源无关量子随机数研究获重要进展

作者：writer 来源：爱科学

本文原地址：https://www.iikx.com/news/progress/12241.html

源无关量子随机数研究获重要进展。中国科学技术大学郭光灿团队王双、韩正甫等人针对源无关量子随机数系统中测量设备的实际特性，提出测量端由于探测器后脉冲、探测效率不匹配、探测器对光源分布敏感等特性所带来的安全性问题，并给出相应的解决方案。该成果日前发表于《njp量子信息》。

源无关量子随机数协议，是2016年提出的一种新型量子随机数协议。该协议通过监测用于生成随机数的相互无偏基的误码，可以在光源不可信的情况下，产生安全的私密随机数。这一协议可同时兼顾随机数发生器的安全性与高速率需求，并可容忍非常高的设备损耗。但其没有考虑探测器后脉冲效应、多探测器的探测效率不匹配、探测器对光源分布敏感等特性所带来的重要安全性隐患，严重限制了协议的实际应用。

王双、韩正甫等人设计了一个包含以上参数的探测器模型，并评估了对现实安全性的影响。针对探测器后脉冲效应，给出窃听者能获得随机数信息的最小熵下界；针对探测效率不匹配和探测器对光源分布敏感问题，提出一种光源分布监测方法，并在充分考虑有限码长效应的条件下给出基于组合安全性的码率公式。

该成果量化分析了测量设备不完美性对源无关量子随机数系统的安全性影响，为实现超快实用化的源无关量子随机数发生器提供了解决方案。（来源：中国科学报 桂运安）

相关论文信息：https://doi.org/10.1038/s41534-020-00331-9