中国成功从太空发送不可破解的密码

“墨子号”量子实验成果发表于《自然》杂志

新华社北京8月10日电（记者 喻菲）中国“墨子号”量子科学实验卫星在国际上首次成功实现从卫星到地面的高速量子密钥分发，为建立最安全保密的全球量子通信网络奠定可靠基础。“墨子号”的这一成果发表在10日出版的国际权威学术刊物《自然》杂志上。《自然》杂志的审稿人称赞星地量子密钥分发成果是“令人钦佩的成就”和“本领域的一个里程碑”。

量子卫星首席科学家、中国科学院院士潘建伟说，“墨子号”量子密钥分发实验采用卫星发射量子信号，河北兴隆与新疆南山地面站分别接收的方式，在北京和乌鲁木齐之间建立了量子密钥。据介绍，“墨子号”过境时与地面光学站建立光链路，通信距离从645公里到1200公里。在1200公里通信距离上，星地量子密钥的传输效率比同等距离地面光纤信道高20个数量级（万亿亿倍）。卫星上量子诱骗态光源平均每秒发送4000万个信号光子，一次过轨对接实验约10分钟可生成300kbit的安全密钥，平均成码率可达每秒1.1kbit。

“这样的密钥发送效率可以满足绝对安全的打电话或银行传输大量数据的需求。”潘建伟说。

他说，这一重要成果为构建覆盖全球的量子保密通信网络奠定了可靠的技术基础。以星地量子密钥分发为基础，将卫星作为可信中继，可以实现地球上任意两点的密钥共享，将量子密钥分发范围扩展到覆盖全球。此外，将量子通信地面站与城际光纤量子保密通信网（如合肥量子通信网、济南量子通信网、京沪干线）互联，可以构建覆盖全球的天地一体化保密通信网络。

绝对安全的保密通信

通信安全是国家信息安全和人类经济社会生活的基本需求，也是当代世界的难题。窃听、反窃听；加密、解密……这些密码学中的矛与盾处于恒久的博弈之中。

保密通信的原理在于，唯有掌握密钥，才能轻易重现传递的信息。信息的安全性主要依赖于密钥的秘密性。然而，传统加密技术在原理上存在着被破译的可能性。随着数学和计算能力的不断提升，经典密码被破译的可能性与日俱增。

有没有绝对安全的保密通信，让窃听、破译者无计可施？所幸的是，量子物理提供了解决这一问题的办法。如果量子计算机是针对传统密码的“利剑长矛”，那么量子密码技术就是抵御它的“坚固盾牌”。量子密码提供了一种不可窃听、不可破译的新一代密码技术。

专家介绍，与经典通信不同，量子密钥分发通过量子态的传输，在遥远两地的用户共享无条件安全的密钥，利用该密钥对信息进行一次一密的严格加密，这是目前人类唯一已知的不可窃听、不可破译的无条件安全的通信方式。

潘建伟说，量子密钥就是在A和B之间共同生成一串只有他们两边知道的随机数，然后用这个随机数来加密。量子密钥一旦被截获或者被测量，其自身状态就会立刻发生改变。截获量子密钥的人只能得到无效信息，而信息的合法接收者则可以从量子态的改变中得知量子密钥曾被截取过。将量子密钥应用于量子通信中，就是量子保密通信。与传统通话方式相比，量子保密通信采用的是“一次一密”的工作机制，通话期间，密码机每分每秒都在产生密码，一旦通话结束，这串密码就会立即失效，且下次通话不会重复使用。

潘建伟打了个比方，古人在信封上用火漆封口，一旦信件被中途拆开，就会留下泄密的痕迹。量子密钥在量子通信中的作用比火漆更彻底，因为一旦有人试图打开“信件”，量子密钥会让“信件”自毁，并让使用者知晓。

从太空突破极限

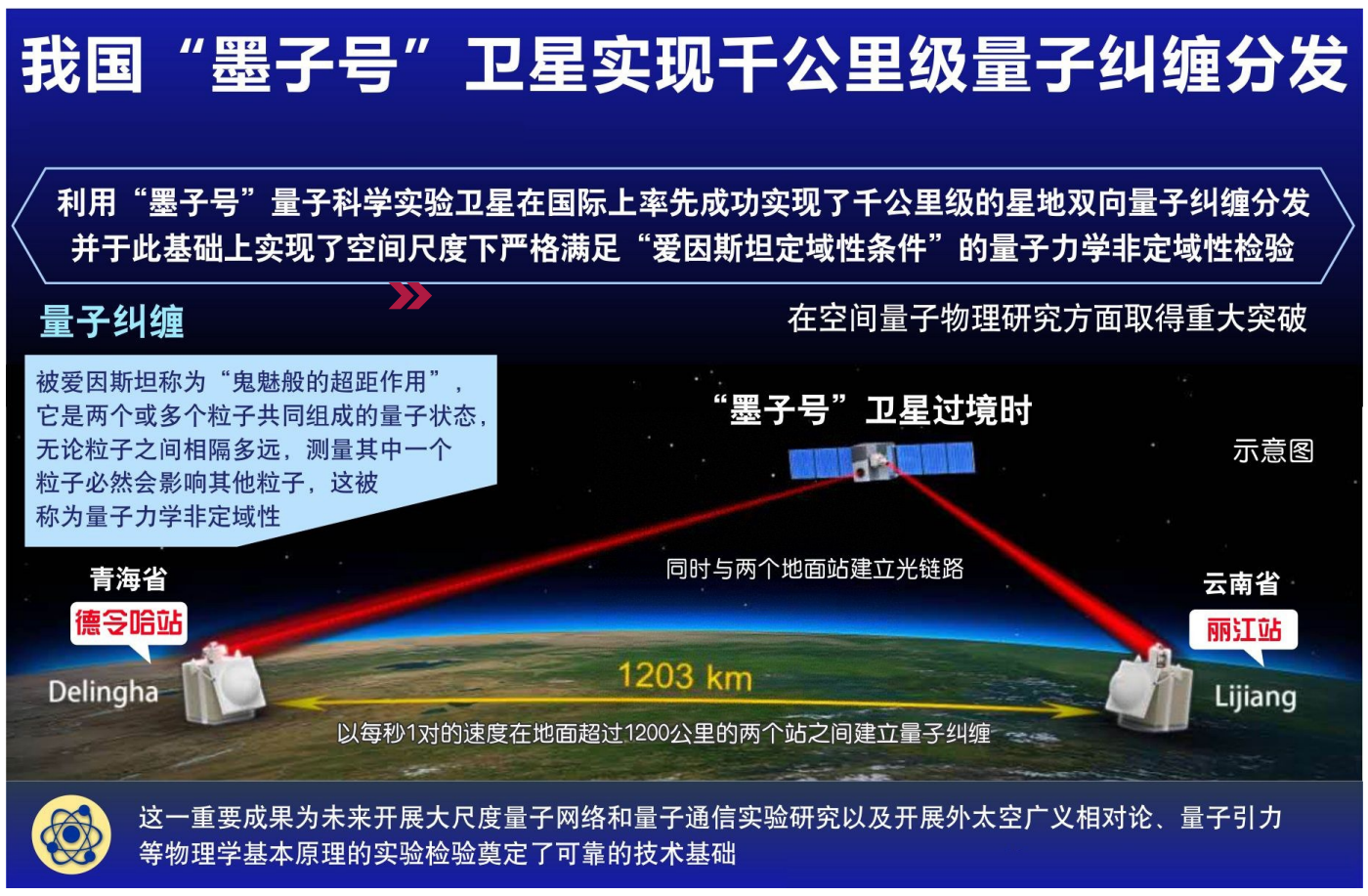
他说，量子通信通常采用单光子作为物理载体，最为直接的方式是通过光纤或者近地面自由空间信道传输。但是，这两种信道的损耗都随着距离的增加而指数增加。由于量子不可克隆原理，单光子量子信息不能像经典通信那样被放大，这使得之前的量子通信的局限在百公里量级。

“根据数据测算，通过1200公里的光纤，即使有每秒百亿发射率的单光子源和完美的探测器，也需要数百万年才能建立一个比特的密钥。因此，如何实现安全、长距离、可实用化的量子通信是该领域的最大挑战和国际学术界几十年来奋斗的共同目标。”潘建伟说。

他说，利用外太空几乎真空因而光信号损耗非常小的特点，通过卫星的辅助可以大大扩展量子通信距离。同时，由于卫星具有方便覆盖整个地球的独特优势，是在全球尺度上实现超远距离实用化量子密码和量子隐形传态最有希望的途径。从本世纪初以来，该方向已成为了国际学术界激烈角逐的焦点。

早在2003年，潘建伟团队已经为实现星地量子通信开展了一系列先驱性的实验研究。

量子通信在国防、军事、金融等领域应用前景广阔。有专家预测，量子通信技术可能在20至30年后对人类社会发展产生难以估量的影响。量子通信因其传输高效和绝对安全等特点，被认为是下一代通信和计算机技术的支撑性研究，也已成为全球物理学研究的前沿与焦点领域。



我国“墨子号”卫星实现千公里级量子纠缠分发。 □新华社记者 卢哲 金立旺 编制

首次实现量子密钥分发和隐形传态

“墨子号”量子卫星实现三大目标

日前，中国科学院在京召开新闻发布会对外宣布，“墨子号”量子科学实验卫星提前并圆满实现全部三大既定科学目标，为中国在未来继续引领世界量子通信技术发展和空间尺度量子物理基本问题检验前沿研究奠定了坚实的科学与技术基础。

抢占量子科技创新制高点，实现“领跑者”的转变

中国科学技术大学潘建伟教授及其同事彭承志等组成的研究团队，联合中国科学院上海技术物理研究所王建宇研究组、微小卫星创新研究院、光电技术研究所、国家天文台等，在中国科学院空间科学战略性先导科技专项的支持下，利用“墨子号”量子科学实验卫星，在国际上首次成功实现了从卫星到地面的量子密钥分发和从地面到卫星的量子隐形传态。两项成果于8月10日同时在线发表在国际权威学术期刊《自然》杂志上。这是继先前在国际上率先实现千公里级星地双向量子纠缠分发和量子力学非定域性检验的研究成果发表在《科学》杂志之后，中国科学家利用“墨子号”量子卫星实现的空间量子物理研究另外两项重大突破。

中国科学院院长、党组书记白春礼表示，“墨子号”开启了全球化量子通信、空间量子物理学和量子引力实验检验的大门，为中国在国际上抢占了量子科技创新制高点，成为了国际同行的标杆，实现了“领跑者”的转变。

唯一已知的不可窃听、不可破译的安全通信方式

通信安全是国家信息安全和人类经济社会生活的基本需求。千百年来，人们对于通信安全的追求从未停止。然而，基于计算复杂性的传统加密技术，在原理上存在着被破译的可能性。随着数学和计算能力的不断提升，经典密码被破译的可能性与日俱增。

通常认为，量子通信主要研究内容包括量子密钥分发（量子保密通信）和量子隐形传态。

量子密钥分发通过量子态的传输，在遥远两地的用户共享无条件安全的密钥，利用该密钥对信息进行一次一密的严格加密，这是目前人类唯一已知的不可窃听、不可破译的无条件安全的通信方式。

“通俗来讲，量子密钥分发，就好比一个人想要传递秘密给另外一个人，需要把存放秘密的箱子和一把钥匙传给接收方。接收方只有用这把钥匙打开箱子，才能取到秘密。没有这把钥匙，别人无法打开箱子，而且一旦这把钥匙被别人动过，传送者会立刻发现，原有的钥匙作废，再给一把新的钥匙，直到确保接收方本人拿到。”潘建伟说。

卫星的辅助可以大大扩展量子通信距离

量子通信通常采用单光子作为物理载体，最为直接的方式是通过光纤或者近地面自由空间信道传输。如何实现安全、长距离、可实用化的量子通信，是该领域的最大挑战和国际学术界几十年来奋斗的共同目标。

中国科学院上海技术物理研究所研究员、量子科学实验卫星工程常务副总师、卫星系统总指挥王建宇说：“利用外太空几乎真空因而光信号损耗非常小的特点，通过卫星的辅助可以大大扩展量子通信距离。同时，由于卫星具有方便覆盖整个地球的独特优势，是在全球尺度上实现超远距离实用化量子密码和量子隐形传态最有希望的途径。”

从本世纪初以来，该方向已成为了国际学术界激烈角逐的焦点。潘建伟团队为实现星地量子通信开展了一系列先驱性的实验研究。

为构建覆盖全球的量子保密通信网络奠定基础

此次完成的星地高速量子密钥分发实验是“墨子号”量子卫星的科学目标之一。

潘建伟表示，这一重要成果为构建覆盖全球的量子保密通信网络奠定了可靠的技术基础。以星地量子密钥分发为基础，将卫星作为可信中继，可以实现地球上任意两点的密钥共享，将量子密钥分发范围扩展到覆盖全球。此外，将量子通信地面站与城际光纤量子保密通信网（如合肥量子通信网、济南量子通信网、京沪干线）互联，可以构建覆盖全球的天地一体化保密通信网络。

地星量子隐形传态实验是“墨子号”量子卫星的另一个科学目标之一。彭承志说，这一重要成果为未来开展空间尺度量子通信网络研究以及空间量子物理学和量子引力实验检验等研究奠定了可靠的技术基础。 （吴月辉）

（《人民日报海外版》8月10日）

“墨子号”完成最难实验

新华社北京8月10日电（记者 喻菲）中国科学家在首颗量子科学实验卫星“墨子号”上完成了一项特殊实验：从地面到太空的量子隐形传态。这也是“墨子号”最难做的一项实验，它还常常被人联想到科幻电影《星际迷航》中的超时空传输。它们是一回事吗？

“墨子号”的地星量子隐形传态实验成果10日发表在国际权威学术期刊《自然》杂志上。《自然》杂志审稿人称赞实验结果代表了远距离量子通信持续探索中的重大突破，“目标非常新颖并极具挑战性，它代表了量子通信方案现实实现中的重大进步”。

中国科学院院士、量子卫星首席科学家潘建伟说，量子隐形传态是量子通信的一个重要内容，它利用量子纠缠可以将物质的未知量子态精确传送到遥远地点，而不用传送物质本身。

这有点像孙悟空的“筋斗云”，也像《星际迷航》中，宇航员在特殊装置中说一句“发送我吧”，他就瞬间转移到另一个星球。

当然，这只是个比喻。科学家指出，量子隐形传态实验中，被传输的是信息而并非实物。把粒子A的未知量子态传输给远处的另一个粒子B，让B粒子的状态变成A粒子最初的状态。注意传的是状态而不是粒子，A、B的空间位置都没有变化，并不是把A粒子传到远处。当B获得这个状态时，A的状态也必然改变，任何时刻都只能有一个粒子处于目标状态，所以并不能复制状态，或者说这是一种破坏性的复制。

潘建伟说，“墨子号”量子隐形传态实验采用地面发射纠缠光子、天上接收的方式。卫星过境时与海拔5100米的西藏阿里地面站建立光链路，地面光源每秒产生8000个量子隐形传态事例，实验通信距离从500公里到1400公里，实验传送了6个量子态，置信度均大于99.7%。

“假设在同样长度的光纤中重复这一工作，需要3800亿年，也就是宇宙年龄的20倍，才能观测到1个事例。”潘建伟说。

他说：“这一重要成果为未来开展空间尺度量子通信网络研究，以及空间量子物理学和量子引力实验检验等研究奠定了可靠的技术基础。”

潘建伟介绍，在“墨子号”开展的星地高速量子密钥分发、量子纠缠分发和地星量子隐形传态三大实验中，量子隐形传态实验是最难的。因为前两个实验都是从卫星向地面传送光子，在起初的490公里真空中不会受到大气影响，只有最后10公里进入大气层最稠密的部分时会受到影响。但是量子隐形传态实验是从地面向卫星发送光子，最初10公里就受到影响，到后来光斑被放大，抖动特别厉害，接收效率就会大大降低。

量子隐形传态是1993年由六位物理学家联合提出的。1997年，潘建伟的老师、奥地利物理学家塞林格带领的团队首次实现了传送一个光子的自旋。他们在《自然》上发表了一篇题为《实验量子隐形传态》的文章，潘建伟是第二作者。这篇文章后来入选《自然》“百年物理学21篇经典论文”，跟它并列的论文包括伦琴发现X射线、爱因斯坦建立相对论、沃森和克里克发现DNA双螺旋结构等。

事实上，在量子态隐形传态的漫长旅程中，每一点距离的进步都可以被视为一座里程碑。虽然最初的传输距离仅为数米，但美国《科学》杂志的评语是：“尽管想要看到《星际迷航》中‘发送我吧’这样的场景，我们还得等上很多年，但量子态隐形传态这项发现，预示着我们将进入由具有不可思议能力的量子计算机发展而带来的新时代。”

人类想离开太阳系去看看，量子隐形传态能否在未来成为人类星际旅行的方式？

潘建伟指出，传送几十、几百个微观粒子会在不久的将来实现，但要传送复杂的实物现在还是一种科学幻想。人是由10的28次方个粒子组成的，所以人类通过这种方式星际旅行还是个遥不可及的梦想。

但他说，300多年前开普勒给伽利略写了一封信，说人类应该造一艘能够在太空中飞翔的帆船，去探索宇宙的奥秘。大约260年后的1969年，美国阿波罗计划让人类登陆月球成为现实，现在人类飞行器已经到了太阳系的边缘。“我不敢说超时空传送真的能实现，但是科学的发展是不能预测的。”

即使这样的科幻永远无法实现，量子隐形传态研究也是有现实意义的。潘建伟说，量子隐形传态可用于量子计算和量子网络方面的研究。科学家正在研发的量子计算机之间未来要实现互联互通，进行协同计算，就需要量子隐形传态。

本报社址：上海市浦东新区丁香路716号B楼 邮政编码：200135 总机：021-68540066转各部门 广告经营许可证：3101520080003 浦东时报社南汇工作站：上海市浦东新区惠南镇北门大街58号 邮政编码：201300 电话：021-58000312 印刷：上海界龙中报印务有限公司