https://www.qcenter.kr

Q REPORT

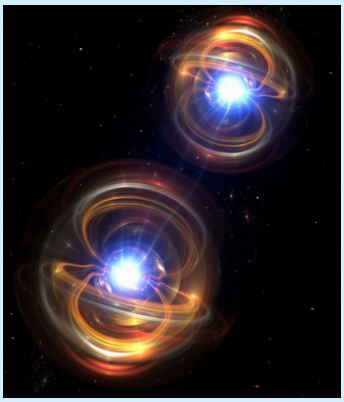
양자정보과학 리포트

양자 인터넷

양자정보연구지원센터
Quantum Information Research Support Center

Q REPORT
양자정보과학 리포트

양자 인터넷 CONTENTS



[들어가는 말]

최근 양자 컴퓨터가 발전함에 따라 양자 인터넷에 대한 관심이 증가하고 있다. 현대 사회에서 인터넷은 우리의 일상에 중요한 기술이 되었고, 인터넷을 통한 분산 (클라우드) 시스템은 한정된 자원의 성능을 높이는데 유용하게 사용되고 있다. 양자 인터넷은 양자 통신, 양자 센싱, 양자 컴퓨터 등 양자정보과학기술 간의 네트워킹 기술로 현재의 디지털 인터넷과 함께 사용되어 정보의 보안성을 높이고(초고신뢰), 분산 클라우드 양자 컴퓨팅(초고속 연산), 양자 센싱(초정밀 계측)이 가능한 차세대 혁신기술로 연구가 진행 중이다. 이러한 양자 인터넷이 구축된다면, 금융, 의료, 공공 부문에서 뿐만 아니라 천문학, 신소재 및 생명공학 분야에서 방대한 양의 연산 및 대규모 감지 실험을 신속하게 수행할 수 있을 것으로 기대된다.

본문에서는 양자 인터넷의 정의 및 개발 단계, 양자 인터넷 활용으로 기대되는 (양자) 보안 통신과 양자 계산(컴퓨팅)에 대해 살펴보고, 양자 인터넷 구축을 위한 국내외 연구 동향에 대해 간략하게 소개 하고자 한다.


Q REPORT
양자정보과학 리포트

CHAPTER

1장 양자 인터넷

일반적으로 네트워크는 하나 이상의 컴퓨터를 연결하는 것이고, 인터넷은 전 세계 컴퓨터를 연결하는 컴퓨터 사이의 관계임. 인터넷(Interconnected Network)은 TCP/IP 프로토콜 단위를 사용하여 전 세계의 다양한 유형의 전기 장치를 연결하는 글로벌 시스템으로, 네트워크의 한 종류이며 네트워크의 네트워크라고 불림. 양자 인터넷은 양자 기기(양자 컴퓨터와 보안 통신을 위한 기구)간 연결을 통해 양자 기술의 집약체라 할 수 있음.

1-1. 양자 인터넷 정의

가. 양자 인터넷

현재 인터넷 기술은 0과 1 각각의 비트(bits)에 정보를 실어 보내지만, 양자 인터넷은 0과 1이 중첩된 임의 양자 상태의 광자에 정보를 담아 전송하며, 이러한 양자정보 단위를 큐비트(qubits)라 함. 정보의 양이 증가할수록 전송 속도가 느려지는 현재 인터넷과 달리 양자 인터넷은 정보량이 많아져도 속도가 거의 줄어들지 않아 꿈의 인터넷으로 불리고 있으며, 전 세계적으로 관심이 증가하고 있음. 양자 정보를 전송하는 양자 인터넷은 초고속 인터넷의 보안 버전이 아니며, 기존 컴퓨터를 연결하는 고전 채널의 전파뿐 아니라 양자 채널을 사용하여 정보를 연결하고 배포할 수 있게 함으로써 현재의 인터넷과 근본적으로 다르게 작동함. 즉, 정보와 양자 자원을 분배하는 양자 네트워크를 통해 양자 컴퓨터, 시뮬레이터 및 센서를 상호 연결하여 작동함.

양자 인터넷은 양자 역학의 특성을 활용한 일부 양자 장치가 정보를 교환할 수 있도록 하는 네트워크로, 고전 채널이 아닌 양자 채널을 통해 큐비트를 전송하고, 미시세계 입자의 “양자 상태(quantum state)"를 효과적으로 활용하는 것을 의미함.
양자 정보에서 데이터는 큐비트 상태로 인코딩될 수 있으며, 양자 컴퓨터나 양자 프로세서와 같은 양자 장치에서 생성될 수 있음. 간단히 말해서, 양자 인터넷은 물리적으로 분리된 여러 양자 장치의 네트워크를 통해 큐비트를 보내는 것을 포함하며, 중첩, 얽힘, 간섭 등 양자 상태에서만 볼 수 있는 고유한 특성에 의해 일어남.

양자 인터넷은 양자의 고유한 속성 중 하나인 얽힘(entanglement)을 활용하여 두 장치 간 상호 통신하며, 양자 통신에서 얽힘은 실제 전송 중에 두 큐비트를 연결하는 물리적 채널이 없이도, 일부 정보를 한 큐비트에서 다른 큐비트로 순간이동(teleportation) 시킬 수 있음. 두 큐비트가 상호 작용하고 얽히게 되면, 그들은 서로 의존하는 속성을 공유하게 됨. 큐비트가 얽힌 상태의 두 입자 중 한 입자의 양자 상태가 바뀌면 물리적으로 멀리 떨어진 다른 입자의 양자 상태도 동시에 바뀌게 됨. 따라서 첫 번째 큐비트 상태는 얽힌 상대의 동작을 보고 읽을 수 있음. 알버트 아인슈타인은 이를 가리켜 "원거리에서 으스스한 행동(spooky action at a distance")라고 함. 얽힌 큐비트는 광섬유 네트워크를 통해 이동할 수 있지만, 100㎞까지 얽힘을 유지할 수 없으며, 전 세계적으로 얽힘 네트워크 구축이라는 거대한 엔지니어링 과제가 남아있음.

순간이동(teleportation)

- 두 입자간 얽힘을 이용하여 아주 먼거리에서 물리적 연결없이 서로 정보를 공유. 이를 통해 사용자 간 데이터의 순간 이동이 가능함. 분산된 얽힘 쌍을 사용하여, 큐비트 상태를 전송할 수 있음

양자 얽힘을 통해 개별 양자 장치를 서로 연결하면, 수천 큐비트 가치가 있는 클러스터가 생성될 수 있음. 이러한 컴퓨팅의 강점을 만드는 것이 실제 양자 인터넷 프로젝트의 궁극적인 목표임. 많은 양자 장치를 연결함으로써, 양자 인터넷은 현재 단일 양자 컴퓨터에서 달성할 수 없는 문제 해결을 시작할 수 있으며, 고전 컴퓨터로는 처리할 수 없는 특정 문제를 단일 양자 컴퓨터를 연결한 양자 인터넷을 통해 연결함으로써 해결할 수 있음.

우리는 이미 인터넷 클라우드 상에서, Amazon AWS Braket, Microsoft Azure, D-wave, IonQ 및 IBM을 통해 많은 실험적인 양자 컴퓨터와 통신하여 양자 알고리즘을 구축하고 테스트하거나 시뮬레이터를 사용할 수 있음. 하지만 양자 컴퓨터의 출력을 공유하는 것과 양자 컴퓨터를 연결하는 것은 별개의 문제임. 양자 컴퓨터의 내부를 연결해서 고성능 양자 컴퓨터를 효과적으로 만들 수 있음. 즉, 파동함수를 붕괴시키지 않고 컴퓨터 내부 상태(얽힘)를 분산시키는 것으로 양자 컴퓨터를 확장할 수 있음.

나. 양자 인터넷 개발

양자 인터넷을 구축하기 위해서는 큐비트를 보내는 양자 컴퓨터 구축 방법을 기능적으로 이해할 필요가 있음. 궁극적으로 안정적인 큐비트(생성, 유지 및 전송)와 양자 컴퓨터는 완전한 기능의 양자 네트워크를 구축하기 위한 핵심 기술이며, 양자 인터넷을 실현하기 위해서는 더 많은 인프라가 필요함.

양자 인터넷의 주요 요소로는 큐비트를 저장하고 연산을 수행할 양자 프로세서, 큐비트를 전송할 양자 통신 채널, 네트워크상에서 큐비트를 보내기 위해 경로를 구성하는 스위치, 양자 리피터, 양자 정보의 도청 방지를 위한 양자 얽힘, 오류정정부호로 구성됨.

양자 인터넷은 아래 세 가지 필수 양자 하드웨어 요소로 구성됨.

첫째, 큐비트 전송을 지원하는 물리적 연결인 양자 채널(quantum channel)이 필요함. 양자 채널은 고전적 정보뿐만 아니라 큐비트의 상태인 양자 정보를 전송할 수 있는 통신 채널로서, 양자 정보를 전달하기 위한 파이프라인으로 간주됨. 그 예로는 현재 고전적인 빛을 전달하는 데 사용되는 표준 통신용 광섬유가 있음.

둘째, 광섬유와 같은 전송매체 기반의 양자채널은 고유한 신호 손실이 있으므로 장거리 통신에 어려우며, 짧은 전송거리를 확장할 수단이 필요함. 고전 통신에서 전송 중 신호 증폭을 위해 증폭기를 사용하지만, 양자 네트워크에서 큐비트는 복사할 수 없으므로 증폭기를 사용할 수 없음. 따라서, 원거리 통신을 위해 양자 리피터(quantum repeater)라는 중간 노드가 필요함.

양자 상태는 환경 잡음에 매우 민감하기 때문에, 양자 얽힘은 제한된 거리에서만 가능하며, 양자 리피터는 얽힘을 장거리로 확장할 수 있는 방법을 제공함.

마지막으로 양자 인터넷에 연결된 양자 프로세서로 종단 노드(end node)가 필요함. 단일 큐비트만 준비하고 측정할 수 있는 매우 단순한 노드에서 대규모 양자 컴퓨터에 이르기까지 다양하며, 양자 인터넷은 고전적 통신을 대체하기 위한 것이 아니라 양자 통신을 보완하기 위한 것임.

[그림 1]
양자 인터넷 개발 단계

출처: Wehner et al,.(2018)

양자 인터넷의 개발 단계

기능적 양자 컴퓨터를 노드로 양자 통신 채널을 통해 연결하는 본격적인 양자 인터넷은 아직 멀었지만, 최초의 장거리 양자 네트워크는 연구 개발 중임. 미래 양자 인터넷을 위한 정확한 물리적 구성 요소를 예측하기는 어렵지만, 양자 인터넷 구축을 위해 양자 중계기와 종단 노드를 구현하기 위한 실질적인 개발이 필요함.
[그림 1]은 2018년 네델란드 QuTech사에서 제시한 양자 인터넷 실현을 위한 여섯 단계의 과정을 기능성 증가를 특징으로 제시하고 있음.

1) 신뢰할 수 있는 중계기 네트워크(Trusted repeater networks)

첫 번째 단계는 큐비트의 종단 간(end-to-end) 전송을 허용하지 않음. 기반 기술이 발전함에 따라 리피터는 향후 진정한 양자 중계기로 업그레이드될 수 있음. 특히, 신뢰할 수 있는 중계기 네트워크(신뢰할 수 있는 노드 네트워크라고도 함)에는 적어도 두 개의 종단 노드와 가까운 중간 중계기 노드를 연결하는 일련의 단거리 링크가 있음. 인접 노드의 각 쌍은 QKD를 사용하여 암호화 키를 교환함. 이러한 네트워크를 업그레이드하기 위한 첫 번째 단계는 측정 장치 독립적인 QKD(Measurement device-independent QKD)일 수 있음.

2) 네트워크 준비 및 측정(Prepare and measure)

이 단계는 종단 간 양자 기능을 제공하는 첫 번째 단계임. 중간 리피터 노드를 신뢰할 필요 없이 종단 간 QKD를 가능하게 하고 다른 작업을 위한 프로토콜 호스트를 허용함. 최종 사용자는 양자 상태를 수신하고 측정함(그러나 얽힘의 양자 현상이 반드시 수반되는 것은 아님). 두 명의 최종 사용자는 자신만 알고 있는 개인 키를 공유할 수 있으며, 사용자는 비밀번호를 공개하지 않고도 비밀번호를 확인할 수 있음.

3) 얽힘 생성 네트워크(Entanglement generation)

세 번째 단계는 종단 간 양자얽힘 생성을 허용함. 이 단계에서 종단 노드는 양자 메모리가 필요하지 않으며, 장치 독립적 프로토콜(device-independent protocols)을 실현할 수 있음. 모든 최종 사용자는 얽힌 상태를 얻을 수 있으며, 이들은 가능한 가장 강력한 양자 암호화를 제공함.

4) 양자 메모리 네트워크(Quantum memory networks)

네 번째 단계는 종단 노드가 로컬 메모리를 보유하는 동시에 보편적인 로컬 제어를 허용하는 기능으로 구별됨. 이를 통해 양자 또는 고전 통신을 수행하는 중에 양자 상태를 임시로 저장해야 하는 훨씬 더 복잡한 프로토콜을 구현할 수 있음. 임의의 최종 사용자는 얽힌 큐비트(정보의 양자 단위)를 획득 및 저장하고 서로 순간이동할 수 있음. 네트워크는 클라우드 양자 컴퓨팅을 가능하게 함.

5) 소수 큐비트 내결함성 네트워크(Few-qubit fault tolerant networks)

다음 단계는 로컬 작업을 내결함성으로 수행할 수 있어야 하며, 내결함성 작업을 사용하면 높은 회로 깊이(depth)의 로컬 양자 계산을 실행할 수 있을 뿐만 아니라, (이론적으로) 임의의 프로토콜을 실행하기 위한 저장 시간의 임의 확장이 가능함. 여기에는 분산 양자 컴퓨팅과 몇 개 큐비트로 제한된 본격적인 양자 컴퓨팅 네트워크용 응용이 포함됨. 데이터 전송 시 오류 수정이 가능한 본격적인 양자 컴퓨터가 네트워크 장비로 사용됨. 이러한 단계는 실험을 통해 다양한 수준의 분산 양자 컴퓨팅 및 양자 센서를 가능하게 함. 이 단계에서는 몇 개의 큐비트만 포함될 수 있음.

6) 양자 컴퓨팅 네트워크(Quantum computing networks)

최종 단계는 임의의 시스템 간 양자 통신이 가능한 양자 컴퓨터 네트워크로 구성됨. 기존 컴퓨터에서 더 이상 효율적으로 찾을 수 없는 계산 문제에 대한 솔루션을 찾을 수 있음. 더 많은 양의 큐비트가 포함될 수 있음.

1-2. 양자 인터넷 활용

양자 인터넷은 기존 컴퓨터가 가질 수 없는 고유한 속성을 가지고 있음. 첫번째, 얽힘을 사용하여 원거리에서 상태를 완벽하게 조정할 수 있음. 예를 들면, 전 세계 어디에서나 두 개의 시계를 완벽하게 동기화할 수 있음. 두번째, 양자 연결은 본질적으로 통신에 사용하기에 안전함. 두 큐비트가 완전히 얽혀 있으면 이 연결을 중간에 가로채는 것은 불가능함. 양자 인터넷은 얽힘 특성을 통해 보안과 개인 정보 보호가 필요한 다양한 응용 프로그램에 적합함.

양자 인터넷이 어느 분야에서 가장 큰 영향을 미칠 것인지, 가장 관련성 높은 세 가지 기회의 영역을 다음과 같이 제시함.

분산 양자 컴퓨팅(Distributed quantum computing)

- 고전 컴퓨터의 성능은 그것이 포함된 CPU(중앙 처리 장치) 수에 대략 비례하지만, 양자 컴퓨터를 네트워킹하여 양자 인터넷을 구축하면 분자 시뮬레이션과 같은 더 크고 복잡한 문제를 해결하여 신약 개발 및 새로운 재료를 설계할 수 있음

보안 통신(secure communications)

- 큐비트는 측정하는 순간 양자 상태가 바뀌므로, 양자 인터넷 상에서 전송되는 데이터는 고전 인터넷에서와 같이 광범위한 도청 공격에 영향을 받지 않음. 양자 인터넷은 기밀 의료 기록의 전송에서 금융 거래에 이르기까지 해킹이 불가능한 보안 통신의 잠재력을 보유하고 있음

양자 센싱(quantum sensing)

- 양자 센싱은 훨씬 더 정확하고 민감한 측정을 제공할 뿐만 아니라, 이전에 측정이 어려웠던 현상들을 측정할 수 있는 기회를 제공함. 예를 들어, 양자 센서는 지구 표면 아래에서 이전에 감지되기 힘들었던 활동을 원격으로 관찰, 분석 및 측정하여 화산 폭발 및 지진과 같은 위협에 대한 조기 경보 시스템을 개선할 수 있음

기타 다양한 응용으로 클라우드에서 보안 양자 컴퓨팅(Secure quantum computing in the cloud), 양자 강화 측정 네트워크(Quantum-enhanced measurement networks), 고정밀-장거리 망원경(Higher-precision, long-baseline telescopes)을 고려할 수 있음.

가. 보안통신(secure communication)

양자 통신은 넓은 의미에서 0과 1이 중첩되어 있는 양자 상태를 송신부에서 수신부로 전송하는 모든 기술을 말함. 양자 통신의 경우 전송되는 정보를 중간에 도청하게 되면, 수신자는 도청자의 존재를 즉각 인식하게 되고 통신을 중단한 후 상황에 맞는 적절한 대처를 하게 됨. 이는 보안상 장점이 되며, 이러한 특성을 암호키 전송에 응용하여 양자암호라 부름. 보안 통신을 위해 사용되는 고전 인터넷과 양자 인터넷에서의 암호화 방법에 대해 제시함.

고전 인터넷 암호화, 공개 키 암호화

현재 많은 통신이 공개 키 암호화(비대칭 암호화)를 통해 보호되지만, 암호화 표준(대칭 암호화 유형)은 오늘날에도 여전히 사용됨. 공개 키 암호화는 개인 키와 공개적으로 사용 가능하고 자유롭게 공유되는 키와 함께 작동됨. 현재 도청자가 개인 키를 손에 넣을 수 있는 경우에만 암호화를 깨뜨릴 수 있고, 도청자가 소인수분해 방법을 사용하여 공개 키에서 개인 키를 얻을 수 있음.

1) 고전적인 포스트 퀀텀 암호화 (classical post-quantum cryptography)

기존 인터넷을 통한 정보 교환에 의존하는 새로운 암호화 기술 개발.

양자 내성(quantum-proof) 또는 양자 저항(quantum-resistant) 암호화라고도 하며, 가능한 솔루션 중 하나는 대칭 키를 사용하는 것임. 그로버 알고리즘을 실행하는 양자 컴퓨터는 이 대칭 키를 파괴할 수 있지만, 키의 크기를 늘리면 양자 내성이 생길 것으로 예상됨. 양자 컴퓨터에 대해 안전할 것으로 여겨지는 공개 키 암호화 시스템의 다른 예로는 격자 기반(lattice-based) 암호, 해시 기반(hash-based) 암호, 코드 기반(code-based) 암호, 다중 변수(multi-variant) 암호 및 초특이 등원 기반(supersingular isogeny-based) 암호가 있음.

2) 양자 키 분배 (quantum key distribution)

암호화 키 생성을 위해 양자 인터넷을 사용하는 것.

1984년 컴퓨터 과학자 C. Bennet과 G. Brassard는 양자역학을 사용하여 키를 안전하게 분배하는 체계를 발명함. 양자 키 분배에서 양자 네트워크를 통해 암호화 키를 만들고, 이를 기존 인터넷으로 보냄. 양자 키 분배는 큰 소수의 인수분해에 의존하지 않기 때문에, 양자 컴퓨터에서 실행되는 쇼어 알고리즘이나 소인수분해를 위한 다른 빠른 알고리즘에 의해 깨질 수 없음.

양자 인터넷 암호화

양자 인터넷 암호화에서 양자 암호키 분배는 일반적으로 광자(빛의 단일 입자)를 사용하며, 프로토콜 구성 방법에 따라 준비 및 판독 기법과 얽힘 기반 기법의 두 가지 유형이 있음.

1) 준비 및 판독(preparation and read out)

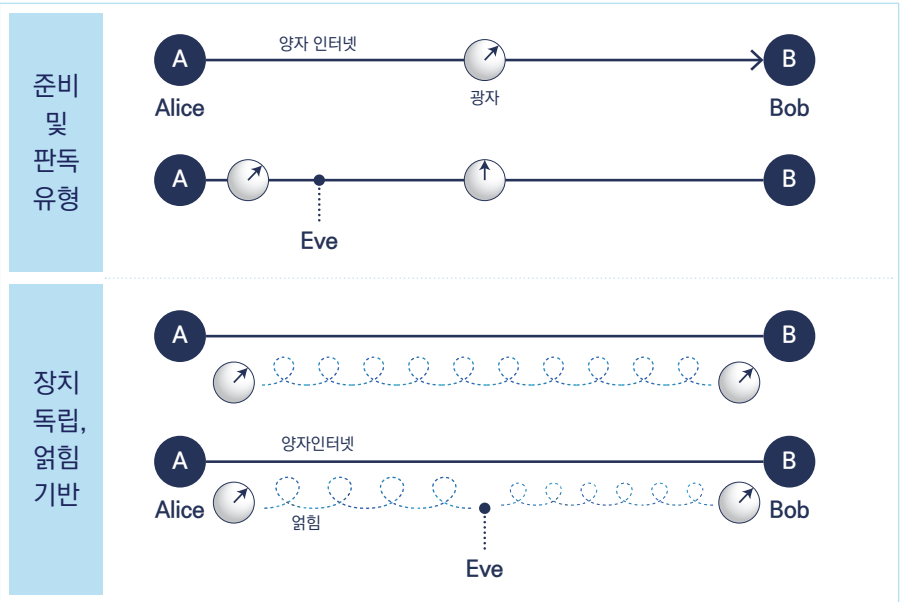
A(Alice)는 특정 상태에서 광자를 준비하고 양자 인터넷 통해 B(Bob)에게 보냄. B(Bob)는 준비된 상태 결정을 위해 광자를 측정함. 이러한 방식으로 Alice와 Bob은 키를 교환함. 만약 Eve(도청자)가 키를 손에 넣기 위해 광자를 측정한다면 광자의 상태가 변하고, 이 변화는 Alice와 Bob이 감지할 수 있음. 따라서 Alice와 Bob은 키를 교환하는 동안 도청 여부를 알 수 있고, 키가 손상되었는지 결정할 수 있음. 손상된 키는 폐기하고, 감지되지 않은 교환에서 생성된 키만 선택해서 보관함(이러한 방식으로 안전하게 키를 교환함).

2) 장치 독립적, 얽힘 기반(device independent, entanglement-based)

A(Alice)와 B(Bob)은 각각 큐비트를 가지고 있음. 이후, 양자 네트워크를 통해 보내는 광자를 사용하여 큐비트 간 얽힘을 설정함. A(Alice)와 B(Bob) 사이의 큐비트 간 얽힘을 사용하여 키를 분배할 수 있음. A(Alice)와 B(Bob)은 큐비트에 대한 측정을 수행하고 이 정보를 공유함.

만약 Eve가 도청을 시도하면, A(Alice)와 B(Bob)의 큐비트 사이의 얽힘을 줄일 것이고, A(Alice)와 B(Bob)은 이를 다시 감지함. 따라서 교환된 키의 손상 여부를 판단할 수 있음(얽힘으로 인해 안전 판단).

[그림 2]
양자 인터넷 암호화 유형



출처: TuDelft

양자 암호화

암호화는 데이터를 암호화하거나 일반 텍스트를 스크램블 텍스트로 변환하여 올바른 키(key)를 가진 사람만 읽을 수 있도록 하는 프로세스임. 양자 암호화는 양자역학의 원리를 사용하여 데이터를 암호화하고 해킹할 수 없는 방식으로 전송함.

양자 암호 이면의 양자역학 원리의 복잡성이 있으며, 이 원칙들은 양자 암호가 작동하는 방식에 중요한 역할을 함.

- 양자 속성을 변경하거나 방해하지 않고는 양자 속성을 측정할 수 없음
- 입자의 일부 양자 속성은 복제할 수 있지만, 전체 입자는 복제할 수 없음

포스트 양자 암호화 vs. 양자 암호화

포스트 양자 암호화(post-quantum cryptography)는 양자 컴퓨터의 공격에 안전하다고 생각되는 암호화 알고리즘(일반적으로 공개키 알고리즘). 양자 암호화(quantum cryptography)는 양자 역학 원리를 사용하여 보안 메시지를 전송하며, 수학적 암호화와 달리 물리적 암호화로 해킹이 불가능함.

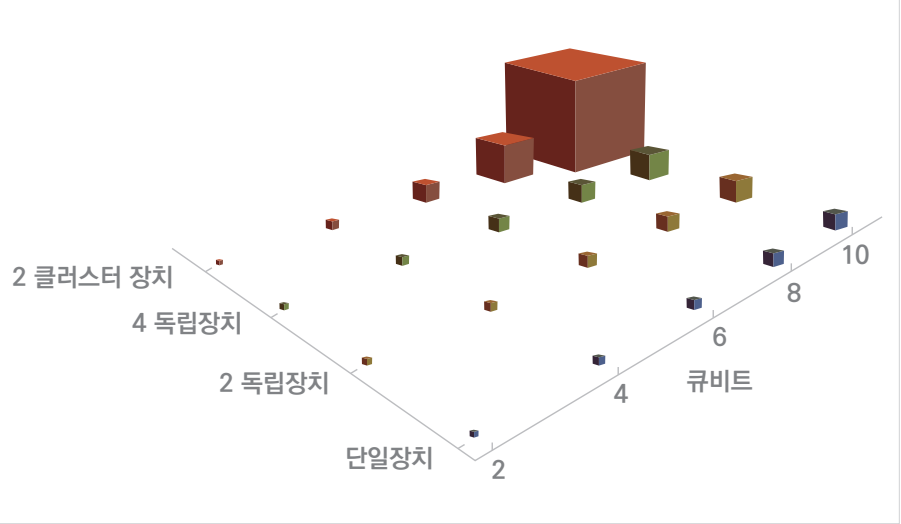
나. 분산 양자 컴퓨팅(Distributed quantum computing)

양자 상태는 환경과의 상호작용으로 깨지기 쉽고, 결잃음(decoherence)이라는 과정을 통해 양자 속성에 손상을 일으켜 컴퓨팅 오류의 원인이 됨. 대규모 연산 문제를 해결할 만큼 충분히 큰 양자 컴퓨터를 구축하는 것은 오류 수정에 많은 물리적 큐비트가 추가로 필요하므로 현재 기술력으로 구현에 어려움이 있음.

양자 역학을 기반으로 한 양자 컴퓨팅에서 큐비트는 양자 계산의 핵심 구성 요소로, 전자 스핀, 편광, 초전도 회로와 같은 다양한 기술로 실현될 수 있음. 양자 컴퓨터의 계산 능력은 상호 연결될 수 있는 큐비트의 수에 의해 결정되므로, 큐비트가 추가될수록 양자 컴퓨팅 성능은 기하급수적으로 향상됨.

만약 "실시간(live)" 큐비트를 연결할 수 있다면, 양자 컴퓨터를 연결함으로써 대규모 양자 컴퓨터로 확장할 수 있음. 원격 노드 간 양자 상태를 공유할 수 있는 네트워크를 통해 여러 대의 양자 컴퓨터를 상호 연결할 수 있는 양자 인터넷이 필요함.

[그림 3]
양자 클라우드 컴퓨팅
속도 향상



출처 : M. Caleffi et al.,(2018)

예를 들어, 두 개의 분리된 10큐비트 양자 컴퓨팅 장치는 중첩 원리에 의해 2^{10} 상태를 나타낼 수 있으며, 단순히 더하면 한 번에 2×2^{10} 상태를 나타냄. 그러나 이 두 양자 컴퓨팅 장치를 양자 인터넷으로 연결하면 [그림 3]과 같이, 결과 클러스터는 기하급수적인 계산 속도 향상과 함께 최대 2^{18} 상태를 나타낼 수 있음.

기존 데이터 센터는 특수 양자 컴퓨팅 장비를 호스팅하기에 좋은 후보로, 기업과 개인 사용자는 클라우드를 통해 양자 컴퓨팅 서비스(QCaaS, Quantum Computing as a Service)에 액세스 할수 있음. IBM은 이미 전 세계 연구원들에게 5, 7, 16, 27 및 127큐비트 양자 장치에 대한 클라우드 액세스를 제공하여 양자 알고리즘 설계를 허용하고 있음. 클라우드 양자 컴퓨팅 서비스를 통해 인터넷 상에서 많은 실험적인 양자 컴퓨터와 통신할 수 있으며, AWS Braket을 사용하여 다양한 양자 프로세서(D-wave, IonQ 또는 Rigetti)에서 양자 알고리즘 구축하고 테스트하거나 시뮬레이터를 사용하고 있음.

얽힘 특성으로 인해 입자에 대한 모든 동작은 다른 입자에도 즉시 영향을 미치며, 입자들이 서로 멀리 떨어져 있을 때에도 유지됨. 얽힘은 복제 불가 정리(no-cloning theorem)와 측정 원리(Measurement)를 위반하지 않고 큐비트를 전송하는 중요한 도구를 제공하며, 소스와 대상 간 공유되는 얽힌 큐비트 쌍으로 두 원격 양자 장치 간에 알려지지 않은 양자 상태를 "전송"하는 것이 가능함.

이 과정을 양자 순간 이동(teleportation)이라고 함. 원본 측정의 출력이 고전 채널을 통해 수신되면 원래 큐비트가 대상에서 재구성됨. 이러한 양자 순간 이동은 여러 원격 양자 장치에 위치한 큐비트 간 작업을 수행해야 하는 분산 양자 컴퓨팅의 핵심 전략임. 결과적으로 여러 양자 장치를 상호 연결하면 [그림 3]과 같이 계산 속도가 기하급수적으로 향상됨.

복제 불가 정리(no-cloning theorem)

- 양자 상태의 복사본을 만들 수 없으며 큐비트도 복사할 수 없음. 신호를 증폭하고 전송하는 것 또한 다른 방식으로 해야 하므로, 양자 정보 전송에 어려움이 있음

측정(Measurement)

- 측정은 양자 중첩상태를 붕괴하고, 모든 큐비트를 1 또는 0과 같은 일반 고전 비트로 전환함

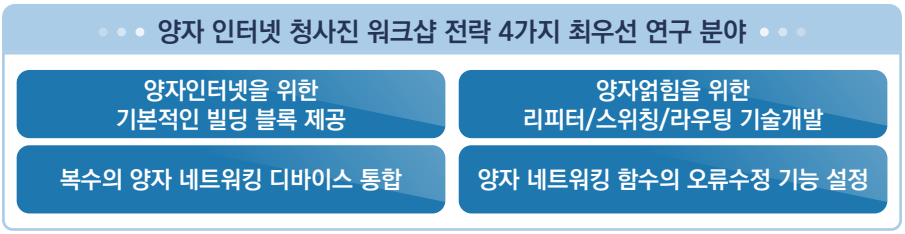
CHAPTER
2장 국내외 양자 인터넷 연구 동향

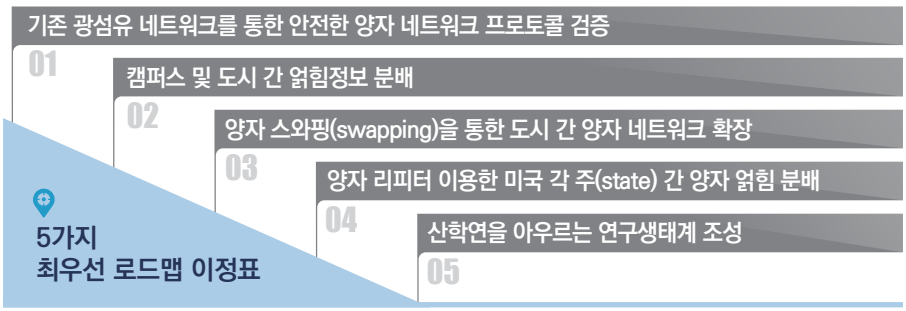
2-1. 국가기관 단위

■ 미국

국가 양자 인터넷(National quantum Internet)을 실현하기 위한 단계별 전략 제시, 양자 중계기 네트워크 구축

- 장거리 얽힘에서 전국적인 양자 인터넷 구축까지. 2020년 2월, 미 에너지부는 최초 전국적 양자 인터넷 구축을 위한 잠재적 로드맵 정의하는 양자 인터넷 청사진 워크숍(Quantum Internet Blueprint workshop)을 주최함





- 2019년 4월, 미 에너지부의 브룩헤이븐 국립 연구소, 스토니브룩 대학 및 DoE 에너지 과학 네트워크(ESNET) 협력체는 휴대용 양자 얽힘 소스와 기존 DoE 광섬유 통신망을 사용하여 18㎞ 장거리 얽힘 달성, 이후 80마일 양자 네트워크 테스트베드 구축함
- 2020년 2월, 아르곤 국립 연구소는 페르미랩에 연결된 52마일 "양자 루프" 얽힘 분포 네트워크를 만들어 3-노드(Argonne, Fermilab 및 Univ. of Chicago) 80마일 양자 통신을 위한 테스트베드 구축

■ 유럽연합(EU)

양자인터넷 전략 수립. 2018년 양자 인터넷 연합 결성(Quantum Internet Alliance)

- 2019년 1월, 광섬유 통해 50㎞ 이상 얽힘 입증
- QuTech 연구소에서 만든 중간 노드를 통해 전달된 양자 정보와 함께, 3개 양자 프로세서 연결하는 최초 네트워크를 성공하였음

■ 중국

위성으로 인한 얽힘 기록 경신. 745마일 기록을 갱신한 QKD 달성

- 2016년, 세계 최초 양자 통신 위성 '묵자(Micius)'호 발사, 중국 베이징과 오스트리아 빈까지 무선 양자 통신 위성(7,600km) 전송 실험 성공 , 미래 양자 인터넷의 중요한 단계
- 베이징과 상하이 사이 세계 최장 거리 2,000km 지상 기반 양자 암호통신 백본망 구축
- 2017년, 안후이성 허페이 세계 최대 양자 연구소 설립 추진
- 2019년 6월, 1,200㎞ 거리에 위성-가능 광자 얽힘 구축(Messier 2019)

2-2. 기업 단위

■ QuTech

지구 상 임의의 두 장소 간 양자 통신 가능케 한 기술 개발

- 델프트(Delft) 헤이그(Hague) 라이덴(Leiden) 및 암스테르담(Amsterdam) 도시 사이 최초의 실제 양자 네트워크 구축. 2022년 가동 실행. ARPANET의 양자 버전

■ Quantum Xchange

QKD 기술 사용. 미국 최초 양자 네트워크 개발 노력

- 미 동부 해안 따라 약 800㎞ 광섬유 케이블 확보. 보스턴에서 워싱턴 DC까지 네트워크 구축. 2018년 11월부터 운영

■ ID Quantique와 SK Broadbnad 협업

- 정부 통신을 확보할 전국 규모의 양자 네트워크가 한국에서 구축 중임
- 양자암호통신(QKD) 시범 인프라 구축 및 운영 사업(디지털 뉴딜의 일부)으로 2020년 보안이 필수적인 17개 구간에 QKD 구축

참고문헌

1. H. J. Kimble (2008). The quantum Internet. Nature, 453(19), 1023-1030

2. S. Wehner, D. Elkouss, R. Hanson (2018). Quantum Internet: A vision for the road ahead. Science, 362(303), 1-9.

3. M. Caleffi, A. S . Cacciapuoti, G. Bianchi (2018). Quantum Internet : from Communication to Distributed Computing. NANOCOM '18

4. Brooks, M. (2019). Beyond quantum supremacy: the hunt for useful quantum computers. Nature, 574(7776), 19-22.

5. D. Castelvecchi (2018). the Entangled Web. Nature, 554, 289-291

6. Quantum Internet Blueprint Workshop (2020). From Long-distance Entanglement to Building a Nationwide Quantum Internet. Report of the DOE

7. D. Castelvecchi (2018). The quantum internet has arrived (and it hasn't). Nature, 554, 289-292

8. R. P. Feynman (1982). Simulating Physics with Computers. International Journal of Teoretical Physics, 21(6), 467-488

9. P. P. Rohde (2021). The Quantum Internet: the second quantum revolution, Cambridge University Press

10. R. V. Meter (2012). Quantum Networking and Internetworking, IEEE Network, 26(4), 59-64

11. S. L. N. Hermans (2022). Qubit teleportation between non-neighbouring nodes in a quantum network, Nature, 605, 663-668

12. 노광석, 허준 (2021). 양자인터넷 연구 동향. 2021년도 한국통신학회 하계종합학술발표회, 630-631

⓭ 배광일, 이은주, 심규석, 이원혁 (2021). 양자 네트워크 연구개발 동향 분석. 2021년도 한국통신학회 하계종합학술발표회, 384-385

⓮ 배준우 (2022). 양자 인터넷의 이해. 한국정보화진흥원(NIA), 5-26

Q REPORT
양자정보과학 리포트

양자 인터넷

필 자 | **임 주 은** 양자정보연구지원센터 연구원
발행일 | 2022.10.24.
발행처 | 성균관대학교 양자정보연구지원센터
16419 경기도 수원시 장안구 서부로 2066
https://www.qcenter.kr