미, 중국 조직에 양자 컴퓨팅 기술 수출 차단

(2021.11.30., 양자정보연구지원센터)

□ 미, 양자 컴퓨팅 기술 보안

○ 미 상무부, 중국 기업과 연구소(8개)에 양자 컴퓨팅 기술 수출 금지

- 미국의 기밀 통신 암호 해독, 새로운 군사 기술 개발 방지 목적
- 기술적으로 미성숙하지만 양자 컴퓨터는 기존 암호화 해독 가능

○ 양자 컴퓨터의 잠재력

- 대스텔스 및 대잠수함 응용 관련 양자 컴퓨팅의 군사적 위험인지
- 신물질 개발로 이어지는 분자 구조 시뮬레이션(재료 과학)
- 응용 프로그램 및 암호화를 깨거나, 깨지지 않는 암호화 개발 능력

○ 양자 컴퓨팅의 혁신 활용

- 미 정부, 양자 후 암호화(post-quantum cryptography) 개발 위해 적극적 프로그램 주도
- 미 기업들, 양자 컴퓨터 개발에 수십억 달러 투자(Google, IBM, Microsoft, Honeywell, IonQ, Rigetti, D-wave 및 Intel 포함)

○ 양자 컴퓨팅 기술 개발 경쟁

- 공개 키 암호화는 오늘날 컴퓨터에 저장되거나 네트워크 통해 전송되는 데이터 보호, 대규모 양자 컴퓨터가 구축되면, 현재 사용 중인 많은 공개 키 암호화 시스템을 깰수 있음
- 양자 후 암호화(post-quantum cryptography) 노력, 양자 컴퓨터에 영향을 미치지 않는 새로운 암호화 알고리즘 생성, 테스트 및 채택, 제품 제공(IBM, Thales etc.) 시작
- 구글, 새로운 센터에 2029년까지 실용적 양자 컴퓨터 구축 계획

(원문)

1. https://www.cnet.com/tech/computing/us-blocks-export-of-quantum-computing-tech-to-chinese-organizations/