专题: 量子信息处理

量子信息处理专题编者按

DOI: 10.7498/aps.74.210101 **CSTR**: 32037.14.aps.74.210101

2025 年诺贝尔物理学奖颁给了三位在量子领域做出突出贡献的物理学家. 量子信息是量子力学与信息技术相结合的新兴交叉学科, 涉及物理学、计算机科学与技术、电子信息科学与技术等领域. 量子信息包含量子计算、量子通信、量子精密测量三大研究方向. 量子计算聚焦量子计算机研发及适配算法设计, 旨在通过量子力学基本原理实现算力突破. 量子通信具有感知窃听的能力, 理论上具有无条件安全性, 可为通信提供高级别的安全性保护. 量子精密测量通过操控量子态可突破经典测量精度极限, 实现高精度测量. 量子科技是国际前沿, 世界各国高度重视量子科技的发展.

受《物理学报》编辑部委托, 我们邀请了国内若干活跃在该领域前沿的专家撰稿, 组织了以短篇综述为主的"量子信息处理"专题, 从不同视角为读者呈现量子信息科技领域的前沿进展, 旨在促进学术交流并激发新的研究思路. 本专题内容涵盖多个重要议题, 较为全面和深入地介绍了多种量子信息技术的最新进展及应用. 研究内容可分为两大类: 一是从理论和实验两方面介绍量子通信的最新研究进展, 包括光子集成的量子密钥分发和量子随机数生成器近期研究进展, 量子秘密共享现状与展望, 量子身份认证研究进展, 以及量子无噪声线性放大研究现状与展望; 二是对量子资源特性和量子态的高效制备进行综述报道, 包括三味中微子振荡的量子资源特性相关研究和量子多模下的非局域量子纠缠制备等.

本专题介绍了量子信息技术近年来在理论和实验方面的突破, 也突显了量子信息对未来科技、军事、经济等领域的深远影响, 可为相关领域的研究者提供有价值的参考, 也希望吸引更多的学者加入到量子信息的研究中来, 为我国在该领域的蓬勃发展注入新鲜活力.

(客座编辑: 龙桂鲁 清华大学; 盛宇波, 周澜 南京邮电大学)

SPECIAL TOPIC—Quantum information processing

Preface to the special topic: Quantum information processing

DOI: 10.7498/aps.74.210101 **CSTR**: 32037.14.aps.74.210101

专题: 量子信息处理

三味中微子振荡的量子资源特性研究*

王光杰 宋学科† 叶柳 王栋

(安徽大学物理与光电工程学院, 合肥 230601)

(2025 年 1 月 7 日收到; 2025 年 2 月 14 日收到修改稿)

中微子振荡是一个有趣的物理现象, 其量子性能够在宏观距离的振荡上得以保持并被检测到. 中微子振荡的量子资源特性是一个值得探索的主题, 这种在粒子物理学和量子信息学之间建立起的联系, 对于研究基本粒子的基本性质以及探索将中微子作为一种资源应用于量子信息处理的可能性而言, 都有着重要意义. 因此, 中微子物理学与量子信息理论的交叉研究受到了越来越多的关注. 这篇综述主要介绍利用量子资源理论来表征三味中微子振荡的量子资源特性, 包括量子纠缠、量子相干、量子非局域性和熵不确定度等. 除此之外, 还介绍了三味中微子振荡中的量子资源理论的权衡关系, 主要基于单配性关系和完全互补性关系, 这些权衡关系可以帮助我们有效理解量子资源如何在中微子振荡中转化和分配. 中微子振荡的量子信息理论研究仍处于不断发展中, 期望本综述能为该领域的发展带来启示.

关键词: 中微子振荡, 量子关联, 量子资源, 权衡关系

PACS: 03.65.–w, 03.67.–a, 03.67.Hk **DOI**: 10.7498/aps.74.20250029

CSTR: 32037.14.aps.74.20250029

1 引 言

在标准物理模型中, 中微子是一种质量极小的费米子, 与其他物质粒子之间的相互作用只有弱亚原子力和引力, 这种弱相互作用的特性也导致它们能够穿过大量普通物质. 中微子振荡的现象早在半个多世纪前就被提出[1,2]. 迄今为止, 一些实验利用太阳中微子[3,4]、大气中微子[5]、反应堆中微子[6,7]以及加速器产生的中微子[8,9], 已经获取了关于不同中微子味之间相互转变的确凿实验证据. 中微子和反中微子同时产生, 并能以三种不同的味态被探测到, 即电子 (e) 中微子、μ 子中微子和 τ 子中微子. 中微子味态是质量本征态的线性组合. 中微子振荡描述了中微子在传播过程中能够从一种给定的味态类型转换成另一种味态类型, 即三种味态在传播过程中可以相互转化. 中微子振荡也意味着中微子具有确定的质量. 近年来, 关于中微子振荡的参数准确测量与分析吸引了大量理论和实验方面的研究[10–12]. 为了验证中微子振荡的量子性, 研究者们考虑了 Leggett-Garg 不等式[13,14], 该不等式被称为 Bell 不等式的“时间模拟”, 能够测试在不同时间测量的单个系统的关联函数. 研究表明, 实验观察到的中微子振荡的振荡概率可以违反 Leggett-Garg 不等式施加的经典极限. 由于中微子的弱相互作用, 在中微子振荡过程中产生的退相干效应相较于其他在量子信息处理过程中被广泛应用的粒子系统中的退相干效应要更弱一些. 在量子信息科学与粒子物理学深度融合的前沿研究领域, 探寻中微子于未来量子信息处理进程中所具备的潜在应用价值, 一个关键的部分就是利用量子资源理论对中微子振荡的量子特性进行量化分析.

* 国家自然科学基金 (批准号: 62471001, 12475009, 12075001, 12175001, 12004006)、安徽省自然科学基金 (批准号: 2022b13020004, 2008085QA43) 和安徽省高校科研计划 (批准号: 2024AH050068, 2024AH040008) 资助的课题.

† 通信作者. E-mail: songxk@ahu.edu.cn

量子资源理论为研究量子物理学中的不同现象提供了一个通用性极强且功能强大的框架[15]. 一个统一且定义严谨的量子资源理论框架能够助力我们研究诸多相关量子问题, 例如在施加约束条件下量子态的表征量化以及操控[16,17], 还有不同量子关联度量之间的权衡关系[18–21]. 量子纠缠、量子相干和量子非局域性等是量子资源理论中最基本的概念, 可以用量子资源理论的工具进行严格的度量和表征[22–25]. 它们在量子信息处理中有许多潜在的应用, 包括量子隐形传态[26,27]、量子密码学[28,29]、量子计算[30,31]、量子密钥分发[32,33]等. 此外, 量子资源理论中的权衡关系对于多粒子系统中量子关联的量化和分类具有重要意义. 量子信息理论中常见的权衡关系有量子关联的单配性关系[34,35]和完全互补性关系[36,37]. 单配性关系主要是基于各种量子关联度量, 探究它们在多体系统中的分配和信息转移关系. 完全互补关系可以将量子系统中的各种量子关联联系起来, 为研究量子关联之间的相互作用 (如纠缠和量子相干) 提供有效途径. 熵不确定性关系对于探究量子系统的不确定度具有重要意义, 能展现中微子振荡在量子通信中的潜在应用价值. 这些量子关联度量和权衡关系对于探究中微子系统的量子资源特性具有重要的研究意义, 第 3 节和第 4 节会展示出它们在三味中微子系统中的具体研究.

量子信息理论在中微子振荡中的研究主要基于量子资源度量和资源分配特性, 例如纠缠和量子相干, 它们通常可以用味态跃迁概率来表示. 在关于中微子振荡的量子特性的诸多研究中, 众多对中微子振荡的量子性验证工作主要聚焦于 Leggett-Garg 不等式[14,38,39]. 然而, 用 Leggett-Garg 不等式检验中微子振荡的量子性存在一些局限性, 主要在于它只能作为判断量子相干性的定性准则. 因此, 违反 Leggett-Garg 不等式不是量化相干性度量的良好指标. 随后, Song 等[40]提出利用量子资源理论中的 l_1 范数相干度量对中微子传播中的量子相干性进行定量分析, 精准地量化了中微子振荡中的相干性. 此后, 利用 l_1 范数相干对中微子振荡的相干性研究吸引了众多研究者们的关注[41–45]. 纠缠作为一种最基本的量子资源, 存在多种量化方法. 近年来, 研究者们用各式各样的纠缠度量方式来量化中微子振荡中的量子性[46–52]. 其中, 对于三味中微子振荡的纠缠量化, Li 等[51]利用真正的多体纠缠度量, 包括广义的几何测量[53,54]、three-π 纠缠[55]、多体共生纠缠[56]、并发填充 (concurrence fill)[57]等, 通过对比分析, 得到了量化三味中微子振荡系统纠缠最优的度量方式. 此外, Blasone 等[58]通过单配性关系构建的剩余纠缠量化了三味中微子振荡的纠缠. 其他类型的量子关联对中微子振荡量子性的研究也受到了众多科研工作者的关注, 包括量子导引[59]、量子失谐[49,50]、Bell 非局域性[60,61]、量子相干的非局域性优势[62,63]、熵不确定性关系[64,65]等. 对中微子振荡的量子特性研究, 除了上述提到的量子资源, 利用量子资源理论的权衡关系对中微子振荡在量子信息理论中的研究也具有重要意义. Li 等[60]和 Wang 等[66]基于各种量子关联的单配性关系研究了三味中微子振荡中的量子资源分配和转化关系. Blasonet 等[58]和 Bittencourt 等[67]利用完全互补性关系研究了量子关联 (例如纠缠和相干) 在中微子振荡中的相互作用. 这些权衡关系在三味中微子振荡中的研究都会在第 4 节展示.

近年来, 对中微子振荡的量子特性研究除了以上提到的量子资源及其权衡关系, 还有其他方面的量子理论在该领域的贡献和探索. 限于篇幅, 本文仅概述三味中微子振荡中的量子资源特性研究, 主要基于常见的量子资源度量以及量子资源间的权衡关系和互补性关系.

2 三维中微子振荡模型

中微子振荡描述的是在中微子传播过程中, 三种不同的中微子味态之间的振荡概率相互转换的现象. 在这种情况下, 可以将中微子振荡的每一个味态作为一个量子比特系统来研究, 此时三味中微子振荡系统就可以看作是一个三量子比特的物理系统. 因此, 可以在量子资源理论框架下研究中微子振荡的多体量子资源特性. 对于中微子振荡的量子特性研究主要基于平面波近似和波包方法下的中微子振荡模型进行研究, 本节主要介绍平面波近似和波包方法下的三味中微子振荡模型.

2.1 平面波近似下的三味中微子振荡

在标准的三味中微子振荡模型中, 三种类型的中微子味态 $|\upsilon_{\mathrm{e}}\rangle$, $|\upsilon_{\mu}\rangle$, $|\upsilon_{\tau}\rangle$ 是其质量本征态 $|\nu_1\rangle$, $|\nu_2\rangle$, $|\nu_3\rangle$ 的线性叠加, 可以表示为[68,69]

$$|v_\alpha\rangle = \sum_k U^*_{\alpha k} |v_k\rangle , \tag{1}$$

式中 $k=1,2,3$, $\alpha = \mathrm{e},\mu,\tau$. $U^*_{\alpha k}$ 是轻子混合矩阵 $\boldsymbol{U}$ 中元素的复共轭形式, 该混合矩阵 $\boldsymbol{U}$ 被叫作 Pontecorvo-Maki-Nakagawa-Sakata 矩阵, 它可以用三个混合角和一个 CP 违反相位表示[70]:

$$\boldsymbol{U} = \begin{pmatrix} c_{12}c_{13} & s_{12}c_{13} & s_{13}\mathrm{e}^{-\mathrm{i}\delta_{cp}} \\ -s_{12}c_{23} - c_{12}s_{13}s_{23}\mathrm{e}^{-\mathrm{i}\delta_{cp}} & c_{12}c_{23} - s_{12}s_{13}s_{23}\mathrm{e}^{\mathrm{i}\delta_{cp}} & c_{13}s_{23} \\ s_{12}s_{23} - c_{12}s_{13}c_{23}\mathrm{e}^{\mathrm{i}\delta_{cp}} & -c_{12}c_{23} - s_{12}s_{13}s_{23}\mathrm{e}^{\mathrm{i}\delta_{cp}} & c_{13}c_{23} \end{pmatrix}, \tag{2}$$

式中 $c_{ij} \equiv \cos\theta_{ij}$, $s_{ij} \equiv \sin\theta_{ij}$. 中微子质量本征态 $|v_k\rangle$ 是能量为 E_k 的哈密顿量的本征态, 其随时间演化的质量本征态 $|v_k(t)\rangle$ 可以表示为

$$|v_k(t)\rangle = \mathrm{e}^{-\mathrm{i}E_k t/\hbar} |v_k(0)\rangle , \tag{3}$$

式中 $|v_k(0)\rangle$ 表示 $t=0$ 时刻的质量本征态. 该式呈现了中微子质量本征态随时间以平面波的形式演化. 利用混合矩阵 $\boldsymbol{U}$, 可以将中微子味本征态的时间演化与中微子质量本征态的时间演化联系起来, 表达式为

$$\begin{aligned} |v_\alpha(t)\rangle &= \sum_k U^*_{\alpha k} |v_k(t)\rangle \\ &= \sum_k U^*_{\alpha k} \mathrm{e}^{-\mathrm{i}E_k t/\hbar} |v_k\rangle, \end{aligned} \tag{4}$$

通过用味本征态来表示质量本征态, 即 $|v_k\rangle = \sum_\beta U_{\beta k} |v_\beta\rangle$, (4) 式可以表示成

$$\begin{aligned} |v_\alpha(t)\rangle &= \sum_\beta \sum_k U^*_{\alpha k} \mathrm{e}^{-\mathrm{i}E_k t} U_{\beta k} |v_\beta\rangle \\ &= \sum_\beta a_{\alpha\beta}(t) |v_\beta\rangle . \end{aligned} \tag{5}$$

在三味中微子振荡情形下, (5) 式可以展开成下列形式:

$$|v_\alpha(t)\rangle = a_{\alpha\mathrm{e}}(t) |v_\mathrm{e}\rangle + a_{\alpha\mu}(t) |v_\mu\rangle + a_{\alpha\tau}(t) |v_\tau\rangle , \tag{6}$$

式中 $a_{\alpha\beta}(t) = \sum_k U^*_{\alpha k} \mathrm{e}^{-\mathrm{i}E_k t/\hbar} U_{\beta k}$ 是味 α 到味 β 的转化振幅, 构成了所谓的味演化矩阵 $\boldsymbol{U}_\mathrm{f}(t)$ 的元素. 在矩阵运算中, $\boldsymbol{\nu}_\alpha(t) \equiv (\nu_\mathrm{e}(t)\nu_\mu(t)\nu_\tau(t))$ 由味演化矩阵 $\boldsymbol{U}_\mathrm{f}(t)$ 与 $t=0$ 时刻的味态联系起来, 即 $\boldsymbol{\nu}_\alpha(t) = \boldsymbol{U}_\mathrm{f}(t)\boldsymbol{\nu}_\alpha(0)$.

已知初始为 α 味中微子, 在振荡过程中探测到 β 味中微子的概率为

$$P_{\alpha\beta} = |a_{\alpha\beta}(t)|^2 = \left| \sum_k U_{\beta k} \mathrm{e}^{-\mathrm{i}E_k t/\hbar} U^*_{\alpha k} \right|^2 , \tag{7}$$

化简后可得到下列形式[71]:

$$\begin{aligned} P_{\alpha\beta} = \delta_{\alpha\beta} &- 4 \sum_{i>j} \mathrm{Re}\left(\hat{U}^*_{\alpha i} \hat{U}_{\beta i} \hat{U}_{\alpha j} \hat{U}^*_{\beta j} \right) \\ &\times \sin^2 \left(\Delta m^2_{ij} \frac{Lc^3}{4\hbar E} \right) \\ &+ 2 \sum_{i>j} \mathrm{Im}\left(\hat{U}^*_{\alpha i} \hat{U}_{\beta i} \hat{U}_{\alpha j} \hat{U}^*_{\beta j} \right) \\ &\times \sin \left(\Delta m^2_{ij} \frac{Lc^3}{2\hbar E} \right) , \end{aligned} \tag{8}$$

式中 $\Delta m^2_{kl} = m^2_k - m^2_l$, E 是中微子的能量, $L \approx ct$ (c 为自由空间中的光速) 为中微子源与探测器之间的距离. 值得注意的是生存概率 $P_{\alpha\beta} = |a_{\alpha\alpha}(t)|^2$ 和振荡概率 $P_{\alpha\beta} = |a_{\alpha\beta}(t)|^2$ 满足 $P_{\alpha\alpha} + P_{\alpha\beta} = 1$. 为了方便计算, (8) 式中的 $\sin^2 \left(\Delta m^2_{ij} \dfrac{Lc^3}{4\hbar E} \right)$ 可以写成

$$\begin{aligned} &\sin^2 \left(\Delta m^2_{ij} \frac{Lc^3}{4E\hbar} \right) \\ &= \sin^2 \left(1.27 \Delta m^2_{ij} \frac{L}{E} \right) . \end{aligned} \tag{9}$$

式中, Δm_{ij} 表示质量平方差, 单位为 eV; L 表示中微子传播距离, 单位为 km; E 表示中微子能量, 单位为 GeV. 这里中微子味态可以被映射为

$$|v_\mathrm{e}\rangle \equiv |1\rangle_\mathrm{e} \otimes |0\rangle_\mu \otimes |0\rangle_\tau \equiv |100\rangle, \tag{10}$$

$$|v_\mu\rangle \equiv |0\rangle_\mathrm{e} \otimes |1\rangle_\mu \otimes |0\rangle_\tau \equiv |010\rangle, \tag{11}$$

$$|v_\tau\rangle \equiv |0\rangle_\mathrm{e} \otimes |0\rangle_\mu \otimes |1\rangle_\tau \equiv |001\rangle. \tag{12}$$

因此中微子味态的跃迁概率变化可以视为三量子比特的状态随着时间发生演化, 即

$$|\psi_\alpha(t)\rangle = a_{\alpha\mathrm{e}}(t)|100\rangle + a_{\alpha\mu}(t)|010\rangle + a_{\alpha\tau}(t)|001\rangle. \tag{13}$$

2.2 波包近似下的三味中微子振荡

本节主要回顾波包方法[72,73]下的中微子振荡理论. 原则上, 中微子系统的状态是由纯态描述的, 例如 (4) 式中的状态. 通过使用波包方法, 描述中微子态 $\rho_\alpha(x,t)$ 演化的密度矩阵依赖于时间和位置,

这种矩阵通过对时间积分, 可以得到[52]

$$\boldsymbol{\rho}_\alpha(x)=\sum_{k,j}U_{\alpha k}U^*_{\alpha j}f_{jk}(x)\left|v_j\right\rangle\left\langle v_k\right|, \tag{14}$$

式中, $f_{jk}(x)=\exp\left[-\mathrm{i}\dfrac{\Delta m^2_{jk}x}{2E}-\left(\dfrac{\Delta m^2_{jk}x}{4\sqrt{2}E^2\sigma_x}\right)^2\right]$. 通过建立标识关系, 可以方便地用中微子振荡的味态特征态来表示 $\rho_\alpha(x)$, 即 $\left|v_\alpha\right\rangle=\left|\delta_{\alpha\mathrm{e}}\right\rangle_{\mathrm{e}}\left|\delta_{\alpha\mu}\right\rangle_{\mu}\left|\delta_{\alpha\tau}\right\rangle_{\tau}$. 结合 $\left|v_i\right\rangle=\sum_\alpha U_{\alpha i}\left|v_\alpha\right\rangle$, 可以得到

$$\boldsymbol{\rho}_\alpha(x)=\sum_{\beta_\gamma}F^\alpha_{\beta\gamma}(x)\left|\delta_{\beta\mathrm{e}}\delta_{\beta\mu}\delta_{\beta\tau}\right\rangle\left\langle\delta_{\gamma\mathrm{e}}\delta_{\gamma m}\delta_{\gamma\tau}\right|, \tag{15}$$

式中, $F^\alpha_{\beta\gamma}=\sum_{kj}U^*_{\alpha j}U_{\alpha k}f_{jk}(x)U_{\beta j}U^*_{\gamma k}$ ($k,j=1,2,3;\beta,\gamma=\mathrm{e},\mu,\tau$). 密度矩阵 (15) 式是一个混态, 可以写成:

$$\boldsymbol{\rho}^\alpha_{\mathrm{e}\mu\tau}(x)=\begin{pmatrix}0&0&0&0&0&0&0&0\\0&F^\alpha_{\tau\tau}(x)&F^\alpha_{\tau\mu}(x)&0&F^\alpha_{\tau\mathrm{e}}(x)&0&0&0\\0&F^\alpha_{\mu\tau}(x)&F^\alpha_{\mu\mu}(x)&0&F^\alpha_{\mu\mathrm{e}}(x)&0&0&0\\0&0&0&0&0&0&0&0\\0&F^\alpha_{\mathrm{e}\tau}(x)&F^\alpha_{\mathrm{e}\mu}(x)&0&F^\alpha_{\mathrm{ee}}(x)&0&0&0\\0&0&0&0&0&0&0&0\\0&0&0&0&0&0&0&0\\0&0&0&0&0&0&0&0\end{pmatrix}. \tag{16}$$

由 $\boldsymbol{\rho}_\alpha(x)$ 描述的中微子在位置 x 转变为 η 味中微子的概率为

$$P_{\alpha\eta}(x)=\left\langle v_\eta\right|\boldsymbol{\rho}_\alpha(x)\left|v_\eta\right\rangle=F^\alpha_{\eta\eta}(x). \tag{17}$$

3 三味中微子振荡中的量子资源

本节介绍量子信息理论在三味中微子振荡中的具体研究, 主要包括基本的量子资源度量, 例如纠缠、相干和非局域性等.

3.1 三味中微子振荡中的量子纠缠

量子纠缠作为最基本的量子资源, 对于量化中微子振荡的量子性具有重要意义. 对于三味中微子振荡, 现有一些研究利用不同的纠缠度量来量化中微子在振荡过程中的纠缠演化. Svetlichny[74] 利用几种真正的多体纠缠度量对三味中微子系统的纠缠进行了量化, 其中主要包括广义的几何测量 (GGM)[53,54]、three-π 纠缠 [55]、多体共生纠缠 (GMC)[56]、并发填充 (concurrence fill)[57] 等. 为了介绍这四种纠缠度量在中微子系统中的具体研究, 需要简述这些纠缠度量的数学表达式. 首先广义几何度量被定义为给定状态与不是真正多方纠缠的所有状态的集合的优化距离, 它可以度量任意粒子数的纯态的纠缠, 对任意一个 N 体纯态 $\left|\psi_N\right\rangle$, 其计算方法如下:

$$G\left(\left|\psi_N\right\rangle\right)=1-\max\left\{\lambda^2_{I:L}\mid I\cup L=\{A_1,\ldots,A_N\},\ I\cap L=\emptyset\right\}, \tag{18}$$

式中 $\lambda_{I:L}$ 是 $\left|\psi_N\right\rangle$ 两体划分 $I{:}L$ 中的最大施密特系数.

three-π 纠缠是基于负熵[75] 的单配性关系构建的剩余纠缠, 对于一个三体系统, 其数学表达式为

$$\pi_{ABC}=\frac{1}{3}\left(\pi_A+\pi_B+\pi_C\right), \tag{19}$$

其中 $\pi_A=N^2_{A(BC)}-N^2_{AB}-N^2_{AC}$, $\pi_B=N^2_{B(AC)}-N^2_{BA}-N^2_{BC}$, $\pi_C=N^2_{C(AB)}-N^2_{CA}-N^2_{CB}$ 是剩余纠缠, $N_{A(BC)}$ 是三体系统在两体划分 A 和 BC 下的负熵, N_{AB} 和 N_{AC} 分别表示子系统 AB 和子系统 AC 的负熵.

真正的多体共生纠缠是一种基于众所周知的并发纠缠的量化多体纠缠的计算方法. 对于三比特纯态 $\left|\psi\right\rangle_{ABC}$, 多体共生纠缠可以表示为[56]

$$C_{\mathrm{GMC}}\left(\left|\Psi_{ABC}\right\rangle\right)=\min\left\{2\left[1-\mathrm{Tr}\left(\boldsymbol{\rho}^2_A\right)\right],\ 2\left[1-\mathrm{Tr}\left(\boldsymbol{\rho}^2_B\right)\right],2[1-\mathrm{Tr}\left(\boldsymbol{\rho}^2_C\right)]\right\}. \tag{20}$$

2021 年, Xie 和 Eberly[57] 基于海伦公式, 引入了一种三粒子纠缠三角测度的 concurrence fill 方法. 与其他三体纠缠方法相比, concurrence fill 有两个优点: 1) 包含更多的信息; 2) 它总是平滑的. 而其他的纠缠度量包含一个取最小值的过程, 这将导致出现具有非解析特征的峰值. Xie 和 Eberly[57] 提出了一个 concurrence 三角形的概念, 其中三角形三条边的长度是这个量子系统的三个二部共生纠缠的平方. 然后将 concurrence fill 定义为并发三角形面积的平方根. 基于此, 给出了 concurrence fill 的表达式:

$$F_{ABC}\equiv\left[\frac{16}{3}Q\left(Q-C^2_{A(BC)}\right)\left(Q-C^2_{B(AC)}\right)\times\left(Q-C^2_{C(AB)}\right)\right]^{1/4}, \tag{21}$$

其中 $C^2_{A(BC)}$, $C^2_{B(AC)}$, $C^2_{C(AB)}$ 分别为 $2[1-\mathrm{Tr}(\boldsymbol{\rho}^2_A)]$, $2[1-\mathrm{Tr}(\boldsymbol{\rho}^2_B)]$, $2[1-\mathrm{Tr}(\boldsymbol{\rho}^2_C)]$. Q 是半周长, 系数 16/3 确保 $0\leqslant F_{ABC}\leqslant 1$.

接着就可以用 (21) 式, 分别求出它们在三味中微子振荡中的纠缠. 当考虑初始 $t=0$ 时刻为电子中微子时, 其三味中微子振荡演化状态为

$$|\psi_{\rm e}(t)\rangle = a_{\rm ee}(t)|100\rangle + a_{\rm e\mu}(t)|010\rangle + a_{\rm e\tau}(t)|001\rangle. \quad (22)$$

对于 $|\psi_{\rm e}(t)\rangle$, 广义的几何测量 (GGM)、three-π 纠缠、多体共生纠缠 (GMC)、concurrence fill 在三味中微子振荡中的纠缠表达式分别为

$$G\left(\rho^{\rm e}_{\rm e\mu\tau}\right) = 1 - \max\left\{\lambda^{\rm e}_{\rm e}, \lambda^{\rm e}_{\mu}, \lambda^{\rm e}_{\tau}\right\}, \quad (23)$$

其中,

$$\begin{aligned}\lambda^{\rm e}_{\rm e} &= \max\{P_{\rm e\tau} + P_{\rm e\mu}P_{\rm ee}\},\\ \lambda^{\rm e}_{\mu} &= \max\{P_{\rm ee} + P_{\rm e\tau}, P_{\rm e\mu}\},\\ \lambda^{\rm e}_{\tau} &= \max\{P_{\rm ee} + P_{\rm e\mu}, P_{\rm e\tau}\}, \end{aligned} \quad (24)$$

$$\begin{aligned}\pi_{\rm e\mu\tau}\left(\rho^{\rm e}\right) = \frac{4}{3}\Big[&- P^2_{\rm ee} - P^2_{\rm e\mu} - P^2_{\rm e\tau} + P_{\rm ee}\sqrt{P^2_{\rm ee} + 4P_{\rm e\mu}P_{\rm e\tau}}\\ &+ P_{\rm e\mu}\sqrt{P^2_{\rm e\mu} + 4P_{\rm ee}P_{\rm e\tau}}\\ &+ P_{\rm e\tau}\sqrt{P^2_{\rm e\tau} + 4P_{\rm ee}P_{\rm e\mu}}\Big], \end{aligned} \quad (25)$$

$$\begin{aligned}C_{\rm GMC}\left(\rho^{\rm e}_{\rm e\mu\tau}\right) = \min\Big\{&4P_{\rm ee}\left(P_{\rm e\mu} + P_{\rm e\tau}\right),\\ &4P_{\rm e\mu}\left(P_{\rm ee} + P_{\rm e\tau}\right), 4P_{\rm e\tau}\left(P_{\rm ee} + P_{\rm e\mu}\right)\Big\}, \end{aligned} \quad (26)$$

$$\begin{aligned}&F\left(\rho^{\rm e}_{\rm e\mu\tau}\right)\\ &= 8\left\{\frac{P^2_{\rm ee}P^2_{\rm e\mu}P^2_{\rm e\tau}\left[P_{\rm e\tau}P_{\rm e\mu} + P_{\rm ee}\left(P_{\rm e\mu} + P_{\rm e\tau}\right)\right]}{3}\right\}^{1/4}. \end{aligned} \quad (27)$$

同样也可以求出 μ 子中微子振荡中的纠缠表达式. 通过对比分析, 可以发现这几种纠缠度量方式在三味中微子振荡中的具体演化方式, 就可以得到量化三味中微子振荡中纠缠的最佳方法. 如图 1 所示, 四个纠缠度量演化趋势相同, 均为先升后降. 然而, 它们在中微子传播过程中所包含的信息量不同. 对于初始电子中微子振荡, concurrence fill 可达到最大值 0.89, 而 GGM, three-π 和 GMC 三种纠缠度量达到的纠缠最大值分别为 0.32, 0.55 和 0.88. 对于三味中微子振荡的纠缠度量, 与其他三种纠缠度量相比, concurrence fill 是一种更自然的度量方式, 原因有两个方面: 1) concurrence fill 随比率 L/E 的变化更平滑, 因为它考虑了所有的两部分纠缠. GGM 和 GMC 具有非解析尖端, 这是由于表达式中的非解析最小参数, 它缺少对整体的纠缠分布的考虑. 2) 在电子和 μ 子中微子传播过程中, concurrence fill 包含了更多的量子资源. concurrence fill 总是大于或等于其他三个纠缠度量方法. 所有这些特性都使 concurrence fill 在量子资源理论中, 对于三味中微子振荡中的纠缠量化, 是一种优秀的纠缠度量方式.

除了上述几种真正的多体纠缠度量方式, 还存在其他的纠缠度量可用于对三味中微子纠缠的量化. Li 等[65] 利用三体形成纠缠[76]、三体共生纠缠[77] 和三体并发负熵[76] 从理论和实验两个方面探究了三味中微子振荡中的纠缠特性, 揭示了它们在三味

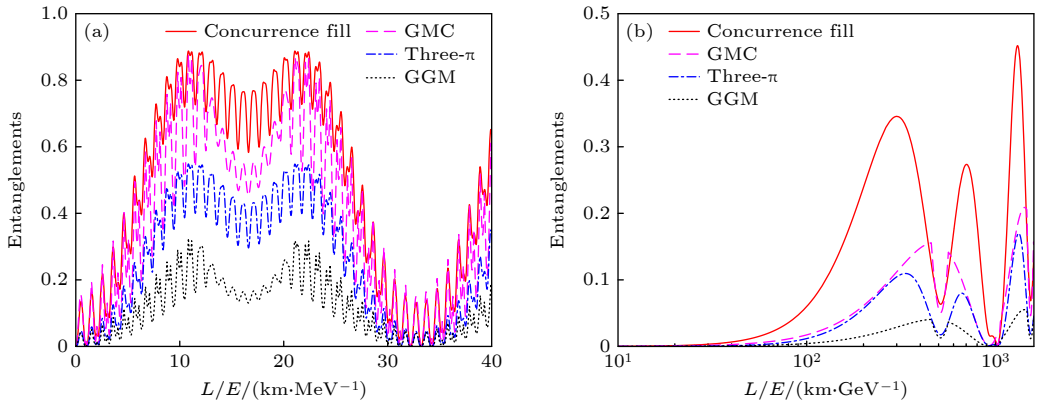


图 1 四种不同种类的纠缠度量, 包括广义的几何测量 (GGM)、three-π 纠缠、多体共生纠缠 (GMC)、concurrence fill, 在三味电子中微子振荡系统和三味 μ 子中微子振荡系统中的时间演化[51] (a) 三味电子中微子系统中不同多体纠缠测度的演化图像; (b) 三味 μ 子中微子系统中不同多体纠缠测度的演化图像

Fig. 1. Four kinds of multipartite entanglement measures, including generalized geometric measure (GGM), three-π, genuinely multipartite concurrence (GMC), and the concurrence fill for three flavors electron neutrino oscillation system and three flavors muon neutrino oscillations[51]: (a) Dynamic of different multipartite entanglement measures in three flavor electron neutrino system; (b) dynamic of different multipartite entanglement measures in three flavor muon neutrino system.

中微子振荡中的层级关系. 其中, 实验方面主要基于对大亚湾中微子和 MINOS 中微子合作组公布的中微子振荡实验数据进行分析. 研究结果表明, 对于电子中微子振荡, 三体共生纠缠是比三体形成纠缠和三体负熵更合适的纠缠度量, 它能捕获更多的量子资源, 而对于 μ 子中微子振荡, 三体共生纠缠和三体负熵都比三体形成纠缠更适合量化中微子振荡系统中的纠缠. 此外, Li 等[65] 基于冯·诺依曼熵的单配关系构建的剩余纠缠, 通过对其三个剩余纠缠求平均构建多体纠缠, 以确保所构建的纠缠度量在味排序改变下保持不变. 通过该方式构建的多体纠缠熵也可以量化三味中微子振荡的纠缠.

3.2 三味中微子振荡中的相干性

三味中微子振荡的相干性可以用定性和定量两种方法来研究. Leggett-Garg 不等式可以作为一种定性标准, l_1 范数可以作为定量度量. 本节从这两个方面来介绍三维中微子振荡中的量子相干性.

1985 年 Legget 与 Garg 提出了 Leggett-Garg 不等式, 该不等式主要有两个基本假设: 宏观实在性和非破坏性测量[72,73]. 第一个假设意味着在系统上执行测量只会显示已存在的值, 即系统总是处于宏观可区分状态中的一个; 第二个假设意味着可以在不改变系统状态及其后续演化的情况下对系统进行测量. 基于这两个假设, 得到的是一系列的不等式. Leggett-Garg 不等式的最简单形式由参数 K_3 构造, 其定义为

$$K_3 = C\left(t_1, t_2\right) + C\left(t_2, t_3\right) - C\left(t_1, t_3\right), \tag{28}$$

其中 $C\left(t_i, t_j\right) = \langle \hat{Q}\left(t_i\right) \hat{Q}\left(t_j\right) \rangle$, $\hat{Q}(t)$ 是一个二分可观测量, 它只能取两个离散值中的一个, 通常由+1 和–1 标记. 因此, 违反 Leggett-Garg 不等式可以证明量子相干性的存在.

Naikoo 等[78] 探究了介质、电荷共轭和宇称破坏效应同时存在的情况下, 三种味中微子振荡的 Leggett-Garg 不等式. 在该项研究中, 主要聚焦于 Leggett-Garg 不等式的 K_3 参数, 通过使用 T2K[79], NOvA[80] 和未来实验 DUNE[81] 中的参数数据来检验 Leggett-Garg 不等式的有效性. 当考虑初始中微子状态为 μ 子中微子, 并选择相等的时间间隔 $(t_0 = 0, t_1 = t, t_2 = 2t)$ 时, Leggett-Garg 不等式中的 K_3 项变为以下相关函数的和:

$$K_3 = C(0,t) + C(t,2t) - C(0,2t) \leqslant 1. \tag{29}$$

为了计算出时间关联函数 C, 选取的二分可观测量为 $\hat{Q} = 2\left|\nu_\alpha\right\rangle\left\langle\nu_\alpha\right| - 1$, 如果中微子状态仍处于初始状态 $\left|\nu_\mu\right\rangle$, 结果为+1, 反之则为–1. 最终可以直接计算出关联函数[78]

$$\begin{aligned} C(0,t) &= 4\delta_{\alpha\mu}\langle\nu_\mu(t)|\nu_\alpha\rangle\langle\nu_\alpha|\nu_\mu(t)\rangle \\ &\quad - 2\langle\nu_\mu(t)|\nu_\alpha\rangle\langle\nu_\alpha|\nu_\mu(t)\rangle - 2\delta_{\alpha\mu} + 1 \\ &= \begin{cases} 2\mathcal{P}_{\mu\to\mu}(t) - 1, & \alpha = \mu, \\ 1 - 2\mathcal{P}_{\mu\to\alpha}(t), & \alpha \neq \mu, \end{cases} \end{aligned} \tag{30}$$

$$\begin{aligned} C(t,2t) &= 1 - 2P_{\mu\to e}(t) - 2P_{\mu\to e}(2t) \\ &\quad + 4\alpha(t)P_{\mu\to e}(2t) + 4\beta(t), \end{aligned} \tag{31}$$

$$\alpha(t) = |U_{\rm f}^{11}(t)|^2, \tag{32}$$

$$\begin{aligned} \beta(t) &= {\rm Re}[U_{\rm f}^{11}(t)\bar{U}_{\rm f}^{21}(t)U_{\rm f}^{22}(2t)\bar{U}_{\rm f}^{12}(2t) \\ &\quad + U_{\rm f}^{11}(t)\bar{U}_{\rm f}^{31}(t)U_{\rm f}^{32}(2t)\bar{U}_{\rm f}^{12}(2t)], \end{aligned} \tag{33}$$

$U_{\rm f}^{ij}$ 是味演化矩阵 $\boldsymbol{U}_{\rm f}$ 中的元素, $\bar{U}_{\rm f}^{ij} = U_{\rm f}^{ij*}$ 是 $U_{\rm f}^{ij}$ 的复共轭. 结合 (13) 式和 (14) 式, 得到 K_3 项为

$$K_3 = 1 - 4P_{\mu\to e}(t) + 4\alpha(t)P_{\mu\to e}(2t) + 4\beta(t). \tag{34}$$

值得注意的是, 当 $\alpha = 0.5$, $\beta = 0$ 时, Leggett-Garg 不等式恢复到平稳极限. Formaggio 等[82] 和 Naikoo 等[83] 研究了在平稳条件下中微子振荡中的 Leggett-Garg 不等式. 图 2 展示了 K_3 对于三个不同实验设置的能量变化, 其中 δ 取值不同得到 K_3 的不同变化. 和反中微子振荡相比, 中微子振荡情况下的 K_3 在更多的能量区间总是大于 1, 即违反 Leggett-Garg 不等式的现象更加突出. 违反 Leggett-Garg 不等式可以解释为量子性的存在, 因为量子性是唯一与 Leggett-Garg 不等式原理相矛盾的理论. 如果进行测量的量子态是哈密顿量本征态的相干叠加, 则揭示了这种量子性. 反之则意味着这个量子态没有足够的相干性.

此外, Fu 和 Chen[39] 分析了基于大亚湾实验参数下的三味中微子振荡中的 Leggett-Garg 不等式. Gangopadhyay 和 Sinha[84] 分析了振荡参数对 Leggett-Garg 不等式违反的影响.

虽然违反 Leggett-Garg 不等式可以证明相干性的存在, 然而即使存在量子相干, 也有可能看不到任何参数空间的 Leggett-Garg 不等式违反. 相反, 如果有足够的相干性就能观察到 Leggett-Garg 不等式的违反. 所以 Leggett-Garg 不等式不是量化相干性的一个良好指标. Song 等[40] 于 2018 年

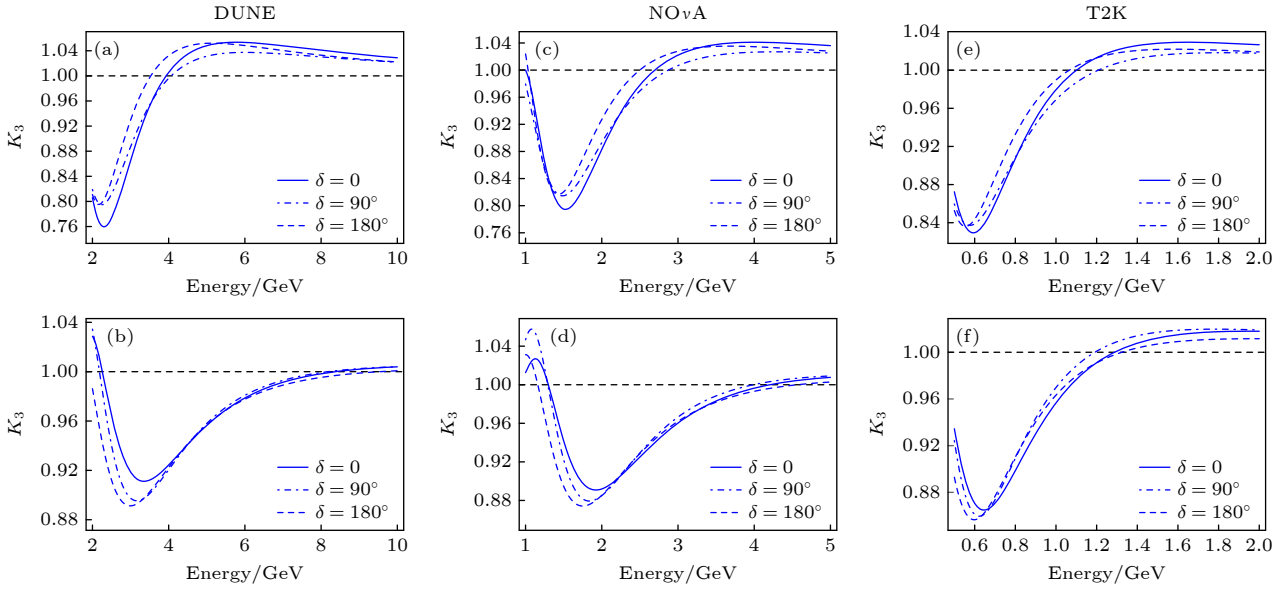


图 2 K_3 对于三个不同实验设置的能量变化[78] (a), (b) DUNE; (c), (d) NOvA; (e), (f) T2K. 其中 CP 破坏相位 δ 取不同的值, 时间可以用长度 (基线) 来确定, DUNE, NOvA 和 T2K 的长度分别为 1300, 810 和 295 km. (a), (c), (e) 对应于初始中微子态; (b), (d), (f) 对应于初始反中微子态

Fig. 2. The Variations in K_3 as a function of the energy for three experimental setups for different values of the CP-violating phase δ[78]: (a), (b) DUNE; (c), (d) NOvA; (e), (f) T2K. The time can be identified with the length (baseline) which is 1300, 810 and 295 km for DUNE, NOνA and T2K, respectively. The panels (a), (c), (e) correspond to the initial neutrino state, and panels (b), (d), (f) correspond to the initial antineutrino state.

提出了利用量子资源理论中的相干性度量的方法来量化三味中微子振荡中的相干性. 对于中微子振荡来说, l_1 范数相干是最容易计算的相干性度量, 它等于给定密度矩阵的所有非对角元素的总和, 即

$$\mathcal{C}(\rho) = \sum_{i \neq j} |\rho_{ij}| \geqslant 0. \tag{35}$$

C 的最大值由 $\mathcal{C}_{\max} = d - 1$ 限定, 其中 d 是密度矩阵 $\boldsymbol{\rho}$ 的维度. 在三味中微子振荡情形下, C 的最大值为 2. 对于三味电子和 μ 子中微子振荡, 其 l_1 范数相干可以由振荡概率表示:

$$\begin{aligned}\mathcal{C}_{\mathrm{e}} = 2 \Bigg[& \sqrt{P_{\mathrm{ee}}(t) P_{\mathrm{e\mu}}(t)} + \sqrt{P_{\mathrm{ee}}(t) P_{\mathrm{e\tau}}(t)} \\ & + \sqrt{P_{\mathrm{e\mu}}(t) P_{\mathrm{e\tau}}(t)} \Bigg],\end{aligned} \tag{36}$$

$$\begin{aligned}\mathcal{C}_{\mu} = 2 \Bigg[& \sqrt{P_{\mu\mathrm{e}}(t) P_{\mu\mu}(t)} + \sqrt{P_{\mu\mathrm{e}}(t) P_{\mu\tau}(t)} \\ & + \sqrt{P_{\mu\mu}(t) P_{\mu\tau}(t)} \Bigg].\end{aligned} \tag{37}$$

当两个振荡概率与生存概率均为 1/3 时, 三味中微子振荡相干性达到最大值为 2. 而当两个振荡概率与复活概率相比很小时, 相干性将接近于零. 此外, 如图 3(a) 中的插图所示, 相干关于复活概率偏导数表明 $P_{\mathrm{ee}}(t)$ 的微小变化将会导致相干的剧烈变化, 对应插图中复活生存概率小于 0.1 和大于 0.9 的相干变化. 为了量化所测量的相干性, 实验上复活概率可以由各个中微子实验合作组给定, 而 $\xi = P_{\mathrm{e\tau}}(t)/P_{\mathrm{e\mu}}(t)$ 是由理论预测确定的. 当 $\xi > 0.5$ 时, 相干随 ξ 的变化平缓; 当 $\xi < 0.5$ 时, 相干随 ξ 的变化较为剧烈. 对于大亚湾中微子振荡, 相干可达到约 0.8, 即使振荡概率小于 10%, 对于 KamLAND 下的三味中微子振荡, 其相干性普遍较高, 甚至最大值可以达到 2, 这意味着更多的量子资源可以用于 KamLAND 实验中的中微子振荡. 对于三味 μ 子中微子振荡, 如图 4 所示, 理论相干性表现出更复杂的行为, 其峰值出现在概率 $P_{\mu\mu}(t)$ 和 $P_{\mu\tau}(t)$ 相同的点上. MINOS 相干性的实验数据分布在理论预测线附近, 这与相干性的理论预测是一致的. 另一方面, T2K 相干性的实验数据也与理论符合得很好. 以上结果都表明 l_1 范数相干可以成为量化数千公里宏观距离上三味中微子振荡中相干性的可靠工具, 证明了中微子是一种除了光子以外可以适用于长距离量子通信的基本粒子.

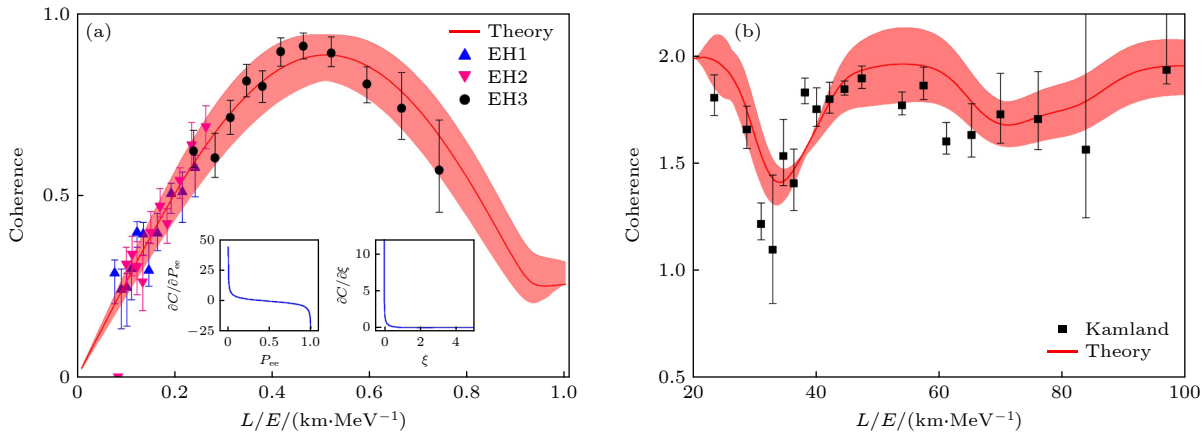


图 3 三味电子中微子振荡情况下理论与实验中的相干[40] (a) 来自于大亚湾三个地下实验所获取的实验数据下的相干, 分别由 EH1, EH2, EH3 对应的误差棒描述; (b) KamLAND 合作实验的中微子振荡相干. 图 (a) 插图分别展示了相干对于中微子生存概率以及比率 ξ 的导数. 图中红线是理论上的相干, 红色带状区域是理论拟合预测值周围的 3σ 置信区间的相干. 误差棒所展示的相干在短距离情况下与理论 3σ 范围内一致

Fig. 3. Coherence in theory and experiment for three-flavor electron neutrino oscillations[40]: (a) Coherence based on the experimental data obtained from the Daya Bay collaboration in three underground experimental halls, which is described by the error bars corresponding to EH1, EH2 and EH3 respectively; (b) coherence of neutrino oscillations under the T2K collaboration. The insets in panel (a) show the derivatives of coherence with respect to the neutrino survival probability and the ratio ξ. The red line in the picture shows the coherence in theory, and the red band indicates the coherence within the 3σ confidence interval around the theoretically fitted prediction. The coherence indicated by the error bars is consistent with the theoretical 3σ range in the short-distance case.

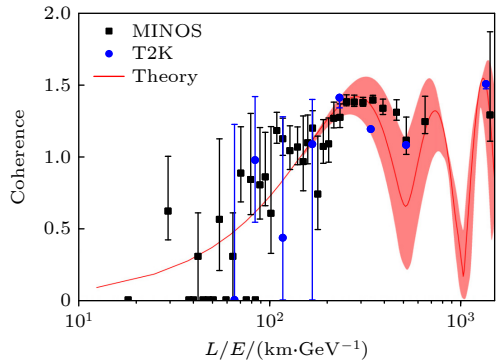


图 4 三味 μ 子中微子振荡情况下理论与实验中的相干[40]. 图中红线是理论上的相干, 红色带状区域是理论拟合预测值周围的 3σ 置信区间的相干, 黑色方块展示的 MINOS 合作实验的中微子振荡相干, 蓝色圆圈是 T2K 实验中微子振荡相干. 误差棒所展示的相干在短距离情况下与理论 3σ 范围内一致

Fig. 4. The coherence in theory and experiment for three-flavor μ neutrino oscillations[40]. The red line shows the coherence in theory, and the red band indicates the coherence within the 3σ confidence interval around the theoretically fitted prediction. The black squares show the coherence of neutrino oscillations in the MINOS collaboration, while the blue circles show the coherence of neutrino oscillations in the T2K collaboration. The coherence indicated by the error bars is consistent with the theoretical 3σ range in the short-distance case.

3.3 三味中微子振荡中的非局域性

三味中微子振荡过程中, 其贝尔非局域性, 即一种模态非局域性是否持久? 针对这个问题, Banerjee 等[50] 利用贝尔不等式的衍生形式 Mermin 不等式和 Svetlichny 不等式对其进行了研究. Mermin 不等式是 Bell 不等式的一种推广形式, 它的违反表明了多体系统中各方之间存在标准的非局域相关性[85]. 这意味着对于一个三体系统, 概率分布 P 不能写成局部形式:

$$P\left(a_1a_2a_3\right)=\int \mathrm{d}\lambda\rho(\lambda)P_1\left(a_1|\lambda\right)\times P_2\left(a_2|\lambda\right)P_3\left(a_3|\lambda\right), \tag{38}$$

这里 λ 是共享局部变量; a_1,a_2,a_3 是测量结果. 然而, 这并不能确保真正的多方非局域性. 如果任意两个子系统是非局部相关的, 但与第三个子系统不相关, 则仍然可以违反 Mermin 不等式. 为了探索真正的非局部相关性, 基于混合非局域-局域实在论[74] 的 Svetlichny 不等式是一个不错的选择, 如下所示:

$$P_B\left(a_1a_2a_3\right)=\sum_{k=1}^{3}P_k\int \mathrm{d}\lambda\rho_{ij}(\lambda)\times P_{ij}\left(a_ia_j|\lambda\right)P_k\left(a_k|\lambda\right), \tag{39}$$

其中 B 代表两体划分部分. 对于一个三比特量子系统, Mermin 不等式参数 M_3[86] 和 Svetlichny 不等式参数[87] 定义为

$$M_3 = ABC + AB'C + ABC' - AB'C', \quad (40)$$

$$S_3 = ABC + AB'C + ABC' - AB'C' + A'BC - A'B'C - A'BC' - A'B'C', \quad (41)$$

其中 X 和 $X'(X = A, B, C)$ 对应于每个量子位的两种不同的测量设置. 两种参数的经典界限分别为 $M_3 \leqslant 2$ 和 $S_3 \leqslant 4$. 值得注意的是, 对于 Mermin 不等式的违反, 至少有一个两体部分必须具有非局域相关性, 而 Svetlichny 不等式只有在所有各方都具有非局域相关性时才会被违反. 如图 5 和图 6 所示, 对于初始三种味 (即电子中微子、μ 子中微子、τ 子中微子) 的中微子振荡, M_3 的经典界限在各个情形中均被突破, 这意味着在系统中存在剩余非局域性. 而对于 S_3 的经典界限, 三种味的中微子振荡均存在未突破的参数区间. 也就是存在真正的多体非局域性缺失的情况. 有趣的是, 对于初始电子中微子振荡, 在其未检测到真正的多体非局域性的时间演化区间, 另外两种味的中微子, 可以观察到更强的振荡行为. 虽然真正的多体非局域关联在时间演化中主要存在 (反过来表明存在真正的三方纠缠), 但也存在其消失的特定演化区间.

本课题组研究了引力效应下三维中微子振荡中的非局域性, 通过改变引力效应的强度来得到不同引力效应下的 Svetlichny 不等式的违反程度, 结果表明在引力效应存在时, 三味中微子振荡过程中所呈现出的真正三方非局域特性将会发生显著变化, 具体表现为既可能出现增强的态势, 也可能出现被削弱的情况[61].

3.4 三味中微子振荡中的熵不确定性关系

不确定性原理被视为量子世界的一个重要特征, 它通常与经典世界中的对应情况有所不同. Renes 和 Boileau[88] 提出了基于熵的三体不确定性关系:

$$S(\hat{R} \mid B) + S(\hat{S} \mid C) \geqslant q_{MU}, \quad (42)$$

其中 $S(\hat{R} \mid B)$ 和 $S(\hat{S} \mid C)$ 是条件冯·诺依曼熵, $S(\hat{R} \mid B) = S(\rho_{\hat{R}B}) - S(\rho_B)$, $q_{\mathrm{MU}} = -\log_2 c(\hat{R}, \hat{S})$. $c = \max_{i,j}\{|\langle \Phi_i^{\hat{R}} \mid \psi_j^{\hat{S}} \rangle|^2\}$ 代表可观测量 $\hat{R}$ 和 $\hat{S}$ 对应本征态 $|\Phi_i^{\hat{R}}\rangle$ 和 $|\Phi_i^{\hat{S}}\rangle$ 的最大重叠.

Li 等[65] 利用熵不确定性关系进一步揭示了三味中微子振荡的量子特征. 为了更好地探索三味中

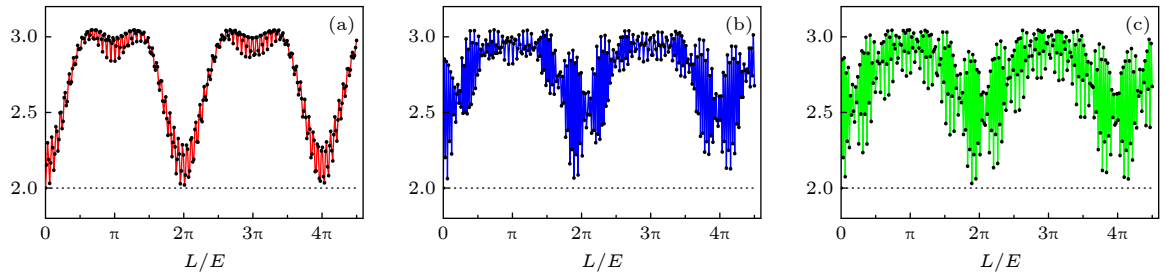


图 5 三味中微子振荡情况下参数 M_3 的变化[50] (a) 初始电子中微子; (b) 初始 μ 子中微子; (c) 初始 τ 子中微子. 黑色虚线对应于 M_3 的经典界限

Fig. 5. Variation of the parameter M_3 for three-flavor neutrino oscillations[50]: (a) Initial electron neutrino oscillation; (b) initial μ neutrino oscillation; (c) initial τ neutrino oscillation. The black dotted line corresponds to the classical bound of M_3.

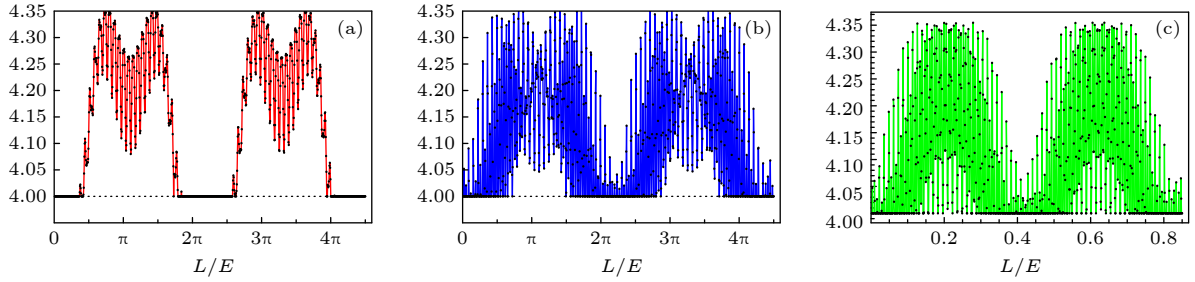


图 6 三味中微子振荡情况下参数 S_3 的变化[50] (a) 初始电子中微子; (b) 初始 μ 子中微子; (c) 初始 τ 子中微子. 黑色虚线对应于 S_3 的经典界限

Fig. 6. Variation of the parameter S_3 for three-flavor neutrino oscillations[50]: (a) Initial electron neutrino oscillation; (b) initial μ neutrino oscillation; (c) initial τ neutrino oscillation. The black dotted line corresponds to the classical bound of S_3.

微子振荡中的熵不确定性关系, Li 等[65] 基于下列不等式:

$$\begin{aligned} S(\mathbb{X}\mid B)+S(\mathbb{Z}\mid C)\geqslant q_{\mathrm{MU}},\\ S(\mathbb{Y}\mid B)+S(\mathbb{X}\mid C)\geqslant q_{\mathrm{MU}},\\ S(\mathbb{Z}\mid B)+S(\mathbb{Y}\mid C)\geqslant q_{\mathrm{MU}}, \end{aligned} \tag{43}$$

其中 $\mathbb{X}$, $\mathbb{Y}$, $\mathbb{Z}$ 是三个非对易算符. 通过相加可以得到总的熵不确定性关系:

$$\begin{aligned} &S(\mathbb{X}|B)+S(\mathbb{Z}|C)+S(\mathbb{Y}|B)+S(\mathbb{X}|C)\\ &+S(\mathbb{Z}|B)+S(\mathbb{Y}|C)\geqslant 3q_{\mathrm{MU}}. \end{aligned} \tag{44}$$

在此, 不相容测量的总不确定度为 $\mathcal{U}=S(\mathbb{X}|B)+S(\mathbb{Y}|B)+S(\mathbb{Z}|B)+S(\mathbb{X}|C)+S(\mathbb{Y}|C)+S(\mathbb{Z}|C)$

在初始电子中微子振荡中, 总熵不确定度为[65]

$$\begin{aligned} \mathcal{U}=&4\left[H_{\mathrm{bin}}\left(\lambda_1\right)-1\right]+P_{\mathrm{e\mu}}\log_2 P_{\mathrm{e\mu}}+P_{\mathrm{e\tau}}\log_2 P_{\mathrm{e\tau}}\\ &-2P_{\mathrm{ee}}\log_2 P_{\mathrm{ee}}+3\left[\left(P_{\mathrm{ee}}+P_{\mathrm{e\mu}}\right)\log_2\left(P_{\mathrm{ee}}+P_{\mathrm{e\mu}}\right)\right.\\ &\left.+\left(P_{\mathrm{e\tau}}+P_{\mathrm{ee}}\right)\log_2\left(P_{\mathrm{e\tau}}+P_{\mathrm{ee}}\right)\right], \end{aligned} \tag{45}$$

其中 $H_{\mathrm{bin}}\left(\lambda_1\right)=-\lambda_1\log_2\lambda_1-\left(1-\lambda_1\right)\log_2\left(1-\lambda_1\right)$, $\lambda_1=\dfrac{1}{2}(1-\sqrt{(P_{\mathrm{ee}}+P_{\mathrm{e\mu}})^2+2(P_{\mathrm{ee}}-P_{\mathrm{e\mu}})P_{\mathrm{e\tau}}+P_{\mathrm{e\tau}}^2})$.

类似地, 可得到 μ 子中微子振荡中总的不确定度:

$$\begin{aligned} \mathcal{U}=&4\left[H_{\mathrm{bin}}\left(\lambda_2\right)-1\right]-2P_{\mathrm{\mu\mu}}\log_2 P_{\mathrm{\mu\mu}}+P_{\mathrm{\mu e}}\log_2 P_{\mathrm{\mu e}}\\ &+P_{\mathrm{\mu\tau}}\log_2 P_{\mathrm{\mu\tau}}+3[\left(P_{\mathrm{\mu e}}+P_{\mathrm{\mu\mu}}\right)\log_2(P_{\mathrm{\mu e}}+P_{\mathrm{\mu\mu}})\\ &+\left(P_{\mathrm{\mu\tau}}+P_{\mathrm{\mu\mu}}\right)\log_2\left(P_{\mathrm{\mu\tau}}+P_{\mathrm{\mu\mu}}\right)], \end{aligned} \tag{46}$$

其中,

$$\lambda_2=\frac{1}{2}\left[1-\sqrt{(P_{\mathrm{\mu e}}+P_{\mathrm{\mu\mu}})^2+2(P_{\mathrm{\mu\mu}}-P_{\mathrm{\mu e}})P_{\mathrm{\mu\tau}}+P_{\mathrm{\mu\tau}}^2}\right].$$

如图 7 所示, 从理论和实验两个方面分析了由 (46) 式所描述的总的熵不确定度 $\mathcal{U}$ 在三味中微子振荡中的变化. 熵不确定度在电子和 μ 子中微子振荡中呈现先减小后增大的趋势且均大于其最低边界, 这表明由 (44) 式描述的熵不确定性关系在三味中微子振荡中总是成立. 此外, Li 等[65] 还研究了三味中微子振荡中熵不确定度与纠缠的关系, 他们发现在中微子传播过程中熵不确定度和纠缠之间呈现出反关联的变化趋势, 当纠缠在振荡中达到最大值时, 熵不确定度达到最小值. 从理论上讲, 这是因为量子纠缠的本质是一种非经典关联, 原则上量子关联越强, 测量的不确定度越小, 即纠缠越大, 测量的不确定度越小, 反之亦然. Blasone 等[63] 和 Wang 等[64] 在两味中微子振荡中也证明了这一理论. 不确定性的降低以及纠缠的增加使得中微子系统能够提供更多的量子资源. 因此, 展现出较高的量子特性将有利于实现中微子中不相容测量的较小不确定度.

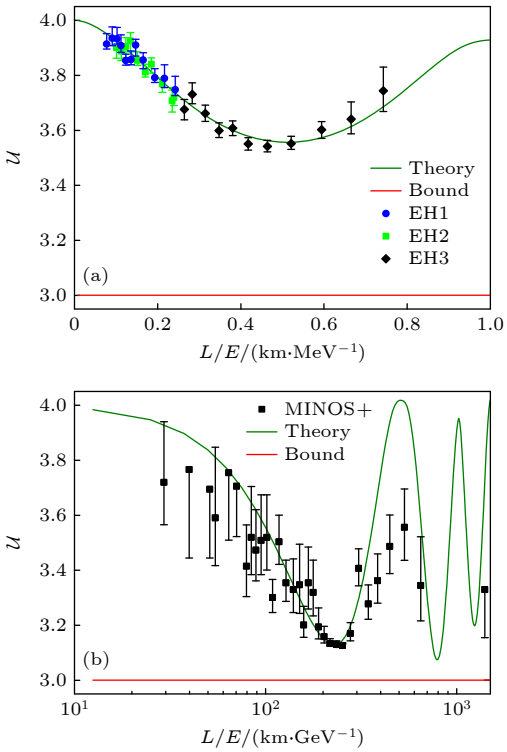


图 7 总的熵不确定度在三味电子和 μ 子中微子振荡中的演化[65] (a) 总的熵不确定度在电子中微子振荡中的演化, 其中 EH1, EH2 和 EH3 是大亚湾合作项目针对三个不同实验提供的数据; (b) 总的熵不确定度在电子中微子振荡中的演化. 橄榄线表示总的熵不确定度的理论值, 红线是 (62) 式中的右式, 对应于总的熵不确定关系的下届, 黑色方块代表 MINOS+合作项目的实验数据

Fig. 7. The evolution of the total entropic uncertainty in three flavor electron and μ neutrino oscillations[65]: (a) The evolution of the total entropic uncertainty in electron neutrino oscillation, where EH1, EH2 and EH3 are the data addressed from Daya Bay collaboration for three different experimental; (b) the evolution of the total entropic uncertainty in muon neutrino oscillation. The olive line represents the theoretical value of the total entropic uncertainty, and the red line corresponds to the lower bound of the total entropic uncertainty relation. The black squares stand for the experiment data from MINOS+ collaboration.

4 三味中微子振荡中的权衡关系

4.1 三味中微子振荡中的单配性关系

在研究多体系统量子相关的过程中, 最重要的性质之一是单配性, 它描述了多体系统中不同组成部分之间共享关联资源的约束条件[34]. 例如, 在三体系统中, A 和 B 双方之间的相关性越强, A 和

C 双方之间的相关性就越少, 它们表现出互补的行为. 单配性关系为研究多体系统的量子关联结构提供了有效途径. 我们团队[66]利用各种量子关联的单配性关系分析了三味中微子系统中的量子关联的分配和转化, 主要基于形成纠缠[89]、量子失谐[90]以及几何失谐[91]等量子关联.

对于任意两体纯态 $|\psi\rangle_{AB}$, 形成纠缠被定义为

$$E_{\mathrm{f}}\left(|\psi\rangle_{AB}\right)=S\left(\rho_A\right)=-\sum\mu_j\log_2\mu_j, \tag{47}$$

这里 $\rho_A=\mathrm{Tr}_B\left(|\psi\rangle_{AB}\langle\psi|\right)$, μ_j 是 ρ_A 的本征值. 对于两体混态 ρ_{AB}, 利用凸顶构造的方法, 可以得到两体混态的形成纠缠

$$E_{\mathrm{f}}\left(\rho_{AB}\right)=\min_{\left\{p_i,|\phi_i\rangle_{AB}\right\}}\sum_i p_iE_{\mathrm{f}}\left(|\phi_i\rangle_{AB}\right), \tag{48}$$

这里最大化是取遍所有的纯态分解 $\rho_{AB}=\sum_i p_i\left|\phi_i\right\rangle_{AB}\left\langle\phi_i\right|$, 其中 p_i 表示纯态分解的概率, 对于一个三量子比特系统, 基于形成纠缠平方的单配性关系由下列等式描述[92]:

$$E_{\mathrm{f}}^2\left(\rho_{A|BC}\right)\geqslant E_{\mathrm{f}}^2\left(\rho_{AB}\right)+E_{\mathrm{f}}^2\left(\rho_{AC}\right), \tag{49}$$

其中 $E_{\mathrm{f}}\left(\rho_{A|BC}\right)$ 量化的是 A 与 BC 之间的纠缠, $E_{\mathrm{f}}\left(\rho_{AB}\right)$ 和 $E_{\mathrm{f}}\left(\rho_{AC}\right)$ 是 A 与 $B(C)$ 之间的纠缠.

除了纠缠, 量子失谐也是一个主要的量子关联度量, 其被定义为

$$D\left(\rho_{AB}\right)=\widetilde{S}\left(\rho_A\mid\rho_B\right)-S\left(\rho_A\mid\rho_B\right), \tag{50}$$

这里 $\widetilde{S}\left(\rho_A\mid\rho_B\right)=\min_{\left\{M_j^B\right\}}\sum_j p_jS\left(\rho_{A|j}\right)$ 是测量诱导的量子条件熵. $\left\{M_j^B\right\}$ 是在子系统 B 上执行的投影测量. 基于失谐平方的单配性关系如下[19]:

$$D^2\left(\rho_{A|BC}\right)\geqslant D^2\left(\rho_{AB}\right)+D^2\left(\rho_{AC}\right). \tag{51}$$

另一方面, 量子失谐的几何测度被定义为两体系统 AB 的给定量子态与最近的经典态之间的最小平方希尔伯特-施密特距离[91]

$$D_{\mathrm{G}}\left(\rho_{AB}\right)=\min_{\sigma_{AB}\in\Omega}\left\|\rho_{AB}-\sigma_{AB}\right\|_2^2, \tag{52}$$

其中最小值是在经典态集合 Ω 上取得的, 这里的距离是 2-范数的平方, 也被称为希尔伯特-施密特范数. 对任意的三比特纯态, 几何失谐的单配性关系被描述为[93]

$$D_{\mathrm{G}}\left(\rho_{A|BC}\right)\geqslant D_{\mathrm{G}}\left(\rho_{AB}\right)+D_{\mathrm{G}}\left(\rho_{AC}\right). \tag{53}$$

为了更好地验证三味中微子振荡的单配性关系, 我们构建了剩余关联度量. 对于三味电子中微子振荡, 基于以形成纠缠和失谐单配性关系的剩余关联如下:

$$E_{\mathrm{R}}^2\left(\rho_{ABC}^{\mathrm{e}}\right)=E_{\mathrm{f}}^2(\rho_{A|BC}^{\mathrm{e}})-E_{\mathrm{f}}^2\left(\rho_{AB}^{\mathrm{e}}\right)-E_{\mathrm{f}}^2\left(\rho_{AC}^{\mathrm{e}}\right), \tag{54}$$

$$D_{\mathrm{R}}^2\left(\rho_{ABC}^{\mathrm{e}}\right)=D^2(\rho_{A|BC}^{\mathrm{e}})-D^2\left(\rho_{AB}^{\mathrm{e}}\right)-D^2\left(\rho_{AC}^{\mathrm{e}}\right). \tag{55}$$

对于几何失谐, 通过计算, 我们得到了 $D_{\mathrm{G}}(\rho_{A|BC}^{\mathrm{e}})=2P_{\mathrm{ee}}(P_{\mathrm{e\tau}}+P_{\mathrm{e\mu}})$, $D_{\mathrm{G}}(\rho_{AC}^{\mathrm{e}})=2P_{\mathrm{ee}}P_{\mathrm{e\tau}}$, $D_{\mathrm{G}}(\rho_{AB}^{\mathrm{e}})+D_{\mathrm{G}}(\rho_{AC}^{\mathrm{e}})=D_{\mathrm{G}}(\rho_{A|BC}^{\mathrm{e}})$. 所以几何失谐在三味中微子振荡中满足:

$$D_{\mathrm{G}}(\rho_{AB}^{\mathrm{e}})+D_{\mathrm{G}}(\rho_{AC}^{\mathrm{e}})=D_{\mathrm{G}}(\rho_{A|BC}^{\mathrm{e}}). \tag{56}$$

类似地可以得到 μ 子中微子振荡中的上述三种量子关联的单配性关系.

如图 8 和图 9 所示, 形成纠缠的平方、量子失谐的平方、几何量子失谐在三味中微子振荡中均呈现出单配性行为. 这些关系的成立会限制中微子振荡中的关联演化, 即在中微子传播过程中, 系统中 A 与 BC 之间的关联提供了一个严格的界限来限制子系统 AB 和 AC 之间的关联. 这种限制使得在中微子振荡中, 两个子系统之间的关联演化产生了互补行为. 在这些单配性关系中, 我们发现量子失谐的平方在中微子振荡中具有单配性, 而量子失谐本身在这种情况下不具有单配性, 这表明对中微子振荡中单配性性质的研究本质上依赖于对合适关联度量的选择. 对于几何量子失谐, 其单配性关系在三味中微子系统中是饱和的, 也就是说, 由几何量子失谐度量的单个子系统与三味中微子振荡系统其余子系统之间的关联包含了简化后的成对中微子子系统的关联. 研究结果还表明, 剩余关联是一种合理的度量方式, 它不仅能够清晰地刻画中微子振荡中量子关联的结构, 还能对中微子振荡中单配性关系所施加的约束进行量化. 这些单配性关系有助于更好地理解三味中微子系统中关联的分布情况, 并为研究量子通信中的信息交流及信息转换提供了一种有效的途径.

对于三味中微子振荡中的单配性研究, 除了上述量子关联的单配性关系, Li 等[60]基于量子相干和两体非局域性的单配性关系研究了相干和非局域性在中微子系统中的分配和转化. 此外, 近期我们基于量子纠缠研究了三味中微子振荡中的完全单配性关系[61], 该关系包含了三味中微子系统中整体以及所有两体子系统之间的纠缠, 在此

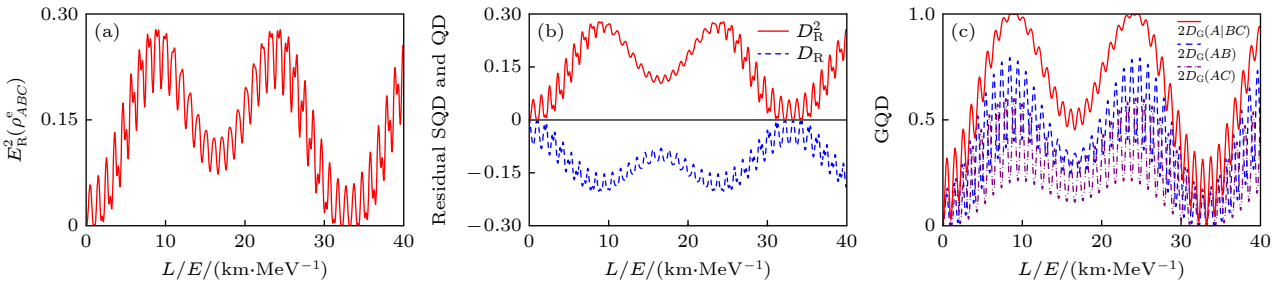


图 8 三味电子中微子振荡情况下的单配性关系验证[66] (a) 电子中微子振荡中的剩余形成纠缠的平方; (b) 剩余失谐的平方与剩余失谐的对比; (c) 电子中微子振荡中几何失谐的单配性验证, 可以观察到单配性关系 $D_{\rm G}(\rho^{\rm e}_{AB})+D_{\rm G}(\rho^{\rm e}_{AC})=D_{\rm G}(\rho^{\rm e}_{A|BC})$ 在电子中微子振荡中始终保持

Fig. 8. Tests of the monogamy relation for three-flavor electron neutrino oscillations[66]: (a) The residual squared entanglement of formation in the electron neutrino oscillations; (b) the residual squared of quantum discord in comparison to the residual quantum discord; (c) the monogamy of the geometric measure of quantum discord in electron neutrino oscillations. One can see that the monogamy relation $D_{\rm G}(\rho^{\rm e}_{AB})+D_{\rm G}(\rho^{\rm e}_{AC})=D_{\rm G}(\rho^{\rm e}_{A|BC})$ holds in electron tineutrino oscillations.

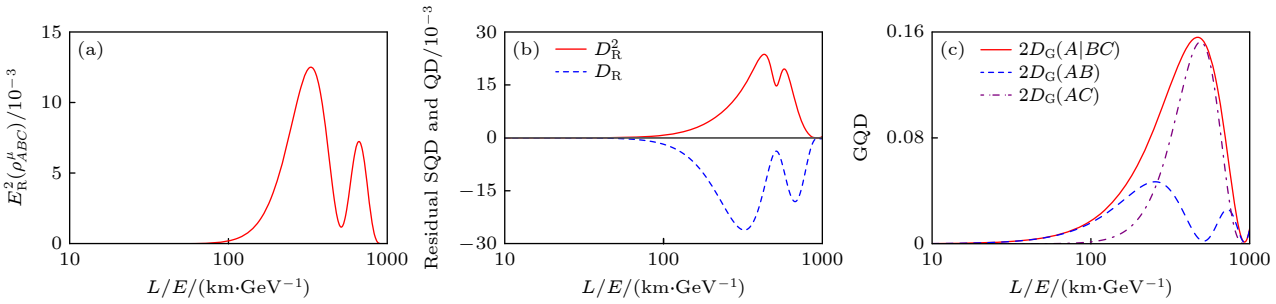


图 9 三味 μ 子中微子振荡情况下的单配性关系验证[66] (a) μ 子中微子振荡中的剩余形成纠缠的平方; (b) 剩余失谐的平方与剩余失谐的对比; (c) μ 子中微子振荡中几何失谐的单配性验证, 可以观察到单配性关系 $D_{\rm G}(\rho^{\rm e}_{AB})+D_{\rm G}(\rho^{\rm e}_{AC})=D_{\rm G}(\rho^{\rm e}_{A|BC})$ 在 μ 子中微子振荡中始终保持

Fig. 9. Tests of the monogamy relation for three-flavor muon neutrino oscillations[66]: (a) The residual squared entanglement of formation in the μ neutrino oscillations; (b) the residual squared of quantum discord in comparison to the residual quantum discord; (c) the monogamy of the geometric measure of quantum discord in μ neutrino oscillations. One can see that the monogamy relation $D_{\rm G}(\rho^{\rm e}_{AB})+D_{\rm G}(\rho^{\rm e}_{AC})=D_{\rm G}(\rho^{\rm e}_{A|BC})$ holds in muon tineutrino oscillations.

情形下, 不仅能够以一种有效的方式探究多体关联, 而且还可以更加详细地研究三味中微子振荡中量子关联的分布.

4.2 三味中微子振荡中的完全互补性关系

在多体量子系统中, 完全互补性关系[94]可以将不同的量子资源联系起来, 例如纠缠、相干、失谐. 完全互补性关系为理解量子系统局域和非局域方面的相互作用提供了一种有效途径. Blasone 等[58]从完全互补性关系的角度研究了中微子振荡中不同量子关联的演化. 为了更好地介绍三味中微子振荡中的完全互补性关系的应用, 接下来简单回顾下完全互补性关系.

给定一个两量子比特纯态, 对于子系统 k 的完全互补性关系如下:

$$\mathcal{P}_k^2+\mathcal{V}_k^2+\mathcal{C}^2=1,\ k=1,2, \tag{57}$$

其中 $\mathcal{P}_k$ 是系统的可预见性, 与系统的先验 (未经性测量) 的粒子性行为有关; $\mathcal{V}_k$ 是可见度, 与系统的相干有关; $\mathcal{C}$ 是共生纠缠, 用来量化子系统 k 与另一个子系统之间的纠缠. 对于三体纯态系统, 完全互补性关系由以下形式描述:

$$P_{\rm hs}\left(\rho_A\right)+C_{\rm hs}\left(\rho_A\right)+C_{\rm hs}^{nl}\left(\rho_{A|BC}\right)=\frac{d_A-1}{d_A}, \tag{58}$$

其中 $P_{\rm hs}\left(\rho_A\right)=\sum_{i=0}^{d_A-1}\left(\rho_{ii}^A\right)^2-\dfrac{1}{d_A}$ 是可预见性度量, $C_{\rm hs}\left(\rho_A\right)=\sum_{i\neq k}^{d_A-1}\left|\rho_{ik}^A\right|^2$ 是希尔伯特-施密特量子相干性 (一种可见性的测量方法), $C_{\rm hs}^{nl}\left(\rho_{A|BC}\right)$ 是 A 和 BC 的非局域相干.

如果将 (58) 式中的单个子系统转化成两体子系统 AB, 完全互补性关系描述为

$$C_{\rm re}\left(\rho_{AB}\right)+P_{\rm vn}\left(\rho_{AB}\right)+S_{\rm vn}\left(\rho_{AB}\right)=\log_2\left(d_Ad_B\right), \tag{59}$$

其中, $S_{\rm vn}$ 是冯·诺依曼熵, 代表子系统 AB 的纠缠; $C_{\rm re}$ 是相对熵相干; $P_{\rm vn}$ 是可预测性度量. 与单个子系统的局域相干相比, 两体子系统的局域相干不会消失. 后文也将探讨中微子系统的这种效应.

对于三体混态情形, 子系统 AB 的完全互补性关系形式如下:

$$\begin{aligned}&P_{\rm vn}\left(\rho_{AB}\right)+C_{\rm re}\left(\rho_{AB}\right)+S_{AB|C}\left(\rho_{ABC}\right)\\&+I_{AB:C}\left(\rho_{ABC}\right)=\log_2\left(d_Ad_B\right),\end{aligned} \tag{60}$$

其中, $I_{AB:C}\left(\rho_{ABC}\right)=S_{\rm vn}\left(\rho_{AB}\right)+S_{\rm vn}\left(\rho_C\right)-S_{\rm vn}\left(\rho_{ABC}\right)$, $S_{AB|C}\left(\rho_{ABC}\right)=S_{\rm vn}\left(\rho_{ABC}\right)-S_{\rm vn}\left(\rho_C\right)$.

在 (13) 式描述的三味中微子态中, $C_{\rm hs}^{nl}(\rho_{{\rm e}|\mu\tau}^{\alpha})=C_{\rm hs}\left(\rho_{{\rm e}\mu}^{\alpha}\right)+C_{\rm hs}\left(\rho_{{\rm e}\tau}^{\alpha}\right)$ 总是成立, 也就是说子系统 e 和 μτ 之间的非局域相干等于子系统 eμ 和 eτ 两体关联之和. 因此 (58) 式可以写成以下形式:

$$P_{\rm hs}\left(\rho_e^{\alpha}\right)+C_{\rm hs}\left(\rho_{{\rm e}\mu}^{\alpha}\right)+C_{\rm hs}\left(\rho_{{\rm e}\tau}^{\alpha}\right)=1/2, \tag{61}$$

其中, $C_{\rm hs}\left(\rho_{{\rm e}\mu}^{\alpha}\right)=\left[a_{\alpha{\rm e}}(t)a_{\alpha\mu}(t)^*\right]^2+\left[a_{\alpha\mu}(t)a_{\alpha{\rm e}}^*(t)\right]^2$, $C_{\rm hs}\left(\rho_{{\rm e}\tau}^{\alpha}\right)=\left[a_{\alpha{\rm e}}(t)a_{\alpha\tau}^*(t)\right]^2+\left[a_{\alpha\tau}(t)a_{\alpha{\rm e}}^*(t)\right]^2$. 由该等式描述的完全互补性关系如图 10 所示, e 和 μ 之间共享的两体关联大于 e 和 τ 之间的两体关联. 因此, 相干项 $C_{\rm hs}\left(\rho_{{\rm e}\mu}^{\rm e}\right)$ 相对于 $C_{\rm hs}\left(\rho_{{\rm e}\tau}^{e}\right)$ 在互补性关系中做出了更为突出的贡献. 而对于 μ 子中微子振荡的情况, 难以区别 $C_{\rm hs}\left(\rho_{{\rm e}\mu}^{\mu}\right)$ 和 $C_{\rm hs}\left(\rho_{{\rm e}\tau}^{\mu}\right)$ 之间的主导贡献, 两者之间呈现一种反关联关系.

针对子系统 eμ, 可以求出由 (59) 式描述的完全互补性关系的相关项:

$$\begin{aligned}S_{\rm vn}\left(\rho_{{\rm e}\mu}^{\alpha}\right)=&-\left(P_{\alpha{\rm e}}+P_{\alpha\mu}\right)\log_2\left(P_{\alpha{\rm e}}+P_{\alpha\mu}\right)\\&-P_{\alpha\tau}\log_2P_{\alpha\tau},\end{aligned} \tag{62}$$

$$\begin{aligned}P_{\rm vn}\left(\rho_{{\rm e}\mu}^{\alpha}\right)=&2+P_{\alpha{\rm e}}\log_2P_{\alpha{\rm e}}+P_{\alpha\mu}\log_2P_{\alpha\mu}\\&+P_{\alpha\tau}\log_2P_{\alpha\tau},\end{aligned} \tag{63}$$

$$\begin{aligned}C_{\rm re}\left(\rho_{{\rm e}\mu}^{\alpha}\right)=&-P_{\alpha{\rm e}}\log_2P_{\alpha{\rm e}}-P_{\alpha{\rm e}}\log_2P_{\alpha{\rm e}}\\&+\left(P_{\alpha{\rm e}}+P_{\alpha{\rm e}}\right)\log_2\left(P_{\alpha{\rm e}}+P_{\alpha{\rm e}}\right).\end{aligned} \tag{64}$$

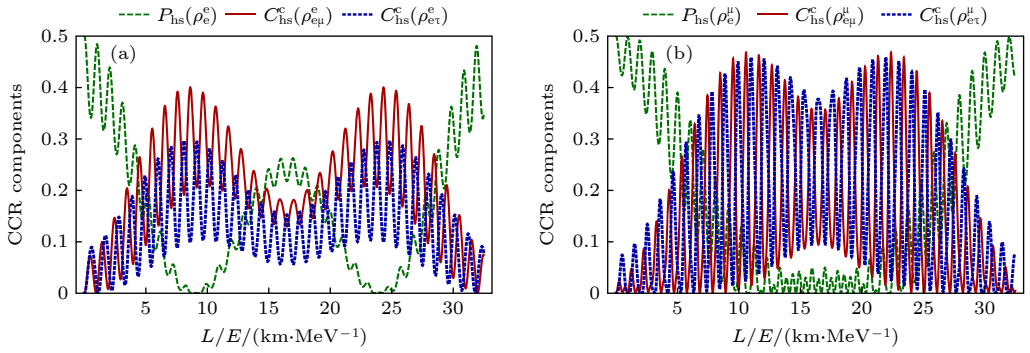


图 10 (55) 式描述的完全互补性关系中的关联度量在三味中微子振荡中的演化[58] (a) 电子中微子振荡中的完全互补性关系中的关联演化; (b) μ 子中微子振荡中的完全互补性关系中的关联演化

Fig. 10. Evolution of the correlation measures in the complete complementarity relations described by Eq. (55) in three-flavor neutrino oscillations[58]: (a) Evolution of the correlation measures in the complete complementarity relations for electron neutrino oscillations; (b) evolution of the correlation measures in the complete complementarity relations for μ neutrino oscillations.

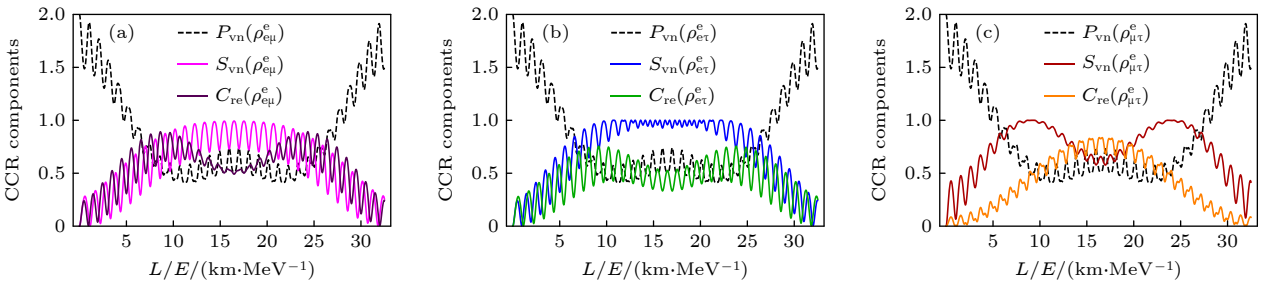


图 11 (53) 式描述的完全互补性关系中的相关项在三味电子中微子振荡中的演化[58] (a) 子系统 eμ 中的完全互补性关系; (b) 子系统 eτ 中的完全互补性关系; (c) 子系统 μτ 中的完全互补性关系

Fig. 11. The complete complementarity relation terms for three-flavor electron neutrino oscillations[58]: (a) The complete complementarity relation terms for eμ subsystem; (b) the complete complementarity relation terms for eτ subsystem; (c) the complete complementarity relation terms for μτ subsystem.

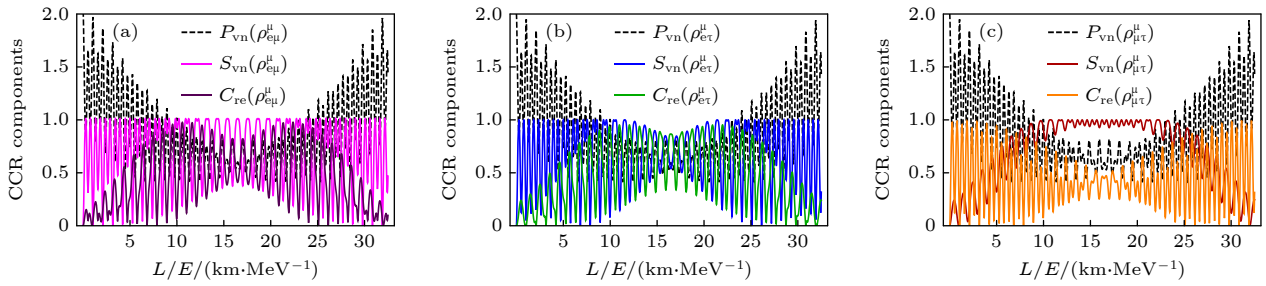


图 12 (53) 式描述的完全互补性关系中的相关项在三味 μ 子中微子振荡中的演化[58] (a) 子系统 eμ 中的完全互补性关系; (b) 子系统 eτ 中的完全互补性关系; (c) 子系统 μτ 中的完全互补性关系

Fig. 12. The complete complementarity relation terms for three-flavor muon neutrino oscillations[58]: (a) The complete complementarity relation terms for eμ subsystem; (b) the complete complementarity relation terms for eτ subsystem; (c) the complete complementarity relation terms for μτ subsystem.

图 11 和图 12 分别给出了由 (59) 式描述的完全互补性关系中的相关项在电子和 μ 子中微子振荡中的演化. 对于 eμ 和 eτ 子系统, 可预测性度量 P_{vn}、相对熵相干 C_{re}、纠缠熵 S_{vn} 三者均呈现出强烈的振荡行为, 而对于 eτ 子系统, 纠缠熵 S_{vn} 会达到一个稳定振荡, 即在最大值附近发生微小振荡变化, 这种行为在较长的时间演化区间内会持续存在. 这种稳定振荡行为可能对量子信息任务很有用.

5 结论与展望

本文主要回顾了三味中微子振荡中的一些量子性研究. 首先阐述了三味中微子常见的振荡模型, 主要基于平面波和波包方法下的中微子振荡. 之后着重介绍了三味中微子振荡中具体的量子性研究, 从量子信息理论中的资源理论中的关联度量和权衡关系两个方面进行介绍分析. 在中微子振荡量子资源特性的研究中, 回顾了纠缠、相干、非局域性和不确定度等常见的资源度量在中微子系统中的具体表现, 揭示了它们在三味中微子振荡中的演化特征. 在三味中微子振荡的纠缠研究中可以通过对比不同的纠缠度量在三味中微子振荡中的具体表现, 得到中微子振荡中最优的纠缠量化方式. 对于中微子振荡的相干性, 可以利用 Leggett-Garg 不等式和资源理论中的相干性度量分别进行定性和定量分析. Mermin 不等式和 Svetlichny 不等式呈现了三味中微子振荡中的模态非局域性的具体表现. 熵不确定性关系解释了中微子振荡中熵不确定度和量子关联之间的反关联关系. 最后简要介绍了单配性关系和完全互补性关系等权衡关系在三味中微子振荡中的具体应用, 单配性关系和完全互补性关系对于研究中微子系统中量子资源的分配和转移具有重要研究意义.

这些资源度量和权衡关系与许多量子信息处理任务直接相关, 不仅在揭示中微子振荡的内在量子特征方面具有不可或缺的作用, 而且对于挖掘中微子作为量子信息处理潜在资源的可能性具有关键的研究价值. 在中微子量子信息理论这一研究领域, 基本物理效应下的中微子振荡的量子性研究目前吸引了众多研究者的关注, 例如引力效应对中微子振荡相干性的影响[95] 和非标准相互作用对中微子振荡中量子关联的影响[96]. 在该研究背景下, 还可以研究基础物理效应存在时, 中微子振荡中量子资源间的分配关系及不确定关系的变化行为. 此外, 考虑 PMNS 矩阵中的 CP 违反相位对中微子振荡量子性的影响也是一个值得探讨的课题. 当引入中微子的自旋性质以及手性振荡时, 中微子可以看作一个超纠缠态[97], 其中自旋、手性以及味态可以看作中微子超纠缠态中不同的自由度, 那么利用量子资源理论可以研究中微子超纠缠态不同自由度之间的相互作用. 最后, 在量子场论的框架下, 研究中微子振荡的量子性也是一个具有重要意义的研究方向, Blasone 等[98] 探讨了中微子振荡中的 Leggett-Garg 不等式. 对中微子量子性的研究, 众多科研工作者正持续深入地进行探索与钻研, 不断推动着该领域边界的拓展与理论的深化. 虽然考虑到目前的技术, 中微子的操纵是一个巨大的挑战, 但对中微子振荡的量子特性研究是迈向中微子量子信息处理的重要一步.

参考文献

[1] Pontecorvo B 1958 *Sov. Phys. JETP* **7** **172** 1958
[2] Maki Z, Nakagawa M, Sakata S 1962 *Prog. Theor. Phys.* **28** 870

[3] Ahmad Q R (SNO Collaboration) 2002 *Phys. Rev. Lett.* **89** 011302
[4] Altmann M, Balata M, Belli P 2005 *Phys. Lett. B* **616** 174
[5] Fukuda S, Fukuda Y, Ishitsuka M 2002 *Phys. Lett. B* **539** 179
[6] Araki T, Eguchi K, Enomoto S 2005 *Phys. Rev. Lett.* **94** 081801
[7] An F P, Bai J Z, Balantekin A B 2012 *Phys. Rev. Lett.* **108** 171803
[8] Ahn M H, Aliu E, Andringa S 2006 *Phys. Rev. D* **74** 072003
[9] Adamson P 2008 *Phys. Rev. Lett.* **101** 131802
[10] An F P, Balantekin A B, Band H R 2015 *Phys. Rev. Lett.* **115** 111802
[11] Minakata H, Smirnov A Y 2012 *Phys. Rev. D* **85** 113006
[12] Gando A, Gando Y, Hanakago H 2013 *Phys. Rev. D* **88** 033001
[13] Emary G, Lambert N, Nori F 2014 *Rep. Prog. Phys.* **77** 039501
[14] Gangopadhyay D, Home D, Roy A S 2013 *Phys. Rev. A* **88** 022115
[15] Chitambar E, Gour G 2019 *Rev. Mod. Phys.* **91** 025001
[16] Devetak I, Harrow A W, Winter A J 2008 *IEEE Trans. Inf. Theory* **54** 4587
[17] Horodecki M, Oppenheim J 2013 *Int. J. Mod. Phys. B* **27** 1345019
[18] Sudha, Usha Devi A R, Rajagopal A K 2012 *Phys. Rev. A* **85** 012103
[19] Bai Y K, Zhang N, Ye M Y, Wang Z D 2013 *Phys. Rev. A* **88** 012123
[20] Yao Y, Xiao X, Ge L, Sun C P 2015 *Phys. Rev. A* **92** 022112
[21] Susa Y, Tanaka S 2015 *Phys. Rev. A* **92** 012112
[22] Hu M L, Hu X, Wang J, Peng Y, Zhang Y R, Fan H 2018 *Phys. Rep.* **762** 1
[23] Vedral V, Plenio M B, Rippin M A, Knight P L 1997 *Phys. Rev. Lett.* **78** 2275
[24] Baumgratz T, Cramer M, Plenio M B 2014 *Phys. Rev. Lett.* **113** 140401
[25] Bancal J D, Branciard C, Gisin N, Pironio S 2009 *Phys. Rev. Lett.* **103** 090503
[26] Bennett C H, Brassard G, Crépeau C, Jozsa R, Peres A, Wootters W K 1993 *Phys. Rev. Lett.* **70** 1895
[27] He Q, Rosales-Zárate L, Adesso G, Reid M D 2015 *Phys. Rev. Lett.* **115** 180502
[28] Horodecki R, Horodecki P, Horodecki M 2009 *Rev. Mod. Phys.* **81** 865
[29] Ekert A K 1991 *Phys. Rev. Lett.* **67** 661
[30] Raussendorf R, Briegel J H 2001 *Phys. Rev. Lett.* **86** 5188
[31] Albash T, Lidar A D 2018 *Rev. Mod. Phys.* **90** 015002
[32] Beaudry J N, Lucamarini M, Mancini S, Renner R 2013 *Phys. Rev. A* **88** 062303
[33] Ma X F, Zeng P, Zhou H Y 2018 *Phys. Rev. X* **8** 031043
[34] Coffman V, Kundu J, Wootters W K 2000 *Phys. Rev. A* **61** 052306
[35] Kim J S, Das A, Sanders B C 2009 *Phys. Rev. A* **79** 012329
[36] Greenberger D M, Yasin A 1988 *Phys. Lett. A* **128** 391
[37] Jaeger G, Horne M A, Shimony A 1993 *Phys. Rev. A* **48** 1023
[38] Cerf N J, Bourennane M, Karlsson A, Gisin N 2002 *Phys. Rev. Lett.* **88** 127903
[39] Fu Q, Chen X 2017 *Eur. Phys. J. C* **77** 775
[40] Song X K, Huang Y Q, Ling J J, Yung M H 2018 *Phys. Rev. A* **98** 050302(R)
[41] Dixit K, Alok A K 2021 *Eur. Phys. J. Plus* **136** 334
[42] Askaripour Ravari Z A, Ettefaghi M M, Miraboutalebi S 2022 *Eur. Phys. J. Plus* **137** 488
[43] Ming F, Fang B L, Hu X Y, Yu Y 2024 *Eur. Phys. J. Plus* **139** 229
[44] Kurashvili P, Chotorlishvili L, Kouzakov K 2021 *Eur. Phys. J. C* **81** 323
[45] Ettefaghi M M, Askaripour Ravari Z 2023 *Eur. Phys. J. C* **83** 417
[46] Blasone M, Dell'Anno F, De Siena S, Illuminati F 2009 *Eur. Phys. Lett.* **85** 50002
[47] Blasone M, Dell'Anno F, Di Mauro M, De Siena S, Illuminati F 2008 *Phys. Rev. D* **77** 096002
[48] Bittencourt V A S V, Blasone M, Zanfardino G 2023 *J. Phys. Conf. Ser.* **2533** 012024
[49] Alok A K, Banarjee S, Sankar S U 2016 *J. Nucl. Phys. B* **909** 65
[50] Banarjee S, Alok A K, Srikanth R, Hiesmayr B C 2015 *Eur. Phys. J. C* **75** 487
[51] Li Y W, Li L J, Song X K, Wang D 2022 *Eur. Phys. J. C* **82** 799
[52] Blasone M, Dell'Anno F, De Siena S, Illuminati F 2015 *Eur. Phys. Lett.* **112** 20007
[53] Das T, Singha Roy S, Bagchi S 2016 *Phys. Rev. A* **94** 022336
[54] Sadhukhan D, Singha Roy S, Pal A K 2017 *Phys. Rev. A* **95** 022301
[55] Ou Y C, Fan H 2007 *Phys. Rev. A* **75** 062308
[56] Ma Z H, Chen Z H, Chen J L 2011 *Phys. Rev. A* **83** 062325
[57] Xie S B, Eberly J H 2021 *Phys. Rev. Lett.* **127** 040403
[58] Blasone M, Dell'Anno F, De Siena S, Matrella C 2024 *Eur. Phys. J. C* **84** 301
[59] Ming F, Song X K, Li L J, Wang D 2020 *Eur. Phys. J. C* **80** 275
[60] Li Y W, Li L J, Song X K, Wang D 2022 *Eur. Phys. J. Plus* **137** 1267
[61] Wang G J, Li L J, Wu T, Song X K, Ye L, Wang D 2024 *Eur. Phys. J. C* **84** 1127
[62] Blasone M, De Siena S, Matrella1 C 2021 *Eur. Phys. J. C* **81** 660
[63] Blasone M, De Siena S, Matrella1 C 2022 *Eur. Phys. J. Plus* **137** 1272
[64] Wang D, Ming F, Song X K, Ye L, Chen J L 2020 *Eur. Phys. J. C* **80** 800
[65] Li L J, Ming F, Song X K, Ye L, Wang D 2021 *Eur. Phys. J. C* **81** 728
[66] Wang G J, Li Y W, Li L J, Song X K, Wang D 2023 *Eur. Phys. J. C* **83** 801
[67] Bittencourt V A S V, Blasone M, DeSiena S, Matrella C 2022 *Eur. Phys. J. C* **82** 566
[68] Bilenky S M, Pontecorvo B 1978 *Phys. Rev.* **41** 225
[69] Giunti C 2007 *J. Phys. G: Nucl. Part. Phys.* **34** R93
[70] Chakraborty P, Dey M, Roy S 2024 *J. Phys. G: Nucl. Part. Phys.* **51** 015003
[71] Gonzalez-Garcia M C, Maltoni M, Schwetz T 2014 *J. High Energy Phys.* **11** 052
[72] Leggett A J, Garg A 1985 *Phys. Rev. Lett.* **54** 857
[73] Giunti C, Kim C W 1998 *Phys. Rev. D* **58** 017301
[74] Svetlichny G 1987 *Phys. Rev. D* **35** 3066
[75] Peres A 1996 *Phys. Rev. Lett.* **77** 1413
[76] Guo Y, Zhang L 2020 *Phys. Rev. A* **101** 032301
[77] Sabín C, García-Alcaine G 2008 *Eur. Phys. J. D* **48** 435
[78] Naikoo J, Kumar Alok A, Banerjee S, Uma Sankar S 2019 *Phys. Rev. D* **99** 095001
[79] Abe K, Abgrall N, Aihara H 2011 *Nucl. Instrum. Methods Phys. Res., Sect. A* **659** 106
[80] Patterson R B 2013 *Nucl. Phys. B, Proc. Suppl.* **235–236** 151

[81] Abi B, Acciarri R, Acero M A 2020 *Eur. Phys. J. C* **80** 978
[82] Formaggio J A, Kaiser D I, Murskyj M M, Weiss T E 2016 *Phys. Rev. Lett.* **117** 050402
[83] Naikoo J, Kumar Alok A, Banerjee S, Uma Sankar S, Guarnieri G, Schultze C, Hiesmayr B C 2020 *Nucl. Phys. B* **951** 114872
[84] Gangopadhyaya D, Sinha Royb A 2017 *Eur. Phys. J. C* **77** 260
[85] Mermin N D 1990 *Phys. Rev. Lett.* **65** 1838
[86] Alsina D, Latorre J I 2016 *Phys. Rev. A* **94** 012314
[87] Bancal J D, Brunner N, Gisin N 2011 *Phys. Rev. Lett.* **106** 020405
[88] Renes J, Boileau J C 2009 *Phys. Rev. Lett.* **103** 020402
[89] Wootters W K 1998 *Phys. Rev. Lett.* **80** 2245
[90] Ollivier H, Zurek W H 2001 *Phys. Rev. Lett.* **88** 017901
[91] Dakic B, Vedral V, Brukner C 2010 *Phys. Rev. Lett.* **105** 190502
[92] Bai Y K, Xu Y F, Wang Z D 2014 *Phys. Rev. Lett.* **113** 100503
[93] Streltsov A, Adesso G, Piani M, Bruss D 2012 *Phys. Rev. Lett.* **109** 050503
[94] Jakob M, Bergou J A 2007 *Phys. Rev. A* **76** 052107
[95] Dixit K, Naikoo J, Mukhopadhyay B, Banerjee S 2019 *Phys. Rev. D* **100** 055021
[96] Yadav B, Sarkar T, Dixit K, Alok A K 2022 *Eur. Phys. J. C* **82** 446
[97] Bittencourt V A S V, Bernardini A E, Blasone M 2021 *Eur. Phys. J. C* **81** 411
[98] Blasone M, Illuminati F, Petruzziello L, Smaldone L 2023 *Phys. Rev. A* **108** 032210

SPECIAL TOPIC—Quantum information processing

Review of quantum resource characteristics in three-flavor neutrino oscillations*

WANG Guangjie SONG Xueke† YE Liu WANG Dong

(*School of Physics and Optoelectronics Engineering, Anhui University, Hefei* 230601, *China*)

(Received 7 January 2025; revised manuscript received 14 February 2025)

Abstract

Studying the quantum resources of neutrino oscillations is a topic worth exploring. This review mainly introduces the use of quantum resource theory to characterize the quantum resource characteristics of three-flavor neutrino oscillations, and the specific evolutionary patterns of different entanglement measures in three-flavor neutrino oscillations. In addition, by comparing the cases of different entanglement evolutions, the optimal method of quantifying entanglement in three-flavor neutrino oscillations can be obtained. Moreover, this review also focuses on the quantifying the quantumness of neutrino oscillation observed experimentally by using the l_1-norm of coherence. The maximal coherence is observed in the neutrino source from the KamLAND reactor. Furthermore, we examine the violation of the Mermin inequality and Svetlichny inequality to study the nonlocality in three-flavor neutrino oscillations. It is shown that even though the genuine tripartite nonlocal correlation is usually existent, it can disappear within specific time regions. In addition, this review also presents the trade-off relations in the quantum resource theory of three-flavor neutrino oscillations, mainly based on monogamy relations and complete complementarity relations. It is hoped that this review can bring inspiration to the development of this field.

Keywords: neutrino oscillations, quantum correlations, quantum resources, trade-off relations

PACS: 03.65.–w, 03.67.–a, 03.67.Hk **DOI:** 10.7498/aps.74.20250029

CSTR: 32037.14.aps.74.20250029

* Project supported by the National Natural Science Foundation of China (Grant Nos. 62471001, 12475009, 12075001, 12175001, 12004006), the Natural Science Foundation of Anhui Province, China (Grant Nos. 2022b13020004, 2008085QA43), and the Scientific Research Project of Universities in Anhui Province, China (Grant Nos. 2024AH050068, 2024AH040008).

† Corresponding author. E-mail: songxk@ahu.edu.cn

专题: 量子信息处理

量子秘密共享研究现状与展望*

尹华磊 1)#† 沈建宇 2)# 陈诺 2)# 陈增兵 2)

1) (中国人民大学物理学院, 北京 100872)

2) (南京大学物理学院, 南京 210093)

(2025 年 4 月 30 日收到; 2025 年 6 月 24 日收到修改稿)

随着量子通信和量子计算的快速发展, 人们对数据隐私保护和分布式量子信息处理的需求不断增高. 量子秘密共享作为经典秘密共享的量子延伸, 借助量子力学的基本原理可以在多方之间安全地共享信息, 提供了信息安全的新范式. 作为多方安全量子通信和分布式量子计算的重要基础, 量子秘密共享一经提出便受到广泛关注. 当前, 量子秘密共享研究已经包含经典和量子的场景, 在理论与实验上不断取得新的进展. 但在实际应用中仍然面临着量子信道噪声、设备不完美及量子资源受限等诸多困难和挑战, 实用性和安全性仍然难以兼顾. 本文将简要介绍不同技术路线下量子秘密共享的研究现状, 总结近年来量子秘密共享的发展趋势, 并对其未来的发展方向进行讨论和展望.

关键词: 量子秘密共享, 量子通信, 量子纠缠, 多方量子协议

PACS: 03.67.–a, 03.67.Dd, 03.67.Hk **DOI:** 10.7498/aps.74.20250586

CSTR: 32037.14.aps.74.20250586

1 引 言

作为现代密码学的一个重要分支, 经典的秘密共享方案最早在 1979 年由 Shamir[1] 和 Blakley[2] 分别独立提出, 是最重要的信息安全密码协议之一. 秘密共享方案的核心思想是将共享的秘密拆分成 n 个子秘密并分发给参与者. 只有当合作的参与者人数达到授权人数 k 时, 共享的秘密才得以被恢复. 任何参与者人数小于授权人数的情况, 共享的秘密都无法被恢复, 并且无法得到有关秘密的任何信息. 此外, Shamir[1] 和 Blakley[2] 证明, 对于任意 k 和 n 的取值均存在相关的 (k,n) 门限方案. 这有效阻止了内部人员窃听导致的秘密信息泄露. 秘密共享的提出为电信系统、互联网以及分布式计算机等现代信息技术提供了可靠安全的通信.

量子密钥分发 (quantum key distribution, QKD) 是目前最接近实际应用的量子技术之一[3–5]. 随着 QKD 的设备和技术逐渐成熟, 量子通信网络用户不断增加, 多用户量子通信协议的需求开始彰显[6–10]. 利用量子资源的秘密共享被称为量子秘密共享 (quantum secret sharing, QSS). QSS 利用量子资源在多方之间共享秘密信息. 1999 年, Hillery 等[11] 基于 GHZ (Greenberger-Horne-Zeilinger) 态提出了第 1 个 QSS 协议. 同年, Cleve 等[12] 基于量子纠错编码理论, 提出了量子 (k,n) 门限方案. 此后, 基于这两篇文章, 各种类型的 QSS 协议被相继提出, 并在实验上得到证明. 与经典的秘密共享不同, QSS 中秘密的信息分割与分发是基于对分布式量子态的局域测量来实现的, 因此 QSS 允许在存在窃听的情况下安全地分配共享的份额. 同时不同于 QKD, QSS 是多方的通信过程, 允许更丰富、

* 国家自然科学基金 (批准号: 12274223) 资助的课题.

同等贡献作者.

† 通信作者. E-mail: hlyin@ruc.edu.cn

更灵活的量子通信. 但 QSS 不仅需要排除外部的窃听行为, 还需要防范通信各方潜在的内部欺骗行为, 因此 QSS 对其协议有更严格的要求.

秘密共享问题可以分为 3 个子问题[13]. 1) CC. 分发者通过分发者和参与者之间私人信道以及每对参与者之间的经典私人信道来共享经典信息. 2) CQ. 分发者通过分发者和参与者之间公共信道以及每对参与者之间的经典或者量子信道来共享经典信息. 3) QQ. 分发者通过分发者和参与者之间共享的公共或者私人的量子信道以及每对参与者之间的经典或者量子信道来共享量子信息. 如图 1 所示, 根据不同的分类方法, QSS 可以分为不同的类型, 但总的来说 QSS 主要研究的就是 CQ 和 QQ 两个子问题. QSS 一方面可以利用量子资源增强经典秘密共享的安全性, 有效抵抗公共信道的窃听行为. 另一方面量子信息的秘密共享, 将为大规模多方量子网络和分布式量子计算的构建提供重要技术支持. 因此 QSS 逐渐成为量子信息技术的一个研究焦点. 本文将分别从共享经典信息的 QSS 和共享量子信息的 QSS 两个主要方向, 梳理和介绍近年来不同技术路线下 QSS 的研究进展与现状, 并对 QSS 的研究趋势和未来的研究方向进行总结和展望.

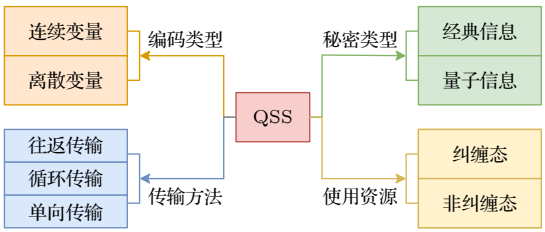


图 1 QSS 协议的类型

Fig. 1. Types of QSS protocol.

2 经典量子秘密共享 (CQ)

2.1 使用纠缠态的经典量子秘密共享

使用纠缠态的经典量子秘密共享指利用量子纠缠态来对经典比特进行秘密共享. 由 Hillery 等[11]于 1999 年提出的 QSS 协议展示了如何使用 GHZ 态去对经典信息和量子信息进行分割与重构, 这个协议也被称为 HBB 协议. 在共享经典信息的 HBB 协议中, Alice, Bob 和 Charlie 分别随机在基 $|\pm x\rangle=(|0\rangle\pm|1\rangle)/\sqrt{2}$ 和 $|\pm y\rangle=(|0\rangle\pm \mathrm{i}|1\rangle)/\sqrt{2}$ 中对三粒子 GHZ 态进行测量:

$$|\psi\rangle_{\mathrm{ABC}}=\frac{1}{\sqrt{2}}(|000\rangle+|111\rangle)_{\mathrm{ABC}}, \tag{1}$$

下标 A, B, C 分别表示属于 Alice, Bob 和 Charlie 的粒子. 三方的测量结果具有关联性, 关联结果如表 1 所示. 通过这些关联性 Alice, Bob 和 Charlie 根据一定的编码规则可以得到一个二进制的密钥串, 满足 $k_{\mathrm{A}}=k_{\mathrm{B}}\oplus k_{\mathrm{C}}$. 只有 Bob 和 Charlie 合作才能知道 Alice 的比特, 实现了秘密共享.

表 1 三方测量结果的关联性

Table 1. Correlation of the measurement results from three parties.

		Alice			
		$\|+x\rangle$	$\|-x\rangle$	$\|+y\rangle$	$\|-y\rangle$
Bob	$\|+x\rangle$	$\|+x\rangle$	$\|-x\rangle$	$\|-y\rangle$	$\|+y\rangle$
	$\|-x\rangle$	$\|-x\rangle$	$\|+x\rangle$	$\|+y\rangle$	$\|-y\rangle$
	$\|+y\rangle$	$\|-y\rangle$	$\|+y\rangle$	$\|-x\rangle$	$\|+x\rangle$
	$\|-y\rangle$	$\|+y\rangle$	$\|-y\rangle$	$\|+x\rangle$	$\|-x\rangle$

但原始的 HBB 协议是不安全的, 不诚实的参与者可以在不引入任何错误的情况下获得所有信息[14]. 2005 年, 通过利用四光子纠缠源制备 GHZ 态, Chen 等[15]首次对 HBB 协议进行了实验实现, 在此之前仅证明了使用伪 GHZ 态[16]实验实现 QSS 的可行性. 在这些方案中, 识别多粒子 GHZ 状态也是必要的. 一般来说, Bell 态的识别比 GHZ 态的识别要容易得多, 大量基于 Bell 态的 QSS 协议被提出[17,18]. 2019 年, Williams 等[19]基于 Bell 态提出并实验演示了一个使用偏振纠缠光子对的实用三方 QSS 协议. 如图 2 所示, 偏振纠缠 QSS 协议依赖泵浦偏振来制备所需的量子态, 而不是在光子对产生后再进行调制. 这一方面可以对产生的纠缠态进行高速调制, 另一方面使得协议不易受损耗的影响, 可以有效保证 QSS 的性能.

三方的 QSS 很快被得到证明, QSS 向着四方乃至更多方的 QSS 发展[20]. 一种高纠缠四光子态[21]也被证明可以实现四方 QSS[22], 表明了利用多光子纠缠实现安全多方量子通信的可行性. Yu 等[23]利用多能级系统构造出了多方 QSS 的一般方案, 并给出了有效测量的一致性条件:

$$A+B+C+\cdots+\Omega=0 \mod d, \tag{2}$$

$$a+b+c+\cdots+\omega=0 \mod d, \tag{3}$$

其中大写字母表示测量基, 小写字母表示给定正交

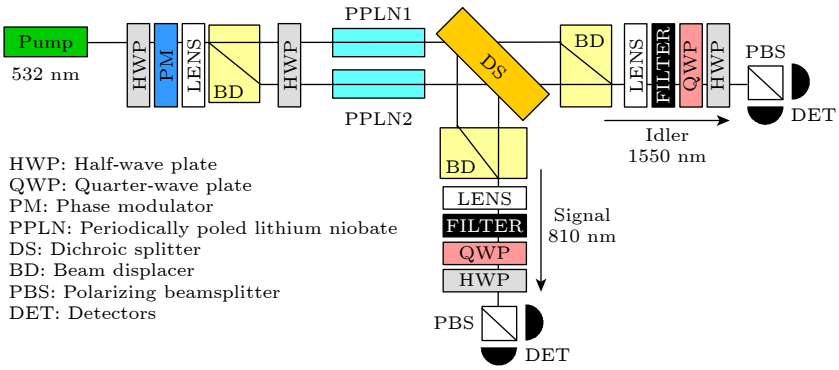


图 2 偏振纠缠光子源示意图[19]

Fig. 2. Schematic of the polarization-entangled photon source[19].

测量基中的向量. 如同 Hillery 等[11] 最初的方案, 参与者首先利用本地操作和经典通信 (local operations and classical communication, LOCC) 确定 (2) 式是否满足, 如果满足, 则 (3) 式表达的就是各方建立的密钥关系. 如果不满足, 则丢弃本轮结果. 对抗截获-重发等攻击的能力对 QSS 的安全性来说非常重要. 常见的二能级系统的 QSS 方案[11] 检测到截获-重发攻击的概率仅为 25%, 因此增强抵抗此类攻击能力的一个最直接的办法就是使用更高维的量子系统来实现 QSS. 更高维的量子系统使得 QSS 协议更加复杂, 攻击者截获-重发攻击未被检测到的概率将大幅降低. 使用非常高维的互无偏基 (mutually unbiased bases, MUBs) 的方案原则上能够完美抵抗此类攻击. 但另一方面, 这也将使得协议需要耗费更多的量子资源, d 维量子系统 QSS 协议的效率只有 $1/d$. 但采用 Xiao 等[24] 提出的基于测量基加密的高效 QSS 方案之后, QSS 协议的效率将能够从 $1/d$ 提高至 100%.

虽然纠缠态的使用能够使窃听者难以单独篡改或者窃取部分信息, 具有很强的安全性. 但是对于使用纠缠态的情况, 增加和删除参与者往往需要改变系统的维度, 这将不得不对源进行复杂的更改, 限制了其可扩展性. 为了解决这一问题, Xiao 等[25] 利用单纠缠光子对源和波分复用技术[26] (wavelength-division multiplexing) 提出了一种在全连接量子网络架构[27] 中的高效源无关 QSS 协议. 基于该量子网络体系, 网络提供商利用单纠缠光子对源产生两体纠缠并通过波分复用技术将两体纠缠分发到多个用户, 该协议可以在不改变纠缠源和网络用户硬件的情况下进行多方扩展, 在城域网以及更大规模量子网络的构建中具有很大的应用潜力.

2.2 使用非纠缠态的经典量子秘密共享

虽然纠缠态的使用使得窃听者无法在不被察觉的情况下获取秘密信息, 给 QSS 协议提供了安全性的保障. 但是就目前来看, 纠缠态的制备需要复杂的实验设备, 仍然很难被高亮度、高保真度地产生、操控和分发[28–32]. 同时由于纠缠态易受光子损耗、偏振畸变等环境噪声的影响, 导致纠缠退化, 难以远距离传输[33], 这限制了 QSS 系统的密钥率和稳定性, 使得 QSS 方案的可靠性大大降低. 2003 年, Guo 等[34] 基于 BB84 QKD 协议首次提出了不依赖纠缠的 QSS 协议, 仅需要使用两量子比特乘积态就能完成共享密钥的建立. 随后, 大量研究表明, 在共享经典信息的 QSS 中纠缠并不是必须的.

2.2.1 单量子比特量子秘密共享

为规避多光子纠缠源的使用, 单光子 QSS 协议应运而生[35–37]. 实验上, 实现单光子 QSS 方案最常见的方案是基于光的偏振[35]. 除此之外还可以利用单光子和零光子的叠加态来构建单量子比特. 2005 年, Schmid 等[38] 基于单光子提出了一种使用单量子比特的 QSS 协议. 在这个协议中, 秘密共享的任务不再需要多粒子纠缠 GHZ 态, 而只需要在一个传递的单量子比特上对其相位进行局域操作就可以实现. 在这里, 量子比特的初态制备为 $|+x\rangle=(|0\rangle+|1\rangle)/\sqrt{2}$. 然后量子比特在各参与者中依次传递, 每个参与者都用如下酉相位算子作用在这个量子比特上:

$$\hat{U}_j(\varphi_j)=\begin{cases}|0\rangle\to|0\rangle,\\ |1\rangle\to \mathrm{e}^{\mathrm{i}\varphi_j}|1\rangle,\end{cases} \tag{4}$$

其中随机选取 $\varphi_j\in\{0,\pi,\pi/2,3\pi/2\}$. 那么通过所有参与者后的量子比特将处于状态:

$$|x_N\rangle\frac{1}{\sqrt{2}}(|0\rangle+\mathrm{e}^{\mathrm{i}\sum_j^N\varphi_j}|1\rangle). \tag{5}$$

当各参与者的类型满足 $\cos(\sum_j^N\varphi_j)=\pm1$ 时, 最后一位参与者在基 $|\pm x\rangle=(|0\rangle\pm|1\rangle)/\sqrt{2}$ 上能够测得 ±1, 此时量子比特有效 (可通过特定的选择使得量子比特总是有效). 此时由于 φ_j 满足余弦关系式, 当最后一位参与者宣布测量结果后, 任何 $N-1$ 方子集都能推断出剩余一方的 φ_j 值, 实现秘密共享.

与纠缠态的方案相比, 单个量子比特更具有实验可实现性和可扩展性. 文献 [38] 中就利用线性光学元件和光子偏振态分析给出了 6 个参与方的实验演示, 是当时实现的量子协议中积极执行的参与方最多的. 除了实验演示外, 单量子比特 QSS 也在光纤中得到实现. 电信级的相位调制器是偏振敏感的, 而在单模光纤中受双折射效应影响, 激光脉冲的偏振会缓慢随机的变化, 这很大程度上影响了相位调制器的正确作用. Bogdanski 等 [39] 基于偏振控制系统和偏振不敏感相位调制器, 在 Sagnac 中提出了补偿单模光纤双折射效应的概念, 解决了单模光纤中双折射漂移的问题 [40], 实现了第 1 个在 1550 nm 单模光纤网络上使用相位编码单量子比特协议的 Sagnac QSS 方案 (三方和四方). 随后, Ma 等 [41] 也在 50 km 单模光纤网络上实现了使用相位编码的鲁棒的三方单光子 QSS 方案, 能见度高达 99.4%. 这表明了单量子比特 QSS 在实际系统中具有良好的应用潜力, 在电信光纤网络上实现量子秘密共享是可行的. 但值得注意的是, 二维的单量子比特 QSS 在安全性方面仍存在一定限制 [42,43], 容易受到特洛伊木马的攻击 [44]. 窃听者可以向参与者的基站发送信号, 并通过测量输出信号来明确地的确定参与者所拥有的私密信息.

另一方面, 一些基于纠缠态的 QSS 协议是可以转化为非纠缠态的. 例如扩展到 d 能级系统的 GHZ 态协议 [23] 可以转化为单个 qudit 顺序传输的协议 [45]. 而在高维形式下, 二维单量子比特顺序传输 QSS 协议的安全漏洞得以解决. 因此更高维的单 qudit QSS 协议被相继提出. 制造高维的单 qudit 一般有两种方式, 一种是利用光子本身的自由度, 一种是利用路径的自由度. 光子本身自由度最常见的就是光子的偏振, 但偏振只有两个自由度, 限制了向更高维度的扩展. 而光子的轨道角动量 [46,47] (orbital angular momentum, OAM) 能够提供无穷维的希尔伯特空间, 为实现高维的量子信息过程提供了一条新途径, 因此可以用来实现单 qudit QSS. Pinnell 等 [48] 利用 OAM 实现了 10 方 QSS 的实验演示, 如图 3(a) 所示. 另外还可以使用经过不同的路径的系列光子的组合来制造 qudit. 例如在信道中使用三臂类马赫-曾德尔干涉仪可以产生单个 qutrit, 从而实现三方 QSS[49], 如图 3(b) 所示.

值得注意的是, 很多理论上基于单光子的 QSS 协议实验上都选择使用弱相干光来实现 [39,41,48,49]. 虽然单光子的产生与纠缠态相比已经更加容易, 但单光子在实验上仍然难以高效地产生和控制. 弱相干光可以通过普通激光源结合可调谐衰减器 (如中性密度滤光片等) 来进行制备, 实验实现简单、技术成熟, 具有高稳定性和易操作性. 另一方面, 单光子源的光子产生率往往较低, 而弱相干光则可以通过调整激光功率和重复频率来提高光子的产生率. 同时, 弱相干光可以使用标准光纤传输, 不需要额外的光子管理技术, 在现有技术下更容易实现远距离传输. 因此弱相干光常常被用作单光子源的替代方案. 但弱相干光的使用会损失单光子带来的安全性. 由于弱相干光服从泊松分布, 其无法避免地存在多光子成分, 这使得弱相干光无法无条件安全地抵御光子数分裂 (photon-number-splitting, PNS) 攻击 [50,51]. 不过, 在实际部署中这种攻击可以通过诱骗态 [52–54] 或者在 QSS 协议中增加额外的安全补偿机制来减轻.

2.2.2 相位编码量子秘密共享

为了抵抗 PNS 攻击, 并进一步简化实验装置, Inoue 等 [55] 基于差分相移 (differential-phase-shift, DPS) 的 QKD, 提出了一种 DPS-QSS[56]. 与之前的协议不同, DPS-QSS 的密钥信息储存在相邻脉冲的相对相位中, 并且需要 Charlie 随机选择脉冲时隙进行测量, 如图 4(a) 所示. 而 PNS 攻击者选择和 Charlie 相同时隙对光子进行计数的概率很低, 因此这个协议对抵抗 PNS 攻击具有很好的鲁棒性. DPS-QSS 的提出为量子秘密共享的实用化、可行化开辟了一条新的路径. 但遗憾的是, Inoue

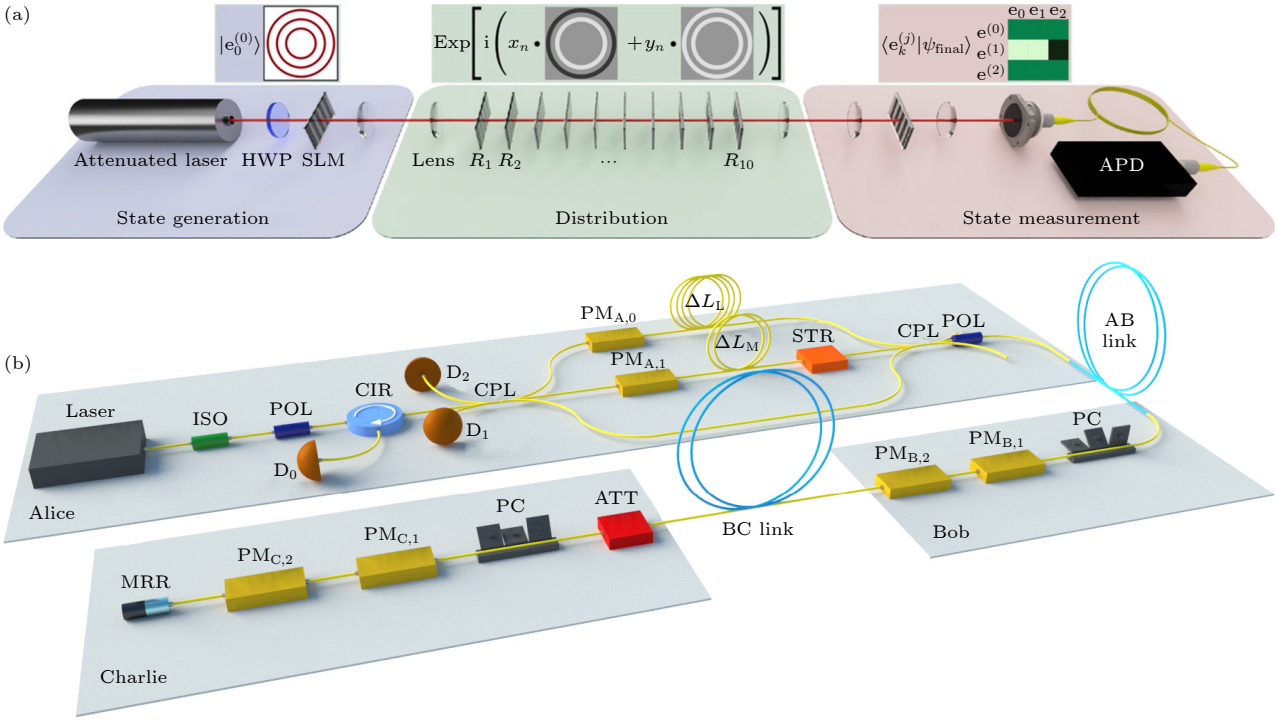


图 3 实现高维单 qudit QSS 的两种方法 (a) 使用光子轨道角动量[48]; (b) 使用多臂类马赫-曾德尔干涉仪[49]

Fig. 3. Two methods for achieving high-dimensional single-qudit QSS: (a) Using the orbital angular momentum of photons[48]; (b) using the multi-arm Mach-Zehnder-like interferometer[49].

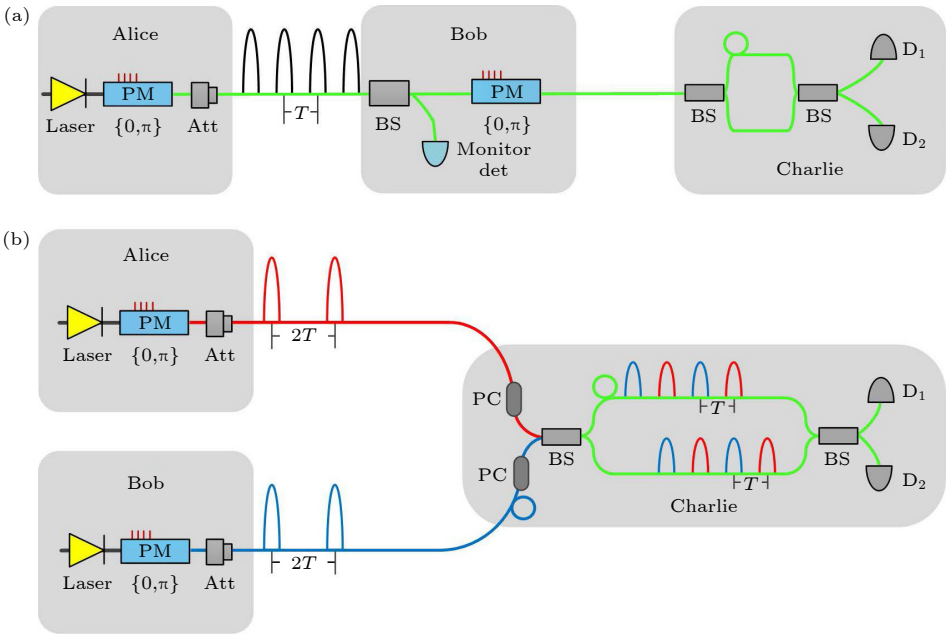


图 4 DPS-QSS 协议的配置[57] (a) 典型 DPS-QSS 的实验配置; (b) 使用双场的 DPS-QSS 的实验配置

Fig. 4. Configuration of DPS-QSS protocol[57]: (a) Setup of typical DPS-QSS; (b) setup of DPS-QSS using a twin field.

最初提出的方案无法抵御特洛伊木马的攻击. 2021 年 Gu 等[57] 结合双场[58–60] 提出了使用双场的 DPS-QSS 协议. 如图 4(b) 所示, 该协议与文献[56] 中的协议是等价的, 但由于使用双场, Alice 的脉冲不需要顺序经过 Bob 并被 Bob 调制, 因此该方案可以安全地抵御特洛伊木马的攻击. 但是 DPS-QSS 协议仍然存在安全局限性, 只能抵抗个体攻击 (例如 PNS 攻击和光束分裂攻击), 而无法抵抗更强大的相干攻击[61](coherent attacks). 2023 年, Shen 等[62] 进一步提出了一种可以抵抗相

干攻击的 QSS 协议, 并通过在相干态上对逻辑位进行相位调制编码, 消除了对强度调制和相位随机化的要求, 简化了实验设置, 为实现 QSS 的安全性和实用性的结合问题提供了解决途径. 但协议[62]针对不同参与者在一些步骤中表现出不对称性, 因此需要事先了解窃听者的身份, 并可能引入安全漏洞. 随后 Wang 等[63]对协议[62]进行了修正, 对所有参与者采用对称程序, 消除了协议[62]因不对称基选择而产生的安全漏洞.

2.3 连续变量量子秘密共享

根据编码类型, 除了前文提到的离散变量 QSS (discrete-variable QSS, DV-QSS) 之外, 还有连续变量 QSS (continuous-variable QSS, CV-QSS). 传统的 QSS 主要利用离散的量子比特实现, 而 CV-QSS 则是在光场的正交分量 (振幅 $\hat{x}$ 和相位 $\hat{p}$) 中对密钥位进行编码. 因其高效的信息编码方式, 成熟的光学实现技术以及较高的容错能力, CV-QSS 成为 QSS 乃至量子密码学的一个重要研究方向. 在 Grosshans 和 Grangier[64]将连续变量引入量子密码学后不久, Tyc 等[65]提出了首个 CV-QSS 协议. 随后 Lance 等[66]对 Tyc 的协议进行了扩展, 利用电光前馈技术验证了 (2, 3) 门限 CV-QSS 协议的可行性, CV-QSS 正式进入历史舞台. 2017 年, Kogias 等[67]给出了 CV-QSS 同时对抗窃听者和不诚实参与者的充分条件, 这适用于所有 (k,n) 门限 CV-QSS 方案.

实现 CV-QSS 的一种方法是使用 Einstein-Podolsky-Rosen (EPR) 纠缠态 ($\hat{a}_{\rm EPR1}$ 和 $\hat{a}_{\rm EPR2}$) 和光的热态 (thermal states)($\hat{\nu}_1^{\rm T}$ 和 $\hat{\nu}_2^{\rm T}$) 来制备束缚纠缠 (bound entanglement, BE) 态, 并将秘密信息 $a_s(a_s^*)$ 调制到 BE 态中[68]:

$$\hat{b}_{1(2)} = (\hat{a}_{\rm EPR1} \pm \hat{\nu}_1^{\rm T} + a_s)/\sqrt{2}, \tag{6}$$

$$\hat{b}_{3(4)} = (\hat{a}_{\rm EPR2} \pm \hat{\nu}_2^{\rm T} + a_s^*)/\sqrt{2}, \tag{7}$$

BE 态处于可分离态和自由纠缠态之间, 其无法表示为分离态的形式, 同时其也是不可提纯的, 无法通过 LOCC 来提纯纠缠[69–71]. 从 (6) 式和 (7) 式中可以看到, 每个子模式都存在较大的噪声背景, 任何一个玩家都无法检索到调制信号比较小的秘密信息. 只有当足够多的参与者合作进行组合噪声测量时, 秘密信息才得以揭示. 除了束缚纠缠态外, 连续变量簇态[72]、连续变量 GHZ 态[73]、连续变量图态[74]等连续变量纠缠态也在逐渐被广泛运用到 QSS 的研究当中. 但正如前文对于离散变量纠缠态所讨论的那样, 使用连续变量纠缠态的 QSS 由于其仍然基于多方纠缠, 当参与者的数目很大时在现有技术下难以实现. 同时, 虽然相比于使用纠缠态的 DV-QSS, 使用纠缠态的 CV-QSS 能够和现代光通信技术有更好的兼容, 但其仍然面临着难以容忍的信道损耗[67].

为避免纠缠态的使用, 基于弱相干态的顺序 CV-QSS 协议被提出[75], 这进一步提高了 CV-QSS 与现代光通信技术的兼容性及其实用性. 同时与单量子比特顺序 QSS 方案相比, 此方案具有天然的抵抗特洛伊木马攻击的能力. 随后, 这个思想被进一步扩展到基于热态[76]和基于离散调制相干态[77,78]的 CV-QSS, 促进了 CV-QSS 的发展. 但不幸的是, 大多数相干态的 CV-QSS 协议要求所有参与者在自己的站点准备自己的激光源, 这种成本是巨大的. 并且所有参与者的独立激光源之间的相位需要严格锁定, 信号同步问题难以解决. 更重要的是, 由于 CV-QSS 要求每个参与者将自己的本振 (local oscillator, LO) 信号通过不安全的信道发送给分发者, 因此本振信号很容易成为攻击者攻击的目标. 2022 年, Liao 等[79]提出了一种基于即插即用 (plug-and-play) 结构[80]和双相调制 (dual-phase modulation) 策略的 CV-QSS 方案, 解决上述问题. 但这需要在不受信任的量子通道中传输未调制的量子信号, 可能会引入新的漏洞. 随后 Liao 等[81]进一步基于本地 LO (local LO, LLO) 技术提出了 LLO-CVQSS 的方案, 彻底堵住了 CV-QSS 系统中传输 LO 导致的可能遭受各种攻击的漏洞. 除此之外, 对于 CV-QSS, 由于经销商的联合测量, 来自其他参与者的信道过剩噪声 (channel excess noises) 的叠加将会使密钥率大幅降低[75,76,79]. 利用将其密钥信息编码到光场的不同边带[82]的多边带调制方法[83], 分发者可以使用单个外差检测器 (heterodyne detector) 提取多个参与者的信息, 并且由于每个参与者的量子信道透射率 (quantum channel transmittance) 和信道过剩噪声等信道参数的评估是独立的, QSS 的量子密钥率和传播距离显著提高. 同时, 利用该方法的硬件架构, 只需要切换经典的后处理程序就可以实现 QSS 和会议密钥协商[84–86](conference key agreement) 的灵活切换. Richter 等[87]也实验演示了一个具有量子加

密敏捷性 (quantum cryptoagility) 和多功能性的系统, 能够在同一平台上实现连续变量量子数字签名 (quantum digital signatures)[88]、连续变量 QSS 和连续变量 QKD[89–91]. 这种利用同一硬件支持不同量子密码协议切换的系统将大幅增加量子通信设备的通用性.

2.4 量子秘密共享的安全性保障

传统的 QSS 会利用信号的扰动检测来保障安全. 发送方通常会将发送的一部分量子比特作为检测比特. 根据量子不可克隆定理, 量子态无法被完美复制, 任何窃听行为都会对量子态造成干扰, 从而在传输的量子比特中引入错误. 因此可以对信号的扰动进行检测来判断通信是否遭到窃听. 通过计算错误比特和总检测比特的比值可以得到量子比特误码率, 如果量子比特误码率超过了某一阈值 (信道固有误码率), 则说明存在窃听者, 本轮通信将被放弃. 这很大程度上提高了 QSS 的安全性. 但是信号扰动检测会损失一部分比特用于检测, 降低了通信效率. 同时在某些攻击 (如特洛伊木马攻击) 的情况下, 误码率可能不会明显上升造成误判. 2021 年, Gu 等[92] 受环回 (round-robin) 差分相移 QKD[93] 和双场 QKD[58] 的启发, 提出了一个不监测信号扰动的三用户 QSS 协议, 即环回 QSS. 这个协议面向内部和外部攻击者是无条件安全的, 并且密钥率能够打破 Pirandola-Laurenza-Ottaviani-Banchi 界限[94]. 环回 QSS 由于其高噪声容忍和抗信号干扰等固有优势, 有较好的应用前景, 但其对可变延迟马赫-曾德尔干涉仪的要求限制了其实际应用.

使用纠缠态的 QSS 即使光源部分被攻击者控制, 只要测量端能够被完美表征并进行测量错误率即可获得安全秘密共享, 因此可以实现光源设备无关的安全性. 但使用单光子或者相干光的 QSS 则是完全依赖于设备的完美表征, 因此设备的不完善性会给实际系统带来安全漏洞. 诸如致盲攻击[95–97]、时移攻击[98]、波长攻击[99]、偏振旋转攻击[100]、饱和攻击[101] 等针对测量设备的侧信道攻击[102](side-channel attacks) 会给量子通信系统的安全性造成极大的威胁. 测量设备无关 (measurement-device-independent, MDI) 的量子通信技术[103] 通过引入不信任的第三方进行来执行测量, 利用后选择纠缠免除了探测器必须由合法分发者保护的必要性, 为侧信道攻击提供了解决方案. 2015 年, Fu 等[104] 提出了第一个 MDI-QSS 协议, 利用后选择 GHZ 态和诱骗态[52,105] 实现了对测量设备攻击和 PNS 攻击的抵抗, 实验装置如图 5 所示. 随后 MDI-QSS 在离散变量[106–109] 和连续变量[110,111] 领域得到广泛发展. 尽管 MDI-QSS 不需要使用纠缠资源, 但传输效率仍然会随着用户数量的增加呈指数级下降. 2023 年, Li 等[112] 基于全光量子中继[113] 和自适应 MDI-QKD[114] 中的空间复用 (spatial multiplexing) 和自适应操作提出了一种更加高效实用的 MDI-QSS. 当通信方的数量增加时, 协议的传输效率可以保持不变, 并在至少 10 个通信方的情况下打破网络上的速度-距离界限[94]. 除了测量设备外, 不完美光源同样会造成侧信道信息泄露, 威胁 QSS 的安全性. 为消除所有实际不完美设备的

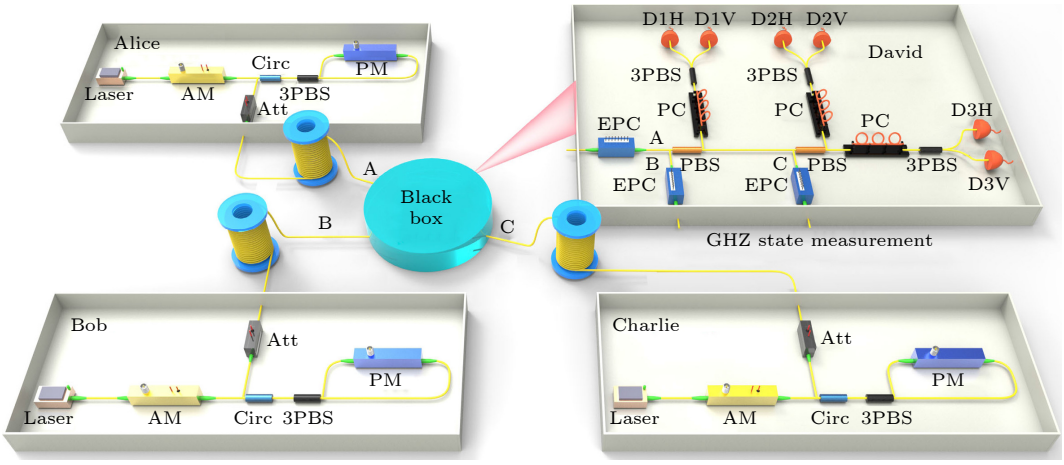


图 5 MDI-QSS 装置的示意图[104]

Fig. 5. Schematic of the MDI-QSS setup[104].

安全漏洞, 设备无关 (device-independent, DI) 的 QSS 被提出[115–117]. 但在实际通信过程中, 目前的 DI-QSS 的性能仍然较低, 尚未有效实现.

QSS 的概念首次提出时, 使用的是量子典型特征的纠缠态来共享经典信息. 但由于纠缠态制备、控制和传输在当前技术条件下实现较为困难、实用性较低. 因此使用单光子的非纠缠态的 QSS 协议被相继提出, 但单光子目前在实验上依然难以高效地产生和控制, 并且与目前的通信光纤有适配性差异. 于是, 作为单光子和纠缠态的替代方案, 使用相干光 QSS 协议被提出, 并得益于其成熟的实验技术在光纤网络上迅速得到实现. 仍需指出的是, 单光子和相干光的使用会损失纠缠态带来的安全性, 相干光也比单光子更容易受到光子数分裂攻击. 为此, 诱骗态、环回、MDI 等方法被使用以提高 QSS 的安全性. 近年来提出的 QSS 协议已经能很好地抵御外部攻击和内部成员攻击等一系列安全性问题. 因此, 虽然近年来, 纠缠态的制备、控制和传输已经取得一系列重要突破[118–125], 但是对于共享经典信息的 QSS 来说纠缠态的使用已经不具备明显优势. 相反, 使用非纠缠态的 QSS 因其高稳定性、易操作性和光纤适配性, 具有更高的实用价值. 但在量子信息的秘密共享领域, 纠缠态仍然发挥着不可替代的作用.

3 量子信息的秘密共享 (QQ)

量子信息的秘密共享 (QQ) 的概念渊源最早可追溯至由 Bennett 等[126] 在 1993 年所提出的量子隐形传态, 发送者借助于量子纠缠资源, 可以在不传递物理粒子的情况下将未知量子态信息传递给接收者. QQ 即可被认为是多方量子隐形传态的一个应用. 1999 年, Hillery 等[11] 使用 GHZ 态和 Bell 基测量提出了首个 QQ 方案, Alice 将未知量子态传送给她的代理组 Bob 和 Charlie, 代理组成员之间仅有一人能够在 Alice 处 Bell 基的测量结果和另一位成员的信息下对量子态秘密进行重构, 因此 QQ 也被称为量子信息分割 (quantum information splitting, QIS) 或量子态共享 (quantum state sharing, QSTS). 本节将依次讨论离散变量情况下 QQ 中的对称性方案、非对称分层方案与基于一种重要量子资源态, 图态的方案, 然后介绍 QQ 中的连续变量方案, 最后展示对纠缠态进行共享和多方量子秘密直接传输的重要工作. 现存 QQ 方案重要的问题主要包括秘密共享方案结构与参与者数量的拓展, 方案共享信息从单量子比特态、多量子比特态到高维量子态的拓展, 以及衡量量子资源消耗、操作复杂度和通信成本, 对具有更高效率方案的研究.

3.1 对称性量子信息秘密共享方案

(k,n) 门限方案是一类具有对称性的重要秘密共享方案. 在 (k,n) 门限方案中, 对于恢复秘密的要求仅为参与者数量. 数量达到门限 k 的任意参与者均成为授权者集合, 合作时可以完美恢复秘密, 少于 k 位参与者的集合则被拒绝访问任何关于秘密的信息. 1999 年, Cleve 等[12] 首次定义了 QQ 中的 (k,n) 门限方案并基于量子纠错码给出了一种通用的构造方式, 与文献 [11] 共同成为 QQ 领域的开创性工作. 设量子态秘密 $|s\rangle$ 的维度为 s, 选择素数 q 满足 $\max(n,s)\leqslant q\leqslant 2\max(n,s)$, 构造有限域 $\mathbb{F}_q$, 其中 $\mathbb{F}=\mathbb{Z}_q$. 对于 $s\in\mathbb{F}$, 可将量子态 $|s\rangle$ 编码为 n 个份额:

$$|s\rangle\mapsto\sum_{c\in\mathbb{F}_q^k,c_{k-1}=s}|p_c(x_0),\cdots,p_c(x_{n-1})\rangle,\tag{8}$$

其中, 多项式 $p_c(t)$ 定义为 $p_c(t)=c_0+c_1t+\cdots+c_{k-1}t^{k-1}$, 系数 $(c_0,c_1,\cdots,c_{k-1})\in\mathbb{F}^k$, 坐标 $x_0,x_1,\cdots,x_{n-1}$ 选取为 $\mathbb{F}$ 上互不相同的 n 个点, 所分发的子份额则为多项式在某个坐标 x_i 上的取值 $p_c(x_i)$.

对于共享量子信息的情况, 量子不可克隆原理要求量子态秘密不可被多次恢复, 限制了 $k\geqslant n/2$. 在所有编码后全局态为纯态的 (k,n) 方案中, 授权集与未授权集均为互补, 即满足条件 $n=2k-1$. 在 $(k,2k-1)$ 门限方案的基础上丢弃份额可以直接得到其他 $k\leqslant n<2k-1$ 方案, 但此时将为混合态方案. 一般而言, Cleve 等[12] 给出的方案需要使用高维量子比特的混合态.

(k,k',n) 斜坡方案为 (k,n) 门限的一种弱化, 在进行秘密共享 n 名参与者中, 任何 k 及以上名参与者的集合能够完美访问秘密, 任何 k' 及以下名参与者无法获取任何秘密信息, 其他情况则面临着量子态秘密泄露的风险. 当 $k'=k-1$ 时, 斜坡方案就成为 (k,n) 门限方案. Senthoor 和 Sarvepalli[127] 在 Cleve 等[12] 工作的基础上构建了一个通用的通信高效量子门限秘密共享方案, 其结合斜坡方案和

标准门限方案, 通过在参与者人数高于门限时根据实际需求灵活选择任意数量的参与方, 提高了秘密恢复的通信效率.

在固定结构的方案之外, 实际情况下, 秘密分发者可能会根据工作需要增加或减少成员, 重新对新代理组进行秘密分发面临高昂的成本, 为此提出了动态量子秘密共享方案 (dynamic quantum secret sharing, DQSS), 其在共享经典信息和量子信息的过程中允许对接收者代理组进行更改. DQSS 源于 CQ 情形下由 2011 年 Yang 等 [128] 首次提出的 (k,n) 门限方案中进行成员扩展的协议. 2012 年, Jia 等 [129] 基于星形簇态, 提出了一种 CQ 和 QQ 的动态方案. 利用星状簇态在泡利测量下的可扩展性, 分发者能够在子份额被分发前与分发后两个阶段对代理组进行增减成员的调整. 若子份额已被分发, 添加新成员则额外需要一名原始成员的授权, 无需重新分配所有份额. Sun 等 [130] 使用单光子偏振态和 CNOT 门操作和 Bell 基测量, 能够在允许增加新用户的代理组中共享量子秘密, 该方案成员扩展的过程无需任何原代理组成员的协助. 但目前工作基本均局限于 (n,n) 门限方案的架构.

量子纠缠是量子隐形传态和 QQ 方案的核心, 纠缠态的特殊性质为处理量子信息任务提供了很好的支持. 自 Hillery 等 [11] 以来, 提出了许多基于不同纠缠态的 QQ 方案设计, 包括 Bell 态 [131–135]、GHZ 态 [11,136]、簇态 [137]、W 态 [138] 等. 在这些方案中, 所有接收者均有能力恢复被发送的未知量子态, 权限结构具有一定的对称性, 因此这一类方案也被称为对称量子信息分割.

在 Hillery 等 [11] 最先的 GHZ 态方案中, 分发者 Alice 将一个初始 GHZ 态 (其中 3 个粒子 a, b, c 分别由 Alice 和接收者 Bob, Charlie 持有) 与秘密量子态 $|\psi\rangle_{\rm A}=\alpha|0\rangle_{\rm A}+\beta|1\rangle_{\rm A}$ 结合, 可得

$$\begin{aligned}|\Psi\rangle &= |\psi\rangle_{\rm A}\otimes\frac{1}{\sqrt{2}}(|000\rangle_{\rm abc}+|111\rangle_{\rm abc})\\ &=\frac{1}{2}\Big[|\Psi^+\rangle_{\rm Aa}(\alpha|00\rangle_{\rm bc}+\beta|11\rangle_{\rm bc})\\ &\quad+|\Psi^-\rangle_{\rm Aa}(\alpha|00\rangle_{\rm bc}-\beta|11\rangle_{\rm bc})\\ &\quad+|\Phi^+\rangle_{\rm Aa}(\beta|00\rangle_{\rm bc}+\alpha|11\rangle_{\rm bc})\\ &\quad+|\Phi^-\rangle_{\rm Aa}(-\beta|00\rangle_{\rm bc}+\alpha|11\rangle_{\rm bc})\Big],\end{aligned}\tag{9}$$

其中,

$$\begin{aligned}|\Psi^{\pm}\rangle_{\rm Aa}&=\frac{1}{\sqrt{2}}\left(|00\rangle_{\rm Aa}\pm|11\rangle_{\rm Aa}\right),\\ |\Phi^{\pm}\rangle_{\rm Aa}&=\frac{1}{\sqrt{2}}\left(|01\rangle_{\rm Aa}\pm|10\rangle_{\rm Aa}\right).\end{aligned}\tag{10}$$

因此, 通过 Alice 对 A, a 粒子 Bell 基测量的结果可以确认秘密量子态的振幅信息, 再结合另一位成员 Bob 对他所拥有粒子的测量结果, Charlie 即可执行相应修正操作在自己的量子比特上恢复原始秘密.

相较于其他纠缠态方案, Bell 态方案具有更好的灵活性和可拓展性, 减轻了方案对复杂纠缠态量子资源的依赖. Li 等 [131] 首次利用纠缠交换与 GHZ 基测量设计了 n 名参与者对单量子比特态的共享方案, Yuan 等 [134] 使用两个 EPR 对, 通过 Bell 基测量和接收者处的单比特酉操作, 能够实现两量子比特态的三方安全共享. Shi 等 [135] 结合 Bell 态和 CNOT 门操作, 提出了一种高效、低资源消耗的多方量子态共享方案, 在向 n 名参与者共享两量子比特态时仅需 n 个 Bell 态的量子资源.

W 态是一类区别于 GHZ 态的多体纠缠态:

$$\begin{aligned}|W_n\rangle_{123}=\frac{1}{\sqrt{2+2n}}\big(&|100\rangle+\sqrt{n}{\rm e}^{{\rm i}\theta}|010\rangle\\ &+\sqrt{n+1}{\rm e}^{{\rm i}\phi}|001\rangle\big).\end{aligned}\tag{11}$$

其中 n 为实数, θ, ϕ 为相位. W 态的三体纠缠度为 0. 相较于 GHZ 态, W 态具有更好的鲁棒性, 在丢失任意一个粒子后, W 态中剩余的两粒子仍保持部分纠缠, 不易退相干 [139]. 利用此类纠缠态, Agrawal 等 [140] 已经实现了双方量子隐形传态. Nie 等 [138] 进一步提出了基于 W 态对任意三量子比特态量子态进行三方秘密共享的方案, 结合三量子比特冯·诺依曼测量结果和局域酉算符操作, 可以实现确定性传输. 簇态 [137] 方案的原理本质上与上述方案类似, 实现了单量子比特态和双量子比特态的三方共享.

3.2 非对称分层量子秘密共享方案

Gottesman[141] 基于 QQ 的 (k,n) 门限方案, 对非对称性的量子信息分割做过初步讨论, 他提出可以对门限方案中的子秘密份额进行捆绑, 向参与者分配不同数量份额, 从而实现复杂结构或部分特定要求. 2010 年, Wang 等 [142] 使用一种 4 量子比特纠缠态 $|\chi\rangle$, 首次提出了非对称分割量子信息的

分层量子秘密共享方案 (hierarchical quantum sharing, HQSS), 这一类量子秘密共享方案考虑到参与者之间具有不同属性带来的能级划分, 例如在公司决策中董事长、经理和普通员工之间具有上下级关系, 不同权限能级的接收者在恢复量子秘密时需要不同的协作条件. 随后他们又提出了基于 6 量子比特簇态 [143] 和 t 量子比特 ($t \geqslant 3$) 图态 [144] 的分层 QQ 方案. 由 Shukla 等 [145] 进一步给出了一个在 n 方接收者中实现分层量子秘密共享的通用方案, 基于 4 量子比特 $|\Omega\rangle$ 态或 4 量子比特簇态. 这些方案均依赖特定多粒子纠缠态来支持分层结构的划分, 使得在分发者进行特定测量后坍缩的量子态下, 普通成员在某些基上只能得到相关测量结果, 因此仅当普通成员合作时无法恢复秘密. 正由于构建非对称性的分层 QQ 方案的纠缠态具有很强的特殊性, 分层 QQ 方案在实际部署和更一般的通用结构设计上都面临极大的挑战.

3.3 基于图态的量子信息秘密共享

图态是一类基于图的多粒子纠缠态. 这类纠缠态具有高度的非局域性质, 是目前实验室中最容易获得的多方资源量子态之一. 图态几乎可以编写所有的多方协议, 被提议为基于测量的量子计算、量子纠错和盲量子计算等各种多方量子信息处理任务中的主要资源态之一. 基于图态的量子秘密共享协议由于其使用的纠缠资源态, 天然具备了与复杂网络协议集成以及在纠缠扩展功能上进一步开发的能力. 图 6 为线性簇态、星形图态 (即 GHZ 态)、树形图态、环形图态、二维方格图态等类型图态.

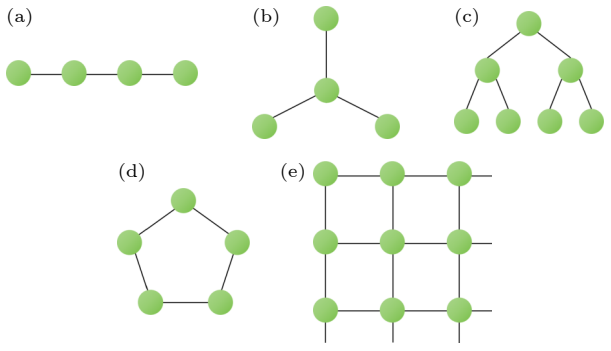


图 6 图态类型 (a) 线性簇态; (b) 星形图态; (c) 树形图态; (d) 环形图态; (e) 二维方格图态

Fig. 6. Types of graph states: (a) Linear cluster state; (b) star-shaped graph state; (c) tree-shaped graph state; (d) ring-shaped graph state; (e) 2D square graph state.

图态本身具有的图形直观地展示了各个部分复杂的纠缠, 提供了一种简化. 图的复杂连接性结构可以支持多样化的各种信息访问结构, 在量子网络的多层复杂通信协议的实现上极具发展前景.

给定一个包含 n 个顶点的无向图 $G = (V, E)$, 其中顶点集合 $V = \{v_i\}$ 表示量子比特, 边集合 $E = \{e_{ij} = (v_i, v_j)\}$ 表示量子比特之间存在的纠缠. 每个顶点上量子比特初始定义为 $|+\rangle = (|0\rangle + |1\rangle)/\sqrt{2}$ 态, 对所有存在边相互连接的量子比特进行受控相位门 $\mathrm{CZ} = \mathrm{diag}(1, 1, 1, -1)$ 操作, 即可得到 n 阶图态:

$$|G\rangle = \prod_{e \in E} CZ_e |+\rangle^{\otimes n}. \tag{12}$$

图态可以通过稳定子生成元的方式来表示, 对于图态中任意第 i 个顶点, 其稳定子算符为

$$K_i = X_i Z_{N(i)}, \tag{13}$$

其中, $N(i)$ 表示图态 G 中与顶点 i 存在边连接的相邻顶点集合, $Z_{N(i)} = \bigotimes_{u \in N(i)} Z_u$.

图态由其稳定子算符的本征方程唯一确定, 这通常也被称为图态的不动点性质:

$$X_i Z_{N(i)} |G\rangle = |G\rangle. \tag{14}$$

在图态的标准框架上, Markham 等 [13] 通过给图态中的顶点附加额外的标签信息, 对稳定子算符作用下部分图态之间的等价性质进行证明, 从而对图态中信息的可访问性给出直观展示.

除去为图态提供了一个优雅的图形化表征之外, 图的相关结论可以被用来对量子性质进行辅助证明和理解. 图论理论为量子光学实验中复杂纠缠态的可构造性提供了新的分析方法 [146]. 图所给出的“流”概念刻画了量子秘密共享协议中秘密信息从分发者到授权者集合的传输路径 [147], 研究 [148,149] 进一步指出了图态中弱奇支配性质在基于图态的量子秘密共享协议中的关键作用. 事实上, 在图态提供的框架下经典信息和量子信息情景下的秘密共享可以形成优雅的统一 [13]. Keet 等 [150] 进一步把由二维量子比特构成的图态扩展至素数维度量子比特的图态, 广义图态下可以实现所有允许的访问结构, 为共享更高维度的经典和量子秘密提供了有用的框架.

基于图态的 CQ 方案中的授权者集合需要满足以下可访问性条件.

可访问性: 给定一个图 $G=(V, E)$, 如果存在集合 $B \subseteq V$, 使得 $\exists D \subseteq B$ 满足 $|D|=1 \mod 2$ 且 $\mathrm{Odd}(D) \subseteq B$, 则称该顶点集 B 具有可访问性, 其中 $\mathrm{Odd}(D)=\{v \in V \mid |N(v) \cap D|=1 \mod 2\}$.

基于图态的 CQ 方案是完美的, 未授权集合 (即所有不满足可访问性的集合) 都被证明具有弱奇支配集 (weak odd domination, WOD 集) 性质. WOD 集的约化密度矩阵与秘密无关, 因此任何未授权集合无法获取任何关于秘密的信息.

WOD 集: 当存在 $C \subseteq V \setminus B$, 使得 $B \subseteq \mathrm{Odd}(C)$ 时, 集合 B 是 WOD 集.

在 QQ 方案的情形下, 授权者集合 B 在满足可访问性条件之外, 量子不可克隆原理还额外要求 B 的补集为 WOD 集. 给定一个 n 阶图态 $G=(V, E)$, Gravier 等[149] 给出 QQ 协议如下.

1) 加密. 分发者将量子态秘密 $|\phi\rangle=\alpha|0\rangle+\beta|1\rangle$ 编码为 $|\Psi\rangle=\alpha|G_0\rangle+\beta|G_1\rangle$, 其中 $|G_0\rangle=|G\rangle$, $|G_1\rangle=Z_V|G\rangle$.

2) 分发. 将 $|\Psi\rangle$ 的每个量子比特分发给对应参与者.

3) 量子态秘密重构. 设集合 B 为授权者集合, B 满足可访问性, 且 B 的补集 $V \setminus B$ 为 WOD 集. 即 $\exists C, D \subseteq B$ 使得 $V \setminus B \subseteq \mathrm{Odd}(C)$, $|D|=1 \mod 2$, 且 $\mathrm{Odd}(D) \subseteq B$.

若参与者选择在 $u \in B$ 上恢复秘密, 则集合 $B \setminus \{u\}$ 中每个参与者将自己的量子比特传递给 u. u 额外使用一个辅助量子比特 $(|0\rangle+|1\rangle)/\sqrt{2}$, 与集合 B 中的量子比特一起构成一个 $(|B|+1)$ 个量子比特的系统, 在其上施加酉算符操作 $\frac{1}{\sqrt{2}}\begin{pmatrix} I & U \\ -U & I \end{pmatrix}$, 其中 $U=(-1)^{|G_D|}X_D Z_{\mathrm{Odd}(D)}$, 可以得到 $\alpha|0\rangle \otimes |G_0\rangle+\beta|1\rangle \otimes |G_1\rangle$.

再对其施加酉算符操作 $\begin{pmatrix} I & 0 \\ 0 & U' \end{pmatrix}$, 其中 $U'=(-1)^{|G_C|}X_C Z_{V \setminus \mathrm{Odd}(C)}$, 则有 $(\alpha|0\rangle+\beta|1\rangle) \otimes |G\rangle$, 秘密在第 1 个量子比特上被重建.

与 CQ 方案不同, 基于图态的 QQ 方案通常是不完美的, 即除了满足可访问性的授权者集合外, 存在其他集合可能会携带部分关于秘密的信息, 可以通过向上述协议引入一次一密来构造量子信息的量子秘密共享 (k, n) 门限方案. 分发者随机选择两个经典比特 $p, q \in \{0, 1\}$ 作为一次一密的密钥, 对量子态 $|\phi\rangle=\alpha|0\rangle+\beta|1\rangle$ 施加 $X^p Z^q$ 操作后再利用上述协议对加密后的新量子态 $|\alpha|p\rangle+\beta(-1)^q|1-p\rangle$ 进行共享. 经典比特 p, q 通过经典信息的 (k, n) 门限方案分发给参与者, 确保了仅当授权者集合 B 的大小 $|B| \geqslant k$ 时, 可恢复 p, q, 规模低于门限 k 的参与者集合将无法获得关于秘密的任何信息.

在 3.1 节已表述了由文献所给出的通用 QQ (k, n) 门限方案, 随着参与者数量的增加, 该方案将面临子份额量子态维度无限扩张的问题. 图态方法允许不依赖于参与者数量, 以较低维度的量子比特纯态设计秘密共享方案, 但会存在无法构造所有门限方案的缺陷. 在量子不可克隆原理的基础上, 基于图态的量子秘密共享 (k, n) 门限方案的门限下界进一步改进为 $k>0.506n$. 目前基于图态的量子秘密共享门限方案的构造均会导致准全体一致协议, 即 $k=n-\mathcal{O}(n)$. Gravier 等[149] 通过随机图证明了对于足够大的 n, 高概率性存在图 G 满足 $k \leqslant 0.811n$, 但尚且没有准全体一致协议的显式构造. 判定一个给定图态 G 的门限是否大于一个给定参数被证明是 NP 完全问题, 人们无法有效地验证一个随机生成的图态是否存在一个小的门限.

Bell 等[151] 首次在全光装置上实现了基于图态的量子秘密共享, 制备图态的主要技术手段从利用自发参量下转换源产生的纠缠光子概率性制备[152] 已经发展到利用原子单个记忆自旋发射的一系列单光子的确定性生成[153], 目前已经突破了简单的一维链型和星型图态, 在实验上实现了二维环型和树型图态的融合生成[154]. 基于芯片的光子图态制备也不断取得进展[155]. 虽然目前生成的光子图态规模尚小, 但原则上可以通过量子逻辑门的操作等方式将它们结合在一起扩展形成更大、更复杂的图态. 具有灵活连接性与能够在原子状态中长期储存信息的图态仍有待研究.

3.4 基于连续变量的量子信息秘密共享

2003 年, Lance 等[66] 提出并实验实现了一种基于连续变量的 $(2, 3)$ 门限量子信息秘密共享方案, 并且为区别于共享经典信息的 QSS. 如图 7 所示, 这个协议利用 1 : 1 分束器将一个秘密相干态 $\hat{a}_{\mathrm{in}}$ 与 EPR 对 $\hat{a}_{\mathrm{EPR1}}$ ($\hat{a}_{\mathrm{EPR2}}$) 中的一个进行干涉, 编码成一个三方纠缠. 分发者进一步使用与正交振幅具有相同相关性的高斯白噪声 (Gaussian white noise) $\delta\mathcal{N}$ 对三方纠缠进行调制, 共享的组分变为

$$\hat{a}_1 = (\hat{a}_{\rm in} + \hat{a}_{\rm EPR1} + \delta\mathcal{N})/\sqrt{2}, \tag{15}$$

$$\hat{a}_2 = (\hat{a}_{\rm in} - \hat{a}_{\rm EPR1} - \delta\mathcal{N})/\sqrt{2}, \tag{16}$$

$$\hat{a}_3 = \hat{a}_{\rm EPR2} + \delta\mathcal{N}^*, \tag{17}$$

其中 $\hat{a}_{\rm in} = (\hat{X}^+ + {\rm i}\hat{X}^-)/\sqrt{2}$, (+) 和 (−) 分别表示振幅和相位正交分量, $\delta\mathcal{N} = (\delta\mathcal{N}^+ + {\rm i}\delta\mathcal{N}^-)/2$ 是高斯噪声, $*$ 表示复共轭. 三方纠缠产生之后, 分别分发给 3 个参与者. 秘密重构阶段, 如果是参与者 1 和参与者 2 合作, 则利用 1:1 分束器的马赫-曾德尔干涉仪来重构量子态. 如果是参与者 1 (参与者 2) 和参与者 3 合作, 则利用一个 2:1 分束器和一个电光前馈环来重构量子态, 这个过程会更加复杂[156]. 正如 Lance 的方案中所提到的, 连续变量量子信息秘密共享的实现需要依赖前馈技术. 而前馈技术涉及到光-电和电-光的转换, 这种转换过程限制了量子信息秘密共享的带宽. 因此, 要拓宽量子信息秘密共享的带宽就要避免涉及到这种光与电之间的转换, 去构建全光的量子信息秘密共享体系. 虽然理论上使用相位不敏感放大器 (phase-insensitive amplifier, PIA) 可以避免前馈技术的使用[157], 但是耦合到 PIA 放大输出态的噪声难以直接控制, 一直以来实验实现较为困难. 2023 年, Chen 等[158] 利用基于双 Λ 构型四波混频过程的低噪声 PIA 代替了光电前馈技术, 实现了确定性的 (2, 3) 门限全光量子信息秘密共享, 在 1.4—2.4 MHz 的带宽范围内重构态的保真度均内超过经典极限. 与 Lance 等[66] 不同, Chen 等[158] 方案中重建态的形式与秘密态是相同的, 不需要对重构态进行后验 (posteriori) 就能得到有意义的保真度. 这为全光宽带量子网络的构建提供了一条途径.

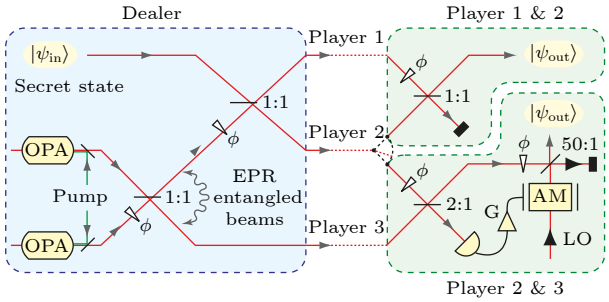


图 7 连续变量 (2, 3) 门限量子信息秘密共享方案示意图[66]

Fig. 7. Schematic of the (2, 3) threshold quantum information secret sharing scheme for continuous variable[66].

3.5 共享纠缠态的量子信息秘密共享

前面所提到的已经实现的一些量子信息秘密共享的方案[66,151,158] 中, 共享的都是纯量子比特态, 纠缠态的共享和恢复仍然没有实现. 2016 年 Lu 等[159] 通过使用一个六光子纠缠态演示了一个 (3, 3) 量子门限方案. 在这个方案中, 共享的保密量子态可以被有效地重建, 并且重建的量子态的保真度能够达到 93%. 如图 8 所示, 分发者将共享的量

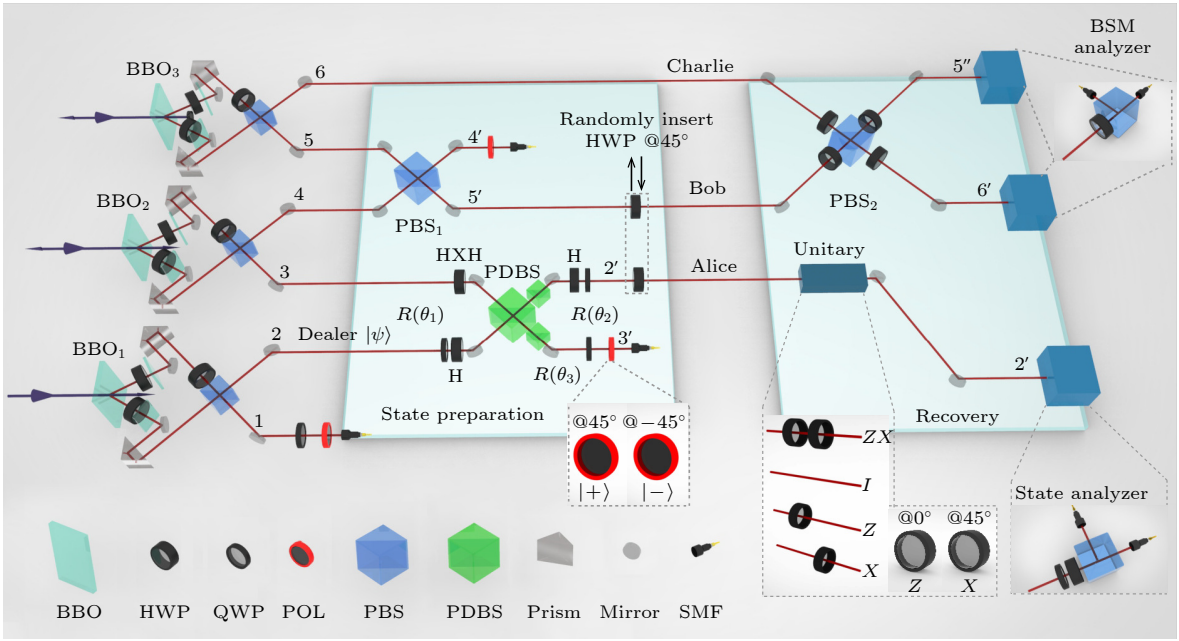


图 8 共享纠缠态的量子信息秘密共享实验装置示意图[159]

Fig. 8. Schematic of the experimental setup for quantum information secret sharing of entangled states[159].

子态 $|\psi\rangle=\alpha|H\rangle+\beta|V\rangle$, 并将其编码在一个三光子混合态中, 然后分发给三位参与者. 当且仅当其中两个参与者在他们的光子上进行 Bell 态测量之后, 第 3 个参与者才能根据他们的测量结果 $\{|\Phi^+\rangle,|\Phi^-\rangle,|\Psi^+\rangle,|\Psi^-\rangle\}$ 对自己的光子施加相应的酉操作 $\{XZ,I,Z,X\}$, 从而恢复 $|\psi\rangle$, 其中 X,Z 是 Pauli 算子, I 是单位算子. Lu 等 [159] 进一步表明, 恢复量子态的纠缠见证 (entanglement witness) $\langle\mathcal{W}\rangle=-0.24\pm0.02<0$, 恢复的量子态仍然与 EPR 对的另一半纠缠在一起, 证明了利用这个方案也可以实现纠缠态的共享和恢复.

3.6 多方量子秘密直接传输

2020 年, Lee 等 [160] 提出了一种多方量子秘密直接传输的 QQ 协议, 并通过一个实验有效验证了他们的量子态传输. 其允许任意数量的分发者将量子态共享给任意数量的接收者, 并且在传输过程中任何一个子方都无法完全访问量子秘密. 协议中 n 名发送者利用 n 粒子 GHZ 态对所共享的量子秘密进行编码, 并和 m 名接收者集合共享一个由 $(n+m)$ 粒子的 GHZ 态作为量子信道, 每名发送方对自己持有的子秘密份额粒子和信道粒子进行分布式 Bell 基测量, 接收方根据所有测量结果在他们持有的 m 个信道粒子上联合施加逻辑泡利操作共同恢复量子态秘密. 去中心化传输无需依赖可信中间节点, 秘密始终由多方进行共享, 避免了单点失效风险, 对量子网络的安全性与容错性有重要意义.

4 总结与展望

二十多年来 QSS 繁荣发展, 表 2 列出了不同类型的 QSS 方案及其特点. 从纠缠态到单光子再到相干光, QSS 不断优化使用的资源, 使其更适配当前的技术水平并更好地兼容电信光纤网络, 增加其实用性. 同时, 环回、MDI 等协议提出也在不断提高着 QSS 的安全性. 但是实用的 QSS 往往面临着安全性问题, 而具有较高安全性的 QSS 又对技术有较高的要求. 迄今为止, 仍然缺乏兼顾实用性和安全性的 QSS 协议. 因此, 找到一个兼具实用性和安全性的 QSS 协议将是未来 QSS 研究的一个重要方向. 值得注意的是, 不论是共享经典信息的 QSS 还是共享量子信息的 QSS, 长久以来都一直受困于传输距离的限制无法远距离传输. 由于量子不可克隆定理, 量子信号无法像经典通信那样直接放大, 量子中继器 [161] 成为实现长距离量子通信的关键技术. 未来, 随着量子中继技术的进一步发展 [114,162,163], 人们不用担心衰减和噪声对通过长光纤发送的量子态的影响, QSS 的距离限制问题将得到解决. 同时量子中继还将为 QSS 提供更灵活的设置. 一方面通过引入中继节点可以构建多点到多点的量子网络, 可以实现动态的参与者选择和调整. 另一方面量子中继器可以缓存部分量子信息,

表 2 不同 QSS 方案的特点

Table 2. Characteristics of different QSS schemes.

QSS方案	特点
使用纠缠态的QSS	由于纠缠特性, 即使光源部分被攻击者控制, 只要测量端能够被完美表征并进行测量错误率即可获得安全的秘密共享. 但目前实验上高效制备纠缠态仍具有较大困难
使用单光子的QSS	相比于纠缠态, 单光子更容易制备和分发, 更具实验性和扩展性. 但仍与目前的通信光纤有适配性差异且容易受到特洛伊木马的攻击
使用相干光的QSS	实验实现简单, 与标准光纤适配更容易实现远距离传输, 具有高稳定性和易操作性. 但相干光存在多光子成分, 无法抵御光子数分裂攻击
离散变量的QSS	利用光子偏振态 $\|H\rangle$ 和 $\|V\rangle$ 或轨道角动量来编码密钥比特, 系统对损耗不敏感、测量和判别精度高. 但信道容量低、单光子制备困难
连续变量的QSS	利用光场的正交分量 $\hat{x}$ 和 $\hat{p}$ 来编码密钥比特, 相比于离散变量可以确定性实现. 但大多数方案要求独立激光源及激光源之间的信号同步, 并且易受到本振攻击
环回QSS	不用监测信号扰动, 密钥率能打破Pirandola-Laurenza-Ottaviani-Banchi界限. 但需要使用可变延迟马赫-曾德尔干涉仪限制了其实际应用
测量设备无关的QSS	能够消除测量端设备不完美带来的攻击风险, 有效增强系统的安全性. 但大多数协议传输效率仍然会随着用户数量的增加呈指数级下降
设备无关的QSS	能够消除所有实际不完美设备的安全漏洞. 但目前协议的性能仍然较低, 尚未有效实现

允许在不同时刻进行量子操作对接, QSS 可以在更宽松的同步条件下运行. 最终能够实现长距离安全实用的 QSS. 此外, 目前提出的 QSS 协议大多是单功能的, 即只能实现 QSS 协议本身, 只有少数协议能在相同硬件实现多种量子密码协议的切换. 要想更进一步地扩展 QSS 的实用性和安全性, 就需要构建具有多功能性和量子加密敏捷性的系统, 实现同一硬件下 QSS 和其他量子密码协议快速切换. QSS 作为多方量子通信的安全保障, 需要在大量用户之间共享秘密信息. 但目前的 QSS 协议大多只进行少数几方的实验演示, 远未达到多方量子通信的要求. 因此扩展 QSS 以容纳更多的用户并在实际通信网络中验证是 QSS 未来发展的一个至关重要的挑战. 在量子信息的秘密共享中, QSS 方案的设计架构很大程度上依赖于多方量子态的纠缠特性, 对于从起初的 GHZ 态到 Bell 态、簇态、W 态、图态等纠缠态的研究与使用为 QSS 方案做出了初步尝试与示范. 对于量子信息的秘密共享而言, 固定的纠缠资源态限制了 QSS 方案的一般性结构拓展, 实验室在制备与储存复杂纠缠态的局限性为量子情形下 QSS 的实际部署造成了很大的障碍. 虽然已经在 GHZ 态、EPR 对、图态等资源上进行了实验演示, 但目前对量子信息 QSS 的研究仍然十分缺乏, 大多数协议仅停留在理论阶段, 实验实现仍然困难. 量子纠错码理论与相关 QSS 方案深刻关联, 期待对于量子纠错码的研究能够为量子信息 QSS 提供更好的见解. 量子信息 QSS 依赖于量子信道的安全分发[133,164], 在随机选择部分粒子作为诱骗粒子进行窃听检测外, 通过部署波长过滤器和光子数分离器可以有效抵御特洛伊木马攻击[165]. 在噪声信道中, 可通过纠缠纯化[166]的方式蒸馏出最大纠缠态来提高量子通信的安全性, 而量子纠错码能够针对光子丢失、操作错误和不诚实参与者等问题进行容错[160,167,168], 提升了协议对噪声的鲁棒性. 但更为具体通用的方案仍待进一步研究. 与此同时, 量子信息的秘密共享作为分布式量子计算的安全基础, 要推动分布式量子计算的发展就需要实现量子信息 QSS 的可行化和实用化. 因此更加可行、高效的量子信息 QSS 协议的提出和实验也将在未来 QSS 的发展中发挥举足轻重的作用. 综上所述, QSS 未来的发展将聚焦在 4 个主要方向: 1) 实用性和安全性; 2) 多功能性和加密敏捷性; 3) 更多方用户和实际通信网络实现; 4) 量子信息 QSS 方案.

在量子时代, CQ-QSS 和 QQ-QSS 将成为高安全性场景的核心工具. 基于 QSS 的多方量子通信作为实现量子多方计算网络的关键要素, 提供了超越经典密码学限制的信息论安全. 虽然目前 QSS 仍然面临着许多挑战, 仍有一系列问题亟待解决. 但大量的研究已经表明 QSS 具有显著优势和广阔的发展前景. 在未来大型量子网络构建和分布式量子计算中, QSS 将发挥着不可替代的作用.

参考文献

[1] Shamir A 1979 *Communications of the ACM* **22** 612
[2] Blakley G R 1979 *Managing Requirements Knowledge, International Workshop on* (IEEE Computer Society) pp313–313
[3] Liao S K, Cai W Q, Liu W Y, et al. 2017 *Nature* **549** 43
[4] Xie Y M, Lu Y S, Weng C X, Cao X Y, Jia Z Y, Bao Y, Wang Y, Fu Y, Yin H L, Chen Z B 2022 *PRX Quantum* **3** 020315
[5] Gu J, Cao X Y, Fu Y, He Z W, Yin Z J, Yin H L, Chen Z B 2022 *Sci. Bull.* **67** 2167
[6] Yin H L, Fu Y, Li C L, Weng C X, Li B H, Gu J, Lu Y S, Huang S, Chen Z B 2023 *Natl. Sci. Rev.* **10** nwac228
[7] Pan D, Long G L, Yin L, Sheng Y B, Ruan D, Ng S X, Lu J, Hanzo L 2024 *IEEE Commun. Surv. Tut.* **26** 1898
[8] Cao X Y, Li B H, Wang Y, Fu Y, Yin H L, Chen Z B 2024 *Sci. Adv.* **10** eadk3258
[9] Jing X, Qian C, Weng C X, Li B H, Chen Z, Wang C Q, Tang J, Gu X W, Kong Y C, Chen T S, Yin H L, Jiang D, Niu B, Lu L L 2024 *Sci. Adv.* **10** eadp2877
[10] Du Y, Li B H, Hua X, Cao X Y, Zhao Z, Xie F, Zhang Z, Yin H L, Xiao X, Wei K 2025 *Light: Sci. Appl.* **14** 108
[11] Hillery M, Bužek V, Berthiaume A 1999 *Phys. Rev. A* **59** 1829
[12] Cleve R, Gottesman D, Lo H K 1999 *Phys. Rev. Lett.* **83** 648
[13] Markham D, Sanders B C 2008 *Phys. Rev. A* **78** 042309
[14] Qin S J, Gao F, Wen Q Y, Zhu F C 2007 *Phys. Rev. A* **76** 062324
[15] Chen Y A, Zhang A N, Zhao Z, Zhou X Q, Lu C Y, Peng C Z, Yang T, Pan J W 2005 *Phys. Rev. Lett.* **95** 200502
[16] Tittel W, Zbinden H, Gisin N 2001 *Phys. Rev. A* **63** 042301
[17] Karlsson A, Koashi M, Imoto N 1999 *Phys. Rev. A* **59** 162
[18] Zhang Z J, Gao G, Wang X, Han L F, Shi S H 2007 *Opt. Commun.* **269** 418
[19] Williams B P, Lukens J M, Peters N A, Qi B, Grice W P 2019 *Phys. Rev. A* **99** 062311
[20] Sen A, Sen U, Żukowski M 2003 *Phys. Rev. A* **68** 032309
[21] Gaertner S, Bourennane M, Eibl M, Kurtsiefer C, Weinfurter H 2003 *Appl. Phys. B* **77** 803
[22] Gaertner S, Kurtsiefer C, Bourennane M, Weinfurter H 2007 *Phys. Rev. Lett.* **98** 020503
[23] Yu I C, Lin F L, Huang C Y 2008 *Phys. Rev. A* **78** 012344
[24] Xiao L, Lu Long G, Deng F G, Pan J W 2004 *Phys. Rev. A* **69** 052307
[25] Xiao Y R, Jia Z Y, Song Y C, Bao Y, Fu Y, Yin H L, Chen Z B 2024 *Opt. Lett.* **49** 4210
[26] Ishio H, Minowa J, Nosu K 1984 *J. Lightwave Technol.* **2**

448
[27] Wengerowsky S, Joshi S K, Steinlechner F, Hübel H, Ursin R 2018 *Nature* **564** 225
[28] Bouwmeester D, Pan J W, Daniell M, Weinfurter H, Zeilinger A 1999 *Phys. Rev. Lett.* **82** 1345
[29] Pan J W, Daniell M, Gasparoni S, Weihs G, Zeilinger A 2001 *Phys. Rev. Lett.* **86** 4435
[30] Zhao Z, Yang T, Chen Y A, Zhang A N, Żukowski M, Pan J W 2003 *Phys. Rev. Lett.* **91** 180401
[31] Huang Y F, Liu B H, Peng L, Li Y H, Li L, Li C F, Guo G C 2011 *Nat. Commun.* **2** 546
[32] Pan J W, Chen Z B, Lu C Y, Weinfurter H, Zeilinger A, Żukowski M 2012 *Rev. Mod. Phys.* **84** 777
[33] Gisin N 2015 *Front. Phys.* **10** 100307
[34] Guo G P, Guo G C 2003 *Phys. Lett. A* **310** 247
[35] Deng F G, Zhou H Y, Long G L 2005 *Phys. Lett. A* **337** 329
[36] Han L F, Liu Y M, Liu J, Zhang Z J 2008 *Opt. Commun.* **281** 2690
[37] Wang T Y, Wen Q Y 2011 *Quantum Inf. Comput.* **11** 434
[38] Schmid C, Trojek P, Bourennane M, Kurtsiefer C, Żukowski M, Weinfurter H 2005 *Phys. Rev. Lett.* **95** 230505
[39] Bogdanski J, Ahrens J, Bourennane M 2009 *Opt. Express* **17** 1055
[40] Kuzin E, Nunez H C, Korneev N 1999 *Opt. Commun.* **160** 37
[41] Ma H Q, Wei K J, Yang J H 2013 *Opt. Lett.* **38** 4494
[42] Deng F G, Li X H, Zhou H Y, Zhang Z j 2005 *Phys. Rev. A* **72** 044302
[43] He G P 2007 *Phys. Rev. Lett.* **98** 028901
[44] Lucamarini M, Choi I, Ward M B, Dynes J F, Yuan Z, Shields A J 2015 *Phys. Rev. X* **5** 031030
[45] Tavakoli A, Herbauts I, Żukowski M, Bourennane M 2015 *Phys. Rev. A* **92** 030302
[46] Shen Y J, Wang X J, Xie Z W, Min C J, Fu X, Liu Q, Gong M L, Yuan X C 2019 *Light Sci. Appl.* **8** 90
[47] Bliokh K Y, Rodríguez-Fortuño F J, Nori F, Zayats A V 2015 *Nat. Photonics* **9** 796
[48] Pinnell J, Nape I, de Oliveira M, TabeBordbar N, Forbes A 2020 *Laser Photon. Rev.* **14** 2000012
[49] Smania M, Elhassan A M, Tavakoli A, Bourennane M 2016 *npj Quantum Inf.* **2** 16010
[50] Brassard G, Lütkenhaus N, Mor T, Sanders B C 2000 *Phys. Rev. Lett.* **85** 1330
[51] Lütkenhaus N, Jahma M 2002 *New J. Phys.* **4** 44
[52] Hwang W Y 2003 *Phys. Rev. Lett.* **91** 057901
[53] Wang X B 2005 *Phys. Rev. Lett.* **94** 230503
[54] Lo H K, Ma X, Chen K 2005 *Phys. Rev. Lett.* **94** 230504
[55] Inoue K, Waks E, Yamamoto Y 2003 *Phys. Rev. A* **68** 022317
[56] Inoue K, Ohashi T, Kukita T, Watanabe K, Hayashi S, Honjo T, Takesue H 2008 *Opt. Express* **16** 15469
[57] Gu J, Cao X Y, Yin H L, Chen Z B 2021 *Opt. Express* **29** 9165
[58] Lucamarini M, Yuan Z L, Dynes J F, Shields A J 2018 *Nature* **557** 400
[59] Curty M, Azuma K, Lo H K 2019 *npj Quantum Inf.* **5** 64
[60] Yin H L, Chen Z B 2019 *Sci. Rep.* **9** 17113
[61] Fröhlich B, Lucamarini M, Dynes J F, Comandar L C, Tam W W S, Plews A, Sharpe A W, Yuan Z, Shields A J 2017 *Optica* **4** 163
[62] Shen A, Cao X Y, Wang Y, Fu Y, Gu J, Liu W B, Weng C X, Yin H L, Chen Z B 2023 *Sci. China Phys. Mech. Astron.* **66** 260311
[63] Wang Y Z, Sun X R, Cao X Y, Yin H L, Chen Z B 2024 *Phys. Rev. Appl.* **22** 044018
[64] Grosshans F, Grangier P 2002 *Phys. Rev. Lett.* **88** 057902
[65] Tyc T, Sanders B C 2002 *Phys. Rev. A* **65** 042310
[66] Lance A M, Symul T, Bowen W P, Sanders B C, Lam P K 2004 *Phys. Rev. Lett.* **92** 177903
[67] Kogias I, Xiang Y, He Q, Adesso G 2017 *Phys. Rev. A* **95** 012315
[68] Zhou Y Y, Yu J, Yan Z H, Jia X J, Zhang J, Xie C D, Peng K C 2018 *Phys. Rev. Lett.* **121** 150502
[69] Horodecki M, Horodecki P, Horodecki R 1998 *Phys. Rev. Lett.* **80** 5239
[70] Shor P W, Smolin J A, Thapliyal A V 2003 *Phys. Rev. Lett.* **90** 107901
[71] Jia X J, Zhang J, Wang Y, Zhao Y P, Xie C D, Peng K C 2012 *Phys. Rev. Lett.* **108** 190501
[72] Lau H K, Weedbrook C 2013 *Phys. Rev. A* **88** 042313
[73] Wu Y D, Zhou J, Gong X B, Guo Y, Zhang Z M, He G Q 2016 *Phys. Rev. A* **93** 022325
[74] Walk N, Eisert J 2021 *PRX Quantum* **2** 040339
[75] Grice W P, Qi B 2019 *Phys. Rev. A* **100** 022339
[76] Wu X D, Wang Y J, Huang D 2020 *Phys. Rev. A* **101** 022301
[77] Liao Q, Liu H J, Zhu L, Guo Y 2021 *Phys. Rev. A* **103** 032410
[78] Liao Q, Liu X Q, Ou B, Fu X Q 2023 *IEEE Trans. Commun.* **71** 6051
[79] Liao Q, Liu H J, Gong Y P, Wang Z, Peng Q Q, Guo Y 2022 *Opt. Express* **30** 3876
[80] Huang D, Huang P, Wang T, Li H, Zhou Y, Zeng G 2016 *Phys. Rev. A* **94** 032305
[81] Liao Q, Fei Z, Huang L, Fu X 2025 *Commun. Phys.* **8** 138
[82] Shen Y, Zou H, Tian L, Chen P, Yuan J 2010 *Phys. Rev. A* **82** 022317
[83] Liu S, Lu Z, Wang P, Tian Y, Wang X, Li Y 2023 *npj Quantum Inf.* **9** 92
[84] Murta G, Grasselli F, Kampermann H, Bruß D 2020 *Adv. Quantum Technol.* **3** 2000025
[85] Cao X Y, Gu J, Lu Y S, Yin H L, Chen Z B 2021 *New J. Phys.* **23** 043002
[86] Proietti M, Ho J, Grasselli F, Barrow P, Malik M, Fedrizzi A 2021 *Sci. Adv.* **7** eabe0395
[87] Richter S, Thornton M, Khan I, Scott H, Jaksch K, Vogl U, Stiller B, Leuchs G, Marquardt C, Korolkova N 2021 *Phys. Rev. X* **11** 011038
[88] Zhang Y F, Liu W B, Li B H, Yin H L, Chen Z B 2024 *Phys. Rev. A* **110** 052613
[89] Diamanti E, Leverrier A 2015 *Entropy* **17** 6072
[90] Liu W B, Li C L, Xie Y M, Weng C X, Gu J, Cao X Y, Lu Y S, Li B H, Yin H L, Chen Z B 2021 *PRX Quantum* **2** 40334
[91] Li S G, Li C L, Liu W B, Yin H L, Chen Z B 2024 *Adv. Quantum Technol.* **7** 2400140
[92] Gu J, Xie Y M, Liu W B, Fu Y, Yin H L, Chen Z B 2021 *Opt. Express* **29** 32244
[93] Sasaki T, Yamamoto Y, Koashi M 2014 *Nature* **509** 475
[94] Pirandola S, Laurenza R, Ottaviani C, Banchi L 2017 *Nat. Commun.* **8** 15043
[95] Lydersen L, Wiechers C, Wittmann C, Elser D, Skaar J, Makarov V 2010 *Nat. Photonics* **4** 686
[96] Makarov V 2009 *New J. Phys.* **11** 065003
[97] Qin H, Kumar R, Makarov V, Alléaume R 2018 *Phys. Rev. A* **98** 012312
[98] Qi B, Fung C H F, Lo H K, Ma X 2007 *Quantum Inf.*

Comput. **7** 073
[99] Huang J Z, Weedbrook C, Yin Z Q, Wang S, Li H W, Chen W, Guo G C, Han Z F 2013 *Phys. Rev. A* **87** 062329
[100] Wei K, Zhang W, Tang Y L, You L, Xu F 2019 *Phys. Rev. A* **100** 022325
[101] Qin H, Kumar R, Alléaume R 2016 *Phys. Rev. A* **94** 012325
[102] Xu F, Ma X, Zhang Q, Lo H K, Pan J W 2020 *Rev. Mod. Phys.* **92** 025002
[103] Lo H K, Curty M, Qi B 2012 *Phys. Rev. Lett.* **108** 130503
[104] Fu Y, Yin H L, Chen T Y, Chen Z B 2015 *Phys. Rev. Lett.* **114** 090501
[105] Ma X, Qi B, Zhao Y, Lo H K 2005 *Phys. Rev. A* **72** 012326
[106] Gao Z, Li T, Li Z 2020 *Sci. China Phys. Mech. Astron.* **63** 120311
[107] Yang Y G, Wang Y C, Yang Y L, Chen X B, Li D, Zhou Y H, Shi W M 2021 *Sci. China Phys. Mech. Astron.* **64** 260321
[108] Liu T, Lai J, Li Z, Li T 2025 *Phys. Rev. Appl.* **23** 034057
[109] Zhang C, Zhang Q, Zhong W, Du M M, Shen S T, Li X Y, Zhang A L, Zhou L, Sheng Y B 2025 *Phys. Rev. A* **111** 012602
[110] Liao Q, Huang L, Fei Z Y, Fu X Q 2025 *Adv. Quantum Technol.* **8** 2400505
[111] Wang Y, Tian C, Su Q, Wang M, Su X 2019 *Science China Information Sciences* **62** 72501
[112] Li C L, Fu Y, Liu W B, Xie Y M, Li B H, Zhou M G, Yin H L, Chen Z B 2023 *Phys. Rev. Res.* **5** 033077
[113] Azuma K, Tamaki K, Lo H K 2015 *Nat. Commun.* **6** 6787
[114] Azuma K, Tamaki K, Munro W J 2015 *Nat. Commun.* **6** 10171
[115] Roy S, Mukhopadhyay S 2019 *Phys. Rev. A* **100** 012319
[116] Zhang Q, Zhong W, Du M M, Shen S T, Li X Y, Zhang A L, Zhou L, Sheng Y B 2024 *Phys. Rev. A* **110** 042403
[117] Zhang Q, Ying J W, Wang Z J, Zhong W, Du M M, Shen S T, Li X Y, Zhang A L, Gu S P, Wang X F, et al. 2025 *Phys. Rev. A* **111** 012603
[118] Zhang Z, Yuan C, Shen S, Yu H, Zhang R, Wang H, Li H, Wang Y, Deng G, Wang Z, et al. 2021 *npj Quantum Inf.* **7** 123
[119] Chen X, Fu Z, Gong Q, Wang J 2021 *Adv. Photon.* **3** 064002
[120] Chopin A, Barone A, Ghorbel I, Combrié S, Bajoni D, Raineri F, Galli M, De Rossi A 2023 *Commun. Phys.* **6** 77
[121] Chen S, Peng L C, Guo Y P, Gu X M, Ding X, Liu R Z, Zhao J Y, You X, Qin J, Wang Y F, et al. 2024 *Phys. Rev. Lett.* **132** 130603
[122] Huang J, Mao J, Li X, Yuan J, Zheng Y, Zhai C, Dai T, Fu Z, Bao J, Yang Y, et al. 2025 *Nat. Photonics* **19** 471
[123] Nemirovsky-Levy L, Pereg U, Segev M 2024 *Optica Quantum* **2** 165
[124] Yan P S, Zhou L, Zhong W, Sheng Y B 2023 *Sci. China Phys. Mech. Astron.* **66** 250301
[125] Hu X M, Huang C X, Sheng Y B, Zhou L, Liu B H, Guo Y, Zhang C, Xing W B, Huang Y F, Li C F, et al. 2021 *Phys. Rev. Lett.* **126** 010503
[126] Bennett C H, Brassard G, Crépeau C, Jozsa R, Peres A, Wootters W K 1993 *Phys. Rev. Lett.* **70** 1895
[127] Senthoor K, Sarvepalli P K 2022 *IEEE Transactions on Information Theory* **68** 3164
[128] Yang Y G, Wang Y, Chai H P, Teng Y W, Zhang H 2011 *Opt. Commun.* **284** 3479
[129] Jia H Y, Wen Q Y, Gao F, Qin S J, Guo F Z 2012 *Phys. Lett. A* **376** 1035
[130] Sun Y, Xu S W, Chen X B, Niu X X, Yang Y X 2013 *Quantum Inf. Process.* **12** 2877
[131] Li Y, Zhang K, Peng K 2004 *Phys. Lett. A* **324** 420
[132] Deng F G, Li X H, Li C Y, Zhou P, Zhou H Y 2005 *Phys. Rev. A* **72** 044301
[133] Deng F G, Li X H, Li C Y, Zhou P, Zhou H Y 2006 *Eur. Phys. J. D* **39** 459
[134] Yuan H, Liu Y M, Zhang W, Zhang Z J 2008 *J. Phys. B* **41** 145506
[135] Shi R H, Huang L S, Yang W, Zhong H 2011 *Quantum Inf. Process.* **10** 231
[136] Pathak A, Banerjee A 2011 *Int. J. Quantum Inf.* **09** 389
[137] Muralidharan S, Panigrahi P K 2008 *Phys. Rev. A* **78** 062333
[138] Nie Y Y, Li Y H, Liu J C, Sang M H 2011 *Opt. Commun.* **284** 1457
[139] Roos C F, Riebe M, Häffner H, Hänsel W, Benhelm J, Lancaster G P T, Becher C, Schmidt-Kaler F, Blatt R 2004 *Science* **304** 1478
[140] Agrawal P, Pati A 2006 *Phys. Rev. A* **74** 062320
[141] Gottesman D 2000 *Phys. Rev. A* **61** 42311
[142] Wang X W, Xia L X, Wang Z Y, Zhang D Y 2010 *Opt. Commun.* **283** 1196
[143] Wang X W, Zhang D Y, Tang S Q, Zhan X G, You K M 2010 *Int. J. Theor. Phys.* **49** 2691
[144] Wang X W, Zhang D Y, Tang S Q, Xie L J 2011 *J. Phys. B* **44** 35505
[145] Shukla C, Pathak A 2013 *Phys. Lett. A* **377** 1337
[146] Chandran L S, Gajjala R 2024 *Quantum* **8** 1396
[147] Kashefi E, Markham D, Mhalla M, Perdrix S 2009 *Electronic Proceedings in Theoretical Computer Science* **9** 87
[148] Javelle J, Mhalla M, Perdrix S 2013 *New Protocols and Lower Bounds for Quantum Secret Sharing with Graph States* (Springer Berlin Heidelberg) pp1–12
[149] Gravier S, Javelle J, Mhalla M, Perdrix S 2013 In Hutchison D, Kanade T, Kittler J, Kleinberg J M, Mattern F, Mitchell J C, Naor M, Nierstrasz O, Pandu Rangan C, Steffen B, Sudan M, Terzopoulos D, Tygar D, Vardi M Y, Weikum G, Kučera A, Henzinger T A, Nešetřil J, Vojnar T, Antoš D, editors. *Mathematical and Engineering Methods in Computer Science*, Vol. 7721 (Berlin, Heidelberg: Springer Berlin Heidelberg) pp15–31
[150] Keet A, Fortescue B, Markham D, Sanders B C 2010 *Phys. Rev. A* **82** 62315
[151] Bell B A, Markham D, Herrera-Martí D A, Marin A, Wadsworth W J, Rarity J G, Tame M S 2014 *Nat. Commun.* **5** 5480
[152] Bell B A, Herrera-Martí D A, Tame M S, Markham D, Wadsworth W J, Rarity J G 2014 *Nat. Commun.* **5** 3658
[153] Cooper E S, Kunkel P, Periwal A, Schleier-Smith M 2024 *Nat. Phys.* **20** 770
[154] Thomas P, Ruscio L, Morin O, Rempe G 2024 *Nature* **629** 567
[155] Huang J, Chen X, Li X, Wang J 2023 *AAPPS Bulletin* **33** 14
[156] Lance A M, Symul T, Bowen W P, Tyc T, Sanders B C, Lam P K 2003 *New J. Phys.* **5** 4
[157] Lance A M, Symul T, Bowen W P, Sanders B C, Tyc T, Ralph T C, Lam P K 2005 *Phys. Rev. A* **71** 033814
[158] Chen Y, Zhu Q, Wang X, Lou Y, Liu S, Jing J 2023 *Adv. Photon.* **5** 026006
[159] Lu H, Zhang Z, Chen L K, Li Z D, Liu C, Li L, Liu N L, Ma X, Chen Y A, Pan J W 2016 *Phys. Rev. Lett.* **117** 030501
[160] Lee S M, Lee S W, Jeong H, Park H S 2020 *Phys. Rev. Lett.* **124** 060501

[161] Briegel H J, Dür W, Cirac J I, Zoller P 1998 *Phys. Rev. Lett.* **81** 5932
[162] Azuma K, Economou S E, Elkouss D, Hilaire P, Jiang L, Lo H K, Tzitrin I 2023 *Rev. Mod. Phys.* **95** 045006
[163] Li C L, Yin H L, Chen Z B 2024 *Rep. Prog. Phys.* **87** 127901
[164] Deng F G, Long G L, Liu X S 2003 *Phys. Rev. A* **68** 42317
[165] Tian Y, Wang J L, Bian G Q, Chang J Y, Li J 2024 *Adv. Quantum. Tech.* **7** 2400116
[166] Deutsch D, Ekert A, Jozsa R, Macchiavello C, Popescu S, Sanpera A 1996 *Phys. Rev. Lett.* **77** 2818
[167] And A 2012 *Commun. Theor. Phys.* **58** 661
[168] Gupta S, Sinha A, Pandey S K 2024 *Quantum Inf. Process.* **23** 58

SPECIAL TOPIC—Quantum information processing

Research status and prospects of quantum secret sharing*

YIN Hualei [1)#†] SHEN Jianyu [2)#] CHEN Nuo [2)#] CHEN Zengbing [2)]

1) (*School of Physics, Renmin University of China, Beijing* 100872, *China*)

2) (*School of Physics, Nanjing University, Nanjing* 210093, *China*)

(Received 30 April 2025; revised manuscript received 24 June 2025)

Abstract

Quantum secret sharing (QSS), as a quantum extension of classical secret sharing, uses the basic principles of quantum mechanics to share information safely among multiple parties, providing a new paradigm for information security. As a key foundation for secure multiparty quantum communication and distributed quantum computing, QSS has attracted considerable attention since its emergence. Currently, research in this field includes both classical and quantum scenarios, and continuous progress has been made in both theoretical and experimental aspects. This paper first reviews the current development of QSS for classical information. In this regard, significant and parallel progress has been made in both discrete-variable QSS and continuous-variable QSS. The QSS protocols for sharing classical information, from entangled states to single photons and then to coherent light, have been continuously optimized to better utilize available resources and achieve more efficient implementation under current technological conditions. Meanwhile, round-robin, measurement-device-independent, and other protocols have been steadily improving the security of QSS. Next, one will focus on QSS scheme for quantum secrets, which begins with the symmetry of access structures and introduces basic (k, n) threshold protocols, dynamic schemes that support adaptive agent groups, and symmetric quantum information splitting through entanglement. It further introduces hierarchical quantum secret sharing schemes for asymmetric splitting of quantum information. Considering practical laboratory conditions of quantum states as resources, an overall discussion is conducted on quantum secret sharing with graph states. Afterwards, the design of a continuous-variable scheme for quantum secret sharing is outlined, and entanglement state sharing and quantum teleportation between multiple senders and receivers are introduced. Finally, this review discusses and outlines the future development directions of QSS, thereby inspiring readers to further study and explore the relevant subjects.

Keywords: quantum secret sharing, quantum communication, quantum entanglement, multiparty quantum protocols

PACS: 03.67.–a, 03.67.Dd, 03.67.Hk **DOI:** 10.7498/aps.74.20250586

CSTR: 32037.14.aps.74.20250586

* Project supported by the National Natural Science Foundation of China (Grant No. 12274223).

# These authors contributed equally.

† Corresponding author. E-mail: hlyin@ruc.edu.cn

专题: 量子信息处理

量子多模下的非局域量子纠缠制备研究进展*

李涛[1)†] 王雪琦[1)] 解志浩[1)2)‡]

1) (南京理工大学物理学院, 江苏省半导体器件光电混合集成研究中心, 南京 210094)

2) (南京大学现代工程与应用科学学院, 微结构国家实验室, 南京 210023)

(2025 年 5 月 1 日收到; 2025 年 5 月 26 日收到修改稿)

非局域量子纠缠是未来量子网络的一种核心资源. 局域产生的量子纠缠在通过量子信道传输时呈现指数衰减的分发效率, 大幅降低了量子网络节点之间生成非局域量子纠缠的效率. 该问题在涉及多对非局域量子纠缠的实际量子技术中将进一步加剧. 空间多模、时间多模以及频率多模等经典多模技术在一定程度上加快了非局域量子纠缠的生成速率, 但并未提升单次信道传输效率. 量子多模技术基于单光子的高维编码, 能够在一次量子信道传输中, 在量子网络节点间同时生成多对非局域量子纠缠. 因此, 量子多模有望提升涉及多对非局域量子纠缠的实际量子技术的性能. 本文介绍了基于量子多模的非局域量子纠缠生成机制, 讨论基于高维单光子传输和高维双光子纠缠分发的量子多模技术在实现非局域量子纠缠中的特点, 分析量子多模在加速非局域量子逻辑纠缠生成中的应用, 并展望其在构建大规模量子网络中的潜在优势.

关键词: 量子网络, 量子多模, 高维光子, 并行量子纠缠

PACS: 03.67.Dd, 03.65.Ud, 03.67.Hk **DOI:** 10.7498/aps.74.20250589

CSTR: 32037.14.aps.74.20250589

1 引 言

量子网络是经典通信网络的量子化对应, 由量子网络节点和量子信道组成[1–3]. 量子网络节点之间的非局域量子纠缠不仅可以用于研究量子力学的基本问题, 还可以应用于各类量子信息技术, 如量子通信、分布式量子计算和分布式量子传感等[3]. 基于纠缠的量子直接通信改变了保密通信框图, 实现了无密码、无密文和无泄漏的量子保密通信[4–14]. 模块化的分布式量子计算可以在快速增加量子计算规模的同时, 消除量子比特之间的串扰[15–21]. 分布式量子传感利用非局域量子纠缠, 在时间同步等领域展现出前所未有的精度[22–27].

生成量子网络节点之间的非局域量子纠缠是实现未来量子网络的关键要求. 目前主要有三类方法制备非局域静态量子比特之间的量子纠缠[28]: 1) 在一个量子节点内生成静态量子比特与光量子比特之间的杂化纠缠[29], 将光量子比特传输到另一个节点与其内静态量子比特作用, 生成非局域纠缠[30–34]; 2) 在两节点各生成一对杂化纠缠, 将两光子传到中间节点进行贝尔态分析, 基于纠缠转移生成目标非局域纠缠[35–38]; 3) 在中间节点生成双光子纠缠[39,40], 将两个光子分别传输到两节点并与静态比特相互作用, 基于量子存储生成目标非局域纠缠[41–47]. 这些方法均受限于光量子比特在量子信道传输中的指数衰减, 限制了纠缠节点之间的距离[3].

基于纠缠蒸馏[48]和纠缠转移[49–51]的量子中继技术可大幅降低信道损耗的影响[30,52,53], 有望实现

* 国家自然科学基金 (批准号: 11904171) 资助的课题.

† 通信作者. E-mail: tao.li@njust.edu.cn

‡ 通信作者. E-mail: zhihaoxie@smail.nju.edu.cn

千公里非局域纠缠. 此外, 引入经典多模技术, 可以使两节点间生成非局域纠缠的效率线性增加[30–32]. 例如, 使用频率多模技术[54], 在节点内同时生成 N 对不同频光子与静态比特的杂化纠缠, 并将所有光子发送给中间节点, 则在中间节点贝尔态分析的效率增加约 N 倍, 从而提升生成单对非局域纠缠的效率. 时间多模和空间多模也可实现类似增强[55–58]. 在光纤量子信道中, 空间多模往往转化为时间多模以节省光纤信道的利用率[58].

量子多模基于单光子高维编码[59–63]加速非局域纠缠生成[64], 可利用单光子传输在两个量子网络节点之间同时生成多对非局域纠缠. 量子多模非局域纠缠生成方法可分为三类, 且每类与无多模的非局域纠缠生成方法对应. 量子多模的核心在于高维编码单光子与多静态比特之间的相互作用[65]. 生成高维单光子与多静态比特间杂化纠缠是前两类方法的前提, 后续调控高维光子态及其与多静态比特相互作用, 可生成多对非局域纠缠[66,67]. 利用高维光子纠缠分发并结合光子态调控, 也可将高维光子纠缠[68]转化为多对静态比特之间的纠缠, 构成第三类方法[69]. 目前量子多模主要利用时间仓模式 (time-bin mode) 高维编码[70–72]. 基于高维单光子传输, 不仅可同时生成多对贝尔纠缠, 还可同时生成多体纠缠态[66], 甚至生成非局域逻辑比特纠缠[73]. 基于高维双光子纠缠分发, 量子多模方法可以同时生成多对非局域纠缠, 并与经典空间多模[30–32]相结合, 进一步加快非局域量子纠缠的生成效率, 用于研究超越线性架构的多量子比特节点量子网络[1,74–76].

2 原子腔耦合系统单光子散射与控制极化翻转单元

一个高效的单光子与单个静态物理量子比特之间的相互作用接口可以通过将天然或人工原子耦合到单边光学腔来实现[77–80]. 在弱入射光场极限下, 原子与光学腔耦合系统的反射系数可以描述为[81]

$$r_{\rm s}(\omega)=1-\frac{2\beta(i\Delta_{\rm s}+1)}{(i\Delta_{\rm s}+1)(i\Delta_{\rm c}+1)+C}, \tag{1}$$

式中, $\Delta_{\rm s}=2(\omega_{\rm s}-\omega)/\gamma$ 是原子偶极跃迁频率 $\omega_{\rm s}$ 与输入光场频率 ω 之间的有效失谐; $\Delta_{\rm c}=2(\omega_{\rm c}-\omega)/\kappa$ 是腔模频率 $\omega_{\rm c}$ 与输入光场频率 ω 之间的有效失谐; $C=4g^2/\kappa\gamma$ 是偶极-腔耦合系统的协同参数, 其中 g 表示原子与腔的耦合速率, $\kappa=\kappa_{\rm c}+\kappa_{\rm l}$ 是腔的总损耗, γ 是原子激发态衰减速率; $\beta=\kappa_{\rm c}/\kappa$ 是将散射光子耦合到输出模式的概率. 当输入光的频率和极化同时与原子跃迁匹配时, 反射系数将表现出特征行为, 可以与输入光的频率或极化不匹配时的行为区分开来. 这种量子态依赖的散射可以用于实现单光子与单个固态自旋之间的确定性相互作用[77].

考虑与单边纳米腔耦合的带负电硅空位 (SiV^-) 色心的偶极跃迁. 金刚石 SiV^- 色心由一个居于晶格间隙的硅原子和两个邻近的碳空位构成[82], 如图 1(a) 所示. 相关能级包括两个电子自旋基态 (即 $|g\rangle$ 和 $|e\rangle$) 和两个激发态 (即 $|g'\rangle$ 和 $|e'\rangle$), 如图 1(b) 所示. 在 737 nm 附近存在两个线性 H 极化偶极跃迁, 频率分别为 $\omega_{\rm g}$ 和 $\omega_{\rm e}=\omega_{\rm g}+\Delta$[83]. 为了实现单光子与单个自旋之间的状态依赖散射, 沿 SiV^- 对称轴施加强磁场调控出大的失谐 Δ, 输入 H 极化光子的频率为 $\omega\approx\omega_{\rm g}$. 此时, 电子自旋状态 $|g\rangle$ ($|e\rangle$) 对应的入射光子将以单位振幅和相位移动 0(π) 散射[66,83].

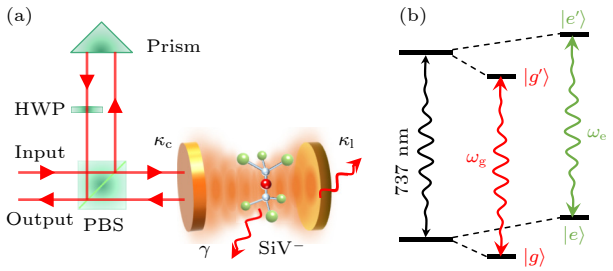


图 1 (a) 受控极化翻转单元示意图; (b) SiV^- 色心的相关能级图和光学跃迁[73]

Fig. 1. (a) Schematic of a controlled-polarization-flip unit; (b) relevant energy levels and optical transitions of a SiV^- color center[73].

通过组合一个 SiV^- 色心与纳米腔耦合系统、一个反射棱镜和一个偏振分束器 (PBS), 可以直接扩展成一个受控极化翻转 (CPF) 单元[73]. PBS 反射 V 极化并透射 H 极化光子模式. 当自旋状态为 $|e\rangle$ 时, CPF 单元翻转光子极化; 当自旋状态为 $|g\rangle$ 时, CPF 单元保持光子极化不变. 在实际散射过程中, SiV^- 与腔耦合系统不可避免地会引入损耗, 降低 H 极化模式中光子的振幅. 为了消除其对 CPF 单元保真度的影响, 可以在 V 极化路径中引入一个可调滤波器以平衡两种模式的振幅. 该滤波器可

以通过调节半波片 (HWP) 的轴向取向与 PBS 组合实现[73]. 在不引起混淆的情况下, 为简化符号表示, 将 CPF 单元简称为与单边腔耦合的对应 SiV^- 电子自旋或 QM.

3 基于极化和时间仓光量子比特编码的两对非局域量子纠缠态制备

2019 年, Piparo 等[64] 首次将量子多模引入非局域量子纠缠态制备, 提出了基于极化和时间仓光量子比特编码的两对非局域量子纠缠态制备方案, 如图 2 所示. $\mathcal{T}$ 表示为光子引入一个时间延迟; H 为半波片, 翻转光子极化状态 $|A\rangle \leftrightarrow |D\rangle$; $\mathrm{PBS_i}$ 表示极化分束器, 透过极化状态为 $|D\rangle$ 的光子并反射极化状态为 $|A\rangle$ 的光子; OS 为光学开关, 实现对光子不同时间仓态的空间输出模式调控. 在理想情况下, 光子与一个电子自旋比特 QM 相互作用后, 系统的量子态演化如下:

$$\begin{aligned} &|g\rangle|D\rangle \to |g\rangle|D\rangle, \quad |g\rangle|A\rangle \to |g\rangle|A\rangle, \\ &|e\rangle|D\rangle \to |e\rangle|A\rangle, \quad |e\rangle|A\rangle \to |e\rangle|D\rangle, \end{aligned} \tag{2}$$

其中 $|D\rangle = (|H\rangle + |V\rangle)/\sqrt{2}$, $|A\rangle = (|H\rangle - |V\rangle)/\sqrt{2}$.

当入射光子初态为 $|D\rangle$, QM 初态为 $|\Psi\rangle_{\mathrm{in}} = (|g\rangle + |e\rangle)/\sqrt{2}$ 时, 光子与 QM1 相互作用后, 进入光子态调控单元 PSE ($|A_{\mathrm{S}}\rangle \to |D_{\mathrm{L}}\rangle$). 系统演化为

$$|S_1\rangle = \frac{1}{\sqrt{2}}(|g_1\rangle|D_{\mathrm{S}}\rangle + |e_1\rangle|D_{\mathrm{L}}\rangle), \tag{3}$$

其中下标 S 和 L 分别表示短时间仓和长时间仓. 随后, 光子与 QM3 相互作用, 生成光子极化和时间仓量子比特与两个 QM 之间的杂化纠缠态:

$$\begin{aligned} |S_2\rangle = \frac{1}{2}(&|g_1\rangle|g_3\rangle|D_{\mathrm{S}}\rangle + |g_1\rangle|e_3\rangle|A_{\mathrm{S}}\rangle \\ &+ |e_1\rangle|g_3\rangle|D_{\mathrm{L}}\rangle + |e_1\rangle|e_3\rangle|A_{\mathrm{L}}\rangle). \end{aligned} \tag{4}$$

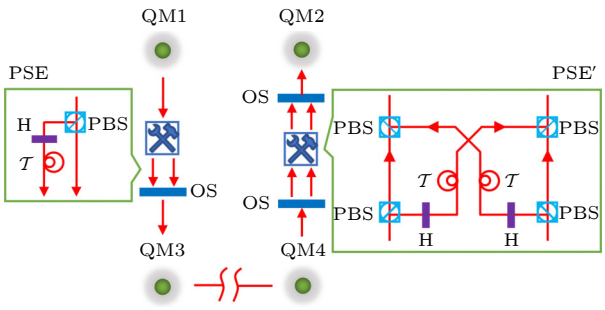


图 2 两对非局域量子纠缠制备方案[64]

Fig. 2. Schematic for nonlocally entangling two pairs of stationary qubits[64].

光子经过信道传输到达邻近网络节点, 与 QM4 相互作用, 并经过光量子态调控单元 PSE′($|A_{\mathrm{S}}\rangle \leftrightarrow |D_{\mathrm{L}}\rangle$) 后, 与 QM2 相互作用. 4 个 QM 与单光子极化和时间仓量子比特系统演化为[64]

$$\begin{aligned} |S_3\rangle = \frac{1}{2}(&|\phi_{12}^+\rangle|\phi_{34}^+\rangle|D_{\mathrm{S}}\rangle + |\psi_{12}^+\rangle|\psi_{34}^+\rangle|A_{\mathrm{S}}\rangle \\ &+ |\phi_{12}^+\rangle|\psi_{34}^+\rangle|D_{\mathrm{L}}\rangle + |\psi_{12}^+\rangle|\psi_{34}^+\rangle|A_{\mathrm{L}}\rangle), \end{aligned} \tag{5}$$

其中 $|\phi_{ij}^+\rangle = (|g_i\rangle|g_j\rangle + |e_i\rangle|e_j\rangle)/\sqrt{2}$, $|\psi_{ij}^+\rangle = (|g_i\rangle|e_j\rangle + |e_i\rangle|g_j\rangle)/\sqrt{2}$ 是两个 QM 贝尔态. 此时, 两个量子网络节点中的两对 QM 均处于贝尔态并与光子纠缠. 在合适的基矢下测量单光子的量子态, 便可以以预报的形式生成两对非局域贝尔态.

4 基于单光子极化和时间仓高维编码的多对非局域量子纠缠态制备

第 3 节简单介绍了引入时间仓量子比特的量子多模非局域量子纠缠制备方案. 单光子的极化和时间仓量子比特编码使得单次单光子传输可生成两对非局域量子纠缠[64]. 考虑光子时间仓编码的高维特性, 引入时间仓高维量子位编码[67,70–72] 有望实现单光子传输生成多对非局域量子纠缠[65].

图 3 给出了一种基于单光子极化和时间仓高维编码生成 n 对非局域量子纠缠的原理图. $\mathcal{T}_{(T_i)}$ 表示为光子引入一个长度为 $T_i = 2^{n-1-i}$ 的时间延迟; $\mathrm{PBS}_{\mathrm{i}}'$ 表示极化分束器, 透过极化状态为 $|A\rangle$ 的光子并反射极化状态为 $|D\rangle$ 的光子; 其他元件与图 2 一致. 光子初态为 $|D\rangle$, 所有电子自旋比特 QM 的初态均为 $|\Psi\rangle_{\mathrm{in}}$. 在量子节点 A 中, 光子每次与一个 QM 作用后, 便通过光子态调控单元 PSE_m 加倍时间仓维度, 将电子自旋比特与光子极化之间的纠缠转化为电子自旋比特与光子时间仓高维量子位之间的纠缠. 这里, PSE_m 实现如下变换 $\mathcal{T}_{(d_l)}|A\rangle \to \mathcal{T}_{(d_l+T_m)}|D\rangle$, 其中 $d_l = 2^{(n-m)l}$, $l = 0, 1, \cdots, 2^{m-1}-1$. 在光子与第 m 个 QM 相互作用后, 它们组成系统的量子态演化为

$$|\Phi\rangle = \frac{1}{\sqrt{2^m}}\sum_{i=0}^{m}\mathcal{T}_n^{(i,m)}|g_1 g_3 \cdots g_{2m-1}\rangle|D\rangle, \tag{6}$$

其中, 算符 $\mathcal{T}_n^{(i,m)}$ 分别表示为

$$\mathcal{T}_n^{(i,m)} = \begin{cases} \mathcal{T}_{(0)}, & i = 0, \\ t_n^i + \sigma_P^X \sigma_{2m-1}^X t_n^{i-1}, & i = 1, 2, \cdots, m, \end{cases}$$

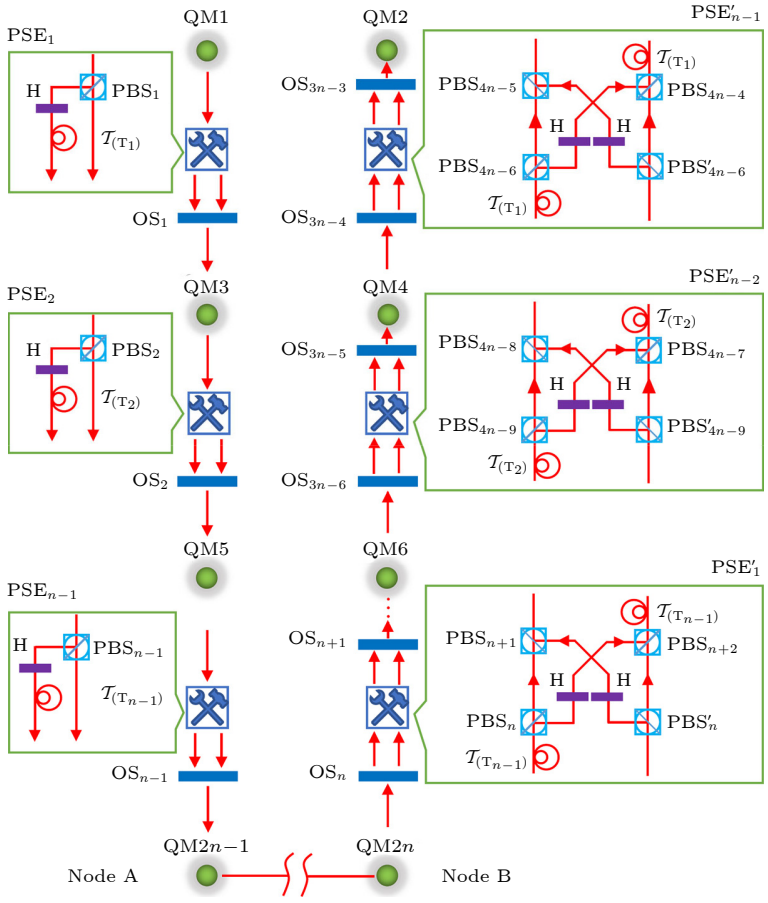


图 3 基于高维单光子编码的 n 对非局域静态量子比特纠缠制备[65]

Fig. 3. Nonlocal entanglement generation for n pairs of stationary qubits based on high-dimensional encoding of a single photon[65].

$$t_n^k = \sum_{\substack{i_1=1,\\ i_1<i_2<\cdots<i_k}}^{m-1} \mathcal{T}_{(T_{i_1})}\cdots\mathcal{T}_{(T_{i_k})}\sigma_{2i_1-1}^X\cdots\sigma_{2i_k-1}^X.$$

在光子与第 n 个 QM 作用后, 光子与量子节点 A 中的 n 个 QM 演化为高维杂化纠缠态:

$$|\Phi_n\rangle = \frac{1}{\sqrt{2^n}}\sum_{i=0}^{n}\mathcal{T}_n^{(i,n)}|g_1g_3\cdots g_{2n-1}\rangle|D\rangle. \tag{7}$$

随后, 光子经信道传输到量子节点 B, 与其中的每一个 QM 相互作用, 除与 QM2 相互作用以外, 其他的每次作用后均引入一个光量子态调控单元 PSE$'_{\rm m}$. 这里, PSE$'_{\rm m}$ 实现光量子态变换 $\mathcal{T}_{(2i)}|A\rangle \leftrightarrow \mathcal{T}_{(2i+1)}|D\rangle$. 最终, 系统的量子态在光子与 QM2 作用后演化为杂化纠缠态[65]:

$$|\Phi_{2n}\rangle = \frac{1}{\sqrt{2^n}}\sum_{i=0}^{n}\mathcal{T}_{n,n}^{(i,n)}|\phi_{1,2}\rangle|\phi_{3,4}\rangle|\cdots|\phi_{2n-1,2n}\rangle|D\rangle, \tag{8}$$

其中,

$$\mathcal{T}_{n,n}^{(i,n)} = \begin{cases} \mathcal{T}_{(0)}, & i=0,\\ t_{n,n}^{i,n} + \sigma_P^X\sigma_1^X t_{n,n}^{(i-1,n)}, & i=1,2,\cdots,n, \end{cases}$$

$$t_{n,n}^{k,n} = \sum_{i_1=1}^{n-1}\sum_{i_1<i_2<\cdots<i_k}^{n-1}\mathcal{T}_{(T_{i_1})}\cdots\mathcal{T}_{(T_{i_k})}\sigma_{2i_1+2}^X\cdots\sigma_{2i_k+2}^X.$$

(8) 式表明高维编码的光子与 n 对电子自旋量子比特纠缠. 在合适的基矢下测量单光子, 可以以预报的形式生成 n 对非局域贝尔纠缠.

5 基于单光子极化和时间仓高维编码的多对多体非局域量子纠缠态制备

非局域多体量子纠缠具有超越两体量子纠缠的特性, 生成非局域多体量子纠缠可以构造结构更复杂、功能更丰富的量子网络[84–95]. 将量子多模用于生成非局域多体量子纠缠同样可以呈现加速效应. 下面介绍量子多模下的多体非局域 Greenberger-Horne-Zeilinger (GHZ) 态制备方法[66].

图 4 给出了一种基于单光子极化和时间仓高维编码生成 M 对 N 量子比特非局域 GHZ 态的方法. 光子初态为 $|D\rangle$, 所有电子自旋比特 s 的初态均为 $|\Psi\rangle_{\rm in}$. 在前 $N-1$ 个量子节点中, 除了电子自

旋比特 $s_{N-1,1}$ 以外, 光子每次与电子自旋比特相互作用后均通过一个如图 4(b) 所示的光子态调控单元 TBE_{k_m}, 加倍时间仓维度, 将电子自旋比特与光子极化之间的纠缠转化为电子自旋比特与光子时间仓高维量子位之间的纠缠. 在光子经过 TBE_{k_m} 调制后, 光子与 m 个电子自旋量子比特的量子态演化为

$$|\Phi_m\rangle = \frac{1}{\sqrt{2^m}} \sum_{t=0}^{2^m-1} \otimes_{i=1}^{m} \hat{\delta}_{1j_i^{(t)}} |g_1, \cdots, g_m\rangle |D_{t_m}\rangle, \quad (9)$$

其中 t 表示一个十进制数, 可以展开为一个 m 位二进制数 $j_1^{(t)} j_2^{(t)} \cdots j_i^{(t)} \cdots j_m^{(t)}$; 下标 t_m 表示时间延迟, $t_m = tk_m T_\Delta$; 当 $j_i^{(t)} = 0$ 时, 第 i 个电子自旋比特的状态为 $|g\rangle$. 当 $j_i^{(t)} = 1$ 时, 第 i 个电子自旋比特的状态为 $|e\rangle$; 当 $j_t^{(t)} = 1$ 时, 算符 $\hat{\delta}_{1j_i^{(t)}} = \hat{\sigma}_i^X = |g\rangle_i\langle e| + |e\rangle_i\langle g|$; 当 $j_t^{(t)} = 0$ 时, 算符 $\hat{\delta}_{1j_i^{(t)}} = \hat{I}_i = |g\rangle_i\langle g| + |e\rangle_i\langle e|$.

为了简便, 将电子自旋比特分为 M 个单元, $S^{(1)}, \cdots, S^{(k')}, \cdots, S^{(M)}$. 当光子与第 $(N-1)M$ 个电子自旋比特 $s_{N-2,M}$ 相互作用后, 系统状态演化为

$$|\Phi_{K+1}\rangle = \frac{1}{\sqrt{2^{K+1}}} \sum_{x=0}^{2^K-1} |G_{S^{(1)}}\rangle_x |G_{S^{(2)}}\rangle_x \cdots |G_{S^{(M)}}\rangle_x \otimes (|g_{N-2,M}\rangle |D_x\rangle + |e_{N-2,M}\rangle |A_x\rangle), \quad (10)$$

其中 $k' = M - k + 1$, $k = 1, 2, \cdots, M$, 并且 $|G_{S^{(k')}}\rangle$ 可以表示为

$$|G_{S^{(k')}}\rangle = \begin{cases} |g_{s_0,M} g_{s_1,M} \cdots g_{s_{N-2,M}}\rangle, k' = 1 \\ |g_{s_0,k} g_{s_1,k} \cdots g_{s_{N-2,k}}\rangle, k' = 2, 3, \cdots, M. \end{cases}$$

(10) 式中的 x 表示时间仓, 可展开为一个二进制数 $j_1 j_2 \cdots j_m \cdots j_K$. $|G_{S^{(k')}}\rangle_x$ 表示光子处于时间仓 x 时 $S^{(k')}$ 的量子态. 当 $k' = 1$ 时, $|G_{S^{(1)}}\rangle_x = \otimes_{m'=0}^{N-3} \hat{\delta}_{1j'_m} |G_{S^{(1)}}\rangle$; 当 $k' = 2, 3, \cdots, M$ 时, $|G_{S^{(k')}}\rangle_x = \otimes_{m'=0}^{N-2} \hat{\delta}_{1j'_m} |G_{S^{(k')}}\rangle$, 其中 m' 是不大于 $(m-k)/M$ 的最大整数. 此时光子与 $(N-1)M$ 个电子自旋之间形成杂化纠缠, 光子的时间仓状态与前 $(N-1)M-1$ 个电子自旋有关, 光子的极化状态与第 $(N-1)M$ 个电子自旋有关.

随后, 光子经过图 4(c) 所示的 AA 光子态调控单元, 交换光子极化状态为 $|A\rangle$, 时间仓为 x 和 $x_1 = j_1^{(1)} j_2^{(1)} \cdots j_m^{(1)} \cdots, j_K^{(1)}$ 的光子态. 这里, $j_m^{(1)} = j_m$, 但当 $m = M, 2M, \cdots (N-2)M$ 时, $j_m^{(1)} = \bar{j}_m$. 依次与量子节点 N 中的所有电子自旋相互作用, 并经过图 4(d) 所示的 $\mathrm{AD}_{k'}$ 调控光子态. 当 $x < x_{k'}$ 时, $\mathrm{AD}_{k'}$ 交换光子状态 $|A_x\rangle \leftrightarrow |D_{x_{k'}}\rangle$; 当 $x_{k'} < x$ 时, $\mathrm{AD}_{k'}$ 交换光子状态 $|A_{x_{k'}}\rangle \leftrightarrow |D_x\rangle$. 这里, $x_{k'} = j_1^{(k')} j_2^{(k')} \cdots j_m^{(k')} \cdots j_K^{(k')}$, $j_m^{(k')} = j_m$, 但是当 $m = k, M+k, \cdots, (N-2)M+k$ 时, $j_m^{(k')} = \bar{j}_m$. 最终, 系统的量子态在光子与电子自旋 $s_{N-1,M}$ 相互作用后演化为[66]

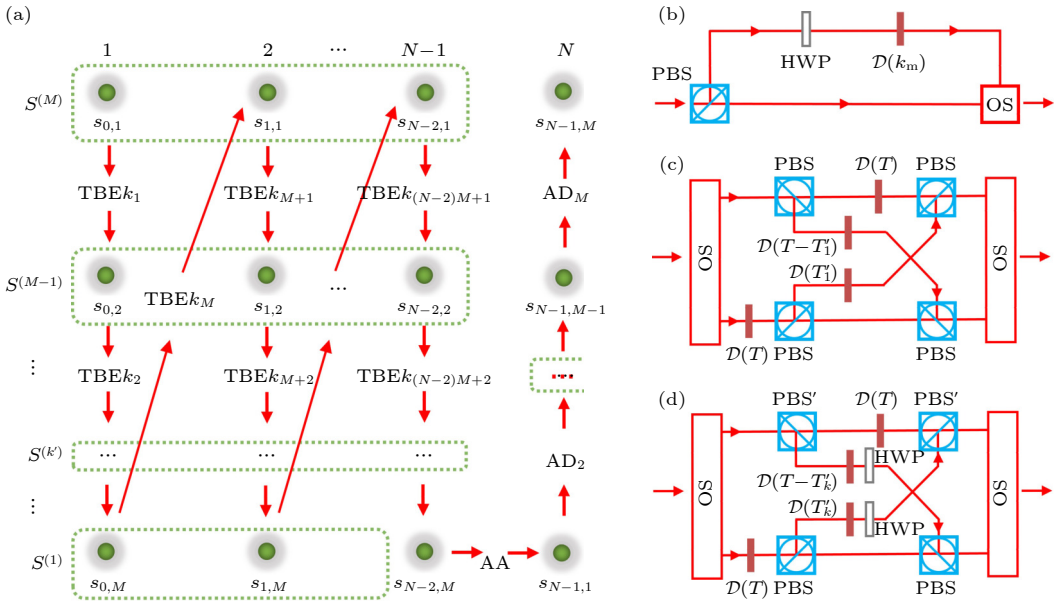


图 4 基于高维单光子编码的 M 对 N 量子比特非局域 GHZ 态制备[66]

Fig. 4. Nonlocal GHZ-state generation for M pairs of N stationary qubits based on high-dimensional encoding of a single photon[66].

$$|\Phi_{MN}\rangle = \frac{1}{\sqrt{2^{K+2}}}\sum_{x=0}^{2^K-1}|\varphi_1\rangle_x \otimes_{K'=2}^{M-1}|\varphi_{k'}\rangle_x[|D_x\rangle \otimes (|G'_{S^{(M)}}\rangle|g_{N-1,M}\rangle + |\bar{G}'_{S^{(M)}}\rangle|e_{N-1,M}\rangle) + |A_x\rangle(|G'_{S^{(M)}}\rangle|e_{N-1,M}\rangle + |\bar{G}'_{S^{(M)}}\rangle|g_{N-1,M}\rangle)], \tag{11}$$

其中,

$$|\varphi_1\rangle_x = \frac{1}{\sqrt{2}}(|G_{S^{(1)}}\rangle_x|G_{1,2}\rangle + |\bar{G}_{S^{(1)}}\rangle_x|\bar{G}_{1,2}\rangle),$$

$$|\varphi_{k'}\rangle_x = \frac{1}{\sqrt{2}}(|G'_{S^{(k')}}\rangle|g_{N-1,k'}\rangle + |\bar{G}'_{S^{(k')}}\rangle|e_{N-1,k'}\rangle),$$

$$|G_{1,2}\rangle = \begin{cases} |g_{N-2,M}g_{N-1,1}\rangle, & x < x_2 \\ |g_{N-2,M}e_{N-1,1}\rangle, & x > x_2 \end{cases},$$

$$|G'_{S^{(k')}}\rangle = \begin{cases} |G_{S^{(k')}}\rangle_x, & x < x_{k'} \\ |G_{S^{(k')}}\rangle_{x_{k'}}, & x > x_{k'} \end{cases},$$

并且 $|G_{S^{(k')}}\rangle_{x_{k'}} = \otimes_{l=0}^{N-2}\hat{\sigma}^X_{S_{l,k}}|G_{S^{(k')}}\rangle_x$, $k' = 2,3,\cdots,M$. 可见, 在合适的基矢下测量单光子, 可以以预报的形式生成 M 对 N 量子比特非局域 GHZ 态, 其中第 k' 个 GHZ 态由时间仓 x 和 $x_{k'}$ 的值确定, 而第 M 个 GHZ 态则由光子的时间仓和极化状态联合确定. 值得注意的是, 上述方法在 $N = 2$ 时等同于第 4 节中的多对非局域贝尔纠缠态制备方法.

6 基于高维光子纠缠分发的量子多模非局域量子纠缠态制备

前文介绍了基于单光子高维编码量子多模非局域量子纠缠态的制备方案. 本节简单介绍基于双光子高维纠缠分发的量子多模非局域量子纠缠态制备方案[69]. 图 5 给出了生成三对非局域量子纠缠的方法. 中间节点产生高维纠缠态[96]:

$$|\Psi_p\rangle = \frac{1}{2\sqrt{2}}\sum_{i=0}^{7}\mathcal{T}_1(i)\mathcal{T}_2(i)|DD\rangle, \tag{12}$$

其中时间算符 $\mathcal{T}_{1(2)}(i)$ 表示对光子 $p_{1(2)}$ 引入 iT_Δ 的时间延迟. 利用 Pockel 盒 (PC′) 将上述时间模式高维纠缠转化为时间仓高维量子位和极化的超纠缠态:

$$|\Psi_{p_1}\rangle = \frac{1}{2}\sum_{i=0}^{3}\mathcal{T}_1(i)\mathcal{T}_2(i)|\phi_{\rm p}\rangle, \tag{13}$$

其中 $|\phi_{\rm p}\rangle = \frac{1}{\sqrt{2}}(|DD\rangle + |AA\rangle)$ 是光子的极化贝尔态.

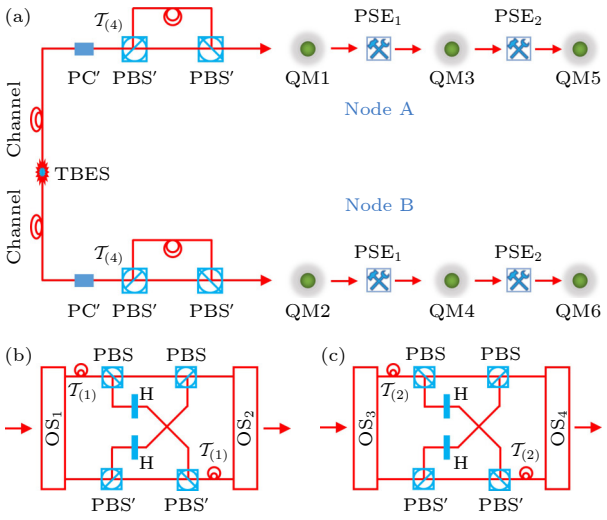


图 5 基于高维双光子纠缠分发的 3 对非局域静态量子比特纠缠制备[69]

Fig. 5. Nonlocal entanglement generation for 3 pairs of stationary qubits based on two-photon high-dimensional entanglement distribution[69].

两个光子分别与 QM1 和 QM2 相互作用, 经过图 5(b) 所示的光子态调控单元 $\rm PSE_1$, 完成光子态变换 $\mathcal{T}(0)|A\rangle \leftrightarrow \mathcal{T}(1)|D\rangle$ 和 $\mathcal{T}(2)|A\rangle \leftrightarrow \mathcal{T}(3)|D\rangle$. 系统的量子态演化为

$$|\xi_1\rangle = \frac{1}{2}[(\phi_{\rm T}^{0,1} + \phi_{\rm T}^{2,3})|\phi_{12}\rangle + (\psi_{\rm T}^{0,1} + \psi_{\rm T}^{2,3})|\psi_{12}\rangle]|\phi_{\rm p}\rangle, \tag{14}$$

其中 $\phi_{\rm T}^{i,j} = \frac{1}{\sqrt{2}}[\mathcal{T}_1(i)\mathcal{T}_2(i) + \mathcal{T}_1(j)\mathcal{T}_2(j)]$, $\psi_{\rm T}^{i,j} = \frac{1}{\sqrt{2}}\times[\mathcal{T}_1(i)\mathcal{T}_2(j) + \mathcal{T}_1(j)\mathcal{T}_2(i)]$, 两个电子自旋比特处于纠缠态, 并与光子的时间仓模式纠缠, 而光子的极化被初始化到贝尔纠缠态 $|\phi_{\rm p}\rangle$ 用于下一对电子自旋量子纠缠的制备.

光子对分别与电子自旋量子比特 QM3 和 QM4 相互作用, 并经过光子态调控单元 $\rm PSE_2$ 交换量子态 $\mathcal{T}(0)|A\rangle \leftrightarrow \mathcal{T}(2)|D\rangle$ 和 $\mathcal{T}(1)|A\rangle \leftrightarrow \mathcal{T}(3)|D\rangle$ 后与 QM5 和 QM6 相互作用. 系统的量子态演化为[69]

$$|\xi_3\rangle = \frac{1}{4}[(\phi_{\rm T}^{0,1} + \phi_{\rm T}^{2,3})|\phi_{12}\rangle|\phi_{34}\rangle + (\psi_{\rm T}^{0,1} + \psi_{\rm T}^{2,3})|\psi_{12}\rangle \otimes |\phi_{34}\rangle + (\psi_{\rm T}^{0,2} + \psi_{\rm T}^{1,3})|\phi_{12}\rangle|\psi_{34}\rangle + (\psi_{\rm T}^{0,3} + \psi_{\rm T}^{1,2})|\psi_{12}\rangle|\psi_{34}\rangle](|\phi_{56}\rangle|\phi_{\rm p}\rangle + |\psi_{56}\rangle|\psi_{\rm p}\rangle). \tag{15}$$

最终, 可以通过独立测量两个光子的量子态, 以预报的形式生成 3 对非局域静态量子比特纠缠. 其中, 前 2 对非局域纠缠态由光子的时间仓确定, 最后 1 对纠缠态则由光子的极化确定. 与单光子高维编码相似[65,66], 通过制备更高维度的双光子纠

缠, 该方法可以扩展用于生成更多对的非局域量子纠缠甚至多体纠缠.

7 基于高维单光子编码的非局域量子逻辑纠缠制备

量子多模不仅可以实现对非局域物理量子比特纠缠制备的加速, 也可以用于加速非局域量子逻辑比特纠缠的制备[97]. 利用高维单光子编码, 适当调节光子量子态, 可以将物理量子比特演化为与光子纠缠的逻辑量子比特, 进而将逻辑量子比特与光子的纠缠转换为两个逻辑量子比特之间的纠缠[73].

图 6 给出了一种基于高维单光子编码的非局域量子逻辑纠缠制备方法. 两个量子节点中的逻辑比特 $L_{\rm A}$ 和 $L_{\rm B}$ 分别由 4 个物理比特构成, 并且 $L_{\rm A}$ 和 $L_{\rm B}$ 的编码空间可以分别看作是稳定子 $S_{\rm A}=\{Z_1Z_3, X_1X_2X_3X_4, Z_2Z_4\}$ 和 $S_{\rm B}=\{Z_{1'}Z_{3'}, X_{1'}X_{2'}X_{3'}X_{4'}, Z_{2'}Z_{4'}\}$ 的偶宇称子空间[98–100], 其中泡利算符 $X_i=|g_i\rangle\langle e_i|+|e_i\rangle\langle g_i|, Z_i=|g_i\rangle\langle g_i|-|e_i\rangle\langle e_i|$. $L_{\rm A}$ 的逻辑计算基矢表示为

$$|\tilde{0}\rangle=\frac{1}{\sqrt{2}}(|g_4g_3g_2g_1\rangle+|e_4e_3e_2e_1\rangle),$$
$$|\tilde{1}\rangle=\frac{1}{\sqrt{2}}(|g_4e_3g_2e_1\rangle+|e_4g_3e_2g_1\rangle). \tag{16}$$

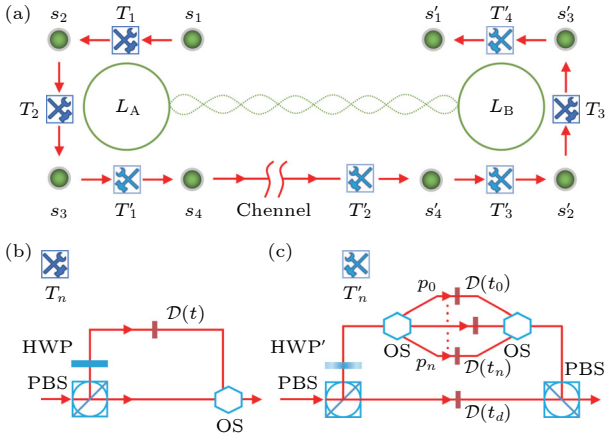


图 6 非局域逻辑量子比特纠缠制备[73]

Fig. 6. Nonlocal logical-qubit entanglement generation[73].

入射光子初态为 $|D\rangle$, 所有电子自旋 s_i 初始化为 $|\phi_i\rangle=\frac{1}{\sqrt{2}}(|g_i\rangle+|e_i\rangle)$. 当光子与 $L_{\rm A}$ 节点中 4 个 SiV^- 电子自旋相互作用并经过光量子态调控单元 $T_{1,2}$ 和 T'_1. 这里, T_n 为加倍时间仓数, 将所有处于 A 极化光子转换为 D 极化. T_1, T_2 和 T_3 分别引入时间延迟 T_Δ, $2T_\Delta$ 和 $8T_\Delta$. 光量子态调控单元 T'_1 交换量子态 $|A_0\rangle\leftrightarrow|A_3\rangle$ 和 $|A_1\rangle\leftrightarrow|A_2\rangle$. 系统的量子态可以演化为

$$|\varphi_1\rangle=\frac{1}{2\sqrt{2}}\sum_{l=0}^{3}(I+X_4X_{\rm p})|l_{L_{\rm A}}\rangle|D_l\rangle, \tag{17}$$

其中 $|0_{L_{\rm A}}\rangle=|\tilde{0}\rangle$, $|1_{L_{\rm A}}\rangle=X_1|\tilde{0}\rangle$, $|2_{L_{\rm A}}\rangle=X_2|\tilde{0}\rangle$, $|3_{L_{\rm A}}\rangle=X_2X_1|\tilde{0}\rangle$. 此时, $L_{\rm A}$ 的 4 个物理比特 $s_1s_2s_3s_4$ 之间已经成功构建一个逻辑比特, 虽然此逻辑比特并没有完全制备在 $\{|\tilde{0}\rangle,|\tilde{1}\rangle\}$ 基矢上, 但是可以根据最终测得的光子状态对物理比特进行旋转, 使其投影到预定的逻辑态上.

随后, 将光子经信道传输到 $L_{\rm B}$ 所在节点, 经光子调控单元 T'_2, 完成变换 $|A_i\rangle\rightarrow|D_{7-i}\rangle$) 后, 与 $L_{\rm B}$ 中的 4 个电子自旋相互作用并调控光子量子态. 当时间仓满足关系式 $l=j_4^{(l)}j_3^{(l)}j_2^{(l)}j_1^{(l)}$ 且 $l\in\{0,\cdots,7\}$, $l'=j_4^{(l)}\bar{j}_3^{(l)}j_2^{(l)}\bar{j}_1^{(l)}$ 时, T'_3 交换量子态 $|A_l\rangle\leftrightarrow|A_{l'}\rangle$; 当时间仓满足关系式 $l=j_5^{(l)}j_4^{(l)}j_3^{(l)}j_2^{(l)}j_1^{(l)}$ 且 $l\in\{0,\cdots,15\}$, $l'=j_5^{(l)}j_4^{(l)}\bar{j}_3^{(l)}j_2^{(l)}\bar{j}_1^{(l)}$ 时, T'_4 交换量子态 $|A_l\rangle\leftrightarrow|A_{l'}\rangle$. 系统的量子态最终演化为

$$|\varphi_2\rangle=\frac{1}{8}\sum_{l=0}^{7}(I+\tilde{X}\tilde{X}')|l_{L_{\rm A}}\rangle(|0_{L_{\rm B}}\rangle|D_l\rangle+|1_{L_{\rm B}}\rangle|A_l\rangle$$
$$+|2_{L_{\rm B}}\rangle|D_{l+8}\rangle+|3_{L_{\rm B}}\rangle|A_{l+8}\rangle), \tag{18}$$

其中 $\tilde{X}=X_3X_1$, $|4_{L_{\rm A}}\rangle=\tilde{X}|1_{L_{\rm A}}\rangle$, $|5_{L_{\rm A}}\rangle=\tilde{X}|0_{L_{\rm A}}\rangle$, $|6_{L_{\rm A}}\rangle=\tilde{X}|3_{L_{\rm A}}\rangle$, $|7_{L_{\rm A}}\rangle=\tilde{X}|2_{L_{\rm A}}\rangle$. 此时, 逻辑比特 $L_{\rm B}$ 被成功生成, 并通过测量光子的量子态, 将 $L_{\rm A}$ 与 $L_{\rm B}$ 投影到非局域的逻辑纠缠态上. 根据光子态测量结果, 对电子自旋施加单比特操控, 可以把 $L_{\rm A}$ 与 $L_{\rm B}$ 两个逻辑比特制备到逻辑纠缠态 $|\Phi^+\rangle=\frac{1}{\sqrt{2}}(|\tilde{0}\rangle|\tilde{0}'\rangle+|\tilde{1}\rangle|\tilde{1}'\rangle)$.

8 讨论与展望

到目前为止, 本文已经分析了理想条件下基于量子多模的非局域量子纠缠制备方法. 假定硅空位色心与单边纳米腔耦合系统可以实现单光子与单电子自旋量子比特的确定性相互作用, 忽略了光量子态调控单元中光学开关引入的插入损耗等[101,102]. 但在实际的非局域纠缠态制备过程中, 单光子与静态量子比特的非理想相互作用将不可避免地影响生成的非局域纠缠的保真度和效率[66,69,73].

目前, 基于硅空位色心与纳米腔耦合系统的量子

网络实验研究已取得诸多重要进展[1,103,104]. Lukin团队[105]从块状金刚石中刻蚀出高品质纳米腔, 并使用电子束曝光在聚合物抗蚀剂中制备纳米级注入窗口, 将硅离子精准注入腔模最大处, 随后在超高真空下高温退火形成 SiV^- 色心. 该工艺显著提升了硅空位色心与纳米腔耦合系统的协同参数 C, 可实现 $C>100$, 对应的 SiV^- 色心与纳米腔的耦合速率、腔损耗率以及 SiV^- 色心激发态的衰减率平均值为 $(g,\kappa,\gamma)=2\pi\times(8.38,21.6,0.12)$ GHz[51]. 通过外加 $B\approx0.5$ T 的磁场并调控应力, 可实现两个基态 $|g\rangle$ 和 $|e\rangle$ 对应偶极跃迁的较大失谐 $\Delta\approx100$, 从而实现 SiV^- 色心自旋态依赖的单光子散射过程[83,105]. 此外, SiV^- 色心具有 D_{3d} 反演对称性, 其基态与激发态的固有电偶极矩为零, 因此跃迁对纳米结构中的电场噪声不敏感[82], 与单边纳米腔耦合的 SiV^- 色心在低温下显示出长相干时间. 在温度约为 100 mK 时, 通过引入动力学解耦等技术, SiV^- 色心的相干时间已延长至 $T_2\approx13$ ms[106].

通过调控腔原子耦合系统参数, 可以引入自避错的单光子散射过程[37,66,107–111], 并利用后选择的方法消除非理想散射对所制备的非局域纠缠保真度的影响[37]. 基于实验可实现的参数[51], 在后选择模式下, SiV^- 色心与纳米腔耦合系统的单光子散射效率将下降为 0.96[66]. 在光学调控模式对称情况下, 光学开关插入损耗对非局域纠缠保真度的影响也可以忽略不计, 但会影响非局域纠缠的制备效率. 只有当开关插入损耗低于一定值时, 量子多模在信道传输中引入的效率增强效应才能得以体现[69]. 随着节点间距的增加, 开关插入损耗的阈值可以适当降低, 但此时需要考虑静态量子比特有限退相干时间对非局域量子纠缠制备的影响. 在不考虑开关插入损耗的情况下, 基于量子多模的非局域纠缠态制备效率随静态量子比特数变化并不明显[65,66]. 在相距 22 km 的两个量子网络节点内, 基于单光子量子多模制备 3 对和 10 对 SiV^- 色心贝尔纠缠的效率分别为 $\eta_3=0.217$ 和 $\eta_{10}=0.069$[65]. 这些效率与无多模加速下, 使用第一类纠缠方法[31–34]制备 1 对相同间距 SiV^- 色心贝尔纠缠的效率 $\eta_1=0.300$ 相当.

量子多模的核心优势在于高维编码可提升单光子所携带的量子信息容量[64–67]. 一个 2^n 维编码的单光子在一次传输所承载的量子信息, 相当于 n 个单量子比特编码的光子所传输的信息总量[65–67]. 在衰减系数为 α 的光纤信道中传输相同距离 L 时, 尽管两种方式所携带的量子信息容量相同, 但其无损耗传输效率分别为 $\eta_\Gamma=\exp(-\alpha L)$ 和 $\eta_{\Gamma'}=\exp(-\alpha nL)$. 传输效率比值 $\eta_\Gamma/\eta_{\Gamma'}$ 将随着距离 L 指数级增长[65]. 量子多模技术通过测量一个单光子即可实现纠缠, 而后者需测量 n 个单光子, 在光子计数率方面也具有明显优势[66,112]. 经典多模的核心是在给定时间内利用多模复用提升生成一对非局域纠缠的速率, 但是其有限的速率提升能力受限于节点内静态量子比特数 N[30–32]. 在 N 给定情况下, 同时生成多对非局域纠缠的速率将随纠缠对数的增加快速降低[32].

在量子多模技术的传输优势不明显的情形下, 即当两个量子网络节点间距较小、所需静态量子比特纠缠较少时, 其所带来的效率提升并不显著[69]. 反之, 量子多模技术则可提供高于经典多模方案的传输效率优势. 例如, 在基于光子纠缠分发制备非局域固态纠缠的方案中, 使用相同数量的光量子比特对 $n=10$ 来制备 $L=50$ km 两节点间 $m=4$ 和 $m=2$ 对 SiV^- 色心贝尔纠缠态时, 引入经典多模机制的 4 维编码量子多模相比经典多模方案可分别获得约 30 倍和 5 倍的效率提升; 与未引入经典多模的量子多模技术相比, 则分别提升约 3 倍和 2 倍[69].

值得注意的是, 量子多模非局域纠缠的制备方法具有一定的普适性, 可直接推广应用于其他单光子与原子相互作用接口[77], 甚至用于产生空间分离原子系综之间的非局域量子纠缠[30]. 此外, 单光子具有多个自由度, 除了时间仓高维编码外, 频率、角动量和空间模式等也可用于编码高维量子位[113–118], 使用一个或多个自由度编码有望进一步增加量子多模的模式数, 从而优化量子多模下的非局域量子纠缠制备及量子态传输等应用[63,119–121].

当前的量子多模非局域纠缠制备主要研究了基于单光子高维编码的第一类非局域方法[64–67,73]. 对于基于双光子高维纠缠分发的第三类方法, 已有三对非局域贝尔纠缠态制备的工作[69], 其在经典多模加速下相较于第一类方法具有明显优势. 从理论上讲, 第三类方法同样可用于制备更多对非局域两体纠缠, 甚至用于制备非局域多体纠缠和逻辑纠缠. 基于纠缠转移实现量子多模非局域量子纠缠制备的第二类方法还未见报道, 其主要难点在于如何有效实现两个高维光子之间的纠缠态分析[122–128]. 一旦具备高性能的高维光子纠缠态分析

方法, 基于第二类方法的量子多模和经典多模技术相结合将有望构建出更高效的量子网络.

参考文献

[1] Ruf M, Wan N H, Choi H, Englund D, Hanson R 2021 *J. Appl. Phys.* **130** 070901
[2] Wehner S, Elkouss D, Hanson R 2018 *Science* **362** eaam9288
[3] Reiserer A 2022 *Rev. Mod. Phys.* **94** 041003
[4] Deng F G, Long G L, Liu X S 2003 *Phys. Rev. A* **68** 042317
[5] Pan D, Liu Y C, Niu P, Zhang H, Zhang F, Wang M, Song X T, Chen X, Zheng C, Long G L 2025 *Sci. Adv.* **11** eadt4627
[6] Ying J W, Sheng Y B, Zhou L, Kwek L C 2025 *Front. Phys.* **20** 33401
[7] Sheng Y B, Zhou L, Long G L 2022 *Sci. Bull.* **67** 367
[8] Zhang W, Ding D S, Sheng Y B, Zhou L, Shi B S, Guo G C 2017 *Phys. Rev. Lett.* **118** 220501
[9] Massa F, Moqanaki A, Baumeler A, Del Santo F, Kettlewell J A, Dakić B, Walther P 2019 *Adv. Quantum Technol.* **2** 1900050
[10] Zhao P, Zhong W, Du M M, Li X Y, Zhou L, Sheng Y B 2024 *Front. Phys.* **19** 51201
[11] Qi Z, Li Y, Huang Y, Feng J, Zheng Y, Chen X 2021 *Light Sci. Appl.* **10** 183
[12] Ying J W, Wang J Y, Xiao Y X, Gu S P, Wang X F, Zhong W, Du M M, Li X Y, Shen S T, Zhang A L, Zhou L, Sheng Y B 2025 *Sci. China Phys. Mech. Astron.* **68** 240312
[13] Liu C, Zhang C, Gu S P, Wang X F, Zhou L, Sheng Y B 2025 *Sci. China Phys. Mech. Astron.* **68** 250311
[14] Cao Z, Wang Y, Chai G, Chen X, Lu Y 2025 *Chin. Phys. B* **34** 020308
[15] Cirac J I, Ekert A K, Huelga S F, Macchiavello C 1999 *Phys. Rev. A* **59** 4249
[16] Jiang L, Taylor J M, Sørensen A S, Lukin M D 2007 *Phys. Rev. A* **76** 062323
[17] Qin W, Wang X, Miranowicz A, Zhong Z, Nori F 2017 *Phys. Rev. A* **96** 012315
[18] Wu Y K, Duan L M 2023 *Acta Phys. Sin.* **72** 230302 (in Chinese) [吴宇恺, 段路明 2023 物理学报 **72** 230302]
[19] Su W, Qin W, Miranowicz A, Li T, Nori F 2024 *Phys. Rev. A* **110** 052612
[20] Hu Z G, Xu K, Zhang Y X, Li B B 2024 *Chin. Phys. Lett.* **41** 014203
[21] Qiu J, Liu Y, Hu L, Wu Y, Niu J, Zhang L, Huang W, Chen Y, Li J, Liu S, Zhong Y, Duan L, Yu D 2025 *Sci. Bull.* **70** 351
[22] Kómár P, Kessler E M, Bishof M, Jiang L, Sørensen A S, Ye J, Lukin M D 2014 *Nat. Phys.* **10** 582
[23] Degen C L, Reinhard F, Cappellaro P 2017 *Rev. Mod. Phys.* **89** 035002
[24] Hosseiny S M, Seyed-Yazdi J, Norouzi M 2025 *Front. Phys.* **20** 24201
[25] Guo H, Wu T, Luo B, Liu Y X 2024 *Physics* **53** 384 (in Chinese) [郭弘, 吴腾, 罗斌, 刘院省 2024 物理 **53** 384]
[26] Jiao Y F, Wang J, Zhang Q, Lin H Z, Jing H 2025 *Funda. Res.* **112** 012421
[27] DeMille D, Hutzler N R, Rey A M, Zelevinsky T 2024 *Nat. Phys.* **20** 741
[28] Munro W J, Azuma K, Tamaki K, Nemoto K 2015 *IEEE J. Sel. Top. Quantum Electron.* **21** 78
[29] Togan E, Chu Y, Trifonov A S, Jiang L, Maze J, Childress L, Dutt M V G, Sørensen A S, Hemmer P R, Zibrov A S, Lukin M D 2010 *Nature* **466** 730
[30] Sangouard N, Simon C, de Riedmatten H, Gisin N 2011 *Rev. Mod. Phys.* **83** 33
[31] Jones C, Kim D, Rakher M T, Kwiat P G, Ladd T D 2016 *New J. Phys.* **18** 083015
[32] van Loock P, Alt W, Becher C, Benson O, Boche H, Deppe C, Eschner J, Höfling S, Meschede D, Michler P, Schmidt F, Weinfurter H 2020 *Adv. Quantum Technol.* **3** 1900141
[33] Wang C, Zhang Y, Jin G S 2011 *Phys. Rev. A* **84** 032307
[34] Li T, Miranowicz A, Hu X, Xia K, Nori F 2018 *Phys. Rev. A* **97** 062318
[35] Cabrillo C, Cirac J I, García-Fernández P, Zoller P 1999 *Phys. Rev. A* **59** 1025
[36] Yu C S, Yi X X, Song H S, Mei D 2007 *Phys. Rev. A* **75** 044301
[37] Li T, Deng F G 2016 *Phys. Rev. A* **94** 062310
[38] Hurst D L, Joanesarson K B, Iles-Smith J, Mørk J, Kok P 2019 *Phys. Rev. Lett.* **123** 023603
[39] Zhang J N, Zhang T Y, Duan J C, Gong Y X, Zhu S N 2024 *Chin. Phys. B* **33** 110301
[40] Zhu P, Wang Y, Du Y, Yu M, Zhang K, Wang K, Xu P 2025 *Sci. China Phys. Mech. Astron.* **68** 260311
[41] Lei Y, Asadi F K, Zhong T, Kuzmich A, Simon C, Hosseini M 2023 *Optica* **10** 1511
[42] Li T, Yang G J, Deng F G 2016 *Phys. Rev. A* **93** 012302
[43] Wang G, Long G 2020 *Sci. China Phys. Mech. Astron.* **63** 220311
[44] Liu X, Hu J, Li Z F, Li X, Li P Y, Liang P J, Zhou Z Q, Li C F, Guo G C 2021 *Nature* **594** 41
[45] Lago-Rivera D, Grandi S, Rakonjac J V, Seri A, de Riedmatten H 2021 *Nature* **594** 37
[46] Wang Y F, Zhou Y, Wang Y, Yan H, Zhu S L 2023 *Acta Phys. Sin.* **72** 206701 (in Chinese) [王云飞, 周颖, 王英, 颜辉, 朱诗亮 2023 物理学报 **72** 206701]
[47] Moiseev S A, Gerasimov K I, Minnegaliev M M, Moiseev E S, Deev A D, Balega Y Y 2025 *Front. Phys.* **20** 23301
[48] Yan P S, Zhou L, Zhong W, Sheng Y B 2023 *Sci. China-Phys. Mech. Astron.* **66** 250301
[49] Li T, Miranowicz A, Xia K, Nori F 2019 *Phys. Rev. A* **100** 052302
[50] Lu C Y, Yang T, Pan J W 2009 *Phys. Rev. Lett.* **103** 020501
[51] Bhaskar M K, Riedinger R, Machielse B, Levonian D S, Nguyen C T, Knall E N, Park H, Englund D, Lončar M, Sukachev D D, Lukin M D 2020 *Nature* **580** 60
[52] Wang T J, Song S Y, Long G L 2012 *Phys. Rev. A* **85** 062311
[53] Sheng Y B, Zhou L, Long G L 2013 *Phys. Rev. A* **88** 022302
[54] Sinclair N, Saglamyurek E, Mallahzadeh H, Slater J A, George M, Ricken R, Hedges M P, Oblak D, Simon C, Sohler W, Tittel W 2014 *Phys. Rev. Lett.* **113** 053603
[55] Chang W, Li C, Wu Y K, Jiang N, Zhang S, Pu Y F, Chang X Y, Duan L M 2019 *Phys. Rev. X* **9** 041033
[56] Zhang S, Shi J, Liang Y, Sun Y, Wu Y, Duan L, Pu Y 2024 *Nat. Commun.* **15** 10306
[57] Wang M, Jiao H, Lu J, Fan W, Li S, Wang H 2025 *Optica* **12** 274
[58] Munro W, Harrison K, Stephens A, Devitt S, Nemoto K 2010 *Nat. Photonics* **4** 792
[59] Erhard M, Krenn M, Zeilinger A 2020 *Nat. Rev. Phys.* **2** 365
[60] Jiang G L, Liu W Q, Wei H R 2024 *Adv. Quantum Technol.* **7** 2400033

[61] Jiang G L, Yuan J B, Liu W Q, Wei H R 2024 *Phys. Rev. Appl.* **21** 014001

[62] Xu C, Huang S, Yu Q, Wei D, Chen P, Nie S, Zhang Y, Xiao M 2021 *Phys. Rev. A* **104** 063716

[63] Lo Piparo N, Hanks M, Gravel C, Nemoto K, Munro W J 2020 *Phys. Rev. Lett.* **124** 210503

[64] Lo Piparo N, Munro W J, Nemoto K 2019 *Phys. Rev. A* **99** 022337

[65] Xie Z, Liu Y, Mo X, Li T, Li Z 2021 *Phys. Rev. A* **104** 062409

[66] Zhou H, Li T, Xia K 2023 *Phys. Rev. A* **107** 022428

[67] Zheng Y, Sharma H, Borregaard J 2022 *PRX Quantum* **3** 040319

[68] Du F F, Fan G, Wu Y M, Ren B C 2023 *Chin. Phys. B* **32** 060304

[69] Xie Z, Wang G, Guo Z, Li Z, Li T 2023 *Opt. Express* **31** 37802

[70] Doda M, Huber M, Murta G, Pivoluska M, Plesch M, Vlachou C 2021 *Phys. Rev. Appl.* **15** 034003

[71] Islam N T, Lim C C W, Cahall C, Qi B, Kim J, Gauthier D J 2019 *Quantum Sci. Technol.* **4** 035008

[72] Vagniluca I, Da Lio B, Rusca D, Cozzolino D, Ding Y, Zbinden H, Zavatta A, Oxenløwe L K, Bacco D 2020 *Phys. Rev. Appl.* **14** 014051

[73] Li J, Xie Z, Li Y, Liang Y, Li Z, Li T 2024 *Sci. China-Phys. Mech. Astron.* **67** 220311

[74] Gong B, Tu T, Guo A L, Zhu L T, Li C F 2021 *Chin. Phys. Lett.* **38** 044201

[75] Canteri M, Koong Z X, Bate J, Winkler A, Krutyanskiy V, Lanyon B P 2024 arXiv: 2406.09480 [quant-ph]

[76] Ruskuc A, Wu C J, Green E, Hermans S L N, Pajak W, Choi J, Faraon A 2025 *Nature* **639** 54

[77] Borregaard J, Sørensen A S, Lodahl P 2019 *Adv. Quantum Technol.* **2** 1800091

[78] Chen K C, Bersin E, Englund D 2021 *NPJ Quantum Inf.* **7** 2

[79] Qin W, Miranowicz A, Li P B, Lu X Y, You J Q, Nori F 2018 *Phys. Rev. Lett.* **120** 093601

[80] Uppu R, Midolo L, Zhou X, Carolan J, Lodahl P 2021 *Nat. Nanotechnol.* **16** 1308

[81] Reiserer A, Rempe G 2015 *Rev. Mod. Phys.* **87** 1379

[82] Radulaski M, Zhang J L, Tzeng Y K, Lagoudakis K G, Ishiwata H, Dory C, Fischer K A, Kelaita Y A, Sun S, Maurer P C, Alassaad K, Ferro G, Shen Z X, Melosh N A, Chu S, Vučković J 2019 *Laser Photonics Rev.* **13** 1800316

[83] Nguyen C T, Sukachev D D, Bhaskar M K, Machielse B, Levonian D S, Knall E N, Stroganov P, Riedinger R, Park H, Lončar M, Lukin M D 2019 *Phys. Rev. Lett.* **123** 183602

[84] Fu Y, Yin H L, Chen T Y, Chen Z B 2015 *Phys. Rev. Lett.* **114** 090501

[85] Gao Z, Li T, Li Z 2020 *Sci. China-Phys. Mech. Astron.* **63** 120311

[86] Wang X, Fu J, Liu S, Wei Y, Jing J 2022 *Optica* **9** 663

[87] Li C L, Fu Y, Liu W B, Xie Y M, Li B H, Zhou M G, Yin H L, Chen Z B 2023 *Phys. Rev. Res.* **5** 033077

[88] Li X L, Zhai S Q, Liu K 2025 *Acta Phys. Sin.* **74** 090301 (in Chinese) [李晓玲, 翟淑琴, 刘奎 2025 物理学报 **74** 090301]

[89] Zhang C, Zhang Q, Zhong W, Du M M, Shen S T, Li X Y, Zhang A L, Zhou L, Sheng Y B 2025 *Phys. Rev. A* **111** 012602

[90] Yang C P, Ni J H, Bin L, Zhang Y, Yu Y, Su Q P 2024 *Front. Phys.* **19** 31201

[91] Ma M, Li Y, Shang J 2024 *Funda. Res.* doi: 10.1016/j.fmre.2024.03.031 (In Press)

[92] Liu Y, Zhou Y, Wu L, Qin J, Yan Z, Jia X 2025 *Funda. Res.* **5** 132

[93] Zhang Q, Ying J W, Wang Z J, Zhong W, Du M M, Shen S T, Li X Y, Zhang A L, Gu S P, Wang X F, Zhou L, Sheng Y B 2025 *Phys. Rev. A* **111** 012603

[94] Du F F, Fan Z G, Ren X M, Ma M, Liu W Y 2025 *Chin. Phys. B* **34** 010303

[95] Zhao P, Ying J W, Yang M Y, Zhong W, Du M M, Shen S T, Li Y X, Zhang A L, Zhou L, Sheng Y B 2025 *Phys. Rev. Appl.* **23** 014003

[96] Du F F, Ma M, Bai Z Y, Tan Q L 2025 *Phys. Rev. A* **111** 032604

[97] Sheng Y B, Zhou L 2024 *Sci. China Phys. Mech. Astron.* **67** 220331

[98] Erhard A, Poulsen Nautrup H, Meth M, Postler L, Stricker R, Stadler M, Negnevitsky V, Ringbauer M, Schindler P, Briegel H J, Blatt R, Friis N, Monz T 2021 *Nature* **589** 220

[99] Devitt S J, Munro W J, Nemoto K 2013 *Rep. Prog. Phys.* **76** 076001

[100] Arab A R 2024 *Front. Phys.* **19** 51203

[101] Borregaard J, Pichler H, Schröder T, Lukin M D, Lodahl P, Sørensen A S 2020 *Phys. Rev. X* **10** 021071

[102] Wang C, Zhang M, Chen X, Bertrand M, Shams-Ansari A, Chandrasekhar S, Winzer P, Lončar M 2018 *Nature* **562** 101

[103] Chakravarthi S, Yama N S, Abulnaga A, Huang D, Pederson C, Hestroffer K, Hatami F, de Leon N P, Fu K M C 2023 *Nano Lett.* **23** 3708

[104] Knaut C M, Suleymanzade A, Wei Y C, Assumpcao D R, Stas P J, Huan Y Q, Machielse B, Knall E N, Sutula M, Baranes G, Sinclair N, De-Eknamkul C, Levonian D S, Bhaskar M K, Park H, Lončar M, Lukin M D 2024 *Nature* **629** 573

[105] Nguyen C T, Sukachev D D, Bhaskar M K, Machielse B, Levonian D S, Knall E N, Stroganov P, Chia C, Burek M J, Riedinger R, Park H, Lončar M, Lukin M D 2019 *Phys. Rev. B* **100** 165428

[106] Sukachev D D, Sipahigil A, Nguyen C T, Bhaskar M K, Evans R E, Jelezko F, Lukin M D 2017 *Phys. Rev. Lett.* **119** 223602

[107] Wang G Y, Li T, Ai Q, Alsaedi A, Hayat T, Deng F G 2018 *Phys. Rev. Appl.* **10** 054058

[108] Ren B C, Deng F G 2017 *Opt. Express* **25** 10863

[109] Cao C, Zhang L, Han Y H, Yin P P, Fan L, Duan Y W, Zhang R 2020 *Opt. Express* **28** 2857

[110] Du F F, Ma M, Tan Q L 2024 *Adv. Quantum Technol.* **7** 2400322

[111] Dong L, Zhang X Y, Lü L, Li S Y, Zhao Z L, Yuan Z Q, Ji Y Q, Xiu X M 2025 *Opt. Laser Technol.* **186** 112583

[112] Chi Y, Yu Y, Gong Q, Wang J 2023 *Sci. China Inf. Sci.* **66** 180501

[113] Liu W Q, Wei H R, Kwek L C 2020 *Phys. Rev. Appl.* **14** 054057

[114] Deng F G, Ren B C, Li X H 2017 *Sci. Bull.* **62** 46

[115] Du F F, Ren X M, Ma M, Fan G 2024 *Opt. Lett.* **49** 1229

[116] Zeng H, Du M M, Zhong W, Zhou L, Sheng Y B 2024 *Funda. Res.* **4** 851

[117] Liu Y K, Hou Y L, Yang Y L, Hou L M, Li Y H, Lin J, Chen X F 2025 *Acta Phys. Sin.* **74** 140303 (in Chinese) [刘圆凯, 侯云龙, 杨宜霖, 侯刘敏, 李渊华, 林佳, 陈险峰 2025 物理学报 **74** 140303]

[118] Xu F, Wang M, Qiao C, Li S, Wang H, Su X 2025 *Sci. Bull.* **70** 876

[119] Yang Y G, Liu B X, Xu G B, Jiang D H, Zhou Y H, Shi W

M, Shang T 2024 *Adv. Quantum Technol.* **7** 2400016
[120] Lü M Y, Hu X M, Gong N F, Wang T J, Guo Y, Liu B H, Huang Y F, Li C F, Guo G C 2024 *Sci. China Phys. Mech. Astron.* **67** 230311
[121] Tubío V D, Dijksman M C, Borregaard J 2025 arXiv: 2505.16751 [quant-ph]
[122] Sheng Y B, Deng F G, Long G L 2010 *Phys. Rev. A* **82** 032318
[123] Wang T J, Lu Y, Long G L 2012 *Phys. Rev. A* **86** 042337
[124] Ren B C, Du F F, Deng F G 2013 *Phys. Rev. A* **88** 012302
[125] He L Y, Wang T J, Wang C 2016 *Opt. Express* **24** 15429
[126] Wang T J, Yang G Q, Wang C 2020 *Phys. Rev. A* **101** 012323
[127] Gong N F, Cai D B, Huang Z G, Qian L, Zhang R Q, Hu X M, Liu B H, Wang T J 2024 *Phys. Rev. Appl.* **22** 054045
[128] Bharos N, Markovich L, Borregaard J 2025 *Quantum* **9** 1711

SPECIAL TOPIC—Quantum information processing

Research progress of nonlocal quantum entanglement preparation based on quantum multiplexing*

LI Tao [1)†] WANG Xueqi [1)] XIE Zhihao [1)2)‡]

1) (*Engineering Research Center of Semiconductor Device Optoelectronic Hybrid Integration in Jiangsu Province, School of Physics, Nanjing University of Science and Technology, Nanjing* 210094, *China*)

2) (*National Laboratory of Solid State Microstructures, College of Engineering and Applied Sciences, Nanjing University, Nanjing* 210023, *China*)

(Received 1 May 2025; revised manuscript received 26 May 2025)

Abstract

Nonlocal quantum entanglement is a fundamental resource for future quantum networks. However, the efficiency of generating nonlocal entanglement between distant nodes is severely limited by the exponential loss incurred when locally generated entangled states are distributed through lossy quantum channels. This limitation becomes more pronounced in practical scenarios requiring the simultaneous distribution of multiple entangled pairs. Although classical multiplexing approaches, such as spatial, temporal, and frequency multiplexing, can increase the nonlocal entanglement generation rate, they do not improve the single-shot transmission efficiency. In contrast, quantum multiplexing, which can be generated by high-dimensional encoding of single photons, allows for the parallel generation of multiple nonlocal entangled pairs in a single transmission round, thereby enhancing the overall efficiency of nonlocal entanglement generation. Quantum multiplexing thus presents a promising route toward scalable quantum networks. This review introduces the mechanisms of generating nonlocal entanglement through quantum multiplexing, and focuses on two main methods: using high-dimensional single-photon encoding and high-dimensional biphoton entanglement distribution. Then it examines how quantum multiplexing can accelerate the generation of nonlocal quantum logical entanglement. Finally, it briefly explores the potential of quantum multiplexing for building large-scale quantum networks.

Keywords: quantum networks, quantum multiplexing, high-dimensional photon, parallel quantum entanglement

PACS: 03.67.Dd, 03.65.Ud, 03.67.Hk **DOI:** 10.7498/aps.74.20250589

CSTR: 32037.14.aps.74.20250589

* Project supported by the National Natural Science Foundation of China (Grant No. 11904171).

† Corresponding author. E-mail: tao.li@njust.edu.cn

‡ Corresponding author. E-mail: zhihaoxie@smail.nju.edu.cn

专题: 量子信息处理

光子集成的量子密钥分发和量子随机数生成器研究进展*

于景春[1)2)] 芦文斌[3)4)] 陈宾[1)2)] 杜永强[1)]
谢锋[1)] 李蔚[3)4)†] 韦克金[1)‡]

1) (广西大学物理科学与工程技术学院, 广西相对论天体物理重点实验室, 南宁 530004)

2) (广西大学计算机与电子信息学院, 南宁 530004)

3) (上海理工大学智能科技学院, 上海 200093)

4) (上海理工大学光子芯片研究院, 上海 200093)

(2025 年 6 月 18 日收到; 2025 年 7 月 17 日收到修改稿)

量子密钥分发凭借其信息理论层面上的无条件安全性及窃听可探测性等独特优势, 在金融、政务、国防等安全敏感领域展现出广阔的应用前景. 集成光子学技术通过将传统量子密钥分发系统的核心器件高密度集成于单一芯片, 显著提升了系统的小型化程度、成本效益与长期稳定性, 是实现量子密钥分发规模化工程应用的核心技术路径. 本文系统综述了近期基于不同材料平台与架构的光子集成量子密钥分发实验进展, 以及用于生成真随机数的集成量子随机数生成器的最新研究动态. 该综述旨在为未来芯片化量子保密通信技术的发展提供技术路线指引.

关键词: 量子密钥分发, 量子随机数, 集成光子学

PACS: 03.67.Hk, 03.67.–a, 42.82.–m **DOI:** 10.7498/aps.74.20250791

CSTR: 32037.14.aps.74.20250791

1 引 言

近年来, 量子计算领域呈现突破性发展[1–4]. 量子计算是基于量子力学原理构建的新型计算架构, 不仅具有超越经典计算的并行处理能力, 其算力更随量子比特数目的增加呈指数级提升. 这一技术演进对基于大数分解、离散对数等数学难题构建的传统密码体系 (如对称加密与非对称加密[5,6]) 构成严峻挑战.

量子密钥分发 (quantum key distribution, QKD) 是一种基于量子力学基本原理的密钥分发技术, 其安全性由量子态不可克隆原理与海森伯不确定性原理共同保障. 该技术通过物理层特征确保任何窃听行为必然扰动量子态并引入可检测误差, 结合安全认证协议可实现攻击的无条件探测, 从而在理论上提供可严格证明的通信机密性[7]. 自 1984 年首个 QKD 协议的提出[8] 及 1992 年首次 QKD 实验的实现[9] 以来, 该领域历经 40 余年发展, 在协议设计、传输距离、成码速率及实用化集成等方面持续突破. 近期, Li 等[10] 利用多像素超导纳米线单光子探测器 (SNSPD) 与硅基光子集成调制器, 在 10 km

* 国家自然科学基金 (批准号: 62171144, 62031024)、广西自然科学基金 (批准号: 2025GXNSFAA069137, GXR-1BGQ2424005) 和广西研究生教育创新计划项目 (批准号: YCBZ2024002) 资助的课题.

† 通信作者. E-mail: weil@usst.edu.cn

‡ 通信作者. E-mail: kjwei@gxu.edu.cn

光纤信道中实现了 115.8 Mbit/s 的安全成码率, 刷新世界纪录; 与此同时, 我国基于“济南一号”微纳卫星平台, 在国际上首次完成了单轨实时量子密钥分发, 并与相距 12900 km 的南非的地面站间实现了密钥生成以及“一次一密”加密传输 [11]. 这些里程碑进展标志着 QKD 技术正从原理验证阶段向高鲁棒性系统构建阶段加速迈进.

尽管 QKD 技术在传输距离与密钥速率等核心指标上取得了显著突破 [12–14], 但其大规模工程化应用仍面临显著挑战. 当前, 开发兼具小型化、低成本、高稳定性且可大规模部署的高性能 QKD 终端, 是该领域亟需攻克的关键技术瓶颈 [15,16]. 值得注意的是, 集成光子学为实现这一目标提供了颠覆性的技术路径. 该技术通过将核心光学器件 (如光源、调制器、探测器) 与驱动控制电路高密度地集成于单一芯片上, 能够从根本上减小设备体积、降低大规模制造成本, 同时显著增强系统的长期运行稳定性与鲁棒性. 近年来, 光子集成的 QKD 技术已发展成为量子保密通信领域最具活力的前沿研究方向, 其技术突破对于加速 QKD 系统的实用化进程具有变革性意义.

量子随机数生成器 (quantum random number generator, QRNG) 是量子保密通信系统中不可或缺的安全熵源. QRNG 通过利用量子物理固有的不可预测性生成真随机数, 其安全性与随机性远超依赖确定性算法的传统伪随机数生成器. QRNG 的安全性根植于量子力学基本原理, 其输出序列具备不可预测性、无偏性及不可复制性等核心特性. 依据物理熵源的差异, 主流的 QRNG 技术路线主要包括: 基于真空量子涨落的方案 [17,18]、基于单光子路径随机性的方案 [19,20]、基于光子到达时间测量不确定性的方案 [21,22] 以及基于自发辐射光子的方案 [23,24]. 其核心性能指标涵盖实时生成速率 (如$>$ 100 Gbit/s)、最小熵以及抗环境干扰的鲁棒性. 随着 QKD 系统向芯片化、集成化方向快速演进, 开发与之深度兼容的微型化集成 QRNG 芯片, 已成为突破 QKD 系统在功耗、成本与兼容性等方面瓶颈的关键路径. 近年来, 基于硅基 [25] 和磷化铟 [26] 等材料平台的单片集成 QRNG 模块研究进展显著, 已实现从理论验证到原型系统的跨越.

本文将重点回顾近期 (2022 年—2025 年) 光子集成 QKD 在不同材料平台与架构上的实验进展和集成 QRNG 的最新研究动态, 旨在为该快速发展领域提供一份及时更新的系统性综述. 更早的文献综述可参考文献 [16,27,28]. 首先, 本文系统对比分析了主流集成光子学平台的关键特性; 在此基础上, 全面梳理并评述了光子集成 QKD 技术的最新研究进展, 重点聚焦离散变量 (discrete variable, DV) 与连续变量 (continuous variable, CV) 两大技术路线的系统级实验验证案例及其性能对比. 随后, 探讨了片上集成 QRNG 的技术路线, 重点分析基于不同物理熵源的实现方案. 最后, 总结了集成光子学平台的优势及其在 QKD 系统中的应用, 并对实现芯片化、高鲁棒性集成 QKD 系统和高性能、高集成度 QRNG 的核心技术路线进行了前瞻性展望.

2 集成光量子平台

现阶段光子集成 QKD 的研究主要集中在利用成熟的微纳加工技术, 将光源、编码器、解调器和探测器等核心器件集成于单一芯片上. 主流的集成光子学平台包括硅基 (SOI)、磷化铟 (InP)、薄膜铌酸锂 (TFLN) 和氮化硅 (Si_3N_4).

SOI 平台 [29,30] 凭借硅材料固有的高折射率差 ($\Delta_n \approx 2.0$), 可实现亚微米尺度的光波导与高度微型化的功能器件, 具备显著的高集成密度优势. 该平台与成熟的互补金属氧化物半导体 (CMOS) 工艺高度兼容, 支持大规模、低成本、高良率的芯片制造, 是发展面向大规模网络部署的集成化 QKD 系统的关键技术平台. SOI 集成光子学平台卓越的 CMOS 工艺兼容性允许将光学编码单元与电子驱动电路进行单片集成, 利用载流子注入 (或耗尽) 型调制器实现超过 GHz 速率的高速量子态制备 [31], 为构建集成化、可规模化部署的 QKD 系统提供了切实可行的技术路径. 然而, 硅作为间接带隙半导体材料, 无法实现高效片上光源集成. 因此, 发展集成光源、调制器及驱动电子学的单片集成 QKD 发射芯片, 是当前该平台研究的核心挑战与热点.

区别于硅基材料, InP 等 III-V 族化合物半导体具有直接带隙特性, 更适于发展高性能集成激光光源. 同时, 得益于其非中心对称的晶体结构, 在外加电场作用下可通过线性电光效应 (普克尔斯效应) 实现折射率的精确调控, 从而完成对光信号相位、幅度的高速调制. InP 的电光系数分量 $r_{41} \approx 1.34$ pm/V(@1550 nm), 可以实现调制速率超过

40 GHz 的高速电光调制器. 此外, 其折射率调制主要受控于外电场, 几乎不引入载流子相关的扰动, 可实现近零啁啾调制. 这些性能优势使其在高速率 QKD 系统的精密相位/强度编码方案中具有重要价值. 目前已经有研究人员通过 InP 平台[32–34]将激光器、高速电光调制器进行单片集成, 为实现高度小型化、高性能的 QKD 发射端芯片提供了极具前景的技术解决方案.

尽管 SOI 和 InP 平台在构建高性能集成化 QKD 系统方面展现出显著优势, 但两者均存在一定局限性: SOI 平台受限于光源集成难题; 同时 SOI 平台和 InP 波导均有相对较高的传输损耗及其调制器通常所需的较高半波电压 ($V_\pi > 4$ V), 在一定程度上制约了集成化 QKD 系统性能的进一步提升. 在此背景下, TFLN 平台[35,36]因其卓越的线性电光特性 (Pockels 系数 $r_{33} \approx 30$ pm/V) 被认为是高性能电光调制器的重要材料平台. 基于 TFLN 平台, 目前已成功实现了兼具高速 (调制带宽>100 GHz)、低半波电压 ($V_\pi < 3$ V) 和低传播损耗 (典型值低于 0.5 dB/cm) 特性的电光调制器. 结合其优异的集成潜力, TFLN 为构建高速、稳定、紧凑且实用的 QKD 编码模块提供了关键硬件基础. 此外, TFLN 平台在实现片上集成纠缠源 (如基于自发参量下转换过程) 以及集成 SNSPD[37]方面也展现出显著潜力. 当前, TFLN 在晶圆级薄膜制备、键合与微纳加工技术方面进展迅速, 如何开发高良率、低成本的大规模生产工艺是该平台走向广泛应用的核心挑战与研究焦点.

相较而言, Si_3N_4 集成光子学平台[38–40]在 1550 nm 通信波段展现出低于 0.1 dB/cm 的超低传播损耗, 可显著降低光信号在波导中的传输衰减. 其宽光谱透明性 (覆盖可见光至近红外波段) 使其能够同时兼容 780 nm(自由空间 QKD) 和 1550 nm(光纤 QKD) 双工作波长. 这些优异的光学特性使得 Si_3N_4 平台特别适合发展低损耗的 QKD 接收端芯片, 以提高系统的量子态探测效率[41,42]. 然而, 该平台的主要挑战在于如何通过异质集成技术, 将高性能的单光子探测器 (如 SNSPD 或 InGaAs 探测器) 与基于 Si_3N_4 的解码单元高效集成, 从而构建功能完备的全集成 QKD 接收端. 克服这一异质集成难题, 实现高探测效率、低暗计数、低时间抖动探测器与低损耗光子回路的协同优化, 是当前该平台研究的重点与热点方向.

表 1 对比了目前主流的集成光子学平台, 分别从折射率、透明窗口、传输损耗、工艺成熟度、光源集成能力、探测器集成能力、调制器性能维度, 系统对比了上述平台的特性. 表中使用符号 (★) 对不同平台在各指标上的表现进行定性评价, 符号数量越多表示该平台在该特性上的性能越优.

表 1 集成光量子平台的比较

Table 1. Comparison of integrated optical quantum platforms.

对比维度	SOI	InP	TFLN	Si_3N_4
折射率 (1550 nm)	~3.48	~3.2	~2.2	~2.0
透明窗口/μm	1.1—8.0	0.9—1.7	0.4—5.0	0.25—6.00
传输损耗	★★★	★★	★★★★	★★★★★
工艺成熟度	★★★★★	★★★	★★	★★★
光源	★★★	★★★★★	★★★	★
探测器	★★★	★★★★	★★★	★★★
调制器	★★★	★★★★	★★★★★	★★

3 QKD 系统验证

基于上述集成光子学平台在 QKD 领域展现出的技术优势, 近年来, 不同研究团队致力于推动 QKD 系统中的核心器件 (包括光学与电子器件) 向集成化、芯片化方向发展. 本节将围绕不同材料平台的 QKD 演示实验展开综述, 表 2 和表 3 分别按时间顺序汇总了近 4 年 DV-QKD 和 CV-QKD 的代表性研究成果. 其中, 上标“a”表示该数值为基于文献及数据图提取的估计值, 符号“√”表示该器件实现芯片集成, “×”则表示没有实现芯片集成.

3.1 离散变量量子密钥分发 (DV-QKD)

在 DV-QKD 系统中, 密钥信息被编码于单光子的离散自由度 (如偏振、相位或路径) 上, 并通过单光子探测技术进行解码. 目前, 基于传统分立光纤光学器件的 DV-QKD 系统已成功实现千公里级光纤传输[13], 及天地一体化卫星量子通信网络.

基于前期偏振编码 QKD 系统被广泛的部署在现有网络中, 同时兼容卫星 QKD 平台, 研究人员率先实现了基于硅基光子学平台的偏振编码 QKD 的片上编码器, 并通过实验验证了其在构建高速、稳定且可扩展 QKD 系统方面的潜力[58–60]. 受限于当时芯片与器件技术水平, 这些集成 QKD 系统通

表 2 基于不同平台集成 DV-QKD 系统

Table 2. Integrate DV-QKD system based on different platforms.

文献	工艺	器件				编码方式	协议	重复频率/MHz	传输损耗/dB	平均速率/kbps
		光源	编码	解调	探测					
[43]	SI	×	√	×	×	偏振编码	BB84	312.5	20[a]	42.7
[44]	Si_3N_4	√	√	√	√	时间戳-相位编码	BB84	3350	10	12170
[45]	Si_3N_4/InP	×	√	√	×	时间戳-相位编码	BB84	1000	9.3	2370
[10]	SI	√	√	×	×	偏振编码	BB84	2500	2.2	115800
[46]	SI	×	√	√	×	偏振编码	BB84	50	18.857	0.24
[47]	SI	×	√	√	×	偏振编码	BB84	50	28.992	0.866
[48]	SI	√	√	√	×	时间戳-相位编码	BB84	2500	39.5	9.4
[49]	TFLN	×	√	√	×	时间戳-相位编码	BB84	2500	4.1	1.1×10^4
[50]	TFLN	×	√	√	×	时间戳-相位编码/相位编码	BB84	10	6.43	0.77

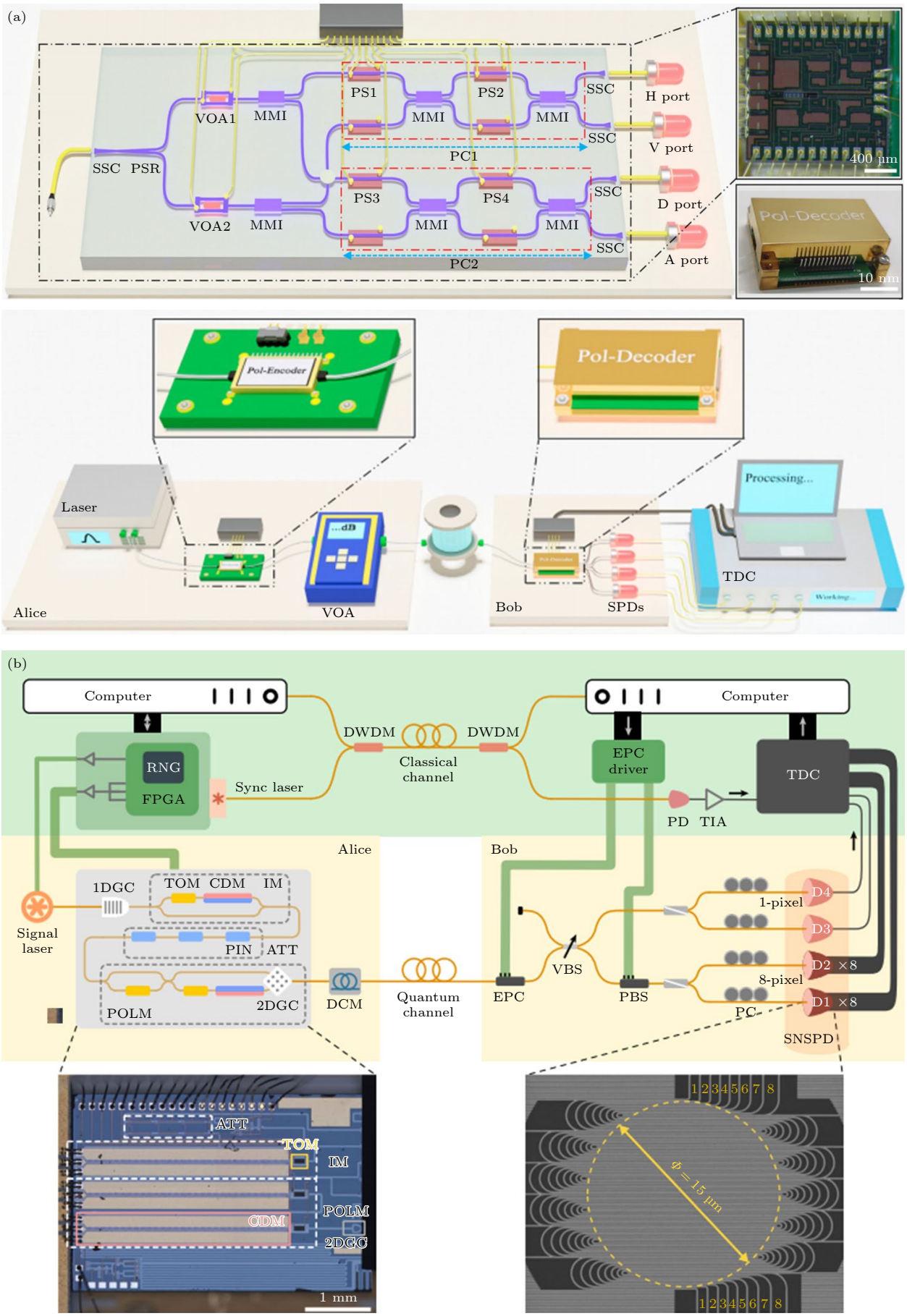
表 3 基于不同平台集成的 CV-QKD 系统

Table 3. Integrate CV-QKD system based on different platforms.

文献	工艺	器件				编码方式	协议	重复频率/ MHz	传输损耗/dB	平均速率/kbps
		光源	编码	解调	探测					
[51]	InP/Si_3N_4	√	×	×	√	相位编码	GG02	250	10[a]	750
[52]	SI	×	×	√	×	相位编码	GG02	1000	5.72[a]	1380
[53]	SI	×	×	√	√	相位编码	GG02	100	4.6	220
[54]	InP	√	√	×	×	相位编码	GG02	16	2.04	78
[55]	SI	×	√	√	√	相位编码	DM CV-QKD	10000	2[a]	3.51×10^5
[56]	SI	×	√	√	√	相位编码	DM CV-QKD	16000	4[a]	2.46×10^5
[57]	SI	×	√	√	√	偏振编码/相位编码	DM CV-QKD	20000	1.98	1.213×10^6

常依赖外部传统光学组件进行解码, 或需采用片外设备进行量子信道偏振补偿. 为攻克这一技术瓶颈, Du 等 [46] 创新性地提出了一种“偏振-路径转换”的芯片架构, 在硅基平台上实现了具备实时偏振追踪能力的硅基偏振解码器, 如图 1(a) 所示. 该团队通过实验验证了该芯片的稳定性及其对光纤偏振漂移的有效补偿能力, 最终在 100 km 光纤链路上实现了 240 bit/s 的安全密钥率. 基于此突破, Wei 等 [47] 进一步融合硅基偏振编解码器芯片, 发展了基于量子比特的异地时钟同步与偏振补偿技术, 提出了一种资源节约型的芯片级 QKD 方案. 该方案无需额外设备, 直接利用芯片制备和测量 BB84 协议所需的 4 种偏振态即可完成异地时钟同步与偏振补偿, 在 150 km 商用光纤链路上实现了 866 bit/s 密钥率, 为低成本、晶圆级制造 QKD 系统奠定了重要基础.

同时集成 QKD 系统在高速方面也有重要突破. 其中, Li 等 [10] 取得了显著进展: 他们开发了片上高速 (系统重频达 2.5 GHz)、高保真度偏振态调制技术 (量子比特误码率<0.35%); 结合尤立星团队 [10] 研制的八像素 SNSPD, 实现了高计数率 (在 5.5×10^9 光子/秒入射时) 下仍保持 62% 探测效率的单光子探测, 如图 1(b) 所示. 基于上述核心技术突破, 该团队在 10 km 标准光纤信道下实现了创纪录的 115.8 Mbit/s 安全密钥率, 较此前最高水平提升约一个数量级. 同年, Sax 等 [48] 提出了一种支持相位编码、时钟频率达 2.5 GHz 的高速集成 QKD 系统, 如图 1(c) 所示. 该系统发射端采用硅光子芯片与外部二极管激光器融合方案; 接收端则利用飞秒激光微加工技术制备了低损耗二氧化硅光子集成电路, 并外接两个单光子探测器. 最终在 202 km 光纤链路上实现了 9.4 kbit/s 的安全密钥率. 近期, Lin 等 [49] 基于 TFLN 光子集成平台, 设计并实现了双偏振时间相位编解码全集成 QKD 系统. 在 2.5 GHz 重频、25 km 传输距离下, 安全成码率高达 11 Mbit/s. Heo 等 [50] 进一步验证了 TFLN 平台相位编码 QKD 芯片的实用性, 将其部署于 32.16 km 城域实地光纤链路, 实现了 770 bit/s 安全密钥率, 证明了集成 QKD 器件在实际复杂环境中的鲁棒性.


(a)
SSC PSR
VOA1
VOA2
MMI
PS1
PS2
PS3
PS4
PC1
PC2
SSC
H port
V port
D port
A port
400 nm
Pol-Decoder
10 mm
Pol-Encoder
Laser
VOA
Alice
Bob
SPDs
TDC
Processing...
(b)
Computer
RNG
FPGA
Sync laser
DWDM
Classical channel
EPC driver
PD TIA
1DGC
TOM CDM IM
PIN ATT
POLM
2DGC
Signal laser
DCM
Quantum channel
EPC
VBS
PBS
1-pixel
8-pixel
D4
D3
D2 ×8
D1 ×8
PC
SNSPD
ATT
TOM
IM
CDM
POLM
2DGC
1 mm
1 2 3 4 5 6 7 8
Φ = 15 μm

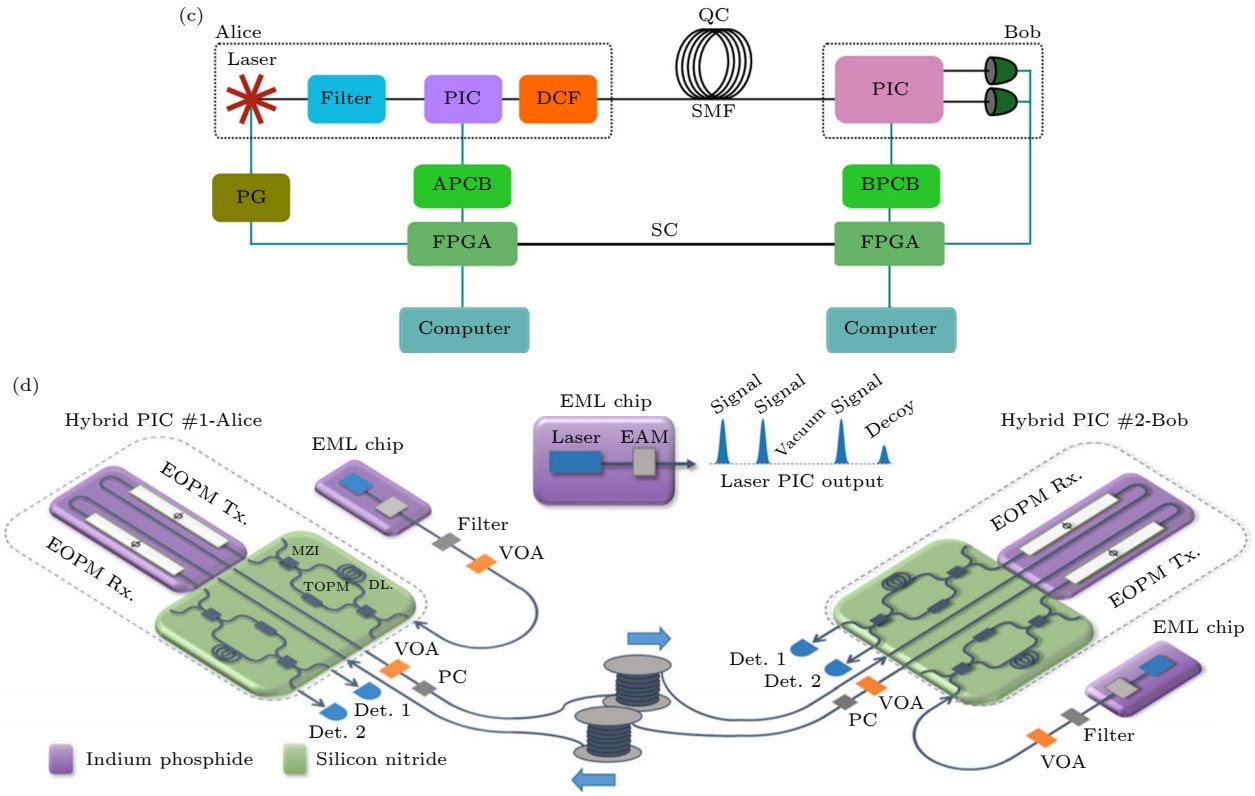


图 1 集成 DV-QKD 系统示意图 (a) 基于硅光子平台的“偏振-路径转换”芯片结构示意图[46]; (b) 基于多像素 SPSPD 的高速 QKD 系统架构图[10]; (c) 2.5 GHz 集成 QKD 系统架构图[48]; (d) 混合集成收发芯片的实验装置图[45]

Fig. 1. Schematic diagram of integrated DV-QKD systems: (a) “Polarization-path conversion” based on silicon photonics platform[46]; (b) architecture diagram of high-speed QKD system based on multi-pixel SPSPD[10]; (c) 2.5 GHz integrated QKD system architecture diagram[48]; (d) experimental setup diagram of hybrid integrated transceiver chip[45].

与此同时, 全集成 QKD 系统的研究正通过硅基光电子集成与异质集成技术持续推进. Zhu 等[43] 基于硅基光电子集成技术开发了小型化硅基发射器芯片, 在 100 km 标准光纤中实现了 42.7 kbit/s 的安全密钥率, 验证了基于集成光电器件 QKD 系统的可行性, 为 CMOS 兼容的 QKD 设备开发奠定了基础. 为克服单一材料平台实现全集成 QKD 的局限性, Dolphin 等[45] 采用混合集成策略, 将超低损耗 Si_3N_4 波导与 InP 高速电光调制器集成, 研制出 GHz 调制速率的低损耗相位编码 QKD 收发器芯片, 如图 1(d) 所示. 结合外部 InP 激光器芯片, 在 10 dB 信道衰减下实现了 1.82 Mbit/s 安全密钥率. Beutel 等[44] 则聚焦接收端集成, 基于 Si_3N_4 平台实现了全集成的四通道波分复用型 QKD 接收芯片, 并成功集成 SNSPD. 该系统在 10 dB 信道衰减下实现了高达 12.17 Mbit/s 的密钥率, 标志着全集成接收芯片技术的重大突破.

3.2 连续变量量子密钥分发 (CV-QKD)

CV-QKD 将密钥信息编码于光场量子态的正交分量上, 并通过相干检测进行解码. 其核心优势在于与现有光通信基础设施的高度兼容性. 近年来, CV-QKD 在协议设计、安全性分析及系统实现方面取得了显著进展, 已成功实现高速安全密钥产生 (如 190 Mbit/s[61]) 和城域网应用探索[62].

与 DV-QKD 类似, 面向大规模部署的实用化 CV-QKD 系统同样依赖于光学芯片集成技术以实现小型化、低成本和高稳定性. 该领域的里程碑工作由 Zhang 等[63] 于 2019 年首次完成. 该团队基于硅基光子平台, 研制了全集成的 CV-QKD 发射器与接收器芯片, 集成了相位调制器、强度调制器、可变光衰减器及零差探测器等关键功能单元, 如图 2 所示. 利用该集成系统, 研究者在 100 km 光纤传输距离下实现了 140 bit/s 的安全密钥率. 这项成果为集成 CV-QKD 系统奠定了坚实基础.

基于本地本振 (LLO) 方案的 CV-QKD 系统展现出解决长距离传输挑战的潜力: 该方案能够保证量子信号在长距离传输后实现量子噪声极限探测, 并通过物理隔离的本振光有效抑制信号串扰, 从而

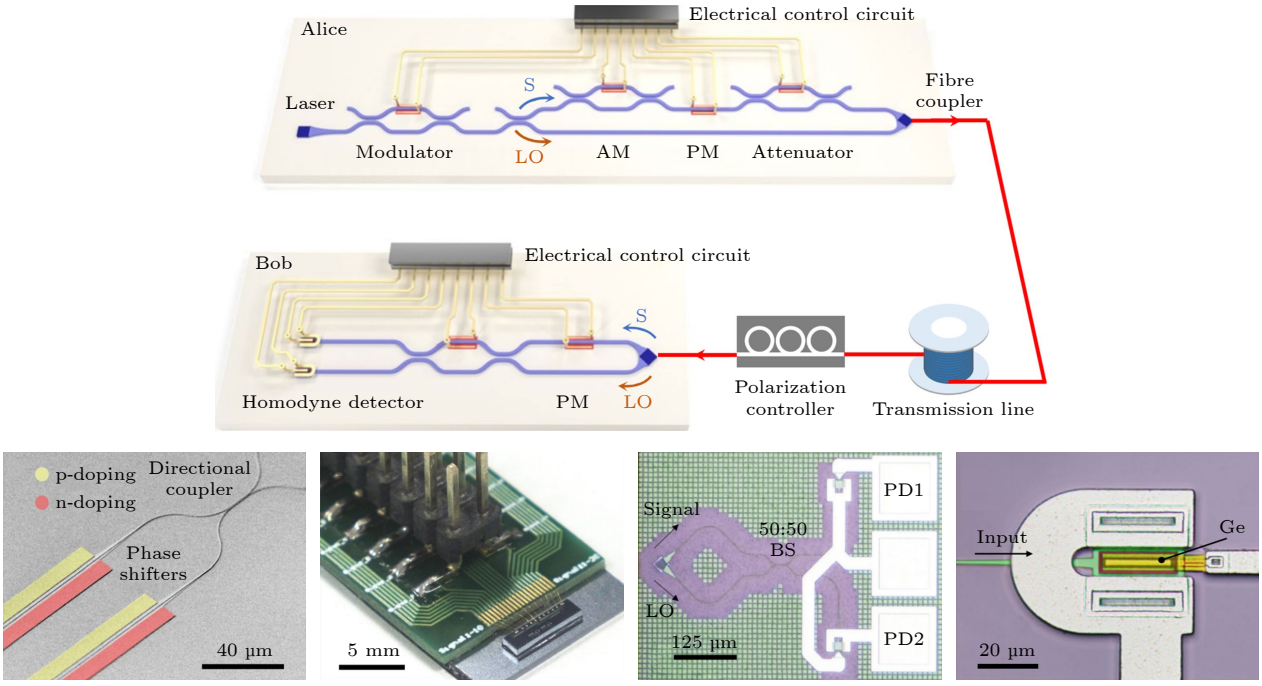


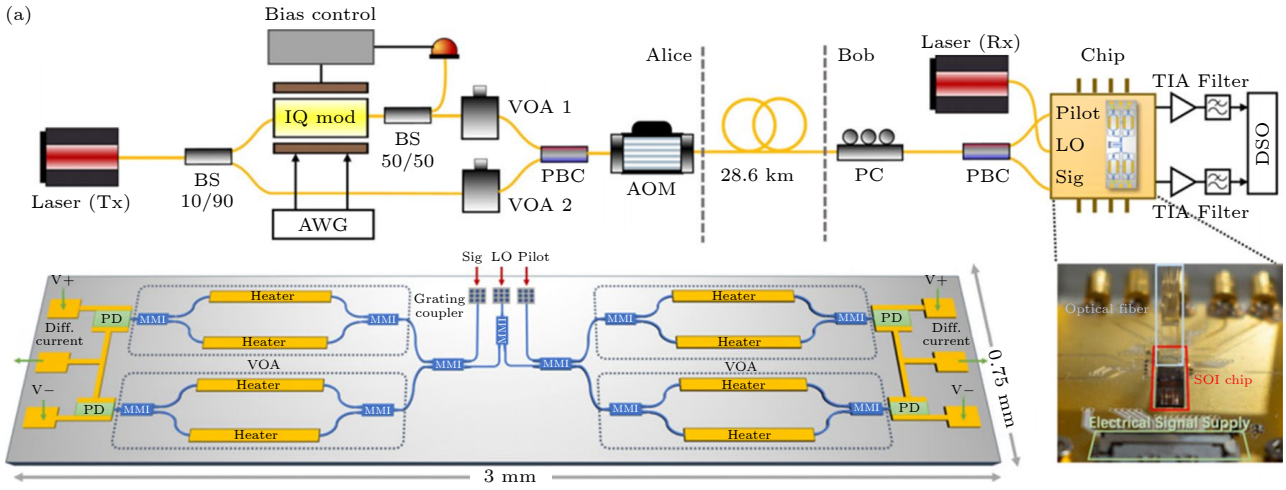
图 2 基于硅光子平台的集成 CV-QKD 系统示意图及该集成芯片的电子显微镜和光学显微镜图像[63]

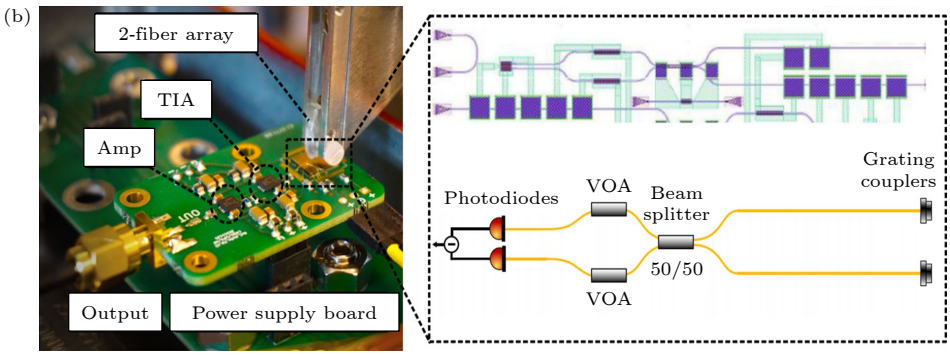
Fig. 2. Schematic diagram of the integrated CV-QKD system based on the silicon photonics platform and electron microscope and optical microscope images of the integrated chip[63].

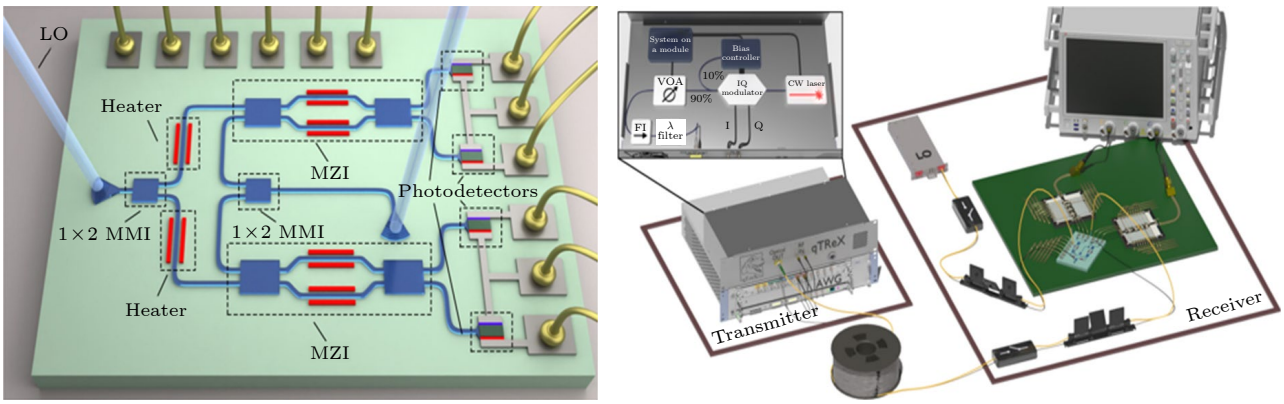
实现高性能、长距离的安全密钥分发. 因此, LLO 方案已成为当前集成 CV-QKD 系统研究的重点方向之一. Bian 等[52] 基于标准绝缘体上硅光子集成平台, 开发了一款 LLO 方案的 CV-QKD 接收器芯片 (尺寸: 3 mm × 0.75 mm), 如图 3(a) 所示. 在 28.6 km 光纤链路上, 该芯片实现了 1.38 Mbit/s 的渐近密钥率, 显著推动了集成 CV-QKD 系统在较长通信距离下实现高密钥速率的研究进程. 随后, Piétri 等[53] 也报道了一种硅基集成 CV-QKD 接收器芯片. 该接收器由光子芯片 (包含采用硅锗工艺制造的平衡零差探测器) 与信号放大电路构成, 如图 3(b) 所示. 在 10 km 和 23 km 距离的仿真实验中, 渐进密钥率分别达到 2.4 Mbit/s 和 0.22 Mbit/s, 这证明了该方案在实现高速、安全通信的全集成设备方面具有潜力.

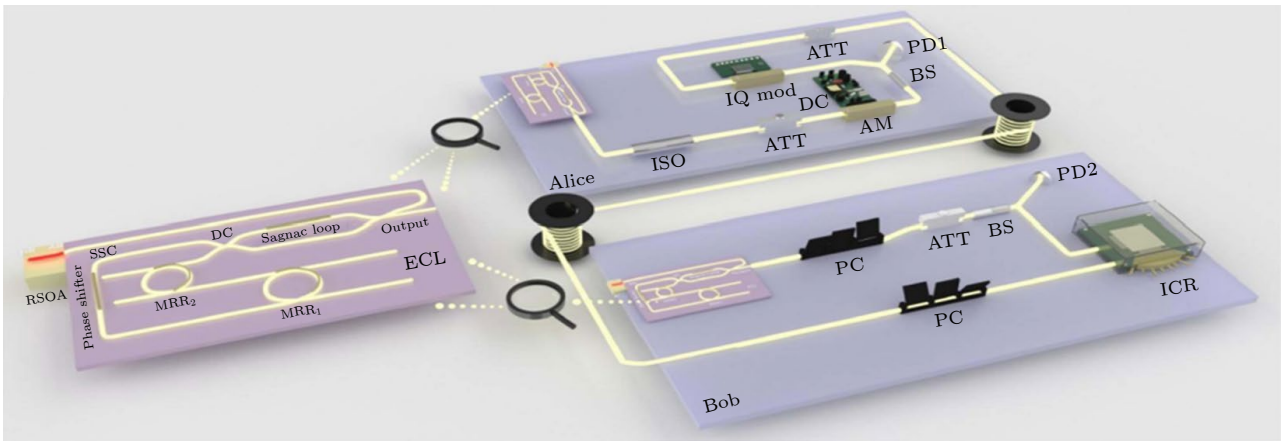
为突破集成 CV-QKD 接收器带宽限制、实现更高安全密钥率, Hajomer 等[55] 提出并实现了一种高性能硅光子集成 CV-QKD 接收器芯片, 如图 3(c) 所示. 该系统采用高带宽集成器件和低噪声设计, 成功在 20 GHz 检测速率下观测到散粒噪声极限特性. 基于此接收器, 在 10 GBaud 符号速率、5 km 光纤距离下实现了 737 Mbit/s 的渐近密钥率, 在 10 km 距离下密钥率可达 315 Mbit/s. 一年后, Hajomer 等[56] 进一步优化系统, 在 16 GBaud 符号速率、20 km 光纤链路条件下, 将渐近密钥率与有限长密钥率分别提升至 289 Mbit/s 与 246 Mbit/s. Ng 等[57] 提出了一种基于硅基集成的 CV-QKD 收发系统, 除激光源外, 所有核心光学组件均实现芯片级集成. 其中发射端采用双偏振复用架构, 通过偏振正交信道并行传输, 将符号率有效提升至 40 Gbaud/s (等效 20 Gbaud/s per polarization). 接收端结合宽带平衡零差探测器与实时数字信号处理技术 (集成色散补偿、导频辅助载波相位恢复等算法), 支持 40 Gbaud/s 超高速量子态测量. 实验基于离散调制 CV-QKD 协议, 在 10 km 光纤链路上实现了高达 1.213 Gbit/s 的密钥速率. 这一系列成果标志着基于光子集成的 CV-QKD 系统向可扩展、经济高效及大规模部署的量子安全通信网络迈出了关键一步.

尽管上述工作在高速率、远距离集成 CV-QKD 方面取得了显著进展, 片上高性能量子光源的实现仍面临重大挑战. 特别是基于 LLO 的 CV-QKD 方案, 对片上光源提出了更高要求, 亟需同时满足高频率调谐性、高输出功率及窄线宽等关键特性. 近期, Li 等[51] 在此方向取得突破: 通过片上集成 Ⅲ-Ⅴ族激光器与低损耗 Si_3N_4 微腔耦合, 如图 3(d)


(a)
Bias control
IQ mod
BS 50/50
VOA 1
VOA 2
PBC
AOM
Alice
Bob
28.6 km
PC
Laser (Rx)
PBC
Chip
Pilot
LO
Sig
TIA Filter
TIA Filter
DSO
Laser (Tx)
BS 10/90
AWG
Sig LO Pilot
Grating coupler
Heater
MMI
PD
VOA
Diff. current
V+
V−
3 mm
0.75 mm
Optical fiber
SOI chip
Electrical Signal Supply


(b)
2-fiber array
TIA
Amp
Output
Power supply board
Photodiodes
VOA
Beam splitter
50/50
VOA
Grating couplers


(c)
LO
Heater
MZI
Photodetectors
1×2 MMI
1×2 MMI
Heater
MZI
Transmitter
Receiver


(d)
ATT
PD1
BS
IQ mod
DC
AM
ATT
ISO
Alice
PD2
ATT
BS
PC
ICR
PC
Bob
SSC
DC
Sagnac loop
Output
ECL
RSOA
Phase shifter
MRR2
MRR1

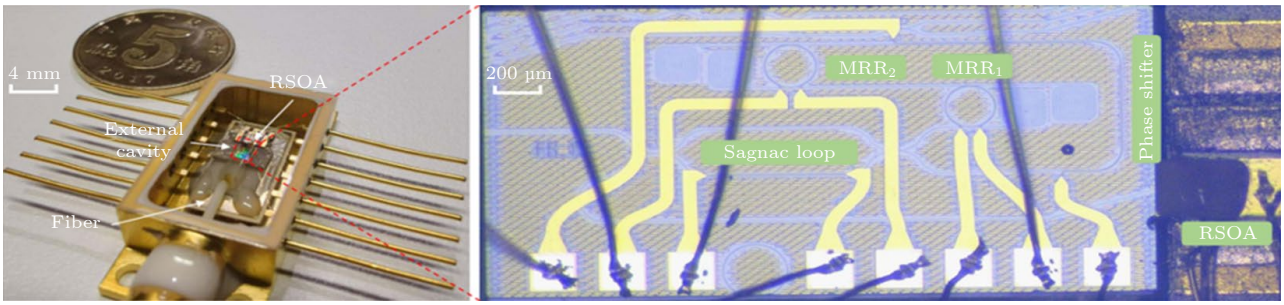
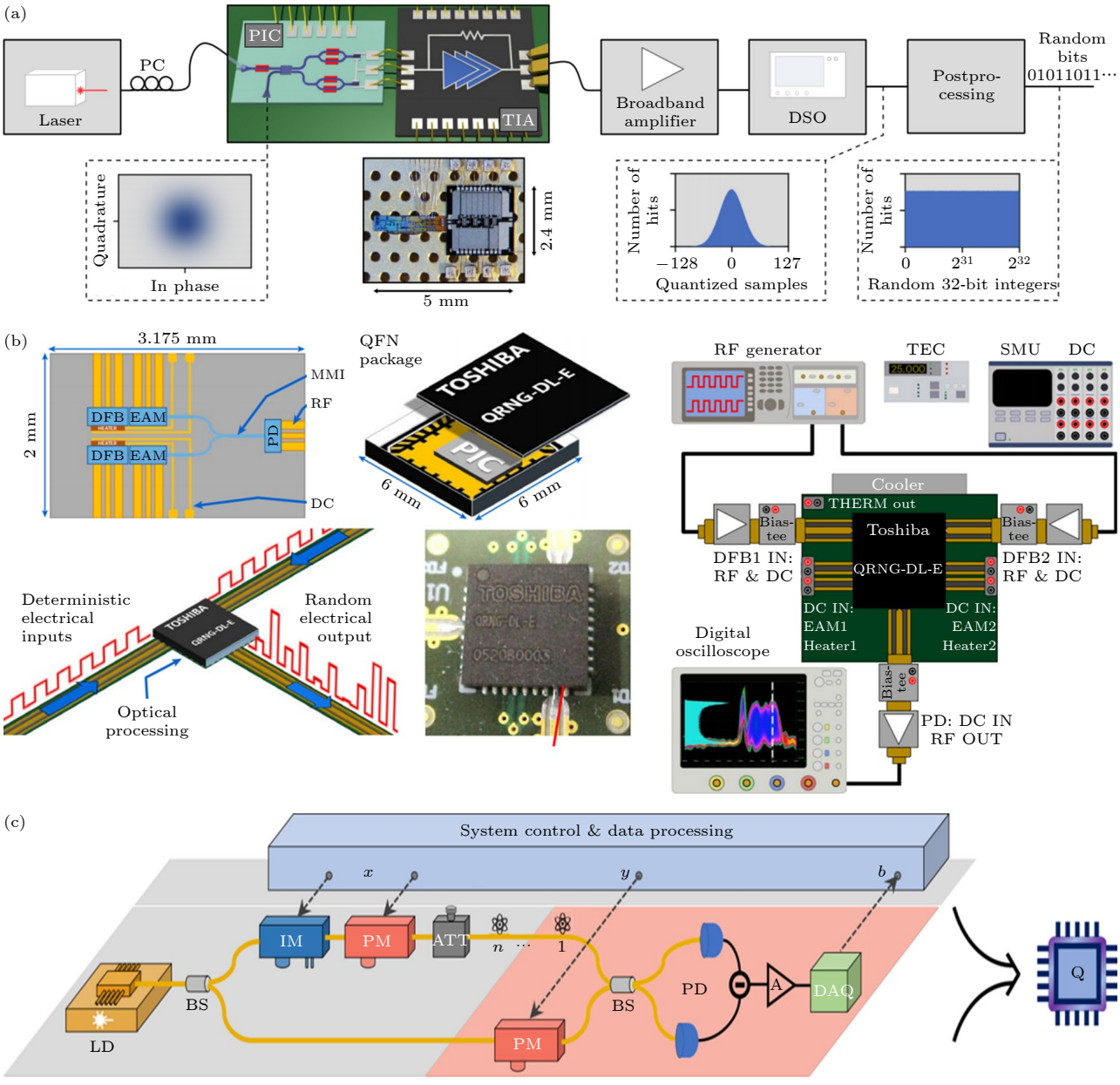


图 3 集成 CV-QKD 系统示意图 (a) 基于硅基集成的 CV-QKD 接收平台[52]; (b) 基于硅基集成的 CV-QKD 接收器芯片[53]; (c) 基于硅基集成的 CV-QKD 接收器结构图及该 CV-QKD 系统[55]; (d) 基于 Ⅲ-Ⅴ/Si_3N_4 的片上激光器[51]

Fig. 3. Schematic diagrams of integrated CV-QKD systems: (a) CV-QKD receiving platform based on silicon-based integration[52]; (b) CV-QKD receiver chip based on silicon-based integration[53]; (c) schematic diagram of the CV-QKD receiver based on silicon-based integration and the CV-QKD system[55]; (d) Ⅲ-Ⅴ/Si_3N_4-based on-chip lasers[51].



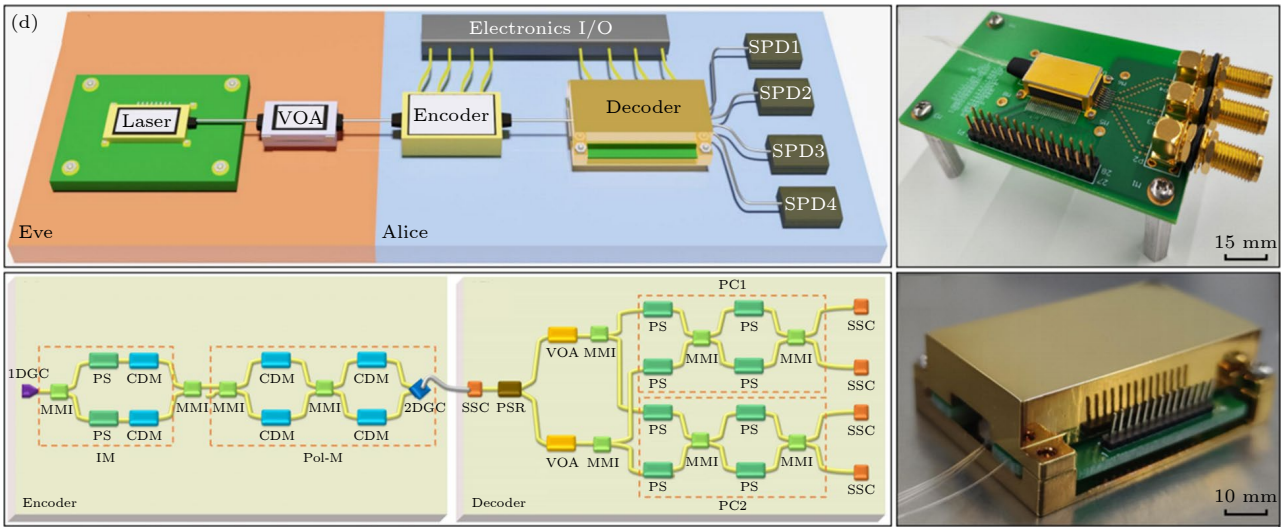


图 4 集成 QRNG 系统示例 (a) 基于硅基集成芯片的完全可信 QRNG 系统[66]; (b) 基于 InP 光学平台的集成 QRNG 系统[26]; (c) 基于自制零差检测器的实验系统[64]; (d) 基于硅基集成芯片的 SI-QRNG 系统[68]

Fig. 4. Examples of integrated quantum random number generator systems: (a) a fully trusted QRNG system based on silicon-based integrated chips[66]; (b) an integrated QRNG system based on an InP optical platform[26]; (c) experimental systems based on self-made aberration detectors[64]; (d) SI-QRNG system based on silicon-based integrated chips[68].

所示, 实现了 1.6 kHz 的超窄线宽激光输出; 进一步利用双微环腔的游标卡尺效应, 获得了超过 70 nm 的宽调谐范围, 且边模抑制比达到 75 dB. 基于该高性能集成光源, 该团队成功演示了超过 100 km 的长距离 QKD 实验.

除硅基平台外, 其他材料体系 (如 InP) 的集成研究也在推进. Aldama 等[54] 提出并实现了一种基于 InP 集成平台的 CV-QKD 发射器芯片, 集成了电吸收调制器、相位调制器和可变光衰减器等组件. 在实验中采用片外激光源, 在 11 km 超低损光纤链路上实现了 0.078 Mbit/s 的渐近密钥率.

4 量子随机数生成器 (QRNG)

QRNG 基于量子力学的不确定性原理, 能够生成具备内在随机性的真随机数, 为 QKD 系统提供高安全性密钥. 典型的 QRNG 由产生量子态的熵源和探测该量子态并输出随机比特的测量装置构成. 当前, 根据对设备的信任程度, QRNG 分为完全可信、设备无关 (DI) 和半设备无关 (Semi-DI) 三类. 得益于高质量光学元件的成熟与光子集成技术的潜力, QRNG 在量子熵源与探测器的小型化方面均取得了显著进展. 表 4 按时间顺序梳理了近期集成 QRNG 的技术进展.

在完全可信的 QRNG 中, 包括光源、探测器在内的所有设备均被视为完全可信且经过精确校准. 随机性源于量子过程, 如单光子探测、真空涨落或激光相位噪声等. 随机数生成速率是 QRNG 的核心性能指标之一, 其瓶颈主要受限于探测器的死区时间、探测效率、量子熵源特性、信号处理链路带宽以及环境噪声等因素. 为突破速率瓶颈, Bruynsteen 等[66] 提出了一种基于硅光子集成芯片的集成化 QRNG 方案, 该方案以真空噪声为熵源, 通过定制化光电集成电路协同设计, 集成了高速平衡零差探测器, 如图 4(a) 所示. 另外还提出了一个设备依赖性安全框架, 该框架能同时抵御经典侧信道信息 (如电子学噪声) 和量子侧信道信息 (如环境纠缠) 的影响, 充分考虑了模数转换器数字化过程中的非线性效应; 实验最终实现了创纪录的 100 Gbit/s 真随机数生成速率. 区别于传统的单通道真空噪声熵源设计, Tanizawa 等[69] 提出了一种基于空间复用的 QRNG 方案. 该方案利用二氧化硅平面光波导电路分束器构建了多通道并行探测架构, 由单个激光二极管驱动多通道平衡零差探测器, 实现了对 4 个通道真空涨落的并行探测, 并采用 FPGA 进行数据的并行处理. 实验验证表明, 该系统的随机数生成速率达到 50 Gbit/s, 且在连续 1 h 运行中, 其输出数据的相对标准偏差小于 1%. 这两项研究显著提升了 QRNG 在高速应用场景下的性能.

随着集成 QRNG 的生成速率不断提升, 其集成度、稳定性及功耗已成为当前的研究热点. 现

表 4 基于不同平台的集成 QRNG

Table 4. Integrated QRNG based on different platforms.

文献	工艺	熵源	设备信任	探测	采样方式	生成速率/Mbps
[64]	SI	真空噪声	测量设备无关	零差探测	FPGA(实时)	—
[65]	InP	自发辐射相位噪声	完全可信	光电探测	示波器(离线)	6110
[66]	SI	真空噪声	完全可信	零差探测	示波器(离线)	1×10^5
[67]	SI	真空态涨落	源设备无关	零差探测	示波器(离线)	146.2
[68]	SI	光子偏振态	源设备无关	单光子探测	单光子探测器+时间数字转换器(离线)	4.04
[69]	SiO_2	真空噪声	完全可信	零差探测	FPGA(实时)	5×10^4
[70]	SI/InP	真空噪声	完全可信	零差探测	FPGA(实时)	1.02
[26]	InP	真空态涨落	完全可信	光电探测	FPGA(实时)	2×10^3
[71]	SI	真空噪声	源设备无关	零差探测	FPGA(实时)	2×10^4
[25]	SI	光子偏振态	源设备无关	单光子探测	单光子探测器+时间数字转换器(离线)	9.49
[72]	SI	真空态涨落	源设备无关	外差探测	示波器(离线)	20212

注: 表中所有基于不同平台集成的QRNG工作均采用了“Toeplitz Hashing”后处理技术.

有的基于硅光子平台的 QRNG 通常需要外接激光器, 难以实现真正的单片集成系统. 针对此问题, Wang 等[70] 研制出一种混合集成芯片的紧凑型 QRNG. 该芯片集成了 InP 激光二极管与硅光子芯片, 并采用对称的 1 × 2 多模干涉仪结构, 实现了大于 40 dB 的共模抑制比. 系统采用锗硅光电二极管构建平衡零差探测器, 在 1 μA 光电流条件下获得了约 9 dB 的量子噪声与经典噪声功率比. 最终该系统在 80 mW 的低功耗下实现了 1.02 Mbit/s 的随机数生成速率, 显著提升了集成 QRNG 的实用化性能. Chrysostomidis 等[65] 则展示了一种基于 InP 光子集成平台的集成 QRNG 芯片. 该芯片集成了两个分布式布拉格反射镜 (DBR) 激光器、一个平衡马赫-曾德尔干涉仪 (MZI) 用于功率分配、一个非平衡 MZI 及一个高速光电探测器. 其中一个 DBR 激光器产生的相位扩散作为量子熵源, 通过非平衡 MZI 将相位随机波动转化为强度波动, 实现高速随机数生成. 在 300 min 测试中, 去除经典噪声后, 芯片输出的最小熵均值保持稳定 (标准差 $\sigma = 0.053$), 随机数生成速率达 6.11 Gbit/s. 近期, Marangon 等[26] 开发出一种基于 InP 光子集成芯片的 QRNG. 其核心是一个紧凑封装 (6 mm × 6 mm) 的光学熵源模块, 如图 4(b) 所示, 该模块集成了完整的片上光学组件 (包含激光器、电吸收调制器、多模干涉仪和探测器). 该方案利用双激光增益开关产生的相位随机化光脉冲在多模干涉仪处干涉作为量子熵源. 在非受控环境中连续运行 38 天后, 该集成 QRNG 输出的物理随机性特征变化极小 (基于超过 2.9×10^6 个采集直方图的分析, 总变差距离均值为 0.007, 标准差为 0.003), 展现出优异的长期稳定性. 通过实时监测和参数调整, 该系统能稳定地以 2 Gbit/s 的速率生成随机数.

在 SDI-QRNG 框架下, 根据测量设备和源的可信与否, 可进一步细分为源无关 QRNG(SI-QRNG) 和测量设备无关 QRNG(MDI-QRNG). 传统的完全可信 QRNG 通常需要精确校准测量设备以完成安全性分析, 而设备表征的困难不仅带来实验挑战, 还可能引入潜在的侧信道漏洞, 危及安全性. 为解决测量设备表征难题, Wang 等[64] 提出并实验演示了一种新型半设备无关量子随机性扩展协议. 该协议完全移除了对测量设备 (零差探测器) 的校准要求, 并严格考虑了有限尺寸效应, 同时移除了测量过程的独立同分布假设, 具备自测试特性和可证明的安全性. 重要的是, 该协议仅使用标准光学元件, 在硅光子集成平台上易于实现. 为验证协议可行性, 研究人员搭建了基于自制高效率零差检测器 (1550 nm 处有效效率达 91.7%) 的光纤实验系统, 如图 4(c) 所示. 系统工作在 2.5 MHz 重复频率下, 在完成 10^{10} 轮协议执行后, 成功实现了 4.98 kbit/s 的净随机性扩展率. 这一成果为发展具有自测试特性和可证明安全性的集成化 QRNG 铺平了道路.

SI-QRNG 的核心假设是随机源不可信, 而测量设备可信. 其核心思想是利用测量结果实时监控源的状态. 这通常需要在不同的 (常为互补的) 测量基之间随机切换, 使得源 (假定受对手控制) 无

法预知后续测量. 传统芯片级 QRNG 依赖量子源 (如真空涨落) 产生随机数, 但量子源本身存在被攻击者操控的风险 (例如通过注入恶意光信号), 可能导致随机数可预测, 构成严重安全威胁. 针对此挑战, Du 等[25] 提出一个基于硅基集成芯片的离散变量 SI-QRNG 方案, 利用 FPGA 控制不可信激光源与硅基偏振解码器芯片, 通过共轭基 (如 X 基和 Z 基) 实时监测光源状态, 实现光子偏振态的片上解码测量. 随后在实验中, 该系统的安全随机数生成速率最高可达 9.49 Mbit/s, 成功展示了基于硅集成芯片的 QRNG 在集成度、速度和安全性间的良好平衡. 集成 SI-QRNG 虽发展迅速, 但其安全性仍依赖测量设备的可信性及精确表征, 实际器件的缺陷会直接影响随机数质量. 为了解决这个问题, Zhao 等[68] 提出了一个基于硅基集成芯片的高安全性的 SI-QRNG, 可从不可信光源和未表征测量设备中提取安全随机数. 不可信源采用基于商用激光器, 实验装置如图 4(d) 所示. 经参数优化 (平均光子数 $\mu = 19.33$), 随机数生成速率达 4.04 Mbit/s, 为开发高安全性、低成本和小型化随机数生成系统提供了有效途径.

在确保安全性的前提下, 为实现高速率的集成 SI-QRNG, 近期研究也在基于连续变量方案的集成 QRNG 方面取得了显著突破. Li 等[67] 提出并实现了一种集成化硅光子芯片 QRNG 方案. 该方案的核心在于利用片上相位调制器随机切换测量基, 并结合为实际芯片环境 (不可拆卸、存在非理想因素) 设计的量子条件最小熵评估框架来保障安全性. 通过实现高带宽 (裸片 27.7 GHz)、低失真的片上锗探测器以及低半波电压 (3.7 V) 的高精度片上相位调制器, 该芯片系统成功实现了 146.2 Mbit/s 的安全随机数生成速率, 其裸片理论极限速率高达 248.47 Gbit/s. 此项工作为 QRNG 在通信、加密等场景的大规模应用奠定了重要基础. Bertapelle 等[72] 也提出了一种基于硅光子学平台的集成 QRNG 方案, 其安全随机数生成速率超过 20 Gbit/s. 该方案将系统分为量子源和外差接收器两个子系统, 其中量子源被视为不可信 (由潜在攻击者控制), 而外差接收器则完全可信并经过严格表征. 研究人员采用 220 nm 绝缘体上硅技术制造了单片光子集成电路, 集成了的 4 × 4 多模干涉仪作为 90°光学混频器, 无需主动相位反馈控制. 实验中以外部 1550 nm 分布反馈激光器作为本振. 在最大本振功率 (~21 mW) 下, 测得量子条件最小熵 $H_{\min(\mathrm{X|E})}$ 下限为 (10.106 ± 0.005) B, 据此提取的安全生成速率达 20.212 Gbit/s. 此外, Bian 等[71] 基于硅光子平台构建的集成 QRNG 实现了 20 Gbit/s 实时生成速率. 该系统将除光源外的核心组件集成于单片硅光子芯片之上, 充分展示了硅光子集成电路技术在实现高速生成随机数方面的潜力.

5 总结与展望

本文系统综述了光子集成 QKD 与集成 QRNG 领域近年来的突破性进展. 通过实现微型化设计、提升稳定性、降低成本、优化性能并增强安全性, 集成光子学平台成为推动 QKD 和 QRNG 从实验室走向大规模应用的关键使能技术. 在 QKD 的系统验证与 QRNG 的研究中, DV-QKD, CV-QKD 以及 QRNG 在光子集成层面的关键突破, 有效推动了相关系统在密钥生成速率、传输距离及运行稳定性等核心性能指标上的显著提升. 尽管该领域已积累丰硕的研究成果, 未来仍面临若干关键挑战.

1) QKD 系统实际安全性分析: QKD 系统在理论上具备无条件安全性, 但实际工程实现中器件的非理想特性 (如光源频率与强度抖动、探测器后脉冲、器件参数与理论模型的偏差) 为窃听者引入了潜在的攻击面. 虽然已有针对上述问题的安全性研究[73–75], 然而, 随着 QKD 系统向集成化、芯片化架构演进以及新型光电器件材料 (如硅光子集成芯片、SNSPD) 的应用, 新型安全威胁持续涌现[76–79](例如量子态制备误差和高速调制引入制备不准确、硅光子强度调制器中的双光子吸收效应会引入漏洞等). 因此, 对集成 QKD 系统进行全面且深入的实际安全性分析, 并据此设计出鲁棒性更强的工程化系统, 是推进其大规模实用化的关键环节.

2) 前沿 QKD 协议的片上实现: 当前基于集成光子芯片的 QKD 研究主要集中于 BB84、测量设备无关等经典协议. 然而, 集成光子技术在器件小型化、功能模块化及系统低功耗化方面的突破性进展, 为新型 QKD 协议提供了极具潜力的实施平台. 相较于经典协议, 例如: 具备长距离成码能力的双场 QKD(TF-QKD) 协议[13,80], 具有低系统复杂度的模式匹配 QKD(MP-QKD) 协议[81,82], 以及具有强抗噪能力的高维 QKD(HD-QKD) 协议[83,84] 等.

这些新型协议的片上实现不仅能突破传统协议在安全密钥率、传输距离及抗环境噪声能力上的固有局限, 还可为未来量子中继、多用户量子网络等先进架构提供技术支撑. 因此, 亟需将更多研究精力投向新型 QKD 协议的集成化实现与性能验证, 以充分释放集成光子平台在协议创新方面的巨大潜力.

3) 实用化全集成 QKD 系统实现: 当前集成化 QKD 系统已从分立器件向芯片级集成迈进, 然而, 实现工程实用化的全单片集成架构仍存在显著挑战. 关键瓶颈包括: 实现基于Ⅲ-Ⅴ族材料的高性能激光器、高速量子态调制器及其驱动电路的高效异质/异构集成; 实现低损耗量子态测量单元与高性能单光子探测器 (如 SNSPD) 在单片或先进封装平台上的协同集成. 攻克上述挑战, 亟需在跨材料体系低温集成技术、晶圆级缺陷检测与工艺控制、低功耗高速调制驱动电路设计以及统一的性能测试等方面取得突破.

4) 集成 QRNG(高性能与高集成度) 的协同优化: 集成 QRNG 当前面临的核心挑战源于硅基平台与 InP 平台的技术特性差异. 硅基平台凭借成熟的 CMOS 兼容性, 易于集成电子逻辑处理单元 (如 SPAD 阵列及后处理电路), 但其光源的非理想性及探测器性能局限 (如暗计数、后脉冲效应), 制约了随机数生成速率的提升; 而 InP 平台虽在量子态制备与操控及相干检测上优势显著 (支持>10 Gbit/s 的高带宽), 却由于Ⅲ-Ⅴ族材料与硅基电子元件的工艺失配, 在高速跨阻放大器 (TIA)、模数转换器 (ADC)、及后处理电路的片上集成方面面临严峻挑战. 为此, 电子-光子异构集成与探测链路优化成为关键突破方向: 通过硅光互连技术 (如混合键合) 实现 InP 光子芯片与硅电子芯片的高效协同集成; 采用 SiGe BiCMOS 工艺开发低功耗宽带 TIA 以抑制噪声; 同时探索光子辅助 ADC 方案 (如光频梳采样) 替代传统电子转换以突破采样率瓶颈.

总之, 集成光学芯片技术是推动量子保密通信从实验室走向大规模实际应用的核心使能技术. 尽管挑战犹存, 该领域持续涌现的创新成果正不断夯实其技术基础. 随着材料、工艺、设计和系统集成能力的协同进步, 集成量子保密通信技术有望在构建未来高度安全的信息基础设施中扮演至关重要的角色.

参考文献

[1] Proctor T, Young K, Baczewski A D, Blume Kohout R 2025 *Nat. Rev. Phys.* **7** 105
[2] Fauseweh B 2024 *Nat. Commun.* **15** 2123
[3] Proctor T, Rudinger K, Young K, Nielsen E, Blume Kohout R 2022 *Nat. Phys.* **18** 75
[4] Ding X, Guo Y P, Xu M C, Liu R Z, Zou G Y, Zhao J Y, Ge Z X, Zhang Q H, Liu H L, Wang L J, Chen M C, Wang H, He Y M, Huo Y H, Lu C Y, Pan J W 2025 *Nat. Photonics* **19** 387
[5] Fujisaki E, Okamoto T 1999 *19th Annual International Cryptology Conference* Santa Barbara, California, USA, August 15–19, 1999 p537
[6] Simmons G J 1979 *ACM Comput. Surv.* **11** 305
[7] Akter M S, Rodriguez C J, Shahriar H, Cuzzocrea A, Wu F 2023 *IEEE International Conference on Big Data (BigData)* Sorrento, Italy, December 15–18, 2023 p5408
[8] Bennett C H, Brassard G 1984 *Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing* Bangalore, India, December 10–12, 1984 p175
[9] Bennett C H, Bessette F, Brassard G, Salvail L, Smolin J 1992 *J. Cryptol* **5** 3
[10] Li W, Zhang L K, Tan H, Lu Y C, Liao S K, Huang J, Li H, Wang Z, Mao H K, Yan B Z, Li Q, Liu Y, Zhang Q, Peng C Z, You L X, Xu F H, Pan J W 2023 *Nat. Photonics* **17** 416
[11] Li Y, Cai W Q, Ren J G, Wang C Z, Yang M, Zhang L, Wu H Y, Chang L, Wu J C, Jin B, Xue H J, Li X J, Liu H, Yu G W, Tao X Y, Chen T, Liu C F, Luo W B, Zhou J, Yong H L, Li Y H, Li F Z, Jiang C, Chen H Z, Wu C, Tong X H, Xie S J, Zhou F, Liu W Y, Ismail Y, Petruccione F, Liu N L, Li L, Xu F, Cao Y, Yin J, Shu R, Wang X B, Zhang Q, Wang J Y, Liao S K, Peng C Z, Pan J W 2025 *Nature* **640** 47
[12] Li W, Zhang L K, Lu Y C, Li Z P, Jiang C, Liu Y, Huang J, Li H, Wang Z, Wang X B, Zhang Q, You L X, Xu F H, Pan J W 2023 *Phys. Rev. Lett.* **130** 250802
[13] Liu Y, Zhang W J, Jiang C, Chen J P, Zhang C, Pan W X, Ma D, Dong H, Xiong J M, Zhang C J, Li H, Wang R C, Wu J, Chen T Y, You L X, Wang X B, Zhang Q, Pan J W 2023 *Phys. Rev. Lett.* **130** 210801
[14] Zhang L K, Li W, Pan J W, Lu Y C, Li W W, Li Z P, Huang Y Z, Ma X F, Xu F H, Pan J W 2025 *Phys. Rev. X* **15** 021037
[15] Diamanti E, Lo H K, Qi B, Yuan Z L 2016 *npj Quantum Inf.* **2** 16025
[16] Liu Q, Huang Y M, Du Y Q, Zhao Z G, Geng M M, Zhang Z R, Wei K J 2022 *Entropy* **24** 1334
[17] Gabriel C, Wittmann C, Sych D, Dong R F, Mauerer W, Andersen U L, Marquardt C, Leuchs G 2010 *Nat. Photonics* **4** 711
[18] Zheng Z Y, Zhang Y C, Huang W N, Yu S, Guo H 2019 *Rev. Sci. Instrum.* **90** 043105
[19] Jennewein T, Achleitner U, Weihs G, Weinfurter H, Zeilinger A 2000 *Rev. Sci. Instrum.* **71** 1675
[20] Ren M, Wu E, Liang Y, Jian Y, Wu G, Zeng H P 2011 *Phys. Rev. A* **83** 023820
[21] Wayne M A, Kwiat P G 2010 *Opt. Express* **18** 9351
[22] Wahl M, Leifgen M, Berlin M, Röhlicke T, Rahn H J, Benson O 2011 *Appl. Phys. Lett.* **98** 171105
[23] Guo Y, Cai Q, Li P, Jia Z W, Xu B J, Zhang Q W, Zhang Y M, Zhang R N, Gao Z S, Shore K A, Wang Y C 2021 *APL Photonics* **6** 066105
[24] Wei S H, Yang J, Fan F, Huang W, Li D S, Xu B J 2017

Rev. Sci. Instrum. **88** 123115
[25] Du Y Q, Hua X, Zhao Z G, Sun X R, Zhang Z R, Xiao X, Wei K J 2025 *Commun. Phys.* **8** 9
[26] Marangon D G, Smith P R, Walk N, Paraïso T K, Dynes J F, Lovic V, Sanzaro M, Roger T, De Marco I, Lucamarini M, Yuan Z L, Shields A J 2024 *Nat. Electron.* **7** 396
[27] Pirandola S, Andersen U L, Banchi L, Berta M, Bunandar D, Colbeck R, Englund D, Gehring T, Lupo C, Ottaviani C, Pereira J L, Razavi M, Shamsul Shaari J, Tomamichel M, Usenko V C, Vallone G, Villoresi P, Wallden P 2020 *Adv. Opt. Photon.* **12** 1012
[28] Xu F H, Ma X F, Zhang Q, Lo H K, Pan J W 2020 *Rev. Mod. Phys.* **92** 025002
[29] Siew S Y, Li B, Gao F, Zheng H Y, Zhang W, Guo P, Xie S W, Song A, Dong B, Luo L W, Li C, Luo X, Lo G Q 2021 *J. Lightwave Technol.* **39** 4374
[30] Chen X, Milosevic M M, Stanković S, Reynolds S, Bucio T D, Li K, Thomson D J, Gardes F, Reed G T 2018 *Proc. IEEE* **106** 2101
[31] Reed G T, Mashanovich G, Gardes F Y, Thomson D J 2010 *Nat. Photonics* **4** 518
[32] Ogiso Y, Ozaki J, Ueda Y, Wakita H, Nagatani M, Yamazaki H, Nakamura M, Kobayashi T, Kanazawa S, Hashizume Y, Tanobe H, Nunoya N, Lda M, Miyamoto Y, Lshikawa M 2019 *J. Lightwave Technol.* **38** 249
[33] Abellan C, Amaya W, Domenech D, Muñoz P, Capmany J, Longhi S, Mitchell M W, Pruneri V 2016 *Optica* **3** 989
[34] Sibson P, Erven C, Godfrey M, Miki S, Yamashita T, Fujiwara M, Sasaki M, Terai H, Tanner M G, Natarajan C M, Hadfield R H, O'Brien J L, Thompson M G 2017 *Nat. Commun.* **8** 13984
[35] Zhang M, Wang C, Kharel P, Zhu D, Lončar M 2021 *Optica* **8** 652
[36] Berikaa E, Alam M S, Li W J, Bernal S, Krueger B, Pittalà F, Plant D V 2023 *IEEE Photon. Technol. Lett.* **35** 850
[37] Lomonte E, Wolff M A, Beutel F, Ferrari S, Schuck C, Pernice W H P, Lenzini F 2021 *Nat. Commun.* **12** 6847
[38] Xiong W J, Wang G L, Li J F, Zhao C, Wang W W, Radamson H H 2021 *J. Mater. Sci-Mater. El.* **32** 1
[39] Wilmart Q, El Dirani H, Tyler N, Fowler D, Malhouitre S, Garcia S, Casale M, Kerdiles S, Hassan K, Monat C, Letartre X, Kamel A, Pu M, Yvind K, Oxenløwe L K, Rabaud W, Sciancalepore C, Szelag B, Olivier S 2019 *Appl. Sci.* **9** 255
[40] Sacher W D, Huang Y, Lo G Q, Poon J K S 2015 *J. Lightw. Technol.* **33** 901
[41] Gyger S, Zichi J, Schweickert L, Elshaari A W, Steinhauer S, Covre da Silva S F, Rastelli A, Zwiller V, Jöns K D, Errando Herranz C 2021 *Nat. Commun.* **12** 1408
[42] Schuck C, Guo X, Fan L, Ma X, Poot M, Tang H X 2016 *Nat. Commun.* **7** 10352
[43] Zhu C X, Chen Z Y, Li Y, Wang X Z, Wang C Z, Zhu Y L, Liang F T, Cai W Q, Jin G, Liao S K, Peng C Z 2022 *Phys. Rev. Appl.* **17** 064034
[44] Beutel F, Brückerhoff Plückelmann F, Gehring H, Kovalyuk V, Zolotov P, Goltsman G, Pernice W H P 2022 *Optica* **9** 1121
[45] Dolphin J A, Paraïso T K, Du H, Woodward R I, Marangon D G, Shields A J 2023 *npj Quantum Inf.* **9** 84
[46] Du Y Q, Zhu X, Hua X, Zhao Z G, Hu X, Qian Y, Xiao X, Wei K J 2023 *Chip* **2** 100039
[47] Wei K J, Hu X, Du Y Q, Hua X, Zhao Z G, Chen Y, Huang C F, Xiao X 2023 *Photon. Res.* **11** 1364
[48] Sax R, Boaron A, Boso G, Atzeni S, Crespi A, Grünenfelder F, Rusca D, Al Saadi A, Bronzi D, Kupijai S 2023 *Photon. Res.* **11** 1007
[49] Lin Z H, Gao Y F, Zhou L, Yuan H H, Zhu Y T, Lin Z J, Zhang W, Huang Y D, Cai X L, Yuan Z L 2025 *Opt. Quantum* **3** 195
[50] Heo H, Woo M K, Park C H, Jang H S, Hwang H, Lee H, Seo M K, Kim S, Kwon H, Jung H, Han S W 2025 *APL Photonics* **10** 031301
[51] Li L, Wang T, Li X H, Huang P, Guo Y Y, Lu L J, Zhou L J, Zeng G H 2023 *Photon. Res.* **11** 504
[52] Bian Y M, Pan Y, Xu X S, Zhao L, Li Y, Huang W, Zhang L, Yu S, Zhang Y C, Xu B J 2024 *Appl. Phys. Lett.* **124** 174001
[53] Piétri Y, Trigo Vidarte L, Schiavon M, Vivien L, Grangier P, Rhouni A, Diamanti E 2024 *Opt. Quantum* **2** 428
[54] Aldama J, Sarmiento S, Vidarte L T, Etcheverry S, Grande I L, Castelvero L, Hinojosa A, Beckerwerth T, Piétri Y, Rhouni A 2024 arXiv: 2412.03208 [quant-ph]
[55] Hajomer A A, Bruynsteen C, Derkach I, Jain N, Bomhals A, Bastiaens S, Andersen U L, Yin X, Gehring T 2024 *Optica* **11** 1197
[56] Hajomer A A, Bomhals A, Bruynsteen C, Sidhique A, Derkach I, Andersen U L, Yin X, Gehring T 2025 arXiv: 2504.09308 [quant-ph]
[57] Ng S Q, Kanitschar F, Zhang G, Wang C 2025 arXiv: 2504.08298 [quant-ph]
[58] Ma C X, Sacher W D, Tang Z Y, Mikkelsen J C, Yang Y S, Xu F H, Thiessen T, Lo H K, Poon J K S 2016 *Optica* **3** 1274
[59] Bunandar D, Lentine A, Lee C, Cai H, Long C M, Boynton N, Martinez N, DeRose C, Chen C C, Grein M, Trotter D, Starbuck A, Pomerene A, Hamilton S, Wong F N C, Camacho R, Davids P, Urayama J, Englund D 2018 *Phys. Rev. X* **8** 021009
[60] Cao L, Luo W, Wang Y X, Zou J, Yan R D, Cai H, Zhang Y, Hu X L, Jiang C, Fan W J, Zhou X Q, Dong B, Luo X S, Lo G Q, Wang Y X, Xu Z W, Sun S H, Wang X B, Hao Y L, Jin Y F, Kwong D L, Kwek L C, Liu A Q 2020 *Phys. Rev. Appl.* **14** 011001
[61] Wang H, Li Y, Pi Y D, Pan Y, Shao Y, Ma L, Zhang Y C, Yang J, Zhang T, Huang W, Xu B J 2022 *Commun. Phys.* **5** 162
[62] Zhang Y C, Chen Z Y, Chu B J, Zhou C, Wang X Y, Zhao Y J, Xu Y F, Xu C, Wang H J, Zheng Z Y, Huang Y D, Xu C C, Zhang X X, Shen T, Huang G, Zheng Y W, Fei Z X, Huang W N, Zhu M L, Huang L Y, Luo B, Yu S, Guo H 2020 *Bull. Am. Phys. Soc.* **65** 1
[63] Zhang G, Haw J Y, Cai H, Xu F, Assad S M, Fitzsimons J F, Zhou X, Zhang Y, Yu S, Wu J, Ser W, Kwek L C, Liu A Q 2019 *Nat. Photonics* **13** 839
[64] Wang C, Primaatmaja I W, Ng H J, Haw J Y, Ho R, Zhang J R, Zhang G, Lim C 2023 *Nat. Commun.* **14** 316
[65] Chrysostomidis T, Roumpos I, Outerelo D A, Troncoso Costas M, Moskalenko V, Garcia Escartin J C, Diaz Otero F J, Vyrsokinos K 2023 *EPJ Quantum Technol.* **10** 5
[66] Bruynsteen C, Gehring T, Lupo C, Bauwelinck J, Yin X 2023 *PRX Quantum* **4** 010330
[67] Li L, Cai M L, Wang T, Tan Z C, Huang P, Wu K, Zeng G H 2024 *Photon. Res.* **12** 1379
[68] Zhao Z G, Hua X, Du Y Q, Xu C Y, Xie F, Zhang Z R, Xiao X, Wei K J 2024 *Opt. Express* **32** 38793
[69] Tanizawa K, Kato K, Futami F 2024 *J. Lightwave Technol.* **42** 1209
[70] Wang X Y, Zheng T, Jia Y X, Huang J, Zhu X Y, Shi Y Q,

Wang N, Lu Z G, Zou J, Li Y M 2024 *Photonics* **11** 468

[71] Bian Y M, Yang J, Jiang H Y, Huang W, Su Q, Yu S, Zhang L, Zhang Y C, Xu B J 2025 *Opt. Lett.* **50** 1216

[72] Bertapelle T, Avesani M, Santamato A, Montanaro A, Chiesa M, Rotta D, Artiglia M, Sorianello V, Testa F, De Angelis G, Contestabile G, Vallone G, Romagnoli M, Villoresi P 2025 *Opt. Quantum* **3** 111

[73] Sun S H, Huang A Q 2022 *Entropy* **24** 260

[74] Chen Y, Huang C F, Chen Z H, He W J, Zhang C X, Sun S H, Wei K J 2022 *Phys. Rev. A* **106** 022614

[75] Zhang C, Hu X L, Jiang C, Chen J P, Liu Y, Zhang W J, Yu Z W, Li H, You L X, Wang Z, Wang X B, Zhang Q, Pan J W 2022 *Phys. Rev. Lett.* **128** 190503

[76] Kang X, Ye P, Wang S, Zhang G W, Wang Z H, Chen J L, Yin Z Q, He D Y, Chen W, Fan Yuan G J, Guo G C, Han Z F 2025 *Phys. Rev. Appl.* **23** 024014

[77] Tan H, Li W, Zhang L K, Wei K J, Xu F H 2021 *Phys. Rev. Appl.* **15** 064038

[78] Li L, Huang P, Wang T, Zeng G H 2021 *Phys. Rev. A* **103** 032611

[79] Ye P, Chen W, Wang Z H, Zhang G W, Ding Y Y, Huang G Z, Yin Z Q, Wang S, He D Y, Liu W, Guo G C, Han Z F 2022 *Opt. Express* **30** 39911

[80] Curty M, Azuma K, Lo H K 2019 *npj Quantum Inf.* **5** 64

[81] Zhu H T, Huang Y Z, Liu H, Zeng P, Zou M, Dai Y Q, Tang S B, Li H, You L X, Wang Z, Chen Y A, Ma X F, Chen T Y, Pan J W 2023 *Phys. Rev. Lett.* **130** 030801

[82] Zeng P, Zhou H Y, Wu W J, Ma X F 2022 *Nat. Commun.* **13** 3903

[83] Wang F X, Chen W, Yin Z Q, Wang S, Guo G C, Han Z F 2019 *Phys. Rev. Appl.* **11** 024070

[84] Sekga C, Mafu M, Senekane M 2023 *Sci. Rep.* **13** 1229

SPECIAL TOPIC—Quantum information processing

Recent progress on photon-integrated quantum key distribution and quantum random number generator*

YU Jingchun [1)2)] LU Wenbin [3)4)] CHEN Bin [1)2)] DU Yongqiang [1)]
XIE Feng [1)] LI Wei [3)4)†] WEI Kejin [1)‡]

1) (*Guangxi Key Laboratory for Relativistic Astrophysics, School of Physical Science and Technology, Guangxi University, Nanning* 530004, *China*)

2) (*School of Computer, Electronics and Information, Guangxi University, Nanning* 530004, *China*)

3) (*School of Artificial Intelligence Science and Technology, University of Shanghai for Science and Technology, Shanghai* 200093, *China*)

4) (*Institute of Photonic Chips, University of Shanghai for Science and Technology, Shanghai* 200093, *China*)

(Received 18 June 2025; revised manuscript received 17 July 2025)

Abstract

Quantum key distribution (QKD) relies on the fundamental principles of quantum mechanics and can theoretically achieve unconditionally secure communication that is provable by information theory. Quantum random number generators, on the other hand, utilize the inherent randomness of quantum phenomena and are capable of generating a truly random entropy source that is unpredictable, unbiased and unrepeatable. These two technologies are crucial for building highly trustworthy and secure communication systems resistant to quantum attacks. However, their large-scale deployment still faces challenges such as system performance optimization, cost control and scale production.

Relying on wafer-level fabrication platforms and micro-nanometer processing, integrated photonics technology integrates the core devices of traditional QKD systems (e.g., light source, modulator, and detector) in a single chip at high density. It significantly improves the miniaturization, operational stability and cost-effectiveness of the system, and enhances the intrinsic security, and becomes a key enabling platform to drive QKD and QRNG from laboratory to engineering applications.

In this paper, we systematically review the recent breakthroughs of photonic integrated QKD based on different material platforms (SOI/InP/TFLN/Si_3N_4) in terms of core metrics, such as transmission distance and key rate, as well as the significant breakthroughs of integrated QRNG in terms of random number generation rate and system integration. Finally, the future development direction of this field is discussed and outlooked from the four dimensions of practical security of QKD systems, on-chip implementation of cutting-edge QKD protocols, practical fully-integrated QKD systems, and synergistic optimization of high performance and high integration of integrated QRNG.

Keywords: quantum key distribution, quantum random number generators, integrated photonics

PACS: 03.67.Hk, 03.67.–a, 42.82.–m **DOI:** 10.7498/aps.74.20250791

CSTR: 32037.14.aps.74.20250791

* Project supported by the National Natural Science Foundation of China (Grant Nos. 62171144, 62031024), the Guangxi Natural Science Foundation, China (Grant Nos. 2025GXNSFAA069137, GXR-1BGQ2424005), and the Innovation Project of Guangxi Graduate Education, China (Grant No. YCBZ2024002).

† Corresponding author. E-mail: weil@usst.edu.cn

‡ Corresponding author. E-mail: kjwei@gxu.edu.cn

专题: 量子信息处理

量子无噪声线性放大*

崔诗荷[1)] 杜明明[2)] 李喜云[1)] 周澜[1)†] 盛宇波[2)]

1) (南京邮电大学理学院, 南京 210023)

2) (南京邮电大学电子与光学工程学院、柔性电子 (未来技术) 学院, 南京 210023)

(2025 年 7 月 2 日收到; 2025 年 7 月 29 日收到修改稿)

量子通信基于量子力学基本原理实现信息的安全传输. 光子是量子通信中重要的信息载体. 基于光子的量子通信协议需要在通信双方传输光子, 但传输过程中由于环境噪声的存在不可避免地会发生光子传输损耗. 光子传输损耗极大地降低了长距离量子通信的通信效率, 甚至威胁通信安全, 成为实现长距离量子通信的主要障碍. 量子无噪声线性放大 (noiseless linear amplification, NLA) 是抵御光子传输损耗的重要方法, 它通过局域操作和后选择, 可有效地提高输出态中目标态的保真度或平均光子数, 且完美保留目标态的编码信息. 因此, 在量子通信中使用 NLA 技术可有效克服光子传输损耗, 延长通信距离, 对于实现远距离量子通信具有重要意义. 近年来, 研究人员提出了许多 NLA 方案, 并完成了部分方案的实验演示, 证明了 NLA 的可行性. 本文重点介绍在离散变量和连续变量量子系统中针对不同量子态的 NLA 方案, 并总结了几个具有代表性的 NLA 实验, 最后, 对 NLA 技术进行总结和展望. 本综述可为未来长距离量子通信网络的实用化发展提供理论支持.

关键词: 量子通信, 量子无噪声线性放大, 连续变量, 离散变量

PACS: 03.67.Pp, 03.67.Hk, 03.65.Ud **DOI:** 10.7498/aps.74.20250865

CSTR: 32037.14.aps.74.20250865

1 引 言

量子通信是基于量子力学基本原理的新型信息传输技术. 与经典通信相比, 量子通信具有发现窃听的能力, 理论上具有绝对安全性. 光子凭借其传输快、易操作等优势, 成为量子通信的重要载体. 然而, 光子在实际的噪声量子信道传输过程中会出现传输损耗. 光子在光纤中的传输效率公式为 $\eta = 10^{-\alpha d/10}$ [1], 目前广泛采用的标准光纤对应 $\alpha = 0.2$ dB/km, 可以看出光子的传输效率随传输距离的增加呈指数式下降. 由于量子不可克隆定理的存在, 我们无法准确复制量子态, 这使得光子的传输存在一个极限距离. 另外, 即使在极限距离之内, 光子也有一定的概率发生丢失. 这将使得单光子态变成一定概率的单光子和真空态的混合态. 在传输距离之内, 光子丢失不仅严重影响量子通信的成功概率和保真度, 而且对量子通信的安全性造成重要威胁[1–4].

对于光子传输丢失的问题, 人们用两种方法来克服. 第一, 使用量子中继来加长光子纠缠的距离[2–7]. 它的核心思想是利用纠缠交换, 实现类似经典中继的功能, 从而加长纠缠信道的距离. 第二, 人们提出了量子放大的思想[8–39]. 量子放大的基本模型可以如下描述, 一个单光子 (纠缠光子对中的单光子) 在信道传播过程中, 传输效率为 p. 那么经过传输, 将变成概率为 p 的单光子态 (纠缠态) 和概率为 $1-p$ 的真空态 (剩余单光子态) 的混合态. 量子比特放大的思想就是要通过局域操作, 使得单光子态 (纠缠态) 的概率 p 增大.

* 国家自然科学基金 (批准号: 12175106, 92365110) 资助的课题.

† 通信作者. E-mail: zhoul@njupt.edu.cn

量子态放大常被称为无噪线性放大 (noiseless linear amplification, NLA), 是抵御光子传输损耗的重要方法. NLA 由 Ralph 和 Lund[8] 于 2009 年首先提出. 它是一种概率性的量子操作, 可以在不引入额外噪声的情况下以一定的增益 $g>1$ 放大量子态的振幅, 实现 $|\psi\rangle \to |g\psi\rangle$, 其核心思想是通过局域操作和后选择实现信号的放大. 该方案于 2012 年获得了实验验证[9]. 随后, 诸多针对离散变量 (discrete variable, DV) 和连续变量 (continuous-variable, CV) 的 NLA 方案相继提出[10–27]. DV 领域内, 2010 年 NLA 被证实还可用于纠缠态的提取[10]. 随后, NLA 被应用到量子通信领域, 多个设备无关量子密钥分发 (device-independent quantum key distribution, DI QKD) 方案采用 NLA 来抵御光子传输损耗, 延长安全通信距离[11–13]. 2012 年, Zhang 等[14] 提出了单光子空间纠缠态的 NLA 方案. 后来, Monteiro 等[15] 改良了 Zhang 等[14] 的方案, 并将 NLA 应用于基于单光子空间纠缠的 QKD 中. 2013 年, 首个基于纠缠态辅助的极化编码纠缠态 NLA 方案提出[16]. 该方案在运行成功时, 可使输出态中目标态的保真度放大为 1(增益达到最大值), 而且成功概率不会随着增益的增加而渐近降低到零. 随后, Kocsis 等[18] 实验实现了单光子极化量子比特的放大, 在实现放大功能的同时可有效保护光子的极化编码特性. 另一方面, NLA 证实可与纠缠浓缩结合, 在对目标纠缠态进行放大的同时将退化后的非最大纠缠态概率性地恢复为最大纠缠态[19]. 2015 年, Zhou 和 Sheng[20] 提出了利用交叉克尔介质的首个可循环使用的单光子空间纠缠态的 NLA 方案, 通过循环使用该方案, 可有效提高方案的总成功概率和增益. 近年来, 研究人员提出了针对单光子多自由度超编码和超纠缠的 NLA 方案[24–26]. 另一方面, CV 领域内研究人员近年提出了多个新型 NLA 方案[28–39]. 例如, 2020 年, Winnel 等[29] 提出了一个基于线性光学元件的广义 n-光子量子剪刀 (quantum scissor, QS) NLA 方案, 该方案可同时实现对 Fock 态的高阶截断和放大. 2021 年, QS 和光催化技术分别用于对频率自由度编码的相干态进行放大[30]. 2022 年, Guanzon 等[32] 提出可利用线性光学元件对任意的 n 阶 Fock 态同时实现理想的量子隐形传态和放大. 除了基于 QS 的方案以外, 基于光子加减法[34]、测量滤波[35]、量子催化[36] 等方案也被相继提出, 并得到广泛应用[37–39].

本文旨在对一些重要的 DV NLA 方案和 CV NLA 方案进行介绍. 第 2 节介绍 DV 量子系统中针对不同量子态的 NLA 理论方案. 第 3 节介绍 CV 量子系统中重要的 NLA 理论方案. 第 4 节介绍几个重要的 QS-NLA 实验. 最后, 第 5 节对 NLA 进行总结和展望.

2 DV 量子系统中的 NLA 方案

2.1 基于 QS 的 DV-NLA 方案

2.1.1 基于 QS 的单光子 NLA 方案

2009 年, Ralph 和 Lund[8] 提出了基于 QS 的单光子 NLA 方案, 这也是目前使用最广泛的 NLA 方案. 该方案的原理图如图 1 所示.

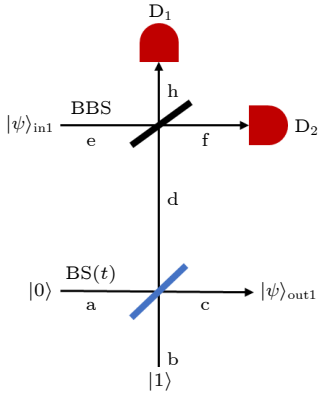


图 1 单光子 QS-NLA 方案原理图[8]. BS(t) 和 BBS 分别是透射率为 t 和 1/2 的分束器, D_1, D_2 为理想的单光子探测器. 输入态和辅助单光子态分别从空间模式 e 和 b 进入 QS. 当探测器 D_1, D_2 只有一个探测到单光子, 另一个没有探测到光子时, 该 NLA 方案运行成功

Fig. 1. Schematic diagram of a single-photon QS-NLA protocol[8]. BS(t) and BBS are beam splitters with the transmittance t and 1/2, respectively. D1 and D2 are ideal single-photon detectors. The input state and auxiliary single-photon state enter the QS from the spatial modes e and b, respectively. When one detector detects only a single photon and the other detector does not detect a photon, the NLA scheme runs successfully.

整个 QS 装置由透射率分别为 t 和 1/2 的两个分束器和能区分入射光子数的理想单光子探测器 (detector, D) D_1 和 D_2 组成. 输入态为叠加态 $|\psi\rangle_{\rm in1}=\alpha|0\rangle+\beta|1\rangle$, $|0\rangle$和$|1\rangle$ 分别代表真空态和单光子态, 系数满足 $|\alpha^2|+|\beta^2|=1$. 首先, 辅助单光子态 $|1\rangle$ 分别由空间模式 a, b 进入透射率为 t 的分束器 (beam splitter, BS). BS(t), 该操作可用算符

表示为

$$U_{\mathrm{BS}(t)} = \exp\left[\theta\left(\hat{a}\hat{a}^{\dagger} - \hat{a}^{\dagger}\hat{a}\right)\right],$$

$$\theta = \arctan\sqrt{(1-t)/t},$$

其中 $\hat{a}^{\dagger}$, $\hat{a}$ 表示相应模式的产生、湮灭算符, 得到辅助纠缠态:

$$|\psi\rangle_{\mathrm{cd}} = U_{\mathrm{BS}(t)}|0\rangle_{\mathrm{a}}|1\rangle_{\mathrm{b}} = \sqrt{t}|0\rangle_{\mathrm{c}}|1\rangle_{\mathrm{d}} + \sqrt{1-t}|0\rangle_{\mathrm{d}}|1\rangle_{\mathrm{c}}. \tag{1}$$

然后, 将空间模式 d 的输出态与从 e 进入的输入态 $|\psi\rangle_{\mathrm{in1}}$ 一起通过透射率为 1/2 的分束器 (balanced beam splitter, BBS), 工作原理为

$$|1\rangle_{\mathrm{e}} \xrightarrow{\mathrm{BBS}} \frac{1}{\sqrt{2}}\left(|1\rangle_{\mathrm{h}} + |1\rangle_{\mathrm{f}}\right),$$

$$|1\rangle_{\mathrm{d}} \xrightarrow{\mathrm{BBS}} \frac{1}{\sqrt{2}}\left(|1\rangle_{\mathrm{h}} - |1\rangle_{\mathrm{f}}\right).$$

此时, 总量子态为

$$\begin{aligned}|\psi\rangle_{\mathrm{chf}} = {} & \alpha\sqrt{t}|0\rangle_{\mathrm{c}}\frac{1}{\sqrt{2}}\left(|1\rangle_{\mathrm{h}}|0\rangle_{\mathrm{f}} + |0\rangle_{\mathrm{h}}|1\rangle_{\mathrm{f}}\right) \\ & + \alpha\sqrt{1-t}|1\rangle_{\mathrm{c}}|0\rangle_{\mathrm{h}}|0\rangle_{\mathrm{f}} \\ & + \beta\sqrt{t}|0\rangle_{\mathrm{c}}\frac{1}{\sqrt{2}}\left(|2\rangle_{\mathrm{h}}|0\rangle_{\mathrm{f}} + |0\rangle_{\mathrm{h}}|2\rangle_{\mathrm{f}}\right) \\ & + \beta\sqrt{1-t}|1\rangle_{\mathrm{c}}\frac{1}{\sqrt{2}}\left(|1\rangle_{\mathrm{h}}|0\rangle_{\mathrm{f}} + |0\rangle_{\mathrm{h}}|1\rangle_{\mathrm{f}}\right). \end{aligned} \tag{2}$$

在两个输出模式 h, 和 f 分别设置一个理想的单光子探测器 D_1 和 D_2. 只有当 D_1 探测到单个光子, D_2 没有探测到光子, 或 D_2 探测到单个光子, D_1 没有探测到光子时, 预示着该 NLA 方案成功运行, 此时输出模式 c 上的输出态为

$$|\psi\rangle_{\mathrm{out1}} = |\psi\rangle_{\mathrm{c}} = \sqrt{t}\left(\alpha|0\rangle \pm g_1\beta|1\rangle\right), \tag{3}$$

其中"+"对应 D_1 响应, "–"对应 D_2 响应. g_1 代表输出态中单光子态的增益, 通过计算可得 $g_1 = \sqrt{(1-t)/t}$, 由分束器的透射率 t 决定, 当 $t < 1/2$ 时, $g_1 > 1$, 说明输出态中单光子态的比例增加, 成功实现对单光子态的放大. 该 NLA 方案的成功概率为 $P_1 = t\alpha^2 + (1-t)\beta^2$. 该方案既可以实现对单光子态的完美放大, 又不破坏输入态中的量子相位关系, 保持了量子相干性.

QS 实现无噪声线性放大的物理原理即为光子的量子隐形传态 (quantum teleportation, QT). 将辅助光子通过 BS(t) 构建单光子在不同路径上的空间纠缠. 将其中一条路径上光子和入射光子通过 BBS 进行单光子干涉和测量, 根据测量结果可将入射光子的全部信息完全传递到输出路径的辅助光子上, 再通过调节 BS(t) 的透射率, 可改变输出态中目标态的保真度, 从而实现对目标态的无噪声线性放大.

2.1.2 基于 QS 的单光子极化量子比特 NLA 方案

贝尔不等式对量子物理学产生了巨大的影响, 贝尔不等式的违反保证了量子非局域关联性的存在. DI QKD 方案基于贝尔不等式的违反来保证产生密钥的安全性[40–42]. 但是, 贝尔不等式的实验检测需要极高的测量精度. 光子传输损耗对贝尔不等式违背的实验实现带来了巨大障碍, 这对 DI QKD 方案的实际安全性也造成了重大威胁. 2010 年, Gisin 等[11] 提出了一种基于单光子源和线性光学的偏振量子比特放大器, 可以克服贝尔测试中的信道损耗问题. 图 2 为该方案的原理图.

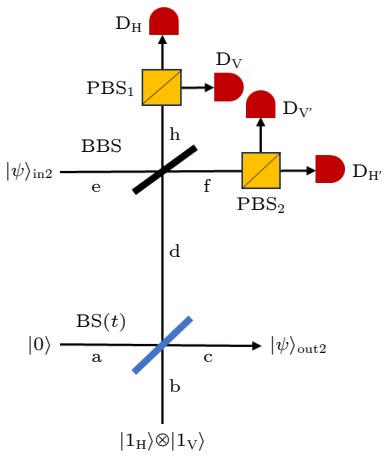


图 2 基于 QS 的单光子极化量子比特 NLA 方案原理图[11]. 处于正交偏振态的两个单光子态 $|1_{\mathrm{H}}\rangle \otimes |1_{\mathrm{V}}\rangle$ 一起作为辅助态进入 QS. PBS 代表偏振分束器, 可以完全透射水平偏振 (H) 的光子, 完全反射垂直偏振 (V) 的光子. $\mathrm{D_H}$, $\mathrm{D_V}$, $\mathrm{D_{H'}}$, $\mathrm{D_{V'}}$ 为 4 个理想单光子探测器

Fig. 2. Schematic diagram of a single-photon polarized qubit QS-NLA protocol[11]. Two single-photon states in orthogonal polarization $|1_{\mathrm{H}}\rangle \otimes |1_{\mathrm{V}}\rangle$ enter the QS together as auxiliary states. Polarization beam splitter (PBS) can totally transmit the horizonal (H) polarization and reflect the vertical (V) polarization. $\mathrm{D_H}$, $\mathrm{D_V}$, $\mathrm{D_{H'}}$, $\mathrm{D_{V'}}$ are four ideal single photon detectors.

该方案将真空态和单光子极化量子比特组成的归一化相干叠加态作为输入态:

$$|\psi\rangle_{\mathrm{in2}} = \alpha|0\rangle + \left(\beta_{\mathrm{H}}|1_{\mathrm{H}}\rangle + \beta_{\mathrm{V}}|1_{\mathrm{V}}\rangle\right). \tag{4}$$

与传统单光子态 NLA 方案[8] 的不同之处在于: 辅

助光子由一个处于水平偏振的单光子态 $|1_{\rm H}\rangle$ 和一个处于竖直偏振的单光子态 $|1_{\rm V}\rangle$ 组成. 2 个辅助光子经 BS(t) 后形成辅助纠缠态:

$$\begin{aligned}|1_{\rm H}\rangle_{\rm b}|1_{\rm V}\rangle_{\rm b} &\xrightarrow{\rm BS(t)} (\sqrt{t}|1_{\rm H}\rangle_{\rm d}+\sqrt{1-t}|1_{\rm H}\rangle_{\rm c})\\ &\otimes(\sqrt{t}|1_{\rm V}\rangle_{\rm d}+\sqrt{1-t}|1_{\rm V}\rangle_{\rm c})\\ =\,& t|1_{\rm H}1_{\rm V}\rangle_{\rm d}+(1-t)|1_{\rm H}1_{\rm V}\rangle_{\rm c}\\ &+\sqrt{t(1-t)}(|1_{\rm H}\rangle_{\rm d}|1_{\rm V}\rangle_{\rm c}+|1_{\rm H}\rangle_{\rm c}|1_{\rm V}\rangle_{\rm d}).\end{aligned}\tag{5}$$

空间模式 d 中的光子与空间模式 e 的输入态 $|\psi\rangle_{\rm in2}$ 一起通过 BBS, 对输出态在 H/V 基上进行测量. 该测量装置由 2 个偏振分束器 (polarization beam splitter, PBS) 和 4 个理想单光子探测器组成. PBS 可完全透射 H 偏振光子, 完全反射 V 偏振光子. 当探测器 $\rm D_H$, $\rm D_V$ 同时响应时, 得到输出态为

$$|\psi\rangle_{\rm out2}=\frac{t}{2}\left[\alpha|0\rangle+g_2\left(\beta_{\rm H}|1_{\rm H}\rangle+\beta_{\rm V}|1_{\rm V}\rangle\right)\right].\tag{6}$$

g_2 代表输出态中单光子极化量子比特的增益, $g_2=\sqrt{(1-t)/t}$, 当 $t<1/2$ 时, $g_2>1$, 放大方案运行成功, 同时输出态完美保留了单光子在极化自由度上的编码信息. 除上述情况外, 当探测器 $(\rm D_H, D_{V'})$, $(\rm D_{H'}, D_V)$ 或 $(\rm D_{H'}, D_{V'})$ 响应时, 通过施加相位翻转操作也可以得到 (6) 式所示输出态, 因此该方案的成功概率为

$$P_2=4\left||\psi\rangle_{\rm out2}\right|^2=t^2\alpha^2+t(1-t)\left(\beta_{\rm H}^2+\beta_{\rm V}^2\right).$$

2013 年, Kocsis 等 [18] 提出了另一种单光子极化量子比特的 NLA 方案, 并完成了实验验证. 其原理图如图 3 所示, 考虑输入态 $|\psi\rangle_{\rm in3}$=$|\psi\rangle_{\rm in2}$. 为保护光子的极化特性, 本方案将输入态通过一个 PBS, 然后在 PBS 对应输出路径上分别放置基于辅助光子 $|1_{\rm H}\rangle$ 和 $|1_{\rm V}\rangle$ 的 QS, 分别记为 $\rm QS_H$ 和 $\rm QS_V$. 当 $\rm QS_H$ 和 $\rm QS_V$ 的探测器均成功响应后, 两个 QS 的输出态再经过一个 PBS 耦合到一条输出路径, 从而得到 (6) 式所示的输出态, 完美保留光子在偏振自由度的编码特性. 方案的总成功概率为

$$P_3=t^2\alpha^2+t(1-t)\left(\beta_{\rm H}^2+\beta_{\rm V}^2\right),$$

增益为 $g_3=\sqrt{(1-t)/t}$, 与单光子 NLA 方案的增益相同.

与单光子 NLA 方案的成功概率 P_1 相比, 当参数 α, t 相同时, 极化量子比特 NLA 方案的成功概率均低于 P_1. 说明本方案以牺牲成功概率为代价, 保留了光子的偏振特性.

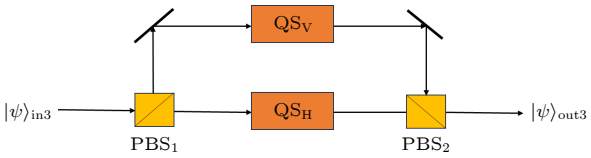


图 3 基于 QS 的单光子极化量子比特 NLA 方案原理图[18]. $\rm QS_H$ 和 $\rm QS_V$ 分别为辅助光子为 $|1_{\rm H}\rangle$ 和 $|1_{\rm V}\rangle$ 的理想的单光子 QS 装置[8], PBS 为偏振分束器

Fig. 3. Schematic diagram of a single-photon polarization qubit QS-NLA protocol[18]. $\rm QS_H$ and $\rm QS_V$ are ideal single-photon quantum scissors with the auxiliary photons $|1_{\rm H}\rangle$ and $|1_{\rm V}\rangle$, respectively[8], and PBS is the polarization beam splitter.

2.1.3 基于 QS 的单光子纠缠态 NLA 方案

单光子纠缠态 (single-photon entanglement state, SPE) 的具体形式为

$$|\psi\rangle_{\rm SPE}=(1/\sqrt{2})\left(|0\rangle_{\rm A}|1\rangle_{\rm B}+|1\rangle_{\rm A}|0\rangle_{\rm B}\right).\tag{7}$$

SPE 是量子通信中的重要资源, 被广泛应用于 QT[43] 和量子非局域测试 [44]. 然而, 在实际应用中, 量子信道中的环境噪声可能导致光子在传输和存储过程中完全丢失变为真空态. 因此, 当 SPE 通过有损信道传输后, 最终会成为混合态: $\rho=\eta|\psi\rangle_{\rm SPE}\langle\psi|+(1-\eta)|00\rangle\langle 00|$, 其中 η 为信道的传输效率, 这代表光子在传输过程中有 $1-\eta$ 的概率丢失. 2012 年, Zhang 等 [14] 提出了一种使用 NLA 保护 SPE 免受光子损耗影响的有效方法.

如图 4 所示, 本 NLA 方案的输入态为混合态:

$$\rho_{\rm in4}=\eta|\psi\rangle_{\rm AB}\langle\psi|+(1-\eta)|00\rangle\langle 00|,$$

其中 $|\psi\rangle_{\rm AB}$=$|\psi\rangle_{\rm SPE}$. 在 A, B 空间模式上分别放置一个理想的单光子 QS, 同时运行两个单光子 QS. 只有两条路径的 QS 同时得到探测器成功响应时, 本方案运行成功. 根据输入态的概率分布, 首先考虑 $|\psi\rangle_{\rm AB}$ 通过 NLA 装置的情况, 两个 QS 的探测器成功响应对应的总输出态为

$$|\psi\rangle_{\rm out4}^{(1)}=\sqrt{t(1-t)}|\psi\rangle_{\rm AB}.\tag{8}$$

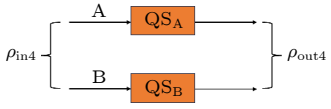


图 4 基于 QS 的 SPE-NLA 方案原理图[14]. $\rm QS_A$ 和 $\rm QS_B$ 为理想的单光子 QS[8], 分别放置于输入态的空间模式 A, B 上

Fig. 4. Schematic diagram of the QS-SPE-NLA protocol[14]. $\rm QS_A$ and $\rm QS_B$ are ideal single-photon QSs[8], which are located on spatial modes A and B of the input state, respectively.

再考虑真空态通过装置的情况, 两个 QS 的探测器成功响应对应的总输出态为

$$|\psi\rangle_{\text{out4}}^{(2)} = t|0\rangle_{\text{A}}|0\rangle_{\text{B}}. \tag{9}$$

因此, 输出的混合态可用密度算符表示为

$$\rho_{\text{out4}} = \frac{\eta(1-t)}{t+\eta-2t\eta}|\psi\rangle_{\text{AB}}\langle\psi| + \frac{t(1-\eta)}{t+\eta-2t\eta}|00\rangle\langle 00|. \tag{10}$$

该放大方案的放大效果可用输出混合态中单光子纠缠态的保真度 F_4 来表征, 具体公式为

$$F_4 = {}_{\text{AB}}\langle\psi|\rho_{\text{out}}|\psi\rangle_{\text{AB}} = \frac{\eta(1-t)}{t+\eta-2t\eta}. \tag{11}$$

输出态中 SPE 的增益为

$$g_4 = \frac{F_4}{\eta} = \frac{(1-t)}{t+\eta-2t\eta}. \tag{12}$$

当 $F_4 > \eta$, 即 $g_4 > 1$ 时, $|\psi\rangle_{\text{SPE}}$ 在输出态中的比例得到放大, 此时仍要求 $t < 1/2$. 该方案成功概率为 $P_4 = t(t+\eta-2t\eta)$, 与单光子 NLA 方案相比, 本方案成功概率更低, 说明本方案通过牺牲成功概率保留了输出态的单光子空间纠缠性质.

2.2 其他类型的 DV-NLA 方案

基于 QS 的 NLA 方案虽然可以实现放大, 得到高保真度的单光子和单光子纠缠态, 但成功概率较低且成功概率随着增益 g 的增加而降低. 当输出态中目标态的保真度接近 1 时, 成功概率接近于 0. 因此, 为了提高放大器性能, 得到更好的放大效果, 近年来科学家们对放大器进行了更深入的研究, 提出了一些改良型 NLA 方案.

2.2.1 具有局域正交压缩操作的 NLA 方案

2013 年, Yang 等 [17] 提出一种将局部正交压缩操作与单光子 QS 相结合的高效 NLA 方案. 放大装置如图 5 所示, 与传统单光子 NLA 方案相比, 辅助光子通过 BS(t) 后, 在空间模式 d 上加入局域正交压缩操作, 得到新的辅助纠缠态:

$$|\psi\rangle_{\text{cd}}' = I_{\text{c}} \otimes \hat{S}(-\xi)|\psi\rangle_{\text{cd}} = \sqrt{1-t}|1\rangle_{\text{c}}\hat{S}(-\xi)|0\rangle_{\text{d}} + \sqrt{t}\frac{\hat{a}\hat{S}(-\xi)}{\sinh(\xi)}|0\rangle_{\text{d}}|0\rangle_{\text{c}}. \tag{13}$$

正交压缩操作是连续变量量子信息处理中的一种常见的技术, 用算符 $\hat{S}(-\zeta) = \text{e}^{-\zeta(\hat{a}^2+\hat{a}^{\dagger 2})/2}$ 表示, $\xi \in [0,1]$ 为压缩系数, 该操作满足关系:

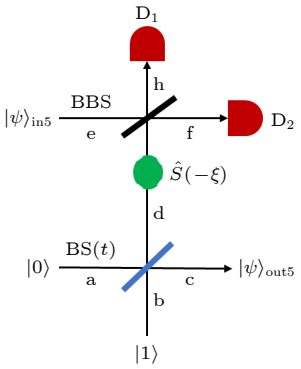


图 5 具有局域正交压缩操作的单光子 NLA 方案原理图 [17]. $\hat{S}(-\zeta)$ 代表局域正交压缩操作

Fig. 5. Schematic diagram of a single-photon NLA protocol with local orthogonal squeezing operation [17]. $\hat{S}(-\xi)$ stands for local orthogonal squeezing operation.

$$\sinh(\xi)\hat{S}(-\xi)|1\rangle = \hat{a}\hat{S}(-\xi)|0\rangle,$$

$$\hat{S}(-\xi)|0\rangle = \frac{1}{\sqrt{\cosh(\xi)}}\sum_{k=0}^{\infty}\left(\frac{1}{2}\tanh(\xi)\right)^k\frac{\sqrt{(2k)!}}{k!}|2k\rangle. \tag{14}$$

当输入态为单光子态和真空态的叠加态 $|\psi\rangle_{\text{in5}} = \alpha|0\rangle + \beta|1\rangle$, 其中 $\alpha^2+\beta^2 = 1$. 当输入态与辅助纠缠态一起通过分束器 BBS, 只有当 $k = 0$, 1 时, 才可能得到成功的探测器响应情况 (D_1 和 D_2 中只有一个探测器探测到 1 个光子, 另一个探测器无响应). 此时, c 端口得到输出态为

$$|\psi\rangle_{\text{out5}} = \sqrt{t}\frac{1}{\cosh(\xi)^{3/2}}(\alpha|0\rangle \pm g_5\beta|1\rangle). \tag{15}$$

增益 g_5 的计算公式为 $g_5 = \sqrt{(1-t)\cosh(\xi)/t}$. 由 (15) 式可以得知, 当压缩参数 $\xi = 0$ 时, 该方案放大效果等于传统单光子 QS 方案的放大效果. 但是, 当 $\xi > 0$ 时, 增益 $g_5 > g_1$. 因此, 可以通过对辅助态施加局域正交压缩操作, 可通过增大压缩系数提高单光子态的增益, 实现高效的 NLA. 并且, 由于压缩操作的加入使辅助纠缠态改变, 进入 BBS 的光子数增加, 探测器成功响应情况增加, 成功概率为

$$P_5 = \frac{\alpha^2 t}{\cosh\xi^3} + \frac{\beta^2(1-t)}{\cosh\xi^4},$$

也得到了提高. 2024 年, Feng 等 [27] 提出将该与局部正交压缩相结合的单光子 NLA 方案扩展到含有极化特性的 SPE 中, 在对 SPE 进行高效放大的同时, 可完美保留光子在极化自由度上的编码信息.

2.2.2 基于纠缠辅助的 NLA 方案

2013 年, 一种基于理想双光子纠缠辅助的单光子极化量子比特 NLA 方案被提出[16]. 该方案在运行成功时, 可使输出态中目标态的保真度放大为 1(增益达到最大值), 而且成功概率不会随着增益的增加而渐近降低到零.

为了方便与 Gisin 提出的极化量子比特 NLA 方案[11] 比较, 考虑同样的输入态, 即

$$|\psi\rangle_{\text{in6}} = \alpha\,|0\rangle + (\beta_{\text{H}}\,|1_{\text{H}}\rangle + \beta_{\text{V}}\,|1_{\text{V}}\rangle)\,.$$

本方案选择极化贝尔态作为辅助态:

$$|\psi\rangle_{\text{a}_1\text{a}_2} = \frac{1}{\sqrt{2}}\left(|1_{\text{H}}\rangle_{\text{a}_1}|1_{\text{H}}\rangle_{\text{a}_2} + |1_{\text{V}}\rangle_{\text{a}_1}|1_{\text{V}}\rangle_{\text{a}_2}\right). \tag{16}$$

辅助光子分别从端口 a_1 和 a_2 进入装置. 如图 6 所示, 输入态以及辅助态经过四个偏振分束器, PBS_{in} 和 PBS_{out} 完全反射竖直偏振, 完全透射水平偏振. 部分偏振分束器 PPBS_1 完全反射竖直偏振光, 以反射率 r 反射水平偏振光, 可以表示为

$$\begin{aligned}
&|1_{\text{H}}\rangle_{\text{a1}} \to -r|1_{\text{H}}\rangle_{\text{D1}} + \sqrt{1-r^2}|1_{\text{H}}\rangle_{\text{out}},\\
&|1_{\text{H}}\rangle_{\text{in}} \to r|1_{\text{H}}\rangle_{\text{out}} + \sqrt{1-r^2}|1_{\text{H}}\rangle_{\text{D1}}\,,\\
&|1_{\text{V}}\rangle_{\text{a1}} \to -|1_{\text{V}}\rangle_{\text{D1}}.
\end{aligned} \tag{17}$$

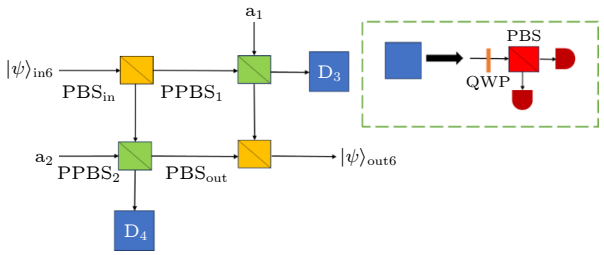


图 6 基于纠缠辅助的极化量子比特 NLA 方案原理图[16]. PPBS_1, PPBS_2 代表部分偏振分束器 (partial polarization beam splitter, PPBS). D_3 和 D_4 是标准偏振分析检测块[45], 每个检测块由一个 1/4 玻片 (quarter wave plate, QWP), 1 个 PBS 和 2 个理想单光子探测器组成

Fig. 6. Schematic diagram of a polarized qubit NLA scheme based on entanglement assistance[16]. PPBS_1, PPBS_2 stand for partially polarized beam splitter. D_3 and D_4 are standard polarization analysis blocks[45], each consisting of a quarter wave plate (QWP), a PBS, and two ideal single-photon detectors.

类似地, PPBS_2 完全反射水平偏振, 以反射率 r 反射竖直偏振光. 放大器是否成功由偏振检测块 D_3 和 D_4 决定[43], 两个探测模块分别在对角基 $(|1_{\text{H}}\rangle + |1_{\text{V}}\rangle)$ 和 $(|1_{\text{H}}\rangle - |1_{\text{V}}\rangle)$ 上对输出光子进行检测, 只有在 D_1 和 D_2 上检测到相同偏振的光子时, 该放大方案运行成功, 得到输出态:

$$|\psi\rangle_{\text{out6}} \to \alpha r\,|0\rangle + \frac{3r^2-1}{2}\left(\beta_{\text{H}}\,|1_{\text{H}}\rangle + \beta_{\text{V}}\,|1_{\text{V}}\rangle\right). \tag{18}$$

增益 $g_6 = \left(3r^2-1\right)^2/\left(4r^2\right)$, 成功概率为

$$P_6 = r^2\left[|\alpha|^2 + g_6\left(|\beta_{\text{H}}|^2 + |\beta_{\text{V}}|^2\right)\right],$$

其大小取决于增益和输入态系数. 当部分偏振分束器反射率 $r=1$ 时, 增益 $g_2=1$, 成功概率 $P_6 = r^2$; 当 $r \to 0$ 时, 输出态中真空项被完全抑制, 目标极化量子比特占比趋于 1, 且 $P_6 \to \left(|\beta_{\text{H}}|^2 + |\beta_{\text{V}}|^2\right)/4$, 成功概率不会降低到零.

考虑到在实际情况下辅助光源的不完美性, 2015 年, Ouyang 等[21] 使用实际的自发参量下转换 (spontaneous parametric down-conversion, SPDC) 产生不完美纠缠态作为辅助态, 理论上证明了 SPDC 光源产生的真空态不干扰放大, 可以自动消除, 因此利用 SPDC 产生的不完美纠缠态作为辅助的 NLA 在现实实验条件下可以较好地实现放大. 2022 年, Li 等[25] 提出了基于纠缠态辅助的偏振-时间片段纠缠态 NLA 方案.

2.2.3 可同时抵御光子损耗和退相干的 NLA 方案

在实际传输过程中, 除了光子丢失外, SPE 也会发生纠缠退相干, 从最大纠缠态退化为非最大纠缠态, 即

$$|\psi'\rangle_{\text{AB}} = \alpha|1\rangle_{\text{A}}|0\rangle_{\text{B}} + \beta|0\rangle_{\text{A}}|1\rangle_{\text{B}},\ \left(|\alpha|^2 + |\beta|^2 = 1\right)$$

这种情况可以通过纠缠浓缩概率性地将非最大纠缠态恢复为最大纠缠态. 2013 年, Zhou 和 Sheng[19] 提出了一种将单光子纠缠态的 QS-NLA 和浓缩相结合的高效 NLA 方案, 既可以增加纠缠态的保真度, 又可以从概率性地低纠缠中提取最大纠缠态.

该方案示意与图 4 所示的基于 QS 的方案类似, 但由于输入态不是最大纠缠态, 因此 QS_{A} 和 QS_{B} 中, BS(t) 的透射率并不相同, 分别设置为 t_1, t_2. 输入态为

$$\rho_{\text{in}_7} = \eta|\psi'\rangle_{\text{AB}}\langle\psi'| + (1-\eta)\,|00\rangle\langle 00|\,,$$

其中 $|\psi'\rangle_{\text{AB}}$ 为非最大纠缠态. 当 QS_{A} 和 QS_{B} 均得到探测器成功响应时, 总输出态为

$$\rho_{\text{out7}} = \eta'|\psi''\rangle_{\text{AB}}\langle\psi''| + (1-\eta')\,|00\rangle\langle 00|\,, \tag{19}$$

其中,

$$|\psi''\rangle_{\mathrm{AB}} = \alpha\sqrt{t_2\,(1-t_1)}|1\rangle_{\mathrm{A}}|0\rangle_{\mathrm{B}} \pm \beta\sqrt{t_1\,(1-t_2)}|0\rangle_{\mathrm{A}}|1\rangle_{\mathrm{B}},$$

$\pm$根据探测器的不同响应情况划分, 保真度为

$$\eta' = \frac{\eta\left(\alpha^2 t_2 + \beta^2 t_1 - t_1 t_2\right)}{\eta\left(\alpha^2 t_2 + \beta^2 t_1\right) + t_1 t_2 - 2\eta t_1 t_2}.$$

我们发现通过调节 $\mathrm{QS_A}$ 和 $\mathrm{QS_B}$ 中可变分束器 (variable beam splitter, VBS) 的透射率, 使其满足:

$$\frac{\alpha^2}{\beta^2} = \frac{t_1\,(1-t_2)}{t_2\,(1-t_1)}. \tag{20}$$

输出态 $|\psi''\rangle_{\mathrm{AB}}$ 成为最大纠缠态. 增益为

$$g_7 = \frac{\alpha^2 t_2 + \beta^2 t_1 - t_1 t_2}{\eta\left(\alpha^2 t_2 + \beta^2 t_1\right) + t_1 t_2 - 2\eta t_1 t_2},$$

当$\eta' > \eta$时, 该放大器成功实现放大, 与之前基于 QS 的 NLA 方案相比, 本方案同时解决了长距离量子通信中光子丢失和退相干问题, 在 SPE 的长距离量子通信中具有重要意义.

2.2.4 单光子空间纠缠态的可循环 NLA 方案

上述提到的关于单光子纠缠态的放大方案都是通过执行一次放大操作来提高输出混合态中 SPE 的保真度. 但是在强噪声环境中, SPE 的初始保真度极低时, 执行一轮放大协议之后得到的纠缠态的质量可能会达不到安全和高效的长距离量子通信的标准. 因此, 2013 年 Zhou 和 Sheng[20] 首次提出通过利用克尔介质构造的量子非破坏性探测 (quantum non-demolition detection, QND) 门, 设计了一种可以多次循环放大 SPE 的高效 NLA 方案.

QND 门构造如图 7 所示, 当相干态 $|\alpha\rangle_{\mathrm{p}}$ 和叠加态 $|\psi\rangle = \gamma|0\rangle_{\mathrm{a}_1} + \delta|1\rangle_{\mathrm{a}_2}$ 通过该 QND 门后, 可得到

$$|\psi\rangle_{\mathrm{p}} = \gamma|0\rangle_{\mathrm{a}1}|\alpha\rangle_{\mathrm{p}} + \delta|1\rangle_{\mathrm{a}2}\left|\alpha\mathrm{e}^{-\mathrm{i}\theta}\right\rangle_{\mathrm{p}}. \tag{21}$$

相干态 $|\alpha\rangle_{\mathrm{p}}$ 的相位移动通过 Homodyne 测量得到. 因此, 通过测量相干态的相移, 可以在不破坏光子的情况下判断对应空间模式上光子的数量.

如图 8 所示, 输入态为混合态:

$$\rho_{\mathrm{in}_8} = \eta|\psi\rangle_{a_1 b_1}\langle\psi| + (1-\eta)\,|00\rangle\langle 00|,$$

其中, $|\psi\rangle_{\mathrm{a_1b_1}}$ 为 SPE. 单光子源 $\mathrm{S_1}$, $\mathrm{S_2}$ 发射辅助单光子沿着 $\mathrm{c_1}$, $\mathrm{d_1}$ 分别通过透射率为 t 的可变分束器 $\mathrm{VBS_1}$, $\mathrm{VBS_2}$ 形成辅助态.

通过操作光开关 (optical switch, OS), 使 $\mathrm{c_2}$, $\mathrm{d_2}$ 上的光子与 $\mathrm{a_1}$, $\mathrm{b_1}$ 上的光子先通过 QND 门, 根据测量结果选择相干态 $|\alpha\rangle_{\mathrm{p}}$ 发生相移 $\pm\theta$ 的项 (Homodyne 测量不能区分 $\pm\theta$), 其余项舍去. 选中的输出项进入 $\mathrm{BBS_1}$ 和 $\mathrm{BBS_4}$, 最终在每个 BBS 的两个输出端放置理想单光子探测器. 当每个 BBS 输出端只有一个探测器探测到光子, 另一个没有探测到光子时, 方案运行成功, 得到输出态:

$$\rho_{\mathrm{out}8}^{(1)} = \eta_1|\psi\rangle_{\mathrm{c_3d_3}}\langle\psi| + (1-\eta_1)\,|00\rangle\langle 00|. \tag{22}$$

$\rho_{\mathrm{out}8}^{(1)}$ 上标 (1) 代表循环次数, 系数

$$\eta_1 = \frac{\eta\,(1-t)}{\eta\,(1-t) + (1-\eta)\,t},$$

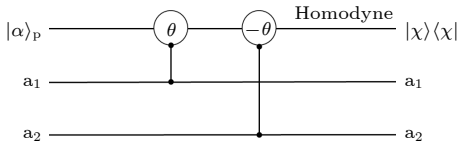


图 7 利用交叉克尔介质构造的非破坏性测量 (quantum non-demolition detection, QND) 门原理图[20]. 空间模式 $\mathrm{a_1}(\mathrm{a_2})$ 的光子与相干态 $|\alpha\rangle_{\mathrm{p}}$ 一起通过交叉克尔介质. 空间模式 $\mathrm{a_1}$ 中的单光子将使相干态 $|\alpha\rangle_{\mathrm{p}}$ 获得 θ 的相移, 而空间模式 $\mathrm{a_2}$ 中的单光子将使相干态 $|\alpha\rangle_{\mathrm{p}}$ 获得 $-\theta$ 的相移

Fig. 7. Schematic diagram of a quantum nondestructive detection (QND) gate using cross-Kerr nonlinear construction[20]. Photons of spatial mode $\mathrm{a_1}(\mathrm{a_2})$ pass through the cross-Kerr medium together with the reference light $|\alpha\rangle_{\mathrm{p}}$. A single photon in the spatial mode $\mathrm{a_1}$ will shift the phase θ acquired by the coherent state $|\alpha\rangle_{\mathrm{p}}$, while a single photon in the spatial mode $\mathrm{a_2}$ will shift the phase $-\theta$ it gains.

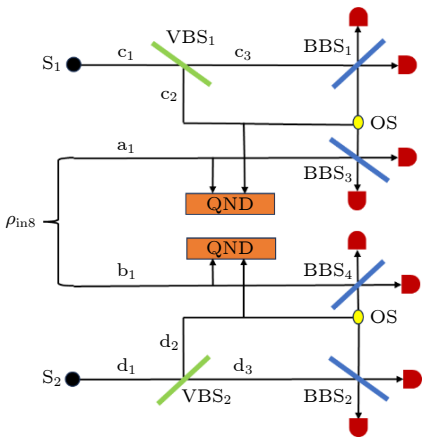


图 8 单光子空间纠缠态的可循环 NLA 方案原理图[20]. $\mathrm{S_1}$ 和 $\mathrm{S_2}$ 为两个单光子源, OS 为光开关, QND 为量子非破坏性探测门

Fig. 8. Schematic diagram of a cyclic NLA protocol for a single-photon spatial-mode entangled state[20]. $\mathrm{S_1}$ and $\mathrm{S_2}$ are two single-photon sources, OS is an optical switch, and QND represents quantum non-demolition detection gate.

成功概率 $P_8^{(1)'}$ 为

$$P_8^{(1)} = \eta t\,(1-t) + (1-\eta)\,t^2,$$

增益 $g_8^{(1)}$ 为

$$g_8^{(1)} = \frac{\eta_1}{\eta} = \frac{(1-t)}{\eta\,(1-t) + t\,(1-\eta)},$$

当 $t < 1/2$ 时, $g_8^{(1)} > 1$, 放大方案成功.

再次操作 OS, 使 c_2, d_2 中第一次探测后被丢弃的项分别与 c_3, d_3 上的光子通过 BBS_2, BBS_3, 探测器成功响应情况同上. 当探测器成功响应后, a_1, b_1 处得到新一轮的输入态:

$$\rho_{\mathrm{out}8}^{(1)\,\prime} = \eta_1' |\psi\rangle_{\mathrm{a}_1\mathrm{b}_1} \langle\psi| + (1-\eta_1')\,|00\rangle\langle 00|\,. \tag{23}$$

系数 η_1' 为

$$\eta_1' = \frac{\eta\left(t^2 - t + 1\right)}{(2\eta - 1)\,t^2 - t^2 - \eta t + 1},$$

成功概率 $P_8^{(1)'}$ 为

$$P_8^{(1)'} = (2\eta - 1)\,t^2 - \eta t + 1.$$

然后, 操作 OS, 重复第一步的操作, 得到第二次循环后的输出态为

$$\rho_{\mathrm{out}8}^{(2)} = \eta_2 |\psi\rangle_{\mathrm{c}_3\mathrm{d}_3} \langle\psi| + (1-\eta_2)\,|00\rangle\langle 00|\,. \tag{24}$$

系数 η_2 为

$$\eta_2 = \frac{\eta_1'\,(1-t)}{\eta_1'\,(1-t) + (1-\eta_1')\,t},$$

成功概率 $P_8^{(2)}$ 为

$$P_8^{(2)} = P_8^{(1)'}\left[\eta' t\,(1-t) + (1-\eta')\,t^2\right],$$

增益 $g_8^{(2)}$ 为

$$g_8^{(2)} = \frac{\eta_2}{\eta_1'} = \frac{(1-t)}{\eta_1'(1-t) + t(1-\eta_1')},$$

当 $t < 1/2$ 时, $g_8^{(2)} > 1$, 放大成功, 证明第二轮放大后获得的态与初始混合态相比 SPE 保真度得到了提高, 循环放大方案成功.

该方案可以推广到对输入态循环 n 次后的情况, 总的成功概率可以表示为

$$P_8^{(\mathrm{total})} = \sum_{n=0}^{\infty} P_8^{(n)}, \tag{25}$$

其中 $P_8^{(n)}$ 为第 n 次放大的成功概率, 满足

$$P_8^{(n)} = P_8^{(n-1)'}\left[\eta_{n-1}' t\,(1-t) + \left(1-\eta_{n-1}'\right) t^2\right],$$

$P_8^{(n-1)'}$ 表示第 n 次放大失败, 获得新的混合输入态的成功概率, 满足 $P_8^{(0)'} = 1$,

$$P_8^{(n)'} = P_8^{(n-1)'}\left[\left(2\eta_{n-1}' - 1\right) t^2 - \eta_{n-1}' t + 1\right].$$

第 n 次放大后输出态中得到 SPE 的保真度用 η_n 表示:

$$\eta_n = \frac{\eta_{n-1}'\,(1-t)}{\eta_{n-1}'\,(1-t) + t\left(1-\eta_{n-1}'\right)}. \tag{26}$$

η_{n-1}' 是第 n 轮放大中初始混合态的保真度, 满足

$$\eta_n' = \frac{\eta_{n-1}'\left(t^2 - t + 1\right)}{\left(2\eta_{n-1}' - 1\right) t^2 - t^2 - \eta_{n-1}' t + 1}.$$

与单次放大相比, 本循环放案的成功概率和保真度都得到提高.

2018 年, Zhou 等 [22] 在该方案的基础上考虑了 SPE 在传输过程中的退相干, 将放大与纠缠浓缩相结合, 提出了一种高效循环放大方案, 既提高了输出目标态的保真度, 又同时将部分纠缠态恢复到最大纠缠态.

该方案示意图与图 4 的不同之处在于 VBS1 和 VBS2 中可变分束器的透射率并不相同, 分别为 t_1, t_2. 当输入态为

$$\rho_{\mathrm{in}8'} = \eta |\psi\rangle_{\mathrm{a}_1\mathrm{b}_1}'\,{}' \langle\psi| + (1-\eta)\,|00\rangle\langle 00|\,,$$

其中 $|\psi\rangle_{\mathrm{a}_1\mathrm{b}_1}'$ 为非最大纠缠态:

$$|\psi\rangle_{\mathrm{a}_1\mathrm{b}_1}' = \alpha|1\rangle_{\mathrm{a}_1}|0\rangle_{\mathrm{b}_1} + \beta|0\rangle_{\mathrm{a}_1}|1\rangle_{\mathrm{b}_1},$$

满足 $|\alpha|^2 + |\beta|^2 = 1$. 通过在每轮放大中保持 VBS1 不变, 重新调整 VBS2 的透射率 t_2, 使其在第 k 次放大中满足:

$$\frac{\alpha^{2k}}{\beta^{2k}} = \frac{t_1\,(1-t_{2,k})}{t_{2,k}\,(1-t_1)}. \tag{27}$$

输出态为最大纠缠态, 且成功概率和保真度都得到提高.

为了方便比较不同的 NLA 方案类型, 表 1 列出不同 NLA 方案对应的目标量子态、增益、成功概率及方案的优势. 可以看出, 基于 QS 的 NLA 方案通过使用 BS(t), BBS 和单光子探测器进行后选择来实现无噪声放大, 但成功概率较低, 且随着增益的增加而减小. 后续改良方案中, 在 QS 中引入压缩操作改变辅助态, 从而可提高目标态的增益和成功概率, 利用双光子纠缠作为辅助纠缠态实现单光子量子比特的高保真放大, 且成功概率不趋零; 在对 SPE 的放大中, 考虑到非最大纠缠的情况, 可以通过动态调节 BS(t)(VBS) 透射系数将其恢复到最大纠缠态、还可以利用克尔介质构造 QND 门进行循环操作逐步提升目标态的保真度和成功概率.

表 1 离散变量量子系统不同 NLA 方案性能对比

Table 1. Performance comparison of different NLA schemes for DV quantum systems.

方案类型	目标态	增益g	成功概率P	特点
单光子NLA[8]	$\|1\rangle$	$\sqrt{(1-t)/t}$	$t\alpha^2+(1-t)\beta^2$	保留量子相干性, 但成功概率随增益增加而降低.
单光子极化量子比特NLA [11,18]	$\|1_{\rm H}\rangle+\|1_{\rm V}\rangle$	$\sqrt{(1-t)/t}$	$t^2\alpha^2+t(1-t)(\beta_{\rm H}^2+\beta_{\rm V}^2)$	分别在水平(H)和垂直(V)路径上独立运行QS, 牺牲成功概率来保护极化自由度的编码信息.
单光子纠缠态NLA[14]	$\frac{\|1\rangle\|0\rangle+\|0\rangle\|1\rangle}{\sqrt{2}}$	$\frac{(1-t)}{t+\eta-2t\eta}$	$t(t+\eta-2t\eta)$	在空间纠缠态的两条路径同时应用QS, 通过后选择提高纠缠保真度.
具有局域正交压缩操作的NLA[17]	$\|1\rangle$	$\sqrt{\frac{\cosh\xi(1-t)}{t}}$	$\frac{\alpha^2 t}{\cosh\xi^3}+\frac{\beta^2(1-t)}{\cosh\xi^4}$	引入正交压缩操作, 提升成功概率和增益.
基于纠缠辅助的NLA[16]	$\|1_{\rm H}\rangle+\|1_{\rm V}\rangle$	$\frac{(3r^2-1)^2}{4r^2}$	$r^2[\|\alpha\|^2+g_6(\|\beta_{\rm H}\|^2+\|\beta_{\rm V}\|^2)]$	利用双光子纠缠态作为辅助资源, 通过部分偏振分束器(PPBS)实现保真度趋近1, 成功概率不随增益趋零.
同时抵御光子损耗和退相干的NLA [19]	$\frac{\|1\rangle\|0\rangle+\|0\rangle\|1\rangle}{\sqrt{2}}$	$\frac{\alpha^2t_2+\beta^2t_1-t_1t_2}{\eta(\alpha^2t_2+\beta^2t_1)+t_1t_2-2\eta t_1t_2}$	—	同时解决光子丢失和退相干问题
可循环NLA[20]	$\frac{\|1\rangle\|0\rangle+\|0\rangle\|1\rangle}{\sqrt{2}}$	每轮增益的总和	每轮成功概率总和	利用交叉克尔介质进行循环操作逐步提高低保真度纠缠态的保真度.

这些方案分别在辅助态的选择、不同目标态的情况下以及性能表现 (增益与成功概率的权衡) 方面都进行了改良提高, 共同构成了 DV-NLA 的多样化方案.

3 CV 量子系统中的 NLA 方案

3.1 基于 QS 的 CV-NLA 方案

3.1.1 多个 1-QS 并行的 CV-NLA 方案

2009 年, Ralph 和 Lund[8] 提出了基于 QS 的单光子无噪声线性放大器. 该放大器可将输入的 Fock 态的光子数截断为一阶, 同时通过增加单光子分量的振幅对截断后的输出态进行放大. 与离散变量不同, 对于弱相干态 (相干态振幅较小), 该放大器可以作为一个理想的 NLA 放大器. 但是当相干态振幅较大时, 该 NLA 方案并不能实现理想的放大. 因此, Ralph 和 Lund[8] 与 Xiang 等[10] 提出并行使用多个 QS 的方案来放大振幅较大的相干态.

如图 9 所示, 输入态为

$$|\psi\rangle_{\rm in9}=|\alpha\rangle=\mathrm{e}^{-\frac{|\alpha|^2}{2}}\sum_{n=0}^{\infty}\frac{\alpha^n}{\sqrt{n!}}|n\rangle,$$

首先通过第一个 N 模 BBS 阵列将振幅均匀地划分为 $\alpha'=\alpha/\sqrt{N}$ ($\alpha'\ll1$), 然后, 每条路径上的弱相干态 $|\alpha'\rangle$ 作为输入态通过一个理想的单光子 QS, 将其截断到单光子态并放大相应的振幅. 当每个 QS 的探测器成功响应时, 将 N 条输出路径的输出态通过第二个 N 模 BBS 阵列耦合到同一路径输出. 若其余 N-1 条输出路径的探测器都没有探测到光子时, 该放大方案运行成功. 当 N 足够大, 满足 $N\gg g|\alpha|$ 时, 得到输出态为

$$|\psi\rangle_{\rm out9}=t^{N/2}\mathrm{e}^{-\left(1-g_9{}^2\right)|\alpha|^2/2}|g_9\alpha\rangle, \tag{28}$$

其中增益 $g_9=\sqrt{(1-t)/t}$, 当 $t<1/2$ 时, $g_9>1$, 成功实现对相干态的放大. 成功概率 $P_9=t^N\times\mathrm{e}^{-\left(1-g^2\right)|\alpha|^2}$, 随着 N 的增加而减小. 这表明, 得到更好放大的代价是降低成功概率.

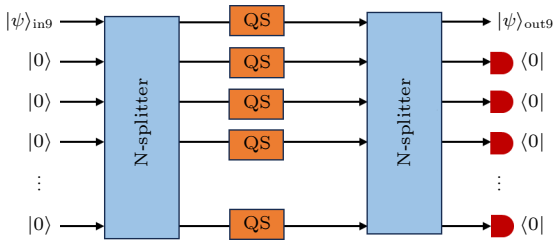


图 9 基于多个单光子量子剪刀 (1-QS) 并行的 NLA 方案示意图[8]. 第一个 BBS 阵列 (N-splitter) 可均匀地将输入态分束到 N 条路径. 第二个 BBS 阵列用于将 N 条路径的输出态耦合到一条路径输出. 当所有 QS 都得到成功的探测器响应且其余 N–1 个输出端没有探测到光子时, 方案成功

Fig. 9. Schematic diagram of multiple 1-QS parallel NLA schemes[8]. The N-splitter is an array of BBSs, which can split the input state into N spatial paths. The second N-splitter is used to couple the beams from N output spatial paths. If all the QSs obtain the successful detector responses and no photons is detected at the other output ports, the protocol is successful.

2021 年, He 等[30] 使用 QS 和光催化技术对频率自由度编码的相干态进行放大. 2023 年 Zhu 等[33] 提出将本方案扩展到对任意极化-时间片段超编码的相干态进行放大, 这些方案在对输入相干态实现了无噪声放大的同时也成功保留了光子在不同自由度上的编码.

3.1.2 基于广义 QS 的 NLA 方案

Ralph 和 Lund 提出的并行使用多个 1-QS 的 CV-NLA 方案只能在 N 足够大的条件下才能实现理想的放大, 当 N 小时运行该 CV-NLA 协议会导致输出态的系数失真, 从而不能实现对相干态理想的放大. 为解决这一问题, 2020 年 Winnel 等[29] 又提出了一种可把输入态截断到更高阶的福克态 (Fock state) 并放大的方案, 被称为广义量子剪刀方案, 它能克服放大后输出态系数失真的问题.

具体方案如图 10 所示, 任意输入态在 Fock 基下可展开为

$$|\psi\rangle_{\text{in10}} = \sum_{n=0}^{\infty} C_n |n\rangle, \quad \sum_n |C_n|^2 = 1.$$

以基于 3-QS 的 NLA 方案为例, 将 3 个辅助光子 (量子态为 $|3\rangle$) 通过透射率为 t 的 BS(t), 并采用由 4 个 BBS 和 4 个单光子探测器组成的四端口单光子测量方案. 当 4 单光子探测器中有 3 个探测到单光子, 一个没有探测到光子时, 方案运行成功, 得到输出态:

$$|\psi\rangle_{\text{out10}}^{(3)} = \frac{\sqrt{6}}{8}\left(\frac{1}{g_{10}^2+1}\right)^{3/2}\left(C_0|0\rangle + g_{10}C_1|1\rangle + g_{10}^2C_2|2\rangle + g_{10}^3C_3|3\rangle\right). \tag{29}$$

$|\psi\rangle_{\text{out10}}^{(3)}$ 上标 (3) 代表输出态被截断和放大到三阶 Fock 态, 增益 $g_{10}^{(3)} = \sqrt{t/(1-t)}$, 当 $t > 1/2$ 时, $g_{10}^{(3)} > 1$ 成功放大. 考虑探测器的不同响应情况, 该 NLA 方案的总成功概率为

$$P_{10}^{(3)} = \frac{3}{8}\left(\frac{1}{g_{10}^2+1}\right)^3\left(|c_0|^2 + |g_{10}c_1|^2 + |g_{10}^2c_2|^2 + |g_{10}^3c_3|^2\right).$$

可以将上述三光子 NLA 方案扩展到对 7 阶 Fock 态的放大, 具体过程如图 11 所示. 本方案使用 7 个光子作为辅助光子 (量子态为 $|7\rangle$) 和 8 端口单光子测量方案. 理论上该 7-QS-NLA 方案可以推广到对输入态进行 ($2S$–1) 阶的截断和放大, 其中 $S = 1, 2, 3$ 等.

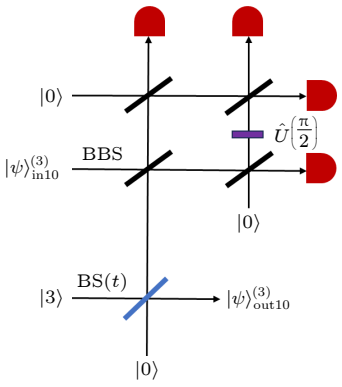


图 10 基于 3 光子 QS (3-QS) 的 NLA 方案示意图[29]. 本方案采用 4 端口单光子测量. 在其中 3 个端口探测到单光子, 另一个端口没有探测到光子的情况下, 该 NLA 方案运行成功. 当方案运行成功时, 需要对其中一条路径上的光子施加 π/2 的相移

Fig. 10. Schematic diagram of NLA protocol based on generalized three-order quantum scissors (3-QS)[29]. The NLA protocol depends on the four-port joint photon measurement. When three of the four ports each have a single photon and the last port does not have photon, the NLA protocol is successful. π/2 phase shift should be present on the photon in one of the paths.

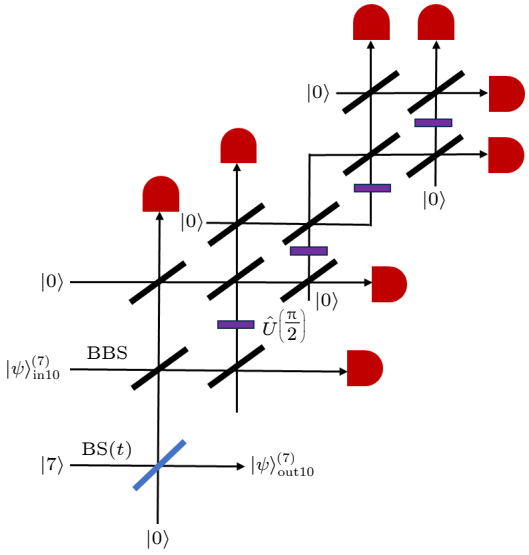


图 11 基于 7 光子 QS (7-QS) 的 NLA 方案原理图[29]. 本方案在 BS(t) 的一个输入端输入 7 光子辅助态. 运行 8 端口单光子测量方案. 当其中 7 个端口探测到单光子, 另一个端口没有探测到光子时, 方案运行成功

Fig. 11. Schematic diagram of the generalized seven-photon QS-NLA protocol[29]. The NLA protocol depends on the seven-photon auxiliary state and the eight-port single-photon measurement module. When seven of the eight ports each detect a single photon and the other port does not, the NLA protocol is successful.

2022 年, Zhong 等[31] 在本文广义 QS 方案的基础上, 设计了针对极化频率超编码相干态的 1-QS 和 3-QS 的 NLA 方案, 实现相干态的单光子截断和三光子截断和放大的同时, 保持了光子极化-频率超编码的特性. 该方案也可以扩展到提高超编码多空间模纠缠上, 在未来的量子信息处理领域具有潜在的应用价值.

3.1.3 基于 n 光子 QS 的 NLA 方案

2022 年, Guanzon 等[32] 提出将传统的基于单光子 QS (1-QS) 的 NLA 方案推广到 n 光子 QS(n-QS), 它可以对任意的阶 Fock 态进行截断和放大. 其作用过程可表示为

$$|\psi\rangle=\sum_{j=0}^{\infty}C_j\,|j\rangle\xrightarrow{n\text{-QS}}|g\psi_n\rangle=N\sum_{j=0}^{n}g^jC_j\,|j\rangle\,. \tag{30}$$

这是之前的 NLA 方案是无法达到的. 该方案也包含了 2020 年提出的只针对 $(2S-1)$ 阶放大方案[29] 的结果.

该方案通过图 12 所示的装置实现, 包括一个透射率为 t 的 BS(t)、一个量子傅里叶变换 (auantum Fourier transform, QFT) 装置、n 个辅助光子和 n 光子探测器. 图 12(a) 和图 12(b) 为放大方案的两种实现方式: 图 12(a) 使用聚束光子 (bunched photon, BP) $|n\rangle$ 作为辅助光子 (BP 方案), 图 12(b) 使用 n 个单光子作为辅助光子 (SP 方案). 输入态为

$$|\psi\rangle_{\text{in11}}=\sum_{n=0}^{\infty}C_n\,|n\rangle\,,$$

QFT 用 $(n+1)$ 模分束器表示, 它能以固定的相位 $(F_{n+1})_{j,k}$ 在其 $(n+1)$ 个输出端口之间均匀地散射光子:

$$(F_{n+1})_{j,k}=\mathrm{e}^{-2\mathrm{i}\pi(j-1)(k-1)/(n+1)}/\sqrt{(n+1)}.$$

图 12(b) 中 QFT 和 BS(t) 的操作均为图 12(a) 中相应操作的共轭转置. 在图 12(a) 中, 辅助态 $|n\rangle$ 和真空态一起通过分束器 BS(t) 获得辅助纠缠态. 分束器的一端与输入态一起进入 QFT, 当 QFT 的输出端有 n 个端口探测到单光子, 一个端口探测到真空态时, 方案运行成功. 在图 12(b) 中, 首先让 n 个单光子和一个真空态进入 QFT, 当输出端有 n–2 个端口没有探测到光子时, 得到辅助纠缠态. 剩余两个端口, 其中一个与输入态一起通过 BS(t), BS(t) 输出端口的探测器一个没有探测到光子, 一个探测到 n 光子时, 方案运行成功. 经过计算, 两种装置的输出态均可表示为

$$|\psi\rangle_{\text{out11}}=|g_{11}\psi_n\rangle=\frac{\sqrt{n!}}{(n+1)^{\frac{n}{2}}\,(g_{11}^2+1)^{\frac{n}{2}}}\sum_{j=1}^{n}g_{11}^jc_j\,|j\rangle\,. \tag{31}$$

该方案的增益 g_{11} 通过调整 BS(t) 的透射率 t 来选择, 二者满足关系式 $g_{11}=\sqrt{t/(1-t)}$. 当 $t>1/2$ 时, $g_{11}>1$. 考虑到探测器的不同响应情况, 两种实现方式对应的成功概率并不相同, 分别为

$$\begin{aligned}P_{11}^{\text{BP}}&=(n+1)\,P_{11},\\ P_{11}^{\text{SP}}&=\frac{(n+1)^n}{(n+1)!}P_{11}.\end{aligned} \tag{32}$$

其中,

$$\begin{aligned}&P_{11}^{\text{BP}}>P_{11}^{\text{SP}},\ n\in\{1,2\}\,,\\ &P_{11}^{\text{BP}}=P_{11}^{\text{SP}},\ n=3,\\ &P_{11}^{\text{BP}}<P_{11}^{\text{SP}},\ n\geqslant 3.\end{aligned} \tag{33}$$

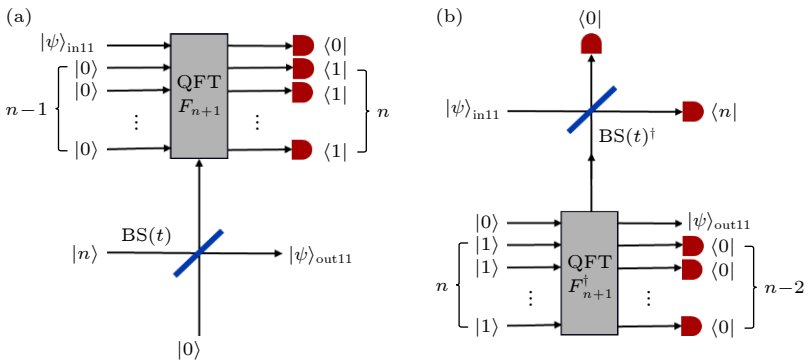


图 12 基于 n 光子 QS (n-QS) 的 NLA 方案示意图[32] (a) 使用 $|n\rangle$ 聚束光子作为辅助态 (BP 方案); (b) 使用 n 个单光子 $\otimes^n|1\rangle$ 作为辅助态 (SP 方案)

Fig. 12. Schematic diagram of NLA scheme based on n-photon QS [32]: (a) $|n\rangle$ bunched photons are used as auxiliary state (BP protocol); (b) n single photons $\otimes^n|1\rangle$ are used as auxiliary state (SP protocol).

由于两种装置输出状态相同, 因此可以根据截断光子的数量 n 来选择不同的装置进行放大.

与并行使用 n 个 1-QS 的方案相比, 本方案只需要调节一个 BS(t) 的透射率即可调整增益, 而且本方案可以更好地放大到任意 n 阶的 FOCK 态得到更高的保真度.

3.2 其他类型的 CV-NLA 方案

除了基于 QS 的 CV-NLA 方案外, 2010 年 Zavatta 等[34] 提出了一种基于光子加法和减法组合的方案, 实现了对弱相干态的无噪声线性放大. 该方案的原理是构造算符 $\hat{G}=(g-2)\,\hat{a}^{\dagger}\hat{a}+\hat{a}\hat{a}^{\dagger}$, 当增益 $g=2$ 时, $\hat{G}=\hat{a}\hat{a}^{\dagger}$. 对于弱相干态 $|\alpha\rangle\approx|0\rangle+\alpha|1\rangle$, 可得

$$\hat{a}\hat{a}^{\dagger}|\alpha\rangle=|0\rangle+2\alpha|1\rangle. \tag{34}$$

实现了对单光子态的放大. Zavatta 等[34] 实验证明了该方案对弱相干态 ($|\alpha|\leqslant 0.65$) 的放大保真度超过 90%, 远高于基于 QS 的 NLA 方案的保真度.

2014 年, Chrzanowski 等[35] 提出了一种基于测量的 CV-NLA 方案, 该方案首先对量子态进行后选择异差测量, 当测量结果 $\alpha=(x+\mathrm{i}p)/\sqrt{2}$ 满足 $\alpha<\alpha_c$ 时, 利用以下滤波函数进行后选择,

$$P(\alpha)=\mathrm{e}^{\frac{1}{2}\left(|\alpha|^2-|\alpha_c|^2\right)\left(1-g^{-2}\right)}, \tag{35}$$

其中 α_{c} 为一个具有高保真度的截止值. 本方法用软件层面的数据处理替代复杂的物理硬件操作, 来模拟放大器的作用. Chrzanowski 等[35] 证明了该方案可以在各种输入态下使用, 而无需重新进行实验配置, 并且更具可扩展性, 可以规避传统放大器硬件导致的效率低下等因素, 它可以实现接近最佳的成功概率、任意精度的放大.

针对高损耗传输问题, 2015 年 Ulanov 等[36] 提出一种利用量子催化技术的 NLA 方案实现对弱双模压缩态的纠缠蒸馏与非真空态的放大. 目标态为 $|\psi\rangle=|00\rangle_{\mathrm{AB}}-\gamma|11\rangle_{\mathrm{AB}}$, 其中 0, 1 代表光子个数. 模式 B 经过透射率为 τ 有损信道后得到混合态:

$$\begin{aligned}\rho=&\left(|00\rangle_{\mathrm{AB}}-\gamma\tau|11\rangle_{\mathrm{AB}}\right)\left(\langle 00|_{\mathrm{AB}}-\gamma\tau\langle 11|_{\mathrm{AB}}\right)\\&+\gamma^2\left(1-\tau^2\right)|10\rangle_{\mathrm{AB}}\langle 10|.\end{aligned} \tag{36}$$

经过有透射率为 t 的分束器和理想单光子探测器组成的量子单光子催化装置, 当探测器探测到单光子时, 该装置成功运行, 得到输出态:

$$\begin{aligned}\rho=&\left(t|00\rangle_{\mathrm{AB}}-\gamma\tau|11\rangle_{\mathrm{AB}}\right)\left(t\langle 00|_{\mathrm{AB}}-\gamma\tau\langle 11|_{\mathrm{AB}}\right)\\&+t^2\gamma^2\left(1-\tau^2\right)|10\rangle_{\mathrm{AB}}\langle 10|,\end{aligned} \tag{37}$$

$$\rho\approx|\psi\rangle=t\left(|00\rangle_{\mathrm{AB}}-\gamma\tau g|11\rangle_{\mathrm{AB}}\right). \tag{38}$$

当 $g=1/(\tau t)$ 时, 可将输出态成功恢复为初始目标态, 当 $g>1/(\tau t)$ 可实现对单光子态的成功放大. Ulanov 等[36] 通过实验证明, 利用量子催化技术可高效恢复纠缠并适用于任意高损耗路径中弱双模压缩态的纠缠蒸馏与放大.

表 2 从对应的目标量子态、增益、成功概率, 及方案的优势等方面对不同 CV-NLA 方案进行比较. 基于多个 1-QS 并行的 NLA 方案, 通过 BBS 阵列和 1-QS 实现对弱相干态的放大, 但成功概率随分束路径数增加而降低; 基于广义 QS 的 NLA 方案利用多光子辅助态和高阶截断技术, 可实现对 Fock 态的 $(2S-1)$ 阶 ($S=1,\,2,\,3$ 等) 截断和放大并避免失真; 基于 n-QS 的 NLA 方案克服了

表 2 连续变量量子系统不同 NLA 方案性能对比

Table 2. Performance comparison of different NLA schemes for CV quantum systems.

NLA方案类型	目标态	增益g	成功概率P	特点
多个1-QS并行[8]	弱相干态	$\sqrt{(1-t)/t}$	$t^N\mathrm{e}^{-(1-g^2)\lvert\alpha\rvert^2}$	放大弱相干态, 成功概率随着分束数量N的增加而降低
广义量子剪刀[29]	Fock态	$\sqrt{t/(1-t)}$	$\frac{3}{8}\left(\frac{1}{g^2+1}\right)^3\left(\lvert c_0\rvert^2+\lvert gc_1\rvert^2+\lvert g^2c_2\rvert^2+\lvert g^3c_3\rvert^2\right)$	可对输入Fock态进行$(2S-1)$阶截断并放大, 其中$S=1,\,2,\,3$等
n光子量子剪刀[32]	Fock态	$\sqrt{t/(1-t)}$	$P^{\mathrm{BP}}=(n+1)P$ $P^{\mathrm{SP}}=(n+1)^nP/(n+1)!$	可以对任意的n阶Fock态进行截断和放大, 有两种实现方式, 可根据截断阶数来选择不同的方案, 得到最优的成功概率
光子加减法[34]	$\lvert0\rangle+\alpha\lvert1\rangle$	—	—	在保真度、增益和噪声控制上均突破经典极限
测量[35]	任意输入态	2	—	通过特定滤波函数进行后选择, 得到接近最佳成功概率, 实现任意精度放大
量子催化[36]	$\lvert00\rangle-\gamma\lvert11\rangle$	$1/t$	$t^2+\gamma^2\tau^2$	可高效恢复纠缠并适用于任意高损耗路径中弱双模压缩态的纠缠蒸馏与放大

广义 QS 方案的局限性, 实现了对 Fock 态任意阶截断和放大. 除了基于 QS 的方案以外, 光子加减法方案通过组合光子加法与减法操作, 以高保真度和低噪声实现对弱相干态的放大, 且无需干涉稳定性; 基于测量的方案通过后选择异差测量和数据处理模拟放大; 量子催化方案适用于高损耗信道中的纠缠态恢复与放大, 适用于极端损耗环境. 这些方案在增益、成功概率和实验复杂度上各有优劣, 共同推动了 CV-NLA 技术的发展, 为量子通信和精密测量提供了多样化解决方案.

4 QS-NLA 方案的实验实现

除了理论进展外, 随着当前量子技术的发展, NLA 的实验实现也取得了较大进步. 基于 QS 的放大器通过光子数截断和后选择实现对目标量子态的无噪声线性放大, 且放大前后保持量子相干性不变, 是量子信息处理中的重要技术. NLA 的实验实现依赖于高精度单光子探测和量子干涉技术, 未来在集成量子光学中有广阔应用前景. 下面简述基于 QS-NLA 方案的几个实验实现方案.

2010 年, Xiang 等 [10] 提出通过线性光学元件与光子计数结合的方法来实现 2009 年 Ralph 和 Lund[8] 提出的相干态的 NLA 方案, 并进行了实验验证. 该实验装置图如图 13 所示. 首先利用 SPDC 产生水平偏振的单光子对 ($|1_H 1_H\rangle$), 作为输入态和辅助光子. 利用半波片 (half wave plate, HWP) 和 PBS 实现可调节分束器的功能. 通过调节 HWP 角度到合适的参数, 根据 D_1 和 D_2 或 D_3 的双光子复合测量进行输入校准和放大操作. 然后再次调节 HWP 的角度, 将放大后的输出态与参考光束进行干涉叠加, 调节相位 ϕ 并记录干涉条纹. 若为无噪声线性放大, 条纹可见度 V 应接近 1; 若为普通线性放大, 条纹可见度会因相位噪声显著降低, 从而验证了放大过程的线性与低噪声特性. 最终将得到的实验结果与理论结果进行比较, 成功在实验室中实现了相干态的 NLA, 为长距离量子通信和纠缠蒸馏提供了重要的技术验证.

同年, Ferreyrol 等 [46] 提出了上述放大方案的另一种实现方式: 使用 SPDC 源生成纠缠光子对, 一个光子作为辅助光子, 另一个光子用于触发方案成功的情况. 输入信号经过高损耗信道后形成混合态, 再输入到放大器中通过使用零差检测和最大似然重构算法 [47] 来确定不同振幅和增益下输出态的 Wigner 准概率分布图像, 验证其噪声特性.

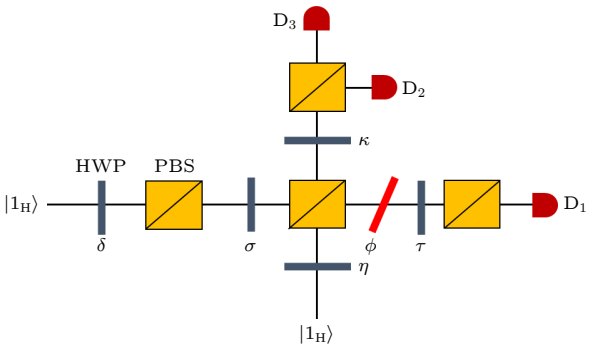


图 13 相干态的 NLA 方案的实验实现 [10]. 采用极化编码, 半波片和 PBS 实现可调谐分束器, 倾斜的 QWP 实现移相器. 辅助光子是一个单光子, 而输入态是由单光子产生的混合态

Fig. 13. Experimental implementation of an NLA protocol of coherent states[10]. In polarization mode, the half-wave plate and PBS are used to achieve a tunable beam splitter, and the inclined quarter-wave plate is a phase shifter. The auxiliary particle is a single photon, while the input state is the mixed state produced by a single photon.

上述两种 NLA 实现方式应用于基于连续变量的量子信息科学中. 在 DV 量子体系中, Osorio 等 [9] 于 2012 年在实验上实现了对电信波段的单光子的无噪声线性放大, 最大增益可达 $g = 1.98 \pm 0.20$, 突出了量子放大器在基于量子中继器的长距离量子通信中的潜力. 随后, 2013 年 Kocsis 等 [18] 通过实验实现了单光子极化量子比特 (qubit) 的放大, 为实现长距离 DI QKD 开辟了新的道路.

5 总结与展望

NLA 作为量子信息处理中的重要技术, 已经在理论研究和实验实现方面取得了显著进展. 尽管仍面临成功概率低、器件效率要求高等技术挑战, 但随着量子操作技术的不断进步, NLA 将在量子通信、量子计算和精密测量等领域发挥越来越重要的作用.

本文将现有的 NLA 方案分为两类: DV 量子系统和 CV 量子系统. 在 DV 量子系统中, 详细介绍了单光子、单光子极化编码量子比特和单光子空间纠缠态的 NLA 方案. 近年来, 科学家们对量子态放大进行了更深入的研究和改进, 并提出在 QS 器件中增加局部正交压缩操作, 以双光子纠缠态作

为辅助态, 与纠缠浓缩相结合, 使用 Kerr 介质进行多次循环放大等高效的 NLA 方案, 不仅提高了方案的成功概率, 而且达到了更好的放大效果. 在 CV 量子系统中, 基于 QS 的 NLA 方案不断改进, 不断提高放大阶数, 改良了放大器在 CV 光场中的放大性能, 基于光子加减法、测量滤波、量子催化等方案也被相继提出, 分别从成功概率和保真度等方面对 CV-NLA 方案进行改良, 并得到广泛应用. 除了理论上的进展, 随着当前量子技术的发展, NLA 的实验实现也取得了很大进展, 介绍 QS-NLA 方案的典型实验实现, 有助于其进一步发展.

随着量子信息技术发展, 科学家们追求以消耗更少的光学器件和辅助量子资源达到更好的放大效果, 提出了基于量子催化的 NLA 方案 [36], 它只使用 QS 方案中 50% 的量子资源, 但在相同的成功概率下得到了更好的增益, 在连续变量的放大中提出将基于 n-QS 方案的无噪声放大器扩展到一般的干涉耦合 [48], 放大过程仅用一个 N 模分束器和对应数量的探测器, 就可以实现将 Fock 态截断到任意阶, 而且成功概率大大提高. 这些方面都将成为以后 NLA 研究的重点, 推动 NLA 的实用化发展.

参考文献

[1] Scarani V, Bechmann-Pasquinucci H, Cerf N J, Dušek M, Lütkenhaus N, Peev M 2009 *Rev. Mod. Phys.* **81** 1301
[2] Briegel H J, Dür W, Cirac J I, Zoller P 1998 *Phys. Rev. Lett.* **81** 5932
[3] Duan L M, Lukin M, Cirac I, Zoller P 2001 *Nature* **414** 413
[4] Zhao B, Chen Z B, Chen Y A, Schmiedmayer J, Pan J W 2007 *Phys. Rev. Lett.* **98** 240502
[5] Briegel H J, Browne D E, Dür W, Raussendorf R, Nest M V den 2009 *Nat. Phys.* **5** 19
[6] Azuma K, Tamaki K, Lo H K 2015 *Nat. Commun.* **6** 6787
[7] Goswami S, Dhara S 2023 *Phys. Rev. Appl.* **20** 024048
[8] Ralph T C, Lund A P 2009 *Proceedings of the 9th International Conference* **1110** 155
[9] Osorio C I, Bruno N, Sangouard N, Zbinden H, Gisin N, Thew R T 2012 *Phys. Rev. A* **86** 023815
[10] Xiang G Y, Ralph T C, Lund A P, Walk N, Pryde G J 2010 *Nat. Photonics* **4** 316
[11] Gisin N, Pironio S, Sangouard N 2010 *Phys. Rev. Lett.* **105** 070501
[12] Curty M, Moroder T 2011 *Phys. Rev. A* **84** 010304
[13] Pitkanen D, Ma X, Wickert R, Van Loock P, Lütkenhaus N 2011 *Phys. Rev. A* **84** 022325
[14] Zhang S, Yang S, Zou X, Shi B, Guo G 2012 *Phys. Rev. A* **86** 034302
[15] Monteiro F, Verbanis E, Vivoli V C, Martin A, Gisin N, Zbinden H, Thew R T 2017 *Quantum Sci. Technol.* **2** 024008
[16] Meyer-Scott E, Bula M, Bartkiewicz K, Černoch A, Soubusta J, Jennewein T, Lemr K 2013 *Phys. Rev. A* **88** 012327
[17] Yang S, Zhang S, Zou X, Bi S, Lin X 2013 *Phys. Rev. A* **87** 024302
[18] Kocsis S, Xiang G Y, Ralph T C, Pryde G J 2013 *Nat. Phys.* **9** 23
[19] Zhou L, Sheng Y B 2013 *J. Opt. Soc. Am. B* **30** 2737
[20] Zhou L, Sheng Y B 2015 *Laser Phys. Lett.* **12** 045203
[21] Ou-Yang Y, Feng Z F, Zhou L, Sheng Y B 2015 *Laser Phys.* **26** 015204
[22] Zhou L, Chen L Q, Zhong W, Sheng Y B 2018 *Laser Phys. Lett.* **15** 015201
[23] Wang D D, Jin Y Y, Qin S X, Zu H, Zhou L, Zhong W, Sheng Y B 2018 *Quantum Inf. Process.* **17** 56
[24] Yang G, Zhang Y S, Yang Z R, Zhou L, Sheng Y B 2019 *Quantum Inf. Process.* **18** 317
[25] Li Y P, Zhang J, Xu B W, Zhou L, Zhong W, Sheng Y B 2020 *Quantum Inf. Process.* **19** 261
[26] Xu B W, Zhang J, Zhou L, Zhong W, Sheng Y B 2021 *Quantum Inf. Process.* **20** 163
[27] Feng Y P, Gu J Q, Zhou L, Zhong W, Du M M, Li X Y, Sheng Y B 2024 *Quantum Inf. Process.* **23** 201
[28] Seshadreesan K P, Krovi H, Guha S 2019 *Phys. Rev. A* **100** 022315
[29] Winnel M S, Hosseinidehaj N, Ralph T C 2020 *Phys. Rev. A* **102** 063715
[30] He M, Malaney R, Burnett B A 2021 *Phys. Rev. A* **103** 012414
[31] Zhong W, Li Y P, Sheng Y B, Zhou L 2022 *Europhys. Lett.* **140** 18003
[32] Guanzon J J, Winnel M S, Lund A P, Ralph T C 2022 *Phys. Rev. Lett.* **128** 160501
[33] Zhu Y, Zhu W, Zhong W, Du M, Sheng Y, Zhou L 2023 *Chin. Sci. Bull.* **68** 2411
[34] Zavatta A, Fiurášek J, Bellini M 2010 *Nat. Photonics* **5** 52
[35] Chrzanowski H M, Walk N, Assad S M, Janousek J, Hosseini S, Ralph T C, Symul T, Lam P K 2014 *Nat. Photonics* **8** 333
[36] Ulanov A E, Fedorov I A, Pushkina A A, Kurochkin Y V, Ralph T C, Lvovsky A I 2015 *Nat. Photonics* **9** 764
[37] Fiurášek J 2024 *Opt. Express* **32** 2527
[38] Xin J 2024 *Opt. Express* **32** 48541
[39] Notarnicola M N, Olivares S 2023 *Phys. Rev. A* **108** 022404
[40] Acín A, Gisin N, Masanes L 2006 *Phys. Rev. Lett.* **97** 120405
[41] Acín A, Brunner N, Gisin N, Massar S, Pironio S, Scarani V 2007 *Phys. Rev. Lett.* **98** 230501
[42] Pironio S, Acin A, Brunner N, Gisin N, Massar S, Scarani V 2009 *New J. Phys.* **11** 045021
[43] Lee H W, Kim J 2000 *Phys. Rev. A* **63** 012305
[44] Hessmo B, Usachev P, Heydari H, Björk G 2004 *Phys. Rev. Lett.* **92** 180401
[45] Halenková E, Černoch A, Lemr K, Soubusta J, Drusová S 2012 *Appl. Opt.* **51** 474
[46] Ferreyrol F, Barbieri M, Blandino R, Fossier S, Tualle-Brouri R, Grangier P 2010 *Phys. Rev. Lett.* **104** 123603
[47] Lvovsky A I 2004 *J. Opt. B: Quantum Semiclassical Opt.* **6** S556
[48] Fiurášek J 2022 *Phys. Rev. A* **105** 062425

SPECIAL TOPIC—Quantum information processing

Quantum non-deterministic noiseless linear amplification*

CUI Shihe [1)] DU Mingming [2)] LI Xiyun [1)] ZHOU Lan [1)†] SHENG Yubo [2)]

1) (*College of Science, Nanjing University of Posts and Telecommunications, Nanjing* 210023, *China*)

2) (*College of Electronic and Optical Engineering and College of Flexible Electronics* (*Future Technology, Nanjing University of Posts and Telecommunications, Nanjing* 210023, *China*)

(Received 2 July 2025; revised manuscript received 29 July 2025)

Abstract

Quantum communication can realize secure information transmission based on the fundamental principles of quantum mechanics. Photon is a crucial information carrier in quantum communication. The photonic quantum communication protocols require the transmission of photons or photonic entanglement between communicating parties. However, in this process, photon transmission loss inevitably occurs due to environmental noise. Photon transmission loss significantly reduces the efficiency of quantum communication and even threatens its security, so that it becomes a major obstacle for practical long-distance quantum communication. Quantum noiseless linear amplification (NLA) is a promising method for mitigating photon transmission loss. Through local operations and post-selection, NLA can effectively increase the fidelity of the target state or the average photon number in the output state while perfectly preserving the encoded information of the target state. As a result, employing NLA technology can effectively overcome photon transmission loss and extend the secure communication distance.

In this paper, the existing NLA protocols are categorized into two types, i.e. the NLA protocols in DV quantum systems and CV quantum systems. A detailed introduction is given to the quantum scissor (QS)-based NLA protocols for single photons, single-photon polarization qubits, and single-photon spatial entanglement in the DV quantum systems. The QS-based NLA can effectively increase the fidelity of the target states while perfectly preserving its encodings. In recent years, researchers have made efforts to study various improvements to the QS-based NLA protocols. In the CV quantum systems, researchers have adopted parallel multiple QS structure and generalized QS to increase the average photon numbers of the Fock states, coherent states and two-mode squeezed vacuum states. In addition to theoretical advancements, significant progress has also been made in the experimental implementations of NLA. The representative experimental demonstrations of QS-based NLA protocols are summarized.

Finally, the future development directions for NLA to facilitate its practical applications are presented. This review can provide theoretical support for practically developing NLA in the future.

Keywords: quantum communication, quantum noise-free linear amplification, continuous variables, discrete variables

PACS: 03.67.Pp, 03.67.Hk, 03.65.Ud **DOI:** 10.7498/aps.74.20250865

CSTR: 32037.14.aps.74.20250865

* Project supported by the National Natural Science Foundation of China (Grant Nos. 12175106, 92365110).

† Corresponding author. E-mail: zhoul@njupt.edu.cn

专题: 量子信息处理

量子身份认证研究进展*

王兴福[1)] 郑艳艳[2)†] 顾世浦[3)] 张琦[1)] 钟伟[4)] 杜明明[3)]
李喜云[1)] 沈淑婷[3)] 张安蕾[1)] 周澜[1)] 盛宇波[3)‡]

1) (南京邮电大学理学院, 南京 210023)

2) (延安大学物理与电子信息学院, 延安 716000)

3) (南京邮电大学电子与光学工程学院、柔性电子 (未来技术) 学院, 南京 210023)

4) (南京邮电大学通信与信息工程学院, 南京 210003)

(2025 年 7 月 12 日收到; 2025 年 9 月 5 日收到修改稿)

量子通信具有感知窃听的功能, 这是其区别于经典通信而独有的优势, 能够为信息安全提供新的保障. 在实际应用中, 量子通信具有绝对安全性的前提是所有通信方均是合法通信方, 然而, 这在实际通信环境中难以保证, 为量子保密通信带来安全性隐患. 因此, 在通信之前对通信方进行身份认证具有重要意义. 量子身份认证利用量子力学基本原理在通信方之间实现单向或双向身份认证, 并能确保身份认证码的绝对安全, 在量子通信领域具有重要的研究价值. 本文系统地梳理了量子身份认证协议的研究历程, 根据所需的不同量子资源对基于单光子、纠缠态、连续变量、混合型变量的量子身份认证协议进行介绍, 又根据身份认证过程中使用的量子协议类型, 介绍了基于量子密钥分发、量子安全直接通信、量子隐形传态以及乒乓协议框架的量子身份认证协议, 并分析各类协议在效率、安全性及实用化方面的优缺点. 最后, 详细地介绍了最新的量子身份认证协议——基于 GHZ 态的多方同步身份认证协议以及具有身份认证功能的极化-空间超编码的三方量子安全直接通信协议, 并对量子身份认证的未来发展方向以及在量子通信领域的应用潜力进行展望. 本综述可为未来量子身份认证的实用化发展提供理论支持.

关键词: 量子身份认证, 量子保密通信, 量子纠缠

PACS: 03.67.Pp, 03.67.Hk, 03.65.Ud **DOI:** 10.7498/aps.74.20250920

CSTR: 32037.14.aps.74.20250920

1 引 言

在数字化浪潮中, 信息交互的广泛性与复杂性对信息安全体系提出了更高要求. 传统公钥密码学依赖大整数分解或离散对数等难题构建的安全屏障[1–3], 正面临量子计算的巨大冲击. 量子计算机通过量子并行性与 Shor 算法[4] 等机制, 可在短时间内破解经典加密体系, 使得金融交易、政务通信、医疗数据等核心领域的信息防护体系面临系统性风险. 在此背景下, 量子通信依托量子态叠加、量子纠缠、量子不可克隆原理、不确定性原理等量子力学的基本原理[5,6], 为构建新型安全通信提供了理论根基. 量子通信包含量子密钥分发 (quantum key distribution, QKD)[7–9]、量子隐形传态 (quantum teleportation, QT)[10–13]、量子秘密共享 (quantum secret sharing, QSS)[14–17]、量子安全直接通信 (quantum secure direct communication,

* 国家自然科学基金 (批准号: 12175106, 92365110) 资助的课题.

† 通信作者. E-mail: yyz@yau.edu.cn

‡ 通信作者. E-mail: shengyb@njupt.edu.cn

QSDC)[18–20] 等重要分支, 理论上具有绝对安全性. 在过去三十年中, 量子通信技术在理论和实验方面都取得了巨大进展[21–53]. 在实际操作中, 任何安全通信协议的成功实施都需要以身份认证为前提, 即必须事先检验实际通信方的身份是否合法. 只有合法的通信方之间才能进一步进行通信. 因此, 构建量子安全认证体系已成为量子保密通信研究的重要课题之一.

量子身份认证 (quantum identity authentication, QIA) 是量子认证的一个重要分支. QIA 允许通信方基于量子力学的基本原理证明自己的身份, 并能确保身份认证码的绝对安全, 通常作为登录量子通信系统的第一步. QIA 是一种有效防止窃听者 (Eve) 在通信中冒充合法用户窃取传递的密钥和信息 (扮演攻击) 的方法. 只有当实际通信方均是合法用户时, 量子通信协议的无条件安全性才能得到保证[54–61]. 早期的 QKD 协议本质上考虑使用经典身份认证协议. 直到 1995 年, Crépeau 和 Salvail[62] 提出了首个基于不经意传输 (oblivious transfer, OT) 的协议. 在该协议提出之后, 出现了一系列关于 QIA 的工作. 1998 年 Zeng 和 Wang[63] 提出了一种 QKD 协议, 该协议允许同时分发密钥和验证通信者的身份. 1999 年, Dušek 等[54] 结合经典识别过程和 QKD 协议提出了两种量子相互认证协议. 这些协议均是通过结合经典认证协议和 QKD 协议提出的, 特别强调一次性密码. 严格来说, 这些协议是混合型的协议. 在伴随量子通信技术的进步的同时, 量子身份认证协议也同步演变和发展.

从应用维度看, QIA 的价值贯穿国家战略至民生领域. 在国家安全层面, 有效防范敌对方的渗透与信息战攻击, 为军事指挥、外交密电、关键基础设施管控等场景提供身份核验保障; 在社会经济领域, 支撑金融系统的大额交易认证、智能电网的隐私数据交互以及电子政务的机密公文传输, 遏制诈骗与数据泄漏风险; 在公共服务方面, 保障远程医疗的诊疗信息安全、跨境物流的电子单证可信性, 推动数字化服务的高效落地; 对于个体用户而言, 其通过保护生物特征、财产账户等隐私数据, 构建了数字身份主权的新型防护范式. 因此, QIA 的研究具有重要的应用价值.

此外, 在许多前沿的多用户量子任务中, QIA 更是发挥着不可或缺的基础安全作用. 例如, 在量子群组密钥分发 (group QKD)[64] 中, 需要首先对所有组成员身份进行认证, 以确保生成的密钥在合法用户间安全共享; 在量子数字签名 (quantum digital signature, QDS)[65] 方案中, 签名方的身份真实性是防止伪造和抵赖的前提; 在基于量子安全多方计算 (quantum secure multi-party computing, QSMPC) 或量子区块链的共识机制中[66], 参与节点的身份认证是防止恶意节点入侵、确保计算与共识结果可信的关键一环; 在量子中继网络中, 对中继节点的身份认证更是构建可信量子通道的基础. 因此, 对 QIA 的研究是推动这些高级量子应用从理论走向实践的必经之路.

本文的其余部分组织如下. 第 2 节从使用的量子资源和量子协议两个方面对现有的 QIA 协议进行分类, 并着重介绍一些关注度高的 QIA 协议. 第 3 节介绍一个最新的 QIA 协议和具有身份认证功能的极化-空间超编码的三方量子安全直接通信协议. 最后, 第 4 节对 QIA 进行了总结和展望.

2 量子身份认证的分类

根据不同的标准可以对量子身份认证进行分类. 本文将从以下两个方面对量子身份认证进行分类介绍, 即根据 QIA 所使用的量子资源和所使用的量子协议. 由于文献数量众多, 我们只对一些代表性工作进行介绍, 有望能清晰地展现各类型协议的执行过程和使用场景.

2.1 根据量子资源分类

根据 QIA 协议中使用的核心量子资源类型, 将 QIA 协议分类如下: 基于单光子、纠缠态、连续变量 (continuous variable, CV) 和混合型变量的 QIA 协议.

2.1.1 基于单光子的协议

利用单光子 (极化光子、相位编码光子等) 作为核心资源, 通过量子态的测量或单粒子操作实现认证. 其特点是资源需求低, 兼容现有量子光学器件 (如单光子探测器); 实验实现简单, 适用于低资源环境 (如量子物联网). 协议的安全性依赖单光子的不可克隆性, 可能需结合经典加密增强.

2009 年 Zhang[67] 提出了一种仅需单光子操作的单向 QIA 协议, 首次引入经典公钥基础设施的

核心思想, 降低了实现复杂度. 2017 年 Hong 等[68]提出了一种单光子态编码优化 QIA 协议, 因为允许使用单个量子比特对两位认证密钥序列进行认证, 该协议对资源的需求相对较低, 并且效率较高. Zawadzki[69] 在 2019 年指出 Hong 等的 QIA 协议存在安全缺陷, 并对该协议提出了改进, 通过哈希函数与动态会话密钥, 进行编码优化与流程精简. 后来在 2021 年 González-Guillén 等[70] 指出 Zawadzki 的协议容易受到密钥空间缩减攻击, 并设计首个针对哈希-量子混合认证协议的攻击策略, 通过实验验证密钥空间几何缩减效应. 有趣的是, Calsi 和 Kohl[71] 在 2024 年再次指出 Hong 等的 QIA 协议存在一个额外漏洞, 该漏洞源于诱骗态生成与管理策略的缺陷, 并展示了一个能有效解决该问题的简易缓解协议. 对已提出的协议, 分析其漏洞, 并设计出无此漏洞的改进协议, 这种密码分析过程在密码学领域非常普遍, 也可视为推动 QIA 发展的一个典型例子. 2023 年 Rao 和 Jayaraman[72] 提出了一种保留预共享密钥信息的新型 QIA 协议, 仅使用单光子与经典信道完成双向认证, 通过动态基矢生成与相位反冲检测, 显著降低预共享密钥泄漏风险.

简述 Rao 和 Jayaraman[72] 的 QIA 协议如下.

步骤 1 协议初始化. Alice 和 Bob 预先共享 n 位密钥 $K=\{k_1,k_2,\cdots,k_n\}$, Alice 随机选择起始位置 i 和距离 r ($1\leqslant i,\ r\leqslant n$), 认证密钥长度 $m=10\%\times n$. Alice 通过经典信道向 Bob 发送 $(i,\ r)$, Bob 随机生成认证密钥 $B_K=\{B_{k1},B_{k2},\cdots,B_{kn}\}$, 两个诱骗态序列 D_{AK}, D_{BK}.

步骤 2 Bob 量子通信阶段. Bob 基于预共享密钥动态生成基矢: $x_t=k_{i-r}\oplus k_{i+r}$, $y_t=k_{i-r}\oplus k_i$, $z_t=k_i\oplus k_{i+r}$ ($t\leqslant m$). 若 $x_t=0$, Bob 将量子态编码为 $|0\rangle$ 或 $|1\rangle$; 若 $x_t=1$, 则编码为 $|+\rangle$ 或 $|-\rangle$. 分别用基矢 y_t 和 z_t 编码诱骗态 D_{AK} 和 D_{BK}. 将序列 QB_{kt}, $QD_{\mathrm{A}kt}$ 和 $QD_{\mathrm{B}kt}$ 通过量子信道发送给 Alice. Alice 使用相同规则生成 x_t, y_t, z_t, 并分别测量 QB_{kt}, $QD_{\mathrm{A}kt}$, $QD_{\mathrm{B}kt}$, 对应存储 B'_{kt}, $D'_{\mathrm{A}kt}$, $D'_{\mathrm{B}kt}$.

步骤 3 诱骗态验证. Alice 公布诱骗态, 通过经典信道发送 D'_{AK} 给 Bob. 比较 D'_{AK} 与 Bob 的原始 D_{AK}, 若错误率大于 QBER, 终止协议, 否则继续.

步骤 4 Alice 量子通信阶段. Alice 随机生成认证密钥 $A_K=\{A_{k1},A_{k2},\cdots,A_{kn}\}$, 动态生成基矢 $D'_{\mathrm{B}kt}\oplus B'_{kt}$, 并用该基矢编码 A_{kt} 为 QA_{kt}, 发送给 Bob. Bob 用相同基矢 $D_{\mathrm{B}kt}\oplus B_{kt}$ 测量 QA_{kt}, 并存储 A'_{kt}.

步骤 5 经典信道身份认证. Alice 公布 A_K, Bob 公布 B_K, 交叉验证是否满足 $A_K=A'_K$ 且 $B_K=B'_K$. 若匹配, 身份认证成功, 进行安全通信; 若不匹配, 则终止协议并重启.

从以上协议可以看出, 协议利用单光子的极化特性进行编码和测量, 强调实用性与效率, 但存在密钥管理漏洞.

2.1.2 基于量子纠缠的 QIA 协议

此类 QIA 协议使用量子纠缠作为核心资源, 通过纠缠特性 (如非局域关联性、不可分割性) 来保障安全性. 其特点是需高精度制备和维持多粒子纠缠态, 实验复杂度较高; 适用于需要高安全性的长距离或多方身份认证场景.

Zeng 和 Zhang[55] 在 2000 年提出了一种基于贝尔态的 QIA 协议. 该协议是量子密码学中首个身份验证与密钥分发一体化协议, 密钥分发通过之前的 Einstein-Podolsky-Rosen(EPR)QKD 协议实现, 身份认证过程通过对称密码协议实现. 尽管受限于当时的量子存储技术, 但其设计思想为后续无信任中心的 QIA 协议奠定了基础. 2006 年, Lee 等[73]提出了利用第三方 Trent 生成 Greenberger-Horne-Zeilinger(GHZ) 态, 执行用户身份认证的 QIA 协议, 首次将用户认证与消息传输结合. 发送方 Alice 无需同接收方 Bob 预先共享密钥, 可以直接向 Bob 发送秘密消息, 且无需 Alice 与 Bob 间的直接量子信道, 适用于受限网络环境. 有趣的是, 在 2007 年 Zhang 等[74] 认为 Lee 的协议假设 Trent 完全可信且不窃取秘密信息, 但未限制 Trent 获取消息的能力. Trent 可通过拦截-测量-重发攻击和单量子比特测量攻击窃取消息, 因此协议存在安全漏洞. 他们将原协议中的比特翻转操作 X 替换为泡利 Z 操作 (相位翻转), 这样的改进不影响计算基的测量结果, 也不破坏协议功能, 但改变叠加态的相位, 使得 Trent 无法通过简单操作还原编码信息.

2014 年, Chang 等[75] 提出了一种基于五粒子团簇态和量子一次性密码的受控量子安全直接通信协议, 旨在实现多方权限控制与高效信息传输. 协议中, 光子 1, 2 用于信息编码, 光子 3, 5 供接收方 Bob 解密, 光子 4 作为控制器 Charlie 的权限标

识. 通过动态酉操作 (I/U) 调制光子 4 的状态 (依据 Bob 的身份码), 确保控制器无法独立获取明文.

2020 年, Zhang 等[76] 提出了一种基于贝尔态和纠缠交换的 QIA 协议, 旨在解决传统协议中存在的第三方信任问题与单向认证局限. 引入半诚实第三方 Charlie 负责制备贝尔态、分发粒子并验证结果, 但无法获取用户的共享密钥. 区别于传统协议中完全可信或不可信的第三方, Charlie 不参与密钥相关操作, 显著降低其窃取密钥的可能性, 支持双向认证且无需用户间额外通信, 效率更高. 2023 年, Dutta 和 Pathak[77] 提出了一种融合受控量子通信与 Bell 态操控技术的 QIA 协议, 在资源效率、安全性和功能性上均优于部分经典协议. 其核心创新在于双向认证机制、第三方半诚实假设下的鲁棒性, 以及对低复杂度量子资源的有效利用, 同时可抵御多种量子攻击.

简述 Zeng 和 Zhang[55] 的 QIA 协议如下.

步骤 1 初始阶段 (通过可信中心建立共享密钥 K_1). Alice 和 Bob 向可信信息中心 (TIC) 注册身份标识 $\mathrm{ID_A}$ 和 $\mathrm{ID_B}$, TIC 分别与 Alice 和 Bob 建立量子信道. TIC 制备两个单态 EPR 对, 可表示为

$$|\Phi_{\mathrm{ac}}\rangle = \sqrt{\frac{1}{2}}\left(|\uparrow_{\mathrm{a}}\downarrow_{\mathrm{c}}\rangle - |\downarrow_{\mathrm{a}}\uparrow_{\mathrm{c}}\rangle\right),$$

$$|\Phi_{\mathrm{bc}}\rangle = \sqrt{\frac{1}{2}}\left(|\uparrow_{\mathrm{b}}\downarrow_{\mathrm{c}}\rangle - |\downarrow_{\mathrm{b}}\uparrow_{\mathrm{c}}\rangle\right),$$

也可写为

$$|\Phi_{\mathrm{ac}}\rangle = \sqrt{\frac{1}{2}}\left(|\nearrow_{\mathrm{a}}\searrow_{\mathrm{c}}\rangle - |\searrow_{\mathrm{a}}\nearrow_{\mathrm{c}}\rangle\right),$$

$$|\Phi_{\mathrm{bc}}\rangle = \sqrt{\frac{1}{2}}\left(|\nearrow_{\mathrm{b}}\searrow_{\mathrm{c}}\rangle - |\searrow_{\mathrm{b}}\nearrow_{\mathrm{c}}\rangle\right).$$

其中, $|\uparrow\rangle$, $|\downarrow\rangle$ 是 $\hat{S}_z$ 的本征态, $|\nearrow\rangle$, $|\searrow\rangle$ 是 $\hat{S}_x$ 的本征态. TIC 发送粒子 a 给 Alice, 粒子 b 给 Bob, 自己保留粒子 c. Alice 和 Bob 独立随机选择测量基 ($\hat{S}_z$ 或 $\hat{S}_x$) 测量各自粒子. 测量后, 粒子处于四个态 $|\uparrow\rangle$, $|\downarrow\rangle$, $|\nearrow\rangle$, $|\searrow\rangle$ 之一. TIC 对剩余粒子进行总自旋测量, 若结果 $s=1$, 则丢弃; 若结果 $s=0$, 则保留, 说明粒子处于单态, Alice 和 Bob 的结果必然相反. Alice 和 Bob 公布测量基, 但不公布结果. 若使用相同基, 测量结果相反, 转换为密钥比特; 若使用不同基, 则丢弃结果. 最终生成共享密钥 K_1. 该过程中 TIC 无法获取 K_1, 因为投影测量 $s=0$ 不泄漏信息.

步骤 2 验证阶段 (身份验证+新密钥分发). 将密钥 K_1 转换为测量基序列 M_{K1}, 可约定密钥 0 对应直角基, 密钥 1 对应对角基, 或者反过来 (如 $K_1=001101$, $M_{K1}=\odot\odot\oplus\oplus\odot\oplus$). Alice 制备 EPR 对为四个贝尔态之一, 如 ($|\psi_{\mathrm{ab}}\rangle=\sqrt{1/2}(|\uparrow_{\mathrm{a}}\downarrow_{\mathrm{b}}\rangle - |\downarrow_{\mathrm{a}}\uparrow_{\mathrm{b}}\rangle)$), 保留粒子 a, 发送粒子 b 给 Bob. Alice 随机选择基测量粒子 a, 则 Bob 粒子 b 的状态发生塌缩. Bob 对粒子 b 进行两种基测量: 身份验证基 M_{K1}(由 K_1 确定的固定基) 和密钥分发基 M(随机选择, 用于生成新密钥). Bob 将 M_{K1} 基的测量结果 m 和位置编号 N_{i} 用 K_1 加密后, 发送密文 y 给 Alice. Alice 用 K_1 解密, 比对自身测量结果: 若匹配, 则 Bob 身份真实. Alice 将解密结果 m'发送给 Bob 验证, 若 $m'=m$, 则 Alice 身份真实. 身份验证通过后, 双方用剩余粒子 (M 基测量结果) 执行标准 EPR 协议, 生成新密钥 K. 丢弃旧共享密钥 K_1, 从新密钥 K 中提取部分比特作为下次共享密钥 K_2.

2.1.3 基于连续变量的 QIA 协议

此类 QIA 协议利用 CV 量子态 (如压缩态、相干态) 的统计特性或纠缠特性实现身份认证. 其特点是利用光场的连续参数 (如相位、振幅) 编码信息, 在短距离城域网中效率优于离散变量协议. 同时, 此类协议的实验复杂度较低 (无需单光子探测), 但需高精度调制技术. 适用于光纤量子通信网络中的高效身份认证和与经典光通信系统融合的混合量子网络.

2016 年, Ma 等[78] 首次将 CV 量子态引入身份认证框架, 提出了一种基于 CV 的 QIA 协议. 该协议利用双模压缩态与相干态实现用户身份的动态验证与密钥更新. 有趣的是, 在相对较短的距离内, CV QKD 协议比其离散变量 QKD 协议表现更好[79–81]. 因此, 对于城域网, 配备 CV QIA 的 CV QKD 有望实现更高效安全的密钥分发. 2024 年, Chen 等[82] 提出了一种基于 CV 系统的双向 QIA 协议, 利用双模压缩光场的纠缠特性实现合法用户间的相互身份验证. 通过引入诱骗态序列与参数 F (表征纠缠度), 协议不仅能够抵御高斯克隆攻击, 还可实时检测窃听者的存在, 为量子通信网络中的身份认证提供了高安全性的解决协议. 比较而言, Ma 等[78] 的协议需要贝尔态测量与位移操作, 实验复杂度较高, 而后者依赖双模压缩态的直接传输, 实验复杂度较低.

简述 Ma 等[78] 的 QIA 协议如下.

Alice 和 Bob 预先共享初始认证密钥 $K_{\rm a}$. Alice 对两个初始真空态 $|0\rangle$ 应用双模压缩算子, 生成两个纠缠模 $\hat{a}_1$ 和 $\hat{a}_2$, 并将 $\hat{a}_2$ 发送给 Bob. Alice 将二进制初始密钥 $K_{\rm a}$ 转换为十进制数 $k_{\rm a}$, 并随机选取两个十进制数 $y_{\rm a}$ 和 $z_{\rm a}$. Alice 分别对真空态应用位移算子 $\hat{D}(\alpha_3)$ 和 $\hat{D}(\alpha_{3\rm D})$, 获得两个分别在 $\hat{a}_3$ 模和 $\hat{a}_{3\rm D}$ 模的纠缠态, 分别用于密钥更新和身份认证. Alice 每次随机选择 $\hat{a}_3$ 或 $\hat{a}_{3\rm D}$ 与 $\hat{a}_1$ 进行联合贝尔态测量, 得到 $X_{\rm u}$ 和 $P_{\rm u}$, 并将其公开给 Bob. Bob 对 $\hat{a}_2$ 应用酉变换 $\hat{D}(u=\sqrt{2}(X_{\rm u}+{\rm i}P_{\rm u}))$, 随机选择基 ($X$ 或 P) 测量, 得到序列 ξ. Alice 公开诱骗态的时间区间, Bob 从 ξ 中提取诱骗态对应结果 $\xi_{3\rm D}$, 剩余为 ξ_3 (用于密钥更新). Bob 将二进制初始密钥 $K_{\rm a}$ 转为十进制数 k'_a, 计算 $z_{\rm b}=\xi_{3\rm D}-\varphi k'_{\rm a}$, 并公开. 通过定义保真度 $H=\langle[z_{\rm b}-\lambda z_{\rm a}]^2\rangle_{\rm min}$ 进行判断: 若 $H=0$, 则 Bob 身份合法, 无窃听; 若 $H>0$, 存在 Eve 或 Bob 非法, 通信中止. 身份验证通过后, Alice 和 Bob 从 ξ_3 提取新密钥 (与 $y_{\rm a}$ 相关).

2.1.4 基于混合型变量的 QIA 协议

基于混合型变量的 QIA 协议结合多种量子资源 (如单光子+纠缠态) 或量子与经典资源 (如哈希函数+量子态), 利用量子物理特性抵御量子攻击, 经典密码学增强协议的鲁棒性. 其特点是平衡资源效率与安全性, 降低对单一量子源的依赖. 然而, 此类协议需协调量子与经典操作的同步性, 可能引入新攻击. 此类 QIA 协议适用于资源受限的量子-经典混合网络 (如边缘计算节点) 和需要兼容现有密码学基础设施的过渡阶段应用.

2009 年, Liu 等[83] 提出了一种改进的确定性安全量子通信 (deterministic secure quantum communication, DSQC) 协议, 结合四量子比特簇态与单光子身份认证机制, 核心创新在于利用四维簇态的纠缠特性, 将每簇态的编码容量提升至 2 比特, 显著优化了经典信息的传输容量与协议安全性. 2020 年, Zhu 等[84] 通过融合身份认证与密钥协商 (quantum key agreement, QKA), 提出了一种无需纠缠的高效 QIA-QKA 协议. 该协议利用单光子编码+动态密钥更新, 实现量子与经典的结合. 传统协议将 QIA 与 QKA 分离, 导致资源冗余. 他们采用单光子编码及动态密钥更新机制, 仅需 2 轮通信, 复杂度低. 协议可抵抗中间人攻击、重放攻击、冒充攻击等, 并支持前向安全性 (动态密钥更新), 在安全性、效率和实用性上均优于传统协议. 另外, 2006 年 Wang 等[85] 提出混合 GHZ 态+经典哈希函数的协议和 2014 年 Yuan 等[86] 提出混合单粒子态+乒乓技术 (量子态动态传输) 的协议也可视为混合型协议.

简述 Liu 等[83] 的协议如下.

步骤 1 Alice 和 Bob 预先共享一个长度为 d 的二进制种子密钥 SK, 经扩展函数 G 生成长度为 k 的扩展密钥 EK, 要求 EK 满足随机性 (0 和 1 出现概率各为 1/2).

步骤 2 将 EK 均分为 Alice 身份密钥 $EK_{\rm A}$ 和 Bob 身份密钥 $EK_{\rm B}$. 进一步将分为基序列信息 $EK_{\rm A1}$ 和比特值序列信息 $EK_{\rm A2}$; $EK_{\rm B}$ 同理分割. 当 Alice 向 Bob 发送消息时, 使用 $EK_{\rm A}$ 认证 Alice 身份.

步骤 3 Alice 制备 N 个四粒子团簇态, 随机处于两个态之一

$$|\varphi\rangle=\frac{1}{2}(|0000\rangle+|0011\rangle+|1100\rangle-|1111\rangle)_{a_1a_2b_1b_2},$$

$$|\varphi'\rangle=\frac{1}{2}(|1001\rangle+|1010\rangle+|0101\rangle-|0110\rangle)_{a_1a_2b_1b_2}.$$

将序列命名为序列 $P=\{P_1(a_1,\ a_2),\ P_1(b_1,\ b_2),\ P_2(a_1,\ a_2),\ P_2(b_1,\ b_2),\ \cdots,\ P_{\rm N}(a_1,\ a_2),\ P_{\rm N}(b_1,\ b_2)\ \}$.

步骤 4 Alice 对每个团簇态的粒子 b_2 施加酉操作 I, σ_x, ${\rm i}\sigma_y$, σ_z. 原团簇态被转换为 8 种可能态之一

$$|\varphi_1\rangle=\frac{1}{\sqrt{2}}\left(|00\rangle_{a_1a_2}|\varphi^+\rangle_{b_1b_2}+|11\rangle_{a_1a_2}|\varphi^-\rangle_{b_1b_2}\right),$$

$$|\varphi'_1\rangle=\frac{1}{\sqrt{2}}\left(|01\rangle_{a_1a_2}|\psi^-\rangle_{b_1b_2}+|10\rangle_{a_1a_2}|\psi^+\rangle_{b_1b_2}\right),$$

$$|\varphi_2\rangle=\frac{1}{\sqrt{2}}\left(|00\rangle_{a_1a_2}|\psi^+\rangle_{b_1b_2}+|11\rangle_{a_1a_2}|\psi^-\rangle_{b_1b_2}\right),$$

$$|\varphi'_2\rangle=\frac{1}{\sqrt{2}}\left(|01\rangle_{a_1a_2}|\varphi^-\rangle_{b_1b_2}+|10\rangle_{a_1a_2}|\varphi^+\rangle_{b_1b_2}\right),$$

$$|\varphi_3\rangle=-\frac{1}{\sqrt{2}}\left(|00\rangle_{a_1a_2}|\psi^-\rangle_{b_1b_2}+|11\rangle_{a_1a_2}|\psi^+\rangle_{b_1b_2}\right)$$

$$|\varphi'_3\rangle=\frac{1}{\sqrt{2}}\left(|01\rangle_{a_1a_2}|\varphi^+\rangle_{b_1b_2}+|10\rangle_{a_1a_2}|\varphi^-\rangle_{b_1b_2}\right),$$

$$|\varphi_4\rangle=\frac{1}{\sqrt{2}}\left(|00\rangle_{a_1a_2}|\varphi^-\rangle_{b_1b_2}+|11\rangle_{a_1a_2}|\varphi^+\rangle_{b_1b_2}\right),$$

$$|\varphi'_4\rangle=-\frac{1}{\sqrt{2}}\left(|01\rangle_{a_1a_2}|\psi^+\rangle_{b_1b_2}+|10\rangle_{a_1a_2}|\psi^-\rangle_{b_1b_2}\right).$$

步骤 5 从粒子序列中提取粒子 a_1 和 a_2 形成

序列 $P_{\rm A}=\{P_1(a_1,\ a_2),\ P_2(a_1,\ a_2),\ \cdots,\ P_N(a_1,\ a_2)\}$, 剩余粒子 b_1 和 b_2 形成序列 $P_{\rm B}=\{P_1(b_1,\ b_2),\ P_2(b_1,\ b_2),\ \cdots,\ P_N(b_1,\ b_2)\}$.

步骤 6 Alice 根据 $EK_{\rm A1}$ 制备光子检测序列 S, 并随机插入序列 $P_{\rm B}$, 发送混合序列给 Bob.

步骤 7 Alice 公开 S 光子在 $P_{\rm B}$ 中的位置, Bob 根据 $EK_{\rm A1}$ 选择 Z 基或 X 基测量 S 中的光子, 并将测量结果与 $EK_{\rm A2}$ 对比, 计算错误率. 若错误率超过阈值, 则终止通信; 否则继续进行下一步.

步骤 8 Alice 对 $P_{\rm A}$ 中的每个粒子 a_1 和 a_2 进行 Z 基测量, Bob 对 $P_{\rm B}$ 中的每个粒子 b_1 和 b_2 进行贝尔基测量, Alice 公开测量结果, Bob 根据该结果和自己的测量结果, 查表解码消息.

表 1 中, 我们对基于不同量子资源的 QIA 协议的优势和局限性进行了总结和比较. 对上述协议而言, 在实验成熟度方面, 单光子协议 (如 Hong2017[68]) 因技术成熟度较高, 已接近实用化. 连续变量协议 (如 Chen2024[82]) 在光纤通信中更具优势, 但需解决信道损耗问题. 在安全性方面, 纠缠态协议理论上提供“无条件安全性”, 但实际安全性受限于设备缺陷 (如纠缠源不可信), 需考虑设备无关 (device-independent) 假设的适用性. 单光子协议需防范光子数分离攻击 (PNS 攻击), 常需诱骗态技术补充. 在未来, 混合型协议可能成为量子网络的主流, 兼顾资源效率与安全性. 连续变量 QIA 与经典光通信的深度融合是重要研究方向.

2.2 根据量子协议分类

根据 QIA 协议中使用的量子协议和通信类型, 将文中提到的 QIA 协议分类如下: 基于 QKD 框架的 QIA 协议、基于 QSDC 框架的 QIA 协议、基于 QT 框架的 QIA 协议、基于 QSS 框架的 QIA 协议以及基于乒乓协议框架的 QIA 协议.

2.2.1 基于 QKD 框架的 QIA 协议

基于 QKD 框架的 QIA 协议将身份认证功能嵌入密钥分发过程, 确保通信双方身份的合法性. 在 QKD 生成密钥的同时, 通过量子态操作或预共享密钥验证身份. 利用贝尔态分发 (如 EPR 对) 或单光子编码等技术, 必要时可借助第三方可信任机构辅助验证. 多用于量子通信网络中的初始身份绑定 (如量子卫星通信) 和需要高安全性的长期密钥分发场景.

基于 QKD 框架的 QIA 协议使用最为广泛, 2000 年, Zeng 和 Zhang[55] 提出的 QIA 协议就是基于 QKD 框架. 同年, Ljunggren 等 [56] 通过引入第三方可信机构 Trent 作为仲裁者, 提出了一种基于授权的 QIA 协议. 当引入第三方后, 可能会出现各种问题, 故在该协议中假设第三方是诚实的. 此外, 第三方的量子能力也是影响认证成功与否的关键. 2001 年, Curty 和 Santos[87] 提出了一种基于量子资源的经典消息认证协议 (CS01 协议), 该协议首次提出仅需共享一个量子比特 (如纠缠态中的单粒子) 作为认证密钥, 即可安全验证二进制经典消息的完整性和发送者身份, 显著地降低了传统方法对长密钥的依赖, 提升了资源效率. 通过设计特定的幺正操作, 将经典消息编码为量子态, 结合纠缠资源生成认证标签, 实现了量子物理特性 (如不可克隆性) 对经典信息的保护, 突破了传统哈希函数与加密算法的局限性. 相较于经典消息认证码 (MAC) 需至少两比特密钥确保安全性, 该协议在单量子比特下即实现信息论安全, 为低资源环境 (如量子物联网) 的认证需求提供了高效解决协议.

简述 Curty 和 Santos[87] 的协议如下.

表 1 根据量子资源分类的 QIA 协议

Table 1. QIA scheme based on quantum resources classification.

量子源类型	核心资源	优势	局限性	信道损耗/噪声容忍度
单光子	极化/相位编码单光子	低资源消耗、易于实现、与现有QKD技术兼容度高	需高效单光子探测器, 抗噪声能力较弱, 需防范光子数分离(PNS)攻击	中等. 对信道损耗敏感, 需使用诱骗态; 散粒噪声会影响误码率
纠缠态	贝尔态、GHZ态、团簇态	高安全性、抗窃听能力强、具备理论上的无条件安全性	实验复杂度高, 依赖稳定纠缠源, 传输距离受纠缠分效率限制	较低. 纠缠分发效率极易受信道损耗和退相干效应影响, 保真度下降快
连续变量	双模压缩态、相干态	城域网效率高, 兼容经典光通信设备, 探测效率高	需高精度调制, 安全性依赖高斯假设, 易受到非高斯攻击	较高. 可采用经典光通信的放大和纠错技术, 但对过量噪声非常敏感
混合型	纠缠态+单光子/经典算法	灵活性强, 平衡效率与安全性, 降低对单一量子源的依赖, 适用复杂场景	安全性需双重验证, 协议设计复杂度高, 需协调量子与经典操作的同步性	可调节. 取决于所采用的具体量子资源组合, 设计上可针对噪声进行优化

步骤 1 初始化. Alice 和 Bob 预先共享一个两量子比特的最大纠缠态 $|\psi\rangle_{\mathrm{AB}}=1/\sqrt{2}\,(|01\rangle_{\mathrm{AB}}-|10\rangle_{\mathrm{AB}})$, Alice 持有粒子 A, Bob 持有粒子 B. 双方公开幺正操作 $U_{\mathcal{E}}$, 消息态空间$\mathcal{E}$是一个四维希尔伯特空间, 包含正交基 $\{|\varphi_0\rangle,|\varphi_1\rangle,|\varphi_2\rangle,|\varphi_3\rangle\}$, $|\varphi_0\rangle,|\varphi_1\rangle$ 分别对应经典信息 0 和 1, 且满足正交性 $\langle\varphi_i|\varphi_j\rangle=\delta_{ij}$, $|\varphi_2\rangle,|\varphi_3\rangle$ 为辅助态, 用于错误检测.

步骤 2 认证编码过程. Alice 发送消息 $i\in\{0,1\}$时, 制备消息态 $|\varphi_i\rangle\in\varepsilon$ (例如 $|\varphi_0\rangle=|00\rangle,|\varphi_1\rangle=|11\rangle$), 对共享密钥粒子 A 和消息态执行幺正操作: $E_{\mathrm{A}\varepsilon}=|0\rangle\langle 0|_{\mathrm{A}}I_{\varepsilon}+|1\rangle\langle 1|_{\mathrm{A}}U_{\varepsilon}$. 若 A 处于 $|0\rangle$, 执行恒等操作; 若 A 处于 $|1\rangle$, 执行 U_{ε} 操作. Alice 发送编码后的消息态给 Bob. 保留密钥粒子 A.

步骤 3 验证解码过程. Bob 接收到消息态后, 对共享密钥粒子 B 和消息态执行解码操作: $D_{\mathrm{B}\varepsilon}=|0\rangle\langle 0|_{\mathrm{B}}\otimes U_{\varepsilon}'+|1\rangle\langle 1|_{\mathrm{B}}\otimes I_{\varepsilon}$. 若 B 处于 $|1\rangle$, 执行恒等操作; 若 B 处于 $|0\rangle$, 执行解码 U_{ε}' 操作. Bob 在消息空间$\mathcal{E}$上对正交基 $\{|\varphi_k\rangle\,|k=0,1,2,3\}$ 进行投影测量. 若测得 $|\varphi_0\rangle$ 则接受消息为 0, 若测得 $|\varphi_1\rangle$ 则接受消息为 1, 即认证通过; 若测得 $|\varphi_2\rangle$ 或 $|\varphi_3\rangle$ 则拒绝消息, 即认证失败.

2.2.2 基于 QSDC 框架的 QIA 协议

QSDC 可以直接通过量子信道传输秘密信息而无需密钥. 通过这种方式, 已认证用户可以采用 QSDC 直接将他们的身份码发送给认证者. 基于 QSDC 框架的 QIA 协议利用量子态的基矢选择或相位参数, 将身份认证信息直接嵌入量子态编码中, 采用极化光子、贝尔态编码、动态密钥更新等技术, 结合诱骗态检测窃听, 实现安全通信与认证一体化. 多用于实时量子安全通信 (如军事指挥系统) 和资源受限的量子物联网设备认证.

2010 年, Liu 等 [88] 提出了一种结合极化光子与贝尔态的 QSDC 改进协议, 通过动态身份认证机制优化了传统协议的实现复杂度与安全性. 相较于依赖 GHZ 态或多光子纠缠的现有协议, 该协议利用极化光子的制备与测量简易性, 将认证过程整合至传统 QSDC 框架内, 硬件成本降低约 30%. 2015 年, Chang 等 [89] 提出了一种改进型 QSDC 协议, 通过单光子序列实现高效通信与动态身份认证. 该协议的核心创新在于将身份标识嵌入光子偏振基矢选择中, 并利用经典异或 (XOR) 加密增强抗攻击能力, 同时优化了传统协议中纠缠态资源依赖与传输效率问题. 相较于依赖纠缠态的 QSDC 协议 (如 Wang 等 [85]2006 年协议需两次光子传输), 该协议通过单次光子传输完成通信, 信道利用率提升约 40%. 此外, 单光子制备与测量技术兼容现有量子光学器件, 实验实现成本降低 30%.

2020 年, QSDC 拓展了新的应用场景, Zhou 等 [90] 提出了一种新型的测量设备无关的 QSDC (MDI-QSDC) 协议, 旨在解决传统 QSDC 中由测量设备缺陷引发的安全漏洞. 通过引入不可信的第三方 (Charlie) 执行 Bell 态测量 (Bell state measurement, BSM), 该协议不仅消除了测量端潜在的攻击风险, 还将通信距离提升至传统 QSDC 的两倍 (例如从 100 km 扩展至 200 km). 随后在 2022 年, Das 和 Paul[91] 提出了一种结合用户身份认证的 MDI-QSDC 协议, 并扩展至量子对话和确定性安全量子通信场景, 为量子密码学提供了新的安全解决协议. 首次将用户认证与 MDI 技术结合, 构建高效且安全的量子通信框架. 2024 年, Li 等 [92] 提出了一种基于单光子的 MDI-QSDC 协议, 首次将身份认证与单光子资源结合, 解决了现有 MDI-QSDC 协议依赖纠缠光子对且缺乏身份验证的缺陷. 协议通过预共享身份标识、诱骗态检测及 BSM, 实现了通信双方的双向身份认证与安全信息直传, 采用离散变量 (单光子) 与 BSM 技术成熟, 资源制备简单, 易于集成现有量子网络设施, 适配光纤通信等实际场景.

简述 Li 等 [92] 的协议如下.

步骤 1 初始化阶段. Alice 和 Bob 约定四个局域酉操作与比特的映射关系: 操作 $\sigma_{00}=I$, $\sigma_{01}=\sigma_x$, $\sigma_{10}=\mathrm{i}\sigma_y$, $\sigma_{11}=\sigma_z$, 分别对应 00, 01, 10, 11 比特. Alice 持有 $\mathrm{ID_A}$, Bob 持有 $\mathrm{ID_B}$, 二者私有且定期更新.

步骤 2 Bob 向 Alice 认证身份. Bob 制备一组 EPR 对序列, 每个 EPR 对随机抽取一个光子, 根据 $\mathrm{ID_B}$ 制备极化光子: $\mathrm{ID_B}$ 比特为 0 制备直角基 ($|0\rangle$ 或 $|1\rangle$), $\mathrm{ID_B}$ 比特为 1 制备对角基 ($|+\rangle$ 或 $|-\rangle$). 将极化光子随机插入 EPR 光子序列, 发送混合序列给 Alice. Alice 使用滤波器 (防不可见光子) 和光子数分离器 (防延迟光子) 检测特洛伊木马攻击, 存储序列. Bob 公开极化光子位置. Alice 随机选择基测量这些光子, 公开测量基和结果. Bob 计算错误率: 若错误率大于阈值, 则终止; 否则, Bob 公开制备基. Alice 修正测量基, 提取 $\mathrm{ID_B'}$. Alice 比较

ID'_B 与 ID_B, 若匹配, 则 Bob 身份合法.

步骤 3 Alice 发送机密信息. Alice 根据机密消息, 对序列中非极化光子施加相应酉操作, 并根据 ID_A 制备极化光子 (规则同 Bob), 随机插入序列, 回传给 Bob.

步骤 4 Alice 向 Bob 认证身份. Alice 公开极化光子位置, Bob 测量光子并公开测量基和结果. Alice 计算错误率, 若低于阈值, 则公开正确基. Bob 修正测量基, 提取 ID'_A, 与 ID_A 比较, 若匹配则 Alice 身份合法, 继续解码.

步骤 5 Bob 解码信息. Bob 对接收到的 EPR 光子和本地保留的配对光子进行贝尔态联合测量, 根据测量结果和酉操作映射 (步骤 1) 解码机密消息, 每个 EPR 对得到 2 比特. Alice 和 Bob 使用经典纠错协议修正传输错误.

步骤 6 身份标识更新. 从已传输的机密消息中截取部分比特, 更新 ID_A 和 ID_B, 供下次通信使用.

2.2.3 基于 QT 框架的 QIA 协议

基于 QT 框架的 QIA 协议利用量子隐形传态传输身份信息或认证密钥, 通过 EPR 对或 GHZ 态分配量子资源, 采用纠缠交换、BSM 和量子态远程制备等技术, 保障通信过程的无条件安全性, 实现跨节点认证. 多用于量子中继网络中的跨节点身份认证和城域量子通信 (如银行数据中心互联).

2005 年, Zhou 等 [93] 提出了一种基于量子隐形传态和纠缠交换的跨中心 QIA 协议. 该协议通过 EPR 纠缠对的完整性传输未知量子态, 确保信息传输的无条件安全性. 而且, 通过操作未直接交互的量子系统, 从而扩展了量子通信距离. 然而, 这种方法需要保证用于纠缠交换的中间设备需要被完全信任, 否则会带来新的安全问题. 2016 年 Ma 等 [78] 的连续变量协议也是与 QT 相结合的.

简述 Zhou 等 [93] 的协议如下.

注册阶段: 用户在归属认证中心 CA 注册身份. 用户归属的客户端服务器 U_{1i} 和认证中心 CA_1 预先共享一个 EPR 对 (光子 2, 3): $|\psi^-\rangle_{23} = (1/\sqrt{2})(|0\rangle_2|1\rangle_3 - |1\rangle_2|0\rangle_3)$. U_{1i} 持有光子 2, CA_1 持有光子 3. U_{1i} 根据用户身份信息制备单光子量子态 $|\varphi\rangle_1 = \alpha|0\rangle + \beta|1\rangle$, 称为认证密钥. U_{1i} 对光子 1 (身份态) 和光子 2 进行贝尔基联合测量, 得到 4 种可能结果之一 (如 $|\psi^+\rangle_{12}$), 并将测量结果通过经典信道告知 CA_1. CA_1 根据收到的测量结果, 对持有的光子 3 施加相应酉操作, 重建出原始身份态 $|\varphi\rangle$. U_{1i} 测量结果和 CA_1 所需操作对应如下:

$$|\psi^-\rangle_{12} \to U = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix},$$

$$|\psi^+\rangle_{12} \to U = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix},$$

$$|\varphi^-\rangle_{12} \to U = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix},$$

$$|\varphi^+\rangle_{12} \to U = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$$

CA_1 将用户身份信息以量子态形式存入数据库, 并通知 U_{1i} 注册成功.

认证阶段: 用户跨中心请求服务. 用户在 U_{2j} 输入用户名、CA 编号 (CA_1) 及身份信息. U_{2j} 将 CA 编号通过经典信道发送给 CA_2. CA_2 根据 CA 编号将请求转发给 CA_1. CA_2 对本地光子 ca_2 和 ca_{2j} 进行贝尔基联合测量, 实现纠缠交换. 测量结果为 4 种贝尔态之一 (如 $|\psi^+\rangle_{ca_2ca_{2j}}$), 此时 CA_1 的光子 ca_1 与 U_{2j} 的光子 u_{2j} 形成纠缠态 (如 $|\psi^+\rangle_{ca_1u_{2j}}$). CA_2 将测量结果通过经典信道告知 CA_1. CA_2 向 U_{2j} 发送操作指令, 通知其准备进行隐形传态. U_{2j} 根据用户输入的身份信息制备单光子态 $|\varphi\rangle_S$, 并对身份态光子 S 和光子 u_{2j} (纠缠交换后与 CA_1 纠缠) 进行贝尔基联合测量, 将结果通过经典信道发送给 CA_2, 然后 CA_2 转发给 CA_1. CA_1 结合两次收到的信息 (CA_2 的纠缠交换结果和 U_{2j} 的贝尔测量结果), 对持有的光子施加相应酉操作, 重建出身份态 $|\varphi\rangle$, 并将其与数据库中存储的该用户认证密钥 K 进行比对. 若匹配则认证成功, CA_1 通知 CA_2 授权服务, CA_2 根据 CA_1 的授权结果, 向用户提供相应服务.

2.2.4 基于纠缠交换框架的 QIA 协议

基于纠缠交换框架的 QIA 协议利用 GHZ 态或团簇态的全局纠缠特性, 实现多方协作式身份认证, 需多用户或第三方共同验证身份. 此类协议采用 GHZ 态分发、诱骗光子插入和经典哈希函数辅助等技术, 利用量子纠缠的非局域关联性, 确保攻击者无法伪造部分参与方的身份. 多用于多方量子会议系统 (如量子区块链共识机制 [66]) 和高安全等级的多机构联合认证 [94](如政府机密系统).

2006 年, Wang 等 [85] 提出了一种基于纠缠交换的多方 QIA 协议, 旨在通过可信第三方 (Trent)

同时认证多个用户的身份. 该协议结合 GHZ 态的量子纠缠特性与经典哈希函数, 试图在提升效率的同时保证无条件安全性. 2009 年, Yang 等[95] 利用 GHZ 态的纠缠特性与诱骗光子技术, 提出了一种多方同时进行的 QIA 协议, 能有效地检测双 CNOT 攻击等复杂攻击. 该协议与 2006 年 Wang 等[85] 的协议类似, 但需要的量子资源更少, 且用户仅需单量子比特测量 (SQM), 显著降低了资源消耗与操作复杂度. 尽管仍依赖可信第三方, 其高效性与安全性为大规模量子网络中的身份认证提供了重要参考.

简述 Wang 等[85] 的协议如下.

步骤 1 可信第三方 Trent 制备 N 个三粒子 GHZ 态, 初始态均为 $|\psi_1\rangle=\dfrac{1}{\sqrt{2}}(|000\rangle+|111\rangle)_{TA_1A_2}$, 自己保留 T 序列, 将 A_1 和 A_2 序列分别发送给 Alice_1 和 Alice_2.

步骤 2 Trent 随机选择部分 GHZ 态作为抽样集, 并随机选择 Z 基 ($|0\rangle$, $|1\rangle$) 或 X 基 ($|+\rangle$, $|-\rangle$) 测量, 公开抽样位置和测量基. Alice_1 和 Alice_2 对相应位置的 A_1 和 A_2 粒子用相同基测量, 并公布测量结果. 根据错误率决定是否继续.

步骤 3 Trent 将剩余 GHZ 态随机分为 M 组, 每组含两个 GHZ 态 (T, T'; A_1, A_1'; A_2, A_2').

步骤 4 Alice_1 和 Alice_2 根据认证密钥 AK_i 对组内粒子施加酉操作. 若比特为 0, 则施加 $\boldsymbol{I}=\begin{pmatrix}1&0\\0&1\end{pmatrix}$; 若比特为 1, 则施加 $\mathrm{i}\sigma_y=\begin{pmatrix}0&1\\-1&0\end{pmatrix}$.

步骤 5 Trent 对每组中的 T 和 T' 粒子随机独立施加 I 或 $\mathrm{i}\sigma_y$ 操作.

步骤 6 Alice_1 和 Alice_2 分别测量每组中的 (A_1, A_1') 和 (A_2, A_2') 粒子对, 并公布结果. Trent 测量 (T, T') 粒子对, 不公布结果. 他根据三方测量结果反推用户操作, 并将反推的密钥比特与预共享的进行比对, 若一致则认证通过. 例如, 若测得 $\left(|\psi^-\rangle_{TT'},|\psi^-\rangle_{A_1A_1'},|\psi^+\rangle_{A_2A_2'}\right)$, 则对应操作组合 $\mathrm{i}\sigma_y\otimes\mathrm{i}\sigma_y\otimes I$, 即 Alice_1 操作 $\mathrm{i}\sigma_y$, 密钥比特 1; Alice_2 操作 I, 密钥比特 0. 该协议也可扩展至多方 (r 个用户), 仅需 Trent 制备 $(r+1)$-粒子 GHZ 态.

2.2.5 基于乒乓协议框架的 QIA 协议

此类 QIA 协议基于量子信道的“请求-响应”机制 (乒乓协议), 量子态在发送方与接收方之间多次传输, 动态更新认证密钥, 采用单光子乒乓传输、CNOT 门操作和动态基矢选择等技术实现身份验证. 量子态传输的不可逆性, 导致攻击者的操作会破坏量子态关联, 从而确保认证过程的安全性. 多用于动态网络环境中的临时身份认证 (如移动量子终端) 和需要频繁更新密钥的短期通信场景.

2006 年, Zhang 等[96] 首次结合乒乓协议 (ping-pong protocol) 和量子控制非门 (CNOT), 提出了一种单向的 QIA 协议, 实现了高效、安全的量子认证与动态密钥更新一体化. 该协议对诸如假冒欺诈攻击和替换欺诈攻击等个体攻击具有安全性. 该协议仅支持单向认证, 即 Alice 被视为可靠的认证机构, 而 Bob 被视为需要验证身份的用户, 双向认证需进一步扩展. 严格地从技术上来讲, 到目前为止所提出的许多协议在这个意义上都是单向的, 当然也可以简单认为通过两次使用相同的过程就可以进行双向认证, 但实现上并不能完全等同, 所以通常不会明确提及. 2014 年, Yuan 等[86] 提出了一种基于单粒子态和乒乓技术的量子身份认证协议, 无需依赖纠缠态即可实现用户身份验证与认证密钥的动态更新. 协议利用单粒子在双向量子信道中的传输特性, 结合异或操作和基矢选择机制, 确保密钥更新与身份验证同步完成. 通过单粒子态与乒乓技术的创新结合, 为量子身份认证提供了高效且安全的解决协议, 其无纠缠依赖与动态密钥更新机制具有重要理论价值.

简述 Zhang 等[96] 的 QIA 协议如下.

可靠认证中心 Alice 验证用户 Bob 的身份. Alice 和 Bob 预先共享一个经典二进制认证密钥 $K_a=\{k_1,k_2,\cdots,k_{2n}\}$.

步骤 1 Alice 制备一个 EPR 纠缠对 $|\Psi\rangle=\dfrac{1}{\sqrt{2}}(|0_\text{h}0_\text{t}\rangle+|1_\text{h}1_\text{t}\rangle)$, 粒子 h 保留, 将粒子 t 通过量子信道发送给 Bob.

步骤 2 Bob 收到粒子 t 后, 根据密钥的当前两位 $k_{2i-1}k_{2i}$ $(1\leqslant i\leqslant n)$ 制备一个信息粒子 m: $|\varphi_m\rangle=|k_{2i-1}\oplus k_{2i}\rangle$, 然后对粒子 t 和 m 施加量子受控非门 (CNOT). 若 $k_{2i-1}=0$, 使用 Z 基 CNOT 门 C_0: $C_0=|0\rangle\langle0|\otimes I+|1\rangle\langle1|\sigma_x$; 若 $k_{2i-1}=1$, 使用 X 基CNOT 门 C_1: $C_1=|+\rangle\langle+|\otimes I+|-\rangle\langle-|\sigma_x$, 操作后生成三粒子纠缠态 $|\Phi_\text{w}\rangle=C_\text{p}(|\Psi\rangle\otimes|\varphi_\text{m}\rangle)$. Bob 保留粒子 t, 并将信息粒子 m 发回 Alice.

步骤 3 Alice 收到粒子 m 后, 对保留的粒子 h 和收到的粒子 m 施加相同的 CNOT 门 C_p(根据密

表 2 基于量子框架分类的 QIA 协议

Table 2. QIA schemes based on quantum framework classification.

分类	信道需求	核心优势	主要局限	适用场景
QKD框架	低损耗	高安全性, 密钥与认证同步	依赖预共享密钥或可信第三方	长期密钥分发的安全通信
QSDC框架	高稳定性	高效信息传输与认证一体化	对量子信道质量要求高	实时安全通信(如军事指挥)
隐形传态框架	中继节点	跨节点认证, 无条件安全性	实验复杂度高, 需可信中继	量子中继网络与城域互联
纠缠交换框架	多方同步	多方协作抗合谋攻击	量子资源消耗大, 依赖可信第三方	多方联合认证(如区块链共识)
乒乓协议框架	双向信道	动态密钥更新, 抗窃听能力强	仅支持单向认证, 需双向信道	移动终端临时认证

钥 k_{2i-1} 选择基): $|\Phi'_{\rm w}\rangle = C_{\rm p}|\Psi_{\rm w}\rangle = |\Psi\rangle \otimes |\varphi_{\rm m}\rangle$, 此时粒子 m 恢复为初始态 $|\varphi_m\rangle = |k_{2i-1} \oplus k_{2i}\rangle$.

步骤 4 Alice 在 σ_z 基下测量粒子 m, 合法 Bob 的测量结果必为 $k_{2i-1} \oplus k_{2i}$. 若结果匹配, 返回步骤 1 进行下一组密钥位的验证. 若所有 n 组密钥均通过, 则 Bob 身份认证成功.

步骤 5 每认证一组密钥位 $k_{2i-1}k_{2i}$ 后, 更新该密钥.

表 2 中, 我们对基于不同量子框架的 QIA 协议的优势、局限性以及适用场景进行了总结和比较.

3 最新的 QIA 协议

随着量子通信的发展, QIA 协议也是不断发展的, 以下介绍 1 个最新的 QIA 协议以及具有 QIA 功能的三方 QSDC 协议.

3.1 基于 GHZ 态的多方 QIA 协议 [97]

如图 1 所示, Alice 为验证方, 她事先与 N 个目标通信方 $\rm Bob'_1$, $\rm Bob'_2$, $\cdots$, $\rm Bob'_N$, 分别通过 BB84 协议共享一组认证密钥序列 K'_1, K'_2, $\cdots$, K'_N. 密钥各不相同, 分别为一系列长度相同的二进制比特串, 每个目标通信方只知道自己与 Alice 的共享密钥序列, 而 Alice 知道所有目标通信方的密钥序列.

步骤 1 Alice 制备一系列相同的 N+1 光子极化 GHZ 态, 取出所有 GHZ 态中的光子 1, 组成序列 $S_{\rm A}$, 并把序列 $S_{\rm A}$ 的光子存储到量子存储器中. Alice 将所有 GHZ 态中的光子 2 组成序列 $S_{\rm B1}$, 将所有 GHZ 态中的光子 3 组成序列 $S_{\rm B2}$……依次操作, 将所有 GHZ 态中的光子 N+1 组成序列 $S_{\rm BN}$.

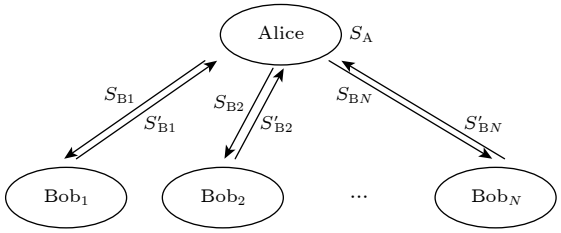


图 1 多方 QIA 协议原理图

Fig. 1. Schematic diagram of multi-party quantum identity authentication.

步骤 2 Alice 随机制备大量直角基 (Z) 或对角基 (X) 单光子, 作为安全检测光子. Alice 将这些光子分别随机插入到序列 $S_{\rm B1}$, $S_{\rm B2}$, ···, $S_{\rm BN}$ 中, 再通过 N 条量子信道将序列 $S_{\rm B1}$, $S_{\rm B2}$, ···, $S_{\rm BN}$ 分别发送给实际通信方 (待证明方) $\rm Bob_1$, $\rm Bob_2$, $\cdots$, $\rm Bob_N$.

步骤 3 待证明方接收到光子后, Alice 公开各条光子序列中安全性检测光子的位置和制备基, $\rm Bob_1$, $\rm Bob_2$, $\cdots$, $\rm Bob_N$ 分别提取出安全性检测光子, 进行第一轮安全性检测, 并公布测量结果. Alice 根据结果估算每条量子信道的错误率, 若均低于事先设定的阈值, 说明所有量子信道中的光子传输过程均安全, 则进行下一步.

步骤 4 Alice 对序列 $S_{\rm A}$ 的光子进行 Z 基测量, $\rm Bob_1$, $\rm Bob_2$, $\cdots$, $\rm Bob_N$ 根据各自的认证密钥 K_1, K_2, $\cdots$, K_N, 分别对剩余光子进行编码操作, 得到序列 $S'_{\rm B1}$, $S'_{\rm B2}$, $\cdots$, $S'_{\rm BN}$. 接着, 随机地在光子序列中插入足够数量的安全性检测光子. 操作完成后, 分别将光子序列再发送回验证方 Alice.

步骤 5 待 $\rm Bob_1$, $\rm Bob_2$, $\cdots$, $\rm Bob_N$ 公开序列中安全性检测光子的位置和制备基后, Alice 进行第二轮安全性检测. 确认安全后, Alice 分别对返回序列中的剩余光子进行 Z 基测量, 根据测量结果, Alice 可推断出 $\rm Bob_1$, $\rm Bob_2$, $\cdots$, $\rm Bob_N$ 的操作, 从而读出 $\rm Bob_1$, $\rm Bob_2$, $\cdots$, $\rm Bob_N$ 传递的认证密钥序列 K_1, K_2, $\cdots$, K_N. 通过与目标通信方的认证密钥 K'_1, K'_2, $\cdots$, K'_N 进行比对, 从而验证 $\rm Bob'_1$, $\rm Bob'_2$, $\cdots$, $\rm Bob'_N$ 的身份.

该协议中, 包含两轮安全性检测. 在待证明方 $\rm Bob_1$, $\rm Bob_2$, $\cdots$, $\rm Bob_N$ 和验证方 Alice 收到光子序

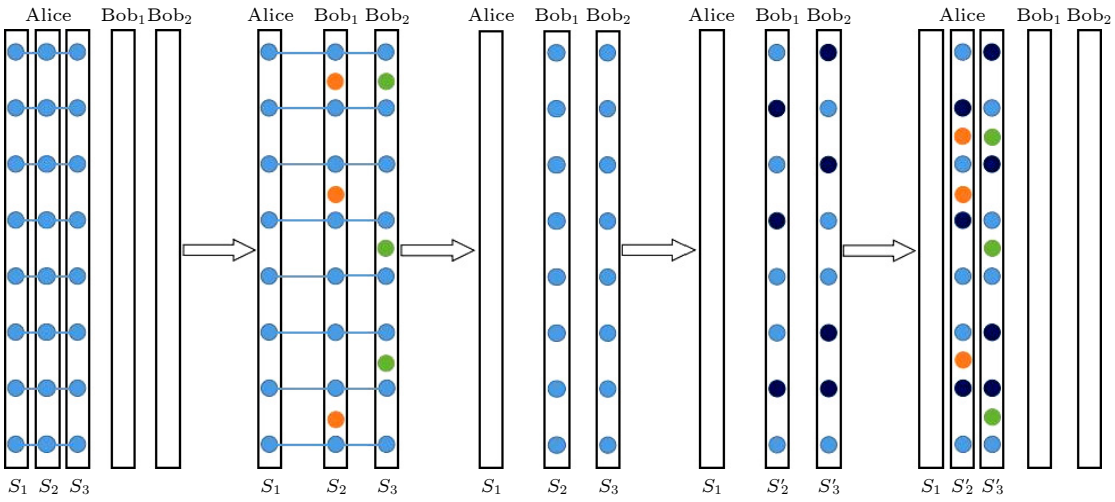


图 2 三方 QIA 协议步骤图

Fig. 2. Schematic diagram of the three-partite QIA protocol.

列后, 均必须确认量子通道的安全性, 才能进行下一步的操作.

为了更清楚地描述协议, 以三用户 QIA 为例说明. 三用户 QIA 协议步骤图如图 2 所示, 其中两个用户 Bob_1, Bob_2 需要向 Alice 认证身份, 该过程忽略安全性检测. Alice 与合法用户 Bob_1', Bob_2' 预先共享的密钥序列 $K_1=\{K_{11}, K_{12}, K_{13}, \cdots, K_{1L}\}$, $K_2=\{K_{21}, K_{22}, K_{23}, \cdots, K_{2L}\}$作为 Bob_1, Bob_2 的身份认证码序列, L 足够大. Alice 制备大量处于相同的量子态的 3 光子 GHZ 态, 属于 8 个 GHZ 态之一. 如果选取其中之一的量子态 $|\varphi_2^+\rangle=\dfrac{1}{\sqrt{2}}(|\mathrm{HVH}\rangle+|\mathrm{VHV}\rangle)_{123}$ 进行制备, 量子态的数量等于认证密钥序列的长度. 验证方 Alice 取出所有 GHZ 态中的光子 1, 2 和 3, 分别组成序列 S_1, 序列 S_2 和序列 S_3. 在待证明方 Bob_1 和 Bob_2 编码前, Alice 对序列 S_{A} 的光子进行 Z 基测量. 假设测量结果是 $|H\rangle$, 则 Bob_1 和 Bob_2 分别为 $|V\rangle$ 和 $|H\rangle$. 然后, Bob_1 和 Bob_2 根据各自密钥 K_1 和 K_2 进行编码操作, 将认证密钥信息加载到纠缠光子上, 编码操作包含两种幺正操作$\{I, \sigma_x\}$. $I=|H\rangle\langle H|+|V\rangle\langle V|$ (不变操作) 代表密钥 0, $\sigma_x=|H\rangle\langle V|+|V\rangle\langle H|$ (比特翻转操作) 代表密钥 1. 对返回的光子序列, Alice 再次进行单光子测量. 如果 Alice 测量 Bob_1 光子结果是 $|H\rangle$ ($|V\rangle$), 她可知 Bob_1 的操作是 $\sigma_x(I)$, 则可推断密钥为 1(0). 同时, 如果 Alice 测量 Bob_2 光子结果是 $|H\rangle$ ($|V\rangle$), 她可知 Bob_1 的操作是 $I(\sigma_x)$, 则可推断密钥为 0(1). 经过逐个判断, Alice 可推断出密钥序列, 如果与预先共享的密钥序列相同, 则可确认其身份, 否则为非法用户.

该协议能够抵御来自认证用户的内部攻击, 以及外部的拦截-测量-重发攻击.

3.2 具有身份认证功能的三方 QSDC 协议[98]

下面介绍身份认证在通信协议中的一个实例, 一种具有身份认证功能的三方 QSDC 协议. 该协议基于极化-空间自由度超编码单光子. 其协议步骤图如图 3 所示. 该协议先通过身份认证, 使信息接收方确定两个信息发送方的身份. 身份确定后, 两个信息发送方分别在极化自由度和空间自由度对单光子进行编码. 编码完成后, 编码单光子重新发送给信息接收方. 信息接收方通过测量, 可同时得到两个发送方传递的秘密信息.

在通信前, Alice 与目标通信方 Bob_1 和 Bob_2 分别共享一组随机密钥序列 K_1 和 K_2 作为 Bob_1 和 Bob_2 的身份码序列.

步骤 1 Alice 随机制备大量极化-空间超编码单光子作为信息传输光子, 组成序列 S_1, 再根据 Bob_1 和 Bob_2 的身份码制备足够多身份认证光子和大量安全检测光子, 随机插入序列 S_1 中, 组成序列 S_1'.

步骤 2 Alice 将序列 S_1' 发给第一个实际通信方 Bob_1', Bob_1' 接收到所有光子后. Alice 公布安全检测光子的位置和量子态, Bob_1' 进行第一轮安全性检测. 若安全性检测未通过, 则终止通信; 若安全性检测通过, 则进行下一步.

步骤 3 Alice 公布用于 Bob_1' 的身份认证光子的位置, Bob_1' 根据自己的身份码选择测量基对其

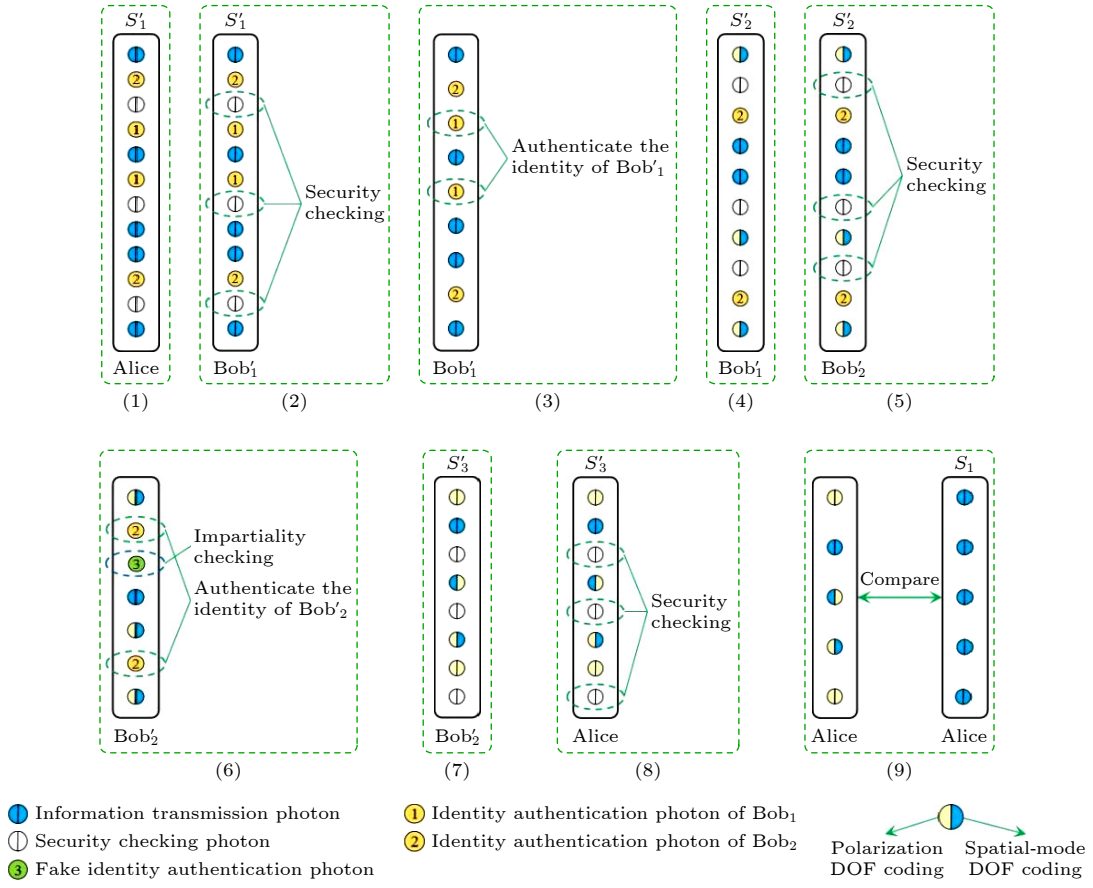


图 3 具有身份认证功能的三方量子安全通信协议示意图

Fig. 3. Schematic diagram of a three-party quantum secure communication scheme with identity authentication function.

进行测量并公开测量结果. Alice 根据公开结果与制备的初始态比较, 进行身份认证. 若身份认证未通过, 则认为第一个实际通信方 Bob'_1 为非法用户, 通信取消; 若身份认证通过, 则认为 Bob'_1 即为目标通信方 Bob_1, 进行下一步骤.

步骤 4 Alice 公布用于 Bob'_2 的身份认证光子的位置, 其余的光子即为信息传输光子, Bob'_1 在其极化自由度上编码, 组成序列 S_2, 并在序列 S_2 中随机插入足够数量的安全检测光子, 组成序列 S'_2.

步骤 5 Bob'_1 将序列 S'_2 发给 Bob'_2, 并公布序列 S'_2 中的安全检测光子的位置和量子态, Bob'_2 进行第二轮安全性检测. 若安全性检测未通过, 则终止通信; 若安全性检测通过, 则进行下一步.

步骤 6 Bob'_2 根据自己的身份码选择测量基对其进行测量并公开测量结果. Alice 根据公开的结果与制备的初始态比较, 进行身份认证.

步骤 7 若身份认证通过, Bob'_2 在信息传输光子空间自由度上编码, 并随机插入足够数量的安全检测光子, 组成序列 S'_3.

步骤 8 Bob'_2 将序列 S'_3 发给 Alice, 并公布序列 S'_3 中的安全检测光子的位置和量子态, Alice 提取出安全检测光子进行第三轮安全性检测.

步骤 9 若安全性检测通过, Alice 对每个信息传输光子的两个自由度进行测量, 再与原始序列 S_1 中对应的信息传输光子的量子态进行比较, 由此解码 Bob'_1 和 Bob'_2 的编码信息.

接下来仅对身份认证部分进行详细说明. Alice 根据 Bob_1 和 Bob_2 的身份码制备一系列在极化自由度上编码的单光子作为身份认证光子, 其制备规则如下: 当 Bob_1 的身份码或 Bob_2 的身份码为“0”时, Alice 利用直角基 (Z 基) 制备 $|H\rangle$ 或 $|V\rangle$ 态的光子; 当 Bob_1 的身份码或 Bob_2 的身份码为“1”时, Alice 利用对角基 (X 基) 制备 $|+\rangle = \dfrac{1}{\sqrt{2}}(|H\rangle + |V\rangle)$ 或 $|-\rangle = \dfrac{1}{\sqrt{2}}(|H\rangle - |V\rangle)$ 态的光子. 对 Bob'_1 进行身份认证流程如下: Alice 公布用于 Bob'_1 的身份认证光子的位置, Bob'_1 从量子存储器中提取出对应的光子, 根据自己的身份码选择测量基对其在极化自

由度进行测量并公开测量结果. Bob_1' 测量规则如下: 当 Bob_1' 的身份码为“0”时, Bob_1' 利用直角基 (Z 基) 测量身份认证光子并公布结果; 当 Bob_1' 的身份码为“1”时, Bob_1' 利用对角基 (X 基) 测量身份认证光子并公布结果. Alice 根据公开结果与制备的初始态比较, 若测量结果与 Alice 制备的初始态一致, 则认为 Bob_1' 的身份码正确; 若测量结果与 Alice 制备的初始态不一致, 则认为 Bob_1' 的身份码错误.

大多数基于纠缠态的 QIA 协议需要量子存储器, 以上两个协议也是如此. 近年来, 量子存储器已经取得了显著的实验进展 [99–103]. 例如, 2017 年, 研究人员报道了一种基于介观钕系集成与光子晶体腔耦合的高保真纳米光子量子存储器 [101]. 2021 年, Liu 等 [102] 实现了吸收式量子存储器之间的预示纠缠分发. 2022 年, 采用单晶片单程配置的自旋波固态量子存储器被成功演示, 该器件对单光子级弱相干脉冲的存储过程保真度达到 91.9%±2.4%[103]. 这些突破性进展表明, 量子存储器可能在不久的将来得以实现.

3.3 两个协议的创新性与优势分析

以上两个协议是本课题组提出的最新方案, 其在协议设计和性能上相较于现有方案具有一定的创新性和优势.

1) 基于 GHZ 态的多方同步身份认证协议创新性与优势:

创新性: 该协议的核心创新在于利用了 GHZ 态“全有或全无”的纠缠特性, 设计了一种多方同步身份认证机制. 验证方 (Alice) 通过单次量子态分发和一轮经典比对, 即可同时验证多个用户 (Bob_1, Bob_2, ···, Bob_N) 的身份, 无需进行多次双边认证, 极大提升了多用户场景下的认证效率.

安全性优势: 协议包含两轮诱骗态安全检测, 能有效抵御信道中的拦截-重发攻击和测量攻击. 更重要的是, 由于 GHZ 态的全局关联性, 任何单个认证用户 (如 Bob_i) 都无法在不被察觉的情况下与外部攻击者 Eve 合谋来伪造另一个用户 (Bob_j) 的身份, 从而有效地抵御了来自认证用户内部的合谋攻击, 这是许多双边认证协议难以实现的.

资源效率与实用性: 协议基于离散变量偏振编码, 与现有 QKD 技术兼容性高. 虽然需要量子存储器, 但随着量子存储技术的快速发展 [99–103], 该协议为未来量子网络中的集中式身份管理系统提供了一个可行的解决方案.

2) 具有身份认证功能的三方 QSDC 协议创新性与优势:

创新性: 该协议的创新点在于实现了身份认证与安全通信在单光子自由度上的深度集成. 利用单个光子的极化自由度和空间自由度分别进行身份认证信息和机密信息的编码 (超编码), 在一个协议框架内依次完成了两个发送方的身份认证和双信息的传输, 实现了“认证即通信”的一体化设计.

安全性优势: 协议流程中嵌入了三轮安全性检测, 确保了光子在各参与方之间传输的全程安全. 身份认证过程依赖于预共享密钥和量子态不可克隆原理, 通信过程则利用了量子超编码和测量技术, 共同构成了端到端的安全保障.

资源效率优势: 与需要制备复杂纠缠态或进行多次量子态传输的方案相比, 该协议主要依赖单光子源和线性光学操作, 降低了对复杂量子资源的需求. 它将两个独立的通信过程 (认证+通信) 融合, 提高了信道利用率和整体协议的效率, 特别适用于对传输效率有要求的有限量子资源场景.

综上所述, 本课题组提出的两个协议分别从多用户认证效率和认证-通信融合架构两个角度进行了创新探索, 在安全性、效率和实用性方面相较于同类协议展现出一定的优势, 为 QIA 在实际量子网络中的应用提供了新的思路.

4 总结与展望

QIA 作为量子通信的重要环节, 本文系统地梳理了 QIA 协议的技术演进脉络, 从早期基于 QKD 的混合认证协议到近年来低资源依赖、高实用性的创新协议, 本文通过分类比较, 全面分析了不同协议的理论基础、实现路径及安全边界, 为 QIA 的理论发展与应用提供了参考.

各类型认证协议各有优缺点. 单光子协议在配合诱骗态监测的条件下, 具备较高的实用化潜力, 但需防范光子数分离攻击; 纠缠态协议虽具备理论上的无条件安全性, 却受限于多粒子纠缠态的制备与维持难度; 连续变量协议在城域网中展现效率优势, 但其安全性依赖高斯假设; 混合型协议通过量子-经典协同设计平衡效率与安全性, 成为复杂网

络环境下的优选架构.

此外, 各类 QIA 协议对实际量子信道中的损耗与噪声的容忍度是其走向实用化的关键指标. 如表 1 所列, 不同类型的协议面临不同的挑战: 离散变量单光子协议需要克服损耗带来的低计数率问题, 并利用诱骗态技术对抗信道噪声 (如 PNS 攻击); 纠缠态协议的核心挑战在于如何长距离、高保真地分发和维持纠缠, 对信道退相干极为敏感; 连续变量协议虽探测效率高, 但必须严格控制系统的过量噪声 (excess noise). 未来, 发展噪声自适应的 QIA 协议、探索与测量设备无关 (MDI) 框架相结合的认证方案、以及设计更强的抗噪声编码和解码方法, 将是提升 QIA 实用性和鲁棒性的重要研究方向.

未来研究需重点关注以下方向: 1) 低资源依赖协议, 进一步优化单光子与连续变量协议, 降低对高精度量子器件的需求; 2) 协议轻量化与集成化, 结合测量设备无关 (MDI) 技术实现身份认证与安全通信的一体化设计; 3) 混合架构的鲁棒性增强, 探索量子-经典混合认证框架的动态密钥管理机制, 抵御量子计算攻击; 4) 实际环境适应性, 针对信道损耗、设备缺陷等现实约束, 发展噪声容忍与后量子安全增强技术. 此外, QIA 与量子物联网、区块链等新兴技术的深度融合, 将为数字身份主权与跨域安全协作提供全新范式. 随着量子通信网络的规模化部署, 高效、普适且抗量子攻击的认证协议将成为构建下一代安全信息生态的核心支柱.

参考文献

[1] Goldenberg L, Vaidman L 1995 *Phys. Rev. Lett.* **75** 1239
[2] Scarani V, Renner R 2008 *Phys. Rev. Lett.* **100** 200501
[3] Liestyowati D 2020 *J. Phys.: Conf. Ser.* **1477** 052062
[4] Shor P W 1994 *Proceedings of the 35th Annual Symposium on Foundations of Computer Science* Santa Fe, USA, November 20–22, 1994 p124
[5] Zhao Q C 2004 *Quantum Computation and Quantum Information (I) — Quantum Computation* (Beijing: Tsinghua University Press) (in Chinese) [赵千川 2004 量子计算和量子信息 (一)——量子计算部分 (北京: 清华大学出版社)]
[6] Zhang Y D 2010 *Advanced Quantum Mechanics* (2nd ed.) (Beijing: Peking University Press) (in Chinese) [张永德 2010 高等量子力学 第 2 版 (北京: 北京大学出版社)]
[7] Bennett C H, Brassard G 1984 *Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing* Bangalore, India, December 10–12, 1984 p175
[8] Ekert A K 1991 *Phys. Rev. Lett.* **67** 661
[9] Bennett C H, Brassard G, Mermin N D 1992 *Phys. Rev. Lett.* **68** 557
[10] Bennett C H, Brassard G, Crépeau C, Jozsa R 1993 *Phys. Rev. Lett.* **70** 1895
[11] Bouwmeester D, Pan J W, Mattle K, Eibl M, Weinfurter H, Zeilinger A 1997 *Nature* **390** 575
[12] Pandey R K, Pathak A, Venugopalan A 2021 *Quantum Inf. Process.* **20** 322
[13] Li J X, Wang Z M, Shi S S, Li Y N, Shang R M, Gu Y J 2022 *Europhys. Lett.* **140** 58001
[14] Hillery M, Bužek V, Berthiaume A 1999 *Phys. Rev. A* **59** 1829
[15] Cleve R, Gottesman D, Lo H K 1999 *Phys. Rev. Lett.* **83** 648
[16] Wang T Y, Wei Z L, Gao F 2021 *Quantum Inf. Process.* **20** 7
[17] Ju X X, Zhong W, Sheng Y B, Zhou L 2022 *Chin. Phys. B* **31** 100302
[18] Long G L, Liu X S 2002 *Phys. Rev. A* **65** 032302
[19] Deng F G, Long G L, Liu X S 2003 *Phys. Rev. A* **68** 042317
[20] Deng F G, Long G L 2004 *Phys. Rev. A* **69** 052319
[21] Eusebi A, Mancini S 2009 *Quantum Inf. Comput.* **9** 950
[22] Hu J Y, Li C L, Zhang C, Liu B, Guo G C 2016 *Light Sci. Appl.* **5** e16144
[23] Zhang W, Ding D S, Sheng Y B, Zhou L, Shi B S, Guo G C 2017 *Phys. Rev. Lett.* **118** 220501
[24] Zhu F, Zhang W, Sheng Y B, Guo G C 2017 *Sci. Bull.* **62** 1519
[25] Hu X M, Zhang C, Zhang C J, Liu B H, Huang Y F, Han Y J, Li C F, Guo G C 2019 *Quantum Eng.* **1** e13
[26] Xu F H, Curty M, Qi B, Qian L, Lo H K 2020 *Rev. Mod. Phys.* **92** 025002
[27] Chen Y A, Zhang Q, Chen T Y, Pan J W 2021 *Nature* **589** 214
[28] Yin Z Q, Li F L, Chen Y A, Pan J W 2021 *Fundam. Res.* **1** 93
[29] Kwek L C, Cao L, Luo Y, Wang Y, Sun S H, Liu X, Lai J, Oh C H 2021 *AAPPS Bull.* **31** 15
[30] Wang X F, Sun X J, Liu Y X, Wang W, Kan B X, Dong P, Zhao L L 2021 *Quantum Eng.* **3** e73
[31] Hajji H, El Baz M 2021 *Quantum Inf. Process.* **20** 4
[32] Zhang C Y, Li C L, Xu J S, Li C F, Guo G C 2021 *Quantum Inf. Process.* **20** 146
[33] Jin A R, Li Y, Zhang Y, Pan J W 2021 *Phys. Rev. Appl.* **16** 034017
[34] Wang S, Chen W, Yin Z Q, Li H W, He D Y, Li Y H, Zhou Z, Guo G C, Han Z F 2022 *Nat. Photonics* **16** 154
[35] Liu B, Xia S, Xiao D, Huang W, Xu B J, Li Y 2022 *Sci. China-Phys. Mech. Astron.* **65** 240312
[36] Liang K X, Li Z Q, Liu J, Wang Q L 2022 *Phys. Rev. Appl.* **18** 054077
[37] Zeng P, Zhou H, Zhang W, Xu B J, Liu B, Gao Z 2022 *Nat. Commun.* **13** 3903
[38] Zhu H T, Zhang C M, Pei C X, Li H W 2022 *PRX Quantum* **3** 020353
[39] Zhou L, Sheng Y B, Long G L 2020 *Sci. Bull.* **65** 12
[40] Qi R Y, Sun Z, Lin Z, Niu J L, Hao P L, Song L J, Gao F 2019 *Light Sci. Appl.* **8** 22
[41] Long G L, Zhang H R 2021 *Sci. Bull.* **66** 1267
[42] Liu X, Li Z J, Luo D, Huang C F, Ma D, Geng M M, Wang J W, Wei K J L 2021 *Sci. China-Phys. Mech. Astron.* **64** 120311
[43] Cao Z W, Yao F W, Xiao X Q 2021 *Phys. Rev. Appl.* **16** 024012
[44] Zhang H R, Sun Z, Qi R Y, Yin L G, Long G L, Lu J H 2022 *Light Sci. Appl.* **11** 83
[45] Liu X, Luo D, Lin G S, Chen Z H, Huang C F, Li S Z, Zhang C X, Zhang Z R, Wei K J 2022 *Sci. China-Phys.*

Mech. Astron. **65** 120311
[46] Sheng Y B, Zhou L, Long G L 2022 *Sci. Bull.* **67** 367
[47] Zhou L, Sheng Y B 2022 *Sci. China-Phys. Mech. Astron.* **65** 250311
[48] Ying J W, Zhou L, Zhong W, Sheng Y B 2022 *Chin. Phys. B* **31** 120303
[49] Niu J L, Liu X C 2022 *Eurphys. Lett.* **139** 38001
[50] Wu J W, Long G L, Hayashi M 2022 *Phys. Rev. Appl.* **17** 064011
[51] Das N, Paul G 2022 *Europhys. Lett.* **138** 48001
[52] Cao Z W, Yao F W, Xiao X Q 2023 *Laser Phys. Lett.* **20** 045201
[53] Zhou L, Sheng Y B, Long G L 2023 *Phys. Rev. Appl.* **19** 014036
[54] Dŭsek M, Haderka O, Hendrych M, Gisin N 1999 *Phys. Rev. A* **60** 149
[55] Zeng G H, Zhang W P 2000 *Phys. Rev. A* **61** 022303
[56] Ljunggren D, Bourennane M, Karlsson A 2000 *Phys. Rev. A* **62** 022305
[57] Shi B S, Jiang Y K, Guo G C 2001 *Phys. Lett. A* **281** 83
[58] Zhang H G, Ji Z X, Wang H Z, Wu W Q 2019 *Chin. Commun.* **10** 1
[59] Tsai C W, Hwang T, Kuo L J 2011 *Commun. Theor. Phys.* **56** 1023
[60] Li J X, Zhang Y S, Guo G C 2021 *Europhys. Lett.* **133** 20004
[61] Dutta A, Pathak A 2022 *Quantum Inf. Process.* **21** 369
[62] Crépeau C, Salvail L 1995 *Quantum Oblivious Mutual Identification* (Berlin: Springer) p133
[63] Zeng G H, Wang X B 1998 arXiv: quant-ph/9812022
[64] Zhu D X, Zhao Z L, Zhang H J, Zhou Z Q, Li Y B, Zhao J, Song L J, Zheng J 2025 *J. King Saud Univ. Comput. Inf. Sci.* **37** 57
[65] Zhao W, Shi R H, Shi J J, Huang P, Guo Y, Huang D 2021 *Phys. Rev. A* **103** 012410
[66] Li Q, Wu J J, Quan J Y, Shi J J, Zhang S C 2022 *IEEE Trans. Inf. Forensics Secur.* **17** 3264
[67] Zhang X L 2009 *Chin. Sci. Bull.* **54** 2018
[68] Hong C H, Heo J, Jang J G, Kwon D 2017 *Quantum Inf. Process.* **16** 236
[69] Zawadzki P 2019 *Quantum Inf. Process.* **18** 7
[70] González-Guillén C E, González Vasco M I, Johnson F, Pérez del Pozo Á L 2021 *Entropy* **23** 389
[71] Calsi D L, Kohl P 2024 *Quantum Inf. Process.* **23** 357
[72] Rao B D, Jayaraman R 2023 *Quantum Inf. Process.* **22** 92
[73] Lee H, Lim J, Yang H J 2006 *Phys. Rev. A* **73** 042305
[74] Zhang Z J, Liu J, Wang D, Shi S H 2007 *Phys. Rev. A* **75** 026301
[75] Chang Y, Xu C X, Zhang S B, Yan L 2014 *Chin. Sci. Bull.* **59** 2541
[76] Zhang S S, Chen Z K, Shi R H 2020 *Int. J. Theor. Phys.* **59** 236
[77] Dutta A, Pathak A 2023 *Quantum Inf. Process.* **22** 13
[78] Ma H Q, Huang P, Bao W S, Zeng G H 2016 *Quantum Inf. Process.* **15** 2605
[79] Pirandola S, Ottaviani C, Spedalieri G, Weedbrook C, Braunstein S L, Lloyd S, Gehring T, Jacobsen, C S, Andersen U L 2015 *Nat. Photonics* **9** 397
[80] Xu F H, Curty M, Qi B, Qian L, Lo H K 2015 *Nat. Photonics* **9** 772
[81] Pirandola S, Ottaviani C, Spedalieri G, Weedbrook C, Braunstein S L, Lloyd S, Gehring T, Jacobsen C S, Andersen U L 2015 *Nat. Photonics* **9** 773
[82] Chen Z P, Yao F W, Xiao X Q 2024 *Laser Phys. Lett.* **21** 115201
[83] Liu W J, Chen H W, Li Z Q, Liu Z H, Hu W B 2009 *Chin. Phys. B* **18** 4105
[84] Zhu H F, Wang L W, Zhang Y L 2020 *Quantum Inf. Process.* **19** 381
[85] Wang J, Zhang Q, Tang C J 2006 *Chin. Phys. Lett.* **23** 2360
[86] Yuan H, Liu Y M, Pan G Z 2014 *Quantum Inf. Process.* **13** 2535
[87] Curty M, Santos D J 2001 *Phys. Rev. A* **64** 062309
[88] Liu D, Pei C X, Quan D X, Zhao N 2010 *Chin. Phys. Lett.* **27** 050306
[89] Chang Y, Zhang S B, Yan L L, Han G H 2015 *Chin. Phys. B* **24** 050307
[90] Zhou Z R, Sheng Y B, Niu P H, Yin L G, Long G L, Hanzo L 2020 *Sci. China-Phys. Mech. Astron.* **63** 230362
[91] Das N, Paul G 2022 *Quantum Inf. Process.* **21** 260
[92] Li G D, Liu J C, Wang Q L, Sun W Q 2024 *IEEE Commun. Lett.* **28** 473
[93] Zhou N R, Zeng G H, Zeng W J, Zhu F C 2005 *Opt. Commun.* **254** 380
[94] Xin X J, He F, Qiu S J, Li C Y, Li F G 2024 *Chin. J. Phys.* **92** 664
[95] Yang Y G, Wen Q Y 2009 *Chin. Phys. B* **18** 3233
[96] Zhang Z S, Zeng G H, Zhou N R, Xiong J 2006 *Phys. Lett. A* **356** 199
[97] Wang X F, Gu S P, Sheng Y B, Zhou L 2023 *Europhys. Lett.* **142** 68002
[98] Zhang Q, Du M M, Zhong W, Sheng Y B, Zhou L 2024 *Ann. Phys. (Berlin)* **536** 2300407
[99] Nicolas A, Veissier L, Giner L, Giacobino E, Maxein D, Laurat J 2014 *Nat. Photonics* **8** 234
[100] Sukachev D D, Sipahigil A, Nguyen C T, Bhaskar M K, Evans R E, Jelezko F, Lukin M D 2017 *Phys. Rev. Lett.* **119** 223602
[101] Zhong T, Kindem J M, Bartholomew J G, Rochman J, Craiciu I 2017 *Science* **357** 1392
[102] Liu X, Hu J, Li Z F, Li X, Li P Y, Liang P J, Zhou Z Q, Li C F, Guo G C 2021 *Nature* **594** 41
[103] Jin M, Ma Y Z, Zhou Z Q, Li C F, Guo G C 2022 *Sci. Bull.* **67** 676

SPECIAL TOPIC—Quantum information processing

Latest research progress of quantum identity authentication*

WANG Xingfu [1)] ZHENG Yanyan [2)†] GU Shipu [3)] ZHANG Qi [1)]
ZHONG Wei [4)] DU Mingming [3)] LI Xiyun [1)] SHEN Shuting [3)]
ZHANG Anlei [1)] ZHOU Lan [1)] SHENG Yubo [3)‡]

1) (*College of Science, Nanjing University of Posts and Telecommunications, Nanjing* 210023, *China*)

2) (*School of Physics and Electronic Information, Yan'An University, Yan'an* 716000, *China*)

3) (*College of Electronic and Optical Engineering & College of Flexible Electronics* (*Future Technology*), *Nanjing University of Posts and Telecommunications, Nanjing* 210023, *China*)

4) (*School of Communications and Information Engineering, Nanjing University of Posts and Telecommunications, Nanjing* 210003, *China*)

(Received 12 July 2025; revised manuscript received 5 September 2025)

Abstract

The absolute security of quantum communication protocols relies on a critical premise: all participating parties are legitimate users. Ensuring the legitimacy of participant identities is paramount in complex real-world communication environments. Quantum identity authentication (QIA), in which fundamental principles of quantum mechanics are used to achieve unilateral or mutual authentication between communicating parties, constitutes an indispensable core component for building a comprehensive quantum secure communication system. It holds significant research value in the field of quantum communication.

This review employs a comparative classification method to systematically outline the research trajectory of QIA protocols. By categorizing protocols based on the required quantum resources and the types of quantum protocols employed, the advantages and disadvantages of various categories are analyzed in terms of efficiency, security, and practicality. Single-photon protocols require low resources, and they are easy to implement, and compatible with existing optical components, but require high-efficiency single-photon detectors and exhibit weak noise resistance. Entangled-state protocols offer high security and strong resistance to eavesdropping, particularly suitable for long-distance or multi-party authentication. However, they greatly depend on the preparation and maintenance of high-precision, stable multi-particle entanglement sources, resulting in high experimental complexity. Continuous-variable (CV) protocols achieve high transmission efficiency in short-distance metropolitan area networks and are compatible with classical optical communication equipment, making experiments relatively straightforward. Yet, they require high-precision modulation technology and are sensitive to channel loss. Hybrid protocols aim to balance resource efficiency and security while reducing reliance on a single quantum source, but their design is complex and may introduce new attack vectors. Quantum key distribution (QKD) framework protocols embed identity authentication in the key distribution process, making them suitable for scenarios requiring long-term secure key distribution, although they often depend on pre-shared keys or trusted third parties. Quantum secure direct communication (QSDC) framework protocols integrate authentication with secure direct information transmission, offering high efficiency for real-time communication, but requiring high channel quality. Measurement-device-independent QSDC (MDI-QSDC)

* Project supported by the National Natural Science Foundation of China (Grant Nos. 12175106, 92365110).

† Corresponding author. E-mail: yyz@yau.edu.cn

‡ Corresponding author. E-mail: shengyb@njupt.edu.cn

represents a key development direction that can resist attacks on measurement devices. Quantum teleportation (QT) framework protocols achieves cross-node authentication and unconditional security, making it suitable for quantum relay networks despite its high experimental complexity. The entanglement swapping framework protocol can resist conspiracy attacks and is suitable for multi-party joint scenarios, but it consumes a lot of resources and relies on trusted third party. Ping-pong protocol framework supports dynamic key updates and exhibits strong resistance to eavesdropping, making it suitable for temporary authentication on mobile terminals, although it typically only supports unilateral authentication and requires a bidirectional channel.

Subsequently, this review details the latest QIA protocols of our research group, including a multi-party synchronous identity authentication protocol based on Greenberger-Horne-Zeilinger (GHZ) states, and a tripartite QSDC protocol with identity authentication capabilities utilizing polarization-spatial super-coding. The GHZ-based multi-party synchronous authentication protocol leverages the strong correlations inherent in GHZ states to achieve simultaneous authentication among multiple parties. Through a carefully designed two-round decoy-state detection mechanism, it effectively resists both external eavesdropping and internal attacks originating from authenticated users, thereby enhancing the efficiency and security of identity management in large-scale quantum networks. The core innovation of the polarization-spatial super-coding tripartite QSDC protocol lies in its deep integration of the authentication process with information transmission by utilizing the spatial degrees of freedom of single photons. This design accomplishes the identity verification of two senders and the transmission of secret information within a single protocol run, ensuring end-to-end security through a three-stage security check. This "authentication-as-communication" paradigm significantly improves the overall efficiency and practicality of the protocol. Its successful implementation also relies on advancements in quantum memory technology.

Finally, the review outlines future research directions for quantum identity authentication and explores its potential applications in quantum communication. The QIA research needs to focus on reducing resource dependency, exploring more efficient protocol designs, further enhancing protocol integration and robustness, prioritizing the development of protocols adaptable to real-world environments, and actively investigating integration with novel scenarios. This comprehensive review aims to provide theoretical research foundations and technical support for the practical development of future quantum identity authentication.

Keywords: quantum identity authentication, quantum secure communication, quantum entanglement

PACS: 03.67.Pp, 03.67.Hk, 03.65.Ud **DOI:** 10.7498/aps.74.20250920

CSTR: 32037.14.aps.74.20250920