Journal of Korea Multimedia Society Vol. 20, No. 8, August 2017(pp. 1321-1329)
https://doi.org/10.9717/kmms.2017.20.8.1321

양자 컴퓨팅 환경에 안전한 NTRU 기반 인증 및 키 분배 프로토콜

정성하†, 이경근††, 박영호†††

Secure NTRU-based Authentication and Key Distribution Protocol in Quantum Computing Environments

SeongHa Jeong†, KyungKeun Lee††, YoungHo Park†††

ABSTRACT

A quantum computer, based on quantum mechanics, is a paradigm of information processing that can show remarkable possibilities of exponentially improved information processing. This paradigm can be solved in a short time by calculating factoring problem and discrete logarithm problem that are typically used in public key cryptosystems such as RSA(Rivest-Shamir-Adleman) and ECC(Elliptic Curve Cryptography). In 2013, Lei et al. proposed a secure NTRU-based key distribution protocol for quantum computing. However, Lei et al. protocol was vulnerable to man-in-the-middle attacks. In this paper, we propose a NTRU(N-the truncated polynomial ring) key distribution protocol with mutual authentication only using NTRU convolution multiplication operation in order to maintain the security for quantum computing. The proposed protocol is resistant to quantum computing attacks. It is also provided a secure key distribution from various attacks such as man-in-the middle attack and replay attack.

Key words: Post Quantum, NTRU, Key Distribution Protocol

1. 서 론

1982년 Richard Feynman[1]은 물리현상을 양자 컴퓨터로 구현할 수 있는 가능성에 대해 발표하였으며 2011년 캐나다의 벤처기업인 D-Wave사에 의해 최초의 양자 컴퓨터가 개발되었다. 양자 컴퓨팅은 큐비트(quantum bit)를 사용한 정보처리 능력으로 현재의 보안시스템은 크게 위협을 받을 수 있다. 1994년 Peter W. Shor[2]는 양자 퓨리에 변환을 이용하여 현재까지 안전하다고 평가받는 소인수분해 문제를 효율적으로 계산 할 수 있는 양자 컴퓨팅 알고리즘을 제안하였다. 현재 가장 널리 사용 되는 공개키 암호 시스템[3]으로 RSA 암호 알고리즘 같은 경우 소인수 분해의 어려움을 기반으로 설계된 암호 알고리즘이다. 하지만 양자 연산 알고리즘인 쇼어 알고리즘이 제안되면서 RSA 암호 알고리즘은 양자 컴퓨팅 환경에서는 더 이상 안전하지 않은 방식이 되었고 이를 사용한 보안 프로토콜들은 심각한 보안 위협을 받게 된다.

양자 컴퓨팅 공격에 안전하다고 알려진 암호는

※ Corresponding Author : YoungHo Park, Address: (702-701) 80 Daehakro, Bukgu, Daegu, Korea, TEL : +82-53-950-7842, FAX : +82-53-950-5505, E-mail : parkyh@knu.ac.kr
Receipt date : May 23, 2017, Revision date : Jun. 27, 2017
Approval date : Jul. 7, 2017
† School of Electronics, Kyungpook National University (E-mail : jeongsh1128@gmail.com)
†† 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).

Code, Lattice, Hash 및 Multivariate 기반의 4가지 암호방식이 있으며 본 논문에서는 격자(Lattice) 기반 암호의 표준으로 채택된 NTRU 공개키 암호를 사용한다. NTRU는 1996년 Jeffrey Hoffstein[4] 등에 의해 제안된 격자 기반 공개키 암호체계로서 기존의 공개키 암호와 비교하여 동일한 안전성을 제공하면서 암호화 및 복호화 속도가 빠르며 양자 연산 알고리즘을 이용한 공격에도 안전하다는 이점이 있다[5].

NTRU를 응용한 보안 프로토콜은 활발하게 연구되고 있다. 2013년 Lei[6] 등은 기존의 공개키 분배 방식인 DH방식 또한 양자 연산 알고리즘에 취약함을 강조하며 NTRU를 활용한 키 분배 프로토콜을 제안하였으며 같은 해 Park[7, 8] 등은 NTRU 영지식 대화형 증명방식을 제안하였다. 하지만 2016년 Valluri[9] 등은 Lei 등의 프로토콜은 중간자 공격에 의해 비밀키가 노출되는 문제점을 증명하였고 같은 해 Park 등의 NTRU 영지식 방식 또한 Jheng[10] 등에 의해 중간자 공격으로 공격자가 서버와의 통신이 가능함을 증명하여 두 논문 모두 중간자 공격에 취약함이 확인되었다.

본 논문은 Lei 등의 프로토콜에 취약점인 중간자 공격으로 인해 비밀키가 노출되는 문제를 해결하기 위해 Park 등이 제안한 NTRU 영지식 대화형 증명방식의 취약점을 보완하여 양방향 상호인증 단계를 제안한다. 제안한 프로토콜은 양방향 상호인증을 통해 중간자 공격에 안전하며 키 분배 프로토콜에 추가적으로 발생될 수 있는 제사용 공격, 세션 키 노출 공격 등에도 안전하다.

2. 관련 연구

2.1 NTRU 기반 공개키 암호

NTRU 암호는 1996년 Jeffrey Hoffstein[4] 등에 의해 제안되었으며 격자 문제를 기반으로 하는 공개키 암호 체계로 기본 연산은 다항식 환(Polynomial rings)상에서 이루어진다. 현재 널리 사용되는 공개키 암호인 RSA, ECC 등과 비교하여 동일한 안정성을 제공하면서 암·복호화 속도가 빠르며 양자 컴퓨팅 공격에 내성이 있다는 이점[11,12]을 갖는다.

2.1.1 다항식 컨볼루션 연산

Z를 정수들의 집합이라고 하자. $Z[X]$로 표시되는 Z에 대한 다항식 링은 Z의 계수들을 갖는 모든 다항식들의 집합이다. 몫 링(Quotient ring) $R=Z[X]/(X^N-1)$로 정의한다. R에 속하는 원소 a는 다항식 또는 벡터로서 다음 식 (1)과 같이 정의 된다.

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

R에 속하는 원소 a와 b에 대한 컨볼루션 곱 $c(c(X)=a(X)*b(X))$는 다음 식 (2)와 같은 계수를 갖는다.

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

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

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

2.1.2 NTRU 기반 공개 키 암호체계

- NTRU는 3가지 공개 파라미터(N,p,q)를 가진다 (p와 q의 최대공약수는 1이고, $p\ll q$임).
- 다항식의 계수들은 mod q or q로 감산된다.
- $f^{-1}\,(\mathrm{mod}\,q)$ 로 표시되는 다항식 f의 mod q 상의 역원은 $f*f^{-1}\equiv 1\,(\mathrm{mod}\,q)$를 만족하는 다항식으로서 정의된다.

IEEE P1363.1 표준 초안[5]은 NTRU에 대한 몇 가지 전형적인 파라미터 집합을 제안하는데 그 중 하나는 $(N,p,q)=(251,2,197)$이다.

2.1.3 키 생성

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

2.1.4 암호화

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

2.1.5 복호화

e를 복호화하기 위해 먼저 $a = e * f \pmod q$ 를 계산한다(a의 계수들이 $A \le a_i < A+q$를 만족하도록 선택한다. 이때 A의 값은 고정되며 나머지 파라미터에 의존하는 간단한 공식에 의해 결정됨). 평문 m은 $m = a \pmod p$로 복구된다.

2.1.6 복호화의 유효성

복호화 과정의 다항식 a는 다음 식 (3)을 만족한다.

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

최종 다항식 $pr * g + m * f \bmod q$ 에 대해서 매개 변수를 적절히 선택하여 계수들이 q보다 작은 길이의 범위 내에 놓이도록 조정할 수 있다. 따라서 α에 대해 다음 식 (4)와 같이 등식이 성립함을 알 수 있다.

$$a = pr * g + m * f = pr * g + m * (1 + pF) \tag{4}$$

즉 다항식 a는 mod q에 대해서가 아닌 정확하게 등식이 성립하므로 $m = a \pmod p$가 되어 메시지를 복원할 수 있다.

2.2 Lei 등의 키 분배 방식

2013년 Lei 등은 기존의 공개키 분배 방식인 DH방식이 양자 연산 알고리즘인 쇼어알고리즘에 취약함과 NTRU의 공개키 암호화 방법과 디지털 서명 방법은 존재하지만 공개 키 분배 방법이 없음을 강조하며 NTRU를 활용한 키 분배 프로토콜을 제안하였다[6].

Fig. 1은 Xinyu Lei 등이 제안한 NTRU 공개키 분배 프로토콜이다.

- 1단계 : Alice는 f_A의 역이 존재하도록 $f_A \in L_f$를 선택하고 $g_A \in L_g$를 선택한다. 그 다음 $h_A \equiv f_A^{-1} * g_A \pmod q$를 계산한 후 h_A를 Bob에게 보낸다.
- 2단계 : Bob은 h_A를 받으면 f_B의 역이 존재하도록 $f_B \in L_f$를 선택하고 $g_B \in L_g$와 $r_B \in L_r$를 선택한다. 그 다음 $h_B \equiv f_B^{-1} * g_B \pmod q$와 $e_B \equiv pr_B + h_A \pmod q$를 계산한 후 h_B와 e_B를 Alice에게 보낸다.
- 3단계 : h_B와 e_B를 받은 Alice는 $r_A \in L_r$를 선택하고 $e_A \equiv pr_A + h_B \pmod q$를 계산한 후 e_A를 Bob에 보내고 $a_A = f_A * e_B \pmod q, K_A = a_A \pmod p = f_A * f_B \pmod p$를 계산한다.
- 4단계 : e_A를 받은 Bob은 $a_B = f_B * e_A \pmod q, K_B = a_B \pmod p = f_A * f_B \pmod p$를 계산한다.

결과적인 공통 세션 키는 $K_A = K_B = f_A * f_B \pmod p$가 된다.

하지만 2016년 Valluri 등은 Lei 등의 NTRU 키 분배 프로토콜은 중간자 공격에 취약함을 증명[9]하였으며 그 방법은 Fig. 2와 같다.

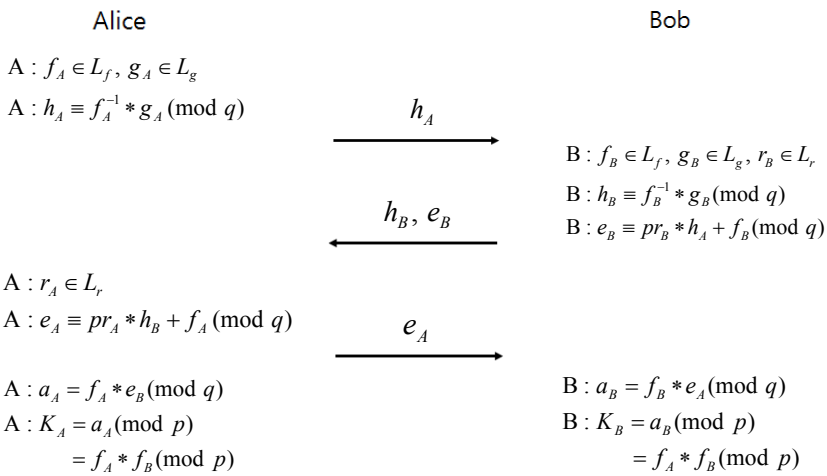


Fig. 1. Key distribution scheme of Lei et al.

- 1단계 : Attacker는 Alice와 Bob의 공개키인 h_A와 h_B를 가로 챈 후 자신의 공개키 $h_{A'}^{'} \equiv f_{A'}^{'-1} * g_{A'}^{'} (\mathrm{mod}\, q)$와 $h_{A'}^{''} \equiv f_{A'}^{''-1} * g_{A'}^{'} (\mathrm{mod}\, q)$을 계산하여 $h_{A'}^{'}$는 Alice에게 $h_{A'}^{''}$는 Bob에게 보낸다.
- 2단계 : $h_{A'}^{''}$를 받은 Bob은 $r_B \in L_r$를 선택하고 $e_B \equiv pr_B + h_{A'}^{''} (\mathrm{mod}\, q)$를 계산한 후 $e_B^{'}$를 Alice에 보내지만 Attacker는 이를 가로챕니다. 동일하게 $h_{A'}^{'}$를 받은 Alice는 $r_A \in L_r$를 선택하고 $e_A \equiv pr_A + h_{A'}^{'} (\mathrm{mod}\, q)$를 계산한 후 $e_A^{'}$를 Bob에게 보내지만 Attacker는 이를 가로챈다.
- 3단계 : Alice와 Bob이 각각 보낸 $e_A^{'}$와 $e_B^{'}$를 사용하여 $w_A = e_A^{'} * f_{A'}^{'} (\mathrm{mod}\, q)$와 $w_B = e_B^{'} * f_{A'}^{''} (\mathrm{mod}\, q)$를 계산하여 w_A와 w_B를 만든 후 $K_A^{'} = w_A * f_{A'}^{'-1} (\mathrm{mod}\, p) = f_A$와 $K_B^{'} = w_B * f_{A'}^{''-1} (\mathrm{mod}\, p) = f_B$를 계산하여 Alice와 Bob의 개인키인 f_A와 f_B를 구할 수 있다.

위와 같이 Lei 등의 프로토콜은 중간자 공격으로 인해 개인키를 구할 수 있게 되는 문제점이 존재한다.

2.3 Park 등의 영지식 인증 방식

2013년 Park등은 NFC 모바일 결제정보보호를 위한 NTRU기반 증명 기법을 제안하였다[7,8]. 이 제안 방식은 사용자를 은행서버에 등록하는 단계와 결제 시 금융결제정보를 상점, VAN사에 노출시키지 않고 은행에 사용자 자신을 증명하는 단계로 구성되며 수행절차는 다음 Fig. 3 및 4와 같다.

2.3.1 사용자 등록 단계

- 1단계 : User는 잘려진 다항식 환 상에서 비밀키 값 f_A와 g_A 그리고 f_A의 역함수 f_{Ap}^{-1}와 f_{Aq}^{-1}를 선택하고 사용자의 공개키 v_A를 계산한다.
- 2단계 : 사용자는 사용자 정보와 v_A를 은행에 제출하고 은행은 사용자의 신원을 검사한 후 사용자 정보로 생성한 신원정보 I와 v_A를 통해 공개키 증명서 $Cert(I, v_A)$를 계산하여 사용자에게 발급한다. 이후 은행은 사용자 정보를 보관한다.

2.3.2 사용자 신원 증명 단계

사용자는 금융거래 시 자신이 정당한 금융결제정보를 보유하고 있다는 것을 증명하기 위해 다음과 같은 단계를 수행한다.

- 1단계 : 사용자는 임의의 다항식 r_A를 선택한 후 사용자 증명을 하기 위해 사용되는 $x = g_A * r_A$를 계산하여 $I, v_A, Cert(I, v_A), x$를 은행에 전송한다.
- 2단계 : 은행은 $Cert(I, v_A)$와 디지털 서명을 이용하여 I와 v_A의 타당성을 인증한 후 임의의 다항식 e를 선택하여 사용자에게 전송한다.
- 3단계 : 사용자는 f_A와 r_A 그리고 e를 사용하여 y를 계산하여 은행으로 전송한다.

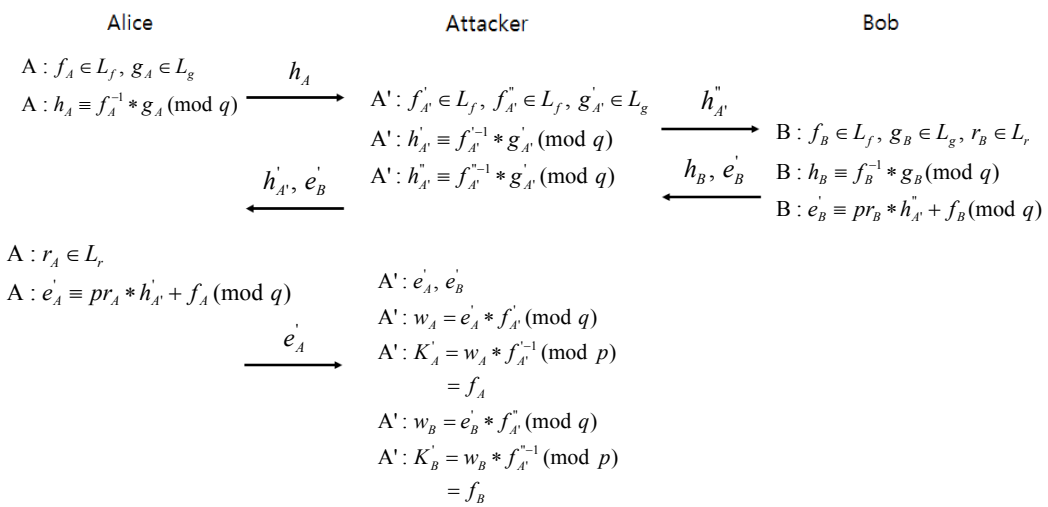


Fig. 2. Cryptanalysis of Lei et al. scheme.

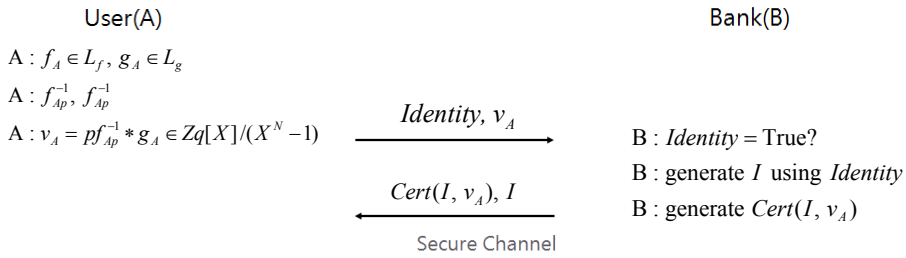


Fig. 3. Registration phase of Park et al. scheme.

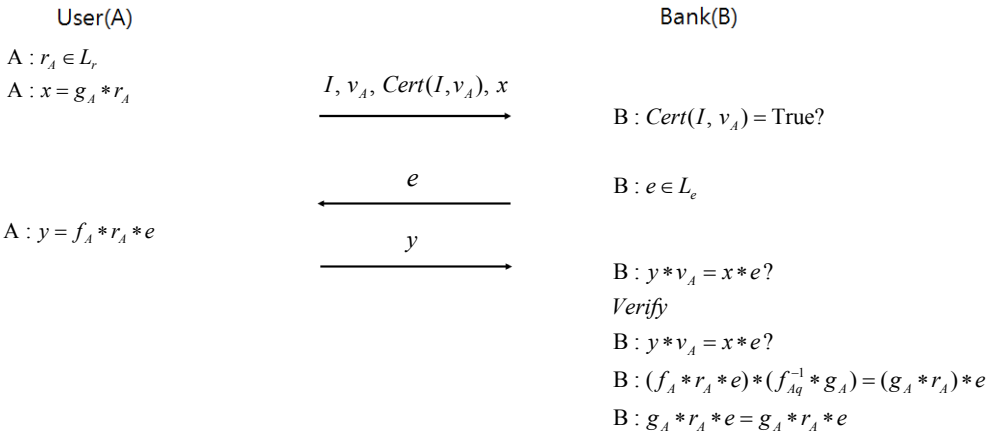


Fig. 4. Identity proof phase of Park et al. scheme.

- 4단계 : 은행은 $y * v_A = x * e$인지 검사하여 사용자를 인증한다.

2016년 Jheng 등은 Park 등의 방식이 중간자 공격에 취약함을 증명하였다[10].

사용자와 은행간의 통신을 도청 할 수 있는 Attacker가 있다고 가정하면 I, v_A, $Cert(I_A, v_A)$, x, e, y를 가질 수 있으며 다음 Fig. 5와 같이 공격을 할 수 있다.

- 1단계 : Attacker는 $x_A' = x_A * e_B$를 계산 후 I_A, v_A, $Cert(I_A, v_A)$, x_A'를 Bank에 보낸다.
- 2단계 : I_A, v_A, $Cert(I_A, v_A)$, x_A'를 받은 Bank는 $Cert(I_A, v_A)$로 무결성을 확인 후 임의의 다항식 e_B'를 선택하여 Attacker에게 보낸다.
- 3단계 : e_B'를 받은 Attacker는 $y_A' = y_A * e_B'$를 계산하여 Bank에게 보낸다.
- 4단계 : y_A'를 받은 Bank는 $y_A' * v_A = x_A' * e_B'$를 계산하여 인증하게 된다.

위와 같이 Park 등의 프로토콜은 중간자 공격으로 도청으로 통해 얻은 값으로 중간자 공격을 하여 공격자가 은행과 인증이 되는 문제점이 존재한다.

3. 제안한 프로토콜

본 논문에서 제안한 방식은 Lei 등의 NTRU 키 분배 프로토콜의 장점을 그대로 보존하면서 Park 등의 NTRU 영지식 방식의 취약한 부분을 보완 후 응용하여 양방향 인증과정을 추가하므로 중간자 공격에 취약함을 보완하였다. 제안된 방식에서는 Alice와 Bob이 각각 임의의 다항식 r을 통해 x를 생성하여 상호인증을 하므로 중간자 공격을 방지 하였다.

3.1 시스템 계수

본 제안방식에서는 다음과 같은 시스템계수를 사용한다.

- $*$: 볼루션 곱셈
- N : 잘려컨진 다항식 환 $R = Z[X]/(X^N - 1)$의 차수

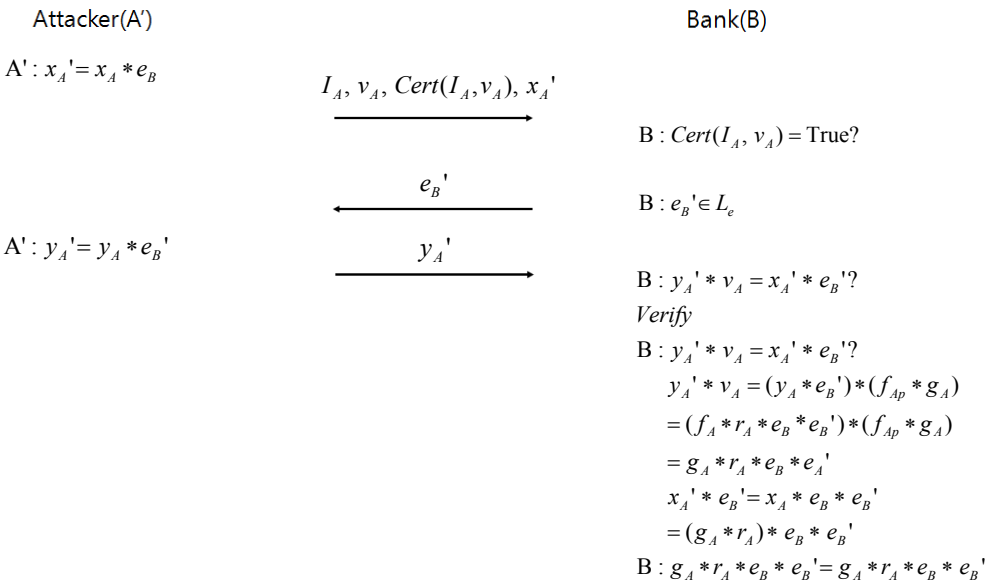


Fig. 5. Cryptanalysis of Park et al. scheme.

를 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 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
- Key : 세션 키

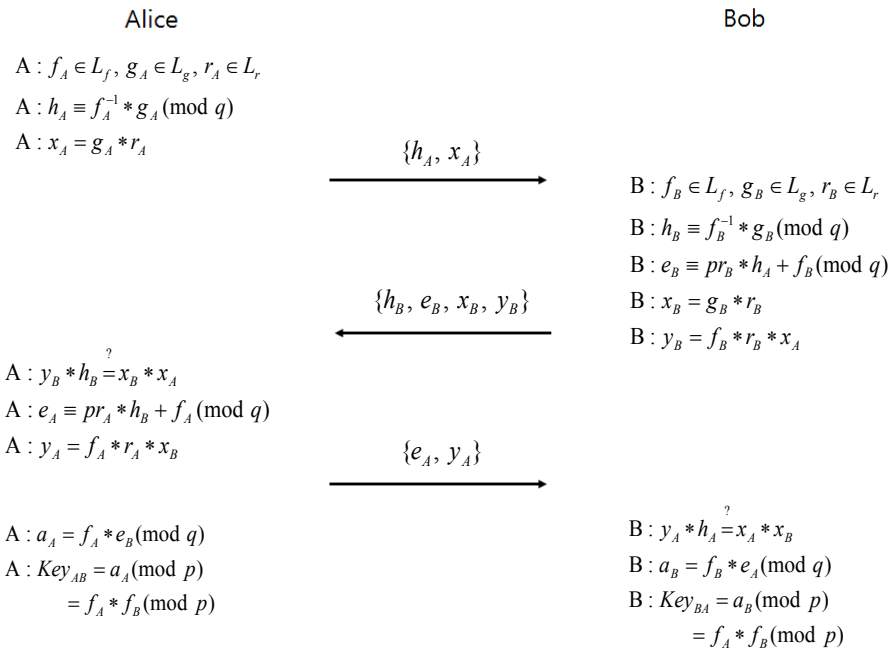
3.2 양방향 인증 NTRU 키 분배 프로토콜

본 논문에서 제안한 방식은 다음 그림 6과 같은 단계로 인증한다.

- 1단계 : Alice는 f_A의 역이 존재하도록 $f_A \in L_f$를 선택하고 $g_A \in L_g$와 임의의 $r_A \in L_r$을 선택한다. $h_A \equiv f_A^{-1} * g_A \pmod q$와 $x_A = g_A * r_A$를 계산한 후 h_A와 x_A를 Bob에게 보낸다.
- 2단계 : Bob은 h_A와 x_A를 받으면 f_B의 역이 존재하도록 $f_B \in L_f$를 선택하고 $g_B \in L_g$와 임의의 $r_B \in L_r$를 선택한다. $h_B \equiv f_B^{-1} * g_B \pmod q$와 $e_B \equiv pr_B * h_A + f_B \pmod q$ 그리고 $x_B = g_B * r_B$와 $y_B = f_B * r_B * x_A$를 계산한 후 h_B와 e_B 그리고 x_B와 y_B를 Alice에게 보낸다.
- 3단계 : h_B와 e_B 그리고 x_B와 y_B를 받은 Alice는 $y_B * h_B = x_B * x_A$를 계산하여 두 값이 맞는지 확인 후 문제가 있으면 세션을 종료하고 맞을 시 $e_A \equiv pr_A * h_B + f_A \pmod q$와 $y_A = f_A * r_A * x_B$를 계산한 후 e_A와 y_A를 Bob에 보낸다.
- 4단계 : e_A와 y_A를 받은 Bob은 $y_A * h_A = x_A * x_B$를 계산하여 두 값이 맞는지 확인 후 $a_B = f_B * e_A \pmod q, Key_{BA} = a_B \pmod p = f_A * f_B \pmod p$를 계산하여 세션 키를 생선하고 Alice 또한 $a_A = f_A * e_B \pmod q, Key_{AB} = a_A \pmod p = f_A * f_B \pmod p$를 계산하여 세션키를 생성한다.

4. 분 석

제안한 방식의 연산량을 비교 분석하면 Table 1과 같다. Lei 등의 키 분배 방식은 인증 단계가 존재하지 않고 Park 등의 인증 방식은 단방향 인증만 가능하여 중간자 공격에 취약하다. 제안된 방식은 Lei 등과 Park 등의 방식에 비해 많은 연산을 필요로 하지만 두 방식의 취약점을 방어하기 위해 양방향 인증이 추가된 키 분배 방식이다. 또한 컨볼루션 곱셈을 활용한 NTRU는 RSA에 비해 암호화 과정에서 5.9배, 복호화 과정에서 14.4배, 키생성 단계에서 5배 이상 빠른 것으로 증명[4]되어 연산량은 문제가 되지 않는다.



$$Key_{AB} = Key_{BA} = a_{AB} \pmod p = f_A * f_B \pmod p$$

Fig. 6. NTRU key distribution protocol of the proposed scheme.

Table 1. Comparison of Computation

		Lei[6]	Park[7, 8]	Proposed scheme
Operation	Registration	-	1C	-
	Proof	6C	5C	15C
traffic	Registration	-	2-pass	-
	Proof	3-pass	3-pass	3-pass

- : None C : Convolution multiplication

본 논문에서 제안한 방식은 다음 informal analysis를 이용하여 안전성을 분석하였으며 Table 2와 같다.

• Confidentiality

기밀성은 허락 되지 않은 사용자 또는 객체가 정보의 내용을 알 수 없도록 하는 것이다. 제안한 방식은 NTRU 기반 공개 키를 사용하므로 데이터의 기밀성을 제공하며 세션키가 노출되어도 세션마다 임의로 생성되는 f와 r로 인해 통신상 기밀성을 제공한다.

• Integrity

허락 되지 않은 사용자 또는 객체가 정보를 함부로 수정할 수 없도록 하는 것이다. 제안한 방식은 NTRUSign을 통해 메시지의 서명값을 생성하여 전달하므로 위·변조가 되더라도 검증과정을 통해 확인이 가능하며 또한 상호인증 단계에서 x, y와 공개키 h를 사용하여 인증과정을 거치므로 무결성을 제공한다.

• Mutual authentication

제안한 방식은 Lei 등과 Park 등의 방식의 취약점을 방어하기 위해 상호인증 단계를 추가하였다. 상호간에 만들어낸 x, y와 공개키 h를 교환하여 Alice와 Bob이 각각 $y_B * h_B = x_B * x_A$와 $y_A * h_A = x_A * x_B$를 계산하면 $g_A * r_A * g_B * r_B = g_A * r_A * g_B * r_B$와 같은 식이 성립되어 상호인증을 제공하며 x와 y는 사용자의 개인키를 활용하여 계산되므로 공격자는 상호

Table 2. Analysis of Proposed Schemes

	Lei[6]	Park[7, 8]	Proposed scheme
Confidentiality	○	○	○
Integrity	×	○	○
Mutual authentication	×	×	○
Man-in-the-middle attack	×	×	○
User impersonation attack	×	×	○
Replay attack	○	○	○
Session key disclosure attack	○	×	○

○ : Preserves the security properties ×: Do not preserve the security properties

인증에 사용되는 정보를 알아내는 것은 불가능하다.

• Man-in-the-middle attack

중간자 공격은 네트워크 통신을 조작하여 통신 내용을 도청하거나 조작하는 공격 기법이다. Lei 등과 Park 등의 방식은 공격자가 정보를 조작하여 서버와 인증 또는 사용자의 개인키를 구할 수 있어 중간자 공격에 취약함을 보여준다. 하지만 제안한 방식은 사용자간에 x, y와 공개키 h를 교환하여 $y_B * h_B = x_B * x_A$, $y_A * h_A = x_A * x_B$를 계산하여 상호인증을 하게 되므로 중간에서 값이 위·변조 되었는지 확인이 가능하여 중간자 공격이 불가능하다.

• User impersonation attack

사용자 위장 공격은 공격자가 사용자로 위장하여 인증을 시도하는 공격이다. 제안한 방식에서 공격자가 사용자인 것처럼 위장하기 위해서는 상호인증에 사용되는 x, y, h를 알아야 한다. 하지만 x, y, h값을 구하기 위해서는 개인키인 g, f와 임의의 값인 r을 알아야하며 이는 NTRU의 암호학적으로 사용되는 수학의 어려움인 큰 크기의 격자에서 작은 벡터를 찾는 수학 문제와 등가이므로 계산 상 불가능하다.

• Replay attack

재사용 공격은 사용자가 사용한 정보를 공격자가 도청으로 가로채 다시 사용하는 공격이다. 제안한 방식은 매 세션마다 임의로 생성되는 r을 사용하여 상호인증에 사용되는 x를 계산하므로 한번 사용한 정보를 재사용하여 인증하는 것은 불가능하다.

• Session key disclosure attack

세션키가 안전하지 않은 메모리에 저장되어 공격자에 의해 노출되어도 제안한 방식의 세션키인 Key_{AB} 또는 Key_{BA}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.

5. 결 론

최근 ETSI 및 IEEE 등의 표준 협회에서는 양자 컴퓨팅의 위협이 실현되기 이전에 안전한 암호를 준비하고 실행하여 방어 체계를 갖춰야 한다고 권고[11]하고 있다. 양자 컴퓨팅에 안전한 암호 중 하나인 격자 기반 암호 표준 NTRU 암호 알고리즘을 이용한 Lei 등의 NTRU 키 분배 프로토콜은 양자 컴퓨팅 공격에는 안전하지만 중간자 공격에 취약함을 보이며 비밀키가 도출되는 문제가 발생하였다.

본 논문은 Lei 등의 NTRU 키 분배 프로토콜의 취약점인 중간자 공격을 양자 컴퓨팅에 보안을 유지하기 위해 NTRU 컨볼루션 곱셈 연산만을 사용하여 상인증 단계를 추가하므로 중간자 공격과 양자 컴퓨팅에 안전한 프로토콜로 개선하였다. 이러한 NTRU 알고리즘은 현재 널리 사용되고 있는 공개키 암호 알고리즘인 RSA나 ECC 보다 빠른 연산으로 컴퓨터 환경만이 아닌 저사양 환경으로 스마트카드, NFC 등에도 효과적으로 적용될 수 있다.

REFERENCE

[1] R.P. Feynman, “Simulating Pysics with Computers,” *International Journal of Theoretical Physics*, Vol. 21, No. 6-7, pp. 467-488, 1982.

[2] P.W. Shor, “Algorithms for Quantum Compu-

tation: Discrete Logarithms and Factoring," *Proceedings of 35th Annual Symposium on Foundations of Computer Science and IEEE Computer Society*, pp. 124-134, 1994.

[3] S.Y. Lee, K.S. Park, Y.H. Park, and Y.H. Park, "Symmetric Key-Based Remote User Authentication Scheme with Forward Secrecy," *Journal of Korea Multimedia Society*, Vol. 19, No. 3, pp. 585-594, 2016.

[4] J. Hoffstein, J. Pipher, and J.H. Silverman, "NTRU: A Ring-Based Public Key Cryptosystem," *Algorithmic Number Theory and Lecture Notes in Computer Science*, Vol. 1423, pp. 267-288, 1998.

[5] 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.

[6] X. Lei and X. Liao, "NTRU-KE: A Lattice-based Public Key Exchange Protocol," *IACR Cryptology ePrint Archive 2013/718*, 2013.

[7] S.W. Park and I.Y. Lee, "Anonymous Authentication Scheme Based on NTRU for the Protection of Payment Information in NFC Mobile Environment," *Journal of Information Processing Systems*, Vol. 9, No. 3, pp. 461-476, 2013.

[8] S.W. Park and I.Y. Lee, "Authentication Scheme Based on NTRU for the Protection of Payment Information in NFC Mobile Environment," *Korea Information Processing Society Transactions on Computer and Communication Systems*, Vol. 2, No. 3, pp. 133-142, 2013.

[9] M.R. Valluri, Cryptanalysis of Xinyu et al.'s NTRU-Lattice Based Key Exchange Protocol, https://arxiv.org/abs/1611.08686v1, 2016.

[10] Y.S. Jheng, "Security Analysis of a NTRU-based Mutual Authentication Scheme," *Proceeding of Asia-Pacific Network Operations and Management Symposium,* pp. 3, 2016.

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

[12] NIST, *Report on Post-Quantum Cryptography*, NISTIR 8105, 2016.

정 성 하

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

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 수석연구원
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, 양자 후 암호체계