Symmetry **2015**, *7*, 1-14; doi:10.3390/sym7010001

OPEN ACCESS

symmetry

ISSN 2073-8994

www.mdpi.com/journal/symmetry

Article

A Study on Electronic-Money Technology Using Near Field Communication

Min Soo Jung

Department of Computer Engineering, Kyungnam University, 7 Kyungnamdaehak-ro,
Masanhappo-gu, Changwon-si 631-701, Korea; E-Mail: msjung@kyungnam.ac.kr;
Tel.: +82-55-249-2217; Fax: +82-55-248-2554

Academic Editors: Young-Sik Jeong, Laurence T. Yang, Stefanos Gritzalis

Received: 11 August 2014 / Accepted: 4 December 2014 / Published: 26 December 2014

Abstract: Recently, due to the introduction of NFC (Near Field Communication), it has become possible to make easy electronic payments. Therefore, a secure communication method is necessary in these environments. NFC can be said to be relatively safe compared to other communication methods, because it carries out communications within 10 cm. However, it has made possible the risk of impersonation attacks by a disguised reader, leaving user information on the reader. In order to solve these problems, in this paper, we propose an authentication scheme that can reduce the weight of computation by using only a hash function and XOR (eXclusive OR) operation algorithms. This paper also shows that our method is safe, since it leaves no information with the other party.

Keywords: NFC; key agreement; mobile payment

1. Introduction

Nowadays, due to the prevalence of smartphones, many people can share information and process finance payments anytime and anywhere [1–3]. Even though this information sharing can be performed by communication with a server in the network, it can also be done through the communication between devices. Furthermore, this payment environment has developed with the mobile as the center, and the method of using SMS (Short Message Service) of mobile core features has also been introduced. However, this, because of the inconvenience of the payment process, is gradually disappearing. In recent years, due to prevalence of Near Field Communication (NFC) equipped smart phones, a variety of information can be obtained more easily [4–6]. NFC is a kind of RFID system. It means that NFC is a kind of TAG to Reader system. NFC carries out *near* communication within 10 cm at a band of 13.56 MHz. By adopting NFC on smartphones, we can make various electronic payments safe because of the short distance of communication. Moreover, this short distance between TAG and Reader implies the user's intention. However, in the NFC environment, security vulnerabilities have been found: illegal reproduction of TAG and acquisition of illegal information by a disguised reader. In order to solve these problems, a recent NFC forum presented the NFC Security Standard.

NFC-SEC as NFC-related security standards have been published 2010 [7–9]. The standards present a way to perform key-agreement processes by using an elliptic curve algorithm [8]. This method is also a public key-based encryption algorithm. The NFC supports functions like "TAG to Mobile", and "Mobile to Mobile". With these functions, NFC can trade or transfer freely large amounts of data and content [10]. NFC provides more a convenient environment of finance payments for the user. Especially, the electronic wallet is highly activated. It must provide a safe communication in this environment [6]. However, important data can be easily exposed to a malicious user [10]. In earlier papers, to solve the above problems, they presented several methods to perform the authentication by using a public key based encryption. They also proposed solutions to perform the key agreement by using a secret key-based encryption scheme. However, their methods are not acceptable in the wireless environment, because their schemes require complex and time-consuming processing. Also, the other side of the user information can remain on the reader or other mobile devices in the process of communication. Thus, it is possible that user impersonation attacks can occur using this information.

In this paper, in order to solve these problems, we present a method that performs a safety user authentication and key agreement using XOR operations and hash function algorithms. Especially, it is robust against user impersonation attack, because it performs the authentication while leaving no information on the other party's mobile or reader.

We describe some characteristics of NFC, the structural environment, and related studies in Section 2. Section 3 gives a description of our proposed method. The safety and efficiency analysis is given in Section 4. The conclusion is given in Section 5.

2. Related Works

The core technology used in this study is the authentication for safe financial payment using NFC. In this chapter, we examine the characteristics of the NFC and look into the various forms of the NFC financial payment methods.

2.1. NFC Characteristics

The NFC performs the communication at the 13.56 MHz frequency band for compatibility with the RFID [10]. NFC communication is shown in Figure 1. The NFC-equipped mobile devices can perform the communication with a trusted third party such as bank, market server and web server. This is also the same in case of the reader side. Especially, the core feature of the NFC is to be able to communicate from device to device, in other words, communicate between mobile devices [7]. The existing TAG has drawbacks that cannot be operated with high-performance encryption algorithms. However, NFC has the advantage that makes it possible to perform the communication without exposing important secrets of personal information including financial transaction data. There are many studies for supporting secure payments, including SET [11], iKP [1], Kungpisdan [2], NFC-SEC [8], Sekhar [12], Hasoo [13,14] and Sung [15] methods. However, their works are disadvantaged in that users' secret information is exposed at the other side of the node. As shown in Figure 1, users can obtain detailed information of the product through the TAG, and then, can complete payment through communication with relevant readers or mobile devices with payment. Thus, the NFC scheme is a convenient method as it can solve the difficulties of card and movement based payments in existing POS (Point of Sales) systems.

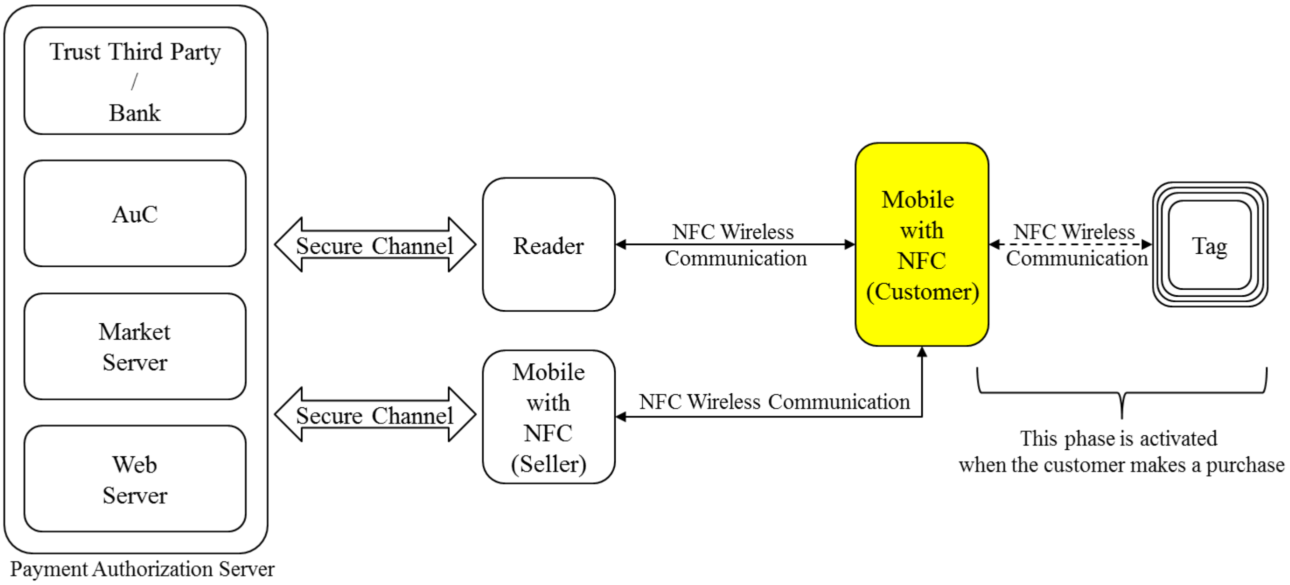
Trust Third Party
/
Bank
AuC
Market Server
Web Server
Payment Authorization Server
Secure Channel
Secure Channel
Reader
Mobile with NFC (Seller)
NFC Wireless Communication
NFC Wireless Communication
Mobile with NFC (Customer)
NFC Wireless Communication
Tag
This phase is activated when the customer makes a purchase

Figure 1. Three kinds of Near Field Communication (NFC).

2.2. Security Standard of NFC

The smart phone manufacturing companies such as SAMSUNG, LG, NOKIA, RIM, have released the smart phone equipped NFC technology [4]. These companies show the usefulness of NFC such as a smart poster, BIS (Bus Information System) that informs the arrival and operation time of buses, and the coupon for the purpose of promotion. Also, NFC can be used for payments in fast food restaurants, movie theaters, *etc*. Bouyges telecom in France is conducting a pilot project whereby urban railway fares in Paris can be paid out through the NFC [15,16]. However, the most remarkable usage of NFC is the wallet application [4]. It can replace everything in people's wallet such as money, credit card, name card, and identification card. To let users pay with NFC, we should solve a security problem for the safe payment [3,4]. So, the NFC-SEC proposed security specifications in the NFC forum. NFC-SEC defined NFCIP-1 (Near Field Communication Interface and Protocol) as a standard. NFC-SEC specifies NFC SSE (Security Services and Protocol) and SCH (Secure Channel Service) [8]. NFC SSE is devised for the safe communication between the NFC devices. The key agreement algorithm which is used in the process can complete SCH by using ECSDVP-DH (Elliptic Curve Secret Value Derivation Primitive, Diffie-Hellman version) based on ECC (Elliptic Curve Cryptosystem) [8]. Because this method is based on ECC, it operates an encryption algorithm based on the public key. Therefore, both NFC nodes participating in the communication should generate a Private Key and Public Key through the ECC algorithm. The method might generate the designated hardware processor, which can operate the ECC code algorithm in USIM-NFC for the sub-miniature computing environment to guarantee an efficient communication execution speed. However, embedding an additional processor has problems in terms of cost. So, a new authentication method to minimize the cost of manufacturing hardware for safe financial payment is needed. We summarized some safety vulnerabilities of NFC in Figure 2. As shown following Figure 2, problems may occur such as TAG cloning, access of illegal TAG, and leaving authentication information on record through a disguised reader or a mobile device, because communication between TAG and mobile devices occurs in a wireless environment. Attacks such as "man-in-the-middle", replay and snatching of the authentication information in communication between a mobile device or a reader and a certification center server may also occur. Therefore, our goal in this paper is to propose a lightweight authentication method and a secure way in response to these attacks.

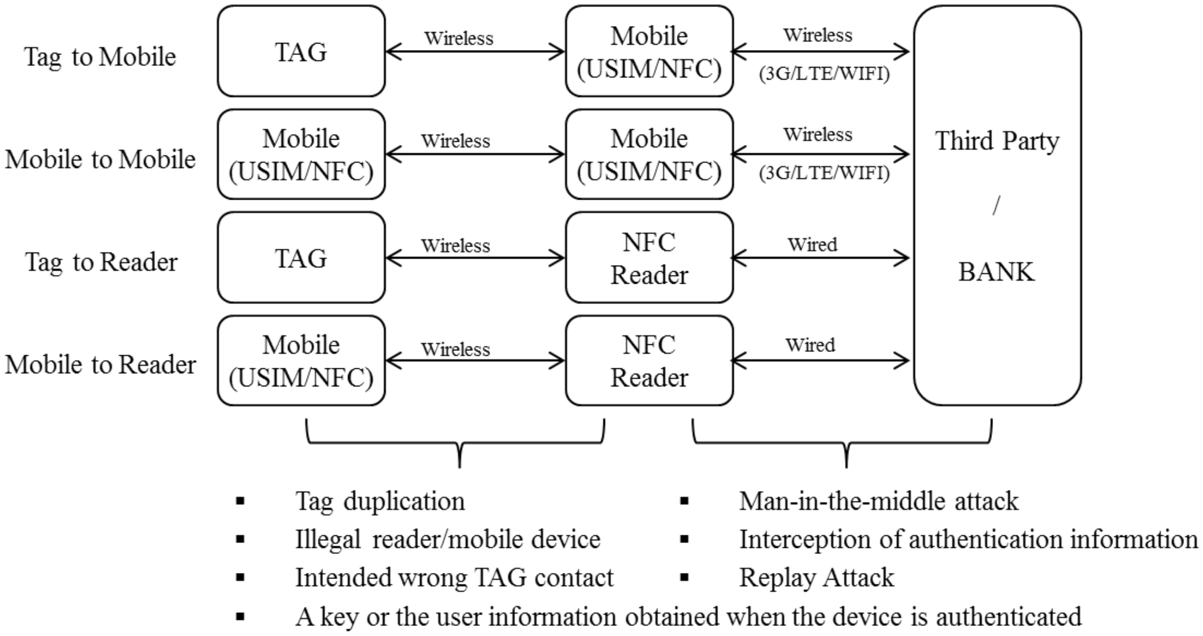

Figure 2. Safety vulnerability of NFC.

2.3. Financial Payment Method Using NFC

The credit cards have been developed for the user to pay through the card connected to his account anytime and anywhere without cash. One of the demerits of payment with credit cards is that you should always be alert for managing many credit cards in your wallet. In order to solve this problem, the user can simply carry out the financial payment anytime and anywhere by using the mobile device. The most useful technology in this environment is NFC.

The various financial payment methods using NFC have been developed based on the safe transaction of credit cards such as VISA and MasterCard. These methods perform the authentication and encrypted communication by using a public key-based way to ensure safety. SET (Secure Electronics Transaction) is a typical public key-based financial transaction [11]. As it is a communication method consisting of a pair of "Request" and "Response", it proceeds to the transaction by obtaining a certification. This method is mainly used for payment with a credit card but the transaction process is complex. iKP method is another public key-based method [1]. It performs communication of the encryption and decryption between the digital signature and the user by using a public key pair. This method also has complex operations such as a public key-based method on the transaction process. The ways of SET and iKP is useful in wired payment environments. However, some delays can occur because of complex and time consuming methods. Kungpisdan is a method that reduces the communication steps of computation algorithm [2]. It has improved the efficiency by using a symmetric key and hash-function. However, the number of the symmetric key usage in customer and merchant is relatively high. Therefore, a more efficient method to relieve this problem is needed. In the case of Sekhar, it uses a symmetric key-based financial payment system [12]. The usage of the symmetric key operation is reduced by one step to Kungpisdan's scheme. Also, the number of the keyed-hash functions is reduced by one step to Kungpisdan's scheme. Sung proposed the authentication method with NFC which guaranteed anonymity [15]. This method carries out the safe user authentication based on the *N*-th degree truncated polynomial Ring Scheme. Especially, the heavy authentication structure of the existing public-key-based method is improved by using a smaller key size and lighter public key method. The guaranteeing of anonymity is based on the zero-knowledge authentication method. However, these methods in the NFC environment are too heavy for mobile communication, because the encryption algorithm related to all nodes should be maintained for communication.

2.4. Security Vulnerabilities that May Occur in the Financial Payment

Security vulnerabilities that may occur in communications using NFC were shown in Figure 2. First, in the structure of the nodes participating in the communications, there are banks or third parties saving and administering TAG and reader, the mobile device and payment information. In communications between TAG and NFC reader, between TAG and the mobile device, between the TAG mode of mobile device and reader mode of the mobile device, and between the TAG mode of the mobile device and NFC reader, all communications obey the NFC standard. Since all of this processing occurs within 10 cm of distance, it is assumed that the communication is executed when the user is willing to transmit data. However, TAG information read by the disguised reader for the purpose of attack can also be used for reproduction of the relevant TAG. Hence, it may lead to illegal uses by the reproduction of legal information. For safe communication, to avoid this kind of attack, we can form a secure channel by performing the authentication. This consideration is presented by the existing NFC-SEC standard. However, in this method, authentication information or user information may be exposed in the authentication process. Especially, in the authentication method of the NFC-SEC standard, the public key is exposed, so the disguised attack may take place. In addition, if the safety in the communication process is not secure, a problem would occur in communication between the reader and the financial corporations later. Therefore, in the communication between the TAG and the reader, the authentication is essential. Hence, it is necessary that new methods for preventing illegal data acquisition and access are established.

Due to security vulnerabilities that may occur in communications between the reader mode of the mobile device and financial corporations or between NFC reader and financial corporations, MITM (Man-in-the-Middle) attacks may take place. Two different attacking methods in the wireless environment are possible. First, there is the attacking method in the mobile device in which transfer is possible, mainly through software like illegal spyware. This allows hackers to embed an illegal program in a mobile device in order to obtain private data and transfer them to an attacker. If the user communicates with NFC to have access to payment, the private information and received information are intercepted. Furthermore, in wired communication processes between the reader and the bank, man-in-the-middle attacks intercept information and remake it into new information so as to make illegal payments possible. As a result, it is essential to solve security vulnerabilities that may occur. In the future, when e-wallet is populated, authentication and session key matching methods are necessary. Of course, these new methods should ensure that safety is reinforced in all sections of communication.

This paper proposes a new authentication method of third party endorsement, improving efficiency with XOR calculation and hash function.

3. Our Proposed Method

For NFC environments, we propose a high-speed processing of authentication and key agreement. Also, we present a method to perform secure communications leaving no information at the other party including with the mobile or reader. Our proposed method can be summarized as in Figure 3. First, all mobile devices must go through the pre-registration process one time. Authentication is performed by using the issued secret information in the registration phase. Following is the detailed description of the proposed method. Some terminologies in this paper are shown in Table 1.

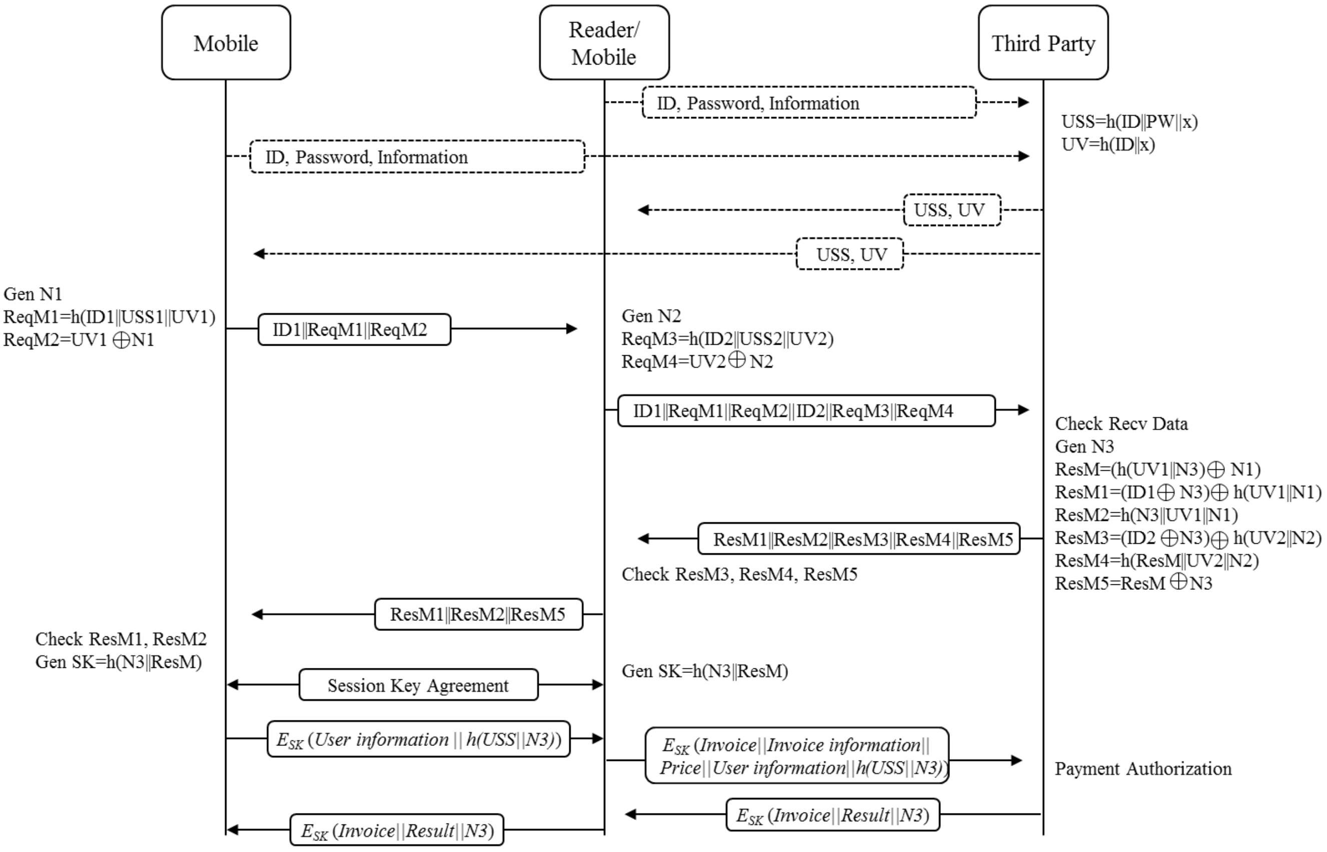

Figure 3. Our proposed scheme.

Table 1. Some terminologies in the paper.

Sign	Description
TP	Third Party
h	One Way Hash Function
N	Nonce
||	Connection
SK	Session Key
USS	User Shared Secret number
UV	User Value
ReqM	Request Message
ResM	Response Message

Our method consists of four phases of Registration, Authentication, Key Agreement, and Payment.

3.1. Registration Phase

The registration of the user's information should be carried out for the effective communication with trustworthy TP and authentication center. The reason why you need to registration stage is to clarify the source of transaction. All users enter the private information and carry out the transactions using this registered information, so pursuing the transactions becomes possible and the transactions cannot be carried out by anyone but the registered user. It can block all the illegal transactions. We assume that this registration process is established with a safe communication channel. In this study, however, how to obtain a secure channel in the registration stage will not be discussed.

The process of pre-registration is as follows. A mobile device which needs to be registered sends its own ID and password to the trusted TP. After this, TP stores the received information into the DB, and generates USS and UV through the following operations.

$$\mathrm{USS} = h(\mathrm{ID}||\mathrm{PW}||x)$$

$$\mathrm{UV} = h(\mathrm{ID}||x)$$

This generated USS and UV values are sent back to the mobile devices through the secure channel. Then, these two values are stored on the mobile and reader securely.

3.2. Authentication Phase

The authentication process is for clarifying the source and for proving the legal registered user based on the pre-registered private information. The proposed method in this study carried out the authentication without exposing private information to the opposite party. The reader can decode only the qualified result for the authentication process to verify all the received information from TAG or reader.

In the authentication phase, initiating user generates N1 as a nonce value, and also generates two request messages with the following operations.

$$\textit{Generate}\ \mathrm{N1}$$

$$\mathrm{ReqM1} = h(\mathrm{ID1}||\mathrm{USS1}||\mathrm{N1})$$

$$\mathrm{ReqM2} = \mathrm{UV} \oplus \mathrm{N1}$$

This generated information ReqM1 and ReqM2 is sent to the reader, and the receiver performs the following operation to obtain the reader's information for ReqM3 and ReqM4.

$$\textit{Generate}\ \mathrm{N2}$$

$$\mathrm{ReqM3} = h(\mathrm{ID2}||\mathrm{USS2}||\mathrm{N2})$$

$$\mathrm{ReqM4} = \mathrm{UV2} \oplus \mathrm{N2}$$

After this operation, the reader sends the information for ID1, ReqM1, ReqM2, ID2, ReqM3, and ReqM4 to the TP.

TP verifies ReqM1, ReqM2, ReqM3 and ReqM4. Then, TP generates nonce value N3, ensuring all received messages are right. After TP generates nonce value N3, it performs various operations as follows.

$$\mathrm{ResM} = h(\mathrm{UV1}||\mathrm{N3}) \oplus \mathrm{N1}$$

$$\mathrm{ResM1} = (\mathrm{ID1} \oplus \mathrm{N3}) \oplus (\mathrm{UV1}||\mathrm{N1})$$

$$\mathrm{ResM2} = h(\mathrm{N3}||\mathrm{UV1}||\mathrm{N1})$$

$$\mathrm{ResM3} = (\mathrm{ID2} \oplus \mathrm{N3}) \oplus h(\mathrm{UV2}||\mathrm{N2})$$

$$\mathrm{ResM4} = h(\mathrm{N3}||\mathrm{UV2}||\mathrm{N2})$$

$$\mathrm{ResM5} = \mathrm{ResM} \oplus \mathrm{N3}$$

After this, TP sends ResM1||ResM2||ResM3||ResM4||ResM5 to the receiving equipment. The reader verifies ResM3, ResM4 and ResM5.

3.3. Key Agreement Phase

The key agreement phase is required for the session key which will be used for exchange of payment information based on the information in the authentication process. The reader device verifies the ResM3, ResM4 and ResM5, and it sends ResM1, ResM2 and ResM5 to the initiating user. As the receiver of these data, so to speak, the initiating user generates a session key as follows, after verifying the received information.

$$\mathrm{SK} = h(\mathrm{N3}||\mathrm{ResM})$$

After this, two devices can communicate safely through this common session key of SK.

3.4. Payment Phase

This phase uses a symmetric key-based way. Based on the previously agreed session key, it performs an encrypted communication between each mobile, reader/mobile and TP as you can see in Figure 3.

In this process, various information can be contained into payment transaction. In other words, different types of information such as invoice, invoice information, price and user information may be allocated to a payload. Replay or user impersonation attack is impossible because that information should be delivered based on *SK* after previous agreement of the key. The payment process of this operation is as follows.

$$E_{SK}\ (Invoice||Invoice\ information||Price||User\ information\ \ldots)$$

4. Analysis

We analyze our method according to usefulness, safety, and efficiency. We also discuss the demerits of our method.

4.1. Usefulness of Electronic Payment Using NFC

We show the usefulness of the proposed method in the process of electronic payment. There are two scenarios; to pay with credit card or with NFC equipped smartphone. Firstly, you can pay with credit card in the following sequence. You take out your wallet, and select one credit card among many. Then, you hand it over to the clerk. The clerk applies your card to the credit card reader, and this reader system starts the communication with the remote host for payment transaction. After a few seconds, when transaction is completed, you put your signature on a receipt. Then, you put your receipt in your wallet.

However, you can pay with NFC equipped smartphone by following this *simple* sequence. You take out your smartphone, and put it over the NFC reader system. Then, this reader system starts the communication with the remote host for payment transaction. At the same time, a payment app program pops up on your phone screen. This app requires your pin number. Then, you put your pin number on the screen of your phone. After a few seconds, when transaction is completed, electronic receipt is generated and stored back into your phone automatically. That is all quite simple. We depicted the scenarios of electronic payment using NFC in Figure 4.

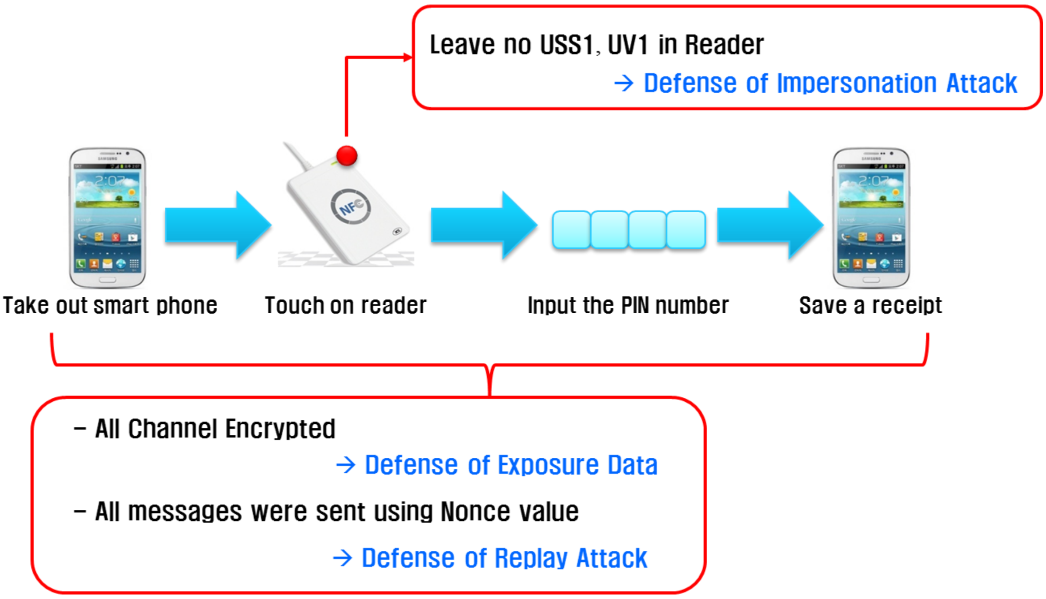
Leave no USS1, UV1 in Reader
→ Defense of Impersonation Attack
NFC
Take out smart phone
Touch on reader
Input the PIN number
Save a receipt
– All Channel Encrypted
→ Defense of Exposure Data
– All messages were sent using Nonce value
→ Defense of Replay Attack

Figure 4. A scenarios of electronic payment using NFC.

4.2. Safety Analysis

In this section, we discuss safety issues within the context of electronic payment using NFC.

As seen in Figure 4, we leave neither USS nor UV with the reader party. We can prevent an impersonation attack. We encrypted all channels, and all messages are protected with the nonce values.

Hence, the proposed method has no exposed data and cannot experience a replay attack. The detailed description about this issue is as follows.

4.2.1. Replay Attack

In our proposed scheme, a key idea that prevents replay attacks is the usage of nonce value. Since the value of the nonce varies in every session, this nonce value participates in the operation of all phases. In other words, the vulnerable information from the communication phase are the values of the ID1, ID2, ReqM1, ReqM2, ReqM3, ReqM4, ResM1, ResM2, ResM3, ResM4 and ResM5. As mentioned above, data can be protected by using the nonce values.

4.2.2. The Verification That No User Information Has Been Left on the Other Device

To ensure no user information has been left on the device of the other party, our proposed scheme performs the authentication through the TP. In this paper, the remaining information on the other side is just ID, ReqM1 and ReqM2. It is important to note that the essential USS and UV cannot be resolved. Although anyone obtains received ResM1, ResM2 and ResM5 through the TP, he cannot open N1, the generated value of nonce by the user. Therefore, all values, except ID, are meaningless. Thus, no one can obtain the information for malicious uses.

4.2.3. User Impersonation Attack

User impersonation attack is performed in conjunction with a replay attack. This type of attack designed to disguise users often occurs using the received information from the other party. Assume that someone acquired the information of ID1, ReqM1 and Re2M2, during the previous communication process or from the wireless communication band. In order to disguise the other user, the user impersonation attack that sends relevant information to other user U3 is possible. In other words, there is a case that user U2 accessing U3 can act as the other user U1. In this case, user U2 sends received information to user U3. Then, user U3 sends the relevant information to TP. TP verifies the right value, and sends generated data to user U3, after generating the ResM1~ResM5. After user U3 receives relevant information, U3 sends ResM1, ResM2 and ResM5 to the U2. To generate a session key, user U2 should be able to perform *h*(N3||ResM). At this point, because the ResM is *h*(UV1||N3||N1), even if you mix ResM1 and ResM2, you cannot create ResM. Hence, the attacker cannot create a session key because he cannot find out the changing values of the UV1 and the N1 in every session. Even if you want to use the previous session key in the previous session, you cannot get a session key, because the N3 changes in every session. In conclusion, the user impersonation attack is impossible.

4.3. Efficient Analysis

The main crypto algorithms in our proposed authentication and key agreement method are hash function and XOR operation. Thus, basically, these *primitive* operations, such as hash function and XOR operation, are far faster than the crypto algorithm based on public key and secret key. Only with these primitive operations, we improved the efficiency using the crypto algorithm that can perform a high-speed operation. Overall time complexity of our method is as follows.

$$15T_{\mathrm{hash}} + 16T_{\mathrm{xor}}$$

At this point, T_{hash} is the time to perform the hash function once. T_{xor} is the time to perform the XOR operation once. Note that the time complexity of our method $15T_{\mathrm{hash}} + 16T_{\mathrm{xor}}$ does not include the payment phase, because all methods including our method have the same time complexity of payment phase for the same application. We define T_{sec} as the run time of the crypto algorithms based symmetric key. It requires nearly $6T_{\mathrm{sec}}$ for payment phase, because it performs the operation using a cryptography system for financial payment. Financial payment is based on a symmetric key after getting the agreement of the session key. Each node is involved in encryption process time, and it is also involved in decryption process time. The time requirement of earlier study for authentication phase and key agreement phase is estimated as follows [1,2,8,11,13–15].

NFC-SEC [8]:	$2T_{\mathrm{KDF}} + 4T_{\mathrm{hash}}$
SET [11]:	$6T_{\mathrm{puk}} + 10T_{\mathrm{sig}} + 3T_{\mathrm{sec}}+ 5T_{\mathrm{hash}}$
iKP [1]:	$2T_{\mathrm{puk}} + 11T_{\mathrm{sig}} + 7T_{\mathrm{hash}} + 1T_{\mathrm{khash}}$
Kungpisdan [2]:	$11T_{\mathrm{sec}} + 2T_{\mathrm{hash}} + 5T_{\mathrm{khash}} + 4T_{\mathrm{kgen}}$
Sekhar [12]:	$11T_{\mathrm{sec}} + 4T_{\mathrm{hash}} + 2T_{\mathrm{khash}} + 4T_{\mathrm{kgen}}$
Hasoo [13,14]:	$2T_{\mathrm{KDF}} + 4T_{\mathrm{hash}} + 4T_{\mathrm{numberGen}}$
Sung1 [15]:	$5T_{\mathrm{CM}}$
Sung2 [15]:	$1T_{\mathrm{CM}} + NT_{\mathrm{sec}} + T_{\mathrm{hash}}$

T_{puk} refers to the operating time of the public key based crypto algorithms. T_{sig} is the time required to generate and verify the signature. T_{khash} means the operating time of keyed-hash functions. T_{kgen} is required time for generating a key. T_{KDF} is the abbreviation of "Key Derivation Function". $T_{\mathrm{numberGen}}$ is the time for new operation algorithm like multiplying. Finally, T_{CM} is the required time for convolutional multiplication operation. The number N in the Sung2 means the number of participants. Note that we use only primitive operations such as Hash function and XOR operation. In other words, we significantly reduced the computing time compared with the earlier studies. Therefore, it is judged that we improved time efficiency.

However, in earlier studies, the process of pre-registration is simpler than our method. Moreover, some other studies do not require the process of pre-registration at all. Securing safety is important in the whole process. Carrying out efficient communication is also essential for carrying out encoding and NFC operating in the USIM. In this process, while NFC-SEC method may be regarded as an efficient method, it defines carrying out only authentication and key agreement for the communication between the devices. So, access to a device with malicious intent is processed like a normal transaction. Hence, their methods have the serious problem of safety. On the other hand, Hasoo's method [14] carries out the calculation with the random number and the improved authentication method to prevent the public key information from exposure, compared to the authentication of NFC-SEC method. So, it is better at coping with the impersonation attack, but it does not consider the authentication execution for communication with the bank or third-party. Hence, if they want to consider the authentication with the third-party, lots of calculations will be required additionally.

4.4. Demerits of the Proposed Method

Our method has several drawbacks. While our method requires pre-registration, others do not. Another drawback of the proposed method is related to the limitation of hash function.

4.4.1. Pre-Registration

The demerit of the proposed method in this study is a requirement of the pre-registration step. All nodes should register its ID and password in the authentic institution for the safe communication. Moreover all communications in this process were assumed as safe communication. This pre-registration process means that the authentication with the unregistered node is impossible, and administrating and sharing registered information should be maintained by the authentic institution.

This additional pre-registration phase is a time consuming work, and it is inconvenient to the users. However, the proposed pre-registration in this study requires just one time. So all transactions, except first time, do not require additional registration process any more. Also, in the case of NFC payment, the pre-registration is acceptable overhead, because NFC app program is pre-installed on smart phone to make electronic payment transaction. Hence, the pre-registration process can be accomplished during the installation time of the NFC app program.

4.4.2. Administration of USS Value and UV Value

After the pre-registration is carried out, all nodes should take care of USS and UV value as its private information. If the USS and UV values are exposed, the safety of all authentication processes cannot be secured. In the proposed method, USS and UV value of the communication process can always be hidden through the hash functions, so the possibility to be exposed depends on the safety of the hash functions. Improved safety of hash functions can be achieved by increasing the number of output bits.

In the case of other existing TAG to Reader systems, the saved information in the node should be maintained within the designated reader system, so it can be considered safe. However, in the case of the smart phone, the various applications share one internal memory and SD memory. As a result, the safe saving and administration of the USS and UV values is very important, but in this study, it was assumed that access to other applications is blocked by the access-control method of the smart card filing system with the ISO7816-4 standard [17].

4.4.3. Trap-Door of One-Way Hash Function

The existing studies detected and verified the information through encoding and decoding. On the other hand, our method carries out the authentication by using only one-way hash functions and XOR calculation. Thus, our method presents a very fast authentication algorithm compared to other existing methods. However, if the trapdoor of the hash function happens because of the characteristic of the complexity and having no decoding sequence, the effect of the proposed authentication method can be useless. So, the one-way hash functions with qualified safety should be used for commercializing applications.

5. Conclusions

A variety of data can be easily obtained by using a smartphone. Moreover, the adoption of the NFC into smartphone makes it possible to perform the communication between the users easily. The electronic money technology allows electronic payment among the many participants. It is well known that this kind of electronic payment process requires safety mechanisms. It also requires light-weight algorithms for the mobile environment. Many previous methods were proposed for the safe financial transactions in this environment, but the endorsement method of third-party was not considered. Furthermore, there is a need to overcome the user impersonation attack and the inefficiency of the authentication phases due to the user data that is left on the reader or device on the other side.

In this paper, we presented an efficient method by using only XOR operations and hash functions. Also, we presented a safe method with the endorsement method of the third-party. Some drawbacks of our method are also presented. We hope that our method can be used efficiently in secure transactions and data exchange between the users with smartphone.

Acknowledgments

This work was supported by Kyungnam University Foundation Grant, 2012.

Conflicts of Interest

The author declares no conflict of interest.

References

1. Bellare, M.; Garay, J.A.; Hauser, R.; Herzberg, A.; Krawczyk, H.; Steiner, M.; Tsudik, G.; Herreweghen, E.V.; Waidner, M. Design, Implementation and Deployment of the iKp Secure Electronic Payment System. *IEEE J. Sel. Areas Commun.* **2000**, *18*, 611–627.
2. Kungpisdan, S.; Srinivasan, B.; Phu, D.L. A Secure account-based mobile payment protocol. In Proceedings of the International Conference on Information Technology: Coding and Computing, Las Vegas, CA, USA, 5–7 April 2004.
3. Peng, K. A Secure Network for Mobile Wireless Service. *J. Inf. Process. Syst.* **2013**, *9*, 247–258.
4. Oh, J.S.; Park, C.U.; Lee, S.B. NFC-based Mobile Payment Service Adoption and Diffusion. *J. Converg.* **2014**, *5*, 8–14.
5. Gnanaraj, J.W.K.; Ezra, K.; Rajsingh, E.B. Smart card based time efficient authentication scheme for global grid computing. *Hum.-Cent. Comput. Inf. Sci.* **2013**, *3*, 1–14.
6. Michahelles, F.; Thiesse, F.; Schmidt, A.; Williams, J.R. Pervasive RFID and Near Field Communication Technology. *IEEE Pervasive Comput.* **2007**, *6*, 2–5.
7. Kuspriyanto, E.H.; Basjaruddin, N.; Purboyo, T.; Purwantoro, S.; Ubaya, H. Efficient Tag-to-Tag Near Filed Communication (NFC) Protocol for Secure Mobile Payment. In Proceedings of the 2nd International Conference on Instrumentation, Communications, Information Technology, and Biomedical Engineering, Bandung, Indonesia, 8–9 November 2011.

8. *Information Technology Telecommunications and Information Exchange between Systems—NFC Security—Part 1: NFC-SEC NFCIP-1 Security Service and Protocol*; ISO/IEC 13157-1:2010; ISO/IEC: Geneva, Switzerland, 2010.
9. *Information Technology Telecommunications and Information Exchange between Systems—NFC Security—Part 2: NFC-SEC Cryptography Standard Using ECDH and AES*; ISO/IEC 13157-2:2010; ISO/IEC: Geneva, Switzerland, 2010.
10. Vincent, J.; Limi, V.; Plateaux, A.; Gaber, C.; Pasquet, M. A Mobile Payment Evaluation Based on a Digital Identity Representation. In Proceedings of the International Conference on Collaboration Technologies and Systems, Denver, CO, USA, 21–25 May 2012.
11. Secure Electronic Transaction Specification, version 1.0. Available online: http://www.maithean.com/docs/set_bk1.pdf (accessed on 23 December 2014).
12. Sekhar, V.C.; Sarvabhatla, M. Secure lightweight mobile payment protocol using symmetric key techniques. In Proceedings of 2012 International Conference on Computer Communication and Informatics (ICCCI), Coimbatore, India, 10–12 January 2012; pp. 1–6.
13. Eun, H.S.; Lee, H.J.; Oh, H.K. Conditional Privacy Preserving Security Protocol for NFC Applications. *IEEE Trans. Consum. Electron.* **2013**, *59*, 153–160.
14. Park, S.W.; Lee, I.Y.; Anonymous Authentication Scheme Based on NTRU for the Proetection of Payment Information in NFC Mobile Environment. *J. Inf. Process. Syst.* **2013**, *9*, 461–476.
15. Cassimon, D.; Engelen, P.J.; Yordanov, V. Compound Real Option Valuation with Phase-Specific Volatility: A Multi-phase Mobile Payments Case Study. *Technovation* **2011**, *31*, 240–255.
16. Shin, D.H. Towards ANS understanding of the consumer acceptance of mobile wallet. *Comput. Hum. Behav.* **2009**, *25*, 1343–1354.
17. ISO7816-4 standard. Available online: http://en.wikipedia.org/wiki/ISO/IEC_7816 (accessed on 24 December 2014).