適用於群組成員不同權限等級之 RFID 安全存取控制協定

The Design of Secure RFID Access Control System with Different Authorized Group

陳育毅	詹進科	曾燕芬
國立中興大學資訊管理學系助理教授	國立中興大學資訊科學與工程學系教授兼系主任	國立中興大學資訊科學研究所研究生
E-mail: chenyuyi@nchu.edu.tw	E-mail: jkjan@cs.nchu.edu.tw	E-mail: w9556004@cs.nchu.edu.tw

摘要

最近幾年，RFID被廣泛的應用在製造業、供應鏈管理、存貨控制等各方面，因為RFID電子標籤能夠被快速及遠距批次處理的特性，提升貨品的管理效能，可以節省作業時間與成本。可是，如果RFID系統應用在個人的身分辨別，未經授權的讀取器可能非法存取電子標籤資料，這將侵犯到使用者的隱私權。在本文中，我們提出一個針對各個讀取器有不同權限之應用，讀取器權限可區分為不同群組，每一群組再分為三級－祖父級、父級與子級，父級讀取器的權限在祖父級之下，子級讀取器的權限在父級之下，並以雜湊函數運算為基礎，能保證達到相互認證、匿名性、機密性和完整性的安全RFID存取控制協定。

Abstract

RFID has been considered as a time- and money-saving solution for a wide variety of applications, such as manufacturing, supply chain management, and inventory control, etc. The major character of RFID tag can be quickly and remotely polled for batch processing. However, there are some security issues should be solved in RFID application, such as user privacy, access control, etc. In this paper, we propose a secure RFID access control protocol for different authorized readers. Our protocol guarantees the security of authentication, anonymity, confidentiality, and integrity.

關鍵詞：RFID、存取控制、授權、認證。

Key Words: RFID, access control, authorization, authentication.

一、簡介

1. RFID 的系統架構

RFID是二十一世紀最重要技術之一，它的全名是：Radio Frequency Identification 的縮寫，中文名稱為無線射頻識別，是一種運用無線射頻電波的非接觸式標籤辨識技術。典型的RFID系統由電子標籤(RF tags)、讀取器(RF readers)和後端的資料庫伺服器(Database Server)所組成，其運作原理是利用讀取器發射無線電波給電子標籤，就可以無線方式讀取電子標籤內儲存的資訊，用以辨認電子標籤所代表的物品或人員的身分。

2. RFID 的多元應用及安全性

由於RFID非接觸式無線辨識及一次讀取多個電子標籤的特性，已被廣泛應用在各領域，以RFID取代傳統條碼，有助於

提升貨品的辨識效率與供應鏈的管理效能，發展延伸的產業應用有：

- 製造業：採購品質與進貨時程追蹤、刀具模具管理、製程庫存管理、自動倉儲－入庫配送分棧、生產自動化管控。
- 運輸產業：道路橋樑收費系統、停車場收費系統、貨櫃運輸、貨櫃辨識、航空行李監控。
- 畜牧農漁業：豬牛羊漁業之管理、乳肉品監控、蔬果生長履歷資料。
- 醫療健康產業：藥品物流管理、血袋管理、醫療廢棄物追蹤、貴重儀器管制。
- 文化藝術產業：博物館文物行動導覽、圖書藝品管理。
- 零售業：即時貨物盤點、貨物追蹤管理、倉儲庫存管理、進出貨管理。

前述應用儲存在電子標籤的是貨品相關資訊，通常不需要特別考量安全的設計。但是如果RFID系統應用在個人的身分辨別，儲存的是個人資訊時，例如保全系統門禁管制、電子門票系統、醫療病歷管理、病患識別、病患接觸史追蹤，這些資料如果沒有適當的保護，可能會被非法的讀取器讀取收集資訊，或攔截電子標籤和讀取器之間的通訊，或甚至竄改電子標籤儲存的內容，就會侵犯到使用者的隱私與資料的安全。

為了保護電子標籤的資料，防止未經授權的讀取器非法存取，一般的設計會對於想要進行存取的讀取器先確認其合法性，電子標籤才回應資訊，以設限及掌控讀取器的存取行為。有關 RFID 系統的存取安全設計，已有一些機制 [4, 6, 8, 9, 12, 13, 14] 被提出如何達成安全的存取控制，可是這些機制都是假設所有合法讀取器均有相同權限，但在某些應用環境需要區隔讀取器的權限時，這些機制即不適用。

在 2006 年，John Ayoade [3] 提出這類應用環境的解決方案，例如醫院中每個住院病人都使用 RFID 電子標籤病歷卡，主治醫生為他診斷並開立處方的資訊都儲存在該電子標籤內，所以，RFID 電子標籤病歷卡內的資訊應做一定程度的保密，就算其他醫生持有合法讀取器也不能讀取，而是只有病人的主治醫生才有權限存取。針對這樣的環境 John Ayoade 提出的解決方法是在後端資料庫伺服器建立讀取器與電子標籤的權限對照表，當讀取器要讀取某個電子標籤的資訊時，電子標籤回應給讀取器其識別碼和加密的資料，讀取器再向資料庫伺服器請求解密的金鑰，而資料庫伺服器會比對權限對照表以判斷是否允許該讀取器進行解密存取，整個的互動關係如圖 1 所示。

John Ayoade 的架構，只說明大致的運作流程，並沒有設計詳細的協定細節，我們認為 RFID 系統應該要有安全的存取控制協定；再者 John Ayoade 的架構資料庫伺服器需要維護權限對照表，如果資料庫伺服器的安全控管不夠嚴謹，則權限對照表可能會被竊取或竄改，使得沒有權限的讀取器可能取得權限，因此我們認為應該排除權限對照表存在的風險，以消除 RFID 系統可能遭受的安全威脅。且在醫院的環境，一般主治醫生之下均有住院醫生及實習醫生，不同層級的醫生應有不同的存取權限，並且這些層級之間有從屬關係，住院醫生的存取權限應在主治醫生之下，實習醫生的存取權限應在住院醫生之下，才能符合實際的應用。

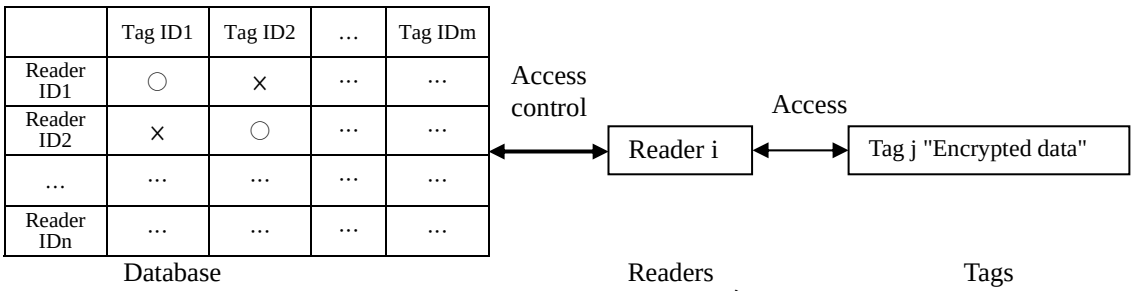

圖 1. Readers 對 tag 的存取控制

二、相關研究

基本上，我們要設計出前述應用環境的 RFID 系統之安全存取控制協定，必須考量一般低成本的 RFID 電子標籤的實際運算能力 [1, 2]：

1. 一般 RFID 被動式電子標籤是接收讀取器所傳送的磁能，轉換成電子標籤內部電路運作電能，所以電子標籤只在很短時間內具有很小的電力可以執行運算功能。
2. 一般 RFID 被動式電子標籤在成本考量下只能使用邏輯閘約為 500 至 5000 個 [13]，其中大部分用來做儲存和傳輸功能，剩下能做安全機制的運算迴路將非常有限。

既然一般的 RFID 被動式電子標籤只能在極短時間有極小電力運作，也只能加入較簡單的安全運算，所以在此限制下這類的研究 [4,5,6,7,8,9,11,12,13] 都只有考量使用雜湊函數(Hash function)與亂數產生器(Random Number Generator)，設計出如何保護通訊資料的安全與存取控制，這類安全的設計有下列幾篇最具代表性的研究：

1. Weis's hash-based access control scheme [12]：
   在 2003 年，Weis 提出以雜湊函數為基礎的存取控制技巧，電子標籤將關鍵值 key 經過雜湊函數運算的值 metaID 傳給讀取器，如果是合法的讀取器即可至後端資料庫伺服器取得符合 metaID 的關鍵值。
2. Weis's randomized access control scheme [12]：
   Weis同時提出另一種設計，將固定不變的metaID值改為加上隨機亂數r與關鍵值key_k之雜湊值，此方法比前一個方法有較好的存取控制，因為加上隨機亂數設計，非法讀取器無法判別是那一個電子標籤所傳出。
3. Gao et al.'s authentication of a "good Reader" scheme [6]：
   Gao et al.應用了要求－回應精神，當讀取器要求讀取，電子標籤傳出隨機亂數 r，合法讀取器必須通過後端資料庫伺服器的驗證，將其 ID 值與隨機亂數 r 運算的雜湊值 a(r)交由該合法讀取器回傳給電子標籤以進行合法的存取。

上述三種方法都沒有描述讀取器和資料庫伺服器如何驗證是合法讀取器，而且假設合法讀取器都可以完成協定的流程而讀取電子標籤的資料，如果直接引用上述這些方法，無法達到合法讀取器有不同權限的設計，除此之外，我們認為一個安全的存取協定在讀取器和資料庫伺服器之間應該要驗證是否為合法讀取器，並且在資料庫伺服器不要存有權限對照表以降低風險，這即是本文提出的存取協定要解決的問題。在討論我們設計的安全存取控制協定之前，先介紹其他研究認為 RFID 系統要達到安全的存取控制，基本上必須滿足下列幾個特性：相互認證 [4, 5, 8, 9, 10]、匿名性 [4, 5, 8, 9, 10]、機密性 [5, 9, 10] 和完整性 [5, 9, 10]，所以在介紹完我們的存取控制協定之後，會以這些特性來分析是否為一個好的存取控制機制。

- 相互認證(Mutual Authentication)

為防止非法讀取器欺瞞電子標籤存取相關資料，電子標籤必須能驗證讀取器是合法的讀取器才能進行存取。也就是讀取器必須能傳送可證明其合法身分的資訊給電子標籤確認，電子標籤才會回應相關資訊。而讀取器收到電子標籤回應的相關資訊，也必須能驗證是合法的電子標籤所傳送，也就是電子標籤必須傳送包含其身分識別的資訊，讀取器才能確保接收的資料是正確的。

- 匿名性(Anonymity)

電子標籤和讀取器之間的通訊，如果很容易被得知或推算出是某個電子標籤，就可能被鎖定追蹤電子標籤的位置或者被蒐集資訊提高破解的風險，因此當電子標籤和讀取器通訊時，必須達到匿名性，才不會被推測出是那一個電子標籤。

- 機密性(Confidentiality)

在 RFID 系統，電子標籤和讀取器之間的通訊資料必須是有保護的，即使被竊聽也

無法得出相關資訊；而如果電子標籤被竊取或拾獲，也無法以物理性的方法正確讀取存在電子標籤內的資料，這樣才不會洩露電子標籤儲存的資料。

- 完整性(Integrity)

電子標籤和讀取器之間的通訊可能會發生位元錯誤或被竄改，如果是位元錯誤可用總和檢查(CRCs)方式校正，而為了保證資料的正確，更必須防止被刻意竄改，如果資料有被竄改，RFID 系統必須能檢查出來，以確保資料的完整性。

三、我們設計的安全群組存取控制協定

因為電子標籤的運算資源受限制，以及有些應用環境並非所有合法的讀取器都有相同的存取權限，我們提出一個以雜湊函數運算為基礎的安全群組存取控制協定，此協定可將讀取器權限區分為不同群組，每一群組再分為三級－祖父級、父級與子級。其從屬關係譬如在醫院的環境，主治醫生之下有住院醫生，住院醫生之下有實習醫生，住院醫生的讀取器權限附屬在主治醫生之下，實習醫生的讀取器權限附屬在住院醫生之下。針對如此三級群組的不同存取權限，我們設計出在後端資料庫伺服器不需儲存權限對照表，可以保證使用者資料的隱私以及電子標籤和讀取器之間能互相驗證的安全存取控制協定，運作流程如圖 2，使用的符號如下：

- $h(\ )$：單向雜湊函數
- K_{SVR}：資料庫伺服器的秘密金鑰
- *GroupID*：每個主治醫生有不同的群組識別碼，主治醫生之下的住院醫生和實習醫生都屬於同一個群組識別碼。
- Key_{VS}：每個主治醫生都有自己的一個讀取器金鑰，由資料庫伺服器將本身K_{SVR}與*GroupID*串連，進行雜湊運算得到的值$h(K_{SVR} \| GroupID)$，事先分別存入主治醫生的讀取器和該群組讀取器有權限讀取的電子標籤內。
- Key_R：存在醫生使用讀取器的金鑰，主治醫生的是Key_{VS}，住院醫生的是$h(Key_{VS})$，實習醫生的是$h(h(Key_{VS}))$，由資料庫伺服器事先存入醫生的讀取器。因為單向雜湊函數不可逆，住院醫生無法由$h(Key_{VS})$、實習醫生無法由$h(h(Key_{VS}))$逆推得出主治醫生讀取器金鑰Key_{VS}，所以住院醫生及實習醫生都不會假冒主治醫生的身份。
- *IDflag*：讀取器身份類別，在後續的協定中，我們以"*Rdt*"代表住院醫生，"*Itn*" 代表實習醫生，同樣是由資料庫伺服器事先存入住院醫生和實習醫生的讀取器。
- *TagID*：電子標籤識別碼
- Key_T：電子標籤金鑰，由資料庫伺服器將本身K_{SVR}與*TagID* 串連，進行雜湊運算得到的值$h(K_{SVR} \| TagID)$。
- Q：讀取器隨機產生的亂數，傳給電子標籤，告知電子標籤將進行存取。
- n：電子標籤被存取過程中，會產生的隨機亂數。
- $Resp_n$：提供電子標籤驗證讀取器是否有權限讀取標籤資訊，讀取器以自己的金鑰Key_R與電子標籤傳送的亂數n做互斥或(exclusion or)運算，並進行雜湊運算得出的雜湊值$h(Key_R \oplus n)$。
- $Dtid_n$：電子標籤將其識別碼*TagID*以安全的形式傳給讀取器及資料庫伺服器，格式為$h((TagID \| Key_{VS}) \oplus n)$。
- C_{tag}：電子標籤內的資訊M均是以Key_T加密成密文$E_{KeyT}(M)$存在。在我們的協定裡面，將C_{tag}區隔成三種區塊$C1_{tag}$、$C2_{tag}$和$C3_{tag}$，$C1_{tag}$是主治醫生可以寫入的區塊，$C2_{tag}$是住院醫生可以寫入的區塊，$C3_{tag}$是實習醫生可以寫入的區塊。
- C_{KeyT}：資料庫伺服器將Key_T傳給讀取器的過程中，是以Key_R加密成密文$E_{KeyR}(Key_T)$的格式。
- H_{tag}：用來檢查讀取器異動電子標籤的更新資料是否完整正確，格式為$h((C_{tag}' \| Key_R) \oplus n)$。

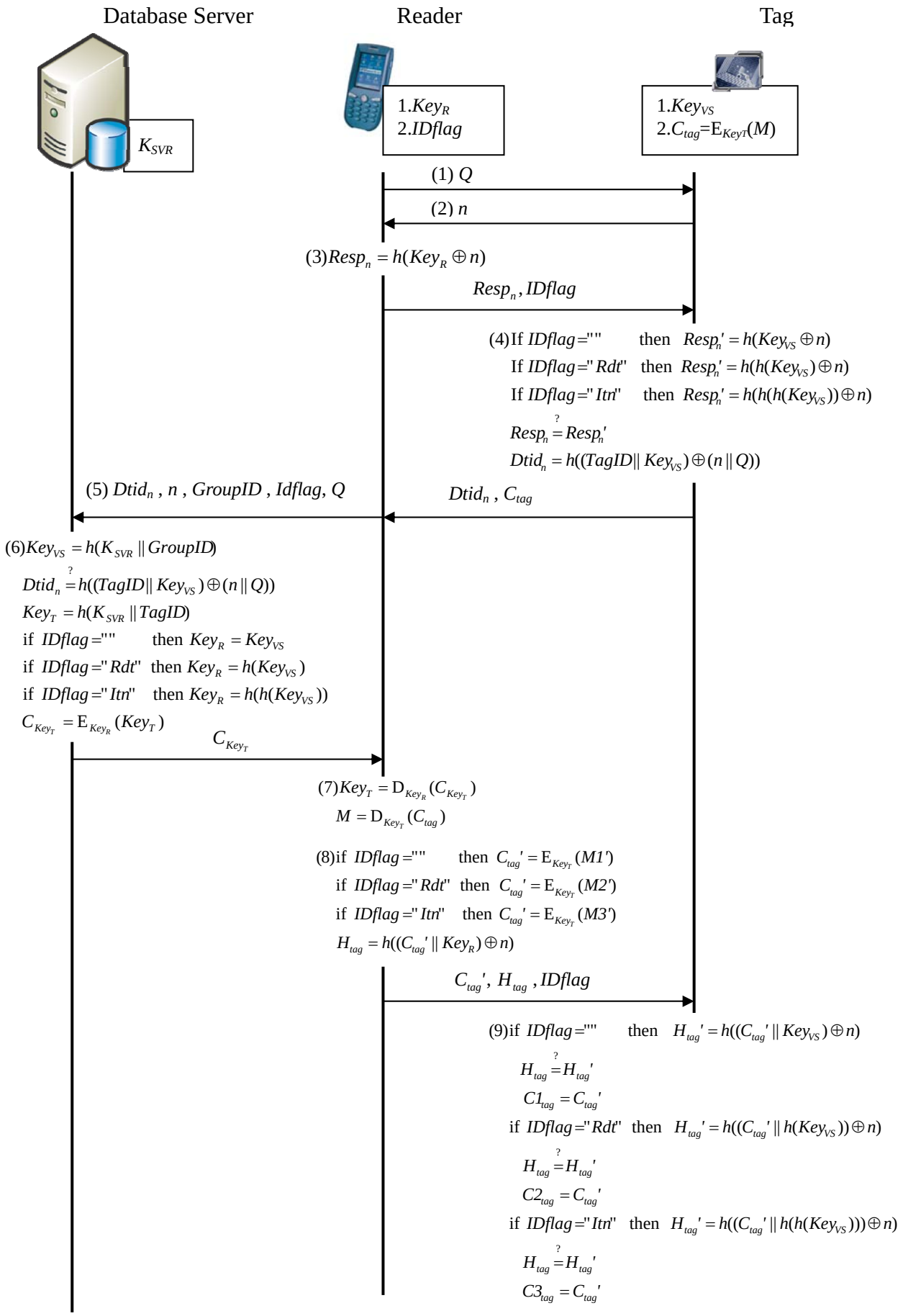

圖 2. 我們設計的安全群組存取控制協定

步驟 1. 讀取器隨機產生亂數 Q，傳給電子標籤，告知電子標籤將進行存取。

步驟 2. 電子標籤隨機產生一個亂數 n 傳給讀取器，要求讀取器回應可驗證身分的雜湊值。

步驟 3. 讀取器以自己的金鑰Key_R與亂數n做互斥或(exclusion or)運算，並進行雜湊運算得出$Resp_n$值：

$$Resp_n = h(Key_R \oplus n)$$

讀取器將$Resp_n$值與身份類別$IDflag$一同傳給電子標籤做驗證。因為單向雜湊函數不可逆，住院醫生無法由$h(Key_{VS})$、實習醫生無法由$h(h(Key_{VS}))$逆推得出主治醫生讀取器金鑰Key_{VS}，所以住院醫生及實習醫生都不會假冒主治醫生的身份。

步驟 4. 電子標籤收到$Resp_n$值與身份類別$IDflag$後，先分辨$IDflag$的值，有下列三種情況：

(1) 當$IDflag$的值為空，代表是主治醫生，電子標籤計算$Resp_n'$值如下：

$$Resp_n' = h(Key_{VS} \oplus n)$$

(2) 當$IDflag$的值為"Rdt"，代表是住院醫生，電子標籤計算$Resp_n'$值如下：

$$Resp_n' = h(h(Key_{VS}) \oplus n)$$

(3) 當$IDflag$的值為"Itn"，代表是實習醫生，電子標籤計算$Resp_n'$值如下：

$$Resp_n' = h(h(h(Key_{VS})) \oplus n)$$

電子標籤比對讀取器傳來的$Resp_n$值與本身計算的$Resp_n'$值是否相等，如果不相等，電子標籤不做任何回應；而如果相等，表示此讀取器是屬於有權限讀取其資料的群組。於是，電子標籤準備將其識別碼$TagID$以安全的形式傳給讀取器，讓讀取器能在資料庫伺服器的協助下取得可解開標籤資訊密文的Key_T。所以，電子標籤將其識別碼$TagID$、主治醫生讀取器金鑰Key_{VS}、亂數n和讀取器傳來的亂數Q做互斥或運算，並進行雜湊運算得出$Dtid_n$值：

$$Dtid_n = h((TagID \| Key_{VS}) \oplus (n \| Q))$$

電子標籤會將$Dtid_n$值與標籤資訊的密文C_{tag}一同傳給讀取器。

步驟 5. 讀取器收到$Dtid_n$後，連同前面收到的亂數n、群組識別碼$GroupID$和自己的身份類別$IDflag$以及亂數Q傳給資料庫伺服器驗證其存取權限。

步驟 6. 資料庫伺服器依據傳來的群組識別碼$GroupID$，即可連同本身的秘密金鑰K_{SVR}代入計算雜湊值得出此群組主治醫生讀取器金鑰Key_{VS}：

$$Key_{VS} = h(K_{SVR} \| GroupID)$$

於是進一步將此Key_{VS}值與亂數值n、亂數值Q，逐一與資料庫伺服器內所有的電子標籤識別碼$TagID$做互斥或並進行雜湊運算得出雜湊值，以搜尋符合$Dtid_n$的$TagID$：

$$Dtid_n \stackrel{?}{=} h((TagID \| Key_{VS}) \oplus (n \| Q))$$

若有符合的雜湊值表示此讀取器有權限存取該電子標籤的資訊，資料庫伺服器就應提供該電子標籤的金鑰給予讀取器，於是用本身的秘密金鑰K_{SVR}與電子標籤識別碼$TagID$計算雜湊值得出電子標籤金鑰Key_T：

$$Key_T = h(K_{SVR} \| TagID)$$

然後，資料庫伺服器依據讀取器傳送$IDflag$的值，計算不同等級讀取器對應的金鑰Key_R：

$$Key_R = \begin{cases} Key_{VS}, & \text{if } IDflag = "" \\ h(Key_{VS}), & \text{if } IDflag = "Rdt" \\ h(h(Key_{VS})), & \text{if } IDflag = "Itn" \end{cases}$$

接著電子標籤金鑰Key_T會以讀取器金鑰Key_R加密成C_{KeyT}，以備能安全傳送：

$$C_{Key_T} = \mathrm{E}_{Key_R}(Key_T)$$

於是，資料庫伺服器將C_{KeyT}傳給讀取器。

步驟 7. 讀取器收到C_{KeyT}後就可以自己的金鑰Key_R解出Key_T：

$$Key_T = \mathrm{D}_{Key_R}(C_{Key_T})$$

再以Key_T將C_{tag}(包含$C1_{tag}$、$C2_{tag}$、$C3_{tag}$，同一群組的醫生皆可讀取電子標籤的資訊)解密：

$$M = \mathrm{D}_{Key_T}(C_{tag})$$

於是，讀取器即可得出電子標籤的資訊M(包含$M1$、$M2$、$M3$)。

步驟 8. 如果讀取器要寫入電子標籤的資料，只能依據自己身份等級的部份寫入，譬如醫生要將新的處方寫入電子標籤內，主治醫生是寫入$M1$的內容，住院醫生是寫入$M2$的內容，實習醫生是寫入$M3$的內容。讀取器會執行下列其中一種計算：

$$C_{tag}' = \begin{cases} \mathrm{E}_{Key_T}(M1'), \text{ if } IDfilag = \text{""} \\ \mathrm{E}_{Key_T}(M2'), \text{ if } IDflag = \text{"}Rdt\text{"} \\ \mathrm{E}_{Key_T}(M3'), \text{ if } IDfilag = \text{"}Itn\text{"} \end{cases}$$

同時為確保資料完整性，讀取器會以C_{tag}'、自己的金鑰Key_R和亂數n做互斥或運算，並進行雜湊運算得出H_{tag}值：

$$H_{tag} = h((C_{tag}' \| Key_R) \oplus n)$$

讀取器將更新的資訊密文C_{tag}'和H_{tag}值以及身份類別$IDflag$，一併傳給電子標籤。

步驟 9. 電子標籤收到讀取器更新的資訊密文C_{tag}'，先分辨$IDflag$的值，依據$IDflag$值對應不同的身份等級寫入不同的資料區塊，有下列三種情況：

(1) 如果$IDflag$的值為空，代表是主治醫生，電子標籤計算H_{tag}'值如下：

$$H_{tag}' = h((C_{tag}' \| Key_{VS}) \oplus n)$$

(2) 如果$IDflag$的值為"Rdt"，代表是住院醫生，電子標籤計算H_{tag}'值如下：

$$H_{tag}' = h((C_{tag}' \| h(Key_{VS})) \oplus n)$$

(3) 如果$IDflag$的值為"Itn"，代表是實習醫生，電子標籤計算H_{tag}'值如下：

$$H_{tag}' = h((C_{tag}' \| h(h(Key_{VS}))) \oplus n)$$

電子標籤比對收到的H_{tag}值與H_{tag}'值是否相等，若兩個值一樣，表示從讀取器傳送過來的資訊密文C_{tag}'是完整且正確的，而且是由認證的讀取器所傳送，所以如果是主治醫生，電子標籤才會將$C1_{tag}$異動為C_{tag}'；如果是住院醫生，電子標籤才會將$C2_{tag}$異動為C_{tag}'；如果是實習醫生，電子標籤才會將$C3_{tag}$異動為C_{tag}'。

四、安全性分析

根據第二節介紹過的 RFID 相關研究[4, 5, 8, 9, 10]，我們知道 RFID 系統要達到安全的存取控制，必須滿足相互認證、匿名性、機密性和完整性，以下即針對這些特性來分析我們設計的存取控制協定。

- 相互認證(Mutual Authentication)

為了防止非法讀取器存取電子標籤相關資料，電子標籤必須有能力確認讀取器是否屬於有權限讀取其資料的群組。在我們設計的存取控制協定採用要求－回應(challenge-response)精神，在步驟 2，電子標籤會傳送一個亂數n給讀取器，以要求讀取器回應可驗證身分的雜湊值。而在步驟 3，讀取器必須以自己的金鑰Key_R計算出下列的回應值$Resp_n$：

$$Resp_n = h(Key_R \oplus n)$$

然後讀取器將$Resp_n$值與身份類別$IDflag$一同傳給電子標籤，所以在步驟 4，電子標籤即可依據$IDflag$的值，以事先儲存有權限存取其資料的主治醫生讀取器金鑰Key_{VS}，做同樣的運算得出$Resp_n'$值：

(1) 如果 $IDflag$ 的值為空，則：

$$Resp_n' = h(Key_{VS} \oplus n)$$

(2) 如果 $IDflag$ 的值為"Rdt"，則：

$$Resp_n' = h(h(Key_{VS}) \oplus n)$$

(3) 如果 $IDflag$ 的值為"Itn"，則：

$$Resp_n' = h(h(h(Key_{VS})) \oplus n)$$

電子標籤比對$Resp_n$值與自己計算的$Resp_n'$值，若兩者一致，電子標籤即可確

認該讀取器是屬於有權限讀取其資訊之合法讀取器的群組。

電子標籤必須確認讀取器是合法之後，才會傳出身分識別的相關資訊，以避免電子標籤的資訊被擷取，這樣的設計才能真正達到互相認證之目的。在我們的設計，步驟 4 電子標籤會傳遞隱含識別碼的$Dtid_n$值給讀取器和資料庫伺服器：

$$Dtid_n = h(TagID \| Key_{VS} \oplus (n \| Q))$$

在步驟 6，資料庫伺服器收到$Dtid_n$值，逐一將所有的電子標籤識別碼$TagID$做同樣的運算，以搜尋符合$Dtid_n$的$TagID$：

$$Dtid_n \stackrel{?}{=} h(TagID \| Key_{VS} \oplus (n \| Q))$$

若有符合的雜湊值，資料庫伺服器即可確認此電子標籤有事先存入的主治醫生讀取器金鑰，是由其所核發的。

因此，電子標籤可從$Resp_n$值確認讀取器為合法的讀取器，而資料庫伺服器可由$Dtid_n$值確認電子標籤是由其所核發，即可達到電子標籤和讀取器與資料庫伺服器之間的相互認證。

上述設計之目的即可避免可能的第三者惡意攻擊，假設，有攻擊者想假冒合法的讀取器欺瞞電子標籤，因為攻擊者沒有金鑰Key_R，無法計算出正確的$Resp_n$值回應給電子標籤比對，電子標籤並不會回傳任何資訊；如果攻擊者要利用攔截的$Resp_n$值做為日後假冒讀取器之用，幾乎是不可能的，因為亂數n是由電子標籤決定，正確的回應值$Resp_n$並非固定的，所以攻擊者無法假冒合法的讀取器在下一次通訊時重複傳送攔截的$Resp_n$值；再者$Resp_n$是雜湊值，單向雜湊涵數是不可逆的，攻擊者亦無法從$Resp_n$逆推出金鑰Key_R。

相對的，如果有攻擊者想假冒電子標籤傳送錯誤的資訊給讀取器，它所傳出的$Dtid_n$值必須包含Key_{VS}和讀取器傳來的亂數Q，才能通過資料庫伺服器的核對，但是攻擊者沒有金鑰Key_{VS}，無法傳出正確的$Dtid_n$值，就無法通過資料庫伺服器的核對；如果攻擊者要利用攔截的$Dtid_n$值做為日後假冒電子標籤之用，也幾乎是不可能的，因為亂數Q是由讀取器決定，正確的回應值$Dtid_n$並非固定的，因此攻擊者無法假冒合法的電子標籤在下一次通訊時重複傳送攔截的$Dtid_n$值；再者$Dtid_n$是雜湊值，單向雜湊涵數是不可逆的，攻擊者亦無法從$Dtid_n$逆推出金鑰Key_{VS}。

所以，在我們的設計中，能夠防止攻擊者假冒合法的讀取器欺瞞電子標籤讀取相關資訊，以及攻擊者假冒電子標籤傳送錯誤的資訊給讀取器，有效預防竊聽和截取風險(Eavesdropping and Intercepting Risks)、重送攻擊(Replay attacks)與中間人攻擊(Man-in-the-middle attacks)。

- 匿名性(Anonymity)

為了降低電子標籤被蒐集資訊提高破解的風險，當電子標籤和讀取器通訊時，必須達到匿名性，亦即電子標籤的識別碼不能明明白白的傳出，才不會被破解是那一個電子標籤。而我們的設計，就是在步驟 4 不直接傳遞電子標籤的識別碼$TagID$，而是傳遞隱含識別碼的$Dtid_n$值：

$$Dtid_n = h((TagID \| Key_{VS}) \oplus (n \| Q))$$

因為電子標籤有亂數產生器，每次通訊都會選擇不同的亂數n，它傳給讀取器的$Dtid_n$值加入亂數n，使得每次通訊時電子標籤傳出的$Dtid_n$值都不一樣，電子標籤與讀取器的通訊就不容易被鎖定蒐集其資訊，竊聽者也無法得知是那一個電子標籤和讀取器通訊，所以可達到匿名性的要求。

- 機密性(Confidentiality)

電子標籤和讀取器之間的通訊資料必須保護，才不會被攔截或竊聽而洩漏電子標籤儲存的資料，在我們的設計步驟 4，電子標籤傳給讀取器的資訊，以及步驟 8，讀取器如果有必要異動電子標籤的資料，都有考量加密的設計，以保護電子標籤和讀取器之間的通訊。

在步驟 4，電子標籤既存的資料是的密文C_{tag}，這些資料直接傳給讀取器，即使通訊資料被攔截，任何人沒有金鑰Key_T，即無法解開C_{tag}內容。

在步驟 8，如果讀取器要異動電子標籤的資料，其在步驟 6 已經由資料庫伺服器取得金鑰Key_T，所以在步驟 8 就可以將異動的資料M' 以金鑰Key_T加密成密文C_{tag}'：

$$C_{tag}' = \mathrm{E}_{Key_T}(M')$$

C_{tag}'傳送寫入電子標籤過程中就算被攔截，任何人沒有金鑰Key_T，即無法解開C_{tag}'內容。

更進一步來說，即使電子標籤被竊取或拾獲，因為電子標籤存放的是密文C_{tag}，所以沒有金鑰Key_T，是無法解開C_{tag}內容。

所以，在我們的設計中，電子標籤和讀取器之間的通訊資料，是以具有一定安全程度的對稱式加密法加密保護的，能夠預防被攻擊者竊聽和截取風險，可達到資料機密性的要求。

- 完整性(Integrity)

為了防止電子標籤和讀取器之間的通訊發生位元錯誤，通常會用總和檢查碼(CRCs)方式校正，在我們的設計步驟1～4，可額外加入這樣的機制，因為讀取器會將標籤資訊解密，如果通訊有位元錯誤，使用總和檢查碼方式即可校正。而在步驟 8，讀取器傳給電子標籤更新的資訊是密文，電子標籤不進行解密檢視明文內容，這裡若只用總和檢查碼是無法確認可能發生的資料竄改或傳輸錯誤，所以在我們的設計，除了傳送更新的資訊密文C_{tag}'之外，還以單向雜湊函數運算出下列的檢查值H_{tag}：

$$H_{tag} = h(C_{tag}' \| Key_R \oplus n)$$

然後，讀取器將更新的資訊密文C_{tag}'、H_{tag}與身份類別*IDflag*值一併傳給電子標籤，如此在步驟 9，電子標籤即可依據*IDflag*的值，以主治醫生讀取器金鑰Key_{VS}做同樣的運算得出H_{tag}'值：

(1) 如果 *IDflag* 的值為空，則：
$$H_{tag}' = h((C_{tag}' \| Key_{VS}) \oplus n)$$
(2) 如果 *IDflag* 的值為"*Rdt*"，則：
$$H_{tag}' = h((C_{tag}' \| h(Key_{VS})) \oplus n)$$
(3) 如果 *IDflag* 的值為"*Itn*"，則：
$$H_{tag}' = h((C_{tag}' \| h(h(Key_{VS}))) \oplus n)$$

電子標籤比對收到的H_{tag}值與H_{tag}'值是否相等，若兩個值一樣，表示從讀取器傳送過來的更新資訊密文C_{tag}'是完整且正確的，而且是由認證的讀取器所傳送。因為單向雜湊函數不可逆，如果H_{tag}被攔截，也無法逆推得出讀取器金鑰Key_R，只有合法讀取器和電子標籤持有讀取器金鑰Key_R，能夠迅速計算檢查值H_{tag}，而且H_{tag}包含亂數n，可以避免遭受重送攻擊，經由檢查值H_{tag}可有效防止資料被竄改以維護資料完整性。

上述設計之目的即可避免可能的第三者惡意攻擊，如果攻擊者攔截在步驟 4 電子標籤傳送給讀取器的標籤資訊密文C_{tag}，因為密文C_{tag}是以電子標籤金鑰Key_T加密，讀取器必須在資料庫伺服器的協助下，取得將電子標籤金鑰Key_T以金鑰Key_R加密的密文C_{KeyT}，同樣的，攻擊者沒有金鑰Key_R，無法解出密文C_{KeyT}得到電子標籤金鑰Key_T，也就無法解出資訊密文C_{tag}。

如果有攻擊者假冒讀取器想寫入電子標籤的資料，必須將寫入的資料以電子標籤金鑰Key_T加密成C_{tag}'，另外還需計算其對應的雜湊值$H_{tag} = h((C_{tag}' \| Key_R) \oplus n)$提供電子標籤檢驗，然而攻擊者沒有讀取器金鑰$Key_R$即無法產出正確的$H_{tag}$值；即使 H_{tag}值被攔截，因為單向雜湊函數不可逆，攻擊者無法逆推得出讀取器金鑰Key_R；而我們假設電子標籤的設計是存在這樣的驗證程序才對資料異動，所以攻擊者便無法不正常寫入電子標籤的資料，可以有效預防中間人攻擊。至於是否攻擊者可攔截既有的資訊密文C_{tag}'和H_{tag}值，供日後做為重送攻擊，因為H_{tag}值包含亂數n，每一次通訊的值不一樣，所以可有效避免遭受重送攻擊。

五、複雜度分析

電子標籤、讀取器和資料庫伺服器具有不同的運算能力，其中是以電子標籤的運算能力最弱，在各種研究當中都顯示[4,5,6,7,8,9,11,12,13]，電子標籤對於處理數值的四則運算、邏輯運算、隨機亂數的產生，都是最基本的功能，所以我們認為這些運算在比較複雜度時都是可以忽略的。至於我們的設計當中，會使用單向雜湊函數的運算，在以往的研究[4,5,6,7,8,9,11,12,13]都認為電子標籤可以執行這樣的運算，但是它比前述的基本功能耗費較多的時間，因此我們將單向雜湊

函數列入複雜度分析；至於在讀取器和資料庫伺服器的運算，因為都增加處理對稱式加密／解密，所以也列入複雜度分析。

- 電子標籤運作的複雜度分析：
  - ♦ 認證讀取器：執行 2 次雜湊函數運算。
  - ♦ 被寫入資料：執行 1 次雜湊函數運算。
- 讀取器運作的複雜度分析：
  - ♦ 被電子標籤認證：執行 1 次雜湊函數運算。
  - ♦ 讀取電子標籤資料：執行 2 次對稱式解密。
  - ♦ 寫入電子標籤資料：執行 1 次對稱式加密和 1 次雜湊函數運算。
- 資料庫伺服器運作的複雜度分析：
  - ♦ 計算主治醫生讀取器金鑰：執行 1 次雜湊函數運算。
  - ♦ 搜尋符合條件的電子標籤：執行 N 次雜湊函數運算（逐一比對資料庫伺服器紀錄中 N 筆電子標籤的識別碼）。
  - ♦ 計算電子標籤金鑰：執行 1 次雜湊函數運算。
  - ♦ 計算讀取器金鑰：執行 1 次雜湊函數運算。
  - ♦ 封裝電子標籤金鑰：執行 1 次對稱式加密。

由上述的分析，我們的設計所需要的時間複雜度都不會太高，對於電子標籤、讀取器和資料庫伺服器的運算能力都是可接受的。但由於目前尚未見到其他設計，在不同權限讀取器所設計的存取控制協定問題，有像我們提出完整協定細節，就像 John Ayoade 提出的架構，只說明大致的運作流程，所以無法進一步比較上述的複雜度。

六、結論

我們有從實務的考量做了複雜度的分析，所設計的存取控制協定對於電子標籤、讀取器和資料庫伺服器的運算能力都是可接受的。另外，在 John Ayoade 提出 RFID 存取控制方法的基礎上，我們檢視其設計上的缺失而提出更合理的機制，例如 John Ayoade 只說明運作流程，沒有提出詳細的協定，無從探究其可行性，而我們設計的協定有明確定義使用的相關參數及詳細的步驟流程，對於醫院中病歷管理的應用，依據醫生的身份，將讀取器存取權限區分為三種等級；再者，John Ayoade 的設計是直接引用傳統的存取控制概念，在資料庫伺服器需要維護讀取器和電子標籤的權限對照表，然而，電腦系統的存取控制研究早已邁入無對照表的概念，以降低伺服器被入侵的風險及維護的成本，所以我們以此精神提出的設計更安全也更具實用性，並且達到了認證、匿名性、機密性和完整性的條件。

七、參考文獻

[1] 林彥君、鄭博仁、余敬虔，“無線射頻辨識防偽機制研究”，國立台灣科技大學資訊工程系碩士學位論文，台北，2006.

[2] 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

[3] John Ayoade, "Security implications in RFID and authentication processing framework", Computers & Security, Vol. 25, No. 3. May 2006, pp. 207–212.

[4] Hung-Yu Chien, "Secure Access Control Schemes for RFID Systems with Anonymity", IEEE International Conference on 10-12 May 2006, pp. 96–99.

[5] Sepideh Fouladgar , Hossam Afifi, "A Simple Delegation Scheme for RFID Systems (SiDeS) ", RFID, 2007. IEEE International Conference on 2007, pp.1 – 6, Gaylord Texan Resort, Grapevine, TX, USA March 26-28, 2007.

[6] Xingxin Gao, Zhe Xiang, Hao Wang, Jun Shen, Jian Huang, Song Song, "An

approach to security and privacy of RFID system for supply chain", E-Commerce Technology for Dynamic E-Business, 2004. IEEE International Conference on 2004, pp.164 – 168

[7] Dirk Henrici, Paul Müller, "Hash-based Enhancement of Location Privacy for Radio-Frequency Identification Devices using Varying Identifiers", Pervasive Computing and Communications Workshops, 2004. Proceedings of the Second IEEE Annual Conference on 14-17 March 2004, pp.149 – 153

[8] Hun-Wook Kim, Shu-Yun Lim, Hoon-Jae Lee, "Symmetric Encryption in RFID Authentication Protocol for Strong Location Privacy and Forward-Security", IEEE International Conference on Hybrid Information Technology - Vol2 (ICHIT'06) 2006 pp. 718-723

[9] Hyun-Seok Kim, Jung-Hyun Oh, Jin-Young Choi, "Analysis of the RFID Security Protocol for Secure Smart Home Network", Hybrid Information Technology, ICHIT'06. International Conference on Volume 2, Nov. 2006 pp.356 – 363

[10] H. Knospe, H. Pohl, "RFID Security", Information Security Technical Report , Volume 9, No. 4, Dec 2004.

[11] M. Ohkubo, K. Suzuki, and S. Kinoshita. "Cryptographic approach to "privacy-friendly" tags", RFID Privacy Workshop, Cambridge, 2003.

[12] S. A. Weis, "Security and Privacy in Radio-Frequency Identification Devices", Master's Thesis, Massachusetts Institute of Technology, 2003.

[13] S. A. Weis, S. E. Sarma, R. L. Rivest, and D. W. Engels, "Security and privacy aspects of low-cost radio frequency identification systems", Security in Pervasive Computing, Lecture Notes in Computer Science, Volume 2802, pp. 201–212, Berlin 2004.

[14] Lan Zhang, Huaibei Zhou, Ruoshan Kong, Fan Yang, "An improved approach to security and privacy of RFID application system", Wireless Communications, Networking and Mobile Computing, 2005. Proceedings. 2005 International Conference on Volume 2, 23-26 Sept. 2005, pp.1195 – 1198.