用於共享經濟的安全行動支付協議

薛夙珍　　吳政典
朝陽科技大學　　朝陽科技大學
資訊管理學系　　資訊管理學系
e-mail：　　e-mail：
schsueh@cyut.edu.tw　s10514605@cyut.edu.tw

摘要

近年來，共享經濟成為了一種新的商業模式，就是將個人的閒置資產租借給他人使用。這種新興的經濟模式，帶來了資訊安全疑慮。共享經濟的交易模式通常使用行動支付，而行動支付使用的智慧裝置，經常使用無線網路進行資料傳輸。在這樣的環境裡，惡意攻擊者將可能使用特殊設備攔截機密資訊。若機密訊息沒有經過特殊處理或加密，惡意攻擊者將可得知訊息內容。因此，本論文設計了共享經濟的安全交易協議。當使用者使用共享經濟平台且啟動交易時，將由服務商產生該筆交易的金鑰與隨機數，讓使用者與資源提供者能共享金鑰，並且透過一次性的隨機數來驗證交易的有效性。因此惡意攻擊者攔截到訊息也無法於下回交易使用，降低了共享經濟交易中的安全風險。

關鍵詞：共享經濟、資訊安全、行動支付。

Abstract

In recent years, sharing economy has become a new business model, that is the personal idle assets leased to others. This emerging model has brought information security problems. The sharing economy transaction usually use mobile payment, while smart devices for mobile payments often use wireless networks for data transmission. In such an environment, a malicious attacker could use special equipment to intercept confidential information. If a confidential message has not been specially processed or encrypted, a malicious attacker will be able to know the message content. Therefore, this paper designs the secure transaction protocol for sharing economy. When the user uses the sharing economy platform and launches the transaction, the key and random number will be generated by the service provider so that the user and the resource provider can share the key to encrypt confidential information, and through the random number to verify. A malicious attacker intercepted the message cannot be used in the next transaction, so the sharing economy payment is more security.

Keywords: Sharing economy, information security, mobile payment.

1. 前言

科技日新月異，使人們的生活越來越便捷，除了傳統的桌上型電腦、筆記型電腦之外，行動智慧裝置更是與人們密不可分。隨著行動智慧裝置的快速發展，也有許多企業針對行動智慧裝置開發付款系統，例如蘋果電腦的 Apple Pay[1]與 Google 公司的 Google Wallet[6]。這一類的行動支付系統，改變了傳統的付款機制，進而改變了整個線下與線上消費的生態。無線網路與行動智慧裝置結合，可以在各個不同的地點使用行動智慧裝置進行小額支付，即時的與可信任的第三方或銀行進行資訊同步，快速的完成付款。

在行動支付快速發展之下，也帶動了電子商務的發展。在電子商務的討論裡，共享經濟成為了近年來的熱門議題。共享經濟又稱為分享型經濟，指的是在網路環境中，任何有形的或無形的資產，都能夠被任何人使用、分享[12]。這種經濟模式能夠使個人或企業共享高單價的產品，減少購買或維修的負擔。換句話說，使用者以租借方式取代購買，進而與世界上的人共享他們的資產，共同使用資源，減少閒置資產的浪費。

消費者已經越來越熟悉共享經濟平台的使用方法與交易模式，透過共享經濟的概念，減少了使用者與資源提供者的使用成本，使用者不必購買自己不常用的物品或資源，資源提供者可以透過共享的方式賺取一定利益。然而，在共享經濟的交易模式中，無法得知使用者使用的平台是否有嚴密的安全機制，無法確認共享經濟平台是否能保護使用者與資源提供者的重要訊息，使用者的訊息可能被惡意的第三方竊取或竄改，進而發生信用卡盜刷或資源提

供者重複請款之問題，造成使用者與銀行的損失。

在本論文中，提出了一個安全的支付協議方案，改善共享經濟平台的交易安全性。透過共享經濟服務商來核發使用者與資源提供者的秘密金鑰，來避免雙方的資訊被惡意第三者竊取，並且秘密金鑰僅能用於當次的交易。若使用者啟動另一筆交易，共享經濟服務商將會重新產生另一把金鑰，透過對稱金鑰進行加解密，安全的傳輸給使用者與資源提供者。在交易流程中，透過數位簽章的方法，驗證一筆資訊是由合法使用者所傳輸，使用數位簽章的訊息包含了銀行發放給使用者的信用額度與使用者傳輸給資源提供者的請款資訊；這兩筆訊息需要透過數位簽章的方式進行保護，以避免惡意的攻擊者擅自竄改信用額度或交易金額，造成使用者的不便與損失。另外，交易架構中使用了隨機數，在每一筆交易中，隨機數皆為不同，利用隨機數的特性避免資訊被重送，避免資訊被竄改的風險。

在第一節，介紹了共享經濟的環境、交易安全問題與研究動機；在第二節，探討過去的文獻中，對於行動支付與共享經濟的研究成果；在第三節，提出了用於共享經濟的安全交易協議，解決共享經濟的支付安全疑慮；在第四節，針對提出的方法進行安全分析與效能評估；在第五節，做出了本文的結論。

2. 文獻探討

2.1 共享經濟

共享經濟指的是將個人資產與他人分享的行為，由資源提供者提供閒置資產，讓使用者支付一定金額的使用費獲得使用權。透過這種經濟模式，減少資源的浪費，讓閒置資產也能產生新的價值[12]。且共享經濟已經有非常長的歷史，過去僅僅是親屬或朋友之間的分享[3]，但近期人們開始透過網路參與共享經濟的活動，以提高資源的使用率[4]，降低不需要的浪費。到現在，向使用資源的人收取一定的費用，使共享經濟成為了一個新的商業模式[3, 5]。

2.2 行動支付

行動支付指的是使用行動設備和無線網路技術支付款項[8]。消費者透過智慧型手機或平板電腦等裝置，支付各項服務或實體商品的費用。行動支付主要分為行動帳單付款、行動網路支付與非接觸型支付[10]。支付流程如表 1。行動帳單付款為經過一次性密碼的雙重認證，支付款項會由消費者的電信帳單中收取，這種方式不需要信用卡，且有手機門號的人都可使用。行動網路支付則是由消費者透過網頁或下載應用程式進行支付，這種方式使用無線應用協議為基礎。非接觸型 NFC 支付，最常用於實體商店與交通設施，消費者使用支援 NFC 的行動裝置，將行動裝置置於讀取器上進行支付，款項可能由銀行帳戶中扣除，或結合行動帳單付款，由電信公司代收款項[13]。

表 1 行動支付之付款流程

行動支付方式	付款流程
行動帳單付款	1.付款時，消費者從電信商取得一次性密碼。 2.輸入一次性密碼至手機。 3.完成付款，交易的款項將從消費者的電信帳單中收取。
行動網路支付	1.消費者開啟支付網頁或支付APP。 2.輸入付款資訊，利用無線網路傳輸交易訊息，完成交易。
非接觸型 NFC 支付	1.消費者使用支援 NFC 的手機。 2.將手機放置在商家的讀取器上。 3.款項可能即時從銀行戶頭扣款，或隨著信用卡帳單、電信帳單扣款。

在 2013 年，由 Pourghomi 等學者[11]，提出了使用 NFC 支付的安全協議，建立了安全且可信任的訊息，透過可信任的電信公司認證，減少了人們的交易流程。Jung 學者[7]在 2014 年發表了使用 NFC 的電子貨幣研究，使用互斥和雜湊函數的特性來保護重要訊息。Luo 等學者[9]在 2016 年提出一個匿名的 NFC 付款機制，讓使用者不被知道真實的身分進行行動支付，並有嚴密的安全機制，但過程過於繁複，加解密次數過多，造成效能較差。Badra 等學者[2]提出了輕量級 NFC 安全支付協議，減少了繁複的非對稱加解密過程，並使用安全元件（Secure Element）來增強安全性，但方法不夠完整。

3. 共享經濟的安全行動支付協議

在無線網路越來越成熟且智慧裝置的快速發展下，傳統的線下支付方式已經逐漸轉換為線上支付。其中，共享經濟平台幾乎都以線上支付為付款方式，線上支付又有一部分為行動支付，適合需要即時付款的共享經濟活動。但行動支付也帶來安全問題，智慧型手機等行動裝置通常使用無線方式連接網際網路，在無線網路環境中，傳輸的資訊比有線方式更容易被竊取，惡意的攻擊者只要有特殊設備就能擷取正在傳輸的訊息，不需入侵使用者的實體設備。因此，本論文提出一個即時支付的安全交易架構，保護共享經濟活動中，使用者與資源提供者的機密資訊，也避免惡意的使用者或資源提供者擅自竄改交易金額，維持交易的正確性。

本交易協議中有四個個體，分別為使用者（User, U）、資源提供者（Resource Provider, RP）、服務商（Service Provider, SP）與銀行（Bank, B）。使用者必須預先於銀行開戶，以減少銀行端的頻繁連線造成負擔，並由銀行核定信用額度給使用者，以進行後續的驗證。在架構中，由使用者啟動交易，服務商產生一個隨機數與一對秘密金鑰，分別傳送給使用者與資源提供者，隨機數用來檢驗本次交易的有效性，避免惡意的資源提供者向銀行進行重複請款。若有任一方無法提供隨機數，交易將終止；秘密金鑰進行機密資訊的加解密，用於保護隨機數與其他重要訊息，透過服務商來發放對加解密金鑰，讓使用者與資源提供者能夠以對稱式方法進行加解密，減少手持裝置之運算負擔。協議中使用之符號如表 2。協議架構如圖 1。協議分為使用者向銀行註冊階段、使用者啟動交易階段與付款階段，詳細流程如下。

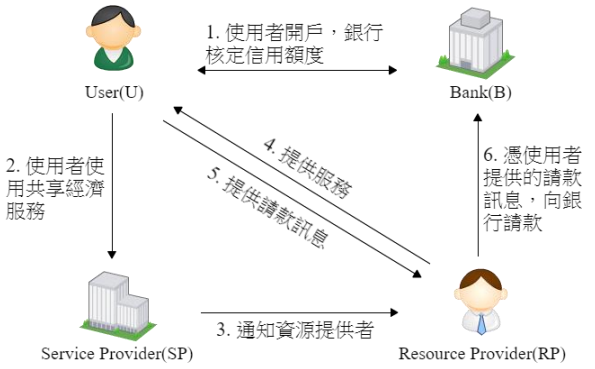

圖 1 協議架構圖

1. 使用者向銀行註冊階段

(1) 使用者預先於銀行開戶。

(2) 銀行確認身分，傳輸信用額度資訊給使用者，且信用額度資訊使用銀行私鑰進行數位簽章。

2. 使用者啟動交易階段

(1) 由使用者啟動交易，服務商產生暫時金鑰與隨機值，供後續傳輸秘密值與驗證使用。

(2) 服務商傳輸資源提供者資訊、暫時金鑰與隨機值給使用者。並傳輸使用者資訊、暫時金鑰與隨機值給資源提供者。

(3) 資源提供者傳輸收到的隨機值給使用者，讓使用者確認資源提供者是否合法。

(4) 使用者驗證完畢後，傳輸信用額度供資源提供者驗證。

(5) 資源提供者確認使用者之信用額度，通知使用者與服務商交易成立

(6) 服務商產生交易流水號，傳輸給資源提供者。並將本次請款資訊傳輸給銀行。

3. 付款階段

(1) 資源提供者傳輸交易金額給使用者。

(2) 使用者確認金額，傳輸請款資訊給資源提供者。

(3) 資源提供者傳輸請款資訊與驗證訊息給銀行。

(4) 銀行驗證無誤後，將交易金額從使用者帳戶扣款，支付至資源提供者帳戶。

表 2 符號表

符號	說明
SP	服務商
RP	資源提供者
U	使用者
B	銀行
ID_i	i 的識別資訊，i=U、RP、SP
K_{x-y}	x 與 y 預先共享的對稱金鑰
SK_i	i 的公鑰，i=U、B
PK_i	i 的私鑰，i=U、B
Credit	U 的銀行信用額度
X_{ACC}	X 的銀行帳號
H()	單向雜湊函數
R_S	本次交易之隨機數
K_{Temp}	本次交易之臨時金鑰
TID	交易流水號
Amount	交易金額
$E_i[x]$	使用 i 加密訊息 x
$SIGN_i[x]$	使用 i 數位簽章訊息 x

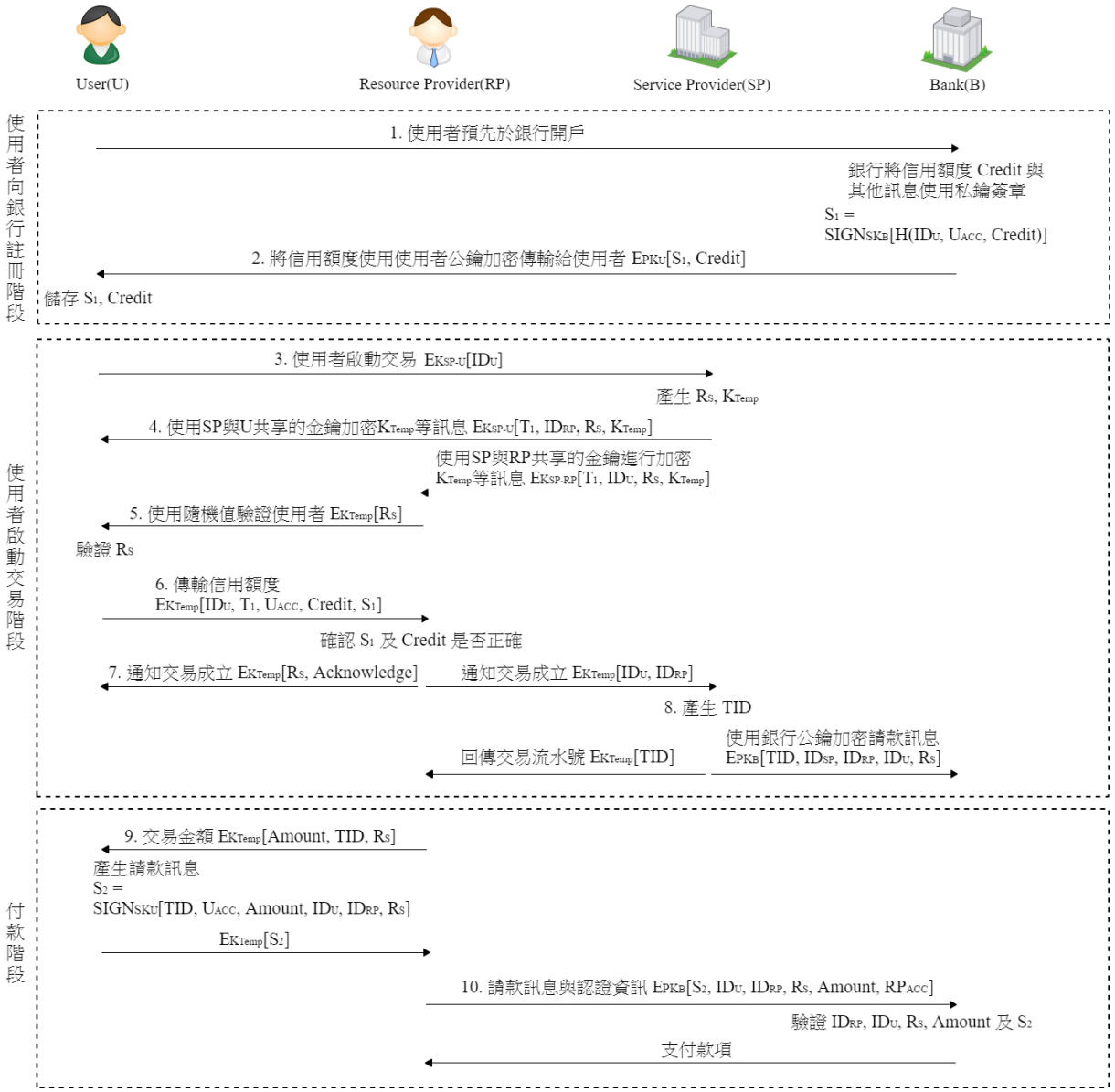

圖 2 交易流程

本協議為一個安全的交易架構用於共享經濟交易活動，其交易流程如圖 2，並依照下述流程進行。

1. 使用者預先於銀行透過線下或線上方式開戶，並由銀行核定信用額度 Credit 後作簽名 $S_1 = \mathrm{SIGN}_{SK_B}[\mathrm{H}(\mathrm{ID_U}, \mathrm{U_{ACC}}, \mathrm{Credit})]$。
2. 將S_1與 Credit 透過使用者公鑰PK_U加密後傳輸給使用者，使用者收到後使用自己的私鑰SK_U解開，儲存S_1與 Credit。
3. 當要使用共享經濟服務時，由使用者將其私鑰SK_U加密ID_U，傳輸給服務商，由服務商產生交易隨機數R_S與暫時金鑰K_{Temp}。
4. 服務商將T_1、ID_{RP}、R_S、K_{Temp}使用使用者預先與服務商共享的對稱金鑰K_{SP-U}加密，傳輸給使用者。T_1、ID_U、R_S、K_{Temp}使用資源提供者預先與服務商共享的對稱金鑰K_{SP-RP}加密，傳輸給資源提供者。
5. 資源提供者使用暫時金鑰K_{Temp}將R_S加密，傳輸給使用者。使用者使用K_{Temp}解密資訊，確認資源提供者的R_S與本身的相同。
6. 使用者將信用額度Credit、S_1與其他驗證資訊ID_U、T_1、U_{ACC}使用K_{Temp}加密，傳輸給資源提供者。資源提供者使用銀行公鑰PK_B解開S_1，驗證信用額度資訊。
7. 資源提供者使用K_{Temp}加密R_S、Acknowledge 傳給使用者。再使用K_{Temp}加密ID_U、ID_{RP}傳輸給服務商。
8. 服務商收到訊息後，產生交易流水號 TID，並使用K_{Temp}加密 TID，傳輸給資源提供者。

使用PK_B加密TID、ID_{SP}、ID_{RP}、ID_U、R_S，傳輸給銀行供請款驗證。

9. 在付款階段，由資源提供者傳輸使用K_{Temp}加密的交易金額Amount、TID、R_S給使用者。使用者確認交易金額無誤後，運算$S_2 = SIGN_{SK_U}[TID, U_{ACC}, Amount, ID_U, ID_{RP}, R_S]$，將$S_2$使用$K_{Temp}$加密，傳輸給資源提供者。
10. 資源提供者收到已加密的S_2，解開並使用銀行公鑰PK_B加密S_2、ID_U、ID_{RP}、R_S、Amount、RP_{ACC}，傳輸給銀行進行驗證。銀行使用使用者公鑰PK_U解開S_2，驗證由資源提供者提供的訊息是否與服務商提供的訊息相同。若兩者相同，即確認此次交易成功，將由使用者帳戶扣除交易金額之款項，並支付至資源提供者帳戶。

4. 安全分析

在本節中，分析所提出方案，可以抵抗各種攻擊和滿足安全需求。

1. 假冒攻擊

協議中的設計可以預防假冒攻擊，若有惡意的資源提供者要仿冒使用者進行交易，可以透過資訊攔截的方式竊取$E_{K_{SP-U}}[ID_U]$，仿冒使用者的身分啟動交易，但在付款階段時，資源提供者無法算出S_2；因為使用使用者私鑰進行簽名，若送了錯誤的S_2給銀行，銀行將驗證失敗而終止交易。

2. 重送攻擊

本文提出之協議可預防重送攻擊，資源提供者重送使用者之交易資訊，意圖重複取得款項，將因為隨機值的存在而無法通過銀行端驗證。每個隨機值僅能取得款項一次，當資源提供者重送訊息S_2，銀行驗證時，將會比對出此訊息中之隨機值已經請款完成，而拒絕付款。

3. 中間人攻擊

在交易過程中，若有惡意人士進行中間人攻擊，接收使用者與資源提供者雙方的資訊，將無法取得每回合交易中使用之暫時金鑰。因為暫時金鑰使用雙方預先共享之對稱金鑰進行加密，惡意攻擊者無法解密訊息，且啟動交易後的訊息皆有使用金鑰加密訊息進行保護。因此，本方法可以預防中間人攻擊。

4. 效能評估

方法中，使用了對稱式金鑰加解密與非對稱式金鑰加解密保護傳輸中的資料，並使用數位簽章技術避免重要交易訊息遭到竄改。整個交易過程中，使用者對稱式金鑰加解密 11 次、非對稱式金鑰加解密 2 次與數位簽章 2 次。透過產生暫時金鑰與預先共享對稱金鑰，減少非對稱式金鑰加解密的次數，取得更好的效能。詳細加解密與數位簽章次數如表 3。

表 3 對稱、非對稱加解密與數位簽章使用次數

	對稱式金鑰加解密	非對稱式金鑰加解密	數位簽章
使用者	3	0	1
資源提供者	4	1	0
服務商	3	1	0
銀行	1	0	1

5. 結論

隨著科技發展，行動支付已經成為新興的付款方式。其中，行動支付適合共享經濟的交易活動，由使用者、資源提供者與服務商組成的新經濟，無論在何處都能進行共享經濟帶來的便利與加值服務。若在一個不安全的交易協議中運作，將會造成極大的安全風險，使用者或資源提供者的敏感資訊可能被第三人竊取，造成巨大的損失。因此，本文設計出一個安全且有效的交易協議，來保護共享經濟交易中的各方單位，由每回合產生的不同數值與數位簽章技術，減少資訊洩漏的風險。攻擊者也無法針對同筆交易進行重複請款，保障使用者的安全。

參考文獻

[1] Apple Pay. (2017). from: http://www.apple.com/apple-pay/

[2] Badra, M. and Badra, R. B., “A Lightweight Security Protocol for NFC-based Mobile Payments,” ***The 7th International Conference on Ambient Systems, Networks and Technologies***, Vol. 83, pp. 705-711, 2016.

[3] Belk, R., “You Are What You Can Access: Sharing and Collaborative Consumption Online,” ***International Journal of Business Research***, Vol. 67, No. 8, pp. 1595-1600, 2014.

[4] Botsman, R. and Rogers, R., ***What's Mine Is Yours: The Rise of Collaborative Consumption***, 1st ed., Harper Business, 2010.
[5] Cheng, M., "Sharing Economy: A Review and Agenda for Future Research," ***International Journal of Hospitality Management***, Vol. 57, pp. 60-70, 2016.
[6] Google Wallet. (2017). from: https://wallet.google.com/
[7] Jung, M.-S., "A Study on Electronic-Money Technology Using Near Field Communication," ***International Journal of Symmetry***, Vol. 7, No. 1, pp. 1-14, 2015.
[8] Kim, C., Mirusmonov, M. and Lee, I., "An Empirical Examination of Factors Influencing the Intention to Use Mobile Payment," ***International Journal of Computers in Human Behavior***, Vol. 26, No. 3, pp. 310-322, 2010.
[9] Luo, J.-N., Yang, M.-H. and Huang, S.-Y., "An Unlinkable Anonymous Payment Scheme Based on Near Field Communication," ***International Journal of Computers and Electrical Engineering***, Vol. 49, pp. 198-206, 2016.
[10] Ondrus, J. and Pigneur, Y., "An Assessment of NFC for Future Mobile Payment Systems," ***International Conference on the Management of Mobile Business***, 2007.
[11] Pourghomi, P., Saeed, M. Q. and Ghinea, G., "A Proposed NFC Payment Application," ***International Journal of Advanced Computer Science and Applications***, Vol. 4, No. 8, pp. 173-181, 2013.
[12] Wallsten, S., "The Competitive Effects of The Sharing Economy: How Is Uber Changing Taxis," Technology Policy Institute, 2015, from: https://www.ftc.gov/system/files/documents/public_comments/2015/06/01912-96334.pdf
[13] Wikipedia, Mobile Payment. (2017). from: https://en.wikipedia.org/wiki/Mobile_payment/