產業供應鏈下具不可追蹤及雙向鑑別之 RFID 認證之研究

李鴻璋
淡江大學資訊管理學系
hclee@mail.im.tku.edu.tw

陳欣郁
淡江大學資訊管理學系
bo7778@gmail.com

摘要

在產業供應鏈下導入 RFID 技術已日漸普及，由於 RFID 為非接觸式的遠距離讀取，且供應鏈上隱含著大量的商業利益，競爭對手希望從中竊取商業機密，因此，在實際應用上，資料的安全性及隱私保護便相當重要。

本論文以 Liu 等人及彭宇弘提出之協定為基礎加以改進，上述兩個協定皆只有作單向 tag-to-reader 認證，我們提出在標籤與讀取器通訊過程中，藉由相互挑戰回應達到雙向鑑別，並結合隨機雜湊鎖之理念，將每回合通訊之認證資訊加入隨值數作運算，以達到不可追蹤性。在三者之安全性比較分析上，所提之 RFID 認證安全度最高。

關鍵詞：無線射頻辨識系統、供應鏈、不可追蹤性、雙向鑑別

壹、 緒論

無線射頻辨識系統(Radio Frequency Identity System，RFID)是一種非接觸式的自動識別系統，運作流程大致上分成三個步驟：1、讀取器發射特定頻率的電磁波給標籤；2、標籤藉由電磁波的轉換得到電源，驅動標籤，並將資料傳回給讀取器；3、讀取器會將接收到之訊息解碼，再傳送至後端伺服器以取出物件的相關紀錄。

與傳統的條碼將較之下，RFID 具有多筆資料識別、資料容量大及基本運算…等多項優勢。對於大型零售商而言，RFID 在倉儲管理找到另一個應用，在高價商品方面，RFID 也能提供具有附加價值的生產履歷，甚至作為商品的防偽及保固憑證[7]。In-Stat 公司認為，RFID 標籤的應用是供應鍊管理的未來驅勢。例如全球最大的零售業者 Wal-Mart，已要求其前百大供應商必須配備無線射頻辨識系統，很快地前三百大供應商也都將加入使用無線射頻辨識[3]。

隨著 RFID 的普及，目前實際應用上特別受到關注的問題便是資料的讀取率、安全性、及隱私的保護。由於 RFID 為非接觸式的遠距離讀取，在空中傳輸機密資料，很容易遭到竊聽及冒用，加上供應鏈上隱含大量的商業利益，競爭對手希望從標籤得知其商業機密，透過可攜式 RFID reader，便能輕易得知商家庫存的變化量、產品售價等營運資料，也可分析出消費者喜好，使商家存在競業風險中。為了維護商業利益，要對標籤及系統做出更安全的機制，例如：達到雙向鑑別讓通訊雙方更具有安全性，且在供應鏈環境下，所有權轉移是相當重要的環節，避免讓前任及繼任擁有者竊取標籤中資訊，讓標籤及系統免於遭受各種攻擊威脅，如重送攻擊、阻斷服務攻擊、追蹤、複製…等。

本論文使用「隨機雜湊鎖（Randomized Hash Locking）」[10]的概念，解決 RFID 所產生的安全與隱私問題，將亂數機制加入雜湊函數中，使得每次傳出的資料都不同，且無法預測，可增加標籤內資料的保護，也可使攻擊者無法辨識標籤所傳輸的固定值進行追蹤。提供一個安全且有效率的機制，避免所傳送的電子標籤資料遭到攔截、複製、或是經由分析進而獲得相關資料，甚至破壞正常運作。

以下論文內容安排如下陳述，第二章描述 RFID 安全需求及討論相關研究，第三章提出適用於產業供應鏈中的安全協定，第四章分析安全性並與其他學者所提機制作比較與討論，第五章為本篇論文之結論。

貳、 文獻探討

一、 RFID 安全需求

為了將 RFID 成功的運用在供應鏈系統中，首先要確認哪些安全需求是必要的。在相關文獻中提出，安全的 RFID 認證機制通常包含以下特點[8]：

- 無辨識能力（Indistinguishability, IND）：即使攻擊者竊取到兩個以上的標籤所傳輸的資訊，也無法辨識是否為同一個標籤所產出。
- 向前與向後安全（Forward and backward Security）：即使攻擊者竊取到標籤內部資訊，也能確保標籤之前資料的安全性及繼任擁有者的隱私不受威脅。

- 重送攻擊（Replay Attack）：攻擊者偽裝成合法的標籤或讀取器，並經由合法的通訊過程，重複將攔截到的資料進行傳輸。
- 阻斷服務攻擊（Denial of Service, DoS）：攻擊者傳送大量的詢問(Query)訊息給標籤，或偽造標籤發送假訊息給讀取器，甚至濫用後端伺服器之資源，導致標籤、讀取器及後端伺服器無法負荷而停止運作。
- 雙向鑑別（Mutual authentication）：讀取器與標籤皆驗證對方的合法性。分別為 tag-to-reader 認證，讓讀取器知道此標籤是否合法，及 reader-to-tag 認證，可以讓標籤知道此讀取器是合法的或是偽造的。
- 所有權轉移（Ownership Transfer）：在 RFID 供應鏈中，所有權轉移是最重要的過程之一。將標籤目前的所有人轉移給新的所有人，並確保沒有隱私入侵的疑慮，即所有權轉移過後，前任擁有者不能再對標籤進行存取。
- 非同步攻擊（De-synchronizes attack）：攻擊者企圖使標籤與後端伺服器在進行秘密金鑰同步更新的動作時，阻隔兩邊的通訊，造成更新不同步而轉移失敗。
- 不可追蹤性（Untraceability）：攻擊者無法藉由標籤與讀取器通訊過程的認證資訊取得標籤相關訊息。

二、 相關研究

此節我們將介紹近期的學者所提出之協定加以探討。

（一） Liu 等人所提機制

2010 年 Liu 等人[8]提出應用於供應鏈的 RFID 協定，改良自 2006 年 Osaka 等人[9]所提出的 RFID 所有權轉移協定，主要是改進其向前安全與 DoS 攻擊的問題。此協定運作前有三項假設：後端伺服器與讀取器之間的通訊視為安全的、標籤與讀取器之間的通訊頻道視為不安全的、並假設標籤為不提供防竄改且較少功能之低成本標籤。運作流程分為三個程序：寫入程序、認證程序及所有權轉移程序，以下將詳細說明三個程序。

1. 寫入程序

製造商出產標籤時，將標籤的 *ID*、*Info(ID)*等資訊寫入標籤中。$E_k(ID)$為製造商產生的一把對稱式金鑰 k，將 *Info(ID)*加密後所產生的，由於 $E_k(ID)$是 k 分別針對每個標籤不同的 *ID* 所加密而成，因此每個標籤的 $E_k(ID)$都不相同。

2. 認證程序

如圖 1 所示，詳細步驟為下列：

（1）讀取器對標籤發出 *Query* 訊息，並產生一隨機亂數 r 給標籤。

（2）標籤將收到的亂數值 r 與本身的 $E_k(ID)$做 XOR 運算，再把運算過後的值做雜湊加密得到 α，即為 $\alpha = H(E_k(ID) \oplus r)$傳送給讀取器。

（3）讀取器再將 α 值與隨機值 r 傳給後端資料庫。

（4）後端資料庫搜尋 *ID* 並計算出 α ，若 $\alpha' = \alpha$，即可得到標籤資訊 *Info(ID)*。

（5）擁有者傳送新的對稱式金鑰 k' 給後段資料庫。

（6）後端資料庫利用新的對稱式金鑰 k' 計算出 $e = H(E_k(ID)) \oplus E_{k'}(ID)$以及 $rta = H(E_k(ID) \oplus E_{k'}(ID))$，並連同標籤資訊 *Info(ID)*傳給讀取器，讀取器再將 e 及 *rta* 傳給標籤。

（7）標籤將收到的 e 與本身的 $E_k(ID)$ 做 XOR 運算後得到 $E_{k'}(ID)$，再利用此 $E_{k'}(ID)$值計算出 rta'，若 $rta' = rta$，將 β 值帶入 $H(E_k(ID))$，並將 $E_k(ID)$ 更新為 $E_{k'}(ID)$；反之，將 β 值帶入一隨機數。

（8）標籤將 β 值傳給讀取器，讀取器再傳給後端資料庫。

（9）後端資料庫用本身的 ID 值計算出 β'，若 $\beta = \beta'$，將 k 更新為 k'，及 $E_k(ID)$更新為 $E_{k'}(ID)$，則認證程序完成。

在此認證程序過程中，當後端資料庫確認 α 值正確後（步驟(4)），可直接將 k 值與 $E_k(ID)$更新，但這樣無法確認標籤與後端資料庫是否同步更新，因此標籤更新完 k 與 $E_k(ID)$後，利用 β 值告知後端資料庫標籤是否更新成功，若標籤更新成功，但後端資料庫接收到的 β 值不正確，則後端資料庫不進行更新的動作，並重複認證程序；若標籤更新成功，且 β 值正確，表示後端資料庫與標籤更新同步，此時後端資料庫才會進行 k 值與 $E_k(ID)$的更新動作（即為圖 1 中□內的動作）。

Osaka 等人所提機制為讀取器傳送 *Request* 要求與 r 給標籤，標籤回覆 $\alpha = H(E_k(ID) \oplus r)$，讀取器再將 α 與 r 傳送給後端伺服器，後端伺服器驗證 α 後產生金鑰 k'，計算 $e = E_k(ID) \oplus E_{k'}(ID)$，並將產品相關資訊與 e 傳給讀取器，讀取器再將 e 傳給標籤。攻擊者可從中竊取到 e，若 $E_{k'}(ID)$洩漏，$E_k(ID)$也可輕易的計算出來，且標籤沒有檢查 e 的完整性。而 Liu 等人所提之機制，與 Osaka 等人所提之機制，最主要有三點不同：

- e 改為 $H(E_k(ID)) \oplus E_{k'}(ID)$，單向雜湊函數保護 $E_k(ID)$達到向前安全。
- 計算 $rta = H(E_k(ID) \oplus E_{k'}(ID))$，以檢查 e 的完整性並防止 DoS 攻擊。
- 標籤更新完成後回覆訊息 $\beta = H(E_k(ID))$，確認標籤與後端伺服器間資訊的同步更新，否則此協定將重覆執行。

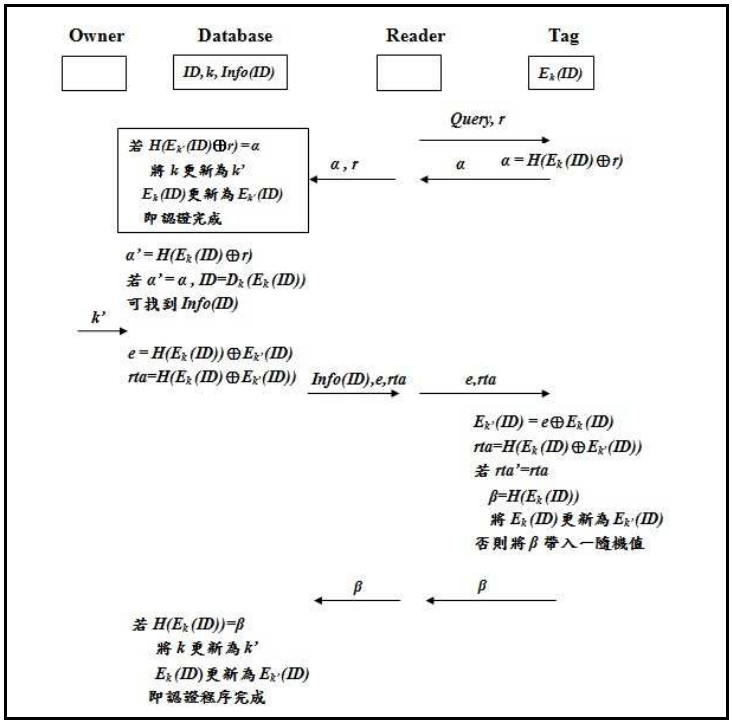

圖 1　Liu 等人提出所有權轉移之認證協定

3. 所有權轉移程序

原有廠商將所有權轉給繼任廠商時，基於安全考量，會將對稱式金鑰 k 更換為新的金鑰 k'，並將 k'、ID、$Info(ID)$等必要資訊經由安全通道轉移給繼任廠商；新的廠商再將 k' 更換為 k'' 成為新的對稱式金鑰。

（二） 彭宇弘所提機制

2011 年，彭宇弘[4]提出適用於生產至零售通路之 RFID 協定，針對貨物供應其間的運送及入庫動作設計安全協定，並將後端伺服器與讀取器之間視為不安全管道。標籤的部分，為了符合建置成本考量，使用低成本標籤，所具備的運算能力有產生隨機數、簡易位元運算和單向雜湊函數運算。此協定分成四個階段：初始化階段、讀取認證階段、安全狀態切換階段及所有權轉移階段，以下詳細說明四個步驟。相關符號定義如相關符號定義如表 1 所示。

表 1　相關符號定義

P_i	供應鏈成員 i
S_i	P_i 所維護的後端伺服器
T_j	RFID 標籤 j
$b_{i,j}$	P_i 與 T_j 共享的祕密金鑰
p_j	安全狀態變數
EPC_j	產品電子編碼
r_n	隨機數，n 為整數值
$H(.)$	單向雜湊函數
$DATA_j$	產品資訊
R_k	RFID 讀取器 k
RID_k	讀取器單次使用的識別碼
$sKey_k(.)$	使用金鑰 $sKey_k$ 的對稱式金鑰加密演算法，$sKey_k$ 為 R_k 與 S_i 共享的祕密金鑰
$\|\|$	位元串接運算
$\oplus$	XOR 運算

1. 初始化階段

l 標籤初始化

假設產品製造商定義為 P_0，在標籤 T_j 首次貼附產品時，P_0 會為該產品指定產品電子編碼 EPC_j，安全狀態變數 p_j 設為 0，P_0 選定與標籤共享的祕密金鑰 $b_{0,j}$，並將（EPC_j, $b_{0,j}$, p_j ）存入標籤 T_j 中，P_0 亦將認證標籤與產品相關資訊（EPC_j, $b_{0,j}$, p_j, $DATA_j$）儲存至資料庫中。

l 讀取器初始化

假設產品製造商的某一讀取器定義為 R_k，P_i 對 R_k 指定單次使用之識別碼 RID_k 與對稱式金鑰 $sKey_k$，並將（RID_k, $sKey_k$）存入 R_k 與 S_i 的資料庫中。

2. 讀取認證階段

步驟為下列，如圖 2 所示：

（1）讀取器發送讀取要求 $Request$ 給標籤。

（2）標籤產生隨機值 r_1 , r_2，計算 $x= r_1 \oplus b_{i,j}$，若標籤在安全狀態下（$p_j = 0$），指定 y 為 EPC_j，反之，y 為隨機值 r_2，在計算 $z = H(x \| r_1 \| y \| b_{i,j})$。

（3）標籤將(x, y, z)傳送給讀取器，讀取器將(x, y, z)連同 RID_k 一並傳給後端伺服器。

（4）後端伺服器檢查 RID_k 是否為合法登錄之讀取器，否則停止認證程序。確認合法後，辨別 y 是否符合產品電子編碼格式，若符合則以 y 來查詢 $b_{i,j}$；不符合則逐一取出資料庫中所有 b 值進行標籤辨識。

（5）後端伺服器利用接收到的 x 與本身的 $b_{i,j}$ 計算出 r_1，並檢驗 z 是否等於 $H(x \| r_1 \| y \| b_{i,j})$，相等表示對標籤認證成功，否則認證失敗。

（6）認證成功後後端伺服器將產品資訊 $DATA_j$ 取出並計算 $m = sKey_k (RID_{k'}, H(RID_{k'}), DATA_j)$，接著將 m 傳給讀取器，$RID_{k'}$ 為新指派之識別碼。

（7）讀取器將 m 解密，確認 $RID_{k'}$ 不等於 RID_k 後，更新 RID_k 為 $RID_{k'}$。最後讀取器計算 $n = H(RID_{k'} \| sKey_k)$，並將 n 傳給後端伺服器，通知識別碼更新完成。

（8）後端伺服器計算 $H(RID_{k'} \| sKey_k)$是否等於 n，相等則表示讀取器識別碼已更新完成，後端伺服器邊將 RID_k 更新為 $RID_{k'}$。

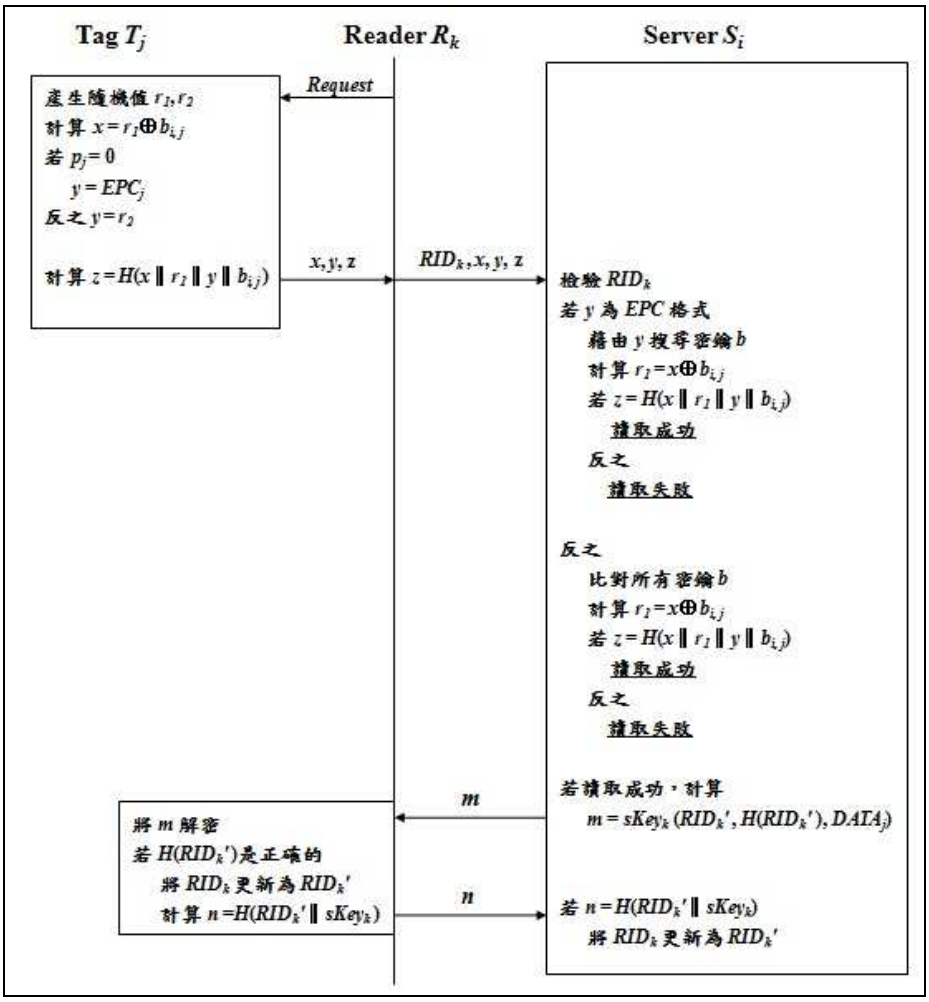

圖 2　讀取認證階段

3. 安全狀態切換階段

P_i 擁有標籤所有權時，可以在如公司內部倉庫環境下，視為安全環境，將標籤更新為安全狀態；在產品流通階段，將標籤更新為非安全狀態，步驟如下：

（1）後端伺服器經由讀取器對標籤執行讀取認證階段，假如認證成功，則執行以下步驟，如圖 3 所示。

（2）後端伺服器設定安全狀態變數 p_j' 及產生隨機值 r_3，並計算 s 與 t，將(p_j', s, t)藉由讀取器傳送給標籤。

（3）標籤利用收到的 s 與本身的 $b_{i,j}$ 計算 r_3，再驗證 $H(s \| r_3 \| p_j')$是否等於 t，相等則更新 p_j 為 p_j'。

（4）標籤產生隨機值 r_4，計算出 $u = H(r_3 \| r_4 \| p_j' \| b_{i,j})$，將$(r_4, u)$藉由讀取器傳送給後端伺服器。

（5）後端伺服器驗證 $H(r_3 \| r_4 \| p_j' \| b_{i,j})$是否等於 u，相等則更新 p_j 為 p_j'。

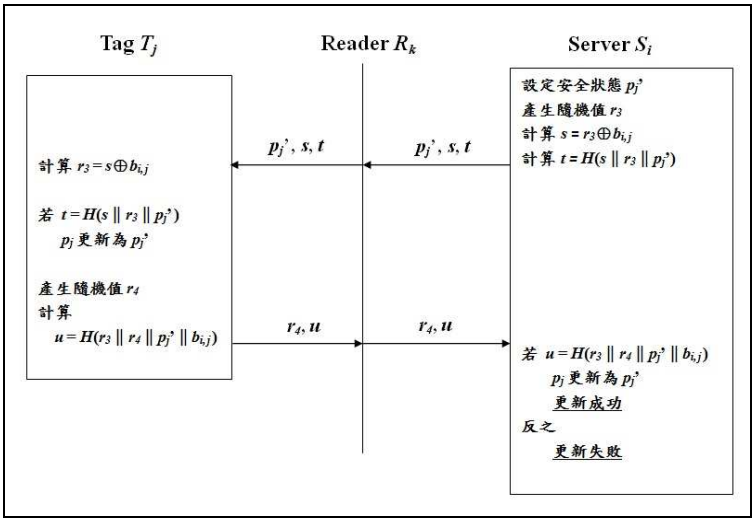

圖 3　安全狀態切換階段

4. 所有權轉移階段

當 P_{i+1} 自 P_i 以安全管道取得標籤認證必要資訊，S_{i+1} 可對標籤進行讀取認證，接著進行所有權轉移，將標籤的祕密金鑰更新，步驟如下：

(1) P_i 透過安全管道將認證標籤與產品相關資訊（$EPC_j, b_{i,j}, p_j, DATA_j$ ）傳送給 P_{i+1}。

(2) 假設 R_k' 為 P_{i+1} 所擁有的讀取器，S_{i+1} 透過 R_k' 對 T_j 執行，讀取認證階段，假如認證成功，則執行以下步驟，如圖 4 所示。

(3) S_{i+1} 產生隨機值 r_5，計算出 s 與 t，將(s, t)藉由讀取器傳送給標籤。

(4) 標籤利用收到的 s 與本身的 $b_{i,j}$ 計算 r_5，再驗證 $H(r_5 \| s)$是否等於 t，相等則計算出新的祕密金鑰 $b_{i,j}$ ，接著產生隨機值 r_6，計算出 $u = H(r_6 \| b_{i+1,j})$，將所有權轉移訊息(r_6, u)藉由讀取器傳給 S_{i+1}。

(5) S_{i+1} 計算出 $b_{i+1,j}$ 後，再驗證 $H(r_6 \| b_{i+1,j})$是否等於 u，相等則完成所有權轉移階段。

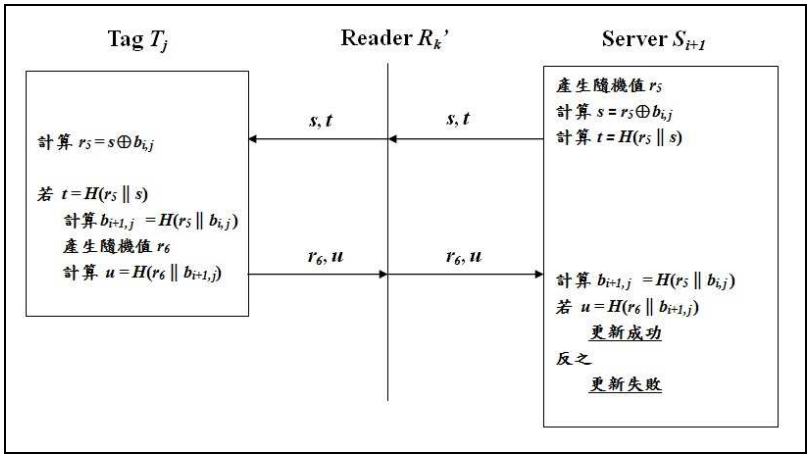

圖 4　所有權轉移階段

參、 所提機制：UMP 認證

此章節將介紹本篇論文所提的機制，我們將此機制命名為 UMP。其取自不可追蹤性(Untraceability)、雙向鑑別(Mutual authentication)及協定(Protocol)等英文單字之字首所組成。

一、　　簡介

供應鏈導入 RFID 技術越來越普及，RFID 已成為一種不可或缺的工具，使製造商能隨時清楚的看到資產的相關動向。由於 RFID 在空中傳輸機密資料，很容易遭到竊聽及冒用，為了解決 RFID 所產生的安全及隱私問題，相關文獻所提出的解決方案主要分成下列四類[11][5]：

- 使標籤部分或完全失效（Restricting or Complete “Killing” of Tags）：刪除標籤內唯一的序號僅保留產品資訊或是將標籤內部資訊完全刪除，使其失去效用，可保護標籤擁有者的隱私。但 “Killing” 指令難以確保正確且完整的被執行，可能再度被有心人士利用。除此之外，標籤一旦失效後，便無法再度啟用。
- 雜湊鎖（Hash Locking）：當標籤內儲存的資料傳送出去之前，先經過 hash 函數運算，作為保護。
- 隨機雜湊鎖（Randomized Hash Locking）：比起雜湊鎖，除了需要單向湊函數外，另外加上隨機數產生器。將亂數機制加入雜湊鎖中，使得每次傳出的資料都不同，且無法預測。
- 干擾標籤（Blocker Tag）：為一套干擾裝置，主要用來阻隔讀取器與標籤之間的通訊，保護標籤不被讀取及追蹤。但此裝置無法辨別是否為惡意讀取器，若合法讀取器要讀取受保護之標籤，也必須將此裝置移除。

本論文使用「隨機雜湊鎖（Randomized Hash Locking）」的概念，利用隨機數的不可預測性，增加標籤內資料的保護，也可使攻擊者無法透過辨識標籤傳輸的固定值進行追蹤。標籤的部分，假設為低成本低預算的標籤，僅具備的運算能力有產生隨機數、簡

易位元運算和單向雜湊函數運算。並且將標籤、讀取器及後端伺服器三方之間的通訊皆設在不安全狀態下。

二、 方法

我們將 UMP 認證分為三個階段：初始定義階段、讀取認證階段、及所有權轉移階段。符號定義如表 2 所示。

表 2 相關符號定義

P_i	現任供應鏈成員
P_n	繼任之供應鏈成員
T_i	RFID 標籤
b_i	P_i 與 T_i 共享之秘密金鑰
b_i^n	P_n 與 T_i 共享之秘密金鑰
EPC_i	產品電子編碼
$DATA_i$	產品相關資訊
RID_i	讀取器單次使用之識別碼
RID_n	讀取器每回合新指派之識別碼
DID	伺服器之識別碼，且作為標籤、讀取器及伺服器間通訊之秘密金鑰
DID_n	每回合新指派之伺服器識別碼，且作為標籤、讀取器及伺服器間通訊之秘密金鑰
r、s、t	隨機產生之亂數值
$h(.)$	單向雜湊函數
$\|\|$	位元串接運算符號
$\oplus$	XOR 運算符號

（一） 初始定義階段

我們將此階段設定在安全狀態下，且沒有任何非法標籤、讀取器、資料庫進行下列初始化之動作。

決定 RFID 標籤成本重要的因素之一，取決於儲存容量的大小，為了達到成本最小化之目標，本研究所提出的機制將標籤內所含的必要欄位盡可能減少。

在 UMP 認證中，參與角色有標籤、讀取器及後端伺服器，因此在流程中各角色所需欄位我們分別定義如下：

- RFID 標籤內存之初始欄位為：EPC_i 、b_i 、DID
- RFID 讀取器內存之初始欄位為：b_i 、RID_i 、DID
- 資料庫內存之初始欄位為：b_i、RID_i 、DID、$DATA_i$

（二） 讀取認證階段

讀取器首先對標籤發出 *Request* 詢問，且在讀取器與標籤通訊過程中，會利用兩個隨機亂數作相互挑戰回應，來達到讀取器與標籤間之雙向鑑別。經由讀取器將標籤回覆訊息傳給後端伺服器，後端伺服器會先確認讀取器合法性後，送出該產品資訊且利用共同擁有之密鑰 *DID* 證明其身分，達到讀取器與後端伺服器間之相互認證。接著，後端伺服器會指派新的讀取器識別碼，當讀取器更新完成後，回覆更新成功訊息給後端伺服器，伺服器同步也會更新此識別碼，則讀取認證階段完成。

詳細流程主要分為 7 個步驟，請參考圖 5，說明如下：

1. 讀取器產生隨機值 r，並計算 $r \oplus DID$，連同 *request* 要求傳送給標籤。
2. 標籤計算出隨機值 r 後與本身的 b_i 計算出 $H(b_i \oplus r)$，再利用共同之密鑰 DID、標籤的產品編碼 EPC_i 及隨機值 r 作 XOR 得到 $DID \oplus EPC_i \oplus r$，最後產生一隨機值 s，並計算 $s \oplus DID$，標籤將這三項資訊回覆給讀取器。
3. 讀取器接收到訊息後，可利用本身之 DID 及 r 來取出 EPC_i 值，藉由此 EPC_i 值可得知正在與哪標籤進行通訊，並取得其 b_i 值，並回應標籤 $H(b_i \oplus s)$。
4. 標籤利用本身之 b_i 計算 $H(b_i \oplus s)$無誤後，表示雙向鑑別完成。接著計算出 $x = H(b_i \oplus r+1) \oplus EPC_i$ 及 $H(x \| H(EPC_i) \| r)$傳送給讀取器。
5. 讀取器自行計算出 $H(b_i \oplus r+1)$後可得 EPC_i 值，並驗證 $H(x \| H(EPC_i) \| r)$是否正確，若正確，用共享之祕鑰 DID 及 r 加密 EPC_i 得到 $H(DID \oplus r) \oplus EPC_i$，並計算 $H(RID_i \| H(EPC_i) \| DID \| r)$ 作為完整性檢查，連同讀取器之識別碼 RID_i 及加密隨之隨機值 $r \oplus DID$，將這 4 個值傳給後端伺服器。
6. 後端伺服器先判別 RID_i 是否為合法讀取器，再利用本身的 DID 及 r 計算出 EPC_i 值，即可向後端伺服器查詢產品相關資訊 $DATA_i$，並驗證 $H(RID_i \| H(EPC_i) \| DID \| r)$是否正確。接著計算 $x = H(DID \oplus r+1)$，向讀取器證明此為合法伺服器所發出之訊息；用密鑰 DID 加密 $DATA_i$ 得到 $H(DID) \oplus DATA_i$ ；產生隨機值 t，計算 $t \oplus DID$，並指派新的讀取器識別碼 RID_n ，利用密鑰 DID 及隨機值 t 加密 RID_n 得到 $y = RID_n \oplus H(DID \oplus t)$，最後計算 $H(x \| H(DID) \| y \| H(RID_n) \| t)$作為完整性檢查；將這 5 個值傳給讀取器。
7. 讀取器利用本身儲存的 DID 驗證此訊息是否為合法伺服器所發出，再以 $H(DID)$ 取出產品相關資訊 $DATA_i$ ，接著利用得到之隨機值 t 計算 $H(DID \oplus t)$取得伺服器所指派之新識別碼 RID_n ，完成更新識別碼。再回傳 $H(RID_n \oplus t)$更新成功之訊息給後端伺服器，伺服器收到此訊息後，表示讀取器完成更新，也同步將識別碼更新。

（三） 所有權轉移階段

此階段要將標籤之秘密金鑰 b_i 及標籤、讀取器與伺服器三方通訊之秘鑰 DID 進行更新，讓新的擁有者取得產品的所有權。進行所有權轉移之前，新的擁有者 P_n 由現任擁有者 P_i 在安全通道下（如：防電磁波洩漏的空間）且在雙方許可的情況之下，取得認證及產品相關資訊(b_i , EPC_i, DID, $DATA_i$)。

詳細流程主要分為 8 個步驟，請參考圖 6，說明如下：

1. 新的擁有者 P_n 給伺服器新的標籤秘密金鑰 b_i^n及標籤、讀取器與伺服器三方通訊之秘鑰 DID_n。
2. 後端伺服器向標籤發送一個 *write request* 訊息。
3. 標籤傳送一個加密過後之挑戰值 $r \oplus DID$ 給後端伺服器。
4. 後端伺服器用唯一之通訊密鑰 DID 計算出 $H(DID \oplus r)$證明為合法之伺服器，並產生一隨機值 s，加密過後為 $s \oplus DID$，將這兩項資訊傳給標籤。

5. 標籤驗證此訊息由合法伺服器所發出後，用標籤之秘鑰計算出 $H(b_i \oplus s)$作回應，並利用 DID 及 s 加密產品編碼 EPC_i，將這兩項訊息傳給後端伺服器。
6. 後端伺服器用本身的 DID 及 s 取得 EPC_i 後，藉由此 EPC_i 值可得知正在與哪標籤進行通訊，取得其 b_i 值，驗證 $H(b_i \oplus s)$是否正確，若正確，則相互認證完成。接著，後端伺服器利用標籤之秘鑰 b_i 將新的標籤秘密金鑰 b_i^n及標籤、讀取器與伺服器三方通訊之秘鑰 DID_n 進行加密，得到 $H(b_i)\oplus b_i^n$及 $H(b_i)\oplus DID_n$，並計算 $H(H(b_i) \| H(b_i^n) \| H(DID_n))$ 作為完整性檢查。
7. 標籤用本身之秘鑰 b_i 計算 $H(b_i)$以取得b_i^n及 DID_n 後，驗證 $H(H(b_i) \| H(b_i^n) \| H(DID_n))$是否正確，若正確則將 b_i 更新為b_i^n，DID 更新為 DID_n，並計算 $z = H(b_i^n \oplus s \oplus DID_n)$；若不正確，則計算 $z = H(s)$。
8. 若後端伺服器接收到的訊息為 $z = H(b_i^n \oplus s \oplus DID_n)$，則表示標籤更新秘鑰成功，而後端伺服器也同步將 b_i 及 DID 更新為b_i^n及 DID_n。

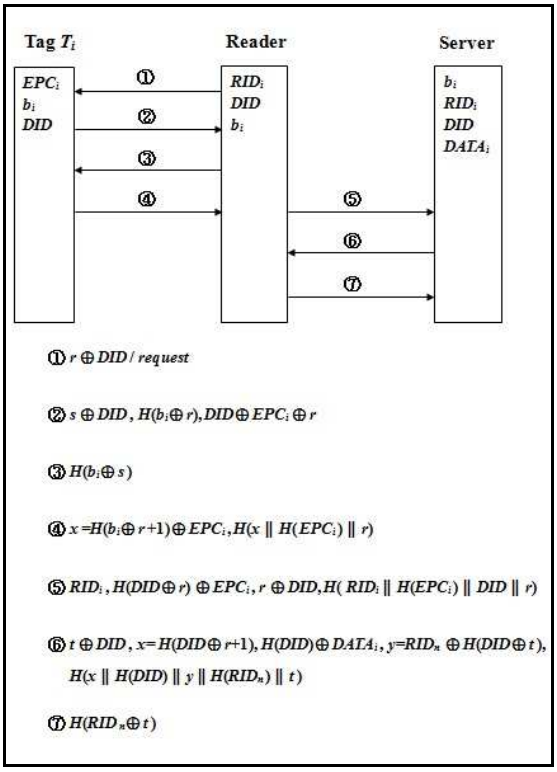

圖 5　UMP 之讀取認證階段

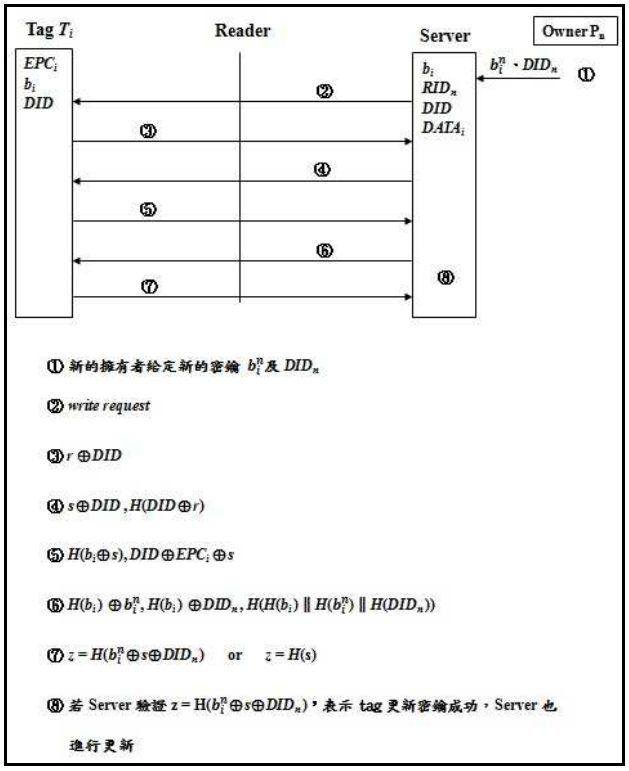

圖 6　UMP 之所有權轉移階段

肆、 分析與討論

一、 安全性分析

本論文所提機制，根據 2.1 節所提出 RFID 安全需求，在此作分析：

- 無辨識能力（Indistinguishability, IND）：由於標籤每回合通訊皆加入隨機值做運算，攻擊者就算攔截到兩個以上的標籤回覆訊息，也無法確定是否為同一個標籤所送出。
- 向前與向後安全（Forward and backward Security）：當 P_n 自 P_i 取得標籤認證相關資訊，是在雙方核可情況下進行，接著 P_n 即傳送新的密鑰 b_i^n及

DID_n 給後端伺服器，當秘密金鑰同步更新後，由於此金鑰與前任擁有者所持有之金鑰無任何相關性，無從得知前任擁有者之金鑰為何，而前任擁有者無法自行計算出新的秘密金鑰，因此沒有向前及向後安全的疑慮。

- 重送攻擊（Replay Attack）：攻擊者偽裝成合法的標籤是無效的，因為每回合皆有隨機產生之亂數加入運算；攻擊者試圖假冒讀取器重送資訊給伺服器也是無效的，原因為讀取器之識別碼 RID_i 為單次使用，每回合皆會更新。
- 阻斷服務攻擊（Denial of Service, DoS）：大量惡意詢問訊息不易防止，但必須要將阻斷服務攻擊之影響降至最低。可透過認證機制，當後端伺服器收到讀取器傳送之訊息時，會先辨別是否為合法之讀取器所送出，確認此合法性後才會進行運算及回覆訊息，避免造成後端伺服器的負擔。
- 雙向鑑別（Mutual authentication）：當讀取器傳送挑戰值 r 給標籤時，標籤利用雙方通訊之秘鑰 DID 及標籤產品編碼 EPC_i 表明身分，再利用標籤秘鑰 b_i 作回應，並送出另一挑戰值 s 給讀取器；讀取器計算出 EPC_i 值後取得標籤秘鑰 b_i，可驗證是否為合法標籤所送出，再利用標籤秘鑰 b_i 及挑戰值 s 回應標籤，證明自己為合法之讀取器。
- 所有權轉移（Ownership Transfer）：新的擁有者 P_n 經由安全通道且在雙方許可的情況之下，取得認證及產品相關資訊後，自行將要更新之秘密金鑰 b_i^n 及 DID_n 傳送到後端伺服器中，由於此金鑰由新的擁有者自行給定，與前任擁有者所持有的金鑰無相關性，當秘鑰在標籤與後端伺服器進行同步更新之後，能有效的將所有權轉移給新的擁有者，且前任擁有者便無法再對標籤進行存取。
- 非同步攻擊（De-synchronizes attack）：當後端伺服器要求標籤進行金鑰更新時，標籤會回傳更新成功訊息，伺服器確認標籤完成更新後，再將自己的金鑰作更新以達到同步狀態。若發現標籤送出之已更新訊息有誤，可及時發現，可能遭受非同步攻擊，應立即處理。
- 不可追蹤性（Untraceability）：標籤與讀取器進行通訊時，每回合的認證資訊皆加入隨機亂數進行運算，使溝通訊息具隨機性，由於每次傳送的資料都不相同且沒有相關，攻擊者無法從中得知關連性也無法進行預測或追蹤。

二、 比較分析

在此小節，我們將 2.2 節相關研究中各學者所提機制及本論文所提之 UMP 機制作比較分析及討論。

在 Liu 等人的方法中，雖然改進了向前安全與 DoS 攻擊，但仍然存在重送攻擊的弱點，只要攻擊者持續傳送不變動的 r ，就可追蹤特定標籤。攻擊者可竊聽到 $\beta = H(E_k(ID))$，並由式子 $e = H(E_k(ID)) \oplus E_{k'}(ID)$可得到 $E_{k'}(ID) = e \oplus \beta$，若將此 $E_{k'}(ID)$複製到空白標籤中，攻擊者即可成功仿冒標籤。

在彭宇弘所提機制中，我們提出以下幾點加以探討及改進：

- 設定安全狀態方法雖然較具彈性，但如何判定此環境視為安全狀態下，較難定義，例如：在公司內部倉庫環境下視為安全狀態，仍然存在竊聽的風險。因此在本論文所提方法中，將所有環境假設為不安全狀態下，免除不必要的疑慮及切換狀態的麻煩。且在讀取認證過程中，若環境設為不安全狀態下，標籤會回覆隨機值，此時後端伺服器必須逐一搜尋比對以找到 $b_{i,j}$，才可以得到產品相關資訊，此方法較耗時且沒有效率；我們提出的方法中，利用三方通訊秘鑰 *DID* 對產品編碼 EPC_i 進行加密，因此後端伺服器能直接利用 EPC_i 找到 $DATA_i$。
- 當讀取器向標籤發出 *Request* 詢問時，標籤沒有對讀取器進行身分識別，便直接將計算過後之資訊 (x, y, z) 傳送給讀取器，因此，在此通訊過程沒有達到雙向鑑別，只有作 tag-to-reader 認證。在 UMP 認證中，當讀取器傳送挑戰值 r 給標籤時，標籤利用雙方通訊之秘鑰 *DID* 及標籤產品編碼 EPC_i 表明身分，再利用標籤秘鑰 b_i 作回應，並送出另一挑戰值 s 給讀取器；讀取器計算出 EPC_i 值後取得標籤秘鑰 b_i，可驗證是否為合法標籤所送出，再利用標籤秘鑰 b_i 及挑戰值 s 回應標籤，證明自己為合法之讀取器，以此進行雙向認證。
- 在所有權轉移方面，現任擁有者 P_i 若竊聽到繼任擁有者 P_{i+1} 的更新要求 (s, t)，也能利用密鑰 $b_{i,j}$ 計算得出 $b_{i+1,j}$，違反了向後安全。我們提出的作法為新的擁有者自行將要更新之秘密金鑰 b_i'' 及 DID_n 傳送到後端伺服器，由於此金鑰與前任擁有者所持金鑰無相關性，當秘鑰在標籤與後端伺服器進行同步更新後，前任擁有者無法自行計算出新的秘密金鑰，現任擁有者也無從得知前任擁有者之秘鑰，因此能有效的將所有權轉移給新的擁有者，前任擁有者便無法再對標籤進行存取，有效達到向前與向後安全。

表 3　相關研究之安全性比較表

	Liu 等人 所提機制	彭宇弘 所提機制	UMP 認證機制
無辨識能力	X	O	O
向前與向後安全	僅符合 向前安全	僅符合 向前安全	O
抵禦重送攻擊	X	O	O
雙向鑑別	X	X	O
抵禦非同步攻擊	O	O	O
不可追蹤性	X	X	O
受阻斷服務攻擊 之影響	小	小	小

伍、 結論

RFID 電子標籤具有非接觸、閱讀速率高等特點，在身分識別、物流方面有越來越多的應用，而目前在 RFID 技術的實際應用上，主要需考量的議題包含成本、安全性及隱私保護等方面。在成本方面，本論文使用 XOR 運算、雜湊函數及亂數產生器，且電

子標籤內僅儲存 EPC_i 、b_i 及 DID，因此所需計算量與儲存量不高，適用於記憶體容量小且價格低廉的被動式電子標籤。在安全性及隱私保護方面，我們使用隨機雜湊鎖結合挑戰回應機制達到雙向鑑別。另外，將每回合通訊之認證資訊加入隨值數作運算，使溝通訊息具隨機性且無關連性，達到不可追蹤。當讀取器與後端伺服器通訊時，讀取器之識別碼為每回合更新，可避免惡意讀取器對後端伺服器進行重送攻擊。

相較於 Liu 等人及彭宇弘所提的方法，如表 3 所示，我們增加了雙向鑑別機制、不可追蹤性及達到向前及向後安全等特點，有效提高 RFID 認證的安全性。

陸、 文獻探討

1. 白如珮、林詠章、曹世昌（2007 年 12 月）。基於所有權轉移特性並增進 RFID 安全協定之效能。「2007 全國計算機會議」，頁 492-499。
2. 呂崇富（2008 年 9 月）。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，頁 715-726。
3. 科技產業實驗室（2006）。RFID 標籤產量於 2010 年將成長 25 倍，取自：http://cdnet.stpi.org.tw/techroom/market/eerfid/rfid039.htm，上網日期：2012 年 1 月 5 日。
4. 彭宇弘（2011）。RFID 於供應鏈安全與隱私保護之研究。碩士論文，大同大學資訊工程研究所。
5. 葉慈章、劉耀元、吳建宏（2008 年 8 月）。RFID 的安全與隱私保護。明新學報，第 34 卷，第 2 期，頁 183-198。
6. 詹進科、陳育毅（2008）。RFID 概念與安全研究議題，取自：rfid.ctu.edu.tw/8_lab/20081210.pdf，上網期：2011 年 11 月 14 日。
7. Chevelle Fu（2011）。RFID 標籤終究獲得大型零售商青睞，取自：http://chinese.engadget.com/2011/02/10/item-level-rfids-get-support-from-big-retailers-track-your-ever/，上網日期：2011 年 12 月 27 日。
8. Liu, L., Chen, Z., Yang, L., Yi, Lu & Wang, H. (2010). Research on the Security Issues of RFID-based Supply Chain. International Conference on E-Business and E-Government, pp. 3267-3270.
9. Osaka, K., Takagi, T., Yamasaki, K., & Takahash, O. (2006). An Efficient and Secure RFID Security Method with Ownership Transfer. Computational Intelligence and Security, vol.2, pp. 1090-1095.
10. Weis, S.A., Sarma, S.E., Rivest, R., & Engels D.W. (2004). Security and privacy aspects of low-cost radio frequency identification systems. Proceedings of the 1st Security in Pervasive Computing, LNCS, vol.2802, pp. 201–212.
11. Zhang, L., Zhou, H., Kong, R., & Yang, F. (2005). An improved approach to security and privacy of RFID application system. in Proceedings of IEEE International Conference on Wireless Communications, Networking and Mobile Computing, pp.1195-1198.

A Study of Untraceability and Mutual Authentication in RFID Supply Chain System

HUNG-CHANG, LEE
Department of Information Management, Tamkang University
hclee@mail.im.tku.edu.tw

SHIN-YU, CHEN
Department of Information Management, Tamkang University
bo7778@gmail.com

Abstract

Radio Frequency Identity (RFID) has become more popular day after day in supply chain. However, because of its contact-less retrieval and substantial commercial interests in the supply chain, attackers would seek market intelligence or privacy over RFID. In order to protect commercial benefits, how to ensure the security of RFID system is extremely important.

In this paper, based on Liu's et al. and Yu-Hung Peng's schemes, we propose a more secure RFID authentication scheme. Proposed scheme add into the reader-to-tag authentication, which eliminate the possibility of hostile reader attack. Furthermore, by equipping hash lock method with random number, our scheme also supports untraceability. Security analysis indicates that the proposed scheme has the highest security.

Keywords: Radio Frequency Identity System (RFID), Supply Chain, untraceability, mutual authentication.