中国科学家成功解决单光子探测系统的安全隐患

文章来源：中国科学技术大学 发布时间：2013-09-29 【字号： 小 中 大 】

最近，由中国科学技术大学潘建伟院士及其同事张强、陈腾云与清华大学马雄峰等组成的联合研究小组，利用与美国斯坦福大学联合开发的高效低噪声上转换单光子探测器，在国际上首次实现了测量器件无关的量子密钥分发，成功解决了现实环境中单光子探测系统易被黑客攻击的安全隐患，大大提高了现实量子密钥分发系统的安全性。该研究成果发表在9月24日出版的《物理评论快报》上。

量子密钥分发以量子物理与信息学为基础，被认为是安全性最高的加密方式。然而，尽管量子密钥分发在理论上具有无条件安全性，由于原始方案要求使用理想的单光子源和单光子探测器，在现实条件下很难实现，导致现实的量子密钥分发系统可能存在各种各样的安全隐患。随着该研究小组2007年在国际上首次实现百公里量级的诱骗态量子密钥分发，成功解决了非理想单光子源带来的安全性漏洞，探测器的不完美性成为“量子黑客”的主要攻击点，国际上多个小组提出了“时间位移攻击”、“死时间攻击”和“强光致盲攻击”等针对探测系统的攻击方案。虽然所有已知的量子黑客攻击均可以通过对现有量子密码系统的适当改造加以防御，但在理论上安全隐患仍然存在。那么是否有一个量子密钥分发系统可以从根本上完美解决所有已知和未知的针对探测系统的攻击呢？

潘建伟小组发展了独立激光光源的干涉技术，并与美国斯坦福大学联合开发了国际上迄今为止最先进的室温通信波段单光子探测器——基于周期极化铌酸锂波导的上转换探测器，在此基础上，结合清华大学马雄峰教授的理论分析，在世界上首次实现了测量设备无关的安全量子密钥分发，该实验先天免疫于任何针对探测系统的攻击，完美地解决了探测系统的安全隐患问题。另外，该实验系统兼顾采用诱骗态方案，同时保证了非理想光源系统的安全性。

由于该工作在实用化量子通信领域的重要意义，被审稿人称赞为“该领域的重要贡献”。同时，《物理评论快报》也以新闻发布的形式向科技界新闻媒体重点推介了该工作，包括《科学》杂志、《物理学观点》和《经济学人》在内的多家欧美科技新闻媒体都对此工作进行了专题报道。

该研究得到了中国科学院、国家自然科学基金委、科技部和山东省的支持，特别是科技部“973”青年项目、中组部“青年千人”、中科院“百人计划”和山东省量子通信公共研发平台等项目的支持。