양자 하드웨어가 드러낸 새로운 보안 취약성 경고

(2026.01.22., 양자정보연구지원센터)

□ **펜실베니아주립대 연구진, 양자 하드웨어가 새로운 보안 취약점을 드러낸다고 보고**

○ 펜실베이니아주립대(Penn State) 연구진은 IEEE 논문을 통해 현재의 양자컴퓨팅 시스템이 예상보다 훨씬 심각한 보안 취약성에 노출되어 있음을 경고함

- 양자컴퓨터의 하드웨어, 소프트웨어, 클라우드 기반 운용 구조 깊숙이 보안 위험이 이미 내재
- 조작, 지식재산 탈취, 결과 왜곡 및 '조용한 사보타주(silent sabotage)' 가능성 제기
- 기존 사용자와 개발자들이 이러한 위협을 충분히 인식하지 못하고 있다는 점을 핵심 문제로 지적

○ 양자컴퓨팅의 특성과 보안 취약성의 근원

- 연구진은 양자컴퓨터의 장점 자체가 새로운 공격 표면을 만든다고 분석
- 클라우드 기반 공유 접근 구조
- 서드파티 도구 및 컴파일러에 대한 높은 의존도
- **지속적인 보정(calibration) 필요성**
- 데이터가 아닌 회로 구조 자체에 민감한 정보가 포함되는 특성
- 이로 인해 공격자가 명확한 흔적 없이 결과를 왜곡하거나 정보를 유출할 가능성 존재

○ 기존 보안 체계의 한계

- 고전 컴퓨팅에서 사용되는 보안 기법은 양자 시스템에 그대로 적

용 불가

- 양자 시스템은 근본적으로 다른 물리적 동작 원리를 가짐
- 현재 상용 양자 제공업체들은 주로 신뢰성과 성능 확보에 집중
- 회로 토폴로지, 인코딩된 데이터, 하드웨어에 내재된 지식재산 등 '양자 고유 자산'은 종단 간 보호가 거의 부재

○ 양자컴퓨팅 상용화 초기 단계의 위험성

- 양자컴퓨팅은 실험실 단계를 넘어 초기 상용 활용 단계에 진입
- 주요 IT 기업들이 실제 양자 하드웨어를 클라우드로 제공
- 정부와 산업계에서 최적화, 화학, 금융, 머신러닝 적용을 시험 중
- 보안 사고는 미래 문제가 아니라 현재 NISQ(잡음 중간 규모 양자) 시스템에 이미 적용되는 문제

○ **회로 구조에 내재된 정보 유출 위험**

- 양자 알고리즘은 회로 구조 자체가 민감 정보를 포함
- 고전 알고리즘은 입력 데이터에 정보가 집중되지만, 양자 알고리즘은 회로 패턴이 문제의 구조를 드러냄
- QAOA, VQE 같은 변분 알고리즘은 문제 크기, 제약 조건, 변수 간 관계를 회로에서 추론 가능
- 공격자는 데이터 접근 없이도 포트폴리오 최적화, 전력망 구조, 독점 모델 정보를 유추할 수 있음

○ **새로운 지식재산(IP) 위협**

- 양자 프로그램 자체가 결과 이전 단계에서도 고부가가치 자산이 됨
- 회로 복사, 역공학, 변조에 대한 보호 장치가 미흡
- 이는 기존 소프트웨어 보안 개념과는 다른 차원의 위험

ㅇ 컴파일러 및 서드파티 도구의 위험

- 양자 컴파일은 극도로 민감한 과정
- 게이트 순서, 타이밍, 큐비트 배치의 미세한 변화가 결과 품질에 큰 영향
- 외부 컴파일러 사용이 증가하면서 악성 변경, 성능 저하, 정보 유출 가능성 확대
- 확률적 출력 특성으로 인해 기존 테스트 방식으로 악의적 조작 탐지 어려움

ㅇ **클라우드 기반 공유 환경의 공격 경로**

- 다중 사용자(multi-tenant) 환경은 양자 시스템에 새로운 간섭 가능성 제공
- 큐비트 간 크로스토크로 인해 한 사용자의 작업이 다른 작업에 물리적 영향을 미침
- 공격자는 인접 작업의 수렴 속도를 늦추거나 출력 왜곡 가능
- 초전도 시스템에서는 swap 연산 증가, 이온 트랩에서는 이온 이동 증가로 성능 저하 유발

ㅇ **하드웨어 및 보정(calibration) 취약성**

- 양자 시스템은 정밀한 아날로그 제어 신호에 의존
- 제어 전자장치(FPGA 등)의 미세한 오류가 출력 분포에 큰 영향
- 보정 서비스가 조작되거나 잘못 보고될 경우 사용자는 이를 검증할 수단이 거의 없음
- 큐비트 품질 편차와 자원 할당 불투명성도 결과 신뢰성을 약화

ㅇ **사후 검증 불가능성의 위험**

- 많은 양자 계산 결과는 고전적으로 검증 불가
- 결과를 완전히 망가뜨리지 않고도 확률 분포를 편향시키는 공격 가능

- 금융, 물류, 인프라 의사결정에 미묘하지만 치명적인 영향 가능
- 고전 컴퓨팅의 재계산·체크섬 기반 보안과 근본적으로 다름

ㅇ 산업적·정책적 시사점
- 보안은 양자컴퓨팅의 '사후 옵션'이 될 수 없음
- 하드웨어, 회로, 시스템, 클라우드 오케스트레이션 전반에 보안 내재화 필요
- 회로 스크램블링, 정보 인코딩, 하드웨어 격리, 역할 기반 접근 제어 요구
- 양자 노이즈를 고려한 새로운 검증·감시 기법 필요

ㅇ 연구의 한계와 향후 과제
- 본 연구는 개별 공격의 실증이 아닌 종합적 위험 분석
- 일부 공격은 실제 환경에서 구현이 어려울 수 있음
- 그러나 물리적·구조적 취약성은 시스템 확장과 함께 지속될 가능성 큼
- 양자 보안 전용 연구 커뮤니티 구축 필요성 제기

ㅇ 본 연구는 양자컴퓨팅이 기술적으로 성숙해질수록 보안 취약성도 함께 확대됨을 경고
- 양자 보안은 고전 보안의 연장 아닌, 새로운 물리 기반 접근 필요
- 국가 안보, 산업 경쟁력, 신뢰 가능한 양자 활용을 위해 조기 대응이 필수
- 연구진은 수학·컴퓨터과학·공학·물리학을 아우르는 양자 보안 연구의 본격화를 촉구함

(원문)

1. https://thequantuminsider.com/2026/01/13/penn-state-researchers-report-quantum-hardware-exposes-new-security-vulnerabilities/