CQ, 양자-강화 암호화 키 생성 플랫폼 출시

(2021.12.21., 양자정보연구지원센터)

□ CQ, Quantum Origin 출시

○ 검증 가능한 양자 무작위성 기반, 세계 최초 상용 암호화키 생성 플랫폼

- NISQ 컴퓨터 사용하여 구축된 최초 상용 제품
- 현재 미래 위협으로부터 전 세계 데이터 보호('hack now, decrypt later')
- 오늘날 RSA 및 AES 같은 암호화 표준으로 시스템 보호, 현재 난수발생기(RNG)는 진실하고 검증가능한 무작위성 부족

○ 양자역학의 예측 불가능한 특성 사용한 클라우드 호스팅 플랫폼

- Quantinuum H-시리즈 양자 컴퓨터(Honeywell 제공)에서 검증 가능한 양자 무작위성 시드된 암호화 키 생성
- 기존 알고리즘(RSA나 AES)과 현재 NIST(미 국립표준기술연구소)에서 표준화하고 있는 양자후(post-quantum) 암호화 알고리즘 지원

○ 주문형 양자 강화 키

- 조직이 양자 강화 키 생성해야 할 때 API 통해 호출, 전송 키 암호화하고 조직으로 안전하게 전달 전에 키 생성
- 기존 사이버 보안 시스템 및 하드웨어에서 사용 가능한 형식으로 제공, on-demand 방식으로 생성, 확장 가능한 동시에 보안 상태 유지

○ Quantum Origin 실제 사용

- 금융 서비스 회사와 사이버 보안 제품 공급업체에 제공 후, 통신, 에너지, 제조, 국방 및 정부 같은 우선순위 높은 다른 분야로 확장 예정
- ISS와 지구 간 양자후 암호화 통신 테스트(Axiom Space), 기존 알고리즘과 양자 강화키 사용, 소프트웨어 정의 광역네트워크(SDWAN)에 통합(Fujitsu)

(원문)

1. https://thequantuminsider.com/2021/12/07/cambridge-quantum-launches-quantum-enhanced-cryptographic-key-generation-platform-to-protect-data-from-advancing-threats/