中国科大提出并实现新型量子随机数发生器

作者：writer 来源：爱科学

本文原地址：https://www.iikx.com/news/progress/19483.html

中国科大提出并实现新型量子随机数发生器。

中国科学技术大学郭光灿院士团队韩正甫教授及其合作者王双、银振强、陈巍等，提出了一种新型的半设备无关量子随机数发生器协议，并进行了实验验证。该协议即使在光源不可信条件下，也无需对探测设备进行表征，使用日常光源即可快速生成安全的量子随机数。该协议全面地提升了量子随机数发生器的安全性与实用性，为半设备无关量子随机数发生器的实用化奠定了坚实基础。相关研究成果日前在线发表于著名国际学术期刊《物理评论快报》。

新型半设备无关量子随机数发生器结构示意图中国科大供图

随机数是信息时代的一种重要基础资源。量子随机数发生器基于量子物理原理产生具有内禀随机性的真随机数，为科学仿真、密码学等领域提供了极大的助力。在目前受到广泛关注的量子保密通信中，量子随机数发生器更是其中的关键环节。然而，现实中的量子随机数发生器可能具有的非理想性会破坏随机数的不可预测性和私密性。虽然完全设备无关型量子随机数发生器可以容忍这些非理想性，但其协议实现困难，随机数产生速率低，成本高昂，距离实用化仍有很远的距离。

半设备无关量子随机数发生器对部分组件的要求大大放宽，提供了一种实际可行的安全实现方案，因而受到广泛关注。但因为已有的半设备无关方案忽略了一些关键因素对其性能的影响，限制了其在现实条件下的应用。

针对这一问题，韩正甫课题组开了深入的研究，于2020年提出容忍探测器后脉冲的源无关协议，2022年进一步降低了源无关量子随机数发生器对非理想因素的敏感性。这些工作显著提高了源无关量子随机数发生器的实用性，但均仍需要对测量设备进行精确的表征。

近期，课题组基于平滑熵的不确定关系和量子剩余哈希定理，提出了一种不需要对测量设备进行表征的新型半设备无关量子随机数发生器协议，并证明了该协议在源端不可信和探测端无表征条件下的安全性。

课题组同时使用卤素灯这一日常光源和激光器完成了验证实验，产生的随机数速率与目前商用随机数发生器相当，但安全性显著优于后者。

该成果在保证随机数快速生成和系统简洁实用的同时，大幅地降低了对设备可信度和刻画表征的要求，其思想和实现方案对突破高性能、高安全量子随机数发生器的研究瓶颈具有重要推动作用。（来源：中国科学报王敏）

相关论文信息：https://doi.org/10.1103/PhysRevLett.129.050506

作者：韩正甫等 来源：《物理评论快报》