# 植基於密碼系統之 RFID 存取控制協定之分析與改進

顧維祺* 劉民德 沈雨澤 陳怡涵 鄭博仁

國立臺中教育大學
資訊科學系
*wcku@ms3.ntcu.edu.tw

**摘要—在 2006 年，Osaka 等人提出一套以對稱式密碼系統為基礎的 RFID 存取控制協定，而在 2008 年，Yoon 與 Yoo 指出 Osaka 等人的存取控制協定不能有效偵測阻斷服務攻擊，並提出一套以對稱式密碼系統為基礎的 RFID 存取控制協定，但我們發現 Yoon-Yoo 存取控制協定仍不能有效防禦位置追蹤攻擊。此外，在 2008 年，Li、Bai 與 Xie 提出一套以對稱式密碼系統為基礎的 RFID 存取控制協定，但我們發現該協定仍不能防禦位置追蹤攻擊。最後，我們提出一套使用密碼系統為基礎的 RFID 存取控制改進協定，並與同類型的 RFID 協定做安全性的比較。**

**關鍵詞：RFID、對稱式密碼系統、存取控制協定。**

## 1. 簡介

RFID (Radio Frequency IDentification；無線射頻識別) 是一種非接觸式的自動辨識系統，系統主要是由 Tag(電子標籤)、Reader (讀卡機) 和 Database(後端資料庫)所組成，其運作原理為 Reader 發送無線電波給 Tag，以無線方式進行資料的存取，並將 Tag 回應的資料送至 Database 進行處理。RFID 具有讀取速度快、儲存資訊量多於一般條碼與可重複使用等優點，近年來已被廣泛地運用在許多方面，例如：物流管理、倉儲管理、圖書館管理、動物監控、門禁系統、智慧家電與醫療用藥管理等。然而，在 RFID 被廣泛應用的同時，其隱私性與安全性亦逐漸受到人們的重視。為了保護使用者隱私與安全，因此，有許多與 RFID 安全性相關的研究不斷被提出，例如：[1][3][4][5][12]等，其中以密碼系統(cryptosystem)為基礎的 RFID 存取控制協定具有較高的安全性。此類 RFID 存取控制協定主要是以對稱式密碼系統(symmetric cryptosystem)或公開金鑰密碼技術(public-key cryptographic techniques)為基礎，其目的在於提高暴力猜測攻擊的困難度，使攻擊者無法藉由猜測取得 Tag 的相關資訊。但是，受限於 Tag 的運算能力，目前此類使用密碼系統為基礎的 RFID 存取控制協定多以對稱式密碼系統為基礎，少有以公開金鑰密碼技術為基礎的 RFID 存取控制協定，而相對於以雜湊函數(hash function)為基礎之身份認證協定，此類協定的安全性通常較高，但其運算複雜度與實作限制亦相對地較高。

在 2006 年，Osaka 等人[7]提出一套以對稱式密碼系統為基礎的 RFID 存取控制協定，提供 Tag 與 Reader 雙向認證並防止 Tag 被追蹤與資料被非法讀取，因 Tag 不需具有加解密功能，故成本較低，適用於大量生產，但我們發現 Osaka 等人的協定不能有效防禦位置追蹤攻擊(location tracking attack)與偵測阻斷服務攻擊(denial-of-service attack)。在 2008 年，Yoon 與 Yoo[6]指出 Osaka 等人的協定不能有效偵測阻斷服務攻擊與前饋安全(forward security)，並提出一套以對稱式密碼系統為基礎的 RFID 存取控制協定，但我們發現 Yoon-Yoo 協定仍不能有效防禦位置追蹤攻擊。在 2008 年，Li、Bai 與 Xie[11]提出一套以對稱式密碼系統為基礎的 RFID 存取控制協定，並宣稱此協定提供 Tag 與 Reader 雙向認證，且能有效防禦位置追蹤攻擊，但我們發現該協定仍不能防禦位置追蹤攻擊與偵測阻斷服務攻擊。在本文中，我們將指出 Osaka 等人的協定、Yoon-Yoo 協定、Li-Bai-Xie 協定的安全弱點，接著，提出一套改進協定並與同類型協定進行安全性比較。

## 2. 相關研究

以密碼系統為基礎的 RFID 存取控制協定，其運算量與實作成本通常高於以雜湊函數為基礎的 RFID 存取控制協定，但此類協定具有較高的安全性。在 2003 年，Juels 等人[2]提出基於公開金鑰密碼系統(public-key cryptosystem)的 RFID 存取控制協定，藉由公開金鑰密碼技術(public-key cryptographic techniques)來達成 Tag 與 Reader 之間的相互認證。然而，在 2003 年，Ohkubo 等人[9]以公開金鑰密碼系統需要大量運算增加成本為由，另提出一套以對稱式密碼系統(symmetric cryptosystem)為基礎的改進協定，使用加密過的匿名 ID(anonymous ID)來避免攻擊者竊聽取得 Tag 的存取控制識別碼，但我們發現該協定並不能有效防禦位置追蹤攻擊。在 2005 年，Zhang 等人[8]根據 Gao 等人[10]提出的以雜湊函數為基礎的 RFID 存取控制協定，另提出一套以使用密碼系統為基礎的 RFID 存取控制協定，此協定包含身份認證機制與 Tag 所有權移轉機制。在身份認證機制中，Tag 先將 Reader 產生的隨機亂數與 TagID 進行 XOR 並用 key 加密，接著，Reader 再利用 Key 解密認證所存的 TagID 是否相同。在 Tag 所有權移轉機制中，Tag 與 Reader 利用 Key 加密 Tag 產生的隨機亂數，接著，Tag 將本身加密結果與 Reader 回傳之加密結果進行比對，以決定是否更新所儲存的 Key，然而，我們發現此協定不能有效防禦位置追蹤攻擊與偵測阻斷服務攻擊。

## 3. 以密碼系統為基礎的 RFID 存取控制協定之安全分析

在本節中，我們將探討以密碼系統(cryptosystem)為基礎的 RFID 存取控制協定，此類協定主要使用密碼系統為主要運算，其運算量與實作成本通常高於以雜湊函數為基礎的 RFID 存取控制協定，但通常具有較高的安全性。首先，我們將介紹三個以密碼系統為基礎的 RFID 存取控制協定，包括 Osaka 等人的協定[7]、Yoon-Yoo 協定[6]與 Li-Bai-Xie 協定[11]，接著，我們將分析各協定的安全性並指出其安全弱點。

### 3.1 Osaka 等人的協定之安全分析

在 2006 年，Osaka 等人[7]提出一套以對稱式密碼系統為基礎的 RFID 存取控制協定，提供 Database 認證 Tag 的功能並防止 Tag 被追蹤與資料被非法讀取，因 Tag 不需具有加解密的計算能力，故成本較低，適用於大量生產，此外，該協定並提供 Tag 所有權移轉的功能。以下，我們將簡要描述 Osaka 等人的 RFID 存取控制協定並說明它的安全弱點。

#### 3.1.1 Osaka 等人的協定簡介

系統中主要包括三類組成元件：Tag、Reader 與 Database。Tag 僅提供簡單運算能力(例如：雜湊計算)，因此必須盡可能降低運算的複雜度，Tag 內儲存{$E_k$(ID)}；Reader 在系統內的功能為讀取 Tag 資料並傳送給 Database 或接收 Database 的資料後傳送給 Tag；Database 儲存所有 Tag 的{ID, $E_k$(ID), k}與 Tag 的相關訊息(以 Info(ID)表示)。協定中假設 Reader 與 Database 之間具有安全通道，並假設系統內 Tag 識別碼之可能數量超過可地毯式搜尋的限度。Osaka 等人的 RFID 存取控制協定包含身份認證機制與 Tag 所有權移轉機制；身份認證機制提供 Database 認證 Tag 的功能，而 Tag 所有權移轉機制提供 Tag 於變更擁有者時的 Reader 更換功能。此協定之符號定義請見(表 1)。

表 1. Osaka 等人的協定之符號說明

| 符號 | 說明 |
|---|---|
| ID | Tag 的識別碼 |
| k | Tag 的存取控制金鑰 |
| $E_k$(ID) | 以金鑰 k 加密後的 Tag 識別碼 |
| $D_k(E_k(ID))$ | 以金鑰 k 解密 $E_k$(ID) 以求得 ID |
| H( ) | 雜湊函數 |
| ⊕ | XOR 運算 |
| r | Reader 產生的亂數 |
| Info(ID) | Tag 相關的資訊 |

<u>身份認證機制</u>

Reader 發出存取要求且產生一個隨機亂數 r 送給 Tag，接著，Tag 以所儲存的 $E_k$(ID)計算 a = H($E_k$(ID)⊕r)並回傳給 Reader，之後，Reader 將 a 與 r 傳送給 Database。接著，Database 利用收

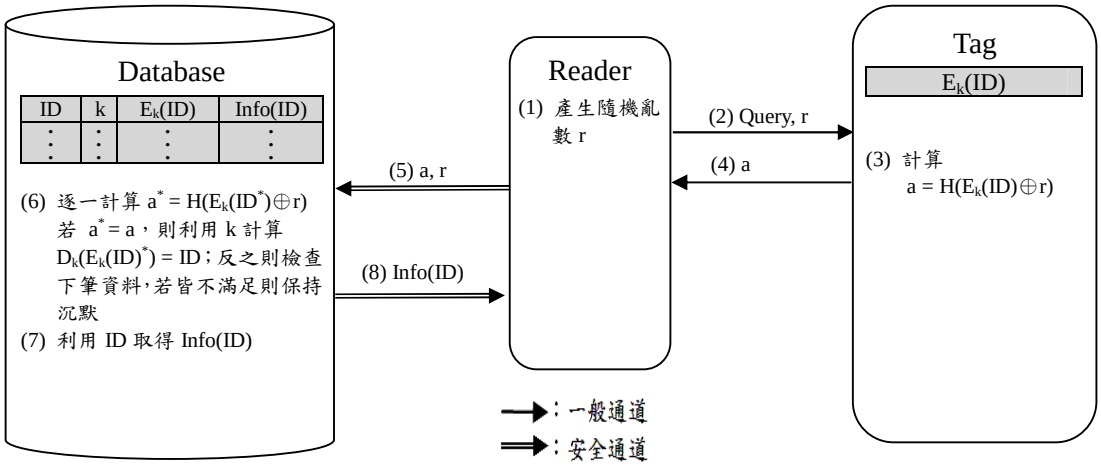


圖 1. Osaka 等人的協定之身份認證機制

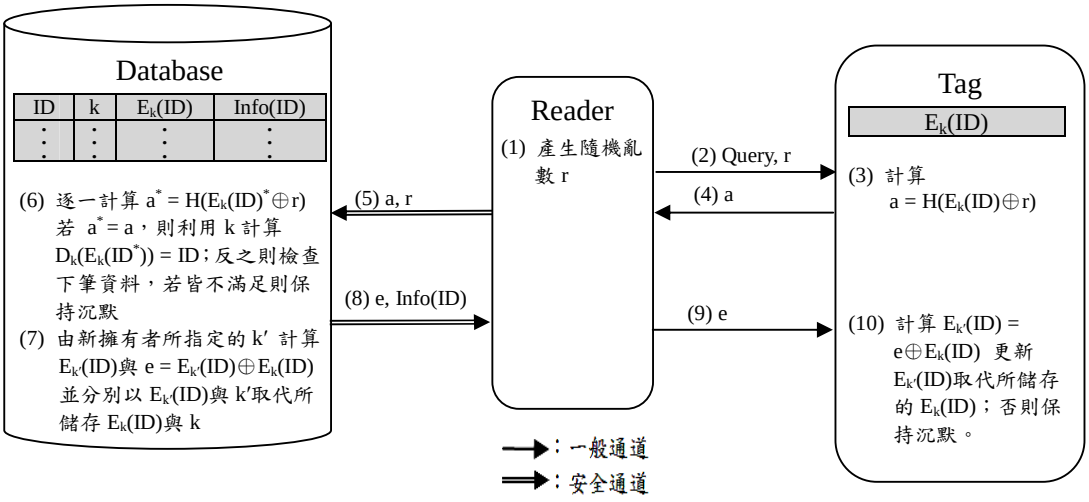


圖 2. Osaka 等人的協定之 Tag 所有權移轉機制

到的 a 與 r 逐一檢查所儲存的 $E_k(ID)^*$ 是否滿足 $a = H(E_k(ID)^* \oplus r)$，若滿足此等式則表示 $E_k(ID)^* = E_k(ID)$，Database 隨即使用所儲存的 k 計算 $D_k(E_k(ID)^*)(= D_k(E_k(ID)))$ 以求得其所對應的 ID；反之，則檢查下筆資料，若皆不滿足，則 Database 對 Reader 要求存取的 Tag 保持沉默。Database 成功認證 Tag 後，隨即將 Tag 的相關資訊回傳給 Reader。身份認證機制之運作流程如(圖 1)所示。

Tag 所有權移轉機制

Reader 發出存取要求且產生一個隨機亂數 r 送給 Tag，接著，Tag 以所儲存的 $E_k(ID)$ 計算 $a = H(E_k(ID) \oplus r)$ 並回傳給 Reader，之後，Reader 將 a 與 r 傳送給 Database。接著，Database 利用收到的 a 與 r 逐一檢查所儲存的 $E_k(ID)^*$ 是否滿足 $a = H(E_k(ID)^* \oplus r)$，若滿足此等式則表示 $E_k(ID)^* = E_k(ID)$，Database 隨即使用所儲存的 k 計算 $D_k(E_k(ID)^*)(= D_k(E_k(ID)))$ 以求得其所對應的 ID；反之，則查下筆資料，若皆不滿足，則 Database 對要求存取的 Tag 保持沉默。Database 成功認證 Tag 後，由新擁有者指定 Tag 的新存取控制金鑰 k′ 並交給 Database，接著，Database 計算 $E_{k'}(ID)$ 與 $e = E_{k'}(ID) \oplus E_k(ID)$，再分別以 $E_{k'}(ID)$ 與 k′ 取代所儲存的 $E_k(ID)$ 與 k，將 e 與 Tag 相關資訊傳送給 Reader，接著，將 e 轉送給 Tag，當 Tag 收到 e 後，以所存的 $E_k(ID)$ 計算 $E_{k'}(ID) = e \oplus E_k(ID)$，之後，以 $E_{k'}(ID)$ 取代所儲存的 $E_k(ID)$，如此一來，即完成 Tag 的所有權移轉機制。所有權移轉機制之運作流程如(圖 2)所示。

3.1.2 Osaka 等人的協定之弱點

我們發現 Osaka 等人的存取控制協定不能有效防禦位置追蹤攻擊(location tracking attack)與偵測阻斷服務攻擊(denial-of-service attack)，攻擊方法描述如下：

位置追蹤攻擊

在 Osaka 等人的存取控制協定之身份認證機制內，攻擊者可以假冒合法 Reader 產生隨機亂數 $r^{\#}$並傳送給欲追蹤的 Tag，之後，攻擊者將紀錄 Tag 回應的 $a^{\#} = H(E_k(ID) \oplus r^{\#})$結果，接著，假設在合法的 Reader 尚未更新 $E_k(ID)$為 $E_{k'}(ID)$前，若攻擊者欲持續追蹤此 Tag 時，攻擊者僅需假冒 Reader 傳送相同的 $r^{\#}$ 給周遭的 Tag，當攻擊者接收到其中一個 Tag 的回應值與先前紀錄的訊息 $a^{\#}$相同時，即表示該 Tag 為欲追蹤的 Tag，攻擊者便可得知欲追蹤之 Tag 在假冒的 Reader 能存取資料的距離範圍內。換言之，攻擊者可輕易假冒合法的 Reader 以追蹤特定的 Tag，藉由 Tag 回應來追蹤特定 Tag 的擁有者所在的位置，侵犯其隱私。

阻斷服務攻擊

在 Osaka 等人的存取控制協定之 Tag 所有權移轉機制內，攻擊者可使 Tag 所屬的 Reader 無法讀取該 Tag，造成服務被阻斷，方法如下：當 Tag 更換所屬 Reader 時，原 Reader 傳送所有權移轉的要求以及一個隨機亂數 r 給 Tag，接著，Tag 利用儲存的 $E_k(ID)$計算 $a = H(E_k(ID) \oplus r)$並回傳給原 Reader，之後，原 Reader 將 a 與 r 傳送給 Database。接著，Database 利用收到的 a 與 r 找出 $E_k(ID)$並使用所儲存的 k 將其解密以求得 ID。接著，由新擁有者指定 Tag 的新存取控制金鑰 k′後交給 Database，接著，Database 計算 $E_{k'}(ID)$與 $e = E_{k'}(ID) \oplus E_k(ID)$，之後，Database 以 k′與 $E_{k'}(ID)$取代所儲存的 k 與 $E_k(ID)$，並將 e 經由 Reader 轉送給 Tag。此時，攻擊者攔截(圖 2)之步驟(9)中傳送的 e，並將它更換為自己隨機產生的亂數 y 後傳送給 Tag。接著，Tag 計算 $E_{k'}(ID)' = y \oplus E_k(ID)$並以 $E_{k'}(ID)'$取代 Tag 中原來的 $E_k(ID)$。在此之後，由於 $E_{k'}(ID)' \neq E_k(ID)$，所以合法的 Reader 將不能通過 Tag 的認證，使得 Tag 將對其所屬 Reader 之存取要求保持沉默，意即攻擊者可阻斷合法的 Reader 讀取 Tag。

**3.2 Yoon-Yoo 協定之安全分析**

Yoon 與 Yoo[6]於 2008 年提出一套以對稱式密碼系統為基礎的 RFID 存取控制協定，該協定指出 Osaka 等人的 RFID 存取控制協定並未能有效防禦阻斷服務攻擊，因此，Yoon 與 Yoo 改進 Osaka 等人的協定[7]並提出自己的安全分析。然而，我們仍發現 Yoon-Yoo 協定並未能有效防禦位置追蹤攻擊。以下，我們將簡要描述 Yoon-Yoo 協定並說明其安全弱點。

3.2.1 Yoon-Yoo 協定簡介

系統中主要包括三類組成元件：Tag、Reader 與 Database。Tag 僅提供簡單運算能力(例如：雜湊計算)，因此必須盡可能降低運算的複雜度，Tag 內儲存加密過的 Tag 的 ID(以 $E_k(ID)$表示)；Reader 在系統內的功能為讀取 Tag 資料並傳送給 Database 或接收 Database 的資料後傳送給 Tag；Database 儲存所有 Tag 的{ID, $E_k(ID)^*$, k}與 Tag 的相關資訊(以 Info(ID)表示)。協定中假設 Reader 與 Database 之間具有安全通道，並假設系統內 Tag 識別碼之可能數量超過可地毯式搜尋的限度。Yoon-Yoo RFID 存取控制協定包含身份認證機制與 Tag 所有權移轉機制，身份認證機制提供 Database 認證 Tag 的功能，而 Tag 所有權移轉機制提供 Tag 於變更擁有者時的 Reader 更換功能。此協定之符號定義請見(表 2)。

表 2. Yoon-Yoo 協定之符號說明

| 符號 | 說明 |
|---|---|
| ID | Tag 的識別碼 |
| k | Tag 的存取控制金鑰 |
| $E_k(ID)$ | 以金鑰 k 加密後的 Tag 識別碼 |
| $D_k(E_k(ID))$ | 以金鑰 k 解密 $E_k(ID)$ 以求得 ID |
| H( ) | 雜湊函數 |
| $\oplus$ | XOR 運算 |
| r | Reader 產生的亂數 |
| Info(ID) | Tag 相關的資訊 |

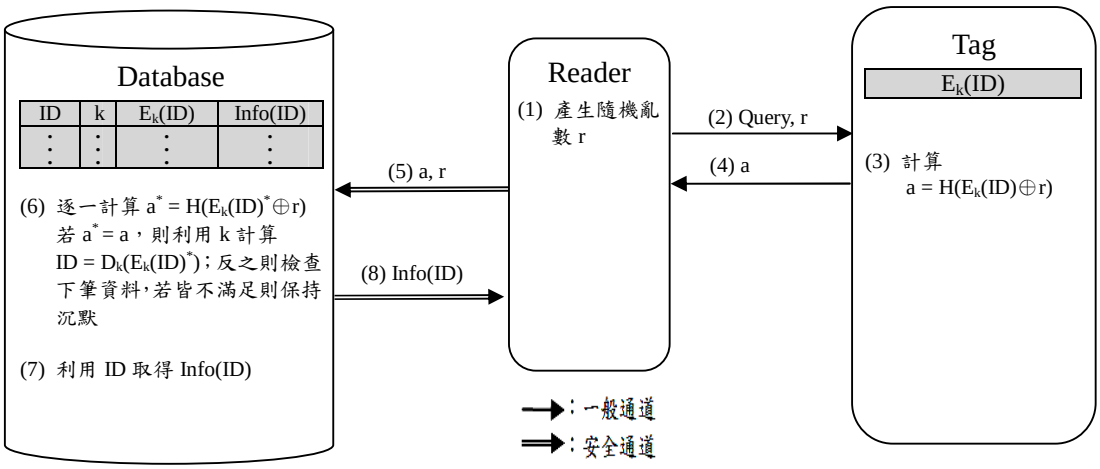


圖 3. Yoon-Yoo RFID 存取控制協定之身份認證機制

身份認證機制

Reader 發出存取要求且產生一個隨機亂數 r 送給 Tag，接著，Tag 以所儲存的 $E_k(ID)$計算 $a = H(E_k(ID) \oplus r)$並回傳給 Reader，之後，Reader 將 a 與 r 傳送給 Database。接著，Database 利用收到的 a 與 r 逐一檢查所儲存的 $E_k(ID)^*$是否滿足 $a^* = H(E_k(ID)^* \oplus r)$，若滿足此等式則表示 $E_k(ID)^* = E_k(ID)$，Database 隨即使用所儲存的 k 計算 $D_k(E_k(ID)^*)(= D_k(E_k(ID)))$ 以求得其所對應的 ID；反之，則檢查下筆資料，若皆不滿足則 Database 對要求存取的 Tag 保持沉默。Database 成功認證 Tag 後，隨即將 Tag 的相關資訊回傳給 Reader。身份認證機制之運作流程如(圖 3)所示。

Tag 所有權移轉機制

Reader 發出存取要求且產生一個隨機亂數 r 送給 Tag，接著，Tag 以所儲存的 $E_k(ID)$計算 $a = H(E_k(ID) \oplus r)$ 並回傳給 Reader，之後，Reader 將 a 與 r 傳送給 Database。接著，Database 利用收到的 a 與 r 逐一檢查所儲存的 $E_k(ID)^*$是否滿足 $a^* = H(E_k(ID)^* \oplus r)$，若滿足此等式則表示 $E_k(ID)^* = E_k(ID)$，Database 隨即使用所儲存的 k 計算 $D_k(E_k(ID)^*)(= D_k(E_k(ID)))$以求得其所對應的 ID；反之，則檢查下筆資料，若皆不滿足則 Database 對要求存取的 Tag 保持沉默。Database 成功認證 Tag 後，由新擁有者指定 Tag 的新存取控制金鑰 k′，並交給 Database，之後，Database 計算 $E_{k'}(ID)$、$e = H(E_k(ID)) \oplus E_{k'}(ID)$與 $mac = H(E_{k'}(ID) \oplus E_k(ID))$，再分別以 $E_{k'}(ID)$與 k′取代所儲存的 $E_k(ID)$與 k 並傳送 e、mac 與 Tag 相關資訊給 Reader，接著，Reader 將 e 與 mac 轉送給 Tag，當 Tag 收到 e 與 mac 後，以所存的 $E_k(ID)$ 計算 $E_{k'}(ID) = e \oplus H(E_k(ID))$，接著，計算 $mac^* = H(E_{k'}(ID) \oplus E_k(ID))$若 $mac^* = mac$，則以 $E_{k'}(ID)$ 取代所儲存的 $E_k(ID)$；否則對要求移轉的 Reader 保持沉默。如此一來，即完成 Tag 的所有權移轉機制。所有權移轉機制之運作流程如(圖 4)所示。

3.2.2 Yoon-Yoo 協定之弱點

我們分析 Yoon-Yoo 協定，發現該協定中如(圖 4)步驟(3)中，Tag 並未產生隨機亂數，因此攻擊者可假冒合法 Reader 對 Tag 傳送隨機亂數，Tag 對攻擊者所傳送的亂數皆會回應相同的訊息，攻擊者可藉此方式來追蹤 Tag 所在的位置。茲將攻擊方法說明如下：

位置追蹤攻擊

在 Yoon-Yoo 存取控制協定之身份認證機制內，攻擊者可以假冒合法 Reader 產生隨機亂數 $r^{\#}$並傳送給欲追蹤的 Tag，之後，攻擊者將紀錄 Tag 回應的 $a^{\#} = H(E_k(ID) \oplus r^{\#})$結果，接著，假設在合法的 Reader 尚未更新 $E_k(ID)$為 $E_{k'}(ID)$之前，若攻擊者欲持續追蹤此 Tag，攻擊者僅需假冒 Reader 傳送相同的 $r^{\#}$給周遭的 Tag，當攻擊者

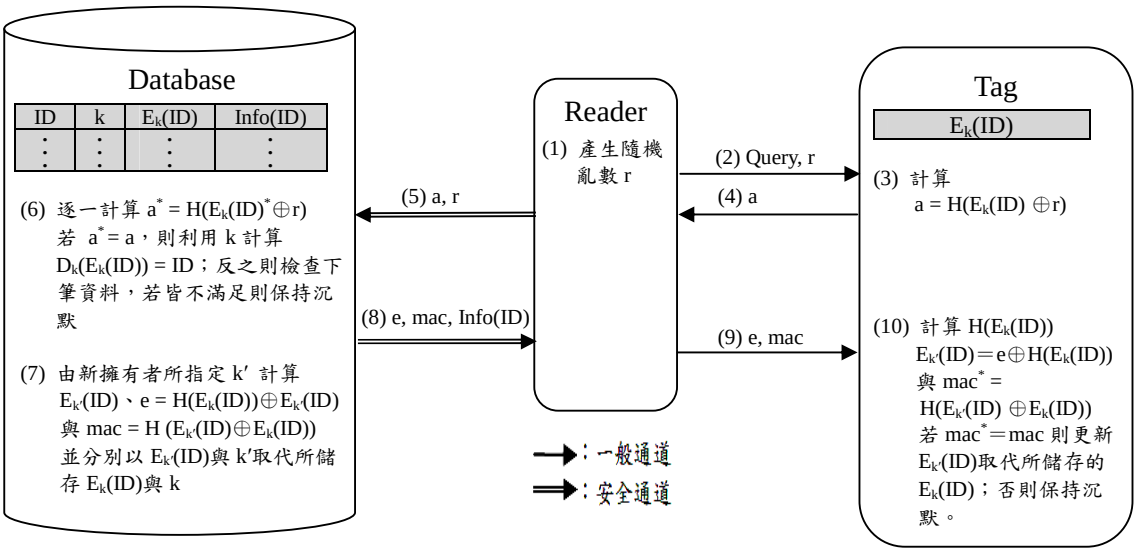


圖 4. Yoon-Yoo RFID 存取控制協定之 Tag 所有權移轉機制

接收到其中有一個 Tag 的回應值與先前紀錄的訊息 $a^{\#}$相同時，即表示該 Tag 為欲追蹤的 Tag，攻擊者即可得知欲追蹤之 Tag 在假冒的 Reader 能存取資料的距離範圍內。換言之，攻擊者可輕易假冒合法的 Reader 以追蹤特定的 Tag，藉由 Tag 回應來追蹤特定 Tag 的擁有者所在的位置，侵犯其隱私。

### 3.3 Li-Bai-Xie 協定之安全分析

在 2008 年，Li、Bai 與 Xie[11](在本論文中，簡稱 Li-Bai-Xie 協定)提出一套以對稱式密碼系統為基礎的 RFID 存取控制協定，並宣稱此協定提供 Tag 與 Reader 雙向認證的功能，且能有效防禦位置追蹤攻擊。然而，我們仍發現 Li-Bai-Xie 協定並未能有效防禦位置追蹤攻擊。以下，我們將簡要描述 Li-Bai-Xie 協定並說明其安全弱點。

#### 3.3.1 Li-Bai-Xie 協定簡介

系統中主要包括三類組成元件：Tag、Reader 與 Database。Tag 內儲存 Tag 的識別碼(以 ID 表示)與 Tag 的存取控制金鑰(以 Ks 表示)；Reader 的功能為傳遞 Tag 與 Database 之間的資訊並具有計算能力；Database 儲存所有 Tag 的識別碼(以 ID 表示)、Tag 的存取控制金鑰(以 Ks 表示)與以金鑰加密的 Tag 識別碼(以 $E_{Ks}(ID)$表示)。協定中假設 Reader 與 Database 之間具有安全通道，並假設系統內 Tag 識別碼之可能數量超過可地毯式搜尋的限度。此協定之符號定義請見(表 3)。

表 3. Li-Bai-Xie 協定之符號說明

| 符號 | 符號表示 |
|---|---|
| ID | Tag 的識別碼 |
| Ks | Tag 的存取控制金鑰 |
| $E_{Ks}(ID)$ | 以金鑰 Ks 加密 Tag 識別碼 |
| $D_{Ks}(E_{Ks}(ID))$ | 以金鑰 Ks 解密 $E_{Ks}(ID)$ |
| $R_A$ | Reader 產生的亂數 |
| $R_B$ | Tag 產生的亂數 |
| $R_c$ | Database 產生的亂數 |
| ⊕ | XOR 運算 |

<u>身份認證機制</u>

Reader 發出存取要求且產生一個隨機亂數 $R_{A1}$ 送給 Tag，接著，Tag 以本身儲存的 Ks 計算 $a = E_{Ks}(R_{A1})$ 與 $b = E_{Ks}(ID) \oplus R_{A1}$ 並回傳給 Reader，之後，Reader 將 a、b 與 $R_{A1}$ 傳送給 Database。接著，Database 計算 $E_{Ks}(ID)^* = b \oplus R_{A1}$，逐一以 Database 所儲存的 Ks 計算 $ID^* = D_{Ks}(E_{Ks}(ID^*))$，若 ID 等於 Database 所儲存的 $ID^*$時，則以此 Ks 計算 $a^* = E_{Ks}(R_{A1})$，若 $a^* \neq a$ 時，則檢查下筆資料，若皆不滿足則對要求存

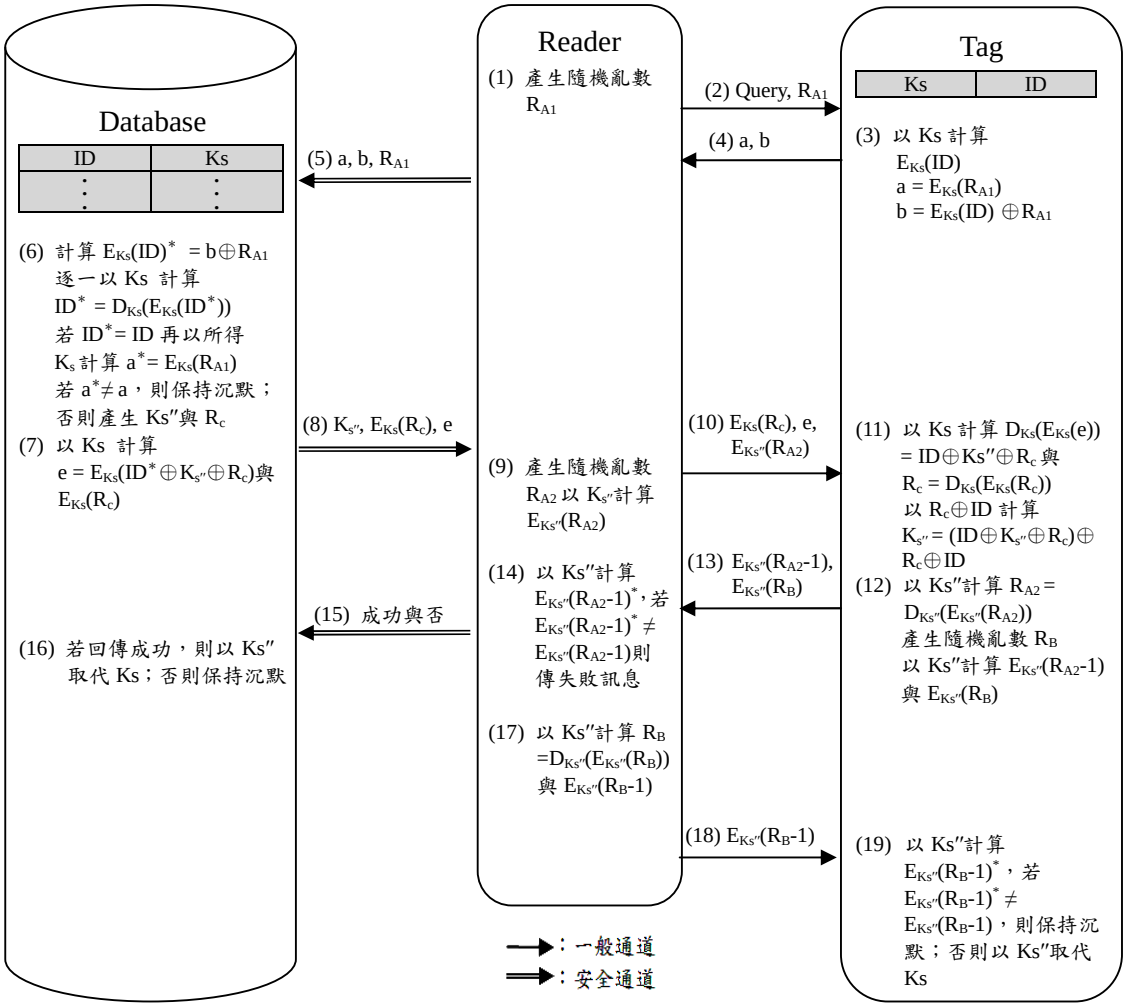


圖 5. Li-Bai-Xie 協定之 Tag 所有權移轉認證機制

取的 Tag 保持沉默；否則產生一個隨機亂數 $R_c$ 與 Tag 的新存取控制金鑰 Ks″，接著，Database 以所存的 Ks 計算 $e = E_{Ks}(ID^* \oplus Ks'' \oplus R_c)$與 $E_{Ks}(R_c)$，並將 e、Ks″與 $E_{Ks}(R_c)$傳送給 Reader，之後，Reader 產生另一個隨機亂數 $R_{A2}$ 並以 Ks″計算 $E_{Ks''}(R_{A2})$，並將 e、$E_{Ks}(R_c)$與 $E_{Ks''}(R_{A2})$送給 Tag。接著，Tag 以所儲存的 Ks 計算 $D_{Ks}(E_{Ks}(e))$ = ID⊕Ks″⊕$R_c$ 與 $R_c = D_{Ks}(E_{Ks}(R_c))$並以所儲存的 ID 計算 $R_c$⊕ID，再計算 Ks″(ID⊕Ks″⊕$R_c$)⊕$R_c$⊕ID 以取得新的 Tag 存取控制金鑰 Ks″，接著，Tag 產生一個隨機亂數 $R_B$ 並以 Ks″計算 $R_{A2} = D_{Ks''}(E_{Ks''}(R_{A2}))$，接著，計算 $E_{Ks''}(R_{A2}–1)$與 $E_{Ks''}(R_B)$傳送給 Reader。Reader 收到後以 Ks″計算 $E_{Ks''}(R_{A2}–1)^*$，再與 Tag 回傳的值進行比對，若不相等則傳送更新失敗訊息給 Database；否則計算 $R_B = D_{Ks''}(E_{Ks''}(R_B))$，並傳送認證成功訊息給 Database。當 Database 收到認證成功訊息後，將 Ks″取代 Database 所存的 Ks；否則對要求存取的 Tag 保持沉默。另外，當 Reader 送出認證成功與否訊息之後，以 Ks″計算 $E_{Ks''}(R_B–1)$傳送給 Tag，接著，Tag 以 Ks″計算 $E_{Ks''}(R_B–1)^*$，再與 Reader 回傳的值進行比對等，若不相等則對要求存取的 Reader 保持沉默；否則將 Ks″取代原本 Tag 所儲存的控制 Ks。身份認證機制之運作流程如(圖 5)所示。

### 3.3.2 Li-Bai-Xie 協定之弱點

Li-Bai-Xie 協定的作者們宣稱 Tag 能有效防禦位置追蹤攻擊，但我們發現該協定並不能有

效防禦位置追蹤攻擊，茲將攻擊方法描述如下：

位置追蹤攻擊

在 Li-Bai-Xie 存取控制協定之身份認證機制內，攻擊者可以假冒合法 Reader 產生隨機亂數 $R_{A1}{}^{\#}$並傳送給欲追蹤的 Tag，之後，攻擊者將紀錄 Tag 回應的 $a^{\#} = E_{Ks}(R_{A1}{}^{\#})$與 $b^{\#} = E_{Ks}(ID) \oplus R_{A1}{}^{\#}$，接著，假設在合法的 Reader 尚未更新 Tag 的存取控制金鑰 Ks 為 Ks″之前，若攻擊者欲持續追蹤此 Tag 時，攻擊者僅需假冒 Reader 傳送相同的 $R_{A1}{}^{\#}$給周遭的 Tag，當攻擊者接收到其中有一 Tag 的回應值與先前紀錄的訊息 $a^{\#}$與 $b^{\#}$相同時，即表示該 Tag 為欲追蹤的目標 Tag，攻擊者即可得知欲追蹤之 Tag 在假冒的 Reader 能存取資料的範圍內。換言之，攻擊者可輕易假冒合法的 Reader 以追蹤特定的 Tag，藉由 Tag 回應來追蹤特定 Tag 的擁有者所在的位置，侵犯其隱私。

## 4. 改進協定

在本節中，我們提出一套以密碼系統為基礎的存取控制改進協定並說明我們的改進協定具有較佳的安全性。

### 4.1 改進協定之說明

我們的改進協定中包括三類組成元件：Tag、Reader 與 Database。Tag 僅提供簡單運算能力 (例如：雜湊計算)，因此必須盡可能降低運算的複雜度，Tag 內儲存{$E_k(ID)$}；Reader 在系統內的功能為讀取 Tag 資料並傳送給 Database 或接收 Database 的資料後傳送給 Tag；Database 儲存所有 Tag 的{ID, $E_k(ID)$, k}與 Tag 的相關資訊(以 Info(ID)表示)。我們的改進協定中假設 Reader 與 Database 之間具有安全通道，並假設系統內 Tag 識別碼之可能數量超過可地毯式搜尋的限度。我們的改進協定包含身份認證機制與 Tag 所有權移轉機制。身份認證機制提供 Database 認證 Tag 的功能；而 Tag 所有權移轉機制提供 Tag 於變更擁有者時的 Reader 更換功能。我們的改進協定之符號定義請見(表 4)。

表 4. 改進協定之符號說明

| 符號 | 符號表示 |
|---|---|
| ID | Tag 的識別碼 |
| k | Tag 的存取控制金鑰 |
| $E_k(ID)$ | 以金鑰 k 加密後的 Tag 識別碼 |
| $D_k(E_k(ID))$ | 以金鑰 k 解密 $E_k(ID)$ 以求得 ID |
| H( ) | 雜湊函數 |
| $\oplus$ | XOR 運算 |
| t | Tag 產生的亂數 |
| r | Reader 產生的亂數 |
| Info(ID) | Tag 相關的資訊 |

身份認證機制

Reader 發出存取要求且產生一個隨機亂數 r 送給 Tag，接著，Tag 產生一個隨機亂數 t 並以所儲存的 $E_k(ID)$計算 $a = H(E_k(ID) \oplus r \| t)$後，將 a 與 t 回傳給 Reader，之後，Reader 將 a、r 與 t 傳送給 Database。接著，Database 利用收到的 a、r 與 t 逐一檢查所儲存的 $E_k(ID)^*$是否滿足 $a = H(E_k(ID)^* \oplus r \| t)$，若滿足此等式則表示 $E_k(ID)^* = E_k(ID)$，Database 隨即使用所儲存的 k 計算 $D_k(E_k(ID)^*)$ $(= D_k(E_k(ID)))$以求得其所對應的 ID；反之，則檢查下筆資料，若皆不滿足則 Database 對要求存取的 Tag 保持沉默。Database 成功認證 Tag 後，隨即將 Tag 的相關資訊回傳給 Reader。身份認證機制之運作流程如(圖 6)所示。

Tag 所有權移轉機制

Reader 發出存取要求且產生一個隨機亂數 r 送給 Tag，接著，Tag 產生一個隨機亂數 t 並以所儲存的 $E_k(ID)$計算 $a = H(E_k(ID) \oplus r \| t)$後，將 a 與 t 回傳給 Reader，之後，Reader 將 a、r 與 t 傳送給 Database。接著，Database 利用收到的 a、r 與 t 逐一檢查所儲存的 $E_k(ID)^*$是否滿足 $a^* = H(E_k(ID)^* \oplus r \| t)$，若滿足此等式則表示 $E_k(ID)^* = E_k(ID)$，Database 隨即使用所儲存的 k 計算 $D_k(E_k(ID)^*)(= D_k(E_k(ID)))$ 以求得其所對應的 ID；反之，則檢查下筆資料，若皆不滿足則 Database 對要求存取的 Tag 保持沉默。Database 成功認證 Tag 後，由新擁有者指定 Tag 的新存取控制金鑰 k′後交給 Database，之後，Database 計算 $E_{k'}(ID)$、$e = H(E_k(ID)) \oplus E_{k'}(ID)$與 mac =

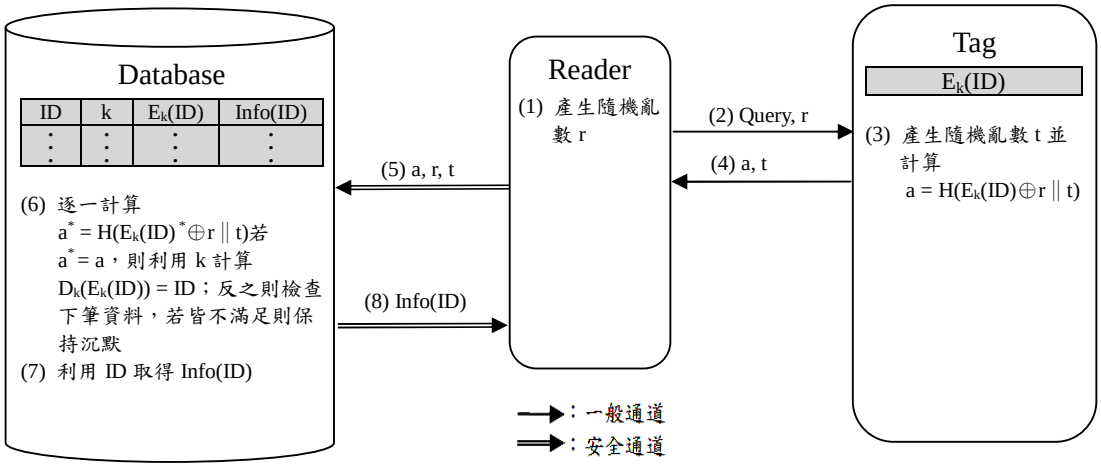


圖 6. 改進協定之身份認證機制

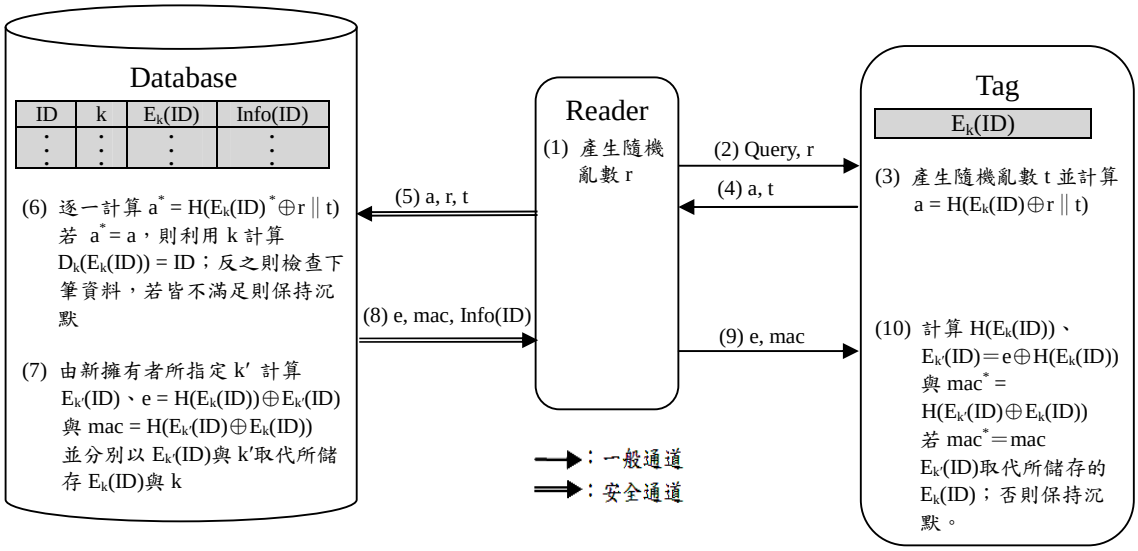


圖 7. 改進協定之 Tag 所有權移轉機制

$H(E_{k'}(ID)\oplus E_k(ID))$，再分別以 $E_{k'}(ID)$與 k′取代所儲存的 $E_k(ID)$與 k 並傳送 e、mac 與 Tag 相關資訊給 Reader。接著，Reader 將 e 與 mac 轉送給 Tag，當 Tag 收到 e 與 mac 後，即以所存的 $E_k(ID)$計算 $E_{k'}(ID) = e \oplus H(E_k(ID))$ 以及 $mac^* = H(E_{k'}(ID)\oplus E_k(ID))$，若 $mac^* = mac$，則 Tag 以 $E_{k'}(ID)$取代所儲存的 $E_k(ID)$，如此即完成 Tag 的所有權移轉；否則 Tag 對要求移轉的 Reader 保持沉默。所有權移轉認證機制之運作流程如(圖 7)所示。

### 4.2 改進協定之安全分析

我們將分析我們的以密碼系統為基礎的 RFID 存取控制改進協定在面對假冒 Tag 攻擊(Tag impersonation attack)、竊聽攻擊(eavesdropping attack)與位置追蹤攻擊的防禦能力並能偵測阻斷服務攻擊，茲將安全分析描述如下：

<u>假冒攻擊的防禦能力</u>

為了防止攻擊者假冒 Tag，Database 需確實認證 Tag。在我們的改進協定之身份認證機制與 Tag 所有權移轉機制中，Reader 傳送一個隨機亂數 r 給 Tag，接著，Tag 產生一個隨機亂數 t 並以所儲存的 $E_k(ID)$計算 $a = H((E_k(ID)\oplus r) \| t)$並回傳給 Reader，再交由 Database 認證 Tag。在傳輸的過程中，若攻擊者竊聽取得 a 與 t，之後企

圖假冒 Tag 以欺騙 Database，此時，Database 將藉由 Reader 傳送新的隨機亂數 r′給攻擊者，接著，攻擊者重送 a 與 t 給 Reader 並轉交給 Database。然而，由於 $a = H((E_k(ID)\oplus r) \| t)$與 Database 所預期的 $a' = H((E_k(ID)\oplus r') \| t)$並不相同，故將無法通過 Database 的認證。因此，我們的改進協定可有效防禦假冒 Tag 攻擊。

阻斷服務攻擊的偵測能力

由於在我們的改進協定之身份認證機制中，並不會更動 Tag 與 Database 所儲存用以認證彼此的資訊，故我們的改進協定之身份認證機制可偵測阻斷服務攻擊。而在我們的改進協定之所有權移轉機制中，當 Tag 通過 Database 認證之後，Reader 收到 Database 傳送的 e、mac 與 Tag 相關資訊，並將 e 與 mac 轉送給 Tag。在傳輸過程中，若攻擊者攔截 $e = E_{k'}(ID)\oplus H(E_k(ID))$，並將 e 置換成自己產生的隨機亂數 $y^{\#}$ 後傳送給 Tag，在收到 $y^{\#}$之後，Tag 將先以所存的$E_k(ID)$計算$H(E_k(ID))$與$E_{k'}(ID)^{\#} = y^{\#}\oplus H(E_k(ID))$，接著，計算 $mac^{\#} = H(E_{k'}(ID)^{\#}\oplus E_k(ID))$，因 $mac^{\#}$與收到的 mac 並不相同，Tag 將中止處理並發送移轉失敗的警示訊息給 Reader。因此，我們的改進協定可偵測阻斷服務攻擊。

竊聽攻擊的防禦能力

為了降低 Tag 資訊被蒐集的風險，Tag 與 Reader 通訊時需隱匿所屬的 $E_k(ID)$，以避免在傳送的過程中遭攻擊者取得。在我們的改進協定中，Tag 以一般通道傳送 r、t 與 $a = H((E_k(ID)\oplus r) \| t)$給 Reader，即使 r、t 與 $a = H((E_k(ID)\oplus r) \| t)$被攻擊者竊聽取得，由於雜湊函數具不可逆性，故攻擊者不能以此求得 $E_k(ID)$。此外，在我們的改進協定之所有權移轉機制中，一般通道傳輸中只有 $e = H(E_k(ID))\oplus E_{k'}(ID)$和 $mac = H(E_{k'}(ID)\oplus E_k(ID))$與 $E_k(ID)$相關，即使攻擊者竊聽取得 e，因為攻擊者無法計算 $H(E_k(ID))$，故不能求得 $E_{k'}(ID)$，另外，由於 Hash( )具不可逆性，故攻擊者不能藉由 $mac = H(E_{k'}(ID)\oplus E_k(ID))$推算出 $E_{k'}(ID)\oplus E_k(ID)$。因此，我們的改進協定可有效防禦竊聽攻擊。

位置追蹤攻擊的防禦能力

在實際應用中，為避免 Tag 被攻擊者追蹤以危及使用者的隱私，藉由 Tag 在每次認證的過程中產生不同的隨機亂數 t 來計算 $a = H((E_k(ID)\oplus r) \| t)$，因每次產生的隨機亂數 $t^{\#}$皆不相同，故攻擊者沒有辦法藉由竊聽上次傳送的 $a = H((E_k(ID)\oplus r) \| t)$來追蹤 $a^{\#} = H((E_k(ID) \oplus r) \| t^{\#})$所在位置。因此，我們的改進協定可有效防禦位置追蹤攻擊。

### 4.3 安全性比較

我們將所提出的改進協定與 Osaka 等人的協定[7]、Yoon-Yoo 協定[6]與 Li-Bai-Xie 協定[11]安全強度的比較。(表 5)顯示我們的以密碼系統為基礎之改進協定的安全性優於第 3 節中所分析的其它同類協定。

## 5. 結論

在本論文中，我們分析三套以密碼系統為基礎的 RFID 存取控制協定之安全性。我們發現 Osaka 等人的協定不能防禦位置追蹤攻擊與阻斷服務攻擊、Yoon-Yoo 與 Li-Bai-Xie 協定不能

表 5：我們的改進協定與類似協定之安全性比較表

| 攻擊 / 協定 | 假冒 Tag 攻擊 | 偵測阻斷服務攻擊 | 竊聽攻擊 | 位置追蹤攻擊 |
|---|---|---|---|---|
| Osaka 等人的協定 | secure | vulnerable | secure | vulnerable |
| Yoon-Yoo 協定 | secure | secure | secure | vulnerable |
| Li-Bai-Xie 協定 | secure | secure | secure | vulnerable |
| 我們的改進協定 | secure | secure | secure | secure |

防禦位置追蹤攻擊。之後，我們提出一套以密碼系統為基礎的 RFID 存取控制改進協定，接著，我們分析所提出的改進協定能有效防禦假冒 Tag 攻擊、竊聽攻擊、位置追蹤攻擊與偵測阻斷服務攻擊，安全性優於同類型協定。

## 參考文獻


[1] A. Juels, R. Rivest, and M. L. Szydlo, "The blocker Tag: Selective blocking of RFID Tags for consumer privacy," Proceedings of the 8th ACM Conference on Computer and Communications Security, pp. 103-111, May 2003.

[2] A. Juels and R. Pappu, "Squealing Euros: Privacy Protection in RFID-Enabled," Lecture Notes in Computer Science, Vol. 2742, pp. 103-121, 2003.

[3] A. Juels, "Minimalist cryptography for low-cost RFID Tags," Lecture Notes in Computer Science, vol. 3352, pp. 149-164, 2005.

[4] A. Juels, "RFID security and privacy: A research survey," IEEE Journal on Selected Areas in Communications, vol. 21, pp. 381-394, Feb. 2006.

[5] A. Juels and S. A. Weis, "Defining strong privacy for RFID," Proceedings of the Fifth Annual IEEE International Conference on Pervasive Computing and Communications Workshops, pp. 342-347, March 2007.

[6] E. J. Yoon and K. Y. Yoo, "Two security problems of RFID security method with ownership transfer," Proceedings of the IFIP International Conference on Network and Parallel Computing, pp. 68-73, 2008.

[7] K. Osaka, T. Takagi, K. Yamazaki, and O. Takahashi, "An efficient and secure RFID security method with ownership transfer," Proceedings of the International Conference on Computational Intelligence and Security, vol. 2, pp. 1090-1095, Nov. 2006.

[8] L. Zhang, H. Zhou, R. Kong, and F. Yang, "An improved approach to security and privacy of RFID application system," Proceedings of the International Conference on Wireless Communications, Networking and Mobile Computing, vol. 2, pp. 1195-1198, 2005.

[9] M. Ohkubo, K. Suzuki, and S. Kinoshita, "Cryptographic approach to 'Privacy-Friendly' Tags," Proceedings of the RFID Privacy Workshop, 2003.

[10] X. Gao, Z. Xiang, H. Wang, J. Shen, J. Huang, and S. Song, "An approach to security and privacy of RFID system for supply chain," Proceedings of the IEEE International Conference on E-Commerce Technology for Dynamic E-Business, pp. 164-168, 2004.

[11] X. Li, E. Bai, and Y. Xie, "A novel authentication protocol with soundness and high efficiency for security problems," Proceedings of the 4th International Conference on Wireless Communications, Networking, and Mobile Computing, pp. 1-3, 2008.

[12] Z. Y. Wang, W. C. Ku, Y. Z. Shen, and M. T. Liu, "Cryptanalysis and improvement of a low computation RFID access control scheme," 2009 全國暨兩岸 RFID 科技論文研討會論文集, Jan. 2009.