3

양자 컴퓨팅이 가져올 혁신

글 | 실비 바락(Sylvie Barak)

2023년은 양자 컴퓨팅에 있어서 이정표로 기억될 것이다. 획기적인 혁신들이 기술적 판도를 바꿔놓고 우리가 복잡한 문제를 풀고 정보를 처리하는 방식을 혁신할 것으로 기대된다. IBM의 획기적인 양자 칩에서부터 스핀파(spin wave) 조작, 분자 구조 시뮬레이션, 양자 통신에 관한 선구적 시험들에 이르기까지, 양자 컴퓨팅의 지형이 일대 변혁을 거치고 있다. 이것이 기술의 미래를 재정의할 것이다.

양자 컴퓨팅이 이론적 탐구에서 실제 구현으로 옮겨감에 따라서 이제는 본격적으로 개발에 박차를 가해야 할 때가 되었다. 이 여정에 장애물이 없는 것은 아니나, 과학자, 엔지니어, 업계 리더들이 협력하는 움직임이 두드러지고 있다. 이것은 양자 컴퓨팅이 제약에서부터 통신에 이르기까지 우리 삶의 모든 영역에서 핵심적인 역할을 하는 미래로 나아가는 길을 놓을 것이다.

IBM이 세운 양자 컴퓨팅 이정표

지난 해에 이룩된 다양한 양자 컴퓨팅 혁신 중에서도 IBM의 최근 진보는 양자 기술이 어떻게 빠르게 진화하고 있으며 실용화 수준을 높이고 있는지 잘 보여준다. IBM은 양자 활용에 있어서 새 시대를 열어젖혔으며, 양자 컴퓨팅의 능력과 응용을 한 단계 끌어올리는 중요한 이정표를 세웠다.

IBM이 최근에 발표한 Condor 프로세서는 양자 컴퓨팅에 있어서 기념비적인 도약을 의미하는 것으로서, 1,121개 초전도 큐비트를 처리함으로써 1,000 큐비트 장벽을 돌파했으며 IBM의 교차 공명 게이트 기술을 선보임으로써 양자 칩 제조에 있어서 규모, 수율, 설계 한계를 끌어올렸다. Condor 프로세서는 큐비트 밀도를 50퍼센트 높이고 단일 희석 냉각기로 1마일이 넘는 고밀도 극저온 플렉스 IO 배선을 특징으로 하는 것으로서, 미래 하드웨어 설계를 위한 등불을 밝히고 있다. IBM의 이전 433 큐비트 Osprey 프로세서에 버금가는 성능을 제공하고, 중요한 확장성 문제를 해결한다.

더불어, IBM은 ibm_torino 양자 시스템으로 Quantum Heron 프로세서를 도입했다. 이 프로세서는 133 정주파수 큐비트와 튜닝가능 커플러를 특징으로 한다. 이 개발은 이전의 플래그쉽 127 큐비트 Eagle 프로세서와 비교해서 3~5배 더 우수한 디바이스 성능을 제공하고 누화를 거의 제거한다. Heron 프로세서는 4년에 걸친 연구개발의 성과로서, IBM의 하드웨어 로드맵에 있어서 주춧돌이자 양자 프로세서 기술에 있어서 한 걸음 큰 진전을 의미한다.

뿐만 아니라, IBM의 Quantum System Two는 확장가능 양자 연산을 위해서 설계된 것으로서, 극저온 인프라와 첨단 제어 전자장치 및 고전적 런타임 서버를 결합했다. 이 시스템이 앞으로 십년에 걸쳐서 확장가능 양자 연산을 위한 발판을 마련할 것으로 기대된다. 이 시스템은 3개 IBM Quantum Heron 프로세서를 채택하고 모듈러 아키텍처를 구현함으로써 양자 중심적 수퍼컴퓨팅으로 병렬 회로 실행을 가능하게 한다.

회로 니팅(circuit knitting) 같은 툴을 사용해서 양자 연산을 응용할 수 있는 영역들이 늘어나고 다중 양자 회로 용으로 새로운 알고리즘들이 등장함에 따라서 IBM의 접근법은 이종 컴퓨팅 아키텍처를 향하고 있다. 이것은 양자 중심적 수퍼컴퓨팅을 실현하고 유틸리티급 양자 애플리케이션으로 가기 위한 길을 열 것이다.

스핀파: 새로운 개척 지대

IBM 같은 기업들의 기술 개발 노력과 더불어, 학계도 양자 기술의 진보를 위해서 힘쓰고 있다. 대학과 연구 기관들이 양자 컴퓨팅에 있어서 큰 걸음을 내딛고 있다. 획기적인 시험과 발견들로 이 분야에 활기를 불어넣고 있다. 그러한 한 예로 델프트 공과대학의 스핀파에 관한 선구적인 연구를 들 수 있다.

이 대학에서 실시한 혁신적인 시험에서 양자 물리학자들은 초전도체를 사용한 칩 상으로 스핀파를 제어하고 조작하는 데에 성공했다.

스핀파는 자기 소재로 발견되는 정보 전달 파로서, 양자 컴퓨팅 같은 에너지 효율적 기술을 위한 초석을 놓을 것으로 오래 전부터 여겨져 왔다. 이 새로운 개발은 이 파를 사용해서 양자 컴퓨터의 장치들을 연결하거나 에너지 효율적 정보 기술을 개발할 수 있는 새로운 가능성들을 제시한다.

이 시험은 이색적인 접근법으로 스핀파가 자기장을 생성해서 초전도체로 하여금 초전류를 발생시키도록 했다. 초전류가 미러로 작용해서 자기장을 다시 스핀파로 반사시킴으로써 이 파의 움직임을 좀더 정밀하게 제어할 수 있도록 한다.

이 연구는 스핀파와 초전도체를 결합한 디바이스를 설계할 수 있는 길을 제시한다. 이러한 디바이스는 최소한의 열과 음파를 발생시킴으로써 휴대전화 회로에 사용되는 주파수 필터나 공진기 같은 부품을 개발할 수 있도록 한다. 좀더 중요하게는, 이 기술을 활용해서 양자 컴퓨터로 큐비트들을 연결할 수 있다.

분자 구조와 양자 시뮬레이션

양자 컴퓨팅과 관련해서 학계 주도의 또 다른 흥미로운 연구로는 양자 컴퓨팅을 활용해서 원자 차원에서 분자 구조를 시뮬레이션하는 것을 들 수 있다. 이것은 배터리, 제약, 비료 개발 같은 다양한 화학 기반 영역을 혁신할 것으로 기대된다. 양자 컴퓨터를 활용해서 분자 상호작용을 정확하게 시뮬레이션함으로써 좀더 효율적이고 효과적인 제품을 설계할 수 있다.

좀더 최근에는 프린스턴 대학의 물리학자 팀이 개별 분자들을 얽히게 해서 분자들이 거리에 상관없이 상관성을 유지하는 양자 상태를 생성하는 데에 성공했다. 양자 얽힘(quantum entanglement)은, 입자 쌍 혹은 집단의 입자들이 서로 거리가 상당히 떨어져 있음에도 불구하고, 각기 입자의 양자 상태를 다른 입자의 상태와 별개로 설명할 수 없는 방식으로 상호작용하는 양자 역학의 한 현상을 말한다. 양자 얽힘은 양자 컴퓨팅의 진보를 위해서 중요한 것으로서, 이 발견은 양자 컴퓨터의 실제 응용을 위해서 중요한 의미를 갖는다. 그 복잡성 때문에 분자를 사용해서 제어 가능한 양자 얽힘을 달성하는 것이 오랜 과제였다. 프린스턴 팀은 정교한 트위저 어레이 시스템을 사용해서 개별 분자들을 얽힘 상태로 조작할 수 있었다. 이 기법은 양자 과학을 위한 토대로서 분자의 타당성을 입증하는 것이다. 특히 양자 정보 처리와 복합 소재 시뮬레이션에 있어서 그렇다.

쇼어 알고리즘: 인수 분해에 있어서 양자 도약

물론 양자 컴퓨팅이 미칠 수 있는 영역은 미시적 세계를 훨씬 뛰어넘는다. 자연의 기본 요소를 시뮬레이션하는 것에서 암호화 보안을 전면적으로 재정의하는 것으로 도약할 수 있다는 것은 양자 기술의 범용적인 능력을 보여주며 우리를 쇼어 알고리즘(Shor's algorithm)의 진보로 이끈다.

1994년에 MIT의 수학자인 피터 쇼어가 소인수를 구하는 것을 극히 빠르게 할 수 있는 양자 알고리즘을 고안했다. 소인수 분해는 인터넷 통신에 사용되는 데이터 암호화 기법의 핵심적인 요소이다. 쇼어 알고리즘은 큰 수를 고전 알고리즘보다 기하급수적으로 더 빠르게 인수분해할 수 있는 양자 알고리즘으로서, 꾸준히 주목을 받아왔으며 수십년 동안 양자 컴퓨터의 잠재력을 입증하는 증거물로 여겨져 왔다. 이 알고리즘은 양자 컴퓨팅이 고전 컴퓨터로는 현실적으로 풀기 어려운 문제를 풀 수 있는 잠재력이 있음을 시사한다. 예를 들면 특정한 암호화 시스템을 해독하는 것을 들 수 있다.

그런데 최근에 뉴욕 대학의 오데드 레게브(Oded Regev)가 새로운 양자 알고리즘을 내놓았다. 이 알고리즘은 효율에 있어서 쇼어의 기법을 능가할 것으로 기대된다.

레게브 알고리즘은 arXiv 서버에 게시된 프리프린트(출판

전 논문)에서 자세히 설명하고 있는데, 큰 수를 인수분해하기 위해서 좀더 효율적인 접근법을 제안하고 있다. 그러므로 더 적은 양자 게이트를 필요로 한다. 이 진보는 더 소형의 양자 컴퓨터를 사용해서 암호화 키를 깨거나 아니면 대형 컴퓨터를 사용해서 암호화 키를 좀더 빠르게 디코딩하는 것을 가능하게 한다. 이 알고리즘은 쇼어 알고리즘으로부터 30년 만에 처음으로 대대적인 향상을 이루는 것으로서, 필요한 게이트 수를 n-비트 정수로 n2에서 n1.5로 줄이도록 한다.

이 새로운 알고리즘은 양자 컴퓨팅 커뮤니티로부터 주목을 받고 있으며, MIT의 비노드 바이쿤타나탄(Vinod Vaikuntanathan)이나 듀크 대학의 케네스 브라운(Kenneth Brown) 같은 전문가들이 이 알고리즘의 잠재적인 영향력을 인정하고 있다. 하지만 레게브의 기법 역시도 과제들을 제기한다. 특히 양자 메모리 요구량에 있어서 그렇다. 이 요구량이 알고리즘의 전반적인 비용을 증가시킬 수 있다.

물론 양자 컴퓨팅이 계속해서 진보함에 따라서 인터넷 암호화가 래티스 암호화 같은 양자 내성 기법으로 전환할 수 있을 것이다. 그럼에도 불구하고 과거에 기록된 인터넷 트래픽을 암호해독 하는 것과 같은 애플리케이션에 레게브 알고리즘이나 쇼어 알고리즘 같은 알고리즘을 여전히 사용할 수 있다. 아마도 무엇보다 중요한 점으로서, 레게브 연구의 참신성은 양자 암호화로 추가적인 혁신을 이루도록 영감을 불어넣는 역할을 할 수 있을 것이다. 이 분야는 많은 중대한 혁신 가능성을 품고 있다.

프로세서 벤치마크를 넘어: 초점의 변화

양자 컴퓨팅 분야로 최근에 두드러지는 또 다른 중요한 경향은 프로세서 벤치마크를 강조하는 것에서 실제 구현에 초점을 맞추는 것으로 변화가 일고 있다는 것이다. 이러한 전환은 양자 컴퓨팅을 이론적 개념에서 실제 애플리케이션으로 기술을 응용하는 것으로 변화시킬 것이다. 2023년 프로젝트들에 대한 최근의 분석을 보면, 2035년에 자동차, 화학, 금융 서비스, 생명 과학 같은 산업들로 양자 컴퓨팅으로 인한 경제적 파급력이 최대 1조3천억 달러에 이를 것으로 전망된다.

양자 컴퓨터의 잠재력을 최대한 활용하기 위해서는 단지 개별적인 양자 알고리즘을 개발하는 것을 넘어서 광범위한 애플리케이션 연구에 초점을 맞추는 것이 필요하다. 이 연구를 위해서는 진정으로 양자 솔루션이 빛을 발할 수 있는 애플리케이션들을 발굴하고 이러한 기술을 기존 컴퓨팅 워크플로우로 통합해야 한다. 이 작업은 결코 만만치 않으며, 양자 정보 과학자, 분야 전문가들, 기업 리더들을 비롯해서 다양한 영역에 걸친 협력이 필요할 것이다. 또 한편으로는 현행 양자 컴퓨터의 한계를 극복하고 사양과 일정이 어떻게 될지 모르는 미래의 애플리케이션에 대비하는 것이 필요할 것이다.

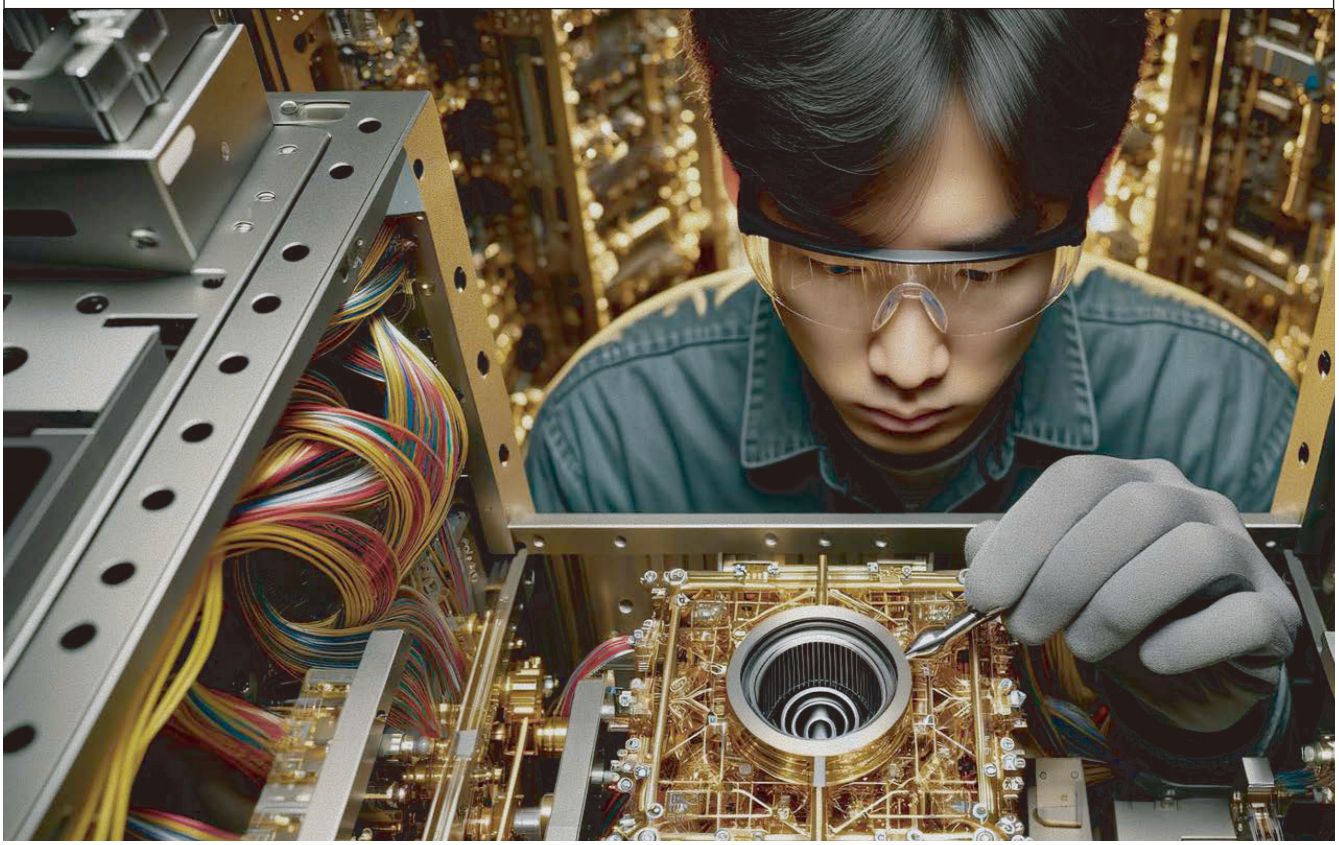
이 과정을 위해서는 그에 필요로 하는 역량과 지식을 쌓아야 한다. 이 여정은 여러 해가 걸릴 수도 있다. 다영역에 걸친 가파른 학습 곡선이 필요할 것이기 때문이다. 양자 컴퓨팅을 기존 워크플로우로 통합하기 위해서 필요한 기술들을 개발해야 할 것이며, 애플리케이션 연구가 계속해서 양자 산업을 견인하는 역할을 할 것이다.

양자 모듈화(quantum modularization)

아키텍처에 있어서도 초기의 장벽들이 무너지고 있다. 양자 모듈화가 대규모 양자 컴퓨터 개발에 있어서 변화를 몰고 오는 새로운 트렌드로 부상하고 있다.

양자 모듈화는 양자 컴퓨팅에 있어서 중요한 진보를 뜻하는 것으로서, 확장 가능하고 유연한 아키텍처를 가능하게 한다. 이것은 비용적으로 효과적인 업그레이드를 가능하게 하고 시스템 접근성을 높일 것이다. 이 개념은 전통적 컴퓨팅의 모듈러 혁신으로부터 영감을 얻은 것으로서, 양자 기술로 회복탄력성, 맞춤화, 보안을 높이도록 한다. 기업들이 양자 시스템을 특정한 필요에 따라서 맞춤화할 수 있도록 하므로, 시스템을 전면적으로 변경할 필요 없이 다양한 애플리케이션을 최적화할 수 있다. 모듈러 디자인은 또한, 이온 트랩과 초전도 양자 컴퓨터 같은 각기 다른 양자 기술들 간에 상호운용을 가능하게 한다. 그러므로 특정 작업들에 가장 적합한 기술을 선택할 수 있다.

결정적으로, 모듈화는 선별적인 수리와 업그레이드를 가능하게 하므로 양자 시스템의 근본적인 취약성(fragility)을 해결할 수 있으며 중단 시간과 유지보수 비용을 낮추도록 한다. 사이버 보안을 높이는 것에 있어서도 중요한 역할을 한다. 사설 클라우드 액세스와, 데이터 침해를 방어하기 위한 보안적



모듈 링펜싱을 가능하게 한다. 모듈러 양자 컴퓨팅으로의 전환은 개별 요소에 초점을 맞춤으로써 연구개발 노력을 능률화할 뿐만 아니라, 양자 네트워킹을 위한 길을 놓는다. 양자 네트워킹은 양자 프로세싱 유닛들을 상호연결하고 협력적으로 작동함으로써 이전에 볼 수 없던 컴퓨팅 성능을 달성하도록 할 것이다. 양자 컴퓨팅 산업이 진보함에 따라서 모듈러 시스템의 실제 구현이 판도를 바꾸고 전세계 기업들이 양자 기술을 좀더 쉽게 접근하고 활용할 수 있도록 할 것이다.

양자 통신의 진보

양자는 통신에 있어서도 물결을 일으키고 있다. 양자 통신에 있어서 최근의 진보는 양자 원리를 활용해서 데이터를 보안적으로 전송하기 위한 기법들을 크게 향상시키고 있다. 이 측면에서 주목할 만한 성취로서 해저 광섬유 케이블을 통해서 양자 통신을 시연한 것을 들 수 있다. 이 개발은 euNetworks Fiber UK가 이끈 것으로서, 224킬로미터의 Rockabill 해저 네트워크를 통해서 영국과 아일랜드 사이에 양자 링크를 구축하는 데에 성공했다. 이것은 양자 통신에 있어서 중대한 전환점을 이루는 것으로서, 긴 거리에 걸쳐서 혹독한 조건으로 보안적인 데이터 전송의 한계를 끌어올리게 되었다.

양자 정보 텔레포테이션(teleportation)

또 다른 혁신적인 진보는 Micius 위성을 통해서 1,200킬로미터가 넘는 거리로 양자 정보 텔레포테이션을 할 수 있게 되었다는 것이다. 이 개발은 양자 통신이 전통적 통신 기법의 능력을 훨씬 뛰어 넘는 엄청난 거리에 걸쳐서 작동할 수 있는 잠재력이 있다는 것을 보여준다.

마이크로칩들 간에 양자 비트 전송

긴 거리에서부터 아주 짧은 거리에 이르기까지, 서식스 대학과 Universal Quantum은 양자 컴퓨터 마이크로칩들 간에 양자 비트(큐비트)를 전송하는 것에 있어서 진전을 이루었다. 이 개발은 양자 컴퓨팅의 실제 구현을 위해서 중요한 것으로서, 다중의 양자 시스템을 통합하는 것을 가능하게 하고 양자 네트워크의 확장성을 높일 것이다.

양자 통신의 한 가지 중요한 측면은 근본적으로 도청에 대해서 보안적이라는 것이다. 빛 입자(광자)가 광 케이블을 통해서 고도로 취약한 상태로 데이터를 전송하기 때문에, 데이

터를 조작하거나 훔치려고 하는 시도가 있으면 입자들이 붕괴된다. 이 점은 은행 계좌 정보 같은 민감한 정보를 보안적으로 전송하고자 할 때 특히 중요하다. 이 점에서 양자 통신은 데이터 전송을 보호하기 위한 견고한 솔루션을 제공한다.

양자 네트워킹의 협력적 혁신

양자가 되었든 다른 무엇이 되었든, 양호한 통신은 무엇보다도 중요하다. 2023년에 학계와 기업이 손을 잡고 양자를 한 걸음 진보시키게 되었다. Amazon Web Services(AWS)는 하버드 대학과 협력해서 양자 네트워킹으로 혁신을 이룸으로써 고전 텔레콤 네트워크의 속도와 효율을 높이게 되었다. 이 연구진은 광섬유를 패키징하는 새로운 기법을 개발함으로써, 거리에 걸쳐서 데이터가 저하되는 오랜 문제를 해결하게 되었다. 이 기법은 광섬유의 가늘어지는 끝과 양자 리피터 같은 디바이스들을 연결함으로써, 빛을 점증적이고도 안정적으로 전송하도록 한다. 인터페이스가 트래픽 잡음으로 인해서 발생되는 것과 같은 미미한 변위에 대해서 내성이 있으므로 실제 애플리케이션에 사용하기에 적합하다.

AWS의 이 혁신은 극저온으로 효과적일 뿐만 아니라 고속 텔레콤 네트워크에 사용되는 변조기와 통합할 수도 있다. 이 호환성은 양자 하드웨어와 고전 하드웨어 사이에 좀 더 효율적인 인터페이스를 향해서 한 걸음 나아갔음을 뜻하는 것으로서, 양자 컴퓨터 및 네트워크가 폭넓게 도입되도록 하는 길을 놓을 것이다.

향상된 오류 교정 기법들

하지만 혁신이 있는 곳에는 오류 또한 따른다. 양자 컴퓨팅 분야가 힘써온 사안 중의 하나가 향상된 오류 교정 기법을 개발하는 것이었다. 양자 컴퓨터는 민감한 특성 때문에 오류를 일으키기 쉬우므로, 신뢰성과 실용적인 응용을 위해서 견고한 오류 교정 기법이 꼭 필요하다. RIKEN 양자 컴퓨팅 센터의 연구자들은 오류 교정에 머신 러닝(ML)을 적용함으로써 이 측면에서 큰 진전을 이루고 있다. 이들이 개발한 자율 교정 시스템은, 비록 근사치이기는 하나, 오류를 교정하기 위한 가장 좋은 방법을 효율적으로 결정할 수 있다. 이 시스템은 ML을 활용해서, 디바이스 오버헤드를 최소화하면서 효과적인 오류 교정 성능을 유지하는 오류 교정 방법을 탐색한다.

이 연구진은 양자 오류 교정을 위해서 자율식 접근법에 초점을 맞춤으로써, 특수하게 설계된 인공 환경이 빈번한 오류 검출 측정을 필요 없게 한다. 이 접근법은 보소닉 큐비트 인코딩(bosonic qubit encoding)에 특히 접합하다. 보소닉 큐비트 인코딩은 초전도 회로를 기반으로 한 몇몇 장래성 높은 양자 컴퓨팅 머신에 사용되는 것으로서, 양자 컴퓨팅의 거대한 탐색 공간에서 이루어지는 복잡한 최적화 작업이다. 이 팀은 강화 학습을 사용해서 이 문제를 해결하게 되었다. 강화 학습은 진화된 ML 기법으로서, 에이전트가 환경을 탐사해서 조치 정책을 학습하고 최적화한다.

더욱이 이 연구진은 놀랍도록 간단한 근사치 큐비트 인코딩이 여타 인코딩에 비해서 디바이스 복잡성을 크게 낮출 수 있다는 것을 발견했다. 간단한 이 인코딩이 오류 교정 능력에 있어서 경쟁자들을 능가했다. 이 발견이 중요한 것은, 덜 복잡한 양자 컴퓨팅 머신이 오류 교정에 있어서 고도로 효과적일 수 있다는 것을 시사하기 때문이다. 이것은 양자 컴퓨팅을 좀더 접근하기 쉽고 실용적이도록 만들 것이다.

Google Quantum AI의 연구자들 역시도 양자 오류 교정에 있어서 중대한 혁신을 이루었다. 이들은 양자 오류 교정에 사용되는 큐비트 수를 늘림으로써 연산 오류 비율을 낮출 수 있다는 것을 확인했다.

맺음말

이렇듯이 2023년은 연구자들이 중요한 성취를 이루고 새로운 트렌드들이 부상하면서 양자 컴퓨팅에 있어서 중요한 한 해로 기억될 것이다. 이러한 개발들은 양자 컴퓨팅이 어떻게 빠르게 진보하고 있는지 보여줄 뿐만 아니라, 가까운 미래에 양자 컴퓨팅이 다양한 분야로 근본적인 영향을 미칠 수 있음을 알려준다. SN