양자컴퓨팅 및 양자암호통신 기술 동향과 산업 전망

유형정 한국과학기술기획평가원 미래기술기획센터 부연구위원

1. 머리말

"미래산업의 게임 체인저. 양자혁명 시대"라는 말이 유행하고 있다. 양자컴퓨팅과 암호통신을 포함한 양자기술(Quantum Technology)은 이공학 문헌에서 자주 보이던 말이지만 이제는 TV 다큐멘터리에서도 심심치 않게 볼 수 있으며, 사람들의 관심도 높은 상황이다. 글로벌 시장조사 전문기관들도 머지않은 미래에 양자 기술 시장이 본격적으로 열려 성장할 것이라는 전망을 내고 있다. 물론 진입 장벽이 높고, 구현하기가 까다롭고 어려운 기술이라 실제 사용되기까지는 시간이 걸리겠지만, 수년 안에 활용할 수 있도록 각국 정부가 크게 주목하고 투자하고 있는 분야이기도 하다.

우리 정부도 이에 발맞춰 2021년 4월 미래 전략기술 확보를 위한 '양자기술 연구개발 투자전략'을 수립하고, 2030년대 양자 기술 4대 강국 진입을 위한 10년 이상의 국가 차원의 중장기 비전을 제시하였다. 이듬해 5월 윤석열 정부가 발표한 110대 국정과제에도 양자기술 및 산업, 통신과 관련된 주요 과제 2개(국정과제 75 및 101)가 들어 있으며, 곧이어 6월 '디지털 패권국가 도약을 위한 디지털 기술혁신 및 확산전략'에도 양자 기술이 포함되어 있다. 그해 10월에는 '기술주권 확보를 통한 과학기술 G5 도약, 국가전략기술 육성방안'을 발표하고 12대 국가전략기술 중 하나로 양자기술을 선정함으로써 양자기술 육성에 국가적 역량을 결집하고자 하는 정부의 의지를 표출한 바 있다.

이러한 양자 기술 시대를 맞이하여 본 고에서는 국내외 양자컴퓨팅 및 암호통신 기술 동향과 산업 전망을 살펴보고자 한다. 또한 우리나라에서 현재 수행 중인 양자기술 정부 R&D 사업을 간략히 소개하고 양자 시대를 대비하는 정책적 제언을 제안한다.

2. 양자 기술·산업 동향

2.1 양자컴퓨팅

최초의 전자식 컴퓨터가 발명된 이후 정보를 다루는 단위는 0과 1의 두 가지 상태 중 하나의 상태만 허용하는 비트였다. 반면 양자역학을 직접 이용하는 새로운 계산 패러다임을 제시한 양자컴퓨팅은 정보의 단위로 양자 비트, 즉 큐비트(qubit)를 사용한다. 큐비트는 0과 1의 양자역학적 중첩 상태를 계산에 이용하며, 이를 통해 고전 컴퓨터의 성능을 뛰어넘는 양자 우월성(quantum supremacy) 또는 양자 이점(quantum advantage)을 보일 수 있다. 이상적인 양자컴퓨팅은 잡음에 의한 오류 보정 기능을 기반으로 임의의 프로그래밍이 가능한 대용량 정보처리

기능을 가지는 것을 의미한다. 하지만 현재까지 양자 알고리즘은 대부분 많은 큐비트와 긴 연산을 필요로 하기 때문에, 많은 큐비트가 필요한 양자 오류 보정 기술은 잠시 뒤로 미뤄둔 채 양자이득을 보이는 계산 수행을 목표로 양자컴퓨팅 기술 개발이 진행되고 있다.

현재 중간 규모인 50~100큐비트 수준의 오류가 있는 양자컴퓨팅 기술이 구현되어 있으며, 이를 NISQ(Noisy Intermediate-Scale Quantum)라고 한다. 실제로 연구자들은 구글과 중국과학기술대학교에서 보유한 NISQ 컴퓨터로 샘플링 문제를 다루어 양자 우월성 및 이점을 보이기도 하였다. 몇 가지 논란이 있기는 하지만 고전 컴퓨팅보다 양자컴퓨팅의 속도가 더 빠르다는 것을 명확히 확인한 것으로, 이를 구현한 일련의 실험들은 양자컴퓨팅의 이정표라 볼 수 있다.

큐비트는 물리적으로 구현하는 방식에 따라 크게 여섯 종류의 플랫폼으로 분류할 수 있으며, 어느 플랫폼이 우월하다고 할 수 없을 정도로 각각의 특성이 명확하고 장단점이 혼재한다. 세계적으로 초전도체, 이온포획 및 광자 등의 순서로 연구개발 투자가 진행되고 있다. 아직 개발 초기단계이며, 이러한 투자 경향은 한동안 지속될 전망이다.

현재 가장 주목받는 방식은 초전도 큐비트 방식이다. 기존 반도체 공정을 이용해 제작하여 확장성이 우수하며, 게이트 조작에 필요한 시간이 짧다는 장점이 있어 구글, IBM 등 선도 기업에서 채택한 방식이다. 클라우드 컴퓨팅 방식으로 먼저 민간에 서비스를 제공하는 등 여러 후보 플랫폼 중 가장 앞서 있다는 평가를 받고 있다. 세계 최초로 양자 우월성을 입증한 구글은 현재 자체 오류정정 기술을 구현하여 고도화하고 있으며, 2029년까지 양자 오류내성 100만 큐비트를 가지는 범용 양자 컴퓨터를 개발한다는 목표다.

IBM은 지난해 433큐비트 양자프로세서 '오스프리(Osprey)'를 공개하였고, 2025년까지 4,000 큐비트 이상급 단일 양자프로세서 개발한다는 계획을 발표하였다. 올해에는 1,121큐비트 양자프로세서 '콘도르(Condor)'와 함께 133큐비트 양자프로세서 '헤론(Heron)'을 함께 선보일 예정이다. 헤론의 경우 모듈형 방식이라 단일 양자컴퓨팅 칩이 아닌 복수 프로세서를 연결할 수 있어 대규모 양자컴퓨터를 분산된 형태로 구축할 수 있다는 장점이 있다. 이러한 분산컴퓨팅 시스템은 양자컴퓨팅 구축 규모와 비용을 획기적으로 개선할 것으로 기대된다.

그 외 다양한 나라에서 초전도체 방식을 연구하고 있다. 중국과학기술대학교의 66큐비트 '조충지' 및 바이두의 10큐비트 '첸시'가 지난해 공개되었으며, 독일 율리히연구소는 오류정정이 가능한 17큐비트 양자프로세서를 발표하였다. 일본의 경우, 후지쯔-리켄연구소가 자체 개발한 64큐비트 양자프로세서의 민간기업 서비스를 올해 4월 출시할 예정이다.

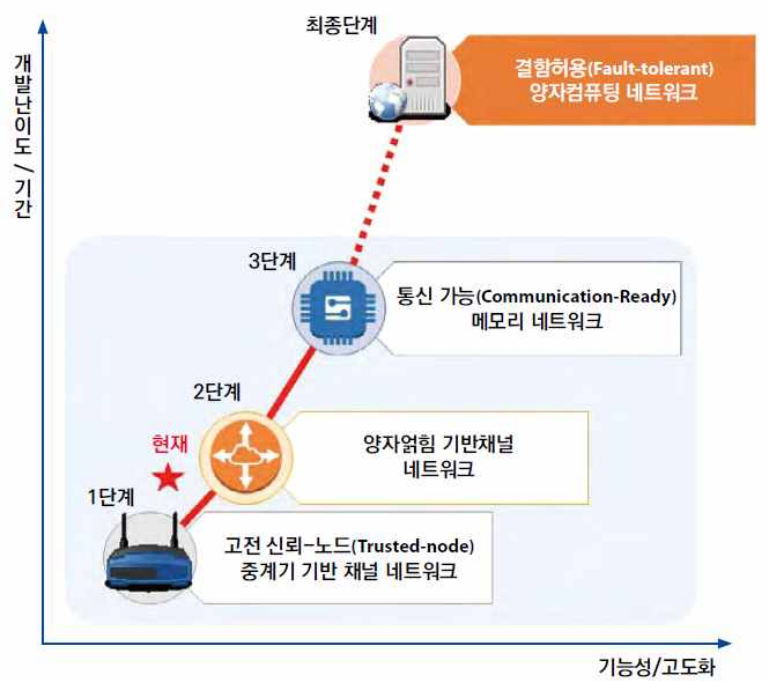
미국 메릴랜드주 소재 스타트업 아이온큐(IonQ)는 이온포획 방식의 양자컴퓨팅 회사로, 초전도체 방식과 마찬가지로 클라우드 서비스를 제공하고 있다. 이온포획은 상온 동작이 가능하고 높은 연결성과 낮은 게이트 에러율을 가져 효율적 연산이 가능하나, 최대 100큐비트까지만 구현 가능하다는 확장성의 한계가 있어 모듈 방식으로 확장을 가능하게 하는 연구개발도 진행되고 있다. 새로운 벤치마크 알고리즘큐비트(AQ)를 제안했으며, 현재 22개의 AQ 수준을 2028년까지 1,024개 수준으로 높이는 것을 목표로 하고 있다. 그 외에도 미국 Qunatinuum은 10큐비트 양자프로세서(System Model H1)를 상용화하였고, 유럽 Alpine Quantum Technologies와 인스부르크 대학은 24개 이온얽힘 상태 구현 및 양자 컴퓨터 개발 연구를 하고 있다.

다양한 플랫폼별로 양자컴퓨팅을 구현하기 위한 연구 및 투자가 활발히 진행 중인 만큼 시장

도 지속 성장할 전망이다. 양자컴퓨팅 시장은 2022년 5억 8,300만 달러에서 2030년 90억 달러 이상으로 확대될 전망이다. 향후 기술개발 성과에 따라 주도적인 플랫폼 방식이 가려질 것으로 예측된다.

2.2 양자암호통신

양자컴퓨팅의 정보 처리 단위로 큐비트가 채택되면 통신망을 이용하는 정보 단위 역시 큐비트가 되어, 기존의 비트를 이용하는 통신망은 큐비트의 특성을 전달할 수 없게 된다. 양자의 특성을 활용한 물리적 보안 통신 및 양자컴퓨터 등 양자 기기 간 연결을 위해서는 궁극적으로 결함허용 양자컴퓨팅 네트워크, 즉 양자인터넷이 실현되어야 한다. 현재 고전 신뢰노드 기반 네트워크 기술에 더해 양자암호키분배(QKD), 양자 중계기, 양자 메모리 및 양자 오류 보정 같은 고차원적인 기술이 추가로 필요한 상황이다. 이미 국외 유수의 연구기관 및 기업에서 양자인터넷을 목표로 기술을 개발하고 있다.



참고: 양자인터넷 핵심원천기술개발사업 기획 보고서

[그림] 양자 네트워크 발전 방향

가장 먼저 실용화된 기술은 기존 디지털 암호체계와 통신망을 대체할 목적의 QKD를 활용하는 양자암호통신이다. 컴퓨터가 큰 수의 소인수분해를 하는데 오랜 시간이 걸리는 점에 착안해 만든 암호체계인 공개키(RSA) 암호 체계는 짧은시간 내에 소인수분해가 가능한 양자컴퓨팅 기술로 무력화될 수 있다. 반면 양자 암호키를 사용하는 경우 통신 과정에서의 불법 도감청 및 중간 정보 탈취를 원천 차단할 수 있다. 하드웨어 기반의 보안 기술 방식으로, 장거리 통신이 어렵고 중간자 공격에 취약하다는 단점은 있다. 국내에서는 SK텔레콤과 KT가 QKD 연구에 집중하고 있다.

또한 소인수 분해 문제가 아닌 수학적 알고리즘을 활용하여 해독이 사실상 불가능한 양자내성암호(PQC) 방식도 있다. QKD와 달리 별도의 전용 하드웨어 장비가 필요없다는 장점이 있다. 국내에서는 LGU+가 PQC에 대한 연구를 집중추진 중이다. 이미 지난해 PQC가 결합된 CCTV를 개발하였고, 올해 1월 PQC를 적용한 커넥티드카 보안 기술도 선보였다.

2016년 세계 최초로 상용 LET망 유선 구간에 양자암호통신 기술을 적용한 SK텔레콤은 QKD 칩을 개발한 스위스의 IDQuantique를 인수하고, 2020년 세계 최초로 양자난수생성기(QRNG)를 장착한 단말기도 출시하였다. 지난해에는 SK브로드밴드와 함께 30여 개의 양자중계기로 연결된 800km 규모의 전국 양자암호망을 구성하고 PQC 기술도 상용화했다.

이와이엘은 2021년 세계 최초로 양자난수를 활용한 도청방지 솔루션을 상용화하였고, 지난해 삼성SDS는 미국 NIST 산하 사이버보안센터가 주도하는 PQC 전환 프로젝트에 아시아 기업최초로 참여하여 양자암호기술을 연구하고 있다. 또한 국내 최장거리인 1km 무선 양자암호통신 시연에 성공한 KT는 올해 전송 거리를 10km로 늘릴 계획이다. 이러한 실증 기술들은 향후 양자전송과 양자 중계기 기반의 양자 노드로 이루어진 양자 네트워크 구축에 기여할 것으로 기대된다.

3. 양자기술 정부연구개발 추진현황

3.1 양자컴퓨팅 인프라구축사업

우리나라는 향후 5년을 양자생태계의 매우 중요한 분기점으로 생각하고, 신속하게 양자컴퓨팅 시스템을 자체 구축하기 위한 투자를 시작하였다. 2022년부터 4년간 490억원을 들여 초전도 방식의 50큐비트 양자컴퓨터를 한국표준과학연구원(KRISS) 주도로 구축하고 있으며, 성공할 경우 미국과 중국에 이어 3번째로 양자우월성을 보일 수 있는 컴퓨팅 시스템을 보유하게 된다. 현재 우리나라는 연구실에서 초전도 8큐비트 칩을 시연한 수준이다.

이 사업 1단계인 2024년까지는 20큐비트 양자컴퓨터 구축과 클라우드 서비스 시연을, 2단계인 2026년 말까지는 50큐비트 국내 서비스 제공을 추진할 계획이다. 연구개발에는 ETRI, UNIST, KAIST, 서울대 등 연구기관과 34개 양자컴퓨팅 활용기업·투자사 등이 함께 한다. 양자소자 설계 및 제어, 제작 및 소프트웨어 기술 등을 확보하고 오류 분석용 에뮬레이터 개발까지 진행할 계획이다. 또한 해외 협력을 위한 초전도체 양자컴퓨팅 국제공동연구센터를 설치하고, 미국 NIST, MIT, 버클리대 등과의 인력 교류도 추진한다.

도전적이고 압축적인 연구개발 사업을 통해 양자컴퓨팅 시스템이 적기에 구축된다면, 국내 양자기술 연구 역량은 획기적으로 제고될 것이다. 연구소, 대학, 산업계의 연구 용도뿐만 아니라 교육 훈련용으로도 쓰여 사용자 교육 기회를 확대할 수 있다. 재료과학, 의학, 금융, 보안 등 다양한 분야에서 선도적 문제해결 응용 사례를 발굴할 수 있다는 점에서도 의미가 있다. 국내 하드웨어 개발·운용 협력 경험으로 비즈니스 모델을 발굴하고 민관 파트너십 활동을 통해 서비스 산업 창출을 촉진할 것으로도 기대된다.

[그림] 양자컴퓨팅 인프라 구축 추진체계

3.2 양자인터넷 핵심원천기술개발 사업

동 사업은 ETRI(총괄)과 KIST(허브)를 중심으로 양자인터넷 구현을 위한 '유무선 양자중계기초기 모델 개발'과 '양자메모리 원천기술 확보'를 목표로 추진 중이다. 2022년부터 4년간 456억원을 투입한다. 우선 2026년까지 현존 네트워크로는 불가능한 양자정보 전달용 양자얽힘 네트워크를 개발하고 시제품을 실증할 예정이다. 산업계(KT, SKT, 우리넷 등)와 학계(POSTECH, GIST, KAIST, 고려대 등)가 참여하며, 미국 NIST, 하버드대 등과의 협업도 추진한다. 초기 단계부터 산·학·연 역량을 결집해 양자인터넷을 실증하고 수요기업이 활용할 수 있는 체계가 구축된 것이다.

연구진은 100km 이상 장거리 양자얽힘 분배용 양자 중계기 개발을 목표로 20km 이상 다중노드간 양자얽힘 분배를 구현하고, 30km 실환경 포함 양자중계기 기반 얽힘 분배 및 세계 최초 50km 이상 장거리 양자원격전송 시연을 연구하고 있다. 이후 2031년까지 양자 중계기 실용화와 필드 테스트를 진행하여 Quantum ARPAnet을 구축하고 이후엔 양자중계기의 양자정보 저장 및 다중연결 구현을 통해 최종 양자인터넷 시범서비스를 2036년까지 제공한다는 청사진도 계획되어 있다. 이를 통해 구현된 양자암호통신망은 보안성이 강화된 미래 국가 기반 시설로 활용될 것이며, 양자중계기 핵심부품 국산화와 산업경쟁력 강화에 기여할 것이다.

4. 맺음말

양자기술 개발을 위한 각국의 기술·산업 동향을 살펴보면 양자기술 활용의 현실화가 실제로 이루어지는 단계에 있는 듯하다. 현재 양자 오류보정에 관한 문제를 극복할 수 없다는 근거도 몇몇 존재하는 것은 사실이지만, 세계적으로 엄청난 연구비를 투자하여 기술 개발에 박차를 가하고 있음은 무시할 수 없는 추세이다. 당연히 양자컴퓨팅의 우월성 도달이나 양자 중계기의 개발 이후에도 이상적인 양자 시스템 개발에는 매우 난해하고 복합한 문제가 남아 있을 것이다.

그럼에도 50큐비트 양자컴퓨팅 수준은 기존의 컴퓨팅과 상호보완하는 형태로 활용 가치가 충분하며, QKD 및 QRNG 등을 통해 이미 양자암호통신이 일부분이나마 실생활에 적용되고 있음을 볼 때, 양자 혁명 시대에 이미 진입하였다는 평가도 충분히 가능하다.
정부의 수많은 전략을 기반으로 연구개발을 시급히 추진해 우리나라 양자산업 생태계를 하루빨리 조성해야 한다. 이를 위해서는 인력 육성에 힘써야 하며, 산업계의 연구개발 협업을 유도하기 위해 구체적인 유인책 등의 동기부여도 필요하다. 양자기술은 미중 기술 패권의 핵심 기술 중 하나이나, 아직 국제협력의 기회가 남아 있어 추격할 여지가 남아 있다. 핵심 장비·부품 수급 문제 및 연구인력 부족 등 어려운 연구 환경 속에서도 2030년대 양자 기술 4대 강국에 진입할 수 있도록 최선을 다해야 할 것이다.

※ 본 연구는 2023년 과학기술정보통신부의 지원을 받아 수행됨[글로벌 기술패권 경쟁 대응 기술주권 주요 이슈 심층분석 및 전략수립 방법론 고도화 연구]

[주요 용어 풀이]
- 양자우월성(Quantum Supremacy): 양자 연산을 통하여 어떠한 고전 컴퓨터로도 실현 불가능한 연산 능력에 도달한 것. 여러 이유로 현재는 양자이점(Quantum Advantage) 표현을 많이 씀
- 알고리즘큐비트(Algorithmic Qubits): 양자컴퓨팅회사 IonQ만의 자체적인 양자컴퓨터 성능 지표
- 양자암호키분배(Quantum Key Distribution): 송신자-수신자 간 광케이블을 통해 비밀키를 분배·관리하여 제삼자가 암호를 해독할 수 없는 기술
- 양자난수생성기(Quantum Random Number Generator): 패턴분석이 근본적으로 불가능한 '순수 난수'를 발생
- 양자내성암호(Post-Quantum Cryptography): 양자컴퓨터의 위협에 대응하는 비대칭 키 암호
- 양자원격전송(Quantum Teleportation): 물질이 직접 이동하지 않으면서 물질의 상태만을 원거리로 전달

[참고문헌]
[1] McKinsey, Quantum computing funding remains strong, but talent gap raises concern, 2022.06.15
[2] 과학기술정보통신부 (2021),「양자기술 연구개발 투자전략(안),」2021.04.30.
[3] 고윤미 외 (2022),「새정부 과학기술 관련 국정과제 주요 내용 및 시사점,」KISTEP 브리프 18호, 2022.06.09.
[4] 과학기술정보통신부 (2022),「디지털 기술혁신 및 확산전략,」2022.06.28.
[5] 과학기술정보통신부 (2022),「국가전략기술 육성 방안(안),」2022.10.28.
[6] 유형정 (2022),「양자정보기술,」KISTEP 브리프 21호, 2022.07.05.
[7] https://www.technologyreview.kr/whats-next-for-quantum-computing/
[8] Rodney Van Meter (2014),「Quantum Networking,」Wiley-ISTE
[9] 과기정통부 (2021),「양자컴퓨팅 인프라구축사업 기획 보고서,」2021.05.

[10] 과기정통부 (2021),「양자인터넷 핵심원천기술개발사업 기획 보고서,」2021.05.

※ 출처: TTA 저널 제205호