

미래 新기술의 정점, 양자컴퓨터(Quantum Computer) 1부

송완영 연구위원

TRUDER FIRST



미래 新기술의 정점, 양자컴퓨터(Quantum Computer) 1부

송완영 연구위원(wysong@hf.go.kr)

- ❖ “꿈의 컴퓨터”로 불리던 양자컴퓨팅 기술이 다양한 분야에서 가시적인 성과를 내기 시작하면서 국가차원 및 글로벌 기업의 미래 핵심기술로 떠오르고 있음
- ❖ 본 논고 1부에서는 양자컴퓨터의 기본원리와 기존 컴퓨터와의 차이, 양자알고리즘 등을 중심으로 살펴보고, 2부에서는 양자컴퓨터 구현 및 응용 분야, 상용화 시 가져올 파급효과, 그리고 한계와 시사점 등에 대해 알아보고자 함

본고의 내용은 집필자의 개인 의견으로 주택금융연구원의 공식적인 견해와 다를 수 있습니다.

1. 양자컴퓨터의 부상

■ 현대사회의 폭발적 정보량 증가 추세와 더불어 그 처리와 활용을 위한 빠르고 효율적인 컴퓨터에 대한 수요 역시 늘어나고 있음

- 항공·우주공학, 신약·신소재 개발, 군사기술, 기상·재해 예측, 교통흐름 제어, 사물인터넷 구축, 인공지능, 빅데이터 등 실생활과 직·간접적으로 관련된 거의 모든 분야 망라
 - 주요 선진국 및 글로벌 기업 등은 막대한 연구비 및 인력을 투자하여 신소재 또는 새로운 동작 원리를 이용한 컴퓨터 개발에 매진
- 양자컴퓨터는 미시세계의 양자역학적 현상을 기본 동작 원리로 사용하는 연산장치로, 특정* 연산에 대해 기존 컴퓨터 성능을 월등히 뛰어넘는 잠재력을 가져 그 구현 가능성에 대해 오랜 기간 연구되어 왔음

* 최적화(Optimization) 문제, 대규모 트래픽 분석, 신약 및 신소재 개발, 양자화학, 인공지능, 빅데이터 활용 금융 서비스, 암호학, 정보보안 등

■ 양자컴퓨터가 부각되는 배경^[5]에는 기존 컴퓨터의 한계가 명확해지는 동시에 최근 들어 실질적 성과를 보여주기 시작했기 때문

- 무어의 법칙(반도체 집적회로의 성능이 18개월마다 2배로 증가한다는 전망) 종말로 대변되는 기존 컴퓨터 한계

- 컴퓨터의 연산 과정은 트랜지스터로 구성된 논리 게이트를 조합한 논리 회로를 통해 구현되며, 따라서 기존 컴퓨터의 연산능력 확대란 제한된 크기의 반도체에 얼마나 많은 트랜지스터를 집적할 수 있느냐의 문제
 - ▶ 예시: '71년 인텔4004 프로세서는 2,300개 트랜지스터 집적 → '16년 i7, 32억 개
 - 현재 실리콘* 기반 반도체 수준에서 10nm(nano meter; 10억 분의 1 미터) 이하 회로 제작 시, 회로를 따라 흘러야 할 전자(electron)들이 회로 밖으로 빠져나가는 양자터널(Quantum Tunneling) 현상 발생확률이 높아져 오류발생 가능성 증가
 - * 탄소나노튜브, 그래핀 등 실리콘 대체 신소재 역시 터널효과로 인한 오류를 완전히 극복할 수는 없음
 - 양자컴퓨터는 새로운 동작원리를 바탕으로 물리적 허용범위 내에서 기존 방식보다 최대 지수함수적 연산속도 향상(exponential quantum speed-up)이 가능
- 반도체 칩 성능개선 한계에 따라 연산 능력 확대는 보다 많은 프로세서 탑재 및 병렬·분산(parallel) 프로그래밍으로 극복 중, 다만 고비용 등 문제 수반
- 연산능력 93 PFLOPS*로 세계 2위인 중국의 “Sunway TaihuLight” 슈퍼컴퓨터는 자체 개발 프로세서 40,000여 개를 합쳐 총 10,649,600 코어 탑재
 - * 페타플롭스(PetaFlops)는 초당 1,000조(10^{15}) 번의 연산처리가 가능함을 의미. 참고로 일반 PC의 i7 CPU는 수 백 GFLOPS(기가플롭스, 초당 십 억, 10^9) 수준
 - 그러나 이는 컴퓨터 거대화에 따른 고가의 구축비용 및 유지비, 대규모 전력 소모 등 문제점을 수반하므로 반도체 칩 한계를 극복하는 대안으로는 부족
- 2001년 이후 양자알고리즘 구현 및 하드웨어 개발 등 양자컴퓨터의 실질적 성과 구현
- 2001년 IBM은 소인수분해를 기존 연산방식보다 빠르게 하는 양자 알고리즘(Shor's algorithm)을 NMR(핵자기공명) 방식 7 큐비트*(qubit) 양자컴퓨터로 구현 성공
 - * 양자컴퓨팅 연산 기본 단위. 2장에서 상술
 - 2015년 Google과 NASA는 캐나다 기업 D-Wave Systems의 양자컴퓨터를 이용하여 특정 최적화 문제에서 싱글 코어 프로세서 탑재 컴퓨터 대비 약 1억 배 빠른 결과를 도출
 - D-Wave 양자컴퓨터가 진정한 의미의 양자컴퓨터인가에 대한 논란은 있으나, 일반 대중은 물론 글로벌 대기업들의 관심 확대에 기여
 - IBM에서 50 큐비트('17년), Intel은 49 큐비트('17년), 그리고 최근 Google이 72큐비트('18년) 양자 프로세서를 발표하는 등 양자컴퓨팅을 위한 하드웨어 개발 진전 본격화

4차 산업혁명을 주도할 미래 핵심 기술로 부상

- 양자컴퓨팅 기술이 더 이상 이론의 영역에 머무르지 않고 실현 및 상용성이 가시화됨에 따라 글로벌 기업뿐만 아니라 국가차원의 미래 전략기술로 대두
 - 국내의 경우 향후 5년 간 양자컴퓨터 핵심 원천 기술개발과 양자알고리즘 기반 소프트웨어 등에 총 445억 원 투자, 2019년에는 총 60억 원 투입^[8] 예정
- MIT, 세계경제포럼(World Economic Forum), Gartner 등 해외 주요 시장 및 기술 분석 기관들은 최근 양자컴퓨터를 10대 핵심 기술* 중 하나로 선정
 - * 가까운 시일(5년에서 10년) 내 기술개발에 있어 정점에 도달할 것으로 예상되고, 잠재력 및 영향력과 활용성에서 두각을 나타낼 것으로 기대되는 기술

〈주요 기관 10대 기술 선정 예시〉

World Economic Forum(2017)[1]	MIT Technology Review(2018)[2]	Gartner (2019)[3]
액체 생체검사 (Liquid Biopsies)	3D 금속 프린팅 (3D Metal Printing)	자율 사물 (Autonomous Things)
물 획득 기술 (Harvesting Clean Water from Air)	인공배아 (Artificial Embryos)	증강 분석 (Augmented Analytics)
시각 작업을 위한 딥러닝 (Deep Learning for Visual Tasks)	스마트 도시 (Sensing City)	인공지능 주도 개발 (AI-Driven Development)
태양광 이용 액체연료 제조기술 (Liquid Fuels from Sunshine)	모두를 위한 인공지능 (AI for everybody)	디지털 트윈 (Digital Twins)
인간세포 도감 (The Human Cell Atlas)	결투신경망 (Dueling Neural Networks)	자율권을 가진 에지 (Empowered Edge)
정밀농업 (Precision Farming)	실시간 통역 (Babel-Fish Earbuds)	몰입 경험 (Immersive Experience)
환경친화 이동수단 촉매 (Affordable Catalysts for Green Vehicles)	탄소제로 천연가스 (Zero-carbon Natural Gas)	블록체인 (Blockchain)
게놈백신 (Genomic Vaccines)	온라인 프라이버시 (Perfecting Online Privacy)	스마트 공간 (Smart Spaces)
지속가능한 디자인 (Sustainable Design of Communities)	유전적 운세 (Genetic Fortune Telling)	디지털 윤리와 개인정보보호 (Digital Ethics and Privacy)
양자컴퓨팅 (Quantum Computing)	재료의 양자 도약 (Materials' Quantum Leap)	양자컴퓨팅 (Quantum Computing)

※ [1] : <https://www.weforum.org/agenda/2017/06/these-are-the-top-10-emerging-technologies-of-2017/>

※ [2] : <https://www.technologyreview.com/lists/technologies/2018/>

※ [3] : <https://www.gartner.com/smarterwithgartner/gartner-top-10-strategic-technology-trends-for-2019/>

2. 양자컴퓨터 기본 원리

■ 양자컴퓨터 연산 단위

- 양자컴퓨터 아이디어의 기반을 이루는 양자역학(Quantum Mechanics)은 원자 단위 수준의 미시세계에서 벌어지는 현상을 다루는 물리학 이론

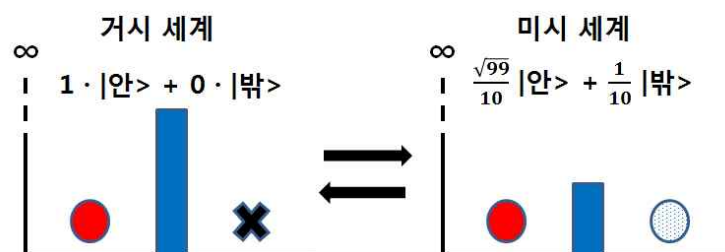
- 19세기 후반부터 이루어진 전자, 양성자 등 소립자와 관련된 실험결과가 기존 고전 역학(Classical Mechanics)으로 설명이 불가능했고 양자역학은 이를 해결하기 위해 정립된 새로운 역학 체계이며, 현대물리학의 근간을 이루고 있음
- 양자역학에서는 어떤 시스템의 상태(State)는 시스템을 기술하기 위한 물리량(위치, 운동량 등)의 고유상태(Eigenstate)들의 중첩(Superposition)으로 표현되고, 외부에서 시스템의 상태를 측정(Measurement)할 때 중첩되어 있던 고유상태 중 하나로 특정 확률로 붕괴(Collapse 또는 결정)됨을 가정

- ▶ 가령 고유상태가 A, B라면 어떤 상태 ψ 는 $|\psi\rangle = (1/2)|A\rangle + (\sqrt{3}/2)|B\rangle$ 등으로 기술되며 이때 $1/2, \sqrt{3}/2$ 등이 진폭(Amplitude), 진폭의 절대값 제곱이 그 고유상태로 결정될 확률임(A 또는 B로 결정될 전체 확률은 1, 즉 $1/4 + 3/4 = 1$). 이 때 확률은 항상 0 이상인 수이나 진폭은 양수, 음수 또는 복소수 값이 가능

* $|\cdot\rangle$ 표기는 양자상태(quantum state) 표기법으로, Dirac ket notation으로 지칭

- 중첩 상태 예시 : 양자터널링 효과(Quantum Tunneling Effect)

- 아래 그림과 같이 장벽에 있는 구슬의 고유상태를 $|\text{안}\rangle, |\text{밖}\rangle$ 이라 할 때, 거시세계에서는 구슬이 벽을 뚫고 장벽 오른쪽에 있을 수 없지만 미시세계에서는 중첩에 의해 장벽의 높이가 어느 정도 낮다면 장벽 밖에서 측정될 확률이 0이 아님



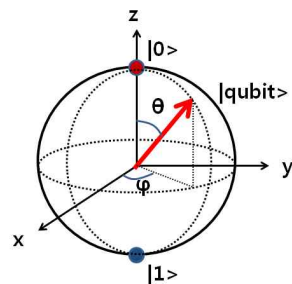
- 거시세계에서 중첩효과가 사라지는 이유는 장벽의 높이가 점점 커지면서 장벽 밖에 존재할 확률이 0에 가까워지기 때문
- 상기 현상을 양자터널링 효과로 부르며 1장에서 설명한 반도체 집적능력 한계의 원인, 즉 회로를 따라 흘러야 할 전자들이 회로 밖으로 빠져나가 오류를 발생시키는 이유가 됨

- 기존 디지털 컴퓨터는 특정 순간 0 또는 1 둘 중 하나의 값(상태)만 가질 수 있음에 반해 양자컴퓨터는 0과 1의 중첩상태를 연산단위로 사용
 - 디지털 연산 기본단위인 비트(bit: binary digit)에 대응하여 양자컴퓨팅에서는 0과 1의 중첩된 상태(정보)에 의한 정보량이 2인 큐비트(qubit: quantum bit)가 기본 연산단위
 - 큐비트 중첩상태는 양자상태 공간에서 길이(확률)가 1인 어느 점이라도 될 수 있음

Classical Bit



Quantum Bit (Bloch Sphere 상에서 시각화)



- 여러 개의 큐비트들 간 상호작용 형성, 즉 양자 얽힘(Quantum Entanglement) 상태를 만들면 연산공간은 지수함수적으로 증가
 - 큐비트가 두 개면 $2 \times 2 = 4$, 세 개면 $2^3 = 8$, N개면 2^N 만큼의 정보공간 생성

2-큐비트	3-큐비트	4-큐비트
$ 00\rangle, 01\rangle$ $ 10\rangle, 11\rangle$	$ 000\rangle, 001\rangle$ $ 010\rangle, 011\rangle$ $ 100\rangle, 101\rangle$ $ 110\rangle, 111\rangle$	$ 0000\rangle, 0001\rangle, 0010\rangle, 0011\rangle$ $ 0100\rangle, 0101\rangle, 0110\rangle, 0111\rangle$ $ 1000\rangle, 1001\rangle, 1010\rangle, 1011\rangle$ $ 1100\rangle, 1101\rangle, 1110\rangle, 1111\rangle$

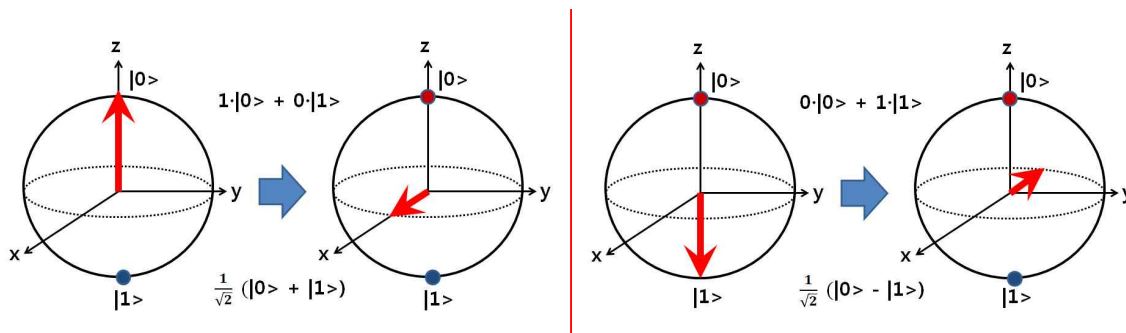
- ▶ 예를 들어, 스위치(on/off) 10개가 표현할 수 있는 상태는 $2^{10} = 1,024$ 개이고 디지털 비트 10개는 1,024개 중 매 순간 하나만 표현 가능하며, 모든 상태를 표현하려면 1,024개의 비트 필요. 큐비트는 on/off 중첩상태를 가지므로 10개면 충분
- 다만, 단순히 중첩 및 얽힘 상태가 준비된다고 해서 연산속도의 비약적 상승이 보장되는 것은 아님
 - 양자시스템은 외부측정 시 고유상태 진폭의 제공에 해당하는 확률로 관측결과가 나오며, 따라서 정답에 필요한 고유상태의 진폭 또는 확률이 작다면 오류 가능성이 커지므로 원하는 해답에 관한 특정 상태가 얻어질 확률을 높이는 연산 및 알고리즘 필요

3. 양자정보처리 및 양자알고리즘

■ 양자컴퓨터 연산과정

- 양자컴퓨팅 연산이란 중첩 및 얽혀있는 큐비트들의 고유상태 진폭을 변화시키는 것을 의미하며 유니타리(Unitary) 변환*, 또는 양자게이트(Gate)로 수행됨
 - 유니타리 변환이란 양자상태 공간에서 길이를 유지하는 변환을 의미하며, Bloch Sphere 상에서 큐비트를 회전시키는 변환 등으로 이해할 수 있음. 실제로는 외부에서 자기장(Magnetic Field)을 걸어주거나 레이저 펄스 등을 쏘주는 방식임
 - 기존 디지털 컴퓨터가 AND, OR, NOT 게이트 등을 이용하여 연산회로를 구성하듯이 양자회로 역시 Hadamard 게이트, C-NOT(Controlled-NOT) 게이트 등 기본 양자게이트를 이용한 알고리즘을 거쳐 연산 작업 수행되며, 기존 디지털 컴퓨터로 계산 가능한 모든 문제들이 양자게이트 순차적용을 통해 구현 가능성이 증명^[9]되며 범용 양자컴퓨터 가능성이 높아짐

〈Hadamard 게이트 작동 예시〉



- 양자정보처리 과정은 ㉠주어진 문제에 적합한 큐비트 중첩 및 얽힘 상태를 준비하고 ㉡문제해결을 위한 연산 또는 알고리즘을 거쳐 ㉢측정으로 결과를 도출하는 것임
- 양자세계 특성을 활용하여 기존 방식 대비 연산속도 향상을 달성하는 알고리즘 개발은 지금도 계속되고 있으며 여기서는 대표적 방법 두 개를 소개하고자 함

■ Shor 알고리즘 : 소인수분해(Prime Factorization)

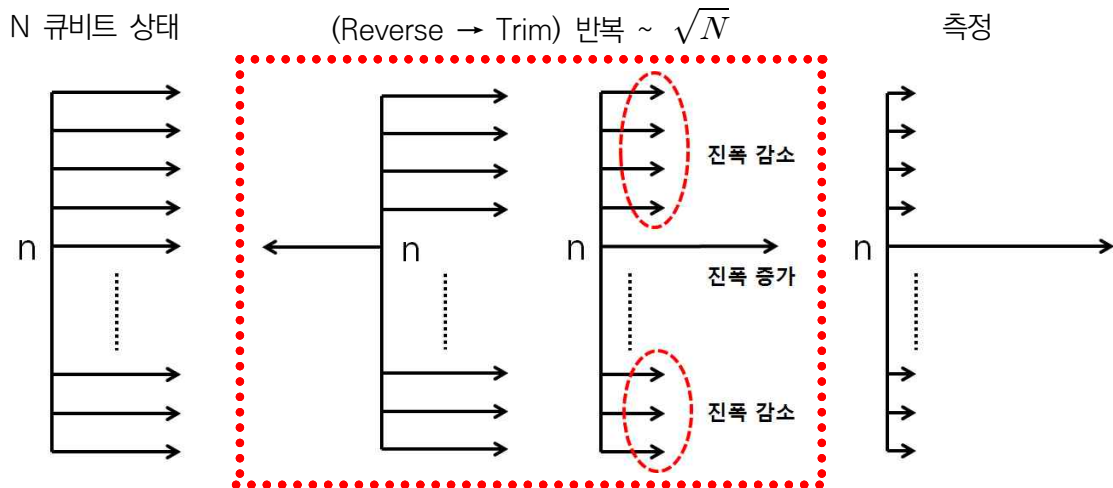
- 소인수분해에 적용되는 Shor 알고리즘은 고전 컴퓨터 대비 우월한 양자알고리즘 존재 가능성을 처음으로 제시

- 기본 단계는 ㉠ 소인수분해 문제를 지수함수 주기 도출 문제로 변환, ㉡ 양자푸리에 (Fourier)변환 게이트 적용, ㉢ 주기관련 상태 관측 등으로 진행
- 기존 방식 소인수분해 복잡도(order) $O(\exp((\log N)^{1/3}))$ 에서 $O((\log N)^2)$ 수준으로 개선하여 지수함수적 속도개선(exponential speed-up) 달성
- 소인수분해 달성속도 개선은 현 공개키 암호화(Public-Key Cryptography)를 신속하게 풀 수 있음을 의미하며, 악용될 경우 사이버 보안체계 붕괴 초래
 - 공개키 암호화는 송신자가 공개키로 데이터를 암호화하여 전송하고 수신자는 비밀키를 이용해 복호화하는 것으로 RSA(Rivest, Shamir, Adleman) 방식 등이 쓰이고 있음
 - 상기 암호화체계는 “작은 수의 소인수 분해는 쉽지만(15 = 5 x 3 등) 큰 수는 어렵다(장시간 소요)”는 것을 이용하여 수백자리 이상의 소인수를 암호화에 이용
 - Shor 알고리즘은 기존 방법으로는 우주의 나이(100억년 이상) 정도 걸리는 400자리 소인수분해에 수 일 소요가 예상되어 양자컴퓨터 상용화 시 기존 보안체계 붕괴 가능성 시사
- 양자컴퓨터 성능이 점차 발전하고 있는 지금, 기술개발이 가져올 보안위험 문제를 인식하고 공공기관 및 기업 역시 대응방안을 마련해야 할 시기 도래
 - 양자컴퓨터로 인한 사이버 보안 붕괴위험 대응을 위해 양자 이후 암호화(Post Quantum Cryptography) 기술 개발이 Google 등을 중심으로 진행 중⁴⁾

■ Grover 알고리즘 : 양자탐색(Quantum Search)

- Grover 알고리즘은 N개의 리스트가 주어졌을 때(순차 정렬되지 않은), 그 중 특정 n을 찾는 탐색 알고리즘의 양자컴퓨팅 버전
 - 기본 단계는 ㉠ 동일 진폭 N개 큐비트 준비, ㉡ n에 해당하는 큐비트 진폭 뒤집기, ㉢ 진폭 평균 구하기, ㉣ 평균을 중심으로 뒤집기, ㉤ ㉡~㉣ 반복, ㉥ 측정 등으로 진행
 - 핵심 아이디어는 찾고자 하는 상태의 진폭은 키우고 나머지 상태의 진폭을 감소시켜 외부 측정 시 정답이 나올 확률을 극대화 시키는 것임
 - 기존 고전 알고리즘 복잡도 $O(N)$ 에서 $O(\sqrt{N})$ 수준으로 향상되어 제곱 수준의 속도개선(quadratic speed-up) 달성

〈Grover 알고리즘 개요〉



- 양자탐색 알고리즘은 기존 대용량 데이터베이스 검색기능 향상뿐만 아니라 암호해독에도 적용 가능
 - 탐색 알고리즘은 검색 대상을 어떤 함수(Function)를 충족하는 답, 즉 역함수 (Inverse Function)를 찾는 것으로 확대 가능
 - 양자탐색은 대칭암호체계를 무력화시키는 무차별대입공격(Brute-Force Cracking)의 속도 향상에 악용될 수 있어 Shor 알고리즘과 더불어 양자컴퓨팅 기술이 미래사회에 가져올 부정적·긍정적인 양면성을 보여주는 사례로 꼽힘

4. 1부 정리 및 2부 개요

- 양자컴퓨터는 큐비트 간 중첩, 얽힘 등 양자역학의 기본 성질을 바탕으로 연산을 행하는 컴퓨팅 방법임
 - 중첩 특성을 이용하여 고전 컴퓨터 대비 대용량의 연산 공간 확보가 가능하고, 얽힘을 통하여 다수의 연산을 한꺼번에 수행할 수 있음
 - 양자 알고리즘은 양자역학적 특성을 극대화하여 고전 컴퓨터 대비 월등한 계산능력을 발휘, 기존 방법의 한계를 극복함과 동시에 새로운 응용 가능성 제시
- 범용 양자컴퓨터 구축을 위한 국가 및 글로벌 기업의 관심이 집중되고 있는 바, 2부에서는 양자컴퓨터 구현의 현주소, 응용 분야 및 시사점 등을 살펴보고자 함

<참고문헌>

- [1] 임현식, “양자역학 원리를 이용한 컴퓨터 개발: 양자컴퓨터”, 물리학과 첨단기술, 2008
- [2] 김재완, “양자원리와 컴퓨터”, 물리학과 첨단기술, 2012.12
- [3] 정원주, 이성환, “양자 기계학습 기술의 현황 및 전망”, Journal of KIISE, Vol. 43, No. 7, 2016
- [4] “미 NSA, 양자 컴퓨팅 실용화에 따른 현 암호화 기술의 붕괴 경고”, 주간기술동향 1788호, 정보통신기술진흥센터, 2017
- [5] 조성선, “양자컴퓨터 개발 동향과 시사점”, 정보통신기술진흥센터, 2018
- [6] 김태현, “양자컴퓨터의 소개 및 전망”, 전자공학회지, 제45권 4호, 2018
- [7] 방정호, 이진형, “양자알고리즘 개발을 위한 머신러닝기법”, 전자공학회지, 제45권 4호, 2018
- [8] 과학기술정보통신부, ‘양자컴퓨팅 기술개발사업 추진계획’, 2019.02
- [9] G. Johnson, “A shortcut through time : The path to the quantum computer”, 2003
- [10] D. Deutsch, "Quantum theory, the Church-Turing principle and the universal quantum compute", Proc. of the Royal Society of London, Vol. A400, pp. 97-117, 1985
- [11] P. Shor, "Algorithms for quantum computation: Discrete log and factoring", Proc. of the 35th Annual Symposium on Foundations of Computer Science, pp. 124-134, 1994
- [12] L. Grover, "A fast quantum mechanical algorithm for database search", Proc. of the Twenty-Eighth Annual ACM Symposium on the Theory of Computing, pp. 212-219, 1996

■ 작성자 : 송완영 연구위원 (051-663-8157 / wysong@hf.go.kr)

■ 본고의 내용은 집필자의 개인의견으로 주택금융연구원의 공식적인 견해와 다를 수 있습니다.