[1]RFID系統雙邊認證協定-兼具防偽及隱私保護之功能

劉昆琁*　陳明陽*　李忠憲*　鄭博仁**
*國立成功大學電機系 **高苑技術學院資管系

q3693433@mail.ncku.edu.tw cmy@crypto.ee.ncku.edu.tw jsli@mail.ncku.edu.tw
abjeng@cc.kyit.edu.tw

摘要

RFID 系統中的 Tag 及 Reader 透過射頻訊號以無線通訊方式進行資料傳輸，在無線的環境中容易因監聽、掃描這些攻擊行為而引起如：破壞資料隱私、位置隱私及偽造(假冒身份)等安全問題。因此，如何確保 RFID 系統與傳輸資料的安全為在建置 RFID 環境時一個重要考量。另外，在 RFID 系統中，Tag 本身的資源與計算能力是相當受到限制。在有限的成本考量下，如何達到雙方認證功能及防止資料洩露為一項挑戰。在本論文中，我們提出一套 RFID 雙向的認證機制，此機制能夠有效的達到雙方認證並防止敏感資料外洩。避免攻擊者利用監聽後重送資訊進行 RFID Tag 偽造的問題，使用此機制也可以達到某些程度下 Tag ID 保密的效果，此外由於不需密碼元件如：Hash、AES 等，因此在製作 RFID Tag 的成本也會相對的降低許多，而讓這套系統的應用能更一般化。

關鍵詞：無線射頻、RFID Security、隱私權、認證。

1. 基本概念介紹

RFID(Radio Frequency Identification)－「無線射頻身份識別系統」，其整個系統主要分成三大部分如圖 1：讀卡機(Reader)、電子標籤(Tag)、後端應用程式資料庫(Backend Database)所組成。Tag 及 Reader 透過射頻訊號以無線通訊方式進行資料傳輸，不須透過實體接觸就可以進行資料交換，且資料交換時亦無方向性的要求，能透過 ID 辨識來分辨、追蹤、管理物件。因此可以廣泛運用於倉儲或物流方面、取代傳統光學條碼(bar-code)及其它各種應用層面。

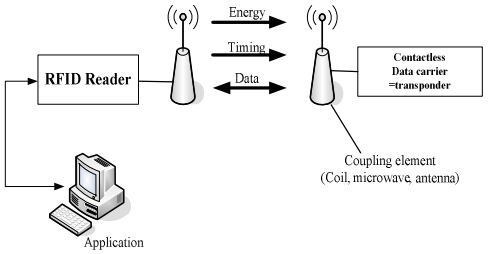

圖 1　RFID 系統方塊圖

今後在 RFID 系統普及時，如何保護個人隱私顯的格外重要。物品持有者會擔心自己在不知不覺下，被有心人士以掃描的方式讀取自己物品的 ID 進而得知商品資訊。如果物品 ID 與個人資訊結合(如電子錢包)時，意圖不軌者則可根據個人常帶上街的物品 ID，追蹤持有者的行蹤及所在位置。此外，當 RFID Tag 應用於商品防偽或門禁卡身分認證時，必需防範有人以描掃、通訊量分析等方式得到 Tag 內所有資訊，並假冒合法 RFID Tag 欺騙消費者或其它合法 Reader。

為了確保 RFID 系統與傳輸資料的安全，我們需考慮在 RFID 系統上達到：(a)確認性，即在建立傳輸通道時必須確認兩端是可靠、並確認其資料來源為無誤。(b)資料保密性，即確保傳送的資料不會遭受被動型態的攻擊(如監聽)。由於 RFID 為一低成本的裝置，因此其資源相當受限，傳統密碼系統的使用不符合 RFID 系統在一般使用上建置的成本考量，所以如何在此環境建立起安全服務為一項挑戰。

基於上述的原因，本論文發展一套簡單且能在低成本的 RFID 系統上，達到 Reader 和 Tag 雙方的認證，並保護使用者位置隱私及 RFID 資料的隱私。本論文將在第二章的部分詳述 RFID 系統可能的安全議題及目前有關 RFID 系統安全研究的相關文獻，並對不同的主題進行文獻分類。第三章則說明我們設計的安全機制與其理念，並對整個運作流程做詳細的說明，之後再利用一簡單的例子對整個機制運作方式做一個完整的描述。並在第四章設計多個攻擊場景來說明我們所設計系統的有效性。最後在第五章的部份做一個簡單總結。

2. 相關研究

本章第一小節會先針對 RFID 系統可能遭受的安全議題做一個簡單的介紹、並分析其攻擊的行為。之後會對目前已提出有關 RFID 系統安全的研究做詳細的描述。

[1] 本論文經費由國科會編號 NSC93-2745-E-244-001 補助

2.1 RFID 系統安全議題

RFID 系統採用無線方式進行通訊，一般而言在沒有安全防護下的無線網路會遭受到不同型態的攻擊，主要可以分為被動及主動這二種型式。

A.被動式攻擊

竊聽或監視傳輸中的資訊，解讀訊息內容或經流量分析得到想要的資料都是屬於這類攻擊，利用此攻擊行為可以獲取未受保護的 RFID Tag ID，並而判斷此物品的內容以及得知目前 Tag 持有人的所在位置。此種攻擊行為將影響 RFID Tag 持有人的物品資料及位置隱私等安全議題。

B.主動式攻擊

涉及資料的竄改或假造，可進一步再細分為四個類型：修改、偽裝、重送訊息、以及阻絕服務。在 RFID 系統環境中，攻擊者可能利用監聽的方式得到未受保護的 RFID Tag ID，進一步利用複製 ID 的方式或訊息重送的方式假冒此合法 Tag 的身份，進而欺騙 Reader。阻絕服務則是利用發出主動的射頻訊號使整個 RFID 系統癱瘓。在主動攻式攻擊下主要會產生 RFID Tag 假冒的問題。

2.2 RFID 系統安全相關研究

我們收集所有目前有關 RFID 系統安全方面的文章，並將這些文章根據不同的分類做不同的歸納整理。主要分別以「安全機制使用的方法」、「達成何種安全目的」、「適用場景」及「可抵抗何種攻擊」進行不同分類的討論。

安全機制使用的方法

A.基於傳統密碼系統

此種方法主要是利用傳統密碼學技術如：對稱式密碼系統、雜湊函數、亂數產生器等元件，並透過雙方交握的通訊方式達到資料的保密性及雙方身份的認證性。[10]中利用共同擁用的秘密資訊(對稱金鑰)來達到雙方認證並利用雜湊函數來保護此秘密資訊的安全。另外加入亂數產生器來避免Tag固定發出相同回應值的問題，可保護位置隱私的問題。在[1][5][6]中則是採用某方送出亂數產生器產生值，另一方接收到後經過其它運算或密碼元件如：AES等加密元件經加密後再回傳，利用雙方相交握的方式來達到彼此的認證。在[8]提到利用雜湊函數鏈的機制來保護Tag的隱私，Tag利用此機制可以產生不同且無法預測的輸出值，進而可達到攻擊者無法追蹤及破解真正存於Tag中的資訊。此外此篇論文也引入Forward Security的觀念，即就算今天用來保護訊息隱私的方法被破解，也不會影響之前被保護的訊息。因此這個機制可防範攻擊者以監聽、收集Tag輸出甚至是得到Tag目前所儲存的資訊等方式來破解此系統，能有效防止攻擊者追蹤到持有人位置及知道持有物的資訊。

B.基於通訊方式

由於在 RFID 系統中，Reader 一次只能和一個 Tag 進行通訊，如果同時有太多 Tag 產生回應，在 Reader 端則會發生碰撞而造成無法正確的讀取 Tag 資料，因此需有防止 Tag 同時回應時產生碰撞問題的機制。在 900MHz 系統中採用 Tree-Walking 的方式、在 13.56MHz 系統中則採用 ALOHA 的方式來防止碰撞的問題發生。而[3][10]用來解決 Tag 資料隱私的問題是基於在 900MHz 系統中，使用 Tree walking 的方式來防止碰撞進而延伸出的方法。在[10]中當發生通訊碰撞後 Reader 會利用上一個 Bit 的資訊並經 XOR 的運算來隱藏下一個要求的 Bit 資訊，可防範因監聽 Reader 端產生資料隱私的問題。另外[3]則是採用一個 Block Tag 主動產生射頻訊號模擬所有可能的 Tag ID 來模糊其它真正所使用的 Tag ID，進而保護消費者所使用的 RFID Tag 的隱私。[2]為另一套基於[3]概念的方法，能提供更具彈性的隱私策略，適合應用在個人公司倉儲管理，可以提供不同權限的主管進行物品的追蹤標籤。

C.其它

在[9]中提出二種方法來保護 Tag ID 的隱私，分別為讓使用者給定一個私人的 ID 來隱藏真正存於 Tag 中固定 ID 或由使用者來指定 Tag 中部分的 ID 序列。上述兩種方式皆可由使用者來控制 Tag ID 的內容，進而保護 Tag ID 的隱私。另外，目前已有用來保護 RFID Tag 隱私的技術，如 The Kill Tag Approach，即利用 kill 的指令使 Tag 功能完全失效；The Faraday Cage Approach，即利用金屬容器使 RFID Tag 所發出的射頻訊號無法通過；The Active Jamming Approach，即消費者攜帶一裝置可主動廣播出射頻訊號來阻斷未授權 Reader 的讀取，也都是用來防止 Tag 資訊洩漏的方法。

適用場景及需達成何種安全目的

RFID 系統可用於客制化的環境中，根據不同的情境設定做不同的應用。如應用於供應鏈中商品的自動化管理、賣場中商品防竊偵測及自動化管理、門禁卡、塑膠貨幣及個人物品自動化管理等等的運用。不同應用環境中有不同的安全考量，在個人物品自動化管理中我們需考量持有人的物品 ID，不被任意 Reader 讀取到其正確的內容；在防竊/防偽偵測及門禁卡上面則需考量認證方面的問題，即如何判斷此 RFID Tag 為合法而不是仿冒。因此在 RFID 系統有關安全議題方面，最關心的莫過於 Tag ID 隱私以及 Reader 和 Tag 雙方認證等兩大問題。Tag ID 被任意讀取洩漏使用者持用物資訊，甚至是暴露所在位置；認證機制的缺乏或強度不足則會產生偽造、冒用的問題。在[2][3][8][9][10]利用傳統密碼技術、主動產生射頻訊號及由使用者自行建立序列 ID 等方式，來保護 Tag ID 的隱私。在[1][4][5][6]則採用雙方共同擁有的資訊，並利用交握詢答的方式，來各自驗證彼此的身份進而達到

Reader 及 Tag 雙方的認證，來防範偽造、冒用等問題。

可抵抗何種攻擊

在 2.1 小節中提到攻擊的形態主要分為被動及主動二大類，在 RFID 系統中被動式的攻擊通常是以監聽及流量分析為主，利用此種攻擊來得取未受保護的 RFID Tag 資訊或判斷 Tag 持有者的所在位置。一般而言，被動式的攻擊比較難預防，因此需有相關的防範機制來保護 Tag ID 的外洩。在[2][3][4][7][8][9][10]中內容主要是討論如何解決有關 RFID Tag ID 隱私的問題，另一類主動攻擊常見的有惡意的掃描或利用監聽後得到的資料進行 Tag 的偽裝，為了避免類似的問題，需要有雙方認證的機制來減少惡意掃描或偽造的問題，在[1][5][6][10]中討論相關的機制來解決這方面的攻擊行為。

3. 具防偽及隱私性功能之雙邊認證系統設計

目前所提出的有關 RFID 系統安全性的機制，著重於 Tag ID 的隱私及 Reader 和 Tag 雙方的認證。由於 Tag 資料是固定的，對於先監聽再進行資料複製或重送等問題為較難防範的一環，因此我們提出一個簡單且有效的方法，不需要使用密碼元件如雜湊函數或加密元件等，就可解決有關 RFID 系統中 Reader 和 Tag 之間雙方認證的問題。同時避免攻擊者利用監聽後重送資訊進行 RFID Tag 偽造的問題，使用此機制也可以達到某些程度下的 Tag ID 保密的功能，此外由於不需密碼元件因此在製作 RFID Tag 的成本也會相對的降低許多。

3.1 基本設計理念

利用一組由 Reader 和 Tag 共同擁有且唯一的認證序列值，透過相互詢問的方式來判斷雙方的身份是否正確，因此在 Tag 認證 Reader 身份是否合法前，不會將 Tag 中所擁有的資訊洩露出來。因此可阻擋非法 Reader 的讀取或掃描，保護 Tag ID 的隱私性。同時 Reader 也可對 Tag 進行認證，防止 Tag 偽造的問題。圖 2 為雙方進行認證時的簡單動作範例，當擁有相同認證序列值的 Reader 及 Tag 進行認證時，首先 Reader 取得和 Tag 同步後會先送出認證序列某部份的值，提供給 Tag 認證自己的身份。同理，換 Tag 提供另一部份的值，讓 Reader 認證其身份是否正確。透過數次交握後認證彼此，接著才進行正常的讀取 ID 動作。

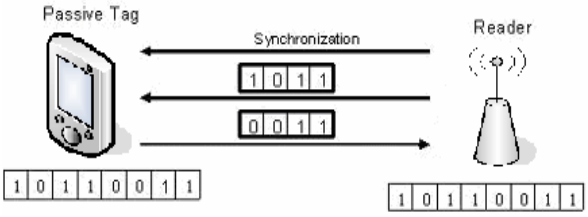

圖 2 基本概念示意圖

3.2 系統設定及假設

為了達到防止所謂的先監聽後重送的問題，我們需每次產生不同的認證序列值，來保護每次的認證。在系統中我們假設RFID Reader及Tag在製造時已設立好一相同秘密金鑰(對稱金鑰)，此外，雙方擁有擬亂數產生器(PRF)來產生不同的亂數值。因此，擬亂數產生器所能產生的亂數值愈亂，此系統的安全性就更高。另外，在Tag中需預先配置好一塊空的記憶體來儲存所運算後的亂數值，並有一指標記錄目前亂數值的位置。由於我們需對認證序列做保護，因此系統中設計由Tag發出隨機一個亂數及雙方所擁有的秘密金鑰做為擬亂數產生器的種子，產生一亂數值來保護認證序值。同理，Tag發出所發出的亂數與秘密金鑰的長度將會影響產生出來亂數。由於每次產生的認證序列及詢問的認證位置都不一樣，因此系統可達到One-Time Pad的安全強度。

3.3 系統流程說明

當 Reader 和 Tag 取得同步通訊後進入認證的程序。在每次認證時 Reader 皆會產生不同的認證序列值，並透過由 Tag 所傳送過來的隨機值和與 Tag 共同分享的秘密金鑰做為種子產生另一組亂數，目的是用來保護認證序值不被攻擊者以監聽的方式取得。同理，Tag 接到此序列值用同樣的方式將此受保護的值解開並得到此次通訊所需的認證序列值，接下來進入雙方認證的階段，Reader 和 Tag 彼此會利用以隨機的方式尋問認證序列值任一位置與其數個對應值的方式，來判斷雙方的身份是否正確，當某方回應為不正確時另一方則結束此次的通訊，並判斷此通訊為非法的行為。圖 3 為系統進入認證階段時的動作流程圖。當雙方認證完畢且判斷互為合法的使用者後，Tag 則開始送出所擁有的資訊給 Reader。

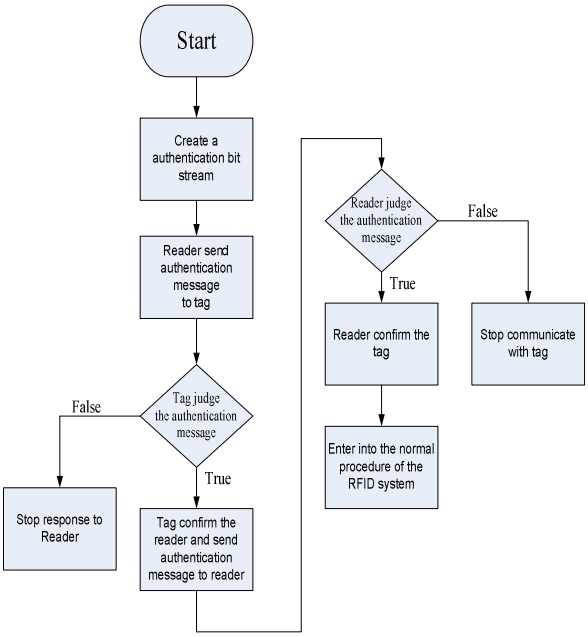

圖 3 認證階段流程圖

我們以圖 4 的例子來說明所提出的認證機制。另外，在認證序列的長度和認證所需回應的位元個數，都是可以依照管理者所需進行不同的設定。下面為進行認證時所需的步驟：

(1).在同步程序後，Tag 先選一亂數 x 並送給 Reader；(2).Reader 利用事先分派的秘密金鑰 Key 及 x 做為 PRF 的輸入產生一亂數值，並與認證序列值 r (Reader 隨機產生)進行 XOR，再傳送給 Tag；(3).在收到 $r \oplus f(Key, x)$後，Tag 利用秘密金鑰 Key 與之前所選之 x 解出認證序列值 r；(4).Reader 送出一個隨機選取位置，與其對應部份認證序列值給 Tag，預設格式如圖 5 ，提供 Tag 進行對此 Reader 的認證；(5).當 Tag 對此 Reader 認證成功後，再回應另一組不同部份的序列值給 Reader 進行認證。

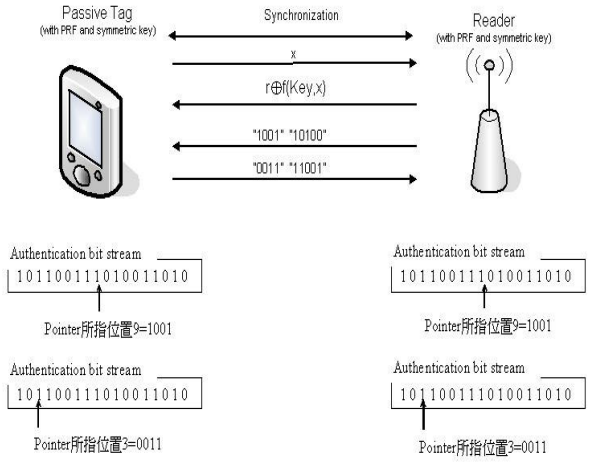

圖 4 實際認證動作範例

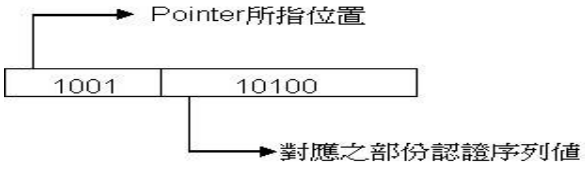

圖 5 認證資料格式

4. 系統分析

此系統中 Reader 每次通訊皆產生不同的認證序列值及 Tag/Reader 會指定不同的序列值位置，因此攻擊者無法以重送攻擊來假冒合法的 Tag。另外，我們所提出的機制除了可以做到一般 Reader 和 Tag 身分認證外、也可以避免非法的 Reader 利用惡意掃描的方式來分析 Tag 持有者的所在位置或進行資料收集的動作，以達保護 Tag 隱私的問題。當雙方認證完成後 Tag 才送出 ID，因此我們所提出的機制也具有防範因攻擊者主動掃描 Tag 而洩露隱私的能力。此外我們也設計了幾個相較於 2.2 節所提到的目前有關於 RFID 系統安全機制更為嚴苛的攻擊方式，也證明了我們所提出的方法在 Tag 或 Reader 身份偽造這部分有相當的防禦能力。在攻擊場景一、二中我們假設攻擊者可以利用監聽合法的 Reader 和 Tag 彼此通訊，或假冒 Reader 或 Tag 的身份等不同方式，來對我們所提出的機制進行安全強度的分析。

A.攻擊場景一

在我們的協定中，我們假設預先存在於 Reader 及各個 Tag 上的秘密金鑰都不會因為外來的物理攻擊而曝露，這個也就是我們將秘密金鑰存在一個不會被破壞竊取(Tamper-Resistant)的硬體裝置中。如此一來，我們的協定的安全性就全基於通訊時候所洩露的訊息了。在攻擊場景一裡，我們一開始先假設如同[10]的環境一樣，監聽者因距離的原故無法得知由 Tag 回傳給 Reader 的任何訊息。監聽者此時只能獲得 $r \oplus f(Key, x)$值，在無法得知其它訊息之下，唯一能知道祕密金鑰的方法只有去猜 r、x 以及 Key 的值來比較所得知的 $r \oplus f(Key, x)$，藉此找出正確的 Key 值。但是我們的協定中，假設 r 為 80 bits，Tag 隨機所產生的 x 也是 80bits，另外，Key 也是 80 bits，所以要猜對 Key 所需要的運算為 $2^{80}*2^{80}*2^{80}$，以目前每秒可處理 2^{30} 次的處理器(CPU 1GHz)來說，破解祕密金鑰所需要的時間約為 $2^{240-30}=2^{210}$ 秒，已可達到密碼學上的理論安全。如果我們假設監聽者不只可以監聽到 Forward Channel(Reader 到 Tag)，而且連 Backward Channel(Tag 到 Reader)都可以進行資料收集的話，攻擊者將多獲得另一個由 Tag 隨機產生的數值 x。不過，雖然如此，攻擊者還是得嘗試至多 2^{160} 次，需要約 2^{130} 秒。這樣的結果也是可達到密碼學上的理論安全。

B.攻擊場景二

在這個攻擊場景中，我們假設攻擊者為惡意的 Tag 且試圖欺騙 Reader，意圖為獲得認證用的字串 r 並進一步求得金鑰 Key。首先攻擊者可以選擇三個隨機數值 x_1、x_2、x_3，並依序送給 Reader，一般來說，Reader 會回應此惡意 Tag $r_1 \oplus f(Key, x_1)$、$r_2 \oplus f(Key, x_2)$、$r_3 \oplus f(Key, x_3)$等值。經過簡單運算，如果 $x_1=x_2=x_3$，攻擊者可以獲得以下互斥或的值：$r_1 \oplus r_2$、$r_1 \oplus r_3$、 $r_2 \oplus r_3$。此時攻擊者(惡意 Tag)無法利用這些故意設計的資訊來解出秘密金鑰及認證序列值 r，因此沒辦法得知下次 Reader 所選的認證字串 r_{i+1}，也就是攻擊者除了直接去猜金鑰之外，沒有其它的辦法。

由上述所設計的場景及系統動作流程可知，此認證機制除了可能利用硬體上的技術破壞、破解系統外，無法以一般攻擊行為來破解此系統。但是以實體特性與所需要的技術、成本來看，攻擊者首先需有對 RFID Tag 硬體的設備、技術等相關知識，因此造成攻擊者入侵難度的增加。同樣地，當成本允許下可以在系統中加入 Tamper-Resistant 的硬體設備，如此可避免系統遭遇硬體上的攻擊。

5. 結論與未來展望

在這篇文章中，我們主要的目地是達到目前所提出的 RFID 系統安全性機制所達不到有關於先監聽再進行資料複製或重送的安全問題，當 RFID 系統用於商品、鈔票的防偽、門禁卡等應用時需有雙方認證機制來辨別彼此的身份，因此我們提出一個簡單且有效的方法，在不需要使用密碼元件如雜湊函數或加密元件等，就可解決有關 RFID 系統中 Reader 和 Tag 之間雙方認證的問題，此機制除了可達有效的雙方認證、及不易因各種攻擊方式達到所謂假冒的安全訴求外，同時也因沒有使用密碼元件而使得降低 RFID 系統的建置成本。由於設備的問題下，我們無法以實際的設備來進行測試，因此在未來的工作中我們希望能有較多的設備，並將我們所提出的安全機制實際佈署於 RFID 系統中，並進行實際的測試，並討論實際下會出現何種相關的問題。

參考文獻

[1] Ari Juels, “Yoking-Proofs' for RFID Tags,” Proceedings of the Second IEEE Annual Conference on Pervasive Computing and Communications Workshops (PERCOMW’04) 2004

[2] Ari Juels and John Brainard, “Soft Blocking：Flexible Blocker Tags on the Cheap,” WPES 2004.

[3] A. Juels, R.L. Rivest, and M. Szydlo. “The blocker tag: Selective blocking of RFID tags for consumer privacy,” In V. Atluri, editor, 8th ACM Conference on Computer and Communications Security, pages 103--111. ACM Press, 2003.

[4] Ari Juels, Ravikanth Pappu RSA LAB. ”Privacy Protection in RFID-enabled banknotes,” Financial Cryptography '03, pages 103-121. Springer-Verlag. 2003. LNCS no. 2742.

[5] David Molnar and David Wagner, “Privacy and Security in Library RFID Issues, Practices and Architectures,” June 8, 2004 http://www.cs.berkeley.edu/~dmolnar/library.pdf

[6] Feldhofer M., “An Authentication Protocol in a Security Layer for RFID Smart Tags,” Proceedings of the IEEE MELECON Conference 2004 (MELECON 2004, May 12-15, 2004, Dubrovnik, Croatia), Vol. II, pp. 759–762

[7] Gildas Avoine, “Privacy Issues in RFID Banknote Protection Schemes,” International Conference on Smart Card Research and Advanced Applications - CARDIS, Toulouse, 22-27 Aug 2004

[8] Miyako Ohkubo, Koutarou Suzuki, and Shingo Kinoshita. “Cryptographic approach to a privacy friendly tag,” In RFID Privacy Workshop, MIT, 2003.

[9] Sozo Inoue and Hiroto Yasuura. “RFID privacy using user-controllable uniqueness,” In RFID Privacy Workshop, MIT, Massachusetts, USA, November 2003. 12

[10] Weis, S. A., Sarma, E. S., Rivest, R. L., and Engels, D. W., “Security and Privacy Aspects of Low-Cost Radio Frequency Identification Systems,” Security in Pervasive Computing, 2003.