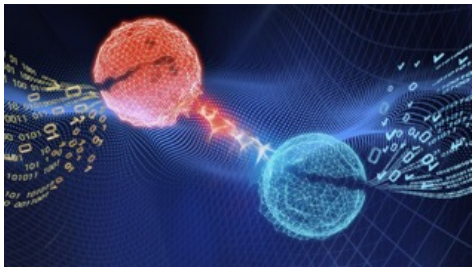
作者：丁佳 来源：科学网 www.sciencenet.cn 发布时间：2018/9/20 9:10:04 选择字号：小 中 大

# 中国科大在国际上首次实现器件无关的量子随机数



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。

Doi：http://dx.doi.org/10.1038/s41586-018-0559-3



相关新闻 相关论文

1 中国科大六十年：频频挺进“科学无人区”
2 还在吐槽量子计负？！你太孤陋寡闻了……
3 中科大在水溶液环境实现单生物分子磁共振谱探测
4 辉煌、非议、坚持：中科大少年班风雨四十年
5 “天河二号”算出量子霸权标准
6 中科院量子存储器：专门打破纪录的“三明治”
7 我国研制成功多自由度复用多功能固态量子存储器
8 我国实现基于星光随机数的贝尔不等式检验

图片新闻

>>更多

一周新闻排行 一周新闻评论排行

1 美英科学家获2018年度诺贝尔化学奖
2 掌控进化：生命这样被改写
3 陈列平与诺奖失之交臂 专家：原因有三
4 今年诺奖自然科学奖“写满”两个字：续命
5 18年里18人获奖，好学术环境比诺奖更重要
6 华人女科学家曹颖获美国“天才奖”
7 科技发展40年：多项指标世界领先
8 考研人数攀升，为何推免比例还更高？
9 院士为栽培技术鸣不平：研发投入勿“跑偏”
10 “上帝粒子”之父利昂·莱德曼逝世

更多>>

- AP版数理物理学百科 3324页
- 物理学定律的特性 feynman
- 波恩的光学原理
- 弦论的发展史
- 时间与物理学
- 矩阵分析 霍恩 (Roger A.Horn)著

更多>>

打印 发E-mail给：

以下评论只代表网友个人观点，不代表科学网观点。

2018/9/20 18:06:06 wangguowen

谁说量子纠缠存在内禀随机性

何谓量子纠缠？按照量子纠缠公式，可以做个比喻：县委书记任命双胞胎兄弟李左和李右各为东乡和西乡的书记，并且任命李左兼任西乡的乡长和李右兼任东乡的乡长。所以，东乡的书记一感冒，西乡的乡长就咳嗽。东乡书记随意掷一下骰子是5点，当然西乡乡长掷的骰子也是5点。何来内禀随机性？机遇与因果哪个更根本？1944年9月7日爱因斯坦在致玻恩的信中说：“在我们的科学期望中，我们已成为对立的两极。你信仰掷骰子的上帝，我却信仰客观存在的世界中的完备定律和秩序。”诺奖得主温伯格的看法是：量子力学波函数随时间演化的方程——薛定谔方程，本身并不涉及概率。它就像牛顿运动方程和引力方程一样具有确定性。

2018/9/20 9:40:35 yspdoudou

我们常用Monte Carlo实验生成随机数。量子产生随机数，与这有什么不同呢?

目前已有2条评论

查看所有评论

需要登录后才能发表评论，请点击 [登录]