

中国科学家在国际上首次实现器件无关的量子随机数

作者：writer 来源：中国科学院

本文原地址：<https://www.iikx.com/news/progress/2185.html>

本文仅供学习交流之用，版权归原作者所有，请勿用于商业用途！

近日，中国科学技术大学教授潘建伟及其同事张强、范靖云、马雄峰等与中国科学院上海微系统与信息技术研究所和日本NTT基础科学实验室合作，在发展高品质纠缠光源和高效率单光子探测器件的基础上，利用量子纠缠的内禀随机性，在国际上首次成功实现器件无关的量子随机数。相关研究成果于北京时间9月20日凌晨在线发表在国际学术期刊《自然》杂志上。这项成果将在数值模拟和密码学等领域得到广泛应用，有望形成新的随机数国际标准。

随机数在科学研究和日常生活中都有着重要的应用：例如，天气预报、新药研发、新材料设计和核武器研制等领域，常常需要通过数值模拟进行计算，而数值模拟的关键就是要有大量随机数的输入；在游戏和人工智能等领域，需要使用随机数来控制系统的演化；在通信安全和现代密码学等领域，则需要第三方完全不知道的随机数作为安全性的基础。

以往通常有两类获取随机数的途径：基于软件算法实现或基于经典热噪声实现。软件算法实现的随机数是利用算法根据输入的随机数种子给出均匀分布的输出。然而，对于确定的输入，固定的算法将给出确定的输出序列，从这个角度上来说，这类随机数本质上是确定性的，并不真正随机。基于经典热噪声的随机数芯片读取当前物理环境中的噪声，并据此获得随机数。这类装置相对于基于软件算法的实现，由于环境中的变量更多，因此更难预测。然而在牛顿力学的框架下，即使影响随机数产生的变量非常多，但在每个变量的初始状态确定后，整个系统的运行状态及输出在原理上是可以预测的，因此这一类装置也是基于确定性的过程，只是某种更难预测的伪随机数(pseudo random number)。量子力学的发现从根本上改变了这一局面，因为其基本物理过程具有经典物理中所不具有的内禀随机性，从而可以制造出真正的随机数(true random number)产生器。

量子力学这种内禀的概率特性，从量子力学理论发展的初期就一直深深困扰着爱因斯坦、薛定谔和温伯格等物理学家。爱因斯坦坚信“上帝是不会掷骰子的”(God does not play dice)，他认为一定存在着一个更高的确定性理论，量子力学只是该理论的近似，而量子力学的内禀随机性则只是因为人们不了解这种理论而带来的误解。爱因斯坦和薛定谔等人提出了量子纠缠的概念，试图用量子纠缠这种奇怪的量子状态来论证量子力学基础的不完备和量子随机性的荒谬。而以玻尔为首的哥本哈根学派则捍卫量子随机性，认为量子力学的基础是完备的。两个学派进行了长达30年的争论，但在当时，两种观念没能给出在实验上可以加以严格区分的精确预言，所有的争论都局限于哲学层面。直到1964年，美国物理学家贝尔发现通过对量子纠缠进行关联测量，量子力学和定域确定性理论会对测量结果有着不同的预言。利用这个特性即可开展贝尔实验检验，从而判定量子力学的基础是否完备和量子随机性是否存在。

贝尔的理论提出之后的几十年中，世界各国的众多科研小组进行了大量的实验，量子力学和量子随机性经受住了相关的实验检验。然而到目前为止，尚有两个漏洞需要关闭，即自由选择漏洞(freedom-of-choice loophole)和塌缩的定域性漏洞(collapse locality loophole)。潘建伟小组长期从事量子力学基础检验，针对这两个漏洞，他们分别利用观察者自主选择和遥远星体发光产生的随机数，于今年分别实验实现了超高损耗下和有观察者参与的贝尔实验检验，文章先后发表在《物理评论快报》[Phys. Rev. Lett.120, 140405 (2018)]、[Phys. Rev. Lett.21, 080404 (2018)]和《自然》[Nature557, 212 (2018)]杂志上，为最终实现无漏洞贝尔实验检验奠定坚实的科学和技术基础。

重要而有趣的是，由于贝尔实验与量子内禀随机性存在着深刻的内在联系，贝尔实验的检验可以从根本上排除定域确定性理论，从而实现不依赖于器件的量子随机数，即器件无关量子随机数。这类随机数发生器被认为是安全性最高的随机数产生装置，即使采用恶意第三方制造的组件，或者窃听者拥有计算能力最强的量子计算机，也无法预测或获知它所产生的随机数。因此目前国际上纷纷开展这种随机数产生器的研制工作，美国国家标准局(NIST)正计划利用器件无关的量子随机数产生器建立新一代的随机数国家标准。

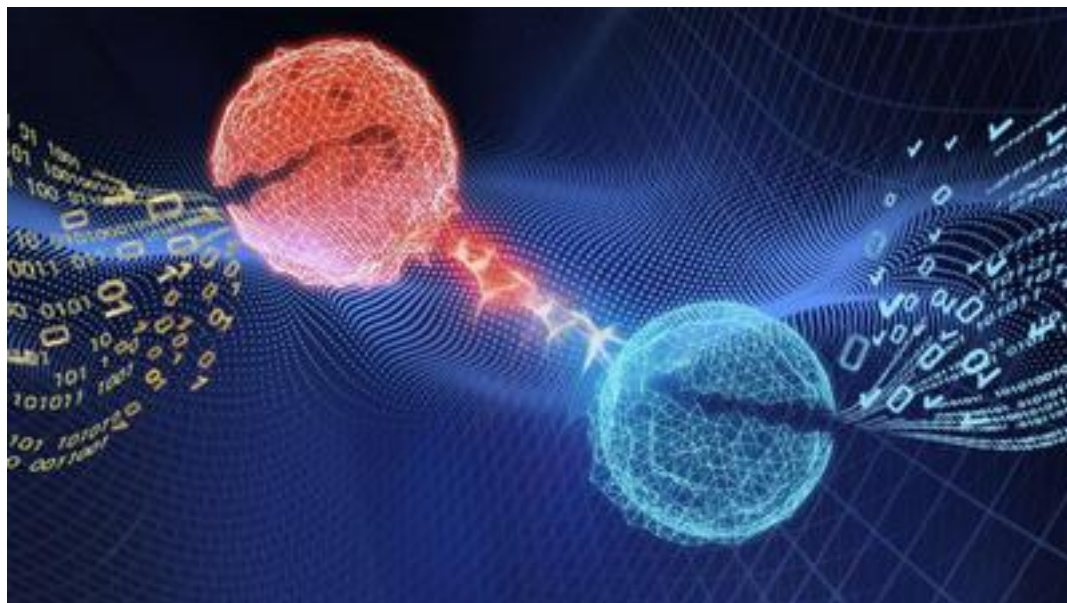
实现器件无关的量子随机数产生器在实验上具有极高的技术挑战：整套随机数产生装置需要以极高的效率进行纠缠光子的产生、传输、调制、探测；同时，不同组件间需要设置合适的空间距离以满足类空间隔要求，才能以最高的安全性保证任何窃听者不能通过内部通信伪造贝尔不等式测试的结果。

潘建伟、张强研究组在此前系列贝尔实验中发展的技术基础上，经过三年多的努力发展了高性能纠缠光源，首先优化了纠缠光子收集、传输、调制等效率，并采用上海微系统所开发的高效率超导单光子探测器件，实现了高性能纠缠光源的高效探测[Phys. Rev. Lett.120, 010503 (2018)]；然后通过设计快速调制并进行合适的空间分隔设计，满足了器件无关的量子随机数产生装置所需的类空间隔要求。最终，在世界上首次实现了器件无关的量子随机数产生器。

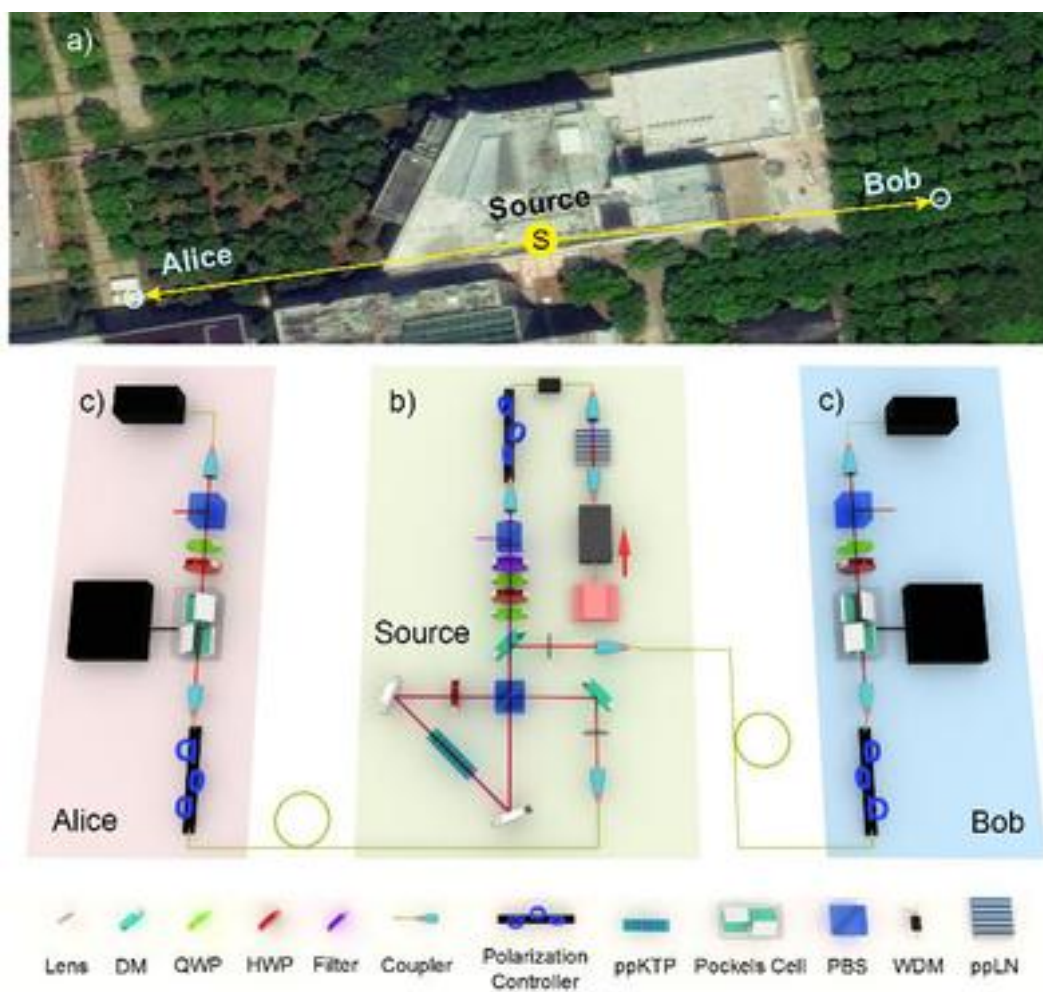
该工作及后续工作将为密码学和数值模拟以及需要随机性输入的各个领域提供真正可靠的随机性来源，同时由于可信任的随机数源是现实条件下量子通信安全性的关键环节，器件无关随机数的实验实现也进一步确保了现实条件下量子通信的安全性。未来，中国科大团队将建设高速稳定的器件无关量子随机数产生装置，通过提供基于量子纠缠内禀随机性的、高安全性的随机数，争取形成新一代的国家随机数标准。

该研究工作得到中科院、科技部、国家自然科学基金委、教育部和安徽省的支持。

文章链接



基于量子纠缠的量子随机数产生示意图



器件无关量子随机数实验装置

更多 科学进展 请访问 <https://www.iikx.com/news/progress/>

本文版权归原作者所有，请勿用于商业用途，[爱科学iikx.com](https://www.iikx.com)转发