中国科大实现设备无关量子随机性扩展实验

来源：科研部 发布时间：2021-04-13 浏览次数：104

近日，中国科学技术大学教授潘建伟及其同事张强、南方科技大学范靖云等，与英国约克大学Roger Colbeck和清华大学马雄峰分别合作，采用不同的理论方法，在国际上首次实现了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发展奠定了坚实基础。相关的研究成果近日分别发表于《自然•物理学》[Nat. Physics17,448 (2021)]和《物理评论快报》[Phys. Rev. Lett. 126, 050503 (2021)]上。

随机性在人类的生产活动中无处不在，也是自然界的基本属性之一，在信息安全、数值模拟、抽样检测和公益彩票等多个领域中有着重要的应用。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。然而，量子随机数产生器若使用了恶意第三方生产的器件或设备，会有随机数泄露的隐患。设备无关的量子随机数产生协议解决了这一问题。与常规的量子随机数产生器不同，根据贝尔理论的指导，它的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。用户在使用这种量子随机数产生器时，只需根据其输入输出数据的统计结果来判断仪器是否发生故障或是否存在对设备构成安全威胁的恶意攻击。一旦统计结果符合协议要求，其安全性就得以保证。

设备无关的量子随机数产生的本质在于，无漏洞贝尔不等式的违背证明了固有的量子相干性是随机性的来源。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，任何基于量子或经典物理的策略都无法对结果进行预测。

潘建伟团队和合作者于2018年首次实验实现了设备无关的量子随机数产生，文章发表在《自然》(Nature)杂志[Nature 562, 548 (2018)]。但是在此实验方案中，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，潘建伟团队及其合作者们设计并实现了设备无关的量子随机性扩展。他们与约克大学Roger Colbeck教授合作，在基于熵累积理论的实验中，约在19.2小时内实现了2.57×10^8比特的随机性净增加。英国Bristol大学的Paul Skrzypczyk博士在《自然·物理学》的News & Views栏目撰文评价该工作“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”（undoubtedly among the highest-quality randomness ever produced. Moreover, they constitute a milestone in the development of quantum technologies）。同时，与清华大学马雄峰教授团队合作，在基于量子概率估计方法的实验中，约在13.1小时内实现了1.08×10^8比特的随机性净增加。该工作被《物理评论快报》审稿人给予高度认可，评论为“量子随机数产生/随机扩展领域中的开创性工作”（I believe it will be considered a seminal work in the field of quantum random number generation/randomness expansion）。两项研究成果分别使用不同的理论方案各自独立完成，为未来设备无关量子随机数的商业化与实用化奠定基础。

该研究工作得到了中科院、科技部“973”项目、国家自然科学基金、教育部、安徽省、上海市和广东省的支持。

文章链接：https://www.nature.com/articles/s41567-020-01147-2

https://journals.aps.org/prl/abstract/10.1103/PhysRevLett.126.050503

（合肥微尺度物质科学国家研究中心、中科院量子信息与量子科技创新研究院、科研部）

电话: 0551-63601954 传真: 0551-63601795 E-mail: ustckjc@ustc.edu.cn
办公地址：安徽省合肥市包河区金寨路96号中国科大东区老图书馆三楼 邮编: 230026