양자내성암호 표준화를 위한 NIST 공모전 동향

Trend of NIST contest for PQC standardization

송민호* ,김현준*, 엄시우* , 서화정**
* 한성대학교 (대학원생), **한성대학교 (교수)

요약

기존에 존재하던 공개키 암호 및 전자서명 스킴들은 양자 알고리즘 Shor, Grover가 제시된 이 후 안정성을 위협받고 있다. 이에 양자내성암호(Post-Quantum Cryptography, PQC)에 대한 연구가 활발히 진행 중이며 본 논문은 그 중에서 특히 PQC 표준화를 위해 진행되는 NIST PQC 공모전에 대한 동향을 소개한다.
NIST는 취약점, 효율성, 실용성 등 다양한 이유를 기반으로 좋은 알고리즘의 표준화를 위한 공모전을 진행하고 있으며 현재 1 라운드부터 4 라운드까지 진행 중이며 추가적으로 전자서명에 대한 공모전을 진행 중이다.

서론

Shor 알고리즘과 Grover 알고리즘이 제시된 이후 양자 컴퓨터가 개발된다면 현재 존재하는 공개키 암호들의 안정성을 더는 보장할 수 없다. 이는 Shor, Grover 알고리즘이 소인수 분해 등 수학적 문제에 기반하는 공개키 암호들을 다항 시간 내에 분석할 수 있기 때문이다. 이에 다양한 암호 알고리즘에 대한 분석과 연구가 진행 되었으며 양자 알고리즘에 내성을 가지는 양자내성암호에 대한 관심도가 높아졌다.
이에 본 논문에서는 양자내성암호 표준화를 위해 진행된 NIST PQC 공모전에 대한 동향을 소개한다. 기존에 진행되었던 공모전을 통해 4개 의 알고리즘이 표준으로 선정되었고 추가적인 표 준화를 위해 4 라운드가 진행 중이다. 또한 새로 이 전자서명 표준화를 위한 공모전이 개최되었으며 현재 진행 중에 있다.

PQC Standardization

3라운드까지 진행사항

NIST는 다양한 알고리즘 후보들을 제출 받았으며 최종적으로 2017년 말 총 69개의 후보들을 1 라운드에 선정하였다. 선정된 알고리즘들의 대부분은 격자 기반 암호였으며 그 다음은 코드 기반 암호들이 주를 이뤘다. 이후 효율성, 실용성, 취약점 등의 이유로 다양한 후보들이 탈락되었고 3 라운드에는 15개의 후보만이 남게 되었다.

표준화 암호 선정

3 라운드 이후 NIST는 2022년 7월 최종적으로 표준화를 위한 알고리즘들을 선정하였다. 총 4개의 알고리즘이 선정되었으며 선정된 알고리즘은 <표 1>과 같다

<표 1> 최종 선정된 알고리즘

유형	공개 키 암호/생성	전자서명
격자	CRYSTALS-KYBER	CRYSTALS-Dilithium Falcon
해시	-	SPHINCS+
총계	**1**	**3**

4라운드

최종 공개 키 암호/생성 방식으로 선정된 후 보는 CRYSTALS-Kyber 단 하나밖에 존재하지 않는다. 이에 추가 선정을 위해 NIST는 4 라운드를 진행하였다. 4 라운드에 선정된 후보는 총 4개이며 <표 2>와 같다.
코드 기반에서는 BIKE, HQC, SIKE, Classic McEliece가 선정되었고 아이소제니 기반에서는 SIKE가 선정되었다. 그러나 SIKE는 치명적인 공격법이 발견되어서 후보에서 제외되었다.

<표 2> 4라운드 선정 후보

유형	공개 키 암호/생성
코드	BIKE HQC Classic McEliece
아이소제니	~~SIKE~~
총계	**4**

PQC Digital-Signature Schemes

기존의 공모전이 4 라운드를 진행하고 있는 도중에 전자서명 표준화를 위한 공모전이 추가로 개최되었다. 전자서명 공모전을 위한 알고리즘 후보들은 2023월 6월 1일까지 모집 받았다. 이후 7월 17일 NIST는 최종후보를 발표하며 1 라운드가 진행되었다. 1 라운드에는 총 40개 의 후보가 등록되었으며 선정된 후보들에 대한 통계는 <표 3>과 같다.
선정된 40개의 후보들 중 다변수 기반 전자 서명이 11개로 가장 많으며 그 뒤로는 격자 기반, 코드 기반, MPC-in-the-head(MPCitH) 기 반이 많은 것을 확인할 수 있다.

<표 3> 전자서명 1라운드 후보 통계

유형	개수
Code	6
Isogeny	1
Lattice	7
MPC-in-the-head	6
Multivariate	11
Symmetric	4
Other	5
총계	**40**

PQC Conference

NIST는 공모전을 진행하는 동시에 표준화 과 정과 관련된 컨퍼런스를 주기적으로 진행한다. 이 컨퍼런스는 라운드에 선정된 후보 알고리즘의 다양한 측면에 대해 논의하는 과정을 갖는다. 후 보 알고리즘에 대한 업데이트 내용이나 부채널 공격 방면에 대한 피드백 내용들이 존재한다. 4 라운드 이후에 개최된 컨퍼런스에서는 NIST가 최종 선정된 4개의 알고리즘에 대한 구체적인 표준화 계획을 밝히기도 하였다.

결론

본 논문에서는 기존에 양자내성암호 표준화를 위해 개최된 NIST PQC 공모전과 최근 추가적으 로 진행된 전자서명 공모전에 대해 소개하였다. 현재 총 4개의 알고리즘들이 최종 선정되었으며 추가적으로 후보들을 선정하기위해 4 라운드 및 전자서명 공모전이 진행 중에 있다. 양자 컴퓨터 시대가 다가올수록 양자내성암호에 대한 관심과 중요성은 더욱 높아질 것이다. 이에 지속적인 연 구가 필요할 것으로 보이며 이러한 과정은 다가 올 시대에 대비하여 효율성, 보안성 방면에서 도 움이 될 것이다.

Reference

[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-crypto graphy-standardization/round-1-submissions
[4] NIST, “Round 3 Submissions”, 2020, https://csrc.nist.gov/Projects/post-quantum-cryptography/post-quantum-crypto graphy-standardization/round-3-submissions
[5] NIST, “Selected Algorithms 2022”, 2022, https://csrc.nist.gov/Projects/post- quantum-cryptography/selected-algorith ms-2022
[6] NIST, “Round 4 Submissions”, 2022, https://csrc.nist.gov/Projects/post-quan tum-cryptography/round-4-submissions
[7] NIST, “Round 1 Additional Signatures”, 2023, https://csrc.nist.gov/Projects/pqc-dig-sig/round-1-additional-signatures
[8] NIST, “Fourth PQC Standardization Conference”, 2022, https://csrc.nist.gov/events/2022/fourth -pqc-standardization-conference