JDCS
디지털콘텐츠학회논문지
Journal of Digital Contents Society
Vol. 24, No. 1, pp. 167-175, Jan. 2023

Check for updates

TLS 1.3에서 양자내성암호 적용 가능성 분석

이 성 우[1] · 손 태 식[2*]
[1]아주대학교 사이버보안학과 석사과정
[2*]아주대학교 사이버보안학과 교수

Feasibility Study of Post Quantum Cryptography in TLS 1.3

Seong-Woo Lee[1] · Tae-Shik Son[2*]

[1]Master's Course, Department of Cyber Security, Ajou University, Suwon, Gyeonggi-do, Korea
[2*]Professor, Department of Cyber Security, Ajou University, Suwon, Gyeonggi-do, Korea

[요 약]

4차 산업혁명 기술의 발전으로 양자컴퓨팅 기술의 가능성이 증가함에따라 수학적 난제에 기반하고 있는 기존 공개키 암호 시스템에 대한 위험이 지속되고 있다. 이에 대응하여 NIST에서는 양자컴퓨팅 양자내성암호(PQC) 표준화 사업을 진행 중에 있다. 양자내성암호 기술을 분석하여 NIST에서 선정한 양자내성암호 알고리즘을 대표적인 무선통신 보안 프로토콜인 TLS 1.3에 적용하기 위한 이슈사항을 확인하고 직접 적용함으로써 각 후보 알고리즘들에 대해 성능평가를 수행한다. 따라서 본 논문에서는 평가의 결과를 토대로 NIST Security Level에서 가장 뛰어난 성능을 보인 알고리즘을 제안함과 동시에 TLS 1.3 프로토콜에 양자내성암호 적용의 가능성을 제안하고자 한다. 본 연구에서는 성능결과를 토대로 Crystals-Kyber와 Crystals-Dilithium 알고리즘을 선정하였다. 향후 계획으로 Ipsec, SSH, Kerberos과 같은 보안 프로토콜에 양자내성암호를 적용가능성을 연구함으로써 양자컴퓨팅환경에 안전한 무선통신 환경을 제공하고자 한다.

[Abstract]

As quantum computers become a reality, concerns about the security of existing public key cryptography relying on mathematical difficulties such as factorization and discrete logarithms are rising. For this reasons, NIST aims to announce international standardization algorithms for KEM and DS. In this paper, we analyze the applicability of the most widely used TLS protocol to apply post-quantum cryptography to various systems. We propose benchmarking results for performance comparison and handshake time for various post-quautum algorithms in Macbook equipped with Apple hip. As a result, It was found that the lattice-based cryptography was the best candidate in KEM and DS algorithms. In this study, Crystals-Kyber and Crystals-Dilithium algorithms were selected based on the performance results. In the future, we intend to provide a secure wireless communication environment by focusing on research on applying post-quantum encryption to various security protocols such as IPSec, SSH, and Kerberos.

색인어 : 양자내성암호, 공개키, 전송 계층 보안, 미국표준기술연구소, 프로토콜

Keyword : Post quantum cryptography, Public key, Tls, Nist, Protocol

http://dx.doi.org/10.9728/dcs.2023.24.1.167

Received 02 November 2022; **Revised** 28 November 2022
Accepted 07 December 2022

***Corresponding Author; Taeshik Shon**

Tel: +82-31-219-1898
E-mail: tsshon@ajou.ac.kr

Ⅰ. 서 론

4차 산업혁명의 발전으로, 다양한 IoT 기기들이 네트워크에 접속하여 상호통신을 통해 사용자에게 스마트한 서비스를 제공하고 있다. 대표적으로 스마트 팩토리, 스마트 그리드, 자율주행, 스마트 팜 등으로 사용자에게 편리한 삶을 제공하고 있다. 하지만, 이러한 스마트 서비스를 제공하는 IoT 기기 간의 통신은 무선으로 이루어져 해킹, 스푸핑과 같은 보안사고에 매우 취약하다. 따라서, 전송되는 데이터는 암호 알고리즘(블록암호, 해시함수 등)을 통해 보안 서비스를 제공 받아야 한다. 그 중 공개키 암호는 보안 서비스의 핵심인 인증과 키 교환을 지원하며, 대부분의 인증 솔루션 및 시스템은 공개키 암호 (RSA, 타원곡선)을 기반을 두고 있다. 공개키 암호 알고리즘은 우리 일상생활에서 Data 암호화를 통한 기밀성과 서명을 통한 인증의 역할을 제공하고 함으로써 실 생활에서 많이 사용되고 있는 중요한 역할을 수행하고있는 암호화 알고리즘이다. 최근 IBM이 공개한 첫 상용 양자컴퓨터의 내용을 보면 '수만년 걸리는 계산을 몇 시간만에 해내는 양자컴퓨터'라는 대목으로 큐비트 수를 127개로 늘린 양자 컴퓨터를 발표하여 현재 양자컴퓨의 성능은 계속해서 발전하고 있다. 실제로 google에서 발표한 자료에 의하면 53-큐비트 프로세서가 탑재 된 양자 컴퓨터 상에서 생성된 난수를 증명하는 것으로 현존하는 슈퍼컴퓨터 상에서는 1만년이 걸리는 문제이지만, 양자컴퓨터는 3분 20초만에 증명이 가능한 것으로 증명되었다.[1]

이러한 수학적 계산식에 기반을 두고 있는 공개키 암호 알고리즘이 양자컴퓨팅환경에 노출 되었을 때 암호화가 무력화가 될 문제를 계기로, 이 문제를 해결하기 위해 최근 미국의 NIST에서 양자컴퓨팅 환경에 대응할 수 있는 암호를 채택하기 위한 양자내성암호(PQC) 표준화 사업을 진행 중에 있다.TLS(Transport Layer Security)는 현재 인터넷에서 트래픽을 보호하는 역할을 하고 있다. 일상 생활에서 자주 사용하는 VPN(Virtual Private Network)에서 대부분 SSL 기반으로 터널링을 하고 있으며, 웹 상에서 HTTP 프로토콜에 SSL/TLS을 조합하여 서버로부터 전송되는 정보를 암호화 시켜 안전한 암호화 통신을 가능하게 하였다. 네트워크 환경에서 자주 사용되고 있는 TLS 프로토콜의 Handshake 과정에서 공개키가 사용되고 있고, Cipher Suite의 구조를 보면 프로토콜, 키교환 알고리즘, 인증서 검증 알고리즘, 대칭키를 이용한 블록 암호화 방식,블록 암호 운용방식, 메시지 인증으로 구성되어 있다. 빠른 연산이 가능한 양자컴퓨팅 환경속에 이러한 공개키 기반으로 동작하는 TLS 프로토콜은 더 이상 안전하지 않은 프로토콜이며 본 논문을 통해 TLS 1.3 프로토콜에 양자내성 암호의 적용가능성을 연구한다.

본 논문에서는 큐비트를 바탕으로 빠른 연산속도가 가능한 양자 컴퓨팅환경이 상용화 되기 전, 수학적 문제에 기반하고 있는 공개키 암호의 종류와 구조를 파악하고 양자내성암호의 기술을 분석한다.

표 1. 양자내성암호 기반 별 특징[2]
Table 1. Characteristics of each base of post-quatum cryptography

based classification	Algorithm	Advantages	Disadvantages
Lattice	NTRU, Saber, Crystals-Kyber	It is fast and has good compatibility on various platforms.	Parameter setting is tricky.
Code	Classic McEliece	Encryption speed is fast.	The key size is large.
Hash	SPINCS+	Security has been proved	The signature size is large.
Multvariable	Rainbow	It provides fast proce-ssing speed.	The key size is large.
Isogeny	SIKE	The key size is small.	The calculation speed is slow.

격자기반, 코드기반, 해시기반, 다변수기반 양자내성암호의 기술들과 특성을 분석하여 공개키 암호의 요구조건에 최적화된 기술이 무엇인지 연구한다. NIST PQC의 표준화 공모전 사업에서 각 양자내성암호의 유형 및 기술별 선정된 후보군에 대해 분석하고, NIST 관련 연구에 동향에 대해서 분석한다.

따라서 본 논문에서는 분석결과를 토대로 TLS 1.3 프로토콜에서 양자내성 암호 적용 가능성을 위해 Handshake과정, 인증서를 분석하여 TLS 1.3 프로토콜에서에서 PQC를 적용하기 위한 고려사항을 파악하고 실제로 적용함으로써 Performance를 측정 및 확인하고 양자내성 암호 적용 가능성 결과를 도출 및 최적 알고리즘을 제시하였다.

본 논문의 구성은 2장에서 공개키 암호 및 TLS 프로토콜과 양자내성암호 특징 및 NIST PQC에 선정된 알고리즘에 대해 살펴본다. 3장에서는 관련 연구 동향에 대해서 분석하고 4장에서는 TLS 프로토콜에 양자내성암호를 적용하기 위한 가능성에 대해 분석하였으며 5장에서는 직접 TLS에 적용하였다. 마지막으로 제 6장에서는 결론과 향후 연구 계획을 제시한다.

Ⅱ. 관련 연구

2-1 NIST PQC 표준화 및 관련 암호 기술 동향

대규모 전자 상거래, IoT, 클라우드 컴퓨팅 등 대부분의 무선통신 기술은 공개키 암호 기반 으로 이루어져 있다. 공개키 기반으로 동작하는 대표적인 프로토콜인 TLS는 디지털 객체간 암호화 된 통신을 제공함으로써 Data의 기밀성을 제공하고, SSL/TLS와 HTTP 프로토콜이 결합된 HTTPS 사용이 권장됨에 따라 공개키 알고리즘에 대한 수요는 계속해서 증가하고 있다. 기밀성 뿐 아니라 X.509 인증서를 통해 인증 서비스를 제공하고 있다. X.509 인증서는 두 객체 사이 제 3자

기관(CA:인증기관)에 의해 서명된 후 발급되며, 서명에 사용되는 서명 알고리즘은 공개키 암호 알고리즘인 RSA가 사용된다. 공개키 기반 암호기반의 구분은 소인수분해의 어려움과 이산대수의 어려움에 기반을 두고 있다.[3]

2-2 양자내성 암호

공개키 암호의 중요한 요소는 Key와 디지털 서명이다. 위에서 언급한 바와 같이, 양자컴퓨팅 환경의 발전은 RSA와 같은 소인수 분해의 어려움을 기반으로 하는 공개키 암호 시스템을 불안정하게 만들 수 있다. 이를 대응하기 위한 양자 컴퓨팅환경에서 내성을 가지는 암호의 기반은 <표 3>과 같이 5가지로 분류할 수 있다. 양자내성암호는 기존 공개키 암호 시스템의 문제를 보완할 수 있고, 수학적 어려움의 기반을 두는 것이 아닌 각 양자내성암호의 기반별 특징마다 안전성을 두고 있다.본 절에서는 양자내성암호 기술(격자기반, 코드기반, 해시 기반, 다변수 기반, 아이소제니 기반)들의 특징 및 알고리즘을 분석한다.

1) 격자기반 암호

격자 기반암호는 Shortest Vector Problem과 Closet Vector Problem과 같이 수학적 어려움을 기반으로 설계된 양자내성암호 기술이다. 즉 많은 차원의 격자 중 한 위치에서 가장 근접한 격자를 찾기 어려운 성질을 기반으로 한다. 1~10 차원의 수에선 격자 포인트를 찾기가 쉽지만, 200차원, 300차원이 되면 격자 포인트를 찾기 어렵다. 임의로 시작하는 지점으로 공개키 만들고, 그 임의로 시작하는 지점과 가까운 격자 포인트르로 개인키를 만드는데, 이것은 양자 컴퓨팅환경에서도 풀기 어렵다고 제시된 바 있다. 대표적인 알고리즘으로 LWE(Learning With Error)과 NTRU가 있다.

2) 코드기반 암호

코드 기반암호는 1978년, McEliece 암호 시스템에 의해 처음으로 제안 되었으며 아직까지 깨지지 않았으며, 이후 오휴 수정코드를 기반으로, 한 시스템들이 등장했다. 암호화 속도가 행렬을 이요하여 연산하므로 상당히 빠르다는 장점이 있으나 대부분의 코드기반 암호 시스템은 키 사이즈가 크다는 단점이 있다. 코드기반 암호는.대표적인 알고리즘으로 McEliece가 있으며, 코드기반 암호화의 문제점인 복호화가 느린 단점을 보완하기 위해 제시되었다. Goppa code를 통해 빠른 속도로 복호화를 할 수 있도록 하였지만 키 사이즈를 줄이진 못했다.

3) 해시기반 암호

해시 기반암호는 해시 함수를 사용하여 구성 된 디지털 전자 서명이다. 해시 함수에 기반을 두는 양자내성암호 시스템으로 해시 함수의 충돌 저항성에 안전성을 기반하고 있다.효율적으로 양자컴퓨팅 환경에 대응하기 위한 해시 기반암호는 서명자가 전에 서명된 메시지의 수를 확인하고, 기록해야 한다는 단점이 있는데, 이 기록이 노출되거나 잘못 기록되면 불안정을 초래한다. 또한 제한된 수의 서명을 생성할 수 있다는 점이다. 서명의 수를 늘리는 것은 가능하지만, 이는 서명의 사이즈가 커지는 단점을 가져온다. 대표적인 알고리즘으로 SPHINCS+ 가 있다.

4) 다변수기반 암호

다변수 기반암호는 유한필드의 다변수 다항식 시스템을 해결하기 어려운 문제를 기반을 두는 양자내성암호 시스템이다. 다변수 다항식을 이용한 계산이므로 Side Channel Attack에 안전하다는 장점이 있다. 하지만 5개의 양자내성 암호 시스템 중 키의 길이가 가장 길다는 단점이 있다. 이런 키 사이즈가 큰 단점으로 주로 서명 방식에 이용되며, 이러한 단점을 보완하기 위해 고안 된 알고리즘이 다변수 기반 암호의 대표 알고리즘인 Rainbow scheme이다. Rainbow scheme이란 키 사이즈를 줄이기 위해 다항식을 여러 단계로 나눔으로써 보안의 레벨은 유지하되, 키 사이즈를 줄인 알고리즘이다.

5) 아이소제니기반 암호

아이소제니 기반암호는 타원곡선 사이, 2개의 타원 곡선 안에서 아이소제니를 구하는 어려움을 기반으로 제안 된 양자내성암호 시스템이며 타원 곡선 아이소제니라고 한다. 제안 된 초기 당시 기존 일반 곡선을 가진 타원 아이소제니 보다 효율이 떨어지는 단점이 있어 주목을 받지 못했으나, SIDH 프로토콜이 제안됨에 따라 효율적인 계산이 가능하게 되었고 이에 따라 많은 연구와 구현이 진행되었다. 위에서 연구한 4개의 양자내성암호 기반보다 매우 작은 키 사이즈를 가진 암호이며, 대표적인 알고리즘으로는 SIKE가 있다.

2-3 NIST PQC 표준화 사업 및 진행 상황

양자컴퓨팅 환경의 발전으로 소인수 분해, 이산대수와 같은 수학적 어려움을 기반으로 두고 있는 기존의 공개키 알고리즘이 해독되는 것이 문재 됨에 따라 이에 대비하기 위한 미국 국립표준기술연구소(NIST, National Institute of Standards and Technology)는 공개 된 절차를 통해 1개 이상의 경쟁력 있는 공개키 알고리즘을 선정 하는 과정에 있으며 NIST PQC 표준화 사업이라고 한다. NIST는 PQC 표준화 사업을 통한 각 Round 과정을 통해 1개 이상의 KEM과, 디지털 서명을 지정하는 과정에 있다. NIST QPC 표준화 사업은 2017년 조건을 만족하는 69개의 후보자 알고리즘으로 Round 1이 진행 되었다. Round 1에서 선정 된 기반 별 알고리즘의 분포 수는 표 2.와 같다. Round 1은 2019년 1월까지 진행이 되었고, 이 과정을 통해 보안성과 성능 조건을 만족하는 26개의 알고리즘이 선정되었다. Round 1에 선정 된 후보 알고리즘은 각각 공개키 암호, 전자서명, KEM 중 하나를 만족하는 알고리즘이다.[5]

표 2. NIST PQC Round 1 알고리즘 분포[4]
Table 2. Selected NIST PQC Round 1 Algorithms

Based classification	KEM	Digital Signature	Sum
Lattice	5	23	28
Code	3	17	20
Hash	3	0	3
Multivariable	8	2	10
Isogeny	0	1	1
Etc	2	5	7
Sum	21	48	69

표 3. 최종라운드 진출 알고리즘. 대체알고리즘
Table 3. NIST Final Round Algorithms and Alternative Algorithms

Based classification	Selected Algorithm	Alternative Algorithm
KEM	Classic McEliece Crystals-Kyber Saber NTRU	BIKE HQC FrodoKEM SIKE NTRU Prime
DS	Crystals-Dllithium Falcon Rainbow	GeMSS Picnic SPINCS+

기존의 소인수 분해, 이산대수의 어려움을 기반을 두고 있는 수학적 기반의 알고리즘과 대비하여 NIST에서 선정한 알고리즘의 KEM(Key Encapsulation Mechanism)과 Digital Signatures은 다른 특징을 가진다.

RSA, ECC와 같은 기존 암호 알고리즘의 키교환 매커니즘은 송신자의 공개키를 이용하여 전달하고자 하는 메시지 를 암호화 하고, 수신자의 개인키를 사용하여 암호화 된 메시지를 복호화 한다. 이 방법은 양자컴퓨팅 환경에 취약한 방법이다. 이를 대응하기 위해 PQC 알고리즘의 키 교환 매커니즘은 대칭키를 사용하여 메시지를 암/복호화 한다. 송신자는 random한 난수를 생성한 후에 키 유도함수(KDF)를 사용하여 대칭키를 생성한다. 즉 패딩을 사용하지 않아 키 사이즈를 크게 줄였다. PQC 알고리즘의 디지털 서명 방식은 송신자의 개인키로 메시지에 서명하고, 수신자는 송신자의 공개키를 이용하여 서명된 메시지를 검증한다.

NIST에서는 Round 1을 통해 선정된 26개의 알고리즘으로 Round 2를 진행하였고, 최적화 된 구현과 성능을 분석하여 최종 라운드인 Round 3에 진출한 8개의 알고리즘과 추가적으로 표준화하기 위한 Alternatives Round 후보자를 선정하였다.선정된 알고리즘은 표 3.와 같다. 최종 Round에 선정된 키교환 매커니즘으로 Classic McEliece, Crystals Kyber, NTRU, Saber 4개의 알고리즘이 선정되었으며, 디지털 서명으로 Crystals Dillithium, Falcon, Rainbow 3개의 알고리즘이 선정되었다.

2-4 TLS 1.3

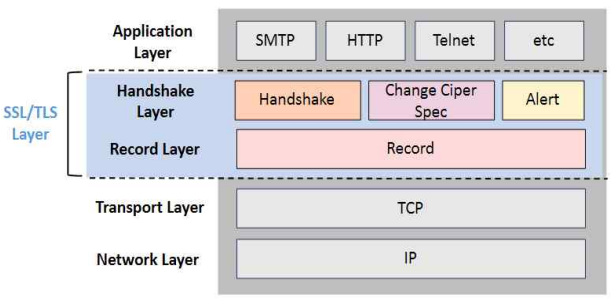

그림 1 TLS 프로토콜 구조
Fig. 1. TLS protocol structure

TLS 1.3의 구조를 보면 다음 그림 1과 같다.[6] Handshake, Change cipher Spec, Alert, Record 프로토콜로 구성 되어있다. Handshake 프로토콜은 서버와 클라이언트의 Data 교환이 이루어지기 전 협상단계에서 수행되는 프로토콜이며, 연결을 위해 cipher Suite (암호화 알고리즘, Key 교환 알고리즘, 압축방식 등)을 협상하는 프로토콜이다. Chage cipher Spec 프로토콜은 서버와 클라이언트 간 Handshake 프로토콜에서 정해진 cipher Suite가 반영 됨을 알리는 프로토콜이다.Alert 프로토콜은 경고 역할을 하며, 두 서버간 또는 서버 와 클라이언트의 SSL/TSL 통신하는 과정에서 Error가 발생하였을 시 알리는 프로토콜이다. Record 프로토콜은 Application 계층으로부터 전달받은 Data와 TLS의 상위 프로토콜에서 적용 된 값을 이용하여 암호화/복호화, Fragmentation, 압축 등의 처리과정을 통해 Header를 추가 한 후 전송하는 역할을 하는 프로토콜이다.

Record 프로토콜의 TLS Header를 붙이는 과정은 그림 2과 같다. Record Protocol Data는 2^14 이상의 Data를 전송하지 못하므로 Fragment 과정이 필요하다. 단편화가 완료되면 Data를 압축한 이후에 MAC을 계산한 후 추가하여 Data를 암호화 한다. 최종적으로 암호화 된 데이터에 콘텐츠 유형, Major 버전, Minor 버전, 압축된 길이가 포함 된 Record 헤더를 추가하여 최종적인 Data를 TCP 전송한다.위 과정을 통해 수신 된 Data는 decryption, 압축된 Data를 풀고, 재조립하는 과정을 통해서 위 계층 User에게 전달한다.

2-4 PQC 최적화 연구 동향

NIST PQC 2021에서는 ARMv8 Micro 프로세서를 대상으로 격자기반 암호 CRYSTALS-Kyber, NTRU, and Saber 대한 최적화 연구가 진행되었다.[7] ARM CPU는 Embedded 단말에 많이 사용되는 프로세서이며 현재 수십억 개의 단말이 Internet에 연결되어 있다. 이에 따라 이러한 Embedded 단말들 간 안전한 무선통신의 필요성이 중요한 요소이며 양자컴퓨팅환경의 발전 속에서 계산속도의 고속화 구현이 안되어 있는 경우, PQC 표준화에 채택은 늦어질 수 있다.

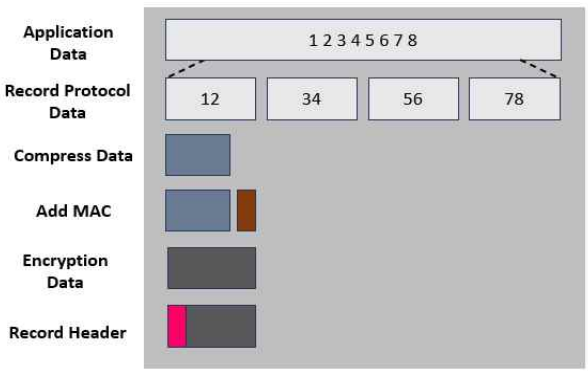

그림 2. Record 프로토콜 Data 처리과정
Fig. 2. Record protocol data processing process

표 4. 최종 후보자에 대한 pk, sk 길이
Table 4. Final Round Algorithm pk,sk Size

	Algorithms	based classification	PK Size	SK SIze
KEM	Classic McEliece348864	Code	261120	6452
	Crystals-Kyber512	Lattice	800	1632
	NTRU 4096821		1230	1590
	LightSaber		992	2304
Digital Signature	Crystals-Dilithium5	Lattice	1760	3856
	Falcon1024		1793	2305
	Rainbow I Classic	Multivariable	161600	103648

ARM의 가장 인기 있는 version은 ARMv8이다. 성능평가는 3.2GHz 주파수로 실행되는 4개의 ARMv8 코어를 포함한 Apple M1 환경의 맥북에어와 1.5GHz ARM72A 코어를 가진 4개의 라즈베리파이로 연구가 진행되었으며 이중 1개의 Core에서만 성능평가에 활용되었다. AVX2/neon 구현을 통해 단말 상에서 Encapsulation과 Decapsulation 속도의 향상을 달성했다.[11]

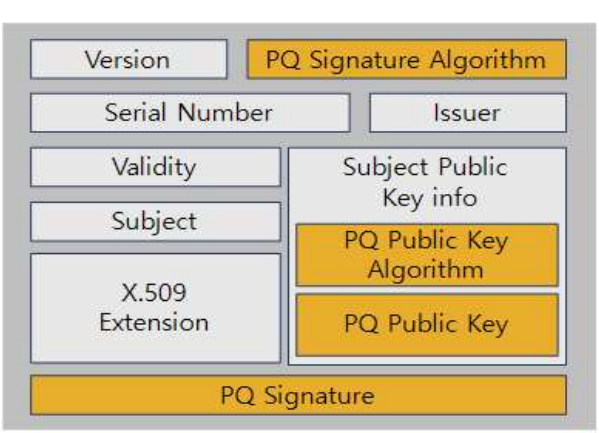

그림 3. PQC 기반 X.509
Fig. 3. PQC-based X.509

Pennsylvania 대학에서는 양자 근사 최적화 알고리즘(Quantum Approximate Optimization Algorithm)을 이용하여 양자내성암호 최적화를 위해 QAOA의 최적 p값을 찾는 연구를 진행했다. 4개의 각자 다른 QAOA Circuit을 두어 각 회로에 주어진 p값을 통해 최적의 선능을 제공하는 값을 찾아 성능결과를 제안하였다. 지금까지 대부분의 연구들은 각 단말에서 양자내성암호의 성능 및 Code의 사이즈를 최적하기 위한 연구가 수행되었다. 하지만 양자컴퓨팅환경에 대응하는 알고리즘의 실제 상용화를 위해서는 프로토콜 관점의 연구가 추가로 필요하다. 본 논문에서 양자내성암호를 적용할 프로토콜인 TLS 1.3에 적용하기 위하여 TLS 프로토콜의 구조(Handshake, Change cipher Spec, Alert, Record)를 파악하고, End-to-End 간 Handshake과정에서 사용되는 기존 X.509 인증서의 구조와 PQC X.509을 파악하여 실제 양자내성암호를 적용하기 위해 고려해야하는 사항을 분석해 실제 서버와 클라이언트간 교환되는 Data에 양자내성암호 알고리즘을 적용하여 성능결과 및 적용 가능성을 도출하는 것이 필요하다.

Ⅲ. TLS 1.3에서 양자내성암호 적용 항목

표 5. X.509 인증서 항목[8]
Table 5. X.509 Certificate category

Category	Necessity	Explanation
Version	essential	version of certificate
Serial Number	essential	serial number of certificate
Signature	essential	signature of Issuer
Issuer	essential	Name type structure of Issuer
Subject	essential	Name type structure of Subject
Subject Public Key Info	essential	Public key of Subject

본 분석에서는 TLS 프로토콜에 PQC를 적용하기 위한 2가지 이슈 사항과 양자내성암호 기반 별 특징에 대해서 분석한다. 먼저, 양자내성암호 기반 별 특징은 표 1.와 같다. 첫 번째는 TLS Record 프로토콜의 규격은 16KB이나, 현재까지 제안 된 대부분의 양자내성암호의 공개키, 서명의 크기는 크기가 큰 사항이다. NIST PQC Final Round에 진출한 양자내성암호 알고리즘의 공개키,개인키의 크기는 다음 표 4.와 같다. KEM(key encapsulation Mechanism)으로 코드기반의 Classic McEliece, 격자기반의 Crystals Kyber, NTRU, Saber 총 4개의 알고리즘과 Digital Signatures로 격자기반의 Crystals Dillithium, Falcon, 다변수 기반의 Rainbow 총 3개의 알고리즘은 기존의 공개키 암호 알고리즘인 RSA(RSA

3072 – pk :387bytes, sk:384bytes)와 ECDSA(ECDSA 384 – pk:48bytes, sk:48bytes)의 공캐키,개인키 크기를 비교 했을 때 상대적으로 큰 크기를 가지고 있는 것을 확인했다. 이러한 양자내성암호의 긴 키 길이 때문에, TLS에 적용하는데 문제가 발생할것으로 보였지만, 양자내성호의 인증서가 16KB를 초과하는 경우 TLS 프로토콜은 Record 프로토콜의 수를 늘려 Fragmentation을 수행한다. 이에 따라 처리속도의 저하의 가능성이 있지만 Cashing과 Compression을 통해 overhead를 개선한다.[9]

두 번째로 고려해야 할 사항은 양자내성암호에 대한 X.509 표준이 없는 사항이다. 기존 X.509 인증서의 필수항목은 표 5.와 같다. X.509 인증서는 Extension을 제외하고 총 7가지의 필수항목이 있으며 Version은 인증서의 version, SerialNumber는 인증서의 일련번호, Signature은 발급자의 서명, Issuer은 발급자의 정보, Vaidity는 인증서의 유효기간, Subject는 주체의 정보, SubjectPublicInfo는 주체의 공개키이다. 양자내성암호를 TLS에 적용하기 위해서는 기존 X.509 인증서의 형식과 PQC 항목을 추가해야 한다.

양자내성 암호 알고리즘이 X.509 인증서를 사용하기 위해선 그림 3과 같이 X.509 인증서 구조에 항목이 추가 되어야 한다. 추가 된 인증서의 구조를 보면 Subject Public Key Info항목에 암호화 통신에 사용한 양자내성 암호 공개키 알고리즘과 양자내성 암호의 공개키를 추가한다.[10] 그리고 추가 된 양자내성 암호 알고리즘을 통해 발급자가 서명하여 PQ signature가 발급된다. 기존의 Signature항목이 발급된 PQ signature항목으로의 변경이 필요하다.[12] 위에서 분석한 양자내성암호의 공개키 사이즈 크기에 대한 이슈사항과 양자내성암호 X.509 인증서 분석을 통해 본 연구의 TLS 1.3 프로토콜의 적용 가능성 분석의 항목으로 적용한다.

Ⅳ. 성능 측정

4-1 성능 측정 환경

표 6. 실험 환경
Table 6. experimental environment

OS	MAC OS M1
CPU	M1
Memory	8GB 3733MHz LPDDR4X

TLS 1.3 프로토콜에서 양자내성암호의 구현을 위해 다음과 같이 환경을 구축하였다. 구축한 실험 환경은 OS : Mac OS, CPU : M1, Mermory : 8GB 3733MHz, LPDDR4X 환경에서 OQS Openssl 라이브러리를 직접 빌드하였다. 위 환경에서 실험을 진행하며 알고리즘에 대한 성능을 먼저 분석하고,[13] 각 알고리즘별 성능 분석한 결과를 바탕으로 TLS Handshkae에 대한 지연시간을 분석한다. 따라서, 본 장에서는 제 1절에서 알고리즘에 대한 성능을 비교한다. 그 다음 제 2절에서 TLS 1.3에 PQC를 적용하여 key encapsulation Mehcanism, Digtal Signature의 Handshake 지연시간을 측정하여 성능을 비교한다.

4-2 실험 시나리오

실험 시나리오는 다음과 같다. 먼저 각 NIST Security Level에 해당하는 KEM,Digital Signature 알고리즘을 분류하여 Handshake과정에서 암/복호화, 키생성 속도를 비교하고, Digital Signature과정에서 서명속도와 검증속도를 비교하여 각 Security Level에서의 최적화 된 알고리즘을 선정한다.

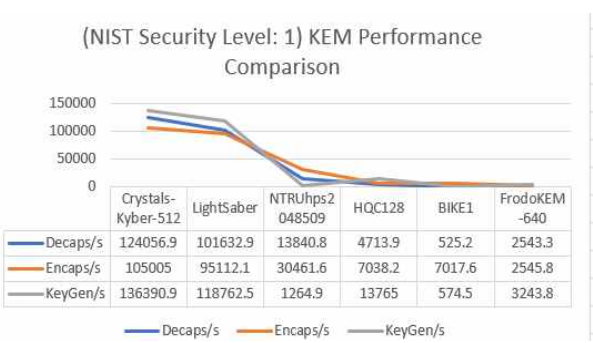

그림 4. NIST Security Level:1 KEM 성능 비교
Fig. 4. NIST Security Level:1 KEM Performance Comparison

4-3 실험 1 알고리즘 성능 (KEM, DS)

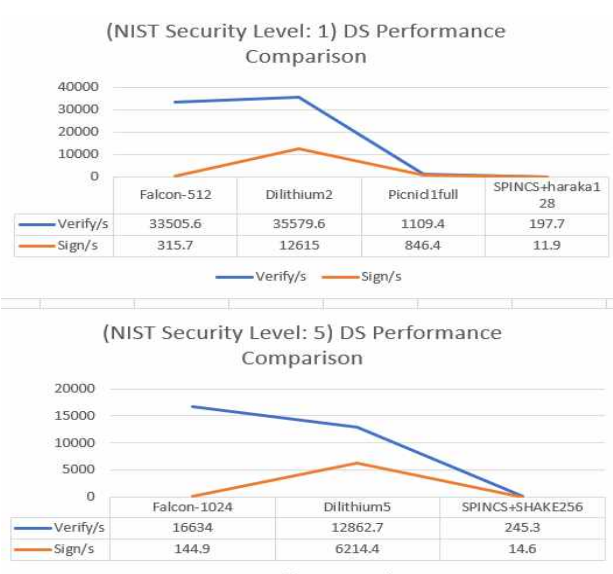

그림 5. NIST Security Level:1,5 DS 성능 비교
Fig. 5. NIST Security Level:1,5 DS Performance Comparison

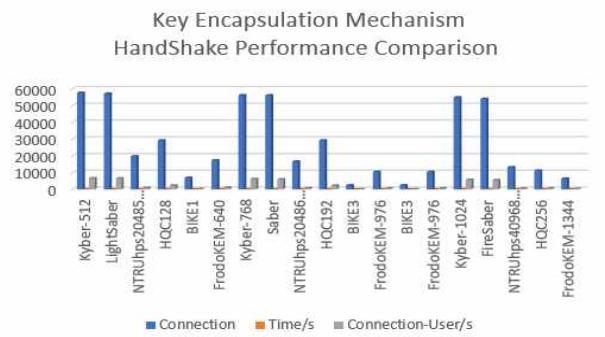

그림 6. KEM Handshake 성능비교
Fig. 6. Performance comparison for KEM Handshake

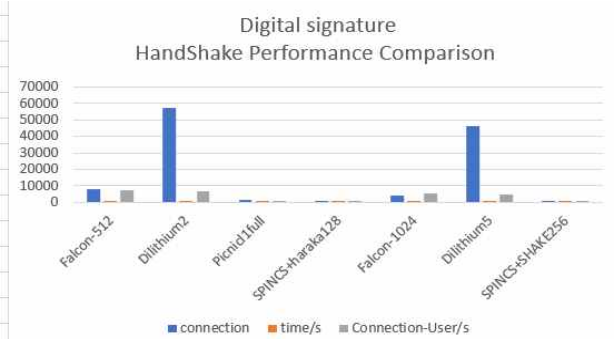

그림 7. DS Handshake 성능비교
Fig. 7. Performance comparison for DS Handshake

먼저 TLS 1.3 프로토콜에 알고리즘 별 key encapsulation Mehcanism의 Encapsulation, Decapsulation, Keygen의 속도를 측정한다. NIST Security Level 1 에 해당하는 알고리즘 별 성능분포는 그림 4과 같다. Encapsulation 항목은 Crystals-Kyber-512가 초당 105,005번으로 가장 빠른 속도를 보였다. Decapsulation 항목은 Crystals-Kyber-512가 초당 124,057번으로 가장 빠른 속도를 보였다. Keygen항목 또한 Crystals-Kyber-512가 초당136,391번으로 가장 빠른 속도를 보였다. TLS 1.3 end-to-end testing 연구에서 KEM 알고리즘 중 Crystals-kyber가 Saber보다 Encapsulation, Decapsulation 항목에서 약 110%높은 성능을 보였으며, Keygen 항목에서 약 120% 높은 성능을 보임으로써 가장 좋은 성능을 나타냈다.

다음 그림 5은 NIST Security Level 1에 해당하는 DS 알고리즘 별 성능분포표이다. Verify 항목은 Dilithium2가 초당 35,579.2번으로 가장 빠른 속도를 보였다. Signature 항목은 Dilithium2가 초당 12,615번으로 가장 빠른 속도를 보였다. 다음 그림 6은 NIST Security Level 5에 해당하는 DS 알고리즘 별 성능분포표이다. Verify 항목은 Falcon-1024가 초당 16,634번으로 가장 빠른 속도를 보였다. Signature 항목은 Dilithium5가 초당 6214.4번으로 가장 빠른 속도를 보였다.

TLS 1.3 end-to-end testing 연구에서 DS 알고리즘 중 Falcon가 Dilithium보다 Verify 항목에서 약 120%높은 성능을 보였으며, 반대로 Signature 항목에서 Dilithium가 Falcon보다 약 430% 높은 성능을 보임으로써 Dilithium과 Falcon은 Trade-off 관계임을 확인했다.

4-4 실험 2 TLS HandShake 성능 (KEM, DS)

위에서 분석한 각 Security Level 에서의 key encapsulation Mechanism 알고리즘의 성능결과를 나타낸 것으로, Key EncyptionTLS 1.3 프로토콜에서 Handshake 과정에서의 성능분포표는 그림 6과 같다.

측정항목은 TLS Connection의 수, Handshake 소요시간, 초당 맺어진 Connection의 수를 측정했다. KEM의 정확한 측정을 위해 전사서명방식은 Dilithium2 알고리즘으로 고정하고 각 KEM 알고리즘의 성능을 측정하였다.격자기반 암호인 Crystals-Kyber 와 Saber 알고리즘이 각 Security Level에서 타 알고리즘에 비해 연결되는 Connection의 수가 많았으며,같은 시간을 비교해 보았을 때 초당 맺어지는 Connection의 수가 많아 좋은 성능을 나타내는 것을 확인할 수 있었다. 그 중 Crystals-Kyber 알고리즘이 Saber 알고리즘보다 10% 나은 성능을 보였으며 Handshake 성능비교에서 분석 된KEM 알고리즘 중 가장 좋은 성능을 나타냈다.

다음 그림 7은 각 Security Level에서의 Digital Signature알고리즘의 성능결과를 나타낸 것으로, Key EncyptionTLS 1.3 프로토콜에서 Handshake 과정에서의 성능분포표이다. 위 실험과같이 측정항목은 TLS Connection의 수, Handshake 소요시간, 초당 맺어진 Connection의 수를 측정했다. Digital Signature 알고리즘의 정확한 측정을 위해 KEM 알고리즘은 Crystals-Kyber 512로 고정하여 측정하였다. 위 KEM Handshake 성능분석과 마찬가지로 격자기반 암호인 Dilithium 알고리즘이 각 Security Level에서 타 알고리즘에 비해 연결되는 Connection의 수가 많았으며,같은 시간을 비교해 보았을 때 초당 맺어지는 Connection의 수가 많아 좋은 성능을 나타내는 것을 확인할 수 있었다. 추가로 Web환경에서는 Falcon 알고리즘의 성능도 좋은 성능결과 지표를 나타냈다. 본 연구를 통해 Kyber와 Dilithitum알고리즘이 각 KEM/DS에서 좋은 성능을 가진 알고리즘으로 확인할 수 있었다. NIST에서 진행하는 PQC 표준화 사업의 표준 발표 당시 Crystals 알고리즘을 주요 알고리즘으로 중용한 점을 고려하면 위 성능 결과를 통해 key encapsulation Mechanism의 Crystals-Kyber 알고리즘과, Digital Signature의 Crystals-Dilithium알고리즘이 기존에 사용이던 공개키 기반의 RSA,ECDDH와 같은 수학적 문제에 기반을 두고 있는 알고리즘을 대체하여 양자컴퓨팅환경에서 안전한 알고리즘 구현의 가능성을 확인할 수 있었다.

Ⅴ. 적용 가능성 분석

OQS-OpenSSL 라이브러리를 서버에 적용하고, liboqs를 빌드하여 성능을 분석하였다. 성능 분석결과 Key Exchage Algorithms으로 BIKE, CRYSTALS-Kyber, FrodoKEM, HQC, NTRU, NTRU-Prime, SABER 알고리즘이 TLS 1.3 프로토콜에서 적용가능을 확인할 수 있었고, Digital Signature Algorithms으로 CRYSTALS-Dilithium, Falcon , Picnic, Rainbow, SPHINCS-Haraka, SPHINCS-SHAK E256 알고리즘이 TLS 1.3 프로토콜에서 적용가능을 확인할 수 있었다. CRYSTALS-Kyber, SABER, CRYSTALS-Dilithium과 같은 알고리즘은 RSA.ECC보다 더 나은 성능을 보여 양자컴퓨팅환경에서 수학적 문제에 기반을 두고 있는공개키 암호 알고리즘을 대체할 수 있음을 확인했다.

Ⅵ. 결론

무선통신환경에서 송,수신자 간 교환하는 데이터의 기밀성과 무결성에 대한 수요는 점차 증가하고 있다. 하지만 양자컴퓨팅환경의 발전으로 0,1 비트를 동시에 계산할 수 있는 큐비트의 개념이 등장함에 따라 인터넷상에서 기존의 수학식 문제의 어려움을 기반으로 두고 있는 공개키 암호 알고리즘 시스템이 빠르게 계산되어 위협에 노출 될 가능성이 있는 상황이다.

본 논문에서는 양자컴퓨팅환경에 대응하기 위해 최근 NIST에서 발표한 PQC 표준화 사업의 동향에 맞추어 각 양자내성암호 기술(격자기반, 코드기반, 해시 기반, 다변수 기반, 아이소제니 기반)을 파악하고 NIST에서 각 Round를 거쳐 선정 된 Key Encapsulation Mechanism, Digital Signature 알고리즘을 TLS 1.3 프로토콜에 적용하기 위한 이슈사항을 확인하고 OQS Library를 통해 직접 TLS End-to-End Testing을 함으로써 TLS 1.3에서 양자내성암호 적용 가능성과 동시에 성능결과를 제시하였다. NIST Security 1~5 Level 중 각 단계 조건에 해당하는 Key Encapsulation Mechanism알고리즘과 Digital Signature 알고리즘을 각각 En/Decapsulation, 서명/검증 성능값을 비교 분석함으로써 각 알고리즘 중 더 나은 성능을 보이는 알고리즘의 결과를 도출하였다. 결과를 통해 TLS Handshake단계에서 좋은 성능을 가진 양자내성암호 알고리즘은 Crystals-Kyber와 Crystals-Dilithium 알고리즘으로 선정하였다.

따라서 본 연구를 통해 고속의 계산처리가 가능한 양자 컴퓨팅 환경에 대응하는 알고리즘을 제안함으로써 기존 공개키 암호 알고리즘을 대체할 수 있으며 안전한 통신의 환경을 구성하고자 한다. 향후 계획으로는 TLS 프로토콜 뿐아니라 Ipsec등 다양한 보안 프로토콜에서 양자내성암호 적용가능성을 연구하는것이 다음 연구의 목표이다.

참고문헌

[1] Peter Schwabe, Douglas Stebila, Thom Wiggers, “Post-Quantum TLS Without Handshake Signatures,” *Conference on Computer and Communications Security*, p.1461-1480, Oct 2020, https://doi.org/10.1145/3372297.3423350

[2] Peter W. Shor, Polynomial-Time Algorithms for Prime “Factorization and Discrete Logarithms on a Quantum Computer,” *SIAM Review*, Vol. 41, p.303-332, Jan 1999. https://doi.org/10.1137/s0036144598347011

[3] Jeffrey HoffsteinJill PipherJoseph H. Silverman, “NTRU: A ring-based public key cryptosystem,” *3rd ANTS 1998: Portland, Oregon, USA*, p.267-288, JAN 2006. https://doi.org/10.1007/bfb0054868

[4] Kyoung-Bae Jang, Hwa-Jeong Seo, “Quantum Computer and Standardization trend of NIST Post-Quantum Cryptography,” *Applied IT Engineering*, p.129-132, May 2019. https://doi.org/10.3745/PKIPS.y2019m05a.129

[5] L Chen, S Jordan, “Report on post-quantum cryptography,” *NIST*, p.3-5. Apr 2016. http://dx.doi.org/10.6028/NIST.IR.8105

[6] Lawrence C. Paulson, “Inductive Analysis of the Internet Protocol TLS,” *ACM Trans. Inf. Syst. Secur*, p332-351, Aug 1999. https://doi.org/10.1145/322510.322530

[7] Kanad Basu, Deepraj Soni, Mohammed Nabeel, Ramesh Karri, “NIST Post-Quantum CryptographyA Hardware Evaluation Study,” *IACR Cryptol*, p1-16, JAN 2019. https://eprint.iacr.org/2019/047

[8] Panos Kampanakis, Peter Panburana, Ellie Daw, Daniel Van Geest, “The Viability of Post-Quantum X.509 Certificates,” *IACR Cryptol*, p1-18, Jan 2018. https://eprint.iacr.org/2018/063

[9] Dimitrios Sikeridis, Panos Kampanakis, Michael Devetsikiotis, “Post-Quantum Authentication in TLS 1.3: A Performance Study,” *IACR Cryptol*, p1-14, Feb 2020. https://doi.org/10.14722/ndss.2020.24203

[10] J.W. Bos, C. Costello, M. Naehrig, and D. Stebila, “Post-quantumkey exchange for the TLS protocol from the ring learning with errorsproblem,” *IEEE Symposium on Security and Privacy*. p553–570, May 2015. https://doi.org/10.1109/sp.2015.40

[11] Duc Tri Nguyen, Kris Gaj, “Optimized Software Implementations of CRYSTALS-Kyber, NTRU, and Saber Using NEON-Based Special Instructions of ARMv8,” *Fairfax*, p1-24, Jun 2021. https://csrc.nist.gov/CSRC/media/Events/third-pqc-standa

rdization-conference/documents/accepted-papers/nguyen-optimized-software-gmu-pqc2021.pdf
[12] Herome Lablanche, Lina Mortajine, Othman Benchaaalal, Pieree-Louis, “Optimized implementation of the NIST PQC submission ROLLO on microcontroller”, *IACR Cryptol*, p1-18, Jul 2019. https://eprint.iacr.org/2019/787
[13] Mahabubul Alam, Abdullah Ash-Saki, Swaroop Ghosh, “Analysis of Quantum Approximate Optimization Algorithm under Realistic Noise in Superconducting Qubits,” *Department of Electrical Engineering*, p1-7. Jul 2019. https://doi.org/10.48550/arXiv.1907.09631

이성우(HyunJin Kim)

2019년 : 성결대학교 정보통신공학과 졸업(학사)
2021년~현 재: 아주대학교 정보통신공학과 석사과정

2020년~2022년: 씨앤아이테크
2021년~현 재: 아주대학교 정보통신공학과 석사과정
※관심분야 : 무선통신, 양자내성암호, 프로토콜 등

손태식(Taeshik shon)

2000년 : 아주대학교 정보및컴퓨터공학부 졸업(학사)
2002년 : 아주대학교 정보통신전문대학원 졸업(석사)
2005년 : 고려대학교 정보보호대학원 졸업(박사)

2004년~2005년 : University of Minnesota 방문연구원
2005년~2011년 : 삼성전자 통신·DMC 연구소 책임연구원
2017년~2018년 : Illinois Insitute of Technology 방문교수
2011년~현 재 : 아주대학교 정보통신대학 사이버보안학과 교수
※관심분야 : ICS/SCADA, DFIR, Anomaly Detection