양자 암호화란, 양자 위협 및 양자 솔루션

(2022.05.30., 양자정보연구지원센터)

□ 양자 위협에 대비한 양자 솔루션, 양자 암호화 연구

○ 양자 암호화(quantum cryptography) : 양자 컴퓨터가 데이터를 저장하고 보호하는 기능에 영향을 미칠 수 있는 방법을 연구하는 분야

- 양자 컴퓨터는 데이터와 메시지 보호 방식에 위협이 되지만, 해킹 불가능한 데이터 저장 및 전송에 이론적 경로를 포함한 다양한 솔루션을 제공함

○ 현재 데이터 보호 방법인 RSA(공개 키 암호화 기술)는 수학적 원리 기반의 알고리즘을 사용, 지정된 당사자만 정보에 접근가능하도록 데이터를 암호화

- 기존 컴퓨터가 해독하기 매우 어려운 반면, 양자 컴퓨터는 이 암호화 방법을 쉽게 깨트릴 수 있음
- 세계 전체 경제 및 안보 시스템이 위험에 처하게 됨

○ **양자 후 암호화(PQC, Post-quantum cryptography)**

- 양자 위협을 무력화할 양자 솔루션으로, 양자 공격에 안전할 것으로 여겨지는 여러 알고리즘 솔루션 제공
- 양자 컴퓨터 사용하여 어려워지는 암호화 방법 구축 경쟁 진행 중

○ **양자 키 분배(QKD, quantum key distribution)**

- 양자 기술 사용하여 당사자 간 공유되는 키 생성함, 클라우드 기반의 (이론상) 완전히 예측할 수 없는 난수를 생성하므로 해킹에 사용할 수 없음
- 키를 생성하고 전송하기만 할 뿐 정보를 보내지 않음

(원문)

1. https://thequantuminsider.com/2022/05/27/what-is-quantum-cryptography-a-look-at-quantum-threats-and-quantum-solutions/