미 정부와 QuSecure, 정부 네트워크 통한 양자 후 암호화 통신 조정

(2022.07.15., 양자정보연구지원센터)

□ 미 정부 네트워크 통한 세계 최초 포스트 양자 암호화 통신 조정

○ QuSecure의 QuProtect PQC(Post-Quantum Cyber security) 솔루션 활용

- 양자 보안 채널 사용, 암호화된 통신 및 데이터를 양자 복원력으로 보호하도록 설계된 업계 최초 종단 간 PQC 소프트웨어 기반 솔루션

○ 양자 탄력적(quantum-resilient) 배포, QuProtect 양자 터널 통해 대역폭이나 지연 문제없이 이전 표준 암호화 사용한 데이터 보호

- 현재 전송 중인 데이터는 QuProtect 시스템 없이 해독 불가능, 미래 양자 컴퓨터를 사용하더라도 해독할 가능성 거의 없음

- QuProtect 플랫폼은 중단없이 지속적인 양자 채널 가동시간으로 인해, 이전에 고전적 암호화되어 양자에 취약했던 비대칭 키 보호에 탁월한 성능 발휘

○ PQC 솔루션에 대한 SBIR(Small Business Lnnovation Research) 3단계 연방 정부 조달 계약에 대한 QuSecure 평가 및 최종 수주 활동으로 가능

- 포스트 퀀텀 위협에 대한 PQC 배포의 필요성 더욱 강조

- 정부의 QuSecure 배포는 레거시 장비 및 시스템에 대한 개방형 인터넷 네트워크 통해 운영

○ QuProtect, 조직 처음으로 양자 복원력 기술 활용하여 사이버 공격 방지 및 네트워크 미래 보장, 양자 후 사이버 위협에 대비

- 양자 복원력있는 암호화 제공, 종단 간 QSaaS (Quantum-security-as-a-Service) 아키텍쳐 사용

- 은행/금융, 의료, 우주/위성, 연방 운영 및 기타 여러 산업 분야에 배치

(원문)

1. https://www.hpcwire.com/off-the-wire/us-gov-and-qusecure-orchestrate-post-quantum-encryption-communication/