中国科大等实现基于器件无关量子随机数信标的零知识证明

作者：writer 来源：中国科学院

本文原地址：https://www.iikx.com/news/progress/25241.html

近日，中国科学技术大学潘建伟、张强等，联合上海交通大学、清华大学、南方科技大学等，首次实现了一套以器件无关量子随机数产生器作为熵源，以后量子密码作为身份认证的随机数信标公共服务，将其应用到零知识证明（ZKP）领域中，消除了非交互式零知识证明（NIZKP）中实现真随机数的困难所带来的安全隐患，提高了NIZKP的安全性。相关研究成果发表在《美国国家科学院院刊》（*PNAS*）上。

零知识证明（ZKP）是一种基本的密码学工具，允许互不信任的通信双方之间，一方向另一方证明某个命题的有效性，同时不泄露任何额外信息。非交互式零知识证明（NIZKP）是ZKP的最重要的变体之一，其特点是通信双方无需多次信息交换。由于简单易行且互相通信次数少，NIZKP广泛应用于数字签名、区块链和身份认证等领域。常用的NIZKP系统的安全性建立在生成可信的真随机数的假设之上。而实际应用中，由于真随机数生成器难以实现，通常会使用确定性的伪随机数算法来替代。已有研究认为，这种方法会产生潜在的安全隐患。

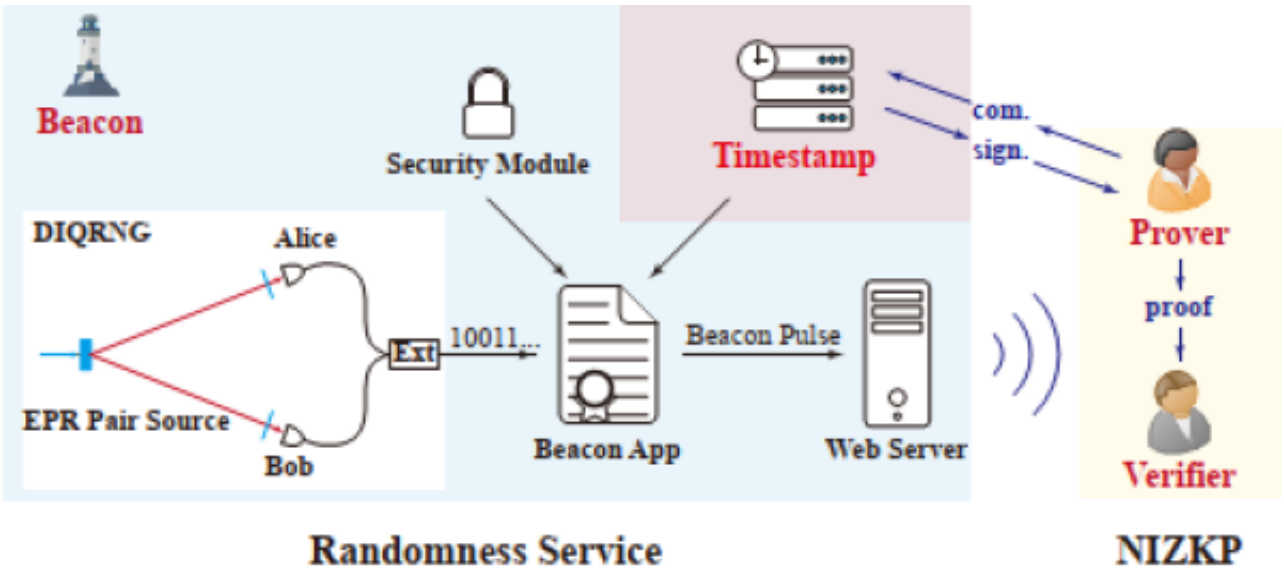
量子物理学的内禀随机性为解决这一安全隐患提供了全新方案。特别地，基于无漏洞贝尔不等式检验的器件无关量子随机数（DIQRNG）可以提供具有最高安全等级的真随机数，其安全性由量子力学基本原理保证，无需用户对量子设备进行任何先验表征或假设。该团队于2018年在国际上首次了实现可抵御量子攻击的DIQRNG，并于2021年提升了随机数产生速度。

该工作搭建了基于DIQRNG的信标公共服务系统，并利用该系统设计并实施了一种不依赖于真随机数假设的NIZKP方案。该随机数信标服务可以实时向公众广播生成的随机数。此外，为确保随机数在广播过程中的安全性，该研究采用了可以抵御量子攻击的量子安全签名算法。进一步，研究利用接收到的来自DIQRNG的随机数代替之前的伪随机数，构建并实验验证了更安全的NIZKP协议。

该研究首次将量子非局域性、量子安全算法和零知识证明三个不同的领域结合起来，提升了零知识证明的安全性。其中，构建的面向公众的随机数服务在密码学和社会公益等领域具有潜在的应用价值。该量子随机数信标公共服务网址为https://randomnessbeacon.com。

研究工作得到科学技术部、国家自然科学基金委员会、中国科学院、安徽省、上海市和山东省的支持。

论文链接



中国科大实现基于器件无关量子随机数信标的零知识证明

研究团队单位：中国科学技术大学

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