A New Third-party Payment Scheme with Anonymity for Mobile Commerce

Jen-Ho Yang[1], Pei-Yu Lin[2, 3]
[1] Department of Multimedia and M-Commerce, Kainan University, Taiwan
[2] Department of Information Communication, Yuan Ze University, Taiwan
[3] Innovation Center for Big Data and Digital Convergence, Yuan Ze University, Taiwan
jenhoyang@mail.knu.edu.tw, pylin@saturn.yzu.edu.tw

Abstract

The traditional commercial transactions have been replaced by mobile transactions in recent years. To increase the security of the mobile transactions, various third-party mobile payment schemes have been proposed. However, we find that the related works have heavy computation and communication costs for mobile devices. In addition, the related schemes have a large number of keys to be maintained and managed by the user, and thus it causes the key management problem and increases the transaction loads for mobile devices. To solve the above-mentioned problems, we propose a new third-party mobile payment scheme for mobile commerce in this paper. In the proposed scheme, we adopt the concept of the trusted service manager (TSM) to be a trusted third party between the mobile user and the merchant. The TSM concept provides the anonymity and unlinkability for mobile users so the user's payment privacy can be well protected. Besides, the computation and communication loads can be greatly reduced for the mobile devices. Therefore, the proposed scheme not only protects the mobile user's payment privacy but also decreases the computation loads for mobile devices. Compared with the related works, the proposed scheme is securer and more efficient for the third-party mobile payment in practice.

Keywords: Third-party payment, Trusted service manager, Mobile commerce, Anonymity, Near field communication payment

1 Introduction

The Trusted Service Manager (TSM) plays an important role for the mobile payment applications in recent years [1]. The TSM concept was firstly introduced by the Global System for Mobile Communications Association (GSMA) [1-2]. Briefly speaking, the key role of the TSM is a trusted third party between the mobile user and the merchant in mobile payment environments. The structure of the mobile payment environments with the TSM has the following roles: the user, the service provider (SP), the banks, and the TSM.

In this structure, the user has the mobile phone with a secure element (SE), which is the storage to save secure parameters and secret keys for the mobile payment. The SE can be an SIM card, an SD card, or an embedded chip, which is pre-deployed by the mobile network operator (MNO) to the mobile phone [3]. The user uses the mobile phone with SE to purchase services and goods from the SP (such as the merchant, the transport company, and the online shop) through the TSM. The payment process can be done by the Near Field Communication (NFC) payment [4] in the physical shop or on the Internet in the online shop. The banks include the issuing bank and the acquirer bank. The issuing bank issues the credit card to the user and manages the user's credit. After the mobile payment finished, the issuing bank transfer money to the SP's acquirer bank through the financial networks. The TSM-based mobile payment structure is shown in Figure 1.

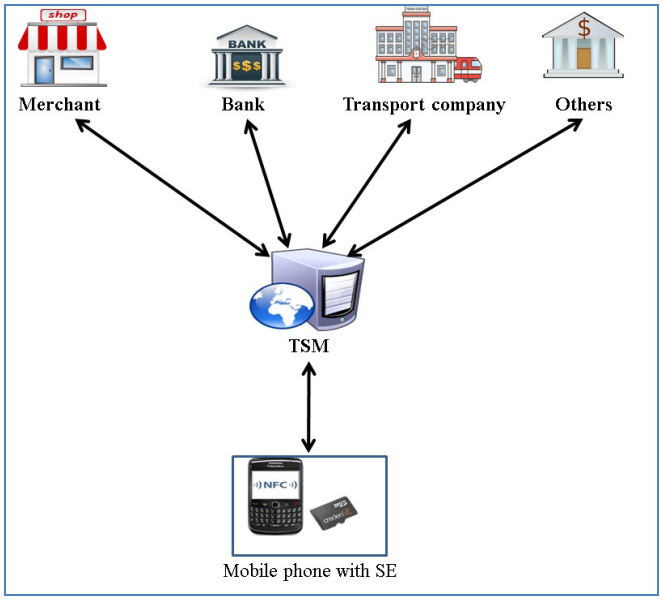

Figure 1. The third-party mobile payment based on TSM

*Corresponding Author: Pei-Yu Lin; E-mail: pylin@saturn.yzu.edu.tw
DOI: 10.3966/160792642018111906028

In the above-mentioned scenario, the TSM provides the major services as follows.

- Virtual currency issuing and management.
- Secure connection and key management for the user.
- Trusted third party between the user and the SP.
- Lifecycle management of the SP, the application, and the user.
- Security management and support for the mobile payment.

Due to the limited space of this article, we just show the major services of the TSM in the above list. The more detailed services of the TSM can be found in [1, 3]. According to the above description, the TSM plays an important role in the mobile payment nowadays. Therefore, various mobile payment schemes based on TSM have been proposed [5-8] in recent years.

In 2016, Luo et al. [9] proposed a NFC mobile payment scheme based on TSM. Their scheme provides unlinkable and anonymous securities for the mobile user, so that the user's payment privacy can be protected. However, we find that their scheme has some problems. First, their scheme use lots of public-key and secret-key en/decryptions to maintain the payment security. Thus, their scheme has heavy computation and communication loads. The mobile device cannot afford these heavy computation costs. Second, they only proposed the processes of the virtual bank account and virtual currency generations among the user, the bank, and the TSM. That is, they only finished the first half of the mobile payment process. Their article did not mention the important part that how the user pays the merchant using the virtual currency. Thus, their scheme is not a completed mobile payment scheme in practice. Third, their scheme separates the SE from the mobile phone. Thus, the SE and the phone have to communicate and exchange some parameters with each other. However, this separation setting is impractical in the real TSM-based mobile payment environments. According to the related TSM-based schemes [5-8], no research adopts this separation setting in practice because it increases the communication and communication costs. To solve the above-mention problems, we propose a new mobile payment scheme with anonymity based on the TSM in this paper.

In the proposed scheme, we use the lightweight computations to design the mobile payment process. Thus, the computation costs can be greatly reduced. In addition, the proposed scheme is a completed mobile payment scheme, which includes the virtual account generation, the paying process, and the real money transferring from the user's account to the merchant's account through the TSM. The proposed scheme provides a completed solution for the mobile payment in the TSM-based environments. Besides, we combine the mobile phone with SE to design our scheme. Therefore, the proposed scheme has less communication costs. Compared with Lu et al.'s scheme, the proposed scheme is more suitable and practical for the most design of the mobile payment applications in the real world. Besides, our scheme also provides the unlinkable and anonymity properties for the user payment privacy. According to the above descriptions, the proposed scheme is more efficient and securer than the related works for the TSM-based mobile payment environments.

2 Lu et al.'s Mobile Payment Scheme

In this section, we review Lu et al.'s scheme based on the TSM. Their scheme has three phases: the bank account generation phase, the anonymous transaction account generation phase, and the issuing virtual credit card phase. Table 1 shows the parameters used in their scheme.

Table 1. The parameters of Lu et al.'s scheme

B, U, SE	The bank, the user, and the secure element
ID_i	The identity of the entity i
AID_i	The anonymous identity of the entity i
TID_i	The transaction identity of the entity i
SID	The session identity
PK_i, SK_i	The public and private key of the entity i [10-11]
$CERT_i^B$	The certificate issued by the bank of the entity i
k_{xy}	The secret key pre-shared between the entities x and y
$Sig_{SK_i}(\cdot)$	The digital signature function signed by the entity i [10-11]
N_j	The nonce which is a random integer
TS	The timestamp
$\|\|$	The concatenation operation
$E_k(\cdot)$, $D_k(\cdot)$	The symmetric encryption and decryption functions with the key k [12]
$X\_Exptime$	The Expiry time of X's certificate
X_Limit	The credit limitation of the entities X
$Binfo$	The billing information
$TSMinfo$	The payment information for the TSM
$TSMBinfo$	The billing information generated by the TSM
$Authdata$	The authentication data information
$Status$	The status of an authentication data
$TID_i\_Creditinfo$	The credit card information for TID_i

The Bank Account Generation Phase:

Step 1. The user chooses N_1 to compute $E_{kBU}(Sig_{SK_U}(ID_U \| N_1))$. Then, the user sends ID_U and $E_{kBU}(Sig_{SK_U}(ID_U \| N_1))$ to the bank. After that, the bank generates N_2 and AID_i, and it sends ID_B and $E_{kBU}(ID_U \| AID_i \| N_2)$ back to the user.

Step 2. The user decrypts $E_{kBU}(ID_U \| AID_i \| N_2)$ to get AID_i and N_2, and he sends ID_U, AID_i and N_2 to the

SE. Then, the SE generates PK_{AID_i} and SK_{AID_i} to compute $a_1 = ID_U \| AID_i \| PK_{AID_i} \| N_2$. Then, the SE sends PK_{AID_i} and $Sig_{SK_{AID_i}}(a_1)$ to the user.

Step 3. The user sends ID_U and $E_{k_{BU}}(Sig_{SK_U}(ID_U \| AID_i \| Sig_{SK_{AID_i}}(a_1) \| N_2))$ to the bank. The bank generates $CERT^B_{AID_i}$ and a session key k_{AID_iB} to compute $a_2 = AID_i \| CERT^B_{AID_i} \| k_{AID_iB}$. Then, the bank sends ID_B, $E_{PK_{AID_i}}(AID_i \| AID_i\_Exptime \| AID_i\_Limit \| CERT^B_{AID_i})$, and $E_{k_{BU}}(a_2)$ to the user.

Step 4. The user sends ID_B and $E_{k_{BU}}(a_2)$ to the SE. Then, the SE decrypts $E_{k_{BU}}(a_2)$ to get $CERT^B_{AID_i}$ and k_{AID_iB}.

The Anonymous Transaction Account Generation Phase:

Step 1. The user generates TID_i, PK_{TID_i} and SK_{TID_i} to compute $Sig_{SK_{TID_i}}(TID_i \| PK_{TID_i} \| TS)$. Then, he sends ID_{TSM} and $E_{PK_{TSM}}(Sig_{SK_{TID_i}}(TID_i \| PK_{TID_i} \| TS))$ to the TSM. After that, the TSM generates k_{TID_iTSM} and sends TID_i and $E_{PK_{TID_i}}(TID_i \| k_{TID_iTSM})$ to the user.

Step 2. The user sends a request message to the SE, and then the SE computes $a_3 = SID \| AID_i \| ID_{TSM} \| ID_B \| N_3 \| AID_i\_Exptime \| AID_i\_Limit$. The SE generates $Binfo = Sig_{SK_{AID_i}}(E_{k_{AID_iB}}(a_3))$, and then it sends $Binfo$ and N_3 to the user.

Step 3. The user generates $TSMinfo = Sig_{SK_{TID_i}}(E_{k_{TID_iTSM}}(a_3))$. Then, he sends ID_{TSM} and $Sig_{SK_{TID_i}}(TID_i \| E_{k_{TID_iTSM}}(TID_i \| TSMinfo \| Binfo))$ to the TSM. After that, the TSM generates $TSMBinfo = Sig_{SK_{TSM}}(E_{PK_B}(SID \| AID_i \| N_4 \| AID_i\_Exptime \| AID_i\_Limit \| k_{TSMB}))$. Then, the TSM sends $E_{PK_B}(ID_B \| AID_i \| Binfo \| SID \| ID_{TSM} \| TSMBinfo)$ to the bank.

Step 4. The bank checks the correctness of $Binfo$ and $TSMBinfo$. If they are both authenticated, and then the bank sends $E_{K_{TSMB}}(AID_i \| Authdata \| N_4)$ to the TSM. After that, the TSM checks the credit of the user and sends TID_i and $E_{k_{TID_iTSM}}(Status \| TID_i\_Exptime \| TID_i\_Limit)$ to the user.

The Issuing Virtual Credit Card Phase:

Step 1. The user sends a request and TID_i to the TSM. Then, the TSM generates PK_{TID_i} and SK_{TID_i} for the TID_i.

Step 2. The user computes $E_{K_{TID_iTSM}}(Sig_{SK_{TID_i}}(AID_i \| N_4 \| TID_i \| PK_{TID_i} \| N_5))$ and sends it to the TSM.

Step 3. The TSM computes $E_{SK_{TID_i}}(TID_i\_Creditinfo \| CERT^B_{AID_i})$ and sends it to the user. Finally, the user stores $TID_i\_Creditinfo$ and $CERT^B_{AID_i}$ to the SE.

According to the above steps of Lu et al.'s scheme, we find that their scheme has the following drawbacks. First, they use too many public and private key pairs to design their scheme. In addition, the required steps and parameters are too complicated. Thus, their scheme has a large number of computation costs. Second, their scheme does not mention the user payment and the money transferring processes. That is, their scheme is not a completed mobile payment scheme. Third, their scheme separates the SE from the mobile phone, and thus the SE has to communicate with the mobile phone. This design increases the computation and communication loads, and no related works adopt this separation design. To solve the above problems, we proposed a new mobile payment scheme based on the TSM in the next section.

Table 2. The notations of the proposed scheme

U, B, AB, SP	The user, the user's bank, the acquiring bank, and the service provider
ID_i	The identity of the entity i
AID_i	The anonymous identity of the entity i
$h(\cdot)$	The secure one-way hash function [13]
x	The secret key of the TSM
$\|\|$	The concatenation operation
$h(ID_i \| x)$	The user i's secret key which is pre-stored in the SE by the TSM
$\oplus$	The exclusive-or operation
$k_{x,y}$	The secret key pre-shared between the entities x and y
N_i	The nonce which is a random integer generated by the entity i
TS_i	The timestamp generated by the entity i
$E_k(\cdot)$, $D_k(\cdot)$	The secret key encryption and decryption functions with the key k
$Credit_U$	The user's credit limitation in the bank
$UC\_Request$	The request message for the user's credit checking
$PInfo$	The payment information
$BInfo$	The bill information
$PSuccess$	The payment success message
$PInfo\_OK$	The message that the $PInfo$ is checked and agreed by the user

3 The Proposed Mobile Payment Scheme

The proposed mobile payment scheme has five roles involved: the user, the TSM, the user's bank, the acquiring bank, and the service provider. In the proposed scheme, the user has the mobile phone with

the SE, which is pre-embedded in the user's mobile phone by the MNO and the TSM. The SE can be an SIM card, an SD card, or an embedded chip. Besides, the service provider can be the transport company, online merchant, physical merchant, or other entities provide shopping services.

The proposed mobile payment scheme is divided into three phases: the anonymity account generation phase, the anonymity payment phase, and the money transferring phase. The notations of the proposed scheme are shown in Table 2.

The Anonymity Account Generation Phase:

Step 1. The user generates N_{U_1} to compute $A_{U_1} = h(ID_U \| x) \oplus N_{U_1}$. Then, the user sends ID_U, ID_B, A_{U_1}, and $h(N_{U_1} \| ID_U)$ to the TSM.

Step 2. The TSM uses its secret key x to compute $h(ID_U \| x)$ and $N'_{U_1} = A_{U_1} \oplus h(ID_U \| x)$, and then it checks if $h(N'_{U_1} \| ID_U)$ is equal to $h(N_{U_1} \| ID_U)$. If the equation holds, then the TSM generates AID_U and TS_1 to compute $C_1 = E_{k_{T,B}}(ID_U, AID_U, h(h(ID_U \| x), TS_1))$ and send *UC_Request*, ID_U, ID_T, and C_1 to the user's bank.

Step 3. The user's bank computes $D_{k_{T,B}}(C_1)$ and checks if TS_1 is in a valid time. If TS_1 is valid, then the bank generates $Credit_U$ and TS_2 to compute $C_2 = E_{k_{T,B}}(Credit_U, TS_2)$. Then, the bank sends ID_B and C_2 to the TSM.

Step 4. The TSM computes $D_{k_{T,B}}(C_2)$ and checks if TS_2 is in a valid time. If TS_2 is valid, then the TSM generates an anonymity account for AID_U. After that, the TSM generates N_{T_1} to compute $A_{T_1} = h(ID_U \| x) \oplus N_{T_1}$ and send AID_U, A_{T_1}, and $h(N_{T_1} \| AID_U)$ to the user.

Step 5. The user computes $N'_{T_1} = A_{T_1} \oplus h(ID_U \| x)$ and checks if $h(N'_{T_1} \| ID_U)$ is equal to $h(N_{T_1} \| ID_U)$. If the equation holds, then the user assures that his anonymity account is successfully established by the TSM.

The Anonymity Payment Phase:

Step 1. The user generates N_{U_2} to compute $A_{U_2} = h(ID_U \| x) \oplus N_{U_2}$. Then, the user sends AID_U, A_{U_2}, and $h(N_{U_2} \| AID_U)$ to the SP. Then, The SP generates the payment information *PInfo* and sends ID_{SP}, *PInfo*, AID_U, A_{U_2}, and $h(N_{U_2} \| AID_U)$ to the TSM.

Step 2. The TSM checks if *PInfo* is less than $Credit_U$. Then, the TSM computes $N'_{U_2} = A_{U_2} \oplus h(ID_U \| x)$ and checks if $h(N'_{U_2} \| AID_U)$ is equal to $h(N_{U_2} \| AID_U)$. If the equation holds, then the TSM generates N_{T_2} to compute $k_{U,T} = (N_{U_2} \| N_{T_2})$, $C_3 = E_{k_{U,T}}(PInfo, ID_{SP})$, and $A_{T_2} = h(ID_U \| x) \oplus N_{T_2}$. After that, the TSM sends A_{T_2}, $h(N_{T_2})$, and C_3 to the user.

Step 3. The user computes $N'_{T_2} = A_{T_2} \oplus h(ID_U \| x)$ and checks if $h(N'_{T_2})$ is equal to $h(N_{T_2})$. If the equation holds, then the user computes $k_{U,T}(N_{U_2} \| N_{T_2})$ to decrypt C_3 to get *PInfo* and ID_{SP}. And, the user checks the correctness of *PInfo* and ID_{SP} and generates the agreement message *PInfo_OK*. Then, the user computes $C_4 = E_{k_{U,T}}(PInfo, PInfo\_OK)$ and sends AID_U and C_4 to the TSM.

Step 4. The TSM computes $D_{k_{U,T}}(C_4)$ to check *PInfo_OK*. Then, the TSM generates *PSuccess* and N_{T_3} to compute $A_{T_3} = h(ID_U \| x) \oplus N_{T_3}$ and $A_{T_4} = h(N_{T_3} \| PInfo)$. After that, the TSM sends AID_U, ID_B, *PSuccess*, A_{T_3}, and A_{T_4} to the SP. Finally, the SP checks *PSuccess* to make sure that the payment is successful and approved by the TSM.

The Money Transferring Phase:

Step 1. The SP sends ID_{SP}, AID_U, ID_B, *PInfo*, A_{T_3}, and A_{T_4} to the its acquiring bank. Then, the acquiring bank sends ID_{AB}, AID_U, *PInfo*, A_{T_3}, and A_{T_4} to the user's bank.

Step 2. The user's bank computes $N'_{T_3} = A_{T_3} \oplus h(ID_U \| x)$ and checks if $h(N'_{T_3} \| PInfo)$ is equal to A_{T_4}. If they are equal, then the user's bank generates *BInfo* and sends it to the user. According to *BInfo*, the user's bank transfers the corresponding amount of money to the acquiring bank.

Unlike Lu et al.'s scheme only mentions the virtual account generation for mobile payment, the proposed scheme is a completed mobile payment scheme including mobile payment and money transferring phases. And, the steps of the anonymity account generation phase in the proposed scheme can totally accomplish the same goals of Lu et al.'s scheme. Thus, Lu et al.'s scheme is too complicated and impractical. Compared with Lu et al.'s scheme, the proposed scheme has less computation costs because it does not adopt any public-key en/decryption [10-11], which is a heavyweight computation for mobile devices. Also, the proposed scheme uses less secret-key en/decryptions [12] to accomplish our goals. Moreover, the proposed scheme provides the anonymity for mobile user so that the payment privacy can be well-protected. According to the above reasons, the proposed scheme is more efficient and practical than Lu et al.'s scheme.

4 The Security Discussions

In this section, we analyze the security of the proposed scheme by performing some possible attacks as follows.

The impersonating attack. Assume that an attack wants to impersonate a legal mobile user to ask the TSM to generate an anonymity account for him. Then, the attacker generates a forged secret key $h(ID_U \| x)''$ and N''_{U_1} to compute $A''_{U_1} = h(ID_U \| x)'' \oplus N''_{U_1}$. For pretending to be a legal user, the attacker sends ID_U, ID_B, A''_{U_1}, and $h(N''_{U_1} \| ID_U)$ to the TSM. However, this attack cannot work because the TSM will compute $N'_{U_1} = A''_{U_1} \oplus h(ID_U \| x)$. Then, the TSM will find that these messages are sent by the attacker because $h(N'_{U_1} \| ID_U)$ is not equal to $h(N''_{U_1} \| ID_U)$. Similarly, an attacker cannot impersonate the TSM because he does not know the secret value $h(ID_U \| x)$ shared between the user and the TSM. Therefore, the impersonating attack is infeasible for the proposed scheme.

The Man-in-the-middle Attack. Assume that an attacker intercepts the communication between the legal user and the TSM, and thus he can get ID_U, ID_B, A_{U_1}, and $h(N_{U_1} \| ID_U)$. Then, the attacker replaces ID_U with his identity ID_{ATT} and re-sends ID_{ATT}, ID_B, A_{U_1}, and $h(N_{U_1} \| ID_U)$ to the TSM. However, the TSM will find that the real messages have been altered because it can be verified by computing $N'_{U_1} = A_{U_1} \oplus h(ID_U \| x)$ and checking if $h(N'_{U_1} \| ID_{ATT})$ is equal to $h(N_{U_1} \| ID_U)$. Obviously, this attack cannot work because $h(N'_{U_1} \| ID_{ATT}) \neq h(N_{U_1} \| ID_U)$. Therefore, the proposed scheme can prevent the man-in-the-middle attack.

The Replay Attack. Assume that an attacker eavesdrops the communications between a legal mobile user and the SP in the anonymity payment phase, then he can get ID_U, ID_B, A_{U_1}, and $h(N_{U_1} \| ID_U)$. After that, the attacker re-sends ID_U, ID_B, A_{U_1}, and $h(N_{U_1} \| ID_U)$ to the SP, and he wants to pay his bill by using these pre-collected messages. However, this attack is impossible because the attacker does not know the secret value $h(ID_U \| x)$. Thus, the attacker cannot compute $N'_{T_2} = A_{T_2} \oplus h(ID_U \| x)$ to get the secret key $k_{U,T} = (N_{U_2} \| N_{T_2})$. Without knowing $k_{U,T}$, the attacker cannot finish the rest steps of the anonymity payment phase such as computing $C_4 = E_{k_{U,T}}(PInfo, PInfo\_OK)$. According to the above reason, the proposed scheme can prevent the replay attack.

The Performance Analysis. Table 3 shows that the computation costs of Lu et al.'s scheme and the proposed scheme. According to [13], the measurement of the above computation costs can be denoted as public-key encryption >> secret-key encryption >> Hash function, where "A >> B" means that the computation cost of A is much larger than that of B. In Table 3, we can see that the computation costs of the proposed scheme are much less than those of Lu et al.'s scheme.

Table 3. The comparison of the computation costs

	Public-key encryption	Secret-key encryption	Hash function
Lu et al.'s scheme	19	18	0
The proposed scheme	0	8	16

5 Conclusions

In this paper, we propose a new mobile payment scheme with anonymity based on the TSM. The proposed scheme has low computation costs because it only adopts the exclusive-or operations and secret-key encryptions, which are lightweight operations for mobile devices. Based on the TSM structure, the proposed scheme provides the benefits of fairness and convenience for the mobile user and the merchant. In addition, the proposed scheme uses the anonymous identity for the mobile user so that the payment privacy can be well-protected. Therefore, the proposed scheme is very efficient and secure for the mobile payment in practice.

Acknowledgements

This work was supported by Ministry of Science and Technology in Taiwan under the grants MOST 105-2410-H-424-005, MOST 106-2221-E-155-010 and MOST 106-2218-E-155 -007.

References

[1] Groupe Speciale Mobile Association, *White Paper: The Role of the Trusted Service Manager in Mobile Commerce*, http://www.gsma.com/digital-commerce/wp-content/uploads/2013/12/GSMA-TSM-White-Paper-FINAL-DEC-2013.pdf, 2013.

[2] Y. L. Jeng, T. C. Huang, Design of a Self-Learning Recommendation System with Integration of Personal Cloud Storage Technology, *Journal of Internet Technology*, Vol. 18, No. 7, pp. 1525-1532, December, 2017.

[3] C. Cox, *Trusted Service Manager: The Key to Accelerating Mobile Commerce*, https://www.firstdata.com/downloads/thought-leadership/fd_mobiletsm_whitepaper.pdf.

[4] N. Alexiou, S. Basagiannis, S. Petridou, Formal Security Analysis of Near Field Communication Using Model

Checking, *Computers and Security*, Vol. 60, pp. 1-14, July, 2016.

[5] C. Wang, H. F. Leung, A Private and Efficient Mobile Payment Protocol, *Computational Intelligence and Security*, Lecture Notes in Computer Science, Vol. 3802, pp. 1030-1035, December, 2005.

[6] J. H. Yang, C. C. Chang, An Efficient Payment Scheme by Using Electronic Bill of Lading, *International Journal of Innovative Computing, Information and Control*, Vol. 6, No. 4, pp. 1773-1779, April, 2010.

[7] J. T. Isaac, S. Zeadally, An Anonymous Secure Payment Protocol in a Payment Gateway Centric Model, *Procedia Computer Science*, Vol. 10, No. 2, pp. 758-765, August, 2012.

[8] M. D. Reuver, E. Verschuur, F. Nikayin, N. Cerpa, H. Bouwman, Collective Action for Mobile Payment Platforms: A Case Study on Collaboration Issues between Banks and Telecom Operators, *Electronic Commerce Research and Applications*, Vol. 14, No. 5, pp. 331-344, September, 2015.

[9] J. N. Luo, M. H. Yang, S. Y. Huang, An Unlinkable Anonymous Payment Scheme Based on Near Field Communication, *Computers and Electrical Engineering*, Vol. 49, pp. 198-206, January, 2016.

[10] R. L. Rivest, A. Shamir, L. Adleman, A Method for Obtaining Digital Signatures and Public Key Cryptosystems, *Communications of the ACM*, Vol. 21, No. 2, pp. 120-126, February, 1978.

[11] T. ElGamal, A Public Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms, *IEEE Transactions on Information Theory*, Vol. 31, No. 4, pp. 469-472, July, 1985.

[12] Advanced Encryption Standard, http://csrc.nist.gov/archieve/aes/.

[13] B. Schneier, *Applied Cryptography: Protocols, Algorithms*, and Source Code in C, 2nd ed., John Wiley & Sons, 1996.

Biographies

Jen-Ho Yang received the B.S. degree in computer science and information engineering from I-Shou University, Kaoshiung in 2002, and the Ph.D. degree in computer science and information engineering from National Chung Cheng University, Chiayi County in 2009. Since 2009, he has been an associate professor with the Department of Multimedia and Mobile Commerce in Kainan University, Taoyuan. His current research interests include electronic commerce, information security, cryptography, authentication for wireless environments, digital right management, and fast modular multiplication algorithm.

Pei-Yu Lin received the M.S. and Ph.D. degrees from National Chung Cheng University, Chiayi, Taiwan, in 2004 and 2009, respectively, both in computer science and information engineering. Currently, she is an Associate Professor with the Department of Information Communication, Yuan Ze University, Taoyuan, Taiwan. Her research interests include image protection, data mining, and information security.