새 양자 아카텍처, RSA-2048 해독 하드웨어 1/10로 감소

(2026.03.04., 양자정보연구지원센터)

□ Majorana 큐비트에 저장된 정보 판독

○ 호주 시드니 소재 Iceberg Quantum 연구진이 새로운 결함 허용(fault-tolerant) 양자컴퓨팅 구조 **‘Pinnacle Architecture’를 제안**

- 해당 구조는 2048비트 RSA 정수(RSA-2048) 소인수분해에 10만 개 미만의 물리 큐비트만으로도 가능하다는 자원 추정 결과를 제시
- 기존 표면 코드(surface code) 기반 추정치(약 100만 개 이상) 대비 약 10분의 1 수준으로 하드웨어 요구량을 대폭 축소
- 연구는 arXiv에 게재, 아직 동료 심사(peer review)는 거치지 않음

○ **기존 접근법과의 차별성: QLDPC 코드 도입**

- 기존 대규모 자원 추정은 주로 ‘표면 코드(surface code)’ 기반 수행
- 표면 코드는 논리 큐비트 1개를 보호하기 위해 수백~수천 개의 물리 큐비트를 요구
- 이로 인해 RSA-2048 해독에는 약 100만 개 이상의 물리 큐비트가 필요하다는 인식이 지배적
- Pinnacle Architecture는 **양자 저밀도 패리티 검사 코드(QLDPC, Quantum Low-Density Parity-Check codes)를 채택**
- 각 큐비트가 소수의 다른 큐비트와만 상호작용하는 희소(sparse) 구조
- 복잡한 전면적(all-to-all) 연결 없이 오류 검출 가능
- 논리 큐비트당 필요한 물리 큐비트 수 줄여 전체 하드웨어 규모 축소
- (구조적 비유) 표면 코드는 격자형으로 촘촘히 연결된 배선 구조에 비유 가능(높은 신뢰성, 높은 자원 소모)
- QLDPC는 적은 연결로도 오류를 잡아내는 희소 네트워크 구조로, 하드웨어 부담이 상대적으로 낮음

○ 아키텍쳐 구성 요소

- (Pinnacle Architecture는 모듈형 구조로 설계) ‘Processing Unit (처리 유닛)’ : QLDPC 코드 블록과 측정 장치 포함
- ‘Magic Engine’ : 매 논리 사이클마다 매직 상태(magic state)를 생성·소비하는 파이프라인 구조
- ‘Memory Block(선택적)’ : 연산 자원과 저장 자원을 분리 가능
- 매직 상태 주입과 논리적 파울리(Pauli) 측정을 결합해 범용 양자 계산(universal quantum computation) 구현
- 매직 엔진은 이전 사이클에서 준비된 상태를 소비하면서 동시에 새 상태를 생성
- 처리량을 유지하면서 하드웨어 증가를 최소화
- (Clifford frame cleaning 기법 도입) 처리 유닛, 필요에 따라 결합·분리 가능
- 전체 시스템을 완전히 얽히게 하지 않고도 병렬성(selective parallelism) 확보
- 하드웨어 수와 실행 시간 간의 유연한 트레이드오프 가능

ㅇ 벤치마크 결과: 물리 및 암호 문제 적용

- 물리학 문제: 페르미-허바드(Fermi-Hubbard) 모델(16×16 격자, 256사이트)
- 물리 오류율 10^{-3} 가정 시 약 6만 2천 개 물리 큐비트 필요
- 기존 표면 코드 추정(약 94만 개) 대비 대폭 감소
- 오류율 10^{-4} 에서는 약 2만2천 개까지 감소
- 암호 문제: RSA-2048 소인수분해
- 물리 오류율 10^{-3} , 코드 사이클 1마이크로초 가정 시 10만 개 미만 물리 큐비트로 가능
- 반응 시간은 코드 사이클의 10배로 가정
- 느린 하드웨어(밀리초 단위)에서는 수백만~천만 개 수준 필요하나, 이는 실행 시간과 자원 간 교환관계 반영
- 자원 추정은 쇼어 알고리즘(Shor’s algorithm) 변형을 기반 수행
- 잔여수 체계(residue number system) 연산 활용, 레지스터 규모 축소

- 일부 소수를 병렬 처리해 실행 시간 단축

ㅇ 암호학적 함의

- **RSA-2048은 현대 공개키 암호의 핵심 방어선 중 하나**
- 대다수 전문가는 대규모 양자컴퓨터 등장 전 '양자내성암호(post-quantum cryptography)'로 전환될 것으로 예상
- 그러나 하드웨어 발전 속도는 불확실
- **10만 개 미만 물리 큐비트로 RSA-2048 해독 가능성 현실화될 경우**
- 암호학적 위험 도달 시점이 기존 예측보다 앞당겨질 수 있음
- '백만 큐비트 장벽'이 필수 조건이 아닐 수 있음을 시사

ㅇ 한계 및 향후 과제

- **수치 시뮬레이션과 이론적 컴파일에 기반,** 실제 실험적 구현은 아직 없음
- 사용된 디코딩 방식(최대우도 추정 기반)은 실시간 저지연 제어에 적합한지 검증 필요
- **매직 상태 증류(magic state distillation)**는 여전히 주요 자원 비용 요소
- 물리 오류율이 높아질수록 폐기율 증가 및 논리 깊이 증가
- 10만 개 수준이라도, 고충실도(high-fidelity) 큐비트를 마이크로초 단위 사이클로 안정화하는 것은 현재 기술(수백~수천 개 규모) 대비 여전히 큰 도전

ㅇ **Pinnacle Architecture는 QLDPC 코드, 모듈형 처리 유닛, 파이프라인식 매직 상태 생산을 결합해 대규모 양자컴퓨터 자원 추정의 패러다임을 재정의**

- RSA-2048 해독에 필요한 물리 큐비트 수를 기존 대비 약 10분의 1로 낮출 수 있음을 제시
- '유틸리티 규모(utility-scale)' 양자컴퓨팅 도달 시점에 대한 전망을 재조정하는 계기 제공

(원문)

1. https://thequantuminsider.com/2026/02/13/new-architecture-could-cut-quantum-hardware-needed-to-break-rsa-2048-by-tenfold-study-finds/