中国科大实现全被动量子密钥分发

作者：writer 来源：中国科学院

本文原地址：https://www.iikx.com/news/progress/24421.html

中国科学技术大学郭光灿院士团队在量子密钥分发研究中取得重要进展。该团队韩正甫、王双、银振强、陈巍与合作者，提出了一种无需主动调制的新型量子密钥分发实现方案，并完成了实验验证，为实现高现实安全的量子密钥分发系统提供了新思路。9月13日，相关研究成果发表在《物理评论快报》（*Physical Review Letters*）上。

量子密钥分发理论上可以实现无条件安全的密钥共享。而器件特性、调制精度、环境干扰等因素可能造成系统的现实安全性问题。例如，郭光灿团队发现，系统中广泛使用的铌酸锂主动调制器件，可能会受到光折变等侧信道攻击而泄漏信息。

为彻底解决主动调制带来的隐患，郭光灿团队与合作者另辟蹊径，设计了无需主动调制的量子密钥分发系统。该系统方案克服了此前无法同时实现“被动”光强调制和量子态编码的矛盾，并给出了考虑“有限长效应”的严格安全密钥率。该团队通过全被动时间戳-相位编码解决信道环境干扰的难题，同时通过优化后选择策略解决数据吞吐量过大的难题，最终完成了无需任何主动调制的量子密钥分发系统，验证了全被动量子密钥分发的安全性与可行性。

安全性是量子密钥分发的核心价值和要求。探索具有更高现实安全性的协议，并设计相应的方案和系统，是推进量子密钥分发走向实用化的关键之一。该研究为实现高现实安全的量子密钥分发系统提供了全新的思路，对推动该领域的实用化和标准化具有重要意义。

研究工作得到科学技术部、国家自然科学基金委员会、中国博士后科学基金会、中国科学院和安徽省的支持。

论文链接

研究团队单位：中国科学技术大学