共享經濟的 RFID 群組驗證架構及機制

奚正德*
文化大學資訊管理學系
xzd@ulive.pccu.edu.tw

摘要

行動科技發展，使得共享經濟的新型商業模式，不斷推陳出新，至今 17 家市值超過十億美元的新創共享企業產生，估計 2025 年全球共享經濟市場價值將超過 3 千億美元。廠商紛紛建置共享平台，享受共享經濟帶來的商機，但是面臨分享資訊的隱私洩漏等資訊安全問題，使發展遇到阻礙。而行動科技中 RFID 的技術成熟，應用於共享經濟，尤其是群組物件，具有多個標籤集合式特性的物品，可充分發揮共享特性的經濟效能。學者 Zhuang et al. 提出 RFID 群組驗證協定，宣稱可應用於共享經濟，並具有保護隱私的功能。在設計的協定中，我們發現兩項問題 (1) 沒有應用情境及架構說明 (2) 虛擬識別碼及群組驗證的效能不足。本文針對上述問題，提出簡易的共享經濟 RFID 群組驗證架構及步驟，並搭配多人露營的共享經濟應用說明，及找出 Zhuang et al. 效能不足原因，在於產生群組驗證及虛擬的標籤識別碼時，使用了訊息遞延及竭盡搜尋的方式，並據此提出改善的方向。

關鍵詞：共享經濟、RFID、群組驗證

RFID grouping-proof architecture and scheme for the sharing economy

Abstract

The mobile technology development has made the new business model of sharing economy advancing all the time. So far, 17 new establish sharing companies with over 10 billion US dollars of market capitalization have arisen. Experts estimate that the value of global sharing economic market will be over 300 billion US dollars during 2025. To enjoy the business opportunity that brings out by sharing economy, a growing number of companies set up the sharing platform. However, when facing the information security problem of leaking privacy, the development has been blocked. Among the mobile technology, the technique of RFID is mature and can apply in sharing economic, especially grouping objects. Multiple tags simultaneously exist in the group. Then sharing characters will create economy efficiency.

*通訊作者 (Corresponding author.): 奚正德, xzd@ulive.pccu.edu.tw

Zhuang et al. presents RFID grouping-proof protocol and declares to apply sharing economy without leaking privacy. In designed protocol, we find out two problems (1) with no application scenario and architecture (2) pseudo identities and grouping-proof with lower system efficiency. In this paper, we propose simplified RFID grouping-proof architecture and multiple camping sample for the sharing economy. For Zhuang et al. protocol, lower efficiency is due to relay one by one for tags and exhaustive search when generating grouping-proof and pseudo identities. Finally, we indicate improvement policy.

Keywords: Sharing economy、RFID、Grouping-proof

壹、前言

首全球化與網路環境日趨成熟，行動裝置發展迅速，造就許多創新商業模式，其中「共享經濟」 (Sharing economy)成長迅速，共乘概念的 Uber，以提供網路運輸服務，創造市值達 412 億美元，短期租屋住宿 Airbnb，也以網路媒合，達成市值 100 億美元，皆是新創共享經濟企業 [1]。2014 Hong et al. [8], 網際網路基本提供了資訊交換的平台功能，加上愈來愈多人體認到「擁有資源」必須付出的代價，遠比「共享資源」高出許多，以致共享經濟開始活絡，近年來甚至呈現指數般的成長，並擴散應用至各領域中。未來共享經濟將創造更多新型態的就業機會與商機，同時孕育許多中小企業與新創事業以共享經濟之商業模式提供創新服務。2015 康廷嶽和黃柏偉學者指出 [17], 網路中介平台顛覆傳統企業經營概念，擁有物品與服務的個人，透過網路中介平台「分享」各種商品或服務，因而使得每個人都可在閒暇之餘提供服務，像打工族一般，亦可將物品出租或再出售給其他人使用，使物品能更有效被運用。也因共享經濟的創新商業模式，使得每個人輕易的加入共享體系。

RFID 電子標籤具有成本低、體積小、容量大、壽命長、可重複使用等特點，目前 RFID 技術已被廣泛應用於工業自動化、商業自動化、交通運輸控制管理等眾多領域，RFID 擁有能在許可的範圍內，一次讀取大量的標籤資訊的特點，明顯的提升物品的管理，也克服了很多傳統條碼的限制與無法滿足的地方。RFID 技術時的關鍵問題之一，就是要保證只有授權使用者，才能夠識別特定標籤，而攻擊者無法對這些標籤進行跟蹤．由於 RFID 標籤的資源受限，要設計安全、高效的 RFID 安全機制，至今仍是一個具有挑戰性的課題。信用卡內建 RFID 可大幅提升工商交易安全與便利，但消費者質疑個人隱私可能受到侵犯，另外商店內用 RFID 標籤，取代現在廣泛使用的條碼標籤。這樣，從商品入庫開始，直到顧客付錢的整個過程中，商家都能夠跟蹤商品的行蹤。同樣隱私被揭露的場景，也極可能發生在共享經濟上。RFID 的安全性備受爭議，故隱私與安全已經成為 RFID 技術發展的重點。但如何在公眾中建立對該項技術的理解和信任

感，並讓消費者確信資料和交易是可靠的，已是無法迴避的問題。

RFID 群組驗證技術的發展快速，已被導入各種應用。2004 年，Juels 提出「共軛驗證」 (Yoking proof) 產生機制以驗證兩個 RFID 標籤 (Tag) 同時存在[11]。2006 年，Bolotnny and Robins [2] 將 Juels 共軛驗證擴展使用，用以證明任意數量的標籤同時存在於一個 RFID 讀寫器 (Reader) 電波有效涵蓋範圍內的情境，此驗證機制一般稱為「群組驗證」 (Grouping proof)。2008 Huang etc al. 設計方案[10]，其 RFID 標籤規格採用 EPCglobal Class-1 Generation-2 標準[7]，因為被動式標籤的計算能力有限，通訊協定中僅使用虛擬亂數產生器、循環冗餘碼等基本運算，並利用群組驗證(Grouping proof) 快速驗證藥盒內的藥品是否齊全正確，搭配住院病人的手環進行身分辨識，以確保病人用對藥品。2016 Zhuang etc al. 提出具保護隱私的 RFID 群組驗證機制 [16]，宣稱可推廣至共享經濟。而群組物件具有多標籤群聚的特性，對共享經濟而言，可提升分享效益，但目前的探討與應用仍十分有限，在 Zhuang etc al. 一文中，尚未將其設計機制結合實際的應用。

本文導入 RFID 群組驗證技術，並應用在共享經濟上。設計簡易的共享經濟 RFID 群組驗證架構與步驟，如圖二，並羅列多個標籤集合式特性的群組物品，以結合實際應用情境。另探討 Zhuang etc al. 提出的 RFID 群組驗證機制，在保護隱私採用虛擬識別碼與建構群組驗證時，造成系統效能的問題，並提出建議。本文分成五個章節進行說明，第二節共享經濟的資安問題與應用情境，第三節簡易的共享經濟 RFID 群組驗證架構與操作步驟，第四節 共享經濟的 RFID 群組驗證機制及系統效能分析與建議，最後結論。

貳、共享經濟的資安問題與應用情境

共享經濟是相對新穎的概念，經由網路，任何資源都能出租，透過科技的力量將閒置資源釋出，不論是技能、空間或是物質資產，任何被認為有其價值之資產皆可進行交易。消費者可透過協同消費，將其固有資產用於賺錢或儲蓄之途，成為個別的微型創業者 [3]。早在 1978 年 Marcus 與 Joe 提出協作消費的概念 [15]，2010 年時 Botsman 和 Rogers 強調全球市場將由過度消費經濟轉變為共享經濟 [3]。2013 年 3 月經濟學人(The Economist) 以「崛起中的共享經濟」為標題 [6]，在網際網路任何事物都可租借，如圖一，但也因網際網路屬於公眾環境，個人資料容易洩漏，物品交付也易產生糾紛等問題。另外共享經濟的精神，除了以租代買外，就是以量制價，愈多人分享，使用費用就愈低廉，例如：多人共同租用車輛、場地等。而物品的租用，是整組套件比單件便宜，這也就是物品群組式的概念。

2.1 資安問題

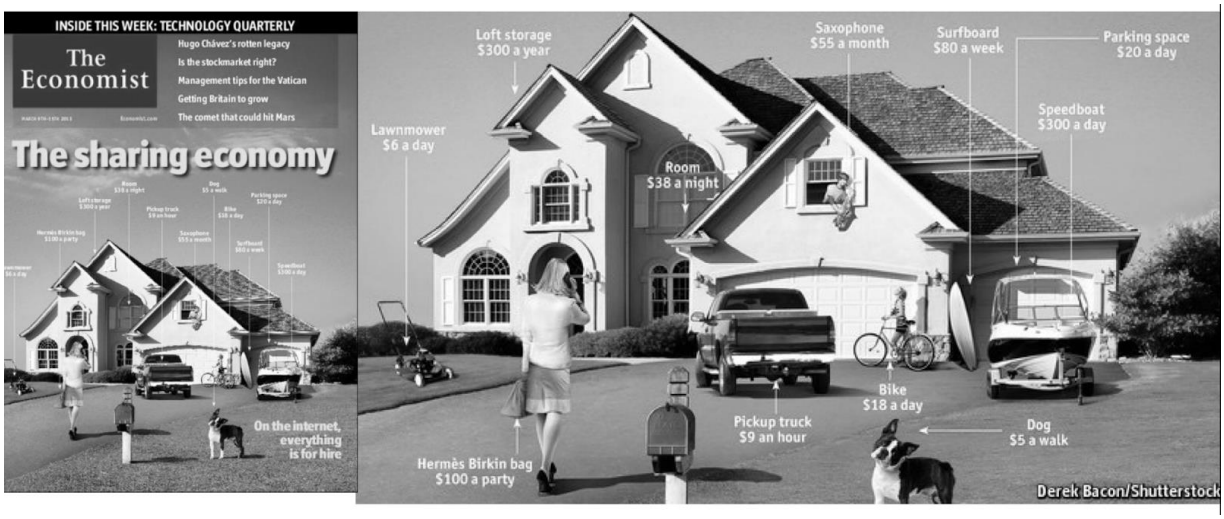
以使用權替代擁有權的共享經濟觀念日漸蓬勃，一個安全可信賴的作業平台，是共

享經濟發展上不可或缺的要素，但是只有少數的大型平臺會透過信任及安全相關機制、措施及程序來降低風險（如：身份驗證、聲譽機制、交易安全機制等）。多數的小型網站因資源不足，難以提供完整的功能，只能靠物品所有者與租用者的自我營銷，期望交易雙方能行約束管制。因此價格相對低廉的前端設備，必須格外重視資訊安全。而 RFID 因技術成熟，被廣泛應用在經濟共享上。但 RFID 讀寫器與標籤之間傳輸，是透過不安全的通道。連帶的隱私洩漏、未經授權的追蹤等資安問題，使人們心存疑慮，而影響了經濟共享的發展。所以雙向認證時，為保護交易雙方的隱私，標籤識別碼的虛擬化或匿名化，成為常見的作法，但也造成讀寫器或後端系統，搜尋真實識別碼的效能問題。另外本文提及的群組式物件，在系統效能上，亦有建構群組證驗的延遲問題。

2.2 應用情境

共享經濟的租借物品中，常見套件式的物品，也就是效益最佳的代表性物件。例如：工具箱，就是由多項工具組合而成，當租借者要完整借用時，交接時，所有者必須證明，箱子內的所有物品，都同時存在於箱子內。另外財團法人車輛研究測試中心（ARTC）指出[18]，「汽車共享 Car-sharing」，乃指一群人共用一輛車或多輛車，使用者擁有使用權，無所有權，符合環保概念，如法國的 Autolib'、德國的 Car2Go 與 Ford2Go 以及美國的 ZipCar，皆擁有大量的使用者與成熟的營運模式，在第三節中，我們將說明一個實際的露營案例，另外將物品依據特性，簡單的歸類如下。

1. 多件物品同時存在，常見於各種組合包，性質雷同，而功能互補的物品。
   (1) 工具箱：螺絲起子、老虎鉗、扳手等。
   (2) 急救箱：紅藥水、OK 蹦、棉花棒等。
   (3) 汽車美容工具箱、整套禮服等。
2. 一件物品是由許多零件組合而成，搬移時，可能須要重新組裝與拆卸的物品。
   (1) 露營帳篷：帳篷帆布、防潮地布、營釘、附屬配件等。
   (2) 各種 DIY 組裝家具：衣櫃、桌子、椅子等。
   (3) 桌上型電腦：滑鼠、螢幕、主機等。
   (4) 拼圖玩具：平面拼圖的零片有 300 件、500 件、750 件、1,000 件等不同的規格。
3. 一件物件提供一個以上的使用者，例如：會議場地、汽車。



圖一：崛起中的共享經濟 [6]

參、簡易的共享經濟 RFID 群組驗證架構與操作步驟

共享經濟以租借代替購買的觀念，是轉移「使用權」不同於「所有權」的轉移。轉移過程，不應該洩漏雙方的隱私，但在共享經濟中，交易經平台成功媒合的關鍵，在於供需雙方的互信。RFID 技術除了建構可信賴的後端平台，前端的標籤與中繼的讀寫器，屬於不安全的無線通訊，必須確保安全及隱私。一般 RFID 的安全需求，包含：授權訪問, 標籤的認證, 前向不可追蹤性, 標籤匿名性, 可信賴平臺 (可問責), 不可連結性(強不可連結性是指攻擊者在任何時刻都不能判定兩個回應是否對應於同一個標籤, 弱不可連結性是指攻擊者無法把標籤被讀寫器成功處理前後發出的回應連結在一起。

本文建構一個簡易的共享經濟 RFID 群組驗證架構及流程，如圖二，亦著重於使用權的釋出，而非所有權的轉移，並適度說明群組驗證架構安全設計的作業要點。在圖二中，每件物品貼附一個標籤，貼附標籤的多件物品可視為同一群的組合，群組內的成員，幾乎同時間內存在，亦即所有標籤與讀寫器完成通聯與驗證，以取得所有的標籤的個別驗證，若驗證組合，經過驗證成功，就可確認通過群組驗證。

在圖二中，是一個經濟共享的露營案例，使用者號召志同道合者，參加露營活動，所需物品急救箱、帳篷與露營車，三項物品屬於群組式物品，並提供給所有參加露營活動的使用者，在租借驗收時，均須完成群組驗證，亦即操作步驟 7 及 8，確認各個標籤均同時存在，在使用者歸還時，所有者亦可加入相同程序，以確認使用者所歸還的物品沒有短缺。

3.1 符號說明

O 所有者、U 使用者、R 讀寫器、T 標籤、S 服務平台

3.2 作業要點

1. 所有者與使用者有各自的讀寫器 R1 和 R2，可透過網路連結後端可信賴平台及互相連結，因為讀寫器運算能力遠較前端標籤強，可選用運算量大，較安全的加解密機制。
2. 標籤與讀寫器間的傳輸，屬於不安全的通道，攻擊者的威脅模式，包含竊聽、未授權追蹤、偽造標籤、遺失標籤、大量無效回應等方式。而標籤屬於輕型計算量的設備，可考慮採用”赫序函數” Hash function 結合”互斥或” XOR 等輕型運算量的函數，進行識別碼匿名、虛擬化及驗證碼產生，達成相互鑑別 (Mutual authentication) 及保護隱私的目的。
3. 授權權杖 (Authorized token)是由服務平台，依據媒合雙方的供需建構完成，一般包含雙方的虛擬或匿名識別碼及物品資訊，(例如：3.3 的 1. 服務物品 (1)-(4))，可經由雙方的通訊金鑰保護，進行如：赫序函數等輕量級的運算，達成雙向鑑別的機制，防止偽造等攻擊，其他步驟，亦可採取類似運算，達成安全傳輸的需求。

3.3 操作步驟

1. 服務物品：R1→S
   所有者以讀寫器查詢持有物品的標籤，將物品資訊上傳服務平台，服務平台儲存及整理物品資訊，(1) 所有者識別碼匿名化 (2) 物品名稱、地點及規格 (3)分享時間及限制 (4) 物品狀態及補充說明。
2. 要求服務：R2→S
   使用者上傳分享物品的需求。
3. 授權權杖：S→R1 & R2
   服務平台依據供需，進行分享物品媒合，產生授權權杖，分別傳送使用者及所有者雙方的讀寫器。
4. 授權權杖：R2→R1
   使用者傳送授權權杖至所有者的讀寫器，並檢查權杖正確性。
5. 存取權限：R1→R2 & T
   所有者設定使用者的存取權限，並回傳給使用者的讀寫器及分享物品的標籤，及變更標籤的存取權限。
6. 交付：O→U
   所有者將分享物品傳遞給使用者。
7. 查詢：R2→T
   使用者以讀寫器收到的存取權限，查詢分享物品標籤資訊。
8. 建構群組驗證：T→R2

各群組標籤依序回應，在不洩漏隱私的狀態，建構群組驗證，使用者讀寫器可據此驗證群組內物件，是否有缺漏或偽造等情事。

9. 通知：R2→R1

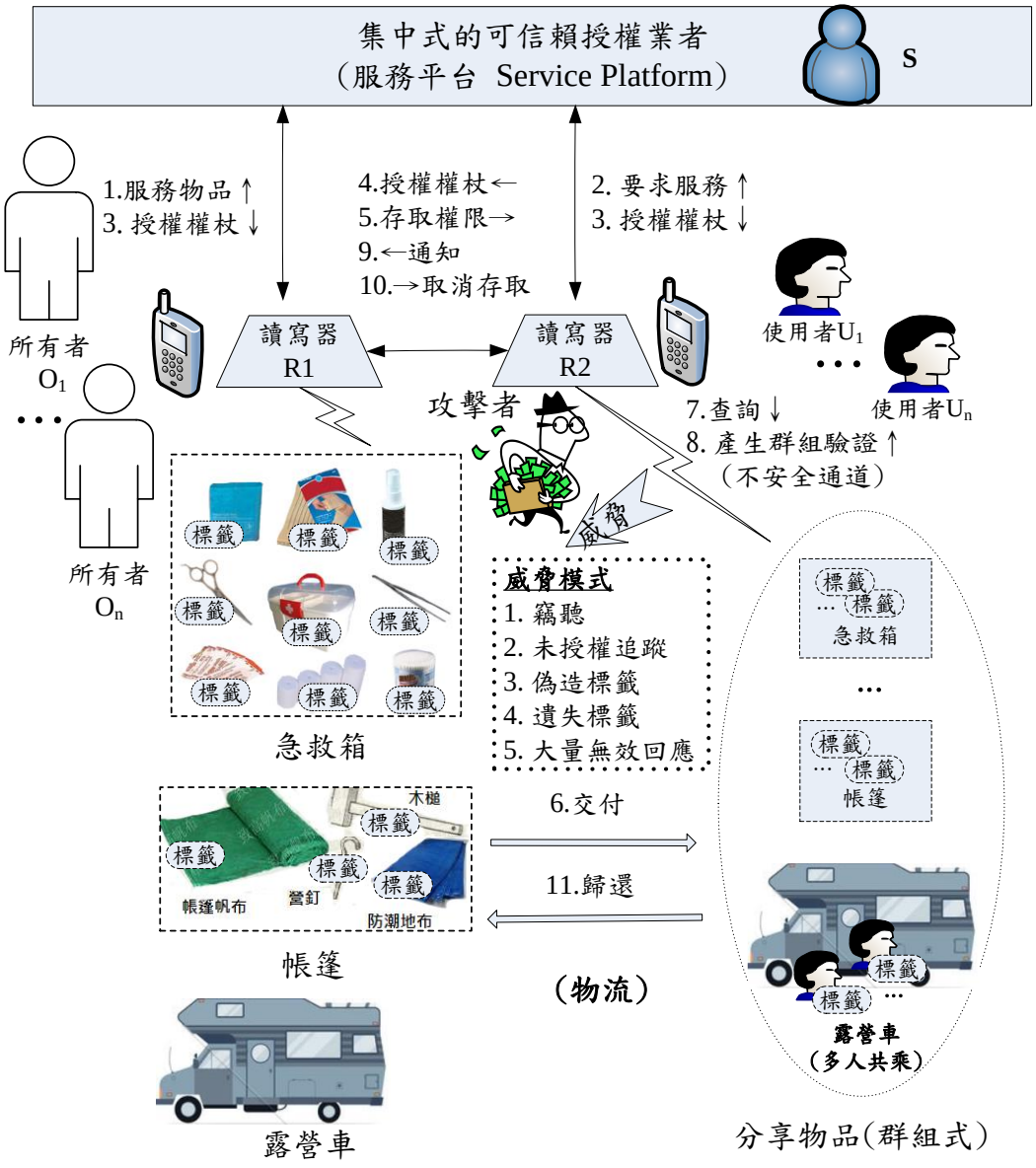
通知所有者的讀寫器，歸還分享物品。

10. 取消存取：R1→R2 & T

所有者的讀寫器取消標籤內使用者的存取權限，並通知使用者。

11.歸還：U→O

使用者歸還分享物品給所有者。



圖二：簡易的共享經濟 RFID 群組驗證架構及流程

肆、共享經濟的 RFID 群組驗證協定及系統效能分析與建議

高安全性的群組驗證，攻擊者將無法偽造一個或更多的標籤，在稍後的時間，產生可通過檢驗的證明。若以共軛驗證的概念來建構群組驗證時 [14, 4, 5, 12]，某一個標籤必須等待收到特定的標籤響應，然後才能繼續執行群組驗證。為保護標籤貼附物品的所有者隱私，避免攻擊者獲取真實的標籤識別碼，匿名或虛擬化識別碼，常被使用，但是 2010 年，Lo and Yeh [13, p.1220] 設計的虛擬化的識別碼機制，存在讀寫器端的真實標籤識別碼，竭盡搜尋的問題 (Exhaustive search)。 2015 Hsi etc al. 提出解決可擴展性的問題的群組驗證協定 [9]，含四項問題 (1) 訊息中繼/遞延 (Message relay/delay) (2) 輕量標籤計算 (3) 識別碼匿名與虛擬 (4) 標籤回應碰撞等。造成問題的原因不外乎是 (1) 群組驗證與讀取標籤的順序有關，(2) 後端依據接收的匿名或虛擬識別碼，必須竭盡搜尋真實識別碼，這均會使驗證的效率降低，驗證的失敗率也會隨之提高。因此當群組驗證的建構，與標籤順序無關時，先由讀寫器廣播訊息，再依據初始階段設定好的標籤回應順序，由標籤按順序逐一回應，可避免碰撞問題，而讀寫器傳送匿名或虛擬識別碼前，建立與真實識別碼對應的索引，當收到標籤回應的匿名或虛擬識別碼，即可快速的採用索引搜尋，避免效能低下的竭盡搜尋。2016 Zhuang etc al. 指出 [16]，行動通訊技術帶動分享經濟，配合安全與隱私的保護，就等於未來經濟繁榮的可靠技術。作者提出一個群組驗證協定，虛擬化真實的標籤識別碼，符合共享經濟的行動通訊特性，可達成隱藏標籤隱私及不可追蹤性的目標。本節分成二部分說明：4.1 Zhuang et al. RFID 群組驗證協定，4.2 系統效能分析與建議。

4.1 Zhuang et al. RFID 群組驗證協定 [16]

群組驗證指的是任意數量的標籤同時存在於一個 RFID 讀寫器 (Reader) 電波有效涵蓋範圍內的情境。作者強調此機制，符合共享經濟的需求，保護隱私及避免多項攻擊，並符合資訊安全的標準，另有關符號說明、假設條件、協定演算法、效能問題及建議，說明如後：

1. 符號說明
   (1) ID_j：標籤 Tag T_j 的真實識別碼。
   (2) K_j：標籤 Tag T_j 的私密金鑰，若經讀寫器 Reader R 鑑別成功後，進行更新。
   (3) K_{j1}, K_{j2}：讀寫器內儲存，標籤 Tag T_j 的舊(K_{j1})和新(K_{j2})金鑰。
   (4) N_j,：標籤 Tag T_j 的計數器,初始值設為 0。
   (5) b_{j-1}：標籤 Tag T_j 產生的 MAC 值，被當作標籤的部分證明 (partial proof)。
   (6) c/r_j：讀寫器產生長度為 l 的隨機數。
   (7) MAC(·)：金鑰的訊息確認碼以標籤私密金鑰 K_j。

(8) F(·)/G(·)：虛擬亂數函數 PRF (pseudo-random function)。

(9) $P_{1,\ldots,m}$：標籤 Tag 1 至 Tag m 的群組驗證。

(10) 符號說明 1-7, j=1…m。

2. 假設條件

(1) 讀寫器 Reader R 結合後端伺服器，和標籤 Tag 1, Tag 2, …, Tag m 的集合每個 Tag j 儲存動態私密金鑰 K_j，並與讀寫器共享。

(2) 讀寫器儲存標籤識別碼 ID_j 和兩個私密金鑰 (K_{j1}, K_{j2})，以避免非同步攻擊。其中 K_{j1} 是舊的私密金鑰，被使用於前一次通訊。而且在初始階段，K_{j2} 是現有的私密金鑰，初始值設定為 K_j。

3. 協定演算法

如圖三所示，每個標籤與讀寫器間，通訊與計算共有四個步驟，群組從標籤 T1 到標籤 Tm，逐一產生各個標籤驗證碼 b_j，讀寫器同時也是驗證者，組合所有的驗證碼及標籤真實識別碼，即是群組驗證碼。

(1) R→T_j (j=1, c; j=2…m, b_{j-1})

標籤 1 執行時，讀寫器產生長度 l 的隨機數 c

其他標籤執行時，讀寫器遞延前一個標籤 T_{j-1} 的 MAC 值，亦即驗證碼 b_{j-1}。

(2) T_j→R (N_j, d_j)

計數器 $N_j=N_j+1$。

標籤識別碼 ID_j 透過虛擬亂數函數 F(·)，產生動態虛擬識別碼 $d_j=F(ID_j, K_j, N_j, b_{j-1})^l$，在不安全的無線傳輸環境下，傳送至讀寫器時，可避免標籤的真實識別碼 ID_j 被竊聽，從而洩漏其隱私。

(3) R→T_j (r_j, V_j)

$r_j \in_R \{0, 1\}^l$

If find (ID_j, K_{j1}, N_j, b_{j-1}) and — 註[1]：標籤 Tag T_1, c 取代 b_{j-1}

F(ID_j, K_{j1}, N_j, b_{j-1})^l = d_j then — 註[2]：竭盡搜尋 (ID_j, K_{j1})

V_j=G(K_{j1}, d_j, r_j)^l — 註[3]：計算讀寫器驗證碼 V_j

Else if find (ID_j, K_{j2}, N_j, b_{j-1}) and — 註[4]：私密金鑰未更新

F(ID_j, K_{j2}, N_j, b_{j-1})^l = d_j then — 註[5]：竭盡搜尋 (ID_j, K_{j2})

V_j=G(K_{j2}, d_j, r_j)^l — 註[6]：計算讀寫器驗證碼 V_j

$K_{j1}=K_{j2}$ — 註[7]：私密金鑰更新

K_{j2}=G(K_{j2}, d_j, r_j, V_j)^l — 註[8]：產生新的私密金鑰

Else

$V_j \in_R \{0, 1\}^l$ and Reject

(4) T_j→R (b_j)

If G(K_j, d_j, r_j)^l=V_j then — 註[9]：驗證讀寫器驗證碼 V_j

K_j=G(K_j, d_j, r_j, V_j)^l — 註[10]：金鑰更新

b_j =MAC(ID_j, K_j, b_{j-1})　　註[11]：產生個別標籤驗證碼

Else

Reject

(5) R (Verifier)

當所有的標籤從 Tag 1 到 Tag m，逐一通過驗證，讀寫器收集到每個標籤 T j 的 (ID_j, b_j)，亦即(真實識別碼，個別標籤驗證碼)，彙總後可得群組的驗證碼，擁有群組驗證碼，即證明同時間內，群組成員都存在。

$P_{1,\ldots,m}$=(ID_1, $\cdots ID_j$, b_1, $\cdots b_j$)

4.2 系統效能分析與建議

Hsi et al. [9] 指出 RFID 群組驗證協定常見的效能問題，並提出解決機制，其中的兩項問題 (1) 訊息遞延 (2) 竭盡搜尋，我們發現 Zhuang et al. [16] 也存在相同問題，造成效能不足，將會延遲到交易，甚或造成超過時間的交易失敗。

1. 訊息遞延(Message Relay)

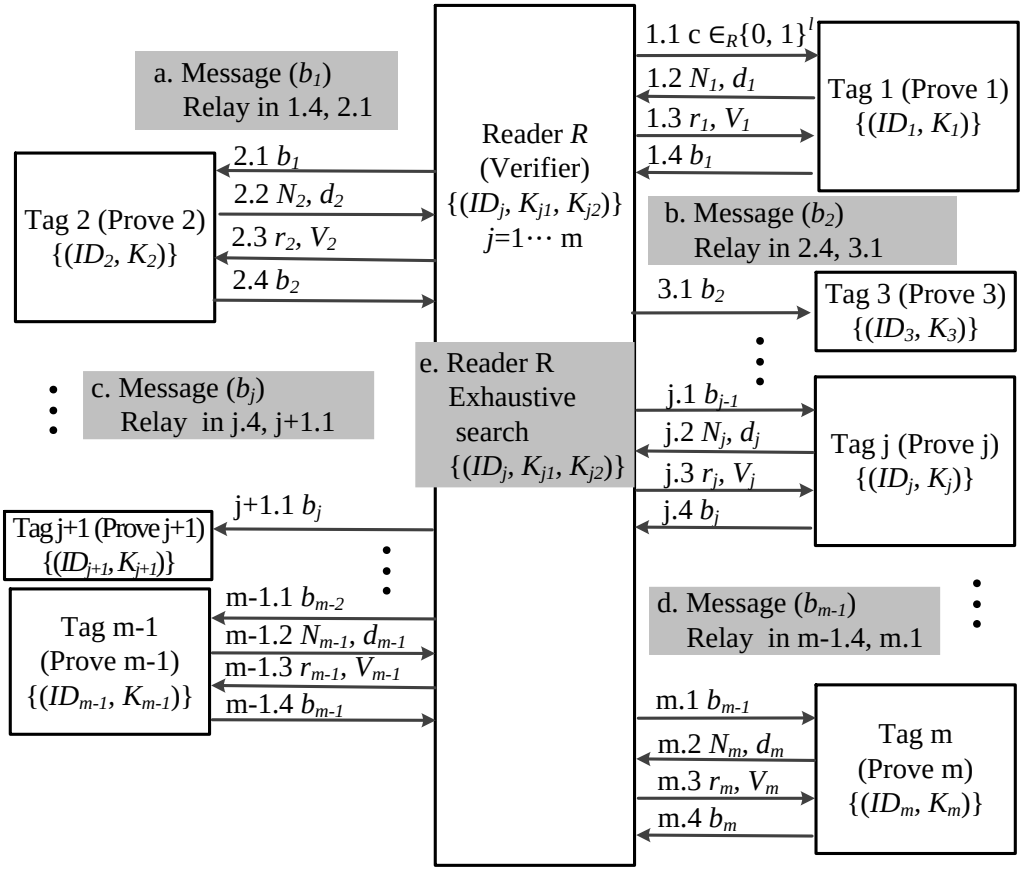
   標籤 Tag j (j=1…m)，於步驟 j.4 將產生的 b_j 回傳讀寫器，讀寫器在下一步 j+1.1 將收到 b_j 的遞延傳送給標籤 Tag j，如圖三 c，另外圖三 a, b, d 也屬於訊息遞延。

2. 竭盡搜尋(Exhaustive Search)

   標籤 Tag T j (j=1…m)，於步驟 j.3 讀寫器竭盡搜尋內部儲存的 m 個標籤，真實的識別碼與私密金鑰{(ID_j, K_{j1}), (ID_j, K_{j2})}。

   (1) 逐項帶入含舊金鑰 K_{j1} 的虛擬亂數函數 F(ID_j, K_{j1}, N_j, b_{j-1})^l = d_j，判斷等式是否成立，若竭盡搜尋所有的標籤 (ID_j, K_{j1}) 結束，如圖三 e，沒有匹配成功，繼續執行下一步。

   (2) 逐項帶入新金鑰 K_{j2} 的虛擬亂數函數 F(ID_j, K_{j2}, N_j, b_{j-1})^l = d_j，判斷等式是否成立，若竭盡搜尋所有的標籤 (ID_j, K_{j2}) 結束，如圖三 e，沒有匹配成功，則拒絕標籤 Tag T j 的請求，表示標籤的驗證失敗。



圖三：Zhuang et al. RFID 群組驗證協定 [16]

伍、結論

綜上所述，共享經濟以租借代替購買及多人共用的商業模式，已成為創新企業的新寵，經濟規模也不斷擴大，個人或企業團體甚至可透過網際網路，進行跨國商業交易，在甚麼都有甚麼都可租借的概念下，大幅擴大了商業規模，但受限於法規仍然有所不足，加上小型企業或個人建置的服務平台，安全度與可信賴度不足，大型企業成為駭客攻擊的目標，就必須加強資訊安全與雙方的信任度。尤其個人主義興起，對交易雙方的隱私保障，必須格外注重。但是資料的開放與封閉，事實上是處於兩難之間。本文設計了一個簡易的共享經濟 RFID 群組驗證架構及操作步驟，如圖二，並結合了一個露營案例，進行說明，以及介紹了 Zhuang et al. RFID 群組驗證協定，如圖三，應用在共享經濟的協定，並分析其效能方面不足的地方。期盼透過本文的探討，促進共享經濟在資安議題上的研究。。

參考文獻

[1] S. Austin, C. Canipe, and S. Slobin, “The Billion Dollar Startup Club”, Wall Street Journal, 2015, http://graphics.wsj.com/billion-dollar-club/ (2016/9/30)

[2] L. Bolotnyy and G. Robins. “Generalized “Yoking-Proofs” for a Group of RFID Tags”, Proceedings of IEEE International Conference on Mobile and Ubiquitous Systems, pp. 1–4, 2006.

[3] R. Botsman and R. Rogers , “What's Mine Is Yours: The Rise of Collaborative Consumption”, HarperBusiness, America, ISBN: 1400119200, 2010.

[4] D. N. Duc, J. Kim and K. Kim, Scalable grouping-proof protocol for RFID tags, 2010 Symposium on Cryptography and Information Security, Japan: Takamatsu, pp. 19-22, 2010.

[5] D. N. Duc, D. M. Konidala, H. Lee, and K. Kim, “A survey on RFID security and provably secure grouping-proof protocols”, International Journal of Internet Technology and Secured Transactions, vol. 2, no. 3-4, pp. 222-249, 2010.

[6] The Economist, “The rise of the sharing economy- On the internet, everything is for hire”, The Economist Publishing, March 9th, 2013.

[7] EPCglobal Inc., “Class-1 generation-2 UHF RFID protocol for communications at 860 MHz–960 MHz versions 1.1.0”, 2007.

[8] S. G. Hong, H. J. Kim, H. R. Choi, K. Lee, and M. J. Cho, “Critical success factors for sharing economy among SMEs”, Mathematical Methods in Engineering and Economics, pp. 70-74, 2014.

[9] C. T. Hsi, Y. H. Lien, J. H. Chiu, Henry K. C. Chang, “Solving scalability problems on secure RFID grouping-proof protocol”, Wireless Personal Communications, vol. 84, no. 2, pp. 1069–1088, 2015.

[10] H. Huang, and C. Ku, “A RFID grouping proof protocol for medication safety of inpatient”, Journal Medical Systems, vol. 33, no. 6, pp. 467-474, 2009.

[11] A. Juels, and R. Pappu, “Squealing euros: Privacy protection in RFID-enabled banknotes”, In: Financial Cryptography, Springer-Verlag, pp. 103–121, 2003.

[12] Y. l. Liu, X. l. Qin, B. H. Li and L. Liu, “A forward-secure grouping-proof protocol for multiple RFID tags”, International Journal of Computational Intelligence Systems, vol. 5, no. 5, pp. 824-833, 2012.

[13] N. W. Lo and K. H. Yeh, “Anonymous coexistence proofs for RFID tags”, Journal of Information Science and Engineering, vol. 26, pp. 1213-1230, 2010.

[14] C. Ma, J. Lin, Y. Wang and M. Shang, Offline RFID grouping proofs with trusted timestamps, TRUSTCOM '12 Proceedings of the 2012 IEEE 11th International

Conference on Trust, Security and Privacy in Computing and Communications, Liverpool, UK, June 25-27, pp. 674-681, 2012.

[15] F. Marcus and S. L. Joe, “Community Structure and Collaborative Consumption: A Routine Activity Approach, ” American Behavioral Scientist March 21, pp. 614-624, 1978.

[16] Y. Zhuang, G. P. Hancke, D. S. Wong, “How to Demonstrate Our Presence Without Disclosing Identity Evidence from a Grouping-Proof Protocol”, Information Security Applications: 16th International Workshop, pp. 423-435, 2016.

[17] 康廷嶽, 黃柏偉, “由國際共享經濟發展探究我國中小企業商機”, 中小企業發展季刊, 2015.

[18] 李盈逸, “汽車共享輕鬆談(上)”, 財團法人車輛研究測試中心, 2009, https://www.artc.org.tw/chinese/03_service/03_02detail.aspx?pid=35 (2016/9/30)