量子密码安全领域研究获重要突破

作者：吴兰 来源：中国新闻网

本文原地址：https://www.iikx.com/news/progress/3596.html

量子密码安全领域研究获重要突破。记者1月4日从中国科学技术大学获悉，该校郭光灿院士团队在量子密码安全领域——量子密钥分发实际安全性研究中获得重要突破，利用探测器雪崩时的漏洞，量子黑客可有效控制该探测器的响应，并获取全部密钥信息而不被感知。

国际著名学术期刊Physical Review Applied近日刊发了以上科研成果。

随着量子密钥分发系统速率不断提高，单光子探测器的后脉冲效应将显著增强。后脉冲是指探测器中的雪崩光电二极管在发生雪崩之后，一段时间内随机产生二次雪崩的现象，其非完美性会带来安全性漏洞，是实际系统安全性测评的重要内容。过去忽略后脉冲效应的模型需要修正。

鉴于此，科研人员基于自身多年来对探测器的深入研究，针对量子密钥分发系统中单光子探测器实际特性提出了新的模型。该模型将高阶后脉冲考虑在内，给出了新的计数率和误码率的计算方法，显著提升了高速实用化系统的核心性能指标。

雪崩光电二极管探测器的非完美性会带来安全性漏洞，是实际系统安全性测评的重要内容。科研人员发现了门控模式单光子探测器的一种潜在漏洞，提出并实现了雪崩过渡区攻击方法。在门控信号从开启到关闭的过渡阶段，探测输出具有很强的非线性特性。通过控制攻击信号的光强和在过渡区的位置，量子黑客可以有效控制该探测器的响应，获取全部密钥信息而不被感知。

据介绍，该攻击方法为实际系统的安全性测评和标准化提供了技术储备。

相关论文信息：https://doi.org/10.1103/PhysRevApplied.10.064032