分色機、電腦繪圖機等，都可以將偽造品達到以假亂真的地步。而這些偽造品輕則造成個人損失，重則擾亂社會金融秩序，不能不加防範。

茲列舉兩例說明如下：

- 2005 年 8 月 28 日晚在中國北京的首都體育館，歌手王菲舉辦了大型演唱會，但是在驗票口竟然發現了上百張的偽造門票。北京啟明演出公司經理盧利明說：(中國)國內演出市場從 2000 年開始就已經出現零星的假票現象，到了 2002 年的時候假票已經很普遍了，而現在全國可以說稍微有影響的商業演出幾乎沒有不被假票困擾的。

  為了防範假票，我們對門票採取了很多防偽措施。比如演唱會的門票我們就使用了嚴格的七重防偽技術，各種印刷高科技幾乎都用上了。

  但是，假票陰影並沒有因此而消失。王菲演唱會前，儘管演出公司在媒體上廣泛宣傳門票的防偽以及敬告消費者到指定地點買票，但還是有為數眾多的假票流入市場，在演出開始前引起了一陣不小的風波。

- 歐元目前已經成為世界流通的主要貨幣，銀行業者擔心歐元的跨國界使用，並且它會被歐盟以外的國家採用為預備金，將引發偽鈔製造者與洗錢客的覬覦；尤其 200 與 500 歐元預期比 100 歐元更容易成為偽鈔製造者的

目標。Electronic Engineering Times 報導指出，有內部消息人士表示，歐洲中央銀行（European Central Bank）正在向半導體製造商尋求提議方案，準備在歐元鈔票內嵌無線射頻辨識晶片來防止偽造。

5.2. 有價票證的防偽措施

因為有價票證常是偽造的最大目標之一，所以無線射頻辨識成為打擊偽造或仿製的矚目焦點，不過，最大的問題就是無線射頻辨識現有的安全功能既不足夠而且有缺陷，因為它本來就不是設計來提供安全標準的「身分辨識」，所以無法仰仗它現有的特性來達到「辨識真偽鈔券」的目的，必需借助適當的防偽機制，再加上管理系統才能達到防偽功能；於是，本論文歸納有價票證的使用特性，結合第 4 章所提出的四個防偽架構，並以安全需求的高低，整理成表 5.2。

表 5.2. 無線射頻辨識在票證上的應用分類

無線射頻辨識應用	票證使用方式			
	一次使用	回收重用	多次使用	
分類編號	V1	V2	V3	V4
標籤種類	被動式	被動式	主、被動式	被動式
資料寫入方式	一次寫入	多次寫入	多次寫入	一次寫入
應用範圍	門票、單程車、船票、彩券、禮券等。	門票、單程車、船票等。	長期車、船票、聯名卡等。	鈔票、股票、債券、支票、會員卡等。
標籤成本	低	中	高	中
安全需求	低	低	中	高
資料管理方式	集中	集中	分散	集中
防偽架構（本論文第 4 章定義）	基本型或開放型	基本型或開放型	混合型	封閉型

表 5.2 所定義的「資料管理方式」係指票證的資料必需集中或分散（各自單獨）管理，如果由一個或多個主系統共同管理一個資料庫，則稱為「集中式管理」；如果資料庫各自獨立管理，只分享其中部分相關資料，則稱為「分散式管理」。另外，表中所列出的「管理架構」係根據本論文第四章所提出的四種防偽架構，實際應用於有價票證的防偽需求，分別說明如下。

5.2.1. 有價票證的 V1 型防偽架構

根據表 5.2，如果有價票證只使用一次，且票證的安全需求低，又採用集中式管理方式，歸類為 V1 型。防偽系統可以採用本論文第四章的「基本型」或「開放型」系統架構，亦即採用無安全管制且資料庫集中管理的系統架構。以下將以售票及入場管理系統為例，說明管理架構的正常運作流程。

1. 每張門票由無線射頻辨識晶片賦予唯一之識別碼，當一張門票預訂或售出時，售票系統會自動將其識別碼記錄於資料管理系統內。如果，採用網路預購方式，訂票者需輸入個人詳細資訊，所以，票證會與個人資料產生關聯。如果採用現場購票，則購票者日後可能帶有一種電子名片，內含使用者姓名、電話及地址等資料，可迅速將門票與持票者資訊一併記入管理系統，便於後續各項服務。
2. 因為售票系統與停車系統連線，如果觀眾已先購票，可憑預購門票或電子名片進入停車場，於是停車資訊就與門票產生關聯，便於後續提供免費停車及出場指示停車位置等服務。另外，如果尚未購票，則停

車票亦是門票，只要停車後，憑停車票在售票口補辦購票程序，並加購車內其他乘客的門票，則全車乘客都能於出場時迅速找到停車位置，不致迷失。

3. 入場時，觀眾持票經過驗票口，讀取器會讀入門票的識別碼，並與資料管理系統比對，以確認此門票的正確性。

4. 若門票比對正確，則經由主控電腦將入口閘道開啟，並在各主要路口皆設有讀取器及顯示器，一路指示座位方向，以便於在大型會場中迅速入座，且不致迷路。如果比對不正確，則發出警告聲，由警衛加以處理，將可完全控管偽票事件。

5. 節目進行中，如果離座而無法找到原座位時，可藉由主要路口之讀取器協助指引回座。

6. 若需尋人服務，只需告知姓名或電話號碼，則可藉由先前預購之個人資料或電子名片讀入的資訊，迅速找到某人座位。另外，如果是在一大型遊樂場或動物園，則遊客是流動的，需藉由設立在各處之讀取器，回報每一持票者的目前位置，以迅速找到親人或朋友。

所以，將無線射頻辨識應用於有價票證上，不但可以防止偽票事件，而且還可為持票者提供多元化的貼心服務，以滿足每位持票者的不同需求。

5.2.2. 有價票證的 V2 型防偽架構

根據表 5.2，V2 型只是 V1 型的改良，主要是因為防偽票證的成本仍高，

所以在出場時，將票證回收重新賦予另外編號，則是表 5.2 的回收重用架構。但是進一步考量，票證可能必需記錄舊有編號，或有任何機制保留舊有序號，以備財稅單位做交易記錄稽查。

5.2.3. 有價票證的 V3 型防偽架構

根據表 5.2，如果有價票證必須多次使用，票證是由許多不同的單位各自控管（例如：悠遊卡），但彼此之間又需對票面價值做共同認定，且票證具有部分安全需求，歸類為 V3 型。防偽系統可以採用「混合型」系統架構，亦即部分資料可以彼此分享，而部分資料又必須納入安全管制，且資料庫採分散管理的系統架構。以下將以台灣捷運公司的「悠遊卡」管理系統為例，說明系統正常運作的流程。

1. 購買捷運悠遊卡時，在卡片內的記憶體寫入該卡的基本資料，目前為無記名的「普通卡」與「學生/軍警卡」，未來計劃發行記名的敬老卡、愛心卡、陪伴卡、普通卡，和無記名的敬老卡、兒童卡和愛心卡等。
2. 適用範圍—台北市大眾捷運、台北市(縣)聯營公車、捷運接駁公車及台北市公有路外停車場。
3. 當卡片接近讀取器有效範圍內（約十公尺），讀取器會與卡片進行確認、溝通及讀取資料工作，然後根據乘客進出站的記錄進行里程金額計算，作扣款及改寫晶片內容，並且開啟閘門；如有錯誤則發出警告聲，請站務人員處理等。

4. 持卡人可至指定機器或商店進行加值處理，則加值機會重寫晶片餘額，並作加值記錄。

5. 各交通系統皆獨立控管，資料是由卡片上所記錄的餘額、卡片種類及使用記錄等內容加以管理，所以雖然分散，但各讀取器會將卡上內容傳給各別的控制電腦，並將最新內容寫回卡上，以達到有效控管的功能。

5.2.4. 有價票證的 V4 型防偽架構

根據表 5.2，如果有價票證必須多次使用，且票證的安全需求高，又採用集中式管理方式，歸類為 V4 型。所管理的票證大多應屬於高價值或高流通性的金融商品，例如：美鈔、歐元等世界性流通的貨幣，都是歹徒最想偽造的目標，因此，防偽系統就應該採用「封閉型」系統架構，亦即採用具有安全管理且完全自主獨立的管理系統。而且，本系統只是其中防偽功能之一，還需採用多項特殊物理防偽技術，例如：特殊紙張、凸起觸感、水印、金屬油墨、變色油墨、安全線及光影變化箔膜等特殊設計，使一般民眾可用肉眼或簡單儀器加以辨識，但是偽造難度高，也使仿冒者難以得逞，

至於，有價票證加上無線射頻辨識標籤後，還需將銀行或金融機構的原有驗鈔機加裝讀取無線射頻辨識的功能，將可以快速又大量的鑑別鈔票真偽。以下考量一個簡單的鈔票防偽系統架構，讓所有資料都只在金融體系間流通且只有合法的使用者才能讀取。：

1. 將原有點鈔機加上無線射頻辨識讀取功能，暫名為「讀取驗鈔機」，先讀取在點鈔機上的所有鈔票號碼，並且與點鈔機數過的鈔票張數比對，若數量不符，則應有部分鈔票不具有無線射頻標籤，就初步研判可能是偽鈔，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，亦研判屬於偽鈔。
3. 將讀出鈔票號碼以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，亦研判屬於偽鈔。

另外，就技術觀點，針對鈔票的序號、讀取驗鈔機及無線射頻標籤等技術，鄭博仁等提出一些防偽的簡單描述如下[38]：

1. 無線射頻標籤需薄如紙張，以便於嵌入鈔票內。
2. 在鈔票印製過程，嚴格控管所有標籤流向，使歹徒不能複製或取得相似標籤。
3. 產生一把中央銀行總裁專門在鈔票做簽章用的私鑰（private key）。
4. 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。
5. 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。
6. 把製成的無線射頻辨識標籤在製鈔過程中嵌入鈔票內。
7. 設計並建置內含央行總裁公鑰以及具備無線射頻辨識接受器功能的特製「讀取驗鈔機」。

8. 根據 FIPS-140-2 [6]的「密碼模組安全需求」設計「讀取驗鈔機」，以防止複製或經由逆向工程而加以破解。

9. 在無線射頻辨識標籤和驗鈔機裡設計一套簡單而適當的「交互鑑別（mutual authentication）」通訊規約，讓無線射頻辨識標籤辨識對方如果是台合法授權的驗鈔機的話，就讓它讀取標籤內的鈔票的簽章，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為真鈔。

5.3. 有價票證的防偽分析

一般在有價票證的外觀及材質上具有一定的防偽功能，可幫助持鈔者以肉眼或便宜的工具加以辨識真偽，至於，加上無線射頻辨識機制則可以在大型商家或投幣式的檢驗機（kiosk）下立即辨別真偽，對於偽造品多了一道把關機制。

有價票證的紙張、印製及發行作業也必須有效管理，才能與防偽機制相互配合，以達到防堵不法集團偽造的目的，管理辦法大約描述如下：

1. 印刷訂製必須委託具有安全管理的專業企業。

2. 對設計票證圖案時應選用複雜圖案（顏色漸變、微縮文字、浮雕效果，手工圖紋加密等）及由原來規則的圖形向隨機圖形變化以防止仿製。

3. □應選用特殊規格訂製的安全防偽紙（浮水印紙，圖案可按需要訂製）或幹式複寫紙。□原材料上應充分體現其物理性（燙金、凹凸表面處理）、化學性（無色墨、螢光墨、光致變、涉透、溫變、磁性墨等）。

4. 時限性（壽命性）：任何防偽都有一個時限性，絕對不能一成不變，以免被仿製。

5. 易於識別性：任何有價票證雖然在製作上採取了較嚴密的防偽措施，但更需要的是應讓使用者容易識別。

6. 建立起嚴密的保防觀念：所有過程均應像處理鈔票一樣謹慎小心，以防患於未然。

至於鈔票加上無線射頻標籤的管理機制雖然仍嫌簡陋而不夠完善，但是由於無線射頻標籤技術上的不易複製[5]，再加上非法的「讀取驗鈔機」無法讀取無線射頻辨識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，使得它們經由「逆向工程（reverse engineering）」或其他類似方法都無法仿製的話，大抵上使用無線射頻辨識標籤的鈔票雖然還沒有辦法做到使偽鈔集團完全歇業的地步，但至少要他們花費相當多的工夫、付出相當大的代價才會得逞。

另外，悠遊卡不只可以應用於交通領域，目前已擴大至校園，將來更可擴大至大樓保全、公共電話、門票、便利商店、速食店、自動販賣機、訂票系統，甚至與信用卡結合等應用範圍。商家應可結合多種單次型有價票證成為「多用途無線射頻卡」，使消費者達到「一卡在手，處處遊走」的便利性；不過必需加上適當安全機制，使卡片擁有者的隱私保護、權利保障以及掛失處理等問題得以解決。

第 6 章 無線射頻辨識的防偽機制應用

本章進一步將第 4 章的四種防偽機制實際應用於解決生活週遭的防偽問題，從 6.1 至 6.4 節分別利用無線射頻辨識及相對防偽架構，以達到藥品、食品、護照及文書等防偽需求。6.5 節則探討無線射頻辨識於應用上所遭遇的問題。

6.1. 無線射頻辨識應用於藥品的防偽機制

- **案例分析：**

FDA 的報告中指出，從上世紀 90 年代後期到 2004 年，有關假藥的調查案例幾乎以平均每年 20%的速度增長，從早先 5 例上升到了 2004 年的 58 例，儘管這不是很大的數字，但是這 58 個案例已經導致了廠家損失超過 3 億美金。

對於製藥廠商來說，無論他們對於藥品本身的防偽技術做得多好，一旦藥品進入供應鏈，他們就對藥品失去了追蹤的能力。在供應鏈內，中盤商是假藥最可能進入的門戶，因為他們被約束的限制最少。於是，很多藥廠訂定了強制性的合約，要求批發商必須直接從廠商購買一些最可能被假冒的藥品。但是，這些強制性的合約只是影響了藥品流通的方式和時間，卻沒有辦法讓零售藥房保證他們銷售的藥品不是假藥。更重要的是，市場上的假藥並未因此有減少的跡象。

- **防偽架構運用：「混合型架構」或「封閉型架構」**

對於一般藥局或藥商可採用「混合型架構」以保護部分處方用藥的隱私資訊（例如威而剛藥品）。對於管制藥品的製造商，其製造、運銷、配售過程則應採用「封閉型架構」，使所有資訊受到保護。

在 FDA 2004 年 2 月發佈的另一份報告[23]就指出藥品防偽的迫切需要以及解決方案，它期望在藥廠與銷售管道之間建立一個藥品的完整歷史記錄，以徹底解決藥品仿冒問題。在報告中明確指出：「無線射頻辨識的技術將是目前最有可能進行這大範圍的產品序列化的管理方案」。

這個電子履歷系統必須結合 EPC 機制，將每一種藥品（甚至小到一個藥瓶）都貼上一個唯一的產品電子碼。這個代碼將伴隨它直到生命結束，包括從何時生產，何時被運到批發商，何時被運到零售商，以及何時被售出都可以被系統透過無線射頻辨識讀取器在貨物經過時（即使是裝在紙箱裏），被自動識別並自動記錄下來。

當藥品被賣出時，商家可以用讀取器把這個產品在系統裏標記為生命結束 EOL（end of life）同時使這個標籤失去作用。當這個產品被遺失或者偷走，系統也可標記它為遺失的狀態。或者當這個產品超過了使用期限時，它也會標記為過期狀態。因此這個藥品無論何時重新又出現在市場上，系統都都會把它識別出來並且自動給買主預警。不僅如此，這樣的系統，還可以幫助製藥廠找出問題藥品出現的時間、地點和模式，使這些有問題藥

品尚未流入消費者之前，就已經迅速地找到假冒藥品源頭。

除了可追蹤性以外，無線射頻辨識標籤本身的資料儲存能力也是藥品防偽的關鍵之一。與傳統的條碼區區幾個位元相比，無線射頻辨識 可以記錄多則數千位元的資料，藥品製造商有足夠的儲存空間把藥品的防偽的各項資料儲存在裏面，包括：藥品的名字、何時出廠、在那裏生產、何時過期等等，甚至廠家可以把每個標籤代碼都透過自己的加密方式產生不同的代碼，記錄在裏面用來驗證使用[26]，因此運用無線射頻辨識科技加上 EPC 的產品電子履歷，應該可以徹底杜絕藥品仿冒及過期等問題所造成的人體傷害。

6.2. 無線射頻辨識應用於食品防偽機制

有問題的食品與有問題的藥品一樣會對人體造成傷害，而他們防偽的手段也非常類似，茲以兩個案例提出解決食品防偽機制的運用。

6.2.1. 防止「病死豬肉」流入市面

- **案例分析：**

2005 年 6 月 11 日正值端午佳節吃棕子的同時，新聞報導說：「市面上又出現病死豬肉混進棕子出售的嚴重問題」。雖然這個問題不是仿冒所造成的，但是仍然能夠利用防止偽藥的手段來解決病死豬肉流入市面的問題。

- **防偽架構運用：「開放型架構」或「混合型架構」。**

對於一般養豬戶採用「開放型架構」最為簡便，因為豬隻的資料並無保密必要。但是農委會等政府機構則需將管理資料做適當保護，建議應採用「混合型架構」。

目前，農委會已著手試辦豬隻產銷履歷制度，但是由於豬隻未強迫植入晶片，所以，遇到有問題的豬肉，還是無法得知個別豬隻的罹病或用藥狀況。而且農委會準備用條碼機制解決豬隻履歷的問題，以及不考慮使用無線射頻辨識晶片植入豬隻計畫等，都無法徹底執行產銷履歷制度。

針對上述問題，提出解決構想如下：

1. 強制每一隻豬都植入晶片，讓牠具有獨一編號，然後從生產、注射、餵食到屠宰、分切、包裝等過程，都可以用電腦控管記錄，
2. 讓同一包裝內的豬肉，全是從同一隻豬身上產出，並且加上無線射頻辨識標籤的包裝。
3. 這項植入晶片工作應推廣至各項栽種及畜養之動植物身上，利用電腦化建立各種農、畜產品的生產履歷，不但為自己建立品質保證，更可以加上許多自動化控管作業，不但增加產量，也節省人力及物力開銷。
4. 在市場或超商廣設無線射頻辨識便利查詢機（kiosk），讓消費者買到產品後，可立即查詢該項產品的生產履歷，就能杜絕各種可能危害人體健康的食品流入市面。

建立產銷履歷制度，不僅能解決病死豬肉流入市面的問題，更為了因

應 WTO（World Trade Organization）制度下，肉類及農產品外銷都需要提供完整的履歷資料，以爭取更高品質及更安全的產銷管道。

6.2.2. 防止飲料中毒事件再發生

- **案例分析：**
  - 2005 年 5 月 17 日發生震驚社會的「毒飲料」事件，歹徒為向保力達公司勒索金錢，竟然在保利達的蠻牛飲料中，利用氰化物下毒，造成五人中毒，一人喪生的慘劇。
  - 2002 年台灣於 WTO 的壓力下，調高米酒價錢，造成假米酒充斥市面，多人因為飲用假酒而喪生。
  - 世界知名品牌的煙酒不斷遭到仿冒，而這些仿冒品又往往造成生命及健康受損。
- **防偽架構運用：「開放型架構」或「混合型架構」。**

一般零售商店可採用「開放型架構」，配合已有的倉儲及進銷存管理系統，使無線射頻辨識的優點完全利用。藥局則應採用「混合型架構」使部分處方藥品的資訊受到適當保護。

另針對上述問題，提出解決構想如下：

1. 在這些飲料商品的瓶蓋上植入無線射頻辨識一次開封後即被破壞（temper proof）的標籤，可防止「毒飲料」事件再發生，也防止真酒瓶填充假酒等事件危害人體。

2. 如同藥品的 EPC 機制，也為每瓶飲料建立「電子履歷」，提供產品編號、製造日期及運送過程等歷史記錄，所有未經正常管道放上貨架的物品，立即會被發現，就可以排除類似千面人下毒、假酒等事件發生。

3. 出售高單價產品（例如：高級洋酒）時，利用 EPC 機制取得產品的記錄，列印產品的「清白身分證明」卡，也就如同銀樓為金飾開出保單一般，不但為產品提出品質保證，也增加饋送禮品的價質感。

4. 使用者可利用各處的便利查詢機或是網際網路查詢該產品的產銷履歷，將可以杜絕各種仿冒、偽造或下毒的事情發生。

6.3. 無線射頻辨識應用於護照的防偽機制

- **案例分析：**

美國政府自從 2001 年 911 恐怖攻擊事件之後，著手研究可以整合臉部辨識等生物辨識技術的「電子護照」（E-passports），誓言要嚴格做好邊境控管，這項技術如果一切順利，預計所有的護照都會有特殊的無線射頻辨識功能。這種擁有特殊無線射頻辨識功能的電子護照，預期能夠偵查出護照竊盜與偽造，預防不法份子盜取美國護照，保護美國本土安全等功能。

- **防偽架構運用：「封閉型架構」。**

「電子護照」（E-passports）又名為「智慧護照」（smart passports），除了可以加速機場及邊境出入境檢查之外，這種護照封面嵌入無線射頻辨識的設計，可以在幾吋內，將資料即時傳送給移民局。經由移民局特殊設備

掃瞄之後，方便讓移民局官員比對護照上以及持照者實際攜帶的資料。只要不一致，就會出現偽造的訊號，可望能夠偵查出護照竊盜與偽造。

不過，由於電子護照無線射頻辨識可儲存臉部辨識的資料，且最後可能還會整合指紋及虹膜掃瞄等隱私資訊。這種晶片可以在有爭議的範圍內，穿透衣服及皮包，讓護照的持有者可能遭到監視、竊取資料等問題。這些安全疑慮讓許多自由團體都向美國政府請願，希望強化隱私的保護。

護照的安全機制與有價票證的防偽構想類似，只是它還可以配合生物辨識功能，以強化整個驗證機制的準確性。至於隱私保護，文獻[13]提出電子護照內整合數位簽章，以及加密技術，對護照的機敏性資料提供保護功能，目前各國政府在全面推展電子護照之前，都必須先解決這個重要問題。

6.4. 無線射頻辨識應用於文書的管理機制

6.4.1. 一般圖書及文書管理系統

- **案例分析：**

無線射頻辨識應用於圖書館系統已逐漸成熟，就以臺北市東門國小圖書館為例，過去借書必須寫填單或是刷條碼，利用無線射頻辨識技術後，大幅降低圖書借閱的管理時間、人力成本，原來費時 30 天的封館盤點，只要 30 分鐘的無線掃讀即可解決。師生僅需花 3 秒鐘 3 個步驟即可完成借、

還書，一改過去逐本讀取書籍條碼或手動操作模式，節省許多人力和時間。

- **防偽架構運用：「基本型架構」或「開放型架構」。**

如果圖書或文書管理不需對外連線則採用「基本型架構」，如果需要進行館際交流書籍，則採「開放型架構」即可，因為書籍管理是為增加借閱方便性，並無安全控管之必要性。

無線射頻辨識自動館藏管理系統的運用方式為：讀者於借書、還書處理皆利用無線射頻辨識。讀者藉由自助借書機，將書本中的無線射頻辨識自動註記為借閱狀態；而於還書時，只需將書放入還書箱即完成還書作業，馬上可以再借書。

此外，櫃台工作站亦可同時處理借還書作業，還可以處理其他較複雜的工作，如續借罰款等作業。而就館藏盤點部份，只需在書架上橫移即可讀取所有館藏，非常有效地節省盤點時間。

所以，圖書及文書管理系統運用無線射頻辨識技術可達到：以無線射頻辨識晶片取代條碼磁條、讀者自助借書及還書、圖書及錄影帶皆可同樣處理、電磁波防盜偵測、快速盤點作業、尋找錯置圖書等特性。

6.4.2. 機密文書管理系統

- **案例分析：**

機密文書的保管確實是政府或企業面臨的一個大問題，往往花費大量人力、物力仍達不到良好的效果，無線射頻辨識應用於機密文書的管理，將

可以提供一個解決之道，

- **防偽架構運用：「基本型架構」或「封閉型架構」。**

機關內的文書、檔案如果沒有與其他單位交換的必要，則採用「基本型架構」最佳。如果資料必需與其他單位交換，則以採用高安全度的「封閉型架構」為宜。

運用現有的圖書管理機制，再加上下列安全控管機制，應該能夠達到更好的安全管理作業：

1. 複印管制：在複印機內部加上無線射頻辨識讀取器，使機密文書的複印程序，必須經由正常申請流程方能啟動複印機，可以確保文書不當複印。
2. 經常盤點：於文書架上裝設固定讀取器，則不需人力介入，就可以不斷進行掃讀和盤點工作，以確保文書資料未經正常手續而離開保管架。

以上設計將可以強化機密文書保管機制，防止流失、竊取及不當複印等問題。

6.5. 應用上所遭遇的問題

Roy Want [29]指出，目前無線射頻辨識除了價格較高，不能普及的問題以外，其實還有：多重標準、隱私保護、資料處理能力及安全等技術問題尚待解決，分述如下：

- **多重標準**

標準（特別是關於資料格式定義的標準）的不統一是限制無線射頻辨識發展的首要因素。每個無線射頻辨識標籤中都有一個唯一的識別碼。如果它的資料格式有很多種且互不相容，那麼使用不同標準的無線射頻辨識產品就不能通用，這對經濟全球化下的物品流通是十分不利的。而資料格式的標準這個問題涉及到各個國家自身的利益和安全，目前已形成了日本泛在（Pan）ID 中心和美國的 EPC Globle 兩大標準組織互不相容的對抗局面。而中國也開始制定自己的無線射頻辨識標準，預計其他的許多國家也會陸續開始制定自己的標準。如何讓這些標準彼此相容，讓一個無線射頻辨識產品能順利的在世界範圍中流通是當前重要而急迫的問題。

關於標準的另一個問題是，目前還沒有正式的關於無線射頻辨識產品（包括各個頻段）的國際標準，ISO/IEC 18000 還只是一個草案。目前各個廠家推出的無線射頻辨識產品互不相容，造成了無線射頻辨識產品在不同市場和應用上的混亂和不相容。這勢必對未來的無線射頻辨識產品互通和發展造成了阻礙。

- **價格**

目前無線射頻辨識系統特別是電子標籤的價格還比較高的。如果要讓所有的商品都能貼上一個電子標籤，那麼電子標籤的成本至少需降到 5 美分以下。要達到這個目標，現在看來至少還需要 5 年的時間。另外，企業應用無線射頻辨識技術需要購買許多讀取器以及相應的管理軟體，另外還有許多如培訓等相

關的成本。這些投資的成本加起來也是十分可觀的。如果應用無線射頻辨識系統的成本太高，而帶來的收益又有限的話，那麼許多中小企業就會因此延遲導入無線射頻辨識的應用。

- **隱私保護**

在歐美國家無線射頻辨識的最大的問題是無線射頻辨識技術可能侵犯個人的隱私權。因此無線射頻辨識的使用受到了許多人權組織和消費者團體的反對，他們示威甚至試圖通過制定法律來阻止無線射頻辨識產品的使用。目前各大無線射頻辨識廠商正努力尋求解決之道，他們嘗試使電子標籤在商品銷售到消費者手中後自動失效，或者利用資料加解密的機制來保護個人隱私。但是，相關技術仍在研發之中，本論文只是描述一些方法，實務應用仍待克服許多問題。

- **資料處理能力**

對於使用無線射頻辨識技術的企業而言，如何有效處理應用無線射頻辨識技術帶來的巨大資料來降低成本，提高生產效率將是非常緊要的問題。企業要導入該項應用，必定需要一個資料管理平臺，它包括後端資料庫、應用程式以及正確的分析能力來處理由無線射頻辨識系統生成的大量資料。否則，企業可能會被大量的資料淹沒而得不到無線射頻辨識技術帶來的好處。目前，許多大應用系統開發商如 Sun、SAP、Oracle、IBM 等公司已經看到這個問題或商機，紛紛開始在其產品中整合無線射頻辨識相關技術，以滿足未來這方面的巨大需

求。

- **安全問題**

目前的無線射頻辨識技術在資訊保密的應用領域還存在著許多缺失，尤其是被動式無線射頻辨識，目前還沒有一套可靠的安全機制，針對本身的數據做很好的保密措施。一旦電子標籤中的資訊被竊取、複製並被非法使用的話，可能會帶來無法估量的損失。本論文所提出的點、線、面整體防偽機制以及四種防偽應用架構，就是期望能提供成本不高又能解決實務問題上的作法。

第 7 章 結論與未來研究方向

7.1. 結論

無線射頻辨識的應用已經悄悄地開始，預計不久就會全面展開。世界各先進國家都不能忽視這個潮流，紛紛投入人力、物力導入這項工作的先期研究及實驗。尤其 EPC 全球網路架構在 Wal-Mart 及 FDA 的推動下，將會取代條碼成為主要商品編號，而它所建立的全球網路商品架構，更會成為防偽機制中非常重要的工具之一。

本論文在應用無線射頻辨識的防偽機制時，提出點（電子標籤或讀取器本身）、線（電子標籤和讀取器之間）及面（全面網路架構）的整體防偽機制，研究如何利用無線射頻辨識解決生活周遭的偽造及仿冒問題。又從面的角度提出四個防偽架構，主要為解決企業在無線射頻辨識防偽應用上所遭遇的問題。因此，對於每一個架構，都深入討論它的應用範疇、配套措施、系統架構及優缺點分析等，將可以協助企業導入相關應用時，具有一些參考架構及適用條件，不會面臨無所適從的困境。並且這些架構將不只運用於防偽架構，其他應用範疇也能參考運用。

另外，對於無線射頻辨識應用上所遭遇的安全問題，本論文從點的角度，提出標籤及讀取器的安全設計方向。另外，從線的角度，在標籤及讀取器之間應用橢圓曲線簽章演算法，為兩者建立正確的認證機制，使非法標籤和讀取器

不能介入正常工作環境，以解決目前許多鼓吹自由團體所關心的隱私及安全問題。

至於從面的角度，則建立一個產品的完整的履歷資料是防偽工作的核心，而且，必須借助無線射頻辨識自動識讀的特性，在每個產品入、出貨時，運用 EPC 的網路架構，為每樣產品都建立完整的履歷，不只達到防偽的目的，也為產品的行銷、倉儲等問題建立一個良好的機制。

無線射頻辨識能夠提供更有效率的方法，意謂能帶來更多的利潤，但我們應將重點放在解決方案而不是科技本身。本論文從無線射頻辨識的防偽架構及網路架構著手，就是希望台灣在此新興領域的應用上，不要只從硬體研發上著手，還必須從軟體、系統、服務及營運模式等加以開發。免得重蹈當初台灣在 Internet 的應用上偏向網路硬體發展，而成為網卡大國，但在服務平臺及軟體系統方面卻幾乎繳了白卷的覆轍[37]。

7.2. 未來研究方向

本論文在 5.2.4 節研討有價票證的 V4 型防偽架構時，提出鈔票的防偽機制，仍面臨下述問題：

1. 鈔票防偽機制只適用於金融行庫，並不適用於普通民眾，以致偽鈔流入市面時，無法在第一道防線加以圍堵，最後在銀行偵測出來時，已較難找出偽鈔的真正來源。

2. 無線射頻辨識加上電子簽章驗證機制將使鈔票數點及查證作業時間

加長，為此，設計一個安全又快速的簽章驗證機制實屬必要。本論文所提的橢圓曲線數位簽章演算法，只考慮在安全度高及資料長度短的條件下所做的選擇，由表 3.2 可知其運算效能是四種公鑰密碼系統中最差的，如以銀行每天必需處理大量鈔票，且要求在很短時間完成驗證機制，可能無法滿足需求。另針對無線射頻辨識所發展的 NTRU 演算法，雖然效能最佳，但其資料太長及安全度不足均備受爭議，仍是企待改進的缺點。因此在線的防偽加強上，尚有很大發展空間。

另外，本論文雖然在第 4 章有價票證的防偽架構上，提出一些拋磚引玉的想法，但如果要達到真正實用、有效的有價票證的防偽解決方法，未來必須繼續加強研發以下提昇無線射頻辨識的防偽功能:

1. 提昇 RFID IC 晶片安全保護機能
2. 增強 RFID 標籤載體(例如非接觸式智慧卡)的防偽機制
3. 使用簡化且有效率的密碼技術來補強 RFID 在防偽功能的先天限制
4. 使用高效能的密碼技術來滿足基本及進階的防偽需求

參考資料

[[1] FDA's counterfeit drug task force interim report, U.S. Department of Health and Human Services, Food and Drug Administration, Rockville, MD, 2003.

[2] A.P., RFID to fight counterfeiting of Viagra, painkilling drugs, *Information Week,* Nov. 15, 2004.

[3] EPCglobal specifications & ratified standards, EPCglobal, 2003, http://www.epcglobalinc.org/standards_technology/specifications.html.

[4] R. Anderson and M. Kuhn., Low cost attacks on tamper resistant devices, 5th *International Workshop on Security Protocols*, LNCS, vol. 1361, pp. 125-136, Apr. 1997.

[5] RFID security issues, *AIM Global Network*, June 30, 2005, http://www.aimglobal.org/members/news/templates/rfidinsights.asp?articleid=392&zoneid=24.

[6] D. L. Evans, Security requirements for cryptographic modules, FIPS PUB 140-2, National Institute of Standards and Technology, May 2001.

[7] M. Feldhofer, S. Dominikus, and J. Wolkerstorfer, Strong authentication for RFID systems using the AES algorithm, Cryptographic Hardware and Embedded Systems, Boston, MA, pp. 357-370, 2004.

[8] A. D. Fernandes, Elliptic-curve cryptography, Dr. Dobb's Journal, vol. 24, no. 12, pp. 56-62, 1999.

[9] K. Finkenzeller, *RFID Handbook: Fundamentals and Applications in Ccontactless Smart Cards and Identification,* New York, NY, Wiley, 2003.

[10] D. Henrici and P. Muller, Hash-based enhancement of location privacy for radio-frequency identification devices using varying identifiers, Workshop on

Pervasive Computing and Communications Security, Orlando, FL, pp. 149-153, 2004.

[11] J. Hoffstein, J. Pipher, and J. H. Silverman, NTRU: A ring-based public key cryptosystem, LNCS, vol. 1423, pp. 267-288, 1998.

[12] J. Hong, J. Han, D. Kwon, and D. Han, Chosen-ciphertext attacks on optimized NTRU, 2002, http://eprint.iacr.org/2002/188.

[13] A. Juels, D. Molnar, and D. Wagner, Security and privacy issues in E-passports, Cryptology ePrint Archive: Report 2005/095, Sep. 2005, http://eprint.iacr.org/2005/095.

[14] A. Juels and R. Pappu, Squealing Euros: privacy protection in RFID-enabled banknotes, LNCS, no. 2742, pp. 103-121, 2003.

[15] P. Karu and J. Loikkanen, Practical comparison of fast public-key cryptosystems, Telecommunications Software and Multimedia Labratory, Helsinki University of Technology, Finland, 2001.

[16] N. Koblitz, Elliptic curve cryptosystems, Mathematics of Computation, vol. 48, no. 177, pp. 203-209, 1987.

[17] V. Miller, Use of elliptic curves in cryptography, LNCS, vol. 218, pp. 417-426, 1985.

[18] G. E. Moore, Cramming more components onto integrated circuits, *Electronics*, vol. 38, no. 8, Apr. 1965.

[19] P. Nguyen and D. Pointcheval, Analysis and improvements of NTRU encryption paddings, LNCS, vol. 2442, pp. 210-225, 2002.

[20] M. Ohkubo, K. Suzuki, and S. Kinoshita, Cryptographic approach to "privacy-friendly" tags, RFID Privacy Workshop, Cambridge, MA, 2003, http://www.rfidprivacy.org/papers/sozo_inoue.pdf.

[21] Sun Microsystems, Software solutions - EPC and RFID, Sun Microsystems,

http://www.sun.com/software/solutions/rfid/.

[22] Commission on Intellectual Property, The fight against piracy and counterfeiting of intellectual property, International Chamber of Commerce, Paris, France, June 2004.

[23] Combating Counterfeit Drugs: A Report of the Food and Drug Administration, U.S. Department of Health and Human Services, Food and Drug Administration, Rockville, MD, Feb. 2004, http://www.fda.gov/oc/initiatives/counterfeit/report02_04.html.

[24] J. Saito, J.-C. Ryou, and K. Sakurai, Enhancing privacy of universal re-encryption scheme for RFID tags, LNCS, vol. 3207, pp. 879-890, 2004.

[25] T. Staake, F. Thiesse, and E. Fleisch, Extending the EPC network: The potential of RFID in anti-counterfeiting, 20th ACM Symp. on Applied Computing, Santa Fe, NM, pp. 1607-1612, Mar. 2005.

[26] D. Sun, RFID and pharmaceutical anti-co----unterfeit, 2005, http://www.scholarlyexchange.org/journals/journalindex.php?journal_id=18&PHPSESSID=e65a768d70df50da9434448b1dc114ef.

[27] C. G. a. M. Szydlo, "Cryptanalysis of the revised NTRU signature scheme," Proc. Proc. of the Int. Conf. on the Theory and Applications of Cryptographic Techniques, London, UK, pp. 299-320, 2002.

[28] K. Traub, et al., EPCglobal Architecture Framework version 1.0, EPCglobal, 2005, http://www.epcglobalinc.org/standards_technology/Final-epcglobal-arch-20050701.pdf.

[29] R. Want, The magic of RFID, *ACM Queue*, vol. 2, no. 7, pp. 41-48, Oct. 2004.

[30] S. H. Weingart, Physical security devices for computer subsystems: A survey of attacks and defenses, LNCS, vol. 1965, pp. 302-317, 2000.

[31] S. A. Weis, S. E. Sarma, R. L. Rivest, and D. W. Engels, Security and privacy

aspects of low-cost radio frequency identification systems, LNCS, vol. 2802, pp. 201-212, 2004.

[32] D. J. Wheeler and R. M. Needham, TEA, a tiny encryption algorithm, LNCS, vol. 1008, pp. 363-366, 1994.

[33] J. Wolkerstorfer, Is elliptic-curve cryptography suitable to secure RFID tags? Workshop on RFID and Light-Weight Crypto, Graz, Austria, July 2005.

[34] J. Yoshida, Euro bank notes to embed RFID chips by 2005, *EE Times*, Dec. 19, 2001, http://www.eetimes.com/printableArticle?doc_id=OEG20011219S0016.

[35] 王連興, RFID 無線身份識別系統及讀卡機架構說明, 台北,電子技術雜誌, vol. 208, 2004, http://epaper.eedesign.com.tw/epaper/epaperpreview.asp?id=185.

[36] 胡宏亮, *票券印刷芻論*, 台中, 印刷出版社, 1992, http://www.cgan.com/book/books/print/stock/index.htm.

[37] 曾建榮, 張善政, 打造幕後資訊流動管道RFID貨暢其流－宏碁, 技術尖兵, vol. 117, 台北, Sep. 2004, http://www.st-pioneer.org.tw/modules.php?name=magazine&pa=showpage&tid=2174.

[38] 鄭博仁, 陳林福, 陳品儀, 謝德鑫, 無線射頻辨識技術與資訊安全應用, 資訊安全技術通訊, vol. 10, no. 2, pp. 78-86, 台北, 2004.

作者簡介

姓名：余敬虔

出生地：台中縣

生日：民國四十五年十二月十日

學歷：民國六十七年　國立高雄工專

機械工程科畢業

民國七十二年　國立臺灣工業技術學院

機械工程技術系畢業

民國八十二年　美國加州州立聖荷西大學

電機工程研究所肄業

民國九十六年　國立臺灣科技大學

資訊工程系研究所畢業

射 频 和 天 线 设 计 培 训 课 程 推 荐

易迪拓培训(www.edatop.com)由数名来自于研发第一线的资深工程师发起成立，致力并专注于微波、射频、天线设计研发人才的培养；我们于 2006 年整合合并微波 EDA 网(www.mweda.com)，现已发展成为国内最大的微波射频和天线设计人才培养基地，成功推出多套微波射频以及天线设计经典培训课程和 ADS、HFSS 等专业软件使用培训课程，广受客户好评；并先后与人民邮电出版社、电子工业出版社合作出版了多本专业图书，帮助数万名工程师提升了专业技术能力。客户遍布中兴通讯、研通高频、埃威航电、国人通信等多家国内知名公司，以及台湾工业技术研究院、永业科技、全一电子等多家台湾地区企业。

易迪拓培训推荐课程列表： http://www.edatop.com/peixun/tuijian/

射频工程师养成培训课程套装

该套装精选了射频专业基础培训课程、射频仿真设计培训课程和射频电路测量培训课程三个类别共 30 门视频培训课程和 3 本图书教材；旨在引领学员全面学习一个射频工程师需要熟悉、理解和掌握的专业知识和研发设计能力。通过套装的学习，能够让学员完全达到和胜任一个合格的射频工程师的要求…

课程网址：http://www.edatop.com/peixun/rfe/110.html

手机天线设计培训视频课程

该套课程全面讲授了当前手机天线相关设计技术，内容涵盖了早期的外置螺旋手机天线设计，最常用的几种手机内置天线类型——如 monopole 天线、PIFA 天线、Loop 天线和 FICA 天线的设计，以及当前高端智能手机中较常用的金属边框和全金属外壳手机天线的设计；通过该套课程的学习，可以帮助您快速、全面、系统地学习、了解和掌握各种类型的手机天线设计，以及天线及其匹配电路的设计和调试...

课程网址： http://www.edatop.com/peixun/antenna/133.html

WiFi 和蓝牙天线设计培训课程

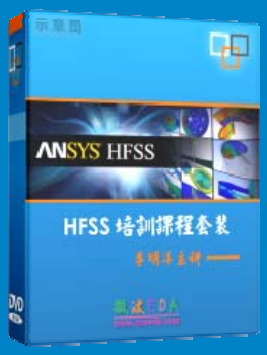
该套课程是李明洋老师应邀给惠普 (HP)公司工程师讲授的 3 天员工内训课程录像，课程内容是李明洋老师十多年工作经验积累和总结，主要讲解了 WiFi 天线设计、HFSS 天线设计软件的使用，匹配电路设计调试、矢量网络分析仪的使用操作、WiFi 射频电路和 PCB Layout 知识，以及 EMC 问题的分析解决思路等内容。对于正在从事射频设计和天线设计领域工作的您，绝对值得拥有和学习！…

课程网址：http://www.edatop.com/peixun/antenna/134.html

CST 学习培训课程套装

该培训套装由易迪拓培训联合微波 EDA 网共同推出，是最全面、系统、专业的 CST 微波工作室培训课程套装，所有课程都由经验丰富的专家授课，视频教学，可以帮助您从零开始，全面系统地学习 CST 微波工作的各项功能及其在微波射频、天线设计等领域的设计应用。且购买该套装，还可超值赠送 3 个月免费学习答疑…

课程网址：http://www.edatop.com/peixun/cst/24.html

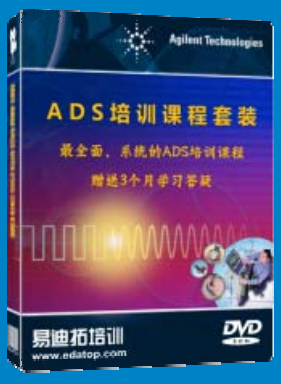


HFSS 学习培训课程套装

该套课程套装包含了本站全部 HFSS 培训课程，是迄今国内最全面、最专业的 HFSS 培训教程套装，可以帮助您从零开始，全面深入学习 HFSS 的各项功能和在多个方面的工程应用。购买套装，更可超值赠送 3 个月免费学习答疑，随时解答您学习过程中遇到的棘手问题，让您的 HFSS 学习更加轻松顺畅…

课程网址：http://www.edatop.com/peixun/hfss/11.html

ADS 学习培训课程套装



该套装是迄今国内最全面、最权威的 ADS 培训教程，共包含 10 门 ADS 学习培训课程。课程是由具有多年 ADS 使用经验的微波射频与通信系统设计领域资深专家讲解，并多结合设计实例，由浅入深、详细而又全面地讲解了 ADS 在微波射频电路设计、通信系统设计和电磁仿真设计方面的内容。能让您在最短的时间内学会使用 ADS，迅速提升个人技术能力，把 ADS 真正应用到实际研发工作中去，成为 ADS 设计专家...

课程网址： http://www.edatop.com/peixun/ads/13.html

我们的课程优势：

※ 成立于 2004 年，10 多年丰富的行业经验，

※ 一直致力并专注于微波射频和天线设计工程师的培养，更了解该行业对人才的要求

※ 经验丰富的一线资深工程师讲授，结合实际工程案例，直观、实用、易学

联系我们：

※ 易迪拓培训官网：http://www.edatop.com

※ 微波 EDA 网：http://www.mweda.com

※ 官方淘宝店：http://shop36920890.taobao.com