“墨子号”实现基于纠缠的无中继千公里量子保密通信

作者：writer 来源：爱科学

本文原地址：https://www.iikx.com/news/progress/10051.html

“墨子号”实现基于纠缠的无中继千公里
量子保密通信

。中国科学院院士、中国科学技术大学教授潘建伟及其同事彭承志、印娟等组成的研究团队，联合牛津大学Artur Ekert、中科院上海技术物理研究所王建宇团队以及微小卫星创新研究院、光电技术研究所等相关团队，利用墨子号量子科学实验卫星，在国际上首次实现千公里级基于纠缠的量子密钥分发。该实验成果不仅将以往地面无中继量子保密通信的空间距离提高了一个数量级，并且通过物理原理确保了即使在卫星被他方控制的极端情况下依然能实现安全的量子通信，取得了量子通信现实应用的重要进展。6月15日，研究团队在《自然》杂志上在线发表了题为基于纠缠的千公里级安全量子加密的研究论文。《自然》杂志发布了题为基于卫星的远距离安全通信的新闻稿加以推介。 量子通信提供了一种原理上无条件安全的通信方式，但要从实验室走向广泛应用，需要解决两大挑战，分别是现实条件下的安全性问题和远距离传输问题。通过国际学术界30余年的努力，目前现场点对点光纤量子密钥分发的安全距离达到了百公里量级。在现有技术水平下，使用可信中继可以有效拓展量子通信的距离，比如世界首条量子保密通信京沪干线通过32个中继节点，贯通了全长2000公里的城际光纤量子网络；而利用墨子号作为中继，在自由空间信道进一步拓展到了7600公里的洲际距离。然而，尽管可信中继将传统通信方式中整条线路的安全风险限制在有限个中继节点范围，中继节点的安全仍然需要得到人为保障。例如，在星地量子密钥分发过程中，量子卫星作为可信中继，掌握着用户分发的全部密钥，如果卫星被他方控制，就存在信息泄漏的风险。 实现远距离安全量子通信的最佳解决方案是结合量子中继和基于纠缠的量子密钥分发。基于纠缠的量子密钥分发的原理是，无论处于纠缠状态的粒子之间相隔多远，只要测量了其中一个粒子的状态，另一个粒子的状态也会相应确定，这一特性可以用来在遥远两地的用户间产生密钥。由于对粒子的测量局域地发生在用户端，纠缠源不掌握密钥的任何信息，即使纠缠源（例如卫星）由不可信的他方提供，只要用户间检测到量子纠缠，就可以产生安全的密钥。因此，量子通信源端不完美带来的安全问题可以得到完全解决，进一步提高了量子通信的现实安全性。原理上，利用量子中继可以实现远距离的量子纠缠分发，但实用化的量子中继还需要较长时间。 利用卫星作为量子纠缠源，通过自由空间信道在遥远两地直接分发纠缠，为现有技术条件下实现基于纠缠的量子保密通信提供了可行的道路。特别是墨子号在2017年首次实现千公里量级的自由空间量子纠缠分发后，实现基于纠缠的远距离量子密钥分发就成为国际学术界热切期盼的目标。 基于墨子号的前期实验工作和技术积累，研究团队通过对地面望远镜主光学和后光路进行升级，实现了单边双倍、双边四倍接收效率的提升。墨子号过境时，同时与新疆乌鲁木齐南山站和青海德令哈站两个地面站建立光链路，以每秒2对的速度在地面超过1120公里的两个站之间建立量子纠缠，进而在有限码长下以每秒0.12比特的最终码速率产生密钥。在实验中，通过对地面接收光路和单光子探测器等方面进行精心设计和防护，保证了公平采样和对所有已知侧

信道的免疫，所生成的密钥不依赖可信中继、并确保了现实安全性。结合最新发展的量子纠缠源技术，未来卫星上可望每秒产生10亿对纠缠光子，最终密钥成码率将提高到每秒几十比特或单次过境几万比特。《自然》杂志审稿人称赞该工作展示了一项开创性实验的结果，这是朝向构建全球化量子密钥分发网络甚至量子互联网的重要一步，……不依赖可信中继的长距离纠缠量子密钥分发协议的实验实现是一个里程碑。该研究工作得到了中科院、国家自然科学基金委、科技部、安徽省、上海市等的支持。（来源：中国科学技术大学）

相关论文信息：https://doi.org/10.1038/s41586-020-2401-y

实验示意图

作者：潘建伟等 来源：《自然》