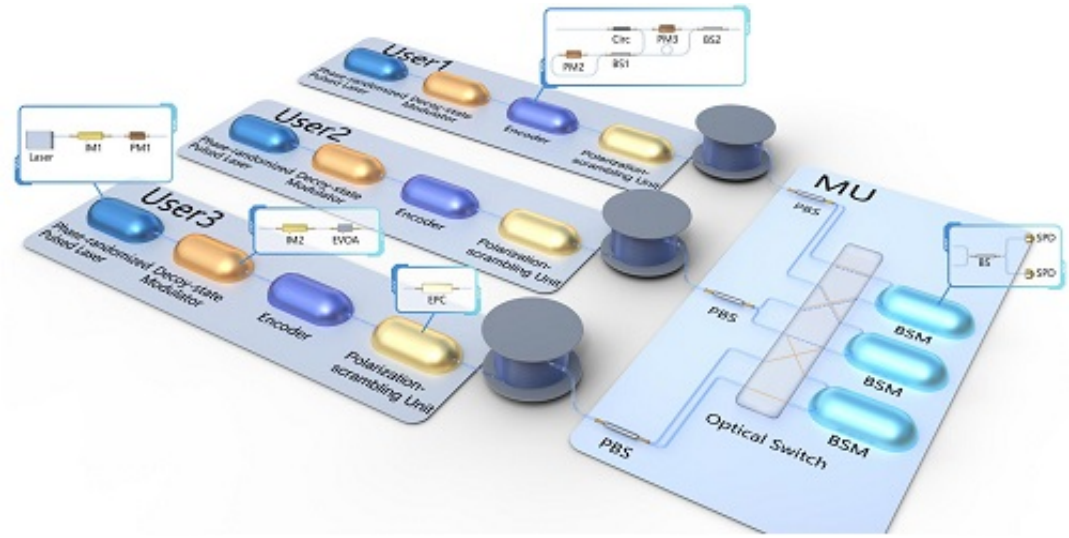
节点不必可信的量子密钥分发网络已实现

作者：writer 来源：爱科学

本文原地址：https://www.iikx.com/news/progress/19326.html

节点不必可信的量子密钥分发网络已实现。

中国科学技术大学郭光灿院士团队韩正甫教授及其合作者王双、银振强、陈巍等，实现了抗环境干扰的非可信节点量子密钥分发网络，全面提高了量子密钥分发网络的安全性、可用性和可靠性，向实现下一代量子网络迈出了重要一步。相关研究成果日前在线发表于国际学术知名期刊《光学》。



测量设备无关量子网络的实施框图 课题组供图

网络安全是信息时代的重要主题，量子密钥分发网络以量子物理原理为基础，可为成千上万的用户提供信息论安全的保密通信服务，构建安全可控的网络环境。当前，量子保密通信网络已在全球各地先后部署，证明了其优越的安全通信能力。

在量子分发网络的过程中，由于技术条件限制，中间会设置接力点——中继节点。为了确保网络的安全性，需要对这些节点进行严格的安全防护，研究人员称之为可信节点。相反地，如果不需要做安全保护，即为非可信节点。

做安全防护需要大量昂贵的硬件，因此建立可信节点量子保密通信网络需要巨大成本，而且太多额外的硬件还会降低系统的安全性。韩正甫介绍，如何免除用户链路上必须可信的中间节点，降低对通信链路的安全性要求，从而构建下一代基于非可信节点的量子网络，是目前急需解决的问题。

测量设备无关量子密钥分发协议（MDI-QKD）通过设置一个非可信节点对编码量子态进行联合测量，可在两个用户间构建安全的通信链路，是构建百公里级城域量子网络的重要角色。然而，联合测量不仅限定了参与用户的数量，还对信道环境的稳定性提出更高要求，不利于在复杂网络环境下进行部署。

多年来，韩正甫课题组围绕这一问题展开深入研究，2015年实现了参考系测量设备双无关系统，解决了相位扰动的问题；2017年设计出环境鲁棒型系统，进一步实现了抗偏振扰动能力；2021年提出非独立组网方案，探索测量设备无关系统的网络化路线。至此，课题组具备解决MDI-QKD网络的多用户可用性和环境干扰下可靠性问题的条件。

此次研究中，课题组设计萨格纳克-马赫-曾德尔结构的非相敏量子编码器，能够免除相位参考系的补偿。同时，课题组借助随机化，擦除了编码量子态的偏振信息，使其具备抗信道偏振扰动能力。最后，课题组重新利用偏振维度进行多用户配对，能够同步实现多对用户的强度干涉（HOM干涉）和联合测量。

在此基础上，课题组完成了测量设备无关量子密钥分发网络的构建，使其同时具备抗环境干扰、无需可信节点、支持多用户灵活组网的特性。

研究成果推动了下一代量子保密通信网络的实用化，为未来量子互联网的具体形态做出有益探索。（来源：中国科学报王敏）

相关论文信息：https://doi.org/10.1364/OPTICA.458937

作者：郭光灿等 来源：《光学》