具有交互認證及隱私保護的無線射頻辨識系統

陳金鈴
朝陽科技大學資訊工程系助理教授
E-mail:clc@cyut.edu.tw

鄧詠元
朝陽科技大學資訊工程系研究生
E-mail:s9527625@cyut.edu.tw

摘要

無線射頻辨識系統是一個新的科技，近年來大量的應用在我們日常生活當中。無線射頻辨識系統為我們的生活增加了許多的便利，但也帶來了隱憂。由於無線射頻辨識系統是利用無線傳輸的方式，環境之中存在有心人士意圖取得無線射頻辨識標籤內的資訊，對使用者的隱私造成威脅。雖然目前有許多無線射頻辨識安全上的研究，但都無法兼顧安全性和降低資料庫的負擔。我們提出一個新的認證加密方式，利用交互認證的概念，確保標籤和讀碼器之間的傳輸是安全的，我們的方法同時也能降低資料庫的負擔。最後利用多種安全觀點來檢視我們提出的新方法，並提供此方法適用的環境。

關鍵詞：無線射頻辨識、安全、隱私、交互認證

1. 簡介

1.1 環境介紹

無線射頻辨識(Radio Frequency Identification, RFID)系統是利用無線射頻辨識標籤(tag)這個很微小的裝置來進行遠端資料的儲存和接收。無線射頻辨識系統的組成包含了標籤、讀碼器(reader)、主機、天線 [12]。在每一個無線射頻辨識物件中都有一個微小而且低成本的標籤，接受讀碼器的讀寫動作。無線射頻辨識讀碼器送出請求訊號，標籤會做出回應。標籤裡面有電子產品碼(Electric Product Code)，提供全球產品的唯一識別。

現今眾多應用二維條碼(Bar-code)系統的環境，都逐漸被無線射頻辨識系統取代，因為無線射頻辨識系統有許多特性優於二維條碼系統。無線射頻辨識系統可以在遠超過視力所及的範圍辨識，而二維條碼系統必須在非常接近、幾乎碰觸的距離才能感應。另外，無線射頻辨識系統也具備大的儲存容量，所以可以讓每個標籤具備獨一無二的唯一識別，二維條碼系統在這方面就無法辦到。所以，無線射頻辨識系統在庫存、銷售管理這方面的表現就非常出色，應用在賣場的商品結帳也可以帶來很多便利。

隨著無線射頻辨識標籤成本的降低，無線射頻辨識系統的應用也越來越廣泛，逐漸的融入了我們日常生活之中，例如出入口管制、寵物辨識、公路自動收費、工業控制、資產管理、家庭自動化等。無線射頻辨識系統由於缺乏共通的標準，而各家廠商又使用不同的運作機制，所以整合性並不理想。因為無線射頻辨識系統會對讀碼器的讀取請求做出回應，所以造成了一個潛在的危機，那就是無線射頻辨識系統的安全問題。

舉例而言，在利用無線射頻辨識的藥物管理系統中，一個病人在醫院看診後領了藥，藥品上都有內嵌無線射頻辨識標籤，當有心人士攜帶讀碼器，對藥品進行讀取的動作，那麼有心人士就可以得知該病人領了什麼藥，甚至更進一步的推斷出他所罹患的疾病。如果有人

從書店買了內嵌無線射頻辨識標籤的書籍，雖然將書籍裝進袋子裡，但只要將讀碼器靠近袋子，就可以知道袋子裡書籍的名稱，同時也得知了消費者的閱讀嗜好。

經由以上的例子我們可以發現，由於無線射頻辨識系統非接觸讀寫的特性，造成系統安全上的隱憂。一個不安全的標籤會洩漏裡面的資訊給鄰近的讀碼器，對使用者的隱私造成威脅。所以，我們透過資訊安全上互相認證的概念，設計出一個安全的存取環境，透過類似認證處理架構(Authentication Processing Framework)的方法 [5]，標籤和讀碼器都必須向資料庫註冊，標籤可以知道讀碼器是否合法，讀碼器也可以得知標籤是否有經過註冊，雙方皆為合法註冊才能進行溝通，充分保護了使用者的隱私和系統的安全。

1.2 相關研究

由以上的介紹我們可以得知，無線射頻辨識系統會被未經授權的攻擊者攻擊，造成使用者隱私的侵犯。目前，防止無線射頻辨識標籤洩漏資訊，主要有以下方式：

(1) 標籤失效(kill)方法 [1,4,5]

一個最直接保護使用者隱私的方法是在標籤交到使用者手上之前先使它失效，永遠不能再被讀取。標準的操作模式是 AutoID Center 提出的，標籤可以由一個特殊的清除指令使得讀碼器讀取標籤內容失效。此法的缺點是標籤只能使用一次。例如超市用此方法處理賣出之商品。但是很多情況下，我們希望使用者手中的標籤仍然是可操作的，因為未來很多無線射頻辨識的發展應用，都需要使用正常狀態的標籤，所以使標籤失效是不切實際的方法。

(2) 法拉第容器(faraday cage)方法 [3,4,5]

使用一個金屬網狀的容器，罩住無線射頻辨識標籤，以阻擋讀碼器發出的訊號，使無線射頻辨識標籤無法被讀碼器讀取。這裡舉個例子，小偷在賣場內將商品放到金屬製的包包內，走出賣場時就不會被感應器偵測到。這個方法雖然有效的解決有心人士非法讀取標籤的問題，但是使用上相當不方便，很難應用在大範圍的目標上。而且這方法另一個缺點是，無線射頻辨識標籤被法拉第容器罩住後，連合法的讀碼器也無法存取。

(3) 主動式人為干擾(active jamming)方法 [4,5]

使用者使用一個射頻廣播裝置，來干擾附近讀碼器的信號。當攻擊者使用非法的讀碼器企圖對無線射頻辨識標籤進行存取時，會被這個射頻廣播裝置干擾，而無法取得無線射頻辨識標籤回應的訊息。這個方法雖然能阻擋攻擊者的攻擊，但是環境中其它合法的讀碼器同樣也無法對無線射頻辨識標籤進行存取。而且廣播的功率如果太大，會造成違法的問題。另外，在某些環境，例如醫院中，使用這種裝置是相當危險的，因為它可能會干擾到其它醫療儀器的運作。

(4) 阻擋標籤(blocker tag)方法 [4,5]

此方法是指使用者攜帶一個阻擋標籤，當有讀碼器發出讀取請求時，阻擋標籤會送出假冒的訊號，使讀碼器無法取得真正無線射頻辨識標籤的資料。這個方法雖然能阻擋攻擊者的攻擊，但是同樣的也會影響到環境中其它合法無線射頻辨識標籤和讀碼器的讀取。因為讀碼器對標籤的搜尋方式是採用樹狀結構的方式，當環境中有阻擋標籤存在時，它會干擾在它之下的所有標籤節點之回應，使整個無線射頻辨識系統無法正常運作。而且這方法在某些環境中使用和主動式人為干擾方法類似，都具有危險性。

(5) 智慧型標籤方法 [4]

以上提到的幾種方式都是採用較直覺的保護方式，且使用者大多需要攜帶額外的裝置，而且這些方法都有個嚴重的缺點，那就是在阻擋攻擊者攻擊的同時，也阻礙了合法讀碼

器和標籤之間的溝通能力。另一種防止攻擊者對讀碼器或是標籤攻擊的方法就是採用加密傳輸的方式，藉由保密標籤和讀碼器之間傳輸的訊息，來達到防範攻擊者攻擊的效果。下表 1 是上述保護方式功能上的比較。

表 1　無線射頻辨識系統保護方式比較

方法 / 功能	標籤失效方法 [1,4,5]	法拉第容器方法 [3,4,5]	主動人為干擾方法 [4,5]	阻擋標籤方法 [4,5]	智慧型標籤方法[4]
避免非法的標籤存取	O	O	O	O	O
標籤仍然可以被操作	X	O	O	O	O
不影響其它讀碼器或標籤	O	O	X	X	O
合法讀碼器仍可讀取標籤	X	X	X	X	O
使用者不需要攜帶額外裝置	O	X	X	X	O

O: 此方法可以達到　X: 此方法無法達到

以下幾種方法是以智慧型標籤為基礎下，其它學者所提出的標籤和讀碼器間通訊的保護方式：

(1)　雜湊鎖(hash lock)方法 [6]

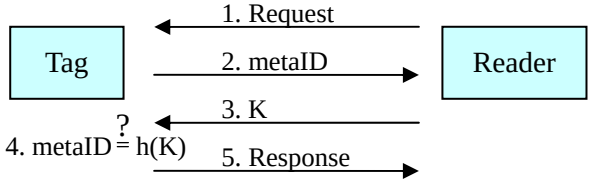

圖 1　雜湊鎖方法流程圖

上圖 1 是雜湊鎖方法的通訊流程圖，雜湊鎖方法是說當讀碼器發出一個讀取請求給標籤後，標籤會回傳一個 metaID 值給讀碼器，metaID 值是標籤和讀碼器事先約定好，使用雜湊函數對 K 運算所得到的值。讀碼器收到 metaID 值後，會在資料庫中進行搜尋，如果有找到相對應的 K 值，就會回傳給標籤。標籤在收到 K 值後，會進行 h(K)的運算，並和原來的 metaID 值比較，確認兩值是否相等。

然而在這個方法中，當攻擊者經由標籤和讀碼器間的通訊取得 metaID 和 K 值後，攻擊者就可以假冒成合法的標籤以及合法的讀碼器，來介入原本標籤和讀碼器的通訊，使訊息不再具有隱私 [7,10]。此外，因為標籤所送出的 metaID 值是固定的，所以攻擊者就算沒有取得 K 值，掌握標籤傳輸的訊息明文，也可以藉由多台讀碼器，取得相同的 metaID 回應，知道是同一標籤所發出，進一步的對標籤持有者追蹤，使用者所在的位置就被攻擊者得知，威脅到使用者的隱私。

(2)　隨機(randomized)雜湊鎖方法 [6]

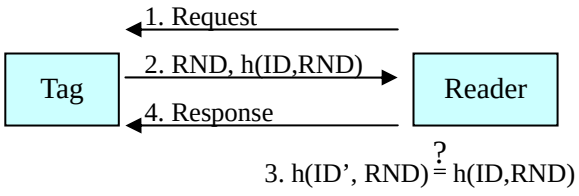

圖 2　隨機雜湊鎖方法流程圖

上圖 2 是隨機雜湊鎖方法的通訊流程圖，隨機雜湊鎖方法是指當讀碼器發出一個讀取請求給標籤後，標籤會隨機選取一個數值，並將這個隨機數值 RND 和 ID 值一起使用雜湊函數加以運算，連同選取的隨機數值一起送往讀碼器。讀碼器收到後會使用這個隨機數值和資料庫中的所有 ID 值逐一做雜湊運算，並比對是否有值和標籤傳來的雜湊值是相同

的；如果相等，讀碼器就會取出對應的 ID 值，並回應給標籤。

雖然這個方法的傳輸有加上隨機數值，但同樣也存在一些安全上的問題 [7,10]。當攻擊者假扮合法的讀碼器向標籤提出讀取請求，標籤回傳之訊息中存在未經保護的隨機數值。這時攻擊者可以攔截隨機數值，並取得讀碼器回傳標籤之確認訊息。此時，攻擊者因為已經知道隨機數值和回傳訊息，就可以對標籤進行未經授權的讀取，以往存在標籤內的資訊將不再受到保障，進一步將危害到使用者的隱私。另外，這個方法需要後端資料庫進行大量的雜湊運算來進行比對，對於整體系統效能是一種很不經濟的做法。

(3) 萬用(universal)加密方法 [8,9]

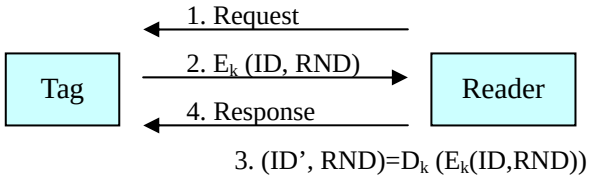

圖 3　萬用加密方法流程圖

上圖 3 是萬用加密方法的通訊流程圖，此方法是當讀碼器發出一個讀取請求給標籤後，標籤會選取一個隨機數值，並且和 ID 值一起使用事先協調好之金鑰加密，將加密後的值送往讀碼器。讀碼器收到標籤傳來的訊息後會使用金鑰解密，得到裡面存放的 ID 值，並將確認訊息用金鑰加密後送回給標籤。

這個方法使用金鑰加密，並加上隨機數值干擾，其安全性改善了，但是同樣的還是存在安全上的問題。因為此方法的金鑰是唯一的，萬一金鑰被攻擊者得知，那攻擊者就可以解開整個無線射頻辨識系統中任何標籤的訊息，對整體無線射頻辨識系統造成安全的威脅。

1.3 安全需求

一個好的無線射頻辨識系統，必須能避免系統的非法存取，造成使用者隱私的威脅，或是對系統產生安全上的危害，以下是常見的無線射頻辨識系統安全議題 [2,7,10,11]：

(1) 非法標籤存取

非法標籤存取是指攻擊者對無線射頻辨識標籤進行非法的存取動作，攻擊者持有非法的讀碼器對標籤送出查詢的指令，企圖取得標籤內敏感的資料內容。

(2) 假扮標籤攻擊讀碼器

此一安全威脅是指攻擊者對合法的讀碼器進行攻擊，攻擊者持有非法的標籤，當讀碼器需要查詢標籤時，非法的標籤傳送假冒的回應，造成讀碼器無法判別收到的訊息，癱瘓整個無線射頻辨識系統。

(3) 中間人攻擊法

攻擊者攻擊標籤和讀碼器之間的通訊，攻擊者扮演一個轉送的角色，當讀碼器要向標籤進行查詢時，攻擊者會攔截讀碼器送出的訊息，再轉送至標籤，當標籤要回應讀碼器時，攻擊者就會再次的攔截，取得標籤的訊息，再送往讀碼器，如此攻擊者就可以掌握標籤和讀碼器之間的傳輸內容。

(4) 使用者嗜好隱私

當攻擊者掌握了使用者標籤內的訊息明文，就會發生這樣的安全問題。由於標籤所送出的電子產品碼沒有經過加密，當攻擊者取得標籤所回應讀碼器的電子產品碼後，攻擊者就可以在資料庫中查詢，取得該標籤相關資料，進而對該標籤持有者的隱私造成威脅。

(5) 使用者位置隱私

這一個安全威脅是指攻擊者掌握了使用者位置的隱私，會發生這樣的安全問題是因為標籤送出的回應被攻擊者得知。雖然標籤可以傳送加密過的訊息，讓攻擊者無法取得解密後的資料，但是攻擊者可以藉由不同位置的讀碼

器對標籤的查詢，得到使用者的位置資訊。

(6) 標籤及讀碼器交互認證

攻擊者會假扮合法標籤攻擊合法讀碼器，也會假扮合法讀碼器攻擊合法標籤，所以需要交互認證來解決這個安全問題。透過認證處理架構，讀碼器以及標籤都分別向第三者註冊，合法讀碼器可以確認對象標籤是否合法，合法標籤也可以確認對象讀碼器是否合法。

2. 我們提出的方法

由於 1.2 節提及的方法[6,8,9]都存在安全上的問題，我們提出一個新的方法來改善以往方法所沒有解決的問題。我們的方法也是採用智慧型標籤的方式保護傳輸的內容，並要求標籤和讀碼器都需要向資料庫進行註冊。讀碼器必須向資料庫註冊，才能取得金鑰解開加密後的標籤訊息。標籤和讀碼器向資料庫註冊時也需要約定一個代號，約定的代號會對應到相對的金鑰，只有向資料庫註冊過的標籤和讀碼器才能互相通訊。藉由這個方式，可以達到交互認證，同時也保護了使用者的隱私。

2.1 符號

以下是我們提出的方法中會使用到的一些符號介紹：

N_i: 標籤和讀碼器分別向資料庫註冊後的代號。

$h(N_i)$: 使用雜湊函式將 N_i 進行雜湊運算。

key_i: 標籤和讀碼器分別向資料庫註冊後所取得的金鑰。

$E_{keyi}(m)$: 使用對稱金鑰 key_i 將傳輸的內容 m 加密。

$D_{keyi}(m)$: 使用對稱金鑰 key_i 將傳輸的內容 m 解密。

ID_{Ti}: 第 i 個標籤的身分識別碼。

ID_{Ri}: 第 i 個讀碼器的身分識別碼。

RND: 讀碼器產生的隨機亂數。

⊕: 互斥或閘運算。

M_{req}: 讀碼器對標籤發出的讀取請求訊息。

M_{resp}: 讀碼器送出對標籤的回應訊息。

2.2 註冊階段

在註冊的階段分成以下兩個部分來介紹，分別是標籤和資料庫註冊以及讀碼器和資料庫註冊。我們以下述步驟來說明註冊階段的流程，以及初值參數的建立。

步驟 1：每一個標籤都具有一個唯一的 ID 值，當某個標籤向資料庫註冊時，它們會約定好很多組的 N 值和金鑰，以便之後的應用。例如，i 號標籤向資料庫註冊時，告知資料庫它的 ID_{Ti} 值，資料庫就會傳回對應的 N_i 值和金鑰 key_i。其中，一個 N_i 值將只會對應到一個唯一的金鑰 key_i，每一個讀碼器也具備多組 N_i 值和金鑰 key_i，所以在標籤向資料庫註冊的同時，也代表了這個標籤將只能被某些讀碼器所讀取。標籤向資料庫註冊流程見下圖 4 所示。

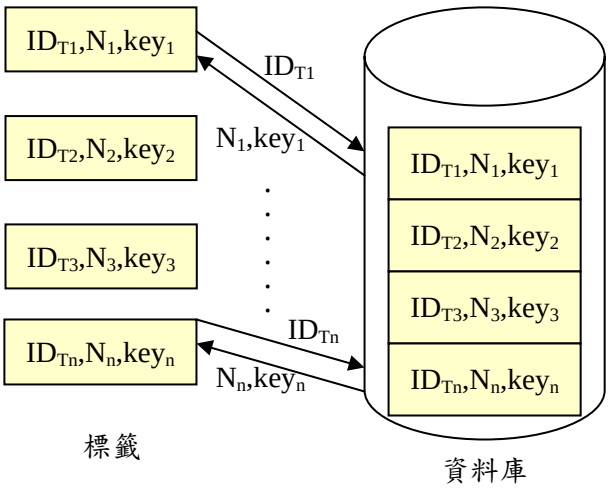

圖 4 標籤向資料庫註冊流程圖

步驟 2：每一個讀碼器具有一個唯一的 ID 值，讀碼器必須向資料庫註冊後才能對標籤進行存取。當某個讀碼器向資料庫註冊時，它們會約定可讀取標籤的 N 值和金鑰 key。例如，i 號讀碼器向資料庫註冊時，告知資料庫它的 ID_{Ri} 值，資料庫就會傳回對應的 N_i 值和金鑰 key_i。因此，該讀碼器只能讀取具備相同 N_i 值和金鑰 key_i 的標籤，所以在讀碼器向資料庫註冊的同時，也限定了該讀碼器的權限(例如可讀取的標籤)。讀碼器向資料庫註冊流程見下圖 5。

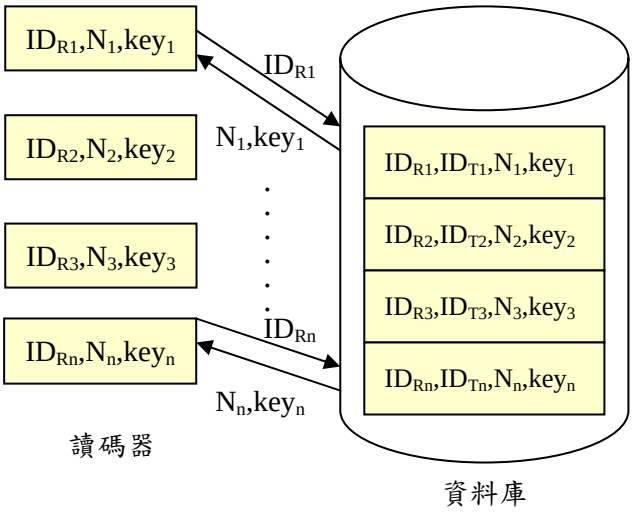

圖 5　讀碼器向資料庫註冊流程圖

2.3 通訊階段

在標籤和讀碼器透過註冊階段，都向資料庫註冊後，就可以開始互相通訊。我們提出的方法可以確保在通訊的過程中滿足許多安全方面的需求，下面就是這個新架構的通訊流程。下圖 6 為本文所提出在通訊階段的流程圖。

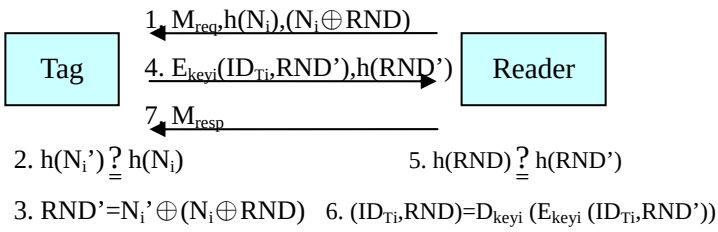

圖 6　我們的方法在通訊階段的流程圖

上面這個標籤和讀碼器的通訊流程圖表達了我們所提出的保護方式，接著就來詳細的解說每一個步驟：

步驟 1：當讀碼器要對標籤進行存取時，會送出 M_{req}、 $h(N_i)$ 和$(N_i⊕RND)$，這個訊息包含了讀取請求，使用雜湊函式保護的 N_i 值，以及將 N_i 值和讀碼器所產生的一個隨機亂數值 RND 使用互斥或閘運算後的值$(N_i⊕RND)$。其中，N_i 值是讀碼器在註冊階段和資料庫約定好的值。

步驟 2：當標籤收到讀碼器傳來的這些資訊後，會判斷 $h(N_i') \stackrel{?}{=} h(N_i)$，亦即將標籤內數個不同的 N_i 值分別使用雜湊函式運算，並和讀碼器傳來的 $h(N_i)$ 值互相比對，檢查是否有相等的值；如果有的話，就會進行後續的運算，如果沒有相等的值，則代表該讀取請求是由攻擊者或是不在允許清單內的讀碼器所發出，那麼標籤就不會再做出更進一步的運算和回應。

步驟 3：如果經過步驟 2 標籤發現有相同雜湊運算後的值，那麼標籤就會將記憶體內已知的 N_i 值和讀碼器傳來的$(N_i⊕RND)$值進行互斥或閘的運算，如此標籤就能夠取得讀碼器所選取的隨機亂數值 $RND'=N_i'⊕(N_i⊕RND)$。

步驟 4：經過步驟 3，標籤取得讀碼器選取的隨機數值之後，會將該隨機數值連同標籤的 ID_{Ti} 值使用金鑰 key_i 加密，得到 $E_{keyi}(ID_{Ti},RND')$，以及使用雜湊函式運算後的該隨機數值 h(RND')，一

起送往讀碼器。其中，加密金鑰 key_i 是標籤和資料庫在註冊階段就約定好的，一個標籤裡存有許多的 N 值，每一個 N 值對應到唯一的金鑰 key。標籤會根據讀取清單內不同讀碼器的 N_i 值，來使用不同的金鑰 key_i 加密，因為系統內有多組的金鑰 key_i，可以增加整體的安全性。

步驟 5：當讀碼器收到標籤的回應訊息後，會檢查 $h(RND) \stackrel{?}{=} h(RND')$驗證式，將先前使用的隨機數值 RND 用雜湊函式加以運算，並和標籤送來的 h(RND') 值比對，看看是否有相同的值，如果有的話，就會進行後續的運算，如果沒有相等的值，則代表該回應是由攻擊者或是不在存取清單內的標籤所送出，那麼讀碼器就不會再做出進一步的運算和回應。

步驟 6：透過註冊的階段，讀碼器和資料庫約定好金鑰 key_i，如果讀碼器能夠找出相同雜湊運算的隨機數值 RND，那麼就會進一步找出使用該隨機數值時是送出哪些的 N_i 值，並將這些 N_i 值所對應的金鑰 key_i 逐一對標籤所送來的加密訊息進行解碼，只要讀碼器找到正確的金鑰 key_i，就可以利用 key_i 解開訊息，得到標籤的 ID_{Ti} 值 $(ID_{Ti},RND)=D_{keyi}(E_{keyi}(ID_{Ti},RND'))$。

步驟 7：讀碼器已經取得了標籤的 ID_{Ti} 值，標籤的合法性已被確認，於是在讀碼器和標籤交互認證的條件下進行傳輸。

3. 安全分析

在本節中我們將針對在 1.3 節所提的安全條件做一審視分析，並與相關研究比較。

3.1 非法標籤存取分析

我們提出的方法可以避免非法的標籤存取，因為在通訊階段步驟 2 的驗證式：

$$h(N_i') \stackrel{?}{=} h(N_i)$$

標籤會逐一比對是否有任何使用雜湊運算後的標籤內所有 N 值與讀碼器送來的 $h(N_i)$值相同，如果有相同的值，標籤才會做後續的處理。攻擊者送給標籤的訊息並不會包含標籤允許的 $h(N_i)$值，所以標籤不會做出任何回應，透過這個方式，就可以避免標籤被攻擊者進行非法的存取。

3.2 假扮標籤攻擊讀碼器分析

我們提出的方法也可以避免攻擊者利用非法標籤對讀碼器進行攻擊，因為在通訊階段步驟 5 的驗證式：

$$h(RND) \stackrel{?}{=} h(RND')$$

讀碼器會將步驟 1 使用過的隨機亂數值 RND 用雜湊函式運算，並且和標籤傳來的 h(RND') 比較，看看是否相符，如果相同，才會進一步的處理。攻擊者送給讀碼器的訊息不會包含正確的隨機數值 RND'，所以讀碼器不會進行後續的運算，攻擊者無法利用這種方式癱瘓整個系統。

3.3 中間人攻擊法分析

這個攻擊方式是指攻擊者攻擊標籤和讀碼器之間的通訊，此種攻擊方式在我們提出的方法上同樣無法成功。因為由通訊階段步驟 1 的 $h(N_i)$，$(N_i \oplus RND)$和通訊階段步驟 4 的 $E_{keyi}(ID_{Ti},RND')$，h(RND')可以看出標籤和讀碼器之間關鍵的傳輸都使用了雜湊函式、互斥或閘運算或是金鑰加以保護，攻擊者無法得知

其中的訊息。另外，因為傳輸過程加入了隨機亂數 RND，讀碼器每完成一次查詢就會更換一個隨機數值 RND，增加攻擊者解碼的困難度。而且，萬一非常不幸的當某一組金鑰 key_i 被攻擊者得知，攻擊者還是無法瓦解整個系統，我們的方法可以讓系統損害降到最低。

3.4 使用者嗜好隱私分析

在保障使用者嗜好隱私這方面，我們的方法理所當然的可以滿足。透過層層的保護，攻擊者無法取得標籤內的 ID 值。因為通訊階段步驟 2 的驗證式：

$$h(N_i') \stackrel{?}{=} h(N_i)$$

攻擊者無法送出標籤允許清單內的 $h(N_i)$值，所以標籤根本不會對非法的讀碼器做出任何回應。另外，透過通訊階段步驟 4 的保護方式 $E_{keyi}(ID_{Ti},RND')$，h(RND')可以看出就算攻擊者想要從中攔截標籤送給合法讀碼器的回應訊息，也只能取得金鑰 key_i 加密後的內容，而無法得知標籤實際的 ID_{Ti} 值。

3.5 使用者位置隱私分析

即使無法取得標籤內的訊息，攻擊者還是會對使用者的位置進行追蹤，但是這點在我們提出的方法中同樣會失敗。通訊階段步驟 1 使用了雜湊函式 $h(N_i)$和互斥或閘$(N_i \oplus RND)$保護傳輸的訊息。且標籤和讀碼器每完成一次傳輸，讀碼器就會更換一個隨機亂數值 RND。所以，攻擊者就算從中攔截了標籤回應合法讀碼器的訊息，也會因為下次訊息傳輸時，讀碼器使用不同的隨機數值 RND，而讓攻擊者誤判為不同的標籤，因此攻擊者將無法鎖定使用者的位置。

3.6 標籤及讀碼器交互認證分析

我們提出的方法可以滿足標籤及讀碼器交互認證，透過通訊階段步驟 2 的驗證式：

$$h(N_i') \stackrel{?}{=} h(N_i)$$

標籤可以確認是否被合法的讀碼器讀取，沒有向資料庫註冊的讀碼器將無法讀取標籤。再由通訊階段步驟 5 的驗證式：

$$h(RND) \stackrel{?}{=} h(RND')$$

讀碼器可以確認是否是合法的標籤回應的訊息。如此一來，標籤驗證了讀碼器，讀碼器也驗證了標籤，的確滿足了標籤和讀碼器交互認證之需求。

3.7 綜合比較

綜合上述，我們將我們提出的方法和智慧型標籤機制下的相關方法，做一個比較，如表 2 所述。

表 2　智慧型標籤機制下之方法比較

方法 / 功能	雜湊鎖方法 [6]	隨機雜湊鎖法 [6]	萬用加密方法 [8,9]	我們的方法
整體安全性	低	中	中	高
資料庫負擔	中	高	低	低
攻擊者追蹤	會	不會	不會	不會
傳輸皆有保護	無	無	有	有
加密方式	雜湊	雜湊	金鑰	雜湊和金鑰
權限管理	無	無	無	有
交互認證	無	無	無	有

4. 結論

在這篇文章中，我們對於無線射頻辨識系統的標籤和讀碼器之間提供了一個安全的交互認證機制。設計一個無線射頻辨識系統，必須要有全面性的安全考量。因為無線射頻辨識系統利用無線傳輸的方式，容易遭受到許多安全方面的挑戰。之前其他學者提出的方法不是無法全面性的應付所有安全需求，就是會對資料庫造成極大的負擔。我們提出的方法可以確保標籤和讀碼器之間的傳輸是安全的，並且保障使用者的隱私不會被有心人士非法取得。

我們使用了交互認證處理架構的概念，要求標籤和讀碼器必須在離線模式先向資料庫註冊，它們才能進行傳輸的動作。在傳輸的過程中，我們的方法使用了雜湊函數和對稱式金鑰加密保護要傳輸的內容，非法的標籤或讀碼器無法得知其中的訊息明文。最後，我們使用多種安全證明觀點來檢視提出的方法，證明這個新方法的確可以解決標籤和讀碼器之間的傳輸安全問題。先前其它方法在讀碼器和標籤間的驗證，必須搜尋完整的資料庫，而本文提的方法只需搜尋少量的標籤資訊，大幅降低了資料庫的負擔。

我們提出的方法可以應用在機場的安全管理上。舉例來說，在未來利用電子護照的環境下，每一本護照上面都有無線射頻辨識標籤，每一家航空公司服務區和登機區都有讀碼器。當某甲向 A 航空公司購買機票，該航空公司會將相關資訊寫入某甲的電子護照。如果某甲欲搭乘的航班是要在 1 號登機門登機，但是某甲走到 2 號登機門，2 號登機門的讀碼器發現某甲電子護照上的無線射頻標籤內的資訊，應該要由 1 號登機門登機，就會發出通知訊息，告知某甲應進入正確的登機門。

這裡再舉另外一個例子，一間醫院裡面的病房分屬不同的樓層，同一樓層內各病房的病人又分屬不同的醫師診治。假設在醫院之中，每一位醫師和每一位樓層護士都有讀碼器，每一位病人身上的手環或病人卡都有無線射頻辨識標籤。1 號病人如果是給甲醫生醫治，並且住在 A 樓病房，那麼只有甲醫生和 A 樓層的護理人員可以讀取該病人的無線射頻辨識標籤。B 樓某病房住了 2 號病人，該病人請乙醫生作為主治醫師，那麼只有 B 樓層護理人員和乙醫生可以讀取病人的無線射頻辨識標籤。此時有一位 3 號病人，住在 B 樓病房並請甲醫生治療，同樣的只有甲醫生和 B 樓層的護理人員可以讀取該病人的無線射頻辨識標籤。透過這樣的管理方式，可以讓病人隱私得到最大的保障，本文確實能夠提供解決相關領域在實務面上碰到的問題。

參考文獻：

[1] S. E. Sarma, S. A. Weis, and D.W. Engels. “Radio-frequency identification systems”. In Burton S. Kaliski Jr., Cetin Kaya Koc, and Christof Paar, editors, CHES '02, Springer-Verlag, 2002. LNCS No. 2523, pp. 454–469.

[2] Istv’an Vajda and Levente Butty’an, “Lightweight authentication protocols for low-cost RFID tags,” 2nd Workshop on Security in Ubiquitous Computing, Seattle, Washington, USA October 12, 2003.

[3] mCloak: Personal / corporate management of wireless devices and technology, 2003. Product description at http://www.mobilecloak.com

[4] Ari Juels, Rivest RL, Szydlo M. “The blocker tag: selective blocking of RFID tags for consumer privacy”, 8th ACM Conference on Computer and Communications Security, pp. 103-111, ACM Press, 2003.

[5] John Ayoade, “Security implications in RFID and authentication processing framework”, Security Advancement Group, National

Institute of Information and Communications Technology, Japan, ELSEVIER Computers & Security, Vol. 25, No. 3, 2006, pp. 207-212.

[6] 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), Boppard, Germany, March 12-14, 2003.

[7] Tassos Dimitriou, “A Lightweight RFID Protocol to protect against Traceability and Cloning attacks”, IEEE International Conference on Security and Privacy for Emerging Areas in Communication Networks, SECURECOMM 2005.

[8] Junichiro Saito, Jae-Cheol Ryou, and Kouichi Sakurai, “Enhancing Privacy of Universal Re-encryption Scheme for RFID Tags”, L. T. Yang et al. (Eds.): EUC 2004, LNCS No.3207, pp. 879-890, 2004.

[9] Stephen A. Weis, Sanjay E. Sanma, Ronald L. Rivest, and Daniel W. Engels, “Security and Privacy Aspects of Low-Cost Radio Frequency Identification Systems”, Security in Pervasive Computing, LNCS, vol. 2802, pp. 201-212, 2004.

[10] Divyan M. Konidala, Kwangjo Kim, “Mobile RFID Security Issues”, SCIS 2006 on Hiroshima, Japan

[11] M. Ohkubo, K. Suzuki and S. Kinoshita, “Cryptographic Approach to Privacy-friendly Tags”, in RFID Privacy Workshop, MIT, 2003.

[12] Simson L. Garfinkel, Ari Juels, Ravi Pappu, “RFID Privacy: An Overview of Problems and Proposed Solutions”, IEEE Security & Privacy, 2005, pp. 34-43.