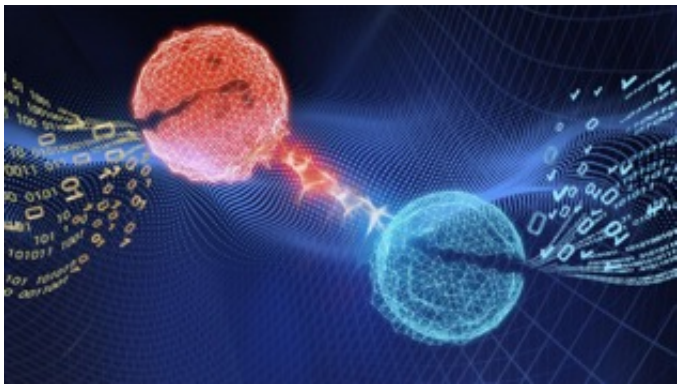
# 中国科大在国际上首次实现器件无关的量子随机数

作者：丁佳 来源：科学网

本文原地址：https://www.iikx.com/news/progress/2179.html





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9月20日凌晨在线发表在《自然》杂志上。

这项突破性成果将在数值模拟、密码学等领域得到广泛的应用，有望形成新的随机数国际标准。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，并采用中科院上海微系统所开发的高效率超导单光子探测器，实现了高性能纠缠光源的高效探测;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、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。

在现有的量子通信系统中，如果采用自己制备的或者可信制造商制备的量子随机数产生器，其安全性是可以得到保障的。但是如果人们不小心采用了恶意第三方所制造的器件，就会发生随机数泄漏。潘建伟说，我们的新成果确保了即使是使用不信任的第三方器件的情况下，也可以产生真随机数，并且不会泄漏，从而确保通信的安全。 潘建伟透露，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际随机数标准。

随机数在科学研究和日常生活中都有着重要的应用，如天气预报、新药设计、材料设计、工业设计、游戏、人工智能、通信安全、现代密码学等领域都有应用。然而，以往基于软件算法或基于经典热噪声实现的随机数都有着各自的缺陷，因此，目前国际上纷纷开展器件无关的量子随机数产生器的研制工作。(来源：科学网 丁佳)