強化隱私保護之 RFID 自我認證及雙向鑑別機制

作者／蔡嘉富少校、李建鵬中校

提要

一、 無線射頻識別(RFID)電子標籤具有能夠被即時追蹤與管理及遠距批次處理的特性，用於供應鏈的環境可大大提升整體效率。由於 RFID 標籤本身具有唯一識別的特性，可以衍生用來判別貨品的真偽，惟 RFID 裝置在通訊過程中，相互傳遞資料的安全問題，一直是大眾的疑慮。

二、 近年來，有許多根基於密碼理論的 RFID 身分認證機制被提出，雖然這些方法在安全的問題上有改善，但是皆無法提供高傳輸效率的保障。因此，在考慮資料安全性的同時，亦需顧慮到可行性問題。

三、 本篇文章利用互斥或(XOR)運算與雜湊(Hash)函數，設計出具隱私保護的 RFID 自我認證機制，此法不僅可避免後端資料庫遭追蹤，提供了具重要地位(後端資料庫)安全防護之特性外，並且可提高運作效率。適用於目前最普遍之計算力弱、記憶體容量小的電子標籤，可應用在國軍後勤等方面以有效支援各項任務。

關鍵詞：自我認證、無線射頻識別、隱私。

前言

無線射頻識別(Radio Frequency Identification, RFID)技術是一項能夠透過無線的方式，同時傳輸資料與電力的技術，而透過射頻信號，來做身分認證為其最主要的用途，就以最普遍為人們所認知的RFID形式－非接觸式晶片卡而言，由早期的具備簡單讀卡能力或是EAS（Electronic Article Surveillance）同時具有讀與寫的能力，演變成具有加密解密功能，甚至是作業系統的能力，進而有一個小型的微控制器。RFID不論在產業界或是學術界都引起許多人的重視，主要的原因是這項技術不僅在現今社會上可改善人員管理的準確性、門禁管理的安全、倉儲管理的便利性及物流管理的迅捷性，還可以掌握即時的資訊。也因這項技術可大大改變以往的一些作業流程，使得在產業界及學術界都針對此項技術加強研究，以擴展其應用的領域，使該項技術可在更多的領域上應用。近年來，RFID應用如雨後春筍般出現，廣泛用於醫療管理、生產線自動化、圖書館管理、智慧住宅及機場行李監控等，許多公司企業願意花錢導入RFID系統、研發、投資新的RFID應用，讓我們了解RFID價值不在科技本身，而是在科技的應用。[1]

[1] 陳志憲，〈RFID 創新應用-智慧型佈告欄及匿名認證系統〉《暨南國際大學資訊管理研究所碩士論文》，民國 98 年，頁 1~2。

隨著RFID技術越來越成熟，應用也越來越多元化，相關機構跟團體也開始發現RFID這項技術所可能產生的問題。以常見的ISO14443標準為例，就有128Kbytes的容量。照道理說，以ISO14443而言，具有簡單的OS與微控制器，安全性應該是綽綽有餘，已經遠超出僅具有基本讀寫功能的非接觸式晶片卡了，然而由於RFID應用的範圍實在太大也太廣，加上遠端存取的功能，不需電力的發送信號，往往讓人於神不知鬼不覺的狀態下，洩漏了RFID內含的資料而不自知。因此，隱私的問題最被廣泛爭論，然而，只要規格符合的讀取器便可以任意讀取標籤，標籤資料的保護便顯得薄弱。另外，若資料於傳輸過程中無妥善保護或完善的存取控制，RFID標籤的特性也讓有心人士可以藉由標籤的資料來取得消費者的資訊，造成隱私的侵犯及資訊的外洩。由於RFID在許多環境裡被採用，逐漸發現有其必須解決的問題，例如：商業機密外洩、偽造虛假資訊及基礎建設遭受破壞、交易發生時的所有權移轉等問題。[2]因此，在目前系統操作上，讀取器的重要性遠比標籤重要，而且也較為昂貴，但在整個系統的運作其實皆是依賴後端資料庫伺服端來主導，所以在系統初步設計、建置及進入運作時，後端資料庫伺服端在系統中的安全防護，將是非常的重要。而如何能在系統設計階段就將此因素納入考量，使整個系統能達到服務不中斷，將是建構時的一大考量。

另外，在無線網路講求安全中，通訊雙方如果一直得透過具公信力的第三者，如認證單位或伺服端，來執行認證動作，恐會造成通訊量頻繁，除加重負載外，還容易暴露了認證單位所在，而遭不法份子攻擊，使其癱瘓無法連線運作或是被偽冒成功等等。因此，在享用其便利性的同時，無線傳輸的方式易存在資料外洩及遭竄改等風險，因為無線電波是透過空氣為媒介來進行資料的傳遞，很難防範有心人士意圖監聽、竊取資料或是偽冒等不法行為，與無線網路碰到等量的資安問題，卻無法提出相同的決解方案，這是RFID技術在發展時在資安上所面臨的一大難題。安全架構設計通常需要考量現有機構的資訊環境，就技術、花費、與管理找出較佳的解決方案。當資訊系統的使用者需要存取資料庫的資料、上線作交易或互相通訊時，可以快速以及安全地提供必要的資訊、交易或通訊服務。鑒於RFID系統的特性，在資訊安全應用侷限於提供身分證明與認證(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。不過基於以上學者所述RFID在資訊安全應用的限制和缺陷，現存的某些特性還是不符合資訊安全應用的需求。因此如何選擇合宜的技術解決方案，並在強調安全性的同時，不會妨礙或危害現有的系統，甚至造成流程變得更複雜而不易維護這是RFID系統導入的重要課題。已有多位學者提出對RFID應用安全及隱私保護的相關解決方法，[3,4]經分析探究後發現這些方法

[2] 長庚大學 RFID 物流與供應鏈資源中心，http://rfid.cgu.edu.tw/xoops/modules/tinyd3/index.php?id=3，2016/3/15。
[3] Dimitriou,T., “A lightweight RFID protocol to protect against traceability and cloning attacks,” in Proceedings of the First

均建立在可信任的第三者，如資料庫應用系統，但這些所謂的公信單位是否就真的百分之百地讓人們可以信任，也有可能遭惡意人士侵入或是偽冒仿用。因此，我們提出一方法，讓系統運作期間可以不需要後端伺服器來執行認證程序，一方面可提升系統運作效率外，另一方面可保護後端伺服器的隱私，減少遭惡意人士偵測、追蹤進而破壞之風險，以避免伺服器遭破壞而無法運作時，整個系統關閉無法正常運行。

本研究依據相關學者所提出之方法加以探討後，提出一具隱私保護之RFID自我認證機制，其方法僅運用了互斥或運算與雜湊函數，不僅可提高運作效率外，也可有效防止追蹤及重送等攻擊，能適用於計算能力較弱、記憶體容量小的被動式電子標籤。建置快速及安全的身分認證機制。本研究的預期成果為：

一、完成註冊程序的通訊雙方可不需再透過後端資料庫伺服端來執行認證作業，以達到自我認證之效。

二、設計可快速認證機制來減少在 RFID 系統運作中往返的通訊及運算量，可提升整體效率。

三、減少通訊資訊遭截取的機會，亦可提升整個運作系統之安全性。

在 RFID 相關應用中，如何維持資料在傳送過程中的安全性與個人隱私保護是極需克服的首要議題，在本文中先對 RFID 作概述介紹，繼而陳述 Dimitriou 及呂崇富等學者提出對 RFID 安全防護及個人隱私保護的研究成果。

RFID 介紹

RFID 是可以將物品透過無線射頻技術被自動偵測的技術。它的組成有電子標籤（Tag，標籤即是類似條碼的物品，是貼在物品上面的，可分成是否附加電池等三種：一種是具有電池的稱為主動式標籤，可儲存較大的記憶體及具有較遠的讀取距離，此種晶片常用於醫療產業上，但其缺點為價格較昂貴。另一種的電源是來自讀取器稱為被動式標籤，不需要電池，所以體積小、價格便宜、使用期限長，所應用的範圍較為廣大，其缺點為記憶體較小且感應距離較短。），讀取器（Reader，讀取器根據本身的頻率範圍、電源供應的方式、資料傳輸的方式、機動性等特性，可分成高頻、低頻、固定式、手持式、無線、有線這些類型的 Reader，[5]在整個系統中扮演物品與應用軟體間溝通的橋樑。主要的功能在於接收主機端的命令及標籤的資訊，並將儲存在讀取器中的資料以有線或無線方式傳送回主機，讀取器內含控制器及天線，且依其特性可分成高頻、低頻、固定式、手持式、無線及有線等。）。其工作原理即是由讀取器來讀取

International Conference on Security and Privacy for Emerging Areas in Communications Networks, 2005, pp.59- 66.

[4] 呂崇富，〈具隱私保護之 RFID 雙向鑑別機制〉《電子商務學報》，第 10 卷第 3 期，2008 年，頁 715-725。

[5] Preradovic, S., Karmakar, N.C., “RFID reader-A review,” 4th International Conference on Electrical and Computer Engineering ICECE 2006, Dhaka, Bangladesh, 2006, pp.34-43.

標籤上的資料，再將標籤上的資料傳送到後端電腦上進行運用。若與現在使用普及的條碼(Barcode)來做比較，RFID 標籤不只是可以做為商品清點時的利器，更因其擁有較大的儲存空間，可以存放更多的資訊，並且是透過無線的技術來傳輸資訊，就不用花費許多的人力及時間來一一的掃描物品。而且 RFID 技術可以一次讀取多個標籤，不像以往一次僅能讀取一個，也可以在惡劣環境下作業，遠距離的同時讀取多筆資料，還具有重複讀寫與高辨識率的優點。因此，近幾年來 RFID 的技術已廣泛地應用於門禁管制、庫儲管理、運輸應用、電子票證、防盜及發展至今的物聯網等領域。

RFID 技術的應用，不但節省了人力而且也縮短了人工辨識的時間，更大大地提昇效率，因為讀取器和標籤是透過無線通訊來傳輸貨品資訊，所以花費的時間比使用條碼的傳統作業快上十幾倍，而且 RFID 具有識別的功能，使得辨識精確度更高、驗證時間更短、作業流程也提昇改善，有效避免爭議及人為疏失。[6]其優點為利用無線電波來傳輸，可以同時且自動的讀取大量的標籤資訊，不像以往靠被動式的讀取方式，是由工作人員手持讀取設備逐一掃描清點；其次，條碼容易受到環境的影響(潮溼、灰塵…等)使得讀取設備會讀不到，而電子標籤是屬於電子產品，在條件苛刻的環境也可使用；還有一點就是，條碼與磁條所能存儲的資料較少，而電子標籤內嵌有晶片，所以資訊儲存量當然比傳統條碼大；此外，條碼與磁條的使用是一次性的，不可改變，而 RFID 尚具有重覆讀寫的特性，所以這也是會被採納的原因。[7]RFID 的種種特性已漸漸取代條碼與磁條，並且能將以往條碼與磁條所無法做到的一一實現，若能結合網路或無線網路功能更可使其優勢發揮極致，[8]表一為條碼與 RFID 功能比較表。

表一 條碼與 RFID 功能比較表

功能	可塑性	通訊距離	可讀寫	同時處理標籤數量	使用次數	穿透性	耐用性
條碼及磁條	尺寸較大且形狀固定	讀取距離較短	無法覆寫	一次讀取一筆	一次	受隔絕即無法讀取	髒污或破損無法讀取
RFID	體積小可製作成各種形狀	讀取距離較長	可重覆讀寫	同時讀取多筆	可重複使用	非金屬物質隔絕也可讀取	可在髒污環境中讀取

資料來源: 余顯強，〈無線射頻識別技術之應用與效應〉《中華民國圖書館學會會報》，第 75 期，2005 年，頁 27-36。

一、RFID 的特性

RFID特性如下：[9]

[6] 陳宏宇，《RFID 系統入門-無線射頻辨識系統》(文魁資訊，2004 年)，頁 17~22。
[7] 鄭同伯，《RFID EPC 無線射頻辨識完全剖析》(博碩文化，2004 年)，頁 54~59。
[8] 余顯強，〈無線射頻識別技術之應用與效應〉《中華民國圖書館學會會報》，第 75 期，2005 年，頁 27-36。
[9] 鄭同伯，《RFID EPC 無線射頻辨識完全剖析》，博碩文化，2004 年，頁 63~66。

(一)可重複讀寫：由於 RFID 不同於條碼不耐磨損，只要標籤外觀及內部構造正常，標籤就可依其類型來看是否能夠重複讀寫。

(二)可一次讀取多個 ：只要通過 RFID 讀取器即可不需接觸，直接將訊息由應用系統讀至資料庫內，且可一次處理多個標籤，並可將物流處理的狀態寫入標籤，以供下一階段物流處理的讀取判斷及決策之用。

(三)微型化／形狀多樣化：RFID 在讀取上並不受尺寸大小與形狀之限制，不需為了讀取精確度而配合紙張的固定尺寸和印刷品質，因此 RFID 標籤更可往小型化與多樣型態發展，以因應不同產品。目前日立（Hitachi）甚至已經發展出厚度僅有 0.1mm、面積為 0.4mm X 0.4mm 的微型 RFID 晶片，輕薄到能夠嵌入紙幣中；歐洲中央銀行甚至打算將 RFID 晶片嵌入歐元紙幣中，以防止偽鈔的橫行。

(四)耐磨損／耐環境性：紙張容易受到髒污會看不清，但 RFID 經封裝後對水、油和化學藥品等物質卻有強力的抗污性；即使 RFID 在黑暗或強光環境之中，也可以讀取資料。

(五)重複使用性：由於 RFID 為電子資料，可被覆寫，也可以回收標籤重複使用；如被動式 RFID 標籤，不需電池就可以使用，沒有維護保養的需要。

(六)非可視／穿透性：RFID 標籤若被紙張、木材和塑料等非金屬或非透明的材質包覆的話，還是能夠進行穿透性通訊。如果是金屬材質的話，就無法進行通訊，除非以特殊的方式處理標籤，才能被判讀。

二、RFID 的應用

RFID 應用範圍相當廣泛，常見的有下列各項：[10]

(一)物流：物流倉儲是 RFID 最有潛力的應用領域之一，可應用於物流過程中的貨物追蹤、信息自動採集、倉儲管理應用、港口應用、郵政包裹及快遞等。

(二)零售：可應用於商品的銷售數據實時統計、補貨及防盜等。

(三)製造業：應用於生產過程的生產數據隨時監控、品質追蹤、自動化生產及個性化生產等。

(四)服裝業：可應用於服裝的自動化生產、倉儲管理、品牌管理、單品管理及通路管理等過程。但是在應用時，必須得仔細考慮如何保護個人隱私的問題。

(五)醫療：可應用於醫院的醫療器械管理，病人身分識別等領域。

(六)身分識別：RFID 技術由於天生的快速讀取與難偽造性，而被廣泛應用於個人的身分識別證件。如現在世界各國開展的電子護照項目等其它各種電子證件。

(七)防偽：可應用於貴重物品（藥品）及票證的防偽等。

[10] 長庚大學 RFID 物流與供應鏈資源中心，http://rfid.cgu.edu.tw/xoops/modules/tinyd3/index.php?id=3，2016/3/15。

(八)資產管理：各類資產（貴重的、數量大相似性高的或危險品等）隨著標籤價格的降低，幾乎可以涉及到所有的物品。

(九)交通：高速列車、出租車管理，公車樞紐管理、鐵路火車識別等已有不少較為成功的案例，應用潛力大。

(十)食品：水果、蔬菜、生鮮及食品等保鮮度管理。

(十一) 動物識別：訓養動物、畜牧牲口、寵物等識別管理、動物的疾病追蹤及畜牧牲口的個性化養殖等。

(十二) 圖書館：書店、圖書館、出版社等應用，可大大減少書籍的盤點、管理時間，實現自動租、借及還書等功能。

(十三) 汽車：製造、防盜、定位，車鑰匙可應用於汽車的自動化、個性化生產，汽車的防盜、汽車的定位，成為安全性極高的汽車鑰匙。

(十四) 航空：飛機零件的保養及品質追蹤、旅客的機票及包裹追蹤。

(十五) 軍事：彈藥、槍支、物資、人員及車輛等識別與追蹤。

(十六) 其它：門禁、考勤、電子巡查、一卡通、消費及電子停車場等。

RFID 的問題探討

在了解RFID之基本特性以及其相關應用後，接下來我們更要了解在運用RFID後所可能衍生出的問題，根據學者專家們的研究RFID協定大致可分為以下數種問題來探討：[11,12,13]

一、保密及匿名問題

在RFID的認證過程中，標籤需傳送其ID至伺服器端作為識別之用，然而有心人士便可透過其持有之讀取器，暗中掃描標籤取得標籤資訊或追蹤此標籤之擁有者的位置。即便將ID資料加密，仍可因每次通訊的ID格式或密文相同，依舊可追蹤標籤下落。

二、阻絕服務攻擊

為了解決匿名問題，部分現有協定中，伺服器與標籤於每次通訊後皆改變共享資訊，因而在認證結束後，需同步更新伺服器與標籤資訊，防止下次通訊被有心人士追蹤。然而攻擊者卻可攔截更新信號，破壞雙方同步作業，造成伺服器資料已更新，而標籤資料卻無法更新的狀況下，被攻擊的標籤便無法再次取得伺服器的識別。

---

[11] Garfinkel, S.L., Juels, A., and Pappu, R., "RFID Privacy: An overview of problems and proposed solutions," IEEE Security and Privacy, 3(3), 2005, pp.34-43.

[12] Juels, A., "RFID Security and Privacy: A research survey," IEEE Journal On Selected Areas In Communications, 24 (2) , 2006, pp.381-394.

[13] Chen, Y.C., Wang, W.L., and Hwang, M.S., "RFID authentication protocol for anti-counterfeiting and privacy protection," IEEE, The 9th International Conference on Advanced Communication Technology,Gangwon-Do, 2007, pp. 255-259.

三、中間人攻擊

由於讀取器與標籤，為無線傳輸方式，而讀取器與伺服器間通信管道，亦可為無線傳輸。因此，攻擊者便可攔截、竄改或重送三方通信之訊息，來獲取重要資訊，假冒任何一方傳遞訊息。

四、偽造標籤

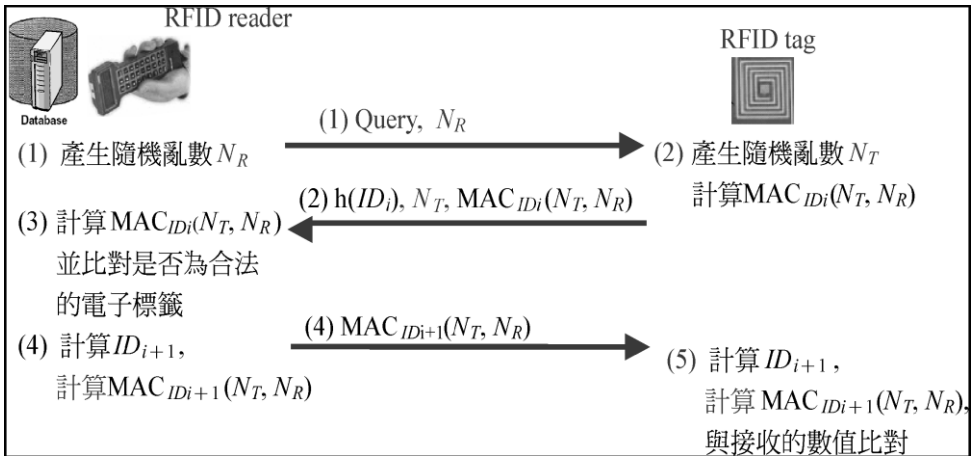
攻擊者可透過複製及蒐集，以沒有保護之標籤傳遞出的資料，重新製作偽造標籤內資訊。如將一貴重物標籤內價格或品名，置換成廉價品的價格資料。[14]

國內外研究探討

一、Dimitriou學者提出的方法

在 2005 年 Dimitriou 提出了一個讀取器與電子標籤的雙向鑑別方法，相關說明如下(運作方式如圖一)：

圖一 Dimitriou 學者所提方法



資料來源: Dimitriou,T., "A lightweight RFID protocol to protect against traceability and cloning attacks," in Proceedings of the First International Conference on Security and Privacy for Emerging Areas in Communications Networks, 2005, pp.59-66.

步驟 1：讀取器產生一個隨機亂數 N_R 後，連同詢問訊息傳送給電子標籤。

步驟 2：當電子標籤收到詢問訊息後，產生隨機亂數，然後回傳 $h(ID_i)$、N_t 及 $MAC_{IDi}(N_T,N_R)$給讀取器，其中 h()為單向雜湊函數，MAC()為訊息鑑別碼函數。

步驟 3：讀取器會將電子標籤回傳的 $h(ID_i)$、N_t 及 $MAC_{IDi}(N_T,N_R)$連同 N_R 一併送至後端資料庫應用系統，其就可以利用 $h(ID_i)$查詢到 ID_i，並進行 $MAC_{IDi}(N_T,N_R)$的計算及比對作業，如果比對相符，即可確認該電子標籤為合法的。

步驟 4：後端資料庫應用系統計算出 ID_{i+1} 以取代 ID_i 成為新的密鑰，並利用 ID_{i+1} 計算出 $MAC_{Idi+1}(N_T,N_R)$後，透過讀取器傳給電子標籤。

[14] 邱博洋，〈低成本可保隱私 RFID 認證協定之研究〉，中國文化大學資訊管理研究所碩士論文，2009 年。

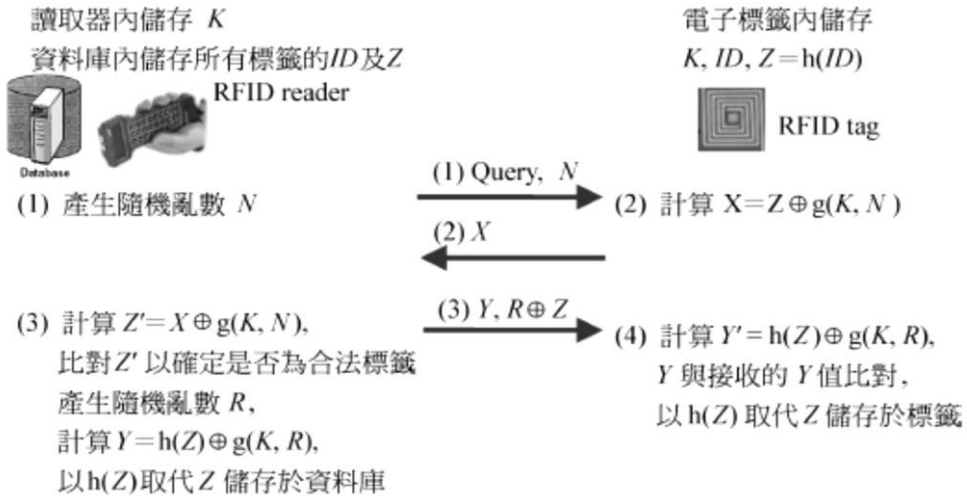
步驟 5：當電子標籤收到讀取器回傳訊息時，先計算出新的密鑰 ID_{i+1} 後，再接著計算出 $MAC_{Idi+1}(N_T,N_R)$，並與接收到的訊息進行比對，如果比對成功，則保留此訊息並刪除 ID_i 及 N_T，如果比對失敗，則刪除此訊息並保留 ID_i。

其方法中，電子標籤及讀取器於每次傳輸時均會進行雙向認證程序，但卻因為 h(IDi)與 h(IDi+1)存在著雜湊鏈(Hash Chain)的關係，面臨著追蹤分析的攻擊風險。

二、呂崇富學者提出的方法

2008 年呂崇富學者提出了一個運用互斥或運算與雜湊函數建構出具隱私保護的安全雙向認證方法，其運作方式如圖二，相關說明如下：

圖二 呂崇富學者所提方法



資料來源: 呂崇富，〈具隱私保護之 RFID 雙向鑑別機制〉《電子商務學報》，第 10 卷第 3 期，2008 年，頁 715-725。

步驟 1：讀取器產生一個隨機亂數 *N* 後，連同詢問訊息傳送給電子標籤。

步驟 2：當電子標籤收到詢問訊息後，隨即以 N 與系統密鑰 K 計算 X=Z⊕g(K,N)，並將 X 回傳給讀取器，其中 g()為單向雜湊函數。

步驟 3：讀取器收到 X 後，即算出 Z'=X⊕g(K,N)，並查詢 Z'是否儲存於後端資料庫中，如果不存在即中斷連線。如果存在，則表示該電子標籤是持有 K 的合法電子標籤，並可取得對應的 ID，隨後產生一隨機亂數 R，並計算 Y=h(Z)⊕g(K,R)，並將 Y 及 R⊕Z 回傳給電子標籤，並以 h(Z)取代 Z 儲存於資料庫中，其中 h()亦為單向雜湊函數。

步驟 4：電子標籤接收到 Y 後，利用已知的 Z 計算出 h(Z)及 R，並計算 Y'= h(Z)⊕g(K,R)，再與讀取器傳來的 *Y* 進行比對，如果不符合，就立即中斷連線，如果相符，便可確定是合法的讀取器，隨即以 h(Z)取代 Z 儲存於電子標籤中。

此方法中，不僅可以防止追蹤、複製與重送等攻擊，還具運作效率，卻因每次通訊皆

需連接到後端伺服器資料端執行驗證程序，面臨遭惡意人士偵測、追蹤進而破壞之風險，造成伺服端遭破壞而無法運作，使得整個系統關閉無法正常運行。

三、研究設計(本方法)

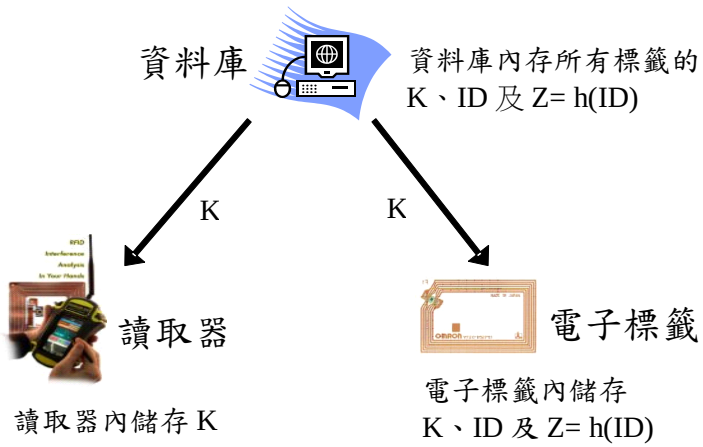
綜整學者提出 RFID 應用安全及隱私保護的相關解決方法，均採可信任的第三者，如資料庫應用系統，在公域的無線通訊環境中，所謂的公信單位也有可能遭惡意人士侵入或是偽冒仿用，因此，我們提出本方法，讓系統運作期間可以不需要後端伺服端來執行認證程序，一方面可以提升系統運作效率，另一方面可以保護後端伺服端的隱私，減少遭惡意人士偵測、追蹤進而破壞之風險，以避免伺服端遭破壞而無法運作時，整個系統關閉無法正常運行；此方法分為註冊及認證階段，分述如下：

(一)註冊階段

步驟 1：資料庫伺服端系統在有限域 Fq 上選取一條安全的橢圓曲線 E(Fq)(q 為一個 160bit 以上之大質數)並在 E(Fq)上選一階數(order)為 n 的基點 G ，使得 nG=O，其中 O 為此橢圓曲線之無窮遠點，並選擇的一個單向無碰撞雜湊函數 H( )。

步驟 2：其運作方式如圖三，相關說明如下：資料庫伺服端傳給讀取器及電子標籤系統密鑰 K。首先先行求得 K1=H(KDB),KDB 為 DB(資料庫伺服端)秘密金鑰，再產生一隨機亂數 N，最後計算出 K= (N · K1)P。

圖三 註冊階段



資料來源：作者繪製。

(二)認證階段

其運作方式如圖四，相關說明如下：

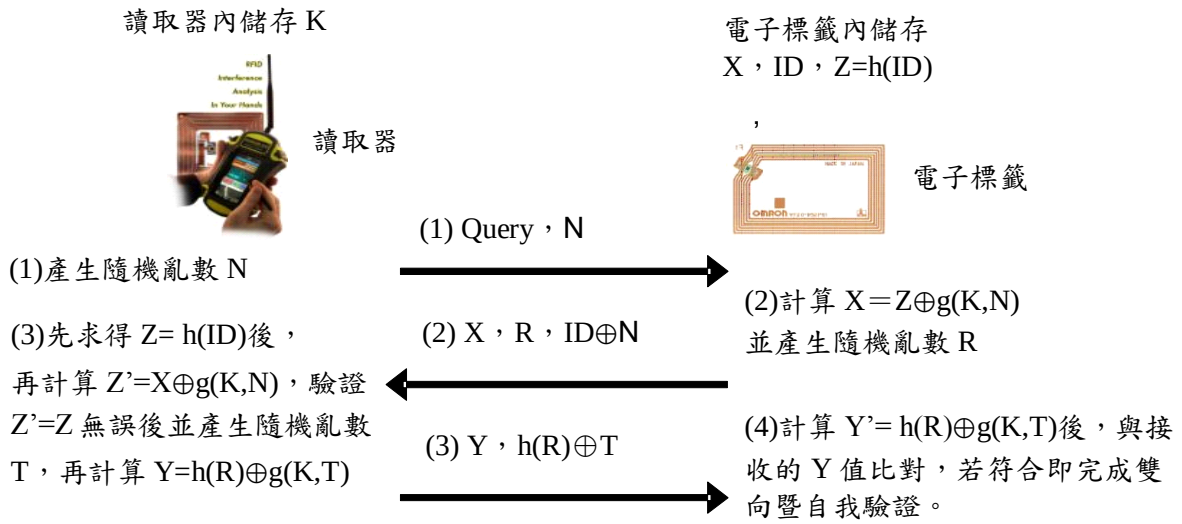
步驟 1：讀取器產生一個隨機亂數 N 後，連同詢問訊息傳送給電子標籤。

步驟 2：當電子標籤收到詢問訊息後，隨即以 N 與系統密鑰 K 計算 X=Z⊕g(K,N)後，再產生隨機亂數 R，最後將 X、R 及 ID⊕N 回傳給讀取器，其中 g()為單向雜湊函數。

步驟 3：讀取器收到參數後，先行計算出 ID 值並求得 Z=h(ID)後，再計算 Z'=X⊕g(K,N)，驗證 Z'=Z，若不符合即中斷連線，如果符合即產生一隨機亂數 T，計算出 Y=h(R) ⊕g(K,T)並將 Y 及 h(R)⊕T 回傳給電子標籤，其中 h()亦為單向雜湊函數。

步驟 4：電子標籤接收到 Y 後，可以利用已知的 R 求得 T，再計算 Y'= h(R)⊕g(K,T)，再與讀取器傳來的 Y 進行比對，如果不符合，就立即中斷連線，如果相符，便可確定是合法的讀取器，即可完成雙向暨自我認證程序。

圖四 認證階段



資料來源：作者繪製。

四、安全性分析與相關探討

本研究所提之自我認證，其安全性主要植基於橢圓曲線離散對數問題(Elliptic Curve Discrete Logarithm Problem, ECDLP)及單向雜湊函數(One-Way Hash Function, OWHF)，並且為了執行效率之考量，本研究所提出的雙向鑑別機制方法則是利用簡單的互斥或運算來建構出可以有效防止追蹤、重送及遭竄改等攻擊，以下針對相關安全性分析來進行探討：

(一)具自我認證性

身分確認性指的是可以提供線上另一使用者的確認性服務，在連線導向的傳輸中，它於建立連線過程中提供發送者或接收者的身分確認。本方法可以離線作業，在系統運作過程中，通訊雙方如果一直得透過具公信力的第三者，如：資料庫伺服端，來執行認證動作，恐會造成通訊量頻繁，除加重負載外，還容易暴露了認證單位所在，而遭不法份子攻擊，使其癱瘓無法連線運作或是被偽冒成功等等。因此，本方法設計了讀取器不需向後端資料庫伺服器連線來對欲連線端(電子標籤)進行認證程序，來達成自我認證之效。如此一來，不僅可提升系統運作效率，還可保護後端資料庫伺服端

安全，防止不法人員追蹤進行攻擊之情事。

(二)可防範不法公信單位

一直以來，我們都認為伺服端是可信任的第三者公信單位，但如果不是可信任單位呢?其有可能遭偽冒進行不法行為，因此，我們設計了一套機制，在使用者向伺服端註冊或伺服端發行公鑰或憑證給註冊者等過程中，彼此隱藏了自己本身的私鑰，這樣一來，可避免遭偽冒之險。

(三)防止資料遭竊取後分析推導的攻擊

雖然每次計算 g(K,N)及 g(K,T)均使用同樣的系統密鑰 K 值，但因亂數 N 及 T 均會隨機改變，g(K,N)及 g(K,T)亦會每次不同且無規則性，所以攻擊者無法分析推導出 g(K,N)及 g(K,T)的相關性與後續的值。而單向雜湊兼具有不可逆與碰撞無法預測之特性，攻擊者也就無法從 g(K,N)及 g(K,T)值分析推導出系統密鑰 K。

(四)防止非法電子標籤(讀取器)欺騙行為

非法電子標籤因為沒有系統密鑰 K，若想要擷取 K 而不被發現，則必須面對破解橢圓曲線離散對數問題。另外，每次通訊所需的 g(K,N)是單向雜湊函數運算出的結果，且會依隨機亂數 N 而改變。因此，非法的電子標籤不能計算出正確的 X=Z⊕g(K,N)值，也無法通過讀取器的認證。再者說到非法讀取器亦沒有系統密鑰 K，想破解亦必須面對破解橢圓曲線離散對數問題，另外亦不能獲得通訊所需 g(K,N)及 g(K,T)以致無法解讀電子標籤傳來之訊息 X=Z⊕g(K,N)亦無法計算出正確的 Y=h(R)⊕g(K,T)。因此，亦是無法通過電子標籤的認證，可以有效鑑別出合法的電子標籤及讀取器。

(五)防止電子標籤複製

讀取器每次發出詢問時都會一起送出隨機亂數 N，因此每次 X=Z⊕g(K,N)值都會因 N 值而不同。再者在最後認證程序中，讀取器送出 Y=h(R) ⊕g(K,T)給電子標籤，也因此每次 Y=h(R) ⊕g(K,T)值因 T 值而改變，所以本方法可以防止惡意人士從中利用擷取傳送之資料，進行複製合法電子標籤進而偽冒或欺騙等不法行為，也可以防止遭擷取資料後進行電子標籤複製。

(六)防止重送攻擊

在認證過程中，讀取器及電子標籤分別送出 X=Z⊕g(K,N)及 Y=h(R) ⊕g(K,T)值給對方驗證，因為每次傳送值都加入了隨機亂數，故於下次認證程序中，X 與 Y 值均與前次的值不同，所以本方法可以防止不法人士利用擷取傳送的資料進行重送攻擊。

(七)防止電子標籤及讀取器非同步攻擊

本方法會同時對電子標籤與讀取器進行雙向鑑別，確定對方的合法性後，才會將原本儲存的 Z 值以 h(R)取代。因此，攻擊者無法成功地分別對電子標籤與讀取器發動非同步攻擊。

(八)本方法預期的成效及相較表

列舉本篇方法可擁有的優點如表二，與其他學者提出方法之比較如表三。

表二 本研究預期成效一覽表

成效	說明
自我認證 (可離線作業)	完成註冊程序的通訊雙方可不需再透過後端資料庫伺服端來執行認證作業，以達到自我認證之效。
快速認證	本方法設計為利用互斥或運算與雜湊函數，可提高運作效率，來達到快速認證之效。
避免遭受欺騙、複製及重送等攻擊	安全性主要植基於橢圓曲線離散對數及單向雜湊函數難題，且加入了隨機亂數，避免中間遭人攻擊擷取讀取器或電子標籤傳送之資料，進而複製、重送及欺騙等攻擊。
提升系統運作效率及後端資料庫安全	設計可快速認證機制來減少在 RFID 系統運作中往返的通訊及運算量，可提升效率外；再者亦可減少通訊資訊遭截取的機會，以及提升整個運作系統之安全性。

資料來源：作者繪製。

表三 與各學者提出方法之比較表

比較項目	Dimitriou 學者所提方法	呂崇富 學者所提方法	本方法
隱私保護	無	有	有
雙向認證	有	有	有
自我認證	無	無	有
面臨遭追蹤分析之風險	有	無	無
電子標籤所需儲存之資料	ID 資訊	ID 資訊、1 把金鑰	ID 資訊、1 把金鑰
通訊資料量	3 回合(共計 6 筆資料)	3 回合(共計 5 筆資料)	3 回合(共計 5 筆資料)
認證程序所需演算法與函數	訊息鑑別碼函數、亂數產生器及單向雜湊函數	互斥或函數、單向雜湊函數及亂數產生器	互斥或函數、單向雜湊函數及亂數產生器

資料來源：作者繪製。

結論

隨著科技技術的日新月異，全新的資訊時代來臨，未來戰爭必然是結合情報、監視、偵察為一體，並以高科技系統、資電優勢及精準武器裝備所主宰之戰場，具有戰鬥節奏快、無固定戰線、無分前後方及後勤補給快速之特質，且講求聯合作戰型態

的戰爭。在伊拉克戰爭中，美軍利用RFID技術建置的視覺化後勤化網路，使美軍的後勤補給能力變得前所未有的強大，美軍可以輕鬆掌握所有後勤補給的即時資訊，幫助美英聯軍打倒海珊政權的關鍵成功因素之一。

後勤為運用資源，建立部隊之生存與持續戰鬥力，並支持戰爭之遂行、達成作戰目標之科學與藝術。舉凡軍隊中一切補給、維修與勤務之供應活動均屬後勤範疇，國軍後勤整備的成效及作業能力，也攸關未來作戰整體之成敗。現階段國軍目前大部分單位仍使用條碼或人工作業等方式來進行物料（流）管理或資產管理，可能會導致國軍後勤支援作業的發展面臨瓶頸，且RFID裝置在通訊過程中，相互傳遞資料的安全問題，也一直是軍方的疑慮。雖有許多根基於密碼理論的RFID身分認證機制被提出，這些方法在安全的問題上也有所改善，但是皆無法提供高傳輸效率的保障，無法有效支援作戰任務。

為此本研究提出一具隱私保護之 RFID 自我認證機制，其方法僅運用了互斥或運算與雜湊函數，此方法不僅可避免後端資料庫遭追蹤，提供了具重要地位(後端資料庫)安全的防護之特性外，並且可提高運作效率，適用於目前最普遍之計算力弱、記憶體容量小的電子標籤，可運用於如：彈藥室及軍械室進出人員之行為監控系統，以紀錄進出彈藥庫人員之行為、物資存放等識別。綜整本研究，達成貢獻如下：

(一) 建置一可快速及安全的身分認證的機制。

(二) 完成註冊程序的通訊雙方可不需再透過後端資料庫伺服端來執行認證作業，以達到自我認證之效。

(三) 設計可快速認證機制來減少在 RFID 系統運作中往返的通訊及運算量，可提升效率外；再者亦可減少通訊資訊遭截取的機會，以及提升整個運作系統之安全性。

參考文獻

一、陳志憲，〈RFID 創新應用-智慧型佈告欄及匿名認證系統〉《暨南國際大學資訊管理研究所碩士論文》，民國 98 年。

二、長庚大學 RFID 物流與供應鏈資源中心，http://rfid.cgu.edu.tw/xoops/modules/tinyd3/index.php?id=3，2016/3/15。

三、邱博洋，〈低成本可保隱私 RFID 認證協定之研究〉，中國文化大學資訊管理研究所碩士論文，2009 年。

四、呂崇富，〈具隱私保護之 RFID 雙向鑑別機制〉《電子商務學報》，第 10 卷第 3 期，2008 年。

五、陳宏宇，《RFID 系統入門-無線射頻辨識系統》，文魁資訊，2004 年。

六、鄭同伯，《RFID EPC 無線射頻辨識完全剖析》，博碩文化，2004 年。

七、余顯強，〈無線射頻識別技術之應用與效應〉《中華民國圖書館學會會報》，第 75 期，2005 年。
八、鄭同伯，《RFID EPC 無線射頻辨識完全剖析》，博碩文化，2004 年。
九、長庚大學 RFID 物流與供應鏈資源中心，http://rfid.cgu.edu.tw/xoops/modules/tinyd3/index.php?id=3，2016/3/15。
十、Garfinkel, S.L., Juels, A., and Pappu, R., “RFID Privacy: An overview of problems and proposed solutions,” IEEE Security and Privacy, 3(3), 2005.
十一、Juels, A., “RFID Security and Privacy: A research survey,” IEEE Journal On Selected Areas In Communications, 24(2), 2006.
十二、Chen, Y.C., Wang, W.L., and Hwang, M.S., “RFID authentication protocol for anti-counterfeiting and privacy protection,” IEEE, The 9th International Conference on Advanced Communication Technology, Gangwon-Do, 2007.
十三、Dimitriou,T., “A lightweight RFID protocol to protect against traceability and cloning attacks,” in Proceedings of the First International Conference on Security and Privacy for Emerging Areas in Communications Networks, 2005.
十四、 Preradovic, S., Karmakar, N.C., “RFID reader-A review,” 4th International Conference on Electrical and Computer Engineering ICECE 2006, Dhaka, Bangladesh, 2006.

作者簡介

蔡嘉富少校，中正理工學院電機系 91 年班、指參班 105 年班，曾任無線電官、資網官、副中隊長、中隊長、情報官，現任資電作戰指揮部作訓情報科參謀。

李建鵬中校，中正理工學院電機系 87 年班、國管指參班 101 年班，曾任電子官、修護長、通參官、科長、資參官、電戰官，現任國防大學國防管理學院國管中心教官。