Journal of Korea Multimedia Society Vol. 21, No. 4, April 2018(pp. 485-492)
https://doi.org/10.9717/kmms.2018.21.4.485

NFC 결제 환경에서 양자 컴퓨팅에 안전한 인증 및 키 분배 프로토콜

김종현[†], 박기성[††], 박영호[†††]

A Secure Quantum-Resistant Authentication and Key Distribution Protocol for NFC Payment Environments

JongHyun Kim[†], KiSung Park[††], YoungHo Park[†††]

ABSTRACT

Recently, the numerous authentication and key distribution protocol for NFC payment environment have been proposed using public key cryptosystems. However, these protocol are vulnerable to quantum computing attack because quantum computing can solve factoring and discrete logarithm problem effectively using Grover and Shor's algorithm. For these reason, the secure authentication and key distribution have become a very important security issue in order to prevent quantum computing attacks. Therefore, to ensure user's payment information and privacy, we propose a secure quantum resistant authentication and key distribution protocol for NFC payment environments.

Key words: NTRU, NFC Payment, Authentication, Key Distribution

1. 서 론

최근 NFC 기술의 발전 및 스마트폰 보급의 확대로 NFC 기술은 교통, 출입통제, 헬스케어, 티켓 및 지불 등 여러 분야에서 활발히 사용되고 있으며 TrendForce사에[1] 따르면 모바일 NFC 결제 시장의 경우 2018년에는 9800억 이상의 총 매출을 기록할 것으로 예상된다. 대표적인 NFC 기반 결제 서비스로는 삼성페이, 애플페이 및 알리페이 등이 있으며 삼성페이는 MST(Magnetic Secure Transmission) 기술을 사용하여 국내 모바일 사용자 약 644만 명에게 결제 서비스를 제공하고 있다. 따라서 NFC 결제 환경에서 안전한 거래를 위한 사용자 인증 및 키 분배는 반드시 보장되어야하는 보안 필수요소이다.

2017년 Chen 등[2]은 NFC 결제 환경에서 공격자의 위조 결제 및 가장 공격을 방어하기 위한 안전한 인증 방식을 제안하였으며 제안된 인증 방식은 ECC (Elliptic Curve Cryptography)를 사용하여 자원이 제약적인 기기에서 효율적으로 동작 가능하다. 그러나 양자 컴퓨터가 실현되면 Shor의 양자 소인수분해 알고리즘[3] 및 Grover의 양자 검색 알고리즘[4]을 통하여 소인수분해 문제와 이산대수 문제를 효율적으로 해결할 수 있으므로 기존의 NFC 결제 환경에서 ECC 및 RSA 기반 인증 방식은 심각한 보안 위협

※ Corresponding Author : YoungHo Park, Address: (41566) Daehak-ro 80, Bukgu, Daegu, Korea, TEL : +82-53-950-7842, E-mail : parkyh@knu.ac.kr
Receipt date : Dec. 19, 2017, Revision date : Feb. 5, 2018
Approval date : Mar. 5, 2018
[†] Department of Information Security, Graduate School, Kyungpook National University
(E-mail : dwjojo@eplatform.com)
[††] School of Electronics Engineering, Graduate School, Kyungpook National University
(E-mail : kisung2@ee.knu.ac.kr)
[†††] School of Electronics Engineering, Kyungpook National University
※ This research was supported by Basic Science Research Program through the National Research Foundation of Korea(NRF) funded by the Ministry of Science, ICT & Future Planning (2017R1A2B1002147).

에 노출될 수 있다. 따라서 유럽전기통신표준화기구 ETSI[5]와 미국표준기술연구소 NIST[6]는 이러한 양자 컴퓨팅 공격에 대비하여 양자 컴퓨팅 공격에 안전한 양자 후 암호시스템 준비를 권고하고 있으며 대표적인 양자 후 암호 방식으로 NTRU 공개키 암호가 있다.

NTRU 공개키 암호 방식[7]은 IEEE P1363.1 격자 기반 암호 표준[8]으로 기존의 ECC 공개키 암호 방식과 비교하여 동일한 안전성을 제공할 뿐만 아니라 효율적인 암호화 및 복호화 연산이 가능하여 다양한 환경에서 효율적으로 사용가능하다. 또한 격자의 가장 짧은 벡터를 찾는 어려움에 기반하여 안전성을 제공하고 양자 컴퓨팅 공격에 안전하여 최근 NTRU를 사용한 인증 및 키 분배 방식이 연구되고 있다[9].

본 논문에서는 NFC 결제 환경에서 양자 컴퓨팅 공격에 안전한 NTRU 기반 인증 및 키 분배 프로토콜을 제안한다. 또한 제안한 프로토콜은 중간자 공격, 재사용 공격, 사용자 가장 공격 및 양자 컴퓨팅 공격에 안전하며 상호인증을 제공하고 기존의 ECC 기반 공개키 암호 인증 방식보다 효율적이다.

2. 관련 연구

2.1 NFC 결제 시스템

NFC(Near Field Communication)는 2002년 소니와 NXP 반도체가 개발한 비접촉식 통신 기술로 13.56 MHz 주파수 대역을 사용하고 2003년 국제표준제정(ISO/IEC 18092)를 통하여 공식적으로 표준화되었다. 또한 NFC는 기존의 RFID 기술과 다르게 리더를 필요로 하지 않아 가격이 저렴하고 4~10cm 근거리 통신 특성으로 상대적으로 보안이 우수하여 현재 VISA, Apple pay, google pay, Alipay 및 Wechat pay 등과 같이 다양한 플랫폼에서 모바일 결제 수단으로 활용되고 있다.

NFC는 리더와 태그 역할을 모두 수행하여 P2P (Peer to Peer) 통신이 가능한 능동통신모드와 리더와 태그간의 통신을 지원하는 수동통신모드를 지원하며 Fig. 1은 NFC의 기본적인 리더, P2P 및 카드 에뮬레이션 동작 모드이다.

NFC 결제 시스템은 NFC를 지원하는 기기, POS 터미널, 서버로 구성되어 있으며 NFC의 기본 동작모드를 활용하여 결제를 수행한다. 먼저 POS 터미널은 NFC 리더기를 사용하여 NFC 기기에 결제 요청하고

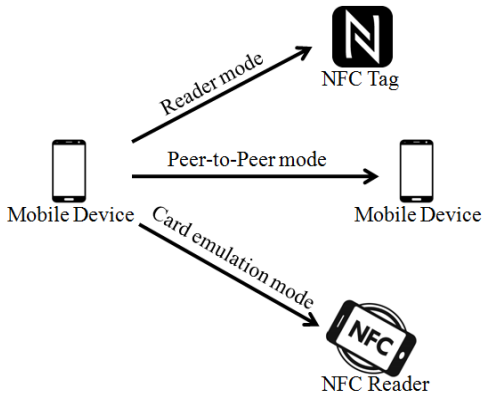

Fig. 1. Basic Operation of NFC.

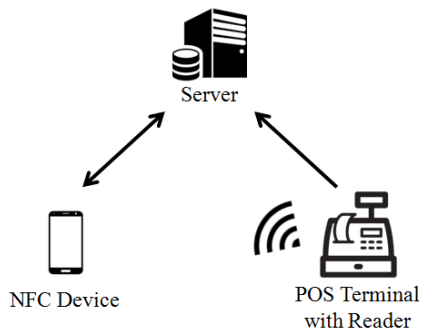

Fig. 2. NFC payment system.

NFC 기기는 POS 터미널의 리더기로 결제 정보를 전송한다. 또한 NFC 기기와 POS 터미널은 결제 및 거래 정보를 서버를 통하여 관리할 수 있다. NFC 결제 시스템의 구조는 Fig. 2와 같다.

2.2 양자 내성 암호체계

현재 양자 컴퓨팅에 안전한 암호체계는 격자 기반, 코드 기반, 해시 기반 및 다변수 암호가 있으며 대표적인 암호체계로는 코드 기반 암호체계 McEliece와 격자 기반 암호체계 NTRU가 있다. McEliece는 오류 정정 능력을 기반으로 하며 오류가 포함된 메시지를 오류 정정 부호를 사용하여 복호화 하고 NTRU는 격자에서 작은 벡터를 찾는 어려움을 기반으로 안전성을 제공하고 메시지를 복호화하는 암호 체계이다. 또한 McEliece 및 NTRU 암호 방식은 기존의 공개키 암호 방식과 비교하여 빠른 암호화 및 복호화 연산을 제공하므로 본 논문에서는 NTRU 공개키 암호 방식을 사용하여 효율적인 인증 및 키 분배 프로

토콜을 제안한다.

2.3 NTRU 기반 공개키 암호

NTRU 공개키 암호는 1996년 Jeffrey Hoffstein 등에 의해 제안된 격자 기반 양자 내성 공개키 암호 방식으로 현재 IEEE P1363.1 격자 기반 공개키 암호 표준이며 R-LWE를 기반으로 다항식 환 상에서 기본 연산을 수행한다. 또한 NTRU는 기존의 공개키 암호 방식인 RSA 및 ECC 등과 비교하여 동일한 안전성을 제공하며 다항식 컨볼루션 연산을 통한 빠른 암호화 및 복호화가 가능하므로 자원이 제약적인 기기에서 효율적으로 동작할 수 있다. NTRU 공개키 암호 방식에 사용되는 다항식 컨볼루션 연산, 키 생성, 암호화 및 복호화, 안전성, 성능 비교는 다음과 같다.

2.3.1 다항식 컨볼루션 연산

다항식 컨볼루션 연산은 NTRU에 사용되는 기본 연산으로 $Z[X]$를 정수들의 집합 Z에 대한 모든 다항식들의 집합이라 할 때 몫 환은 $R=Z[X]/(X^N-1)$로 정의되며 환 R에 속하는 원소 a는 벡터 또는 다항식으로 표현 가능하며 다음 식 (1)과 같다.

$$a(X)=\sum_{i=0}^{N-1} a_i X^i=[a_0, a_1, ..., a_{N-1}] \tag{1}$$

환 R에 속하는 원소 a와 b에 대한 컨볼루션 곱셈 연산 $c(c(X)=a(X)*b(X))$는 다음 식 (2)와 같으며 이때 $X^N\equiv 1 \bmod (X^N-1)$이다. 또한 NTRU에 사용되는 다항식 컨볼루션 연산은 원소 a 또는 b 중 어느 하나가 작은 계수를 가지므로 N^2개의 정수 곱셈을 요구하지 않아 효율적인 연산이 가능하다.

$$c_k=\sum_{i=0}^{k} a_i b_{k-1}+\sum_{i=k+1}^{N-1} a_i b_{N+k-1}=\sum_{i+j\equiv k(\bmod N)} a_i b_j \tag{2}$$

2.3.2 키 생성

NTRU의 키 생성 단계는 다항식 환 R에 속하며 작은 계수들을 갖는 $N-1$차의 다항식 $f\in L_f$, $g\in L_g$를 임의로 선택하고 $f_q^{-1}*f\equiv 1(\bmod q)$, $f_p^{-1}*f\equiv 1(\bmod p)$ 및 $h=pf^{-1}*g \pmod q$를 계산한다. 이 때 f와 g는 비밀키이며 h는 공개키이다.

2.3.3 암호화

NTRU 메시지 암호화 단계는 평문 다항식을 $m\in L_m$을 선택하고 작은 계수를 갖는 $N-1$차의 다항식 $r\in L_r$을 임의로 선택한 후 암호문 $e=r*h+m \pmod q$를 계산한다.

2.3.4 복호화

암호문 e를 복호화하기 위하여 a의 계수들이 $A\le a_i<A+q$를 만족하는 $a=e*f \pmod q$를 계산하고 $m=a \pmod p$ 연산으로 평문 m을 얻는다. 이 때 A는 고정된 값으로 파라미터 값에 의존하여 변하며 자세한 복호화 단계는 식 (3)과 같다.

$$\begin{aligned} a&=e*f \pmod q \\ &=(r*h+m)*f \pmod q \quad (\because e=r*h+m) \\ &=pr*g+m*f \pmod q \quad (\because h*f=pg*f^{-1}*f=pg) \\ &=pr*g+m*f=pr*g+m*(1+pF) \end{aligned} \tag{3}$$

식 (3)의 값 $pr*g+m*f \bmod q$에 대해서 매개 변수를 적절히 선택하여 다항식의 계수들이 q보다 작은 길이의 범위 내에 놓이도록 조정할 수 있으므로 $a=pr*g+m*(1+pF)$를 얻을 수 있다. 따라서 다항식 a를 $\bmod p$ 연산하여 암호문 e를 복호화 가능하다.

2.3.5 성능비교 및 안전성 분석

NTRU의 컨볼루션 연산은 기존 공개키 암호 연산보다 빠르고 효율적이며 기존의 공개키 암호와 NTRU의 키 사이즈 및 연산 속도 비교 분석은 Table 1과 같다.

Graham 등[10]과 Jaulmes 등[11]은 NTRU 공개키 암호가 meet-in-the-middle attack에 취약하고 CCA(Chosen Ciphertext Attack)로 비밀키가 복구되는 문제점이 있음을 입증 하였다. 따라서 NTRU Crytosystems[12, 13] 2002년 CCA와 meet-in-the middle attack에 안전한 NTRU 패딩 암호화 방식을 제안하였으나 2003년 Howgrave-Graham[14]은 NTRU 패딩 암호화 방식이 복호화 실패 가능성을 고려하지 않아 증명가능 안전성으로 안전성이 입증되지 않음을 밝히고 이를 개선한 NEAP NTRU 패딩 암호화 방식을 제안하였다. 따라서 NTRU는 증명가능 안전성으로 안전성이 입증된 안전한 공개키 암호화 방식이다.

Table 1. Performance analysis of NTRU with existing public key cryptosystems

Algorithm	Message Size (bits)	Key size (bits)	Key generation (ms)	Encryption (ms)	Decryption (ms)
RSA1024	1024	1024	1432	4.28	48.5
ECC168	160	169	65	140	67
NTRU263	416	1841	19.8	1.9	3.5

3. 제안한 프로토콜

본 논문에서는 양자 컴퓨팅 공격에 취약한 기존의 ECC 기반 인증 방식을[1, 14] 개선하기 위하여 NTRU 기반 인증 및 키 분배 프로토콜을 제안한다. 제안한 방식은 양자 컴퓨팅 공격, 가장 공격, 중간자 공격 등 다양한 공격에 안전하며 상호 인증을 제공하고 자원이 제약적인 환경에 효율적으로 활용될 수 있다. 제안한 방식에서 사용된 시스템 파라미터 및 프로토콜은 다음과 같다.

3.1 시스템 파라미터

- $*$: 컨볼루션 곱셈
- N : 다항식 환 $R=Z[X]/(X^N-1)$의 차수를 정하는 파라미터 (N=소수)
- p, q : $\gcd(p,q)=1$을 만족하는 공개 파라미터
- f, g : 비밀키 다항식, $f \in L_f, g \in L_g$
- f_p^{-1}, f_q^{-1} : 비밀키 f의 역함수
- h : 공개키, $h=pf_q^{-1} * g \in Z_q[X]/(X^N-1)$
- r : 임의의 다항식, $r \in L_r$
- L_f, L_g, L_r : 잘려진 다항식 환 R의 부분집합
- SK : 세션 키

3.2 NTRU 기반 인증 및 키 분배 프로토콜

제안하는 인증 및 키 분배 프로토콜은 Fig. 3과 같으며 각 단계는 다음과 같다.

- 1단계 : 사용자는 $f_A \in L_f$, $g_A \in L_g$와 임의의 값 $r_A \in L_r$를 선택하고 f_A의 역원 f_{Ap}^{-1}와 f_{Aq}^{-1} 및 공개키 $h_A = f_{Aq}^{-1} * g_A \pmod q$, $x_A = g_A * r_A$를 계산하고 공개키 h_A와 x_A를 리더기에 전송한다.
- 2단계 : 사용자의 정보를 받은 리더기는 사용자의 공개키 h_A를 검증하여 올바른 사용자인지 확인하

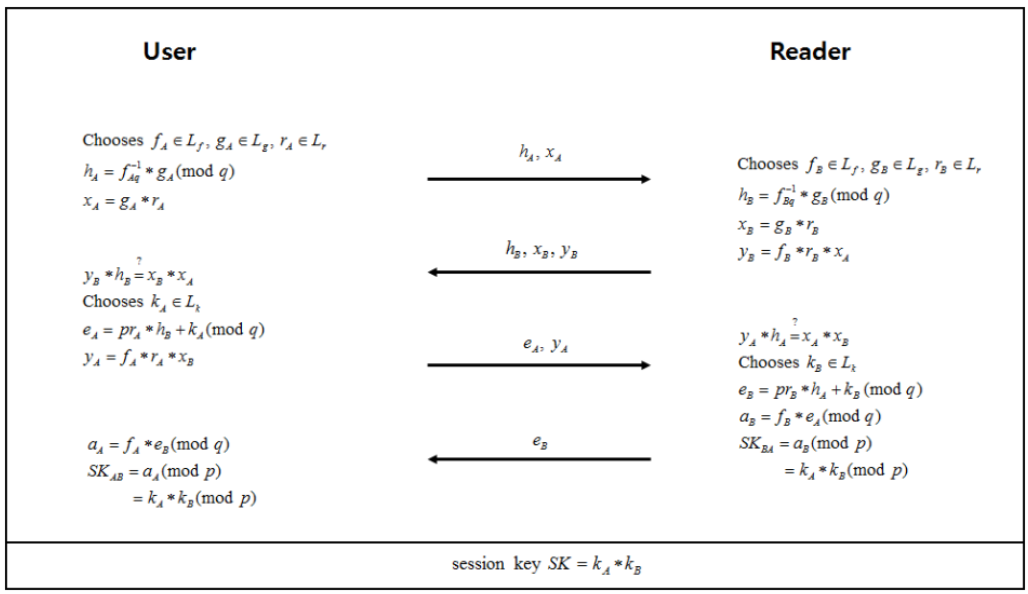

Fig. 3. Proposed protocol.

고 $f_B \in L_f$, $g_B \in L_g$와 임의의 값 $r_B \in L_r$를 선택한 후 f_B의 역원 f_{Bp}^{-1}와 f_{Bq}^{-1} 및 공개키 $h_B = f_{Bq}^{-1} * g_B \pmod q$를 계산한다. 그 후 리더기는 $x_B = g_B * r_B$와 $y_B = f_B * r_B * x_A$를 계산하여 사용자에게 h_B, x_B와 y_B를 전송한다.

• 3단계 : 리더기의 정보를 받은 사용자는 리더기의 공개키 h_B를 검증한 후 $y_B * h_B$를 계산하여 $x_B * x_A$와 값이 일치하는지 확인한다. 또한 임의의 키인 k_A를 선택하고 $e_A = pr_A * h_B + k_A \pmod q$, $y_A = f_A * r_A * x_B$를 계산하여 e_A와 y_A를 리더기에 전송한다.

• 4단계 : 사용자의 정보를 받은 리더기는 $y_A * h_A$를 계산하여 $x_A * x_B$와 값이 일치하는지 확인하고 임의의 키인 k_B를 선택한 후 $e_B = pr_B * h_A + k_B \pmod q$로 암호화 하여 사용자에게 e_A를 전송한다. 그 후 리더기는 $a_B = f_B * e_A \pmod q$를 계산하고 a_B를 사용하여 암호문을 복호화 한 후 세션키 $SK_{BA} = k_A * k_B \pmod p$를 계산한다.

• 5단계 : 리더기의 정보를 받은 사용자는 a_A를 사용하여 암호문을 복호화 한 후 세션키 $SK_{AB} = k_A * k_B \pmod p$를 계산한다.

4. 분 석

본 논문에서는 제안한 프로토콜과 기존의 Liao 등과 Chen 등이 제안한 프로토콜의 연산량을 비교 분석하였으며 informal 분석으로 제안한 프로토콜의 안전성을 분석하였다.

4.1 연산량 분석

제안한 NTRU 기반 프로토콜은 컨볼루션 곱을 활용하여 기존의 ECC 기반 인증 프로토콜[1, 13]과 비교하여 암호화, 복호화 및 키 생성 단계에서 효율인 연산이 가능하다. Table 2는[15] 리눅스 환경에서 (500MHZ celeron 프로세서 사용) ECC와 NTRU의 성능을 비교한 것이며 NTRU는 ECC 보다 암호화 연산은 약 80배, 복호화 연산은 약 20배 정도 빠르다.

제안한 프로토콜은 매 세션마다 임의의 다항식을 재생성 하므로 비밀번호 변경 단계가 필요하지 않다. Table 3은 기존의 ECC 기반 인증 프로토콜과 제안한 프로토콜의 연산량 비교분석을 한 것이며 Chen 등의 방식은 POS와 은행을 모두 Reader로 포함하여 분석하였다. Laio와 Hsiao의 방식은 총 12번의 ECC 곱셈 연산, 3번의 ECC 덧셈 연산, 8번의 해시 연산이 요구되며 Chen 등의 방식은 총 8번의 ECC 곱셈 연산, 4번의 ECC 덧셈 연산, 2번의 해시 연산 및 4번의 대칭키 연산이 필요하다. 그러나 제안하는 방식은 18번의 컨볼루션 연산과 10번의 모듈러 연산만 필요로 하므로 NFC 결제 환경에 보다 효율적인 인증 및 키 분배 방식이다.

4.2 안전성 분석

본 논문에서는 informal 분석으로 기존의 방식과 제안한 방식의 안전성을 분석하였다. 기존의 Liao and Hsiao 및 Chen 등의 방식은 내부자 공격과 양자 컴퓨팅 공격에 취약하나 제안하는 방식은 기밀성 및

Table 2. Performance of ECC and NTRU (500MHZ Celeron processor)

	ECC112	ECC168	ECC196	NTRU167	NTRU263	NTRU503
Key generation speed(ms)	25	65	115	8.3	19.8	71.2
Encryption speed(ms)	60	140	255	0.8	1.9	6.6
Decryption speed(ms)	26	67	119	1.4	3.5	12.7

Table 3. Performance analysis

Scheme	User	Reader	Total
Liao and Hsiao [16]	$7T_{ecm}$, $2T_{eca}$, $6T_h$	$5T_{ecm}$, $1T_{eca}$, $2T_h$	$12T_{ecm}$, $3T_{eca}$, $8T_h$
Chen et al. [2]	$3T_{ecm}$, $1T_{eca}$, $1T_h$	$5T_{ecm}$, $3T_{eca}$, $1T_h$, $4T_{sym}$	$8T_{ecm}$, $4T_{eca}$, $2T_h$, $4T_{sym}$
Our Protocol	$9T_c$, $5T_m$	$9T_c$, $5T_m$	$18T_c$, $10T_m$

(T_c : convolution operation T_h: one-way hash operation, T_{ecm} : ECC multiply operation, T_{eca} : ECC addition operation, T_m : modulo operation, T_{pair} : pairing operation, T_{sym} : symmetric enc/dec operation)

Table 4. Informal analysis

	Liao and Hsiao [16]	Chen et al.[2]	Our Protocol
Confidentiality	○	○	○
Integrity	○	○	○
Insider attack	×	○	○
Mutual authentication	○	○	○
Man-in-the-middle attack	○	○	○
User impersonation attack	○	○	○
Replay attack	○	○	○
Session key disclosure attack	○	○	○
Quantum computing attacks	×	×	○

○ : ensuring security property, × : do not ensuring security property

무결성을 보장하며 상호 인증을 제공할 뿐만 아니라 또한 중간자 공격, 재사용 공격, 세션키 노출 공격, 사용자 가장 공격 및 양자 컴퓨팅 공격 등 여러 가지 공격에 안전하다. 기존의 인증 방식과 informal 안전성 분석 비교는 Table 4와 같다.

• 기밀성(Confidentiality)

기밀성은 허락 되지 않은 사용자 또는 객체가 실제 전송되는 데이터의 정보를 알 수 없어야 함을 의미하며 제안한 방식은 NTRU 기반 공개키 암호화 방식을 사용하므로 공격자는 비밀키 없이 암호문을 복호화 할 수 없다. 또한 세션키가 노출되더라도 r과 k 값이 세션마다 임의로 생성되므로 제안하는 방식에서 기밀성은 보장된다.

• 무결성(Integrity)

무결성은 허락 되지 않은 사용자 또는 객체가 데이터 정보를 수정할 수 없어야 함을 의미하며 제안한 방식은 NTRUSign을 통해 메시지의 서명 값을 생성하여 전달하므로 메세지가 위·변조가 되더라도 서명 검증 과정에서 확인이 가능하다. 또한 사용자와 리더기 간의 상호 인증을 제공하므로 제안한 방식은 데이터 무결성을 보장한다.

• 상호 인증(Mutual Authentication)

제안한 방식에서 사용자와 리더는 x, y와 공개키 h를 사용하여 $y_B * h_B = x_B * x_A$와 $y_A * h_A = x_A * x_B$를 계산하고 값이 일치하면 서로를 인증한다. 또한 공격자는 사용자의 개인키 없이 x와 y를 알 수 없으므로 제안한 방식은 상호 인증을 제공한다.

• 중간자 공격(Man in the Middle Attack)

중간자 공격은 공격자가 송수신자 사이에서 네트워크 통신을 조작하여 통신 내용을 도청하거나 조작하는 공격이며 제안한 방식은 사용자와 리더기 간의 상호 인증 및 데이터 무결성을 제공하므로 중간자 공격에 안전하다.

• 사용자 가장 공격(User Impersonation Attack)

제안한 방식에서 공격자는 사용자의 비밀키 없이 사용자의 공개키로 암호화된 암호문을 복호화 할 수 없으므로 사용자로 가장 할 수 없다.

• 재사용 공격(Replay Attack)

재사용 공격은 사용자가 사용한 정보를 공격자가 도청하여 다음 세션에 재사용하는 공격으로 제안한 방식은 r과 k를 매 세션마다 임의로 생성하여 사용하므로 한번 사용한 정보를 재사용할 수 없다.

• 세션키 공개 공격(Session Key Disclosure Attack)

제안한 방식에서 사용자의 세션키가 공격자에 노출되더라도 공격자는 NTRU의 격자에서 작은 벡터를 찾는 어려움을 해결할 수 없으므로 세션키 SK를 사용하여 사용자의 개인키 또는 정보를 얻을 수 없다.

• 양자 컴퓨팅 공격(Quantum Computing Attacks)

제안한 NTRU 기반 인증 및 키 분배 방식은 소인

수 분해 및 이산대수문제가 아닌 격자에서 작은 벡터를 찾는 어려움에 기반하여 안전성을 제공하므로 양자 컴퓨팅 공격에 안전하다.

5. 결 론

오늘날 모바일 결제 시장은 매년 확대되고 있으며 NFC 기술은 이러한 모바일 결제 시장의 핵심기술로 사용되고 있다. 그러나 기존의 NFC 결제 환경에서의 암호시스템은 소인수분해 및 이산대수의 어려움에 기반하여 안전성을 제공하므로 양자컴퓨터가 실현되면 양자 소인수분해 알고리즘 및 검색 알고리즘에 의하여 효율적으로 해결될 수 있다. 따라서 NFC 결제 환경에서 사용자의 프라이버시를 보장하고 안전한 통신을 위하여 양자 컴퓨터가 실현되기 이전에 양자 컴퓨팅 공격에 안전한 인증 및 키 분배 방식이 필요하다.

본 논문에서는 최근 제안된 NFC 결제 환경에서 ECC 기반 Li 등의 인증 및 키 분배 방식이 양자 컴퓨팅 공격에 취약함을 지적하고 이를 개선하기 위하여 NTRU 기반 인증 및 키 분배 방식을 제안한다. 또한 제안한 방식은 중간자 공격, 사용자 가장 공격, 재사용 공격 및 양자 컴퓨팅 공격 등과 같은 다양한 공격에 안전하며 상호 인증, 무결성 및 기밀성을 제공한다. 따라서 제안하는 방식은 컨볼루션 연산을 기반으로 저사양 환경에서 효율적인 뿐만 아니라 다양한 환경에 적용가능한 안전한 인증 및 키 분배 방식이다.

REFERENCE

[1] TrendForce Says Global Mobile Payment Market to Reach US$620 Billion in 2016 with Apple and Samsung Staking Large Claims in the Ecosystem, https://press.trendforce.com/node/prints/2298 (accessed Dec., 17, 2017).

[2] X. Chen, K. Choi, and K.J. Chae, “A Secure and Efficient Key Authentication Using Bilinear Pairing for NFC Mobile Payment Service,” *Wireless Personal Communications*, Vol. 97, No. 1, pp. 1-17, 2017.

[3] P.W. Shor, “Algorithms for Quantum Computation: Discrete Logarithms and Factoring,” *Proceeding of 35th Annual Symposium Foundations of Computer Science and IEEE Computer Society and Los Alamitos and CA*, pp. 124-134, 1994.

[4] L.K. Grover, “A Fast Quantum Mechanical Algorithm for Database Search,” *Proceedings of the 28th Annual ACM Symposium on Theory of Computing*, pp. 212-219, 1996.

[5] ETSI, *Quantum Safe Cryptography and Security*, NO. 979-10-92620-09-0, 2015.

[6] NIST, *Report on Post-Quantum Cryptography*, IR 8105, 2016.

[7] J. Hoffstein, J. Pipher, and J.H. Silverman, “NTRU: A Ring-Based Public Key Cryptosystem,” *ANTS 1998: Algorithmic Number Theory,* Vol. 1423, pp. 267-288, 1998.

[8] IEEE, *IEEE P1363.1 Draft 10: Draft Standard for Public Key Cryptographic Techniques Based on Hard Problems over Lattices*, International Association for Cryptologic Research Eprint Archive, 2008.

[9] S.H. Jeong, K.K. Lee, and Y.H. Park, “Secure NTRU-based Authentication and Key Distribution Protocol in Quantum Computing Environments,” *Journal of Korea Multimedia Society*, Vol. 20, No. 8, pp. 1321-1329, 2017.

[10] NTRU Cryptosystems, *A Meet-In-The-Middle attack on an NTRU Private Key*, Technical Report, 2003.

[11] E. Jaulmes and A. Joux. “A Chosen Ciphertext Attack against NTRU,” *Proceeding of 20th Annual International Cryptology Conference Santa Barbara,* pp. 21-36, 2000.

[12] J. Hoffstein and J. Silverman. “Optimizations for NTRU,” *Proceedings of Public Key Cryptography and Computational Number Theory*, pp. 77-86, 2001.

[13] NTRU Cryptosystems, *Protecting NTRU against Chosen Ciphertext and Reaction Attacks,* Technical Report, 2000.

[14] N.H. Graham, J.H. Silverman, A. Singer, and W. Whyte. “NAEP: Provable Security in the Presence of Decryption Failures,” *IACR*

Cryptology, 2003.
[15] Practical Comparison of Fast Public-key Cryptosystems, http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.96.5694& rep=rep1&type=pdf (accessed Feb., 05, 2018).
[16] Y.P. Liao and C.M. Hsiao, "An Novel Multi-server Remote User Authentication Scheme using Self-certified Public Keys for Mobile Clients," *Future Generation Computer Systems*, Vol. 29, No. 3, pp. 886-900, 2013.

김 종 현

2010년 2월 계명대학교 경영정보학 학사
2014년 2월 계명대학교 경영정보학 석사
2016년 3월~현재 경북대학교 대학원 정보보호학과 박사과정
2002년~2008년 명신컴퓨터시스템 대표이사
2008년~2014년 (주)드림웨어시스템 대표이사
2014년~현재 (주)이튜 총괄이사
관심분야 : 정보보호, 네트워크보안, 모바일 컴퓨팅

박 기 성

2015년 2월 경북대학교 산업전자전기공학부 학사
2017년 2월 경북대학교 대학원 전자공학부 석사
2017년 3월~현재 경북대학교 대학원 전자공학부 박사과정
관심분야 : 정보보호, 네트워크보안, PQ암호

박 영 호

1989년 2월 경북대학교 전자공학과 학사
1991년 2월 경북대학교 전자공학과 석사
1995년 2월 경북대학교 전자공학과 박사
1996년~2008년 상주대학교 전자전기공학부 교수
2003년~2004년 Oregon State Univ. 방문교수
2008년~2014년 경북대학교 산업전자공학과 교수
2014년~현재 경북대학교 전자공학부 교수
관심분야 : 정보보호, 네트워크보안, 모바일 컴퓨팅