继对撞机、引力波之后，又一个“高冷”物理名词——量子，近年来逐渐从幕后走向了台前。在科学家们眼中，这一扑朔迷离的量子究竟是何方神圣？它有哪些神奇绝技，又有何用？

中国科学院院士潘建伟揭秘

量子信息技术带来第二次量子革命

在近日举行的两院院士大会上，中国科学技术大学教授、中国科学院院士潘建伟带来了一场有关量子的精彩介绍。

1 神奇的量子

量子是构成物质的最基本单元，由于具有相干叠加特性，可以产生“量子纠缠”，因而与相对论一起，带来了第二次科学革命

一旦确定了初始状态，根据力学方程，所有粒子未来的运动状态都是可以精确预言的——这是基于牛顿力学得出的结论。

“如果按照这个思路再往下思考，一切事件(比如今天的会议)都是在宇宙大爆炸时就已经确定好的吗？个人的努力还有意义吗？但人显然是有自由意志的。”潘建伟引用霍金的一句话：即使是相信一切都是上天注定的人，在过马路时也会左右看。

“所以，尽管我们对牛顿力学非常满意，但对其中蕴含着的决定论，仍持有异议。”潘建伟说。

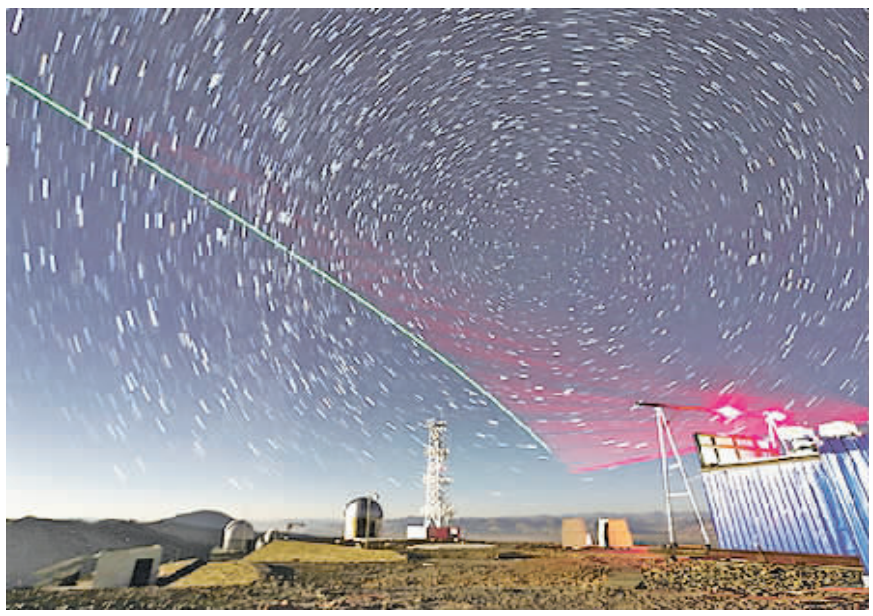
上世纪初，归功于普朗克、爱因斯坦、玻尔、海森堡等众多杰出科学家的共同努力，又一扇科学之门徐徐打开。到底是什么改变了牛顿力学的基本观念？其中一个就是量子力学。量子是构成物质的最基本单元，是能量的最基本携带者，不可分割。所有人们所熟知的分子、原子、电子、光子等微观粒子，都是量子的一种表现形态。

根据经典物理学，一个客体的状态(用0和1表示)就像最简单的二进制开和关，只能处于开或者关中的某一个状态，即要么是0要么是1，这就好比一只猫，要么是生要么是死，不能同时“又生又死”。但这一理论并不适用于量子世界。“比如在量子世界，一个氢原子的状态，可以是激发态和基态的相干叠加，可以0和1状态同时共存。”潘建伟举例。

这种所谓的量子相干叠加正是量子世界与经典世界的根本区别，由此有了量子力学不确定原理：量子体系中一般情况下一个物理量的值并不能预先确定，而是依赖于采取何种测量基，进一步，对处于量子纠缠的两个粒子，对其中一个粒子的测量结果会瞬间确定另一个粒子的状态，不论它们相距多么遥远。这就是“量子纠缠”，爱因斯坦称这个现象为“幽灵般的超距作用”。

潘建伟打了个比方：一个代表团从北京到法兰克福去访问，如果在飞行途中睡着了，不知道是途经莫斯科还是新加坡，到北京时，他们会觉得“又冷又热”，感觉好像同时穿越了两条路线。但如果飞行途中一直睁着眼睛去看，或者有仪器测量，那么检测到的状态是飞机只会处于一条航线上，代表团抵达北京时要么感觉冷，要么感觉热。

“叠加原理认为，一个量子客体可以处于不确定的状态，也就是说在测量之前，连上帝都不知道，观测者的行为还可以影响体系的演化。这种颠覆性的认知和相对论一起，带来了第二次科学革命，进而催生了新的产业变革。”潘建伟说。



“墨子号”量子科学实验卫星与阿里量子隐形传态实验平台建立天地链路(合成照片)。

2 安全的通信

利用量子相干叠加原理所产生的量子保密通信，成功克服了经典加密技术的内在安全隐患，可以从根本上解决信息安全传输问题

从春秋时期的虎符到古希腊的加密棒，以及罗马帝国凯撒大帝发明的字符移动加密术，再到二战时出现的复杂密码……人类追求信息安全的脚步从未停止。

为确保被授权的用户身份不被窃取，可以用加密算法进行身份认证；为保证传输过程中信息不被窃听，可以进行传输加密；为保证传输内容不被篡改，可以用加密算法进行数字认证。某种意义上，现在的信息安全是建立在加密算法或者加密技术的基础之上。

“然而，经典加密算法依赖于计算的复杂度，如果计算能力足够强大，原则上都会被破解。人们早就怀疑‘以人类的才智无法构造人类自身不可破解的密码’，这是目前经典加密算法面临的困境。”潘建伟说。

幸运的是，量子力学的发展已经为解决这一问题做好了准备。量子叠加的“分身术”，具有一个最为直接的应用——就是广受关注的量子保密通信。

潘建伟说，科学家们可以利用单光子来传输密钥。如果有窃听者想截取单光子，测量其状态并发送，那么，单光子就会从原有状态“0+1”变成0或者1，通信中就会引入扰动并会被使用者察觉。当然，经典光通信中还有一种窃听方法——截获一部分光，让其余部分继续传送，仅对截获到的部分进行状态测量获取密钥信息。但是，由于单光子不可分割，窃听者不可能如同在经典光通信中那样，把信号分成一模一样的两半，窃听也由此失败。

“量子通信克服了经典加密技术内在的安全隐患，因为其安全性不依赖于计算复杂度，这是原理上无条件安全的一种通信方式，一旦存在窃听必然被发现。”潘建伟称。

单光子的不可分割性和量子态的不可复制性从原理上保证了信息的不可窃听，再结合“一次一密”的加密方法，就可以实现信息的不可破解，从而确保了身份认证、传输加密以及数字认证等技术手段的无条件安全。

不过，要在现实条件下实现远距离的量子通信，并非听起来那么简单。量子信号因为不能被复制，所以不能被放大，信号会随着传输距离的拉长，变得越来越弱。比如，长度为1200公里的商用光纤中，即使有每秒百亿发射率的理想单光子源和完美的探测器，也需要数百万年才能传送一个量子比特。这样的传输速率显然不适于远距离传输。

怎么办？目前国际上公认有两种可行的途径：一种是利用中继器进行分段传输，另一种是利用卫星中转进行自由空间单光子传输，实现数千公里甚至是全球化的量子通信。

2016年，随着全球第一颗量子科学实验卫星——墨子号发射成功，实现信息“绝对安全”的梦想又向前迈进了一步。“去年，千公里级量子密钥分发速率达到1kbps，比同距离光纤提高20个数量级；现在，每秒钟可以稳定分发十万个密钥甚至几十万个密钥。”潘建伟说。

3 可期的未来

潘建伟表示，以量子信息技术为代表的第二次量子革命，一定会带来人类社会物质文明的巨大进步

量子通信不是唯一应用。

大数据时代，人类对计算能力的需求与日俱增。然而，目前人类拥有的计算能力还相当有限。例如，集全世界计算能力的总和都无法在一年内完成对280个数据的穷举搜索。与此同时，随着晶体管的尺寸逐步接近纳米级，晶体管的电路原理将不再适用。而通过超大规模处理器集成的超级计算机由于能耗惊人，也面临着发展模式不可持续的难题。以AlphaGo为例，下一盘围棋需要消耗10吨煤产生的电量。

“利用量子相干叠加原理，可以构造具有强大并行计算和模拟能力的量子计算机。”潘建伟说，量子计算机的计算能力随可操纵的粒子数呈指数增长，一台操纵100个粒子的量子计算机，对特定问题的处理能力可达到目前全世界计算能力总和的100万倍。利用万亿次经典计算机分解三百位大数大约需要15万年，这正是目前广泛使用的RSA公钥密码体系安全性的基石——现有计算能力无法在短时间内破解密码，然而利用同样工作频率的量子计算机则只要一秒钟。由此可见，一旦量子计算机研制成功，对现有密码体系的冲击将是崩溃性的。不过，量子力学在提供了破解密码“最锋利的矛”的同时，也为我们提供了信息安全“最牢固的盾”——量子通信的安全性与计算能力无关，即使在量子计算机时代，照样可以保障信息的无条件安全。

当然，量子计算机造出来还需时日。“届时，量子计算可为人工智能、密码分析、气象预报、石油勘探、基因分析、药物设计等所需的大规模计算难题提供解决方案，并可揭示量子相变、高温超导、量子霍尔效应等复杂物理机制。”潘建伟表示。

不仅如此，利用高精度的量子信息处理技术，还可对时间、位置、重力等物理信息实现超越经典技术极限的量子精密测量，大幅度提升卫星导航、激光制导、水下定位、医学检测和引力波探测等的准确性和精度。例如，利用目前最好的传统自主导航技术，水下航行100天后，定位误差达数十公里，需要定期上浮使用卫星修正；而利用原子干涉重力仪等高精度量子自主导航系统，水下定位航行能力可大幅提升，不需卫星修正就可实现长期自主导航。

“第一次量子革命已经在20世纪对我们的社会面貌和生活方式产生了巨大影响。可以预期，以量子信息技术为代表的第二次量子革命也一定会带来人类社会物质文明的巨大进步。”潘建伟说。

据经济日报