可自测的硅光子量子随机数生成器芯片制成

作者：writer 来源：科学网

本文原地址：https://www.iikx.com/news/progress/40317.html

可自测的硅光子量子随机数生成器芯片制成
。科技日报北京6月9日电（记者张梦然）新加坡国立大学设计与工程学院研究团队日前宣布，开发出一款可实现自测功能的硅光子量子随机数生成器芯片。这一突破解决了数十年来随机数生成器完全信任硬件所致的安全隐患，为数字基础设施提供了可证明的量子级安全保障。该成果发表于最新一期《PRXQuantum》期刊。

在现代密码体系中，随机数是加密密钥、安全交易和数字签名的基石，其不可预测性直接决定系统安全性。传统方案，包括量子随机数生成器，均要求用户完全信任硬件制造商对组件特性的标定，一旦探测器因老化或恶意篡改出现偏差，输出可能变得可预测而无法被察觉。随着量子计算发展，此类硬件漏洞可能被量子攻击者利用，构成实质性威胁。

团队此次彻底改变了这一现状。该芯片无需信任读取光信号的光电探测器，仅需保证输入光态的可信度。每次运行中，芯片制备并测量已知量子光态，通过比对输出结果与量子理论预测值，实时验证硬件完整性。若评分达标，原始数据被提炼为认证随机比特；若异常则立即终止。

团队采用八英寸标准硅晶圆工艺集成信号编码器与探测器，实现室温运行，避免了量子系统常见的低温冷却需求。针对硅基光调制器中相位调整与亮度变化的耦合效应，他们设计出特殊驱动方案，利用调制器非线性响应抵消干扰，确保量子态纯度。实验显示，芯片探测器效率达69.1%，超过协议要求的67%的安全阈值，且可证实其生成的是真正独立的新鲜随机数。

不过，当前实验速率仅为每秒64比特，低于传统可信设备量子随机数生成器超每秒100千兆比特的速度，但其安全等级达到芯片级最高水平。团队透露，速度的主要限制因素是探测器效率，采用已验证的效率达92.4%的新型光电二极管进行模拟，预计速率可提升至每秒68兆比特，比目前的实验值高出五个数量级以上。

该芯片有望广泛应用于密码学、金融服务、AI、医疗健康及物联网等领域，为构建抗量子攻击的安全系统提供可行路径。

作者：张梦然 来源：科技日报