새 연구, 클라우드 양자 컴퓨터의 보안 위험 경고

(2025.09.22., 양자정보연구지원센터)

□ 새 연구, 클라우드 양자 컴퓨터의 다중 사용자 환경에서 보안 취약점 경고

○ 연구 개요

- Northwestern University 연구팀이 초전도 양자컴퓨터에서 새로운 보안 공격(QubitVise)을 실험적으로 입증
- 클라우드 기반 다중 사용자 환경에서 한 사용자가 다른 사용자의 계산 결과를 의도적으로 왜곡 가능함을 확인
- 기존 단일 방향 간섭 연구를 넘어 양방향(double-sided) 공격을 제시하여 위험성 확대

○ 공격 방식

- 핵심 취약점: **CNOT 게이트 사용 시 발생하는 crosstalk(누설 잡음)**
- 공격자는 다수의 CNOT 게이트를 활용한 회로를 피해자 회로 주변에 배치 → 출력 결과를 교란
- 특권 권한 불필요, 일반 사용자 수준에서 실행 가능
- 공격 회로는 합법적인 알고리즘(QAOA 등)과 유사해 탐지·차단이 어려움

○ 실험 및 결과 (Rigetti Ankaa-3, Amazon Braket)

- 공격 회로: 18개의 CNOT 게이트 활용
- 피해 회로: Bell state, 4-큐빗 Ising, 6-큐빗 GHZ 등
- 총 1,000회 반복 실행하여 통계적 분포 비교
- 총변동거리(TVD) 기준 평균 13% 이상 오류 증가, 최대 35% 이상
- 일부 사례(2-큐빗 Bell)에서는 223%까지 증가 → 신뢰성 심각 저해 가능성 확인

ㅇ 의미와 파급효과

- 데이터 절취는 불가능하나, 연산 결과 조작 위험 존재
- 신약 개발, 금융, 암호 분야 등 고부가가치 계산에서 신뢰성 약화 우려
- 고성능·대규모 양자 시스템 상용화 시 피해 가능성 확대
- 기존 고전 컴퓨터 공격(Rowhammer, 캐시 타이밍 누출 등)과 유사한 물리적 부작용 기반 공격

ㅇ 연구팀 제언

- 클라우드 양자 환경의 보안 강화 필요
- 다중 사용자 동시 실행 시 회로 배치 규제 강화
- 공격 패턴 자동 탐지, crosstalk 감소를 위한 하드웨어 설계 개선
- 보안·신뢰성 확보가 상용화의 핵심 과제로 부각

ㅇ 결론

- 클라우드 기반 다중 사용자 양자컴퓨터에서 하드웨어 수준의 보안 위협이 실제로 발생할 수 있음을 보여줌
- QubitVise 공격은 데이터 절취가 아니라 결과 왜곡을 통해 신뢰성을 무너뜨린다는 점에서 산업적 활용에 심각한 장애가 될 수 있음
- 특히 대규모 양자 연산이 요구되는 신약 개발, 금융, 암호 분야에서는 작은 오류도 큰 피해로 이어질 수 있음
- 회로 배치 규제, 공격 패턴 탐지, 하드웨어 설계 개선 등 보안 중심의 인프라 강화가 시급함
- 궁극적으로는 다중 사용자 환경에서 신뢰성과 안정성을 보장할 수 있는 보안 아키텍처 확립이 상용화를 위한 핵심 과제임

(원문)

1. https://thequantuminsider.com/2025/08/18/new-study-warns-of-security-risks-in-cloud-quantum-computers/