Journal of Korea Multimedia Society Vol. 20, No. 11, November 2017(pp. 1768-1775)
https://doi.org/10.9717/kmms.2017.20.11.1768

# SIP에서 NTRU 기반 인증 및 키 분배 프로토콜

정성하[†], 박기성[††], 이경근[†††], 박영호[††††]

# A NTRU-based Authentication and Key Distribution Protocol for SIP

SeongHa Jeong[†], KiSung Park[††], KyungKeun Lee[†††], YoungHo Park[††††]

## ABSTRACT

The SIP(Session Initiation Protocol) is an application layer call signaling protocol which can create, modify and terminate the session of user, and provides various services in combination with numerous existing protocols. However, most of cryptosystems for SIP cannot prevent quantum computing attack because they have used ECC(Elliptic Curve Cryptosystem). In this paper, we propose a NTRU based authentication and key distribution protocol for SIP in order to protect quantum computing attacks. The proposed protocol can prevent various attacks such as quantum computing attack, server spoofing attack, man-in-the middle attack and impersonation attack anonymity, and our protocol can provide user's anonymity.

**Key words:** Post Quantum, NTRU, Key Distribution Protocol, Session Initiation Protocol

## 1. 서 론

SIP는 1999년 IETF(Internet Engineering Task Force) 네트워크 워킹 그룹에 의해 제안[1, 2]된 시그널링 프로토콜로 인터넷 음성, 영상 전화 및 메신저와 같은 응용 서비스의 세션을 구성하고 관리하기 위해 사용된다. 또한 SIP는 request/response 구조로 TCP와 UDP에 모두 사용할 수 있으며 SIP URL을 사용하여 사용자를 구분하므로 IP주소에 종속되지 않고 서비스를 제공받을 수 있다. 따라서 SIP는 인터넷에 사용되는 다양한 프로토콜과 결합하여 사용자에게 효율적인 세션 관리 및 서비스를 제공할 수 있다. 대표적인 서비스로는 mVoIP(mobile Voice Over Internet Protocol)가 있으며 이는 무선 인터넷망을 활용해 무료로 음성통화를 하는 서비스로 카카오톡, 라인 및 facebook 등의 스마트폰 메신저에서 사용되고 있으며 facebook의 경우 현재 사용자 수가 약 18억 명에 이르렀다. 만약 SIP의 보안이 취약하면 메신저를 사용하는 모든 사용자들은 프라이버시를 보장받지 못한다.

현재 사용 중인 대부분의 SIP 암호 시스템들은 RSA(Rivest-Shamir-Adleman) 및 ECC를 사용하여 소인수분해와 이산대수의 어려움을 기반으로 안전성을 제공하고 있으며 2016년 Mishira 등[3]과 Arshad[4]은 효율적인 인터넷 음성 및 멀티미디어 서비스를 제공하기 위하여 ECC 기반 SIP 인증 방식을 제안하

※ Corresponding Author : YoungHo Park, Address: (702-701) 80 Daehakro, Bukgu, Daegu, Korea, TEL : +82-53-950-7842, FAX : +82-53-950-5505, E-mail : par-kyh@knu.ac.kr
Receipt date : Sep. 13, 2017, Revision date : Oct. 17, 2017
Approval date : Oct. 30, 2017
[†] School of Electronics, Kyungpook National University, (E-mail : jeongsh1128@gmail.com)
[††] School of Electronics, Kyungpook National University (E-mail : kisung2@ee.knu.ac.kr)
[†††] Samsung Electronics inc, (E-mail : crypto.knu@gmail.com)
[††††] School of Electronics, 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).

였다. 그러나 양자 컴퓨터가 실현되면 Peter W. Shor [5]의 양자 소인수분해 알고리즘 및 Lov K. Grover [6]의 양자 검색 알고리즘을 사용하여 소인수분해 문제와 이산대수 문제를 효율적으로 계산할 수 있게 되므로 이산대수 문제를 기반으로 하는 ECC를 사용한 SIP 방식은 심각한 보안 위협에 노출될 수 있다.

양자 컴퓨팅 공격에 대비하여 ETSI[7] 및 NIST [8] 등은 양자 컴퓨터가 실현되기 이전에 양자 컴퓨팅 공격에 안전한 양자 후 암호를 준비하고 실행하여 방어 체계를 갖추어야 한다고 권고하고 있으며 현재 주목 받는 양자 후 공개키 암호 시스템은 코드 및 격자(lattice) 기반 암호가 있다. 격자 기반 암호 표준인 NTRU 공개키 암호는 1996년 Jeffrey Hoffstein [9] 등에 의해 제안되었으며 기존의 공개키 암호와 비교하여 동일한 안전성을 제공하면서 암호화 및 복호화 속도가 빠르며 양자 컴퓨팅 공격에 안전하다 [10,11].

본 논문에서는 양자 컴퓨팅 공격에 취약한 기존의 ECC 기반 SIP 인증 방식의 문제점을 개선하기 위해 양자 내성을 가지는 NTRU 공개키 암호를 활용하여 인증 및 키 분배 프로토콜을 제안한다. 제안한 프로토콜은 양자 내성 외에도 사용자와 서버간의 로그인 및 상호인증 과정과 임의의 다항식을 매 세션마다 재생성하여 기존 SIP 키 분배 프로토콜[12]에 취약할 수 있는 중간자 공격, 사용자 가장 공격 등에 안전하며 사용자 익명성을 보장한다.

## 2. 관련 연구

### 2.1 SIP(Session Initiation Protocol)

SIP는 인터넷전화 및 메신저와 같은 멀티미디어 응용 서비스의 세션을 구성하고 관리하기 위하여 사용되는 시그널링 프로토콜로 IETF RFC 3261 표준 [2]으로 채택되었으며 SIP의 필수 구성요소는 다음과 같다.

- SIP UA(user agent) : 통신의 주체로 SIP 요청 메시지를 생성하는 UAC(user agent client)와 수신된 요청 메시지에 응답하는 UAS(user agent server)로 동작한다.
- Proxy/Redirect Server : UAC가 call을 요청하는 INVITE 메시지를 UAS에게 전달해 주는 기능을 한다. Proxy Server는 요청받은 INVITE 메시지를 목적지까지 포워딩 해주는 역할을 하며 re-direct server는 UAS에 대한 정보를 UAC에게 전달해 주어 UAC가 UAS에게 직접 INVITE 메시지를 보낼 수 있도록 해주는 역할을 한다.
- Registrar Server : 사용자는 registrar server에 REGISTER 메시지를 전송함으로 자신의 위치정보를 location server에 등록할 수 있다.
- Location Server : UA의 실질적인 위치를 저장하고 있는 서버이다.

두 사람간의 통신을 위해서 SIP를 사용하여 사용자간의 세션을 설정하고 종료하는 과정은 Fig. 1과 같다[13].

### 2.2 NTRU 기반 공개키 암호

NTRU 공개키 암호는 1996년 Jeffrey Hoffstein 등에 의해 제안[9]되었으며 R-LWE를 기반으로 하는 격자 기반 공개키 암호 체계로 기본 연산은 다항식 환 상에서 이루어진다. 또한 현재 널리 사용되는 공개키 암호인 RSA, ECC 등과 비교하여 동일한 안정성을 제공하면서 암·복호화 속도가 빠르며 양자 컴퓨팅 공격에 안전하다[7,10].

#### 2.2.1 다항식 컨볼루션 연산

$Z$를 정수들의 집합이라고 하자. $Z[X]$로 표시되는 $Z$에 대한 다항식 링은 $Z$의 계수들을 갖는 모든 다항식들의 집합이다. 몫 링 $R=Z[X]/(X^N-1)$로 정의한다. $R$에 속하는 원소 $a$는 다항식 또는 벡터로서 다음 식 (1)과 같다.

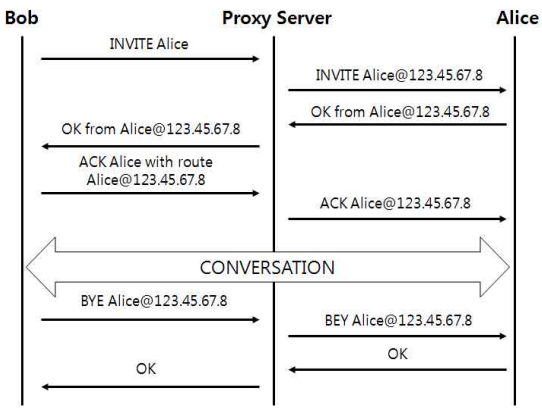


Fig. 1. SIP Protocol.

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

$R$에 속하는 원소 $a$와 $b$에 대한 컨볼루션 곱 $c(c(X)=a(X)*b(X))$는 다음 식 (2)와 같다.

$$c_k=\sum_{i=0}^{k}a_ib_{k-1}+\sum_{i=k+1}^{N-1}a_ib_{N+k-1}=\sum_{i+j\equiv k(\mathrm{mod}\,N)}a_ib_j \quad (2)$$

여기서 $X^N\equiv 1\mathrm{mod}(X^N-1)$이다.

이 연산은 $N^2$개의 정수 곱셈을 필요로 하여 그 연산량이 많다. 그러나 NTRU에 사용되는 다항식 컨볼루션 연산은 일반적으로 $a$또는 $b$ 중 어느 하나가 작은 계수를 가지게 된다. 따라서 $a*b$의 계산은 매우 빠르다.

2.2.2 NTRU 기반 공개 키 암호체계

- NTRU는 3가지 공개 파라미터$(N,p,q)$를 가진다 ($p$와 $q$의 최대공약수는 1이고, $p\ll q$임).
- 다항식의 계수들은 $\mathrm{mod}\,p$ 또는 $q$로 감산된다.
- $f^{-1}\,(\mathrm{mod}\,q)$ 로 표시되는 다항식 $f$의 $\mathrm{mod}\,q$ 상의 역원은 $f*f^{-1}\equiv 1\,(\mathrm{mod}\,q)$를 만족하는 다항식이다.

IEEE P1363.1 표준 초안[10]은 NTRU에 대한 몇 가지 전형적인 파라미터 집합을 제안하는데 그 중 하나는 $(N,p,q)=(251,2,197)$이다.

2.2.3 키 생성

$R$에 속하며 작은 계수들을 갖는 $N-1$차의 다항식 $F,g$를 임의로 선택한다. 그 후 $F$를 사용하여 $F_q*f\equiv 1\,(\mathrm{mod}\,q)$와 $F_p*f\equiv 1(\mathrm{mod}\,p)$를 계산한다. 공개키 $h$는 다항식 $g$를 이용하여 $h=pf^{-1}*g\ (\mathrm{mod}\,q)$로 계산한다.

2.2.4 암호화

메시지를 나타내는 다항식을 $m$이라고 할 때 작은 계수를 갖는 $N-1$차의 다항식 $r$을 임의로 선택하고 $e=r*h+m\ (\mathrm{mod}\,q)$를 계산한다.

2.2.5 복호화

$e$를 복호화하기 위해 먼저 $a=e*f\ (\mathrm{mod}q)$ 를 계산한다($a$의 계수들이 $A\le a_i<A+q$를 만족하도록 선택한다. 이때 $A$의 값은 고정되며 나머지 파라미터에 의존하는 간단한 공식에 의해 결정됨). 평문 $m$은 $m=a\ (\mathrm{mod}\,p)$ 로 복구한다.

2.1.6 복호화의 유효성

복호화 과정의 다항식 $a$는 다음 식 (3)과 같다.

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

최종 다항식 $pr*g+m*f\,\mathrm{mod}\,q$ 에 대해서 매개 변수를 적절히 선택하여 계수들이 $q$보다 작은 길이의 범위 내에 놓이도록 조정할 수 있다. 따라서 $a$에 대해 다음 식 (4)와 같다.

$$a=pr*g+m*f=pr*g+m*(1+pF) \quad (4)$$

즉 다항식 $a$는 $\mathrm{mod}\,q$에 대해서가 아닌 정확하게 등식이 성립하므로 $m=a\ (\mathrm{mod}\,p)$가 되어 메시지를 복호화 한다.

## 3. 제안한 프로토콜

본 논문에서는 SIP에서 ECC를 활용한 기존의[3, 4] 인증 및 키 분배 프로토콜에 취약점인 양자 컴퓨팅 공격을 개선하기 위하여 양자 컴퓨팅 공격에 안전한 NTRU를 활용한 인증 및 키 분배 프로토콜을 제안한다.

### 3.1 시스템 계수

제안한 프로토콜에서 사용하는 시스템 계수는 다음과 같다.

- $*$: 컨볼루션 곱셈
- $N$: 잘려진 다항식 환 $R=Z[X]/(X^N-1)$의 차수를 정하는 차원 파라미터 값($N$=소수)
- $p,q$ : $\gcd(p,q)=1$을 만족하는 공개 값
- $f,g$ : 비밀키 다항식, $f\in L_f, g\in L_g$
- $f_p^{-1}, f_q^{-1}$ : 비밀키 $f$의 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 $R$의 부분집합
- $SC$ : 스마트카드
- $B$ : 생체 정보
- $H(.)$ : 해쉬 함수

- $\oplus$ : XOR 연산
- $SK$ : 세션 키

### 3.2 NTRU 인증 및 키 분배 프로토콜

제안하는 프로토콜은 등록, 로그인, 인증 및 키 분배 단계로 이루어진다.

#### 3.2.1 등록 단계

등록 단계에서는 사용자가 자신의 신원 정보인 $I_A$와 공개키 $h_A$를 서버에 등록하고 개인화 된 스마트카드를 얻는다. 등록 단계에 대한 설명은 다음 절차에 의해 이루어지며 Fig. 2와 같다.

- 1단계 : 사용자는 자신의 $ID_A$와 $PW_A$를 선택한다. 그 후 $f_A \in L_f$와 $g_A \in L_g$를 선택하고 $f_A$의 역원 $f_{Ap}^{-1}$와 $f_{Aq}^{-1}$를 계산한 뒤 공개키 $h_A = pf_{Aq}^{-1} * g_A \in Z_q[X]/(X^N-1)$를 계산하고 $I_A = H(ID_A \| PW_A)$를 생성해 안전한 채널로 서버에 전송한다.
- 2단계 : 등록 요청을 받은 서버는 $I_A$를 확인 후 데이터베이스에 존재하는지 여부를 확인한다. $I_A$가 존재하면 임의의 값 $x_A$를 생성해 사용자의 공개키 $h_A$와 매치 시켜 데이터베이스에 저장한다. 그 후 $SC$에 $H(I_A \| h_A) \oplus x_A$를 저장하고 사용자에게 $SC$와 서버의 공개키 $h_B$를 전송한다.
- 3단계 : 스마트카드 $SC$를 받으면 사용자는 자신의 생체 정보 $B_A$를 등록하고 $V = H(ID_A \| PW_A \| H(B_A))$를 $SC$에 저장한다.

#### 3.2.2 로그인 단계

로그인 단계에서는 유효한 스마트카드 $SC$를 가진 합법적인 사용자만이 서버에 로그인이 가능하다. 먼저 카드 판독기에 자신의 스마트카드 $SC$를 삽입하고 $ID_A$와 $PW_A$를 입력하고 $B_A$를 인증하면 스마트카드 $SC$는 입력된 정보가 유효한지 확인 후 로그인 메시지를 생성한다. 로그인 단계에 대한 설명은 다음 절차에 의해 이루어진다.

- 1단계 : 입력된 값 $\{ID_A, PW_A, B_A\}$를 수신하면 스마트카드는 $V = h(ID_A \| PW_A \| H(B_A))$를 검증한다.
- 2단계 : 검증이 성립하면 스마트카드는 임의의 다항식 $r_A$와 $k_A$를 선택하여 $e_A = pr_A * h_B + k_A \pmod q$와 $c_A = x_A \oplus H(k_A)$를 계산해 공개키 $h_A$와 함께 서버에 전송한다.

#### 3.2.3 인증 및 키 분배 단계

서버는 로그인 메시지 $e_A$, $c_A$ 및 $h_A$를 수신하면 해당 메시지를 검증한 후 사용자가 확인되면 서버는 공통 비밀 세션 키 $SK$를 생성하여 서용자와 안전한 통신을 하게 된다. 인증 및 키 분배 단계에 대한 설명은 다음 절차에 의해 이루어진다.

- 1단계 : 서버는 $e_A$를 개인키를 사용해 복호화 한

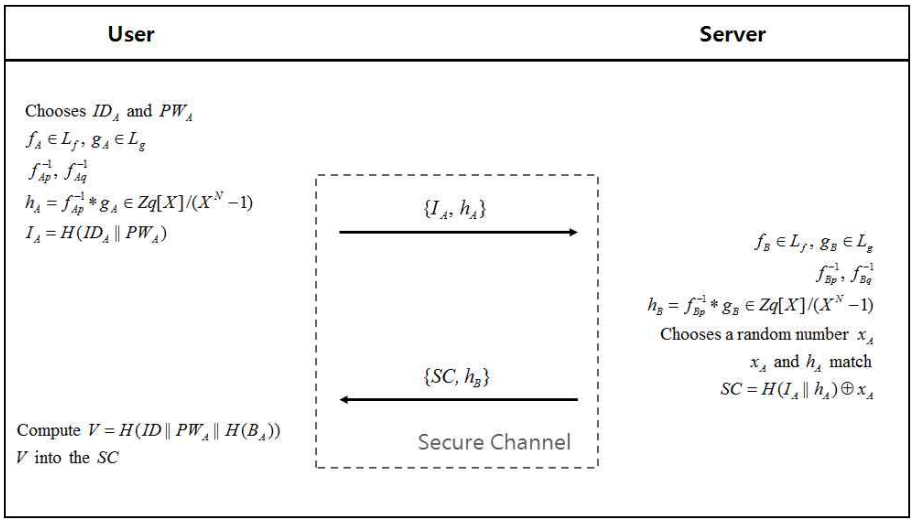


Fig. 2. Registration phase.

후 $c_A$를 계산해 두 값이 모두 $k_A$가 맞으면 로그인 요청을 승인한다.

- 2단계 : 승인 후 서버는 임의의 다항식 $r_B$와 $k_B$를 선택하여 $e_B = pr_B * h_A + k_B \pmod q$와 $c_A = x_A \oplus H(k_A)$를 계산해 사용자에게 전송하고 세션키 $SK = k_A * k_B \pmod p$를 생성한다.
- 3단계 : 사용자는 $e_B$를 개인키를 사용해 복호화한 후 $c_B$를 계산해 두 값이 모두 $k_B$가 맞는지 검증한다. 검증이 유효하지 않으면 세션을 종료하고 그렇지 않으면 계산된 세션 키 $SK = k_A * k_B \pmod p$를 유효한 세션 키로 간주한다.

로그인과 인증 및 키 분배 단계는 Fig. 3과 같다.

## 4. 분 석

제안한 프로토콜은 Tu 등과 Mishra 등이 제안한 SIP 프로토콜과 비교 분석하였으며 연산량 및 안전성 분석은 다음과 같다.

### 4.1 연산량 분석

연산량 분석은 기존의 ECC를 활용한 프로토콜과 비교 분석한다. 제안한 프로토콜은 NTRU를 활용하여 기존의 프로토콜[3,12]과 연산량을 정확히 비교 분석하는 것은 적절치 않으나 NTRU는 ECC보다 암·복호화 및 키 생성 단계에서 연산이 효율적인 것으로 증명[9,10] 되어 연산량 측면에서 보다 효율적이다. 연산량 분석은 Table 1과 같으며 제안한 프로토콜에서는 임의의 다항식을 매 세션마다 재생성하여 비밀번호 변경 단계가 필요하지 않다.

### 4.2 안전성 분석

본 논문에서는 안전성을 informal analysis로 분석하였으며 제안하는 방식은 사용자 익명성을 보장하며 중간자 공격 및 사용자 가장 공격 등에 안전하다. 기존의 인증 방식들과 안전성 비교는 Table 2와 같다.

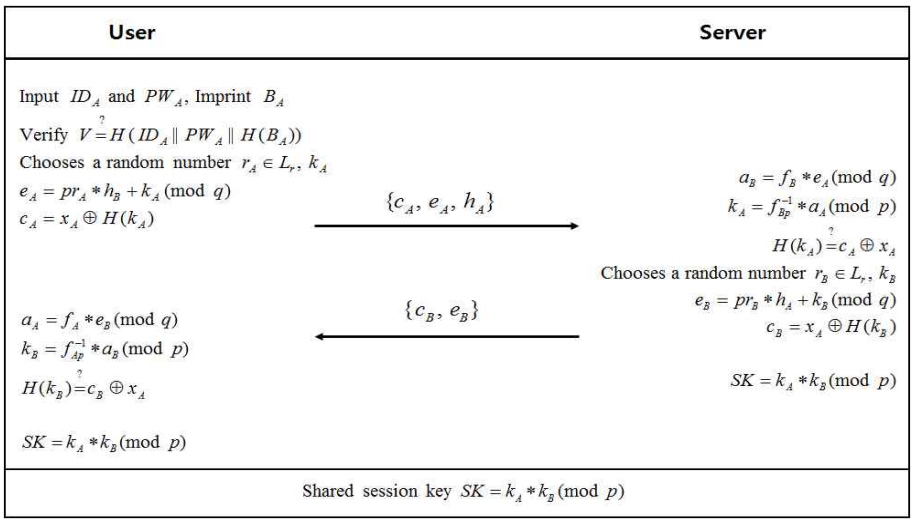


Fig. 3. Login, authentication and key distribution phase.

Table 1. Computation comparison

| Scheme | Registration phase | Login and authentication phase | Password change phase |
|---|---|---|---|
| Tu et al.[12] | $2T_h$, $1T_{ecm}$ | $8T_h$, $6T_{ecm}$, $1T_{eca}$ | $5T_h$, $1T_{ecm}$, $4T_{sym}$ |
| Mishra et a.[3] | $3T_h$, $1T_H$ | $11T_h$, $3T_{ecm}$, $1T_H$ | $3T_h$, $2T_H$ |
| Our Proposed | $2T_c$, $2T_h$, $1T_H$ | $7T_c$, $5T_h$, $1T_H$ | - |

($T_c$ : convolution multiplication operation, $T_h$: one-way hash function, $T_H$ : biohashing function, $T_{ecm}$ : elliptic curve point multiplication operation, $T_{eca}$ : elliptic curve point addition, $T_{sym}$ : symmetric key encryption/decryption)

Table 2. Informal analysis

| | Tu et al.[12] | Mishra et al.[3] | Our Protocol |
|---|---|---|---|
| Confidentiality | ○ | ○ | ○ |
| Integrity | ○ | ○ | ○ |
| User anonymity | × | ○ | ○ |
| Mutual authentication | ○ | ○ | ○ |
| Man-in-the-middle attack | × | ○ | ○ |
| User impersonation attack | × | ○ | ○ |
| Replay attack | ○ | ○ | ○ |
| Session key disclosure attack | ○ | ○ | ○ |
| Quantum computing attacks | × | × | ○ |

○ : Pr]eserves the security properties × : Do not preserve the security properties

• 기밀성 (Confidentiality)

기밀성은 허락 되지 않은 사용자 또는 객체가 정보의 내용을 알 수 없도록 한다. 제안한 방식은 NTRU 기반 공개 키를 사용하므로 데이터의 기밀성을 제공하며 세션 키가 노출되어도 세션마다 임의로 생성되는 $r$과 $k$로 인해 통신상 기밀성을 제공한다.

• 무결성(Integrity)

무결성은 허락 되지 않은 사용자 또는 객체가 정보를 수정할 수 없어야 한다. 제안한 방식은 NTRU Sign을 통해 메시지의 서명 값을 생성하여 전달하므로 위·변조가 되더라도 검증과정을 통해 확인이 가능하며 또한 서버에 등록된 $x$를 사용하여 인증과정을 거치므로 무결성을 제공한다.

• 익명성(User anonymity)

익명성은 어떠한 행위를 한 사람이 누구인지 드러나지 않아야 한다. 제안한 방식은 본인의 $ID$, $PW$ 및 생체 정보 $B$를 모두 해쉬하여 사용하므로 사용자의 정보는 누구도 알 수 없으며 그로인해 익명성을 제공한다.

• 상호 인증(Mutual authentication)

제안한 방식은 사용자와 서버만이 알고 있는 $x$를 사용하여 $c_A = x_A \oplus H(k_A)$와 $c_B = x_A \oplus H(k_B)$를 생성하여 암호화된 정보와 비교해 상호인증을 제공한다. 서버의 정보가 노출되어 $x$의 정보를 알아도 개인키 $f$를 알지 못하면 $k$에 대한 정보를 알 수 없으므로 안전하다.

• 중간자 공격(Man-in-the-middle attack)

중간자 공격은 네트워크 통신을 조작하여 통신 내용을 도청하거나 조작하는 공격이다. 제안한 방식은 사용자와 서버만이 알고 있는 $x$를 사용하여 상호인증을 하게 되므로 중간에서 값이 위·변조 되었는지 확인이 가능하여 중간자 공격이 불가능하다.

• 사용자 가장 공격(User impersonation attack)

사용자 위장 공격은 공격자가 사용자로 위장하여 인증을 시도하는 공격이다. 제안한 방식에서 공격자가 사용자인 것처럼 위장하기 위해서는 사용자의 스마트카드, $ID$, $PW$ 및 생체 정보가 필요하므로 불가능하다.

• 재사용(Replay attac)

재사용 공격은 사용자가 사용한 정보를 공격자가 도청으로 가로채 다시 사용하는 공격이다. 제안한 방식은 매 세션마다 임의로 생성되는 $r$과 $k$를 사용하므로 한번 사용한 정보를 재사용하여 인증하는 것은 불가능하다.

• 세션키 공개 공격(Session key disclosure attack)

세션키가 안전하지 않은 메모리에 저장되어 공격자에 의해 노출되어도 제안한 방식의 세션키인 $SK$를 사용하여 사용자의 개인키 또는 정보를 알아내는 것은 NTRU의 암호학적으로 사용되는 수학의 어려움인 큰 크기의 격자에서 작은 벡터를 찾는 수학 문제와 등가이므로 계산 상 불가능하다.

• 양자 컴퓨팅 공격(Quantum computing attacks)

제안한 방법은 양자 연산 알고리즘인 Shor 알고리즘과 Grover 알고리즘에 내성을 지니는 격자기반 암호방식인 NTRU 암호 시스템을 사용하였으며 기존의 암호 시스템들과 동일한 안전성을 제공하며 향후 양자 컴퓨팅 공격에도 안전하다.

## 5. 결 론

2011년 캐나다의 벤처기업인 D-Wave사에 의해 최초의 양자 컴퓨터가 개발되었으며 구글, NASA 등 많은 기업과 연구소들이 양자 컴퓨터 개발에 많은 투자를 하고 있다. 양자 컴퓨터가 실현되면 아주 복잡한 영역의 연구에 응용되어 많은 도움이 될 것이라 예상되지만 현재 사용 중인 암호 시스템은 큰 위협을 받게 될 것이며 이를 대비해 양자 컴퓨터가 실현되기 이전에 안전한 암호를 준비하고 실행하여 방어 체계를 갖추어야한다.

본 논문은 SIP에서 ECC를 사용한 Mishra 등의 인증 및 키 분배 프로토콜의 취약점인 양자 컴퓨팅 공격을 방어하기 위해 양자 연산 알고리즘에 내성이 있는 NTRU를 활용하였으며 임의의 다항식을 매 세션마다 재생성하여 비밀번호 변경 단계를 생략하여 보다 효율적인 프로토콜을 제안하였다. 제안한 프로토콜은 기존 SIP의 취약점인 익명성을 보장 하며 중간자 공격, 사용자 가장 공격 등 다양한 공격에 안전하며 사용자 익명성을 보장한다.

## REFERENCE


[1] IETF, *HTTP Authentication: Basic and Digest Access Authentication*, RFC 2617, 1999.

[2] IETF, *SIP: Session Initiation Protocol,* RFC3261, 2002.

[3] D. Mishra and A.K. Das, "A Secure and Efficient ECC-based User Anonymity-preserving Session Initiation Authentication Protocol Using Smart Card," *Peer-to-Peer Networking and Appications*, Vol. 9, No. 1, pp. 171-192, 2016.

[4] H. Arshad and M. Nikooghadam, "An Efficient Sand Secure Authentication and Key Agreement Scheme for Session Initiation Protocol Using ECC," *Multimedia Tools and Applications*, Vol. 75, No. 1, pp. 181-197, 2016.

[5] P.W. Shor, "Algorithms for Quantum Computation: Discrete Logarithms and Factoring," *Proceedings 35th Annual Symposium on Foundations of Computer Science*, pp. 124-134, 1994.

[6] L.K. Grover, "A Fast Quantum Mechanical Algorithm for Database Search," *Proceedings of the Twenty-eighth Annual Association for Computing Machinery Symposium on the Theory of Computing*, pp. 212-219, 1996.

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

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

[9] J. Hoffstein, J. Pipher, and J.H. Silverman, "NTRU: A Ring-Based Public Key Cryptosystem," *Proceeding of International Algorithmic Number Theory Symposium*, Vol. 1423, pp. 267-288, 1998.

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

[11] S.H. Jeong, K.S. Park, 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.

[12] H. Tu, N. Kumar, N. Chilamkurti, and S. Rho, "An Improved Authentication Protocol for Session Initiation Protocol Using Smart Card," *Peer-to-Peer Networking and Appications*, Vol. 8, No. 5, pp. 903-910, 2014.

[13] NIST, *Security Considerations for Voice Over IP Systems*, SP 800-58, 2005.

정 성 하

2013년 2월 대구한의대학교 IT콘텐츠학과 학사
2016년 3월～현재 경북대학교 대학원 전자공학부 석사과정
관심분야 : 정보보호, 무선통신보안, 네트워크보안, 양자 후 암호

박 기 성

2015년 2월 경북대학교 산업전자공학과 학사
2017년 2월 경북대학교 대학원 전자공학부 석사
2017년 3월～현재 경북대학교 대학원 전자공학부 박사과정
관심분야 : 정보보호, 무선통신보안, 네트워크보안, PQ 암호

이 경 근

1999년 2월 경북대학교 전자공학과 학사
2001년 2월 경북대학교 대학원 전자공학과 석사
2006년 2월 경북대학교 대학원 전자공학과 박사
2006년 3월～현재 삼성전자 무선사업부 재직
관심분야 : 정보보호, 네트워크보안, 모바일 컴퓨팅

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