연구진, 복제할 수 없는 새로운 양자 암호화 방식 개발

(2026.09.10., 양자정보연구지원센터)

□ UCSB와 UCLA 연구진, 복제할 수 없는 새로운 양자 암호화 방식 개발

○ 양자역학의 ‘복제 불가능성’을 활용한 새로운 양자 암호화 기술 제시

- UCSB(Unversity of California, Santa Barbara)와 UCLA(University of California, Los Angeles) 연구진은 **고전적 암호키만으로 구현하면서도 정보이론적으로 안전한 ‘복제 불가능 암호화(Unclonable Encryption)’ 방식**을 제안

- 양자 상태를 완벽하게 복제할 수 없다는 양자 **no-cloning 정리**를 활용해, 암호키가 공개된 이후에도 암호문을 두 개의 유용한 복사본으로 만드는 공격을 방지

- 단일 비트 메시지를 대상으로 완전한 정확성을 보장하면서, 공격자가 암호문을 두 개로 복제해 모두 올바르게 해독할 확률을 **50% + 지수적으로 작아지는 미미한 수준**으로 제한

- 암호화에는 단일 큐비트 Clifford 게이트, 복호화에는 국소 Pauli 측정을 사용해 기존 이론적 방식보다 효율적인 구현 가능성을 제시

○ **기존 양자 암호화의 한계를 극복하는 새로운 보안 증명**

- 기존 방식은 양자 복호화 키, 이상적인 양자 랜덤 오라클 또는 계산적으로 비현실적인 알고리즘 등에 의존하는 한계가 존재

- 연구진은 기존의 BB84 상태 기반 방식 대신 **Random Tensor Pauli 구조를 활용**하고, 양자정보이론의 수학적 도구를 통해 보안성을 엄밀하게 증명

- 보안이 공격자의 계산 능력이나 특정 수학적 난제에 의존하지 않고 **양자역학의 기본 법칙 자체에 기반한 정보이론적 보안**을 달성

○ **보안 통신 및 디지털 콘텐츠 보호 등 활용 가능성**

- 암호화된 정보 자체의 복제를 물리적으로 제한할 수 있어 보안 통신, **디지털 저작권 관리(DRM)** 등에서 새로운 보안 기능으로 활용될 가능성
- 특히 암호키가 사후에 공개되더라도 제3자가 암호문을 복제해 여러 개의 유효한 정보를 얻는 것을 어렵게 하는 것이 핵심

○ 현재는 이론적 연구 단계로 추가적인 기술 개발 필요

- 현재 제안된 방식은 **1비트 메시지를 1회용 키로 암호화하는 수준**으로, 장문 메시지·키 재사용·실제 서비스 적용 등은 향후 해결해야 할 과제
- 연구 결과는 아직 arXiv에 공개된 프리프린트로, 동료평가를 거치지 않은 초기 이론 연구라는 점에서 후속 검증이 필요함

○ **AI를 활용한 양자 암호 연구의 새로운 사례**

- 이번 연구는 암호화 방식뿐 아니라 AI가 이론적 암호학 연구의 구성과 증명 과정에도 활용된 사례라는 점에서 주목할 만함
- 연구진은 핵심 암호화 구조와 증명 아이디어가 AI 모델 “Codex(GPT-5.6 Sol Ultra)”를 통해 생성됐다고 밝히면서도, 최종적인 주장과 수학적 증명에 대한 검증 및 책임은 연구진이 직접 수행했다고 설명
- 이는 향후 양자정보·암호학 등 고도의 수학적 연구에서 **AI를 연구 보조 및 새로운 이론 탐색 도구로 활용하는 가능성**을 보여주는 사례로 평가됨.

(원문)

1. https://thequantuminsider.com/2026/08/05/researchers-say-new-quantum-encryption-method-cant-be-copied//