資訊安全之 RFID 架構

蕭進松
亞洲大學光電與通訊學系
教授
cshsiao@asia.edu.tw

饒晉彰
彰化信義國小教師
Jimjan_tw@yahoo.com.tw

摘要

RFID 不需要透過接觸即可利用讀取器（Reader）讀取電子標籤(Tag)的訊號資訊，其電子標籤是採用電子數據的方式，可以覆寫並且回收使用，因此在新增、修改、刪除儲存資料上沒有使用次數的限制。因為 Tag 具有重覆讀取的特性，因此如果處理不當，可能使 RFID 的安全性備受爭議，致使客戶的隱私可能遭受到侵犯，故隱私與安全已經成為 RFID 技術發展的重點。本文的研究在於探討 RFID 的有效認證機制，防止在使用 RFID 時，個人隱私遭受侵犯，以保護個人隱私資料及防止遭到追蹤，達到 RFID 資訊安全的目標。

關鍵詞：無線射頻辨識、安全架構、個人隱私.

Abstract

Radio Frequency Identification (RFID) systems utilizes a small tag containing an electronic product code that allows the embedded data to be transmitted. The RFID tag can be read by a reader from a distance, and it can be used repetitively. Once the data is read, RFID allows the stored data in the tag to be transmitted and processed in various ways such as add, modify or delete at a host computer. The characteristic of unlimited access to the tag by the readers leads to potential security and privacy issues. Due to the lack of security and unlimited access by RFID readers, the privacy of the consumer might be violated. Thus, developing better security systems and protecting user privacy has become a research focus in RFID technology. The purpose of this research is to study a effective implementation of RFID systems in focusing on preventing data loss during transmission processes, avoiding violation of personal privacy, protecting personal information from being stolen or tracked, and achieve a secured information process in RFID systems.

Keywords: Radio Frequency Identification (RFID), Security Structure, Personal Privacy.

1. 前言

無線射頻辨識系統（Radio Frequency Identification, RFID）是一種利用非接觸式的方式進行自動識別的系統，它是將電子標籤(Tag)貼在物件上，然後利用讀取器發送電磁波來傳送訊息，同時將互相收到的訊息在後端資料庫電腦系統中進行資料辨識及存取。RFID 系統的組成元件主要分為三個部分：天線、電子標籤和讀取器，其中電子標籤是利用一個晶片進行數位類比訊號轉換與儲存的動作，並內建所需要的不同頻率環境所設計的天線來和讀取器的射頻天線間進行接收通訊並產生回應。讀取器是作為感應電子標籤和讀寫資料的硬體，具有發射電磁波的功能。RFID 擁有特性如可以反覆的覆寫並且回收使用，因此在新增、修改、刪除儲存資料上沒有使用次數的限制，甚至可以使用數十萬次甚至數百萬次以上，不需要透過接觸即可利用讀取器(Reader)

讀取電子標籤的訊號資訊，針對讀取一至多個標籤，選擇處理資料是否寫入標籤，然而這些卻可能使 RFID 的安全性備受爭議。因為 Tag 具有重覆讀取的特性，因此如果處理不當，客戶的隱私可能遭受到侵犯。本論文藉由了解 RFID 私密金鑰使用機制及安全問題，提出系統架構，進行安全與效率分析，因此研究的目的在於探討 RFID 的有效認證機制，防止使用者在資訊傳輸或是標籤使用後個人隱私遭受侵犯，以保護個人隱私資料外露及防止個人遭到追蹤。達到 RFID 資訊安全的目標。

因為 RFID 和讀取器採用非接觸的通訊方式，物品的相關資訊不需接觸就會被讀取，所以必須詳加規範其應用領域。而且如果驗證機制的不完備，特別是在 RFID 標籤無法對閱讀器進行身份驗証時，當 RFID 標籤一旦接近讀取器，就會無條件自動發出訊息，如果無法辨識該 RFID 讀取器是否合法，可能會使個人隱私權受到侵犯的危險。電子標籤易被複製及安全性的問題是 RFID 所存在的一些隱憂。RFID 產生的隱私權問題為如何在 RFID 系統中建置保護隱私的能力，預防未授權的追蹤，保護用戶的個人信息及相關信息使其不洩漏。其中一極為可行的方式為透過演算法加密的方式，因此，如能透過一些加密演算法，用於標籤對讀寫器實現身份認證，只對通過身份認證的讀寫器傳送信息。在認證過程中，標籤需要記錄通過認證的讀寫器的身分識別碼，讀寫器也以廣播的形式向標籤發送身分識別碼。為了保證自身身分識別碼不被其他攻擊者截獲，讀寫器與標籤之間必須實現加密傳送。一旦標籤對讀寫器的認證沒有通過，標籤將拒絕傳送所儲存的信息。但是，這種帶密鑰的認證策略同樣有可能會受到中間人扮演攻擊(man in the middle attack)、重送攻擊(replay attack)等方式的攻擊。因此開發更有效、更安全的加密機制，改變 RFID 傳送資訊，以避免非法者追蹤，是未來 RFID 應用上的研究目標及被迫切關注的議題。接著在第三章中我們將建立本論文的研究方法，進一步探討如何建立一有效之安全加密機制，應用於 RFID 系統中。

近年來由於無線射頻識別技術的快速發展，使得 RFID 的相關應用逐漸增加。EPC Class-1 Generation-2 (簡稱 Gen-2)標準為 EPC global Inc.近來發佈的 RFID 重要標準，標準中明確定義 RFID 讀取機與 RFID 電子標籤的通訊方式、運作程序、指令及標籤的相關規範。Gen-2 標籤為一被動式的標籤，標籤內含有一電子產品編碼(Electronic Product Code, EPC)可識別特定單一物品，其主要安全特性是：僅支援擬亂數產生函數(PRNG)與循環冗餘碼(CRC)產生函數，而不支援進階的密碼函數，例如：單向雜湊及加解密函數等。

RFID 認證機制主要是用來確認 RFID 電子標籤的有效性並保護 RFID 電子標籤的隱私。目前大部分的 RFID 認證機制是需要線上伺服器的參與，也就是線上伺服器-RFID 讀取機-RFID 電子標籤這種模式，其中，RFID 讀取機只負責轉傳的動作，真正執行認證動作的是線上伺服器與 RFID 電子標籤，且線上伺服器與 RFID 讀取機之間是安全的通道。在上述的模式中，這個安全通道必須是可靠且持續保持連線的，然而在某些應用中，並不容易去維護這樣持續連線的安全通道，因此發展出具離線伺服器的 RFID 認證機制，在這種模式中，每次執行認證動作的是 RFID 讀取機與 RFID 電子標籤，而伺服器只有在必要的時候參與即可。

2. 相關方法回顧

1. Duc *et al.*安全架構: Duc *et al.* 於[1] 2006 年，提出了一個適用 Gen-2 的認證機制。原有的 EPC Class 1 Generation 2 RFID 系統的安全機制為後端 server 下達 kill 指令，使標籤失去效用，如此即可保障標籤不使用時，或商品售出後標籤資訊之安全。然而，此種 kill 模式為我們所不樂見的，因為 kill 指令

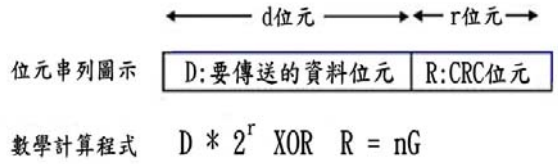
將使標籤失去效用，除了使標籤無法再利用，增加使用成本外; 此外，在商品售出後，顧客如需售後服務或作生產資訊查詢，也將無法有效利用 RFID 標籤登載資訊的優點。因此, Duc *et al.* 提出適合 EPC Class 1 Generation 2 RFID 系統的安全性增強機制，可防止攻擊者(attacker)的惡意追蹤及標籤複製，亦不需要利用 kill 指令，可使 RFID 標籤達到再利用的需求。在 Duc *et al.* 的安全機制中，利用兩種重要的函式運算: XOR 及 CRC(Cyclic Redundancy Check Code)錯誤偵測技術，分別說明如下:

1. XOR 運算: XOR 閘用來執行 XOR 運算，即若 X 與 Y 執行 XOR 運算，則 X 或 Y 恰一為 1 時，則輸出 Z 之值為 1。表 1 所示為 XOR 邏輯閘的真值表，X,Y 為 XOR 邏輯閘的輸入，而 Z 為輸出。

表 1 XOR 運算

輸入		輸出
X	Y	Z
0	0	0
0	1	1
1	0	1
1	1	0

2. CRC 錯誤偵測技術:又稱循環冗餘檢查碼(cyclic redundancy check)，CRC 的編碼運作說明如下



首先傳送端和接收端必須先要協議出某一個 r+1 位元的內容，我們稱它為產生器並以 G 來表示。傳送節點要將 d 位元的資料 D 傳送給接收節點，R 表示傳送端所選擇的 r 個額外位元，使得產生的(d+r)的二進位位元內容，使用 2 模數除法計算後剛好可以被 G 整除，如此可藉以判斷接收的資料是否正確，也就是說接收節點 將收到的(d+r)除以 G 之後，如果餘數是零，表示接到的資料是正確的，反之如果有餘數就是表示資料有錯誤，從 D 乘以 2r 除以 G 的餘數是 R，可用來計算 R。

Duc *et al.* 的安全認證機制程序如圖 1[1]所示:

首先後端 server 和每一個 tag 都分享了 tag 的 EPC 碼、PIN 和起始 key K0 ，而 Ki 表示在第 i 次認證後更新的金鑰。

1.Reader→Tag: Query request.
說明：讀取器產生詢問請求訊號，並傳送至標籤，通知標籤開始進行辨識。

2.Tag: 計算 M1=CRC(EPC ‖ r) ⊕ Ki 和 C=CRC(M1 ⊕ r).
說明：標籤計算:利用CRC計算出M1及C。

3.T→R→S: M1, C, and r.
說明：標籤Tag將M1, C及r送至讀取器Reader，讀取器Reader再進一步把M1, C及r送至後端伺服器server。

4.Server→Reader ,verify M1 and C.
說明：對於伺服器Server資料庫中的每一組變數(EPC,Ki)，伺服器Server 驗證是否M1 ⊕Ki = CRC(EPC‖r) ? 以及 C=CRC(M1 ⊕ r) ? 如果比對成功，伺服器Server將通過驗證並將標籤tag的資訊傳送到讀取器Reader進行下一個步驟。否則，伺服器Server將會停止進行並發出拒絕標籤Tag的程序。

5.S: M2= CRC(TID‖PIN‖r)⊕Ki, 然後 R 傳送 M2 to T.
說明：Server 伺服器計算M2= CRC(EPC‖PIN‖r)⊕Ki,將M2傳送給讀取器Reader , 讀取器 Reader進一步將M2傳送給標籤Tag

6. S→R→T: S 傳送 M2 經過 R 然後給 T 驗證, 計算K_{i+1}=f(Ki) 更新 Ki
說明：在伺服器server計算的M2傳送給標籤Tag作為驗證之用。標籤Tag利用自己本身的

(PIN, r, EPC, Ki)驗證來自於伺服器Server的M2是否正確，如驗證成功，將會把標籤Tag本身的認證碼Ki更新至K_{i+1}，以做為下階段Tag讀取傳送之用。

變數說明如表1所示，其中Ki為認證碼，r為虛擬隨機碼，T為標籤，R為讀取器, S為後端伺服器。

表 1 Duc *et al.* 安全架構之變數說明

符號	解釋說明
$\mathcal{T}$	RFID Tag 標籤
$\mathcal{R}$	RFID Reader 讀取器
$\mathcal{S}$	Backend Server 後端伺服器
EPC	Electronic Product Code 電子產品碼
$f(.)$	PRNG Function PRNG 函數
$CRC(.)$	CRC Function CRC 函數
K_i	Session Key for i-th Session 第i次會議金鑰
PIN	Personal Identification Number個人身份確認碼
r	A Pseudo-random Number Pseudo 亂數
$\mathcal{A}$:	實體A的動作
$\mathcal{A} \rightarrow \mathcal{B}$	從A到B的通訊
$\mathcal{A} \leftrightarrow \mathcal{B}$	在A和B之間的相互動作

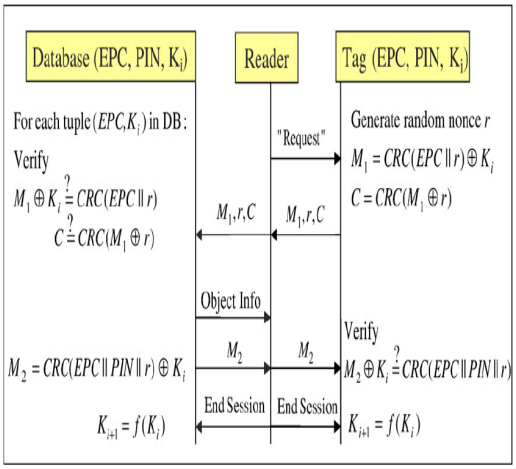


圖 1 Duc *et al.* 安全架構

Duc *et al.* 提出之 RFID 安全性架構如圖[1]所示，然而此架構卻仍存在有惡意阻斷、偽造標籤、及無法達到向前安全等安全問題，其安全疑慮如下：

1. 惡意阻斷(Denial-of-Service):當攻擊者惡意阻斷第六階段 S→R→T 間的 Ki 更新動作時，將影響 Server 更新認證碼，造成 Server 更新為 K_{i+1}，而標籤卻仍停留在 K_i，使得 Server 認證碼與 Tag 認證碼變的不一致，造成阻斷。因此，Chien *et al.* 於 2007 年提出標籤與 Server 共同驗證架構，以解決惡意阻斷之問題 [2]。
2. 偽造標籤: 如攻擊者惡意阻斷 Ki 更新動作時，此時如有一偽造標籤送出先前的(M1, r, C)碼，則會使系統誤認為其為合法之標籤，達到偽造的效果。
3. 無法達到向前安全: 假設某一個標籤洩露，而被攻擊者取得 (EPC, PIN, Ki)的值，並從之前 Tag 的通訊中竊取到(M1, M2, r)的資料，藉由驗證 M1⊕M2= CRC(EPC⊕r)⊕CRC(EPC || PIN || r)，可以認定此通訊是否來自相同的 Tag，然後利用取得的(EPC, PIN, Ki)值和竊聽到的 r 值，攻擊者可以用相同的計算來確認此為與先前商品售出時是否為同一標籤，使顧客之隱私洩漏。

Chien *et al.* 安全架構

Chien *et al.* 指出 Duc *et al.* 架構有惡意阻斷、偽造標籤、向前安全之缺點。基於改善 Duc *et al.* 認證機制，Chien *et al.* 提出了新的認證機制，以解決惡意攻擊的問題如圖2[2]所示。此架構利用 K_{x_i} 認證碼(authentication key)及 P_{x_i} 達成碼(access key)雙認證的機制，解決惡意阻斷及偽造標籤的功能。在每一次使用標籤後，認證碼及達成碼將會同時更新。其架構運作模式如下:

1. R→Tagx ：N1

Reader 初始先送隨機碼 N1 通知 Tag.

2. Tagx→R→S: M1, N1, and N2.

Tag產生隨機碼N2，並計算M1=CRC(EPCx || N1 || N2) ⊕ K_{x_i}，然後將M1, N1, 和N2回傳到reader，再由reader送至後端server。server計算出 I_{old}=M1⊕K_{old}及 I_{new}=M1⊕K_{new}，並驗證 I_{old}

或I_{new}是否等於M1，如果驗證成功，則伺服器將會進行下一步，如驗證失敗，則伺服器將送出failure訊息給reader停止運作。

3. S→R: M2,DATA

如果第2階段中，server對tag的驗證成功的話，伺服器會根據K_{old}或K_{new}何者滿足第2階段的認證計算程式？藉以計算$M2=CRC(EPCx \| N2) \oplus P_{old}$ 或 $M2=CRC(EPCx||N2) \oplus P_{new}$，同時更新$K_{old}=K_{new}$、$P_{old}=P_{new}$、$K_{new}=PRNG(K_{new})$、$P_{old}=PRNG(P_{new})$，並將M2和DATA送至reader。

4. R→Tagx: M2

Reader 藉由資料DATA更新產品資訊並將M2進一步傳送給Tag

當Tag收到M2時，Tag驗證$M2 \oplus P_{x_i}$是否等於$CRC(EPCx \| N2)$，如驗證成功，將更新$K_{x_i+1}=PRNG(K_{x_i})$及$P_{x_i+1}=PRNG(P_{x_i})$。

透過Key的更新，可以抵抗replay及偽造標籤攻擊，對每一個Tag同時保有新和舊的Key認證碼之雙向認證機制，可有效防止DOS惡意阻斷的惡意攻擊，Chien *et al.*的安全架構如圖2[2]所示。

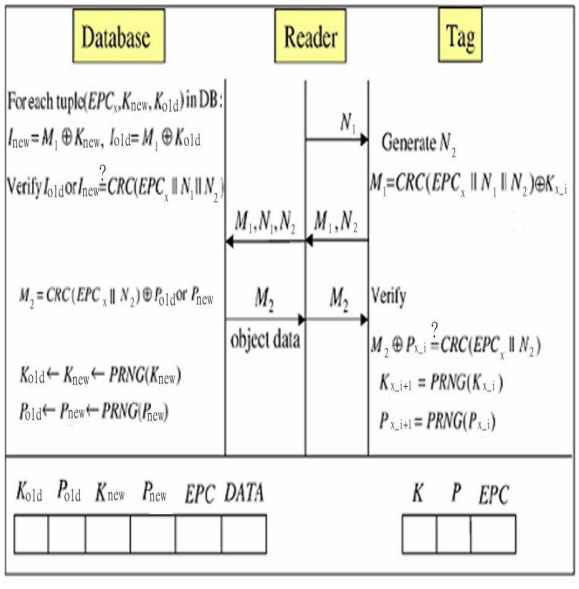


圖 2 Chien *et al.*安全架構

但是 Chien *et al.*提出的機制在所有現存及將來的 RFID 應用當中，仍舊存在偽造標籤及無法達到向前安全的問題。如果其標籤洩露，被攻擊者取得 (Pi,Ki,EPC)的值，並從之前 Tag 的通訊中竊取到(M1,M2,N1,N2)的資料，攻擊者仍然可能藉由驗證 M2⊕Pi 是否等於 CRC(EPC‖N2)中，追蹤到此通訊是否來自相同的 Tag，因而可確認此為與先前商品售出時是否為同一標籤。由此可知，建立一更為有效之 RFID 安全架構有其必要性。

3. 本論文方法

本研究目的在探索應用 RFID 時所產生的隱私權問題，並希望能找出增進 RFID 安全性的方式。因此本研究架構為透過分析已發表的 RFID 相關文獻探討其機制，研究其安全性，並提出一新的機制，研究架構如圖 3 所示。

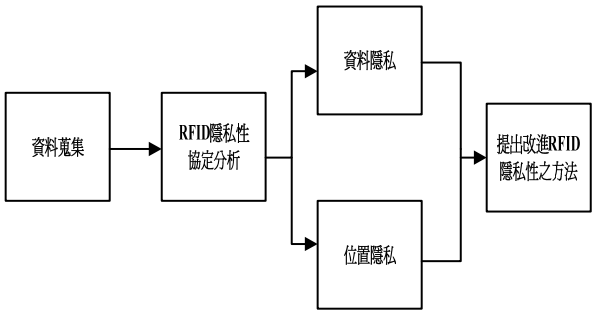


圖 3 研究架構

目前大部分的 RFID 認證機制是需要後端資料庫的參與，也就是後端資料庫-RFID 讀取機-RFID 電子標籤這種模式。2006 年，Duc *et al.*提出了一個適用 Gen-2 標準的具線上伺服器的認證機制，但是此機制仍存在有阻斷服務(Denial-of-Service)、偽造標籤(Counterfeit Tag)、及無法達到向前安全(Forward Security)等安全問題。而後續許多研究均針對此 Duc *et al.*的方式，作改進及探討，因此在以下研究中，我們將針對此安全協定作探究，並提出 RFID 隱私性之機制，其研究流程如圖 4 所示。

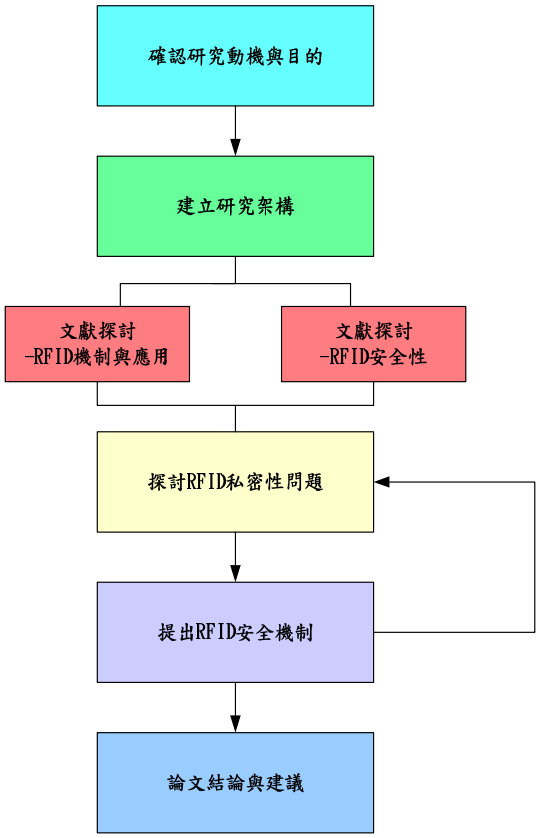


圖 4 研究流程圖

我們提出一適用於 EPC Class 1 Generation 2 RFID 系統的新穎安全架構，並對此架構作探討。此架構特點為，我們將透過建立兩項階段碼，同步應用於標籤與 Server 中，並對虛擬隨機碼與兩項階段碼先進行 XOR 運算，使惡意阻斷者無法藉由重覆讀取的方式，取得此標籤資訊，以增進安全性。我們提出之架構如圖 5 所示，說明如下：變數說明：a_i, b_i 為階段碼，z_i 為系統更新驗證碼，r 和 n 為虛擬隨機碼，T 為標籤，R 為讀取器，S 為後端伺服器。

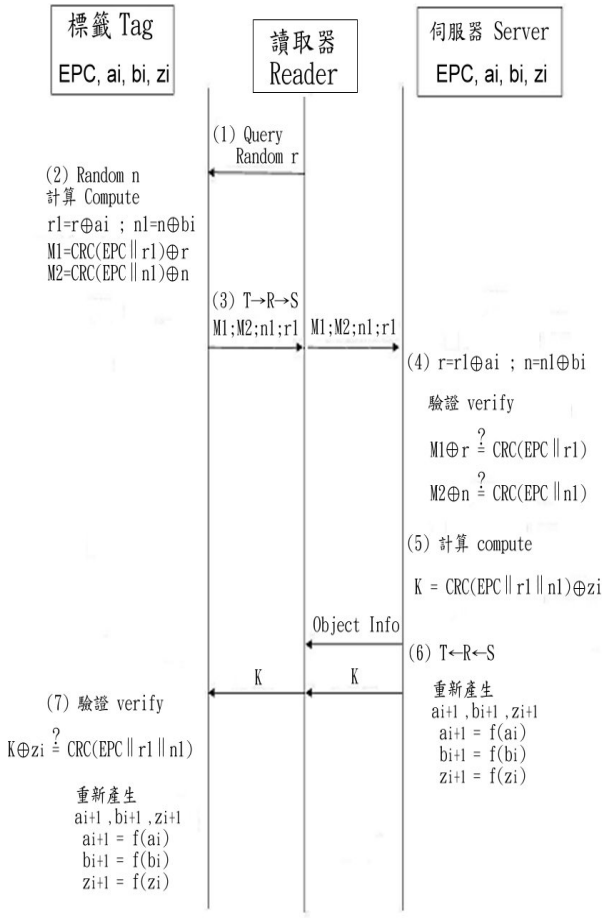


圖 5 我們提出之 RFID 安全架構

其架構運作模式如下:

1. Reader→Tag: Query request.
讀取器產生詢問請求訊號，同時產生一個亂數r，並傳送至標籤，通知標籤開始進行辨識。
2. Tag: 產生亂數n,計算
r1=r⊕ai,n1=n⊕bi,M1=CRC(EPC ‖ r1)⊕r1和M2=CRC(EPC ‖ n1)⊕n1
3. T→R→S: M1 ; M2 ; n1 ; r1
Tag 經由Reader將M1 ; M2 ; n1 及 r1傳送到Server
4. Server: 計算r=r1⊕ai,n=n1⊕bi
並驗證是否M1⊕r=CRC(EPC ‖ r1)? 和M2⊕n=CRC(EPC ‖ n1)?

5. Server: 計算
   K=CRC(EPC‖r1‖n1)⊕Zi
6. S→R→T: Server 將 K 經由Reader傳送到Tag
7. Tag驗證是否K⊕Zi=CRC(EPC‖r1‖n1)? 如驗證成功,將會把Tag階段碼ai,bi 及系統更新驗證碼zi更新至a_{i+1} b_{i+1} z_{i+1}，以做為下階段Tag讀取傳送之用。

本研究的RFID資訊安全主要是經由亂數值r,n將ai,bi 及EPC 隱藏起來， 所以Tag在傳送EPC時能夠防止ID的外洩使標籤受到保護達到私密性的要求，即使受到偽造標籤的攻擊也無法讓攻擊者從傳送的資訊之中獲得 Tag 的ID [3]。

Tag 跟 Server 兩端內存有有共同的a_i ,b_i ,z_i，透過XOR的計算，將隨機碼r隱藏在與階段變數作用之r1及n1中，使攻擊者不易經由重覆讀取攻擊(replay attack)竊取標籤之隱私。在第(5)~(7)的階段，我們利用Server對Tag提出的認證機制，使攻擊者不易經由惡意阻斷的攻擊，破壞標籤的再利用，可有效達到安全防護的需求。

4. 安全性分析

為了達到良好的安全性，一個RFID架構必須在互相認證和私密匿名性上達到使用上的要求，並能面對攻擊者的入侵與破壞，在此將針對我們方法的特性，分析其私密匿名性和互相認證性：

A. 互相認證性：首先在標籤和後端資料庫內存有共同階段碼及系統更新驗證碼和標籤的EPC 做為互相認證之用，通過亂數的產生及簡單的加密，讓彼此的訊息在安全和保密的狀況之下經由挑戰與回應的過程進行會議的通訊，在確認通訊的雙方彼此互相經過解密計算和互相驗證 EPC 的合法性之後，以完成對讀取器的信任。

B. 私密和匿名性：在互相傳送過程中我們沒有直接傳送EPC的訊息，也就是用隨機亂數和金鑰將EPC隱藏起來，有效的保護了標籤的個別資料，使客戶的隱私不被洩露，達到了私密性的要求。

4.1 抵擋受攻擊性分析

我們將針對RFID在應用中，比較可能遇到的攻擊加以探討分析，我們就此提出的攻擊模式如：重送攻擊、偽造攻擊、向前金鑰安全、猜測攻擊，經過分析之後，我們的方法可以承受這些的攻擊：

A. 重送攻擊：由於我們的讀取器和標籤內在每一回合中都加入了亂數並且對階段碼和系統更新驗證碼進行XOR的加密計算，而且在每回合結束後對階段碼和系統更新驗證碼作更新，使攻擊者即使取得上回合的金鑰，作重送攻擊的動作，也無法通過後端資料庫的認證。

B. 偽造攻擊：如同以上的攻擊，Tag 跟Server兩端所有共同的 a_i ,b_i ,z_i，在每一回合都更新過，就算標籤的EPC被取得，因為我們將隨機碼r隱藏在與階段變數作用之r1及n1中，並且透過XOR的計算，在偽造的Tag 要去取得後端資料庫的認證時，仍然無法通過驗證，所以我們的方法可以抵擋偽造攻擊。

C. 向前金鑰安全：我們在每一回合的會議時，將更新過的金鑰以及隨機亂數和傳送的訊息經由XOR結合和CRC偵錯，確保訊息的正確和私密性，就算舊的金鑰被取得，因為前後回合沒有任何關聯，所以可以確保訊息不被破解。

D. 猜測攻擊：由於我們每一次的會議程序都會將金鑰更新而且金鑰是由 PRNG 函數隨機產生的，所以攻擊者無法在有效的時間內猜測出正確的金鑰。

5. 結論

我們的研究以達到讓使用者在要求服務時

的隱私性，使通訊內容保密且讓使用者真正達到匿名性。在 RFID 標籤使用過程中，一個未受安全保護的標籤，攻擊者可以經由竊聽或者實體攻擊取得標籤內容，進而分析解讀儲存在標籤內的資訊，去取得個人的資料或產品的資訊，個人的資料或產品的資訊便被洩露了。因此需要藉由一適當之安全認證機制，使 RFID 能同時滿足再利用性與安全性之需求。由於惡意攻擊者可以利用非法的讀取器或偽造標籤施以主動式攻擊，取得使用者標籤用來交換金鑰的秘密。因此本論文所提出的改進方法需能有效抑制阻斷及偽造標籤之惡意攻擊，讓 RFID 在使用時具有產生亂數能力的隨機雜訊標籤，使得該標籤所產生用來保護正常通訊之雜訊碼無法被辨識與重製。

參考文獻

[1] D.N. Duc, J. Park, H. Lee, and K.G. Kim,“Enhancing Security of EPC global Gen-2 RFID Tag against, “The 2006 Symposium on Cryptography and Information Security, 2006.

[2] H.Y. Chien and C. H. Chen,“Mutual Authentication Protocol for RFID Conforming to EPC Class 1 Generation 2 Standards,” Computers Standards & Interfaces. Vol.29, pp. 254-259, 2007.

[3] D. Henrici and P. Müller, “Tackling Security and Privacy Issues in Radio Frequency Identification Devices,” Security in Pervasive Computing, LNCS 3001, pp. 219-224, 2004.