양자정보 안전하게 백업하는 방법 최초 발견

(2026.01.22., 양자정보연구지원센터)

□ 암호화된 큐비트 복제 가능, 양자정보를 안전하게 백업하는 최초의 방법 발견

○ 캐나다 워털루대학교(University of Waterloo) 연구진이 양자컴퓨팅의 근본적 제약으로 여겨져 온 ‘복제 불가 정리(no-cloning theorem)’를 우회하는 획기적 방법을 제시함

- 해당 성과는 양자 정보의 안전한 백업과 분산 저장을 가능하게 하는 새로운 개념을 제시
- 연구 결과는 국제 학술지 Physical Review Letters에 「Encrypted Qubits can be Cloned」라는 제목으로 게재됨

○ 양자컴퓨팅과 큐비트의 기본 개념

- 양자컴퓨팅에서는 정보가 큐비트(qubit)라는 최소 단위에 저장·처리됨
- 큐비트는 전자, 광자, 원자, 이온, 미세 전류 등 다양한 물리적 시스템에 구현 가능
- 전 세계 대학, 산업계, 정부는 큐비트를 정밀하게 제어하고 대규모로 결합해 신뢰성 있는 양자컴퓨터를 구축하기 위해 막대한 투자를 진행 중

○ **양자컴퓨팅의 응용 가능성과 한계**

- 양자컴퓨팅은 사이버보안, 신소재 개발, 의료 연구, 최적화 문제 해결 등에서 강력한 응용 잠재력을 보유
- 그러나 고전 컴퓨팅과 달리 정보 복제가 불가능하다는 점이 실용화의 주요 장애 요인
- 이는 양자 정보가 매우 섬세한 방식으로 저장되기 때문에 발생하

는 근본적 물리 법칙에 기인

○ **복제 불가 정리**(no-cloning theorem)의 의미

- 복제 불가 정리는 임의의 양자 상태를 동일하게 복사하는 것이 불가능함을 의미
- 고전 컴퓨팅에서 일반적인 정보 복사·공유·백업 방식이 양자컴퓨팅에서는 적용되지 않음
- 이로 인해 분산 시스템, 클라우드 저장, 장애 대비 백업 등 인프라 구축에 제약이 존재

○ 비유를 통한 양자 정보의 특성 설명

- Kempf 교수는 양자 정보의 특성을 '비밀번호 분할'에 비유
- 비밀번호의 절반씩을 각각 보유하면 단독으로는 무의미하지만, 결합 시 완전한 정보가 됨
- 개별 큐비트는 정보량이 적지만, 여러 큐비트가 결합될 때 비로소 방대한 정보가 나타남

○ 양자 얽힘과 정보 용량

- 큐비트 간 정보 공유의 핵심은 **양자 얽힘**(quantum entanglement)
- 얽힘을 통해 정보는 개별 큐비트가 아닌 시스템 전체에 분산 저장
- 예를 들어 100개의 큐비트는 동시에 2^{100} 가지 방식으로 정보를 공유할 수 있음
- 이는 현재의 모든 고전 컴퓨터로도 저장이 불가능한 정보량에 해당

○ 복제 불가 정리를 우회하는 새로운 접근

- 연구진은 양자 정보를 복제하면서 동시에 암호화하는 방법 고안
- 암호화된 상태로는 여러 복사본을 생성할 수 있음
- 이는 복제 자체를 허용하지 않는 기존 정리와 달리, 정보 접근을 제어하는 방식으로 문제를 해결

ㅇ 암호화 기반 양자 복제의 원리

- 핵심은 **‘1회용 복호화 키(one-time-use key)’** 개념
- 여러 암호화된 복사본 중 하나를 선택해 복호화하면, 해당 키는 즉시 소멸
- 따라서 하나의 복사본만 실제 정보로 복원 가능하며, 나머지는 접근 불가
- 이로 인해 물리 법칙을 위반하지 않으면서도 실질적인 백업 기능 구현 가능

ㅇ 실질적 응용: 양자 클라우드 스토리지

- 본 기술은 양자 클라우드 인프라 구축의 핵심 기반 기술로 평가
- ‘양자 드롭박스’, ‘양자 구글 드라이브’와 같은 분산 양자 저장 서비스 가능성 제시
- 동일한 양자 정보를 여러 서버에 중복·암호화 저장해 장애 대응과 보안 강화 실현

ㅇ 양자컴퓨팅 인프라 구축에의 의미

- 본 성과는 대규모 양자컴퓨팅 인프라 형성에 필수적인 기술적 진전
- 안전한 저장과 백업은 실험 단계를 넘어 실제 서비스 단계로 이동하기 위한 전제 조건
- 양자컴퓨팅의 신뢰성, 가용성, 확장성을 동시에 향상시킬 수 있음

ㅇ 연구진과 기관의 역할

- 본 연구는 Achim Kempf 교수와 Koji Yamaguchi 박사가 공동으로 수행
- Yamaguchi 박사는 연구 당시 Kempf 연구실의 박사후연구원으로, 현재는 일본 규슈대학교 조교수로 재직
- Kempf 교수는 워털루대학교 응용수학과 교수이자 양자정보·AI

분야 석좌 교수

ㅇ 워털루대학교의 양자 연구 리더십

- 본 성과는 워털루대학교의 글로벌 양자 연구 경쟁력을 다시 한번 입증
- 워털루 양자컴퓨팅연구소(IQC)는 기초 연구와 상용화를 연계하는 전략으로 국제적 명성 확보
- 현재까지 센싱・보안・컴퓨팅 분야에서 23개 이상의 양자 스타트업 창출

ㅇ 본 연구는 양자 정보가 복제 불가능하다는 오랜 제약을 암호화를 통해 실질적으로 극복

- 양자컴퓨팅의 인프라・클라우드・백업이라는 현실적 과제를 해결하는 중요한 전환점
- 양자 기술의 상용화와 대규모 시스템 구축을 앞당기는 핵심 기술로 평가됨

(원문)

1. https://thequantuminsider.com/2026/01/08/qubits-can-be-cloned-scientists-discover-first-method-to-safely-back-up-quantum-information/