IBM, Signal-Threema와 함께 양자 내성 메시징 기술 연구

(2026.03.19., 양자정보연구지원센터)

□ IBM, Signal-Threema 양자 안전 메시징 연구

ㅇ 배경 및 필요성

- 전 세계 수많은 사용자가 메시징 앱을 통해 일상적 소통 수행
- Signal 등은 종단간 암호화(E2EE)를 통해 높은 보안성 제공
- 기존 암호는 고전 컴퓨터로는 해독이 거의 불가능하지만, 양자 컴퓨터 발전 시 위협 가능성 존재

ㅇ 양자 컴퓨팅과 암호 위협

- 양자 컴퓨터는 큐비트, 중첩, 얽힘을 활용하여 기존보다 빠른 계산 수행 가능
- 현대 암호 체계(소인수분해, 이산로그 등)는 양자 컴퓨터에 의해 약화될 수 있음
- 이에 따라 양자 내성(Post-Quantum Cryptography) 기술 개발 필요
- 2024년 NIST가 양자 내성 암호 표준 일부 발표 (IBM 연구진 참여)

ㅇ IBM과 Signal 협력 연구

- 기존 암호 기술을 양자 안전 방식으로 전환하는 연구 진행
- 특히 그룹 메시징 프로토콜의 양자 내성화에 집중
- 단순히 기존 암호를 대체할 경우 네트워크 대역폭이 최대 100배 증가하는 문제 발생

ㅇ 프로토콜 재설계 핵심 아이디어

- 서버 중심 구조 → 사용자 참여형 검증 구조로 변경

- 서버는 암호화된 데이터 저장 및 권한 관리만 수행
- 사용자에게 가명 키(pseudonym key)를 부여하여
→ 개인정보 노출 없이 활동 추적 가능
- 기존 프라이버시 보호 구조 유지하면서 효율성 개선

○ 적용된 암호 기술
- ML-DSA(격자 기반 디지털 서명) → 키 재랜덤화 기능 추가
- 새로운 보안 모델 설계 → 사용자/서버 침해 상황까지 고려
- 목표: 보안성 + 효율성 + 확장성 동시에 확보

○ 보안 위협 대응(Harvest Now, Decrypt Later)
- 현재 암호 데이터를 수집 후 미래에 해독하는 공격 존재
- Signal은 2023년부터 대응 기술 적용
- 2025년 SPQR 프로토콜 도입 → 보안 강화

○ Threema와의 협력
- Threema 역시 양자 내성 메시징 기술 도입 검토
- ML-KEM(격자 기반 키 교환 알고리즘) 적용 연구 진행
- IBM과 협력하여 차세대 보안 통신 기술 개발 추진

○ 의의 및 전망
- 양자 컴퓨팅 시대에 대비한 차세대 보안 메시징 기술 기반 구축
- 기존 서비스의 프라이버시 유지하면서 양자 내성 확보 시도
- 향후 실제 서비스 적용 시 안전한 글로벌 통신 환경 구축 가능

(원문)

1. https://thequantuminsider.com/2026/03/10/ibm-signal-threema-quantum-safe-research/