Regular Paper

Communications of the CCISA
Vol. 28 No. 3 Aug. 2022

多所有者多權重之 RFID 標籤所有權轉移

羅嘉寧 [1,*]、楊明豪 [2] 許書瑜 [3]
[1] 國防大學資訊工程學系、[2] 中原大學資訊工程學系、[3] 銘傳大學電腦與通訊工程學系
[1]deer@ccit.ndu.edu.tw、[2]mhyang@cycu.edu.tw

摘要

近幾年來，無線射頻識別 (Radio Frequency Identification, RFID) 已成為供應鏈上不可或缺的技術。藉由貼在產品上的 RFID 標籤會經由上游的原料供應商、製造商、批發商轉移至消費者手上。在特定的情況下，一個 RFID 標籤所代表的物品會有多名所有者，一個所有者也會擁有多個 RFID 標籤，同時每個所有者對於不同的標籤所擁有的權重也不盡相同。更進一步的，RFID 標籤的部分所有權也可以在使用者間轉讓。本論文提出一個利用可信任第三方來負責分發所有權的管理協定，不僅能確保所有權間轉讓的正確性，同時標籤也僅需極少的計算量。最後，我們證明所提出的方法能抵禦目前大部分已知的 RFID 攻擊。

關鍵詞：秘密共享、無線射頻識別、所有權轉移、供應鏈管理

* 通訊作者 (Corresponding author.)

Regular Paper

Communications of the CCISA
Vol. 28 No. 3 Aug. 2022

An RFID Ownership Transfer Protocol based on multiple owners and different weights

Jia-Ning Luo[1,*], MingHour Yang[2], Shu-Yu Hsu[3]
[1]Department of Computer Science and Information Engineering, National Defense University,
[2]Department of Information and Computer Engineering, Chung Yuan Christian University,
[3]Department of Information and Telecommunications Engineering, Ming Chuan University
[1]deer@ccit.ndu.edu.tw、[2]mhyang@cycu.edu.tw

Abstract

In recent years, Radio Frequency Identification (RFID) has become an important technology in the supply chain management. With an RFID tag attached to the product, it will be transferred to consumers through material suppliers, manufacturers, and wholesalers. In a specific case, an item represented by an RFID tag will have multiple owners, and one owner will also own multiple RFID tags. Also, each owner has different weights for different tags. Furthermore, partial ownership of RFID tags can also be transferred between users. This paper proposes a management protocol that uses a trusted third party (TTP) to manage ownerships, which not only ensures the correctness of the transfer between ownerships, but also requires a minimal amount of computation for RFID tags. Finally, we show that the proposed method is resistant to most of the known RFID attacks.

Keywords: Secret Sharing, Radio Frequency Identification, Ownership Transfer, Supply Chain Management

壹、前言

無線射頻辨識 (Radio Frequency Identification, RFID) 由 RFID 標籤 (tag)、讀取器 (reader) 及相關應用系統所組成[1]。早在第二次大戰期間，英國空軍利用此技術來分辨戰機是敵是友[2]，1970 年之後陸續應用在商業上，包括供應鏈管理、門禁管理系統、醫療系統、ETC 等等[3]。在 2005 年美國的跨國零售業龍頭沃爾瑪 (Wal-Mart) 要求底下的供應商們要採用無線射頻辨識 RFID 技術[4]用於供應鏈管理。供應鏈管理是指產品經由上游的原料供應商、製造商、批發商至下游的零售商，最後再到消費者手上的轉移過程。貼在貨物上的 RFID 標籤會經過無數次的轉移，因而在轉移過程中，如何有效的管理產品的流向是供應鏈管理中一個重要的議題，在轉移的過程中，標籤裡的資訊可能會有外洩的疑慮，所以陸續學者們提出可以安全轉移所有權的協定。

Saito 等人[5]是最早提出針對單一所有者轉移單一 RFID 標籤的所有權轉移協議。Saito 等人的協定利用對稱加密的方法來防止原所有者在將一個 RFID 標籤轉移給新所有者之後還有權限可以再存取標籤。但該協議因為原所有者傳送新所有者共享金鑰導致有向前安全性的問題，還有 RFID 標籤於所有權轉移過程中並沒有跟新的所有者確認雙方是否皆已更新金鑰，所以會導致標籤金鑰不同步的問題，造成轉移失敗。Osaka 等人[6]利用了對稱加密及雜湊函數來滿足 RFID 系統安全性，但隨後 Jin 等人[7]、Wang 等人[8]、Kapoor 等人[9]、Yang[10]等人中說明了 Osaka 等人[6]的方法仍舊會有向前安全性、向後安全性等等的問題。Kulseng 等人[11]提出輕量的 RFID 相互認證身份的方法，只有經過身份驗證的讀取器及標籤才可互相通信，這樣可以減少標籤被竊聽及複製的發生，進而保護標籤以進行所有權轉移。但是 Kulseng 等人的協議還是有重送攻擊及非同步攻擊的問題。隨後 Cui 等人[12]改進 Kulseng 等人[11]協議中相互認證及所有權轉移的訊息結構，以抵禦先前提到的攻擊並增加所有權轉移協議的安全性。Chen 等人[13]提出了一種用於行動 RFID 且符合 EPC Class-1 Gen-2 標準的所有權轉移協議。

但隨著 RFID 的應用上越來越廣泛，單一所有者擁有單個標籤所有權轉移已經無法滿足其他的應用環境上，所以一些學者陸續提出多個所有者或多個標籤的所有權轉移。Sundaresan 等人[14]為多個所有者把多個標籤的所有權轉移的方法，該協議符合 EPC Class-1 Gen-2 標準。Tsai 等人[15]考慮了供應鏈中會有大量貨物進行所有權轉轉移的情況，必須確保所有貨物的所有權交給新所有者，所以該協議同時滿足了群組證明和所有權轉移並能抵禦大部分的攻擊。Moazami 等人[16]除了對 Zhu 等人[17]的協議提出詳細的說明非同步攻擊的步驟，另外也針對 Lee 等人[18]的協議說明該協議會遭受到秘密洩漏攻擊、向前安全性、可追蹤攻擊，因此 Moazami 等人就以 Lee 等人的協議為基礎提出了新的協議，並證明可以抵禦大部分的攻擊。

然而在特殊的應用下，會有一個 RFID 標籤具有多個所有者，而每一個所有者的權重皆不相同。例如在供應鏈的管理中，會有多個人擁有一個產品的管理權限。但是越高層級的所有者所擁有的管理權限越高，代表著對於該產品上的所有權重越高。因此在進

行 RFID 標籤多所有權轉移時，必須確認同意轉移的所有者們所擁有的權重是否達到門檻。Gan 等人的論文中[19]提出了一個多個所有者會在一個 RFID 標籤上擁有不同的權重值，並且該權重值可以在標籤有效期間內轉移至其他擁有者。Gan 等人作者利用拉格朗日 (Lagrange) 共享金鑰的方式把共享金鑰依照所有者擁有的權重多寡來分配不同份量的子金鑰給所有者。所有者之間可以互相把自己的權重值出售給其他所有者，也可以收購其他所有者的權重值。當進行出售或收購時，新所有者跟原所有者的權重值會有所改變。於所有權轉移時，所有者們須一一跟標籤進行相互認證並更新彼此間的金鑰，當進行標籤上的所有權轉移時，如果標籤知道所有者的權重已改變，便產生新的共享金鑰，標籤會將新的子金鑰分配給相對應權重的新所有者。但我們發現該論文方法中的標籤是負責分發子金鑰跟更新金鑰，因此標籤不僅需要進行大量的運算，且需要更新所有人的金鑰。

本論文為了改善上述的問題，我們提出一個利用可信任第三方 (Trusted Third Party, TTP) 來負責分發子金鑰及更新金鑰的多所有者具有不同權重的 RFID 標籤轉移協議。我們所提出的方法不僅能確保唯有當超過門檻值的多數所有者同意下，所有權方能透過可信任第三方轉移。此外，我們的方法相較於 Gan 等人的方法，可大幅減輕標籤的計算負擔。

貳、方法

我們提出了一個多所有者擁有 RFID 標籤上不同所有權的所有權轉移的方法。我們的方法參考 Sundaresan 等人[14]的架構。我們的所有權轉移架構如圖 1 所示，參與的角色分別有提出所有權轉移的讀取器R_1、原所有者讀取器集合R、新所有者讀取器集合R'、TTP 及 RFID 標籤。第一步由原多所有者讀取器內其中之一的原所有者讀取器R_1向 TTP 發出所有權轉移請求。在第二步中，TTP 通知原多所有者讀取器要轉移的訊息，若原多所有者讀取器同意轉移的權重大於門檻值則可進行所有權轉移。第三步由 TTP 重新計算新多所有者讀取器的權重，之後產生新金鑰S、分發新的子金鑰s_i。並使用偽隨機數加密的子金鑰s_i及標籤資訊一起發送給新多所有者。多新所有者讀取器對訊息進行身份驗證，驗證訊息是否屬於自己的，並利用共享金鑰解密收到各自的子金鑰及標籤資訊。最後每個新所有者讀取器向 TTP 回覆訊息。第四步是 TTP 驗證從所有新所有者讀取器那裡收到的訊息確認，然後跟標籤進行身份驗證，標籤解密接收到每個新所有者讀取器資訊後，向 TTP 發送回覆訊息。第五步，新所有者讀取器執行所有權測試協議以確保他們可以存取標籤。

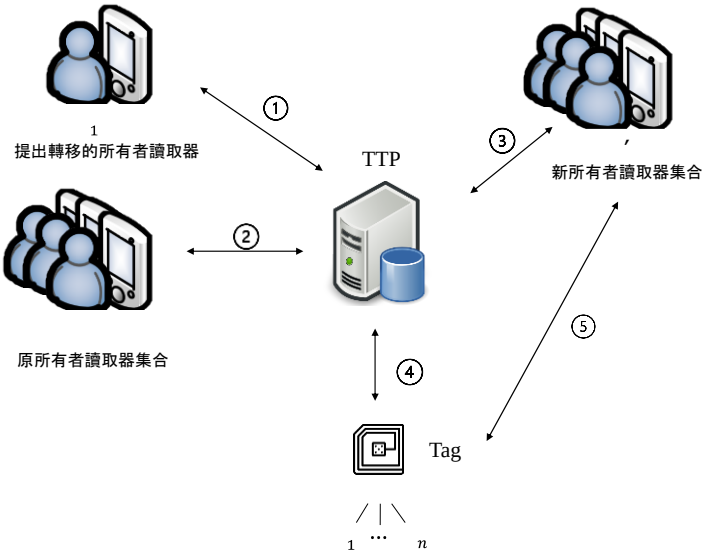

圖 1 所有權轉移架構

2.1 子初始化階段

在初始化階段時，TTP 分別計算$T_{id} = h(TID, T_s)$及$O_{id} = h(OID, O_s)$，並將計算過後的值儲存在所有者讀取器及標籤上。TTP 也分別與標籤共享金鑰ST_s及與所有者讀取器共享金鑰SO_s。每個所有者上儲存的元組$\{OID, O_{id}, SO_s, SO_s', T_{id}, PT_s\}$。標籤會為每個有權存取標籤的所有者儲存一次元組$\{TID, T_{id}, PT_s, PT_s'\}$及元組$\{O_{id}, OT_s, OT_s'\}$。我們的方法中所使用的符號定義表如表 1 所示。

表 1 符號定義表

符號	說明
t	權重的門檻值
n	所有者總人數
i	第i個所有者
w_i	第i個所有者的權重值
$p_i^{w_i}$	第i個所有者權重w_i的模數(mod)
S', S	TTP 產生的上一輪與舊的金鑰秘密值
S_n	TTP 產生的新金鑰祕密值
s_i	第i個所有者擁有的子金鑰
R	原多所有者讀取器集合
R_1	R其中一個所有者讀取器
R'	新多所有者讀取器集合
Tag	RFID 標籤

TTP	可信任第三方
v	要轉移的權重值
PO_s, PO_s'	每個 TTP 與每個所有者之間先前與前一輪的共享金鑰
PO_{s_n}	每個 TTP 與每個所有者之間新的共享金鑰
OT_s	所有者和標籤之間舊的共享金鑰
OT_s'	所有者和標籤之間上一輪的共享金鑰
$P1_r, P2_r$	TTP 產生的隨機數
TID	標籤的識別碼
T_{id}	計算過的雜湊函數值$h(TID, T_s)$
T_s	使用於計算T_{id}的金鑰，只有 TTP 知道
OID	所有者的識別碼
O_{id}	計算過後的雜湊函數值$h(OID, O_s)$
O_s	使用於計算O_{id}的密鑰，唯有 TTP 知道
RND_T	標籤向 TTP 發送的盲因子，用來隱藏偽隨機數
RND_o	新所有者向所有者發送的盲因子，用來隱藏偽隨機數
ACK_o	新所有者傳送確認給 TTP
ACK_T	標籤傳送確認給 TTP
$E(key, msg)$	對稱金鑰加解密，利用金鑰將訊息加解密

另外，TTP要產生金鑰祕密值S之前，需要選擇權重模數(mod)參數。假設所有者$R_1, \dots, R_n$分別擁有權重$w_1, \dots, w_n$，每份子金鑰的權重值為$w_i (1 < w_i < t)$，步驟如下：

步驟 1：

假設所有者子金鑰具有最小的權重 $(i.e, w_i = 1)$，TTP 產生數列:$p_1^1 < p_2^1 \dots < p_n^1$ 及整數p_0，須滿足以下條件：

(1) $p_0 \cdot p_{n-t+2}^1 \cdot \dots \cdot p_n^1 < p_1^1 \cdot p_2^1 \cdot \dots \cdot p_t^1$

(2) $\gcd(p_0, p_i^1) = 1,\ i = 1,2, \dots, n$

步驟 2：

TTP 在Z_{p_0}集合選擇整數金鑰S 以及產生整數α，需滿足以下條件：

(1) $S + \alpha p_0 \in Z_{p_{n-t+2}^1 p_{n-t+3}^1 \cdot \dots \cdot p_n^1, p_1^1 \cdot p_2^1 \cdot \dots \cdot p_t^1}$

步驟 3：

假設所有者的子金鑰具有較大的權重$(i.e., w_i > 1)$，TTP 產生p_i^w，需符合以下條件：

(1) $\prod_{i=t-w_i+1}^{t} P_i^1 < P_i^{w_i} < \prod_{i=n-t+2}^{n-t+(1+w_i)} P_i^1$

(2) $\gcd(p_0, p_i^{w_i}) = 1$

步驟 4：

TTP 計算子金鑰 $s_i = S + \alpha p_0 \bmod p_i^{w_i}$之後分別發給所有者$R_1, \dots, R_n$。

2.2 所有權轉移過程

所有權轉移分為三個部分，第一部分是詢問原多所有者是否轉移所有權，第二部分是 TTP 跟多新所有者讀取器集合相互認證並發送子金鑰；第三部分為 TTP 跟標籤相互認證並確定標籤的所有權已轉移至多新所有者讀取器。第一部分 (步驟 1～步驟 3) 如圖 2 所示；第二部分 (步驟 4～步驟 6) 如圖 3 所示。第三部分 (步驟 7～步驟 9) 如圖 4 所示。

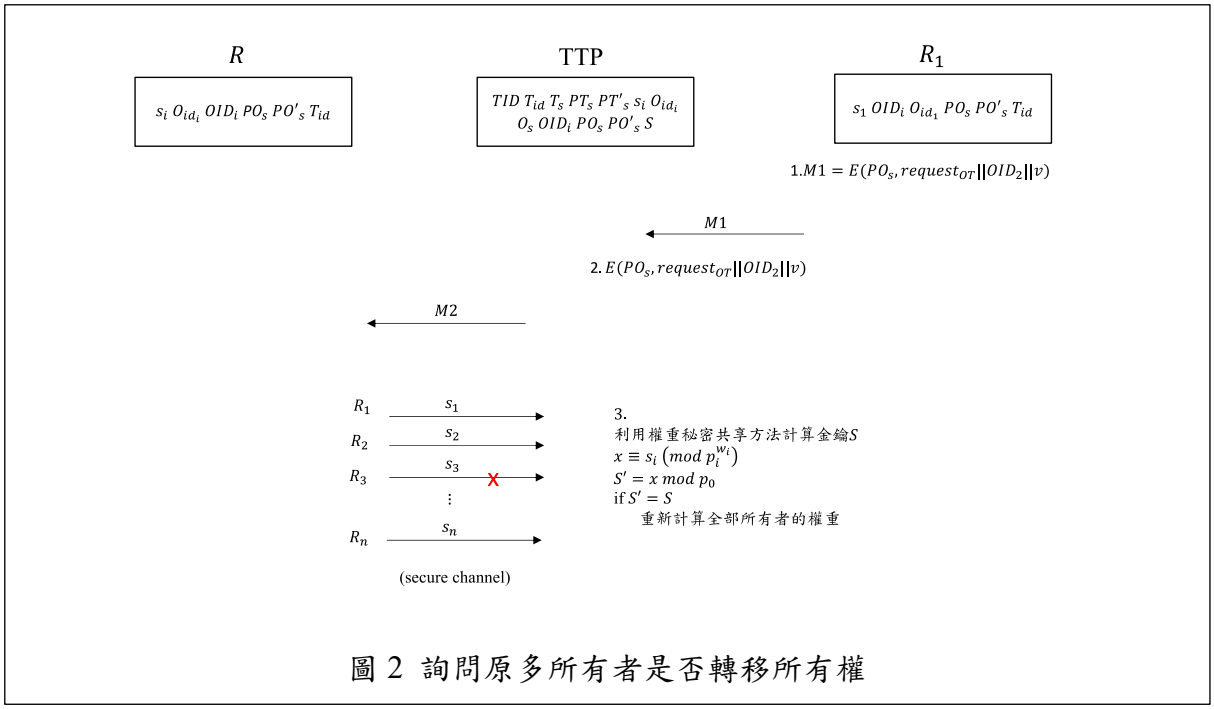

圖 2 詢問原多所有者是否轉移所有權

步驟 1：

當原多所有者讀取器集合R其中一個所有者讀取器R_1要將自己的所有權轉移給R_2時，所有者讀取器R_1將所有權請求、轉移目標所有者讀取器R_2的識別碼、要轉出的權重v利用PO_s加密後製作成訊息$M1$，要求 TTP 詢問其他所有者是否同意所有權轉移。

步驟 2：

TTP 收到訊息$M1$後利用共享金鑰PO_s解密。當接收到原所有者讀取器R_1要將自己的所有權權重進行轉移的請求時，TTP 將所有權請求、轉移目標所有者讀取器R_2的識別碼、要轉出的權重v再利用共享金鑰PO_s加密後製作成訊息$M2$傳送給原多所有者讀取器R中每個所有者讀取器來詢問是否同意所有權轉移。

步驟 3：

當原多所有者讀取器R收到訊息$M2$時，利用原多所有者讀取器R與 TTP 共享金鑰PO_s解開訊息$M2$詢問是否同意所有權轉移，同意的所有者讀取器分別將自己的子金鑰傳給 TTP。TTP 將收集到的子金鑰用權重秘密共享的方法[20]先算出$x \equiv s_i (mod\ p_i^{w_i})$，並利用$x$算出金鑰$S' = x\ mod\ p_0$，如果跟 TTP 儲存的金鑰$S$不相符，表示不同意所有權轉移。反之，表示同意所有權轉移。

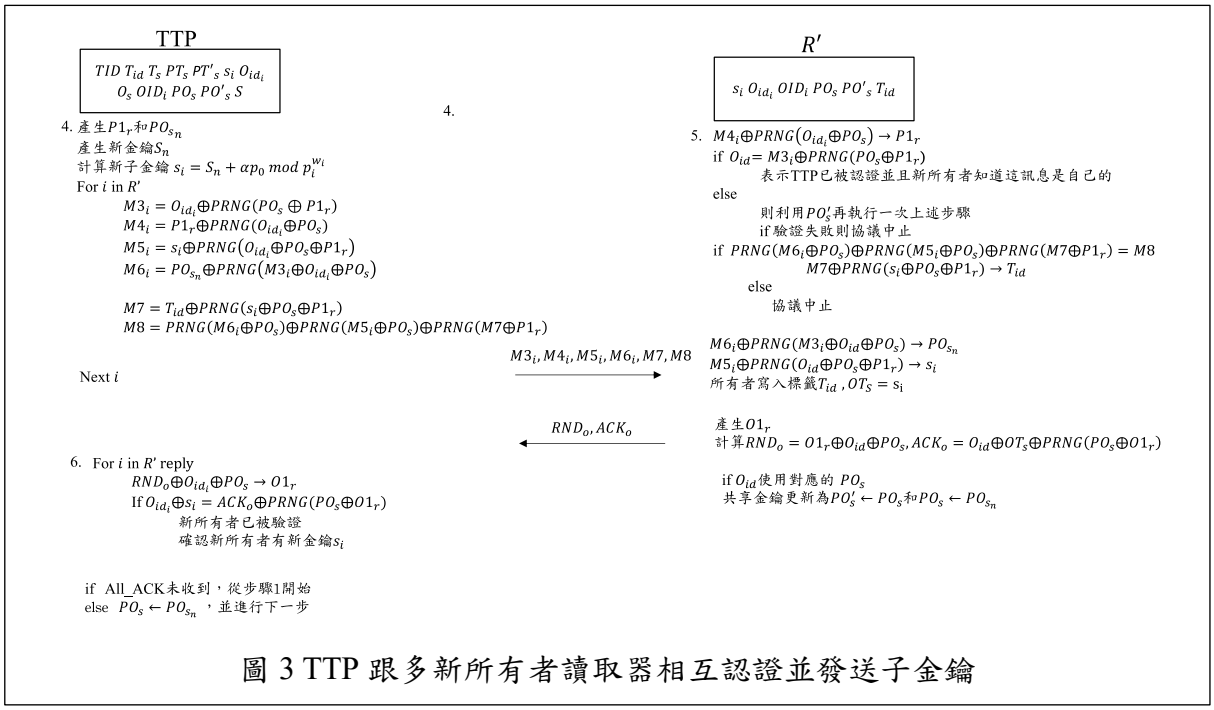

圖 3 TTP 跟多新所有者讀取器相互認證並發送子金鑰

步驟 4：

TTP 產生偽隨機數$P1_r$、TTP 與新多所有者讀取器集合R'的共享金鑰PO_{s_n}以及新金鑰S_n。然後會為每個新所有者讀取器依照新權重來計算子金鑰$s_i = S_n + \alpha p_0\ mod\ p_i^{w_i}$並計算$M3_i = O_{id_i} \oplus PRNG(PO_s \oplus P1_r), M4_i = P1_r \oplus PRNG(O_{id_i} \oplus PO_s), M5_i = s_i \oplus PRNG(O_{id_i} \oplus PO_s \oplus P1_r), M6_i = PO_{s_n} \oplus PRNG(M3_i \oplus O_{id_i} \oplus PO_s), M7 = T_{id} \oplus PRNG(s_i \oplus PO_s \oplus P1_r), M8 = PRNG(M6_i \oplus PO_s) \oplus PRNG(M5_i \oplus PO_s) \oplus PRNG(M7 \oplus P1_r)$，最後 TTP 將訊息$M3_i, M4_i, M5_i, M6_i, M7, M8$傳給新多所有者讀取器集合$R'$。

步驟 5：

每個新所有者讀取器使用儲存的O_{id}, PO_s從訊息$M4_i$取得$P1_r$並驗證是否$O_{id} = M3_i \oplus PRNG(PO_r \oplus P1_r)$。如果驗證失敗，新所有者讀取器會使用前一輪的共享金鑰PO'_s再重新對O_{id}進行驗證，如果其中一個共享金鑰相符，表示 TTP 通過身分驗證以及每個新所有者讀取器知道該訊息是給自己的。該驗證可以確定$M3_i$和$M4_i$在傳輸過程中不受攻擊者竄改。再來，每個所有者讀取器驗證訊息是否$M8 = PRNG(M6_i \oplus PO_s) \oplus PRNG(M5_i \oplus PO_s) \oplus PRNG(M7 \oplus P1_r)$，該驗證為了確保訊息

$M6_i, M5_i, M7$不受攻擊者竄改，之後從訊息$M7$取出T_{id}，如果標籤驗證失敗，則協議中止。

每個所有者從訊息$M6_i$取出PO_{s_n}以及從訊息$M5_i$取得s_i。然後，新所有者讀取器寫入被授權存取的標籤T_{id}。完成後，新所有者讀取器產生偽隨機數$O1_r$，計算$RND_O = O1_r \oplus O_{id} \oplus PO_s$及$ACK_O = O_{id} \oplus OT_s \oplus PRNG(PO_s \oplus O1_r)$。之後將訊息$RND_O, ACK_O$傳回給TTP。最後，如果$O_{id}$是使用對應的共享金鑰$PO_s$，新所有者讀取器將共享金鑰更新為$PO'_s \leftarrow PO_s$ 和$PO_s \leftarrow PO_{s_n}$。

步驟 6：

TTP 會根據每個新所有者讀取器回覆，從訊息RND_O取得$O1_r$並驗證是否 $O_{id_i} \oplus s_i = ACK_o \oplus PRNG(PO_s \oplus O1_r)$。如果成功，表示新的所有者讀取器已通過身份驗證，並且確認該新所有者有新的子金鑰。然而如果 TTP 未收到所有新所有者讀取器的確認，將從步驟 4 重新開始。反之，TTP 將更新共享金鑰$PO_s \leftarrow PO_{s_n}$，然後開始進行下一步。

步驟 7：

TTP 產生偽隨機數$S1_r$，之後會每個新所有者讀取器i計算$M9_i = s_i \oplus PRNG(S \oplus P2_r), M10_i = O_{id_i} \oplus PRNG(s_i \oplus S \oplus P2_r), M11_i = PRNG(M9_i \oplus P2_r \oplus S_n) \oplus PRNG(M10_i \oplus S), M12 = T_{id} \oplus PRNG(T_{id} \oplus S \oplus P2_r), M13 = P2_r \oplus PRNG(T_{id} \oplus S), M14 = S_n \oplus PRNG(M12 \oplus T_{id} \oplus S)$，最後 TTP 分別將訊息$M9_{(1,\dots,i)}, M10_{(1,\dots,i)}, M11, M12, M13, M14$傳給標籤。

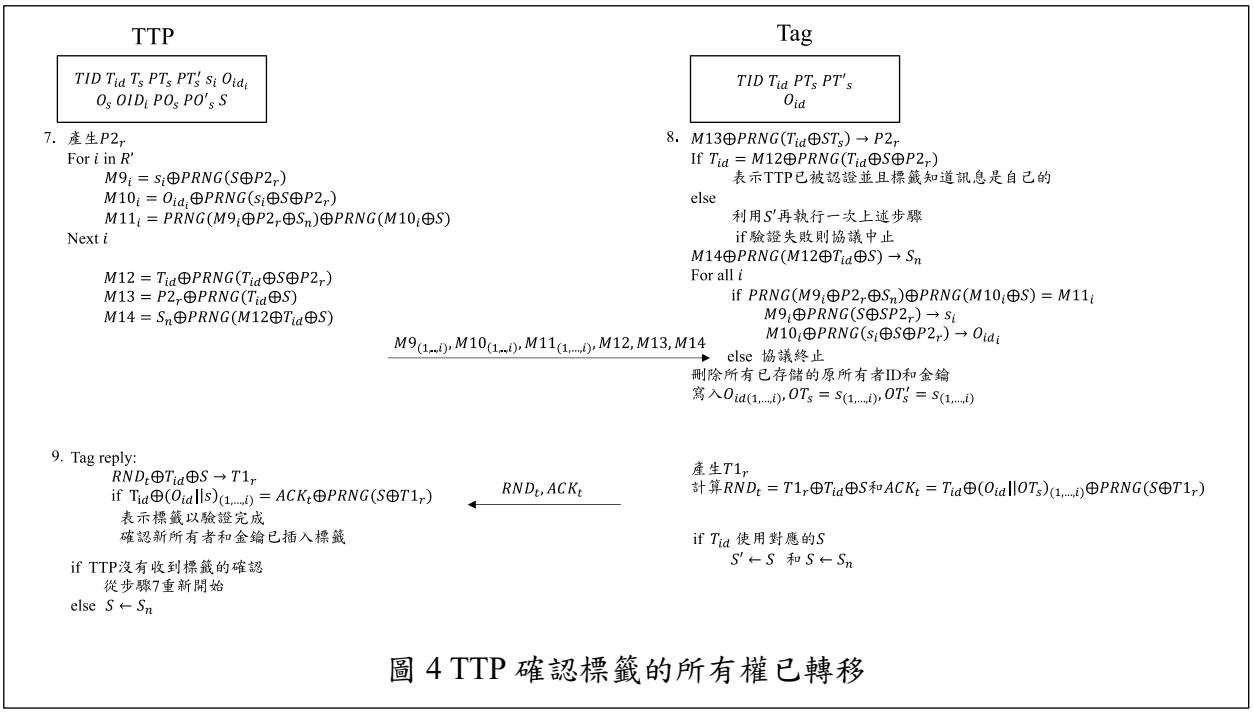

圖 4 TTP 確認標籤的所有權已轉移

步驟 8：

標籤接收到訊息$M9_{(1,\dots,i)}, M10_{(1,\dots,i)}, M11, M12, M13, M14$時，使用儲存的$T_{id}, S$從訊息$M13$取得$P2_r$並驗證是否$T_{id} = M12 \oplus PRNG(T_{id} \oplus S \oplus P2_r)$。如果驗證失敗，標籤會使

用上一輪的共享金鑰S'再重頭開始，如果其中一個共享金鑰相符，表示 TTP 通過身分驗證以及標籤知道該訊息是給自己的。該驗證可以確定$M12$和$M13$在傳輸過程中不受攻擊者竄改。再來，標籤從訊息$M14$取得S_n並利用接收到的所有新所有者i的訊息$M11_i = PRNG(M9_i \oplus P2_r \oplus S_n) \oplus PRNG(M10_i \oplus S)$進行驗證，該驗證為了確保訊息$M9_i, M10_i, M14$不受攻擊者竄改，之後從訊息$M9_i$取出$s_i$及訊息$M10_i$取出$O_{id_i}$。如果有任何$i$檢查失敗，則協議中止。

每個標籤刪除所有已儲存的原所有者 ID 及金鑰，並寫入新所有者$Oid_{(1,..,i)}$，並將現在和上一輪的共享金鑰設置為$OT_s = s_{(1,...,i)}, OT'_s = s_{(1,...,i)}$完成後，新所有者產生偽隨機數$T1_r$，計算$RND_t = T1_r \oplus T_{id} \oplus S$及$ACK_t = T_{id} \oplus (O_{id} || OT_s)_{(1,...,i)} \oplus PRNG(S \oplus T1_r)$。之後將訊息$RND_t, ACK_t$傳回給 TTP。最後，如果$T_{id}$使用對應的金鑰$S$，標籤將金鑰更新為$S' \leftarrow S$和$S \leftarrow S_n$。

步驟 9：

TTP 會根據標籤的回覆，從訊息RND_t取得$T1_r$並驗證是否$T_{id} \oplus (O_{id} || s)_{(1,..,i)} = ACK_t \oplus PRNG(S \oplus T1_r)$。如果成功，表示標籤已通過身份驗證，以及確認新所有者和金鑰已寫入標籤。然而如果 TTP 未收到所有新所有者讀取器的確認，將從步驟 7 重新開始。反之，TTP 更新金鑰$S \leftarrow S_n$。

2.3 所有權測試協議

我們使用 Sundaresan 等人的方法去確保多新所有者擁有標籤所有權，該協議假設是在虛擬環境中進行。對於標籤中的每個新所有者讀取器i和標籤，將O_{id_i}, T_{id}發送到標籤。標籤會檢查是否$T'_{id} = T_{id}$，如果符合，則使用對應的O_{id_i}的OT_s計算$M_{tst} = O_{id_i} \oplus OT_s \oplus T_{id}$。之後$M_{tst}$發送給新所有者讀取器。收到標籤的回覆之後，每個新所有者讀取器會檢查$O_{id_i} \oplus OT_{s_i} = M_{tst} \oplus T_{id}$，如果相符，則確認標籤所有權並在此時退出 For 迴圈以減少處理時間。如果全部的所有者未在規定的時間內辨識標籤，就會重新啟動所有權測試協議。

參、效能分析比較

我們分析本論文所提出的所有權轉移的計算量。我們和 Gan 等人的方法比較時針對轉移一個含有os個舊所有者擁有一個標籤所有權轉移給ns個新所有者所需的計算量進行比較。T_{RNG}標示產生一個隨機數的時間，T_E表示進行一次加解密所需的時間，T_H表示進行一次雜湊函數運算所需的時間，T_L表示進行一次拉格朗日秘密共享運算所需的時間。

我們所提出的所有權轉移方法及 Gan 等人的標籤及讀取器計算量如表 2 所示。由於 xor 運算及比較運算相對於加密方法相比的計算量過輕所以我們認為可以忽略計算量。另外，我們將訊息加密及解密的運算分別都計算一次T_E的加解密運算。

表 2 計算量比較表

方法名稱	設備名稱	計算量
Gan等人[19]	標籤	$(ns+os)T_{RNG}+2(ns+os)T_H+T_L$
	讀取器	$(ns+os)T_{RNG}+(ns+os)T_H$
我們的方法	標籤	$(5+3ns)T_{RNG}$
	讀取器	$(os)T_E$+$(6\text{ns}+2)T_{RNG}$

接下來我們將我們所提出的方法與 Gan 等人的方法做執行效能的比較，圖 5、圖 6 為我們及 Gan 等人的方法的標籤及讀取者所需要花費的時間，我們以 Gan 等人論文中標籤計算量的實驗條件為基準來做比較，對於參與所有權轉移的所有者人數及所需還原金鑰的權重總和進行了三種情況做分析。第一種情況是參與所有權轉移的所有者人數為 3、所需還原金鑰的權重總和為 2。第二種情況是參與所有權轉移的所有者人數為 4、所需還原金鑰的權重總和為 5。第三種情況是參與所有權轉移的所有者人數為 4、所需還原金鑰的權重總和為 9。

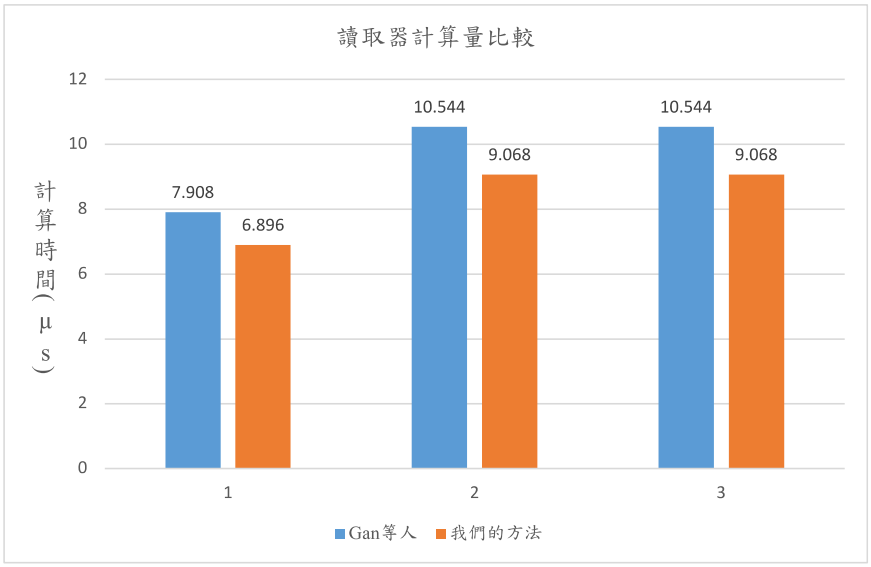

圖 5 讀取器的計算量比較

我們使用 AES[21]、SHA-256 等加密方法，計算出兩者的所有權轉移方法需消耗的時脈週期後，假設 RFID 標籤一秒內執行 3.55M 個時脈週期[22]，讀取器則假設一秒內執行 1G 個時脈週期，可以計算出每個所有權轉移所需花費的時間，之後將單位為秒轉換成微秒(μs)來做比較。

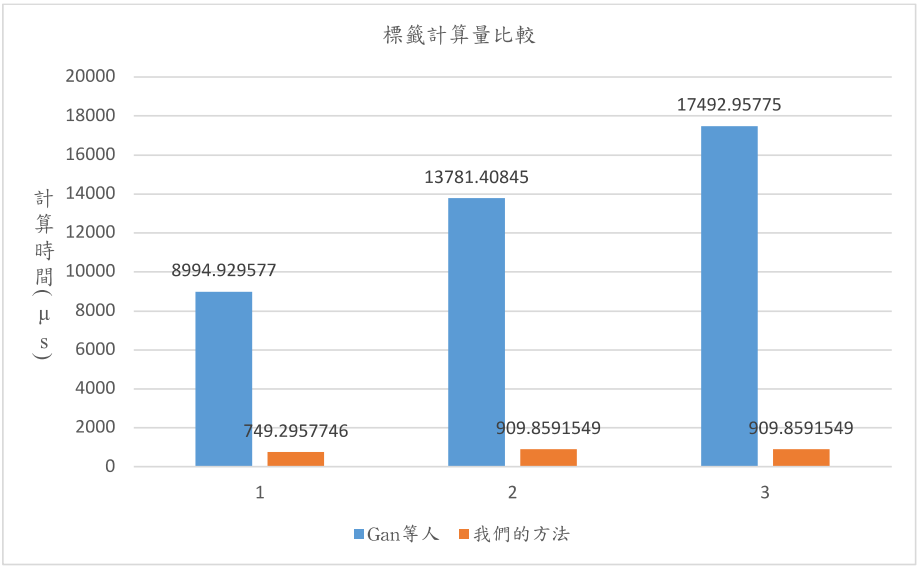

圖 6 標籤的計算量比較

由圖 6 可以看出我們的方法在標籤中的運算時間遠小於 Gan 等人的方法，因為在 Gan 等人的方法中，標籤需要負擔大部分的計算量，包括與所有者相互認證及拉格朗日秘密共享的計算。其中，拉格朗日秘密共享的方法會隨著所需的權重總和造成標籤計算量增加。而我們的方法是將大部分的計算交由 TTP 來完成，包括 TTP 與新所有者或與標籤的相互認證及權重秘密共享的計算，所以在第二種及第三種的情況中，當參與所有權轉移的所有者人數相同，但所需還原金鑰的權重總和不同時，我們的方法的標籤計算量也不會因此改變。而由圖 5 可以看出我們的方法在讀取器中的運算也小於 Gan 等人的方法，因為我們的方法除了計算了一次加解密運算外，其他部分都只使用 xor、PRNG 和偽隨機數來完成所有權轉移。然而，Gan 等人的方法則利用雜湊函數和隨機數來完成所有權轉移。所以整體來說所有權轉移所需要花費的時間，我們的方法遠小於 Gan 等人的方法。

肆、安全性分析

我們以下分析主要針對我們的方法中的標籤和讀取器的機密性、防止重送攻擊、匿名性、保護位置隱私、向前安全性、中間人攻擊及非同步阻斷服務攻擊進行安全性分析。

(1) 機密性：

每次的通訊中使用共享金鑰與產生的偽隨機數來確保安全性。

(2) 防止重送攻擊

通過在每一階段都會產生新偽隨機數確保每一輪中所有訊息的唯一性。因此攻擊者重送之前的訊息無法驗證成功。

(3) 標籤/所有者匿名

以標籤來說，T_{id}僅包含實際TID的預先計算的雜湊值。由於雜湊函數是單向的特性，攻擊者將無法從T_{id}中找到TID。同理，所有者也是利用此原則達到匿名性

(4) 標籤/所有者位置隱私

上述原則也適用提供標籤及所有者位置隱私。

(5) 向前安全性

協議中的標籤訊息RND_t及ACK_t使用偽隨機數$T1_r$以及T_{id}來計算，$T1_r$以及T_{id}在每次執行所有權轉移協議都會不一樣，所以可以確保訊息的唯一性。即使攻擊者知道共享金鑰ST_s和ST_s'也無法解密標籤之前的訊息，進而達到向前安全性。另外，相同的原則也適用在新所有者讀取器傳送的訊息RND_o及ACK_o。

(6) 中間人攻擊

在所有權的轉移過程中，設備之間會利用彼此的共享金鑰來確認彼此的身份，確認完畢之後才能進行所有權轉移。然而攻擊者沒有共享金鑰，無法利用重送攻擊的方式來完成認證，所以攻擊者無法偽造讀取器或標籤來進行中間人攻擊。

(7) 非同步阻斷服務攻擊

攻擊者可以通過TTP與標籤的共享金鑰或TTP與新所有者之間的共享金鑰的不同步造成阻斷服務攻擊(Denial of Service attack, DoS)。當攻擊者惡意阻斷訊息或訊息在傳送的過程中遺失可能就會造成此攻擊。所以在我們的協議中標籤及讀取器保留了更新前後與TTP的共享金鑰，這樣攻擊者惡意阻斷訊息或金鑰更新的訊息遺失時，可再利用保留的更新前的金鑰去做認證，可以避免TTP和標籤不同步而造成無法讀取的問題。

伍、結論

目前已提出多種運用在供應鏈上的各種情況的多所有者的所有權轉移，但都是在多所有者擁有標籤相等所有權的情況，所以本論文提出一個在不同權重下的多所有者RFID 標籤所有權轉移協定，我們用權重秘密共享的方式來確保當原本的多所有者之間，同意的所有者擁有的權重超過一定的門檻值才能進行所有權轉移。能在 TTP 跟新的多所有者之間進行相互認證時，就將新的子金鑰交給每個新所有者，之後就只有新所有者能夠存取標籤的權限。

我們分析標籤、讀取器的計算量和 Gan 等人的方法進行效能比較。因為我們將大部分的計算都交由 TTP 去運算，可證明我們的方法的計算量明顯小於 Gan 等人的方法的計算量。另外，我們的方法能防止重送攻擊、向前安全性、中間人攻擊、非同步阻斷服務攻擊，並且可以保護標籤及所有者的隱私，令攻擊者無法獲取他們的資訊。

我們的協議可以運用在供應鏈管理中的特殊情況下。當多個人擁有一個產品的管理

權限，並且該產品的權限中，每個人的權重有所不同。而此種情況，可透過我們提出的方法，轉移所有者的部分權重。在所有權轉移過程中，我們透過 PRNG 以及 xor 運算，可確保所有權轉移的安全性，並且有效率地進行轉移。

參考文獻

[1] C. M. Roberts, "Radio frequency identification (RFID)," *Computers & security,* vol. 25, no. 1, pp. 18-26, 2006.

[2] J. Landt, "The history of RFID," *IEEE potentials,* vol. 24, no. 4, pp. 8-11, 2005.

[3] K. Ahsan, H. Shah, and P. Kingston, "RFID applications: An introductory and exploratory study," *arXiv preprint arXiv:1002.1179,* 2010.

[4] A. Juels, "RFID security and privacy: A research survey," *IEEE journal on selected areas in communications,* vol. 24, no. 2, pp. 381-394, 2006.

[5] J. Saito, K. Imamoto, and K. Sakurai, "Reassignment scheme of an RFID tag's key for owner transfer," in *International Conference on Embedded and Ubiquitous Computing*, 2005: Springer, pp. 1303-1312.

[6] K. Osaka, T. Takagi, K. Yamazaki, and O. Takahashi, "An efficient and secure RFID security method with ownership transfer," in *RFID security*: Springer, 2008, pp. 147-176.

[7] Y. Jin, H. Sun, and Z. Chen, "Hash-based tag ownership transfer protocol against traceability," in *2009 IEEE International Conference on e-Business Engineering*, 2009: IEEE, pp. 487-492.

[8] C.-H. Wang and S. Chin, "A new RFID authentication protocol with ownership transfer in an insecure communication environment," in *2009 Ninth International Conference on Hybrid Intelligent Systems*, 2009, vol. 1: IEEE, pp. 486-491.

[9] G. Kapoor and S. Piramuthu, "Single RFID tag ownership transfer protocols," *IEEE Transactions on Systems, Man, and Cybernetics, Part C (Applications and Reviews),* vol. 42, no. 2, pp. 164-173, 2010.

[10] M. H. Yang, "Across-authority lightweight ownership transfer protocol," *Electronic Commerce Research and Applications,* vol. 10, no. 4, pp. 375-383, 2011.

[11] L. Kulseng, Z. Yu, Y. Wei, and Y. Guan, "Lightweight mutual authentication and ownership transfer for RFID systems," in *2010 Proceedings IEEE INFOCOM*, 2010: IEEE, pp. 1-5.

[12] P.-y. Cui, "An Improved Ownership Transfer and Mutual Authentication for Lightweight RFID Protocols," *IJ Network Security,* vol. 18, no. 6, pp. 1173-1179, 2016.

[13] C.-L. Chen, Y.-C. Huang, and J.-R. Jiang, "A secure ownership transfer protocol using EPCglobal Gen-2 RFID," *Telecommunication Systems,* vol. 53, no. 4, pp. 387-399, 2013.

[14] S. Sundaresan, R. Doss, W. Zhou, and S. Piramuthu, "Secure ownership transfer for multi-tag multi-owner passive RFID environment with individual-owner-privacy," *Computer Communications,* vol. 55, pp. 112-124, 2015.

[15] K.-Y. Tsai, M. H. Yang, J. N. Luo, and W.-T. Liew, "Novel designated ownership transfer with grouping proof," *Applied Sciences,* vol. 9, no. 4, p. 724, 2019.

[16] F. Moazami and M. Safkhani, "SEOTP: a new secure and efficient ownership transfer protocol based on quadric residue and homomorphic encryption," *Wireless Networks,* pp. 1-22, 2020.

[17] D. Zhu, W. Rong, D. Wu, and N. Pang, "Lightweight anonymous RFID group ownership transfer protocol in multi-owner environment," in *2017 IEEE 19th International Conference on High Performance Computing and Communications; IEEE 15th International Conference on Smart City; IEEE 3rd International Conference on Data Science and Systems (HPCC/SmartCity/DSS)*, 2017: IEEE, pp. 404-411.

[18] C.-C. Lee, C.-T. Li, C.-L. Cheng, and Y.-M. Lai, "A novel group ownership transfer protocol for RFID systems," *Ad Hoc Networks,* vol. 91, p. 101873, 2019.

[19] Y. Gan, Y. X. Zhang, L. He, and Q. K. Zhang, "Research on a Dynamic Transfer Protocol for Multi-owner Tag Ownership," in *2019 IEEE 11th International Conference on Communication Software and Networks (ICCSN)*, 2019: IEEE, pp. 647-651.

[20] L. Harn and F. Miao, "Weighted Secret Sharing Based on the Chinese Remainder Theorem," *IJ Network Security,* vol. 16, no. 6, pp. 420-425, 2014.

[21] V. Rijmen and J. Daemen, "Advanced encryption standard," *Proceedings of Federal Information Processing Standards Publications, National Institute of Standards and Technology,* pp. 19-22, 2001.

[22] A. S. Man, E. S. Zhang, V. K. Lau, C. Y. Tsui, and H. C. Luong, "Low power VLSI design for a RFID passive tag baseband system enhanced with an AES cryptography engine," in *2007 1st Annual RFID Eurasia*, 2007: IEEE, pp. 1-6.

[作者簡介] Biography

羅嘉寧博士為國立交通大學資訊工程系博士，現為國防大學理工學院資訊工程學系副教授兼任網路攻防組組長及資訊安全中心助理。其主要研究專長為網路安全，物聯網系統及機器人控制。