基於單向雜湊函數鏈的 RFID 安全協定

葉 慈 章
明新科技大學資訊管理系
cheer@must.edu.tw

徐 謚
明新科技大學資訊管理系
supant@seed.net.tw

摘要

RFID 技術近年來隨著成本的降低與標準的制定，逐漸取代條碼，已廣泛地應用於許多領域，號稱二次 IT 革命。由於無線傳輸的方式，使其安全性備受關注；近年來許多學者已提出許多解決方案，其中單向雜湊函數鏈提供了較佳的向前安全性。

2006 年 Lee 等人使用單向雜湊函數鏈保護 RFID 訊息的傳遞，達到雙向鑑別、機密性與向前安全性，並避免因訊息遭攔截，Tag 與資料庫不同步而造成的阻斷服務攻擊；然而 Reader 未經鑑別，非法的 Reader 因此可讀取 Tag 的資料並向資料庫取得對應的紀錄;此外，由於伺服器無法確認收到訊息的真確性，無法避免 Tag 假冒的問題。在本篇論文中，我們將詳細分析上述問題產生的原因，並提出修正協定以避免這些問題。

關鍵字：RFID、安全、隱私

Abstract

Recently, with the reduction of cost and establishment of standards, the RFID (Radio Frequency Identification) technology has been widely applied to many domains, and has gradually substituted for the bar code, leading possibly to a second IT revolution.

The widespread deployment of RFID tags threatens individual's and organization's privacy and security. In recent years many researchers have proposed various solutions; among them, one-way hash-chain function can provide better forward security.

In 2006, Lee et al. used one-way hash-chain function to protect information transmission of RFID, achieved mutual authentication with confidentiality and forward security, and avoided service breakdown due to information interception and asynchronousness between tags and the back-end server. However, since Lee et al.'s protocol does not provide authentication of the readers, illegal readers may read tag information and obtain the corresponding records in the back-end server; furthermore, the back-end server is unable to guarantee information integrity, creating the problem of counterfeit tags .In this paper, we analyze the above problems, and propose a correction protocol to avoid these problems.

Keywords： RFID、Security、Privacy、Forward Security

1.簡介

無線射頻識別 (Radio Frequency Identification, RFID)被視為本世紀最重要的十大技術之一，此技術早在二次世界大戰時就已經使用於軍方的敵我辨識系統。RFID 是一種非接觸式的射頻辨識系統，主要是由標籤(Tag)、讀取器(Reader)和後端資料庫（Back-End Database）所組成。

- 標籤(Tag)：由具有類比、數位與記憶體功能的晶片，以及依不同頻

率、應用環境而設計之天線所組成。Tag 可分成三種：被動式(Passive)－由讀取器的 RF 電場獲得能量以回傳資訊，本身無電池，體積小、使用期限較長，但讀取的距離較短，主要用在物流和目標追蹤；主動式(Active)－本身有電池與喚醒裝置，平時標籤是處於休眠的狀態，當標籤進入喚醒裝置的範圍時，即進入工作模式，開始傳送相關資訊。由於本身具備電源故傳輸距離較長，可達數十公尺，但體積較大、需更換電池及成本較高；半被動式(Semi-Passive)－具備電源，但電源僅供 Tag 內部的運作；仍需透過 Reader 傳送的無線電波，以產生感應電流回傳內存訊息。

- 讀取器(Reader)：由類比控制、數位控制、中央處理單元以及讀取天線組所組成，讀取器能同時辨識數百個不同的 Tag，將讀取到的 Tag 訊息傳送到後端資料庫以取出對應的記錄。
- 後端資料庫（Back-End Database）：儲存產品及 Tag 內容的相關資料，如：產品名稱、Tag 的 ID 編號等。

隨著技術進步與成本的下降，RFID 廣泛應用在許多領域；如供應鏈管理、門禁系統、電子付費、動物自動化管理、自動收費系統、品質管理等方面等。據 Wal-Mart 內部評估，導入 RFID 系統後一年內省下的成本高達 83.5 億美元，而根據國外研究單位 SROC-B1 的估計，2008 年全球 RFID 直接產值將高達 30 億美元、間接產值更高達 90 億以上[1]，RFID 技術在物流業的應用潛力已受到全世界矚目，對產業界所造成的衝擊影響範圍頗為深遠，各國政府多積極輔導協助業界導入，因此有人以「二次 IT 革命」來形容此技術的潛能及發展性。

表 1　RFID 與 Bar Code 比較

特性	RFID	Bar Code
傳輸方式	無線射頻傳送	紅外線掃瞄讀取
資料儲存容量	晶片記憶體容量大	位元數制容量小
重複寫入	可覆寫資料	無法重覆寫入
安全性	高	易被偽造
成長度	不斷有新編碼標準推出	已達極限無新技術
價格	成本逐漸下降	便宜
損毀	不因外表模糊而無法使用	遭塗改則不易辨識
讀取數量	可同時多個	一次一個

(資料來源:[2])

RFID 的開發運用提高了便利性，相對地也延伸了安全性與隱私權的問題，例如：衣服的晶片遭非法讀取，洩漏出穿著價值，引誘犯罪；或是嵌入鞋內的 Tag 則可發送行蹤動向訊息，分析出使用者的習性與偏好等[16]。

2. 文獻探討

在 RFID 系統中，Tag 與 Reader 的訊息是透過空氣傳遞無線訊息來進行溝通，駭客能攔截或竊聽以進行非法行為，我們由相關文獻[8,15]整理出探討目前常見的 RFID 可能的威脅如下：

- 重送攻擊：攻擊者攔截 Tag 與 Reader 間傳送的資訊，事後非法重送欺騙合法裝置以通過鑑別。
- 向前安全性攻擊：日後標籤內容若遭破解，其之前的交易訊息可過去的紀錄中被辨識出與追蹤。

- 阻斷服務攻擊：攻擊者惡意傳送大量訊息，導致 RFID 系統癱瘓無法提供正常的服務;或是從中攔截竄改訊息，造成 Tag 與 Server 因不同步而無法完成鑑別。
- 隱私顧慮：駭客在 RFID 的無線傳送中竊聽傳輸的訊息，藉此分析出消費者的購物習性；或藉由 Tag 中的固定值進行追蹤。
- 身分假冒：攻擊者可能假冒 Reader 非法讀取 Tag，並向資料庫取得 Tag 的對應紀錄；攻擊者也可能假冒 Tag 傳送特定訊息以干擾系統的運作。

針對 RFID 的安全與隱私問題，目前有下列方法：

I. 物理方法：

- Kill command[7]：由 Auto-ID Lab 中心提出，執行 “kill”的命令，則 Tag 的所有功能都將被永久關閉無法再使用；消費者可在購買產品後執行 kill 命令讓 Tag 失效，但這種方法限制了 Tag 日後的應用功能，例如：產品的售後服務、回收等。
- Faraday Cage[10]：法拉第遮罩，利用電磁原理把 Tag 放置於由金屬網或金屬薄片組成的容器中阻隔無線射頻訊號，防止讀取。
- Active jamming[11]：利用主動發出無線干擾信號的設備對無射頻信號進行干擾，使附近射頻辨識系統的 Reader 無法正常運作，達到保護隱私的目的。但這種方法多數情況下是違法，會干擾正常使用的 RFID 設備，也可能影響其他無線電設備的使用，形成另一種阻斷服務模式。
- Blocker Tag[5]：由 RSA 公司提出的阻擋標籤，可以選擇性的阻擋讀取設定為隱私狀態的 Tag，但不影響設定為開放狀態的 Tag 之正常運作。例如當商品在未被選購時，Tag 設定為開放狀態，商家的 Reader 可以讀取 Tag 訊息；商品出售時 Tag 則被設為隱密狀態，確保物品訊息不被任何 Reader 再讀取。缺點在於顧客必須持有阻擋標籤才能保證隱私不被侵犯，造成顧客額外的負擔。
- Clipped Tags[9]：IBM 公司所推出分離 Tag 的方法，將 Tag 上的天線與晶片分開，結帳後消費者可自行撕去天線，縮短 Tag 的讀取距離，以增加隱私保護，Tag 仍可運作，提供日後貨品的售後服務或退貨的處理，但此方法成本較高。

II. 密碼學方法：

- Hash-lock protocol[18]：由 Weis 等人在 2003 年提出，以單向赫序函數進行存取控制。Tag 與 Reader 共享一個秘密金鑰。Reader 詢問時，Tag 將秘密金鑰進行單向赫序函數運算產生 MetaID 傳給 Reader，Reader 再以此值至後端資料庫找出對應的 Unlock Key，以將 Tag 狀態轉為 Unlock，便可讀取 Tag 的內存資訊。然而由於 MetaID 為固定值，駭客因此能透過此固定值對 Tag 進行追蹤。
- Randomized Hash-lock[19]：加入亂數的使用，使得 Tag 每次傳出的回應訊息成為無法預測的非固定值，增加隱私保護避免追蹤。
- Re-encryption：Juel 和 Pappu [21]將嵌在歐元紙鈔裡的 Tag 序號以法定的公開金鑰加密，未持有相對私密金鑰的 Reader 即使讀出也無法解密，為避免被追蹤，經公開金鑰加密產生的密文會定期經 Reader 作重新加密；然而這

種方法需要有大量計算能力的設備，成本過高。

- Hash-Chain Protocol：Ohkubo[4]等人提出使用單向雜湊函數鏈來保護RFID傳遞的訊息，可達到機密性與向前安全性[3] [13]，然而無法避免重送攻擊。Avoine [6]提出了解決重送攻擊的方法，利用挑戰與回應，使駭客無法使用竊聽到的資訊進行重送攻擊。然而在 Ohkubo 與 Avoine 的協定中，當傳遞的訊息遭攔截或竄改，會造成 Tag 與資料庫兩端金鑰更新不同步，產生阻斷服務攻擊。LEE 等人[12]利用儲存金鑰的新值與舊值，解決更新不同步的問題；但 Selwyn [14]指出在 Lee 等人的協定中，伺服器無法確保訊息的真確性，駭客修改 Tag 的回傳訊息，DB Server 未能查覺而通過鑑別，造成 Tag 的假冒；此外，上述各協定中 Reader 皆未經鑑別，非法的 Reader 可任意讀取 Tag 的資料並向資料庫取得對應的紀錄。

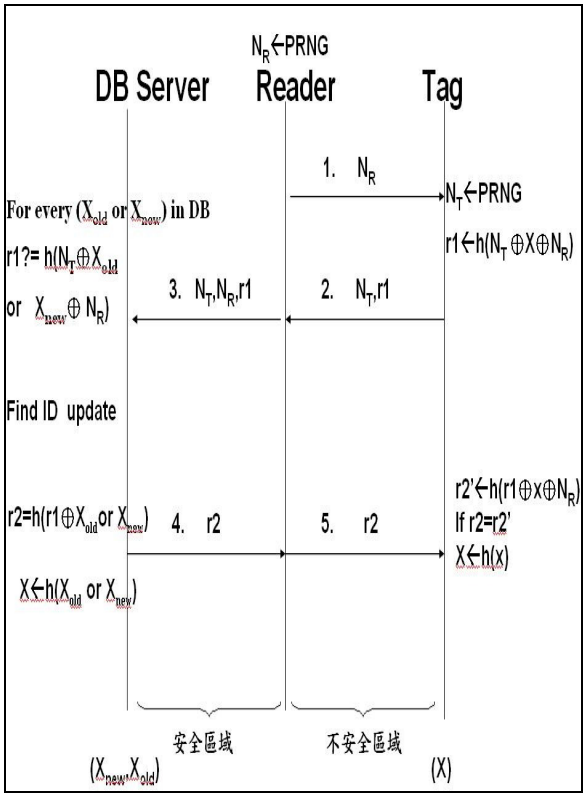

圖 1 Lee 等人的協定

3. Lee 等人的協定

表 2 符號說明

符號	說明
X	Tag 與 Server 共享的密鑰。
h()	hash function 單向赫序函數。
⊕	Exclusive-OR (XOR)運算。
Data	DB Server 中儲存 Tag 對應的物品資料。
X_{new}	DB Server 中儲存 Tag 對應的鑑別新值。
X_{old}	DB Server 中儲存 Tag 對應的鑑別舊值。

各設備內存的資訊：

Tag： X

DB server：X_{new}, X_{old}, Data

流程說明：

1.Reader → Tag： Reader 產生亂數 N_R 傳給做為讀取請求。

2.Tag → Reader：Tag 產生亂數 N_T，將 N_T 與 Tag 內存的密鑰 X 與收到的 N_R 做 XOR 後經雜湊函數運算為 r1；並與 N_T 一起傳送給 Reader。

3.Reader → Server：Reader 將收到的 N_T、r1 連同 N_R 一起傳給 Server。

- Server 進行下列運算；逐一將資料庫每筆記錄中的(X_{new}、X_{old})帶入 X 計算 h(N_T⊕X⊕N_R)，找出 r1 值相等的對應紀錄，並確認該次讀取共享密鑰 X 是以新值(X_{new})或是舊值(X_{old})來通過鑑別。

- 將通過鑑別的 X_{old} 或 X_{new} 與 r1 做 XOR 後經赫序函數運算為 r2。
- 若通過鑑別的為記錄中 X_{new}，則以新值取代舊值($X_{new}=X_{old}$)；否則重新產生新值 $X_{new}=h(X_{new})$，如果通過鑑別的為 X_{old}，Server 則停止更新 X_{old} 持續以 X_{old} 來鑑別 Tag。

4.Server → Reader：Server 產生 r2 傳送給 Reader。

5.Reader → Tag：Reader 轉送 Server 傳來的 r2，跟 Tag 內存的 X 與 r1 經雜湊函數產生的 r2'比對是否一致，如鑑別成功，Tag 更新密鑰 X 為 h(X)。

4. Lee 等人的協定問題

- **重送攻擊**：駭客將 Reader 傳給 Tag 的讀取請求 N_R 竄改為 0，以騙取 Tag 回傳的 $r1=h(N_T \oplus X \oplus 0)$，再將 Tag 回傳的 N_T 竄改為$(N_T \oplus N_R)$。Reader 收到遭竄改過的 r1、N_T後連同自己產生的N_R傳給 Server；Server 以資料庫中儲存的 X(逐筆代入)與收到的 N_T、N_R 自行計算出 $r1=h((N_T \oplus N_R) \oplus X \oplus N_R)=h(N_T \oplus X)$，再與收到的 r1 比對，相同則通過鑑別。由於 Server 無法查覺訊息已被竄改，接下來駭客再攔截或竄改 r2，使 Tag 無法完成驗證與更新 X 值，此後便可以 $r1=h(N_T \oplus X)$重送給 Server，假冒 Tag 通過鑑別。如此消費者則可以便宜物品的 Tag 來替代昂貴物品上的 Tag 通過結帳。
- **隱私顧慮**：假設後端資料庫及 Reader 為安全的傳輸區域，Data 資訊以明文傳送，但許多實際的應用上多使用手持式的 Reader 與後端資料庫以無線傳輸作連結[22]，在此協定中駭客可偽造合法的 Reader 進行中間人攻擊[17]，即使的訊息是以 SSL 加密保護傳送，亦無法確保 Reader 的合法身分[20]。
- **身分假冒**：只鑑別 Tag 與 Server，而未鑑別 Reader 的身分，非法的 Reader 則可讀取 Tag 的資料並向資料庫取得對應的紀錄。

5. 我們提出的協定

我們沿用上述的符號定義，唯新增 Reader 的唯一識別碼 RID。

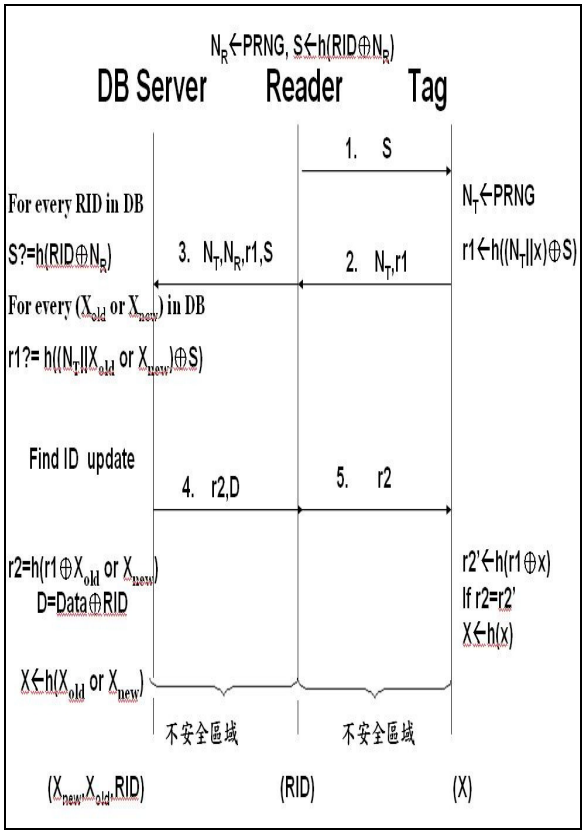

圖 2 我們提出的協定

各設備內存的資訊：

Tag：X

Reader：RID

DB server：RID ,X_{new} ,X_{old} ,Data

流程說明：

1.Reader → Tag：Reader 產生亂數 N_R，並與 RID 經雜湊函數計算出 $S=h(RID \oplus N_R)$，傳給 Tag 做為讀取請求。

2.Tag → Reader：Tag 產生亂數 N_T，將 $r1(N_T$ 與內存的密鑰 X 先做連結，再與收到的 S 做 XOR 後經雜湊函數運算出 r1) 傳送給 Reader。

3.Reader → Server：Reader 將收到的 N_T、r1 連同 N_R、S 一起傳給 Server。

- Server 進行下列運算；先將 Reader 傳來的 N_R 與資料庫中的 RID 逐筆搜尋計算找出 S 值相等的對應紀錄，其中比對 Tag 收到 Reader 傳來經計算的 S 及 Reader 傳回的 S 是否一致；再來逐一將資料庫每筆記錄中的 (X_{new}、X_{old})帶入 X 計算 $h((N_T \| X \oplus N_R)$，找出 r1 值相等的對應紀錄，並確認該次讀取共享密鑰 X 是以新值(X_{new})或舊值(X_{old})來通過鑑別。
- 將通過鑑別的 X_{old} 或 X_{new} 與 r1 做 XOR 經赫序函數運算後為 r2。
- 若通過鑑別的為記錄中 X_{new}，則以新值取代舊值($X_{new}=X_{old}$)；否則重新產生新值 $X_{new}=h(X_{new})$，如果通過鑑別的為 X_{old}，Server 則停止更新 X_{old}，持續以 X_{old} 來鑑別 Tag 。

4.Server → Reader：Server 將儲存對應 Tag 的物品資料 Data 與 RID 計算後為 D，與計算的 r2 一起傳送給 Reader。

5.Reader → Tag：Reader 以 RID 經 XOR 計算取出 Data，並轉送 Server 傳來的 r2 給 Tag， Tag 將內存的密鑰 X 與 r1 經雜湊函數產生的 r2'比對是否一致，如鑑別成功 Tag 更新密鑰 X 為 h(X)。

6. 協定之分析

- **重送攻擊**： Lee 等人的協定[12]產生重送的原因在於 Server 無法查覺所收到的資訊被竄改，並以收到經竄改的 $N_T' = (N_T \oplus N_R)$，帶入計算 $r1=h((N_T \oplus X) \oplus N_R \oplus N_R)$，藉由消去 N_R 得到 $r1=h(N_T \oplus X)$，與收到的 r1 相同而通過鑑別。在我們的協定中 Reader 將產生的亂數 N_R 以 Reader 與 Server 的共享密鑰 RID 保護，當作挑戰值 S，攻擊者若竄改傳給 Server 的 N_R 或 S，兩者將因不具一致性而為 Server 查覺。此外，我們將 r1 中 N_T 與 X 間的運算子由 XOR(⊕)改為連結(‖)，使攻擊者即便將 N_T 竄改為($N_T \oplus S$)而得到 $r1=h((N_T \oplus S) \| X) \oplus S)$，也無藉由消去 S 而通過 Server 的驗證。
- **向前安全性**：利用單向雜湊函數鏈不可逆推的特性，駭客無法藉由破解 Tag 中存的 $h^n(X)$，而逆推出之前的內存值 $h^{n-1}(X)$、$h^{n-2}(X)$、…，因此無法由過去的交易紀錄中進行辨識與追蹤。
- **阻斷服務攻擊**：Server 存有新舊 X_{new}、X_{old} 兩值，以避免訊息遭攔截時 Tag 與資料庫不同步的問題所造成的阻斷服務攻擊。
- **隱私顧慮**：駭客能竊聽並收集傳輸期間的訊息，但訊息皆為亂數和單向雜湊函數保護，駭客無法追蹤出交易內容。
- **身分假冒**：現有的協定多只鑑別 Tag 和 Server 兩者的身分，我們增加了對 Reader 的鑑別，以避免非法的 Reader 讀取 Tag 的資料並向資料庫取得對應的紀錄。

我們將提出的協定與 Lee 等人的協定做分析比較如表 3。

表 3 安全協定之比較

協定 / 威脅	Lee 等人的協定[12]	我們提出的協定
重送攻擊	X	O
向前安全性	O	O
阻斷服務攻擊	O	O
隱私顧慮	X	O
身分假冒	Reader	O

7. 結論

RFID 技術已廣泛地應用於許多領域，逐漸取代條碼，使用者的隱私與安全顧慮也隨之提升。目前許多學者已提出許多解決方案，其中運用單向雜湊函數鏈的協定能提供較佳的向前安全性；目前使用單向雜湊函數鏈的協定均仍有安全上的問題，為了避免這些問題，我們提出了一個改善協定，以提升 RFID 的隱私與安全。

誌謝

本研究承蒙行政院國家科學委員會計畫（NSC 96-2416-H-159-001）經費之助，僅此致謝。

參考文獻

[1] 台灣微軟技術中心，http://www.microsoft.com/taiwan/mtc/event4.aspx

[2] RFID應用推動辦公室網站，http://rfid.org.tw/publish_review.php

[3]S. Kinoshita, M. Ohkubo, F. Hoshino and al, ”Privacy Enhanced Active RFID Tag”, ***Proceedings of 1st International Workshop on Exploiting Context Histories in Smart Environments***, Mark Weal, University of Southampton, UK, Feb. 23, 2005.

[4]Miyako Ohkubo, Koutarou Suzuki, and Shingo Kinoshita, Cryptographic approach to privacy-friendly Tags", ***RFID Privacy Workshop***, November 2003.

[5]Ari Juels, Ronald Rivest, and Michael Szydlo, The blocker Tag： selective blocking of RFID Tags for consumer privacy", ***ACM Conference on Computer and Communications Security, ACM CCS***, pp. 103- 111, October 2003.

[6]G. Avoine, E. Dysli, P. Oechslin, “Reducing Time Complexity in RFID Systems”, ***Proceedings of the 12th Annual Workshop on Selected Areas in Cryptography (SAC'05)***, 2005, pp. 291 – 306.

[7] S. E. Sarma, S. A. Weis, and D. W. Engels. “Radio frequency-identification security risks and challenges”, ***CryptoBytes***, 6(1), 2003.

[8] S. A.Weis, S. Sarma, R. Rivest, and D. Engels, “Security and privacy aspects of low-cost radio frequency identification systems”, ***In First Internation al Conference on Security in Pervasive Computing 2003***, LNCS 2802, pp. 201-212

[9] G. Karjoth and P. Moskowitz. “Disabling RFID Tags with visible confirmation： “Clipped Tags are silenced.” Research Report RC 23710, ***IBM Research Division,*** Zurich, Switzerland, 2005.

[10] Gildas Avoine and Philippe Oechslin, “RFID traceability： a mulilayer problem", ***Financial Cryptography FC***, pp. 125-140, March 2005.

[11] T. Hjorth. “Supporting privacy in RFID systems”, Master thesis, Technical University of Denmark, Lyngby, Denmark, December 2004.

[12] Sangshin Lee, Tomoyuki Asano, Kwangjo Kim, ”RFID Mutual Authentication Scheme based on Synchronized Secret Information” ***SCIS 2006***,Jan. 17-20, 2006.

[13] M. Ohkubo, K. Suzuki and S. Kinoshita, “RFID privacy issues and technical challenges”, ***Commun ACM,*** vol. 48, pp. 66-71, 2005.

[14] Selwyn Piramuthu, “Protocols for RFID Tag/reader authentication”, ***Decision Support Systems***, v.43 n.3, p.897-914, April, 2007

[15]William Knight, “RFID – another technology, another security mess?”, ***Infosecurity Magazine***, May June 2006.

[16]Position statement on the use of RFID on consumer products, http://www.spychips.org/jointrfid_position_paper.html, November 2003

[17] J. Yang, J. Park, H. Lee, K. Ren, K. Kim, “Mutual authentication protocol for low-cost RFID”, ***Handout of the Ecrypt Workshop on RFID and Lightweight Crypto,*** 2005.

[18] S. A. Weis. “Radio-frequency identification security and privacy”. Master's thesis, M.I.T. May 2003.

[19] S. A.Weis, S. Sarma, R. Rivest, and D. Engels.Security and privacy aspects of low-cost radio frequency identification systems. ***In First Internation al Conference on Security in Pervasive Computing 2003,*** LNCS 2802, pp. 201-212

[20] C. Ellison and B. Schneier, ”Ten Risks of PKI”, ***Computer Security Journal***, v 16, n 1, 2000, pp. 1-7

[21]A. Juels and R. Pappu. Squealing Euros, ”Privacy protection in RFID-enabled banknots”, ***Financial Cryptography03***, LNCS 2742, pp. 103-121, Springer-Verlag, 2003.

[22] J. Yang, J. Park, H. Lee, K. Ren, K. Kim, “Mutual authentication protocol for low-cost RFID”, ***Handout of the Ecrypt Workshop on RFID and Lightweight Crypto***, 2005