中国科大在量子密钥分发实际安全性研究方面取得进展

作者：writer 来源：中国科学院

本文原地址：https://www.iikx.com/news/progress/6937.html

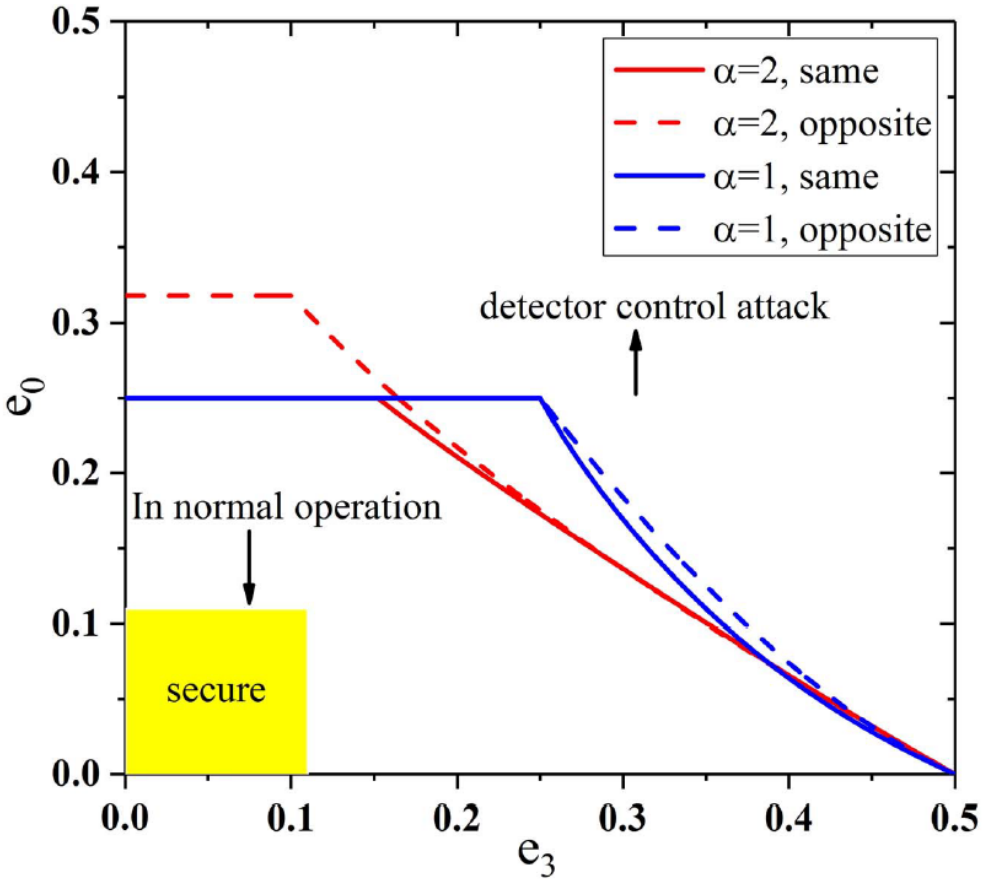
中国科大在量子密钥分发实际安全性研究方面取得进展。中国科学院院士、中国科学技术大学教授郭光灿团队的王双、陈巍、银振强、韩正甫等人提出并验证了一种可以有效抵御量子密钥分发系统探测器控制攻击的方法，为提高实用化BB84量子密钥分发系统的安全性提供了新思路。该研究成果于9月11日发表在期刊Optica上。

量子密钥分发是量子信息领域实用化程度最高的技术，它在协议上允许异地通信双方共享信息论安全的密钥。由于实际器件的不完美，单光子探测器是量子密钥分发系统接收端最容易被攻击的核心器件。探测器控制攻击是其中最主要的一类探测器侧信道攻击方法。攻击者采取截取-重发策略，在特定条件下可以控制接收端单光子探测器的输出信号，从而窃取密钥而不被感知。采用测量器件无关的量子密钥分发协议可以彻底消除单光子探测器的漏洞，然而该协议尚未在已有的量子密钥分发试验网络中得到广泛部署;另一类有效方案是针对探测器的具体漏洞采取防御措施，其实施方法与探测器的实现细节相关，只能解决针对具体漏洞的特定攻击。例如，监控雪崩光电二极管的光电流可以有效防御探测器致盲控制攻击，但该方法难以同时防御韩正甫课题组最近提出的雪崩过渡区攻击(Physical Review Applied, 10, 064062(2018))。

为了有效抵御探测器控制攻击，韩正甫研究组提出一种可变衰减探测器防御模型：该模型将单光子探测器作为一个黑盒子，通过在单光子探测器前增加一个可变衰减器，并随机改变可变衰减器的衰减值。根据理论上严格证明的防御判据，对计数率和量子比特误码率进行对比分析，可以有效防御这一类探测器控制攻击。同时，由于该防御模型和探测器具体的实现方式无关，因此适用于半导体单光子探测器、超导探测器以及光电倍增管等多种单光子探测器。

该防御方法只需将现有量子密钥分发系统中的单光子探测器替换成可变衰减单光子探测器，在系统实际安全性和复杂性之间取得了较好的平衡。该方法提供的新思路不依赖于探测器的具体技术参数，具有普适性，可有效用于量子密钥分发系统的安全性测评和标准化。

博士生钱泳君和高级工程师何德勇是文章的共同第一作者，王双为文章的通讯作者。这项工作得到科技部、国家自然科学基金委、中科院和安徽省的资助。



两种衰减下量子比特误码率的安全界限