# 基于多尺度纠缠重整化假设的测量设备无关量子密钥分发协议*

赖红#† 王珊珊# 黄钟锐

(西南大学计算机与信息科学学院, 重庆 400715)

(2025 年 10 月 24 日收到; 2025 年 12 月 7 日收到修改稿)

测量设备无关量子密钥分发 (measurement device independent quantum key distribution, MDI-QKD) 协议因其对测量端攻击的天然免疫性而成为当前量子通信领域的研究热点, 但其密钥生成依赖于两个独立光子同时干涉成功, 导致成功概率随通信距离增大和信道损耗增大而急剧下降, 严重限制了远距离量子通信能力. 且一次成功干涉仅能提取 1 比特密钥信息, 编码效率较低, 难以满足高密钥率应用场景的需求. 针对这些关键问题, 本文提出将多尺度纠缠重整化假设 (multi-scale entanglement renormalization ansatz, MERA) 应用于测量设备无关量子密钥分发协议, 并设计了 3 种具体实现方案: 基于 MERA 态第 $L$ 层压缩单光子态的 MDI-QKD、基于 MERA 态第 $L-1$ 层压缩纠缠态的 MDI-QKD 和混合模式下的 MDI-QKD. 这些方案利用 MERA 独特的分层压缩结构, 每次压缩均显著减少光子数量, 最终仅需传输两个甚至单个光子, 即可重构出多层包含多个光子的矩阵乘积态 (matrix product state, MPS), 从而一次性实现多比特的高效密钥生成, 极大地减少了量子信道的使用次数. 通过动态调整压缩深度, 这 3 种方案能够根据实际网络环境和误码率情况灵活优化量子资源使用效率, 避免低层次网络资源的浪费. 同时, 相比经典 MDI-QKD 协议每次干涉仅产生 1 比特密钥, 本文提出的方案实现了密钥规模的指数级增长. 通过仿真实验, 基于 MERA 第 $L$ 层压缩单光子的 MDI-QKD 协议在通信距离为 150 km 时, 较经典 MDI-QKD 协议提高了约 22931% 的密钥生成率. 基于 MERA 第 $L-1$ 层压缩纠缠态的 MDI-QKD 和混合模式下的 MDI-QKD 协议, 在 350 km 处仍能保持 $10^{-11}$ bit/pulse 的密钥生成率, 较经典 MDI-QKD 协议, 有效通信距离延长了约 150 km.

**关键词:** 测量设备无关, 多尺度纠缠重整化假设, 长距离通信, 密钥生成率

**DOI:** 10.7498/aps.75.20251450 **CSTR:** 32037.14.aps.75.20251450

## 1 引 言

量子密钥分发 (quantum key distribution, QKD) 为通信双方提供了一种理论上可实现无条件安全密钥共享的通信方式. 自 1984 年 Bennett 和 Brassard[1] 提出了 BB84 协议以来, QKD 在理论[2–5] 和实验上[6–9] 均获得了广泛研究. BB84 协议基于量子力学原理, 确保任何窃听行为都会在通信过程中留下可检测的痕迹, 从而保障了密钥分发的安全性. 但由于实际系统的不完美, 使窃听者能够从源端或测量端实施攻击. 例如特洛伊木马攻击[10]、光子数分离攻击[11]、致盲攻击[12] 等.

为了抵御这些攻击, Acín 等[13] 提出了设备无关 (device independent, DI)-QKD 协议, 解决系统中的量子设备漏洞. DI-QKD 对系统中的设备不做任何可信任的假设, 其安全性来源于无漏洞的 Bell 测试[14]. 尽管 DI-QKD 协议具有较高的安全

* 国家自然科学基金 (批准号: 61702427) 和西南大学 2025 年校级重点教改项目 (批准号: 2025JY008).

# 同等贡献作者.

† 通信作者. E-mail: hlai@swu.edu.cn

 

性, 但要求系统检测效率超过 82.6%[15], 在目前的技术条件下实现仍有较大难度, 导致其可用性受到了很大限制. 2012 年, Lo 等[16] 提出了测量设备无关 (measurement-device-independent, MDI) QKD 协议, 通过时间反演纠缠分发思想[17], 从原理上免疫测量端攻击, 同时简化测量设备要求, 降低系统复杂度, 在安全性与实用性间取得良好平衡, 且天然适配多资源类型的多尺度纠缠重整化假设 (multi-scale entanglement renormalization ansatz, MERA)[18] 量子调控框架. 2018 年, Lucamarini 等[19] 又提出了双场 (twin field, TF) QKD 协议, 该协议基于异地双场的单光子干涉, 突破了成码率与距离的线性界限, 进一步推进了 MDI-QKD 的发展进程. 近年来, 基于异步双光子干涉的异步 MDI-QKD 协议[20–22], 通过放宽对光子到达时间严格同步的要求, 有效降低了系统实现的复杂度, 为 MDI-QKD 的实用化提供了新的技术路径. 尽管目前 MDI-QKD 已取得了显著突破, 但其密钥生成仍依赖于光子的成功干涉, 成功概率随信道损耗呈指数下降, 在高损耗与长距离场景下面临密钥率低、容错与鲁棒性受限等问题. 且一次成功干涉仅能传递 1 比特经典信息, 难以满足高速通信场景需求.

为解决上述问题, 本文提出将 MERA 应用于 MDI-QKD(统称 MERA-MDI-QKD). 通过利用 MERA 的层级结构进行无损压缩和解压缩, 将一次成功干涉事件所承载的经典信息扩展为 MERA 的多层级比特信息. 本文的主要贡献包括: 1) 提出基于 MERA 态第 $L$ 层压缩单光子态的 MDI-QKD 协议, 提高密钥生成率; 2) 提出基于 MERA 态第 $L-1$ 层压缩纠缠态的 MDI-QKD 协议, 有效缓解了长距离信道的高损耗与噪声干扰的影响; 3) 提出混合模式下的 MDI-QKD 协议, 可根据实时信道条件动态切换 MDI-QKD 方案, 实现不同场景下的性能最优适配.

本文的其余部分安排如下: 第 2 节介绍 MERA 的基本原理与编码规则. 第 3 节详细阐述 基于 MERA 的 MDI-QKD 协议的具体设计思路. 第 4 节进行性能评估. 第 5 节进行安全性分析. 第 6 节总结全文.

## 2 理论基础

本节主要介绍本文提出的基于 MERA 的 MDI-QKD 协议的核心理论基础, 重点阐述矩阵乘积态 (matrix product state, MPS) 与 MERA 的基本原理, 同时明确协议中关键算符的编码规则, 为后续协议设计与分析奠定理论基础.

### 2.1 矩阵乘积态

矩阵乘积态 (MPS)[23] 是一种用于高效描述一维量子多体系统波函数的张量网络表示方法. 对于一个由 $N$ 个量子比特组成的系统, 其 MPS 的标准表述形式如 (1) 式所示:

$$|\psi\rangle_{\mathrm{MPS}}=\sum_{i_1,i_2,\ldots,i_N}\mathrm{Tr}\big(A_{i_1}^{[1]}A_{i_2}^{[2]}\cdots A_{i_N}^{[N]}\big)|i_1\,i_2\cdots i_N\rangle, \tag{1}$$

其中, 两端 $A_{i_1}^{[1]}$ 和 $A_{i_N}^{[N]}$ 是二阶张量, 中间部分 (如 $A_{i_2}^{[2]}$ ) 是三阶张量. Tr 表示矩阵求迹运算.

目前, MPS 可以通过连续的受控非门和单比特旋转门组合实现的量子线路[24]、冷原子系统的光晶格[25] 或对数深度量子电路[26] 等多种方法进行制备. 然而, 虽然 MPS 对短程纠缠态表现出色, 但其顺序性结构导致在表示长程纠缠的能力上存在限制. 具体表现为纠缠熵受限于键维数, 导致难以有效表示系统内远距离粒子间的强关联纠缠. 由于上述限制, 近年来研究逐渐转向能更好捕捉长程纠缠特征的张量网络方法, 如 MERA 或投影纠缠对态 (projected entangled pair states, PEPS).

### 2.2 多尺度纠缠重整化假设 (MERA)

MERA[27] 是一种具有层次化结构的张量网络. 通过引入解纠缠算符 $U$ 与等距映射算符 $W$, 实现对量子态在不同尺度上的有效编码. MERA 态的表达式为

$$\begin{aligned}|\varphi^{(l)}\rangle&=W_l|\varphi^{(l-1)}\rangle\\&=W_lW_{l-1}U_{l-1}W_{l-2}U_{l-2}\cdots W_1U_1|\varphi^{(0)}\rangle,\end{aligned} \tag{2}$$

其中, 初始态 $|\varphi^{(0)}\rangle$ 是预先制备的 MPS 态; $|\varphi^{(l)}\rangle$ 表示第 $l$ 层的压缩量子态, 而 $|\varphi^{(l-1)}\rangle$ 则是第 $l-1$ 层的压缩量子态. 解纠缠算符 $U$ 为局部幺正操作, 用于在粗粒化之前消除相邻自由度间的短程纠缠, 满足: $UU^{\dagger}=U^{\dagger}U=I\otimes I$. 等距映射算符 $W$ 则是将多个局域自由度映射到更少自由度的线性变换, 满足: $W^{\dagger}W=I$. 图 1 展示了 MERA 的层级结构, 其中矩形代表 $U$ 算符, 三角形代表 $W$ 算符.

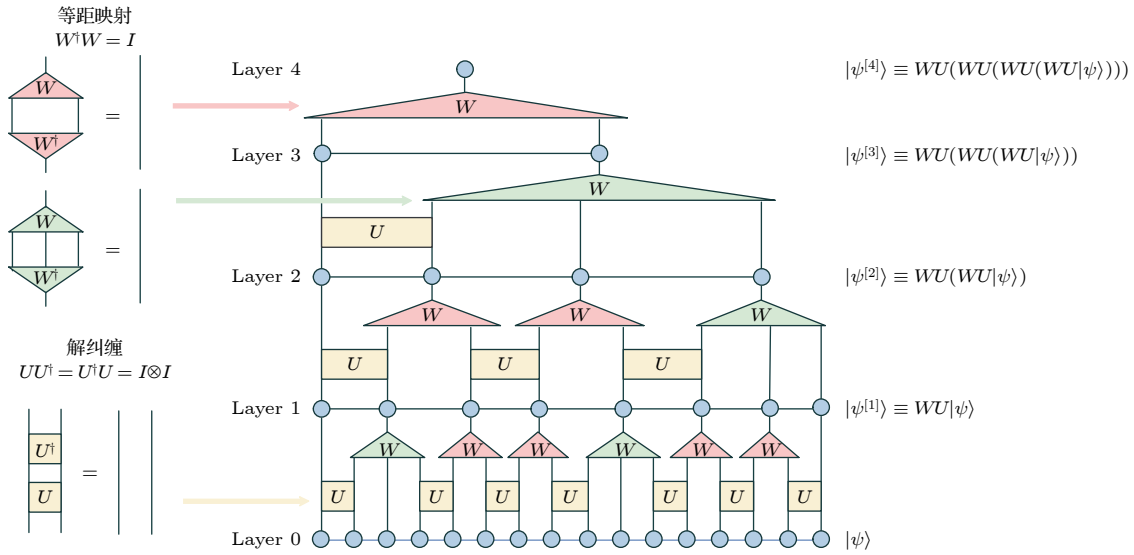


图 1 MERA 结构

Fig. 1. The structure of MERA.

我们考虑图 1 的初始状态为: $|\varphi^{(0)}\rangle = \frac{1}{\sqrt{16}} \times (|0000110111100110\rangle + \cdots + |1101111001011110\rangle)$从底层 $|\varphi^{(0)}\rangle$构建至上一层 $|\varphi^{(1)}\rangle$的具体步骤如下.

1) **初始随机分割**: 底层粒子 $|\varphi^{(0)}\rangle$ 采用二元或三元编码随机相互交织分割成若干组, 为后续对每组粒子的统一变换奠定基础.

2) **应用 $U$算符**: 对分割后的每组粒子施加 $U$ 算符 (按顺序分别使用$u_1$, $u_1$, $u_2$, $u_2$, $u_2$, $u_1$, $u_2$, 其中 $u_1$, $u_2$ 的矩阵表达式详见 2.3 节), 以此消除组内粒子间的短程纠缠, 降低后续变换的复杂度.

3) **应用 $W$算符**: 在 $U$ 算符处理后, 对每组粒子施加 $W$ 算符 (按顺序分别使用$w_3$, $w_2$, $w_2$, $w_4$, $w_1$, $w_1$, 其中各 $w_i (i = 1, 2, 3, 4)$ 的矩阵表达式详见 2.3 节), 将每组粒子映射到更高层次的有效自由度, 实现态的压缩, 最终得到上一层态:

$$|\varphi^{(1)}\rangle = \frac{1}{\sqrt{8}} (|00101000\rangle + \cdots + |00011010\rangle) .$$

MERA 的关键优势在于其能够同时保留层内纠缠与层间关联, 通过 $U$ 和 $W$ 消除短程纠缠, 建立长程纠缠, 从而在保持高编码效率的同时, 具备较强的鲁棒性, 为构建高容量、抗干扰的 QKD 协议提供了理想的理论框架.

## 2.3 编码规则

在 MERA 框架中, 量子态的逐层压缩与解压缩过程由 $U$ 和 $W$ 两类算符共同实现. 为便于基于 MERA 的 MDI-QKD 协议的设计与实现, 需对算符类型及其作用规则进行明确编码. 根据文献 [28,29] 及协议需求, 本文定义两类算符的具体矩阵形式如下:

$$u_1 = \begin{bmatrix} \frac{1}{\sqrt{2}} & 0 & 0 & \frac{1}{\sqrt{2}} \\ 0 & \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} & 0 \\ 0 & \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} & 0 \\ \frac{1}{\sqrt{2}} & 0 & 0 & -\frac{1}{\sqrt{2}} \end{bmatrix},$$

$$u_2 = \begin{bmatrix} \frac{1}{\sqrt{2}} & 0 & 0 & -\frac{1}{\sqrt{2}} \\ 0 & \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} & 0 \\ 0 & \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} & 0 \\ \frac{1}{\sqrt{2}} & 0 & 0 & \frac{1}{\sqrt{2}} \end{bmatrix},$$

$$w_1 = \begin{bmatrix} \frac{1}{\sqrt{2}} & 0 & 0 & \frac{1}{\sqrt{2}} \\ 0 & \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} & 0 \end{bmatrix},$$

$$w_2 = \begin{bmatrix} 0 & \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} & 0 \\ \frac{1}{\sqrt{2}} & 0 & 0 & \frac{1}{\sqrt{2}} \end{bmatrix},$$

$$w_3=\begin{bmatrix} \frac{1}{\sqrt{2}} & 0 & 0 & 0 & 0 & 0 & 0 & \frac{1}{\sqrt{2}} \\ 0 & \frac{1}{\sqrt{6}} & \frac{1}{\sqrt{6}} & \frac{1}{\sqrt{6}} & \frac{1}{\sqrt{6}} & \frac{1}{\sqrt{6}} & \frac{1}{\sqrt{6}} & 0 \end{bmatrix},$$

$$w_4=\begin{bmatrix} 0 & \frac{1}{\sqrt{6}} & \frac{1}{\sqrt{6}} & \frac{1}{\sqrt{6}} & \frac{1}{\sqrt{6}} & \frac{1}{\sqrt{6}} & \frac{1}{\sqrt{6}} & 0 \\ \frac{1}{\sqrt{2}} & 0 & 0 & 0 & 0 & 0 & 0 & \frac{1}{\sqrt{2}} \end{bmatrix}.$$

值得注意的是, $W$ 和 $U$ 不是固定的, 可以根据具体情况优化选择. 为简化不同类型算符在数值实践中的处理, 本文采用一种二进制编码策略对算符进行分类编码, 确保每个算符对应唯一的二进制序列, 并引入对应的解压缩规则, 以便在 MERA 态的高层编码和具体操作之间建立明确对应关系. $U$ 类算符包括两种基本操作, 分别用 1 比特进行编码; $W$ 类算符包含 4 个基本操作, 采用 2 比特进行编码. 具体编码规则如下:

$$\mathrm{enc}(U_i)=\begin{cases} 0, & i=1 \\ 1, & i=2 \end{cases} \quad \mathrm{enc}(W_j)=\begin{cases} 00, & j=1 \\ 01, & j=2 \\ 10, & j=3 \\ 11, & j=4 \end{cases}$$

表 1 算符 $W$ 与 $U$ 的编码及解压规则表

Table 1. Encoding table with decompression Rules for operator $W$ and $U$.

| 矩阵 | 二进制编码 | 解压缩态 | 解压缩编码规则 |
|---|---|---|---|
| $U_1$ | 0 | — | — |
| $U_2$ | 1 | — | — |
| $W_1$ | 00 | $\|00\rangle$ | 000(对应 $\|00\rangle$ ) |
| | | $\|11\rangle$ | 001(对应 $\|11\rangle$ ) |
| $W_2$ | 01 | $\|01\rangle$ | 010(对应 $\|01\rangle$ ) |
| | | $\|10\rangle$ | 011(对应 $\|10\rangle$ ) |
| $W_3$ | 10 | $\|000\rangle$ | 100(对应 $\|000\rangle$ ) |
| | | $\|111\rangle$ | 101(对应 $\|111\rangle$ ) |
| $W_4$ | 11 | $\|000\rangle$ | 110(对应 $\|000\rangle$ ) |
| | | $\|111\rangle$ | 111(对应 $\|111\rangle$ ) |

其中, $\mathrm{enc}(x)$ 表示对 $x$ 进行二进制编码.

在解压缩过程中, 接收方根据二进制编码, 将接收到的比特串映射回对应的 $W$ 或 $U$ 算符, 进而逐层恢复原始的量子态信息. 具体操作如表 1 所示.

## 3 基于 MERA 的 MDI-QKD 协议

为解决经典 MDI-QKD 在长距离、高噪声信道环境下密钥率受限等问题, 本文提出 3 种基于 MERA 的 MDI-QKD 改进方案. 通过利用 MERA 的层级纠缠结构对量子信息进行压缩编码, 以提升协议的密钥生成率与抗噪声能力. 本节详细介绍这 3 种方案的实现过程.

### 3.1 协议的初始化

在基于 MERA 的 MDI-QKD 协议中, 通信双方 (Alice 与 Bob) 根据信道损耗、噪声水平及安全需求等实际条件, 预先公开协同设计 4 种不同拓扑结构的 MERA 态. 这些 MERA 态的底层粒子数可根据通信规模灵活配置: 更多粒子意味着更大的潜在密钥空间, 适用于大规模量子网络的高密钥量需求; 减少底层粒子数则可降低算符操作复杂度, 提升协议执行效率. 同时可通过调整解纠缠算符 $U$ 与等距映射算符 $W$ 的作用域, 动态优化密钥生成效率.

为清晰阐述协议原理, 本文定义如图 2 所示的 4 种 MERA 结构 (记为构型 A, B, C, D), 并作如下约定.

**第 $L$ 层:** 该层为压缩单光子量子态. 预定义构型 A 与 B 的第 $L$ 层压缩单光子态为 $|0\rangle$, 构型 C 与 D 的第 $L$ 层压缩单光子态为 $|1\rangle$. 进一步规定构型 A 与 D 编码为经典比特“0”, 构型 B 与 C 编码为经典比特“1”.

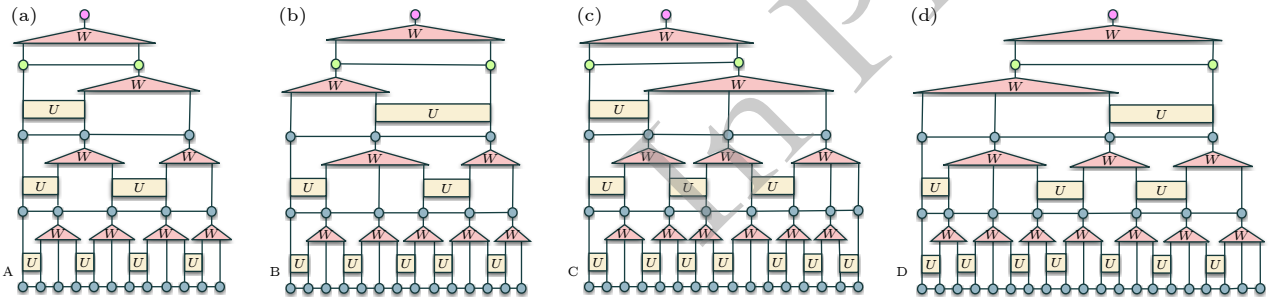


图 2 4 种 MERA 结构示意图, 构型 A 与 D 编码为 0, 构型 B 与 C 编码为 1

Fig. 2. Schematic diagram of the four MERA structures. Structures A and D are encoded as 0, while structures B and C are encoded as 1.

**第 $L-1$ 层:** 该层为压缩双粒子纠缠态, 预定义构型 A 和 B 的第 $L-1$ 层压缩纠缠态为 $|\Phi^+\rangle = \frac{1}{\sqrt{2}}\left(|00\rangle + |11\rangle\right)$, 构型 C 和 D 的第 $L-1$ 层压缩纠缠态为 $|\Psi^+\rangle = \frac{1}{\sqrt{2}}\left(|01\rangle + |10\rangle\right)$.

## 3.2 协议方案

### 3.2.1 方案一: 基于 MERA 态第 $L$ 层压缩单光子态的 MDI-QKD

方案一量子密钥分发的核心流程如图 3 所示. 图 3 中蓝色小球代表诱骗态, 红色、橙色、绿色和紫色小球分别代表来自 4 种不同 MERA 态 (A, B, C, D) 的量子态. 其中, 图 3(a)—(e) 的小球表示对应颜色代表的 MERA 态的第 $L$ 层压缩单光子态; 图 3(f) 的小球表示对应颜色代表的 MERA 态解压缩后可用于建立密钥的量子态. 红色虚线框表示 Alice 和 Bob 选择的基不相同, 丢弃本次结果. 绿色虚线框表示 Alice 和 Bob 都选用的 X 基, 该测量结果用于窃听检测. 具体步骤如下:

**步骤 1 量子态制备.** Alice 与 Bob 各自独立且随机地从 4 种预先定义的 MERA 态中选择 1 种. 在 MERA 第 $L$ 层制备压缩单光子态, 并随机插入诱骗态以增强实际系统的安全性. 本文采用包含一个信号态与两个诱骗态的诱骗态方案[30], Alice 和 Bob 分别将其光源调制为 3 个不同强度 $\{\mu, \nu_1, \nu_2\}$, 其中 $\mu$ 为信号态强度 (即每个光脉冲的平均光子数), $\nu_1$ 和 $\nu_2$ 为两个诱骗态的强度, 且满足 $\mu > \nu_1 > \nu_2 \geqslant 0$. 在基选择方面, 仅信号强度在 Z 基中编码, 其他诱骗强度都在 X 基中编码, 以用于后续的窃听检测. 为确保双方能协调生成密钥, 通过特定的酉矩阵, 对第 $L-1$ 层的纠缠态进行操作, 使得不同 MERA 的第 $L$ 层能得到预定义的量子态 (详见 3.1 节).

本协议中诱骗态方案的引入, 是针对物理实现中光源非理想性的安全措施, 独立于核心的 MERA 编码逻辑. MERA 编码在算法层面操作的是理想的逻辑 qubit; 而诱骗态则在物理层面, 为整个系统提供了对抗现实光源缺陷的标准化的安全验证与参数估计能力, 确保了协议在实际部署中的安全性.

**步骤 2 量子态发送.** 制备完成后, Alice 和 Bob 将光子通过量子信道发送至第三方测量节点 Charlie.

**步骤 3 Bell 态测量.** Charlie 对接收到的双光子进行联合 Bell 态测量 (Bell state measurement, BSM), 并公开测量结果, 不泄漏任何具体的比特

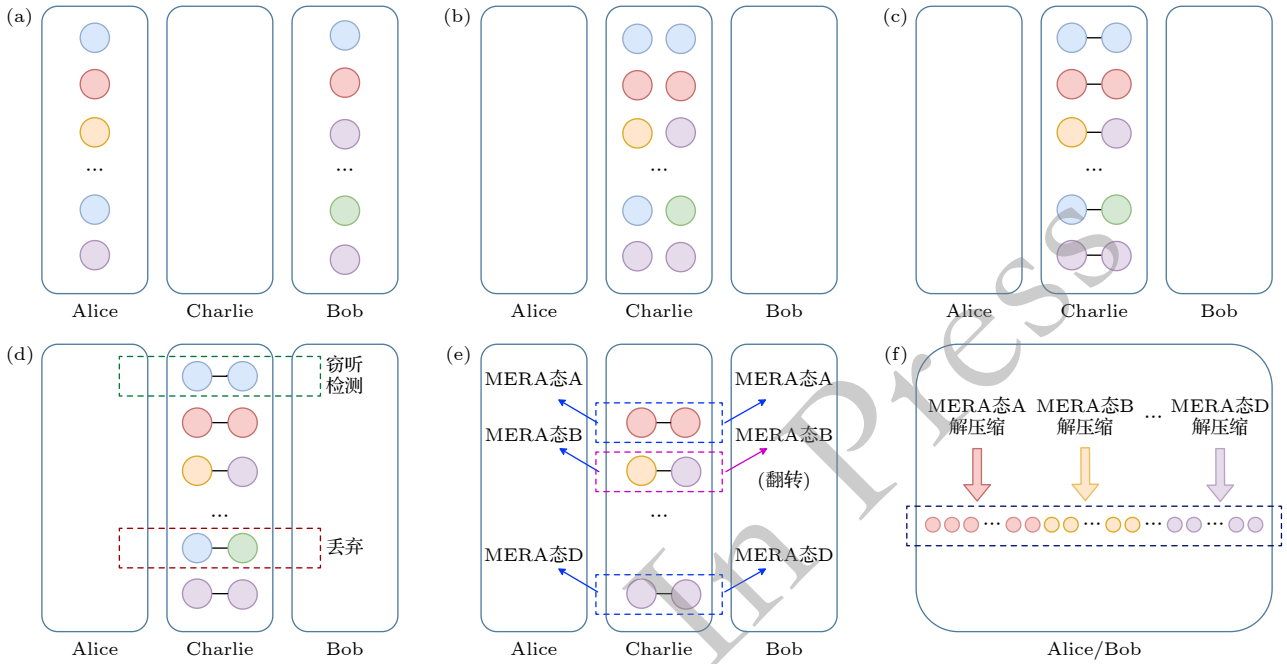




图 3 基于 MERA 态第 $L$ 层压缩单光子态的 MDI-QKD 协议原理图 (a) 量子态的制备; (b) 发送量子态给 Charlie; (c) Bell 态测量; (d) 基匹配筛选; (e) 匹配 MERA 结构; (f) MERA 解压缩提取密钥

Fig. 3. Schematic of the MDI-QKD protocol based on a compressed single-photon state at layer $L$ of a MERA state: (a) Quantum-state preparation; (b) transmission of the quantum states to Charlie; (c) Bell-state measurement; (d) basis-matching sifting; (e) MERA-structure matching; (f) MERA decompression and key extraction.

信息, 以此确保测量设备的无关性. Alice 和 Bob 根据 Charlie 公布的结果, 将其分类为两种经典事件: 若结果为 $|\Phi^+\rangle$ 或 $|\Phi^-\rangle$, 他们将其记录为“关联”事件, 这表明 Alice 与 Bob 所发送的第 $L$ 层单光子态同为 $|0\rangle$ 或同为 $|1\rangle$. 若结果为 $|\Psi^+\rangle$ 或 $|\Psi^-\rangle$, 他们将其记录为“反关联”事件, 这表明 Alice 与 Bob 所发送的第 $L$ 层单光子态互为正交态, 即一方为 $|0\rangle$, 另一方为 $|1\rangle$.

需要注意的是, Charlie 仅能判断 Alice 与 Bob 所发送的第 $L$ 层单光子态是否相同, 而无法获知具体的 MERA 构型. 若为反关联事件, 则表明 Alice 与 Bob 所选用的 MERA 构型不同. 此时, Bob 需将其第 $L$ 层的压缩单光子态进行比特翻转 ($|0\rangle \leftrightarrow |1\rangle$), 为后续步骤中双方能够正确协调 MERA 结构奠定基础.

**步骤 4 基匹配筛选.** Alice 和 Bob 通过经典信道公开比较其所选的测量基 (Z 基或 X 基). 仅当双方选择相同测量基时, 该次事件才被保留: 选择 Z 基的事件用于最终密钥生成, 选择 X 基的事件用于信道窃听检测. 基匹配筛选规则详见表 2.

表 2 基匹配筛选结果

Table 2. Sifting results of basis matching.

| Alice选择的基 | Bob选择的基 | 是否保留 | 原因 |
|---|---|---|---|
| Z基 | Z基 | 保留 | 用于密钥生成 |
| X基 | X基 | 保留 | 用于窃听检测 |
| Z基 | X基 | 不保留 | 基不匹配 |
| X基 | Z基 | 不保留 | 基不匹配 |

**步骤 5 匹配 MERA 结构.** Charlie 公布 BSM 结果后, Alice 与 Bob 直接公开他们所选的 MERA 结构编码 (A, D 编码为“0”, B, C 编码为“1”). 双方根据 BSM 结果及表 3 所定义的规则, 同步执行必要的翻转操作, 确保后续解压缩时使用一致的 MERA 结构, 从而生成相同的密钥.

表 3 Bell 态测量结果与比特翻转对应关系

Table 3. Mapping relationship between Bell-state measurement results and bit flip transformations.

| Alice/Bob基 | $\|\Psi^-\rangle$ | $\|\Psi^+\rangle$ |
|---|---|---|
| Z基 | 比特翻转 | 比特翻转 |
| X基 | 比特翻转 | 无翻转 |

**步骤 6 MERA 解压缩提取密钥.** 基于 Charlie 公开的 Bell 态测量结果, 结合 Alice 与 Bob 预先约定的 MERA 私有编码规则, 双方分别在本地执行逻辑层面的解压缩操作——通过逐层施加 MERA 压缩过程的逆操作 ($W^{-1}$ 与 $U^{-1}$ 算符), 重构出与原始多 qubit 纠缠态等价的逻辑量子态, 最终通过本地测量得到经典密钥比特串. 为确保在噪声信道下量子态的完整性, 引入多层保真度验证机制.

定义第 $l$ 层理想目标态为 $|\phi^{(l)}_{\text{ideal}}\rangle$, 实际解压缩得到的量子态为 $|\phi^{(l)}_{\text{real}}\rangle$. 该层的保真度定义为

$$F_l = \left|\langle\phi^{(l)}_{\text{ideal}}|\phi^{(l)}_{\text{real}}\rangle\right|^2. \tag{3}$$

设定一个保真度阈值 $F_{\text{threshold}}$. 若 $F_l \geqslant F_{\text{threshold}}$, 则认为第 $l$ 层通过验证; 否则, 该层数据作废. 若在某轮解压缩中, 所有层均未通过验证, 或 Alice 与 Bob 之间没有共同通过验证的层级, 则丢弃本轮次的所有数据, 并通过经典信道广播丢弃该事件, 并重新开始密钥生成流程.

在通过保真度验证的层级中, Alice 与 Bob 确定一个公共的有效层级集合 $U_{\text{layer}}$. 随后按以下步骤生成所需密钥.

(1) **层级选择:** 双方一致选定集合 $U_{\text{layer}}$ 中的某一层级 $l$.

(2) **构建二进制序列:** 对于每个选定的层级 $l \in U_{\text{layer}}$, Alice 与 Bob 将该层的量子态信息转换为经典二进制序列, 并通过协调确保双方序列一致:

$$k_l = A_l = B_l, \tag{4}$$

其中, $A_l$ 与 $B_l$ 分别为 Alice 与 Bob 在第 $l$ 层获得的比特序列.

(3) **构建原始密钥:** 将各有效层级 $l \in U_{\text{layer}}$ 产生的比特序列 $k_l$ 按照层级序号从高到低的顺序进行级联, 构成原始密钥 $K$:

$$K = \|_{l\in U_{\text{layer}}}\, k_l, \tag{5}$$

其中, 符号 $\|$ 表示级联操作.

(4) **提取最终密钥:** 重复执行 $n$ 次上述光子对发送与处理过程, 将各轮次产生的原始密钥 $K_i$ 进行级联:

$$K_{\text{final}} = \|_{i=1}^{n}\, K_i. \tag{6}$$

然后对 $K_{\text{final}}$ 执行标准的后处理步骤 (包括纠错与隐私放大), 生成最终的安全密钥.

### 3.2.2 方案二: 基于 MERA 态第 $L-1$ 层的压缩纠缠态的 MDI-QKD

方案二量子密钥分发的核心流程如图 4 所示.

图 4 中蓝色小球代表诱骗态, 红色、橙色、绿色和紫色小球分别代表来自 4 种不同 MERA 态 (A, B, C, D) 的量子态. 其中, 图 4(a)—(e) 的小球表示对应颜色代表的 MERA 态的第 $L-1$ 层压缩纠缠态; 图 4(f) 的小球表示对应颜色代表的 MERA 态解压缩后可用于建立密钥的量子态. 具体步骤如下:

**步骤 1　量子态的制备.** Alice 和 Bob 各自独立且随机地从 4 种预先定义的 MERA 态中选择一种. 通过特定的酉矩阵, 将 MERA 态第 $L-1$ 层制备成预定义的压缩纠缠态, 并采用如 3.2.1 节步骤 1 所述的诱骗态方案随机插入诱骗态, 以用于后续的窃听检测.

**步骤 2　量子态的分发.** 如图 4(b) 所示, 量子态制备完成后, Alice 和 Bob 分别保留光子 A1 和 B1, 将光子 A2 和 B2 通过量子信道发送至 Charlie.

**步骤 3　Bell 态测量.** Charlie 对接收到的来自 Alice 和 Bob 的光子进行 BSM. 测量完成后, Charlie 仅公开其测量结果, Alice 和 Bob 判断属于关联事件 (Alice 与 Bob 的光子状态相同) 或反关联事件 (Alice 与 Bob 的光子状态互补).

**步骤 4　基匹配筛选.** Alice 与 Bob 通过经典信道公开比较其测量基的选择情况. 根据 BSM 所涉及粒子的来源, 将事件分为 3 类并进行筛选. 情形一: BSM 两个光子均来自纠缠对 (都使用 Z 基). 此时, 通过纠缠交换, Alice 与 Bob 保留的粒子将形成新的纠缠态. 该类事件被保留用于密钥生成. 情形二: BSM 中一光子来自纠缠对, 另一光子为诱骗态 (一边使用 Z 基, 一边使用 X 基). 此类事件的结果及其对应的光子均被丢弃, 不参与后续密钥生成. 情形三: BSM 两个光子均为诱骗态 (都使用 X 基). 该类事件的 BSM 结果用于窃听检测.

**步骤 5　匹配 MERA 结构.** Alice 与 Bob 在本地测量各自保留的光子 A1 和 B1, 并结合 Charlie 公布的 BSM 关联性结果, 相互推断对方所持有的第 $L-1$ 层压缩纠缠态. 随后, 双方采用与方案一中相同的 MERA 结构匹配方法 (详见第 3.2.1 节), 通过公开交换有限的编码信息, 协调出一致的 MERA 构型, 确保双方找到相同的 MERA 态以进行解压缩和密钥提取.

**步骤 6　保真度验证和密钥建立.** 此步骤与方案一中的步骤 6 完全一致 (详见第 3.2.1 节). 双方

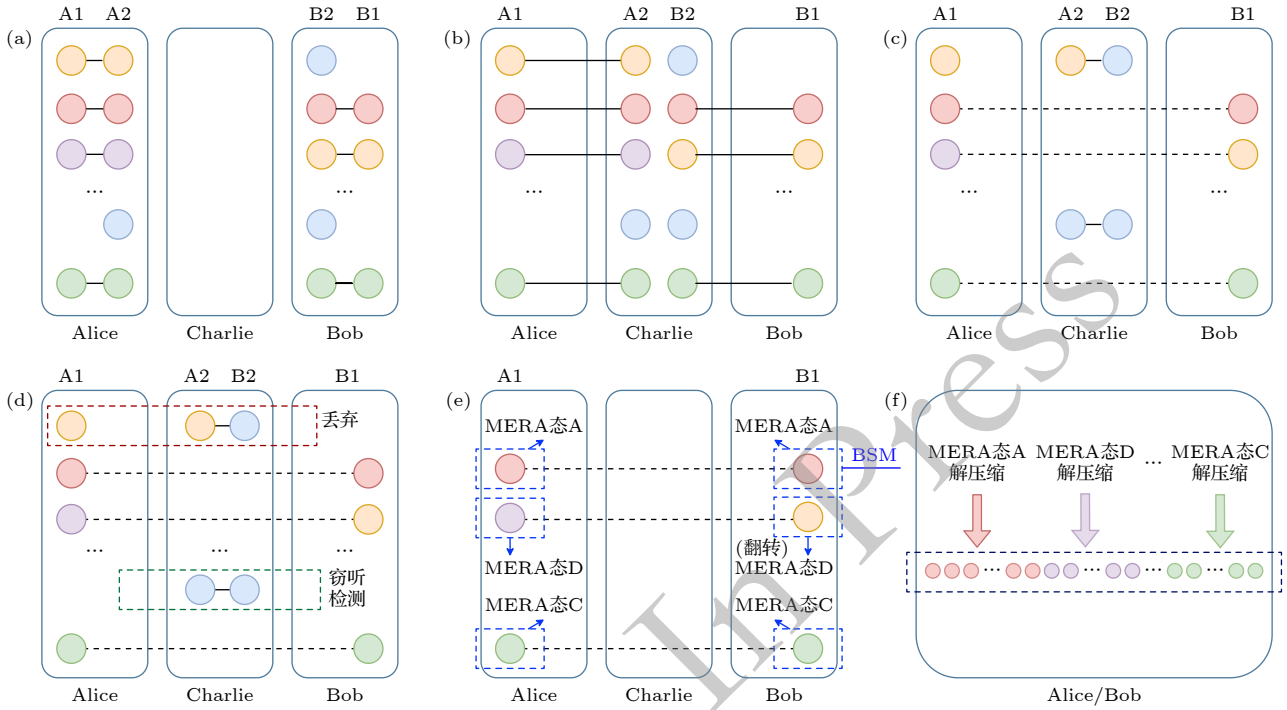


图 4　基于 MERA 态第 $L-1$ 层的压缩纠缠态的 MDI-QKD 协议原理图　(a) 量子态的制备; (b) 发送量子态给 Charlie; (c) Bell 态测量; (d) 基匹配筛选; (e) 匹配 MERA 结构; (f) MERA 解压缩提取密钥

Fig. 4. Schematic of the MDI-QKD protocol based on a compressed entangled state at layer $L-1$ of a MERA state: (a) Quantum-state preparation; (b) transmission of the quantum states to Charlie; (c) Bell-state measurement (BSM); (d) basis-matching sifting; (e) MERA-structure matching; (f) MERA decompression and key extraction.

基于协调好的 MERA 结构, 执行逐层解压缩与保真度验证, 从通过验证的层级中提取二进制序列, 并通过级联操作形成原始密钥 $K_{\text{final}}$. 最终经纠错与隐私放大后, 生成安全密钥.

### 3.2.3 方案三: 混合模式

为兼顾不同信道条件下的密钥生成速率与抗噪能力, 本文进一步提出一种自适应混合操作模式, 可根据实时信道条件动态选择使用基于 MERA 态第 $L$ 层压缩单光子态的 MDI-QKD(方案一) 或基于 MERA 态第 $L-1$ 层压缩纠缠态的 MDI-QKD (方案二).

**动态选择机制:** 考虑实时检测量子信道的量子误码率 (quantum bit error rate, QBER)、光子传输效率等参数.

1) 当信道质量较好 (QBER 较低、传输效率高) 时, 优先使用方案一, 以提高密钥生成速率.

2) 当信道质量较差 (QBER 较高、传输效率低) 时, 切换至方案二, 利用纠缠态的强关联性增强抗噪声能力.

**调度函数:** 为量化上述动态选择策略, 本文定义一个调度概率 $p$, 用以表示在通信中采用方案一的比例. 相应地, $1-p$ 则为采用方案二的比例. 该概率由以下公式动态计算:

$$p = \alpha \cdot \frac{1}{1+\mathrm{e}^{k(\mathrm{QBER}-Q_{\text{th}})}} + \beta \cdot \frac{\eta}{\eta_{\max}}, \tag{7}$$

其中, $\alpha$ 与 $\beta$ 为权重系数, 满足 $\alpha+\beta=1$, 用于平衡 QBER 与传输效率的影响; $Q_{\text{th}}$ 为预设的 QBER 阈值; $k$ 为调节系数; $\eta$ 为实测信道传输效率; $\eta_{\max}$ 为理论最大传输效率.

基于上述机制, 混合模式下的 MDI-QKD 协议按以下步骤执行.

**量子态制备与发送:** Alice 与 Bob 根据调度函数计算得到的 $p$, 按比例随机选择制备并发送基于 MERA 态第 $L$ 层的压缩单光子态或基于 MERA 态第 $L-1$ 层的压缩纠缠态. 在发送过程中, 采用如 3.2.1 节步骤 1 所述的诱骗态方案随机插入诱骗态以进行窃听检测.

**Bell 态测量:** Charlie 对接收到的量子态进行 BSM. 对于单光子态, 公布其结果是否为“相同态”; 对于纠缠态, 则公布其结果是否为“关联态”.

**基匹配筛选与 MERA 结构匹配:** Alice 与 Bob 根据本轮次实际使用的量子态类型, 分别调用对应的处理方法: 若使用基于 MERA 态的第 $L$ 层单光子态, 则执行与方案一完全相同的基匹配筛选与 MERA 结构匹配方法 (详见第 3.2.1 节); 若使用基于 MERA 态的第 $L-1$ 层纠缠态, 则执行与方案二完全相同的基匹配筛选与 MERA 结构匹配方法 (详见第 3.2.2 节).

**MERA 解压缩提取密钥:** 此步骤与方案一中的步骤 6 完全一致 (详见第 3.2.2 节).

需要明确的是, 使用 MERA 结构本身并不会增加信息熵, 而是将其作为一个高效的编码调度框架, 使得在后续的 MDI-QKD 量子传输中, 单次成功事件所能提取和利用的有效安全信息量得到极大提升. 这一设计的核心价值在于, 在给定安全标准下, 显著降低生成目标长度密钥所需的量子信道使用次数、BSM 次数等, 从而有效对抗信道损耗, 提升协议的实际性能.

值得注意的是, 本协议的安全性源于“公开 MERA 结构”与“私有编码规则”的分离设计: MERA 的拓扑结构公开, 但每一层压缩/解压缩所采用的 $W/U$ 算符、量子态与经典比特的映射关系, 均由 Alice 和 Bob 秘密共享. 窃听者即便截获传输的单 qubit 态, 由于缺乏私有编码规则, 无法确定正确的逆操作; 即便侥幸猜对部分算符, 解压缩后得到的仍是 Alice 和 Bob 之间的私有纠缠态, 窃听者因未持有纠缠伙伴粒子, 无法通过局部测量获取有效信息. 这种“经典私有规则+量子纠缠关联”的双重保障, 使得窃听者的解压缩错误概率随层数指数级增长, 最终成功窃取密钥的概率可忽略不计. 同时, 成码率的提升并非“无中生有产生随机比特”, 而是通过 MERA 的纠缠压缩特性, 让单 qubit 传输高效承载原始多 qubit 纠缠态的随机信息, 未引入任何额外信息泄漏, 完全满足 QKD 的安全与效率要求.

本协议中“私有编码规则”的安全性来源是: 双方首先运行一轮标准的 QKD 协议 (如 BB84), 以生成一个较短的共享密钥. 此短密钥即可作为“密钥种子”, 衍生出本协议所需的私有编码规则. 因此, 私有编码规则的安全性, 归根结底由标准 QKD 协议的物理原理保障. 在协议执行中, 该规则的功能是作为一个预共享的“解码本”, 指导通信双方如何从单次量子传输事件所确立的有限安全关联中, 高效提取出更长的经典比特序列. 这一过程严格遵守信息守恒原理, 并未增大安全信息的总熵. 其核心价值在于大幅提升了单位传输的量子资源消耗

所对应的有效安全密钥产出, 从而增强了协议对抗信道损耗的能力.

## 4 性能评估

本文旨在突破经典 MDI-QKD 密钥生成率低、长距离通信能力弱等瓶颈. 本节通过构建数学模型, 从密钥生成率与编码容量两个核心指标对协议性能进行量化评估, 结合仿真实验验证方案的有效性.

### 4.1 密钥生成率

#### 4.1.1 基于 MERA 第 $L$ 层压缩单光子态的 MDI-QKD 协议的密钥生成率

**增益:** 在 Z 基下, 基于 MERA 第 $L$ 层压缩单光子态的 MDI-QKD 协议的成功增益 $Q^{\text{rect}}$ 定义为量子比特成功传输并产生有效探测事件的联合概率, 可表示为

$$Q^{\text{rect}} = \sum_{n,m} Q^{\text{rect}}_{n,m}, \tag{8}$$

其中, $Q^{\text{rect}}_{n,m}$ 表示两个合法用户分别发送 $n$ 和 $m$ 个光子时的增益.

**量子比特误码率 (QBER):** 假设在水平基即 Z 基下的误码率为 $e^{\text{rect}}$, 则总体的量子比特误码率 $E^{\text{rect}}$ 为

$$E^{\text{rect}} = \frac{1}{Q^{\text{rect}}} \sum_{n,m} Q^{\text{rect}}_{n,m} e^{\text{rect}}_{n,m}. \tag{9}$$

**MERA 解压缩成功率:** 在密钥提取过程中, 需对 MERA 态进行逐层解压缩, 并以保真度作为验证标准. 第 $l$ 层解压缩成功的概率定义为

$$P_l = \Pr\left(F_l \geqslant F_{\text{th}}\right), \tag{10}$$

其中, $\Pr(F_l \geqslant F_{\text{th}})$ 指第 $l$ 层保真度数值落在 $F_l \geqslant F_{\text{th}}$ 区间内的对应概率.

**可恢复的安全比特上界:** 设 MERA 底层量子数为 $n$, MERA 的分支因子为 $b \in \{2,3\}$. MERA 的最大层数表示如下:

$$L = \left\lceil \log_b n \right\rceil. \tag{11}$$

则 MERA 第 $l$ 层 $(0 \leqslant l \leqslant L)$ 所包含的有效量子比特数为

$$n_l = \left\lfloor \frac{n}{b^l} \right\rfloor. \tag{12}$$

在理想情况下, 一个 MERA 态压缩包含的总量子态信息量可表示为

$$n^l_{\text{MERA}} = \sum_{l=0}^{L} n_l. \tag{13}$$

**成功制备单个 MERA 态的概率模型:** 假设纠缠光源服从特定统计分布, 源端产生 $n$ 对纠缠光子的概率为[31]

$$P'(n) = \frac{(n+1)\lambda^n}{(1+\lambda)^{n+2}}. \tag{14}$$

其中, $\lambda$ 表示纠缠源的参量, 定义为 $\lambda = \sinh^2 \chi$.

MERA 态的制备可采取文献 [32,33] 所提供的方案, 先制备底层 MPS 态, 随后依次使用算符 $W$ 和 $U$ 逐层生成上层 MPS 态. 底层 MPS 态可采用文献 [34,35] 所提供的融合方式由纠缠对拼接得到. 若需要制备底层量子数为 $m_0$ 的 MPS 态, 则需要先产生至少 $m_0 - 1$ 对纠缠对, 并进行 $m_0 - 2$ 次融合. 用 $N$ 光子编码来区分四种逻辑 Bell 态, 单次融合成功概率可达 $P_{\text{fus}} = 1 - 1/4^N$ [36]. 因此, 制备单个 MERA 态的成功概率为

$$P(1) = \sum_{n=m_0-1}^{\infty} \frac{(n+1)\,\lambda^n}{(1+\lambda)^{n+2}} P_{\text{fus}}^{m_0-2} \sum_{l=1}^{L} P_{wu}(l), \tag{15}$$

其中, $P_{wu}(l)$ 表示使用算符 $W$ 和 $U$ 制备 MERA 态第 $l$ 层的成功率.

执行单层 MERA 的压缩操作, 其核心物理过程等效于实现一个特定构型量子线路. 该线路主要由线性光学受控相位门以及相应调制器构成. 采用的底层约 $N$ 个物理光子的 MERA 结构, 每一层的解纠缠算符 $U$ 与等距映射算符 $W$ 仅作用于 2 或 3 个相邻量子态, 其总数随底层模式数近似线性缩放, 数量级为 $O(N)$. 一层 MERA 操作引入的附加插入损耗可合理估计为若干 dB 的常数量级.

**光纤损耗模型:** 对于 Alice 与 Bob 传输给 Charlie 的两个量子信道, 光纤损耗模型可分别写成:

$$\eta_a(L_{\text{ac}}) = 10^{-\alpha L_{\text{ac}}/10}, \quad \eta_b(L_{\text{bc}}) = 10^{-\alpha L_{\text{bc}}/10}, \tag{16}$$

其中, $\alpha$ 为光纤衰减系数, 通常取 0.2 dB/km; $L_{\text{ac}}$ 和 $L_{\text{bc}}$ 分别为 Alice 和 Bob 至 Charlie 的通信距离.

在 X 基下, 通信双方采用诱骗态进行窃听检测与量子比特误码率估计, 不涉及 MERA 结构选择. 诱骗态的引入使得窃听者无法区分信号态与诱骗态, 以此保障协议的安全性.

基于 MERA 第 $L$ 层压缩单光子态的 MDI-QKD

协议中, 密钥生成率不仅依赖于基匹配概率与量子比特误码率等因素, 还受到 MERA 态逐层解压缩成功率的影响. 因此, 考虑该协议在一次成功事件中可生成多层级密钥的特性, 其密钥生成率 $R_{\rm si}$ 可以由 (17) 式[16,30] 给出:

$$R_{\rm si}\geqslant\sum_{l=1}^{L}m_lP_l^{(A)}P_l^{(B)}\frac{n_{\rm MERA}^{l'}}{n_{\rm MERA}^{l}}\Big[P(1)Y_{\rm rect}^{1,1}\big(1-H_2(e_{\rm X}^{1,1})\big)-Q^{\rm rect}f\big(E^{\rm rect}\big)H_2\big(E^{\rm rect}\big)\Big],\tag{17}$$

$$e_{\rm X}^{1,1}=\frac{1}{2}-\frac{t_{\rm a}t_{\rm b}\eta_{\rm d}^2(1-e_{\rm d})^2(1-Y_0)^2}{4Y_{\rm rect}^{1,1}},\tag{18}$$

$$Y_{\rm rect}^{1,1}=(1-Y_0)^2\Big[4Y_0^2(1-t_{\rm a}\eta_{\rm d})(1-t_{\rm b}\eta_{\rm d})+2Y_0\Big(t_{\rm a}\eta_{\rm d}+t_{\rm b}\eta_{\rm d}-\frac{3}{2}t_{\rm a}t_{\rm b}\eta_{\rm d}^2+\frac{1}{2}t_{\rm a}t_{\rm b}\eta_{\rm d}^2\Big)\Big],\tag{19}$$

其中, $L$ 是 MERA 结构的层数; $m_l$ 为 MERA 第 $l$ 层所包含的量子比特数, 即该层可提取的密钥比特数; $t_{\rm a}=\eta_{\rm a}(L_{\rm ac})=10^{-\alpha L_{\rm ac}/10}$, $t_{\rm b}=\eta_{\rm b}(L_{\rm bc})=10^{-\alpha L_{\rm bc}/10}$, $L_{\rm ac}$ 和 $t_{\rm a}$ ( $L_{\rm bc}$ 和 $t_{\rm b}$ ) 表示从 Alice (Bob) 到 Charles 的信道距离和传输效率; $P_l^{(\rm A)}$ 和 $P_l^{(\rm B)}$ 分别表示 Alice 与 Bob 端 MERA 的第 $l$ 层解压缩成功的概率; $\eta_{\rm d}$ 是探测器效率; $e_{\rm d}$ 是偏振失配误差; $Y_0$ 是假设与光子脉冲检测无关的背景概率, 包括探测器暗计数和其他背景贡献; $n_{\rm MERA}^{l'}/n_{\rm MERA}^{l}$ 表示每次得到的逻辑比特数占完整 MERA 态信息的比例, 在方案一中, 理想情况下 $n_{\rm MERA}^{l'}=n_{\rm MERA}^{l}$. $P(1)$ 是制备单个 MERA 态的概率; $Y_{\rm rect}^{1,1}$ 是 Charlie 宣布事件成功的概率; $e_{\rm X}^{1,1}$ 是 X 基的误码率; $Q^{\rm rect}$ 和 $E^{\rm rect}$ 分别为 Z 基上的总增益和误码率, 可直接测量[30]. 根据文献 [30] 提出的多强度诱骗态方法, 选择信号和诱骗态的最佳强度值, 以估计 $Y_{\rm rect}^{1,1}$ 和 $e_{\rm X}^{1,1}$ 的取值, 详见 (18) 式和 (19) 式.

误码率纠错效率函数为 $f(E^{\rm rect})>1$, $H_2(E^{\rm rect})$ 和 $H_2(E^{\rm diag})$ 分别对应 Z 基和 X 基的 Shannon 熵, 用来反映量子比特误码率引起的不确定性. 其公式为

$$H_2(x)=-x\log_2x-(1-x)\log_2(1-x).\tag{20}$$

#### 4.1.2 基于 MERA 第 $L-1$ 层压缩纠缠态的 MDI-QKD 协议的密钥生成率

在前述基于 MERA 第 $L$ 层压缩单光子态的 MDI-QKD 协议基础上, 本文进一步考虑 Alice 和 Bob 端使用纠缠态的情形. 与方案一显著不同的是, 方案二中 Alice 和 Bob 分别各自采用 MERA 第 $L-1$ 层的纠缠态, 双方均保留纠缠态中的一个光子用于后续本地测量, 而将另一个光子通过量子信道发送至中继节点 Charlie 执行 BSM. 该过程的本质是纠缠交换, 通过对来自 Alice 和 Bob 的两个独立纠缠对的一半光子进行 BSM, 使得双方保留的本地光子投影至一个确定的纠缠态, 从而建立远程纠缠.

在 MERA 第 $l$ 层, 相邻两点之间的格距 $r(l)$ 为

$$r(l)=b^l,\tag{21}$$

其中, $b$ 为 MERA 的分支因子. 该两点间的相关联度 $C(x,y)$ 服从幂律衰减:

$$C(x,y)\equiv r^{-q},\quad r=r(l)=b^l,\quad q>0,\tag{22}$$

其中, $q$ 为由缩放维度决定的有效幂律指数.

根据文献 [37,38] 和 (22) 式, 误码率 $E_{\rm ent}$ 可建模为

$$E_{\rm ent}=\frac{1}{2}(1-C(x,y)\eta(L)),\tag{23}$$

其中, $\eta(L)$ 是为标准光纤损耗模型下的信道效率.

当 Alice 与 Bob 分别产生 $n$ 对和 $m$ 对纠缠光子时, 成功实现纠缠交换并在双方本地均探测到光子的联合概率如 (24) 式[31]:

$$Y_{n,m}=[1-(1-Y_0)(1-\eta_{\rm a})^n][1-(1-Y_0)(1-\eta_{\rm b})^m]\times[1-(1-Y_0)(1-\eta_{\rm ac})^n][1-(1-Y_0)(1-\eta_{\rm bc})^m],\tag{24}$$

其中, $\eta_{\rm a}$, $\eta_{\rm b}$ 分别为 Alice 与 Bob 的本地探测器效率, $\eta_{\rm ac}=\eta_a(L_{\rm ac})\cdot\eta_{\rm c}$ 和 $\eta_{\rm bc}=\eta_b(L_{\rm bc})\cdot\eta_{\rm c}$ 表示从 Alice 和 Bob 到 Charlie 的信道传输效率与 Charlie 端探测器效率的乘积, $Y_0$ 为探测器暗计数概率.

根据文献 [30], 在渐近条件下, 单对纠缠光子在 X 基下的误码率 $e_{\rm ent}^{1,1}$ 为

$$e_{\rm ent}^{1,1}=\frac{1}{2}-\frac{\eta_{\rm ac}\eta_{\rm bc}\eta_{\rm a}\eta_{\rm b}(1-e_{\rm d})^2(1-Y_0)^2}{4Y_{1,1}}.\tag{25}$$

综上, 在渐近情况下, 基于 MERA 第 $L-1$ 层压缩纠缠态的 MDI-QKD 协议的密钥生成率可由 (26) 式给出[30,31]:

$$R_{\text{ent}}=\sum_{l=1}^{L} m_l P_l^{(\text{A})} P_l^{(\text{B})} \frac{n_{\text{MERA}}^{l''}}{n_{\text{MERA}}^{l}}\Big[P(1)Y_{1,1}(1-H_2(e_{\text{ent}}^{1,1}))$$
$$-Q_{\text{ent}} f(E_{\text{ent}}) H_2(E_{\text{ent}})\Big], \tag{26}$$

其中, $L$ 是 MERA 结构的层数; $m_l$ 为 MERA 第 $l$ 层所含量子比特数; $P_l^{(\text{A})}$ 和 $P_l^{(\text{B})}$ 分别为 Alice 和 Bob 端 MERA 第 $l$ 层的解压缩成功率; $Q_{\text{ent}}^{1,1}$ 和 $e_{\text{ent}}^{1,1}$ 是 Alice 与 Bob 各自产生一对纠缠光子时的增益和误码率; $Q_{\text{ent}}$ 和 $E_{\text{ent}}$ 是总增益和误码率; $P(1)$ 是制备单个 MERA 态的概率, 详见 (15) 式; $n_{\text{MERA}}^{l''}/n_{\text{MERA}}^{l}$ 表示每次得到的逻辑比特数占完整 MERA 态信息的比例, 在方案二中, MERA 解压缩是从 $L-1$ 层开始, 故 $n_{\text{MERA}}^{l''}=n_{\text{MERA}}^{l}-1$.

#### 4.1.3 混合模式密钥生成率

在混合模式下, 系统的整体密钥生成率 $R_{\text{hybrid}}$ 为方案一与方案二的加权和, 其表达式为

$$R_{\text{hybrid}}=pR_{\text{single}}+(1-p)R_{\text{entangled}}, \tag{27}$$

其中, $R_{\text{single}}$ 与 $R_{\text{entangled}}$ 分别由 (17) 式与 (26) 式给出; $p$ 为动态调度概率, 由调度函数 (7) 式所决定.

### 4.2 编码容量

编码容量 (encoding capacity) 是衡量 QKD 协议信息传输效率的重要指标, 其定义为单次成功探测事件所能承载的经典密钥比特数. 在本文中指在一次成功的联合探测事件后, 通信双方基于 MERA 层级结构, 在满足无条件安全条件下, 所能提取的有效密钥比特数的理论上界. 这一上界的提升, 源于 MERA 结构使得单次探测事件能够解锁多个层级的编码信息.

在经典 MDI-QKD 协议中, 每个成功传输的光子最多可生成 1 比特密钥, 假设通信双方共发送 $n$ 个光子 (Alice 与 Bob 各发送 $n/2$ 个), 其有效编码容量为

$$K_{\text{effective}}^{\text{MDI-QKD}}=\frac{n}{2}\cdot P_{\text{basis}}, \tag{28}$$

其中, $P_{\text{basis}}$ 是通信双方均选择 Z 基的概率, $K_{\text{effective}}^{\text{BB84}}$ 为产生的有效比特数.

本文所提出基于 MERA 的 MDI-QKD 协议, 其核心优势在于利用 MERA 的层级纠缠结构对量子信息进行压缩编码, 通过解压缩可逐层提取密钥, 使得每一对成功探测的光子能够提取出多个层级的经典密钥信息. 由于方案一、方案二、方案三的编码核心机制相同, 仅在传输的量子态类型上存在差异, 因此统一建立编码容量模型. 则基于 MERA 的 MDI-QKD 协议的有效编码容量可表示为

$$K_{\text{effective}}^{\text{MERA}}=\sum_{i=1}^{n/2}\sum_{l=1}^{L} m_{il}\cdot P_l^{(\text{A})}\cdot P_l^{(\text{B})}\cdot P_{\text{basis}}, \tag{29}$$

其中, $n$ 为 Alice 与 Bob 各自发送的光子数; $m_{il}$ 表示第 $i$ 个光子对应的 MERA 态在第 $l$ 层解压缩后所能提取的有效密钥比特数; $P_l^{(\text{A})}$ 和 $P_l^{(\text{B})}$ 分别为 Alice 和 Bob 端在 MERA 第 $l$ 层解压缩成功的概率; $L$ 是 MERA 结构的总层数; $P_{\text{basis}}$ 是通信双方均选择 Z 基的概率.

### 4.3 实验

本文的比较基准为渐近安全框架下采用标准三强度诱骗态的经典 MDI-QKD 协议[16] 与混合源 MDI-QKD 协议[39], 二者与本文共享相同的安全框架、诱骗态方案及标准器件参数模型 (0.2 dB/km 光纤损耗、典型探测效率与暗计数率), 确保对比的公平性与有效性. 需说明的是, Liu 等[40] 报道的 442 km MDI-QKD 实验是有限码长下的工程化里程碑成果, 其定制化高性能器件配置与极限距离优化目标, 与本文聚焦的“编码方案理论性能探索”存在定位差异, 因此未直接纳入对比. 该实验为 MDI-QKD 的远距离实用化奠定了重要基础, 本文方案与其实验成果具有显著互补性, 未来可结合有限码长优化与高性能器件技术, 进一步拓展 MERA-MDI-QKD 的远距离应用潜力.

为了更直观地展示仿真结果, 本文仿真采用底层量子数为 128, 层数 $L=6$ 的 4 种构型不同的 MERA 态, 并采用标准的对称信道模型. 仿真所采用的核心参数见表 4, 数据源自文献 [16,30,36,38,41]. 其中, $p$ 是调度函数权重系数; $q$ 是 MERA 第 $L-1$ 层相邻两光子相关联度的幂律指数; $P_{\text{fus}}$ 是 MPS 态的单次融合成功率; $f_{\text{e}}$ 是纠错效率因子; $Y_0$ 是探测器暗计数概率; $e_{\text{d}}$ 是探测器固有错误率, $\eta_{\text{d}}$ 是探测器效率, 本文假设 Alice, Bob 和 Charlie 的探测器效率都相等 $\eta_{\text{a}}=\eta_{\text{b}}=\eta_{\text{c}}=\eta_{\text{d}}$.

表 4 仿真参数

Table 4. Simulation parameters.

| $\eta_{\text{d}}$ | $e_{\text{d}}$ | $Y_0$ | $f_{\text{e}}$ | $P_{\text{fus}}$ | $q$ | $p$ |
|---|---|---|---|---|---|---|
| 14.5% | 1.5% | $6.02\times10^{-6}$ | 1.16 | 98.4% | 0.35 | 50% |

图 5 展示了不同 MDI-QKD 协议在 0—400 km 通信距离下的密钥生成率变化趋势. 其中横轴为 Alice 与 Bob 之间的总通信距离, 纵轴为每脉冲产生的密钥比特数. 蓝色实线表示文献 [16] 所提出的经典 MDI-QKD 协议; 绿色实线表示文献 [39] 提出的多模干涉建模框架下采用混合源的 MDI-QKD, 即一方使用弱相干脉冲 (weak coherent pulse, WCP) 源, 而另一方使用自发参数下转换 (spontaneous parametric down-conversion, SPDC) 源; 橙色、红色和紫色实线分别表示本文提出的基于 MERA 态第 $L$ 层压缩单光子态的 MDI-QKD、基于 MERA 态第 $L-1$ 层压缩纠缠态的 MDI-QKD 和混合模式下的 MDI-QKD.

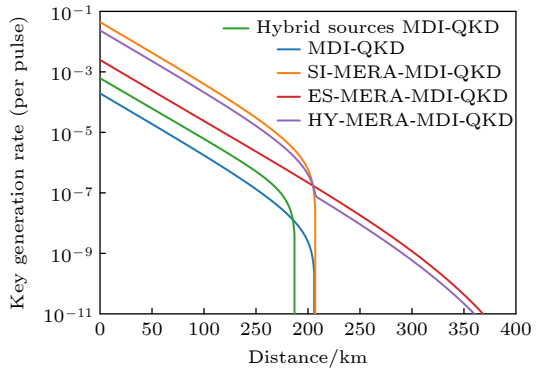


图 5 不同 MDI-QKD 协议密钥生成率随距离变化的情况

Fig. 5. Key generation rate versus distance for different MDI-QKD protocols.

从图 5 可以看出, 所有协议的密钥生成率均随通信距离的增大呈衰减趋势. 经典 MDI-QKD 在中短距离具有一定的密钥生成率, 但衰减速率较快, 在 205 km 左右密钥生成率已趋近于零, 无法生成有效密钥. 混合源 MDI-QKD 在 0—180 km 性能较优于 MDI-QKD, 但其密钥生成率在 180 km 后快速衰减, 长距离通信能力仍未突破. 而本文所提出的 SI-MERA-MDI-QKD 在 0—200 km 范围内展现出最高的密钥生成率. 以 150 km 为例, MDI-QKD 的密钥生成率约为 $1.324\times10^{-7}$ bit/pulse, SI-MERA-MDI-QKD 的密钥生成率约为 $3.036\times10^{-5}$ bit/pulse, 较 MDI-QKD 提高了约 22931% 的密钥率. ES-MERA-MDI-QKD 在 0—200 km 的通信能力虽低于其他两个基于 MERA 的 MDI-QKD 方案, 但其衰减趋势最为平缓, 在 350 km 处仍能维持超过 $10^{-11}$ bit/pulse 的有效密钥生成率, 将有效通信距离拓展至 350 km 以上. HY-MERA-MDI-QKD 融合了 SI-MERA-MDI-QKD 和 ES-MERA-MDI-QKD 的优势, 既在中短距离具备与 SI-MERA-MDI-QKD 相当的高密钥生成率, 又能在长距离保持与 ES-MERA-MDI-QKD 近似的缓慢衰减特性.

图 6 展示了不同 MDI-QKD 协议在通信距离为 50 km, 100 km, 200 km 和 300 km 下的密钥生成率, 清晰地呈现了各协议在特定距离点上的性能差异. 在通信距离为 50 km 和 100 km 时, 本文提出的 3 种基于 MERA 的 MDI-QKD 方案的柱高远高于其余方案, SI-MERA-MDI-QKD(橙色柱) 与 HY-MERA-MDI-QKD(红色柱) 处于最高梯队水平, ES-MERA-MDI-QKD(绿色柱) 次之. 在 200 km 处, 基于 MERA 的 MDI-QKD 方案与其余方案出现明显“断层”, MDI-QKD(蓝色柱) 的密钥生成率已降至 $2.396\times10^{-9}$ bit/pulse, 混合源 MDI-QKD (紫色柱) 已逼至零区, 难以给出有效密钥. 而 3 种基于 MERA 的 MDI-QKD 协议仍能维持在同一数量级 $10^{-7}$ bit/pulse 的有效密钥生产率 (各柱高度明显非零). 在 300 km 处, 仅 ES-MERA-MDI-QKD (绿色柱) 和 HY-MERA-MDI-QKD(红色柱) 仍保持有效密钥生成率, 其余协议均已无法产生有效密钥.

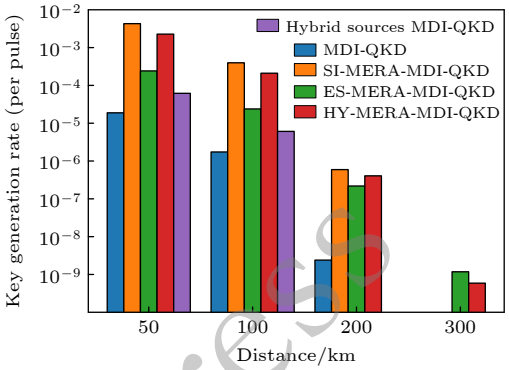


图 6 不同 MDI-QKD 协议在 50 km, 100 km, 200 km 和 300 km 时, 密钥生成率的变化情况

Fig. 6. Key generation rate at 50, 100, 200, and 300 km for different MDI-QKD protocols.

图 7 给出了探测器效率 $\eta_{\rm d}=0.1$, 0.2, 0.3, 0.4 时, 各 MDI-QKD 协议密钥生成率随通信距离变化的情况. 随着 $\eta_{\rm d}$ 的提高, 所有协议的密钥生成率曲线整体上移, 且拐点距离右移, 通信距离得以拓展. 同时, 在任意 $\eta_{\rm d}$ 条件下, 基于 MERA 的 3 种方案的密钥生成能力始终优于对比方案, 且 HY-MERA-MDI-QKD(紫色曲线) 和 ES-MERA-MDI-QKD(红

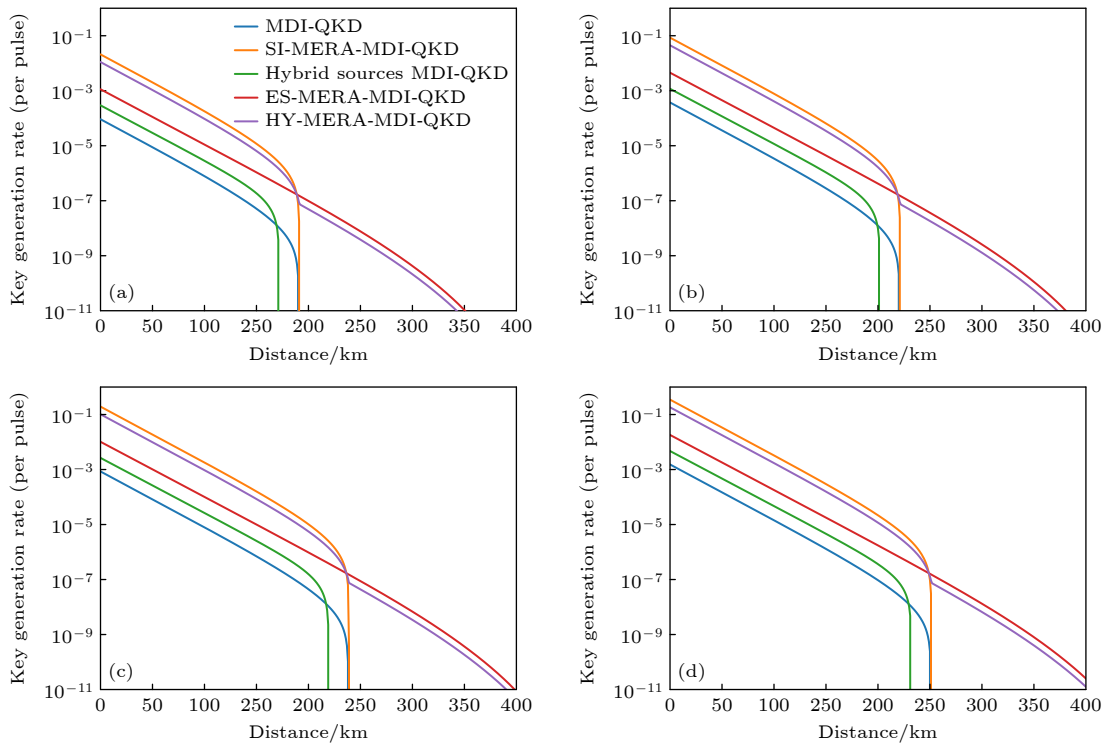


图 7 不同探测器效率下密钥生成率随通信距离变化的情况 (a) 探测器效率为 0.1; (b) 探测器效率为 0.2; (c) 探测器效率为 0.3; (d) 探测器效率为 0.4

Fig. 7. Key generation rate as a function of communication distance for different detector efficiencies: (a) Detector efficiency = 0.1; (b) detector efficiency = 0.2; (c) detector efficiency = 0.3; (d) detector efficiency = 0.4.

色曲线) 的有效通信距离更远. 以 $\eta_{\rm d}=0.3$ 为例, SI-MERA-MDI-QKD(橙色曲线) 在 0—240 km 时曲线始终保持最高密钥率, HY-MERA-MDI-QKD 和 ES-MERA-MDI-QKD 次之. 同时, HY-MERA-MDI-QKD 和 ES-MERA-MDI-QKD 在 400 km 时仍能保持 $10^{-11}$ bit/pulse 以上的有效密钥生成率, 相比之下, 其他协议在不到 210 km 时有效密钥生成就已终止.

图 8 给出了信道损耗为 0.1 dB/km, 0.2 dB/km, 0.3 dB/km, 0.4 dB/km 时, 不同 MDI-QKD 协议密钥生成率随通信距离变化的情况. 如图 8 所示, 随着信道损耗增大, 所有协议的密钥率曲线拐点均呈现左移趋势, 且最大通信距离相应缩短. 尽管如此, 在所有测试的损耗条件下, 基于 MERA 的 MDI-QKD 方案在密钥生成性能上始终优于对比方案. 以 0.4 dB/km 的信道损耗为例: 在 0—100 km 范围内, SI-MERA-MDI-QKD(橙色曲线) 的密钥生成率始终处于最高水平, HY-MERA-MDI-QKD(紫色曲线) 和 ES-MERA-MDI-QKD(红色曲线) 次之. 同时, 经典 MDI-QKD 在约 100 km 处已无法生成有效密钥, 而 HY-MERA-MDI-QKD 与 ES-MERA-MDI-QKD 在 170 km 处仍可维持约 $10^{-11}$ bit/pulse 的密钥生成率.

图 9 给出在 3 种误码率条件 (QBER = 0%, 8%, 10%) 下基于 MERA 的 MDI-QKD 协议与文献 [16] 的 MDI-QKD 协议的经典比特编码量随传输的总光子数 (包含诱骗态) 变化的情况. 整体来看, 不论在无误码还是有误码环境中, MERA-MDI-QKD 的曲线始终位于经典 MDI-QKD 协议之上, 并且随着光子数线性增长, 两者的差距不断扩大. 例如, 当发送光子数为 500 时, MERA-MDI-QKD 在 QBER = 0 条件下可编码约 27610 个经典比特, 而经典 MDI-QKD 仅能编码约 125 个经典比特, 编码能力提高了近 221 倍. 即使在 QBER = 10% 时, MERA-MDI-QKD 协议仍可编码高于 24890 个经典比特, 而经典 MDI-QKD 协议仅编码 113 比特. MERA-MDI-QKD 利用其分层 MERA 结构, 可使每个光子编码 2—3 个经典比特的信息. 随着层级数目的增加, 每个成功解压缩的光子可能编码更多经典比特的信息, 这使得 MERA-MDI-QKD 协议的编码能力远超 MDI-QKD 协议. 但这种提高并非无限的, 增加层数 $L$ 会面临边际效益递减和更高的实现复杂度, 而且低层纠缠更易受噪声影响, 因此在实际中需要权衡 $L$ 的选择.

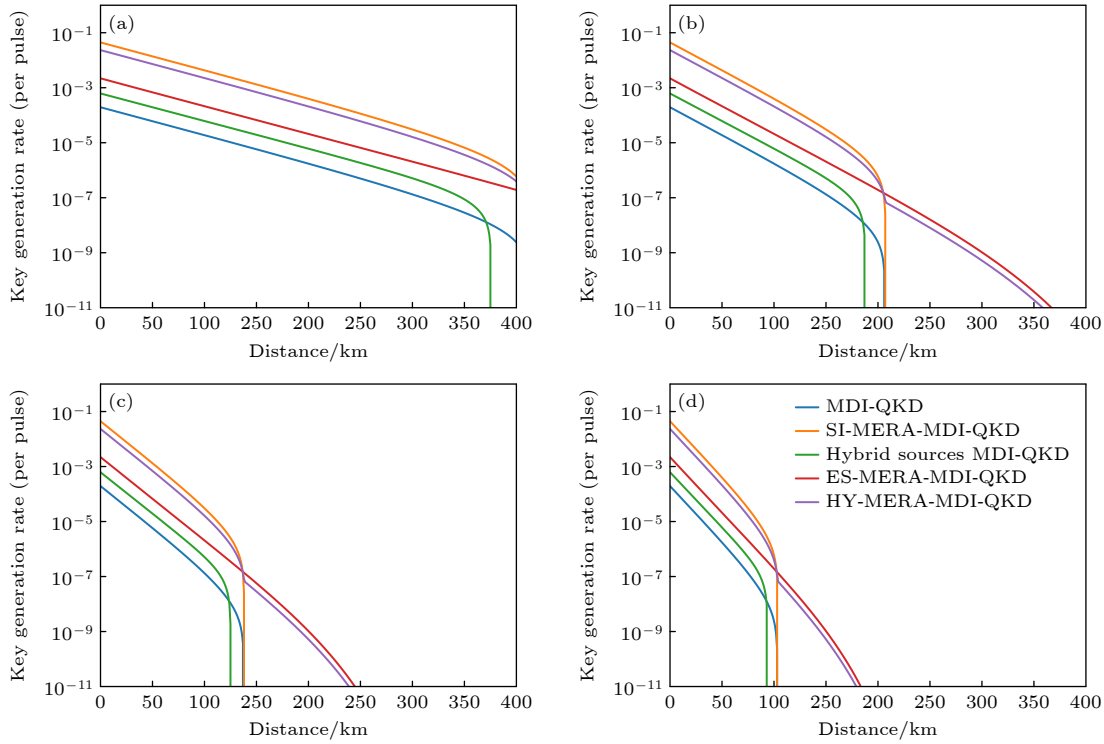


图 8 不同信道损耗下密钥生成率随通信距离变化的情况 (a) 0.1 dB/km; (b) 0.2 dB/km; (c) 0.3 dB/km; (d) 0.4 dB/km

Fig. 8. Key generation rate as a function of communication distance under different channel losses: (a) 0.1 dB/km; (b) 0.2 dB/km; (c) 0.3 dB/km; (d) 0.4 dB/km.

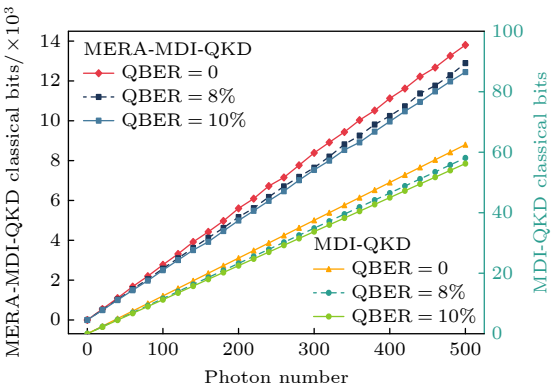


图 9 文献 [16] 所提出的 MDI-QKD 与基于 MERA 的 MDI-QKD 编码能力随总传输光子数变化的情况

Fig. 9. The variation of the coding capacity of MDI-QKD proposed in Ref. [16] and MERA-based MDI-QKD with the total number of transmitted photons.

综合上述仿真结果, 基于 MERA 的 MDI-QKD 协议在密钥生成率、通信距离上限和鲁棒性上全面超越经典 MDI-QKD 方案. 其中, SI-MERA-MDI-QKD 中短距离 (0—200 km) 性能最优, 密钥率高. ES-MERA-MDI-QKD 长距离 (大于 200 km) 性能最优, 抗噪声能力强. HY-MERA-MDI-QKD 实现全距离性能均衡, 为不同场景下的量子保密通信提供了多维度的技术支撑, 显著推动了 MDI-QKD 的实用化进程.

需要特别说明的是, 本文的数值仿真旨在从原理上揭示基于 MERA 的 MDI-QKD 协议相对于传统协议在密钥率与传输距离上的理论潜力与性能上限. 因此, 当前的仿真模型主要考虑了信道传输的损耗与探测器的固有参数, 尚未将 MERA 物理实现所引入的附加器件损耗显式地纳入总信道效率的计算框架. 实现相关的器件损耗模型化, 并在此基础上重新优化协议参数与系统架构, 是本研究一个明确且重要的后续拓展方向.

## 5 安全分析

本节旨在系统分析本文所提出的 3 种基于 MERA 的 MDI-QKD 方案在面对典型攻击模型 (集体攻击、拦截-重发攻击、特洛伊木马攻击) 时的安全性.

### 5.1 集体攻击

在集体攻击中, 攻击者 (Eve) 对量子信道中的每一次传输独立执行相同的联合操作, 在协议执行

完毕后进行集体测量以获取最大信息量. 在基于MERA 的 MDI-QKD 协议中, 由于采用了 MERA 的多层纠缠结构, 每个发送的量子态实质上编码了多个比特的冗余信息, 这种内在的冗余特性增强了对集体攻击的鲁棒性.

#### 5.1.1 基于 MERA 第 $L$ 层压缩单光子态的 MDI-QKD 在集体攻击下的安全性分析

在方案一中, Alice 和 Bob 在 MERA 的第 $L$ 层将多比特信息压缩为单光子态 $|\varphi_0\rangle$ 或 $|\varphi_1\rangle$ 进行发送, 并随机插入诱骗态 $|\varphi^+\rangle$ 或 $|\varphi^-\rangle$ 用于窃听检测. Eve 的集体攻击可建模为在两个信道上分别实施酉操作 $U_{\rm AE}$ 与 $U_{\rm BE}$, 并引入其初始辅助态 $|0\rangle_{e1}$ 与 $|0\rangle_{e2}$. 设 $|\varepsilon_{ji}\rangle_{e1}$ 与 $|\tau_{\ell k}\rangle_{e2}$ 分别为 Eve 在 Alice 与 Bob 信道攻击后的辅助态分量. 攻击过程可形式化表示为

$$E_1:|\varphi_i\rangle_{\rm A}|0\rangle_{e1}\xrightarrow{U_{\rm AE}}\sum_{j=0}^{1}|\varphi_j\rangle_{\rm A}|\varepsilon_{ji}\rangle_{e1},\tag{30}$$

$$E_2:|\varphi_k\rangle_{\rm B}|0\rangle_{e2}\xrightarrow{U_{\rm BE}}\sum_{l=0}^{1}|\varphi_l\rangle_{B}|\tau_{lk}\rangle_{e2},\tag{31}$$

其中 $i,k\in0,1$ 表示 Alice 或 Bob 发送的量子态的基矢指标, 而 $j,l$ 表示 Eve 干扰后可能导致的信号态塌缩分支. 成功的 Bell 态测量将整个复合系统(包括 Eve 的辅助系统) 的量子态投影到满足关联条件的子空间, 可记理想纠缠态为

$$|\Phi\rangle_{\rm AB}=\frac{1}{\sqrt{2}}\left(|\varphi_0\rangle_{\rm A}|\varphi_0\rangle_{\rm B}+|\varphi_1\rangle_{\rm A}|\varphi_1\rangle_{\rm B}\right).\tag{32}$$

在 Eve 实施攻击后, 全局量子态演化为

$$|\alpha^{(1)}_{{\rm AB}e1e2}\rangle=(U_{\rm AE}\otimes U_{\rm BE})(|\Phi\rangle_{\rm AB}|0\rangle_{e1}|0\rangle_{e2}).\tag{33}$$

若 Charlie 成功测得纠缠关联, 即投影满足 $\langle\Phi|\alpha^{(1)}_{{\rm AB}e1e2}\rangle=0$. 若要避免引入误码, 必须满足对于所有 $i\neq j$ 或 $k\neq l$ 都有:

$$\langle\tau_{lk}|\varepsilon_{ji}\rangle=0.\tag{34}$$

综上, 当且仅当零误码事件时, Eve 各辅助态分量间相互正交. 这意味着在误码率为零时, Eve 无法从其辅助系统中获取任何关于原始密钥比特的区分信息. 反之, 若 Eve 试图通过使其辅助态非正交来窃取信息, 则必然破坏上述条件, 从而导致出现误码, 进而被合法通信方所察觉. 因此, 方案一在集体攻击下是无条件安全的: 任何窃听行为都将转化为可观测的误码率提升, 从而确保密钥的安全性.

#### 5.1.2 基于 MERA 第 $L-1$ 层压缩即纠缠态的 MDI-QKD 在集体攻击下的安全性分析

在方案二中, Alice 与 Bob 分别使用 MERA 的第 $L-1$ 层压缩纠缠态. Alice 使用以下两种形式之一:

$$|\Phi^+\rangle_{\rm A_1A_2}=(|0\rangle_{\rm A_1}|0\rangle_{\rm A_2}+|1\rangle_{\rm A_1}|1\rangle_{\rm A_2})/\sqrt{2},$$

$$|\Psi^+\rangle_{\rm A_1A_2}=(|0\rangle_{\rm A_1}|1\rangle_{\rm A_2}+|1\rangle_{\rm A_1}|0\rangle_{\rm A_2})/\sqrt{2}.$$

Bob 使用以下两种形式之一:

$$|\Phi^+\rangle_{\rm B_1B_2}=(|0\rangle_{\rm B_1}|0\rangle_{\rm B_2}+|1\rangle_{\rm B_1}|1\rangle_{\rm B_2})/\sqrt{2},$$

$$|\Psi^+\rangle_{\rm B_1B_2}=(|0\rangle_{\rm B_1}|1\rangle_{\rm B_2}+|1\rangle_{\rm B_1}|0\rangle_{\rm B_2})/\sqrt{2}.$$

Alice 和 Bob 分别保留粒子 $\rm A_1$ 和 $\rm B_1$, 将粒子 $\rm A_2$ 和 $\rm B_2$ 通过量子信道发送至 Charlie. Eve 在 Alice → Charlie 与 Bob → Charlie 信道上实施集体攻击:

$$E_1:|\varphi_i\rangle_{\rm A_2}|0\rangle_{e1}\xrightarrow{U_{\rm A_2E}}\sum_{j=0}^{1}|\varphi_j\rangle_{\rm A_2}|\varepsilon_{ji}\rangle_{e1},\tag{35}$$

$$E_2:|\varphi_k\rangle_{\rm B_2}|0\rangle_{e2}\xrightarrow{U_{\rm B_2E}}\sum_{l=0}^{1}|\varphi_l\rangle_{\rm B_2}|\tau_{lk}\rangle_{e2}.\tag{36}$$

此时 Alice 和 Bob 粒子以及两个辅助粒子在内的整个系统都处于:

$$|\alpha^{(1)}_{{\rm A_2B_2}e1e2}\rangle=(U_{\rm B_2E}\otimes U_{\rm B_2E})(|\varphi_i\rangle_{\rm A_2}|\varphi_k\rangle_{\rm B_2}|0\rangle_{e1}|0\rangle_{e2}).\tag{37}$$

若 Charlie 成功测得纠缠关联, 即投影满足 $\langle\Phi|\alpha^{(1)}_{{\rm A_2B_2}e1e2}\rangle=0$. 若要避免引入误码, 任意 $i\neq j$ 或 $k\neq\ell$ 都有:

$$\langle\tau_{lk}|\varepsilon_{ji}\rangle=0.\tag{38}$$

因此, 方案二对集体攻击同样满足“无误码则无信息”的安全准则. 值得注意的是, 由于本方案中 Charlie 本身并不值得信任, 若其故意公布错误的测量结果, 也会在诱骗态检测中出现超出阈值的误码率而被立即发现.

#### 5.1.3 基于混合模式的 MDI-QKD 在集体攻击下的安全性分析

混合方案在每轮发送时随机选择使用方案一的压缩单光子态或方案二的压缩纠缠态, 这种随机切换本质上引入了额外的混淆机制: Eve 无法预知

每轮通信所使用的编码类型, 从而难以优化统一的攻击策略.

方案三中 Eve 能够获得的最大信息量为

$$I_{\mathrm{E}}^{(3)} = pI_{\mathrm{E}}^{(1)} + (1-p)I_{\mathrm{E}}^{(2)}, \tag{39}$$

其中, $p$ 是使用方案一的概率; $I_{\mathrm{E}}^{(1)}$ 和 $I_{\mathrm{E}}^{(2)}$ 分别为方案一和方案二中 Eve 可获得的最大信息量. 由于方案一和方案二均已证明在零误码条件下 Eve 无法获取有效信息, 因此方案三在零误码条件下同样能保证 $I_{\mathrm{E}}^{(3)}$ 为零的安全水平.

混合模式不仅保持了前两种方案的安全特性, 还通过随机切换增加了 Eve 的攻击不确定性. 例如 Eve 尝试攻击单光子却遇到纠缠态轮次, 将更难还原有效信息. 此外, 协议可根据实时监测的误码率动态调整编码方案, 当检测到误码率异常升高时, 可自适应地增加抗干扰能力更强的纠缠态使用比例, 从而进一步降低信息泄漏风险.

## 5.2 拦截–重发攻击

### 5.2.1 基于 MERA 第 $L$ 层压缩单光子态的 MDI-QKD

1) **信源结构**: Alice 与 Bob 在 MERA 第 $L$ 层将多比特信息压缩至单光子态 $\{|\phi_0\rangle, |\phi_1\rangle\}$, 并随机插入诱骗态 $\{|\phi_+\rangle, |\phi_-\rangle\}$.

2) **Eve 的拦截-重发**: Eve 拦截每个光子, 随机选取 Z 基或 X 基进行测量, 然后根据测量结果制备相应态重发给 Charlie.

3) **误码率分析**: 当 Eve 选择的测量基与发送方不一致时 (概率约为 50%), 有 50% 的概率导致其测量结果与原始量子态不相符, 导致重发后 Charlie 的 Bell 态测量结果错误; 在安全检测回合, Alice 与 Bob 通过公开比较会比较在所有诱骗态轮次上的测量结果, 能够识别出异常的误码率. 若存在拦截-重发攻击, 检测到的误码率将显著超过协议安全阈值.

综上, 在方案一中, 任何拦截-重发攻击都会导致误码率超过安全阈值, Alice 与 Bob 可通过监测到的异常误码率及时终止协议并丢弃相关数据, 从而保证密钥安全性.

### 5.2.2 基于 MERA 第 $L-1$ 层压缩纠缠态的 MDI-QKD

在方案二中, 当 Eve 截获 Alice 或 Bob 发送的纠缠光子 (分别为 $\mathrm{A}_2$ 或 $\mathrm{B}_2$) 并进行测量时, 会不可避免地破坏原始的纠缠关系. 随后, Eve 面临两种重发策略的选择.

1) **重发单光子态**: Eve 根据测量获得的量子比特信息, 制备对应的单光子态并发送给 Charlie. 然而, 此操作破坏了 Alice 和 Bob 原本应建立的纠缠关联, Charlie 的 BSM 将难以观察到有效纠缠事件.

2) **重发纠缠态**: Eve 企图“伪造”一个纠缠态光子, 即让重发光子与发送方保留的另一个光子保持某种纠缠, 以进行有效的 BSM. 但由于 Eve 无法获取 Alice 与 Bob 共享纠缠对的完整信息, 实际上不可能制备出与原始纠缠态一致的量子态.

因此, 无论 Eve 采取何种重发策略, 其恢复原始纠缠性的概率都是极低的. 在窃听检测中, 由于 Eve 的破坏, Alice 和 Bob 要么观测到纠缠关联的严重丢失 (比如 Charlie 几乎未测到有效纠缠态), 要么观测到误码率远高于阈值 $Q_{\mathrm{th}}$. 发现这两种异常, Alice 和 Bob 都将终止协议并丢弃所有数据.

### 5.2.3 基于 MERA 的混合模式的 MDI-QKD

混合模式通过随机切换编码方案进一步增强了协议的抗攻击能力. Eve 在不知道当轮是方案一还是方案二的情况下, 难以选择最佳的应对策略. 如果 Eve 当作单光子态而进行测量, 但实际上该轮是纠缠态时, 其操作等价于对纠缠对的一半做测量, 正如上述方案二分析, 将立即破坏纠缠关联并被检测, 反之亦然. 如果 Eve 尝试针对两种情况分别优化策略, 例如先进行某种可以同时涵盖单光子和纠缠态的联合测量, 由于这两类态在 Hilbert 空间中的表示差异 (一个是单体态, 一个是二体纠缠态), 但目前不存在一种测量能在不降低正确判别率的前提下兼容两者. Alice 和 Bob 在公开比较随机插入的单光子诱骗态和纠缠诱骗态结果, 发现异常的误码率或关联丢失率即可判定有攻击行为发生.

## 5.3 特洛伊木马攻击

特洛伊木马攻击 (Trojan-horse attack, THA) 是指 Eve 向 Alice(或 Bob) 端口注入强相干脉冲, 并收集调制器反射以及散射光以窃取部分信息. 攻击目标是要发送到信道上的光子. 该攻击的核心特征在于: Eve 试图在不干扰正常量子信道传输的前

提下, 通过光学副通道获取密钥, 从而绕过量子态本身的随机性防御.

根据第 4.1.1 节中介绍的基于压缩单光子的 MERA-MDI-QKD 协议模型, 以及 Tan 等 [42] 对 MDI-QKD-THA 的严格分析, 本文将 THA 引入 MERA-MDI-QKD 协议, 对单光子 X 基误码率和增益进行修正, 得到如 (40) 式所示的密钥生成率下界:

$$\begin{aligned} R_{\mathrm{si}}^{\mathrm{THA}} \geqslant & \sum_{l=1}^{L} m_l P_l^{(\mathrm{A})} P_l^{(\mathrm{B})} \frac{n_{\mathrm{MERA}}^{l'}}{n_{\mathrm{MERA}}^{l}} \\ & \times \left[ P(1) Y_{\mathrm{rect}}^{1,1} \left(1 - H_2(e_{\mathrm{X,T}}^{1,1})\right) \right. \\ & \left. - Q^{\mathrm{rect}} f\left(E^{\mathrm{rect}}\right) H_2\left(E^{\mathrm{rect}}\right) \right], \end{aligned} \tag{40}$$

其中, $n_{\mathrm{MERA}}^{l'}/n_{\mathrm{MERA}}^{l}$ 表示每次得到的逻辑比特数占完整 MERA 态信息的比例; $P_l^{(\mathrm{A})}, P_l^{(\mathrm{B})}$ 表示 Alice 和 Bob 端 MERA 第 $l$ 层解压缩成功概率; $P(1)$ 是制备单个 MERA 态的概率; $Y_{\mathrm{rect}}^{1,1}$ 是 Charlie 宣布事件成功的概率; $e_{\mathrm{X,T}}^{1,1}$ 表示考虑 THA 后的误码率; $Q^{\mathrm{rect}}$ 和 $E^{\mathrm{rect}}$ 分别表示 Z 基上的总增益与总误码率. 基于压缩纠缠态的 MERA-MDI-QKD 类似, 将 $e_{\mathrm{ent}}^{1,1}$ 替换为考虑 THA 后的误码率.

将 THA 模型纳入考虑时, THA 引入的偏差可以用迹距离来确定 (同样适用于纠缠对), THA 引入的误差为

$$\begin{aligned} e_{\mathrm{X,T}}^{1,1} = & e_{\mathrm{X}}^{1,1} + 4\Delta'(1-\Delta')(1-2e_{\mathrm{X}}^{1,1}) \\ & + 4\sqrt{\Delta'(1-\Delta')e_{\mathrm{X}}^{1,1}(1-e_{\mathrm{X}}^{1,1})}, \end{aligned} \tag{41}$$

$$\Delta = \frac{1}{2}\left[1 - \mathrm{e}^{(-2\mu_{\mathrm{out}})} \cos^2(\mu_{\mathrm{out}})\right], \tag{42}$$

$$\Delta' = \Delta / Y_{\mathrm{rect}}^{1,1}, \tag{43}$$

其中, $e_{\mathrm{X}}^{1,1}$ 表示无攻击情形下误码率; $\mu_{\mathrm{out}}$ 表示 Eve 向 Alice 或 Bob 注入并反射回的平均光子数; $\Delta$ 表示由 THA 引入的迹距离偏差; 由此, 可直接将 (41) 式中的 $e_{\mathrm{X,T}}^{1,1}$ 代入 (40) 式, 得到 THA 下的 MERA-MDI-QKD 协议的安全速率下界.

为评估本文提出的基于 MERA 的 MDI-QKD 协议对 THA 的抵抗能力, 本文通过数值仿真分析了在 THA 存在下的安全密钥生成率. 已有研究表明, 相较于相位调制器, 强度调制器导致的信息泄漏对密钥率的影响更为显著 [42,43]. 因此, 本文采用每个脉冲从强度调制器反射的特洛伊木马光子平均数为 $\mu_{\mathrm{THA}} = 1.818 \times 10^{-12}$ 的数据进行仿真, 结果如图 10 所示.

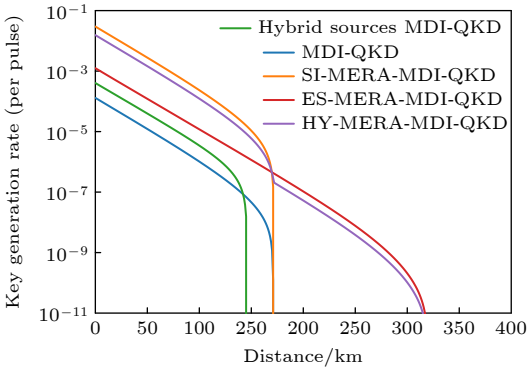


图 10 考虑 THA 后, 不同 MDI-QKD 协议的密钥生成率随通信距离的变化情况

Fig. 10. Dependence of key generation rate on communication distance for different MDI-QKD protocols considering Trojan-horse attacks.

图 10 给出了考虑 THA 后, 不同 MDI-QKD 协议的密钥生成率随通信距离的变化情况. 如图 10 所示, 各协议的密钥生成率随通信距离的增大而逐渐下降. 在 $\mu_{\mathrm{out}} = 1.818 \times 10^{-12}$ 的 THA 下, 经典 MDI-QKD(蓝色曲线) 的密钥生成率在约 170 km 处迅速下降, 混合源 MDI-QKD(绿色曲线) 的密钥生成率在约 145 km 处迅速下降, 二者对 THA 更为敏感. 在相同的 THA 条件下, 基于 MERA 第 $L$ 层压缩单光子态的 MDI-QKD(橙色曲线) 的有效密钥生成率虽也在约 170 km 处迅速下降, 但其在 0—170 km 时的密钥生成率均较经典 MDI-QKD 高出两个数量级, 展现出该方案在中短距离内具有更强的信息泄漏抑制能力和更高的实用价值. 基于 MERA 第 $L-1$ 层压缩纠缠态的 MDI-QKD (红色曲线) 和基于 MERA 的混合模式的 MDI-QKD(紫色曲线) 仍能在相同攻击强度下进一步将传输极限推至约 320 km.

总的来说, 本文提出的基于 MERA 的 MDI-QKD 协议借助 MERA 的多尺度纠缠结构将密钥信息分散到不同层级的纠缠态中, 使 Eve 难以通过单次攻击获取完整密钥, 在面对 THA 时仍能维持较优的安全密钥生成率, 且不同的 MERA 态编码对 THA 防御均优于经典 MDI-QKD 协议.

## 6 总 结

本文提出了 3 种基于 MERA 的 MDI-QKD

方案: 基于 MERA 态第 $L$ 层压缩单光子态的 MDI-QKD、基于 MERA 态第 $L-1$ 层压缩纠缠态的 MDI-QKD 和混合模式下的 MDI-QKD. 在 MDI-QKD 框架下引入 MERA 层级编码, 实现了单个光子对多比特信息的编码传输, 并借助多层保真度校验机制有效增强了协议在噪声信道下的鲁棒性. 本文详细阐述了上述协议的构建原理与流程, 设计了四种 MERA 结构, 并给出了包括量子态制备、Bell 态测量、基筛选、结构比对、信息解码和密钥提取等步骤的完整操作流程. 性能分析结果表明, 相较经典 MDI-QKD 协议, 本文所提出基于 MERA 的 MDI-QKD 协议编码效率提高了近 221 倍. 且基于 MERA 第 $L-1$ 层压缩纠缠态的 MDI-QKD 与混合模式下的 MDI-QKD 两种方案在 350 km 距离处仍能维持有效密钥生成, 将经典 MDI-QKD 协议的有效通信距离拓展了约 150 km.

需要指出的是, 尽管本文在数值仿真中采用的 MERA 结构其底层粒子数为 128, 但已有研究表明可制备底层规模达 243 的大规模 MERA 结构[44]. 随着光学器件与纠缠制备技术等的持续发展, MERA 的规模仍有拓展空间, 可进一步提升本文所提协议的信息承载能力与抗噪声能力.

未来工作将重点开展 MERA-MDI-QKD 的实验实现可行性研究, 包括 MERA 张量网络的物理实现方案、多比特并发纠错算法优化等. 同时, 将本协议中 MERA 编码的核心思想推广至异步 MDI-QKD 等量子密钥分发架构, 以期满足更高速率、更广覆盖范围的量子安全通信需求. 此外, 本文 MERA 联合操作框架具备通用性, 可拓展至 DI-QKD 场景. 未来可聚焦现实器件效率、信道损耗等约束, 探索基于 MERA 的纠缠态优化与贝尔不等式高效检测方案, 助力 DI-QKD 远距离实用化.

## 参考文献


[1] Bennett C H, Brassard G 1984 *In Proceedings of IEEE International Conference on Computers, System and Signal Processing* pp175–179
[2] Ekert A K 1991 *Phys. Rev. Lett.* **67** 661
[3] Zapatero V, Leent T, Arnon-Friedman R, Liu W, Zhang Q, Weinfurter H, Curty M 2023 *npj Quantum Information* **9** 10
[4] Wang W, Lütkenhaus N 2022 *Phys. Rev. Res.* **4** 043097
[5] Ding H J, Liu J Y, Zhou X Y, Zhang C H, Li J, Wang Q 2023 *Phys. Rev. Appl.* **19** 044022
[6] Zhang Y, Ding X, Li Y, et al. 2025 *Phys. Rev. Lett.* **134** 210801
[7] Chen J P, Zhang C, Liu Y, et al. 2020 *Phys. Rev. Lett.* **124** 070501
[8] Wang S, Yin Z Q, He D Y, et al. 2022 *Nat. Photonics* **16** 154
[9] Liu Y, Zhang W J, Jiang C, et al. 2023 *Phys. Rev. Lett.* **130** 210801
[10] Gisin N, Fasel S, Kraus B, Zbinden H, Ribordy G 2006 *Phys. Rev. A* **73** 022320
[11] Brassard G, Lütkenhaus N, Mor T, Sanders B C 2000 *Phys. Rev. Lett.* **85** 1330
[12] Lydersen L, Wiechers C, Wittmann C, Elser D, Skaar J, Makarov V 2010 *Nat. Photonics* **4** 686
[13] Acín A, Brunner N, Gisin N, Massar S, Pironio S, Scarani V 2007 *Phys. Rev. Lett.* **98** 230501
[14] Rosenfeld W, Burchardt D, Garthoff R, Redeker K, Ortegel N, Rau M, Weinfurter H 2017 *Phys. Rev. Lett.* **119** 010402
[15] Woodhead E, Acín A, Pironio S 2021 *Quantum* **5** 443
[16] Lo H K, Curty M, Qi B 2012 *Phys. Rev. Lett.* **108** 130503
[17] Inamori H 2002 *Algorithmica* **34** 340
[18] Vidal G 2007 *Phys. Rev. Lett.* **99** 220405
[19] Lucamarini M, Yuan Z L, Dynes J F, Shields A J 2018 *Nature* **557** 400
[20] Xie Y M, Lu Y S, Weng C X, et al. 2022 *PRX Quantum* **3** 020315
[21] Zeng P, Zhou H, Wu W, Ma X 2022 *Nat. Commun.* **13** 3903
[22] Shao S F, Zhou L, Lin J, Minder M, Ge C, Xie Y M, Shen A, Yan Z, Yin H L, Yuan Z 2025 *Phys. Rev. X* **15** 021066
[23] Perez-Garcia D, Verstraete F, Wolf M M, Cirac J I 2007 *Quantum Info. Comput.* **7** 401
[24] Ran S J 2020 *Phys. Rev. A* **101** 032310
[25] Zhou L, Choi S, Lukin M D 2021 *Phys. Rev. A* **104** 032418
[26] Malz D, Styliaris G, Wei Z Y, Cirac J 2024 *Phys. Rev. Lett.* **13** 2
[27] Cincio L, Dziarmaga J, Rams M M 2008 *Phys. Rev. Lett.* **100** 240603
[28] Lai H, Huang Z, Ren L, Pieprzyk J, Zhao Q, Kwek L 2025 *Phys. Rev. A* **111** 022603
[29] Lai H, Ren L, Huang Z R, Wan L C 2024 *Acta Phys. Sin.* **73** 230301 (in Chinese) [赖红, 任黎, 黄钟锐, 万林春 2024 物理学报 **73** 230301]
[30] Xu F, Curty M, Qi B, Lo H K 2013 *New J. Phys.* **15** 113007
[31] Ma X, Fung C H F, Lo H K 2007 *Phys. Rev. A* **76** 012307
[32] Vidal G 2008 *Phys. Rev. Lett.* **101** 110501
[33] Pomarico D 2023 *Dynamics* **3** 622
[34] Browne D E, Rudolph T 2005 *Phys. Rev. Lett.* **95** 010501
[35] Wei Z Y, Malz D, González-Tudela A, Cirac J I 2021 *Phys. Rev. Res.* **3** 023021
[36] Qi J, Yu C Q, Yuan R Y, Yang Z, Ren B C 2025 *Opt. Laser Technol.* **192** 113385
[37] Scherer A, Sanders B C, Tittel W 2011 *Opt. Express* **19** 3004
[38] Pfeifer R N C, Evenbly G, Vidal G 2009 *Phys. Rev. A* **79** 040301
[39] Deng J J, Lu F Y, Zhong Z Q, et al. 2025 *Phys. Rev. Appl.* **24** 044045
[40] Liu J Y, Ma X, Ding H J, Zhang C H, Zhou X Y, Wang Q 2023 *Phys. Rev. A* **108** 022605
[41] Erkilic O, Conlon L, Shajilal B, Kish S, Tserkis S, Kim Y S, Lam P K, A S 2023 *npj Quantum Inf.* **9** 29
[42] Tan H, Li W, Zhang L, Wei K, Xu F 2021 *Phys. Rev. Appl.* **15** 064038
[43] Lucamarini M, Choi I, Ward M B, Dynes J F, Yuan Z L, Shields A J 2015 *Phys. Rev. X* **5** 031030
[44] Berezutskii A V, Luchnikov I A, Fedorov A K 2025 *Phys. Rev. Res.* **7** 013063

# Measurement-device-independent quantum key distribution based on the multi-scale entanglement renormalization ansatz*

LAI Hong #† WANG Shanshan # HUANG Zhongrui

(*School of Computer and Information Science, Southwest University, Chongqing* 400715, *China*)

( Received 24 October 2025; revised manuscript received 7 December 2025 )

**Abstract**

Measurement-device-independent quantum key distribution (MDI-QKD) has attracted widespread attention due to its effective defense against attacks on the detection side. However, its key generation rate is limited by the success probability of two-photon interference, which drops sharply under high channel loss and thereby limits high-throughput long-distance communication. moreover, each successful interference event yields only 1 bit of key information. To overcome these limitations, we propose the introduction of the multi-scale entanglement renormalization ansatz (MERA) into the MDI-QKD protocol. This constructs a hierarchical entanglement structure capable of efficiently encoding multi-bit information, aiming to significantly enhance the key rate, extend communication distance, and maintain theoretical security.

We design three MERA-based MDI-QKD implementation schemes: 1) A single-photon scheme based on the compressed single-photon state at the $L$-th layer of MERA, which compresses multi-layer information into a single-photon state, enabling the extraction of multiple key bits from a single successful interference event, making it suitable for short-to-medium distance scenarios requiring high key rates; 2) an entanglement-based scheme based on the compressed entangled state at the $(L-1)$-th layer of MERA, which leverages the strong correlations of entangled states to enhance noise resistance, making it suitable for long-distance and high-loss channels; 3) a hybrid adaptive scheme that dynamically switches between the above two modes based on real-time channel quality, achieving optimal performance adaptation across all distances.

All schemes employ the hierarchical compression mechanism of MERA, utilizing the disentangling operator $U$ and the isometric mapping operator $W$ to compress the quantum state layer by layer, and reconstructing the state via inverse operations for multi-level key extraction. The protocol incorporates the decoy-state method for eavesdropping detection, and uses basis sifting and multi-layer fidelity verification to ensure information integrity and security. Additionally, by designing four predefined MERA topological structures, efficient structural matching and information synchronization are achieved.

Numerical simulations show that,Within the 0—200 km range, the single-photon scheme SI-MERA-MDI-QKD improves the key generation rate by approximately 22931% compared to classical MDI-QKD. The entanglement-based scheme ES-MERA-MDI-QKD and the hybrid scheme HY-MERA-MDI-QKD still maintain an effective key rate of $10^{-11}$ bit/pulse at 350 km, extending the effective communication distance of classical MDI-QKD by approximately 150 km.Under varying detector efficiencies and channel loss conditions, the proposed schemes all demonstrate significant performance advantages. Coding capacity analysis shows that,



* Project supported by the National Natural Science Foundation of China (Grant No. 61702427) and the Southwest University's 2025 School-Level Teaching Reform Program, China (Grant No. 2025JY008).

# These authors contributed equally.

† Corresponding author. E-mail: hlai@swu.edu.cn

under zero-error conditions, the encoding capability of MERA-MDI-QKD can exceed that of classical MDI-QKD by more than 221 times.

Security analysis shows that the proposed schemes exhibit strong robustness against collective attacks, intercept-resend attacks, and Trojan-horse attacks. Under collective attacks, any eavesdropping behavior leads to the non-orthogonality of ancillary states, resulting in detectable errors. Under intercept-resend attacks, attackers struggle to reconstruct the original entanglement structure. Under Trojan-horse attacks, the protocol still maintains a high secure key rate through multi-layer encoding.

**Keywords:** measurement-device-independent, multi-scale entanglement renormalization ansatz, long-distance communication, key generation rate

**DOI:** 10.7498/aps.75.20251450 **CSTR:** 32037.14.aps.75.20251450