ISSN 2635-618X

2019-07(통권 제265호)

Korea Institute of S&T Evaluation and Planning

KISTEP Issue Paper

빛의 속도로 계산하는 꿈의 컴퓨터, 양자컴퓨터

정지형 · 최병철

KISTEP

Korea Institute of S&T Evaluation and Planning

KISTEP 한국과학기술기획평가원
Korea Institute of S&T Evaluation and Planning

빛의 속도로 계산하는 꿈의 컴퓨터, 양자컴퓨터

Quantum Computer,

the Dream Computer that Calculates at the Speed of Light

정지형 · 최병철

Ji Hyong CHUNG · Byoung Chul CHOI

I. 양자컴퓨터에 대한 이해

II. 양자컴퓨터 기술개발 이슈와 동향

III. 국내외 양자컴퓨터 정책 동향

IV. 양자컴퓨터 기술개발 활성화를 위한 정책 제언

[참고문헌]

I. What is Quantum Computing?

II. New Technologies and Development Trends on Quantum Computers

III. Quantum Computer Policy in Major Countries

IV. Policy Suggestions for R&D on Quantum Computer

[References]

KISTEP 한국과학기술기획평가원
Korea Institute of S&T Evaluation and Planning

요 약

양자컴퓨터에 대한 이해

- 양자컴퓨터는 중첩(superposition), 얽힘(entanglement) 등 양자의 고유한 물리학적 특성을 이용하여, 다수의 정보를 동시 처리할 수 있는 새로운 개념의 컴퓨터
- 현대 반도체 칩의 미세회로에서 발생하는 누설전류로 인한 고전컴퓨터 성능 한계 돌파를 위한 대안으로 양자컴퓨터 필요성이 대두
- 양자컴퓨터는 양자적 정보 단위인 양자비트 또는 큐비트(qubit)를 정보처리의 기본단위로 하는 양자병렬처리를 통해 정보처리 및 연산 속도가 지수 함수적으로 증가하여 빠른 속도로 문제 해결이 가능

시장 및 기술 동향

- 양자컴퓨터는 최적경로탐색, 소인수분해, 대량 데이터 탐색 등 복잡한 계산과 대량 데이터 처리에 강점이 있어 금융, 화학, 제약 등 다양한 산업 분야에 혁신을 가져올 것으로 기대
- 세계 양자컴퓨팅 시장은 2018년 16억 3,000만 달러에서 2023년 64억 1,000만 달러로 연평균 31.5% 성장할 것으로 전망
- 주요국과 거대 ICT 기업이 경쟁적으로 양자컴퓨터를 개발 중이지만 양자컴퓨터의 실제 구현은 큐비트의 중첩 및 얽힘 제어, 오류 정정 등 양자역학적 난제로 인해 쉽지 않은 상황
- 2018년 초 구글, IBM, 인텔 등이 각각 수십 큐비트의 양자 프로세서들을 경쟁적으로 공개하면서 양자게이트 기반 양자컴퓨터 구현에 대한 긍정적 기대감이 형성
- 주요국가들과 기업들의 양자컴퓨터 기술개발 방향이 큐비트 구현 개수 증가에서 최근 동작안정성, 오류정정 등의 부문으로 변화되고 있는 상황
- 아날로그 양자컴퓨터의 일종으로서 최적경로탐색에 강점을 가진 양자어닐러는 최근 2000큐비트 이상의 어닐링 칩이 개발된 상태이지만 실제 기능에는 개선 여지가 남은 상황

주요국의 양자컴퓨터 관련 정책

- 미국, EU, 중국 등 주요국들은 기초과학부터 응용기술까지 포함한 다양한 양자컴퓨터 관련 과학기술 분야에 정책적 지원을 제공 중
- 미국은 2009년 「국가양자정보과학비전」 발표 후 정보기관 중심의 기술 개발을 추진해왔으며, 2018년 9월에는 양자컴퓨터 부문의 기술우위 유지를 위한 「양자정보과학 국가전략」을 발표
- 미국 연방상원은 2018년 12월, 향후 5년간 최대 12억 달러 예산을 양자컴퓨터를 포함한 양자정보과학기술에 투자하는 「국가양자주도법(National Quantum Initiative Act)」을 통과시켰음
- EU는 Quantum Flagship 프로그램을 통해 2018년부터 10년간 10억 유로를 양자기술 개발에 투자할 계획
- 국내에서는 전반적으로 취약한 생태계를 고려하여 기초체력 확충 및 연구 저변 확대에 주력하면서 양자통신을 중심으로 양자정보기술 정책이 수립되어 왔음
- 2019년 국내 양자정보통신 기술개발 관련 과학기술정보통신부의 예산 투자는 250억 원 수준으로 예상되며, 2019년 하반기까지 「양자정보통신 진흥 종합계획(가칭)」을 수립할 예정

결론 및 정책제언

- 양자컴퓨터는 새로운 ICT 패러다임을 만들어낼 기술로써 세계 최고 기술 선도국 미국도 원천기술을 개발하려 분투 중인 분야이므로 추격형 기술개발 전략이 적합하지 않은 분야
- 실리콘, 금속 등 다양한 재료를 이용해 안정적인 양자컴퓨터를 구현하는 것은 세계적으로 기초 연구 단계인 만큼 국내 연구진의 과감한 도전과 장기적 안목에서의 투자 필요
- 현재 양자컴퓨터는 안정성이 확보되지 않은 상황인 만큼 초전도체, 이온트랩 등과는 다른 방식의 큐비트 개발에 대한 도전적 투자가 필요
- 국내 출연연, 대학, 기업이 모두 접근 가능하며 국내외 인재와 지식을 모을 수 있는 양자컴퓨터 기술개발 허브의 확보가 필요

- 양자물리학, 나노공학, 전산학, 수학, 전자공학 등 다양한 기초과학과 공학 지식이 모이면서 혁신이 일어나야 하는 만큼 단기적 이해를 뛰어넘을 수 있는 국가 차원의 기술개발 허브 설립과 지원이 필요

※ 본 이슈페이퍼는 한국과학기술기획평가원의 공식 의견이 아닌 필자들의 견해임을 밝힙니다.

Abstract

What is Quantum Computing?

- A quantum computer is a new concept of computer that can process multiple pieces of information simultaneously by using quantum's unique physical characteristics such as superposition and entanglement.
- A quantum computer is needed as an alternative to overcome the performance limitations of classical computers due to leakage currents in microcircuits of modern semiconductor chips.
- Quantum computers can solve problems at high speed by exponentially increasing information processing and computation speed through quantum parallel processing using quantum bits or qubits as basic units of information processing.

Market and Technology Trends

- Quantum computers are expected to revolutionize various industries such as finance, chemistry, and pharmaceuticals because they have strengths in complex calculations and data processing such as optimal path search, prime factorization, and mass data search.
- The global quantum computing market is expected to grow to $ 6.4 billion in 2023 from $ 1.63 billion in 2018.
- Major countries and large ICT companies are developing quantum computers competitively, but the actual implementation of quantum computers is not easy due to quantum mechanical difficulties such as overlapping and entanglement control of qubits and error correction.

- As early as 2018, Google, IBM, and Intel unveiled quantum processors with 50~70 qubuits and positive expectations for quantum gate-based quantum computer implementations emerged.
- The direction of quantum computer technology development of major countries and companies is changing from the increase in the number of qubit implementations to the areas of operation stability and error correction.
- As an analog quantum computer, the quantum annealer, which has strength in optimizing the optimal path, has recently developed annealing chip of more than 2000 qubits, but there is still room for improvement in actual function.

Quantum Computer Policy in Major Countries

- Major countries such as the US, EU, and China are providing policy support to various quantum computer related science and technology fields, from basic science to applied technology.
- Since the announcement of "A Federal Vision for Quantum Information Science" in 2009, the United States has been promoting technology development centered on information agencies, and in September 2018, announced the National Strategy for Quantum Information Science to maintain technological superiority in the quantum computer sector.
- In December 2018, the US Senate passed "the National Quantum Initiative Act (NQI)", which invests up to $ 1.2 billion in quantum information science and technology, including quantum computers, over the next five years.
- EU plans to invest € 1 billion in quantum technology development over the next 10 years through 2018 through the Quantum Flagship program.
- In Korea, quantum information technology policies have been established around quantum communication, focusing on expanding basic strength and expanding research base in consideration of the weak ecosystem.

- The budget investment of the Ministry of Science and ICT for the development of domestic quantum information and communication technology is expected to reach 25 billion won in 2019, and the quantum information and communication promotion plan (tentative name) will be established by the second half of 2019.

Conclusion and Policy Suggestions

- Quantum computer is a technology to create a new ICT paradigm, and the United States, the world's best nation, is struggling to develop original technology.
- As quantum computers are still not stable in the operation, we might need to invest in new qubit implementation methodologies, which could be different from superconductors and ion traps.
- Implementation of stable quantum computer using various materials such as silicon and metal is the basic research stage in the world, so it is necessary for the domestic researchers' bold challenges and long-term investment.
- It is necessary to establish quantum computer technology development hub that can be accessed by domestic actors, universities, and companies, and attracts domestic and international talent and knowledge.
- As various knowledge of basic science and engineering such as quantum physics, nanotechnology, computer science, mathematics, and electronic engineering are gathered and innovation must take place, it is necessary to establish and support a national hub for the quantum computer development that can surpass short-term understanding.

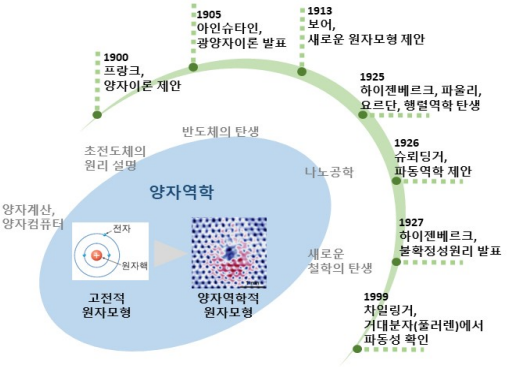
Ⅰ 양자컴퓨터에 대한 이해

1. 양자의 특성과 양자컴퓨터의 개념

- 양자컴퓨터는 중첩(superposition), 얽힘(entanglement) 등 양자의 고유한 물리학적 특성을 이용하여, 다수의 정보를 동시 처리할 수 있는 새로운 개념의 컴퓨터

  - 양자컴퓨터는 양자적 정보 단위인 양자비트 또는 큐비트(qubit)를 정보처리의 기본단위로 하는 양자병렬처리를 통해 고전컴퓨터* 대비 정보 처리 및 연산 속도가 지수 함수적으로 증가하여 비약적으로 빠른 속도로 문제 해결이 가능

  * 현재 널리 사용하고 있는 PC, 슈퍼컴퓨터 등의 bit 기반 컴퓨터

양자 (Quantum)	▪ 더 이상 작게 나눌 수 없는 에너지의 최소 단위를 가진 입자 상태	[양자역학의 역사와 영향력] 
광자 (Photon)	▪ 입자와 파동의 성질을 갖는 빛의 양자상태가 광자(光子, Photon)임	
양자의 특징	▪ (중첩성) “0” 또는 “1”의 상태 값을 가지면서 중첩상태(“0”이면서 동시에 “1”인 상태)의 선형결합도 형성할 수 있는 성질 ▪ (불확정성) 서로 교환가능하지 않은 물리량(예; 위치와 운동량)을 함께 측정할 때 두 물리량을 동시에 측정할 수 없는 성질 ▪ (비가역성) 양자 상태 측정은 시간에 대해서 되돌릴 수 없는 과정으로 관측 후에는 이전 상태로의 복원이 불가능한 성질 ▪ (얽힘) 거리에 무관하게 두 개의 양자 쌍에 대한 특수 상관관계가 존재하여 무한대의 원격지에서도 하나의 입자 상태 값이 변경되면, 다른 쪽의 양자 상태 값도 즉각적으로 변동하는 성질	

[자료] 미래창조과학부(2016), 과학기술정보통신부·정보통신기획평가원(2018) 재구성

[그림 1] 양자의 기본 개념과 특징

- 1981년 IBM과 MIT가 개최한 제1회 컴퓨터 물리학 콘퍼런스 기조연설에서 리처드 파인만이 양자현상을 이용한 컴퓨팅이라는 개념을 처음으로 제시

※ 파인만의 개념은 1985년 영국 물리학자 데이비드 도이치 교수의 양자 알고리즘으로 구동 가능성이 검증되었고, 1994년 MIT 수학과 교수 피터 쇼어 교수가 큰 수의 소인수분해와 이산 로그 문제를 빠른 시간에 해결할 수 있는 양자를 이용한 암호해독 알고리즘을 발표하면서 양자컴퓨팅이 본격적으로 주목받기 시작함

현대 반도체 칩의 미세회로에서 발생하는 누설전류로 인한 고전컴퓨터의 성능 한계 돌파를 위한 대안으로써 양자컴퓨터가 필요

- 컴퓨터에 사용되는 반도체 칩의 미세한 회로(현재 컴퓨터에 사용되는 반도체 칩 공정은 일반적으로 14나노미터로 머리카락 두께의 약 5700분의 1 수준에 불과)들에 전류가 흐르느냐, 흐르지 않느냐에 따라 0과 1이라는 신호를 내재하고, 이 신호들을 조합하여 연산을 실시

- 그런데, 반도체 칩 내 회로가 10나노미터 수준까지 축소되면 회로에 흐르는 전자들이 양자터널효과*를 경험하는 양자역학적 현상에 노출

* 양자터널효과는 입자가 자신의 에너지 준위보다 높은 장벽을 확률적으로 통과하는 양자역학적 현상으로서, 이로 인해 매우 얇은 회로에서는 전자들이 도선에서 새어나가는 현상이 발생하게 됨

- 현대의 반도체 기술로서는 미세회로 내 양자터널효과를 제어하기 불가능하기에 향후 고전컴퓨터 연산장치 고도화가 어려울 것으로 예상되며 이 문제를 해결하기 위해 필요한 기술 개념이 양자컴퓨터임

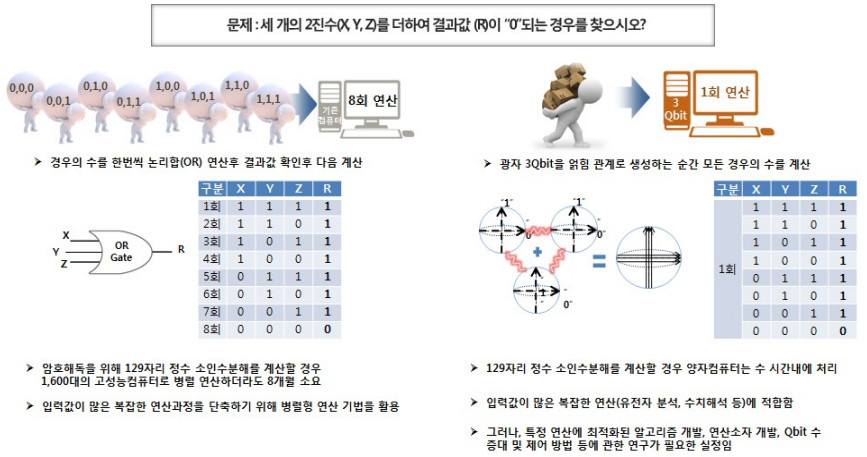
- 또한 양자컴퓨터는 슈퍼컴퓨터의 거대화와 막대한 전력소모의 한계를 극복 가능한 대안임

※ 현재 세계에서 가장 빠른 컴퓨터인 중국의 텐허 2호(Tianhe-2) 슈퍼컴퓨터는 축구장 절반 정도의 크기에 한 개 도시의 소비전력과 맞먹는 24MW의 전력을 소비(발전소 1개 분량)

고전컴퓨터는 한 번에 하나의 숫자에 대한 계산을 수행하기에 속도 향상에 제약이 존재하나, 양자컴퓨터는 중첩 특성을 이용해 대량·고속의 정보처리가 가능

- 고전컴퓨터는 0과 1 각각에 대해 한 번에 한 개 숫자씩 계산을 수행해야 하나, 양자컴퓨터는 중첩 상태를 이용할 수 있어 한 번의 프로세스로 0과 1에 대한 연산을 동시에 수행* 가능

* 양자 병렬성(quantum parallelism): 단 한 번에 모든 숫자의 연산을 수행할 수 있는 성질



[자료] 미래창조과학부(2016)

[그림 2] 양자컴퓨터의 계산 원리

- N비트짜리 양자컴퓨터는 2^N으로 병렬처리가 가능하여 5비트 양자컴퓨터는 32(2^5)개 CPU를 가진 고전컴퓨터처럼, 32비트 양자컴퓨터는 약 43억(2^{32})개 CPU를 가진 고전컴퓨터처럼 병렬처리가 가능

※ 고전컴퓨터는 1000비트 숫자를 소인수 분해 하는 데에 백만 년이 걸릴 수 있으나 양자컴퓨터는 1초~1일 정도에 계산할 수 있을 것으로 기대

[표 1] 고전컴퓨터(슈퍼컴퓨터)와 양자컴퓨터 비교

슈퍼컴퓨터(비트 기반 디지털 기술)	양자컴퓨터(양자기술)
▪ (계산능력 한계) 슈퍼컴퓨터는 현대암호 체계 분석 불가	▪ (동시 계산 처리) 초고속 대용량 연산을 통한 신속한 계산 가능
- 순서대로 반복적 계산: 3bit 고전컴퓨터의 경우 8회 	- 양자 특성을 이용해 동시에 계산: 3qubit 양자컴퓨터의 경우 1회
- 암호 해독(612자리 정수) : 백만 년 	- 암호 해독(612자리 정수): 수 분 이내
- 세계 1위 슈퍼컴퓨터의 전력 소모량: 세종시의 0.5배(15MW) 	- D-Wave 양자컴퓨터의 전력 소모량: 0.025MW(슈퍼컴퓨터의 1/600배)

[자료] 미래창조과학부(2016)

- 현재 쓰이고 있는 RSA 암호체계* 안정성은 고전컴퓨터가 큰 수를 소인수 분해하기 어렵다는 점에 의존하는데, 압도적인 소인수분해 능력을 가진 양자컴퓨터가 실용화된다면 RSA 암호체계가 붕괴될 것으로 예상됨

* 현재 공인인증서 등에 널리 활용되고 있는 공개키 암호체계

양자컴퓨터는 큐비트 구현방법, 연산회로 구현방식에 따라 크게 아날로그 방식과 디지털 방식으로 분류 가능

- 아날로그 방식 양자컴퓨터는 2011년 5월 캐나다의 D-Wave Systems가 상용화한 양자 어닐링 방식의 양자컴퓨터가 대표적이며 최적경로탐색 문제 해결에 강점을 가짐

- 디지털 방식인 양자 게이트 방식은 논리적 정보연산을 통해 다양한 알고리즘을 수행할 수 있어 범용 양자컴퓨터로서 기대를 모으고 있음

- 또한, 분자, 원자 수준에서 일어나는 양자물리화학적 동적변화를 시뮬레이션하기 위해 큐비트를 활용하는 양자시뮬레이터도 특별한 형태의 아날로그 양자컴퓨터라 할 수 있음

※ 이론적으로는 모든 화학, 생화학 반응을 온전하게 시뮬레이션할 수 있기 때문에 물리적 실험 없이 신약개발, 신물질 설계 등이 가능

양자정보처리의 기본단위로서 ‘큐비트’를 이용하는데 초전도체 내 전류, 전자스핀, 반도체 내 양자점, 이온 등 다양한 방식으로 큐비트를 구현할 수 있음

- ① 물질의 원자를 전기적 성질을 지닌 이온으로 만든 뒤 빛과 자기장으로 조절하는 '이온트랩', ② 반도체로 전자를 분리해 '스핀'이라는 양자역학적 성질로 큐비트를 만드는 '반도체 양자점', ③ 초전도체를 이용하는 '초전도 방식', ④ 다이아몬드 안에 일부 존재하는 공간을 이용해 전자나 원자의 정보를 큐비트로 활용하는 '다이아몬드 방식' 등 크게 네 가지 방식이 활발히 연구되고 있음

- 한때는 이온트랩을 이용한 양자컴퓨터가 가장 앞서 개발되다가 최근에는 초전도소자를 이용한 양자컴퓨터가 더 앞서 나가고 있음

[표 2] 양자컴퓨터의 종류

종류	설명	주 사용 분야	작동환경	주요기관
Gate 방식 양자컴퓨터	큐빗에 대해 양자 로직 게이트 연산 적용을 통해 양자상태를 변경시킴으로써 양자계산을 수행하는 것으로 고전컴퓨터의 논리 게이트 적용으로 계산이 수행되는 것과 유사. 양자게이트는 X, Y, Z, S, T, H, CNOT 등이 있음. 연산방법은 회로모델, 1방향연산모델 등이 있고, 에러율 저하와 양자상태 유지시간 향상 연구 등이 중요	소인수분해 데이터 검색 행렬계산 추천알고리즘 양자게임 암호해독(예상) 인공지능(예상) 빅데이터(예상)	극저온 차폐환경 또는 저온/진공 저압환경	IBM 구글 Regetti IonQ Oxford 인스브룩대 인텔 MS
양자 시뮬레이터	다체(many body)문제 등 양자화학, 양자물리의 문제를 풀기 위해 큐빗으로 모델링하고 양자 연산을 통해 양자적 거동을 직접 수행함으로써 문제를 푸는 양자시스템	촉매 거동 해석 광합성 해석 원자핵 분석		하버드 IonQ
양자 어닐러	풀고자하는 문제를 큐빗에 의한 에너지의 분포로 표현하고 에너지 최소 상태를 양자 터널링 등의 방법으로 순식간에 찾아냄으로써 계산을 수행되는 컴퓨터. 여러 가지로 차선의 해법이 있어서 최선의 최적화 해법을 찾기 어려운 문제에 적용 시 효과를 발휘	물류 최적화 공정 최적화 투자포트폴리오	극저온 차폐환경	D-Wave 구글
디지털 어닐러	양자 어닐러와 같은 방법으로 표현된 에너지 분포에 대해 몬테카를로법 등 다른 방법으로 에너지 최소 상태를 찾아내는 방법. 양자적 방법은 아니지만 상온동작, 스케일업, 디지털컴퓨터와의 통합 등에서 유리한 점이 있음	상동	상온 고전컴퓨터 작동 환경	후지쯔
SW 시뮬레이터	게이트 방식 양자컴퓨터의 기능(큐빗의 중첩, 얽힘 등)을 PC, 클라우드, 슈퍼컴퓨터 등의 고전컴퓨터에 SW적으로 구현한 시뮬레이터. 50큐빗 정도 얽힘을 표현하더라도 140테라바이트의 메모리가 필요하므로 무한정 많은 큐빗을 표현할 수 없음	게이트 방식 양자컴퓨터와 동일	상온 고전컴퓨터 작동 환경	MS IBM Atos 알리바바

[자료] 박성수·송호영(2019)

2. 양자컴퓨터 시장 동향

■ 양자컴퓨터는 IBM, 구글, 인텔, 마이크로소프트와 같은 전통적 글로벌 ICT 기업들이 5년 내 상용화를 목표로 기술개발을 주도하면서 주도권 확보를 위한 경쟁이 치열

- IBM은 2016년 5월 일반 대중이 클라우드를 통해 IBM 양자 컴퓨터에 연결할 수 있게 해주는 세계 최초의 양자컴퓨팅 서비스(QCaaS)인 IBM 퀀텀 익스피리언스(Q Experience)를 발표했으며, 2019년 50큐비트급 양자컴퓨터를 상용화하겠다는 계획을 발표

※ IBM에 따르면, 2018년 5월 현재 8만 명의 IBM Q 익스피리언스 사용자가 400만 회 이상의 실험을 실시했으며, 관련 발표 연구 논문의 수는 65개 이상

- 구글은 2018년 3월 IBM을 넘어서는 72큐비트 양자 프로세서 'Bristlecone'을 공개했으며, 인텔도 2018년 1월 49큐비트 양자칩 'Tangle-Lake'를 발표

※ 구글에 따르면 브리슬콘은 단일 큐비트에서는 0.1%, 2큐비트의 게이트에서는 0.6%의 에러율을 기록

- 마이크로소프트는 아직 큐비트를 만들지 못하고 뒤처져 있지만, 큐비트를 개발하는 순간 바로 49큐비트급 머신을 만들 수 있는 수준(구글과 다른 접근법을 채택)이라는 평가를 받고 있으며, 양자컴퓨터용 프로그래밍 언어인 '큐샵(Q#)'을 공개하고 개발자 생태계를 구축 중

- 알리바바는 2018년 2월 클라우드에서 사용할 수 있는 11큐비트급 양자컴퓨터를 공개, 5년 이내에 미국을 넘어 세계 최고 양자컴퓨터 기업으로 거듭나겠다는 포부를 발표

- 이온큐(IonQ)*, 리게티(Rigetti)** 등과 같이 자금력과 기술력을 갖춘 스타트업도 존재

* 메릴랜드대 물리학 교수인 크리스토퍼 먼로와 듀크대 전자공학과 교수인 김정상이 2016년 공동설립했으며, 진공 중에 떠있는 이테르븀 원자를 큐비트로 이용하는 이온트랩 방식의 양자컴퓨터를 개발

** IBM 등에서 양자컴퓨터 개발에 관여했던 채드 리게티가 2013년 설립했으며, 최근 8큐빗을 지원하는 양자칩 개발에 성공했고 양자알고리즘 개발 인프라 '포레스트'를 공개했음

세계 양자컴퓨팅 시장은 2018년 16억 3,000만 달러에서 2023년 64억 1,000만 달러로 연평균 31.5% 성장할 전망(Mind Commerce, 2018)

- HW는 2018년 13억 400만 달러에서 2023년 37억 8,200만 달러로 23.7% 증가하고, SW는 2억 7,700만 달러에서 20억 5,100만 달러로 49.2%, 서비스는 4,900만 달러에서 5억 7,700만 달러로 63.8% 성장할 전망

[표 3] 세계 유형별 양자컴퓨팅 시장 전망

(단위: 백만 달러)

구분	2018	2019	2020	2021	2022	2023	CAGR
하드웨어	1,304	1,529	2,168	2,653	3,193	3,782	23.7%
소프트웨어	277	353	615	1,030	1,545	2,051	49.2%
서비스	49	79	147	277	412	577	63.8%
합계	1,630	1,961	2,930	3,960	5,150	6,410	31.5%

[자료] Mind Commerce(2018). 본 표의 저작권은 Mind Commerce Publishing에 있으며, Mind Commerce Publishing의 동의하에 사용되었습니다. 추후 이용 시 Mind Commerce Publishing에 문의하시기 바랍니다.

- 용도별로는 2023년 금융/보험 14억 2,900만 달러, 헬스케어/제약 11억 9,200만 달러, 정부/공공안전 10억 5,100만 달러, 국방/항공 6억 6,000만 달러, 교통/자동차 5억 7,000만 달러, 에너지/전력 5억 4,500만 달러, 화학 2억 8,800만 달러, 제조/공급망 2억 8,200만 달러, 통신/IT 1억 6,700만 달러, 사이버안보 7,700만 달러, 오락/미디어 7,700만 달러, 기타 7,100만 달러 순으로 전망

[표 4] 세계 용도별 양자컴퓨팅 시장 전망

(단위: 백만 달러)

구 분	2018	2019	2020	2021	2022	2023	CAGR
헬스케어/제약	339	404	592	780	979	1192	28.6%
금융/보험	293	367	571	840	1133	1429	37.3%
정부/공공안전	228	282	437	618	829	1051	35.7%
국방/항공	205	243	346	436	546	660	26.3%
에너지/전력	129	157	240	329	433	545	33.4%
교통/자동차	112	137	217	309	438	570	38.4%
화학	88	102	147	190	237	288	26.8%
통신/IT	77	82	111	115	139	167	16.8%
제조/공급망	62	76	117	166	221	282	35.4%
사이버안보	36	39	53	59	67	77	16.5%
오락/미디어	28	33	47	59	67	77	22.7%
기 타	33	37	53	59	62	71	16.7%
합계	1,630	1,961	2,930	3,960	5,150	6,410	31.5%

[자료] Mind Commerce(2018). 본 표의 저작권은 Mind Commerce Publishing에 있으며, Mind Commerce Publishing의 동의하에 사용되었습니다. 추후 이용 시 Mind Commerce Publishing에 문의하시기 바랍니다.

■ 양자컴퓨터의 활용 용도는 무궁무진하여 인공지능 분야는 물론, 금융, 화학, 제약 등 모든 산업분야에 혁신을 가져올 것으로 기대

- 양자컴퓨터는 복잡하면서 빠른 계산이 필요한 산업분야에서 유용하게 쓰일 수 있음

※ 양자컴퓨터는 고전컴퓨터가 약점을 가진 최적경로탐색 기반 최적화, 소인수분해, 대량 데이터 탐색 등에 있어서 강점을 가진 것으로 평가됨

- 투자 포트폴리오 설계, 물류 효율 개선 등 복잡한 계산이 대량으로 수행되어야 하는 산업분야에서 양자컴퓨터의 유용성이 확인될 것으로 예상됨

- 인공지능 등을 위한 데이터 계산량이 급증하면서 고전컴퓨터 대비 월등한 연산속도를 가진 양자컴퓨터를 활용하려는 시도가 증가

※ 가트너(Gartner) 하이프 사이클에 따르면 양자정보통신은 혁신 태동기를 지나 시장의 기대가 확대되는 시기로 진입이 임박(Gartner, 2018)

- 양자컴퓨터의 범용화단계까지는 상당한 시일이 소요되겠지만 기존 기술로 풀기 어려운 시뮬레이션, 금융, 화학, 의료, IT, 물류, 제약, 자동차, 항공우주 등에 산업 전반에 다양하게 적용되어 기술적 진보를 이끌어 갈 전망

[표 5] 양자컴퓨터 활용이 기대되는 분야

분야	응용 예	사례	분야	응용 예	사례
금융	• 포트폴리오 최적화 • 리스크 관리 • 옵션·가격 결정	• 2016년 5월, D-Wave Systems와 1Qbit이 “Quantum for Quants” 설립	물류	• 비행기, 선박, 트럭 등의 물류 최적화	• PLC와 Manchester Met. 대학의 물류 알고리즘 공동 개발
화학	• 분자 설계 최적화 • 화학 반응의 양자역학적 시뮬레이션 • 전지와 촉매의 최적화	• IonQ의 화학시뮬레이션 SW 개발 • MS의 기초 연구 • ETH, Harvard 대학 등의 연구	제약	• 단백질의 3차원 구조 최적화/분석 (알츠하이머병 등의 특효약 개발)	• Stanford 대학의 “Folding@home” 프로젝트 • Harvard 대학/D-Wave Systems의 단백질 분석 실험
의료	• 암 치료용 약물 발견/최적복용량 산출 • 개인 맞춤형 의료의 고속화	• Stanford 대학, Texas 대학에서 연구	자동차	• 도시 교통 서비스 최적화	• Volkswagen과 Google의 공동 개발 • Volkswagen의 주문형 이동 서비스를 위한 알고리즘 개발
IT	• 머신 러닝을 위한 고속 클러스터링 • 이미지 인식 고속 학습	• Google/D-Wave Systems의 이미지 인식 정확도 향상 • (중) USTC, NMR 기술 이용 4 큐비트 양자 프로세서 개발	항공우주	• 유체 역학적으로 최적화된 기체 설계 • 비행 제어 시스템의 버그 잡기 최적화	• NASA의 비행체 날개 설계 최적화 • Lockheed Martin과 Airbus의 제어 시스템 버그 탐색 SW 개발 (6개월→6주)

[자료] Masayuki Minato(2018), 조성선(2018)에서 재인용

Ⅱ 양자컴퓨터 기술개발 이슈와 동향

■ 현재 양자컴퓨터 개발의 핵심 과제는 상관시간(Coherence Time)* 증가, 구현 큐비트 수 증가, 에러율 감소 등 양자역학적 특성에 기인한 기술적 난제의 극복임

* 양자가 안정된 상태를 유지하는 시간

- 양자컴퓨터의 기초 이론은 완성되었다고 할 수 있지만, 아직은 기술적, 공학적 측면의 문제로 양자 우월성*을 입증할 만한 정도의 제품이 제대로 구현되어 사용되고 있지는 못한 상황임

* 양자컴퓨터가 고전컴퓨터보다 우수한 성능을 가지는 것을 증명하는 것으로, 전문가들은 양자컴퓨터가 고전컴퓨터를 앞서는 기준으로 50큐비트 이상을 제시(50큐비트 양자컴퓨터는 2^{50}, 약 1126조 비트의 정보를 연산할 수 있는 수준으로 현재 최고 성능 슈퍼컴퓨터보다 뛰어난 수준)

- 최근 발표되는 50큐비트, 70큐비트급 양자컴퓨터들은 큐비트를 물리적으로 만들어 나열은 했지만, 실제 활용 가능한 계산장치를 구현했다고 보기는 어려워 상용화는 요원한 상황

※ 양자는 비트 수가 늘어날수록 다루기가 매우 어렵기 때문에 일반적으로 실용적이라고 할 수 있는 수백 비트급 양자컴퓨터는 향후 10년 이상이 걸릴 것으로 전망

- 양자는 어느 정도 작동하다가 불안정한 상태를 보이는 특성 때문에 불안정함을 줄이고 안정된 상태인 상관시간을 늘리는 것이 매우 중요

- 고전컴퓨터는 전류의 흐름을 통제하는 것만으로 기초 연산자인 비트를 제어할 수 있었지만, 양자역학적 현상을 일으키는 큐비트를 만들어서 제어하는 것은 매우 어려운 문제로, 현재는 초전도 등을 이용해야 제대로 된 제어가 가능한 정도

- 큐비트는 극단적으로 불안정하여 노이즈에 의해서 오류가 쉽게 일어나기 때문에 보통 초저온 및 밀폐된 구동 환경이 필요하며, 현재의 양자 프로세서는 단일 큐비트가 아닌 여러 비트를 조합해 오류에 대응

※ 큐비트는 미세한 온도 변화나 소음, 진동만으로도 에너지가 누출되어 연산에 실패하는 '결잃음(decoherence)'상태에 빠질 수 있는데, 큐비트 수가 증가할수록 큐비트를 '얽힘'상태로 유지하는 것이 어려워져, 단지 큐비트 개수를 넘어 양자컴퓨팅 시스템 전체 오류율이 충분히 낮아야 함

■ 양자게이트 기반 양자컴퓨터는 IBM 등의 노력으로 큐비트 수가 증가해왔으나 최근에는 큐비트 증가보다는 동작안정성, 오류정정 등에 집중하는 분위기

- 2018년 초 구글, IBM, 인텔 등이 각각 수십 큐비트의 양자 프로세서들을 경쟁적으로 공개하면서 양자게이트 기반 양자컴퓨터 구현에 대한 긍정적 기대감이 형성

※ 2018년 초반 인텔이 49큐비트 초전도 양자칩 탱글레이크(Tangle Lake)를, 구글은 72큐비트 양자칩 브리슬콘(Bristlecone)을, IBM은 50큐비트 양자칩을 각각 공개

- 거대 ICT 기업 중심의 큐비트 개수 증가 노력에도 불구하고 짧은 중첩·결맞음 유지 시간, 높은 빈도의 오류발생 등의 문제는 여전한 난제로 남아 있는 상황

- IBM은 'Q 시스템'이라는 20큐비트 양자컴퓨터 온라인 접속 서비스를 제공하고 있는데 연구자들이 양자정보처리 알고리즘을 시험해보는 용도로 사용 중

■ 양자게이트 기반 컴퓨터의 동작안정성 증가와 오류정정은 범용 양자컴퓨터 개발에 가장 중요한 이슈로 부각 되었으나, 뚜렷한 해법은 보이지 않고 있음

- 위스콘신 대학, 하버드 대학 등은 중성원자 기반 큐비트 기술을 개발 중인데 양자연산 중 오류발생가능성이 상대적으로 낮을 것이라는 기대를 모으고 있음

- 구글, 인텔, IBM 등 거대기업들도 오류발생가능성 감소, 오류정정 등의 기술에 집중하고 있는 것으로 알려져 있으나 주목할 만한 성과가 발표된 바는 없음

[표 6] 주요 기업 및 기관의 양자컴퓨터 큐비트 구현 수준

기업·기관	컴퓨팅 방식	큐비트 방식	큐비트 개수	큐비트 목표
인텔	양자게이트	초전도체	49	TBD
구글	양자게이트	초전도체	72	TBD
IBM	양자게이트	초전도체	50	TBD
Rigetti	양자게이트	초전도체	19	128
USTC (China)	양자게이트	초전도체	10	20
IonQ	양자게이트	이온트랩	11	79
IQOQI/Univ.Ulm/Univ.Innsbruck	양자게이트	이온트랩	20	TBD
NSFSTAQProject	양자게이트	이온트랩	N/A	≥64

기업·기관	컴퓨팅 방식	큐비트 방식	큐비트 개수	큐비트 목표
Intel	양자게이트	스핀	26	TBD
Silicon Quantum Computing	양자게이트	스핀	N/A	10
CEA-Leti/INAC/InstitutNéel	양자게이트	스핀	N/A	100
Univ.ofWisconsin	양자게이트	중성원자	49	TBD
Harvard/MIT	양자시뮬레이터	Rydberg Atoms	51	TBD
Univ.ofMaryland/NIST	양자시뮬레이터	이온트랩	53	TBD
D-Wave	어닐러	초전도체	2048	5000
iARPAQEOResearchProgram	어닐러	초전도체	N/A	100

[자료] Quantum Computing Report(2019).

■ 최적경로탐색 등 특수문제해결 능력으로 주목받았던 양자어닐러는 최근 2000큐비트 이상의 어닐링 칩이 개발된 상태이지만 실제 기능에는 의문이 남은 상황

- 캐나다 D-Wave 사는 2017년 2000큐비트급의 어닐링 머신 D-Wave 2000Q를 출시해 양자어닐러 부분에서 최고의 기술력을 과시

- 어닐링방식은 큐비트 간 물리적 연결을 제어함으로써 노드 간 최적 경로를 시뮬레이션하는데 2차원 칩 상에서 큐비트 간 연결 구현에 한계가 있다는 점이 최근 어닐링머신이 직면한 기술적 문제임

  - 1,000개 노드와 499,500개 엣지가 존재하는, 서로 완전히 연결된 노드 간의 경로최적화 문제를 해결하려면 1,000개 큐비트 각각이 999개의 다른 큐비트와 물리적으로 연결되어 있는 어닐링칩이 필요함

  - 하지만 현재의 어닐링칩은 1,000개 큐비트를 구현하더라도 각 큐비트에 연결용엣지를 수 개만 구현할 수 있다는 물리적 한계에 부딪힌 상황

- 큐비트 구현기술이 진화하면서 양자어닐러의 큐비트 간 연결확장 및 제어 문제도 함께 해결될 것으로 예측됨

■ 양자시뮬레이터는 미국 메릴랜드대학, 하버드대학 등이 대표적인 연구기관이며 수십 큐비트 수준의 시뮬레이터 개발에 성공한 상태임

- 2017년 11월 미국 메릴랜드대학교·국립표준기술연구소는 53큐비트 양자 시뮬레이터 개발을 선언

- 이테르븀(Yb) 이온으로 채워진 원자를 금으로 코팅, 전극에 가두는 방식으로 53큐비트 양자 시뮬레이터를 제작

- 2017년 미국 MIT와 하버드대학이 공동으로 발표한 51큐비트 양자 시뮬레이터는 루비듐을 활용

- 각 큐비트가 특정 중첩상태를 가지도록 조작하고 특정한 물리적 위치에 배열한 후에 큐비트 간 상호작용이 일어나게 유도함으로써 자연계의 양자물리화적 반응을 시뮬레이션

- 이론적으로 자연계 원자, 분자들의 상호작용을 흉내 낼 가능성이 있지만, 큐비트의 상태조작, 특정 위치 배열로 촉발되는 상호작용 초기 조건 등을 자유롭게 제어하기 위한 응용기술과 이론의 개발이 부족한 것이 현실

- 양자게이트 기반 범용 양자컴퓨터는 양자시뮬레이터를 대체할 가능성이 있어 양자시뮬레이터가 효율적인 컴퓨팅 방식인지에 대해서는 논란이 있을 수 있음

※ 고전컴퓨터의 발전 과정에서도 아날로그 컴퓨터 구현에 대한 노력이 있었지만 디지털 컴퓨터의 지수적 성능 향상 때문에 아날로그 컴퓨터는 도태되었음

Ⅲ 국내외 양자컴퓨터 정책 동향

1. 주요국 양자컴퓨터 정책 동향

- 미국, EU, 중국 등 주요국들은 기초과학부터 응용기술까지 포함한 다양한 양자컴퓨터 관련 과학기술 분야에 정책적 지원을 제공 중

- 미국은 2009년 「국가양자정보과학비전」 발표 후 정보기관 중심의 기술개발을 추진해왔으며, 2018년 9월에는 양자컴퓨터 부문의 기술우위 유지를 위한 「양자정보과학 국가전략」 을 발표

  - 2009년 「국가양자정보과학비전」 발표 후 다양한 정보기관, 국방부, 연구소를 중심으로 양자통신, 양자컴퓨팅 기술개발을 추진

  - 중국 등의 양자정보 역량이 강화되자 트럼프 정부는 미국의 기술우위 유지를 위해 2018년 9월 인력 양성, 산학연 협력, 주요 인프라 구축 등을 담은 「양자정보과학 국가전략」 을 발표

  - 「양자정보과학 국가전략」 핵심은 정부지원 확대를 통해 양자정보과학 분야 신기술개발을 지원하고, 기술적 난제 해결 연구에 예산 우선순위를 두는 것

  - 또한 연방상원은 2018년 12월, 향후 5년간 최대 12억 달러 예산을 양자컴퓨터를 포함한 양자정보과학기술에 투자하는 「국가양자주도법(National Quantum Initiative Act)」 을 통과시켰음

[표 7] 미국 국가양자주도 법안 관련 주요투자 계획

기 관	주요 역할	연간 예산
양자 컨소시엄 (NIST)	- 미국 양자산업 발전을 위해 필요한 척도, 표준, 사이버 보안 등을 파악 - 현재 연구 수준과 개선 부문을 평가 및 제언	8,000만 달러
범학제 양자연구 교육 센터(NSF)	- 양자과학에 대한 기초연구 및 교육 지원금 제공 - 교과과목 개발 및 인력 개발 활동 지원금 제공	센터당 매년 1,000만 달러
국립 양자정보과학 연구 센터(DOE)	- 양자정보과학 기초연구 수행 - 국립연구소, 대학, 연구센터 등이 협력해 센터 유치 가능. 에너지부(DOE)와의 협력을 통해 연구 지원	센터당 매년 2,500만 달러

[자료] 한국과학기술기획평가원(2018)

■ EU는 「Quantum Flagship 프로그램」을 통해 2018년부터 10년간 10억 유로를 양자기술 개발에 투자할 계획

- 2016년 처음 발표된 Quantum Flagship은 슈퍼컴퓨터를 능가하는 양자컴퓨터 개발을 목적으로 한 EU 내 연구개발 프로그램
  - 예산은 양자컴퓨터, 양자통신, 양자시뮬레이션, 양자계측센싱 등의 분야로 구분되어 배정되고 예산 절반은 EU에서, 나머지 절반은 회원국들이 분담
- Quantum Flagship은 EU가 추진해온 「Graphene Flagship, Human Brain Flagship」 등에 이은 세 번째 FET(Future and Emerging Technology) 프로그램
  - 2018년 10월 EU는 「Quantum Flagship」을 통해 추진할 20개의 기술개발 사업을 선정했고 향후 3년간 1.32억 유로가 투자될 예정임
  - 20개 사업 분야와 예산 배분 비율을 살펴보면 양자계측센싱 26%, 양자통신 24%, 양자기초과학 20%, 양자컴퓨터 14%, 양자시뮬레이션 13%, 지원 3% 등의 비율로 예산 배분

■ 중국은 국가 차원에서 양자정보기술 개발에 대규모 투자를 진행 중이지만, 양자컴퓨터 부문보다는 양자통신 부문에 집중하는 상황

- 2006년 「국가중장기과학기술발전계획요강(2006~2020)」에서 미래 지속가능한 혁신과 경제사회발전을 위한 4대 중대 기초과학연구로 양자제어를 포함함
- 2012년 「양자제어 연구 국가중대과학기술 프로그램 12·5 전문규획」에서 양자 및 나노기술에 5년간 2,900억 원 투자계획을 세웠음
- 2016년 「13차 5개년 국가과학기술규획(2016~2020)」에서 2030년까지 국가전략을 구현하는 「6대 중대과기프로젝트」에 양자통신과 양자컴퓨터를 포함
- 양자과학기술 강국 도약을 위해 2017년부터 안이후성 허페이시에 세계 최대 규모의 양자정보과학국가연구소를 설립하기로 하고, 2018년부터 5년간 1천억 위안(약 17조 원) 투입을 선언

2. 국내 양자컴퓨터 정책 동향 및 기술개발 전략

■ 국내에서는 전반적으로 취약한 생태계를 고려하여 기초체력 확충 및 연구 저변 확대에 주력하면서 양자통신을 중심으로 양자정보기술 정책이 수립되어 왔음

- 2013년 3월 「국가초고성능컴퓨팅 활용 및 육성에 관한 법률」 제정으로 양자컴퓨팅 기술개발의 근거가 마련되었으나 이후 기술개발 전략과 정책은 양자암호통신 등을 중심으로 수립

- 2014년 12월 국제적 도·감청 사건을 계기로 미래창조과학부에서 「양자정보통신 중장기 추진전략」을 수립하여 정보통신전략위원회에 상정·보고

- 2016년 7월 양자통신, 양자컴퓨터 등의 기술개발을 위한 '양자정보통신 중장기 기술개발사업' 예비타당성 조사가 신청되었으나 2018년 말 통과 실패로 결론

  - 양자 수요기술을 조사해 양자암호통신, 양자소자 등 총 12개 핵심 과제를 도출해 2017년 8월 변경 기획(안)을 다시 제출했으나 이 역시 실패함

- 2019년 국내 양자정보통신 기술개발 관련 과학기술정보통신부의 예산 투자는 250억 원 수준으로 예상되며, 2019년 하반기까지 「(가칭)양자정보통신 진흥 종합계획」을 수립할 예정임

  - 과학기술정보통신부는 2019년 1월 「양자컴퓨팅 기술개발사업 추진계획」 을 마련, 향후 5년간(2019~2023) 양자컴퓨터 하드웨어 등 핵심원천기술개발과 양자컴퓨팅 신아키텍처, 양자알고리즘, 기반 소프트웨어 등에 총 445억 원의 투자계획을 발표

  - 양자암호통신·양자센서·양자컴퓨팅 기술을 개발한 국내 기업이 소자·부품·장비 성능이나 안정성, 상호호환성 등을 검증하는 개방형 양자 테스트베드도 구축할 계획

  - 아울러, 부족한 국내 양자컴퓨팅 연구 저변을 보완확대하기 위해 과학과 공학 분야 연구자 간의 융합연구를 촉진하고 글로벌 연구생태계와의 교류·협력 활성화도 지원할 계획

  - 「(가칭)양자정보통신 진흥 종합계획」은 산학연 전문가들로 작업반을 구성하여 수립 중이며, 양자정보통신의 다양한 연구개발 수요를 반영하고, 수요 예측에 기반을 둔 인력 양성, 초기단계에 있는 산업육성을 위한 지원 인프라와 제도적 지원방안 등을 담을 예정

[표 8] 양자컴퓨팅 기술개발사업 주요 내용

분 야	주요 내용
핵심원천기술 개발	양자컴퓨터, 양자시뮬레이터 등 양자컴퓨팅 HW 구현에 필요한 기초적 핵심기술 확보 추진 - (양자컴퓨팅 핵심기술 개발) 2023년까지 5큐비트급, 신뢰도 90% 이상 양자컴퓨팅 시스템 실증 - (양자시뮬레이터 개발) 경제·사회적 파급효과가 높은 분야의 문제해결에 특화한 양자시뮬레이터를 개발하고 효과를 실증
미래유망기술 개발	양자컴퓨팅 시스템 기술, 알고리즘 및 응용기술 등 차세대 양자컴퓨터 구현에 필요한 기반·응용 SW 연구 - (양자컴퓨팅 시스템기술 개발) 대규모 양자시스템에서 정보를 효율적으로 호출·처리·저장하기 위한 보조HW·아키텍쳐 및 기반 SW 기술 - (알고리즘 및 응용기술) 고전 시스템 대비 양자이점(quantum advantage)을 실현할 수 있는 다양한 양자알고리즘 연구 및 응용SW 개발
연구생태계 조성	부족한 국내 양자컴퓨팅 연구 기반을 보강하기 위한 교육·컨퍼런스 등의 운영과 글로벌 협력체계 구축 - 양자컴퓨팅 융합포럼 구성지원, 용어정립·기술체계 등 백서발간, 워크샵·세미나·교육프로그램 등을 통한 인력양성 지원 등

[자료] 과학기술정보통신부(2019)

■ 한편, 과학기술정보통신부는 2018년 「ICT R&D 기술로드맵 2023」을 통해 2040년까지의 양자컴퓨팅 분야 기술로드맵과 기술개발 전략을 발표

● 선도국과의 기술격차가 큰 양자컴퓨팅 분야는 전문연구기관 등 전략적 투자를 통하여 핵심인력과 전문기술 확보, 선도국 연구개발 방향 분석 등을 통해 선제적인 연구개발 계획 수립이 필요함을 제시

- 양자정보통신 기술수준은 최고기술 보유국인 미국의 73.0%로 4.0년의 기술격차를 보이며, 분야별로는 양자통신이 82.5%로 기술격차 2.7년으로 가장 적고, 양자 소자·부품 및 양자센서는 72.5%로 3.2년, 양자컴퓨터는 66.3%로 5.8년의 기술격차로 가장 열세

[표 9] 양자정보기술 분야 기술수준

대분류	소분류	기술수준		최고기술 보유국
		상대수준(%)	격차(년)	
양자통신	양자암호	83.3	2.0	미국
	양자네트워크 및 통신	80.0	3.0	
	양자통신 전체	82.5	2.7	
양자소자·부품 및 양자센서	양자정보통신 공통 소자부품	74.3	3.0	미국
	양자센서	68.3	3.5	
	양자소자·부품 및 양자센서 전체	72.5	3.2	
양자 컴퓨팅	큐빗 빌딩 블록 구현기술	63.3	6.5	미국
	큐빗 인터페이스 기술	63.3	6.5	
	양자컴퓨팅 시스템 기술	73.3	4.0	
	양자컴퓨팅 활용 기술	73.3	4.0	
	양자컴퓨팅 전체	66.3	5.8	
전체(합계)		73.0	4.0	미국

[자료] 정보통신기술진흥센터(2018)

- 양자컴퓨터는 부가가치가 높고 미래 핵심기술 가운데 하나지만 기술적·인적 자원 및 산업 기반이 열악하여, 기술개발, 표준, 인력 양성, 기반 조성, 제도·규제 개선 등의 전 분야에 걸쳐서 정부 주도적 추진계획을 수립

[표 10] 양자컴퓨팅 기술개발 전략

분야	기술개발 전략
양자 시뮬레이터	양자정보통신 연구에서 차지하는 비중은 매우 크지만, 국내 연구기반이 취약하여 추격형 연구 위주로 추진 - 중규모(10~100개) 양자시스템(이온트랩, 초전도체, 리드버그 원자 등)을 대상으로 시스템 복잡도 향상 기술개발 - 양자계 분석을 위한 소프트웨어, 개발편의성 향상을 위한 도구 개발 및 실험적 분석 기반 구축 추진
물리양자비트	기초적이고 공통된 핵심기술로 연구개발 확대를 통해 초기 단계에서 신속히 확보 - 범용 양자컴퓨팅을 목표로 확장성이 확보되고 모든 양자비트의 제어, 측정 및 얽힘이 가능한 소규모의 다중 양자비트 기반 연산소자 개발 - 양자비트 소자의 제작, 제어, 측정의 최적화를 통해 대규모 양자컴퓨팅 기술개발을 추구하는 제반 기술 확보

분야	기술개발 전략
논리양자비트	양자컴퓨터 구성 기본단위로 물리적 구현에 따라 기능적 한계가 결정되므로 다양한 방식의 논리 비트와 신뢰도 향상을 위한 오류정정 기술개발 추진 - 측정 기반 양자연산(Measurement Based Quantum Computation)과 같이 일반적 양자 상태를 이용하여 양자계산을 할 수 있는 논리적 양자 비트 개발 - 양자 상태의 결 어긋남(Decoherence)을 상쇄할 수 있는 조건 및 양자 큐빗의 알맞은 결맞음 상태를 유지할 수 있는 다양한 방법론 개발
양자소프트웨어	결함허용 양자비트, 양자 생성/제어 기술 등 해결되어야 하는 선행기술이 있어서 중간 단계에서 활용할 수 있는 형태의 연구개발 추진 - 상온에서 동작하는 양자 컴퓨터 개발되기 전까지는 격리되어 운용되는 양자컴퓨터를 활용하기 위한 원격 접속 및 인터페이스 기술개발 - 양자컴퓨팅 이론 및 알고리즘 연구의 초기에는 고전 컴퓨터를 통한 검증이 필요하므로 이를 위한 양자 에뮬레이션 기술개발 추진 - 결함허용 양자컴퓨터 시스템이 궁극적인 목표이므로 양자컴퓨터 소프트웨어 아키텍처, 양자 알고리즘 최적화 등과 같은 기반기술 연구 병행

[자료] 과학기술정보통신부·정보통신기획평가원(2018)

Ⅳ 양자컴퓨터 기술개발 활성화를 위한 정책제언

기초과학과 정보기술 양측에서 미래 선도형 R&D 전략이 필요

- 양자컴퓨터는 새로운 ICT 패러다임을 만들어낼 기술로써 세계 최선도국 미국도 원천기술을 개발하려 분투 중인 분야이므로 추격형 기술개발 전략이 적합하지 않은 분야
- 과거에는 큐비트 수를 늘리는 연구개발이 주를 이루었었으나, 향후에는 큐비트 수와 게이트의 정확도를 동시에 높이는 것이 중요
- 양자계산 우수성을 보이거나 논리적 큐비트 유효성을 입증하는 수준의 하드웨어기술 확보가 필요
- 양자컴퓨터는 다른 프로그래밍 언어를 요구할 뿐만 아니라 프로그래밍에 대한 근본적으로 다른 사고방식을 필요로 하기때문에 소프트웨어에 대한 연구개발도 함께 추진 필요

국내 양자정보기술 정책은 단기적으로도 성과가 가능한 양자통신에 집중해 왔으나, 시장규모나 파급효과가 큰 양자컴퓨터 분야에 대한 투자 확대가 필요

- 양자통신, 적어도 국내 양자정보기술 정책이 집중하고 있는 양자암호통신은 기술개발을 넘어서 국제 기술 표준화가 진행 중이며 SK텔레콤 등 민간업체가 세계 수위의 경쟁력을 성공적으로 확보해가고 있음
- 따라서 인공지능과 함께 모든 산업의 판도를 바꿀 것으로 예상되는 양자컴퓨터 분야에 정부 주도의 기술개발 집중이 필요

현재 양자컴퓨터는 큐비트 동작 안정성이 확보되지 않은 상황인 만큼 초전도체, 이온트랩 등 현존하는 큐비트 구현방식 이외의 기술개발 시도도 필요

- 절대 0도 수준의 냉각, 전자기적 잡음의 완전한 차폐 등에도 불구하고 동작 안정성이 확보되지 않은 큐비트는 사실상 양자컴퓨터 대중화가 요원함을 의미

- 진공관으로 구현되었던 초기 디지털 컴퓨터들 또한 진공관의 물리적 동작 불안정성으로 인해 성능 향상이 제한되었다가 트랜지스터 집적회로의 발명과 함께 동작 안정성이 확보되면서 디지털 컴퓨터의 지수적 성능 향상이 시작되었음
  - 1940년대의 진공관은 스스로 발생시키는 열과 전자기적 잡음에 의해 파손되고 잦은 오동작을 일으켜 복잡한 연산의 수행이 어려웠음
- 실리콘, 금속 등 다양한 재료를 이용해 잡음에 강하면서 소형화 가능한 양자컴퓨터를 구현하는 것은 세계적으로 기초 연구 단계인 만큼 국내 연구진의 도전이 필요

■ 많은 큐빗을 집합적으로 관리하고 조작하는 일이 가능하다고 하더라도 양자컴퓨터의 실용적 사용처와 적합한 알고리즘을 찾아내는 것이 중요

- 양자컴퓨터가 더 잘할 수 있는 알고리즘은 지금까지 몇 가지밖에 고안되지 않았으며, 그중 가장 유명한 알고리즘은 MIT 피터 쇼어가 개발한 정수의 소인수를 구하는 알고리즘임
  - 쇼어 알고리즘 등이 프로그래밍 언어로 기술된 알고리즘이라는 오해가 있는데 현재 양자 알고리즘들은 결과 도출을 위한 양자게이트 연결구조의 설계인 원시적 알고리즘
  - 쇼어 알고리즘은 입력된 큐비트에 대한 소인수분해 결과를 생성할 수 있는 양자게이트들의 연결구조로 표현됨
- 양자컴퓨터 하드웨어보다 더 많은 사용자들이 이용할 수 있는 애플리케이션인 소프트웨어 알고리즘 개발도 필요
  - 큐비트 경쟁이나 시장경쟁에서는 누가 실제로 사람들에게 유용한 솔루션을 만들어내는지가 관건이 될 것이며, 더 많은 사용자가 사용할수록 양자컴퓨터용 소프트웨어 알고리즘도 더욱 빠르게 개선될 것으로 기대

■ 국가에 의한 양자컴퓨터 시뮬레이션 센터 설립 등을 통해 양자정보처리 알고리즘 개발을 격려하는 전략도 시도해볼 필요가 있음

- 양자알고리즘의 개발은 양자게이트를 시뮬레이션하는 고전적 디지털 컴퓨터에서 이루어지고 있는데 현재 국내에는 대형 양자컴퓨터 시뮬레이션 설비가 없음

- 오류정정 등의 문제가 해결되고 양자컴퓨터가 대중화된다면 양자게이트 기반 알고리즘 설계 기술력이 양자컴퓨팅 칩의 기술수준을 결정할 것임
- 따라서 국가적 투자를 통해 연구기관 또는 대학 등의 거점에 양자컴퓨터 시뮬레이션 설비를 갖추고 국내외 연구진에게 개방하는 전략이 필요하다고 여겨짐

※ 수십 년간 CPU 제조 기술력을 독점했던 인텔은 집적회로 제작 기술이 아니라 다양한 연산 알고리즘을 트랜지스터 기반 논리게이트로 구현하는 기술을 가진 기업임

국내 양자컴퓨터 기술개발 허브 확보가 필요

- IBM 등 미국의 거대 ICT 기업들이 양자컴퓨터 HW·알고리즘 개발을 선도하는 R&D 허브가 되면서 인재와 지식을 흡수하는 중
- 국내 출연연, 대학, 기업이 모두 접근 가능하며 국내외 인재와 지식을 모을 수 있는 양자컴퓨터 기술개발 허브의 확보가 필요
- 양자물리학, 나노공학, 전산학, 수학, 전자공학 등 다양한 기초과학과 공학 지식이 모이면서 혁신이 일어나야 하는 만큼 단기적 이해를 뛰어넘을 수 있는 국가 차원의 기술개발 허브 설립과 지원이 필요

세계 최고 수준의 인재 양성과 국제적 인재 획득 전략이 요구

- 기술 진화 방향이 결정되지 않은 미래 기술인만큼, 세계 최고 수준의 인적 자원 확보가 가장 중요한 기술개발 전략이 될 수 있음
- 서울대, KAIST 등 일부 연구중심 대학에서 양자컴퓨터 관련 연구와 교육을 진행하고 있으나, 해당 분야 최고 수준의 인재는 미국 유학행을 선택
- 마이크로소프트, IBM 등 거대 ICT 기업들이 양자컴퓨터 분야 대학교수와 연구팀에 전략적 투자를 통해 핵심 인재를 독점하는 상황
- 해외 인재의 국내 유입과 국내 대학, 출연연 등에서 최고 수준의 연구와 교육이 이루어질 수 있는 환경 조성이 필요

- 기업 차원에서는 우수한 기술력을 보유한 해외 스타트업 입수나 합병 등을 통해 기술력을 보강하는 전략도 필요
  - SKT가 양자암호통신 기술력 보강을 위해 양자 SW 스타트업이자 양자암호통신 1위 기업 'IDQ'를 인수했던 바와 같이 기술력 확보의 수단으로서 국내외 업체 간 M&A를 고려할 수 있음
  - 한편, 자금과 인력이 열세인 중소기업은 이미 선행기업들이 제공하기 시작한 클라우드 서비스를 활용해 차별화된 응용프로그램을 개발하여 시장을 선점하는 전략이 필요

참 고 문 헌

- 과학기술정보통신부 (2019), '꿈의 컴퓨팅', 양자컴퓨팅 핵심기술 개발 첫 발 뗀다, 과학기술정보통신부 보도자료.
- 과학기술정보통신부 & 정보통신기획평가원 (2018), ICT R&D 기술로드맵 2023, 정보통신기획평가원.
- 권문주 외 (2018), 미래 핵심 기술인 양자정보통신기술 진흥법안 입법 추진현황, 정보통신산업진흥원.
- 김지소 (2019), ICT의 새로운 진화, 양자정보통신을 향한 주요국의 도전, ICT SPOT ISSUE SPOT 2019-15, 정보통신기획평가원.
- 니시모리 히데토시 외 (2018), 1억배 빠른 양자컴퓨터가 온다, 로드북.
- 미래창조과학부 (2016), 양자정보통신 중장기 기술개발 사업기획보고서.
- 박성수, 송호영 (2019), "양자정보통신기술 현황과 전망", 전자통신동향분석 제34권 제2호.
- 백충헌, 황용수, 김태완, 최병수 (2018), "양자컴퓨팅 기술 연구개발 동향", 전자통신동향 분석 제33권 제1호.
- 송영근 (2017), 양자 통신/컴퓨팅 도메인 분석: 시장 전망 및 기술개발사업 타당성 분석, ETRI Insight Report 2017-39, ETRI 기술경제연구본부.
- 이해웅 (2017), 양자 정보학 강의, 사이언스북스.
- 정보통신기술진흥센터 (2018), ICT 기술수준조사보고서.
- 정지형 (2019), 양자정보기술 동향 및 시사점, ETRI Insight Report 2019-04, ETRI 기술경제연구본부.
- 조성선 (2018), 양자컴퓨터 개발 동향과 시사점, ICT SPOT ISSUE S18-02, 정보통신기술진흥센터.
- 최병수 (2018), 양자컴퓨팅 연구개발 동향, 2018 KRnet 발표자료.
- 한국과학기술기획평가원 (2018), 이슈분석: 주요국 양자정보기술 지원정책 동향, 과학기술 & ICT 정책·기술 동향 제114호.
- 황용수, 백충헌, 김태완, 허재두 (2019), 양자정보기술 연구개발의 거대한 물결, 전자통신동향 분석 제34권 제1호.

- Gartner (2018), '5 Trends Emerge in the Gartner Hyper Cycle for Emerging Technologies 2018'.
- Mind Commerce (2018), Quantum Computing 2018-2023, Mind Commerce Publishing.
- Quantum Computing Report (2019), "Qubit Count," https://quantumcomputingreport.com/scorecards/qubit-count/

필자 소개

▸ 정지형

- 한국전자통신연구원 기술정책연구본부 경제사회연구실 책임연구원
- T. 042-860-5643 / E. jhc123@etri.re.kr

▸ 최병철

- 한국전자통신연구원 기술정책연구본부 산업제도연구실 책임연구원
- T. 042-860-1223 / E. cbc@etri.re.kr

KISTEP ISSUE PAPER 2019-07 (통권 제265호)

‖ 발행일 ‖ 2019년 9월 3일

‖ 발행처 ‖ 한국과학기술기획평가원 혁신전략연구소
서울시 서초구 마방로 68 동원산업빌딩 9~12층
T. 02-589-5262 / F. 02-589-2222
http://www.kistep.re.kr

‖ 인쇄처 ‖ 주식회사 동진문화사(T. 02-2269-4783)