기술

미 NIST, 포스트양자암호화(PQC) 첫 번째 표준 발표

DATE: 2024.08.13 | #양자정보통신

NIST(국립표준기술원)는 양자 컴퓨터의 사이버 공격 대응을 위해 2016년부터 포스트양자암호화(Post-Quantum Cryptography, PQC) 표준화 작업을 추진해 왔으며, 최종 암호화 알고리즘 4개 중 3개를 연방정보처리표준(FIPS)으로 발표하였다.

- 표준 초안 발표('23.8) 이후 버전 지정을 위해 알고리즘 이름 변경
  - (FIPS 203) 일반 암호화를 위한 기본 표준으로 사용되며, ML-KEM 알고리즘 기반
  - (FIPS 204) 디지털 서명 보호를 위한 주요 표준으로 ML-DSA 알고리즘 사용
  - (FIPS 205) 디지털 서명을 위해 설계된 표준으로 SLH-DSA 알고리즘 사용. ML-DSA와 다른 수학적 접근 방식을 기반으로 하며, ML-DSA가 취약한 것으로 판명될 경우를 대비한 백업 방법으로 사용됨

  ※ FALCON으로 구축된 'FIPS 206' 표준 초안은 FN-DSA로 명명되어 2024년 말 발표 예정

- 이번 발표된 세 개 알고리즘에 대한 백업 표준으로 사용할 알고리즘 세트 평가 중
  - (세트 1) 일반 암호화를 위해 설계된 세 개 알고리즘으로 구성. 2024년 말까지 알고리즘 중 1~2개 채택 발표 계획
  - (세트 2) 디지털 서명을 위해 설계된 알고리즘 그룹*으로 근시일내 테스트 및 평가를 진행할 약 15개 알고리즘 발표 예상

  * 제출 요청('16) 이후 암호학자들의 추가 아이디어를 수용하기 위해 추가 알고리즘 요청('22)을 하였으며, 이에 대해 평가하는 프로세스 시작

ML-KEM

Module-Lattice-Based Key-Encapsulation Mechanism Standard의 약자로 CRYSTALS-Kyber 알고리즘 기반

ML-DSA

Module-Lattice-Based Digital Signature Standard의 약자로 CRYSTALS-Dilithium 알고리즘 기반

SLH-DSA

Stateless Hash-Based Digital Signature Standard의 약자로 SPHINCS+ 알고리즘 기반

FN-DSA

FFT(fast-Fourier transform) over NTRU-Lattice-Based Digital Signature Algorithm의 약자로 FALCON 알고리즘 기반

참조문서

TTA, 해외 ICT 표준화 동향정보 (2022년 07월), 미국 NIST, 포스트양자암호화 표준을 위한 후보 알고리즘 공개

TTA, 해외 ICT 표준화 동향정보 (2023년 08월), 미국 NIST, 포스트양자암호화 알고리즘에 대한 표준 초안 발표

기사원문 미국 NIST, NIST Releases First 3 Finalized Post-Quantum Encryption Standards, https://www.nist.gov/