南　華　大　學

資 訊 管 理 學 系

碩士論文

最近幾個 NFC 研究系統的評論

Comments on Several Recent Secure NFC Studies

研 究 生：黃素卿

指導教授：周志賢 博士

中華民國 106 年 1 月 5 日

南 華 大 學

資訊管理學系碩士班

碩 士 學 位 論 文

最近幾個 NFC 研究系統的評論

Comments on Several Recent Secure NFC Studies

研究生：黃泰峻

經考試合格特此證明

口試委員：劉建人

周志賢

指導教授：周志賢

系主任(所長)：陳郁惠

口試日期：中華民國 106 年 1 月 5 日

南華大學碩士專班研究生

論文指導教授推薦函

資訊管理 系碩士專班 黃素卿 君所提之論文

Comments on Several Recent Secure NFC Studies 係由

本人指導撰述，同意提付審查。

指導教授 周志賢

106 年 1 月 7 日

南華大學資訊管理學系碩士論文著作財產權同意書

立書人：黃素卿 之碩士畢業論文

中文題目：最近幾個 NFC 研究系統的評論

英文題目：Comments on Several Recent Secure NFC Studies

指導教授：周志賢 博士

學生與指導老師就本篇論文內容及資料其著作財產權歸屬如下：

☑ 共同享有著作權

☐ 共同享有著作權，學生願「拋棄」著作財產權

☐ 學生獨自享有著作財產權

學　　生：黃素卿（請親自簽名）

指導老師：周志賢（請親自簽名）

中　華　民　國　106年　1　月　7　月

誌　　謝

過去的學分班及研究所共兩年半的學習生涯，即將告一段落了，這當中有苦有樂，情緒的曲折及波動，是我人生中的難忘的一段記憶。

首先，我要感謝指導教授周志賢老師循序漸進的教導，讓我從一知半解到對密碼學及資訊安全概念的知悉，從而更體驗到它的奧妙之處。

在口試過程中，也很感謝口試委員王昌彬老師及劉建人老師不吝指教，使得論文更臻完備；感謝促使我踏入這段學習的第一線推手，博文主任、瑞男老師及秀芬老師；感謝洪銘建教授這一路的鼓勵及關懷；感謝同窗的好友，大家的鼓勵是讓我支撐下去的力量；更感謝最愛的老公及小孩在這兩年半的時間裡，給予我最大的支持及體諒，促成我得以完成研究所的學業。

今後，我將秉持著「活到老學到老」的精神及「堅持不放棄」的理念，做為我人生精進的一個動力。

黃 素 卿 謹 誌 于

南 華 大 學 資 管 所

106 年 1 月 5 日

最近幾個 NFC 研究系統的評論

學生:黃素卿　　指導教授:周志賢博士

南 華 大 學　資訊管理學系碩士班

摘　要

NFC 技術在現實生活中具有廣泛的應用，例如電子付款、門禁卡、交通票等。雖然，它很容易安裝使用，且現在已變得流行，但它可能會有使用上的安全漏洞。本研究為了確保交易過程之資訊安全，探究如何運用 NFC 來做安全的電子交易。因此我們藉由閱讀了近期有關 NFC 安全問題的幾篇文獻，透過本研究將透過 Liao 等人所主張以智慧卡做身份認證的十個安全要求及採用 Mao 所著之*現代密碼學*一書中所提到的平行會議(parallel session)攻擊來探討文獻所提 NFC 身分認證與訊息交易系統的安全問題，我們發現其中幾篇之弱點，並分別提出其修正案。

關鍵字:NFC，智慧卡，密碼，安全元件，身份，認證，移動的

Comments on Several Recent Secure NFC Studies

Student: HUANG SU- CHIN Advisors: Dr. CHOU JUE-SAM

Department of Information Management
The Graduated Program
Nan-Hua University

ABSTRACT

The NFC technology has a wide applications in the real life such as, electronic payments, access cards, traffic tickets, and so on. Although, the NFC payment scheme is easy to install and use, and has become popular, it may incur usage risk. Hence, the security issue is particularly important. To ensure the correct transaction process, this study first reads several recent schemes relating to NFC security issues. Then, we explore the NFC security issues of these proposed protocols by way of examining the ten security requirements for a smart card on authentication system insisted in Liao et al's article and by checking the parallel session attack described in *Modern Cryptography* of Mao's book. After analysis, we found their the weaknesses and further proposed amendments to them, respectively.

Keywords: NFC, smart cart, password, security element(SE), ID,authentication, mobile

目　　錄

List of Figures

1.Introduction

NFC (Near Field Communication) is a short-range high-frequency wireless communication technology, which can let devices communicate through point-to-point non-contact data transmission. It also allows the devices to read Near Field Communication (NFC) tags that contain product information. The NFC technology has three operating modes:

(1) Card emulation mode: This model is actually the equivalence of an IC card using RFID technology, for instance, shopping malls credit card, access, control card, travel tickets, and so on. The card is powered by the RF field of the contactless card reader. Even if the user device (such as mobile phones) may exhaust its energy, the card in the phone can be powered by the reader. In an NFC device with card emulation-related applications, the NFC chip is usually equipped with a security element (SE).

(2) Peer-to-Peer Mode: In this mode, the data is exchanged with a shorter transmission distance and with a faster speedity, but with a lower power consumption. In this mode, multiple devices such as, digital cameras, PDAs, computers and mobile phones, can exchange data or services effectively.

(3) Reader/Writer mode: NFC acts as a contactless card reader to read the relevant information on the posters or the exhibition.

This study will explore several recent NFC secure protocols by way of checking the ten security requirements for a smart card on authentication system insisted in Liao et al's article [15] or by the parallel session attacks described in *Modern Cryptography* of Mao's book [19]. We found their weaknesses and further proposed amendments to them, respectively.

2. Review of several ascure schemes in the literature NFC

In this section, we review several studies about NFC security issue. For abbrevitation, we only depict them respectively and briefly.

(a)The design of secure mobile coupon mechanism with the implementation for NFC smartphones

(1) The original scheme

In the paper [8], they design and implement a secure mobile coupon for NFC smartphones to enhance the customer shopping experience. Not only the mobile coupon using mechanism but also the loyalty point earning mechanism are designed. In the protocol. Customers can collect loyalty points to redeem mobile coupons. Moreover, retailers can generate their loyalty points efficiently. Please refer to [8] for the details.

(2)Weakness

The announcement of promotion activity in the original scheme is shown in **Fig. 1**.

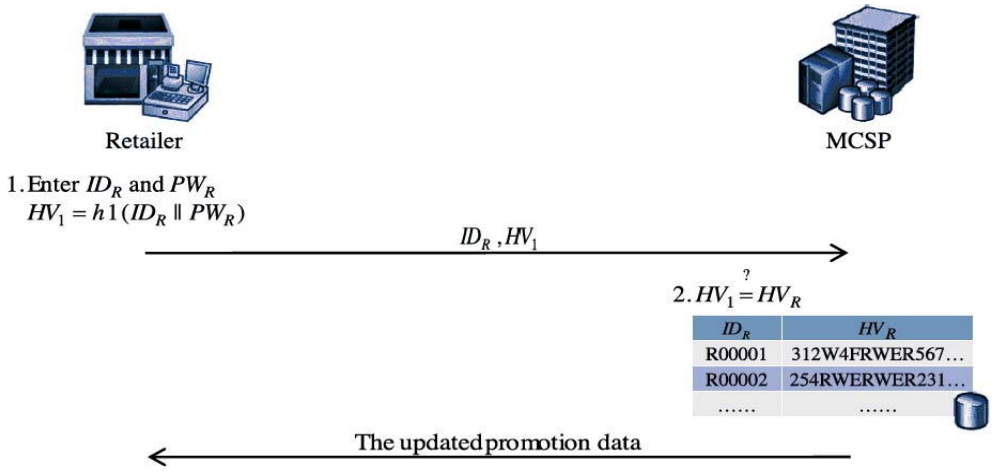


Fig. 1.The announcement of promotion activity.

In the figure, the retailer sends MCSP web site the credentials information ID_R and HV_1 without any timestamps or random numbers. This may result in that the attacker can launch a password guessing attack, because after the attacker M recording ID_R and HV_1, he can guess password as pw'_R and verify whether $HV_1 = h_1(ID_R \| pw'_R)$. If they are equal, his guessing is right. In addition, it also suffers replay attacks and violates one of the ten security requirements mentioned in [15] that no verifier table is stored in the server's storage.

(3)Modification

Retailer	MCSP
Enter ID_R and PW_R Selects a random r_R Computes $MN_R = r_R \oplus X_{MCSP-R}$ $MO_R = h(r_R \| h(r_R \oplus pw_R))$ $rPW = r_R \oplus h((pw_R \oplus r_R) \| T_1)$	
$\{ID_R, ID_{MCSP}, MN_R, MO_R, rPW, (T_1)\}$ →	
	Checks if $\| T_1 - T_C \| < \Delta T$ Computes $r_R' = MN_R \oplus X_{MCSP\_R}$ $h(pw_R \oplus r_R') \| T_1 = r_R' \oplus rpw$ $MO_R? = h(r_R' \| h(r_R' \oplus pw_R'))$ Selects a random r_m $MM = h(X_{MCSP-R} \| r_R') \oplus r_m$ $Q = h(r_m \oplus r_R)$
← The updated promotion data ,MM,Q	
$r_m' = MM \oplus h(X_{MCSP-R} \| r_R)$ $Q = ?h(r_R \oplus r_m')$	

Fig. 2. The modification of promotion activity announcement.

In the modification, we let both the retailer and the MCSP web site send the credential information with time stamp and random numbers to each other, so that the security requirements can be met. The password authentication table is therefore unnecessary to be stored on the server. We depict it in figure 2

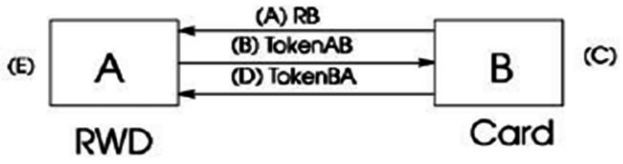
(4) Security analysis

In the modification, we let both the retailer and MCSP share a common secret X_{MCSP-R}, and each selects a random number when communicating at both sides. Hence, if M intercepts the communicating message, he obtains nothing other than the timestamp, both sides' identities and random numbers. Although he obtains the parameters, however, without the knowledge of X_{MCSP-R}, he has no way to calculate the randoms r_R or r_m. Therefore, the modified protocol is secure.

(b)Transport ticketing security and fraud controls

(1) The original scheme

The paper considers the technology problems of several electronic ticket solutions. Among them, it lists the approach ISO 9798-2 and states that MIFARE classic approximates to this method, but according to recent publications, it is vulnerable in four areas. For brevity, we only list the the figure fig.3 in [17]. As for the details, please refer to [17] .



The tokens are structured as follows:

TokenAB= $eK_{AB}(R_A \| R_B \| B \| Text2)$.
TokenBA= $eK_{AB}(R_B \| R_A \| Text4)$.

Fig. 3. Example ISO 9798-2 mutual authentication process.

(2) Weakness

Other than the four vulnerbilitres in the original paper, here we list an attack (as shown in Fig.4) on the scenario.

1).An attacker M pretends A which we denote M_A to communicate with B. After B sending him R_b , M now pretends B which we denote as M_B to send it to A.

2).A sends the message 3 to M_B, then M_A resend it to B as message 4.

3).After B sending out message 5 to M_A, M_B resends it to A as message 6.

From the above, we can easily see that M can attain his goal to fool both A and B by using the names of B and A, respectively.

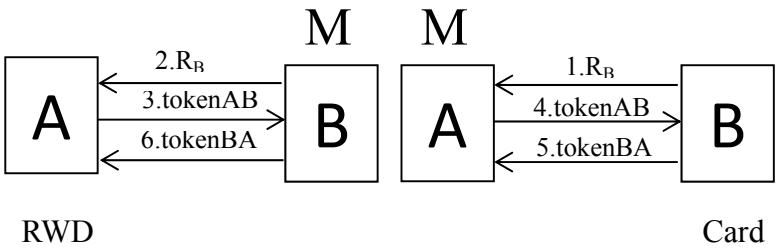
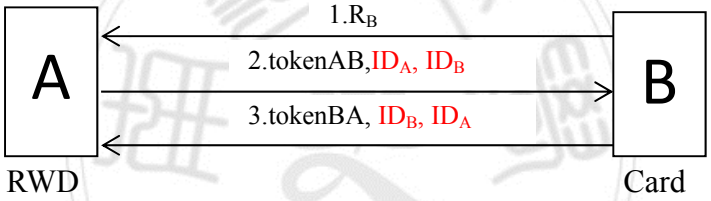


Fig. 4. The waknesses of ISO 9798-2 mutual authentication process.

(3) Modification

To remedy the weaknesses, we can simply add both side's identites to message 3 through 6 as shown in fig. 5.



$$\text{TokenAB}=eK_{AB}(R_A\|R_B\|ID_A\|ID_B\|Text2)$$

$$\text{TokenBA}=eK_{AB}(R_B\|R_A\|ID_B\|ID_A\|Text4)$$

Fig. 5. The modification of ISO 9798-2 mutual authentication process.

(4) Security analysis

If attacker M wants to launch an attack which we launched on the original scheme, he can succeed, because he can not successfully replace one of the identities with his own without A or B's awareness, so he can not fool A and B in the name of B and A. respectively.

(c).A privacy-preserving smart parking system using an IoT elliptic curve based security platform

(1) The original scheme

In the original scheme, they provides a generic ECC implementation on smart parking system that runs on different host operating systems, such as Contiki, TinyOS, iSenseOS, ScatterWeb and Arduino. Furthermore, it runs on smartphone platforms such as, Android and iPhone and also any possible linux based systems (e.g., raspberry Pi), allowing a single implementation to

run natively on heterogeneous networks. It can and protect a user's privacy by adapting the tool of zero knowledge proofs (ZKP). For abbreviation ,please refer to [6] for the details.

(2) Weakness

For that the equation $m=r+c \cdot x \pmod n$ is a Diophantine equation with GCD(1，c)=1, a set of solutions (r_0,x_a) can be found.

In fact, the general solution: $s=\{(r,x) \mid r= r_0-ck, x= x_0 +k，k\in z\}$. Therefore the secret x can be found.

Prover		Verifier
$G \in E/Fn$, $B \in E/Fn$		
radom r Fn $D= r^2 \cdot G$	D →	computes radom
	← c	c=HASH(G,B,D)
computes		
$m=r^2+c\ x \pmod n$	m →	checks
		$p=m \cdot G - c\ B$
		$=(r^2+c\ x) \cdot G - c\ B$
		$= r^2G + c\ x\ G - c\ x\ G$
		$= r^2G$
		$= D$

Fig. 6.the modified protocol of the original scheme

(3)Modification

From section 2, we see that the weaknesses results from the linear property of Diophantine equation. Therfore, we must break the linear property of Diophantine equation. We modify m to be $m=r^2+cx$ and let $D=r^2 \cdot G$.

(4) Security analysis

For that our modification now doesn't possess the linear property of Diophantine equation, we therefore patch the security hole in the original scheme.

(d).On-siteDriverID: A secure authentication scheme based on Spanish eID cards for vehicular ad hoc networks

(1) The original scheme

The original scheme is a security authentication method based on the Spanish eID smart card which is already in use and is applied to the VANET road authority. In the paper, they

proposed a security protocol that allows authorities to quickly obtain the driver's true identity in a VANET scenario. Please refer to [25] for the details. In the following, for brevity, we only list the figure of the original scheme in figure [7].

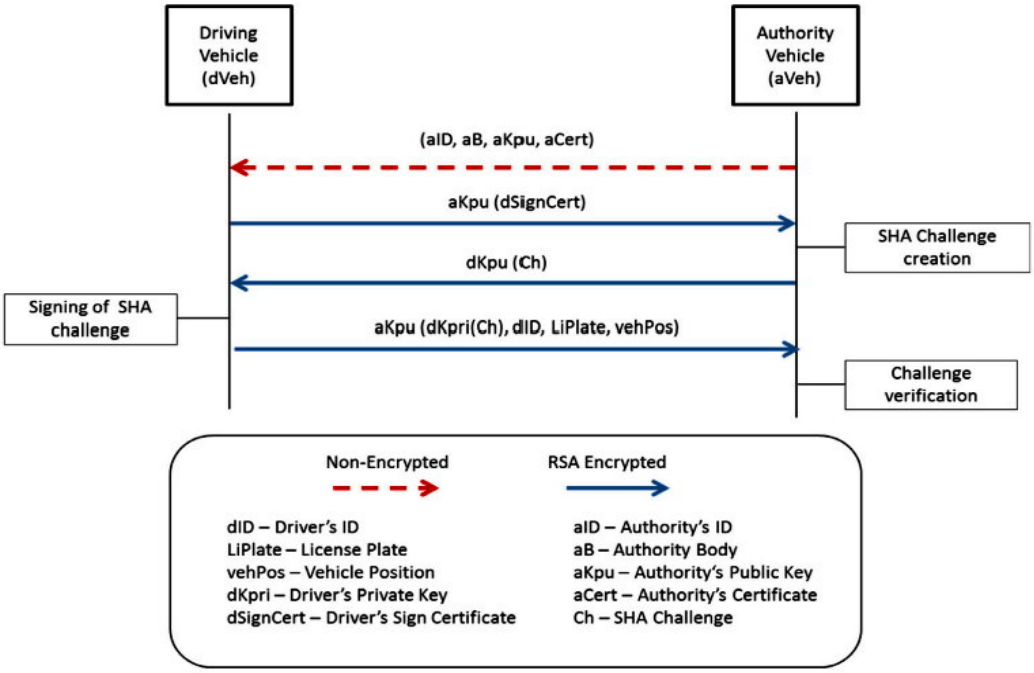


Fig. 7.Messages exchange for driver identification.

(2) Weakness

We now list the scheme's weaknesses by using Fig.8.

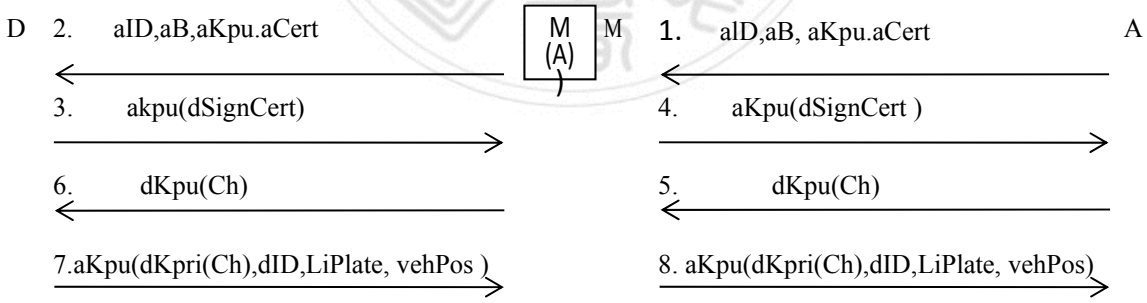


Fig. 8. The weakness of Messages exchange for driver identification.

1)M uses his real identity to communicate with A. Once A has sent message 1 to M, M pretends A to communicate with D by resending message 1 which is from A and now is message 2.

2)After receiving message 2 from M which now pretends A (which we denote M_A), D sends message 3 to M_A. M then responds to A with this message named message 4.

3)A sends message 5 to M and M_A sends it to D.

4)D sends message 7 to M_A, M then transfers this message to A.

From the above steps, we can easily see that M successfully fools D by using the name of A.

(3)Modification

To remedy the weaknesses, we can simply add both sides' identites to message 2 through 4.

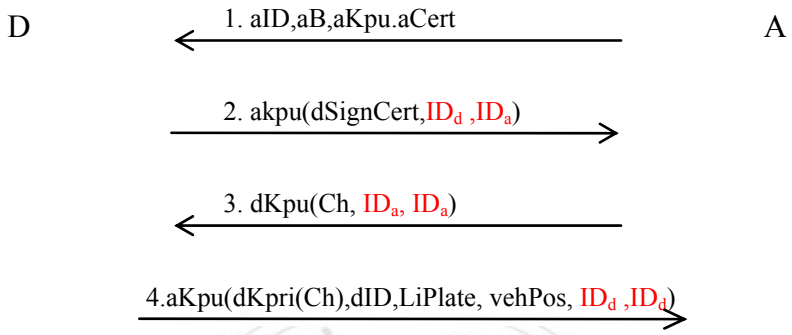


Fig. 9. The modification of Messages exchange for driver identification.

(4) Security analysis

If an attacker M launches the attack as described in the above section, he can not succeed. Because when M_A receives message 3 from D, he can not succeed in resending this as message 4 to A in the name of M successfuliy as shown in Fig.8. Since then, A will find out that this message is not sent from M. It's from D.

(e). Authentication in mobile cloud computing: A survey

(1) The original scheme

Mobile cloud computing (MCC) is the state-of-the-art mobile distributed computing model. In MCC, execution time and energy consumption are significantly improved by transferring execution of resource-intensive tasks such as image processing, 3D rendering, and voice recognition from the hosting mobile to the cloud-based resources. Under this situation, user authentication in MCC is hence a critical requirement in securing cloud-based computations and communications. For brevity, we only list the original scheme in Fig.10. For the details, please refer to [4] .

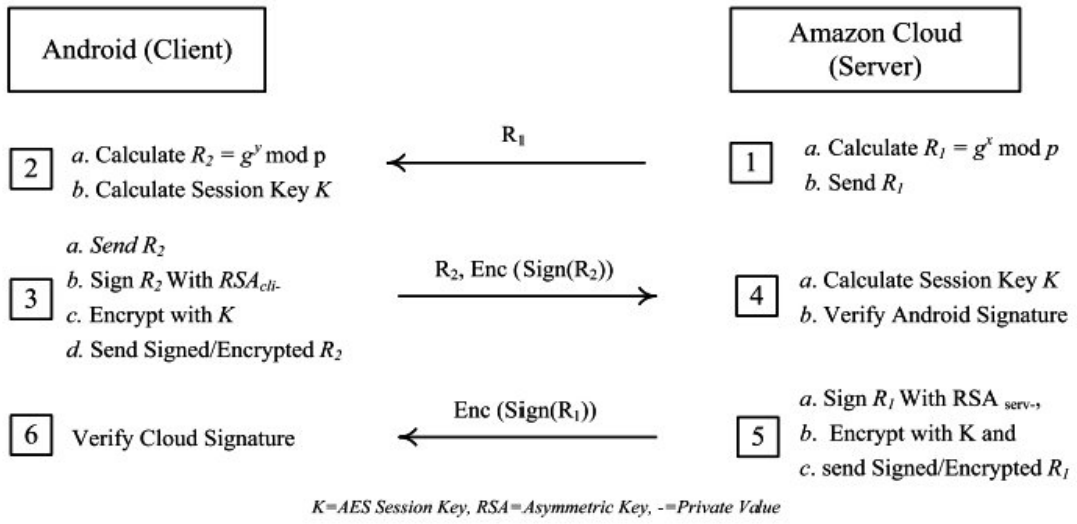


Fig. 10. Entity authentication protocol.

(2)Weakness

The weaknesses of this scheme is similar to that of scheme (d) [25]. We therefore omit the descriptions of both modification and security analysis sections by only show the weaknesses in Fig.11. and the modified protocol in Fig.12. for the corresponding section.As for the security analysis, it's also similar to that of scheme (d). We therefore omit it.

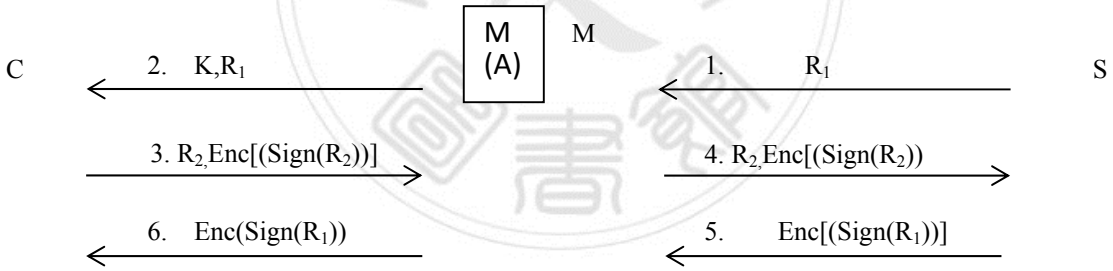


Fig. 11. The weaknesses of entity authentication protocol.

(3)Modification

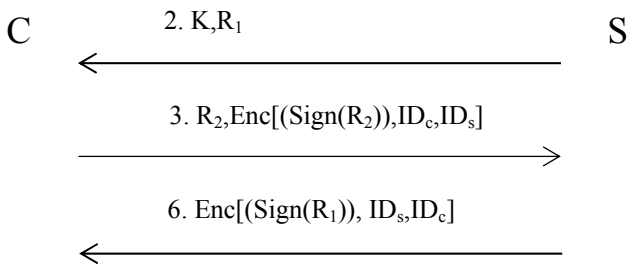


Fig. 12. The modification of entity authentication protocol.

(f).An unlinkable anonymous payment scheme based on near field communication

(1) The original scheme

In the proposed protocol, a user applies an anonymous virtual credit card from a trusted service manager. The sensitive information of the applied credit card is stored in the secure elements of user's mobile device. They claimed that their protocol can ensure various imperative security properties such as anonymity, unlinkability, and non-repudiation etc. Please refer to [16] for the details.

(2)Weakness

In the scheme, we found three problems. We list then below:

weakness 1: Charactters missing in step 3 section 2.5. We show it as follows.

> Step 3. The user encrypts the message and forwards the self-signed message $E(K_{TIDi,TSM}, SIGN(SK_{TID_i}, AID_i\ Nonce_1 || TID_i || P_{TID_i} || Nonce_2) || P_{TID_i} || Nonce_1)$ to TSM.

Weakness 2:The tangling usage of public key and private key in step 4 of section 2.5. We show it below.

> Step 4. The TSM issues a virtual credit card $TID_i\_CreditINFO$ that is protected by SK_{TID_i}, and a certificate $CERT^{TSM}_{TID_i}$. Last, $CERT^{TSM}_{TID_i}$ and $TID_i\_CreditINFO$ are stored into SE.

Besides, TSM must use the corresponding shared key $K_{TIDi,TSM}$ shared with user i, $1 \le i \le n$ to decrypt the self-signed message. This is too time consuming.

Weakness 3: Figure 3 is copied from Figure 1.

(3)Modification

In the following, we show the modifications for the respective weaknesses.

Weakness 1:

> **Step 3.** The user encrypts the message and forwards the self-signed message $E(K_{TIDi,TSM}, SIGN(SK_{TIDi}, AID_i || Nonce_1 || TID_i || PK_{TIDi} || Nonce_2) || PK_{TIDi} || Nonce_1)$ to TSM.

Weakness 2: the step 4 in section 2.5 should be protected by PK_{TIDIi} rather than SK_{TIDIi}.

3. Discussion

Near Field Communication (NFC), is a short-range high-frequency wireless communication technology that allows non-contact, peer-to-peer data transmission between electronic devices,and can operate fast and smoothly. With attractive properties, smart phones embedded with NFC become very popular. It brings mobile device users dynamic usage experience which lets users operate in a new interactive wireless way. At present, many researchers of NFC technology have gradually developed it with smart card (SC) to form the mobile payment scheme on the market. In the mobile payment life cycle, the data is from the mobile

device through the wireless network to reach the payment platform. Then, the payment instructions on the card are implemented to complete the payment action. We also can use the characteristics of ECC to design the efficient wireless payment transaction with same security level which needs more complex computation when using the other cryptosystems such as, RSA, Bilinear pairing and so on.

Due to that ECC cryptography key length is far more less than the other public key cryptosystems (such as RSA, Elgamal, Bilinear pairing), and thus is far more faster to process at same security level, when compared with the others. Thus, our for applications such as, smart cards, mobile phones, wireless memory devices, such as NFC limited resource environment.

4. conclusion

In this research, we reviewed several recent secure NFC systems, and demonstrated their weaknesses. Further,we proposed modifications, respectively. After security analyses, we comfirmed that the modified schemes are secure.

References

[1] Ahamad, Shaik Shakeel, Siba K. Udgata, and Madhusoodhnan Nair. "A *secure lightweight and scalable mobile payment framework.*" Proceedings of the International Conference on Frontiers of Intelligent Computing: Theory and Applications (FICTA) 2013. Springer International Publishing, (2014).

[2] Ahson, Syed A., and Mohammad Ilyas, eds. "*Near field communications handbook* ".CRC Press, (2011).

[3] Alexiou, Nikolaos, Stylianos Basagiannis, and Sophia Petridou. "*Formal security analysis of near field communication using model checking.*" Computers & Security 60 (2016): 1-14.

[4] Alizadeh, Mojtaba, et al. "*Authentication in mobile cloud computing: A survey.*" Journal of Network and Computer Applications 61 (2016): 59-80.

[5] Badra, Mohamad, and Rouba Borghol Badra. "*A Lightweight Security Protocol for NFC-based Mobile Payments.*" Procedia Computer Science 83 (2016): 705-711.

[6] Chatzigiannakis, Ioannis, Andrea Vitaletti, and Apostolos Pyrgelis. "*A privacy-preserving smart parking system using an IoT elliptic curve based security platform.*" *C*omputer Communications (2016).

[7] Chen, Hsing-Chung. "*A multi-issued tag key agreement with time constraint for homeland defense sub-department in NFC environment.*" Journal of Network and Computer Applications 38 (2014): 88-98.

[8] Chen, Yu-Yi, Meng-Lin Tsai, and Fong-Jia Chang. "T*he design of secure mobile coupon mechanism with the implementation for NFC smartphones*." Computers & Electrical Engineering (2016).

[9] Das, Raghu. "*NFC-enabled phones and contactless smart cards 2008–2018*." Card Technology Today 20.7 (2008): 11-13.

[10] Dierks T and Rescorla E. "*Transport Layer Security (TLS) Protocol Version"* 1.2.RFC 5246; (2008).

[11] Dragusha, Kushtrim. "*Center for Electronic Payments NFC Payment*." *International Stability*. Vol. 15. No. 1. (2013).

[12] Frisby W, Moench B, Recht B, and Ristenpart T. "*Security Analysis of Smartphone Point-of-Sale Systems*". USENIX Workshop on Offensive Technologies. 2012; p. 22-33.

[13] Grassie, Kai. "Easy handling and security make NFC a success." *Card Technology Today*" 19.10 (2007): 12-13.

[14] Jambusaria, Utsav, Neerja Katwala, and Dharmeshkumar Mistry. "*Secure Smartphone Unlocking Using NFC.*" Procedia Computer Science 45 (2015): 465-469.

[15] Liao, I-En, Cheng-Chi Lee, and Min-Shiang Hwang. "*A password authentication scheme over insecure networks.*" Journal of Computer and System Sciences 72.4 (2006):

727-740.

[16] León-Coca, Jose Maria, et al. "*Authentication systems using ID Cards over NFC links: the Spanish experience using DNIe*." Procedia Computer Sci*ence* 21 (2013): 91-98.

[17] Luo, Jia Ning, Ming Hour Yang, and Szu-Yin Huang. "*An Unlinkable Anonymous Payment Scheme based on near field communication.*" Computers & Electrical Engineering 49 (2016): 198-206.

[18] Mayes, Keith E., Konstantinos Markantonakis, and Gerhard Hancke. "*Transport ticketing security and fraud controls.*" information security technical report 14.2 (2009): 87-95.

[19] Mao, Wenbo. "*Modern cryptography*"*: t*heory and practice. Prentice Hall Professional Technical Reference, (2003).

[20] Ok, K., V. Coskun, and B. Ozdenizci, "*Near Field Communication:* From Theory to Practice", Istanbuh NFC Lab-lstanbul, ISIK University, (2012)

[21] Pacific, Asia. "*On-card fingerprint matching secures NFC payment sbiometric.*" Biometric Technology Today (2011): 2.

[22] Rawat, Danda B., ed. "*Security, Privacy, Trust, and Resource Management in Mobile and Wireless Communications*". IGI Global, (2013).

[23] Rizzardi, Alessandra, et al. "*AUPS: An Open Source AUthenticated Publish/Subscribe system for the Internet of Things.*" *Information Systems* (2016).

[24] Roland, Michael, "*Security Issues in Mobile NFC Device*", Springer International Publishing, (2015).

[25] Rosati T and G., Zaverucha G. "*Elliptic Curve Certificates and Signatures for NFC Signature Records*". Research In Motion, Certicom Research; (2013).

[26] Sabella, Robert P. et al., "*NFC For Dummies*", John Wiley & Sons, Inc., (2015).

[27] Sánchez-García, J., et al. "*On-siteDriverID: A secure authentication scheme based on Spanish eID cards for vehicular ad hoc networks.*" *Future Generation Computer Systems* 64 (2016): 50-60.

[28] Urien, Pascal, and Selwyn Piramuthu. "*Elliptic curve-based RFID/NFC authentication with temperature sensor input for relay attacks.*" *Decision Support Systems* 59 (2014): 28-36.

[29] Urien P. LLCPS: "*A new security framework based on TLS for NFC P2P applications in the Internet of Things*". IEEE Consumer Communications and Networking Conference; (2013). p. 845-846.