NIST 양자내성암호 표준화 현황

송보연

한국과학기술정보연구원

bysong@kisti.re.kr

The Current State of NIST PQC Standardization

Boyeon Song

Korea Institute of Science and Technology Information (KISTI)

요 약

본 논문은 국외 양자내성암호(Post-Quantum Cryptography, PQC) 표준화의 주축을 이루고 있는 미국 국립표준기술연구소(NIST, National Institute of Standards and Technology)의 PQC 표준화 과정 및 현황을 조사함으로써, PQC에 관한 연구 동향을 파악하고 이를 바탕으로 향후 연구 방향을 모색하고자 한다.

Ⅰ. 서 론

양자 컴퓨터(Quantum Computer)에 대한 연구가 활발하게 진행됨에 따라 양자 컴퓨팅 환경에서도 안전한 암호 통신을 하기 위한 차세대 암호 기술에 대한 연구가 주목을 받고 있다. 그 일환으로 양자내성암호(Post-Quantum Cryptography, PQC)에 대한 연구도 국내외에서 다양한 각도로 진행되고 있다.

PQC란 양자 컴퓨터의 암호학적 공격에 안전한 암호 알고리즘(일반적으로 공개키 알고리즘)을 의미한다.[1] 구체적으로, 현재 컴퓨터에서 안전하다고 판단되어 표준화되고 상용화 중인 공개키 암호 알고리즘들은 인수분해 문제 또는 이산대수 문제를 기반으로 하고 있다. 그러나, 초고속 연산이 가능한 대규모 양자 컴퓨팅에서는 양자의 성질을 이용하여 인수분해 문제와 이산대수 문제를 다항식 시간 내에 풀 수 있다는 것이 증명되었다.[2,3] 따라서, 양자 컴퓨터 환경에서도 안전한 내성을 가진 공개키 암호에 대한 연구가 필요하며, 이들은 양자 컴퓨터에서도 풀기 어려운 새로운 차원의 수학적 난제를 기반으로 한 알고리즘이어야 할 것이다.

본 논문에서는 PQC의 연구 현황을 파악하기 위한 근간으로 PQC 분야에서 표준화를 선도하고 있는 미국의 국립표준기술연구소(NIST, National Institute of Standards and Technology)의 표준화 현황을 조사하고 그에 따른 PQC 관련 향후 연구 방향을 모색하고자 한다.

Ⅱ. PQC의 NIST 표준화

본 장에서는 PQC 표준화를 시작하게 된 NIST의 동기를 살펴보고, PQC 표준화 진행과정 및 현황을 기술하고자 한다.

2.1 PQC 표준화 필요성 및 동기

대규모의 양자 컴퓨터가 만들어진다면 현재 사용 중인 많은 공개키 암호 시스템이 깨질 수 있게 된다.[2,3,4] 이는 인터넷 상의 디지털 암호 통신의 기밀성(Confidentiality)과 무결성(Integrity)이 심각하게 위협받게 됨을 의미한다.[4] 따라서, PQC의 목적은 양자 컴퓨터와 클래식 컴퓨터에서 모두 안전한 암호 시스템이어야 할 것이고, 존재하는 통신 프로토콜과 네트워크에서 상호작용할 수 있는 것이어야 할 것이다.[4]

양자컴퓨터 시대가 언제 도래할지 정확한 시간은 예측하기 어렵지만, NIST는 양자 컴퓨팅에 저항할 수 있는 정보보호 시스템을 준비하는 것이 필요하다고 생각했다.[4] 이에, PQC 알고리즘을 공개적으로 모집하고 이를 검증하는 과정을 가져 표준화하는 프로젝트를 2016년에 시작하였다.[4,5]

2.2 NIST PQC 표준화 과정

NIST는 양자 컴퓨터 시대의 도래를 포함하여 가까운 미래에 정부의 민감한 정보를 보호할 수 있는 새로운 공개키 암호(Public-Key Encryption, PKE) 및 키 생성 방법(Key-Establishment Mechanism, KEM) 알고리즘과 디지털 서명(Digital Signature)을 표준화하기 위한 작업을 2016년에 시작했다.[4,5] 이 과정을 PQC 표준화라 부르며, PQC 알고리즘을 모집하고 검증하는 과정을 거쳐 표준화하는 프로젝트이다. 선정된 새로운 PQC 표준화 결과는 FIPS(Federal Information Processing Standards) 또는 SP(Special Publications)로 문서화될 예정이다.[4]

PQC 표준화 과정의 첫 번째 단계로 후보 알고리즘을 공모하기 위한 최소한의 채택 요구사항, 제출 요구사항, 평가 기준 등을 2016년 8월 2일에 공개하고 외부 논평(comments)을 받아 수정한 버전을 발표했다. 그리고 2016년 12월 20일에 PQC 표준화를 위한 알고리즘 공모를 시작했으며, 공모 마감일인 2017년 11월 30일 전에 총 82개의 알고리즘들이 제안되었다.[4,5]

1라운드(2017년 12월~2019년 1월)에서 응모한 알고리즘들 중 69개의 알고리즘들이 채택되었고, 이 중 거의 25개 정도의 알고리즘들은 공격이 가능하다고 판명되었다.[4,5] 2019년 1월 30일에 26개의 알고리즘들이 선정되어 2라운드에 진출했다. 즉, 2라운드에 진출한 알고리즘들은 PKE & KEM 알고리즘들이 17개이고 디지털 서명 알고리즘들이 9개이다.[4,5]

2라운드(2019년 1월~2020년 7월)에 진입한 26개의 알고리즘들 중 8개의

알고리즘들이 공격에 취약하다고 발견되었고, 2020년 7월 22일에 7개의 최종 후보 알고리즘들(Finalists)과 8개의 대안이 되는 알고리즘들(Alternate Candidates)이 선정되었다.[4] 전자는 NIST 기준 3라운드에서 표준화 준비가 될 것으로 예상되는 유력한 후보들에 해당하며, 4개의 PKE & KEM 알고리즘들(Kyber, NTRU, SABER, Classic McEliece)과 3개의 디지털 서명 알고리즘들(Dilithium, Falcon, Rainbow)이 이에 해당된다.[4,5] 후자는 잠재적인 후보들을 말하며 다음 라운드에서 재고할 필요가 있는 알고리즘들로서, 5개의 PKE & KEM 알고리즘들과 3개의 디지털 서명 알고리즘들이 이에 해당된다.[4,5]

3라운드에서 평가 기준(evaluation criteria)인 안전성, 성능, 알고리즘과 실행 특성 등의 적합성을 고려하여 2022년 7월 5일에 최종적으로 표준화를 진행할 4개의 알고리즘들을 선정하고, 또한 4개의 후보군 알고리즘들을 발표했다[4]. 최종 선정된 PQC 알고리즘들은 <표1>에서 보이는 바와 같이 PKE & KEM 방식에서는 격자(lattice) 기반 암호 알고리즘인 CRYSTALS-KYBER가 유일하게 채택되었고, 디지털 서명 방식으로는 격자 기반 암호 알고리즘인 CRYSTALS-Dilithium과 FALCON, 그리고 해쉬 기반 암호 알고리즘인 SPHINCS+이 채택되었다.[4] NIST는 이 중에서 PKE & KEM 방식인 CRYSTALS-KYBER와 디지털 서명 방식인 CRYSTALS-Dilithium을 주요 알고리즘으로 사용하길 권고한다. 이들이 가장 강력한 안전성을 제공하고 효율적인 실행이 가능한 알고리즘이라 보고 있으며, 대부분의 응용 환경에서 잘 적용될 것으로 기대하고 있다. FALCON의 경우는 CRYSTALS-Dilithium이 사이즈가 너무 커서 적용이 어려운 상황에 대체할 알고리즘으로 적합하다고 언급하고 있으며, SPHINCS+는 격자 기반의 안정성에 의존하는 것을 피하기 위해 표준화 알고리즘으로 선정하였다고 한다.[4] 이들은 24년까지 표준화 문서로 출판하는 것을 목표로 일정을 추진하고 있다.

<표 1> 3라운드에서 표준화 진행으로 선정된 PQC 알고리즘

기반 문제	PKE & KEMs	Digital Signatures
Multivariate		
Code-based		
Lattice-based	CRYSTALS-KYBER	CRYSTALS-Dilithium FALCON
Isogeny		
Hash-based		SPHINCS+

또한, 4개의 후보 알고리즘들은 현재 4라운드에 진입해서 추가적인 검증을 진행하는 중이다. 이는 <표2>에서 보이는 바와 같이 모두 PKE & KEM 방식에 해당하는 것으로서 코드(Code) 기반 암호 알고리즘인 BIKE, Classic McEliece, HQC가 있고 아이소제니(Isogeny) 기반 암호 알고리즘인 SIKE가 있다. 이 중 SIKE는 공격법이 발견되어서 안전하지 않다고 공지했다.[4]

디지털 서명 방식으로서 4라운드 진출하는 알고리즘은 한 개의 후보도 없는 상태이다.

<표 2> 4라운드에 진출하는 PQC 후보 알고리즘

기반 문제	PKE & KEMs	Digital Signatures
Multivariate		None
Code-based	BIKE Classic McEliece HQC	
Lattice-based		
Isogeny	SIKE (Not secure)	
Hash-based		

2.3 NIST PQC 표준화 현황

2022년 9월에 NIST는 PQC 표준화 과정으로 추가적인 디지털 서명 알고리즘 공모를 새롭게 시작했다. 이유는 현재 표준화 진행 중인 3개의 알고리즘 외에 4라운드에서 고려 대상에 있는 후보 알고리즘이 전혀 없기 때문이다.

2023년 6월 1일이 제출 마감일이었고, 2023년 7월 17일에 NIST는 제출 요건에 모두 부합하는 40개의 추가적인 디지털 서명 후보군(Round 1 Additional Signatures)을 발표했다. <표3>에서 보이는 바와 같이 해당하는 알고리즘들의 기반 문제는 코드 기반, 아이소제니 기반, 격자 기반, MPC(Multi Party Computation)-in-the-Head, 다변수 기반, 대칭(Symmetric) 기반 문제 등으로 다양하다.

<표 3> 1라운드에 진출하는 추가적인 PQC 서명 알고리즘

기반 문제	# of Digital Signatures
Code-based	6
Isogeny	1
Lattice-based	7
MPC-in-the-Head	7
Multivariate	10
Symmetric-based	4
Other signatures	5

NIST는 2023년 8월 24일에 3개의 Draft FIPS 203, 204, 205를 발표하고 이에 대한 공개적인 논평을 2023년 11월 22일까지 요청했다. 이는 PQC 표준화 3라운드에서 최종으로 선정된 4개 알고리즘들 중 3개에 해당하는 CRYSTALS-KYBER, CRYSTALS-Dilithium, SPHINCS+를 표준 PQC 알고리즘으로 상세하게 기술한 표준 문서들의 초안이다.

- Draft FIPS 203: Module-Lattice-Based Key-Encapsulation Mechanism Standard
- Draft FIPS 204: Module-Lattice-Based Digital Signature Standard
- Draft FIPS 205: Stateless Hash-Based Digital Signature Standard

NIST는 24년에 3라운드에서 최종 선정된 4개의 암호 알고리즘에 대한 표준화 문서 작업을 모두 마무리할 계획이다.[4]

이와 같이 NIST는 양자컴퓨터가 현재 표준화 암호로 사용 중인 RSA 등을 무력화시키는 시기를 대비하기 위해 PQC 체계를 단계별로 준비하고 있다.[6]

Ⅲ. 결론

PQC 표준화의 주축을 이루고 있는 NIST의 PQC 표준화 과정을 조사하면서 이에 따른 PQC 알고리즘 연구의 동향을 엿볼 수 있었다. 현재 PQC 알고리즘의 기반이 되는 문제들은 양자 컴퓨팅으로도 해결하기 어렵다고 여겨지는 다변수(Multivariate), 코드(Code), 격자(Lattice), 아이소제니(Isogeny), 해쉬(Hash) 기반 등 여러 난제들을 들 수 있다.

표준화 진행 중인 4개의 알고리즘 중 3개는 격자 기반 문제에 근간을 두고 있고, 현재 4라운드에 진출한 알고리즘 3개는 모두 코드 기반 문제를 바탕으로 하고 있다. 새롭게 모집되어서 1라운드에서 검증 중인 추가적인 디지털 서명 후보군은 다양한 난제를 기반으로 알고리즘들이 제안되었는데 격자 기반, 해쉬 기반, 또는 코드 기반 알고리즘 외에 새로운 기반 문제를 근간으로 하는 표준화 알고리즘들이 나올지 향후 귀추가 주목된다.

양자 컴퓨터에서도 쉽게 풀 수 없는 다각적인 난제를 기반으로 하는

PQC 알고리즘에 대한 연구가 확대 및 지속될 것으로 유추할 수 있다. 특히, 최근 MPC-in-the-Head 패러다임을 기반으로 하는 알고리즘에 대한 연구가 가속화되고 있다. 향후 해당 난제를 기반으로 하는 PQC 알고리즘에 대한 연구를 계속 수행해보고자 한다.

ACKNOWLEDGMENT

이 논문은 2024년도 한국과학기술정보연구원(KISTI)의 기본사업으로 수행된 연구입니다.(과제번호: No. K-24-L04)

참 고 문 헌

[1] Wikipedia, 'Post-quantum cryptography', available at https://en.wikipedia.org/wiki/Post-quantum_cryptography

[2] P. W. Shor, "Algorithms for quantum computation: discrete logarithms and factoring," Proceedings 35th Annual Symposium on Foundations of Computer Science, Santa Fe, NM, USA, 1994, pp. 124-134.

[3] Grover, Lov K. "A fast quantum mechanical algorithm for database search." Proceedings of the twenty-eighth annual ACM symposium on Theory of computing. 1996.

[4] NIST, 'Post-Quantum Cryptography Standardization', available at https://csrc.nist.gov/Projects/post-quantum-cryptography/post-quantum-cryptography-standardization

[5] D. Moody, 'The Beginning of the End: The First NIST PQC Standards', Presented at. PKC 2022, March 8, 2022.

[6] 송민호, 이민우, 서화정, "NIST PQC 표준화 동향", ASK 2023 학술발표대회 논문집, 30권 1호, 2023.