芯片嵌入的高效量子数字签名

作者：writer 来源：科学网

本文原地址：https://www.iikx.com/news/progress/33449.html

芯片嵌入的高效量子数字签名。 导读

作为现代密码学的基石，加密和数字签名可以保障信息安全的四个基本要素——保密性、完整性、真实性和不可抵赖性。与经典密码学不同，量子密码学依托量子力学基本原理提供了一种不依赖窃听者计算能力假设的量子密码工具箱。其中量子密钥分发保障信息传输的保密性，量子数字签名（QDS）确保信息传输的完整性、真实性和不可抵赖性。自2001年，首个QDS协议提出以来，国内外学者在QDS理论和实验方面进行了大量研究，致力于推进QDS的实用化进程。

近日，广西大学、国家信息光电子创新中心、中国人民大学以及南京大学合作，利用硅光子集成技术和单诱骗态一次全域哈希QDS协议，成功克服了QDS在实际应用中面临的设备体积大、成本高以及系统签名率低的难题。研究团队提出并验证了一种芯片嵌入的高效率量子数字签名网络。在200 km的通信距离下，签名1 Mbit文件实现了0.04次每秒的签名速率。该成果以Chip-integrated quantum signature network over 200 km为题发表在国际光学顶尖期刊《Light: Science Applications》，博士生杜永强（广西大学）、李炳宏（南京大学）、曹啸宇（南京大学）以及国家信息光电子创新中心华昕博士为该论文共同第一作者，广西大学韦克金教授、国家信息光电子创新中心总经理肖希以及中国人民大学副教授尹华磊为共同通信作者。

研究背景

在传统加密技术面临量子计算威胁的背景下，量子通信因其在信息安全性上的独特优势而备受关注。其中，量子数字签名（QDS）作为一种重要的密码学工具，因其能够保障信息传输的完整性、真实性和不可抵赖性，在电子商务、数字货币以及区块链等领域具有重要的应用价值。目前，QDS已经从概念验证迅速发展到成熟的系统演示，有望成为下一个商用量子密码技术。然而，此前所有的QDS系统均依赖昂贵、复杂的光纤光学设备，使其在大规模部署以及与现有通信基础设施无缝集成方面存在挑战。因此，发展低成本、高效率和易扩展的芯片化QDS网络具有重要的研究价值和广泛的应用前景。

研究内容

广西大学韦克金教授和国家信息光电子创新中心肖希博士团队长期致力于发展保障信息全要素安全的芯片级量子保密通信系统。该合作团队先后报道了具有偏振追踪能力的偏振编码量子密钥分发解码器芯片[Chip 2, 100039 (2023)]、资源节约型的芯片量子密钥分发系统[Photon. Res. 11, 1364-1372 (2023)]、源无关芯片量子随机数发生器[Opt. Express 32, 38793-38804 (2024), Commun. Phys. 8, 9 (2025)]。最近，该研究团队与中国人民大学尹华磊团队合作，提出了一种创新的星型拓

扑QDS网络架构，并发展了单诱骗态一次全域哈希QDS协议，提高系统性能的同时极大降低了系统硬件和数据后处理的复杂度。并基于硅基编码器和解码器芯片完成三节点量子数字签名网络示范。

图1为合作团队提出的芯片嵌入的星型QDS网络架构。将复杂且难以集成的测量设备集中部署在网络中心节点。而每个用户只需持有一个小型化和低成本的发射器芯片即可在不同用户间执行数字签名任务。此外，这种网络架构能够集成到现有的通信基础设施中，并且通过灵活配置集成测量单元（IMU），使其能够适用测量设备无关类协议，从而提升网络性能。

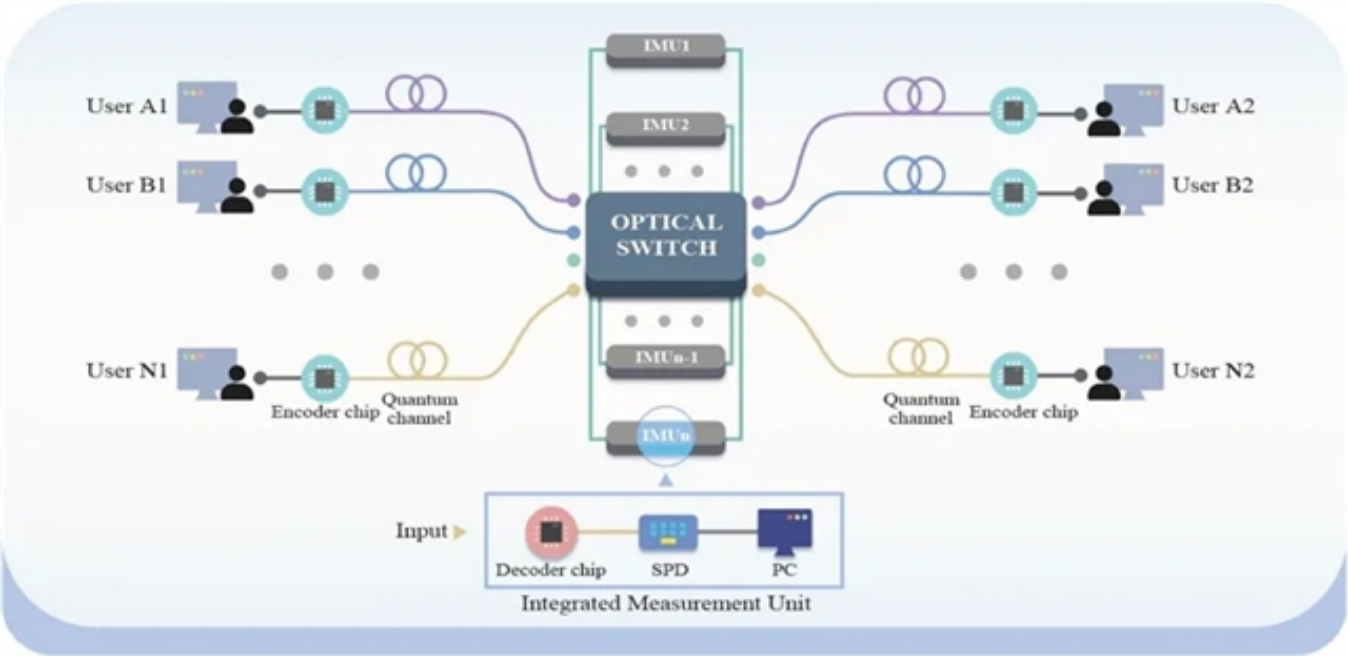

图1. 星型拓扑结构的芯片QDS网络示意图。

为了提升上述集成QDS网络性能的同时增强其与硅基芯片的兼容性，研究团队还发展了单诱骗态一次全域哈希QDS协议（图2）。该协议的运行主要分为分发阶段和消息阶段，其优势在于：1、不需要制备真空态，从而降低硅基芯片上强度调制器消光比的要求，以此减小发射器芯片制造复杂度；2、在消息阶段可以直接利用未经隐私放大的非完美密钥，因此可以极大的减小数据后处理所需的计算资源，并减小系统延迟。

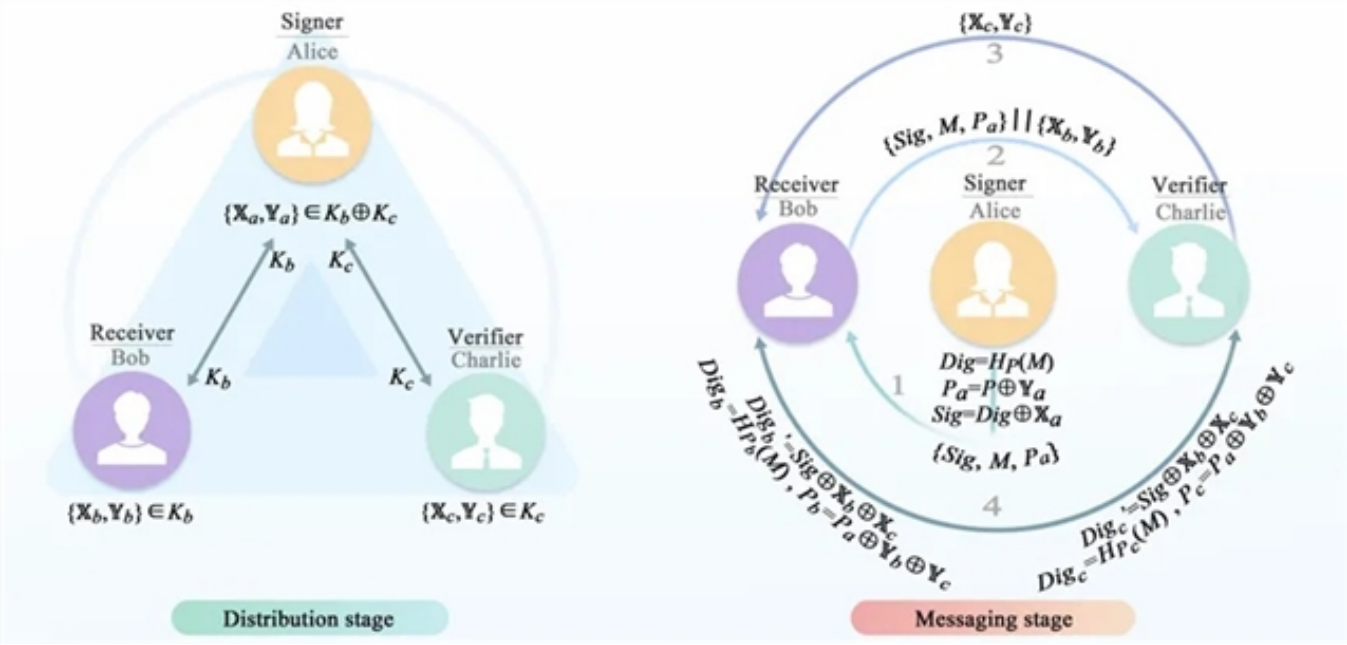

图2. 高效QDS协议运行示意图。

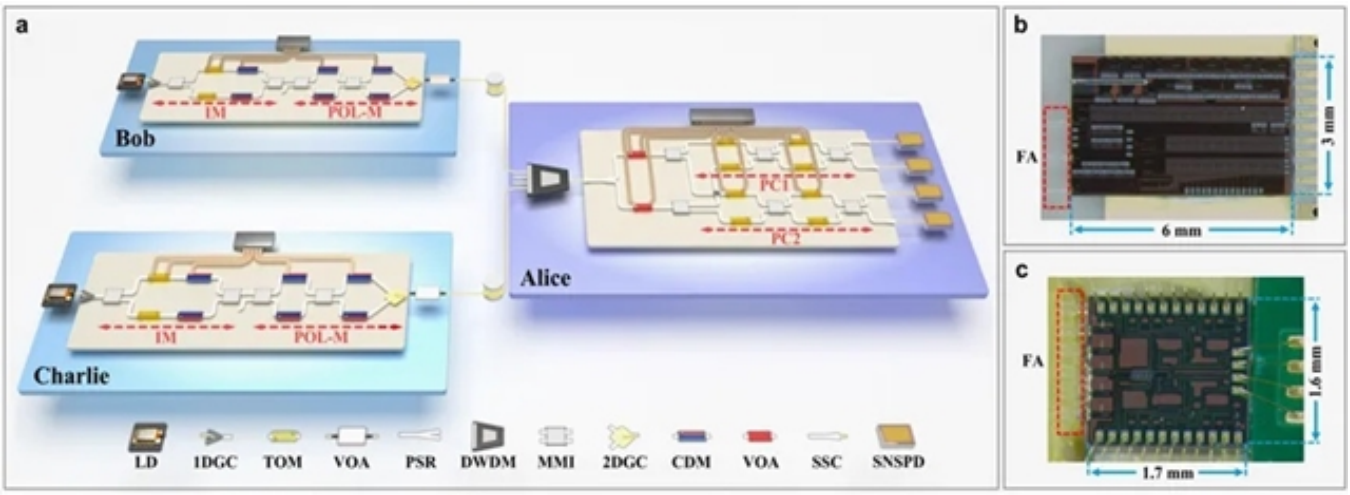

图3. 实验设置。(a) 基于芯片的三节点量子网络。(b) 硅基编码器芯片的显微图。(c) 硅基解码器芯片的显微图。

为了验证图1所示的芯片化QDS网络，研究团队构建了一个如图3所示的三节点芯片量子网络。这个网络包括一个中心节点，分配给签名者Alice，以及两个子节点，分配给接收者Bob和验证者Charlie。其中，Bob和Charlie各自持有一只硅基编码器芯片，Alice持有一只硅基解码器芯片。研究团队基于该网络配置，采用发展的新型QDS协议开展实验。为了展示该工作带来的突破，研究人员在图4中汇总了不同距离下开展QDS实验获得的结果。值得一提的是，所提的芯片化QDS方案在200 km的光纤距离下，签名1 Mbit文件实现了0.04次每秒的签名速率。

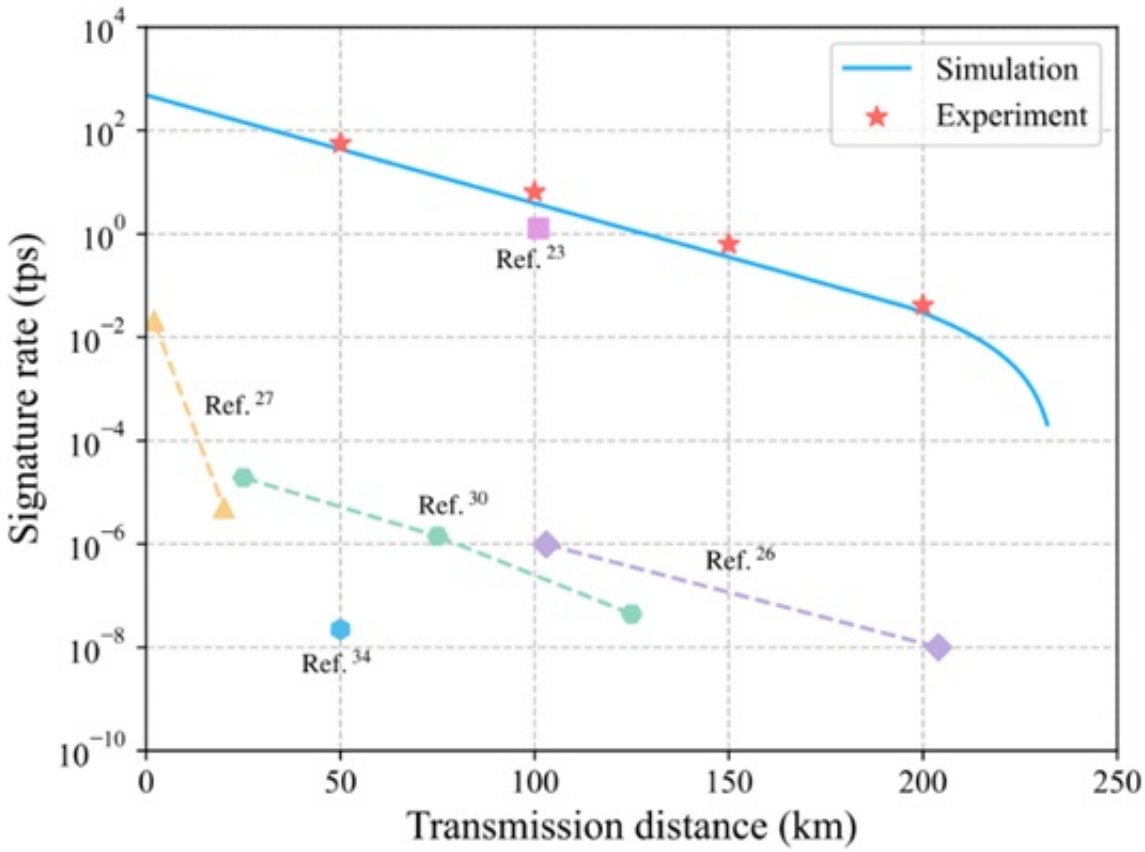

图4. 不同传输距离下的签名率。

总结与展望

在本研究中，研究团队提出了一种基于芯片的QDS网络，并通过发展单诱骗态一次全域哈希QDS协议，提高该网络性能的同时，降低了系统的复杂度。随后通过硅基编解码芯片构建了一个三节点QDS网络开展实验验证。实验结果表明在200 km的通信距离下，签名1 Mbit文件签名速率达到了0.04次每秒。研究团队表示，这一研究不仅推动了QDS技术的实用化进程，还在量子电子商务、量子区块链等其他量子通信领域具有广泛的应用价值。（来源：LightScienceApplications微信公众号）

相关论文信息：https://doi.org/10.1038/s41377-025-01775-4

作者：韦克金等 来源：《光：科学与应用》