量子科技：飞向未来的船与帆

潘建伟（中国科学院院士、中国科学技术大学常务副校长）

中共中央政治局近日就量子科技研究和应用前景举行了第二十四次集体学习。量子科技是事关国家安全和社会经济高质量发展的战略性领域，其具体应用包括量子通信、量子计算、量子精密测量等。

当前，量子科技已进入到深化发展、快速突破的新阶段，迫切需要多学科的紧密交叉和各项关键技术的系统集成。在量子科技领域整合科技资源、集中力量突破，已在世界范围内形成广泛共识。

今天，量子信息技术正在引领一场新的科技革命，将深远地影响人类社会。放眼更久远的未来，量子科技发展所取得的突破或许将帮助人类实现如今难以企及的梦想。从这个意义上说，量子科技正是带领我们“飞向未来的船与帆”。

“墨子号”量子科学实验卫星过境，乌鲁木齐南山观测站科研人员在做实验（合成照片）。 新华社发

第一次量子革命

为突破“摩尔定律”做好准备

量子的概念最早由德国物理学家普朗克提出来，从某种意义上讲，普朗克应该算是旧量子力学的祖父。爱因斯坦和玻尔是旧量子力学之父，他们又是新量子力学的祖父。海森堡、薛定谔和狄拉克等则建立了新量子力学——真正有方程去求解的量子力学，从而引发了第一次量子革命。

量子力学给人类带来了许多技术革新，核能、晶体管、激光、核磁共振、高温超导材料、巨磁阻效应等发现和发明都和它有关。可以说，量子力学是现代信息技术的硬件基础，数学则是软件基础，数学和物理结合在一起，奠定了整个现代信息技术的基础。

其实，从日常使用的一部手机里，就可以看到很多与量子力学相关的基础研究成果。有人统计，共有八项诺贝尔奖成果在手机里面：半导体器件是2009年诺贝尔物理学奖、集成电路是2000年诺贝尔物理学奖……（见下图）

正是有了半导体，才有现代意义上的通用计算机；然后在加速器的数据往全世界传递的过程中，催生了互联网；为了检验相对论，人们利用量子力学造出了非常精确的原子钟，在原子钟的帮助下，我们可以进行全球卫星导航定位。可以说，第一次量子革命直接催生了现代信息技术。

随着技术的进一步发展，现代信息技术遇到了两大挑战：一是信息安全瓶颈，二是计算能力的不足。

实现信息的安全传送，自古以来就是人类的梦想。人类早在公元前就发明了一些非常聪明的加密算法，此后又不断设计出更加复杂的密码，但随着计算能力的提高，这些加密算法都被破解了。人类究竟能不能构建一种自己破解不了的密码呢？

计算能力的提高，可以帮我们破解密码，同时也刺激我们产生更为巨大的算力需求。随着大数据时代的到来，全球数据量呈指数级增长，每两年翻一番，对计算能力的需求非常巨大。上世纪40年代，一台计算机重达1吨，每秒运算五千次。而到了2010年，一台智能手机已可每秒钟运算很多亿次，功耗不超过5瓦，计算能力却相当于美国阿波罗登月计划计算能力的总和。

一般来说，提升计算能力需要通过加强芯片的集成度。但目前，摩尔定律即将逼近极限，估计再过十年，就会达到亚纳米尺寸。到那时，晶体管的电路原理将不再适用。怎么解决信息科技面临的这些问题？目前的量子力学已经初步为突破信息安全和计算能力的瓶颈做好了准备。

第二次量子革命

进入主动操纵量子的崭新时代

如果说第一次量子革命是人类对量子规律的被动观测和应用，那么第二次量子革命则是人类对量子状态的主动调控和操纵，目前主要发展的应用领域就是量子信息技术。

第二次量子革命可从1935年算起，到1950年产生了量子纠缠，1972年之后发展出了较好的技术，能够对一个个量子状态进行主动操纵，比如可实现单光子的产生、操纵和探测。这个过程其实非常困难。就拿一个15瓦电灯泡来说，它每秒钟发射出10^{21}个单光子，要从这么多光子中拿出一个个光子去做信息处理，对实验技术要求非常高。

不过，一旦能够从下往上对微观粒子进行组装、操纵，其实就掌握了搭建整个世界每一块积木的本领。这种进步，相当于从孟德尔通过被动观察总结出遗传定律，进步到基因工程主动调控生命形态。

量子信息技术主要有两方面：一是量子通信，可实现原理上无条件的安全通信方式；二是量子计算，可提供一种超快的计算能力。

量子通信的应用之一是量子密钥分发。它的原理很简单，根据量子不可克隆定理，单光子不可分割，所以当人们用一个个光子来传输密钥时，就算窃听存在，也一定会被察觉，那么我们就丢弃那些存在窃听的风险密钥，保留安全密钥，再加上“一次一密”的保障，加密内容就不可破译，这是基于物理学原理的无条件安全。

利用量子纠缠可以把量子态从一个物体传送到另一个物体上，但原来的信息载体不用传送过去。比如说，我们在上海有一个微观体系，它由成千上万个原子组成。如果上海和北京之间有很多对纠缠原子，就可以把上海的体系和在上海的纠缠原子做一个联合测量，再把测量结果通过无线电台发送到北京，北京只需对手中的原子进行操作，就可以把上海的体系重新给制备出来——这就相当于在上海的体系被传送到了北京一样，但我们并没有把在上海的任何一个实体原子送到北京。

这本质上是一个量子态传输的结果，几十、几百个原子的状态，只要操作得足够快，就可以在网络里传来传去，这样一种操作便构成了量子计算机的基本单元：量子信息在网络里可以走来走去之后，就可利用量子叠加来进行量子信息的处理，这就是量子计算机。利用这种特质，可以设计一些相关的算法，实现快速分解大数、快速求解线性方程组等，如果制造出来，就可应用于破解经典密码以及人工智能、大数据等领域。

量子保密通信

“绝对安全”信息传输渐行渐近

量子通信的发展目标是要在更大范围内实现安全的信息传输，发展路线是通过光纤实现城域的量子通信网络、通过中继实现城际的量子网络、通过卫星中转实现远距离量子通信。

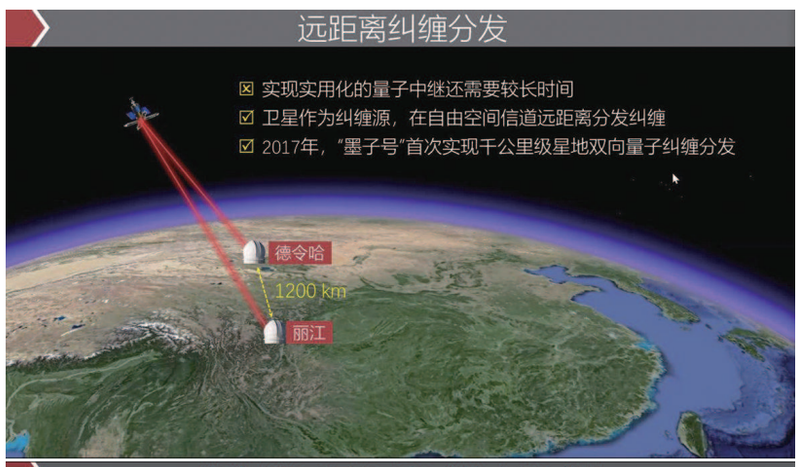
在量子通信这一领域，中国科学家有很多重要的贡献。比如，清华大学段路明教授在量子中继方面做了很好的工作；在光纤城域网络领域，清华大学王向斌教授也有很好的工作。

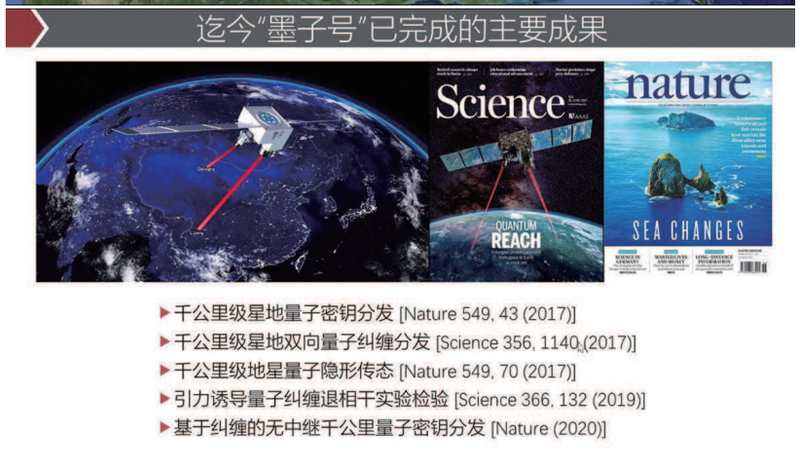
基于可信中继技术，中科大量子通信团队在2007年首次把光纤量子通信的安全距离拓展到100公里。2008年，我们建设了一个小型网络，2012年又建成了规模化的量子通信网络，并投入了永久使用。最后，我们逐步把这些局域网连起来，变成了现在的“京沪干线”。将来，量子中继可能是最终解决远距离量子通信问题的路径之一。

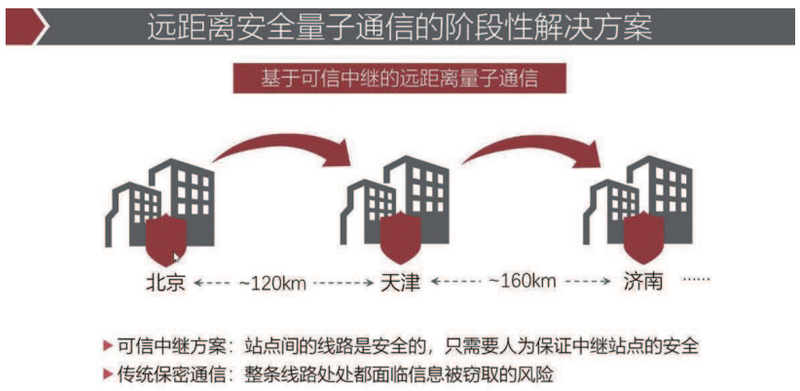
以目前的技术，要实现远距离的量子通信，需要卫星的中转。通过十几年的努力，我们和中科院上海技术物理研究所、微小卫星创新研究院的联合团队，研制成功了国际上第一颗量子科学实验卫星“墨子号”，并于2016年8月成功发射。目前，卫星已在轨运行四年多，状态和性能依然良好。

“墨子号”有三大科学实验任务。一是星地间量子密钥分发，即在1200公里的距离上，目前每秒可点对点发送十万个安全密钥，这比相同距离的光纤传输速率提高了20个数量级。二是实现了德令哈到乌鲁木齐、德令哈到丽江之间，相距约1200公里的量子纠缠分发。三是实现了上千公里的量子隐形传态。这些工作在2017年完成后，“墨子号”就实现了天地之间的量子通信，再加上“京沪干线”所实现的千公里级光纤城际量子通信网络，共同构成了天地一体化广域量子通信网络的雏形——这是国际上量子信息领域两个标志性事件之一。

在“墨子号”成功实施之后约一年，欧盟启动了量子旗舰计划，而美国则启动国家量子行动计划，量子信息在全球开始热起来了。







量子计算的未来

破解经典计算机解决不了的问题

量子计算发展的第一阶段是量子优越性，这已由谷歌公司于2019年10月实现，即针对某些特殊问题，造出一台比目前超级计算机算得更快的量子计算机，大概需要约50个比特。这也是量子信息技术的两大标志性事件之一。

该系统名字叫作“悬铃木”，约能操纵53个超导量子比特。它需要200秒算完的任务，目前世界排名第一的“顶点”超级计算机大概需要算一万年左右。

第二阶段，科学家希望能够操纵四五百个量子比特，以构造一种专用的量子模拟机，针对一些复杂物理系统，比如高温超导机制、新材料设计等目前超级计算机算不了的问题，用量子模拟机来进行运算，解决一些实实在在的问题。

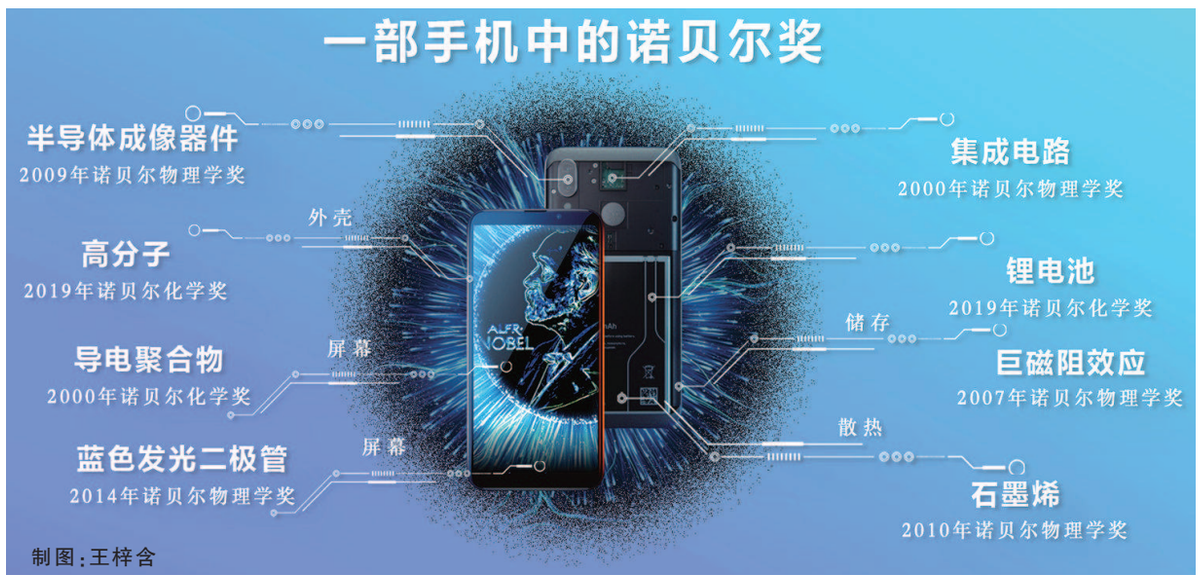
二三十年后，人类也许能造出一台可编程的通用量子计算机。这需要通过各种体系来开展相关工作，比如清华大学薛其坤教授所研究的拓扑量子计算、段路明教授从事的离子阱量子计算等。

除了上述提到的工作外，目前我国在量子计算领域的研究主要集中在三个方向：第一是光量子计算，今年大概能够实现50个光子相干操纵，也能够达到量子优越性，我们采用了与谷歌不同的技术途径。第二，在超导量子计算方面，希望在今年年底，能做到60个左右的量子比特。第三，希望量子计算能真正用来解决一些物理学、化学、材料科学中很重要、但用经典计算机解决不了的问题，目前已有比较好的进展。

展望未来，在量子通信方面，我们希望能够在外太空搭建一个非常精准的光钟，这个光钟的稳定度大概可以达到10万亿年误差不超过1秒钟——再结合广域量子通信技术，就可以提供一种引力波探测的新途径。

我们也希望，将来可以在地球和月球之间的拉格朗日点放一个量子纠缠光源的载荷，如果未来还可在月球上放一个基站，那就可以在地球和月球之间开展光秒量级距离的、有观测者参与的量子力学非定域性的检验。

（本版文章授权整理自微信公众号“知识分子”〈The-Intellectual〉、“墨子沙龙”）



“潘”谈量子

什么是量子？

其实量子非常简单，所有构成物质世界的最基本单元就叫做量子。举个例子，每天光照过来，就有好多光量子打到你身上——对于组成物质的小颗粒而言，如果它小到不能再分割，那么这就是量子。

量子在哪里？

量子有一个非常奇怪的特征——不确定性。简单而言，在经典世界里，人或物体在某一时间里只能在一个地方。而在量子世界里，在某些特定的情况下，如果说整个宇宙中没有一个人、一台仪器知道你在哪里的时候，你就可以在所有的地方。

为什么会这样？因为宏观世界里，你在运动时，周围有好多人或设备在探测你的轨迹。但到微观世界中，当一个原子在运动的时候，周围都是真空，就没有东西来测量它处于什么状态，在这种情况下，它就会出现在任何一个地方。这个分析在微观世界里面是成立的，并已经被无数实验所证实。

什么是量子纠缠？

在量子力学中，“薛定谔的猫”是非常著名的一个思想实验：一只猫在日常生活中能处在死或活两个状态，但是在量子世界里，它可以处于死和活两个状态的相干叠加，死和活这两个状态如果代表0和1，这两个死和活可以变来变去，就意味着信息的单元是可以处理、可以发生变化的。

到了量子世界里，因为它可以处于这种0和1状态的相干叠加，所以这个状态是永远测不准的，测不准之后它就不能被精确地复制。

当我们把这样一个单粒子的体系拓展到两粒子体系的时候，一种更奇怪的现象就发生了，我们把它叫做量子纠缠。一只猫可以处于死和活状态的相干叠加，如果有两只猫的话，是不是可以处于这样一种活活和死死状态的叠加呢？量子力学是允许的，这意味着一旦处于纠缠的两个客体，不管它们相距多么遥远，其中一个状态发生变化，另外一个状态也会发生相应的变化，我们把这种东西就叫做“遥远地点之间的诡异互动”，也就是量子纠缠。

量子理论可以溯源宇宙？

当我们把量子力学和相对论结合在一起时，我们就可以来建立宇宙起源的大爆炸理论。这个理论告诉我们，在138亿年前，宇宙是诞生于一个奇点的爆炸。

这个爆炸是怎么产生的呢？这正是由量子涨落产生的。所以，大爆炸几分钟之后，我们才会有氢、氘、氦元素的形成。而在那之前，由于温度太高，高达几亿摄氏度，所以只有质子、中子、光子、电子存在。直到大爆炸30万年后，宇宙中才有原子形成，亿年之后才会形成恒星。

所以，宇宙经过了相当于100亿年的“怀孕”之后，我们的太阳才正式诞生。而要等到太阳系形成，地球各种行星才慢慢形成了稳定的结构，又经过亿万年的进化，地球生命才进化为现在的人。

量子计算有多强？

我们现在把全世界所有的计算机、手机的计算能力加起来，计算能力大约是2^{80}。如果量子计算机诞生，那么它的计算能力将会超过目前地球上计算能力的100万倍。当这种技术走向实用，它将是非常强大的——这种算力如果分给每个人的话，我们每个人在计算能力上的财富，都是远远超过世界首富的。

曾有人预言，当量子计算机发展到50个量子位时，就能实现“量子称霸”，其计算能力将超过世界上任何传统计算机，解决许多传统计算机解决不了的问题。就在去年，谷歌宣布实现了这一目标。如今，大家又在向着更高的目标迈进。

量子计算会给人工智能带来什么？

经典的人工智能机器人根本就没有自由意志，它连一个非常简单的事情都决策不了，因此根本不会认识到自己的存在。但是，量子力学第一次把观测者的意识与物质的演化结合起来。所以我们高度相信，尽管还没被科学最后证实，量子力学必然会参与自我意识的产生。

由于我们每个人大脑里面想什么，是相互不可知的，这才保证了个体的多样性。量子力学告诉我们，想要一模一样复制大脑中的所有信息，是做不到的。我们既然这么独一无二，所以相信量子力学跟我们意识肯定紧密相连，我们也相信通过对量子计算机的研制，可能会为我们人脑一些机理的研究提供有价值的东西。

量子理论可以实现星际旅行吗？

1609年，科学家开普勒在给他的好朋友伽利略的信中写道：“应该建造适合飞向神圣天空的船与帆，然后也会有这样的先驱者，面对无边的太空，他们毫不退缩。”那时的人们不会想到，在300多年之后，1961年人类首次进入了太空，1969年人类首次登月。

1997年，世界上第一个量子隐形传态实验完成。十年后，我们中国科大的团队首次能够传送两个粒子的状态。而到2016年，随着“墨子号”的发射，我们的技术能力已经能够实现地星间的1000千米量子隐形传态。

如果人类要更深远地探索宇宙，目前的飞行手段连离开太阳系都难以实现，但也许300年、500年之后，我们能够利用现在量子科技的发现，找到进行星际旅行的新途径。