1. 정의 및 필요성

A. 양자 컴퓨팅의 정의

양자 컴퓨팅(Quantum Computing)는 양자역학에서 다루는 매우 작은 원소들의 행동 특성을 이용하여 정보를 가공하기 위한 컴퓨팅 방법입니다. 기존의 컴퓨팅 방법과는 다른 형태의 컴퓨팅 방법인데, 가장 큰 차이점으로는 비트의 상태입니다. 기존의 컴퓨팅에서는 비트의 상태가 0과 1만 사용하여 계산을 했다면, 양자 컴퓨터는 0과 1 그리고 0과 1이 동시에 될 수 있는 중첩(Superposition)의 상태가 있습니다. 이것을 양자컴퓨팅에서는 큐비트(Qubits)라고 합니다.

큐비트 외에도 기존의 컴퓨팅 방식과 다른 양자 컴퓨팅의 핵심 개념으로써 중첩, 양자얽힘, 양자 간섭(Quantum Interference)이 있습니다.

큐비트(Qubits): 양자 정보의 단위로써 0, 1, 또는 그 둘의 중첩 상태가 될 수 있습니다.

중첩(Superposition): 큐비트가 여러 상태(0과 1)에 동시에 존재할 수 있는 현상

얽힘(Entanglement): 두 큐비트가 서로 강하게 연결되어 있어, 한쪽을 바꾸면 다른 쪽도 즉시 바뀜

양자 간섭(Quantum Interference): 잘못된 계산 경로는 취소하고, 올바른 경로를 증폭시키는 원리

핵심 개념들을 더 직관적으로 설명하자면, 먼저 큐비트는, 동전이 앞면 또는 뒷면이 나오는 것이 비트(Bit)라고 하면 동전을 회전시킬 때 앞면과 뒷면이 동시에 보이는 것처럼 0과 1이 동시에 존재하고, 계산이 끝나고 관측하면 비로소 0 또는 1의 값으로 결정됩니다. 중첩에 대해서 설명하자면, 기존 컴퓨팅은 미로를 풀 때 한가지 길을 차례대로 가면서 시도하였다면, 양자컴퓨팅은 동시에 모든 갈래 길을 탐험함으로써 더 빠른 계산이 가능하게 합니다. 얽힘은 두개의 동전이 서로 연결되어 있어 한 개의 동전이 앞면이면 다른 동전도 동시에 자동으로 앞면으로 정해지는 것으로 생각할 수 있습니다. 마지막으로 양자 간섭은 미로의 예시로 다시 설명할 수 있는데, 모든 길을 탐색한 후 틀린 길은 다 지워버리고, 옳은 길만 강조해주는 것입니다.

B. 양자 컴퓨팅의 필요성

위의 핵심 개념들을 통해서 양자 컴퓨팅의 필요성을 말할 수 있습니다.

큐비트를 통해 회전하는 동전처럼 동시에 여러 상태가 가능하고, 중첩으로 여러가지를 한번에 계산할 수 있으며, 얽힘 현상 때문에 멀리 있어서 즉각적으로 서로 영향을 주는 연결이 가능하며, 양자 간섭은 잘못된 계산 경로를 지우고 정답 쪽으로 경로를 강조합니다. 따라서 양자 컴퓨팅으로는 일반 컴퓨터로는 풀기 어려운 문제들을 풀어 낼 수 있는 능력과 잠재력이 있기 때문에 그 필요성이 대두됩니다.

i. 보안 및 암호해독

양자 컴퓨터는 현재 사용하는 RSA와 같은 암호를 쉽게 풀어낼 수 있고, 그와 반대로 절대 해킹이 불가능한 양자 암호도 구현할 수 있습니다.

ii. 신약 개발과 재료과학

분자나 원자 단위의 시뮬레이션은 고전 컴퓨팅 기술로는 한계가 있지만 양자 컴퓨터는 자연 상태 그대로의 시뮬레이션을 할 수 있습니다.

iii. 최적화 문제

물류, 금융, 인공지능 분야에서 자주 등장하는 복잡한 선택 문제를 신속하게 해결 할 수 있습니다.(투자 최적 조합, 최단 경로 등)

iv. 머신러닝

머신러닝을 하기 위해서 방대한 양의 데이터를 처리해야 하는데 그 처리 속도를 높일 수 있고 데이터 학습 속도 또한 향상시킬 수 있습니다.

2. 장점과 문제점

A. 양자 컴퓨팅의 장점

장점	설명
초고속 연산 능력	여러 계산을 동시에 수행할 수 있어서, 일부 문제에서 고전 컴퓨터보다 수천~수억 배 빠른 속도 가능
암호 해독 능력	기존 암호체계를 빠르게 해독할 수 있음
복잡한 시스템 시뮬레이션	분자, 원자, 화학 반응 등을 정확하게 시뮬레이션 가능 신약 개발, 재료 과학 등 활용성
최적화 문제 해결	물류, 금융, 인공지능에서 사용하는

	복잡한 조합문제를 효율적으로 계산 가능
에너지 효율성	이론적으로는 고전 컴퓨터보다 적은 에너지로 복잡한 문제를 처리 할 수 있음

B. 양자 컴퓨팅의 문제점 및 한계

문제점	설명
하드웨어 기술의 미성숙	현재까지 안정적으로 작동하는 큐비트를 수십~수백 개 수준으로만 구현됨 (수천 개 이상 필요
에러율이 높음	큐비트는 환경에 매우 민감해서 계산 도중에 쉽게 오류가 생김
양자 상태 유지 어려움	큐비트의 중첩/얽힘 상태는 금방 깨짐 이를 오랫동안 유지하기 위해서는 절대영도에 가까운 환경이 필요
매우 큰 비용	양자 컴퓨터는 제조와 유지비용이 천문학적임
소프트웨어와 알고리즘 부족	양자컴퓨터 전용 알고리즘 개발이 미진한 단계
범용 컴퓨팅으로서 역할 부재	엑셀, 워드, 웹서핑과 같은 일반 작업은 고전 컴퓨팅이 더 적합

3. 활용될 수 있는 ICT

양자 컴퓨팅을 실용화하기 위해서는 양자 컴퓨팅 기술 단독으로는 불가능합니다. 따라서 양자기술뿐만 아니라 통신기술, 컴퓨팅 인프라, 센서, IoT, AI와 같은 융합기술이 필요합니다. 이 모든 기술들이 서로 융합되어 작용할 때 양자 컴퓨팅을 실용화 할 수 있습니다.

A. 양자 컴퓨팅 기술의 ICT기술과 복합 작용하는 시나리오

i. 양자 컴퓨터를 이용하여 계산된 의료 데이터가 양자 암호화된 네트워크를 통해 클라우드로 전송되어 병원의 의료장비로 실시간 공유될 수 있습니다.

ii. 양자 컴퓨터와 AI 그리고 초고속 통신망을 이용하여 예상치 못한 금융

리스크에 빠르게 반응하고 대응할 수 있고, 해커나 외부의 침입자로부터 데이터의 탈취 가능성이 없어집니다.

B. 다음은 양자 컴퓨팅을 위해 활용 될 수 있는 ICT 기술 목록 입니다.

ICT 기술	활용 방식
클라우드 컴퓨팅	양자 컴퓨터는 대형 장비이기 때문에 대부분 클라우드 방식의 원격으로 접속이 필요
초고속 통신망	양자 컴퓨터와 사용자를 연결하거나, 양자 간 네트워크 통신을 위한 기반 인프라 5G/6G
인터넷	얽힘을 이용해 보안성이 극도로 높은 인터넷 통신 구현 가능 차세대 통신 기술
암호통신	양자 컴퓨터가 기존 암호를 깰 수 있으므로, 양자 기반 암호통신 기술(양자 키 분배)이 중요 양자 암호통신 (QKD)
사물인터넷(IoT)	양자 암호를 적용한 보안 IoT 통신이 가능
센서 기술	양자 현상을 활용한 정밀 센서 기술은 의료, 항공우주, 군사 등에 활용 양자 센서(Quantum Sensors)
슈퍼컴퓨터/고성능 컴퓨팅	양자 컴퓨터와 함께 문제를 나누어 푸는 하이브리드 시스템에서 기존 고성능 컴퓨터 필요

4. 결론

A. 양자 컴퓨터의 현재와 미래

양자 컴퓨팅은 미래 기술 중 가장 주목받는 기술 중에 하나 입니다. 암호 해독, 신약 개발, 금융 투자 전략, 최적화 문제, 기후 예측, 인공지능 고도화와 같은 분야에서 기존의 컴퓨팅 기술보다 훨씬 빠르고 정밀한 분석와 의사결정을 가능하게 합니다. 하지만 현재에는 아직 초기의 개발 단계로써

여러가지 난관에 봉착해 있습니다. 큐비트의 불안정성, 높은 오류율, 극저온 유지 기술, 막대한 비용들의 문제와 더불어 양자 컴퓨팅을 위한 소프트웨어와 알고리즘 개발도 여전히 더 많은 개발을 요합니다. 그럼에도 불구하고 양자 컴퓨팅은 점차 현실로 다가오고 있는 근접한 미래의 기술입니다. 기존의 컴퓨팅 기술의 한계를 극복하여 복잡하고 방대한 기존의 난제들을 쉽고 빠르게 처리할 수 있는 새로운 계산 기술입니다.

양자역학의 과학적 원리를 활용해 큐비트의 중첩과 얽힘 이라는 물리적 특성을 활용해 동시에 수많은 연산을 할 수 있다는 점에서 혁신적인 기술이라고 할 수 있는 동시에, 양자 컴퓨터는 단독으로 존재하는 것이 아니라 클라우드 컴퓨팅, 인공지능, 초고속 통신망, 양자암호통신 등 다양한 ICT 기술과 유기적으로 상호작용하여 융합 될 때 진정한 가치를 발산합니다. 가까운 미래에는 금융, 보안, 의료, 과학 등 여러 산업 분야에서 양자 컴퓨팅이 기존의 기술과 결합하여 실제적인 경쟁력과 핵심 혁신이 될 것입니다.