基于广义等距张量的压缩多光子纠缠态量子密钥分发*

赖红†

(西南大学计算机与信息科学学院, 重庆 400715)

(2023 年 4 月 13 日收到; 2023 年 6 月 2 日收到修改稿)

等距张量 (即张量 $\boldsymbol{\omega}$ 满足 $\boldsymbol{\omega}^{\dagger}\boldsymbol{\omega}=\boldsymbol{I}$) 为实现张量网络态 (tensor network states, TNSs) 中确定纠缠态的压缩提供了一种新颖而强大的数学构造算法. 结合等距张量, 本文发现在量子密钥分发 (quantum key distribution, QKD) 中可能采取完全不同的密钥生成方法, 即在不改变纠缠态结构和性质的情况下, 将任意多光子纠缠态压缩成单光子态或者 Bell 态. 在提出的 QKD 协议中, 输入态由任意纠缠态组成, 这些输入态首先被发送方 Alice 压缩成单光子态 $|0\rangle$ 或 $|1\rangle$ 或 Bell 态, 使得提出的协议同时达到了多模存储和确定性传输的要求, 且减少了需要传输和存储的量子比特数量, 从而提高了 QKD 协议的编码能力. 然后再添加诱骗态在这些单光子态 $|0\rangle$ 和 $|1\rangle$ 中, 再通过量子信道一起发送给接收方 Bob, 以制备密钥. 最后, Alice 和 Bob 利用筛选出来的压缩态 $|0\rangle$ 和 $|1\rangle$ 以及他们对应的等距张量的共轭转置来协商出共享密钥. 本文提出的协议比一般协议中的单光子能编码更多的经典比特, 显著提高了编码效率, 减少了量子资源的使用. 本文提出的 QKD 协议还保持了生成密钥的完美安全性.

关键词: 纠缠压缩, 广义等距张量, 张量网络态, 解压缩

PACS: 03.67.Ac, 03.67.Bg, 03.67.Dd, 03.67.Hk **DOI:** 10.7498/aps.72.20230589

1 引 言

1984 年, Bennett 和 Brassard[1] 提出了第一个量子密钥分发 (quantum key distribution, QKD) 协议, 即著名的 BB84 协议. 然而, BB84 协议有以下 3 个不足之处. 1) 为了保护协议免遭窃听, Bob 随机选择线性测量基“⊕”或者对角测量基“⊗”来测量收到的光子, 然而这会导致一半传输的光子不能用于加密密钥的生成. 结果, 少于 50% 的传输量子比特用于生成密码钥匙. 这意味着量子比特的利用率很低[2]. 2) 两光子量子态只能传输 1 比特经典信息, 即编码能力低. 3) 为了获得一个光子的信息, Alice 和 Bob 需要交换至少 2 比特经典信息. 换句话说, Bob 需要告诉 Alice 他为每个收到量子比特选择了什么测量基. Alice 需要告诉 Bob, 哪些量子态他们使用的是相同的测量基. 因此, 总的比特信息传输速率低 (大约 25%). 1991 年, Ekert[3] 提出了第一个基于纠缠的 QKD 协议, 即 Ekert91 协议. Ekert91 协议的不足之处与 BB84 协议一样. 但是 Ekert91 协议的安全性是通过分析贝尔不等式来论证的. 然而, 如果纠缠粒子完全退相干, 则测量结果是完全随机的. 换句话说, 量子通信的安全性不能用贝尔不等式来论证. 1992 年, Bennett 等[4] 提出了一个 Ekert91 协议的改进版本, 即 BBM92 (Bennett-Brassard -Mermin) 协议. 与 Ekert91 协

* 国家自然科学基金 (批准号: 61702427)、重庆市面上自然科学基金 (批准号: CSTB2022NSCQ-MSX0749) 和西南大学 2022 年校级教改项目 (批准号: 2022JY086) 资助的课题.

† 通信作者. E-mail: hlai@swu.edu.cn

议不同, BBM92 协议不是采用贝尔不等式进行安全性分析, 而是采用与 BB84 协议相同的安全分析. Greenberger 等 [5] 提出了一种方法来生成一组两个以上粒子的纠缠态, 即 Greenberger-Horne-Zeilinger (GHZ) 态. 后来, Bouwmeester 等 [6] 提出了关于 GHZ 态行为的实验观察. 同时 GHZ 态被用于设计三方 QKD 协议 [7−23]. 随后, 许多新颖的 QKD 协议被提出 [24−26].

最近, 量子数据压缩已成为热门话题, 因为量子存储仍然存在非常昂贵且供不应求的问题 [27−35]. 例如, Fan 等 [27] 设计了两种量子数据压缩协议, 分别适用于压缩四个和五个完全相同的量子比特. Bostroem 和 Felbinger[28] 在他们的协议中提出了一个无损、瞬时量子数据压缩协议. 该协议应用了可变长度量子消息的框架. Plesch 和 Bužek [30] 同样提出了利用 N 个相同的制备的量子编码. Rozemae 等 [31] 证明 N 个相同制备的量子比特的集合可压缩到 $\log_2^N$ 量子比特. 而且, 学者还提出使用机器学习和量子自动编码器来改善压缩. 而基于纠缠态的 QKD 研究中的一个中心问题是纠缠态是否可以被压缩成单光子态. Acoleyen 等 [36] 已经肯定地回答了这个问题. 他们证明纠缠压缩可以通过在多尺度纠缠重整化假设 (multiscale entanglement renormalisation ansatz, MERA) 的等距和矩阵乘积算符 (matrix product operator, MPO) 的局域张量之间构建映射来实现. 2023 年, Lai 等 [37] 将 MERA 压缩方法用到 QKD 协议的设计中, 即提出用构造的等距张量压缩多光子纠缠态. 但是, 在 Lai 等 [37] 的协议里, 没有进一步扩展它们构造的等距张量在 QKD协议的应用, 以及缺少相应的功能分析和安全性分析.

尽管量子数据压缩带来了很多优势, 但也带来了挑战. 最重要的是它的安全性. Evenbly[38] 提出了一类可用作监督学习中的分类器的数态保迹张量网络. 但他发现纠缠态的乘积态无法将中间态与经典数据联系起来. 这意味着可解释性损失. 然而, 本文却相信正是这种可解释性损失可以用来确保 QKD 的安全性. 具体地, 本文应用 Evenbly[38] 提出的数态保迹的等距矩阵, 基于 Lai 等 [37] 构造的广义等距张量来更系统更全面地展示 QKD 中压缩纠缠态的优势及其安全性分析, 同时解决 BB84, Ekert91, BBM92 和基于 GHZ 的 QKD 协议的不足. 因此, 本文的扩展超越了简单减少需要传输和存储的量子比特数量以及消耗更少的量子资源 (量子比特和内存). 此外, 本文的 QKD 协议允许将经典信息更有效地编码为量子比特. 更容易保护协议免受退相干. 本文通过例子来介绍本文的协议. 在示例中, Alice 使用等距张量从 $N\,(N \geqslant 3)$ 光子 GHZ 态制备一个压缩的数态 $|0\rangle$ 或 $|1\rangle$ 或 Bell 态. 然后, Alice 通过量子信道将压缩后的数态与诱骗态一起发送给 Bob. 最后, Alice 和 Bob 可以通过筛选出来的压缩态 $|0\rangle$ 和 $|1\rangle$ 解压缩达成一致密钥. 此外, 本文的协议还保持了共享密钥的完美安全性.

2 背景知识

首先介绍等距矩阵的定义及其性质, 然后给出了用于纠缠压缩的广义等距张量的严格数学定义.

2.1 等距矩阵及其性质

定义 1 (等距矩阵 [38]) 给定一个 $d_1 \times d_2$ 矩阵 $\boldsymbol{\omega}$ 使得 $\boldsymbol{\omega}^\dagger\boldsymbol{\omega} = \boldsymbol{I}$ (当 $d_1 < d_2$) 或 $\boldsymbol{\omega}\boldsymbol{\omega}^\dagger = \boldsymbol{I}$ (当 $d_1 > d_2$), 则 $\boldsymbol{\omega}$ 称为等距矩阵.

例如, 令 $\boldsymbol{\omega} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & \sin\theta & \cos\theta & 0 \end{pmatrix}$, 可易得 $\boldsymbol{\omega}\boldsymbol{\omega}^\dagger = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \boldsymbol{I}$. 所以 $\boldsymbol{\omega}$ 是等距矩阵. 这里等距是指内积 (模) 保迹映射, 即:

$$\begin{aligned} &|\psi\rangle \to \boldsymbol{\omega}\,|\psi\rangle\,, \quad |\boldsymbol{\Phi}\rangle \to \boldsymbol{\omega}\,|\boldsymbol{\Phi}\rangle\,, \\ &\boldsymbol{\omega}^\dagger\boldsymbol{\omega} = I \Rightarrow \langle\boldsymbol{\Phi}\mid\psi\rangle = \langle\boldsymbol{\Phi}|\,\boldsymbol{\omega}^\dagger\boldsymbol{\omega}\,|\psi\rangle\,. \end{aligned} \tag{1}$$

(1) 式表明等距矩阵 $\boldsymbol{\omega}$ 保证两个量子态在小空间的内积等于它们映射到大空间的像的内积.

2.2 广义等距张量及其性质

定义 2 (第一类广义的等距张量 [37]) 广义的等距张量 $\boldsymbol{w}(\boldsymbol{w}_{N1}, \boldsymbol{w}_{N2})$, $N \geqslant 3$ 定义如下:

$$\begin{aligned} \boldsymbol{w}_{N1} &= \begin{bmatrix} \dfrac{\sqrt{2}}{2} & 0 & \cdots & 0 & \dfrac{\sqrt{2}}{2} \\ 0 & \dfrac{\sqrt{2}}{2} & \cdots & \dfrac{\sqrt{2}}{2} & 0 \end{bmatrix} \\ &= \frac{\sqrt{2}}{2}\begin{bmatrix} 1 & 0 & \cdots & 0 & 1 \\ 0 & 1 & \cdots & 1 & 0 \end{bmatrix}, \end{aligned} \tag{2}$$

$$\boldsymbol{w}_{N2}=\begin{bmatrix}0 & \sqrt{2}/2 & \cdots & \sqrt{2}/2 & 0\\ \sqrt{2}/2 & 0 & \cdots & 0 & \sqrt{2}/2\end{bmatrix}=\frac{\sqrt{2}}{2}\begin{bmatrix}0 & 1 & \cdots & 1 & 0\\ 1 & 0 & \cdots & 0 & 1\end{bmatrix}. \tag{3}$$

注意, 在下文第 3 节中, 等距张量 $\boldsymbol{w}(\boldsymbol{w}_{N1},\boldsymbol{w}_{N2})$ 被用于实现纠缠压缩. 显然, $\boldsymbol{w}(\boldsymbol{w}_{N1},\boldsymbol{w}_{N2})$不是一个可逆映射, 但它可以导出一个逆映射$\boldsymbol{w}^{\dagger}(\boldsymbol{w}_{N1}^{\dagger},\boldsymbol{w}_{N2}^{\dagger})$, 而逆映射 $\boldsymbol{w}^{\dagger}(\boldsymbol{w}_{N1}^{\dagger},\boldsymbol{w}_{N2}^{\dagger})$可以对压缩纠缠态进行解压缩. 其中 $\boldsymbol{w}(\boldsymbol{w}_{N1},\boldsymbol{w}_{N2})$满足以下条件:

$$\boldsymbol{\omega}:\boldsymbol{\nu}_{\rm in}\to\boldsymbol{\nu}_{\rm out},\boldsymbol{\omega}\boldsymbol{\omega}^{\dagger}=\boldsymbol{I}=\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix}, \tag{4}$$

并且

$$\boldsymbol{\omega}^{\dagger}:\boldsymbol{\nu}_{\rm out}\to\nu_{\rm in},\ \boldsymbol{\omega}\boldsymbol{\omega}^{\dagger}=\begin{pmatrix}1 & 0 & \cdots & 0\\ 0 & 1 & \cdots & 0\\ \vdots & \vdots & \vdots & \vdots\\ 0 & \cdots & 0 & 1\end{pmatrix}. \tag{5}$$

第一类广义等距张量可用于压缩任何 N-光子 GHZ 纠缠态为单光子态.

定义 3 (第二类广义的等距张量[37]) 广义的等距张量$\boldsymbol{w}'(\boldsymbol{w}'_{N1},\boldsymbol{w}'_{N2})$定义如下:

$$\boldsymbol{w}'_{N1}=\begin{bmatrix}1 & 0 & 0 & 0 & 0 & \cdots & 0\\ 0 & 1/\sqrt{2^{N-1}-1} & 0 & 1/\sqrt{2^{N-1}-1} & 0 & \cdots & 0\\ 0 & 0 & 1/\sqrt{2^{N-1}-1} & 0 & 1/\sqrt{2^{N-1}-1} & \cdots & 0\\ 0 & 0 & 0 & 0 & 0 & \cdots & 1\end{bmatrix}_{4\times 2^N}, \tag{6}$$

注意在等距张量$\boldsymbol{w}'_{N1}$的第 2, 3 行, 非零元的个数为$2^{N-1}-1$.

$$\boldsymbol{w}'_{N2}=\begin{bmatrix}0 & 1/\sqrt{2^{N-1}-1} & 0 & 1/\sqrt{2^{N-1}-1} & 0 & \cdots & 0\\ 1 & 0 & 0 & 0 & 0 & \cdots & 0\\ 0 & 0 & 0 & 0 & 0 & \cdots & 1\\ 0 & 0 & 1/\sqrt{2^{N-1}-1} & 0 & 1/\sqrt{2^{N-1}-1} & \cdots & 0\end{bmatrix}_{4\times 2^N}. \tag{7}$$

注意在等距张量$\boldsymbol{w}'_{N2}$的第 1, 4 行, 非零元的个数为$2^{N-1}-1$. 其中$\boldsymbol{w}'(\boldsymbol{w}'_{N1},\boldsymbol{w}'_{N2})$满足以下条件:

$$\boldsymbol{w}':\boldsymbol{\nu}_{\rm in}\to\boldsymbol{\nu}_{\rm out},\ \ |\boldsymbol{\varphi}'\rangle=\boldsymbol{w}'|\boldsymbol{\varphi}\rangle,$$

$$\boldsymbol{w}'\boldsymbol{w}'^{\dagger}=\boldsymbol{I}\otimes\boldsymbol{I}=\begin{pmatrix}1 & 0 & 0 & 0\\ 0 & 1 & 0 & 0\\ 0 & 0 & 1 & 0\\ 0 & 0 & 0 & 1\end{pmatrix},$$

$$\boldsymbol{w}'^{\dagger}:\boldsymbol{\nu}_{\rm out}\to\nu_{\rm in},\ \ |\boldsymbol{\varphi}'\rangle=\boldsymbol{w}'^{\dagger}|\boldsymbol{\varphi}\rangle.$$

第二类广义等距张量可用于压缩任何 N-光子 GHZ 纠缠态为 Bell 态.

3 基于纠缠压缩的 QKD 协议

本节将展示如何使用广义等距张量设计两个基于纠缠压缩的 QKD 协议. 设计这样协议的目的是减少通信和存贮的开销和全面的揭示纠缠压缩的 QKD 协议的优势. 在这里, 通信和存储开销被理解为在协议执行期间交换和存储的量子比特数. 由于量子信息处理设备的许多想法都是基于在网络节点之间用一个相对较小的量子处理器发送量子信息的, 因此找到用于压缩传输的量子数据的协议具有重要的实际意义. 更一般地, 大部分量子信息理论都涉及在局域约束[39]下对数据的进行操作, 因此本文提出协议自然地与这些研究需求相关联. 在协议中, 本文假设 Alice 可以制备任何纠缠态且独立地利用一系列等距张量将这些纠缠态压缩为单光子态或者 Bell 态, 然后将压缩后的单光子态或者 Bell 态纠缠光子通过量子信道发送给 Bob, Bob 随机选择测量基测量这些压缩的单光子态, 然后对筛选后的压缩的单光子态或者 Bell 态纠缠光子进行解压缩来得到密钥.

3.1 第一个协议的描述

给定 $N\geqslant 3$, 本文取 N 光子 GHZ 纠缠态. 本文的 QKD 协议按以下步骤执行.

步骤 1 制备压缩单光子态. 该步骤由 Alice 执行. 利用 (2) 式和 (3) 式中的等距张量 $\boldsymbol{w}(\boldsymbol{w}_{N1},\boldsymbol{w}_{N2})$.

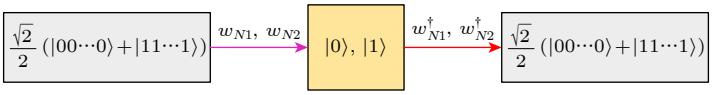

图 1 利用 w_{N1}, w_{N2}, N 光子 GHZ 纠缠态 $(\sqrt{2}/2)(|00\cdots0\rangle+|11\cdots1\rangle)$ 被随机压缩为数态 $|0\rangle$或 $|1\rangle$, 利用 $\boldsymbol{w}_{N1}^{\dagger},\boldsymbol{w}_{N2}^{\dagger}$, $|0\rangle$或 $|1\rangle$ 被解压缩为 N 光子 GHZ 纠缠态 $(\sqrt{2}/2)(|00\cdots0\rangle+|11\cdots1\rangle)$ 示意图

Fig. 1. The schematic compression of $(\sqrt{2}/2)(|00\cdots0\rangle+|11\cdots1\rangle)$ into $|0\rangle$ or $|1\rangle$ using $\boldsymbol{w}_{N1},\boldsymbol{w}_{N2}$, and decompression of $|0\rangle$ or $|1\rangle$ into $(\sqrt{2}/2)(|00\cdots0\rangle+|11\cdots1\rangle)$ using $\boldsymbol{w}_{N1}^{\dagger},\boldsymbol{w}_{N2}^{\dagger}$.

N 光子 GHZ 纠缠态被 Alice 压缩为数态$|0\rangle$和$|1\rangle$(参见图 1). 即 $(\sqrt{2}/2)(|00\cdots0\rangle+|11\cdots1\rangle)$使用 $\boldsymbol{w}(\boldsymbol{w}_{N1},\boldsymbol{w}_{N2})$后被压缩的数态分别为$|0\rangle$和$|1\rangle$, 具体数学表达式为

$$\boldsymbol{w}_1\left(\frac{\sqrt{2}}{2}(|00\cdots0\rangle+|11\cdots1\rangle)\right)=\begin{bmatrix}\frac{\sqrt{2}}{2} & 0 & \cdots & 0 & \frac{\sqrt{2}}{2}\\ 0 & \frac{\sqrt{2}}{2} & \cdots & \frac{\sqrt{2}}{2} & 0\end{bmatrix}\begin{pmatrix}\sqrt{2}/2\\0\\\vdots\\0\\\sqrt{2}/2\end{pmatrix}=\begin{pmatrix}1\\0\end{pmatrix},\tag{8}$$

$$\boldsymbol{w}_{N2}\left(\frac{\sqrt{2}}{2}(|00\cdots0\rangle+|11\cdots1\rangle)\right)=\begin{bmatrix}0 & \frac{\sqrt{2}}{2} & \cdots & \frac{\sqrt{2}}{2} & 0\\ \frac{\sqrt{2}}{2} & 0 & \cdots & 0 & \frac{\sqrt{2}}{2}\end{bmatrix}\begin{pmatrix}\sqrt{2}/2\\0\\\vdots\\0\\\sqrt{2}/2\end{pmatrix}=\begin{pmatrix}0\\1\end{pmatrix}.\tag{9}$$

步骤 2 压缩单光子态的传输. Alice 通过一个量子信道将压缩后的单光子态发送给 Bob. 在这里 Alice 和 Bob 约定, 当得到压缩态为数态$|0\rangle$和$|1\rangle$时, 分别解压缩得到 n 比特的经典信息$00\cdots0$和$11\cdots1$. 这些通过量子信道的传输的压缩单光子态受到诱骗态的保护.

步骤 3 用于窃听检测的诱骗态. Alice 随机选择基 $B_z=\{|0\rangle,|1\rangle\}$, $B_x=\{|+\rangle,|-\rangle\}$用于产生诱骗态, 其中$|+\rangle=(|0\rangle+|1\rangle)/\sqrt{2}$. 随后将诱骗态随机插入到压缩单光子态序列中, 并记录这些诱骗态的位置及初始态. 一旦 Bob 确认收到粒子后, Alice 公布诱骗态的位置及测量这些诱骗态的测量基. Bob 完成测量后, 通过认证广播信道通知 Alice 他的测量结果. 通过比较诱骗态的初始态与参与者测量得到的态, Alice 可计算这些诱骗态的错误率. 如果错误率高于某个预先设定的阈值, 则协议中止, 否则继续.

步骤 4 压缩纠缠态的测量. 该步骤类似于 BB84[1] 的相应步骤. 在接收到一个压缩纠缠态后, Bob 随机选择一个基进行测量. 接下来, Bob 用认证广播信道告诉 Alice 其选择的基. 最后, 通过对基后, Alice 通过认证广播信道通知 Bob 等距张量用于解压缩相应的压缩纠缠态. 最后, 他们使用 $\boldsymbol{w}_{N1}^{\dagger},\boldsymbol{w}_{N2}^{\dagger}$解压缩最后筛选出来的压缩纠缠态如下所示:

$$\boldsymbol{w}_{N1}^{\dagger}|0\rangle=\frac{\sqrt{2}}{2}\begin{pmatrix}1 & 0\\0 & 1\\\cdots & \cdots\\0 & 1\\1 & 0\end{pmatrix}\begin{pmatrix}1\\0\end{pmatrix}=\begin{pmatrix}\sqrt{2}/2\\0\\\vdots\\0\\\sqrt{2}/2\end{pmatrix}=\frac{\sqrt{2}}{2}(|00\cdots0\rangle+|11\cdots1\rangle),\tag{10}$$

$$\boldsymbol{w}_{N2}^{\dagger}|0\rangle=\frac{\sqrt{2}}{2}\begin{pmatrix}0&1\\1&0\\\vdots&\vdots\\1&0\\0&1\end{pmatrix}\begin{pmatrix}0\\1\end{pmatrix}=\begin{pmatrix}\sqrt{2}/2\\0\\\vdots\\0\\\sqrt{2}/2\end{pmatrix}=\frac{\sqrt{2}}{2}\left(|00\cdots0\rangle+|11\cdots1\rangle\right),\tag{11}$$

整个过程如表 1 所示.

步骤 5 密钥协商. 此步考虑被解压缩回 N 光子 GHZ 态所编码的经典比特信息. 当 Alice 和 Bob 解压缩被筛选出来的单光子为 $(\sqrt{2}/2)(|00\cdots0\rangle+|11\cdots1\rangle)$, 他们根据步骤 2 的约定, 可得到经典信息 $00\cdots0$ 和 $11\cdots1$, 把它们串接到一起就得到了生密钥.

3.2 第二个协议的描述

本节描述了一种将任何 N 光子 GHZ 态压缩为 Bell 态的协议 (参见图 2). 其实很多量子信息理论都与局域约束下 [39] 的量子数据操作有关, 因此本文的协议自然与这些研究相关. 对于任何纠缠态, 本文基于 Lai 等 [37] 定义的广义等距张量展示了一种最佳压缩它们的方法, 且充分利用了 Alice 和 Bob 之间压缩贝尔态的相关性来实现 QKD. 本文的第 2 个 QKD 协议步骤如下.

步骤 1 制备压缩 Bell 态. 首先, 在奇数位的和偶数位的压缩 Bell 态分别为 $\frac{\sqrt{2}}{2}(|00\rangle+|11\rangle)$, $\frac{\sqrt{2}}{2}(|01\rangle+|10\rangle)$. 该步骤由 Alice 执行. 利用 (6) 式和 (7) 式中的等距张量 $\boldsymbol{w}'(\boldsymbol{w}'_{N1},\boldsymbol{w}'_{N2})$, N 光子 GHZ 态被 Alice 压缩为 Bell 态 (参见图 2). 这是因为任何 N 光子 GHZ 态可以被转化为了一个矩阵 $\boldsymbol{V}_{2^N\times1}$, $\boldsymbol{w}'(\boldsymbol{w}'_{N1},\boldsymbol{w}'_{N2})$是行列为 4×2^N 的矩阵, 于是 $\boldsymbol{w}'\boldsymbol{V}$ 的行列为 4×1 的矩阵, 且可以进一步转化为 Bell 态.

以 3 光子 GHZ 态即 $(\sqrt{2}/2)(|000\rangle+|111\rangle)$ 为例, 其矩阵表达形式为 $(\sqrt{2}/2\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ \sqrt{2}/2)^{\mathrm{T}}$, Alice 使用 $\boldsymbol{w}'(\boldsymbol{w}'_{31},\boldsymbol{w}'_{32})$将 3 光子 GHZ 态 $\frac{\sqrt{2}}{2}(|000\rangle+|111\rangle)$ 压缩为 $(\sqrt{2}/2)(|00\rangle+|11\rangle)$, $(\sqrt{2}/2)(|01\rangle+|10\rangle)$, 具体数学表达式为

表 1 压缩纠缠态用于在 Alice 和 Bob 之间生成密钥的例子

Table 1. An example of transmitting the compressed entangled state for generating a secret key between Alice and Bob.

Alice随机制备纠缠态	$(\sqrt{2}/2)(\|000\rangle+\|111\rangle)$	$(\sqrt{2}/2)(\|0000\rangle+\|1111\rangle)$	$N(N\geqslant5)$ 光子GHZ态
Alice随机选择等距张量	$\boldsymbol{w}_{31}$	$\boldsymbol{w}_{41}$	$\boldsymbol{w}_{N2}$
Alice压缩纠缠态	$\|0\rangle$	$\|0\rangle$	$\|0\rangle$
Alice随机选择测量基	B_x	B_z	B_z
Bob随机选择测量基	B_z	B_z	B_x
对基	否	是	否
筛选出的共享压缩态	—	$\|0\rangle$	—
解压缩共享压缩态	—	$(\sqrt{2}/2)(\|0000\rangle+\|1111\rangle)$	—

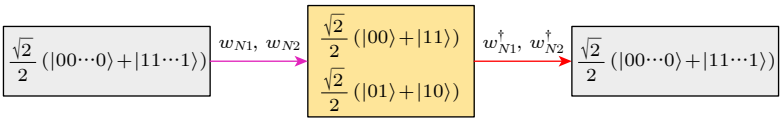

图 2 利用 $\boldsymbol{w}'_{N1},\boldsymbol{w}'_{N2}$, N 光子 GHZ 纠缠态 $(\sqrt{2}/2)(|00\cdots0\rangle+|11\cdots1\rangle)$ 被随机压缩为 Bell 态 $(\sqrt{2}/2)(|00\rangle+|11\rangle)$ 或 $(\sqrt{2}/2)(|01\rangle+|10\rangle)$, 利用 $\boldsymbol{w}'^{\dagger}_{N1},\boldsymbol{w}'^{\dagger}_{N2}$, Bell 态 $(\sqrt{2}/2)(|00\rangle+|11\rangle)$ 或 $(\sqrt{2}/2)(|01\rangle+|10\rangle)$ 被解压缩为 N 光子 GHZ 纠缠态 $(\sqrt{2}/2)(|00\cdots0\rangle+|11\cdots1\rangle)$ 示意图

Fig. 2. The schematic compression of $(\sqrt{2}/2)(|00\cdots0\rangle+|11\cdots1\rangle)$ into $(\sqrt{2}/2)(|00\rangle+|11\rangle)$ or $(\sqrt{2}/2)(|01\rangle+|10\rangle)$ using $\boldsymbol{w}'_{N1}$, $\boldsymbol{w}'_{N2}$, and decompression of $(\sqrt{2}/2)(|00\rangle+|11\rangle)$ or $(\sqrt{2}/2)(|01\rangle+|10\rangle)$ into $(\sqrt{2}/2)(|00\cdots0\rangle+|11\cdots1\rangle)$ using $\boldsymbol{w}'^{\dagger}_{N1},\boldsymbol{w}'^{\dagger}_{N2}$.

$$\boldsymbol{w}'_{31}\left((\sqrt{2}/2)\left(|000\rangle+|111\rangle\right)\right)$$

$$=\begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & \frac{1}{\sqrt{3}} & 0 & \frac{1}{\sqrt{3}} & 0 & \frac{1}{\sqrt{3}} & 0 & 0 \\ 0 & 0 & \frac{1}{\sqrt{3}} & 0 & \frac{1}{\sqrt{3}} & 0 & \frac{1}{\sqrt{3}} & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}_{4\times 8}\begin{pmatrix} \sqrt{2}/2 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ \sqrt{2}/2 \end{pmatrix}_{8\times 1}=\begin{pmatrix} \sqrt{2}/2 \\ 0 \\ 0 \\ \sqrt{2}/2 \end{pmatrix}=\frac{\sqrt{2}}{2}(|00\rangle+|11\rangle), \tag{12}$$

$$\boldsymbol{w}'_{32}\left((\sqrt{2}/2)\left(|000\rangle+|111\rangle\right)\right)$$

$$=\begin{bmatrix} 0 & \frac{1}{\sqrt{3}} & 0 & \frac{1}{\sqrt{3}} & 0 & \frac{1}{\sqrt{3}} & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & \frac{1}{\sqrt{3}} & 0 & \frac{1}{\sqrt{3}} & 0 & \frac{1}{\sqrt{3}} & 0 \end{bmatrix}_{4\times 8}\begin{pmatrix} \sqrt{2}/2 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ \sqrt{2}/2 \end{pmatrix}_{8\times 1}=\begin{pmatrix} 0 \\ \sqrt{2}/2 \\ \sqrt{2}/2 \\ 0 \end{pmatrix}=\frac{\sqrt{2}}{2}(|01\rangle+|10\rangle). \tag{13}$$

步骤 2　压缩 Bell 态的传输. Alice 通过量子信道将每个压缩后的 Bell 态中的一个光子发送给 Bob, 另一个自己保留. 在这里, Alice 和 Bob 约定: 当得到压缩 Bell 态分别为 $(\sqrt{2}/2)\left(|00\rangle+|11\rangle\right)$, $(\sqrt{2}/2)\left(|01\rangle+|10\rangle\right)$, 解压缩得到 n 比特的经典信息就分别为 $00\cdots0$ 和 $11\cdots1$. 这些通过量子信道的传输的压缩 Bell 态纠缠光子受到诱骗态的保护.

步骤 3　用于窃听检测的诱骗态. Alice 随机选择基 $B_z=\{|0\rangle,|1\rangle\}$, $B_x=\{|+\rangle,|-\rangle\}$用于产生诱骗态, 其中 $|+\rangle=(|0\rangle+|1\rangle)/\sqrt{2}$. 随后将诱骗态随机插入到压缩单光子态序列中, 并记录这些诱骗态的位置及初始态. 一旦在 Bob 确认收到粒子后, Alice 公布诱骗态的位置及测量这些诱骗态的测量基. Bob 完成测量后, 通过认证广播信道通知 Alice 他的测量结果. 通过比较诱骗态的初始态与参与者测得的态, Alice 可计算这些诱骗态的错误率. 如果错误率高于某个预先设定的阈值, 则协议中止, 否则继续.

步骤 4　压缩 Bell 态的测量. 该步骤类似于 BBM92[4] 的相应步骤. 在接收到一个压缩纠缠态光子后, Bob 随机选择一个基进行测量. 接下来, Bob 用认证广播信道告诉 Alice 其选择的基. 然后通过对基后, 根据步骤 1 的约定, Alice 和 Bob 可以得到相应的压缩 Bell 态. 最后, Alice 通过认证广播信道通知 Bob 等距张量用于解压缩相应的压缩纠缠态, 即他们使用 $\boldsymbol{w'}^{\dagger}_{N1},\boldsymbol{w'}^{\dagger}_{N2}$ 解压缩最后筛选出来的压缩 Bell 态. 这里以等式 (12) 和 (13) 为例说明, 可得如下等式:

$$\boldsymbol{w}^{\dagger}_{31}\left(\frac{\sqrt{2}}{2}\left(|00\rangle+|11\rangle\right)\right)=\frac{\sqrt{2}}{2}\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1/\sqrt{3} & 0 & 0 \\ 0 & 0 & 1/\sqrt{3} & 0 \\ 0 & 1/\sqrt{3} & 0 & 0 \\ 0 & 0 & 1/\sqrt{3} & 0 \\ 0 & 1/\sqrt{3} & 0 & 0 \\ 0 & 0 & 1/\sqrt{3} & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}\begin{pmatrix} 1 \\ 0 \\ 0 \\ 1 \end{pmatrix}=\begin{pmatrix} \sqrt{2}/2 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ \sqrt{2}/2 \end{pmatrix}=\frac{\sqrt{2}}{2}\left(|000\rangle+|111\rangle\right), \tag{14}$$

$$\boldsymbol{w}_{32}^{\dagger}\left(\frac{\sqrt{2}}{2}\left(|01\rangle+|10\rangle\right)\right)=\frac{\sqrt{2}}{2}\begin{bmatrix}0&1&0&0\\1/\sqrt{3}&0&0&0\\0&0&0&1/\sqrt{3}\\1/\sqrt{3}&0&0&0\\0&0&0&1/\sqrt{3}\\1/\sqrt{3}&0&0&0\\0&0&0&1/\sqrt{3}\\0&0&1&0\end{bmatrix}\begin{pmatrix}0\\1\\1\\0\end{pmatrix}=\begin{pmatrix}\sqrt{2}/2\\0\\0\\0\\0\\0\\0\\\sqrt{2}/2\end{pmatrix}=\frac{\sqrt{2}}{2}\left(|000\rangle+|111\rangle\right). \quad (15)$$

步骤 5　密钥协商. 考虑被解压缩回 N 光子 GHZ 态所编码的经典比特信息. 当 Alice 和 Bob 解压缩被筛选出来的单光子为 $\frac{\sqrt{2}}{2}(|00\cdots0\rangle+|11\cdots1\rangle)$, 他们根据步骤 2 的约定, 可得到经典信息 $00\cdots0$ 和 $11\cdots1$, 把它们串接到一起就得到生密钥.

4　性能分析

4.1　压缩性和解压缩性

本文的 QKD 协议可以利用等距张量将任何纠缠态压缩为单光子态或 Bell 态. 确切地说, 本文使用等距张量 $\boldsymbol{w}(\boldsymbol{w}_{N1},\boldsymbol{w}_{N2})$, $\boldsymbol{w}'(\boldsymbol{w}'_{N1},\boldsymbol{w}'_{N2})$ 将 $\frac{\sqrt{2}}{2}(|00\cdots0\rangle+|11\cdots1\rangle)$ 压缩为 $\frac{\sqrt{2}}{2}(|00\rangle+|11\rangle)$, $\frac{\sqrt{2}}{2}(|01\rangle+|10\rangle)$ 和单光子态 $|0\rangle,|1\rangle$. 同时, $\frac{\sqrt{2}}{2}(|00\rangle+|11\rangle)$, $\frac{\sqrt{2}}{2}(|01\rangle+|10\rangle)$ 和单光子态 $|0\rangle,|1\rangle$ 可以通过 $\boldsymbol{w}'^{\dagger}_{N1},\boldsymbol{w}'^{\dagger}_{N2},\boldsymbol{w}^{\dagger}_{N1},\boldsymbol{w}^{\dagger}_{N2}$ 完全解压缩为 $\frac{\sqrt{2}}{2}(|00\cdots0\rangle+|11\cdots1\rangle)$. 特别强调的是, 虽然本文构造的等距张量并非方阵组成, 其转置并非其逆, 但是因为构造的等距张量的巧妙性, 使得可以保证完全的解压缩回原来的态, 具体例子请看等式 (10), (11), (14) 和 (15), 故压缩对信息传递是无影响的.

不仅压缩和解压缩的过程非常简单, 而且使用等距张量进行纠缠压缩可以使用量子电路和当前技术来实现. 由于量子信息处理设备的许多想法都是基于在网络节点之间用一个相对较小的量子处理器发送量子信息的, 因此找到用于压缩传输的量子数据的协议具有重要的实际意义. 更一般地, 大部分量子信息理论都涉及在局域约束 [39] 下对数据的进行操作, 因此本文提出的协议自然地与这些研究需求相关联.

4.2　抗退相干性

在 Ekert91[3] 和 BBM92[4] 协议中和基于 GHZ 态的 QKD 协议中 [7−23] 要求是纠缠态. 然而, 纠缠粒子在实际传输和存储过程中会相互作用, 从而导致纠缠系统的粒子之间的退相干 (或纠缠退化). 这在本文的第一个协议中是可以避免的, 因为纠缠态被压缩成一个单光子态. 因此, 本文的协议可以抗退相干. 更多的细节在下面的表 2 可见.

表 2　本文的协议与文献 [4, 16, 20] 中的协议进行了比较
Table 2.　Our protocol compares with the protocols in Refs.[4, 16, 20].

	BBM92[4]	Pivoluska等[16]的协议	Xia等[20]的协议	本文的协议
量子源	贝尔态	贝尔态和GHZ态	N光子的GHZ态	任何压缩纠缠态
压缩	否	否	否	是
抵抗测量攻击	是	是	是	是
抵抗拦截和重放攻击	是	是	是	是
抵抗纠缠测量的攻击	是	是	是	是
抗退相干	否	否	否	是

4.3　低量子传输和量子存储开销

对于 Ekert91[3] 和 BBM92[4] 协议和基于 GHZ 态的 QKD 协议 [7−23], 每个光子最多只能生成两个密钥, 故需要传输和存储大量的光子. 而在 QKD 中, 量子比特比经典比特更昂贵, 主要是因为其技术成本高、安全性要求高和易失性高等原因. 本文的协议是先将任何纠缠态压缩为单光子态或 Bell 态, 再发送给接收方. 即本文使用相应的等距张量来实现了大大减少需要传输和存储的量子光子数. 尽管等距张量构造和存储本身应该也有开销, 但是, 众所周知, 经典的传输和存储开销比量子的开销要低很多. 更重要的是由于等距张量在本文的构造很有规律性 (见等式 (2), (3), (6), (7)), 因此, 可以通过优化算法来构造和存储协议中使用的等距张量进一步减少相应的开销. 综上所述, 本文的 QKD 协议具有较低的量子传输和量子存储开销.

4.4 高编码容量

对于 BB84[1], Ekert91[3] 和 BBM92[4] 协议, 以及基于 GHZ 态的 QKD 协议[7–23], 每个成功传送并被正确测量光子只能编码 1 比特经典信息. 这极大地限制了 QKD 协议的实际使用效率. 相比之下, 在本文的协议中, 一个压缩数态 $|0\rangle$或 $|1\rangle$或 $(\sqrt{2}/2)(|00\rangle+|11\rangle)$, $(\sqrt{2}/2)(|01\rangle+|10\rangle)$以同样的方式成功传送并被正确测量, 却可以被编码成多位经典信息. 因为我们可以通过等距张量方法将一个 n 比特的纠缠态压缩为一个 2 量子比特的纠缠态或者 1 量子比特的单光子, 其中 $2<n$. 然后可以使用这个 2 量子比特纠缠态或者 1 量子比特单光子来传输和存储信息. 在接收端, 可以使用等距张量转置方法将这个 2 量子比特纠缠态或者 1 量子比特单光子解压缩为一个 n 量子比特的纠缠态, 从而恢复出原始的信息. 也就是说, Alice 只需要传输和存储 1 量子比特的光子, 就可以结合相应的等距张量来生成 n 比特的生密钥. 从而实现高效量子比特的利用率和高编码能力. 因此, 我们的协议实现了高容量编码. 故压缩的态不仅减少了需要传输和存储的量子位元的数量, 而且还增加了一个额外的定性特性, 即增加了 QKD 协议的编码能力. 这就同时实现了多模式存储和确定性传输的要求.

5 结 论

本文研究了在 QKD 协议中对纠缠态源执行压缩的问题. 研究发现可以利用 QKD 协议中的压缩的相关性来提高众所周知的 BB84 和 BBM92 的编码能力. 该协议的优点是普遍使用的纠缠态包括 Bell 态和 N 光子 GHZ 态都可以通过使用特定的等距张量压缩成 $(\sqrt{2}/2)(|00\rangle+|11\rangle)$, $(\sqrt{2}/2)(|01\rangle+|10\rangle)$和单光子态$|0\rangle,|1\rangle$. 这种方法在使用量子态的数量上比传统使用纠缠态的 QKD 更有效. 同时, 展示了如何获得一个类似的等距张量来获得解压缩的压缩纠缠态. 此外, 结合等距张量, 本文还可以获得纠缠态的系数, 克服其他纠缠压缩的主要限制. 最重要的是, 由等距张量构造的张量网络等价于量子电路, 使本文的提出的协议在当前技术下具有可实施性, 也同时实现了多模式存储和确定性传输的要求.

参考文献

[1] Bennett C H, Brassard G 1984 *Proceedings of the IEEE International Conference on Computers, Systems, and Signal Processing* Bangalore, India, December 10–12, 1984 pp175–179

[2] Wang B, Zhang B F, Zou F C, et al. 2021 *Optik* **235** 166628

[3] Ekert A K 1991 *Phys. Rev. Lett.* **67** 661

[4] Bennett C H, Brassard G, Mermin N D 1992 *Phys. Rev. Lett.* **68** 557

[5] Greenberger D M, Horne M A, Zeilinger A 1989 *Bell' s Theorem, Quantum Theory and Conceptions of the Universe* (Dordrecht: Springer) pp69–72

[6] Bouwmeester D, Pan J W, Daniell M, Weinfurter H, Zeilinger A 1999 *Phys. Rev. Lett.* **82** 1345

[7] Guo Y, Shi R, Zeng G 2010 *Phys. Scr.* **81** 045006

[8] Xu G B, Wen Q Y, Gao F, Qin S J 2014 *Quantum Inf. Process.* **13** 2587

[9] Castañeda Valle D, Quezada L F, Dong S H 2021 *Ann. Phys. Berlin* **533** 2100116

[10] Zhao N, Guo X, Wu T 2021 *Phys. Rev. A* **104** 062616

[11] Upadhyaya T, van Himbeeck T, Lin J, et al. 2021 *PRX Quantum.* **2** 020325

[12] Jiang C, Yu Z W, Hu X L, Wang X B 2021 *Phys. Rev. A* **103** 012402

[13] Lim C C W, Xu F, Pan J W, Ekert A 2021 *Phys. Rev. Lett.* **126** 100501

[14] Long G L and Liu X S 2002 *Phys. Rev. A* **65** 032302

[15] Chang C H, Yang C W, Hwang T 2016 *Int. J. Theor. Phys.* **55** 3993

[16] Pivoluska M, Huber M, Malik M 2018 *Phys. Rev. A* **97** 032312

[17] Zhu K N, Zhou N R, Wang Y Q, et al. 2018 *Int. J. Theor. Phys.* **57** 3621

[18] Zhou H, Lv K, Huang L, et al. 2022 *IEEE/ACM T. Network.* **30** 1328

[19] Wang X L, Chen L K, Li W, Huang H L, Liu C, Chen C, Luo Y H, Su Z E, Wu D, Li Z D, Lu H, Hu Y, Jiang X, Peng C Z, Li L, Liu N L, Chen Y A, Lu C Y, Pan J W 2016 *Phys. Rev. Lett.* **117** 210502

[20] Xia Y, Lu P M, Zeng Y Z 2012 *Quantum Inf. Process.* **11** 605

[21] Huang Y F, Liu B H, Peng L, et al. 2011 *Nat. Commun.* **2** 1

[22] Xia Y, Song J, Ning Y, et al. 2010 *JETP Lett.* **90** 735

[23] Svozil K 2022 *Found. Phys.* **52** 4

[24] Yin H L, Fu Y, Li C L, et al. 2023 *Nati. Sci. Rev.* **10** 228

[25] Xie Y M, Lu Y S, Weng C X, et al. 2022 *PRX Quantum.* **3** 020315

[26] Gu J, Cao X Y, Fu Y, et al. 2022 *Sci. Bull.* **67** 2167

[27] Fan C R, Lu B, Feng X T, et al. 2021 *Quant. Engineer.* **3** e67

[28] Bostroem K, Felbinger T 2002 *Phys. Rev. A* **65** 032313

[29] Datta N, Renes J M, Renner R, et al. 2013 *IEEE Inform. Theory* **59** 8057

[30] Plesch M, Bužek V 2010 *Phys. Rev. A* **81** 032317

[31] Rozema L A, Mahler D H, Hayat A, Turner P S, Steinberg A M 2014 *Phys. Rev. Lett.* **113** 160504

[32] Yang Y, Chiribella G, Ebler D 2016 *Phys. Rev. Lett.* **116** 080501

[33] Yang Y, Chiribella G, Hayashi M 2016 *Phys. Rev. Lett.* **117** 090502

[34] Romero J, Olson J P, Aspuru-Guzik A 2017 *Quantum Sci. Technol.* **2** 045001

[35] Pepper A, Tischler N, Pryde G J 2019 *Phys. Rev. Lett.* **122** 060501

[36] Van Acoleyen K, Hallam A, Bal M, Hauru M, Haegeman J, Verstraete F 2020 *Phys. Rev. B* **102** 165131

[37] Lai H, Pieprzyk J, Pan L 2023 *Sci. China Inf. Sc.* **66** 180510

[38] Evenbly G 2022 *Front. Phys.* **10** 1146

[39] Bennett C H, DiVincenzo D P, Smolin J A, Wootters W K 1996 *Phys. Rev. A* **54** 3824

Generalized isometric tensor based quantum key distribution protocols of squeezed multiphoton entangled states*

Lai Hong †

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

(Received 13 April 2023; revised manuscript received 2 June 2023)

Abstract

Isometric tensor offers a novel and powerful tool that can compress an entangled state into its tensor network state (TNS). The resulting quantum compression provides a new opportunity for enhancing quantum key distribution (QKD) protocols. The main idea explored in this work is to use the quantum compression to improve the efficiency of QKD. In a nut-shell, a collection of any multi-photon entangled states that carry encoded classical bits is compressed into a single-photon state before the corresponding photon is sent to the receiver that measures the qubit and decompresses it. In this paper, we first show how to obtain the generalized isometric tensors for compressing any entangled states and their inverse isometric tensors for decompression. In our proposed QKD protocol, the input state consists of any multi-photon entangled states, which are first compressed into a single-photon state $|0\rangle$ or $|1\rangle$ or Bell states by the sender Alice. A sequence of single-photon states $|0\rangle$ and $|1\rangle$ and one photon from the Bell state mixed with decoy qubits is sent to the receiver Bob via a quantum channel. Bob obtains the final sifted compressed states $|0\rangle$ and $|1\rangle$ and conjugate transpose of the isometric tensors. Using our protocols, Bob can decompress the received states $|0\rangle$ and $|1\rangle$ into original entangled states. Since quantum processors that are used to send quantum information between nodes are relatively primitive and low in power and the preparation of many-photon entanglement is relatively difficult at present, finding suitable protocols for the compression of transmitted quantum data brings important practical benefits. More generally, the quantum information theory primarily investigates quantum data manipulation under locality constraints, so our protocols connect naturally to these investigations. Our protocols increase the encoding capacity of QKD protocols. Not only our proposed processes of compression and decompression are very simple, but also entanglement compression using isometric tensors can be implemented by using quantum circuits and current technology. Because many ideas for designing of quantum information processing equipment envision that a network composed of relatively small quantum processors sending quantum information between nodes, it is greatly significant to find appropriate protocols for compressing the transmitted quantum data .

Keywords: entanglement compression, generalized isometric tensors, tensor network states, decompression

PACS: 03.67.Ac, 03.67.Bg, 03.67.Dd, 03.67.Hk **DOI:** 10.7498/aps.72.20230589

* Project supported by the National Natural Science Foundation of China (Grant No. 61702427), the Natural Science Foundation of Chongqing, China (Grant No. CSTB2022NSCQ-MSX0749), and the Southwest University's 2022School-level Teaching Reform Project, China (Grant No. 2022JY086).

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

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

基于广义等距张量的压缩多光子纠缠态量子密钥分发

赖红

Generalized isometric tensor based quantum key distribution protocols of squeezed multiphoton entangled states

Lai Hong

引用信息 Citation: Acta Physica Sinica, 72, 170301 (2023) DOI: 10.7498/aps.72.20230589
在线阅读 View online: https://doi.org/10.7498/aps.72.20230589
当期内容 View table of contents: http://wulixb.iphy.ac.cn