

科学家提出并实现误差容忍高安全量子密钥分发

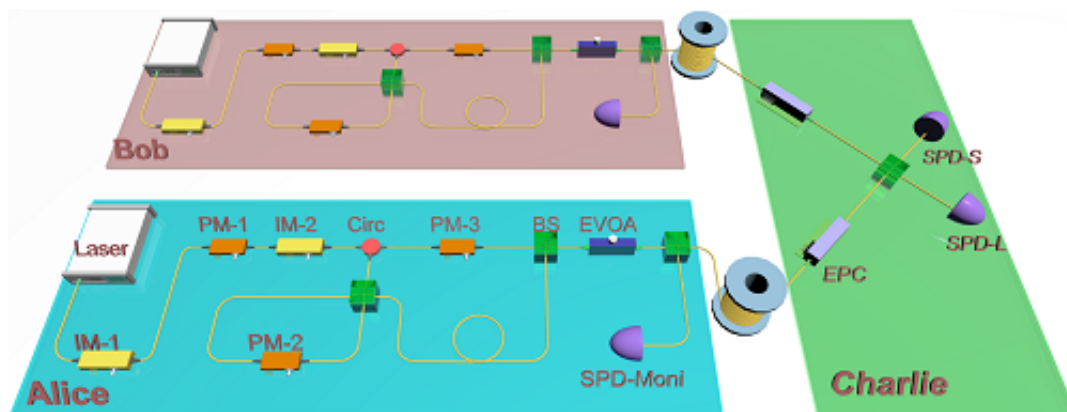
作者：writer 来源：爱科学

本文原地址：<https://www.iikx.com/news/progress/19745.html>

本文仅供学习交流之用，版权归原作者所有，请勿用于商业用途！

科学家提出并实现误差容忍高安全量子密钥分发。

中国科学技术大学郭光灿院士团队的韩正甫教授及其合作者银振强、王双、陈巍等，提出了兼具高稳定性和高安全性的误差容忍测量设备无关量子密钥分发协议，并从安全性分析和实验验证两方面证实了该协议对源端非理想特性具有极强的容忍能力，有力推动了新一代量子密钥分发技术的实用化进程。相关研究成果在线发表于《光学》。



误差容忍测量设备无关量子密钥分发实验结构图

信息安全是当今时代的重要主题，量子密钥分发技术以量子物理原理为基础，可实现理论上无条件安全的密钥分发。然而，这种理论安全性需要两个重要的假设，即用户拥有符合理论模型描述的理想设备，以及窃听者不能侵入系统的探测端和源端。

测量设备无关量子密钥分发可以免疫所有针对探测端的潜在攻击行为，是新一代量子密钥分发技

术的典型协议。然而，其依然保留了对源端的诸多安全性假设，例如量子态调制中的误差和噪声就会违背这些安全性假设，不仅会显著降低量子密钥分发系统的性能，还会给潜在窃听者带去可乘之机。在复杂的实际环境中，用户不得不耗费大量的资源以监控和校准源端，不仅会降低协议执行的效率，也可能带来潜在的安全问题。

为推进新一代量子密钥分发技术的实际应用，韩正甫团队通过将源端常见的非理想特性纳入安全性证明框架中，提出了兼具高稳定性和高安全性的测量设备无关协议——误差容忍测量设备无关协议。该协议在免除了对探测端所有安全假设的同时，还免除了源端的单光子态不可区分假设和纯态假设。由于免除了这两条假设，测量设备无关协议对量子态调制中的信号畸变和噪声具有极强的容忍能力。

经过严格的安全性分析，团队证明了这些源端设备的非理想特性不会破坏测量设备无关协议的安全性，也不会降低系统的安全密钥生成速率，因此误差容忍协议兼具高安全和高稳定两大特性。

韩正甫团队进一步搭建测量设备无关系统，对提出的误差容忍协议进行实验验证。团队首先通过自主设计的Sagnac-AMZI编码器和四强度诱骗态调制装置实现了原始测量设备无关协议，并通过该系统观察测量调制信号具有不同误差时原始协议性能的变化。随后，团队使用同一系统执行误差容忍测量设备无关量子密钥分发协议，在不对选基信号进行预先校准的情况下实现了几乎恒定速率的安全密钥分发。

通过前后性能对比，证明了误差容忍测量设备无关协议的高稳定特性，以及对于实际应用的重要价值。由于实际量子密钥系统往往需要工作在复杂快变的环境中，很难实现源端的精确实时校准。韩正甫团队的这项成果极大推进了测量设备无关量子密钥分发技术的实用化进程，也为量子密钥分发技术真正走向无条件安全奠定了理论和实验基础。（来源：中国科学报 王敏）

相关论文信息：<https://doi.org/10.1364/OPTICA.454228>

版权声明：凡本网注明来源：中国科学报、科学网、科学新闻杂志的所有作品，网站转载，请在正文上方注明来源和作者，且不得对内容作实质性改动；微信公众号、头条号等新媒体平台，转载请联系授权。邮箱：shouquan@stimes.cn。

作者：韩正甫等 来源：《光学》

更多 科学进展 请访问 <https://www.iikx.com/news/progress/>

本文版权归原作者所有，请勿用于商业用途，[爱科学iikx.com](https://www.iikx.com)转发