

基于离散调制连续变量的量子密钥分发

作者：writer 来源：科学网

本文原地址：<https://www.iikx.com/news/progress/36369.html>

本文仅供学习交流之用，版权归原作者所有，请勿用于商业用途！

基于离散调制连续变量的量子密钥分发。 导读

量子密钥分发（QKD）作为量子物理赋能的加密技术，可为通信双方提供信息安全的密钥交换。特别是离散调制（DM）连续变量（CV）QKD协议，由于其简单性和与标准高速电信技术的兼容性，是大规模部署量子安全通信的合适候选。其理论安全性已趋成熟，却始终缺乏可组合安全性的实验验证——即生成的密钥可直接用于更复杂的密码任务且安全可量化。

近日，来自丹麦技术大学、奥地利理工学院等的科研人员首次实验演示了一种四态离散调制连续变量量子密钥分发（DM CVQKD）系统，可防止20公里光纤通道上的集体攻击。使用 2.3×10^9 个相干量子态实现了 11.04×10^{-3} 比特/符号（bits/symbol）的正可组合密钥率，最终获得25.94 Mbit可组合安全密钥。为使用标准电信组件大规模部署量子密钥分发网络奠定了坚实基础。该研究工作以Experimental composable key distribution using discrete-modulated continuous variable quantum cryptography为题发表在国际顶尖光学期刊《Light: Science Applications》。

什么是"可组合安全性"？

可组合安全性是密码学的黄金标准，要求协议输出的密钥在任意后续密码任务中均保持安全。其核心在于安全参数的量化——表示攻击者区分真实密钥与理想密钥的最大优势。例如本工作设定 $\epsilon=10^{-10}$ ，即攻击者成功概率不足百亿分之一。传统QKD实验多在渐近假设下验证，而可组合安全性需严格处理有限样本效应与设备缺陷，是实用化部署的核心门槛。

研究亮点

1.协议设计：四态调制与双层检测保障安全性

研究团队采用图1所示QPSK调制协议，其核心创新在于严格的可组合安全框架：

- 量子态制备：Alice随机发送四种相干态（ $|\alpha|e^{i\pi/4}$, $|\alpha|e^{3i\pi/4}$, $|\alpha|e^{5i\pi/4}$, $|\alpha|e^{7i\pi/4}$ ）
- 双层检测机制：Bob随机抽查kT个符号，验证光子数截断假设（截断数 $n_c=20$ ）进行能量检测，以及通过统计估计器确认量子态位于预设接受任一检测失败则协议终止，从源头排除安全风险。

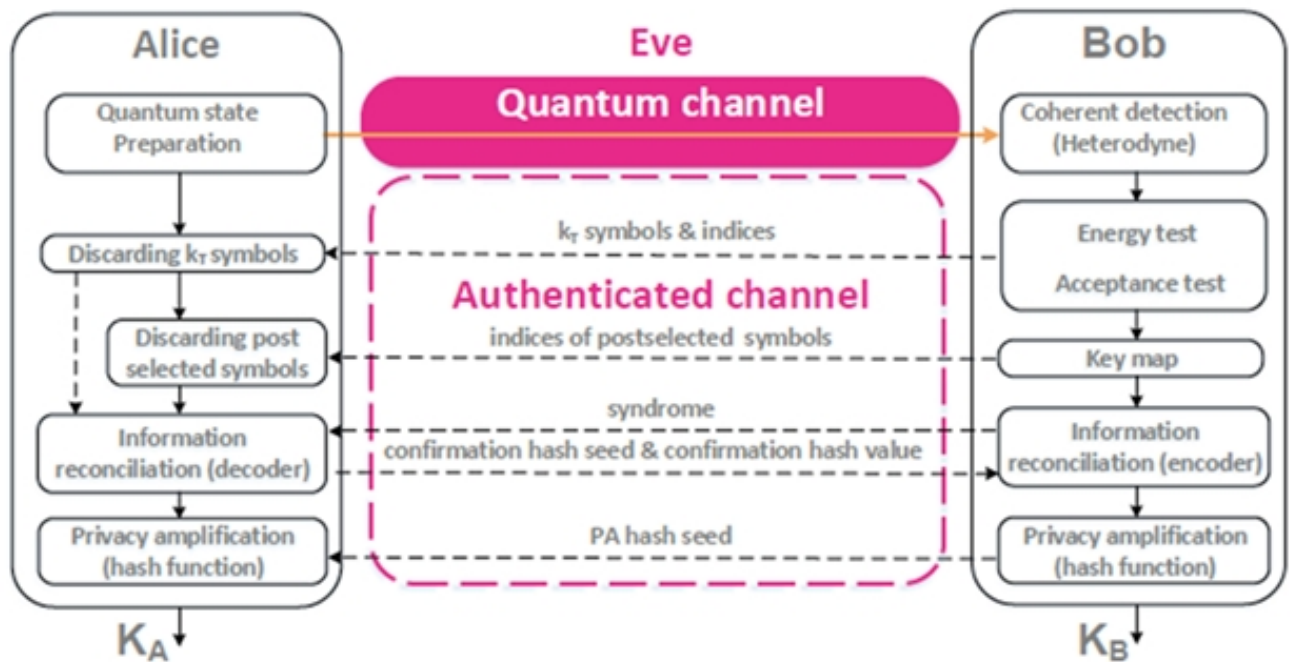


图1：DM CVQKD协议流程图。

2.系统实现：高速稳定收发与精准校准

实验系统深度融合高速电信技术，发送端使用1550nm激光器 + IQ调制器，以125 MBaud速率生成QPSK态，DAC采样率达1 GSample/s。在接收端利用外差检测+数字信号处理（DSP），通过非对称卡尔曼滤波实现载波相位恢复。最后基于可信接收机效率（68%）反向优化相干态振幅（ $|\alpha| = 0.71$ ）进行校准，突破传统信道建模依赖。

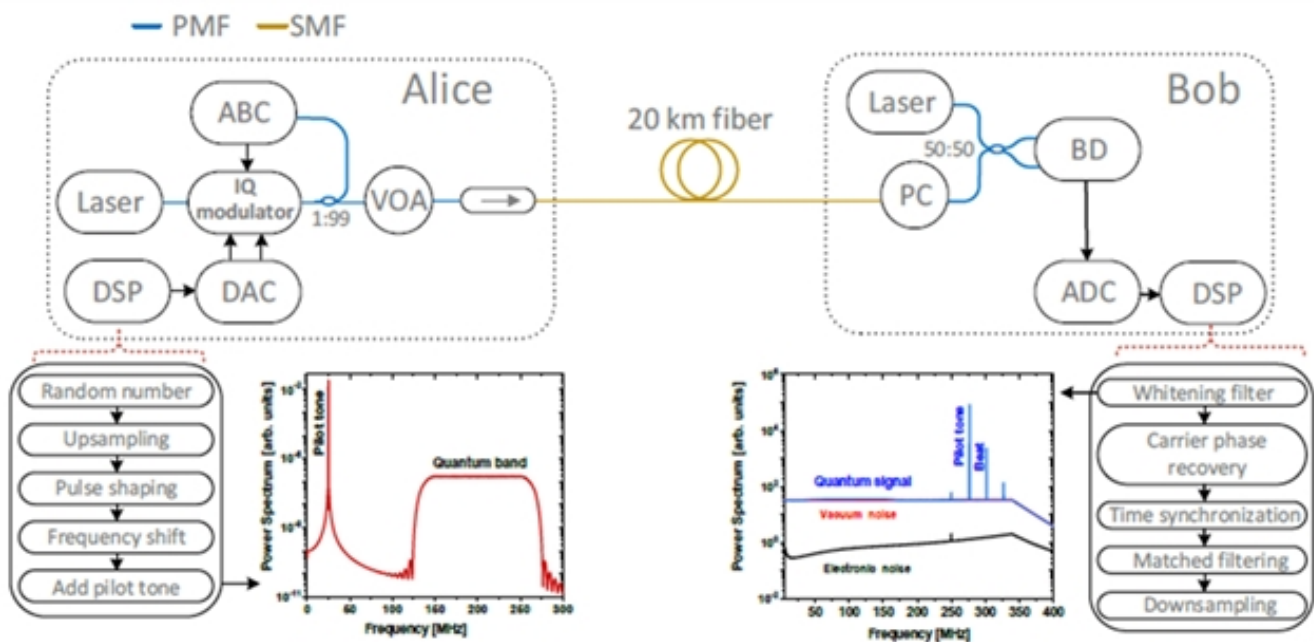


图2：DM CVQKD实验系统。

3.后处理优化与可组合安全证明

通过径向后选择（Radial Post-selection）平衡误码率与丢弃率，应用安全性证明框架，突破三大难点：通过能量检测将无限维希尔伯特空间映射至有限维通过能量检测将无限维希尔伯特空间映射至有限维（ $n_c=20$ ），并开发了密钥率公式，使用权重因子 $w \in [10^{-7}, 3 \times 10^{-7}]$ 平衡安全性与计算复杂度。

总结与展望

本研究工作首次实现了可组合安全性的DM CVQKD实验验证，但实用化仍需突破，例如利用高速有线组件提升符号率至千兆波特级。此外，可向64-QAM等高阶调制演进，逼近高斯调制性能极限。还可开发专用硬件加速LDPC解码（当前单核处理需1ms/迭代），结合CV多用户QKD理论，构建量子安全网络架构。正如作者所言：这项工作为使用标准电信组件构建实用、高性能、低成本、高安全的量子密钥分发网络迈出关键一步。（来源：LightScienceApplications微信公众号）

相关论文信息：<https://doi.org/10.1038/s41377-025-01924-9>

特别声明：本文转载仅仅是出于传播信息的需要，并不意味着代表本网站观点或证实其内容的真实性；如其他媒体、网站或个人从本网站转载使用，须保留本网站注明的“来源”，并自负版权等法律责任；作者如果不希望被转载或者联系转载稿费等事宜，请与我们联系。

作者：Tobias Gehring 来源：《光：科学与应用》

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

本文版权归原作者所有，请勿用于商业用途，[爱科学iikx.com](https://www.iikx.com)转发