tlomarketing

국가과학기술연구회 공동TLO마케팅사무국이란?

국가과학기술연구회 소관 25개 정부출연연구소(이하 출연(연))의 연구성과에 대한 공동 마케팅을 통해
기술이전과 출자 등 **기업의 기술사업화 지원을 위한 전문조직** 입니다.

공동 TLO 마케팅 사무국

공동TLO마케팅사무국을 통해 무엇을 도움 받을 수 있나요?

신규 사업 아이템 및 기술 업그레이드 등 기술 고민이 있는 예비창업자 및 기존 사업자에게 25개 출연(연)이 보유하고 있는
약 10만여 건의 특허 외에 연구자 노하우 및 연구 · 시험장비 등을 활용하여 **기업의 기술애로를 해결해드리고 있습니다.**

기업 애로해결 지원

· 기술도입 및 사업화 유망기술 발굴
· 기술창업용 출자기술 발굴
· 공동연구 대상 전문연구자 연계

정부과제 소개 지원

· 기술도입형 R&BD
과제 연계

연구장비 지원

· 분석 및 실험장비 연계

IP인수보증 자금 연계 지원

· 기술보증기금,
신용보증기금 등

nst
National Research Council of Science & Technology

국가과학기술연구회

과학기술분야 정부출연연구기관을 지원육성하고 체계적으로 관리함으로써 국가 연구사업 정책 지원 및
지식산업발전을 견인하고자 만든 과학기술정보통신부 산하 정부기관임

KIST 한국과학기술연구원 · 국가녹색기술연구소 NATIONAL INSTITUTE OF GREEN TECHNOLOGY · KBSI 한국기초과학지원연구원 · KASI 한국천문연구원 · 한국생명공학연구원 · KISTI 한국과학기술정보연구원 · 한국한의학연구원
KITECH 한국생산기술연구원 · ETRI 한국전자통신연구원 · NSR · KICT 한국건설기술연구원 · KRRI 한국철도기술연구원 · KRISS 한국표준과학연구원 · KFRI 한국식품연구원
세계김치연구소 · KIGAM 한국지질자원연구원 · KIMM 한국기계연구원 · KAIRI · KIER · KERI 한국전기연구원 · KRICT 한국화학연구원
KIT 안전성평가연구소 · KAERI 한국원자력연구원 · KIMS 한국재료연구원 · KFE 한국핵융합에너지연구원

문의처

국가과학기술연구회
T. 044-287-7369 E. gylee@nst.re.kr

공동TLO마케팅사무국
T. 042-862-6015 E. seungtae100@wips.co.kr

TLO Tech Trends 2024

국가과학기술연구회 공동 TLO 마케팅 사무국
Technology Licensing Organization

공동 TLO 마케팅 사무국

WIPS 윕스

공동 TLO 마케팅 사무국

WPS 윕스

Contents

01 양자과학기술의 세계

양자과학기술의 필요성

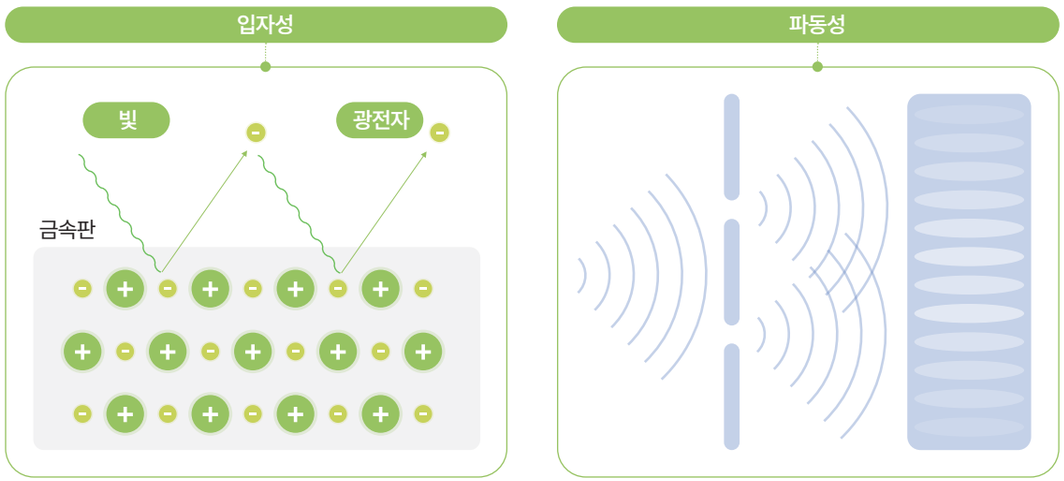
양자(Quantum)란 아주 작은 에너지 덩어리로, 동시에 두 가지 성질을 가지고 있다. 하나는 '입자'처럼 작고 분리된 모습이고, 또 하나는 '파동'처럼 퍼져나가는 모습으로 이것이 바로 양자의 독특한 점이다. 이러한 이유로 발생한 잘못된 오해 중 하나는 양자를 단순히 '작은 입자'로만 생각하는 것이지만, 실제로 양자는 입자와 파동의 특성을 동시에 가지고 있는 것이다.

양자역학은 이런 양자의 특성을 설명하는 학문으로 양자가 어떻게 움직이고 다른 물질과 어떻게 상호작용하는지를 연구한다. 양자역학은 눈에 보이지 않는 아주 작은 세계의 법칙을 다루기 때문에 어렵게 느껴질 수 있는데, 양자 세계의 법칙은 원자보다도 작은 100나노미터(nm) 이하의 단위에서 관측되는 운동 법칙을 따르기 때문이다.

양자과학기술(Quantum Science & Technology)은 양자의 '얽힘(Entanglement)'과 '중첩(Superposition)'같은 특성을 활용하여 혁신적인 기술로 컴퓨팅, 통신, 센서 등의 정보기술에 적용되고 있다. 이를 통해 기존 기술의 한계를 뛰어넘는 초고속 연산, 초신뢰 통신, 초정밀 계측을 가능하게 할 수 있을 것으로 보고 있다.

양자과학기술은 기존 기술로는 불가능하거나 이론적 한계에 도달한 기술을 구현할 수 있다. 특히 첨단 산업과 국방 영역에서 큰 영향력을 미칠 것으로 예상, 양자 컴퓨팅을 통해 기존 컴퓨터로는 불가능한 초고속 연산이 가능해지고, 양자 통신을 통해 완벽한 보안 통신이 실현되며, 양자 센서를 통해 100배 이상 정밀한 계측이 가능할 것이다.

양자의 이중성



출처 : 네이버 물리학백과, 한국물리학회

양자 용어 정리

양자의 이중성 Wave-particle duality

양자현상이 나타나는 미시 세계에서는 일반적으로 느끼는 물리 법칙과는 다르게 두 가지 성질을 동시에 가진 존재가 될 수 있다. 즉 입자의 성질과 파동의 성질을 함께 가지고 있는데, 측정 방법에 따라 그 성질이 결정된다.

양자의 불연속성 Quantum Discontinuity

아주 작은 미시 세계에서는 에너지가 불연속적이다. 만약 에너지가 물이라면, 강처럼 흐르는 것이 아니라 빗방울처럼 단절되어 있다.

불확정성 원리 Uncertainty Principle

입자의 위치와 운동량을 동시에 정확히 측정할 수 없다는 원리. 위치와 운동량을 동시에 정확하게 측정하는 것에 한계가 있다는 의미로, 위치를 정확히 측정하면 운동량은 상대적으로 덜 정확하게 측정될 수 밖에 없다. 그 반대의 경우도 마찬가지이다.

얽힘 Entanglement

한 쌍의 얽힌 양자는 멀리 떨어져 있어도 얽힌 상태를 유지하는데, 이 중 하나를 관측해 상태가 정해지면, 다른 하나의 상태도 정해진다. 두 입자가 아무리 멀리 떨어져 있더라도, 수백광년 떨어진 다른 은하에 있더라도 이 결정은 동시에 이루어진다.

중첩 Superposition

물리적인 상태가 한가지 상태로 결정된 것이 아니라 여러 가지 상태가 동시에 존재하는 현상. 양자는 관측되기 전까지는 상태를 알 수 없고, 확률적으로 모두가 존재하는 것이 가능하다. 디지털 정보는 2진법과 0과 1 가운데 한 상태만을 가졌지만, 양자는 0과 1이 동시에 존재할 수 있다.

복제 불가 No-cloning theorem

양자의 형태 뿐만 아니라 시간, 위치 등 모든 정보를 똑같이 복제·복사·증폭할 수 없다는 원리. 불확정성 원리에 의해 양자의 모든 정보를 정확하게 측정할 수 없고, 그렇기 때문에 복제가 불가능하다. 만약 양자 상태를 복사할 수 있으면 양자역학이 틀린 것이 되어 버린다.

큐비트 QUBIT, Quantum bit

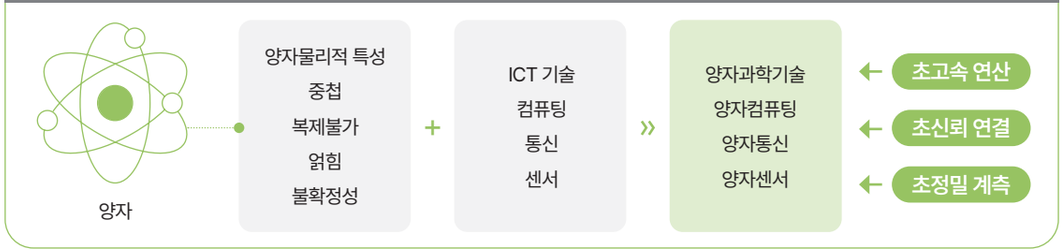
양자정보기술의 기본 정보 단위. 현재 사용되는 디지털컴퓨터에 비트가 있다면 양자컴퓨터에는 큐비트가 있다. 양자컴퓨터의 큐비트 수를 n개로 늘리면 한번에 처리할 수 있는 정보의 양이 2n(=2의 n제곱)개로 늘어난다.

양자 우위 Quantum Supremacy, 양자우월성

양자의 특성을 이용하여 기존 기술의 한계를 넘어서는 성능을 실현하는 것을 말한다. 양자컴퓨터의 경우, 양자 우월성의 기준은 현존하는 슈퍼컴퓨터의 능력이고, 양자센서는 기존 고감도 센서의 잡음 한계값이 기준이 될 것이다. 최근 양자컴퓨터의 개발에 박차를 가하면서 언론 등에서 양자컴퓨터의 연산 능력과 비용, 효율 면에서 의미있는 변곡점이라는 뜻을 사용하는 경우가 많다.

출처 : 네이버 물리학백과, 한국물리학회

양자 과학 기술 개념도



출처 : 대한민국 양자과학기술 비전, 과학기술정보통신부, 2023.6.27

양자과학기술 주요 정책 및 미래 전망

2008
- 국가양자정보 과학비전

2015
- 국가양자 기술전략

2016
- 양자정보과학 발전계획
- 양자성명서(Quantum Manifesto)
- 제13차 국가과학기술계획('16-'20)

2017
- 광 · 양자기술 새로운 전개 추진방안, Q-Leap 플래그십 프로그램
- 세계 최대 양자연구소 설립 발표
- Quantum Flagship 프로그램

2018
- 양자법(Quantum initiative Act)

2020
- 양자 인터넷전략, 국가안보 20대 유망기술 선정
- 양자혁신전략, Moonshot 프로젝트
- 양자과학기술 발전전략 강화

2021
- 독일 연방정부 양자컴퓨터 로드맵
- 양자기술 연구개발 투자전략('21.4.)

2022
- 양자 미래사회 비전
- 양자기술 프로그램 확대(600만 파운드)
- 양자기술 전략로드맵 수립('23 확정)

출처 : KISTEP Inl Vol.45「양자기술 전략로드맵,수립과 의의, KISTEP, 2023.7

	기존 기술	양자 기술
 양자컴퓨터 2035	1,024비트 암호해독에 100만년 전력 소모 30MW	**양자컴퓨터 2035** 1,024비트 암호해독에 100만 년 전력 소모 30MW **초고속 연산** 1,024비트 암호해독에 10시간전력 소모 0.05MW(/600)
 양자암호통신 2030	해저 광케이블 국제적 도감청 발생, NFC, 위성통신 등 무선통신 해킹 가능	**양자암호통신 2030** 해저 광케이블 국제적 도감청 발생, NFC, 위성통신 등무선통신 해킹 가능 **초신뢰 보안** 도감청시 파괴되는 양자암호 키 방식으로 불법 도감청 및 해킹 원천 차단
 양자센서 2025	MRI로 5mm이하 암세포 식별 라이다로 100m 내외 탐지,투과 불가능, 스텔스 탐지 불가능	**양자 센서 2025** MRI로 5mm 이하 암세포 식별 라이다로 100m 내외 탐지, 투과 불가능, 스텔스기 탐지 불가능 **초정밀 계측** 양자 MRI로 0,05mm 이하 암세포 식별 양자 이미징 센서로 45km 이상 탐지, 스텔스기 탐지

출처 : 양자기술 연구개발 투자전략, 과기부, 2021.4.30

양자과학의 발전 전략

구분	현재	1단계 '23 ~ '27 양자센서 · 양자암호 통신 산업화 촉진	2단계 '28 ~ '31 양자컴퓨팅 시스템 및 서비스 국산화	3단계 '32 ~ '35 글로벌 양자 일류 국가 도약
핵심인력(누적)	384명	700명	1400명	2500명
양자컴퓨팅	10 큐비트급 양자 컴퓨터	50큐비트급 양자컴퓨터 구축 및 클라우드 서비스 개시	1,000큐비트급 양자컴퓨터 구축 및 클라우드 서비스 개시(오료율 0.5%이하)	양자컴퓨터 상용화
양자통신	양자암호 통신 상용화 진입	양자네트워크 요소기술 개발 (양자전송, 양자메모리 원천기술)	도시 간 양자 네트워크 초기 실증 (양자 메모리 기반 양자 중계기 시작품)	전국망 기반 양자 인터넷 시범 구축
양자센서	양자센서 원천기술	이차전지 등 첨단산업 활용 양자센서 상용화	국방/의료/반도체 활용 세계 최고 수준 양자 센서 융복합 시스템 (시작품) 개발	양자센서로 양자산업 기반 마련
인프라	 양자팹(단일) 운영	 공공 개방형* 양자팹 확층 공정인력 집중 양성 (*연구자 직접 사용)	 공공 전문생산 양자팹(파운드리) 구축 · 운영	 민간 전문 생산 양자팹 (파운드리) 확산
목표		국내 양자 분야 기술 수준을 최선도국 대비 70%로 향상 산업화 초기 단계로 원천기술개발	국내 양자 분야 기술 수준을 최선도국 대비 80%로 향상, 양자과학기술 공급망 보호를 위한 양자 시스템 구성 소부장 산업화	국내 양자 분야 기술 수준을 최선도국 대비 85%로 향상, 양자 기기 간 연계를 실증하여 양자과학기술의 파괴적 혁신 견인

양자기기 (양자컴퓨팅-통신-센서 간) 연계 실증

출처 : 대한민국 양자과학기술 비전, 과학기술정보통신부, 2023.6.27

02 양자 기술의 혁신

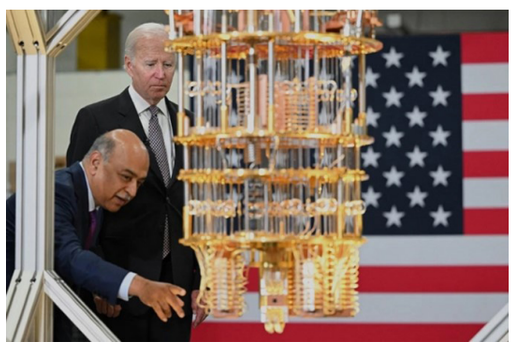
양자컴퓨터의 새로운 이정표 (IBM)

2019년 세계 최초로 선보인 범용 양자 컴퓨터인 '퀀텀 시스템 원(System One)'은 지금도 가동하고 있으며, 클라우드로 접속할 수 있다. IBM社는 2020년에 양자 로드맵을 발표하며 첨단양자 시스템을 구축하기 위한 양자 HW·SW 기술 전반을 확장 계획을 보여주었다. 이후 2023년 양자 개발 로드맵을 2033년까지로 연장하며 향상된 게이트 운영을 통해 양자 컴퓨팅의 품질을 크게 향상시킨다는 목표를 세웠다. IBM社는 양자 개발 로드맵에 따라 여러가지 연구 개발을 수행 하였는데, 우선 1,121개의 초전도 큐비트를 가진 새로운 프로세서 퀀텀 콘도르(Condor)를 공개했다. Condor는 큐비트 밀도를 50% 증가시키고, 큐비트 제작과 적층 크기의 혁신을 통해 대규모 양자 컴퓨팅 가능성을 확장하여 향후 양자 컴퓨팅 하드웨어 설계에 중요한 이정표가 될 것으로 보고있다. 양자 프로세서인 퀀텀 헤론(Heron)은 133개의 고정 주파수 큐비트를 갖추고 있으며, 이전 모델인 Eagle에 비해 3-5배 향상된 성능과 교차 간섭이 거의 없게 되었다. 게다가 IBM의 뉴욕 연구소에서 운영 중인 IBM Quantum System Two는 확장 가능한 양자 계산을 위한 플랫폼을 개발, 이 플랫폼은 세 개의 Heron 프로세서를 포함하여 병렬 회로 실행과 고성능 양자-고전 연산을 지원하는데, 이는 양자-중심 슈퍼컴퓨팅을 실현하기 위한 중요한 인프라로 보고 있다.

2024년, Qiskit 1.0 소프트웨어가 출시되어 회로 구성, 컴파일 시간, 메모리 사용량을 크게 개선하여 더 빠르고 효율적인 양자 컴퓨팅이 가능해졌다. 특히 AI를 활용한 양자 회로 컴파일 서비스로 더욱 혁신적으로 다가온다. AI 플랫폼 Watsonx을 통해 양자 코드 자동 생성 기능을 통해 더 쉽게 만들고 있다. AI를 활용한 이 플랫폼은 양자 컴퓨팅의 가능성을 더욱 확장할 것으로 기대하고 있다.

또한 병렬 회로 실행과 고전적 연산을 결합한 양자-중심 슈퍼컴퓨팅 비전을 제시하며 양자 컴퓨팅의 잠재력을 최대한 활용하여 더 빠르고 복잡한 문제를 해결하고자 한다. 마지막으로 양자 기술의 발전에 맞춘 Quantum Safe 프로그램이라는 새로운 양자 암호화 기술을 개발하여, 보안분야까지 강화하고 있다.

IBM CEO가 조 바이든 미국 대통령에게 양자컴퓨터를 소개하는 모습



출처 : 네이처(Nature)

상용 양자 컴퓨팅 혁신, 양자 어닐링 (D-Wave Systems)

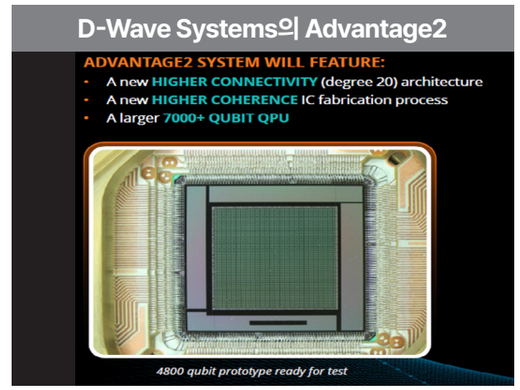
D-Wave Systems社는 양자컴퓨팅을 주사업으로 하고 있는 캐나다의 하드웨어 기업으로, 양자 어닐링 기술을 통해 양자 컴퓨팅의 상용화를 선도하고 있다. D-Wave는 세계 최초의 상용 양자 컴퓨터를 출시하였으며, 양자 컴퓨팅를 활용한 실제 문제를 해결하는 사례를 만들고 있다.

D-Wave Systems의 핵심 기술인 양자 어닐링은 조합 최적화 문제해결 방식으로 문제의 최적 해를 찾기 위해 가능한 많은 해를 동시에 탐색한다. 2023년도에는 5000개 이상의 큐비트가 설계된 Advantage 양자 프로세서를 출시하였는데, 더 복잡한 문제를 해결할 수 있는 능력을 갖추고 있으며 양자 컴퓨팅의 가능성을 넓히고 있다.

양자 컴퓨팅을 실제 상용화 하고 있는 D-Wave Systems은 다양한 산업 분야에서 새로운 혁신을 보여주고자 한다. 대표적으로 최근 이탈리아 트렌토 대학에서 대규모 숫자의 소인수 분해를 가능하게 한 연구는 과학 저널 'Scientific Reports'에 게재되었다. 이는 암호화 알고리즘보안과 밀접하게 관련되어 있어, 숫자가 커질수록 암호화 시스템의 안정성을 보장하는 요소로 활용될 수 있다.

기존 제품인 Advantage의 후속 제품으로 Advatage2를 개발하고 있으며, 이는 7000개 이상의 큐비트를 포함하여 2025년 출시 예정에 있다.

D-Wave Systems의 Advantage2



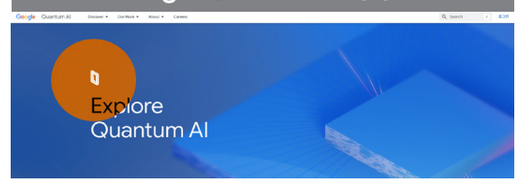
출처 : D-Wave Systems

구글 퀀텀 AI 로드맵
100만 큐비트 목표 (Google)

모든 컴퓨터에는 정보 연산이나 전송 과정에서 다양한 이유로 인해 오류를 발생시킬 수 있다. 그렇기에 컴퓨터에는 '오류 정정 코드' 기술이 들어가야만 하며, 양자 컴퓨터도 역시 필요하다. 그러나 0과 1로 표현되는 일반컴퓨터과 다르게 양자컴퓨터에는 0과 1이 중첩된 큐비트 상태로 존재하기에 새로운 오류 정정 코드가 필요하다. 이에 대해 구글은 2023년 양자 오류 보정에 대한 실험적 유의미한 결과로 세계 최초로 시연하며 네이처에 게재되었다. 기존 슈퍼컴퓨터로 1만년이 걸리는 작업을 3세대 프로세서인 시카모어(Sycamore)를 통해 200초 안에 수행할 수 있음을 실험적으로 증명하였으며 이를 통해 양자 우위에 도달하였다고 보고있다. 무작위 양자 회로를 샘플링하여 확률 분포를 출력하는 작업을 통해 정말 유용한 유형의 문제를 해결할 수 있는 양자 프로세서를 계속하여 개발하고 있다.

구글 연구팀은 양자컴퓨터 상업화를 구글 퀀텀 AI 로드맵에 대해 여섯가지 마일스톤을 목표로 하고있다. 현재 첫번째 마일스톤으로는 고전 컴퓨터를 뛰어 넘는 '양자 우위'(Quantum Supremacy)를 실현하였으며, 이어 2단계 이정표를 따르고 있으며, 최종 여섯번째 마일스톤은 실제로 100만개의 물리적 큐비트에 도달하는 것을 보고 있다. 이는 양적인 측면에서도 100만개의 물리적 큐비트를 달성하는 것으로 100만개의 알고리즘마다 하나의 오류가 있을 정도로 만드는 것인데, 구글 양자 컴퓨팅 부문 총괄 하트무트 네벤은 '그 단계가 되면 상업적 가치를 자신있게 약속할 수 있다.' 고 말하였다. 최근 설계한 퀀텀 가상 머신(Quantum virtual machine)을 설계하며 오픈소스로 누구나 사용할 수 있게 하였다. 이는 실제 하드웨어를 기반으로 학습된 가상 머신을 구축하여 사람들이 사용할 수 있으며 가상 버전인 시카모어 프로세서를 이용해 다양한 양자적 계산 방법을 알아보려고 한다면 누구나 알고리즘을 구축하여 실제로 적용하여 답을 얻을 수 있다.

Google Quantum AI 서비스



출처 : Google

산업 속 양자기술 활용 모습

양자 컴퓨터

LG전자

한국의 양자컴퓨터의 선두

LG전자는 최근 양자 컴퓨팅 기술의 발전을 위한 다양한 협력과 연구를 진행해오고 있다. 우선 2021년, 네덜란드의 양자 컴퓨팅 개발업체 큐앤코(Qu&Co)와 다중 물리 시뮬레이션을 위한 양자 컴퓨팅 기술 개발을 목표로 연구 협약을 체결하며 본격적인 양자 컴퓨팅 연구에 나섰다.

2022년에는 미국의 IT 기업 IBM이 결성한 'IBM 퀀텀 네트워크'에 합류하여 양자 컴퓨팅 기술 개발에 대한 협력을 강화하였다. 이 협력은 양자 컴퓨팅 기술의 상용화와 혁신을 가속화하는 데 중요한 역할로 보고있다.

이후에 2024년 LG전자의 성과로 양자 보안 직접 통신(QSDC)용 새로운 프로토콜을 개발하였다. 이 프로토콜은 양자 통신 시스템의 보안성과 전송률을 동시에 향상시키는 혁신적인 기술로, 시간과 위상 상태(Phase state)를 활용하여 단일 광자 기반의 고차원 프로토콜을 구현하고 있다. 이 기술은 기존의 전송률 제한 문제를 극복하는 데 큰 도움이 될 것으로 예상된다.

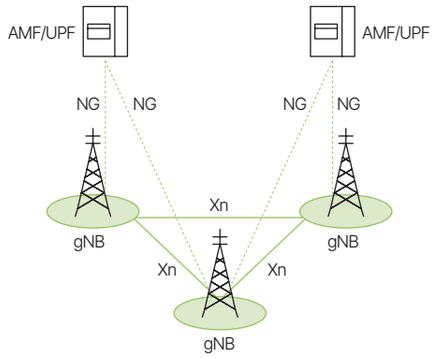
이러한 협력과 연구 성과를 통해 LG전자는 국내 양자 컴퓨팅 기술의 발전을 선도하고 있으며, 향후 양자 컴퓨팅 분야에서의 성장이 기대된다.

01 복잡한 물리적 문제를 해결하기 위해 기존의 '고전 컴퓨팅'과 '양자 컴퓨팅'을 함께 활용하는 방식을 만들었다. 이는 고전 컴퓨터가 문제의 초기값과 경계 조건을 설정하고, 양자 컴퓨터가 그 데이터를 바탕으로 문제를 해결한 후, 그 결과를 고전 컴퓨터가 받아 시각화하고, 최적화하는 방식으로 구현하였다.

다중 물리 문제 해결용 디바이스 도식화 블록도 (KR 10-2024-7017800)

02 양자 프로세싱 장치로부터 x, y, z축에 대한 관측(벡터) 데이터를 확보하고, 이 데이터를 이용하여 에러 완화 장치가 블로흐 구(Bolch Spher)라는 공간 상 연산을 수행하여 보정된 결과를 도출한다. 이런 방식을 통해 정보 손실을 줄일 수 있으며, 양자 도메인에서 발생하는 에러를 줄일 수 있게 되었다. (KR 10-2023-7012922)

03 양자 통신 시스템에서 두 개의 얽힌 광자 상태를 정확하게 식별하기 위한 고속 벨 상태 분석 장치를 개발하였다. 빔 스플리터와 편광 빔 스플리터를 이용해 광자의 지연 시간과 간섭 결과를 분석하여 얽힌 상태를 판단, 이를 통해 기존 기술보다 더 많은 정보를 단위 시간당 획득할 수 있어 양자 상태 측정의 성공률과 처리 효율이 최적화하였다.



무선 접속기술이 적용되는 차세대 무선 접속 네트워크의 시스템 구조 (KR 10-2024-7010427)

양자 통신

SK telecom

IT 장애까지 AI가 해결

글로벌 양자 기업 ID Quantique(IDQ)와 협력하여 구독형 양자암호 통신 서비스 QaaS(QKD as a service)를 출시하여 제공하고 있다. 기존의 양자 암호키 분배기(QKD)와 양자 암호키 분배기가 만든 양자 암호키를 통신에 적용할 수 있게 돕는 별도의 장비가 필요했던 반해, 하나의 양자키 관리 시스템을 통해 별도의 장비없이 기존 일방 통신 장비에 양자 암호키를 바로 적용할 수 있게 되었다.

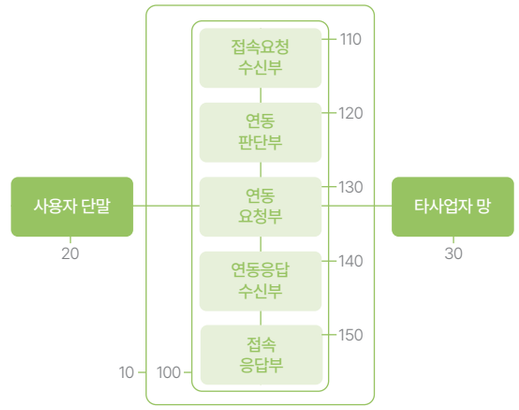
기존에 사용되는 VPN 서버 장비에 양자난수생성기(QRNG) 칩셋을 연동하여 양자암호통신 기반의 VPN을 개발하였다. 이는 기존 VPN 대비 별도의 장비가 필요가 없으며, 양자암호로 고수준의 보안을 실현하였다. 그리고 SKT는 양자암호와 양자내성암호를 통합해 관리하는 솔루션(Key Management Solution) 연구 진행을 통해 양자암호키와 양자내성암호를 통합적으로 운영할 계획이다. 이러한 양자키분배 기술을 적용한 구간과 양자내성암호 기술을 적용한 구간을 연결하여 통신 전 구간을 양자컴퓨터의 공격으로부터 보호할 수 있을 것이다.

이러한 꾸준한 연구 개발로 최근에는 SKT는 과기부의 '위성 탑재향(向) 장거리 무선 QKD 시스템 개발' 을 한국전자통신연구원과 한국천문연구원, 한국산업기술시험원, 경희대학교가 함께 컨소시엄을 진행하고 있어 더욱 기대된다.

SKT-엑스게이트-IDQ 고성능 퀀텀 VPN 기술개발 검증

출처 : SK 텔레콤 뉴스룸

01 특정 사용자 단말로부터 양자암호통신을 요청 받으면, 그 정보를 다른 통신망으로 전달하여 응답을 받은 후 사용자가 원하는 지역에서 양자암호통신 서비스를 제공할 수 있게 해주는 시스템을 개발했다. 이를 통해 다양한 사용자에게 양자 암호 통신을 편리하게 받을 수 있다.



양자암호통신시스템 구성요소 (KR 10-2023-0008145)

02 양자키 분배(QKD) 시스템을 이용해 네트워크 보안을 강화하는 것으로, 서비스 요청에 따라 생성된 양자키를 사용하여 데이터를 암호화하고, 전송 후 사용된 양자키를 폐기함으로써 데이터 전송의 보안 허점을 방지하는 장치를 개발하여 전송 네트워크의 보안을 향상시켰다.

보안강화 전송방법 (KR 10-202-0169350)

03 수동소자에 기반하는 양자암호키 분배(QKD)를 위한 수신장치를 개발, BB84 프로토콜을 사용하는 양자 암호키 분배 시스템에서, 두 개의 간섭계를 사용하면서도 두 개의 단일 광자 검출기만으로 작동할 수 있도록, 수동소자를 기반으로 편광 의존성을 없애는 수신장치를 만들었다. (KR 10-2020-0109876)

양자 암호

kt 양자암호 시스템 이 시대의 최강 보안 솔루션

4차 산업혁명의 시대, 기술의 발전에 따라 보안의 중요성은 더욱 커지고 있다. 특히 금융, 생체 같은 개인 정보 해킹은 사회의 안전을 위협하기에 해결책으로 '양자암호' 시스템을 선보이고 있다. 기존 통신의 보안은 난수 기반 암호키로 슈퍼컴퓨터나 양자컴퓨터의 수학적 분석이 가능하였는데, 양자 암호 통신은 시스템간 구간을 설정하여 양자암호키 분배시스템을 통해 암호키를 주고 받는다. 이는 양자 상태를 이용하여 암호키를 전달하기에 복제가 불가하며 탈취도 어렵기에 불가능한 암호체계 통신으로 보고 있다.

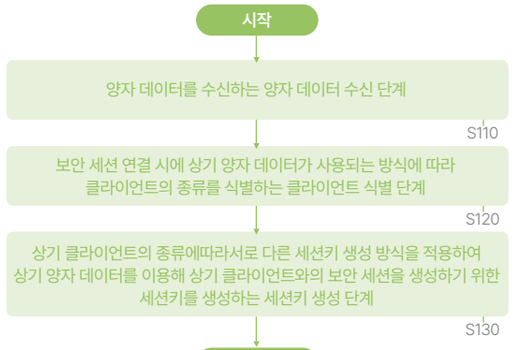
최근에는 KT가 초당 15만 개의 비밀키 정보를 생성하는 양자 암호키분배(QKD; Quantum Key Distribution) 장비를 개발하여 선보였다. 이 비밀키로 암호화하면 복제가 불가능하며 1분에 3만5천 대 이상의 암호화 장비에 양자 비밀키를 생산할 수 있을 것으로 보고 있다. 뿐만 아니라 양자암호화 통신장비인 QENC(Quantum Encrytor)를 독립형 모델로 자체 개발하고 솔루션 서비스 양자내성암호(PQC; Post-Quantum Cryptography)를 설계하였다.

양자암호키 분배장치에서 생성되는 암호키를 비롯한 PQC 알고리즘으로도 암호키를 제공받을 수 있어 하이브리드형 양자 보안망을 구축할 수 있다. 이러한 기술력을 기반으로 양자 암호 통신 서비스 품질 향상과 국내 양자 산업 역량 강화에 기여할 수 있을것이라 생각한다.

KT 양자내성암호(PQC) 솔루션

출처 : KT enterprise

01 가상 사설망(VPN)과 같은 통신망에서 양자 기술을 SSL 같은 보안 세션을 연결함으로써 보안을 강화했다. 우선 서버가 양자키 분배 장치에서 생성된 양자 데이터를 받으면 서버가 연결된 클라이언트의 종류를 식별한다. 이후 클라이언트 종류에 따라 서로 다른 방식의 세션 키를 생성하는데, 이때 양자 데이터를 사용하여 보안 세션을 설정하게 되는데, 결과적으로 클라이언트 종류에 따라 맞춤형 보안키를 생성하게 된다.



보안 세션 연결 방법 순서도 (KR 10-2024-0088616)

02 게다가 단일 광자를 이용한 양자 암호 통신 시스템을 통해 보안을 강화하였으며, 필터의 파장을 조정하여 더 정확한 통신이 가능하게 되었다. 이 때 가변 대역 통과 필터 및 단일 광자 검출기 등을 통해 검출 효율과 키 분배 속도를 개선했다. (KR 10-2022-0170399)

03 편광된 광 및 광 위상 변조기를 사용하여 암호 키를 안전하게 분배할 수 있는 양자 암호 키 분배 시스템을 만들었다. 별도의 편광 상태 보정 없이 작동 가능하여 양자암호키 분배 시스템의 구조를 단순화하며 제조 비용을 감소시켰다. (KR 10-2022-0169922)

04 게다가 양자 채널을 사용하여 원격 사용자 간 암호 키 분배하기 위한 장치를 개발하여 송신기와 수신기 사이의 외부 충격 또는 통신 문제가 발생 하더라도 끊김없이 양자암호 통신 서비스를 가능하게 하는 '양자 채널 자동 절체 복구 기술'을 개발했다. (KR 10-2022-0169733)

양자 암호

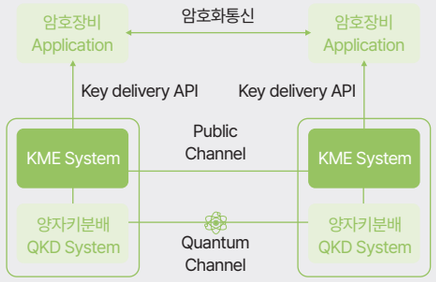
드림시큐리티 국가 통신망 강화를 위한 양자암호

2023년, 드림시큐리티는 양자키관리장비(QKMS)에 대해 국정원 보안 검증 갘국내 1호갘로 통과하여 양자 컴퓨터 시대의 암호기술을 공고히 하였다. 국정원 보안성 검증을 획득한 Magic QKMI는 양자키분배장비(QKD)의 제약을 해소할 수 있으며, 양자암호장비에 안정적으로 양자키를 제공하여 다양한 양자암호 네트워크 토폴로지를 구성할 수 있다.

뿐만 아니라, 대칭키나 해시 암호 알고리즘은 그루버 알고리즘에 대응할 수 있어 안전성을 확보하였으며, 공개키 알고리즘인 DH(Diffie-Hellman) 키교환, RSA, ECC를 양자 내성암호 알고리즘(PQC)로 전환 솔루션을 확보 하였다. 이를 통해 공개키 알고리즘이 적용되어 있는 모든 암호시스템과 공개키 전자서명을 사용하는 인증시스템에 활용할 수 있으며, 국가 통신망 등에 양자암호기술 및 양자 암호키분배기술을 적용하여 완전한 통신 보안 체계를 구축할 수 있다.

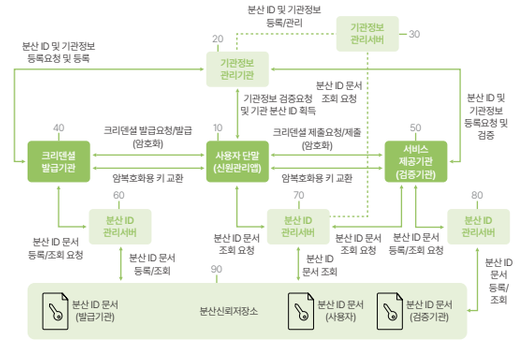
현재 드림시큐리티는 데이터를 보호할 수 있는 양자내성암호(PQC)를 지원용 Magic Qcrupto라는 양자내성암호모듈과 Magic TLS for PQC라는 양자내성암호(PQC)를 지원하는 전송 데이터 구간을 암복호화 솔루션을 확보하였으며, 양자암호통신망의 양자키를 안전하고 안정적으로 공급 관리할 수 있는 Magic QKMI라는 양자키관리 솔루션도까지 확보하였다.

드림시큐리티 양자키관리장비 특장점



출처 : 드림시큐리티 공식홈페이지

01 공공 ID를 이용해 서비스 제공자의 공개키를 얻고, 이 공개키를 암호화된 통신 암호키로 사용하여 데이터의 기밀성을 유지하며, 안전하게 메시지를 주고받을 수 있도록 설계된 기술을 개발하였다. 이 과정에 ID 공개키로 암호화하며 검증 단계가 있기에 보다 기밀성을 확보했다.



분산 ID 기반 서비스의 암복호화 통신 시스템 구성도
(KR 10-2022-0140396)

02 양자암호 기술을 TLS 프로토콜의 비밀키 생성 과정에 통합하여 보안을 강화하였다. 이 방식은 클라이언트와 서버 간의 암호화된 연결을 설정하기 위해 공개키 알고리즘으로 비밀키를 설정하고, 이 비밀키를 활용해 추가적인 보안 정보를 생성할 때 양자암호를 적용하여 암호화의 안전성을 높일 수 있게 되었다. 즉, 양자암호를 사용하여 더욱 안전한 비밀키를 생성하고, 이를 통해 통신의 보안을 향상킬수 있다.

공유키 확장 방법에 대한 순서도
(KR 10-2023-0074202)

03 국가전략기술 '양자' 이야기

국가전략기술로서의 '양자'

양자 기술은 더 이상 쪼갤 수 없는 물리량의 단위를 '양자'에 기반으로, 양자 역학의 원리를 ICT에 적용해 정보 전송과 연산 수행의 새로운 가능성을 열어주는 기술이다. 양자 기술의 주요 특성으로는 복제 불가능성, 중첩성, 얽힘 현상, 불확정성이 있다. 중첩성은 두 가지 성질을 동시에 가지는 특성으로, 예를 들어 큐비트(양자 컴퓨터의 기본 단위)는 0과 1의 상태를 동시에 가질 수 있다. 얽힘 현상은 두 개 이상의 양자가 특정한 관계를 맺어 서로의 상태에 영향을 주는 특성이며, 불확정성 원리는 입자의 정확한 운동량과 위치를 동시에 파악할 수 없음을 의미한다.

양자 기술의 범위는 크게 양자 컴퓨팅, 양자 통신, 양자 센싱으로 볼 수 있다. 양자 컴퓨팅은 양자 역학적 현상을 이용해 큐비트 기반의 확률적·가역적 연산방법을 사용하는 컴퓨팅 기술이다. 기존의 이진법 컴퓨팅과 달리 양자 컴퓨터는 동시에 여러 계산을 수행할 수 있어 복잡한 문제를 빠르게 해결할 수 있다.

양자 통신은 송·수신자 사이에서 단일 광자 또는 공유된 얽힘 상태를 이용해 양자 정보를 전달하는 기술로 보안성과 효율성을 높일 수 있다. 양자 센싱은 준비된 양자 상태가 계측 환경과 상호작용하면서 변화되는 것을 감지하는 기술로 기존 센서보다 훨씬 높은 정확도와 민감도를 자랑한다. 양자 기술은 기존 암호체계를 무력화시키거나, 암호 통신을 통해 보안을 강화하는 양면성을 가지며, 국가 간 경쟁이 치열해 안보적 측면에서 기술 확보가 필수적이다.

출처 : 대한민국 양자과학기술 전략, 과기부, 2023.06.27

국내 '양자' 기술의 위치와 잠재력

우리나라는 양자 R&D 후발국으로, 15년 이상 지원을 통해 성장해온 선도국에 비해 기술수준이 낮고, 인력과 인프라 기반이 미흡한 실정이다. 2000년대 중반부터 준비한 미국이나 유럽, 일본, 중국같이 선도국에 비해 양자 이론이나 초전도, 저온 물리 등 기반 기술뿐만 아니라 HW/SW 분야에서도 기술 수준이 낮은 상황이다.

양자 컴퓨팅 분야의 선도국들은 50~70큐비트의 양자컴퓨팅 시스템 시제품을 개발하고, 일부는 클라우드 서비스로 제공하며, 큐비트 확장과 오류 보정을 포함한 성능 고도화를 추진하고 있다. 반면 우리나라는 8큐비트 양자 프로세서를 개발했으며 소자와 기반 기술(냉동공학, 초전도 등), 소프트웨어와 알고리즘 개발 역시 선진국에 비해 뒤처져 초기 단계에 머물러 있다.

양자 통신 분야의 선도국은 초기 상용화 수준의 양자암호통신 시범 서비스를 운영 중이며, 100km 전송 한계를 극복하고 유무선 채널 다변화를 위한 연구를 진행하고 있다. 이에 우리나라 SKT가 5G 네트워크를 통해 서울-대전-대구 간 380km, KT가 전남도청-해군사령부 간 45km의 일부 유선 시범 서비스를 운영하며 초기 상용화 기술을 확보하였으나, 생산성 향상과 기존 인프라와의 연동, 장거리 양자 전송 및 유무선 채널 연구는 과제로 남아있다.

양자 센서 선도국들은 의료와 네비게이션 같은 시장성이 큰 분야에서 상온 동작이 가능한 소형화 연구를 진행하여, AOsense(미국), Cold QuantBosch(독일), Qnami(스위스) 등의 기업들이 시제품을 개발하고 있다. 우리나라에서는 실험실 단위에서 초소형 원자시계(표준연), 양자 자기장·자이로센서(ADD) 시제품 등을 개발하였으며, 현재 표준연(관성·자기장), 서울대(자기장), SKT(양자라이다), 우리로(단일광자) 등에서 기술 개발이 진행되고 있다. 양자 기술의 파급효과로 고도의 네트워크 보안, 초고속 계산, 초정밀 계측을 가능하게 하여 4차 산업혁명의 주요 산업들을 한 단계 발전시킬 것으로 전망한다. 예를 들어, 제조 및 물류 분야에서는 고성능 양자컴퓨터를 활용한 빅데이터 분석으로 최적화 문제를 해결할 수 있으며, 자율주행 분야에서는 양자기반 측위 센서를 통해 차량의 움직임과 교통 흐름을 실시간으로 분석·통신하여 자율·무인주행 실현에 기여할 수 있다. 또한, 국방, 금융, 의료 분야에서는 정보 보안이 중요한 만큼, 암호 탈취가 원천적으로 불가능한 양자암호통신이 기존의 사이버보안 체계를 대체할 것이다.

뿐만 아니라 의료 분야에서도 양자컴퓨팅의 연산 능력을 신약 개발, 유전자 및 의료 영상 분석 등의 바이오인포메틱스에 활용할 것으로 제약 및 화학업계의 임원들은 양자컴퓨터 기술이 향후 신약 개발 성공률을 5~50% 향상시키고, 개발 시간을 15~20% 줄일 것으로 전망하고 있다. 이는 2019년 매킨지 보고서에서도 언급된 바 있다. 이러한 기술적 진보는 각 산업 분야에서 혁신을 촉발하고, 효율성을 극대화하며, 새로운 기회를 창출하는 데 기여할 것이다.

전 세계 주요 국가들은 양자 기술을 미래 산업 생태계를 변화시킬 혁신 기술로 보고 적극적인 육성 전략을 펼치고 있다. 미국은 2018년에 '국가양자이니셔티브' 법안을 제정하여 양자 기술의 연구, 개발, 시연, 응용을 지원하고 있으며, 2020년에는 '양자인터넷 전략적 비전'을 발표해 양자 분야에서 인터넷의 파급효과를 실현하고자 한다. 일본은 2010년부터 양자 기술 개발을 시작해 2016년에 양자과학기술·연구개발기구(QST)를 설립했으며, 양자 기술을 인공지능, 바이오와 함께 3대 국가 전략 기술로 지정했다. 최근에는 FIRST, ImPACT, ERATO 등의 프로그램을 통해 양자 기술 연구를 진행하고 있다. 중국은 2017년에는 세계 최대의 국립 양자기술연구소를 설립하고 13조 원 규모의 투자를 발표, 캐나다는 대학을 중심으로 양자 기술을 육성하며, 정부 차원의 전폭적인 지원을 통해 글로벌 경쟁우위를 강화하고 있다. 유럽은 2016년에 양자 선언문을 발표하고 2018년에 양자 플래그십 프로젝트를 출범하여 각국의 양자 기술 연구를 지원하고 있다. 양자 기술의 혁신성과 글로벌 경쟁양자 기술은 고도의 네트워크 보안, 초고속 계산, 초정밀 계측을 가능하게 하여 4차 산업혁명의 주요 산업을 한 단계 발전시킬 것으로 기대된다. 이처럼 각국은 양자기술의 중요성을 인식하고, 이를 기반으로 한 국가 경쟁력 강화를 위해 다양한 노력을 기울이고 있다.

정부 주도의 양자 암호통신 육성을 위한 국책연구과제 및 전국 규모의 망 구축 사업이 진행 중이며, 대기업과 연구기관을 중심으로 양자컴퓨팅, 암호통신 기술 개발이 활발하게 이루어지고 있음

국가수준의 양자네트워크 구축과 양자 전용 위성 활용 등 양자 암호통신 분야에서 최고수준의 기술을 보유하고있으며, 양자분야에 대한 지속적인 투자를 진행

양자통신의 원천기술인 양자광학 연구에서 매우 우수한 연구결과를 가지고 있으며, 양자 네트워크 핵심기술 개발 성과가 지속적으로 나타나고 있음

유럽연합을 관통하는 국가 연합 양자 네트워크 구축 프로그램을 통해 양자통신 기술의 개발과 적용이 활성화되고 있으며, 학문적 전통을 기반으로 한 기초 연구력을 확보하고 있음

20년 양자 인터넷 전략 비전 발표, 22년 백악관 산하 국가 양자 이니셔티브 위원회 신설 등을 통해 양자분야에 지속적인 투자를 진행하고 있으며, 국가 수준의 양자 네트워크 구축 실적과 양자 전용 위성을 이미 활용 중임

국가별 양자 기술수준 근거

2022년도 기술수준평가 결과(안), 과기부

'양자' 중점기술분야

양자컴퓨팅

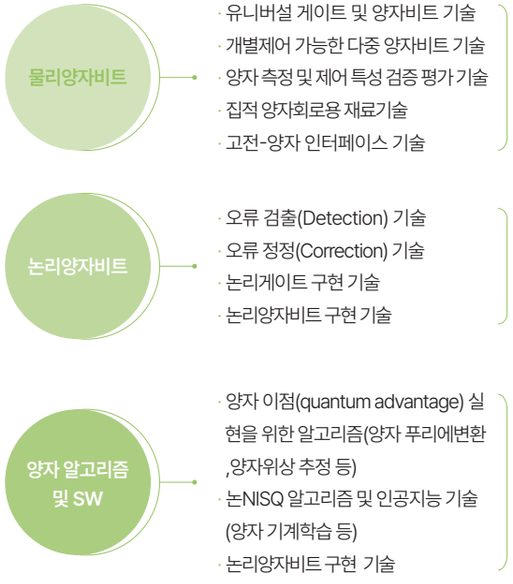
#알고리즘 #프로그래밍 #아키텍처

양자 컴퓨팅은 고도의 연산 능력을 통해 다양한 산업 분야에서 혁신을 촉발할 잠재력을 가지고 있다. 예를 들어, 복잡한 문제를 해결하는 데 있어 기존 컴퓨터가 100만 년 이상 걸리는 2,048비트 RSA 공개키 암호를 양자 컴퓨터는 1초 만에 풀 수 있다. 이러한 기술적 특성으로 인해 양자 컴퓨팅은 AI, 신약 개발, 에너지 등 다양한 산업 분야에서 새로운 가능성을 열어 줄 것으로 기대된다.

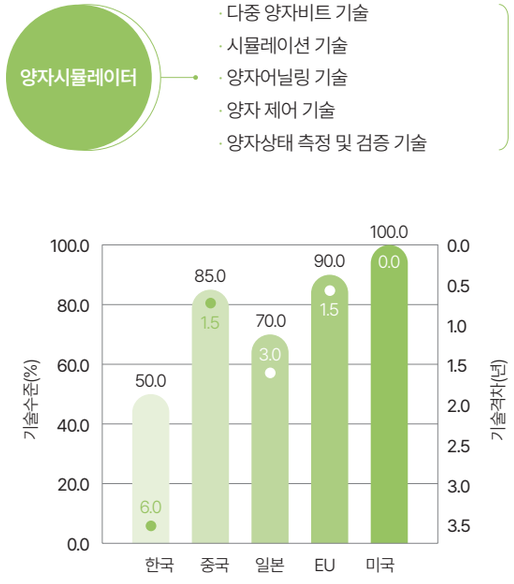
양자 컴퓨팅은 양자역학적 현상을 이용해 큐비트(Q-bit) 기반으로 확률적이고 가역적인 연산방법을 사용하는 컴퓨팅 기술이다. 이는 기존의 이진법 컴퓨터와 달리 양자 중첩과 얽힘 현상을 활용해 동시에 여러 상태를 계산할 수 있다. 양자 컴퓨팅의 주요 요소기술로는 물리 큐비트, 양자 알고리즘 및 소프트웨어, 그리고 양자 프로세서가 있다. 이러한 기술을 통해 양자 컴퓨터는 기존 컴퓨터로는 불가능한 수준의 월등한 연산 능력을 갖추게 된다.

글로벌 기술 및 산업 동향을 보면, 구글, IBM 등 주요 기업들이 시장 선점을 위해 양자 컴퓨터 개발에 박차를 가하고 있다. 구글은 2029년 양자 컴퓨터 상용화를 목표로 하고 있으며, 중국과기대는 2021년 5월에 세계 최고 수준의 62큐비트급 양자 컴퓨터 개발에 성공했다고 발표했다. 이에 반해, 한국은 후발국으로서 양자 이론, 초전도, 저온 물리 등 기반 기술과 하드웨어/소프트웨어 모든 면에서 기술 수준이 낮은 상황이다.

큐비트 플랫폼 발전 양상에 따라 빠르게 추격할 기회가 존재하므로 집약된 연구개발(R&D)을 통해 양자 컴퓨팅의 활용성과를 창출할 필요가 있다. 특히, 바이든 정부 출범 이후 미·중간 양자 컴퓨터 경쟁이 가속화되고 있으며, 한-미 정상회담에서도 양자 기술을 주요 협력 의제로 논의하는 등 외교적 가치가 높아지고 있다.



출처 : ICT R&D 기술로드맵 2025, 정보통신기획평가원, 2020.12.16



출처 : 2022년도 기술수준평가 결과(안), 과기부, 2024.02.29

양자통신

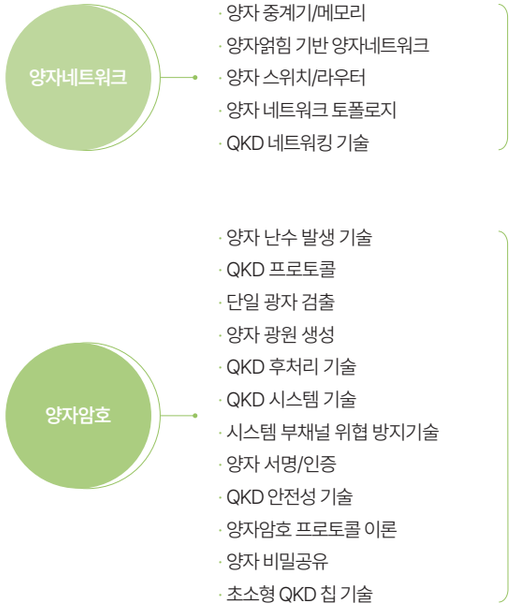
#암호학 #보안 프로토콜 #네트워크 #보안감시

양자통신은 송·수신자 사이의 단일광자 또는 공유된 얽힘을 통해 고전 통신기술의 도움으로 양자 정보를 전달하는 기술로, 주요 요소기술로는 유무선 양자암호, 양자키분배(QKD) 네트워크, 양자전송 등이 있다. 이 기술은 기존의 암호화 방식과는 달리, 중간에 도청이나 정보 탈취가 원천적으로 불가능하다는 특징을 갖는데, 이는 정보통신 분야에서 획기적인 변화를 일으킬 수 있는 기술로, 특히 보안이 중요한 분야에서 큰 주목을 받고 있다.

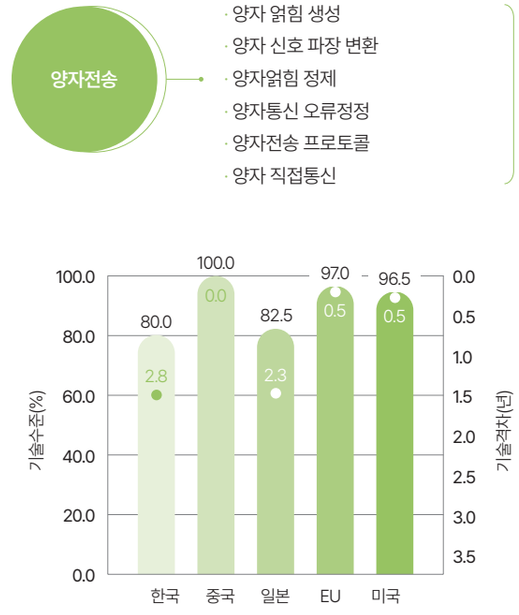
장기적으로는 기존의 인터넷처럼 정보를 양자 상태로 전송하는 '양자인터넷'으로 발전할 전망으로 현재 양자통신 실용화에 가장 가까운 기술 중 하나로, 미국, 중국, 한국 등에서 일부 유선 통신 서비스를 제공하고 있다. 특히 중국은 양자위성통신에서 독보적인 위치를 차지하고 있으며, 세계 최초의 양자위성인 '묵자호'를 통해 양자 통신 실험을 성공적으로 수행한 바 있다.

한국은 양자키분배(QKD) 분야에서 경쟁력을 확보하고 있으며, 유선 양자암호통신의 상용화 기술 기반도 일부 갖추고 있다. 특히 SK텔레콤이 인수한 IDQ는 양자통신 프로토콜 기반 양자키분배 모듈과 양자 난수발생기 등 상용화에 성공한 바가 있듯이, 이러한 기술적 성과를 바탕으로 한국은 글로벌 시장에서의 경쟁력을 강화하고 있다.

그러나 각국의 암호통신 서비스를 통한 시장 주도권 경쟁이 심화되고 있는 상황에서, 한국도 글로벌 수준의 제품 개발과 기술 경쟁력을 확보해야 할 필요성이 있다. 이를 통해 미래 시장을 선도하고, 양자통신 분야에서의 입지를 더욱 공고히 할 수 있을 것이다. 양자통신 기술은 고도의 보안성과 신뢰성을 제공함으로써, 다양한 산업 분야에서 혁신적인 변화를 일으킬 것으로 기대된다.



출처 : ICT R&D 기술로드맵 2025, 정보통신기획평가원, 2020.12.16



출처 : 2022년도 기술수준평가 결과(안), 과기부, 2024.02.29

양자센싱

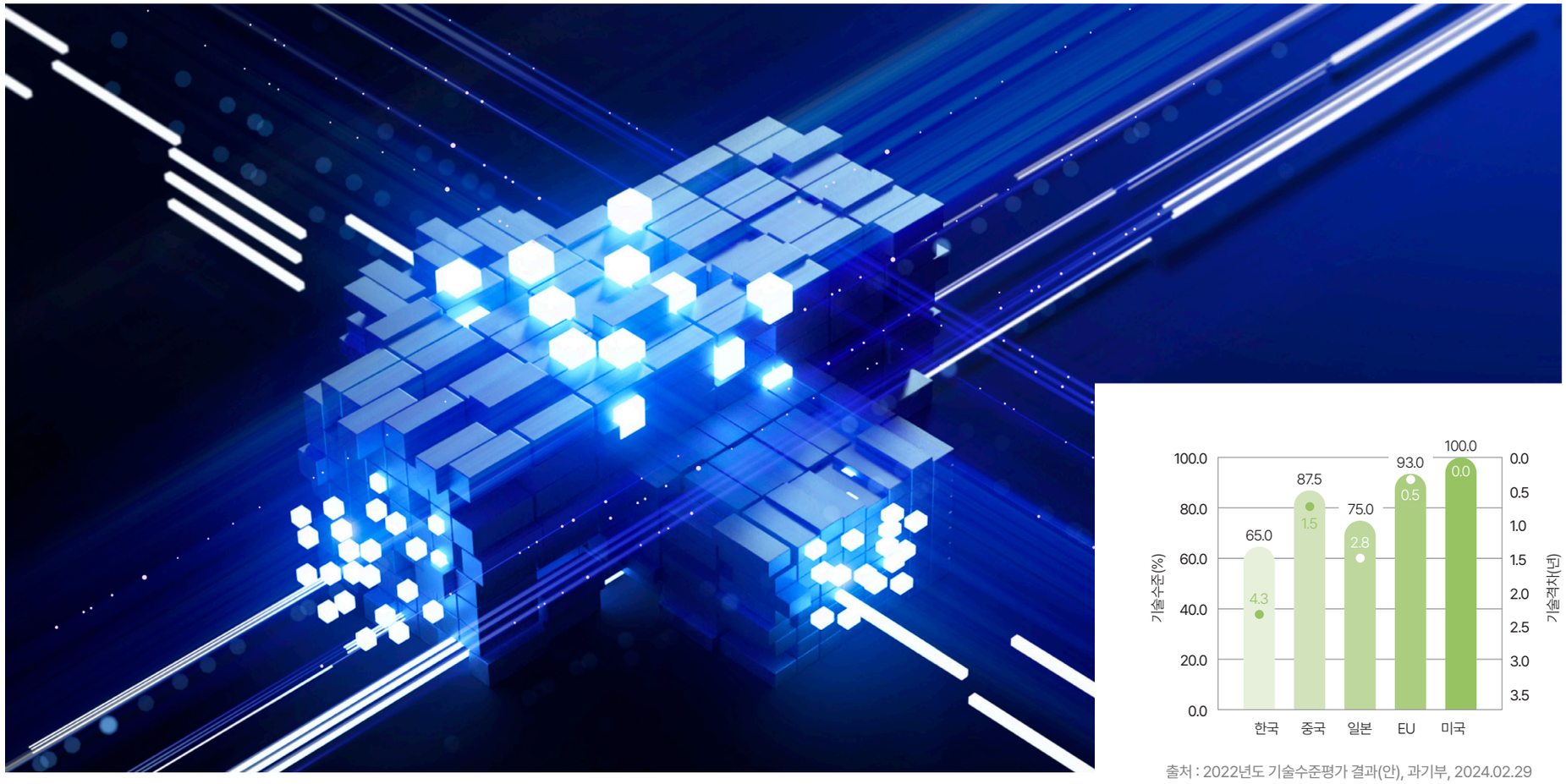
#센서네트워크 #특이점검출 #양자측정

양자 센싱은 준비된 양자 상태가 계측 환경과 상호작용하면서 변화되는 것을 양자 측정을 통해 감지하는 기술로 주요 요소 기술로는 양자 관성 센싱, 양자 전·자기장 센싱이 있다. 특히, 양자역학의 특성을 활용한 양자 센싱 기술은 기존 기술로는 구현할 수 없는 고도의 정밀도와 정확도를 구현할 수 있다.

양자 센싱 기술은 현재 다양한 산업 분야에서 연구개발이 진행되고 있어, 특히 양자 관성, 자기장, 이미징 센서를 중심으로 정밀도와 분해능을 향상시키고 상온에서 동작할 수 있도록 기술적 난제를 해결하는 데 중점을 두고 있다. 이러한 기술 발전은 의료, 항해, 자율주행, 자원 개발 등에서 높은 활용성을 가지고 있다.

한국의 양자 센서 기술 수준도 KIST, KRISS, KAIST 등에서 다이아몬드, 원자 자력계, SQUID 센서 연구가 활발하게 진행되어 빠르게 상승하고 있다. 이러한 연구 덕분에 양자 센서 응용 분야의 기술 수준이 비교적 높아 산업화 가능성을 가지고 있는데, 특히 일부 분야에서는 글로벌 기술 수준을 선도하고 있어 적극적인 육성이 필요하다.

양자 센싱 기술은 기존의 성능을 초월하는 센서로, 향후 우주, 항해, 의료 등 산업 전반에 걸쳐 큰 수요가 예상된다. 그러나 아직 산업화되지 않아 시장성이 적기 때문에 정부의 선제적 투자가 필요하며, 이러한 투자를 통해 양자 센싱 기술의 선제적 기술력을 확보하고, 향후 다양한 산업 분야에서 활용될 수 있는 기반을 마련해야 한다.



출처 : 2022년도 기술수준평가 결과(안), 과기부, 2024.02.29

양자 시간측정 센서
- 유양자 노드 간 얽힘 생성
- 원자 스핀 압착 기술
- 핵전이 주파수 탐색 기술
- 초발광 유도기술
- 원자 증기셀 소형화 기술
- 광주파수 합성 소형화 기술
- 광회로 집적화 기술
- 양자 비파괴 측정 기술
- 측정 정확도 검증 기술

양자 자기장·전기장 센서
- 고순도 단결정 양자소재 성장 기술
- 양자 단일/복합 불순물 생성기술
- 양자 단일/복합 광원 생성기술
- 초분극 발생 기술
- 양자 간섭계 제작 기술
- 양자 결맞음 유지 기술
- 원자 증기셀 제작 기술
- 양자 자기공명 측정 기술
- 양자 자기공명 영상화 기술
- 원자 전기장 측정 기술

양자 광학 센서
- 양자 간섭계 제작 기술
- 고감도 양자분광센서 기술
- 비접촉 양자이미징
- 양자현미경 기술
- 양자얽힘 생성/측정 기술
- 압착광원 간섭계 제작 기술
- 양자상태 단층분석
- 양자얽힘 평가지수 측정
- 측정 정확도 검증 기술

양자관성 센서
- 원자 간섭신호 생성 기술
- 레이저 냉각/포획 장치 소형화
- 고진공 챔버 소형화 기술
- 원자 스핀 압착 생성 기술
- 라만 레이저 광회로 집적 기술
- 나노역학계 냉각 기술
- 광역학계 잡음 측정 기술
- 비가우시안 상태 생성 기술
- 양자 잡음 이론
- 양자 비파괴 측정 기술
- 측정 정확도 검증 기술

출처 : 2022년도 기술수준평가 결과(안), 과기부, 2024.02.29

04 출연(연) 보유 '양자' 기술

한눈으로 보는 출연(연) 기술 보유현황

양자 중점기술 분야별
기술 보유현황

출연(연) 보유 양자
주요기술

ETRI | KISTI | KIST | KRISS | KIMS

양자 컴퓨터

KIMS · 시뮬레이션 및 데이터 과학 활용 신소재 탐색 설계 / 오창석

KRISS · 초전도양자컴퓨팅 시스템연구단 / 이용호
· 양자기술연구소 / 이상민

양자 통신

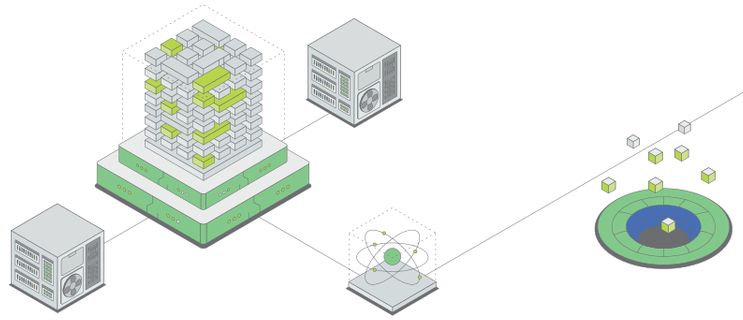
KISTI · 양자키 운영관리 기술 / 오창석

ETRI · AI 반도체/NPU를 위한 컴파일러 V1.0 (NEST-C V1.0) / 김태호
· 양자내성암호 기반 보안채널 생성 기술 / 윤승용

양자 센싱

KIST · 단일 광자 광원을 이용하여 다이아몬드을 국소적이고 선택적으로 개질하는 방법 / 김철기

KRISS · 음향파의 거동을 제어할 수 있는 굴절률분포형 음향양자결정 평면렌즈 / 최원재
· 양자얽힘과 비검출 기술을 통한 양자광센싱 기술 / 이선경



'양자' 기술개발 연구자 인터뷰

양자 컴퓨터 시대를 대비한 양자 키 릴레이 기술

KISTI
이찬균 박사

양자컴퓨터와 양자알고리즘의 발전으로 인해, 복잡한 수학기반의 현재 인터넷 보안 체계가 위협받고 있습니다. 양자 암호 통신은 양자의 물리적 성질을 활용하여 안전하게 생성된 양자키를 데이터 암복호화에 활용하는 기술로, 보안체계를 수학적 복잡도에 기반하는 것이 아닌 양자의 물리적 특징에 기반하고 있습니다. 따라서 다가오는 양자 컴퓨터 시대에도 안전한 보안통신을 가능하게 합니다. 현재 양자 기술력에서는 양자키를 생성하는데 소모되는 양자자원이 비싸고 희소하여, 양자 암호 통신의 상용화를 제한하는 요소입니다. 따라서 제한된 양자자원을 정보통신 기술에 적용할 때, 해당 양자자원을 효율적이고 효과적으로 관리 및 운영하는 양자 키 운영관리 기술은, 현실적인 양자 암호 통신의 성능을 좌우하는 주요 기술이라고 할 수 있습니다.

현재 양자 키 분배 기술력에서는 인접한 두 양자 키 분배 노드 간 거리에 제약이 있습니다. 이 거리 제약을 극복하기 위해 신뢰할 수 있는 릴레이 노드를 중간에 설치하여, 양자 키를 릴레이하여 단대단(end-to-end) 양자 키를 생성합니다. 양자 키 릴레이 과정에서 다수의 양자 키가 소모되며, 이 소모되는 양자 키는 비싸고 희소한 자원이므로, 효율적인 양자 키 릴레이 알고리즘이 요구됩니다. 본 기술에서는 양자 암호 통신망 노드 간 보유 중인 양자키의 개수를 고려하여 양자 키 릴레이가 필요한 두 개의 단대단 노드를 결정하고, 노드 간 경로를 결정합니다. 특히 제안하는 기술에서는 양자 키 개수의 차분(differential)을 고려하는 방법을 통해 보다 효과적으로 양자 자원을 소모하여 단대단 키를 생성합니다.

또한 양자 암호 통신에서는 양자 키를 중간에 릴레이할 때 지연시간이 발생할 수 있습니다. 이는 기존의 암호 통신에서는 없는 문제입니다. 따라서 본 기술에서는 양자 암호 통신 서비스 요청 발생 전이라도 특정 조건을 만족하는 경우에는 단대단 양자 키를 미리 생성하며, 향후 해당 양자 키를 요구하는 양자 암호 서비스가 발생하는 경우 무지연 양자 키 제공 서비스를 사용할 수 있어 기존 암호 서비스 대비 양자 암호 서비스의 단점을 극복할 수 있습니다.

미국, 유럽, 일본, 중국은 양자 암호 통신망 테스트베드를 구축하였으며, 각각 기존의 네트워크 라우팅 알고리즘을 모사한 양자 키 릴레이 알고리즘이 적용된 사례가 있습니다. 본 기술은 4개 노드로 구성된 KISTI 양자 암호 통신망 테스트베드에 적용 중이며, 테스트베드에서의 광범위한 실험을 통해 본 기술의 적용 가능성을 검증할 예정입니다.

상용화 전에 개발 기술에 관한 광범위 검증이 필요합니다. 본 기술은 양자키 릴레이를 위한 경로를 계산하는 방법을 포함하기에, 본 기술을 검증하기 위하여는 다수의 노드와 링크로 구성된 대규모 다중경로 양자암호통신망이 필요합니다. 현재 48개의 노드와 164개의 링크로 구성된 대규모 백본토폴로지 상에서 광범위한 시뮬레이션을 통해 해당기술에 대한 동작 검증을 완료하였으며, 특히 수식에 기반한 최적 알고리즘대비 최대 10% 이내의 양자자원추가소모 성능검증을 확인하였습니다. 또한 최적 알고리즘대비 99.9%의 계산시간 절감효과를 확인하여 개발 알고리즘의 대규모 네트워크 적용 가능성을 검증하였습니다. 논문지 발표 (Optica, Journal of Optical Communications and Networking 2023)를 통해 개발 기술의 학술적 검증을 완료했습니다. 상용화를 위해서는 앞으로 실제 양자암호통신망 장비에 개발 기술을 적용하여 검증이 필요합니다. 현재 양자암호통신망을 구성하는 양자키분배모듈은 고가의 장비로, 이웃한 모든 노드 쌍간 해당 모듈이 설치되어야 합니다. 따라서 대규모의 다중경로 양자암호통신망을 구축하여 개발 기술의 상용화를 위한 검증을 수행하는 것은 매우 어려우며, 현재 실장비로 구성된 KISTI 양자암호통신망 테스트베드 (4개 노드, 12개 링크) 에 개발 기술을 적용하고 있습니다. 테스트베드 대규모 검증을 통해 개발기술 상용화를 준비하고 있습니다.

각국은 양자 기술 연구에 집중하고 있으며, 향후 양자 컴퓨터 시대가 도래하기 전에 양자 암호 통신 기술 기반의 보안 체계 전환이 필요할 것입니다. 특히 정보 통신에 적용되는 기술은 성능과 더불어 비용 효율적인 측면이 기술의 성패를 좌우합니다. 본 양자키 운영 관리 기술은 양자 암호 통신에서 가장 제한되고 고비용인 양자 자원을 효율적이고 효과적으로 활용하여 양자 암호 서비스를 달성하는 기술입니다. 또한, 기존 암호 통신 대비 양자 암호 통신의 단점으로 부각되었던 키 지연 시간을 극복하는 기술로서, 양자 암호 통신망의 성능과 상용화의 성패를 좌우하는 기술이라고 할 수 있습니다. 따라서 가까운 미래에 대규모 다경로 양자 암호 통신망이 상용화될 때 적용 가능성이 매우 높은 기술이라고 할 수 있습니다.

일본 KDDI 연구소 방문 연구원 재직
삼성전자 차세대 사업팀, 네트워크 사업부
KISTI 양자통신 연구단

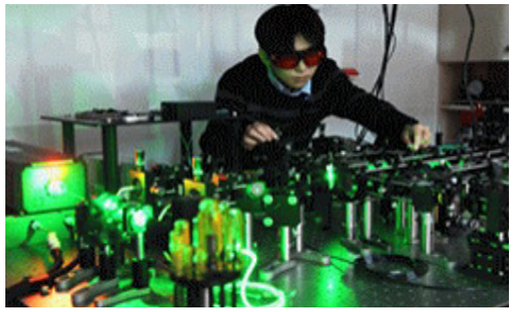
출처 : 한국과학기술정보연구원 유튜브

양자 컴퓨터 시대를 대비한 양자 키 릴레이 기술

한국표준과학연구원
이선경 박사

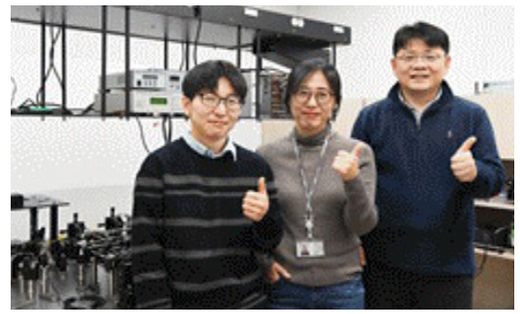
기존의 고전적 광센싱 방법은 샘플에 조사된 광의 변화를 측정하는 방식으로, 레이저와 같은 고전 광원의 파장과 광량에 의해 분해능과 정확도에 한계가 있고, 고출력 광원을 사용해야 하며 샘플을 파괴할 위험이 있어 실질적인 제한이 많습니다. 이에 양자광센싱(이미징 및 분광)은 양자얽힘 광자쌍이나 단일 광자와 같은 비고전 광원을 활용하여 고전적 측정 한계를 넘어서는 기술입니다. 양자광센싱은 고전광원 대신 얽힘 상태의 광자쌍을 사용합니다. 여기서 양자 '얽힘'이란 두 개 이상의 광자가 서로 연관되어 있어 고전적인 설명으로는 이해할 수 없는 상태를 의미합니다. 이 특성 덕분에 양자광센싱은 기존의 한계를 극복하고 높은 정확도와 낮은 잡음으로 측정을 수행할 수 있으며, 특히 단일 광자쌍을 사용하는 경우 샘플이 파괴될 우려가 없습니다. 게다가 얽힘광자 기반 광센싱에서는 하나의 광자만 샘플을 통과시키고, 다른 광자는 통과시키지 않아 두 광자의 동시 측정을 통해 샘플을 분석합니다. 그러나, 보통 얽힘광자 기반 광센싱의 경우, 하나의 광자만 샘플을 통과시키고 다른 짝광자는 샘플을 통과시키지 않으며, 두 광자 동시 측정의 변화를 통해 샘플을 분석합니다. 이때 여전히 단일광자 검출기 파장 한계에 의해 측정이 제한되고, 측정 효율도 단일 모드만 측정하는 경우에 비해 매우 낮아 측정 시간이 오래 걸리게 됩니다. 최근에는, 양자간섭계를 부가적으로 활용하여 샘플에 조사된 광자는 측정하지 않고 얽힘 관계의 짝광자만 측정하여 샘플의 특성을 분석하는 비검출 광자기반 광센싱 기술이 구현되었습니다. 이는 측정 효율 뿐 아니라, 조사광의 파장과 무관하게 발달된 고효율 검출기를 활용할 수 있어 고전적인 측정장치 한계를 극복할 수 있습니다.

양자광 센싱 기술은 기존의 센싱 기술보다 더 정확하고 선명하며, 잡음이 적고 장비의 한계를 극복할 수 있는 기술입니다. 이 기술은 양자 '얽힘'과 같은 특수한 광학적 성질을 이용하여 비검출 광자기반 양자광센싱 기술은 서로 다른 파장대역을 가진 광자쌍을 사용하여 물질의 특성을 분석하며, 조사된 광자를 직접 측정하는 대신 얽힘 관계를 가진 짝광자를 측정하여 샘플의 정보를 추출함으로써 더 정확하고 효과적인 측정을 가능하게 합니다. 이때 세 가지 요소 기술은 크게 양자광원, 유도 양자간섭계, 그리고 단일광자 검출기가 있습니다. 첫 번째로, 얽힘 광자쌍을 생성하는 방법에 대해 말씀드리면, 가장 알려진 방법은 비선형 광결정을 통해 빛의 자발매개하향변환(SPDC)을 이용한 것입니다. 이는 레이저(펌프광)가 비선형 매질에 가해질 때 매질 내 원자가 펌프광의 에너지를 얻어 여기되었다가 자발방출에 의해 낮은 에너지의 얽힘 광자쌍을 생성하는 현상을 말합니다. 이때, 광자쌍의 특성(파장, 생성율, 빔폴질, 스펙트럼, 밴드폭 등)은 에너지 보존 법칙과 운동량 보존법칙에 의해 결정이 되고, 따라서 대상 샘플에 맞게 광원 시스템을 설계하고 구성할 수 있습니다. 두 번째로, 유도 양자간섭계란 두 개의 비선형 광결정을 포함하는 비선형 간섭계인데, 두 개의 경로 중 한 경로에 광자쌍(시그널-아이들러)이 존재하는 경로 얽힘 상태와 아이들러 광자의 경로지움을 통해 시그널 광자의 간섭이 유도되는 "유도결맞음"이라는 양자 현상을 활용합니다. 세 번째로, 단일광자검출기란 단일 광자 에너지 측정이 가능한 고감도/저잡음 검출기로, 상용화된 Si/InGaAs SPAD, SNSPD 단일/멀티 채널 단일광자검출기나, EMCCD/CMOS 어레이 검출기를 활용합니다.



KRISS 비검출광자 양자센서 실험

현재 이 기술은 산업화된 사례가 없으며, 향후에는 가스 센싱, 바이오 이미징, 분자 이미징, 라이다 등 다양한 분야에서 응용 가능성을 가지고 있어, 기초 연구 단계로 실용화를 위한 검증이 필요합니다. 비검출 광자기반 양자광센싱 기술의 상용화를 위해서는 크게 1.광대역 파장얽힘 광원 2.복합 대역 양자간섭계 안정화 및 유도 간섭 구현, 3.고전 계측법과의 이론·실험적 비교 및 양자이득 분석 4.센싱 파라미터 성능 표준화가 필요합니다. 하지만, 범용 양자광센서를 개발하기 위한 현재 기술의 한계점은 1.양자광원, 유도 양자간섭계 파라미터 성능 간의 원리적·기술적 상충 관계, 2.고전 계측 방식과의 이론적·실험적 비교를 통한 양자이득 실증 프로토콜 확립, 3.양자광센싱의 복합적인 양자이득(분해능, 감도,장치극복) 가능성 검토 등이 있습니다. 이러한 한계점들로 인해 충분한 기초 연구 및 다양한 구현 사례를 확보할 필요가 있으며, 활용 범위를 확장하기 위해 최첨단 고전 측정 기술과의 융합 연구와 광집적회로 기반의 소형화 기술 개발이 필요합니다.



비검출광자 양자센서 연구진

양자 얽힘광원 기반 양자광센싱 기술은 차세대 라이다, 레이더, 고분해능 현미경, 초정밀 분광 센싱 등에서 기존 기술의 한계를 극복할 수 있는 가능성이 큽니다. 특히, 국방 안보, 대기환경 이미징, 의료 이미징 등 다양한 분야에서 응용될 수 있습니다. 더불어, 개발한 양자 계측법을 고전적 리소스 기반으로 모사 하는 경우에도 고전 센서 기술 발전을 동반할 수 있습니다. 따라서, 양자광센싱 원천 기술 개발은 세계 양자측정 표준 기술 발전에 기여하고, 양자센싱 시장에 진입할 수 있을 것으로 기대합니다. 또한, 앞에 언급한 바와 같이 양자상태 정밀 측정을 기반으로 하는 양자광센싱 기술은 다른 양자정보기술의 기반 기술로, 기술 발전 시 타 광정보 기반 양자기술도 함께 성장할 수 있을 것으로 기대합니다.

고전광센싱과 양자광센싱 기술 개념도