양자 보안 전환은 과잉 대응 아닌 신중한 접근 필요

(2025.12.10. 양자정보연구지원센터)

□ 양자 보안 전환, 과잉 대응 아닌 신중한 접근 필요

○ 양자 컴퓨터 위협 평가와 현실

- 현재 공개된 양자 하드웨어는 RSA-2048 등 기존 암호 체계를 깨기에는 물리적 큐비트 수, 오류율, 연결성 등에서 여전히 수십만~수백만 배 규모 개선 필요
- **“양자 우위(Quantum advantage)”** 발표 대부분은 실질적 암호 공격과 무관한 특수 문제에서의 성과이며, 실제 위협과는 거리가 있음
- 암호화 관련 위험은 즉시 도래하지 않았으나, 장기 기밀 데이터를 대상으로 한 “지금 수집, 나중에 해독(Harvest now, decrypt later)” 공격은 즉각 대응 필요

○ 장기 기밀 데이터 보호 전략

- **하이브리드 암호화 방식**: 기존 고전적 암호와 포스트-양자 암호 결합 → 미래 양자 공격 대비 + 현재 보안 유지
- **암호화와 디지털 서명 구분**: 디지털 서명은 과거 데이터 노출과 무관 → 불필요한 조기 전환 위험 존재
- **블록체인 적용**: 비공개 정보 없는 블록체인은 양자 공격 위험 낮음, 프라이버시 중심 블록체인은 우선 대응 필요

○ 비트코인과 블록체인 특수 문제

- 양자 위협보다 거버넌스 지연, 미사용 코인 문제로 전환 계획 필요
- 양자 공격은 단계적, 선택적 진행 → 노출된 주소/코인 우선 위험
- PoW(작업증명) 기반 보안은 양자 컴퓨터로도 근본적 파괴 어렵고, 속도 향상은 제한적

○ 포스트-양자 암호화 위험과 구현 문제

- 포스트-양자 암호는 구현 난이도 높고 성능 저하, 사이드 채널 취약점 존재
- 해시 기반, 격자 기반 등 다양한 수학적 접근법 존재 → 장단점 존재, 표준화 과정에서 이미 몇몇 후보군이 일반 컴퓨터 공격으로 깨짐
- 블록체인 서명 집계 등 복잡한 응용에서는 추가 연구와 신중한 도입 필요

ㅇ 권장 대응 전략

- **장기 기밀 데이터**: 즉시 하이브리드 암호화 적용
- **서명/업데이트**: 성능 영향 적은 경우 해시 기반 서명 조기 도입
- **블록체인**: 프라이버시 중심 체인 우선 전환, 일반 체인은 계획과 정책 수립 → 급한 도입 자제
- 개발자 우선 과제: 코드 감사, 형식 검증, 사이드 채널/결함 공격 대응
- 국가 차원: 양자 컴퓨팅 연구 지속 지원, 경쟁국 대비 전략적 관점 유지

ㅇ 결론

- 양자 암호 공격은 대부분 먼 미래 문제, 단기 과잉 대응은 오히려 취약점 유발 가능
- 장기 기밀 보호, 신중한 포스트-양자 암호 도입, 블록체인 준비 등 균형 잡힌 전략 필요
- 기술적 성과 발표는 위험 신호가 아닌 넘어야 할 기술적 과제로 인식해야 함

(원문)

1. https://thequantuminsider.com/2025/12/06/a16z-researcher-calls-for-measured-quantum-security-shift-not-panic/