NIST, 최초의 4가지 양자 저항 암호화 알고리즘 발표

(2022.07.06., 양자정보연구지원센터)

□ NIST, 미래 양자 컴퓨터 공격 대비한 첫 암호화 도구 그룹 선택

○ 선택된 4개 암호화 알고리즘은 NIST 포스트 퀀텀 암호화 표준의 일부로, 2년 안에 완성 예상

- 미래 사이버 공격 가능성 대비, 민감한 데이터 보호에 주요 이정표

○ **포스트 양자 암호화(post-quantum cryptography standardization)** 프로그램

- 미래 양자 컴퓨터 공격에 저항할 암호화 방법 고안 검사 요청, 2016년부터 6년간 노력의 결과
- 기관의 포스트 양자 암호화표준화 프로젝트의 피날레 시작 구성
- 전 세계 암호화 분야 최고 전문가 활용하여 표준 제시, 디지털 정보 보안 향상, 첫 번째 양자 저항(quantum-resistant) 알고리즘 그룹 생성

○ 일반적인 암호화, CRYSTALS-kyber 알고리즘 선택

- 일반적인 암호화는 공용 네트워크를 통해 교환되는 정보 보호
- 두 당사자가 쉽게 교환할 수 있는 비교적 작은 암호화 키와 작동 속도가 CRYSTALS-kyber 알고리즘의 장점

○ 디지털 서명에는 세 가지 알고리즘 선택

- 디지털 서명 : 신원 인증 또는 원격으로 문서에 서명할 때 사용
- CRYSTALS-Dilithium(기본 알고리즘 권장), FALCON(더 작은 서명이 필요한 응용 프로그램에 사용) 및 SPHINCS+ 알고리즘(백업으로 가치) 선택

○ 표준이 완성되기 전에 알고리즘 변경이 가능하므로 시스템에 적용하지 않도록 함

(원문)

1. https://thequantuminsider.com/2022/07/05/nist-announces-first-four-quantum-resistant-cryptographic-algorithms/