於使用唯讀式標籤之 RFID 系統保護被連結資訊的方法

許義昌[1]、王盈文[2] 、吳建興[3*]
[1]長庚大學資訊管理學系、[2]台灣川崎汽船股份有限公司、[3]長庚大學企業管理研究所
[1]m9244107@gmail.com、[2]iris.wang215@gmail.com、[3]kenhing.wu@gmail.com

摘要

本研究提出的方法，包含一個「保護運算式」與對應的一個「回復運算式」；這兩個運算式都是在資訊系統上執行，可應用於使用唯讀式標籤之 RFID 系統中保護被連結之資訊。「保護運算式」的執行，可將「個體的識別用資料」、「連結個體之標籤的序號」、及「被授權讀取個體資訊之人員的授權碼」等三項資料轉換成一個「對應關係替代碼」，使得系統中不必記錄標籤序號與個體識別用資料之對應關係；故，僅根據標籤序號或僅根據授權碼，並無法連結到個體的識別用資料，也無法得知個體之資訊。個體的識別用資料之取得，可以使用「連結該個體之標籤的序號」、「被授權讀取該個體資訊之人員的授權碼」、及對應的「替代碼」等三項資料作為「回復運算式」之輸入，其輸出即為該個體的識別用資料；若有任一項輸入是錯誤的，就無法回復出正確的識別用資料。

關鍵詞：無線射頻識別(RFID)、資訊保護、授權、個體識別

Method for Protecting Information for Systems Connected with RFID Read-only Tags

Yi-Chang Hsu[1]、Ying-Wen Wang[2]、Chyen-Hsing Wu[3]*
[1]Department of Information Management, Chang Gung University、[2]"K"LINE (TAIWAN) LTD.、[3]The Graduate Institute of Business and Management, Chang Gung University
[1]m9244107@gmail.com、[2]iris.wang215@gmail.com、[3]kenhing.wu@gmail.com

Abstract

This study presents a “protected operation computation” corresponding to a “reverse operation computation”, both performed within data systems. Using the “protected operations computation”, “individual identifying data”, “linking of individual tag serial numbers” and “access to personal information authorization codes” to create a “substitution code”, the system needs not record the relationships between tag serial numbers and individual identifiers. Thus, since the tag serial numbers and authorization codes can’t be found in the system, even if someone gains access to tag serial numbers or authorization codes only, the

* 通訊作者 (Corresponding author.)：吳建興, kenhing.wu@gmail.com

data can't be linked to specific individuals. Acquired personal identifier data must use "links to individual tag serial numbers", "access to personal information authorization codes" and the corresponding "substitution code" as inputs for the "reverse operation computation", resulting in output of personal identifier data. If any one or more inputs for the "reverse operation computation" are incorrect, the output will not provide personal identifier data.

Keywords: RFID, Information Protection, Authorization, Identification

壹、前言

無線射頻識別(Radio Frequency Identification, RFID)技術源自 Harry Stockman 於 1948 年發表的論文：Communication by Means of Reflected Power[19]，是一種非接觸式自動識別技術，組成元件包含讀取器(reader)、電子標籤(tag)和後端資訊系統。

電子標籤是 RFID 應用系統中使用量最多的元件。無論是哪一種電子標籤，標籤內一定會寫入一個具唯一性的「標籤序號」；這個序號的編號規則通常是根據全球性標準組織所訂定之標準，例如 EPCglobal 制定的 EPC Tag Data Stabdard[3]。有些電子標籤除了存有標籤序號外，還可以再被寫入資料；若依電子標籤記憶體可讀寫的次數來區分，可分為三類：不可再寫入資料的「唯讀式(Read-Only, RO)標籤」、可再寫入一次資料的「一寫多讀(Write-Once Read-Many, WROM)標籤」和可以重複寫入資料的「可讀寫(Read/Write, RW)標籤」。

RFID 技術的發展已經有一段時間，應用在許多領域 [14][18][22][25]；其中，RFID 技術的主要效益，是提昇個體識別的效率與準確性。

RFID 應用系統建置時，必須先將人與物的資訊儲存於資訊系統中。在資訊系統中，人與物的資訊是透過多個屬性集合而成，例如由姓名、地址、性別、職業等屬性集合成一個人的資訊，又或是由名稱、材質、體積、顏色等屬性集合成一個物體的資訊，本文將人與物體通稱為「個體」，這些屬性的集合即為個體資訊。不同個體的資訊不會完全相同，一定會在某些屬性上存在差異，因此，可以依據個體屬性間的差異進行個體識別。

在識別不同個體時，可以依據某個具有唯一性的屬性來進行識別，例如在中華民國，兩個人的身分證號碼不會相同，因此身分證號碼常做為識別人的屬性，這類作為個體識別之屬性，本研究中稱為「識別用屬性」，也稱之為「識別用資料」。

常見的識別用資料有身分證號碼、病人的病歷號碼、學生的學生證號碼、商店裡的物品編號、銀行的帳號(自然人或法人的帳號)、或者是一個全球性標準組織所賦予的具唯一性之識別碼。

RFID 系統運作時，可將標籤貼附在被識別的物件上，或將標籤發給被識別的人員配載，利用標籤內具唯一性的資料作為「識別用資料」；之後，後端資訊系統接收讀取

器以非接觸的方式讀取之標籤內的「識別用資料」，進而根據「識別用資料」與「個體資訊」之關聯，即兩項資訊的「連結」(connection)關係，搜尋得到被識別之個體的資訊。

學者 Ohkubo 等人[16]指出，若 RFID 系統未經特別的設計，電子標籤內的資料可以被任意讀取，則無論被連結之個體的資訊儲存於單一個資料庫，或者分散儲存在多個資料庫，只要取得標籤內的「識別用資料」，就有可能根據識別用資料與系統存放之個體資訊的關連取得個體的資訊。目前所使用的讀取器，可以裝在手機或類似的行動裝置上使用，若將讀取器藏於衣袖，就可能不被人查覺而取得標籤內的資料；也就是說，個體資訊有可能被未經授權的人取得，產生個體資訊隱私可能被揭露的疑慮。

目前被 RFID 標籤連結之個體的資訊隱私保護，多是使用限制標籤讀取的方式[6]，或者採用具運算能力之標籤來執行密碼學方法[2]；這些技術可以滿足 RFID 系統在應用上所需要的許多安全性質，例如避免標籤內存資料被未經授權者讀取、避免標籤位置追蹤的位置隱私(location privacy)保護、標籤防偽等等；由於只有被授權者才能讀取或解讀標籤的內容，因此保護了後端資訊系統中與標籤相連結的個體相關資訊不被未經授權者取得。但是，這些技術的實施需要採用具有運算能力的標籤、特殊設計的標籤， 或是額外的設備，有較大的成本負擔。

本研究主要著眼於使用較低成本之唯讀式標籤的 RFID 系統應用情境，提出標籤內識別用資料(即標籤之序號)與後端資訊系統中之個體相關資訊的「連結關係」的方法。根據本研究之方法所建置的 RFID 系統，可以使用標籤序號來建立標籤與個體資訊間的連結關係並加以保護，且只有被授權的人才可以回復該連結；若是非授權人士讀取到標籤之序號，因為無法回復與後端資訊系統儲存之資訊之間的「連結關係」，因而難以搜尋到對應的個體資訊，在不降低個體識別效率的前提下兼顧個體資訊隱私之保護。

貳、文獻探討

在 RFID 技術的應用中，個體與其資訊之間關連的建立，是先建立個體與標籤的連結，一般可透過將標籤貼附在物件上，或是將標籤發給人員配戴之方式來建立；之後，再建立標籤與個體資訊的連結關係。

標籤與個體資訊的連結關係，主要是在標籤內寫入個體「識別用資料」，因此建立兩者的關連，由於識別用資料具有唯一性，因此可作為搜尋個體資訊的索引值；但是此方式只適用於一寫多讀或可讀寫標籤。

不論是可再寫入資料的標籤或是唯讀式標籤，其內部均具有「標籤序號」，所以可以利用「標籤序號」作為個體「識別用資料」，建立出標籤與個體資訊間的連結關係。這樣的方式可適用於各種類型的標籤。

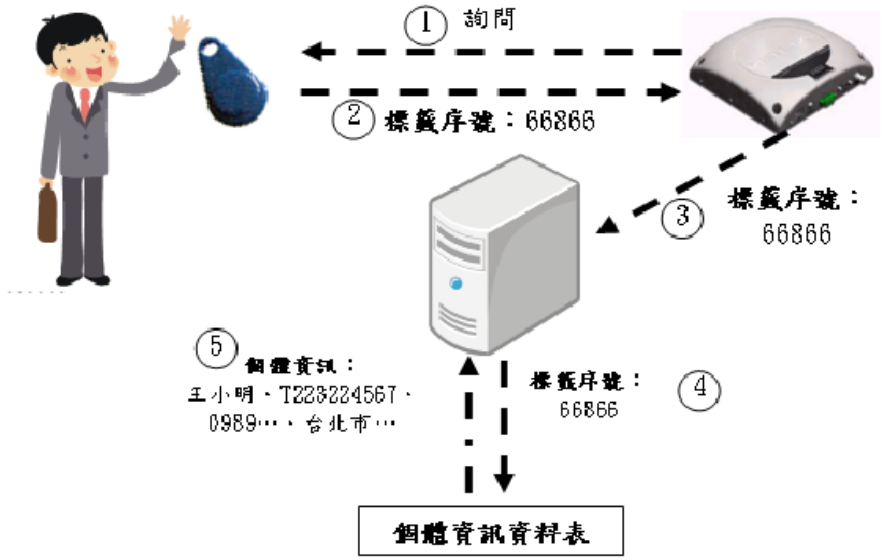
舉例來說，假設叫王O明被存放於後端資訊系統的個人資訊，包含身分證號碼、姓名、電話以及地址，如表一所示之範例；具有唯一性的身分證號碼(T223224567)作為搜

尋個體資訊的索引值，也是王小明的「識別用資料」。

表一：王小明的個人資訊

身分證號碼(識別用資料)	姓名	電話	地址
T223224567	王小明	0989…	台北市…

在應用 RFID 技術時，可讓王小明配戴一個電子標籤，如圖一；在此假設標籤之序號為 66866；由於 RFID 系統中被識別個體可能有許多，這些個體的資訊可能會儲存在一起，成為一個個體資訊資料表；只在個體資訊資料表中加入一個欄位，在該欄位中存放對應個體所配戴之標籤的標籤序號，便可建立標籤與個體資訊之間的連結；範例如表二。



標籤序號	身分證號碼(識別用資料)	姓名	電話	地址
89654	T223224567	李大大	0989....	台北市...
69315	Q458896325	徐一山	0955....	新竹市
66866	T223224567	王小明	0989....	桃園市
21058	F658452236	林小雨	0989....	基隆市
....	....	....	....	....

圖一：透過個體資訊資料表中的「標籤序號」來搜尋個體資訊

當系統接收到讀取器送來的「標籤序號」後，於關聯表中搜尋出對應的「識別用資料」，再以個體的「識別用資料」於個體資訊資料表中取得個體的資訊。此一過程如圖一之示意。

表二：RFID 後端系統中的個體資訊表

標籤序號	身分證號碼(識別用資料)	姓名	電話	地址
89654	T223224567	李大大	0989....	台北市...
69315	Q458896325	徐一山	0955....	新竹市
66866	T223224567	王小明	0989....	桃園市
21058	F658452236	林小雨	0989....	基隆市
....	....	....	....	....

現行保護電子標籤內存資料的方法，可分為三類。第一類方法是經過電路設計的特殊標籤，可以執行特定指令以保護資料不被未經授權者取得、第二類方法是透過額外的設備來防止或是干擾標籤與讀取器間的通訊，避免標籤內容被未經授權者讀取、第三類方法則是使用可以執行以密碼學為設計基礎之保護機制的電子標籤。

第一類可以執行特定指令的標籤，包括由 Auto-ID 與 EPCglobal 於 2003 年提出可以自行「銷毀」的電子標籤[6][4]。當標籤收到一個由 RFID 讀取器所傳送之「Kill」指令時，該電子標籤將會永久失效，讀取器不論對標籤下達讀取或寫入動作，標籤都不會有任何反應；並且，在讀取器下達 Kill 指令時，必須要先傳送正確的密碼給標籤，以防止攻擊者發出 Kill 指令來破壞標籤內的資料。

另有一種可以執行「休眠」功能的標籤[6][4]，其概念與上段所述類似。當支援休眠功能的標籤收到讀取器傳來的「Sleeping」指令，就會進入休眠狀態，而不再執行讀取或寫入資料的指令；與技援 Kill 指令之標籤不同的是，休眠的標籤並不會永久失效，只要收到讀取器傳送的「Wake」指令，標籤就會恢復正常運作。同樣的，為避免攻擊者下達 Sleeping 指令，標籤必須收到正確的密碼才會執行 Sleeping 指令。

第三種特殊標籤是具有比對密碼功能的標籤，它的保護機制是當讀取器對標籤下達讀取或寫入動作時，必須同時傳送存取密碼(access password)[6][4]，當標籤確認密碼正確後才會進行讀取器所下達之動作；若標籤比對密碼得到不正確的結果，就不對讀取器做出回應。

第二類採用特殊設備來干擾或阻絕讀取器與標籤之間資訊傳送的方法，例如使用法拉地籠(Faraday cage)以及使用主動干擾(active jamming)設備等[6]。

法拉地籠是由金屬網罩或金屬箔片所製成。由於金屬的靜電特性可以阻隔電磁訊號，只要將電子標籤置入法拉地籠，就能阻隔外界讀取標籤資料的訊號。

主動干擾設備是能夠發出無線射頻訊號的裝置，可以持續地發送干擾訊號給讀取器，也可使用主動廣播的方式以保護位於廣播區域內的標籤不被讀取，防止標籤內之資訊洩漏。也有一些干擾器是經過特殊設計的標籤，稱為「阻擋標籤(blocker tag)」，其用途例如消費者所購買的商品，原本可能貼有識別商品用的標籤，商家可提供嵌有阻擋標籤的專用購物袋給消費者，消費者將購買的商品放入該購物袋中，其阻檔標籤則會不斷發出訊號來混淆讀取器，使得讀取器將訊號視為不需要的資訊或是垃圾資訊而予以忽

略；因此可以保護商品上的標籤不被讀取。

除了以上的保護方式，許多學者也已提出採用可執行密碼學計算之標籤的保護方法；作為保護方法之設計基礎的密碼學方法，主要包括對稱式金鑰密碼法(Symmetric cryptography)、公開金鑰密碼法(Asymmetric cryptography)、虛擬亂數產生器(Pseudo-Random Number Generator, PRNG)，以及雜湊函數(hash function)。

Feldhofer 等人於 2003 年實作出符合 ISO/IEC 18000 標準的雙向挑戰與回應之 RFID 驗證機制[2]，並於 2004 年實作出執行此機制的硬體[10]。使用此方法時，標籤上需使用 AES(Advanced Encryption Standard)對稱式金鑰加密法進行加密，所使用的金鑰長度為 128 個位元(bit)。

德州儀器公司在 2005 年發展應用於藥品供應鏈的 RFID 驗證技術[17]，利用公開金鑰密碼法製作數位簽章並寫入標籤中，再透過驗證簽章來判別產品真偽。Juels 等人於 2003 年提出同樣運用數位簽章概念的「再加密(re-encryption)保護方法」[8]，主要是做為鈔票的辨識防偽，而且能防止鈔票的持有者被追蹤之可能；之後，Zhang 等人於 2005 年提出 Juels 之方法的改進設計[24]。

在使用虛擬亂數方面。2004 年 Molnar 等人於圖書館管理的應用情境，提出使用具備虛擬亂數產生器之標籤驗證機制[13]，以保證標籤的內容不被未經授權者得知。2005 年時，Molnar 等人提出基於虛擬亂數函數(Pseudo-Random Number Function, PRF)的保護機制[12]，使得標籤回應後端資訊系統的驗證時，每次都能以不同的假名回應，加強了資訊的保護。

在運用雜湊函數的 RFID 標籤讀取保護方法方面，2003 年 Weis 等人提出雜湊鎖定(hash-lock)的方法[23]。此方法是使用具備雜湊函數運算能力且具有記憶體空間之標籤，於標籤內之記憶體空間存放一暫時值，稱為 metaID；此 metaID 即標籤內所存放之 key 值的雜湊值，即 metalID=hash(key)。這一型式的標籤有兩種狀態：鎖定(lock)和解鎖(unlock)狀態。一開始標籤處於鎖定狀態，只會回傳 metaID 給讀取器做為索引的依據，從後端資訊系統取出對應 key 值，並將該 key 直傳送給標籤；標籤接收讀取器所傳送之 key 值後，便對接受到之 key 值進行雜湊運算，並將計算後之 key 值的雜湊值與標籤記憶體所存放的 metalID 進行比對；若比對得到相符的結果，則標籤狀態轉變為解鎖狀態，傳送標籤的序號給讀取器。

Ohkubo 等人於 2003 年提出同樣是運用雜湊函數的 RFID 標籤讀取保護方法[15]。此方法是利用兩個不同的雜湊函數 G 與 H 來保護標籤內的資訊。首先，將標籤之 ID 與對應的 key 值 Si 成對的儲存於後端資訊系統中，並在每個標籤內寫入各別的 key 值 Si，當讀取器對標籤下達讀取動作時，標籤以雜湊函數 G 對內部儲存的 Si 進行運算，得到一個雜湊值 ai，並將 ai 傳送回讀取器，並以雜湊函數 H 對 Si 進行運算，產生一個 Si 的雜湊值 Si+1，用以更新標籤內原本存放的 Si；讀取器取得 ai 後，送至後端資訊系統進行驗證，將後端資訊系統原本紀錄的標籤 ID 所對應之 Si，逐一計算 G(Hn(Si))，其中 Hn 表示連續計算 n 次雜湊函數 H，直到 G(Hn(Si))與接收的 ai 相符為止，藉此找出標籤

之 ID。

運用密碼學方法的 RFID 標籤內容保護方法眾多[1][5][7][9][11] [20][21]，不再贅言。

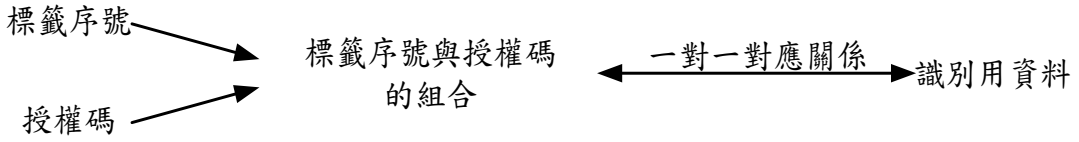
參、被標籤連結之資訊的保護方法

在本研究提出的方法中，被允許讀取的人應先通過授權驗證；這樣的設計符合現行資訊系統要求使用者進行登入驗證的作法。此授權驗證的計算完全在後端資訊系統或讀取器上執行，並不假設標籤上必須具備任何計算能力。

以下分別就保護方法的設計及使用之運算式的選擇給予說明。

3.1 保護方法的設計

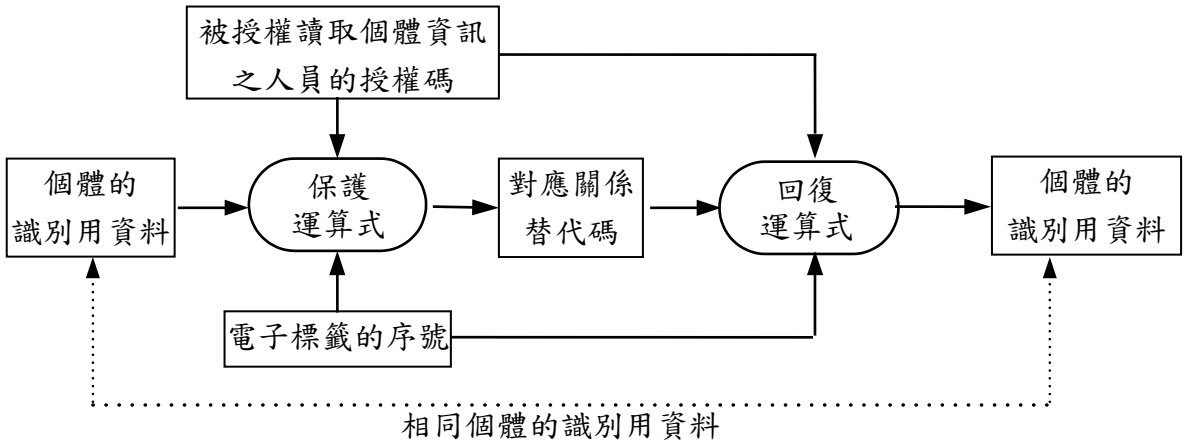
在本研究提出的方法中，被授權讀取個體相關資訊的人，必須先設定一個「授權碼」；之後，利用「授權碼」與「標籤序號」之組合，建立與個體「識別用資料」的一對一連結關係，如圖二所示的概念。換言之，必須在「正確授權碼」與「標籤序號」同時存在的情況下，才能得知所連結的「個體識別資料」。



圖二：標籤序號與授權碼的組合與識別用資料之一對一對應關係的概念圖

如此，後端資訊系統除了接收讀取器送來的「標籤序號」，也必須要求意圖讀取個體相關資訊的人輸入其「授權碼」，接著將「標籤序號」及「授權碼」進行組合，再根據上述的對應關係找到被連結之個體的「識別用資料」，便能透過所找到的識別用資料作為索引，取得被連結之個體的相關資訊。若系統根據接收的「授權碼」及「標籤序號」之組合找不到對應的「識別用資料」時，則表示讀取者並未輸入正確的「授權碼」，原因可能是讀取者並未被授權，也可能是授權者並未正確的輸入授權碼。

上段所述的「授權碼」可以是被授權的人自主選擇的，並且不能直接儲存在後端資訊系統，以避免未經授權的人即使沒有正確的授權碼，只要利用讀取器讀取「標籤序號」，仍能根據「標籤序號」與「識別用資料」的對應關係，找到被連結之個體的「識別用資料」，進而存取到個體的資訊。也就是說，組合了「授權碼」與「標籤序號」之後的資訊，它與個體「識別用資料」的對應關係必須適當的保護方式。



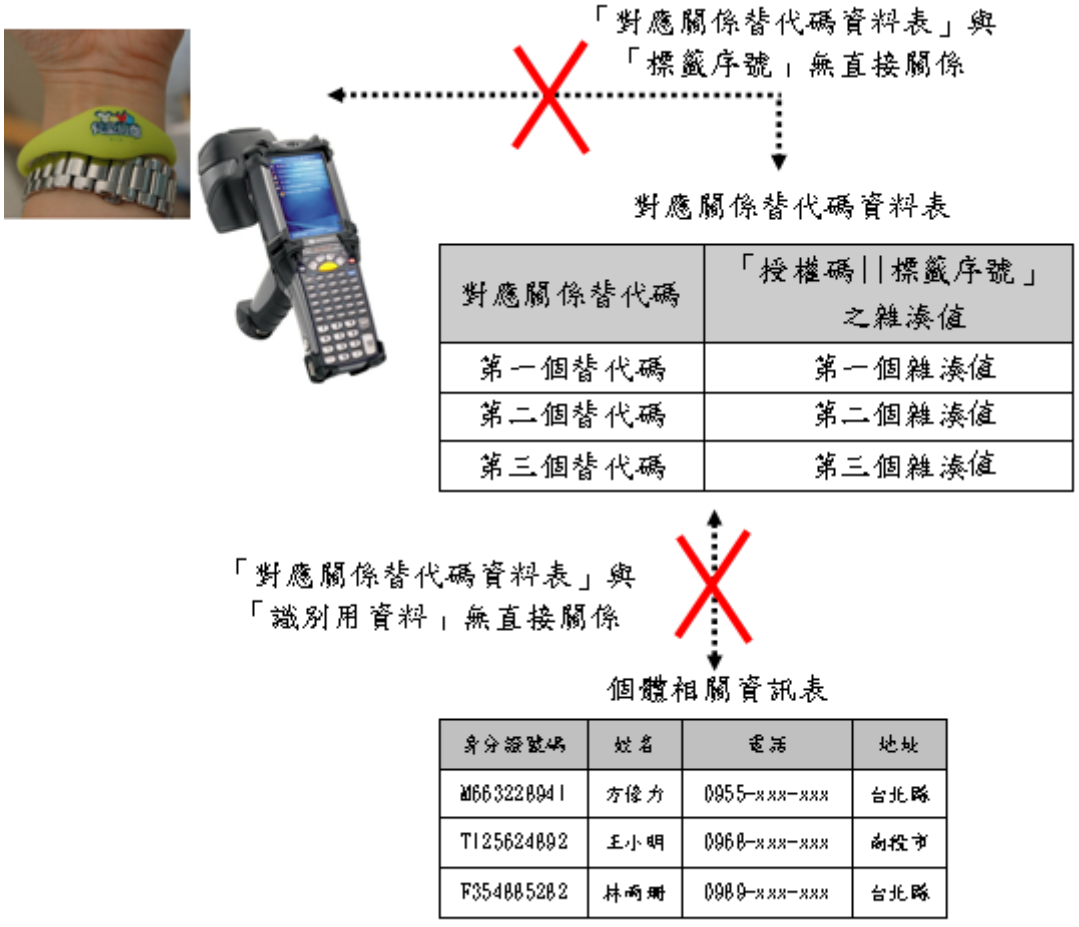
圖三：保護運算式及回復運算式之轉換關係概念圖

圖四：儲存「對應關係替代碼」之資料表與標籤和個體資訊間無直接關係

本研究的方法利用一個保護運算式來隱藏上段所述的對應關係，把原本的對應關係轉換成一個「對應關係替代碼」，之後再儲存於後端資訊系統，形成一個「對應關係替代碼資料表」。對應關係經過保護之後，後端資訊系統沒有儲存「授權碼」的需要，而

是在接收「標籤序號」及「授權碼」之後，找出配對的「對應關係替代碼」，再經過一個回復運算式來計算對應的「識別用資料」。以上概念如圖三所示。

利用保護運算式，被標籤連結之個體資訊間的對應關係轉換成一個「對應關係替代碼」。在不使用回復運算式的情形下，「對應關係替代碼」與連結該個體的「標籤序號」不存在直接的對應關係，且「對應關係替代碼」與存放個體相關資訊表中的「識別用資料」也沒有直接的對應關係，如圖四所示。



圖五：儲存「對應關係替代碼」與對應的「授權碼||標籤序號」之雜湊值資料表與標籤和個體資訊之間無直接關係

由於「對應關係替代碼資料表」中可能存在多個「對應關係替代碼」，故「回復運算式」執行之前，系統必須能根據接收到的「授權碼」及「標籤序號」來找到相關的「對應關係替代碼」作為「回復運算式」之輸入，輸出結果才會是欲識別之個體的「識別用資料」。若「回復運算式」並未使用正確的「對應關係替代碼」作為輸入，其輸出的結果雖然不是欲識別之個體的「識別用資料」，但不能排除此一輸出的結果正好與其他個體之識別資料相同，因而造成存取個體資訊的錯誤。

為解決上段所述之問題，系統每次執行「保護運算式」得到「對應關係替代碼」時，可以再將作為輸入的「授權碼」及「標籤序號」串接在一起(以「授權碼||標籤序號」表示串接之結果)，接著計算「授權碼||標籤序號」的雜湊值，並將計算所得的雜湊值與「對應關係替代碼」成對存放，如表三所示。之後，系統在執行「回復運算式」時，根據接收到的「授權碼」及「標籤序號」，可以計算得到一個雜湊值作為索引，尋找到對應的「對應關係替代碼」；若系統無法找到與該雜湊值成對儲存之「對應關係替代碼」，則不執行「回復運算式」。

表三：將「對應關係替代碼」與「授權碼||標籤序號之雜湊值」成對存放

對應關係替代碼	「授權碼||標籤序號」之雜湊值
第一個替代碼	第一個雜湊值
第二個替代碼	第二個雜湊值
第三個替代碼	第三個雜湊值
第四個替代碼	第四個雜湊值

回顧圖四，其中的「對應關係替代資料表」中只存放「對應關係替代碼」，改為成對存放「對應關係替代碼」及「授權碼||標籤序號」雜湊值之後，重新繪製如圖五所示。

3.2 「保護運算式」與「回復運算式」的公式選擇

「保護運算式」之選擇有其條件，包括(1)運算所得的「對應關係替代碼」必須不會洩漏「個體的識別用資料」、「連結個體之標籤的序號」、及「被授權讀取個體資訊之人員的授權碼」；(2)以不同的「標籤序號」、「授權碼」、及「識別用資料」作為運算式之輸入時，必須能輸出不同的「對應關係替代碼」；及(3)只取得「標籤序號」及「識別用資料」必須不會洩漏「授權碼」。

「回復運算式」之選擇也有其條件，包括(1)將輸入到「保護運算式」的「標籤序號」、「授權碼」、及「保護運算式」輸出的「對應關係替代碼」作為「回復運算式」之輸入時，「回復運算式」輸出之「識別用資料」必須與輸入到「保護運算式」的「識別用資料」相符合；及(2)只取得「標籤序號」及「對應關係替代碼」必須不會洩漏「識別用資料」。

關於「保護運算式」及對應的「回復運算式」，目前已有被公開的運算方法可供選擇，例如對稱式密碼學的 AES 加解密方法。對稱式密碼學的加解密方法具有無法從密文推導出被加密之明文及秘密金鑰的特性，且當秘密金鑰更換或明文不同時，加密計算後的密文不會相同，滿足「保護運算式」及「回復運算式」的選用條件。

我們可以利用「標籤序號」與「授權碼」之組合作為秘密金鑰來加密「識別用資料」，而加密後的密文即為「對應關係替代碼」。根據對稱式密碼學加解密方法的特性，若利

用相同的「標籤序號」與「授權碼」之組合作為秘密金鑰，則可從「對應關係替代碼」解密得到原先被加密的「識別用資料」；也就是說，對稱式密碼學的加密方法可以作為「保護運算式」，而解密方法則可作為「回復運算式」。

中華民國第 I255121 號專利「用於保護數位祕密的方法及其系統」[26]，其技術內容中包含了「數位秘密分割演算法」及對應的「數位秘密回復演算法」，也是「保護運算式」及「回復運算式」的可行選擇。根據該專利的技術內容為設計基礎，「保護運算式」表達如以下公式(1)，「回復運算式」則如公式(2)。

$$\text{對應關係替代碼} = (\text{hash}(\text{標籤序號}\|\text{授權碼}) + \alpha \times \text{識別用資料}) \bmod q \quad (1)$$

$$\text{識別用資料} = (\alpha^{-1} \times \text{對應關係替代碼} + (-(\alpha^{-1} \times \text{hash}(\text{標籤序號}\|\text{授權碼})))) \bmod q \quad (2)$$

上述兩個公式中的 hash 代表雜湊函數運算，mod 是取餘數之運算，符號 q 是大於 hash()之輸出最大值的一個正整數，符號 α 是一個與 q 互質的正整數，符號 α^{-1} 則是 α 在 mod q 運算的乘法反元素。

肆、分析與結論

本研究提出於使用唯讀式標籤之 RFID 系統保護被連結資訊的方法，所使用到的計算，皆是於系統或是具有運算力之讀取器上執行；同時，在運作上不需要於電子標籤內寫入任何資料，故可採用成本較低的唯讀式標籤，降低導入 RFID 應用的成本。

「保護運算式」與「回復運算式」為本研究所提出之方法的兩個核心。保護運算式的執行目的，是將「標籤序號」、個體的「識別用資料」以及被授權讀取者的「授權碼」等三者的連結關係轉換成一個「對應關係替代碼」，以令後端資訊系統不必存有從任何標籤序號取得對應之個體資訊的軌跡，而個體的識別用資料也無法於後端資訊系統中找到對應的標籤序號。當後端資訊系統接收到藉由電子標籤序號來請求讀取對應之個體資訊時，若作為回復運算式之輸入「標籤序號」、「對應關係替代碼」、「授權碼」有任一項是錯誤的，則無法回復出正確的「識別用資料」。

要求使用者輸入授權碼的設計，並不會增加資訊系統設計與使用的複雜度。要求使用者輸入登入系統之帳號及通行密碼(password)，以驗證使用資訊系統的權力，是常見於資訊系統的作法；因此，可以將使用者之通行密碼同時作為授權碼使用。更進一步來說，因為標籤序號係由讀取器取得，而對應關係替代碼則是依據標籤序號串接授權碼後之雜湊值作為索引而取得；若系統無法找到與該串接後雜湊值對應之替代碼，可以不必再執行回復運算式，並且可合理推論所接收的授權碼是錯誤的。也就是說，具有驗證個體資訊讀取請求者是否已被授權的效益。

以「授權碼||標籤序號」之雜湊值作為「對應關係替代碼」的索引，好處之一是雜

湊函數具有不可逆的特性，即無法由函數之輸出值推導其輸入值。因此，即使「授權碼||標籤序號」之雜湊值及「對應關係替代碼」被成對存放於一個資料表，仍然不會存在推導「授權碼」及「標籤序號」的線索。在沒有「授權碼」及「標籤序號」的情形下，入侵資料庫取得上述資料表儲存的「授權碼||標籤序號」雜湊值及「對應關係替代碼」的攻擊者，無法推導出個體的識別用資料。

雜湊函數還具有抗碰撞的特性，即不同的輸入值不易產生相同的輸出值。因此，當一位被授權之讀取者被授予讀取多個個體之資訊時，由於每一個體分別被不同的標籤所連結，即使該授權者重覆使用同一個授權碼作為保護運算式之輸入，相同的授權碼串接不同標籤序號之結果不會相同，串接結果的雜湊值也不會相同；也就是說，作為「對應關係替代碼」之索引的「授權碼||標籤序號」雜湊值發生重覆的機會微乎其微。

總結上述之說明，本研究達到的效益包含：可以在不降低個體識別效率的前提下兼顧個體資訊隱私之保護；可適用於使用唯讀式標籤的情境，具有成本上的優勢；根據本研究之方法所實作的系統，其工作流程、系統建置、系統操作、個體識別方式等，與一般的 RFID 資訊系統應無差異。

參考文獻

[1] S. Dominikus, E. Oswald and M. Feldhofer, “Symmetric Authentication for RFID Systems in Practice,” *Workshop on RFID and Lightweight Crypto*, pp. 14-15, 2005.

[2] M. Feldhofer, “A Proposal for Authentication Protocol in a Security Layer for RFID Smart Tags,” *Stiftung Secure Information and Communication Technologies SIC*, 2003.

[3] GS1, EPC Tag Data Standard, Version 1.9, Ratified, Nov-2014, http://www.gs1.org/sites/default/files/docs/epc/TDS_1_9_Standard.pdf(2017/3/2).

[4] GS1, EPC™ Radio-Frequency Identity Protocols Generation-2 UHF RFID, http://www.gs1.org/sites/default/files/docs/epc/uhfc1g2_2_0_0_standard_20131101.pdf (2017/3/3).

[5] A. Juels, “Minimalist Cryptography for Low-cost RFID Tag,” *Conference on Security in Communication Networks*, pp. 149-164, 2004.

[6] A. Juels, “RFID Security and Privacy: A Research Survey,” *IEEE J. Selected Areas in Comm.*, vol. 24, .iss 2, pp. 381-394, 2006.

[7] A. Juels, “Strengthening EPC Tags Against Cloning,” *ACM Workshop on Wireless Security*, pp.67-76, 2005.

[8] A. Juels and R. Pappu, “Squealing Euros: Privacy Protection in RFID-Enabled Banknotes,” *Proc. Financial Cryptography*, pp.103-121, 2003.

[9] S. M. Lee, Y. J. Hwang, D. H. Lee and J. I. Lim, “Efficient Authentication for Low-Cost

RFID systems," *International Conference on Computational Science and its Applications - ICCSA 2005*, pp.619-627, 2005.

[10] M. Lehtonen, T. Staake, F. Michahelles, and E. Fleisch, "From identification to authentication - a review of RFID product authentication techniques," *Workshop on RFID Security - RFIDSec 2006*, 2006.

[11] T.-L. Lim, T. Li and T. Gu, "Secure RFID Identification and Authentication Triggered Hash Chain Variants," *14th IEEE International Conference on Parallel and Distributed Systems*, pp.583-590, 2008.

[12] D. Molnar, A. Soppera and D. Wagner, "A Scalable, Delegatable Pseudonym Protocol Enabling Ownership Transfer of RFID Tags," *Selected Areas in Cryptography*, pp.276-290, 2005.

[13] D. Molnar and D. Wagner, "Privacy and Security in Library RFID: Issues, Practices, and Architectures," *Conference on Computer and Communications Security – CCS 2004*, pp.210–219, 2004.

[14] E.W.T. Ngai, K.K.L. Moon, F.J. Riggins and C.Y. Yi, "RFID research: an academic literature review (1995-2005) and future research directions," *International Journal of Production Economics*, vol. 112, pp. 510-520, 2008.

[15] M. Ohkubo, K. Suzuki and S. Kinoshita, "Cryptographic Approach to Privacy-Friendly Tags," *RFID Privacy Workshop*, 2003.

[16] M. Ohkubo, K. Suzuki and S. Kinoshita, "RFID Privacy Issues and Technical Challenges," *Communications of the ACM*, vol. 48, iss. 9, pp. 66-71, 2005.

[17] J. Pearson, "Securing the Pharmaceutical Supply Chain with RFID and Public-key Infrastructure (PKI) Technologies," *Texas Instruments White Paper*, 2005.

[18] A. Sarac, N. Absi and S. Dauzre-Prs, "A literature review on the impact of RFID technologies on supply chain management," *Int. J. Prod. Econ.*, vol. 128, pp. 77-95, 2010.

[19] H. Stockman, "Communications by means of reflected power," *Proceedings of IRE*, vol. 36, iss. 10, pp. 1196-1204, 1948.

[20] G. Tsudik, "YA-TRAP: Yet Another Trivial RFID Authentication Protocol," *International Conference on Pervasive Computing and Communications*, 2006.

[21] P. Tuyls and L. Batina, "RFID-Tags for Anti-Counterfeiting," *The Cryptographers' Track at the RSA Conference (CT-RSA)*, LNCS Vol.3860, pp.115–131, Feb 13-17, 2006.

[22] S.F. Wamba, A. Anand and L. Carter, "A literature review of RFID-enabled healthcare applications and issues," *Int J Inf Manag*, vol. 33, iss. 5, pp. 75-891, 2013.

[23] S. Weis, S. Sarma, R. Rivest and D. Engels, "Security and Privacy Aspects of Low-Cost Radio Frequency Identification Systems," *in 1st Intern. Conference on Security in*

Pervasive Computing (SPC), pp. 12-14, 2003.

[24] X. Zhang and B. King, "Integrity Improvements to an RFID Privacy Protection Protocol for Anti-Counterfeiting," *Information Security Conference*, pp. 474-481, 2005.

[25] X. Zhu, S. K. Mukhopadhyay and Kurata, H., "A review of RFID technology and its managerial applications in different industries," *J. Eng. Technol. Manag*, vol. 29, iss. 1, pp. 152-167, 2012.

[26] 黃景彰，用於保護數位祕密的方法及其系統，中華民國發明專利第 I255121 號，2006。