科学家实现模式匹配量子密钥分发

作者：writer 来源：中国科学院

本文原地址：https://www.iikx.com/news/progress/21805.html

科学家实现模式匹配量子密钥分发
。近日，中国科学技术大学潘建伟、陈腾云等与清华大学马雄峰合作，首次在实验上实现了模式匹配量子密钥分发（Mode-pairing QKD）。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（QKD）基于量子力学基本原理，可以实现理论上无条件安全的保密通信，近几十年来一直是学术界的研究热点。模式匹配量子密钥分发协议（MP-QKD）是清华大学马雄峰研究组于2022年提出的新型测量设备无关量子密钥分发协议，要求通信双方首先将信息编码在单个光学模式中，基于探测响应结果，通信双方按照一定规则进行配对，再根据配对情况进行基矢比对、参数估计等后处理操作来产生最终的安全密钥。相较于原始的测量设备无关协议（MDI-QKD），MP-QKD可以将更多的探测事件用于成码，可以很大程度提高成码率；相较于双场量子密钥分发协议（TF-QKD）和相位匹配协议（PM-QKD），MP-QKD无需复杂的激光器锁频锁相技术，节省了成本、降低了实际应用难度，并对环境噪声有更好的抗干扰能力。

潘建伟、陈腾云研究组基于清华大学马雄峰研究组提出的模式匹配量子密钥分发（MP-QKD）协议，利用极大似然估计的数据后处理方法精确地估算出两个独立激光器的频率差用于参数估计，并结合中科院上海微系统与信息技术研究所尤立星团队研制的高效率单光子探测器，实现了实验室标准光纤百公里级、两百公里级、三百公里级以及超低损光纤四百公里级的安全成码，相较于之前的原始MDI实验，成码率有明显提升，且在三百公里和四百公里距离上较之前实验成码率提升了3个数量级。

上述研究成果表明，MP-QKD在不需激光器锁频锁相的条件下可以实现远距离安全成码且在城域距离有较高成码率，极大地降低了协议实现难度，对未来量子通信网络构建具有重要意义。

研究工作得到科技部、中科院、国家自然科学基金、安徽省等的支持。

论文链接

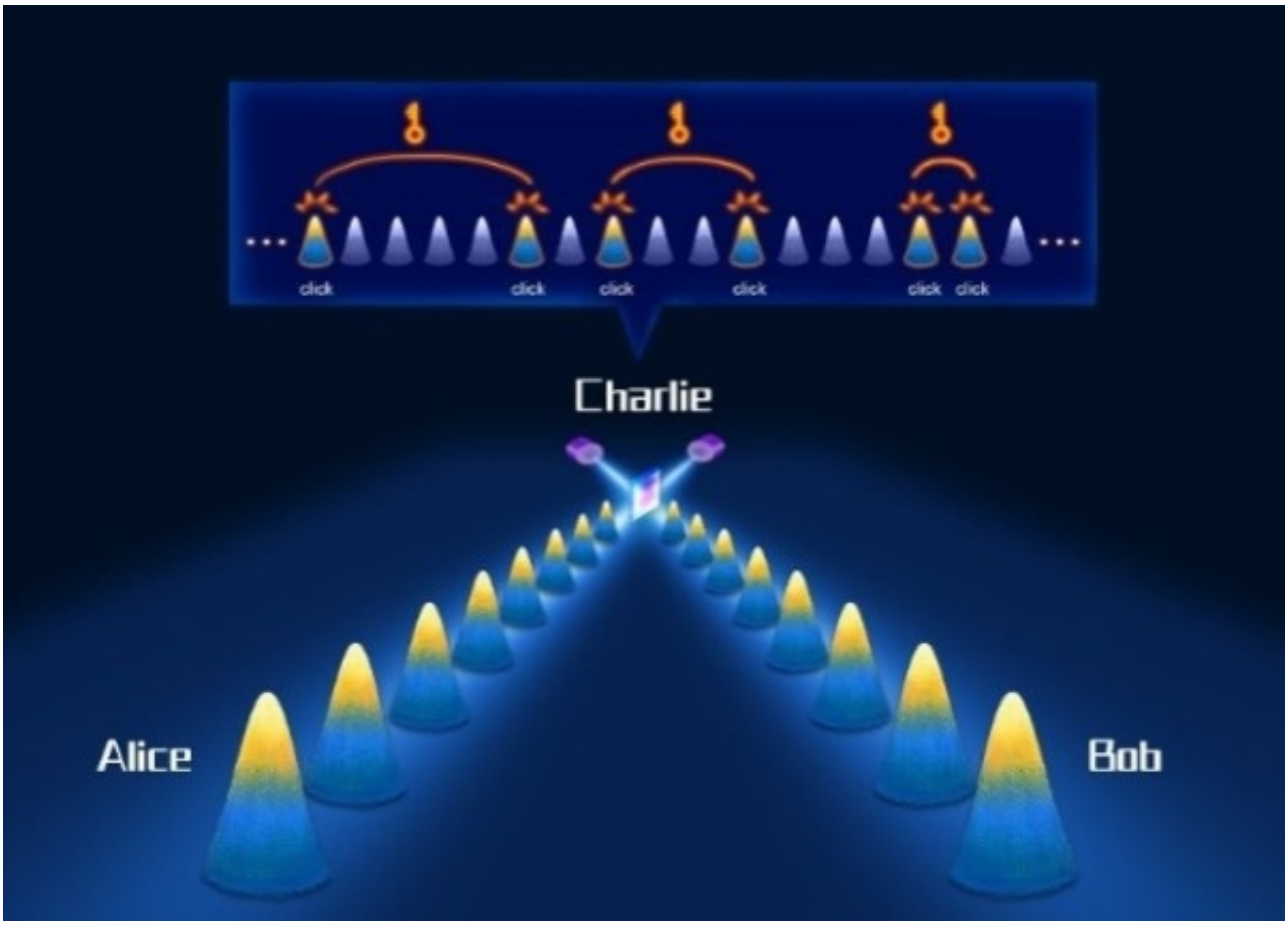

图1.模式匹配量子密钥分发协议示意图

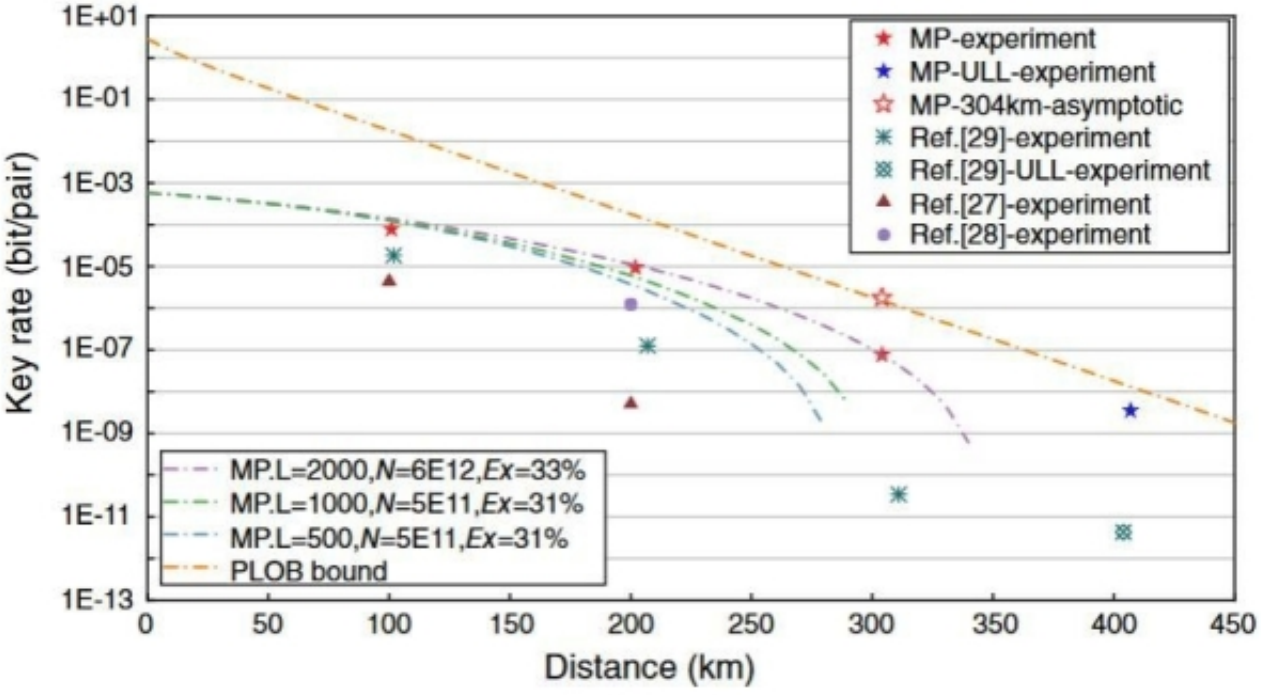

图2.模式匹配协议的成码率比较图

研究团队单位：中国科学技术大学