中国科大在量子密钥分发实际安全性研究中取得突破

作者：writer 来源：中国科学院

本文原地址：https://www.iikx.com/news/progress/3571.html

中国科大在量子密钥分发实际安全性研究中取得突破。中国科学院院士、中国科学技术大学教授郭光灿团队在量子密码安全领域取得新进展，该团队的王双、银振强、陈巍、韩正甫等人针对量子密钥分发系统中单光子探测器实际特性展开研究，提出了包含后脉冲效应的系统优化模型，并利用雪崩过渡区非线性特性实现量子黑客攻击，为量子密钥分发系统的实际安全性分析和测评提供了新思路和技术手段。这两项成果同期发表在2018年12月的Physical Review Applied上。

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。过去忽略后脉冲效应的模型需要修正：一方面后脉冲会在系统中引入更多的错误响应，另一方面系统参数的优化可有效提高安全密钥生成率。因此，韩正甫研究组基于自身多年来对探测器的深入研究[J. Lightwave. Technol. 34, 3610 (2016); J. Lightwave. Technol. 35, 4996 (2017)]，利用后脉冲过程的非马尔科夫特性，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。韩正甫研究组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。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。

这两篇论文的第一作者分别是博士生范元冠杰、钱泳君和实验师何德勇(共同第一作者)，中国科大教授王双和银振强为文章的通讯作者。这项工作得到科技部、国家自然科学基金委、中科院和安徽省引导项目的资助。

论文链接：1 2

图1.不同后脉冲率下新旧模型的密钥率对比

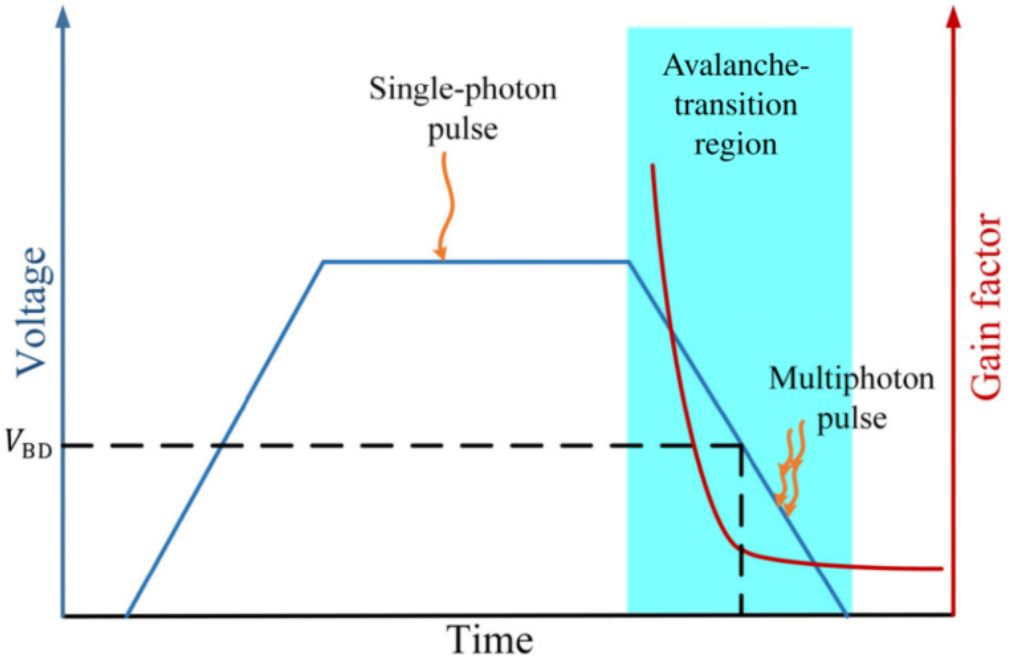

图2.雪崩过渡区原理图