RFID EPC Class-1 Generation-2 標準協定之改善

葉慈章* 羅仕京

明新科技大學資訊管理研究所

摘 要

無線射頻辨識(Radio Frequency Identification, RFID)系統由於具有遠距離自動辨識的能力，逐漸取代傳統條碼成為新一代的電子標籤，然而由於透過空氣傳輸的資料容易遭到竊聽、攔截或竄改，因此產生許多安全與隱私的問題。

EPC Class-1 Generation-2 是低成本被動式標籤的全球新標準，由於標籤的運算能力有限無法進行複雜的運算。2009 年 Choi 等人針對此標準協定提出改善，以避免其資訊洩漏與重送攻擊的問題；然而我們發覺 Choi 等人的協定仍有追蹤攻擊、向前安全攻擊與阻斷服務攻擊等問題，本研究將詳細分析此協定，並提出改善以避免上述的問題，使消費者能安心的享受 RFID 帶來的便利。

關鍵詞：無線射頻辨識，EPC Class-1 Generation-2，安全，鑑別

Improvement on Standard Protocol of RFID EPC Class-1 Generation-2

Tzu-Chang Yeh* and Shih-Ching Lo

Institute of Information Management, Minghsin University of Science and Technology

ABSTRACT

RFID, capable of remote automatic identification, is taking the place of barcodes to become electronic tags of the new generation. However, the information transmitted in the air could easily be eavesdropped, interrupted or modified due to its radio transmission nature. On top of this, its prevalence has brought the stress on its security and privacy issues.

EPC Class-1 Generation-2, a new global standard for passive tags, has limited computation and memory capacity due to its implementation cost constraint. In 2009, Choi et al. proposed an improved protocol to avoid information leakage and replay attacks which the standard suffers from. However, we found that their protocol is still vulnerable to tracking attacks, forward secrecy attacks and denial of service attacks. This paper will give demonstrations on what have caused these weaknesses, and more of that, an improved protocol is proposed to avoid the problems mentioned above. That allows consumers to enjoy the technological convenience brought by RFID.

Keywords: RFID, EPC Class-1 Generation-2, security, authentication

文稿收件日期 100.9.8; 文稿修正後接受日期 101.12.6;*通訊作者
Manuscript received September 8, 2011; revised December 6, 2012; *Corresponding author

一、前　言

無線射頻辨識(Radio Frequency Identification, RFID)系統由標籤、讀取器與後端伺服器組成，讀取器以無線射頻的方式讀取標籤的內存資訊，再以此資訊自後端伺服器查詢標籤的對應記錄；RFID 具有遠距離自動辨識的能力，最早應用於第二次世界大戰時的敵我辨識系統以避免誤擊[1]，目前已廣泛地應用於供應鏈管理、物流管理、動物追蹤、醫療保健、門禁系統、非接觸式信用卡及電子收費系統等各種領域，逐漸取代傳統條碼成為新一代的電子標籤，大幅降低人為疏失並有效提升效率。

由於 RFID 是透過無線射頻進行辨識，在空氣中傳輸資料時容易遭到竊聽、攔截或竄改而產生許多安全問題，我們由相關文獻[1-9]整理出 RFID 常遇到的安全問題如下：

(1) 資訊洩漏(Information Leakage)：攻擊者使用未經授權的讀取器非法讀取標籤或藉由竊聽通訊訊息以取得相關的內存機密資料。
(2) 重送攻擊(Replay Attack)：攻擊者藉由竊聽取得傳輸的資訊，於事後非法重送，以假冒合法裝置通過鑑別。
(3) 追蹤攻擊(Tracking Attack)：藉由標籤傳出的可預期訊息追蹤標籤或其持有者的位置。
(4) 向前安全攻擊(Forward Secrecy Attack)：攻擊者破解標籤取得內存資訊後，再由過去的交易記錄中辨識出與該標籤相關者。
(5) 阻斷服務攻擊(Denial of Service Attack)：指 RFID 的訊息受到阻斷、癱瘓、攔截或竄改，造成系統無法正常運作。例如：使用法拉第遮罩阻斷通訊訊息；傳送大量訊息給標籤或讀取器，使系統癱瘓無法正常運作；攔截或竄改通訊訊息，使標籤與後端伺服器不同步而無法通過鑑別。

RFID 標籤根據是否內建電源區分為以下三類[1, 2, 8]：

(1) 被動式標籤(Passive Tag)：本身不具備電源，透過讀取器傳送的無線電波來產生感應耦合電流以回傳內存資訊，標籤體積較小、成本低、但傳輸距離短；主要應用於動物晶片、物流管理、門禁系統和汽車防盜等。
(2) 主動式標籤(Active Tag)：本身具備電源，主動發送內存資訊，傳輸距離較遠，讀取速度較快、體積大、成本較高；主要應用於高價品，如軍事、醫療等。
(3) 半被動式標籤(Semi-Passive Tag)：本身具備的電源僅供標籤內部的運作，仍需透過讀取器傳送的無線電波來產生感應耦合電流以回傳內存資訊；主要應用於偵測環境的變化。

RFID 的普及需要靠成本的降低，2004 年 EPCglobal 發佈低成本被動式標籤的全球新標準 EPC Class-1 Generation-2 (以下簡稱 Gen-2)，並於 2006 年被納為 ISO18000-6C 標準[10]，其主要特性如下[3, 4, 6, 7, 10]：

(1) 頻率介於 860MHz 至 960MHz，讀取距離最遠達 6 公尺。
(2) 僅支援擬亂數產生器(Pseudo-Random Number Generator, PRNG)與循環冗餘碼(Cyclic Redundancy Code, CRC)。
(3) 可選擇性儲存存取密碼(Access Password)，使用者需輸入此密碼以對標籤進行存取，以防止未授權的存取。
(4) 具有銷毀密碼(Kill Password)，標籤收到此密碼後，將停止所有功能，使讀取器無法再讀取標籤，以保護安全與隱私問題。
(5) 標籤記憶體區分為下列四個部分：
  - 保留記憶體(Reserved memory)：儲存存取密碼及銷毀密碼。
  - EPC 記憶體(EPC memory)：儲存每個物品唯一的 EPC 碼，包含產品製造商代碼、產品型號與序號。
  - TID 記憶體(TID memory)：如同網路卡的 MAC Address，每個標籤均有唯一的 TID 碼，包含標籤製造商代碼與序號。
  - 使用者記憶體(User memory)：儲存使用者的特定資訊。

Gen-2 標準協定的概要流程(圖 1)：讀取器需先傳送讀取請求 *Query* 給標籤，取得標籤回應的亂數 *RN16* 後再傳送包含 *RN16* 的 *ACK* 指令；標籤確認 *ACK* 指令包含的 *RN16* 為先前回應的 *RN16* 後，再回應內存的 *EPC* 碼等相關資訊；讀取器再以收到的資料向後端伺服

器查詢該標籤的對應記錄，接下來若需存取或銷毀標籤，則再傳送包含 *RN16* 的亂數請求 *ReqRN* 給標籤以取得其回應亂數 *handle*，讀取器再回傳 *Access Password*⊕*handle*(存取標籤) 或 *Kill Password*⊕*handle*(銷毀標籤)，接下來標籤將收到的資料與自行產生的 *handle* 作 XOR 計算取出的值若與內存的 *Access Password* 相同則開啟讀取權限，若與 *Kill Password* 相同則銷毀標籤。

低成本的 Gen-2 標籤由於運算能力有限，無法進行複雜的運算，因此仍存在資訊洩漏、重送攻擊、追蹤攻擊、向前安全攻擊與阻斷服務攻擊等問題[4, 6, 7]。

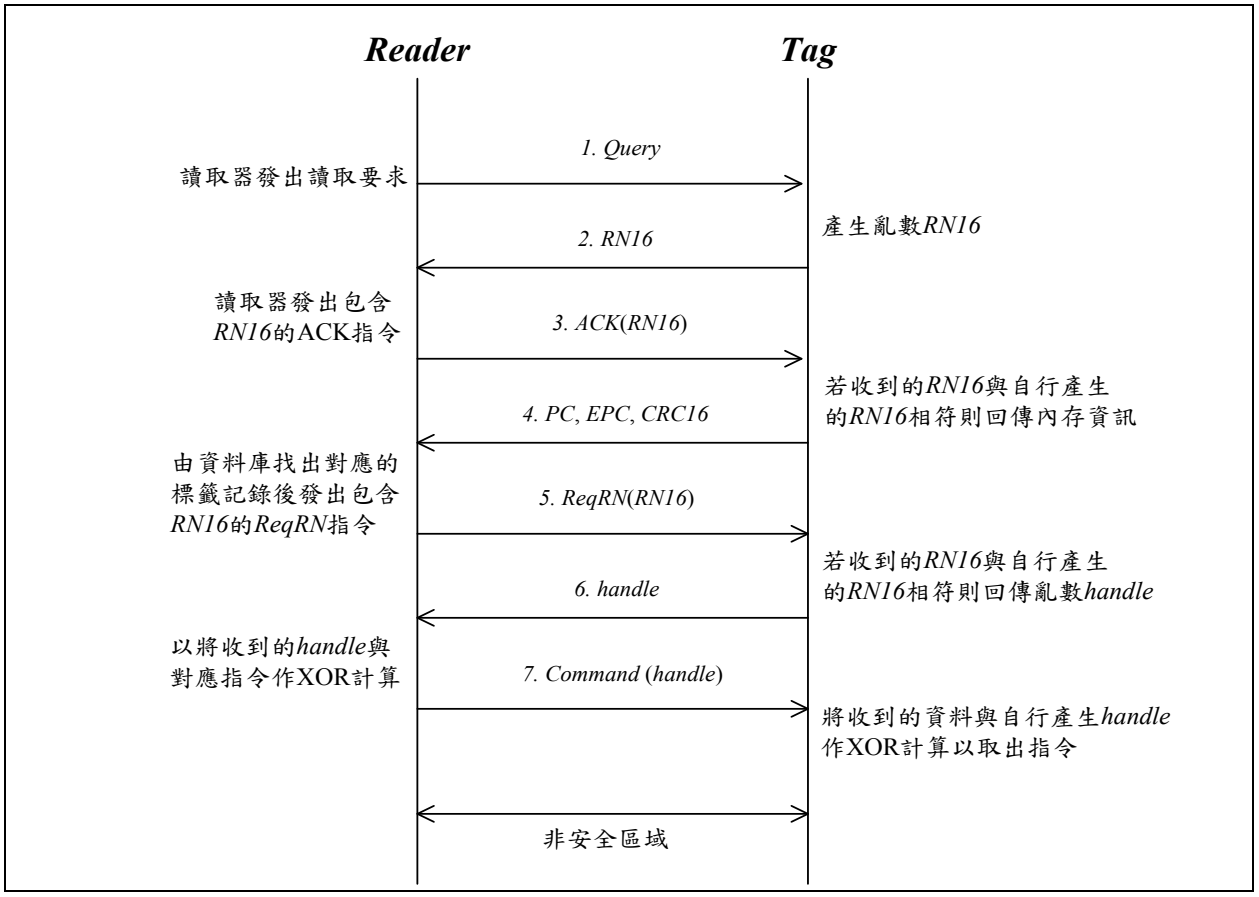

圖 1. EPC Class-1 Generation-2 標準協定流程

過去雖然有不少文獻提出適用於 RFID Gen-2 標籤的安全協定，然而這些協定多未遵循 Gen-2 既有的標準協定流程，接下來我們將針對以 Gen-2 的標準協定流程為基礎的文獻作探討。

2006 年 Kim 等人[6]最早針對 Gen-2 標準流程提出改善協定，藉由讀取器與標籤產生的當次亂數及後端伺服器與標籤的共享機密資訊來保護資訊的傳送，以解決資訊洩漏與追蹤攻擊，但 Deursen 與 Radomirovic 指出其有重送攻擊[4]，此外我們發現其亦有向前安全攻擊與阻斷服務攻擊等問題。

2009 年 Sun 與 Ting 等人[7]則在 Gen-2 中標籤傳送 EPC 碼前增加標籤對後端伺服器的鑑別，其餘流程不變，因此仍存在 Gen-2 所面臨的各種安全問題。

2009 年 Choi 等人[4]再提出 Gen-2 標準流程之改善協定，藉由後端伺服器與標籤共存的 *Access Password*、*Kill Password* 與 *TID* 相互鑑別身分，並避免明文傳送 EPC 碼，解決了資訊洩漏與重送攻擊的問題，然而我們發現其有追蹤攻擊、向前安全攻擊與阻斷服務攻擊等問題。

本研究將詳細分析 Gen-2 標準與 Choi 等

人協定的安全性，並提出改善，以避免上述問題，期望低成本的 Gen-2 標籤可以應用於高安全需求的環境，使消費者能安心的享受 RFID 帶來的便利。

二、Gen-2標準協定與分析

Gen-2標準協定的詳細流程說明如下：

(1) Reader→Tag：*Query*
讀取器傳送查詢請求 *Query* 給標籤。

(2) Tag→Reader：*RN16*
標籤產生亂數 *RN16* 回傳給讀取器。

(3) Reader→Tag：*ACK*(*RN16*)
讀取器傳送包含 *RN16* 的 *ACK* 指令回應給標籤。

(4) Tag→Reader：*PC*, *EPC*, *CRC16*
標籤收到的 *RN16* 若與步驟 2 傳出的 *RN16* 一致，標籤即進入應答狀態，並將內存訊息 *PC*、*EPC* 與 *CRC16* 回傳給讀取器。

(5) Reader→Tag：*ReqRN*(*RN16*)
讀取器傳送包含 *RN16* 的 *ReqRN* 指令回應給標籤。

(6) Tag→Reader：*handle*
標籤收到的 *RN16* 若與步驟 2 傳出的 *RN16* 一致，則回應亂數 *handle* 給讀取器。

(7) Reader→Tag：*Command*(*handle*)
讀取器傳送存取指令給標籤存取，*Command* 分為存取與銷毀兩類：

－存取：

若標籤存有 *Access Password* 且記憶體被鎖定，讀取器應先發送 *Access* 命令及 *Lock* 指令使標籤方可執行 *Read* 及 *Write* 等存取命令；若標籤未存有 *Access Password* 且記憶體被鎖定則省略標籤對讀取器的鑑別，讀取器僅需發送 *Lock* 命令解除標籤記憶體的鎖定即可進行存取，步驟如下：

(7-1) 讀取器將步驟 2 收到的 *RN16* 與後 16 位元的 *Access Password* 作 XOR 計算後，連同 *handle* 傳給標籤；由於 *Access Password* 是 32 位元，因此分為前 16 位元與後 16 位元作兩次處理。

(7-2) 標籤收到的 *handle* 若與步驟 6 傳出的 *handle* 一致，則以 *RN16* 與收到的 1/2 *Access Password*⊕*RN16* 作 XOR 計算取出後 1/2 *Access Password* 並回應相同的 *handle*。

(7-3) 讀取器再次傳送 *ReqRN*(*handle*)指令給標籤。

(7-4) 標籤收到的 *handle* 若與步驟 6 傳出的 *handle* 一致，則回應新的 *RN16*。

(7-5) 讀取器將新的 *RN16* 與前 16 位元的 *Access Password* 作 XOR 計算後連同 *handle* 傳送至標籤 (1/2 *Access Password*⊕*New RN16*, *handle*)。

(7-6) 標籤收到的 *handle* 若與步驟 6 傳出的 *handle* 一致，則以新的 *RN16* 與收到的 1/2 *Access Password* ⊕ *New RN16* 作 XOR 計算取出前 1/2 *Access Password*，若收到的與內存的 *Access Password* 兩者相同則回應相同的 *handle*。

(7-7) 讀取器傳送 *Lock* 命令連同 *handle* 傳送至標籤。

(7-8) 標籤收到的 *handle* 若與步驟 6 傳出的 *handle* 一致，則再次回應 *handle* 並對記憶體解除鎖定。

(7-9) 讀取器依需求傳送 *Read* 或 *Write* 等存取命令至標籤；*Read* 命令需指定讀取的記憶體區段連同 *handle* 傳送至標籤，標籤收到的 *handle* 若與步驟 6 傳出的 *handle* 一致則回傳指定區段的內存資訊；*Write* 命令則需再次執行 *ReqRN* 指令取得新的 *RN16*，再將欲寫入的資料與新的 *RN16* 作 XOR 計算後連同 *handle* 與指定區段位址傳送至標籤，標籤收到的 *handle* 若與步驟 6 傳出的 *handle* 一致，則以新的 *RN16* 與 Word to be written⊕ *New RN16* 作 XOR 計算取出欲寫入的資料並寫入指定區段。

－銷毀：

(7-1) 讀取器將步驟 2 收到的 *RN16* 與後 16 位元的 *Kill Password* 作 XOR 計算後連同 *handle* 傳給標籤 (1/2 *Kill Password*⊕*RN16*, *handle*)。

(7-2) 標籤收到的 *handle* 若與步驟 6 傳出的 *handle* 一致，則以 *RN16* 與收到的 1/2 *Kill Password*⊕*RN16* 作 XOR 計

算取出後 1/2 *Kill Password* 並回應相同的 *handle*(由於 *Kill Password* 是 32 位元，因此分為前 16 位元與後 16 位元分別與不同的 *RN16* 作 XOR 計算後傳送)。

(7-3) 讀取器再次傳送 *ReqRN*(*handle*)指令給標籤。

(7-4) 標籤收到的 *handle* 若與步驟 6 傳出的 *handle* 一致，則回應新的 *RN16*。

(7-5) 讀取器將新的 *RN16* 與前 16 位元的 *Kill Password* 作 XOR 計算後連同 *handle* 傳送至標籤(1/2 *Kill Password* ⊕*New RN16*, *handle*)。

(7-6) 標籤收到的 *handle* 若與步驟 6 傳出的 *handle* 一致，則以新的 *RN16* 與收到的 1/2 *Kill Password*⊕*New RN16* 作 XOR 計算取出前 1/2 *Kill Password*，若收到的與內存的 *Kill Password* 兩者相同則回應相同的 *handle* 並進入銷毀狀態。

我們由過去的相關文獻[2, 4, 7, 11-18]整理出Gen-2標準中的安全問題如下：

(1) 資訊洩漏：攻擊者透過竊聽合法通訊的訊息取得明文傳送的 *EPC* 碼，即可透過 EPCglobal 的 Object Naming Service[19]找出物品的相關資訊，影響使用者的隱私；此外，攻擊者將 *RN16* 與步驟 7 作 XOR 運算即可取得 *Access Password* 或寫入標籤的資料，之後即可假冒讀取器對標籤進行存取或取得標籤所更新的內存資訊。

(2) 重送攻擊：攻擊者藉由竊聽合法通訊，取得明文傳送的 *PC*、*EPC* 碼及 *CRC16*，接下來即可透過重送上述資訊以假冒合法標籤通過鑑別。

(3) 追蹤攻擊：攻擊者可使用非法讀取器讀取標籤或竊聽合法的通訊，由標籤以明文傳出的固定 *EPC* 碼來追蹤標籤或其持有者的位置。

(4) 向前安全攻擊：標籤日後若遭破解，攻擊者可取得標籤內存的 *EPC* 碼，即可由過去的交易記錄中辨識出該標籤的相關交易資訊。

(5) 阻斷服務攻擊：當步驟 7 為更新 *Access Password* 的 *Write* 命令時，若遭受攻擊者攔截或竄改，將造成後端伺服器已更新而標籤未更新，雙方因更新不同步，使下次通訊時，後端伺服器無法以更新後的 *Access Password* 通過標籤的鑑別。

三、Choi等人的Gen-2協定改善

Choi 等人針對 Gen-2 標準協定提出改善，加密保護訊息的傳送以改善 Gen-2 的資訊洩漏與重送攻擊。假設後端伺服器與讀取器之間為安全區域，而讀取器與標籤之間為非安全區域，符號說明如表 1。

表 1. 符號說明

符　號	說　明
⊕	XOR 運算
‖	資料串連
f(.)	擬亂數產生器(PRNG)
K	標籤的對稱式金鑰
EPC	標籤的電子產品碼
TID	後端伺服器與標籤共享的標籤唯一編號
C	以 *K* 為金鑰對 *EPC*‖*TID* 作加密，即 E_K(*EPC*‖*TID*)
I(*C*)	取 *C* 的前 96 位元資料，作為後端伺服器資料庫索引值，於出廠時寫入標籤
RR32	讀取器產生的亂數
RT32	標籤產生的亂數
Read(*TID*)	讀取標籤中 *TID* 記憶體位置的命令
Write(Reserved)	寫入標籤中 Reserved 記憶體位置的命令
Access Password	後端伺服器與標籤共享的存取密碼
Kill Password	後端伺服器與標籤共享的銷毀密碼
CRC16	循環冗餘碼

各設備內存資訊：

— 標籤：*TID*、*I*(*C*)、*Access Password*、*Kill Password*

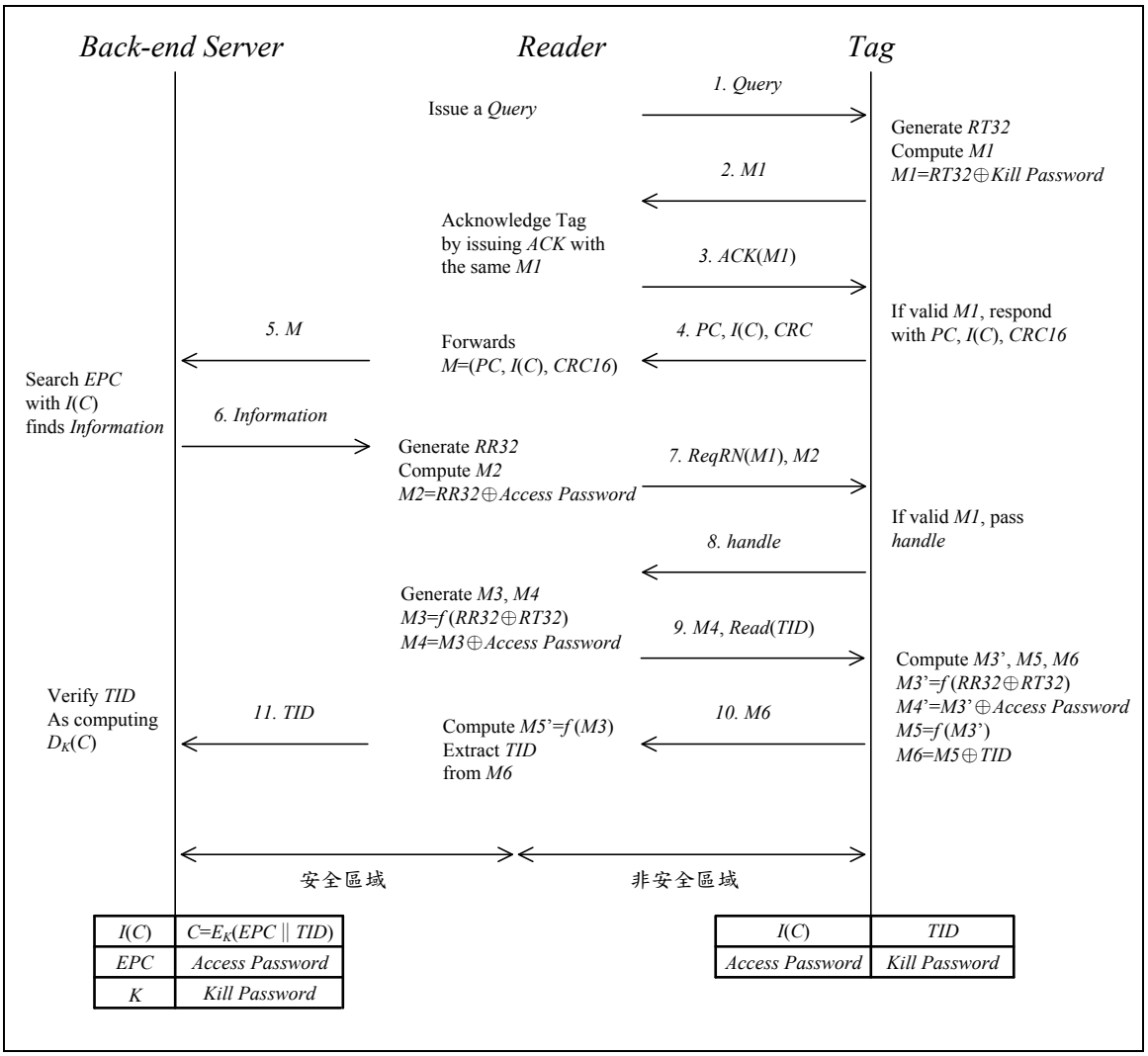

圖 2. Choi 等人的 RFID 協定

－ 後端伺服器：$I(C)$、EPC、$E_K(EPC \| TID)$、K、*Access Password*、*Kill Password*

協定流程如下(圖 2)：

(1) Reader→Tag：*Query*
讀取器傳送查詢請求給標籤。

(2) Tag→Reader：*M1*
標籤產生亂數 *RT32* 並計算 *M1=RT32*⊕*Kill Password* 回傳給讀取器。

(3) Reader→Tag：*ACK*(*M1*)
讀取器傳送包含 *M1* 的 *ACK* 回應給標籤。

(4) Tag→Reader：*PC*, *I*(*C*), *CRC16*
標籤由 *ACK* 指令中取出的 *M1*，若與步驟 2 傳出的 *M1* 一致，則將內存訊息 *PC*、*I*(*C*) 與 *CRC16* 回傳給讀取器。

(5) Reader→Back-end Server：*M*
讀取器以收到的資料打包成 *M*=(*PC*, *I*(*C*), *CRC16*)傳給後端伺服器。

(6) Back-end Server→Reader：*Information*
後端伺服器以 *I*(*C*)為索引值於資料庫中找出與標籤相對應的記錄，並回傳該標籤的 *Access Password* 與 *Kill Password* 給讀取器。

(7) Reader→Tag：*ReqRN*(*M1*), *M2*
讀取器產生亂數 *RR32*，並計算 *M2=RR32*⊕*Access Password*，再連同包含 *M1* 的 *ReqRN* 指令傳給標籤。

(8) Tag→Reader：*handle*
標籤由 *ReqRN* 指令中取出的 *M1*，若與步驟 2 傳出的 *M1* 一致，則將收到的 *M2* 與自己內存的 *Access Password* 作 XOR 計算取出 *RR32*，然後回應亂數 *handle* 給讀取器。

(9) Reader→Tag：*M4*, *Read*(*TID*)
讀取器將步驟 2 收到的 *M1* 與步驟 6 收到的 *Kill Password* 作 XOR 計算取出 *RT32*，

並與步驟 7 自行產生的 *RR32* 計算出 *M3*=*f*(*RR32* ⊕ *RT32*) 及 *M4*=*M3* ⊕ *Access Password*，然後傳送 *M4* 與 *Read*(*TID*)命令給標籤。

(10) Tag→Reader：*M6*
標籤將步驟 8 取出的 *RR32* 與步驟 2 自行產生的 *RT32* 計算出 *M3*'，再以 *M3*'與內存的 *Access Password* 計算出 *M4*'，若 *M4*'與自讀取器端收到的 *M4* 一致，則通過對讀取器的鑑別；接下來再計算 *M5*=*f*(*M3*')與 *M6*=*M5*⊕*TID*，並將 *M6* 傳給讀取器。

(11) Reader→Back-end Server：*TID*
讀取器自行計算 *M5*'=*f*(*M3*)，再與 *M6* 作 XOR 計算後取出 *TID* 傳給後端伺服器。後端伺服器以步驟 6 找到的標籤對應記錄中的 *K* 對 $E_K(EPC \| TID)$作解密取出 *TID*，若與自讀取器端收到的 *TID* 一致，則通過對標籤鑑別。

四、Choi等人協定的安全分析

我們針對 Choi 等人的協定就各方面的安全性詳細分析如下：

(1) 資訊洩漏：每次讀取時皆以當次亂數 *RT32* 與 *RR32* 保護訊息的傳送；此外，*EPC* 碼未以明文傳送，改傳送經加密保護之 *I*(*C*)，因此可避免資訊洩漏。

(2) 重送攻擊：步驟 4 標籤傳送的 *I*(*C*)未以亂數保護且為固定值，但攻擊者即使重送步驟 4 也無法假冒標籤通過讀取器的鑑別，因每次讀取時，皆以當次亂數 *RT32* 與 *RR32* 保護訊息的傳送，攻擊者無法取得 *TID*、*Access Password* 與 *Kill Password* 來計算步驟 2 與步驟 10 中標籤需送出的 *M1* 與 *M6*。

(3) 追蹤攻擊：標籤未鑑別讀取器的身分即於步驟 4 回傳 *I*(*C*)，由於 *I*(*C*)為固定值且未更新，因此攻擊者可以非法讀取器傳送 *Query* 給標籤以騙取其回傳的 *M1*，再以 *M1* 產生 *ACK*(*M1*)回傳給標籤，等標籤回應 *I*(*C*)，再藉此固定值來追蹤標籤或其持有者。

(4) 向前安全攻擊：若攻擊者破解標籤取得其內存資訊，可從過去的交易記錄資料庫中，逐筆記錄代入計算比對，將步驟 2 傳送的 *M1* 與內存 *Kill Password* 作 XOR 計算取出 *RT32*'，並將步驟 7 傳送的 *M2* 與 *Access Password* 作 XOR 計算取出 *RR32*'，再計算 *f*(*RR32*'⊕*RT32*')，若其值等於 *M4* 與 *Access Password* 作 XOR 計算出的 *M3*'，則可確認此筆交易記錄與該標籤有關。

(5) 阻斷服務攻擊：標籤更新 *Access Password* 時，若 *Write* 命令(新的 *Access Password*⊕*RN16*)遭到攔截或竄改，將造成標籤與後端伺服器更新不同步，使標籤無法再次通過鑑別。分別說明如下：
- 攔截：由於後端伺服器先更新內存資訊後才傳送 Write 命令給標籤，此命令若遭攔截將使標籤未更新內存資訊，造成雙方更新不同步。
- 竄改：因標籤收到的資料經過竄改，故標籤以 *RN16* 與收到的資料做 XOR 運算後會取出錯誤的新 Access Password，並以此做更新，造成與後端伺服器的更新不同步。

五. 本研究提出的改善協定

由於 Choi 等人傳送的 *I*(*C*)為固定值且未更新內存資訊，因此產生追蹤攻擊及向前安全攻擊的問題；因此本論文以亂數保護 *I*(*C*)的傳送並且更新雙方內存資訊以解決上述問題。

各設備內存資訊：
- 標籤：*TID*、*I*(*C*)、*Access Password*、*Kill Password*
- 後端伺服器：*I*(*C*)、*EPC*、$E_K(EPC \| TID)$、*K*、$Access\ Password_{\_new}$、$Access\ Password_{\_old}$、*Kill Password*

協定流程如下(圖 3)：

(1) Reader→Tag：*Query*
讀取器傳送查詢請求給標籤。

(2) Tag→Reader：*M1*
標籤產生亂數 *RT32* 並計算 *M1*=*RT32*⊕*Kill Password* 回傳給讀取器。

(3) Reader→Tag：*ACK*(*M1*)
讀取器傳送包含 *M1* 的 *ACK* 回應給標籤。

(4) Tag→Reader：*PC*, *N2*, *CRC16*
標籤由 *ACK* 指令中取出的 *M1*，若與步驟 2 傳出的 *M1* 一致，則與自行產生的 *M1*

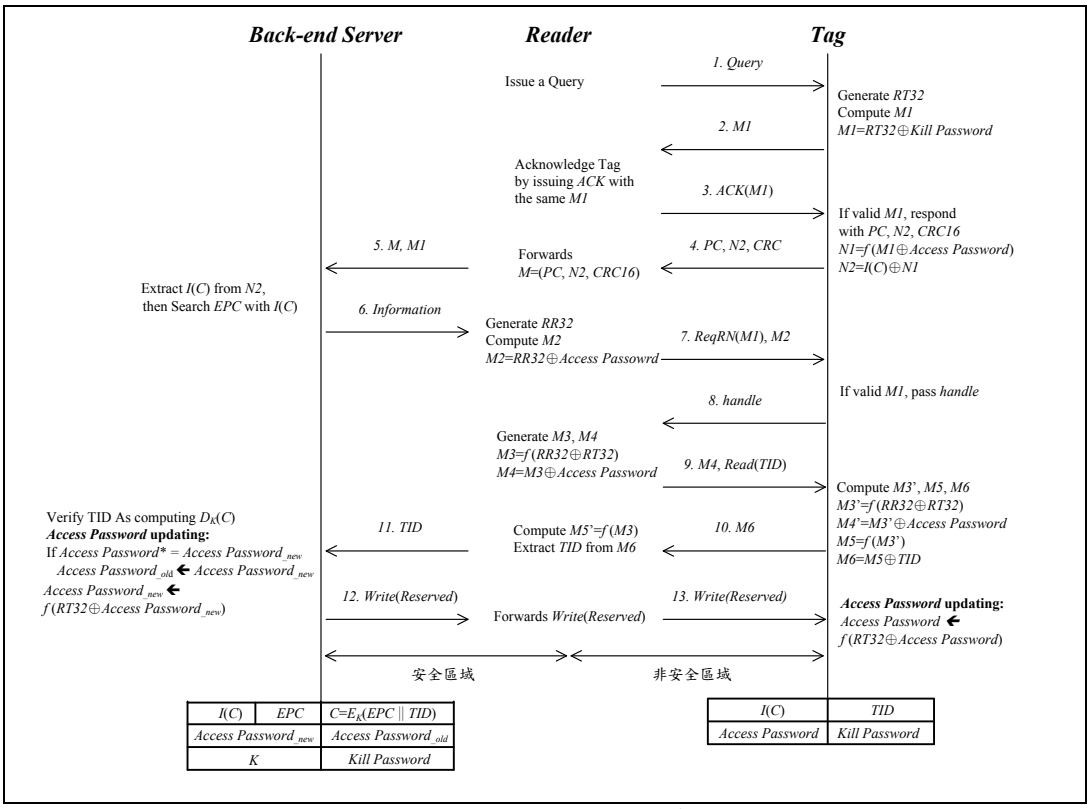

圖 3. 本研究提出的改善協定

計算 *N1=f*(*M1* ⊕ *Access Password*) 及 *N2=I*(*C*)⊕*N1*，並回傳 *PC*、*N2*、*CRC16* 至讀取器。

(5) Reader→Back-end Server：*M*, *M1*
讀取器以收到的資料打包成 *M*=(*PC*, *N2*, *CRC16*)並與 *M1* 一起傳給後端伺服器。

(6) Back-end Server→Reader：*Information*
後端伺服器先將資料庫中每筆標籤記錄的 *Access Password**與收到的 *M1* 逐筆運算出 *N1=f*(*M1*⊕*Access Password**)及 *N2=I*(*C*)⊕*N1*，若自行計算出的 *N2* 與自讀取器收到的 *N2* 相同，即確認出資料庫中標籤相對應的記錄，再回傳 *Access Password**與 *Kill Password* 至讀取器。(*Access Password**先以 *Access Password*$_{new}$ 代入，若未找到對應的記錄再以 *Access Password*$_{old}$ 代入)。

(7) Reader→Tag：*ReqRN*(*M1*), *M2* 讀取器產生亂數 *RR32*，並計算 *M2=RR32*⊕*Access Password*，再連同包含 *M1* 的 *ReqRN* 指令傳給標籤。

(8) Tag→Reader：*handle*
標籤由 *ReqRN* 指令中取出的 *M1*，若與步驟 2 傳送的 *M1* 一致，則將收到的 *M2* 與自己內存的 *Access Password* 作 XOR 計算取出 *RR32*，然後回應亂數 *handle* 給讀取器。

(9) Reader→Tag：*M4*, *Read*(*TID*)
讀取器將步驟 2 收到的 *M1* 與步驟 6 收到的 *Kill Password* 作 XOR 計算取出 *RT32*，並與步驟 7 自行產生的 *RR32* 計算出 *M3=f*(*RR32* ⊕ *RT32*) 及 *M4=M3* ⊕ *Access Password*，然後傳送 *M4* 與 *Read*(*TID*)命令至標籤。

(10) Tag→Reader：*M6*
標籤將步驟 8 取出的 *RR32* 與步驟 2 自行產生的 *RT32* 計算出 *M3*'，再以 *M3*'與內存的 *Access Password* 計算出 *M4*'，若 *M4*'與自讀取器端收到的 *M4* 相同，則通過對讀取器的鑑別。接下來再計算 *M5=f*(*M3*')與 *M6=M5*⊕*TID*，將 *M6* 傳給讀取器。

(11) Reader→Back-end Server：*TID*
讀取器自行計算 *M5*'=*f*(*M3*)，再與 *M6* 作 XOR 計算後取出 *TID* 傳給後端伺服器。

(12) Backend Server→Reader：*Write*(Reserved)
後端伺服器將步驟 6 中找到的標籤對應記錄，以 *K* 對 $E_K(EPC \| TID)$作解密取出 *TID*，若與自讀取器端收到的 *TID* 一致，則通過對標籤的鑑別。此時進入更新階段，若 *Access Password**=*Access Password*$_{new}$（即標籤通過後端伺服器鑑

別的 *Access Password* 值等於後端伺服器的 *Access Password*$_{new}$ 值) ，則將 *Access Password*$_{old}$ 更新為 *Access Password*$_{new}$；若 *Access Password**=*Access Password*$_{old}$，則不更新 *Access Password*$_{old}$；接下來將 *Access Password*$_{new}$ 更新為 *f*(*RT32* ⊕ *Access Password*$_{new}$)，之後傳送 *Write*(Reserved) 命令至讀取器。

(13) Reader→Tag：*Write*(Reserved)
標籤收到命令後將 *Access Password* 更新為 *f*(*RT32*⊕*Access Password*)。

六. 改善協定分析

我們針對改善協定各方面分析如下：

(1) 資訊洩漏：我們沿用 Choi 等人的協定 *EPC* 碼未以明文傳送，改傳送經加密保護之 *I*(*C*)，並以當次亂數 *RT32* 與 *RR32* 保護資訊的傳送，以防止資訊洩漏，使得每次傳送的訊息皆不同且無法預期，因此攻擊者無法藉由竊聽取得的資訊計算出內存資訊。

(2) 重送攻擊：與 Choi 等人協定相同，攻擊者無法透過重送資訊來假冒標籤通過讀取器的鑑別，因每次讀取時，皆以當次亂數 *RT32* 與 *RR32* 保護訊息的傳送，攻擊者無法取得 *TID*、*Access Password* 與 *Kill Password* 來計算步驟 2 與步驟 10 中標籤需送出的 *M1* 與 *M6*。

(3) 追蹤攻擊：由於 Choi 等人協定以明文傳送固定值的 *I*(*C*)且未更新，因此產生追蹤攻擊；我們的改善協定於步驟 4 中以當次亂數 *RT32*、*Kill Password* 與 *Access Password* 來保護 *I*(*C*)的傳送，因此每次傳送的值皆不同且無法預期，可避免追蹤攻擊。

(4) 向前安全攻擊：由於 Choi 等人協定並未於每次通訊後更新內存的資訊，因此有向前安全攻擊的問題；我們的改善協定於每次標籤讀取後以擬亂數產生器更新後端伺服器與標籤內存的 *Access Password*，使攻擊者無法藉由破解後得到的 *Access Password*，從資料庫中辨識出與該標籤相關的交易記錄。

(5) 阻斷服務攻擊：若 Choi 等人協定傳送的更新命令遭受攔截或竄改，將產生阻斷服務攻擊的問題；我們的改善協定於後端伺服器儲存 *Access Password* 的新、舊值，以避免後端伺服器與標籤更新 不同步而造成的阻斷服務攻擊。

表 2. 符合 Gen-2 標準流程之協定安全分析

	Kim 等人的協定	Sun 與 Ting 的協定	Choi 等人的協定	本研究提出 Choi 等人協定的改善
資訊洩漏	O	X	O	O
重送攻擊	X	X	O	O
追蹤攻擊	O	X	X	O
向前安全攻擊	X	X	X	O
阻斷服務攻擊	X	X	X	O
O：安全　X：非安全				

表 3. 符合 Gen-2 標準流程之協定效能分析

	Kim 等人的協定	Sun 與 Ting 的協定	Choi 等人的協定	本研究提出 Choi 等人協定的改善
標籤計算量	5 XOR 1 PRNG 1 Addition mod 2^m	1 Majority function	4 XOR 2 PRNG	7 XOR 4 PRNG
標籤內存資訊量	**Gen-2 標籤基本內存資訊** *EPC* 碼：96 位元、*Access Password*：32 位元、*Kill Password*：32 位元、*TID*：32 位元、共 192 位元			
	S：96 位元	*Keypool*：256 位元	以同為 96 位元的 *I*(*C*)取代 *EPC* 碼	以同為 96 位元的 *I*(*C*)取代 *EPC* 碼
	共 288 位元	共 448 位元	共 192 位元	共 192 位元

本研究將 Gen-2 標準流程的相關改善協定之安全分析與效能分析分別整理於表 2 與表 3；由於 Sun 與 Ting 的協定的目的僅在標籤傳送 *EPC* 碼前，增加對讀取器身分的鑑別，其他步驟均沿用 Gen-2 的流程，因此仍然存在 Gen-2 所面臨的安全問題。

Gen-2 標準支援密集讀取器模式(Dense Reader Mode)，以降低同時使用多個讀取器時

所造成的訊號碰撞，提升資訊讀取的準確性。本研究提出的改善協定雖能提升 Gen-2 標準協定的安全性，但增加了讀取器與標籤間的訊息傳輸次數以及標籤端的運算量，因此讀取器與標籤間的存取效能會稍受影響。

七. 結　論

RFID 已廣泛地應用於各種領域，然而由於透過空氣傳輸的資料容易遭到竊聽、攔截或竄改，產生了許多安全問題。RFID 的普及需要靠成本的降低，然而低成本的 Gen-2 標籤因運算能力有限無法進行複雜的運算，存在資訊洩漏、重送攻擊、追蹤攻擊、向前安全攻擊與阻斷服務攻擊等問題。2009 年 Choi 等人針對 Gen-2 標準提出改善協定，但其仍有追蹤攻擊、向前安全性與阻斷服務攻擊的問題；本研究詳細分析 Gen-2 標準與 Choi 等人協定的安全性，並提出改善，以避免上述問題，期望低成本的 Gen-2 標籤可以應用於高安全需求的環境，使消費者能安心的享受 RFID 帶來的便利。

誌　謝

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

參考文獻

[1] Roberts, C. M., “Radio frequency identification (RFID),” *Computers and Security*, Vol. 25, pp. 18-26, 2006.

[2] 陳昱仁、廖耕億、許建隆及林仲志，RFID 概論，鍾乾癸等(編)，台北：華泰文化，2009。

[3] Chien, H. Y. and Chen, C. H., “Mutual authentication protocol for RFID conforming to EPC Class 1 Generation 2 standards,” *Computer Standards and Interfaces*, Vol. 29, pp. 254-259, 2007.

[4] Choi, E. Y., Lee, D. H., and Lim, J. I., “Anti-cloning protocol suitable to EPCglobal Class-1 Generation-2 systems,” *Computer Standards and Interfaces*, Vol. 31, pp. 1124-1130, 2009.

[5] Deursen, T. and Radomirovic, S., “Attacks on RFID Protocols,” *Cryptology ePrint Archive*, pp. 1-56, 2008.

[6] Kim, K. H., Choi, E. Y., Lee, S. M., and Lee, D. H., “Secure EPCglobal Class-1 Gen-2 RFID System Against Security and Privacy Problems,” *Lecture Notes in Computer Science*, Vol. 4277, pp. 362-371, 2006.

[7] Sun, H. M. and Ting, W. C., “A Gen2-Based RFID Authentication Protocol for Security and Privacy,” *Transactions on Mobile Computing*, Vol. 8, pp. 1052-1062, 2009.

[8] Weinstein, R., “RFID: A Technical Overview and Its Application to the Enterprise,” *IEEE Computer Society*, pp. 27-33, 2005.

[9] Xiao, Q., Boulet, C., and Gibbons, T., “RFID Security Issues in Military Supply Chains,” *Second International Conference on Availability*, Reliability and Security (ARES'07), 2007.

[10] EPCglobal Inc., “EPC™ Radio-Frequency Identity Protocols Class-1 Generation-2 UHF RFID Protocol for Communication at 860 MHz-960 MHz Version 1.2.0,” Retrieved July. 2011, from http://www.gs1.org/gsmp/kc/epcglobal/uhfc1g2/uhfc1g2_1_2_0-standard-20080511.pdf, 2008.

[11] Burmester, M., Medeiros, B., Munilla, J., and Peinado, A., “Secure EPC Gen2 compliant Radio Frequency Identification”, *Lecture Notes in Computer Science*, Vol. 5793, pp. 227-240, 2009.

[12] Duc, D. N., Park, J., Lee, H., and Kim, K., “Enhancing security of EPCglobal GEN-2 RFID tag against traceability and cloning”, *Symposium on Cryptography and Information Security*, 2006.

[13] Kok, Guido R., RFID Jamming, Faculty of Electrical Engineering, Mathematics and Computer Science of the University of Twente, 2007.

[14] Lo, N. W. and Yeh, K. H., “A Secure Communication Protocol for EPCglobal Class 1 Generation 2 RFID Systems”, *IEEE Information Networking and Applications Workshops*, Vol. 10, pp. 562-566, 2010.

[15] Peris-Lopez, P., Hernandez-Castro, J. C., Estevez-Tapiador, J. M., and Ribagorda A.,

"LMAP: A Real Lightweight MutualAuthentication Protocol for Low-cost RFID tags", *Workshop on RFID Security(RFIDSec'06)*, 2006.

[16] Rieback, M. R., Crispo, B., and Tanenbaum, A. S., "The Evolution of RFID Security", *Pervasive Computing IEEE*, Vol. 5, pp. 62-69, 2006.

[17] Roberts, C. M., "Radio Frequency Identification (RFID)", *Computers and Security*, Vol. 25, pp. 18-26, 2006.

[18] Rotter, P., "A Framework for Assessing RFID System Security and Privacy Risks", *Security & Privacy*, Vol. 7, No. 2, pp. 70-77, 2008.

[19] EPCglobal Inc., EPCglobal Object Name Service (ONS) Standard Version 1.0, 2005.