RSA는 안전한가, 새로운 연구, 양자컴퓨터가 직면한 한계 주장

(2026.04.06., 양자정보연구지원센터)

□ 양자컴퓨터가 직면한 한계, RSA 안전성에 대한 새로운 연구 주장

○ Proceedings of the National Academy of Sciences에 게재된 연구는 양자컴퓨터 성능에 근본적 한계가 존재할 수 있음을 제시하며, 기존 암호체계인 RSA 암호의 안전성 유지 가능성을 주장

- Tim Palmer이 제안한 “Rational Quantum Mechanics(RaQM)” 이론 기반
- 양자역학의 수학적 기반이 연속적이 아닌 이산적 구조라는 새로운 가설 제시

○ 핵심 이론(RaQM)

- RaQM은 양자 상태를 표현하는 공간(힐베르트 공간)이 실제로는 유한한 정보 용량을 갖는 이산 구조라고 주장
- 양자 시스템이 담을 수 있는 정보량에 상한이 존재하며, 이에 따라 활용 가능한 큐비트 수 제한 발생
- 현재 기술 기준 약 200~400 큐비트, 이론적으로도 약 1,000 큐비트 수준에서 한계 도달 가능성 제시

○ 기술적 의미

- 기존 양자컴퓨팅은 큐비트 수 증가 시 지수적 상태 공간 확장을 전제로 성능 향상을 기대
- RaQM은 “큐비트 정보 용량(qubit information capacity)”이 선형적으로 증가한다고 주장
- 일정 규모 이상에서는 양자 상태를 모두 표현하지 못해 계산 이점 상실
- 대규모 얽힘(entanglement) 기반 알고리즘의 성능이 특정 규모 이상에서 정체 또는 감소 가능

○ 암호 및 산업적 영향

- 쇼어 알고리즘 기반 **RSA 해독 위협에 대한 근본적 재검토**
- 2048-bit RSA 해독에는 이론적 한계를 초과하는 큐비트 필요 →

실제 해독 불가능 가능성 제시

- QC 산업은 대규모 범용 시스템보다 제한된 규모 내 응용 중심 전략 필요

○ 적용 가능 분야

- NISQ(중간 규모 잡음 양자컴퓨터) 환경에서는 기존 양자역학과 동일한 결과 도출 가능
- 화학, 소재, 최적화 등 현재 연구 분야에서는 여전히 유효한 활용 기대
- 한계는 대규모 시스템에서만 나타나는 것으로 분석

○ **이론적 접근 방법**

- 양자 상태를 연속적 실수 아닌 유리수 기반의 유한 정보(bit string)로 표현
- 힐베르트 공간을 연속 구조에서 이산 구조로 재정의
- 중력 효과가 양자 상태 구조 결정에 중요한 역할을 한다는 가설 포함

○ **검증 방법 및 실험 방향**

- 대규모 얽힘이 필요한 알고리듬(예: 양자 푸리에 변환) 통해 검증 가능
- 큐비트 수 증가 시 성능이 정체되면 RaQM 지지 근거 확보
- 반대로 지수적 성능 향상 지속 시 이론 반증

○ 한계 및 논쟁점

- 기존 양자역학은 다양한 실험에서 이미 검증된 이론으로 RaQM은 아직 가설 단계
- 소규모 시스템에서는 기존 이론과 구별 불가 → 실험 검증 어려움
- 오류 정정(QEC)이 한계를 극복할 수 있는지 여부도 미검증

○ 수백 큐비트 수준 양자컴퓨터 발전과 함께 단기적 실험 검증 가능성 존재

- 이론이 맞을 경우 양자컴퓨팅 발전 방향 및 물리학 기본 개념 재정립 필요, 틀릴 경우 기존 양자컴퓨팅의 지수적 성능 향상 기대 유지
- 양자역학과 중력 통합 문제 해결을 위한 새로운 접근 가능성 제시

(원문)

1. https://thequantuminsider.com/2026/03/19/is-rsa-safe-new-study-argues-quantum-computers-face-a-hard-ceiling/