中国科大实现无需参考系校准的测量设备无关型量子密钥分配实验系统

文章来源：中国科学技术大学 发布时间：2015-10-20 【字号： 小 中 大 】 我要分享

中国科学技术大学教授、中国科学院院士郭光灿领导的中科院量子信息重点实验室在探测设备无关型量子密钥分配的研究方面取得新进展：该实验室量子密码研究组的银振强、王双、韩正甫、陈巍等在国际上首次实现了无需参考系校准的测量设备无关型量子密钥分配（MDI-QKD）实验系统，显著增强了系统的实际安全性和工作稳定性，对推动此类设备无关型量子密钥分配技术在实际环境中可靠、稳定的应用具有重要意义。该研究成果作为编辑推荐发表在10月15日的《物理评论快报》上，实验室的博士生王超、宋浩天是该系列工作的共同第一作者。

量子密钥分配基于量子力学的原理，可以在信息论的层面实现通信双方之间无条件安全的密钥传输。但是由于实际器件和设备的不完美，量子密钥分配实际系统的安全性与理论协议之间存在着一定的差距。从协议层面而不只从技术参数对抗的角度解决系统的实际安全问题，是当前研究者探讨的重点之一。2012年，加拿大H. K. Lo研究组提出了MDI-QKD协议。该协议无需对测量端的量子设备进行任何安全性假设，就能够有效地免疫所有探测端攻击，有效提升了量子密钥分配系统的实际安全性，受到了国际上的广泛关注。

然而，与BB84等协议类似，该协议的有效执行需要量子态制备与测量时的参考基准（参考系）严格一致，否则将产生系统误码，极大地降低安全密钥生成率并造成安全隐患。由于系统收发各方所处的环境不同且在不断变化，因此通信双方或者多方之间参考系的校准是必不可少的。参考系校准过程将消耗更多的系统资源，且有可能引入额外的安全隐患。特别是在复杂的网络应用环境下，多个参考系之间的校准工作将可能严重的影响其有效的密钥生成能力和稳定性。

研究组基于MDI-QKD协议中的Bell态投影测量的思想，通过将经典信息编码到光子路径这一物理量上，有效地避免了环境干扰对编解码的影响，设计了无需参考系校准的MDI-QKD协议。协议通过对路径中的编解码单元进行相位调制和解调，可以有效地监测系统的工作状态和安全参数。课题组进一步基于具有自主知识产权的“法拉第-迈克尔逊”干涉仪结构，通过对其增加光量子高速路径选择单元，实现了满足MDI-QKD要求的环境干扰免疫的光量子相位编解码干涉仪。研究组同时解决了独立光源量子干涉、异地时钟精准同步、线路自动纠偏等MDI-QKD系统实现中的关键技术问题，首次在实验上有效验证了无需参考系校准的MDI-QKD协议的安全性和稳定性。实验结果证实这一方案可以有效降低通信者之间对参考系校准的要求，避免了在参考系校准过程中引入额外的系统开销或安全隐患，可以有效提升测量设备无关量子密钥分配技术在复杂网络环境下的可用性。

这项工作得到了科技部、国家自然科学基金委、中科院和教育部的资助。

文章链接

（责任编辑：叶瑞优）

热点新闻

中科院与铁路总公司签署战略合...

中科院举行离退休干部改革创新发展形势...
中科院与内蒙古自治区签署新一轮全面科...
发展中国家科学院中国院士和学者代表座...
中科院与广东省签署合作协议 共同推进粤...
白春礼在第十三届健康与发展中山论坛上...

视频推荐

【新闻联播】“率先行动”计划 领跑科技体制改革

【新闻直播间】中科院：粤港澳交叉科学中心成立

专题推荐