제235회 한림원탁토론회

흥미로운
양자정보기술 ±20년

일 시 : 2025년 5월 9일(금), 15:00

장 소 : 한림원회관 1층 성영철홀
(온·오프라인 동시 진행)

주 최 : 한국과학기술한림원, 한국차세대과학기술한림원

KAST 한국과학기술한림원 The Korean Academy of Science and Technology

KAST Young Korean Academy of Science and Technology

Program

사 회 배준우 KAIST 전기 및 전자공학부 교수

시 간	프로그램	내 용
15:00~15:05 (5분)	**핵심 주제 개요**	
	배준우 KAIST 전기 및 전자공학부 교수	
15:05~17:00 (115분)	**주제발표 및 토론**	
	양자 오류 정정	**이승우** KIST 양자기술연구단 책임연구원
	중성원자 양자컴퓨팅	**안재욱** KAIST 물리학과 교수
	이온 트랩 양자컴퓨팅	**김기환** Tsinghua University 물리학과 교수
	양자통신 및 보안	**배준우** KAIST 전기 및 전자공학부 교수
	양자 얽힘 이론과 수학	**이수준** 경희대학교 수학과 교수
	얽힘과 헷갈림의 양자역학에서 피어난 양자정보	**김윤호** POSTECH 물리학과 교수
	양자암호 기술 상용화	**최정운** SKT Quantum팀 팀장
	토론요약 및 질의응답	

참여자 주요 약력

주제발표자

이 승 우

KIST 양자기술연구단 책임연구원

- 한국광학회 양자광학 및 양자정보 분과 위원장
- 한국물리학회 양자특별위원회 실무이사
- 前 고등과학원 QUC연구교수

안 재 욱

KAIST 물리학과 교수

- 한국물리학회 이사 및 대전충남세종 지부장
- 국제순수및응용물리연합(IUPAP) 원자분자광물리코미션 위원장
- 파스칼 코리아 과학고문

김 기 환

Tsinghua University 물리학과 교수

- 前 재중한인과학기술자협회 회장

참여자 주요 약력

주제발표자

배 준 우

KAIST 전기 및 전자공학부 교수

- 한국차세대과학기술한림원 회원
- 前 IEC SEG14 Co-Convenor
- 前 2014 EU Marie Sklodowska-Curie Fellow

이 수 준

경희대학교 수학과 교수

- 한국양자정보학회 국제교류이사
- 前 한국양자정보학회 총무이사 겸 실무이사장
- 前 과학기술정보통신부 양자과학기술 연구개발사업 추진위원

김 윤 호

POSTECH 물리학과 교수

- 미국광학회(Optica) Fellow
- 前 오크리지 국립연구소 Eugene Wigner Fellow

참여자 주요 약력

주제발표자

최 정 운

SKT Quantum팀 팀장

- 前 스위스 IDQuantique SA 수석연구원
- 前 ETRI 암호기술연구팀 선임연구원

I

주제발표

주제발표 1 양자 오류 정정

- **이승우** KIST 양자기술연구단 책임연구원

주제발표 2 중성원자 양자컴퓨팅

- **안재욱** KAIST 물리학과 교수

주제발표 3 이온 트랩 양자컴퓨팅

- **김기환** Tsinghua University 물리학과 교수

주제발표 4 양자통신 및 보안

- **배준우** KAIST 전기 및 전자공학부 교수

주제발표 5 양자 얽힘 이론과 수학

- **이수준** 경희대학교 수학과 교수

주제발표 6 얽힘과 헷갈림의 양자역학에서 피어난 양자정보

- **김윤호** POSTECH 물리학과 교수

주제발표 7 양자암호 기술 상용화

- **최정운** SKT Quantum팀 팀장

주제발표 1

양자 오류 정정

이 승 우

KIST 양자기술연구단 책임연구원

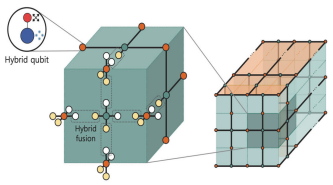
한림원탁토론회 (흥미로운 양자정보기술 ±20년)

Quantum Error Correction

Tackling the Error Problem in Quantum Info. Technology

양자오류정정

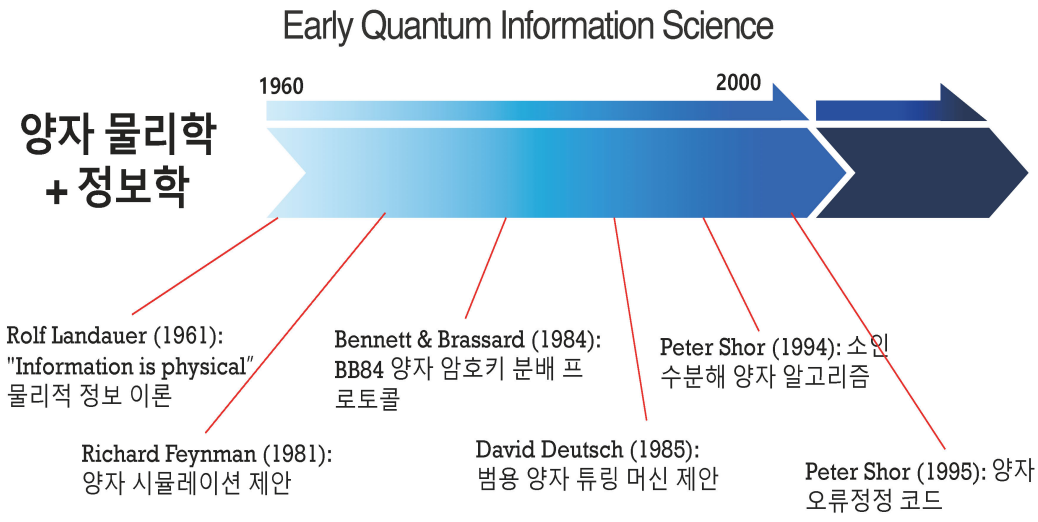
이 승 우 Seung-Woo Lee



양자정보기술의 과거와 현재

Past and Current Status of Quantum Info. Technologies

양자정보학의 시작: 가능성의 발견 (1960 ~)



3/22

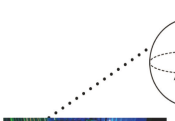
개념 증명의 시대: 학문에서 기술로? (2000 ~)

양자 센싱

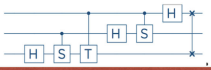
양자 통신

양자 컴퓨팅

미시에서
거시로 확장

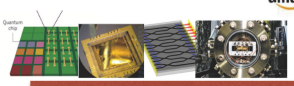


Lab scale



Proof-of-concept scale

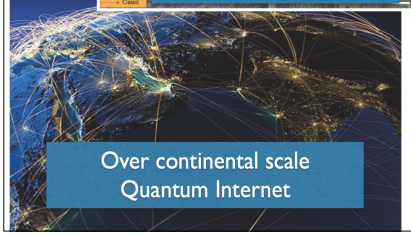
Metropolitan scale



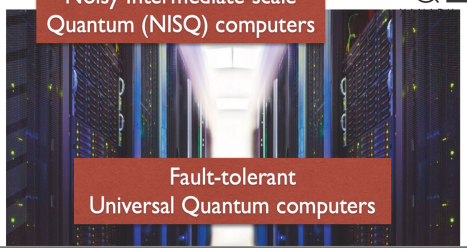
amazon IONQ IBM Honeywell QUANTINUUM Google IQuEra

We are now
in NISQ era

Noisy Intermediate-scale
Quantum (NISQ) computers



Over continental scale
Quantum Internet

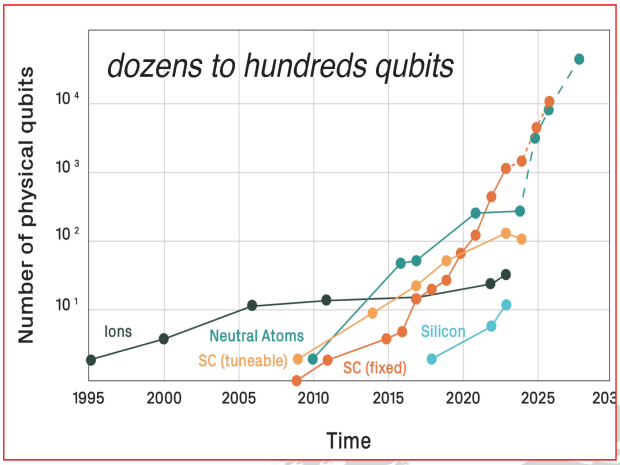


Fault-tolerant
Universal Quantum computers

Noisy Intermediate-Scale Quantum (NISQ)
- era of quantum computing with a limited number of that are susceptible to error.

4/22

NISQ 시대: 양자 시스템 구현 기술의 발전 (2010 ~ 현재)



Riverland report 2024.10

Google AI Quantum aws QUANTINUUM
IBM Quantum PsiQuantum
IQuEra Computing Inc. IONQ rigetti
XANADU ALICE & BOB ORCA Computing
PASQAL Infleqtion
QUANDELA

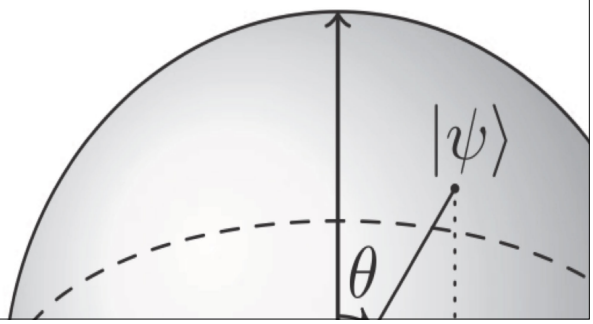
Global Race to develop
Quantum Computing

But 여전히 잡음(Noise)과 오류(error) 발생 문제 !

5/22

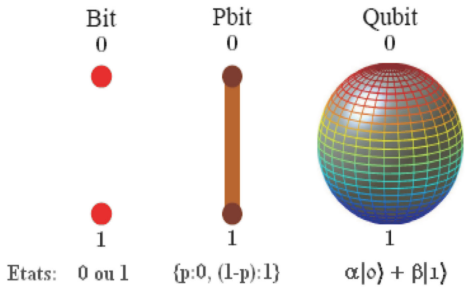
양자컴퓨팅의 오류 문제

Error Problems in Quantum Computing

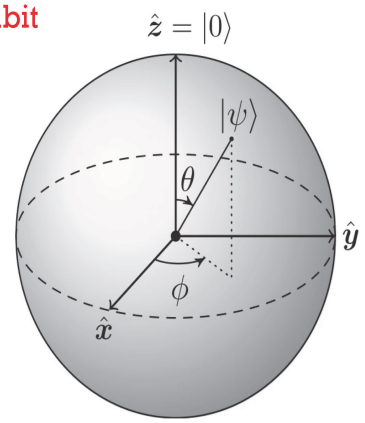


양자 상태에 입력된 정보(큐비트)

- 고전 정보 처리 : bit 0 or 1 연산
- 양자 정보 처리:
  Quantum bit (Qubit) 0과 1의 중첩



Qubit

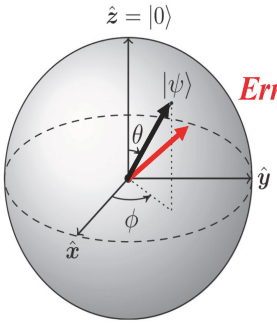


$$|\psi\rangle = \cos\frac{\theta}{2}|0\rangle + e^{i\phi}\sin\frac{\theta}{2}|1\rangle$$

$$|\cos(\theta/2)|^2 + |e^{i\phi}\sin(\theta/2)|^2 = 1$$

7/22

양자 상태에 입력된 정보(큐비트)는 쉽게 깨짐



Error!

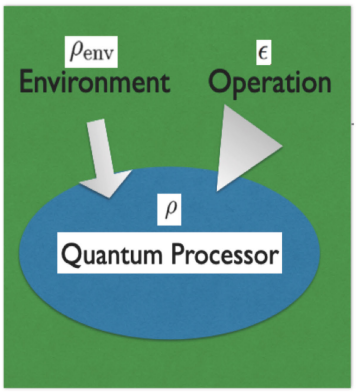
- Environmental decoherence

$$\mathcal{E}(\rho) = \mathrm{tr}_{\mathrm{env}}\left[U(\rho \otimes \rho_{\mathrm{env}})U^{\dagger}\right]$$

- Coherent quantum errors (gate)

$$p_{\mathrm{error}} \approx (N\epsilon)^2$$

$$P(|0\rangle) = \cos^2(N\epsilon) \approx 1 - (N\epsilon)^2,$$
$$P(|1\rangle) = \sin^2(N\epsilon) \approx (N\epsilon)^2.$$



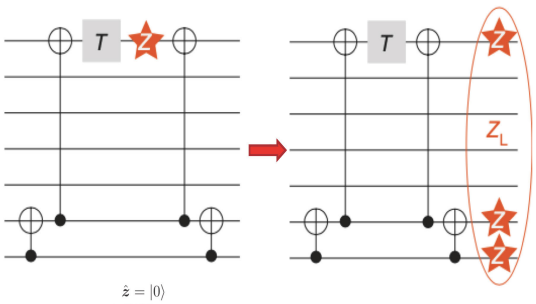
$$U(\delta\theta, \delta\phi)|\psi\rangle = \cos\frac{\theta+\delta\theta}{2}|0\rangle + e^{i(\phi+\delta\phi)}\sin\frac{\theta+\delta\theta}{2}|1\rangle$$
$$= \alpha_I \mathbb{1}|\psi\rangle + \alpha_X X|\psi\rangle + \alpha_Z Z|\psi\rangle + \alpha_{XZ} XZ|\psi\rangle$$

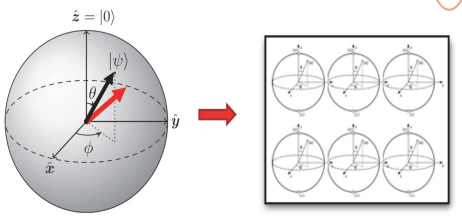
- Bit-flip error $X|\psi\rangle = \alpha X|0\rangle + \beta X|1\rangle = \alpha|1\rangle + \beta|0\rangle$
- Phase-flip error $Z|\psi\rangle = \alpha Z|0\rangle + \beta Z|1\rangle = \alpha|0\rangle - \beta|1\rangle$

- 큐비트는 환경의 영향(decoherence)으로 발생하는 노이즈, 불완전한 게이트 연산 등으로 오류가 쉽게 발생
- 임의의 오류는 X(bit-flip)와 Z(phase-flip)로 decomposed

8/22

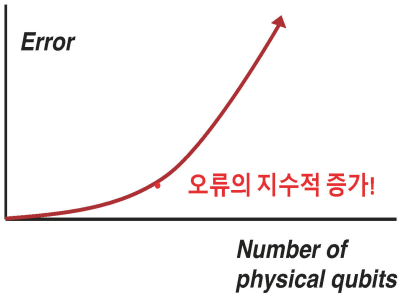
큐비트 수가 많아지면 오류가 빠르게 전파&누적

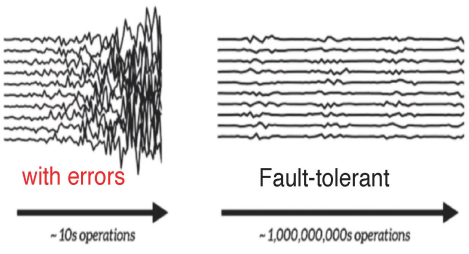




Error in Single qubit

Errors in Multiple qubits

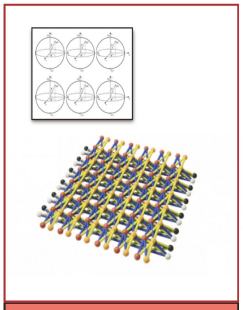
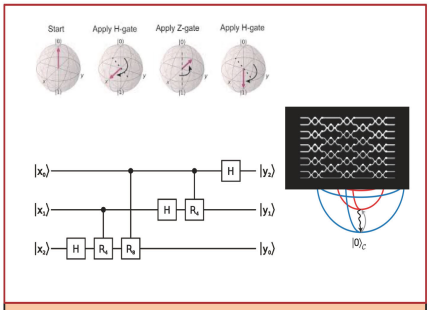
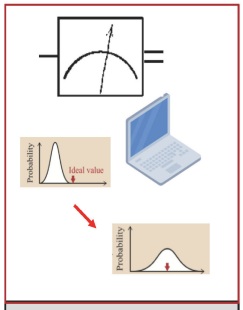




9/22

물리 큐비트에 발생하는 오류를 줄이는 방법

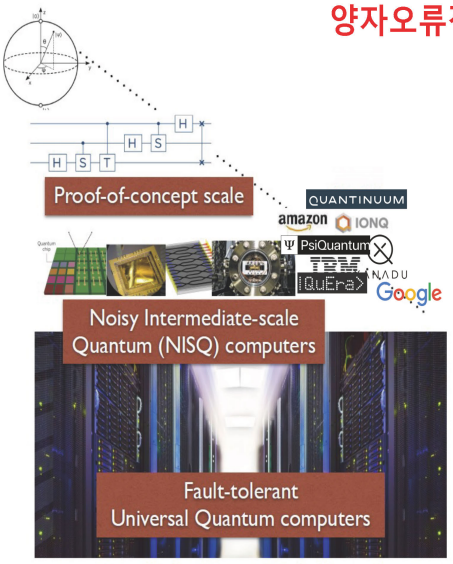
다양한 양자오류완화 기법

Preparation	In-line processing	Post-processing
		
Decoherence Free Subspace (DFS), Noiseless Subspace (NS)	Dynamical Decoupling (DD), Randomized Compiling (RC), or Twirling	Quantum Error Mitigation (QEM) - extrapolation, probabilistic cancellation, virtual distillation

- but 실용적인 연산 수행 규모로 확장 어려움 (fault-tolerance 달성 불가)

10/22

실용적인 양자 컴퓨팅 & 양자 이득 달성을 위해서는?



양자오류정정(Quantum Error Correction) 구현 필요

Recent numerous evidences[1,2,3,4] have shown that achieving quantum advantage in NISQ era is challenging, highlighting **the critical need of developing QEC toward fault-tolerant quantum computing.**

NISQ era

Quantum Error Correction

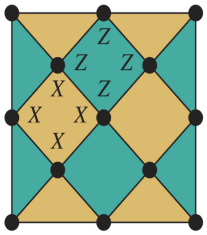
Fault-tolerance

[1] "Limitations of optimization algorithms on noisy quantum devices", Nature Physics 17, 1221 (2021).
[2] "The Complexity of NISQ", Nature Comm. 14, 6001 (2023).
[3] "Classical algorithm for simulating experimental Gaussian boson sampling", Nature Physics 20, 1461 (2024).
[4] "Exponentially tighter bounds on limitations of quantum error mitigation", Nature Physics 20, 1648 (2024).

11/22

양자오류정정 소개

Introduction to Quantum Error Correction



양자오류정정 Quantum Error Correction (QEC):

정보를 여러 개의 물리 큐비트 또는 확장된 양자 공간에 입력하여, 발생하는 오류를 효과적으로 발견하고 수정할 수 있는 기술

Redundant encoding *e.g. multiple physical qubits, larger Hilbert space*

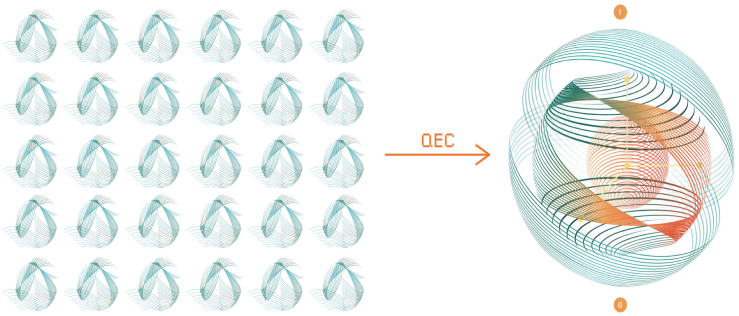
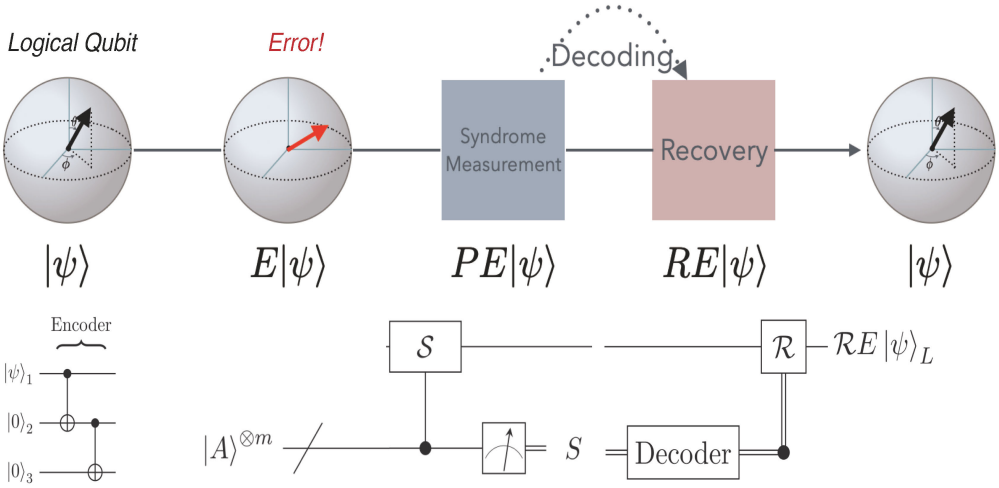


Figure from Riverland report 2024

여러 개의 물리 큐비트 *논리 큐비트*

13/22

양자오류정정 수행 과정 :



QEC process should be ***repeatedly performed*** *throughout the computation*

14/22

양자오류정정 (QEC)이 고전 정보처리 오류정정과 다른점

고전 오류정정

- 입력된 정보의 무제한 복제가 가능함

  0100110011 → 0100110011, 0100110011

  arbitrary duplicated 0100110011

- 한가지 오류만 발생

  bit-flip error only 0 ⟷ 1

- 입력된 정보를 읽어도 (측정해도) 정보에 변화가 없음

  "0100110011"

  0100110011 → 0100110011

VS

양자 오류정정

- 입력된 임의의 정보의 복제가 불가능

  $U_{\text{clone}}(|\psi\rangle \otimes |0\rangle) \not\rightarrow |\psi\rangle \otimes |\psi\rangle$

  No cloning theorem

- 오류의 종류가 2가지 **bit-flip & phase-flip**

  $X|\psi\rangle = \alpha X|0\rangle + \beta X|1\rangle = \alpha|1\rangle + \beta|0\rangle$

  $Z|\psi\rangle = \alpha Z|0\rangle + \beta Z|1\rangle = \alpha|0\rangle - \beta|1\rangle$

  simultaneously

- 입력된 정보를 읽으면 (측정하면) 정보가 사라짐 (양자 상태 붕괴) **Collapse**

  $|\psi\rangle = a|0\rangle + b|1\rangle$ → Collapse $|0\rangle$ or $|1\rangle$

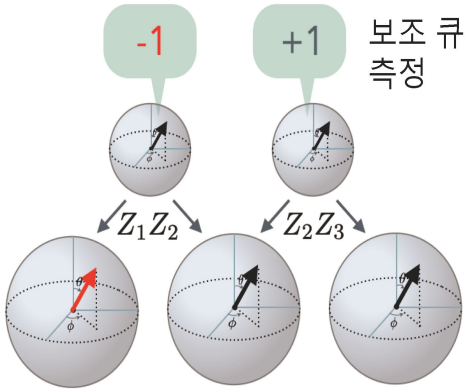
  $|0\rangle$ → Readout '0' or '1'

15/22

$\alpha|100\rangle + \beta|011\rangle$

각 물리큐비트를 측정하면,
논리큐비트에 입력된 정보가
깨짐 **Collapse**

Error Detection. Not Correction.



보조 큐비트
측정

Error	Z_1Z_2	Z_2Z_3
No Error	1	1
X_1	-1	1
X_2	-1	-1
X_3	1	-1

$\alpha|100\rangle + \beta|011\rangle$

$\alpha|000\rangle + \beta|111\rangle$

16/22

다양한 양자오류정정 코드 (QEC code)

9 Qubit Code (P. Shor 95) –bit and phase flip correction

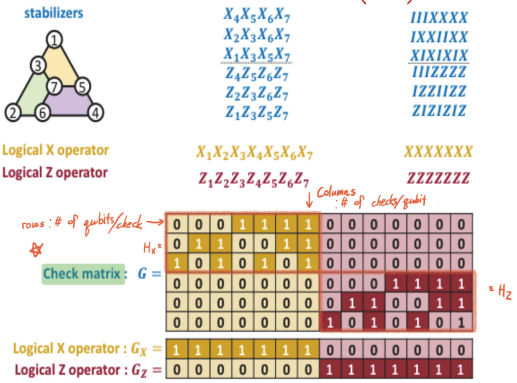
$$|0\rangle_L = \frac{1}{\sqrt{8}}(|000\rangle + |111\rangle)(|000\rangle + |111\rangle)(|000\rangle + |111\rangle)$$

$$|1\rangle_L = \frac{1}{\sqrt{8}}(|000\rangle - |111\rangle)(|000\rangle - |111\rangle)(|000\rangle - |111\rangle)$$

7 Qubit Steane Code (A. Steane 96)

Calderbank-Shor-Steane (CSS) codes

▶Examples – [7, 1, 3] Steane code



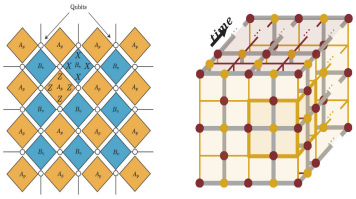
$$C = [[n, k, d]]$$

n : # of physical qubits
k : # of logical qubits
d : minimum distance in C
(minimum weight of logical gates)

Code rate ***R=k/n***
Correctable error ***t, d=2t+1***

Topological 2-D Code (A. Kitaev 97)

- defined over a 2-dim lattice of qubits



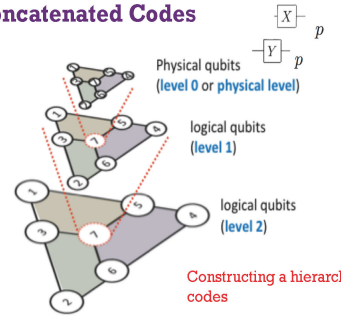
Toric, Surface (Planar Surface)

https://errorcorrectionzoo.org ; Various QEC code

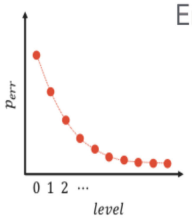
17/22

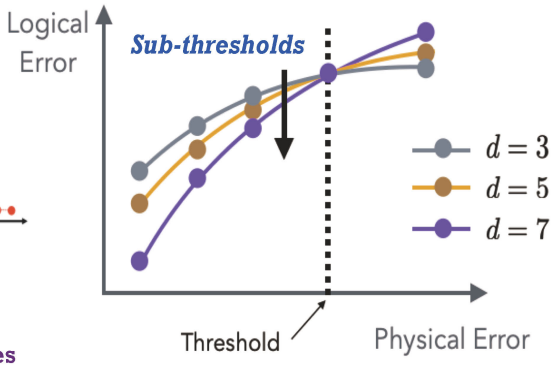
양자오류정정의 목표: 결함허용 달성 (시스템이 커져도 오류가 누적되지 않고 감소)

Concatenated Codes

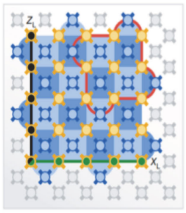


Constructing a hierarchy of codes

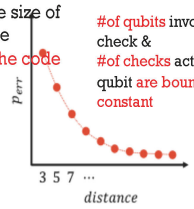




Quantum low-density parity check (qLDPC) codes



Increasing the size of the code while maintaining the code structure



#of qubits involved in each check &
#of checks acting on each qubit are bounded by a constant

Nature **614**, 676–681 (2023)

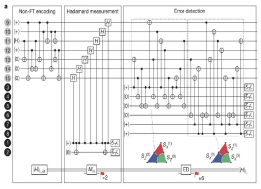
Goal of QEC is achieving **sub-thresholds**

= exponential suppression of logical errors as *d* increases

18/22

양자오류정정의 실험적인 구현: 기초적인 수준

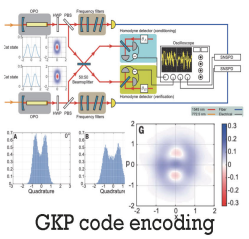
[Nature. 605, 675 (2022)]



7-qubit color code logical qubit and operation

Ion trap

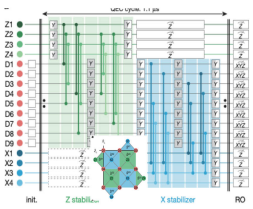
[Science. 383, 289 (2024)]



GKP code encoding

Photonic (Bosonic)

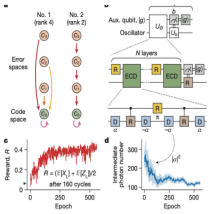
[Nature. 605, 669 (2022)]



17-qubit surface encoding

Superconducting

[Nature. 616, 50 (2023)]



GKP and real-time QEC

Superconducting (Bosonic)

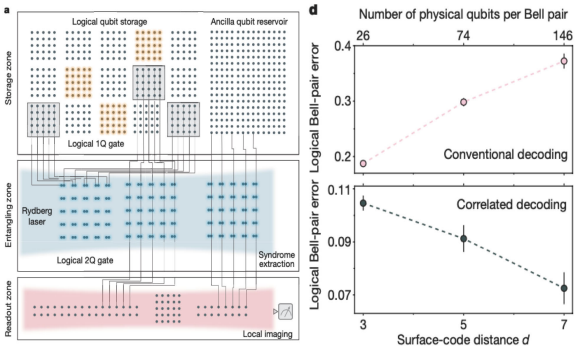
기초 QEC protocol/encoding 또는 Break-even 달성 데모 수준

* Break-even : 논리 큐비트 오류율이 물리 큐비트 오류율과 동률

[Nature. 626, 58 (2023)]

Article

Logical quantum processor based on reconfigurable atom arrays *Neutral Atoms*



- 280 개의 물리큐비트로 48개의 논리 큐비트 입력과(by 3D [[8,3,2]] detection code)과 효과적인 logical operation 구현

Up to 280 qubits (rubidium atoms trapped in 2D array)
- Surface code - Color code

Challenge: 느린 프로세스, 오류정정 반복 수행 어려움

19/22

Article

Quantum error correction below the surface code threshold

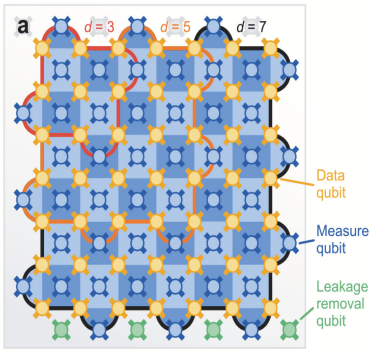
[Nature. 638, 920 (2025)]

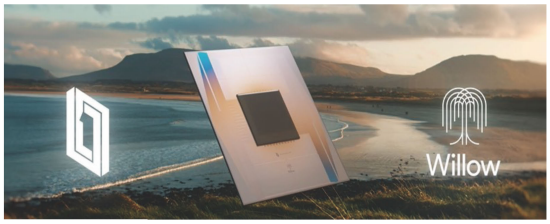
Google Quantum AI and Collaborators*

- 105개의 물리 큐비트로 1개의 논리 큐비트 구현
- 반복적인 오류정정 수행
- Leakage 오류 억제
- Distance 증가에도 오류의 지수적인 감소 달성

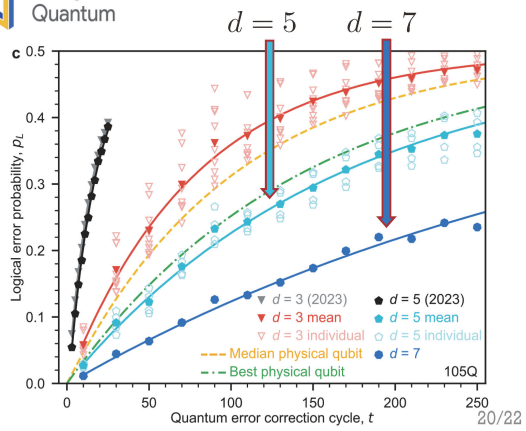
현재 달성 수준 =
메모리 역할
논리 큐비트 1개
반복 오류정정 수행

Superconducting qubits



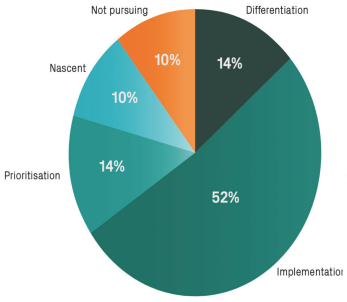


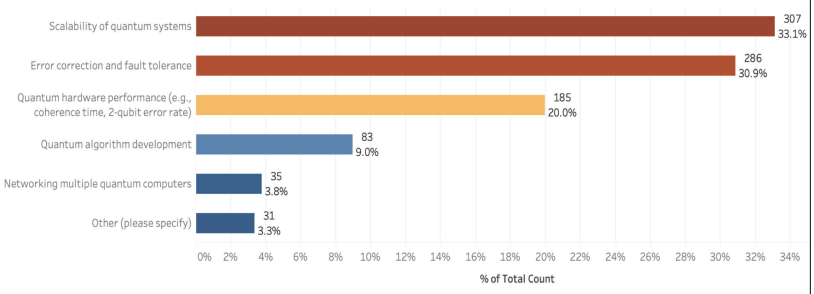
Google AI Quantum



20/22

글로벌 양자컴퓨팅 개발 로드맵 (NISQ → 결함허용 양자컴 FTQC by QEC)





29 Leading Quantum Computing Companies' approach to QEC (Riverlane report 2024.10),

Now, **most quantum computing companies are working on QEC.**

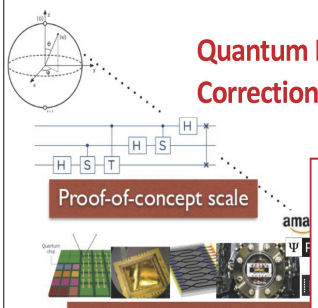
Only 10% hold the NISQ Strategy.

Survey on 'the most significant current challenges of Quantum Computing' (Quera survey 2024.7)

Majorities of quantum communities regard **the scalability and QEC are the most significant current challenges** in quantum computing.

21/22

Fault-tolerant 양자컴퓨팅 (FTQC)을 위한 해결 과제



Quantum Error Correction 필수!!

Proof-of-concept scale

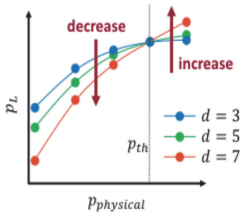
Noisy Intermediate-scale Quantum (NISQ) computer

Fault-tolerant Universal Quantum computers

"QEC era is just beginning"
Challenge toward FTQC

✓ *Sub-threshold*

- P < Pth
- 시스템(코드) Size가 커지며 오류 감소



서 발생하는 오류를 고려
게 증가 시킴

- [n,k,d] 코드에서 발생하는 m-bit 결과는 2^m가지의 신드롬 처리 필요
- d=5 Surface code [41,1,5]에서 $2^{40} = 10^{12}$ 데이터 처리

Minimum weight preface matching (MWPM) for Surface code

✓ *Overhead*

- 시간과 공간, 자원 Overhead가 Exponential 증가 문제
- Constant Scale을 위한 접근법 pLDPC but non-local connectivity

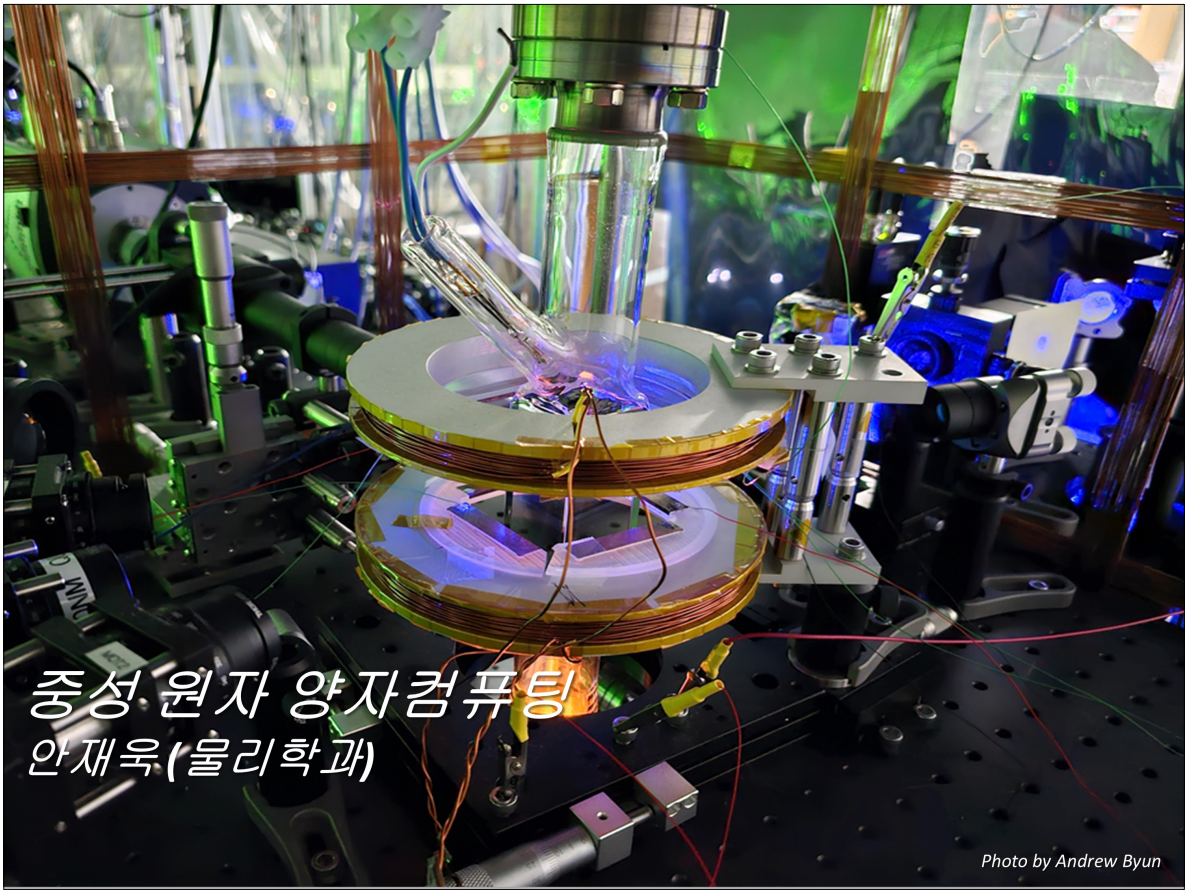
22/22

주제발표 2

중성원자 양자컴퓨팅

안 재 욱

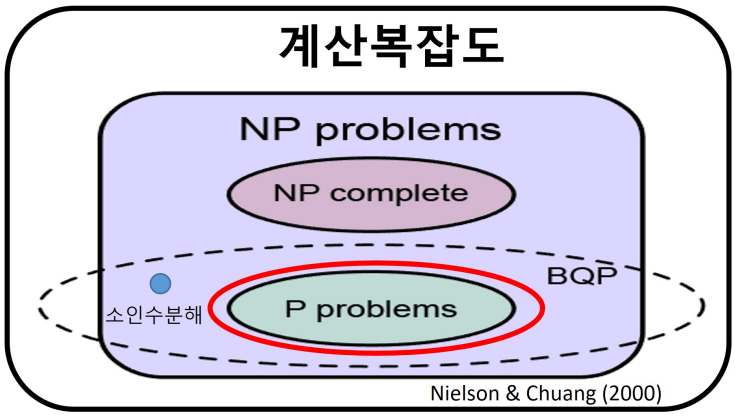
KAIST 물리학과 교수



양자컴퓨터가 무엇에 쓰는 물건인고?

1. 현재의 컴퓨터가 감당하지 못하는 문제를 계산하는 장치

   (a) 양자 문제
   (b) 고전 문제 중에서 계산복잡도가 높은 문제 (예, 조합최적화)



2. 양자물질을 만드는 장치 (양자 공작기계 = Quantum Mother Machine)

"중성 원자 양자컴퓨터"의 다른 이름

= 리드버그 양자 컴퓨터 **(Rydberg atom array)**
또는 광집게 트랩 양자 컴퓨터 **(optical tweezers)**

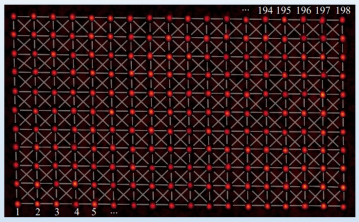
- 리드버그 원자 (Rydberg atom) : 마이크론 크기 원자 (주양자수 ~100)
- 광집게 트랩 (optical tweezer trap) : 현미경으로 개별 원자를 제어함

- 특징
  (1) 정확도 (accuracy)가 높다 ← 물리량의 유효자리수가 많다
  (2) 상대 정밀도 (dx/x)가 높다 ← 리드버그 원자의 크기(x)가 크다
  (3) 양자역학적 현상: 위상변화 = f (x, dx/x)

- 장점
  (1) 큐비트 개수가 매우 많다 (이미 6000개, 조만간 10,000개 돌파)
  (2) 해밀토니안이 NP-문제와 밀접하게 관련된다
  (3) 큐비트의 양자 계산중 재배치 (동적 큐비트)

- 단점 이면서 기회: 역사가 짧다 (10년), 연구자가 많지 않다 (한국은 상대적으로 풍부)

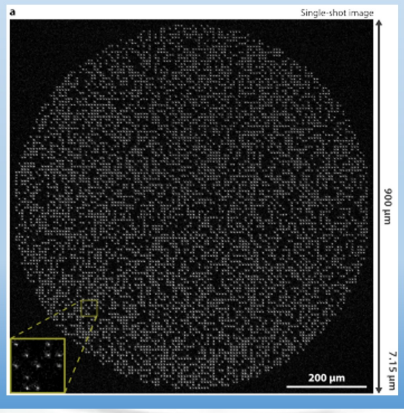
수백-수천개의 원자 큐비트를 활용



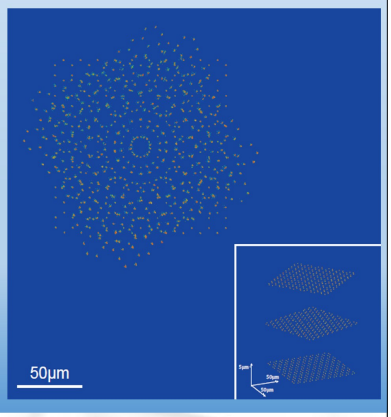
K. Kim et al., Scientific data 11, 111 (2024).

Paris-Saclay + Pasqal (2024).

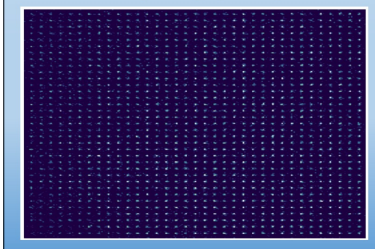
Caltech group (2024)



USTC (2025)

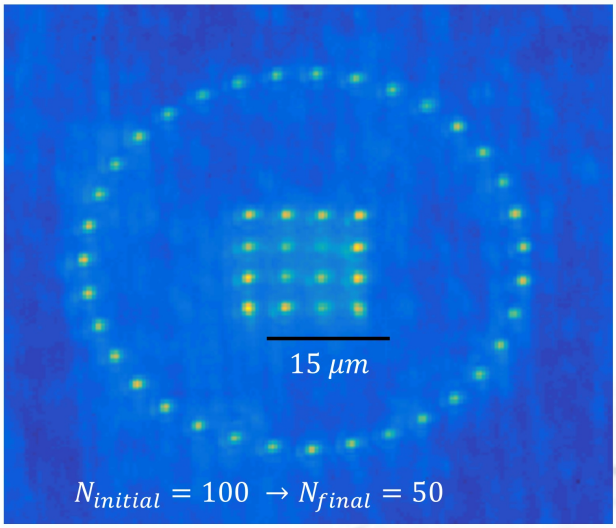


Atom computing (2024).



광집게 트랩으로 원자를 이동 배치

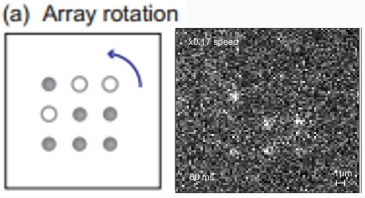
광집게를 제어하여 2차원에 원자 배치
간격 d = 2-10 μm, 위치 정밀도 Δx < 0.1 μm



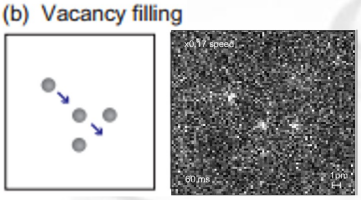
KAIST에서 최초 구현 (미국 특허 확보)

원자 테트리스 게임

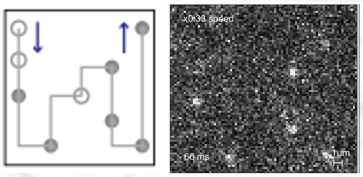
(a) Array rotation



(b) Vacancy filling

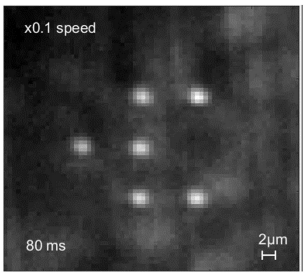


(c) "Worm running"



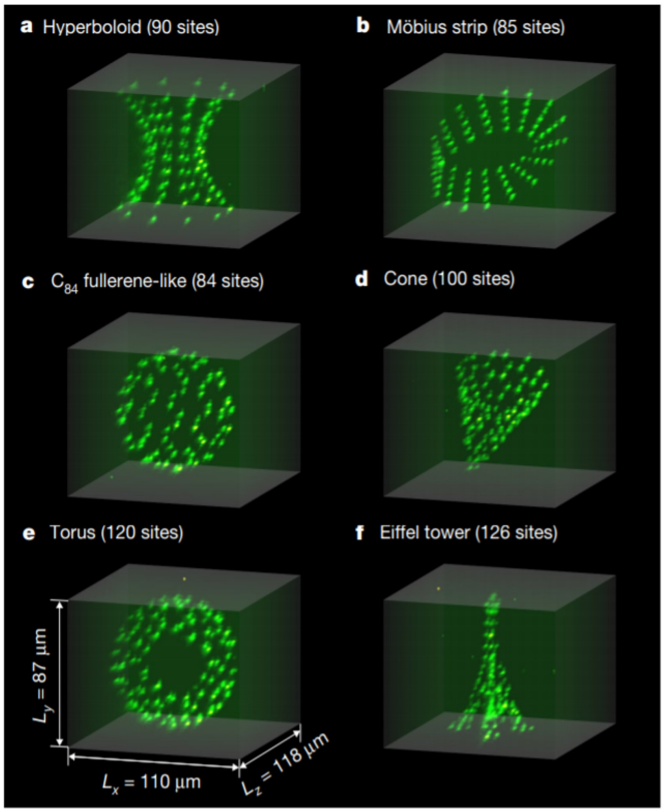
W. Lee, H. Kim, JA, Optics Express **24**, 9816 (2016).
H. Kim and W. Lee et al., Nature Comm. 7, 13316 (2016).

3차원 원자 배치



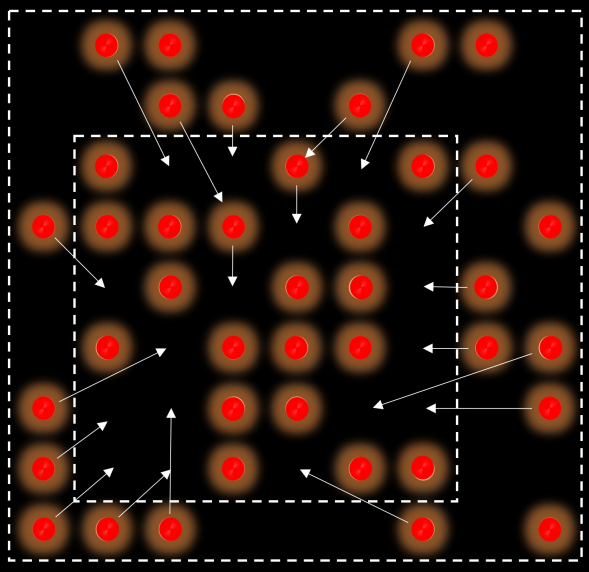
Lee et al., "3D rearrangement of single atoms using actively controlled optical microtraps,"Optics Express (2016).

Barredo et al., "Synthetic 3D atomic structures assembled atom by atom," Nature (2018).



광집게 원자열 구성 방법

1. 레이저 원자 냉각
2. 광집게 원자 포획
3. **원자 재배치 기술**
4. 원하는 원자열 구성



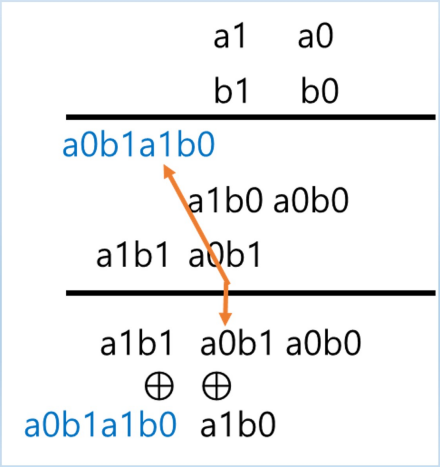
Hyosub Kim, Woojun Lee, et al., "In situ single-atom array synthesis using dynamic holographic optical tweezers," Nature Comm. 7, 13317 (2016). → US PATENT (2019)

원자를 배치하여 소인수 분해 문제를 프로그램하는 방법

6 = 2 x 3

$(N_2N_1N_0)_2 = (a_1a_0)_2(b_1b_0)_2$

multiplication table



① $N_0 = a_0b_0 = 0$

② $N_1 = a_0b_1 + a_1b_0 = 1$

③ $N_2 = a_1b_1 + a_0b_1a_1b_0 = 1$

Conjunctive normal form

$a_1b_1(\bar{a}_0 + \bar{b}_0)(a_0 + b_0) = 1$

SAT Boolean expression

$\boldsymbol{\Psi = C_1 \wedge C_2 \wedge C_3 \wedge C_4}$

$\boldsymbol{C_1} = a_1$

$\boldsymbol{C_2} = b_1$

$\boldsymbol{C_3} = \bar{a}_0 \vee \bar{b}_0$

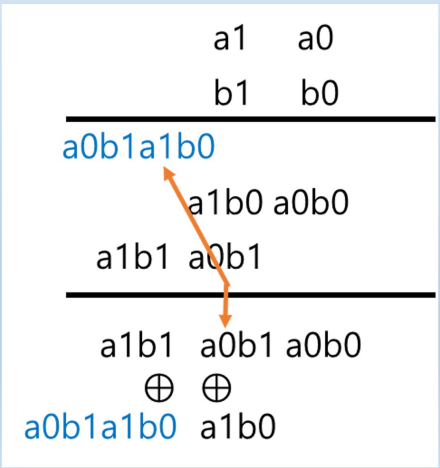
$\boldsymbol{C_4} = a_0 \vee b_0$

원자를 배치하여 소인수 분해 문제를 프로그램하는 방법

6 = 2 x 3

$(N_2N_1N_0)_2 = (a_1a_0)_2(b_1b_0)_2$

multiplication table



① $N_0 = a_0b_0 = 0$

② $N_1 = a_0b_1 + a_1b_0 = 1$

③ $N_2 = a_1b_1 + a_0b_1a_1b_0 = 1$

Conjunctive normal form

$a_1b_1(\bar{a}_0 + \bar{b}_0)(a_0 + b_0) = 1$

SAT Boolean expression

$\boldsymbol{\Psi = C_1 \wedge C_2 \wedge C_3 \wedge C_4}$

$\boldsymbol{C_1} = a_1$

$\boldsymbol{C_2} = b_1$

$\boldsymbol{C_3} = \bar{a}_0 \vee \bar{b}_0$

$\boldsymbol{C_4} = a_0 \vee b_0$

원자를 배치하여 소인수 분해 문제를 프로그램하는 방법

$$6 = 2 \times 3$$

$$(N_2N_1N_0)_2 = (a_1a_0)_2(b_1b_0)_2$$

① $N_0 = a_0b_0 = 0$

② $N_1 = a_0b_1 + a_1b_0 = 1$

③ $N_2 = a_1b_1 + a_0b_1a_1b_0 = 1$

Conjunctive normal form

$$a_1b_1(\bar{a}_0 + \bar{b}_0)(a_0 + b_0) = 1$$

SAT Boolean expression

$$\Psi = C_1 \wedge C_2 \wedge C_3 \wedge C_4$$

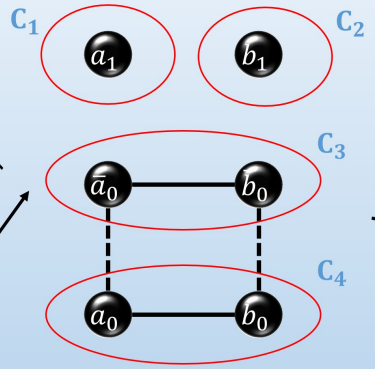
$$C_1 = a_1$$

$$C_2 = b_1$$

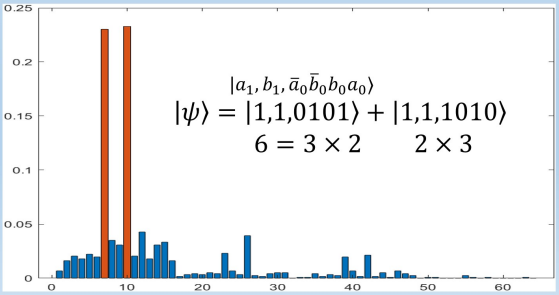
$$C_3 = \bar{a}_0 \vee \bar{b}_0$$

$$C_4 = a_0 \vee b_0$$

MIS graph

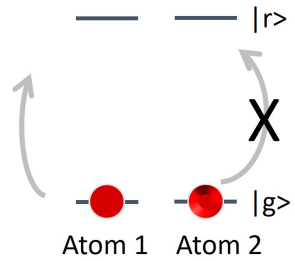


Many-body ground states



Jeong et al., "Quantum computing of 3-SAT…", (2022).

리드버그 원자(마이크로 미터 크기)의 강한 상호작용 → 양자 얽힘



리드버그 원자 쌍극자 봉쇄 현상
Rydberg-atom dipole-blockade effect

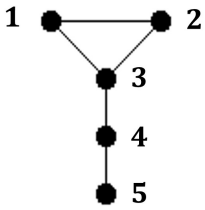
2큐비트 양자 얽힘 상태

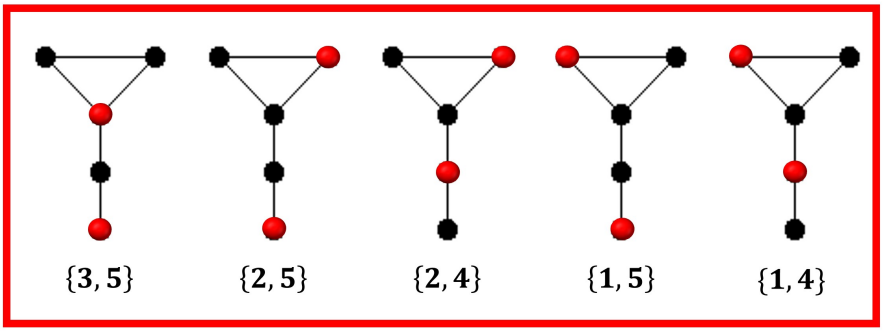
$$|\psi_{12}\rangle = \sqrt{1/2}\,(|g\rangle_1|r\rangle_2 + |r\rangle_1|g\rangle_2)$$

최대 독립집합 문제 : NP-완전 문제

최대독립집합 문제는 주어진 그래프 G (V,E)의 독립집합(간선으로 연결되지 않은 않은 꼭지점) 중 제일 큰 것을 구한다 → 조합최적화 문제의 대표적 예

$G = \overline{P}_{g6:DKs}$



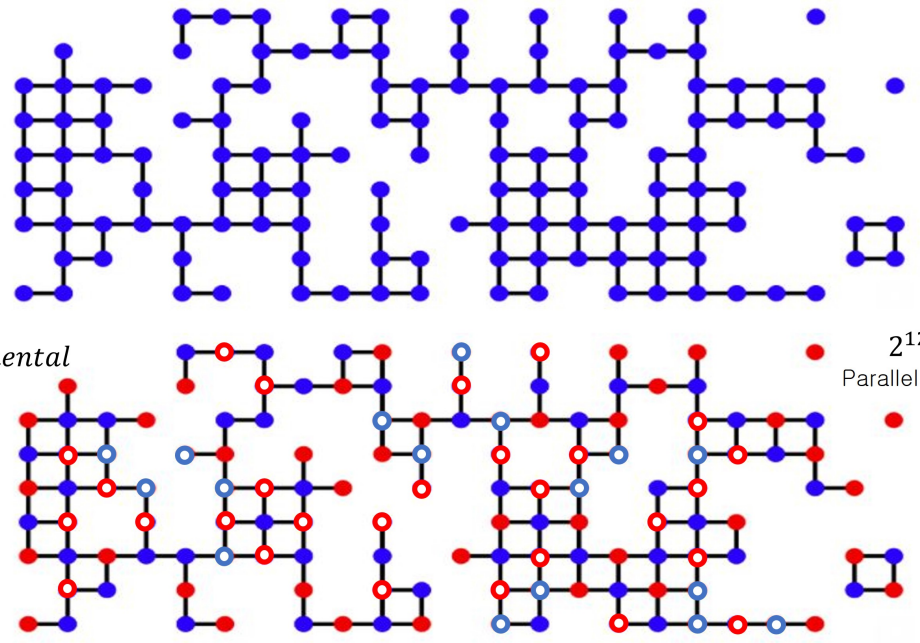


Max-independent-Set (MIS) : $\{3,5\},\{2,5\},\{2,4\},\{1,5\},\{1,4\}$
MISL (length of MIS) = 2

최대독립집합문제는 NP-완전문제의 하나로, 효율적인 고전 알고리듬이 없음
리드버그 원자 그래프의 해밀토니안은 최대독립집합과 밀접하게 관련됨

* H. Pichler, S. Choi, et al., arXiv:1808.10816 (2018).

126개의 원자의 양자얽힘 실험 → 최대독립집합을 계산함



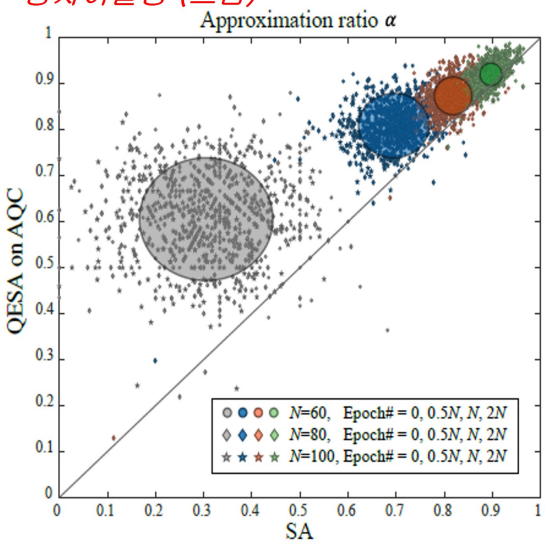
Experimental

$2^{126} = 10^{38}$
Parallel computing

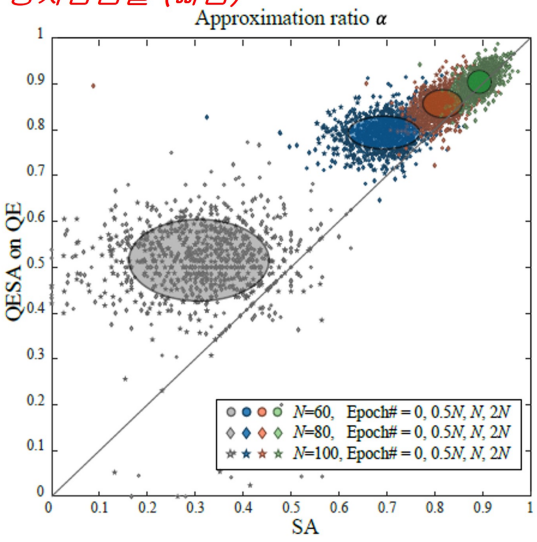
양자실험으로 시작하는 "Warm-Start" 방식의 고전컴퓨팅
"양자" 컴퓨팅 = 전처리 + 양자 컴퓨팅 + 후처리

노이즈가 있는 양자 컴퓨팅 데이터를 고전 컴퓨팅의 입력으로 사용한다

양자어닐링 (느림)



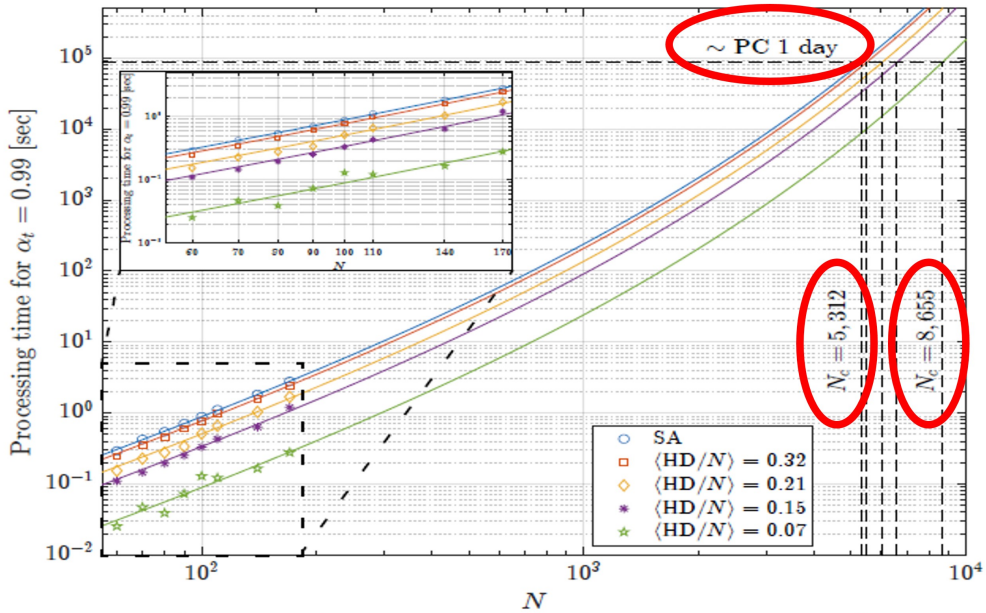
양자담금질 (빠름)



Seokho Jeong et al., "Quantum-enhanced simulated annealing using Rydberg atoms," preprint (2025).

양자컴퓨터(QPU)를 슈퍼컴퓨터의 가속 장치로 활용

Preliminary estimation: Need around 5000 atom graphs



Seokho Jeong et al., "Quantum-enhanced simulated annealing using Rydberg atoms," preprint (2025).

결론:

(1) 중성 원자 양자컴퓨터가 주목(?) 받고 있다.

(2) 발전 속도가 매우 빠르다.

(3) 독특한 물리적 장점이 있다.
- 시스템 확장성이 매우 좋다
- 다체 해밀토니안에 조합최적화 문제와 관련된다.
- 동적 큐비트 아키텍처에 적합하다.

(4) 학술적, 기술적, 상업적 활용도가 있다.

(5) 한국이 상대적으로 잘하는(?) 양자컴퓨터 기술분야다.

“중성 원자 양자컴퓨팅” 발표 개요

발표자: 안재욱 (KAIST 물리학과 교수)

표지 사진 : 중성 원자 양자컴퓨터 실험 장치

양자컴퓨터란?

- (1) 양자문제 계산 장치
- (2) NP문제 계산 장치
- (3) 다체 양자상태 생성·제어 공작기계

중성 원자 양자컴퓨터

- 리드버그 양자컴퓨터, 광집게 트랩 양자컴퓨터와 동일
- **특징**: 높은 정확도와 상대 정밀도
- **장점**:
  큐비트 확장성 우수
  해밀토니안이 NP 문제와 관련
  동적 큐비트 재배치 가능 등
- **단점**: 급부상한 분야로 상대적으로 낮은 인지도

최근 연구 동향 (2024년)

- 100 큐비트급 양자계산 시연
- 1000개급 원자 배열 달성

기술 설명

- 원자 재배치 기술 (KAIST 최초 개발)
- 3차원 원자 배치 가능
- 광집게로 원자를 포획·배치
- 예제: 소인수분해 문제를 계산하는 원자 배열
- 리드버그 상호작용을 이용해 양자 얽힘 생성
- 원자 간 상호작용 → 최대 독립집합(Maximal Independent Set) 문제와 관련

연구 사례

- 126개 원자의 양자 얽힘 실험
- 양자실험 결과를 “Warm-Start” 기법에 활용

활용 전망 : 양자컴퓨터를 슈퍼컴퓨터 가속기로 활용 (추정)

결론 : 중성 원자 양자컴퓨터가 주목받고 있음

주제발표 3
이온 트랩 양자컴퓨팅

김 기 환

Tsinghua University 물리학과 교수

제235회 한림원탁토론회: 흥미로운 양자기술 ±20년

이온트랩 양자컴퓨팅

2025년 5월 9일

김기환

칭화대학교 물리학과

清華大學物理系

Department of Physics, Tsinghua University

2001 KIAS 양자 컴퓨터 양자정보학회

Workshop on Quantum Computation and Quantum Information

November 1-3, 2001
KIAS International Conference Hall, Seoul, Korea

Invited Speakers

- Bouwmeester, D. (Univ. of Oxford, UK)
- Cirac, I. (Univ. of Innsbruck, Austria)
- Ekert, A. K. (Univ. of Oxford, UK)
- Gilbert, G. (MITRE, US)
- Long, G.-L. (Tsinghua Univ., China)
- Polzik, E. S. (Univ. of Aarhus, Denmark)

http://conf.kias.re.kr/QuantumComp/

이온트랩 양자컴퓨팅 – 최초로 제안된 양자컴퓨터 플랫폼 (1995)

VOLUME 74, NUMBER 20 PHYSICAL REVIEW LETTERS 15 MAY 1995

Quantum Computations with Cold Trapped Ions

J. I. Cirac and P. Zoller*
Institut für Theoretische Physik, Universität Innsbruck, Technikerstrasse 25, A-6020 Innsbruck, Austria
(Received 30 November 1994)

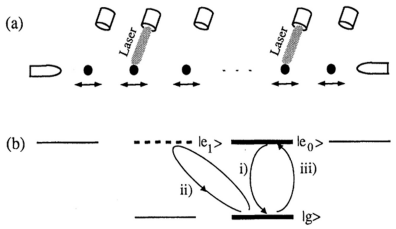


FIG. 1. (a) N ions in a linear trap interacting with N different laser beams; (b) atomic level scheme.

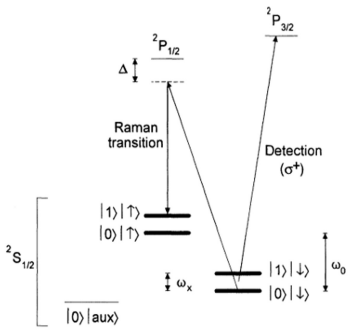
양자컴퓨터 플랫폼으로
이온트랩이 최초로 제안됨

VOLUME 75, NUMBER 25 PHYSICAL REVIEW LETTERS 18 DECEMBER 1995

Demonstration of a Fundamental Quantum Logic Gate

C. Monroe, D. M. Meekhof, B. E. King, W. M. Itano, and D. J. Wineland
National Institute of Standards and Technology, Boulder, Colorado 80303
(Received 14 July 1995)

We demonstrate the operation of a two-bit "controlled-NOT" quantum logic gate, which, in conjunction with simple single-bit operations, forms a universal quantum logic gate for quantum computation. The two quantum bits are stored in the internal and external degrees of freedom of a single trapped atom, which is first laser cooled to the zero-point energy. Decoherence effects are identified for the operation, and the possibility of extending the system to more qubits appears promising.

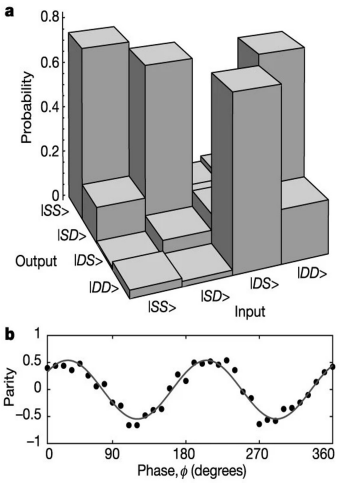


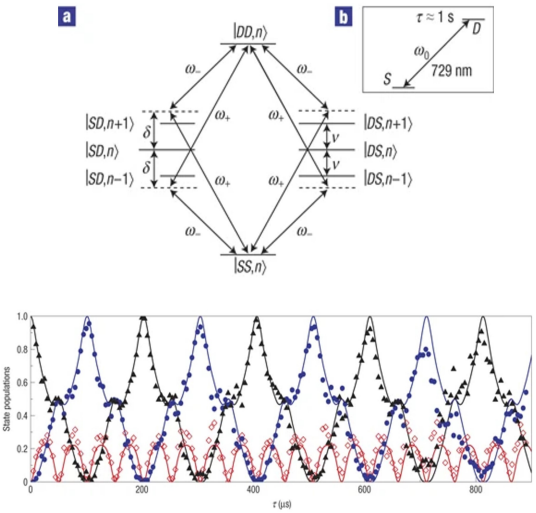
Input state → Output state

$|0\rangle|\downarrow\rangle \rightarrow |0\rangle|\downarrow\rangle$
$|0\rangle|\uparrow\rangle \rightarrow |0\rangle|\uparrow\rangle$
$|1\rangle|\downarrow\rangle \rightarrow |1\rangle|\uparrow\rangle$
$|1\rangle|\uparrow\rangle \rightarrow |1\rangle|\downarrow\rangle$.

단일 이온 + 단일 진동모드 이용
CNOT gate 구현함

두 이온간의 양자게이트 구현





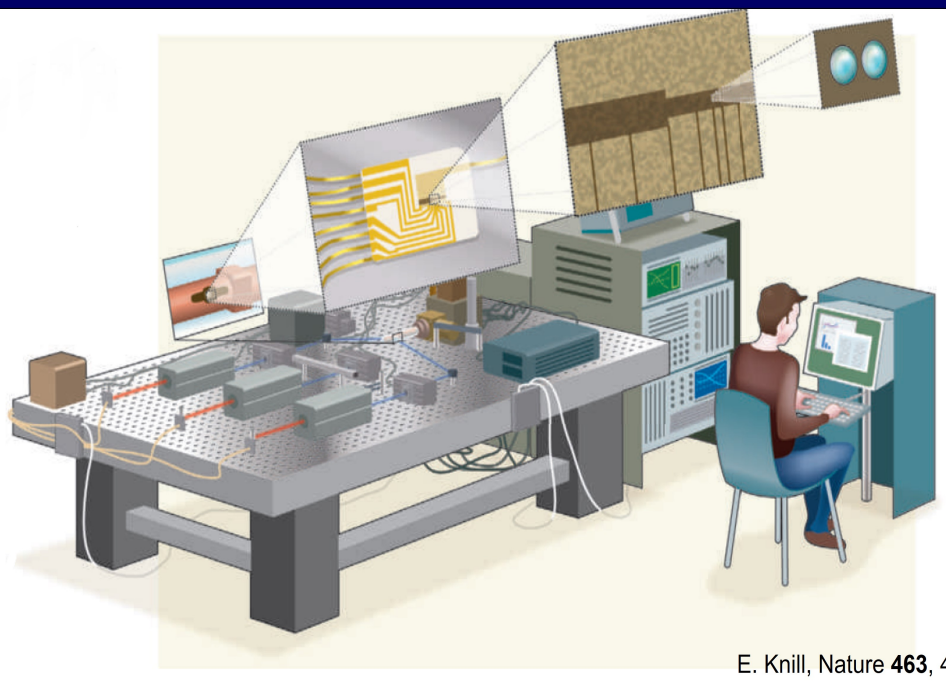
게이트 성공률 71%

Innsbruck group, Nature 422, 408 (2003)

게이트 성공률 99.2%

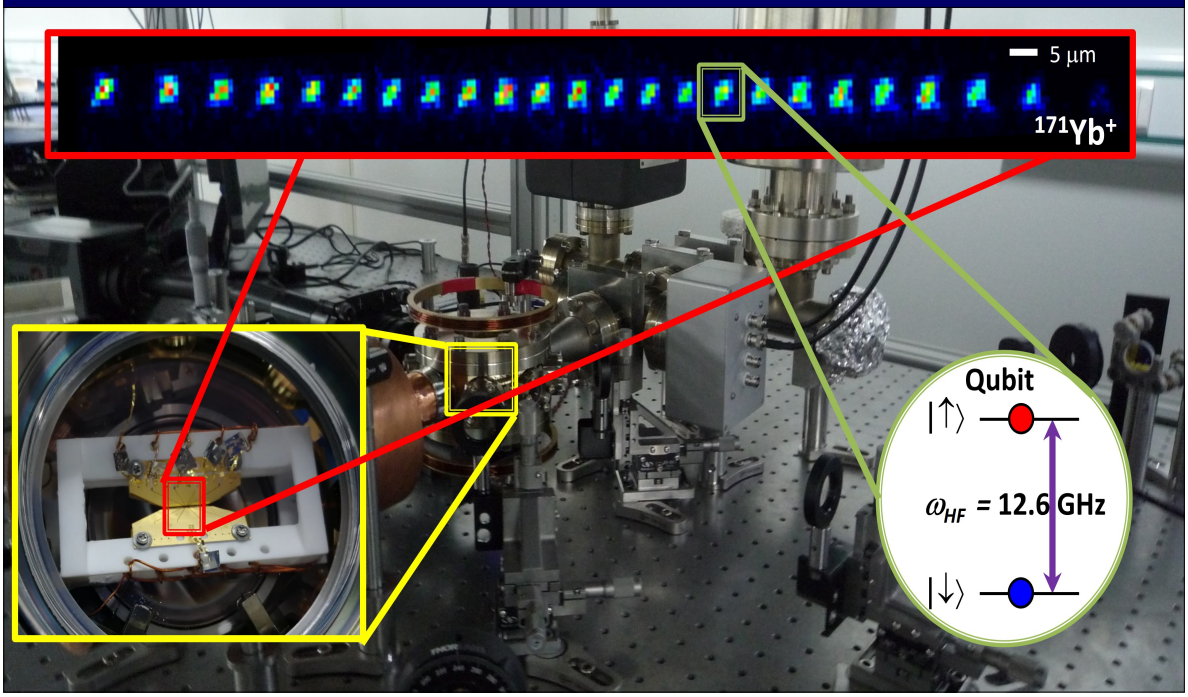
Innsbruck group, Nat. Phys. 422, 408 (2008)

이온트랩 양자컴퓨터 개념도

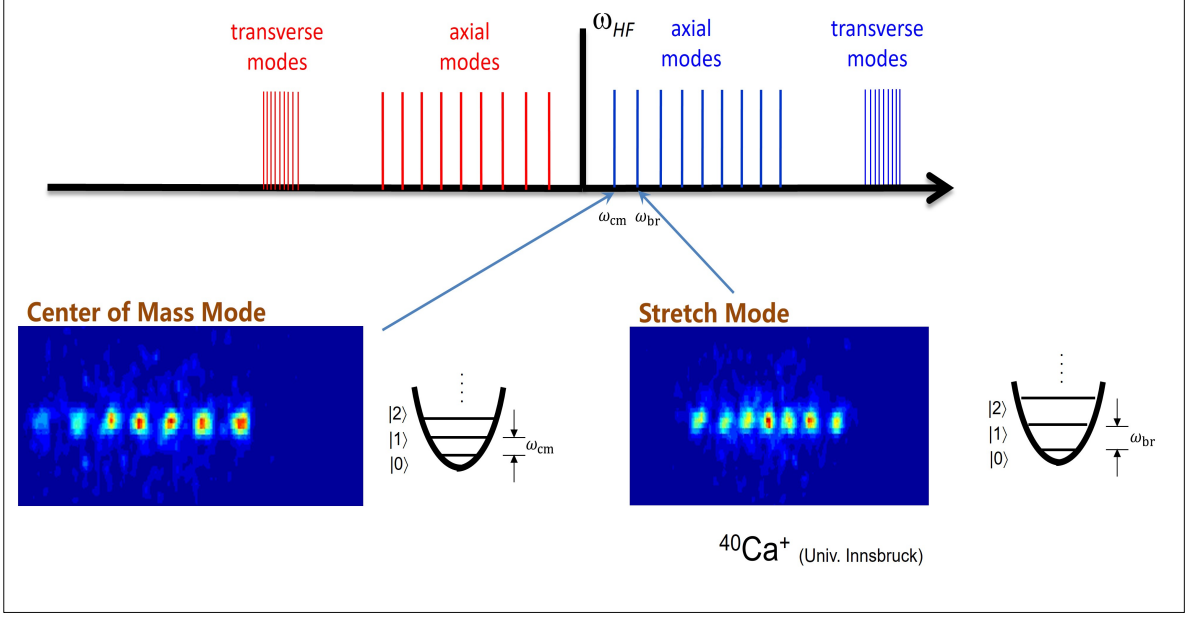


E. Knill, Nature **463**, 441 (2010).

이온트랩장치 Ion Trap System @ Tsinghua

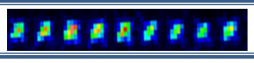


Ion Trap System – vibrational modes

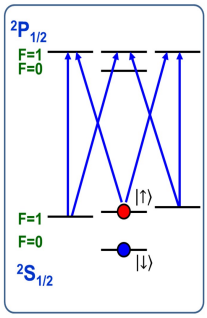


Basic Procedure of Trapped Ion Quantum Computation

1. Doppler Cooling and Ground State Cooling < 1 mK



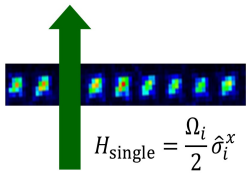
2. Initialization
by optical pumping



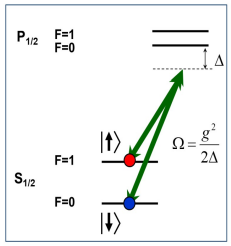
- Duration ~ 1 μs
- Efficiency ~ 99.5%

3. Quantum Operations

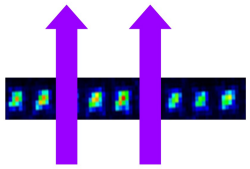
1) Single-qubit gate



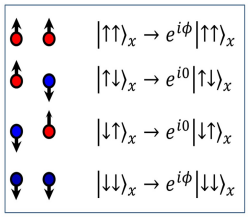
$$H_{\text{single}} = \frac{\Omega_i}{2}\hat{\sigma}_i^x$$



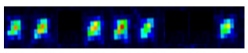
2) Two-qubit gate



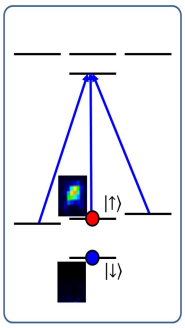
$$H_{\text{two}} = J_{3,5}\hat{\sigma}_3^x\hat{\sigma}_5^x$$



4. Detection



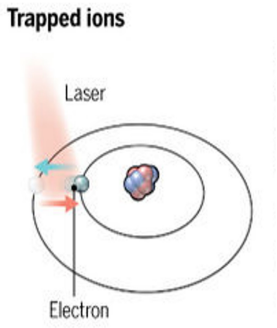
$|\uparrow\rangle$ $|\uparrow\rangle|\downarrow\rangle|\uparrow\rangle|\uparrow\rangle|\uparrow\rangle|\downarrow\rangle|\downarrow\rangle$ $|\uparrow\rangle$



- Duration ~ 0.4 ms
- Efficiency ~ 98.5%

S. Olmschenk, et al., PRA **76**, 052314 (2007)

Experimental Platform – Trapped Ions

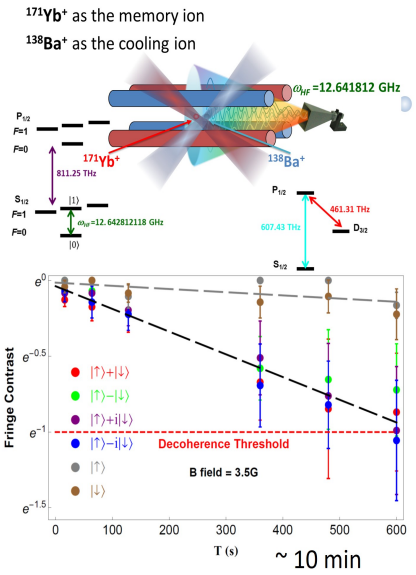


Coherence time (s) ≈ 5500 s
Two-qubit gate fidelity> 99.97%
Entangled qubit number: 50
Quantum volume: 2^{21} (Quantinuum)
Algorithmic qubit: 35 (IonQ)

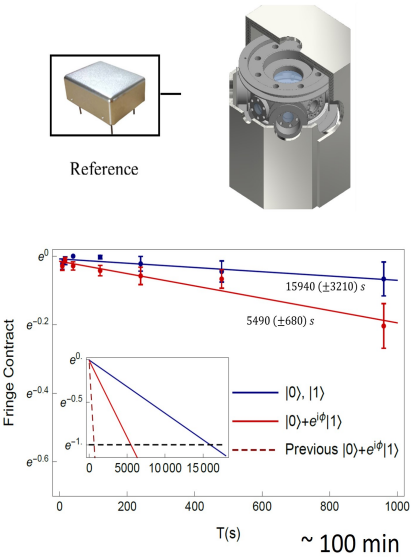
@2024 Dec

- **Coherence time 중첩유지 시간**
  10s (NIST), 50s (Oxford), 600s and 5500s (Tsinghua)
- **Two-qubit gate fidelity 연산 정확도**
  99.9% (NIST, Oxford), 99% (Tsinghua)
  99.9% (Tsinghua using error mitigation methods)
  99.94% (GTRI), 99.97% (Oxford Ionics)
- **Qubit numbers 큐빗수**
  - **Entanglement**
    50 (Quantinuum), 24 (Innsbruck), 9 (Tsinghua), 6 (Mainz), 5 (UMD), 4 (NIST, Tsinghua)
  - **Universal quantum computation**
    56 (Quantinuum), 35 (IonQ), ~20 (Duke), ~20 (Innsbruck)
  - **Quantum simulation**
    53 (UMD), ~50 (Innsbruck), ~16 (Tsinghua)

World Record of Coherene Time

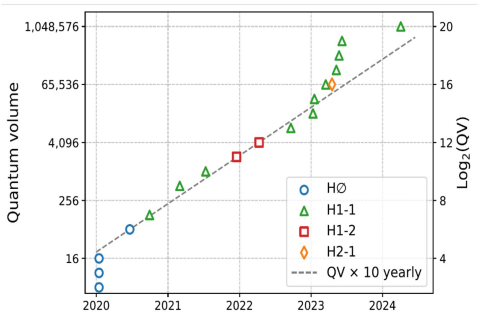


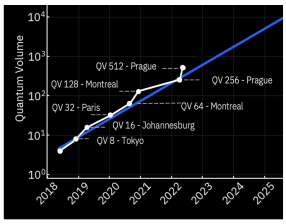
Y. Wang, et al., Nature Photon. 11, 646 (2017)



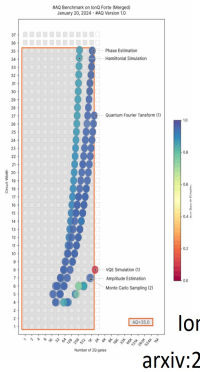
P. Wang, et al., Nature Commun. 12, 233 (2021)

Quantum volume



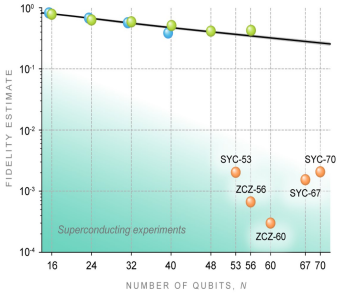


Algorithmic Qubit



IonQ (2024)
arxiv:2308.05071

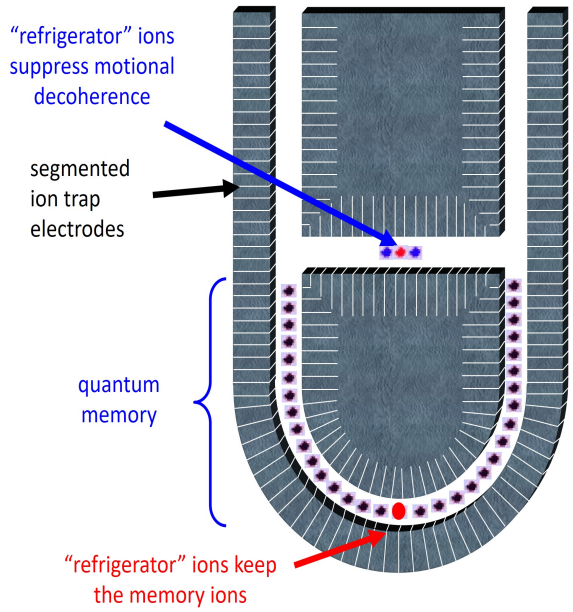
Random Gate Sampling

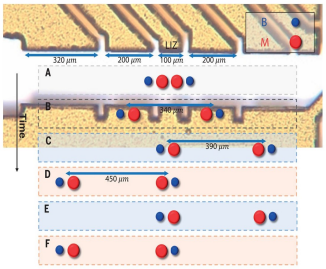


Quantinuum (2024)
arxiv:2406.02501

Scale up by Shuttling Ions

D. Kielpinski, et al. Nature 417, 709 (2002)

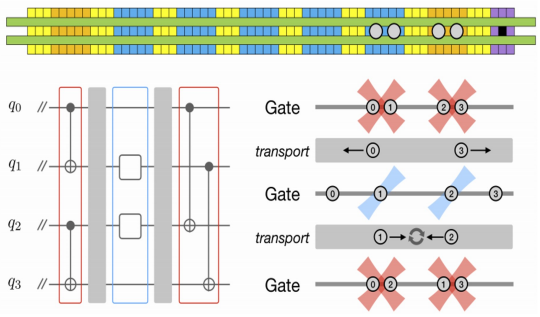




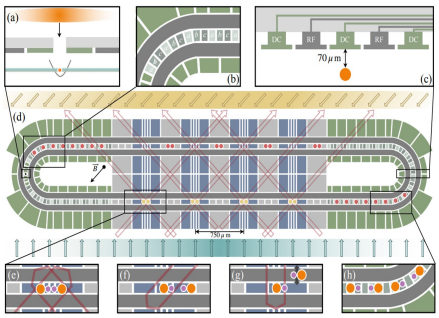
PRL **96**, 253003 (2006)
PRL **102**, 153002 (2009)
Nature **459**, 683 (2009)
Science **325**, 1227 (2009)
Nature Phys. **6**, 13 (2010)
Nature **471**, 197 (2011)
Nature **476**, 181 (2011)
Nature **504**, 415 (2013)
Nature **512**, 57 (2014)
Nature **528**, 380 (2015)
…
Science **364**, 875 (2019)
…

Quantinuum Quantum Roadmap
https://www.quantinuum.com/

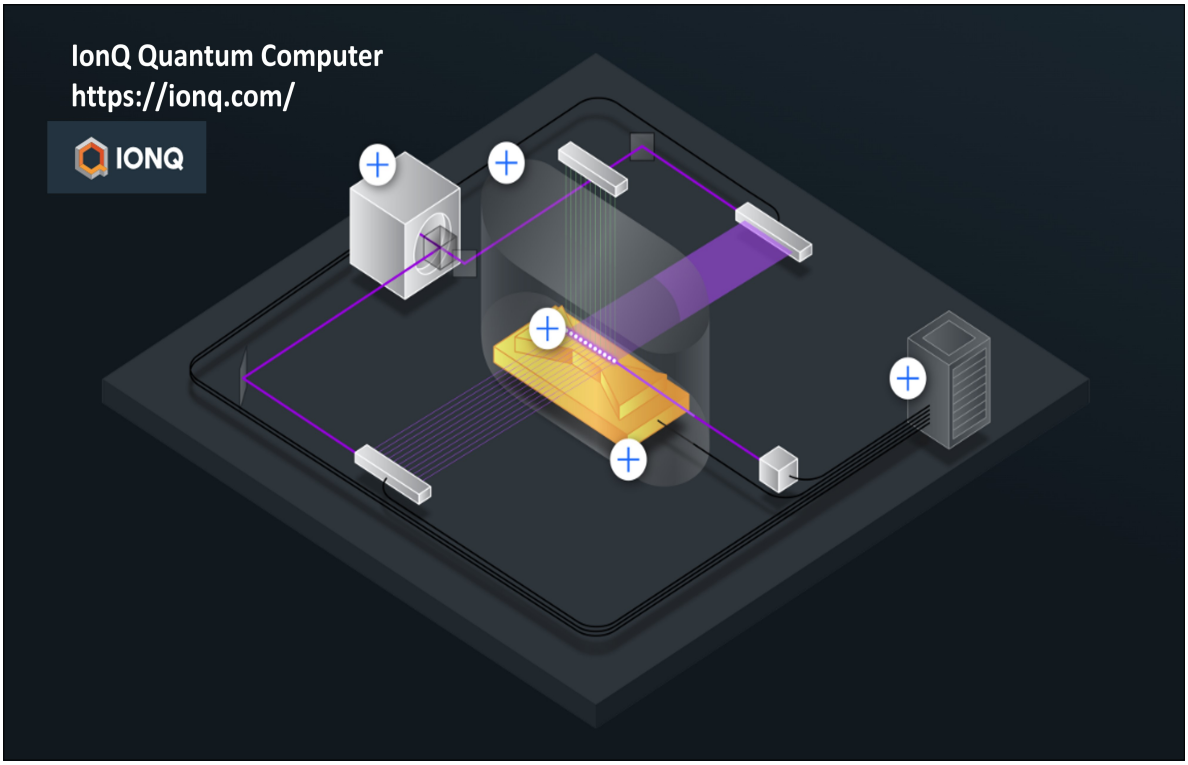
	2020	2023	2025	2027	2029
	H1	H2	HELIOS	SOL	APOLLO
PHYSICAL QUBITS:	20	56	96	192	1000's
PHYSICAL 2-QUBIT GATE ERROR:	1×10^{-3}	1×10^{-3}	$< 5 \times 10^{-4}$	$< 2 \times 10^{-4}$	1×10^{-4}
LOGICAL QUBITS:		> 12	~ 50	~ 100	100's
LOGICAL ERROR RATES:		1×10^{-3}	$< 10^{-4}$	$\sim 10^{-5}$	1×10^{-5} to $1 \times 10^{-10*}$

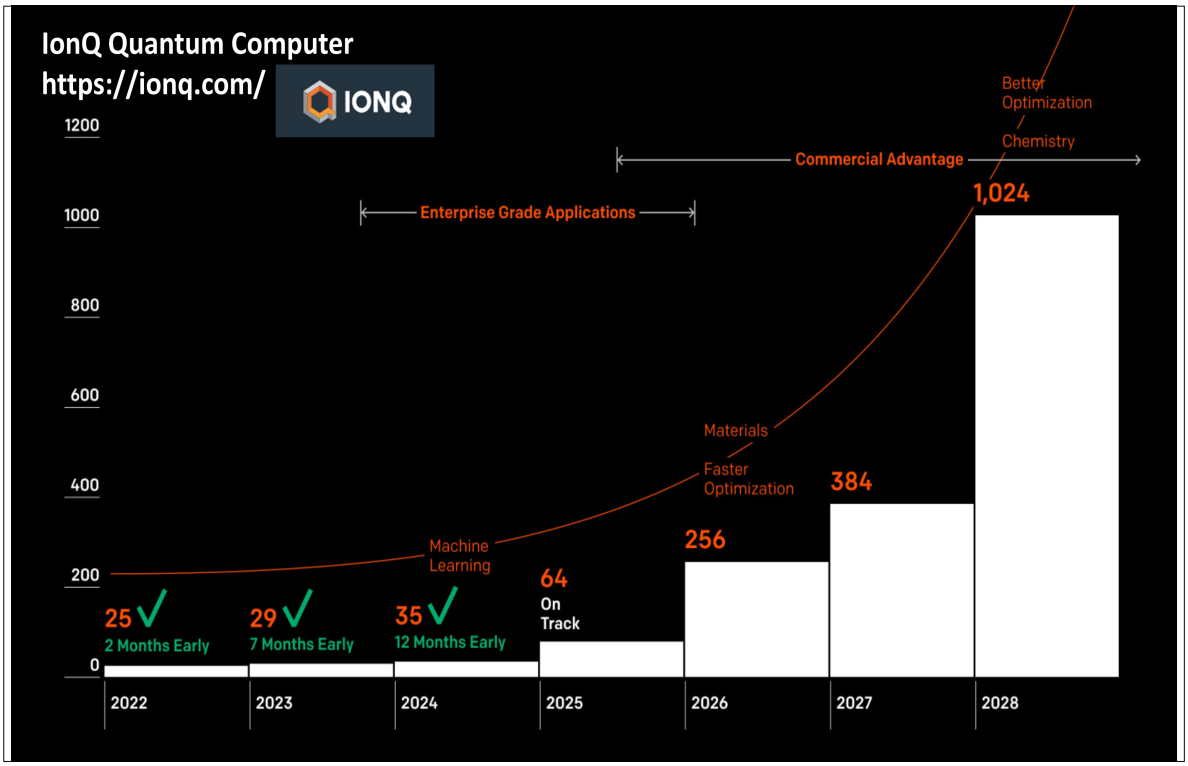


Demonstration of the trapped-ion quantum CCD computer architecture, Nature 592, 209 (2021).

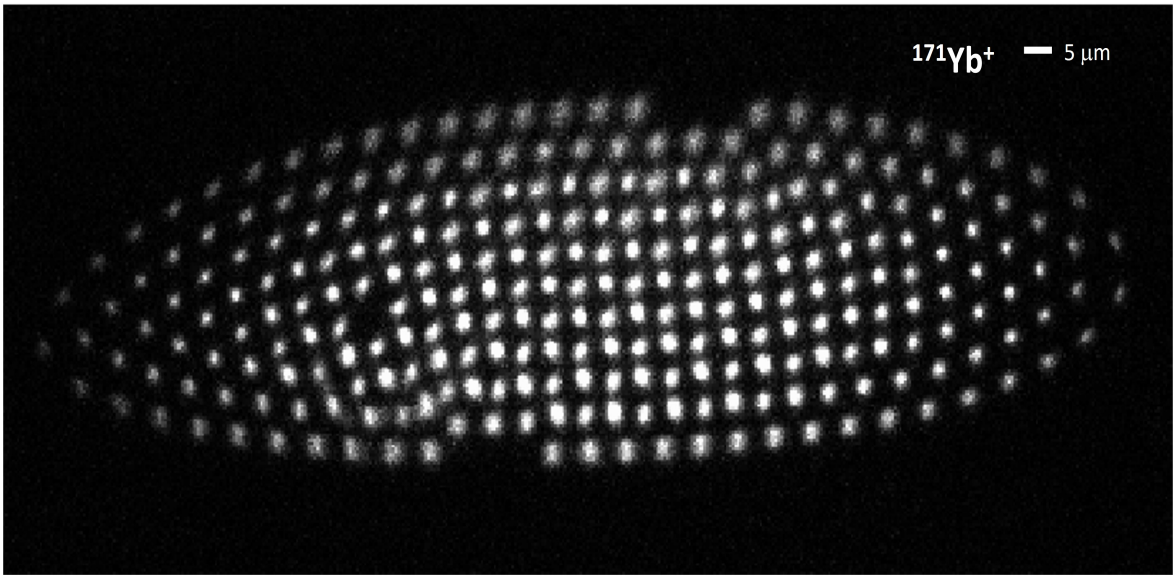


A Race Track Trapped-Ion Quantum Processor, PRX (2024) arXiv:2305.03828


IonQ Quantum Computer
https://ionq.com/
IONQ

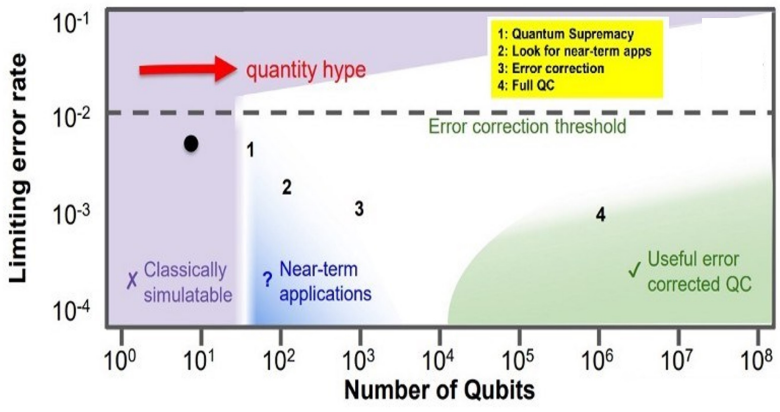

IonQ Quantum Computer
https://ionq.com/
IONQ
1200
1000
800
600
400
200
0
Commercial Advantage
Enterprise Grade Applications
Better Optimization
Chemistry
Materials
Faster Optimization
Machine Learning
25
2 Months Early
29
7 Months Early
35
12 Months Early
64
On Track
256
384
1,024
2022
2023
2024
2025
2026
2027
2028

2D crystal of ions



20년후?

- 이온 트랩을 이용한 궁극적인 양자컴퓨터의 실현을 위해서는 앞으로 가야할 길이 많이 남이있다.
- 발전이 느린 것처럼 보이지만 많은 연구가 활발히 이루어지고 있으며 곳곳에서 놀라운 발전이 계속 발표되고 있다.
- 다양한 분야들의 인재들이 양성되고 협력하여 돌파구들을 이룰 필요가 있다.



주제발표 4
양자통신 및 보안

배 준 우

KAIST 전기 및 전자공학부 교수

Quantum Communication & Security

Joonwoo Bae

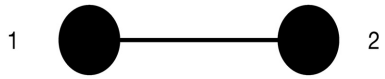
Korea Advanced Institute of Science and Technology (KAIST)

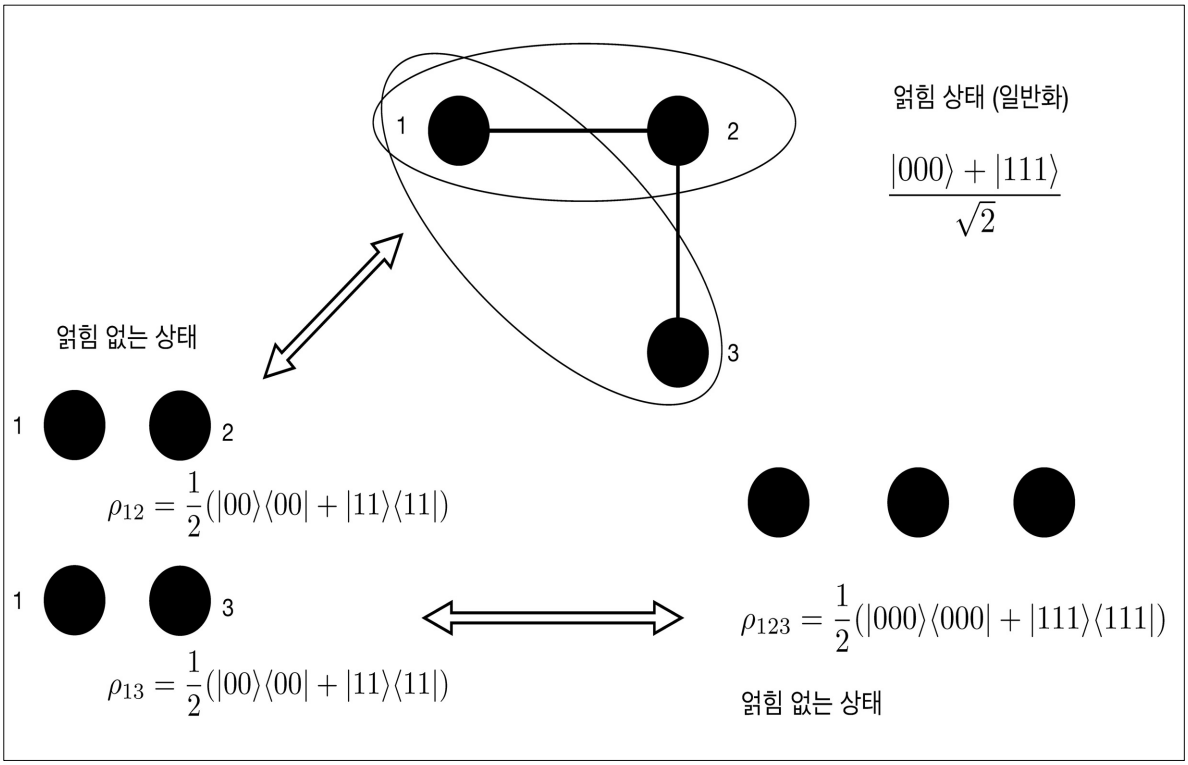
KAIST

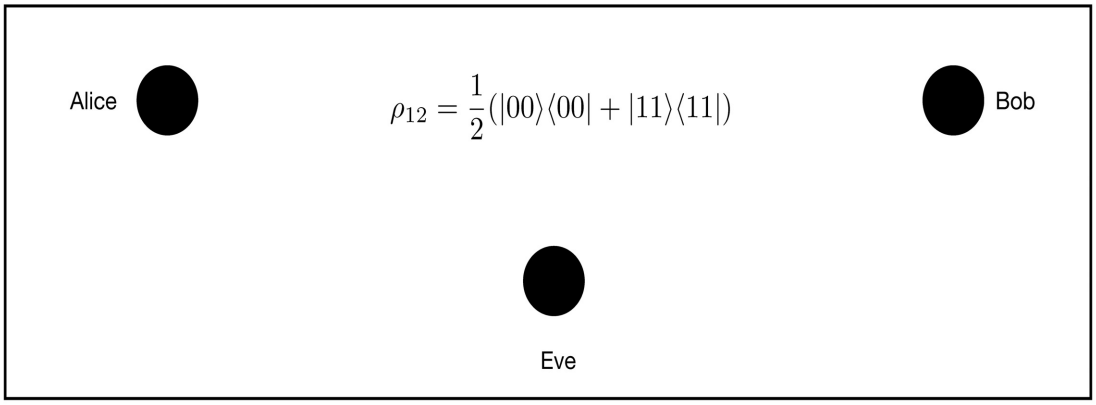
Quantum Information ±20 Years @ KAST

1 Entangled Bit (EBIT)

$$\phi^+ = \frac{|00\rangle + |11\rangle}{\sqrt{2}}$$





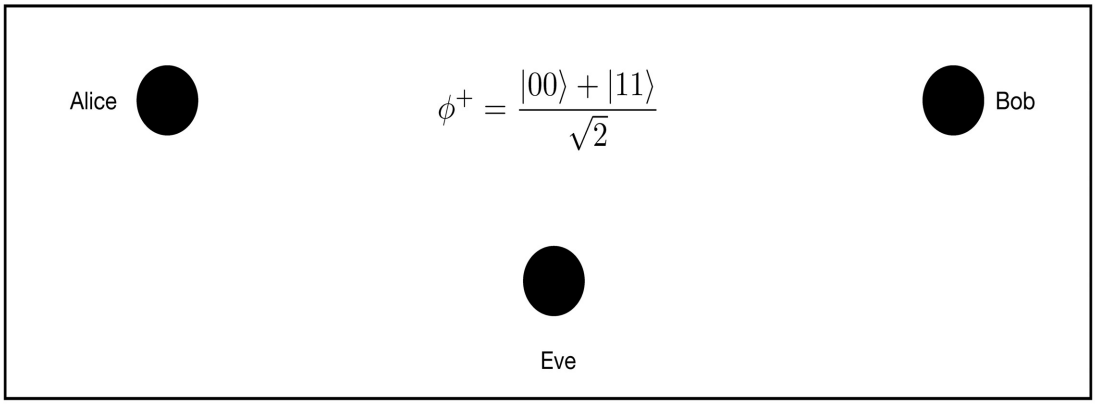


$$\rho_{12} = \frac{1}{2}(|00\rangle\langle 00| + |11\rangle\langle 11|)$$

가능한 확장 상태 $\dfrac{|000\rangle + |111\rangle}{\sqrt{2}}$

Eve knows all about Alice and Bob

$$\rho_{123} = \frac{1}{2}(|000\rangle\langle 000| + |111\rangle\langle 111|)$$

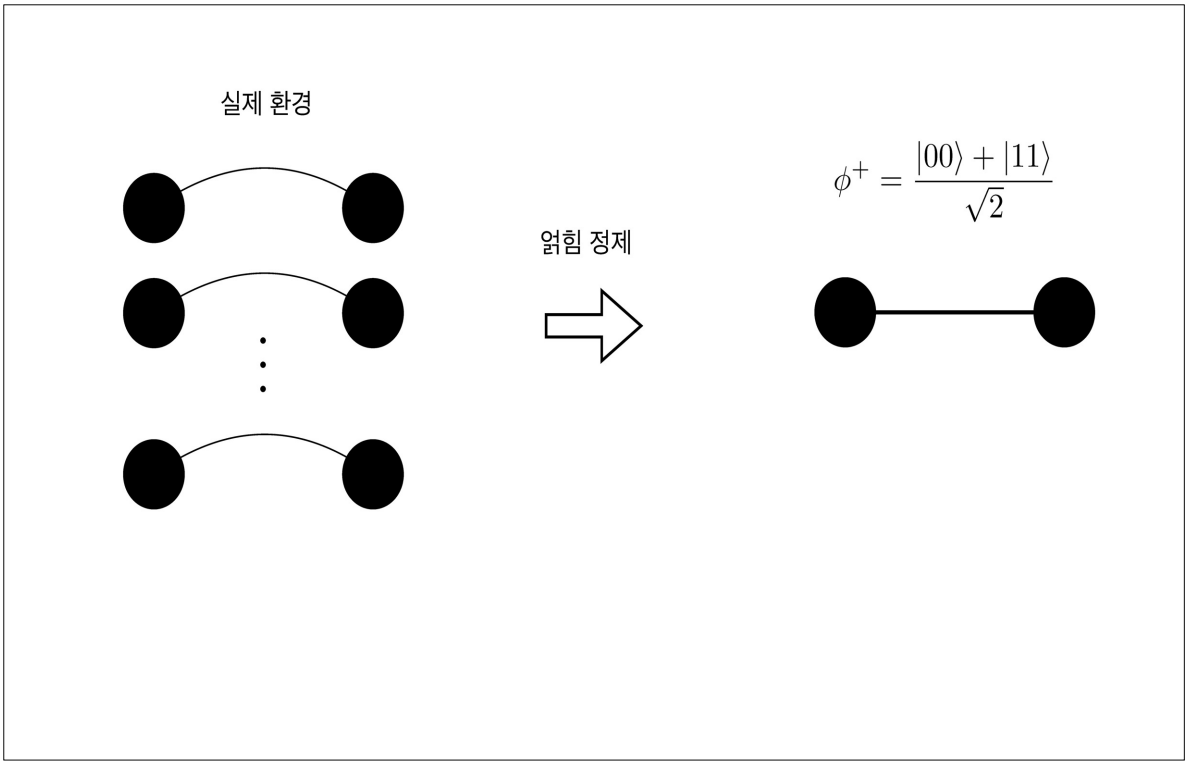


$$\phi^+ = \frac{|00\rangle + |11\rangle}{\sqrt{2}}$$

유일한 확장 상태 $\rho_{ABE} = |\phi^+\rangle_{AB}\langle\phi^+| \otimes \rho_E$ Eve is independent to Alice & Bob

$$\Longleftrightarrow \quad p(ABE) = p(AB)p(E)$$

Privacy, information-theoretic security (정보이론적 보안성)



프로토콜: 이론

1998

Purification of Noisy Entanglement and Faithful Teleportation via Noisy Channels

Charles H. Bennett[1], Gilles Brassard[2], Sandu Popescu[3], Benjamin Schumacher[4], John A. Smolin[5], and William K. Wootters[6]

Show more

Phys. Rev. Lett. **76**, 722 – **Published 29 January, 1996** | Erratum Phys. Rev. Lett. **78**, 2031 (1997)

DOI: https://doi.org/10.1103/PhysRevLett.76.722

Quantum Privacy Amplification and the Security of Quantum Cryptography over Noisy Channels

David Deutsch[1], Artur Ekert[1], Richard Jozsa[2], Chiara Macchiavello[1], Sandu Popescu[3], and Anna Sanpera[1]

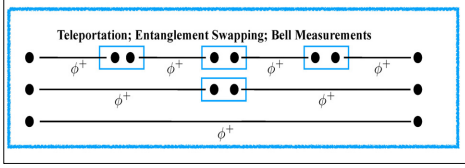
Show more

Phys. Rev. Lett. **77**, 2818 – **Published 23 September, 1996** | Erratum Phys. Rev. Lett. **80**, 2022 (1998)

DOI: https://doi.org/10.1103/PhysRevLett.77.2818

Quantum Repeaters: The Role of Imperfect Local Operations in Quantum Communication

H.-J. Briegel, W. Dür, J. I. Cirac, and P. Zoller
Phys. Rev. Lett. **81**, 5932 – Published 28 December 1998



PoC: 양자 광학
(원자, 광자)

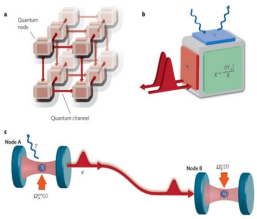
2010

Review Article | Published: 18 June 2008

The quantum internet

H. J. Kimble

Nature **453**, 1023–1030 (2008) | Cite this article



Letter | Published: 05 October 2006

Quantum teleportation between light and matter

Jacob F. Sherson, Hanna Krauter, Rasmus K. Olsson, Brian Julsgaard, Klemens Hammerer, Ignacio Cirac & Eugene S. Polzik

Nature **443**, 557–560 (2006) | Cite this article

Letter | Published: 02 June 2013

Deterministic quantum teleportation between distant atomic objects

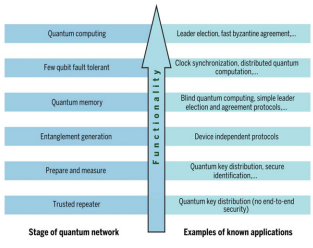
H. Krauter, D. Salart, C. A. Muschik, J. M. Petersen, Heng Shen, T. Fernholz & E. S. Polzik

Nature Physics **9**, 400–404 (2013) | Cite this article

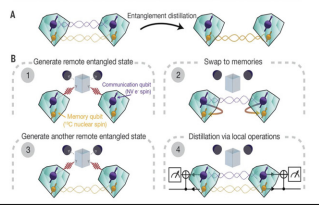
PoC: 고체

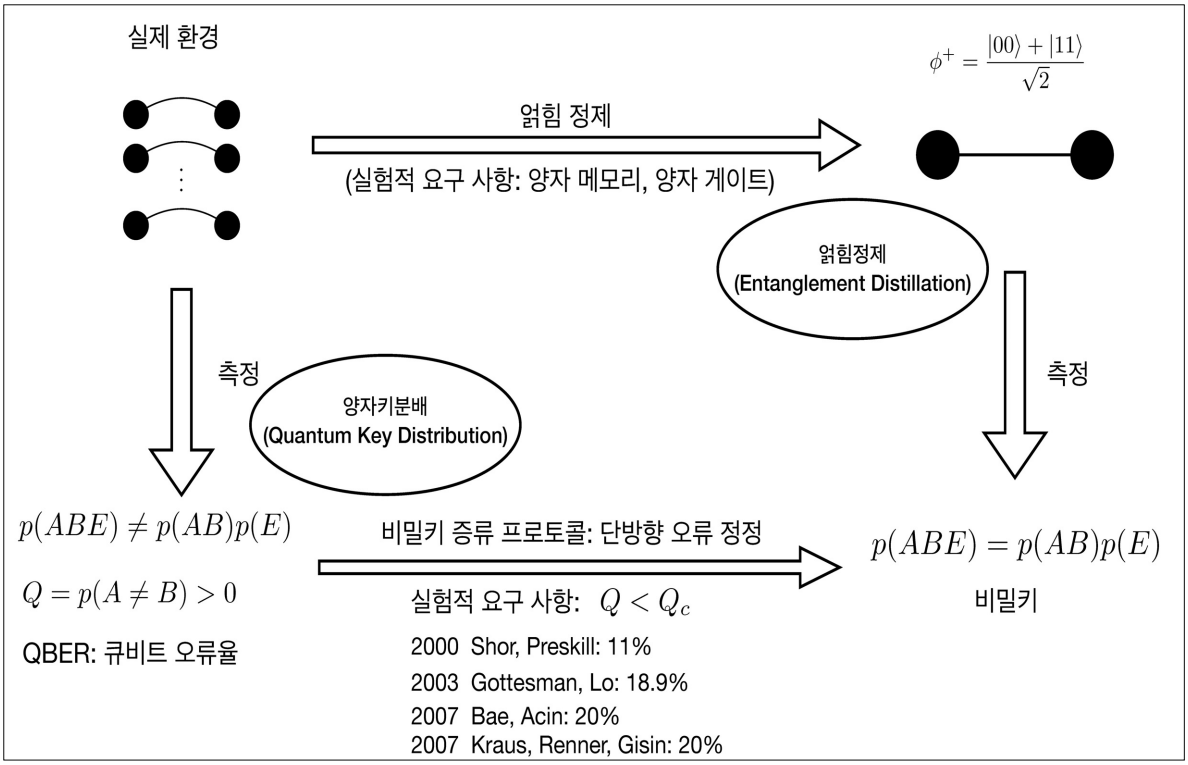
2020

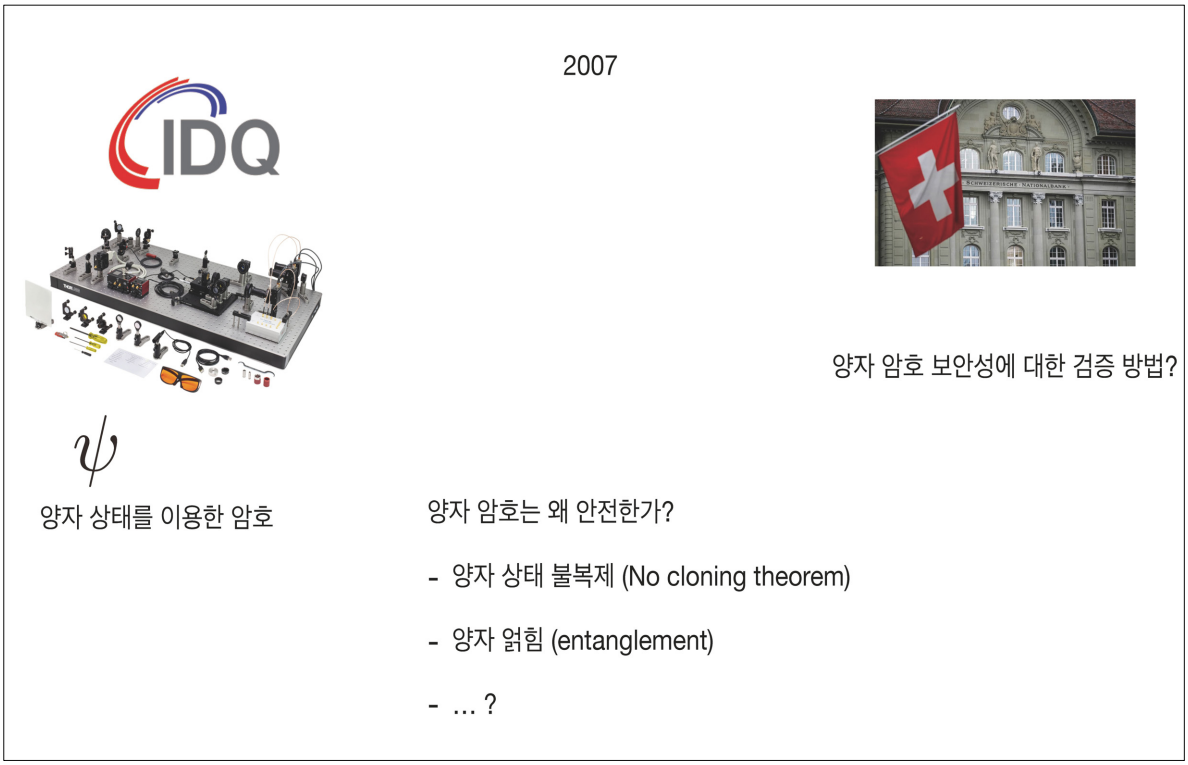
Quantum internet: A vision for the road ahead



Entanglement distillation between solid-state quantum network nodes

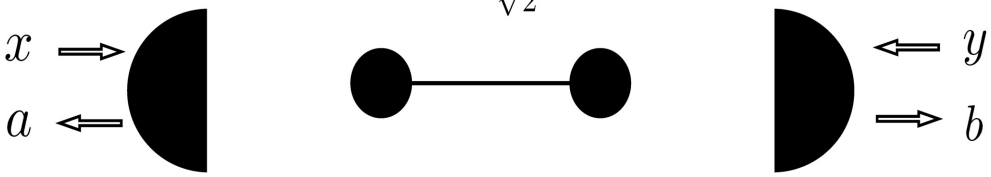



실제 환경
$\phi^+ = \frac{|00\rangle + |11\rangle}{\sqrt{2}}$
얽힘 정제
(실험적 요구 사항: 양자 메모리, 양자 게이트)
얽힘정제
(Entanglement Distillation)
측정
양자키분배
(Quantum Key Distribution)
측정
$p(ABE) \neq p(AB)p(E)$
$Q = p(A \neq B) > 0$
QBER: 큐비트 오류율
비밀키 증류 프로토콜: 단방향 오류 정정
실험적 요구 사항: $Q < Q_c$
2000 Shor, Preskill: 11%
2003 Gottesman, Lo: 18.9%
2007 Bae, Acin: 20%
2007 Kraus, Renner, Gisin: 20%
$p(ABE) = p(AB)p(E)$
비밀키


2007
IDQ
양자 암호 보안성에 대한 검증 방법?
ψ
양자 상태를 이용한 암호
양자 암호는 왜 안전한가?
- 양자 상태 불복제 (No cloning theorem)
- 양자 얽힘 (entanglement)
- ... ?

공유한 양자 상태를 검증: 검증 프로토콜

$$\phi^+ = \frac{|00\rangle + |11\rangle}{\sqrt{2}}$$



물리적으로 검증할 수 없는 사실:

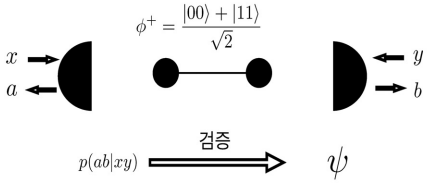
양자 상태 (힐베르트 공간)의 차원

$$p(ab|xy) \xrightarrow{\text{검증}} (U \otimes V)\frac{1}{\sqrt{2}}(|0_d 0_d\rangle + |1_d 1_d\rangle) \approx \phi^+$$

$$\sum_{abxy} (-1)^{a+b+xy} p(ab|xy) = 2\sqrt{2}$$

양자 암호 프로토콜 (보안성)

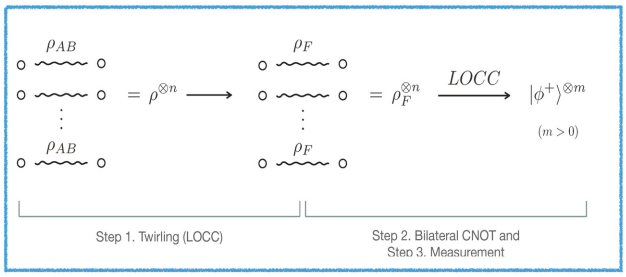
2000	2010	2020
양자 채널 잡음: $Q < Q_c$	검증 가능 프로토콜	네트 워크 확장 가능성
2000 Shor, Preskill: 11%	장치-무관 양자암호 (Device-independnet QKD)	거리 증가: Twin-Field QKD
2003 Gottesman, Lo: 18.9%	측정-장치-무관 양자암호 (Measurement-device-independnet QKD)	네트워크 확장
2007 Bae, Acin: 20%		네트워크 보안
2007 Kraus, Renner, Gisin: 20%		“Composability”



양자 상태 검증

얽힘 증류 -> 보안성

얽힘 정제



Quantum repeaters based on entanglement purification

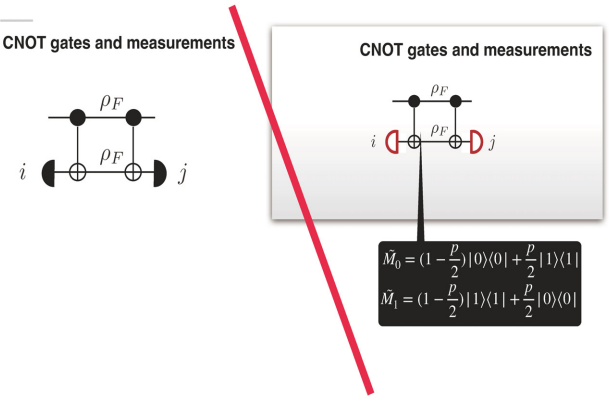
W. Dür[1], H.-J. Briegel[1,2,*], J. I. Cirac[1], and P. Zoller[1]

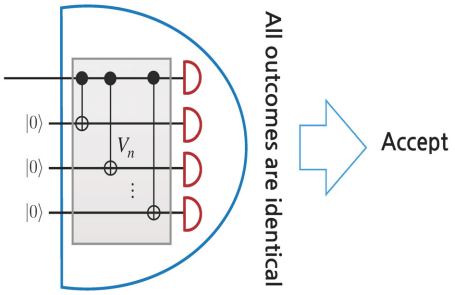
Show more

Phys. Rev. A **59**, 169 – **Published 1 January, 1999** | Erratum Phys. Rev. A **60**, 725 (1999)

DOI: https://doi.org/10.1103/PhysRevA.59.169

잡음있는 측정을 통해 얽힘 정제 불가능 영역 존재

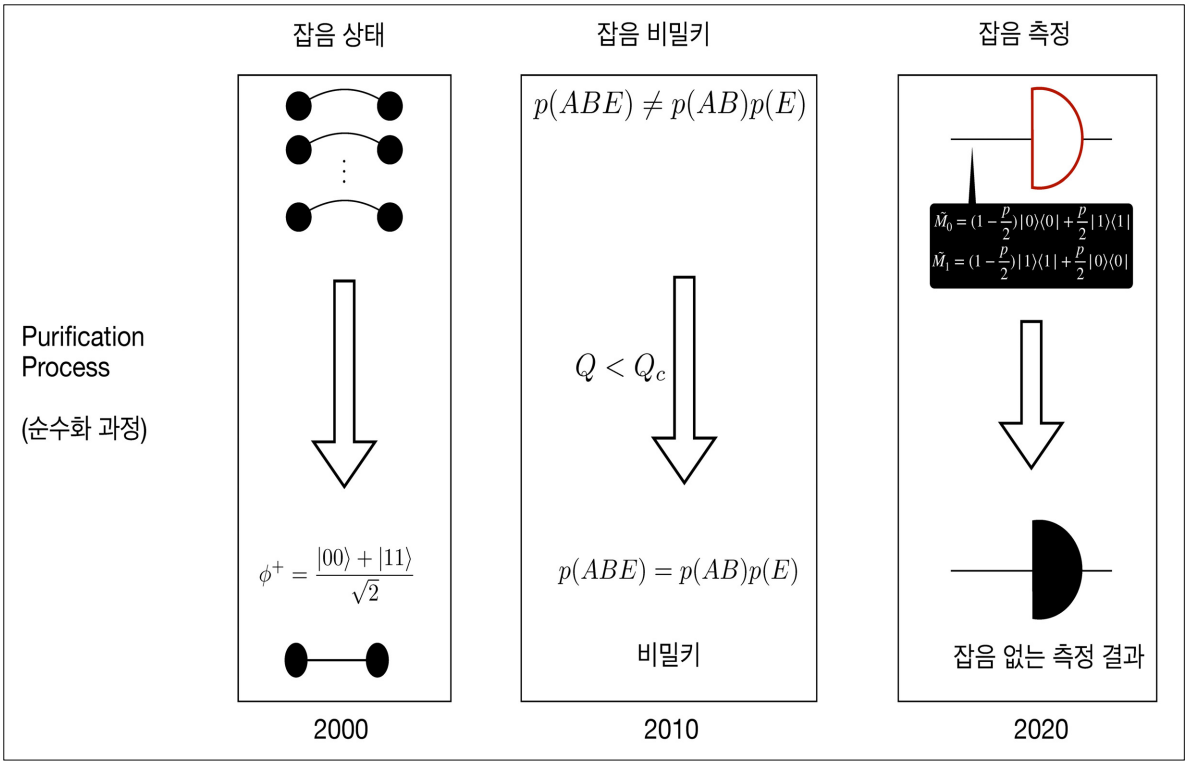


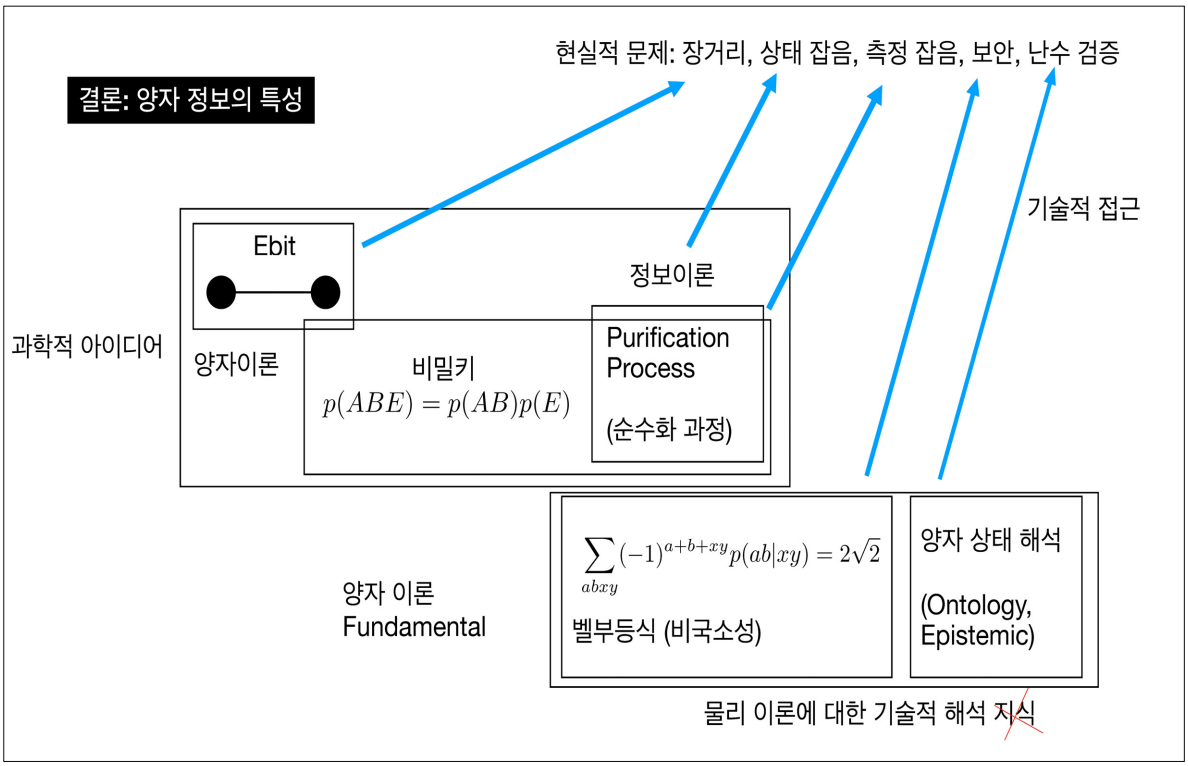


잡음 있는 측정을 반복하여

잡음 없는 측정 결과 수렴

JPA 2025

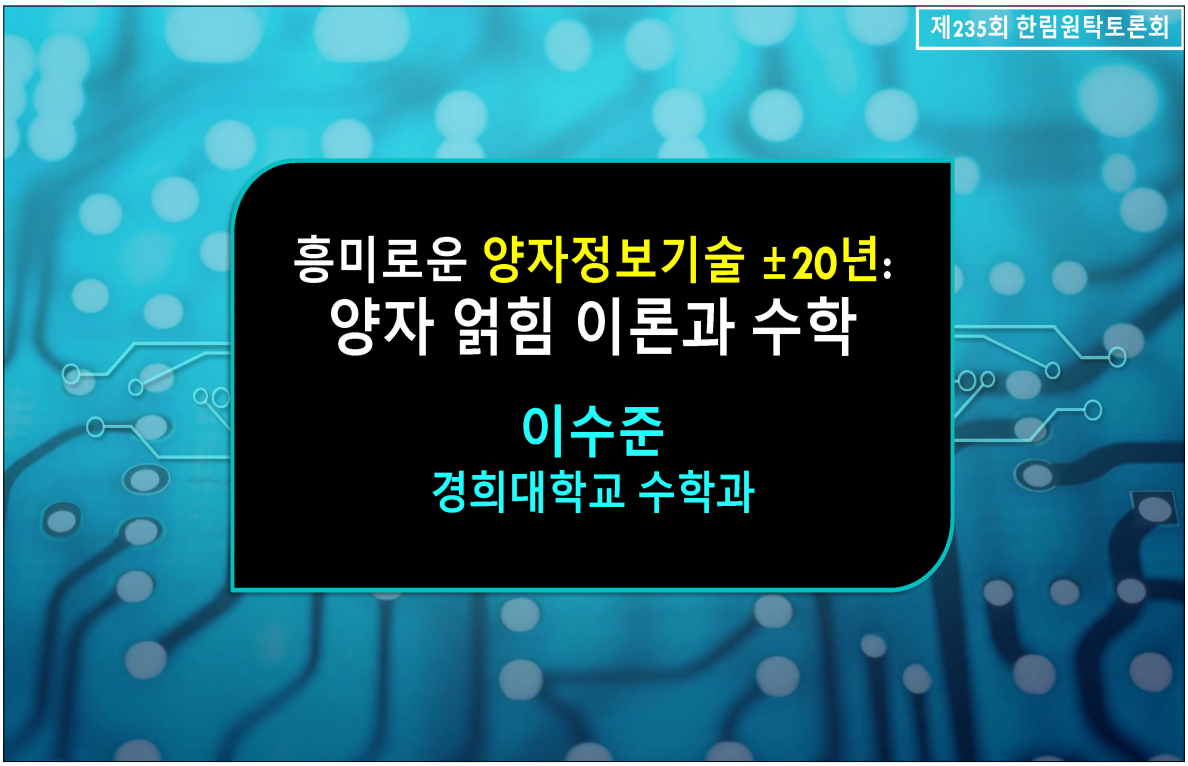

잡음 상태
잡음 비밀키
잡음 측정
Purification Process
(순수화 과정)
$p(ABE) \neq p(AB)p(E)$
$Q < Q_c$
$\phi^+ = \frac{|00\rangle + |11\rangle}{\sqrt{2}}$
$p(ABE) = p(AB)p(E)$
비밀키
잡음 없는 측정 결과
2000
2010
2020

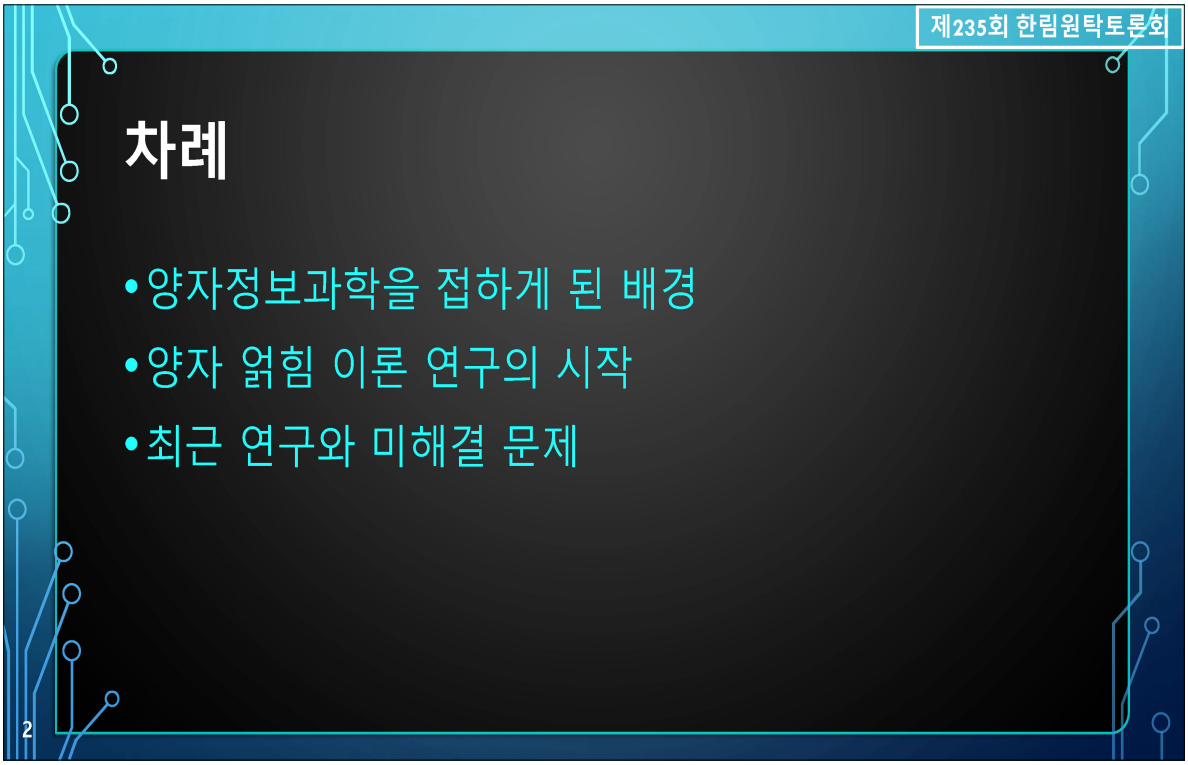

현실적 문제: 장거리, 상태 잡음, 측정 잡음, 보안, 난수 검증
결론: 양자 정보의 특성
기술적 접근
Ebit
정보이론
과학적 아이디어
양자이론
비밀키
$p(ABE) = p(AB)p(E)$
Purification Process
(순수화 과정)
$\sum_{abxy}(-1)^{a+b+xy}p(ab|xy) = 2\sqrt{2}$
벨부등식 (비국소성)
양자 상태 해석
(Ontology, Epistemic)
양자 이론
Fundamental
물리 이론에 대한 기술적 해석 지식

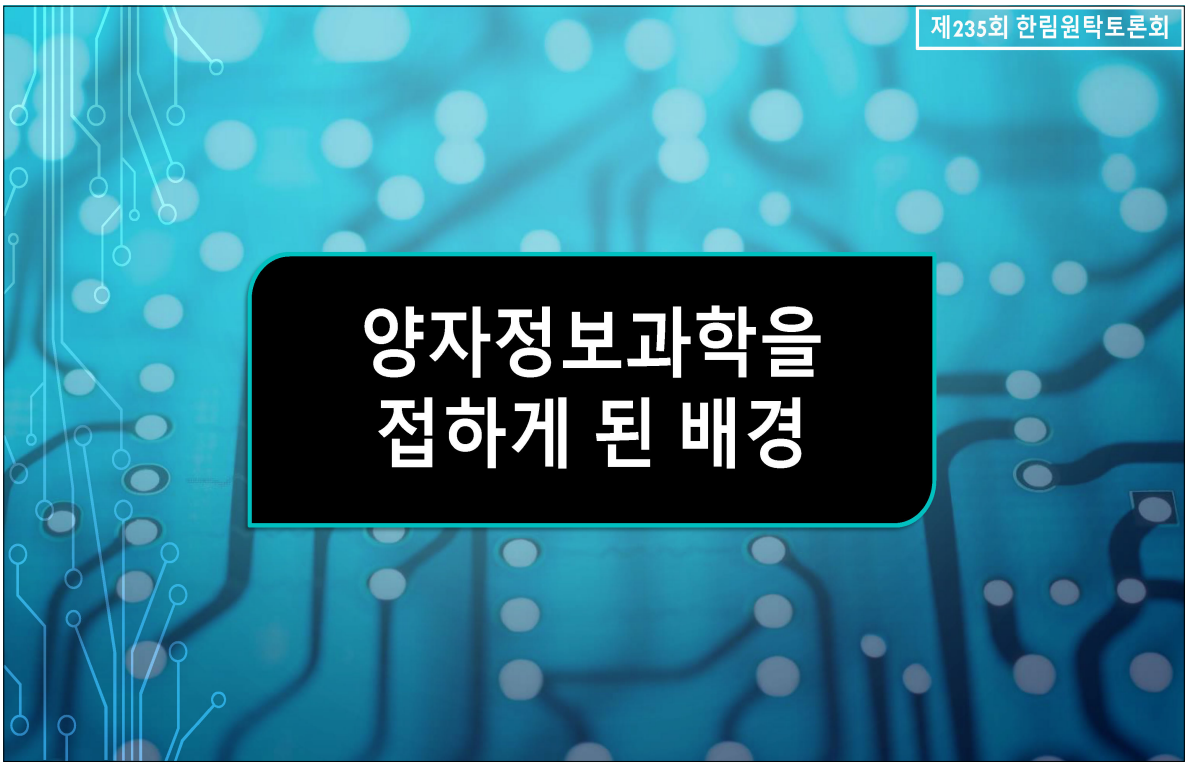
주제발표 5
양자 얽힘 이론과 수학

이 수 준

경희대학교 수학과 교수




제235회 한림원탁토론회
차례
•양자정보과학을 접하게 된 배경
•양자 얽힘 이론 연구의 시작
•최근 연구와 미해결 문제
2


제235회 한림원탁토론회
양자정보과학을
접하게 된 배경

저의 박사학위 과정

- 기간: 1998년 3월 ~ 2002년 2월
- 미분기하, 동역학계, 기호 동역학
- 1999년 2학기 수업
  - John Preskill's Lecture Note
    - Quantum Computation
  - https://www.preskill.caltech.edu/ph229/
- 학위논문명
  - On Quantum Computational Algorithms

4

양자정보과학과 수학

- International Congress of Mathematicians (4년마다 개최)
  - Fields상, Abacus (Nevanlinna)상, Gauss상, Chern상, Leelavati상, Noether 강연

14. Mathematical Aspects of Computer Science

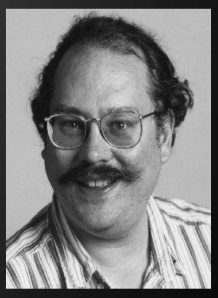
Complexity theory and design and analysis of algorithms. Formal languages. Computational learning. Algorithmic game theory. Cryptography. Coding theory. Semantics and verification of programs. Symbolic computation. Quantum computing. Computational geometry, computer vision.

5

제235회 한림원탁토론회

PETER W. SHOR

- 소인수 분해 quantum algorithm 개발 (1994)
  - 양자 컴퓨터에 의한 우월한 양자계산 가능
- 1998년 국제수학자대회에서 Rolf Nevanlinna 상 수상
- 현재 MIT 수학과 교수



Peter W. Shor
(AT&T Labs;
quantum computation,
computational geometry)

6

제235회 한림원탁토론회

양자 얽힘 이론 연구의 시작

제235회 한림원탁토론회

양자 얽힘(ENTANGLEMENT)

- 양자 얽힘: 양자정보처리의 중요한 자원
  - 양자 암호
  - 양자 전송 및 양자 통신
- 양자 얽힘 이론
  - 양자 얽힘 상태 판별
  - 양자 얽힘의 정도 계산
  - 양자 얽힘의 성질
  - 양자 얽힘의 응용

8

제235회 한림원탁토론회

행렬의 전치(TRANSPOSE)

$$A = \begin{bmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 7 & 8 & 9 \end{bmatrix} \quad \Rightarrow \quad A^T = \begin{bmatrix} 1 & 4 & 7 \\ 2 & 5 & 8 \\ 3 & 6 & 9 \end{bmatrix}$$

- 양자상태는 행렬
- (부분) 전치는 양자상태를 양자상태로 보내지 않을 수 있다.
  - 부분 전치(Partial Transposition)

9

제235회 한림원탁토론회

전치에 의한 양자 얽힘 상태 판별

- 부분 전치는 양자상태를 양자상태로 보내지 않을 수 있다.
- Peres (1996)
  - ρ^{AB}: 얽힘이 없는 양자상태 ⇒ 부분 전치(ρ^{AB})도 양자상태
  - 부분 전치(ρ^{AB})가 양자 상태가 아니면, ρ^{AB} 는 얽힘이 없다.
- 부분 전치(ρ^{AB})도 양자상태인 양자상태 ρ^{AB} 를 PPT라고 한다.
- Horodecki *et al.* (1996)
  - 낮은 차원($2 \otimes 2$, $2 \otimes 3$) : 얽힘 없음 ⇔ PPT
  - 높은 차원 : 얽힘 없음 ⇒ PPT, 역은 성립하지 않음

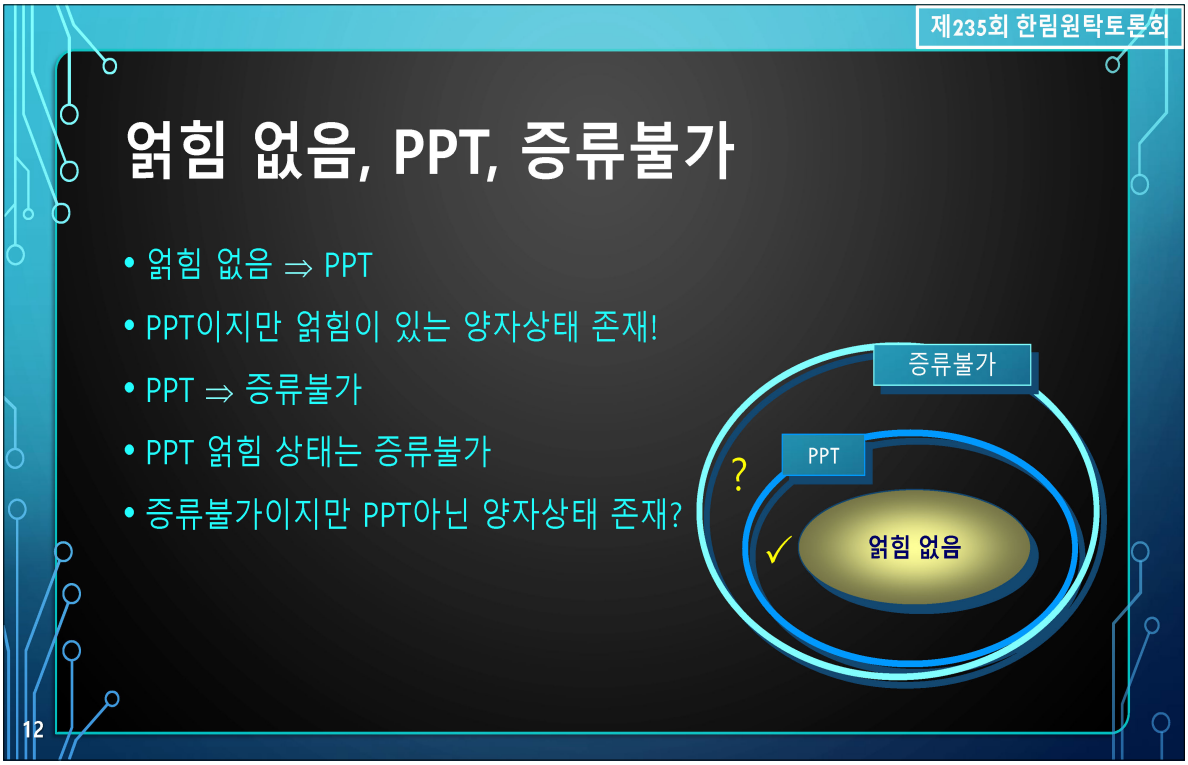
10

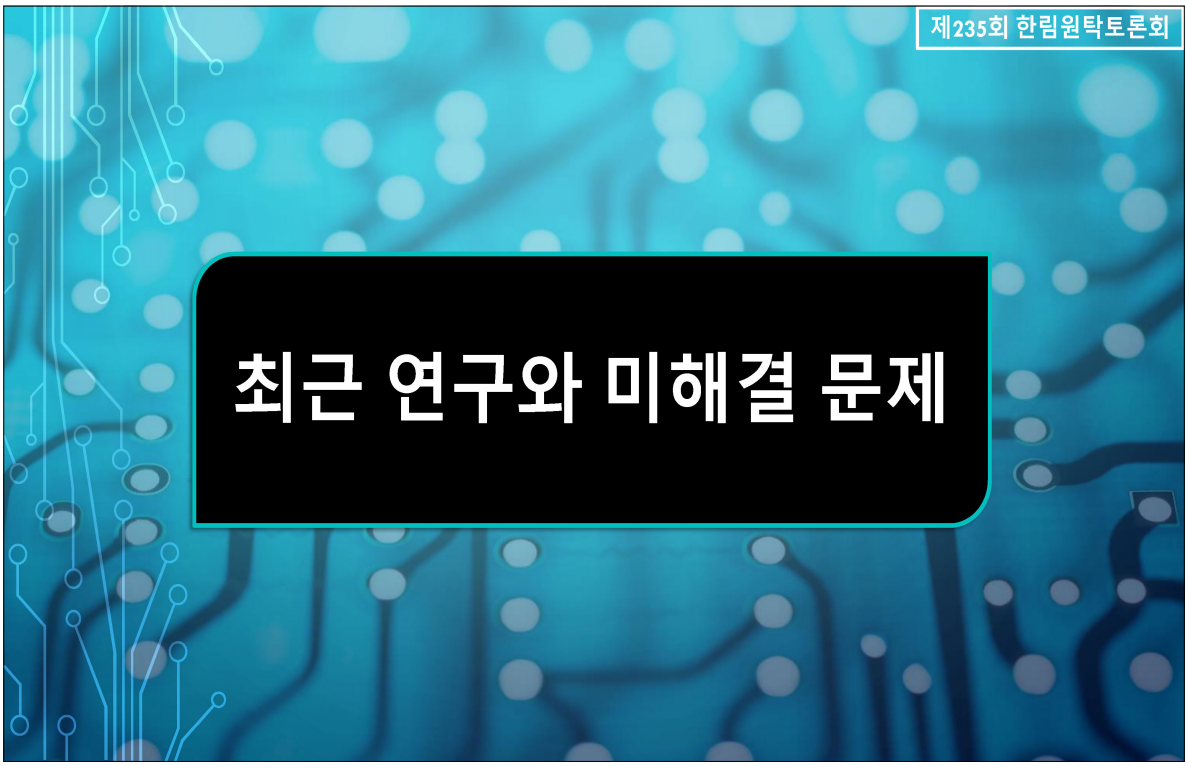
제235회 한림원탁토론회

양자정보처리에 사용하기 좋은 얽힘

- 좋은 얽힘을 만드는 방법(Entanglement Distillation)
  - ρ : 덜 좋은 얽힘이 있는 양자상태
  - $\rho \otimes \rho \otimes \ldots \otimes \rho$ $\Rightarrow^{LOCC}$ 좋은 얽힘이 있는 양자상태
- 얽힘이 있는 모든 양자상태로부터 좋은 얽힘을 만들 수 없다.
  - 좋은 얽힘을 만들지 못하는 상태를 증류불가(undistillable) 상태라고 한다.
- PPT ⇒ 증류불가
- 두 입자 중 하나의 차원이 2인 양자 상태($2 \otimes n$)에 대해서는 PPT ⇔ 증류불가

11


제235회 한림원탁토론회
얽힘 없음, PPT, 증류불가
• 얽힘 없음 ⇒ PPT
• PPT이지만 얽힘이 있는 양자상태 존재!
• PPT ⇒ 증류불가
• PPT 얽힘 상태는 증류불가
• 증류불가이지만 PPT아닌 양자상태 존재?
증류불가
PPT
?
얽힘 없음
12


제235회 한림원탁토론회
최근 연구와 미해결 문제

새로운 양자 얽힘 상태 판별법

- J. An and SL (in preparation, 2025)
- ρ^{AB}: 얽힘 없는 양자상태 ⇒ rank[ρ^{AB}] = rank[(I⊗T)ρ^{AB}]

$$\rho_H = \begin{bmatrix} \frac{1}{10} & 0 & 0 & 0 & \frac{1}{10} & 0 & 0 & 0 & \frac{1}{10} \\ 0 & \frac{1}{10} & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & \frac{1}{10} & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & \frac{1}{10} & 0 & 0 & 0 & 0 & 0 \\ \frac{1}{10} & 0 & 0 & 0 & \frac{1}{10} & 0 & 0 & 0 & \frac{1}{10} \\ 0 & 0 & 0 & 0 & 0 & \frac{1}{10} & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & \frac{3}{20} & 0 & \frac{\sqrt{3}}{20} \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & \frac{1}{10} & 0 \\ \frac{1}{10} & 0 & 0 & 0 & \frac{1}{10} & 0 & \frac{\sqrt{3}}{20} & 0 & \frac{3}{20} \end{bmatrix} \quad \rho_H^{T_A} = \begin{bmatrix} \frac{1}{10} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & \frac{1}{10} & 0 & \frac{1}{10} & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & \frac{1}{10} & 0 & 0 & 0 & \frac{1}{10} & 0 & 0 \\ 0 & \frac{1}{10} & 0 & \frac{1}{10} & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & \frac{1}{10} & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & \frac{1}{10} & 0 & \frac{1}{10} & 0 \\ 0 & 0 & \frac{1}{10} & 0 & 0 & 0 & \frac{3}{20} & 0 & \frac{\sqrt{3}}{20} \\ 0 & 0 & 0 & 0 & 0 & \frac{1}{10} & 0 & \frac{1}{10} & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & \frac{\sqrt{3}}{20} & 0 & \frac{3}{20} \end{bmatrix}$$

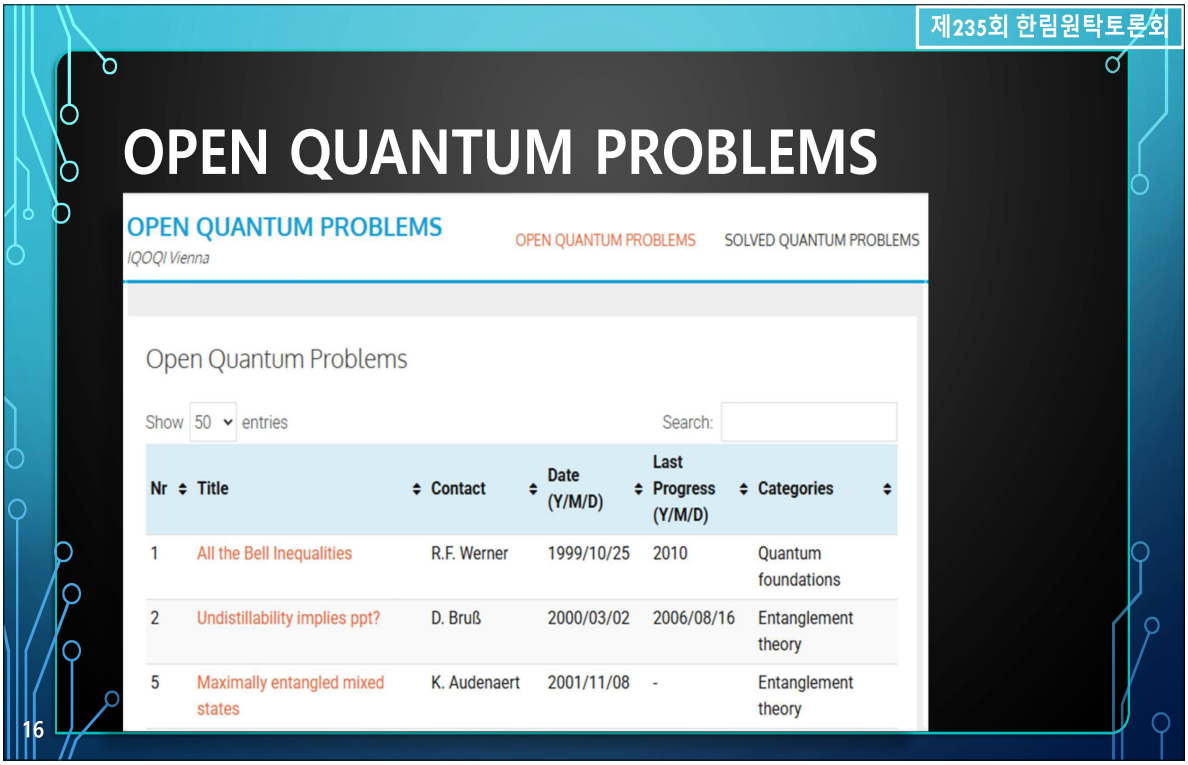
$$\mathrm{rank}(\rho_H) = 8 \neq 7 = \mathrm{rank}(\rho_H^{T_A})$$

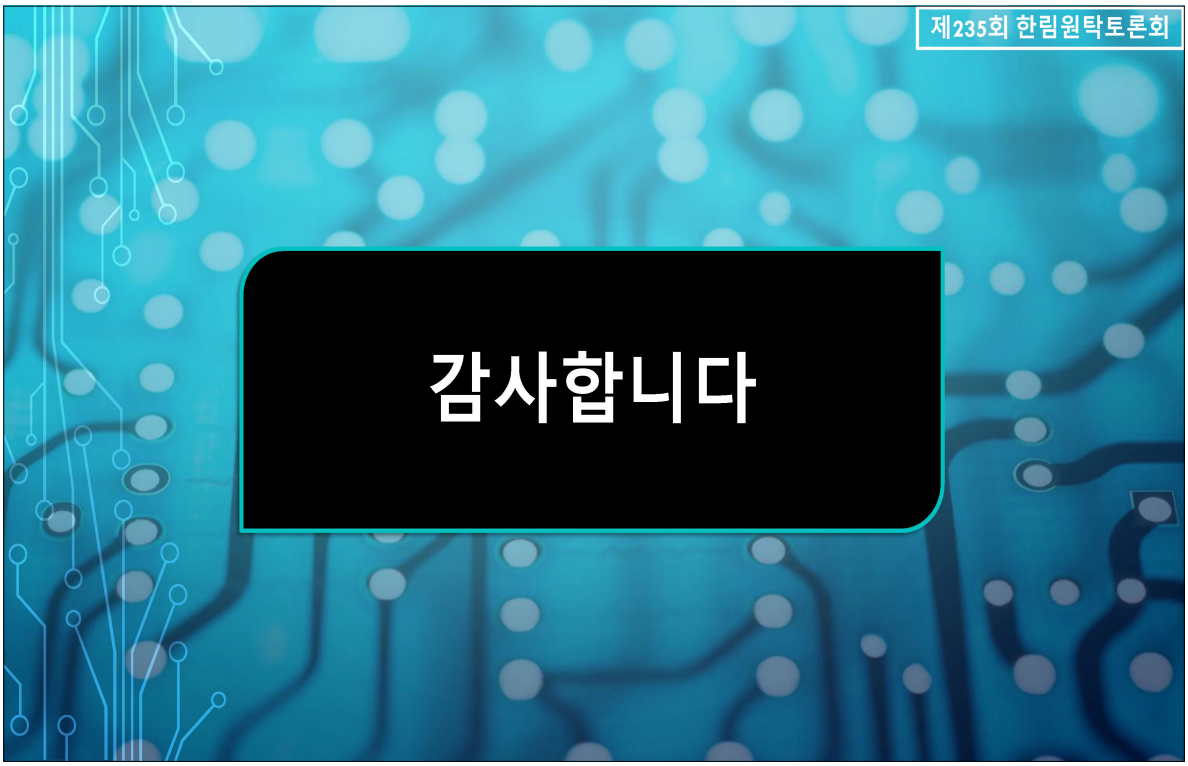
14

미해결 문제

- PPT ⇒ 증류불가
- PPT 얽힘 상태는 증류불가
- 증류불가 ⇒ PPT?
  - 증류불가이지만 PPT아닌 양자상태 존재?

15


제235회 한림원탁토론회
OPEN QUANTUM PROBLEMS
OPEN QUANTUM PROBLEMS
IQOQI Vienna
OPEN QUANTUM PROBLEMS
SOLVED QUANTUM PROBLEMS
Open Quantum Problems
Show 50 entries
Search:
Nr
Title
Contact
Date (Y/M/D)
Last Progress (Y/M/D)
Categories
1
All the Bell Inequalities
R.F. Werner
1999/10/25
2010
Quantum foundations
2
Undistillability implies ppt?
D. Bruß
2000/03/02
2006/08/16
Entanglement theory
5
Maximally entangled mixed states
K. Audenaert
2001/11/08
-
Entanglement theory
16

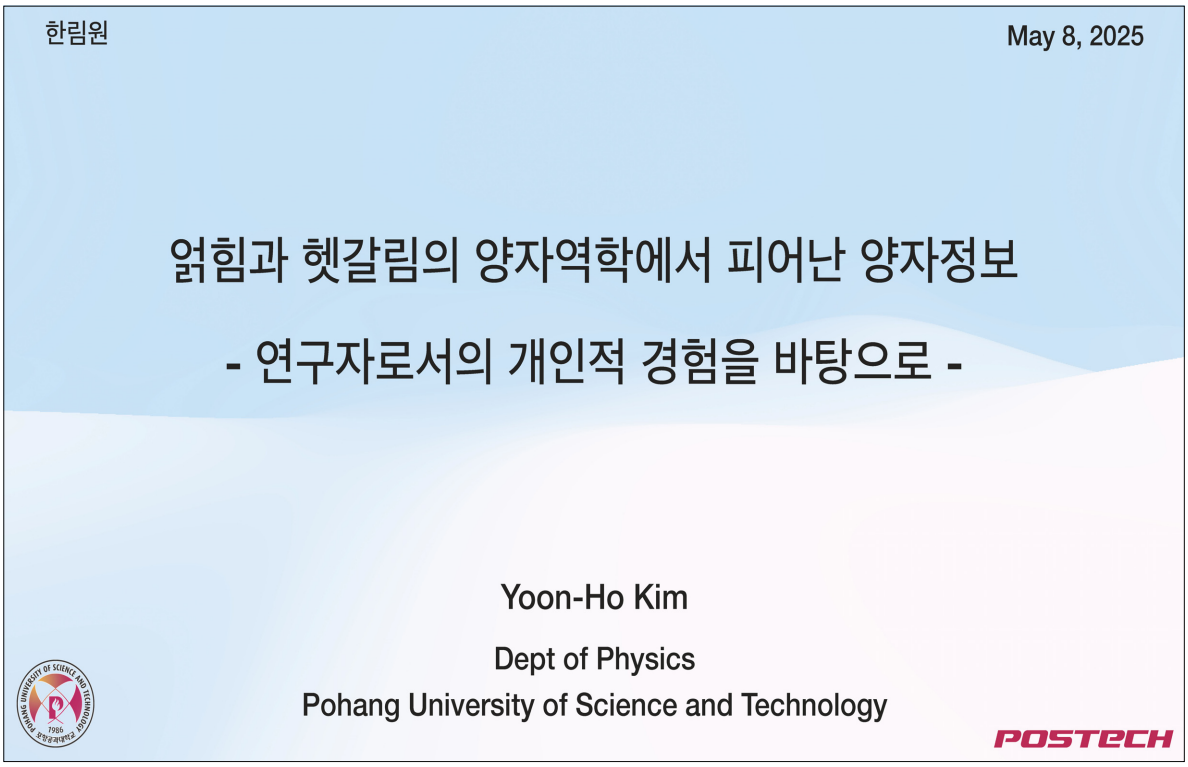

제235회 한림원탁토론회
감사합니다

주제발표 6

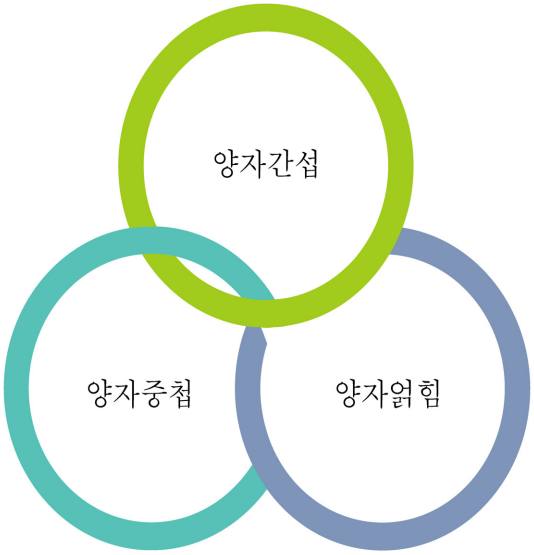
얽힘과 헷갈림의 양자역학에서 피어난 양자정보

김 윤 호

POSTECH 물리학과 교수

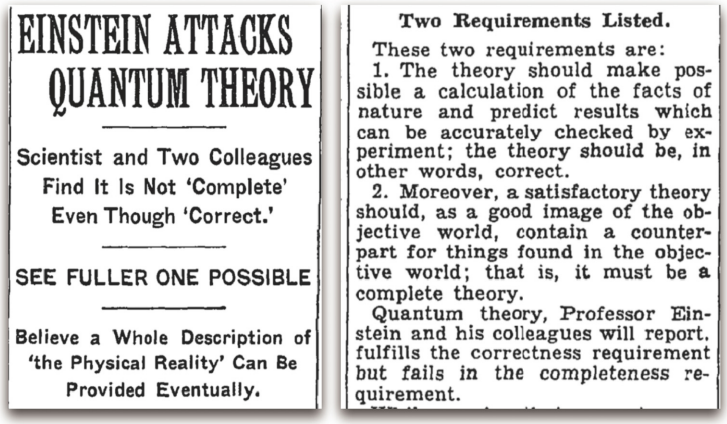


양자정보의 핵심 개념



양자역학의 불확정성원리와 Einstein-Podolsky-Rosen paradox

$$\Delta x \Delta p \geq \frac{\hbar}{2}$$



EINSTEIN ATTACKS QUANTUM THEORY

Scientist and Two Colleagues Find It Is Not 'Complete' Even Though 'Correct.'

SEE FULLER ONE POSSIBLE

Believe a Whole Description of 'the Physical Reality' Can Be Provided Eventually.

Two Requirements Listed.

These two requirements are:

1. The theory should make possible a calculation of the facts of nature and predict results which can be accurately checked by experiment; the theory should be, in other words, correct.

2. Moreover, a satisfactory theory should, as a good image of the objective world, contain a counterpart for things found in the objective world; that is, it must be a complete theory.

Quantum theory, Professor Einstein and his colleagues will report, fulfills the correctness requirement but fails in the completeness requirement.

The New York Times, Sat. May 4 (1935)

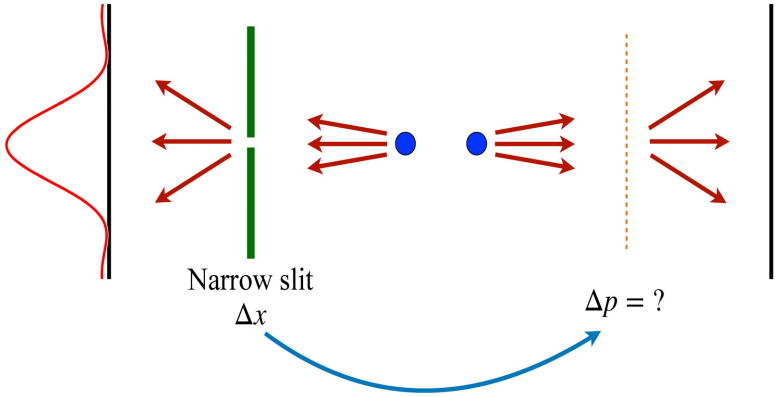
Einstein-Podolsky-Rosen 얽힘

$$\Delta p_1 = \Delta p_2 = \infty \qquad \Delta x_1 = \Delta x_2 = \infty$$

$$\Delta(p_1 + p_2) = 0 \qquad \Delta(x_1 - x_2) = 0$$

PR 47, 777 (1935)

Karl Popper의 사고실험



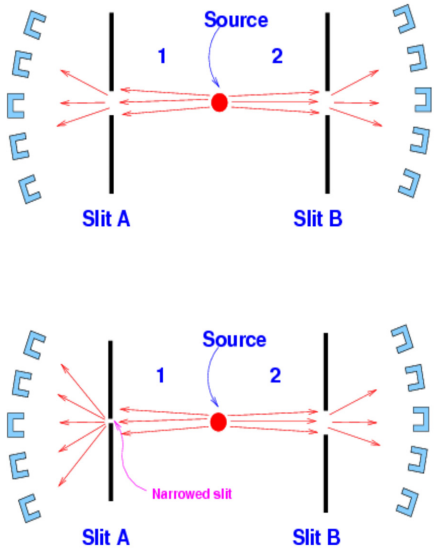
파동함수의 붕괴

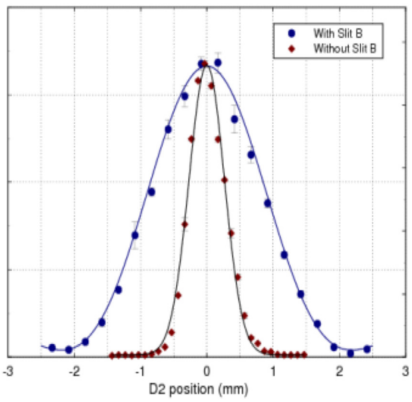
⇓

불확정성 원리의 위배?

K. Popper (1980)

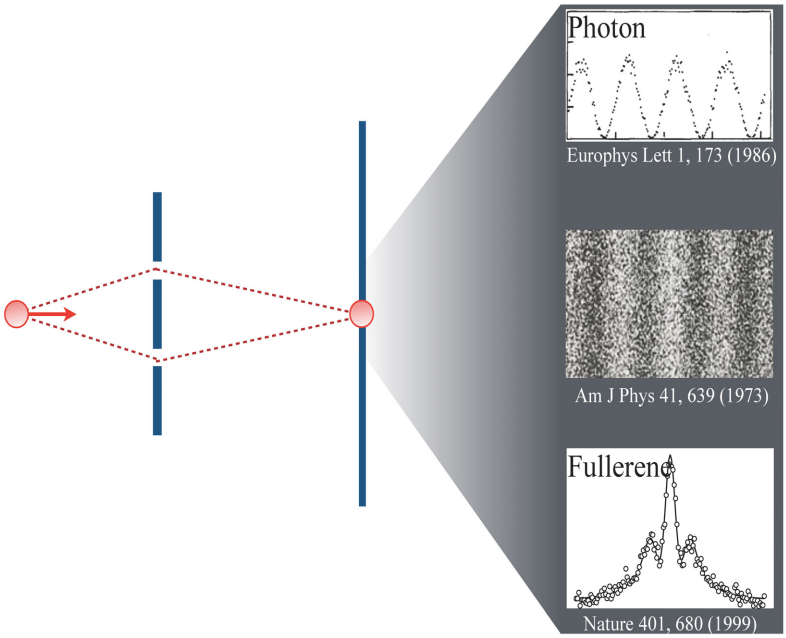
Popper의 사고실험의 구현



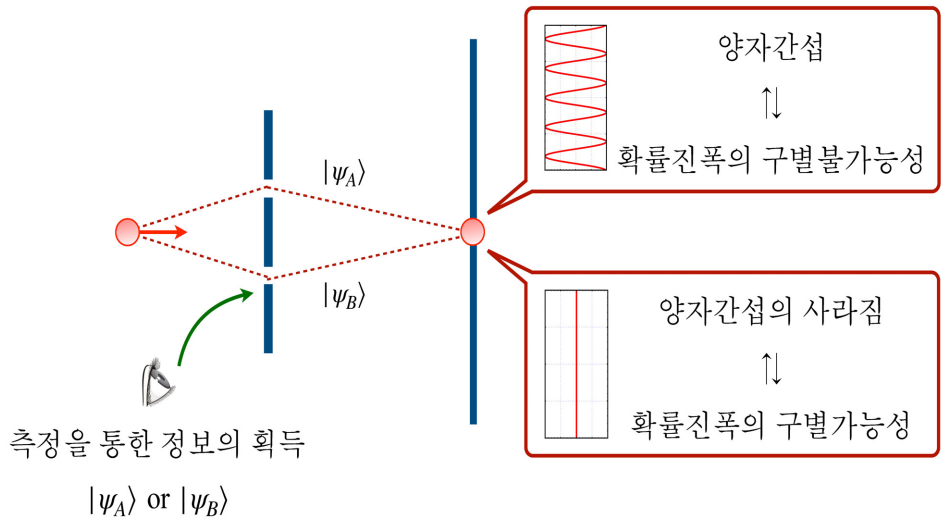


Found Phys 29, 1849 (1999)

단일입자의 양자간섭과 파동-입자 이중성



불확정성원리, 확률진폭의 구별가능성, 그리고 양자간섭



양자지우개 개념을 활용한 불확정원리로부터 독립적인 상보성 검증

PHYSICAL REVIEW A VOLUME 25, NUMBER 4 APRIL 1982

Quantum eraser: A proposed photon correlation experiment concerning observation and "delayed choice" in quantum mechanics

Marlan O. Scully and Kai Drühl
Max-Planck Institut für Quantenoptik, D-8046 Garching bei München, West Germany and Institute for Modern Optics, Department of Physics and Astronomy, University of New Mexico, Albuquerque, New Mexico 87131
(Received 2 April 1981)

We propose and analyze an experiment designed to probe the extent to which information accessible to an observer and the "eraser" of this information affects measured results. The proposed experiment could also be operated in a "delayed-choice" mode.

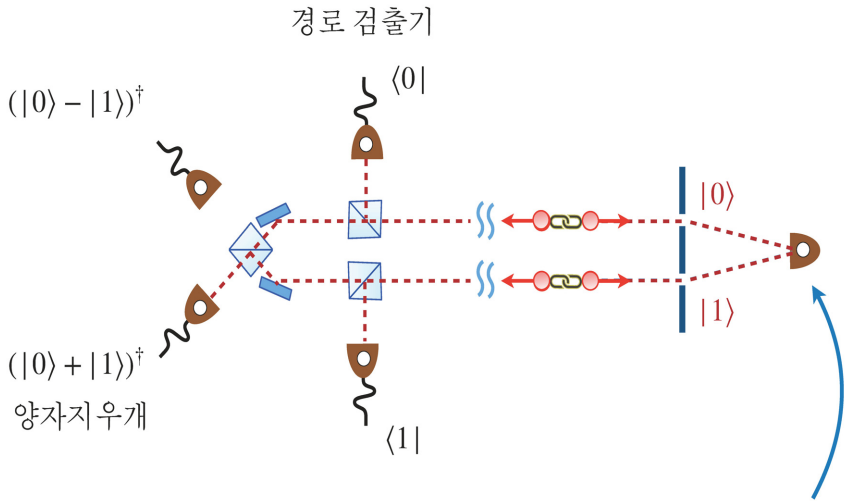
Quantum optical tests of complementarity

Marlan O. Scully, Berthold-Georg Englert & Herbert Walther

Simultaneous observation of wave and particle behaviour is prohibited, usually by the position–momentum uncertainty relation. New detectors, constructed with the aid of modern quantum optics, provide a way around this obstacle in atom interferometers, and allow the investigation of other mechanisms that enforce complementarity.

PRA 25, 2208 (1982)
Nature 351, 111 (1991)

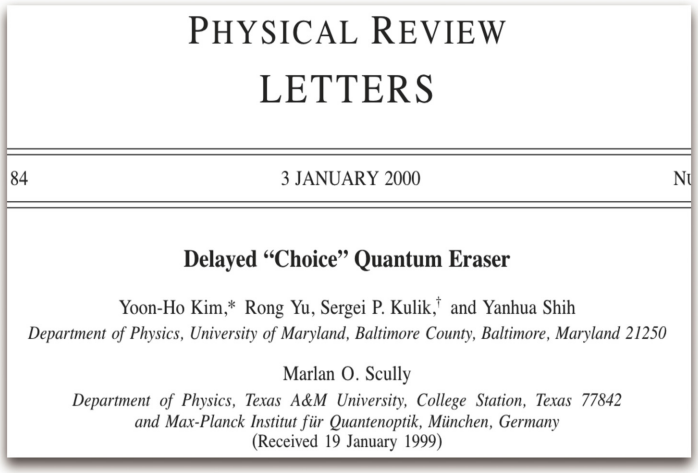
양자얽힘을 활용한 지연선택 양자지우개와 상보성 원리의 검증



양자얽힘과 양자지우개를 이용해 양자입자의 입자성-파동성을 검출된 후에도 결정 가능

PRL 81, 1 (2000)

양자얽힘을 활용한 지연선택 양자지우개와 상보성 원리의 검증

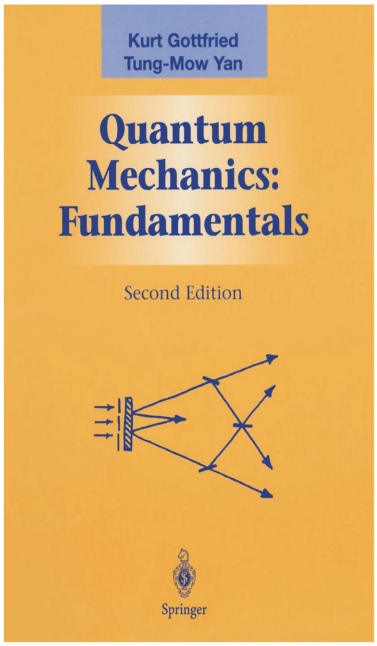

PHYSICAL REVIEW
LETTERS

84 3 JANUARY 2000 Nu

Delayed "Choice" Quantum Eraser

Yoon-Ho Kim,* Rong Yu, Sergei P. Kulik,† and Yanhua Shih
Department of Physics, University of Maryland, Baltimore County, Baltimore, Maryland 21250

Marlan O. Scully
Department of Physics, Texas A&M University, College Station, Texas 77842
and Max-Planck Institut für Quantenoptik, München, Germany
(Received 19 January 1999)



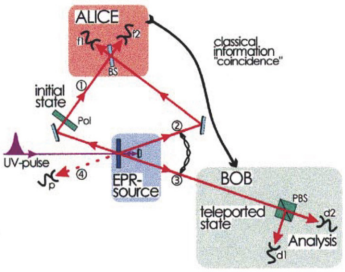
PRL 81, 1 (2000)

Quantum Teleportation

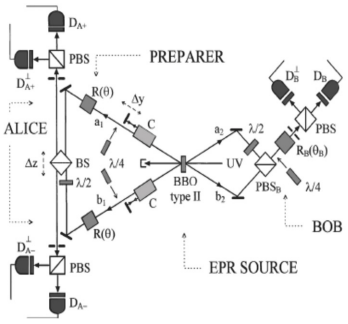
VOLUME 70 29 MARCH 1993 NUMBER 13

Teleporting an Unknown Quantum State via Dual Classical and Einstein-Podolsky-Rosen Channels

Charles H. Bennett,(1) Gilles Brassard,(2) Claude Crépeau,(2),(3)
Richard Jozsa,(2) Asher Peres,(4) and William K. Wootters(5)



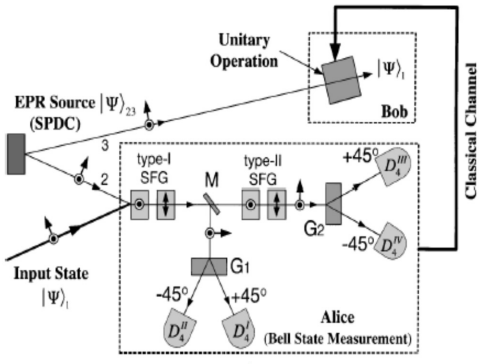
Nature 390, 575 (1997)



PRL 80, 1121 (1998)

완전한 양자전송의 실험적 구현

초고속 얽힘광원



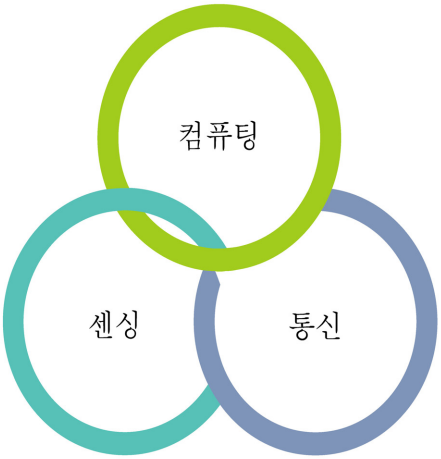
완전한 Bell-상태 측정

단일광자 파장 변환 기술

PRL 86, 1370 (2001)

양자정보과학

양자자원을 활용해 고전적 한계를 넘는 양자이득의 가능성 추구

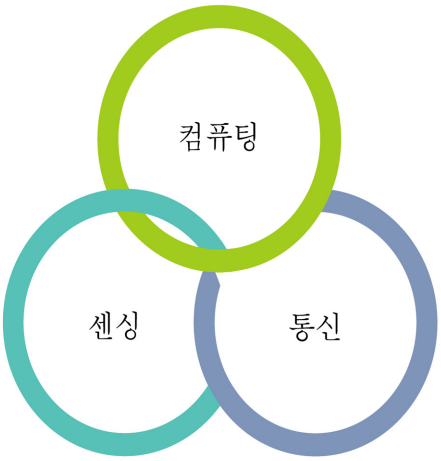


⇒ 양자이득

- 고전 컴퓨터보다 더 빠른 양자 계산
- 고전 측정 한계를 넘는 측정 정밀도 향상
- 고전적으로 불가능한 정보 전달 방법론

양자정보과학

양자자원을 활용해 고전적 한계를 넘는 양자이득의 가능성 추구



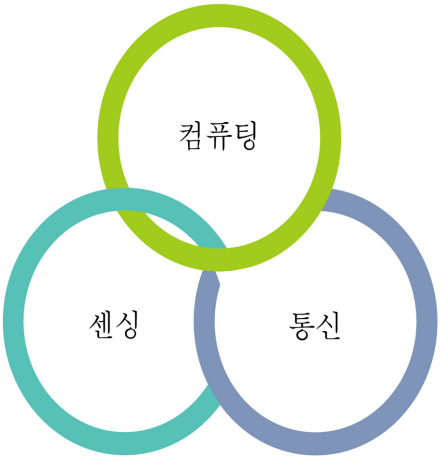
⇒ 양자이득

- 고전 컴퓨터보다 더 빠른 양자 계산
- 고전 측정 한계를 넘는 측정 정밀도 향상
- 고전적으로 불가능한 정보 전달 방법론

가능성, 필요성, 효용성 ?

양자정보과학

양자자원을 활용해 고전적 한계를 넘는 양자이득의 가능성 추구



⇒ 양자이득 ?

- 고전 컴퓨터보다 더 빠른 양자 계산
- 고전 측정 한계를 넘는 측정 정밀도 향상
- 고전적으로 불가능한 정보 전달 방법론

⇒ 양자자원

- 양자중첩 및 양자얽힘
- 양자자원의 정량화 및 새로운 양자자원 탐구
- 양자상태 생성, 제어, 측정의 새로운 방법론
- 고전자원과 양자자원의 활용 한계 탐구

주제발표 7

양자암호 기술 상용화

최 정 운

SKT Quantum팀 팀장

양자 암호 기술 상용화

제235회 한림원탁토론회

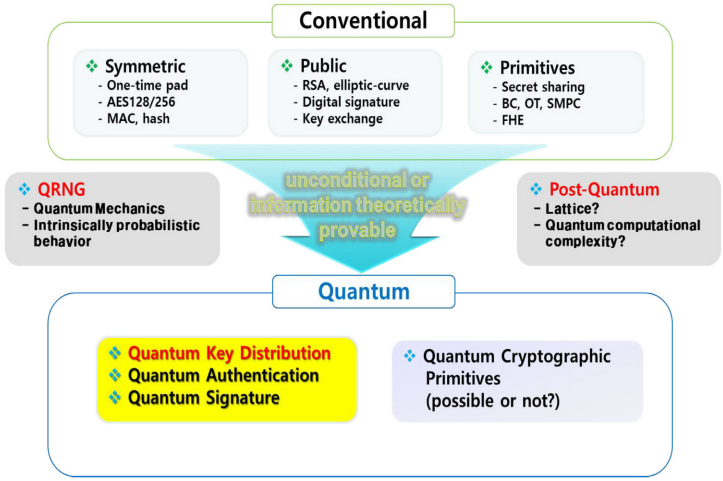
2025.05.09.

최정운

SK Telecom

상용 양자암호통신 기술 분야

다양한 암호 primitive 기술들을 '양자 정보 체계'를 기반으로 안전성을 극대화
Information Theoretical Security (증명 가능 안전성 제공)

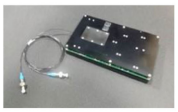


1

QKD 상용화

네트워크 상의 임의의 두 노드 간에 안전성이 보장된 암호키를 나눠 갖는 것이 가능하도록
실험실 수준에서 국가 인증 확보 수준으로 기술 및 제도/정책 성장

	Clavis 300	Clavis XG
		
• Secret Key Rate	40kb/s (@12dB)	100kb/s (typ.@12dB)
• Dynamic range	18, 24 dB	24 dB (Optional 30dB)
• Protocol:	BB84	BB84
• Dimensions	6U, 23.4 kg	1U, 14kg
• System clock frequency:	125 MHz	1 GHz
• Temperature range:	+5°C to 35°C	+5 to 40°C
• Management	Optional blade	Embedded


[단일광자검출기]


[고속 난수생성기]


[광 간섭계]


[고속 암복호화기]

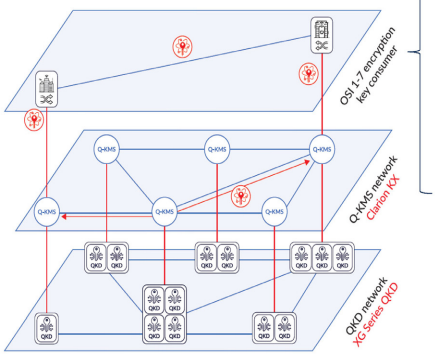
- 국가정보원 국가용 보안요구사항 (QKD, QKMS, QENC) 준수
- 보안기능확인서 확보 ('25년1월)

2

QKD 상용화

네트워크 상의 임의의 두 노드 간에 안전성이 보장된 암호키를 나눠가질 수 있도록
QKD 기술 자체와 각종 통신/네트워킹 기술, 암호 기술들이 집합체

45U 19" server rack
W 700 X D 1100 X H 2200

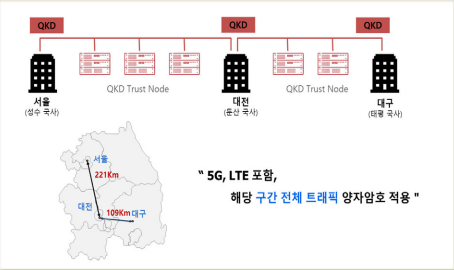


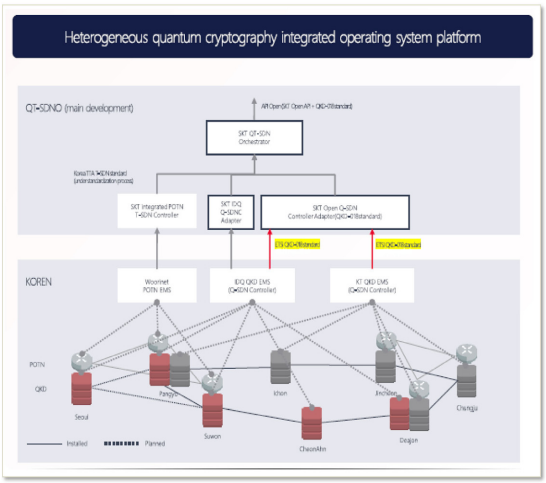
IP VPN IPSec	THALES, FORTINET, cisco, XN
MPLS VPN	HITACHI Inspire the Next
Ethernet VPN MACSec	THALES, JUNIPER, IDQ
OTN/WDM encryption	ADVA, ciena, ribbon, NOKIA, PacketLight, WOORINET

3

QKD 네트워크

정부기관, 연구소, 공공/민간 기업 들을 대상으로 1,200km 이상의 구간에 QKD 네트워크 구축

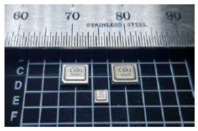


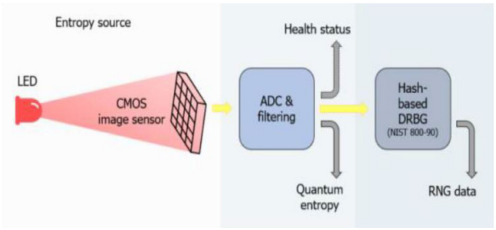


4

QRNG chip 상용화

Photon number fluctuation 기반의 양자난수생성 기술 chip化





PHYSICAL REVIEW APPLIED **15,** 054048 (2021)

Quantum Entropy Model of an Integrated Quantum-Random-Number-Generator Chip

Gaëtan Gras,[1,2,*] Anthony Martin,[1] Jeong Woon Choi,[1] and Félix Bussières[1]
[1] *ID Quantique SA, CH-1227 Carouge, Switzerland*
[2] *Group of Applied Physics, University of Geneva, CH-1211 Geneva, Switzerland*

5

세계 최초 5G 스마트폰 QRNG 상용 적용

세계 최초로 QRNG칩이 탑재된 스마트폰 출시

6

Q-HSM(Quantum Hardware Security Module)

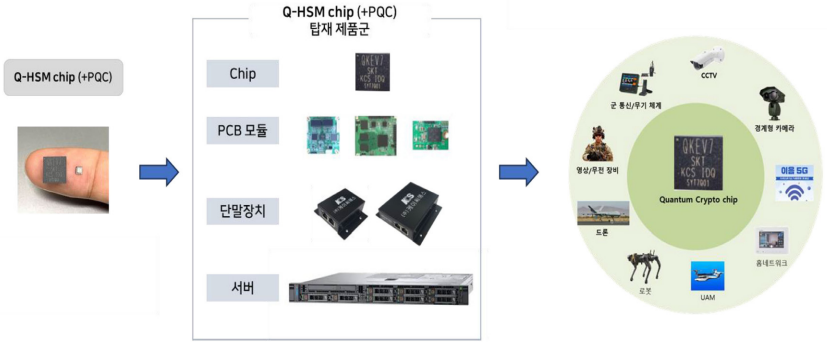
Edge 단말(CCTV, 통신단말, 월패드 등) 영역에 Q-HSM 제품을 중심으로 국방/공공/민간 사업 추진 중

상품 정의

- Edge 단말 네트워크의 보안성 향상을 위한 chip 기반의 구간 암호 솔루션

특장점

- 양자난수발생기(QRNG), 물리적 복제방지 기능(PUF), 현대암호(대칭키, 공개키) 기능을 모두 one-chip으로 구현
- Q-HSM chip 국정원 암호모듈검증 KCMVP Level 2 인증 획득('24년 11월)
- 단말기/서버 제품군 보안기능확인서 획득 예정('25년 4월)
- 미국 NIST 표준 PQC 알고리즘 chip 포함 전 제품군 탑재 완료



7

PQC-QKD hybrid

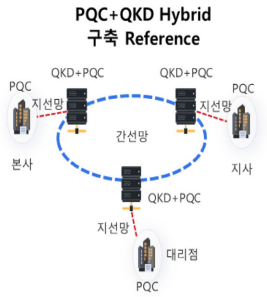
Edge 단말(CCTV, 통신단말, 월패드 등) 영역에 Q-HSM 제품을 중심으로 국방/공공/민간 사업 추진 중

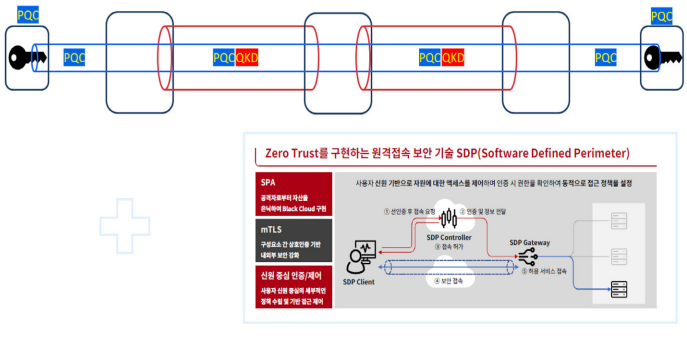
상품 정의

- 양자 역학 기반 최고의 보안 기술인 QKD와 수학 알고리즘 기반 소프트웨어 보안 기술인 PQC를 결합한 hybrid 솔루션
- Smart-WAN(SDP) 기술과의 연동을 통한 신규 total 양자보안 솔루션 사업화 추진 중 (데이터 통신 암호 + Zero Trust)

특장점

- 간선망(코어/백본)에는 QKD 와 PQC 두 개의 암호화가 동시에 진행되는 이중 암호화로 최상위 보안 레벨 제공
- 지선망(엣지/백홀)에는 소프트웨어 PQC 를 적용하여 양자컴퓨팅 공격에 대한 기본적인 안전성 확보
- 기존 QKD 단독 솔루션 대비 다양한 고객 요구 사항에 유연하게 대응이 가능하고, 보안 커버리지 확장

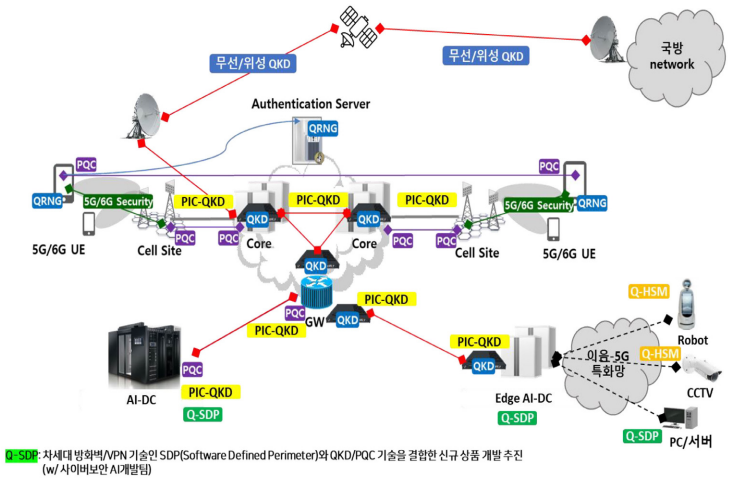




8

SKT 양자암호 상품/기술 구성도

Edge 단말부터 AI-DC 및 5G/6G infra까지
통신 네트워크 특성에 맞는 다양한 양자암호 상품/기술을 통한 최적의, 최고수준의 안전성 제공



Q-SDP: 차세대 방화벽/VPN 기술인 SDP(Software Defined Perimeter)와 QKD/PQC 기술을 결합한 신규 상품 개발 추진
(w/ 사이버보안 AI개발팀)

9

감사합니다

한림원탁토론회는...

한림원탁토론회는 국가 과학기술의 장기적인 비전과 발전전략을 세우고, 동시에 과학기술 현안문제에 대한 해결방안을 모색하기 위한 목적으로 개최되고 있는 한림원의 대표적인 정책토론 행사입니다.

지난 1996년 처음 개최된 이래 지금까지 200회 이상에 걸쳐 초중등 과학교육, 문·이과 통합문제, 국가발전에 미치는 기초과학 등 과학기술분야의 기본문제는 물론 정부출연연구소의 발전방안, 광우병의 진실, 방사능, 안전 방제 등 국민생활에 직접 영향을 미치는 문제에 이르기까지 광범위한 주제를 다루고 있습니다.

한림원은 과학기술 선진화에 걸림돌이 되는 각종 현안문제 중 중요도와 시급성에 따라 주제를 선정하고, 과학기술 유관기관의 최고책임자들을 발제자로 초빙하여, 한림원 석학들을 비롯해 산·학·연·정의 전문가들이 심도 깊게 토론을 진행하고 있습니다.

토론결과는 책자로 발간, 정부, 국회와 관련기관에 배포함으로써 정책 개선방안을 제시하고 정책 입안자료를 제공하여 여론 형성에 기여하도록 힘쓰고 있습니다.

▌한림원탁토론회 개최실적 (2022년 ~ 2025년) ▐

회차	일 자	주 제	발제자
194	2022. 1. 25.	거대한 생태계, 마이크로바이옴 연구의 미래	이세훈, 이주훈, 이성근
195	2022. 2. 14.	양자컴퓨터의 전망과 도전: 우리는 무엇을 준비해야 할까?	이진형, 김도헌
196	2022. 3. 10.	오미크론, 기존 바이러스와 무엇이 다르고 어떻게 대응할 것인가?	김남중, 김재경
197	2022. 4. 29.	과학기술 주도 성장: 무엇을 해야 할 것인가?	송재용, 김원준
198	2022. 6. 2.	더 이상 자연재난은 없다: 자연-기술 복합재난에 대한 이해와 대비	홍성욱, 이호영, 이강근, 고상백
199	2022. 6. 17.	K-푸드의 가치와 비전	권대영, 채수완
200	2022. 6. 29.	벤자민 버튼의 시간, 노화의 비밀을 넘어 역노화에 도전	이승재, 강찬희
201	2022. 9. 26.	신약개발의 새로운 패러다임	김성훈, 최 선, 김규원
202	2022. 9. 29.	우리는 왜, 어떻게 우주로 가야 하는가?	문홍규, 이창진
203	2022. 10. 12.	공학과 헬스케어의 만남 - AI가 여는 100세 건강	황 희, 백점기
204	2022. 10. 21.	과학기술과 사회 정의	박범순, 정상조, 류석영, 김승섭
205	2022. 11. 18.	지속 가능한 성장과 가치 혁신을 위한 수학의 역할	박태성, 백민경, 황형주
206	2022. 12. 1.	에너지와 기후변화 위기 극복을 위한 기초과학의 역할	유석재, 하경자, 윤의준
207	2023. 3. 15.	한국 여성과학자의 노벨상 수상은 요원한가?	김소영, 김정선
208	2023. 3. 22.	기정학(技政學) 시대의 새로운 과학기술혁신정책 방향	이승주, 이 근, 권석준
209	2023. 4. 13.	우리 식량 무엇이 문제인가?	곽상수, 이상열

회차	일 자	주 제	발제자
210	2023. 5. 24.	대체 단백질 식품과 배양육의 현재와 미래	서진호, 배호재
211	2023. 6. 14.	영재교육의 내일을 생각한다	권길헌, 이덕환, 이혜정
212	2023. 7. 6.	후쿠시마 오염수 처리 후 방류의 국내 영향	정용훈, 서경석, 강건욱
213	2023. 7. 12.	인구절벽 시대, 과학기술인재 확보를 위한 답을 찾아서	오현환, 엄미정
214	2023. 8. 17.	과학·영재·자사고 교장이 이야기하는 바람직한 학생 선발과 교육	허우석, 오성환, 김명환
215	2023. 10. 27.	과학기술을 통한 삶의 질 향상 시리즈 (Ⅰ) 국민 삶의 질 향상을 위한 과학기술정책의 대전환	정선양, 박상철
216	2023. 11. 9.	과학기술을 통한 삶의 질 향상 시리즈 (Ⅱ) 삶의 질 향상을 위한 데이터 기반 식단 및 의학	박용순, 정해영
217	2023. 12. 5.	과학기술을 통한 삶의 질 향상 시리즈 (Ⅲ) 삶의 질 향상을 위한 퍼스널 모빌리티	공경철, 한소원
218	2023. 12. 19.	새로운 의료서비스 혁명: 디지털 치료제	서영준, 배민철
219	2024. 1. 31.	노쇠와 근감소증	원장원, 권기선, 고홍섭
220	2024. 3. 13.	필수의료 해결을 위한 제도적 방안	박민수, 김성근, 홍윤철
221	2024. 3. 19.	코로나보다 더 큰 위협이 올 수 있다, 어떻게 할까?	송대섭, 신의철
222	2024. 3. 20.	퍼스트 무버(First Mover)로의 필수 요소 - 과학네트워킹	김형하, 이상엽, 조희용
223	2024. 5. 10.	시민, 과학자가 되다	홍성욱, 박창범, 김 준
224	2024. 5. 29.	GMO, 지속가능성을 위한 전략	하상도, 김해영
225	2024. 6. 21.	전략기술시리즈 (Ⅰ) K-반도체 위기 극복을 위한 국제 협력 전략	정은승

회차	일 자	주 제	발제자
226	2024. 8. 21.	조류인플루엔자의 위협: 팬데믹의 전조인가?	윤철희, 김우주, 송대섭
227	2024. 8. 28.	전략기술시리즈 (Ⅱ) AI로 과학하기: 새로운 패러다임	문용재, 백민경, 서재민
228	2024. 11. 18.	전략기술시리즈 (Ⅲ) K-방산의 완성: 첨단 항공기 엔진 독자 개발	심현석, 이홍철, 김재환
229	2024. 12. 3.	과학기술 정책은 얼마나 과학적인가?	이정동, 이성주
230	2024. 12. 17.	전략기술시리즈 (Ⅳ) 첨단 바이오, 난치병 치료의 게임 체인저	최강열, 신영기, 천병년
231	2024. 12. 20.	뉴럴링크: 뇌와 세상의 소통	임창환, 정재승
232	2024. 12. 24.	전략기술시리즈 (Ⅴ) 식탁 위 숨겨진 건강 비밀: 마이크로바이옴이 열어가는 미래	이주훈, 김상범, 방예지
233	2025. 2. 25.	연구성과의 가치, 어떻게 평가할 것인가?	이학연
234	2025. 4. 29.	한국 AI의 미래 시리즈 (Ⅰ) AI 3대 강국을 향한 우리의 전략	이경우, 김진형

제235회 한림원탁토론회

흥미로운
양자정보기술 ±20년

이 사업은 복권기금 및 과학기술진흥기금 지원을 통한 사업으로
우리나라의 공익적 가치 증진에 기여하고 있습니다.

문 의 **한국과학기술한림원(KAST)** 경기도 성남시 분당구 돌마로 42(구미동) (우)13630
전화 (031)726-7900 **팩스** (031)726-7909 **이메일** kast@kast.or.kr