【科技日报】量子密钥分发系统可免遭黑客攻击

文章来源：科技日报 吴长锋 发布时间：2013-09-28 【字号： 小 中 大 】

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。相关成果发表在9月24日出版的国际权威物理学期刊《物理评论快报》上。

尽管量子密钥分发在理论上具有无条件安全性，但由于原始方案要求使用的理想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安全隐患。2007年，该研究组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，但随后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。是否有一个量子密钥分发系统可以从根本上解决所有针对探测系统的攻击？

基于这一构想，潘建伟小组发展了独立激光光源的干涉技术，并与斯坦福大学联合开发了迄今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，该实验系统同时保证了非理想光源系统的安全性。该工作在实用化量子通信领域具有重要意义，包括《科学》在内的多家权威科技媒体都对此进行了报道。

（原载于《科技日报》 2013-09-28 01版）