多方量子密钥协商：架构、最新进展与开放问题

Malik Mouaji、Saif Al-Kuwari,

arXiv:2603.03225v1 [quant-ph] 3 Mar 2026

摘要—**多方量子密钥协商（MQKA）使 $n \geq 3$ 互不信任的用户能够通过协作式量子协议建立共享的秘密密钥。本文全面回顾了该领域，并指出，理解MQKA的最佳方式是将其视为一个沿三个相互正交又紧密耦合的维度组织起来的设计空间：（1）网络架构，决定量子态如何在参与者之间传递；（2）量子资源，编码实现所用的物理自由度；（3）安全模型，界定对设备和基础设施的信任假设。我们不把MQKA视为一系列彼此孤立、线性排列的协议，而是采用这一三维视角，揭示反复出现的模式、鲜明的权衡取舍以及尚未探索的设计空间。我们将MQKA协议划分为不同的结构类别，将其与底层量子资源对应起来，并分析不同安全模型如何影响公平性和抗合谋性。此外，我们还指出了可组合安全框架、原生网络集成和设备无关实现方面的开放挑战，并提出一项研究路线图，推动发展适用于后NISQ时代未来量子互联网部署的混合资源、玻色编码和公平感知多方量子密钥协商。**

索引词—**多方量子密钥协商、量子密码学、公平性、抗串谋、测量设备无关协议。**

I. 引言

量子密码学常被宣传为“基于物理定律而非数学假设的安全性” [1, 2, 3]。量子密钥分发（量子密钥分发）最初由BB84协议正式提出，它以优雅的方式体现了这一理念，适用于双方场景 [3, 4, 5, 1]。然而，现实中的量子网络很少仅以双方配对的方式运行 [6,7]。现代分布式基础设施——数据中心、卫星、政府机构、边缘设备——要求多个彼此从未完全信任的利益相关方之间进行安全通信 [8, 9]。这种场景引入了双方量子密钥分发中不存在的关键区别：谁参与密钥生成，以及各方如何公平地分享控制权，其重要性不亚于能否阻止外部窃听者 [10,11]。

多方量子密钥协商（MQKA）正是为应对这一场景而提出的 [12]。在多方量子密钥协商中，一组 n用户希望建立一把供所有人共同使用的密钥，但没有人愿意让其他人单方面决定密钥内容 [10, 13]。该协议必须确保每一方的贡献都真正编码在最终密钥中，同时防止串谋联盟操纵协商结果，并且这一切都必须考虑现实信道中的损耗、探测器缺陷和技术限制 [14]。近期进展凸显了多方量子密钥协商在新兴应用中的重要性日益提升；在这些应用中，公平性至关重要，包括量子云中的安全多方计算 [15, 16],、分布式量子传感网络 [17, 18], 、受区块链启发的量子账本 [19], 、门限密码学 [20],以及联邦量子机器学习 [21, 22, 23]。

然而，与双边对应方案相比，多方量子密钥协商的研究仍然不足，部分原因在于它结合了量子力学复杂性 [24, 25] 与博弈论和对抗性推理 [26]。量子密钥分发与量子密钥协商之间的区别构成了多方量子密钥协商研究的核心动机 [17]: 量子密钥分发由一个可信参与方（Alice）生成并向其他参与方（Bob、Charlie 等）分发秘密密钥，其安全模型侧重于检测外部窃听者；尽管量子密钥分发实现了信息论安全性，却无法应对内部威胁 [27, 28]。相比之下，量子密钥协商要求所有参与方平等地参与密钥生成，确保最终密钥是所有参与者输入的对称函数；其安全要求不仅包括对外部窃听者的检测，还包括内部公平性保证，从而确保任何一组不诚实参与者都无法预先计算或操纵协商好的密钥 [29, 30,31]。具体到多方量子密钥协商，情况更加微妙，因为部分参与者可能会串通攻击协议，试图迫使协议接受预定密钥，同时不被发现 [32]。这引入了量子密钥分发中完全不存在的对抗性博弈论要素。

本文认为，多方量子密钥协商的设计由三个紧密关联的选择所驱动：（1）承载量子态的网络架构；（2）这些量子态所蕴含的量子资源；以及（3）规范信任与对手的安全模型。通过沿这些维度对相关文献进行分类，我们揭示了拓扑结构与量子资源如何相互作用以实现或妨碍公平性的反复模式，以及安全保证、效率、实现复杂度和噪声容忍度之间显著的权衡。我们还指出了尚未探索的空白领域，其中蕴藏着开展重要新研究的机会，例如采用双场技术以扩展安全距离 [9],，或使用有望在噪声环境中实现更高密钥率的高维系统 [33]。近来，玻色量子纠错领域的进展——尤其是 GKP 和猫态编码——为实现容错、抗噪的多方量子密钥协商开辟了全新的前沿。

本综述的主要贡献有四点：第一，我们提出了一种多方量子密钥协商的组织原则，将表面上彼此无关的协议统一起来，揭示其隐含的

Malik Mouaji 任职于卡塔尔多哈的哈马德·本·哈利法大学科学与工程学院卡塔尔量子计算中心。Saif Al-Kuwari 任职于卡塔尔多哈的哈马德·本·哈利法大学科学与工程学院卡塔尔量子计算中心。

结构与权衡；第二，我们将公平性和串谋提炼为实用的设计约束，并阐释不同拓扑结构和资源选择如何体现参与者之间隐含的权力结构；第三，我们分析了各主要类别中的代表性协议——环形、树形、星形、完全图和混合架构——并考察其采用的多种量子资源与安全模型；第四，我们重点介绍新兴前沿，包括混合 GHZ/W 态、高维系统、基于玻色编码的多方量子密钥协商、设备无关的发展趋势、半量子模型，以及适用于实际量子互联网部署的网络原生多方量子密钥协商。

本综述论文的其余部分结构如下：第II节回顾经典多方密钥协商，奠定概念基础；第III节形式化多方量子密钥协商的安全性与公平性要求；第IV节全面分析作为密码学策略的网络架构；第V节考察量子资源及其实现挑战；第VI节讨论从设备相关到设备无关框架的安全模型；第VII节涵盖公平性、串谋以及博弈论视角；第VIII节讨论实际考量，包括性能指标、噪声鲁棒性与网络集成；第IX节指出开放挑战与研究方向；第X节以综合总结与路线图作结。

II. 经典多方密钥协商

在开创性的Diffie-Hellman（DH）协议中， [34]，两名参与方Alice与Bob利用公开素数模数 p 及生成元g [35, 36]，通过模幂运算计算共享秘密。然而，将其扩展到多方会引入双方场景中并不存在的复杂性：参与方如何确保所有 N 贡献都会影响最终密钥？我们如何防止由（$N-1$）名不诚实参与方组成的串谋联盟强制设定预定密钥？

Burmester-Desmedt 协议 [37] 基于 DH 假设，为 n 个参与方实现恒定轮数的群组密钥协商。使用阶为 q 、生成元为g的无环群 G。该协议由以下步骤描述 [38]：

1）设置：参与方就公开参数（G、q、g）达成一致。每个参与方 P_i 选择随机秘密值 x_i 并广播

$$z_i = g^{x_i}$$

2）第 1 轮：每个参与方 P_i 计算并广播

$$X_i = \left(\frac{z_{i+1}}{z_{i-1}}\right)^{x_i}$$

3）第 2 轮：每个参与方 P_i 计算

$$K_i = (z_{i-1})^{nx_i} X_{i-1}^{n-2} X_{i+1}^{n-2} ... X_{i-1}^{n-2}$$

4）最终密钥：

$$K = g^{x_1x_2+x2x_3+...+x_nx_1}$$

尽管该协议在判定性 Diffie-Hellman（DDH）假设下实现了贡献公平性（每个 x_i影响 K）以及对被动对手的安全性，但它需要认证信道来防止主动攻击。

然而，经典多方密钥协商面临基本限制：
1）计算假设：安全性依赖于困难性假设（因数分解、离散对数），而这些假设会因 Shor 算法而受到量子计算机的威胁。2）认证信道：大多数经典协议需要预先建立的认证信道，从而增加基础设施复杂度。3）公平性验证：经典方案无法在没有事后明确密码学证明的情况下，防止不诚实方通过在协议执行过程中偏离而获得优势。4）串谋检测：在没有事后分析谁获知了什么的情况下，检测串谋联盟的能力有限。

量子力学提供了根本不同的保障 [1] ：信息论安全性独立于计算假设，测量诱导扰动能够实现实时窃听检测，而基于纠缠的关联则使公平性验证能够直接嵌入协议物理机制中 [39]。

III. 多方量子密钥协商

多方量子密钥协商（MQKA）是一类协议，互不信任的参与方通过量子信道和认证经典信道进行交互，以建立共同秘密密钥。参与者共同执行量子操作和测量，使最终密钥由集体决定，而非由任何单一参与方选定；同时，每位参与者的贡献均等，因此任何适当子集都无法单方面确定或预测协商出的密钥。因此，MQKA 位于量子密码学、分布式系统和对抗性博弈论的交汇处：它不仅必须抵御外部窃听者，还必须防范内部人合谋，同时还要在含噪、有损的量子信道和不完美硬件等实际约束下运行。

严谨的多方量子密钥协商协议必须同时满足以下几个条件：

- 正确性。 所有遵循协议的诚实参与者最终都会得到相同的密钥 K（除非发生概率可忽略的情况） [10]。这确保合法参与方能够建立共享秘密，以供后续密码操作使用。
- 抗外部窃听者安全性。 任何未参与协议的外部对手（即 Eve）都无法在不被发现的情况下获取有关最终密钥的信息。Eve 的窃听必须使量子比特误码率（QBER）超过经典噪声水平，从而触发协议中止并被探测到。这项要求与量子密钥分发的安全性要求相似。
- 公平性。 每位参与者的输入对最终密钥的影响权重相同。形式上：即使拥有无限计算能力并可任意选择输入比特，任何真子集 $S \subset \{P_1, P_2, ..., P_n\}$ 都无法单方面确定最终密钥。这确保（$m-1$）不诚实参与者无法强迫其他人接受预定密钥 [40]。这是多方量子密钥协商与量子密钥分发之间的本质区别。
- 个体贡献隐私。 对于使用语义有意义输入（包含身份

信息）的协议，参与者的个体贡献必须保持隐藏。知晓自己的子密钥和最终密钥不应泄露他人的子密钥 [41]。对于使用随机比特输入的协议，这一要求不那么关键。

MQKA设计的根本难点在于同时实现外部安全性与公平性。安全性借鉴了从QKD沿袭而来的成熟量子探测原理，而公平性则要求采用复杂的编码方案，以抵御参与者的策略性串通——这是一个兼具量子信息论与对抗博弈论的问题。此外，在维持$O(N)$量子信道的同时，实现针对不受限制的合谋的信息论公平性，似乎从根本上难以做到。这促使人们提出了三种权衡方法（本文将对此进行详细分析）：

- 增加量子信道（完全图量子密钥协商）：牺牲效率以保证公平性
- 渐近公平性（分区方法）：通过分组实现抗串谋
- 宽松公平性（半可信模型）：引入第三方验证，或限制对手联盟

实用的MQKA设计由三个相互正交但紧密耦合的维度决定：

1）网络架构：网络架构决定量子态如何在参与者之间传递。每种架构都会形成特定的共谋模式，并带来不同的公平性挑战。2）量子资源：这些是MQKA协议中用作信息载体的一系列量子态矢量（单量子比特、多量子比特和纠缠态）；每一类都具有独特的噪声特性、制备与测量复杂度以及可扩展性。3）安全模型：这些模型定义了关于设备的假设，并决定必须明确应对哪些侧信道，以及如何证明公平性。

IV. 网络架构

从图的角度来看，多方量子密钥协商协议将参与者和量子信道嵌入具有不同安全性和效率特征的拓扑结构中。拓扑结构隐含地决定了密钥控制权的分配方式。表（ IV-E）简要概述了多方量子密钥协商（MQKA）协议采用的各种架构。该总结突出了各架构的不同特征与功能，展示了它们在提升量子通信系统的安全性和效率方面各自发挥的作用。在以下各节中，我们将进一步介绍每种网络架构。

A. 环形架构

在环形或环形结构架构中，MQKA协议围绕一个“传递式量子令牌”组织，该令牌沿闭环依次访问所有n 参与者。每位参与者对传入的载体（通常是单量子比特或贝尔对的一半）应用局域幺正操作，以编码其私有贡献，然后如图1所示将其转发给下一位用户。这种拓扑结构仅需 O（n）个量子信道，并具有非常自然的路由结构：一条返回源点的单向路径，因此非常适合光纤环网 [42]、卫星链路或城域暗光纤环路等线性基础设施。所采用的量子态通常是贝尔对，例如

$$|\Phi^+\rangle = \frac{1}{\sqrt{2}}\left(|00\rangle + |11\rangle\right),$$

传输子系统不断累积编码序列 [43]。

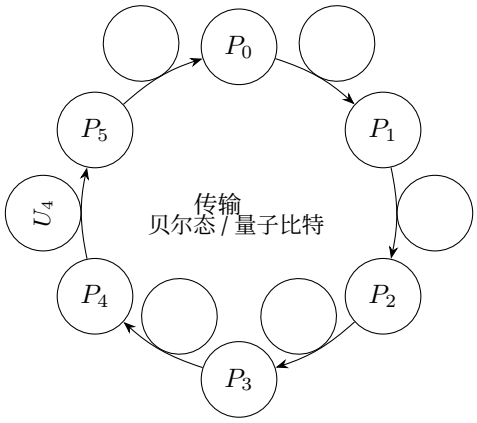

图 1. 环形多方量子密钥协商拓扑：一个游走的纠缠载体（贝尔对或单量子比特）依次访问所有参与方 P_0、.....、P_{n-1}，每个参与方在转发前施加局域酉变换 U_i。

一轮通用的环形多方量子密钥协商按如下方式进行：每个参与者 P_i 随机采样一个随机秘密 S_i，由指定参与方（例如 P_0）制备初始纠缠态 $|\psi\rangle$，并沿环形结构发送其中一个子系统。在步骤 i，参与者 P_i 施加酉变换 U_i（S_i）来编码其贡献，并将载体转发给 P_{i+1} ，直至其返回起点。经过一整圈传递后，最终量子态编码了所有贡献的异或（或其他对称函数）；通过诱骗态和 QBER 阈值监测窃听，在低噪声条件下，密钥率通常接近每个密钥比特对应一个

$$r \approx 1 - h(Q)$$

原始量子比特。外部安全性可通过贝尔不等式检验来保障；例如，CHSH 违背 > 2 可证明存在能够检测截获-重发攻击的非经典关联，这与基于纠缠的量子密钥分发类似。

环形架构的主要局限在于串谋情况下的公平性 [43]。由于令牌按固定顺序经过各参与方，因此会产生结构性不对称：在某些情况下，靠后的参与者和某些相邻联盟可能会撤销或重新编码先前的贡献，或重构有关诚实用户份额的部分信息。Liu 等 [43] 已验证了串谋攻击：两个处于策略位置的不诚实参与方在协议中途测量传递中的令牌，以提取诚实方秘密的异或值，随后再翻转编码，从而迫使协议产生预定密钥，同时仍未达到窃听阈值

。后续研究通过采用针对量子态区分界设计的非正交编码 [14], 、为每个源使用异构酉算子集 [44, 45], 或将参与者渐近划分为子环 [45, 46], , 缓解了这些漏洞；但若无额外机制，环形结构固有的位置偏差使得实现强公平性并非易事。

B. 完全图架构

完全图量子密钥协商协议假设每一对参与者之间至少共享一个量子信道，从而形成一个完全连接图，覆盖 n 个用户，如图2所示。在这种设置下，典型的设计模式是为所有 $\binom{n}{2}$ 条链路建立成对密钥——通常通过基于贝尔态的量子密钥分发或量子密钥协商变体实现——然后使用经典组合层，将这些成对秘密压缩为单个群密钥 [32]。这种极端冗余带来了强大的安全性和公平性：由于每个诚实参与者贡献的信息分散在许多独立链路上，联盟必须控制图中压倒性多数的部分，才能确定性地迫使最终密钥取某个值或预测最终密钥。

全连通的代价是资源消耗巨大。量子信道的数量按 $O(n^2)$扩展，并且每条链路都需要纠缠态分发、测量和经典认证，因此随着 n 的增长，总资源预算会大幅增加。由于验证开销过高，密钥率可能受到影响；有效渐近速率通常近似为 $r \approx 1 - nh(Q)$，这反映了在大量链路上执行纠错和奇偶校验所产生的累积影响。在近期硬件上，实现超出 $n \approx 20$ 的规模具有挑战性，因为这需要数千条彼此独立的量子连接以及它们之间的同步。

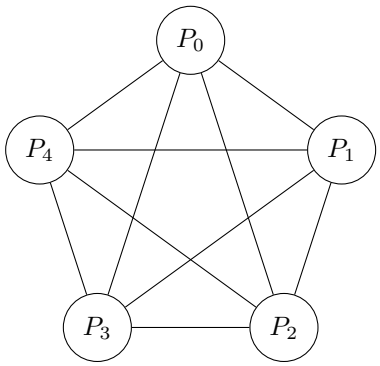

图 2. 完全图量子密钥协商拓扑：每对参与者 P_i, P_j至少共享一个量子信道以导出 K_{ij}，经典层则将成对密钥压缩为一个全局群密钥。

积极的一面是，完全图架构能够提供强有力、近乎信息论级别的公平性保证 [32]，因为任何小型联盟都无法全面获知所有诚实用户的成对密钥；此外，还可以设计经典组合规则，使每个诚实参与方的份额在足够多的参与方串谋之前始终保密。这类协议表明，至少从理论上说，多方量子密钥协商可以通过牺牲效率并接受量子基础设施的二次规模增长，来实现对任意串谋的公平性。在实践中，这类方案最适用于规模较小、安全性要求较高的群体，在这些群体中，最大限度的鲁棒性和公平性比部署与维护开销更为重要。

C. 树形架构

基于树的多方量子密钥协商协议将参与者嵌入生成树拓扑，其中叶节点代表最终用户，内部节点沿分层分支聚合子密钥 [47, 48]。量子关联（通常是沿树向下分发的 GHZ 态或贝尔态）将贡献从叶节点传向根节点，根节点据此将所有叶节点输入作为对称函数，重构出全局密钥。图 3 展示了一种典型的树形架构。这种架构以更具可扩展性的结构取代了完全图的高度冗余，同时仍支持并行聚合：对于深度为 d 的树，内部节点组合本地子密钥，根节点则通过对所有聚合的分支贡献进行异或或哈希来导出最终密钥 k [44]。

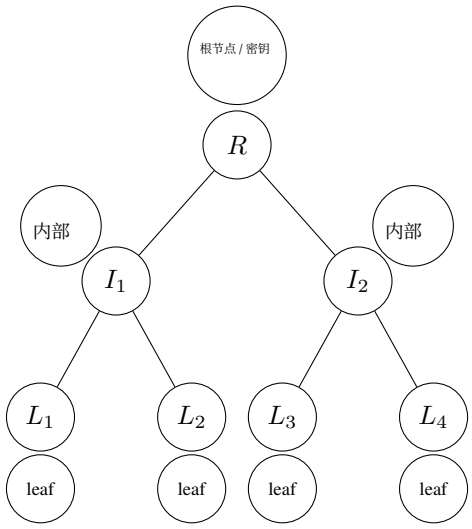

图 3. 树型多方量子密钥协商拓扑：叶节点参与者贡献本地子密钥，内部节点将其聚合，根节点则通过合并所有叶节点的贡献来导出最终密钥。

从性能角度来看，基于树的方案比全连接拓扑更具扩展性 [48, 44]。量子信道的数量保持为 $O(n)$，而逻辑开销随树深度增长；计入经典后处理后，密钥率表达式通常为 $r \approx log(n) - h(Q)$。通过诱骗态和分支测试来防范窃听，其检测概率可根据测试轮次的数量 [44] 进行界定。公平性通过层级结构得到保障：局限于某一分支的串谋只会影响该分支的聚合结果，其他分支仍保持不变；但根节点和高层内部节点处于天然的控制瓶颈位置，因此需要加强保护。

具体的基于树的多方量子密钥协商协议，例如受BB84启发且带有身份认证的方案，表明该架构可支持数十名参与者，同时将量子与经典开销保持在可控范围内 [47, 49]。身份认证层——例如，量子

数字签名 [50, 51]或与量子交互记录承诺绑定的经典消息认证码 [52, 53]——有助于防止内部节点上的冒充，并通过确保仅合法叶节点对全局密钥作出贡献来增强公平性。其代价是，相较于简单的环形设计，协议复杂度有所增加，并且需要加固根节点和中间节点，以抵御外部攻击与内部人员攻击，但树型架构对于中等规模、按层级组织的量子网络仍然具有吸引力。

D. 星形（客户端—服务器）架构

在星形架构（亦称客户端—服务器架构）中，参与者连接到一个中心枢纽（通常称为量子服务器或中继），由其协调纠缠分发与测量；外围客户端仅执行局部编码和经典校验 [11]。枢纽可以生成并分发多体 GHZ 态

$$|GHZ_n\rangle = \frac{1}{2}\left(|0\rangle^{\otimes n} + |1\rangle^{\otimes n}\right)$$

或等效的簇态，并通过不同的量子链路向每个客户端发送一个量子比特 [54]。随后，每个客户端应用局部相位或比特操作来编码其贡献，枢纽则在 X 或 Z基下进行联合测量，以揭示全局关联；这些关联可映射为对称函数 $K = f(k_1, k_2, \ldots\ldots, k_n)$，通常是所有用户输入的异或 [22]。图 4 展示了星形架构。

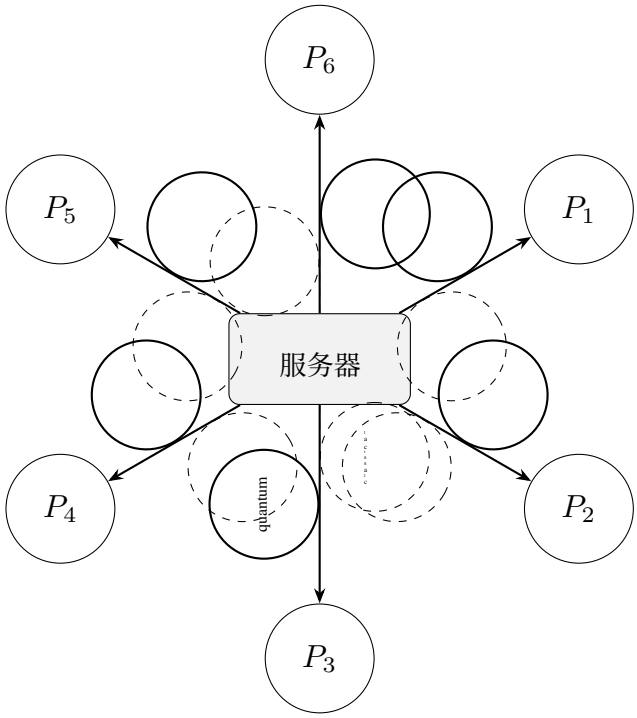

图 4. 星形/客户端—服务器多方量子密钥协商拓扑：中心枢纽分发多体纠缠并协调测量，外围客户端 P_i 执行局部编码和经典校验。

这种架构与新兴的量子接入网络十分契合：少数位于中心位置的节点拥有高端量子硬件，而许多边缘用户的能力有限。量子信道复杂度按 $O(n)$ 扩展，枢纽则可集中执行 GHZ态生成和多量子比特探测等昂贵操作。原则上可以实现 $r \approx 1 - h(Q)$ 的密钥率，但实际性能取决于 GHZ保真度和多光子干涉可见度。从安全性角度看，如果枢纽是诚实的，协调公平性会更容易，因为中心节点可以强制执行对称接受准则和奇偶校验，以确保每位客户端的贡献都体现在最终密钥 [55] 中。

然而，星型拓扑引入了一个影响力巨大的中心节点。恶意或遭入侵的枢纽可以关联态制备与测量选择，从而偏置密钥或部分获知密钥；枢纽与部分客户端串谋也可能破坏公平性，除非安全模型明确对此加以处理。测量设备无关多方量子密钥协商变体通过将枢纽严格视为不受信任的中继，并让其执行黑盒类GHZ测量，来缓解这一问题；同时假设客户端的源设备可信 [11, 54]，从而将探测器侧信道排除在讨论范围之外。近期协议 [56, 57] 还探索了半量子星型架构，其中一些客户端为经典设备，并将量子操作委托给枢纽。这进一步降低了客户端的要求，但需要谨慎证明针对枢纽和客户端联盟的公平性。

E. 混合架构

混合多方量子密钥协商架构有意结合多种基础拓扑——最常见的是环形、星形和树形——以发挥它们各自的优势，并更好地适应异构网络条件。文献中常见图5所示的混合架构，因为它在各种量子通信场景中具有更大的灵活性和适应性。例如， [45]中的作者采用星形枢纽生成纠缠并执行粗粒度协调，同时由客户端环依次编码贡献，以更均匀地分配影响力 [45]。另一种常见模式是通过一个或多个共享参与者连接若干环形或树型子网，使每个子网内部兼顾公平性和效率，同时通过子网间耦合实现全局密钥协商 [58]。

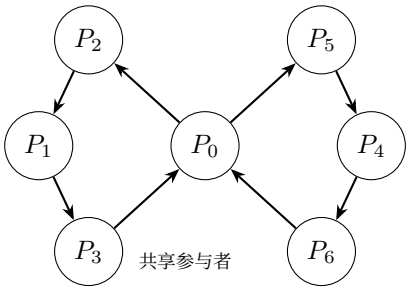

图 5. 混合环-环多方量子密钥协商拓扑：两个环型子网共享一个参与者 P_0，如基于 W态的混合架构中， P_0 连接并协调两个环形结构。

架构	直观人格	串通／公平性影响	实现说明	《量子》通道	纠缠Type	噪声容忍性ance
圆形（环形）	在 trav- 上顺序令牌传递 eling 纠缠载体 [14]	自然对称性，但与位置相关的串谋可能会发生，前提是后加入的参与方能够撤销先前的贡献 [14, 22, 55]	简单路由，量子比特数量多效率 [42]	$O(N)$	双量子比特	中等
Star	辐射式或客户端-服务器结构 [22]	公平性通过中央协调-协调；由枢纽的串谋信任模型和协议规则 [22]	与量子接入网络相连，以及客户端-服务器架构 [59, 60]	$O(N)$	N量子比特	中等
Tree	分层聚合子-密钥（生成树风格） [44, 60]	分支式串谋受限 by 层级结构；根节点 以及互- nal 节点需要谨慎保护措施 [44]	比完全图更具可扩展性；资源开销适中 [44]	$O(N)$	N量子比特	Low
完全图	完全连接的两两信道以及后处理 [61, 32]	由于冗余而具有很强的弹性，但公平性被转移到经典处理 [61]	资源消耗大；对于大型而言较差 n [61]	$O(N^2)$	双量子比特	High
混合	星形、环形和树形边 [45]	可调节的稳健性与公平性和效率之间的权衡 [45, 62]	灵活但更加复杂 plex 工程 [10, 62]	$O(N)$	混合	High

表 I 多方量子密钥协商架构及其定性属性。

这些配置开辟了丰富的设计空间，可在鲁棒性、公平性和效率之间进行灵活权衡。在环形结构上叠加星形边，可以减少纯环形协议固有的位置偏差，同时仍能受益于子环内的简单路由以及子环之间的集中式路由。在这类混合架构中使用W态纠缠取代GHZ态，可增强弹性，因为单个量子比特丢失时，W态的退化过程较为平缓。因此，采用W态资源的混合星环方案在有损条件下仍能维持可接受的密钥率和公平性保证，而这些条件会使基于GHZ态的协议失效。同样，可以将树形组件嵌入更大的星形或环形骨干结构中，以局部化串谋风险，并降低任何单个分支发生故障所造成的影响。

混合设计的主要缺点是工程复杂性较高。它们需要在不同子网络之间，甚至不同物理资源类型之间，谨慎协调纠缠生成、路由和测量（例如，将 GHZ 态片段接入 W态或簇态片段）。尽管如此，随着量子网络朝着异构基础设施发展，混合多方量子密钥协商架构显得越来越自然。它们使协议设计者能够更精细地塑造权力分配和公平性属性——例如，选择哪些节点位于共享枢纽上、哪些参与者连接环形结构，以及哪些分支由更稳健的纠缠提供保护——同时仍能维持量子信道数量整体上的 $O(n)$ 扩展性。

V. 量子资源

在多方量子密钥协商领域，量子资源的选择对于决定协议的可行性、效率、抗噪能力和安全性起着至关重要的作用保证 [64]。本节探讨支撑 MQKA 协议的各种量子资源，详细介绍它们各自的特性及其对性能的影响。我们将深入考察离散变量态、高维态、连续变量、双场配置和混合态等关键资源。表 IV 总结了这些资源，重点介绍其独特属性，以及它们对密钥交换系统整体安全性和效率的贡献。了解这些量子资源，有助于我们更好地认识它们对 MQKA 发展的影响，以及相关挑战。

A. 离散变量（*DV*）资源

离散变量纠缠态，尤其是贝尔态、GHZ态和W态，构成了许多现有MQKA协议的骨干结构。离散变量（DV）纠缠态以不同且可计数的值为特征，例如光子的偏振或粒子的自旋态，因此能够进行精确的操控和测量 [65, 66]。MQKA协议中的DV态利用了其成熟的安全性证明和鲁棒性，因此成为连续变量密钥可靠生成的首选方案（见 V-C 节）。

a) 贝尔态：贝尔态是最大纠缠的双量子比特态，例如 [67, 68]

$$|\Phi^{\pm}\rangle = \frac{1}{\sqrt{2}}\left(|00\rangle \pm |11\rangle\right)$$

and

$$|\Psi^{\pm}\rangle = \frac{1}{\sqrt{2}}\left(|01\rangle \pm |10\rangle\right)$$

贝尔态广泛用作成对方案和环形方案中的核心资源（这些方案得益于成熟的光子技术和离子阱技术的支持），因为每个纠缠对都可以编码一位

N	保真度	实验状态
2（贝尔）	>95%	常规
3（GHZ）	90%	已验证
4 (GHZ)	80%	具有挑战性
5-6 (GHZ)	60-70%	困难；演示有限
7+ (GHZ)	<50%	演示 极高的技术难度
损失下的脆弱性	$\|GHZ_N\rangle \rightarrow$	未纠缠态。

表 II GHZ态的保真度与实验状态

共享随机性 [69, 70]。这类量子态在概念上简单、能够高保真度地生成，且与基于贝尔不等式的安全性证明直接相关，因此在离散变量多方量子密钥协商 [46] 早期及当前的实验实现中尤其具有吸引力。然而，基于贝尔态的多方量子密钥协商通常需要多个成对信道或重复多轮，才能覆盖所有参与者。随着群组规模扩大，这会增加资源消耗和验证开销。

*b) GHZ*态：另一方面，GHZ态提供真正多方纠缠，将所有参与方联系到单一的全局关联模式中 [58, 71]

$$|GHZ_n\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle^{\otimes n} + |1\rangle^{\otimes n}\right)$$

这支持星形 [11] 与树 [49] 架构，其中一个n量子比特资源可为共同密钥比特以及基于多体奇偶关系的公平性检查提供支持。在实践中，GHZ态会随着 n 的增加而变得脆弱：报告的保真度从三个量子比特时的90%以上下降到六个量子比特时的70%以下，甚至单次光子损失就可能使该量子态实际上无法使用 [72]。因此，基于GHZ的多方量子密钥协商目前仅对中小型群体切实可行，至少就近期硬件而言是如此 [58]。GHZ态的主要保真度与状态要点可概括如表 II

*c) W*态：W态代表一种不同风格的多体纠缠，具有独特的鲁棒性 [73,72]。一个 n量子比特W态具有如下形式

$$|W\rangle = \frac{1}{n}\left(|100...00\rangle + ... + |00...01\rangle\right)$$

其中，单个激发由所有参与方共享。如果一个量子比特丢失或被测量，剩余系统仍保持纠缠，形成较小的 W态；而在相同情况下，GHZ态往往会失去几乎所有有用的关联。这种在损耗下逐渐退化的特性，使基于W态的多方量子密钥协商在噪声大且存在损耗的网络链路中颇具吸引力 [45, 74]。

实验研究表明，与相近规模的 GHZ 态相比，中等规模的 W态通常更容易以高保真度制备 [45]。在 W态多方量子密钥协商中，中心节点可以分发一个 W态，随后参与者通过局域操作编码各自的贡献，既可以沿着小型环形结构依次进行，也可以采用星形配置。分析表明，这类协议能够容忍几个百分点量级的比特翻转错误率，同时保持非零密钥率，并在现实硬件条件下支持数十名用户组成的群体。与基于GHZ态的方案相比，它们牺牲了一些理想关联强度，以显著提高对不完美因素的鲁棒性 [72, 45]。W态的保真度和状态可概括如下表 III 所示。

N	保真度	状态
3	>90%	已验证可常规实现
4	85%	已验证；复杂度适中
5	75%	具有挑战性；演示有限
6+	可变	研究前沿

表 III 实验 W 态的保真度与现状

d) Dicke 态：Dicke 态是一类自然的多体纠缠态，其特点是固定数量的激发分布在 n 个量子比特 [75]中k 。具有 n 个量子比特和 k 个激发的 Dicke 态 $|D_n^k\rangle$是如下对称叠加

$$|D_n^k\rangle = \frac{1}{\sqrt{\binom{n}{k}}} \sum_{\text{perms}} |1^{\otimes k}0^{\otimes(n-k)}\rangle.$$

这是所有恰有 n 个量子比特处于 $|1\rangle$ 、其余 $n-k$ 个量子比特处于 $|0\rangle$ [76] 的基态的等幅叠加。与 W态（$k=1$）类似，Dicke 态具有鲁棒的多体纠缠，但将这种鲁棒性推广到了更大的激发比例和更复杂的纠缠结构 [75, 76]。

在多方量子密钥协商场景中，如同量子网络 [77, 78], , Dicke 态协议通常会牺牲部分最大关联，以增强对损耗、退相干和不完美探测器的弹性。与 W态和 GHZ态相比，Dicke 态处于两者之间：它对量子比特损耗具有更强的鲁棒性（代价是适度的 k ），并具有丰富的多体关联，这在误差预算现实的网络中颇具优势。

e) 簇态：簇态也称为图态，是一类独特的多体纠缠资源。其构造方法是先将量子比特初始化为 $|+\rangle$ 态，再沿所选图 [79]的边施加受控-Z 门。 n量子比特簇态将纠缠编码在图结构中，从而支持基于测量的量子密钥分发和身份认证协议；密钥提取通过由拓扑 [80]引导的自适应单量子比特测量来实现。这种图嵌入纠缠具有模块化可扩展性（$2D$ 或 $3D$ 晶格），并且有望对某些损耗和测量不完美性保持鲁棒性，其安全性和分发特性由拓扑决定。

光子、离子阱和超导平台上均已有实验演示，但可扩展的生成与验证、 [81], 以及分布式多方量子密钥协商场景中的动态测量自适应性仍是当前面临的挑战。实践中，簇态多方量子密钥协商利用顺序或自适应测量来驱动信息流和密钥生成步骤， [82],从而实现灵活的架构，以适应不同的网络拓扑和资源约束 [83,84, 85]。仍需进一步研究如何根据图拓扑和硬件特定噪声模型量化性能指标（密钥率、损耗容忍度和误差阈值）。

B. 高维多方量子密钥协商

高维多方量子密钥协商以 d能级系统取代量子比特，这类系统称为量子比特（qudit） [33]。在这些协议中，会使用 $\mathcal{C}$ 上的广义贝尔态或图态，例如

$$|\Psi^+\rangle = \frac{1}{\sqrt{d}} \sum_{k=0}^{d-1} |k\rangle_A |k\rangle_B$$

而且，每个纠缠对原则上都能承载超过一比特的原始熵。对于固定数量的传输载体，这能提高信息密度，并有望提升密钥率；同时，扩大的结果空间也可能削弱某些攻击的效果。

其缺点主要在于实际应用。生成高质量的d–维纠缠态、执行稳定的 d–元编码，以及在高维基下进行测量，都需要更复杂的光学设备和探测 [86]。近期采用 $d = 4$和 $d = 8$的方案表明，基于量子位的多方量子密钥协商能够显著提高原始密钥率，使其优于量子比特基线，但也凸显了从两能级系统迈向更高维度所需付出的工程代价 [87]。目前，这类方案最适合在专用平台上实现较小维度的系统，但它们为构建更高容量的多方量子网络指明了清晰的发展方向。

C. 连续变量（*CV*）资源

连续变量方案利用光的场正交分量而非离散能级来实现多方量子密钥协商 [88]。参与方通过光纤发送相干态 $|\alpha\rangle$，并进行零差或外差测量，以获取相关的实数结果，随后将其离散化并处理为密钥比特。这种方法可重复利用标准电信硬件——激光器、调制器、平衡探测器——并能与经典流量共存；连续变量量子密钥分发已在经典信道上实现超过 $100\ km$ 的传输 [89]。理论密钥率可表示为

$$r_{CV} \approx \log(1 + S/N) - \chi(E : AB)$$

其中第一项刻画信噪比，第二项则对窃听者所获信息给出上界。离散调制连续变量协议与有限规模安全性分析的最新进展缩小了理论与实践之间的差距 [90]。将这些工具扩展到多方量子密钥协商，意味着设计多方调制、筛选与协调规则，在利用连续变量信道高带宽与长距离优势的同时保持公平性。

D. 双场多方量子密钥协商

双场量子密码学依赖于中心测量站的单光子干涉，而非端到端直接传输 [91]。每个参与方都向一个中间节点发送带有相位编码的弱相干脉冲；当来自不同用户的脉冲发生干涉时，探测统计取决于全局相位组合： $e^{i(\phi_1+\ldots+\phi_n)}$。将这一思路应用于多方量子密钥协商后，最终密钥便能对称地取决于所有用户的相位 [9], , 同时保留使双场量子密钥协商颇具吸引力的距离标度优势。

其主要优势在于能够延长距离：秘密密钥率随信道透射率的平方根变化，而非呈线性变化；与直接传输方案相比，安全距离上限实际上可延长约一倍 [92]。与此同时，双场多方量子密钥协商也带来了新的挑战，例如处理多个参与方产生的多光子事件、公平地加权所有贡献，以及确保中心站作为不可信中继的安全性 [9]。早期框架 [93]证明了该方案对于三至四名用户的小规模群组具有可行性，但在扩展至更大规模 n的同时保持强公平性，仍是一个有待解决的关键问题。

E. 混合资源

混合与新兴资源族旨在结合不同纠缠结构与纠错编码的优势。一个方向是融合GHZ与W态 [94]，其中GHZ资源支持强多方奇偶校验测试与公平性检查，而W态对损耗和噪声具有更好的鲁棒性。通过在不同协议阶段切换这些资源，或利用局部补操作将一种转换为另一种，多方量子密钥协商方案可使其物理层适应当前信道条件与安全性需求。

一条更具前瞻性的研究方向探索玻色量子纠错码，例如GKP与猫态编码 [95]。这些编码将逻辑量子比特编码到连续变量模式中，并在硬件层面纠正小的位移误差，从而在物理噪声到达协议逻辑之前消除其中大部分。早期实验 [96, 97] 已在超导与腔平台上验证玻色编码达到或接近盈亏平衡点，表明在此类编码量子比特上实现逻辑层多方量子密钥协商或可在下一代硬件中成为可行。

VI. 安全模型

安全模型的选择决定了必须明确应对哪些对手能力，以及哪些能力可以忽略或交由硬件假设处理。本节探讨与多方量子密钥协商相关的四种安全模型，即依赖设备、测量设备无关、半量子和设备无关多方量子密钥协商。表 V 总结了这四种模型之间的主要权衡，重点介绍其信任假设、处理公平性和侧信道的方式，以及各自的实用性和开销。

A. 设备相关多方量子密钥协商

在依赖设备的多方量子密钥协商中，安全性分析以理想化假设为起点：所有用户硬件，包括光源、调制器和探测器，均按规格运行，且不受对手控制 [98]。在此模型下，主要的不确定性来自信道噪声和蓄意窃听，两者都可以通过标准的信息论分析加以刻画，其方法与量子密钥分发中使用的方法非常相似 [99]。首先，根据测试轮次估算出的观测量子比特误码率，与外部对手对原始密钥所掌握信息的上界相关联，

资源类型	描述	影响
贝尔态	最大双量子比特纠缠的态。	保真度高，且可直接用于量子安全性证明。适合小型群组。
GHZ态	真正的多体纠缠量子态。	密钥分发中的强关联，但易受损耗影响；适用于实际应用适用于小型至中型群体。
W态	损耗后仍能保持纠缠的稳健多体态损耗后的纠缠。	损耗下性能平稳退化；更适用于噪声信道。适合更大的群体。
Dicke 态	具有固定激发数的量子态，分布于量子比特。	以部分理想关联换取鲁棒性；可针对性能进行适配在各种网络中。
簇态	图态提供模块化纠-缠。	适用于基于测量的协议，但在生成方面面临挑战和动态测量方面。
连续变量	使用字段正交分量（例如，高斯态）。	信息容量高；可与经典流量共存，但实现起来更复杂。
高维态	量子比特（d能级系统）编码更多信息。	可实现更高的密钥率，但需要复杂的技术；前景看好，有望用于未来的协议。
双场资源	依赖单光子干涉的协议。	有效扩展安全距离，但在公平性方面带来挑战和扩展性。
混合资源	结合各种量子re-光源（例如 GHZ/W态）。	兼顾不同量子态的优势；增强鲁棒性和协议设计的适应能力。

表 IV MQKA协议中的资源汇总

随后应用隐私放大，将原始密钥压缩为更短的秘密密钥，使对手掌握的信息可以忽略不计。公平性和抗合谋性是多方量子密钥协商特有的性质，通常会单独进行处理：在所有设备均遵循协议描述的前提下，论证编码规则和验证步骤能够防止任何真子集的参与者以超过可忽略优势的程度操纵或预测最终密钥 [22]。

这种设备依赖视角的主要优势在于，它使证明与实现相对简单，因为可以直接复用成熟的量子密钥分发技术，以及针对单光子和多光子攻击、信道损耗和噪声的模型 [27]。它也与当前实验平台高度契合：光源和探测器由运行协议的同一操作者构建并校准，因此至少在受控实验室环境中，硬件按预期工作是合理的。因此，许多现有多方量子密钥协商方案隐式采用该模型，将分析重点放在公平性的组合与博弈论方面，同时将底层量子层视为行为良好的黑箱 [23, 71, 84, 14]。

然而，这种简化使多方量子密钥协商容易受到实现层面漏洞的影响。在实践中，探测器存在侧信道，例如计时、强度或波长依赖性；光源也可能因不完美隔离或失准而泄露信息，而这些问题都未被理想设备模型所涵盖 [100]。安全性证明往往流于临时拼凑，将一般的信息论界与针对特定协议的推理相结合，以判断真实硬件可能或不可能泄露哪些信息，因此难以比较不同方案的安全性强弱，也难以推理其与高层应用的组合方式。对于多方量子密钥协商而言，内部威胁和串谋本就十分复杂，这些未经控制的设备假设又增添了一层不确定性，因此促使人们转向信任程度更低的安全模型 [85]。

B. 测量设备无关多方量子密钥协商

测量设备无关多方量子密钥协商（MDI-MQKA）旨在直接应对探测器长期以来的脆弱性；探测器一直是已部署量子密钥分发系统遭受成功攻击的主要途径之一 [54, 101]。在这一范式中，所有测量设备都被移至一个明确指定、且可能由对手控制的中继节点，用户实验室中只有态制备单元被假定为诚实且可得到合理建模。每位参与者制备量子态——通常是利用偏振、相位或时间箱自由度编码的单光子——并将其发送至中继节点；中继节点执行联合测量，例如GHZ型投影，并广播经典测量结果。随后，用户对满足特定关联约束的联合测量结果进行后选择，以确定原始密钥比特，从而确保仅保留所有诚实方的贡献均相干参与的事件。

从安全性角度来看，该模型有两项关键优势。首先，由于中继被视为不可信，只要观测统计量仍处于预期安全区域内，探测阶段的任何操纵或泄漏都会自动归咎于对手，而不能直接危及密钥。因此，探测器侧信道、时序攻击和校准问题成为威胁模型的一部分，而非假设，与设备相关方案相比大幅增强了稳健性 [46, 61, 100]。其次，公平性可以直接编码进后选择规则：仅使用对称依赖于所有参与者输入的测量结果，从而将各方对密钥的影响与可测量的关联模式联系起来，而不是依赖于某一特定探测器被假定的诚实性。这种对称性在多方GHZ设计中尤为自然，其中接受事件对应于特定的多光子符合，而这些符合不能仅归因于任何单一方的态。

在实验方面，测量设备无关多方量子密钥协商采用与测量设备无关会议密钥协商相同的光学基础设施 [100], ，因此可受益于近期利用线性光学、贝尔态分析仪和单光子

光源的演示成果 [54]。主要的额外挑战是确保在存在不完美干涉、损耗和有限尺寸效应时，公平性约束仍然得到满足，从而避免涉及中继和部分用户的串谋在无人察觉的情况下左右最终密钥。尽管如此，随着量子网络向配备中心测量节点的辐射式架构演进，测量设备无关多方量子密钥协商似乎尤其契合这类架构：它将网络核心中最脆弱的硬件视为不可信基础设施，并仅在用户端保留相对简单且特性更明确的制备设备 [100]。

C. 设备无关多方量子密钥协商

完全设备无关的多方量子密钥协商（DI-MQKA）代表了安全模型谱系中最具雄心的方向，其目标是设计这样的协议：其保密性和公平性保证仅依赖于观测到的非局域关联（例如贝尔不等式违背），而不依赖于对光源或探测器内部工作机制的任何详细假设 [102]。在这一设想中，每位用户的实验室都被视为一个黑箱，接收经典输入并返回经典输出；量子行为的唯一证据来自网络中这些输出的联合统计。如果这些统计以足够大的幅度违背适当的多方贝尔不等式，那么原则上就能界定对手可获取的信息，并证明任何联盟——包括控制设备本身的联盟——都无法既通过测试，又显著地操纵或预测最终密钥。将这一思路从双体量子密钥分发扩展到多方密钥协商，在概念上颇具吸引力，但在技术上颇具挑战，因为这要求在对抗性且存在串谋的环境中，将设备无关的保密性与强公平性约束结合起来。

鉴于实现无漏洞多体贝尔测试的实验难度，以及相关安全性证明的复杂性，目前的多方量子密钥协商研究往往聚焦于半设备无关的 [103, 104, 105] 方案，在不追求完全设备无关的前提下放宽部分假设。例如，某些模型假设光源可信而探测器不可信；另一些则属于“单态”场景，即仅对制备态作出非常粗略的假设，而测量设备仍不作表征 [100]。这些中间方案旨在保留设备无关方案的大部分鲁棒性，尤其是抵御探测器攻击的能力，同时避免严格设备无关实现所需的全部实验开销。它们也与设备无关和测量设备无关会议密钥协商中已探索的架构自然契合；在这些架构中，多体图态或 GHZ 态已被用于在现实光子实验装置中展示安全密钥建立。

将这些进展转化为真正的MQKA协议，需要在保密性之上增加额外结构 [46, 100]。该协议不仅必须保证外部对手对密钥几乎一无所知，还必须保证任何内部联盟都无法将其行为与设备的隐藏行为相关联，从而在仍能复现所需非局域关联的同时，使密钥分发偏向于自身。这设备假设、非局域性与博弈论公平性的交织，使设备无关多方量子密钥协商成为一个开放且具有挑战性的研究前沿 [102]。尽管如此，其发展轨迹是清晰的：随着多体贝尔测试以及设备无关或测量设备无关会议密钥协商的实验技术日趋成熟，它们为构建信任要求越来越低、可组合性更强的MQKA安全模型提供了具体基础，从而在不放弃将多方公平性作为核心设计目标的前提下，逐步降低对理想化硬件假设的依赖。

D. 半量子多方量子密钥协商

半量子多方量子密钥协商通过放宽所有参与者都必须具备完整量子能力这一要求，采用了另一条通往实际部署的路径 [62, 57]。在这类协议中，网络明确具有异构性：部分“量子”用户能够制备、操控和测量量子态，而“经典”用户则只能执行非常有限的操作，例如反射收到的量子比特、应用固定的经典门，或执行随机置换；他们无法制备或测量叠加态 [62]。一种典型构造是：具备量子能力的参与方生成纠缠态，并将子系统发送给经典参与方；后者执行规定的确定性或随机变换，再将系统送回。随后，量子参与方进行最终测量和密钥筛选。该方案旨在确保经典用户尽管量子工具有限，仍能在逻辑上参与最终密钥的生成，并享有与完全量子场景相当的公平性保证 [106]。

半量子多方量子密钥协商的主要动机，是适应现实部署场景：只有一部分节点（例如数据中心或专用网关）能够承载先进的量子硬件，而许多终端用户则在资源受限的设备上运行。通过允许经典参与方仅使用简单、稳健的操作参与密钥协商，这些协议有望降低采用门槛，并使多方量子密码学与现有网络边缘设备兼容 [84]。与此同时，它们必须仔细刻画串通的经典用户能够做什么、不能做什么，因为即便是有限的操作，在与具备量子能力的对手协同下，也可能对量子态进行非平凡的操纵。因此，安全性证明往往更为复杂，因为它们必须对经典参与方受限的对抗行为、其与量子盟友的交互，以及对保密性和公平性的相应影响进行建模 [57]。

在实际应用中，半量子多方量子密钥协商往往需要在密钥率和噪声容忍度方面作出取舍，以降低硬件要求 [62]。由于经典用户无法执行完整的量子测量，可能需要更多轮次以及额外的诱骗或验证步骤来检测窃听和偏离协议的行为，因此与全量子设计相比，效率会有所降低。尽管如此，近期研究 [107,62]已表明，可以构造这样的半量子多方量子密钥协商协议：即使参与者从未执行过任何一次量子测量，仍然能够安全地为共享密钥作出贡献

，前提是对共谋结构作出明确假设。这一研究方向表明，半量子模型将在理想化的多方量子密码学与大规模异构量子—经典网络的限制之间发挥重要的桥接作用。

VII. 公平性与串谋

公平性对于维护参与者之间的诚信与信任至关重要，可确保任何一方都无法通过策略性操纵获得不正当优势。我们探讨如何运用博弈论原理来构建公平性，并着重说明在协议中进行明确设计如何提升安全性。我们还分析了不同协议拓扑所引发的共谋模式，揭示这些模式如何影响不诚实联盟的成功概率，以及能够减轻其影响的防御措施。最后，我们讨论实现信息论公平性与应对潜在串谋现实之间固有的权衡，并强调在 MQKA 的实际实现中，效率与安全性之间需要谨慎平衡。这些要素共同凸显了周密协议设计对于促进公平、安全的量子通信的重要性。

在博弈论框架下，可以严谨地刻画多方量子密钥协商中的公平性：每位参与者既是博弈者，也可能成为对手。协议将博弈定义为：偏离诚实操作不应使任何联盟的预期优势超出可忽略的范围 [40]。若协议满足以下条件，则可实现强公平性：

1) 任何真子集都无法将特定密钥的实现概率提高到超过均匀分布概率可忽略的优势：对于任意联盟 $S \subset \{P_1, P_2, ..., P_n\}$ 和任意密钥值 K'，

$$Pr(\text{final key} = K'|S'\text{action}) \leq \frac{1}{2^n} + negl(n)$$

2) 任何参与者都无法通过选择性学习或中止来获取优势。这意味着，任何博弈者都不能通过策略性测量或中止，在其他参与者之前获知最终密钥；也不能根据密钥值选择性泄露信息，或强制协议失败以操纵结果。

将公平性直接融入关键组件，可增强协议的安全性与完整性。首先，应合理设计编码规则，使特定操纵在物理上与噪声无法区分，从而确保传输信息的安全。其次，筛选程序必须采用随机选择方法，防止参与者进行任何策略性操纵，进而确保密钥协商过程的结果公平 [41]。此外，应建立验证协议，以较高概率有效检测偏离预期行为的情况，从而提高系统的整体可靠性。近期进展还引入了混合验证方案，利用多项式承诺方案进一步强化公平性证明，并为多方量子密钥协商提供额外的安全保障 [22, 41]。这种全面的方法不仅保障了整个过程，也促进了参与者之间的信任。

多方量子密钥协商中的共谋策略和成功概率会受到协议拓扑和资源选择 [85]的显著影响。在基于环形结构的共谋模式中，朴素环形协议中的线性可预测性可能使后续参与者占据优势。例如，处于位置 $N-1$ 的参与者可以测量部分结果，以预测先前的贡献。此外，处于位置 $N-1$ 和 N 的参与者若进行合作，就能抵消或翻转先前的编码。这种可预测性也延伸至测量基选择；不诚实参与方可以利用这一点，预先得知将要测试哪些测量基。

为应对这些漏洞，可以采用多种防御机制。非线性后处理可以破坏串谋者利用的线性性 [43],，而使用诱骗态可以随机打乱测试态的插入方式 [108, 109],，从而阻止其策略性地选择测量基。此外，通过随机排列持续随机化参与者的顺序，可以消除任何固定的位置优势 [110], ，进而增强协议完整性。

在客户端-服务器合谋模式中，星型拓扑因中心节点集中化而面临独特挑战。功能强大的枢纽能够关联制备基与测量基，从而可能导致密钥推断或偏差。不诚实客户端可能与枢纽合作，强行设定预定结果，因此公平性测试必须验证所有参与者的贡献都得到对等体现。有趣的是，与诚实枢纽互动的客户端联盟受到更严格的限制，因为它们无法通过量子信道直接通信，任何操纵都需要枢纽配合。如果枢纽的测量基确实随机且不为他方所知，那么在这种情形下，公平性可能自然实现。近期研究系统地分类了合谋策略，并提出了相应的反合谋设计原则 [22, 32, 43,85]。这些原则包括打破对称性，确保任何两方联盟无论处于何种位置都无法得逞；将验证分散到所有参与者，以防止任何一方单独控制结果；以及在物理层嵌入随机性，以挫败确定性合谋策略。

在多方量子密钥协商中，信息论公平性与可能发生的不受限制的（N –1）–方串谋之间存在根本性的权衡。在维持 O（N）量子信道的同时确保公平性，似乎从根本上颇具挑战性 [22]。为防止 $N-1$ 不诚实参与方强行确定密钥，其余诚实参与方必须提供串谋者未知的信息。然而，在 O（N）信道拓扑中——例如环形、树形或星形拓扑——这名诚实参与方的通信路径不可避免地会经过串谋参与方。这种连接为串谋者提供了可利用的信息泄露途径。解决这一难题的可能方案包括将量子信道数量增加到 O（N^2），以实现完美公平性，但代价是效率降低 [32]。或者，我们可以将串谋限制在 t–方场景中，其中 $t < N-1$，从而在采用 O（N）信道的情况下实现渐近公平性。另一种方案是引入可信第三方 [11, 54], ，尽管这有悖于多方量子密钥协商的初衷

方面	依赖设备	MDI	设备无关	半量子
信任假设	光源 + 探测器可信；仅信道是对抗性的。	光源可信；中继/测量不可信。	被视为黑箱的设备；安全性来自观测到的关联。	《量子》参与方完全量子；经典参与方受到严格限制。
主要目标	复用 QKD式证明；add MQKA 公平性/共谋分析。	移除探测器 side 信道；在后选择中实现公平性在后选择中。	安全性 + 即使在公平性面对恶意设备时也能得到保障。	支持异构网-络与经典参与-参与者。
覆盖充分	信道攻击；内部逻辑方的不当行为。	探测器攻击；中继的不当行为；信道攻击。	任意设备篡改与测试统计量相符。	串谋 with 受限经典的操作。
通过.....处理公平性	编码规则 + 经典诚实设备下的校验。	对称 GHZ 类 ac-中继处接-	非局域博弈结构限制联盟偏差。	使.....的协议结构经典操作具有对称影响力。
对缺陷的鲁棒性	低（设备侧信道存在问题）。	中等偏高（探测器不可信；光源至关重要）。	理论上较高；实验上要求很高。	中等（量子节点是信任锚）。
成熟度	最成熟	经实验已验证	主要为理论研究	早期阶段
开销	最低开销	额外的后选择损耗	高开销	更多轮次/检查

表 V
多方量子密钥协商安全模型比较

同时实现 $O(N)$ 效率。最后，结合量子与经典博弈论强制机制的混合方法或许能提供一种可行的解决方案。

VIII. 迈向实用化多方量子密钥协商

尽管测量量子密钥协商（多方量子密钥协商，MQKA）的实际实现极为困难，近期研究已在克服基础性挑战方面取得显著进展 [9, 45]。这些进展有赖于开发创新协议、提高抗噪能力，并确保与经典系统成功集成。随着该领域迈向实用化量子网络，对有效性能指标、稳健设计和无缝互操作性的需求变得至关重要。这为全面评估多方量子密钥协商不断演进的格局及其在促进安全量子通信方面的作用奠定了基础。

A. 超越密钥率的性能指标

要现实地评估多方量子密钥协商，就需要采用超越传统渐近密钥率的指标。一个关键指标是量子比特效率，定义为每个最终密钥比特所消耗的量子比特数 [111]。在此背景下，不同协议的效率各异：环形协议每比特使用 1 个量子比特 [14]，树形协议每比特需要 $\log(n)$ 个量子比特 [60],而完全图每比特需要 n个量子比特 [61]。

另一个重要指标是噪声和损耗阈值，它们表示特定硬件实现所能容忍的最大错误率。例如，GHZ协议可以容忍低于 1% 的比特翻转错误率 [58, 72],，而 W态协议能够应对 2% 至 3% 的错误率‘[45, 72]。连续变量（CV）协议的阈值在某些工作区间内可超过 10% [112], ，具体取决于存在的高斯噪声。

此外，轮次复杂度——即生成每个密钥比特所需的通信轮数——也发挥着重要作用，尤其是在延迟敏感型应用中。环形协议通常需要 $O(N)$ 轮，而树形协议只需 $\log(n)$ 轮，如表 IV 所述。此外，经典通信开销包括为生成量子安全密钥而通过经典方式交换的比特，其中包括身份认证、基底公布和窃听检测等任务，从而产生了相当大的开销。

最后，同步要求也至关重要，尤其是在多跳网络中。环形协议需要严格的时序协调，而星形协议对异步的容忍度更高。不同协议的实现复杂度也各不相同，涉及多个因素：态制备的难度（如 GHZ态、W态和图态之间的差异）、量子存储器需求（直接方案无需量子存储器，而基于中继器的方案则需要大量量子存储器）、每位参与者所需的量子门数量，以及测量装置的复杂程度。评估多方量子密钥协商协议的实用性和效率时，这些因素都至关重要。

B. 抗噪设计与抗错误编码

噪声必须从多方量子密钥协商系统设计之初就作为首要设计约束加以对待，而不能当作事后补救。基于W态的协议通过显式建模现实中的不完美因素来体现这一原则，从而确保在损耗条件下实现优雅降级 [45]。例如，在单光子损失的情况下，协议仍可借助$(N-1)$–粒子W态继续运行。在涉及多粒子损耗的场景中，渐近密钥率会平缓下降，而非灾难性崩溃，通常可容忍10%至20%的损耗而不中止协议。就噪声容忍度而言，基于W态的协议能够承受2%至3%的退极化噪声率，而密钥率不会显著降低。此外，与GHZ协议相比，它们对由振幅阻尼引起的光子损失表现出更强的鲁棒性。

为增强多方量子密钥协商的能力，研究人员提出了结合离散变量与连续变量的混合方法。该策略旨在发挥两种范式各自的优势：离散变量具有强大的安全性证明，且易于验证量子态；连续变量则具有较高的信息容量，并支持更长的传输距离。一种提出的架构是在连续变量中采用相位编码来传递信息

[88], 类似于双场方法 [9],，同时采用离散变量窃听检查。

玻色量子纠错的最新进展为增强多方量子密钥协商协议 [100, 102, 95] 带来了令人振奋的机遇。GKP码在连续变量谐振子模中编码一个逻辑量子比特，并可自动纠正微小的相空间位移 [102]。这种纠错能够同时防护比特翻转错误和相位翻转错误，而且只需一个物理模即可编码一个逻辑量子比特；相比之下，表面码则需要约 1，000 个物理量子比特。值得注意的是，纠错可以持续运行，无需暂停协议。通过完全在逻辑量子比特层面进行密钥生成，光子损失和相位退相干等物理噪声可由纠错层吸收，使协议能够在无噪声逻辑量子比特上有效运行。这种方法的优势包括大幅提升噪声容忍度、通过为每个逻辑量子比特使用单个物理模实现可扩展性，以及与容错量子计算架构兼容。近期规划显示，采用当前超导腔技术的原型演示有望于 2025年 至 2026年 间实现，并预计到 2027 年将其全面整合进 MQKA协议 2030 [113]。

C. 网络集成与量子互联网互操作性

多方量子密钥协商最终必须与多域量子网络中的经典认证、密钥管理和路由层集成。这种集成对于确保在多样化量子环境中的通信安全高效至关重要 [60]。为促进这一集成，必须满足若干网络原生要求。

首先，由于不同的网络角色需要量身定制的设计，因此有必要制定标准化的多方量子密钥协商变体。对于需要长距离、低频传输的骨干链路，双场或基于连续变量的多方量子密钥协商更为适宜。相比之下，适用于短距离、高频通信的簇内密钥则受益于离散变量多方量子密钥协商，因为它具有高吞吐量。

其次，亟需实现路由集成，尤其是在必须支持多方纠缠分发的量子中继网络中。这需要调整生成树算法 [60] ，使其适用于量子原生系统。密钥调度也是一个关键方面，因为必须有效管理重叠参与者组之间多个同时进行的多方量子密钥协商会话。协议调度器必须在管理资源竞争的同时防止密钥重用攻击。异构设备支持也至关重要，因为单个量子网络可能包含多种量子技术。因此，选择多方量子密钥协商协议时，必须考虑可用设备的能力，以确保兼容性。

诸如软件定义量子网络（SDQNs） [114, 115] 等新兴概念，进一步提升了动态集成的潜力。在SDQNs中，控制平面会根据多种因素动态选择合适的MQKA协议，包括当前的网络拓扑、可用的量子资源、参与者需求（如延迟、安全级别和公平性模型），以及历史性能指标。然而，实现这一愿景面临着重大挑战，需要快速、自动地合成MQKA协议；目前这尚不可行，但无疑是未来研究的一个令人振奋的方向。这一演进对于构建高效、可扩展且能够适应不同条件和需求的量子网络至关重要。

IX. 未解决问题

A. 可组合安全框架

MQKA 面临的一项重要未解决问题，是建立严谨的安全基础，使其能够与现代量子密钥分发（QKD）相媲美。这需要开发可组合安全框架，以有效涵盖公平性以及参与方串通带来的挑战 [61, 54]。目前，大多数针对 MQKA协议的安全性证明都是孤立进行的，因此难以获得可组合性保证；而这对于将 MQKA 密钥安全地集成到更大型的密码系统中至关重要。

为解决这一问题，研究工作应着重于将经典密码学中的可组合安全框架应用于多方量子场景。具体而言，采用 IITM 框架（内部参数化迭代任务机） [116]，将 MQKA 形式化为资源供给任务，是一条很有前景的探索方向。此外，利用通用组合定理 [117]有助于证明多方量子密钥协商资源的实现是安全的，确保它们能够与使用所生成密钥的任意协议安全地组合。解决这一未解决问题，对于增强 MQKA 的安全保障并推动其在复杂密码系统中的实际应用至关重要。

B. 超越 $O(N)$ 信道的信息论公平性

多方量子密钥协商中另一个引人关注的开放问题是：在存在任意（$N-1$）–方串谋的情况下，环形或其他 $O(N)$ 拓扑协议能否实现信息论公平性。近期证据表明，这可能存在基本极限，因为设计能够确保强公平性的（$O(N)$ 协议，往往面临两项重大挑战 [40]。首先，此类协议可能无意中依赖无法检测的信任假设，从而损害其鲁棒性。其次，此类协议可能需要牺牲密钥率，导致性能不佳。

为解决这一问题，可以采取若干研究思路：

1）信息论下界：证明公平性、 $O(N)$ 信道与诚实多数假设相结合会导致内在矛盾，这有助于阐明可行协议设计的局限。2）混合经典—量子机制：探索量子协议与经典博弈论机制（如保证金和声誉系统）的结合，可为通过经济手段确保参与者诚实提供一种途径。

3）近似公平性框架：开发近似公平性框架，使参与者获得的收益低于 2^{-2}，有助于刻画可实现的安全性—效率前沿，并为设计更具韧性的协议提供参考。

通过研究这些途径，研究人员可以更深入地理解其中涉及的权衡，并找出突破 $O(N)$ 信道拓扑限制、提升多方量子密钥协商系统公平性的途径。

C. 混合资源

系统地研究混合多体资源（例如 GHZ 态、W态与其他较不常见的纠缠态之间的组合或插值），是提升多方量子密钥协商在现实实验条件下性能的一条有前景的方向。超越理想化的纯 GHZ 或纯W范式，或许能够发现一些态族，它们在纠缠深度、抗损耗与退相干的鲁棒性以及生成难易度之间实现了权衡，因此更适用于特定的网络拓扑结构或噪声模型。若干候选资源类别值得重点研究。排列成二维或三维晶格的簇态不仅具有高度的多体纠缠，还具备内嵌的图结构优势，可用于路由、误差缓解或基于测量的基本操作 [83]。连续变量压缩态 [112, 118]为多体关联提供了另一种编码方式；其抗噪性在很大程度上取决于压缩程度和实验缺陷，因此在容易获得光学压缩的平台上可能更具优势。光子图态 [119] 和时隙复用的 [120] 资源支持基于测量的量子信息处理；将这些构造应用于MQKA协议——包括开发可扩展的生成与分发技术——仍是一个有待解决的工程与理论问题。更普遍地说，若能建立一套系统方案，依据性能指标（密钥率、损耗下的保真度、设备缺陷阈值）对混合态进行分类，并将不同态族与硬件能力相对应，将有助于找出在实际多方量子密钥协商场景中优于简单 GHZ 或 W态方案的近期可用资源。

D. 用于多方量子密钥协商的 *Dicke* 态

设计并分析基于Dicke态的多方量子密钥协商协议，使其达到与当今基于GHZ态和基于Bell态的方案相当的安全性和公平性保证，自然成为一项明确的开放问题。尽管GHZ态、W态、贝尔态和簇态均已应用于具体的多方量子密钥协商协议构造中，但迄今为止，Dicke态主要被视为具有鲁棒多体纠缠的有前景网络资源，而非密钥协商协议的核心基元。Dicke态介于GHZ态和W态的特性之间，可调节激发数量，并且已在中小规模系统中经实验验证具有抵抗损耗和退相干的鲁棒性 [75]。然而，人们尚未系统地理解这些特性如何转化为多方量子密钥协商特定目标例如在串谋情况下实现强公平性、量子比特效率，以及在不同网络架构下获得切实可行的密钥率。

一个具体的研究方向是构建以多体 Dicke 态（$|D_n^k\rangle$）为基本纠缠资源的客户端–服务器或混合多方量子密钥协商协议，并在本综述所确定的三个维度上刻画其性能：网络架构、量子资源和安全模型。在架构维度上，可以考察 Dicke 态在星形、树或混合拓扑结构中的表现，并与已在这些场景中部署的 GHZ 和 W态资源进行比较 1.3。在资源维度上，目标是将密钥率、噪声和损耗阈值以及抗合谋性量化为 (n, k) 的函数，从而可能揭示 Dicke 态在鲁棒性–公平性权衡上严格优于 GHZ 或 W态的参数区间。在安全模型维度上，人们希望开展依赖设备、测量设备无关以及最终半设备无关的分析，将针对 Dicke 态的关联检验纳入公平性定义和可组合安全框架。总体而言，将 Dicke 态确立为一等的多方量子密钥协商资源——配以定制的编码规则、参数估计策略和公平性证明——仍是一个开放问题，它有望显著扩展现实量子网络中公平感知多方量子密钥协商的工具集。

E. 玻色编码与量子纠错

将玻色编码和量子纠错融入多方量子密钥协商协议，是大幅提升其在真实设备中鲁棒性的最有前景的途径之一。一种自然的范式是将多方量子密钥协商操作提升至逻辑量子比特层级：通过玻色编码对物理模进行编码，并在受逻辑保护的量子态上执行整个协议。在离子阱或腔量子电动力学平台上，GKP（Gottesman–Kitaev–Preskill）编码能够抵御小幅位移误差，并有助于实现连续变量模式的高保真度逻辑操作 [121]；因此，在 GKP 逻辑层级实施多方量子密钥协商，有望减少分发和处理过程中的误差传播。在超导平台上，猫态编码和二项式编码因能够针对主要误差通道提供经专门设计的保护而颇具吸引力 [122], ，还有望实现寿命更长的共享资源，或节点间更可靠的纠缠操作。另一种强有力的方法是级联：在更高层级的拓扑码（如表面码） [123] 之下叠加玻色编码，在有利条件下可显著提高有效阈值，并随着级联深度增加而指数级抑制逻辑错误率。尽管仍面临实际挑战——包括容错逻辑操作、适用于分布式协议的综合征提取，以及连续变量稳定化所需的资源开销——但结合玻色保护与传统量子纠错技术，为实现能够抵御主流硬件平台主要噪声过程的多方量子密钥协商提供了明确路径。

F. 设备无关多方量子密钥协商

完全设备无关多方量子密钥协商（DI-MQKA）的概念代表着一个理论上严谨的目标，旨在仅基于观测到的

非局域关联来确保安全性和公平性。然而，由于当前存在重大的实验和概念障碍，阻碍了该理想模型的实际实现，因此实现这一模型仍只是一个愿景。

在迈向更现实的设备无关方案方面已取得进展。一条有前景的路径是半设备无关多方量子密钥协商，其中光源受到信任，但测量过程则不受信任 [124]。伪心灵感应奇偶博弈技术的最新进展在这一领域展现出前景，使得在测量设备未完全受信任的情况下仍能获得一定程度的安全性。

此外，改造设备无关量子会议密钥协商（DI-QCKA）实验的努力凸显了宝贵的进展机遇。测量设备无关量子会议密钥协商的最新实验演示，尤其是使用光子图态的演示 [46, 100], , 为多方量子密钥协商提供了天然的试验平台。这些实验为在设备无关框架下探索多方量子密钥协商的能力与局限铺平了道路。

最后，无漏洞贝尔检验的出现为设备无关协议提供了坚实基础。近期通过无漏洞演示违反贝尔不等式的成果——同时采用光子系统与离子系统——强化了可支撑设备无关多方量子密钥协商的基本原理，为量子密钥协商系统未来的研究与发展提供了一条充满前景的途径。

G. 新兴应用

在密码学领域，多方量子密钥协商密钥可有效用于（t, n）门限方案，其中需要 t 份额才能恢复密钥。这引出了一个值得探讨的问题：量子力学能否提升这些门限方案的安全性？研究这一潜在交叉领域，或可推动密码学实践取得重大进展，利用量子系统的独特属性来增强安全保障。

多方量子密钥协商技术的应用不止于密钥协商，还可扩展至更广泛的多方量子协议，例如量子隐私比较。多方量子密钥协商所蕴含的公平性和抗合谋性原则，同样适用于这些协议，从而增强其安全性和功能。此种关联凸显了多方量子密钥协商方法的多样性，有助于拓展量子通信应用的范围。

另一个颇具前景的应用领域，是将多方量子密钥协商与区块链技术相结合，构建混合经典—量子账本。在此背景下，量子密钥可提供共识抗性认证，显著增强账本内交易的安全性和合法性。实施公平感知多方量子密钥协商，对于确保分布式量子账本系统的有效性至关重要，因为用户之间的公平参与和信任是其关键所在。

X. 结论

本文重点阐述了多方量子密钥协商在现代主要应用中的重要作用。我们从三个紧密关联的维度——网络架构、量子资源和安全模型——梳理文献，指出理解多方量子密钥协商的最佳方式，是将其视为一个由相互作用的选择构成的设计空间，而非一系列彼此孤立的协议。这一视角清晰揭示了拓扑（环形、星形、树形、完全、混合）、纠缠结构（贝尔、GHZ、W态、高维、连续变量、双场、玻色编码）以及设备假设如何共同决定公平性、抗合谋性和噪声鲁棒性。

从安全性角度来看，公平性和抗合谋性是多方量子密钥协商区别于量子密钥分发和量子会议密钥协商的核心挑战。环形方案提供了量子比特高效路由，但在编码操作和经典后处理未能明确打破线性性的情况下，容易受到位置串通的结构性攻击。树形和星形架构在可扩展性或现实客户端–服务器环境中的可实现性方面更具优势，但会形成必须通过测量设备无关和半设备无关技术谨慎管控或缓解的中心影响点。混合架构，例如由共同参与者共享的双环，或采用 W态的星形–环形布局，展示了如何通过结合不同拓扑结构与资源，更均衡地分配权力，同时提升有损链路上的噪声容忍度。

在物理层面，我们的分析表明，量子资源的选择并非无关紧要，而是从根本上决定了性能和鲁棒性。GHZ态和簇态能够产生强大的多体关联，但在损耗下会急剧退化；相比之下，W态、连续变量方案或双场方案在现实信道中仍能维持有用的关联，这表明未来的多方量子密钥协商部署将高度依赖这类抗噪资源。对新兴玻色编码（猫态和GKP码）的讨论展现了一种长期愿景：在容错硬件上直接于逻辑层级实现多方量子密钥协商，使密钥协商成为量子处理器和中继器的原生服务。

最后，我们指出了一系列开放问题，它们为多方量子密钥协商确立了具体的未来研究议程，包括能够同时涵盖公平性与内部威胁的可组合安全框架；支持大规模动态群体且不会导致资源开销呈二次方增长的可扩展架构；基于近期多体贝尔实验和会议实验的设备无关或半设备无关多方量子密钥协商；以及以统一方式利用 GHZ、W态、连续变量和玻色编码的混合资源方案。应对这些挑战需要进一步推动量子信息论、密码学、分布式系统和博弈论之间的深度融合，但其潜在收益十分可观：多方量子密钥协商有望成为新兴量子互联网中安全多方计算、量子云服务和量子感知共识的基础构件。

参考文献

[1] Charles H Bennett. “量子密码学：将不确定性用于隐私保护”。载于：《科学》257.5071 (1992)，第 752–753 页。

[2] Charles H Bennett、Gilles Brassard 和 Artur K Ekert。“量子密码学”。载于：科学美国人 267.4 (1992)，第 50–57 页。[3] Stefano Pirandola 等人。“量子密码学的进展”。载于：光学与光子学进展 12.4 (2020)，第 1012–1236 页。[4] Mathieu Bozzio 等人。“超越密钥分发的量子密码学：理论与实验”。载于：现代物理评论97.4 (2025)，第 045006 页。[5] Anne Broadbent 和 Christian Schaffner。“超越量子密钥分发的量子密码学”。载于：设计、编码与密码学78.1 (2016)，第 351–382 页。[6] Gláucia Murta 等人。“量子会议密钥协商：综述”。载于：*Advanced QuantumTechnologies*3.11 (2020)，第 2000025 页。[7] Robert Bedington、Juan Miguel Arrazola 和 Alexander Ling。“卫星量子密钥分发的进展”。载于：*npj*量子信息3.1 (2017)，第 30 页。[8] Emir Dervisevic 等人。“量子密钥分发网络—密钥管理：综述”。载于：*ACM*计算综论57.10 (2025)，第 1–36 页。[9] Venkat Abhignan 和 R Srikanth。“基于双场的多方量子密钥协商”。载于：美国光学学会期刊*B*42.2 (2025)，第 267–279 页。[10] Jiawei Liu 等人。“推进多方量子密钥协商协议：双层方法的优势”。载于：《量子信息处理》23.3 (2024)。[11] Guo-Dong Li 等人。“一种具有身份认证的测量设备无关多方量子密钥协商协议”。载于：《量子信息处理》22.12 (2023)。[12] Bin Liu 等人。“使用单粒子的多方量子密钥协商”。载于：《量子信息处理》12.4 (2013)，第 1797–1805 页。[13] Hao Cao 和 Wenping Ma。“基于量子搜索算法的多方量子密钥协商”。载于：*Scientific Reports*7.1 (2017)，第 45046 页。[14] Song Lin 等人。“多方量子密钥协商”。载于：《物理评论*A*》104.4 (2021)，第 042421 页。[15] D Dhinakaran 等人。“面向云计算中结合量子密钥分发的隐私保护型分布式多方数据外包新方案”。载于：*arXiv* 预印本 *arXiv:2407.18923*(2024)。[16] Abhay Kumar 等人。“面向网络安全应用的量子增强安全多方计算”。载于：智能计算与大数据分析国际会议。施普林格。2024，第 127–145 页。[17] Alexander Pickston 等人。“量子网络中的会议密钥协商”。载于：*npj*量子信息9.1 (2023)，第 82 页。[18] Mrityunjay Singh 和 Dheerendra Mishra。“面向无线传感器网络的后量子安全认证密钥协商协议”。载于：电信系统84.1 (2023)，第 101–113 页。[19] Ranadeep Reddy Palle。《量子区块链：揭示量子密码学在分布式账本中的潜力》。载于：()。[20] Harry WH Wong、Jack PK Ma 和 Sherman SM Chow。《使门限签名的安全多方计算更加高效》。载于：*NDSS*。互联网协会。2024年。[21] Aakar Mathur、Ashish Gupta 和 Sajal K Das。《联邦学习遇上量子计算：综述与研究机会》。载于：*arXiv* 预印本 *arXiv:2504.08814*（2025年）。[22] Zhiwei Sun 等人。《一种能够抵御串谋攻击的新型公平多方量子密钥协商》。载于：科学报告 9.1（2019年），第17177页。[23] Min Hou、Yue Wu 和 Shibin Zhang。《使用 n 粒子 GHZ态的多方量子隐私比较协议》。载于：《数学》13.21 （ 2025 年），第 3422 页。[24] Geoffroy Caillat-Grenier 和 Andrei Romashchenko。《多方密钥协商通信复杂度的谱方法》。载于：*arXiv* 预印本 *arXiv:2305.01355*（2023年）。[25] Harry Buhrman 等人。《多方量子通信复杂度》。载于：《物理评论*A*》60.4（1999年），第2737页。[26] Ibrahim H Ahmed 等人。《通过抽象多智能体交互实现量子安全认证与密钥协商》。载于：实用智能体与多智能体系统国际会议。施普林格。2021年，第14–26页。[27] Ivan B Djordjevic。《量子密钥分发（QKD）基础》。载于：《物理层安全、量子密钥分发与后量子密码学》。施普林格，2025年，第305–362页。[28] Horace P Yuen。《量子密钥分发的安全性》。载于：*IEEE Access* 4（2016年），第724–749页。[29]Youssouf Achouri、Rima Djellab 和 Khaled Hamouid。《量子密钥协商协议概述》。载于：量子科学国际研讨会：应用与挑战。施普林格。2023年，第1–14页。[30] Wen-Jie Liu 等人。《委托量子计算的多方半量子密钥协商》。载于：《国际理论物理学杂志》56.10（2017年），第3164–3174页。[31] Song-Kong Chong 和 Tzonelih Hwang。《基于 BB84 的量子密钥协商协议》。载于：《光学通信》283.6（2010年），第1192–1195页。[32] Ping Wang、Zhiwei Sun 和 Xiaoqiang Sun。《能够抵御串谋攻击的多方量子密钥协商协议》。载于：《量子信息处理》16.7（2017年），第170页。[33] Huan-Huan Li、Li-Hua Gong 和 Nan-Run Zhou。《基于高维单粒子态的新型半量子密钥协商协议》。载于：《中国物理*B*》29.11（2020年），第110304页。[34] Michael Steiner、Gene Tsudik 和 Michael Waidner。《扩展至群组的 Diffie-Hellman 密钥分发

通信》。载于：第*3*届*ACM*计算机与通信安全会议论文集。1996年，第31–37页。[35] Eric Rescorla。*RFC2631*：*Diffie-Hellman* 密钥协商方法。1999年。[36] Paul C Van Oorschot 和 Michael J Wiener。《关于使用短指数的 Diffie-Hellman 密钥协商》。载于：密码技术理论与应用国际会议。施普林格。1996年，第332–343页。[37] Mike Burmester 和 Yvo Desmedt。《安全且可扩展的组密钥交换系统》。载于：《信息处理快报》94.3（2005年），第137–143页。[38] Lein Harn 和 Changlu Lin。《高效的群组 Diffie–Hellman 密钥协商协议》。载于：《计算机与电气工程》40.6（2014年），第1972–1980页。[39] Nicolas Gisin 和 Stefan Wolf。《噪声信道上的量子密码学：量子与经典密钥协商协议》。载于：《物理评论快报》83.20（1999年），第4200页。[40] Kun-Fei Yu 等人。《具有强公平性的量子密钥协商协议设计》。载于：*arXiv* 预印本 *arXiv:1510.02353*（2015年）。[41] Lei Li 和 Zhi Li。《基于重复码的可验证多方量子密钥分发协议》。载于：《信息科学》585（2022年），第232–245页。[42] Li-Zhen Gao 等人。《面向光学环形量子通信网络的认证多方量子密钥协商》。载于：《物理学前沿》10（2022年），第962781页。[43] Bin Liu 等人。《针对“环形”多方量子密钥协商协议的串谋攻击》。载于：《量子信息处理》15.5（2016年），第2113–2124页。[44] Rima Djellab 等人。《一种用于安全多方通信的新型树型量子密钥协商协议》。载于：《电信与信息技术杂志》（2024年），第43–50页。[45] A. Moustapha M. Ndam。《基于 W 态的多方量子密钥协商》。硕士论文。林贝：非洲数学科学研究所（AIMS）喀麦隆，2025年5月。[46] Shuaishuai Liu 等人。《多方量子秘密共享与会议密钥协商的实验演示》。载于：*npj*量子信息 9.1（2023年），第92页。[47] Kai Dong 等人。《基于树型拓扑的量子密钥中继策略：用于安全组播服务》。载于：《光学通信与网络杂志》12.5（2020年），第120–132页。[48] Qiang Zhao、Zhuohua Li 和 John Lui。《基于树型密钥图的动态量子群组密钥协商》。载于：*arXiv* 预印本 *arXiv:2312.04107*（2023年）。[49] Yu-Guang Yang 等人。《针对串谋攻击的树型多方量子密钥协商协议中的信息泄露》。载于：《国际理论物理学杂志》62.7（2023年），第148页。[50] Hua-Lei Yin、Yao Fu 和 Zeng-Bing Chen。《实用量子数字签名》。载于：《物理评论*A*》93.3（2016年），第 032316 页。[51] Daniel Gottesman 和 Isaac Chuang。《量子数字签名》。载于：*arXiv* 预印本 *quant-ph/0105032*（2001年）。[52] Amit Behera、Or Sattath 和 Uriel Shinar。《适用于消息认证码的抗噪量子令牌》。载于：*arXiv* 预印本 *arXiv:2105.05016*（2021年）。[53] Ágnes Villányi。《量子态的经典承诺》。博士论文。麻省理工学院，2024年。[54] Bing-Xin Liu 等人。《测量设备无关多方量子密钥协商》。载于：量子科学与技术前沿2（2023年），第 1182637 页。[55] Hussein Abulkasim、Atefeh Mashatan 和 Shohini Ghose。《抵御串谋攻击的安全多方量子密钥协商》。载于：*ScientificReports* 11.1（2021年），第 9456 页。[56] Jingjing Yang 等人。《无纠缠 MSTSA 结构中的单轮半量子诚实密钥协商方案》。载于：《量子信息处理》20.5（2021年），第 188 页。[57] Wan-li Hong 等人。《基于多粒子纠缠态的多方半量子密钥协商协议》。载于：激光物理快报 21.12（2024年），第 125212 页。[58] Ya-Xi Shu、Chen-Ming Bai 和 Sujuan Zhang。《基于 GHZ 态的多方量子密钥协商》。载于：*EPJ*量子技术12.1（2025年），第 1–24 页。[59] E Dervisevic 等人。《量子密钥分发网络——密钥管理：综述。arXiv 2024》。载于：*arXiv* 预印本 *arXiv:2408.04580*（）。[60] Anton Trushechkin、Hermann Kampermann 和 Dag-marBruß。《量子网络中会议密钥传播的生成树打包协议》。载于：*arXiv* 预印本 *arXiv:2506.04105*（2025年）。[61] Lewis Wooltorton、Peter Brown 和 Roger Colbeck。《标准设备无关会议密钥协商无需真正多方纠缠》。载于：《物理评论快报》135（2025年），第 220803 页。[62] Jing Li、Jiaxin Xiong 和 Xianmin Wang。《无需参与者测量的多方半量子密钥协商协议》。载于：*Physica Scripta* 100.9（2025年），第 095122 页。[63] As’Ad Mahmoud As’Ad Alnaser 等人。《量子网络中多用户安全量子通信》。载于：电气电子工程师学会通信学会开放期刊（2025年）。[64] Adriana Marais、Thomas Konrad 和 Francesco Petruccione。《差分相移量子密钥分发中的安全性与纠缠》。载于：*arXiv* 预印本 *arXiv:1002.0953*（2010年）。[65] Shuntaro Takeda 等人。《离散变量与连续变量之间的纠缠交换》。载于：《物理评论快报》114.10（2015年），第 100501 页。

[66] Ivan B Djordjevic。《离散变量（dv）量子密钥分发》。载于：《物理层安全、量子密钥分发与后量子密码学》。施普林格，2025年，第 363–423 页。[67] Nicolas Gisin 和 Helle Bechmann-Pasquinucci。《n 个量子比特的贝尔不等式、贝尔态和最大纠缠态》。载于：*Physics LettersA* 246.1-2（1998年），第 1–6 页。[68] Denis Sych 和 Gerd Leuchs。《广义贝尔态的一个完全基》。载于：*NewJournal of Physics*11.1（2009年），第 013006 页。[69] Ye-Feng He、Yibo Pang 和 Man Di。《基于贝尔态的相互认证量子密钥协商协议：Y.-F. He 等人》。载于：《量子信息处理》21.8（2022年），第 290 页。[70] Xing-Qiang Zhao 等人。《基于纠缠交换的多方量子密钥协商协议》。载于：《国际理论物理学杂志》58.2（2019年），第 436–450 页。[71] Hang Gao 和 Ri-Gui Zhou。《基于 G 类态和χ+ 态的多方量子密钥协商协议》。载于：《国际理论物理学杂志》61.2（2022年），第 16 页。[72] Ellie D'Hondt 和 Prakash Panangaden。《W态和 GHZ 态的计算能力》。载于：*arXiv* 预印本 *quant-ph/0412177*（2004年）。[73] Pankaj Agrawal 和 Arun Pati。《利用 W态实现完美量子隐形传态和超密编码》。载于：《物理评论*A*——原子、分子与光学物理》74.6（2006年），第 062320 页。[74] Yao-Hsin Chou 等人。《动态群组多方量子密钥协商》。载于：*Scientific Reports*8.1（2018年），第 4633 页。[75] Jeffery Yu 等人。《Dicke 态的高效制备》。载于：《物理评论快报》136.3（2026年），第 030601 页。[76] Bernd Lücke 等人。《检测 Dicke 态的多粒子纠缠》。载于：《物理评论快报》112.15（2014年），第 155304 页。[77] Robert Prevedel 等人。《实验实现多方量子网络所需的多达六量子比特 Dicke 态》。载于：《物理评论快报》103.2（2009年），第 020503 页。[78] Philip Walther。《实验实现多方量子网络所需的多达六量子比特 Dicke 态》。载于：《物理评论快报》（2022年）。[79] Ping Dong 等人。《簇态的生成》。载于：《物理评论*A*——原子、分子与光学物理》73.3（2006年），第 033818 页。[80] Michael A Nielsen。《簇态量子计算》。载于：*Reportson Mathematical Physics*57.1（2006年），第 147–161 页。[81] Michael A Nielsen。《使用簇态的光学量子计算》。载于：《物理评论快报》93.4（2004年），第 040503 页。[82] Taichao Li、Xu Wang 和 Min Jiang。《通过非最大纠缠簇态实现量子密钥协商》。载于：《国际理论物理学杂志》60.7（2021年），第 2429–2444 页。[83] Hussein Abulkasim、Eatedal Alabdulkreem 和 Safwat Hamad。《基于四量子比特簇态的改进型多方量子密钥协商》。载于：计算机、材料与连续体73.1（2022）。[84] Nan-Run Zhou、Qiang Liao 和 Xiang-Fu Zou。《基于四量子比特簇态的多方半量子密钥协商协议》。载于：《国际理论物理学杂志》61.4（2022），第114页。[85] Jun Gu 和 Tzonelih Hwang。《关于通过非最大纠缠簇态实现的量子密钥协商的串谋攻击与反击》。载于：《国际理论物理学杂志》60.1（2021），第331–337页。[86] Zhiwei Sun 等。《采用单 *d*能级量子系统且可抵御串谋攻击的高效多方量子密钥协商》。载于：*IEEEAccess*7（2019），第102377–102385页。[87] Ya-Xi Shu 等。《基于d维d维贝尔态的多方量子密钥协商》。载于：*AdvancedQuantumTechnologies* 7.11（2024），第2400204页。[88] Yi-Hua Zhou 等。《基于第三方的连续变量多方量子密钥协商》。载于：*Modern Physics LettersB* 34.06（2020），第2050083页。[89] Adnan AE Hajomer 等。《在120公里光纤上实现连续变量量子密钥分发与经典数据共存》。载于：*arXiv*预印本 *arXiv:2502.17388*（2025）。[90] Qi Yuan 等。《一种改进的多方协作群组量子密钥分发协议》。载于：*Scientific Reports* 15.1（2025），第526页。[91] Syed M Arslan 等。《双场量子密钥分发：协议、安全性与开放问题》。载于：*arXiv*预印本 *arXiv:2510.26320*（2025）。[92] Feng-Yu Lu 等。《双场量子密钥分发的实际问题》。载于：*New Journal ofPhysics*21.12（2019），第123030页。[93] Xiao-Yu Cao 等。《基于双场的相干单向量子会议密钥协商》。载于：*NewJournal of Physics* 23.4（2021），第043002页。[94] Volkan Erol。《退相干下W态与GHZ态叠加的量子费 Fisher 信息》。载于：*arXiv*预印本 *arXiv:1704.07367*（2017）。[95] TIMO HILLMANN。《近期设备及未来的玻色量子计算》。载于：（2025）。[96] Steven Touzard。《超导电路中玻色编码的稳定化》。载于：博士论文（耶鲁大学，*2019*）（2019）。[97] Christopher S Wang 等。《利用超导玻色处理器高效采样多光子分子振电子光谱》。载于：*PhysicalReview X* 10.2（2020），第021060页。[98] Ernest Y-Z Tan。《依赖设备与设备无关密码学中的记忆效应》。载于：*arXiv*预印本 *arXiv:2308.07869*（2023）。[99]Víctor Zapatero 等。《设备无关量子密钥分发的进展》。载于：*npj*量子信息9.1（2023），第10页。

[100] Kui-Xing Yang 等。《实验测量设备无关量子会议密钥协商》。载于：《物理评论快报》133.21（2024），第210803页。[101] Xiao-Qiu Cai 等。《长距离测量设备无关三方量子密钥协商》。载于：《物理学*A*：统计力学及其应用》607（2022），第128226页。[102] Hao Yang 等。《采用单粒子测量的单态多方量子密钥协商》。载于：《熵》27.4（2025），第405页。[103] Jéré my Ribeiro、Gláucia Murta 和 Stephanie Wehner。《完全设备无关会议密钥协商》。载于：《物理评论*A*》97.2（2018），第022307页。[104] Aby Philip 等。《多方内禀非局域性与设备无关会议密钥协商》。载于：《量子》7（2023），第898页。[105] Karol Horodecki、Marek Winczewski 和 Siddhartha Das。《设备无关量子会议密钥协商的基本限制》。载于：《物理评论*A*》105.2（2022），第022604页。[106] Xuejiao Xu 和 Xiaoping Lou。《半量子密钥协商协议的改进与灵活的多方扩展》。载于：《国际理论物理学杂志》62.11（2023），第252页。[107] Han Guo 等。《基于最大三量子比特纠缠态的半量子密钥协商》。载于：第七届通信与信息处理国际会议论文集。2021年，第132–136页。[108] Shlok Nahar、Twesh Upadhyaya 和 Norbert Lütkenhaus。《不完美相位随机化与广义诱骗态量子密钥分发》。载于：*PhysicalReviewApplied* 20.6（2023），第064031页。[109] Hoi-Kwong Lo、Xiongfeng Ma 和 Kai Chen。《诱骗态量子密钥分发》。载于：*Physical Review Letters*94.23（2005），第230504页。[110] Run-Hua Shi 和 Yi-Fei Li。《量子秘密置换协议》。载于：《*IEEE*计算机汇刊》72.5（2022），第1223–1235页。[111] Justin Yirka 和 Yi˘git Subaşı。《利用量子比特重置实现量子比特高效的纠缠谱学》。载于：《量子》5（2021），第535页。[112]Yi-Chen Zhang 等。《利用压缩态实现连续变量测量设备无关量子密钥分发》。载于：《物理评论*A*》90.5（2014），第052325页。[113] Adam LEWIS 等。《欧洲量子技术的未来方向》。载于：（2025）。[114] WojciechKozlowski、Fernando Kuipers 和 Stephanie Wehner。《面向量子互联网的P4数据平面》。载于：第三届欧洲*P4*研讨会论文集。2020年，第49–51页。[115] Wojciech Kozlowski、Axel Dahlberg 和 Stephanie Wehner。《量子网络协议设计》。载于：第*16*届国际会议论文集新兴网络实验与技术。2020年，第1–16页。[116] Daniel Rausch、Ralf Küsters和Céline Chevalier。“将UC模型嵌入IITM模型”。载于：密码学理论与应用年度国际会议。施普林格。2022年，第242–272页。[117] Ran Canetti和Tal Rabin。“具有联合状态的通用组合”。载于：年度国际密码学会议。施普林格。2003年，第265–281页。[118] Alexander Franzen等人。“压缩态连续变量纯化的实验演示”。载于：《物理评论快报》97.15（2006年），第150505页。[119] Philip Thomas等人。“确定性生成的光子图态的融合”。载于：自然629.8012（2024年），第567–572页。[120] Jin-Hun Kim等人。“在波长复用光纤网络上利用时间-bin纠缠进行量子通信”。载于：*APL*光子学7.1（2022年）。[121] Éloi Descamps、Arne Keller和Pérola Milman。“单光子连续模态变量中的Gottesman-Kitaev-Preskill编码”。载于：《物理评论快报》132.17（2024年），第170601页。[122] Lingzhen Guo、Tangyou Huang和Lei Du。“利用量子晶格门构建玻色编码”。载于：通讯物理8.1（2025年），第414页。[123] Marzio Vallero等人。“表面码补偿超导设备中辐射事件的有效性”。载于：*SC24*：高性能计算、网络、存储与分析国际会议。电气电子工程师学会。2024年，第1–15页。[124] WeiHuang等人。“对一种基于单粒子的多方量子密钥协商协议的密码分析”。载于：《量子信息处理》13.7（2014年），第1651–1657页。