RFID 門禁身分認證系統之安全架構探討

洪燕竹[1]　蔡佳偉[2]　洪嘉鴻[3]
國立嘉義大學資訊工程所
[1]Andrew@mail.ncyu.edu.tw
[2]s0930316@mail.ncyu.edu.tw
[3]chhong@csie.ncyu.edu.tw

摘要

RFID 技術演進至今已超過 60 年,近年來 RFID 技術更是被加以廣泛利用，例如：取代傳統的二維條碼、物流管理、倉儲管理、軍事管理、身分辨識…等，全球大企業也已制訂出無線射頻辨識技術(RFID)計劃,RFID 儼然成為新一代殺手級的應用。但因 RFID 使用無線傳輸的特質，而也引出了新的資訊安全議題，而在現今已制定完成的 RFID 標準規格書中也未對此提出安全議題的解決方法，因而本研究希望用 Hash、AES、Random values、XOR 四項技術結合三方認證架構，提出一個可實作於硬體受限的 RFID smart card 上之安全認證機制，以解決現在使用 RFID smart card 身分辨識與門禁系統上的安全憂慮。

關鍵詞：RFID、RFID Smart card、AES、HASH

1.前言

自從二次大戰時用在辨識敵機或是我機開始，RFID 技術演進至今已超過 60 年，現在全球年銷售額在 50 億美元以上的大企業，已經有 70%企業已制訂出 RFID 技術計劃，由此可見 RFID 技術已受到百貨零售業、政府機關與倉儲業..等的青睞,RFID 技術儼然成為新一代殺手級的應用。RFID 除了常被運用在物流倉儲管理外，另一項應用則是將 RFID tag 嵌入 smart ic card 中，其此項的運用層面非常的廣泛，例如:台北捷運的悠遊卡、大樓門禁管理的識別牌、政府和學校工作證和學生證…等，藉著 RFID 無線傳輸、非接觸性的特質，改善了原先接觸式 smart card 使用上的不便性和易被偽造…等問題；但也因 RFID 使用無線頻率溝通、傳送資料，其新的安全議題也漸漸浮出檯面，而加上 RFID 系統安全議題在現今國際標準規格書中尚未完整規範,使得 RFID 系統在安全上有著極大的爭議性。

本篇研究所討論的 RFID 標籤(tag)頻率為 13.56MHz，在 ISO/IEC18000-3 規定其屬於被動式標籤(Passive Tag)，在標籤中未內建電池，體積上也有所限制，故標籤的運算能力有限且記憶體容量不大，而使用傳統的加密演算法和認證機制無法在其上實行。因此，在本篇研究中，希望可以使用 Hash、AES、Random values、XOR 四項技術結合三方認證架構,提出一個運算量少、安全強度高的 RFID smart card 安全認證機制，以解決現在使用 RFID smart card 身分辨識與門禁系統上的安全憂慮， 除外，別於一般的安全認證機制，本研究更加入主動式防護機制，以此進一步強化系統的安全性，降低 RFID smart card 內資料被竊聽、偽造…等惡意攻擊成功的機率。

2.背景知識

2.1 射頻辨識系統(RFID)

RFID 是指 Radio Frequency Identification 系統，RFID 系統有點類似 Smart card 系統，它是針對接觸式系統的缺點而開發，利用射頻訊號以無線方式傳送數位資料，因此識別卡並不須與讀卡機接觸即可達成資料交換。以這種方式傳送資料並無方向性的要求，卡片置於口袋或皮包內就可立即辨識。它是一種『貼卡』式微型雙面無線電波的晶片，是將一個簡單的積體電路器（IC），只用兩個接點連到另一個天線（Antenna）上，即完成可接收訊號的裝置。當對其發出電磁波遙控訊號的問題時，該卡隨即可以數位無線電波訊號回答出所要的資料，無線射頻辨識系統主要由四大部分組成,分別為 RFID tag、RFID reader、Back-end database、Frequency radio。[1][2][3]

（1）RFID tag

貼置或嵌入於商品、貨品、smart card 上之 RF 晶片，主要的結構包含：CLK 電路、AC to DC 整流濾波器、變調器（Demod）、編解碼電路（Codec）、微處理器（uP）、記憶體（Memory）。

RFID tag 主要分為二種，主動式與被動式：

A.主動式標籤(Active Tag)

內建一顆小電池，記憶體容量可達 1MB，使用電波通訊,擁有較長無線通信距離(可達 100 公尺)，但使用期限受到限制，使用期限約七~十年， 相對成本高。

B.被動式標籤(Passive Tag)

沒有內建電池，標籤內線圈可以經由 reader 發

出的電場取得能量，因使用電磁感應通訊故通訊距離短，然而成本也較為低、體積小、壽命長較具競爭力，未來極有可能成為市場主流。如下表 2-1 對主動式與被動式 RFID tag 做比較。

表 2-1 主動式與被動式比較

	主動式	被動式
電源裝置	內建	未內建
感應距離	較遠	較短
使用年限	有	無
設備體積	大	小
環境狀況	對高、低溫較敏感	能適應於較差的環境
價　　位	較高	較低

（2）RFID reader

讀取、接收貼置或嵌入商品、貨品、smart card 內 RF 標籤(tag)的接收器，主要的結構包含：鎖相迴路和電壓控制盪器、變調器（Demod）、編解碼電路（Codec）、微處理器（uP）、記憶體（Memory）、時脈產生器，RFID reader 可以利用天線對 RF 標籤(tag)做讀取或寫入的動作，不同的 RFID 系統各有其不同的天線種類，如賣場出入口的讀取器，因所攜出的物品高度不一，其天線可達一人高，此天線不必隨時做傳輸啟動 tag，可以配合踏墊感應器做傳送啟動。讀取器可以分為固定式和手持式二類，固定式的讀取機可以置於賣場出口、賣場貨架、倉庫出入口、貨車、貨櫃場出入口、機場...等，手持式則輕巧許多，具有方向性且感應距離不長。

(3) Back-end database

主要功能為紀錄 RF 標籤(tag)的詳細資料，當讀取器收到 RF 標籤(tag)訊號，會以無線或有線網路連結 back-end database，取得該 RF 標籤(tag)的詳細資料整合後，供給其他應用程式使用。

(4) Frequency radio

RFID 的頻率，串聯起電子標籤與讀卡器之間的資訊傳輸，由讀卡機發出頻率到電子標籤，而電子標籤再回傳電子標籤內的資訊給讀卡機，頻率的選擇主要是根據 RF 讀取器(reader)和 RF 標籤(tag)之間的距離，一個較低的頻率意味一個較低的讀取範圍，以及較慢的資料傳輸率，但在金屬與濕氣的環境下相對於高頻率卻擁有較佳的讀取能力，除外，也要考慮到各國家開放的頻率而定；每一個國家所可以使用的頻帶不盡相同，一般而言，低頻帶的 RF 讀取器(reader)和 RF 標籤(tag)之間的資料傳輸和通訊頻率是不受國家政府管制的，而極高頻的頻帶就會受到限制，以日本政府而言，已決定將 950~960MHz 的頻帶開放給 RFID 系統使用。RFID 系統以頻率來做分類的話，可分為四類：低頻(LF, 125KHz~135KHz)、高頻(HF,13.56MHz)、極高頻(UHF , 100MHz~960MHz)、微波(Microwave, 1GHz 以上)。

2.2 RFID 安全問題

RFID 系統為透過無線方式傳輸資訊，因而，若 RFID 系統若沒有提供完善的安全機制的話，在可傳輸訊息的範圍內，攻擊者都可以任意存取、竄改、刪除及毀損 RFID tag 資訊，此項弱點已明顯的威脅到組織、企業、個人的資料安全和隱私權，下文將指出攻擊者透過 RFID 技術此項弱點，可能造成的安全問題。[4][8]

2.2.1 竊聽(Eavesdropping)

因 RFID 系統以無線方式作為資料傳輸、溝通的管道，故攻擊者可以在 reader 和 tag 溝通範圍中竊聽資料、訊息，此種攻擊方式稱為「竊聽(Eavesdropping)」；在 RFID 系統的傳輸通道中，可大致分為 reader-to-tag(forward channel)、tag-to-reader(backward channel)。forward channel 由 reader 所產生，故距離長、範圍大(可達到 100 公尺)，故較容易遭受竊聽，且不容易察覺；backward channel 由 tag 所產生，距離短、範圍較小，竊聽困難度較高，不容易發覺系統被竊聽。其可以下圖 2-1 圖表示：

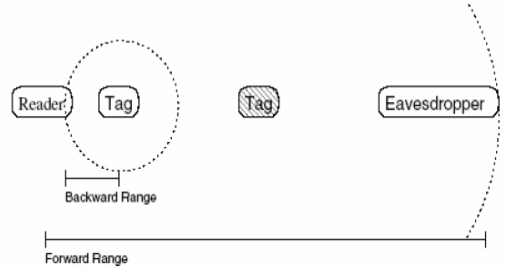

圖 2-1 Forward、Backward 範圍

竊聽(Eavesdropping)此安全問題將會造成二項重大危害，一為個人資料外漏，另一為商業間諜行為。

（1）個人資料外漏

在個人資料外漏部份，目前已經被廣泛使用的 RFID smart card 中，常常存儲持卡人的個人隱私資料，例如：健保卡中存放就醫紀錄、個人資本資料...等個人資料，這些資料都為持卡人不願公開，也必須保護的資料，但 RFID 系統為非接觸式卡，也因此讓個人隱私資料外漏機率相對提高。

（2）商業間諜行為

現在製造業、物流業、零售業、軍事機構...等，以極力推廣 RFID 系統的使用，而其 RFID 對其也帶來相當可龐大的利益、便利，然而，在這陣 RFID 風潮下，所隱藏的將是被攻擊者監控、竊取資料的

風險，RFID 系統使得廠商可以利用存於 tag 記憶體的資料，快速的得到其貨品名稱、型號、原料、物流流程…等貨品資料，相對的攻擊者也以此方式獲得、監控貨品資料，使得商業間間諜活動更加猖獗，若不進一步提出安全機制防範將會帶來嚴重的後果。

2.2.2 跟蹤(Traceability)

在 RFID 系統中，RFID reader 可以透過 RF 標籤(tag)的回傳訊息來取得資料、追蹤貨品，也應此特性使得攻擊者可以藉由 RF 標籤(tag)回傳訊息追蹤貨品或使用人，此攻擊稱為「跟蹤(Traceability)」。攻擊者可以追蹤 tag 行蹤，主要的原因在於 tag 回傳值往往是固定不變，有些 RF 標籤(tag)是直接回傳 UID 值，UID 又為此 RF 標籤(tag)獨一無二辨識值，故攻擊者只要在許多定點設置 reader 就可藉由此特性掌握貨品或使用者行蹤，例如：球鞋廠商為了做物流、倉儲管理，而鞋子內部嵌入 RF 標籤(tag)晶片，當消費者 A 購買此雙球鞋後，攻擊者就可以透過定點 RFID reader 跟蹤 A 的行蹤，使 A 隱私性蕩然無存。

2.2.3 欺騙(Spoofing)

在介紹完竊聽、跟蹤二項 RFID 安全性議題後，另外一個安全性議題為欺騙(Spoofing)，此議題主要包二項：偷竊(Theft)、偽造(Counterfeiting)。

（1）偷竊(Theft)

透過欺騙合法 RF 標籤(tag)，攻擊者可以透過 RFID 系統特性欺騙自動化結賬系統、門禁安全系統，例如：攻擊者能重寫或者從更便宜的東西用替換昂貴東西上的 RF 標籤(tag)資料，或者攻擊者能使竄改一大批 RF 標籤(tag)，混亂整個供應鏈管理。

（2）偽造(Counterfeiting)

偽造(Counterfeiting)被定義為能讀或攔截竄改一個 RF 標籤(tag)的資料。攻擊者可以透過偽造 RF 標籤(tag)資料，來欺騙 RFID 系統，例如：偽造門禁系統 IC card，侵入公司或軍事機構。

2.3 RFID 現行安全對策

現在 RFID 安全問題被提出的解決對策主要可分為二大類，分別為:Non-Cryptographic Scheme 和 Cryptographic Scheme。

在此對數個重要的解決方案做簡單的敘述，在 non-cryptographic scheme 部分，介紹 Kill tag approach、Rewriteable memory，在 cryptographic scheme 部分，介紹 Hash based access control、Randomized access control、Hash chain。[5][6][7][9][10]

（1）Kill tag approach

為了避免 RF 標籤(tag)到使用者手上後，所產生安全性議題，故此解決方式是在 RF 標籤(tag)到使用者手上前將其記憶體資料刪除，其方式的執行方式是在每一個 RF 標籤(tag)中都存放一個 8 bits 密碼，當 RF 標籤(tag)收到此密碼時，就執行 kill 指令。而 Kill tag approach 卻存在二個問題，一為必需製造廠商支援，另為很難確定 kill 指令是否已經確定執行。

（2）Rewriteable memory

將嵌在 RF 標籤(tag)中的記憶體分成 ROM、RAM 二部份，ROM 存放可公開資料，RAM 中存放隱私資料，reader 存取 RAM 資料必須通過認證；以方式常搭配 cryptographic scheme 實作。

（3）Hash based access control

主要使用 Hash 的不可逆性來做認證，其架構如下圖 2-2 所示：

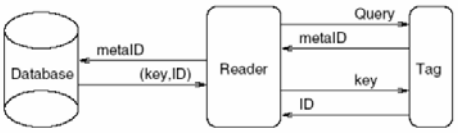

圖 2-2 Hash based access control

在 RF 標籤(tag)中會預先存入 metaID 值(metaID = hash(key))，當 reader 質問 RF 標籤(tag)時，RF 標籤(tag)回傳 metaID，reader 搜尋後端 database 找出符合的 key 值完成認證步驟。此方法解決了 RF 標籤(tag)資料被竊聽的問題，但因 RF 標籤(tag)固定回傳 metaID 值，故無法防止攻擊者跟蹤。

（4）Randomized access control

此方法改進Hash based access control可被跟蹤的問題，在回傳值內加入一亂碼值R，以此改變每次回復reader質問的值，其回傳值為｛R ,h(ID_k ‖ R)｝，其架構如下圖 2-3 所示：

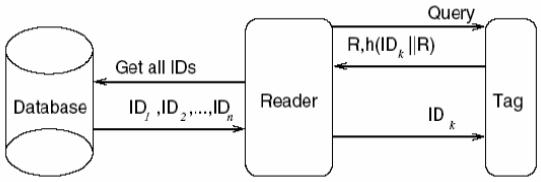

圖 2-3 Randomized access control

（5）Hash chain

在RF標籤(tag)中回存入一個初始值s(s1)，而其與reader溝通方法相似，只是回傳值改成$a_i = G(s_i)$，而在回應reader後，立即改變$s_i+1=H(s_i)$，其中G、H都為hash function，其架構如下圖 2-4 所示：

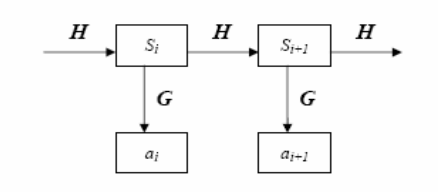

圖 2-4 Hash chain

3.系統架構

3.1 概述

現行門禁系統中，已多屬採用 RFID smart card 做為使用者之識別證，以此 RFID 技術可以讓使用者更加方便、快速的完成身分認證，但隨此便利性相對引出了安全性議題，在本研究中，我們提出一個使用對稱式加密演算法(AES)、HASH、Random value 和三方認證的 RFID smart IC card 門禁安全認證系統架構，此系統架構不只保護使用者資料隱私性、仿止偽造、盜用，並可以進一步保護持卡人不被跟蹤，此外，不同於其他安全系統架構只專注於被動式的安全保護，在本系統中，將提出主動性偵測 smart IC card 安全性機制，在 card 遇到攻擊後，主動啟動對應措施，使其資料安全性、隱私性保護更進一層，其系統架構如下圖 3-1 所示：

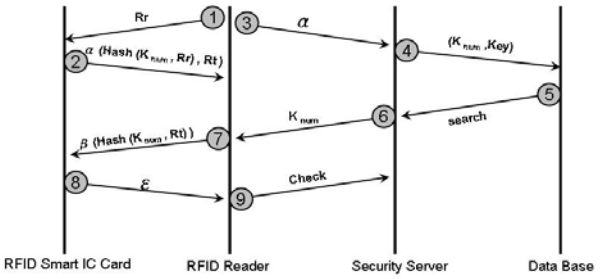

圖 3-1 系統架構

本研究所討論之RFID smart IC card為13.56Mhz頻率之RF標籤(tag)，故必須遵照ISO / IEC 18000 規格書之規範，因此，在硬體上有許多限制，在本研究中，我們在RF標籤(tag)中嵌入一個hash運算器、random產生器，及數個邏輯閘，此方式並未違反規格書硬體限制之規定；在介紹系統架構流程之前，我們先定義存儲於RF標籤(tag)記憶體、security system database中的資料結構，在RF標籤(tag)之資料結構為{S_ count , Key $_{num}$, P_k (Data)}，S_ count紀錄此張RFID smart IC card被RFID reader掃描次數，K_{num}為此RFID smart IC card中持卡人資料加密使用金鑰之識別序號，P_k (Data)為持卡者資料以K_{num}之金鑰加密後產生的密文。在security system database之資料結構分別有{K_{num} ,Key_i}、{ID , S_C_count}，Key_i為系統加密使用金鑰中的其中之一，K_{num}為對應Key_i金鑰的識別序號，ID為使用者之識別碼， S_C_ count為記錄系統和此持卡者完成認證次數。其系統data structure如下圖 3-2 所示：

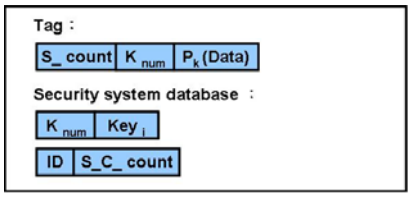

圖.3-2 Data Structure

3.2 系統流程

在此開始說明圖.3-1 的系統流程架構，將系統流程步驟分成九個步驟來說明：

(1) 持卡者持 RFID Smart card 進行身份確認時，持卡者將卡片置入 RFID reader 可存取範圍內後，RFID reader 將對 RFID smart card 發出質問訊息，此質問訊息包含 Rr 值，Rr 為 reader 隨機產生之 128 bits 亂數碼。

(2) RFID smart IC card進入reader感應範圍，藉由電磁感應產生所需電力，會先將儲存於RF標籤(tag)中的S_ count值累加，產生 α 訊息作為回應，α ={F_t(K_{num} , Rr)|| Rt}，Ft為嵌入tag中之hash function，Rt嵌入於RF標籤(tag)中亂碼產生器所產生之亂數。其RFID reader所發出的質問訊息和IC card所回應的 α 訊息格式都會以ISO/IEC 18000-3 規格書所定義的通訊架構作為傳輸，其通訊架構如下圖 3-3、3-4 所示:

SOF	Flags	Com code	IC Mfg	UID	Signed data Rr	CRC	EOF
	8 bit	8 bit	8 bit	64 bit	128 bit	16 bit	

圖. 3-3 質問訊息架構

SOF	Flags	UID	Signed data α	CRC	EOF
	8 bit	64 bit	128 bit	16 bit	

圖. 3-4 α 訊息架構

(3) RFID reader 將接收到的 α 值回傳給後端系統，做認證比對。

(4) 安全系統搜尋後端資料庫所儲存K_{num}後，比對F_r(K_j , Rr)和 α 。

(5) 將所得持卡者所持有IC card資料的金鑰Key $_i$和K_i傳回系統，若搜尋所有K_{num}後，並未找吻合K_i，則回傳錯誤訊息。

(6) RFID reader將發出 β 訊息以試圖取得RFID smart IC card 之持卡人資料， β =F_r(K_i , Rt)。

(7) RF標籤(tag)確認 β 訊息，比對其K_i是否等於K_{num}。

(8) 確認 β 訊息正確無誤後，回傳 ε ， ε =(P_k

(Data) || S_count) ⊕ F_t(Rr)。

(9) RFID reader透過所持有的Key_i、Rr、S_C_count值對持卡人資料以進行身分核對工作，其核對方式是利用Fr(Rr) ⊕ ε 取得P_k (Data) || S_count，在使用金鑰解密出P_k (Data)之Data值，以核對持卡人身份。

上述 9 個步驟為被動是安全認證機制的運作過程，而在上文我們提到本系統提供主動式安全認證機制，其運作方法如下文所述，系統將應實際需求制定二個安全門檻值(T_1、T_2)，而在安全認證步驟(9)，安全系統會在 ε 訊息中取得S_count，計算S_count和S_C_count差值n後，將n和系統內訂門檻值做比對，若n大於T_1則系統將對持卡人發出警告，告知卡片可能已被攻擊，若超過T_2則鎖著此RFID smart IC card，並請持卡人至資訊部門申請開卡，系統安全管理人員將使用不同的金鑰對持卡人私人資料重新加密和更改K_{num}值，以此方式達到主動安全防護的機制，提高認證系統的安全強度。

3.3 安全性分析

在第二章節中，已介紹 RFID 系統的安全性問題，在此小節中我們將本研究所提出之安全認證機制對其 RFID 系統安全問題一一做安全性分析，以證實本系統架構的安全性，在此研究中，我們假設 RFID reader 和後端資料系統傳輸資料、溝通時都處於在一個安全的環境中，故本研究並不討論 RFID reader 和後端資料系統傳輸連線的安全議題。

3.3.1 竊聽(Eavesdrop)

在本系統傳輸架構中，RFID smart IC card和RFID reader的認證過程(見圖 3-1，步驟 1、2、7)、資料傳送(見圖 3-1，步驟 8)，傳輸資料都受hash function加密保護，而hash function有著不可逆性，縱使攻擊者竊聽到此認證過程之訊息，其也不能逆推出原本的訊息，此外，認證過程中使用了Rr、Rt二個亂數值，使每一次認證都有著不同的資料訊息，增加攻擊者使用暴力法的困難度。傳送持卡人資料時，系統會對資料先和F_t(Rr)做xor運算後傳送，持卡人的資料已是以密文儲存於RF標籤(tag)記憶體中，縱使攻擊者使用竊取到Rr 值，計算出F_t(Rr)值，破解xor運算保護後，攻擊者取得P_k (Data)加密的資料，也因系統有著數把不同的加密金鑰而使破解所需花費成本和時間提高，例如：使用暴力法破解 128bits金鑰AES加密演算的資料需要花費2^{128}，若金鑰數為 2^5，則破解所需的花費將增至2^{640}，故攻擊者無法從竊取到P_k (Data)值解出持卡人的私密資料。

3.3.2 欺騙(Spoofing)

在門禁系統中，身分辨識IC Card被偽造、盜用嚴重安全議題之一，在本系統中，攻擊者可以使用竊聽方式取得P_k (Data|| S_count) *xor* F_t(Rr)值，若攻擊者可以分析解譯出P_k (Data)值後，加以偽造IC Card試圖欺騙安全系統時，也會因安全系統在核對身分資料前必須先通過認證步驟(見圖 3-1，步驟 1、2、3)，此時，攻擊者必須要一併持有此RFID smart IC card的K_{num}值才完成認證步驟進入核對階段，而K_{num}在傳輸過程中都會經hash function、random value加密，攻擊者無法透過竊聽資料中取得K_{num}值，故空持有P_k (Data)也無法完成其欺騙系統的目的。

3.3.3 跟蹤(Traceability)

傳統 RFID 系統中，攻擊者只要利用數個固定位置的 RFID reader 就可以透過持卡人的 RFID smart IC card 中內嵌的 RF 標籤(tag)晶片，利用其回答 attacker reader 質詢之固定回覆訊息，來跟蹤持卡人的行蹤，本研究所提出的安全機制中，因在 RFID tag 中額外嵌入 hash 計算器、random 產生器，故每次整個 RF 標籤(tag)和 RFID reader 溝通傳輸(見圖 3-1，步驟 1、2、7、8)的訊息值都不會是固定值，因此攻擊者無法由固定的回覆訊息得知 RF 標籤(tag)的行蹤。

3.3.4 Man-in-the middle attack

若攻擊若擷取合法之RFID reader和RF標籤(tag)訊息加以偽造後傳送，執行完成攻擊Man-in-the middle attack後，可取得(P_k (Data) || S_count) ⊕ F_t(Rr)值，則攻擊者面臨如上述欺騙攻擊防護一樣的難題，攻擊者必須破解二道加密程序才可以取得持卡人私密資料，故本安全系統架構可以有效仿止Man-in-the middle attack。

3.3.5 Replay attack

不管是安全系統端或是 RF 標籤(tag)端，若發生認證無法通過的情況時，會立即停止回覆訊息，此外，系統使用了二個亂數值和主動安全防禦機制，如此重送攻擊根本無法對系統產生攻擊效果。

3.3.6 主動應變措施

別於其他安全機制，我們在RF標籤(tag)記憶體中加入S_ count、S_C_ count二個計數值和二個安全門檻值(T_1、T_2)，當攻擊者的RFIF reader試圖存取此RFID smart IC card時，若無法完成認證過程，則S_ count、S_C_ count值就會產生差異值，當合法RFID reader完成認證步驟，取得RF標籤(tag)記憶體中資料，比對S_ count、S_C_ count值差異後，若發現S_

count、S_C_ count差異大於T_1時，系統會對持卡人發出其IC card已被攻擊的訊息，若其差值大於T_2後，將會要求持卡者到安全部門更新IC card內資料，使用不同的金鑰對私人資料重新加密和更改K_{num}值，以此確保系統的安全性與持卡人的隱私性；而系統在此使用二層門檻值的原因在於RFID smart IC card和RFID reader傳輸資料溝通間可能因一些不可預期的因素而發生溝通、傳送資料失敗的情況，例如:雨天空氣中溼氣過重、持卡者使用金屬製品放置RFID smart IC card…等，故使用二個門檻值來免除使用者因不可預期因素而必須時常更換卡片資料的不便性。

4.結論

RFID 技術的發展為人們帶來了極大便利性，但其安全問題也是其最大弊病，若不提出解決方法，將會嚴重威脅到到個人、公司、軍方和政府機構資料安全性；本研究提出一 RFID smart card 門禁系統認證機制，以 Hash、AES、Random values、XOR 四項技術，結合三方認證，以解決 RFID smart card 所會面臨到竊聽、跟蹤、偽造…等安全問題，並且所嵌入 RF 標籤(tag)硬體也符合 ISO/IEO 18000-3 的標準規定，故其實踐可能性極高，除外，在架構中也加入主動式的防護系統，進一步加強安全性系統的強度，防止攻擊者可能使用重送攻擊或 DoS 攻擊癱瘓安全系統的潛在危險性。

5.參考文獻

[1]. 鄭同柏,"RFID EPC無線射頻辨識完全剖析", 2004 年 1 月,博碩文化。

[2]. 陳宏宇,"RFID 系統入門 無線射頻辨識系統",2004 年 12 月,松崗。

[3]. Flor, T.; Niess, W.; Vogler ,"RFID: the integration of contactless identification technology and mobile computing", ConTEL 2003, Telecommunications, Volume: 2 , 11-13 June 2003.

[4]. Juels and R. Pappu, (2003), "Squealing euros: Privacy protection in RFID-enabled banknotes", In proceedings of Financial Cryptography – FC'03, LNCS, volume 2742, Springer-Verlag, pages 103-121.

[5]. Juels, R. L. Rivest and M. Szydlo, (2003), "The Blocker Tag: Selective Blocking of RFID Tags for Consumer Privacy", In V. Atluri, ed. 8th ACM Conference on Computer and Communications Security, pages 103-111. ACM Press, (CCS 2003), October.

[6]. M. Ohkubo, K. Suzki and S. Kinoshita, (2003),"Cryptographic Approach to 'Privacy Friendly' Tags", Nippon Telegraph and Telephone, November.

[7]. Martin Feldhofer," An Authentication Protocol in a Security Layer for RFID Smart Tags",IEEE Melecon 2004,May.

[8]. S. Weis, (2003), "Security and Privacy in Radio-Frequency Identification Devices", Masters Thesis, MIT. May.

[9]. S. A. Weis, S. E. Sarma, R. L. Riovest, and D. W. Engels, (2004), "Security and Privacy Aspects of Low-Cost Radio Frequency Identification Systems", In D. Hutter et al. (Eds.): Security in Pervasive Computing 2003, LNCS, volume 2802, Springer-Verlag, pages 201–212.

[10]. Xingxin Gao, Zhe Xiang;,Hao Wang;,Jun Shen; Jian Huang, Song Song ,"An Approach to Security and Privacy of RFID System for Supply Chain", IEEE International Conference on , 13-15 Sept. 2004.