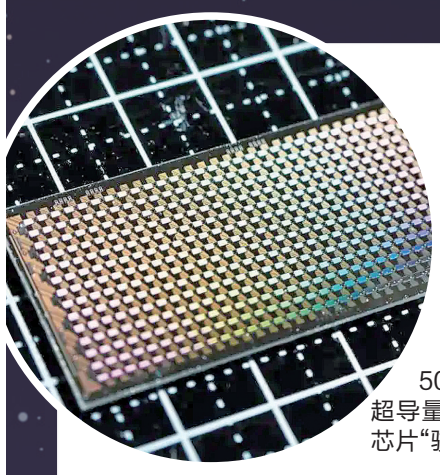
跨半球连亚非
中国实现12900多公里星地量子通信
若你不太明白这条信息，来看看我们对其背后的揭秘



504比特超导量子计算芯片“骁鸿”

记者20日从中国科学技术大学了解到，学校科研人员潘建伟、彭承志、廖胜凯等与国内外多个科研团队合作，在国际上首次实现量子微纳卫星与小型化、可移动地面站之间的实时星地量子密钥分发，在单次卫星通过期间实现了多达100万比特的安全密钥共享，并在中国和南非之间相隔12900多公里的距离上建立了量子密钥，完成对图像数据“一次一密”的加密和传输，为实用化卫星量子通信组网铺平了道路。

基于量子密钥分发的量子保密通信，是迄今唯一可实现“信息论可证”安全性的通信方式，将大幅提升现有信息系统的信息安全传输水平。利用卫星平台进行自由空间量子密钥分发，能够突破光纤等传输限制，实现全球范围的量子保密通信。

此前中国科研人员利用“墨子号”量子科学实验卫星首次实现了星地量子密钥分发，然而其成本高、覆盖面有限。科研人员尝试发射造价更低、身材更“苗条”的微纳卫星，多颗组网构建高效率、实用化、全球化量子通信网络。

2022年7月，中国发射国际首颗量子微纳卫星。“这颗微纳卫星的成本只有‘墨子号’的二十分之一，卫星自重、载荷重量也降低约一个数量级，但光源频率提升约6倍。”廖胜凯说，研究团队同时升级了小巧轻便的地面站系统。

此次，量子微纳卫星与中国济南、合肥、武汉、北京、上海以及南非的斯泰伦博斯等地面光学站建立光链路，实现实时星地量子密钥分发实验。以卫星作为可信中继，研究团队进一步实现了地面相距12900多公里的北京站和南非斯泰伦博斯站之间的密钥共享和数据中继。

这一研究工作为未来发射多颗微纳卫星构建“量子星座”奠定了坚实基础，不仅为大规模实用化量子通信网络的建设提供了关键技术支撑，更为量子互联网的全球部署开辟了新的发展路径。

3月20日，国际权威学术期刊《自然》杂志在线发表了这一成果，审稿人称赞此成果是“技术上令人钦佩的成就”“展示了卫星量子密钥分发技术的成熟”。 据新华社

揭秘

1 量子不是玄学，是打开微观世界的钥匙

中国科学技术大学郭光灿院士指出：“量子不是玄学，而是一把打开微观世界的钥匙，它的应用早已渗透到现代社会的每个角落。”那么，量子究竟是什么？

量子听上去与原子、电子等非常相似，很容易让人误以为它也是一种具体粒子。其实，量子并不是一个实体的“东西”，而是一种物理概念。简单说来，量子就是一种物理量中不可再分割的最小单位。

假设将全人类视为一个物理量，那么它的最小单位便是“一个人”，不存在半个人，“一个人”便是全人类这个物理量的量子。再比如上楼梯时，你只能站在第1、第2个台阶，却无法停在1.5个台阶。这就是量子化的生动比喻。

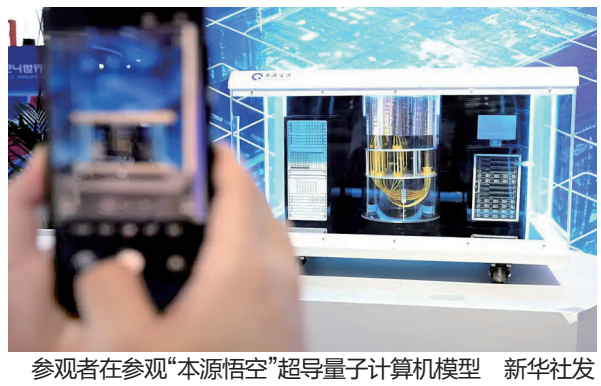
而量子“叠加”与“纠缠”的特性，则反映了它在微观世界的“超能力”。

所谓“叠加态”，是指电子可以同时处于多个位置，如同孙悟空的分身术，可以在同一时间处理多种不同任务。因此，利用量子叠加，我们可以实现计算机的并行计算。例如，分解一个300位的大数，用传统计算机可能需要15万年，而利用量子叠加技术并行运算，仅需一秒钟即可完成。

再比如一枚硬币，当它静止时，我们可以将其视为一个经典比特，这是经典计算机中的基础逻辑单元，它只能表示硬币的一面朝上或朝下。然而，如果我们让硬币开始旋转，它便能同时表达正面和反面两种状态，这就像量子计算机中的量子比特。

在量子力学中，还存在一个奇妙现象——量子纠缠，这是指两个粒子即使相隔千里，状态仍紧密关联，被爱因斯坦称为“鬼魅般的超距作用”。当大量的量子彼此纠缠时，它们所构成的计算空间，便会以指数级方式扩展，从而带来计算能力的指数级增长。

正是因为量子的这些特性，催生了量子通信和量子计算的革命性突破。



参观者在参观“本源悟空”超导量子计算机模型 新华社发

搭载量子微纳卫星的“力箭一号”运载火箭成功发射（资料图）

2 量子通信，拒绝“第三者”插足

在武汉等城市的一些电信营业厅里，量子SIM卡、量子密话等新产品琳琅满目，激起不少人的好奇心。

用户办理“量子密话”套餐后，营业厅将提供首次免费换卡服务——将普通SIM卡更换为量子SIM卡，用户在手机应用市场下载“量子密信”APP后，就能享受量子加密的移动通信服务。

“更换量子SIM卡，手机网速不受任何影响，通信安全将更有保障。”武汉电信云网发展部专家张珣介绍，“量子密信”APP可进行加密通话、发送加密短信等，无惧监听破译和信息泄露。

为什么量子技术能保障通信安全？张珣解释，传统加密依赖于数学难题，而量子通信则基于物理定律，任何窃听都会扰动量子态，使其立即暴露行踪。

比如把一个光子比作一个乒乓球，从球台一边飞到另一边，会形成一个独一无二的固定轨迹；若乒乓球在飞行途中被人截取，再抛向球台另一边，尽管乒乓球仍朝目标区域飞去，但原始飞行轨迹将产生偏差。

因此，量子通信是单纯的“二人世界”，只有发送方和接收方能“点对点”查看信息，所有监听行为都将改变量子系统状态，任何“插足的第三者”只能收到乱码。

使用“量子密信”APP拨打加密音视频电话时，拨打和接听双方均需持有量子SIM卡的手机。通话过程中，双方的SIM卡会各消耗一支“量子密钥”，每次通话密钥均不相同，一话一密。

目前，一张新的量子SIM卡配有约13万支密钥，一般足够使用4至5年。密钥用尽后，需到营业厅给SIM卡补充密钥。

基于量子通信的特性，多媒体消息“阅后即焚”功能是一大亮点，消息焚毁后再无法找回。而市面上即时通讯App的消息撤回功能，技术人员通过专业软件仍可恢复消息内容。

我国2016年发射的“墨子号”卫星，首次实现千公里级量子密钥分发，误码率低于1%，为全球量子通信网奠定了基础。

3 量子密码，用于金融、军事和安全保障等领域

上海交通大学金贤敏教授说：“量子密码具有信息论可证的安全性，量子攻防与更具现实安全性方案的不断迭代，使量子密码技术日臻完善，使人类追寻了几千年的绝对安全通信几近最终实现。量子密码在金融、军事和公共信息安全等方面展现出极大的应用前景。未来，量子密码系统的芯片化、集成化将进一步推升信道容量并降低成本，实用化和产业化前景可期。”量子密码究竟是“何方神圣”，让很多人竞相追求呢？金贤敏说：“传统密码系统利用两个极大质数相乘产生的积来加密，反向寻找质数会花费很多时间，也会耗费计算机大量处理能力，其安全性正是建立在对这种单向问题的求解上。”尽管这些密码足够强大，足以守护现代社会的很多秘密，如银行账户的密码、秘密数据库的密码等，但它们也很脆弱。一个有决心的人，只要拥有一台足够强大的计算机，就能破解它。或者未来足够强大的计算机，可以破解过去较低难度的密码，导致秘密信息的泄漏。而量子密码利用了量子力学的物理性质，从原理上来说是无法破解的。金贤敏解释说：“信息的发送者用单个光子携带用于加密和解密的密钥信息。如果有第三方试图盗取，必然‘雁过留痕’。收发双方通过确认单光子的状态，就能判断信息是否被监听。”“量子密码在原理上是不可破解的，因为使用者可以很快觉察到第三方的出现：任何窃听者不改变它，甚至不摧毁它是无法看到这些光子的。”金贤敏强调说。如此一来，这样一个安全的系统可用来传输包含机密信息的加密语音通话、传真和电子邮件等，有望在金融、军事和安全保障等领域“大显身手”。 据科技日报