國立臺灣大學 National Taiwan University

量子電腦之緣起與現況及未來的應用

Hao-Chung Cheng (鄭皓中)

haochung@ntu.edu.tw

Department of Electrical Engineering

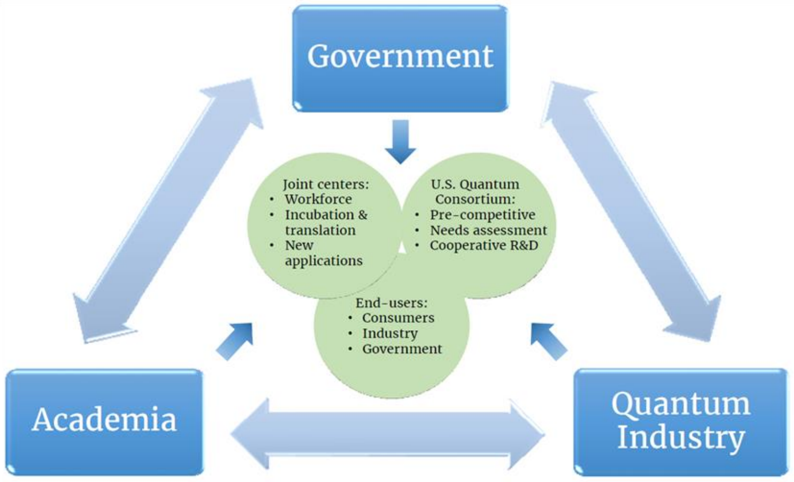
National Taiwan University

臺北區網專題會議, November 2, 2021

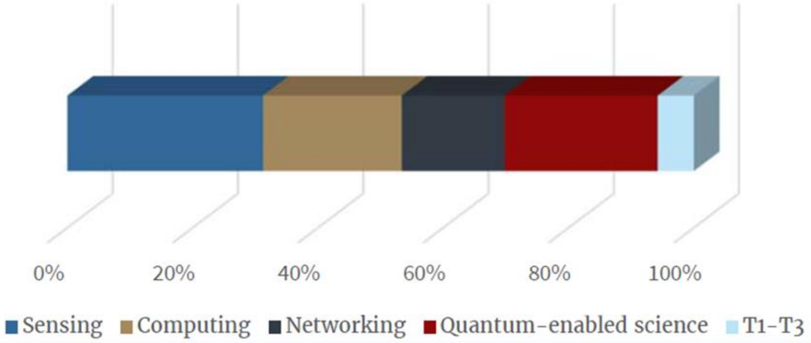
Quantum Information Projects – US

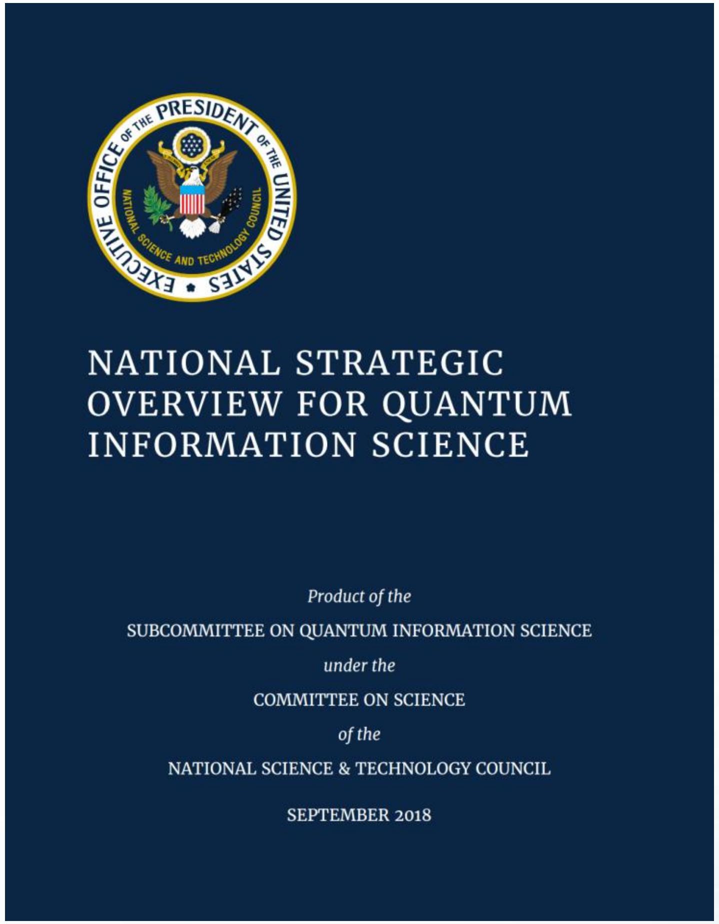
⟨quantum|gov⟩

2018 – 2023: $1.2B



U.S. Government research spending by area




NATIONAL STRATEGIC OVERVIEW FOR QUANTUM INFORMATION SCIENCE

Product of the

SUBCOMMITTEE ON QUANTUM INFORMATION SCIENCE

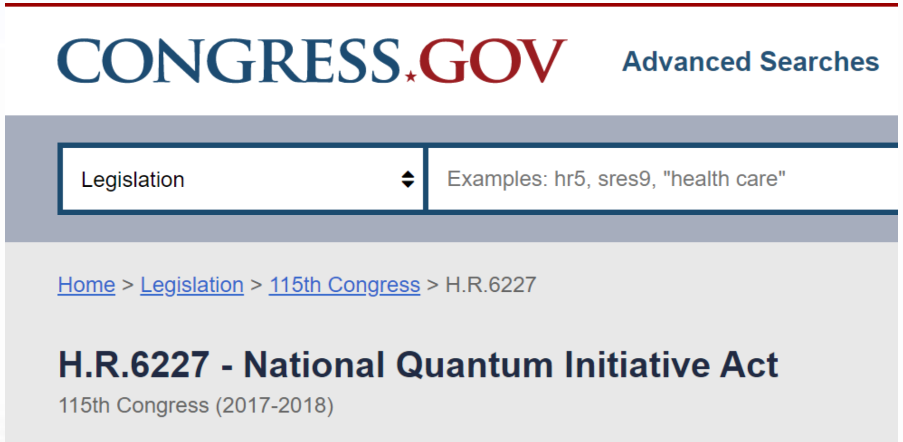
under the

COMMITTEE ON SCIENCE

of the

NATIONAL SCIENCE & TECHNOLOGY COUNCIL

SEPTEMBER 2018



QUANTUM FRONTIERS
REPORT ON COMMUNITY INPUT TO THE NATION'S STRATEGY FOR QUANTUM INFORMATION SCIENCE

Product of

THE WHITE HOUSE

NATIONAL QUANTUM COORDINATION OFFICE

October 2020

A STRATEGIC VISION FOR AMERICA'S QUANTUM NETWORKS

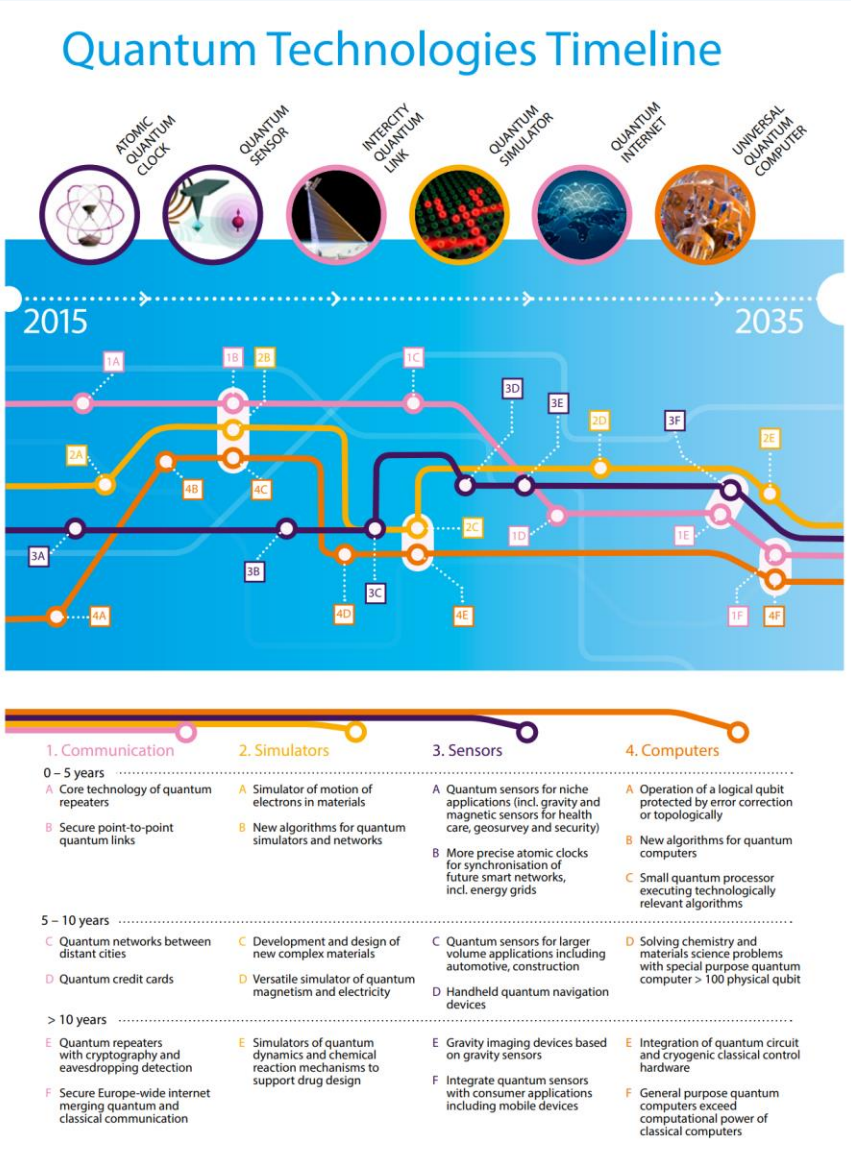
Product of

THE WHITE HOUSE

NATIONAL QUANTUM COORDINATION OFFICE

February 2020

Quantum Information Projects – EU



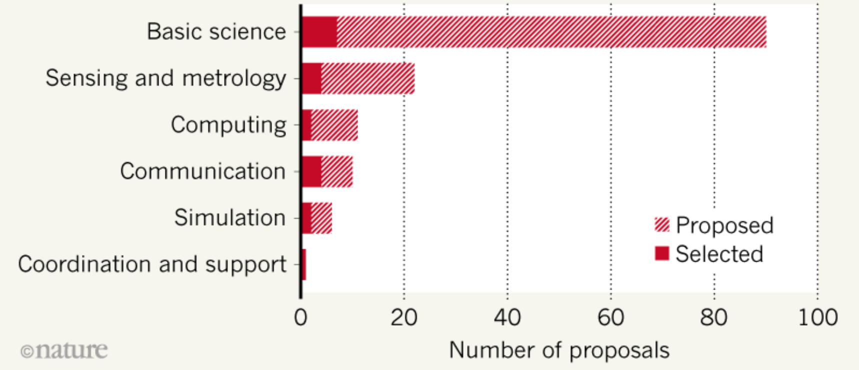
The future is Quantum.

The Second Quantum Revolution is unfolding now, exploiting the enormous advancements in our ability to detect and manipulate single quantum objects. The Quantum Flagship is driving this revolution in Europe.

01	02	03	04
1b €	**10+ yrs**	**5000+**	**140**
Quantum Technology will be funded with at least one billion Euro by the European Commission.	Flagship's timescale	researchers residing in all EU and associated countries involved	Research and Innovation Actions (RIA) proposals submitted in response of the first Quantum Flagship call

QUANTUM WINDFALL

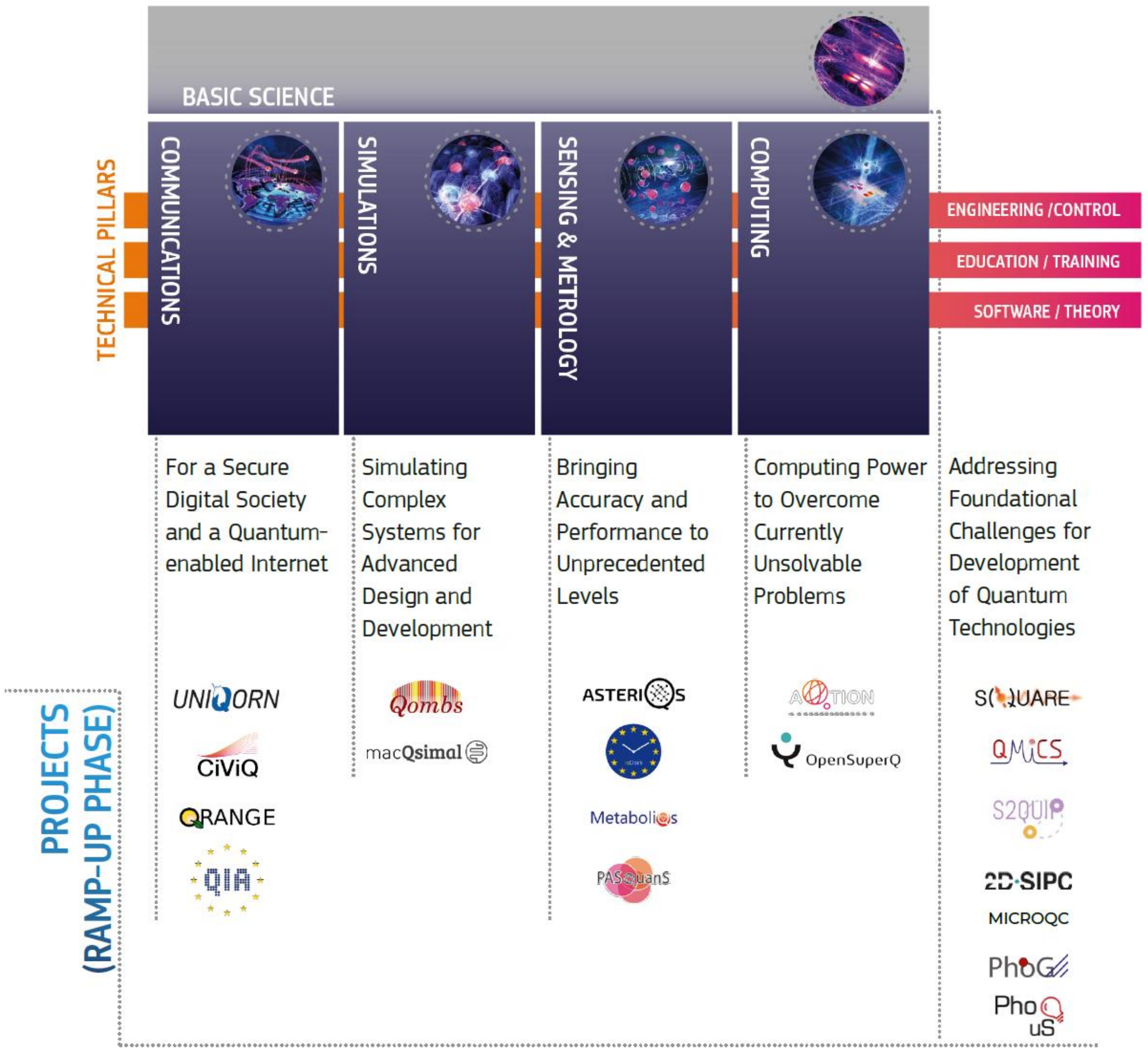
Europe's Quantum Flagship programme will spend €132 million (US$150 million) overall on 20 projects spanning 6 themes for its first 3 years.



PILLARS OF ACTIVITY

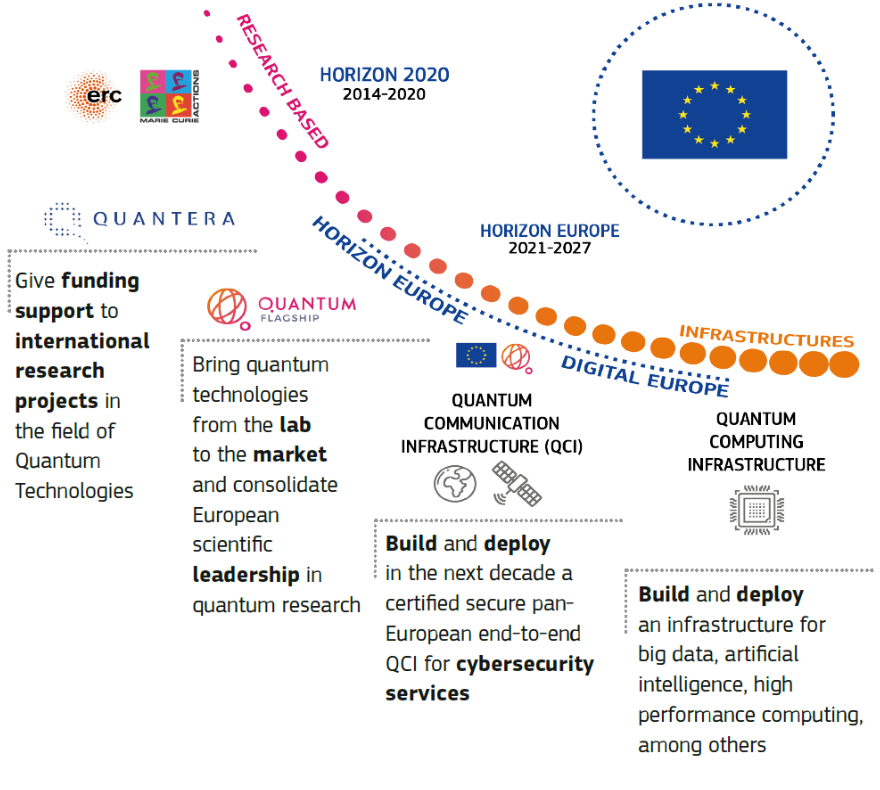
OF THE QUANTUM FLAGSHIP

Developments in leading areas of quantum technologies can be expected to produce transformative applications with real practical impact on society. That is why the Quantum Flagship has divided research and innovative efforts in five main areas of research and innovation.



FROM VISION TO REALITY

FUNDING OPPORTUNITIES NOW AND IN THE FUTURE

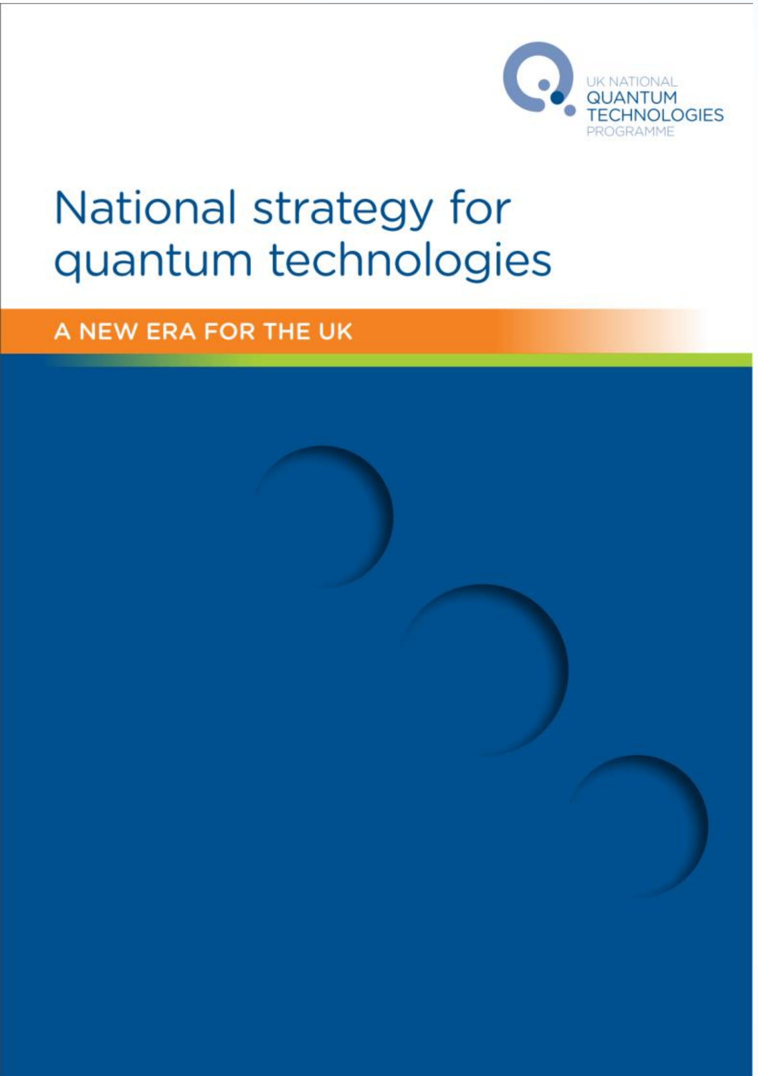


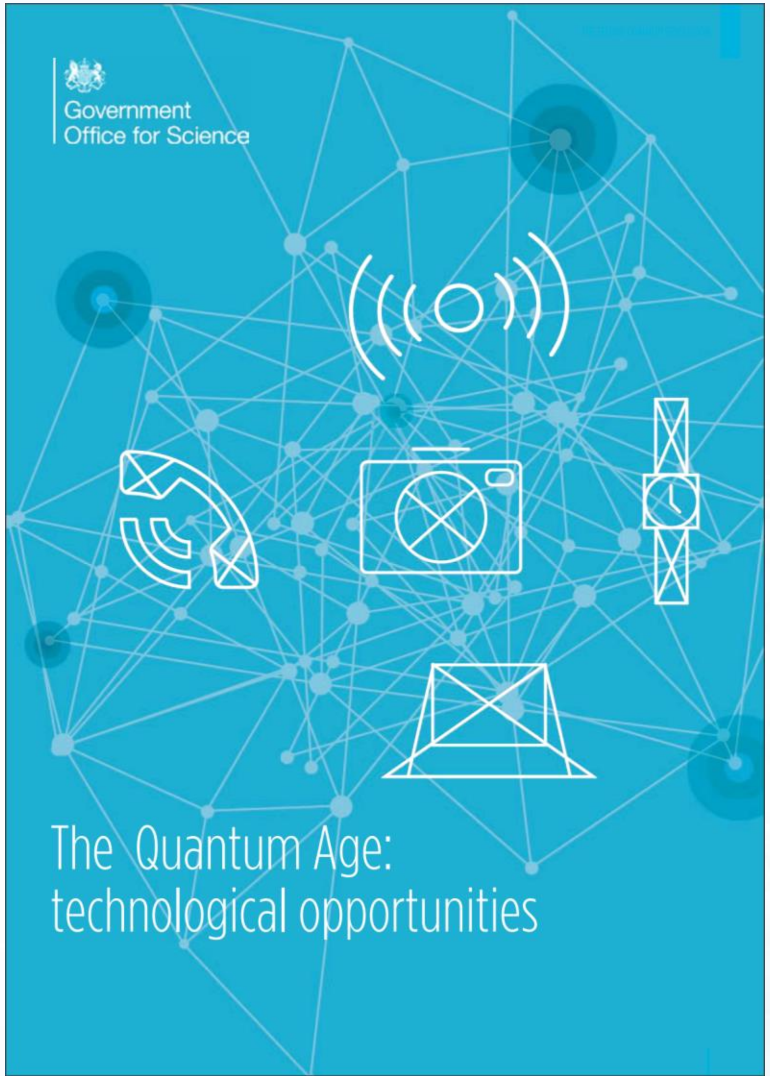
QIA QUANTUM INTERNET ALLIANCE

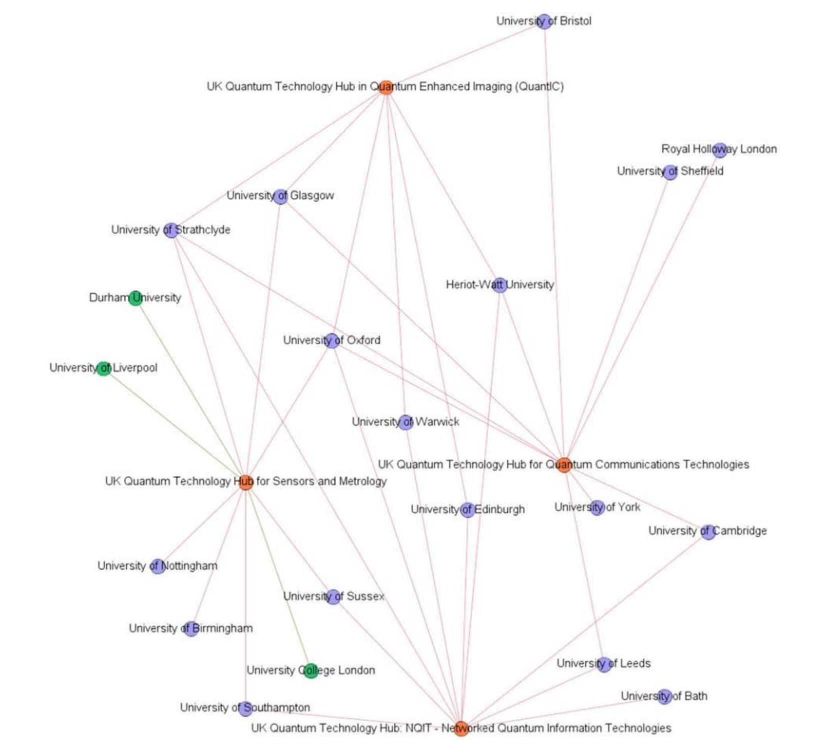
QUANTUM FLAGSHIP

Quantum Information Projects – UK

- A five-year £270M programme started from 2014 → more than £1B until now







Quantum Technology Hubs

- Networked Quantum Information Technologies (NQIT)
- Quantum Sensing and Metrology
- Quantum Communications Technologies
- Quantum-Enhanced Imaging (QuantIC)

4 Lead Universities, 16 partner Universities, many companies, and Government departments

National Facilities

- Quantum Metrology Laboratory (National Physical Laboratory)
- Kelvin Nanotechnology (University of Glasgow)
- Optoelectronic Research Center (University of Southampton)
- Defense Science and Technology Laboratory. (DSTL)

& others

Quantum Systems Engineering Skills Hubs

- Quantum Engineering and Science
- Quantum Enterprise
- Innovation in Quantum Business

3 Lead Universities, several partner Universities, many companies, several Government departments

Quantum Information Projects – Australia

CENTRE FOR
QUANTUM COMPUTATION &
COMMUNICATION TECHNOLOGY

AUSTRALIAN RESEARCH COUNCIL CENTRE OF EXCELLENCE

EQUS
Australian Research Council
Centre of Excellence for
Engineered Quantum Systems

We are Sydney Quantum Academy

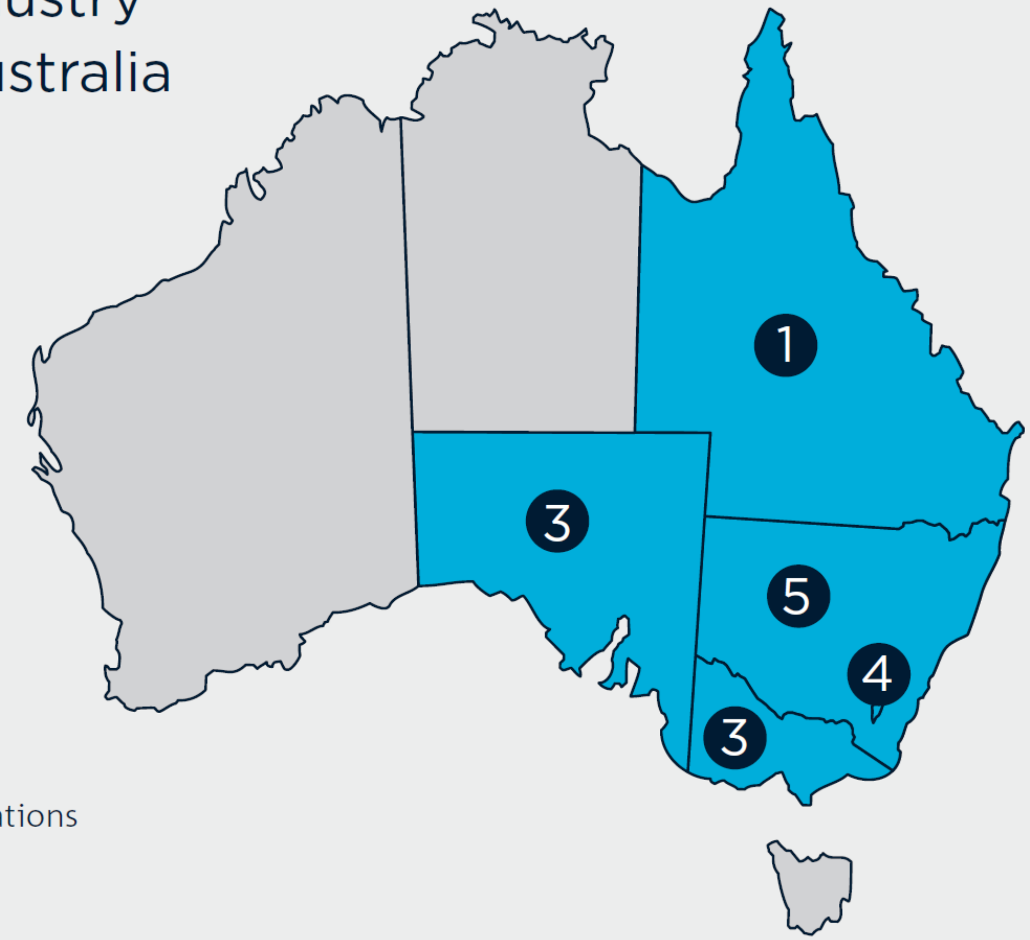
An innovative collaboration between four NSW universities to support the development of a quantum ecosystem through education, industry and community engagement, and entrepreneurship.

Partners

THE UNIVERSITY OF SYDNEY · UTS · MACQUARIE University SYDNEY · AUSTRALIA · UNSW SYDNEY

AUSTRALIA
Australian Government
Australian Research Council

Quantum industry activity in Australia



Quantum sectors

- Quantum computing
- Quantum sensing
- Quantum communications
- Consultancy
- Enabling technology

Queensland
- Max Kelsen

New South Wales
- Microsoft (US)
- Silicon Quantum Computing
- Redback Systems
- Lucigem
- Q-CTRL

Australian Capital Territory
- Quantum Brilliance
- Nomad Atomics
- QuintessenceLabs
- Liquid Instruments

Victoria
- IBM (US)
- h-bar Consultants
- MOGlabs

South Australia
- Archer
- Rigetti Computing (US)
- Cryoclock

16 Quantum-related private organisations around Australia

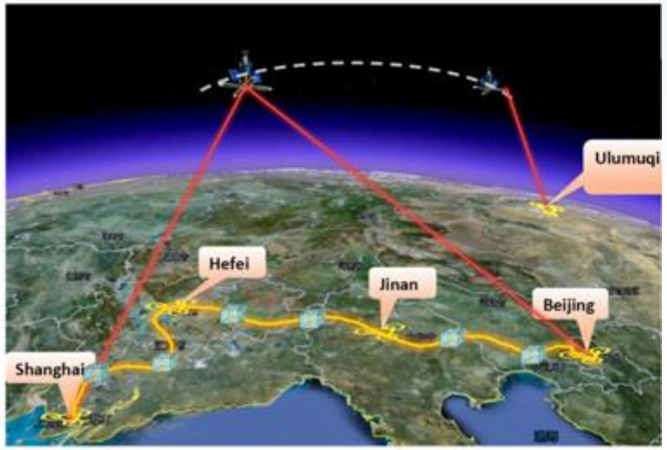
$125m+ Funding and investment (2017–2019)

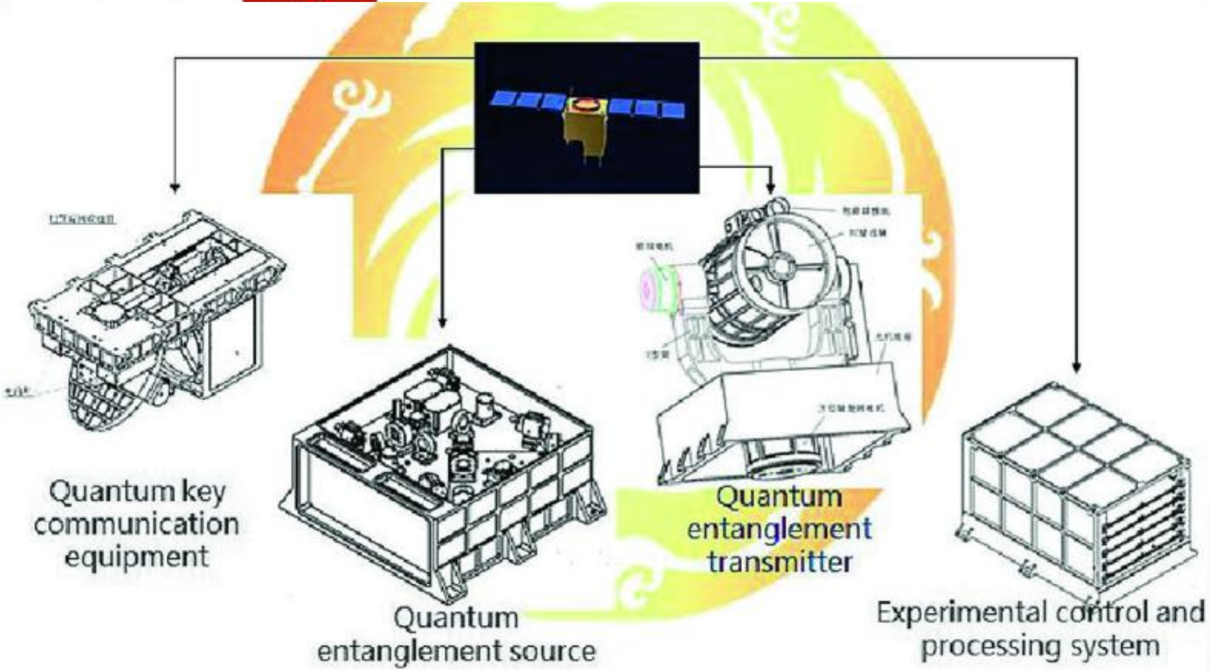
CSIRO

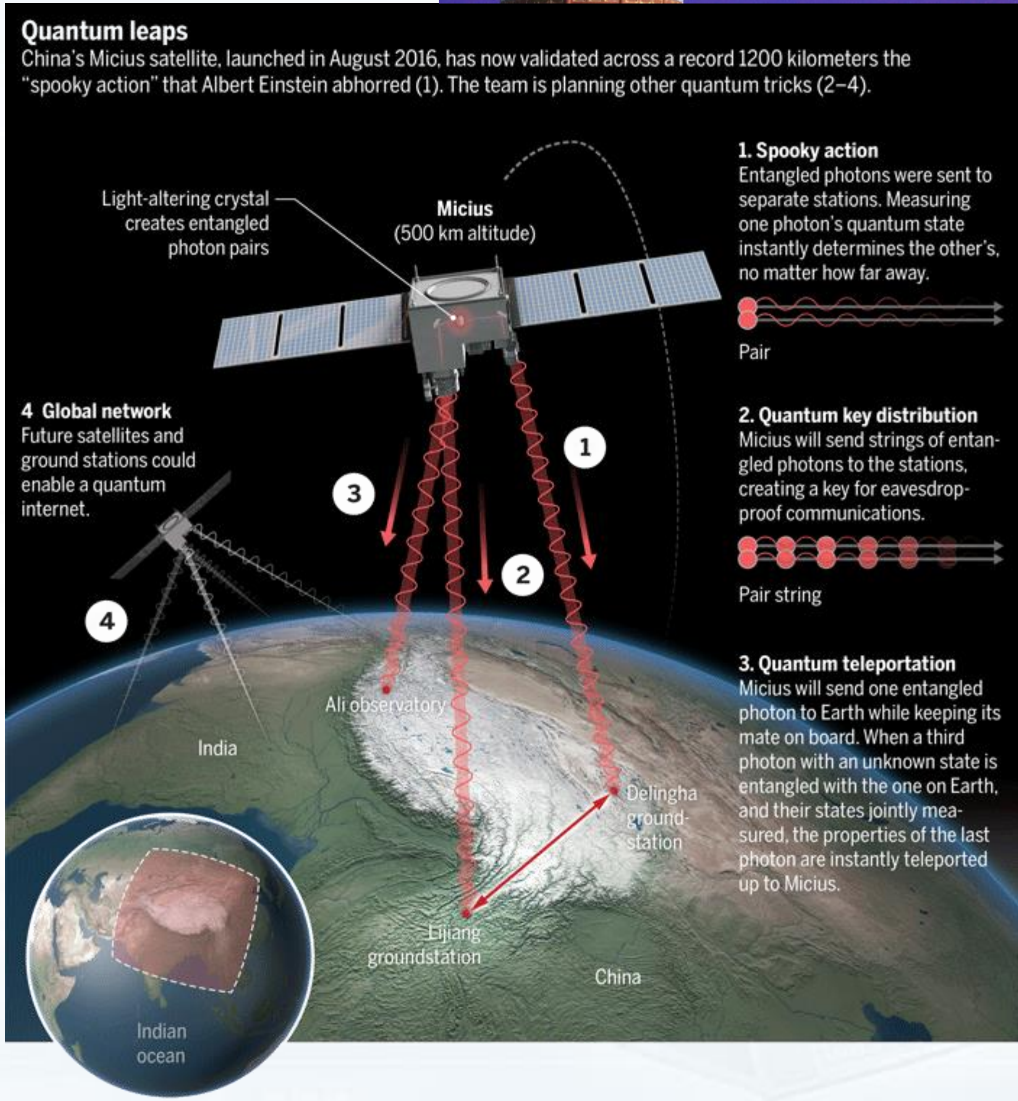
Quantum Information Projects – China

Year	Project	Funding	Total estimated amount (USD)
1998–2006	Minor projects mixed with other fields	NSFC	10 M
2006–2010	1. Quantum control 2. Single quantum state detection and interaction 3. Long distance quantum communication 4. Key technology research and verification of quantum experiments at space scale	1. MOST 2. NSFC 3. CAS 4. CAS	150 M
2011–2015	1. Quantum control 2. Quantum metrology 3. National major scientific research instruments and equipment development **4. Quantum experiments at space scale** 5. Coherent control of quantum systems and metrology physics in atomic systems 6. Quantum secure communication backbone	1. MOST 2. NSFC 3. NSFC 4. CAS 5. CAS 6. NDRC, CAS, etc.	490 M
2016–now	1. Quantum control	1. MOST	337 M

Quantum Experiments at Space Scale







nature

Explore our content ⌄ Journal information ⌄

nature > letters > article

Published: 09 August 2017

Ground-to-satellite quantum teleportation

Ji-Gang Ren, Ping Xu, [...] Jian-Wei Pan

Nature **549**, 70–73(2017) | Cite this article

Science Contents News Careers Journals

SHARE

RESEARCH ARTICLES | PHYSICS

Satellite-based entanglement distribution over 1200 kilometers

Juan Yin[1,2], Yuan Cao[1,2], Yu-Huai Li[1,2], Sheng-Kai Liao[1,2], Liang Zhang[2,3], Ji-Gang Ren[1,2], Wen-Qi Cai[1,2], Wei-Yue Liu[1]...
+ See all authors and affiliations

Science 16 Jun 2017:
Vol. 356, Issue 6343, pp. 1140-1144
DOI: 10.1126/science.aan3211

PHYSICAL REVIEW LETTERS **120**, 030501 (2018)

Editors' Suggestion | Featured in Physics

Satellite-Relayed Intercontinental Quantum Network

Sheng-Kai Liao,[1,2] Wen-Qi Cai,[1,2] Johannes Handsteiner,[3,4] Bo Liu,[4,5] Juan Yin,[1,2] Liang Zhang,[2,6] Dominik Rauch,[3,4] Matthias Fink,[4] Ji-Gang Ren,[1,2] Wei-Yue Liu,[1,2] Yang Li,[1,2] Qi Shen,[1,2] Yuan Cao,[1,2] Feng-Zhi Li,[1,2] Jian-Feng Wang,[7] Yong-Mei Huang,[8] Lei Deng,[9] Tao Xi,[10] Lu Ma,[11] Tai Hu,[12] Li Li,[1,2] Nai-Le Liu,[1,2] Franz Koidl,[13] Peiyuan Wang,[13] Yu-Ao Chen,[1,2] Xiang-Bin Wang,[2] Michael Steindorfer,[13] Georg Kirchner,[13] Chao-Yang Lu,[1,2] Rong Shu,[2,6] Rupert Ursin,[3,4] Thomas Scheidl,[3,4] Cheng-Zhi Peng,[1,2] Jian-Yu Wang,[2,6] Anton Zeilinger,[3,4] and Jian-Wei Pan[1,2]

nature

Explore our content ⌄ Journal information ⌄

nature > articles > article

Published: 09 August 2017

Satellite-to-ground quantum key distribution

Sheng-Kai Liao, Wen-Qi Cai, [...] Jian-Wei Pan

Nature **549**, 43–47(2017) | Cite this article

nature

Explore our content ⌄ Journal information ⌄

nature > articles > article

Article | Published: 15 June 2020

Entanglement-based secure quantum cryptography over 1,120 kilometres

Juan Yin, Yu-Huai Li, Sheng-Kai Liao, Meng Yang, Yuan Cao, Liang Zhang, Ji-Gang Ren, Wen-Qi Cai, Wei-Yue Liu, Shuang-Lin Li, Rong Shu, Yong-Mei Huang, Lei Deng, Li Li, Qiang Zhang, Nai-Le Liu, Yu-Ao Chen, Chao-Yang Lu, Xiang-Bin Wang, Feihu Xu, Jian-Yu Wang, Cheng-Zhi Peng, Artur K. Ekert & Jian-Wei Pan

Nature **582**, 501–505(2020) | Cite this article

REPORT

Quantum computational advantage using photons

Han-Sen Zhong[1,2,*], Hui Wang[1,2,*], Yu-Hao Deng[1,2,*], Ming-Cheng Chen[1,2,*], Li-Chao Peng[1,2], Yi-Han Luo[1,2], Jian Qin[1,2], Dian Wu[1,2], Xing Ding[1,2], Yi Hu[1,2], Peng Hu[3], Xiao-Yan Yang[3], Wei-Jun Zhang[3], Hao Li[3], Yuxuan Li[4], Xiao Jiang[1,2], Lin Gan[4], Guangwen Yang[4], Lixing You[3], Zhen Wang[3], Li Li[1,2], Nai-Le Liu[1,2], Chao-Yang Lu[1,2], Jian-Wei Pan[1,2,†]

[1] *Hefei National Laboratory for Physical Sciences at Microscale and Department of Modern Physics, University of Science and Technology of China, Hefei, Anhui 230026, China.*

[2] *CAS Centre for Excellence and Synergetic Innovation Centre in Quantum Information and Quantum Physics, University of Science and Technology of China, Shanghai 201315, China.*

[3] *State Key Laboratory of Functional Materials for Informatics, Shanghai Institute of Microsystem and Information Technology, Chinese Academy of Sciences, Shanghai 200050, China.*

[4] *Department of Computer Science and Technology and Beijing National Research Center for Information Science and Technology, Tsinghua University, Beijing 100084, China.*

† Corresponding author. Email: pan@ustc.edu.cn

* These authors contributed equally to this work.

Science 03 Dec 2020:
eabe8770
DOI: 10.1126/science.abe8770


合肥综合性国家科学中心
Hefei Comprehensive National Science Center

量子体系架构
Quantum Architecture

目标 Aims

支持量子算法的运行，支撑量子人工智能应用，提供 Quantum infrastructure as a Service (QaaS) 综合服务平台。

To support quantum algrithms and quantum AI;

To provide a comprehensive Quantum infrastructure as a Service (QaaS).

方向 Key Areas

- 统一编程平台 Unified Programming Platform
- 分布式量子信息处理 Distributed Quantum Information Processing
- 量子硬件接口 Quantum Hardware Interface
  1. 量子控制（"量脉"）Quantum Control ("Quanlse")
  2. 超导电路设计方案 Superconducting Circuit Design
- 量子网络和因特网 Quantum Network and Internet
- 量子和后量子密码 Quantum and Post-Quantum Crypto

量子人工智能
Quantum AI

目标 Aims

利用量子计算技术促进人工智能领域发展
To utilize quantum computing technoques to promote the development of AI

利用人工智能技术突破量子计算发展瓶颈
To break through the bottlenecks of quantum computing with the advantages of AI

方向 Key Areas

- 机器学习 Machine Learning
  1. 量子神经网络 Quantum Neural Networks
  2. 混合量子网络 Hybrid Quantum-Classical Networks
  3. 嘈杂中型量子算法 Noise Intermediate-Scale Quantum Algorithms
- 信息安全 Information Security
- 区块链 Blockchain

量子算法
Quantum Algorithm

目标 Aims

针对具体任务设计高效的量子算法
To design efficient quantum algorithms for specfic tasks

推广经典算法设计思路和分析技巧到量子情形
To extend the design and analysis of classical algorithms to the quantum scenario

优化现有量子(经典)算法，探索可行性和局限性
To optimize existing quantum (classical) algorithms and explore their feasibility and limitations

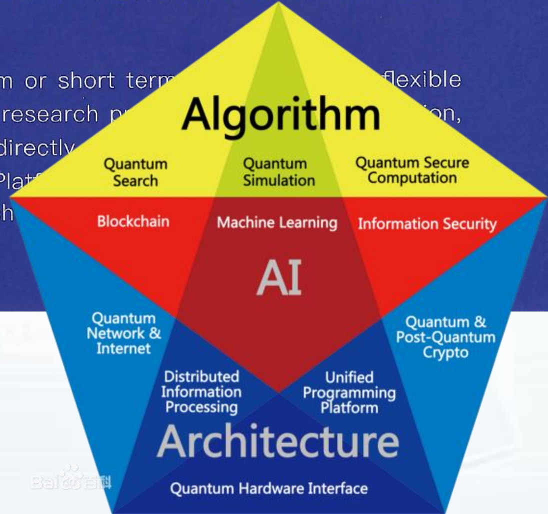
方向 Key Areas

- 量子模拟 Quantum Simulation
- 量子搜索 Quantum Search
- 量子安全计算 Quantum Secure Computation

职位
Positions

无论你是希望长期加入百度量子计算团队，还是进行短期学习交流，我们都将为你提供灵活多变的岗位选择，宽松自由的学习成长环境，先进前沿的研究课题。获取更多信息，请发送邮件到 quantum@baidu.com 或咨询现场人员。衷心期待你的加入！同时，欢迎大家体验我们团队的量脉设计平台，助力科研项目。最后，诚邀大家申请百度研究提供的“北极星计划”，感受产研协同合作。

in the long term or short term ... flexible
... cutting-edge research ... on,
... or talk to us directly
... by our Quanlse Plat...
... Baidu Research



Quantum Software Engineer, Design Automation

Location: Hangzhou

Job description:

As a Quantum Software Engineer focusing on Design Automation, you will work with our scientists and engineers together to support theoretical modeling, simulation and design of superconducting quantum computer.

Responsibility:

- Perform electromagnetic field simulations of microwave and superconducting quantum devices.
- Perform electric circuit simulations.
- Code implementation to support module integration and automation flow design for cross-function and multi-scale simulation.

Requirements:

- Master's or PhD degree in physics, electrical engineering, mathematics, computer science, or other related subjects.
- At least 3 years of experience in software development or application of electromagnetic field and circuit simulation. Experience in simulation of superconducting devices is desirable but not required.
- Proficiency in Python or C/C++. Experience in Perl, Julia, or shell scripts is desirable but not required.
- Knowledge of quantum physics, solid state physics, material science, computational electromagnetics, inverse problem, matrix analysis, or complex analysis is desirable but not required.

Quantum Scientist, Hardware

Locations: Hangzhou

Job description:

As a Quantum Scientist focused on hardware, you will work in a multifunctional team to solve various scientific and engineering problems on the implementation of quantum computing with superconducting circuits.

Responsibility:

- Develop high-performance quantum hardware based on superconducting circuits, including design, fabricate, test, and analyze superconducting quantum devices.
- Perform fundamental researches on fault-tolerant quantum systems based on superconducting circuits.
- Work with the other team members on setting up a new lab.

Requirements:

- Demonstrate a record of research accomplishments in one or more of the following areas: experimental quantum computing, quantum error correction, superconducting device, low-temperature physics, microfabrication, and microwave electronics.
- Strong software engineering skills related to data acquisition, experimental design, and data analysis.

Quantum Process Engineer

Locations: Hangzhou

Job description:

As a Quantum Process Engineer, you will work in a multifunctional team with scientists and engineers to develop the fabrication processes of superconducting quantum circuits.

Responsibility:

- Develop the fabrication processes of superconducting devices.
- Establish and monitor baseline processes of the equipment in QuFab.
- Commission new equipment and perform in-house modifications and upgrades on existing equipment.
- Perform necessary device or film characterization using SEM, AFM, FIB and etc.
- Support Fab manager for necessary user training and orientation.

Requirements:

- Master Degree in a relevant science and engineering fields, such as Electrical Engineering, Physics, Material Science and Chemistry. Ph. D degree preferred.
- Minimum 3-year experience in the fabrication of superconducting/semiconductor-based devices or integrated circuits. Strong expertise in at least one fabrication process of lithography, etching and material growth. Hands-on experience with multiple fabrication processes is a plus.
- Knowledge of chemistry, electrical and optical characterization techniques, packaging techniques, and epitaxial material growth is a plus.
- Experience in both research laboratory and industrial production environments is also desirable.
- Extensive experience in operating and maintaining an electron-beam lithography system is desirable.

Quantum Scientist, Error-Correction

Locations: Hangzhou, Seattle

Job description:

The goal of quantum error-correction is to realize logical qubits with minimum overhead and under hardware constraints. You will work together with a team of quantum error-correction experts to cover a diverse range of important topics, from finding new codes and optimally implementing error-correction, to fundamental questions in the field.

Requirements:

- PhD degree with focus on quantum error correction
- Demonstrated outstanding research capabilities in his/her area of expertise.

Quantum Computer Architect

Location: Hangzhou

Job description:

Quantum Computer Architecture is an exciting emerging discipline on the layer between quantum programs and elementary quantum computing devices. The goal here is to control the quantum devices to optimize key performance factors such as precision, efficiency, scalability, reliability, portability, etc. While many concepts from classical computer architecture such as microarchitecture, instruction set, etc., will continue to be useful, the many new challenges will inspire new concepts and techniques. As a Quantum Computer Architect, you will work with teammates with expertise spanning device physics to classical computer architecture and compilers, and our superconducting quantum processor team, to distill key solution concepts for quantum computer architecture, prototype and implement such solutions in a superconducting quantum computer. This position is based in Hangzhou.

Requirements:

- Ph.D. degree with a focus on computer architecture, or a strong record in industrial computer architecture R&D.
- Experience with high speed digital signal processing.
- Passionate about building a quantum computer; prior experiences on superconducting quantum computing are desirable but not required.

Quantum Scientist, Algorithms

Location: Seattle, Hangzhou

Job description:

As a Quantum Scientist with a focus on algorithms, you will add to the current strength of AQL on quantum algorithms, work with an interdisciplinary and international team to research and implement super-fast quantum and quantum-classical hybrid algorithms for solving fundamental and real-world problems.

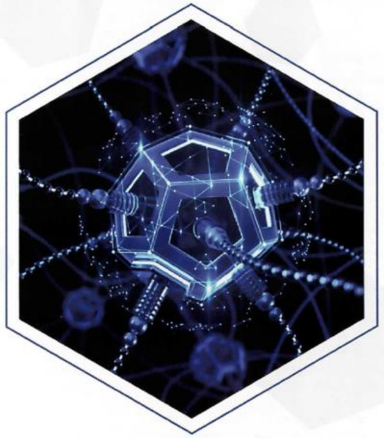
Requirements:

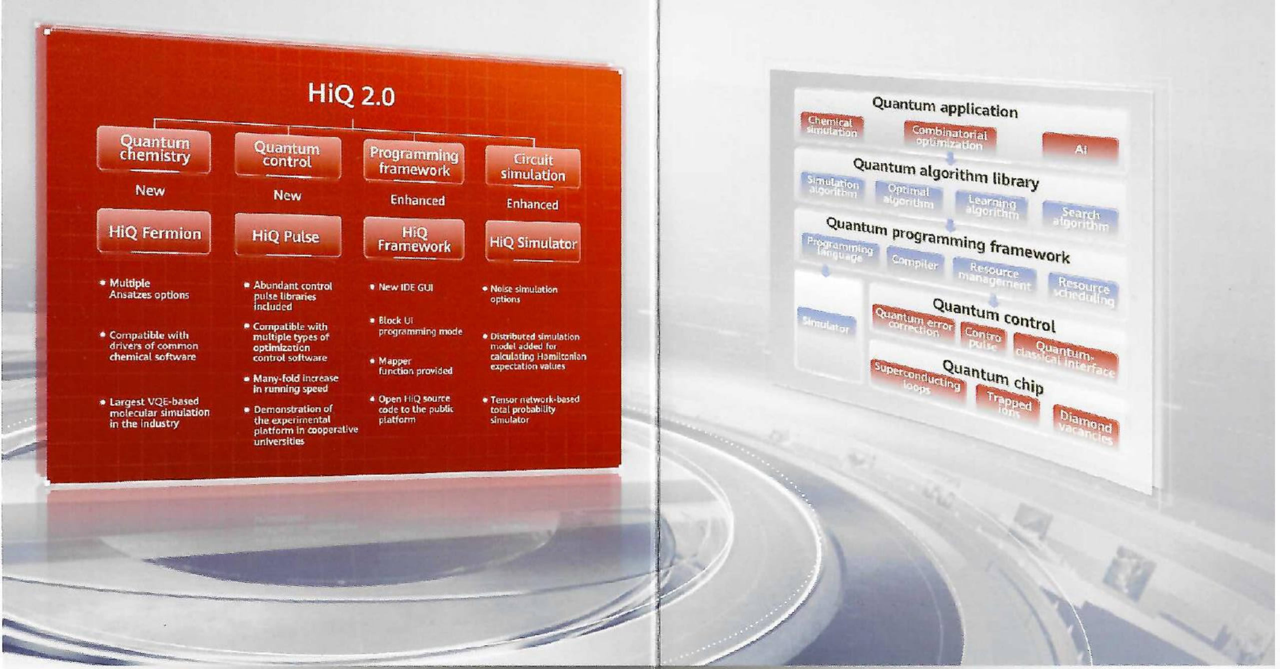
- Ph.D. degree in Mathematics, Physics, Computer Science or closely related field.
- Demonstrated outstanding research capabilities in his/her area of expertise and experience developing quantum algorithms and implementing algorithms on quantum computing architectures.
- Evidence of a strong quantum computing programming background using high-level languages such as Python, C++.
- Experience in gate-based and/or adiabatic quantum computation is required and experience in quantum simulation, machine learning methods, high performance computing or circuit synthesis will be taken into consideration.

DAMO
ALIBABA DAMO ACADEMY

Career
@Alibaba Quantum Lab

Realizing the potentials of quantum computing





HiQ

Huawei Quantum Cloud Service Platform

Abstract:

Leveraging Huawei's leading capability in integrated information and communication technology (ICT), Huawei launched HiQ cloud platform for the development of quantum computing software. Aiming at the promotion of global cooperation, Huawei's HiQ cloud platform is open to the public, where a wide spectrum of developers, researchers, teachers and students can perform fundamental research and develop industrial applications in quantum computing technology.

HiQ Software Solution

Quantum hardware design and verification

Quantum software exploration, research, and verification in advance

Quantum algorithm exploration, design, and verification in advance

Education and popularization of quantum computing

Based on this platform, Huawei will continue to add QC-related ICT enabling technologies

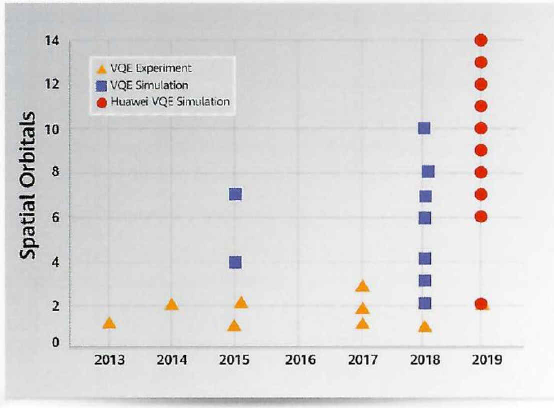
Huawei HiQ Fermion

HiQ Fermion is developed for the recent killer application, quantum chemistry simulation, of NISQ quantum devices. Huawei HiQ Fermion provides a one-step quantum chemistry simulation solution on HUAWEI ClOUD.

Huawei quantum chemistry software HiQ Fermion

1. **Comprehensive** initial-state ansatz library, including UCC, Hardware Efficient, and Qubit CC
2. **Compatible** with drivers of common classical quantum chemistry software such as Gaussian, NWChem, PySCF, and Psi4
3. Multiple **mainstream** Fermi encoding methods provided: Jordan-Wigner, Parity, Bravyi-Kitaev, etc.
4. Optimizers that support **parallel** computing gradients, providing **faster** convergence
5. **Largest VQE-based molecular simulation (H2S, 11 orbitals) in the industry (Core techniques: high-quality initial-state ansatz preparation, effective parameter reduction, circuit optimization, parallel gradient calculation, etc.)**
6. User-friendly GUI-based programming experience

Quantum Chemistry Simulation Benchmarking



1. Multi-parameter reduction algorithm, reducing parameters by up to 80%
2. Multi-parameter gradient optimizer, with 300+ parameters tested
3. Quantum circuits simplified by up to 70%

HUAWEI

HUAWEI HiQ

Quantum Computing Cloud

HiQ Simulator 量子线路模拟

HiQ Fermion 量子化学模拟

HiQ Pulse 量子调控

HiQ Framework 量子计算机架构

HiQ Free Account Registration

https://hiq.huaweicloud.com

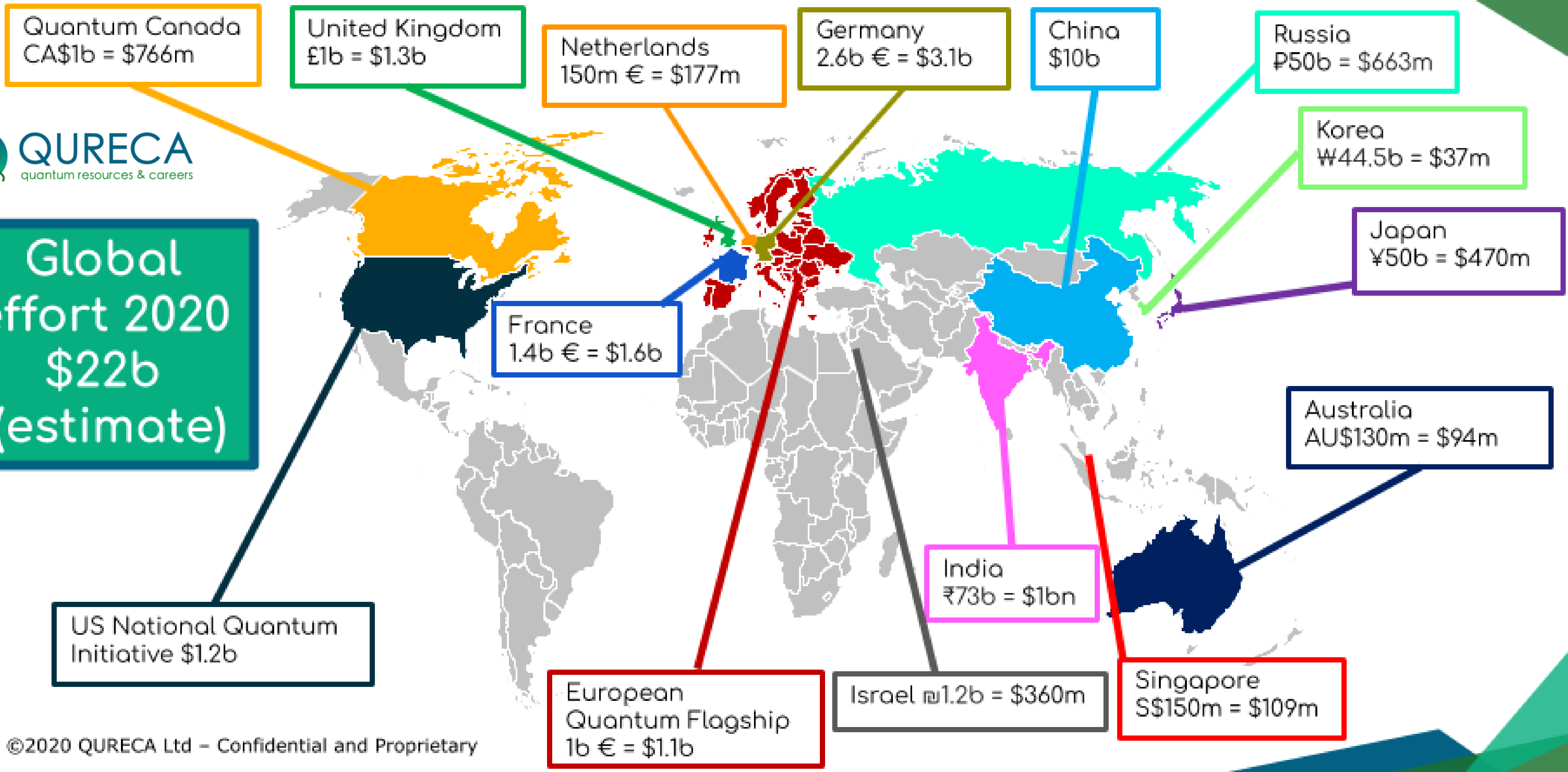
https://github.com/Huawei–HiQ/

HiQ

Quantum effort worldwide

QURECA
quantum resources & careers

Global effort 2020 $22b (estimate)



Quantum Information (Qubits)

- A bit of *classical* information - A binary digit can have only one of two values, and may be physically represented with a two-state device, e.g. {0,1}.
- A bit of *quantum* information – a two-state quantum-mechanical system.


PHYSICS TODAY

HOME BROWSE▾ INFO▾ RESOURCES▾ JOBS

Home > Physics Today > Volume 44, Issue 5 > 10.1063/1.881299

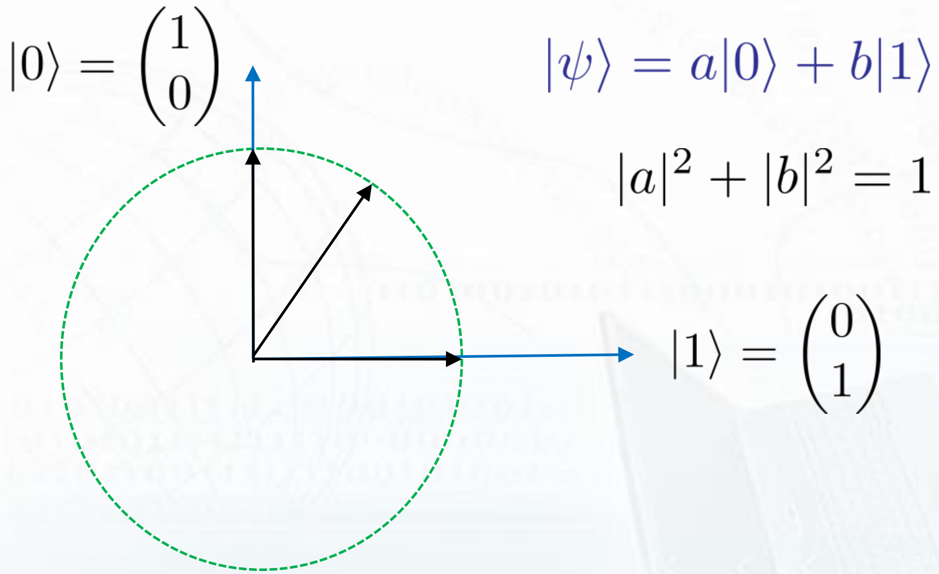
01 MAY 1991 • page 23

Information is Physical

There are no unavoidable energy consumption requirements per step in a computer. Related analysis has provided insights into the measurement process and the communication schannel, and has prompted speculations about the nature of physical laws.

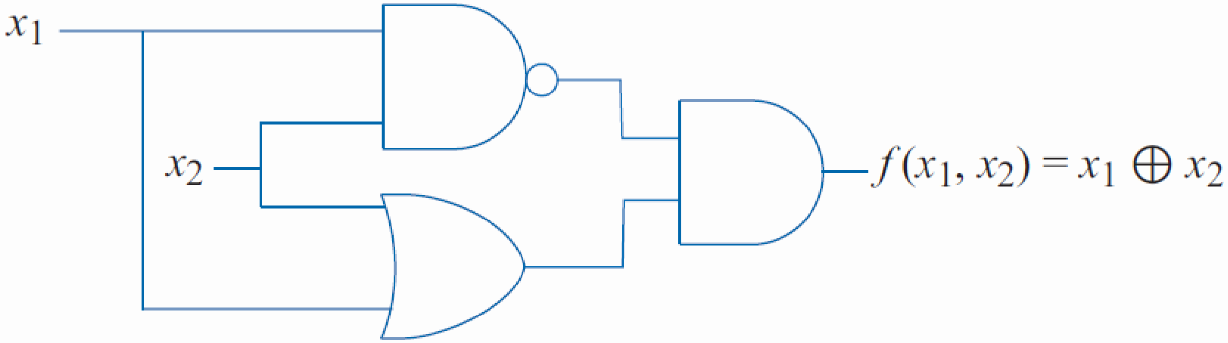
Rolf Landauer

Thomas J. Watson Research Center, Yorktown Heights, New York



What's Computation?

- Classical digital computers (under the Boolean circuit model) uses binary digit (*bits*, 0s or 1s) to store, transfer, manipulate data

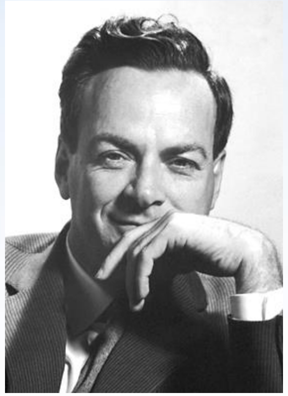


Alan Turing (1912-1954)

- A *bit* can possibly be only one of two states: it is either a one or a zero.
- The two states of each bit are represented in the computer by a two-level system.
- A quantum computer is a device that leverages specific properties described by quantum mechanics to perform computation

  → Quantum computer uses quantum bits (*qubits*).

Brief History of Quantum Computation (1/2)



Richard Feynman
(1918-1988)

- Paul Benioff (1979):
  "The computer as a physical system: A microscopic quantum mechanical Hamiltonian model of computers as represented by Turing machines.
- Feynman (1981): "Why don't we store information on individual particles that already follow the very rules of quantum mechanics that we try to simulate?

"Nature Isn't classical, dammit, and if you want to make a simulation of nature, you'd better make it quantum mechanical."

- David Deutsch (1985) described what a quantum algorithm would look like, and Richard Jozsa (1992) demonstrated a *deterministic* quantum advantage.
- Umesh Vazirani and Ethan Bernstein (1993) pushed it forward (bounded error).
- Daniel Simon (1994) demonstrated an exponential speedup.

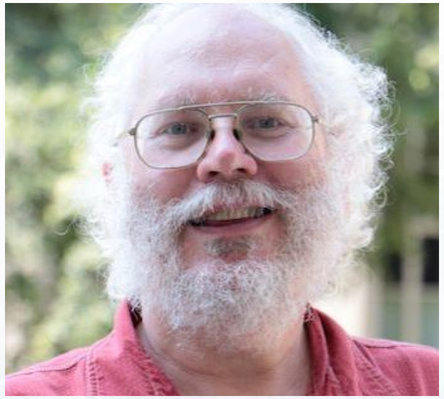
Brief History of Quantum Computation (2/2)

- Seth Lloyd (1993) described a method of building a working quantum computer.
- Peter Shor (1994) invented a polynomial-time quantum algorithm for factoring.
- David DiVincenzo (1996) outlined the key criteria of a quantum computer.
- Isaac Chuang *et al.* (2001) implemented Shor's algorithm on a nuclear magnetic resonance (NMR) system to factor the number 15 as a demonstration.

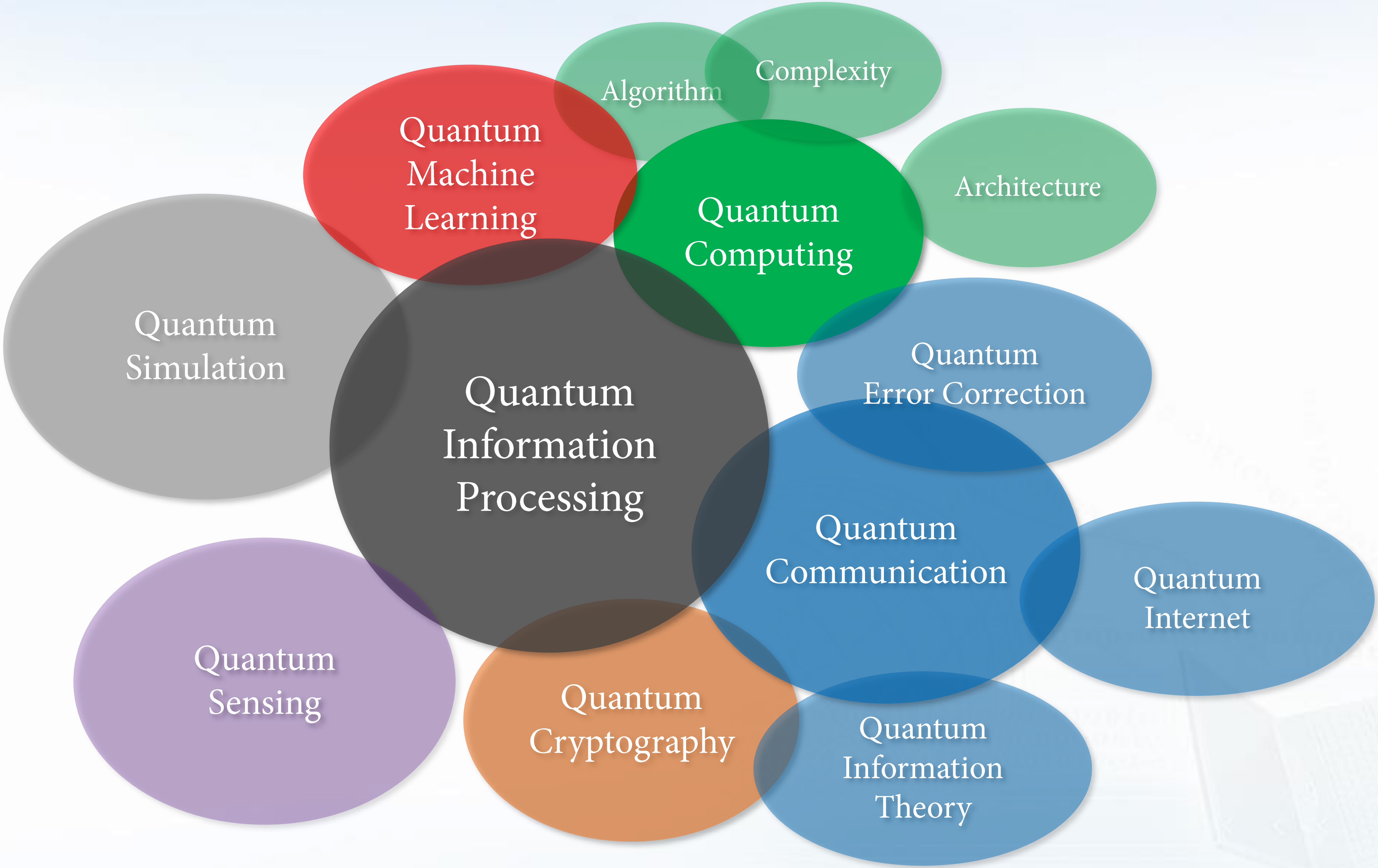
⋮

- → A variety of interdisciplinary fields such as Quantum Computation, Quantum Communication, Quantum Simulation, Quantum Sensing, Quantum Chemistry, etc.

Quantum Information Science

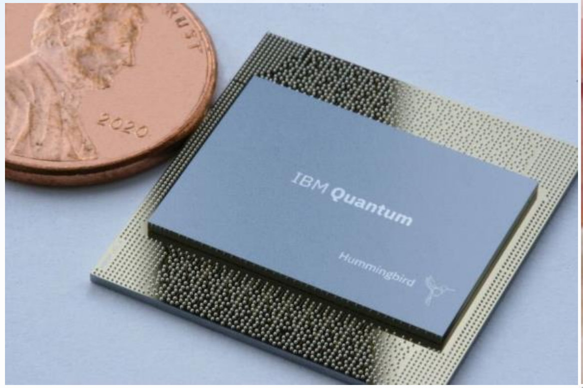


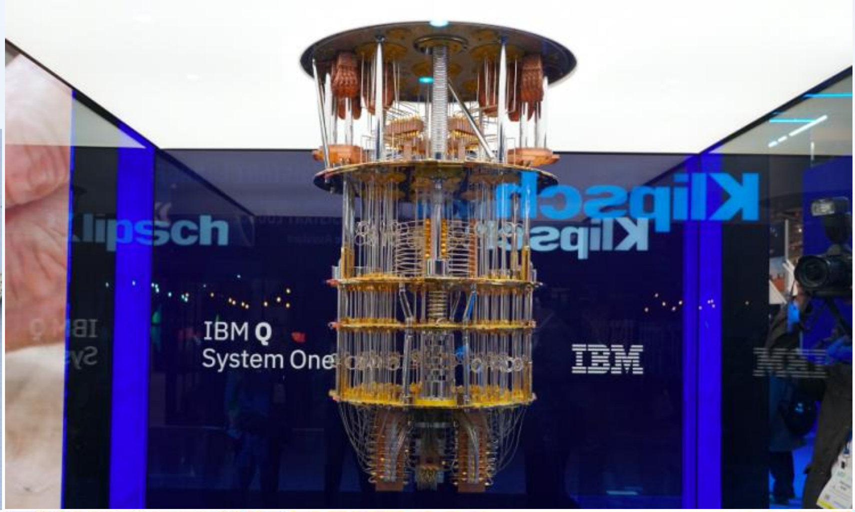
Peter Shor (1959 -)


Algorithm
Complexity
Quantum Machine Learning
Quantum Computing
Architecture
Quantum Simulation
Quantum Information Processing
Quantum Error Correction
Quantum Communication
Quantum Internet
Quantum Sensing
Quantum Cryptography
Quantum Information Theory

Realizing Quantum Processors

- IBM
  - IBM Q System One Computer Center
  - 53, 65-qubit processor for IBM Q Network
- Google AI
  - 54-qubit processor “Sycamore”
  - 72-qubit processor “Bristlecone”
- Microsoft
  - Quantum Development Kit
  - Q# Programming Language
  - Azure Quantum – cloud service
- intel
  - 49-qubit processor





nature

Explore our content | Journal information

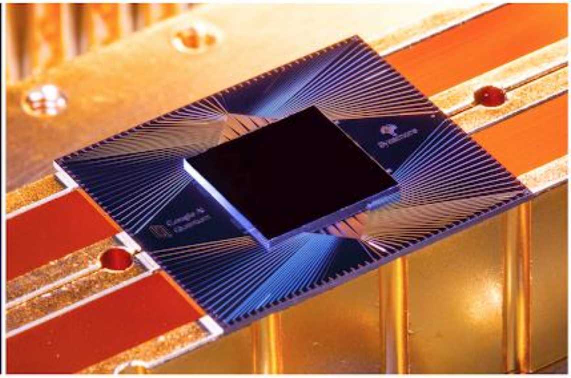
nature > articles > article

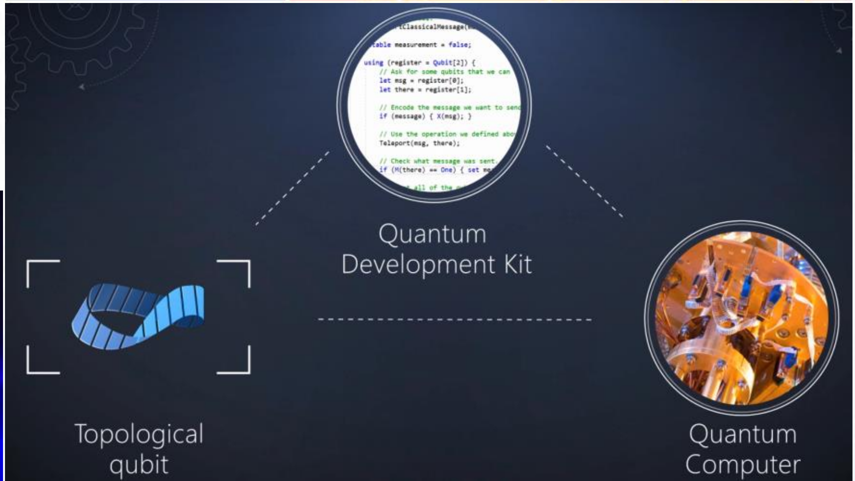
Article | Published: 23 October 2019

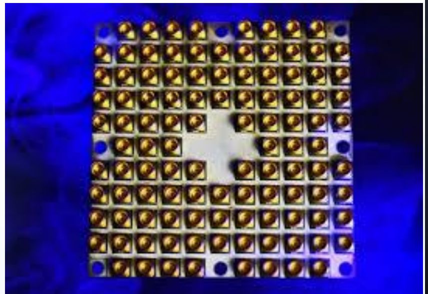
Quantum supremacy using a programmable superconducting processor

Frank Arute, Kunal Arya, [...] John M. Martinis

Nature **574**, 505–510(2019) | Cite this article

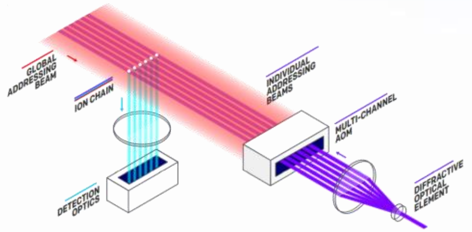




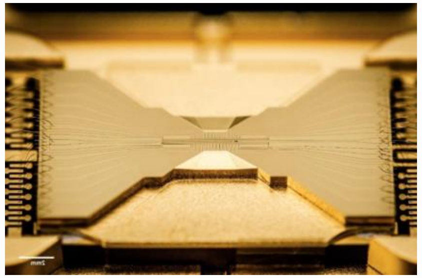


Other Quantum Processors

Trapped Ion



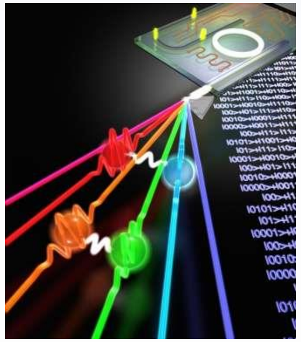
IONQ



(32 qubits)

Honeywell

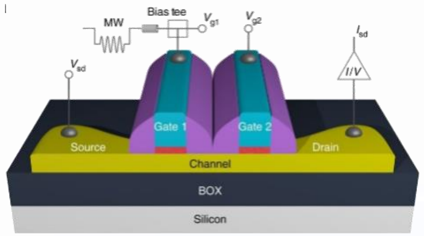
Photonics



XANADU

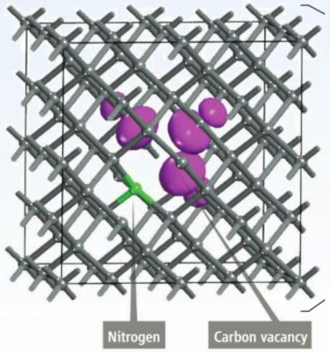
Ψ PsiQuantum

Silicon-Based Spin



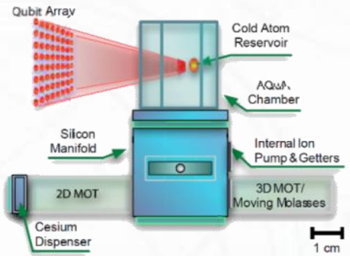
Silicon Quantum Computing

NV Center-in-Diamond

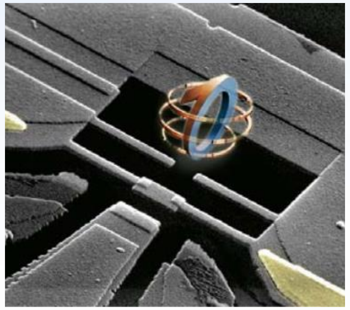


QUANTUM BRILLIANCE

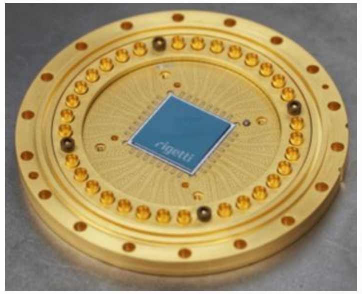
NMR



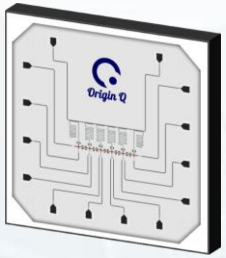
Superconducting



rigetti



本源量子 Origin Quantum

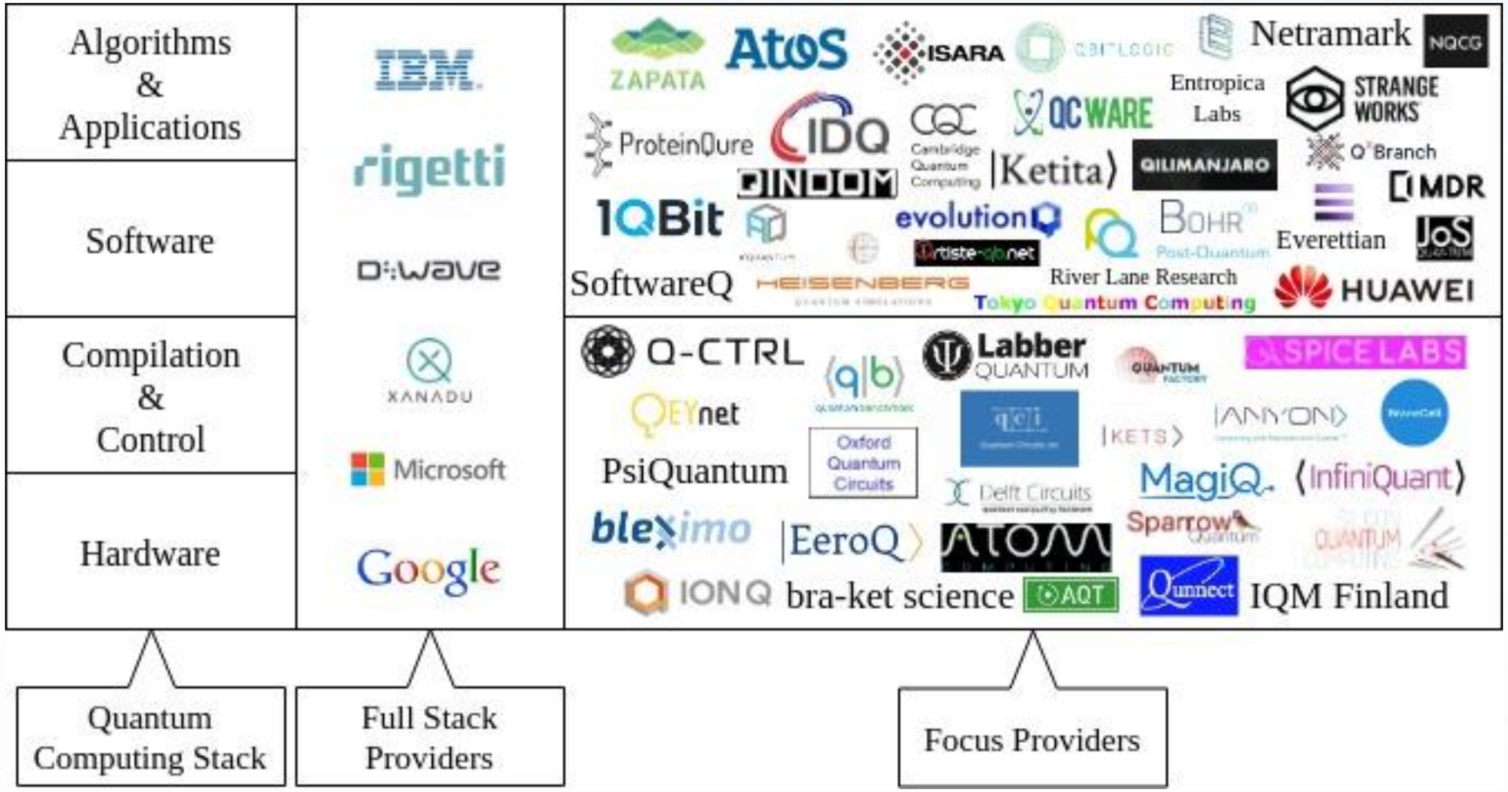


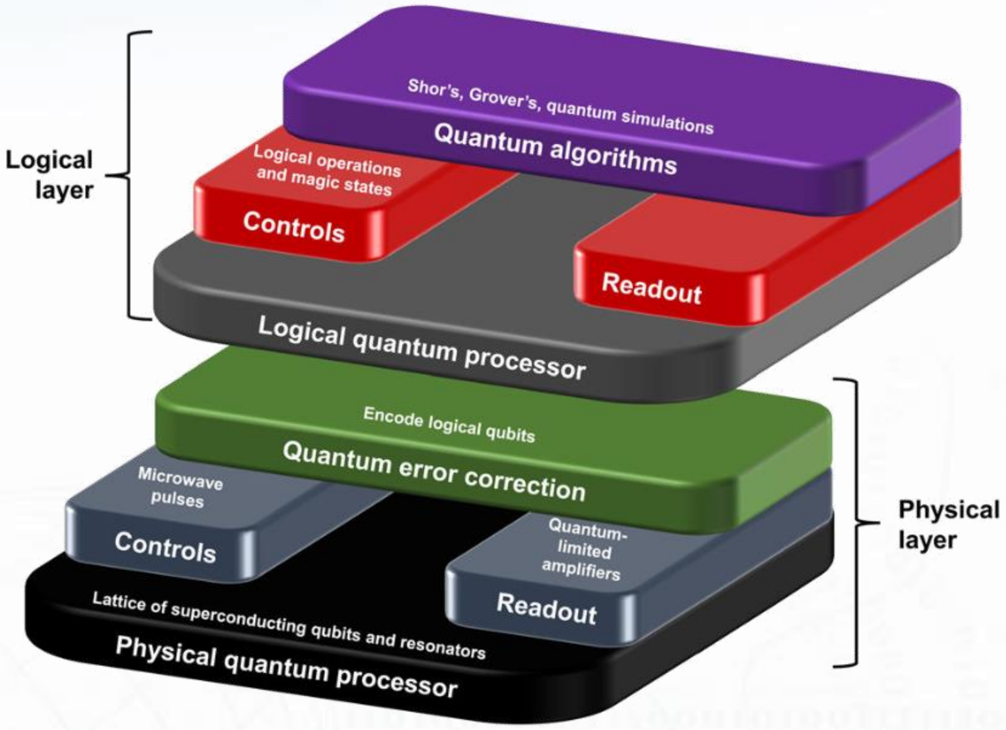
Development Roadmap

IBM **Quantum**

	2019	2020	2021	2022	2023	2024	2025	2026+
Enterprise Clients	Use case exploration Problem mapping Skills building				Workflow integration Application development Skills building			
Model developers					Quantum model services: Natural Sciences, Finance, Optimization, Machine Learning			
Algorithm developers		Qiskit application modules: Natural Sciences, Finance, Optimization, Machine Learning			Prebuilt quantum runtimes		Prebuilt quantum + HPC runtimes	
Kernel developers	Circuits		Qiskit Runtime	Dynamic circuits	Circuit libraries		Advanced control systems	
Quantum systems	**Falcon** 27 qubits	**Hummingbird** 65 qubits	**Eagle** 127 qubits	**Osprey** 433 qubits	**Condor** 1121 qubits	**Beyond** 1K - 1M+ qubits		
IBM Cloud	Circuits		Programs		Models			

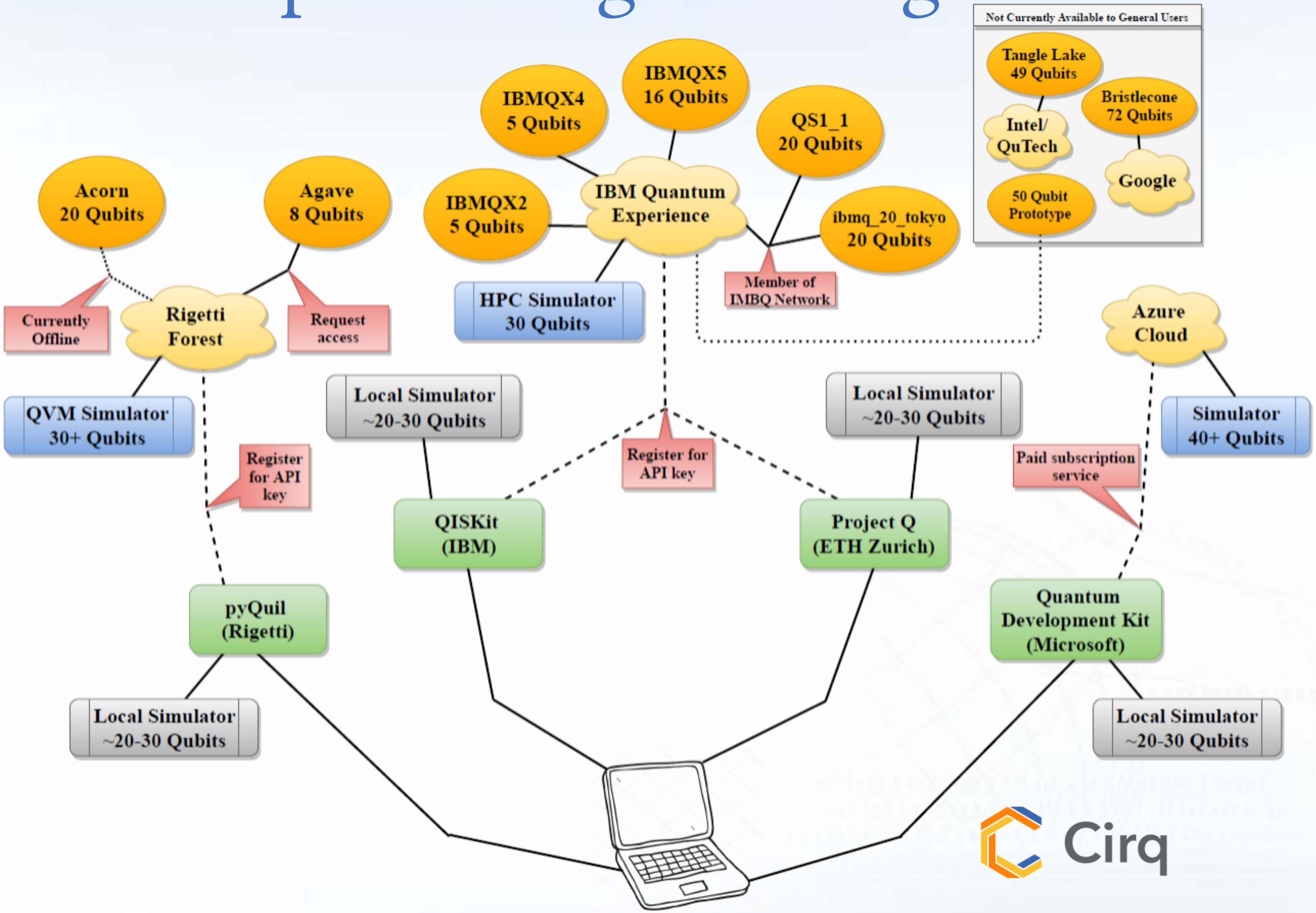
Quantum Computer Stacks





[https://quantumcomputingreport.com/review-of-the-cirq-quantum-software-framework/]
[J. Gambetta, J. Chow, M. Steffen, "Building logical qubits in a superconducting quantum computing system," *npj Quan. Info.*, 2017]

Quantum Computer Programming

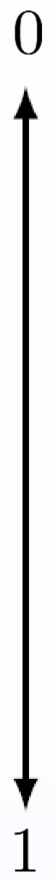


[R. LaRose, "Overview and comparison of gate level quantum software platforms," *Quantum*, 3:130, 2019]

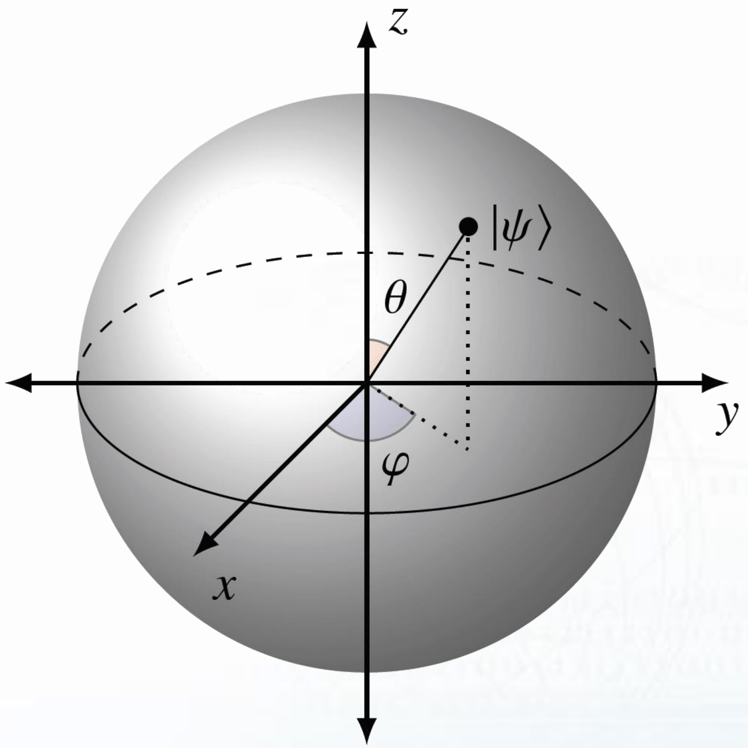
Bloch Representation for a Qubit

$$\Rightarrow |\psi\rangle = \cos(\tfrac{\theta}{2})|0\rangle + \sin(\tfrac{\theta}{2})e^{i\varphi}|1\rangle,\ \theta \in [0,\pi],\ \varphi \in [0, 2\pi]$$

Classical Bit



$|0\rangle \quad \leftarrow (\theta, \varphi) = (0, 0)$



$|1\rangle \quad \leftarrow (\theta, \varphi) = (\pi, 0)$

Quantum Bit

Elementary Quantum Gates

- Pauli gates $X := \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ $Y := \begin{pmatrix} 0 & -\mathrm{i} \\ \mathrm{i} & 0 \end{pmatrix}$ $Z := \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$

- Rotation gates

$$R_x(\phi) := \mathrm{e}^{-i\frac{\phi}{2}X} = \begin{pmatrix} \cos(\frac{\phi}{2}) & -\mathrm{i}\sin(\frac{\phi}{2}) \\ -\mathrm{i}\sin(\frac{\phi}{2}) & \cos(\frac{\phi}{2}) \end{pmatrix}$$

$$R_y(\phi) := \mathrm{e}^{-i\frac{\phi}{2}Y} = \begin{pmatrix} \cos(\frac{\phi}{2}) & -\sin(\frac{\phi}{2}) \\ \sin(\frac{\phi}{2}) & \cos(\frac{\phi}{2}) \end{pmatrix}$$

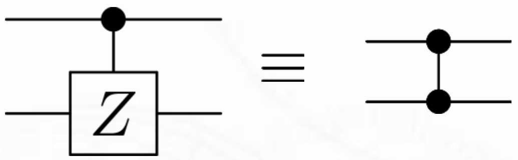
Phase gate

$$R_z(\phi) := \mathrm{e}^{-i\frac{\phi}{2}Z} = \begin{pmatrix} 1 & 0 \\ 0 & \mathrm{e}^{\mathrm{i}\phi} \end{pmatrix} \quad S := R_z(\tfrac{\pi}{2}) \quad T := R_z(\tfrac{\pi}{4})$$

- Hadamard gates

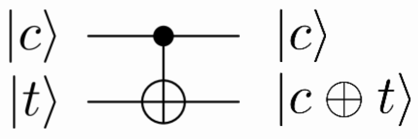
$$H := \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

- Controlled-Z gates



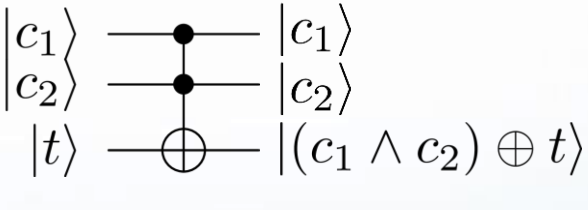
$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix}$$

- CNOT gate



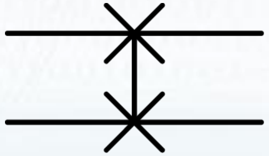
$$\begin{pmatrix} I_2 & 0 \\ 0 & X \end{pmatrix}$$

- Toffoli (CCNOT) gate



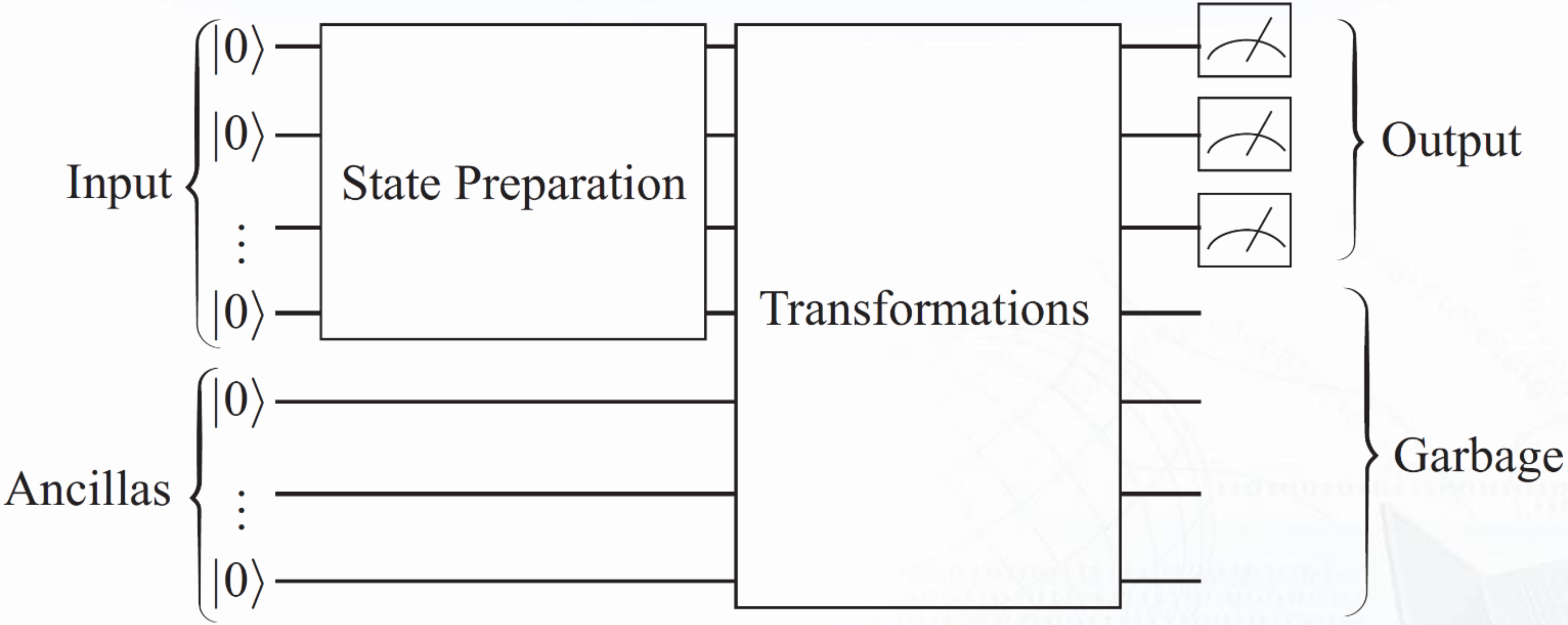
$$\begin{pmatrix} I_3 & 0 & 0 \\ 0 & I_3 & 0 \\ 0 & 0 & X \end{pmatrix}$$

- Swap gate $|\psi\rangle|\phi\rangle \mapsto |\phi\rangle|\psi\rangle$



$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

Gate-Based Quantum Computation



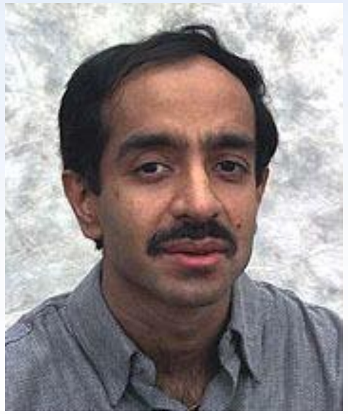
Quantum Advantages

Quantum Features

- Coherence – superposition → More rooms!
  - Quantum parallelism
  - Larger spaces (non-fixed basis)
  - Resource for simulating quantum operations

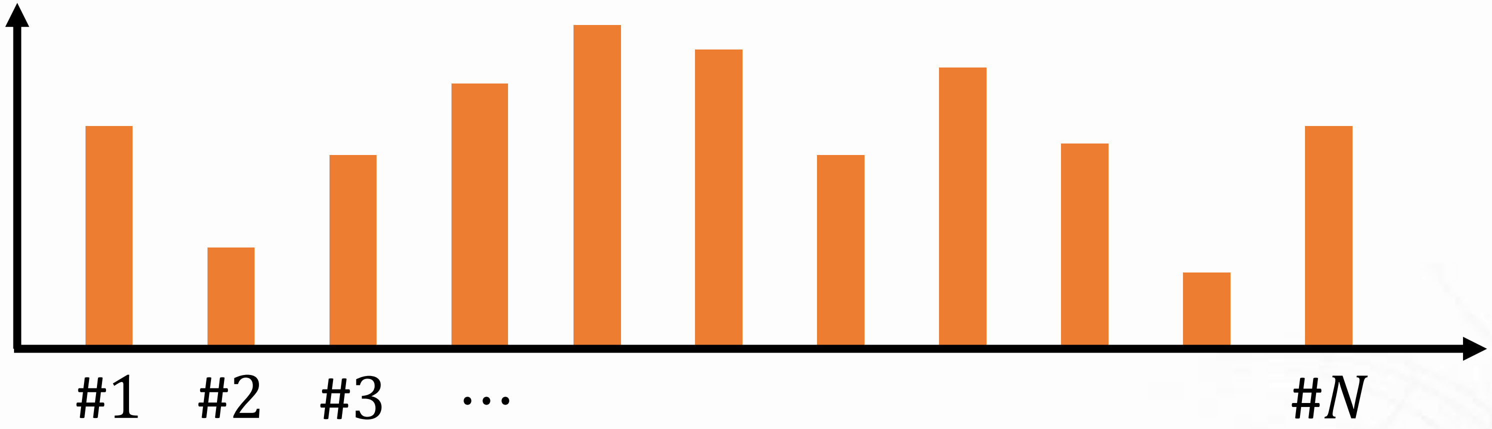
- Entanglement – a correlation → New dimension!
  - Entanglement-assisted communication
  - Resource for quantum communication (teleportation) and computing
- Challenges
  - Non-cloning theorem
  - Non-commutativity (hard to analyze)
  - Quantum state is fragile

Quantum Computing – Unstructured Search



Lov Grover (1961 –)

- Searching in an unstructured list with size N



The best classical algorithm requires number of queries proportional to N

→ Lov Grover (1996) proposed a quantum algorithm requires $\approx \sqrt{N}$ queries

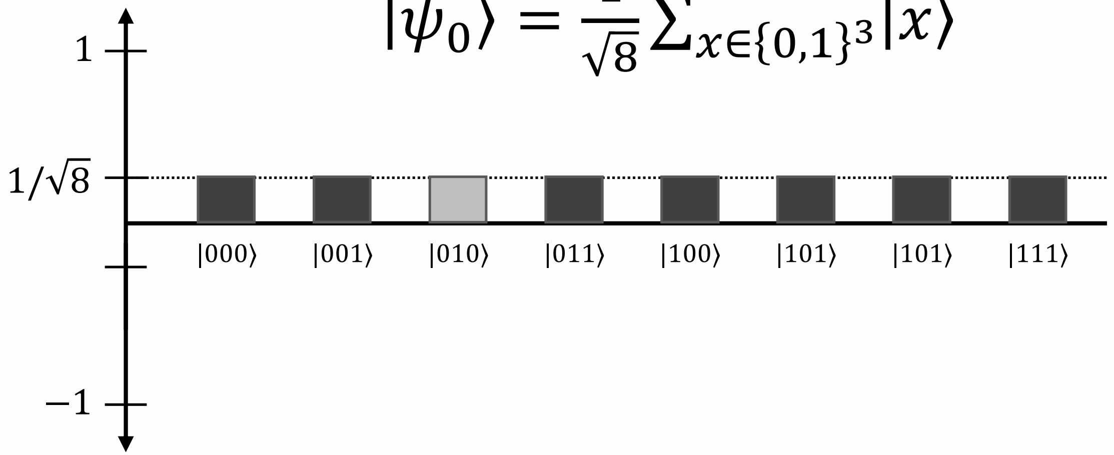
https://rumschuettel.bitbucket.io/grover/index.html

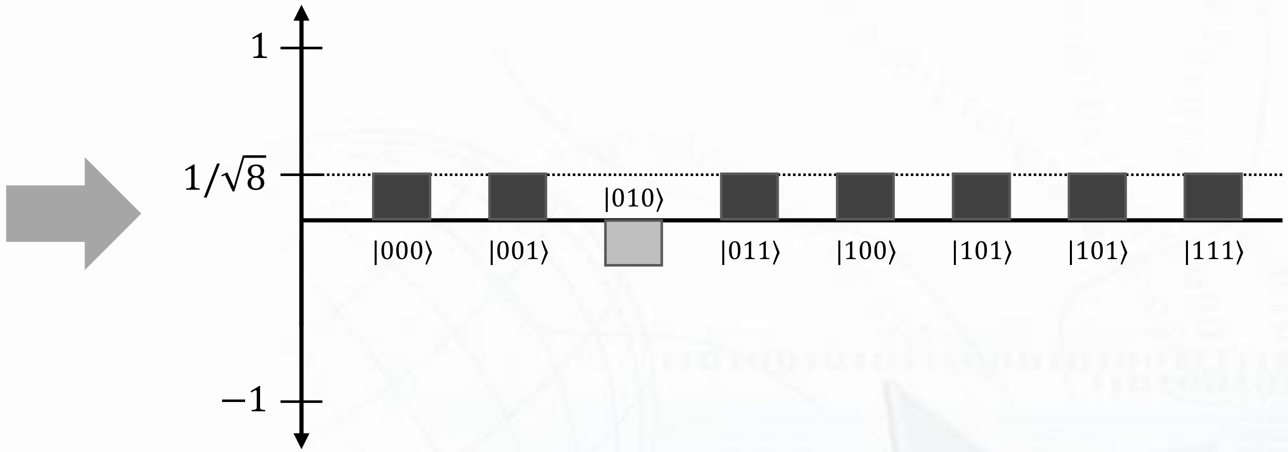
Grover's Search Algorithm (1/3)

- Goal: Transform the superposition such that $|x_0\rangle$ will be measured with high prob.

1. *Flipping the sign* → creating the phase difference: $I_{|x_0\rangle}|x\rangle = \begin{cases} |x\rangle & \text{if } x \neq x_0 \\ -|x_0\rangle & \text{if } x = x_0 \end{cases}$

$$|\psi_0\rangle = \frac{1}{\sqrt{8}}\sum_{x\in\{0,1\}^3}|x\rangle$$

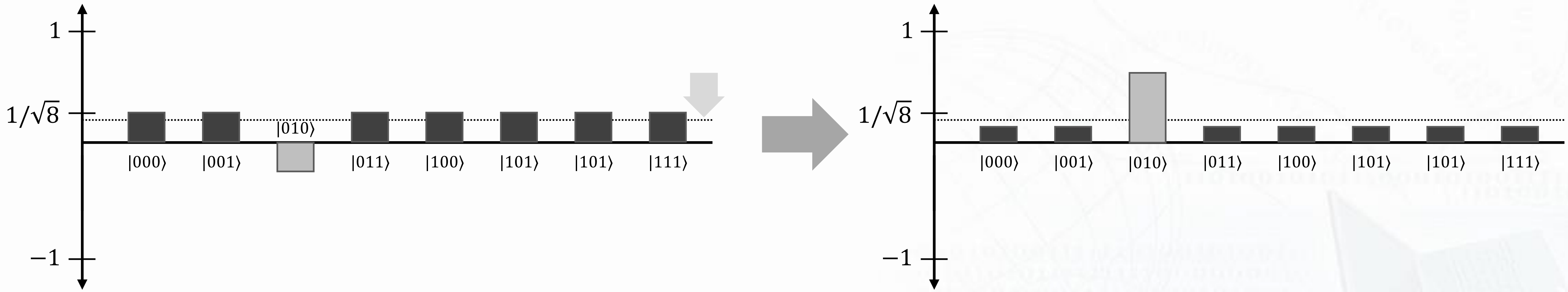




Grover's Search Algorithm (2/3)

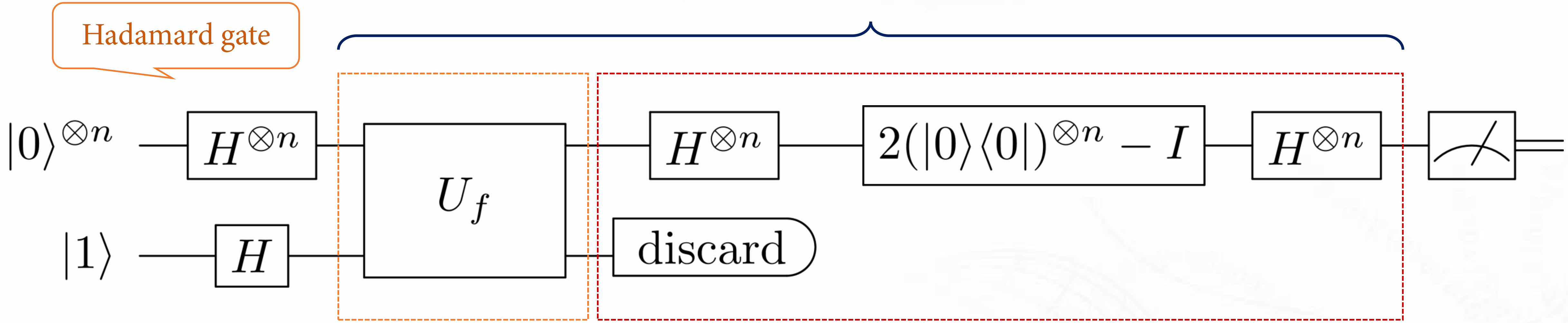
2. *Inversion about mean*:
   Let $\{a_x\}_x$ be a collection of numbers and $\bar{a}$ be the mean. Then the numbers $\{2\bar{a} - a_x\}_x$ are the inversion about mean $\bar{a}$.

$$-I_{|\psi_0\rangle} = 2|\psi_0\rangle\langle\psi_0| - I,\ |\psi_0\rangle := \frac{1}{\sqrt{2^n}} \sum_{x\in\{0,1\}^n} |x\rangle$$



Grover's Search Algorithm (3/3)

Repeat $\frac{\pi}{4}\sqrt{2^n}$ times



Flipping the sign of target x_0

$$I_{|x_0\rangle}|x\rangle = (-1)^{f(x)}|x\rangle$$

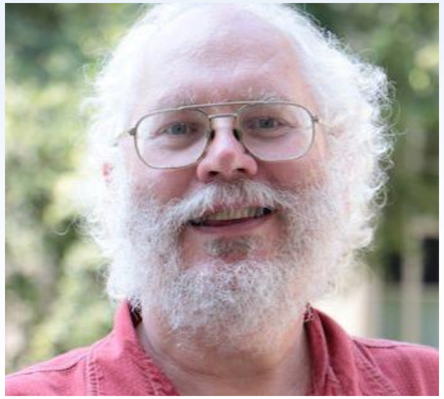
Inversion about mean

$$I_{|\psi_0\rangle} := 2|\psi_0\rangle\langle\psi_0| - I$$

$$= H^{\otimes n}\left(2(|0\rangle\langle 0|^{\otimes n} - I\right) H^{\otimes n}$$

https://rumschuettel.bitbucket.io/grover/index.html

Quantum Computing – Factorization


Peter Shor (1959 -)

- Integer Factorization used in the RSA cryptography system

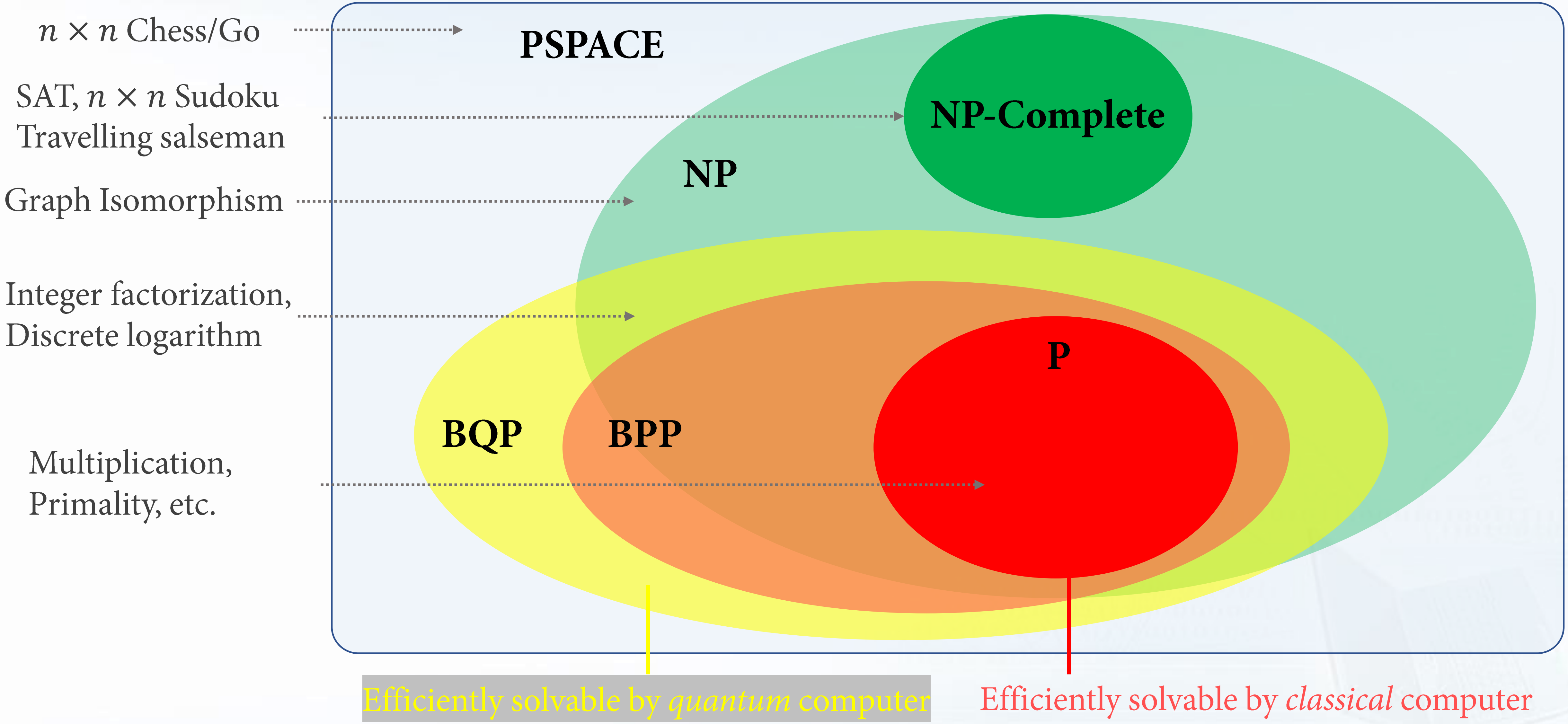
  Example: $\underbrace{463570199875051}_{\approx 2^{49}} = 27644437 \times 16769023$

  The computational complexity of the best known classical algorithm scales *exponentially* in the number of bits of the integer.

  → Peter Shor (1994) invented a *polynomial-time* quantum algorithm

- Other cryptosystem such as the *Diffie–Hellman key exchange security* (based on the hardness of the *discrete logarithm problem*) and the *Elliptic curve cryptography* can be broke in polytime by applying Shor's idea.

Relations – A Glimpse of The Complexity Zoo

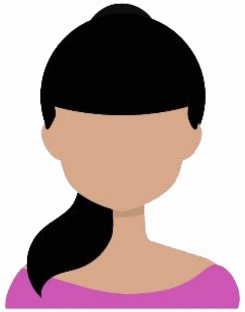


Quantum Advantages – Cryptography & Communication

Secure Communication

- In 1926 Vernam proposed the first provably secure cryptographic protocol, known as the *one-time pad* , or *Vernam cipher.*
- The key is represented by a *random string* of bits, which is used to lock and unlock the confidential message.
- The message itself is another string of bits. *Binary addition* is used for ciphering.

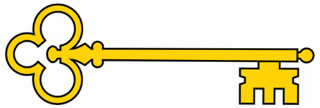
$$0\oplus0=1\oplus1=0;\ \ 0\oplus1=1\oplus0=1$$



Ciphertext: $b\oplus k=11101010$

Source text: $b=01101100$

Deciphered text: $b\oplus k\oplus k=01101100$



Key: $k=10000110$

Key: $k=10000110$

Key Distribution

- The one-time pad protocol is *secure* only if the key distribution is secure and hidden from others, but how to do it in a *secure* way?
- Some public key crypto systems (such as RSA) relies on the computational hardness of the integer factorization.
- *Quantum key distribution* (QKD) provides a method for Alice and Bob to generate a shared secret key over public classical and quantum channels without the need to meet or to use a trusted intermediary party.
  Moreover, it is *provably secure* against eavesdropping.
  - BB84 (C. Bennett and G. Brassard 1984) uses four qubit non-orthogonal states;
  - B92 (C. Bennett 1992) uses only two non-orthogonal qubit states;
  - E91 (A. Ekert 1991) uses an entangled pair of qubits and the Bell theorem.
  - Etc. [Gisin et al., 2002] & [Pirandola, 2020]

Mutually Unbiased Bases

- *Mutually unbiased bases* (MUB): $\mathcal{B}_0 = \{|\psi_{00}\rangle, |\psi_{10}\rangle\}$ and $\mathcal{B}_1 = \{|\psi_{01}\rangle, |\psi_{11}\rangle\}$.

$$|\psi_{00}\rangle = |0\rangle$$
$$|\psi_{10}\rangle = |1\rangle$$
$$|\psi_{01}\rangle = |+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$$
$$|\psi_{11}\rangle = |-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

- $\mathcal{B}_0 = \{|\psi_{00}\rangle, |\psi_{10}\rangle\}$ is the computational basis (or the Pauli Z eigenbasis);
  $\mathcal{B}_1 = \{|\psi_{01}\rangle, |\psi_{11}\rangle\}$ is the conjugate basis (or the Pauli X eigenbasis).

- These bases are called mutually unbiased if any state of one basis is measured in the other basis, the outcomes are always *equally likely*.

An Example

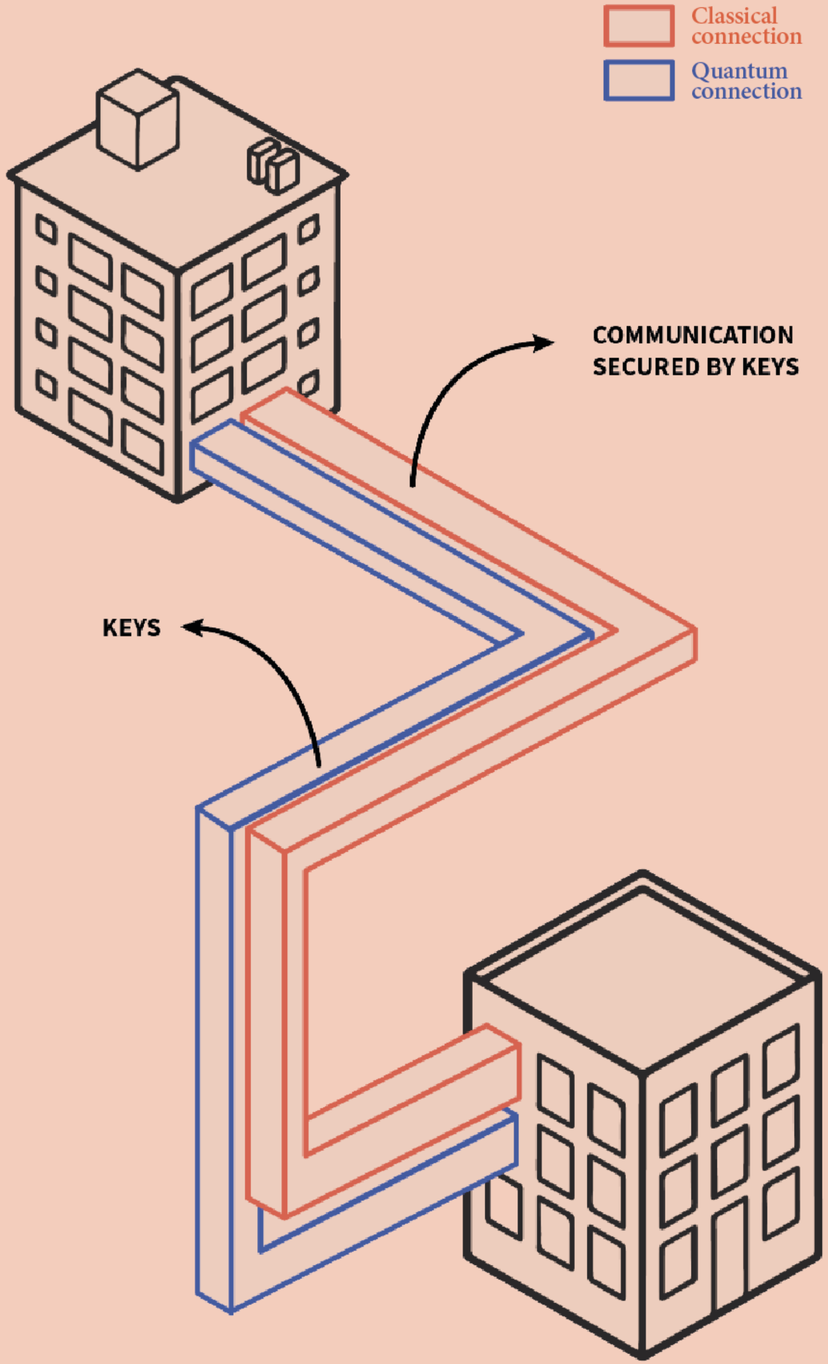
Alice's bit string x	1	0	1	1	0	1	0	1
Alice's basis string y	1	0	0	1	0	1	1	0
	X	Z	Z	X	Z	X	X	Z
Qubit states	$\|-\rangle$	$\|0\rangle$	$\|1\rangle$	$\|-\rangle$	$\|0\rangle$	$\|-\rangle$	$\|+\rangle$	$\|1\rangle$
Bob's basis string y'	1	1	0	0	1	0	1	0
	X	X	Z	Z	X	Z	X	Z
Bob's resulting states	$\|-\rangle$	$\|+\rangle$	$\|1\rangle$	$\|1\rangle$	$\|-\rangle$	$\|0\rangle$	$\|+\rangle$	$\|1\rangle$
Bob's resulting bits x'	1	0	1	1	1	0	0	1
Right basis?	Y	N	Y	N	N	N	Y	Y
Key string $\tilde{x} = \widetilde{x'}$	1		1				0	1

Long Distance QKD System

The Long Distance QKD System operates with a quantum channel in the telecom C-band for the longest possible range and highest possible secure key rate. It can tolerate limited bandwidths of multiplexed data within the C-band.

Key Features:

1. Typical key rate = 300 kb/s for 10dB loss
2. Range of up to 120km
3. Two fibers required
4. Efficient BB84 protocol with decoy states and phase encoding
5. Key failure probability of less than 10^{-10} equivalent to less than once in 30,000 years
6. Proprietary self-differencing semiconductor detectors



Quantum Communication

- Teleportation (Bennett *et al.* 1993)

nature photonics

Explore our content ⌄ Journal information ⌄

nature > nature photonics > review articles > article

Published: March 2007

Quantum communication

Nicolas Gisin & Rob Thew

Nature Photonics **1**, 165–171(2007) | Cite this article

nature photonics

Explore our content ⌄ Journal information ⌄

nature > nature photonics > review articles > article

Published: 25 April 2014

Quantum information transfer using photons

T. E. Northup & R. Blatt

Nature Photonics **8**, 356–363(2014) | Cite this article

Quantum Communication

- Teleportation (Bennett *et al.* 1993)

nature photonics

Explore our content ⌄ Journal information ⌄

nature › nature photonics › review articles › article

Published: March 2007

Quantum communication

Nicolas Gisin & Rob Thew

Nature Photonics **1**, 165–171(2007) | Cite this article

nature photonics

Explore our content ⌄ Journal information ⌄

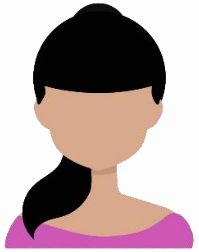
nature › nature photonics › review articles › article

Published: 25 April 2014

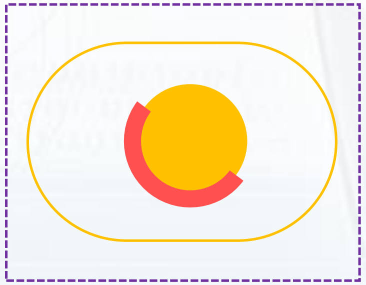
Quantum information transfer using photons

T. E. Northup & R. Blatt

Nature Photonics **8**, 356–363(2014) | Cite this article



$b_0 b_1$



Local operation

Quantum Communication

- Teleportation (Bennett *et al.* 1993)

nature photonics

Explore our content ⌄ Journal information ⌄

nature > nature photonics > review articles > article

Published: March 2007

Quantum communication

Nicolas Gisin & Rob Thew

Nature Photonics **1**, 165–171(2007) | Cite this article

nature photonics

Explore our content ⌄ Journal information ⌄

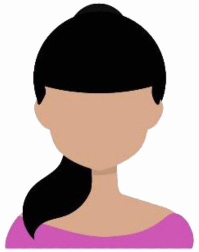
nature > nature photonics > review articles > article

Published: 25 April 2014

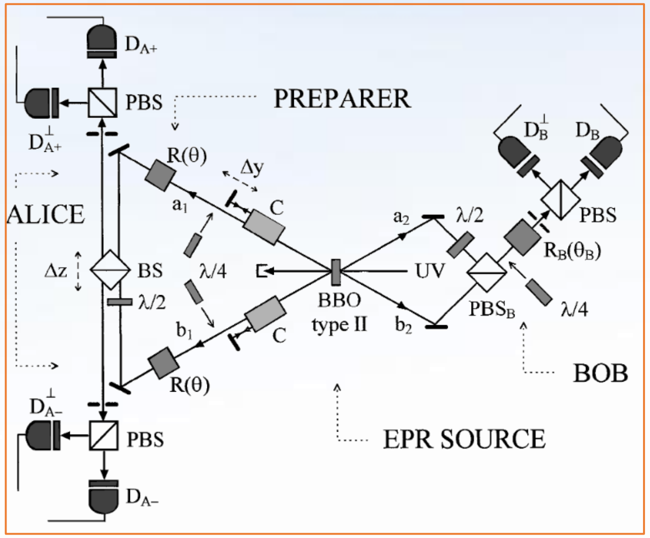
Quantum information transfer using photons

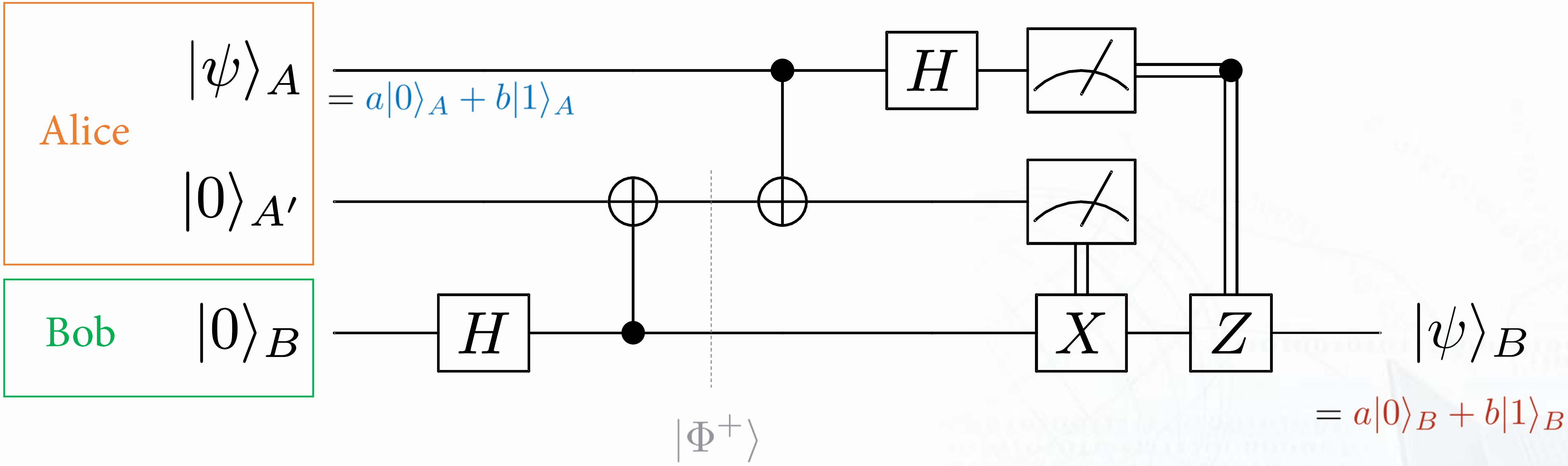
T. E. Northup & R. Blatt

Nature Photonics **8**, 356–363(2014) | Cite this article



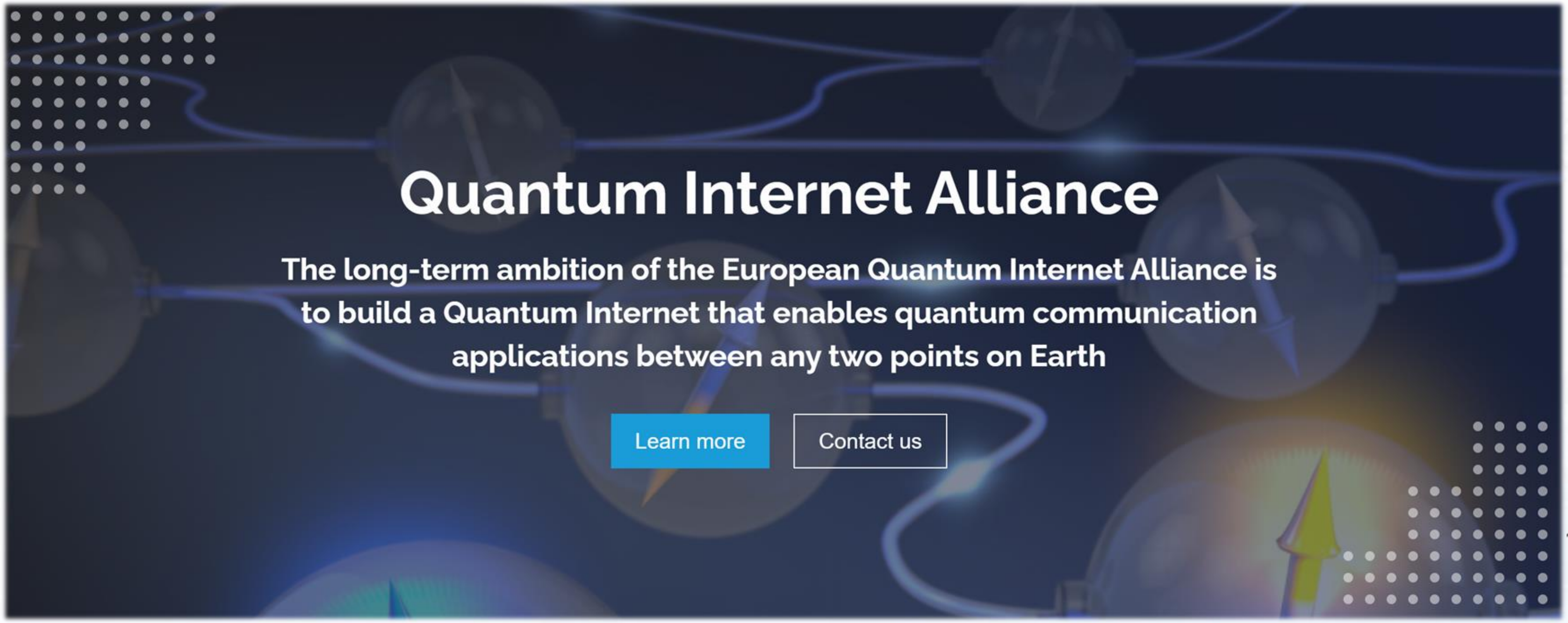
Protocol of Quantum Teleportation

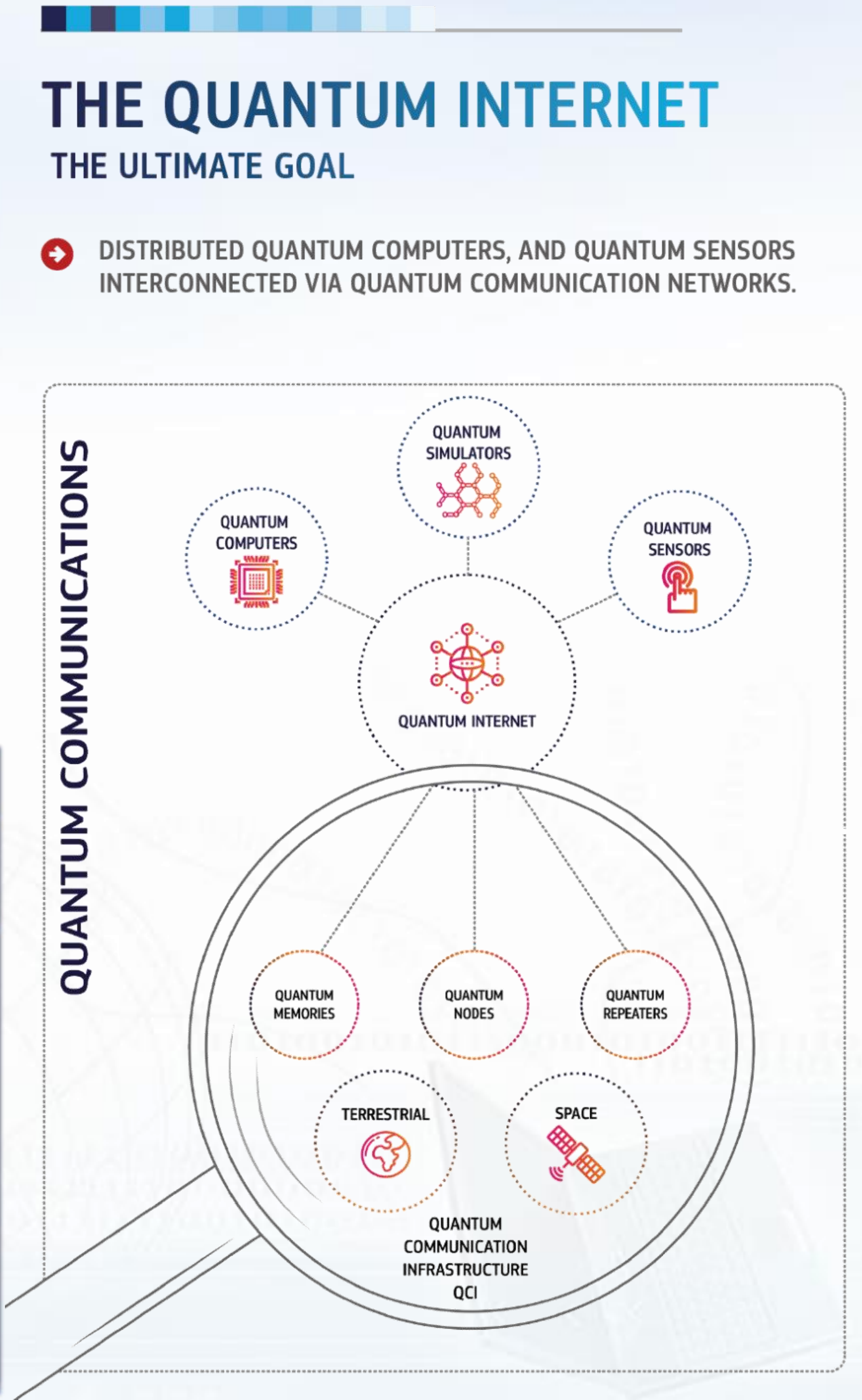




Why Quantum Communication?

- Communicating quantum bits
- Quantum key distribution (cryptography)
- Simulating global quantum computation
- Secure remote quantum computation





Science Contents News Careers Journals

SHARE

REVIEW

Quantum internet: A vision for the road ahead

Stephanie Wehner[1,*], David Elkouss[1], Ronald Hanson[1,2]
+ See all authors and affiliations

Science 19 Oct 2018:
Vol. 362, Issue 6412, eaam9288
DOI: 10.1126/science.aam9288

QUTech

Surf Internet

qpnt. TIME PROVISIONING

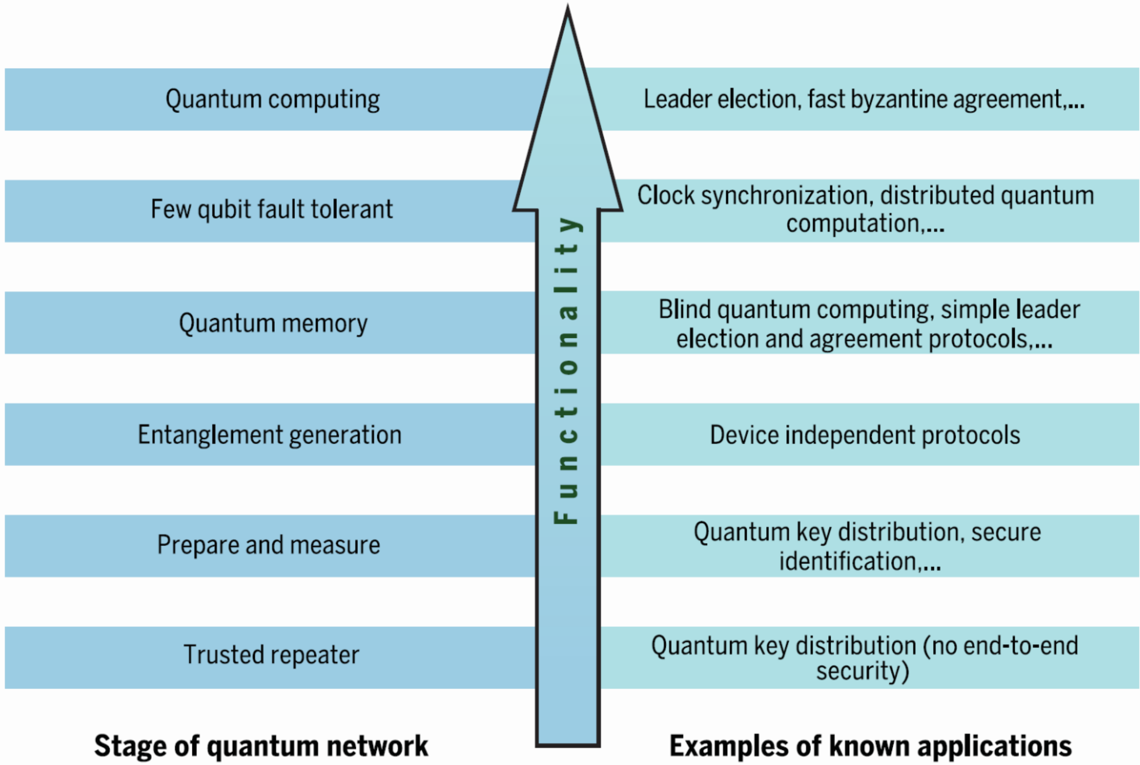
kpn

TUDelft Delft University of Technology

universität innsbruck

IQI

MPQ



Stages in the development of a quantum internet. Each stage is characterized by an increase in functionality at the expense of greater technological difficulty. This Review provides a clear definition of each stage, including benchmarks and examples of known applications, and provides an overview of the technological progress required to attain these stages.

Quantum Simulation

- Simulating natural reaction
  - Nitrogen fixation for fertilizers
  - Nuclear vibration
  - Condensed matter physics
  - Many-body dynamics
  - Material design
- Constrained optimization
  - Satisfiability problems
  - Semidefinite program

nature

Explore our content ⌄ Journal information ⌄

nature > letters > article

Published: 14 September 2017

Hardware-efficient variational quantum eigensolver for small molecules and quantum magnets

Abhinav Kandala, Antonio Mezzacapo, Kristan Temme, Maika Takita, Markus Brink, Jerry M. Chow & Jay M. Gambetta

Nature **549**, 242–246(2017) | Cite this article

Science Contents ▾ News ▾ Careers ▾ Journals ▾

SHARE

RESEARCH ARTICLE

Hartree-Fock on a superconducting qubit quantum computer

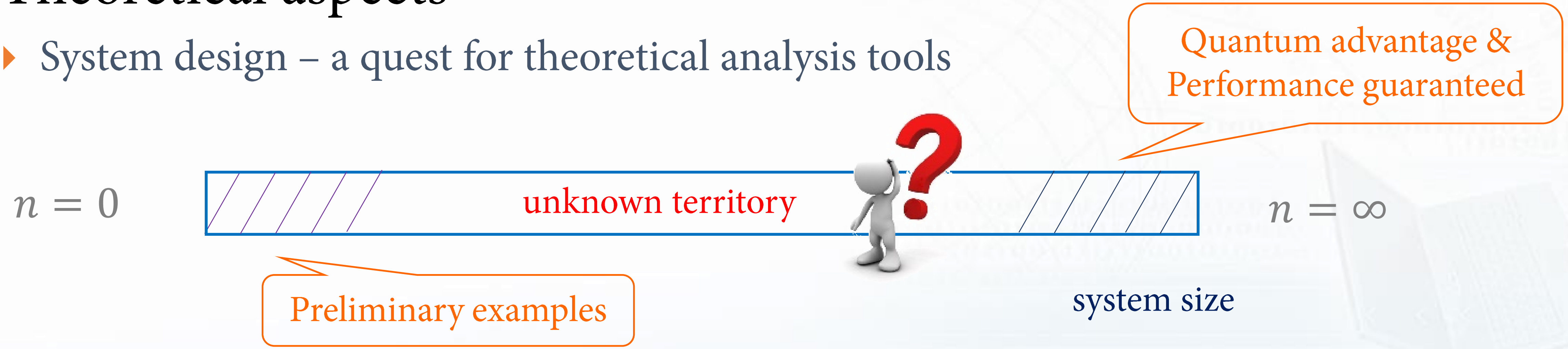
Google AI Quantum and Collaborators*,†, Frank Arute, Kunal Arya, Ryan Babbush, Dave Bacon, Joseph C. Bardin, Rami Bare...
+ See all authors and affiliations

Science 28 Aug 2020:
Vol. 369, Issue 6507, pp. 1084-1089
DOI: 10.1126/science.abb9811

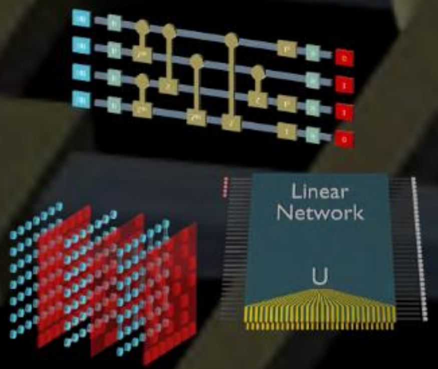
Prospects and Outlooks

Challenges

- Experimental aspects
  - Realizing large-scale universal and programmable quantum processors
- Interface
  - Interconnects – transfer of information between different physical media
  - Efficiently loading classical data into quantum memories and read-out
- Theoretical aspects
  - System design – a quest for theoretical analysis tools

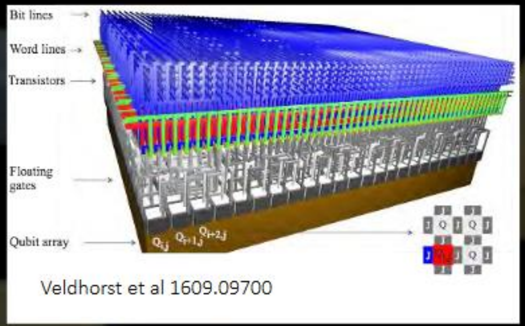


A potential quantum (near) future



Intermediate quantum computing regime:

- Error mitigation
- Testable advantage
- Approximate optimizers
- Quantum simulators



50 qubits — 1,000 — 10,000 — 100,000...

- 50 qubits: 99.7% fidelity; FT qubit; Classical/quantum frontier; <12 months (Google, IBM)
- 1,000 – 10,000: Unambiguous quantum computational supremacy and commercially relevant applications , 2 – 10 years; 99.99% fidelity
- 99.999% fidelity; 10+ years
- 100,000...: Universal quantum computing...

Figure credit by Michael Bremner

How to Join the Community?

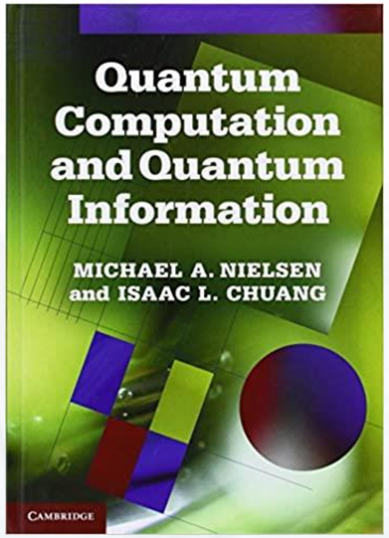
- News
  - https://quantumcomputingreport.com/
  - https://thequantumdaily.com/

Quantum Computing Report
Where Qubits Entangle with Commerce

THE QUANTUM DAILY
QUANTUM COMPUTING AND BEYOND

- ArXiv: https://arxiv.org/list/quant-ph/
- Conference: The Annual Conference on Quantum Information Processing (QIP)
- Final words:
  Quantum information science is not going to change our world immediately, but lots of entrepreneurs, governments, and researchers have dived in.
- What to do?
  Catch up with the state-of-the-art development and watch out hype!

Textbooks



Hao-Chung Cheng (鄭皓中)
haochung@ntu.edu.tw

Thank you