量子信息导论
PHYS5251P

中国科学技术大学
物理学院/合肥微尺度物质科学国家研究中心

陈凯

2024.2

联系方式

- 主讲教师1：陈凯，
  E-mail: kaichen@ustc.edu.cn
  Tel. 63607083；Office: 物质B楼1013-1室
  主页: http://staff.ustc.edu.cn/~kaichen
  https://faculty.ustc.edu.cn/chenkai/
- 主讲教师2：徐飞虎教授 feihuxu@ustc.edu.cn
- 助教 魏君豪, weijunhao@mail.ustc.edu.cn
  杨挪亚, nyyang@mail.ustc.edu.cn

参考书目

教材

- Quantum computation and quantum information by M.A. Nielsen and I.L. Chuang, Cambridge University Press, 2010

其他参考书

- 量子信息

马雄峰、张行健、黄溢智，《量子信息简明教程》，清华大学出版社，2023.

- 量子力学

王向斌、沈艺鑫、于云龙、秦季茜、徐海，《量子力学基础教程》，清华大学出版社，2023.

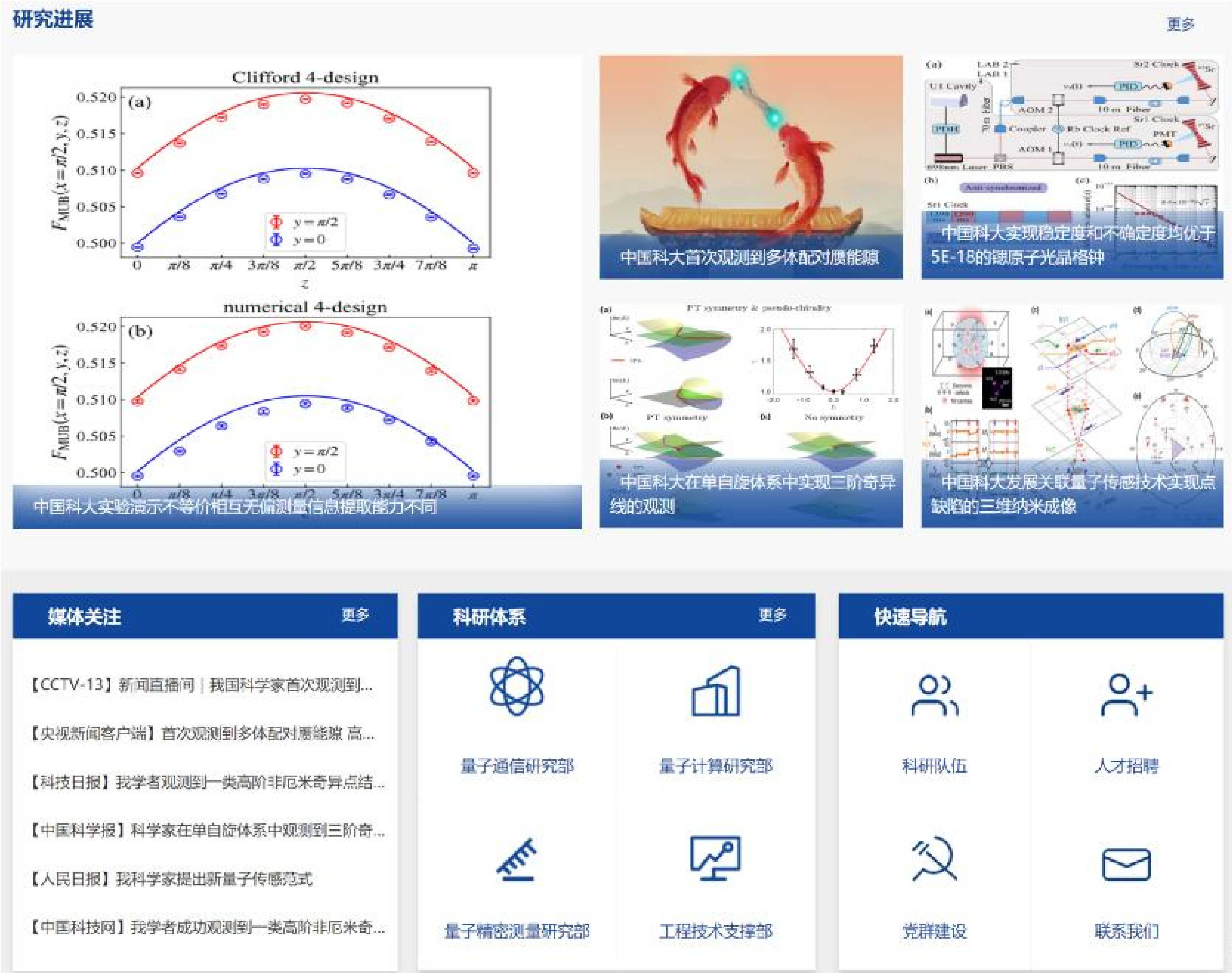
Course Description

This course is open to all graduate students and undergraduates. The final grades are based on:

- final exam (60%),
- homework and attendance of the class (20%),
- a report about quantum information (20%, the subject can be arbitrary, which is preferably related to your current research project, recent progress or your own ideas along one specific area on theoretical or experimental quantum information)

Visit http://www.quantumcas.ac.cn/

Visit http://www.quantumcas.ac.cn/

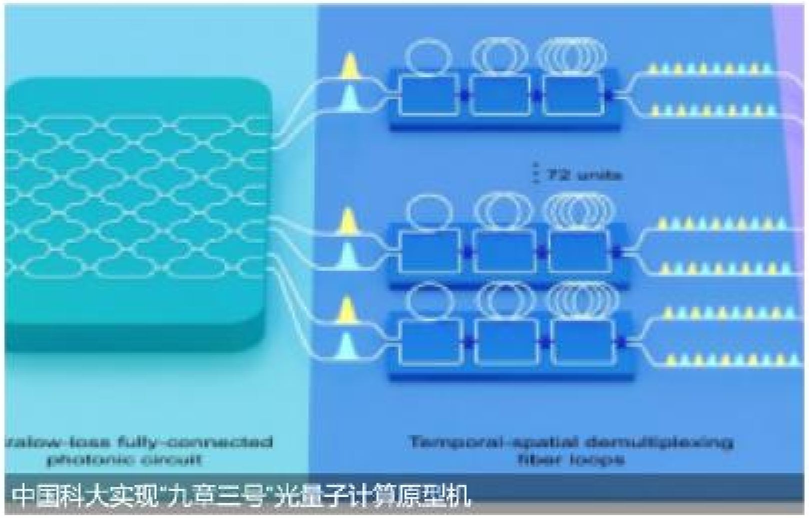


Visit us at http://quantum.ustc.edu.cn

量子物理与量子信息研究部

Explore quantum mystery, enable quantum applications!

首页 | 研究方向 | 量子卫星 | 团队成员 | 新闻动态 | 研究进展 | 学术报告 | 论文发表 | 公告通知 | 招生信息 | 相关链接



关于我们

量子物理与量子信息研究部成立于2001年，研究部主任为潘建伟院士。研究领域为量子光学与量子信息，研究方向包括量子力学基本原理检验、光纤量子通信、自由空间量子通信、量子存储与量子中继、光学量子计算、超导量子计算、超冷原子量子模拟、量子精密测量以及相关理论研究等。我们已经搭建了众多相关实验平台，建立和发展了一整套与量子信息实验研究相关的分析探测设备和手段，研究条件具有国际先进水平。

阅读更多

新闻动态

2023-12-27 徐飞虎教授获2023年度中国科学院青年科学家奖
2023-12-20 陆朝阳教授获2023年何梁何利基金科学与技术创新奖
2023-03-18 我校成果入选2022年度中国科学十大进展
2022-12-20 中国科大实数量子力学检验实验入选2022年国际物理学十大进展
2022-12-16 中国科大成果入选2022年度国际物理学十大突破
2022-07-27 世界首颗量子微纳卫星成功发射
2022-03-01 我校成果入选2021年度中国科学十大进展

研究进展

2023-10-11 中国科大实现"九章三号"光量子计算原型机
2023-07-12 中国科大成功实现最大规模的51比特量子纠缠态制备
2023-06-07 九章光量子计算原型机求解图论问题
2023-05-26 我国科学家实现千公里无中继光纤量子密钥分发
2023-03-14 中国科大实现百兆比特率量子密钥分发
2023-02-04 中国科大实现模式匹配量子密钥分发
2022-12-02 中国科大首次制备高相空间密度的超冷三原子分子系综

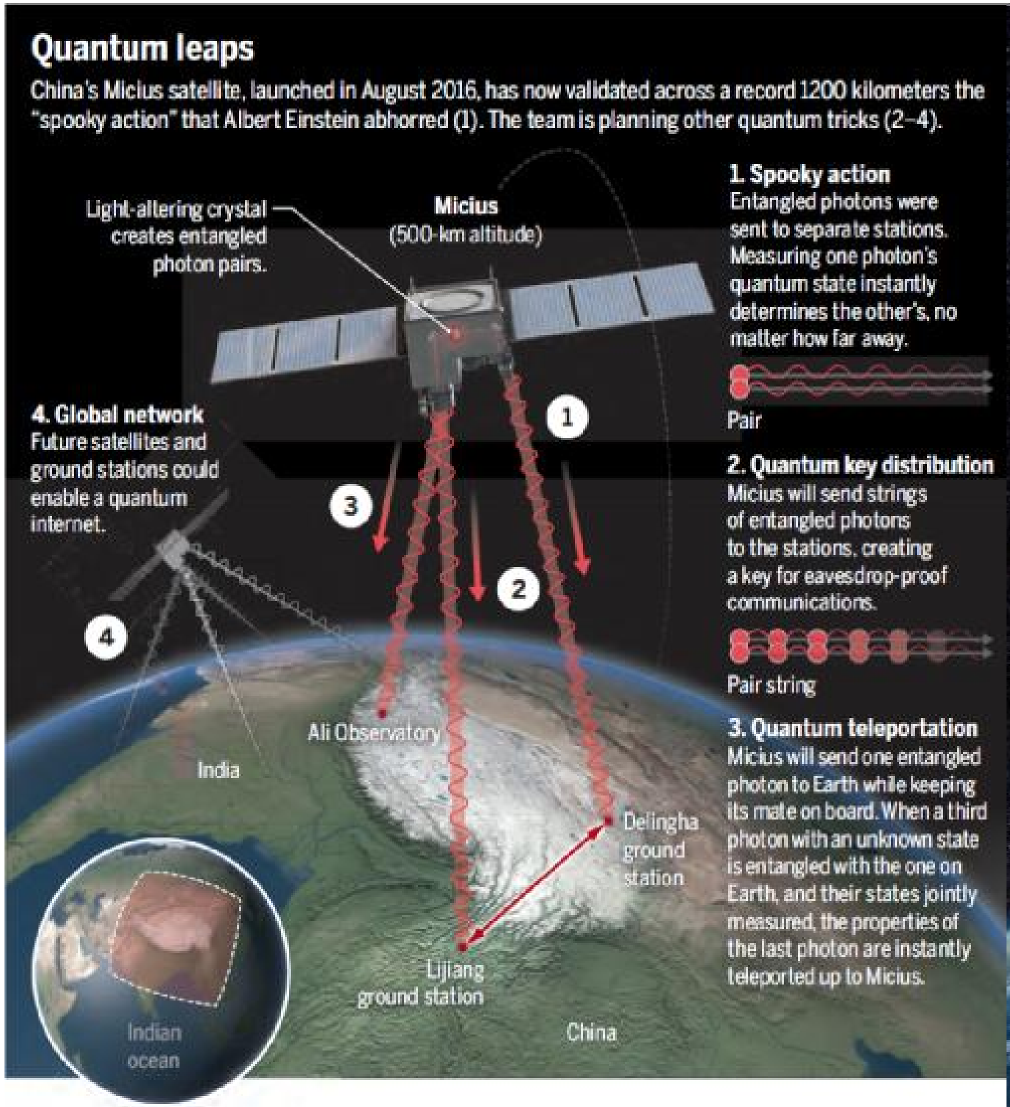
学术报告

2024-01-11 高速铌酸锂薄膜光电子芯片
2024-01-05 Verifiable IQP Supremacy: Constructions, Attacks, and Implementations
2023-12-22 从地球的深处仰望宇宙
2023-12-15 Quantum information processing with color centers in hexagonal boron ni...
2023-11-30 Microwave-shielded polar molecules: from ultracold chemistry to quantum...
2023-11-23 一沙一世界：从宇宙到原子的量子隧穿
2023-11-10 氦物理基础研究和极低温技术研发

量子卫星成功发射

2016年8月16日1时40分，我国在酒泉卫星发射中心用长征二号丁运载火箭成功将世界首颗量子科学实验卫星发射升空。

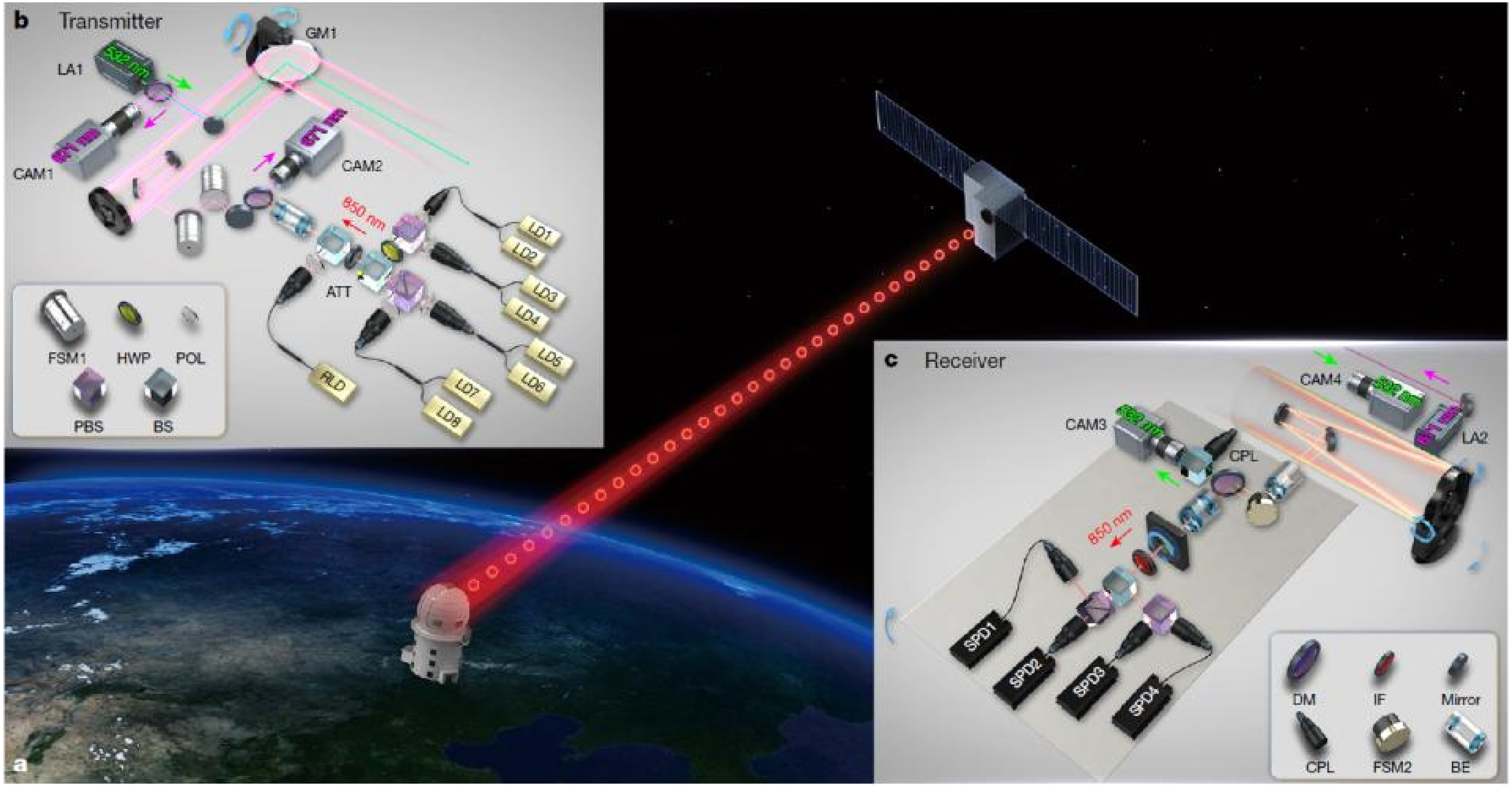
Satellite-based entanglement distribution over 1200 kilometers



J. Yin *et al.*, **Science** 356 (2017) 1140–114

中国科学技术大学 陈凯

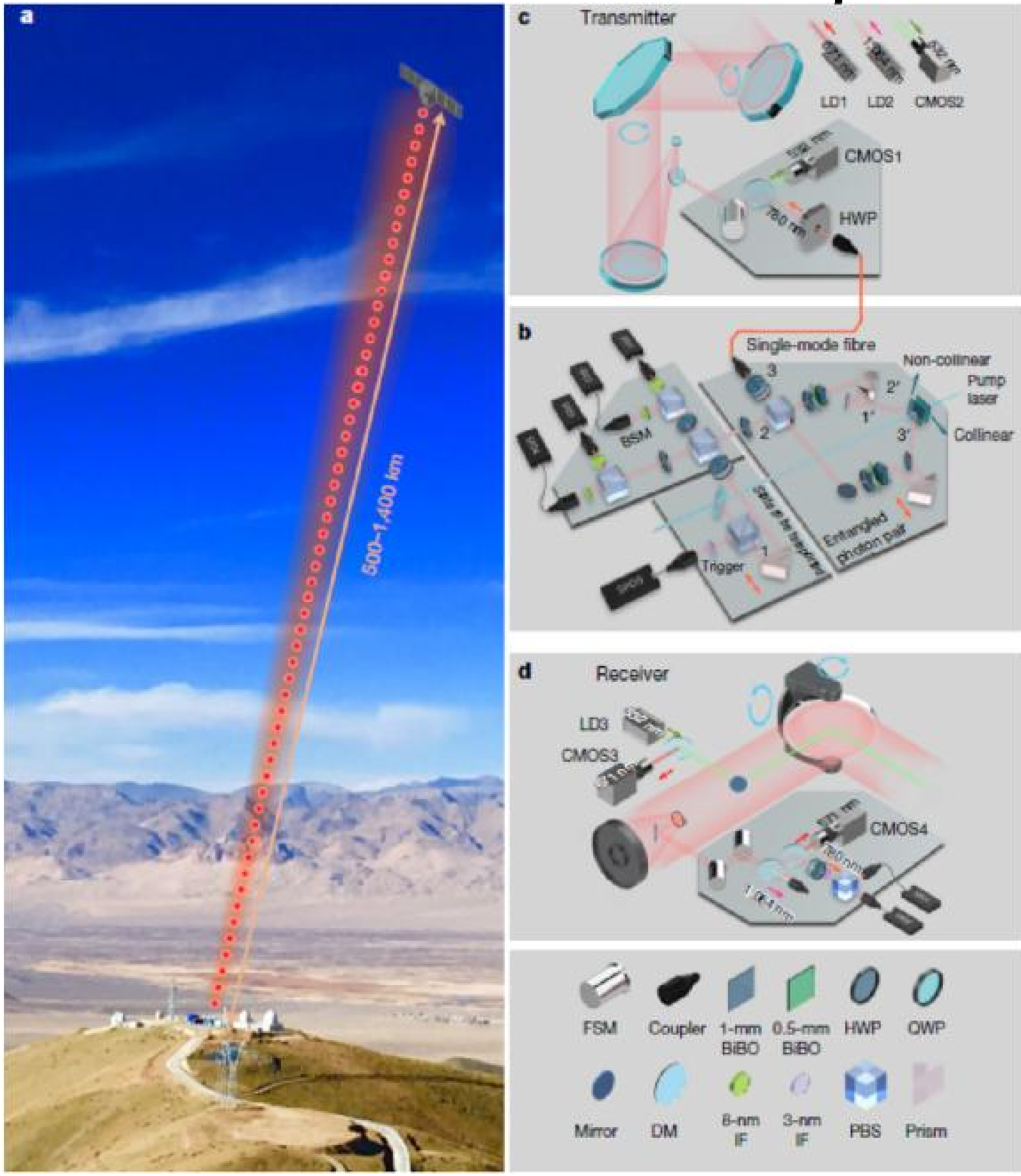
Satellite-to-ground quantum key distribution



Satellite-to-ground quantum key distribution. *Nature*
http://dx.doi.org/10.1038/nature23655

S.-K. Liao *et al.*, **Nature** 549 (2017) 43–47

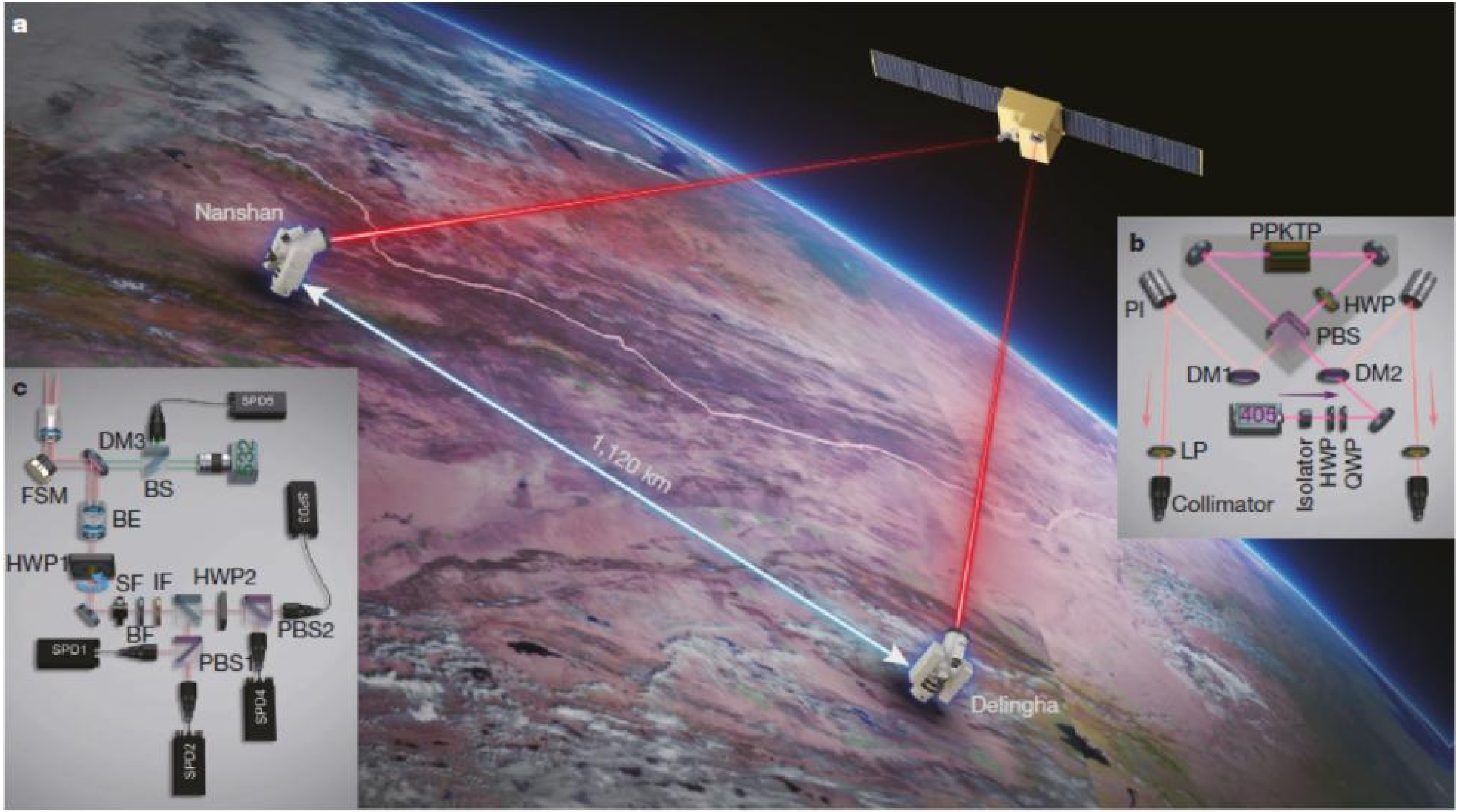
Ground-to-satellite quantum teleportation



Ground-to-satellite quantum teleportation. Nature http://dx.doi.org/10.1038/nature23675 (2017).

J.-G. Ren *et al.*, **Nature** 549 (2017) 70–73

“墨子号”实现基于纠缠的无中继千公里量子保密通信

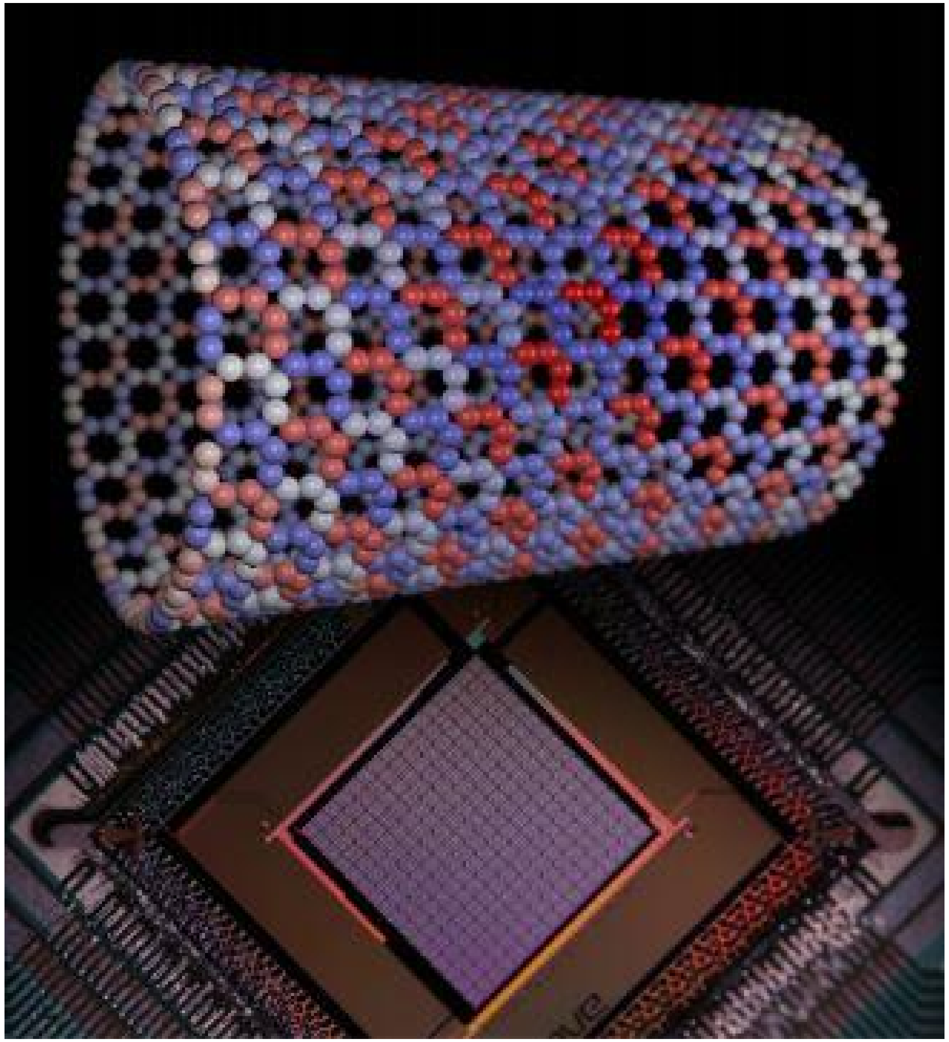


J. Yin *et al.*, **Nature** 582 (2020) 501-505

世界首颗量子微纳卫星成功发射

2022年7月27日，世界首颗量子微纳卫星在酒泉卫星发射中心搭载“力箭一号”运载火箭成功发射。该卫星的科学目标是在世界上首次实现基于微纳卫星和小型化地面站之间的实时星地量子密钥分发，为构建低成本、实用化的天地一体化广域量子保密通信网络奠定基础。

Quantum simulation

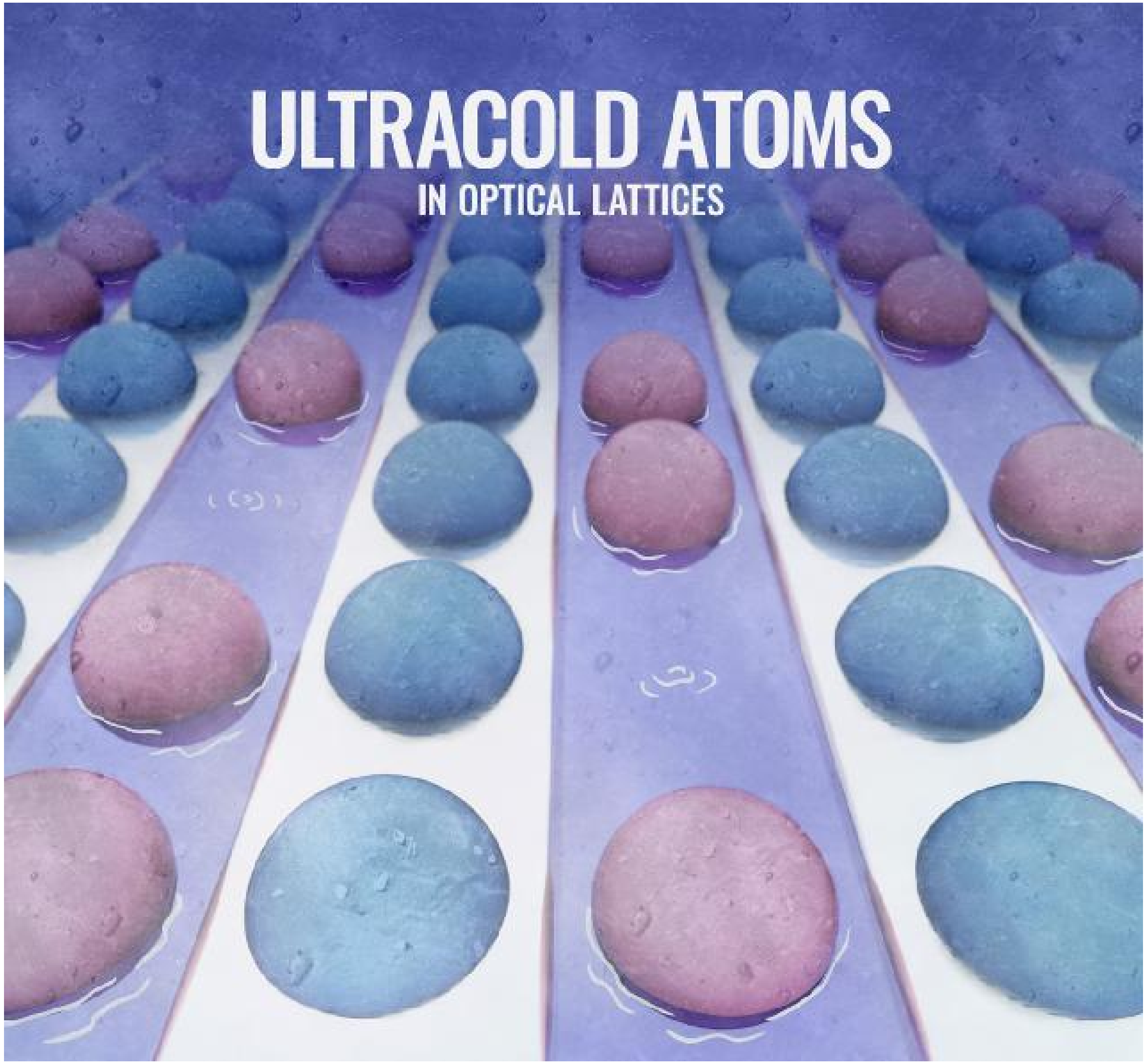


Programmable simulation of quantum magnets

Observation of topological phenomena in a programmable lattice of 1,800 qubits
https://doi.org/10.1038/s41586-018-0410-x

A.D. King *et al.*, **Nature** 560 (2018) 456-460

量子模拟

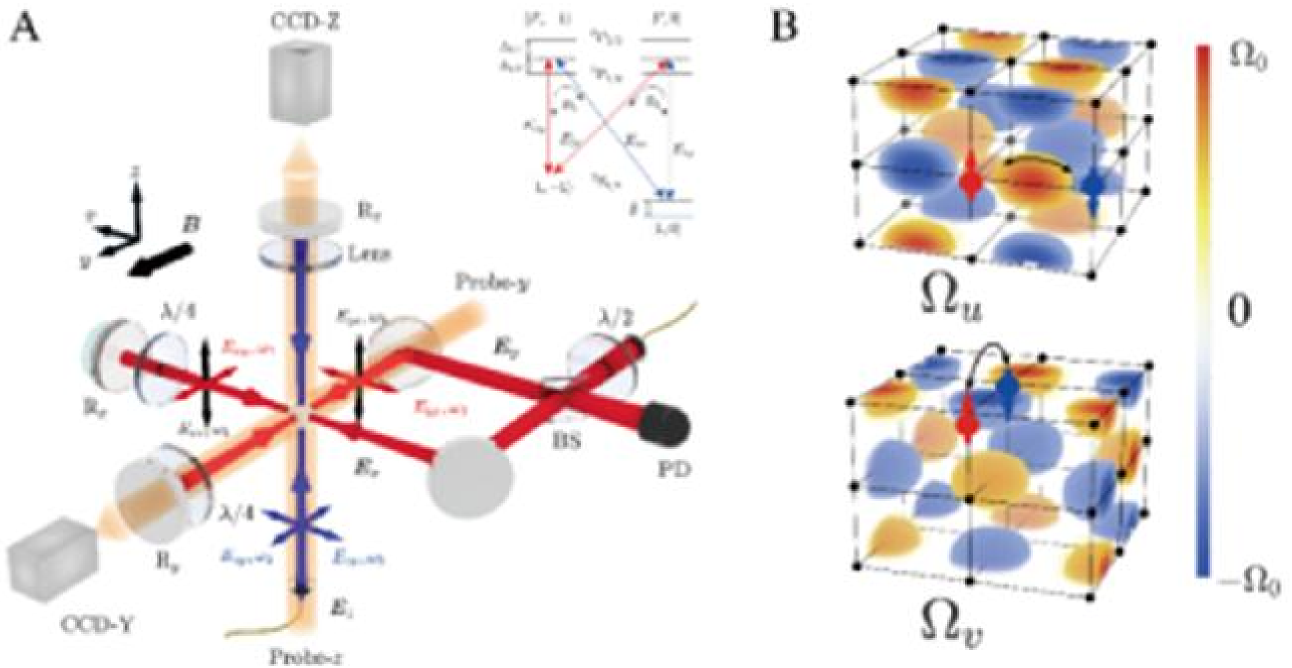


B. Yang *et al.*, **Science** 369 (2021) 550-553

在超冷原子光晶格中实现大规模高保真度量子纠缠对的同步制备

获得了纠缠保真度为99.3%的1250对纠缠原子!

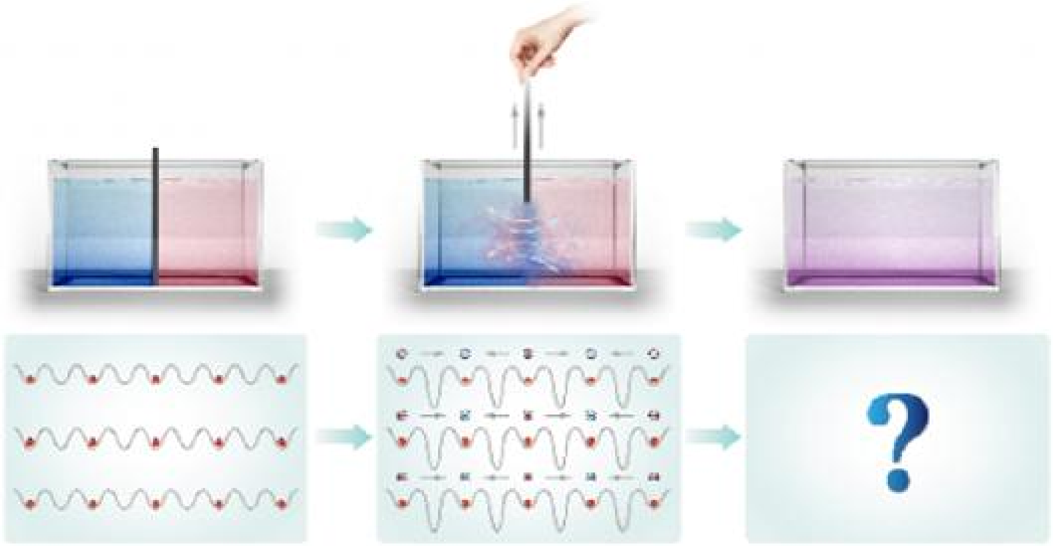
Quantum simulation



研究团队在国际上首次利用超冷原子体系实现了三维自旋轨道耦合，并构造出有且仅有一对外尔点的理想外尔半金属能带结构。

Z.-Y. Wang *et al.*, **Science** 372 (2021) 271-276

量子模拟

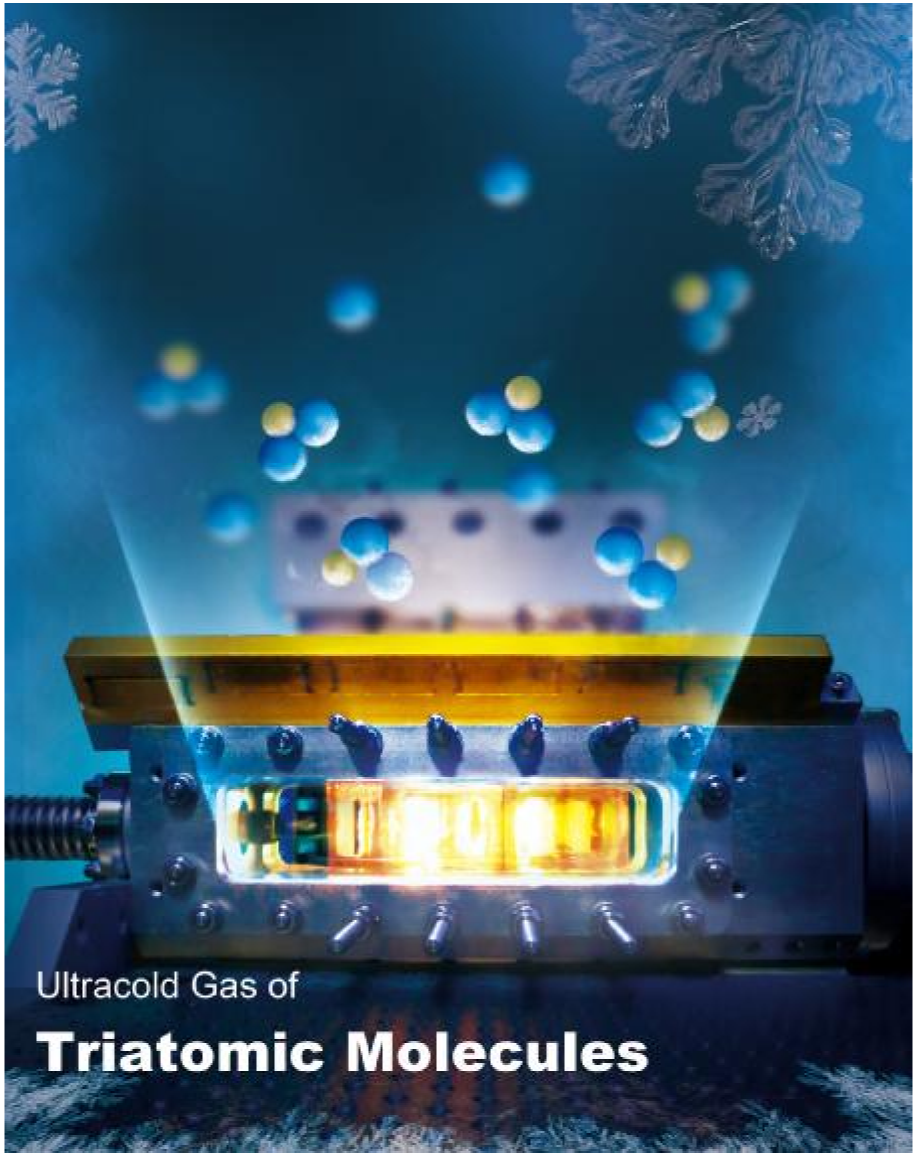


从非平衡态过渡到平衡态的热化动力学示意图。上图：经典图像类比。容器左、右半部分装有温度不同的水，当快速抽离中间隔板时，系统处于非平衡态，经过两个子系统中水分子的交换和碰撞，最终达到热平衡。**下图：**本工作研究的物理问题。束缚在光晶格中的原子被制备到满足特定规范对称性的量子多体初态，通过调控实验参数快速改变原子之间的相互作用，把系统置于一个非平衡态，该强关联量子多体系统能否通过特定的热化机制达到平衡态？（制图：陈磊，周肇宇，梁琰，苑震生）

首次实验研究了规范对称性约束对量子多体系统热化动力学的影响，并且观测到具有相同守恒量的不同初态热化到同一个平衡态的过程，验证了热化过程造成的量子多体系统初态信息的“丢失”，建立了规范场理论早期非平衡动力学与最终热平衡态之间的联系，在使用规模化的量子模拟器求解复杂物理问题的道路上取得了重要进展。

Z.-Y. Zhou *et al.*, **Science** 377 (2022) 311–314

量子模拟

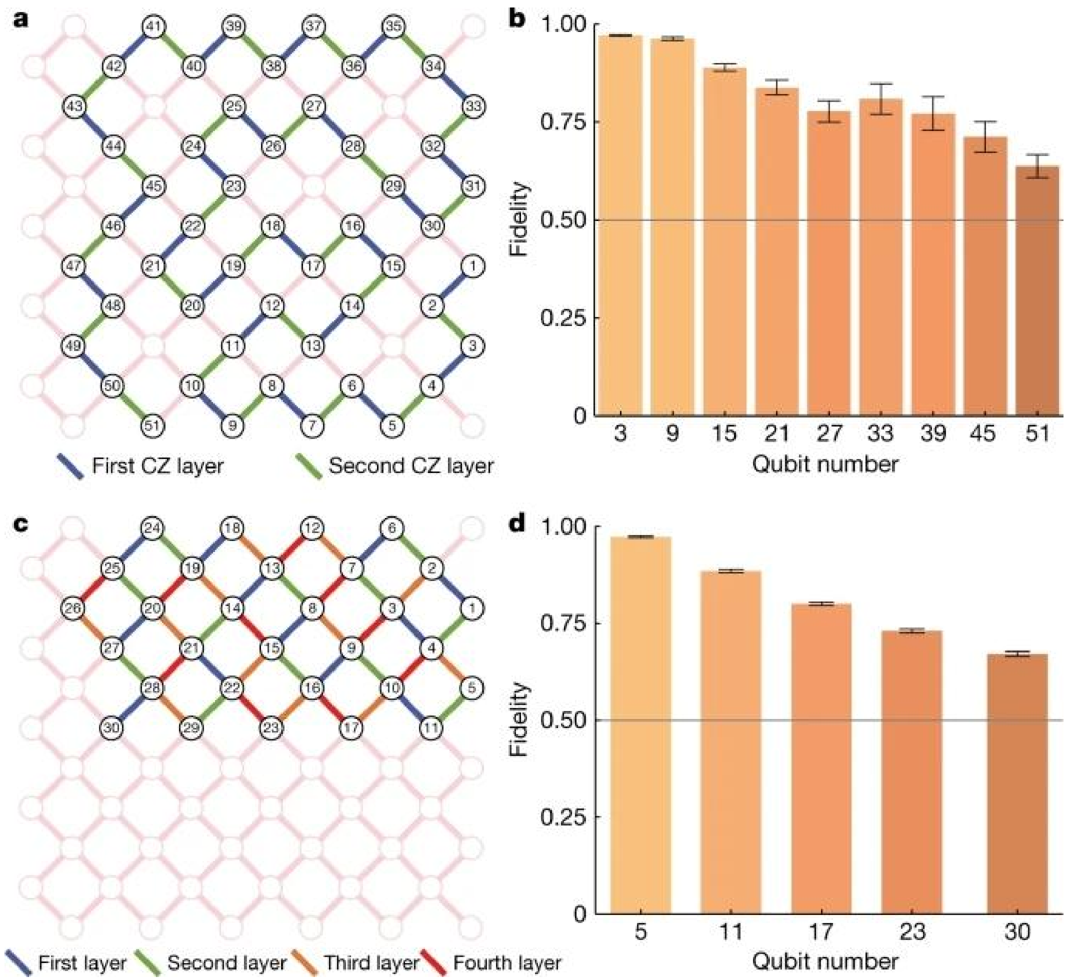


Creation of an ultracold gas of triatomic molecules from an atom–diatomic molecule mixture

利用相干合成方法在国际上首次制备了高相空间密度的超冷三原子分子系综。研究团队基态双原子分子和原Feshbach共振附近利用磁缔合技术从简并的钠钾分子-钾原子混合气中制备了超冷三原子分子系综，向基于超冷分子的超冷量子化学和量子模拟研究迈出了重要一步。

H. Yang, J. Cao, Z. Su, J. Rui, B. Zhao and J.-W. Pan
Science 378 (2022) 1009–1013

量子计算



Generation of genuine entanglement up to 51 superconducting qubits

研究团队成功实现了51个超导量子比特簇态制备和验证，刷新了所有量子系统中真纠缠比特数目的世界纪录，并首次实现了基于测量的变分量子算法的演示。该工作将各个量子系统中真纠缠比特数目的纪录由原先的24个大幅突破至51个，充分展示了超导量子计算体系优异的可扩展性，对于多体量子纠缠研究、大规模量子算法实现以及基于测量的量子计算具有重要意义。

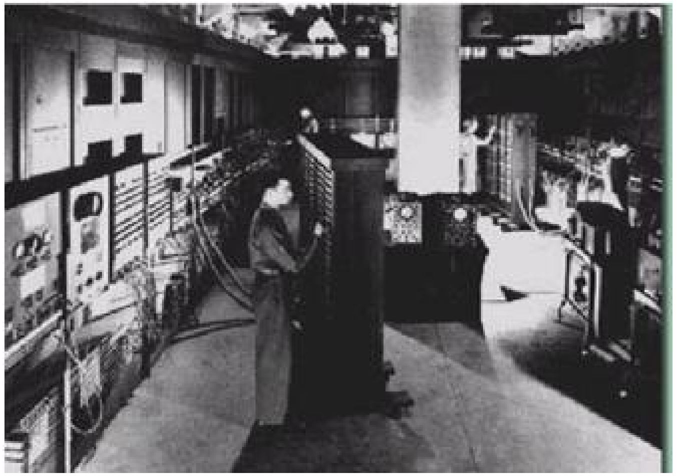
S.-R. Cao *et al.*, **Nature** 619 (2023) 738–742

绪论

量子信息概念、历史和展望

经典计算机和信息处理

冯·诺依曼



第一代计算机

Roadrunner超级计算机

NASA太空高速互联网

联想笔记本

苹果笔记本

阿里云

超级计算机

Frontier（美国）

Summit（美国）

Fugaku(富岳)

Sierra（美国）

Lumi （芬兰）

神威 太湖之光 中国

全球超级计算机500强榜单

超级计算机

TOP10 System - November 2023

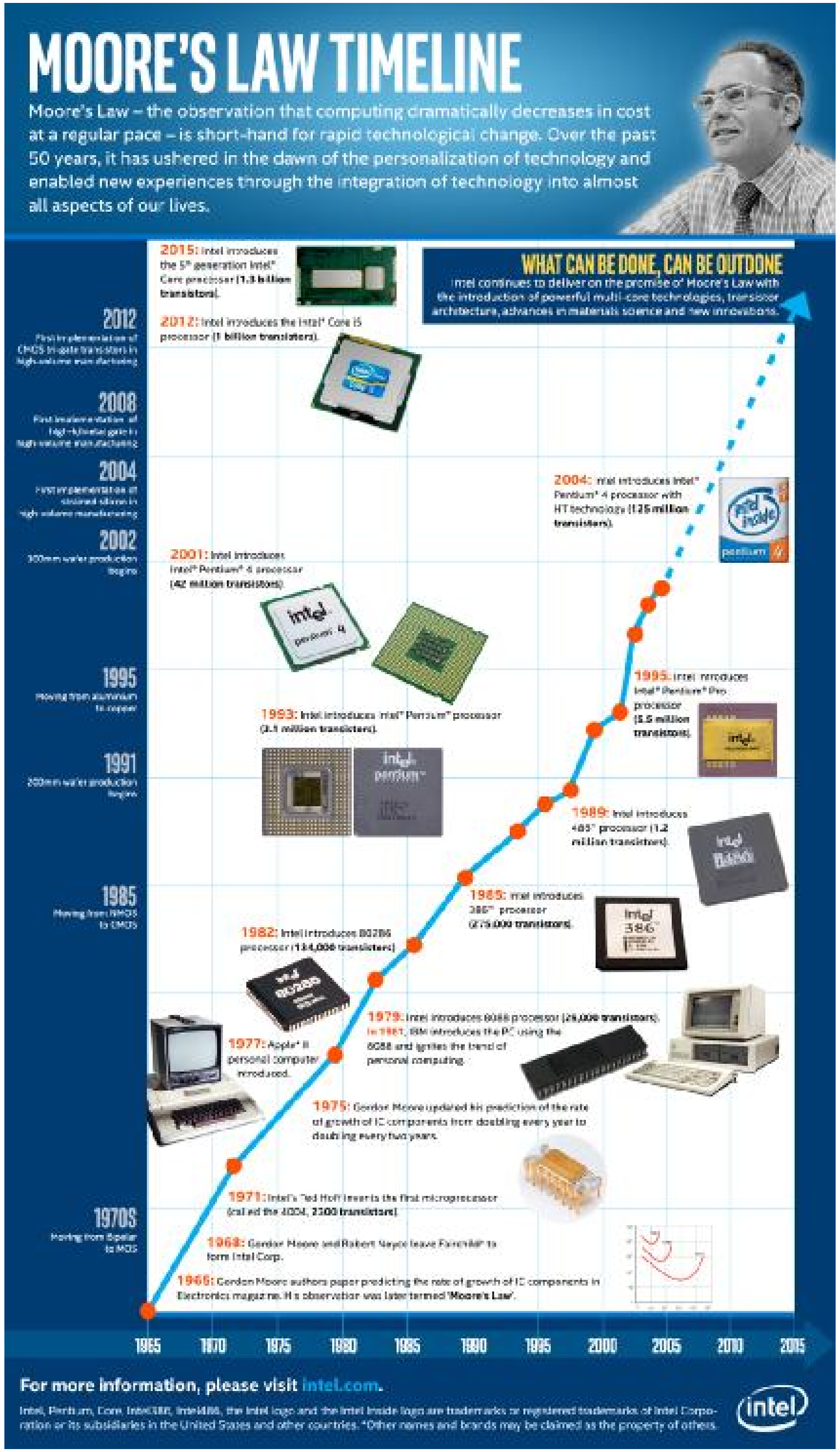
R_{max} and R_{peak} values are in PFlop/s.

For more details about other fields, check the TOP500 description.

R_{peak} values are calculated using the advertised clock rate of the CPU. For the efficiency of the systems you should take into account the Turbo CPU clock rate where it applies.

https://www.top500.org/lists/top500/2023/11/

Rank	System	Cores	Rmax (PFlop/s)	Rpeak (PFlop/s)	Power (kW)
1	**Frontier** - HPE Cray EX235a, AMD Optimized 3rd Generation EPYC 64C 2GHz, AMD Instinct MI250X, Slingshot-11, **HPE** DOE/SC/Oak Ridge National Laboratory United States	8,699,904	1,194.00	1,679.82	22,703
2	**Aurora** - HPE Cray EX - Intel Exascale Compute Blade, Xeon CPU Max 9470 52C 2.4GHz, Intel Data Center GPU Max, Slingshot-11, **Intel** DOE/SC/Argonne National Laboratory United States	4,742,808	585.34	1,059.33	24,687
3	**Eagle** - Microsoft NDv5, Xeon Platinum 8480C 48C 2GHz, NVIDIA H100, NVIDIA Infiniband NDR, **Microsoft** Microsoft Azure United States	1,123,200	561.20	846.84	
4	**Supercomputer Fugaku** - Supercomputer Fugaku, A64FX 48C 2.2GHz, Tofu interconnect D, **Fujitsu** RIKEN Center for Computational Science Japan	7,630,848	442.01	537.21	29,899
5	**LUMI** - HPE Cray EX235a, AMD Optimized 3rd Generation EPYC 64C 2GHz, AMD Instinct MI250X, Slingshot-11, **HPE** EuroHPC/CSC Finland	2,752,704	379.70	531.51	7,107
6	**Leonardo** - BullSequana XH2000, Xeon Platinum 8358 32C 2.6GHz, NVIDIA A100 SXM4 64 GB, Quad-rail NVIDIA HDR100 Infiniband, **EVIDEN** EuroHPC/CINECA Italy	1,824,768	238.70	304.47	7,404
7	**Summit** - IBM Power System AC922, IBM POWER9 22C 3.07GHz, NVIDIA Volta GV100, Dual-rail Mellanox EDR Infiniband, **IBM** DOE/SC/Oak Ridge National Laboratory United States	2,414,592	148.60	200.79	10,096
8	**MareNostrum 5 ACC** - BullSequana XH3000, Xeon Platinum 8460Y+ 40C 2.3GHz, NVIDIA H100 64GB, Infiniband NDR200, **EVIDEN** EuroHPC/BSC Spain	680,960	138.20	265.57	2,560
9	**Eos NVIDIA DGX SuperPOD** - NVIDIA DGX H100, Xeon Platinum 8480C 56C 3.8GHz, NVIDIA H100, Infiniband NDR400, **Nvidia** NVIDIA Corporation United States	485,888	121.40	188.65	
10	**Sierra** - IBM Power System AC922, IBM POWER9 22C 3.1GHz, NVIDIA Volta GV100, Dual-rail Mellanox EDR Infiniband, **IBM / NVIDIA / Mellanox** DOE/NNSA/LLNL United States	1,572,480	94.64	125.71	7,438

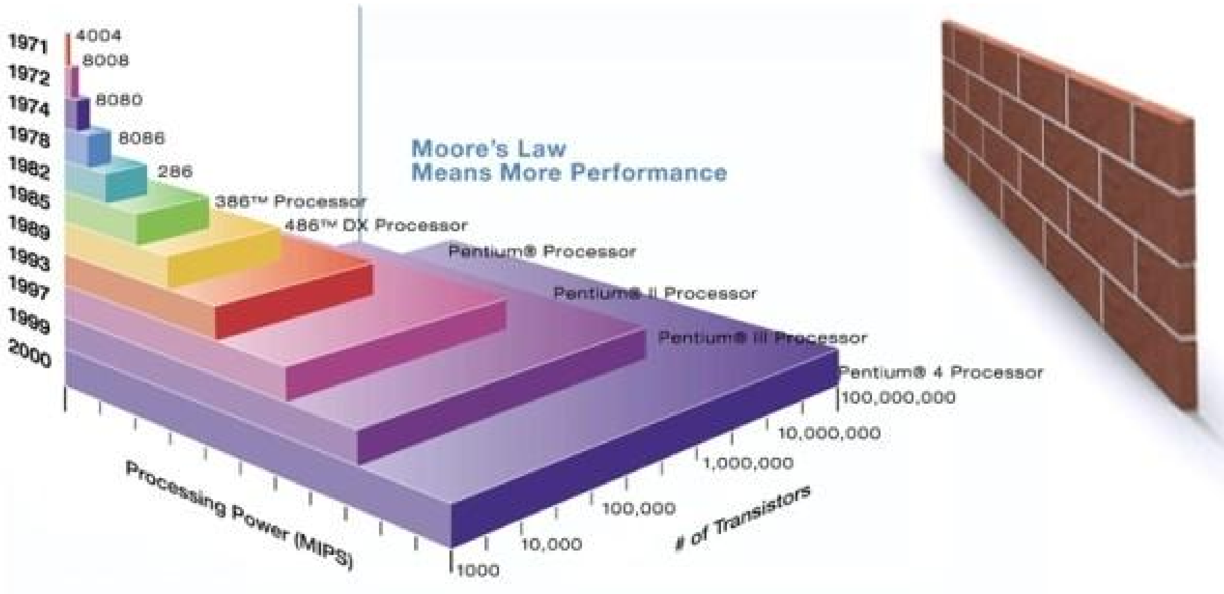


MOORE'S LAW TIMELINE
Moore's Law – the observation that computing dramatically decreases in cost at a regular pace – is short-hand for rapid technological change. Over the past 50 years, it has ushered in the dawn of the personalization of technology and enabled new experiences through the integration of technology into almost all aspects of our lives.
WHAT CAN BE DONE, CAN BE OUTDONE
Intel continues to deliver on the promise of Moore's Law with the introduction of powerful multi-core technologies, transistor architecture, advances in materials science and new innovations.
2015: Intel introduces the 5th generation Intel® Core processor (1.3 billion transistors).
2012: Intel introduces the Intel® Core i5 processor (1 billion transistors).
2012
2008
2004
2002
300mm wafer production begins
2004: Intel introduces Intel® Pentium® 4 processor with HT technology (125 million transistors).
2001: Intel introduces Intel® Pentium® 4 processor (42 million transistors).
1995
Moving from aluminum to copper
1995: Intel introduces Intel® Pentium® Pro processor (5.5 million transistors).
1993: Intel introduces Intel® Pentium® processor (3.1 million transistors).
1991
200mm wafer production begins
1989: Intel introduces 486™ processor (1.2 million transistors).
1985
Moving from NMOS to CMOS
1985: Intel introduces 386™ processor (275,000 transistors).
1982: Intel introduces 80286 processor (134,000 transistors).
1979: Intel introduces 8088 processor (29,000 transistors).
In 1981, IBM introduces the PC using the 8088 and ignites the trend of personal computing.
1977: Apple® II personal computer introduced.
1975: Gordon Moore updated his prediction of the rate of growth of IC components from doubling every year to doubling every two years.
1971: Intel's Ted Hoff invents the first microprocessor (called the 4004, 2300 transistors).
1970S
Moving from Bipolar to MOS
1968: Gordon Moore and Robert Noyce leave Fairchild® to form Intel Corp.
1965: Gordon Moore authors paper predicting the rate of growth of IC components in Electronics magazine. His observation was later termed 'Moore's Law'.
1965
1970
1975
1980
1985
1990
1995
2000
2005
2010
2015
For more information, please visit intel.com.
Intel, Pentium, Core, Intel386, Intel486, the Intel logo and the Intel Inside logo are trademarks or registered trademarks of Intel Corporation or its subsidiaries in the United States and other countries. *Other names and brands may be claimed as the property of others.

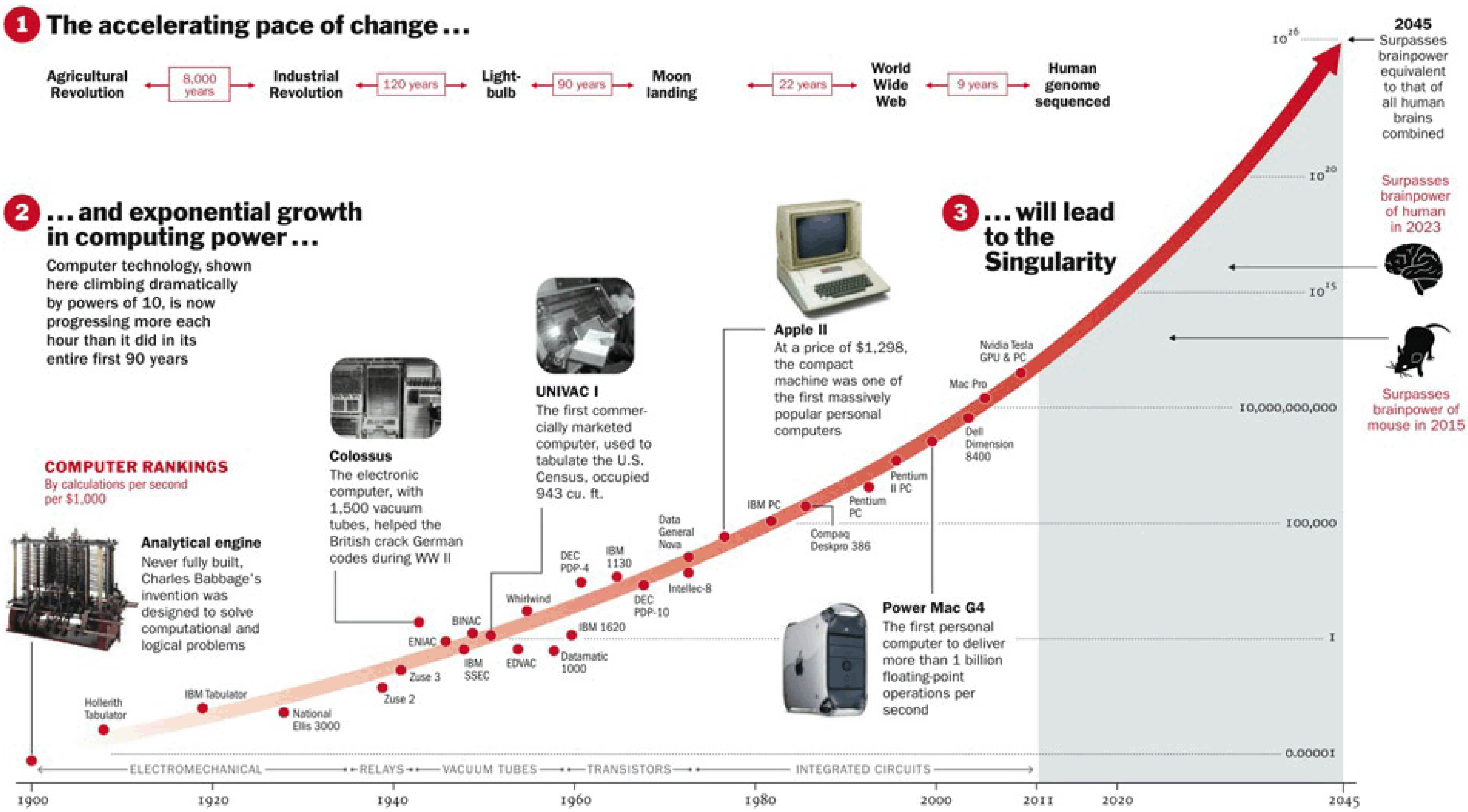
经典计算机和信息处理

"The number of transistors per chip doubles within two years"

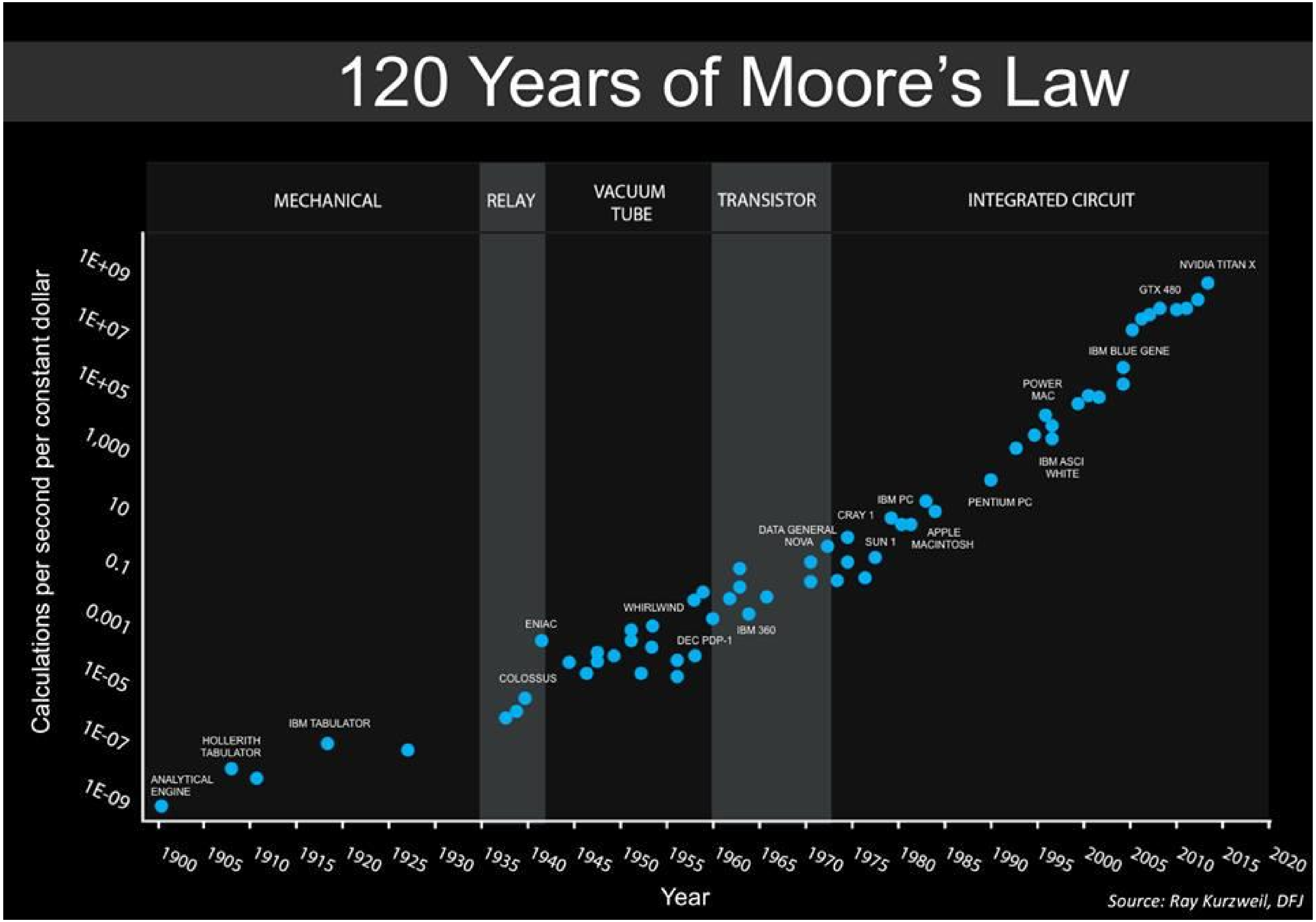
(Apr 19, 1965)



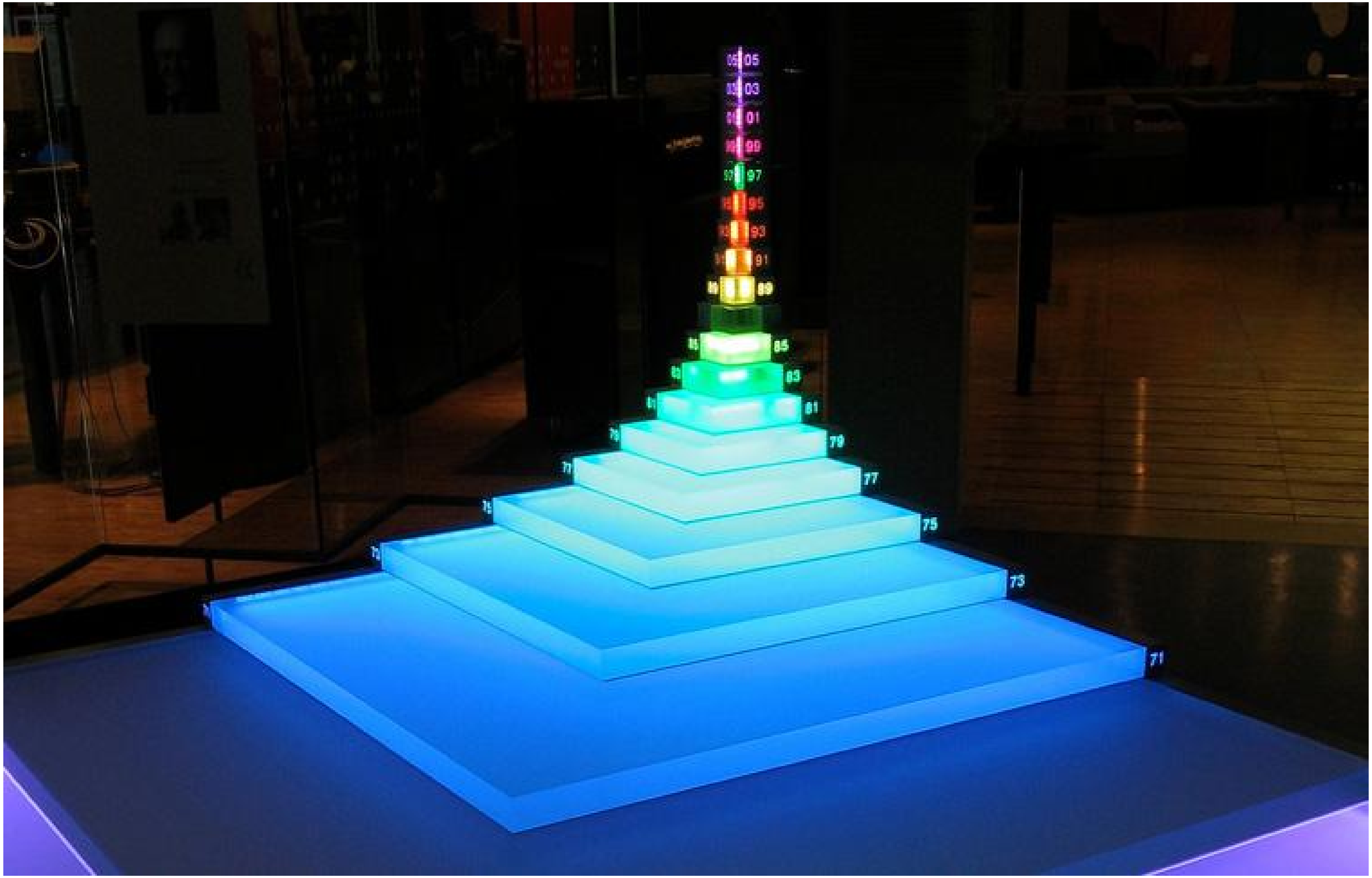
Gordon E. Moore,
Co-founder of Intel


1 The accelerating pace of change …
Agricultural Revolution
8,000 years
Industrial Revolution
120 years
Light-bulb
90 years
Moon landing
22 years
World Wide Web
9 years
Human genome sequenced
2 … and exponential growth in computing power …
Computer technology, shown here climbing dramatically by powers of 10, is now progressing more each hour than it did in its entire first 90 years
3 … will lead to the Singularity
COMPUTER RANKINGS
By calculations per second per $1,000
Analytical engine
Never fully built, Charles Babbage's invention was designed to solve computational and logical problems
Colossus
The electronic computer, with 1,500 vacuum tubes, helped the British crack German codes during WW II
UNIVAC I
The first commercially marketed computer, used to tabulate the U.S. Census, occupied 943 cu. ft.
Apple II
At a price of $1,298, the compact machine was one of the first massively popular personal computers
Power Mac G4
The first personal computer to deliver more than 1 billion floating-point operations per second
2045
Surpasses brainpower equivalent to that of all human brains combined
Surpasses brainpower of human in 2023
Surpasses brainpower of mouse in 2015
Hollerith Tabulator
IBM Tabulator
National Ellis 3000
Zuse 2
Zuse 3
ENIAC
IBM SSEC
BINAC
EDVAC
Whirlwind
Datamatic 1000
IBM 1620
DEC PDP-4
IBM 1130
DEC PDP-10
Data General Nova
Intellec-8
IBM PC
Compaq Deskpro 386
Pentium PC
Pentium II PC
Dell Dimension 8400
Mac Pro
Nvidia Tesla GPU & PC
10^{26}
10^{20}
10^{15}
10,000,000,000
100,000
1
0.00001
ELECTROMECHANICAL
RELAYS
VACUUM TUBES
TRANSISTORS
INTEGRATED CIRCUITS
1900
1920
1940
1960
1980
2000
2011
2020
2045

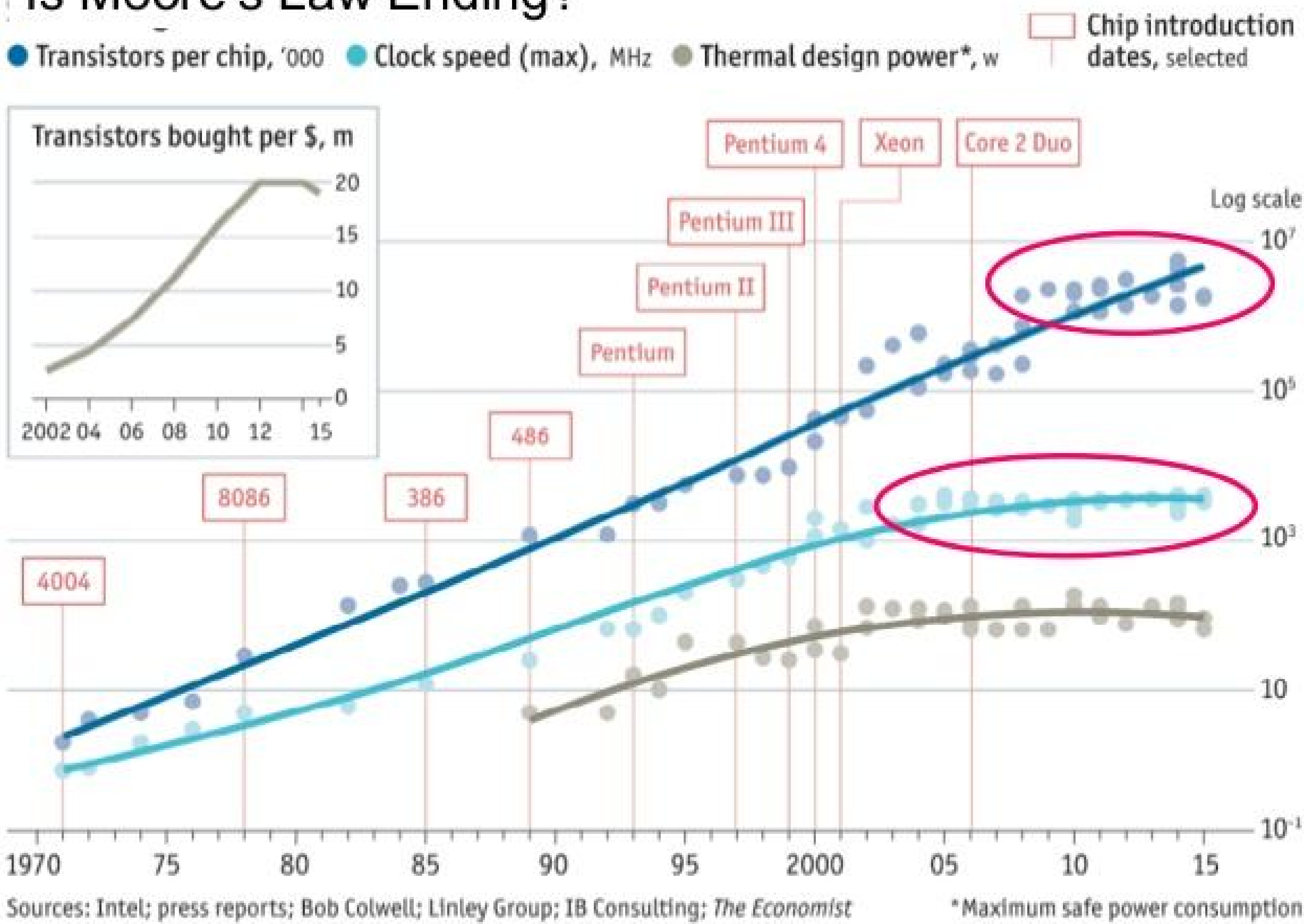
中国科学技术大学 陈凯


120 Years of Moore's Law
MECHANICAL
RELAY
VACUUM TUBE
TRANSISTOR
INTEGRATED CIRCUIT
Calculations per second per constant dollar
1E+09
1E+07
1E+05
1,000
10
0.1
0.001
1E-05
1E-07
1E-09
ANALYTICAL ENGINE
HOLLERITH TABULATOR
IBM TABULATOR
COLOSSUS
ENIAC
WHIRLWIND
DEC PDP-1
IBM 360
DATA GENERAL NOVA
CRAY 1
SUN 1
IBM PC
APPLE MACINTOSH
PENTIUM PC
POWER MAC
IBM ASCI WHITE
IBM BLUE GENE
GTX 480
NVIDIA TITAN X
1900
1905
1910
1915
1920
1925
1930
1935
1940
1945
1950
1955
1960
1965
1970
1975
1980
1985
1990
1995
2000
2005
2010
2015
2020
Year
Source: Ray Kurzweil, DFJ

中国科学技术大学 陈凯


05
03
01
99
97
95
93
91
89
85
83
81
79
77
75
73
71

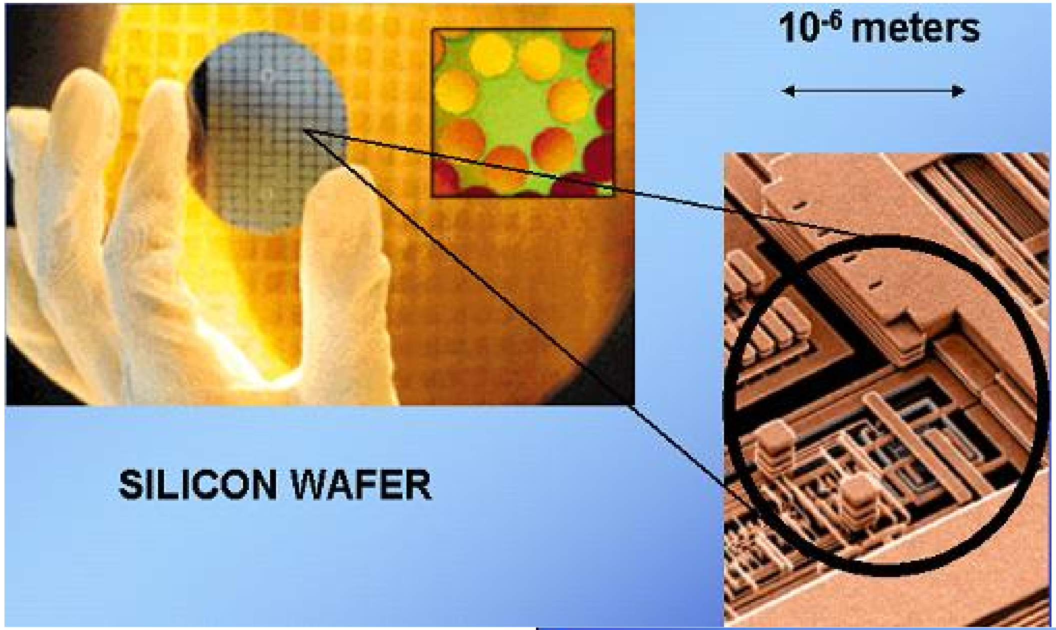
Is Moore's Law Ending?

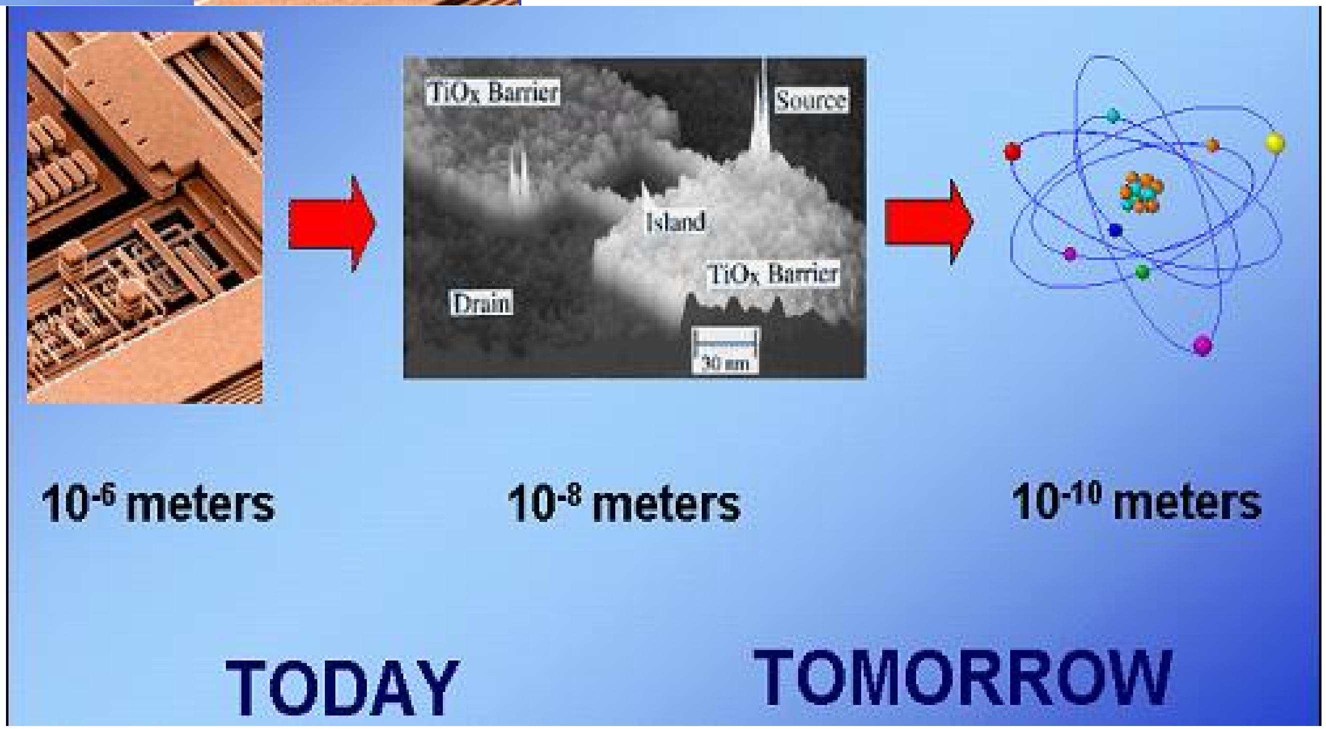


Economist, March 12-18, 2016

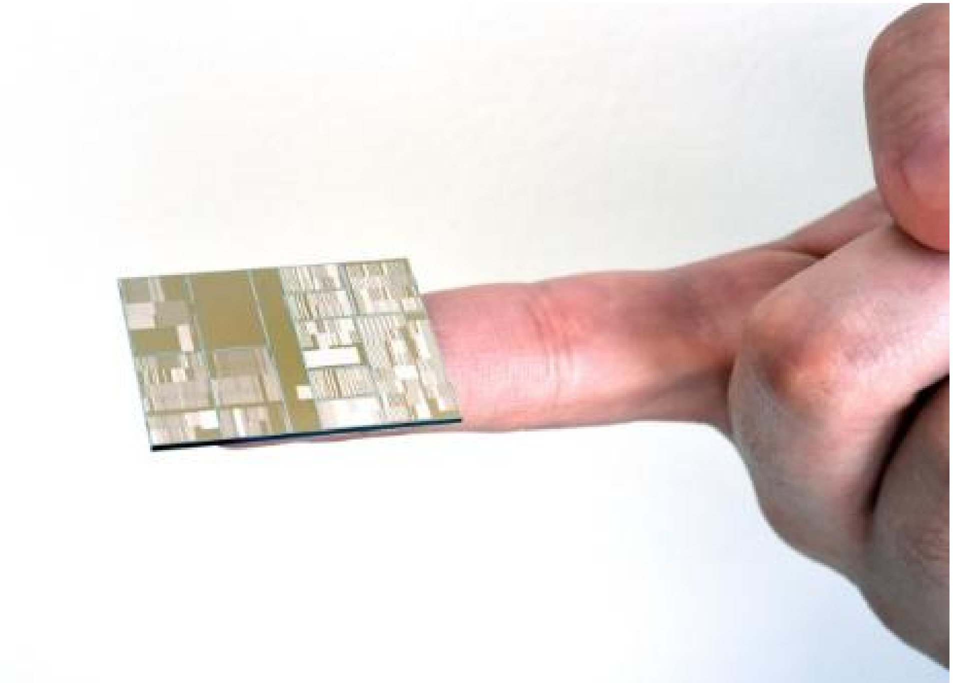
中国科学技术大学 陈凯

经典计算机发展状况


10^{-6} meters
SILICON WAFER


TiOx Barrier
Source
Island
TiOx Barrier
Drain
30 nm
10^{-6} meters
10^{-8} meters
10^{-10} meters
TODAY
TOMORROW

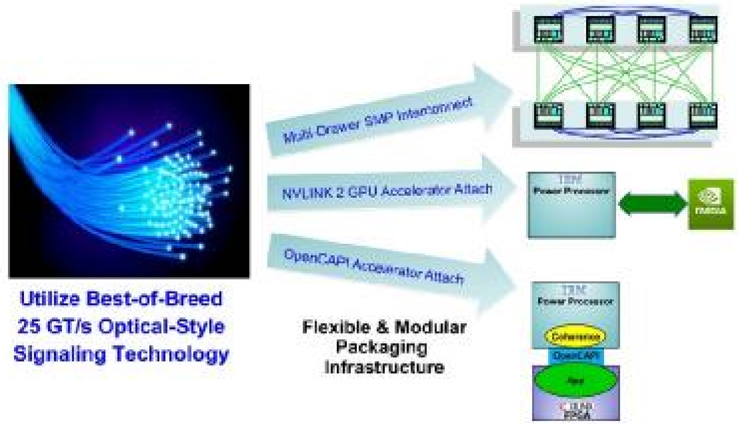
IBM 7nm chip

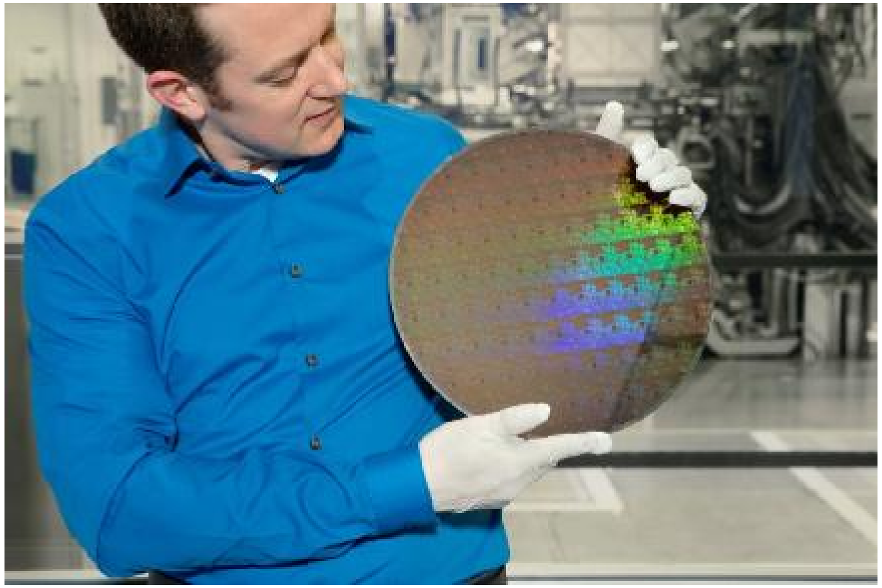


Beyond silicon: IBM unveils world's first 7nm chip
With a silicon-germanium channel and EUV lithography(extreme ultraviolet lithography), IBM crosses the 10nm barrier. –July 2015

IBM 技术

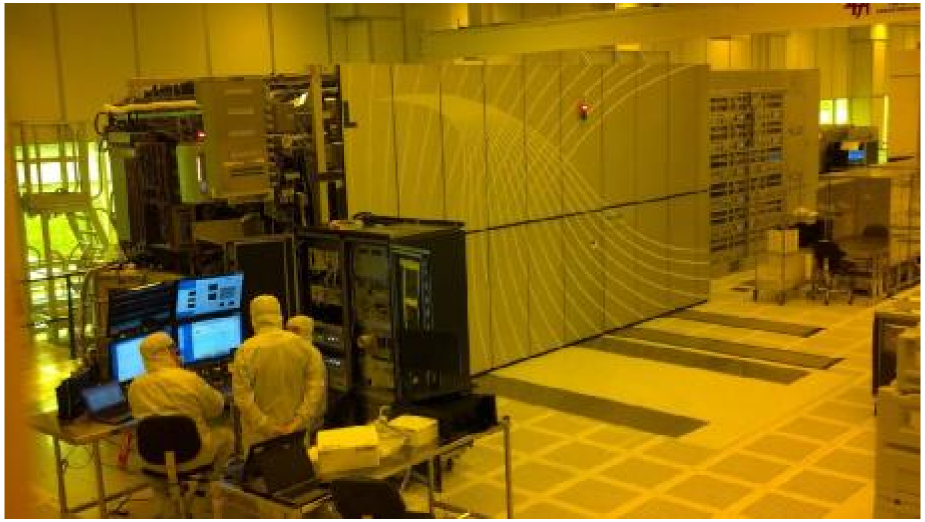
PowerAXON → High-speed 25 GT/s Signaling





20 billion transistors

30 billion transistors



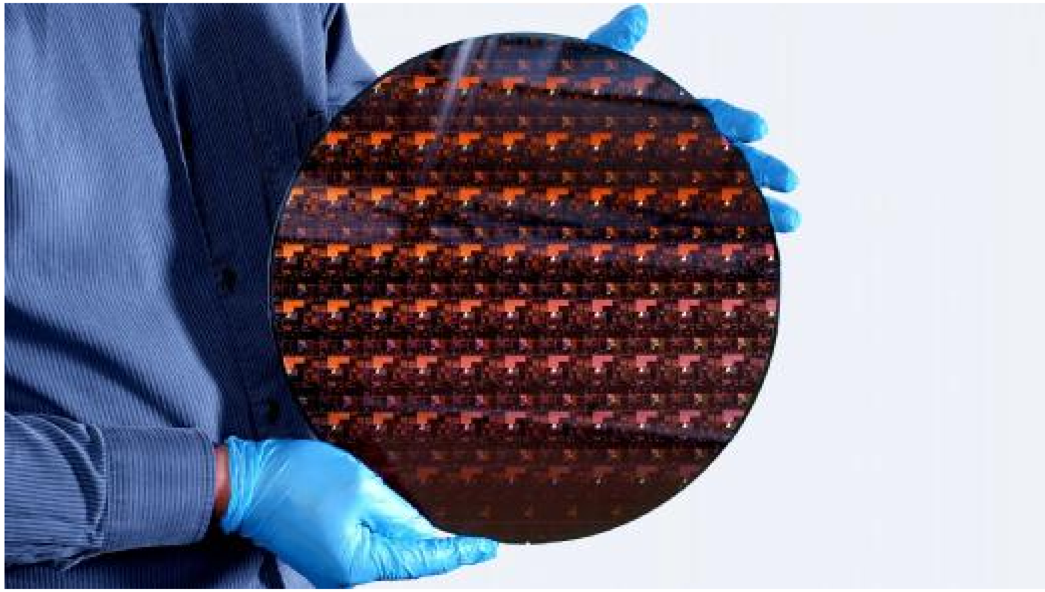
05 Jun 2017

Wafer of chips with 5nm silicon nanosheet transistors

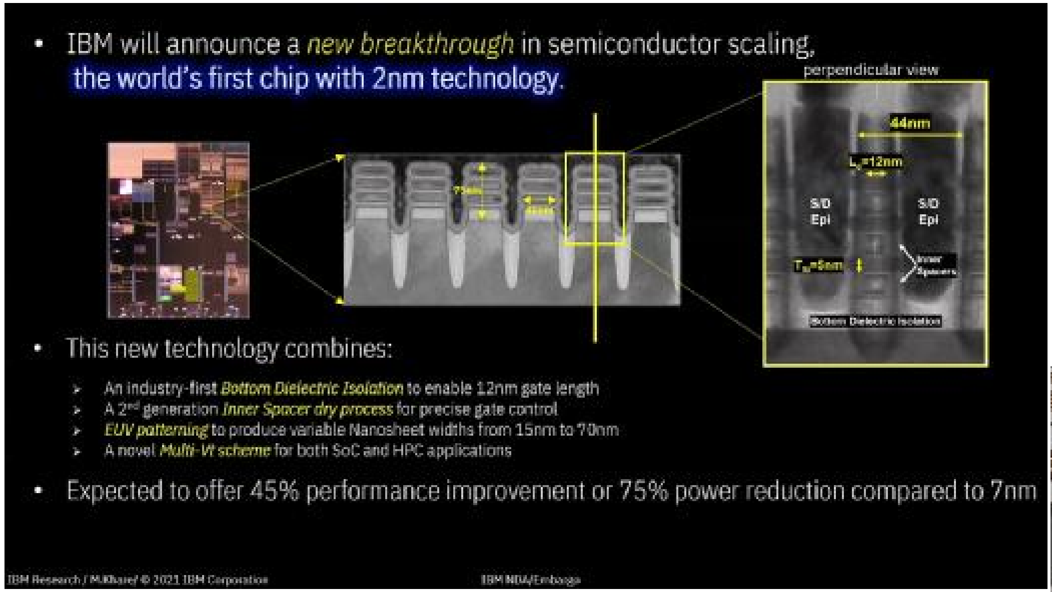
IBM Research scientist Nicolas Loubet holds a wafer of chips with 5nm silicon nanosheet transistors manufactured using an industry-first process that can deliver 40 percent performance enhancement at fixed power, or 75 percent power savings at matched performance. (Credit: Connie Zhou)

6 May 2021

IBM 技术 2nm



According to IBM, the new 2nm process is capable of fitting 50 billion transistors on a chip the size of a fingernail—up from the 30 billion transistors on the 5nm node.
https://www.pcmag.com/news/ibm-unveils-2-nanometer-chip-process-but-actual-products-are-still-years



The potential benefits of these advanced 2 nm chips could include:

- **Quadrupling cell phone battery life**, only requiring users to charge their devices every four days.
- **Slashing the carbon footprint of data centers,** which account for one percent of global energy use. Changing all of their servers to 2 nm-based processors could potentially reduce that number significantly.
- **Drastically speeding up a laptop's functions,** ranging from quicker processing in applications, to assisting in language translation more easily, to faster internet access.
- **Contributing to faster object detection** and reaction time in autonomous vehicles like self-driving cars.

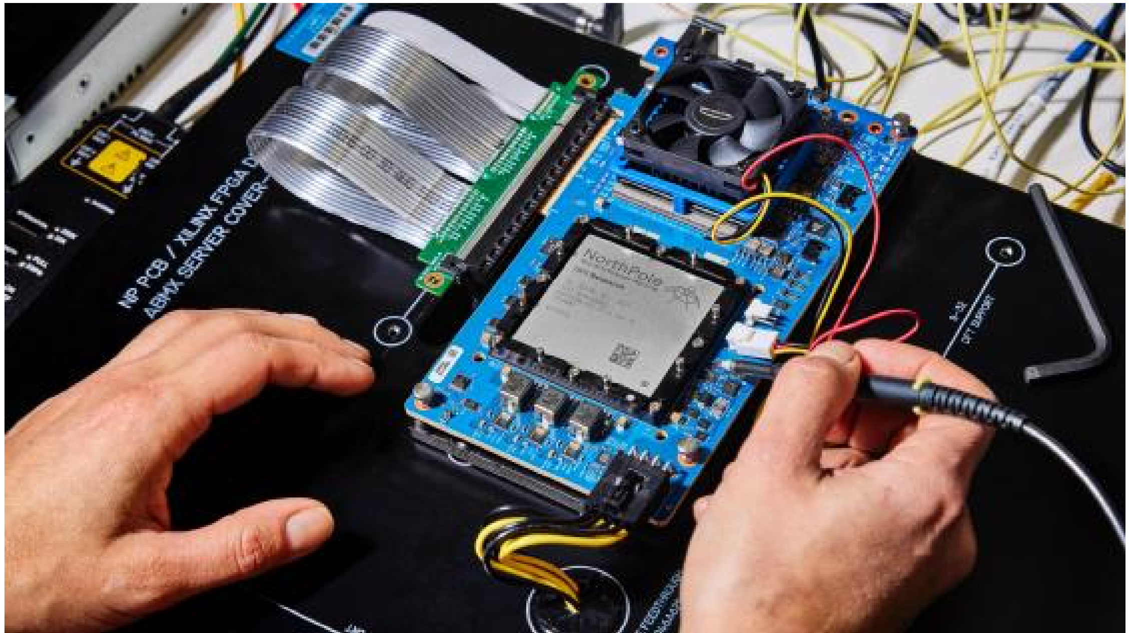
20 Oct. 2023

IBM 技术 AI Chip

A new chip architecture points to faster, more energy-efficient AI

The first promising set of results from NorthPole chips were published today in Science. NorthPole is a breakthrough in chip architecture that delivers massive improvements in energy, space, and time efficiencies, according to Modha. Using the ResNet-50 model as a benchmark, NorthPole is considerably more efficient than common 12-nm GPUs and 14-nm CPUs. (NorthPole itself is built on 12 nm node processing technology.) In both cases, NorthPole is 25 times more energy efficient, when it comes to the number of frames interpreted per joule of power required. NorthPole also outperformed in latency, as well as space required to compute, in terms of frames interpreted per second per billion transistors required. According to Modha, on ResNet-50, NorthPole outperforms all major prevalent architectures — even those that use more advanced technology processes, such as a GPU implemented using a 4 nm process.

https://research.ibm.com/blog/northpole-ibm-ai-chip

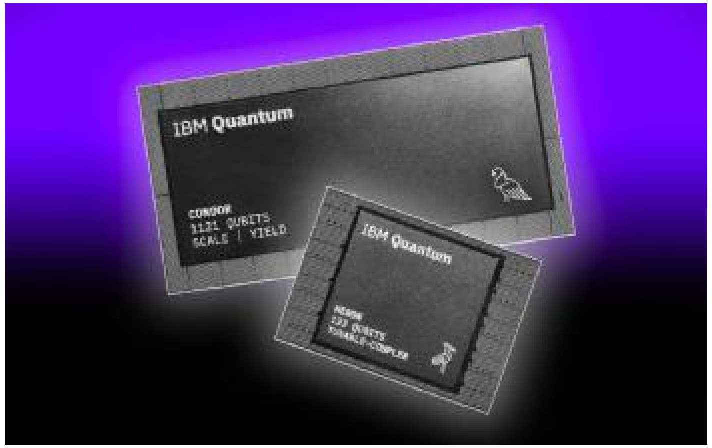


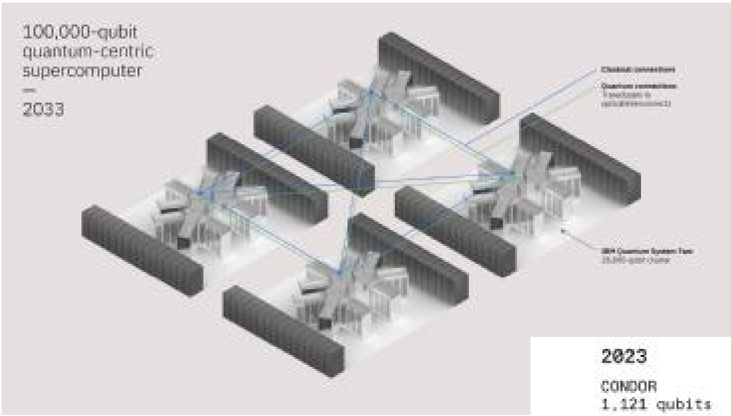
Since the birth of the semiconductor industry, computer chips have primarily followed the same basic structure, where the processing units and the memory storing the information to be processed are stored discretely. While this structure has allowed for simpler designs that have been able to scale well over the decades, it's created what's called **the von Neumann bottleneck**, where **it takes time and energy to continually shuffle data back and forth between memory, processing, and any other devices within a chip**. The work by IBM Research's Dharmendra Modha and his colleagues aims to change this, taking inspiration from how the brain computes. "**It forges a completely different path from the von Neumann architecture**," according to Modha.

IBM Quantum

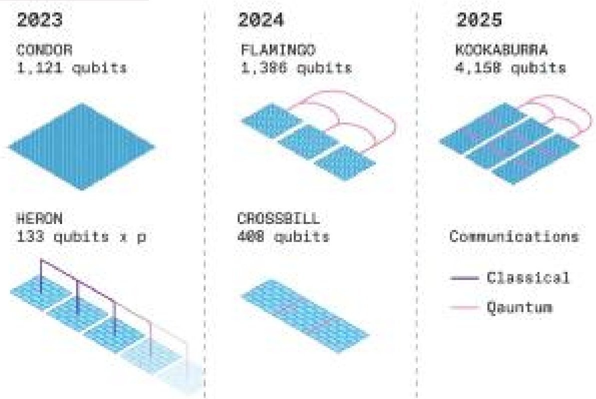
At IBM Quantum Summit 2023, '**IBM Quantum Heron**' was released as IBM's best performing quantum processor to date, with newly built architecture offering up to five-fold improvement in error reduction. (Credit: Christopher Tirrell for IBM)

IBM Heron is the first in IBM's new class of performant processors with significantly improved error rates, offering a five-times improvement over the previous best records set by IBM Eagle.



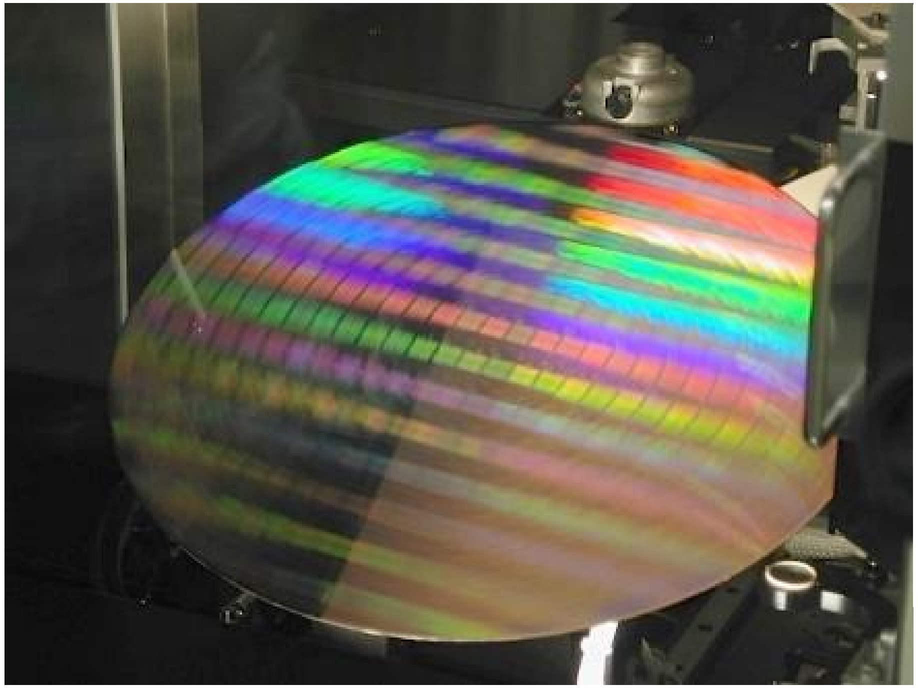


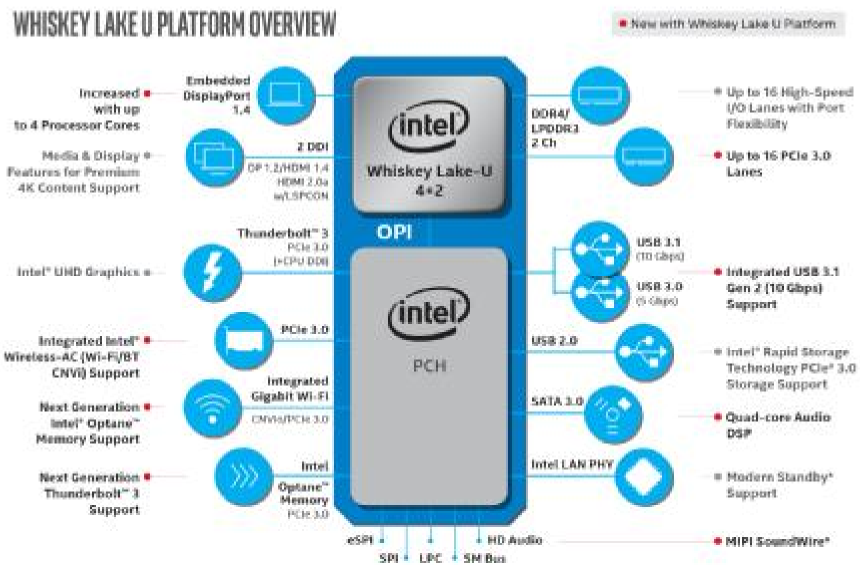
A visual rendering of IBM Quantum's 100,000-qubit quantum-centric supercomputer, expected to be deployed by 2033. (Credit: IBM)



We've added a new dimension to our roadmap: the innovation roadmap, calling out key advances required to bring about error-corrected quantum computing at scale. After demonstrating Condor, our 1,121-qubit concept processor in 2023, we'll now focus on modular scaling by introducing l- and m-couplers with Flamingo and Crossbill, and in 2026, c-couplers with Kookaburra. These new breakthroughs will put us on course for an error-corrected quantum system running 100 million gates by 2029 and a billion gates by 2033.

Intel





An Intel wafer. Chipmakers may find it more difficult to justify the huge costs of developing the next generations of chip technology.

华为人工智能芯片—麒麟系列

华为人工智能芯片—麒麟系列

华为麒麟9000系列

麒麟9000关键特性

•Process
•• 5nm
•CPU
•• 1 x Cortex-A77@ 3.13 GHz
• 3 x Cortex-A77@ 2.54 GHz
• 4 x Cortex-A55@2.05 GHz
•GPU
•• 24-core Mali-G78, Kirin Gaming+ 3.0
•AI
•• HUAWEI Da Vinci Architecture 2.0
• Ascend Lite*2+Ascend Tiny*1
•5G
•• SA&NSA,Sub-6G&mmWave
•ISP
•• Kirin ISP 6.0,Quad-pipeline
•System Cache
•• 8MB
•Memory
•• LPDDR 5/4X

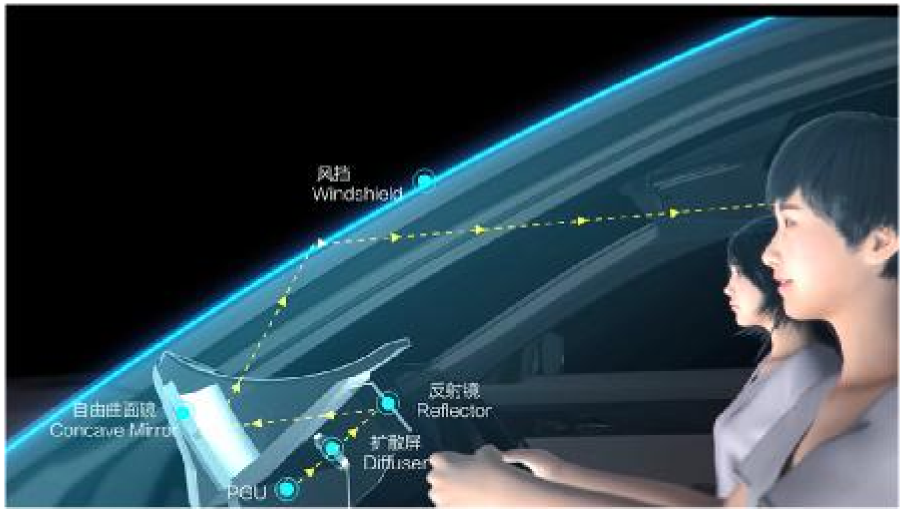
麒麟9000S是HUAWEI Mate 60系列搭载的处理器。

2023年8月29日，搭载麒麟9000S的华为Mate60 Pro发布。目前搭载该芯片的机型有华为Mate 60、华为Mate 60 Pro、华为Mate 60 Pro+及华为Mate60 Ultimate Design非凡大师

麒麟9000S的CPU部分为支持超线程技术的新一代泰山架构内核，采用8核心12线程，其中包括1颗2.62Ghz的泰山核心，三颗2.15Ghz的泰山核心和四颗1.53Ghz的A510核心；GPU型号为自研的Maleoon 910

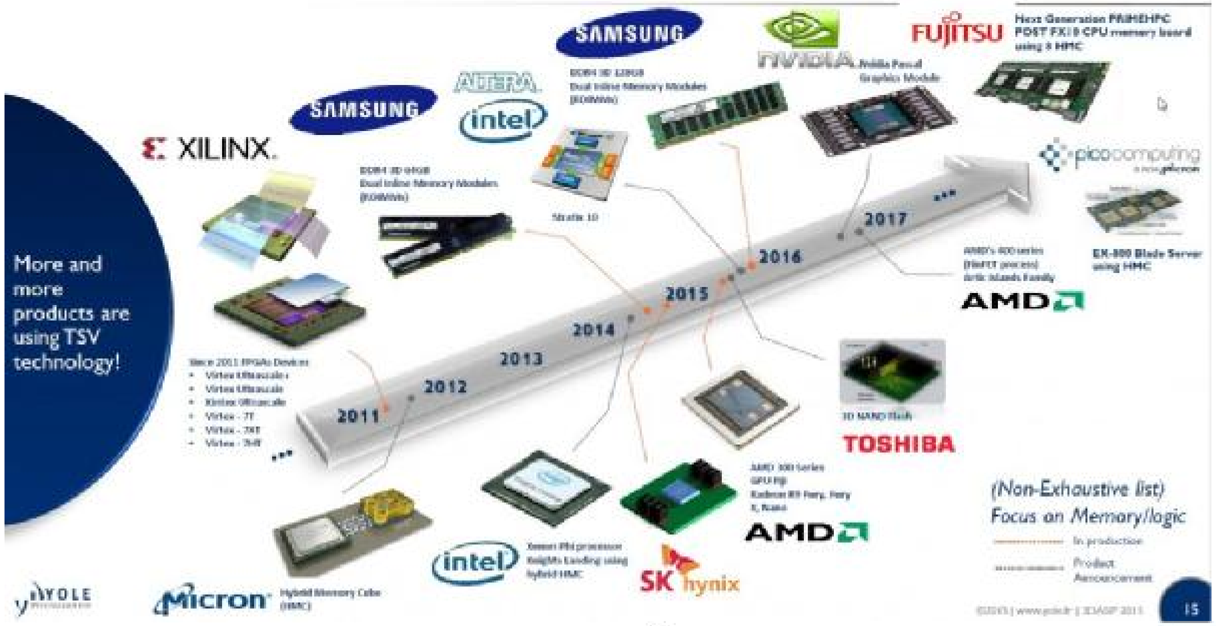
华为


HarmonyOS
华为全场景 新品来袭
一生万物，万物归一
HarmonyOS 是新一代的智能终端操作系统，为不同设备的智能化、互联与协同提供了统一的语言，带来简捷、流畅、连续、安全可靠的全场景交互体验。


风挡
Windshield
自由曲面镜
反射镜
Reflector
扩散屏
Diffuser
PGU

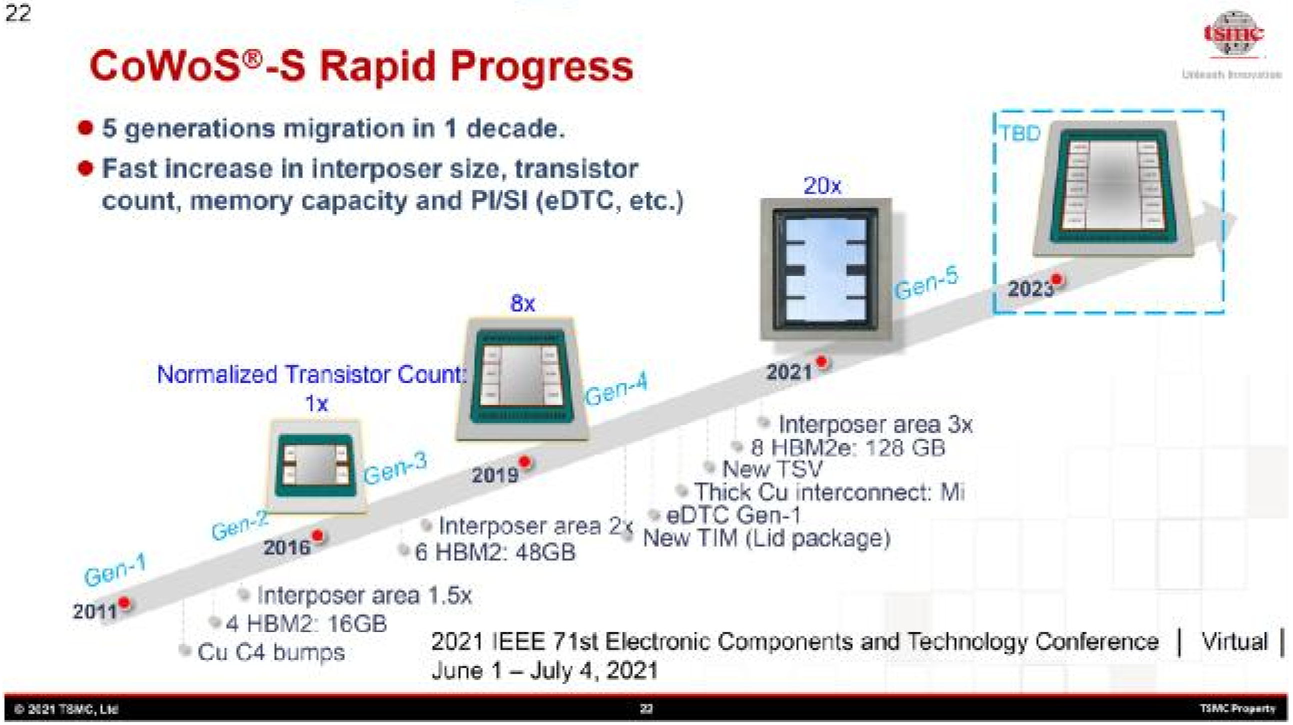

80M
85
90
6.0

相关技术



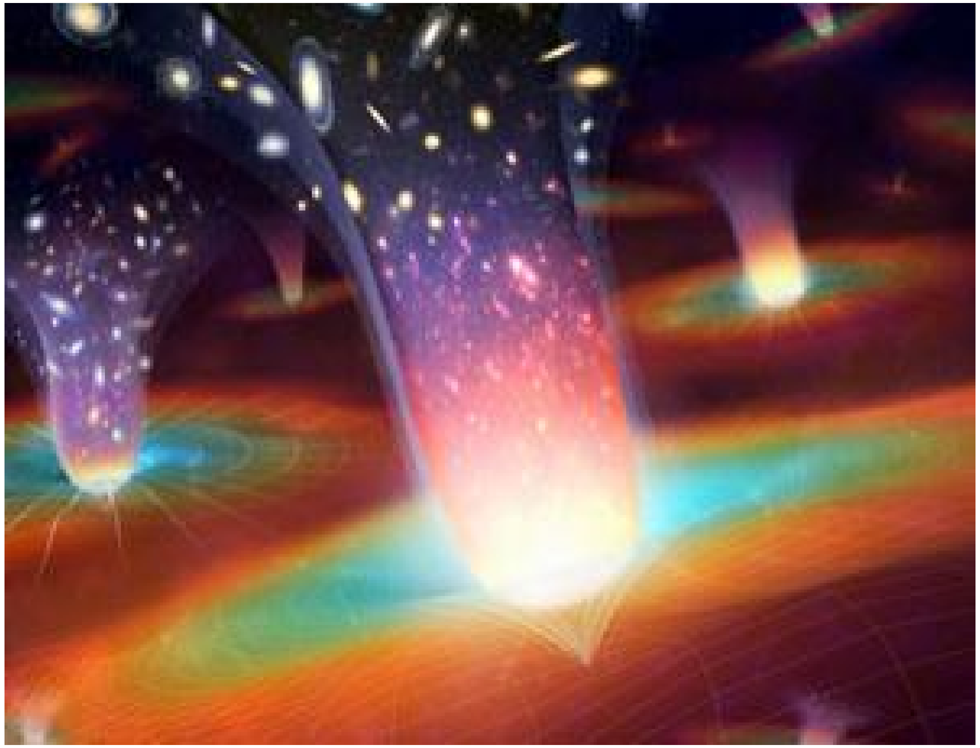
22

Memory Architecture –
3D TSV Memory Packaging



What is quantum information?

"Information is physical." 1960s *by Rolf Landauer* from IBM Research

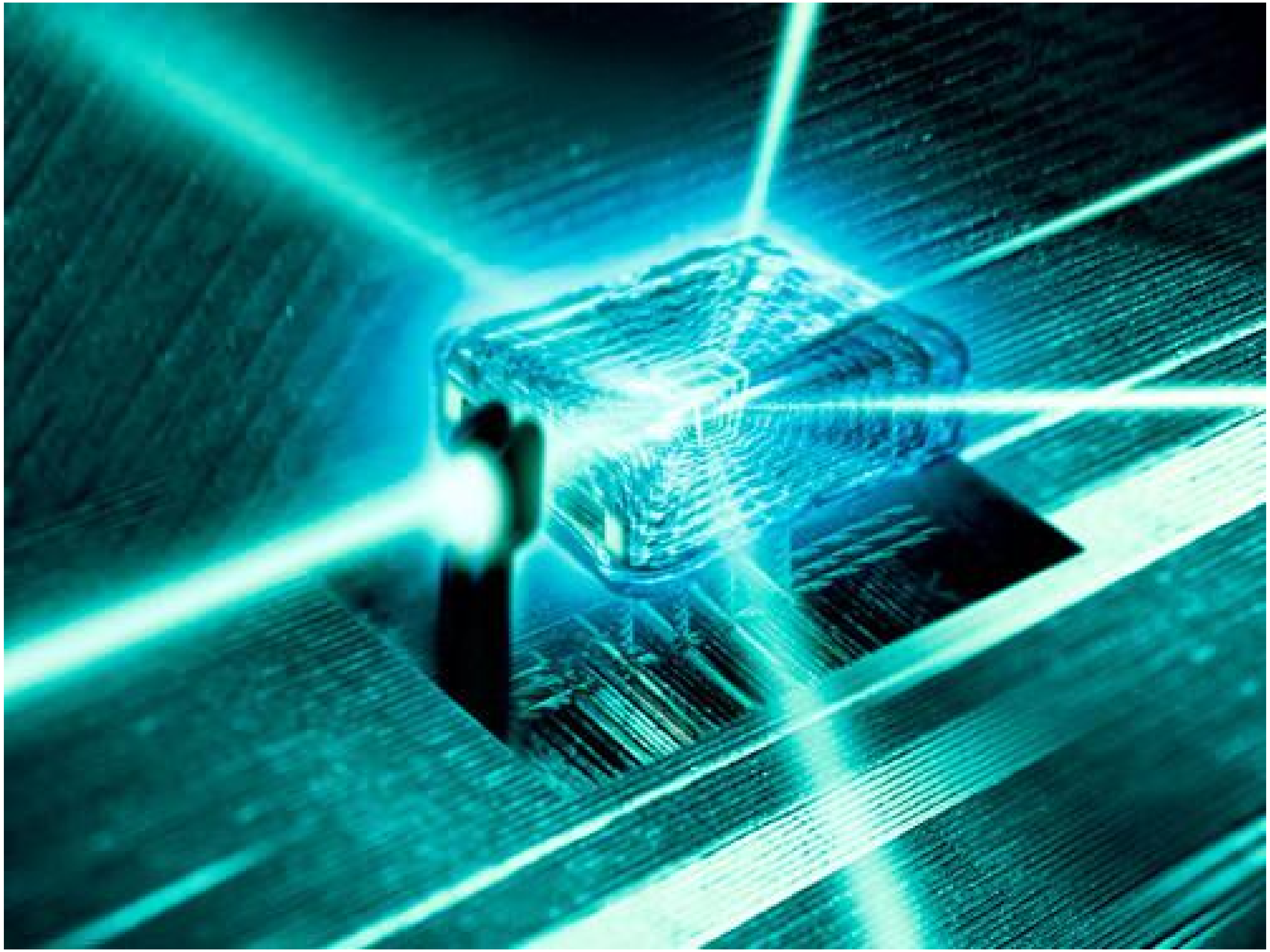


Quantum information is that kind of information which is carried by quantum systems from the preparation device to the measuring apparatus in a quantum mechanical experiment. *by R.F. Werner*

from New Scientist

Getting inside the mind of God

from New Scientist



If we can harness the fuzziness of quantum entities to crunch vast amounts of data instantaneously, the sky will be no limit. **Vlatko Vedral** is your guide

Image: Richard Kail/Science Photo Library

from New Scientist

Spooky action at a distance

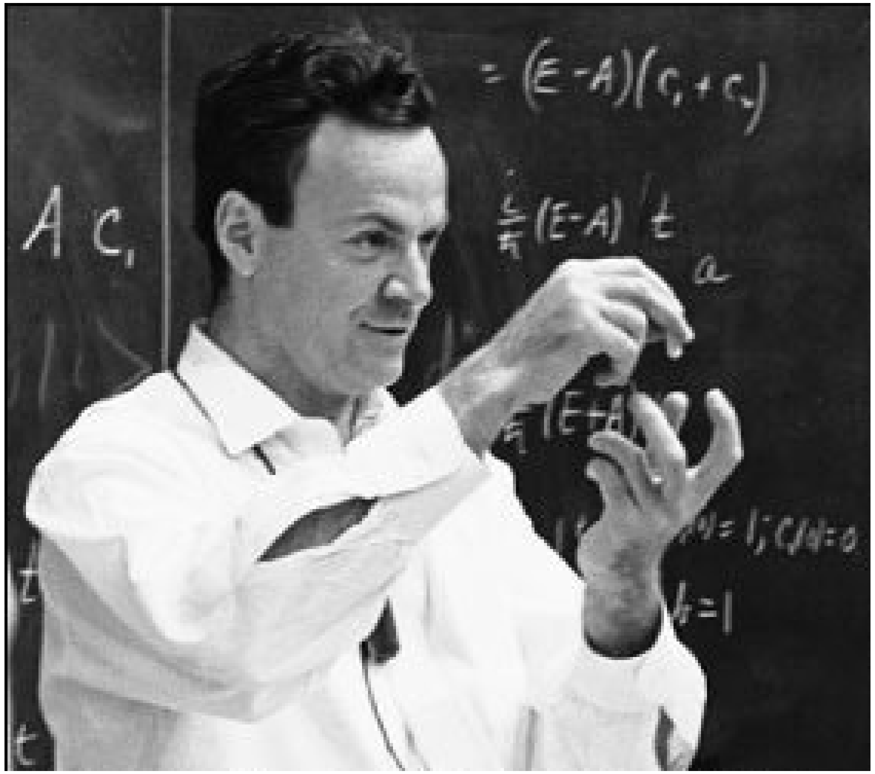
Wave-Particle Duality

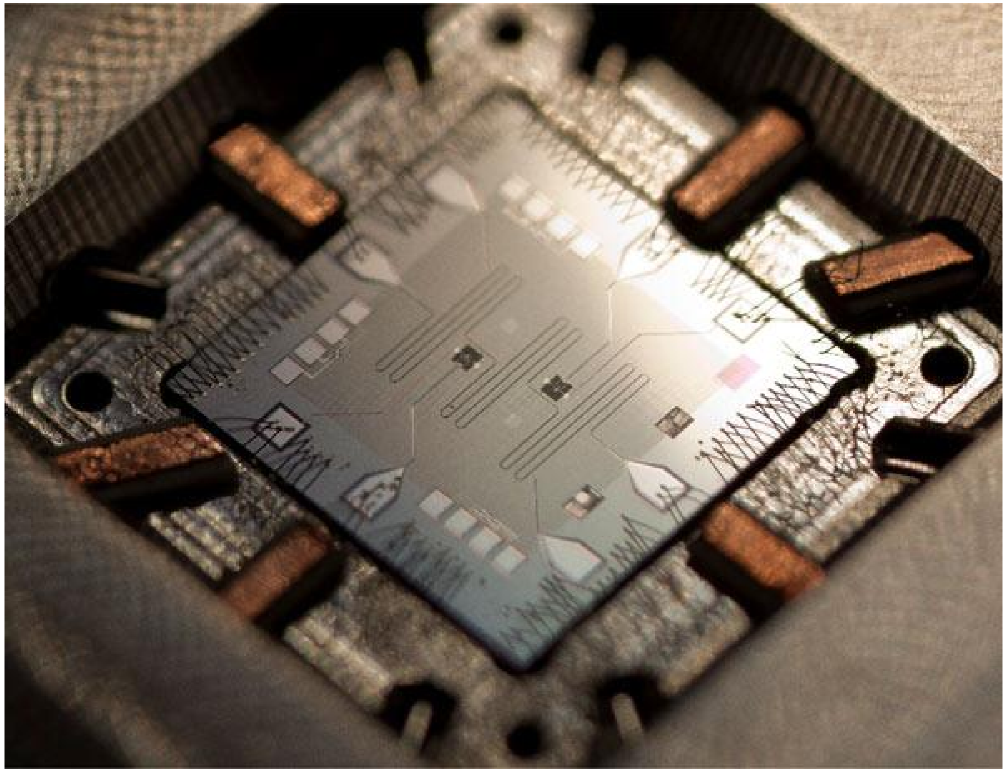
from New Scientist

"There is plenty of room at the bottom." (Dec 29, 1959)

"It seems that the laws of physics present no barrier to reducing the size of computers until bits are the size of atoms, and quantum behavior holds dominant sway."

——Richard P. Feynman (1985)





Nobel prize 1965

from New Scientist

量子世界

(Max Planck)

$$E = \frac{\hbar c}{\lambda}$$

$$E = mc^2$$

(Albert Einstein)

(Louis de Broglie)

$$\lambda = \frac{\hbar}{mc}$$

互补性和不确定原理

(Neils Bohr)

(Werner Heisenberg)

量子测量 塌缩

经典和量子比特

经典和量子信息处理中的本质不同在于存贮和处理信息的方式

在经典信息处理中，信息是由宏观的比特来表示通常取值为二进制的值

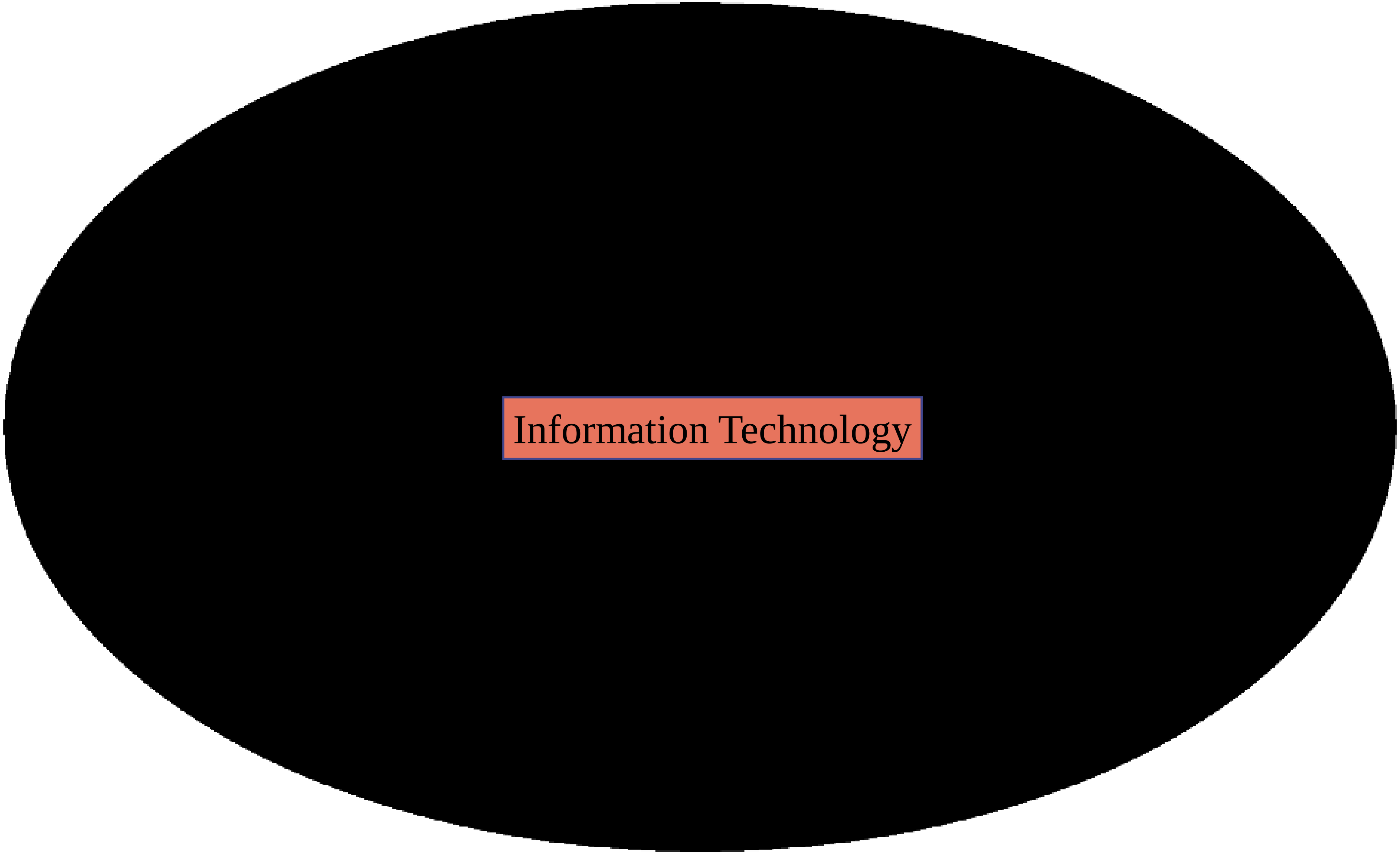
0 或者 1

在量子信息处理中，信息是由微观的量子比特来表征，通常取值不可数的多值形式

$\alpha|0\rangle + \beta|1\rangle$

其中α, β其中为满足下式的任意两个复数

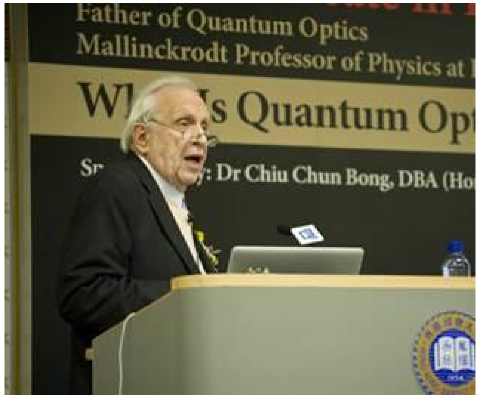
$|\alpha|^2 + |\beta|^2 = 1.$


Information Technology

量子信息处理的概念和内涵

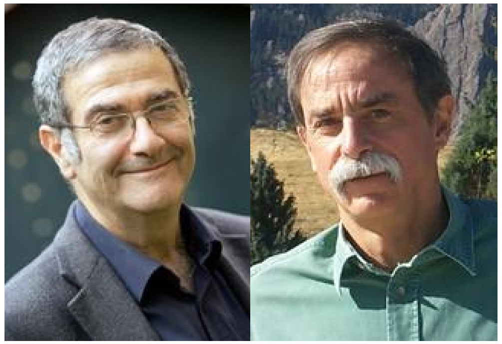
- 量子信息处理是指以量子力学基本原理为基础、利用量子态的相干特性来编码、传输和操控信息，进而实现量子计算、量子通信、量子精密测量、量子模拟等功能的全新信息处理方式。
- 由于携带量子信息的载体可以工作在原子分子层次上，从而只需要损耗更少的能量来进行处理、存储和传输。
- 是经典信息处理的大幅拓展，探索和发展更有效地进行计算、通信、测量等的方式

量子信息的重要科学意义



- Roy J. Glauber 由于在量子光学理论及其在量子信息科学应用上的重要贡献获2005年诺贝尔物理学奖

- Anton Zeilinger等由于在量子物理和量子信息领域重要的实验成就获2010年沃尔夫物理学奖



- Serge Haroche和David Wineland由于在量子系统测量与操控及其在量子信息科学应用上的重要贡献获2012年诺贝尔物理学奖

- Peter Zoller和Ignacio Cirac由于在量子信息、量子光学和冷原子物理领域的开创性理论贡献获2013年沃尔夫物理学奖

Press release: The Nobel Prize in Physics 2022

English
English (pdf)
Swedish
Swedish (pdf)

KUNGL.
VETENSKAPS
AKADEMIEN
THE ROYAL SWEDISH ACADEMY OF SCIENCES

4 October 2022

The Royal Swedish Academy of Sciences has decided to award the Nobel Prize in Physics 2022 to

Alain Aspect
Institut d'Optique Graduate School – Université Paris-Saclay and École Polytechnique, Palaiseau, France

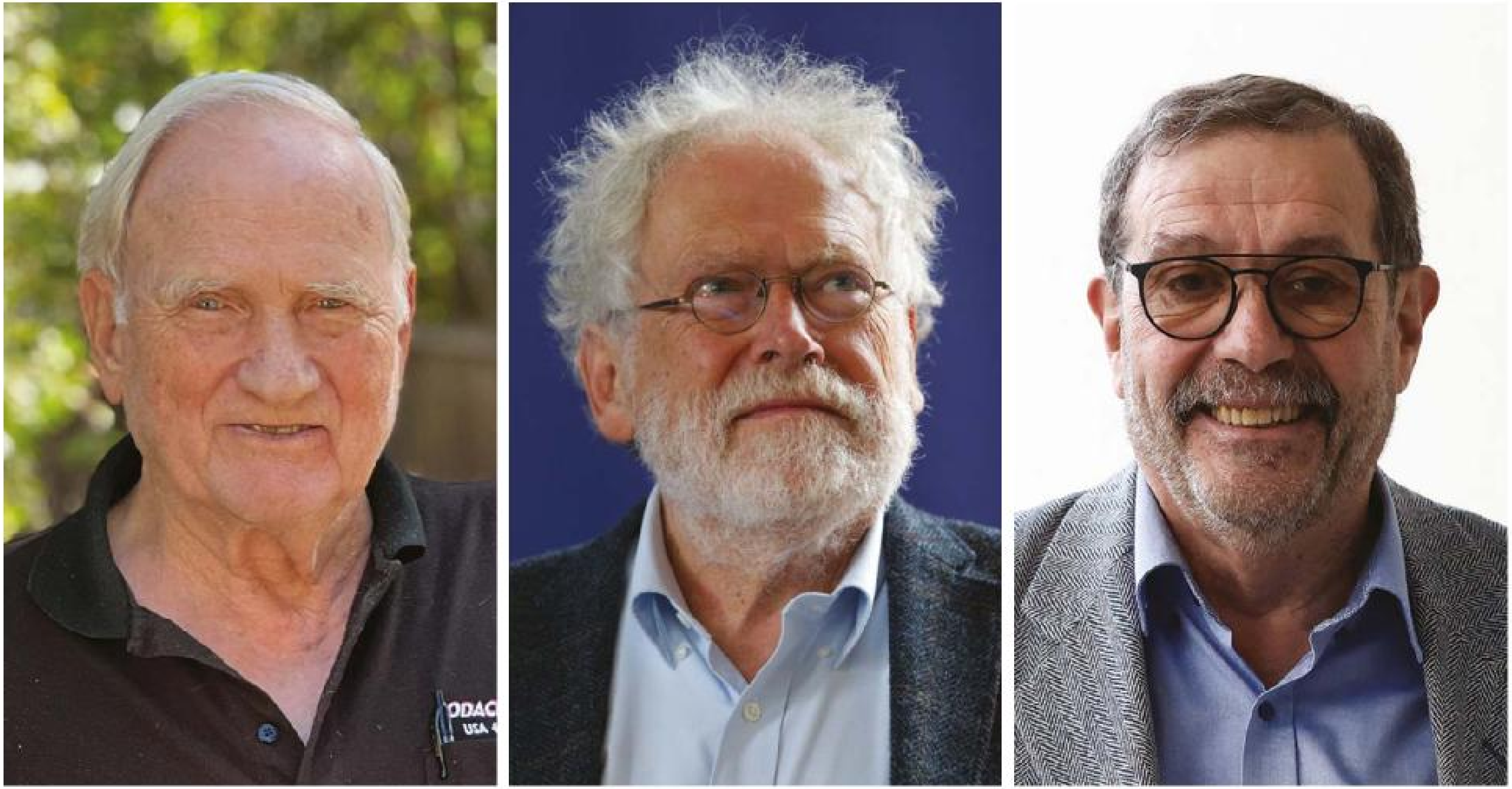
John F. Clauser
J.F. Clauser & Assoc., Walnut Creek, CA, USA

Anton Zeilinger
University of Vienna, Austria

"for experiments with entangled photons, establishing the violation of Bell inequalities and pioneering quantum information science"

Entangled states – from theory to technology

Alain Aspect, John Clauser and Anton Zeilinger have each conducted groundbreaking experiments using entangled quantum states, where two particles behave like a single unit even when they are separated. Their results have cleared the way for new technology based upon quantum information.



From left: John Clauser, Anton Zeilinger and Alain Aspect won this year's physics Nobel prize.

PHYSICS NOBEL FOR 'SPOOKY' QUANTUM ENTANGLEMENT

Award goes to three physicists whose research laid the groundwork for quantum information science.

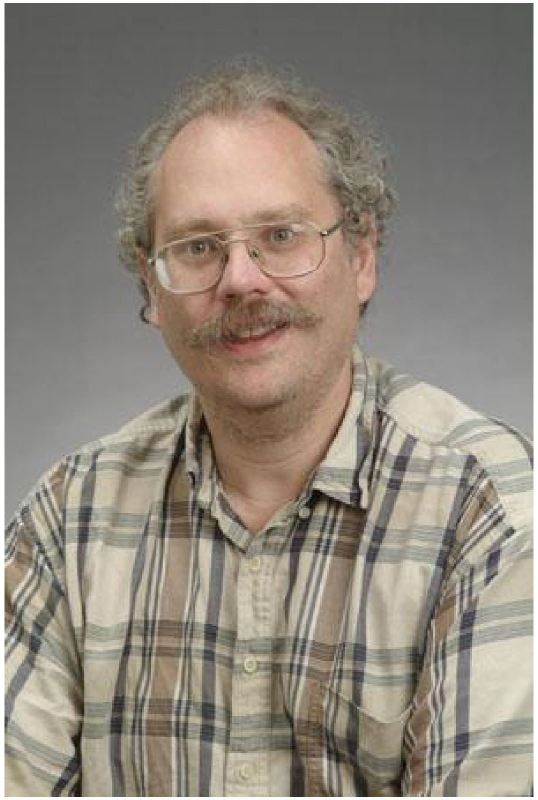
Nature | Vol 610 | 13 October 2022 | 241

中国科学技术大学 陈凯

量子信息处理

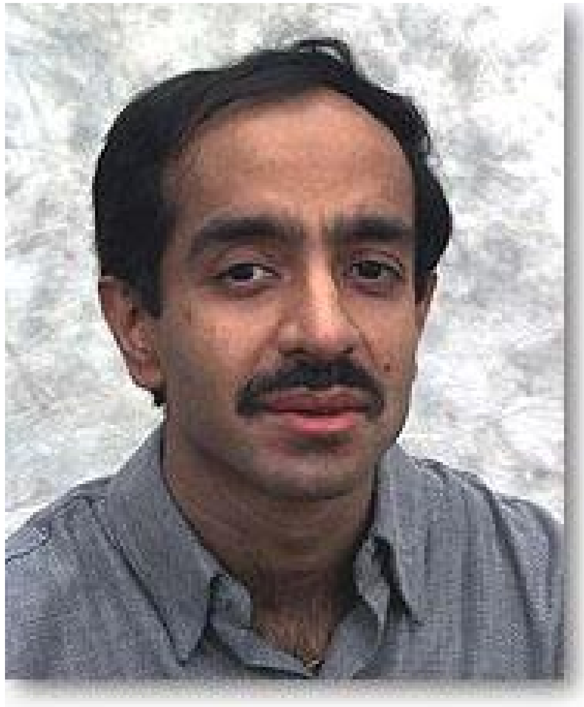
It’s a “mystery”. THE mystery. We don’t understand it, but we can tell you how it works. *(Feynman)*

量子信息发展史



Peter Shor 算法(1994)

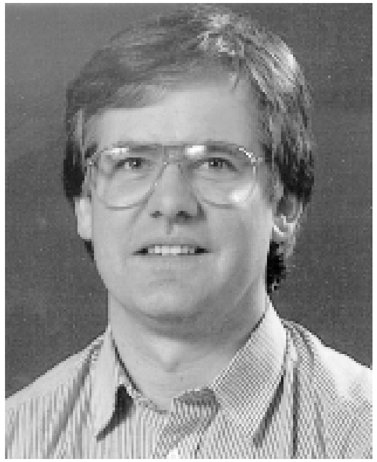
Lov Grover算法(1997)



Seth Lloyd

Deutsch普适量子计算

Deutsch－Jozsa算法



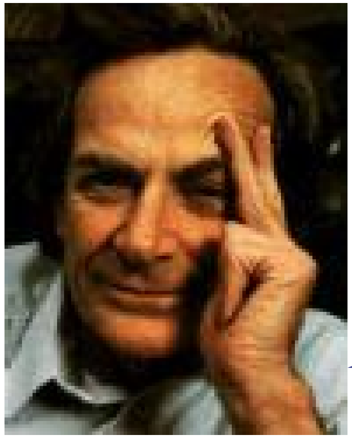
Ekert(E91协议)

Steane纠错码

Cirac，Zoller

量子信息理论

量子信息发展史

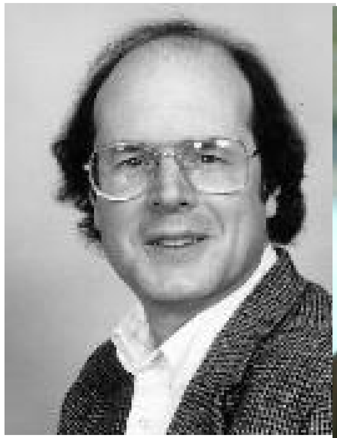


(Richard Feynman)

"There's plenty of room at the bottom"

(Paul Benioff)

Quantum Turing machine



(C. Bennett) (G. Brassard)

Quantum key distribution BB84

(David Deutsch)

Universal QC

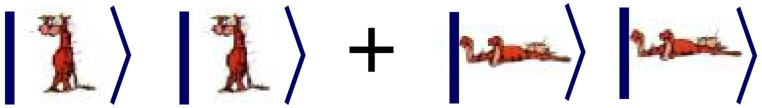
Quantum Communication Complexity

Andrew Chi-Chih Yao

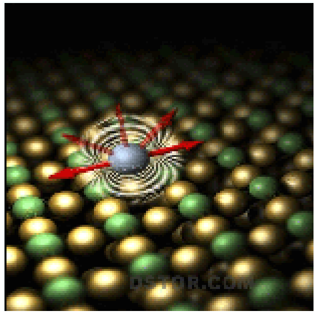
量子比特与量子纠缠

量子　物质最基本单元的物理描述
例如光量子，是传递电磁相互作用的基本粒子
不可分割

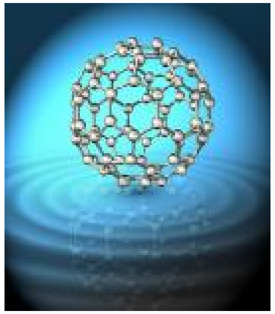
量子纠缠



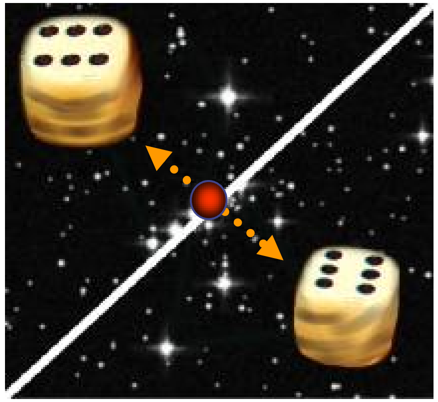
光子



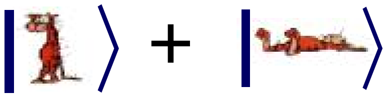
原子



分子

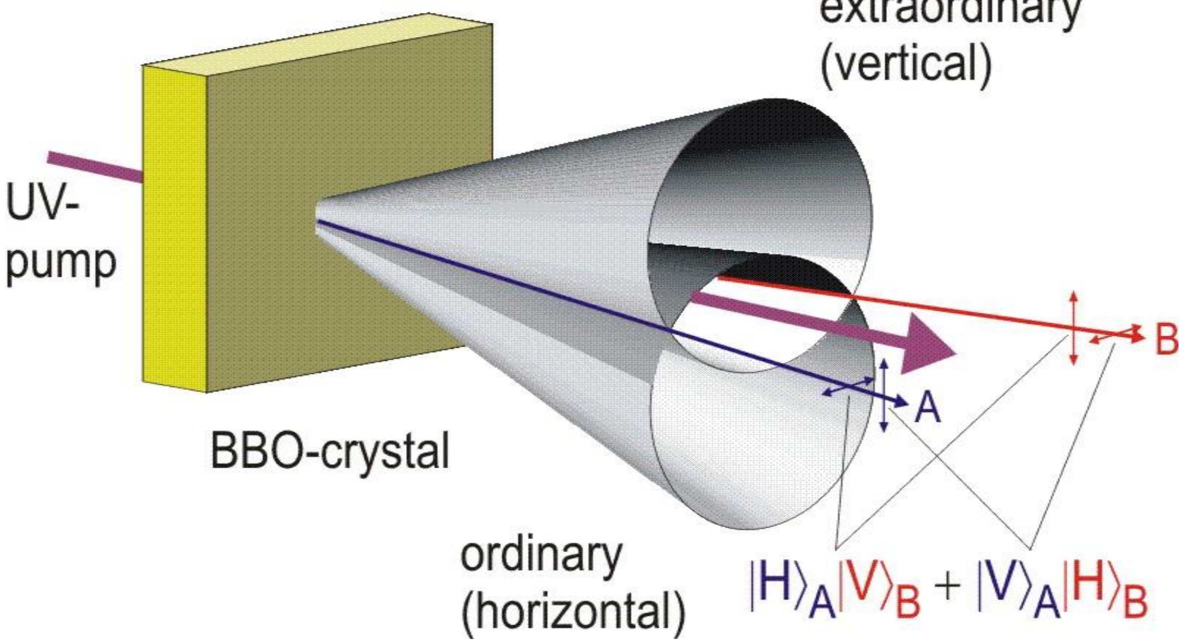


遥远地点之间的惊人关联！

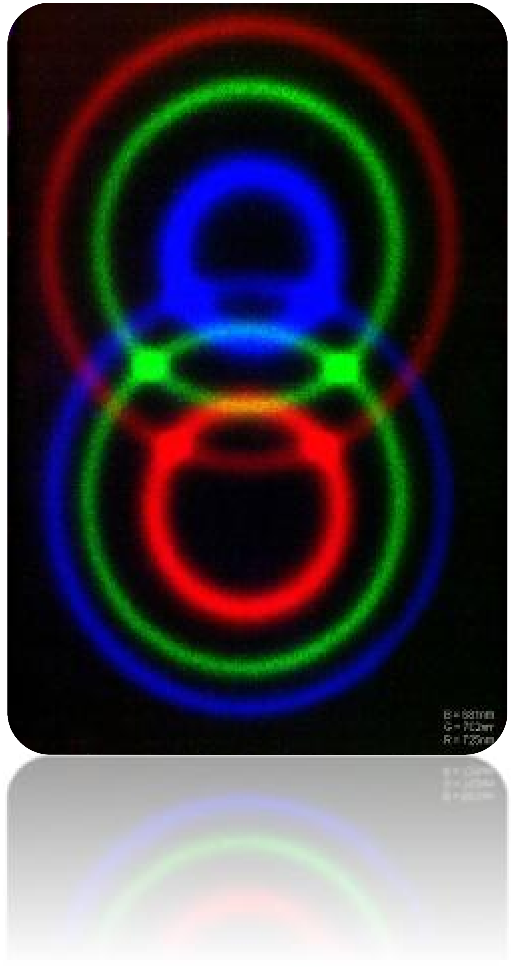
		
经典比特	0	1
量子比特	$\|0\rangle$	$\|1\rangle$
叠加态		
光子极化		

中国科学技术大学 陈凯

Polarization Entanglement Source



PDC

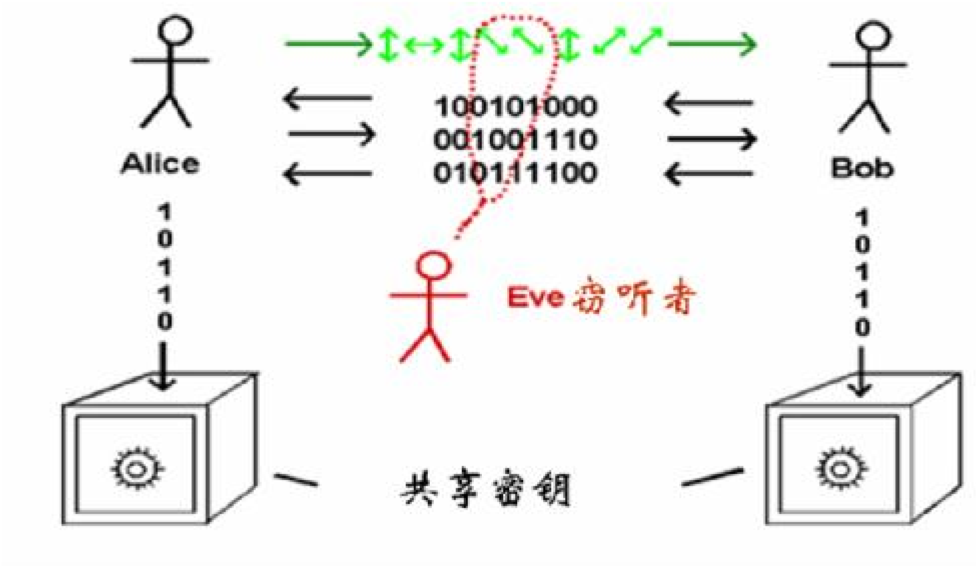


$$|\Phi^{\pm}\rangle_{12} = \frac{1}{\sqrt{2}}\left(|H\rangle_1|H\rangle_2 \pm |V\rangle_1|V\rangle_2\right)$$

$$|\Psi^{\pm}\rangle_{12} = \frac{1}{\sqrt{2}}\left(|H\rangle_1|V\rangle_2 \pm |V\rangle_1|H\rangle_2\right)$$

- P. G. Kwiat et al., Phys. Rev. Lett. 75, 4337 (1995)

量子通信技术:量子加密术



单粒子方案
Bennett & Brassard (1984)

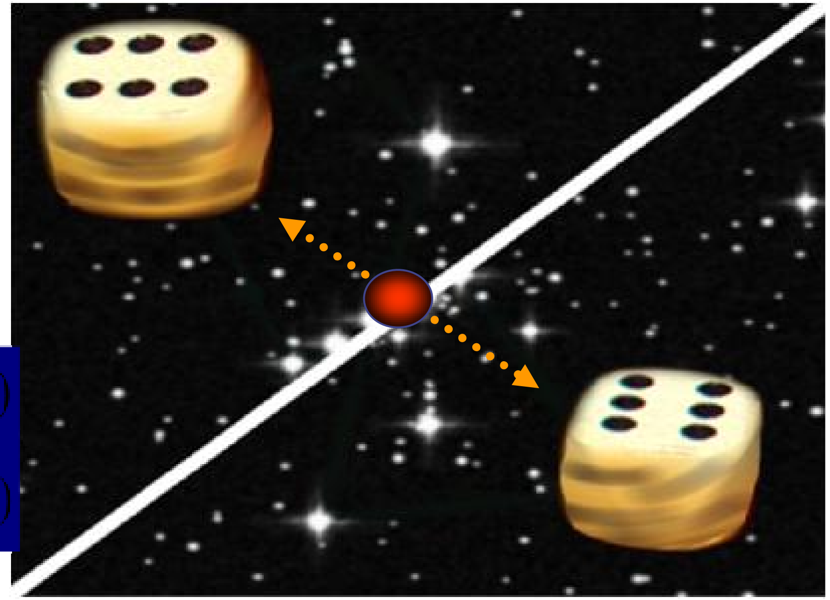
无条件安全的密钥生成

纠缠态方案

Ekert, PRL 67, 661 (1991)

$$|\Phi^{\pm}\rangle_{12} = \frac{1}{\sqrt{2}}(|\leftrightarrow\rangle_1|\leftrightarrow\rangle_2 \pm |\updownarrow\rangle_1|\updownarrow\rangle_2)$$

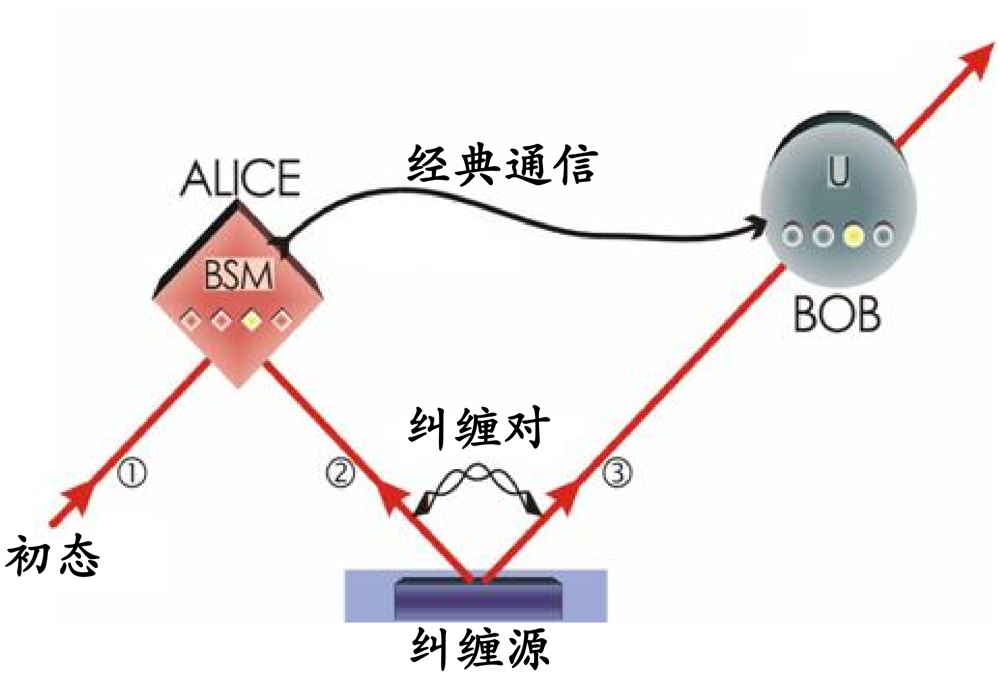
$$|\Psi^{\pm}\rangle_{12} = \frac{1}{\sqrt{2}}(|\leftrightarrow\rangle_1|\updownarrow\rangle_2 \pm |\updownarrow\rangle_1|\leftrightarrow\rangle_2)$$



- 量子不可克隆定理
- 量子不可分割
- 一次一密，完全随机

→ **无条件安全**

量子通信技术:量子隐形传态



初态 $|\Phi\rangle_1 = \alpha|\leftrightarrow\rangle_1 + \beta|\updownarrow\rangle_1$

纠缠对 $|\Phi^+\rangle_{23}$

$$
\begin{aligned}
|\Psi\rangle_{123} \; = \; & |\Phi^+\rangle_{12} \otimes (\alpha|\leftrightarrow\rangle_3 + \beta|\updownarrow\rangle_3) + \\
& |\Phi^-\rangle_{12} \otimes (\alpha|\leftrightarrow\rangle_3 - \beta|\updownarrow\rangle_3) + \\
& |\Psi^+\rangle_{12} \otimes (\alpha|\updownarrow\rangle_3 + \beta|\leftrightarrow\rangle_3) + \\
& |\Psi^-\rangle_{12} \otimes (\alpha|\updownarrow\rangle_3 - \beta|\leftrightarrow\rangle_3)
\end{aligned}
$$

Bennett et al., PRL 73, 3801 (1993)

量子计算与量子通信

量子并行性

经典比特	量子比特
0 或 1	0 + 1
00，01，10 或 11	00 + 01 + 10 + 11
000，001，010……	000 + 001 + 010 + ……
⋮	⋮

量子并行性使得量子计算机可以同时对 2^N 个数进行数学运算，其效果相当于经典计算机重复实施 2^N 次操作。

$$U\sum_{i=1}^{2^N} a_i|i\rangle = \sum_{i=1}^{2^N} a_i U|i\rangle, \quad 2^N!$$

Shor算法

$$Exp(\sqrt[3]{\log(N)}\cdot\sqrt[3]{\log\log(N)^2}\cdot O(1))$$

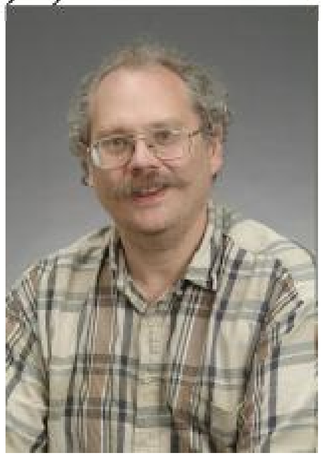
$$\Rightarrow O((\log(N))^3)$$

ã N比特整数，计算步数

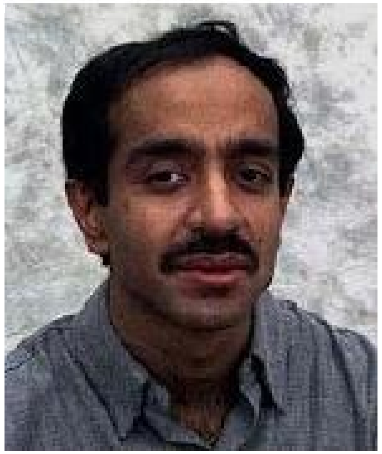
ã 利用经典THz计算机分解300位的大数，需10^{24}步，150000年。

ã 利用Shor算法THz计算机，只需10^{10}步，1秒！

ã RSA将不再安全！



P. W. Shor



L. K. Grover

Grover搜寻算法

ã 如何在草堆中找到一根针？

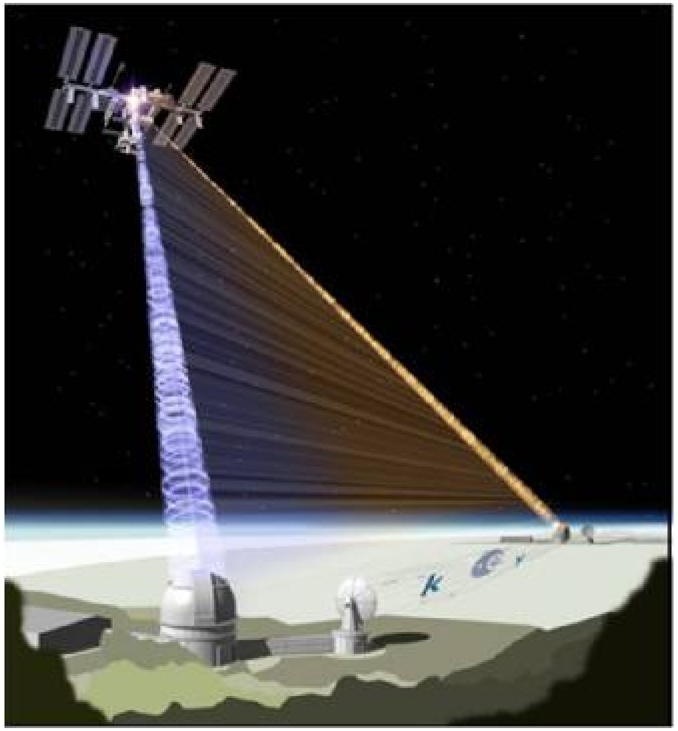
ã 经典搜寻：N 步

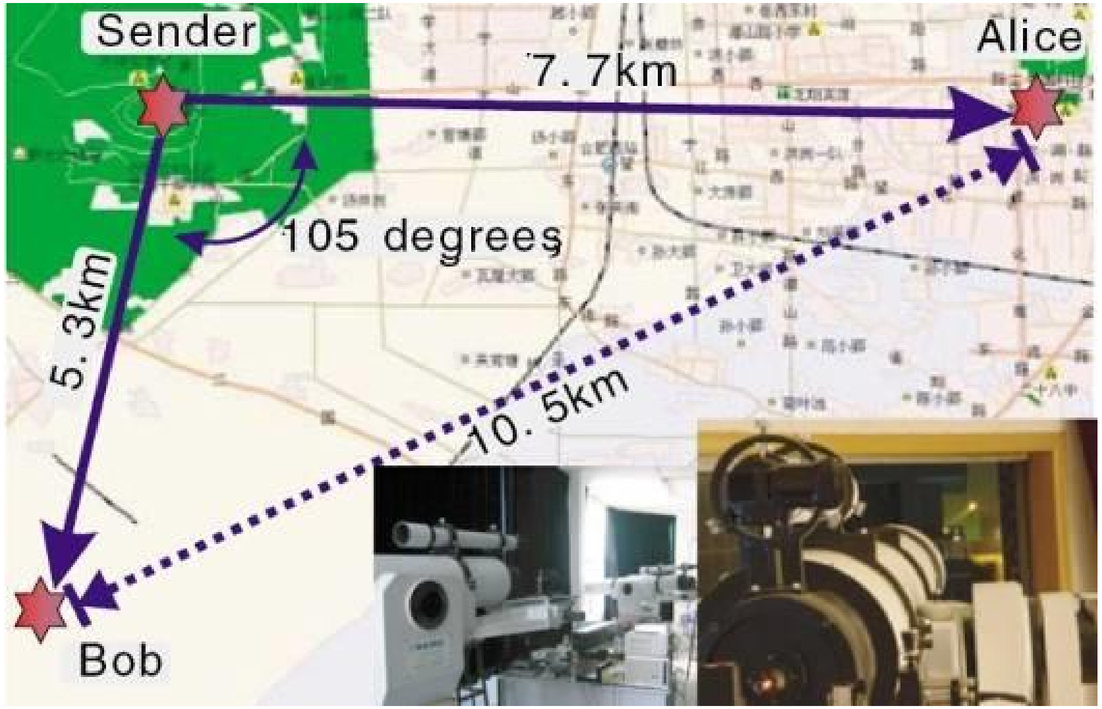
ã 量子搜寻：$N^{1/2}$ 步

ã 可破译DES密码：2^{56} 个数中搜寻密钥

1000年 $\Rightarrow$ 4分钟

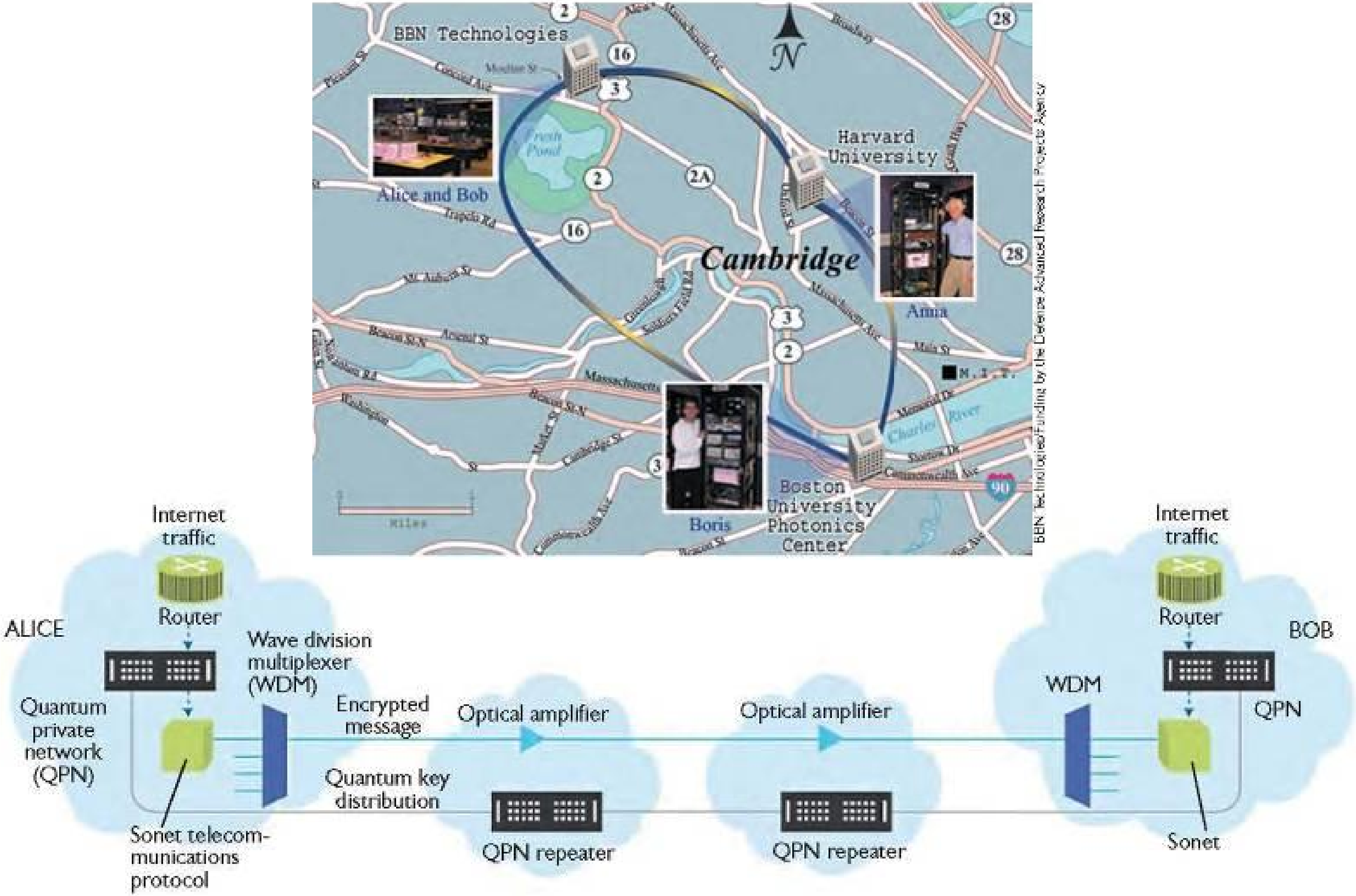
远程量子通信：
自由空间纠缠光子分发



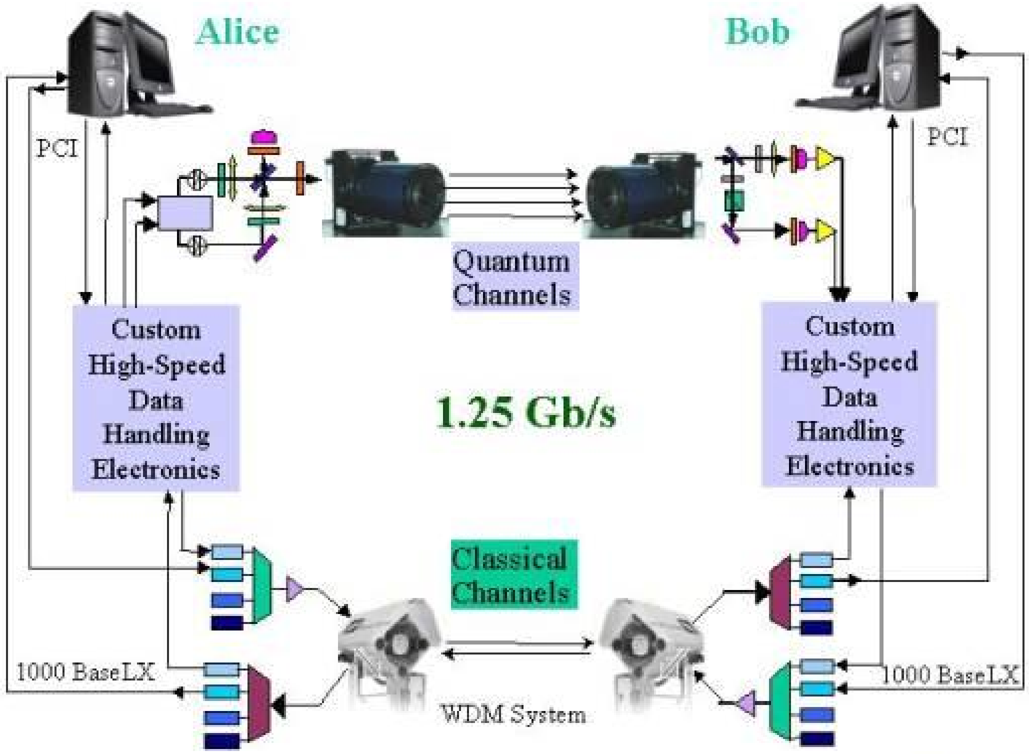


- 1km M. Aspelmeyer et al., Science 301, 621 (2003)
- 13km C.-Z. Peng et al., PRL 94, 150501 (2005)

The DARPA Quantum Network



NIST Quantum Communication Testbed



PCI interface high-speed electronics boards for Alice (left) and Bob (right).

1 Mbit/s over 4km (2006年)

SECOQC QKD网络拓扑和分布

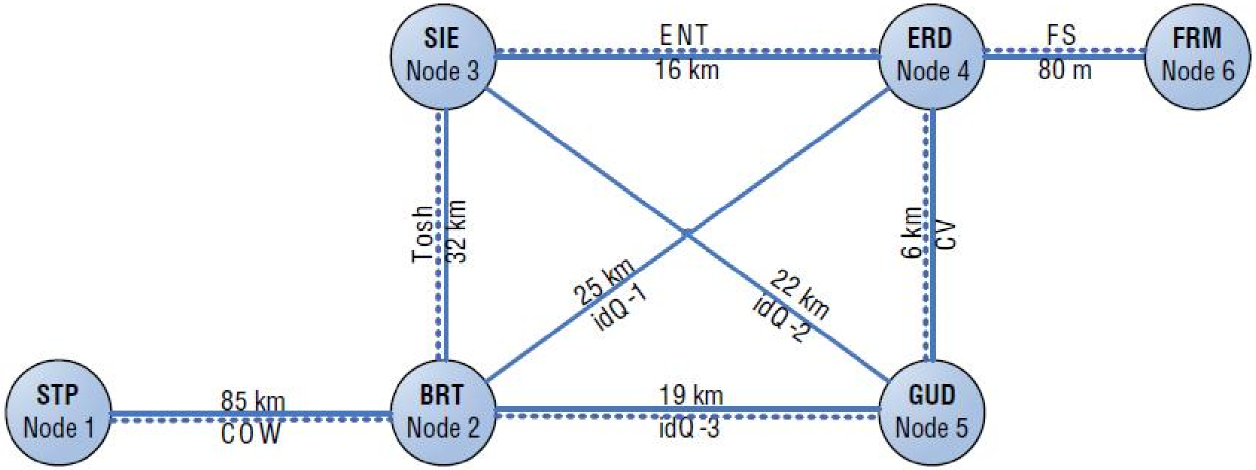


Figure 3. Satellite map with the locations of the nodes of the prototype.

SECOQC QKD节点组成

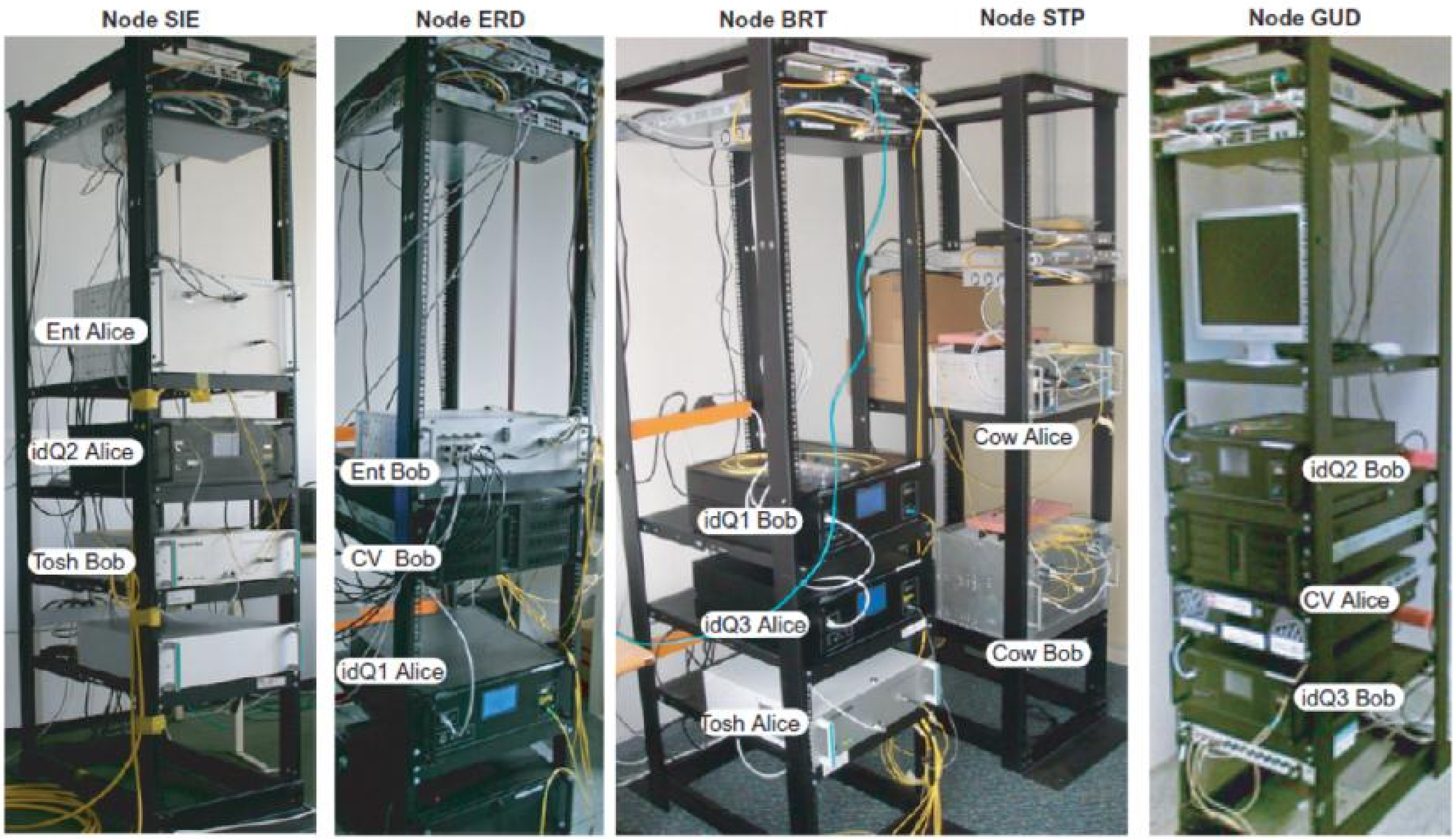
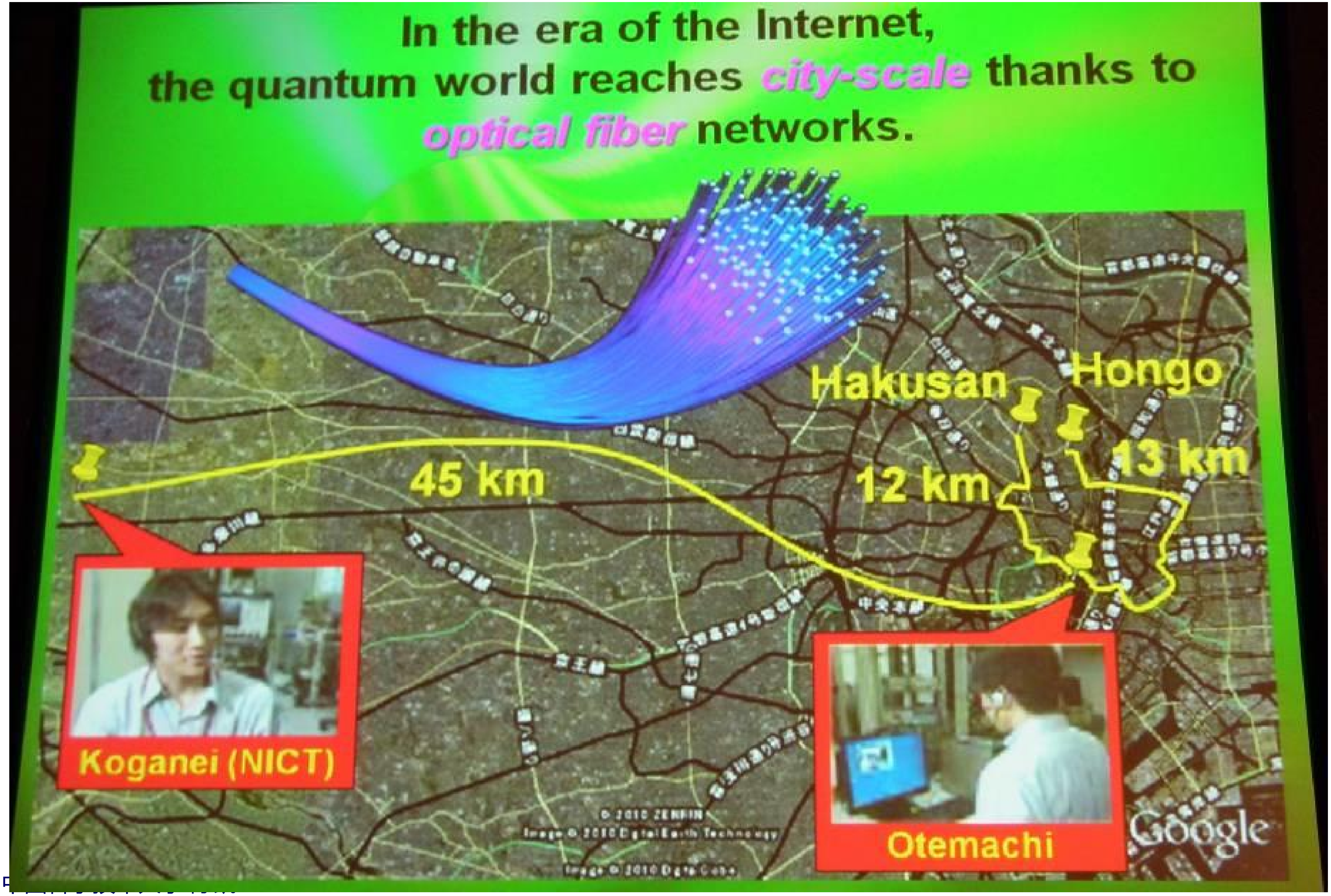


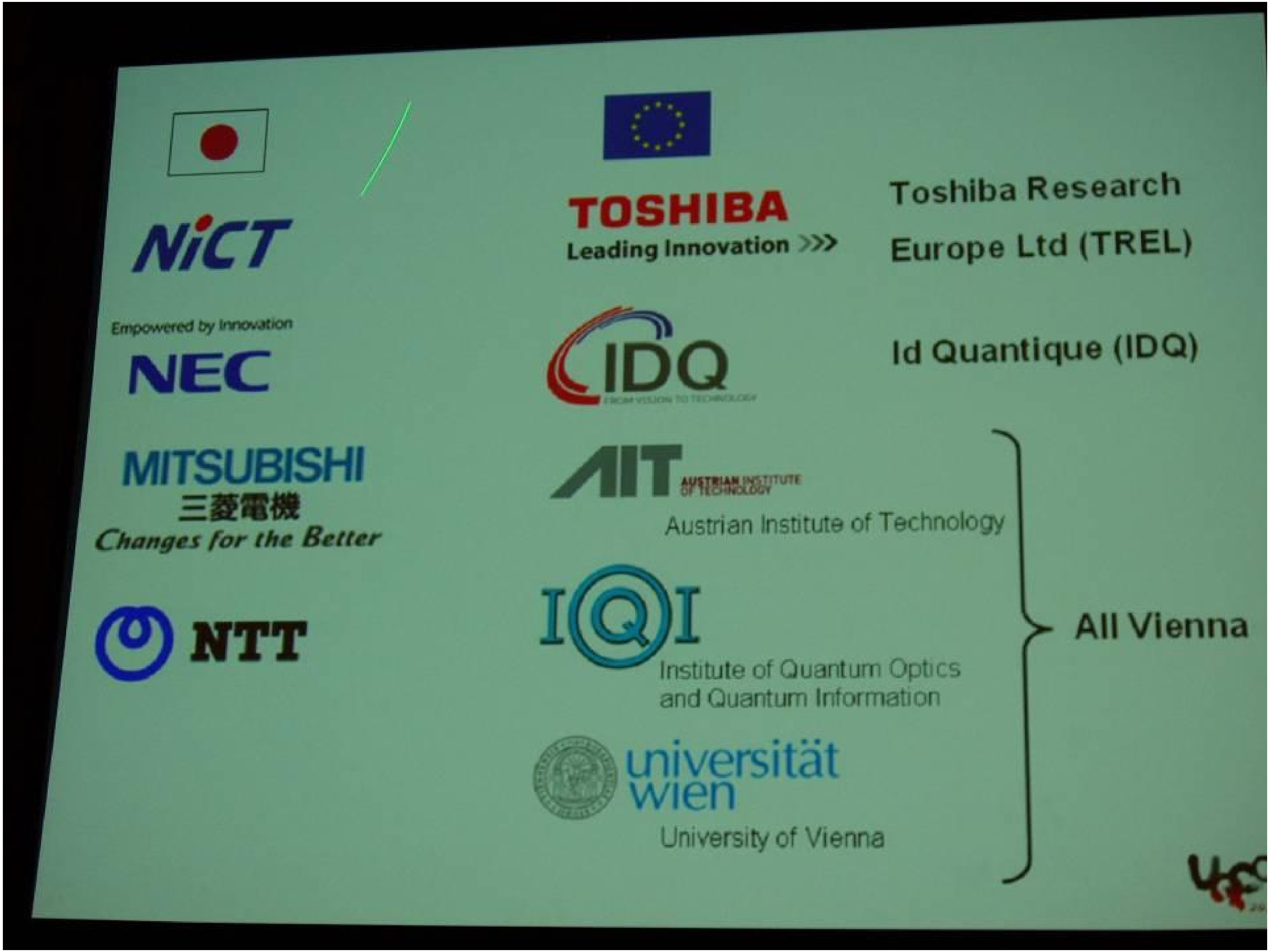
Figure 5. Photographs of the SECOQC network node racks.

成码率：0.6～10kbps (2008年)

Tokyo QKD network

(2010年)





NiCT
Empowered by Innovation
NEC
MITSUBISHI
三菱電機
Changes for the Better
NTT
TOSHIBA
Leading Innovation >>>
Toshiba Research
Europe Ltd (TREL)
IDQ
Id Quantique (IDQ)
AIT
Austrian Institute of Technology
IQI
Institute of Quantum Optics
and Quantum Information
universität
wien
University of Vienna
All Vienna

Tokyo QKD network网络架构

- 基于JGN2plus（Japan's Gigabit Network ）
- 星形结构

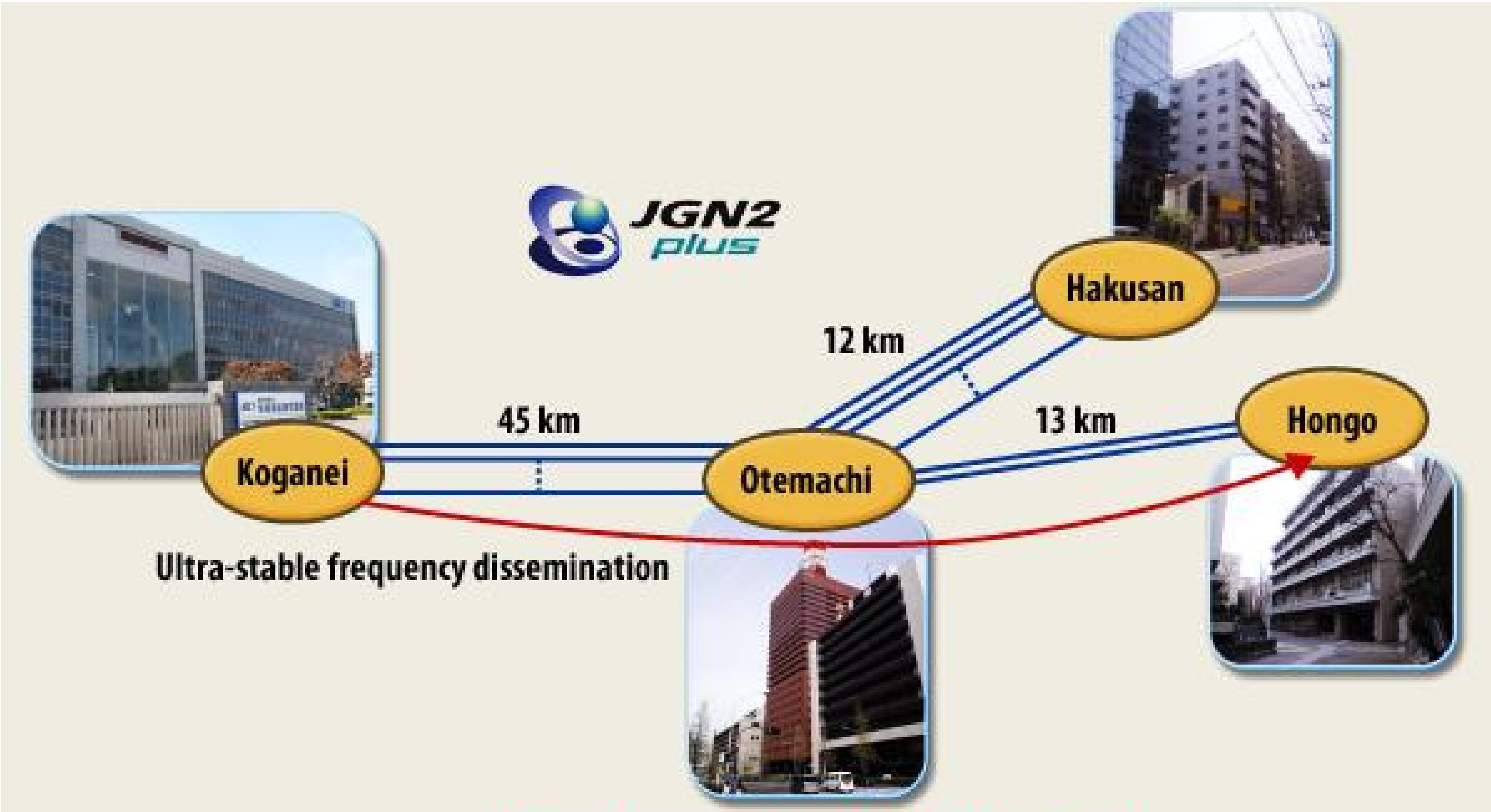
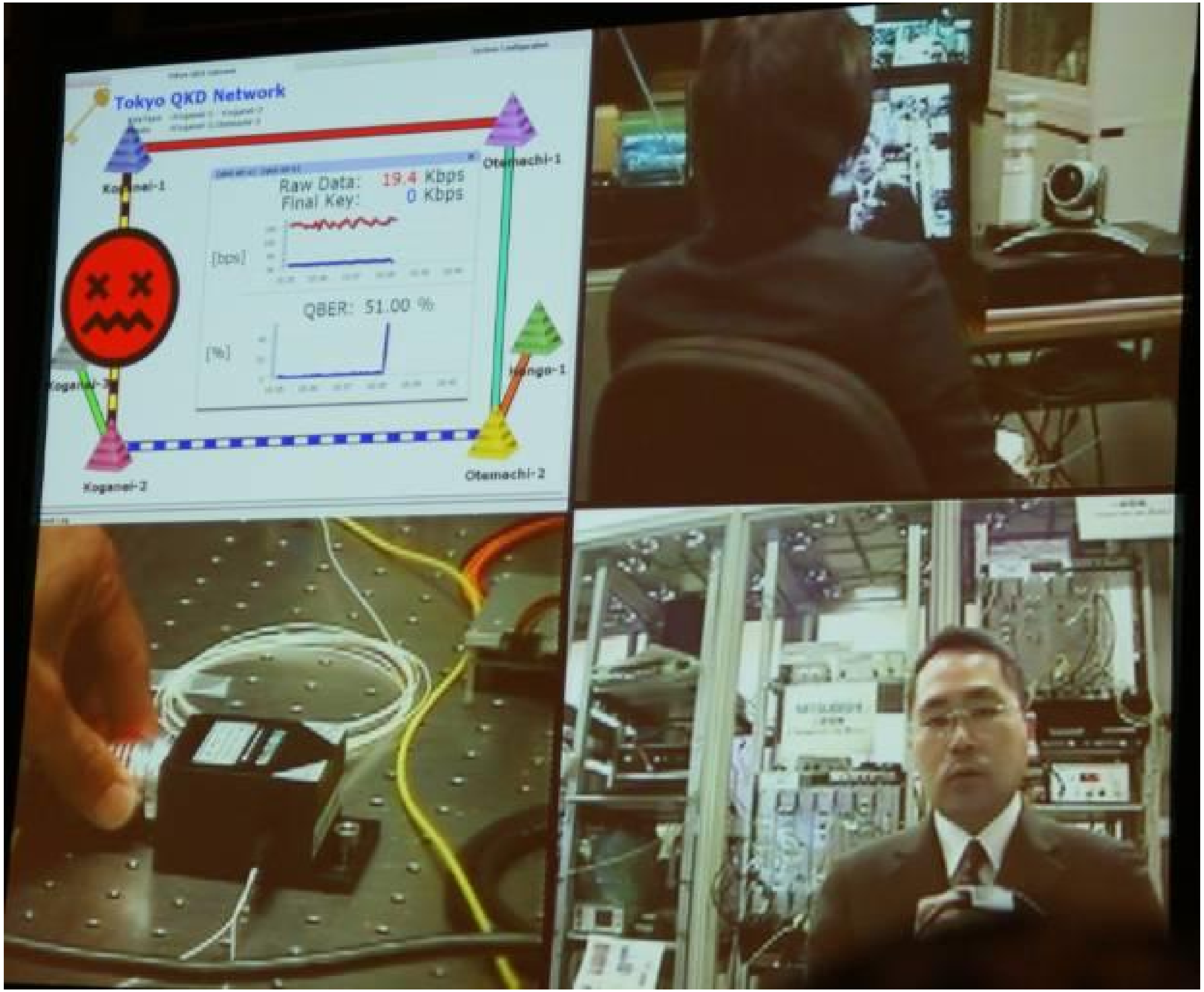
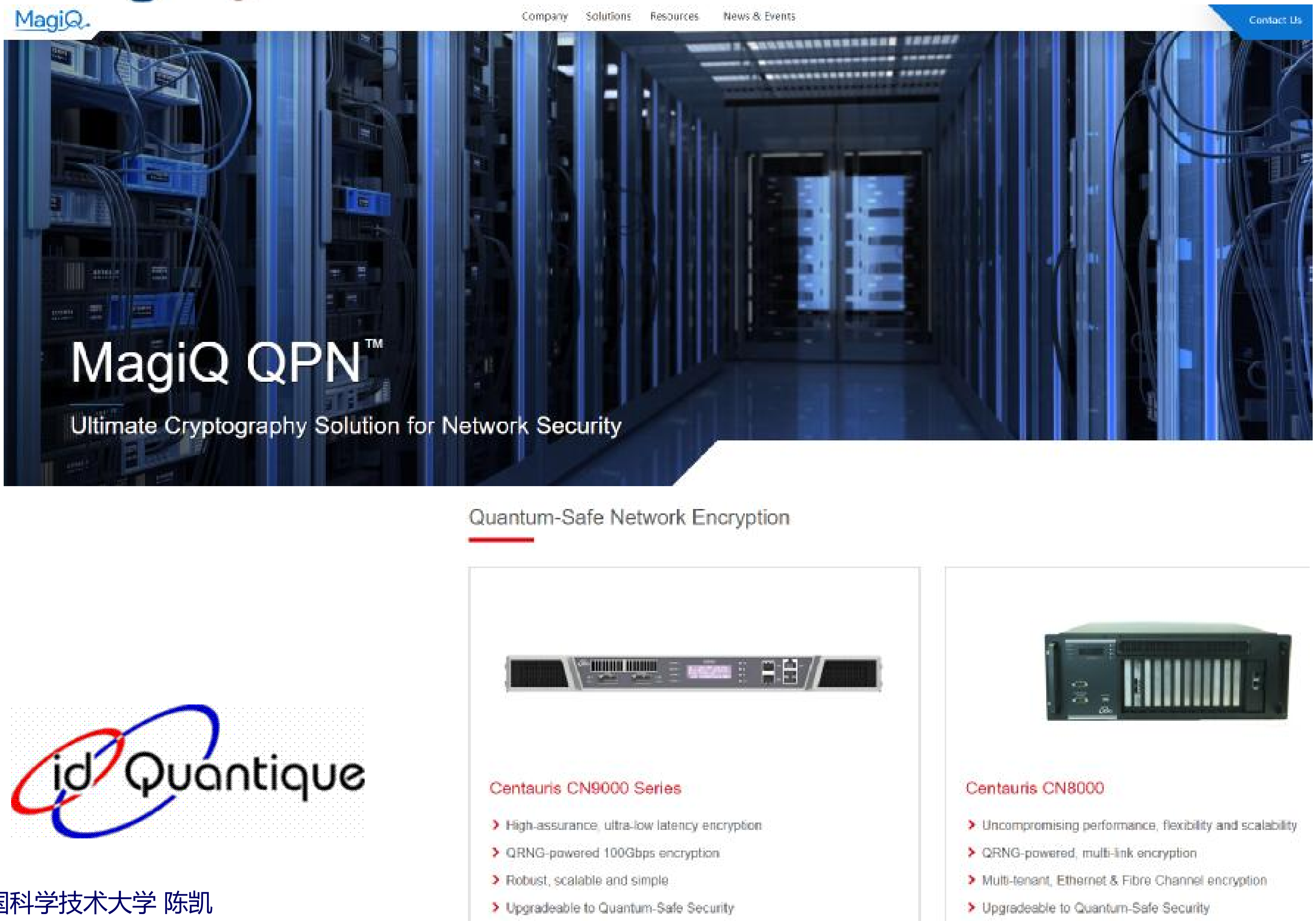


Fig. 1 Network Layout of the Tokyo QKD Network

Tokyo QKD Network视频会议演示

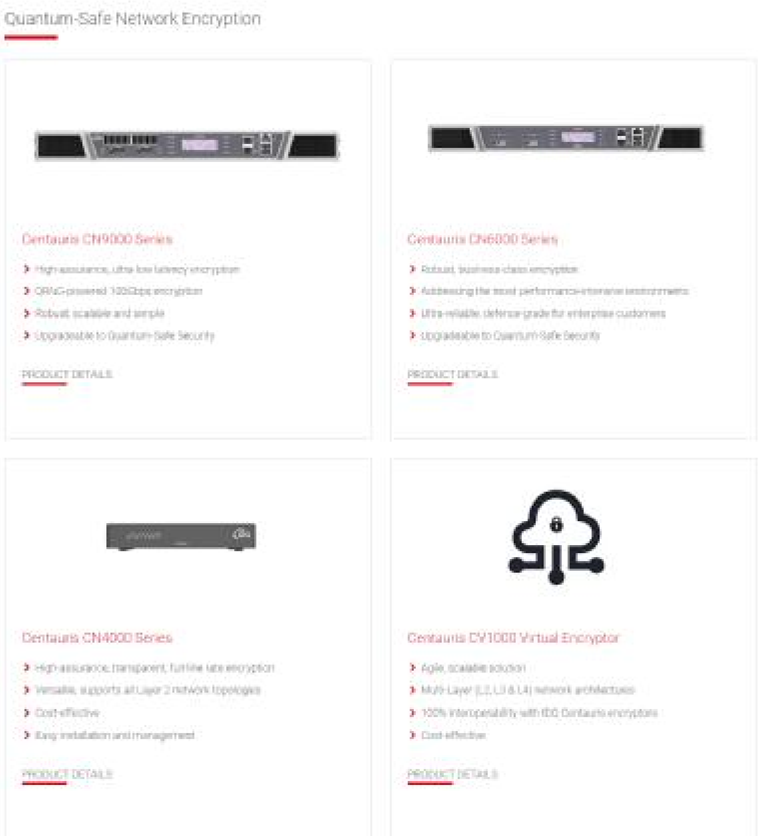


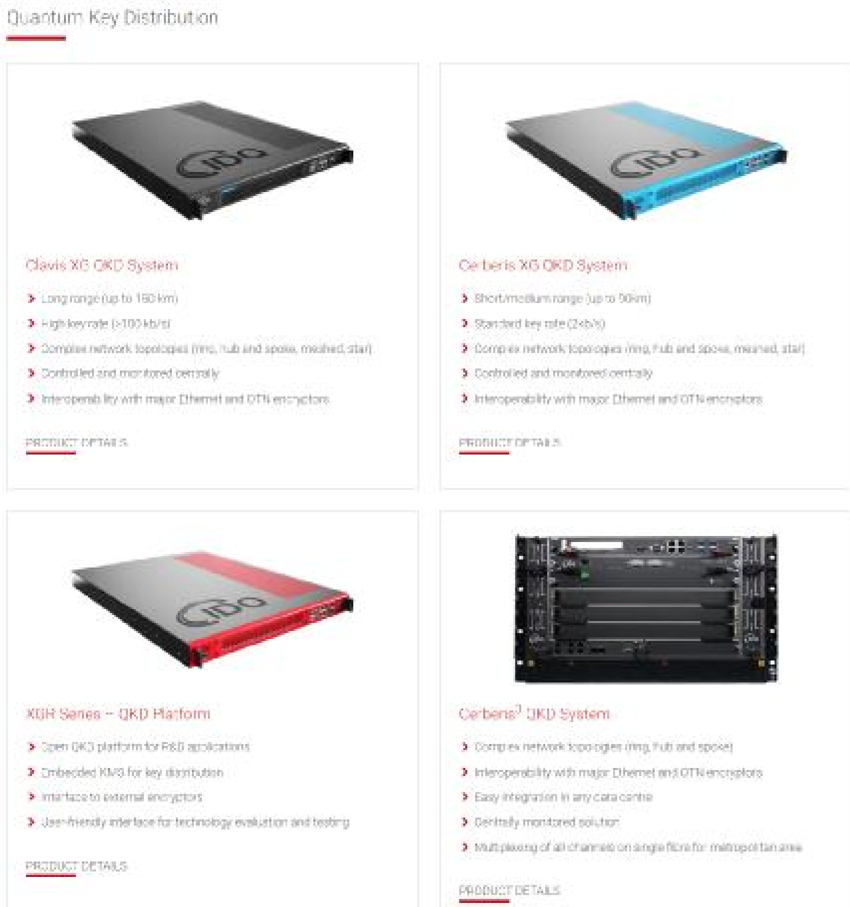
商用QKD产品


MagiQ
Company
Solutions
Resources
News & Events
Contact Us
MagiQ QPN™
Ultimate Cryptography Solution for Network Security
Quantum-Safe Network Encryption
Centauris CN9000 Series
High-assurance, ultra-low latency encryption
QRNG-powered 100Gbps encryption
Robust, scalable and simple
Upgradeable to Quantum-Safe Security
Centauris CN8000
Uncompromising performance, flexibility and scalability
QRNG-powered, multi-link encryption
Multi-tenant, Ethernet & Fibre Channel encryption
Upgradeable to Quantum-Safe Security

ID Quantique 产品

- id Quantique (IDQ) 在2001年建于Geneva
- 公司产品
  - Centauris Layer 2 Encryptors: High speed multi-protocol encryptors
  - Cerberis: A fast and secure solution of high speed encryption combined with quantum key distribution。典型的基于AES应用
  - Clavis^2: QKD for R&D Applications
  - 探测器，随机数发生器，短脉冲激光源等





ID Quantique

2010 FIFA 世界杯

Durban, South Africa – The first use of ultra secure quantum encryption at a world public event，基于AES 256

2019 SK Telecom Continues to Protect its 5G Network with Quantum Cryptography Technologies

SK Telecom Continues to Protect its 5G Network with Quantum Cryptography Technologies

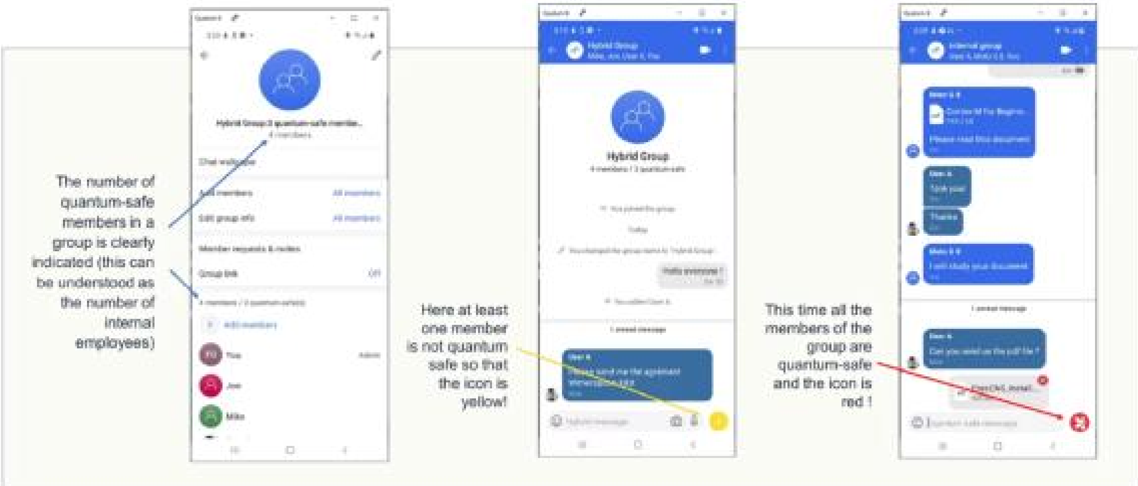
- SK Telecom applied Quantum Random Number Generator (QRNG) to the subscriber authentication center of its 5G network

- SK Telecom plans to apply Quantum Key Distribution (QKD) technology to the Seoul-Daejeon section of its LTE and 5G networks to prevent hacking and eavesdropping

- SK Telecom is playing a pivotal role in global standardization of QKD and QRNG technologies at ITU-T.

ID Quantique

Quantique and CryptoNext partner to deliver next-gen, quantum-safe messaging



The solution aims at enabling governments, enterprises and organizations of all types to manage sensitive communications for specific groups of people, such as executive teams, and/or specific projects.

Telefonica, Fortinet & IDQ demonstrate the first Quantum-Safe IPVPN connection suitable for managed datacentre interconnect

7th October 2021

Telefonica, Fortinet and IDQ have jointly demonstrated the first Quantum-Safe IPVPN connection suitable for offering a fully managed datacenter interconnection service.

DISCOVER MORE

MagiQ

- 1999建立于美国，目前设有Boston总部和纽约Office。
- 大致从2008年起建立了MagiQ Research Labs， 与US Army, DARPA, NASA以及与包括世界500强的多个公司进行联合研究。

MAGIQ QPN™ 8505

MagiQ


MagiQ
MagiQ QPN™
Ultimate Cryptography Solution for Network Security


DEFENSE
EXPLORE
TELECOMMUNICATIONS
EXPLORE
ENERGY EXPLORATION
EXPLORE
NETWORK SECURITY
MAGIQ QPN™
EXPLORE


Army
DARPA
JTRS
NASA
Navy

MagiQ

MagiQ QPN™: State of the Art Quantum Cryptography

MagiQ QPN is a market leading Quantum Cryptography solution that delivers advanced network security and fool-proof defense against the numerous cryptographic key distribution and management challenges.

Keys generated and disseminated using QPN quantum cryptography consist of truly random characters that are distributed based upon the laws of quantum mechanics, which guarantees that **keys cannot be intercepted during the key exchange session.** Therefore, MagiQ QPN provides security that will remain secure against future advances in algorithms, computational power, hardware design, and even quantum computing.

How it Works | **Who Needs It?** | Features & Benefits

Protecting **financial information** is one of the highest priorities of corporations and entities involved in financial management and securities exchange. With MagiQ QPN, financial organizations can secure their most critical communication links to prevent intrusion and data theft. MagiQ QPN supports a variety of network architectures and provides the cryptographic key exchange infrastructure to protect the information channels.

Storage area networks offer the promise of protecting corporate assets offsite by creating electronic copies of critical information for future retrieval. Encryption is used to protect the data link to the storage site (data in transit) and to protect the data at the site (data at rest). QPN guarantees high-security in storage area network applications to better meet customer security requirements now and for the future.

Military and Government

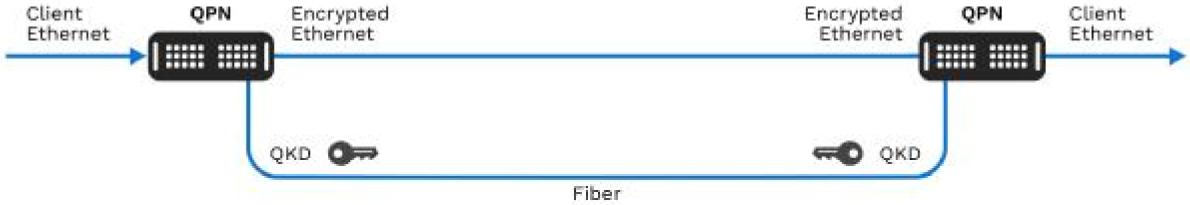
Hostile forces are a real and a continuous threat to government and military network security. QPN can safeguard against hackers and unwanted network security breaches by "trusted" insiders attempting to access highly-classified government and military information.

MagiQ QPN enables future-proof quantum security for other industries as well:

- R&D companies looking to protect trade secrets, intellectual properties, patents and business plans
- Voice and data service providers who need to secure confidential customer data and/or access to the network command channel
- Large Power Grid Providers open to terrorist or malicious hacking into the command and control channel interfaces

How it Works | Who Needs It? | Features & Benefits

The security of quantum cryptography lies in its ability to exchange the encryption keys with absolute security – Quantum Key Distribution. By sending the key bits encoded at the single photon level on a photon-by-photon basis, quantum mechanics guarantees that the act of an eavesdropper observing a photon irretrievably changes the information encoded on that photon. Therefore, the eavesdropper can neither copy nor clone, nor read the information encoded on the photon without modifying it; eavesdropping is instantly detected making this key exchange uncompromisingly secure.



QPN implements the BB84 protocol, invented by Bennet and Brassard in 1984. This protocol assumes that the sender and recipient share an optical link (fiber) and a classical (non-quantum) unsecured communication channel, for example, a standard internet link.

QPN sends photons over the fiber to create the secure keys between two QPN stations. A photon is an elementary light particle that has measurable properties, like polarization, which can be 'up' or 'down'. These can be used to encode and transmit a value of a bit from one QPN station to the other. The transmitting QPN station uses a truly random number generator to come up with the value of the bit encoded on the photon.

The security of the BB84 protocol is based on the fundamental Heisenberg Uncertainty Principle, that states that observing a photon (eavesdropping) does change its properties, i.e., in the presence of eavesdropping, the values of the received bits will differ from the values of the bits sent. This fundamental principal eliminates the ability of any eavesdropper to hide his/her 'footprints on the photon.

3节点光量子电话网络

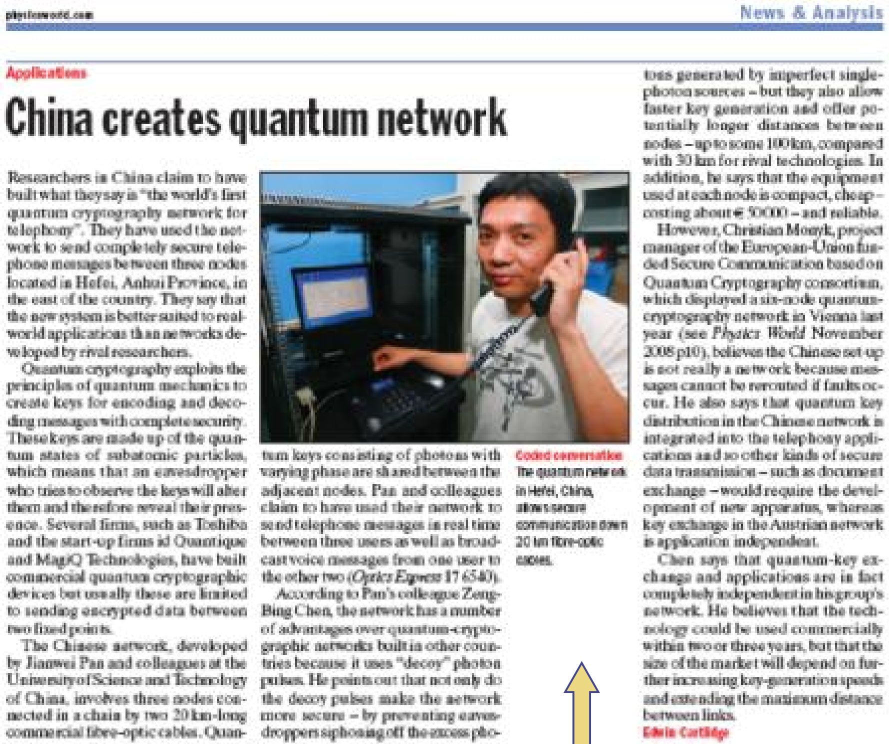
- 任意两节点间的量子电话
- 任意节点对于另外两个节点的加密广播

Quantum Phone Calls

Certain conversations or transactio[illegible] meant to be private. Yet despite th[illegible] of digital communication in one fo[illegible] mechanics closes that loophole [illegible] Sharing quantum mechanically–en[illegible] photons can provide a secure key [illegible] to encrypt and send a message, sa[illegible] knowledge that the message cannot be opened by an eavesdropper, at least not without alerting you to the breach. Chen *et al.* demonstrate a quantum key distribution protocol in a real-world application scenario, with the quantum [illegible]uted over a network consisting of [illegible]ons linked by 20 km of commercial [illegible]er. The generated keys can be used [illegible]ely in the context of encrypted real-[illegible]elephone conversations between the separated stations. With such a demonstration, quantum privacy in your own home may not be a too distant prospect. — ISO

有了这样的演示，量子隐私进入千家万户不会是很遥远的未来。

*Science*的报道



physicsworld.com

News & Analysis

Applications

China creates quantum network

Researchers in China claim to have built what they say is "the world's first quantum cryptography network for telephony". They have used the network to send completely secure telephone messages between three nodes located in Hefei, Anhui Province, in the east of the country. They say that the new system is better suited to real-world applications than networks developed by rival researchers.

Quantum cryptography exploits the principles of quantum mechanics to create keys for encoding and decoding messages with complete security. These keys are made up of the quantum states of subatomic particles, which means that an eavesdropper who tries to observe the keys will alter them and therefore reveal their presence. Several firms, such as Toshiba and the start-up firms id Quantique and MagiQ Technologies, have built commercial quantum cryptographic devices but usually these are limited to sending encrypted data between two fixed points.

The Chinese network, developed by Jianwei Pan and colleagues at the University of Science and Technology of China, involves three nodes connected in a chain by two 20 km-long commercial fibre-optic cables. Quantum keys consisting of photons with varying phase are shared between the adjacent nodes. Pan and colleagues claim to have used their network to send telephone messages in real time between three users as well as broadcast voice messages from one user to the other two (*Optics Express* 17 6540).

According to Pan's colleague Zeng-Bing Chen, the network has a number of advantages over quantum-cryptographic networks built in other countries because it uses "decoy" photon pulses. He points out that not only do the decoy pulses make the network more secure – by preventing eavesdroppers siphoning off the excess photons generated by imperfect single-photon sources – but they also allow faster key generation and offer potentially longer distances between nodes – up to some 100 km, compared with 30 km for rival technologies. In addition, he says that the equipment used at each node is compact, cheap – costing about €5000 – and reliable.

However, Christian Monyk, project manager of the European-Union funded Secure Communication based on Quantum Cryptography consortium, which displayed a six-node quantum-cryptography network in Vienna last year (see *Physics World* November 2008 p10), believes the Chinese set-up is not really a network because messages cannot be rerouted if faults occur. He also says that quantum key distribution in the Chinese network is integrated into the telephony applications and so other kinds of secure data transmission – such as document exchange – would require the development of new apparatus, whereas key exchange in the Austrian network is application independent.

Chen says that quantum-key exchange and applications are in fact completely independent in his group's network. He believes that the technology could be used commercially within two or three years, but that the size of the market will depend on further increasing key-generation speeds and extending the maximum distance between links.

Edwin Cartlidge

Coded conversation The quantum network in Hefei, China, allows secure communication down 20 km fibre-optic cables.

*Physics World*的报道

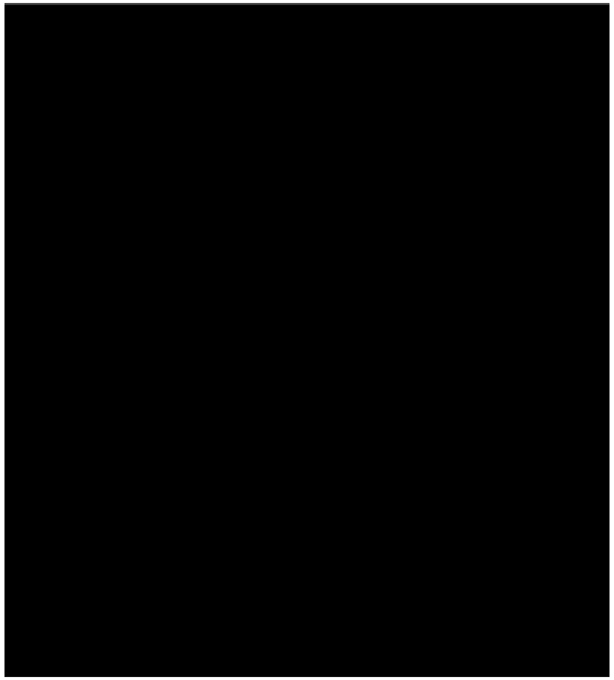
T.-Y. Chen *et al.*, *Optics Express* Vol. 17, Iss. 8, pp. 6540–6549 (2009).

5节点星型量子密钥分配网络系统

全通型量子通信网络

Chen *et al.*, Optics Express 18, 27217 (2010)

系统集成

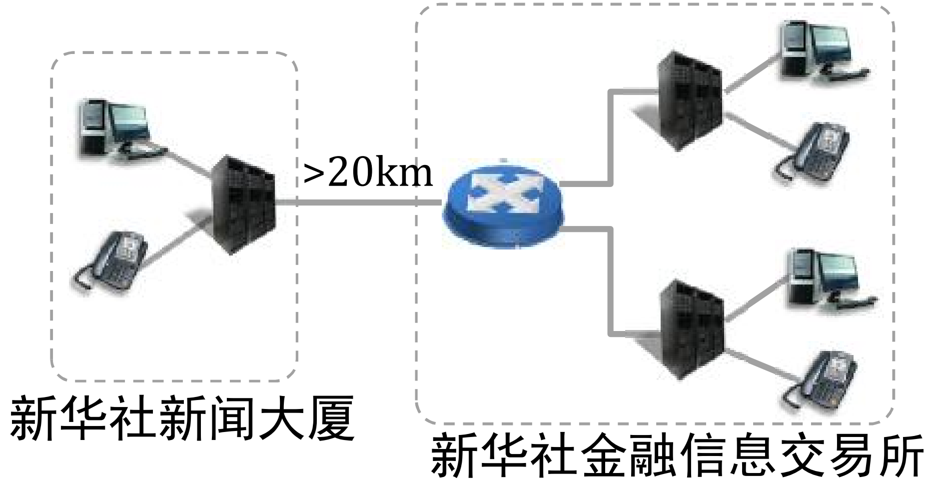


实用化城域量子通信网络

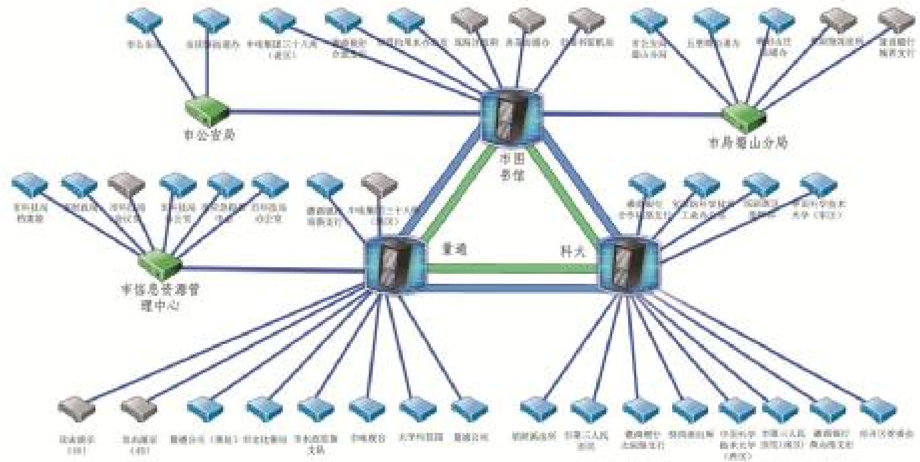
合肥全通型城域量子通信网络

Chen *et al.*, Opt. Express 17, 6540 (2009)

Chen *et al.*, Opt. Express 18, 27217 (2010)



金融信息量子通信验证网(2012)



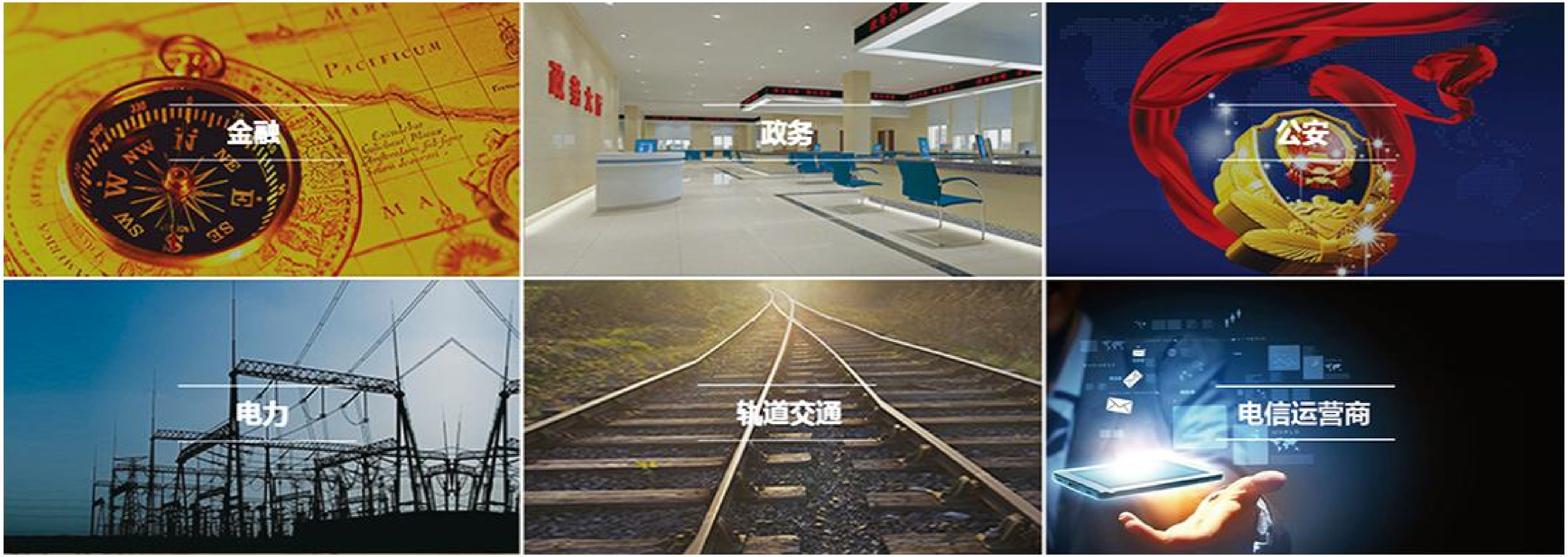
合肥城域量子通信试验示范网
(46个节点, 2012年)

量子通信产业化


我 们 的 征 程 是 星辰大海
科大国盾量子技术股份有限公司
用量子技术保护每一个比特 | Quantum Secures Every Bit


问天量子
首页
公司介绍
产品中心
解决方案
新闻中心
人才招聘
联系我们
量子技术
问天量子 服务安全
专业从事量子信息安全服务

科大国盾量子技术股份有限公司
（QuantumCTek Co., Ltd.）

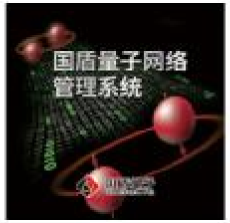


科大国盾量子技术股份有限公司
（QuantumCTek Co., Ltd.）

量子保密通信网络核心设备

量子安全应用产品

管控软件



核心组件

科学与科研仪器

大容量商用化超长距量子共纤传输应用

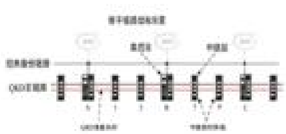
北京农商银行城域环网量子技术应用

交通银行企业网银用例建设

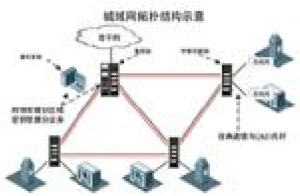
网商银行云上量子加密通信案例

工商银行异地数据千公里级量子加密传输应用

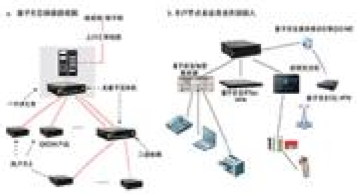
骨干网应用



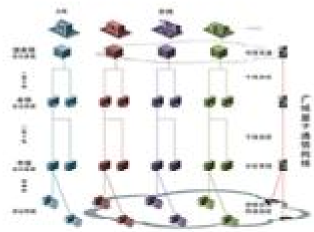
城域网应用



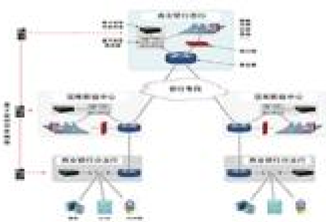
局域网应用



政务应用



金融应用



国盾量子


QuantumCTek
用量子技术保护每一个比特
Quantum Secures Every Bit
开拓者 实践者 引领者


国盾量子
QuantumCTek
股票简称：国盾量子
股票代码：688027
不忘初心 光量未来
科大国盾量子技术股份有限公司首次公开发行股票并在科创板上市仪式
保荐机构（主承销商）：国元证券股份有限公司
二〇二〇年七月九日

科大国盾量子技术股份有限公司

量子安全加密路由器

量子安全加密路由器是结合量子保密通信技术与经典通信技术的高保密量子安全产品。该产品采用量子保密通信技术，结合设计理念和模块化可扩展的平台，凭借“安全可靠、性能强劲、一机多能、弹性扩展、轻松易维、绿色节能”六大特性，满足用户当前和未来各种业务部署的需求，为实现信息高安全传送提供智能而有弹性的设备平台。

量子安全SSL VPN

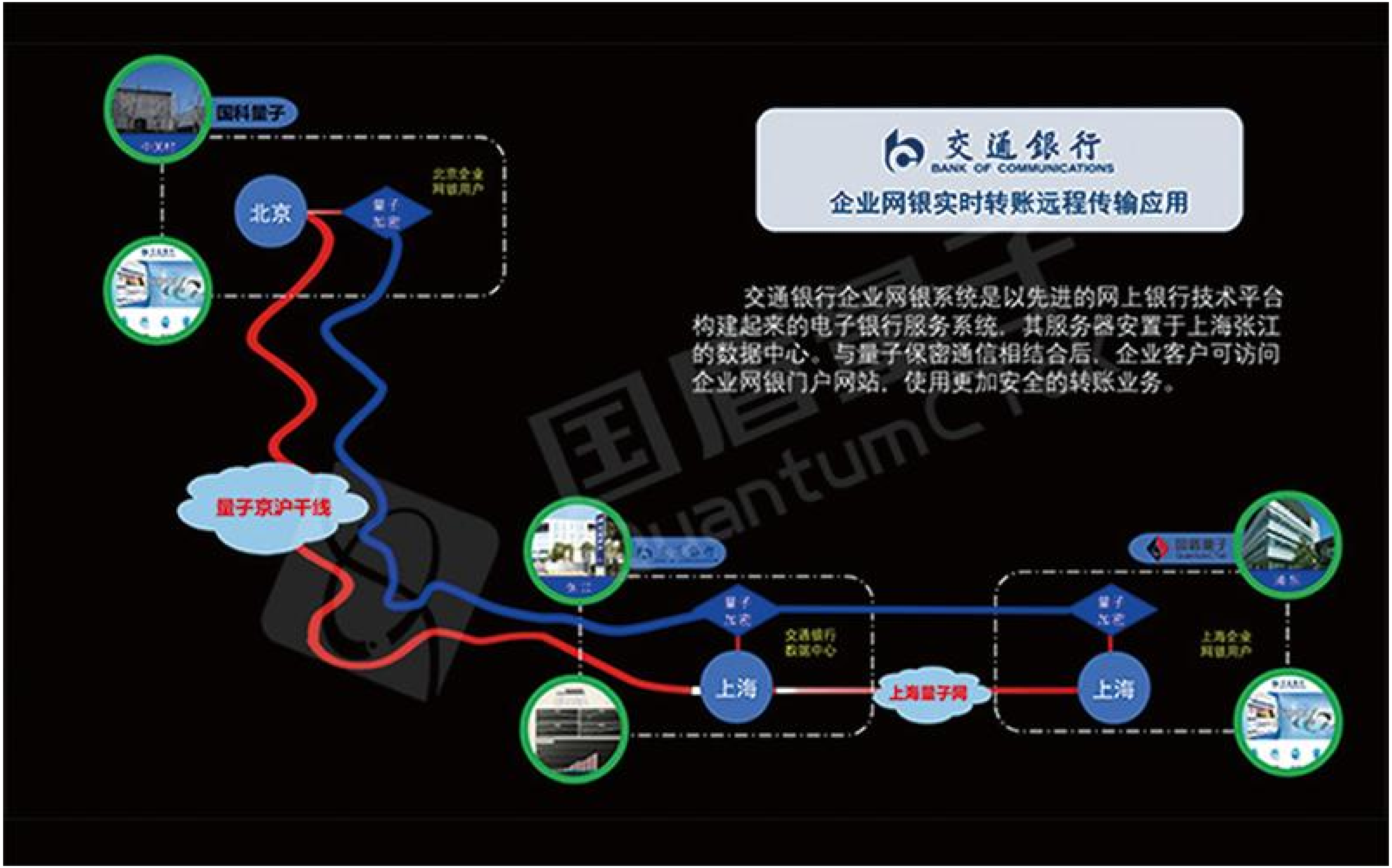
量子安全SSL VPN产品是结合量子保密通信技术与SSL VPN技术的一款高保密量子安全产品，该产品为科大国盾量子携手深信服科技推出的量子安全SSL VPN产品，具备量子密钥保护、全面安全、快速接入等特性。

ez-Q™ Engine超导量子计算操控系统

中国科学技术大学 陈凯

科大国盾量子技术股份有限公司
（QuantumCTek Co., Ltd.）

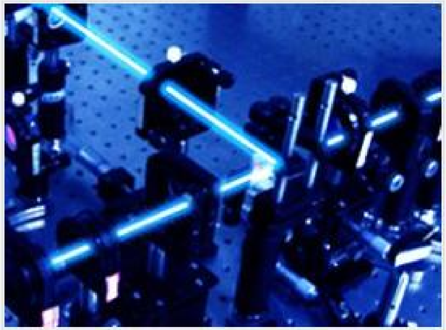
科大国盾量子技术股份有限公司
（QuantumCTek Co., Ltd.）



安徽问天量子科技股份有限公司

量子密钥分配终端

量子密码通信应用设备



量子密钥分配实验系统

激光器

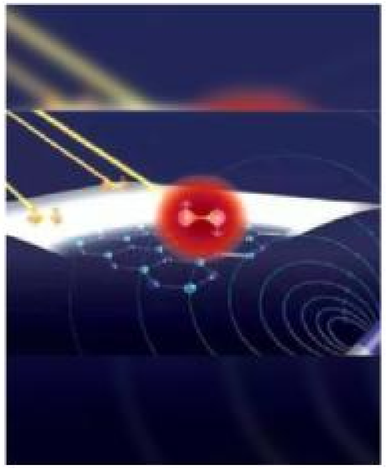
中国科学技术大学 陈凯

国仪量子技术有限公司

量子测控系统解决方案
AWG | ASG | DAQ | TDC
了解详情

让自主高端科学仪器
更好地赋能各行各业
高 瓴 领 投 · 国 仪 量 子 完 成 数 亿 元 B 轮 融 资

国仪量子技术有限公司



高保真度量子控制

利用微波脉冲可以控制NV色心自旋态的翻转，从而构成量子逻辑门。通过精巧的设计脉冲序列，可以使得单比特量子逻辑门操作保真度达到99.99%。这是目前单比特量子逻辑门保真度的记录，并且达到了容错阈值。

推荐产品：量子钻石单自旋谱仪

量子算法

量子算法利用量子力学许多基本特性，如相干叠加性、并行性、纠缠性、测量坍缩等等，这些纯物理性质为计算效率的提高带来极大帮助，形成一种崭新的计算模式——量子算法。利用NV色心体系，演示了D-J算法，大数分解算法等，向实现室温量子计算机迈出了重要一步。

推荐产品：量子钻石单自旋谱仪

量子钻石原子力显微镜

基于NV色心和AFM扫描成像技术的量子精密测量仪器

量子钻石单自旋谱仪

基于NV色心的以自旋磁共振为原理的量子实验平台

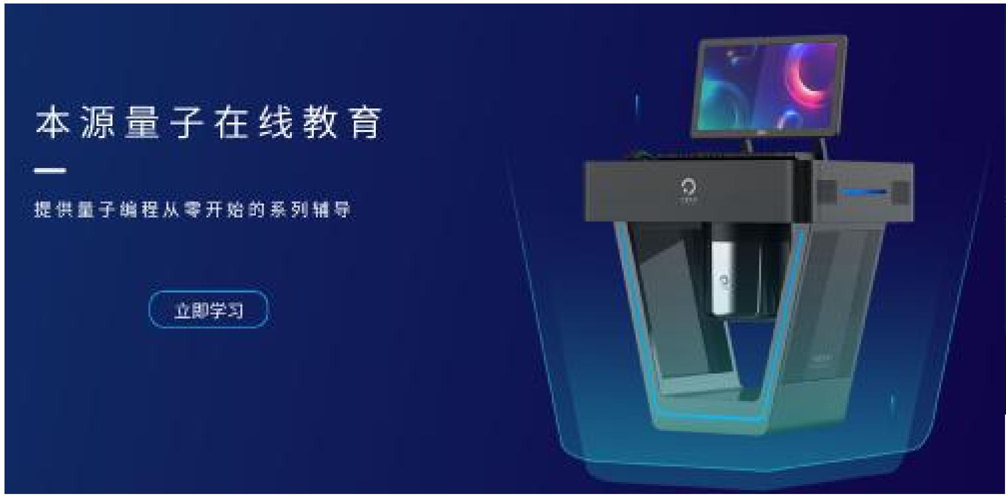
金刚石量子计算教学机

基于NV 色心自旋磁共振为原理的量子教学仪器

任意波形发生器

拥有四个相互独立的波形输出的高性能任意波形发生器

合肥本源量子计算科技有限责任公司

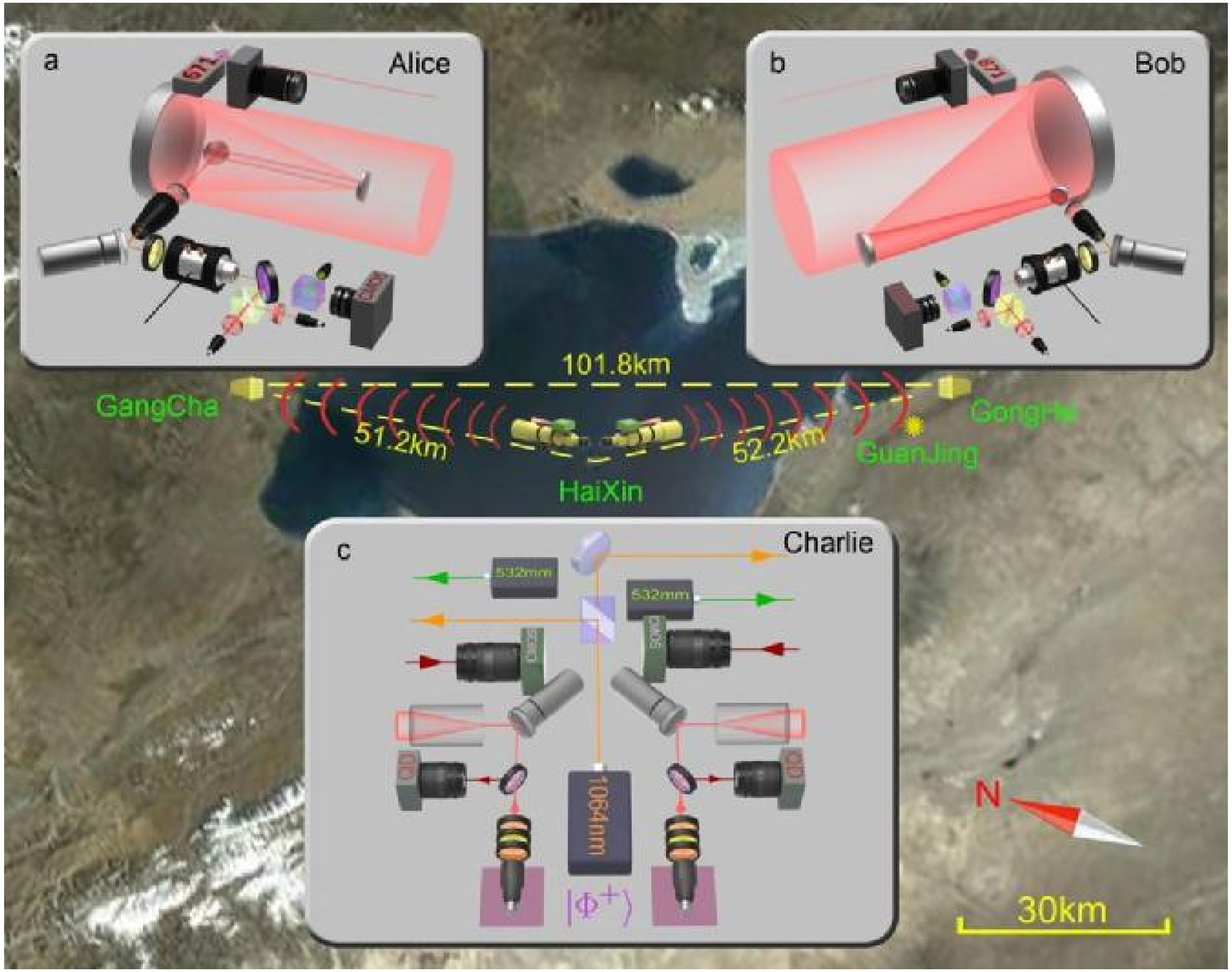


中国科学技术大学 陈凯

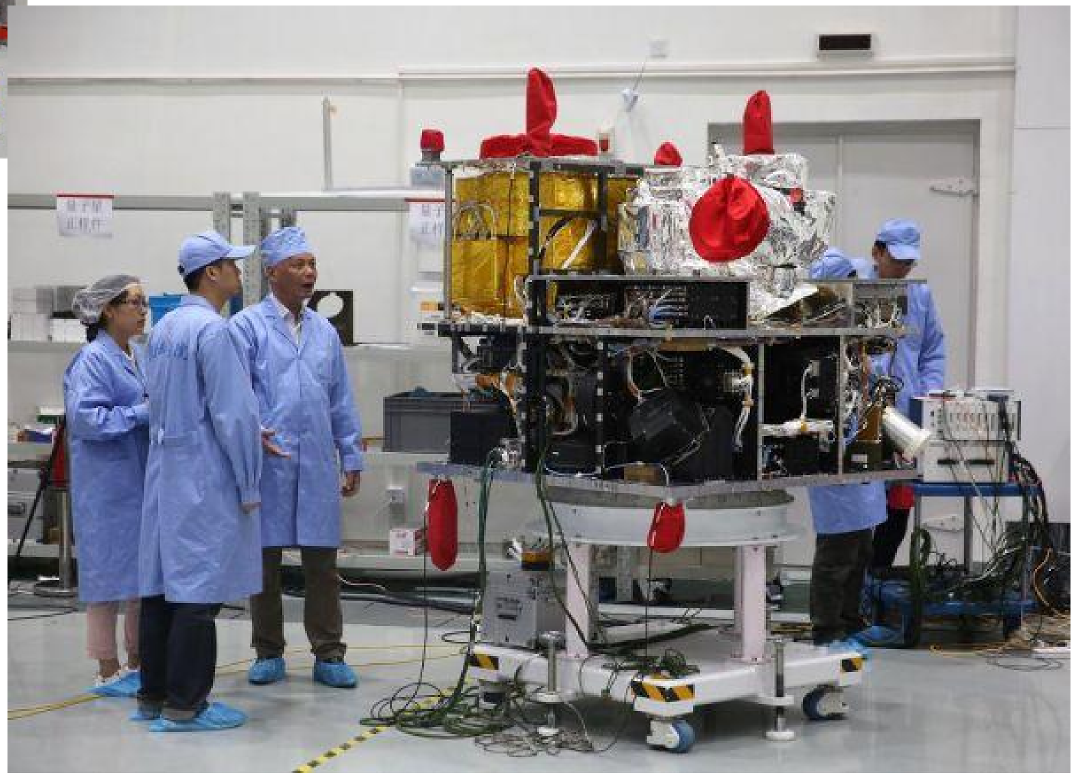
Free-Space Quantum Communication

Free-space quantum entanglement distribution (over 100km)

Yin *et al*., **Nature** 488, 185 (2012)



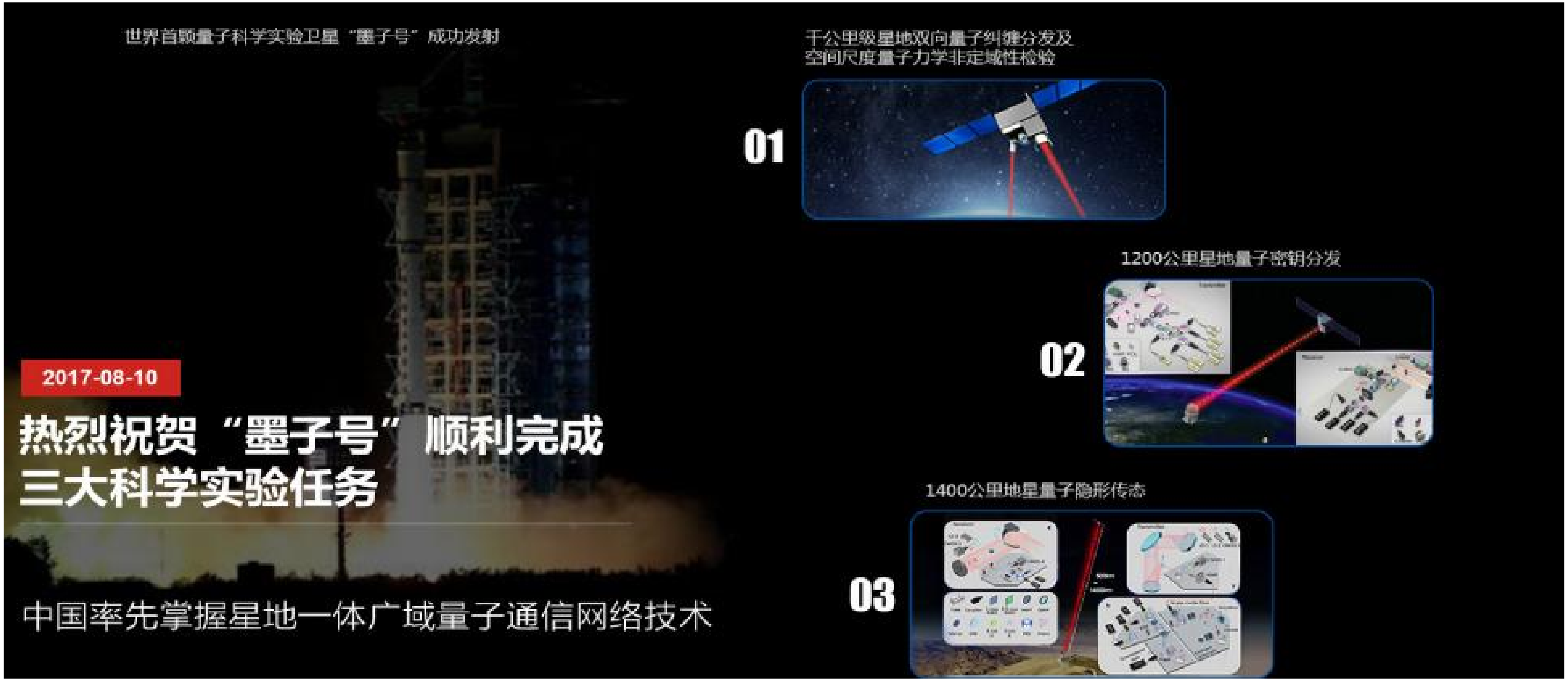
世界首颗量子卫星



“墨子号”量子卫星与地面站通信试验照片公布

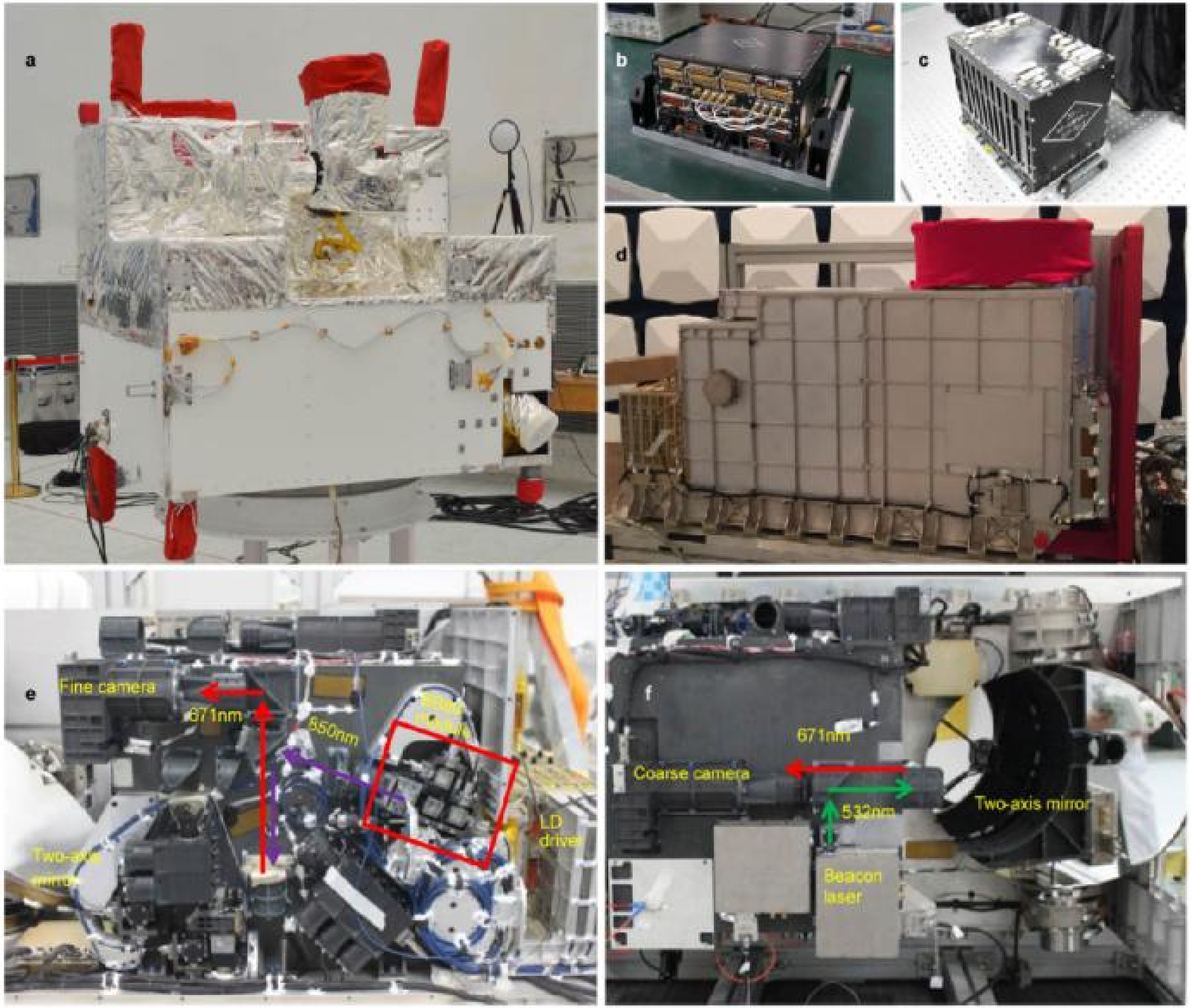
中国科学技术大学 陈凯

“墨子号”量子卫星与地面站量子通信



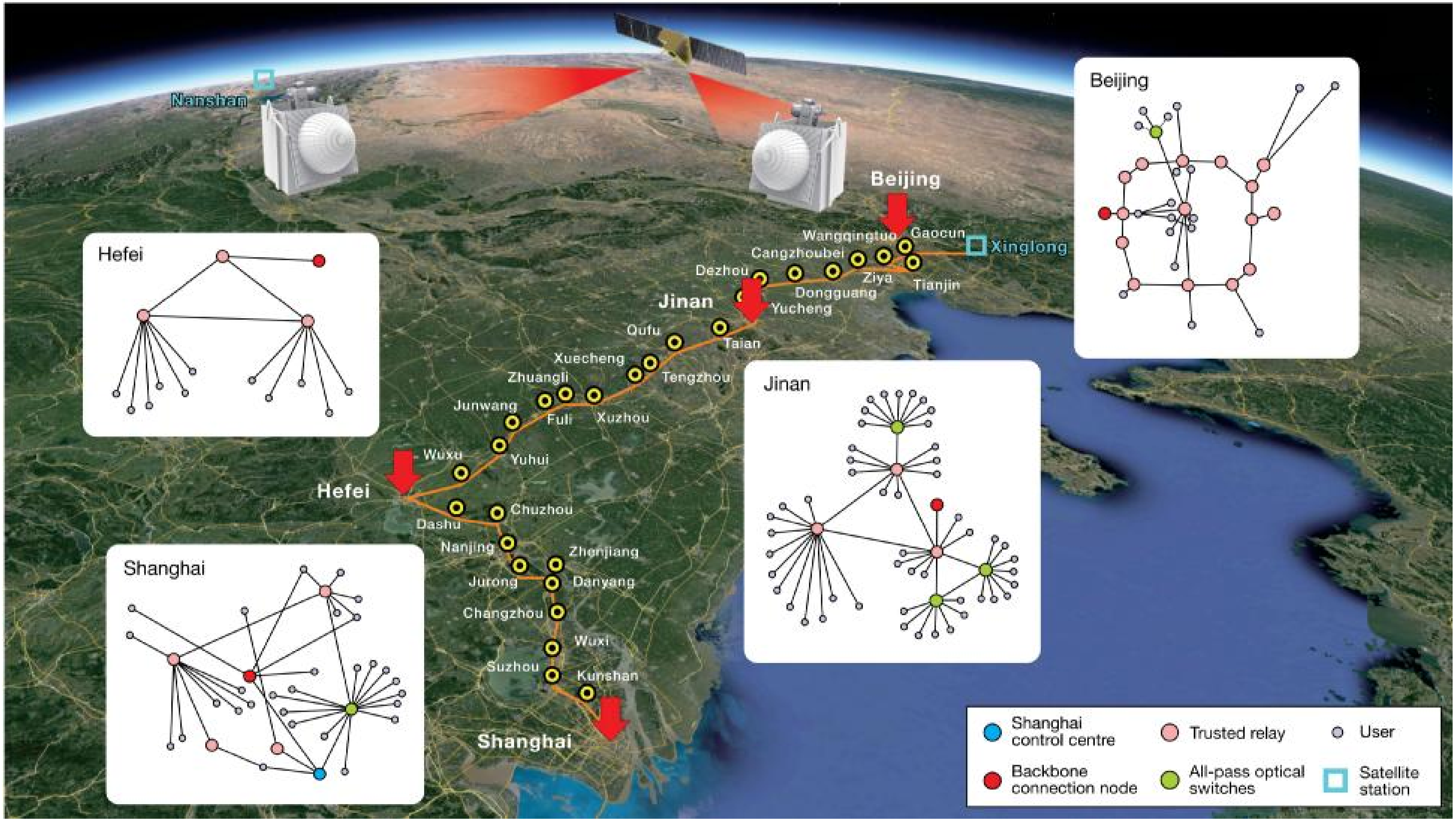
摘自国盾量子新闻

“墨子号”量子卫星与地面站装置图



Extended Data Figure 2 | The Micius satellite and the payloads. **a**, A full view of the Micius satellite before being assembled into the rocket. **b**, The experimental control box. **c**, The APT control box. **d**, The optical transmitter. **e**, Left side view of the optical transmitter optics head. **f**, Top side view of the optical transmitter optics head.

跨越4600公里的天地一体化量子通信网络



Y.A. Chen *et al.*, Nature 589, 214-219 (2021)

自由空间量子光学实验

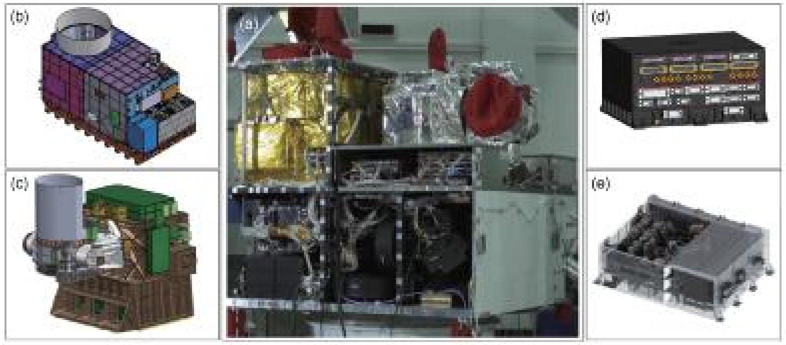


FIG. 18. Full view of the Micius satellite and the main payloads. (a) Photograph of the Micius satellite prior to launch. (b) Transmitter 1 for QKD, entanglement distribution, and teleportation. (c) Transmitter 2, especially designed for entanglement distribution. (d) Experimental control box. (e) Entangled-photon source.

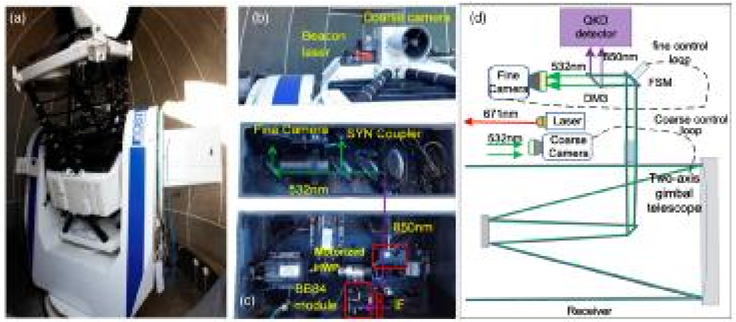


FIG. 23. Typical receiving ground station for the Micius satellite. (a) Two-axis gimbal telescope. (b) Beacon laser and coarse camera. (c) One of the two layers of the optical receiver box. (d) Typical optical design of the receiver including the receiving telescope, the ATP system, and the QKD-detection module. From Liao *et al.*, 2017a.

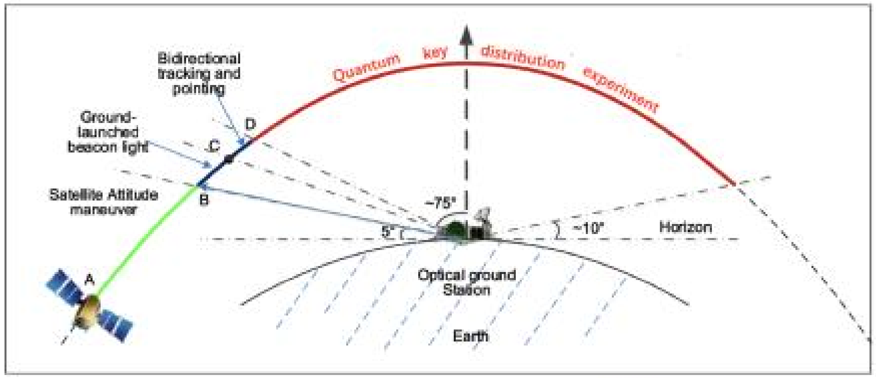


FIG. 27. Tracking and QKD processes during an orbit. From Liao *et al.*, 2017a.

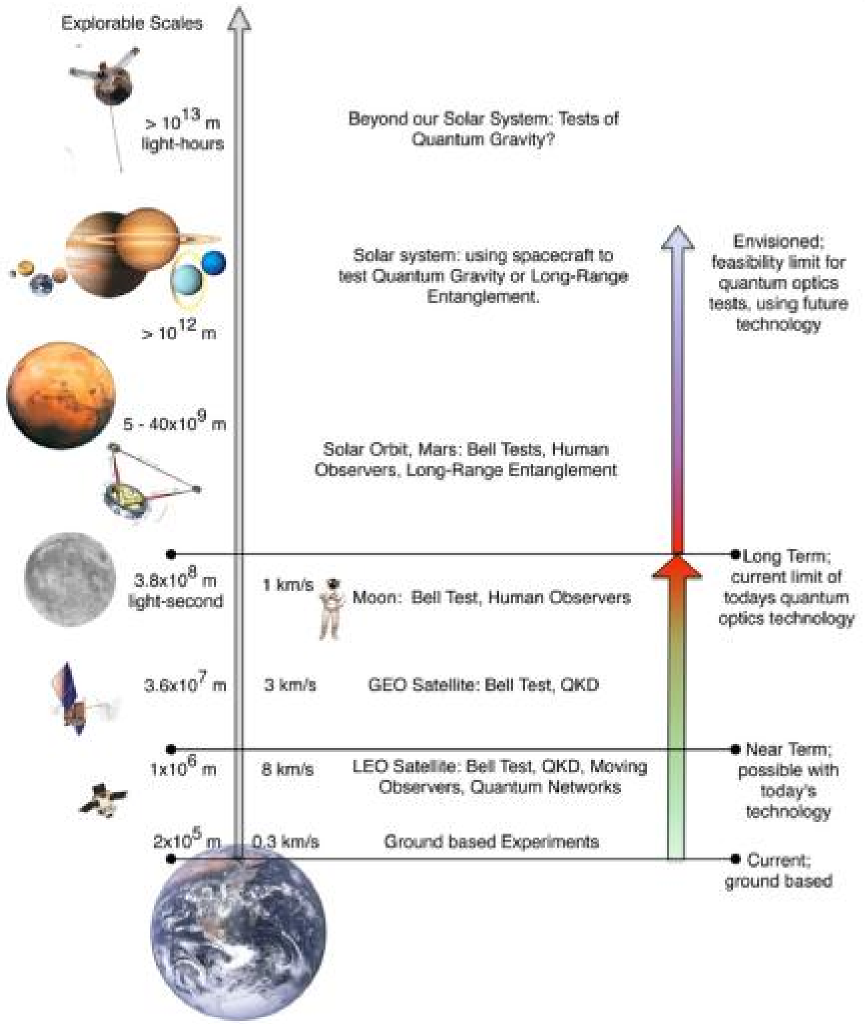


Figure 1. Overview of the distance and velocity scales achievable in a space environment explorable with man-made systems, with some possible quantum optics experiments at each given distance.

C.-Y. Lu *et al.*, Micius quantum experiments in space, Rev. Mod. Phys., 94 (2022) 035001.

美国量子信息国家战略
——以LANL为例

The Quantum Institute
at Los Alamos National Laboratory

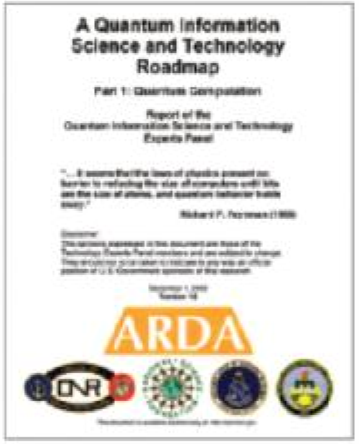
- 鼓励交叉研究
- 理论与实验相结合

. . . the development of a fully operational quantum computer would demolish the concept of national security. Whichever country gets there first will have the ability to eavesdrop on the plans of its enemies. Although still in its infancy, quantum computing presents a potential threat to global security.

Simon Singh, *The Code Book*

Advanced computing

Manhattan Project



A Quantum Information Science and Technology Roadmap

Part 1: Quantum Computation

Report of the Quantum Information Science and Technology Experts Panel

ARDA

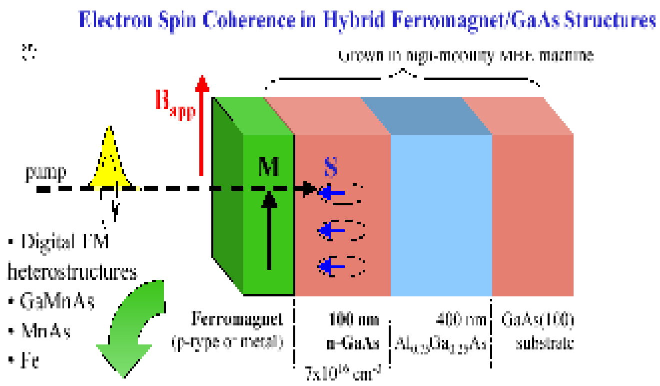
Leading the international effort to plan the future of quantum information science.

Cold-war deterrence

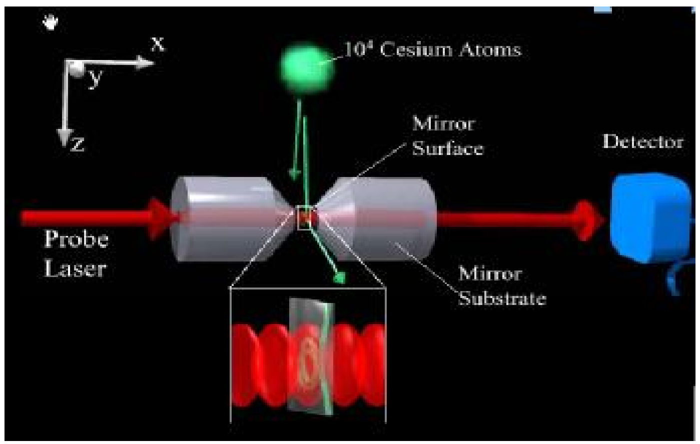
Non-proliferation space technology

量子信息处理的物理实现

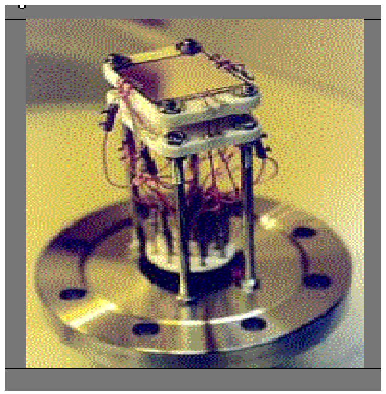
- **Liquid-state NMR**
- **NMR spin lattices**
- **Linear ion-trap spectroscopy**
- **Neutral-atom optical lattices**
- **Cavity QED + atoms**
- **Linear optics with single photons**
- **Nitrogen vacancies in diamond**
- **Electrons on liquid He**
- **Small Josephson junctions**
  - **"charge" qubits**
  - **"flux" qubits**
- **Spin spectroscopies, impurities in semiconductors**
- **Coupled quantum dots**
  - **Qubits: spin,charge,excitons**
  - **Exchange coupled, cavity coupled**



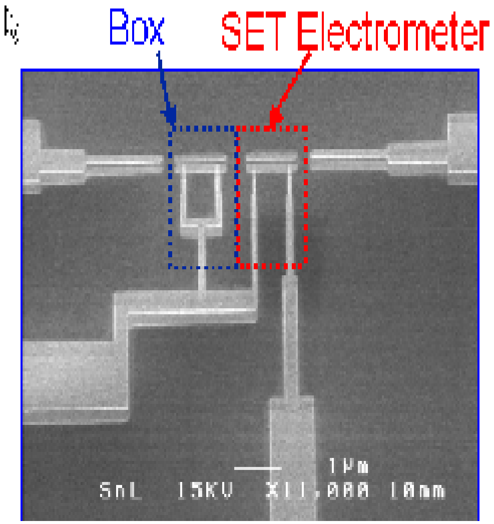
Spintronics



Cavity QED

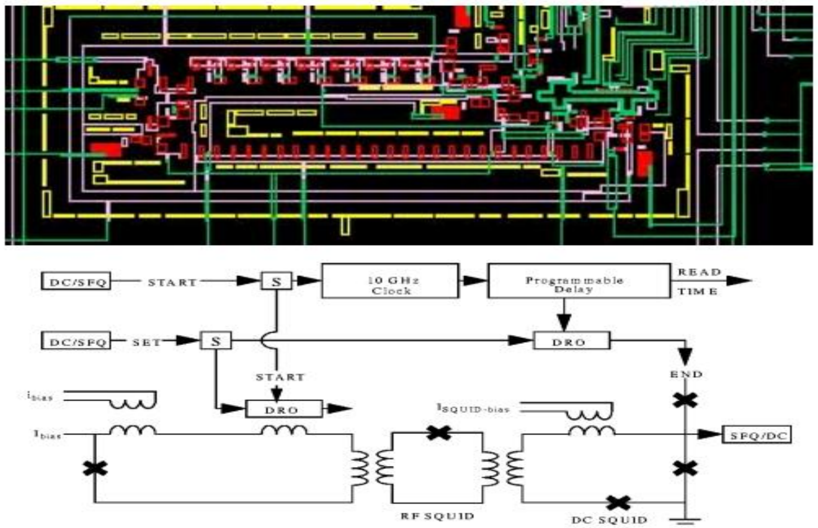


Atom Chip



Cooper

Pair Box

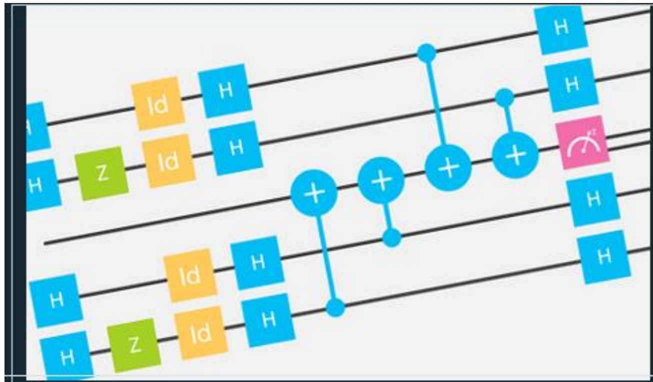


RF-SQUID

量子信息，谁在做？

- Aarhus
- Berkeley
- Caltech
- Cambridge
- College Park
- Delft
- DERA (U.K.)
- École normale supérieure
- Geneva
- HP Labs (Palo Alto and Bristol)
- Hitachi
- id Quantique
- IBM Research (Yorktown Heights and Palo Alto)
- Innsbruck
- Los Alamos National Labs
- McMaster
- MagiQ
- Max Planck Institute-Munich
- Melbourne
- MIT
- NEC
- New South Wales
- NIST
- NRC
- Orsay
- Oxford
- Paris
- Queensland
- Santa Barbara
- Stanford
- Toronto
- USTC
- Vienna
- Waterloo
- Yale
- many others…

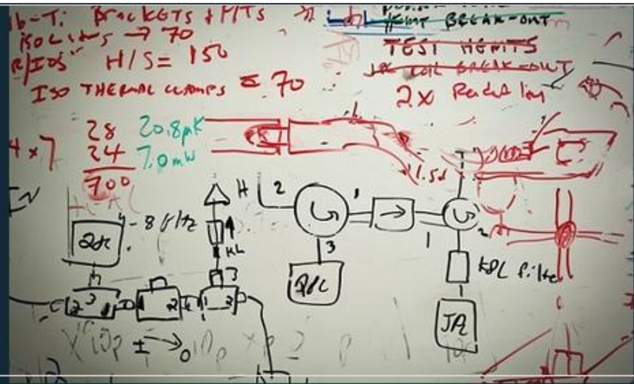
量子计算



Demo: IBM Quantum Experience

Watch a demo of how to use the world's first quantum computing platform delivered via the IBM Cloud.

Watch the video



Quantum Computing on the Cloud

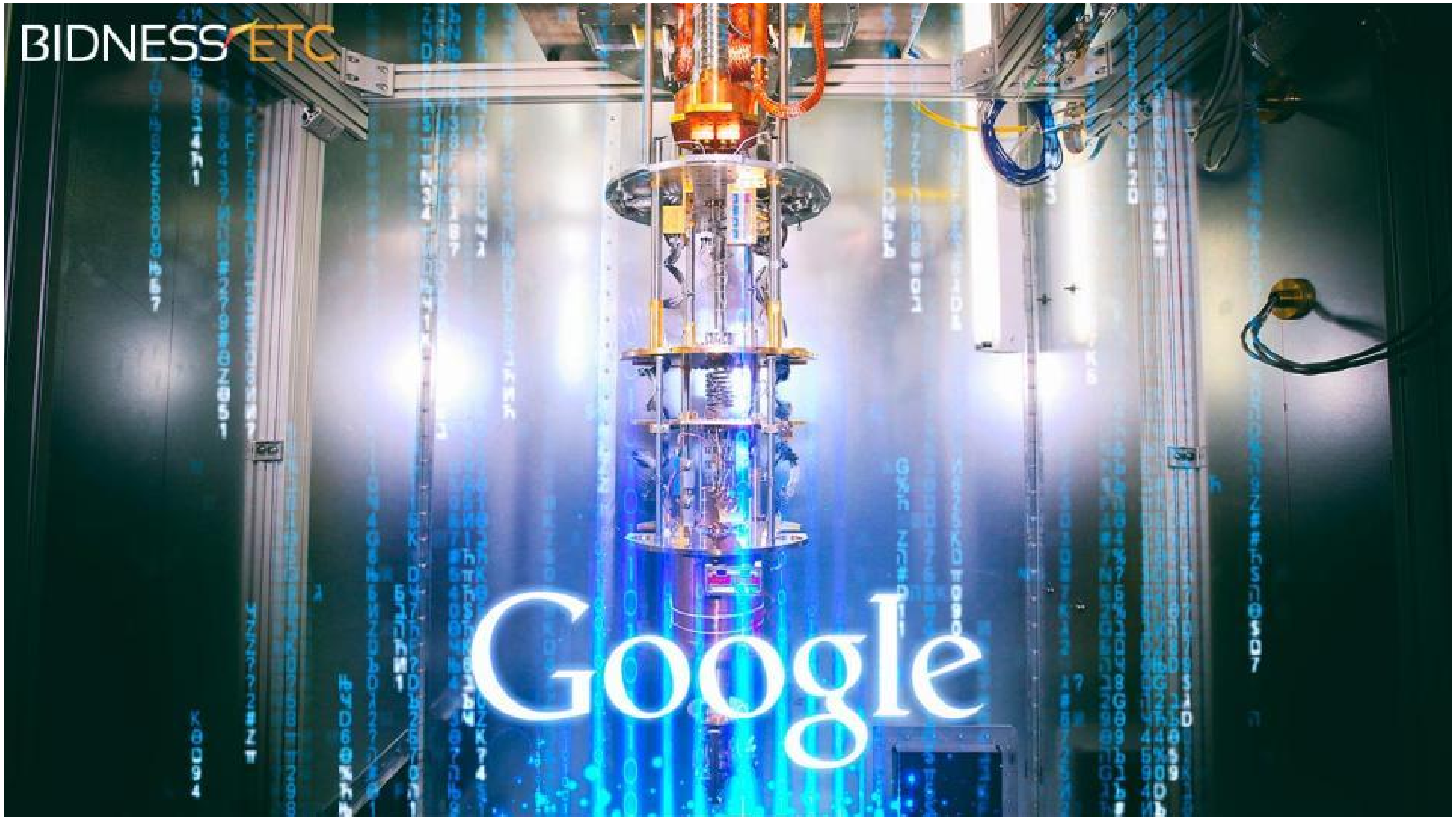
Hear from IBM experts about the new cloud-enabled quantum computing platform.

Watch the video

IBM Quantum Computing Lab Tour

Explore a 360 degree look at the IBM Quantum Computing Lab at the Thomas J Watson Research Center.

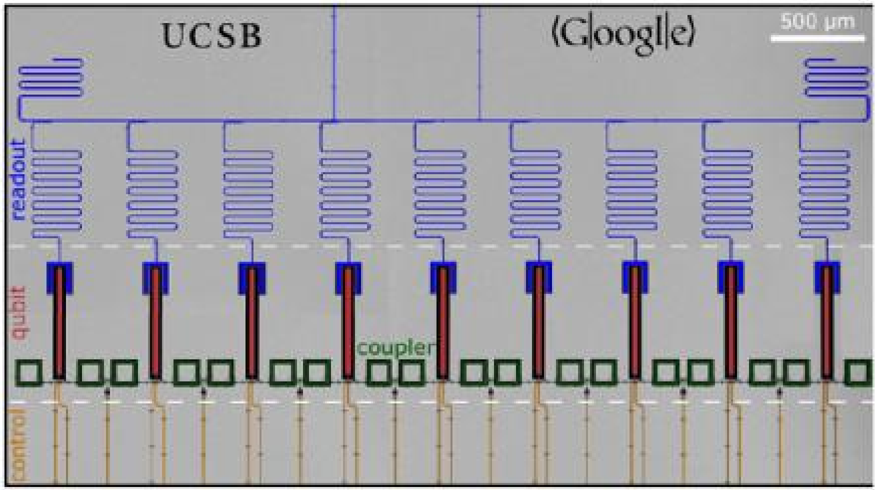
Watch the video

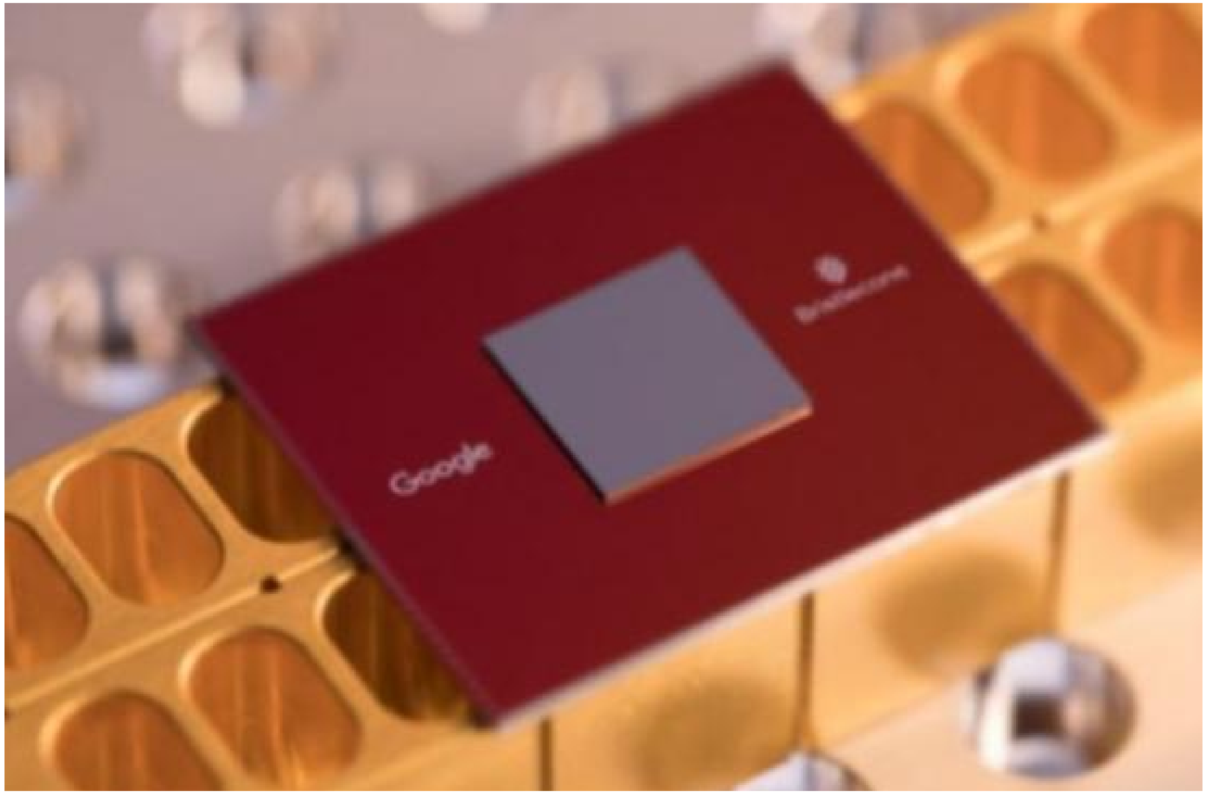

BIDNESS ETC
Google

量子计算？*有争议！*

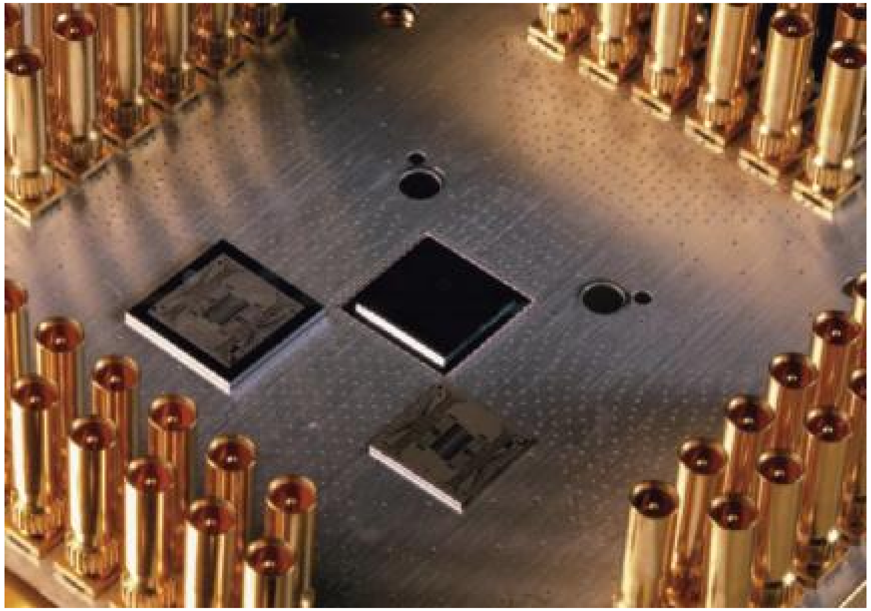

D:WAVE
The Quantum Computing Company
fabricated and used in the very first D-Wave One system delivered for
customer use in December, 2010.
This chip is certified to have been cooled to 20 degrees milli-Kelvin.
29/100

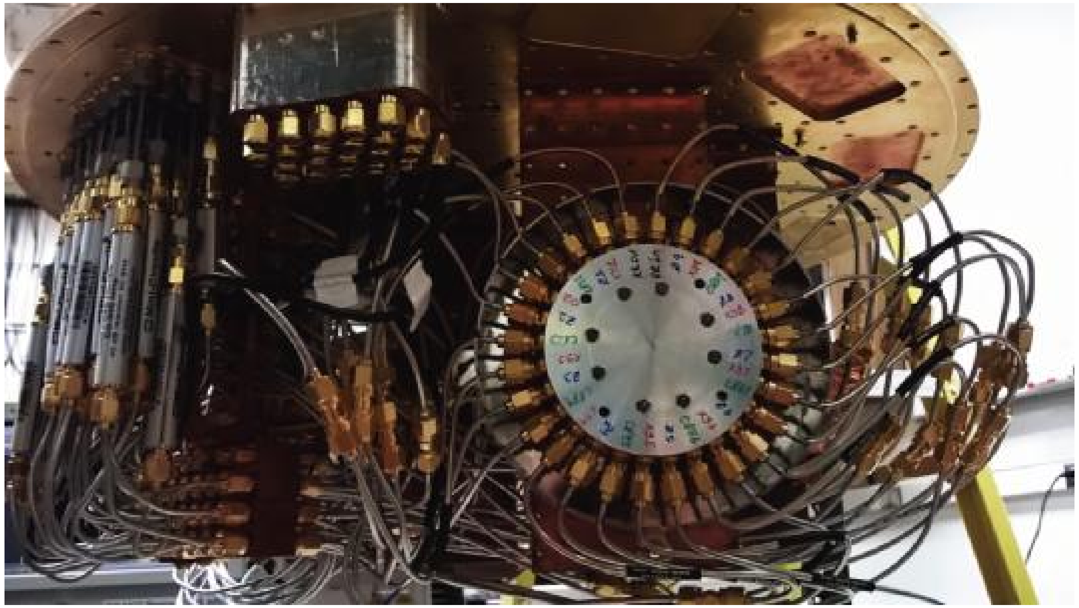
Google量子计算



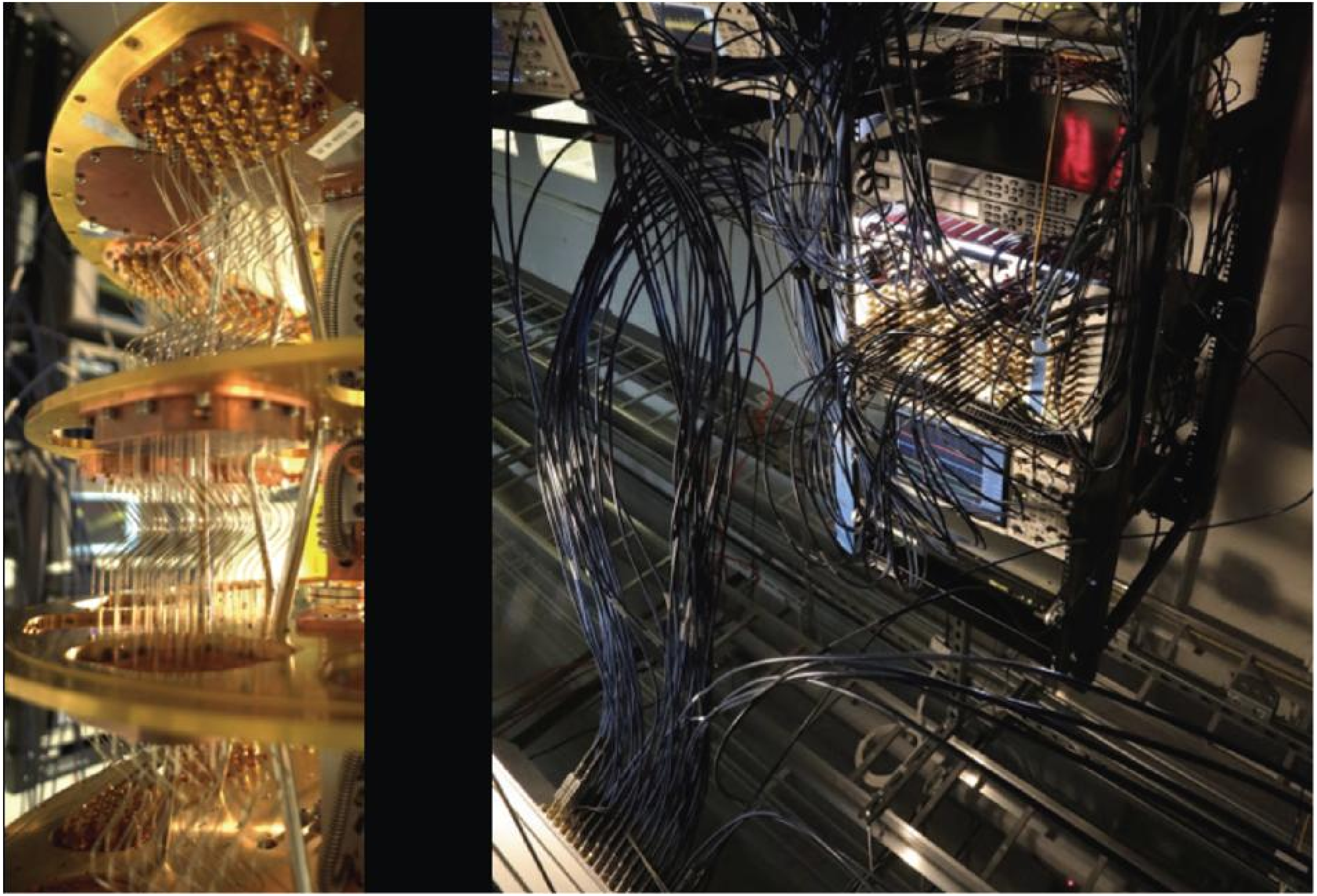


Google





Google



中国科学技术大学 陈凯

Google

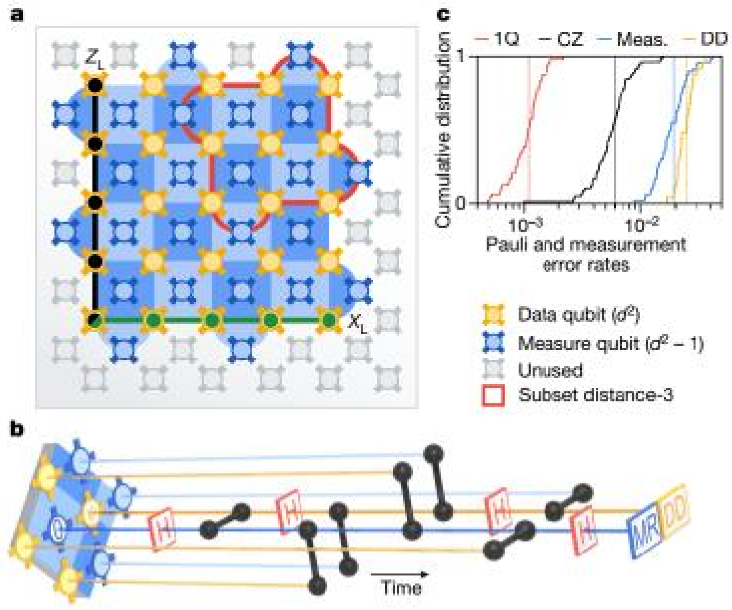
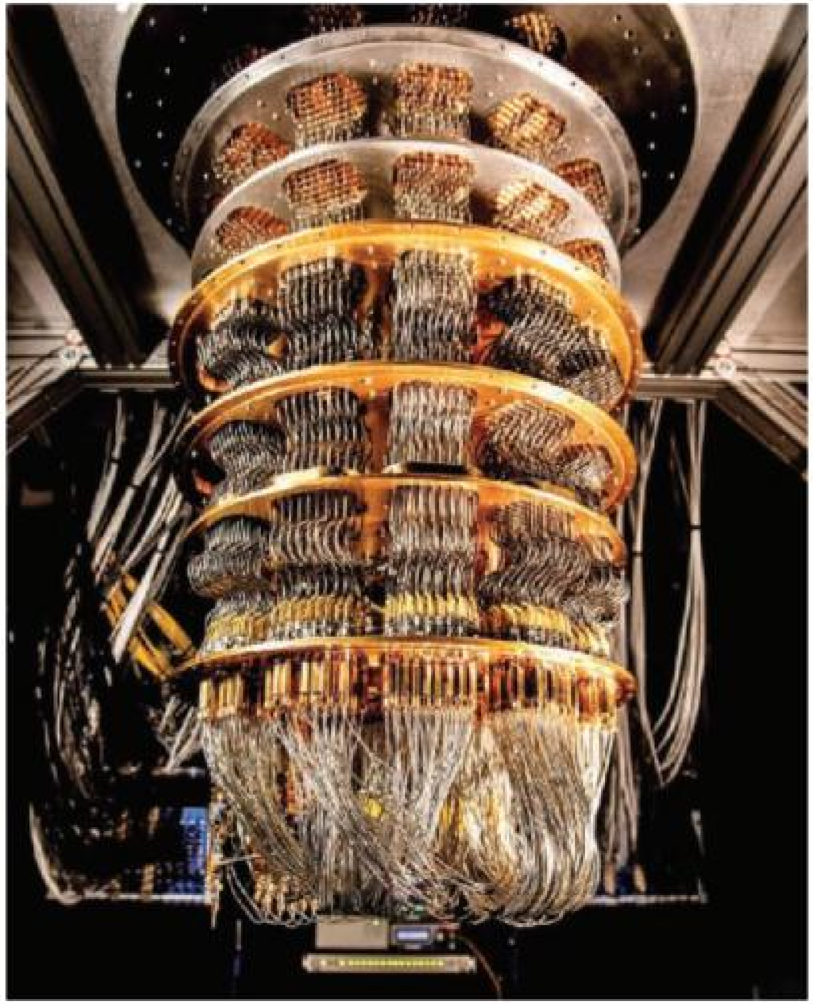


Fig. 1 | Implementing surface code logical qubits. a, Schematic of a 72-qubit Sycamore device with a distance-5 surface code embedded, consisting of 25 data qubits (gold) and 24 measure qubits (blue). Each measure qubit is associated with a stabilizer (blue coloured tile, dark: *X*, light: *Z*). Representative logical operators Z_L (black) and X_L (green) traverse the array, intersecting at the lower-left data qubit. The upper right quadrant (red outline) is one of four subset distance-3 codes (the four quadrants) that we compare to distance-5. **b**, Illustration of a stabilizer measurement, focusing on one data qubit (labelled ψ) and one measure qubit (labelled 0), in perspective view with time progressing to the right. Each qubit participates in four CZ gates (black) with its four nearest neighbours, interspersed with Hadamard gates (H), and finally, the measure qubit is measured and reset to |0⟩ (MR). Data qubits perform dynamical decoupling (DD) while waiting for the measurement and reset. All stabilizers are measured in this manner concurrently. Cycle duration is 921 ns, including 25-ns single-qubit gates, 34-ns two-qubit gates, 500-ns measurement and 160-ns reset (see Supplementary Information for compilation details). The readout and reset take up most of the cycle time, so the concurrent data qubit idling is a dominant source of error. **c**, Cumulative distributions of errors for single-qubit gates (1Q), CZ gates, measurement (Meas.) and data qubit dynamical decoupling (idle during measurement and reset), which we refer to as component errors. The circuits were benchmarked in simultaneous operation using random circuit techniques, on the 49 qubits used in distance-5 and the 4 CZ layers from the stabilizer circuit[38,39] (see Supplementary Information). Vertical lines are means.

Suppressing quantum errors by scaling a surface code logical qubit

•Google Quantum AI

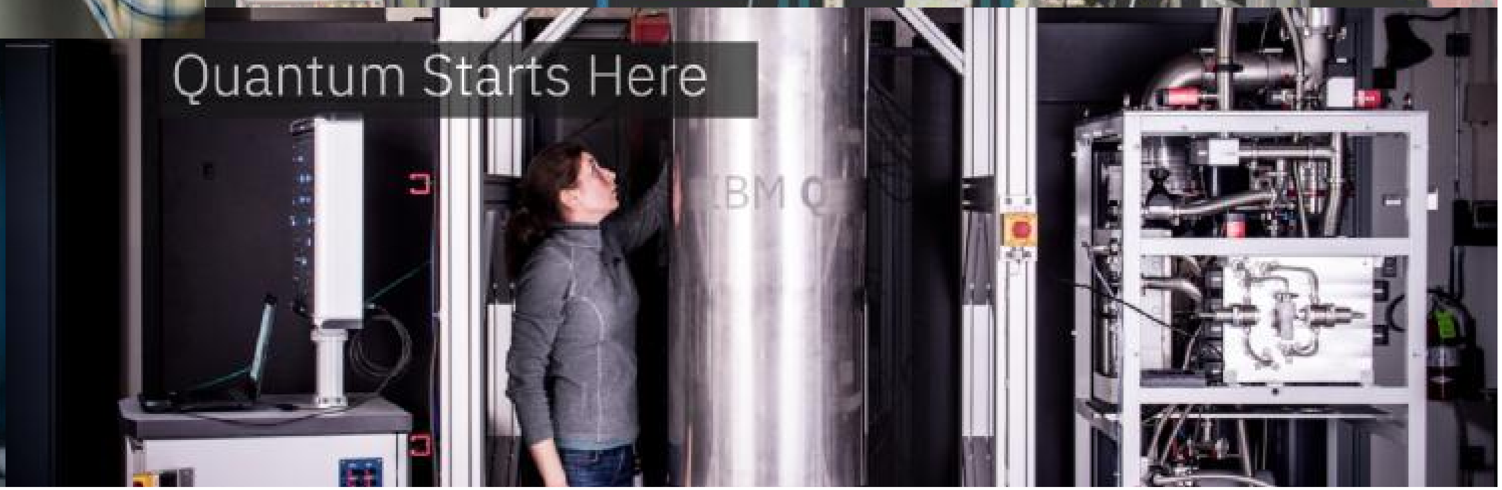
Nature 614, 676–681 (2023)



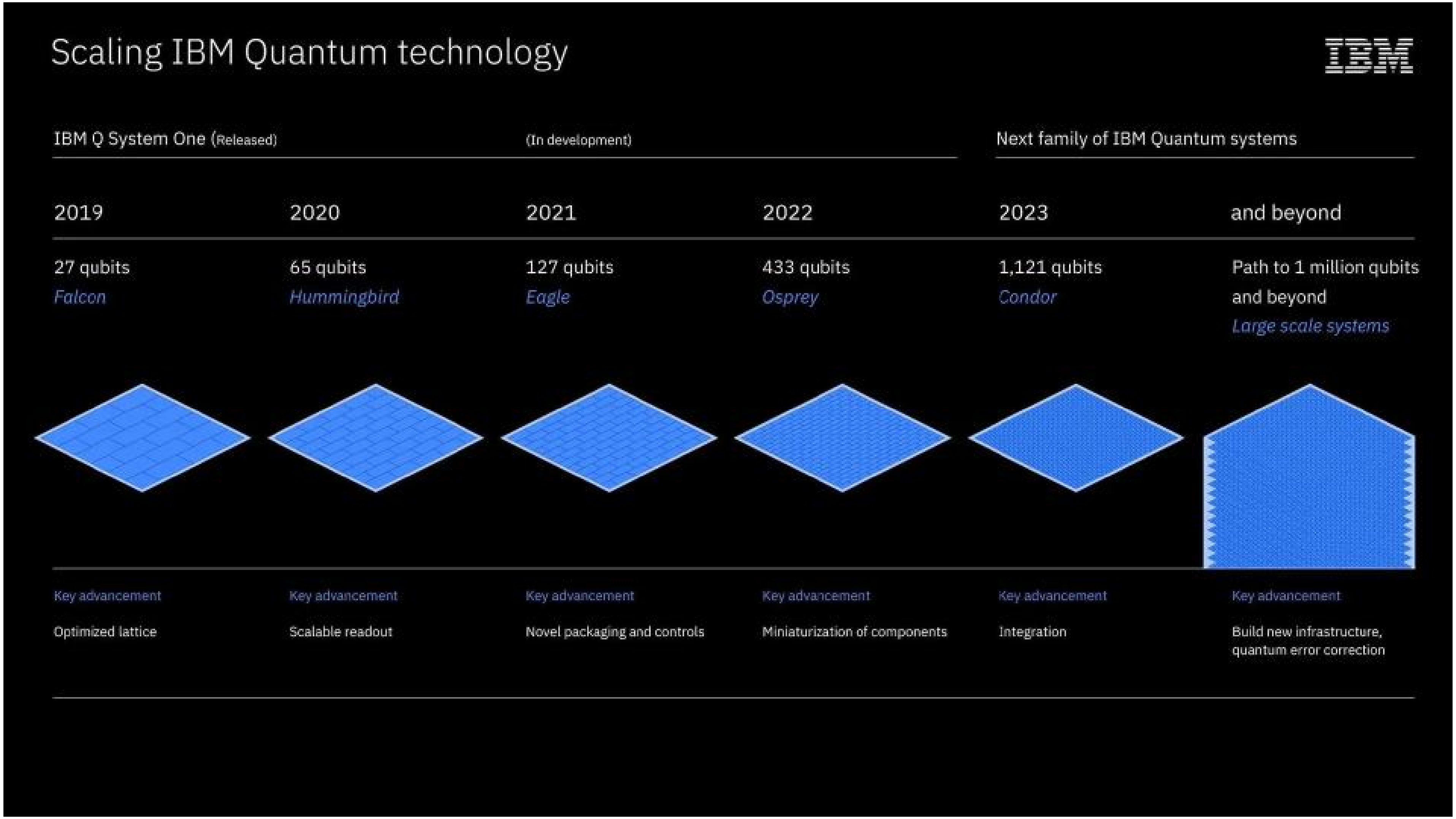
A refrigerator festooned with microwave cables cools Google's quantum chip nearly to absolute zero.

中国科学技术大学 陈凯

IBM量子计算



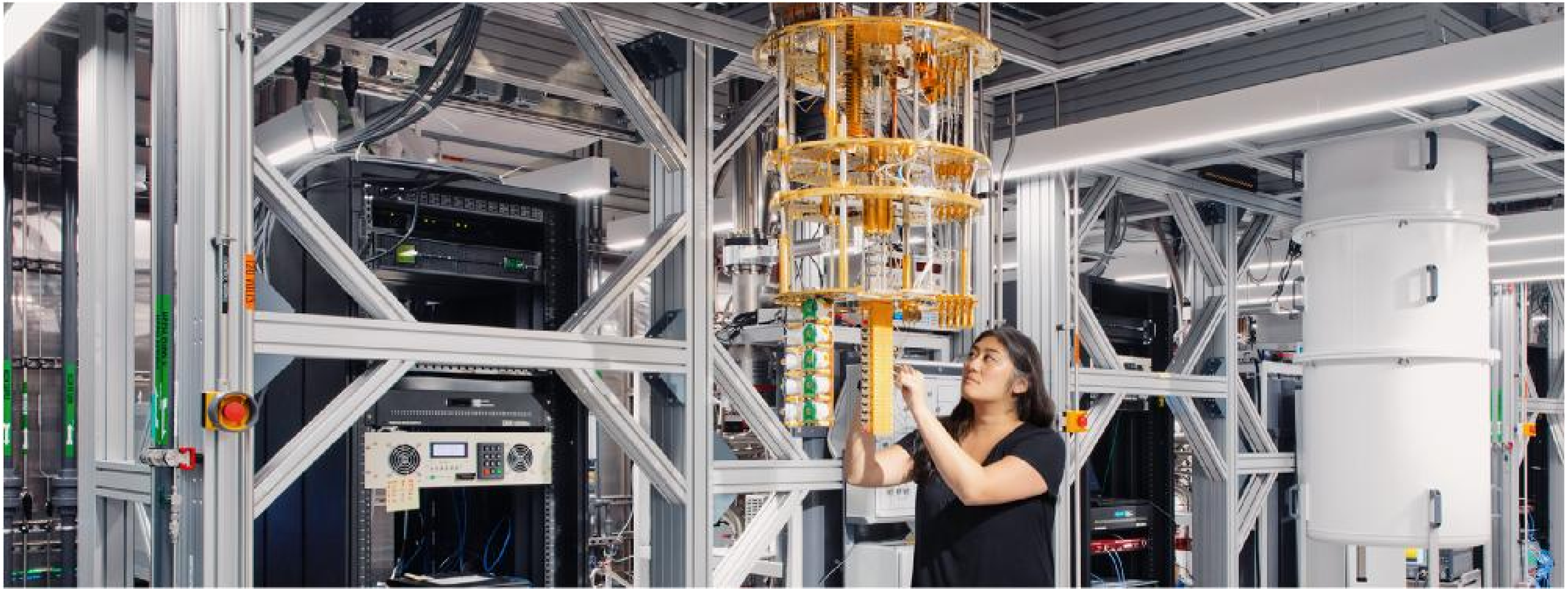
IBM量子计算

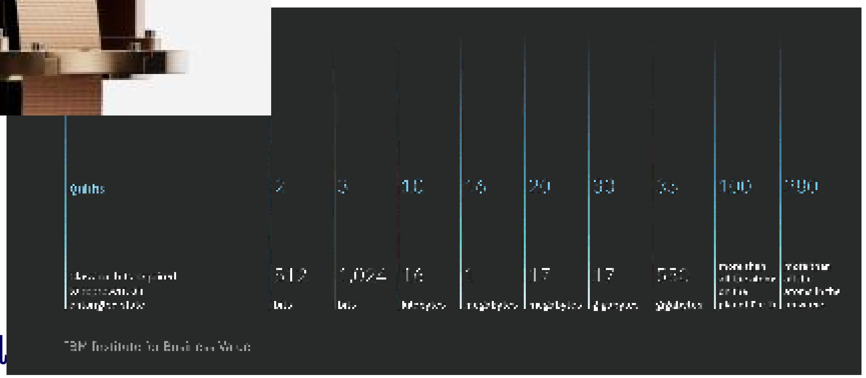


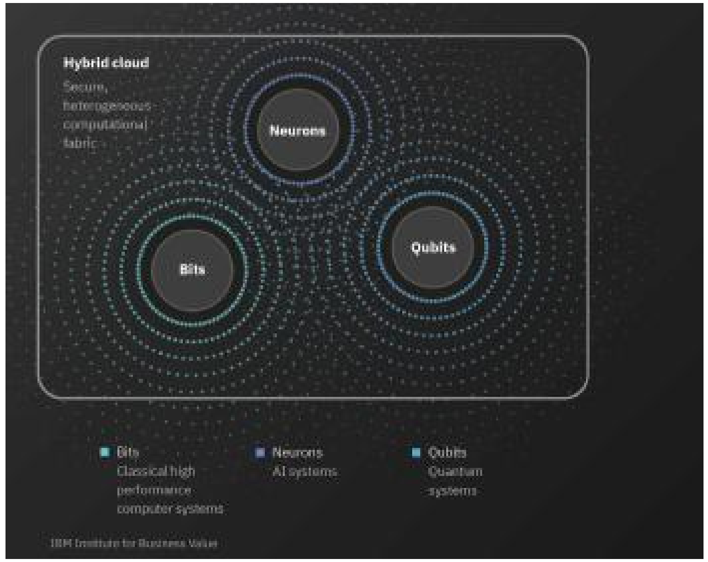
A look at IBM's roadmap to advance quantum computers from today's noisy, small-scale devices to larger, more advance quantum systems of the future. Credit: StoryTK for IBM

https://www.ibm.com/blogs/research/2020/09/ibm-quantum-roadmap/

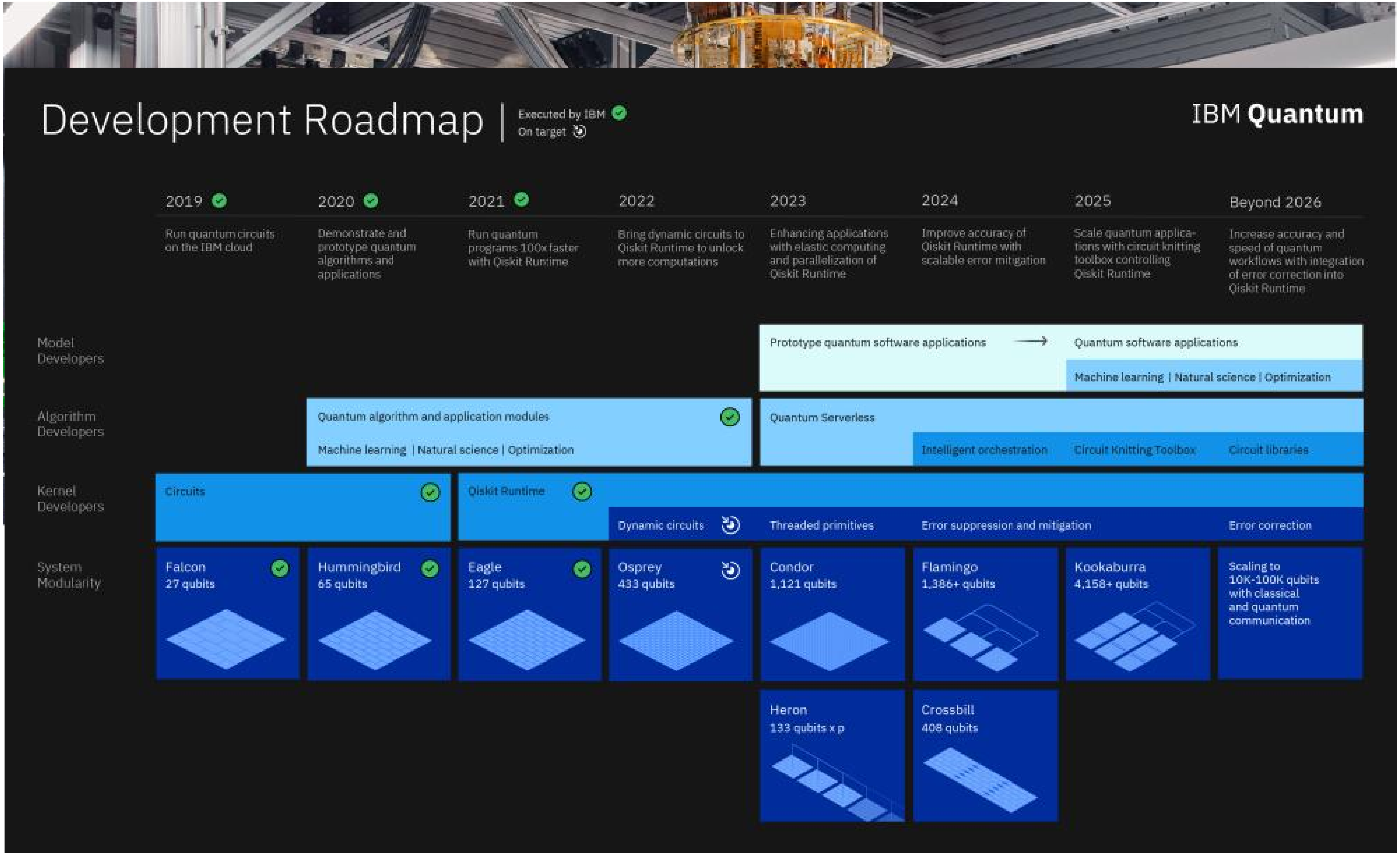
IBM量子计算




Qubits

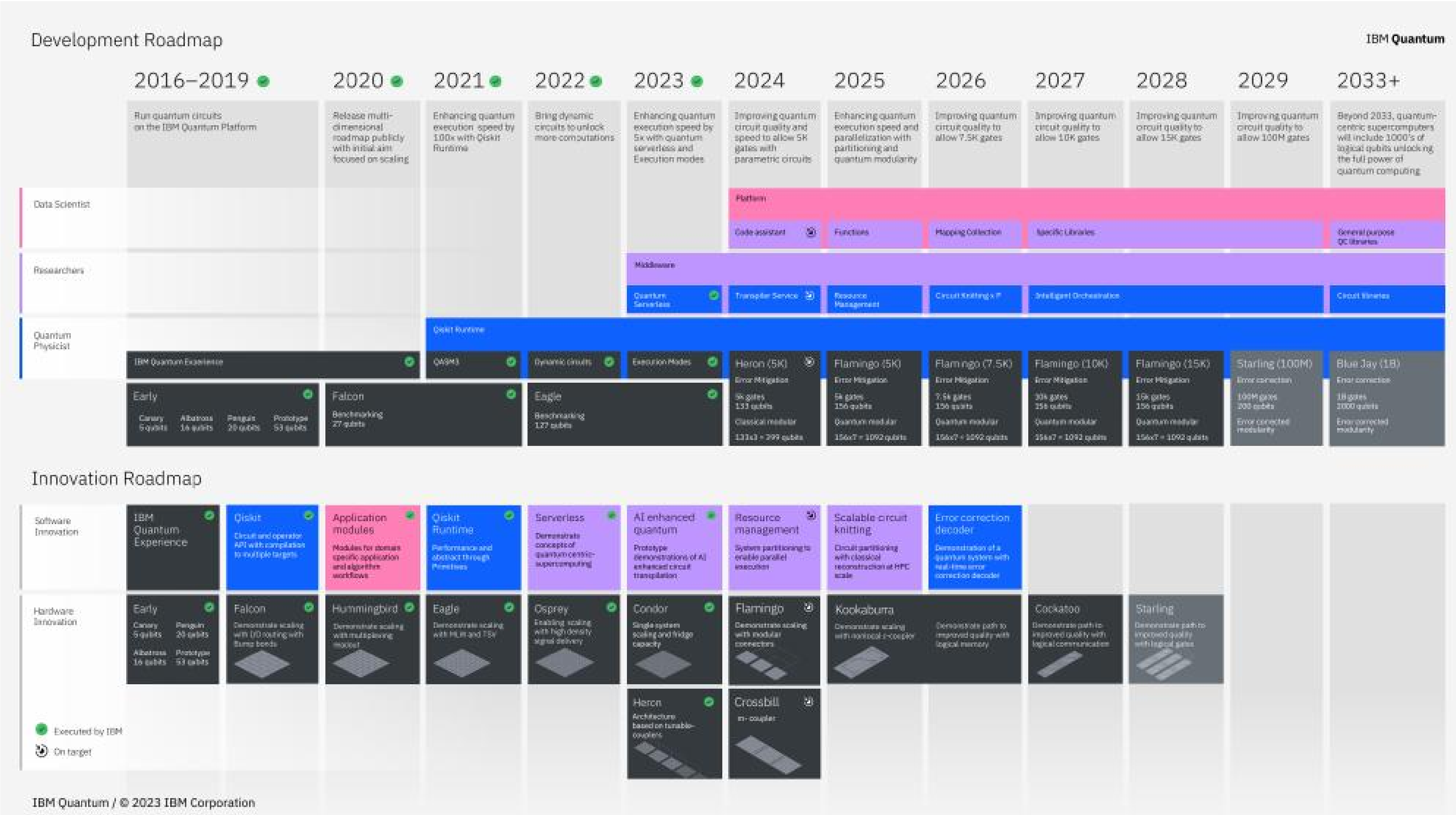

Hybrid cloud
Secure, heterogeneous computational fabric
Neurons
Bits
Qubits
Bits
Classical high performance computer systems
Neurons
AI systems
Qubits
Quantum systems
IBM Institute for Business Value

IBM量子计算



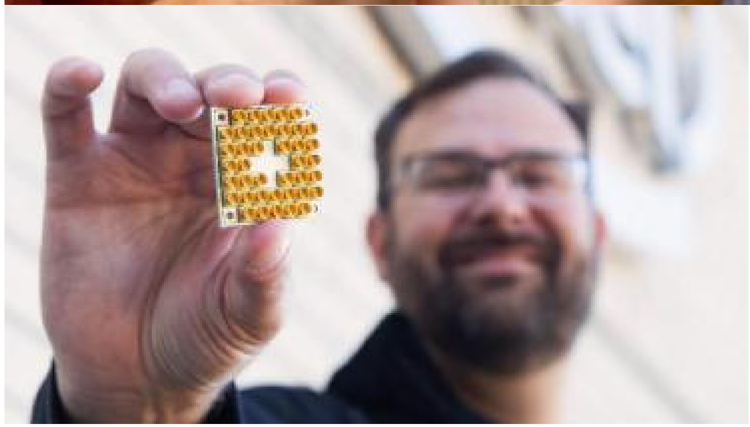
Development Roadmap
Executed by IBM
On target
IBM Quantum
2019
Run quantum circuits on the IBM cloud
2020
Demonstrate and prototype quantum algorithms and applications
2021
Run quantum programs 100x faster with Qiskit Runtime
2022
Bring dynamic circuits to Qiskit Runtime to unlock more computations
2023
Enhancing applications with elastic computing and parallelization of Qiskit Runtime
2024
Improve accuracy of Qiskit Runtime with scalable error mitigation
2025
Scale quantum applications with circuit knitting toolbox controlling Qiskit Runtime
Beyond 2026
Increase accuracy and speed of quantum workflows with integration of error correction into Qiskit Runtime
Model Developers
Prototype quantum software applications
Quantum software applications
Machine learning | Natural science | Optimization
Algorithm Developers
Quantum algorithm and application modules
Machine learning | Natural science | Optimization
Quantum Serverless
Intelligent orchestration
Circuit Knitting Toolbox
Circuit libraries
Kernel Developers
Circuits
Qiskit Runtime
Dynamic circuits
Threaded primitives
Error suppression and mitigation
Error correction
System Modularity
Falcon
27 qubits
Hummingbird
65 qubits
Eagle
127 qubits
Osprey
433 qubits
Condor
1,121 qubits
Flamingo
1,386+ qubits
Kookaburra
4,158+ qubits
Scaling to 10K-100K qubits with classical and quantum communication
Heron
133 qubits x p
Crossbill
408 qubits

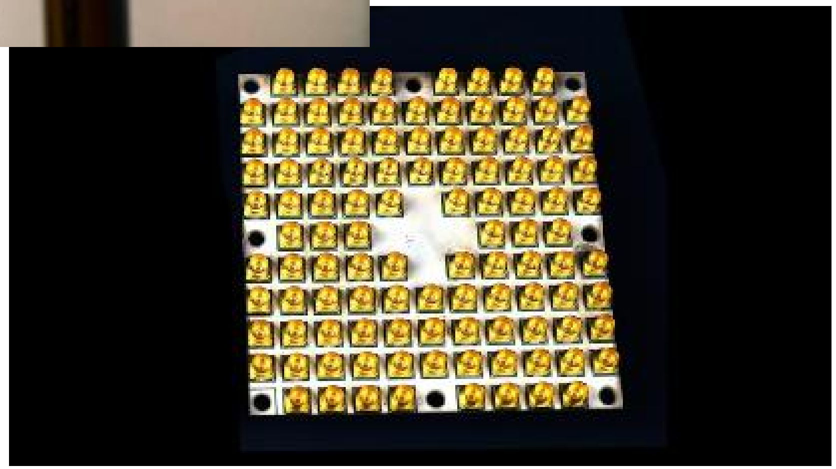
IBM量子计算



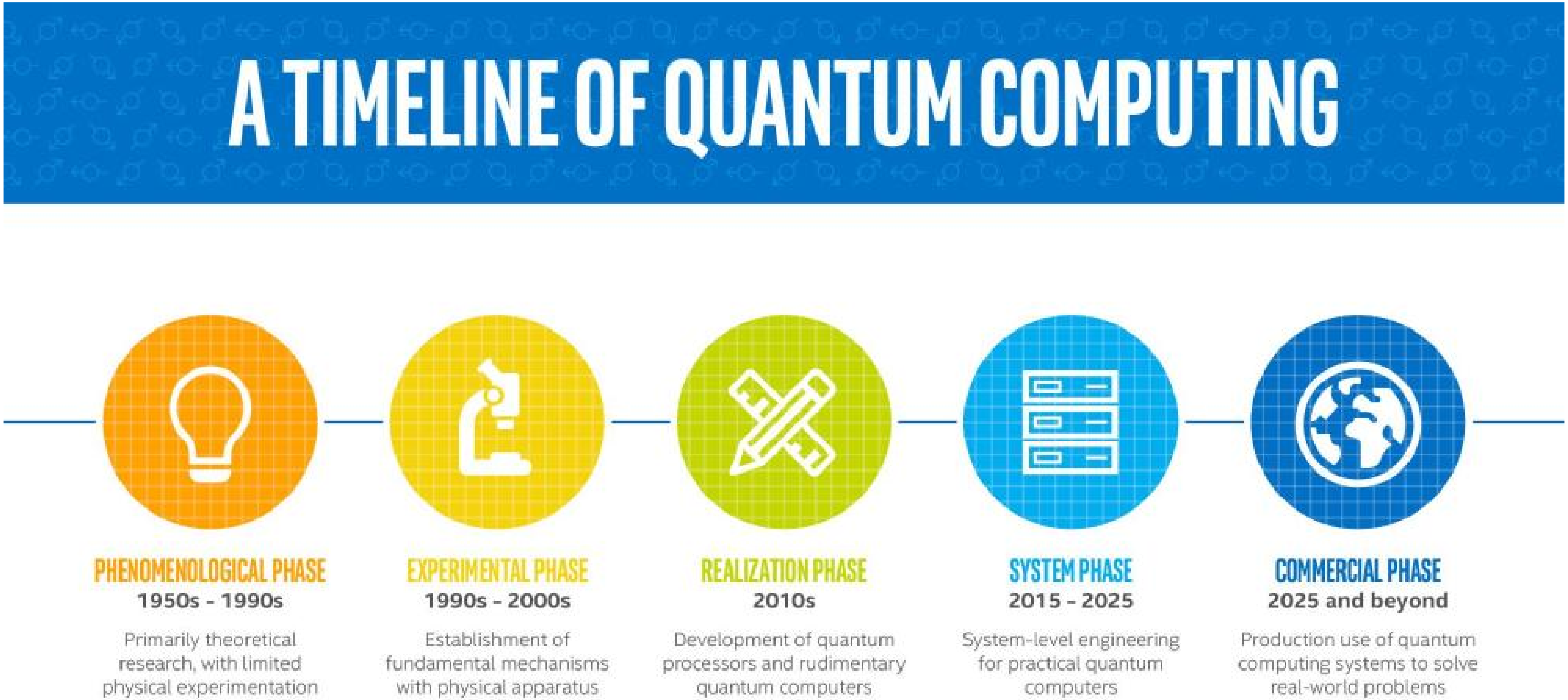
中国科学技术大学 陈凯

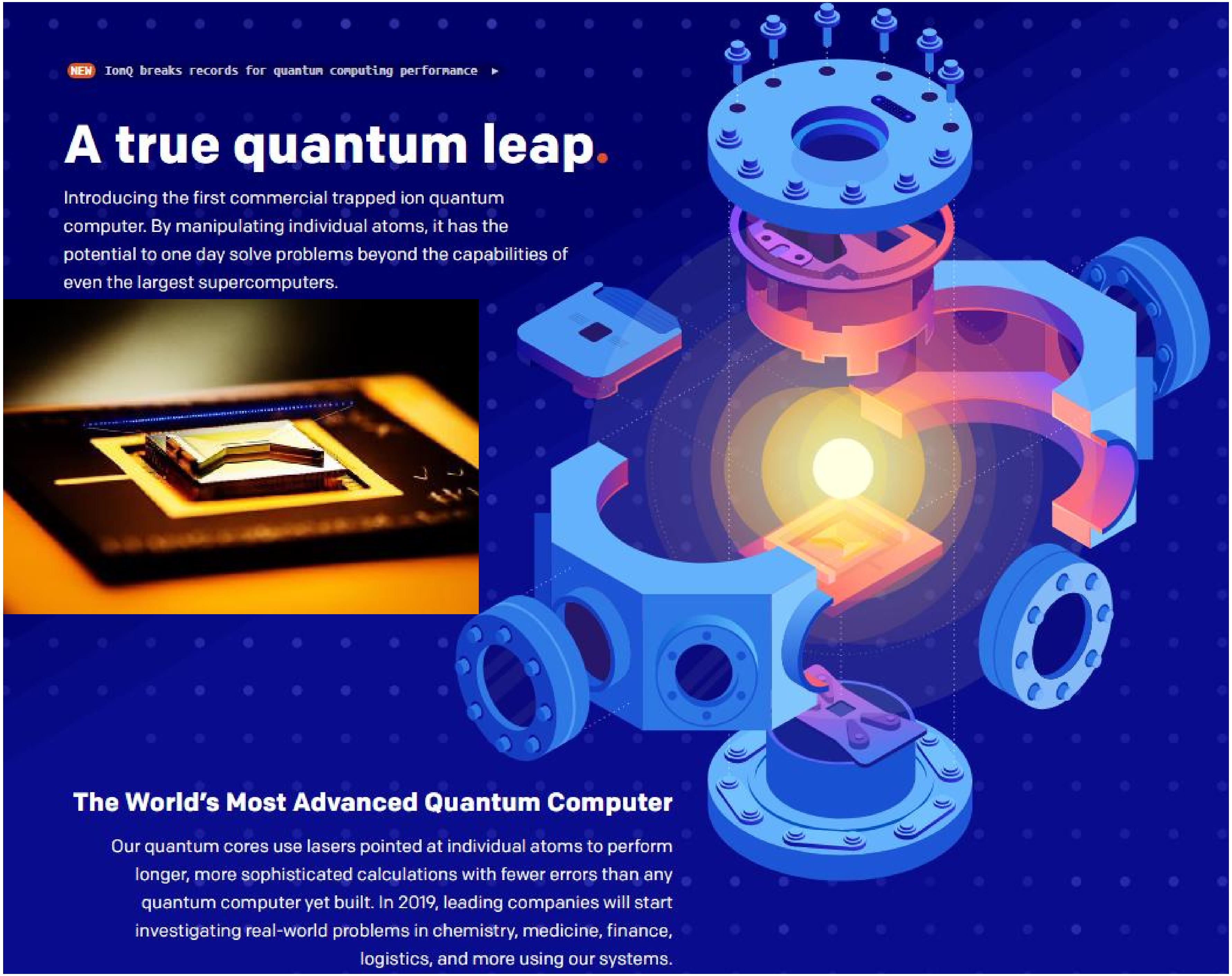
Intel量子计算





Intel量子计算


A TIMELINE OF QUANTUM COMPUTING
PHENOMENOLOGICAL PHASE
1950s - 1990s
Primarily theoretical research, with limited physical experimentation
EXPERIMENTAL PHASE
1990s - 2000s
Establishment of fundamental mechanisms with physical apparatus
REALIZATION PHASE
2010s
Development of quantum processors and rudimentary quantum computers
SYSTEM PHASE
2015 - 2025
System-level engineering for practical quantum computers
COMMERCIAL PHASE
2025 and beyond
Production use of quantum computing systems to solve real-world problems


NEW IonQ breaks records for quantum computing performance ▶
A true quantum leap.
Introducing the first commercial trapped ion quantum computer. By manipulating individual atoms, it has the potential to one day solve problems beyond the capabilities of even the largest supercomputers.
The World's Most Advanced Quantum Computer
Our quantum cores use lasers pointed at individual atoms to perform longer, more sophisticated calculations with fewer errors than any quantum computer yet built. In 2019, leading companies will start investigating real-world problems in chemistry, medicine, finance, logistics, and more using our systems.

Preliminary benchmark test results on IonQ hardware as of December 10, 2018.

Qubits

Qubits are the basic unit of information storage on a quantum computer. After they're initialized, logical operations—called gates—are performed on them.

Maximum loaded 160 qubits

Single-qubit gates performed on up to 79 qubits

Two-qubit gates performed on all pairs of up to 11 qubits

Error Rate

Gate fidelity is a measure of the accuracy of a single gate. Gates that manipulate one qubit at a time are less complex and less error-prone than gates that operate on two qubits. The following benchmarks were captured on a fully-connected 11-qubit configuration.

Average fidelities

Single-qubit gates >99%

Two-qubit gates >98%*

Best fidelities

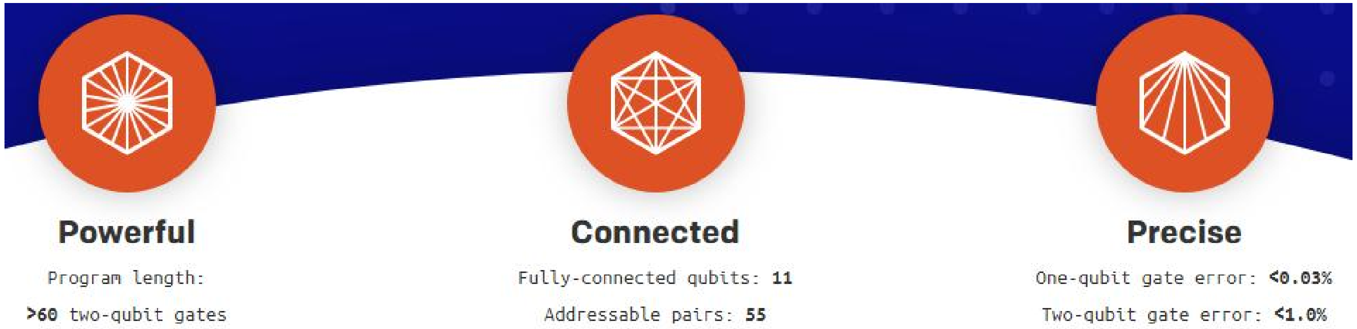
Single-qubit gates 99.97%

Two-qubit gates 99.3%*

Minimum fidelities

Single-qubit gates >99%

Two-qubit gates >96%*



* not corrected for state preparation and measurement errors.

Benchmark: Bernstein-Vazirani Algorithm

The Bernstein-Vazirani Algorithm is a basic test of the ability of a quantum computer to simultaneously evaluate possibilities that conventional computers must calculate one at a time. The complexity of the test is determined by the maximum length in bits of an oracle—an arbitrary number the computer must determine.

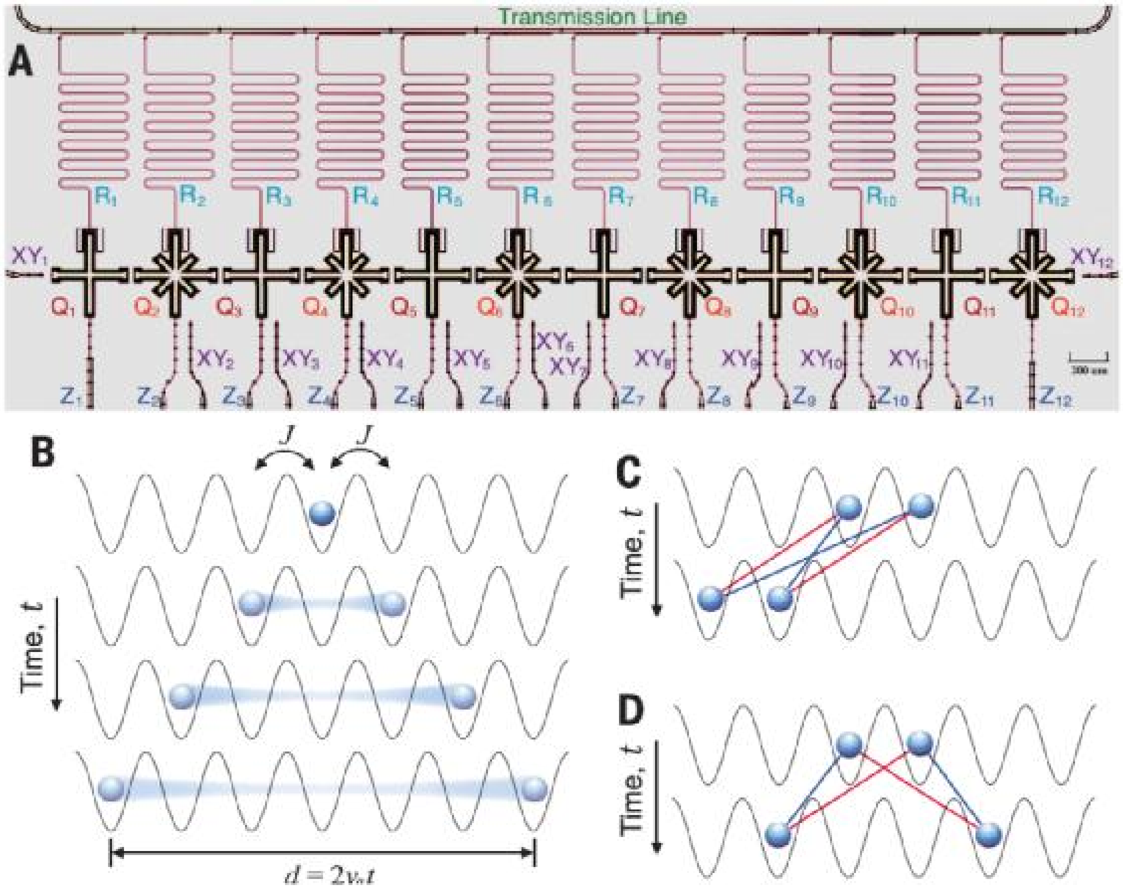
10-qubit oracle success rate 73.0%

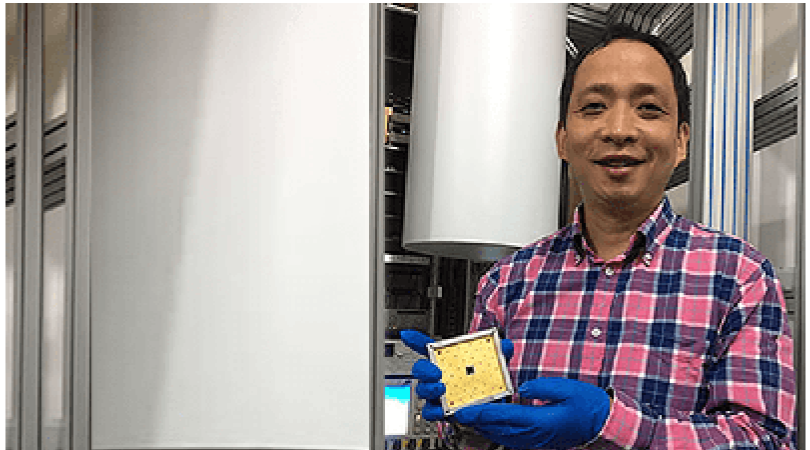
Classical computer success rate ~0.2%

我国量子计算

USTC，清华，浙大，中科院等；阿里巴巴，腾讯，百度，华为等

Yan *et al.*, Science 364, 753–756 (2019)

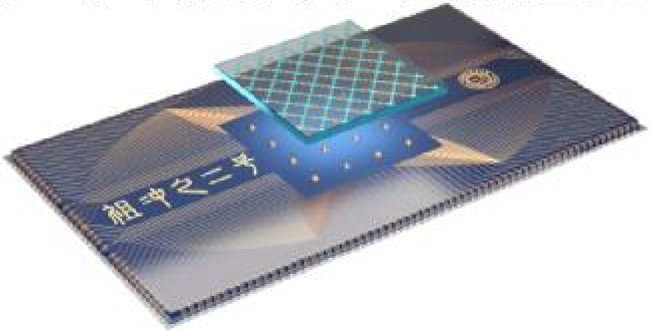




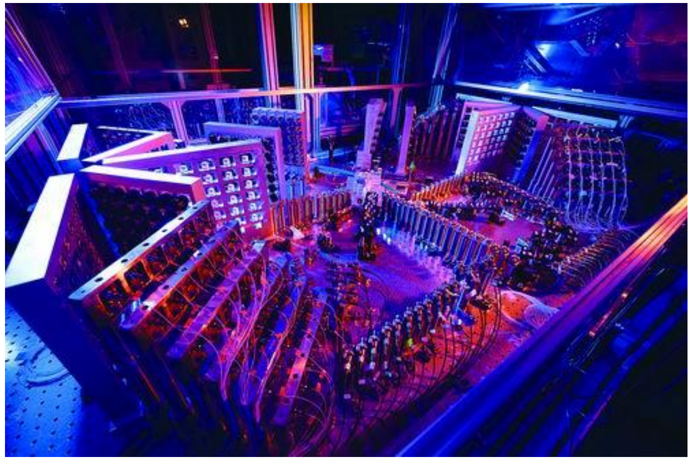
我国量子计算

USTC，清华，浙大，中科院等；阿里巴巴，腾讯，百度，华为等

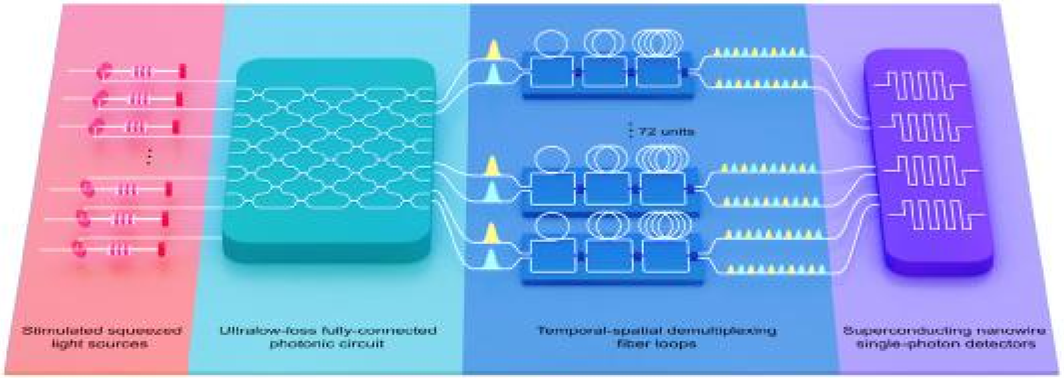
可编程二维 62 比特超导处理器“祖冲之号”的量子行走



66比特可编程超导量子计算原型机“祖冲之二号”



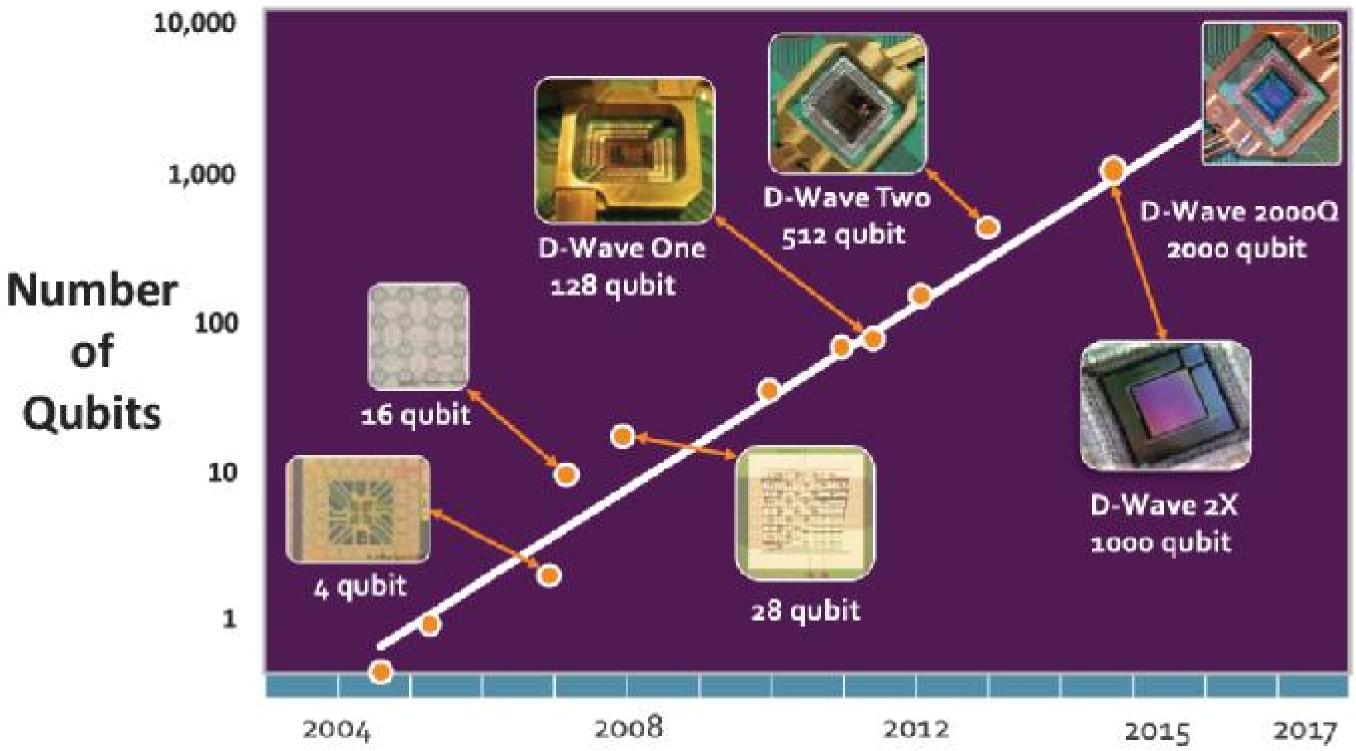
113个光子144模式的量子计算原型机“九章二号”



255个光子的量子计算原型机“九章三号”

D-Wave

D-Wave Product Generations



D-Wave The Quantum Computing Company

D-Wave


It's Time to Start Your Quantum Journey
Don't be left behind. Forward-thinking organizations see quantum as an opportunity to leap ahead of the competition. From finding efficiencies and reducing waste to decreasing time to solution and solving problems abandoned due to complexity, the business value is real.
Get Access to the Quantum Computing Industry Report
40% of large enterprises
surveyed are already experimenting with quantum computing.
Source: 451 Research


QBTS
LISTED
NYSE


advantage2
NEXT-GENERATION
EXPERIMENTAL PROTOTYPE


Get Business Advantage
From 25 hours of work to 2 minutes per week. 80% less manufacturing waste. 60% return on investment. 57% reduction in emissions. This is what quantum can do today for real-world applications.
Explore Customer Success Stories

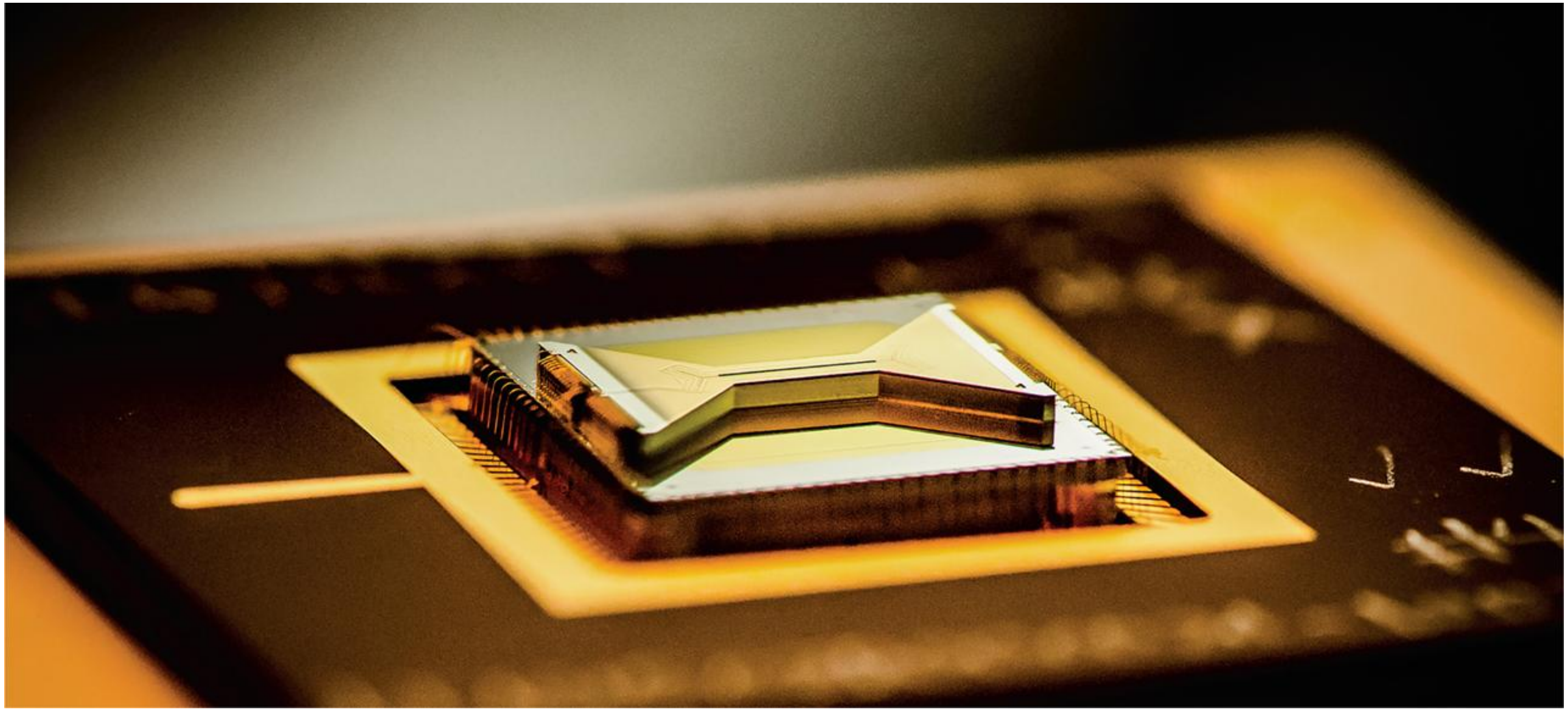
D-Wave


DEVELOPER TOOLS
Accelerate Quantum Development with Ocean
The Ocean software fits between applications and the compute resources.
Social Network Analysis
Traffic Flow
Web Advertising
New Application
Portfolio Optimization
Scheduling
Circuit Fault Detection
New Application
Ocean Software
Graph Mapping
Constraint Compilation
New Mapping Method
Problem Suitable for QPU: Binary Quadratic Model (BQM)
Simulated Annealing
D-Wave API
Hybrid Sampler
New Sampler


5000+
Qubits
A world-class annealing quantum processor design with continued growth in qubits, connectivity, and coherence.
1 Million
Variables
Built to support real-world size applications with up to 1 million variables and 100,000 constraints via our quantum-classical hybrid solver service in Leap.
250+
Applications
More than 250 early applications across domains like manufacturing, financial services, and life sciences already exist using D-Wave quantum systems today.

美国能源部推进量子计算

A chip that traps ions is the basis for a Department of Energy testbed quantum computer.



Adrian Cho Science 2018;359:141-142

Science AAAS

美国能源部推进量子计算

A quantum computing to-do list

Adrian Cho Science 2018;359:141-142

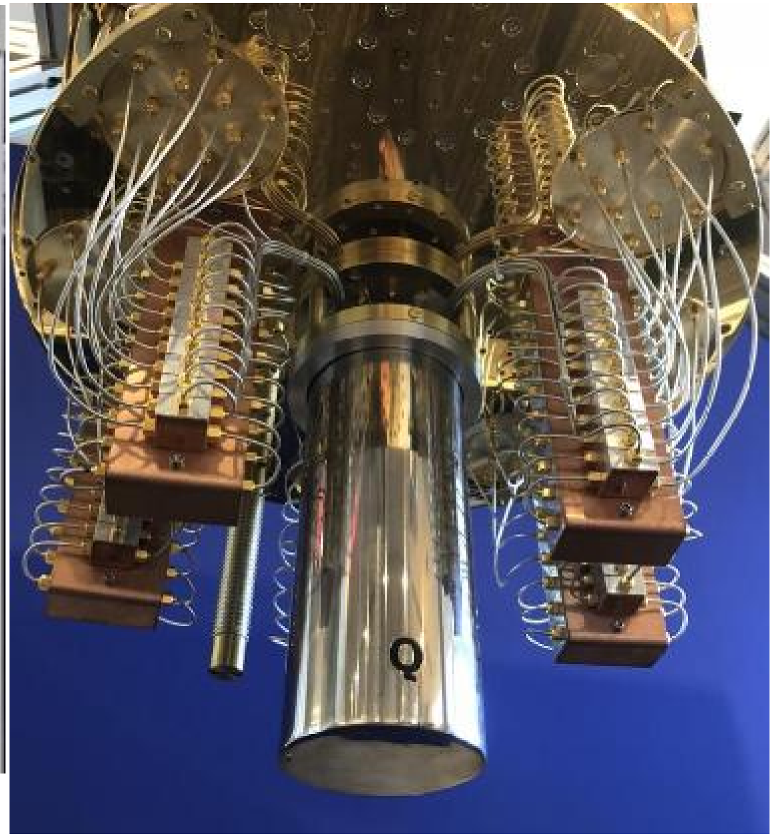
Researchers have several general ideas for scientific applications of quantum computers.

FIELD	TASK
Chemistry	Calculate molecules' energies and structures, model catalysis.
Materials science	Design novel materials from the atom up.
Nuclear physics	Calculate energies and structures of nuclei and particles such as protons.
Particle physics	Optimize search for subtle signals.

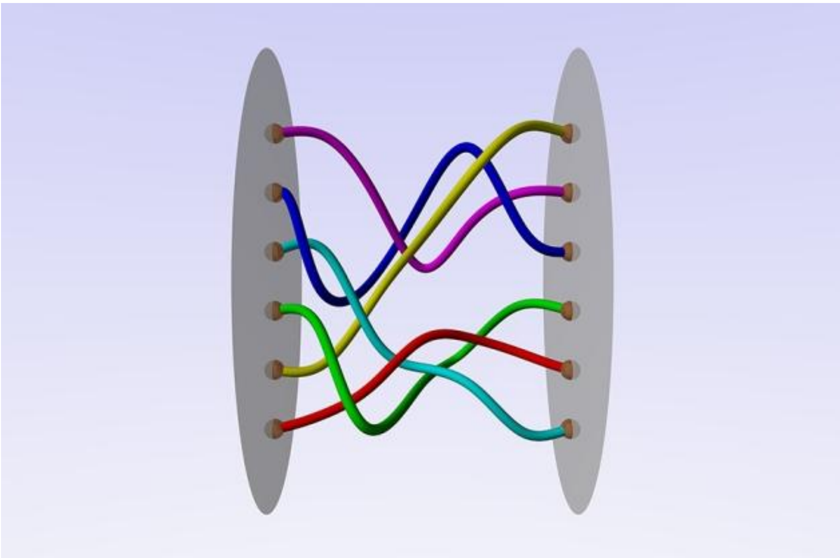
DOE Office of Science: Contributions to Quantum Computing

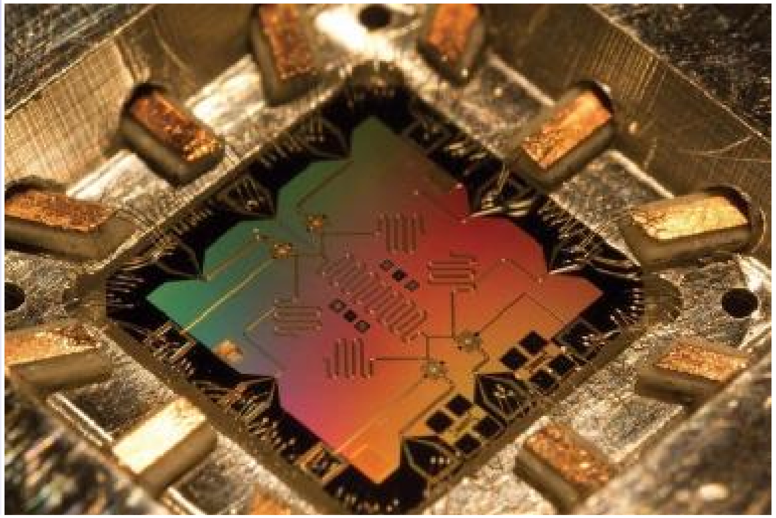
Support for quantum computing research originated in the Advanced Scientific Computing Research program in 2017 and rapidly spread across the Office of Science. The research portfolio now includes applications in nuclear and particle physics, plasma science, chemistry, and materials. It also includes improving the fundamental building blocks of quantum computers, developing sophisticated control to make the most of any group of qubits, and computer science research that will ultimately make quantum computers easier to use.

量子计算机竞赛



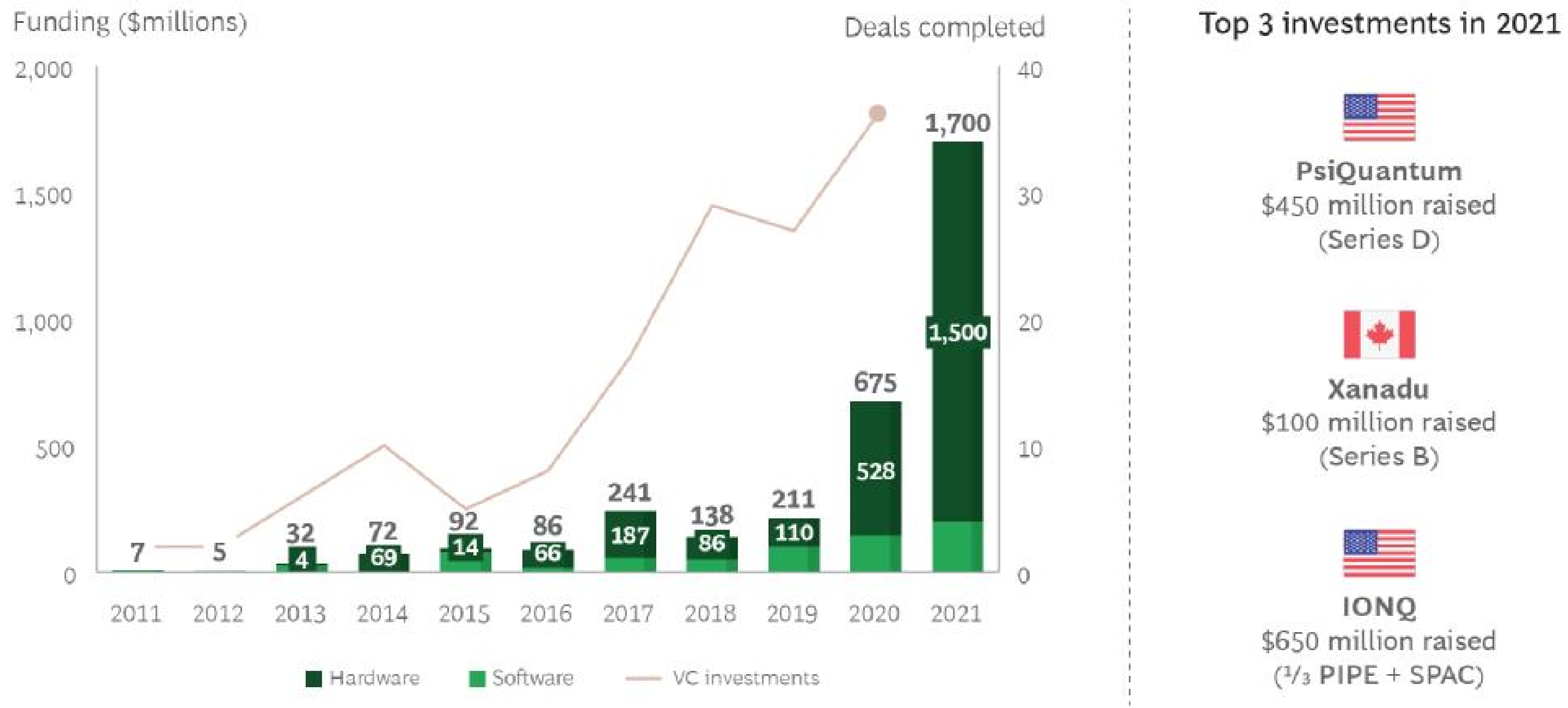
Google,
IBM, 微软,
Intel等





量子计算

Exhibit 1 - Acceleration of Investments in Quantum Computing



Sources: PitchBook; BCG analysis.

Note: PIPE = private investment in public equity; SPAC = special-purpose acquisition company.

2022年8月25日，波士顿咨询集团（BCG）发布的研究报告

《Can Europe Catch Up with the US (and China) in Quantum Computing?》

中国科学技术大学 陈凯

量子计算

Exhibit 2 - Quantum Computing Will Create Value Across Several Industries and Use Cases

	Applications	Private landscape Value creation potential ($billions)[1] Low	High
Cryptography ($40 billion to $80 billion)	Encryption/decryption	40	80
Optimization ($100 billion to $220 billion)	Aerospace: Flight route optimization	20	50
	Finance: Portfolio optimization	20	50
	Finance: Risk management	10	20
	Logistics: Vehicle routing/network optimization	50	100
Machine learning ($150 billion to $220 billion)	Automotive: Automated vehicles, AI algorithms	0	10
	Finance: Fraud and money laundering prevention	20	30
	High tech: Search and ads optimization	50	100
	Other: Varied AI applications	80+	80+
Simulation ($160 billion to $330 billion)	Aerospace: Computational fluid dynamics	10	20
	Aerospace: Materials development	10	20
	Automotive: Computational fluid dynamics	0	10
	Automotive: Materials and structural design	10	15
	Chemistry: Catalyst and enzyme design	20	50
	Energy: Solar conversion	10	30
	Finance: Market simulation (e.g., derivatives pricing)	20	35
	High tech: Battery design	20	40
	Manufacturing: Materials design	20	30
	Pharma: Drug discovery and development	40	80

Sources: Academic research; industry interviews; BCG analysis.

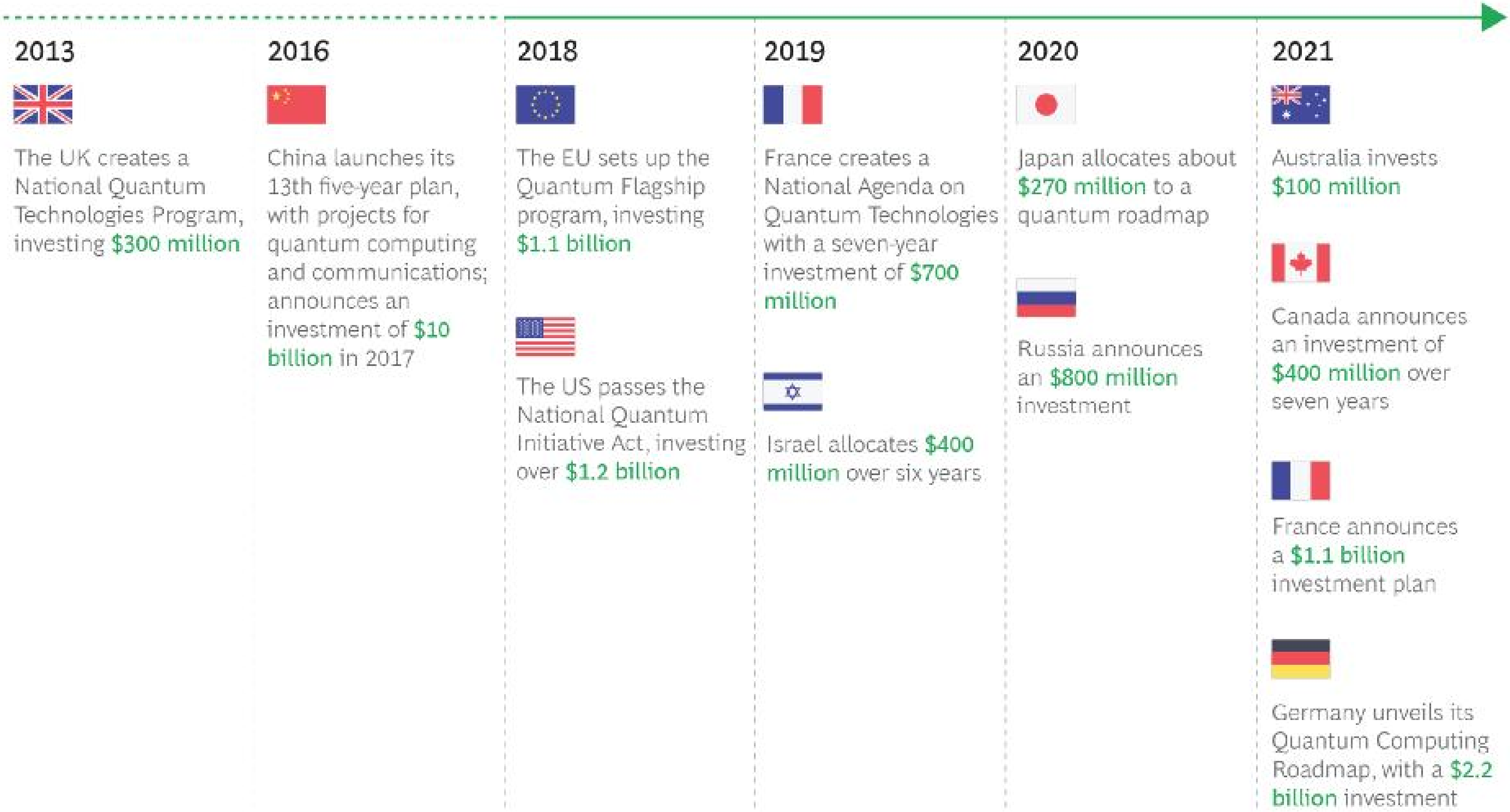
[1]Represents value creation opportunity of mature technology.

2022年8月25日，波士顿咨询集团（BCG）发布的研究报告《Can Europe Catch Up with the US (and China) in Quantum Computing?》

中国科学技术大学 陈凯

量子计算

Exhibit 3 - The EU's Competitive Start in Quantum Computing

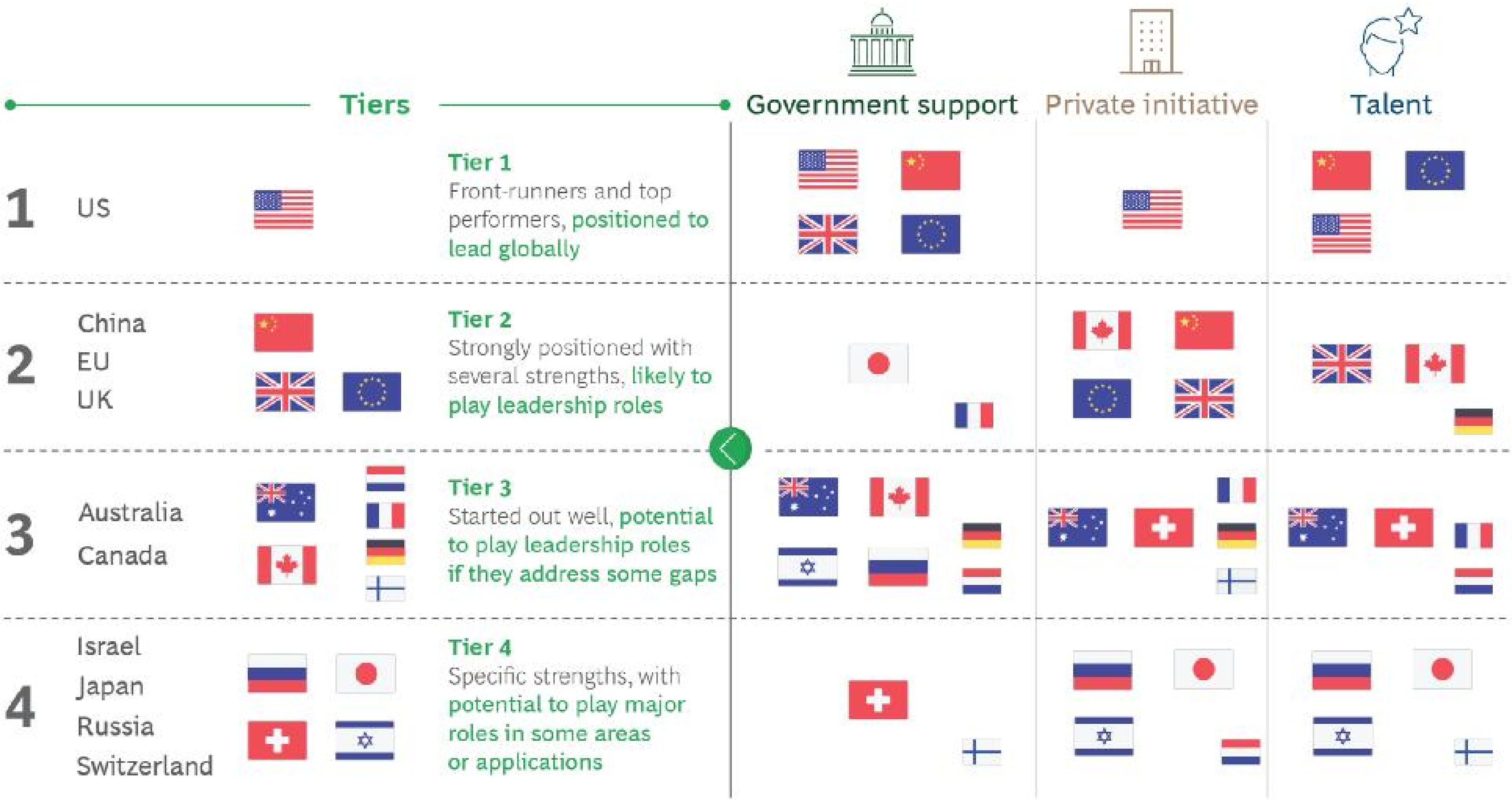


Sources: Literature search; BCG analysis.

2022年8月25日，波士顿咨询集团（BCG）发布的研究报告
《Can Europe Catch Up with the US (and China) in Quantum Computing?》

量子计算

Exhibit 4 - The 2022 Quantum Computing Country Rankings



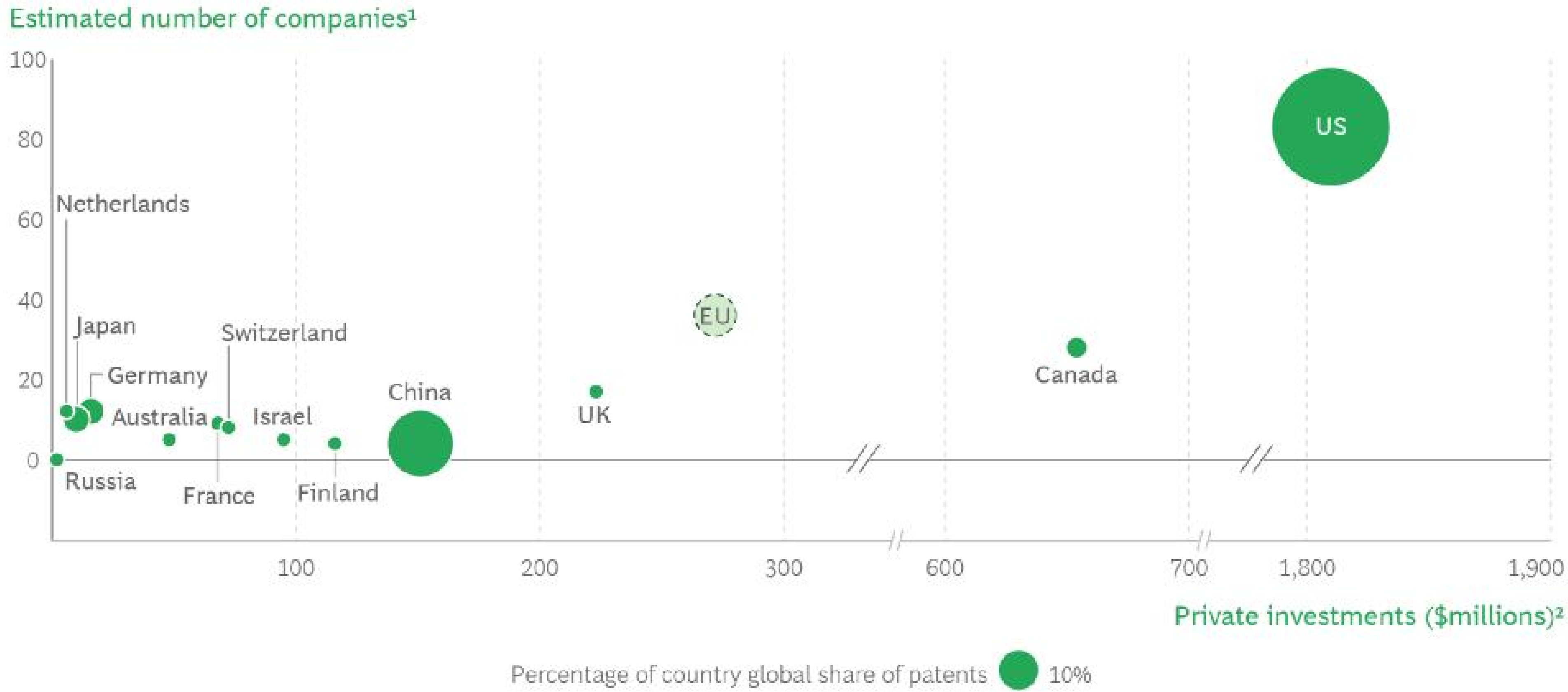
2022年8月25日，波士顿咨询集团（BCG）发布的研究报告

《Can Europe Catch Up with the US (and China) in Quantum Computing?》

中国科学技术大学 陈凯

量子计算

Exhibit 7 - The US Has the Most Startups, Private Investments, and Patents in Quantum Computing

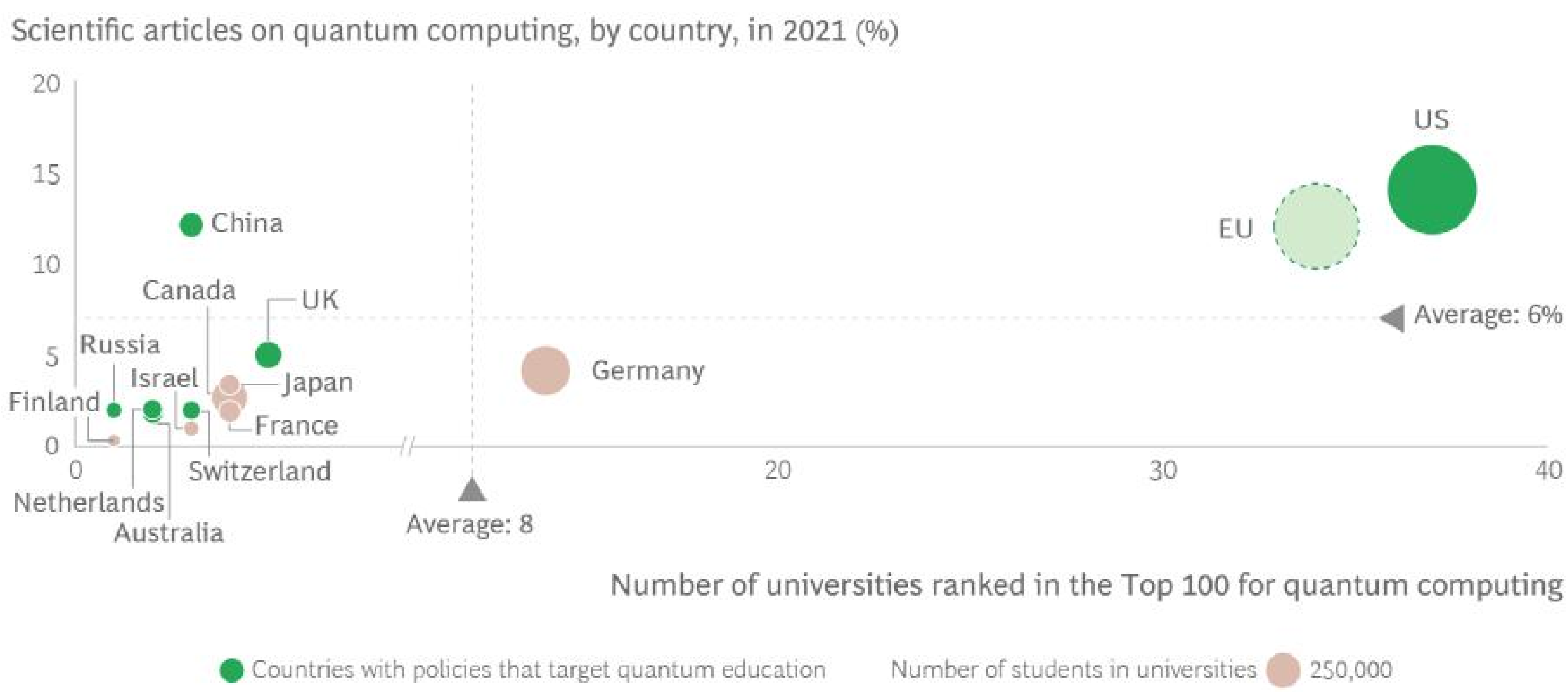


2022年8月25日，波士顿咨询集团（BCG）发布的研究报告
《Can Europe Catch Up with the US (and China) in Quantum Computing?》

中国科学技术大学 陈凯

量子计算

Exhibit 8 - The EU Is Second Only to the US in Scientific and Educational Capabilities



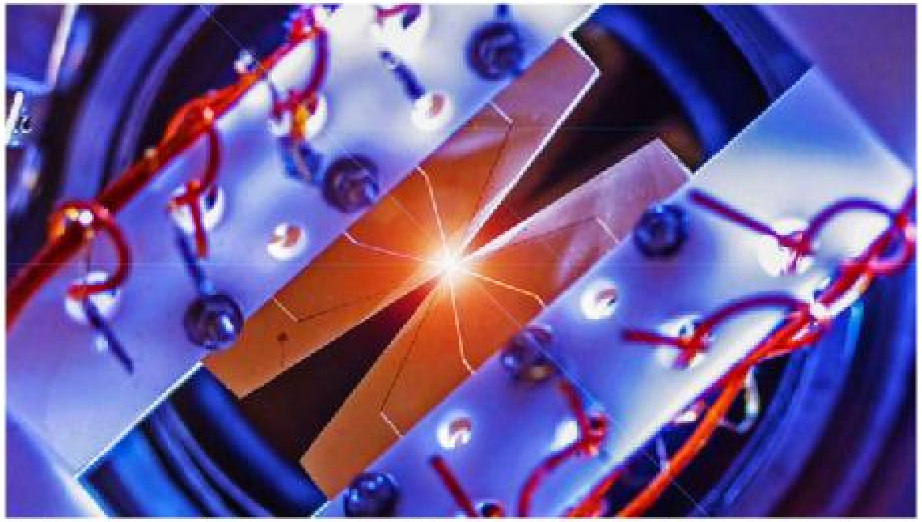
Sources: EduRank; Web of Science; Literature search; BCG analysis.

Note: The number of articles and universities for the EU represents the sum of the individual totals for each EU country.

2022年8月25日，波士顿咨询集团（BCG）发布的研究报告

《Can Europe Catch Up with the US (and China) in Quantum Computing?》

美国推进国家量子计划



Ions trapped between gold blades serve as information-carrying qubits in a prototype quantum computer. E. EDWARDS/JOINT QUANTUM INSTITUTE

Update: Quantum physics gets attention—and brighter funding prospects—in Congress

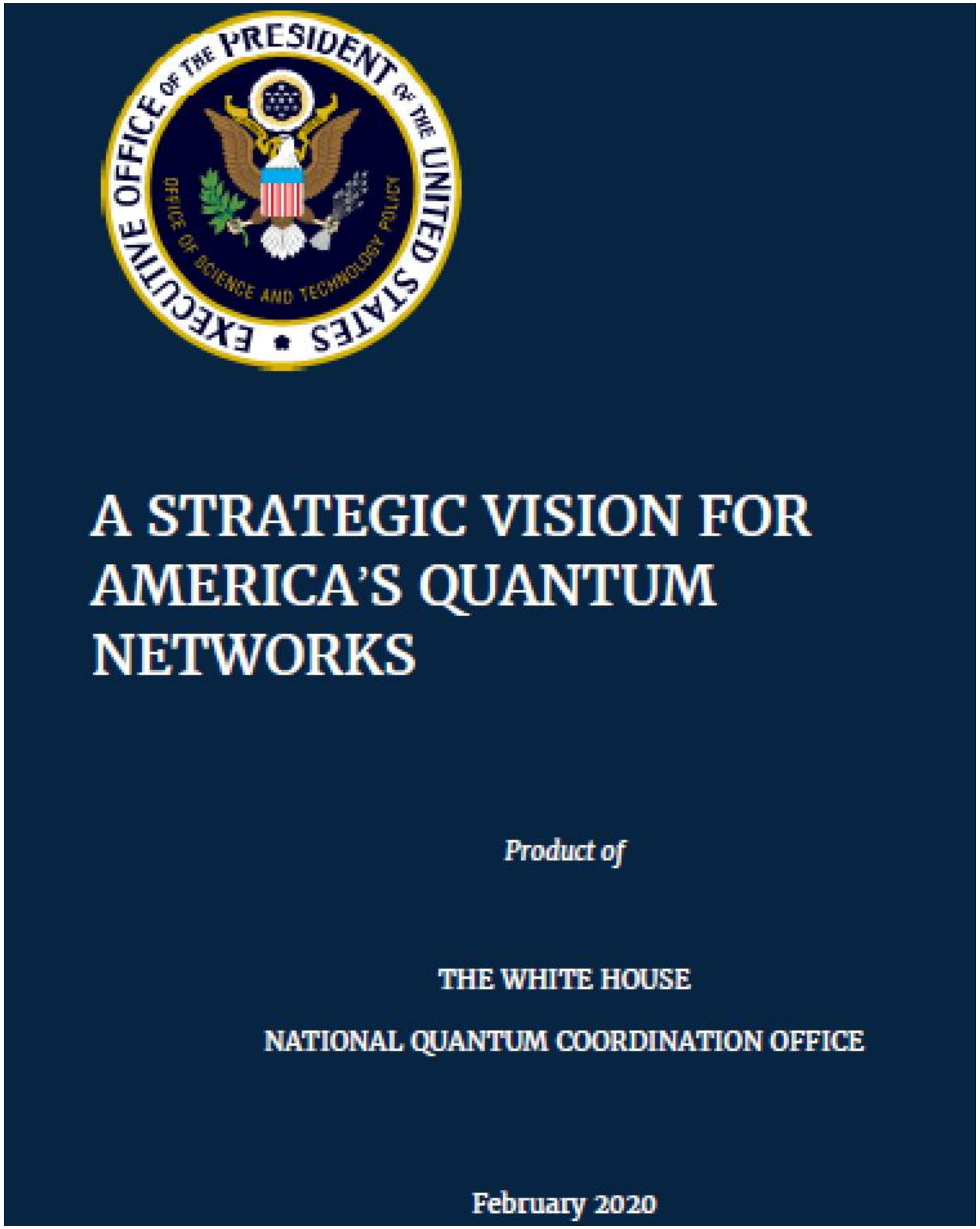
By Gabriel Popkin | Jun. 27, 2018 , 12:30 PM

COMMITTEE ON
SCIENCE, SPACE, & TECHNOLOGY
Lamar Smith, Chairman

National Quantum Initiative Act

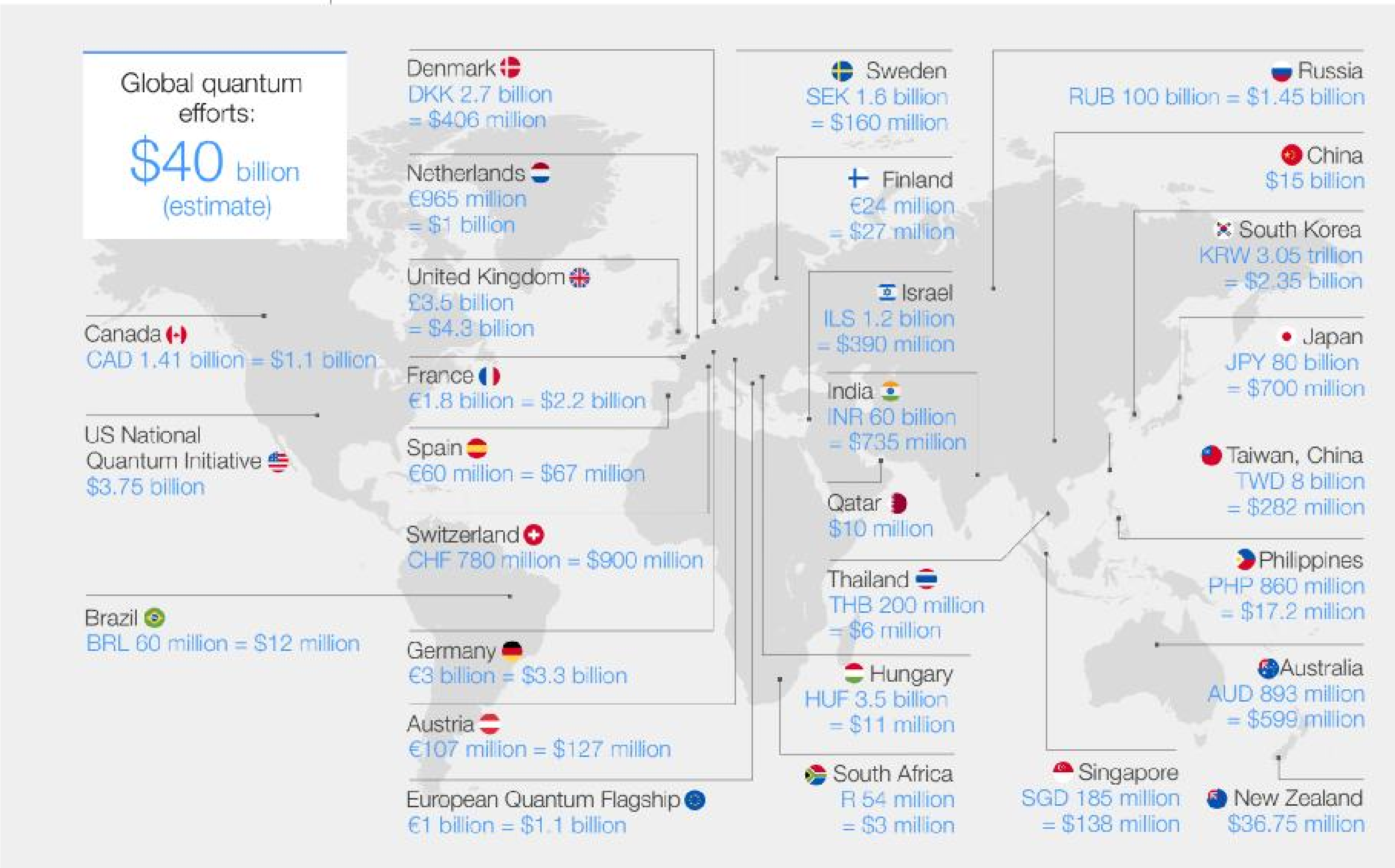
The National Quantum Initiative Act establishes a federal program to accelerate quantum research and development for the United States' economic and national security.

美国推进量子网络战略构想



世界范围内的量子技术

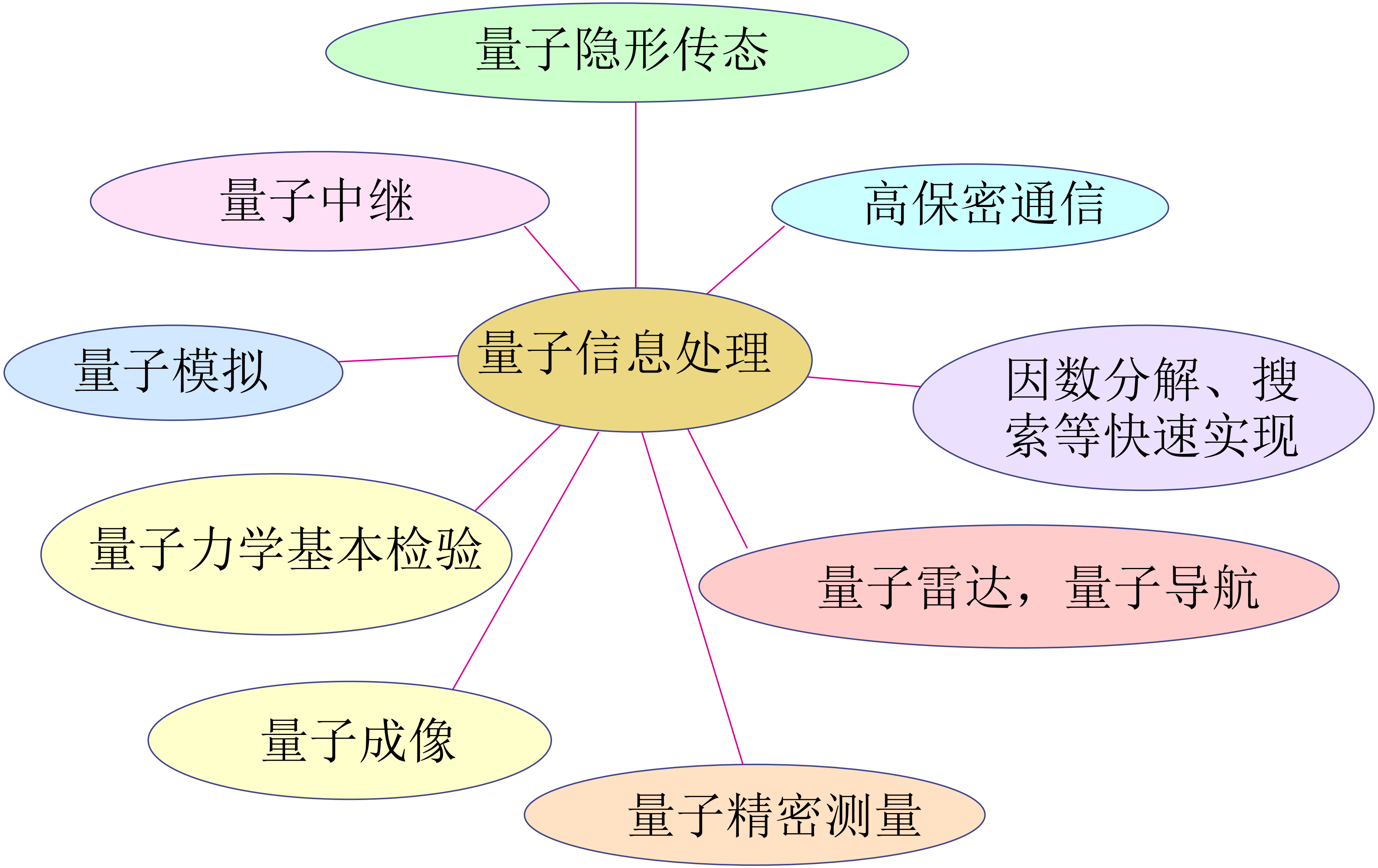
FIGURE 1 | **Public sector investments in quantum technologies worldwide**



Note: Not exhaustive; timelines for funding vary by country.

Sources: "Overview of Quantum Initiatives Worldwide 2023", *QURECA*, 19 July 2023, https://qureca.com/overview-of-quantum-initiatives-worldwide-2023/; Department of Industry, Science and Resources, Australia; ETH Domain (ETH Zurich, EPFL, PSI).

量子信息能做什么？



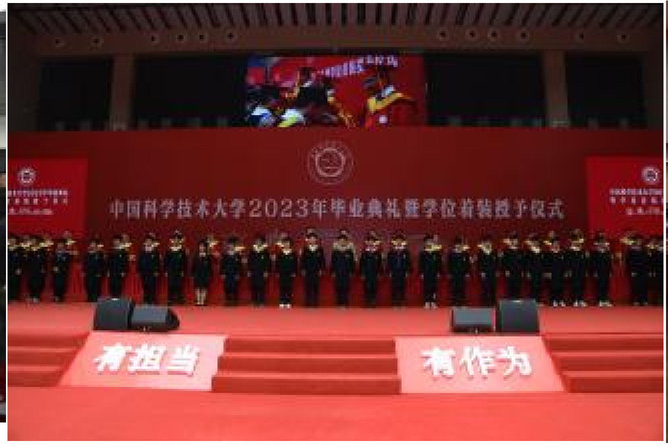
量子隐形传态
量子中继
高保密通信
量子模拟
量子信息处理
因数分解、搜索等快速实现
量子力学基本检验
量子雷达，量子导航
量子成像
量子精密测量

寄语同学们

习近平主席：科大是一所很值得敬重的大学，同学们应该为能在科大学习感到自豪。同学们要做有理想、有追求的大学生，做有担当、有作为的大学生，做有品质、有修养的大学生。

红专并进
理实交融

包信和校长:
来科大，读好书，在这里你们要读好红专并进的报国之书。
来科大，读好书，在这里你们要读好理实交融的科学之书。
来科大，读好书，在这里你们要读好追求卓越的励志之书。






课程安排

- 绪论 量子信息概念，历史和展望
- 第一章 量子体系 量子态， Schmidt分解，混合态，密度矩阵，量子测量，量子不可克隆定理等。
- 第二章 量子纠缠 纠缠和可分型，纠缠判据 ，纠缠量化，多粒子推广等
- 第三章 量子关联表现 局域实在论，Bell不等式，多体推广，纠缠与非定域性的关系等
- 第四章 量子通信 量子通信方案，通信基本形式包括量子隐形传态、稠密编码，量子密钥分发等；非理想条件下量子保密通信方案和实验，数据处理方法，安全性分析；与纠缠关系
- 第五章 量子纠错 量子纠错码，原理、构造、应用
- 第六章 量子计算 量子算法、应用
- 新进展：量子成像等（徐飞虎老师）

谢谢

http://quantum.ustc.edu.cn/

http://www.quantumcas.ac.cn/

练习题

1. 实验上随机地以$|C_0|^2$的几率制备|0>，并以$|C_1|^2$的几率制备|1>。这样类型的量子态如何刻画与描述？比较其与量子态$C_0|0> + C_1e^{i\theta}|1>$的异同（$C_0$，$C_1$，和θ均为实数）。

2. 以光学实验的偏振量子态为例，用半波片和四分之一波片的组合从|0>态制备$C_0|0> + C_1e^{i\theta}|1>$。对于实现任意的单量子比特幺正变换，试探索分析这样的组合最少的波片数目为多少，如何操作？