第 19 屆行動計算研討會

EMV-based mobile payment protocol for offline transaction – with the ability of mutual authentication

Jia-Ning Lou(羅嘉寧)
銘傳大學
deer@mail.mcu.edu.tw

Ming-Hour Yang(楊明豪)
中原大學
mhyang@cycu.edu.tw

Yu-Cheng Ho(何宇承)
中原大學
yucheng@wns.cycu.edu.tw

摘要

現行信用卡的標準 EMV 協定存在著下列的安全性問題: (1)僅由讀卡機單向認證卡片。(2)非接觸式的 EMV 感應卡在進行無線傳輸時的交易個人資料未經過加密，導致惡意使用者能夠利用這些訊息進行交易。(3)進行離線交易時，商店無法即時確認信用卡的有效性。惡意使用者可以利用上述問題進行詐騙。2013 年楊等人提出了一個改進 EMV 的協定以解決上述問題；但是在其方法中，雖對離線交易進行驗證，但卻無法解決在多次離線交易後所造成的額度擴張問題，而導致所使用的金額超過風險控管的範圍。為改善楊等人的方法，本論文提出了一個相容於 EMV 之交易安全機制來改善離線交易之安全性。協定中，在進行離線交易之前使用者需先向銀行申請一有限額度且可分割之離線交易授權，再將此授權之重要資訊儲存在手機之安全晶片內。透過此授權使用者可以在往後的每次交易前製作依據交易之金額將所獲得之額度分割成該次交易所需額度的離線憑證。每次進行離線交易時除了會交予商家購買商品所需金額之外亦會附帶該次交易額度之授權憑證以保證有效性。最後，商家請款的時候可將多次使用者所消費之金額合併請款，增加了商家使用上的便利性。本論文所提出之方法適用於多間商家消費的環境，且可有效解決多次離線消費導致之額度擴張問題，使得 EMV 交易更加安全與可靠。

關鍵詞：*NFC*、*EMV*、行動交易、風險控管、*Payword*。

Abstract

The standards for Europay, MasterCard and Visa (EMV) have been widely adopted by current major financial services corporations but there are certain security threats: (1) authentication is one-way only, i.e. from a reader to a card. (2) EMV-compatible contactless smartcards do not encrypt sensitive data in the mobile transactions, which allows attackers to steal the users' personal information. (3) During offline transactions, the merchants cannot verify whether a credit card has been revoked. In 2013, Yang proposed a protocol to enhance the security of EMV standards. Yang's method can perform mutual authentication between a point-of-sale (POS) and a credit card, but the users can exceed the credits after multiple offline transactions. To improve Yang's method, we propose a new offline transaction mechanism that is compatible with the EMV standards. In our scheme, a user is required to apply for a limited and divisible credits from a bank, and stores the credits into his NFC phone's security elements (SE). During an offline transaction, the user has to send his certificate and the specific amount of credits to the merchant. The merchant verifies user's certificate, collects the credits, and redeems the payments from the bank. Our protocol is suitable for the offline environment that accommodates multiple merchants; it prevents exceeding the limitation in multiple offline transactions; and it enhances the security of EMV standards.

Keywords: *NFC, EMV, Mobile Payment, Risk Management, Payword*

一、緒論

信用卡在今日已經成為重要的交易工具之一，因為信用卡在消費時所帶來的便利使得信用卡與生活擁有密不可分的關係。起初人們所使用的信用卡為磁條信用卡，但是磁條信用卡擁有信用卡資訊安全的問題：由於磁條信用卡所使用的架構會把信用卡的擁有者名稱、到期日期以及卡片號碼等等資料儲存在磁條上面，導致所有的資訊都容易被看見並且容易複製其內容 [2][3]，因此磁條信用卡擁有著相當高的風險被惡意的使用者或商家進行竊取並偽造信用卡的資料，也就造成了信用卡盜刷的案件。

為了克服磁條信用卡的安全疑慮，國際標準化組織及國際電工委員會共同規範了 ISO/IEC 7816 晶片智慧卡規格[4]，並且由三大國際組織 Euro Pay、MasterCard 以及 Visa 共同訂定了 EMV 晶片信用卡的標準[5]。晶片信用卡顧名思義就是使用智慧晶片(Integrated Circuit)的信用卡，智慧晶片擁有執行運算與儲存資料的能力；在使用晶片信用卡進行交易的時候，需將卡片插入專屬的智慧晶片讀卡機以進行交易的作業。晶片信用卡相較於磁條信用卡的好處在於：晶片信用卡除了擁有相較於磁條信用卡高的儲存空間與計算的能力之外，還擁有驗證卡片擁有者的機制，使用密碼取代擁有者的親筆簽名，並且晶片信用卡的密碼是儲存在智慧晶片之中不易被破解，所以經過加密之後對於被竊取資料以及偽造卡片變得不再容易。

但是晶片信用卡交易時所需要將卡片插入讀卡機的接觸方式較耗費時間，因此只要靠近讀卡機便可完成交易的非接觸式 NFC 感應信用卡技術漸漸被廣泛使用，MasterCard 和 Visa 兩大國際組織亦各有發表其非接觸式的感應信用卡，分別是 PayPass[6]以及 payWave [7]。將原本晶片信用卡須插入讀卡機才能交換訊息的接觸式變成用只要靠近感應即可交換訊息的非接觸式，操作起來更加便利與快速。NFC (Near Field Communication)是一個作用在行動設備上的近距離無線通訊技術，最早是由 Ecma 建立標準 (ECMA-340[8] 、ECMA-352[9])，再被接受於 ISO/IEC 訂定標準(ISO/IEC 18092[10]、ISO/IEC 21481[11])，並且 NFC 相容於標準 ISO/IEC 14443[12]非接觸式智慧卡的架構，其主要的目的是希望讓行動設備能夠以無線的傳輸方式近距離交換資料，為信用卡帶來更加便利的工作方式。NFC 技術將晶片信用卡之交易過程從須要將卡片插入讀卡機的接觸式改變為非接觸式的感應方式；在進行交易的時候，若使用非接觸式的 NFC 技術僅需要將 NFC 信用卡靠近讀卡機進行感應即可進行交易，不再需要將卡片交給服務人員請他插入讀卡機讀取信用卡的繁瑣動作才能進行交易。

利用 NFC 技術固有的卡片模擬功能，將 NFC 智慧型手機模擬成為可以使用的虛擬信用卡。首先需要思考的議題是將信用卡資訊安全的放入 NFC 智慧型手機內，因此便有學者提出方法將信用卡放進手機的安全空間內[13][14]，甚至 Google 和 Microsoft 亦提出將信用卡放進 NFC 智慧型手機的方法[15][16]，爾後便不斷有學者提出信用卡作用於 NFC 手機的架構[17][18][19][20][21][22]，試著讓信用卡放入 NFC 智慧型手機內來達到便利性。

在 NFC 智慧型手機內放置虛擬信用卡為人們的生活帶來了便利，在進行消費的時候不再需要帶好幾張晶片信用卡在身上，只要拿出有存放虛擬信用卡的 NFC 智慧型手機便可取代；也因為他為非接觸式的傳輸方式，消費起來更加快速與便利。但對於便利而言，安全成為了位於另一方面的拉鋸，NFC 的安全議題浮出檯面，學者們紛紛提出論文並分析 NFC 的安全性[23][24][25][26]，以下說明了幾項在上述論文中提出的安全性議題。

因為 NFC 為無線的傳輸方式，在發送訊息時 NFC 設備的附近都會收到此電磁波訊號，因此惡意使用者不需要很靠近也可以進行竊聽並拿到可用的訊息；而惡意使用者除了進行竊聽亦可以試著修改其內容，最簡單的情況下就是擾亂 NFC 所傳輸的訊息造成訊息損壞導致 NFC 讀卡機無法解讀所收到的訊息，造成阻斷式服務攻擊(Denial Of Service)；另外使用中間人攻擊讓通訊的雙方誤以為和對方正在通訊，但事實上每次通訊時都會先經過惡意使用者才會到另一方，惡意使用者可以收到所有交換的訊息並修改成自己想要的訊息，但這個攻擊方式對於 NFC 而言擁有一定的難度，因為 NFC 是很短距離的通訊方式，惡意使用者要使用此方法時必須非常靠近兩個設備(NFC 發送和接收訊息的設備)；除此之外，NFC 設備的系統安全亦必須非常重視，應用程式是在手機裡面執行，而手機就像一個設備簡化的小型電腦，亦可能感染到惡意的程式而讓惡意使用者達到竊取敏感資料等目的；最後是隱私的議題，因為每台 NFC 設備的識別編號都是唯一的並且被規定做不能修改，而此身份編號在傳輸時又是明文傳輸，因此 NFC 設備的使用者便暴露出來，所做的行為也因此可以被追蹤，比方說某個使用者在某個時段都會去買某個藥或者是在某個時段都會在哪搭乘大眾運輸工具等等。

上述所提到的安全性議題，皆為 NFC 在一般環境所使用時會遇到的，但是在使用 NFC 的時候有可能會是在較特殊的環境，例如想要在飛機上這個無網路的環境下使用擁有虛擬信用卡的 NFC 智慧型手機進行消費，便會有更多的安全性議題需要討論。因為在離線的交易環境下不能及時傳送訊息到後端的伺服器(銀行)進行認證或授權，也因此商店無法像線上交易一樣能夠及時向銀行確認此虛擬信用卡的可用性，例如此虛擬信用卡是否已失竊或已停用等等問題，惡意的使用者可以因此來進行詐騙而獲取不法利益[27]。EMV 在協定中提出了三項條件[5]來規定當離線交易遇到這些條件時必須強制性的進行線上交易，分別為超過累計的消費金額上限、連續離線消費的次數上限以及抽查機率隨交易金額成正比的「隨機交易選擇」。但是 EMV 規範裡所說明的離線風險控管機制沒有辦法避免若惡意的使用者將交易的金額控制在門檻以下，便無法強制進行線上交易因而詐騙得逞[28]；此外，因為虛擬信用卡儲存於手機中，若保管不當而連續消費的計數值遭到修改，那麼連續消費次數超過上限便會強制進行線上交易的機制會因此失效。

近期改善 EMV 協定的論文陸續出現。2003 年 Al-Meaither 和 Mitchell 提出了將 EMV 適用於阿拉伯的 Murabaha 交易[29]，將 EMV 的信用卡協定能使用於阿拉伯國家的環境裡。2008 年 Balfe 和 Paterson 提出了使用 TPM(Trusted Platform Module)[16]取代 EMV 的晶片來模擬 EMV 協定[30]，透過 TPM 可確保是否為合法使用者。2011 年 Ruiter 和 Poll 將 EMV 協定套用於他們所提出規格化的模組[31]，並且透過這個規格化的模組可使用第三方驗證工具進行正式的分析與驗證 EMV 的協定。2012 年 Ogundele 等人分析了 EMV 磁條卡的安全漏洞，並且分析在 EMV 卡片由磁條卡轉換成晶片卡的過渡期，晶片與磁條共同存在卡片上的安全性以及可能會遭遇到的攻擊與安全威脅[32]。2013 年 Chen 等人提出了對於 EMV 卡片金鑰產生機制的改善[33]，認為在 EMV 卡片裡的認證金鑰的產生方式可以套用於現有並且公開的安全機制，使得各家 EMV 卡片金鑰的產生方式簡單、一致並且擁有安全的保障。2014 年 Murdoch 和 Anderson 設計了數項證據的規範[34]，認為電子商務都可以套用於他們所提出的規範也因此可以看出電子商務的缺陷；尤其是 EMV 協定，他們甚至直接說出可能會遭遇到的危脅，並在後面提出改善 EMV 協定威脅的想法。Alhothaily 等人認為許多攻擊都是因為 EMV 協定裡的卡片擁有者驗證機制過於簡單甚至沒有進行擁有者的驗證，因此他們提出了讓使用者因為安全程度的需求而自行控制的多項條件驗證方式[35]，由此來解決卡片擁有者驗證方式過於簡單的問題。

楊等人在 2013 年提出了虛擬信用卡並且相容於 EMV 線上與離線交易的方法[36]，他們將原有的 EMV 協定以相容的方式加入了雙向認證，來解決因為只認證卡片而沒有認證讀卡機導致任何人都可以使用讀卡機來讀取卡片的問題，透過雙向認證可以確認雙方的合法性，以排除非法使用者盜取卡片資料的行為。並且在所有傳輸的訊息上使用共享金鑰進行加密，來解決由接觸式的讀卡方式轉變為非接觸式的感應方式所造成交易的重要訊息被暴露到空氣中，導致竊聽者可以輕易竊聽到重要的交易訊息，經過共享金鑰加密後縱使惡意使用者縱使竊聽到交易傳輸的訊息也沒辦法知道內容是什麼。以及關於離線交易的部分，在虛擬信用卡的環境下卡片會存在於手機之中，對於 EMV 所做的三項限制而言，若是保護不當使用者可以修改離線交易的累積次數計數器的值，來達成可以一直使用離線交易而不需要回到線上去做卡片合法性的認證；因此楊等人提出在離線交易前，由銀行發予一個短時間對於額度限制的離線憑證，讓使用者有能力可以進行離線的消費行為。

離線憑證需要在離線交易前和銀行進行申請，申請後表示自己擁有離線交易的權力，通過認證之後使得商家無法即時請求銀行驗證使用者合法性的離線交易變得擁有安全的保障。但楊等人所提出的離線憑證對於額度僅設定了限制[35]，無法解決在多次離線交易後所造成的額度擴張問題，而導致所使用的金額超過風險控管的範圍。其他許多研究亦想針對離線交易的部分增加其安全性，Blaze 等人提出將風險控管機制如消費金額上限、使用時間等限制加入倒使用者從發行者銀行獲得的憑證中來降低離線付款的風險[37]。Rivest 和 Shamir 提出交易前必須先向發行者銀行申請內含到期日以及信用額度的憑證，使用者在進行離線消費時會再產生不超過信用額度的 PayWord[36][38]。但這些方法都有著 double spending 的問題，所造可能造成的交易損失將無法控制。

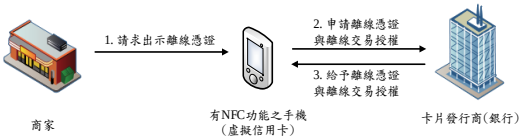
為改善楊等人的方法，我們提出了加強離線交易安全的新機制，透過此離線交易機制，使用者所使用的 NFC 手機端會依照規範所限制的金錢額度來依序使用並且商家可以在離線的狀態下及時驗證離線交易的合法性。我們提出的方法是利用 EMV 規範裡的保留欄位來放置我們所要增加的功能，使得方法相容於現有的 EMV 協定。在這新的機制裡，

要獲得離線交易的授權是需要向銀行索取，因此在離線交易之前使用者須先向銀行申請一個有線額度且可分割之交易授權。透過此授權使用者可以在往後的每次交易前製作根據交易之金額將所獲得之額度分割成該次交易所需額度的離線憑證。每次進行離線交易時亦會附帶該次交易額度之授權憑證以保證有效性。但是我們並不相信使用者手機的安全，因此我們將重要的交易資訊與認證金鑰接放在安全晶片之中，倘若手機造惡意程式攻擊亦無法獲取或修改重要的交易資訊。對於離線交易額度限制的部份我們使用 PayWord 的反向雜湊鏈來達成我們的需求，相較於 PayWord 環境我們所使用的是擁有安全晶片保護重要資訊的 NFC 手機環境，我們嚴格規範資料安全的驗證方法與認證手段，因此原 PayWord 所擁有的 double spending 問題也獲得防範。

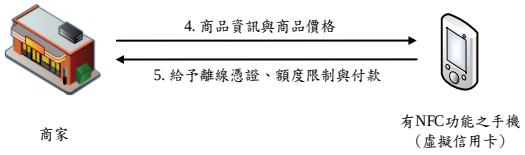
PayWord 擁有僅能使用於單一間商家的限制，並不符合我們在離線環境下會與多間不同商家交易的需求，因此，在眾多 PayWord 衍生於多間不同商家的論文裡，有研究於和多間不同商家交易為目的的 PayWord，我們將他歸類為可實現於多間商家的 PayWord。Esmaeeli 和 Shajari 提出可用於多商家的 PayWord[39]，在製作憑證與交易時需要一直回傳訊息給銀行去詢問可用性與合法性。這是屬於需要持續和銀行連線才能做的交易，但我們希望能在一開始發完憑證之後到最後商家要進行請款錢都不再和銀行進行溝通以達到離線的環境，我們的方法目的是要做離線的發行憑證並進行離線交易。Kim 等人提出一個可將 PayWord 直接分割給許多商家的協定[40]，他使用了兩個反向雜湊鏈在協定中，第一個雜湊鏈代表金額的 PayWord 分割，第二個雜湊鏈代表每間商家所對應的序號，但他的方法在註冊憑證階段使用者須向銀行索取離線憑證之外亦要拿到所有在雜湊鏈裡雜湊過後的雜湊值，用以代表未來交易時所給予商家的序號，因此傳輸量非常的大。Huszti 將每個 PayWord 的雜湊鏈個別給予一個商家，讓每間商家會獨自擁有一個 PayWord 的雜湊鏈來使用，並且 Huszti 認為在 PayWord 協定裡，商品訊息的資料嚴重不足，因此他將商品資訊放進交易的認證訊息內來增加交易的可靠性[41]。因為我們的環境是需要允許使用者在多間商家進行消費的離線環境，因此參考最接近我們環境可使用於多商家的 PayWord，以此來套用於我們在離線交易額度限制的製作之中。

二、協定流程

圖一為離線憑證申請階段(步驟 1-3)，圖二為交易階段(步驟 4-5)。(1) 商家會先向使用者的 NFC 手機請求出示離線憑證。(2)手機向發卡銀行申請離線交易時所需的離線憑證與離線交易授權。(3)發卡銀行製作離線憑證，並做出用於離線交易的分割憑證所需要的交易授權與額度限制，將之存放於手機端之安全晶片。(4)使用者購買產品時，手機端將顯示產品資訊及價格讓使用者做確認。(5)使用者確認無誤後，給予商家離線憑證與額度限制，並進行付款。商家在收到這些訊息之後，便可立即驗證此次離線交易的合法性，無須再向銀行提出驗證交易的請求。

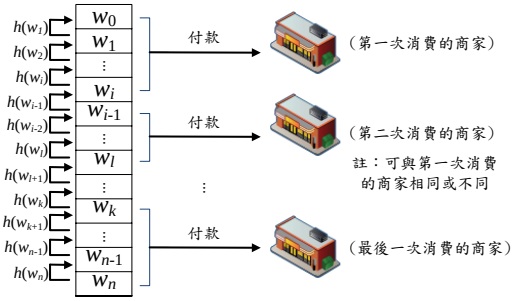


圖一：離線憑證申請階段示意圖



圖二：交易階段示意圖

我們所使用的是 PayWord 的反向雜湊鏈來做離線交易額度的限制，如圖三所示，此次申請的離線額度可以消費到 n 元。如果第一次消費時消費金額為 i 元，商家會拿到雜湊鏈的最後一項 w_0 與此次消費到的金額 w_i，商家可以馬上進行驗證 w_i 是否合法，以此類推最後消費到 n 元時便無法再進行消費。



圖三：簡易離線交易額度使用示意圖

三、結論

我們提出了 EMV 適用於多間商家消費的離線交易協定，利用 EMV 協定裡訊息所保留的欄位來放入我們所增加的功能，達成相容於現有的 EMV 協定。在每次離線交易時，將離線交易之授權進行分割，使得擁有可以使用此次交易之能力。對於離線交易所會限制之金錢

額度訂定了明確之使用方法與規則限制，有效解決多次離線消費導致之額度擴張問題；使用者須在規範下進行離線消費以及在離線狀態下之商家能夠及時確認使用者之消費是否合法，保障商家權益免於受到損害。

四、致謝

感謝指導老教授楊明豪老師與共同指導教授羅嘉寧老師，透過他們細心的教導之下，讓我對於學術研究的專業領域更加了解，並且明白經驗累積所產生的智慧是如此壯觀且令人崇拜。除了在學術上的研究討論之外，許多時間老師們亦會非常關心我們的生活起居，遇到有什麼困難亦會非常樂意地幫我們解決，真是很好的師長，在我心中充滿了感激之情。

參考文獻

[1] 楊明豪、羅嘉寧、洪聖翔，“相容 EMV 具雙向認證且適合離線及線上交易之行動付款協定”，碩士論文，中原大學資訊工程學研究所，2013。

[2] P. d. Bruyne, “New Technologies In Credit Card Authentication,” in *Proceedings of IEEE 1990 International Carnahan Conference on Security Technology: Crime Countermeasures*, 1990, pp.1–5.

[3] G. Masters, P. Turner, “Forensic data recovery and examination of magnetic swipe card cloning devices,” in *Proceedings of The 7th annual digital forensic research workshop(DFRWS)*, Vol.4, Supplement, 2007, pp.16–22.

[4] Identification cards -- Integrated circuit cards -- Part 1–Part 15, ISO/IEC 7816.

[5] EMVCo: EMV – Integrated Circuit Card Specifications for Payment System, Version 4.3 ed., EMVCo, LLC, 2011.

[6] MasterCard PayPass – ISO 14443 Implementation Specification Version 1.1, March 2006.

[7] Visa payWave – Visa Contactless Payment Specification(VCPS) Version 2.1, May 2009.

[8] ECMA INTERNATIONAL: Standard ECMA-340, Near Field Communication Interface and Protocol (NFCIP-1), 3rd edition, 2013.

[9] ECMA INTERNATIONAL: Standard ECMA-352, Standard ECMA-340, Near Field Communication Interface and Protocol -2 (NFCIP-2), 3rd edition, 2013.

[10] Information technology - Telecommunications and information exchange between systems - Near Field Communication Interface and Protocol -1 (NFCIP-1), First edition, ISO/IEC 18092:2013, 2013.

[11] Information technology - Telecommunications and information exchange between systems - Near Field Communication Interface and Protocol -2 (NFCIP-2), First edition, ISO/IEC 21481:2012, 2012.

[12] Identification cards -- Contactless integrated circuit cards -- Proximity cards -- Part 1–Part 4, ISO/IEC 14443.

[13] E.-J. Steffens, A. Nennker, Z. Ren, M. Yin, and L. Schneider, “The SIM-based mobile wallet,” in *Proceedings of The 13th International Conference on Intelligence in Next Generation Networks(ICIN)*, 2009, pp.1–6.

[14] H. C. Cheng, J. W. Chen, T. Y. Chi, and P. H. Chen, “A Generic Model for NFC-based Mobile Commerce,” in *Proceedings of The 11 International Conference on Advanced Communication Technology*, 2009, pp.2009–2014.

[15] Google Corp., Google Wallet [Online] Available: http://www.google.com/wallet/

[16] Microsoft Corp., “Trusted Platform Module(TPM) Virtual Smart Card Management Protocol Specification”, http://msdn.microsoft.com/en-us/library/hh880895(prot.20).aspx

[17] M. Pasquet, J. Reynaud, C. Rosenberger, “Secure Payment with NFC Mobile Phone in the SmartTouch Project,” in *Proceedings of International Symposium on Collaborative Technologies and Systems (CTS)*, 2008, pp.121–126.

[18] J. C. Paillès, C. Gaber, V. Alimi, and M. Pasquet, “Payment and Privacy: A Key for the Development of NFC Mobile,” in *Proceedings of 2010 International Symposium on Collaborative Technologies and Systems (CTS)*, 2010, pp.378–385.

[19] L. Mainetti, L. Patrono, and R. Vergallo, “IDA-Pay: an innovative micro-payment system based on NFC technology for Android mobile devices,” in *Proceedings of The 20th International Conference on Software, Telecommunications and Computer Networks (SoftCOM)*, 2012, pp.1–6.

[20] S. U. Rehman and J. Coughlan, “An Efficient Mobile Payment System Based on NFC Technology,” in *Proceedings of World Academy of Science, Engineering and Technology*, Vol.7, 2013.

[21] P. Urien and S. Piramuthu, “Securing NFC Mobile Services with Cloud of Secure Elements (CoSE),” in *Proceedings of The 5th International Conference on Mobile Computing, Applications and Services (MobiCASE)*, 2013, pp.322–331.

[22] P. Urien, “EMV-TLS, a Secure Payment Protocol For NFC Enabled Mobiles,” in *Proceedings of The 2014 International Conference on Collaboration Technologies and Systems (CTS)*, 2014, pp.203–210.

[23] E. Haselsteiner and K. Breitfuß, “Security in Near Field Communication (NFC),” in *Proceedings of the RFIDSec’06 on RFID Security*, 2006.

[24] G. Madlmayr, J. Langer, C. Kantner, and J. Scharinger, “NFC Devices: Security and Priva-

cy," in *Proceedings of the Third International Conference on Availability, Reliability and Security (ARES)*, 2008, pp.642–647.

[25] G. V. Damme, K. Wouters, and B. Preneel, "Practical Experiences with NFC Security on mobile Phones," in *Proceedings of the RFID-Sec'09 on RFID Security*, 2009.

[26] D. Nelson, M. Qiao, and A. Carpenter, "Security of the Near Field Communication Protocol: An Overview," Journal of Computing Sciences in Colleges, Vol.29, No.2, 2013, pp.94–104.

[27] M. Levi, P. Bissell, and T. Richardson, "The Prevention of Cheque and Credit Card Fraud," Crime Prevention Unit: Paper No. 26, London Home Office, 1991.

[28] M. Bond, O. Choudary, and S. J. Murdoch, "Chip and Skim: Cloning EMV Cards with the Pre-Play Attack," Computing Research Repository (CoRR), arXiv:1209.2531 [cs.CY], 2012.

[29] M. Al-Meaither and C. J. Mitchell, "Extending EMV to support Murabaha transactions", in *Proceedings of the 7th Nordic Workshop on Secure IT Systems*, 2003, pp.95–108.

[30] Shane Balfe Royal Holloway and Kenneth G. Paterson Royal Holloway, "e-EMV Emulating EMV for Internet Payments with Trusted Computing Technologies", in *Proceedings of the 3rd ACM workshop on Scalable trusted computing (STC)*, 2008.

[31] J. de Ruiter and E. Poll, "Formal Analysis of the EMV Protocol Suite," Theory of Security and Applications (TOSCA 2011) (March 2011), S. Moedersheim and C. Palamidessi, Eds., Vol.6693 of LNCS, Springer, pp.113–¬¬¬¬¬129.

[32] O. Ogundele, P. Zavarsky, R. Ruhl, and D. Lindskog, "Fraud Reduction on EMV Payment Cards by the Implementation of Stringent Security Features," International of Journal of Intelligent Computer Research (IJICR), Vol.3, No.1/2, 2012.

[33] C. Chen, S. Tang, and C. J. Mitchell, "Building General-Purpose Security Services on EMV Payment Cards", in *Proceedings of the 8th International Conference on Security and Privacy in Communication Networks*, 2012.

[34] S. J. Murdoch and R. Anderson, "Security Protocols and Evidence: Where Many Payment Systems Fail", in *Proceedings of the 8th International Conference on Financial Cryptography and Data Security*, 2014.

[35] A. Alhothaily, A. Alrawais, X. Cheng, and R. Bie, "Towards More Secure Cardholder Verification in Payment System", in *Proceedings of the 9th International Conference on Wireless Algorithms, Systems, and Applications (WASA)*, 2014, pp.356–367.

[36] M. Blaze, J.Ioannidis, A. D. Keromytis, "Offline Micropayments without Trusted Harware," in *Proceedings of the 5th International Conference on Financial Cryptography*, 2001, pp.21–40.

[37] R. Rivest, and A. Shamir, "PayWord and MicroMint: Two Simple Micropayment Schemes," in *Proceeding of Security Protocols Workshop on Security Protocols*, 1996, pp.69–81.

[38] F. Liu, "Secure Micropayment Mechanism for Universal Mobile Internet Service," [Online] Available http://ntur.lib.ntu.edu.tw/handle/246246/54231 [Accessed: 4 June 2013].

[39] A. Esmaeeli and M. Shajari, "MVPayword: Secure and Efficient Payword-Based Micropayment Scheme," in *Proceedings of the Second International Conference on the Web Technologies (ICADIWT)*, 2009.

[40] S. Kim and W. Lee, "A PayWord-Based Micropayment Protocol Supporting Multiple Payments," in *Proceedings of the 12th International Conference on Computer Communications and Networks (ICCCN)*, pp.609–612.

[41] A. Huszti , "Multi-Vendor PayWord with Payment Approval," in *Proceedings of the International Conference on Security and Management (SAM)*, 2013.