

# Anonymous Authentication Scheme based on NTRU for the Protection of Payment Information in NFC Mobile Environment

Sung-Wook Park\* and Im-Yeong Lee\*

**Abstract**—Recently, smart devices for various services have been developed using converged telecommunications, and the markets for near field communication mobile services is expected to grow rapidly. In particular, the realization of mobile NFC payment services is expected to go commercial, and it is widely attracting attention both on a domestic and global level. However, this realization would increase privacy infringement, as personal information is extensively used in the NFC technology. One example of such privacy infringement would be the case of the Google wallet service. In this paper, we propose an zero-knowledge proof scheme and ring signature based on NTRU for protecting user information in NFC mobile payment systems without directly using private financial information of the user.

**Keywords**—NFC Mobile Payment, Zero Knowledge Proof, NTRU, Ring Signature

## 1. INTRODUCTION

Near Field Communication (NFC) is a short-range wireless communication standard defined in the ISO/IEC 18092 standard. In the future, it is expected that most mobile devices will be equipped with an NFC interface. NFC operates at 13.56 MHz and it can be used for communication between two active devices, or an active device and a passive device. Active devices are powered by a battery, whereas passive devices obtain their energy from the initiator and an NFC target. An active device can have both roles, whereas a passive device is always an NFC target. The initiator sends requests to a target and the target answers these requests. NFC operates electromagnetic field of the active device. Communication always occurs between an NFC tag and NFC reader operates in a manner that is highly intuitive for the user. Two NFC devices start communicating after bringing them close together (known as “touching” each other). Recently, smart devices for various services have been developed using converged telecommunications, and the markets for near field communication mobile services is expected to grow rapidly. In particular, the realization of mobile NFC payment services is expected to go commercial, and it is widely attracting attention both on a domestic and global level. However, there are growing issues with privacy infringement due to increasing personal information exchange via NFC

\* This research was supported by Basic Science Research Program through the National Research Foundation of Korea(NRF) funded by the Ministry of Education, Science and Technology (2013R1A1A2012940) and the Soonchunhyang University.

Manuscript received October 5, 2013; accepted March 7, 2013.

**Corresponding Author: Sung-Wook Park**

\* Department of Computer Software Engineering, Soonchunhyang University, Asan-si, Republic of Korea (swpark@sch.ac.kr, imylee@sch.ac.kr)




	Collection		Storage		use		offer		
	Collected Information	Collect ed Path	Stored Information	Stored Path	Used Information	Purpose of use	Offered Information	Purpose of Offer	Receiver
 Merchant	Credit Card Info payment history	Wired/W ireless network	Credit Card Info payment history	Computer, Cabinet					
 VAN	Credit Card Info payment history	Wired/W ireless network	Credit Card Info payment history	• DB(VAN)			payment history	Credit Card Info payment history	• Merchant
 Card Issuer	payment history	Wired/W ireless network	payment history	• DB(Card issuer) • Cabinet	Credit Card Info	Whether to approve payment	Credit Card Info payment history	Payment authorizati on notice	• VAN
			payment history	• Wallet App	Contact Information	Payment authorizatio n notice			

Fig. 1. Payment Flows of NFC Mobile Card

technology. According to documents released by KISA(Fig 1), these problems are attributable to the following: partially unsupported privacy encryption, spill concerns affecting corporate internal privacy, excessive privacy requirements, and collection and storage. A privacy disclosure case related to the Google Wallet service can be used as evidence to support these issues. This paper is organized as follows. Section 2 analyzes security threats and the security requirements of NFC mobile environments. Section 3 explains the basic NFC concept, existing Google Wallet service, zero-knowledge proof scheme, ring signature, and the NTRU(N-th degree truncated polynomial ring) scheme. Section 4 proposes an anonymous authentication scheme based on NTRU that ensures payment information protection in NFC mobile environments. Section 5 presents our analysis of the proposed scheme and its security requirements. Section 6 contains our conclusions.

## 2. SECURITY THREATS AND REQUIREMENTS

In this chapter, we briefly review the security threats that affect communication between an NFC mobile and an NFC reader for providing a secure payment service in NFC mobile payment environments. We also analyze the security requirements for proposed service environments.

### 2.1 Security Threats to NFC Mobile Services

#### 2.1.1 Security Threats between NFC Mobiles and NFC Readers

- Man-in-the-Middle Attack: Sun et al. stated that the role of “NFC is to support the physical properties of proximity communication. Therefore, DoS Attack and MITM (Man-in-the-Middle) Attack in NFC communication are close to impossible”[12]. However, entity authentication is not performed during the first communication between NFC devices. Therefore, DoS and MITM attacks are possible during NFC communications.
- Eavesdropping: NFC communication usually occurs between two devices in close proximity, i.e., usually no more than 10 cm apart. The main question is how close an attacker needs to be located to retrieve a usable RF signal. Unfortunately, there is no easy answer to this question. This is because a large number of parameters can affect the answer. The distance may depend on the following parameters, among others[13].
  - The RF field characteristics of a specific sender device (i.e., antenna geometry, any shielding effect of the case, the process control block (PCB), and the environment)

- Characteristic of the attacker's antenna (i.e., antenna geometry and the possibility of changing position in all three dimensions)
- Quality of the attacker's receiver
- Quality of the attacker's RF signal decoder
- Setup of the location where the attack is performed (including barriers such as walls or metal, and the noise floor level)
- Power emitted by the NFC device

## 2.2 Security Requirements of the Proposed Scheme

The proposed scheme needs to address the security threats that affect NFC mobile payment environments (reviewed in Section 3.1). In addition, the proposed scheme needs to perform efficiently in a limited device environment and fulfill all the basic security requirements.

- Confidentiality: The data used in communication should be shared only with legitimate communication objects and, even if it is exposed during communication, the value of data cannot be inferred.
- Mutual authentication: Each object should provide mutual authentication to verify the legality of objects.
- Non-repudiation: Each object should ensure non-repudiation of data transmitted between legal objects.
- Efficiency: The proposed scheme should be computationally efficient in a limited device environment.
- Secrecy: The proposed scheme should maintain a high level of security about payment information. It should also satisfy the security requirements of the basic zero-knowledge proof protocol.

## 3. RELATED WORK

In this chapter, we describe the NFC concept, the structure of payment services based on NFC, and a public NTRU cryptosystem based on lattices. We also analyze the zero-knowledge proof scheme and ring signature scheme between a bank and a user.

### 3.1 Near Field Communication

NFC is a short-range wireless communication standard defined in the ISO/IEC 18092 standard. NFC operates at 13.56 MHz and it can be used for communication between two active devices, or between an active device and a passive device. NFC devices facilitate two-way communication between "intelligent devices." They also ensure security by applying NFC-SEC.

Communication between devices can reach a speed of up to 424 kbps but the maximum range of NFC communication is 4 cm. NFC services can be used as a payment method, ID card, coupon, and so on. NFC allows the authentication of corporate access rights, while NFC devices can also be used as contactless cards and for reading RF tags. NFC can operate in the following three modes. If the Card Emulation Mode is enabled, a device can be used as a contactless card. When the Reader/Writer Mode is enabled, a device can interact with RF tags. The P2P (Peer-to-Peer) Mode is enabled during bi-directional device communication. NFC Mobile architecture consists of an NFC device, SP, TSM, and a card issuer. Each NFC mobile device contains a

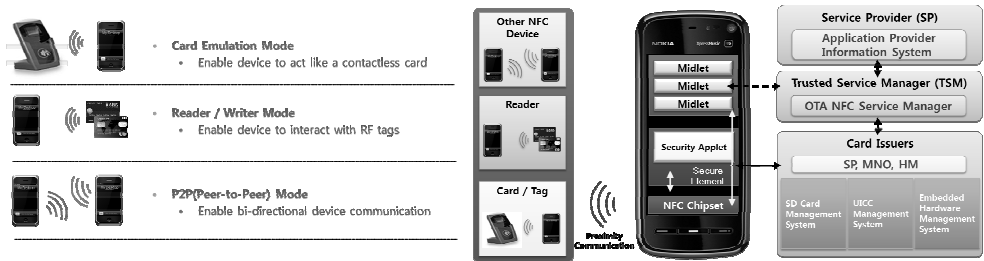


Fig. 2. Three NFC modes of NFC an used in NFC mobile architecture

MIDlet, Secure Element(SE), and NFC chipset. The NFC chipset supports proximate communications via any of the three NFC modes. The SE is managed by card issuers and used to store payment information.

### 3.2 Google Wallet Service

Recently, Google officially launched its NFC-based Google Wallet mobile payment service[1]. In addition, Google added NFC support to Android and launched Nexus S. The Google payment flow is shown in Fig 3. Credit information related to users can be collected by the card issuer, merchant, van, and other parties. Google stated that “All credit information is more secure than a physical wallet due to encryption using the NFC payment standard ‘M/Chip 4’ (Mobile MasterCard(R) PayPass™ M/Chip 4)”[2]. However, this has not been verified. However, Google researchers discovered a way of hacking Google Wallet and potentially stealing a user’s financial information. Thus, hackers could crack the personal identification number used to secure the service. This threat forced Google to disable its prepaid card. According to the NFC standard documents specified by ISO, this method used ISO7816-4. However, ISO7816-4 such as privacy encryption that is not supported. Therefore, many problems may occur with the NFC service. The Google Wallet process flow is shown in Figure 3.

- In the first step, a user registers information with the credit card issuer in a bank.

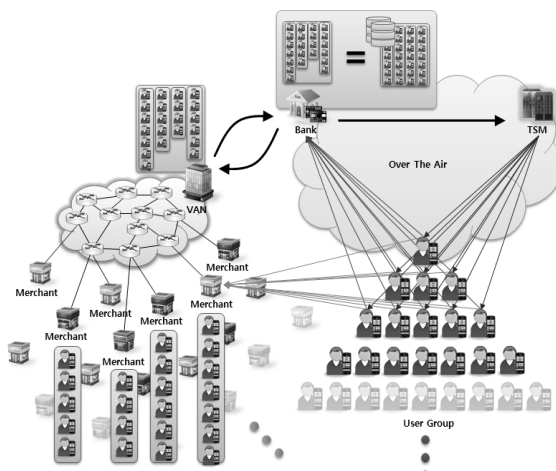


Fig. 3. Google Wallet

- The bank verifies the communication privacy and sends a transmission to a Trusted Service Manager (TSM)
- The TSM issues digital credit card to the user.
- Subsequent personal information flow with the Google Wallet service is shown in the figure.

### 3.3 NTRU

In the rump session of Crypto'96, N-th degree truncated polynomial ring (NTRU) was introduced by Hoffstein et al. as a public key cryptosystem based on the difficulty of finding particularly small vectors in lattices. This method uses a fast encryption/decryption and signature scheme. It also requires a smaller key size than other public key cryptosystems. The speed of the NTRUEncrypt Public Key Cryptosystem and its low memory usage indicates that it can be used in applications such as mobile devices and smartcards. The system is fully acceptable by IEEE P1363 standard that have been specified for lattice-based public key cryptography. In April 2011, NTRUEncrypt was accepted as an X9.98 Standard for use in the financial services industry[3].

#### 3.3.1 Truncated Polynomial Rings

The coefficient of NTRU is an integer. Its degree uses a polynomial with  $N - 1$ .

$$a = a_0 + a_1X + a_2X^2 + \dots + a_{N-2}X^{N-2} + a_{N-1}X^{N-1}$$

In the above equation, the coefficient  $a_0, \dots, a_{N-1}$  uses an integer but zeros can also be used. The set of all polynomials is defined in Ring R. If we add the polynomial coefficients in R, the following can be derived (Arbitrary polynomial : a, b).

$$a + b = (a_0 + b_0) + (a_1 + b_1)X + \dots + (a_{N-1} + b_{N-1})X^{N-1}$$

The NTRU multiplication method and polynomial multiplication method is similar, but has other features. If they are multiplied, we replace 1 with  $X^N$ , X with  $X^{N+1}$ , and  $X^2$  with  $X^{N+2}$ . In R, the multiplied polynomial can be summarized as follows.

$$a \times b = c_0 + c_1X + c_2X^2 + \dots + c_{N-2}X^{N-2} + c_{N-1}X^{N-1}$$

#### 3.3.2 NTRU Encryption

NTRU is set up with three integers (N, p, q) where

- N is prime
- p and q are relatively prime,  $\gcd(p, q) = 1$ , and
- q is considerably larger than p.

NTRU is based on polynomial additions and multiplications in the ring  $R = \mathbb{Z}[X] = (X^N - 1)$ . We use "\*" to denote a polynomial multiplication in R, which is the cyclic convolution of two polynomials. After completing a polynomial multiplication or addition, the coefficients of the resulting polynomial need to be reduced to either modulo q or p. It should be noted that the key creation process also requires two polynomial inversions, which can be computed using the extended Euclidean algorithm. These procedures are outlined briefly below.

**KeyGen** - To receive a public key, the user must do the following:

- select a secret key, (i.e., a random secret polynomial  $f \in R$  with coefficients reduced to modulo  $p$ )
- select a random polynomial, (i.e.,  $g \in R$  with coefficients reduced to modulo  $p$ )
- compute the inverse polynomial  $f_q$  of the secret key  $f$  in modulo  $q$ .

After completing this process, the public key,  $h$ , is given as follows:

$$h = pf_q * g(\text{modulo } q)$$

**Encryption** - The encrypted message is computed as

$$e \equiv pr * h + m(\text{modulo } q)$$

where the coefficients of the message,  $m \in R$ , and the random polynomial,  $r \in R$ , are reduced to modulo  $p$ .

**Decryption** - The decryption procedure requires the following steps:

$$\begin{aligned} a &= f * e(\text{modulo } q) \\ a &= f * (r * h + m)(\text{modulo } q) \\ a &= f * (r * pf_q * g + m)(\text{modulo } q) \\ a &= pr * g + f * m(\text{modulo } q) \\ b &= pr * g + f * m(\text{modulo } p) \\ b &= f * m(\text{modulo } p) \\ c &= fp * b(\text{modulo } p) \\ c &= m(\text{modulo } p) \end{aligned}$$

The final decryption step requires the user to compute the inverse polynomial  $F_p$  of the secret key  $f$  in modulo  $p$ . The decryption process outlined above subsequently recovers the original message.

### 3.4 Ring Signature

The ring signature was proposed by Rivest et al[5]. Ring signature is based on the RSA signature scheme. We call it *RSA-based ring signature*. Suppose that Alice wishes to generate a ring signature of a message  $m$  for a ring of  $n$  individuals  $A_1, A_2, \dots, A_n$ , where the signer Alice is  $A_s$ ,  $1 \leq s \leq n$ . Denote  $S = \{A_1, A_2, \dots, A_n\}$ . Each  $A_i \in S$  is called a ring member. The public key of  $A_i$  is  $P_i$  and the corresponding private key is  $S_i$ . In this paper, we will not distinguish between the ring member and its public key. Therefore,  $S$  will also be used to denote the set of public keys of all ring members.

A ring signature scheme consists of the following two algorithms :

- ring-sign ( $m, S$ ) : Given a message  $m$  and the set of ring members  $S = \{P_1, P_2, \dots, P_n\}$ , the actual signer  $A_s$  can produce a ring signature  $\sigma$  using  $S$  and her own private key  $S_s$ .

- ring-verify ( $m, \sigma$ ) : Given a message  $m$  and a ring signature  $\sigma$ , which includes  $S = \{ P_1, P_2, \dots, P_n \}$ , a verifier can determine whether  $(m, \sigma)$  is a valid ring signature generated by one of the ring members.

Combining functions : A combining function  $C_{k,v}(y_1, y_2, \dots, y_n)$  takes as input a key  $k$ , an initialization value  $v$ , and a list of arbitrary values  $y_1 = g_1(x_1), \dots, y_n = g_n(x_n) \in \{0, 1\}^b$ , such that for any given  $k, v, s, 1 \leq s \leq n$ , and any fixed values of all the other inputs  $y_i, i \neq s$ , the function  $C_{k,v}$  is a one-to-one mapping from  $y_s$  to the output  $z$ . Moreover, this mapping is efficiently solvable. However, it should be infeasible to solve the verification equation for  $x_1, \dots, x_n$  without knowing any of the private keys and inverting any of the trapdoor functions  $g_1, \dots, g_n$ .

In [5], a combining function is proposed as follows:

$$\begin{aligned} z &= C_{k,v}(g_1(x_1), \dots, g_n(x_n)) \\ &= E_k(g_n(x_n) \oplus E_k(\dots \oplus E_k(g_1(x_1) \oplus v))) \end{aligned}$$

Equivalently, we have

$$\begin{aligned} y_s &= E_k(g_{s-1}(x_{s-1}) \oplus \dots \oplus E_k(g_1(x_1) \oplus v)) \\ &\oplus E_k^{-1}(g_{s+1}(x_{s+1}) \oplus \dots \oplus E_k^{-1}(g_n(x_n) \oplus E_k^{-1}(z))) \end{aligned}$$

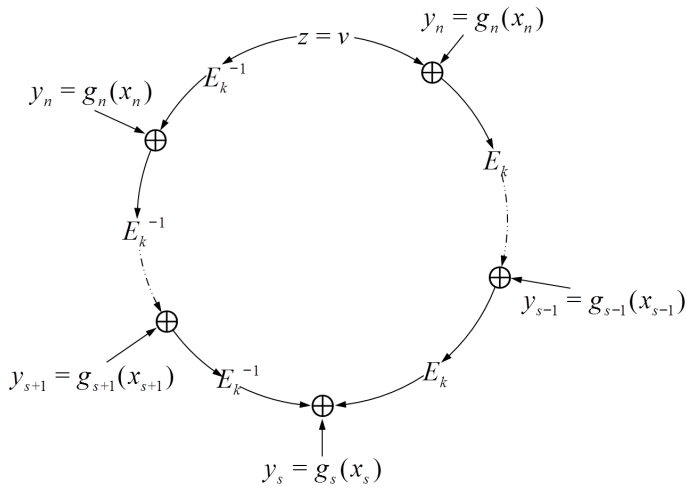


Fig. 4. Concept of Ring Signature

### 3.5 User Proof Scheme between a User and a Bank

#### 3.5.1 Fiat-Shamir Authentication Scheme

The Fiat-Shamir authentication scheme combines a zero-knowledge proof scheme and a crypto-scheme based on ID[4,7,8,9]. The Fiat-Shamir authentication scheme provides security

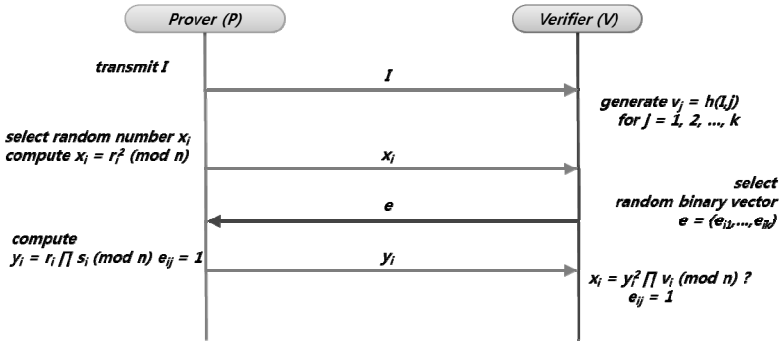


Fig. 5. Fiat-Shamir authentication scheme

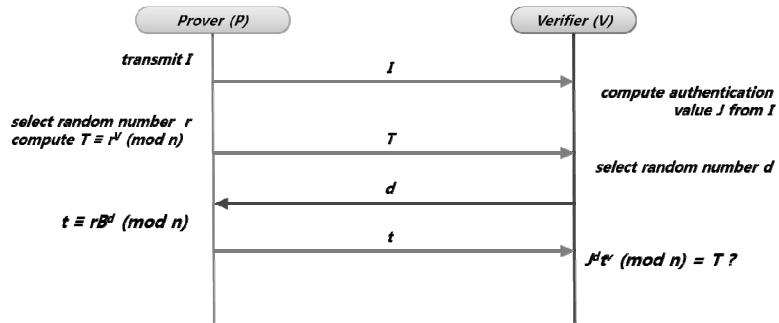


Fig. 6. Guillou-Quisquater authentication scheme

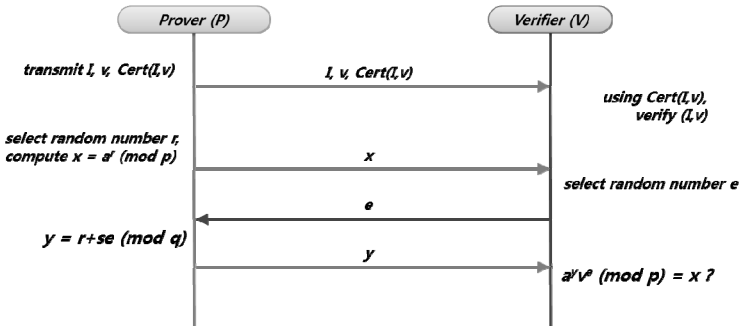


Fig. 7. Schnorr authentication scheme

based on the difficulty of finding  $n$  as the quadratic residue of  $x^2 \equiv a \pmod n$ . However, this method requires numerous repeated operations and high memory capacity because it computes  $t$  rounds during the authentication step.

### 3.5.2 Guillou-Quisquater Authentication Scheme

The Guillou-Quisquater authentication scheme consists of an authentication step with three moves for one round[10], and it has low memory requirements. However, the Guillou-Quisquater authentication scheme experiences difficulty in providing security when computing



$A$  in  $A \equiv J^{J^v} \pmod{n}$  because it requires numerous repeated operations.

### 3.5.3 Schnorr Authentication Scheme

Schnorr et al. proposed an efficient authentication scheme for use in environments smart-cards[11]. This method ensures security based on the difficulty of factoring a large number and a discrete logarithm problem. However, it has high computational complexity due to exponential computation.

## 4. PROPOSED SCHEME

In this paper, we propose a mutual authentication scheme based on NTRU as well as a zero-knowledge proof scheme based on NTRU for protecting NFC mobile payment information.

### 4.1 System Parameters

The system parameters in the proposed method are as follows

- \*: Object (A: User, B: Bank)
- $Z$ : Set of integers
- $N$ : (Prime) dimension
- $L_f, L_g$ : Subset of  $R$
- $p, q$ : Large prime number that satisfies  $GCD(p, q) = 1, p > q$
- $f, g$ : private key polynomial of \*, ( $f^* \in L_f, g^* \in L_g$ )
- $f_{*p}^{-1}, f_{*q}^{-1}$ : Inverse polynomial of  $f$
- $g_{*p}^{-1}, g_{*q}^{-1}$ : Inverse polynomial of  $g$
- $h, v^*$ : Public key on truncated polynomial  $R$
- $I$ : User identity
- $Cert^*$ : Certificate generated by the certificate authority
- $H$ : Hash function

### 4.2 Zero-Knowledge Mutual Proof Scheme based on NTRU

We propose a zero-knowledge proof scheme based on NTRU for protecting NFC mobile payment information. The proposed scheme consists of a user registration phase and a user identity proof phase, as follows.

#### 4.2.1 User Registration Phase

If a user wants to use the NFC mobile payment service, he or she needs to be registered in the following manner.

**Step 1:** The user calculates  $f_A, g_A, f_{Ap}^{-1}, f_{Aq}^{-1}$ , and  $v_A$  on the truncated polynomial ring.

$$\begin{aligned}
 A: f_A &\in L_f, g_A \in L_g \\
 A: f_{Ap}^{-1}, f_{Aq}^{-1} & \\
 A: v_A &= pf_{Ap}^{-1} \bullet g_A \in Zq[X]/(X^N - 1)
 \end{aligned}$$

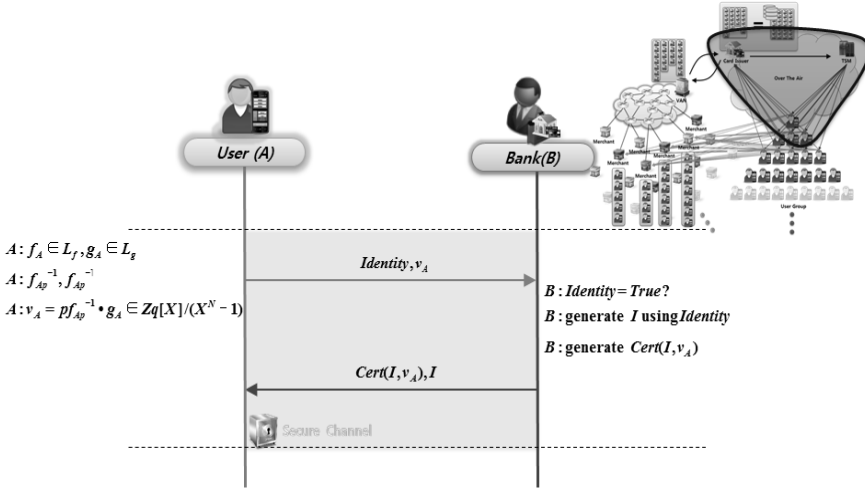


Fig. 8. Registration Phase

**Step 2:** The user submits his or her information and  $v_A$  to the bank, which verifies the identity of the user. The bank issues a public key certificate, which is generated based on the user identity ( $I$ ) and  $v_A$  of the user. The user information is stored in the bank.

$$A \rightarrow B: I, v_A$$

$$B: I = True?$$

$$B: Cert(I, v_A)$$

#### 4.2.2 User Identity Proof Phase

The user is required to perform the following operations to validate his or her identity.

**Step 1:** The user selects a random polynomial  $r_A$ . He or she then calculates data to prove his or her identity. Next,  $I, v_A, Cert(I, v_A)$ , and  $x$  are transmitted to the bank.

$$A: x = g_A \cdot r_A$$

$$A \rightarrow B: I_A, v_A, Cert(I, v_A)$$

$$A \rightarrow B: x$$

**Step 2:** The bank verifies the integrity of  $Cert(I, v_A)$  using a certification system. A random polynomial  $e$  selected by the bank is given to the user.

$$B: e \in L_e$$

$$B \rightarrow A: e$$

**Step 3:** The value of  $y = f_A \cdot r \cdot e_A$  is calculated by the user and submitted to the bank.

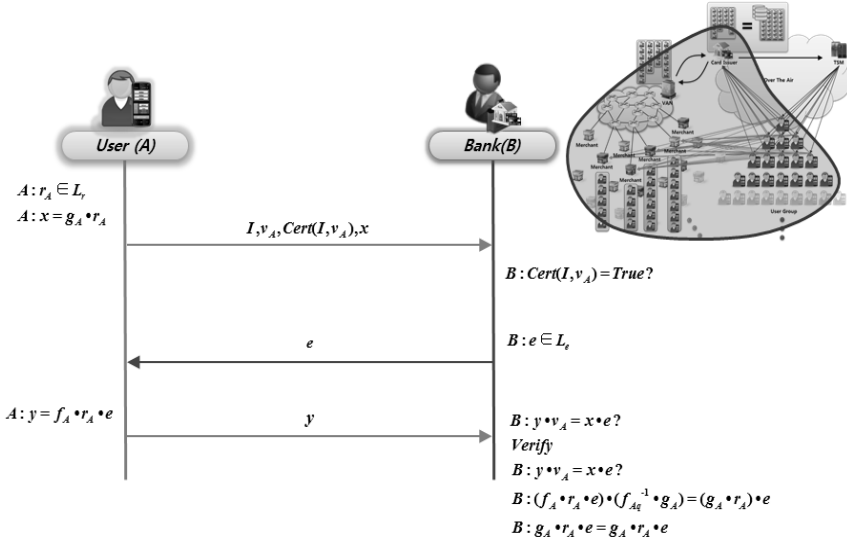


Fig. 9. Identity Proof Phase

$$A: y = f_A \bullet r_A \bullet e$$

$$A \rightarrow B: y$$

**Step 4:** The bank verifies the integrity of  $y \bullet v_A = x \bullet e$  and authenticates the user.

$$B: y \bullet v_A = x \bullet e?$$

$$B: (f_A \bullet r_A \bullet e) \bullet (f_{Aq}^{-1} \bullet g_A) = (g_A \bullet r_A) \bullet e$$

$$B: g_A \bullet r_A \bullet e = g_A \bullet r_A \bullet e$$

#### 4.2.3 Bank Identity Proof Phase

The bank is required to perform the following operations to validate its identity.

**Step 1:** The bank selects a random polynomial  $r_B$ . It then calculates data to prove its identity. Next,  $I_B, v_B, Cert(I_B, v_B), x_B$ , and  $e_B$  are transmitted to the user.

$$B: x = g_A \bullet r_A$$

$$B \rightarrow A: I, v_A, Cert(I, v_A)$$

$$B \rightarrow A: x_B, e_B$$

**Step 2:** The user verifies the integrity of  $Cert(I_B, v_B)$  using a certification system. He or she then computes  $y_A$  as his or her proof, selects a random polynomial  $e_A$ , and gives it to the bank.

$$A : e_A \in L_e$$

$$A \rightarrow B : e_A, y_A$$

**Step 3:** The bank authenticates the user. The value of  $y_B = f_B \cdot r_B \cdot e_A$  is calculated by the bank and submitted to the user.

$$B : y_A \cdot v_A = x_A \cdot e_B ?$$

$$B : (f_A \cdot r_A \cdot e_B) \cdot (f_{Aq}^{-1} \cdot g_A) = (g_A \cdot r_A) \cdot e_B$$

$$B : g_A \cdot r_A \cdot e_B = g_A \cdot r_A \cdot e_B$$

$$B : y_B = f_B \cdot r_B \cdot e_A$$

$$B \rightarrow A : y_B$$

**Step 4:** The user verifies the integrity of  $y_B \cdot v_B = x_B \cdot e_A$  and authenticates the user.

$$A : y_B \cdot v_B = x_B \cdot e_A ?$$

$$A : (f_B \cdot r_B \cdot e_A) \cdot (f_{Bq}^{-1} \cdot g_B) = (g_B \cdot r_B) \cdot e_A$$

$$A : g_B \cdot r_B \cdot e_A = g_B \cdot r_B \cdot e_A$$

### 4.3 Ring Signature Scheme based on NTRU

We propose a ring signature scheme based on NTRU using characteristics of convolution multiplication on truncated polynomial rings. we use to private key  $f$  and  $g$  by changing to generation method of NTRU parameter. In case of conventional NTRU scheme, they are selected small polynomial  $f, g$  of two and generated inverse  $f$  on truncated polynomial ring  $R$ . But, In this

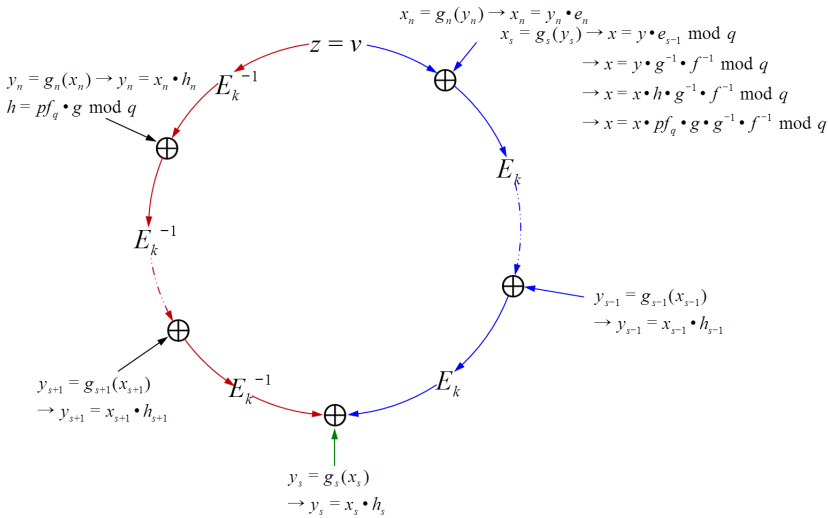


Fig. 10. Proposed Ring Signature Scheme

paper, we need inverse  $g$ . Therefore we choose  $g$  using generation method of parameter  $f$  for select of small polynomial.

In this paper, we used polynomial ring trapdoor permutation method without using the RSA trapdoor permutation method. Proposed polynomial ring trapdoor permutation method is shown below.

$$y_n = g_n(x_n) \rightarrow y_n = x_n \bullet h_n$$

$$h = pf_q \bullet g \text{ mod } q$$

$$x_s = g_s(y_s) \rightarrow x = y \bullet e_{s-1} \text{ mod } q$$

$$\rightarrow x = y \bullet g^{-1} \bullet f^{-1} \text{ mod } q$$

$$\rightarrow x = x \bullet h \bullet g^{-1} \bullet f^{-1} \text{ mod } q$$

$$\rightarrow x = x \bullet pf_q \bullet g \bullet g^{-1} \bullet f^{-1} \text{ mod } q$$

We propose a ring signature scheme based on NTRU for protecting NFC mobile payment information. The proposed scheme consists of ring-sign phase and ring-verify phase, as follows.

#### 4.3.1 Ring-Sign Phase

Suppose that Alice wishes to sign a message  $m$  with a ring signature for the ring of  $n$  individuals  $A_1, A_2, \dots, A_n$ , where Alice is  $A_s$  for some  $s, 1 \leq s \leq n$ . Given the message  $m$  to be signed,  $A_s$ 's private key  $S_s=(f, g, f_p^{-1}, f_q^{-1}, g_p^{-1}, g_q^{-1})$ , and the sequence of NTRU public keys  $P_1, P_2, \dots, P_n$  of all the ring members,  $A_s$  computes a ring signature as follows:

**Step 1:** Choose a key. The signer  $A_s$  first computes the symmetric key  $k$  as follows:

$$y_n = g_n(x_n) \rightarrow y_n = x_n \bullet h_n$$

$$h = pf_q \bullet g \text{ mod } q$$

$$k = H(m, P_1, P_2, \dots, P_r)$$

**Step 2:** Pick a random glue value. The signer picks an initialization value  $v \in \{0,1\}^b$  uniformly at random.

**Step 3:** Pick random  $x_i$ 's.  $A_s$  picks random  $x_i$  for all the other ring members  $1 \leq i \leq n, i \neq s$  uniformly and independently from  $\{0,1\}^b$ , and computes

$$y_i = g_i(x_i)$$

**Step 4:** Solve for  $y_s$ .  $A_s$  solves the following ring equation for  $y_s$  :

$$\begin{aligned}
 C_{k,v}(y_1, y_2, \dots, y_r) &= v \\
 z &= C_{k,v}(g_1(x_1), \dots, g_n(x_n)) \\
 &= E_k(g_n(x_n) \oplus E_k(\dots \oplus E_k(g_1(x_1) \oplus v))) \\
 y_s &= E_k(g_{s-1}(x_{s-1}) \oplus \dots \oplus E_k(g_1(x_1) \oplus v)) \\
 &\oplus E_k^{-1}(g_{s+1}(x_{s+1}) \oplus \dots \oplus E_k^{-1}(g_n(x_n) \oplus E_k^{-1}(z))) \\
 y_s &= E_k(y_{s-1} \oplus \dots \oplus E_k(y_1 \oplus v)) \\
 &\oplus E_k^{-1}(y_{s+1} \oplus \dots \oplus E_k^{-1}(y_n \oplus E_k^{-1}(v)))
 \end{aligned}$$

**Step 5:** Invert  $y_s$  using  $A_S$ 's trapdoor permutation.  $A_S$  uses her knowledge of the trapdoor to invert  $g_s$  on  $y_s$  to obtain  $x_s$  :

$$x_s = g_s^{-1}(y_s)$$

**Step 6:** Output the ring signature. The signature on the message  $m$  is defined to be

$$(P_1, P_2, \dots, P_r; v, x_1, x_2, \dots, x_r)$$

#### 4.3.2 Ring-Verify Phase

A verifier can check an alleged signature on message  $m$  as follows:

**Step 1:** Apply the trapdoor permutations. For  $i=1, 2, \dots, n$ , the verifier computes

$$y_i = g_i(x_i)$$

**Step 2:** Obtain  $k$ . The verifier hashes the message  $m$ :

$$k = h(m)$$

**Step 3:** Verify the ring equation. The verifier checks that the  $y_i$ 's satisfy

$$C_{k,v}(y_1, y_2, \dots, y_r) = v$$

If the ring equation is satisfied, the verifier **Accepts** the ring signature as valid. Otherwise, the verifier **Rejects**.

## 5. ANALYSIS OF THE PROPOSED SCHEME

The proposed scheme satisfies the following requirements.

- **Confidentiality:** An attacker cannot know the session keys  $K_A$  and  $K_S$  generated by the public key of a legal object. Even if the keys are exposed, confidentiality is ensured by the randomly generated keys  $f_A$  and  $r_S$ .

Table 1. Analysis of The Proposed Schemes

		FS[9]	GQ[10]	Schnorr[11]	RS[5]	Proposed Scheme 1	Proposed Scheme 2
Secrecy		○	○	○	○	○	○
		Based on discrete logarithm problem (NP Problem)	Based on discrete logarithm problem (NP Problem)	Based on discrete logarithm problem (NP Problem)	Based on discrete logarithm problem (NP Problem)	Based on polynomial (NP Problem)	Based on polynomial (NP Problem)
Efficiency		X	△	△	△	○	○
		Repeated operation	Exponential computation	Exponential computation	Exponential computation	Multiplication computation	Multiplication computation
Whether to transmit directly or request payment info		x	x	x	x	x	x
Computation Quantities	Registration	1M + H	1M	1M	1M+ $\infty$ E+H	1C	1C+ $\infty$ E+H
	Authentication	2M	4M	3M	1M+ $\infty$ E+H	5C	1C+ $\infty$ E+H
Traffic	Registration	2-pass + $\infty$	2-pass	2-pass	2-pass	2-pass	2-pass
	Authentication	3-pass + $\infty$	3-pass	3-pass	2-pass	3-pass	2-pass

○ : offer, secure, △ : usually-offer, × : non-offer, insecure

H: hash algorithm; E: symmetric key cryptography; U: public key cryptography; C: convolution multiplication

- **Mutual Authentication:** Mutual authentication is ensured by the Certificate  $Cert_A$  based on PKI and zero-knowledge proof based on NTRU.
- **Non-repudiation:** Non-repudiation is ensured by the signature generated by the secure key  $f_A$ .
- **Efficiency:** The proposed method is very efficient because it only uses addition, multiplication, and shift operations.
- **Secrecy:** It is computationally impossible to decode  $g_A$ ,  $f_A$ , and  $r_A$  using  $x$  and  $y$  because this is equivalent to the mathematical problem of decoding a small vector on a large lattice.

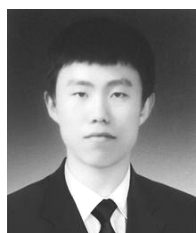
## 6. CONCLUSION

The development of IT technology is leading to the development of a wide range of services based on personal information; accordingly, a variety of authentication technologies have emerged for protecting personal information. However, the efficiency and payment information protection of these technologies must be guaranteed if NFC mobile payment services are to be widely used. In this paper, we proposed ring signature scheme based on NTRU for providing authentication between an bank and client where a zero-knowledge proof scheme based on NTRU ensures private financial information protection. In this paper, two cryptography schemes (ring signature, zero-knowledge proof) were chosen for providing to unconditionally anonymity in NFC mobile payment application services. but, two cryptography schemes are very inefficient in NFC mobile payment application services. Therefore, our scheme modified ring signature by NTRU for efficiency and secure. Our scheme satisfies the necessary require-

ments on NFC mobile payment environment. Therefore, our scheme could be effectively applied in an NFC mobile payment environment. However, since we do not have the source code of the proposed scheme, it is difficult to directly compare computational times or other numerical measures. In future work, we will compare our proposed method with previous models through an implementation of proposed scheme.

## REFERENCES

- [1] "Google Wallet: Security", Google, 2011
- [2] "MasterCard PayPass", MasterCard, 2011
- [3] J. Hoffstein, J. Pipher, J. H. Silverman, "NTRU : A Ring Based Public Key Cryptosystem", in Algorithmic Number Theory(ANTS III), 1998.
- [4] S.Goldwasser, SMicali and C.Rackoff, "The Knowledge Complexity of Interactive Proof Systems", SIAM Journal on Computing, 18(1989), pp.186-208.
- [5] R.L. Rivest, A. Shamir, Y. Tauman, "How to Leak a Secret", Advances in Cryptology-ASIACRYPT, 2001.
- [6] "A Study on the Development of Cryptosystems for the Next Generation", National Security Research Institute, 2006
- [7] S.Goldwasser, SMicali and C.Rackoff, "The Knowledge Complexity of Interactive Proof Systems", SIAM Journal on Computing, 18(1989), pp.186-208.
- [8] A.Shamir, "ID-Based Cryptosystems and Signature Schemes", Crypto'84, pp.47-53, 1985.
- [9] A.Fiat and A.Shamir, "How to Prove Yourself: Practical Solution to Identification and Signature Problem", Crypto'86, VFol 263, pp.186-194, 1986
- [10] L.C.Guillou and J.J.Quisquater, "A Paradoxical Identity-Based Signature Scheme Resulting from Zero-Knowledge", Crypto'88, p.216-231, 1988
- [11] C.P.Schnorr, "Efficient Signature Generation by Smart Card", Journal of Cryptology, pp.161-174, 1991.4
- [12] S.H Lim, J.W Jeon, J.I Jin, O.Y Lee, "Study on NFC Security Analysis and UICC Alternative Effect", Korea Information and Communications Society, 2011
- [13] Ernst Haselsteiner, Klemens Breitfuß, "Security in near field communication(NFC)", Workshop on RFID Security RFIDSec, 2006



### Sung-Wook Park

Sung-Wook Park received the B.S. and M.S. degrees in Department of Computer Software Engineering from Soonchunhyang University, Korea, in 2011 and 2013, respectively. He is now a Ph.D. candidate in Department of Computer Software Engineering from Soonchunhyang University, Korea. His research interests include NFC Security, NTRU Cryptography, Ultra Lightweight Cryptography, etc.



### Im-Yeong Lee

Im-Yeong Lee is corresponding author. He received the B.S. degrees in Department of Electronic Engineering from Hongik University, Korea, in 1981 and the M.S. and Ph.D. degrees in Department of Communication Engineering from Osaka University, Japan, in 1986 and 1989, respectively. From 1989 to 1994, he had been a senior researcher at ETRI (Electronics and Telecommunications Research Institute), Korea. Now he is a professor in Department of Computer Software Engineering from Soonchunhyang University, Korea. His research interests include Cryptography, Information theory, Computer & Network security.