基于多尺度纠缠重整化假设的量子网络通信资源优化方案*

赖红#† 任黎# 黄钟锐 万林春

(西南大学计算机与信息科学学院, 重庆 400715)

(2024 年 10 月 2 日收到; 2024 年 10 月 29 日收到修改稿)

量子密钥分发 (quantum key distribution, QKD) 技术因在确保通信安全方面的潜力而备受关注, 但其在大规模网络中的应用受限于量子资源的稀缺性和低效的利用率. 尤其在 Ekert91 协议中, 尽管利用了纠缠对进行密钥生成, 实际参与密钥生成的纠缠对数量有限, 导致资源利用率不高. 为了克服这一挑战, 本文提出一种基于多尺度纠缠重整化假设 (multiscale entanglement renormalization ansatz, MERA) 的 QKD 优化方案, 以提高纠缠资源的利用效率. 该方案利用 MERA 的分层结构和多体态压缩特性, 有效减少量子存储需求, 并显著提升纠缠对的利用率. 实验模拟显示, 在相同的加密请求 (1024 比特) 和物理条件下, 与传统方法相比, 本文的方案节省了 124151 对纠缠资源, 既显著提高了资源的利用效率, 又未降低密钥生成过程的安全性, 有助于推动 QKD 技术在资源受限的环境中进一步发展和应用.

关键词: 量子密钥分发, 多尺度纠缠重整化假设, 资源利用率, 安全性

PACS: 03.67.–a, 03.67.Dd, 03.67.Hk, 03.67.Mn **DOI**: 10.7498/aps.73.20241382

CSTR: 32037.14.aps.73.20241382

1 引 言

量子密钥分发 (quantum key distribution, QKD) 技术基于量子不可克隆定理[1], 为安全通信带来了革命性突破, 提供了传统加密技术无法匹敌的安全性. 在量子通信网络中, 由于大量通信业务的加密需求, 量子密钥的需求量巨大. 然而, 传统依赖可信中继[2–4] 的 QKD 的网络面临较高的可信管理成本, 因此, 越来越多的研究聚焦于纠缠网络[5–9] 的探索与发展.

当前量子纠缠网络面临三大挑战[10]: 1) 纠缠对稀缺; 2) 量子态失真; 3) 量子态存储. 本文主要关注其中的纠缠对稀缺问题. 一般而言, 导致稀缺的主要原因有三点: 首先, 远距离纠缠对的建立需要消耗大量链路资源, 链路条件、纠缠成功率和纠缠交换成功率都将影响纠缠对的建立; 其次, 基于纠缠的 QKD 方案[11,12] 资源利用率较低, 如 Ekert91 协议中, 只有 2/9 的纠缠对用于生成原始密钥, 生成安全密钥的比例更低; 最后, 用户的加密需求繁多, 且密钥需求与纠缠资源呈正相关, 随着需求增加, 资源消耗迅速上升, 进一步加剧了资源稀缺问题. 对此, 研究人员提出了不同的方案来缓解这个问题. 在文献 [8,13] 中, 作者通过优化纠缠路由算法提升网络吞吐量, 增加可用的纠缠对数量, 从而更有效地利用纠缠网络资源. 赖红[14] 提出

* 国家自然科学基金 (批准号: 61702427, 62301454)、重庆市自然科学基金 (批准号: CSTB2022NSCQ-MSX0749, CSTB2023NSCQ-MSX0739)、中国国家留学基金委 (批准号: 202306990061) 和西南大学 2022 年校级教改项目 (批准号: 2022JY086) 资助的课题.

同等贡献作者.

† 通信作者. E-mail: hlai@swu.edu.cn

了一种广义等距张量压缩多光子纠缠态的 QKD 协议, 该协议通过将多光子纠缠态压缩为单光子态或 Bell 态[15], 显著提高了编码效率, 并减少了纠缠对的使用. 这些工作在提升纠缠对数量和降低纠缠对消耗方面取得了进展, 但考虑到量子网络中对纠缠对资源的巨大需求, 纠缠对稀缺问题值得进一步研究.

针对上述问题, 本文进一步提出将多尺度纠缠重整化假设 (multiscale entanglement renormalization ansatz, MERA)[16] 应用于 QKD 网络. 通过利用 MERA 的独特酉矩阵结构进行无损压缩[17], 旨在减少存储成本和纠缠资源的消耗, 同时提高密钥分发效率. 本文的主要贡献包括: 1) 提出了一种基于 MERA 架构的 QKD 方案, 显著降低了纠缠资源的消耗; 2) 通过引入安全参数, 在保障 QKD 安全性的前提下, 提升了密钥分发效率, 以满足高需求量子网络的要求. 通过这些优化, 本文为 QKD 技术在实际中的应用提供了新的解决方案. 该方案在现有 QKD 网络基础上显著提高了资源利用率和整体网络性能, 展示了广泛的应用潜力.

2 相关工作

在远程通信对之间建立纠缠对以进行密钥分发的方法, 虽然能够提供高安全性的通信, 但资源消耗大、成本高. Shi 等[8] 提出的 Q-CAST 算法有效提升了纠缠网络的吞吐量, 然而, 由于物理限制[18–20], 随着通信距离的增加, 成功建立远距离纠缠对的概率仍然很低, 因此无法满足大规模加密的需求. 此外, 量子态在节点中的存储[21–23] 也是一个挑战. 尽管当前量子存储器技术[24–26] 已取得显著进展, 存储时长和量子比特数得到显著提升, 但仍无法满足现有的通信需求.

为应对这些挑战, 研究人员提出了多种方法, 包括量子压缩和密钥扩展, 以提升 QKD 的效率和安全性. 首先, Zhang 等[27] 提出了量子密钥扩展 (quantum key expansion, QKE) 协议, 不仅能扩展密码密钥, 提升密钥产生速率, 还能生成更长的密钥, 并抵御多种攻击, 从而增强 QKD 协议的安全性. 其次, MERA 作为一种层次化的张量网络, 被 Lai 等[17] 用于构建层次量子秘密共享 (hierarchical quantum secret sharing, HQSS) 方案. 该方案利用 MERA 的层次结构, 将参与者的信任和权限层次与 MERA 结构相关联, 并通过二元和三元 MERA 生成秘密份额. 这一动态结构允许对参与者进行晋升或降级, 以及新参与者的加入和旧参与者的退出, 确保了 HQSS 方案的灵活性和安全性. 尽管 Lai 等设计了等距映射 W 和解纠缠操作 U 来压缩原始态, 并通过逆映射无损地解压缩为原始态, 但尚未扩展其设计的等距张量在 QKD 协议中的应用. 最后, 纠缠态源的压缩也成为 QKD 协议中的一个重要研究方向. 由于当前量子处理器的原始性和多光子纠缠制备的难度, 对传输的量子数据进行压缩具有重要的实际意义. Lai 等[28] 通过构建等距张量实现了纠缠压缩, 这种压缩不仅提高了 QKD 协议的效率, 还能更好地抵御窃听, 提升了系统的安全性.

MERA 展示了一种分层结构, 每一层对应于特定的长度或能量尺度. Lai 等[17] 设计了等距映射算符 W 和解纠缠算符 U, 这些操作能够有效地将原始态压缩, 并通过逆映射无损地解压缩回原始态. MERA 的分层特性特别适合应用于 QKD, 尤其在资源有限和量子存储技术受限的情况下, 因此本文提出了基于 MERA 的 QKD 方案. 本文的方案利用纠缠网络在通信双方之间进行纠缠分发, 双方使用这些纠缠对构建一个共享的矩阵乘积态并将该态压缩后存储. 压缩后的光子数量显著少于原始多体态中的光子数量, 从而降低了存储成本. 此外, 当前量子存储器能够长时间保存压缩态, 因此可以利用这段时间, 通过多次解压缩生成所需的密钥.

3 背景知识

本节主要介绍本文提出的协议所依赖的背景知识. 首先, 介绍 MERA 的基本概念和结构特点. 接着, 重点讲述 Lai 等[17] 构建的等距张量如何用于 MERA 的压缩与还原过程, 为协议的设计提供理论基础和技术支持.

3.1 MERA 定义与性质

MERA 是一种层次化的张量网络结构 (如图 1 所示), 由一系列的等距映射算符 W 和解纠缠算符 U 组成. W 用于降低系统的自由度, 而 U 则用

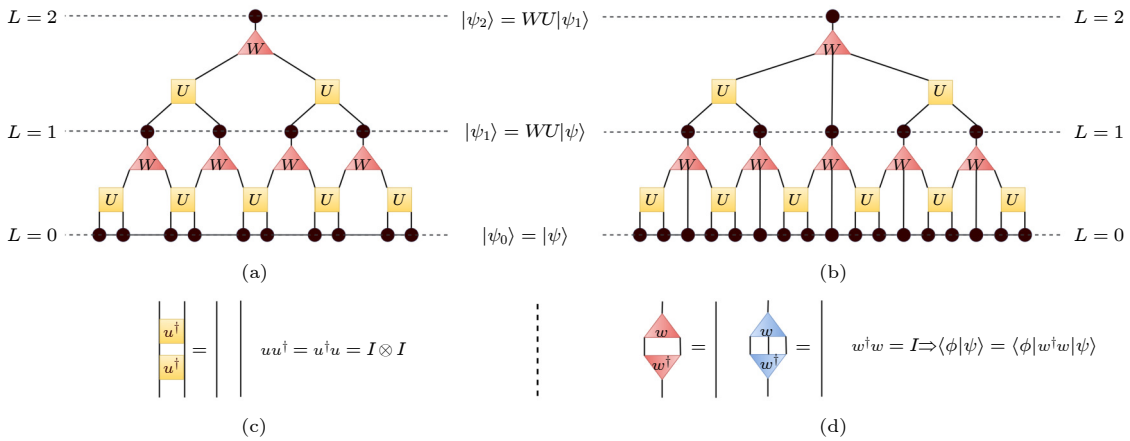


图 1 MERA 结构 (a) 二元 MERA; (b) 三元 MERA; (c) 解纠缠算符 U; (d) 等距映射 W

Fig. 1. The structure of MERA: (a) Binary MERA; (b) ternary MERA; (c) disentangling operator U; (d) isometric mapping W.

于消除局部纠缠. 这种结构使得在计算物理量时能够减少计算复杂度, 同时保留系统的关键纠缠信息.

MERA 通过多次纠缠重整化 (entanglement renormalization group, ERG) 形成, 一次 ERG 包括以下两步: 1) 边界变形: $|\psi\rangle \to U|\psi\rangle$; 2) 粗粒化: $U|\psi\rangle \to WU|\psi\rangle$. 随着 ERG 的迭代深入, 量子态中的短程纠缠被逐步规范化并排除, 而长程纠缠的特性则被逐渐揭示. 这表明, 每个 ERG 层次都记录了原量子态在特定长度尺度上的纠缠特征.

$$\frac{1}{\sqrt{2}}(|00\rangle+|11\rangle)=\frac{1}{\sqrt{2}}\begin{bmatrix}1\\0\\0\\1\end{bmatrix},$$

$$\frac{1}{\sqrt{2}}(|01\rangle+|10\rangle)=\frac{1}{\sqrt{2}}\begin{bmatrix}0\\1\\1\\0\end{bmatrix}. \tag{1}$$

3.2 纠缠态的压缩与还原

Lai 等[17] 注意到 MERA 的分层结构, 这种层级结构可以与分层秘密共享结合起来, 为了能够完成秘密共享, 他们设计了合适的 W 和 U. 所设计的 U 有 6 种, $U=\{\boldsymbol{u}_1,\boldsymbol{u}_2,\boldsymbol{u}_3,\boldsymbol{u}_4,\boldsymbol{u}_5,\boldsymbol{u}_6\}$, W 有 4 种, $W=\{\boldsymbol{w}_1,\boldsymbol{w}_2,\boldsymbol{w}_3,\boldsymbol{w}_4\}$.

U 可以将纠缠态转换为直积态, 即解纠缠. 假设两点之间的纠缠如 (1) 式, 下面用 $\boldsymbol{u}_1$ 举例进行验证.

$$\boldsymbol{u}_1=\begin{bmatrix}\frac{1}{\sqrt{2}} & 0 & 0 & \frac{1}{\sqrt{2}}\\ 0 & \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} & 0\\ 0 & \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} & 0\\ \frac{1}{\sqrt{2}} & 0 & 0 & -\frac{1}{\sqrt{2}}\end{bmatrix}. \tag{2}$$

解纠缠:

$$\boldsymbol{u}_1\left(\frac{1}{\sqrt{2}}\begin{bmatrix}1\\0\\0\\1\end{bmatrix}\right)=\begin{bmatrix}\frac{1}{\sqrt{2}} & 0 & 0 & \frac{1}{\sqrt{2}}\\ 0 & \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} & 0\\ 0 & \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} & 0\\ \frac{1}{\sqrt{2}} & 0 & 0 & -\frac{1}{\sqrt{2}}\end{bmatrix}\begin{bmatrix}\frac{1}{\sqrt{2}}\\0\\0\\\frac{1}{\sqrt{2}}\end{bmatrix}=\begin{bmatrix}1\\0\\0\\0\end{bmatrix}=|00\rangle. \tag{3}$$

因为 $\boldsymbol{u}$ 是酉矩阵 ($\boldsymbol{u}^\dagger=\boldsymbol{u}^{-1}$), 所以通过它的逆操作, 可以将解纠缠后的态还原为纠缠态.

$$\boldsymbol{u}_1^{\dagger}|00\rangle = \boldsymbol{u}_1^{\dagger}\begin{bmatrix}1\\0\\0\\0\end{bmatrix} = \begin{bmatrix}\frac{1}{\sqrt{2}} & 0 & 0 & \frac{1}{\sqrt{2}}\\ 0 & \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} & 0\\ 0 & \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} & 0\\ \frac{1}{\sqrt{2}} & 0 & 0 & -\frac{1}{\sqrt{2}}\end{bmatrix}\begin{bmatrix}1\\0\\0\\0\end{bmatrix} = \begin{bmatrix}\frac{1}{\sqrt{2}}\\0\\0\\\frac{1}{\sqrt{2}}\end{bmatrix} = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle). \tag{4}$$

不同的 U 作用在不同的纠缠态上, 可以得到相同或不同的直积态, 其映射关系如图 2 所示. 所设计的 W 可以将纠缠态压缩为单光子态, 其映射关系如图 3 所示.

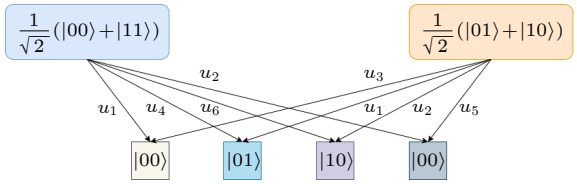


图 2 U 与 $|00\rangle$, $|01\rangle$, $|10\rangle$, $|11\rangle$ 的映射关系

Fig. 2. The mapping relationship between U and $|00\rangle$, $|01\rangle$, $|10\rangle$, $|11\rangle$.

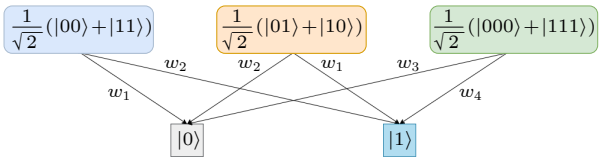


图 3 W 与 $|0\rangle$, $|1\rangle$ 的映射关系

Fig. 3. The mapping relationship between W and $|0\rangle$, $|1\rangle$.

在 Lai 等 [17] 的工作中, 通过这些操作可以完成 MERA 态的制备, 形成不同层次的秘密, 同时参与者也可以通过这些操作的逆操作恢复出所共享的秘密. 本文发现, MERA 的分层结构能够与加密请求的不同等级相对应, 从而实现差异化处理. 更为关键的是, Lai 等 [17] 设计的等距映射矩阵 W 和解纠缠算符 U 可以无损地对 MERA 态进行压缩和还原. 压缩后的光子数显著少于压缩前的光子数, 这在现有的物理硬件条件下有助于大幅降低存储成本. 基于这些发现, 本文提出了一种基于 MERA 的 QKD 方案.

4 基于 MERA 的量子网络通信

在量子通信网络中, 随着大量通信业务的加密需求, 量子密钥的需求也急剧增长. 安全通信通常采用一次一密 (one time pad, OTP)[29] 方案, 进一步增加了资源消耗. 尽管现有方法通过优化纠缠路由提升了网络吞吐量, 但仍难以满足大规模的加密需求. 本文提出将 MERA 应用于 QKD 网络, 这一方案能够在现有技术条件下有效减少资源消耗, 同时满足通信加密的需求. 本节将详细介绍该方案的实现过程, 并构建数学模型, 以进一步验证方案的有效性.

4.1 量子密钥分发网络的结构

本文根据量子网络的特点, 将网络结构简化为两层——控制层和基础设施层, 如图 4 所示.

1) 控制层: 本层由控制器组成. 控制器负责在网络中管理通信对 (S-D) 之间的密钥生成, 并执行态的压缩和解压缩操作. 在压缩过程中, 控制器向 S-D 下发命令, 该命令包括压缩层数以及使用的 U 和 W 操作的序列编号. 但所有的 U 和 W 均为公开信息, 窃听者也能获取. 为了降低传输成本, 控制器在下发压缩命令时仅传输操作的序列号, 而非操作本身. 解压缩时, 控制器向通信双方发送命令, 仅包含层数信息, 通信双方据此命令将光子解压缩到相应层.

2) 基础设施层: 本层包含了经典网络设备以及与量子相关的设备——纠缠源、量子节点、量子中继器、量子信道. 本层与大多数随机拓扑的量子网络一致, 主要功能是在控制器的控制下建立通信对之间的远距离纠缠.

4.2 量子密钥分发过程

本方案的密钥分发流程如图 5 所示, 详细过程分为以下 8 个步骤. 1) 计算纠缠对数量: 当通信双方有加密请求时, 控制器根据请求的特性计算所需的纠缠对数量. 2) 生成纠缠对: 通信双方通过纠缠网络生成所需数量的纠缠对. 3) 生成和共享矩阵

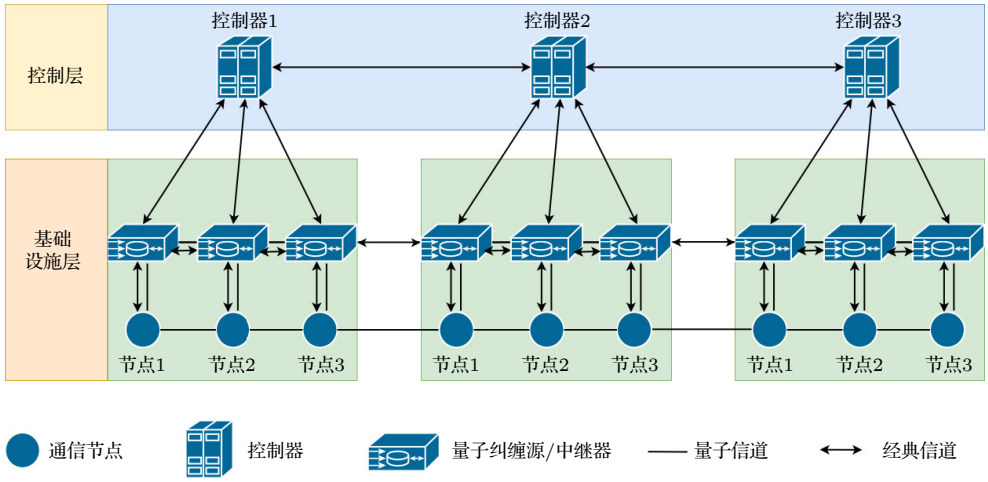


图 4 网络结构

Fig. 4. Network structure.

乘积态 (matrix product state, MPS)[30]: 利用成功建立的纠缠对生成 MPS 态, 并在通信双方之间共享该态 (注: 即使在没有当前密钥需求时, 用户之间也可以提前制备纠缠, 并通过步骤 3) 和 4) 进行压缩后存储在量子存储器中, 以备未来需要时直接使用). 4) 压缩存储: 通信双方根据控制器的指令压缩手中的多体态, 并将压缩后的量子态存储. 5) 解压缩: 控制器根据请求的特性向通信双方下达解压缩命令, 双方根据命令将手中的态解压缩到指定层. 6) 安全性验证: 双方使用 Hash 函数验证是否接收到相同的解压缩命令, 若一致则将生成的密钥作为完整密钥的一部分, 若不一致则丢弃. 7) 后处理阶段: 进行误码纠错和隐私放大, 确保双方获得一致的安全密钥. 8) 密钥长度检查: 检查密钥长度是否满足需求, 若不足, 则重复步骤 5)—8), 直至密钥长度满足要求.

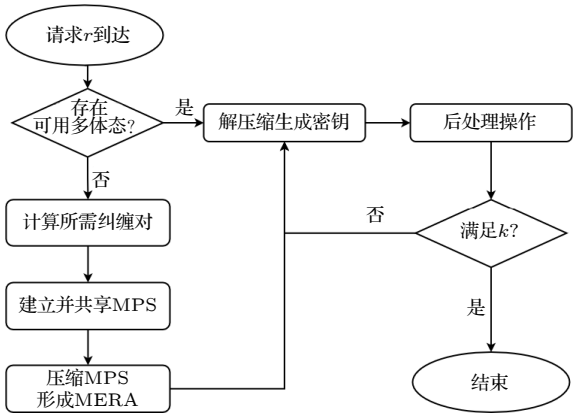


图 5 量子密钥分发流程图

Fig. 5. Quantum key distribution flowchart.

4.3 量子密钥网络的数学模型

4.3.1 通信请求

在 QKD 网络中, 通信请求可用元组 $r=(S, D, k, P, \Delta t)$ 进行描述, 具体如表 1 所列. 某一时刻, 网络中的所有请求组成集合 $R=\{r_1, r_2, \cdots, r_n\}$.

表 1 网络请求属性及其取值范围

Table 1. Network request attributes and their value ranges.

属性	描述	取值范围
S	发送方	N/A
D	接收方	N/A
k	需求量	[1024, 4096]
P	优先级	[1, 5]
Δt	可接受时延	[1, 60]

4.3.2 纠缠分发

控制器维护一个二维状态表 (见图 6), 用于判断请求到达时是否存在可用的多体态. 该状态表以对称矩阵的形式表示, 其中每个矩阵元素表示通信对之间的状态信息. 矩阵中元素 $M_{ij}=M_{ji}=0$ 表示第 i 个节点与第 j 个节点之间没有可用的多体态, 而 $M_{ij}=M_{ji}=1$ 表示存在可用的多体态. 如果存在可用的多体态, 则直接跳过该步骤; 如果不存在, 则需要生成纠缠对以创建 MPS 态. 控制器会根据请求的特性来估算生成 MPS 态所需的纠缠对数量. 由于 MPS 态中包含的光子数越多, 解压缩时底层光子数越多, 因此每次解压缩生成的密钥

长度会更长, 从而减少解压缩次数, 提升密钥生成速率. 为了优化这一过程, 本文在文献 [31] 的基础上, 综合考虑请求的需求量、优先级和可接受时延, 设计了 (5) 式来计算所需的纠缠对数量, 从而优化密钥生成效率, 满足方案的需求.

$$Q_{\text{MPS}} = \left\lceil \alpha \cdot \left(\frac{k - k_{\min}}{k_{\max} - k_{\min}} \right) + \beta \cdot \left(\frac{P - P_{\min}}{P_{\max} - P_{\min}} \right) + \gamma \cdot \left(\frac{\Delta t - \Delta t_{\min}}{\Delta t_{\max} - \Delta t_{\min}} \right) + \delta \right\rceil, \tag{5}$$

其中, $\alpha, \beta, \gamma, \delta$ 分别代表需求量 k 的权重系数、优先级 P 的权重系数、可接受时延 Δt 的权重系数、基础纠缠对数量. 假设本文选择以下权重系数: $\alpha = 10,\ \ \beta = 5,\ \ \gamma = 5,\ \ \delta = 80$, 存在两个请求 $r_1(A, B, 2048, 3, 10)$, $r_2(C, D, 1024, 1, 30)$, 代入(5) 式得到结果为: $Q_{\text{MPS-AB}} = 97$, $Q_{\text{MPS-CD}} = 88$. 可以观察到 r_1 是一个优先级高、密钥需求大的紧急请求, 因此需要较多的纠缠对; r_2 优先级、需求量相对较低, 可接受时延较长. 显然, 通过这种计算方式可以清晰地反映不同请求之间的差异.

M_{11}	M_{12}	$\cdots$	M_{1n}
M_{21}	M_{22}	$\cdots$	$\vdots$
$\vdots$	$\cdots$	$\ddots$	M_{n-1n}
M_{n1}	$\cdots$	M_{nn-1}	M_{nn}

图 6 状态表

Fig. 6. State table.

4.3.3 MPS 态的生成与压缩

1) MPS 态的生成: 在纠缠网络完成纠缠对的分发后, 通信双方利用这些纠缠对建立原始的 MPS 态, 并共同共享这个多体态.

$$|\psi\rangle = \sum_{s_1 s_2 \cdots s_{n-1} s_n} \boldsymbol{A}^{s_1} \boldsymbol{A}^{s_2} \cdots \boldsymbol{A}^{s_{n-1}} \boldsymbol{A}^{s_n} |s_1 s_2 \cdots s_{n-1} s_n\rangle, \tag{6}$$

其中, $\boldsymbol{A}^{s_i}$ 是第 i 个量子比特上的张量, s_i 是量子比特的状态, n 是 MPS 的长度. 例如: 三光子态 $|\Psi\rangle = \frac{1}{\sqrt{3}}(|001\rangle + |011\rangle + |110\rangle)$ 的 MPS 形式可以表示为

$$\begin{aligned} |\Psi\rangle = & \begin{bmatrix} \frac{1}{\sqrt{3}} & 0 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} \begin{bmatrix} 1 \\ 0 \end{bmatrix} |001\rangle \\ & + \begin{bmatrix} \frac{1}{\sqrt{3}} & 0 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 1 \\ 0 \end{bmatrix} |011\rangle \\ & + \begin{bmatrix} 0 & \frac{1}{\sqrt{3}} \end{bmatrix} \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 0 \\ 1 \end{bmatrix} |110\rangle. \end{aligned} \tag{7}$$

2) MPS 态的压缩: 在共享 MPS 态之后, 控制器向双方下发压缩命令, 包括矩阵 U 和 W 的序列及压缩层数 L. MERA 的总层数 L 表示如下:

$$L = \lfloor \log_2 N \rfloor, \tag{8}$$

其中 N 代表 MPS 态所含光子数. 对于 128 光子的 MPS 态, $128 = 2^7$, 则最大层数为 7, 且能够将 MPS 态压缩为单光子 $|0\rangle$ 或 $|1\rangle$; 也可以压缩到第 6 层, 双光子态 $|00\rangle, |01\rangle, |10\rangle, |11\rangle$; 以此类推. 为了减少存储成本, 本文一般将其压缩到三光子或者更少. 并且由于每层选取的 W 和 U 操作的不同, 所形成的 MERA 态也不同.

3) 双方根据命令进行压缩, 完成后向控制器返回确认信息. 为了后续的解压缩过程, 双方需保存 U 和 W 操作的序列. 这些操作的共轭转置是解压缩的关键, 因为它们能够将压缩后的量子态恢复到原始态.

4.3.4 密钥分发

1) 解压缩: 在密钥分发过程中, 本文实际执行一系列解压缩操作, 直到生成的密钥满足通信需求. 解压缩阶段优先选择解压缩到接近原始态的底层态, 以便生成更长的密钥. 这意味着, 不同的解压缩层级会影响密钥生成速率, 使本文能够根据不同的紧急程度和需求处理通信请求. 在本文的方案中, 控制器在解压缩时会随机选择第 1—3 层态进行操作. 这些层级的选择确保了生成的密钥长度既不过短, 又能保持所需的安全性. 基于这一策略, 本文可以估算解压缩操作的最大和最小次数.

$$\text{Min}_t = \left\lfloor \frac{k}{N/2} \right\rfloor, \tag{9}$$

$$\text{Max}_t = \left\lfloor \frac{k}{N/2^3} \right\rfloor, \tag{10}$$

其中, k 表示请求的密钥需求量, t 表示解压缩次数, N 表示 MPS 态所含光子数. 例如, 一个长度为 2048 的密钥请求, 在 MPS 态为 256 个光子, MERA

态最高层为 8 时该请求需要 [16, 64] 次解纠缠才能满足要求.

$$\mathrm{Min}_t = \left\lfloor \frac{k}{N/2} \right\rfloor = \left\lfloor \frac{2048}{256/2} \right\rfloor = 16, \tag{11}$$

$$\mathrm{Max}_t = \left\lfloor \frac{k}{N/2^3} \right\rfloor = \left\lfloor \frac{2048}{256/8} \right\rfloor = 64. \tag{12}$$

2) Hash 验证: 在每一轮生成密钥后, 双方根据提前共享的安全的哈希函数 $H(x)$ 将自己手中的密钥 K_s 进行计算, 即 $H(K_{sA})$, $H(K_{sB})$. 并且以广播的方式进行哈希值的对比, 若 $H(K_{sA}) = H(K_{sB})$, 则双方的密钥 K_{sA}, K_{sB} 一致, 则保留该密钥 K_s; 否则, 不一致, 废弃该密钥, 因为控制器在下发层数命令时, 可能受到信道噪声影响而导致通信双方接收到的命令不一致; 当废弃的次数过多时, 则表明密钥分发过程受阻, 中断本次通信.

3) 对保留的 K_s 进行后处理操作得到 K_E, 保证双方得到的是正确的、一致的安全密钥.

4) 判断当前密钥量是否满足通信需求, 若满足, 则结束密钥分发; 若不满足则继续进行分发过程, 直至满足需求.

5 性能分析

本方案旨在最大化现有资源的利用效率, 有效降低资源消耗及成本. 本节将从资源消耗、成本效益和安全性三个关键维度, 对本文的方法进行全面的性能评估.

5.1 资源消耗

本节将深入探讨量子密钥分发过程中的资源消耗问题, 重点关注量子资源与经典资源的利用效率. 并详细分析传统 Ekert91 协议的资源消耗, 与本文提出方案进行比较.

5.1.1 传统方法

在传统方法中, 依赖于纠缠网络在通信双方之间建立远距离的量子纠缠. 这一过程是密钥分发的基础, 为 Ekert91 协议提供了必要的纠缠对. 随后, 利用这些纠缠对, 通过 Ekert91 协议的步骤进行密钥分发.

1) 纠缠分发: 纠缠分发通过中继节点利用纠缠交换, 在 S 和 D 之间建立远距离纠缠, 纠缠交换的核心操作是贝尔态测量 (Bell state measurement BSM). BSM 可以产生以下四种测量结果:

$$|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle), \quad |\Phi^-\rangle = \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle),$$
$$|\Psi^+\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle), \quad |\Psi^-\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle),$$

分别用 00, 01, 10, 11 表示. 测量结果通过经典信道传递给 S (或 D), 然后根据结果执行相应的操作 (如比特翻转或相位翻转), 以实现 S 和 D 之间的纠缠. 1 跳纠缠分发, 需要消耗 2 比特经典信息和 2 个纠缠对; 若推广至 K 跳路径, 则需消耗 $2K$ 比特经典信息和 $K+1$ 个纠缠对. 同时, 在纠缠网络中, 建立远距离纠缠需要多次短距离纠缠生成和纠缠交换, 这受到物理因素的限制. 关键影响因素包括链路纠缠成功率 (p) 和纠缠交换成功率 (q). 对于 1 跳纠缠路径, 纠缠分发成功率为 $P_1 = p^2 q$. 推广至 K 跳路径, 成功率如 (13) 式所示. 因此, 所需的纠缠分发次数 M 可以通过 (14) 式计算: 大约要 $\dfrac{N}{p^{K+1}q^K}$ 次纠缠分发才能成功建立 N 个纠缠对.

$$P_K = p^{K+1}q^K, \tag{13}$$

$$M \cdot p^{K+1}q^K = N. \tag{14}$$

2) Ekert91 协议: Alice 和 Bob 测量基为 Alice, $\{X, Z, T\}$; Bob, $\{X, S, T\}$. 对于每一个纠缠对, 双方随机选择一个测量基进行测量. 在一段时间后, 双方通过经典信道交换基的信息 (三种选择, 每种用 2 比特表示). 假设进行 N 次测量, 则需要消耗 $2 \cdot N \cdot 2 = 4N$ 比特的经典信息. 为了生成密钥, 双方保留了同时选择 X 和 T 基的测量结果. 在理想情况下, 大约 2/9 的纠缠对测量结果可以用于生成原始密钥.

$$S = \frac{-Z - X}{\sqrt{2}}, \tag{15}$$

$$T = \frac{Z - X}{\sqrt{2}}. \tag{16}$$

3) 后处理: 由于系统中的缺陷, 如退相干和量子信道噪声, 原始密钥中可能会出现错误, 从而导致一定的误码率. 例如, 对于贝尔态 $|\psi^+\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle)$, Alice 与 Bob 的测量结果应当是反相关的 (01 或 10). 若得到相同的结果 (11 或 00), 则表示出现了错误. 为确保双方获得一致且正确的密钥, 必须进行后处理, 包括误码纠错和保密增强. 本文选择低密度奇偶校验码 (low-density parity-check code, LDPC) 讨论误码纠错过程. 文献 [32]

给出了该方式码率 R_1 的计算公式:

$$R_1 = 1 - f(e)H_2(e), \tag{17}$$

$$f(e)=1.1 + |e - 0.1|, \tag{18}$$

$$H_2(e) = -e\log_2 e - (1-e)\log_2(1-e), \tag{19}$$

其中, e 代表误码率, QKD 协议中提取绝对密钥的最大错误阈值为 11%[33]; $f(e)$ 代表纠错效率, 该值越接近 1 就说明需要额外传输的信息越少, 效率越高; $H_2(e)$ 是二进制熵函数, 反映了信息的不确定性.

本文选择 Toeplitz 矩阵方法 [34] 讨论保密增强过程. 假设 $\boldsymbol{K}_A$ 的长度为 n, 最终密钥长度为 $G\boldsymbol{K}_A$ 的目标长度为 m, 则得到 K 的方法是构造一个 $m \times n$ 的 Toeplitz 矩阵 $\boldsymbol{T}_{m\times n}$, 并使之与 $\boldsymbol{K}_A$ 组成的列向量相乘. M 可以称为安全密钥长度, 其与根据系统参数所计算出的安全码率 R_2 关系如 (20) 式, 文献 [35] 给出 R_2 的计算方式如 (21) 式.

$$m = R_2 \times n, \tag{20}$$

$$R_2 \approx 1 - H_2(e). \tag{21}$$

通过误码纠错和保密增强, 通信双方可以建立安全的密钥. 由上述过程可以得到安全密钥长度 k 与原始码长度 n 之间的关系如 (22) 式, 又因为 $n = (2/9)\cdot N$, 所以可以进一步计算所需纠缠对数量 N.

$$n = \frac{k}{(1-H_2(e))(1-H_2(e)f(e))}, \tag{22}$$

$$N = \frac{9k}{2(1-H_2(e))(1-H_2(e)f(e))}. \tag{23}$$

至此, 可以得出如下的资源消耗的计算方式:

$$C_{\mathrm{E}} = 2K\cdot\frac{N}{p^{K+1}q^K} + 4\cdot N, \tag{24}$$

$$Q_E = \frac{N(K+1)}{p^{K+1}q^K} + N, \tag{25}$$

$$S_{\mathrm{E}} = C_{\mathrm{E}} + Q_{\mathrm{E}}, \tag{26}$$

其中, C_{E} 表示 Ekert91 协议所消耗的经典资源, Q_{E} 表示所消耗的量子资源, S_{E} 表示所消耗的总资源.

5.1.2 MERA 方式

本文提出的基于 MERA 的量子密钥分发方案依然依赖纠缠网络来提供远距离纠缠对, 但这些纠缠对并不直接用于生成密钥, 而是用于制备 MPS 态. 随后, 通过压缩生成 MERA 态, 再通过解压缩生成密钥. 该方案主要包括以下步骤: 纠缠分发、MPS 态建立、MERA 态压缩、密钥生成.

1) 纠缠分发: 与传统方式类似, K 跳纠缠建立过程中资源的消耗可以表示为:

经典资源消耗

$$\frac{2KN}{p^{K+1}q^K}; \tag{27}$$

量子资源消耗

$$\frac{(K+1)N}{p^{K+1}q^K}, \tag{28}$$

其中, 所需纠缠对数量 N 的计算方式为

$$N = 10\cdot\left(\frac{k-k_{\min}}{k_{\max}-k_{\min}}\right) + 5\cdot\left(\frac{P-P_{\min}}{P_{\max}-P_{\min}}\right) + 5\cdot\left(\frac{\Delta t-\Delta t_{\min}}{\Delta t_{\max}-\Delta t_{\min}}\right) + 80. \tag{29}$$

2) MPS 态建立: MPS 态的生成方式有多种[36–38], 本文选择了通过 AKLT 态 [38,39] 进行构建. 实际上, AKLT 态的生成涉及到贝尔态, 这与本文的方案紧密契合. 这里本文主要关注所需传输的经典信息量. 在一次投影测量中, 需传输 2 比特的经典信息. 对于 N 对贝尔态, 需传输 $2N$ 比特的经典信息.

3) MERA 压缩: 为了减少存储成本, 本文把原始的 MPS 态进行压缩. 压缩时, 由控制器下发命令, 本文所使用的 U 一共有 6 种, 用 3 比特表示; W 一共有 4 种, 用 2 比特表示, 产生的经典信息为

$$\left(\sum_{l=1}^{L} D_{l-1\to l}\cdot 3 + \sum_{l=1}^{L} I_{l-1\to l}\cdot 2\right)\cdot 2, \tag{30}$$

其中, $D_{l-1\to l}$ 表示从第 $l-1$ 层到第 l 层的解纠缠的次数; $\sum_{l=1}^{L} I_{l-1\to l}$ 表示从第 $l-1$ 层到第 l 层的等距映射的次数.

4) 密钥生成: 在密钥分发过程中, 控制器需要向双方发送层数命令. 双方根据接收到的层数, 使用相应的矩阵操作序列和逆操作进行解压缩. 因此, 主要传输的经典信息为层数. 由于本文的方案中层数的范围在 $[1,10]$, 因此使用 4 比特的经典信息来表示层数. 最终传输的经典信息量为

$$4\cdot D_e\cdot 2, \tag{31}$$

其中, D_e 表示所需解压缩次数. 同时每次解压缩完成时, 需要验证命令的可信性, 通过 SHA-256 验证. 一次需要 256 比特的经典信息传输. 产生的经典信息为

$$256 \cdot D_e. \tag{32}$$

综上所述, MERA 方式的资源消耗可以表示为

$$C_{\mathrm{M}} = \frac{2KN}{p^{K+1}q^K} + 2 \cdot N + \left(\sum_{l=1}^{L} D_{l-1\to l} \cdot 3 + \sum_{l=1}^{L} I_{l-1\to l} \cdot 2 \right) \cdot 2 + 264 \cdot D_e, \tag{33}$$

$$Q_{\mathrm{M}} = \frac{(K+1)N}{p^{K+1}q^K} + N, \tag{34}$$

$$S_{\mathrm{M}} = C_{\mathrm{M}} + Q_{\mathrm{M}}, \tag{35}$$

其中, C_{M} 表示 MERA 方案所消耗的经典资源, Q_{M} 表示所消耗的量子资源, S_{M} 表示所消耗的总资源.

5.1.3 实 验

本节基于前述分析进行了实验设计, 并展开了详细分析. 本文观察到, 误码率、平均路径跳数、链路纠缠成功率以及纠缠交换成功率对资源消耗具有关键影响. 由于这些参数是实际 QKD 网络中的重要物理因素, 对它们进行深入讨论是必要的.

1) 需求量 k 对资源消耗的影响

图 7 展示了在不同需求下, 传统方式与 MERA 方式的量子资源消耗情况. 实验参数设置为 $K = 4$, $e = 0.08$, $p = 0.95$, $q = 0.95$. 传统方式的消耗量用左侧纵轴表示, 范围为 150000—400000; 而 MERA 方式的消耗量用右侧纵轴表示, 范围为 1150—1325. 从图 7 可以看出, 随着需求的增加, 传统方式下的量子资源消耗显著上升, 表明需求增长会导致资源快速消耗; 相较之下, MERA方式的资源消耗较少, 且增长速度较为平缓. 相比传统方式, MERA 方式在相同需求下显著降低了量子资源的消耗, 展现出其在高需求情况下的资源利用效率优势. 例如, 当需求量为 1024 比特时, MERA 方式节省了 124151 对纠缠资源. 这表明, 在量子密钥分发网络中, MERA 方式通过优化资源使用, 能够更有效地应对不断增长的需求.

根据图 8, 虽然经典资源的消耗也呈上升趋势, 但总体上远高于量子资源的消耗. 根据 (24) 式, (25) 式, (33) 式和 (34) 式, 经典资源的消耗与量子资源消耗密切相关. 主要的资源消耗集中在建立远距离纠缠的过程中, 这不仅需要大量链路纠缠, 还涉及多次贝尔态测量, 因此会消耗大量经典资源. 由此可见, 经典资源的消耗趋势与量子资源的消耗趋势相似. 鉴于这一关系, 后续讨论将重点关注量子资源的消耗.

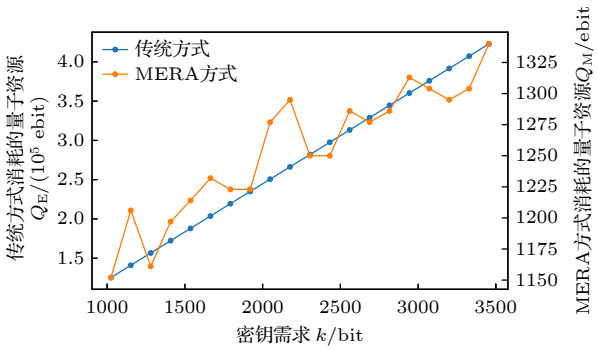


图 7 传统方式与 MERA 方式下量子资源消耗随需求变化的关系

Fig. 7. Relationship between quantum resource consumption and demand in traditional versus MERA.

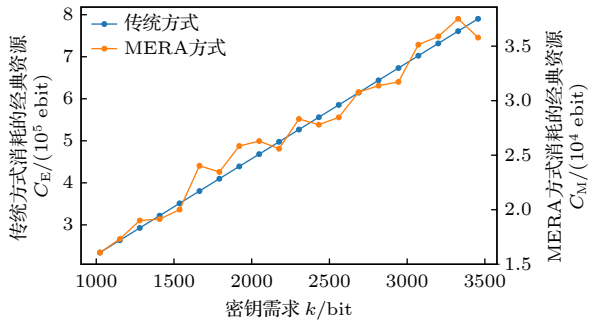


图 8 传统方式与 MERA 方式下经典资源消耗随需求变化的关系

Fig. 8. Relationship between classical resource consumption and demand in traditional versus MERA.

图 9 展示了量子资源和经典资源总和的变化趋势, 随着需求量的增加, 总资源消耗逐渐上升. 然而, 传统方式的资源消耗增长速度远高于 MERA 方式. 这主要是因为传统方式的密钥生成直接依赖于大量纠缠资源, 而 MERA 方式对纠缠资源的需求较弱, 因此其资源消耗增长较为缓慢. 由此可见, MERA 方式在资源消耗方面具有显著优势.

2) 平均路径跳数对资源消耗的影响

实验参数设置为 $e = 0.08$, $p = 0.95$, $q = 0.95$, $k = 1024$. 从图 10 可以看出, 随着路径跳数的增加, 两种方法的纠缠资源消耗均呈指数增长. 这是因为随着路径跳数的增加, 成功建立远距离纠缠的概率呈指数下降. 然而, 如图 11 所示, 无论路径长度如何, 本文的方法所需的资源明显少于传统

方法. 根据 (25) 式和 (34) 式, 它们之间的资源消耗比为 $Q_{\rm E}/Q_{\rm M}=N_1/N_2$, 表明所需纠缠对的数量比与成功建立远距离纠缠对的数量呈正相关. 当 $K=4$ 时, 传统方法消耗的纠缠对数量是 MERA 方法的 106 倍.

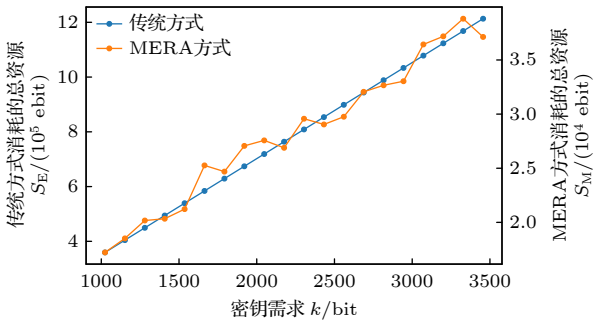


图 9 传统方式与 MERA 方式下总资源消耗随需求变化的关系

Fig. 9. The relationship between total resource consumption and demand in traditional versus MERA.

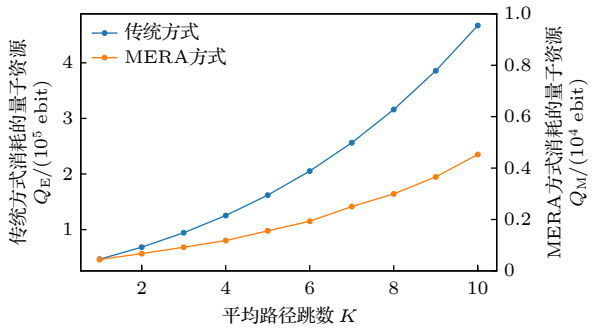


图 10 所需量子资源随平均路径跳数从 1 到 10 的变化情况

Fig. 10. Variation in quantum resource requirements as average path length increases from 1 to 10.

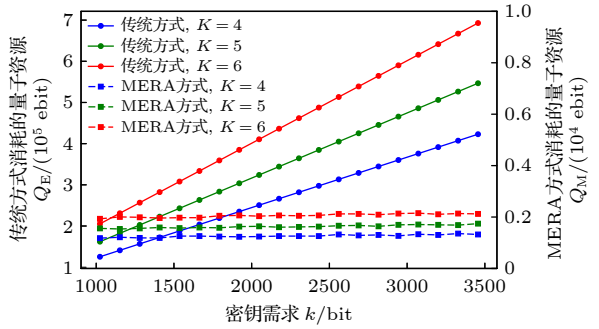


图 11 平均路径跳数为 4, 5, 6 时, 量子资源消耗随请求量的变化

Fig. 11. Quantum resource variation with request volume at average path lengths of 4, 5, and 6.

3) 误码率对资源消耗的影响

实验参数设置为 $K=4$, $p=0.95$, $q=0.95$, $k=1024$. 根据图 12, 误码率对 MERA 方法几乎没有影响. 根据前面的分析, 误码率主要在后处理阶段影响安全密钥长度, 从而影响原始密钥长度. 传统方法生成一位原始密钥至少需要消耗一个纠缠对, 而 MERA 方式只消耗一次解压缩后中的一位, 不直接消耗纠缠对. 因此, 在较高的误码率下, 本文的方法表现出明显的优势. 例如, 在误码率为 10% 时, 本文的方法节省了 158960 对纠缠. 此外, 图 13 展示了在误码率分别为 7%, 8% 和 9% 时, 两种方法在不同请求量下消耗的量子资源变化情况.

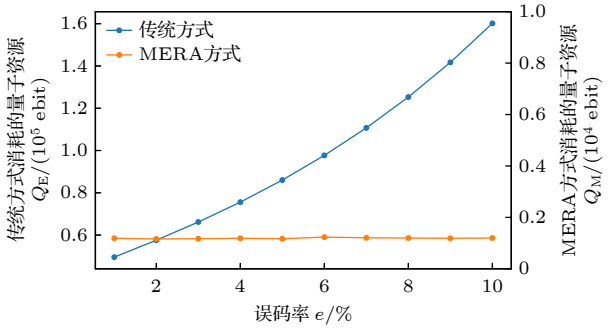


图 12 误码率从 1%—10% 变化时, 所需量子资源的增长情况

Fig. 12. Variation in quantum resource requirements as error rate changes from 1% to 10%.

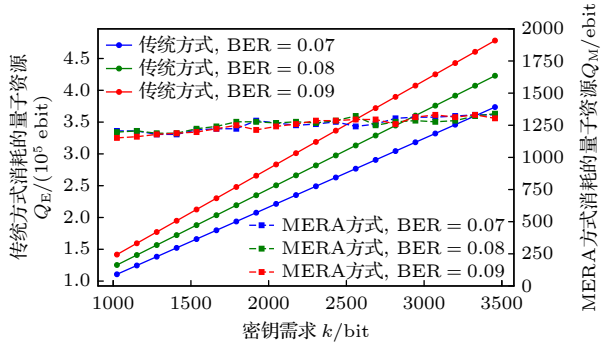


图 13 误码率为 7%, 8%, 9% 时, 量子资源随请求量变化的情况

Fig. 13. Quantum resource variation with request volume at error rates of 7%, 8%, and 9%.

4) 链路纠缠成功率对资源消耗的影响

实验参数设置为 $K=4$, $e=0.08$, $q=0.95$, $k=1024$. 根据图 14, 链路纠缠成功率是量子网络中的关键物理参数, 受到具体物理器件性能的影响. 该参数直接决定远距离纠缠分发的成功率: 链路纠缠成功率越高, 远距离纠缠成功率也相应提高. 链路纠缠成功率提升时, 两种方式所需纠缠对的数量均呈指数级下降. 此外, 如图 15 所示, 在相同成功率下, MERA 方法的资源消耗显著低于传统方法.

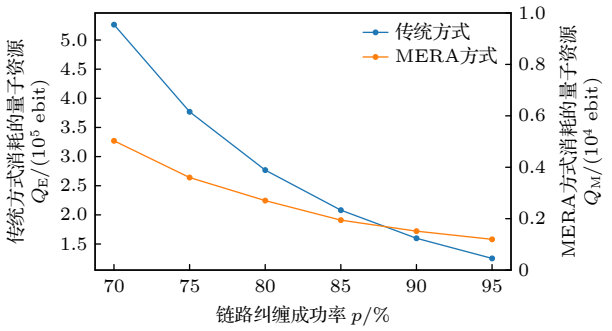


图 14 链路纠缠成功率从 70% 到 95% 变化时, 所需量子资源数量的变化趋势

Fig. 14. Quantum resource variation as link entanglement success rate ranges from 70% to 95%.

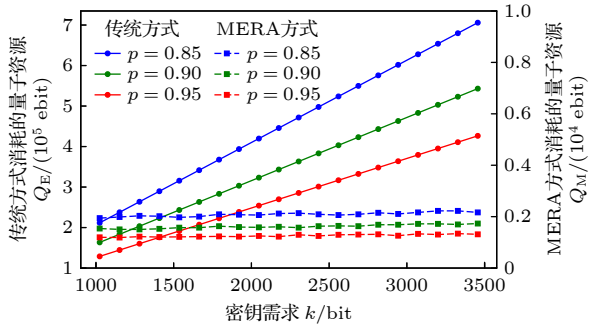


图 15 链路纠缠成功率分别取 85%, 90%, 95% 时, 量子资源的变化趋势

Fig. 15. Quantum resource variation at link entanglement success rates of 85%, 90%, and 95%.

5) 纠缠交换成功率对资源消耗的影响

实验参数设置为 $K=4$, $e=0.08$, $p=0.95$, $k=1024$. 纠缠交换成功率与链路纠缠成功率同样影响远距离纠缠的成功率, 所需量子资源数量的变化趋势如图 16 所示, 但相比之下, 链路纠缠成功率对远距离纠缠成功率的影响更为显著. 纠缠交换成功率越高, 远距离纠缠的成功率提升幅度也越大. 图 17 展示了在纠缠交换成功率为 85%, 90% 和 95% 时, 两种方法在不同请求量下消耗的量子资源变化情况.

通过对比实验可以发现, 平均路径跳数、链路纠缠成功率、纠缠交换成功率和误码率对资源消耗有显著影响. 具体来说, 平均路径跳数越大、链路纠缠成功率越低、纠缠交换成功率越低、误码率越高, 所需资源量也随之增加. 同时, 在相同的物理条件下, 本文的方法资源消耗明显低于传统方法, 且随着需求量的增加, 本文的方法对量子资源的需求增长更为平缓. 在量子资源有限的情况下, 本文的方法展现出了更大的优势.

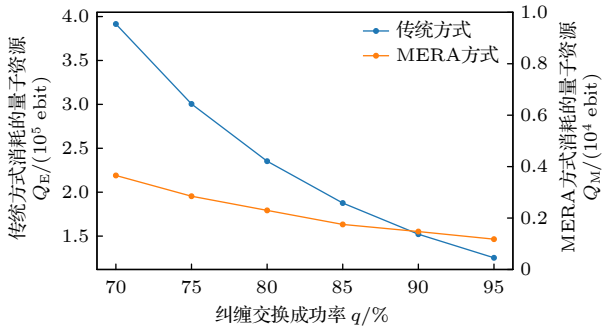


图 16 纠缠交换成功率从 70% 到 95% 变化时, 所需量子资源数量的变化趋势

Fig. 16. Quantum resource variation as entanglement swapping success rate ranges from 70% to 95%.

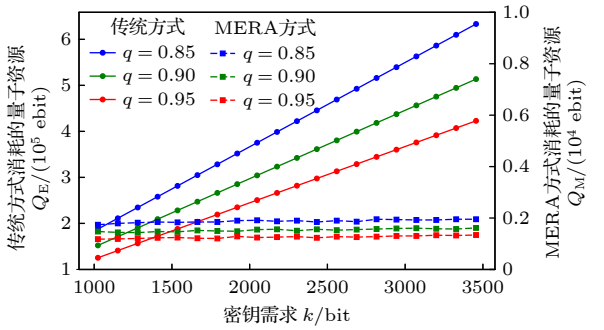


图 17 纠缠交换成功率为 85%, 90%, 95% 时, 量子资源的变化趋势

Fig. 17. Quantum resource variation at entanglement swapping success rates of 85%, 90%, and 95%.

5.2 成本分析

5.2.1 存储成本

在 S-D 之间生成的原始 MPS 态量子比特数量较多, 现有的存储技术难以满足需求. 为了解决这一问题, 本文通过应用无损压缩技术, 将原始 MPS 态压缩为单光子或少量光子的压缩态. 这种处理方式使得在现有技术条件下, 可以实现更长时间的量子态存储. 此外, 存储成本与所需的资源数量密切相关. 因此, 相较于传统方法, 本文的方法在存储成本上具有显著优势.

5.2.2 传输成本

本文方法的传输成本主要包括三个部分: 首先是 S-D 对之间共享的 MPS 态, 其资源消耗与 MPS 态的长度相关; 其次是控制器向 S-D 对下发的命令, 这些命令通过专用信道传输, 成本较高. 不过, 最频繁传输的是层数, 因此资源需求较少. 此外, 本文对 W 和 U 操作采用编号形式传输操作序列, 而非直接传输矩阵本身, 这大大降低了传

输成本. 总体而言, 传统方法的资源消耗显著高于 MERA 方法, 因此其传输成本也远高于 MERA 方法.

5.3 安全性分析

本文提出的方案在安全性上与传统 QKD 方法保持一致, 并未影响已有的安全性分析模型, 且优化了纠缠资源的使用. 与传统 QKD 协议相同, 本文方案依赖于不可克隆定理来确保纠缠对的安全分发. 然而, 由于本方案增加了步骤, 在安全性方面需应对新的挑战. 这里重点分析两方面的增强: 一是控制信息的安全传输, 二是共享矩阵积态 (MPS) 的保密性. 通过详细分析证明了这些增强不影响传统的安全性理论, 并保持了方案的整体安全性.

首先, 协议要求传输经典控制信息 (包括 MPS 态长度、压缩所用的酉变换及解压缩层数), 这一需求在传统 QKD 协议中并不存在. 尽管如此, 这些信息通过安全专用信道传输, 确保不受窃听威胁. 其次, 解压缩层数采用随机选择, 使窃听者难以推测正确的解压缩过程. 例如, 对于长度为 2048 的密钥请求, 若 MPS 态包含 256 个光子, MERA 态最高层数为 8, 需进行 $[16, 64]$ 次解纠缠. 假设解压缩次数为 32 次, 即便窃听者已获得共享的 MPS 态, 由于解压缩层数的随机性, 其每次猜对的概率为 $1/8$, 完全猜对 32 次的概率为 $1/2^{32}$, 几乎不可能破解密钥.

此外, 协议要求通信双方共享 MPS 态. 为防止窃听者获取, 设置安全参数 δ, 保证密钥分发的安全性. 若窃听者试图自行制备, 猜测单个量子比特的正确概率为 $1/2$, 对于长度为 128 的 MPS 态, 其成功猜测的概率为 $1/2^{128}$. 本协议设置 $\delta = 128$, 即 MPS 态长度 $n \geqslant 128$, 使窃听者的成功概率极低. 即便窃听者截获 MPS 态, 本协议不直接使用原始态, 而是通过压缩后的 MERA 态生成密钥, 进一步提升了安全性.

6 总 结

本文针对基于纠缠的 QKD 协议中的资源消耗问题, 提出了一种优化方案, 该方案充分利用了 MERA 的层次结构. 研究发现, 通过应用 MERA, 可以将 MPS 压缩为单光子或双光子态, 有效降低了量子存储的成本和复杂性. 在密钥分发过程中, 本文引入了安全参数以防止潜在的攻击, 并通过随机解压缩策略增强了安全性. 为了适应不同的通信需求, 本文方案采取了差异化处理: 在确保安全性的前提下, 仅使用一个共享的 MERA 态, 并允许对其底三层进行重复使用, 直到生成足够的密钥. 除非必要, 否则避免重新生成 MERA 态, 从而减少了额外的量子资源消耗. 这一策略在纠缠网络中尤为有效, 因为它减少了对链路纠缠的依赖, 而这些链路纠缠的建立通常受到距离、路径跳数和链路成功率等物理因素的限制.

通过理论分析和实验验证, 本文证明了所提方案在减少经典与量子资源使用方面的显著优势. 在现有技术条件下, 该方案满足了大规模量子密钥分发的需求, 为量子通信网络的资源优化提供了一种切实可行的策略.

参考文献

[1] Wootters W K, Zurek W H 1982 *Nature* **299** 802
[2] Peev M, Pacher C, Alléaume R 2009 *New J. Phys.* **11** 075001
[3] Dianati M, Alléaume R, Gagnaire M 2008 *Security Commun. Networks* **1** 57
[4] Aguado A, Lopez V, Lopez D 2019 *IEEE Commun. Mag.* **57** 20
[5] Donetti L, Hurtado P I, Munoz M A 2005 *Phys. Rev. Lett.* **95** 188701
[6] Li Z, Xue K P, Li J 2023 *IEEE Commun. Surv. Tutor.* **25** 2133
[7] Pant M, Krovi H, Towsley D 2019 *npj Quantum Inf.* **5** 25
[8] Shi S, Zhang X, Qian C 2024 *IEEE/ACM Trans. Netw.* **32** 2205
[9] Li J, Wang M, Xue K P 2022 *IEEE Trans. Commun.* **70** 6748
[10] Gu H Y, Li Z Y 2024 *IEEE/ACM Trans. Netw.* **1** 125
[11] Ekert A 1991 *Phys. Rev. Lett.* **67** 661
[12] Bennett C H, Brassard G, Mermin N D 1992 *Phys. Rev. Lett.* **68** 557
[13] Li C, Li T, Liu Y X 2021 *npj Quantum Inf.* **7** 10
[14] Lai H 2023 *Acta Phys. Sin.* **72** 170301 (in Chinese) [赖红 2023 物理学报 **72** 170301]
[15] Kim Y H, Kulik S P, Shih Y 2001 *Phys. Rev. Lett.* **86** 1370
[16] Cincio L, Dziarmaga J, Rams M M 2008 *Phys. Rev. Lett.* **100** 240603
[17] Lai H, Pieprzyk J, Pan L 2022 *Phys. Rev. A* **106** 052403
[18] Pirandola S, García-Patrón R, Braunstein S L 2009 *Phys. Rev. Lett.* **102** 050503
[19] Pirandola S, Laurenza R, Ottaviani C 2017 *Nat. Commun.* **8** 1500
[20] Wehner S, Elkouss D, Hanson R 2018 *Science* **362** 9288
[21] Bernien H, Hensen B, Pfaff W 2013 *Nature* **497** 86
[22] Olmschenk S, Matsukevich D N, Maunz P 2009 *Science* **323** 486
[23] Pan J W, Bouwmeester D, Weinfurter H 1998 *Phys. Rev. Lett.* **80** 3891

[24] Bravyi S, Cross A W, Gambetta J M 2024 *Nature* **627** 778
[25] Bersin E, Sutula M, Huan Y Q 2024 *PRX Quantum* **5** 010303
[26] Fan R, Bao Y, Altman E 2024 *PRX Quantum* **5** 020343
[27] Zhang Q, Lai H, Pieprzyk J 2022 *Phys. Rev. A* **105** 032439
[28] Lai H, Pieprzyk J, Pan L 2023 *Sci. China Inf. Sci.* **66** 180510
[29] Shannon C E 1949 *Bell Syst. Tech. J.* **28** 656
[30] Orús R 2014 *Ann. Phys.* **349** 117
[31] Chen L Q, Zhao M N, Yu K L 2021 *Quantum Inf. Process.* **20** 1
[32] Elkouss D, Martinez J, Lancho D 2010 *IEEE Information Theory Workshop on Information Theory* Cairo, Egypt, October 10–13, 2010 p1
[33] Gisin N, Ribordy G, Tittel W 2002 *Rev. Mod. Phys.* **74** 145
[34] Wu X, Zhu W P, Yan J 2017 *IEEE Trans. Veh. Technol.* **66** 8223
[35] Bennett C H, Brassard G, Robert J M 1988 *SIAM J. Comput.* **17** 210
[36] Eibl M, Kiesel N, Bourennane M, et al. 2004 *Phys. Rev. Lett.* **92** 077901
[37] Briegel H J, Raussendorf R 2001 *Phys. Rev. Lett.* **86** 910
[38] Affleck I, Kennedy T, Lieb E H 2004 *Condensed Matter Phys. Exactly Soluble Models: Selecta Elliott* (Berlin: Springer-Verlag) pp249–252
[39] Affleck I 1989 *J. Phys. Condens. Matter* **1** 3047

Quantum network communication resource optimization scheme based on multi-scale entanglement renormalization ansatz*

Lai Hong #† Ren Li # Huang Zhong-Rui Wan Lin-Chun

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

(Received 2 October 2024; revised manuscript received 29 October 2024)

Abstract

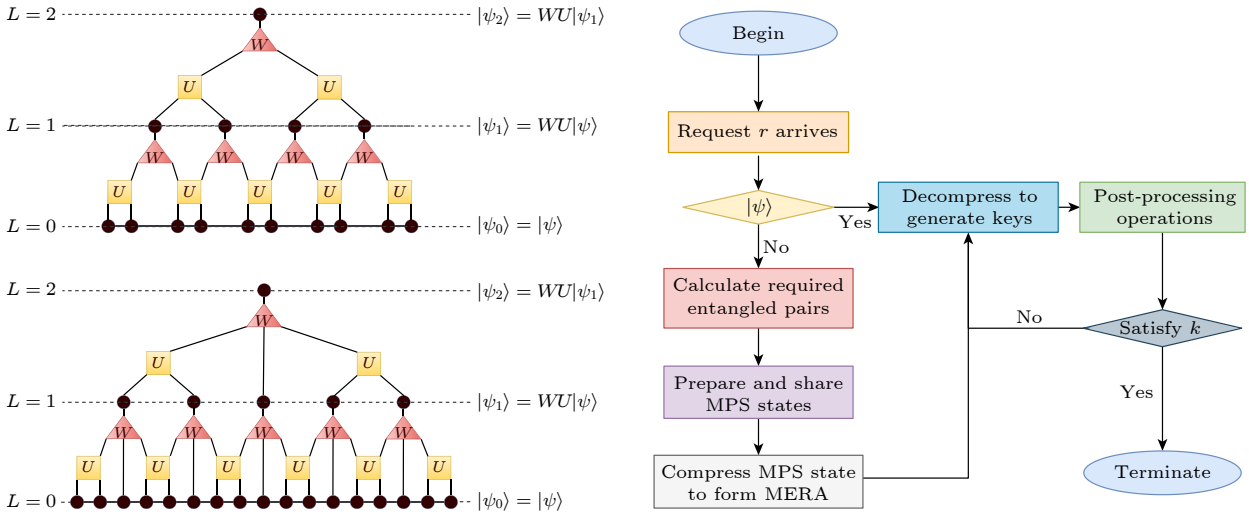
Quantum key distribution (QKD) is a pivotal technology in the field of secure communication by using the principles of quantum mechanics to implement theoretically unbreakable encryption. However, QKD faces significant challenges in achieving large-scale deployment. The primary hurdle lies in the scarcity of quantum resources, especially entangled photon pairs, which are fundamental to protocols such as Ekert91. In traditional QKD implementations, only a small potion of the generated entanglement pairs contribute to generating the original key, resulting in lower efficiency and resource waste. Resolving this limitation is crucial to the advancement and scalability of QKD networks.

This paper introduces an innovative approach to QKD by integrating the multiscale entanglement renormalization ansatz (MERA), a technique which is originally developed for many-body quantum systems. By utilizing MERA's hierarchical structure, the proposed method not only improves the efficiency of entanglement distribution but also reduces the consumption of quantum resources. Specifically, MERA compresses many-body quantum states into lower-dimensional representations, allowing for the transmission and storage of entanglement in a more efficient manner. This compression significantly reduces the number of qubits required, optimizing both entanglement utilization and storage capacity in quantum networks.

To evaluate the performance of this method, we conduct simulations under standardized conditions. In the simulation, a 1024-bit encryption request, an 8% error rate, an average path length of 4 hops in the quantum network, and a 95% success rate for link entanglement generation and entanglement swapping operations are assumed. These parameters reflect the real physical conditions in contemporary QKD networks. The results demonstrate that compared with traditional QKD protocols, the MERA-based approach saves 124151 entangled pairs, which is impressive. This significant reduction in resource consumption indicates the potential application of MERA in improving the efficiency of QKD systems without sacrificing security. Importantly, the security of the key exchange process remains intact, for the method inherently adheres to the principles of quantum mechanics, particularly the no-cloning theorem and the use of randomness in the decompression layer.

Some conclusions can be drawn below. The MERA not only enhances the scalability of QKD by optimizing quantum resource allocation, but also maintains the necessary security guarantees for practical cryptographic

applications. By integrating MERA into existing QKD frameworks, we can significantly reduce the resource overhead and make large-scale, secure quantum communication more feasible. These findings contribute a new dimension to the field of quantum cryptography, indicating that advanced quantum many-body techniques like MERA have the potential to unlock the full potential of quantum networks in real world.



Keywords: quantum key distribution, multi-scale entanglement renormalization ansatz, resource utilization, security

PACS: 03.67.–a, 03.67.Dd, 03.67.Hk, 03.67.Mn **DOI:** 10.7498/aps.73.20241382

CSTR: 32037.14.aps.73.20241382

* Project supported by the National Natural Science Foundation of China (Grant Nos. 61702427, 62301454), the Natural Science Foundation of Chongqing, China (Grant Nos. CSTB2022NSCQ-MSX0749, CSTB2023NSCQ-MSX0739), the Foundation of China Scholarship Council (Grant No. 202306990061), and the Southwest University's 2022 School-Level Teaching Reform Program, China (Grant No. 2022JY086).

# These authors contributed equally.

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

物理学报 Acta Physica Sinica
Chinese Physical Society
Institute of Physics, CAS

基于多尺度纠缠重整化假设的量子网络通信资源优化方案

赖红 任黎 黄钟锐 万林春

Quantum network communication resource optimization scheme based on multi-scale entanglement renormalization ansatz

Lai Hong Ren Li Huang Zhong-Rui Wan Lin-Chun

引用信息 Citation: Acta Physica Sinica, 73, 230301 (2024) DOI: 10.7498/aps.73.20241382
在线阅读 View online: https://doi.org/10.7498/aps.73.20241382
当期内容 View table of contents: http://wulixb.iphy.ac.cn