

量子十问之六

量子计算，这可是一个颠覆性的新技术

郭光灿[†]

(中国科学技术大学 中国科学院量子信息重点实验室 合肥 230026)

2018-09-12收到

[†] email: gguo@ustc.edu.cn

DOI: 10.7693/wl20190308

量子计算机是一类遵循量子力学规律进行高速数学和逻辑运算、存储及处理量子信息的物理装置。当某个装置处理和计算的是量子信息、运行的是量子算法时，它就是量子计算机。现在或许还无法准确预测“量子计算机时代”何时到来，但在科学家看来，已经没有什么原理性的困难可以阻挡这种革命性、颠覆性产品的诞生。

以半导体芯片为核心的计算机的发明成就了现代信息技术产业(硬件、软件、网络、通信等)的高速发展，深刻改变了人类的社会活动形式，甚至是国防安全和国家核心竞争力。半导体集成电路芯片几十年以来一直沿着“摩尔定律”发展，单位芯片上晶体管数目越来越多，集成度越来越高。

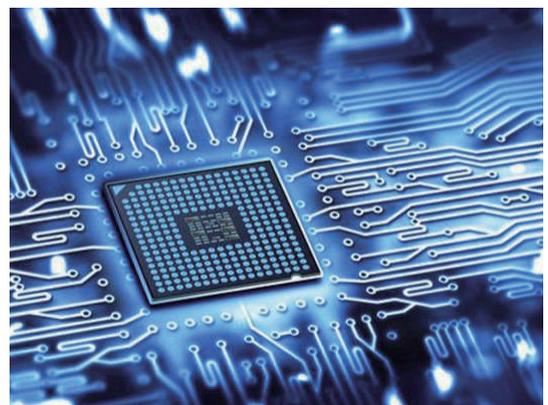
截止到目前，集成电路芯片制造工艺处于14&10 nm技术代量产阶段，更小尺寸的技术代(7 nm和5 nm)处于研发阶段。在可预见的未来将达到控制电子的物理极限，当单个晶体管缩小到只能容纳一个或几个电子时，就会出现单电子晶体管(量子点)，量子隧穿效应将不可避免地影响电子元器件的正常工作。尽管科研人员正在努力通过各种手段进一步延续晶体管的制程尺寸并同时开发多核芯片技术，但相关技术只能在有限范围内优化传统芯片性能，无法阻止“摩尔定律”必将被打破的历史趋势。

当现代计算机芯片在经典物理领域内无法进一步提升结构性能时，可以研究探索有别于当前计算机架构的新型结构和多核芯片，或者研究量子力学规律开发量子计算。新型结构需要抛弃当前计算机所遵循的冯·诺依曼架构，而量子计算则需要改变现有半导体芯片的基本结构，利用量子叠加和量子纠缠来实现逻辑运算。国际半导体技术发展路线图认为多核芯片等技术只能短期延续摩尔定律，中长期必然要发展以量子物理为基础的量子计算等颠覆性、革命性新型器件来超越摩尔定律，信息的量子化趋势将不可避免。量子计算是芯片尺寸突破经典物理极限的必然产物，是后摩尔时代具有标志性的技术。

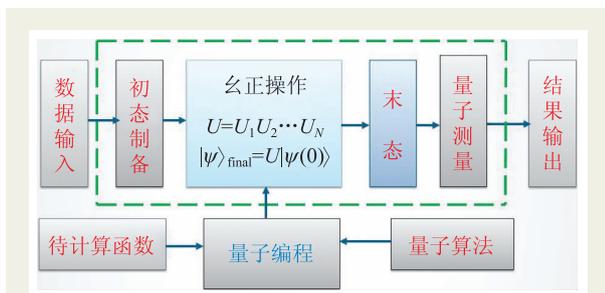
对于现代计算机而言，通过控制晶体管电压的高低电平，从而决定一个数据到底是“1”还是“0”，采用“1”或“0”的二进制数据模式，俗称经典比特，其在工作时将所有数据排列为一个比特序列，对其进行串行处理。而量子计算机使用的是量子比特，能秒杀传统计算机得益于两个独特的量子效应：量子叠加和量子纠缠。量子叠加能够让一个量子比特同时具备0和1的两种状态，量子纠缠能让一个量子比

特与空间上独立的其他量子比特共享自身状态，创造出一种超级叠加，实现量子并行计算，其计算能力可随着量子比特位数的增加呈指数增长。理论上，拥有50个量子比特的量子计算机性能就能超过目前世界上最先进的超级计算机“天河二号”，拥有300个量子比特的量子计算机就能支持比宇宙中原子数量更多的并行计算，量子计算机能够将某些经典计算机需要数万年来处理的复杂问题的运行时间缩短至几秒钟。这一特性让量子计算机拥有超强的计算能力，为密码分析、气象预报、石油勘探、药物设计等所需的大规模计算难题提供了解决方案，并可揭示高温超导、量子霍尔效应等复杂物理机制，为先进材料制造和新能源开发等奠定科学基础。

此外，量子计算的信息处理过程是幺正变换，幺正变换的可逆性使得量子信息处理过程中的能耗较



集成电路芯片(图片来源于网络)



量子计算机工作原理(图片来源于网络)

低，能够从原理上解决现代信息处理的另一个关键技术——高能耗的问题。因此，量子计算技术是后摩尔时代的必然产物。

量子计算技术不仅能克服现代半导体工艺因为尺寸减小而引起的热耗效应，还能利用量子效应实现功能强大的并行计算，极大地提高计算速度和信息处理能力。规模化通用量子计算机的诞生将极大地满足现代信息的需求，在海量信息处理、重大科学问题研究等方面产生巨大影响，甚至对国家的国际地位、经济发展、科技进步、国防军事和信息安全等领域发挥关键性作用。

(1) 国家影响力

信息是当今世界最为重要的战略资源，计算机技术是现代信息技术的核心，信息处理能力是信息时代的基本生产力，是国家的核心竞争力，体现国家综合实力的重要标志。“二战”结束以来，美国一直占据超级计算机研发的尖端，最初主要用于计算导弹弹道以及核武器模拟计算等军事活动，后来逐步应用到科研、产品研发、金融等各个领域。随后，计算机和互联网技术在美国迅速发展壮大，并在世界范围内扩展和加速全球化进程，美国在此过程中积累了其强大的国际影响力。量子计算科技革命给了我国一个从经典信息技术时代的跟踪者、

模仿者转变为未来信息技术的引领者的、不可错过的伟大机遇。量子计算技术是一种颠覆性技术，关系到一个国家未来发展的基础计算能力，一旦形成突破，会使掌

握这种能力的国家迅速建立起全方位战略优势，引领量子信息时代的国际发展。

(2) 经济影响力

量子计算机能克服现代计算机发展所遇到的能耗和量子效应问题，从而摆脱半导体行业面临的摩尔定律失效的困境，同时突破经典极限，利用量子加速、并行特性解决经典计算机难以处理的相关问题。作为现代计算机的颠覆者，未来量子计算机机会像经典计算机一样形成庞大的技术产业链，在国民经济生活中产生重大影响。其突破必将为信息和材料等科学技术的发展开辟广阔的空间，成为后摩尔时代和后化石能源时代人类生活的技术依托。量子计算机的研制必将带动包括材料、信息、技术、能源等一大批产业的飞跃式发展。量子计算机强大的并行计算和模拟能力，将为密码分析、气象预报、石油勘探、药物设计等所需的大规模计算难题提供解决方案，从而为提高国家整体经济竞争力创造条件。

(3) 科技影响力

过去50年以来，半导体及信息行业的技术发展经历过数次突破，从处理器的运算速度到存储器容量，再到网络带宽，每一次突破之后都能带来巨大的社会进步。目前，海量数据处理已成为急需攻克

的能力非常薄弱，传统计算机已经远远无法满足信息量爆炸式增长的需求，迫切需要从原理上突破超大信息容量和超快运算速度的瓶颈，而量子计算机正好能有效满足这一需求。量子计算机在科学研究领域具有广泛应用前景。学术界认为，在量子计算机达到大规模应用的比特数之前，将首先用于对量子体系的模拟。量子计算机利用其特殊的量子力学原理，将为强关联等物理学提供完美的检验平台。同时量子计算对于生物制药、机器学习、人工智能领域将产生深远影响，并对提高国家科技影响力起到积极作用。

(4) 军事影响力

量子物理与计算科学第一次大规模结合的直接原因就是研制核心武器的需求。在计算技术的发展历程中，军事应用价值始终是其重要推动力之一。量子计算机的强大功能应用到国防建设时，其强大的运算、搜索、处理能力，将为未来武器研发提供计算、模拟平台，缩短研发周期，提高武器研发效率。还将在未来战场上破译加密密文，为及时高效准确的情报和战况分析提供技术支撑，提升作战能力，同时在战场计划、组织决策、后勤保障等方面发挥巨大作用，甚至有可能改变未来战争的形态，掌握其核心技术能够极大地增强国防综合实力。

(5) 国家信息安全

量子计算机最受关注的重要应用之一是破译现代密码体系。理论研究表明，目前使用的RSA公开密钥体系在量子计算机面前将不堪一击。构建于经典保密系统之上的安全体系将变得无秘可言。此外，量子计算对于信息安全的威胁还具有

前瞻性,如果现在的通信网络流量遭到窃听并被存储下来,未来潜在的对手利用量子计算能力,就能对这些通常加密的信息进行破解,从而在多年以后将威胁范围追溯到当前。量子计算机的研制已经成为国际社会关注的焦点,其对国家安全体系的重大意义不言而喻。

量子计算机纵然有无比强大的颠覆性功能,然而通用量子计算机的研制过程是相当复杂的。研制量子计算机的关键在于量子比特的制备。量子比特非常脆弱,外界任何微弱的环境变化都可能对其造成破坏性影响。因此,量子计算机的核心部件通常处于比太空更加寒冷的密封极低温环境中,防止受到其他环境因素的干扰。量子比特的制备方式存在多种方案,经过近二十年的发展,国际主流研究集中到了超导量子比特、半导体量子点、囚禁离子、钻石空位和拓扑量子比特等。

由于量子计算对于国家安全及经济发展的巨大影响,世界各国政府持续高强度资助量子计算机的研制。毫无疑问,美国在量子计算机研制上是国际最领先的,并且有着完整的布局。虽然量子计算研究的进展低于十年前的预期,但还是让人们看到了突破可集成化量子计算机技术瓶颈的希望。特别当量子比特的保真度突破了容错量子计算的阈值,使得一些基本量子算法得到演示。这些巨大的成就吸引了一些国际商业机构和政府部门的极大关注。

量子计算机研制已经进入一个十分关键的时刻,国际上超大计算机、信息企业都投入巨大的人力、物力来研制量子计算机。主要包括:2012年微软研究院(美国)成立了量子体系结构与计算研究组,主

要目标是实现量子计算机软件体系结构,包括量子程序设计语言及编译系统。2013年谷歌公司与美国国家航空航天局(NASA)联合成立了量子人工智能实验室,研究如何将量子计算机应用于大数据分析机器学习。2014年9月2日谷歌宣布美国UCSB大学Martinis教授研究组加入谷歌公司研发量子计算机处理器。2014年IBM宣布耗资30亿美元研发下一代芯片(五年计划),主要是量子计算与神经计算。2015年世界最大的芯片制造商Intel公司宣布投入巨资与荷兰代尔夫特

理工大学合作研发基于硅量子点的量子计算机,并于2016年11月开发出了将量子计算机需要的超纯硅附着在传统微电子工业标准晶圆上的技术,2018年1月在工业标准晶圆上实现了硅基量子点的制备,以期抢占半导体量子计算机研制的制高点。2015年5月,全球最大的国防工业企业洛克希德·马丁(Lockheed Martin)与马里兰大学合作研发集成量子计算平台。2016年5月4日IBM公司发布了5个量子比特的量子计算云服务。2016年8月4日马里兰大学与美国国家标准与技术研究院(NIST)发布5个量子比特的可编程量子计算机。美、日、欧等发达国家在前期已经投入大量研发资金之后,2016年4月欧盟又宣布于2018年启动总额10亿欧元的量子技术项目,促进包括通用量子计算机等在内的多项量子技术的发展。同月,澳大利亚政府宣布在澳大利亚



人工智能(图片来源于网络)



中国科学院量子信息重点实验室在“国家重大科技计划”支持下开展固态量子芯片研究

量子计算与通信技术中心成立量子计算实验室,进一步集中对半导体硅基量子芯片等研究加大投入,以期抢占半导体量子计算的制高点。

我国政府也很重视量子信息技术的发展,在《国家中长期科学和技术发展规划纲要(2006—2020年)》中将“量子调控研究”列为四个重大科学研究计划之一,给予量子信息技术稳定的研究支持,做出了一系列创新性研究成果,在某些方面已经处于国际领先地位,特别是基于量子物理的新型量子保密通信技术已逐步迈向实用化产业化。

然而实用化量子计算机的研制是一个系统工程,既要量子物理为基础进行量子计算模型的原理性创新,又要从材料体系、结构工艺、系统构架和软件控制等工程技术创新和积累,我国在现代工艺技术上的基础薄弱,在核心电子器件、高端通用芯片、基础软件、极

大规模集成电路制造装备等长期落后，也导致我国量子计算的研究大都局限于原理验证性和演示性层面，缺乏系统深入的实验平台和以实用化量子计算机为目标的研究队伍。特别是在可扩展的固态量子比特研究体系上，国内只有中国科学技术大学、南京大学、清华大学、浙江大学和中国科学院物理研究所等少数单位开展相关研究。虽然经过近几年不懈努力，我们在半导体量子点和超导量子比特研究中取得

了一系列重大突破，在某些方面达到了世界一流水平，但是与国际领先水平还有差距，特别是在人力和物力方面的投入与欧美国家相比还远远不足。

量子计算机的研制需要物理、材料、信息和计算机科学等多学科的紧密协调和结合，从而实现从大规模器件的制备向微电子工程方面迈进。通用量子计算机的研制还有很长的路要走，量子计算机的研制将伴随着经典计算的发展一起前

进，相信随着量子比特的保真度达到容错量子计算的阈值，量子计算机的研究已经从实验室阶段向工程技术化阶段迈进，越来越多的研究单位和大型公司企业将进入，从而加速可实用化通用量子计算机研制的进程。从先进的发展模式而言，各大公司与研究机构合作研制量子计算机是集科研机构、公司、政府部门等于一体的研发模式，这可能是未来推进量子计算机研制的一种有效模式。

新书推荐

内容简介：诺贝尔奖获得者朗道院士为理论物理学作出了巨大贡献。他发表了一系列出色的论文，编写了被世界各国广泛使用的十卷本《理论物理学教程》，开创了极具影响力的朗道学派，该学派的代表人物如今活跃在这一学科各个领域。

这位伟大的物理学家还创立了一个关于应该如何生活的“幸福公式”，这一理论同样具有非凡的意义。朗道不仅“教书”，而且“树人”。有些年轻人对自己的命运漠不关心，对形势缺乏判断，缺乏追求幸福的渴望，对此朗道感到十分气愤。他的劝导充满了能量，能够振奋人心、让人告别懒惰，激发他人对于生活和工作的渴望。

这是第一本中文朗道传记，作者是朗道夫人的甥女迈娅·比萨拉比。与以往介绍朗道的文章大都着重其科学成就和学术风格不同，本书更多的从

个人生活角度揭示了朗道管控自己和追求幸福的方式，可以帮助了解朗道其人及其学派，大为提升学习《理论物理学教程》的兴味。

推荐理由：本书是苏联最伟大的理论物理学家朗道的第一本中文传记。中科院郝柏林院士生前为该书作序。首先，作者对于朗道太熟悉了（朗道是她的二姨夫），把发生在朗道身上的所有重要事情都讲了。其次，文字很朴实，译文也好得让人觉得这是一位朋友在讲述他身边的故事，太容易上瘾了。第三，珍贵的历史图片很多，还把朗道拍得那么帅。第四，纸张考究，装帧精美，排版讲究。第五，译文对物理内容翻译准确，译者是俄语专业的，不是搞物理的，但是显然受到了一些物理大拿的操控，想挑刺也不容易。

读者和编者

