

# 量子计算发展白皮书

## (2019 年)

赛迪智库电子信息研究所

2019 年 9 月

## 前言

量子信息技术可以突破现有信息技术的物理极限，在信息处理速度、信息容量、信息安全性、信息检测精度等方面均能够发挥极大作用，进而显著提升人类获取、传输和处理信息的能力，为未来信息社会的演进和发展提供强劲动力。当前，人类对量子信息技术的研究与应用主要包括量子计算、量子通信和量子测量等。其中，量子计算是一种基于量子力学的、颠覆式的计算模式，具有远超经典计算的强大计算能力，将在化学反应计算、材料设计、药物合成、密码破译、大数据分析和机器学习、军事气象等领域产生颠覆性影响。

近年来，一些国家以及企业纷纷加码布局量子计算，在相关领域的技术研究和应用不断提速。在此形势下，赛迪智库电子信息研究所编写了《量子计算发展白皮书（2019年）》，阐述了量子计算的基本内涵，系统梳理量子计算的技术路线及发展路线图，介绍了国内外发展态势，并提出了我国量子计算发展面临的挑战及相关对策建议。

如有商榷之处，欢迎大家批评指正。

# 目 录

一、量子计算发展综述 .....	1
(一) 量子计算的内涵 .....	1
(二) 量子计算的发展背景与历程 .....	5
(三) 量子计算的应用展望 .....	7
二、量子计算技术与发展路线图 .....	9
(一) 量子计算关键技术 .....	9
(二) 量子计算的发展路线图 .....	16
三、国际量子计算发展现状 .....	19
(一) 主要国家的战略规划 .....	19
(二) 量子计算的技术与产业进展 .....	22
四、我国量子计算发展现状 .....	29
(一) 我国的量子计算国家战略 .....	29
(二) 我国量子计算的进展 .....	29
五、我国量子计算发展面临的问题与挑战 .....	31
(一) 关键技术研发仍属起步阶段，与国际水平存在差距 ...	31
(二) 市场尚在培育阶段，技术和应用场景不成熟 .....	31
(三) 国内企业参与度较低，缺乏全面战略布局 .....	32
(四) 人才体系单一、集中，尚未形成全面培养体系 .....	32
六、对策建议 .....	34
(一) 加强前沿科技领域产业化布局 .....	34
(二) 加大对关键核心领域的研发支持 .....	34
(三) 完善对专业人才梯队建设的全面布局 .....	34
(四) 积极构建量子计算应用生态体系 .....	35

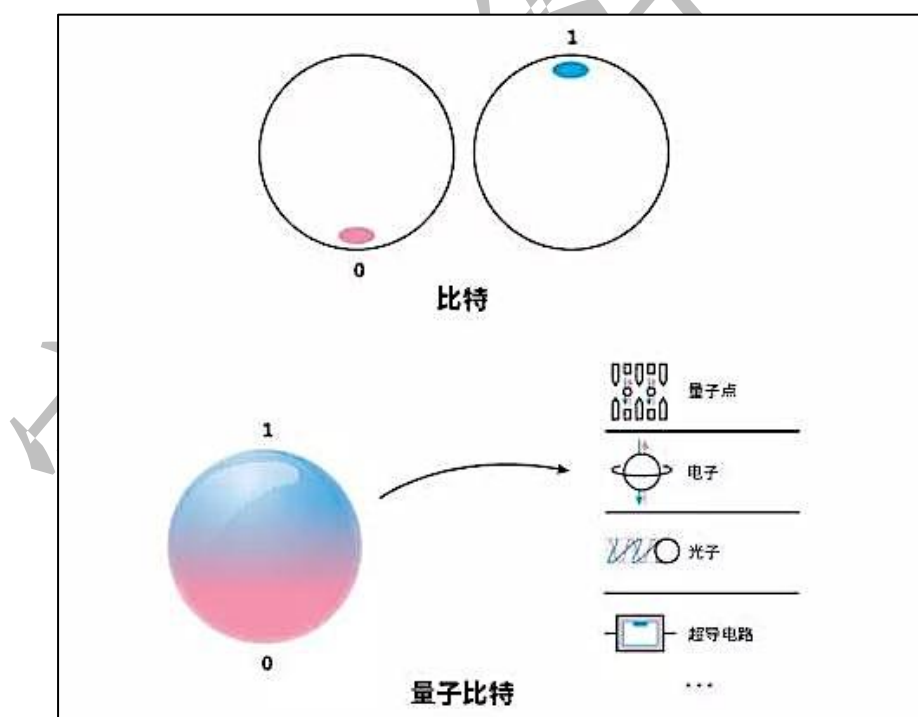
## 一、量子计算发展综述

### （一）量子计算的内涵

#### 1、量子信息科学的基本概述

量子信息科学是量子物理与信息科学交叉的新生学科，其物理基础是量子力学。量子是构成物质的基本单元，是不可分割的微观粒子的统称。量子力学就是研究和描述微观世界基本粒子结构、性质及相互作用的一门科学。量子信息技术就是基于量子力学，通过对光子、电子等微观粒子系统及其量子态进行人工观测和调控，借助量子叠加和量子纠缠等独特物理现象，以经典理论无法实现的方式获取、传输和处理信息的一类技术。

图 1 量子比特的概念示意图



数据来源：Visure Science, 2019年7月

在量子信息技术中，包含量子比特、量子叠加和量子纠缠等几个基本概念：**一是量子比特**。比特是计算机技术中信息量的基本度量单位，量子比特则是量子计算中的最小信息单位。一个量子比特可以表

---

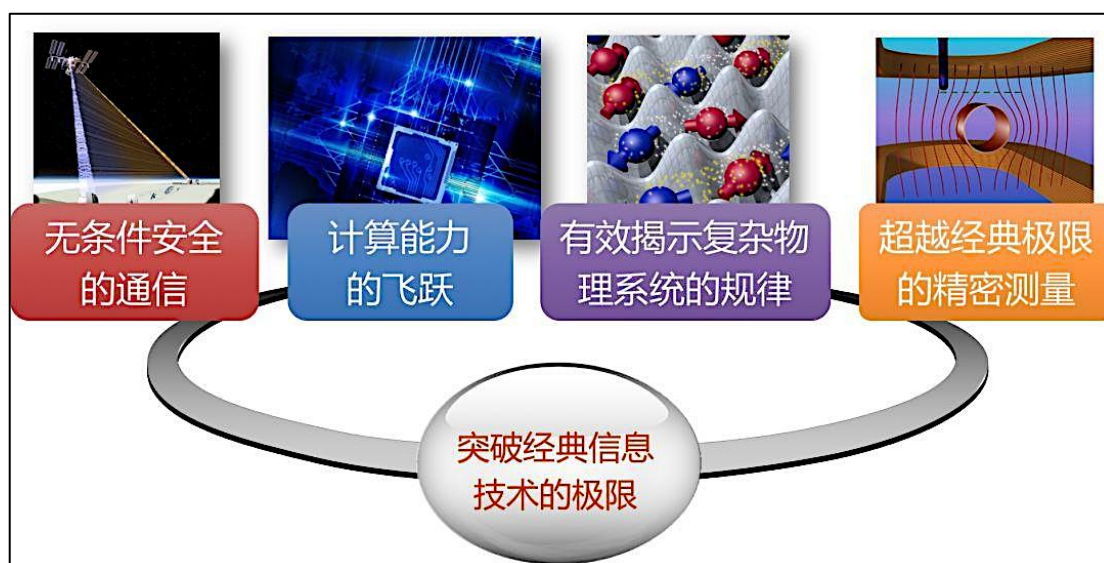
示 0、1 或 0 和 1 的叠加，因此其搭载的信息量远超智能表示 0 或 1 的经典比特。**二是量子叠加。**指一个量子系统可以处在不同量子态的叠加态上。在量子系统中，量子态是指微观粒子所处的一系列不连续的恒稳运动状态。在无外界观测干扰时，量子系统可处于一系列量子态叠加态上，也即是著名的“薛定谔的猫”。**三是量子纠缠。**指微观粒子在由两个或两个以上粒子组成系统中相互影响的现象。在量子系统中，存在量子关联的多个粒子即使在空间上被分隔开，也能够相互影响运动状态，这是量子通信等的技术基础。

当前，量子信息技术主要包括量子计算、量子通信和量子测量等三个技术领域。量子计算是基于量子态受控演化的一类计算技术。量子计算具有经典计算无法比拟的巨大信息携带和超强并行处理能力，有望成为未来几乎所有科技领域加速发展的“新引擎”。量子通信利用微观粒子的量子叠加态或量子纠缠效应等进行信息或密钥传输，主要包括量子隐形传态和量子密钥分发两类。量子通信可大幅提升通信的安全性，将对信息安全和通信网络等领域产生重大变革和影响。量子测量可基于微观粒子系统及其量子态的精密测量，完成被测系统物理量的执行变换和信息输出。量子测量主要包括时间基准、惯性测量、重力测量、磁场测量和目标识别等方向，其在测量精度、灵敏度和稳定性等方面比传统测量技术有明显优势。

## 2、量子计算的基本原理与特征

量子计算以量子比特为基本单元，通过量子态的受控演化实现数据的存储计算。量子计算机就是遵循量子力学规律，基于上述原理进行信息处理的一类物理装置。当前，量子计算机可大致分为三类：量子退火、嘈杂中型量子（NISQ）计算、容错型通用量子计算。

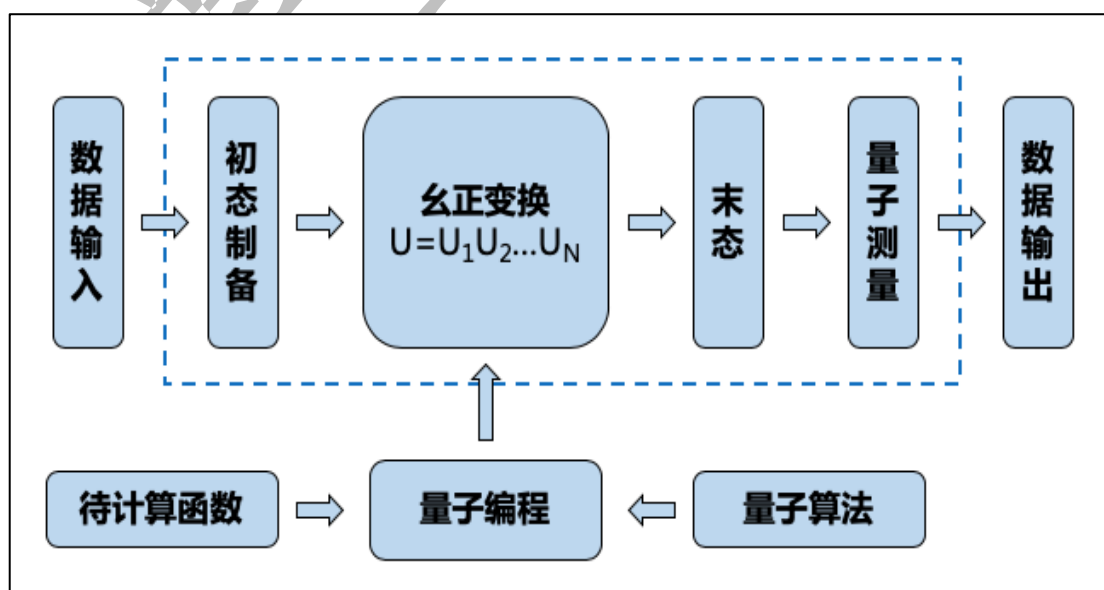
图2 新一轮量子信息科学变革的主要突破领域



数据来源：《走进新量子革命》，陆朝阳，2019年7月

一般而言，量子计算机的计算过程可以分为数据输入、初态制备、量子逻辑门操作、量子测算和数据输出等步骤。其中，量子逻辑门操作是一个幺正变换，这是一个可以人为控制的量子物理演化过程。对量子计算机的可用性而言，需要从量子比特数、长相干时间保护、高保真度量量子操作等多个维度进行综合衡量。

图3 量子计算机工作原理流程图

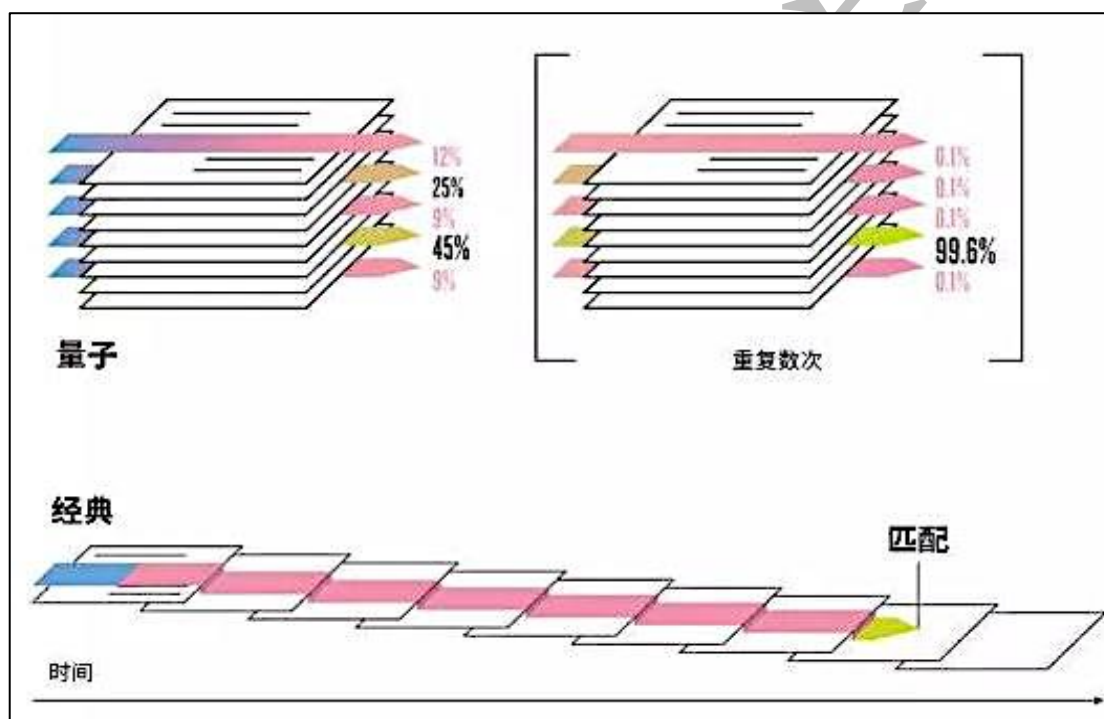


数据来源：《量子信息技术发展概况》，郭光灿，2019年7月

与经典计算相比，量子计算具有以下特点：

一是并行计算能力更强。一般地，描述  $n$  个量子比特的量子计算机需要  $2^n$  个系数数字，当  $n$  增大时所有状态所需数字很大。但由于量子叠加效应，量子计算过程中的幺正变换可以对处于叠加态的所有分量同时进行操作（也即量子并行性）。因此，量子计算机可以同时进行多路并行运算，这也是量子计算机超强信息处理能力的源泉。

图 4 量子计算的并行计算示意图



数据来源：Visure Science, 2019年7月

二是能耗更低。当前，经典计算中运算速度遇到的一大瓶颈就是能耗问题对芯片集成度的制约。有研究表明，能耗产生于计算过程中的不可逆操作。直观而言，传统芯片的特征尺寸很小（数纳米）时，量子隧穿效应开始显著，电子受到的束缚减小，使得芯片功能降低、能耗提高，这即是传统摩尔定律面临失效的原因。因此，必须将不可逆操作改造为可逆操作，才能大大提高芯片的集成度。相较之下，量子计算中的幺正变换属于可逆操作，因而信息处理过程中的能耗较低，这有利于大幅提升芯片的集成度，进而提升量子计算机算力。

---

## （二）量子计算的发展背景与历程

### 1、传统计算技术供给不足成为量子计算重要驱动因素

当前，传统计算技术迭代提升面临瓶颈，而各领域算力需求则快速攀升。一方面，集成电路技术在材料和制程工艺方面越来越逼近物理极限，摩尔定律日渐趋缓，传统计算技术的发展面临体系性困局。冯·诺依曼架构数据读写瓶颈日益凸显，程序执行时处理器在程序计数器的指引下顺序读取指令和数据，带来高延迟、低带宽等问题。此外随着数据量的日益增加，传统云计算面临网络带宽压力、服务响应缓慢、安全与隐私隐患、资源利用率低等诸多挑战。另一方面，随着信息化社会的飞速发展，人类对信息处理能力的要求越来越高，低延时、低能耗、高性能的计算需求应运而生。多种学科的融合创新发展与复杂的人类活动催生了诸多新兴计算场景，亟待利用新的计算技术与模式进行分析与评估。例如，人工智能技术的导入，带来海量、非结构化数据存储与处理需求，同时对计算技术的解释性、推理能力以及举一反三能力等方面均具有较高需求。因此，传统计算领域供给不足与需求攀升之间的矛盾愈发突出，这成为了驱动量子计算技术发展的重要因素之一。

### 2、量子计算技术突破随着科技巨头介入而提速

基于量子力学的量子信息科学是上世纪最为重要的科学发现之一，自问世以来先后孕育出原子弹、激光、核磁共振等新技术。近年来，随着人类对微观粒子系统观测和调控能力的提升，利用量子力学中的叠加态和纠缠态等独特物理特性进行信息的采集、处理和传输已经成为可能。人类对微观粒子系统的探索从“探测时代”向“调控时代”迈进，量子信息科学因此迎来新一轮快速发展。在这一轮发展浪潮中，量子信息技术的突破点集中在量子计算、量子通信和量子测量等领域。其中，量子通信的技术难度相对较小，产业化进程也最快，



---

目前人类已在积极探索基于卫星或光纤网络的长距离传输和广域组网应用。相比之下，量子计算尚未取得关键技术突破。然而，伴随着近年来国内外科技巨头的大力布局，量子计算的技术突破大大加速。例如，近十年内，在 IBM、谷歌等的推动下，量子比特数量的增加速度明显加快。尤其在近五年内，由 9 位迅速提升至 72 位，实现了 8 倍提升。此外，围绕量子计算的产业生态也初具雏形，形成了科研机构、科技巨头、初创企业协力研发，各垂直领域企业纷纷布局的发展态势。

### 3、量子计算正处于技术验证和原理样机研制阶段

迄今为止，量子计算的发展可分为三个阶段。一是 20 世纪 90 年代以前的理论探索时期。量子计算理论萌生于上世纪 70 年代，80 年代处于基础理论探索阶段。1982 年，Benioff 提出量子计算机概念，Feynman 也提出利用量子系统进行信息处理的设想。1985 年，Deutsch 算法首次验证了量子计算并行性。二是 20 世纪 90 年代的编码算法研究时期。1994 和 1996 年，Shor 算法和 Grover 算法分别提出。前者是一种针对整数分解问题的量子算法，后者是一种数据库搜索算法。这两种量子算法在特定问题上展现出优于经典算法的巨大优势，引起了科学界对量子计算的真正重视。三是 21 世纪以来，随着科技企业积极布局，量子计算进入了技术验证和原理样机研制的阶段。2000 年，DiVincenzo 提出建造量子计算机的判据。此后，加拿大 D-Wave 公司率先推动量子计算机商业化，IBM、谷歌、微软等科技巨头也陆续开始布局量子计算。2018 年，谷歌发布了 72 量子位超导量子计算处理器芯片。2019 年，IBM 发布最新 IBM Q System One 量子计算机，提出衡量量子计算进展的专用性能指标——量子体积，并据此提出了“量子摩尔定律”，即量子计算机的量子体积每年增加一倍。若该规律成立，则人类有望在 10 年内实现量子霸权。

# 每日报告

不要错过让你洞察整个商业世界的  
每日报告

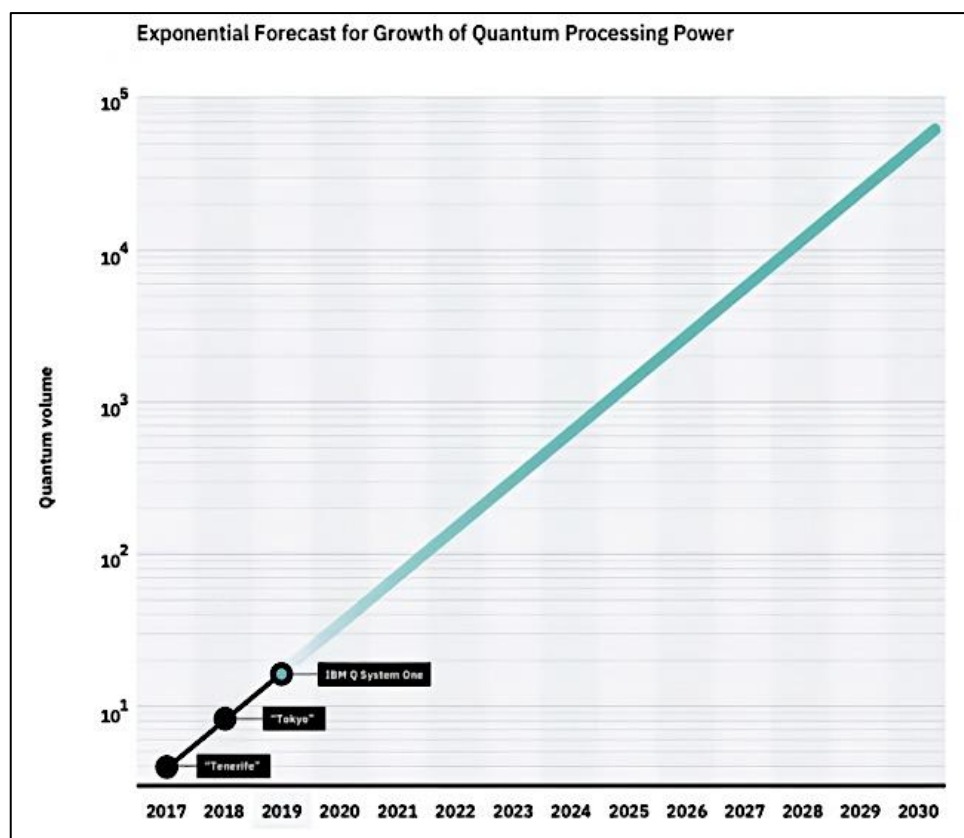
如何免费入群？扫码加好友后回复  
【入群】

每日精选3份最值得学习的资料给您  
，不定期分享顶级外文期刊



撩他！撩他！

图 5 IBM 量子计算系统开发路线图（量子摩尔定律）



数据来源：IBM，2019年3月

### （三）量子计算的应用展望

当前，量子计算的产业化仍处于最初阶段。因此，在未来 5-10 年内，倘若量子计算技术未能取得跨越式突破，则其市场规模将较为有限。据 BCC Research 预测，全球量子计算市场规模有望于 2022 年超过 1.5 亿美元，2027 年有望达到 13 亿美元。此外，据波士顿咨询报告，预计到 2035 年，全球市场规模将达到 20 亿美元。从中远期来看，若量子计算技术迭代速度超出预期，则 2035 年的市场规模可突破 600 亿美元，2050 年则有望接近 3000 亿美元。相比之下，当前全球计算市场的总规模约为 8000 亿美元。

量子计算具有经典计算技术难以企及的并行计算能力和信息携带量，有望成为满足未来计算需求、加速科技创新的新引擎。在可预期的未来，量子计算机不会完全取代经典计算机，但会依托其在并行

---

计算、量子行为模拟等方面的独特优势，在算力需求极高的特定场景中发挥作用。例如，量子计算有望用于基础科研、化工、能源、材料、人工智能、信息安全、加密通信、太空探索等领域，对各国科技创新、产业发展乃至经济社会的各个方面带来颠覆性影响。

从中短期来看，量子计算主要可在量子模拟、量子优化和量子增强人工智能等方面发挥作用。

**量子模拟。**在传统计算中，由于难以精确求解方程，当前的计算化学方法严重依赖近似值。相比之下，量子计算所依赖的量子力学是自然界最基本的物理原理，因此量子计算天然适于模拟各类物理、化学过程，能够在更长时间范围内准确模拟分子行为，因此能够大幅提升建模精度，在生物药物、能源材料、化工材料等领域提升研发效率、缩短产品开发周期。例如，在生物医药领域，药物研发的前、中、后期都需要大量数据计算，尤其在中期环节，需要极高的计算能力以支撑分子性质模拟和药品功能设计。

**量子优化。**优化问题需要从诸多解决方案中找到最优解，对传统计算而言，在大规模物流网络等复杂系统中，设计满足各种需求的最优路线的计算量很大。例如，对仅有数百个集散地的物流网络而言，而穷尽所有可能性，传统计算机需要数十亿年时间。量子计算则能大幅提升计算效率，从而在物流运输、航空旅行、交通管制、金融资产管理、网络基础设施等领域中提升运营效率、减少碳排放等。

**量子增强人工智能。**人工智能对算力需求的一大特征即海量异构数据的并行计算，这也是传统 CPU 芯片难以胜任，从而导致 GPU、FPGA、ASIC 等芯片在人工智能领域大受欢迎的原因。如上文所述，量子计算的超强算力源自量子并行性，因而其十分适于进行人工智能所需的并行计算。当前，量子计算已经开始用于提升机器学习在数据聚类等领域的能力。

## 二、量子计算技术与发展路线图

量子芯片以及量子算法是研发量子计算机的两个关键技术环节。量子芯片即为量子计算机的物理实现与硬件系统，量子算法则是将量子计算机计算效率最大化的软件系统。

### （一）量子计算关键技术

#### 1、量子芯片

表 1 量子芯片技术体系对比

技术体系 品质因数	超导	半导体量子点	离子阱	光学	量子拓扑
比特操作方式	全电	全电	全光	全光	NA
量子比特数	20	2	20	10	从 0 到 1 的过程中
相干时间	~50us	~100us	>1000s	~10us	受拓扑保护，理论上可以无限长
两比特门保真度	99.4%	92%	99.9%	97%	理论上可以到 100%
两比特门操作时间	~50ns	~100ns	~10us	NA	NA
可实现门数	~10 <sup>3</sup>	~10 <sup>3</sup>	~10 <sup>8</sup>	NA	NA
主频	~20Mhz	~10Mhz	~100Khz	NA	NA
业界支持	谷歌、IBM、英特尔、耶鲁、ETH	普林斯顿、代尔夫特、中科大	IonQ、NIST、桑迪亚国家实验室、中科大	中科大、MIT	微软、代尔夫特、清华、北大、物理所

数据来源：华为公司，2019年7月

将量子力学理论与计算机技术相结合的概念由美国物理学家 Feynman 于 1982 年首次提出。3 年后，英国牛津大学的 Deutsch 团队

---

对量子计算机的概念进行了进一步阐述，并提出研究如何由量子逻辑门构成逻辑网络是实现通用量子计算机的核心。目前，量子计算的各类物理体系虽都取得了较大进展，但未来哪种物理实现系统最终可研制成通用量子计算机尚无定论。

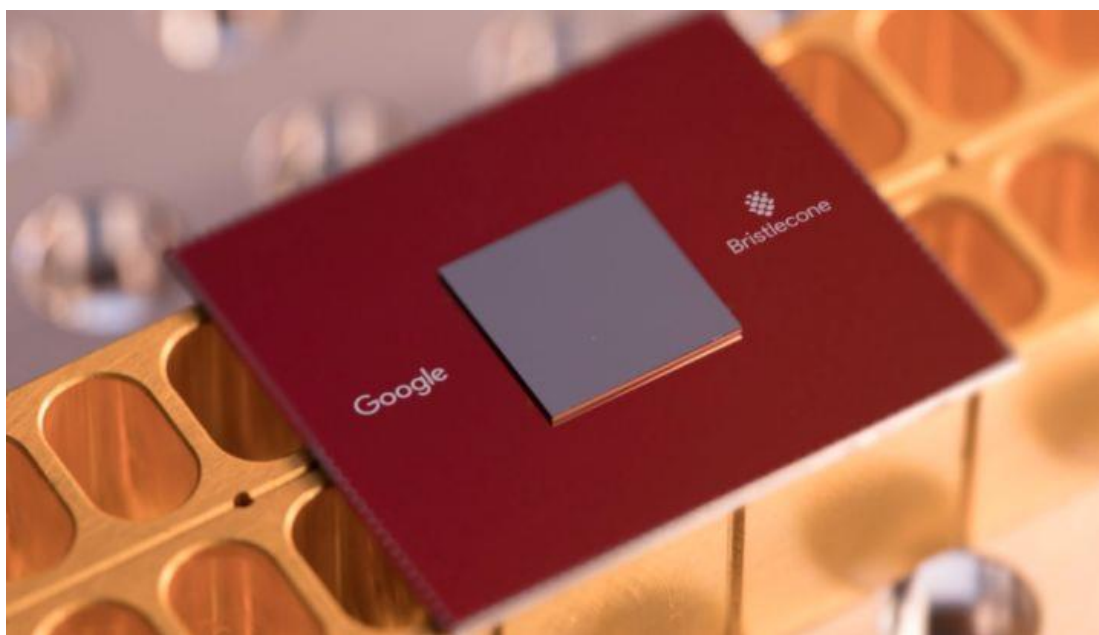
### （1）超导量子计算

超导量子计算利用超低温“冻结”粒子的运动进而实现粒子状态的控制，量子比特有超导相位、超导磁通和超导电荷三种形式。超导量子计算的核心单元是约瑟夫森结，约瑟夫森结是一种“超导体—绝缘体—超导体”的三层结构。利用超导约瑟夫森结来观测宏观量子现象最早由 Leggett 于 1985 年提出，随后研究人员在超导约瑟夫森结器件中陆续观测并实现了能级量子化、量子隧穿、量子态叠加、量子相干振荡等现象。

超导量子计算是目前进展最快最好的一种固体量子计算实现方法。由于超导量子电路的能级结构可通过外加电磁信号进行调控，电路的设计定制的可控性强。同时，得益于基于现有的成熟集成电路工艺，超导量子电路具有多数量子物理体系难以比拟的可扩展性。但是在实现超导量子比特体系过程中，由于量子体系的不可封闭性，环境噪声、磁通型偏置噪声等大量不易操控的自由度导致耗散和退相干。此外，超导量子系统工作对物理环境要求极为苛刻（超低温）均是超导量子计算实现过程中不可避免的问题。

目前谷歌、IBM、英特尔等企业均在积极开展超导量子比特实验研究。2018 年 3 月 3 日，谷歌量子人工智能实验室发布狐尾松（Bristlecone）量子处理器。该处理器可实现 72 个量子比特长度上的单比特门操纵，单量子比特门最佳保真度 99.9%，双量子比特门的最佳保真度 99.4%。

图 6 谷歌狐尾松 (Bristlecone) 量子处理器



数据来源: TechSpot, 2019年7月

## (2) 半导体量子点

半导体量子点也是基于现有半导体工艺的一种量子计算物理实现方法。在平面半导体电子器件上制备出的单电子晶体管,其电子服从量子力学运动规律,电子自旋的向上和向下组成的系统可作为一个量子比特。根据电子的泡利不相容原理,通过自旋和电荷之间的关联,可以通过普通的电子开关(门)对电子自旋进行控制,完成包括单量子比特操作、两量子比特操作及结果的读出等在内的对电子自旋编码的量子比特的各种操作<sup>①</sup>。

半导体量子点体系具有良好的可扩展性,量子点的原子性质可以通过纳米加工技术和晶体生长技术来人为调控,比一般的量子体系更容易集成。此外,半导体量子点的制备可与现有半导体芯片工艺完全兼容,因而成熟的传统半导体工艺可为半导体量子点的技术实现与后续部署带来极大便利。但是半导体量子点体系受周围核自旋影响严重,面临退相干以及保真度不足两大挑战。

<sup>①</sup> 陈瑞亭,《量子计算物理实现体系》,《电脑知识与技术》,2015年12月,第139~140页。

---

技术进展方面，荷兰代尔夫特大学的 Kouwenhoven 团队于 2004 年在半导体器件上首次实现了自旋量子比特的制备。3 年后，代尔夫特大学的 Vanderspyen 团队在同一块半导体量子点器件上实现了量子比特制备、量子逻辑门操作、量子相干与测量等自旋量子计算的全部基本要素。2014 年新南威尔士大学获得了退相干时间 120 微秒、保真度 99.6% 的自旋量子比特。2017 年，日本理化研究所在硅锗系统上获得了退相干时间达到 20 微秒、保真度超过 99.9% 的量子比特。2018 年中国科技大学郭光灿院士团队制备了半导体六量子点芯片，并实现了三量子比特的 Toffoli 门操控，成为国际上首个在半导体量子点体系中实现的三量子比特逻辑门。

### （3）离子阱量子计算

离子阱的技术原理是利用电荷与电磁场间的交互作用力牵制带电粒子体运动，并利用受限离子的基态和激发态组成的两个能级作为量子比特<sup>②</sup>。尽管离子阱技术本身的发展可以追溯到 1980 年，但是利用离子阱技术实现量子计算由奥地利奥地利因斯布鲁克大学（Innsbruck）Blatt 实验室的 Circa 和 Zoller 于 1995 年首次提出。2003 年，该实验室实现利用失谐激光束照射和激光冷却控制非门，同年该实验室第一次成功地利用离子阱技术实现了 Deutsch-Jozsa 算法。

离子阱量子计算具有量子比特品质高，相干时间较长以及量子比特的制备和读出效率较高三大特点。然而，离子阱技术目前仍面临四大难点：一是离子阱暂时难以储存多条离子链；二是由于外加激光强度、频率及相位的不稳定，且离子对电场噪声敏感导致的消相干问题；三是可扩展性差；四是体积庞大，小型化尚需时日。

目前开展离子阱量子计算技术研究的有 IonQ、NIST、Sandia National Lab、ETH。IonQ 于 2018 年 12 月 11 日公布了两个新型离子

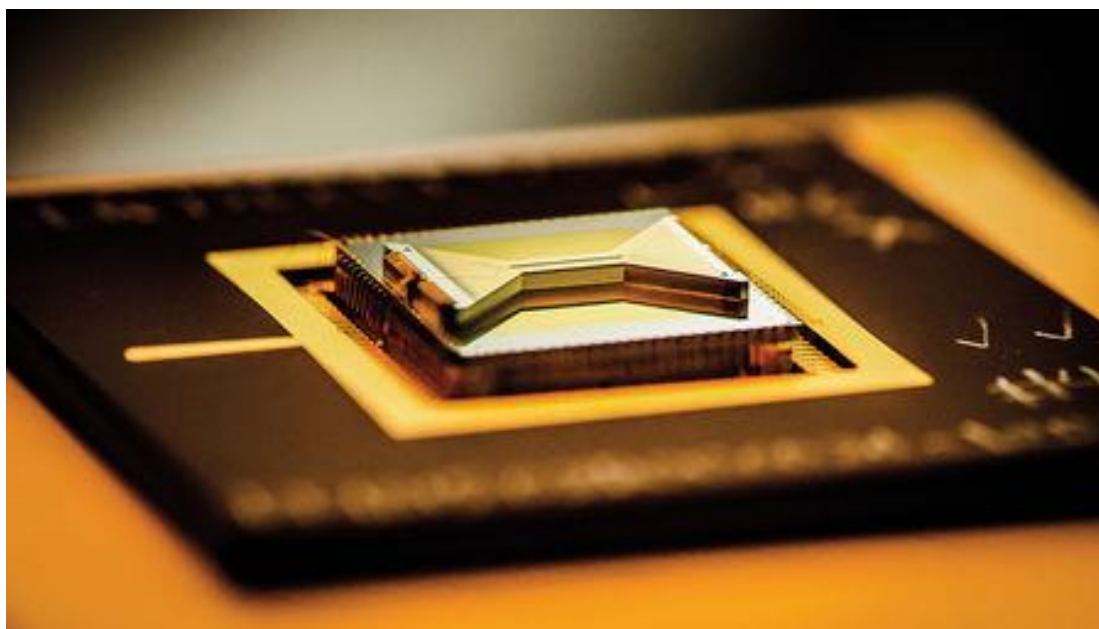
---

<sup>②</sup> 陈瑞亭，《量子计算物理实现体系》，《电脑知识与技术》，2015 年 12 月，第 139~140 页。



阱量子计算机，具有 160 个存储量子比特，可实现 79 个量子比特长度上的单比特门操纵，11 比特长度上双比特操纵。保真度方面，单比特平均保真度 99%，双比特平均保真度 98%。

**图 7 IonQ 芯片照片**



数据来源：ciencemag, 2019年7月

#### **(4) 光学量子计算**

光学量子计算（OQC）是基于测量的量子计算方案，利用光子的偏振或其他自由度作为量子比特，光子是一种十分理想的量子比特的载体，以常用的量子光学手段即可实现量子操作。光学量子计算根据其物理架构分为两种：KLM 光学量子计算以及团簇态光学量子计算。KLM 光学量子计算仅使用单光子、线性光学和测量，允许通过和可扩展光学量子计算，目前已经实现了光子-光子之间的两量子位的逻辑操作。团簇态光学量子计算由一个高度纠缠的成为团簇态的多粒子态组成，与单量子测量和前馈相结合，实现可扩展的通用量子计算，具有降低整体复杂性和放宽测量过程的物理需求，以及物理资源的更有效利用等技术优势。

由于光子与环境相互作用很小，光学量子计算具有相干时间长、操控手段简单、与光纤和集成光学技术的相容性，以及简单的资源可

---

扩展性等优点。但也正是由于光子之间相互作用微乎其微，导致两量子比特之间的逻辑门操作难以实现。

技术进展方面，目前中国研究团队已经在实验室产生了同时具备高系统效率（33%）、高纯度（97%）和高全同性（90%）的高品质单光子源和基于参量下转换的 10 光子纠缠。在此基础上，光学量子计算的基本操作（如概率性的控制逻辑门）和各种算法（大数分解算法、数据库搜索、线性方程组求解算法、机器学习、波色取样）的简单演示验证也已经实现。在光学量子计算可集成研究方面，麻省理工学院、牛津大学、布里斯托大学、维也纳大学、昆士兰大学等小组基于硅光子学、铌酸锂波导、二氧化硅波导等平台，通过刻蚀或激光直写等方式产生 10 个通道左右的量子线路用于少数光子数的原理性研究。单光子探测方面，美国国家技术标准局、荷兰代尔夫特大学等机构以及可以生产同时具备高探测效率（93%），高重复频率（150MHz）的超导纳米线单光子探测器。

### （5）量子拓扑计算

拓扑量子计算建立在全新的计算思路之上，应用任意子的交换相位，交换过程的“编辫”程序实现量子计算的信息处理<sup>③</sup>。拓扑学研究几何形象在几何元素的连续变形下保持变的性质。如果构成量子比特的元素是拓扑不变的，基于这些量子比特的运算结果也具有拓扑不变性。由此构造的量子计算对环境干扰、噪音、杂质有很大的抵抗能力。但拓扑量子计算尚停留在理论层面，实际上还未把这些理论付诸成器件化的现实。

## 2、量子算法

与传统计算机同理，为便于控制并使用通用量子计算机，可利用量子计算机程序设计语言作为人与量子计算机之间的传递信息的媒

---

<sup>③</sup> 方粮，刘汝霖，汤振森，隋兵才，池雅庆，《量子计算机：量子算法与物理实现》，《计算机工程与科学》，2012 年第 34 卷第 8 期，第 32~43 页。

---

介。现有量子算法一般固化于专用量子计算设备中，如果需要改变量子算法就必须重新设计量子计算设备。因此，量子计算机程序设计语言将成为未来通用量子计算机算法实现过程中必不可少的系统软件。

### （1）舒尔算法

1994 年，美国麻省理工贝尔实验室数学家彼得·舒尔（Peter Shor）提出了一个针对整数分解问题的量子算法，即舒尔算法（Shor's Algorithm）。舒尔算法包含两个部分：一是将因子分解问题转化成周期问题，该部分可以用传统方式实现；二是使用量子手段来搜寻这个周期，这一部分是舒尔算法中体现量子加速的主要部分。

大整数分解问题是数论中的经典困难问题，在舒尔算法提出之前，没有已知算法可以在多项式时间内分解大整数分解问题。著名的公钥密码体制 RSA 正是基于大整数分解问题的困难性来进行加密的。据微软研究院的人士估计，破解 2048 比特强度的 RSA 密钥可能需要当今最快的经典计算机耗费 10 亿年以上的的时间，而运行舒尔算法的量子计算机只需要不到 100 秒就可以完成。

舒尔算法的提出，不仅对 RSA 密码体制构成了威胁，更让人们认识到，量子计算具有非常强大的计算与应用潜力。从而促使量子计算机的研究迈上一个新的台阶。

### （2）格罗弗算法

1996 年，同在麻省理工贝尔实验室的格罗弗提出了格罗弗搜索算法（Grover's Algorithm），格罗弗算法的实现基于概率幅放大。与其他的量子算法相同，格罗弗算法亦是概率性的。该算法为数据库搜索算法，数据库相当于是一张存有未知函数的所有输出值的表，以对应的输入值为索引。

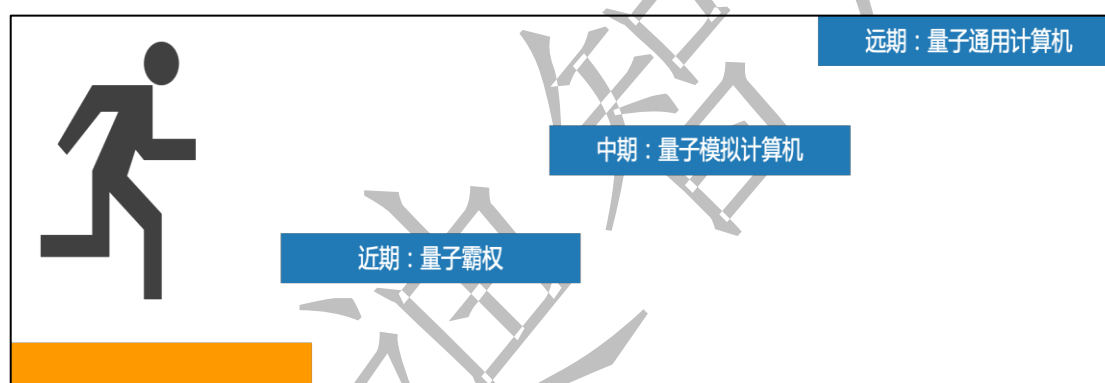
量子计算的格罗弗搜索算法远超出了经典计算机的数据搜索速度，但不像其他的量子算法可能会比相应的经典算法有指数级的加快，

格罗弗算法对许多计算问题的传统算法呈现平方加速。即便如此，加速程度也相当可观，格罗弗算法可以在大约 264 次迭代内穷举破解一个 128 比特的对称密钥，在大约 2128 次迭代内穷举破解一个 256 比特的密钥。

## （二）量子计算的发展路线图

虽然国际上量子计算各种物理实现的原理性验证发展迅速，都取得了较大进展，并且有加速现象，但国际上公认短期内无法实现量子通用计算机，量子计算的发展预计将分为近期、中期与远期三个阶段。

图 8 量子计算发展路线图

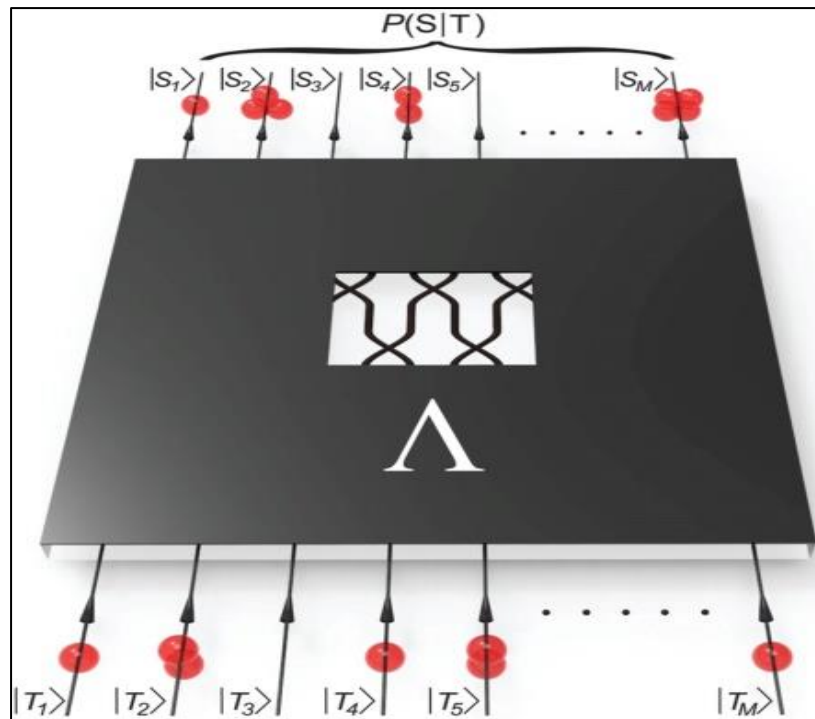


数据来源：赛迪智库，2019年7月

### 1、近期：量子霸权

量子霸权是指量子计算机拥有一项超越现有经典计算机的计算能力，则可称该量子计算机实现量子霸权。由于目前具体实现通用量子计算机仍尚有时日，但只需实现实用化的专属目的的量子计算机即可带来巨大的学术以及工业价值。随着量子计算物理体系研究进展不断突破，量子霸权的实现正日益临近，而称霸标准也已成为量子计算领域最为重要的问题之一，玻色采样即为一种针对光子（玻色子）系统的量子霸权测试案例。但量子霸权仅为技术研发初期的的一种特有概念形式，实现量子霸权离实现真正的量子计算机仍将有很大距离。

图 9 波色采样示意图



数据来源：中国科学技术大学，2019年7月

## 2、中期：量子模拟机

量子模拟机利用可控的人造量子系统实现对复杂物理过程的高效量子模拟。目前业界主流的模拟方案有两类，一类是存储量子状态的所有振幅，此类模拟方案，基本都在超级计算机上实现，因为存储 45 比特的量子状态需要 Petabyte 量级的内存，在存储这么多数据的同时对该量子态进行操作并进行计算，需要不断地在不同的计算节点之间交换数据，这样的通讯开销对于普通云服务是难以承受的。另一类对于任意振幅都可以迅速计算得到结果。任务拆分后可以将子任务十分均衡地分配到不同节点，极少的通信开销使得模拟器适配现在广泛提供服务的云计算平台。

### 3、远期：通用量子计算机

18

### 三、国际量子计算发展现状

#### （一）主要国家的战略规划

当前，量子技术研究已成为世界科技研究的一大热点，世界主要国家高度关注量子信息技术发展，纷纷加大政策和资金支持，力争抢占新兴信息技术制高点。

美国从上世纪 90 年代即开始将量子信息技术作为国家发展重点，在量子相关学科建设、人才梯队培养、产品研发及产业化方面进行大量布局，联邦政府机构对量子计算领域的支持在每年 2 亿美元以上。近两年来，美国政府频繁参与量子计算布局。2018 年，美国推出《国家量子计划法案》，计划拨付更多资金，全力推动量子科学发展。2019 年，美国政府发布未来工业发展计划，将量子信息技术等四大关键技术视为未来科技和产业未来的“基础设施”，认为发展量子信息科学能够保持美国在全球产业变革中的主导地位。政策上的持续加码，正不断提升量子计算在美国未来发展中的地位。

**表 2 美国有关量子计算的政策计划**

年份	事项
2002	制定了“量子信息科学和技术发展规划”
2004	制定了量子计算发展的主要战略步骤和时间安排
2006	创设联合量子研究所（JQI），加大科研力量的融合力度
2007	将量子科技列入战略规划，加大政策支持
2009	发布“量子信息科学跨学科研究计划”
2009	出版《量子信息科学的联邦愿景》
2014	创设量子信息和计算机科学联合中心（QuICS）

年份	事项
2015	将量子信息科学列入战略投资领域
2015	提出 2015-2030 财年量子信息科学研究目标与基础设施建设目标
2016	发布《推进量子信息科学发展：美国的挑战与机遇》
2016	发布《与基础科学、量子信息科学和计算交汇的量子传感器》
2016	海陆空三军量子科学与工程制造项目（QSEP）
2016	推进工程中通信量子信息研究（ACQUIRE）项目
2018	编制《美国国家量子信息科学战略概述》，提出了美国量子信息科学发展的四大目标、六大举措
2018	签署《国家量子计划法案》，将制定量子信息长期发展战略，未来 5 年向量子相关研发领域投入 12 亿美元资金
2019	发布未来工业发展规划，将量子信息科学视为美国未来科技和产业发展的四大“基础设施”

数据来源：赛迪智库，2019年7月

欧盟在上世纪 90 年代即发现了量子计算的巨大潜力，开展相关的合作研究。进入 21 世纪，欧盟从战略层面推出相关的规划及技术标准，力图率先在量子计算上取得突破，成为未来欧盟技术发展战略的基石。

英国、德国和荷兰等国也出台了针对量子计算、量子通信等量子技术的支持计划。英国已启动“国家量子技术计划”，计划投资超过 10 亿英镑建立量子通信、传感、成像和计算四大研发中心，推动产学研合作；德国提出“量子技术——从基础到市场”框架计划，希望推动实现量子技术的产业化发展；荷兰已制定了 10 年期量子计算发展



计划。

**表 3 欧洲有关量子计算的政策计划**

年份	国别	事项
2013	英国	建立了量子计算研究院
2014	英国	制定 5 年量子技术计划，每年投入 2.70 亿英镑支持量子技术产学研发展
2015	英国	发布《英国量子技术路线图》，将量子技术上升为影响未来国家创新力和国际竞争力的重要战略
2015	荷兰	制定了 10 年期量子计算发展计划
2016	欧盟	发布《量子宣言（草案）》，明确了发展重点
2016	英国	制定量子技术劳动力培训计划，加强人才支撑
2016	德国	宣布 QUTEQA 计划，将投资 6.5 亿欧元
2017	英国	发布《量子技术：时代机会》，提出建立一个政府、产业、学界之间的量子技术共同体
2018	欧盟	启动“量子技术旗舰计划”，将为从基础研究到工业化，为整个欧洲量子价值链提供资助

数据来源：赛迪智库，2019年7月

日本于 2001 年起开始量子技术的布局，将该技术作为重点开发研究之一。2013 年，日本成立量子信息和通信研究促进会以及量子科学技术研究开发机构，将在未来 10 年投入 400 亿日元支持量子技术研发。2017 年 2 月，日本量子科技委员会发表了名为《关于量子科学技术的最新推动方向》的中期报告，为未来日本在量子科学技术领域

的发展明确了方向。

韩国重点发展量子通信领域，于 2014 年发布《量子信息通信中长期推进战略》，目标为在 2020 年成为全球量子通信领先国家，在量子通信领域的积累使得韩国在量子计算领域已具备部分发展基础。

**表 4 日本、韩国有关量子计算的政策计划**

年份	国别	事项
2001	日本	将量子通信技术列入国家级高技术研究开发计划
2011	日本	下设“光·量子束研发作业委员会”
2014	韩国	发布《量子信息通信中长期推进战略》
2015	韩国	电信运营商 SKT 开始分阶段建设境内量子通信网络
2016	日本	将“光 / 量子技术”列入《第五期科学技术基本计划（2016-2020）》的核心基础技术
2017	日本	发布《关于量子科学技术的最新推动方向》

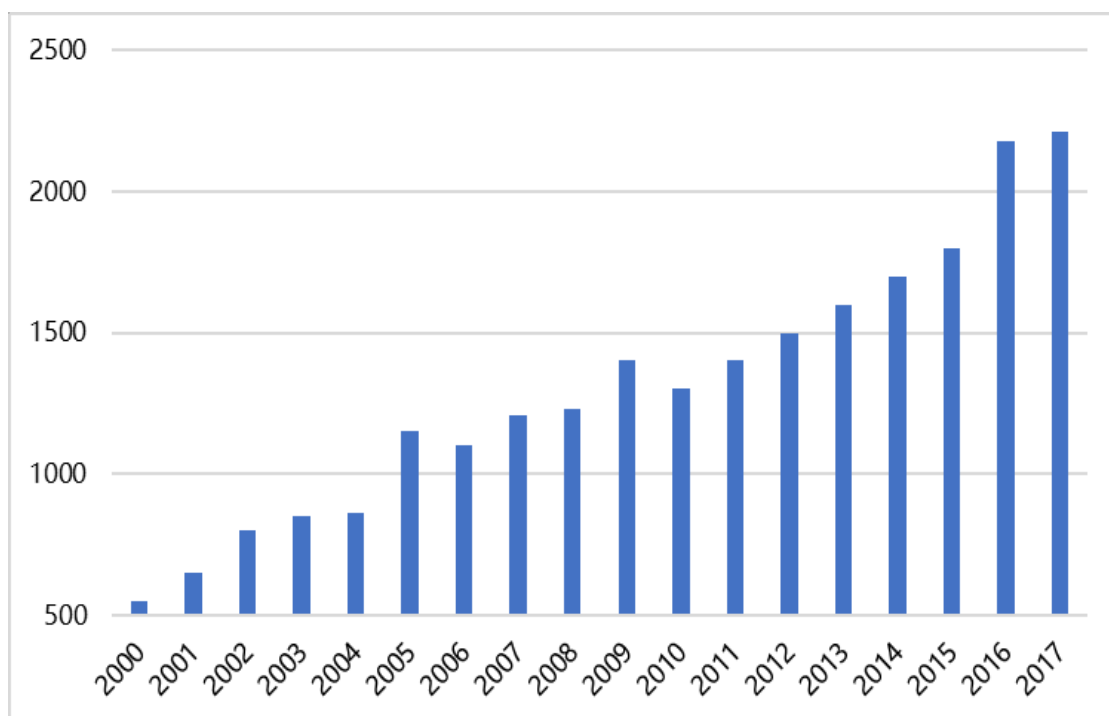
数据来源：赛迪智库，2019年7月

## （二）量子计算的技术与产业进展

### 1、全球量子计算产业发展水平不断提升

从上世纪 90 年代开始，全球量子计算领域的研究即进入快速发展期，新型计算逻辑相继提出，量子计算领域的研究水平不断上升。2000 年至 2017 年，量子计算的论文年均增长数保持约 10%的增速。

图 11 全球量子计算 SCI 论文增加数

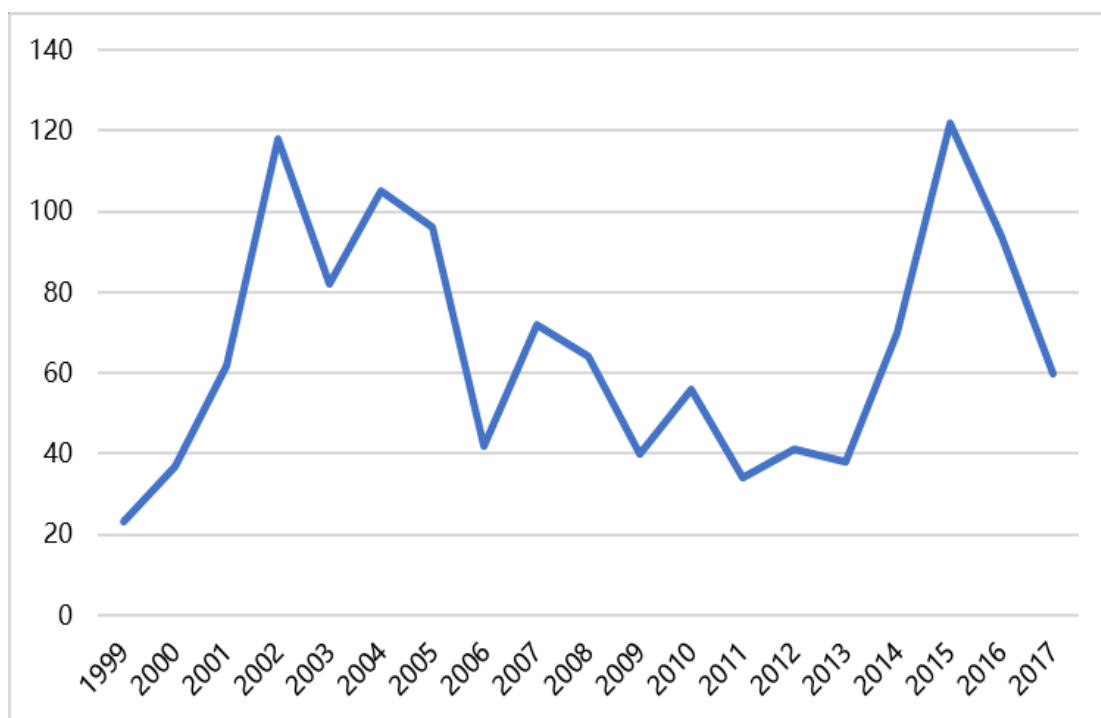


资料来源：国务院发展研究中心，2019年7月

专利申请方面，全球经历两次量子计算专利申请高潮，专利数持续上升。全球首个基于核磁共振方案的量子计算机原型的问题带动了第一次专利申请高潮，1998 年至 2004 年的量子计算专利申请量剧增。谷歌研究基于超导的量子计算机带动了第二次高潮，2014 年至 2016 年专利申请大幅增多。

量子计算机方面，利用超导量子器件实现量子计算是当前的主流方案，IBM、谷歌、英特尔均已公布基于超导器件的量子计算芯片方案。目前谷歌已经推出了 72 量子比特的量子处理器，IBM 推出全球首款可商用的量子计算机 Q System One，可操控 20 量子比特。

图 12 全球量子计算专利申请数



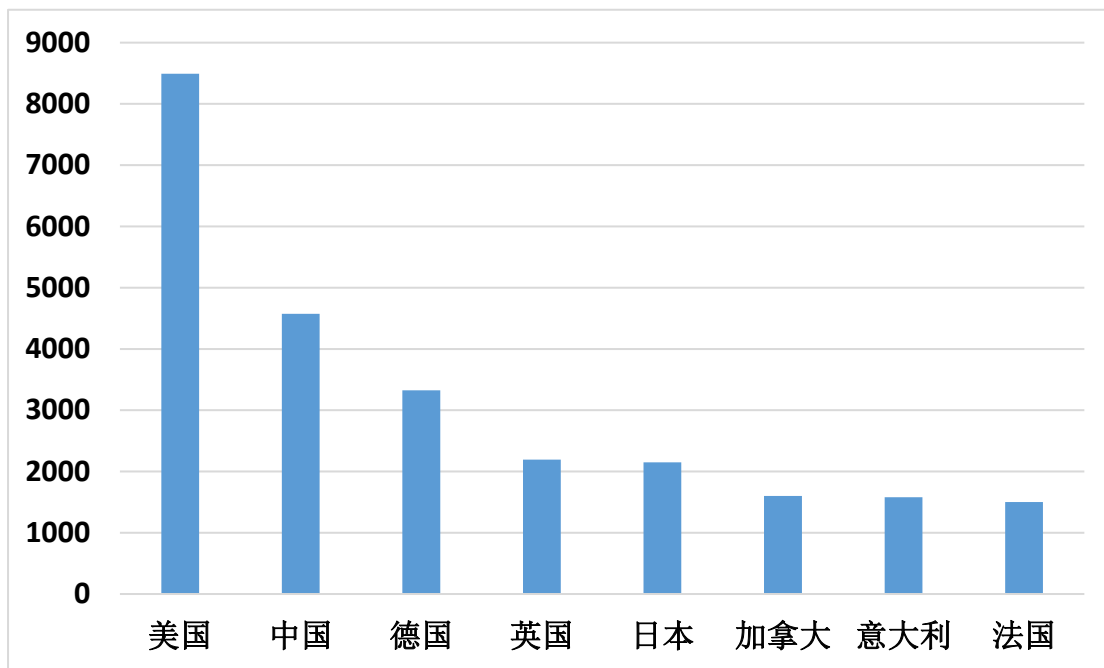
资料来源: Google Patents, 2019年7月

## 2、美国综合实力强劲，处于产业领先地位

从整体发展态势上看，美国在量子计算领域的综合实力全球领跑，已经形成政产学研多方协同的良好局面，欧洲发展较为强劲，日、韩、澳等国均处于跟随位置。

从 SCI 论文总数上看，美国处于大幅领先地位。截至 2018 年 9 月，美国以 8492 的论文总量远远领先于其他国家，占全球量子计算论文的 30%左右。中国、德国以 4500、3300 左右的论文总数位列二、三名，英国、日本、加拿大、意大利、法国等国的论文总数超过 1000 篇，具备一定的研究基础。

图 13 八个国家量子计算 SCI 论文数量



资料来源：国务院发展研究中心，2019年7月

从全球发表 SCI 论文量前 20 的顶尖研究机构数上看，美国拥有加州大学系统、美国能源部等量子计算领域的知名机构，占据机构当中的 7 席，中国、法国各占据 3 席，德国、英国、意大利、俄罗斯、加拿大、新加坡各占 1 个席位。

表 5 量子计算科研机构论文发表数量排名

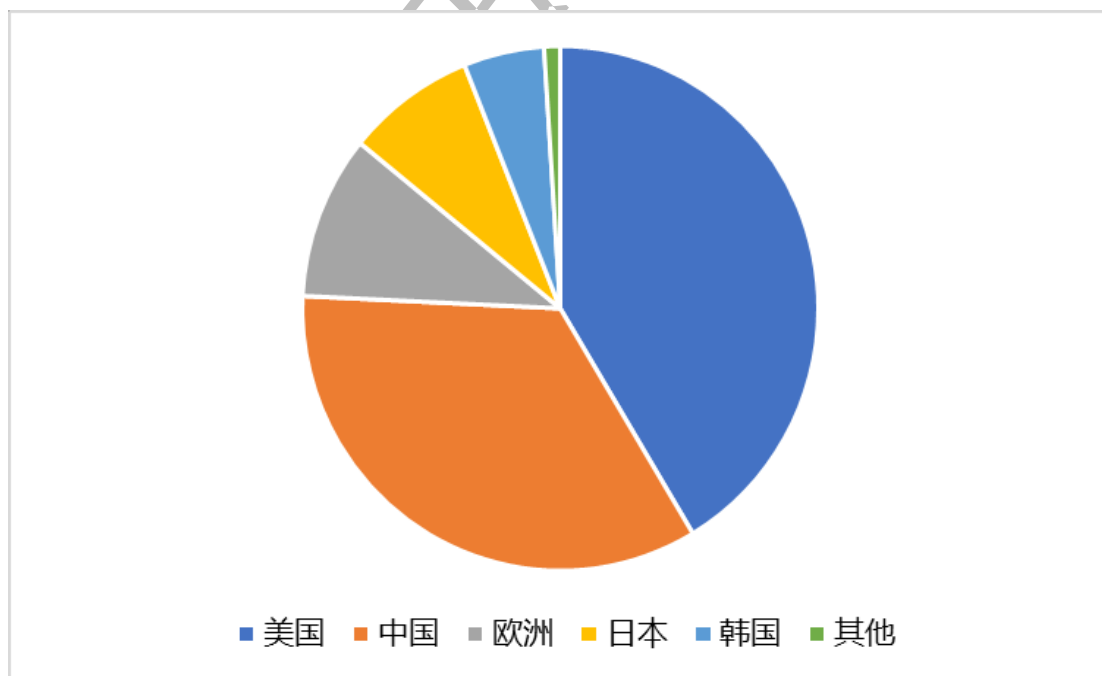
论文数排名	机构名称	所属国家
1	加州大学系统	美国
2	法国国家研究中心	法国
3	中国科学院	中国
4	美国能源部	美国
5	马克思普朗克协会	德国
6	俄罗斯科学院	俄罗斯
7	中国科学技术大学	中国
8	麻省理工学院	美国
9	牛津大学	英国
10	意大利国家研究委员会	意大利

论文数排名	机构名称	所属国家
11	滑铁卢大学	加拿大
12	法国蔚蓝海岸大学联盟	法国
13	加州理工学院	美国
14	马里兰大学系统	美国
15	新加坡国立大学	新加坡
16	东京大学	日本
17	清华大学	中国
18	哈佛大学	美国
19	巴黎-萨克雷大学联盟	法国
20	马里兰大学帕克分校	美国

资料来源：国务院发展研究中心，2019年7月

从专利申请数上看，2016 年全球量子技术相关专利申请总数约为 1000 个，美国、中国为申请主力，占据 75%以上专利申请量，欧洲各国、日本、韩国分列三至五位。

**图 14 一些国家量子计算 SCI 论文总数**









资料来源：Google Patents，2019年7月

### 3、产业巨头开展全球合作，推动技术与应用加速发展

基础研究方面，谷歌、IBM、英特尔等巨头积极开展全球合作，与耶鲁大学、麻省理工学院、加州大学系统等科研机构联合攻关共性技术，主要集中在超导量子计算领域，目前这些企业已经在超导量子计算领域取得较好成果。

图 15 超导量子计算发展现状

机构	规模	两比特门精度	技术优势
	72(22)比特	99%	有较好的微加工及软硬件支撑，技术累积较好
	5(5)比特	99%	有较好的微加工及软硬件支撑，技术累积较好
	50(20)比特	96%	有较好的微加工及软硬件支撑
	49(8)比特	96%	有较好的微加工及软硬件支撑
	4(4)比特	99%	有较好的微加工及软硬件支撑，主要集中在腔量子比特研究
	50(20)比特	95%	有较好的微加工及软硬件支撑

数据来源：中国科学技术大学，2019年7月

量子技术产业化方面，自 2007 年来自加拿大的初创企业 D-WAVE 宣布研制成功 16 位量子比特的超导量子计算机以来，IBM、谷歌、微软、英特尔等巨头纷纷宣布进军量子计算机科研和应用领域。IBM 在量子技术的商业化上独树一帜，在 2016 年，IBM 即开发了 5 位量子比特的量子计算机供研究者使用。2019 年 1 月，IBM 在 CES 展会上推出了全球首款商用量子计算机。谷歌在 2014 年即建成了 9 量子比特的计算机，并于 2018 年发布了 72 位量子比特的量子处理

---

器，产品计算能力业内领先。微软于 2005 年微软开始进入量子计算技术，提出了一种在半导体-超导体混合结构中建造拓扑保护量子比特的方法，并于 2016 年宣布计划斥巨额资源开发量子计算机的原型产品。英特尔与 2015 年投资 5000 万美元于硅量子点技术（silicon quantum dots）进入该领域，然而基于硅材料的量子点技术目前落后于超导量子技术。

产业应用方面，传统产业巨头也加入量子计算的产业链当中，开展新兴领域的业务拓展。戴姆勒与谷歌达成战略合作协议，共同开展量子计算的研究。基于此合作协议，戴姆勒专业研究团队可以使用谷歌量子计算机，并针对未来出行方案提供解决方案。该合作是科技企业与传统汽车企业合作的一次创新突破，具有探索意义。波音公司成立了颠覆性计算和网络组织，将探索人工智能、量子通信和计算、神经形态处理等前沿新兴技术在航天领域的应用。



## 四、我国量子计算发展现状

### （一）我国的量子计算国家战略

为抢占量子技术革命的制高点，近年来我国对量子计算的支持力度逐步加大。先后启动“自然科学基金”、“863”计划和重大专项，支持量子计算的技术研发和产业化落地。在 2018 年 5 月两院院士座谈会上，习总书记强调“以人工智能、量子信息、移动通信、物联网、区块链为代表的新一代信息技术加速突破应用”，进一步肯定了量子信息的战略地位。

**表 6 我国量子计算相关政策**

时间	文件	内容
2016 年	“十三五”国民经济和社会发展规划	量子信息技术是体现国家战略意志的重大科技项目之一
2016 年	国家创新驱动发展战略	将量子信息技术列入发展引领产业变革的颠覆性技术
2017 年	“十三五”国家基础研究专项规划	将量子计算机列为“十三五”器件“事关我国未来发展的重大科技战略任务”的首位
2017 年	“十三五”科技军民融合发展专项规划	推动包括量子计算在内的新一轮军民融合重大科技项目论证与实施

资料来源：赛迪智库整理，2019年7月

### （二）我国量子计算的进展

近年来，我国在量子计算领域研究发展较快，但主要以理论研究为主，参与者主要是以科研机构、高校，在核心论文数量、研究机构数上处于世界前列，基础研究能力仅次于美国。尤其在多光子纠缠领域，我国一直在国际上保持领先的地位，已经实现了 18 个光量子的纠缠，国内第一台“波色取样”在特定任务上超越最早期两台经典光

---

量子计算原型机。但在专利产出方面，我国明显弱于美国、英国、德国、日本等，基础研究成果转化有待加强。工程化及应用推动方面，我国与美国差距明显，国内企业的发展远远落后于 IBM、谷歌、微软等企业。

高校和科研机构方面，我国主要有中国科学技术大学、浙江大学、中国科学院、清华大学、南京大学、北京计算科学研究中心等高校和机构参与量子计算的产业发展，在相关领域已取得一定成果。

企业方面，阿里巴巴、腾讯、百度和部分 ICT 企业也积极参与产业生态建设，纷纷建立相关实验室。目前，已有企业发布了量子计算的云服务平台，可模拟十万级纠错电路，同时量子计算模拟一体机原型也已推出。而在量子芯片方面，已有企业进行了深入研究，将其作为未来战略发展重点。

---

## 五、我国量子计算发展面临的问题与挑战

### （一）关键技术研发仍属起步阶段，与国际水平存在差距

我国量子计算机研究发展迅速，但起步较晚，在量子计算机硬件、软件等各方面仍然存在重大的技术障碍，已有的研究基本处于原理验证和实验演示的阶段，关键技术研发尚处于起步阶段，与欧美国家差距巨大。具体表现在以下几个方面：一是相比于美国在量子计算机硬件、软件等全方面的布局和集中攻坚，我国量子软件研发能力显著落后，严重制约了我国量子计算机的发展步伐，易导致在国际竞争中长期处于被动状态。二是在编写量子计算算法、控制量子纠错等方面，使用独特的量子特征（如纠缠现象）编写量子算法，实现低错误率提升量子位稳定性是全世界量子计算科研工作者面临的一个重大挑战，我国在这一技术领域属于技术跟随者。三是大数据、人工智能等技术与量子计算的融合仍处于理论探索阶段。虽然量子计算机可以使人工智能技术更好的理解海量数据的价值，但目前我国在大量数据与量子态的相互转化等技术实现上仍处于理论探索阶段，距离未来技术融合应用尚有很大距离。

### （二）市场尚在培育阶段，技术和应用场景不成熟

目前，我国量子计算逐渐走出实验室，但是从硬件到软件到算法都需要提升核心技术，距离商业落地仍有较远距离。一是商用条件苛刻且成本高。量子计算机对正常运行的环境要求十分苛刻，量子芯片的工作温度仅比绝对零度（-273.15℃）高出 1/100 摄氏度，即大约-270.42℃。为达到量子芯片运行温度，需要配备一种专业冷冻机，但其成本高昂，不适合推广普及。二是未来应用场景模糊，距离应用落地尚有很大距离。相比较经典计算，通用量子计算对运算类型的要求较高，因此场景适应性较难，恐将在长时间内难以超越经典计算的普

---

及性的应用场景。专用量子计算机研发难度略低于通用计算机，但其导入仍需要技术标准体系、支撑设备、应用软件等多方面的体系化支撑。

### （三）国内企业参与度较低，缺乏全面战略布局

Google、IBM、Intel 等国际巨头积极开展量子计算研究，并不断取得重大突破。以谷歌为例，2018 年谷歌率先开发出 72 比特量子处理器 Bristlecone，并于 2019 年初研发出为量子计算量身定制的电路，成为未来扩大量子计算机系统规模的关键基础设备。与国外企业相比，我国企业在量子计算的技术累积、研发投入以及产业发展方向的战略布局方面差距非常大，而且预计在未来几年内会继续保持跟跑态势。以国内 BAT 为例，2015 年，阿里与中科院合作成立量子计算实验室，引入施尧耕等国际量子计算顶级专家，但受限于国内整体研究团队水平和人才的不足，目前研究应用主要集中于模拟量子系统和帮助互联网公司优化计算能力方面，缺少前瞻布局。腾讯建立了量子实验室，探索量子计算的的实际应用场景，建设量子安全平台对通信进行加密，但平台的研发仅属于量子通信加密的局部应用，且尚未取得普惠性应用。百度的量子计算研究所成立时间较晚，仍处于团队筹建过程。可见，BAT 对于量子计算的研究均处于起步阶段，技术途径也以跟随国际研发路径为主，缺少全面战略布局，研发成果与国际龙头企业差距较远。

### （四）人才体系单一、集中，尚未形成全面培养体系

量子计算机的实现尚且需要较长时间的研发，但量子人才的培养刻不容缓，关乎国际间关于核心技术、综合话语权的综合竞争，甚至直接影响我国国家安全。量子计算属于基础学科的前沿技术，研究准入门槛高，进展难度大，对人才要求较高，使众多研究者望而却步。

---

目前，全球均存在严重的量子计算人才缺口，我国的人才缺口现象更为严重。一是现有的量子计算专业人才数量极少，特别是中高层人才数量稀缺，已有专业人才主要集中于中科大、清华、浙大等国内几所高校的研究团队。二是量子计算人才的专业匹配度较低，人才知识结构单一，不符合量子计算的专业要求，大规模量子计算迫切需要量子体系结构、量子编程语言、量子编译等专业背景人才。三是国内高等教育机构缺乏针对量子计算技术发展的系统化学科布局和建设，致使高校未承担起量子计算人才输送地的重要责任。

---

## 六、对策建议

### （一）加强前沿科技领域产业化布局

一是推动国内龙头企业积极开展量子计算产业布局，组织工程技术研发，加大研发投入力度，鼓励围绕量子计算的实际应用方向共建联合实验室、建设科技创新孵化平台等，培育一批量子计算领域的骨干企业。二是积极发挥政府的引导和服务职能，不断完善产业布局，强化产业能力建设，加速推动量子计算研究成果与实体经济的融合。三是鼓励开放创新，深化国际合作，支持企业通过海外技术并购、参股、合作等方式跟踪国际先进技术发展动态。

### （二）加大对关键核心领域的研发支持

一是集中优势资源着力攻克技术薄弱环节，重点聚焦量子比特规模和性能、提高量子比特相干时间、实现噪音环境下的高保真度量量子逻辑门等技术瓶颈。二是完善产学研协同创新机制，畅通校企合作的沟通渠道，促进重大关键共性技术协同攻关，通过在企业内部设立院士专家工作站等方式深化产学研合作，强化技术研发与实际应用的融合。三是采取积极财政政策为量子计算研究提供资金支持。充分利用国家重大科技专项资金，对突破关键技术的研发给予经费扶持。

### （三）完善对专业人才梯队建设的全面布局

培养模式是我国量子计算人才发展的短板，为补齐人才短板，需要加强对专业人才梯队建设的全面布局，不仅要培养一批本土的高端技术人才队伍，同时还应以市场环境为依托，通过政策导向集聚全世界最优秀的量子计算相关专家。一方面鼓励企业打造量子精英团队，通过内部培训、外聘专家等多种形式为企业领军人才充电，将其打造为量子精英，帮助其了解量子计算及对本行业的潜在影响和未来前景。另一方面，前瞻布局高校在量子计算方向的学科建设，围绕量子计算

---

前沿技术研究所需专业素养，遴选部分试点高校开设相关专业或细分方向，引导高校和企业联动发力增加人才储备。

#### （四）积极构建量子计算应用生态体系

一是鼓励行业龙头企业发挥牵头带动作用，带领量子计算机的硬件和软件研发。二是支持量子计算产业上下游企业通过参股合资、长期战略合作等形式，畅通资源和信息对接渠道，加强产业协同和技术交流合作。三是支持企业、行业协会、科研机构等深化合作，成立量子计算联盟、完善政府、科研机构与企业之间的沟通机制和合作模式，共同开展量子计算关键共性技术研究。四是借鉴国外发展经验，支持具备较强技术和资源能力的企业采取国外并购、战略合作等多种形式，弥补技术短板，加快形成国内量子计算全产业链发展格局。

# 赛迪智库

面向政府·服务决策

## 关于我们

电子信息研究所是工业和信息化部赛迪研究院专业从事电子信息产业战略与规划研究的咨询服务部门，是国内最早的电子信息领域专业研究机构之一。研究方向覆盖电子信息各细分行业领域及新兴领域。电子所长期致力于为政府部门和企业提供电子信息产业和互联网产业发展政策、战略、规划、方案、可行性报告等研究服务，作为主要成员参与国家多份规划政策的编制起草，承担完成多项国家级、省部级重大项目。

电子信息研究所是中国超高清视频产业联盟（CUVA）、人工智能产业创新联盟、虚拟现实产业联盟（IVRA）、中国云服务联盟等行业组织的核心单位。



中国电子信息产业发展研究院

电子信息研究所

地址：北京市万寿路 27 号院 8 号楼 12 层

邮编：100846

电话：010-68209529

邮箱：wenxiaojun@ccidthinktank.com