NIST PQC 표준화 동향

송민호[1], 이민우[1], 서화정[2]
[1]한성대학교 융합보안학과 석사과정
[2]한성대학교 융합보안학과 교수
smino0906@gmail.com, minunejip@gmail.com, hwajeong84@gmail.com

NIST PQC standardization trends

Min-Ho Song[1], Min-Woo Lee[1], Hwa-Jeong Seo[2]
[1,2]Dept. of Convergence Security, Hansung University

요 약

양자 컴퓨팅의 발전과 양자 알고리즘의 등장으로 기존의 암호 체계는 위협을 받고 있다. 이에 기존의 암호를 대신해 양자 공격에 대응할 수 있는 양자 내성 암호의 중요성이 높아지고 있다. 본 논문에서는 양자 내성 암호 표준화를 위해 진행된 NIST PQC 공모전과 공모전에서 최종 선정된 암호에 대한 표준화 목표에 대해 알아보도록 한다.

1. 서론

양자 컴퓨팅의 발전과 Shor, Grover 알고리즘과 같은 양자 알고리즘의 등장으로 수학적 문제를 기반으로 하는 기존의 암호 체계는 큰 위협을 받고 있다. 이에 양자 공격에 대응할 수 있는 양자 내성 암호에 대한 관심과 중요성이 높아지고 있다. 다양한 양자 내성 암호 알고리즘에 대한 개발이 이루어졌고 많은 진전을 보여주었으나 보안성, 효율성 등에 미치지 못하는 알고리즘들도 다수 존재한다. 그래서 적절한 양자 내성 암호를 선정해야하며 또 이에 대한 표준화가 필요하다. 따라서 본 논문에서는 적절한 알고리즘 선정을 위한 공모전, 선정된 알고리즘에 중점을 두고 양자 내성 암호 표준화 동향에 대해 조사한다.

본 논문의 2장에서는 양자 내성 암호에 대해 알아본다. 3장에서는 NIST PQC 공모전에 대해 알아보고, 4장에서는 공모전에서 최종 선정된 암호에 대한 표준화 목표에 대해 알아보도록 한다. 마지막으로 5장에서는 본 논문의 결론을 내린다.

2. 양자 내성 암호

양자 내성 암호란 양자 공격에 대응할 수 있는 암호화 알고리즘을 의미한다. 양자 컴퓨터는 고전 컴퓨터보다 특정 수학적 연산을 훨씬 빠르게 할 수 있다. Shor 알고리즘은 인수 분해와 같이 고전 컴퓨터에서 오래 걸리는 계산을 보다 효율적으로 할 수 있어 RSA와 같이 큰 수를 소수로 분해하는 문제의 어려움을 기반으로 하는 알고리즘에 대해 치명적이다[1]. Grover 알고리즘은 정렬되지 않은 데이터베이스 상에서 특정 값을 찾는 속도를 높여준다[2]. 이는 brute force attack을 가속화시켜 기존 대칭키 암호 알고리즘을 깨는 시간을 줄여준다. 이에 이러한 알고리즘을 기반으로 하는 공격에 대한 내성을 갖는 양자 내성 암호가 필요하다.

양자 내성 암호에 대한 연구가 활발히 이루어지는 분야로는 격자 기반 암호 체계, 코드 기반 암호 체계, 해시 기반 암호 체계 등이 있다. 격자 기반 암호 체계는 격자라는 기하학적 구조를 활용한 암호 체계이다. 코드 기반 암호 체계는 노이즈가 있는 채널에서 데이터가 전송될 때, 데이터의 무결성을 보장하기 위한 에러 정정 코드를 기반으로 하는 암호 체계이다. 해시 기반 암호 체계는 복원하기 어려운 해시함수의 특징을 기반으로 하는 암호 체계이다.

3. NIST PQC 표준화 공모전

NIST(National Institute of Standards and Technology)는 양자 컴퓨터의 발전에 따라 양자 공격에 저항할 수 있는 새로운 양자 내성 암호(Post-Quantum Cryptography, PQC) 알고리즘을 선정하기 위해 표준화 공모전을 개최하였다. 이 공모전은 2016년부터 시작되었으며 최초 제출 마감일인 2017년 말까지 59개의 공개키 암호화/키 생성 방식

알고리즘, 23개의 서명 방식 알고리즘을 제출 받았다.

3.1 Round1

제출받은 82개의 알고리즘들 중에서 NIST는 철회된 알고리즘 5개를 포함하여 총 69개의 양자 내성 암호 알고리즘을 Round1에 선정하였다[3]. 선정된 알고리즘의 절반 이상이 격자 기반 암호 체계였으며, 그 다음으로 많은 알고리즘은 코드 기반 암호 체계이다.

3.2 Round2

Round2는 2019년 1월에 진행되었다. Round1에서 선정된 알고리즘 중에서 효율성, 실용성, 발견된 공격법 등에 의한 이유로 제외된 암호 알고리즘 외에 총 26개의 암호 알고리즘이 후보로 선정되었다[4]. Round1과 마찬가지로 격자 기반 암호체계와 코드 기반 암호체계가 주를 이루며 그 수는 격자 기반 12개, 코드 기반 7개에 해당한다.

3.3 Round3

Round3에 선정된 알고리즘은 NIST의 기준 하에 7개의 Finalists, 8개의 Alternate로 나누어졌다[5]. Finalists는 NIST 기준 Round3 말에 표준화 준비가 될 것으로 예상되는 유력한 후보들이며 Alternate는 Round3 이후에 선정될 가능성이 있는 잠재적인 후보들이다. Finalists와 Alternate에 해당하는 암호 알고리즘은 <표 1>, <표 2>와 같다.

<표 1> Finalists

유형	공개 키 암호/키 생성	서명
격자	CRYSTALS-KYBER NTRU SABER	CRYSTALS-Dilithium FALCON
코드	ClassicMcEliece	
다변수다항식		Rainbow

<표 2> Alternate

유형	공개 키 암호/키 생성	서명
격자	FrodoKEM NTRU Prime	
코드	BIKE HQC	
해시		SPHINCS+
다변수다항식		GeMSS
아이소제니	SIKE	
제로지식증명		Picnic

2022년 7월 NIST는 최종적으로 표준 양자 내성 암호를 선정하였다[6]. 선정된 암호 알고리즘으로는 공개 키 암호/키 생성 방식에는 격자 기반 암호 체계인 CRYSTLALS-KYBER, 서명 방식에는 격자 기반 암호 체계인 CRYSTALS-Dilithium, FALCON, 해시 기반 암호 체계인 SPHINCS+가 있다.

3.4 Round4

최종 암호 선정 이후 Round4가 진행되었다. 공개 키 암호/키 생성 방식으로 선정된 알고리즘은 CRYSTALS-KYBER가 유일하여 다른 알고리즘을 선정하기 위해서다. 선정된 알고리즘으로는 코드 기반 암호 체계의 BIKE, Classic McEliece, HQC가 있고 아이소제니 기반 암호 체계의 SIKE가 있다[7]. 이 중 아이소제니 기반의 SIKE는 공격법이 발견되어서 제외되었다.

4. NIST PQC 표준화 계획

본 장에서는 Round3에서 최종 선정된 암호 알고리즘의 표준화 계획에 대해 알아보도록 한다. NIST는 Round4 이후 개최된 표준화 컨퍼런스에서 최종 선정된 암호에 대한 표준화 목표를 밝혔다[8]. 또한 NIST는 표준화의 기준이 되는 보안 정도를 AES, SHA 공격에 필요한 자원을 기준으로 양자 후 보안 레벨로 제시하였으며 <표 3>과 같다.

<표 3> NIST Security Level

LEVEL	보안 정도
1	AES128 (exhaustive key search)
2	SHA256 (collision search)
3	AES192 (exhaustive key search)
4	SHA384 (collision search)
5	AES256 (exhaustive key search)

4.1 CRYSTALS-KYBER

NIST는 CRYSTALS-KYBER의 여러 버전 중 KYBER-768, KYBER-1024를 표준화할 것이라고 밝혔다. 이는 보안 레벨 3, 4에 해당한다. 보안 레벨 1에 해당하는 KYBER-512에 대한 표준화는 확정이 나지 않았으나 표준화할 확률이 높다고 전달했다. 마지막으로 90S버전은 표준화 목록에서 제외되었다.

4.2 CRYSTALS-Dilithium

NIST는 CRYSTALS-Dilithium이 기본 서명 알고리즘으로 사용하는 것이 좋다고 전달했다. Dilithium

에 대한 표준화 계획으로는 파라미터 셋을 조절하여 보안 레벨 2, 3, 5를 맞추는 것이다. 다른 버전인 Dilithium-AES는 표준화 목록에서 제외되었다. Dilithium-AES는 Round2에 대해 업데이트한 변형 모델로 카운터 모드에서 SHAKE대신 AES-256을 사용한 버전이다.

4.3 FALCON

FALCON은 CRYSTALS-Dilithium에 비해 상대적으로 크기가 작아 비용이 저렴한 편이다. 이러한 이유 등으로 선정되었으며 NIST가 밝힌 표준화 계획에서의 보안 레벨은 1, 5이다. 격자 기반 서명 방식의 기준이 되는 CRYSTALS-Dilithium의 표준화가 완전히 이루어진 후 FALCON에 대한 표준화가 진행될 것이라고 밝혔다.

4.4 SPHINCS+

SPHINCS+의 표준화 계획에서 보안 레벨은 1, 3, 5이다. SHA2를 사용한 경우가 보안 레벨 1이며, SHA256과 SHA512를 같이 사용한 경우가 보안 레벨 3, 5이다. SPHINCS+는 버전이 다양한데 이 중 SIMPLE 버전에 대해 표준화를 진행할 것이라고 밝혔다. ROBUST 버전은 제외되었다. ROBUST 버전은 Round1에 제출한 버전으로 SIMPLE 버전보다 속도가 3배 정도 느리다. 이외에도 FAST 버전과 SMALL 버전도 표준화 계획에 들어있다.

5. 결론

본 논문은 양자 내성 암호를 선정하기 위한 NIST PQC 공모전과 선정된 암호에 대한 표준화 계획을 알아보았다. NIST에서는 다양한 평가 기준을 통해 표준화를 위한 새로운 암호 알고리즘 선정에 노력을 가하고 있으며, 전 세계의 연구자들도 새로운 알고리즘을 위해 연구 및 개발을 이어나가고 있다. 아직 양자 컴퓨터의 시대가 오지 않았으나, 양자 내성 암호 알고리즘의 빠른 표준화와 보급은 다가올 시대에 대비하여 높은 보안성과 효율성을 보여줄 것이라고 생각된다.

6. Acknowledgements

This work was partly supported by Institute for Information & communications Technology Promotion(IITP) grant funded by the Korea government(MSIT) (No.2018-0-00264, Research on Blockchain Security Technology for IoT Services, 50%) and this work was partly supported by Institute of Information & communications Technology Planning & Evaluation (IITP) grant funded by the Korea government(MSIT) (No.2022-0-00627, Development of Lightweight BIoT technology for Highly Constrained Devices, 50%).

참고문헌

[1] SHOR, Peter W. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. SIAM review, 1999, 41.2: 303-332.

[2] GROVER, Lov K. A fast quantum mechanical algorithm for database search. In: Proceedings of the twenty-eighth annual ACM symposium on Theory of computing. 1996. p. 212-219.

[3] NIST, “Round 1 Submissions”, 2017, https://csrc.nist.gov/Projects/post-quantum-cryptography/post-quantum-cryptography-standardization/round-1-submissions

[4] NIST, “Round 2 Submissions”, 2019, https://csrc.nist.gov/Projects/post-quantum-cryptography/post-quantum-cryptography-standardization/round-2-submissions

[5] NIST, “Round 3 Submissions”, 2020, https://csrc.nist.gov/Projects/post-quantum-cryptography/post-quantum-cryptography-standardization/round-3-submissions

[6] NIST, “Selected Algorithms 2022”, 2022,https://csrc.nist.gov/Projects/post-quantum-cryptography/selected-algorithms-2022

[7] NIST, “Round 4 Submissions”, 2022, https://csrc.nist.gov/Projects/post-quantum-cryptography/round-4-submissions

[8] NIST, “Fourth PQC Standardization Conference”, 2022, https://csrc.nist.gov/events/2022/fourth-pqc-standardization-conference