

약 1만 큐비트로도 실용적 양자컴퓨터 구현 가능성 제시

(2026.04.20., 양자정보연구지원센터)

□ 캘리포니아 공과대(Caltech) Oratomic 연구팀, 약 1만 ~2만 큐비트로 실용 양자컴퓨터 구현 가능성 제시

○ 기존 수백만 큐비트 필요라는 기존 인식을 뒤집고, 오류 정정 효율화로 요구 자원 대폭 감소

○ 핵심 기술: 초고효율 양자 오류 정정 구조 개발

- 기존 약 1,000개 물리 큐비트가 1개 논리 큐비트를 구성하던 구조 개선

- 새로운 방식에서 약 5개 물리 큐비트로 1개 논리 큐비트 구현 가능

- 오류 정정 오버헤드를 2차수(order of magnitude) 수준으로 감소

○ 중성원자 기반 양자컴퓨팅 활용

- 중성원자 배열과 광집계(optical tweezers)를 이용한 큐비트 구성

- 원자 간 장거리 연결 및 재배치 가능, 높은 확장성 확보

- 6,100개 규모 큐비트 배열 실험 성공 사례 존재

○ 기술적 차별성

- 기존 표면코드(surface code) 대비 연결 구조의 자유도 증가

- 먼 거리 큐비트 간 직접 얽힘(entanglement) 가능

- 하나의 물리 큐비트가 여러 논리 연산에 참여 가능

○ 양자컴퓨터 규모 재정의

- 최소 1,000개 논리 큐비트 기준으로도 전체 시스템은 1만~2만 큐비트 수준으로 축소 가능

- 기존 100만 큐비트 필요 구조 대비 획기적 감소

- 연구 의미 및 전망
 - 기존 “수십 년 소요” 전망에서 “향후 수년 내 구현 가능” 수준으로 단축 가능성 제기
 - 10년~20년 이후로 예상되던 오류내성 양자컴퓨터 시점 앞당김
- 암호 보안 영향
 - RSA, ECC 등 현재 암호체계는 쇼어 알고리즘에 의해 해독 가능
 - 디지털 금융·통신 보안 취약성 조기 도래 가능성 경고
 - 양자내성암호(PQC)로의 전환 필요성 강조
- 물리학적 기반 및 원리
 - 양자중첩(superposition), 얽힘(entanglement) 활용
 - 양자 상태는 계산 중 오류 발생 시 쉽게 붕괴되는 취약성 존재
- 기술적 한계 및 과제
 - 대규모 시스템 통합 및 낮은 오류율 유지 필요
 - 중성원자 배열 확장 및 제어 기술 추가 발전 요구
- 산업 및 연구 협력
 - Caltech-Oratomic 협력 기반 스타트업 연계 연구
 - 오류내성 양자컴퓨터 상용화를 위한 로드맵 제시
 - 향후 교내 양자 슈퍼컴퓨터 구축 계획
- 결론
 - 오류 정정 효율 혁신으로 양자컴퓨터 실현 가능성 크게 앞당겨짐
 - 1만~2만 큐비트 수준에서 실용적 양자컴퓨팅 구현 가능성 제시

(원문)

1. <https://thequantuminsider.com/2026/03/31/research-team-finds-useful-quantum-computers-could-be-built-with-as-few-as-10000-qubits/>