The Secure Transaction Protocol in NFC Card Emulation Mode

Yi-Lun Chi[1,2], Iuon-Chang Lin[3,4], Cheng-Hao Chen[3], and Min-Shiang Hwang[1,5]
(Corresponding author: Iuon-Chang Lin)

Department of Computer Science and Information Engineering, Asia University[1]
500, Lioufeng Rd., Wufeng, Taichung 41354, Taiwan
Department of Marketing and Supply Chain Management, Overseas Chinese University[2]
100, Chiao Kwang Rd., Taichung 40721, Taiwan
Department of Management Information Systems, National Chung Hsing University[3]
250 Kuo-Kuang Rd., Taichung 402, Taiwan
(Email: corresponding_iclin@nchu.edu.tw)
Department of Photonics and Communication Engineering, Asia University[4]
500, Lioufeng Rd., Wufeng, Taichung 41354, Taiwan
Department of Medical Research, China Medical University Hospital, China Medical University[5]
(Received Feb. 15, 2015; revised and accepted Mar. 26 & Apr. 21, 2015)

Abstract

The NFC wallet is more popular in the world than before. Many people want to have a convenient payment in shopping, so the NFC wallet becomes an excellent choice for them. The NFC wallet uses the Card Emulation mode to achieve the transaction process. However, the Card Emulation mode does not have the specified secure transaction protocol. Our research provides a secure transaction protocol for the Card Emulation mode. It applies the Diffie-Hellman Key Exchange method and Elliptic Curve Cryptosystem to the protocol. It not only fulfills five secure requirements which are Data Confidentiality, Data Integrity, Unobservability, Unlinkability and Traceability, but also has the less calculation size and amount of transference than another proposed method. It is more suitable for mobile devices which do not have high calculation ability and storage space.

Keywords: Elliptic curve cryptosystem, NFC security, secure transaction protocol

1 Introduction

The mobile technology is more common than before, many people have smart phone or tablet for daily using. Near Field Communication (NFC) is a popular technology for payment which let users do not take their wallet out. It can establish a connected channel with touching. This behavior is simple and easy for use. The NFC transaction distance is in the 4 center meters. It is suitable for payment which reduces the risk of eavesdropping when transaction is being. The convenience make it been apply to many areas. Users usually use the NFC technology for transaction in the open environment [2]. Although every process is finished in few seconds, it still has many threats. Most importantly, the Peer-to-Peer mode has the secure protection protocol only, but the Card Emulation mode and Reader/Writer mode do not have any specified secure protocol in transaction. These two modes need mobile phone manufactures to design protection protocol when using mobile device in payment. Or users have to be careful for transaction object.

Our research considers it still have to take a secure protocol to protect private messages would not reveal when data exchanges. There are four international standards be introduced in next section. They are the base of NFC technology. In that part, our research describes the three operation modes for using in the NFC. We suppose the secure transaction protocol in the third partition. Our protocol uses the Diffie-Hellman Key Exchange method [7, 10, 11] and Elliptic Curve Cryptosystem [1] to build a key for exchanging the information between both sides. There is a comparison of our method and Hasoo et al. method [3] in Section 4. In addition, there is a security analysis about our protocol. In the conclusion, we provide some directions for research in future.

2 NFC Protocols and Operation Modes

The International Standard Organization (ISO) and International Electrotechnical Commission (IEC) have

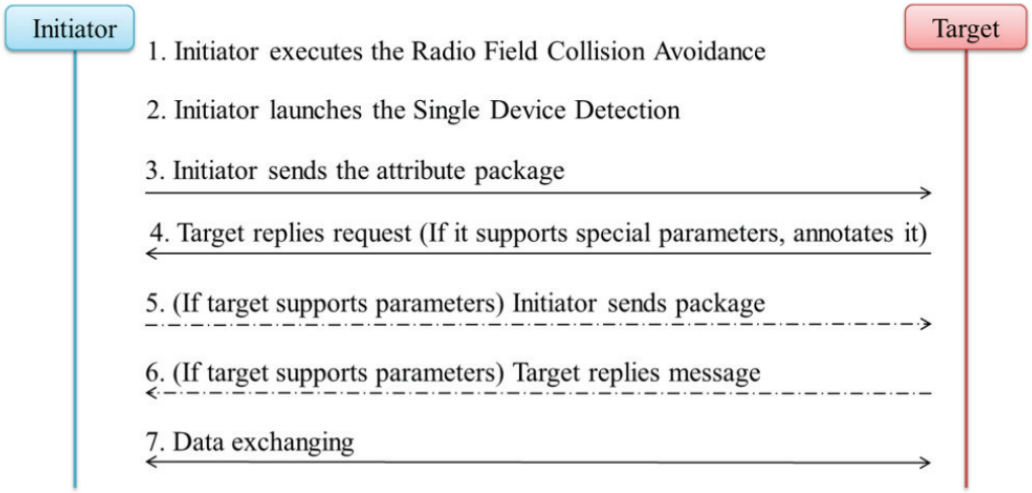

Figure 1: ISO/IEC 18092 passive communication mode

specified many standards for NFC communication. The ISO/IEC 18092 is the most important standard of NFC. The European Computer Manufacturers Association (ECMA) also defined the NFC security services and a protocol in ECMA International 385 standard and ECMA International 386 standard. In addition, NFC combines the smart card technology becomes a popular application. It makes mobile phone will be a tool which can pay the bill by NFC function. The detail specification has written in the ISO/IEC 14443 standard. In this section, here introduces the four international standards and three NFC operation modes.

2.1 ISO/IEC 18092 Standard

This standard defines the communication distance of NFC in the 4 centimeters. It make two devices can exchange data in short range. This feature elevates its security more for transaction. It also specified the two roles of objects which named "Initiator" and "Target" [4]. The initiator should launch a radio field for transaction at first and the target would get the radio waves from the initiator. If the target activates its radio field to communication with initiator, the mode names "Active Communication Mode", or it is called "Passive Communication Mode." The standard specified the NFC operating at center frequency is 13.56MHz. The transfer speeds are 106 kbit/s, 212 kbit/s and 424 kbit/s. The Figure 1 shows the detail procedure of initial process of Passive Communication Mode.

Step 1. When the initiator want to perform a transaction with target, it needs to execute the Radio Field Collision Avoidance (RFCA). It could detect there is existing the NFC radio field. If NFC field existed, this initiator should wait for other radio field disappeared after activates its radio field. If there are two radio fields operating in the same time, it may occur the data collision. If there is not, the initiator executes following steps.

Step 2. The initiator chooses the only one target for doing transaction. It decides the transfer speed and activates a radio field before using the Single Device Detection (SDD) to choose the target. For example, there are five targets in the area of radio field of initiator. The initiator should launch a polling request. The account of time slots is the data of the polling request. The time slot number is hexadecimal number which is '00', '01', '03', '07' or '0F' and it should be added 1. It means that the time slots number may be the one, two, four, eight or sixteen. As Figure 2, five targets have chosen the random number by themselves. When the delay time finished, they responds their numbers which match the number of time slots. If one slot has two responses of different targets that means there occurs a responding collision. According the rule, the initiator would decrypt the messages which sent by the target 1, target 2, target 4 and target 5. The initiator would find the target for transaction by their messages.

Step 3. The transaction target should be confirmed in Step 2. The initiator sends the attribute request to the target. Because it wants to know the ID of target and what transfer speed which target could support.

Step 4. Target would reply content of the request. If the target supports other special parameters or wants to adjust some current settings, it writes the requests down in the package. An instance is the target wants to enhance the transfer speed to higher rate, and it would write the need to the message and send to the target.

Step 5. If the initiator finds the target supports the special parameters by decrypting the message from the

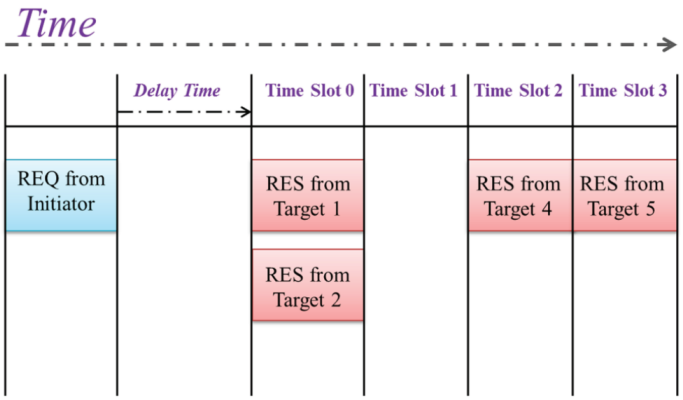

Figure 2: Single device detection method

target, it sends the request package to target. Or the initiator executes the Step 7 directly.

Step 6. The target receives the request and replies it. The content of package includes the adjusted items which the target wants. For example, the target wants to use higher speed for transaction that it should adjust the transfer rate from the 106 kbit/s to 212 kbit/s or 424 kbit/s.

Step 7. The initial process has finished that two sides would execute data exchanging procedure. Basically, all NFC transactions will do above steps before they start the data exchanging. However, if the target doesn't support the special parameters or does not want to change the current situation, it will not send the request to the initiator in the Step 4. So, the Step 5 and Step 6 are not must have be executed in every time.

2.2 ECMA International 385 and 386 Standards

The two international standards are specified by The European Computer Manufacturers Association (ECMA). They are used in the Peer-to-Peer mode of NFC operating mode. The two services of them which are shared secret service (SSE) and secure channel service (SCH) [8, 9]. The structure of ECMA international 385 standard describes the three layers as Figure 3. It divided to NFC-SEC User, NFC-SEC and NFC. When the user wants to contact to another one, its request would be written in the NFC-SEC-SDU (Service Data Unit). The NFC-SEC-SAP (Service Accessing Point) will invoke the communication service. And it combines the NFC-SEC-SDU with the NFC-SEC-PCI (Protocol Control Information) to the NFC-SEC-PDU (Protocol Data Unit). After the NFC-SEC-SAP contacts with the NFC-SAP (Service Accessing Point), it sends the NFC-SEC-PDU to the NFC-SAP. The NFC-SAP will send the communication request to another NFC-SAP for establishing a connection. This process makes them to coordinate the shared secret key to protect the privacy. It is called shared Secret service (SSE) and secure channel service (SCH). The implement method is described in the ECMA International 386 standard. The realized process is using the Elliptic Curve Cryptosystem and the Diffie-Hellman Key Exchange method to generate the secret key for transaction.

2.3 ISO/IEC 14443 Standard

It defines the transaction protocol which smart card communicates with card reader and specifies the 13.56MHz is the main radio frequency. It originally consists of two transmission technologies which are NFC-A and NFC-B. But the SONY Corporation wants to make their technology "FeliCa" been combined to this international standard, so SONY had written a draft and sent to related organization for judging. The International Standard Organization judged the draft is fail, because the specified content is similar the ISO/IEC 18092. However, the non-profit organization for promoting the NFC technology which named NFC Forum, it still make the three transmission technologies "ISO/IEC 14443A", "ISO/IEC 14443B", and "SONY FeliCa" to be named "NFC-A", "NFC-B" and "NFC-F". The mission of NFC Forum is formed to advance the NFC by developing related specifications and ensuring the interoperability among devices. The three technologies are divided by their encoded modes, Modulation Types and data rates. As the Figure 4, there is an initial process before exchanging data between two devices [5, 6]. Here introduces the detail about the procedures.

Step 1. The mobile phone which embedded the smart card or secure chip should touch the reader device.

Step 2. The smart card (It represents that mobile phone) waits for a wake-up command for executing following process for this transaction.

Step 3. Reader sends the wake-up commands to mobile phone.

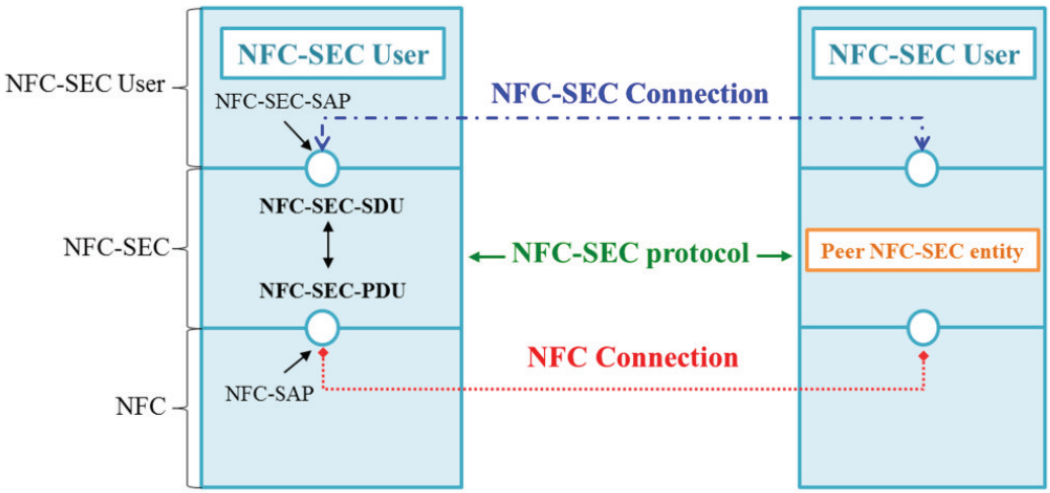

Figure 3: NFC-SEC architecture

Step 4. Smart card replies the request from the reader. If smart card supports some special parameters or like to change current settings, it should write requirements down in this message and send to reader.

Step 5. In order to avoid the data collision, the reader activates the anti-collision protocol. It would detect does there have other smart card in the radio field. If there only one smart card in the field, the reader executes the next step.

Step 6 & step 7. Because the target has confirmed, the reader sends the request to smart card for getting the unique ID of smart card. However, the unique ID had divided three parts by smart card. It is used to check the card's specification that conforms to the ISO/IEC 14443 standard. So they execute these two steps three times for getting complete ID and inspecting the specification of card is eligible.

Step 8. If the smart card annotated the special parameters in the message of step 4, the reader should send the attribute package to card. Otherwise, the Step 8 and Step 9 do not be executed.

Step 9. If card received the package from the reader, it fills in the information which it needs in this transaction and sends it back. The reader should adjust the current settings according by the message.

Step 10. If all situation is right, they start to exchange data.

3 The Secure Transaction Protocol in NFC Card Emulation Mode

In the card emulation mode, it does not have a transaction protocol which like the ECMA International 385 and ECMA International 386 standards. The transaction security of card emulation mode depends on the defense of software or hardware by the manufactures. We got the inspiration from those two standards. Our method uses the Diffie-Hellman Key Exchange method and Elliptic Curve Cryptosystem (ECC) in the card emulation mode. It describes our method as following.

Our method is established by Elliptic Curve Cryptosystem and Diffie-Hellman Key Exchange method. It helps two sides of transaction can obtain a same session key for transmission. They can use the key to encrypt their information when exchange secret data. If the key would not easily to be cracked, the transaction process should be more safety. First, the user's smart card and the NFC reader of store have to know their ID by each other. Then, they choose a huge prime number p. The elliptic curve $y^2 = x^3 + ax + b$ should in the finite field of Z_P. The $a,b \in Z_p$ and $a,b < p$. The a,b also should fulfill the condition which $4a^3 + 27b^2 \neq 0$. The elliptic curve which is $y^2 = x^3 + ax + b \bmod p$ can be used to encrypt and decrypt. The smart card and reader choose the base point from this curve which named G. It would be used to generate the public key. When all of above has done, it would execute the protocol. The notation follows Table 1.

As follow Figure 5 to Figure 8, it includes ten steps for executing the transaction in our protocol. It describes the steps detailed in this section. The Steps 1 and 2, there are in the Figure 5.

Step 1. The smart card generates a random number x , it uses the point multiplication with base point G for

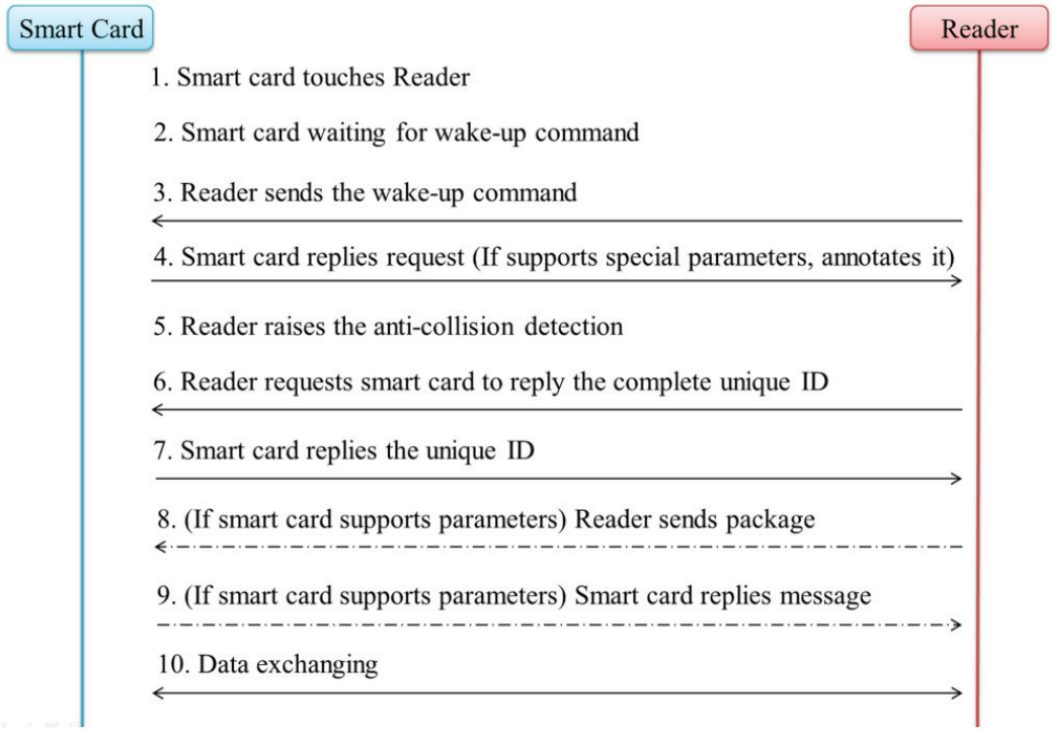

Figure 4: ISO/IEC 14443 communication mode

Table 1: Notations

Symbol	Description
x, y	Random numbers
Q_x, Q_y	Public keys
s	Secret number
K	Session key
fc	Function of AES in XCBC-PRF-128 mode
ID_x, ID_y	Random ID value
$MacTag_x$ $MacTag_y$	Key certificated tags
EL	Encrypted shopping list
l	Shopping list
TP_x, TP_y	Total price
P_t	Price table
TPA	Total price and APDU commands
$APDU$	Application protocol data unit
ER	Enrypted result
R	Result of executing
stc	Credit card's three secure codes
pK	Public key of bank
$phone$	User's phone number

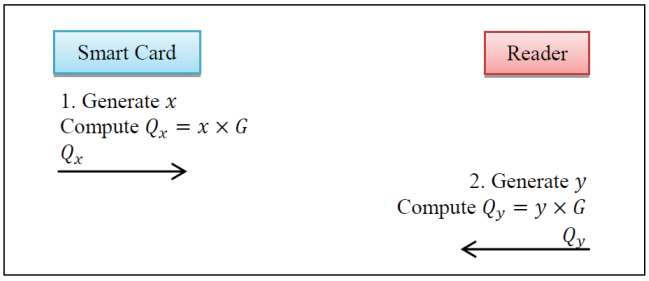

Figure 5: Exchange the key each other

generating the public key of card which is Qx. The card sends the key to reader.

Step 2. After the reader receives the message, it would make a random number which is y. Reader uses the same method to generate public key Qy and sends it to smart card.

Step 3. After card had received Qy from reader, it took the random number x and Qy to do point multiplication of elliptic curve. It got the point P of $y^2 = x^3 + ax + b \bmod p$ and set the value of x-way which named s. The smart card used the AES-XCBC-PRF-128 algorithm to encrypt (Qx,Qy,s), and got the key K. As the same time, the reader got Qx from smart card, it took Qx do the point multiplication by random number y. It can take the value s from the

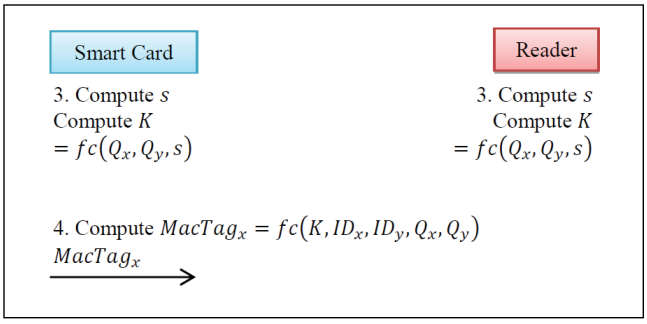

Figure 6: Generate the session key and certificated tag

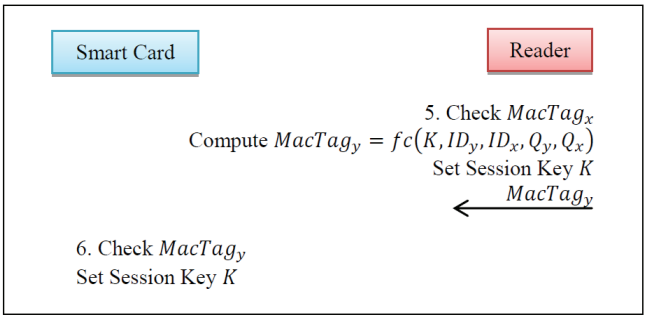

Figure 7: Set session key process

x-way which the point P of $y^2 = x^3 + ax + b \bmod p$. The reader device used the AES-XCBC-PRF-128 algorithm to encrypt (Qx,Qy,s), and would gain the same key K as smart card.

Step 4. The smart card encrypted five items which are session key K, two random identified value IDx and IDy, and two public keys Qx and Qy to the $MacTag_x$ by AES-XCBC-PRF-128 algorithm. It sent the tag to the card reader for checking the identity. The AES-XCBC-PRF-128 algorithm is a design on Cipher Block Chaining Message Authentication Code Calculation. This method would divide a data to many blocks. The 1 to $n-1$ blocks have same length. The length is uniquely 128 bits. The length of final block is in the 1 bit to 128 bits. If one user takes his data for encrypting by this algorithm, he can send the ciphertext to another user. That receiver would check the result which using own data to encrypt by the algorithm is identical or not. It could identify their data is totally same or not at all.

Step 5. When reader had received $MacTag_x$, it would identify the validity. If pass, card reader encrypted the key K, their identification IDy and IDx, their public keys Qx and Qy to the $MacTag_y$ by AES-XCBC-PRF-128 algorithm. The reader has known the key K which they own are same, and it set the key as the session key for this transaction. Reader sent the $MacTag_y$ to smart card.

Step 6. The card identified the content of $MacTag_y$. If correct, the smart card set the key K as the session key.

Step 7. The card used the session key K to encrypt user's shopping list and sent encrypted shopping list EL to card reader of store.

Step 8. After reader received the data, it decrypted the list by the session key K. It checked each items' price and calculated the total price of customer should pay as TP_y. Reader took the key K to encrypt the TP_y and the APDU commands became a data which was named TPA. It sent the TPA to smart card.

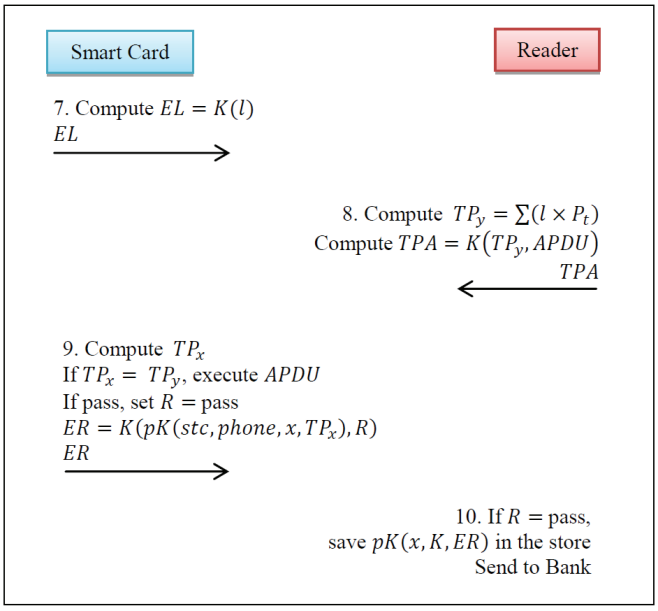

Figure 8: The process of message transportation

Step 9. Card calculated the total price first, it has named TP_x. If TP_x equals to TP_y, the smart card would execute APDU commands. If the process was smoothly and successfully, card created the result of executing which was named R. The content of R should be set pass. The smart card uses the bank's public key pK to encrypt the Credit card's three secure codes, user's phone number, random number x and TP_x. It took this data and R has been encrypted by key K. The card sent the encrypted result ER to reader.

Step 10. If checked result of R was pass, the reader would use bank's public key pK to encrypt the random number x, session key K and encrypted result ER. This ciphertext should be stored into database of the store. Finally, it would be sent to bank for follow-up process.

4 Performance and Security Analysis

4.1 Comparison with Hasoo et al.'s Method

Hasoo et al. has proposed a communication method on NFC card emulated mode [3]. It also used the ECMA International 385 Standard and ECMA International 386 Standard to build the procedure. However, the method of Hasoo et al. has described the process of transaction until two sides had agreed on session key K. It equals as our method of step 1 to 6. This article would take the data calculation and the amount of transmission for comparison with Hasoo et al. method. These two methods has been proposed secure method on Card Emulated Mode, therefore our comparison aim at smart card exclusive of the reader side. The result shown as Table 2.

Table 2: The comparison of two methods

Methods	Data Calculation	Amount of Transmission
Ours	2432 bits	592 bits
Hasoo et al.	1728 bits	480 bits

4.2 Security Analysis of Protocol

Our protocol not only has less calculation than Hasoo et al. method, but also satisfies five secure requirements of NFC transaction which proposed by Hasoo et al. Here, we would describe the five items as follows.

4.2.1 Data Confidentiality

"Data Confidentiality" means the data would not be accessed, traced or analyzed by unauthorized user. In our protocol, if a smart card wants to communicate with reader, and it would uses the Elliptic Curve Cryptosystem and Diffie-Hellman Key Exchange method to make a session key. If anyone likes to fake this key, he has to solve the discrete logarithm problem first. It is still a very difficult thing now. On the other hand, it can protect data would not be used by unauthorized user in our protocol.

4.2.2 Data Integrity

"Data Integrity" represents the data should keep its integrity when transmitting, and it would not be adjusted or edited by illegal one. As the ISO/IEC 18092 standard describes "Any device should activate the Radio Field Collision Avoidance (RFCA) and the Single Device Detection (SDD) before communicating with others." It promises the target would be only one until finish that process. In other words, there does not have third party could steal, adjust or edit the data before transaction completed. So our protocol satisfies this requirement.

4.2.3 Unobservability

"Unobservability" describes that any unauthorized user can not find the specified user's data by observing or analyzing. Our method proposes the smart card should take a random number be the base number of smart card's public key. When the transaction has finished, the key would be abandoned. If illegal man intruded the database of store, he could not observe the specified user's identification.

4.2.4 Unlinkability

"Unlinkability" is which two data had generated by same user, and it does not have any linkability between them. In our protocol, even a user has many times for shopping in same store, his transaction identification is different every time. Because the unique ID of smart card and the base number of user's public key were randomly selected out, it makes others can not find the relationship of every shopping record in the database of store.

4.2.5 Traceability

"Traceability" defines if there was a transaction problem occurred, it has a property for investigating the truth in the dispute between two sides. This character is usually held by a third party. Due to there has a data of transaction being stored in the store's database in our method, it would help to investigate the truth. The third party can decrypt the data and get the import items just like the user's phone number, the original random number which was the base of user's public key and final transaction result which had authorized by user. They would help to solve the problem.

5 Conclusions

Our research has found there is not a standardized secure transaction protocol for Card Emulation Mode, so this article uses the Diffie-Hellman Key Exchange method and Elliptic Curve Cryptosystem to build a secure communication protocol for the mode. It fulfills five secure transaction requirements which are unobservability, data integrity, data confidentiality, unlinkability, and traceability. And the data calculation and the amount of transmission are better than Hasoo et al. method. Hence, our protocol has nice performance in security and calculation.

References

[1] S. Basu, "A new parallel window-based implementation of the elliptic curve point multiplication in multi-core architectures," *International Journal of Network Security*, vol. 14, no. 2, pp. 101–108, 2012.

[2] A. K. Das, "Improving identity-based random key establishment scheme for large-scale hierarchical wireless sensor networks," *International Journal of Network Security*, vol. 14, no. 1, pp. 1–21, 2012.
[3] E. Hasoo, "Conditional privacy preserving security protocol for nfc applications," *Proc. 2013 IEEE Int. Conf. On Consumer Electronics*, 2013.
[4] ISO/IEC 18092:2013, *Information Technology - Telecommunications and Information Exchange between Systems - Near Field Communication - Interface and Protocol (NFCIP-1),* ISO/IEC 18092:2013.
[5] ISO/IEC FCD 14443-3, *Identification Cards - Contactless Integrated Circuit(s) Cards - Proximity Cards - Part 3: Initialization and Anti-collision,* ISO/IEC FCD 14443-3 (Revision).
[6] ISO/IEC FCD 14443-4, *Identification Cards - Contactless Integrated Circuit(s) Cards - Proximity Cards - Part 4: Transmission Protocol,* ISO/IEC FCD 14443-4 (Revision).
[7] J. Liu and J. Li, "A better improvement on the integrated Diffie-Hellman-DSA key agreement protocol," *International Journal of Network Security*, vol. 11, no. 2, pp. 114–117, 2010.
[8] Standards ECMA 385 NFC-SEC, *NFCIP-1 Security Services and Protocol,* Standards ECMA 385 NFC-SEC.
[9] Standards ECMA 386 NFC-SEC-01, *NFC-Sec Cryptography Standard Using ECDH and AES,* Standards ECMA 386 NFC-SEC-01.
[10] S. Wu and Y. Zhu, "Proof of forward security for password-based authenticated key exchange," *International Journal of Network Security*, vol. 7, no. 3, pp. 335–341, 2008.
[11] Z. Yong, Ma Jianfeng, and S. Moon, "An improvement on a three-party password-based key exchange protocol using weil pairing," *International Journal of Network Security*, vol. 11, no. 1, pp. 14–19, 2010.

Yi-Lun Chi received her M.S. degrees in Management of Information Systems and Technology from School of Information Systems and Technology, Claremont Graduate University, USA in 2006 and in Computer Science from University of Southern California in 1997. She is currently being an instructor at Overseas Chinese University and pursuing the Ph.D. degree in the department of Computer Science and Information engineering at Asia University. Her research interests include electronic commerce, internet marketing, data mining, and knowledge management.

Iuon-Chang Lin received the Ph.D. in Computer Science and Information Engineering in March 2004 from National Chung Cheng University, Chiayi, Taiwan. He is currently a professor of the Department of Management Information Systems, National Chung Hsing University, Taichung, Taiwan. His current research interests include electronic commerce, information security, RFID Information Systems, and cloud computing.

Cheng-Hao Chen received the M.S. in Management Information Systems from Chung Hsing University, Taiwan, in 2014; His current research interests include mobile agent, information security, and cryptography.

Min-Shiang Hwang received the B.S. in Electronic Engineering from National Taipei Institute of Technology, Taipei, Taiwan, Republic of China, in 1980; the M.S. in Industrial Engineering from National Tsing Hua University, Taiwan, in 1988; and the Ph.D. in Computer and Information Science from National Chiao Tung University, Taiwan, in 1995. He also studied Applied Mathematics at National Cheng Kung University, Taiwan, from 1984-1986. Dr. Hwang passed the National Higher Examination in field "Electronic Engineer" in 1988. He also passed the National Telecommunication Special Examination in field "Information Engineering", qualified as advanced technician the first class in 1990. From 1988 to 1991, he was the leader of the Computer Center at Telecommunication Laboratories (TL), Ministry of Transportation and Communications, ROC. He was also a project leader for research in computer security at TL in July 1990. He obtained the 1997, 1998, and 1999 Distinguished Research Awards of the National Science Council of the Republic of China. He is a member of IEEE, ACM, and Chinese Information Security Association. His current research interests include database and data security, cryptography, image compression, and mobile communications.