中外学者合作实现设备无关量子随机性扩展实验

作者：writer 来源：爱科学

本文原地址：https://www.iikx.com/news/progress/13460.html

中外学者合作实现设备无关量子随机性扩展实验。

中国科学技术大学潘建伟院士及其同事张强、南方科技大学研究员范靖云等，分别与英国约克大学教授Roger Colbeck、清华大学教授马雄峰合作，采用不同理论方法，在国际上首次实现设备无关的量子随机性扩展，为设备无关量子随机数的实用化奠定坚实基础。相关研究成果近日分别发表于《自然—物理学》和《物理评论快报》。

随机性在人类的生产活动中无处不在，在信息安全、数值模拟、抽样检测和公益彩票等领域中有着重要应用。基于量子物理内禀特性产生的量子随机数，被认为是区别于经典随机数的一种真正不可预测的随机性资源。设备无关的量子随机数安全性仅仅与系统的输入、输出相关，而并不依赖于物理设备的质量和可信度。即使在极端条件下，设备本身不可信或受到第三方控制，乃至窃听者拥有强大的量子计算机，该方案产生的随机比特仍然具有目前最高等级的安全性。

潘建伟团队和合作者于2018年首次实验实现设备无关的量子随机数产生。但在此实验方案中，随机数产生过程中消耗的随机性远远大于产出，随机数产生的不可持续性，阻碍了其在实际应用中的推广。针对这一问题，潘建伟团队和合作者设计并实现了设备无关的量子随机性扩展。他们与Roger Colbeck合作，在基于熵累积理论的实验中，约在19.2小时内实现2.57×108比特的随机性净增加。英国学者Paul Skrzypczyk认为，该工作毫无疑问提供了最高质量的随机数，是量子技术快速发展的一个里程碑。

同时，他们与马雄峰团队合作，在基于量子概率估计方法的实验中，约在13.1小时内实现1.08×108比特的随机性净增加。《物理评论快报》审稿人认为，这是一项量子随机数产生、随机扩展领域中的开创性工作。（来源：中国科学报桂运安）

相关论文信息：

https://doi.org/10.1038/s41567-020-01147-2

https://doi.org/10.1103/PhysRevLett.126.050503

作者：潘建伟等 来源：《自然—物理学》