符合 EPC Class 1 Generation 2 的 RFID 向前安全性協定

葉慈章* 王志翔 吳家陞

明新科技大學資訊管理研究所

摘 要

RFID（Radio Frequency Identification）逐漸取代傳統條碼並廣泛地應用於日常生活中，消費者使用過含有標籤的物品後可能隨意丟棄，攻擊者取得標籤並破解內存的祕密訊息後，便可由過去的交易資料庫中辨識出與該標籤相關的記錄，追蹤該標籤或其持有者，此向前安全性將成為RFID應用上的重要議題。2008年Song與Mitchell學者提出具向前安全性的RFID協定，然而仍有假冒、DoS與追蹤的問題，且未能符合EPC Class 1 Generation 2標準。本研究將分析此協定，並提出改善以避免上述問題。

關鍵詞：無線射頻識別，向前安全性，隱私

A Forward-Secure RFID Protocol Conforming to EPC Class 1 Generation 2 Standard

Tzu-Chang Yeh*, Zhi-Xiang Wang, and Chia-Sheng Wu

Institute of Information Management, Minghsin University of Science and Technology

ABSTRACT

RFID (Radio Frequency Identification) is gradually replacing traditional barcode and is anticipated to be widely used in our daily life. Objects with embedded RFID tags can be carelessly discarded by consumers after being used. By acquiring an abandoned tag, an attacker can get the data stored in the tag and then identify its transaction records in the transaction database to track the tag or its owner. Therefore, forward secrecy will become a major issue of RFID in the near future. In 2008, Song and Mitchell proposed a RFID forward-secure protocol. However, we found that their protocol is vulnerable to attacks of impersonation, denial-of-service or tracking. Moreover, the protocol does not conform to EPC Class 1 Generation 2 standard. This paper analyzes what caused these weaknesses, and then a lightweight improved protocol is proposed to avoid the problems mentioned above.

Keywords: RFID, forward Secrecy, privacy

文稿收件日期 100.3.21.; 文稿修正後接受日期 101.3.6; * 通訊作者
Manuscript received March 21, 2011; revised March 6, 2012; * Corresponding author

一、前　言

無線射頻識別（Radio Frequency Identification, RFID）最早應用於二次世界大戰期間英國軍方的敵我辨識系統[1]。隨著標籤的成本下降、體積縮小，使得RFID的使用率大幅成長。ABI調查報告[2]指出，2010年RFID整體市場價值將達到53億美元，預期2014年將增加到82億美元，相當於未來五年內有14%的年複合成長率。RFID主要由標籤（Tag）、讀取器（Reader）和伺服器（Server）所組成，讀取器利用無線通訊的方式讀取標籤的內存訊息後，向伺服器查詢標籤的對應記錄。

由於 RFID 的訊息傳輸是透過無線通訊，在通訊過程中可能遭攻擊者的竊聽、重送、竄改等，產生安全上的問題。我們由相關文獻[3-6]整理出 RFID 常遇到的安全問題如下：

(1) 假冒攻擊（Impersonation Attack）：攻擊者透過重送或偽造訊息等方式假冒合法裝置以通過鑑別。
(2) 重送攻擊（Replay Attack）：攻擊者竊聽 RFID 傳送的訊息，於事後非法重送。
(3) 向前安全問題（Forward Secrecy Problem）：標籤日後若遭破解，攻擊者取得內存的祕密資訊後，可從過去竊聽儲存的交易資料庫中辨識出與該標籤相關的記錄，對標籤或持有者進行追蹤。
(4) 阻斷服務攻擊（Denial of Service Attack）：泛指 RFID 的訊息傳輸受到阻斷、癱瘓、攔截或竄改而無法正常運作。例如：利用物理方法，如法拉第遮罩阻斷標籤的讀取；傳送大量訊息給標籤或伺服器，造成系統癱瘓無法運作；攔截或竄改傳送的訊息，導致標籤與伺服器不同步而無法再通過鑑別進行通訊。
(5) 資訊隱私問題（Information Privacy Problem）：攻擊者利用非法讀取器讀取標籤內存訊息或竊聽傳輸的資訊，藉此得知個人身上攜帶的物品資訊，或分析其消費偏好等機密資訊。
(6) 追蹤攻擊（Tracking Attack）：藉由標籤回傳的可預期訊息以追蹤標籤或其持有者。

由於過去 RFID 的研究主要偏向固定式讀取器的傳統式架構，讀取器是透過有線網路連結伺服器，因此大部分研究都假設伺服器與讀取器間的通道為安全的。然而，近年來許多 RFID 裝置已配合實際作業需求改為行動式（稱為 mRFID，Mobile RFID），讀取器與伺服器間改為無線傳輸，容易遭攻擊者竊聽、重送、竄改等，產生安全上的問題。2009 年 Wang 與 Chin[7]指出當假設伺服器與讀取器間為非安全通道時會有安全上的問題。由於 RFID 標籤的低成本與便利性，使其逐漸取代傳統條碼並廣泛地應用於我們的日常生活中，然而消費者使用含有標籤的物品後可能隨意丟棄，攻擊者可以容易地取得標籤，再破解內存的祕密訊息，便可由過去的交易記錄中辨識出與該標籤相關者以進行追蹤，因此隨著 RFID 的普及，向前安全性將成為 RFID 應用上的重要議題。

RFID 的全面普及關鍵在於標籤成本的降低，2004 年國際標準組織 EPCglobal 針對低成本被動式 RFID 標籤發佈全球新標準 EPC Class 1 Generation 2（以下簡稱 Gen-2），Gen-2 並於 2006 年 2 月被納為 ISO 18000-6C 標準[8, 9]。

Gen-2 標籤由於成本的限制，無法支援雜湊函數、對稱式或非對稱式加密等複雜運算，僅支援擬亂數產生器(Pseudo-Random Number Generator, PRNG) 與循環冗餘碼 (Cyclic Redundancy Code, CRC)等簡單運算。過去許多滿足向前安全性的解決方案，大多需要複雜的運算，無法適用於 Gen-2；針對 Gen-2 提出的解決方案亦各有其安全上的問題。

我們將提出符合 Gen-2 標準的 RFID 向前安全性協定，以避免上述問題，且適用於 mRFID 的環境，無需假設伺服器與讀取器間為安全通道，使協定可應用於更高安全需求的環境。

二、具向前安全性之 RFID Gen-2 協定

目前文獻中提出具向前安全的 RFID 協定均透過每次標籤讀取後更新伺服器與標籤內存的共享金鑰的方式來達成向前安全性；更新的方法則可分為雜湊函數與亂數兩種，然而 Gen-2 標籤無法支援雜湊函數運算，因此我們將符合 Gen-2 標準且具向前安全性之 RFID 協定逐一分析說明如下：

— 2006 年 Peris-Lopez 等學者提出 UMAP 家

族協定[10-12]，假設讀取器與伺服器為同一端；利用簡單的位元運算 *XOR*、*OR*、*AND*、*Addition mod* 2^m 與亂數來保護資訊的傳送，以防止重送攻擊並達到向前安全性。然而，三個協定中的標籤皆無法驗證所收到訊息 *C* 的真確性；此外，由於亂數僅由讀取器單方產生，加上訊息是以明文傳送或保護不足，因此有阻斷服務攻擊、資訊隱私[13-15]與追蹤攻擊的問題。2007 年，Chien 與 Huang 學者再根據 Li 與 Wang 學者[14]和 Li 等學者[15]的假設與方法提出更有效率的攻擊方式[16]。

- 2007 年 Chien 學者針對 Peris-Lopez 等學者的 UMAP 家族協定[10-12]提出改善協定 SASI[17]，於標籤中儲存共享金鑰的新舊值，以避免更新不同步產生的阻斷服務攻擊；增加 *Rot*(*x*, *y*)函數的計算來保護資訊的傳送；但與 UMAP 家族協定相同，由於亂數僅由讀取器單方產生，加上訊息是以明文傳送或保護不足，因此仍有重送攻擊[18]、阻斷服務攻擊[18, 19]、資訊隱私與追蹤攻擊[19, 20]的問題。
- 2007 年 Le 等學者提出 O-FRAKE 協定[21]，將亂數與共享金鑰以亂數轉換函數轉換為五個亂數以保護資訊隱私、達到向前安全並避免重送攻擊；然而，若非法讀取器向標籤發送亂數或竄改步驟 1 傳送的訊息，或最後一個步驟遭竄改、攔截或遺失，將造成標籤與伺服器更新不同步而引起阻斷服務攻擊；此外，由於僅對標籤與伺服器進行鑑別，攻擊者可假冒合法讀取器讀取標籤後，向伺服器取得相對應的記錄。
- 2008 年 Peris-Lopez 等學者以 Chien 學者的 SASI 架構[17]為基礎，提出一個極輕量型的改善協定 Gossamer[22]。主要的改變是增加 *MIXBITS*(*x*, *y*)函數與 π 的計算來保護金鑰的傳送，使攻擊者無法經由未經授權的讀取器重送先前竊聽的通訊訊息以非法讀取標籤。然而，與 SASI 協定一樣有重送攻擊、阻斷服務攻擊與追蹤攻擊的問題。
- 2009 年 Peris-Lopez 等學者再以其提出的 UMAP 家族協定中之 LMAP[12]架構為基礎提出 ULAP 協定[23]，以改善其追蹤攻擊的問題；主要的改變是將步驟 2 傳送的 *IDS* 值（固定值）改以動態的 *SessionIDS* 取代—標籤接收到讀取器傳來的讀取請求與亂數 *challenge* 後，立即將 *challenge* 與內存的 *IDS* 計算出當次的 *SessionIDS*，使標籤每次回應的 *SessionIDS* 值皆不同，以避免追蹤的問題；然而此協定與 UMAP 家族協定相同—標籤皆無法驗證步驟 3 所收到的訊息 *C* 之真確性；此外，由於亂數僅由讀取器單方產生，加上訊息是以明文傳送或保護不足，因此與 LMAP 協定一樣有阻斷服務攻擊與追蹤攻擊的問題。

考慮上述協定的既有安全問題，我們將以 2008 年 Song 與 Mitchell 提出的協定[5]為基礎，提出符合 Gen-2 標準的 RFID 向前安全性協定，以避免上述問題。

三、2008 年 Song 與 Mitchell 學者的協定與分析

3.1 協定介紹

符號說明如下：

⊕	*XOR* 運算
r_1	由讀取器產生的亂數，長度為 L 位元
r_2	由標籤產生的亂數，長度為 L 位元
T_i	第 *i* 個標籤（$1 \le i \le N$）
t_i	第 *i* 個標籤內存的鑑別金鑰，供伺服器鑑別標籤
t_{i_new}	伺服器儲存的新鑑別金鑰，供伺服器鑑別標籤
t_{i_old}	伺服器儲存的舊鑑別金鑰，供伺服器鑑別標籤
t_i^*	當次通過鑑別的鑑別金鑰，值可能為 t_{i_new} 或 t_{i_old}
u_{i_new}	伺服器儲存的新存取金鑰，供標籤鑑別伺服器
u_{i_old}	伺服器儲存的舊存取金鑰，供標籤鑑別伺服器
u_i^*	當次通過鑑別的存取金鑰，值可能為 u_{i_new} 或 u_{i_old}
D_i	伺服器中第 *i* 個標籤所對應的記錄
$h(.)$	雜湊函數
$f_{ti}(M)$	以金鑰 t_i 對訊息 *M* 作雜湊函數計算作為訊息驗證碼
$M >> N$	將訊息 *M* 向右循環位移 N 個位元

M <<N　將訊息 M 向左循環位移 N 個位元
A→B　A 傳送訊息給 B

設備內存的資訊

標籤：t_i
伺服器：u_{i_new}, u_{i_old}, t_{i_new}, t_{i_old}, D_i

協定流程分為初始階段與鑑別階段，說明如下（圖 1）：

初始階段

運作前，廠商隨機產生亂數 u_0，標籤端設定 $t_0=h(u_0)$；伺服器端設定 $u_{i\_new}=u_0$、$t_{i\_new}=h(u_0)$、t_{i_old} 與 u_{i_old} 皆為空值。

鑑別階段

(1) *Reader* → *Tag*：r_1
讀取器產生亂數 r_1，並傳給標籤。

(2) *Tag* → *Reader*：M_1, M_2
標籤亦產生一個亂數 r_2，再計算 $M_1=t_i\oplus r_2$ 與 $M_2=f_{ti}(r_1\oplus r_2)$傳給讀取器。

(3) *Reader* → *Server*：M_1, M_2, r_1
讀取器將收到的 M_1、M_2 與步驟(1)產生的亂數 r_1 一起傳給伺服器。

(4) *Server* → *Reader*：D_i, M_3
伺服器收到讀取器傳來的資料後，進行下列運算：

- 將資料庫儲存的記錄逐筆帶入計算驗證，先以 t_{i_new} 與 M_1 作 *XOR* 取得 r_2'，再計算 M_2'=$f_{ti}(r_1\oplus r_2')$，若 M_2' 與自讀取器收到的 M_2 相同，則通過對標籤的鑑別並設定 $t_i^*=t_{i\_new}$、$u_i^*=u_{i\_new}$，若不一致，再改以 t_{i_old} 帶入，如通過鑑別則設定 $t_i^*=t_{i\_old}$、$u_i^*=u_{i\_old}$，若所有資料庫記錄皆未通過比對，表示未有對應的標籤記錄，則停止此次通訊。
- 計算 $M_3=u_i^*\oplus(r_2>>L/2)$，將 D_i 與 M_3 一起傳送給讀取器。
- 更新內存金鑰：$u_{i\_old}=u_i^*$、$t_{i\_old}=t_i^*$、$u_{i\_new}=(u_i^*<<L/4)\oplus(t_i^*>>L/4)\oplus r_1\oplus r_2$、$t_{i\_new}=h(u_{i\_new})$，供下次鑑別使用。

(5) *Reader* → *Tag*：M_3
讀取器將收到的 M_3 轉送給標籤後，標籤自行計算取出 $u_i^*=M_3\oplus(r_2>>L/2)$，並將 u_i^*經雜湊函數運算後與內存的 t_i 比對，若相同則完成對伺服器的鑑別，接著更新內存的金鑰 $t_i=h((u_i^*<<L/4)\oplus(t_i>>L/4)\oplus r_1\oplus r_2)$ 供下次鑑別使用。

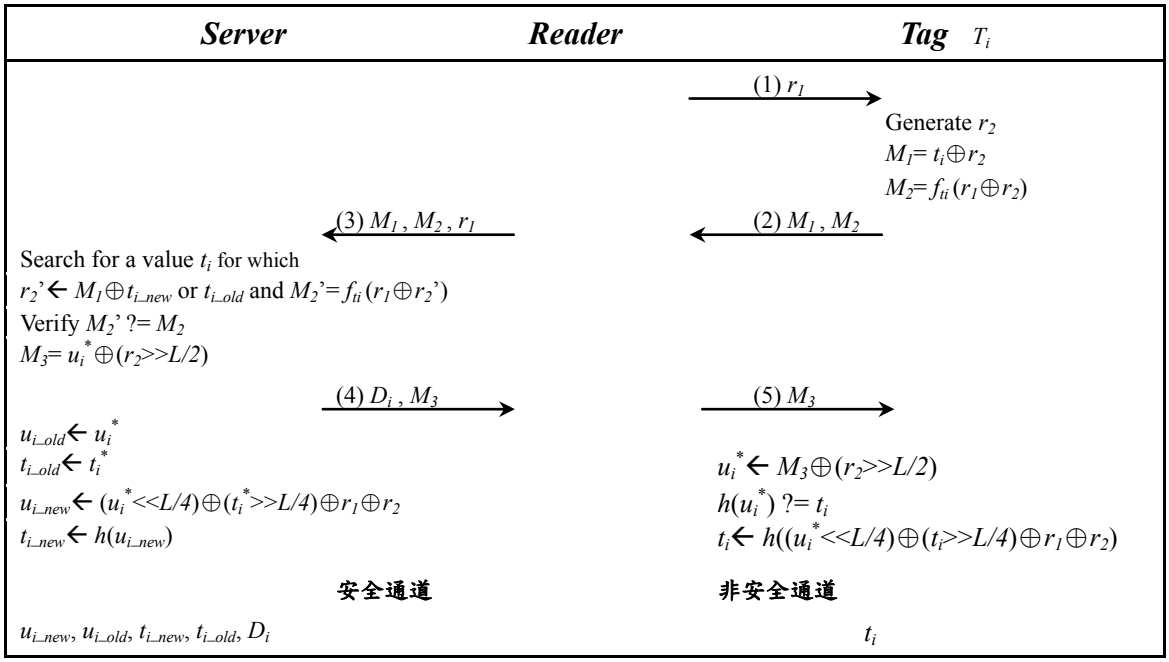

圖 1. 2008 年 Song 與 Mitchell 學者的協定

3.2 協定分析

(1) **假冒攻擊**：此協定有下列兩種假冒攻擊，詳細說明如下：

A. 中間人攻擊[24]

1. 攻擊者先假冒讀取器發出 $\bar{r}_1$ 給標籤，以獲取標籤計算的 $M_1=t_i\oplus r_2$ 與 $M_2=f_{ti}(\bar{r}_1\oplus r_2)$。
2. 攻擊者再假冒標籤，在收到讀取器發出的 r_1 後，計算 $\overline{M}_1=M_1\oplus\bar{r}_1\oplus r_1$ 與 $\overline{M}_2=M_2$ 回傳給讀取器。
3. 讀取器再將收到的 $\overline{M}_1$、$\overline{M}_2$ 與前步驟自己產生的 r_1 給伺服器。
4. 伺服器逐筆記錄帶入自行計算 $r_2'=\overline{M}_1\oplus t_i$ 與 $M_2'=f_{ti}(r_1\oplus r_2')$，$t_i$ 分別以 t_{i_new} 與 t_{i_old} 代入。

$$\begin{aligned}M_2'&=f_{ti}(r_1\oplus r_2')\\&=f_{ti}(r_1\oplus\overline{M}_1\oplus t_i)\\&=f_{ti}(r_1\oplus M_1\oplus\bar{r}_1\oplus r_1\oplus t_i)\\&=f_{ti}(t_i\oplus r_2\oplus\bar{r}_1\oplus t_i)\\&=f_{ti}(\bar{r}_1\oplus r_2)\\&=M_2=\overline{M}_2\end{aligned}$$

5. 接下來伺服器確認與收到的 $\overline{M}_2$ 相同，即通過對標籤的鑑別，以收到的 r_1 與 $\overline{M}_1$ 取出的 $r_2'=\overline{M}_1\oplus t_i=M_1\oplus\bar{r}_1\oplus r_1\oplus t_i=r_2\oplus\bar{r}_1\oplus r_1$ 來更新其內存的共享金鑰，並計算 $M_3=u_i*\oplus(r_2'>>L/2)$ 連同標籤的對應記錄 D_i 傳至讀取器，讀取器再將 M_3 傳給攻擊者。
6. 攻擊者收到 M_3 後，以先前收到的 r_1 與自己產生的 $\bar{r}_1$ 計算 $\overline{M}_3$，再假冒讀取器傳給標籤。

$$\begin{aligned}\overline{M}_3&=M_3\oplus[(r_1\oplus\bar{r}_1)>>L/2]\\&=u_i^*\oplus(r_2'>>L/2)\oplus(r_1\oplus\bar{r}_1>>L/2)\\&=u_i^*\oplus[(r_2\oplus\bar{r}_1\oplus r_1)>>L/2]\oplus[(r_1\oplus\bar{r}_1)>>L/2]\\&=u_i^*\oplus(r_2>>L/2)\end{aligned}$$

7. 標籤收到 $\overline{M}_3$ 後，計算 $u_i^*=\overline{M}_3\oplus(r_2>>L/2)=[u_i^*\oplus(r_2>>L/2)]\oplus(r_2>>L/2)=u_i^*$。由於標籤內存的 t_i 與自 $\overline{M}_3$ 取出的 u_i^* 皆為當次通訊所使用的共享金鑰，因此 $t_i=h(u_i^*)$，標籤通過對攻擊者（假冒讀取器）的鑑別後，即以收到的的 $\bar{r}_1$ 與自己產生的 r_2 更新共享金鑰 t_i（伺服器以 r_1 與 r_2' 更新共享金鑰），使得標籤與伺服器分別以不同的亂數進行更新，產生 DoS 攻擊問題。

B. 讀取器假冒[24-26]

1. 攻擊者先竊聽正常通訊過程中的資訊 r_{1_1}、M_{1_1}、M_{1_2}，並攔截 M_{1_3} 使標籤未更新內存的 t_i（M_{x_y}，x 代表第幾次通訊，y 代表該次通訊的訊息編號）。
2. 攻擊者再假冒讀取器啟動新的通訊，發出 $\bar{r}_{2\_1}$ 給標籤，標籤即產生亂數 r_{2_2} 並計算 $M_{2\_1}=t_i\oplus r_{2\_2}$ 與 $M_{2_2}=f_{ti}(\bar{r}_{2_1}\oplus r_{2_2})$回傳給攻擊者。
3. 攻擊者將標籤回傳的 M_{2_1} 與上次通訊竊聽的 M_{1_1} 與攔截的 M_{1_3} 計算出 $\overline{M}_{2\_3}$，再傳回給標籤。

$$\begin{aligned}\overline{M}_{2\_3}&=M_{1\_3}\oplus[(M_{1\_1}\oplus M_{2\_1})>>L/2]\\&=u_i^*\oplus(r_{1\_2}>>L/2)\oplus\{[(t_i\oplus r_{1\_2})\oplus(t_i\oplus r_{2\_2})>>L/2\\&=u_i^*\oplus(r_{1\_2}>>L/2)\oplus[(r_{1\_2}\oplus r_{2\_2})>>L/2]\\&=u_i^*\oplus(r_{1\_2}>>L/2)\oplus(r_{1\_2}>>L/2)\oplus(r_{2\_2}>>L/2)\\&=u_i^*\oplus(r_{2\_2}>>L/2)\end{aligned}$$

4. 因標籤在上次通訊結束時未更新內存的 t_i，標籤計算 $\overline{M}_{2\_3}\oplus(r_{2\_2}>>L/2)$ 取出的 u_i^* 與標籤的內存金鑰 t_i 皆屬於上次通訊使用的鑑別金鑰，因此 $h(u_i^*)=t_i$，標籤通過對攻擊者（假冒讀取器）的鑑別並更新內存的共享金鑰 t_i，然而伺服器因不知情而未更新內存金鑰，造成更新不同步而產生 DoS 問題。

(2) **重送攻擊**：每次讀取時，讀取器與標籤分別產生亂數 r_1 與 r_2 以保護機密訊息的傳送，使傳送的訊息 M_1、M_2、M_3 每次皆不同且無法預期，並於成功讀取後更新雙方的內存金鑰，因此攻擊者無法藉由重送之前竊得的訊息通過鑑別。

(3) **向前安全問題**：由於每次讀取時，資料的傳輸皆經由當次產生的亂數 r_1 與 r_2 作保護，標籤於每次鑑別完成後亦更新內存金

鑰 t_i，因此即使攻擊者攔截步驟(4)或(5)使標籤未進行更新，再破解標籤取得內存金鑰 t_i^*，也只能藉由 t_i^*與攻擊者竊聽儲存的交易記錄資料庫中每筆記錄的 M_1、M_2與 r_1，逐筆代入計算 $r_2'=M_1\oplus t_i^*$，再以 r_2'計算出 $f_{ti}*(r_1\oplus r_2')$，若與該筆記錄的 M_2一致，則可確認出標籤被破解前的最後一筆交易記錄。若欲辨識更早的交易紀錄，須先取得當次通訊的：

— 亂數 r_2，再從交易紀錄資料庫中逐筆代入計算 $t_i'=M_1\oplus r_2$，若 $f_{ti'}(r_1\oplus r_2)$等於 M_2。

或

— 鑑別金鑰 t_i，一樣從交易資料庫中逐筆代入計算 $r_2'=M_1\oplus t_i$，若 $f_{ti}(r_1\oplus r_2')$等於 M_2。

若一致則確認此筆記錄屬於此標籤。然而，每次通訊 r_2與 t_i皆非明文傳送，攻擊者無法在通訊過程中竊聽取得，因此可避免向前安全性的問題。

(4) **阻斷服務攻擊**：雖然伺服器有儲存鑑別金鑰的新舊值，可避免步驟(4)或(5)遭攔截所引起的 DoS，然而攻擊者仍可藉由前述的中間人攻擊或讀取器假冒的方式通過對方鑑別，引起阻斷服務攻擊。

(5) **資訊隱私問題**：每次鑑別時，讀取器與標籤均各產生亂數以保護資訊的傳送，避免資訊外洩。

(6) **追蹤攻擊**：2009 年 Peris-Lopez 等學者指出此協定有追蹤攻擊的問題[27]，攻擊者只需持續於通訊過程中進行竊聽，並攔截 M_3以避免標籤更新，即可利用 M_3與 M_1計算出的固定值 $M_3\oplus(M_1>>L/2)=[u_i*\oplus(r_2>>L/2)]\oplus[(t_i\oplus r_2)>>L/2]=u_i*\oplus(t_i>>L/2)$來追蹤標籤，但此攻擊只適用於標籤未正常更新內存金鑰的情況下。

(7) **假設伺服器與讀取器間為安全通道**：由於伺服器未鑑別讀取器，而且 D_i為明文傳送，因此此協定需假設伺服器與讀取器間為安全通道；然而目前許多的應用是使用手持式（行動式）讀取器透過無線通訊與伺服器連結，在空氣中傳輸的資料容易遭竊聽或篡改，攻擊者可假冒讀取器藉由重送步驟(3)騙取伺服器回傳標籤的對應紀錄 D_i，造成資訊洩漏。

(8) **Gen-2 標準**：由於使用 Gen-2 標準未支援的雜湊函數，因此未能應用於 Gen-2 標籤。

四、本研究提出的改善協定

由於 2008 年 Song 與 Mitchell 學者提出的協定[5]需假設伺服器與讀取器間為安全通道，並且因為 *XOR* 運算的特性[24]，使攻擊者可透過假冒攻擊引起阻斷服務攻擊[24-26]，以及通訊訊息間相互計算產生出的固定值引起之追蹤攻擊[27]；此外，因使用雜湊函數而未能符合 Gen-2 的標準。因此我們提出的改善協定增加讀取器的識別碼 *RID* 供伺服器鑑別讀取器，並保護標籤記錄 D_i的傳送，因此無需假設讀取器到伺服器間為安全通道。再將 M_2的計算方式由⊕改為 ‖ ，以及原協定 M_3中的 r_2以 *PRNG* 作保護，以避免因 *XOR* 計算的特性引起的假冒攻擊與追蹤攻擊，同時解決 DoS 的問題。此外，並將 Song 與 Mitchell 學者協定中使用的雜湊函數改為 *PRNG* 運算，以符合 Gen-2 的標準。

設備內存的資訊

標籤：t_i

讀取器：*RID*

伺服器：u_{i_new}, u_{i_old}, t_{i_new}, t_{i_old}, D_i, *RID*

本研究提出的改善協定流程如下（圖 2）：

初始階段

正式運作前，廠商作下列設定：

— 設定每個讀取器的 *RID*。

— 隨機產生亂數 u_0，標籤端設定 $t_i=PRNG(u_0)$；伺服器端設定 $u_{i\_new}=u_0$、$t_{i\_new}=PRNG(u_0)$，而 t_{i_old}與 u_{i_old}皆設為空值。

鑑別階段

(1) *Reader* → *Tag*：r_1

讀取器產生亂數 r_1，並傳給標籤作為挑戰值。

(2) *Tag* → *Reader*：M_1, M_2

標籤產生亂數 r_2，並計算 $M_1= t_i\oplus r_2$ 與 $M_2= PRNG(t_i \| r_1 \| r_2)$，再傳送給讀取器。

(3) *Reader* → *Server*：M_1, M_2, M_3, r_1

讀取器計算 $M_3=PRNG(RID \| r_1 \| M_1 \| M_2)$，連同收到的 M_1、M_2和自己產生的 r_1一併傳給伺服器。

(4) *Server* → *Reader*：*Info*, M_4, M_5

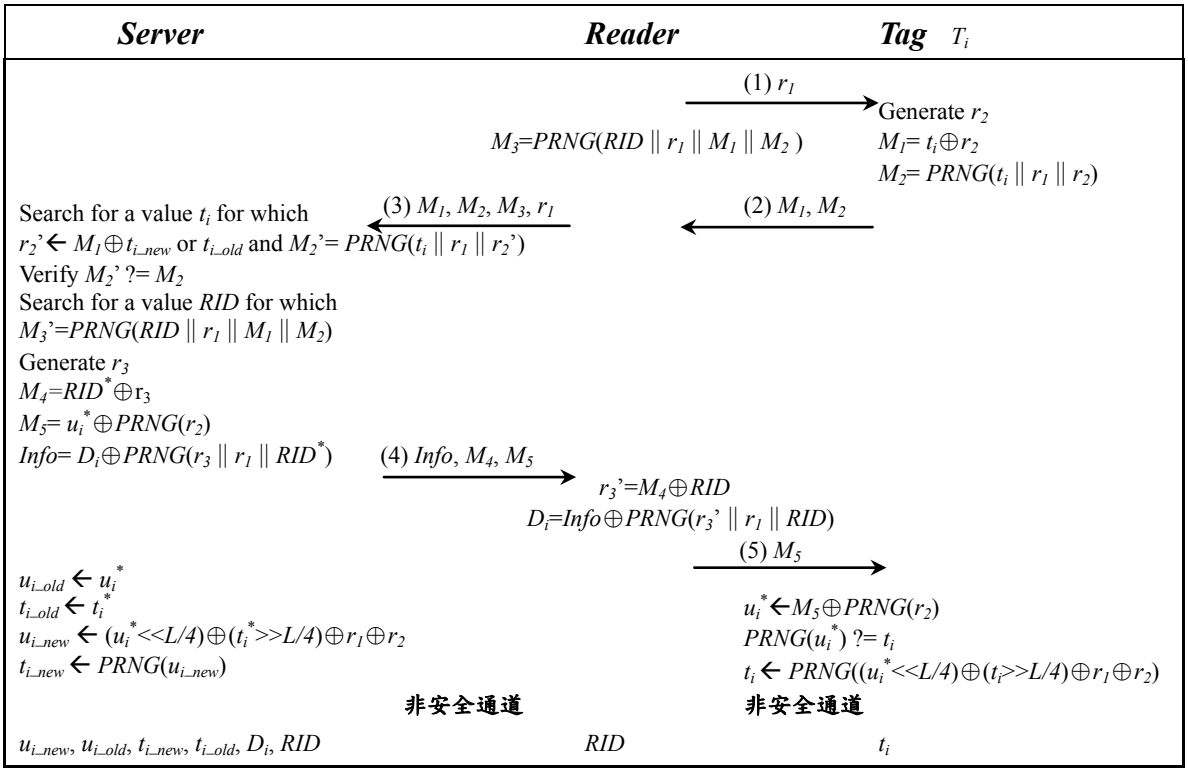

圖 2. 本研究提出的改善協定

伺服器收到讀取器傳來的資料後，進行下列步驟：

- 將儲存的標籤記錄逐筆帶入計算驗證，先以該筆記錄的 t_{i_new} 與 M_1 作 *XOR* 取得 r_2'，再計算 $M_2'= PRNG(t_i^* \| r_1 \| r_2')$，若 M_2'與自讀取器收到的 M_2 相同，則通過對標籤的鑑別並設定 $t_i^*=t_{i\_new}$、$u_i^*=u_{i\_new}$，若不一致，再改以 t_{i_old} 代入，如通過鑑別則設定 $t_i^*=t_{i\_old}$、$u_i^*=u_{i\_old}$，若所有資料庫記錄皆未通過比對，表示未有對應的標籤記錄或讀取器與標籤的通訊訊息遭竄改，則停止此次通訊。
- 將儲存的 RID 逐筆代入，計算 $M_3'=PRNG(RID \| r_1 \| M_1 \| M_2)$，若 M_3'與自讀取器收到的 M_3 相同，則確認出該讀取器 RID^*。若所有資料庫記錄皆未通過比對，表示未有對應的讀取器記錄或傳送訊息遭到竄改，則停止此次通訊。
- 產生亂數 r_3，計算 $M_4=RID \oplus r_3$、$M_5=u_i^* \oplus PRNG(r_2)$ 與 $Info=D_i \oplus PRNG(r_3 \| r_1 \| RID^*)$，將 $Info$ 與 M_3 一起傳給讀取器。
- 更新內存金鑰：$u_{i\_old}=u_i^*$、$t_{i\_old}=t_i^*$、$u_{i\_new}=(u_i^* << L/4) \oplus (t_i^* >> L/4) \oplus r_1 \oplus r_2$、$t_{i\_new}= PRNG(u_{i\_new})$，供下次鑑別使用。

(5) *Reader* → *Tag*：M_5

讀取器收到 $Info$、M_4 與 M_5 後，將收到的 M_4 與內存的 RID 作 *XOR* 運算取出 r_3'，再將收到的 $Info$ 與 r_3'、自己產生的 r_1、內存的 RID 計算 $Info \oplus PRNG(r_3' \| r_1 \| RID)$計算取出 D_i，最後將 M_5 轉送給標籤。標籤將收到的 M_5 與步驟(2)中自行產生 r_2 計算 $PRNG(r_2) \oplus M_5$ 取出 u_i^*，再將 u_i^*作 *PRNG* 運算後與內存的 t_i 比對是否相同，若相符則完成對伺服器的鑑別，接著更新內存資料 $t_i= PRNG((u_i^* << L/4) \oplus (t_i >> L/4) \oplus r_1 \oplus r_2)$，供下次鑑別使用。

伍、改善協定的安全性分析

我們針對改善協定作各方面的分析如下：

(1) **假冒攻擊**：除了伺服器與標籤相互鑑別

外，我們增加 *RID* 以達到伺服器與讀取器的相互鑑別，以避免非法的讀取器由伺服器取得標籤的記錄；此外將 M_2 中的⊕改為 ‖ ，並將 M_5（原協定之 M_3）中的 r_2 以 *PRNG* 作保護，以避免假冒攻擊。

(2) **重送攻擊**：每次讀取時，讀取器、標籤與伺服器分別產生亂數 r_1、r_2 與 r_3 以保護當次訊息傳輸的機密性，使回傳的訊息 M_1、M_2、M_3、M_4、M_5 與 *Info* 每次皆不同且無法預期，並於成功讀取後更新雙方的內存金鑰，因此攻擊者無法藉由重送之前竊得的訊息以通過鑑別。即使步驟(3)遭重送，但因攻擊者無法得知讀取器的 *RID*，因此無法取出標籤的記錄 D_i。

(3) **向前安全問題**：與 2008 年 Song 與 Mitchell 的協定相同，由於每次讀取時資料的傳輸皆經由當次產生的亂數作保護，標籤與伺服器於每次鑑別完成後亦更新內存金鑰。即使攻擊者攔截 M_5 使標籤未進行更新，再破解標籤取得鑑別金鑰 t_i^*，也只能辨識出破解標籤前的一筆交易記錄。若欲辨識出更早的交易記錄，則須先取得當次通訊的亂數 r_2 或鑑別金鑰 t_i，然而 r_2 與 t_i 皆非明文傳送，因此可避免向前安全性的問題。

(4) **阻斷服務攻擊**：幾位學者針對 2008 年 Song 與 Mitchell 協定提出的假冒攻擊，皆是因為 *XOR* 運算的特性而導致假冒攻擊，進而產生阻斷服務攻擊，因此我們提出的改善協定將 M_2 中的⊕改為 ‖ ，並將 M_5（原協定 M_3）中的 r_2 以 *PRNG* 作保護，以避免 *XOR* 運算的特性造成的問題。

(5) **資訊隱私問題**：每次鑑別時，伺服器、讀取器與標籤均各產生亂數 r_1、r_2 與 r_3，並增加讀取器識別碼 *RID* 以保護資訊的傳送。

(6) **追蹤攻擊**：由於 Song 與 Mitchell 學者提出的協定中，在標籤未正常更新前將 M_1 與 M_3 作運算將為固定值，攻擊者可藉此作追蹤。因此我們將 M_5 中的 r_2 以 *PRNG* 運算作保護，使 M_1 與 M_5 即使在金鑰未更新前作 *XOR* 運算也不會產生固定值，以防止追蹤攻擊。

(7) **假設伺服器與讀取器間為安全通道**：本研究為了使協定能應用於 mRFID 環境，因此假設讀取器至伺服器之間為非安全通道。為了避免資訊洩漏，增加伺服器對讀取器的鑑別並保護標籤紀錄 D_i 的傳送，即使攻擊者取得 *Info* 與 M_4，因無 *RID* 未能計算取出亂數 r_3，因此無法取得標籤相關記錄 D_i。

(8) **Gen-2 標準**：僅使用 Gen-2 標準支援的 *PRNG* 與 *XOR* 等運算，因此符合 Gen-2 標準。

我們將具向前安全性的 Gen-2 RFID 協定進行分析比較，整理於表 1。

六、結　論

隨著 RFID 的普及，向前安全性成為 RFID 應用上的重要議題；然而，Gen-2 標籤受限於計算能力與容量，無法支援複雜的密碼學運算。我們以 Song 與 Mitchell 學者的協定為基

表 1. 具向前安全性的 Gen-2 RFID 協定比較分析

	UMAP 家族協定	SASI 協定	Le 等學者的協定	Gossamer 協定	S-M 協定	ULAP 協定	本研究
假冒攻擊	X	O	O	O	X	X	O
重送攻擊	O	X	O	X	O	O	O
向前安全問題	O	O	O	O	O	O	O
阻斷服務攻擊	X	X	X	X	X	X	O
資訊隱私問題	X	X	O	X	O	X	O
追蹤攻擊	X	X	O	X	X	X	O
讀取器與伺服器間需為安全通道	需要	需要	不需要	需要	需要	需要	不需要
Gen-2 標準	符合	符合	符合	符合	不符合	符合	符合

礎，僅使用 Gen-2 支援的簡單運算，於每次標籤讀取後利用亂數更新伺服器與標籤內存的共享金鑰以達成向前安全性；並保護讀取器與伺服器間的資訊傳送，因此無需假設其為安全通道；同時仔細分析 XOR 的運算特性以避免可能引起的安全問題，提出符合 Gen-2 標準的 RFID 向前安全性協定，有效地提升 RFID 應用的安全性，讓消費者可以更安心地享受 RFID 技術所帶來的便利。

誌　謝

本研究承蒙行政院國家科學委員會計畫（編號：NSC 100-2410-H-159-003）經費之補助，謹此誌謝。

參考文獻

[1] Roberts, C. M., “Radio Frequency Identification (RFID),” Computers & Security, Vol. 25, No. 1, pp. 18-26, 2006.

[2] ABI Research, “RFID Market to Reach $5.35 Billion This Year,” avaliable at http://www.abiresearch.com/press/1618-RFID+Market+to+Reach+$5.35+Billion+This+Year, Nov 2010.

[3] Ohkubo, M., Suzuki, K., and Kinoshita, S., “RFID Privacy Issues and Technical Challenges,” Communications of the ACM, Vol. 48, No. 9, pp. 66-71, 2008.

[4] Rotter, P., “A Framework for Assessing RFID System Security and Privacy Risks,” Pervasive Computing IEEE, Vol. 7, No. 2, pp. 70-77, 2008.

[5] Song, B. and Mitchell, J. C., “RFID Authentication Protocol for Low-Cost Tags,” in Proceedings of the First ACM Conference on Wireless Network Security, pp. 140-147, 2008.

[6] Chen, Y., Chou, J. S., and Sun, H. M., “A Novel Mutual Authentication Scheme Based on Quadratic Residues for RFID Systems,” Computer Networks, Vol. 52, No. 12, pp. 2373-2380, 2008.

[7] Wang, C. H. and Chin, S., “A New RFID Authentication Protocol with Ownership Transfer in an Insecure Communication Environment,” Hybrid Intelligent Systems, pp. 486-491, 2009.

[8] EPCglobal Inc., "EPCTM Radio-Frequency Identity Protocols Class-1 Generation-2 UHF RFID Protocol for Communication at 860 MHz-960 MHz Version 1.0.9," 2005.

[9] EPCglobal Inc., "EPCglobal Tag Data Standards Version 1.4," 2005.

[10] Peris-Lopez, P., Hernandez-Castro, J. C., Estevez-Tapiador, M. J., and Ribagorda, A., “M^2AP : A Minimalist Mutual-Authentication Protocol for Low-Cost RFID tags,” LNCS, Vol. 4159, pp. 912-923, 2006.

[11] Peris-Lopez, P., Hernandez-Castro, J. C., Estevez-Tapiador, M. J., and Ribagorda, A., “EMAP: An Efficient Mutual-Authentication Protocol for Low-Cost RFID Tags,” LNCS, Vol. 4277, pp. 352-361, 2006.

[12] Peris-Lopez, P., Hernandez-Castro, J. C., Estevez-Tapiador, M. J., and Ribagorda, A., “LMAP: A Real Lightweight Mutual Authentication Protocol for Low-Cost RFID Tags,” in Proceedings of the Second Workshop on RFID Security, 2006.

[13] Li, T. and Deng, R., “Vulnerability Analysis of EMAP-An Efficient RFID Mutual Authentication Protocol,” in Proceedings of the Second International Conference on Availability, Reliability and Security, pp. 238-245, 2007.

[14] Li, T. and Wang, G., “Security Analysis of Two Ultra-Lightweight RFID Authentication Protocols,” in Proceedings of the IFIP-New Approaches for Security, Privacy and Trust in Complex Environments, Vol. 232, pp. 109-120, 2007.

[15] Li, T., Wang, G., and Deng, R. H., “Security Analysis on a Family of Ultra-lightweight RFID Authentication Protocols,” Journal of Software, Vol. 3, No. 3, 2007.

[16] Chien, H. Y. and Huang, C. W., “Security of Ultra-Lightweight RFID Authentication Protocols and Its Improvements,” SIGOPS Operating Systems Review, Vol. 41, No. 2, pp. 83-86, 2007.

[17] Chien, H. Y., “SASI: A New Ultralightweight RFID Authentication Protocol Providing Strong Authentication and Strong Integrity,” in Proceedings of the

IEEE Transactions on Dependable and Secure Computing, Vol. 4, No. 4, pp. 337-340, 2007.

[18] Sun, H. M., Ting, W. C., and Wang, K. H., "On the Security of Chien's Ultralightweight RFID Authentication Protocol," IEEE Transactions on Dependable and Secure Computing, Vol. 8, No. 2, pp. 315-317, 2009.

[19] Cao, T. J., Bertino, E., and Lei, H., "Security Analysis of the SASI protocol," IEEE Transactions on Dependable and Secure Computing, Vol. 6, No. 1, pp. 73-77, 2009.

[20] Phan, R. C. W., " Cryptanalysis of New Ultralightweight RFID Authentication Protocol-SASI," IEEE Transactions on Dependable and Secure Computing, Vol. 6, No. 4, pp. 316-320, 2008.

[21] Le, T. V., Burmester, M., and Medeiros, B. D., "Universally Composable and Forward-Secure RFID Authentication and Authenticated Key Exchange," in Proceedings of the Second ACM Symposium on Information, pp. 242-252, 2007.

[22] Peris-Lopez, P., Hernandez-Castro, J. C., Estevez-Tapiador, J. M., and Ribagorda, A., "Advances in Ultralightweight Cryptography for Low-cost RFID Tags: Gossamer Protocol," In Proceedings of the workshop on Information Security Applications, LNCS, Vol. 5379, pp. 56-68, 2008.

[23] Peris-Lopez, P., Hernandez-Castro, J. C., Estevez-Tapiador, J. M., and Ribagorda, A., "An Ultra Light Authentication Protocol Resistant to Passive Attacks under the Gen-2 Specification," Journal of Information Science and Engineering, Vol. 25, No. 1, pp. 33-57, 2009.

[24] Cai, S., Li, Y., Li, T., and Deng, R., "Attacks and Improvements to an RFID Mutual Authentication Protocol and its Extensions," In Proceedings of the Second ACM Conference on Wireless Network Security — WiSec'09, pp. 51-58, 2009.

[25] Van Deursen, T., Mauw, S., Radomirovic, S., and Vullers, P., "Secure ownership and ownership transfer in RFID systems," LNCS, Vol. 5789, pp. 637-654, 2009.

[26] Rizomiliotis, P., Rekleitis, E., and Gritzalis, S., "Security analysis of the Song-Mitchell authentication protocol for low-cost RFID tags," Communications Letters, Vol. 13, No. 4, pp. 274-276, 2009.

[27] Peris-Lopez, P., Hernandez-Castro, J. C., Estevez-Tapiador, M. J., Li, T., and Li, Y., "Vulnerability analysis of RFID protocols for tag ownership transfer," Computer Networks, pp. 1502-1508, 2010.