Post Quantum Cryptography(PQC) 소개

(2023.03.10., 양자정보연구지원센터)

□ Post Quantum Cryptography(PQC, 양자 후 보안)

○ 소개

- 인터넷의 급속한 성장으로 우리가 교환하는 정보(이메일, 문자, 인터넷 검색, 가상 서명 전송, 은행 플랫폼 로그인 등) 교환을 위한 보안 시스템이 중요해짐
- 양자 컴퓨터는 현대의 암호화 기술을 깨뜨릴 잠재력을 가지고 있으므로, 현대 디지털 생활의 복잡성 증가와 함께 **사이버 보안 위험에 대한 기업의 우려 증대**

○ 양자 보안이 중요한 이유

- 양자 컴퓨터의 성능은 중첩과 얽힘에서 나오며, 양자 얽힘은 얽힘 상태를 유지할 수 있는 양자 컴퓨터가 얽힌 각 큐비트에 대한 계산 능력을 기하급수적으로 향상시킬 수 있음
- 데이터 및 개인 정보 보호에 사용되는 대부분의 프로토콜이 미래 양자 컴퓨터에 취약한 상태
- Shor 알고리즘은 충분한 성능의 양자 컴퓨터에서 실행될 때 소수의 정수를 찾을 수 있으며, 소인수분해의 복잡성은 RSA 및 타원곡선 암호화(ECC) 같은 현재의 공개키(비대칭) 암호화 체계가 데이터를 보호하기 위해 구축되는 방식임

○ 지금 행동해야 하는 이유

- 사이버 보안 전문가들은 사이버 범죄자들의 “Steal now, decrypt later “ 공격을 우려
- 미국은 모든 정부 기관에 향후 6개월 이내 대응 계획 작성 요구(2022.1), 미 연방 기관은 양자 컴퓨팅 사이버 보안 대비법(Quantum Computing Cybersecurity Preparedness Act) 도입(2022.4)

- 유럽연합 집행위원회는 유럽 양자통신 인프라(EuroQCI) 이니셔티브 제정(2019), 양자 키 분배(QKD) 사용하여 2027년까지 유럽 양자 보안 인터넷 시스템 구현 목표

ㅇ PQC에 대한 다양한 접근 방식 분석

- 미, NIST는 측정, 통신 및 보안 분야에서 광범위한 산업 기기 규정 및 분석 지표 설정하는 연구 시설, PQC에서 국가 표준에 대한 적격 후보 결정에 7년 프로그램 시작(2022년 7월 발표)
- NIST 후보 기준으로 판단, 가능한 표준화를 위한 최종 4차 라운드 경쟁을 통해, 3개의 최종 후보와 1개의 대안 선택
- 결과 알고리즘은 공개 키 암호화와 디지털 서명으로 구분, 수학적 암호화 제품군으로 세분화
- 4개 알고리즘 중 3개는 다항식의 어려운 분해를 활용하거나 오류로 흩어져 있는 행렬을 발견하는 방법인 격자 계열, **격자 알고리즘**은 암호화와 검증 모두에 사용 가능한 범용 응용 프로그램
- 다른 알고리즘은 높은 **엔트로피 해시 함수**, SPHINCS+ 같은 보안 해싱 알고리즘은 큰 키가 필요하고 암호화 속도는 느리지만 격자 방식에 대한 안정적인 백업을 제공함

ㅇ 주요 일부 회사 및 사례 연구

- 양자 보안 데이터베이스는 QKD, 양자 난수 생성기(ORNG), PQC 및 전반적으로 필요한 하드웨어 작업을 포함
- 양자 보완 회사: QUANTROPI, QRYPT, ARQIT, PQSHIELD
- 기업과 정부는 조기에 양자 보안 공급자와 협력, 제품 제공의 견고성과 양자 보안 환경의 구현 용이성 평가를 권장
- 주요 고려 사항: 기술 및 팀의 품질, 실행 속도 및 지원, 구현에 의해 제공되는 장기적 유연성(암호화 민첩성) 및 솔루션의 견고성

(원문)

1. https://thequantuminsider.com/2023/03/01/tqi-exclusive-an-introduction-to-post-quantum-cryptography/