強化的極輕量 RFID 鑑別協定

葉慈章*
明新科技大學資訊管理學系

吳家陞
明新科技大學資訊管理學系

摘要

隨著無線射頻辨識系統（Radio Frequency Identification; RFID）成本逐年降低，標籤已逐漸取代傳統條碼，廣泛地應用於我們的日常生活中。然而，由於透過無線傳輸進行辨識，在空氣中傳輸機密資料容易遭到竊聽、竄改或攔截，產生安全與隱私的問題。低成本的 RFID 標籤因運算能力有限，無法支援複雜的密碼學運算，因此其安全協定的設計更具挑戰性。2007 年 Chien 利用簡單的位元運算提出極輕量的鑑別協定 SASI，兼顧安全與隱私保護；然而其無法避免阻斷服務攻擊、完全洩漏攻擊與追蹤攻擊。本論文將詳細分析 SASI 協定的安全問題，並提出改善協定，以有效地提升 RFID 應用的安全性，讓消費者可以安心地享受 RFID 技術所帶來的便利性。

關鍵詞：RFID、SASI、安全、極輕量、鑑別

* 本文通訊作者。電子郵件信箱：cheer@must.edu.tw
2010/10/11 投稿；2011/04/07 修訂；2011/04/17 接受

An Enhanced Ultralightweight RFID Authentication Protocol

Tzu-Chang Yeh*
Department of Information Management, Minghsin University of Science and Technology

Chia-Sheng Wu
Department of Information Management, Minghsin University of Science and Technology

Abstract

RFID (Radio Frequency Identification) is a kind of contactless automatic identification system. As its cost declines, RFID is gradually replacing the traditional barcode and is anticipated to be widely used in our daily life. However, owing to the radio transmission nature of RFID, the information transmitted in the air could easily be eavesdropped on, modified, or intercepted. The issues of security and privacy are thus raised. Because the low-cost RFID tags are with extremely limited resources, traditional security primitives cannot be incorporated well. The design of security protocol is thus more challenging. In 2007, Chien proposed an ultralightweight strong authentication and strong integrity (SASI) protocol for very low-cost tags. Using only simple bitwise operations on tags, SASI is highly efficient. However, it was found to be vulnerable to DoS attacks, full-disclosure attacks and tracking attacks. This paper will give demonstrations on what have caused these weaknesses, and more of that, an improved protocol is also proposed which is free from worries of those problems mentioned above. The improved protocol could thus be applied in environments requiring high level of security.

Keywords: RFID, SASI, Security, Ultralightweight, Authentication

* Corresponding author. Email: cheer@must.edu.tw
2010/10/11 received; 2011/04/07 revised; 2011/04/17 accepted

壹、緒論

無線射頻辨識系統（Radio Frequency Identification; RFID）被視為本世紀最重要的十大技術之一，最早應用於第二次世界大戰時之敵我辨識系統（Rieback et al. 2006; Sheng et al. 2008）。RFID由標籤（Tag）、讀取器（Reader）與後端伺服器（Database Server）所組成（Lehtonen et al. 2006），可遠距離自動辨識，能在高速移動中讀取，不需將標籤置於可視直線（Line-of-sight）上，當標籤進入讀取器的讀取範圍時即可進行辨識，可一次讀取多個標籤，也可穿透物質進行辨識，並於後端伺服器取出標籤對應的記錄。

隨著標籤成本下降、體積縮小以及國際標準的整合，RFID 的使用率大幅成長，目前已逐漸取代傳統條碼成為新一代的電子條碼。2003 年美國零售業龍頭 Wal-Mart 要求旗下前百大供應商於 2005 年前全面導入 RFID 技術後，各種領域應用快速普及（Roberts 2006）。全球 RFID 標籤的使用量快速成長，預估 2011 年全球標籤數量將超過 100 億個（賴秋香 2008）；IDtechEx（2006）指出 HF 與 UHF 為現階段產值最大的頻段，其中 HF 多應用於個人身分識別方面，如：非接觸式信用卡、門禁卡等；UHF 則多用於供應鏈管理，如：出貨管理、物流管理等，市場潛力雄厚。然而由於技術成熟與市場的飽合，加上讀取距離增長的需求，其中超過八成為超高頻 UHF 被動式標籤，未來在物流、安全、醫療、金融及交通等相關產業的應用極具潛力。

由於 RFID 是透過無線通訊進行辨識，在空氣中傳輸的資訊容易遭到竊聽、竄改或攔截，因此安全與隱私保護的議題備受關注。我們由相關文獻（Li & Deng 2007; Li & Wang 2007; Li et al. 2007; Chen et al. 2008; Ohkubo et al. 2008; Rotter 2008）整理出 RFID 常遇到的安全與隱私問題如下：

1. 重送攻擊（Replay Attack）：攻擊者竊取相關訊息，並於事後非法重送，試圖假冒合法裝置通過鑑別。
2. 阻斷服務攻擊（Denial of Service Attack）：攻擊 RFID 系統並造成系統無法正常運作。攻擊方式如：發送超過系統能處理的大量訊息或以金屬遮蓋 RFID 標籤，使得系統癱瘓無法運作；或者攔截或竄改通訊中的訊息，造成標籤與後端伺服器更新不同步，使雙方無法繼續進行鑑別而造成讀取失敗。
3. 完全洩漏攻擊（Full-disclosure Attack）：攻擊者藉由使用未經授權的讀取器非法讀取標籤或竊聽通訊訊息以取得機密資料。
4. 追蹤攻擊（Tracking Attack）：藉由竊聽標籤所傳輸的固定值或可預期訊息追蹤特定標籤或其持有者的位置。

Chien（2007）依標籤端需支援的密碼學運算能力，將 RFID 安全協定分為下列四類：

1. 完善（Full-fledged）：標籤需支援各種密碼學機制，如：雜湊函數（Hash function）、對稱式加密與非對稱式加密法。
2. 簡單（Simple）：標籤需支援擬亂數產生器（Pseudo-Random Number Generator, PRNG）與雜湊函數，但不支援對稱式加密與非對稱式加密法。
3. 輕量（Lightweight）：標籤需支援擬亂數產生器與一些簡單函數，如：循環冗餘碼（Cyclical Redundancy Check, CRC），但不支援雜湊函數。
4. 極輕量（Ultralightweight）：標籤僅支援簡單的位元運算如：XOR，AND，OR，Rot (x, y)與 Addition mod 2^n 等。

RFID 的普及需要靠標籤成本的降低，然而低成本的標籤運算能力有限，因此安全與隱私的保護更不容易。過去許多學者提出的 RFID 安全協定，大多需要複雜的運算，無法適用於低成本的標籤。

Peris-Lopez 等（2006a, 2006b, 2006c）利用簡單的位元運算提出極輕量的 UMAP 家族協定（包含 LMAP，M^2AP 與 EMAP 三個協定），然而三個協定均存在阻斷服務攻擊與完全洩漏攻擊的問題（Chien & Huang 2007; Li & Deng 2007; Li & Wang 2007; Li et al. 2007），此外還有追蹤攻擊的問題。

Chien（2007）提出 SASI 協定，希望改善 UMAP 家族協定的阻斷服務攻擊與完全洩漏攻擊的問題，然而此協定仍然無法真正避免阻斷服務攻擊（Cao et al. 2009; Sun et al. 2011）與完全洩漏攻擊（D'Arco & De Santis 2011），此外還有追蹤攻擊（Phan 2009; Cao et al. 2009）的問題。

Peris-Lopez 等（2008）提出的 Gossamer 協定以 SASI 協定的架構為基礎，希望解決阻斷服務攻擊與完全洩漏的問題，增加了 *MIXBITS*（x, y）函數與π的計算來保護金鑰的傳送。然而，與 SASI 協定相同仍有重送攻擊、阻斷服務攻擊與標籤被追蹤的問題。

Peris-Lopez 等（2009）提出的 ULAP 協定以其 2006 年提出的 LMAP 協定架構為基礎，利用簡單的位元運算與亂數保護資訊的傳送，目的在解決 UMAP 家族協定的追蹤攻擊問題，將步驟 2 傳送的 *IDS* 改為經當次亂數保護的 *SessionIDS*，但仍有阻斷服務攻擊與追蹤攻擊的問題。

本論文將詳細分析 SASI 的安全問題，並提出改善協定以避免上述問題，使低成本的 RFID 標籤亦能應用於高安全需求的環境。

貳、Chien 的雙向鑑別協定 SASI

Chien（2007）提出的 SASI 協定，利用簡單的位元運算改善 Peris-Lopez 等（2006a, 2006b, 2006c）所提出協定的安全問題。協定假設讀取器與後端伺服器為同一端，並假設讀取器和後端伺服器之間的傳輸通道為安全通道，而讀取器和標籤之間的傳輸通道為非安全通道。協定使用的符號說明如表 1。

表 1：符號說明

$\vee$	OR 運算
$\oplus$	XOR 運算
$+$	Addition mod 2^n 位元加法運算（n=96，為各金鑰與索引值之位元長度）
Rot (*x*,*y*)	字元組 X 向左旋轉 Y 個位元
n1, *n2*	讀取器產生的亂數
ID	標籤的識別碼
IDS	後端伺服器端存的標籤索引值
K1, *K2*	後端伺服器端存的共享金鑰，供讀取器與標籤相互鑑別身分
IDS_{next}	標籤端存的新索引值
IDS_{old}	標籤端存的舊索引值
$K1_{next}$, $K2_{next}$	標籤端存的新共享金鑰，供讀取器與標籤相互鑑別身分
$K1_{old}$, $K2_{old}$	標籤端存的舊共享金鑰，供讀取器與標籤相互鑑別身分
IDS^*	當次通過鑑別的索引值（IDS_{next} 或 IDS_{old}）
$K1^*$, $K2^*$	當次通過鑑別的共享金鑰（$K1_{next}$ 或 $K1_{old}$, $K2_{next}$ 或 $K2_{old}$）
$A \rightarrow B$	*A* 傳送訊息給 *B*

索引值、金鑰等僅存放在 RFID 標籤與後端伺服器，讀取器只有與特定 RFID 標籤互動時，才會暫存相關資料。標籤內存（*ID*, IDS_{next}, IDS_{old}, $K1_{next}$, $K1_{old}$, $K2_{next}$, $K2_{old}$），而讀取器內存（*ID*, *IDS*, *K1*, *K2*）。後端伺服器於初始階段產生三個亂數 *IDS*, *K1* 和 *K2* 作為資料庫中該標籤記錄的初始值，並設定為標籤內存欄位的初始值（$IDS_{next}=IDS_{old}=IDS$, $K1_{next}=K1_{old}=K1$, $K2_{next}=K2_{old}=K2$）。每次標籤讀取的運作流程分成下列三個階段（圖 1）：

Reader		***Tag***
Tag identification:		
	1. *hello* →	The tag first responds with the next *IDS*, and then the old *IDS* if necessary
use *IDS* to find a matched record	← 2. *IDS*	
Mutual authentication:		Extract *n1* from *A*, and *n2* from *B*
$A=IDS \oplus K1 \oplus n1$	3. $A\|\|B\|\|C$ →	$\overline{K1}=Rot(K1^* \oplus n2, K1^*)$
$B=(IDS \vee K2)+n2$		$\overline{K2}=Rot(K2^* \oplus n1, K2^*)$
$\overline{K1}=Rot(K1 \oplus n2, K1)$	← 4. D	$\overline{C}=(K1^* \oplus \overline{K2})+(\overline{K1} \oplus K2^*)$
$\overline{K2}=Rot(K2 \oplus n1, K2)$		Verity C ?= $\overline{C}$
$C=(K1 \oplus \overline{K2})+(\overline{K1} \oplus K2)$		If OK,
$\overline{D}=(\overline{K2}+ID) \oplus ((K1 \oplus K2) \vee \overline{K1})$		$D=(\overline{K2}+ID) \oplus ((K1^* \oplus K2^*) \vee \overline{K1})$
Verity D ?= $\overline{D}$		
Pseudonym updating and key updating:		
$IDS=(IDS+ID) \oplus (n2 \oplus \overline{K1})$		$IDS_{old}=IDS^*$
$K1=\overline{K1}$; $K2=\overline{K2}$		$IDS_{next}=(IDS^*+ID) \oplus (n2 \oplus \overline{K1})$
		$K1_{old}=K1^*$; $K1_{next}=\overline{K1}$
		$K2_{old}=K2^*$; $K2_{next}=\overline{K1}$
$ID, IDS, K1, K2$		$ID, IDS_{next}, IDS_{old}, K1_{next}, K1_{old}, K2_{next}, K2_{old}$

圖 1：Chien 學者的 SASI 協定

一、標籤識別（Tag identification）

1. *Reader*→*Tag*：*hello*
   讀取器傳送讀取請求"*hello*"給標籤。
2. *Tag*→*Reader*：*IDS*（IDS_{next} 或 IDS_{old}）
   標籤收到讀取器的讀取請求後，先回傳 IDS_{next}，讀取器以其為索引值並自

資料庫找出標籤的對應記錄；若找不到，讀取器再發出讀取請求，標籤則改回傳 IDS_{old}。接下來，在資料庫找到對應記錄的標籤端索引值與共享金鑰分別以 IDS^*，$K1^*$，$K2^*$ 表示。

二、雙向鑑別（Mutual authentication）

3. *Reader*→*Tag*：$A||B||C$

讀取器產生兩個亂數 $n1$ 與 $n2$，並以該標籤的記錄計算出 $A=IDS \oplus K1 \oplus n1$，$B=(IDS \vee K2)+n2$，$\overline{K1}=Rot(K1 \oplus n2, K1)$，$\overline{K2}=Rot(K2 \oplus n1, K2)$ 與 $C=(K1 \oplus \overline{K2})+(\overline{K1} \oplus K2)$，並傳送 $A||B||C$ 給標籤，供其鑑別讀取器。

4. *Tag*→*Reader*：D

標籤將收到的 A 與內存的 IDS^*、$K1^*$作 XOR 計算以取出 $n1$，並將收到的 B 與 IDS^*、$K2^*$作計算以取出 $n2$；然後自行計算 $\overline{K1}=Rot(K1^* \oplus n2, K1^*)$，$\overline{K2}=Rot(K2^* \oplus n1, K2^*)$ 與 $\overline{C}=(K1^* \oplus \overline{K2})+(\overline{K1} \oplus K2^*)$，若 $\overline{C}$ 與讀取器傳來的 C 一致，則通過對讀取器的鑑別；接下來標籤自行計算 $D=(\overline{K2}+ID) \oplus ((K1^* \oplus K2^*) \vee \overline{K1})$ 並回傳給讀取器，供其鑑別標籤的身分；最後讀取器自行計算 $\overline{D}=(\overline{K2}+ID) \oplus ((K1 \oplus K2) \vee \overline{K1})$，並與自標籤收到的 D 比對，若一致，則通過對標籤的鑑別。

三、資料更新（Pseudonym updating and key updating）

讀取器與標籤完成相互鑑別後，各自更新內存的資訊。讀取器將 IDS 更新為 $(IDS+ID) \oplus (n2 \oplus \overline{K1})$，$K1$ 與 $K2$ 分別更新為 $\overline{K1}$ 與 $\overline{K2}$；標籤將 IDS_{old} 更新為 IDS^*，IDS_{next} 更新為 $(IDS^*+ID) \oplus (n2 \oplus \overline{K1})$，$K1_{old}$ 與 $K2_{old}$ 分別更新為 $K1^*$ 與 $K2^*$，$K1_{next}$ 與 $K2_{next}$ 分別更新為 $\overline{K1}$ 與 $\overline{K2}$。

身份鑑別成功後，讀取器與標籤即依雙方的通訊指令格式進行資料的讀取或寫入。

參、SASI 協定的問題

SASI 協定以 IDS 當索引值，使讀取器無需逐筆計算即可在資料庫中找到對應的標籤記錄，以減輕資料庫的負擔；讀取器和標籤藉由共享金鑰 $K1$ 與 $K2$ 進行相互鑑別；使用簡單的位元運算 XOR, OR, Addition mod 2^n, Rot (x, y) 與亂數來保護資料的傳送；標籤端儲存共享金鑰的新舊值以防止更新不同步所造成的阻斷服務攻擊。然而，此協定仍有阻斷服務攻擊、完全洩漏攻擊與追蹤的問題，詳細分

析如下：

一、阻斷服務攻擊

（一）Cao 等（2009）指出 SASI 協定有三種阻斷服務攻擊問題：

1. 攻擊者竄改步驟 3 傳送的 $A||B||C$，更改 A 與 C 的 LSB（Least Significant Bit）為 $A'=A\oplus[I]_0$ 與 $C'=C\oplus[I]_0$（$[I]_0$=00..001），再將 $A'||B||C'$傳給標籤；在 $K2$ mod n=0 與 $K2_{LSB}\oplus\overline{K1}_{LSB}$=0 的情況下（n=96，為各金鑰與索引值之位元長度），標籤將無法察覺而通過對讀取器的鑑別。若此時 ID_{LSB}=0，攻擊者再攔截標籤回傳的 D'（以 A'取出的錯誤亂數 $n1'$計算得出），並計算 $D''=D'\oplus[I]_0$ 傳給讀取器，讀取器將無法察覺此非法行為，而通過對標籤的鑑別。接下來，雙方各自更新內存資訊，後端伺服器利用該次自行產生的亂數（$n1, n2$）作更新，而標籤則以（$n1', n2$）來更新其內存訊息，雙方因此更新不同步，造成阻斷服務攻擊。
2. 攻擊者竄改步驟 3 傳送的 $A||B||C$，更改 B 與 C 的 LSB 為 $B'=B+1$ 與 $C'=C\oplus[I]_0$，再將 $A||B'||C'$傳給標籤；在 $K1$ mod n=0，$K1_{LSB}\oplus\overline{K2}_{LSB}$=0 與 $n2_{LSB}$=0 的情況下，標籤將無法察覺而通過對讀取器的鑑別，並回傳 D'（以 B'取出的錯誤亂數 $n2'$計算得出）；若此時 $K1_{LSB}\oplus K2_{LSB}$=1，讀取器亦將無法察覺此非法行為，而通過對標籤之鑑別。接下來，雙方將各自更新內存資訊，後端伺服器利用該次自行產生的亂數（$n1, n2$）作更新，而標籤則以（$n1, n2'$）來更新其內存訊息，雙方因此更新不同步，造成阻斷服務攻擊。
3. 攻擊者竄改步驟 3 傳送的 $A||B||C$，更改 A 的 LSB 為 $A'=A\oplus[I]_0$，並從 C 的 LSB 開始逐次計算 $C'=C+[I]_i$ 和 $C''=C-[I]_i$（i 為 0 到 95，$[I]_0$=00..001, $[I]_1$=00..010，…，$[I]_{95}$=10..000），再將 $A'||B||$（C'或 C''）傳給標籤，在 $K1_{LSB}\oplus\overline{K2}_{LSB}$=0 的情況下，標籤將通過對讀取器的鑑別，並回傳 D'（以 A'取出的錯誤亂數 $n1'$作計算），讀取器亦將無法察覺此非法行為，而通過對標籤之鑑別。接下來，雙方將各自更新內存的資訊，後端伺服器利用該次自行產生的亂數（$n1, n2$）作更新，而標籤則以 A'取出的錯誤亂數（$n1', n2$）來更新其內存訊息，雙方因此更新不同步，造成阻斷服務攻擊。因 C 為 96 位元，攻擊者最多只需嘗試 192 次。

（二）Sun 等（2011）再提出另外兩種阻斷服務攻擊：

1. 首先假設標籤內存的 IDS_{next} 與後端伺服器內存的 IDS 一致（值均等於 IDS_1）。接下來的標籤讀取中，攻擊者記錄步驟 3 的 $A_1||B_1||C_1$ 並攔截步驟 4 的 D_1，使標籤更新為 $IDS_{old}=IDS_1$，$IDS_{next}=IDS_2$，而後端伺服器因未收到

D_1 故未更新；接下來讓標籤與讀取器進行正常讀取，因後端伺服器找不到標籤傳來的 $IDS_{next}=IDS_2$，故讀取器與標籤改以 $IDS_{old}=IDS_1$ 通過鑑別，因此標籤更新為 $IDS_{old}=IDS_1$，$IDS_{next}=IDS_3$，後端伺服器則更新為 IDS_3。最後，攻擊者假冒合法讀取器讀取標籤，並假裝在後端伺服器中找不到標籤回傳的 IDS_{next}（$=IDS_3$）並要求標籤改送 IDS_{old}=（IDS_1），此時攻擊者將先前記錄的 $A_1||B_1||C_1$ 重送給標籤，標籤因無法察覺此非法重送而將內存資訊更新為 $IDS_{old}=IDS_1$，$IDS_{next}=IDS_2$，此後讀取器內存的 IDS_3 與標籤的內存資訊 IDS_1 與 IDS_2 已完全不同，無法再通過鑑別，因此造成阻斷服務攻擊。

2. 首先假設標籤內存的 IDS_{next} 與後端伺服器內存的 IDS 一致（值均等於 IDS_1）。接下來的正常標籤讀取中，攻擊者記錄步驟 3 的 $A_1||B_1||C_1$，標籤更新為 $IDS_{old}=IDS_1$，$IDS_{next}=IDS_2$，而後端伺服器則更新為 $IDS=IDS_2$；接下來攻擊者假冒合法讀取器讀取標籤，並假裝在後端伺服器中找不到標籤回傳的 IDS_{next}（$=IDS_2$）而要求標籤改送 IDS_{old}（$=IDS_1$），攻擊者再將上次記錄的 $A_1||B_1||C_1$，每次更改 A_1 的一個位元值與 C_1 的 MSB（Most Significant Bit）值，再將 $A_1'||B_1||C_1'$ 傳給標籤；此時若被更改的位元正好被旋轉到 $\overline{K2}$ 的 MSB，標籤將無法察覺此非法行為而通過對讀取器的鑑別，接下來便自 A_1'取出錯誤的亂數 $n1'$，並以（$n1'$, $n2$）來更新標籤的內存訊息，而後端伺服器則未更新，雙方因此更新不同步，造成阻斷服務攻擊（因 A_1 與 C_1 均為 96 位元，攻擊者最多只需嘗試 96 次）。

二、完全洩漏攻擊

D'Arco 與 De Santis（2011）指出 SASI 的完全洩漏攻擊問題，攻擊者先竊聽標籤與讀取器間一次正常的通訊訊息，並針對步驟 3 傳送的 $A_1||B_1||C_1$，計算出 $A_1'=A_1 \oplus [I]_i$，$C_1'=C_1+[I]_i$，$C_1''=C_1-[I]_i$（i 為 0 到 95，$[I]_0$=00..001，$[I]_1$=00..010，…，$[I]_{95}$=10..000），然後再假冒讀取器將 $A_1'||B_1||$（C_1'或 C_1''）傳給標籤，再藉由標籤回傳的 D_1'後與之前竊聽到的 D_1 即可進行相關運算推導出多組可能的 ID 與 $\overline{K2}$，接下來攻擊者再假冒讀取器傳送讀取請求“*hello*”給標籤，並假裝在後端伺服器中找不到標籤回傳的 IDS_{next}（$=IDS_2$）而要求標籤改送 IDS_{old}（$=IDS_1$），攻擊者便將之前竊聽的 $A_1||B_1||C_1$ 傳給標籤，讓讀取器與標籤恢復同步，然後再連續竊聽兩次正常的通訊訊息，接下來即可利用竊聽到的三筆正常通訊的內容進行相關的運算與驗證，推導出標籤內存的所有秘密資訊。

三、追蹤攻擊

SASI 協定的三種追蹤攻擊方式如下：

1. Phan（2009）指出假設攻擊者可選擇兩個標籤（*ID* 一個為奇數，一個為偶數）進行測試，竊聽正常標籤讀取中傳送的 *C* 與 *D*，並計算 $C_{LSB} \oplus D_{LSB}$ 即可得知那一個標籤被讀取。由於位元運算的下面兩個特性：
   - 最低有效位元（LSB）進行 Addition（+）或 XOR（⊕）運算結果相同。
   - XOR（⊕）與 OR（∨）運算結果有 3/4 的機率相同。

   因此當計算 $C_{LSB} \oplus D_{LSB}$ 時，把其中原來的 Addition 與 OR 運算均改為 XOR 運算後，其結果即有 3/4 的機會為正確的 ID_{LSB}，因此可藉此辨識出該標籤以進行追蹤。由於猜中一個位元的機率為 1/2，而 SASI 協定的 ID_{LSB} 被猜中的機率為 3/4，因此無法滿足不可追蹤性。
2. Cao 等（2009）指出攻擊者先竊聽讀取器與各標籤間的所有通訊記錄，再破解選定的標籤實體以取出內存的（*ID*, IDS_m, $K1_m$, $K2_m$, IDS_{m+1}, $K1_{m+1}$, $K2_{m+1}$），將 IDS_m 與之前竊聽到的通訊記錄中每筆記錄步驟 2 傳送的 *IDS* 作比對，值相同者即為該標籤遭破解前的最近一次的通訊記錄；接下來要再往前找出一筆該標籤的通訊記錄，可自之前的竊聽到的通訊記錄逐筆代入計算（$IDS_m \oplus$（*IDS* +*ID*））$\oplus K1_m$ 以取得 *n2*，再由 $K1_m = Rot(K1_{m-1} \oplus n2, K1_{m-1})$ 驗算出 $K1_{m-1}$，接著計算 $K2_{m-1} =$（*C*-（$K1_{m-1} \oplus K2_m$））$\oplus K1_m$ 與 $n1 = A \oplus IDS \oplus K1_{m-1}$，再以 $K2_{m-1}$ 與 *n1* 代入計算（$IDS \vee K2_{m-1}$）+ *n2* 與（$K2_m$+*ID*）⊕（（$K1_{m-1} \oplus K2_{m-1}$）∨ $K1_m$），若分別等於該筆通訊記錄的 *B* 與 *D* 值，即可確認此筆記錄為該標籤遭破解前的倒數第二筆通訊記錄；以同樣方式即可一路向前辨識出該標籤的所有通訊記錄以進行追蹤。
3. 本論文發現 SASI 協定還有另一種追蹤的問題，假設標籤正常讀取後目前內存值更新為 $IDS_{next}=IDS_2$，$IDS_{old}=IDS_1$；在下次合法讀取器進行正常讀取時，標籤才會再更新其內存值為 $IDS_{next}=IDS_3$，$IDS_{old}=IDS_2$。此時非法讀取器可不斷地傳送讀取請求"*hello*"給標籤，標籤先針對非法讀取器傳來的第一個讀取請求回傳 IDS_{next}（$=IDS_2$）後，因未收到讀取器應回傳的 $A||B||C$ 而未更新標籤的內存資訊並針對第二次非法讀取器傳來的讀取請求回傳 IDS_{old}（$=IDS_1$），標籤針對接下來非法讀取器傳來的讀取請求亦因未收到讀取器應回傳的 $A||B||C$ 而未更新標籤的內存資訊並於下次收到讀取請求時回傳 IDS_{old}（$=IDS_1$），攻擊者即可藉由此固定的 IDS_{old} 值（$=IDS_1$）追蹤標籤或其持有者，直到下次合法讀取器進行正常讀取，標籤更新其內存值為 $IDS_{next}=IDS_3$，$IDS_{old}=IDS_2$ 為止。

肆、本研究提出的改善協定 SASI

由於 SASI 協定僅由讀取器單方產生亂數（標籤未產生亂數），加上訊息是以明文傳送或保護不足，因此引起阻斷服務攻擊、完全洩漏攻擊與追蹤攻擊；本研究提出的改善協定，增加了標籤端的亂數 *R1* 與讀取器的識別碼 *RID* 來保護訊息的傳送，以防止上述的問題。正式運作前，廠商將隨機產生的亂數 *R1* 存入標籤中，並設定後端伺服器內存的（*ID*, *IDS*, *K1*, *K2*, *RID*）與標籤內存的（*ID*, IDS_{next}, IDS_{old}, $K1_{next}$, $K1_{old}$, $K2_{next}$, $K2_{old}$, *RID*, *R1*），詳細的改善協定流程如下（圖 2）：

一、標籤識別（Tag identification）

1. *Reader*→*Tag*：*hello*
   讀取器傳送讀取請求"*hello*"給標籤。
2. *Tag*→*Reader*：（*IDS*||*IDS*）⊕（*RID*||*R1*）, *RID*⊕*R1*
   標籤收到讀取器的讀取請求後，以內存資訊計算出當次的亂數值 *R1*=（$K1_{next} \oplus K2_{old}$）+（（$K2_{next} \oplus K1_{old}$）∨*R1*），並計算（$IDS_{next}||IDS_{next}$）⊕（*RID*||*R1*） 與 *RID*⊕*R1*，傳至讀取器供其識別標籤；若讀取器在後端伺服器中找不到對應的 *IDS*，則再要求標籤改傳 （$IDS_{old}||IDS_{old}$）⊕（*RID*||*R1*） 與 *RID*⊕*R1*（為使 XOR（⊕）運算左右兩邊運算位元長度一致，因此傳送相同的兩串 IDS_{next} 或 IDS_{old} 值）。

二、雙向鑑別（Mutual authentication）

3. *Reader*→*Tag*：（*A*||*B*||*C*）+*R1*
   讀取器以內存的 *RID* 與 *RID*⊕*R1* 作 XOR 取出 *R1*，再計算（*RID*||*R1*）與收到的 *IDS*=（*IDS*||*IDS*）⊕（*RID*||*R1*）作 XOR 取出 *IDS*，接下來以 *IDS* 為索引值自資料庫找出標籤的對應記錄，然後再產生兩個亂數 *n1* 與 *n2*，並計算 *A*=*IDS*⊕*K1*⊕*n1*，*B*=（*IDS*∨*K2*）+*n2*，$\overline{K1}$=*Rot*（*K1*⊕*n2*, *K1*），$\overline{K2}$=*Rot*（*K2*⊕*n1*, *K2*）與 *C*=（*K1*⊕$\overline{K2}$）+（$\overline{K1}$⊕*K2*），並傳送（*A*||*B*||*C*）+*R1* 給標籤，供其鑑別讀取器。
4. *Tag*→*Reader*：*D*
   標籤將收到的（*A*||*B*||*C*）+*R1* 與 *R1* 作計算取出（*A*||*B*||*C*）後，將 *A* 與 IDS^*、$K1^*$作 XOR 計算以取出 *n1*，並將收到的 *B* 與 IDS^*、$K2^*$計算以取出 *n2*，再計算 $\overline{K1}$=*Rot*（$K1^* \oplus n2$, $K1^*$）、$\overline{K2}$=*Rot*（$K2^* \oplus n1$, $K2^*$）與 $\overline{C}$=（$K1^* \oplus \overline{K2}$）+（$\overline{K1} \oplus K2^*$），若 $\overline{C}$ 與自讀取器收到的 *C* 一致，則通過對

讀取器的鑑別；接下來自行計算 $D=(\overline{K2}+ID)\oplus((K1^{*}\oplus K2^{*})\vee\overline{K1})$ 並回傳給讀取器供其鑑別標籤的身分；最後讀取器自行計算 $\overline{D}=(\overline{K2}+ID)\oplus((K1\oplus K2)\vee\overline{K1})$，並與由標籤收到的 D 比對，若一致，則通過對標籤的鑑別。

Reader		***Tag***
Tag identification:	1. *hello* →	The tag responds with the *next IDS*, and then the *old IDS* if necessary $R1=(K1_{next}\oplus K2_{old})+((K2_{next}\oplus K1_{old})\check{}R1)$
	← 2. $(IDS^{*}\|\|IDS^{*})\oplus(RID\|\|R1)$, $RID\oplus R1$	
R1= $RID\oplus$R1$\oplus RID$		
get *IDS* from $(IDS\|\|IDS)\oplus(RID\|\|R1)\oplus(RID\|\|R1)$		
use *IDS* to find a matched record		
Mutual authentication:		Extract *n1* from *A*, and *n2* from *B*
Generate *n1*, *n2*		$n1=A\oplus IDS\oplus K1^{*}$
$A=IDS\oplus K1\oplus n1$		$n2=B-(IDS\vee K2^{*})$
$B=(IDS\vee K2)+n2$		$\overline{K1}=Rot(K1^{*}\oplus n2, K1^{*})$
$\overline{K1}=$Rot$(K1\oplus n2, K1)$	3. $(A\|\|B\|\|C)+R1$ →	$\overline{K2}=Rot(K2^{*}\oplus n1, K2^{*})$
$\overline{K2}=$Rot$(K2\oplus n1, K2)$		$\overline{C}=(K1^{*}\oplus\overline{K2})+(\overline{K1}\oplus K2^{*})$
$C=(K1\oplus\overline{K2})+(\overline{K1}\oplus K2)$	← 4. *D*	Verify C ?= $\overline{C}$
$\overline{D}=(\overline{K2}+ID)\oplus((K1\oplus K2)\vee\overline{K1})$		If OK,
Verify D ?= $\overline{D}$		$D=(\overline{K2}+ID)\oplus((K1^{*}\oplus K2^{*})\vee\overline{K1})$
Pseudonym updating and key updating:		
$IDS=(IDS+ID)\oplus(n2\oplus\overline{K1})$		$IDS_{old}=IDS^{*}$
$K1=\overline{K1}$; $K2=\overline{K2}$		$IDS_{next}=(IDS^{*}+ID)\oplus(n2\oplus\overline{K1})$
		$K1_{old}=K1^{*}$; $K1_{next}=\overline{K1}$
		$K2_{old}=K2^{*}$; $K2_{next}=\overline{K2}$
ID, *IDS*, *K1*, *K2*, *RID*		*ID*, IDS_{next}, IDS_{old}, $K1_{next}$, $K1_{old}$, $K2_{next}$, $K2_{old}$, *RID*, *R1*

圖 2：本研究提出的改善協定

三、資料更新（Pseudonym updating and key updating）

資料更新步驟與 SASI 協定相同。

身份鑑別成功後，讀取器與標籤即依雙方的通訊指令格式進行資料的讀取或寫入。

伍、協定分析

我們將提出的改善協定針對各方面進行分析如下：

一、重送攻擊

由於 SASI 協定中標籤端未產生亂數，因此攻擊者可藉由重送讀取器傳給標籤的 $A||B||C$，使標籤無法察覺此非法行為而通過對讀取器的鑑別。我們的改善協定在標籤端產生亂數 $R1$ 以保護 $A||B||C$ 的傳送，使每次傳送的訊息皆不同，因此攻擊者無法藉由重送先前竊聽的步驟 3 訊息而通過鑑別。

二、阻斷服務攻擊

SASI 協定中，攻擊者可藉由竄改或重送步驟 3 傳送的 $A||B||C$ 而產生阻斷服務攻擊。我們的協定以標籤產生的亂數 $R1$ 來保護 $A||B||C$ 的傳送，如果攻擊者竄改或重送 $A||B||C$，標籤可藉由比對不合而察覺，因此可避免讀取器與標籤更新不同步而造成阻斷服務攻擊。

三、完全洩漏攻擊

由於 SASI 協定中標籤端未產生亂數，攻擊者可竊聽 $A||B||C$ 並竄改後再假冒讀取器將竄改過的值傳給標籤，然後根據標籤在步驟 4 的回傳值與竊聽的三筆正常通訊內容進行相關的運算與驗證，即可推導出標籤內存的所有秘密資訊。因此我們的協定增加了標籤端的亂數 $R1$ 保護訊息的傳送，使每次傳送的訊息皆不同，讓攻擊者無法藉由竊聽並竄改而推導出標籤的內存訊息。

四、追蹤攻擊

SASI 協定中讀取器與標籤內存的祕密資訊雖於每次鑑別後均作更新，然而由於 IDS 是以明文傳送，加上標籤端未產生亂數以保護訊息的傳送，造成追蹤攻擊。因此我們於標籤每次接收到讀取器傳出的讀取請求“*hello*”後，立即與內存資

訊作計算產生當次的亂數 *R1* 以保護 *IDS* 與 *A*||*B*||*C* 的傳送，使步驟 2, 3, 4 的傳送值於每次通訊時皆不同，讓攻擊者無法再藉由竊聽傳送的資訊進行相關運算以追蹤標籤或其持有者。

本協定增加了標籤端的亂數 *R1* 與讀取器的識別碼 *RID* 來保護訊息的傳送，以避免上述的問題，然而也因此增加了運算的成本；我們將極輕量 RFID 協定的分析比較整理如表 2。

表 2：極輕量 RFID 協定之比較

		LMAP	M2AP	EMAP	Gossamer	ULAP	SASI	Our Protocol
重送攻擊		○	○	○	X	○	X	○
阻斷服務攻擊		X	X	X	X	X	X	○
完全洩漏攻擊		X	X	X	○	○	X	○
追蹤攻擊		X	X	X	X	X	X	○
標籤端運算次數	XOR（⊕）	14	13	21	6	14	10	14
	OR（∨）	1	2	2	0	1	2	3
	AND（∧）	0	2	2	0	0	0	0
	Addition mod 2^n (+)	9	8	0	44	7	4	5
	Rot (x, y)	0	0	0	18	0	2	2
	MIXBITS (x, y)	0	0	0	3	0	0	0

陸、結論

RFID 隨著成本的降低，越來越普及於我們的日常生活中，然而由於其無線傳輸的特性，在空氣中傳送的資訊易遭到竊聽、竄改與攔截，因此在安全與隱私保護上的議題備受關注。目前相關文獻提出的安全協定，大多需要複雜的密碼學運算，而無法適用於低成本的標籤。Chien（2007）利用簡單的位元運算提出極輕量的安全協定 SASI，但仍有阻斷服務攻擊、完全洩漏攻擊與追蹤攻擊的問題，本論文詳細分析其安全問題，並提出改善協定避免上述的問題，以有效地提升 RFID 應用的安全性，讓消費者可以安心地享受 RFID 技術所帶來的便利性。

我們提出的改善協定與既有的許多 RFID 協定一樣，假設讀取器和後端伺服器間屬於公司內部的有線傳輸通道而假定其為安全通道，故僅針對讀取器和標籤之間的無線傳輸進行改善；然而目前許多的 RFID 應用（如零售、物流、製造、醫療、行動商務等）多需以移動式的手持讀取器來提供使用上的方便性，即讀取

器和後端伺服器亦為無線傳輸，因此接下來我們期望能提出無需假設後端為安全通道的極輕量安全協定，使 RFID 能運用在高安全需求環境中。

誌謝

本研究承蒙行政院國家科學委員會計畫（計畫編號：NSC 97-2410-H-159-004）經費之補助，謹此致謝。

參考文獻

賴秋香（2008），『《市場篇》台灣 RFID 的發展現況與商機探討』，*Intelligent Times*, available at http://web.iii.org.tw/itmag/article_single_513.htm (accessed 20 June 2010).

Cao, T.J., Bertino, E. and Lei, H. (2009), 'Security analysis of the SASI protocol', *IEEE transactions on dependable and secure computing*, Vol. 6, No. 1, pp. 73-77.

Chen, Y., Chou, J.S. and Sun, H.M. (2008), 'A novel mutual authentication scheme based on quadratic residues for RFID systems', *Computer Networks: The International Journal of Computer and Telecommunications Networking*, Vol. 52, No. 12, pp. 2373-2380.

Chien, H.Y. (2007), 'SASI: a new ultralightweight RFID authentication protocol providing strong authentication and strong integrity', *IEEE Transactions on Dependable and Secure Computing*, Vol. 4, No. 4, pp. 337-340.

Chien, H.Y. and Huang, C.W. (2007), 'Security of ultra-lightweight RFID authentication protocols and its improvements', *ACM SIGOPS Operating Systems Reviews*, Vol. 41, No. 2, pp. 83-86.

IDTechEx (2006), available at http://www.idtechex.com/ (accessed 24 July 2010).

Lehtonen, M., Staake, T., Michahelles, F. and Fleisch, E. (2006), 'From identification to authentication-a review of RFID product authentication techniques', *Proceedings of Workshop on RFID Security (RFIDSec)* .

Li, T. and Deng, R.H. (2007), 'Vulnerability analysis of EMAP-an efficient RFID mutual authentication protocol', *Proceedings of the Second International Conference on Availability, Reliability and Security*, pp. 238-245.

Li, T. and Wang, G. (2007), 'Security analysis of two ultra-lightweight RFID authentication protocols', *Proceedings of the IFIP-New Approaches for Security, Privacy and Trust in Complex Environments*, Vol. 232, pp. 109-120.

Li, T., Wang, G. and Deng, R. H. (2007), 'Security analysis on a family of ultra-lightweight RFID authentication protocols', *Journal of Software*, Vol. 3, No. 3, pp. 1-10.

Ohkubo, M., Suzuki, K. and Kinoshita, S. (2008), 'RFID privacy issues and technical challenges', *Communications of the ACM*, Vol. 48, No. 9, pp. 66-71.

D'Arco, P. and De Santis, A. (2011), 'On ultralightweight RFID authentication protocols', *IEEE Transactions on Dependable and Secure Computing*, Vol. 8, No. 4, pp. 548-563.

Peris-Lopez, P., Hernandez-Castro, J.C., Estevez-Tapiador, J.M. and Ribagorda, A. (2008), 'Advances in ultralightweight cryptography for low-cost RFID tags: gossamer protocol', *Proceedings of the Workshop on Information Security Applications, LNCS*, Vol. 5379, pp. 56-68.

Peris-Lopez, P., Hernandez-Castro, J.C., Estevez-Tapiador, J.M. and Ribagorda, A. (2006a), 'EMAP: an efficient mutual authentication protocol for low-cost RFID tags', *Proceedings of the OTM Federated Conferences and Workshop: IS Workshop, LNCS,* Vol. 4277, pp. 352-361.

Peris-Lopez, P., Hernandez-Castro, J.C., Estevez-Tapiador, J.M. and Ribagorda, A. (2006b), 'LMAP: a real lightweight mutual authentication protocol for low-cost RFID tags', *Proceedings of the Second Workshop on RFID Security.*

Peris-Lopez, P., Hernandez-Castro, J.C., Estevez-Tapiador, J.M. and Ribagorda, A. (2006c), 'M^2AP: a minimalist mutual-muthentication protocol for low-cost RFID tags', *Proceedings of the Third International Conference on Ubiquitous Intelligence and Computing LNCS*, Vol. 4159, pp. 912-923.

Peris-Lopez, P., Hernandez-Castro, J.C., Estevez-Tapiador, J.M. and Ribagorda, A. (2009), '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.

Phan, R.C.W. (2009), 'Cryptanalysis of a new ultralightweight RFID authentication protocol-SASI', *IEEE Transactions on Dependable and Secure Computing*, Vol. 6, No. 4, pp. 316-320.

Rieback, M.R., Crispo, B. and Tanenbaum, A.S. (2006), 'The evolution of RFID security', I*EEE Pervasive Computing*, Vol. 5, No. 1, pp. 62-69.

Roberts, C.M. (2006), 'Radio frequency identification (RFID)', *Computers and Security*, Vol. 25, No. 1, pp. 18-26.

Rotter, P. (2008), 'A framework for assessing RFID system security and privacy risks',

IEEE Pervasive Computing, Vol. 7, No. 2, pp. 70-77.

Sheng, Q.Z., Li, X. and Zeadally, S. (2008), 'Enabling next-generation RFID applications: solutions and challenges', *IEEE Computer*, Vol. 41, No. 9, pp. 21-28.

Sun, H.M., Ting, W.C. and Wang, K. H. (2011), 'On the security of Chien's ultralightweight RFID authentication protocol', *IEEE Transactions on Dependable and Secure Computing,* Vol. 8, No. 2, pp. 315-317.