NIST, PQC 위한 다섯 번째 알고리즘으로 HQC 선택

(2025.03.20., 양자정보연구지원센터)

□ NIST, 포스트-양자 암호화를 위한 백업 알고리즘 HQC 선택

○ 개요

- NIST는 양자 컴퓨터 공격에 대비할 수 있는 암호화 알고리즘을 표준화해왔으며, 올해는 이를 보완할 수 있는 백업 알고리즘 HQC를 선택함
- HQC는 ML-KEM 암호화 알고리즘의 보조 방어책으로 선택되었으며, 인터넷 트래픽과 저장된 데이터를 보호할 수 있도록 설계됨
- 양자 컴퓨터가 발전함에 따라 현재의 암호화 방안을 해독할 수 있을 위험에 대비하기 위해 NIST는 여러 암호화 알고리즘을 연구해왔음

○ HQC 알고리즘의 특징과 선택 이유

- (ML-KEM과 HQC의 차이점) HQC는 ML-KEM을 대체하려는 목적이 아니라, 다른 수학적 접근법을 사용하여 예비 방어책을 제공
- **ML-KEM은 구조적 격자(structured lattices)를 기반**으로 하고, **HQC는 오류 정정 코드(error-correcting codes)를 기반**으로 함
- HQC는 계산 자원이 더 많이 소모되지만, 안정성과 보안성 측면에서 충분한 평가를 받아 백업 알고리즘으로 선정됨
- NIST의 Dustin Moody 수학자는 “ML-KEM이 취약점에 노출될 경우를 대비해 HQC를 선택했다”고 설명

○ 현재와 미래의 표준화된 암호화 알고리즘, NIST의 포스트-양자 암호화 프로젝트

- NIST는 2016년부터 양자 컴퓨터의 위협에 대비해 암호화 알고리즘 개발을 시작했으며, HQC는 네 번째 라운드에서 선택된 유일한 알고리즘
- HQC는 이전에 선택된 네 가지 알고리즘 중 하나로, 그 중 세 가

지는 이미 표준화 완료됨

- ML-KEM은 FIPS 203(Federal Information Processing Standard) 표준의 핵심, 두 개의 디지털 서명 알고리즘은 FIPS 204 및 FIPS 205로 완성되어 이미 사용되고 있음
- FIPS 206은 FALCON 알고리즘을 기반으로 한 디지털 서명 알고리즘으로, 곧 초안이 공개될 예정

○ HQC 알고리즘의 향후 발표와 피드백, 표준화 과정과 향후 일정

- NIST는 HQC를 포함한 표준으로 2027년까지 최종 공개할 예정이며, 그 전에 1년 후 공개 초안을 발표하고 90일 간의 피드백 기간을 거칠 예정
- HQC는 “키 캡슐화 메커니즘(KEM)”으로, 공개 네트워크에서 두 당사자가 기밀 정보를 교환할 수 있도록 돕는 역할을 함
- 최근 NIST는 KEM 알고리즘의 구현 가이드라인을 담은 초안을 발표, 이를 바탕으로 KEM 사용에 대한 보안 권장사항을 제공

○ HQC과 ML-KEM의 역할

- HQC과 ML-KEM을 대체하지 않고 보완하는 역할을 하며, 이를 통해 향후 양자 컴퓨터에 대비한 암호화 기술을 더욱 강화할 수 있음
- NIST는 향후 더 많은 연구를 통해 양자 컴퓨터에 대비한 암호화 기술을 발전시키고, 그에 따른 표준화 과정을 지속적으로 진행할 계획

○ NIST는 양자 컴퓨터의 위협에 대비하기 위해 HQC를 새로운 암호화 알고리즘으로 선택, ML-KEM을 보완하는 백업 방어책 역할

- 향후 HQC 표준화가 완료되면, 더 강력한 데이터 보호가 가능해질 것임

(원문)

1. https://thequantuminsider.com/2025/03/11/nist-selects-hqc-as-fifth-algorithm-for-post-quantum-encryption/