科学家首次实现设备无关量子密钥分发

作者：writer 来源：爱科学

本文原地址：https://www.iikx.com/news/progress/19482.html

科学家首次实现设备无关量子密钥分发。

中国科学技术大学潘建伟院士及其同事张强、徐飞虎等，通过发展设备无关理论协议和构建高效率的光学量子纠缠系统，首次在国际上实验实现了设备无关量子密钥分发（DI-QKD）的原理性演示。研究成果以编辑推荐的形式在线发表于《物理评论快报》。

设备无关量子密钥分发实验装置 中国科大供图

量子密钥分发（QKD）相比于传统通信协议，能够使得两个远距离的用户之间共享信息理论安全性的密钥，结合一次一密的加密方式，可以确保原理上无条件安全的通信。传统QKD方案通常需要对使用的设备有一定了解和信任，然而在现实条件下，设备可能存在某些不完美特性。这些特性往往会为攻击者提供威胁系统安全的侧信道，造成现实条件下的潜在安全隐患。目前的主要解决方案是对设备进行检测并制定相关标准，从而确保其在现实条件下的安全性。

设备无关量子密钥分发（DI-QKD）基于无漏洞量子力学基础检验，提供了一套全新的不依赖于设备具体功能和特性的安全成码方案。基于该协议，不需要对设备进行任何标定，并且可以保证QKD的现实安全性。然而，DI-QKD的实现十分困难，如在光学系统中，现有理论大都给出了不低于90%的系统探测效率要求，远远超出了现有的技术水平。

为实现这一目标，潘建伟团队分别从理论和实验两方面进行探索研究。理论方面，团队提出原创的随机后选择DI-QKD理论方案。其核心思想是通过在实验测量结果中随机添加噪声，并将其中包含少量关联信息但拥有较大错误的结果剔除掉，从而有效提升系统对于损耗的容忍度，使得现有技术水平下DI-QKD的实现成为可能。

实验方面，团队利用自发参量下转换的原理，通过优化空间光路的参数搭建了高效率的光学纠缠源，并结合高效率的单光子探测器，使系统效率达到87.5%，超过了以往所有报道的相关光学实验。同时，使实验中产生的量子态保真度达到99.5%，满足了理论方案对于系统性能的要求。

在此基础上，潘建伟团队首次实现了基于全光学系统的DI-QKD原理演示，成码率达到466bps，并且验证了该系统在光纤长度达到220m时，仍然可以产生安全的量子密钥。

据悉，这是潘建伟团队在设备无关量子信息处理方面，继设备无关量子力学基础检验和设备无关量子随机数产生之后的又一重要进展。这项工作对于揭示量子力学基础检验和量子信息处理之间内在的深刻联系，发展安全的密钥分发、构建未来的量子网络均具有重要意义。（来源：中国科学报王敏）

相关论文信息：https://doi.org/10.1103/PhysRevLett.129.050502

作者：潘建伟等 来源：《物理评论快报》