

# 양자 컴퓨터가 온다, 양자 소프트웨어는

(2021.10.26., 양자정보연구지원센터)

## □ 양자 소프트웨어(툴, 알고리즘, 프로그래밍 언어 및 응용 프로그램)

### ○ 양자 소프트웨어 필요성

- 큐비트 및 양자 컴퓨팅 지원하는 하드웨어 기술 개발과 함께 소프트웨어 구성 요소 개발 필요
- 현재 소프트웨어는 양자 컴퓨터에 적용되지 않으므로, 새로운 소프트웨어 만들어야 함
- 양자 장치로 작업하기 위해 프로그래밍 언어, 컴파일러, 테스트 프로그램 및 최적화 도구 측면에서 다양한 솔루션 필요

### ○ 양자 컴퓨터를 위한 프로그래밍 언어 개발

- Rigetti(양자 프로그램 작성 및 실행 환경인 Forest), IBM (Qiskit, Quantum Information Software Kit), Microsoft(양자 개발 키트, QDK), Google(Cirq), Xanadu(광자기반 양자컴퓨터 Strawberry, Blackbird)
- 기타 하드웨어 공급업체와 협력, 자체 양자 소프트웨어 생태계 및 프로그래밍 언어(Q-CTRL, Zapata Computing 등) 개발

### ○ CQC(Cambridge Quantum Computing) 개발 플랫폼

- 양자 개발 플랫폼(tket<sup>TM</sup>) 개발, 클라이언트와 파트너가 서로 다른 양자 장치에서 소프트웨어 사용 및 여러 플랫폼에서 작업 가능
- 알고리즘 최적화하여 길이와 지속시간을 줄임, 현재 NISQ 컴퓨터 고유의 노이즈 및 오류 문제에 유용하며 계산 결과 향상됨

## □ 양자 컴퓨팅의 놀라운 기술

### ○ 고전 컴퓨터와 다른 점

- 양자 역학을 기반으로 하는 양자 컴퓨터는 중첩(양자 물체가 동시에 여러 상태로 존재)과 얽힘(두 입자가 서로 분리되어 있어도

동기화되어 있음)을 사용

- 고전 컴퓨터가 0 또는 1이 되는 비트를 사용한다면, 양자컴퓨터는 큐비트 사이의 얽힘과 중첩 관련된 확률로 많은 양의 데이터를 빠르게 처리
- 구축 기술 면에서 시스템의 간섭이나 노이즈가 중첩 특성에 영향을 미치므로, 양자 컴퓨터는 당분간 절대 영도(100mK) 가까운 온도에서 실행

○ 양자 컴퓨터 필요성

- 최적화 문제에서 분자 구조 시뮬레이션 및 모델링
- 화학 산업(신소재 개발 가능성), 핀테크(포트폴리오 최적화), 물류 및 자동차 산업(교통 최적화 및 배터리 개선), 제약(신약 개발) 및 방어(사이버 보안)
- 몇 년 안에 양자 컴퓨터가 대부분 인터넷 사이트 암호화를 깨트릴 수 있으며, 사이버 보안 및 암호화에서 전체 데이터 보안 구조 재구성해야 함

○ 경쟁 우위

- 양자 컴퓨팅 분야는 하드웨어 구성 요소, 소프트웨어, 응용 프로그램, 양자 감지 및 보안 같은 다양한 측면 다루는 주요 업체 및 신생 기업과 함께 지속적 발전
- 전 세계 명문대학은 양자 정보 기술의 잠재력과 미래 가능한 응용 프로그램 탐구를 위한 연구 프로젝트 수행
- 'Quantum ready' 깨지지 않는 암호화 시스템 보유 및 양자 컴퓨팅의 엄청난 잠재력 이해

(원문)

1. <https://www.supertrends.com/what-about-quantum-software/>
2. <https://www.supertrends.com/quantum-computing-is-no-black-magic/>