https://doi.org/10.7840/kics.2017.42.11.2200

양자 컴퓨터 공격에 안전한 격자 기반 키 교환 방식의 비교

최 락 용◆, 안 형 철*, 이 지 은**, 김 성 숙**, 김 광 조°

Comparison of Lattice-Based Key Exchange Protocols for Quantum Computing Attack

Rakyong Choi◆, Hyeongcheol An*, Jeeun Lee**, Sungsook Kim**, Kwangjo Kim°

요 약

격자 기반 암호는 양자 컴퓨터를 이용한 공격에도 안전한 포스트 양자 암호(Post Quantum Cryptography, PQC)의 하나로 각광받고 있으며, 함수형 암호, 준동형 암호, 준동형 서명, 난독화 등 다양한 목적으로 연구가 진행 중에 있다. 격자 기반 키 교환 프로토콜은 기존에 사용하고 있는 DH(Diffie-Hellman) 키 교환 프로토콜을 비롯한 정수론 기반의 키 교환 프로토콜을 대체하는 기술로 본 논문에서는 총 7가지의 격자 기반 (인증) 키 교환 프로토콜에 대해 기반 문제, 샘플링 알고리즘, 보안도 및 안전성 분석 기법, 구현 효율성 등을 비교하고 향후 연구를 제시하였다.

Key Words : Lattice-based Cryptography, Key Exchange(KE) Protocol, Learning with Errors(LWE) Problem, Quantum-accessible Random Oracle Model(QaROM)

ABSTRACT

Lattice-based cryptography is one of attractive candidates for Post Quantum Cryptography(PQC), which remains secure from quantum adversaries. Lattice-based cryptography is currently applied to many cryptographic schemes like functional encryption, homomorphic encryption, homomorphic signature, and obfuscation. Likewise, lattice-based key exchange protocols replace DH-like key exchange protocols in a quantum world. In this paper, we study 7 known lattice-based (authenticated) key exchange protocols and compare those protocols over hard problem, sampling algorithm, security analysis, and efficiency followed by further work.

Ⅰ. 서 론

이산 대수 문제, 소인수 분해 문제의 어려움에 기반한 키 교환(Key Exchange, KE) 프로토콜 및 인증 키 교환(Authenticated Key Exchange, AKE) 프로토콜은 Shor 알고리즘에 따라 양자 컴퓨터의 공격에 대단히 취약하다. 따라서 양자컴퓨터의 공격에도 안전한 KE가 필요하다. 포스트 양자 암호(Post-Quantum Cryptography)의 필요성이 제기되고 있으며, 그 중 하나로 격자 기반 KE 프로토콜이 알려져 있다. 또한 인

※ 본 연구는 2017년도 정부(과학기술정보통신부)의 재원으로 정보통신기술진흥센터의 지원을 받아 수행되었습니다. (No.2017-0-00555, 양자 컴퓨터 환경에서 래티스 문제를 이용한 다자간 인증키교환 프로토콜 연구)
◆ First Author : School of Computing, KAIST, thepride@kaist.ac.kr, 학생회원
° Corresponding Author : Graduate School of Information Security, KAIST, kkj@kaist.ac.kr, 정회원
* Graduate School of Information Security, KAIST, anh1026@kaist.ac.kr
** School of Computing, KAIST, jeeun.lee@kaist.ac.kr, kusino@kaist.ac.kr
논문번호 : KICS2017-08-228, Received August 31, 2017; Revised November 8, 2017; Accepted November 13, 2017

증과정이 추가된 AKE 프로토콜은 기존의 KE 프로토콜에 비하여 상호간의 인증 정보를 교환하여 중간자 공격(Man-in-the-Middle Attack)에 안전하다.

본 논문에서 분석한 격자 기반 KE 및 AKE 프로토콜은 DXL12[1], BCNS15[2], NewHope16[3], Frodo16[4], ZZD+15[5], spKEX17[6], Kyber17[7]의 총 7 가지로 최근 Ring-LWE 기반 키 교환 프로토콜에 대해 에러 보정 함수의 취약점 또는 격자 상의 특별한 기저를 이용하여 공격하는 논문이 Fluhrer[8], Gong과 Zhao[9], Ding 등[10]에 의해 각각 발표된 가운데 각각의 프로토콜에 대하여 소개하고 기반 문제, 실행시간, 데이터 전송량, 샘플링 알고리즘 등에 대하여 비교한다.

1.1 논문의 구성

본 논문의 구성은 다음과 같다. Ⅱ장에서 격자 및 LWE 문제에 대한 설명과 KE와 AKE 프로토콜, ROM(Random Oracle Model) 및 QaROM(Quantum accessible Random Oracle Model)에 대하여 간략히 설명한다. 이후 Ⅲ장은 7 가지의 격자 기반 KE 및 AKE 프로토콜 대하여 소개한다. Ⅳ장에서는 앞서 설명한 프로토콜에 대하여 기반 문제, 실행시간, 데이터 전송량, 샘플링 알고리즘, 디지털컴퓨터와 양자 컴퓨터에 대한 보안도에 대하여 비교하고 표로 정리한다. 마지막으로 Ⅴ장에서는 향후 격자 기반 키 교환 프로토콜을 활용한 연구과제에 대하여 논의하고 결론을 내린다.

Ⅱ. 배경지식

2.1 격자 및 LWE 문제

2.1.1.격자(Lattice)

격자(Lattice) L 이란 실수 공간 $\mathbb{R}^n$의 부분집합으로 덧셈 연산을 가지는 이산 부분군(discrete subgroup)을 이룬다.

$$L=\left\{\sum_{i\le n} x_i b_i : x_i \in \mathbb{Z}\right\} \quad (1)$$

이 때 격자 L을 생성해주는 생성 집합(generating set) $B=\{b_i\}_{i=1}^{k\le n}$을 기저(basis)라고 말하며, 특히 격자 L의 모든 벡터가 정수 공간 $\mathbb{Z}^m$ 상에 있을 경우 이러한 격자를 정수 격자(integer lattice)라고 칭한다.

격자 L에서 가장 작은 크기를 가지는 0인 아닌 벡터 b에 대해 $\lambda_1(L)=\|b\|$라고 정의할 때, γ-Shortest Vector Problem(SVP_γ) 문제는 크기가 $\|b\|\le\gamma\cdot\lambda_1(L)$인 벡터 b를 찾는 문제로 최악의 경우에 어려운(worst-case hard) 문제 중 하나로 잘 알려져있다.

격자를 이용한 어려운 문제 중 암호학에서 주로 이용되는 문제로는 Learning With Errors(LWE) 문제와 Small Integer Solution(SIS) 문제가 있으며 각각의 문제들은 평균적으로 어려운(average-case hard) 문제로 SVP_γ 문제로 축약(reduction) 가능하며 따라서 LWE 문제나 SIS 문제를 해결할 수 있을 경우 어떠한 격자에 대해서도 SVP_γ 문제를 해결할 수 있다.

2.1.2 LWE 문제

LWE 문제는 Search LWE 문제와 Decision LWE 문제가 있으며 Search LWE 문제는 비밀 벡터 $s\in\mathbb{Z}_q^n$와 임의의 벡터 $a_i\in\mathbb{Z}_q^n$, 가우시안 분포 D가 있어 작은 크기의 에러 e_i를 가우시안 분포 D에서 추출할 때 쌍 $\{a_i, a_i^T s+e_i\}_i \in \mathbb{Z}_q^n\times\mathbb{Z}_q$에서 비밀 벡터 s를 찾아내는 문제이다.

Decision LWE 문제는 LWE 문제 쌍 $\{a_i, a_i^T s+e_i\}_i \in \mathbb{Z}_q^n\times\mathbb{Z}_q$와 임의의 쌍 $\{a_i, b_i'\}\in\mathbb{Z}_q^n\times\mathbb{Z}_q$을 구분할 수 없는 문제로 Search LWE 문제와 Decision LWE 문제는 동치이며 키 교환 프로토콜 설계 및 안전성 증명에서는 Decision LWE 문제가 이용된다.

이밖에 효율적인 격자 기반 암호를 설계하기 위해 에러 추가를 임의의 가우시안 분포에서 다른 분포로 변경할 수 있는 방법(Renyi Divergence)[11], 작은 크기의 비밀 벡터를 가지는 small-secret LWE 문제[12], 에러 추출을 결정론적(deterministic)으로 하는 Learning With Rounding(LWR) 문제[13], 격자 L이 다항식 환(polynomial ring) $\mathbb{Z}[x]/f$에서 부분군이 아닌 아이디얼(ideal) 또는 가군(module)이 되는 Ring-LWE[14] 및 Module-LWE[15] 문제 등이 있다. 특히 Ring-LWE 문제의 경우 빠른 다항식 연산을 가능하게 하여 구현 시 실용적이며, Module-LWE 문제는 Ring-LWE 문제를 이용해 격자 기반 암호 설계 시 보안 매개변수를 변경하려면 환을 변경해야하는 것에 반해 환을 변경하지 않아도 보안 매개변수의 유연성(flexibility)를 제공하여 보안 매개변수 설정이 쉽도록 제안된 문제이다.

2.2 KE와 AKE 프로토콜

키 교환(Key Exchange, KE) 프로토콜은 그림 1과 같이 신뢰되지 않은 환경에서의 양자(Two-party)간 통신을 안전하게 하기 위한 알고리즘으로 비밀 정보를 공유하지 않은 상태에서 암호학적으로 안전한 공통 비밀키를 생성할 수 있는 방법으로 DH(Diffie-Hellman) KE 프로토콜이 널리 알려져 있다. 그러나 인증 과정이 없으면 중간자 공격 등에 취약하기 때문에 인증 키 교환(Authenticated Key Exchange, AKE) 프로토콜이 필요하다.

AKE 프로토콜은 그림 2와 같이 상호 간의 인증과정이 추가되어 기존 KE 프로토콜이 도청만이 가능한 수동적 공격자 모델에 대해서만 안전성을 보장하는 것을 극복하고 각각의 유저에 대한 인증성(authenticity)을 제공하여 중간자 공격 등 통신 중 데이터에 대한 위·변조가 가능한 능동적 공격자 모델에 대해서도 안전성을 보장해주는 프로토콜이다.

일반적으로 AKE를 달성하기 위하여 KE 프로토콜에서 해시함수나 공개키 암호화를 활용하여 인증 과정을 추가한다.

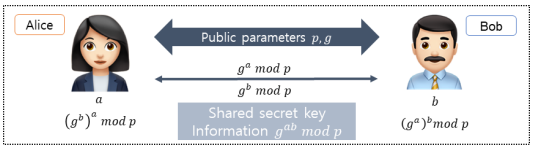

Fig. 1. KE protocol

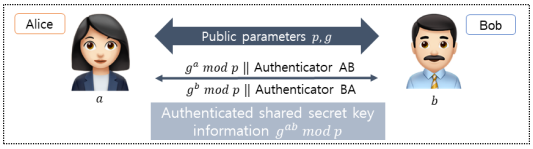

Fig. 2. AKE protocol

2.3 ROM과 QaROM

암호 시스템의 안전성을 증명하기 위해서는 공격자 모형을 제시하고 안전하다고 알려진 가정으로 환원시키거나 가상의 이론적 모델을 사용하여 공격자의 이점(advantage)이 무시해도 될 정도(negligible)인지 계산한다. 이와 같은 방법은 실제로 엄밀하게 증명하지 않다는 문제점이 있으나 사용된 암호함수에 대한 엄밀한 안전성 분석이 어렵기 때문에 보편적으로 많이 사용되고 있다. 본 연구에서는 격자 기반 키 교환 프로토콜의 안전성을 증명하기 위해 고전 컴퓨터와 양자 컴퓨터 능력을 가진 공격자를 가정하고 각각의 안전성을 증명할 계획이다.

사용자와 공격자 모두 고전 컴퓨터를 사용하는 경우 Bellare와 Rogaway[16]가 제시한 랜덤 오라클 모델(Random Oracle Model, ROM)을 사용하여 안전성을 증명한다. 랜덤 오라클은 입력 질의에 대해 유사난수 함수 기반으로 임의의 결과를 출력하는 이론적인 블랙박스이다. 예를 들어 암호화 스킴 Π = (KeyGen, Enc, Dec)과 공격자 $A=(A_1,A_2)$의 경우 atk $\in$ {CPA, CCA1, CCA2}와 보안 수준 $k\in N$에 대하여 공격자의 이점(advantage)은 다음과 같이 계산할 수 있다.

$$Adv_{A,\Pi}^{\mathrm{ind-atk}}(k) := 2 \cdot \Pr[(pk,sk)\leftarrow \mathrm{KeyGen}(1^k); (m_0,m_1,s)\leftarrow A_1^{O_1}(pk); b\leftarrow\{0,1\}; c\leftarrow \mathrm{Enc}_{pk}(m_b): A_2^{O_2}(m_0,m_1,s,c)=b] - 1 \quad (2)$$

이 때, atk = CPA인 경우 $O_1=O_2=\varepsilon$ (empty string), atk = CCA1인 경우 $O_1=\mathrm{Dec}_{sk}$, $O_2=\varepsilon$, atk = CCA2인 경우 $O_1=O_2=\mathrm{Dec}_{sk}$ 이다. 다항시간 공격자에 대하여 $Adv_{A,\Pi}^{\mathrm{ind-atk}}$가 무시할 수 있는 값인 경우 암호화 스킴 Π가 IND-atk에 안전하다고 말한다.

사용자는 고전 컴퓨터, 공격자는 양자 컴퓨터를 사용하는 경우에는 Boneh[17] 등이 제시한 QaROM을 사용하여 안전성을 증명한다. QaROM은 양자 유사난수 함수를 기반으로 임의의 결과를 출력하며, 입력 질의로 양자 상태를 제시할 수 있다. 최근 양자 컴퓨터의 발전에 따라 다양한 포스트 양자 암호 시스템이 제안되고 있고 따라서 기존의 ROM 뿐만 아니라 QaROM로 안전성을 증명하는 다양한 논문[18][19]들이 발표되고 있다.

Ⅲ. Lattice 기반 KE 프로토콜

이번 장에서는 총 7가지의 격자 기반 KE 및 AKE에 대하여 설명한다. 각 프로토콜의 매개변수 크기는 각 프로토콜의 매개변수 크기는 현재 알려진 SVP 문제에 대한 공격 방법 중 가장 효율적인 방법인 sieving[20]을 이용하여 보안 매개변수 λ에 대한 기존 컴퓨터[21]와 양자 컴퓨터[22]의 n, q 값을 계산하는 것으로 표 1[23]에 정리하였다.

3.1 DXL12

DXL12 프로토콜은 Ding 등이 2012년에 발표한 프로토콜로 격자 기반 KE 프로토콜 중에서 가장 먼저

Table 1. Comparison of parameters for lattice-based key exchange protocol

	DXL12	BCNS15	NewHope16	Frodo16	ZZD+15	spKEX17	Kyber17
n	1024	1024	1024	752	1024 / 2048	570 / 710	256
q	$2^{32}-1$	$2^{32}-1$	12289	2^{15}	$2^{45} \sim 2^{50}$	$2^{12} \sim 2^{14}$	7681
λ	128	86	229	144	75-230	128, 256	161

n : Dimension of Matrix or Vector, q : Modulus Value, λ : Security Parameter

발표되었다. 이후 이 프로토콜은 Peikert[24]에 의해 발전되었다. Ring-LWE 기반 문제로 설계되어 효율성이 증가하였다. 그러나 실제 구현은 이루어지지 않았다는 단점이 있다. 또한 매개변수 크기가 $q=2^{32}-1$로 크기 때문에 Ring-LWE를 사용했음에도 LWE문제를 사용한 프로토콜에 비하여 효율성이 크게 증가하지는 않는다.

3.2 BCNS15

BCNS15 프로토콜은 Bos 등에 의해 2015년 발표된 프로토콜로 DXL 프로토콜을 실제 최적화 하여 구현하였다. 이 프로토콜에서 사용하는 이산 가우시안 분포는 타이밍 공격(Timing Attack)에 취약하다[25]. 또한 CPU의 캐시 메모리를 활용한 캐시 공격(Cache Attack)[26]의 가능성이 있다. 그러나 격자 기반 KE에서 OpenSSL에 추가되어 상용화를 시도하였고, TLS/SSL 프로토콜에서 추가하여 사용하고 있다.

3.3 NewHope16

NewHope16 프로토콜은 Alkim 등에 의해 BCNS 프로토콜의 단점을 보완하여 설계 및 구현하였다. BCNS 프로토콜은 매개변수 중 $q=2^{32}-1$로 다른 KE 프로토콜에 비하여 크기 때문에 안전하지 않으며 효율성이 떨어진다. 그러나 NewHope에서는 $q=12,289<2^{14}$까지 줄여서 취약점을 보완하였고, 효율성이 증가하였다. 또한 NTT(Number Theoretic Transform) 연산에서 Intel CPU에서 지원하는 AVX2(Advanced Vector Extensions)을 사용하기 때문에 프로토콜의 속도가 증가하였다.

현재 Google Chrome Canary 브라우저와 서버 간의 통신과정에서 KE 프로토콜로 NewHope을 사용하고 있다는 것이 특징이다. 앞서 설명한 BCNS의 에러 샘플링 알고리즘을 이산 가우시안 분포에서 이항분포로 바꾸어 타이밍 공격에 대하여 안전하다.

3.4 Frodo16

Frodo16 프로토콜은 Bos 등이 설계하고 구현한 프로토콜로 Ring-LWE 문제를 사용한 NewHope의 위험성을 가정하고, LWE 문제를 기반으로 하는 것이 가장 큰 특징이다. 매개변수의 크기는 $n=752$이며, $q=2^{15}$이다. Ring-LWE 문제를 기반으로 설계한 BCNS 프로토콜과 비교하여 실행시간의 차이가 크게 나지 않는 것은 $q=2^{15}<2^{32}-1$로 매개변수의 크기가 크게 줄었기 때문에 LWE 문제를 기반으로 했음에도 불구하고 오히려 HTTP 환경에서는 더 빠른 것을 알 수 있다.

3.5 ZZD+15

앞서 설명한 KE 프로토콜들과 ZZD+15 프로토콜의 가장 큰 차이는 인증과정이 있다는 것이다. 이전의 KE 프로토콜은 매개변수의 크기가 고정되어 있지만, 매개변수의 크기가 가변적으로 설정할 수 있다. n의 크기를 1024-bit와 2048-bit로 설정하여 각각의 매개변수 크기에 대하여 보안도를 가변적으로 조절할 수 있다.

인증과정에서는 공격자가 세션 키를 바꿀 수 없는 HMQV[27] 프로토콜을 사용하였다. 해시함수를 추가한 방법으로 효율성이 증가하였다.

3.6 spKEX17

spKEX17 프로토콜은 Bhattacharya 등에 의해 2017년 발표된 프로토콜로 sparse-ternary LWR 문제를 제안하고 이를 기반으로 설계되었다. sparse-ternary LWR 문제란 LWR 문제의 변형 문제로 비밀벡터 s가 $s \in \{-1,0,1\}^n$에서 나오며 s의 Hamming 무게 $wt(s)$가 최대 h인 경우에도 어려운 문제로 spLWE 문제[28]를 LWR로 해석한 문제이다.

spKEX17 프로토콜은 매번 새로운 공개키 A를 생성하여 순방향 비밀성(Forward Security)을 제공하며, 에러 보정 방법을 개선하여 Frodo와 비교하여 30% 이상 뛰어난 데이터 전송량을 가진다.

3.7 Kyber17

Kyber17 프로토콜은 Bos 등에 의해 2017년 발표된 프로토콜로 CPA 안전 암호를 설계한 뒤 QaROM에서의 Fujisaki-Okamoto 방법[29,30]을 이용하여 이로부터 QaROM에서 CCA 공격에 안전한 KE 프로토콜, AKE 프로토콜을 각각 설계하였다.

Kyber 프로토콜의 안전성은 Module-LWE 문제의 어려움을 통해 증명 가능하며 따라서 기존의 Ring-LWE 문제 기반 KE/AKE 프로토콜과 달리 보안 매개변수 선택에 유연성을 제공한다.

Ⅳ. KE 프로토콜 비교

이번 장에서는 기반문제, 실행시간, 데이터 전송량, 에러 샘플링, 그리고 보안도를 중심으로 각 프로토콜을 비교한다. 각 프로토콜의 비교는 표 2[28]에 정리하였다. 실험은 Intel CPU 3.4GHz에서 실행시간을 측정하였다.

4.1 실행시간

비교한 7 가지의 프로토콜 중 가장 빠른 프로토콜은 NewHope16와 Kyber17이며 약 0.3ms의 실행시간이 걸린다는 것을 확인할 수 있다. 이는 기반문제가 Ring-LWE 및 Module-LWE를 사용하여 프로토콜 과정의 고속화에 기여하였고, 소프트웨어 최적화가 이루어졌다는 것으로 분석할 수 있다. 또한 LWE 문제를 사용한 Frodo16의 경우 2.6ms가 걸렸고, 이것은 BCNS15의 2.8ms와 비슷한 실행시간을 가진다는 것을 알 수 있다.

4.2 데이터 전송량

데이터 전송량에서는 NewHope16 프로토콜이 4KB로 7 가지의 프로토콜 중 가장 적은 양을 사용한다. Kyber17 프로토콜도 약 4.4KB로 적은 양의 데이터를 사용한다는 것을 알 수 있다. 반면에 Frodo16는 대략 6배의 23KB의 데이터를 전송한다. LWE 문제를 사용하면 데이터의 전송량이 커진다는 단점이 존재한다. NewHope16 프로토콜의 경우 Ring-LWE를 사용하였지만, Frodo16는 LWE 문제를 사용하여 데이터 전송량에서 단점을 가지고 있다. BCNS15는 약 8KB의 데이터가 전송되며 Frodo16보다 적은 것을 알 수 있다. ZZD+15는 다른 프로토콜과는 달리 인증과정이 추가되어 최대 25KB의 데이터가 전송된 다는 것을 확인할 수 있다. 그러나 AKE 프로토콜인 Kyber17은 인증과정이 추가되었음에도 불구하고 NewHope16과 비슷한 데이터 전송량을 가지는 것을 확인할 수 있다.

4.3 에러 샘플링

DXL12, BCNS15, ZZD+15은 이산 가우시안 분포(Discrete Gaussian Distribution)을 에러 샘플링 알고리즘으로 사용하였다. 또한 NewHope16과 Kyber17은 이항 분포(Binomial Distribution)을 사용하였고,

Table 2. Comparison of lattice-based key exchange protocol

	DXL12	BCNS15	NewHope16	Frodo16	ZZD+15	spKEX17	Kyber17
Protocol	KE	KE	KE	KE	AKE	KE	AKE
Hard Problem	LWE/ Ring-LWE	Ring-LWE	Ring-LWE	LWE	Ring-LWE	sp-LWE	Module-LWE
Execution Time (ms)	-	2.8	0.3	2.6	37.8-119.5	3.6	0.3
Payload (KB)	-	8	4	23	12-25	15.3	4.4-4.6
Distribution for Error Sampling	Discrete Gaussian distribution	Discrete Gaussian distribution	Binomial distribution	Continuous Gaussian distribution	Discrete Gaussian distribution	N/A	Binomial distribution
Classical Security Level (bit)	128	86	229	144	75-230	128	-
Quantum Security Level (bit)	-	78	206	130	-	256	161
Way of Security Proof	-	-	-	-	ROM	-	QaROM

Frodo16은 Rounded 연속 가우시안(Rounded Continuous Gaussian Distribution) 분포를 사용하였다. 한편 spKEX17의 경우 에러 추출 대신 라운딩을 이용한 LWR 문제를 기반으로 하여 에러 샘플링을 사용하지 않았다.

4.4 보안도(Security Level)

7가지의 KE 및 AKE 프로토콜은 격자 기반의 프로토콜로 양자 컴퓨터의 공격에 안전하다. 따라서 디지털 컴퓨터의 보안도와 양자 컴퓨터의 보안도로 구분된다. 종래 보안도는 디지털 컴퓨터를 이용한 현재 알려진 가장 효과적인 격자 기반 문제에 대한 공격을 사용하여 정의한다. DH KE 프로토콜의 경우 1,024-bit의 매개변수를 사용하면 80-bit의 보안도를 가진다. 기존 디지털 컴퓨터에서 7 가지의 KE 및 AKE 프로토콜의 보안도는 86-bit에서 256-bit까지 나타나 있다. 따라서 분석한 프로토콜 모두 실제 환경에서 안전성에 문제없이 사용할 수 있다는 것을 알 수 있다.

양자 보안도의 경우 공격 모델이 현재 사용하고 있는 디지털 컴퓨터가 아닌 양자 컴퓨터를 활용한 공격에서의 안전성을 뜻한다. 양자 보안도는 양자 컴퓨터를 이용한 현재 알려진 가장 효과적인 격자 기반 문제에 대한 공격을 사용하여 정의한다. DXL12과 ZZD+15 프로토콜의 양자 보안도는 공개되지 않았고, NewHope16 프로토콜이 206-bit인 것을 확인할 수 있다. 이것은 양자 컴퓨터가 상용화되어도 KE 프로토콜의 안전성을 보장한다고 할 수 있다.

V. 결론 및 향후 연구

본 논문에서는 양자 컴퓨터 환경에서 격자 기반 다자(Multi-party)간 인증 키 교환 프로토콜 설계를 위해 기존 격자 기반 KE/AKE 프로토콜인 DXL, BCNS, NewHope, Frodo, ZZD+, spKEX, Kyber 프로토콜에 대한 특징 및 각각의 보안 매개변수에 대해 소개하고 각 프로토콜에 대해 기존 컴퓨터와 양자 컴퓨터에서의 기반 문제, 샘플링 알고리즘, 보안도 및 안전성 분석 기법, 구현 효율성 등을 비교하였다.

앞서 분석한 기존 프로토콜들은 모두 양자간에 사용할 수 있도록 설계되었으며 다자간에 적용할 경우 안전성을 확인할 수 없다. 또한 안전성 증명에서 Kyber 프로토콜을 제외하고는 양자 컴퓨터를 사용할 수 있는 공격자가 아닌 일반적인 공격자를 가정하여 양자 컴퓨터를 이용한 공격에 대한 이론적 안전성이 정리되어있지 않다.

따라서 향후 연구로는 다자간 계산(Multi Party Computation, MPC), QaROM 등 양자 컴퓨터 공격자 모델 등에 대해서 연구하고, 이를 바탕으로 SSL, TLS 등 실제 인터넷 환경에서 구현 가능한 다자간 KE/AKE 프로토콜을 설계하고자 한다.

References

[1] J. Ding, X. Xie, and X. Lin, *A simple provably secure key exchange scheme based on the learning with errors problem*, Cryptology ePrint Archive, Report 2012/688, 2012.

[2] J. Bos, et al., “Post-quantum key exchange for the TLS protocol from the ring learning with errors problem,” in *2015 IEEE Symp. Security and Privacy (S&P)*, pp. 553-570, San Jose, USA, May 2015.

[3] E. Alkim, et al., “Post-quantum key exchange - A new hope,” in *USENIX Secur. Symp. Usenix*, pp. 327-423, Austin, USA, Jan. 2016.

[4] J. Bos, et al., “Frodo: Take off the ring! practical, quantum-secure key exchange from LWE,” in *Proc. 23rd ACM Conf. Comput. and Commun. Secur. (CCS) ACM*, pp. 1006-1018, Vienna, Austria, Oct. 2016.

[5] J. Zhang, et al., “Authenticated key exchange from ideal lattices,” *EUROCRYPT 2015,* Springer, pp. 719-751, Sofia, Bulgaria, Apr. 2015.

[6] S. Bhattacharya, et al., *spKEX: An optimized lattice-based key exchange*, Cryptology ePrint Archive, Report 2017/709, 2017.

[7] J. Bos, et al., *CRYSTALS-Kyber: a CCA-secure module-lattice-based KEM*, Cryptology ePrint Archive, Report 2017/634, 2017.

[8] S. R. Fluhrer, *Cryptanalysis of ring-LWE based key exchange with key share reuse*, Cryptology ePrint Archive, Report 2016/085, 2016.

[9] B. Gong and Y. Zhao, “Cryptanalysis of RLWE-Based one-pass authenticated key exchange,” *PQCrypto,* Springer, pp. 163-183, Utrecht, the Netherlands, Jun. 2017.

[10] J. Ding, et al., *Leakage of signal function with reused keys in RLWE key exchange*, Cryptology ePrint Archive, Report 2016/1176, 2016.

[11] S. Bai, et al., "Improved security proofs in lattice-based cryptography: using the Rényi divergence rather than the statistical distance," *Asiacrypt 2015,* Springer, pp. 3-24, Auckland, New Zealand, Nov. 2015.

[12] D. Micciancio and C. Peikert, "Hardness of SIS and LWE with small parameters," *CRYPTO 2013,* Springer, pp. 21-39, Santa Barbara, USA, Aug. 2013.

[13] A. Banerjee, C. Peikert, and A. Rosen, "Pseudorandom functions and lattices," *EUROCRYPT 2012,* Springer, pp. 719-737, Cambridge, United Kingdom, Apr. 2012.

[14] V. Lyubashevsky, C. Peikert, and O. Regev, "On ideal lattices and learning with errors over rings," *EUROCRYPT 2010,* Springer, pp. 1-23, Monaco, Monaco, May 2010.

[15] A. Langlois and D. Stehlé, "Worst-case to average-case reductions for module lattices," *Designs, Codes and Cryptography,* vol. 75, no. 3, pp. 565-599, 2015.

[16] M. Bellare and P. Rogaway, "Random oracles are practical: A paradigm for designing efficient protocols," in *Proc. 1st ACM Conf. Comput. and Commun. Secur. (CCS)*, pp. 62-73, Fairfax, USA, Nov. 1993.

[17] D. Boneh, et al., "Random oracles in a quantum world," *Asiacrypt 2011,* Springer, pp. 41-67, Seoul, Korea, Dec. 2011.

[18] M. Zhandry, "Secure identity-based encryption in the quantum random oracle model," *CRYPTO 2012*, Springer, pp. 758-775, Santa Barbara, USA, Aug. 2012.

[19] D. Boneh and M. Zhandry, "Secure signatures and chosen ciphertext security in a quantum computing world," *CRYPTO 2013,* Springer, pp. 361-379, Santa Barbara, USA, Aug. 2013.

[20] M. Ajtai, M. Kumar, and D. Sivakumar, "A sieve algorithm for the shortest lattice vector problem," in *Proc. 33rd Annu. ACM Symp. Theory of Comput. (STOC),* pp. 601-610, Crete, Greece, Jul. 2001.

[21] A. Becker, et al., "New directions in nearest neighbor searching with applications to lattice sieving," in *Proc. 27th Annu. ACM-SIAM Symp. Discrete Algorithms (SODA),* pp. 10-24, Arlington, USA, Jan. 2016.

[22] D. Micciancio and P. Voulgaris. "Faster exponential time algorithms for the shortest vector problem," in *Proc. 21st Annu. ACM-SIAM Symp. Discrete Algorithms (SODA)*, pp. 1468-1480, Austin, USA, Jan. 2010.

[23] H. An, et al., "Comparison of lattice-based key exchange protocols," *CISC-S*, Korea, Jun. 2017.

[24] C. Peikert, "Lattice cryptography for the internet," *PQCrypto,* Springer, pp. 197-219, Waterloo, Canada, Oct. 2014.

[25] M. Saarinen, *Gaussian sampling precision and information leakage in lattice cryptography*, Cryptology ePrint Archive, Report 2015/953, 2015.

[26] D. Osvik, A. Shamir, and E. Tromer, "Cache attacks and countermeasures: the case of AES," *Cryptographers' Track at the RSA Conf. (CT-RSA),* Springer, pp. 1-20, Feb. 2006.

[27] H. Krawczyk, "HMQV: A high-performance secure diffie-hellman protocol," *CRYPTO 2005,* Springer, pp. 546-566, Santa Barbara, USA, Aug. 2005.

[28] J. Cheon, et al., "A practical post-quantum public-key cryptosystem based on spLWE," *ICISC,* Springer, pp. 51-74, Seoul, Korea, Nov. 2016.

[29] E. Targhi and D. Unruh, "Post-quantum security of the Fujisaki-Okamoto and OAEP transforms," *TCC 2016-B,* Springer, pp. 192-216, Beijing, China, Oct.-Nov. 2016.

[30] D. Hofheinz, K. Hövelmanns, and E. Kiltz, *A modular analysis of the Fujisaki-Okamoto transformation*, Cryptology ePrint Archive, Report 2017/604, 2017.

최 락 용 (Rakyong Choi)

2011년 2월 : KAIST 수리과학과 졸업
2013년 8월 : KAIST 수리과학과 석사
2014년 3월~현재 : KAIST 전산학부 박사과정

<관심분야> 포스트 양자 암호, 래티스 기반 암호, 준동형 서명, 키 교환 프로토콜

안 형 철 (Hyeongcheol An)

2016년 8월 : 세종대학교 수학과 졸업
2016년 9월~현재 : KAIST 정보보호대학원 석사과정
<관심분야> 포스트 양자 암호, 키 교환 프로토콜

이 지 은 (Jeeun Lee)

2013년 2월 : KAIST 물리학과 졸업
2013년 3월~현재 : KAIST 전산학부 석박사통합과정
<관심분야> 포스트 양자 암호, 양자 암호, 안전성 증명

김 성 숙 (Sungsook Kim)

2011년 2월 : 육군사관학교 운영분석학과 졸업
2016년 2월~현재 : KAIST 전산학부 석사과정
<관심분야> 포스트 양자 암호, 안전성 증명

김 광 조 (Kwangjo Kim)

1980년 2월 : 연세대학교 전자공학과 졸업
1983년 8월 : 연세대학교 전자공학과 석사
1991년 3월 : 요코하마 국립대 전자공학과 박사
1998년 1월~2006년 8월 : ICU 전산학과 교수
2006년 8월~2009년 2월 : ICU 전산학과장
2009년 3월~현재 : 카이스트 전산학부 정보보호대학원 교수
2010년 1월~현재 : 한국 정보보호학회 명예회장
2014년 4월~현재 : IFIP TC-11 한국 대표
2017년 3월~현재 : 세계암호학회(IACR) 석학회원(Fellow)
<관심분야> 암호 및 정보보호 이론과 응용