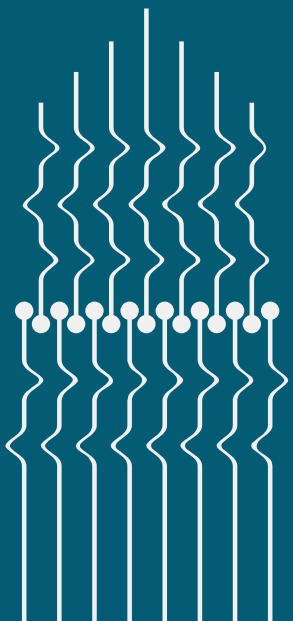
양자정보 기술용어집



CONTENTS

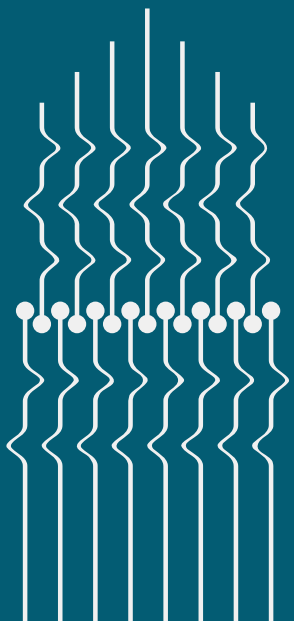
1. 양자통신

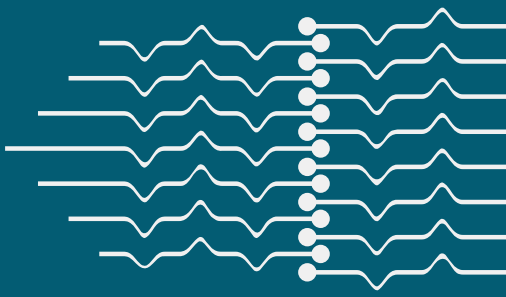
2. 양자센싱

3. 양자컴퓨팅

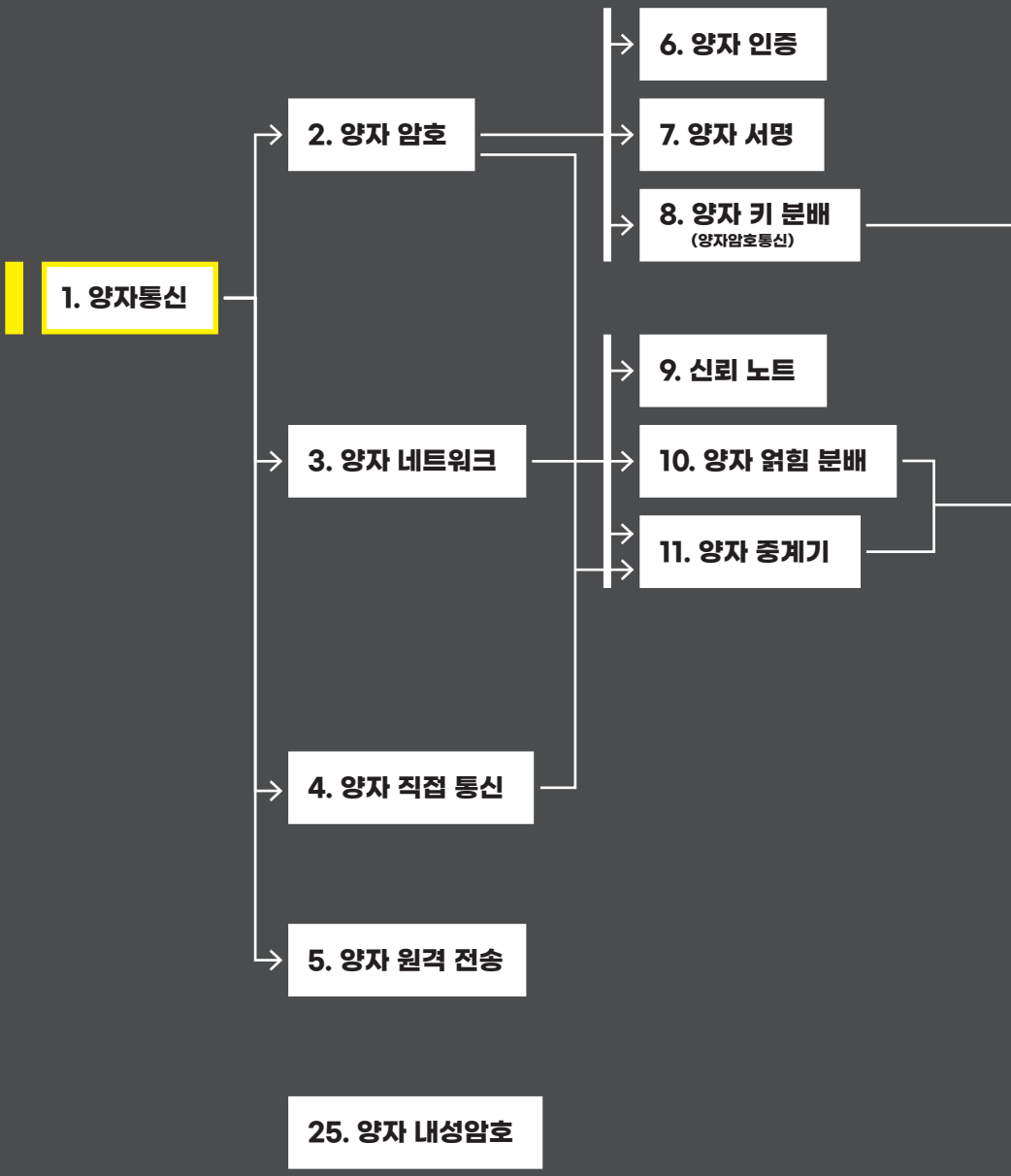
부록

1. 양자통신





양자통신 용어 MAP


1. 양자통신
2. 양자 암호
3. 양자 네트워크
4. 양자 직접 통신
5. 양자 원격 전송
6. 양자 인증
7. 양자 서명
8. 양자 키 분배
(양자암호통신)
9. 신뢰 노트
10. 양자 얽힘 분배
11. 양자 중계기
25. 양자 내성암호


12. 양자 키 분배 프로토콜
13. 양자 키 분배 시스템
14. 양자 해킹
15. 양자 난수 생성기
16. 양자 위성 통신
17. 유선 양자 키 분배
18. 무선 양자 키 분배
19. 양자 키 분배 후처리 과정
20. 키 생성률
21. 양자 비트 오류율
22. 디코이 프로토콜
23. 양자 통신을 위한 광원
24. 양자 통신을 위한 양자 상태 측정

1. 양자 통신
(Quantum Communication)

양자 통신은 양자역학 원리를 기반으로 정보를 전달하는 다양한 형태의 통신을 의미한다. 기존 고전 통신과 다르게, 양자 통신은 양자 상태 중첩(superposition), 양자 측정의 비가역성(irreversible of quantum), 복제 불가의 법칙(no-cloning theorem), 불확정성 원리(uncertainty principle)등의 양자역학 원리를 기반으로 정보 보안을 극대화하면서 정보를 전달할 수 있다. 대표적인 양자 통신 기술로, 첫째, 양자 얽힘(quantum entanglement)을 이용하여 정보를 전달하는 양자 원격 전송, 둘째, 정보 자체를 양자 상태로 직접 전송하는 양자 직접 통신, 그리고 양자역학 원리를 통해 암호통신에 필요한 비밀키를 안전하게 분배하고, 분배된 양자 비밀키를 이용하여 통신하는 양자 암호 통신 등이 있다.

2. 양자 암호
(Quantum Cryptography)

양자 암호는 양자 통신의 한 분야로, 정보의 보안성을 극대화하기 위한 차세대 통신 기술을 의미한다. 기존의 비대칭키 기반 현대 암호화 시스템(RSA, Rabin, ElGamal 등)은 수학적 계산 복잡도에 기반하여 안전성을 보장하지만, 양자 컴퓨터의 개발로 인해 그 보안성에 대한 우려가 커지고 있다. 양자 암호 통신은 이러한 문제를 해결하고 양자 컴퓨팅 환경에서 높은 보안성을 제공하기 위해 개발된 기술이다. 양자 암호 분야 중 가장 기술이 성숙된 분야가 양자 키 분배(quantum key distribution, QKD) 기술이기 때문에 양자 키 분배 기술을 양자 암호라 지칭하기도 한다.

원리 및 특징

양자 암호 통신은 정보 보안을 수학적 계산 복잡도가 아닌 양자 역학의 물리적 특성에 의존하여 무조건적인 안전성을 제공한다. 양자 암호화는 불확정성 원리와 양자 얽힘 등의 원리를 사용하여 도청을 방지하고, 도청 시 이를 감지할 수 있다.

주요 보안 서비스

양자 암호 통신은 기존 현대 암호화 시스템에서 제공하는 보안 서비스들과 동일한 수준의 보안을 목표로 한다:

1. 기밀성 (Confidentiality)

양자 키 분배를 통해 제3자가 무단으로 접근할 수 없는 고도의 비밀 통신을 구현한다.

2. 인증 (Authentication)

양자 상태와 결합된 인증 기술을 통해 송신자와 수신자 간의 신원을 확인할 수 있다.

3. 무결성 (Integrity)

전송된 정보의 일관성을 보장하며, 양자 측정의 특성상 정보가 변조될 경우 이를 감지할 수 있다.

4. 부인 방지 (Non-repudiation)

송신자가 전송한 정보를 나중에 부인할 수 없도록, 양자 암호 통신 기술을 적용하여 신뢰성을 확보한다.

3. 양자 네트워크 (Quantum Networks)

양자 네트워크는 양자 통신 기술을 활용하여 양자 상태를 장거리로 전송하고, 정보를 안전하게 교환할 수 있는 네트워크 시스템이다. 양자 네트워크는 단순히 정보 전달을 넘어 양자 컴퓨터 간의 연결, 양자 센서의 네트워크화, 그리고 양자인터넷으로 나아갈 수 있는 기반 기술이다. 네트워크 구조는 기본적으로 양자 노드(node) 사이를 연결하는 양자 채널로 구성되고, 양자 채널은 자유공간 혹은 광섬유 기반 형태로 구현될 수 있다. 각 양자 노드에는 양자 정보를 저장하는 기능이 있는 메모리와 양자 컴퓨터가 위치해 있을 수 있다. 양자 네트워크를 위해 양자 얽힘 분배 기술, 얽힘 교환 기술, 양자 중계기 등의 기술 개발이 필수적이다.

4. 양자 직접 통신
(Quantum Direct Communication, QDC)

양자 직접 통신은 양자 상태에 정보를 인코딩하여 실시간으로 직접 전송하는 통신 방식이다. QDC에서 송신자는 양자 상태 자체에 정보를 담아 전송하고 수신자는 전달된 양자 상태를 측정하여 전송된 정보를 얻는다.

원리 및 과정

1. 양자 상태 인코딩

송신자는 정보를 양자 상태에 직접 인코딩하여 생성한다. 예를 들어, 광자의 편광 상태나 스핀 상태를 사용해 정보를 표현할 수 있다.

2. 정보의 양자 상태 전송

인코딩 된 양자 상태는 실시간으로 수신자에게 전송된다.

3. 수신자의 양자 상태 측정

수신자는 송신자로부터 전달받은 양자 상태를 측정하여 정보를 획득한다. 이 과정은 양자 측정의 비가역성을 기반으로 하며, 한 번 측정된 양자 상태는 재사용할 수 없다.

주요 특징

1. 고도의 보안성

QDC는 양자 측정의 비가역성과 복제 불가 법칙을 기반으로, 전송된 정보를 제3자가 무단으로 복사하거나 측정하는 것이 불가능하다. 정보 도청 시 양자 상태가 변경되기 때문에, 송신자와 수신자는 이를 쉽게 감지할 수 있다.

2. 구현의 어려움

QDC에서 양자 상태를 안정적으로 유지하며 장거리로 전송하는 것은 기술적으로 어려운 과제이다. 양자 상태는 환경적 요인에 민감하기 때문에, 정보가 전송되는 동안 쉽게 손상될 수 있다. 이를 해결하기 위해 양자중계기 기술이 연구되고 있으나 아직 해결해야 할 기술적 난제가 많이 남아 있다.

5. 양자 원격 전송 (Quantum Teleportation)

양자 원격 전송은 양자 정보의 전송 방식 중 하나로, 양자 얽힘을 이용하여 한 위치의 양자 상태를 다른 위치로 전송하는 기술이다. 이 방법은 양자 상태를 물리적으로 직접 이동시키지 않고, 양자 얽힘과 고전적인 통신을 결합하여 정보를 전달한다.

원리 및 과정

1. 양자 얽힘 공유

송신자와 수신자는 양자 얽힘 상태(예: 얽혀 있는 두 개의 광자)를 공유한다. 이 양자 얽힘 상태는 서로 물리적으로 멀리 떨어져 있어도 그 상태가 서로 연결되어 있다.

2. 송신자의 양자 상태 생성

송신자는 보내고자 하는 특정 양자 상태를 별도로 생성한다.

3. 벨 측정 (Bell State Measurement, BSM)

송신자는 자신이 별도로 만든 양자 상태와 얽힘 상태 중 자신의 가지고 있는 양자 상태에 대해 벨 측정을 수행하여, 고전적인 측정결과 정보를 얻는다.

4. 고전적 정보 전송

송신자는 고전적인 측정결과 정보를 수신자에게 고전 채널을 통해 전송한다.

5. 양자 상태 복원

수신자는 송신자로부터 받은 고전적인 측정결과 정보를 바탕으로, 자신이 가진 양자 얽힘 상태에 적용해야 하는 양자 연산을 선택하고, 그 연산을 수행한다. 이 연산 결과에 따라 수신자의 양자 상태는 송신자가 별도로 생성한 양자 상태로 복원된다. 즉, 결과적으로 송신자가 별도로 생성한 양자 상태가 수신자에게 같은 형태로 전송된다.

주요 특징

1. 빛보다 빠르지 않음

양자 얽힘은 즉각적인 상관성을 가지고 있지만, 정보의 전달 과정은 고전적인 통신(LOCC, local operations and classical communication)을 필요로 한다. 고전적 정보의 전달 속도는 빛의 속도보다 빠를 수 없으므로, 양자 원격 전송 과정은 상대성 이론에 위배되지 않는다.

2. 복제가 아닌 복원

양자 원격 전송 과정은 양자 상태의 복제가 아니라 복원이다. 복제 불가 법칙에 의해 양자 상태를 완전히 동일하게 복제할 수 없으며, 벨 측정을 통해 얻은 송신자의 정보에 따라 수신자가 양자 상태를 복원하게 된다. 즉, 수신자는 송신자의 측정 결과에 따라 다른 양자 연산을 수행하여 원래의 상태를 재구성한다.

6. 양자 인증 (Quantum Authentication)

양자 인증은 안전한 양자 암호 통신을 위해 반드시 선행되어야 하는 핵심 기술이다. 이 기술은 양자역학의 원리를 이용하여 안전성을 제공한다. 양자 인증의 목적은 사용자가 신뢰할 수 있는 정당한 개체인지 확인하거나, 전송된 메시지가 신뢰할 수 있는 개체로부터 온 것인지를 확인하는 것으로, 각각 양자개체인증, 양자메시지인증으로 분류할 수 있다. 일반적으로 개체(identity)는 사람 또는 장치를 의미하고, 개체인증은 비밀번호, 일회성 비밀번호, challenge-response, zero-knowledge 등으로 세분화할 수 있다.

양자 암호 통신은 기존의 현대 암호와 마찬가지로 기밀성, 인증, 무결성, 그리고 부인방지와 같은 보안서비스를 모두 제공되어야 한다. 그러나 많이 연구되고 있는 양자 키 분배는 기밀성만을 제공한다고 알려져 있으며, 다른 보안서비스들을 제공하기 위해서는 추가적인 양자보안기술이 필요하다. 따라서 양자인증 기술은 안전한 양자 암호 통신을 위해 필수적으로 선행되어야 한다.

7. 양자 서명 (Quantum Signature)

안전한 양자 암호 통신을 위해 개체의 신원을 보장할 수 있는 양자인증에서 더 나아가, 양자서명 기술은 필수적이다. 양자 서명은 양자역학의 원리를 이용하여 무결성, 메시지인증, 부인방지를 보장할 수 있으며, 기존의 고전 서명 기법 보다 더 안전한 보안을 제공한다. 대부분의 양자 서명의 암호화 방법은 Pauli 연산자 암호화, (I, H) 타입 연산자 암호화, 일회성 key-controlled-'I' 암호화, 그리고 범용(universal) 양자 암호화 등을 사용한다. 특히 범용 양자 암호화 방법은 양자 서명 연구의 중요한 전환점이 된 위조 공격 Gao's forgery에 대해 안전성이 증명되었다. 양자 서명 과정에서 도청자의 목표는 서명 키를 획득하거나, 서명된 메시지를 위조하는 것으로, 이러한 공격 방식에 대응하는 여러가지 프로토콜이 제안되고 있다.

8. 양자 키 분배(양자암호통신) (Quantum Key Distribution, QKD)

양자 키 분배는 양자 암호 통신에서 핵심적으로 연구되고 있는 기술로, 양자 역학의 원리를 이용해 통신구성원들이 안전하게 비밀키를 교환할 수 있게 하는 방식이다. 양자 직접 통신과는 다르게, QKD는 양자 비밀키를 교환하고, 이 비밀키로 정보를 암/복호화(encryption/decryption)하는데 사용한다. 비밀키는 암호화된 정보의 안전성을 보장해주며, 교환한 비밀키 자체는 의미를 담고 있지 않아 안전성을 더 높여준다. 이러한 특징에 의해 QKD는 기존의 RSA 알고리즘을 대체할 수 있는 차세대 비밀키 교환 방식으로 주목받고 있다.

양자 키 분배는 구현 방법에 따라 광 섬유(optical fiber) 선로를 채널로 이용하는 유선 방법과 자유공간(free-space)을 채널로 이용하여 신호를 전송하는 무선 방법이 있다. 유선 QKD의 경우 국내 기술이 주요 선진국 기술을 빠르게 추격하고 있다. 2000년대 초반부터 KIST, ETRI 등의 출연연과 몇몇 대학에서 원천기술을 연구하고 있으며, SKT, KT 등의 통신 기업에서 유선 QKD 상용화를 위한 연구 개발에 집중하고 있다. 반면 무선 QKD의 경우, 위성 QKD 등 상당한 성과가 있는 해외와는 다르게 아직까지는 기술격차가 크게 벌어져 있는 실정이다.

9. 신뢰 노드 (Trusted Node)

신뢰 노드는 양자 통신에서 두 송신자 간의 양자 상태를 안전하게 중계하거나 조정하는 기능을 수행한다. 이는 송신자와 수신자의 암호키를 저장하고 기밀성을 유지 및 관리하기 위한 보안 메커니즘을 구현하며, 다른 요소들과의 상호작용을 처리한다. 이러한 신뢰 노드는 특히 양자 통신 네트워크에서 필수적인 요소로, 통신거리를 확장하는데 중요한 역할을 한다. 그러나 신뢰 노드가 해킹되었거나 보안 취약점을 가질 경우, 양자 통신 전체의 보안이 약화될 수 있다. 따라서 신뢰 노드의 설계 및 운영에 있어 높은 수준의 보안이 요구되지만, 아무리 보안 관리가 철저하더라도 실제 환경에서 이 신뢰성을 100% 보장하기 어렵다. 원천적으로 보안성을 강화하기 위해 양자 얽힘 상태 분배 기술이나 양자 중계기 기반의 양자 노드로 이루어진 양자 네트워크에 대한 연구가 진행되고 있다.

10. 양자 얽힘 분배 (Quantum Entanglement Distribution)

양자 얽힘 분배는 양자 얽힘(entanglement) 상태를 여러 노드에 분배하는 기술이다. 양자 얽힘 상태를 생성하는 대표적인 방법은 2차 비선형 매질의 상호작용을 이용하는 매개하향변환(spontaneous parametric down-conversion, SPDC) 과정이 있다. 이는 광자쌍이 생성되는 과정으로, 주로 PPKTP(periodically-poled-KTP)나 BBO(Beta Barium Borate)등의 비선형 매질을 이용한다.

또한, 간섭계를 구성하여 얽힘 광자를 생성하는데, 주로 사냑 간섭계, 마하젠더 간섭계가 사용된다. 이렇게 생성한 양자 얽힘 광자는 광섬유나 자유 공간을 통해 여러 노드로 분배된다. 양자 얽힘 상태를 이용한 양자 통신은 양자역학의 특성상 높은 보안성을 제공하고, 통신거리를 확장에 중요한 역할을 하며, 더 나아가 양자 네트워크로 나아가는 기반이 된다. 그러나 현시점에서는 얽힘 상태를 장거리에서 유지하는 데에 기술적인 한계가 존재한다.

11. 양자 중계기 (Quantum Repeater)

최근 양자 통신에 대한 연구는 통신 거리 확장을 중심으로 활발히 진행되고 있다. 기존의 양자 통신은 장비의 감쇄율, 검출기의 효율, 전송 채널의 잡음 등을 포함하여 약 100km 내외로 통신거리 확장의 한계를 가지고 있다. 이러한 통신거리 한계를 극복하기 위해 다양한 연구가 진행되고 있으며 궁극적으로는 양자중계기를 활용한 양자 통신 기술이 필수적이다. 광자를 이용한 양자 통신에서 채널 손실로 인해 통신 효율이 급격히 감소하는데, 양자 측정의 비가역성과 복제 불가능성 때문에 고전 통신처럼 단순한 신호 증폭 중계기를 사용할 수 없다. 이를 해결하기 위해 양자 중계기는 양자 상태를 직접 증폭하지 않고, 얽힘 교환(entanglement swapping)과 양자 메모리(quantum memory)를 이용해 정보를 전달한다.

얽힘 교환의 원리는 다음과 같다. 송신자-중계기, 중계기-수신자 사이에서 각각 양자 얽힘을 생성 및 분배하고, 이를 중계기에서 측정하면 얽힘 교환 원리에 의해서 송신자와 수신자 간의 장거리 얽힘 상태로 확장할 수 있다. 이를 현실적으로 구현하기 위해서는 송신자와 수신자 노드에 양자 상태를 저장할 수 있는 양자 메모리가 필요하다. 양자 메모리는 양자 상태를 일시적으로 저장하고 유지하는 역할을 하며, 이를 통해 이론적으로 양자 상태의 결맞음 시간을 연장할 수 있다. 양자메모리의 대부분 연구결과는 양자메모

리 효율을 높이는 것과 저장 시간을 증가시키는 연구에 집중하고 있다. 비록 양자 중계기와 양자 메모리는 아직 기술적으로 많은 한계를 가지고 있지만, 매우 빠른 기술발전 속도를 가지고 있다. 이를 바탕으로 양자 인터넷과 양자네트워크 구축이 현실화될 수 있으며 장거리에서도 암호 통신을 가능하게 할 중요한 기술이다.

12. 양자 키 분배 프로토콜 (QKD Protocol)

QKD 기술은 단일 광자의 편광이나 time-bin 등 불연속적인 모드에 0과 1의 정보를 인코딩하는 이산변수(discrete variable, DV) QKD와 연속적인 빛의 위상과 진폭에 정보를 인코딩 하는 연속변수(continuous variable, CV) QKD로 나눌 수 있다.

12-1. BB84

BB84 프로토콜은 1984년 Charles Bennett와 Gilles Brassard가 제안한 최초의 QKD 프로토콜로, 양자의 특성을 이용하여 통신원 간에 비밀 키를 안전하게 분배하는 방법이다. BB84 프로토콜은 정보이론적으로 보안성이 잘 증명된 프로토콜이며, 가장 널리 쓰이고 있다. BB84 프로토콜을 이용한 양자 암호 통신은 광자의 편광, 위상, time-bin 등의 상태에 정보를 실을 수 있다. 프로토콜의 자세한 설명을 위해 이 중에서 편광을 이용한 동작에 대해 기술한다.

원리 및 과정

1. 양자 상태 인코딩

송신자와 수신자는 0과 1의 비트를 수평-수직 기저(rectangular basis)에서 각각 수평 편광 (0˚)과 수직 편광 (90˚)으로 약속하고, 대각-반대각 기저(diagonal basis)에서는 각각 대각 편광 (45˚)과 반대각 편광 (135˚)으로 약속한다. 이에 따라서 송신자는 4개 중 무작위로 선택한 편광을 가진 양자 상태를 생성한다.

2. 양자 상태 전송

신자는 생성한 무작위 양자 상태를 양자채널을 통해 수신자에게 전송한다.

3. 양자 상태 측정

수신자는 무작위로 기저를 선택해 전달받은 양자 상태를 측정한다. 만약 수신자가 선택한 기저가 송신자가 사용한 기저와 일치한다면, 수신자는 100% 확률로 편광상태를 정확하게 측정한다. 그러나, 만약 선택한 기저가 다를 경우, 50%확률로 측정오류가 발생하게 된다.

4. 고전 정보 공유

송신자와 수신자는 고전 채널을 통해 서로의 기저 정보를 교환한다.

5. 시프팅 과정

교환한 기저정보를 바탕으로, 서로의 기저가 일치할 경우의 측정 결과만으로 비트열을 만들며, 이때 해당 비트 열을 sifted key라고 한다.

6. 후처리 과정

이 후 시스템으로 구현했을 때 발생할 수 있는 오류를 정정하고 오류정정시 발생할 수 있는 정보 유출에 대한 대응으로 비밀성을 증폭할 수 있는 신호처리 과정을 거친다.

12-2. E91

1991년에 Artur Ekert가 개발한 E91 프로토콜은 얽힘 상태를 이용한 QKD 프로토콜이다. 송신자와 수신자는 서로 얽힘 상태의 입자를 나눠 가지며, 각각 단일 측정을 수행한다. 이 후 시프팅과 후처리 과정을 거쳐 비밀키를 생성한다. E91 프로토콜은 양자 얽힘을 사용하기 때문에, Bell 부등식의 위배를 통해 도청 여부를 확인할 수 있다. 얽힘 상태 기반 양자 키 분배의 안전성은 널리 사용되는 BB84 프로토콜과 동일하다고 증명되었다.

12-3. Measurement-Device-Independent (MDI) QKD

기존 QKD 프로토콜의 보안성이 이론적으로 증명되어 있지만, 실제 시스템을 구성하는 양자 장치들은 부채널(side-channel)을 갖고 있기 때문에 다양한 부채널 공격(side-channel attack)에 노출된다. 이로 인해 장치의 불완전성에 관계없이 안전하게 동작하는 Device-Independent(DI) QKD가 연구되고 있으며, 그 중에서도 불완전한 검출기에 무관하게 안전한 MDI QKD 기법이 제안되었다. MDI QKD의 전체 과정은 다음과 같다. 송신자와 수신자는 독립적으로 양자 상태를 생성하여 중재자인 측정부에게 동시에 전송하고, 중재자는 Bell State Measurement(BSM)을 수행한다. 이어서 중재자는 측정에 성공한 시점과 그 결과를 기록하고 송신자와 수신자에게 공표한다. 송신자와 수신자는 시프팅 과정과 후처리 과정을 거쳐서 비밀키를 분배한다. 이 구조는 중재자가 측정 결과를 통해 비밀키를 추정할 수 없으므로 실제 구현 시 검출기의 불완전성으로 인한 공격에 대한 원천적인 해결책이다.

12-4. Twin-Field (TF) QKD

TF QKD는 2018년에 M. Lucamarini가 처음 제안한 기법으로, 프로토콜 구조만으로 양자 통신 거리 확장의 한계를 극복할 수 있는 방법이다. 송신자와 수신자가 생성한 광 필드(field)에 위상 차이를 인가하여 중재자에게 전송한다. 중재자인 측정부에서 일차 간섭(single photon interference)이 일어나고 해당 측정 결과로 비밀키를 분배할 수 있다. 두 필드의 글로벌 위상이 유사(twin)할수록 간섭 패턴의 가시성(visibility)이 상승하여 키 생성률이 증가한다. MDI QKD와 마찬가지로 제3자인 중재자가 측정하는 구조이기 때문에 검출부 도청 공격에 대해 안전하다. 또한, 수신부에서 단일 광자 클릭만 유효하게 취급하는 특성 때문에, 결과적으로 전송채널의 투과율이 기존 QKD의 투과율(transmittance, η)에 비해 루트오더로 감소하게 되고. 따라서 장거리 양자통신이 가능하게 된다. 여기서 투과율은 전송되는 광신호의 손실을 말한다.

12-5. Continuous Variable (CV) QKD

CV QKD는 양자 상태의 이산적 변수가 아닌 연속 변수를 활용하여 비밀키를 분배하는 기법이다. 이 프로토콜에서는 빛의 쿼드러처에서 연속적으로 변하는 두 가지 물리적 변수인 위상과 진폭을 변조하여 키를 분배한다. CV QKD는 기존의 QKD 시스템과 달리, 고전 광통신 레이저 기술 및 저비용 검출기를 사용하여 구현할 수 있어 비용 효율성과 실용성이 높다.

13. 양자 키 분배 시스템 (QKD System)

QKD 시스템에는 크게 one-way 방식과 PnP(plug and play) 방식이 있다. one-way 방식에서는 송신자가 신호를 보내고, 수신자가 이를 측정하는 역할을 맡는다. 신호의 송신과 측정이 분리되어 있기 때문에 보안성이 높다는 장점이 있지만, 간섭계의 경로 차이를 일치시키거나 안정적인 편광 상태를 유지하는 것이 기술적으로 어렵다는 단점이 있다. 반면, PnP 방식은 수신자가 초기 신호를 송신자에게 전송하면, 송신자가 Faraday Mirror를 이용해 이를 다시 수신자에게 되돌려 보내는 방식으로, 수신자가 초기 신호 송신과 측정을 모두 담당하게 된다. PnP 방식은 간섭계와 편광 신호의 안정적 동작을 위한 별도의 능동 장치가 필요하지 않아 구현이 상대적으로 쉽다는 장점이 있지만, 송신자가 신호를 수신하고 송신하는 동작 중에 안전성이 떨어질 수 있다는 단점이 존재한다.

유선 광통신망에서 QKD 시스템을 구현하기 위해서 주로 위상 인코딩 방식을 사용하기 때문에, 이를 위한 간섭계를 활용하게 된다. 간섭계는 빛의 간섭 현상을 관찰할 수 있는 장치로, QKD 시스템에서는 주로 일차간섭(single photon interference)에 기반한 Michelson 간섭계, Mach-Zehnder 간섭계, Sagnac 간섭계와 이차간섭(two photon interference)에 기반한 Hong-Ou-Mandel 간섭계가 사용된다.

Michelson 간섭계는 비대칭 빔 스플리터를 사용해 신호의 위상을 비교하는 데 적합하며, 두 경로의 길이를 조정하여 간섭 효과를 극대화할 수 있다. Mach-Zehnder 간섭계는 두 개의 빔 스플리터와 두 개의 거울을 이용해 간섭 현상을 생성하는 방식으로, 신호의 위상을 효과적으로 조정할 수 있다. Sagnac 간섭계는 두 개의 광 경로가 서로 간섭하여 출력 신호의 세기를 조절하는 방식으로, 특히 시간 지연을 활용하여 신호를 인코딩하는 데 유용하다. Hong-Ou-Mandel 간섭계는 두 개의 광원이 생성한 광자 쌍이 결합하여 간섭을 일으키는 방식으로, 두 광자의 양자적 상관관계를 활용해 높은 보안성을 제공하는 QKD 구현에 적합하다.

14. 양자 해킹 (Quantum Hacking)

양자 해킹은 QKD 시스템의 취약점을 이용해 도청자가 정보를 탈취하거나 송신자와 수신자 간의 통신을 교란하려는 다양한 시도를 의미한다. 대표적인 공격 기법으로는, 다광자 상태에서 일부 광자를 가로채는 방식으로 정보를 도청하는 기법인 광자 수 분할 공격, QKD 장치의 물리적 특성을 분석하여 정보를 얻는 부채널 공격, 도청자가 송신된 신호를 차단하고 위조된 신호를 Bob에게 전송하는 위조 신호 공격, 그리고 송신 또는 수신 장치에 외부 신호를 주입해 내부 정보를 탐지하는 Trojan-Horse 공격이 있다. 이러한 해킹 시도를 알아채거나 막기 위해 MDI 프로토콜, decoy 프로토콜 등 여러가지 보안 방법이 연구되고 있다.

광자 수 분할 공격

(Photon Number Splitting Attack, PNS Attack)

광자 수 분할 공격은 QKD 시스템에서 발생할 수 있는 공격 방식 중 하나로, 공격자가 송신자가 전송한 신호에서 두 개 이상의 광자가 포함된 경우에 발생할 수 있다. 이상적인 QKD에서는 단일 광자 광원을 가정하지만, 실제로는 단일 광자 수준의 약한 결맞음 상태를 이용한다. 이 경우 신호의 광자의 수는 푸아송 분포(Poisson distribution)를 따르며, 다광자일 확률이 존재한다. 송신자가 전송하는 신호에 여러 개의 광자가 포함된 경우, 도청자는 해담 시점에서 일부 광자를 측정하여 정보를 가로챌 수 있다. 예를 들어, 송신자가 두 개의 광자를 포함한 신호를 보낸 경우, 공격자는 하나의 광자를 가로채어 정보를 확보할 수 있다. 이러한 공격 방식은 송신자가 보낸 신호의 평균 광자수가 높을수록 여러 개의 광자가 발생할 확률이 높아지며, PNS 공격으로 얻을 수 있는 정보량이 증가한다. 양자 암호 통신에서 PNS 공격을 근본적으로 방지하기 위해서 디코이 상태(decoy state) 기법을 사용한다.

15. 양자 난수 생성기 (Quantum Random Number Generator, QRNG)

양자 난수 생성기는 양자 역학의 불확정성 원리를 이용해 진정한 무작위 숫자를 생성하는 장치이다. 기존의 고전적인 난수 생성기는 컴퓨터 알고리즘을 사용해 난수를 생성하기 때문에 예측 가능성과 주기성을 완전히 배제할 수 없지만, QRNG는 양자 현상을 기반으로 하므로 예측이 불가능한 진정한 난수를 생성할 수 있다.

QRNG는 주로 빛의 양자적 특성인 단일 광자의 편광 상태, 광자의 경로 선택, 또는 양자 얽힘을 활용하여 난수를 생성한다. 예를 들어, 빔 스플리터(beam splitter, BS)를 사용해 광자가 어느 경로로 나가는지를 측정하는 방식으로 난수를 만들 수 있다. 단일 광자를 BS에 입사시키면, 양자역학적 확률에 따라 광자는 두 가지 경로 중 하나를 선택하게 되며, 이 선택은 중첩 상태에 놓인다. 이를 측정하여 광자가 선택한 경로를 0과 1로 변환함으로써 무작위 숫자를 얻을 수 있다. 이러한 방식은 본질적으로 양자역학의 비결정론적 특성을 이용하므로, 생성된 숫자는 완전히 무작위이며 예측하거나 재현할 수 없다. QRNG는 특히 보안이 중요한 분야에서 유용하며, QKD와 같은 양자 암호 시스템에서 진정한 난수를 제공하여 무작위 기저 선택이나 디코이 상태(decoy state) 생성에 중요한 역할을 한다.

16. 양자 위성 통신 (Quantum Satellite Communication)

양자 위성 통신은 무선 통신의 한 종류로 지상 간 장거리 양자 통신을 하기 위해 인공위성을 활용하는 기술이다. 양자 위성 통신에서 위성은 지상의 송신자와 수신자 사이에서 양자 상태를 전송해주는 신뢰점으로 사용되거나, 얽힌 상태의 광자를 생성하여 지상에 전달하는 역할을 한다. 이를 통해 지상에서 직접 연결하기 어려운 먼 거리 간에도 양자 통신을 수행할 수 있다. 실제로 세계 최초의 양자 위성인 중국의 Micius 위성은 약 1200km의 양자 전송과 약 7600km의 QKD 시스템을 성공적으로 시연하여 양자 위성 통신의 가능성을 입증했다.

17. 유선 양자 키 분배
(Wired QKD, Optical Fiber QKD)

유선 양자 키 분배는 광 섬유 선로를 전송 채널로 사용하는 QKD로, 전자기 간섭이나 외부 잡음에 비교적 강하여 안정적인 통신 환경을 제공한다.

최근 유선 QKD 분야에서는 통신 거리의 확장, 네트워크 구현, 비용 절감 등 상용화를 위한 다양한 연구가 진행되고 있다. 특히 통신 거리의 확장은 QKD의 주요 과제 중 하나로, 유선 QKD는 광섬유를 통해 전송되는 신호의 감쇄(loss)가 크기 때문에 이를 해결하기 위한 기술들이 연구되고 있다. 이를 극복하기 위해 신뢰 노드(trusted node), 양자 중계기(quantum repeater), 검출기 노이즈 제거 기술 및 효율 향상, 프로토콜 구조 개선 등 여러 방면으로 연구 개발되고 있다. 특히 단일 광자 검출기의 효율을 개선하고, 광 신호의 고속 변조 기술을 발전시키며, 효율적인 프로토콜 구조를 제안하는 등의 연구를 통해 유선 QKD의 전송 거리가 점점 증가하고 있다. 2023년에 중국과학기술대학은 실험실 환경에서 최대 1000km의 유선 QKD를 구현하는데 성공하였다. 또한, 국내에서의 QKD 기술은 기존에 포설되어 있는 광 섬유 네트워크를 이용할 수 있기 때문에 상업화에 유리하여 유선 QKD를 중심으로 연구 개발되고 있다.

18. 무선 양자 키 분배 (Wireless QKD, Free-space QKD)

무선 양자 키 분배는 자유공간(대기 중)으로 신호를 전송하는 QKD로, 광섬유 같은 물리적 전송 매체 없이 양자 상태를 전송하는 방식이다. 이 방식은 미리 설치된 광섬유가 필요하지 않기 때문에 광섬유 설치가 어려운 환경에서, 특히 이동하는 지점 간에도 통신이 가능하다는 장점이 있다.

무선 QKD의 대표적인 성과인 위성 양자 키 분배는 양자중계기 없이도 수백 km 거리 제한을 벗어난 장거리 통신이 가능하다. 주로 광자 손실이 일어나는 대기권에서는 산란, 흡수 및 날씨의 영향 등을 많이 받아 신호 전송 품질에 영향을 크게 미치지만, 그 이후 구간에서는 광자 손실이 거의 발생하지 않는다. 다만 거리가 길어질수록 광 신호의 퍼짐 현상으로 인해 신호 수신 효율이 떨어지는 단점이 발생한다.

최근 위성 이외에도, 드론을 이용한 무선 QKD에 관한 연구도 활발하게 진행되고 있다. 드론에 양자 키 분배 시스템을 탑재하기 위해서는 소형화 및 경량화가 필수적이다. 또한, 위성과 달리 드론은 대기권에서 동작하므로 날씨와 기상 조건에 의해 드론의 통신 환경이 수시로 변한다. 이러한 환경적 요인은 광자의 전송 경로에 큰 영향을 미쳐, 자유 공간에서의 광자 손실을 유발할 수 있다. 따라서 자유공간에서의 광자 손실을 최소화하기 위한 기술 개발이 필수적이다.

유선 QKD는 1550nm 파장 대역을 이용하는 반면 무선 QKD는 자유공간에서의 전파 특성 및 측정 장치 효율을 고려하여 700~800nm 파장 대역으로 주로 통신한다. 2016년 중국이 발사한 Micius 위성을 이용하여 1200km 지상국 간 양자 키 분배를 최초 시연한 이후로 해외에서 많은 기술 개발이 진행되고 있으며, 국내에서는 KT와 ETRI, KIST에서 고정형 무선 QKD 실험에 성공한 바 있다.

19. 양자 키 분배 후처리 과정 (Post-processing)

QKD 시스템은 양자 채널의 노이즈, 검출기의 효율 저하, 결어긋남(decoherence), 잠재적인 도청 시도 등 여러 요인으로 인해 오류가 발생할 수 있다. 후처리 과정은 이러한 오류를 수정하고 보안을 강화하는 절차로, QKD 시스템에서 송신자와 수신자가 공유한 원시 키를 신뢰할 수 있는 비밀 키로 추출하는 데 필수적인 과정이다. 후처리 과정은 크게 오류 정정과 개인정보 증폭의 두 단계로 이루어진다.

19-1. 오류 정정 (Error Correction)

오류 정정은 송신자와 수신자가 공유한 원시 키에서 발생한 불일치를 교정하는 과정이다. 이 과정에서 송신자와 수신자는 고전 통신 채널을 통해 서로 정보를 교환하며, 주로 Cascade 프로토콜, Winnow 프로토콜, LDPC와 같은 오류 정정 알고리즘을 사용한다. Cascade 프로토콜은 다단계로 이루어진 반복적인 정보 교환과 수정 및 제거 과정을 통해 송수신자 간에 동일한 키를 얻을 수 있게 한다. 오류 정정 과정에서 일부 키가 제거되기 때문에, 결과적으로 키 생성률이 감소하게 된다.

19-2. 개인정보 증폭 (Privacy Amplification)

개인정보 증폭은 Eve가 도청을 통해 일부 정보를 얻었을 가능성에 대비하여, Eve가 획득한 정보를 무력화해 보안성을 강화하는 과정이다. 이는 오류 정정이 끝난 원시 키에 유니버설 해싱과 같은 알고리즘을 적용함으로써 이루어진다. 유니버설 해싱 알고리즘은 무작위로 선택된 해시 함수를 사용해 원시 키를 압축하고, 그 결과 생성된 해시 함수 집합 중 하나를 선택해 키를 짧고 안전한 비밀 키로 변환하는 알고리즘이다. 이 과정을 거친 후에는 도청자가 일부 원시 키 정보를 알고 있더라도, 최종 비밀 키에 대한 정보는 거의 얻을 수 없게 된다.

20. 키 생성률 (Key Rate)

키 생성률은 QKD 시스템에서 보안 키를 생성하는 속도를 나타내는 중요한 지표다. 이는 단위 시간당 송수신자 간에 성공적으로 교환된 비밀 키의 양을 의미하며, 일반적으로 bits per second, [bps] 단위로 나타낸다. 이 지표는 시스템의 성능을 평가하는 데 핵심적인 역할을 한다. QKD의 효율성은 키 생성률에 크게 좌우되며, 신호의 전송 거리, 오류율, 그리고 사용된 양자 채널의 품질에 따라 변동될 수 있다. 키 생성률은 크게 두 가지로 나눌 수 있는데, 첫번째는 원시 키 생성률(raw key rate)이고, 두번째는 비밀 키 생성률(secret key rate)이다.

20-1. 원시 키 생성률 (Raw Key Rate)

원시 키 생성률은 QKD 시스템에서 송신자와 수신자 간에 생성되는 원시 키의 비율을 나타내며, 이는 암호화 통신에 사용할 수 있는 잠재적 키를 의미하지만 실제로 사용할 수 있는 유효 키는 아니다. 또한, 원시 키 생성률은 광원, 검출기의 성능과 양자 채널의 품질, 적용되는 QKD 프로토콜의 특성에 크게 영향을 받는다.

20-2. 비밀 키 생성률 (Secret Key Rate, SKR)

비밀 키 생성률은 원시 키에 오류율을 줄이는 오류 정정(error correction)과 보안성을 강화하는 개인정보 증폭(privacy amplification) 등의 후처리 과정(post-processing)을 적용하여 생성된, 실제로 사용할 수 있는 최종 비밀 키의 비율을 의미한다. 이 후처리 과정을 거치기 때문에 비밀 키 생성률은 원시 키 생성률보다 낮을 수밖에 없으며, 시스템이 도청에 얼마나 강력하게 방어할 수 있는지, 그리고 채널에서 발생한 오류를 얼마나 효과적으로 수정할 수 있는지에 따라 두 값의 차이가 달라진다. 따라서 비밀 키 생성률은 QKD 시스템의 실제 보안 능력을 평가하는 중요한 지표이다.

21. 양자 비트 오류율 (Quantum Bit Error Rate, QBER)

양자 비트 오류율은 QKD 시스템에서 송신자와 수신자 간에 전송된 양자 비트 중 오류가 발생한 비트의 비율을 나타내는 중요한 지표다. QBER은 시스템의 안정성을 평가하는 데 필수적이며, 비밀 키의 품질에 직접적인 영향을 미친다.

QBER은 일반적으로 전송된 양자 비트 중에서 수신자가 잘못 인식한 비트의 수를 기반으로 계산된다. 예를 들어, 송신자가 100개의 양자 비트를 전송했을 때, 수신자가 5개의 비트를 잘못 인식했다면 QBER은 5%가 된다. 이 비율은 도청자의 존재 여부나 전송 채널의 품질을 판단하는 데 유용하다. 특히 QKD에서는 QBER이 너무 높으면 통신이 불안정하거나 도청이 발생했을 가능성이 크므로, QBER을 일정 값 이하로 유지하는 것이 중요하다.

QBER이 높아지는 주요 요인은 여러 가지가 있다. 첫째, 전송 과정에서 발생하는 노이즈, 감쇄는 오류를 유발하여 QBER을 높이는 원인이 된다. 둘째, 전송 경로의 특성에 따라 QBER이 달라질 수 있다. 예를 들어, 광섬유의 품질이나 기후 변화는 신호의 품질에 영향을 미쳐 오류율에 변화를 일으킬 수 있다. 셋째, 송신자와 수신자의 장비, 즉 광원과 검출기의 성능이 QBER에 큰 영향을 준다. 고성능 장비일수록 QBER이 낮아질 가능성이 높으며, 이는 전체 QKD 시스템의 안정성을 향상시킨다.

QBER은 QKD 시스템의 성능을 평가하는 데 중요한 요소이며, 비밀 키 생성률(secret key rate)과도 밀접한 관계가 있다. 따라서 QBER을 모니터링하고 관리하는 것은 QKD의 보안성을 확보하기 위해 필수적이다.

22. 디코이 프로토콜 (Decoy Protocol)

디코이 상태는 QKD 시스템에서 PNS 공격을 방어하기 위한 중요한 기술이다. 송신자는 실제로 비밀키를 생성하기 위한 약한 결맞음 상태 외에도, 의도적으로 세기가 매우 약한 디코이 상태를 함께 전송한다. 이러한 디코이 상태를 보내는 이유는, 공격자가 신호에서 여러 개의 광자를 가로채려고 할 때 이 신호가 디코이 상태일 가능성을 이용해 도청행위를 감지하기 위함이다. 공격자는 디코이 신호와 실제 신호를 구별할 수 없기 때문에, 만약 디코이 상태에서 여러 개의 광자를 가로챈다면 수신자는 그 신호에서 비정상적으로 높은 오류율을 관측할 수 있다. 여기서 비정상적인 오류율이란, 정상적인 신호에서는 일정한 비율로 관측되는 오류가 갑자기 증가하는 현상을 의미한다.

디코이 상태는 이러한 방식으로 QKD 시스템에서 발생할 수 있는 PNS 공격뿐만 아니라, 다른 유형의 공격에 대해서도 효과적인 방어를 제공한다. 따라서 디코이 상태를 사용한 QKD 시스템은 더 안전하고 신뢰할 수 있는 비밀키를 생성할 수 있다.

23. 양자통신을 위한 광원 (Quantum State for Quantum Communication)

양자 통신에 사용되는 양자 상태는 주로 광자를 이용하여 생성한다. 기존의 광통신기술은 광자 다발(수백만 개 이상의 광자)을 사용해 정보를 전달하지만, 양자 통신은 단일 광자(single photon), 약한 결맞음 상태(weak coherent state), 그리고 얽힘 상태(entangled state)를 활용하여 정보를 전달하며, 양자역학적 원리를 기반으로 보안성을 강화할 수 있다. 하지만 실제 구현에는 많은 기술적 제약이 존재한다.

단일 광자는 하나의 광자로 구성되는 가장 기본적인 양자 상태로, 단일 광자를 사용하는 양자 통신에서 측정의 비가역성과 복제 불가의 법칙을 통해 도청 행위를 감지할 수 있다. 단일 광자는 다양한 기술로 생성할 수 있으며, 대표적인 방법으로는 양자점(quantum dot), 점결함(single defect) 소자를 이용한 방법이 있다. 하지만 이러한 방법들은 광원 구현의 복잡성, 구현 비용 등의 문제로 인해 상용 양자 통신에 바로 적용되기에는 한계가 있다.

대신 평균 광자수를 단일 광자 수준으로 조절한 약한 결맞음 상태가 양자 통신에서 더 실용적으로 사용된다. 결맞음 상태는 결맞음 시간동안 전역 위상(global phase), 주파수, 그리고 진폭이 일정하게 유지되는 상태로, 주로 레이저를 이용하여 생성된다. 이때 레이저로 생성되는 결맞음 상태는 다광

자(multi-photon) 상태를 포함하며, 광 세기 감쇄기(attenuator)를 통해 평균 광자수를 낮춘다. 약한 결맞음 상태의 광자수-확률 분포는 푸아송 분포 (Poisson distribution)을 따르며, 평균적으로는 하나 이하의 광자가 존재하지만, 낮은 확률로 다광자가 포함될 확률이 존재한다. 약한 결맞음 상태는 단일 광자 상태와 유사한 특성을 가지면서도 구현이 상대적으로 용이하고 비용 측면에서 효율적이기 때문에, 실제 양자 통신 시스템에서 광원으로 널리 사용된다. 그러나 다광자가 포함될 가능성이 존재하므로, 이로 인해 도청자가 일부 정보를 가로챌 가능성이 있으며, 이는 보안성에 잠재적인 위험을 초래할 수 있다. 이를 보완하기 위해 디코이 프로토콜이 사용된다.

양자 통신에서는 정보 전달 용량을 증가시키기 위해서 이차원 양자 상태(큐비트; qubit)보다 다차원 양자 상태(큐딧; qudit)를 활용하는 방식을 사용하기도 한다. 다차원 양자 상태는 한 번에 더 많은 양의 정보를 인코딩할 수 있어, 통신 효율과 정보 전송량을 극대화할 수 있다. 이를 위해 다양한 방법으로 양자 상태를 준비할 수 있으며, 대표적인 방법은 광자수상태(definite photon number state), OAM(orbital angular momentum), 편광-경로 혼합, 타임 빈(time-bin) 등이 있다. 각각의 방법은 다양한 물리적 속성을 활용하여 양자 상태를 다차원으로 확장할 수 있으며, 그에 따라 정보 전송 효율이 향상된다. 예를 들어, OAM 방식은 광자의 궤도 각운동량을 활용하여 다차원 상태를 만들 수 있고, 타임 빈 방식은 광자의 도착 시간을 사용해 신호를 전송할 수 있으며, 장거리 전송에서 특히 유리하다.

24. 양자통신을 위한 양자 상태 측정 (Quantum State Measurement for Quantum Communication)

측정 장치는 다양한 물리 정보를 추출하고 이를 분석하거나 제어하는데 필수적인 역할을 한다. 특히 양자 통신에서는 단일 광자 수준의 양자 상태를 측정해야 하기 때문에 측정장치의 성능이 아주 중요하다. 광자를 정확히 감지하는 측정 효율, 얼마나 짧은 시간에 신호를 측정하고 결과를 출력할 수 있는지, 광자가 검출된 시간의 정확성, 잡음 내성, 높은 fidelity, 그리고 광자 수 분해능(resolution) 등이 검출기의 성능을 결정한다. 성능이 좋은 검출기를 통해 양자 통신의 통신 거리를 늘릴 수 있고, 낮은 오류율과 높은 키 생성률에 도달할 수 있다.

24-1. 단일 광자 검출기 (Single Photon Detector, SPD)

단일 광자 검출기는 단일 광자를 측정하는데 특화되어 있는 장치로 대표적으로 SPAD(single photon avalanche diode)와 SNSPD(superconducting nanowire single photon detector)등이 있다.

SPAD는 애벌랜치 효과(avalanche effect)를 통해 미약한 신호를 소자 내부에서 증폭하여 단일 광자를 검출하는 매우 민감한 소자이다. SPAD는 소재에 따라 성능과 특성이 달라지며, 대표적으로 실리콘(Si)과 인듐 갈륨 비소(InGaAs) 소재가 많이 사용된다. 실리콘 SPAD는 400nm에서 1000nm 사이의 파장 범위에서 높은 성능을 발휘하며, 가시광선 영역에서 주로 사용된다. 실리콘 SPAD는 상온 동작이 가능하며, 낮은 동작 전압, 높은 신호 대 잡음비(signal to noise rate, SNR), 높은 탐지 효율, 그리고 저렴한 비용 등의 여러 가지 장점이 있다. 그러나 1000nm 이상의 적외선 영역에서는 성능이 크게 저하되므로, 유선 통신에 주로 사용되는 1550nm의 적외선 통신 파장에서 사용하기에는 적합하지 않다. InGaAs SPAD는 900nm에서 1700nm의 파장 범위에서 높은 성능을 발휘하며, 특히 1550nm의 적외선 통신 파장에서 주로 사용된다. InGaAs SPAD는 적외선 대역에서 실리콘 SPAD에 비해 뛰어난 탐지 효율을 제공하므로, 유선 양자 통신에 필수적이다. 그러나 InGaAs SPAD는 아직 최대효율이 30%내외이며, 높은 다크 카운트, 낮은 신호 대 잡음비(SNR), 높은 동작 전압, 그리고 비싼 제조 비용 등의 단점이 있다.

SNSPD는 나노 크기의 초전도 와이어를 이용해 단일 광자를 검출하는 방식으로 동작한다. 빛이 와이어에 흡수되면 와이어의 초전도 상태가 깨지면서 저항이 발생하고, 이를 통해 광자를 감지하는 방식이다. SNSPD는 높은 검출 효율, 높은 정확도, 잡음 내성의 특징을 가지고 있지만, 매우 낮은 온도(2~4K)에서만 동작하는 제약이 있다.

24-2. Photon Number Resolving (PNR) 검출기

PNR 기능이 있는 검출기는 단일 광자 뿐만 아니라, 여러 개의 광자를 동시에 감지하고 그 광자수를 정확하게 측정할 수 있는 고성능 검출기이다. 일반적인 단일 광자 검출기는 광자의 유무만을 감지할 수 있지만 PNR 검출기는 광자수를 측정할 수 있기 때문에 양자 정보 처리나 양자 통신 등의 분야에서 매우 중요한 역할을 한다. 이 기술을 구현하는 대표적인 장치로는 transition edge sensors(TES)와 microwave kinetic inductance detectors(MKID)등이 있다.

TES는 초전도체를 이용하여 단일 광자 및 다광자를 감지하는 검출기로, 초전도 상태에서 전도 상태로 전이할 때의 미세한 온도 변화를 이용한다. 온도가 상승하면 저항이 0에서 변화하는데 이때 저항 변화는 광자의 에너지와 비례하므로, 들어온 광자의 수를 측정할 수 있다. 하지만 극저온 환경(~10mK)에서 작동해야 하므로 기술적으로 비용이 많이 든다.

MKID는 마이크로파 영역에서 작동하는 초전도 검출기로 광자 수를 정확하게 측정할 수 있는 검출기이다. 광자가 초전도체에 입사할 때 초전도체의 유도성(inductance)가 변하는데, 광자의 수에 따라 유도성 변화가 달라지기 때문에 이를 통해 광자수를 감지할 수 있다. MKID는 TES에 비해 빠른 응답속도를 가지고 있지만 마찬가지로 극 저온 환경에서 작동한다.

최근에는 SNSPD에 PNR 기능을 추가한 검출기가 연구되고 있다. 기존의 SNSPD는 여러 광자가 동시에 검출기에 도달하면 이를 구분하지 못하고 단일 광자 이벤트로만 인식하는 한계가 있다. 그러나 PNR기능이 추가된 SNSPD는 동일한 검출 픽셀에 여러 광자가 동시에 도달하는 확률을 최소화하는 방향으로 광자수를 측정할 수 있도록 설계된다. 이 기능은 주로 temporal multiplexing 방법과 spatial multiplexing 방법을 통해 구현된다.

1. Temporal Multiplexing (시간 다중화)

이 방법은 시간적으로 들어온 광자 간에 지연을 가해, 각각의 광자를 구분한다. 이를 위해 긴 광섬유를 이용해 광자 신호를 시간 차이로 분리하는데, 이 과정에서 시스템의 부피가 커지고 복잡해지는 단점이 있다.

2. Spatial Multiplexing (공간 다중화)

이 방법은 검출 픽셀을 증가시켜 여러 광자를 개별적으로 감지하는 방식이다. 그러나 광자수가 증가할수록 더 많은 픽셀이 필요하며, 검출기에서 생성되는 전기신호가 점점 커지다가 포화상태에 이르게 된다. 이때 더 많은 광자가 들어오면 추가 신호를 생성하지 못하고 신호 대 잡음비(SNR)가 감소하는 한계가 있다.

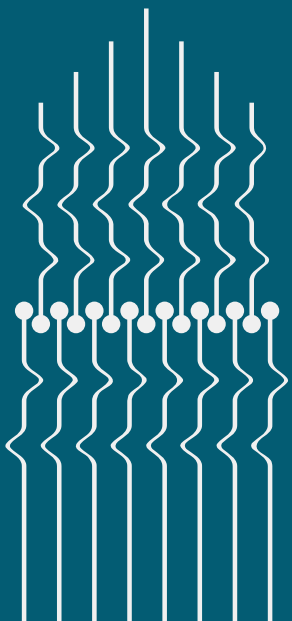
3. Spatiotemporal Multiplexing (시공간 다중화)

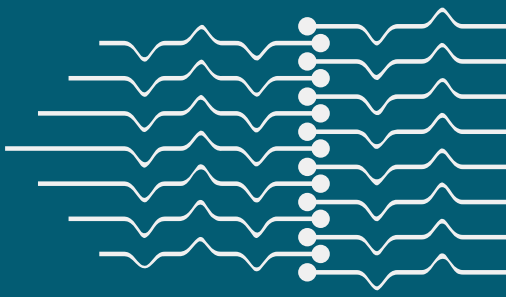
이 방법은 temporal multiplexing과 spatial multiplexing을 결합한 방식으로, 광자 신호에 지연을 주면서 동시에 픽셀 수를 증가시켜 다중 광자를 보다 효과적으로 구분할 수 있다.

25. 양자 내성 암호 (Post Quantum Cryptography, PQC)

양자 내성 암호는 양자 암호와 마찬가지로, 양자 컴퓨터의 개발 및 발전에 따라 안전성이 위협받고 있는 현대암호 체계의 문제를 해결하기 위한 또 하나의 방법이다. 양자 내성 암호는 양자 통신 채널 또는 양자 신호를 사용하지 않고, 기존의 통신 및 네트워크 인프라에서 구현 가능하며, 현재 사용 중인 인터넷과 호환이 된다. 따라서 양자 내성 암호는 양자 암호보다 쉽게 구현이 가능하며, 현재의 보안 시스템에 쉽게 도입할 수 있다. 하지만, 물리적 법칙에 의존하여 무조건적으로 안전성을 제공하는 양자 암호와는 다르게 양자 내성 암호는 수학적 복잡도를 기반으로 하여 안전성을 보장하므로 안전성 측면에서는 한계가 있다. 양자 내성 암호 알고리즘은 양자 컴퓨터가 개발되어도 쉽게 풀 수 없는 수학적 문제이며, 이러한 수학적 복잡성을 이용하여 보안을 유지한다. 대표적으로 격자 기반 암호화(lattice-based cryptography), 해시 기반 암호화(hash-based cryptography), 다항식 기반 암호화(code-based cryptography) 등이 있다.

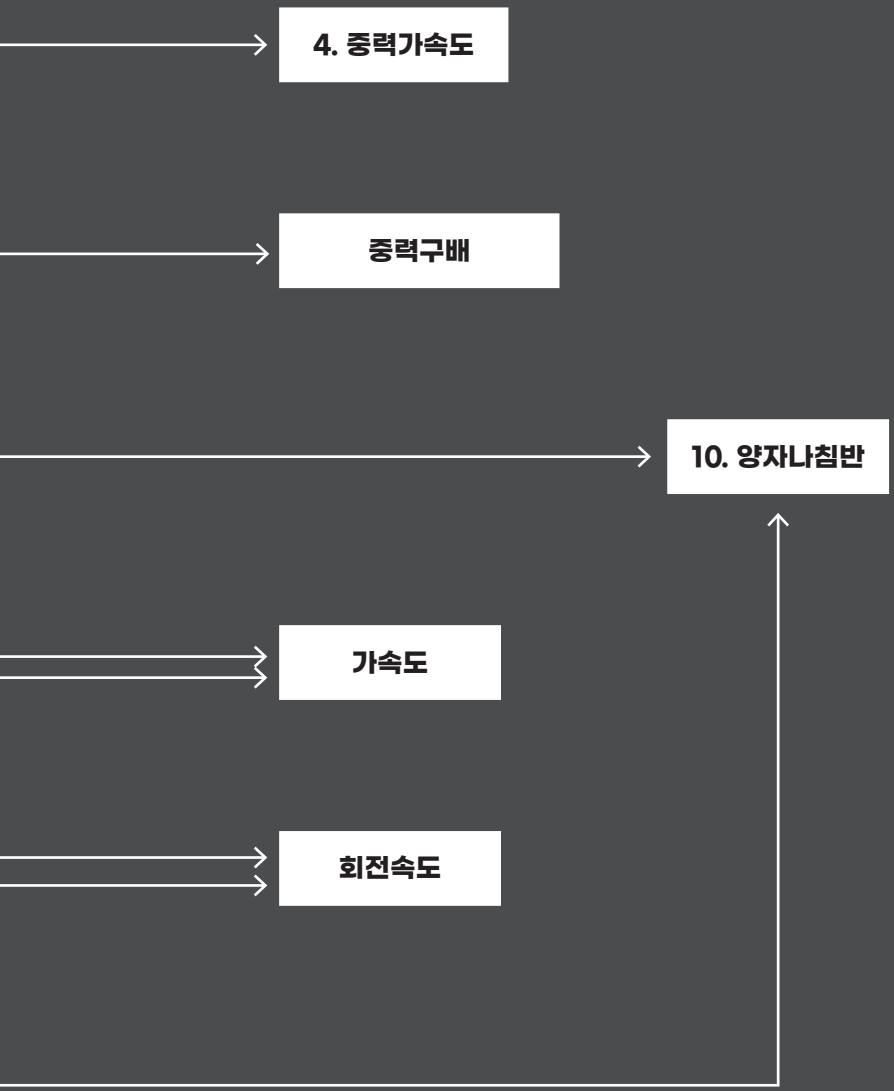
2. 양자센싱





양자관성센서 용어 MAP

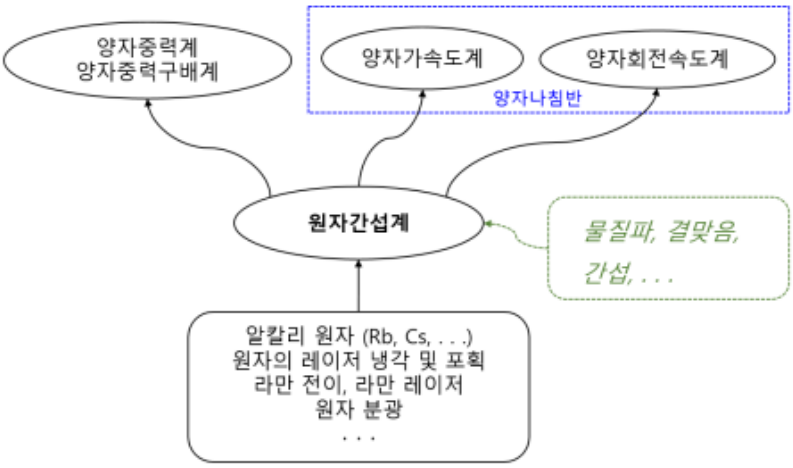
* 용어MAP은 분류체계에 따라 제시하였으나 지면의 한계로 인하여 일부만 교재에 담았습니다.
* 형광색 박스는 중요 기반 기술 또는 관련 기술을 의미합니다.


4. 중력가속도
중력구배
10. 양자나침반
가속도
회전속도

1. 양자관성센서

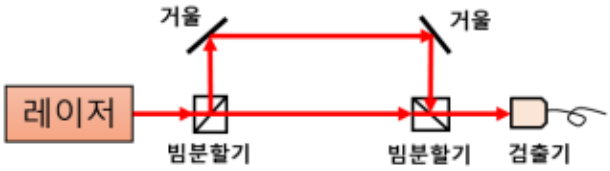
양자관성센서는 중력, 가속도, 회전속도 등의 물리량을 얽힘, 압축, 간섭, 결맞음 등의 양자 현상을 이용하여 측정하는 센서를 말한다. 양자관성센서는 국방분야, 자동차 자율주행 등의 분야에서 고정밀 관성항법이나 지문항법을 위한 센서로 활용 가능하다. 양자관성센서는 가속도센서(중력 및 중력구배 센서 포함)와 회전센서(자이로스코프, 또는 자이로라고 불리기도 함)로 분류할 수 있으며, 센서의 종류는 아래 그림과 같다.

특히, 원자간섭계는 양자중력계, 양자가속도계, 양자회전센서(또는, 양자자이로)의 기반이 되는 기술이며, 이 기술을 이용하는 양자관성센서는 기본의 관성센서의 성능한계를 뛰어넘는 센서로 연구되고 있다. 원자간섭계를 이용하면, 한 개의 센서시스템에서 가속도와 회전을 동시에 측정하는 센서를 만들 수 있는데, 이를 양자나침반(Quantum compass)이라고 부르기도 한다 (아래 그림 참조).



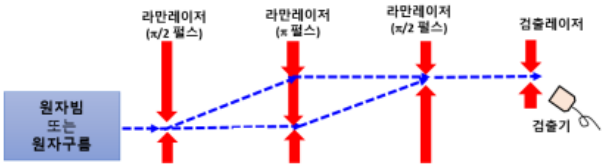
2. 원자간섭계

원자간섭계는 원자의 물질파 특성을 이용하여 간섭현상을 발생시키기 위해 구성되는 장치 또는 시스템을 말한다. 레이저를 이용하는 광학간섭계과 비교하면, 원자간섭계에서는 빛과 물질이 서로 반대로 바뀐 역할을 한다. 광학간섭계에서는 레이저 빔분할기를 이용하여 레이저 빔을 두 개로 나누고, 거울과 빔분할기를 이용하여 나눈 두 빔을 다시 합치도록 하여 간섭계를 구성한다.



[레이저 기반의 광학간섭계]

원자간섭계에서는 레이저를 이용하여 원자빔(또는 원자구름)을 분할하거나 반사하여 간섭계를 구성한다.



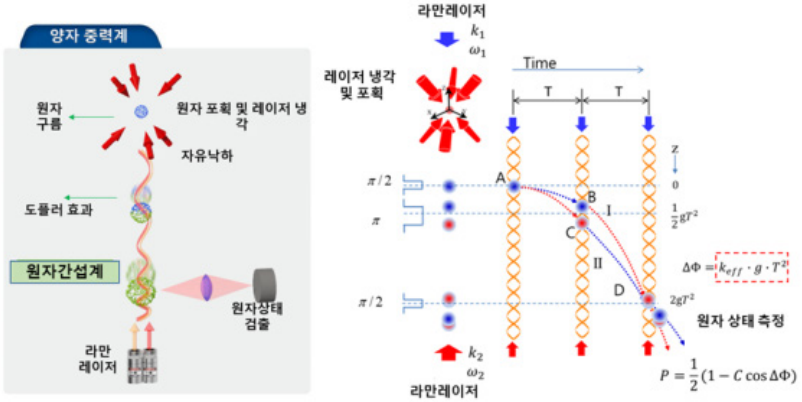
[원자간섭계]

라만레이저는 두 개의 레이저로 구성되어 원자와 상호작용하는 시간을 조절하여 원자의 전이율을 조정할 수 있다. 라만레이저의 펄스폭을 조절하여 원자빔 (또는 원자구름)을 분할하거나 방향을 바꿀 수있다. 이렇게 하여 위 그림과 같이 원자간섭계를 구성할 수 있다.

3. 양자중력센서

양자중력센서(양자중력계)는 양자 간섭 현상을 이용하여 중력가속도를 측정하는 센서로 원자간섭계 기반의 양자중력계와 초전도 현상을 이용한 양자중력계가 있으나, 국제적으로 원자간섭계 기반의 양자중력계만을 의미하는 용어로 사용하기도 한다. 본 용어집에서도 원자간섭계 기반의 양자중력계로 국한하여 기술한다.

양자중력계는 원자를 레이저 냉각 및 포획한 후 레이저를 이용하여 원자구름을 위로 쏘아올리거나, 또는 자유낙하시킨다. 그러면 원자는 중력에 의해 힘을 받아 아래로 떨어진게 된다. 이때, 떨어지는 원자 구름에 중력 방향으로 원자간섭계를 구성하면, 두 경로의 원자 구름에 의한 원자간섭신호는 중력가속도에 의한 영향을 포함하게 되고, 적절한 신호 처리를 통해 중력가속도를 산출할 수 있다. 즉, 이와 같이 양자중력계는 원자간섭계를 이용하여 중력가속도를 측정한다.



[양자중력계 개념도 및 원리]

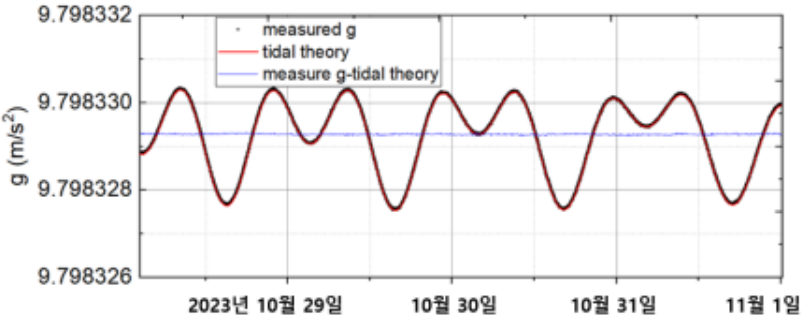
4. 중력가속도

지구와 물체간의 만유인력 상호작용으로 서로 끌어당기게 된는데, 이때 떨어지는 물체의 가속도를 중력가속도라 한다. 뉴튼의 만유인력 법칙은 질량을 가진 두 물체는 서로 끌어당기게 되고, 이때 끌어당기는 힘은 두 물체의 질량에 비례하고 거리에 제곱에 반비례한다. 지구의 질량을 M, 떨어지는 물체의 질량을 m, 지구 중심과 물체 중심 사이의 거리를 r 이라고 하면, 서로 끌어당기는 힘 F 는 다음과 같이 표현된다.

$$F = G\frac{mM}{r^2} = mg$$

위 식에서 G 는 중력상수 또는 만유인력 상수라고 하고, 중력가속도 g 는 $g=GM/r^2$ 이 된다.

실제 중력가속도는 여러 가지 영향을 받아 바뀌게 된다. 대표적인 것이 달과 태양에 의한 중력가속도의 변화이다. 지구가 태양 주위로 자전 및 공전하고, 달이 지구 주위를 공전하므로, 중력가속도는 하루 주기의 변화, 대략 한달 주기의 변화, 그리고 일년 주기의 변화를 가지게 된다. 또한, 지구 자전축의 변화, 달의 인력에 의한 조수 간만, 지구 내부의 질량 분포, 대기압, 대기의 수증기량 등 다양한 요인에 의해 달라지게 된다.

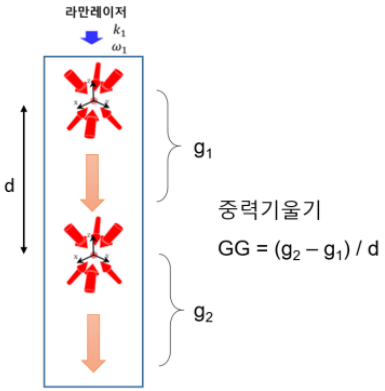


[한국표준과학연구원 실험실에서 측정한 중력가속도]

5. 양자중력구배센서

중력구배는 중력가속도의 기울기를 나타내는 양인데, 단위는 E(에트뵈스)이다. 에트뵈스(Eötvös)는 헝가리 물리학자의 이름에서 따온 것이며, 1 E는 거리가 1 m 떨어진 두 지점사이의 중력차이가 1 nm/s^2 일때를 말한다.

양자중력구배센서는 두 개의 동일한 양자중력계를 일정한 거리를 두고 하나의 시스템내에 구성하고 원자를 레이저 냉각하는 레이저와 원자간섭계를 구성하는 레이저 등을 모두 공유하게 한 후 동시에 중력측정이 이루어지도록 동작시키는 센서이다. 두 지점에서 측정된 중력값의 차이는 진동 잡음이나 레이저 잡음 등의 공통잡음이 상쇄되게 된다. 이렇게 함으로서 보다 중력가속도 변화를 보다 민감하게 감지할 수 있고, 진동 등의 환경이 좋지 않은 상황에서도 동작이 가능하게 된다.

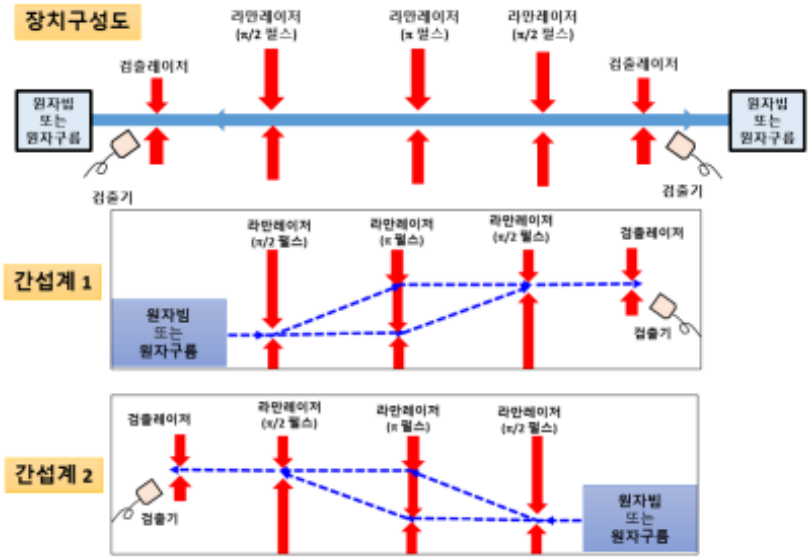


[양자중력구배센서 개념도]

6. 원자간섭계 양자가속도센서

원자간섭계 기반의 양자가속도센서는 양자중력계와 같은 원리가 적용된다. 중력가속도는 가속도의 한 종류이며, 중력에 의해 발생되는 가속도이므로 가속도의 방향이 중력 방향과 일치한다. 일반적으로 가속도는 물체에 가해지는 힘의 방향으로 발생하므로 모든 방향의 성분을 가질 수 있다.

가속도센서에서는 중력계와 달리 원자를 임의의 방향으로 움직이게 하고, 움직이는 방향으로 간섭계를 구성하면 원자의 운동방향의 가속도를 측정하게 된다. 실제적으로는 움직이는 방향으로 간섭계 구성이 힘들므로, 서로 반대방향으로 움직이는 원자빔 또는 원자구름을 생성하고 운동방향의 수직방향으로 2 개의 간섭계를 구성한다. 그리고 두 간섭계 신호로부터 가속도 성분을 추출하게 된다.

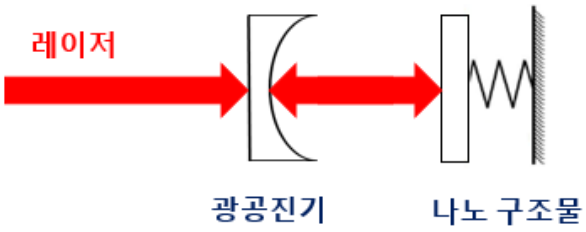


[원자간섭계 양자가속도센서 개념도]

항법에서는 3 축 방향의 가속도를 모두 알아야 가능하므로 3 개의 가속도 센서로 구성된 시스템을 이용한다.

7. 광역학계 양자가속도센서

광역학계 양자가속도센서는 가속도에 의해 발생되는 나노 구조물의 위치 변화를 부착된 초소형 광공진기를 이용하여 측정하고 이로부터 가속도를 측정하는 센서이다. 일반적으로 광역학계는 광공진기와 나노 구조물로 구성되는데, 광공진기의 공명조건과 나노 구조물의 위치간의 광역학적 상호작용을 이용한다.



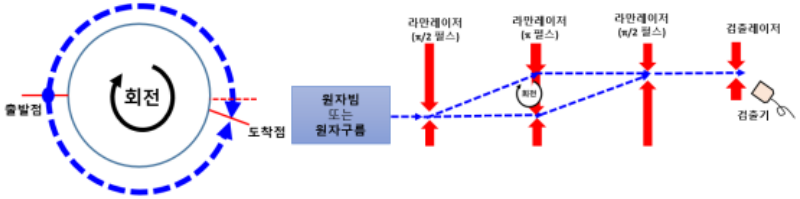
[광공진기 광역학계 개념도]

가속도가 작용하게 되면 나노 구조물의 위치가 변하게 되고, 따라서 광공진기의 공명주파수가 변하게 된다. 광공진기에서 반사 또는 투과되는 레이저의 주파수 변화를 측정하여 변위를 측정하고, 이 변위로부터 가속도를 알 수 있게 된다.

광역학계 양자가속도계에서는 광공진기와 MEMS 기술을 이용하여 초소형의 역학계와 광공진기를 만들어 미세한 힘 즉, 미세한 가속도를 감지할 수 있도록 제작한다. 또한, 압착광을 이용하거나 양자간섭계를 구성하여 민감도를 향상시키는 연구도 시도되고 있다.

8. 원자간섭계 양자회전센서

원자간섭계 양자회전센서는 물체의 회전할 때 원자간섭계의 두 빔의 경로가 달라지는 달라지는 효과를 이용하여 회전속도를 측정하는 센서이다. 광학 회전속도계(또는 과학 자이로)의 샤냑 효과(Sagnac effect)와 유사하게, 두 개 경로로 나누어진 원자빔이 물체의 회전방향에 따라 다른 영향을 받아 원자간섭계 신호에 회전 성분이 나타나게 되는 원리를 이용한다.

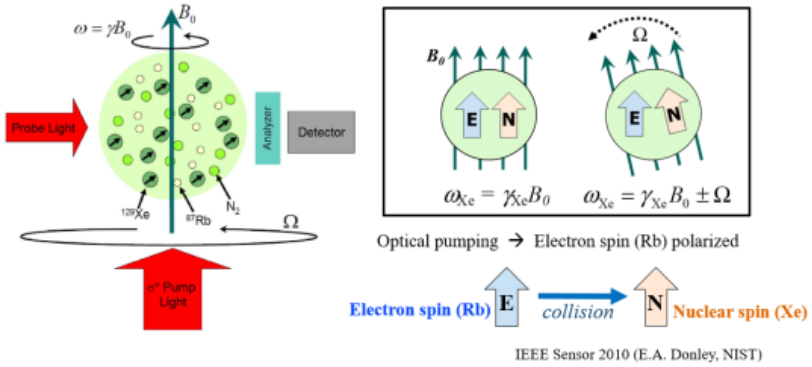


물체의 위치를 계속 추적하는 항법은 3 축 방향으로 회전속도를 모두 알아야 가능하므로 3 개의 회전속도계로 구성된다.

참고로 회전속도센서는 자이로스코프 또는 줄여서 자이로라고 불리기도 한다.

9. 원자스핀 양자자이로

원자의 스핀을 이용하여 회전속도를 측정하는 장치를 원자스핀 자이로스코프라고 한다. 원자스핀 자이로는 알칼리 원자(Cs, Rb, K 등)와 비활성 기체 원자(Xe 등), 그리고 원자셀에는 벽면과의 충돌 등을 막기 위해서 버퍼가스 등이 들어있는 원자셀을 이용한다. 레이저를 이용하여 알칼리 원자의 스핀을 정렬하면, 원자간 충돌에 의해 알칼리 원자의 스핀이 비활성 기체 원자(Xe 등)의 핵스핀에 전달된다. 이때 원자셀에 일정한 자기장을 가해주면 정렬된 핵스핀은 자기장축 방향 중심으로 세차 운동을 하게 된다. 핵스핀은 가해준 자기장의 세기에 따라 고유의 주파수를 가지고 세차운동을 하게 되는데, 이때 가해준 교류 자기장의 주파수가 세차 운동의 주파수와 일치하면 자기공명이라는 공명현상이 나타난다. 물체의 회전속도에 따라 달라지는 세차운동 주파수를 자기공명을 이용하여 측정하면, 이로부터 물체의 회전속도를 추출할 수 있다. 이와 같이 원자스핀 자이로(ASG)는 핵스핀과 자기공명을 이용하기 때문에 핵자기공명자이로(NMRG)라고 부르기도 한다.



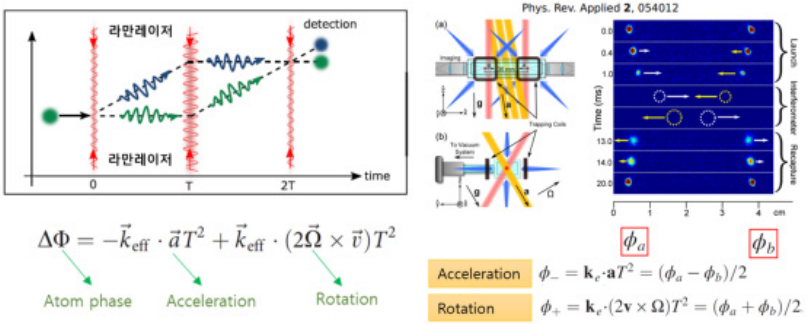
[원자스핀 자이로 동작 원리]

10. 양자나침반

원자간섭계 기술을 이용하여 가속도와 회전속도를 동시에 측정하여 위치를 알아내는 사용되는 장치를 양자나침반이라고 부른다. 2018년 영국 Imperial College London과 M Squared 사에서 처음으로 “Quantum Compass”라는 용어를 사용하였고, 이를 한국어로 번역한 것이 양자나침반이다.

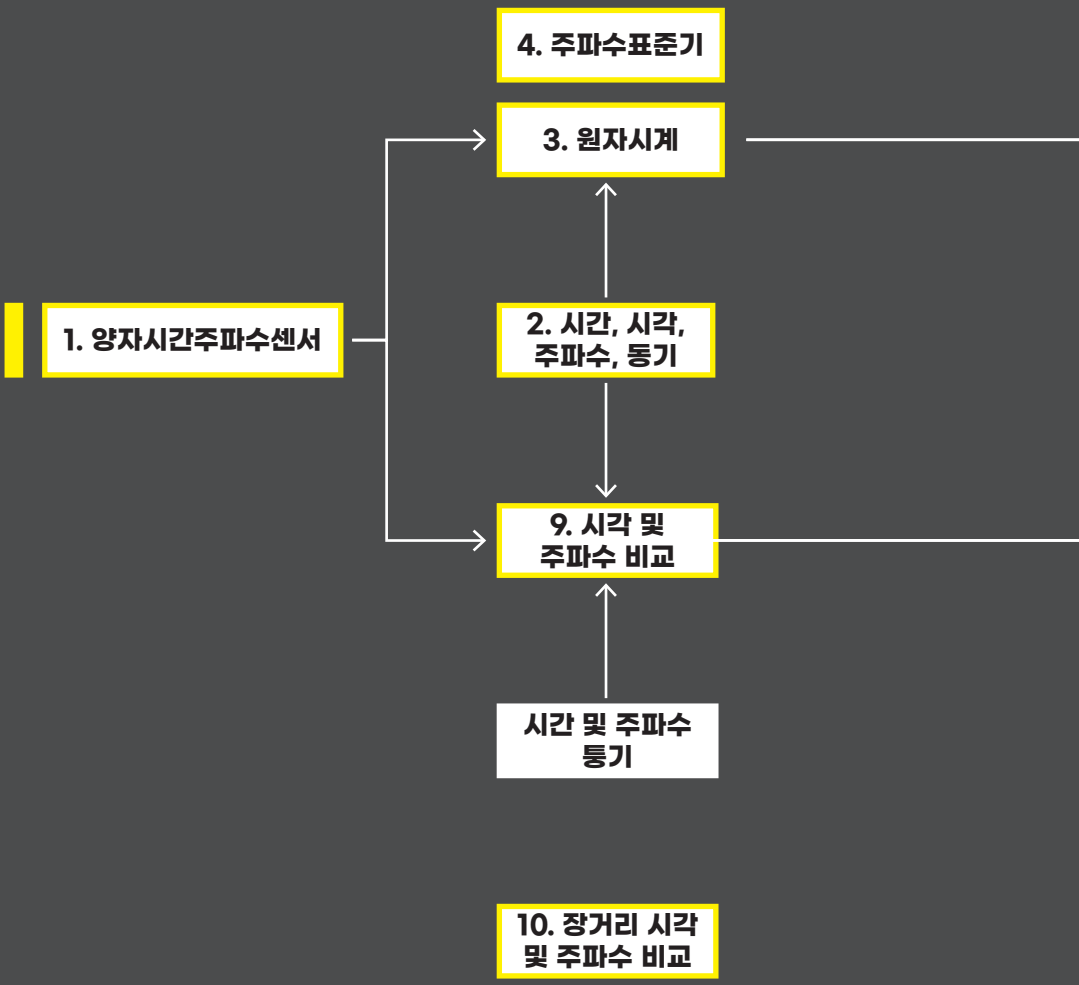
하나의 시스템에 2 개의 원자간섭계를 적절히 구성하면 가속도와 회전속도를 동시에 측정하는 것이 가능하다. (용어 “원자간섭계 양자가속도센서”에 있는 개념도 참조) 두 개의 간섭계로부터 측정된 두 신호를 서로 더하면 회전속도 성분만 남게 되고, 빼면 가속도 성분만 남게 구성할 수 있다. 즉. 측정된 2 개의 원자간섭신호부터 가속도와 회전을 동시에 추출하는 것이 가능하다.

그림에서 예시는 미국 Sandia National Lab.에서 레이저 냉각된 원자를 서로 마주 보는 방향으로 원자 구름을 발사하고 원자 운동의 수직 방향의 라만레이저로 원자간섭계를 구성하여 가속도와 회전속도를 동시에 측정한 것을 보여준다.



[양자나침반 동작원리]

양자시간주파수센서 용어 MAP



* 용어MAP은 분류체계에 따라 제시하였으나 지면의 한계로 인하여 일부만 교재에 담았습니다.


마이크로파원자시계
광펌핑원자시계
원자분수시계
소형 원자시계
5. 초소형원자시계
7. 광빗
광주파수합성기
6. 광시계
중성원자광시계
이온광시계
이동형광시계
소형광시계
8. 핵시계
단방향 비교
단파 및 장파 방송
위성신호 수신
동시수신 비교
항법위성 동시수신
LORAN 동시수신
양방향 비교
양방향 위성 비교
광섬유 이용 비교

1. 양자시간주파수센서

양자시간주파수센서는 시간 및 주파수의 발생, 측정, 동기화 등을 구현하는 원자시계, 칩스케일 원자시계, 광주파수 합성기 등을 말하는데, 시각, 시간 간격, 주파수의 세 가지의 시간 관련 정보를 발생시키거나 측정하는데, 그리고 동기하는데 사용된다.

양자시간주파수센서는 방송, 통신, 국방분야, 첨단 산업 등 당양한 분야에 필수적인 시각 및 주파수를 공급하는 것 뿐만 아니라, 일상생활을 하는 모든 사람들에도 필수적인 것이라고 할 수 있다.

2. 시간, 시각, 주파수, 동기

일반적으로 시간(time)은 시각(time-of-day)과 시간간격(time interval)의 의미가 혼용되어 있다. “우리는 9시 정각에 출발하여 9시 31분에 도착하여 이동에 31분이 걸렸다”라는 예시에서 ‘9시’와 ‘9시 31분’은 각각 출발과 도착의 시점(시각)을 가리키고, ‘31 분’은 두 시점사이의 시간적인 거리(시간간격)를 말한다.

시계는 일정한 주기의 신호를 발생시키는 장치로 특정 시점을 지정하는 시각을 측정하는 센서로도 사용된다. 또한 시계는 일정한 시간간격을 발생시키는 장치로 사용될 수도 있고, 시간간격을 측정하는 장치로도 사용될 수 있다.

다시 말하면, 시계는 시각 및 시간간격을 만들기 위해 일정한 신호를 만들어내는 주파수발생기의 한 종류이며, 시각 및 시간간격을 측정하는 장치이다. 주파수발생기는 특정한 주기적인 신호를 발생시키는 장치인데, 이때 반복되는 신호의 시간적인 길이(시간간격)를 주기라고 하고, 주파수는 주기의 역수(즉, 주파수 = 1 / 주기)이다.

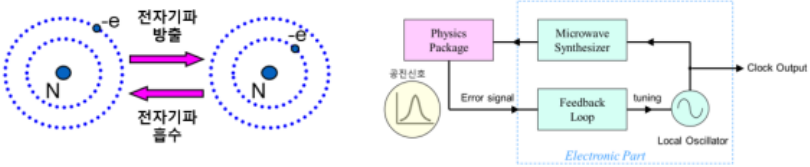
시각 및 시간간격은 필수적으로 동기라는 조건이 필요하다. 어떤 사람 A가 다른 사람 B에게 시각이나 시간간격을 말하면, B에게도 A와 같은 시각이나 시간간격이 되어야 한다. 이와 같이 되도록 하는 것이 시각동기, 시간간격

동기라고 한다. 일정하게 반복되는 시간간격의 경우. 주기(시간간격)의 역수가 주파수이므로 이때 시간간격 동기는 주파수 동기와 같은 의미로 사용될 수 있다.

3. 원자시계

시계는 일정하게 반복되는 현상을 이용하여 일정한 주기신호발생시키는 장치, 즉 주파수발생기이다. 태양의 일정한 반복운동(실제로는 지구의 자전과 공전)을 이용하는 해시계, 추의 반복운동을 이용하는 진자시계, 수정결정의 일정한 진동을 이용하는 수정시계 등이 있으며, 원자시계는 원자를 이용하여 일정한 주기의 신호를 발생시키는 장치이다.

원자는 빛이나 마이크로파와 같은 전자기파를 흡수하거나 방출할 때 특정한 주파수의 전자기파를 흡수하거나 방출한다. 원자는 핵과 전자로 이루어져 있고, 핵 주변에 분포하는 전자는 여러 에너지 준위를 가지는데, 이 에너지 준위는 연속적이지 않고 불연속적으로 떨어져 있다. 원자가 전자기파를 흡수하거나 방출할때는 한 에너지 준위에서 다른 에너지 준위 사이에 해당하는 주파수 가진 전자기파만을 흡수 또는 방출한다. 원자시계는 이를 이용하는데, 로컬 주파수발진기로 신호를 만들어 원자에 보내고 흡수 또는 방출이 최대가 되는 공명현상이 발생하도록 로컬발진기의 주파수를 되먹임하면 로컬발진기의 주파수는 원자의 고유 주파수와 일치하게 된다. 이렇게 만들어진 주파수발생기가 원자시계이다.



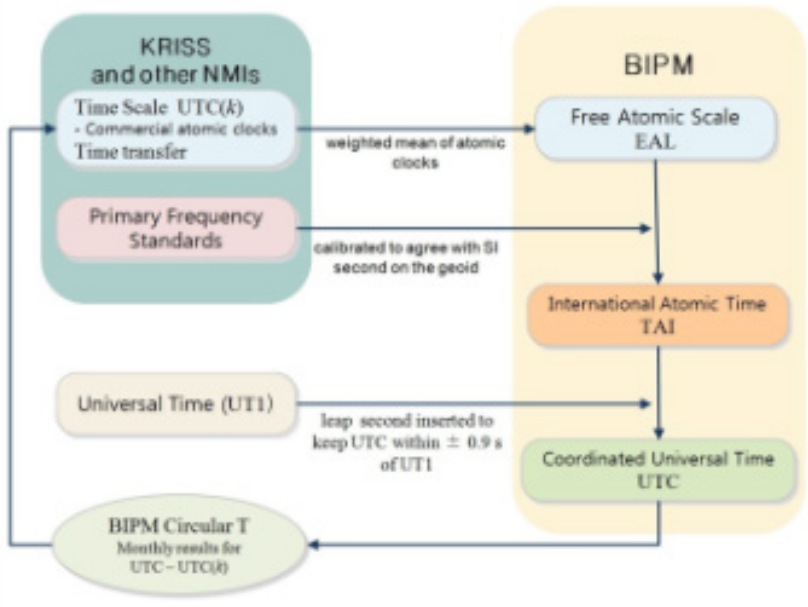
[원자시계 개념도]

4. 주파수표준기

주파수표준기는 고정밀 시계로 크게 두 가지 의미로 사용된다. 첫째는 정확도 및 정밀도가 높아 다른 시계의 기준이 되는 것을 시계를 지칭한다. 통신이나 방송의 경우 많은 시계(주파수발생기)들이 사용되는 이때 제 1 계위에 사용되거나 다른 시계를 보정하는데 사용되는 시계를 주파수표준기 또는 주파수기준기라고 한다.

두 번째는 시간의 기본 단위인 s(second, 초)를 실현하는 장치로 국제원자시, 세계협정시, 국가표준시를 발생 및 유지하는데 사용되는 시계를 주파수표준기 또는 1차 주파수표준기라고 한다. 1차 주파수표준기는 정확도가 10^{-15}~10^{-19} 으로 가장 정밀한 측정장치로 기본물리상수, 일반상대성 이론 검증, 지구 지오이드 측정 등의 기초과학 분야가 이용되며, 길이, 질량, 전류 등의 다른 물리량의 측정에도 사용된다.

주파수표준기로는 현재의 초의 정의를 실현하는 광펌핑 원자시계, 원자분수시계 등이 있으며, 차세대 초의 정의에 이용될 것으로 기대되는 광시계 등이 있다.



[1차 주파수표준기의 역할]

5. 초소형원자시계

원자시계는 여러 종류가 있지만, 특히 MEMS 기술을 이용하여 초소형이면서 저전력인 시계를 초소형원자시계하고 한다.

[원자시계의 종류]

초소형원자시계는 MEMS 기술을 이용하여 원자증기셀을 1 mm 수준의 크기로 제작하고, VCSEL이라는 저전력의 반도체 레이저를 이용하므로 대체로 크기가 수십 cm^3, 소모전력이 1 W 이하이다. 최근에는 크기가 수 cm^3 수준인 초소형 원자시계를 개발하려는 연구도 시도되고 있다.

MEMS 기술로 제작된 원자셀에는 Cs 또는 Rb 원자가 들어 있으며, 원자의 벽면과 충돌을 줄이기 위한 버퍼가스가 일정한 압력으로 함께 들어있다. VCSEL를 원자의 에너지 준위 차이에 해당하는 주파수로 변조하여 원자셀을 지나게 하면 결맞음밀도포획(CPT 현상)에 의해 좁은 선폭의 원자 공진 신호를 얻을 수 있는데, 초소형원자시계에서는 이 원리를 이용한다.

6. 광시계

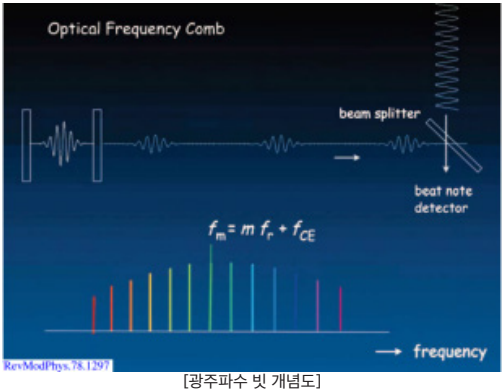
원자시계는 원자의 특정한 두 에너지 준위 사이의 전이(시계전이)를 이용하는데, 주로 사용되고 있는 세슘 원자나 루비듐 원자, 수소 원자 등의 경우 시계전이선의 주파수는 마이크로파 영역에 속한다. 광시계는 시계전이선의 주파수가 광주파수 영역인 원자시계를 말한다. 광시계가 개발되면서 기존의 마이크로파 전이를 이용하는 원자시계를 마이크로파 원자시계, 광전이를 이용하는 원자시계를 광시계로 분류하고 있다. 광시계에는 중성원자를 이용하는 중성원자 광시계(주로 광격자 시계)와 이온 광시계가 있다.

이용되는 광주파수는 마이크로파 원자시계에 사용되는 주파수 보다 10^4~10^5 배 크므로 광시계는 그 만큼 더 정확할 수 있다. 현재의 시간의 단위인 초의 정의는 세슘원자를 기반으로 하고 있는데, 가까운 미래에 광시계를 기반으로 하는 새로운 초의 정의로 바뀔 것으로 기대되고 있다.

중성원자 광시계는 스트론튬, 이터품 등의 중성 원자를 레이저에 의해 만들어진 격자 모양의 포덴셜인 광격자에 포획하여 사용하고, 이온 광시계는 알루미늄, 수은, 이터븀, 인듐, 칼슘 등의 이온을 전기장과 자기장으로 포획하여 사용한다. 광격자 시계는 여러 개의 원자를 이용하는 장점을, 이온 광시계는 장시간 안정적으로 포획된 이온을 이용하는 장점을 가지고 있다. 중성원자 광시계와 이온 광시계의 정확도는 10^{-17}~10^{-19} 수준으로 아직 연구가 활발히 진행되는 단계이며, 두 종류의 광시계간의 세계 최고 정확도 순위는 계속 바뀌고 있다.

7. 광빗, 광주파수합성기

모드 잠금 레이저를 이용하여 펄스폭이 펨토초(10-15 s)인 펄스열을 발생시키고, 이 펄스를 주파수 영역에서 보면 일정한 간격의 주파수 성분이 마치 빗처럼 나열된 모양으로 나타나게 되는데, 이를 광주파수 빗 또는 줄여서 광빗이라 한다.



[광주파수 빗 개념도]

광빗에서 두 개의 주파수(옵셋주파수와 반복주파수)를 조정하여 일정하게 유지하면 광빗중 하나를 원하는 주파수로 만들 수 있다. 이렇게 광주파수를 원하는 주파수로 만들게 되면 광주파수영역에서 주파수를 합성하는 광주파수합성기로 사용할 수 있게 된다. 특히, 광빗의 옵세주파수와 반복주파수를 광시계 등을 이용하여 일정하게 유지하면, 광빗의 모든 빗은 각각 광시계에 소급되어 절대값(절대주파수)을 가진 광주파수 빗으로 사용할 수 있게 된다.

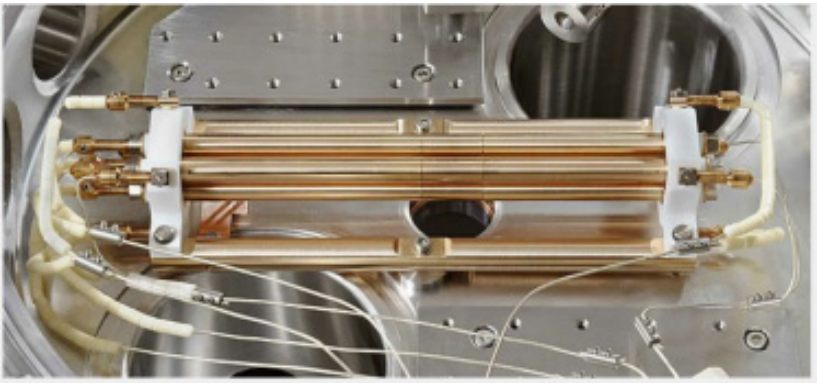
특히, 광빗은 현재 초의 정의인 세슘 원자의 마이크로파 주파수와 광시계의 광주파수를 연결하기 위해서는 여러 단계의 복잡한 시스템으로 연결이 가능했던 것을 높은 정밀도로 직접 연결하는 것이 가능하도록 하는 중요한 역할을 하고 있다.

8. 핵시계

핵시계는 핵광시계라고 불리며 원자시계의 한 종류이다. 핵시계에서 이용되는 시계전이선은 원자핵의 에너지 준위사이에 일어나는 전이이다. 핵시계는 광시계는 보다 높은 주파수의 시계전이선을 이용하므로 더 정확한 원자시계가 될 수 있다. 또한, 원자의 핵은 전자에 의해 둘러싸여 있어 외부 환경의 영향을 적게 받으므로 핵시계는 현재의 광시계 보다 더 정확한 시계가 될 것으로 기대되고 있다.

핵시계에 이용될 수 있는 원자는 ^{229}Th 이 대표적이며, 결정에 Th 원자를 도핑하여 이용하거나, 이온 포획 방법으로 Th 이온을 포획하여 이용한다. 이때 이용되는 시계전이선의 파장은 200 nm 보다 작은 VUV(Vacuum UltraViolet) 영역이다.

이온 포획 방법을 이용하여 $^{229}Th^{3+}$ 이온을 한 개 또는 여러개의 체인 형태로 포획하여 이용하는 시계를 이온 포획 핵시계라고 한다. 고체에 Th을 도핑하여 이용하는 방식의 시계를 고체 핵시계라고 하는데, 이 경우 많은 수의 Th 원자를 이용할 수 있는 장점이 있는 반면, 주위의 있는 다른 원자나 원자핵의 영향을 받는 단점이 있다.



[독일 PTB의 229Th 이온 포획 장치]

9. 시각 및 주파수 비교

서로 다른 장소에 있는 시각 및 주파수를 비교 또는 동기하는 것을 의미하는데, 비교를 위해 시각 및 주파수를 한 장소에서 다른 장소로 보내야 하므로 시각 및 주파수 전송(time and frequency transfer)이라는 용어를 사용하기도 한다.

시각 및 주파수 비교는 다양한 방법이 있는데, 첫 번째로 한 장소에서 일방적으로 시각 및 주파수 정보을 전송하는 방송이다. 단파 또는 장파의 무선방송을 이용하거나, 인터넷을 통한 전송, 전송 케이블 이용한 전송, 위성을 이용한 전송 등이 있으며, 많은 사용자들이 시각 및 주파수 정보를 수신하여 사용하는 형태이다. 예를 들어 휴대폰은 통신회사, 또는 GPS와 같은 항법위성으로부터 시각 정보를 수신하여 시각을 표시해 준다.

두 번째로는 동시수신 비교 방법이다. 위성 또는 LORAN(장거리 무선항법 시스템)에서 시각 및 주파수 정보를 방송하면 두 사용자 또는 여러 사용자에서 동시에 수신하여 각자의 시간정보와 비교한 결과들을 한곳에 모아 서로 빼기를 하면, 공통의 시계 정보가 배제된 사용자 간의 시각 및 주파수 정보를 비교하는 결과를 얻을 수 있다. 이때 신호 전송에 걸리는 시간을 보상해주어야 하는 어려움이 있다.

세 번째는 양방향 시각 및 주파수 비교 방법이 있다. 이 방법은 두 사용자가 서로 신호를 주고 받아 신호를 전송하는데 걸리는 시간을 정밀하게 측정하여 보상할 수 있기 때문에 고정밀 시각 및 주파수 비교에 사용된다. 양방양 시각 및 주파수 비교는 양방향 통신 위성, 광섬유 등이 사용되고 있다.

10. 장거리 시각 및 주파수 비교

시간은 방송, 통신, 항법 등 다양한 분야에서 활용되고, 전세계에서 공유하는 경우가 많으므로 장거리 시각 및 주파수를 비교하거나 동기하는 것이 필요하다. 그리고 필요에 따라 고정밀 시각비교가 필요한데, 특히, 정확도가 매우 높은 광시계를 비교하기 위해서는 광시계와 유사 또는 더 정밀하게 비교하는 방법이 필요하다. 짧은 거리의 경우 광섬유를 통해 시각 및 주파수 양방향 비교 방법을 이용하면 가능하지만, 이는 근거리에서 가능하고, 장거리 비교에는 많은 제약이 따른다. 특히, 이 방법은 대륙간 장거리 비교에는 적용할 수 없다.

장거리 특히, 대륙간 장거리 비교에는 양방향 통신위성을 이용하거나 천문관측용인 VLBI를 이용하는 방법, 항법위성의 반송파 위상을 이용하는 방법 등이 사용하고 있다. 하지만, 이러한 비교 방법의 정확도가 광시계의 정확도에 못 미치기 때문에 비교의 정확도를 높이는 방법을 연구하거나 다른 방법을 모색하고 있다.

장거리 시각 및 주파수 비교의 다른 방법으로 이동형 광시계를 이용하는 것이다. 광시계는 실험실 환경에서 넓은 공간을 차지하는 시계로 이동이 불가할 뿐 아니라 이동후 재동작시키는데는 많은 시간이 소요된다. 이동형 광시계는 광시계의 정확도를 유지하면서 트럭 등에 탑재하여 이동할 수 있는 크기, 그리고 진동 등 충격에 강하게 만들어 이동후 짧은 시간에 재동작을 할

수 있도록 만든 시계이다. 이동형 광시계를 한 장소에 있는 시계와 비교하고, 다른 장소로 이동후 비교한 후 두 측정결과를 서로 비교하면 두 장소의 시계가 서로 비교된 결과를 얻을 수 있다.

양자 전기장 센서 용어 MAP

양자 전기장 센서 (Quantum electric field sensor)

1. 리드버그 원자 (Rydberg atom)

- 특성
  - 2. 전기 쌍극자 모멘트 (electric dipole moment)
  - 3. 전기 분극률 (electric polarizability)
  - 4. 암흑 상태 (dark state)
  - 5. 양자 결함 (quantum defect)
- 분광법
  - 6. 광 펌핑 (optical pumping)
  - 7. 전자기 유도 투과 (electromagnetically induced transparency)
- 저주파 특성
  - 8. DC 스타크 효과 (DC Stark effect)
  - 9. 정적 이온화 필드 (Static ionization field)
- 고주파 특성
  - 10. AC 스타크 효과 (AC Stark effect)
  - 11. 오틀러-타운스 더블릿 (Autier-Townes doublet or AT splitting)

1. 리드버그 원자 (Rydberg atom)

리드버그 원자는 주양자수(n)가 매우 큰 에너지 상태의 원자이다. 주양자수가 크기 때문에 리드버그 원자의 크기가 매우 크다. 보어 원자모형에 의한 원자의 반지름은 $r = \frac{4\pi\epsilon_0\hbar^2}{mc^2}n^2$ (ϵ_0: 유전상수, $\hbar$: 플랑크 상수, e: 전자전하, m: 전자질량)으로 주어지기 때문에, n=100인 리드버그 원자의 크기는 마이크로미터에 육박하게 된다. 리드버그 원자는 기저상태의 원자로 전이하는 확률이 작고, 따라서 자발 방출에 의하여 붕괴하는 시간이 매우 길다 (n=100인 리드버그 원자의 붕괴 시간은 약 1ms). 따라서, 리드버그 원자를 이용한 원자 물리 현상을 기술하는 시간과 거리의 척도는 각각 ms와 μm가 되어, 일반적인 원자의 시간 척도 ns과 비교하여 백만 배, 거리 척도 Å 와 비교하여 만 배 확장된다.

알칼리 원자의 리드버그 에너지 준위는 내각 전자들의 전하량이 모두 원자 코어에 의해 전기적으로 가려지기 때문에 최외각 전자의 결합에너지는 간단하게 $E_{n,l,m} = E_\infty - \frac{Ry}{(n-\delta_{n,l})^2}$ (E_∞: 이온화 에너지, Ry: 리드버그 상수)로 주어진다. 리드버그 원자의 에너지 준위 공식은 양자 결함 (quantum defect)이라고 불리는 상수인 $\delta_{n,l}$만큼 수소 원자의 에너지 준위와 차이를 갖게 된다. 원자핵과 전자의 결합 에너지가 매우 작기 때문에, 약한 전기장에도 최외각 전자는 원자 코어의 쿨롱 포텐셜 (Coulomb potential)을 쉽게 넘는다. 이와 같은 리드버그 원자의 특성은 표 1과 같다.

표 1. 리드버그 원자의 특성 [1]

특성	n-scaling	Rb (50p)
결합 에너지	n^{-2}	6.2 meV
인접 n 상태 사이 에너지	n^{-3}	0.22 meV
붕괴 시간	n^{3}	106 μm
미세구조 에너지 간격	n^{-3}	~0.9 MHz
궤도 반지름	n^{2}	0.17 μm
쌍극자 모멘트 $\langle np\|er\|nd\rangle$	n^{2}	3200 ea_0
Geometric Cross-section	n^{4}	0.096 μm^2
스칼라 분극률	n^{7}	~GHz cm^2/V^2

리드버그 원자는 일반 원자와 비교하여 주양자수 7승에 비례하는 엄청난 크기의 전기적 분극률(electric polarizability)을 갖는다. 또한 매우 큰 값의 영주 전기적 쌍극자 모멘트와 유도 전기적 쌍극자 모멘트를 가질 수 있기 때문에, 이러한 특성을 가지고 전기장 측정을 목적으로 연구되고 있다. DC 전기장부터 THz만큼의 주파수 대역을 가지고 있어 전기장 측정하는 센서의 역할로 아주 큰 이점을 가진다.

참고

[1] 리드버그 원자의 물리, 안재욱

[2] Gallagher, Thomas F. “Rydberg atoms.” Reports on Progress in Physics 51.2 (1988): 143.

[3] Liu, Bang, et al. “Electric field measurement and application based on Rydberg atoms.” Electromagnetic Science 1.2 (2023): 1-16.

2. 전기 쌍극자 모멘트 (Electric dipole moment)

전기 쌍극자 모멘트 (EDM)은 전기적으로 중성인 시스템에서 양전하와 음전하가 분리되어 형성하는 전기 쌍극자의 크기를 나타낸다. 안정적인 입자가 EDM을 가지기 위해서는 시간 반전 대칭(T)과 패리티 대칭(P)이 모두 깨져야 한다. 이는 EDM이 기본적으로 시간 반전과 공간 반전에 대해 비대칭성을 가지기 때문이다.

예를 들어, 전하 q가 다른 전하 -q와 거리 r만큼 떨어져 있다면 EDM은 $d=q \cdot r$ 형태를 가진다. 기본 입자의 EDM은 입자의 스핀 축에 따라 정렬된다. 이는 스핀 축에 수직 방향의 모든 성분이 평균적으로 0이 되기 때문이다.

여기에 시간 반전이 발생하면 스핀 방향이 반대로 바뀌지만, EDM의 방향은 변하지 않는다. 왜냐하면 스핀이 시계 방향으로 회전하고 있는 입자가 있다면, 시간 반전이 적용되면 반시계 방향으로 회전하는 것으로 나타낸다. 반면, EDM은 입자 내부의 전하 분포에 따라 정의되는 전기 쌍극자 모멘트로, 전하의 분포와 관련이 있을 뿐, 시간의 흐름 방향과 연관되기 때문이다. 만약 시간 반전이 좋은 대칭성을 갖는다면, 스핀과 EDM의 정렬 방식이 평행하거나 반대 방향으로 평행함에 따라 에너지 준위가 이중으로 축퇴되어야 한다. 하지만, 자연적으로 이러한 축퇴가 나타나지 않기 때문에 EDM이 존재한다는 것은 T 대칭이 깨져 있다는 것을 의미한다.

EDM은 유도된 EDM과 영구 EDM (permanent EDM)으로 구분할 수 있다. 유도된 EDM은 외부 전기장이 적용되었을 때 나타낸다. 영구 EDM은 전자와/또는 핵자 (nucleon)의 EDM, P와 T 대칭을 깨는 핵자-핵자 상호작용, 그리고 전자-핵자 또는 전자-전자 상호작용에 의해 발생할 수 있다. 또한 외부 전기장이 극히 약해도 선형적인 스타크 효과 (linear Stark effect)를 발생시킨다.

실험적으로 입자의 EDM을 검출하기 위해 입자를 외부 전기장에 놓고, 입자와 외부 장 사이의 상호작용 에너지가 전기장 E에 선형으로 비례하는지를 확인하는 방법이 있다.

참고

[1] Bernreuther, Werner, and Mahiko Suzuki. "The electric dipole moment of the electron." Reviews of Modern Physics 63.2 (1991): 313.

[2] Fortson, Norval, Patrick Sandars, and Stephen Barr. "The search for a permanent electric dipole moment." Physics Today 56.6 (2003): 33-39.

3. 전기 분극률 (Electric polarizability)

원자는 양전하를 띤 핵과 음전하를 띤 전자구름으로 구성되어 있으며, 전기장이 가해지면 양전하와 음전하는 서로 다른 방향으로 약간 이동하게 된다. 이에 따라 원자는 내부적으로 쌍극자 모멘트 p를 가지게 된다. 즉, 전기장이 가해진 방향으로 작은 쌍극자가 형성되며, 이 쌍극자 모멘트는 전기장 E에 비례하여 생성된다.

이때 양전하와 음전하가 서로 끌어당기는 힘이 전기장에 의한 밀어내는 힘과 균형을 이루어, 원자는 분극 된 상태(polarized)를 유지하게 된다. 유도된 쌍극자 모멘트 p는 전기장 E와 동일한 방향을 가지며, $p = \alpha \cdot E$ (α는 electric polarizability (전기 분극률))와 같은 관계를 가진다.

분자의 경우는 어떤 방향에서 전기장이 가해지느냐에 따라 다른 정도로 분극될 수 있다. 예를 들어, 이산화탄소(CO2)는 분자의 축을 따라 전기장이 가해질 때와 수직 방향으로 전기장이 가해질 때 분극률이 다르다. 전기장이 분자 축에 대해 일정한 각도로 가해지는 경우는 전기장을 분자 축에 평행한 성분과 수직 성분으로 나누어 각각의 분극률을 적용하여 계산해야 한다. $\vec{p} = \alpha_{\perp}\vec{E}_{\perp} + \alpha_{\parallel}\vec{E}_{\parallel}$ ($\alpha_{\parallel}$: 분자 축 방향의 분극률, $\alpha_{\perp}$: 분자 축에 수직 방향의 분극률)

참고

[1] Griffiths, David J. Introduction to electrodynamics. Cambridge University Press, 2023.

4. 암흑 상태 (Dark state)

원자의 암흑 상태는 양자역학적 간섭 효과인 coherent population trapping (CPT, 결맞음 인구 트래핑)에 의해 특정한 빛을 흡수하지 않는 현상에 의해 형성된다. 이 현상은 알칼리 원자(예를 들어, 루비듐, 세슘 등)에서 발생할 수 있으며, 주로 두 개의 다른 주파수를 가진 빛들을 이용하여 특정 상태 간의 coherent(결맞음)를 연구할 수 있다.

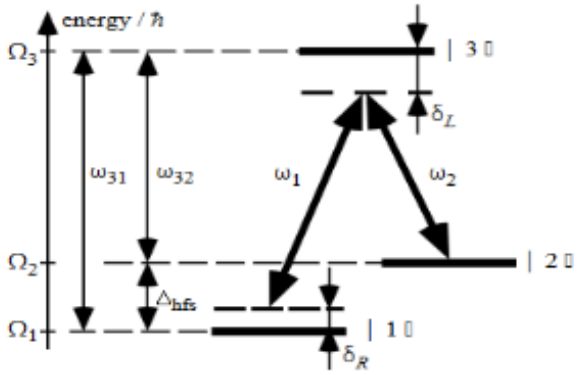


그림 2. The three-level system

CPT는 두 개의 긴 수명을 가진 바닥 상태($|1\rangle, |2\rangle$)와 하나의 여기 상태($|3\rangle$)로 이루어진 Λ 시스템에서 발생한다. 두 개의 빛은 각각 $|1\rangle \rightarrow |3\rangle$와 $|2\rangle \rightarrow |3\rangle$

전이에 작용한다. 양자역학적 간섭은 이러한 이중 전이에서 발생하며, 특정 조건에서 빛의 흡수가 억제되는 암흑 상태가 생성된다. 이 상태는 이중 주파수 빛에 대해 흡수되지 않으며, 이는 자기장, 레이저 편광 등의 외부 요인을 고감도로 측정하는 데 유리하다.

참고

[1] Wynands, R., and A. Nagel. “Precision spectroscopy with coherent dark states.” Applied Physics B: Lasers & Optics 68.1 (1999).

5. 양자 결함 (Quantum defect)

양자 결함 이론(quantum defect theory, QDT)은 리드버그 공식(Rydberg's formula)으로부터 발전되었으며, 이는 원자 내부에서 전자가 특정 핵 주위를 움직일 때의 에너지 준위를 설명하기 위한 이론적 틀이다.

리드버그 공식은 원자 에너지 준위를 파라미터화 하는데 사용되며, 특히 이온화 한계(에너지가 0으로 설정된)를 기준으로 원자의 특정 에너지 준위 $E_{n,l,m} = E_{\infty} - \frac{Ry}{(n-\delta_{n,l})^2}$ (E_{∞}: 이온화 에너지, Ry: 리드버그 상수, $\delta_{n,l}$: 양자 결함)을 나타낸다. 양자 결함 값은 전자가 원자핵 주위의 이온 코어(ionic core)와 상호작용을 하면서 발생하는 에너지 차이를 반영한다. 이 값은 전자가 코어에 얼마나 가까이 접근하는지에 따라 다르다. 낮은 l 값을 가진 전자만 코어 근처에 접근할 수 있기 때문에, 높은 l 값을 가진 전자들에게는 $\delta_{n,l}$이 거의 무시될 정도로 작아진다.

수소 원자는 단일 양성자 핵을 가지고 있어 양자 결함이 존재하지 않지만, 나트륨과 같은 알칼리 원자 금속 원자에서는 다른 전자들과의 상호작용으로 인해 양자 결함이 발생한다.

참고

[1] Greene, C., U. Fano, and G. Strinati. "General form of the quantum-defect theory." Physical Review A 19.4 (1979): 1485.

[2] Rau, A. R. P., and Mitio Inokuti. "The quantum defect: Early history and recent developments." American Journal of Physics 65.3 (1997): 221-225.

6. 광 펌핑
(optical pumping)

광 펌핑이란, 실험 온도에서의 일반적인 볼츠만 분포와는 다른 에너지 준위 분포를, 빛을 이용하여 특정 시스템에 생성하는 과정을 의미한다. 광 펌핑의 대상은 주로 자기 에너지 준위(magnetic energy levels)로, 원자들의 정렬(alignment)이나 방향성(orientation)을 제어하는 데 사용된다. 이는 빛의 특정 방향성 또는 편광을 통해 이루어진다. 때에 따라서는 전자 상태가 광 펌핑의 대상으로 선택되고, 이 경우 레이저 작용을 위한 조건을 마련하기 위해 특정 전자 상태를 채우는 목적이 있을 수 있다.

예를 들어, $^2S_{1/2}$ 바닥 상태와 $^2P_{1/2}$ 및 $^2P_{3/2}$ 두 개의 여기 상태를 가진 가상의 알칼리 금속 원자를 가정하자. 이들 상태 간의 광학적 전이는 각각 D1과 D2 line을 형성하고, 이 실험에서는 D1 line만 이용한다고 가정한다.

원자가 외부 자기장 H_0에 놓이게 되면, 원자의 에너지 준위가 분리된다. 원자의 최외각 전자의 스핀 자기 모멘트는 자기장과 상호작용을 하여 $E = g\beta H_0 m_S$ (g는 Lande g-factor, β는 보어 마그네톤, m_S는 자기 양자수로, 여기에서는 $\pm\frac{1}{2}$ 의 값)의 에너지를 가지게 된다. 원형 편광된 D1 line 빛에 의해 원자들은 $^2P_{1/2}$ 상태로 여기되고, 이 과정에서 전이 선택 규칙(transition selection rule)에 의해 스핀 자기 양자수 $\Delta m_S = \pm 1$의 상태 변화가 허용된다. 전이 선택 규칙을 고려하여 그림 2처럼 가능한 전이는 A →

D로의 전이를 나타낸다. 여기 상태의 수명(lifetime)이 짧기 때문에, 여기된 원자는 빠르게 빛을 방출하고, 만약 비정렬화(disorientation) 현상이 없다면, 바닥 상태 A, B 같은 확률로 돌아온다. 시간이 지나면서 원자 분포는 상태 A에서 B로의 인구 이동이 된다. 상태 B에 원자가 축적되는 것은 원자의 각운동량 방향이 한쪽으로 정렬되는 것을 의미한다. 이처럼 광 펌핑은 특정 상태에 원자를 모아 특정 방향성을 부여하는 것이 광 펌핑의 목표 중 하나이다.

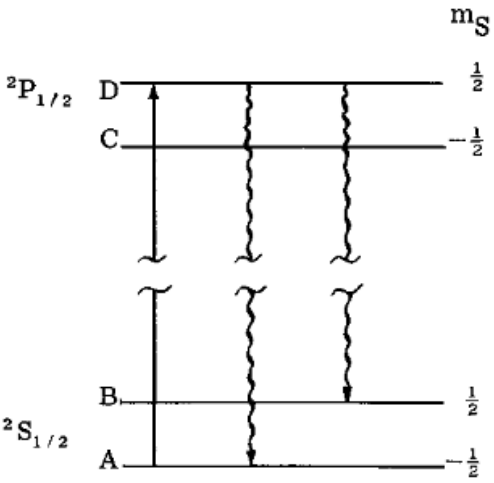


Figure 2-3 Absorption with $\Delta m_S = +1$ and spontaneous emission.

그림 1. 광 펌핑

참고

[1] Bernheim, Robert. "Optical pumping." New York (1965).

7. EIT, 전자기 유도 투과 (Electromagnetically Induced Transparency)

EIT는 레이저에 의해 유도된 간섭으로 인해 발생하며, 원자 내 coherence(코히어런스)가 생겨 특정 주파수의 프로브 빛이 거의 흡수되지 않고 투명하게 통과하는 현상이다. 이로 인해, 원래는 불투명한 매질이 투명해질 수 있다. EIT 효과는 매질의 굴절률 특성도 크게 변형할 수 있다. 보통 굴절률이 높으면 흡수도 높아지는 경향이 있지만, EIT로 인해 이러한 상관관계가 깨지고, 독특한 광학적 특성을 갖는 매질을 형성할 수 있다.

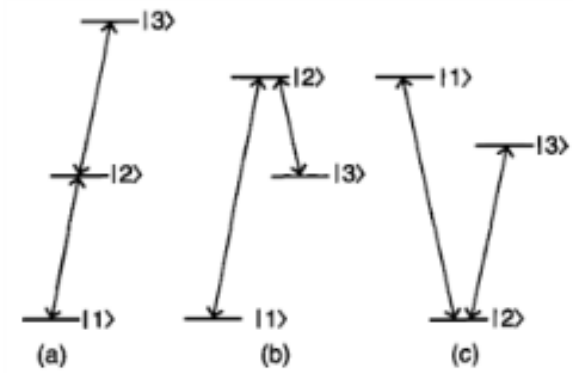


그림 4. EIT three-level scheme

EIT 실험에서 사용되는 3준위 구조는 그림 4에 나와 있는 (a) Ladder(계단형) 구조, (b) Λ 구조, (c) V 구조로 구분된다. 계단형 구조 EIT를 예로 들면, 두 개의 레이저 필드는 프로브 필드, 커플링 필드라고 하며, 각각 상태 $|1\rangle$에서, $|2\rangle$그리고 $|2\rangle$에서 $|3\rangle$으로 이어지는 단계적인 전이 과정을 거친다. 각각 필드가 전이 주파수와 동일하고, 커플링 필드가 강하다면 간섭 효과로 인해 상태 간의 투명성이 발생하게 된다.

참고

[1] Marangos, Jonathan P. “Electromagnetically induced transparency.” Journal of modern optics 45.3 (1998): 471-503.

8. DC 스타크 효과
(DC Stark effect)

DC Stark effect(DC 스타크 효과)는 외부 DC 전기장에 의해 원자의 에너지 준위에 미치는 영향을 다루는 양자역학적 현상이다. 전기장은 원자의 에너지 준위를 이동시키며, 이는 특히 리드버그 상태에서 강하게 나타난다. Coulomb(쿨롱) 전기장과 스타크 전기장이 결합된 원자의 포텐셜은 $V(\vec{r}) = -\frac{1}{r} + Fz$ ($V(\vec{r})$는 입자 위치 $\vec{r}$에서의 전위, $-\frac{1}{r}$은 순수한 쿨롱 전기장 (원자핵으로부터 거리 r에서의 전위), Fz: static uniform (정적 균일) 전기장 F로 인한 스타크 전기장)으로 정의된다.

일반적으로 수소 원자의 스타크 효과는 수소 원자의 간단한 구조 때문에 잘 알려졌지만, 나트륨(Na), 칼륨(K), 루비듐(Rb), 바륨(Ba)과 같은 알칼리 금속 원자에서 관찰된 스타크 효과는 비대칭적인 스타크 레벨의 형태와 극성에 의존하는 진동 패턴으로 인해 복잡한 구조를 가지고 있다.

예를 들어, [2]나트륨 $3^2P_{3/2}$ 상태에서 DC 전기장 하에 photoionization (광이온화) 스펙트럼을 측정하고 분석하는 실험을 진행했다고 하자. 이때, 실험 결과는 비대칭적인 공명 피크를 보여주며, 이는 간섭 효과를 발생시키는 non-hydrogenic(비수소형) 코어의 존재로 설명된다. 코어와 전자가 강하게 상호작용하기 때문에 수소 원자에서 발생하는 정밀한 스타크 효과와 달리 비대칭적인 모양이 나타나는 것이다.

참고

[1] Harmin, David A. “Theory of the Stark effect.” Physical review A 26.5 (1982): 2656.

[2] Harmin, David A. “Theory of the nonhydrogenic stark effect.” Physical review letters 49.2 (1982): 128.

9. 정적 이온화 필드
(Static ionization field)

리드버그 상태에서 필드 이온화는 중요한 개념이다. 이 상태는 전자가 원자핵으로부터 멀리 떨어져 있기 때문에 매우 쉽게 이온화될 수 있기 때문이다. 이온화가 발생하기에 충분한 전기장을 이온화 필드라고 하며 스타크 효과와 스타크 상태에서의 에너지, 공간적 분포를 고려하면 $E = \frac{1}{9n^4}$(E: 이온화를 위해 필요한 전기장의 크기)와 같이 주어진다.

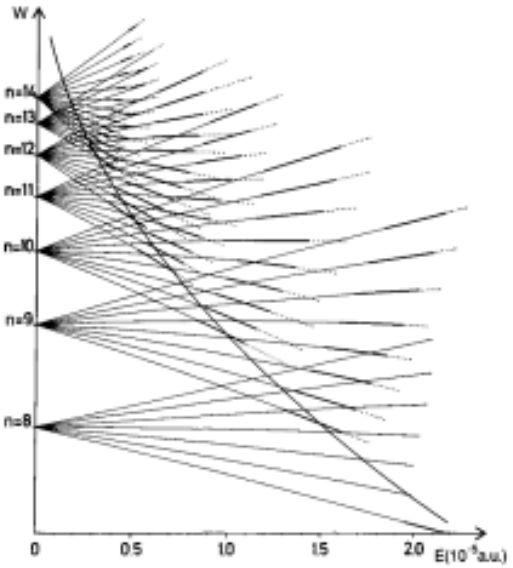


그림 3. 스타크 구조와 필드 이온화 특성
[실선: lifetime(수명)이 $\tau > 10^{-6}s$인 quasi-discrete(준연속) 상태,
굵은 실선: 수명이 $5 \times 10^{-10} < \tau < 5 \times 10^{-6}s$인 field broadened(필드 확장) 상태,
$\tau < 5 \times 10^{-10}s$인 field ionization(필드 이온화) 상태,
필드 확장 스타크 상태는 대략 W > W_c인 경우에만 나타난다. Saddle point(안장점) 한계는 $W_s = -2\sqrt{E}$ 로 굵은 곡선]

그림 3은 n=8에서 n=14까지의 수소 원자의 |m| = 1 에너지 레벨 이동을 정적 전기장 강도 범위 0에서 10^5 V/cm까지 보여준다. 이 그림에서는 에너지 레벨이 선형적으로 이동하다가 강한 전기장에서 이온화가 발생한다. 이온화될 때 정적 전기장을 정적 이온화 필드라고 한다. 필드 이온화 한계는 안장점 한계라고도 하며, 이는 이온화가 발생할 수 있는 임계 전기장을 나타내는 값이다.

참고

[1] Gallagher, Thomas F. “Rydberg atoms.” Reports on Progress in Physics 51.2 (1988): 143.

10. AC 스타크 효과
(AC Stark effect)

AC Stark effect(AC 스타크 효과)는 레이저의 영향을 받아 원자 에너지 준위가 변화하는 현상이다. DC 전기장은 원자 에너지 준위를 이동시키며, 에너지 보존 법칙이 성립한다. 그러나 레이저에서는 에너지 보존이 성립하지 않으며, 에너지 준위의 Stark shift(스타크 이동)는 외부 monochromatic field(단색 필드)가 있을 때만 정의될 수 있다. 이러한 관계는 Floquet 정리에 의해 설명이 된다.

Floquet 정리는 주기적인 계수의 선형 동차 미분 방정식을 푸는 것과 관련이 있는 정리이다. 주기적인 계수를 가진 외부 단색 필드에 의해 영향을 받는 계의 파동함수는 $\Psi(r,t) = \exp(-iE_a t)\varphi(r,t)$와 같이 표현된다. $\varphi(r,t)$는 주기 함수로, 시간 t에 대해 푸리에 급수를 전개하면 파동함수는 여러 stationary state (정상 상태)의 중첩으로 표현되며, 각 상태는 quasi-energy state (준 에너지 상태)라 부른다. 준 에너지 상태는 각각의 고유 에너지를 가지며, 이것이 quasi-energy spectrum(준 에너지 스펙트럼)이다. 이 스펙트럼은 원자와 전자기장이 상호작용을 하여 새로운 시스템을 형성한 결과로 나타나는 에너지 준위를 나타내며, 이는 dressed atom(드레스드 원자)이라 한다.

AC 스타크 효과는 리드버그 상태에서 중요하게 다루어진다. 리드버그 상태

에서는 이웃한 에너지 준위 사이의 간격이 n^{-3}에 비례하여 빠르게 감소한다. 즉, 주양자수가 클수록, 에너지 준위 간격이 작아진다. 레이저는 고주파수 필드로 작용하여 리드버그 상태의 전이에 영향을 미치게 된다.

참고

[1] Delone, Nikolai Borisovich, and Vladimir P. Krainov. “AC Stark shift of atomic energy levels.” Physics-Uspekhi 42.7 (1999): 669.

11. 오틀러-타운스 더블릿 (Autler-Townes doublet / AT splitting)

Autler와 Townes는 1955년에 OCS 분자의 마이크로파 전이가 강한 공명 마이크로파 필드에 의해 세 번째 상태와 결합할 때 두 개의 구성 요소로 분리될 수 있음을 보여주었다. 이때 발생하는 이중 항은 Autler-Townes doublet 또는 dynamic Stark splitting(동적 스타크 분리)이라고 부른다.

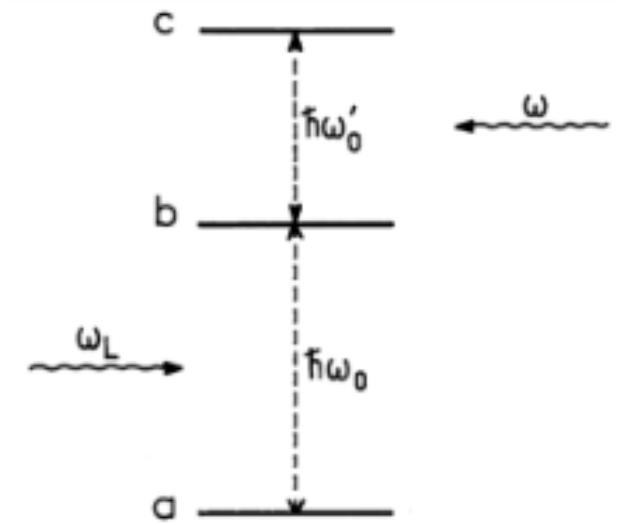


그림 5. Three-level atom. 강한 quasi-resonant field ω_L는 a ↔ b 전이를 유도하고, 약한 필드 ω는 b ↔ c 전이를 probe(탐침)한다.

a, b 두 상태는 ω_L에 의해 결합하여 두 상태는 서로 밀어내고 새로운

dressed state (드레스드 상태)로 변형된다. 드레스드 상태로 변형된 후 원래 ω'_0에 가까운 하나의 주파수로 나타내는 흡수 스펙트럼이 이제는 Autler-Townes doublet이라고 불리는 두 개의 주파수로 분리된다. 이와 같은 현상은 리드버그 원자를 이용한 고주파 측정 기술에 이용되며 EIT 실험에 추가적으로 고주파 필드를 가하여 AT splitting 현상을 일으켜 진행한다.

참고

[1] Chiao, Raymond Y., ed. Amazing light: a volume dedicated to Charles Hard Townes on his 80th birthday. Springer Science & Business Media, 2012.

양자 자기장 센서 용어 MAP

1. 양자 자기장 센서

- 1-1. 고체 양자 자기장 센서(Solid-State Quantum Magnetometer)
- 1-2. 원자자력계(Atomic Magnetometer)
- 1-3. 초전도양자간섭 자력계 (Superconducting Quantum Interference Device Magnetometer)

1. 양자자기장 센서

양자 자기장 센서란, 고체 내부에 존재하는 원자크기의 자성 불순물이나 원자 같은 양자객체(quantum object), 초전도체 등으로 이루어진 양자소자(quantum device), 또는 이들 간의 얽힘(entanglement)등 양자현상을 이용하여 자기장을 측정하는 센서이다. 양자 자기장 센서는, 홀센서, 플러스게이트 자력계 등 기존 고전 자기센서가 갖지 못한 공간분해능 또는 자기장 민감도를 가질 수 있어 다양한 응용 분야에서 주목받고 있다. . 양자 자기장 센서의 대표적인 예로는 고체 양자 자기장 센서, 원자자력계, 및 초전도 양자간섭 자력계 등이있다.

1-1. 고체 양자 자기장 센서 (Solid-State Quantum Magnetometer)

정의

고체 내부에 존재하는 원자 크기의 자성 결함을 이용해 자기장을 나노미터에서 밀리미터까지 다양한 분해능으로 측정할 수 있는 양자 자기장 센서.

종류

다이아몬드 질소빈자리(diamond nitrogen vacancy, DNV), 육방정계 질화붕소(h-BN), 탄화규소 실리콘 빈자리(SiV in SiC) 등이 있다.

측정 원리

고체 내부 결함에 특정 파장의 빛을 인가 할 때 결함이 발광(fluorescence)하는 빛의 세기가 외부자기장과의 연관성을 가진다는 원리를 기반으로 자기장을 측정. 사용하는 고체 내부 결함 개수에 따라 나노미터(단일결함)에서 마이크로미터(앙상블결함)까지의 다양한 공간분해능을 갖는다.

활용 범위

1) 나노미터 영역

자화 물질내부 자기장 분포, 2차원 물질에서의 전류의 흐름 또는 나노소자 내부의 자기장/전기장을 등을 나노미터 수준의 분해능으로 측정할 수 있다. 또한 자기공명(NMR) 및 자기공명영상(MRI) 측정을 통해 세포막 단백질 구조를 정밀하게 분석할 수 있어 신약설계 등에 활용할 수 있다.

2) 마이크로미터 영역

세포의 구조를 마이크로미터 수준에서 자기공명 및 자기공명영상을 통해 측정함으로써, 세포에 대한 보다 심층적인 이해를 할 수 있는 연구가 가능하고, 사람의 생체 내 신경 연결망을 마이크로미터 수준의 비파괴적이고 안전한 방식으로 분석할 수있어 인간의 뇌를 더욱 깊이 이해하는데 기여할 수 있을 것으로 보인다. 뿐만 아니라 다층구조로 집적된 회로에서 발생하는 불량을 마이크로미터 수준의 분해능으로 정확히 파악하는 것도 가능하다.

3) 밀리미터 영역

소형화 센서를 이용해 지구 자기장을 기반으로 하는 위치, 항법 및 시각(positioning, navigation and timing, PNT)장치, 철강 등에 존재하는 자성 불량을 감지하는 비파괴 검사 장치, 그리고 광섬유와 결합해 인체 내부 자기이상을 찾아 낼 수 있는 의료 장치 등 다양한 분야에서 활용이 가능하다.

핵심 센서 성능 평가지표

1) 자기장 민감도

자기장 민감도는 센서가 측정할 수 있는 최소 자기장 크기에 측정시간의 제곱근을 곱한 값이다. 고체 양자 자기장 센서에서는 센서의 발광세기 또는 발광 대조비가 클수록, 결맞음 시간이 길수록 자기장 민감도가 좋아지기 때문에 보다 작은 자기장을 측정할 수 있다. 공간 분해능에 따라 자기장 민감도는 수십 nT/√Hz 에서 1 pT/√Hz 정도의 값을 갖는다.

2) 공간 분해능

공간 분해능은 물리적 공간에서 두 개의 서로 다른 지점을 구별할 수 있는 능력을 의미한다. 예를 들어, 1 mm의 공간 분해능을 가지는 센서는 서로 1 mm 떨어진 두 개의 지점을 구분할 수 있다는 뜻이다. 단일 고체 양자센서를 사용하는 경우 수 나노미터의 공간 분해능을 가지고, 집단(ensemble) 고체 양자센서를 사용하는 경우 분해능은 포함하는 양자 센서의 개수에 따라 마이크로미터에서 밀리미터까지 다양하다.

핵심 센서 특성

1) 결맞음시간(coherence time)

양자 센서로 사용하는 고체 내부의 자성 결함의 자화 값이 대략 37% 정도로 감소될 때까지 걸리는 시간이다. 결맞음시간이 길면, 더욱작은 자기장을 잘 측정할 수 있다. 고체 자기장 양자 센서는 고체 내 결함 구조와 주변 환경 노이즈로 인해 결맞음시간이 감소하므로 이를 효과적으로 제어할 수 있는 기술이 필수적이다.

2) 발광 대조비(odmr contrast)

고체 양자 자기장 센서에 광학적 자기공명현상(Optically Detected Magnetic Resonance, ODMR)이 발생할 때의 센서가 가지는 발광량과 광학적 자기공명이 발생하지 않을 때 센서가 가지는 발광량의 비율을 발광 대조비라 한다. 발광대조비가 클수록 우리가 얻고자 하는 정보를 담은 신호를 잘 구분할 수 있어 더 정밀한 자기장 측정이 가능하다.

3) 자성불순물 농도

고체양자자기장 센서의 내부에 존재하는 ^{13}C, $^{14,15}N$, ^{29}Si 등과 같은 자성불순물은 결맞음시간을 감소시켜 센서의 성능을 저하시킨다. 따라서 센서 활용에 따라 자성불순물의 농도에 대한 최적화가 필요하다.

1-2. 원자자력계 (Atomic Magnetometer)

정의

고온 알칼리 원자증기의 스핀상태와 레이저 빛의 상호작용 이용해 매우 미세한 수준의 자기장 측정이 가능한 양자 자기장 센서

종류

측정 방식에 따라 자기장의 방향과 크기를 모두 측정할 수 있는 영자기장 자력계(zero field magnetometer), 자기장의 크기만 측정하지만 지구 자기장 아래에서 사용이 가능한 절대자력계(total field magnetometer)가 있다. 원자자력계에 사용되는 원자증기는 Rb, Cs, K 등이다.

측정원리

고온 알칼리 원자증기를 통과하는 편광된 빛의 세기가 원자 증기 주변의 자기장세기에 따라 변하는 현상을 이용해 펨토테슬라(fT)수준의 자기장을 측정한다. 원자자력계는 원자증기가 담긴 증기셀의 크기에 따라 자기장 공간분해능이 결정되고 일반적으로 밀리미터 수준의 공간분해능을 갖는다.

활용 범위

1) 의료 분야

뇌자도(MEG, Magnetic-Encephalography) 및 심자도(MCG, Magneto-Cardiogram)와 같이 생체에서 발생하는 미약한 자기장을 측정해 의학적 진단에 활용할 수 있다.

2) 방위산업 활용 분야

뛰어난 자기장 민감도를 바탕으로 수중 자성물질, 지뢰탐지 등에 활용이 가능하다.

3) 산업적 활용

철광석 같은 지하자원 탐사, 배터리 내부 자성불량 탐지, 우주 자기장 측정 등에 활용이 가능하다.

핵심 센서성능 평가지표

1) 자기장 민감도

자기장 민감도는 센서가 측정할 수 있는 최소 자기장 크기를 측정시간의 제곱근을 곱한 값이다. 상용 원자자력계의 경우 동작방식에 따라 10 fT/√Hz - 1 pT/√Hz 가량의 값을 갖는다.

2) 동적범위

원자자력계는 일반적으로 150 Hz 이하의 DC 자기장 신호 측정에 최적화 되어있다.

3) 공간 분해능

공간분해능은 센서가 구분할 수 있는 가장 작은 공간적 자기장 변화를 의미한다. 원자자력계는 증기셀의 물리적 크기로 인해 일반적으로 센치미터 수준의 공간분해능을 갖지만, 최근 개발된 칩스케일 원자자력계의 경우 증기셀의 크기를 효과적으로 줄여 밀리미터 수준의 공간 분해능을 갖는다.

핵심 기술

1) SERF(Spin-Exchange Relaxation-Free)

일반적으로 센서가 가지는 자화의 결잃음 현상은 스핀교환(spin-exchange)에 따른 자화 이완(relaxation)으로 발생한다. 원자자력계가 동작하는 매우 낮은 자기장 및 고농도의 원자증기 상태에서는 이러한 스핀교환 현상이 원자증기의 세차 주기보다 매우 빠르게 발생해서, 평균적으로 원자 증기끼리의 스핀교환으로 인한 자화 이완이 상쇄되는 현상을 말한다.

2) 증기셀

고온의 알칼리 금속 원자(Rb, K, Cs 등)와 완충가스(Xe, N_2 등)를 포함하는 밀봉된 유리 또는 실리콘 진공 챔버를 말한다. 최근에는 반도체 공정을 이용해 밀리미터 크기의 증기셀을 제작하고 이를 이용해 저전력 칩스케일 원자자력계를 구현한다.

1-3. 초전도양자간섭 자력계 (Superconducting Quantum Interference Device Magnetometer)

정의

절연체로 분리된 초전도체 접합인 조셉슨 접합(Josephson junction)의 두 초전도체 사이의 간섭현상을 이용해서, 극저온에서 미세 자기장을 측정할 수 있는 양자 자기장 센서.

원리

조셉슨 접합을 포함하는초전도 고리를 만들 경우, 고리 내부 자속(magnetic flux)이 일정한 값을 유지하려는 자속 양자화 현상이 나타나고 이를 이용해 자기장을 측정한다. 외부 자기장이 초전도 고리에 유입되면, 자속 양자화를 유지하기 위해 흐르는 전류가 초전도 고리 위치에 따라 달라져 전압 신호가 발생한다. 이때 전압 신호는 외부 자기장 크기에 관련이 있다.

활용 범위

극저온 냉매를 사용해 센서의 온도를 낮춘 환경에서 측정해야 하기 때문에 측정장치의 크기가 커지는 단점을 갖고 있지만, 매우 미세한 자기장을 잘 측정할 수 있기 때문에 아직까지도 뇌/심자도 같은 의료분야와, 암흑물질 탐사 등 다양한 분야에 활용되고 있다.

핵심 센서 성능 평가지표

1) 자기장 민감도

초전도양자간섭 자력계는 펨토테슬라(10^{-12} T) 수준의 약한 자기장을 감지할 수 있어 수 fT/Hz 이하의 작은 민감도를 갖는다. 현존하는 양자자기장 센서 중 가장 민감한 센서이다.

2) 공간 분해능

상온 시료의 경우 초전도양자간섭 자력계가 포함하는 극저온 냉매 용기와 측정 대상 사이의 거리로 인해 일반적으로 수 밀리미터 이상의 공간분해능을 갖는다.

핵심 기술

1) 조셉슨 접합(Josephson junction)

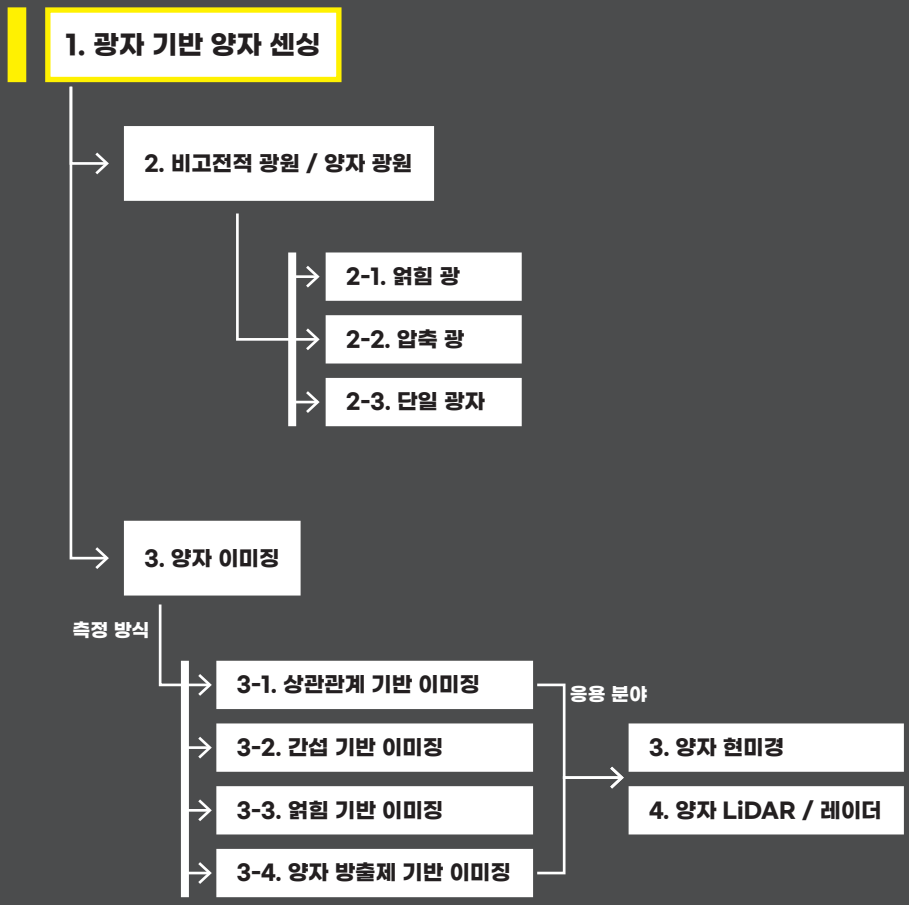
두개의 초전도체가 절연막을 통해 근접 할 때 외부 전압과 상관없이 작은 초전류가 흐르는 접합구조로, 초전도양자간섭계의 자기장 민감도에 큰 역할을 한다.

2) 고온 초전도체 양자간섭계

극저온 환경을 필요로 하는 초전도 양자간섭계는 극저온 환경을 유지하기 위해 많은 비용이 드는 문제가 있다. 이를 해결하기 위해, 상온보다는 매우 낮지만 기존 초전도체 양자간섭계가 작동하는 극저온 보다는 높은 온도인

액체 질소 온도에서도 초전도 현상을 보이는 YBCO와 같은 고온 초전도체를 사용해 초전도체 양자간섭계를 제작하였다. 기존보다 높아진 온도로 인해 잡음이 커지는 단점이 있지만, 유지보수 비용이 매우 낮은 장점이 있다.

광자 기반 양자 센싱 용어 MAP



1. 광자 기반 양자 센싱 (photonic quantum sensing)

광자 기반 양자 센싱은 빛의 기본 입자인 광자의 양자 역학의 특성을 활용하여 측정의 정밀도와 민감도를 향상시키는 기술이다. 광자 기반 양자 센싱의 핵심은 광자의 양자 상태(예: 압축 상태, 얽힘 상태 및 비고전적 상태)를 활용하며, 중첩, 얽힘, 양자 간섭 등의 양자 특성을 통해 측정 민감도를 고전적 한계를 넘어서 개선하는데 있다. 광자의 양자 상태를 이용하여 피사체를 직접적으로 관찰하는 양자 이미징 뿐만 아니라 넓은 범위로는 시간, 위치, 힘, 자기장 등 물리량을 측정하는데, 광자의 양자 상태를 적용하는 기술을 포함하며(예: 간섭계를 이용한 중력파 검출에 양자 상태를 활용하여 민감도 향상), 이를 통해 고전적인 광학 기술로는 얻을 수 없는 정밀도와 정확도를 얻을 수 있다.

응용 분야에 따라 양자 이미징/현미경, 양자 레이더/LiDAR 등이 있으며, 광자를 이용한 다양한 측정 분야에 광범위한 응용 가능성을 갖고 있다.

2. 비고전적 광원 / 양자 광원 (non-classical light / quantum light)

비고전적 광원(또는 양자 광원)은 광자 기반 양자 센싱 기술의 핵심으로 고전적인 빛과는 구별되는 특징을 가지며, 새로운 방식의 제어와 활용 방법을 가질수 있다.

2-1) 얽힘 광 (entangled light)

얽힘 광은 두 개 이상의 광자가 성질(파장, 위치, 시간 등)이 서로 연관되어 있는 상태이다. 얽힘 광자들은 서로 멀리 떨어져 있어도 한 광자에 대한 측정이 다른 광자의 상태에 즉시 영향을 미치며 (양자 얽힘 현상: quantum entanglement) 양자 센싱 기술에서 중요한 역할을 한다.

2-2) 압축 광 (squeezed light)

압축광은 광자의 위상 또는 진폭 특성 중 하나의 불확실성을 줄인 광자 상태이다. 압축광 상태는 측정의 정밀도를 높이는 데 사용 가능하며, 특히 간섭계 및 정밀 측정등 양자 센싱 기술에서 중요한 역할을 한다.

2-3) 단일 광자 (single photon)

단일 광자 상태는 특정 모드에서 단 하나의 광자만 존재하는 상태를 의미하며, 광자들이 일정한 시간 간격을 두고 방출되는 현상으로, photon antibunching 현상이 나타난다.

3. 양자 이미징 / 현미경 (quantum imaging / microscopy)

양자 이미징은 광자의 양자적 특성을 활용하여 기존의 고전적인 이미징 한계를 뛰어 넘는 향상된 해상도와 민감도 특성을 얻을 수 있는 이미징 기술을 의미한다. 양자 현미경은 비고전적 광원을 이용하여 고전 광학 현미경이 가진 한계를 넘어 더 세부적인 형태나 미세한 구조 감지가 가능한 현미경 기술을 의미한다.

양자 이미징을 통해 얻는 이득에 따라서 샷노이즈 한계 이하의 신호를 감지하는 서브샷노이즈 (sub-shot noise) 이미징, 더 미세한 크기를 감지하는 sub-rayleigh 이미징이 있다.

양자 현미경을 구현하는 방식에 따라 분류하면 아래와 같다:

3-1) 상관관계(correlation) 기반 이미징

광자쌍의 상관관계 특성을 이용한 이미징 방식으로 하나의 광자는 물체를 투과/반사하고, 나머지 하나의 광자는 물체를 거치지 않는다. 양자 이미징 구현하는 방법에 따라 높은 감도의 서브샷노이즈 이미징을 구현하거나, 물체를 거치지 않은 광자를 이용하여 이미징을 하는 고스트 이미징 (ghost imaging) 등으로 구현할 수 있다.

3-2) 간섭(interference) 기반 이미징

광자쌍의 간섭을 이용한 이미징 방식으로 물체를 거치지 않은 광자를 두 번째 광자쌍과 간섭을 유도하게 되면 물체를 거치지 않은 광자로 이미징이 가능하게 된다. 고스트 이미징과 차별적으로 물체를 거치지 않은 광자만으로(undetected photon) 이미징이 가능하여 검출기가 적절하지 않은 영역에서도 이미징이 구현 가능하다.

3-3) 얽힘(entanglement) 기반 이미징

얽힘 상태에 있는 광자쌍 모두를 피사체를 거친 후 이미징 하는 방식으로, 특히 N개의 광자가 얽힘 상태에 있는 NOON 상태와 같은 양자 상태를 이용하면, Rayleigh 한계 이상의 분해능을 갖는 이미징이 가능하다.

3-4) 양자 방출체 (quantum emitter) 기반 이미징

단일 광자를 방출하는 양자 방출체(반도체 양자점, 단일 점결함 등)를 이용한 이미징 방식으로 단일 광자의 antibunching 특성을 이용하여 이미징에 활용하면 분해능 향상이 가능한 이미징이 가능하다.

양자 현미경은 생물학, 재료 과학, 나노기술, 의학 등 다양한 분야에서 광범위하게 활용될 수 있으며, 광량에 민감하거나 높은 민감도를 요구하는 생물학적 연구, 진단 및 의료 분야 등에 큰 활용처가 될 수 있다.

4. 양자 LiDAR / 레이더 (quantum LiDAR / RADAR)

기존 LiDAR (Light Detection and Ranging)는 레이저 빛을 이용하여 물체까지의 거리를 측정하는 원격 탐지 기술인데, 양자 LiDAR는 양자 광원의 양자적 특성을 활용하여 시스템의 정밀도, 범위 및 민감도 향상이 가능한 기술이다. 양자 LiDAR의 장점은 비고전적인 빛을 사용함으로써 잡음 효과를 줄이고 높은 감도의 측정이 가능케한다.

사용하는 양자 광원이나 측정 방식에 따라 분류하면 아래와 같다:

4-1) 얽힘 기반 양자 LiDAR

얽힘 상태의 광자쌍중 하나는 대상 물체로 보내지고, 다른 하나는 상관 관계 측정하는데 활용하는 방식이다. 양자 현미경과 마찬가지로 감도를 높이는 것이 가능하여 먼 거리에 있는 물체를 더 정확하게 탐지하거나 약한 신호를 탐지하기 어려운 환경에서 더 정밀하게 측정을 기대할 수 있다.

광자쌍 측정 방법에 따라서 고스트 이미징 기법이나 유도 간섭 기술 적용하는 등의 응용 기술등이 개발되고 있다.

4-2) 압축광 기반 양자 LiDAR

압축 광자 상태를 이용한 LiDAR 기술로, 압축된 빛 상태에서는 광자의 위상

이나 진폭과 같은 특성이 더 정확하게 정의되어, LiDAR 시스템의 측정 불확실성이 줄어들고 정밀도가 향상될 수 있다. 특히 조도가 낮거나 노이즈가 큰 환경에서 고전적인 LiDAR 시스템이 겪는 잡음 문제를 줄여주어 더 나은 측정을 기대할 수 있다.

빛을 이용한 LiDAR 와 비교하여 라디오파를 이용하는 RADAR 의 경우 양자 상태 생성이 까다로워서 양자 RADAR 구현에 상대적으로 어려움이 있다. 얽힘 광자와 마찬가지로 라디오파 대역에서 바로 얽힘 상태를 생성하는 방식과 동시에 가시광 또는 적외선 대역의 얽힘 광자쌍을 라디오파로 파장 변환하는 방식등이 제안되고 있다.

고전적인 레이더에서는 탐지하기 어려운 물체(예: 스텔스 항공기나 작은 드론)를 양자 레이더가 더 정확하게 탐지할 수 있는 큰 장점이 존재하여 군사 및 방위 분야, 감시 시스템, 항공 교통 제어 및 저반사 목표물 탐지 등에 사용 가능할 것으로 예상된다. 양자 LiDAR는 기존 시스템의 정확도 및 민감도를 능가하여 자율 주행 자동차, 환경 모니터링, 항법 분야 등, 다음 세대의 원격 탐지 및 이미징 기술에 큰 응용처가 될 수 있다.

양자계측 용어 MAP

양자계측

- 1. 양자 파라미터 추정 및 양자 메트롤로지
  - 2. 추정자와 추정값
  - 3. 추정 편향 및 추정 정확도
  - 4. 추정 불확도 및 추정 정밀도
  - 5. 크래머-라오 부등식
  - 6. 피셔 정보
  - 7. 표준 양자 한계
  - 8. 하이젠베르크 한계
- 9. 양자 토모그래피
  - 10. 압축 토모그래피 또는 그림자 토모그래피

1. 양자 파라미터 추정 및 양자 메트롤로지 (Quantum Parameter Estimation & Quantum Metrology)

양자 파라미터 추정 또는 양자 메트롤로지는 양자 역학의 원리를 활용하여 물리량을 정밀하게 측정하고 추정하는 핵심 기술이다. 양자 파라미터 추정은 상태 준비, 인코딩, 측정, 추정의 과정을 통해 물리량을 정확하고 정밀하게 추정하며, 양자 얽힘, 양자 중첩, 압축 상태 등 비고전적 양자 자원을 활용하여 샷-노이즈 한계(shot-noise)와 표준 양자 한계(standard quantum limit)를 넘어서는 정밀도를 달성하는 것을 목표로 한다. 시간, 위상, 전기장, 자기장 등 다양한 물리량의 측정에 활용되며, 크래머-라오(Cramér-Rao) 부등식과 양자 피셔 정보(quantum Fisher information)와 같은 이론적 도구를 활용해 초정밀도 목표를 실현하려는 연구가 진행되고 있다.

2. 추정자 와 추정값 (Estimator & Estimate)

추정자(estimator)는 관측된 데이터를 바탕으로 미지(uknown)의 파라미터를 추정하기 위한 규칙이나 함수이다. 추정자는 데이터를 입력받아 추정값(estimate)을 산출하며, 통계적 분석에서 핵심적인 역할을 한다. 예를 들어, 표본 평균이나 최대우도(maximum-likelihood) 추정자가 있다. 추정자의 성능은 편향(bias)과 분산(variance)에 의해 평가되며, 효율적인 추정자를 선택하는 것이 중요하다.

3. 추정 편향 및 추정 정확도 (Bias & Accuracy)

추정 편향(bias)은 추정값(estimate)의 평균이 파라미터 참값(true value)에서 얼마나 벗어나는지를 나타내는 척도로서, 추정자가 시스템적인 오류나 불완전한 모델링으로 인해 추정값이 일관되게 참값보다 크거나 작게 산출되는 현상을 의미한다. 이러한 편향이 존재하면 추정의 정확도(accuracy)가 떨어지게 된다. 추정 정확도는 추정값이 실제값과 얼마나 가까운지를 나타내는 척도로, 편향이 작을수록 추정 정확도가 높다고 할 수 있다. 따라서 추정 정확도를 높이기 위해서는 추정 편향을 최소화하는 것이 매우 중요하다. 추정 편향은 추정 방법의 선택, 데이터의 특성, 측정 과정에서의 오류 등에 의해 발생할 수 있으며, 양자 메트롤로지에서는 이러한 추정 편향을 최소화하여 측정의 신뢰성과 정확성을 확보하는 데 주력하고 있다.

4. 추정 불확도 및 추정 정밀도 (Uncertainty & Precision)

추정 불확도(uncertainty)는 유한한 횟수의 측정을 반복했을 때 얻게되는 추정값이 가지는 신뢰도 또는 재현성을 뜻한다. 일반적으로, 동일한 샘플링을 매우 많이 반복한다고 가정했을 때 얻게되는 추정값 분포의 표준편차(standard deviation) 또는 분산(variance)로 정의된다. 추정 불확도가 높으면 추정 정밀도(precision)가 낮다고 말하며, 반대로 추정 불확도가 낮으면 추정 정밀도가 높다고 말한다. 이는 측정의 일관성을 평가하는 데 중요하며, 정밀도가 높으면 동일한 조건에서 반복 추정하더라도 추정값이 크게 변하지 않는다. 반면에 정밀도가 낮으면, 추정값이 반복된 추정에 따라 추정 값이 크게 변함을 뜻한다. 즉, 추정 신뢰도가 낮아지는 것이다. 따라서 추정 정밀도를 높이는 것이, 즉 추정 불확도를 낮추는 것은 측정의 신뢰성과 품질을 높이고, 정확한 측정과 신뢰성 있는 결과를 얻기 위해 필수적이다. 양자 메트롤로지에서는 자원의 효율적인 활용과 최적의 측정 전략을 통해 추정 정밀도를 극대화하는, 즉 추정 불확도를 최소화하는 것을 목표로 한다.

5. 크래머-라오 부등식 (Cramér-Rao)

크래머-라오(Cramér-Rao) 부등식은 편향 없는 추정자의 분산에 대한 하한을 제시하며, 피셔 정보(Fisher Information)의 역수로 정의되는 크래머-라오 경계(Cramér-Rao Bound)를 통해 이론적으로 달성 가능한 최소 추정 불확도를 나타낸다. 이를 양자 역학적 상황으로 확장한 양자 크래머-라오(Quantum Cramér-Rao) 부등식은 측정 연산자나 검출기를 최적화함으로써 피셔 정보를 양자 피셔 정보(Quantum Fisher Information)로 대체하게 된다. 부등식의 하한인 양자 크래머-라오 경계(Quantum Cramér-Rao Bound)는 양자 피셔 정보의 역수로 정의되며, 주어진 양자상태가 달성할 수 있는 최고의 정밀도를 의미한다. 따라서, 양자 메트롤로지에서는 양자 얽힘이나 압축 상태와 같은 비고전적 자원을 활용하고, 측정 연산자나 검출기를 최적화하여 최대 양자 피셔 정보를 확보함으로써, 고전적 한계를 넘어서는 정밀도를 가능하게 한다.

6.피셔 정보 (Fisher Information)

피셔 정보(Fisher Information)는 관측 데이터 또는 확률 분포가 파라미터에 대해 가지는 정보량을 정량화한 척도로, 파라미터 추정의 정밀도와 불확도를 평가하는 데 사용된다. 피셔 정보가 클수록 파라미터 추정이 더 정밀해지며, 이는 크래머-라오 경계(Cramér-Rao Bound)와 같은 이론적 추정 불확도 한계를 결정하는 데 핵심적이다. 크래머-라오 부등식은 전통적인 통계적 설정에서 피셔 정보를 기반으로 편향 없는 추정자의 분산에 대한 하한을 제시하며, 주어진 양자상태 및 측정연산자 또는 검출기에 따라 한계가 달라진다. 반면, 양자 크래머-라오 부등식은 피셔 정보를 양자 피셔 정보(Quantum Fisher Information)로 확장하고, 모든 가능한 측정 연산자와 검출기를 최적화하여 고전적 한계를 넘어서는 정밀도를 달성한다. 이를 통해 양자 메트롤로지에서는 양자 얽힘과 같은 비고전적 자원을 활용하여 측정 정밀도를 극대화하고, 양자 이득(Quantum Advantage)을 실현하기 위한 전략을 개발한다. 이러한 이론적 도구는 양자 센싱과 메트롤로지의 발전에 기여하며, 정밀 측정과 효율적인 자원 활용을 가능하게 하는 중요한 기반을 제공한다.

7. 표준 양자 한계 (Standard quantum limit)

표준 양자 한계(standard quantum limit)는 양자 센싱과 메트롤로지에서 고전적 자원을 사용할 때 달성할 수 있는 측정 정밀도(precision)의 궁극적인 한계를 의미한다. 이는 측정 및 추정에 사용된 자원의 양, 예를 들어 입자 수의 제곱근 역수에 비례하여 제한됨을 나타낸다. 표준 양자 한계는 샷-노이즈 한계와 밀접하게 연관되어 있으며, 고전적 측정 방법으로는 이 한계를 넘어서는 정밀도를 달성할 수 없다. 그러나 양자 얽힘(entanglement)이나 압축 상태(squeezed states)와 같은 양자 자원을 활용하면 표준 양자 한계를 뛰어넘어 더 높은 정밀도를 실현할 수 있다. 이는 하이젠베르크 한계(Heisenberg limit)와 같은 더욱 향상된 정밀도 한계를 가능하게 하여, 양자 메트롤로지에서 중요한 목표가 된다. 따라서 표준 양자 한계는 양자 기술의 발전과 양자 이득을 실현하기 위한 중요한 기준점으로 작용하며, 정밀 측정의 한계를 이해하고 이를 극복하기 위한 전략을 수립하는 데 필수적인 개념이다. 양자 메트롤로지 연구자들은 이러한 한계를 넘어서는 측정 기술을 개발함으로써, 과학적 연구와 산업 응용에서 더욱 정확하고 신뢰성 있는 결과를 도출하고자 노력하고 있다.

8. 하이젠베르크 한계 (Heisenberg Limit)

하이젠베르크 한계(Heisenberg limit)는 양자 물리계에서 달성할 수 있는 측정 정밀도(precision) 또는 불확도(uncertainty)의 궁극적인 한계를 의미한다. 이는 하이젠베르크의 불확정성 원리(uncertainty principle)에 기반하여 특정 조건에서 측정 가능한 최대 정밀도 또는 최소 불확도를 정의한다. 일반적으로 양자 얽힘과 같은 양자 특성을 활용하면 하이젠베르크 한계에 도달할 수 있다는 것이 알려져 있다. 이 한계에서는 정밀도가 자원의 평균 입자 수의 역수로 스케일링되며, 이를 하이젠베르크 스케일링이라고 한다. 하이젠베르크 한계는 측정 자원과 측정 기법을 최적화하여 달성 가능하며, 샷-노이즈 한계(shot-noise limit)와 표준 양자 한계(standard quantum limit)를 뛰어넘는 정밀도를 달성할 수 있으므로 양자 센싱과 양자 메트롤로지에서 중요한 목표가 된다. 따라서, 양자 기술 발전에 있어 하이젠베르크 한계는 이론적 지침이자 실제 기술적 도전 과제이다.

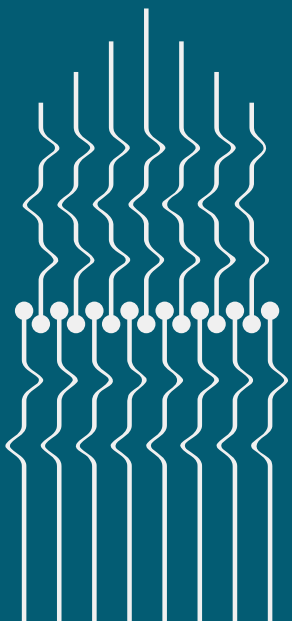
9. 양자 토모그래피 (Quantum Tomography)

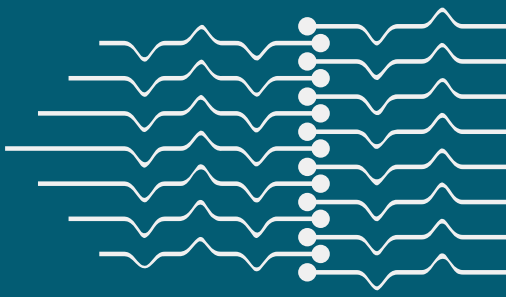
양자 토모그래피(Quantum Tomography)는 양자 상태, 양자 프로세스, 또는 양자 검출기의 특성을 정밀하게 추정하고 재구성하는 방법론이다. 이는 측정을 통해 대상의 행렬 요소를 추정하여 양자 시스템의 상태와 동작을 파악하는 데 사용된다. 양자 토모그래피는 크게 양자 상태 토모그래피, 프로세스 토모그래피, 검출기 토모그래피로 구분된다. 양자 상태 토모그래피(state tomography)는 시스템의 밀도 행렬(density matrix)을 추정하여 양자 상태를 재구성하는 기술이다. 프로세스 토모그래피(process tomography)는 양자 연산 과정을 분석하며, 검출기 토모그래피(detector tomography)는 검출기의 반응 특성을 모델링한다. 이 기술은 양자 컴퓨팅, 양자 통신, 양자 센싱 등 다양한 분야에서 필수적이다. 전통적인 토모그래피는 높은 정확도를 제공하지만, 시스템 크기가 커질수록 요구되는 자원이 기하급수적으로 증가하는 문제가 있다. 이를 해결하기 위해 압축 토모그래피나 그림자 토모그래피와 같은 새로운 방법론이 개발되고 있다.

10. 압축 토모그래피 또는 그림자 토모그래피 (Compressed Tomography or Shadow Tomography)

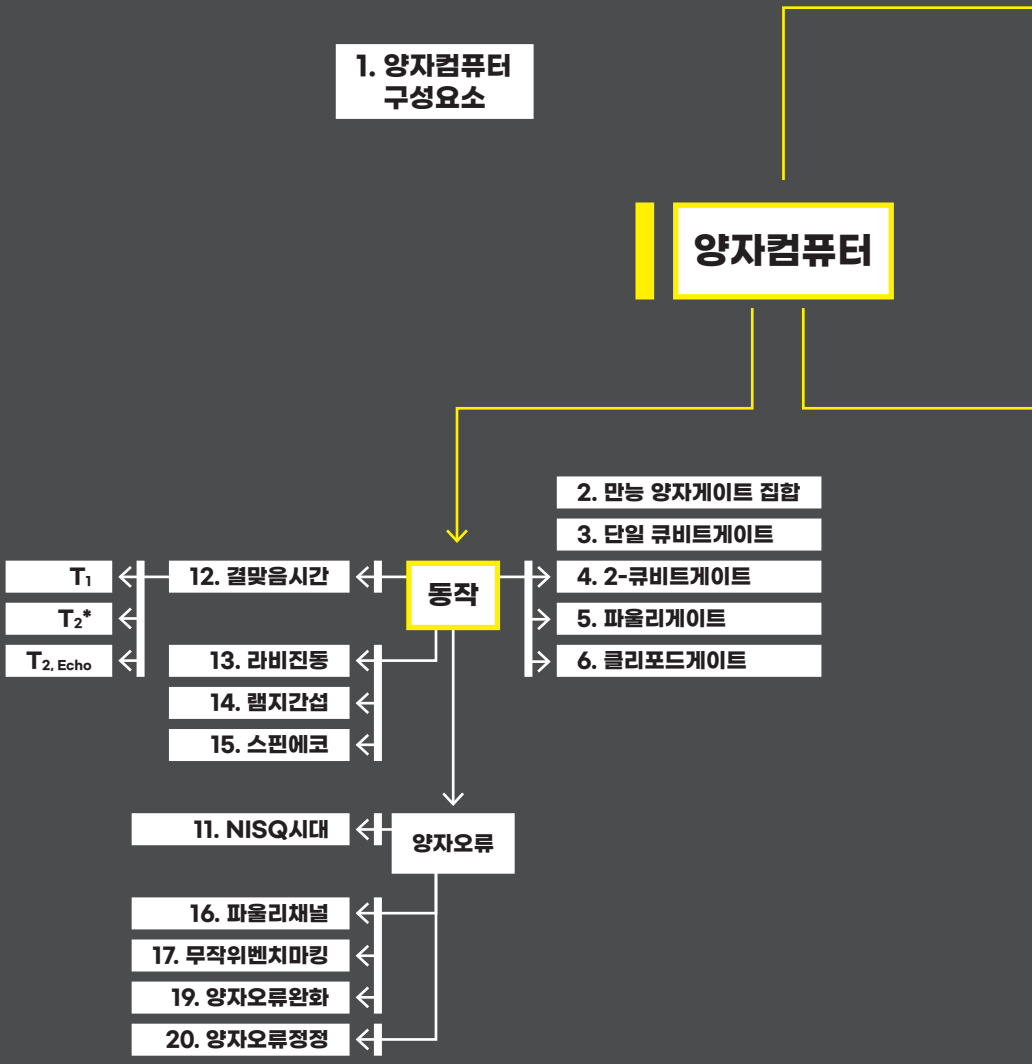
압축 토모그래피(Compressed Tomography)와 그림자 토모그래피(Shadow Tomography)는 양자 상태와 프로세스를 효율적으로 추정하기 위한 두 가지 핵심 기법으로, 각기 다른 목적과 강점을 가진다. 압축 토모그래피는 전체 상태의 복원을 목표로 하며, 압축 감지(compressed sensing) 이론을 활용하여 적은 측정으로 대규모 양자 시스템에서도 정확한 상태 재구성을 가능하게 한다. 이 기법은 상태의 희소성이나 구조적 특성을 활용해 측정 자원을 줄이고, 양자 컴퓨팅, 통신, 센싱 등 다양한 분야에서 실용적이다. 반면, 그림자 토모그래피는 양자 상태의 특정 성질(예: 기대값, 충실도 등)을 추출하는 데 중점을 두며, 무작위 측정을 통해 필요한 물리량만 선택적으로 계산하여 자원을 더욱 절약한다. 그림자 토모그래피는 전체 상태를 복원하지 않으면서도 대규모 시스템에서 신속한 데이터 처리를 통해 정밀한 물리량 추정을 가능하게 하며, 효율적인 양자 정보 처리를 위한 중요한 기술로 활용된다. 두 기법 모두 노이즈와 결맞음 붕괴 등 실환경 문제에 강인하며, 목적에 따라 상호 보완적으로 적용될 수 있다.

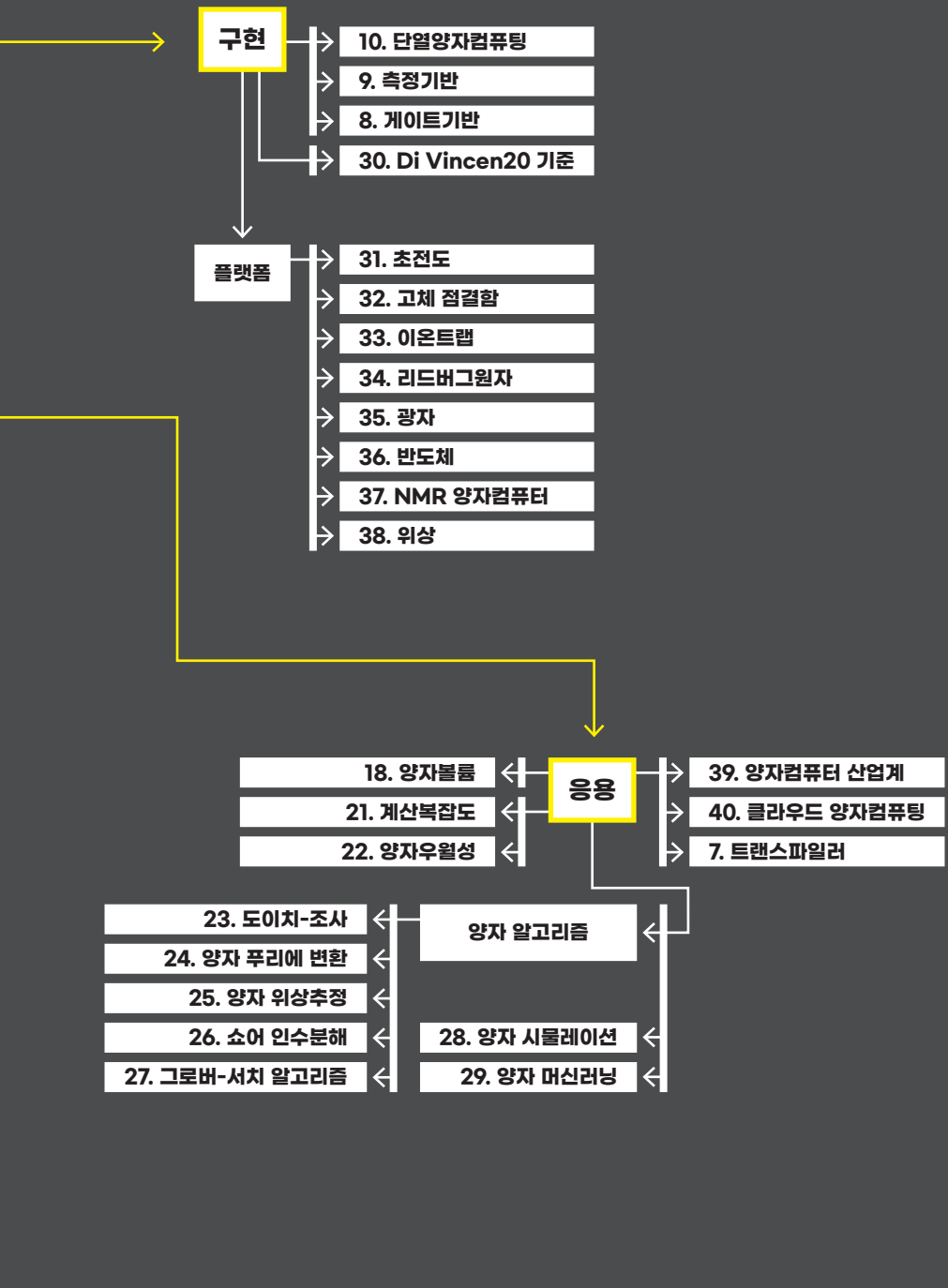
3. 양자컴퓨팅





양자컴퓨팅 용어 MAP


1. 양자컴퓨터 구성요소
양자컴퓨터
2. 만능 양자게이트 집합
3. 단일 큐비트게이트
4. 2-큐비트게이트
5. 파울리게이트
6. 클리포드게이트
동작
12. 결맞음시간
T_1
T_2^*
$T_{2,\,Echo}$
13. 라비진동
14. 램지간섭
15. 스핀에코
양자오류
11. NISQ시대
16. 파울리채널
17. 무작위벤치마킹
19. 양자오류완화
20. 양자오류정정


구현
10. 단열양자컴퓨팅
9. 측정기반
8. 게이트기반
30. Di Vincen20 기준
플랫폼
31. 초전도
32. 고체 점결함
33. 이온트랩
34. 리드버그원자
35. 광자
36. 반도체
37. NMR 양자컴퓨터
38. 위상
18. 양자볼륨
21. 계산복잡도
22. 양자우월성
응용
39. 양자컴퓨터 산업계
40. 클라우드 양자컴퓨팅
7. 트랜스파일러
23. 도이치-조사
24. 양자 푸리에 변환
25. 양자 위상추정
26. 쇼어 인수분해
27. 그로버-서치 알고리즘
양자 알고리즘
28. 양자 시뮬레이션
29. 양자 머신러닝

1. 양자컴퓨터 구성 요소

양자컴퓨터는 양자역학의 원리를 활용하여 정보를 저장하고 처리하는 장치로 큐비트, 양자게이트, 양자측정으로 구성된다.

큐비트(Qubit)는 양자 정보를 저장하고 처리하는 최소 단위로, '양자(Quantum)'와 '비트(Bit)'의 합성어다. 큐비트는 0과 1뿐만 아니라 두 상태가 동시에 존재하는 중첩(Superposition) 상태를 표현할 수 있다. 또한, 양자얽힘(Entanglement)을 통해 하나의 큐비트 상태를 읽는 것이 다른 큐비트 상태에 영향을 미칠 수 있다.

양자게이트는 큐비트의 상태를 특정 규칙에 따라 변화시키며, 이를 조합해 양자 알고리즘을 구현한다. 중첩과 양자얽힘 특성을 활용하면 특정 문제에 대해 기존 컴퓨터보다 훨씬 빠른 계산이 가능하다는 것이 잘 알려져 있다.

양자측정은 중첩 상태에 있는 큐비트를 특정한 상태로 붕괴시키며, 그 결과는 확률적으로 나타난다. 예를 들어, 큐비트 상태 $|\psi\rangle=a|0\rangle+b|1\rangle$를 반복해서 측정하면, 0과 1로 읽힐 확률은 각각 $|a|^2$와 $|b|^2$이다.

고전컴퓨터에서 비트가 전압이나 자화 방향 등 다양한 물리적 상태로 구현되고 그에 따라 논리게이트와 읽는 방식이 달라지는 것처럼, 초전도 회로, 광자, 이온, 중성원자 등 다양한 양자 시스템을 활용해 양자컴퓨터를 구현하며 각각 고유한 기술적 장단점이 있다.

2. 만능 양자게이트 집합

고전컴퓨터에서 대표적인 만능 논리게이트로는 NAND 게이트와 NOR 게이트가 있다. 이들 중 하나만을 사용해도 AND, OR, NOT 게이트를 포함한 모든 논리 게이트를 구현할 수 있으며, 더 나아가 모든 이진 함수를 구현할 수 있다는 사실이 잘 알려져 있다.

양자컴퓨터에서도 임의의 양자연산을 구현할 수 있는 만능 양자게이트 집합이 존재한다. Solovay-Kitaev 정리에 따르면 유한한 수의 양자게이트만으로도 임의의 양자연산을 원하는 정확도로 효율적으로 근사할 수 있다. 대표적인 만능 양자게이트 집합으로는 Hadamard 게이트, T 게이트, CNOT 게이트로 구성된 집합이 있으며, 이는 이 세 가지 양자 게이트를 신뢰성 있게 구현할 수 있다면 모든 양자 알고리즘을 실행할 수 있는 만능 양자 컴퓨터를 만들 수 있다는 것을 뜻한다. 이러한 이유로 연구자들은 만능 양자게이트 집합을 구성하는 기본 게이트들을 효율적이고 정밀하게 구현하는 기술 개발에 집중하고 있다.

3. 단일 큐비트 게이트

고전적인 비트는 0 또는 1의 두 가지 상태만을 가지므로 적용 가능한 단일 비트 게이트는 상태를 반전시키는 것뿐이다. 그러나 큐비트는 |0>과 |1>의 다양한 중첩 상태를 가질 수 있어 다양한 단일 큐비트 연산이 가능하다. 이는 다음과 같은 2차원 복소수 공간에서의 유니터리 변환(Unitary transformation)으로 기술된다.

$$|\psi\rangle = a|0\rangle + b|1\rangle = \begin{pmatrix} a \\ b \end{pmatrix} \Rightarrow U|\psi\rangle = U\begin{pmatrix} a \\ b \end{pmatrix} = \begin{pmatrix} c \\ d \end{pmatrix} = c|0\rangle + d|1\rangle$$

따라서 모든 단일 큐비트 게이트는 2x2 복소 행렬 U로 나타낼 수 있다. 다음은 $|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$ 과 $|1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$ 기저로 표현한 대표적인 단일 큐비트 게이트 예시를 보여준다.

Indentity	$I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$
Pauli-X	$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$
Pauli-Y	$Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}$
Pauli-Z	$Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$
Hadamard	$H = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$
T	$T = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\frac{\pi}{4}} \end{pmatrix}$

4. 2-큐비트 게이트

2-큐비트 게이트는 |00>, |01>, |10>, |11>의 선형 결합으로 이루어진 2-큐비트 상태에 작용하는 유니터리 변환이다. 간단하게 말하면, 두 큐비트의 양자상태를 다른 상태로 변환하는 게이트이다.

2-큐비트 게이트의 기본적인 예로는 두 큐비트의 상태를 서로 바꾸는 SWAP 게이트가 있다. 큐비트 1의 상태가 $|\psi\rangle_1$, 큐비트 2의 상태가 $|\phi\rangle_2$일 때, SWAP 게이트를 적용하면 두 큐비트의 상태가 서로 바뀌어 큐비트 1은 $|\phi\rangle_1$이 되고, 큐비트 2는 $|\psi\rangle_2$가 된다.

$$\mathrm{SWAP}(|\psi\rangle_1 \otimes |\phi\rangle_2) = |\phi\rangle_1 \otimes |\psi\rangle_2$$

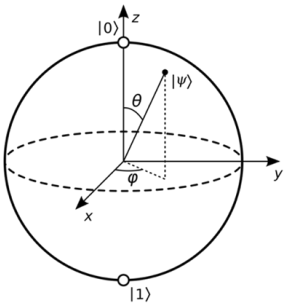
또 다른 중요한 2-큐비트 게이트로는 제어 게이트가 있다. 이 게이트가 적용되는 두 큐비트를 각각 제어 큐비트(Control qubit)와 타겟 큐비트(Target qubit)라고 할 때, 제어 큐비트 상태에 따른 조건부 단일 큐비트 게이트를 타겟 큐비트에 작용한다. 예를 들어 제어 큐비트가 |0> 상태일 때는 타겟 큐비트에 아무런 변화를 주지 않고, 제어 큐비트가 |1> 상태일 때에 타겟 큐비트에 X게이트를 작용하는 CNOT (Controlled-NOT) 게이트가 이에 해당된다.

$$\mathrm{CNOT}[(a|0\rangle_c + b|1\rangle_c) \otimes |\phi\rangle_t] = a|0\rangle_c \otimes |\phi\rangle_t + b|1\rangle_c \otimes X|\phi\rangle_t$$

이러한 조건부 작용을 잘 활용하면 두 큐비트의 상관관계를 형성할 수 있어 양자 얽힘을 구현하는데 중요한 역할을 한다.

5. 파울리 게이트

파울리 게이트란 파울리 행렬로 표현할 수 있는 게이트를 의미한다. 파울리 행렬 X, Y, Z의 작용은 각각 블로흐 구의 X, Y, Z 축을 기준으로 큐비트 상태를 180도 회전시키는 연산을 의미한다.



[그림: 블로흐 구 위에 표현한 큐비트[1]]

참고로 큐비트 상태는 길이가 1인 벡터로 표현되며 고도각(θ)과 방위각(ϕ)만으로 블로흐 구 표면에 특정된다: $|\psi\rangle = \cos\frac{\theta}{2}|0\rangle + \sin\frac{\theta}{2}e^{i\phi}|1\rangle$. 이를 바탕으로 생각해볼 때 $|\psi\rangle = a|0\rangle + b|1\rangle$ 상태에 가해지는 각 파울리 게이트의 작용은 다음과 같다.

$$X|\psi\rangle = b|0\rangle + a|1\rangle,\ Y|\psi\rangle = -ib|0\rangle + ia|1\rangle,\ Z|\psi\rangle = a|0\rangle - b|1\rangle$$

X는 |0>과 |1> 상태를 반전시켜 비트 반전 게이트, Y는 비트와 위상을 동시에 반전시켜 비트-위상 반전 게이트, Z는 위상을 반전시켜 위상 반전 게이트라는 별칭을 가지고 있다. X⊗Z와 같이 여러 큐비트에 작용하는 파울리 행렬도 파울리 게이트에 해당된다.

1 https://en.wikipedia.org/wiki/Qubit

6. 클리포드 게이트

항등 행렬 I와 파울리 행렬의 텐서곱으로 표현되는 n-큐비트 파울리 행렬에 게이트 작용을 하였을 때 n-큐비트 파울리 행렬로 남아 있다면 해당 게이트를 클리포드 (Clifford) 게이트라고 한다. 이를 수학적으로 표현하면 다음과 같다. $C: P \in P_n \mapsto CPC^\dagger \in P_n$. 여기서 P는 임의의 n-큐비트 파울리 행렬, P_n은 n-큐비트 파울리 행렬 집합, C는 클리포드 게이트를 나타낸다.

대표적인 클리포드 게이트로는 파울리 게이트, Hadamard 게이트, CNOT 게이트가 있다. 예를 들어, Hadamard 게이트를 작용한 파울리 Z 행렬은 여전히 파울리 행렬로 남아 있다: $HZH^\dagger = X$.

당연히 모든 양자 게이트가 클리포드 그룹에 속하는 것은 아니다. 비-클리포드 게이트의 대표적인 예는 T 게이트이다. $TXT^\dagger = e^{i\frac{\pi}{4}}\begin{pmatrix} 0 & -i \\ 1 & 0 \end{pmatrix}$와 같이 파울리 행렬에 T 게이트를 적용하더라도 그 결과가 파울리 행렬이 아닐 수 있다.

Gottesman-Knill 정리에 따르면 클리포드 게이트만으로 구성된 양자 회로는 고전컴퓨터로도 효율적으로 시뮬레이션 할 수 있다. 따라서 고전컴퓨팅보다 빠른 양자컴퓨팅을 시연하기 위해서는 비-클리포드 게이트의 활용이 필수적이다.

7. 트랜스파일러

트랜스파일러(Transpiler)는 양자 하드웨어의 물리적 연결 구조나 활용 가능한 양자게이트를 고려하여 양자 회로를 변환하고 최적화하는 기술이다. 일반적으로 다음의 순서로 구현된다. 먼저 복잡한 다중 큐비트 게이트들은 1-큐비트, 2-큐비트 기본 게이트 조합으로 분해한다. 그 다음, 하드웨어의 물리적 큐비트 배열에 맞춰 큐비트들을 배정하고 하드웨어의 큐비트 연결 방식을 고려하여 큐비트 간 게이트 연산을 최적화한다. 마지막으로, 양자회로를 하드웨어에서 사용할 수 있는 게이트 집합으로 변환한 후 최소한의 게이트로 회로가 실행될 수 있도록 한다. 더 나아가 노이즈를 최소화하고 실행 속도를 개선하기 위한 노력이 수반되어야 효율적인 양자컴퓨팅이 가능하다.

8. 게이트 기반 양자컴퓨팅

게이트 기반 양자컴퓨팅(Gate-based quantum computing)은 양자회로 모델(Quantum circuit model)을 사용하여 양자 알고리즘을 양자게이트 단위의 기초 연산으로 나누어 연산하는 방식이다. 고전 컴퓨터가 논리게이트를 통해 데이터를 처리하듯이, 양자 컴퓨터는 양자게이트를 사용해 큐비트의 상태를 조작하여 연산을 수행한다.

게이트 기반 양자컴퓨팅의 연산은 세 단계로 이루어진다. 우선 큐비트를 |0> 상태 또는 특정 상태로 초기화한다. 이 후 양자 알고리즘에 따라 다양한 양자 게이트를 큐비트에 적용하여 상태를 변화시킨다. 이 과정에서 중첩과 얽힘 상태가 생성될 수 있다. 최종적으로 큐비트 상태를 측정하여 양자정보를 고전정보로 변환한다.

쇼어 소인수 분해 알고리즘, 그로버 검색 알고리즘 등 대부분의 양자 알고리즘은 양자 회로 모델로 개발되어 있어 게이트 기반 양자컴퓨터에서의 구현이 용이하다. 이 방식은 현재 가장 널리 활용되고 있는 양자컴퓨터 구현 방식이다.

9. 측정 기반 양자컴퓨팅

측정 기반 양자컴퓨팅(Measurement-based quantum computing)은 사전에 대규모 양자 얽힘 상태를 준비하고 연속적인 측정을 통해 양자 알고리즘을 구현하는 방식이다. 확정적인 2-큐비트 게이트를 만들기 힘든 광자 시스템에서 주로 고려된다.

측정 기반 양자컴퓨팅의 과정은 다음과 같다. 먼저 대규모 양자 얽힘 상태인 클러스터 상태로 큐비트들을 준비한다. 이 후 양자 연산을 위해 각 큐비트들을 순차적으로 측정하면서 측정 결과에 따른 피드포워드 작용을 다른 큐비트에 가한다. 양자적으로 얽혀 있는 상태에서는 한 큐비트의 측정 결과가 다른 큐비트에 영향을 끼치기 때문에 측정 기저에 따라 다양한 양자게이트 구현이 가능하다. 연산은 한 방향으로만 진행되며, 마지막 큐비트까지 측정이 완료되면 전체 연산이 끝나고 원하는 결과를 얻을 수 있다.

측정 기반 양자컴퓨팅과 게이트 기반 양자컴퓨팅은 구현 방식에서 차이가 있지만 이론적으로는 동치인 모델이다. 둘 다 범용 양자계산을 수행할 수 있으며 동일한 계산을 구현할 수 있음이 알려져 있다.

10. 단열 양자컴퓨팅

단열 양자컴퓨팅(Adiabatic quantum computing)은 단열정리(adiabatic theorem)에 기반한 모델로 양자 시스템을 천천히 변화시켜 계산이 어려운 특정 상태의 해를 얻는다.

구체적인 단열 양자컴퓨팅의 과정은 다음과 같다. 먼저 우리가 쉽게 계산하고 준비할 수 있는 헤밀토니안의 바닥 상태를 준비한다. 그 다음 구하고자 하는 해를 바닥 상태로 가지는 헤밀토니안이 되도록 시스템의 헤밀토니안을 천천히 변화시킨다. 여기서 중요한 점은 단열 정리가 적용될 만큼 시스템을 충분히 느리게 변화시켜야 한다는 것이다. 그래야만 시스템이 최종 헤밀토니안의 바닥 상태에 머물게 된다. 이 후 시스템이 목표로 하는 헤밀토니안에 도달하면, 최종 상태를 측정하여 문제의 바닥 상태 해를 얻는다.

단열 양자컴퓨팅의 단열 변화를 위해 요구되는 시간이 고전컴퓨팅의 연산 시간보다 빠르다면 양자 이득을 보일 수 있다. 단열 양자컴퓨팅은 최적화 문제에 효과적일 수 있다고 알려져 있지만 단열 조건을 만족 시키기 어려운 유형의 문제에 대해서는 효율성을 보장하지 않는다.

11. NISQ 시대

NISQ 시대(Noisy Intermediate-Scale Quantum era)는 2018년 John Preskill교수가 제안한 용어로 현재와 근시일 내의 양자 컴퓨팅 상태를 잘 나타낸다. 현재의 양자 컴퓨터는 적지 않은 오류가 있으며, 큐비트 수가 제한되어 있어 큰 규모의 문제를 해결하는 데에는 한계가 있다.

양자 물리계는 외부 환경과 고립되어 있을 때 안정적인 양자 상태를 유지할 수 있지만 제어 및 측정을 위해서는 큐비트를 외부와 연결해야 하기에 노이즈를 최소화하는 것이 매우 어렵다. 양자오류보정을 통해 노이즈를 줄일 수 있다고 알려져 있지만, 최근에 들어서야 양자오류보정의 유용성이 실험적으로 시연되기 시작하였다. 아직까지는 온전한 양자오류보정을 위한 충분한 큐비트 수와 기술력 확보에는 시간이 걸릴 것으로 보인다.

많은 연구자들은 NISQ 시대에서도 고전컴퓨터를 뛰어넘은 양자컴퓨터의 유용성을 보일 수 있을 것으로 전망하며 활발한 연구를 진행 중이다.

12. 결맞음 시간

큐비트는 외부와 상호작용을 하면서 양자적 성질을 잃는 결어긋남(decoherence) 과정을 겪게 된다. 큐비트가 안정적으로 양자상태를 유지할 수 있는 시간 한계를 결맞음 시간(coherence time)이라 부르고 다음과 같이 T_1과 T_2로 대표된다. T1은 높은 에너지 상태인 큐비트 |1> 상태를 얼마나 오래 동안 유지할 수 있는지를 의미하는 이완 시간(relaxation time)이다. 즉, |1> 상태가 에너지를 잃고 낮은 에너지 상태인 |0> 상태로 뒤집히는데 걸리는 시간을 의미한다. T_2는 큐비트 중첩상태에서 상대적 위상 (phase) 차이를 얼마나 일관되게 유지할 수 있는지를 나타내는 위상 어긋남 시간(dephasing time)이다. T_2는 에너지 이완에 영향을 받아 최대 T_1의 2배로 제한되며, 추가적인 위상 어긋남 효과가 있다면 $2T_1$보다 더 낮아진다.

양자컴퓨터에서의 대부분의 오류는 결어긋남에 의해서 발생한다. 따라서 결맞음 시간이 길수록 양자게이트의 오류를 줄일 수 있어 복잡한 양자컴퓨팅 수행이 가능하다.

13. 라비 진동

라비 진동(Rabi oscillation)은 두 양자 상태 사이에서 일어나는 주기적인 전이를 의미한다. 원자의 에너지 간격(공진 주파수)과 전자기파의 진동 주파수가 일치하면 강한 상호작용이 발생하여 원자 양자 상태의 주기적으로 변화가 발생한다.

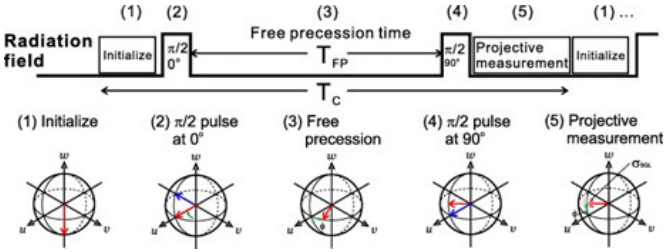
초기 상태가 바닥 상태에 있을 경우, 흥분 상태와 바닥 상태 전이가 반복되며 시간에 따른 바닥 상태 존재 확률은 다음과 같다.

$$P_0(t) = \frac{\sin^2\left(\frac{\sqrt{\Omega^2+\delta^2}}{2}t\right)}{1+(\delta/\Omega)^2}.$$

Ω는 라비 진동수이고, 전자기장과 2준위 원자 간의 상호작용 세기에 비례한다. δ는 원자의 공진 주파수와 전자기파의 진동 주파수 간의 차이를 의미한다. 전자기장의 세기가 세질수록 라비 진동수가 증가하며, 전자기장의 주파수가 공명주파수에서 멀어질수록 라비 진동의 진폭은 감소하지만 라비 진동수는 증가한다.

라비 진동은 양자 시스템의 양자 상태 제어에 필수적인 현상이다. 중성원자, 이온 트랩, 다이아몬드 점결함, 초전도 회로, 반도체 양자점 등 다양한 큐비트 시스템에 전자기파를 인가하여 라비 진동을 유도할 수 있다. 이를 통해 큐비트의 상태를 정확히 제어하고 양자게이트를 구현할 수 있다.

14. 램지 측정



[그림] 단계별 램지 측정 설명[2]

램지 측정(Ramsey measurement)는 큐비트의 위상 어긋남 시간 T_2를 측정하고, 큐비트의 공명 주파수를 보다 정밀하게 측정하는데 활용된다. 큐비트 주파수가 ω_q일 때 $\omega_d=\omega_q+\delta$의 주파수로 전자기파 펄스를 가하면 라비 진동이 일어난다. 만약 $Y_{\pi/2}$ 게이트에 해당하는 만큼 동안만 전자기파 펄스를 |0> 상태 큐비트에 가하면 $(|0\rangle+|1\rangle)/\sqrt{2}$로 중첩 상태를 만들 수 있으며, 이후 큐비트는 |0>과 |1> 사이에 고유 주파수의 속도로 상대 위상 변화를 겪는다.

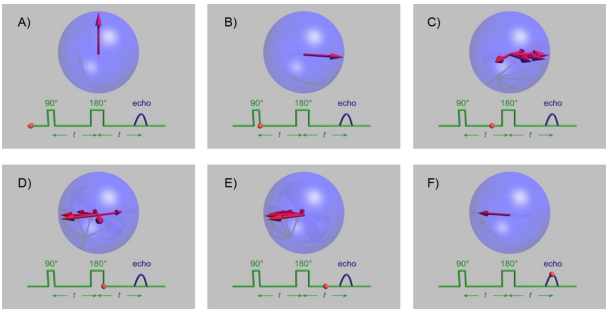
추가적으로 동일한 $Y_{\pi/2}$에 해당하는 전자기파 펄스를 쏴주면 |1>상태로 전이하는데, 만약 큐비트 주파수와 펄스 주파수가 일치하지 않으면 |1>로 온전히 전이하지 않고 두 $Y_{\pi/2}$ 펄스의 시간 간격에 따라 진동하는 신호가 관측

2 N Shiga and M Takeuchi 2012 New J. Phys. 14 023034

된다. 이 때 신호 진동 주파수는 두 주파수의 차이 δ에 해당되어 이를 통해 큐비트의 정확한 공진 주파수를 알 수 있다.

또한 큐비트 위상 어긋남 효과에 의해서 램지 측정의 진동 진폭이 감소한다. 이 감소 효과를 분석함으로써 큐비트의 위상 어긋남 시간 T_2^* 값을 추정할 수 있다.

15. 스핀 에코 측정



[그림] 단계별 스핀 에코 측정 설명[3]

스핀 에코(Spin Echo) 측정은 램지 측정과 비슷하지만, 두 $Y_{\pi/2}$펄스 사이에 추가로 파울리 Y 게이트 해당하는 Y_{π}펄스를 삽입해 저주파 위상 노이즈를 일부 제거한 후 위상 어긋남 효과를 측정하는 방법이다. 스핀 에코 측정으로 얻은 큐비트의 결맞음 시간은 $T_{2,Echo}$로 표현되며 램지 측정으로 얻은 T_2^*보다는 높은 값을 가진다.

CPMG(Carr-Purcell-Meiboom-Gill) 방법은 보다 확장된 형태로, 두 $Y_{\pi/2}$ 펄스 사이에 Y_{π} 펄스를 여러 번 반복하여 큐비트의 결맞음 상태를 더 오랫동안 유지하는 방법이다. 펄스 간격이 줄어들수록 더 높은 고주파 노이즈를 제거할 수 있으며 이를 활용해 양자게이트를 만들거나 외부 노이즈로부터 큐비트를 보호할 수 있다.

3 https://en.wikipedia.org/wiki/Spin_echo

16. 파울리 채널

파울리 채널(Pauli channel)은 양자컴퓨팅에서 발생하는 확률적 오류를 기술하는 대표적인 양자 오류 모델이다. 이 모델에서는 원치 않는 파울리 게이트들이 특정 확률로 양자 상태에 적용되며, 클라우스(Kraus) 표현법을 사용하여 다음과 같이 나타낼 수 있다 .

$$\mathcal{E}(\rho) = \sum_{P \in \mathbb{P}^{\otimes n}} p_P \, P\rho P^\dagger$$

$\mathcal{E}$는 n-큐비트 시스템에 대해 적용되는 파울리 채널이며, P는 n-큐비트 파울리 그룹에 속하는 파울리 게이트, p_P는 각 파울리 오류가 발생할 확률을 나타낸다.

파울리 오류 X, Y, Z는 비트 반전, 비트-위상 반전, 위상 반전에 해당하여 직관적인 이해가 가능하며, 양자 채널을 다양한 파울리 게이트로 감싸는 파울리 트윌링(twirling) 기법을 사용하여 복잡한 양자채널을 파울리 채널로 변환이 가능하다. 따라서 대다수의 양자정보 기술 프로토콜과 양자오류정정 연구에서는 파울리 채널로 오류를 가정한다.

17. 무작위 벤치마킹

무작위 벤치마킹(Randomized Benchmarking)은 양자컴퓨터의 게이트 오류율을 측정하는 대표적인 기법이다. 구체적으로는 측정결과가 |0>이 나오도록 무작위적인 클리포드 게이트 시퀀스를 준비하고, 구체적으로 클리포드 양자 게이트 시퀀스의 깊이에 따른 |0> 상태 측정확률을 얻는다. 이 측정확률은 시퀀스 깊이에 따라 기하급수적으로 감소할 것이며, 이를 피팅하여 게이트가 만들어내는 오류율을 추정할 수 있다. 이 방법은 SPAM 오류(State preparation and measurement; 상태 준비 및 측정 오류)를 제외한 게이트 자체의 오류만을 얻어내는 데 유용하다.

무작위 회로를 실행한 후, 측정된 분포와 이상적인 양자 상태 분포 간의 교차 엔트로피를 계산하여 시스템의 성능을 평가하는 교차 엔트로피 (Cross-entropy) 벤치마킹, 파울리 게이트를 사용하여 각 게이트의 파울리 오류를 평가하는 기법인 순환 (Cycle) 벤치마킹 등 다양한 무작위 벤치마킹 기법들이 양자 컴퓨터의 성능을 보다 정밀하게 평가하기 위해 활발히 연구되고 있다.

18. 양자 볼륨

양자 볼륨(Quantum Volume)은 양자 컴퓨터의 확장성(scalability)을 보다 종합적으로 평가할 수 있는 성능 지표로, 2018년 IBM에서 제시한 개념이다. 양자 볼륨은 게이트 오류율, 큐비트 연결성과 같은 요소들도 함께 고려하여, 큐비트 수(N)와 실질적으로 활용가능한 회로 깊이(d)를 동시에 평가한다. 예를 들어, 큐비트 수가 많더라도 오류율이 높고 큐비트 연결성이 낮다면 양자 볼륨은 낮게 평가된다. 주요 양자 컴퓨팅 기업들은 양자 볼륨을 통해 시스템 성능을 발표하는 추세이며, 이를 양자 컴퓨터 발전을 측정하는 중요한 척도로 활용하고 있다.

19. 양자오류완화

양자오류완화(Quantum error mitigation)는 여러 번의 측정으로 양자 컴퓨터의 오류를 추정하고 고전적인 계산 기법으로 보정하여 양자 연산 결과의 정확도를 높이기 위한 방법이다. 오류 추정 및 고전 계산에는 많은 시간이 추가로 소요되어 양자 연산의 이득이 많이 희석되는 단점이 있다. 그러나 이는 NISQ 장치에서도 유용한 양자 컴퓨팅 결과를 얻을 수 있도록 돕는다. 오류완화 기법은 오류를 후처리하는 데 초점을 맞추고 있으며, 실시간으로 양자 상태의 오류를 보정하는 양자오류보정(quantum error correction)과는 차이가 있다.

대표적인 오류완화 방법으로는 ZNE(zero-noise extrapolation)가 있다. ZNE는 타겟 양자회로를 수정하여 노이즈의 양을 의도적으로 증가시킨 후 양자 연산의 결과를 얻는다. 여러 노이즈 양에 대한 결과를 바탕으로 역산하여 노이즈가 없는 연산 결과를 추정한다. 양자회로를 구현할 때 노이즈를 의도한대로 증가시키지 못한다면 추정 모델에 오류가 발생하여 역산한 연산 결과가 틀려질 수 있다.

또 다른 오류완화 방법인 PEC(probabilistic error cancellation)는 여러 연산 결과를 확률적으로 더하고 빼는 방식으로 조합해 오류 없는 연산 결과를 복원하는 방법이다. 이 방법은 역산과정없이 측정 결과를 얻을 수 있다는 장점이 있지만, ZNE에 비해 노이즈에 민감하며 더 많은 측정이 필요하다.

20. 양자오류보정

양자오류보정(Quantum error correction)은 상태 초기화, 양자 게이트, 양자 측정 등 다양한 양자 연산 과정에서 발생하는 오류를 실시간으로 탐지하고 수정하여 양자 컴퓨팅의 신뢰성을 높이는 필수 기술이다. 고전오류보정은 비트를 중복 인코딩하여 다수결로 오류를 검출하고 수정하지만, 양자상태는 복제 불가능성 정리(no-cloning theorem)에 의해 정보를 복사할 수 없다. 대신 양자오류보정은 여러 물리 큐비트로 구성된 양자 얽힘 상태를 하나의 논리 큐비트로 사용하여 오류를 감지하고 보정합니다.

오류가 발생한 위치와 종류를 파악하기 위한 측정을 신드롬 측정(Syndrome measurement)라 하며, 양자얽힘 상태를 논리 큐비트로 사용하면 큐비트 정보를 붕괴시키지 않고 오류 정보를 얻어낼 수 있다. 양자오류보정의 과정은 다음과 같다. 신드롬 측정 결과를 디코딩하여 오류 위치와 종류를 파악하고 이에 맞는 보정 연산을 적용해 원래 상태로 복원한다.

양자오류보정이 효과적이려면 시스템의 오류율이 임계 오류율 이하이어야 하며, 이를 만족하면 물리 큐비트 수를 늘려 오류율을 기하급수적으로 낮출 수 있다. 따라서 양자오류보정을 실현하기 위해서는 임계 오류율 이하의 연산과 많은 물리 큐비트가 함께 필요하다.

21. 계산복잡도

계산복잡도 이론(Computational complexity theory)은 특정 문제를 해결하는 데 필요한 시간과 메모리와 같은 자원에 따라 계산 난이도를 분석한다. 이는 주어진 문제가 얼마나 효율적으로 해결될 수 있는지를 평가하며, 문제의 입력 크기(input size)가 증가함에 따라 시간과 공간 복잡도가 어떻게 변하는지를 분석한다. 이를 정량화하는 데 'Big O' 표기법을 사용한며, 예를 들어 시간 복잡도가 $O(n^2)$ 인 문제는 입력 크기가 n배이면 해결에 필요한 시간이 n^2배 증가한다.

복잡도 종류(Complexity class)는 계산 복잡도에 따라서 문제를 분류한 것이다. 대표적인 고전 컴퓨터의 복잡도 클래스는 다항 시간 안에 풀 수 있는 P 문제, 확률적 다항 시간 내에 해결할 수 있는 BPP문제, 다항 시간 안에 정답을 확인할 수 있지만 정답을 찾기는 어려운 NP문제 등이 있다. 메모리 공간에 따른 분류도 존재하며, 예를 들어 PSPACE는 다항 공간 안에 해결 가능한 문제, EXPSPACE는 지수 공간을 요구하는 문제를 나타낸다.

양자 컴퓨터에서는 양자컴퓨터가 확률적 다항 시간 내에 풀 수 있는 BQP문제가 있으며 NP와 유사한 QMA 문제 등이 있다. 그러나 일부 양자 클래스가 고전 클래스보다 강력한지 여부가 명확하지 않다. 예를 들어, BQP와 NP, P의 관계는 아직 확립되지 않아 양자 컴퓨터의 효율성에 대한 연구가 진행중이다.

22. 양자우월성

양자이득(Quantum advantage)은 특정 문제에서 양자 컴퓨터가 고전 컴퓨터보다 효율적으로 문제를 해결할 수 있는 능력을 의미하며, 양자 우월성(Quantum supremacy)은 양자 컴퓨터가 고전 컴퓨터로는 사실상 풀기 어려운 문제를 실질적으로 해결하는 경우를 가리킨다. 양자우월성을 주장하려면 문제가 명확히 정의되어야 하고, 이를 해결하는 알고리즘이 존재하며, 고전 컴퓨터로 해결할 수 있지만 계산 복잡도가 높은 문제가 있어야 한다. 또한, 실험적으로 양자 알고리즘이 고전 알고리즘보다 더 효율적임을 입증해야 한다.

현재 양자우월성의 대표적인 후보로는 소인수 분해를 수행하는 쇼어 소인수 분해 알고리즘이 있다. 고전 알고리즘은 기하급수적인 시간이 걸리지만, 양자컴퓨터로 쇼어 알고리즘을 활용하면 다항 시간에 할 수 있다. 다만, 쇼어 알고리즘을 큰 수에 대해 실행하려면 오류보정이 가능한 양자컴퓨터와 많은 큐비트가 필요해, 이를 통한 양자 우월성의 검증은 아직 요원하다.

NISQ시대에서는 오류보정 없이도 특정 문제에서 고전 컴퓨터보다 양자 컴퓨터가 우수한 성능을 보이는 양자 이득에 더 주목하고 있다. 제한된 조건에서라도 양자 컴퓨터를 유용하게 활용할 수 있는 방법에 대한 연구가 활발히 진행 중이다.

23. 도이치-조사 알고리즘

도이치-조사 (Deutsch-Jozsa) 알고리즘은 양자 병렬성을 활용해 고전 알고리즘보다 빠르게 문제를 해결할 수 있는 양자 알고리즘이다. 이 알고리즘은 단 한 번의 계산으로 주어진 함수가 상수 함수인지 균형 함수인지를 판별할 수 있다.

함수 f(x)는 1비트의 입력을 받아 1비트의 출력을 생성한다. f(x)는 출력이 항상 0이거나 1인 상수 함수일 수도 있고, 절반의 입력에서 1을 출력하고 나머지 절반에서 0을 출력하는 균형 함수일 수도 있다. 고전적으로는 최소한 2번 이상 f(x)를 호출해야 이 문제를 해결하 수 있지만, 도이치-조사 알고리즘은 한번의 호출만으로 이를 해결할 수 있다.

도이치-조사 알고리즘은 입력 큐비트와 출력 큐비트를 사용하며 과정은 다음과 같다. 우선 Hadamard 게이트로 모든 가능한 입력들의 중첩상태를 생성한다. 그 다음 오라클(oracle)을 통해 모든 입력들에 대해 f(x)를 연산한 후, 출력 큐비트를 통하여 f(x)가 상수함수인지 균형함수인지 판별한다.

이 알고리즘은 실용적인 문제를 해결하는 데 사용되지는 않지만, 양자 컴퓨터의 유용성과 양자 병렬성의 잠재력을 보여주는 중요한 예이다.

24. 양자 푸리에 변환 알고리즘

양자 푸리에 변환 (Quantum Fourier transform) 알고리즘은 양자 상태에 대해 푸리에 변환을 수행하는 알고리즘이다. 고전적인 이산 푸리에 변환 (Discrete Fourier transform)의 양자 버전으로 이해할 수 있다. 고전 알고리즘 중 가장 효율적으로 알려진 FFT(Fast Fourier transform) 알고리즘을 사용해도 $O(N \log N)$의 시간 복잡도를 요구한다. 반면, 양자 푸리에 변환 알고리즘은 양자 중첩을 활용하여 주어진 양자 상태를 주파수 성분으로 분해하며 $O(\log^2 N)$의 시간 복잡도를 가진다. 즉 $N=2^n$개의 진폭에 대해서 푸리에 변환을 할 때 양자컴퓨터는 고전 컴퓨터에 비해 지수적인 속도 향상을 제공한다.

양자 푸리에 변환 알고리즘은 쇼어 소인수 분해 알고리즘, 양자위상추정 알고리즘 등 다양한 양자 알고리즘에 활용되며 양자 우월성을 제공하는 핵심적인 역할을 한다.

25. 양자위상추정 알고리즘

양자위상추정 (Quantum phase estimation) 알고리즘은 주어진 양자 연산자 U의 고유값($e^{2\pi i\theta}$)을 효율적으로 추정하는 방법이다. 이 고유값은 양자 시스템의 상태를 분석하거나 양자 상태의 동역학을 이해하는 데 활용될 수 있다.

양자위상추정 알고리즘은 다음의 과정을 거친다. 두개의 양자 레지스터들을 준비한다. 첫 번째 레지스터는 측정용 큐비트로 구성되며, 두 번째 레지스터는 입력 큐비트를 위한 것이다. 첫 번째 레지스터의 큐비트들을 중첩 상태로 만들고 후 입력 큐비트에 고유값을 알고자 하는 유니타리 연산자 U에 대한 제어 게이트를 적절하게 반복 적용하여, 위상 정보를 첫 번째 레지스터에 저장한다. 그 다음, 첫 번째 레지스터에 양자 푸리에 변환을 적용하고, 측정하면 위상 θ의 근사값이 출력된다. 이 근사값의 정밀도는 첫 번째 레지스터의 큐비트 수에 따라 결정된다.

양자 위상 추정 알고리즘은 양자 화학, 양자 최적화, 양자 기계 학습 등 다양한 분야에서 유용하게 사용된다. 특히, 복잡한 양자 시스템의 에너지 준위 계산이나 고유 상태 분석에 큰 도움이 된다. 또한 양자 컴퓨팅의 핵심적인 알고리즘 중 하나로, 다른 많은 양자 알고리즘의 기초가 된다.

26. 쇼어 소인수 분해 알고리즘

쇼어 소인수 분해 알고리즘(Shor's factorization algorithm)은 양자 컴퓨터의 강력한 계산 능력을 활용하여 소인수 분해 문제를 효율적으로 해결하는 양자 알고리즘이다. 고전 컴퓨터에서는 소인수 분해가 지수적 시간 복잡도를 가지는 어려운 문제로 알려져 있지만, 쇼어 알고리즘을 사용하면 이 문제를 다항 시간 내에 해결할 수 있다.

이 알고리즘은 먼저 주어진 수 N의 소인수 찾기 문제를 주기성 찾기 문제로 변환한다. 이후 양자 푸리에 변환을 적용하여 해당 주기를 빠르게 발견하고, 이를 통해 N의 인수를 계산한다. 양자 푸리에 변환의 효율성 덕분에 고전적인 방법보다 훨씬 빠른 연산이 가능하다.

RSA와 같은 현대의 공개키 암호 시스템은 큰 정수의 소인수 분해가 짧은 시간 내에 불가능하다는 것을 기반으로 하고 있다. 따라서 쇼어 알고리즘은 현대 암호체계를 무력화할 잠재력을 가지고 있다. 이로 인해 양자 컴퓨터의 발전에 대비하기 위한 양자 내성 암호 (post-quantum cryptography) 연구가 활발히 이루어지고 있다.

27. 그로버 검색 알고리즘

그로버 검색 알고리즘(Grover's search algorithm)은 쇼어 알고리즘과 함께 양자 우월성을 입증할 수 있는 대표적인 양자 알고리즘이다. 이 알고리즘은 정렬되지 않은 데이터베이스에서 특정 항목을 효율적으로 검색하는 방법을 제공한다.

그로버 검색 알고리즘은 초기 단계에서 모든 가능한 양자 상태를 중첩시키고, 이 상태들을 간섭시켜 특정 상태(정답)의 확률을 증폭한다. 이러한 병렬 연산 과정 덕분에 고전적인 알고리즘보다 훨씬 더 빠르게 답을 찾을 수 있다. 고전적인 검색 알고리즘은 평균적으로 O(N)의 시간 복잡도를 가지지만, 그로버 알고리즘은 O(√N)의 시간 복잡도로 문제를 해결할 수 있다.

이 알고리즘은 데이터베이스 검색뿐만 아니라 최적화 문제 등 다양한 문제에도 적용될 수 있다. 비록 고전적인 검색 알고리즘에 비해 지수적으로 빠른 속도를 제공하지는 않지만, 제곱근 속도 향상은 여전히 큰 의미를 가진다.

28. 양자 시뮬레이션

양자 시뮬레이션(quantum simulation)은 양자 시스템의 동역학을 모방하고 물리적 성질을 예측하는 응용 분야이다. 양자 시스템은 차원이 기하급수적으로 증가하여 고전컴퓨터로 시뮬레이션 하는 것이 사실상 불가능하지만, 양자 시스템을 사용하면 특정 양자 시스템을 효과적으로 모방하고 그 동작을 효율적으로 시뮬레이션할 수 있다.

양자 시뮬레이션은 실험적으로 제어 가능한 물리적 시스템을 이용하여 특정 모델의 양자 특성을 분석하는 데 중점을 둔다. 이를 통해 양자 시스템의 동역학, 상관관계 및 다양한 물리적 특성을 모사함으로써 물질의 성질, 화학 반응, 고체 물리학, 분자 구조 등 다양한 분야의 문제를 해결하는 데 기여할 수 있다.

양자 시뮬레이션은 크게 두 가지 접근 방식으로 나뉜다. 아날로그 양자 시뮬레이터는 시뮬레이터의 해밀토니안을 관심 있는 물리 시스템의 해밀토니안과 일치시켜 문제를 해결하는 접근이다. 디지털 양자 시뮬레이터는 양자 회로를 사용해 주어진 양자 시스템을 높은 정확도로 모사하려는 방식이다. 이 방식은 특정 양자 시스템의 모방을 목적으로 한다는 점에서 보편적인 계산을 수행하려는 양자 컴퓨터 알고리즘과는 다르다.

29. 양자 머신러닝

양자 머신러닝(Quantum machine learning)은 양자컴퓨터의 계산 능력을 활용하여 기계 학습 알고리즘의 성능을 향상시키려는 연구 분야이다. 학습 프로세스에서 양자컴퓨터가 제공할 수 있는 이점을 탐구하며, 특히 양자 기술이 머신러닝에 필요한 계산 자원 및 학습 속도를 얼마나 개선할 수 있는지를 중요한 주제로 다룬다. 고전 컴퓨터에서 GPU가 병렬 처리를 통해 딥러닝을 가속화한 것처럼, 양자 컴퓨터의 중첩과 얽힘이라는 독특한 특성이 머신러닝 성능을 향상시킬 것으로 기대되고 있다.

양자 컴퓨터는 양자 게이트를 매개변수화하여 뉴럴 네트워크와 유사한 방식으로 훈련할 수 있으며, 이를 통해 고전 데이터를 학습할 뿐만 아니라 양자 상태 데이터를 학습하는데 활용될 수 있다. 또한, 연구 영역은 양자 화학, 양자 최적화 등 여러 분야로 확장되고 있으며, 양자 오토인코더, 양자 서포트 벡터 머신, 양자 컨볼루션 신경망 등 새로운 양자 머신러닝 기법들이 활발히 개발되고 있다.

30. 디빈센초 기준

디빈센초 기준(DiVincenzo's criteria)은 실용적인 양자컴퓨터 구현을 위해 필요한 다섯 가지 조건으로, 양자 시스템이 양자컴퓨터로 활용될 수 있는지 판단하는 기준을 제공한다. 디빈센초 조건의 요소는 다음과 같다.

1. 큐비트의 잘 정의된 상태: 큐비트는 |0>과 |1>의 중첩 상태를 표현할 수 있어야 하며, |0>과 |1> 두 상태는 명확히 구분되어야 한다.

2. 큐비트 초기화: 큐비트를 |0> 상태로 초기화할 수 있어야 한다.

3. 긴 결맞음 시간: 큐비트의 결맞음 시간이 충분히 길어서 양자 연산 중 오류가 충분히 작아야 한다.

4. 범용적인 양자 게이트 구현: 1-큐비트 및 2-큐비트 게이트를 구현할 수 있어야 하며, 이를 조합하여 임의의 양자연산을 효율적으로 수행할 수 있어야 한다.

5. 큐비트 상태의 측정: 큐비트 상태를 측정할 때, 상태 변화의 방해 없이 정확한 측정이 가능해야 한다.

현재 활발히 연구되고 있는 초전도, 고체 점결함, 이온트랩, 중성원자 등의 양자컴퓨팅 시스템은 이러한 조건을 만족하며, 이 조건은 양자 컴퓨팅 플랫폼을 비교하고 평가하는 데 중요한 역할을 한다.

31. 초전도 양자컴퓨터

초전도 양자컴퓨터는 초전도 물질로 만든 전자회로의 양자 상태를 큐비트로 활용하는 방식이다. 초전도 회로는 일반적인 축전기와 인덕터뿐만 아니라 조셉슨 접합(Josephson junction)을 회로 요소로 사용한다. 초전도체에서는 쿠퍼 쌍(Cooper pair)이 전하를 운반하는데, 두 초전도체 사이에 얇은 절연층이나 반도체를 끼워 만든 조셉슨 접합에서는 쿠퍼 쌍이 터널링을 통해 이동한다. 이 과정에서 조셉슨 접합은 비선형적인 인덕터가 되고, 이를 활용한 비조화 진동자를 설계함으로써 큐비트를 구현할 수 있다..

초전도 큐비트는 회로 구성 방식에 따라 여러 유형으로 나뉜다. 대표적으로 전하 (Charge) 큐비트, 위상 (Phase) 큐비트, 자속 (Flux) 큐비트가 있으며, 트랜스몬 (Transmon) 큐비트와 플럭소니움 (Fluxonium) 큐비트 같이 기존 큐비트의 안정성을 개선한 형태도 널리 활용되고 있다. 마이크로파를 이용한 빠른 제어와 상태 측정이 가능하며, 기존 반도체 공정 기술을 활용하여 양산에 강점이 있다.

하지만 초전도 양자컴퓨터 구동을 위해서는 극저온 환경이 필수적이며, 큐비트 수가 늘어날수록 냉각 시스템의 공간 및 냉각 용량 한계로 인해 확장에 어려움이 따른다. 최근에는 극저온에서 양자 상태를 제어하고 측정하여 발열을 줄이고, 초전도 양자 프로세서를 안정적으로 연결하여 확장성을 높이는 연구가 주목받고 있다.

32. 고체 점결함 양자컴퓨터

고체 점결함 양자컴퓨터는 고체 내 특정 결함 구조를 이용해 큐비트를 구현하는 방식이다. 고체 내에서 특정 원자가 빠지거나 다른 원자로 대체되는 결함을 점결함이라 하며, 이 점결함의 전자 스핀 상태를 큐비트로 사용한다.

대표적인 예로 다이아몬드 질소-빈자리(NV, Nitrogen Vacancy) 구조가 있으며, 이는 다이아몬드에서 탄소 원자 자리에 질소와 빈자리가 위치한 결함이다. 다이아몬드 NV 센터는 중성(NV^0) 및 음성(NV^-) 상태를 가질 수 있는데, 음성 상태에서 바닥 상태가 스핀 삼중항(triplet) 구조로 되어 있어, 자기장을 가해 스핀 큐비트의 에너지 갭을 조절할 수 있다. 이러한 큐비트는 레이저 광펌핑을 통해 상태 초기화가 가능하고, 마이크로파로 상태를 제어하며, 발광을 통해 측정할 수 있다. 다이아몬드 내에는 여러 NV 센터가 존재할 수 있으며, 불균일한 자기장을 가해 각 NV 센터의 에너지 갭을 구분되게 할 수 있다. 또한, 주변의 탄소 동위원소 핵스핀을 활용해 다중 큐비트 시스템으로 확장할 수 있다.

고체 점결함을 이용한 큐비트는 NV 센터 외에도 다이아몬드 내 실리콘-빈자리(Silicon Vacancy), 실리콘 카바이드(Silicon Carbide) 내 실리콘-빈자리 및 탄소-빈자리 등 다양한 형태로 존재하며, 다른 결정에서도 큐비트를 만드는 연구가 활발히 진행 중이다.

33. 이온트랩 양자컴퓨터

이온트랩 (Ion trap) 양자컴퓨터는 이온의 에너지 상태를 큐비트로 활용하는 방식으로, 주로 양전하를 띤 원자를 전자기장을 사용해 위치를 고정한다. 이온 포획에는 2차원 평면에 고정하는 페닝 트랩(Penning trap)이나 3차원 공간에서 안정적으로 가두는 폴 트랩(Paul trap)이 사용된다. 트랩된 이온은 레이저 펄스나 마이크로파를 통해 제어되며, 이를 통해 개별 이온의 양자 상태를 정확하게 제어하고 측정할 수 있다.

이온의 양자 상태는 광학적으로 제어 및 측정이 용이하며, 외부 환경의 잡음에 강해 비교적 긴 시간 동안 양자 상태를 유지할 수 있어 양자 게이트의 충실도(fidelity)가 높다. 또한, 이온 간의 여러 진동 모드를 활용하여 멀리 떨어진 큐비트 간에도 상호작용을 구현할 수 있어 높은 큐비트 연결성을 제공한다. 다만, 큐비트 수가 증가할수록 이온을 안정적으로 포획하는 데 한계가 있어 대규모 시스템 구현에는 어려움이 따른다. 이를 해결하기 위해 셔틀링(shuttling) 기술이 활발히 연구되고 있으며, 이는 여러 이온트랩 프로세서 사이에서 이온을 이동시키는 방식으로 확장성을 높이는 방법으로 주목받고 있다.

34. 리드버그원자 양자컴퓨터

리드버그원자 (Rydberg atom) 양자컴퓨터는 중성원자의 리드버그 상태를 활용하여 큐비트를 구현하는 기술이다. 리드버그 상태의 원자는 전자가 높은 주양자수로 들떠 있어 매우 큰 원자 궤도를 형성하는데, 주양자수가 100일 경우 원자의 크기가 수 마이크로미터에 이를 수 있다. 이처럼 큰 궤도로 인해 리드버그 원자는 상호작용 거리가 길고, 전자기장이나 주변 원자들과의 상호작용에 민감하다.

리드버그 원자에서는 기저 상태를 0, 리드버그 상태를 1로 설정하여 큐비트를 정의하고, 레이저 펄스로 상태 변환을 유도할 수 있다. 두 원자가 가까이 있을 때, 하나의 원자가 리드버그 상태로 여기되면 인접한 원자들이 여기되는 것을 막는 리드버그 봉쇄 (Rydberg blockade) 현상이 발생한다. 이러한 봉쇄 효과를 통해 원자들 간 강력한 상호작용이 가능해져 다중 큐비트 게이트 구현이 가능해진다.

리드버그 원자 양자컴퓨터는 레이저 기술을 활용하여 큐비트 준비 및 제어가 용이하다는 점에서 많은 주목을 받고 있다. 특히 2023년 하버드 대학의 Lukin 교수 연구팀이 최대 60개의 리드버그 원자 간 병렬 얽힘 게이트 구현에 성공하여 이 플랫폼의 확장성과 신뢰성에서 중요한 돌파구를 제시하면서 큰 기대를 모으고 있다.

35. 광자 양자컴퓨터

광자 양자컴퓨터는 광자의 다양한 자유도를 이용해 양자 정보를 저장하고 처리하는 방식의 양자컴퓨팅이다. 대표적으로 광자의 수직 및 수평 편광 상태 또는 원형 편광 상태를 이용한 편광 큐비트, 광자의 시간 차이를 이용한 시간 빈 큐비트, 광자의 경로 모드를 이용한 경로 큐비트 등 다양한 종류의 큐비트들이 있다.

광자는 원천적으로 환경과 잘 상호작용하지 않아 결어긋남에 강하며, 먼 거리 전송이 용이하다는 특징이 있어 양자 컴퓨팅과 양자 통신 분야에서 활발히 연구되고 있다. 또한, 선형 광학 시스템을 이용하여 단일 큐비트 게이트를 쉽게 구현할 수 있다는 강점이 있다.

광자 양자컴퓨터는 단일 광자 광원 또는 양자 얽힘 광원으로 큐비트를 준비하고, 광자 검출기를 이용해 측정하며, 광학 기구들을 사용해 회로를 구성한다. 주요 광학 기구로는 빔 분할기(beam splitter), 위상 변조기(phase shifter), 그리고 비선형 매질(nonlinear medium)이 있다. 특히 비선형 매질을 사용하면 광자 간 상호작용을 만들어낼 수 있다. 하지만 광자 간의 상호작용이 약하기 때문에, 2-큐비트 게이트를 만드는 것이 어렵다. 그 대안으로 작은 수의 광자가 얽혀 있는 양자상태를 퓨전 (fusion) 작용으로 엮어 많은 수의 광자가 얽혀 있는 클러스터 양자 얽힘 상태를 준비하고, 측정을 통해 양자 연산을 수행하는 측정 기반 양자컴퓨팅 구현에 집중하고 있다.

36. 반도체 양자컴퓨터

반도체 양자컴퓨터는 양자점(Quantum dot)을 기반으로 하는 양자 컴퓨팅 기술로, 양자점은 반도체 물질 내에 형성된 매우 작은 나노구조이다. 이 구조는 전자 또는 양공(hole)을 가두어 두는 공간으로 작용하며, 양자점 내부의 전자나 양공은 인공 원자처럼 동작하고 불연속적인 에너지 준위를 갖는다.

양자점은 일반적으로 반도체 이종접합(heterostructure)을 통해 생성된다. 이종접합 계면에서는 2차원 전자 가스(2DEG)가 형성되고, 그 위에 금속 전극을 통해 게이트를 설정하여 전위를 가함으로써 전자를 가둘 수 있는 3차원 반도체 양자점이 만들어진다. 이러한 방식으로 다양한 이종접합 소재들이 연구되고 있으며, 대표적인 예로는 28Si/SiGe, Ge/SiGe, GaAs/AlGaAs 등이 있다.

반도체 양자점 구조를 활용하면 여러 가지 유형의 큐비트를 설계할 수 있습니다. 전자의 스핀을 기반으로 하는 스핀 큐비트(spin qubit), 전하의 존재 여부를 활용한 전하 큐비트(charge qubit), 그리고 스핀 큐비트와 전하 큐비트의 특성을 결합한 하이브리드 큐비트(hybrid qubit)가 그 예이다. 이러한 반도체 양자점 큐비트는 기존 반도체 기술과의 호환성이 뛰어나며, 양자컴퓨팅 기술의 실용화를 위한 중요한 연구 분야로 부상하고 있다. 반도체 기술의 지속적인 발전은 이들 큐비트의 응용 가능성을 더욱 확장할 것으로 기대된다.

37. NMR 양자컴퓨터

NMR(Nuclear Magnetic Resonance, 핵자기 공명)을 이용한 양자컴퓨터는 분자 내 원자핵의 스핀 상태를 큐비트로 사용하는 방식이다. 핵자기 공명은 외부 자기장 속에서 원자핵의 스핀을 조절하는 기술로, 특정 주파수의 자기장을 가하면 원자핵의 에너지 준위가 변화하며 스핀 상태가 변한다. 이러한 스핀 상태를 큐비트로 사용할 수 있다.

NMR 양자컴퓨터에서는 분자 내 여러 원자핵의 핵스핀이 여러 개의 큐비트로 정의되며, 외부 자기장과 핵스핀 간의 상호작용을 통해 단일 및 다중 큐비트 게이트를 구현할 수 있다. 또한, 라디오파 펄스를 이용해 큐비트 간의 상호작용을 제어하거나 스핀 상태를 측정할 수 있다.

초기 양자컴퓨터 연구에서 NMR 방식이 많이 연구되었지만, 확장성 및 오류 보정의 한계로 인해 개발에 어려움을 겪고 있다.

38. 위상양자컴퓨터

위상양자컴퓨터(Topological Quantum Computer)는 1997년 Alexei Kitaev가 제안한 개념으로, 2차원 공간의 비-아벨리안 애니온(Non-abelian anyon)을 활용하여 양자 정보를 저장하고 처리한다. 비-아벨리안 애니온은 고유한 특성으로 인해 두 입자를 교환할 때마다 유니터리 연산을 생성하는데, 이 교환 과정은 "꼬임(braiding)"이라 불리며 양자 게이트 구현의 핵심 원리로 사용된다.

위상양자컴퓨터는 양자 정보를 위상적 상태에 저장해, 꼬임 경로에 무관하게 양자게이트 구현되어 정보가 안정적으로 보호되는 특징이 있다. 이는 환경적 노이즈나 결어긋남 오류에 상대적으로 강해, 오류 내성을 갖춘 안정적인 양자 컴퓨터 구현의 강력한 후보로 꼽힌다.

현재 비-아벨리안 준입자인 마요라나(Majorana) 페르미온을 실험적으로 관측하고, 이를 활용해 위상적 꼬임을 시연하려는 연구가 활발히 진행되고 있다. 다른 플랫폼에 비해 상대적으로 발전이 더디지만 오류 저감과 안정성 측면에서 강점을 가져 결함 허용 양자 컴퓨터 구현의 유망한 후보 중 하나로 자리 잡고 있다.

39. 양자컴퓨터 산업계

양자컴퓨터 산업은 하드웨어와 소프트웨어 양 측면에서 활발한 발전을 이루고 있다. 하드웨어 분야에서는 양자 프로세서 개발이 중요하다. 대표적으로 IBM Quantum, Google Quantum AI, IQM은 초전도 기반, D-WAVE는 초전도 양자 어닐링, IonQ와 Quantinuum은 이온트랩 기반, QuEra와 Pasqal은 중성원자 기반, PsiQuantum과 Xanadu는 광자 기반 프로세서를 개발하고 있다. QuantWare와 Rigetti 같은 기업들은 양자 프로세서 설계와 파운드리 서비스를 제공하여 양자 컴퓨팅 생태계 확장에 기여하고 있다.

양자컴퓨터 구현에는 극저온 환경과 정밀 광학·레이저 기술이 필수적이므로, 소재·부품·장비 기업들도 중요한 역할을 맡고 있다. Bluefors, Oxford Instruments, Montana Instruments는 극저온 장치를 제공하며, Toptica, NKT Photonics, Coherent 등은 고성능 광학 및 레이저 부품을 공급해 양자 컴퓨터의 안정성과 성능을 지원한다. 이 외에도 전자기적 차폐 장치, 정밀 제어 시스템, 전송 라인 부품을 공급하는 기업들이 있다.

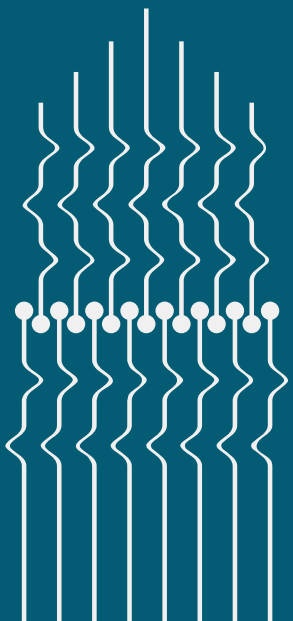
소프트웨어 분야에서는 양자 컴퓨터의 설계, 제어, 최적화 소프트웨어를 개발하는 기업들과 양자 컴퓨팅 활용에 집중하는 기업들이 있습니다. 활용 분야로는 분자 구조 계산, 신물질 개발, 금융모델 계산, 로지스틱스 최적화 등이 주목받고 있다.

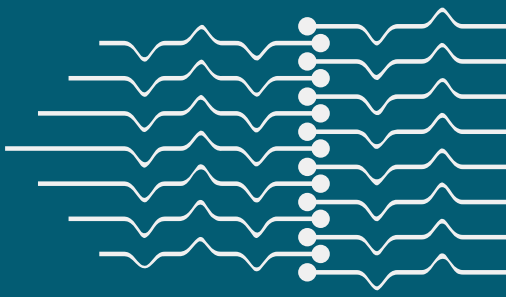
40. 클라우드 양자컴퓨팅

클라우드 양자컴퓨팅(Cloud Quantum Computing)은 사용자가 양자 컴퓨터를 직접 소유하거나 관리하지 않아도 인터넷을 통해 원격으로 양자 컴퓨터에 접속해 연산을 수행할 수 있는 서비스이다. 이를 통해 양자 컴퓨터가 없는 연구자, 기업, 개발자들도 노이즈가 있는 실제 양자 컴퓨터에서 자신들의 이론이나 프로토콜을 검증하고 양자 계산을 실험할 수 있다. 대표적으로 IBM Qiskit은 자체 클라우드 양자 컴퓨팅 서비스를 제공하며, IonQ, Quera, Rigetti 등 대부분의 양자컴퓨터 하드웨어 기업은 Microsoft Azure Quantum, Amazon Braket과 같은 클라우드 플랫폼을 통해 양자 컴퓨팅 서비스를 제공한다.

[부록]

양자정보기술 기초용어





양자정보기술 기초용어를 자율적으로 학습할 수 있는 공간입니다.
다양한 학습자료를 활용하여 각 용어의 개념을 익혀보시기 바랍니다.

*본문 내의 간단한 설명은 위키백과를 참조하여 작성하였습니다.

양자

더 이상 나눌 수 없는 에너지의 최소량의 단위.
물리학에서 상호작용과 관련된 모든 물리적 독립체의 최소단위.

양자역학

분자, 원자, 기본 입자(전자, 소립자 원자핵 등) 미시적인 계의 현상을 연구하는
물리계의 아주 작은 입자들을 연구하는 물리학의 한 분야

파동

공간 상에서 평형 상태로부터의 변화 혹은 진동이 전달되는 현상

입자

물리적 성질과 화학적 성질을 가진 작은 물체이다. 원자보다 작은 아원자 입자, 원자가 몇 개 단위로 구성된 미시적 크기의 미립자, 거시적 크기의 밀가루와 같은 입자 등으로 나뉨

중첩

**두 개(또는 그 이상)의 양자 상태가 함께 더해질 수 있으며,
결과는 또 다른 유효한 양자 상태가 되는 것**

얽힘

**두 개 이상의 입자가 서로 강하게 연결되어 있는 상태.
한 입자의 상태가 결정되는 순간 다른 입자의 상태도 즉시 결정되어 마치 정보가
순식간에 이동한 것처럼 보임**

슈뢰딩거의 고양이

1935년에 오스트리아의 물리학자 에르빈 슈뢰딩거가 '코펜하겐 해석'을 반박하기 위해 고안한 사고 실험

파동 입자 이중성

양자역학에서 모든 물질이 입자와 파동의 성질을 동시에 지니는 성질

파동 함수

물질을 구성하는 입자 또는 파동의 위치 상태를 확률적으로 표현한 함수.
다시 말해, 특정한 시간에 특정한 위치에서 입자를 발견할 확률적 크기.

불확정성 원리

두 개의 관측가능량(observable)을 동시에 측정할 때, 둘 사이의 정확도에는
물리적 한계가 있다는 원리

결맞음(Coherence)

파동이 간섭 현상을 보이게 하는 성질

확률분포

확률 변수가 특정한 값을 가질 확률을 나타내는 함수를 의미

큐피트

양자 컴퓨터는 정보를 0과 1의 상태를 동시에 갖는 큐비트 단위로 처리하고 저장

정보 엔트로피

정보이론에서 시스템은 송신자, 채널, 수신자를 이용하여 모형화하는데 이 맥락에서 정보 엔트로피(또는 섀넌 엔트로피)는 각 메시지에 포함된 정보의 기댓값(평균).

양자 회로

양자 정보 이론에서 고전 회로와 유사한 양자 계산을 위한 모델

양자 우위

양자 컴퓨터가 기존의 슈퍼 컴퓨터 성능을 능가하는 것을 말함

양자 알고리즘

양자 알고리즘이라는 용어는 일반적으로 양자 중첩 또는 양자 얽힘과 같은 양자 역학적 특징을 필수적으로 사용하는 알고리즘을 의미

기저

선형대수학에서, 어떤 벡터 공간의 기저(基底, 영어: basis)는 벡터 공간의 임의의 벡터에게 선형결합으로서 유일한 표현을 부여하는 벡터들

위상 큐피트

초전도-절연체-초전도(SIS) 조셉슨 접합을 기반으로 한 초전도 장치로, 양자 비트 또는 큐비트로 작동하도록 설계

스핀

스핀(spin)은 양자역학에서 입자의 운동과 무관한 고유 각운동량

광자

광자(光子, photon) 또는 빛알은 기본입자의 일종으로, 가시광선을 포함한 모든 전자기파를 구성하는 양자이자 전자기력의 매개입자

이중 슬릿 실험

양자역학에서 실험 대상이 파동인지 입자인지를 구분하는 실험

코펜하겐 해석

양자역학에 대한 다양한 해석 중의 하나로 논의의 중심이었던 코펜하겐의 지명으로부터 이름이 붙여진 것이며, 20세기 전반에 걸쳐 가장 영향력이 컸던 해석으로 꼽힘

집필진

분야	세부분야	역할	이름	소속	직책
통신		원고	임나희	KIST	박사과정
		원고	이승재	KIST	박사과정
		자문	한상욱	KIST	단장
		자문	염다현	아이디퀀티크	박사
센싱	양자 관성 센싱	원고	권택용	KRISS	그룹장
	양자 시간 · 주파수 센싱	원고	권택용	KRISS	그룹장
	양자 전기장 센싱	자문	김기웅	충북대학교	교수
	양자 자기장 센싱	원고	박성현	충북대학교	박사과정
		자문	오상원	아주대학교	교수
		원고	고의진	아주대학교	박사과정
	양자 광 센싱	원고	고영호	ETRI	박사
	양자 계측	원고	이창협	KRISS	박사
컴퓨팅		원고	진승원	고려대학교	석박사통합과정
		자문	김요셉	고려대학교	교수

양자정보기술 용어집

발행월 | 2025년 3월
발행인 | 황종성
발행처 | 한국지능정보원(NIA) 양자산업생태계지원센터(KQIC)
디자인 | 이현중
기획·편집 | KMA한국능률협회
ISBN | 978-89-8483-901-4

NIA 한국지능정보원
대구광역시 동구 첨단로 53
www.nia.or.kr

KQIC 양자산업생태계지원센터 Korea - Quantum Industry Center
경기 성남기 수정구 대왕판교로 815
판교제2테크노벨리 2층
www.kqic.kr

KMA
서울 영등포구 의사당대로 22
이룸센터 9-10층
www.kma.or.kr