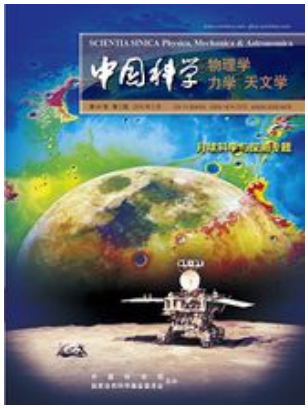


# 基于八量子比特图态的六方(3,5)阈量子操作共享

# Six-party (3,5)-threshold quantum operation sharing with 8-qubit graph state

| | |
|---|---|
| 期刊： | 中国科学: 物理学 力学 天文学 |
| 稿件ID： | SSPMA-2025-0299.R3 |
| 稿件栏目： | 论文 |
| 作者提交日期： | 2025-07-31 |
| 参与作者列表： | 吉施羽, 袁好, 余金华, Li Bo, 张战军 |
| 关键词： | (3/5)阈, 量子操作共享, 六方, 八量子比特图态 |
| 英文关键词： | (3/5)-threshold, quantum operation sharing, six-party, 8-qubit graph state |
| 学科领域： | 物理(II) |
| 专题： | |

中国科学: 物理学 力学 天文学 2025 年 第 50 卷 第 1 期: 123456
SCIENTIA SINICA Physica, Mechanica & Astronomica phys.scichina.com

论 文

# 基于八量子比特图态的六方(3,5)阈量子操作共享

吉施羽[1], 袁好[2], 余金华[1], 李波[3], 张战军[1*]

1. 浙江工商大学信息与电子工程学院(萨塞克斯人工智能学院), 杭州 310018;
2. 皖西学院电气与光电工程学院, 六安 237012;
3. 浙大城市学院计算机与计算科学学院, 杭州 310015
*联系人, E-mail: zhangzhanjun@zjgsu.edu.cn

收稿日期: 2025-05-?; 接受日期: 2025-?-?; 网络出版日期: 2025-?-?
国家自然科学基金(编号: 12075205, 12175147)和浙江省自然科学基金(编号: LZ24A050005)资助项目

**摘要** 量子操作共享是重要的量子远程控制技术，可用于量子信息的远程加密或解密. 目前已有的量子操作共享方案中，共享者必须都合作才可以最终共享量子操作，即所谓的(n,n)阈方案. 本文基于八量子比特图态，提出了一种六方(3,5)阈量子操作共享协议，即 5 位共享者中有 3 位合作就可以共享操作初有者的任意量子操作. 文中分析讨论了协议的安全性，实现量子操作共享的共享者对称性、协议的局限性、操作共享成功概率、及当前实验技术可行性，揭示了对称性与局限性的物理本质与原因. 研究发现：该协议是安全的; 每个共享者与其两个相邻伙伴或两个非相邻伙伴都可以成功共享量子操作; 根据当今实验技术，未来本协议的实验实现应已可期。

**关键词** (3,5)阈, 量子操作共享，六方，八量子比特图态

**PACS:** 03.67.Hk, 03.67.Dd, 03.65.Ud

## 1 引言

量子信息与量子计算是经典信息理论、经典计算理论与量子力学结合的产物. 自上世纪它们被提出以来，其发展非常迅猛，目前已成当今世界科技热门领域并发展出许多分支，如量子密钥分发[1-6]、量子离物传态[7-12]、量子秘密分享[13-25]、量子态远程制备[26-27]、量子安全直接通信[28-44]、量子操作远程实现[45-46]及其它一些分支等. 它们超越经典方式处理相应任务的强大功能吸引了许多研究者的注意.

2011 年 Zhang 和 Cheung 首次明确提出了量子操作共享[47]. 作为一种量子任务，其在最简单的情形下，基本思想是, 利用远程分享的量子纠缠、局域量子操作和经典通信, 当且仅当两个共享者合作, 一个量子操作的实施者才能够确保这个操作可以安全正确地作用到两个共享者共同拥有的一个目标量子比特上. 由于实施者仅信任共享者整体而非其中任意一位, 因此实施者必须确保任一共享者不可以单独获得该操作作用在目标量子比特上. 量子操作分享作为一种量子信息处理技术, 在未来的量子网络上可以用于量子态(量子信息)加密、解密和破坏. 由于共享者

引用格式: 吉施羽, 袁好，余金华，等。基于八量子比特图态的(3,5)阈量子操作共享. 中国科学: 物理学 力学 天文学, 2025, ?: ??
Ji S Y, Yuan H, Yu J H, et al. (3,5)-threshold quantum operation sharing with 8-qubit Graph state (in Chinese). . Sci Sin-Phys Mech Astron, 2025, ?: ??, doi: 10.1360/SSPMA2016-00000

们可以通过合作来共享加密或解密的量子信息，从而可以用来激活一些重要过程, 如分布式量子计算机的安全操作、共享一些难以构建的辅助态、量子集体封缄和拆封、量子货币的联合发布与认证以及远程联合销毁、多方共同管控的核导弹发射等等, 近年来量子操作共享研究发展得很快且受到很多关注[48-76].

在量子操作共享中, 量子通道里的量子纠缠是必不可少的量子资源. 目前已经有许多量子纠缠态被应用在一些量子操作分享协议中, 如 Bell 态[47]、W 态[52,54]、GHZ 态[55]、Brown 态[63,68]、Genuine 态[49,65]、Cluster 态[48,56]等量子纠缠纯态以及部分源于纯态的量子纠缠混态.图态作为一种重要的量子纠缠资源，其一经提出就受到了很多关注，并被用于量子秘密分享等[77-79]. 然而，我们发现迄今其尚未被用于量子操作共享. 另外我们还发现，目前已有的量子操作共享协议中，所有共享者（n 个）必须全部合作才能最终成功共享操作初有者的量子操作，即通常所谓的（n,n）阈协议. 这对于量子操作共享应用是一种限制. 因此，突破这种限制，提出一种部分共享者（m≤n）合作即可最终成功共享操作初有者的任意量子操作的协议[即（m,n）阈协议]，则显得尤为必要. 出于上述两方面考虑，本文基于八量子比特图态，首次提出了一种六方(3,5)阈量子操作共享协议，即 5 位共享者中有 3 位合作就可以共享操作初有者的任意量子操作.

本文其它部分的结构安排如下: 第 2 节将简略介绍下图态并给出其定义中算子的两条性质. 第 3 节将首先给出本文使用的一种八量子比特图态, 其次将利用其作为量子通道提出一种六方(3,5)阈量子操作分享协议. 第 4 节将从协议实施的安全性、共享者对称性、协议局限性、成功概率以及目前实验技术下协议可行性等几个方面做一些分析讨论, 并揭示其中的深层物理. 最后一节对本文做个小结.

## 2 图态简介

k 个量子比特的图态是希尔伯特空间$\mathcal{H}_2^{\otimes k}$中的量子态，其对应的图是一个由 $k$ 个顶点和若干条边构成的无向图 $\mathrm{T}=(D,B)$，其中 $D=\{d_k\}$表示此图中所有顶点的集合，$B=\{b_{\mathrm{mn}}|1\le \mathrm{m}<n\le k\}$则为此图中全部边的集合，$b_{\mathrm{mn}}=(d_{\mathrm{m}},d_{\mathrm{n}})$表示连接顶点$d_{\mathrm{m}}$与$d_{\mathrm{n}}$的边. 顺便说一下，并非任意两个顶点之间都有边相连接. 顶点 $d_1,d_2,\cdots,d_{\mathrm{k}}$ 依次分别对应量子比特 1,2,⋯,k. 图所对应的量子态可通过对所有由边相连的均处在$|+\rangle$的二量子比特施加受控相位门 $\mathcal{P}$ 来构造. 有 k 个顶点和若干条边的图，它所对应的图态$|\mathrm{T}\rangle$为

$$|\mathrm{T}\rangle_{12\ldots\mathrm{k}}=\prod_{b_{\mathrm{mn}}\epsilon B}\mathcal{P}_{\mathrm{mn}}\left(|+\rangle_1|+\rangle_2\ldots|+\rangle_{\mathrm{k}}\right)$$
$$=\prod_{b_{\mathrm{mn}}\epsilon B}\mathcal{P}_{\mathrm{mn}}|+\rangle^{\otimes k},\#(1)$$

其中受控相位门 $\mathcal{P}$ 的算子形式为

$$\mathcal{P}_{\mathrm{xy}}=|0\rangle_{\mathrm{x}}\langle 0|\otimes\sigma_{\mathrm{y}}^{(0,0)}+|1\rangle_{\mathrm{x}}\langle 1|\otimes\sigma_{\mathrm{y}}^{(1,1)},\#(2)$$

$|+\rangle=(|0\rangle+|1\rangle)/\sqrt{2}$. $\mathcal{P}$ 算子中的$\sigma^{(0,0)}=|0\rangle\langle 0|+|1\rangle\langle 1|$是单位算子，$\sigma^{(0,1)}=|1\rangle\langle 0|+|0\rangle\langle 1|$是一个 Pauli 算子. 后文中$\sigma^{(1,0)}=|1\rangle\langle 0|-|0\rangle\langle 1|$和$\sigma^{(1,1)}=|0\rangle\langle 0|-|1\rangle\langle 1|$是另外两个 Pauli 算子. 注意，单个受控相位门 $\mathcal{P}$ 具有性质$\mathcal{P}_{\mathrm{xy}}=\mathcal{P}_{\mathrm{yx}}$. 对于多个受控相门，它们具有彼此对易的性质. 即在构造图态时，它们的实施顺序不影响最终的图态.

## 3 基于八量子比特图态的六方(3,5)阈量子操作共享方案

### 3.1 八量子比特图态

本文使用一种八量子比特图态，其所对应的图见图 1(a). 八量子比特分别用数字 1 至 8 标记，它们分别位于图中的八个顶点(亦分别标记为数字 1 至 8). 图中，顶点 1, 2, 3, 4, 5 通过首尾相连构成一个五边形. 这五个顶点分别与顶点 6、顶点 6 与顶点 7、顶点 7 与顶点 8 也通过边相连. 根据式(1)，这个图所对应的量子态可写为

$$|\mathrm{T}_{\mathrm{viii}}\rangle_{12345678}=(\mathcal{P}_{67}\mathcal{P}_{78})\left(\prod_{i=1}^{5}\mathcal{P}_{6i}\right)$$
$$(\mathcal{P}_{12}\mathcal{P}_{23}\mathcal{P}_{34}\mathcal{P}_{45}\mathcal{P}_{51})|+\rangle_{12345678}^{\otimes 8}.\#(3)$$

同样根据式(1)，原图中由顶点 1, 2, 3, 4, 5, 6 及它们的边构成的子图所对应的量子态可写为

$$|\mathrm{T_{vi}}\rangle_{123456}=\left(\prod_{i=1}^{5}\mathcal{P}_{6i}\right)(\mathcal{P}_{12}\mathcal{P}_{23}\mathcal{P}_{34}\mathcal{P}_{45}\mathcal{P}_{51})|+\rangle_{123456}^{\otimes 6}.\#(4)$$

## 3.2 六方(3,5)阈量子操作共享方案

假定未来的量子网络中存在两个区域：Dealer 区域和 Players 区域[见图 1(a)]. 在 Dealer 区域有一位量子操作初有者(本文中称之为$O_6$)，她拥有八量子比特 1,2,3,4,5,6,7,8，它们处于图态$|\mathrm{T_{viii}}\rangle_{12345678}$. 该图态将作为本文提出的六方(3,5)阈量子操作共享协议中使用的量子纠缠资源. 在 Players 区域有五位量子操作共享者，他们分别被称作为$S_1$、$S_2$、$S_3$、$S_4$和$S_5$. 五位共享者共同拥有一个目标量子比特 t. 它处在某个量子态，不失一般性，该态可写为

$$|\mu\rangle_{\mathrm{t}}=\alpha|0\rangle_{\mathrm{t}}+\beta|1\rangle_{\mathrm{t}},\#(5)$$

其中的系数$\alpha$和$\beta$满足归一化条件$|\alpha|^2+|\beta|^2=1$. 注意，量子比特 t 可以储存在任一共享者的量子网络节点上. 不失一般性，本文假设它在共享者$S_3$处.

$O_6$想将她掌握的某一量子操作 $U$ 让$S_1$、$S_2$、$S_3$、$S_4$与$S_5$共享. 具体来说，就是她想让这个 $U$ 作用到远处共享者们的目标量子比特 t 的量子态上，即 $U|\mu\rangle=|\varphi\rangle$ (该量子态在后文称之为目标态). 为实现此量子操作共享，本文提出了一种六方(3,5)阈量子操作共享协议，具体如下:

(一) $O_6$首先引入一个辅助量子比特 a，其处在量子态$|0\rangle$. 其次$O_6$实施一个量子受控非门操作，其中 a 是作为靶量子比特，量子比特 8 是作为控制量子比特[见图 1(b)]. 这里的量子受控非门算子形式为

$$\mathcal{F}_{\mathrm{xy}}=|0\rangle_{\mathrm{x}}\langle 0|\otimes\sigma_{\mathrm{y}}^{(0,0)}+|1\rangle_{\mathrm{x}}\langle 1|\otimes\sigma_{\mathrm{y}}^{(0,1)}.\#(6)$$

在该操作下，八量子比特系统与辅助比特 a 的量子态变为

$$|\mathrm{L_{ix}}\rangle_{12345678\mathrm{a}}=\mathcal{F}_{8\mathrm{a}}|\mathrm{T_{viii}}\rangle_{12345678}|0\rangle_{\mathrm{a}}.\#(7)$$

经过略微繁琐的推导，以及利用公式(6)给出的定义，公式(7)可改写为

$$|\mathrm{L_{ix}}\rangle_{12345678\mathrm{a}}=\frac{1}{\sqrt{2}}\left(|0\rangle_7+|1\rangle_7\sigma_6^{(1,1)}\sigma_8^{(1,1)}\right)\times|\mathrm{T_{vi}}\rangle_{123456}|\mathcal{B}_{00}\rangle_{8\mathrm{a}},\quad(8)$$

其中

$$|\mathcal{B}_{ij}\rangle_{\mathrm{xy}}=\sigma_{\mathrm{x}}^{(i,j)}\frac{1}{\sqrt{2}}(|00\rangle+|11\rangle)_{\mathrm{xy}}=\sigma_{\mathrm{y}}^{(i,j)\dagger}\frac{1}{\sqrt{2}}(|00\rangle+|11\rangle)_{\mathrm{xy}},\quad i,j\in\{0,1\}\#(9)$$

是本文中所使用的 Bell 态的定义.

(二) $O_6$将量子比特 1, 2, 3, 4, 5 依次分发给五位共享者$S_1$至$S_5$. 分发后，目标量子比特 t 与量子态$|\mathrm{L_{ix}}\rangle_{12345678\mathrm{a}}$的量子态可表示为$|\mathrm{L_{ix}}\rangle_{12345678\mathrm{a}}\otimes|\mu\rangle_{\mathrm{t}}$，如图 1(c)所示.

(三) $S_3$对他的量子比特对(t, a)实施 Bell 态测量，然后将测量结果对应的两比特经典信息通过经典信道发送给$O_6$，示意见图 1(d). 本文中约定两量子比特的四个 Bell 态$|\mathcal{B}_{ij}\rangle$对应的两比特经典信息为"$ij$". Bell 态测量的算符形式为

$$|\mathcal{B}_{ij}\rangle\langle\mathcal{B}_{ij}|,\ i,j\epsilon\{0,1\}.\#(10)$$

在此测量下，整个系统的量子态变为

$$|\mathcal{B}_{ij}\rangle_{\mathrm{at}}\langle\mathcal{B}_{ij}||\mathrm{L_{ix}}\rangle_{12345678a}|\mu\rangle_{\mathrm{t}}=\frac{1}{\sqrt{2}}|\mathcal{B}_{ij}\rangle_{\mathrm{at}}\langle\mathcal{B}_{ij}|\left(|0\rangle_7+|1\rangle_7\sigma_6^{(1,1)}\sigma_8^{(1,1)}\right)\times|\mathrm{T_{vi}}\rangle_{123456}|\mathcal{B}_{00}\rangle_{8\mathrm{a}}|\mu\rangle_{\mathrm{t}}.\#(11)$$

令

$$\mathrm{R_{678}}={}_{\mathrm{at}}\langle\mathcal{B}_{ij}|\left(|0\rangle_7+|1\rangle_7\sigma_6^{(1,1)}\sigma_8^{(1,1)}\right)|\mathcal{B}_{00}\rangle_{8\mathrm{a}}|\mu\rangle_{\mathrm{t}}.\#(12)$$

通过简单的推导可得

$$\begin{aligned}\mathrm{R_{678}}&=\left(|0\rangle_7+|1\rangle_7\sigma_6^{(1,1)}\sigma_8^{(1,1)}\right)_{\mathrm{at}}\langle\mathcal{B}_{00}|\sigma_{\mathrm{a}}^{(i,j)\dagger}|\mathcal{B}_{00}\rangle_{8\mathrm{a}}|\mu\rangle_{\mathrm{t}}\\&=\left(|0\rangle_7+|1\rangle_7\sigma_6^{(1,1)}\sigma_8^{(1,1)}\right)_{\mathrm{at}}\langle\mathcal{B}_{00}|\sigma_8^{(i,j)}|\mathcal{B}_{00}\rangle_{8\mathrm{a}}|\mu\rangle_{\mathrm{t}}\\&=\left(|0\rangle_7+|1\rangle_7\sigma_6^{(1,1)}\sigma_8^{(1,1)}\right)\sigma_8^{(i,j)}{}_{\mathrm{at}}\langle\mathcal{B}_{00}||\mathcal{B}_{00}\rangle_{8\mathrm{a}}|\mu\rangle_{\mathrm{t}}\\&=\frac{1}{2}\left[|0\rangle_7\sigma_8^{(i,j)}+(-1)^{i\oplus j}|1\rangle_7\sigma_6^{(1,1)}\sigma_8^{(i\oplus 1,j\oplus 1)}\right]|\mu\rangle_8.(13)\end{aligned}$$

因此，公式(11)可以改写为

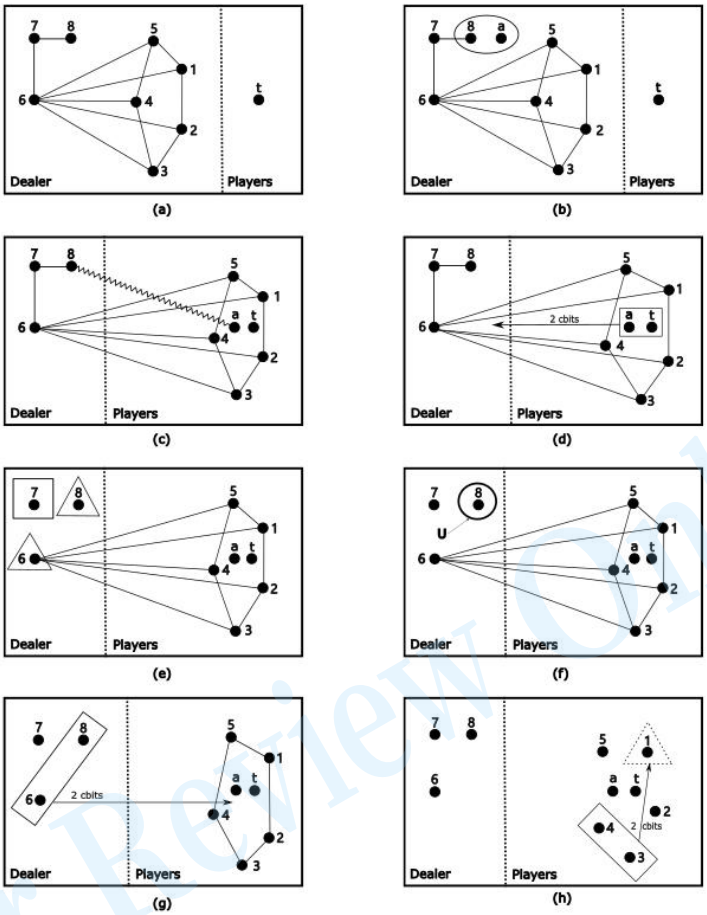



**图 1** 基于八量子比特图态的(3,5)阈量子操作共享示意图. 实线椭圆、弹簧线、实线矩形、实线正方形、实线三角形、实线圆、虚线三角形、箭头依次分别表示量子非门操作、量子比特 8 与 a 的纠缠、Bell 态测量、单粒子测量、单粒子 Pauli 操作、拟共享的量子操作 $U$、Hadmard 门操作加 Pauli 操作、经典信息流向. cbit 是经典比特. (a)八量子比特图态的制备；(b)$O_6$引入辅助粒子 a 并实施量子受控非门；(c) $O_6$将量子比特从 Dealer 区域分发给 Players 区域的五位共享者；(d) $S_3$ 对量子比特 a 与 t 实施 Bell 态测量，并将结果告诉$O_6$；(e) $O_6$ 对量子比特 6 与 8 做 Pauli 操作、量子比特 7 做单粒子测量；(f)$O_6$将拟分享的量子操作作用于量子比特 8；(g)$O_6$ 对量子比特 6 与 8 做 Bell 态测量，并将测量告诉共享者们；(h)确定最终持有目标态量子比特的共享者($S_1$)，之后对其合作伙伴($S_3$ 与 $S_4$)的量子比特对(3 和 4)实施 Bell 态测量. 具体说明见行文.

**Figure 1** Illustration of (3,5)-threshold quantum operation sharing with 8-qubit graph state (EQGS). The solid ellipse, the spring line, solid rectangles, the solid square, solid triangles, the solid circle, the dashed triangle, and arrows represent in turn the operation of 2-qubit controlled-NOT gate, the entanglement between qubits 8 and **a**, the Bell-state measurements, the single-qubit (SQ) measurement, SQ Pauli operations, the quantum operation $U$ to be shared, the joint Hadmard and Pauli operation, and the classical message transfer. Cbits mean classical bits. (a) the EQGS preparation. (b) $O_6$ introduces an auxiliary qubit **a** and implements a quantum controlled-NOT gate. (c) $O_6$ distributes the qubits from the Dealer region to five sharers in the Players region. (d) $S_3$ measures qubits **a** and t with Bell-state bases, and tells $O_6$ the result. (e) $O_6$ carries out Pauli operations on her qubits 6, 8, and measures qubit 7 with computational bases. (f) $U$ is applied to qubit 8. (g) $O_6$ measures qubits 6 and 8 with Bell-state bases and

broadcasts the result. (h) After determining the sharer whose qubit ultimately inhabits the target state, a Bell-state measurement is performed on the qubit pair held by his cooperation partners ($S_3$ and $S_4$). See text for more details.

$$\begin{aligned}&\left|\mathcal{B}_{ij}\right\rangle_{\mathrm{at}}\left\langle\mathcal{B}_{ij}\right|\left|\mathrm{L_{ix}}\right\rangle_{12345678a}|\mu\rangle_{\mathrm{t}}\\&=\frac{1}{2\sqrt{2}}\left|\mathcal{B}_{ij}\right\rangle_{\mathrm{at}}\left[|0\rangle_7|\mathrm{T_{vi}}\rangle_{123456}\sigma_8^{(i,j)}|\mu\rangle_8\right.\\&\left.+\sigma_6^{(1,1)}|\mathrm{T_{vi}}\rangle_{123456}(-1)^{i\oplus j}|1\rangle_7\sigma_8^{(i\oplus 1,j\oplus 1)}|\mu\rangle_8\right].\end{aligned}\quad(14)$$

(四) $O_6$使用计算基$\{|0\rangle, |1\rangle\}$对她的量子比特 7 进行单粒子测量[见图 1(e)]. 之后根据她的测量结果以及收到的$S_3$发来的两比特经典信息"$ij$"，对量子比特 8 实施相应的 Pauli 操作. 具体如下：从公式(14)可见，如果她测得$|0\rangle_7$，则量子比特 1,2,3,4,5 和 6 的量子态坍缩到图态$|\mathrm{T_{vi}}\rangle_{123456}$，量子比特 8 的量子态为$\sigma_8^{(i,j)}|\mu\rangle_8$. 在此种情形下，她对量子比特 8 实施$\sigma^{(i,j)}$操作，即

$$\sigma_8^{(i,j)}\sigma_8^{(i,j)}|\mu\rangle_8=|\mu\rangle_8.\#(15)$$

可见原先在量子比特 t 上的态$|\mu\rangle$已转到量子比特 8 上. 同理，若她测得$|1\rangle_7$，则量子比特 1,2,3,4,5,6 与量子比特 8 的量子态分别坍缩到量子态$\sigma_6^{(1,1)}|\mathrm{T_{vi}}\rangle_{123456}$和$\sigma_8^{(i\oplus 1,j\oplus 1)}|\mu\rangle_8$. 在这种情况下，她对量子比特 6 和量子比特 8 分别实施量子操作$\sigma^{(1,1)}$和$\sigma^{(i\oplus 1,j\oplus 1)}$，即

$$\sigma_6^{(1,1)}\sigma_6^{(1,1)}|\mathrm{T_{vi}}\rangle_{123456}=|\mathrm{T_{vi}}\rangle_{123456},\#(16)$$

$$\sigma_8^{(i\oplus 1,j\oplus 1)}\sigma_8^{(i\oplus 1,j\oplus 1)}|\mu\rangle_8=|\mu\rangle_8.\#(17)$$

可见，量子比特 1,2,3,4,5,6 的量子态也已转化到图态$|\mathrm{T_{vi}}\rangle_{123456}$，量子态$|\mu\rangle$也已转到量子比特 8 上.

(五) $O_6$将拟分享的量子操作 $U$ 作用于量子比特 8 上[示意见图 1(f)]，即

$$U_8|\mu\rangle_8=|\varphi\rangle_8.\#(18)$$

至此，目标态$|\varphi\rangle$已经在量子比特 8 上实现. 由量子比特 1,2,3,4,5,6 和 8 构成的系统(后面称之为系统 $\mathcal{S}$)的量子态为

$$|\mathrm{L_{vii}}\rangle_{1234568}=|\mathrm{T_{vi}}\rangle_{123456}|\varphi\rangle_8.\#(19)$$

(六) $O_6$对她的量子比特对$(6,8)$实施Bell态测量，然后根据约定，将测量结果对应的两比特经典信息通过经典信道发给共享者们[见图 1(g)]. 测量后，系统 $\mathcal{S}$ 的量子态为

**表 1** 步骤(八)中的合作伙伴的操作与 S1 所做的相应 Pauli 操作. 最后一列中的"$ij$"是$O_6$公布的经典信息.

**Table 1** Partners' performance and $S_1$'s corresponding Pauli operations in step 8. "$ij$" are classical bit message published by $O_6$ in the last column.

| 合作伙伴 | 合作伙伴的 Bell 态测量结果 | 合作伙伴给 $S_1$ 的两比特经典信息 | $S_1$ 的 Pauli 操作 |
|---|---|---|---|
| $S_3$、$S_4$ ($S_2$、$S_5$) | $\|\mathcal{B}_{11}\rangle_{34}$ ($\|\mathcal{B}_{00}\rangle_{25}$) | 11 (00) | $\sigma^{(i,j)}$ |
| | $\|\mathcal{B}_{01}\rangle_{34}$ ($\|\mathcal{B}_{11}\rangle_{25}$) | 01 (11) | $\sigma^{(i,j\oplus 1)}$ |
| | $\|\mathcal{B}_{00}\rangle_{34}$ ($\|\mathcal{B}_{01}\rangle_{25}$) | 00 (01) | $\sigma^{(i\oplus 1,j)}$ |
| | $\|\mathcal{B}_{10}\rangle_{34}$ ($\|\mathcal{B}_{10}\rangle_{25}$) | 10 (10) | $\sigma^{(i\oplus 1,j\oplus 1)}$ |

的量子态为

$$\left|\mathcal{B}_{ij}\right\rangle_{86}\left\langle\mathcal{B}_{ij}\right|\mathrm{L_{vii}}\rangle_{1234568}=\left|\mathcal{B}_{ij}\right\rangle_{86}\left|S_{ij}\right\rangle_{12345},\#(20)$$

其中

$$\left|S_{ij}\right\rangle_{12345}={}_{86}\langle\mathcal{B}_{ij}|\mathrm{T_{vi}}\rangle_{123456}|\varphi\rangle_8.\#(21)$$

(七) 共享者们商量确定哪三位共享者通过合作最终获取目标态：首先决定最终在哪位共享者的量子比特上获取目标态；其次确定另外两位合作者，即他的两位邻居或者他的两位非邻居. 本文中邻居的定义为：如果图上两个顶点$d_{\mathrm{m}}$和$d_{\mathrm{n}}$之间若存在一条边$b_{\mathrm{mn}}$连接，则此两个顶点对应的共享者互为邻居.

(八) 两位邻居（或两位非邻居）对他们的量子比特对实施 Bell 态测量，然后将测量结果对应的两比特经典信息通过经典信道发送给那位最终在其量子比特上获取目标态的共享者.

(九) 最终在其量子比特上获取目标态的共享者，先对他的量子比特实施量子操作 $H$，之后结合$O_6$之前发送的两比特经典信息，他再对他的量子比特作出相应的 Pauli 操作.

步骤(七)至(九)示意见图 1(h).

不失一般性，假设(七)中商定最终在 $S_1$ 的量子比

特 1 上获取目标态，那么 $S_1$ 的两位非邻居(两位邻居)则为 $S_3$ 和 $S_4$ ($S_2$ 和 $S_5$). 进一步假设(八)中是 $S_1$ 的两个邻居 $S_3$ 、$S_4$ 与其合作，那么两位合作者对他们的量子比特 3 和 4 实施 Bell 态测量[见图 1(h)]. 他们测量前，也即$O_6$已对她的量子比特对$(6,8)$实施 Bell 态测量后，根据公式(9)、(4)和(18)以及它们的性质，量子比特 1，2，3，4 和 5 的量子态$\left|\mathrm{S_{ij}}\right\rangle_{12345}$可改写为

$$\begin{aligned}
\left|S_{ij}\right\rangle_{12345} &= {}_{86}\langle\mathcal{B}_{ij}|(\mathcal{P}_{12}\mathcal{P}_{23}\mathcal{P}_{34}\mathcal{P}_{45}\mathcal{P}_{51})\\
&\left(\prod_{k=1}^{5}\mathcal{P}_{6k}\right)|+\rangle_{123456}^{\otimes 6}|\varphi\rangle_8\\
&=(\mathcal{P}_{12}\mathcal{P}_{23}\mathcal{P}_{34}\mathcal{P}_{45}\mathcal{P}_{51})_{86}\langle\mathcal{B}_{00}|\sigma_6^{(i,j)\dagger}(\mathcal{P}_{26}\mathcal{P}_{56})(\mathcal{P}_{36}\mathcal{P}_{46})\\
&\left[|0\rangle_6\langle 0|\sigma_1^{(0,0)}+|1\rangle_6\langle 1|\sigma_1^{(1,1)}\right]|{+}{+}\rangle_{61}\,|+\rangle_{2345}^{\otimes 4}|\varphi\rangle_8\\
&=\frac{1}{2}(\mathcal{P}_{12}\mathcal{P}_{23})\mathcal{P}_{34}(\mathcal{P}_{45}\mathcal{P}_{51})H_1{}_{86}\langle\mathcal{B}_{00}|\sigma_6^{(i,j)\dagger}\\
&\left(|\mathcal{B}_{00}\rangle_{25}+|\mathcal{B}_{01}\rangle_{25}\sigma_6^{(1,1)}\right)\left(|\mathcal{B}_{00}\rangle_{34}+|\mathcal{B}_{01}\rangle_{34}\sigma_6^{(1,1)}\right)|\mathcal{B}_{00}\rangle_{61}|\varphi\rangle_8\\
&=\frac{1}{2}\mathcal{P}_{34}(\mathcal{P}_{21}\mathcal{P}_{23})(\mathcal{P}_{54}\mathcal{P}_{51})H_1\\
&[(|\mathcal{B}_{00}\rangle_{25}|\mathcal{B}_{00}\rangle_{34}+|\mathcal{B}_{01}\rangle_{25}|\mathcal{B}_{01}\rangle_{34})\sigma_1^{(i,j)}|\varphi\rangle_1\\
&+(|\mathcal{B}_{00}\rangle_{25}|\mathcal{B}_{01}\rangle_{34}+|\mathcal{B}_{01}\rangle_{25}|\mathcal{B}_{00}\rangle_{34})\sigma_1^{(1,1)}\sigma_1^{(i,j)}|\varphi\rangle_1]\\
&=\frac{1}{\sqrt{2}}[|\mathcal{B}_{00}\rangle_{25}|\mathcal{B}_{11}\rangle_{34}+|\mathcal{B}_{11}\rangle_{25}|\mathcal{B}_{01}\rangle_{34}\sigma_1^{(0,1)}\\
&+|\mathcal{B}_{01}\rangle_{25}|\mathcal{B}_{00}\rangle_{34}\sigma_1^{(1,0)}+|\mathcal{B}_{10}\rangle_{25}|\mathcal{B}_{10}\rangle_{34}\sigma_1^{(1,1)}]H_1\sigma_1^{(i,j)}|\varphi\rangle_1,
\end{aligned}\tag{22}$$

其中 $H=\frac{1}{\sqrt{2}}[\sigma^{(0,1)}+\sigma^{(1,1)}]$是 Hadmard 算子. $S_3$、$S_4$ 对他们的量子比特 3 和 4 实施 Bell 态测量后，将测量结果所对应的两比特经典信息发送给共享者 $S_1$. 接着，$S_1$ 对他的量子比特 1 实施量子操作 $H$，并结合 $O_6$发来的经典信息"$ij$"作出相应的 Pauli 操作(见表 1). 同理，根据公式(22)，若合作伙伴为 $S_1$ 的两个邻居 $S_2$、$S_5$，也可得到类似结果. 表 1 详细展示了合作伙伴(非邻居 $S_3$ 与 $S_4$ 或邻居 $S_2$ 与 $S_5$)在测得不同的 Bell 态时所对应发送的经典信息，以及最终在其量子比特上获取目标态的共享者 $S_1$ 在此种情况下所要实施的相应 Pauli 操作.

## 4 讨论与分析

上一小节我们详细描述了基于一种八量子比特图态的六方$(3,5)$阈量子操作共享方案. 下面我们从五个方面对它作一些简单的讨论与分析.

(I) 协议安全性. 量子操作共享实质是量子离物传态和量子态秘密共享的结合.作为一个秘密共享协议, 它的安全性是要予以保证的. 协议安全性需要考虑两部分：1、量子通道安全性. 量子比特在分发过程中, 可能会遭到内外部攻击, 如截留后发送替代量子比特或者测量后再发送等。关于这些攻击，已经有成熟的侦测策略与技术, 如量子比特批次传输加样本检测[3,28]. 因此，量子通道安全性可以得到保障. 2、某些 共享者单独获取目标态. 从公式(22)中可以看到目标态最后是包含在五个共享者的五个量子比特纠缠态之中. 由于量子比特彼此纠缠, 任何一位共享者在没有另两位共享者的协助下都不可能单独获取目标态的. 因此，操作共享的安全性也是可以保证的.

(II) 共享对称性及其物理本质. 从公式(3)和图(a)可以看出量子比特 1 到 5，任意两个量子比特之间交换，图和态都不变，即它们具有交换对称性。另外，由于交换对称性量子比特 1 到 5 也具有旋转对称性，这点从图可以很容易看出。因此，协议里选择在哪位共享者的量子比特最终获取目标态以及这位共享者的合作伙伴，可以有很多选择和组合，具体见表 2.

(III) 共享局限性及其物理原因. 从协议中可以看出，虽然是（3，5）阈协议，但并非任意三个共享者合作都能最终获取目标态. 具体而言，只有所选的那位最终在其量子比特上获取目标态的共享者和其两位邻居或者两位非邻居才能最终实现量子操作的共享，其它情况则不能够. $O_6$已对她的量子比特对$(6,8)$实施 Bell 态测量后，量子比特 1，2，3，4 和 5 的量子态$\left|\mathrm{S_{ij}}\right\rangle_{12345}$还可写为

$$\begin{aligned}
\left|S_{ij}\right\rangle_{12345} &= {}_{86}\langle\mathcal{B}_{ij}|(\mathcal{P}_{12}\mathcal{P}_{23}\mathcal{P}_{34}\mathcal{P}_{45}\mathcal{P}_{51})\\
&\times\left(\textstyle\prod_{k=1}^{5}\mathcal{P}_{6k}\right)|+\rangle_{123456}^{\otimes 6}|\varphi\rangle_8\\
&=\tfrac{1}{\sqrt{2}}[|\zeta_1\rangle_{2345}+|\zeta_2\rangle_{2345}\sigma_1^{(0,1)}\\
&+|\zeta_3\rangle_{2345}\sigma_1^{(1,0)}+|\zeta_4\rangle_{2345}\sigma_1^{(1,1)}]H_1\sigma_1^{(i,j)}|\varphi\rangle_1,
\end{aligned}\tag{23}$$

其中

$$\begin{aligned}
|\zeta_1\rangle_{2345} &= |\phi_{00}\rangle_{35}|\phi_{11}\rangle_{24}+|\phi_{01}\rangle_{35}|\phi_{10}\rangle_{24}\\
&-|\phi_{10}\rangle_{35}|\phi_{01}\rangle_{24}+|\phi_{11}\rangle_{35}|\phi_{00}\rangle_{24},
\end{aligned}\tag{24}$$

$$\begin{aligned}
|\zeta_2\rangle_{2345} &= |\phi_{00}\rangle_{35}|\phi_{10}\rangle_{24}-|\phi_{01}\rangle_{35}|\phi_{11}\rangle_{24}\\
&-|\phi_{10}\rangle_{35}|\phi_{00}\rangle_{24}-|\phi_{11}\rangle_{35}|\phi_{01}\rangle_{24},
\end{aligned}\tag{25}$$

$$\begin{aligned}
|\zeta_3\rangle_{2345} &= |\phi_{00}\rangle_{35}|\phi_{01}\rangle_{24}+|\phi_{01}\rangle_{35}|\phi_{00}\rangle_{24}\\
&-|\phi_{10}\rangle_{35}|\phi_{11}\rangle_{24}+|\phi_{11}\rangle_{35}|\phi_{10}\rangle_{24},
\end{aligned}\tag{26}$$

$$\begin{aligned}
|\zeta_4\rangle_{2345} &= |\phi_{00}\rangle_{35}|\phi_{00}\rangle_{24}-|\phi_{01}\rangle_{35}|\phi_{01}\rangle_{24}\\
&-|\phi_{10}\rangle_{35}|\phi_{10}\rangle_{24}+|\phi_{11}\rangle_{35}|\phi_{11}\rangle_{24}.
\end{aligned}\tag{27}$$

**表 2** 步骤(七)至(九)中两合作伙伴的操作与最终在其量子比特上获取目标态的共享者所做的相应 Pauli 操作. 其中"$|\mathcal{B}_{mn}\rangle$"对应合作伙伴

发送的两比特经典信息"$mn$"，"$ij$"为$O_6$所公布的经典信息.

**Table 2** Two partners' performance and the corresponding Pauli operations applied by the sharer to finally obtain the target state on his qubit from step 7 to step 9. "$|\mathcal{B}_{mn}\rangle$" corresponds to 2 bits classical message sent by partners and "$ij$" are classical bit message published by $O_6$.

| 合作伙伴 | 合作伙伴的测量结果及态对应的经典信息 | 最终目标态量子比特持有者及其的 Pauli 操作 | 合作伙伴 | 合作伙伴的测量结果及态对应的经典信息 | 最终目标态量子比特持有者及其的 Pauli 操作 |
|---|---|---|---|---|---|
| $S_1$、$S_3$ ($S_4$、$S_5$) | $\|\mathcal{B}_{11}\rangle_{13}$ ($\|\mathcal{B}_{00}\rangle_{45}$) | $S_2$ / $\sigma_2^{(i,j)}$ | $S_5$、$S_3$ ($S_1$、$S_2$) | $\|\mathcal{B}_{11}\rangle_{53}$ ($\|\mathcal{B}_{00}\rangle_{12}$) | $S_4$ / $\sigma_4^{(i,j)}$ |
| $S_1$、$S_3$ ($S_4$、$S_5$) | $\|\mathcal{B}_{01}\rangle_{13}$ ($\|\mathcal{B}_{11}\rangle_{45}$) | $S_2$ / $\sigma_2^{(i,j\oplus1)}$ | $S_5$、$S_3$ ($S_1$、$S_2$) | $\|\mathcal{B}_{01}\rangle_{53}$ ($\|\mathcal{B}_{11}\rangle_{12}$) | $S_4$ / $\sigma_4^{(i,j\oplus1)}$ |
| $S_1$、$S_3$ ($S_4$、$S_5$) | $\|\mathcal{B}_{00}\rangle_{13}$ ($\|\mathcal{B}_{01}\rangle_{45}$) | $S_2$ / $\sigma_2^{(i\oplus1,j)}$ | $S_5$、$S_3$ ($S_1$、$S_2$) | $\|\mathcal{B}_{00}\rangle_{53}$ ($\|\mathcal{B}_{01}\rangle_{12}$) | $S_4$ / $\sigma_4^{(i\oplus1,j)}$ |
| $S_1$、$S_3$ ($S_4$、$S_5$) | $\|\mathcal{B}_{10}\rangle_{13}$ ($\|\mathcal{B}_{10}\rangle_{45}$) | $S_2$ / $\sigma_2^{(i\oplus1,j\oplus1)}$ | $S_5$、$S_3$ ($S_1$、$S_2$) | $\|\mathcal{B}_{10}\rangle_{53}$ ($\|\mathcal{B}_{10}\rangle_{12}$) | $S_4$ / $\sigma_4^{(i\oplus1,j\oplus1)}$ |
| $S_2$、$S_4$ ($S_1$、$S_5$) | $\|\mathcal{B}_{11}\rangle_{24}$ ($\|\mathcal{B}_{00}\rangle_{15}$) | $S_3$ / $\sigma_3^{(i,j)}$ | $S_1$、$S_4$ ($S_2$、$S_3$) | $\|\mathcal{B}_{11}\rangle_{14}$ ($\|\mathcal{B}_{00}\rangle_{23}$) | $S_5$ / $\sigma_5^{(i,j)}$ |
| $S_2$、$S_4$ ($S_1$、$S_5$) | $\|\mathcal{B}_{01}\rangle_{24}$ ($\|\mathcal{B}_{11}\rangle_{15}$) | $S_3$ / $\sigma_3^{(i,j\oplus1)}$ | $S_1$、$S_4$ ($S_2$、$S_3$) | $\|\mathcal{B}_{01}\rangle_{14}$ ($\|\mathcal{B}_{11}\rangle_{23}$) | $S_5$ / $\sigma_5^{(i,j\oplus1)}$ |
| $S_2$、$S_4$ ($S_1$、$S_5$) | $\|\mathcal{B}_{00}\rangle_{24}$ ($\|\mathcal{B}_{01}\rangle_{15}$) | $S_3$ / $\sigma_3^{(i\oplus1,j)}$ | $S_1$、$S_4$ ($S_2$、$S_3$) | $\|\mathcal{B}_{00}\rangle_{14}$ ($\|\mathcal{B}_{01}\rangle_{23}$) | $S_5$ / $\sigma_5^{(i\oplus1,j)}$ |
| $S_2$、$S_4$ ($S_1$、$S_5$) | $\|\mathcal{B}_{10}\rangle_{24}$ ($\|\mathcal{B}_{10}\rangle_{15}$) | $S_3$ / $\sigma_3^{(i\oplus1,j\oplus1)}$ | $S_1$、$S_4$ ($S_2$、$S_3$) | $\|\mathcal{B}_{10}\rangle_{14}$ ($\|\mathcal{B}_{10}\rangle_{23}$) | $S_5$ / $\sigma_5^{(i\oplus1,j\oplus1)}$ |

利用公式(24-27)，很容易验证$\langle\zeta_i|\zeta_j\rangle=\delta_{ij}$, $(i,j\in\{1,2,3,4\})$. 因此，$\{|\zeta_i\rangle\}$是$2^4$维希尔伯特空间中一个四维子空间当中的正交完备基. 因此，通过正交基$\{|\zeta_i\rangle\}$对量子比特 2, 4, 3, 5 测量，那么量子比特 1 会坍缩到相应的单粒子态，这可从公式(23)中看出，且这些单粒子态可以通过相应的 Hadmard 门与 Pauli 操作转化为目标态. 但必须指出的是，$|\zeta_i\rangle$是量子比特 2, 4, 3, 5 的纠缠态，因此对它们的测量必须是持有量子比特 2, 4, 3, 5 的四位共享者 $S_2$、$S_3$、$S_4$、$S_5$ 共同合作才能实现. 注意，四量子比特 2, 4, 3, 5 的纠缠正交基$|\zeta_i\rangle$并不可以简单地分解为两组量子比特对的 Bell 态的直积，也即公式(23)不可转化为公式(22)的形式. 因此，无法通过只对两量子比特(2, 4)[或(3, 5)]进行 Bell 态测量使得量子比特 1 坍缩为一个单粒子纯态. 实际上，在此测量后，量子比特 3, 5[或 2, 4]与量子比特 1 是纠缠的. 因此，量子比特 1 实质处于量子混态. 综上所述，可知并非任意三个共享者合作都能最终获取目标态，这是此协议的局限性.

(IV) 成功概率. 从前面我们的方案过程介绍中容易看出, 本文提出的六方(3,5)阈协议是确定性的，也就是在理想情况下，理论上本协议可百分百成功共享目标量子操作.

(V) 实验可行性. 本文协议中所有量子操作都是局域的，其中的幺正操作包括单量子比特 Pauli 操作、两量子比特控制相位门操作和两量子比特控制非门操作，非幺正操作包括两量子比特 Bell 态测量和单量子比特计算基测量. 单量子比特 Pauli 操作和计算基测量在各种实验上早已经实现. 另外一些文献也报道了两量子比特控制相门操作和两量子比特控制非门操作以及两量子比特 Bell 态测量在离子阱、光学、光学微腔、腔量子电动力学等多种物理系统中得以实现[80-88]. 综上所述，随着实验技术的进一步发展，此协议的实验实现未来可期.

## 5 小结

本文基于八量子比特图态，提出了一种六方(3,5)阈量子操作共享协议. 文中分析讨论了该协议的一些性质, 如安全性、分享者对称性、共享局限性、成功概率、当前实验技术可行性等等，并讨论了部分性质的物理本质与原因. 结果表明, 该协议是安全的; 任一共享者与特定两位共享者合作，可确定性的获得目标量子态，即共享了目标量子操作； 根据文献报道的当前实验技术能力，根据当今实验技术，未来本协议的实验实现应已可期

## 参考文献

1 Bennett C H, Brassard G. Quantum cryptography: Public key distribution and coin tossing. In: Proceedings of Computers, Systems and Signal Processing. New York: IEEE, 1984. 175–179

2 Ekert A K. Quantum cryptography based on Bell's theorem. Phys Rev Lett, 1991, 67: 661–663

3 Long G L, Liu X S. Theoretically efficient high-capacity quantum-key-distribution scheme. Phys Rev A, 2002, 65: 03230

4 Deng F G, Long G L. Controlled order rearrangement encryption for quantum key distribution. Phys Rev A, 2003, 68: 042315

5 Kwek L C, Cao L, Luo W, et al. Chip-based quantum key distribution. AAPPS Bull, 2021, 31: 15

6 Liu B, Xia S, Xiao D, et al. Decoy-state method for quantum-key-distribution-based quantum private query. Sci China-Phys Mech Astron, 2022, 65: 240312

7 Bennett C H, Brassard G, Crépeau C, et al. Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels. Phys Rev Lett, 1993, 70: 1895–1899

8 Bouwmeester D, Pan J W, Mattle K, et al. Experimental quantum teleportation. Nature, 1997, 390: 575–579

9 Zhang Z J, Liu Y M. Perfect teleportation of arbitrary n-qudit states using different quantum channels. Phys Lett A, 2007, 372: 28–32

10 Cheung C Y, Zhang Z J. Criterion for faithful teleportation with an arbitrary multiparticle channel. Phys Rev A, 2009, 80: 022327

11 Ren J G, Xu P, Yong H L, et al. Ground-to-satellite quantum teleportation. Nature, 2017, 549: 70–73

12 Sheng Y B. Certifying quantum teleportation experimentally. Quantum Eng, 2019, 1: e22

13 Hillery M, Bužek V, Berthiaume A. Quantum secret sharing. Phys Rev A, 1999, 59: 1829–1834, arXiv: quant-ph/9806063

14 Tittel W, Zbinden H, Gisin N. Experimental demonstration of quantum secret sharing. Phys Rev A, 2001, 63: 042301

15 Lance A M, Symul T, Bowen W P, et al. Tripartite quantum state sharing. Phys Rev Lett, 2004, 92: 177903

16 Xiao L, Long G L, Deng F G, et al. Efficient multiparty quantum-secret-sharing schemes. Phys Rev A, 2004, 69: 052307

17 Deng F G, Li X H, Zhou H Y, et al. Improving the security of multiparty quantum secret sharing against Trojan horse attack. Phys Rev A, 2005, 72: 04430

18 Zhang Z J, Yang J, Man Z X, et al. Multiparty secret sharing of quantum information using and identifying Bell states. Eur Phys J D, 2005, 33: 133–136

19 Zhang Z J, Li Y, Man Z X. Multiparty quantum secret sharing. Phys Rev A, 2005, 71: 044301

20 Deng F G, Li X H, Li C Y, et al. Multiparty quantum-state sharing of an arbitrary two-particle state with Einstein-Podolsky-Rosen pairs. Phys Rev A, 2005, 72: 044301

21 Zhang Z J, Man Z X. Multiparty quantum secret sharing of classical messages based on entanglement swapping. Phys Rev A, 2005, 72: 022303

22 Zhang Z J, Cheung C Y. Minimal classical communication and measurement complexity for quantum information splitting. J Phys B-At Mol Opt Phys, 2008, 41: 015503

23 Sheng Y B, Deng F G, Zhou H Y. Efficient and economic five-party quantum state sharing of an arbitrary m-qubit state. Eur Phys J D, 2008, 48: 279–28424 Lu H, Zhang Z, Chen L K, et al. Secret sharing of a quantum state. Phys Rev Lett, 2016, 117: 030501

25 Zhang Z, Lin S, Yuan H, Xie C, Ye B. Three-party quantum state sharing with six-qubit entangled mixing state. Sci China-Phys Mech Astron, 2023, 53: 110312. [张战军, 林诗凡, 袁好, 谢传梅, 叶表良. 基于六量子比特纠缠混态的三方量子态分享.中国科学: 物理学 力学 天文学 2023 年 第 53 卷 第 11 期: 110312]

26 Lo H K. Classical-communication cost in distributed quantum-information processing: A generalization of quantum-communication complexity. Phys Rev A, 2000, 62: 012313

27 Bennett C H, DiVincenzo D P, Shor P W, et al. Remote State Preparation. Phys Rev Lett, 2001, 87: 077902

28 Deng F G, Long G L, Liu X S. Two-step quantum direct communication protocol using the Einstein-Podolsky-Rosen pair block. Phys Rev A, 2003, 68: 042317

29 Deng F G, Long G L. Secure direct communication with a quantum one-time pad. Phys Rev A, 2004, 69: 052319

30 Zhang Z J, Li Y, Man Z X. Improved Wojcik's eavesdropping attack on ping-pong protocol without eavesdropping-induced channel loss. Phys Lett A, 2005, 341: 385

31 Lee H, Lim J, Yang H J. Quantum direct communication with authentication. Phys Rev A, 2006, 73: 042305

32 Z. J. Zhang, J. Liu, D. Comment on “Quantum direct communication with authentication”. Phys Rev A, 2007, 75: 026301

33 Zhang W, Ding D S, Sheng Y B, et al. Quantum secure direct communication with quantum memory. Phys Rev Lett, 2017, 118: 220501

34 Chen S S, Zhou L, Zhong W, et al. Three-step three-party quantum secure direct communication. Sci China-Phys Mech Astron, 2018, 61: 090312

35 Yang L, Wu J W, Lin Z S, et al. Quantum secure direct communication with entanglement source and single-photon measurement. Sci ChinaPhys Mech Astron, 2020, 63: 110311

36 Zhou L, Sheng Y B, Long G L. Device-independent quantum secure direct communication against collective attacks. Sci Bull, 2020, 65: 12–20

37 Li T, Long G L. Quantum secure direct communication based on single-photon Bell-state measurement. New J Phys, 2020, 22: 063017

38 Long G L, Zhang H. Drastic increase of channel capacity in quantum secure direct communication using masking. Sci Bull, 2021, 66: 1267–1269

39 Qi Z, Li Y, Huang Y, et al. A 15-user quantum secure direct communication network. Light Sci Appl, 2021, 10: 183

40 Ye Z D, Pan D, Sun Z, et al. Generic security analysis framework for quantum secure direct communication. Front Phys, 2021,16: 21503

41 Liu X, Luo D, Lin G, et al. Fiber-based quantum secure direct communication without active polarization compensation. Sci China-Phys Mech Astron, 2022, 65: 120311

42 Zhou L, Sheng Y B. One-step device-independent quantum secure direct communication. Sci China-Phys Mech Astron, 2022, 65: 250311

43 Sheng Y B, Zhou L, Long G L. One-step quantum secure direct communication. Sci Bull, 2022, 67: 367

44 Hong Y P, Zhou L, Zhong W, et al. Measurement-device-independent three-party quantum secure direct communication. Quantum Inf Process, 2023, 22: 111

45 Huelga S F, Vaccaro J A , Chefles A, et al. Quantum remote control: Teleportation of unitary operations. Phys Rev A, 2001, 63: 042303

46 Huelga S F, Plenio M B, Vaccaro J A. Remote control of restricted sets of operations: Teleportation of angles. Phys Rev A, 2002, 65: 042316

47 Zhang Z, Cheung C Y. Shared quantum remote control: quantum operation sharing. J Phys B-At Mol Opt Phys, 2011, 44: 165508

48 Wang S, Liu Y, Chen J, et al. Deterministic single-qubit operation sharing with five-qubit cluster state. Quantum Inf Process, 2013, 12: 2497–2507

49 Ye B L, Liu Y M, Liu X S, et al. Remotely sharing a single-qubit operation with a five-qubit genuine state. Chin Phys Lett, 2013, 30: 020301

50 Liu D, Liu Y, Xie C, et al. Shared quantum control via sharing operation on remote single qutrit. Quantum Inf Process, 2013, 12: 3527–3542

51 Liu D C, Liu Y M, Yin X F, et al. Generalized three-party qubit operation sharing. Int J Quantum Inf, 2013, 11(1): 1350011

52 Ji Q, Liu Y, Yin X, et al. Quantum operation sharing with symmetric and asymmetric W states. Quantum Inf Process, 2013, 12: 2453–2464

53 Xing P F, Liu Y M, Xie C M, et al. Generalized three-party sharing of operations on remote single qutrit. Int J Quantum Inf, 2014, 12: 1450011

54 Ji Q, Liu Y, Xie C, et al. Tripartite quantum operation sharing with two asymmetric three-qubit W states in five entanglement structures. Quantum Inf Process, 2014, 13: 1659–1676

55 Xing H, Liu D, Xing P, et al. Deterministic tripartite sharing of eight restricted sets of single-qubit operations with two Bell states or a GHZ state. Int J Quantum Inform, 2014, 12: 1450012

56 Xing H, Liu Y M, Xie C M, et al. Four-party deterministic operation sharing with six-qubit cluster state. Quantum Inf Process, 2014, 13(3): 1553–1562

57 Xing H, Liu Y, Xie C, et al. Four-party deterministic operation sharing with six-qubit cluster state. Quantum Inf Process, 2014, 13: 1553–1562

58 Xie C, Liu Y, Xing H, et al. Probabilistic three-party sharing of operation on a remote qubit. Entropy, 2015, 17: 841–851

59 Duan Y J, Zha X W. Remotely sharing a single-qubit operation via a six-qubit entangled state. Int J Theor Phys, 2015, 54: 877–883

60 Zhang K J, Zhang L, Song T T, et al. A potential application in quantum networks – Deterministic quantum operation sharing schemes with Bell states. Sci China-Phys Mech Astron, 2016, 59(6): 660302

61 Peng J. Tripartite operation sharing with a six-particle maximally entangled state. Quantum Inf Process, 2015, 14: 4255–4262

62 Peng J. Tripartite operation sharing with five-qubit Brown state. Quantum Inf Process, 2016, 15: 2465–2473

63 Zhou S, Bai M, Zhang C. Analysis and construction of four-party deterministic operation sharing with a generalized seven-qubit Brown state. Mod Phys Lett B, 2017, 31: 1750190

64 Peng J Y, Bai M Q, Mo Z W. Multicharacters remote rotation sharing with five-particle cluster state. Quantum Inf Process, 2019, 18: 339

65 Zhang Z J, Zhang W B, Ye B L, Tripartite quantum operation sharing with six-qubit entangled state. Int J Theor Phys, 2020, 59(5): 1605–1611

66 Yuan H, Zhang W B, Yin X F. Simplistic quantum operation sharing with a five-qubit genuinely entangled state. Quantum Inf Process, 2020, 19: 122

67 Zhang Z J, Li D, Zhang L, et al. Efficient tripartite quantum operation sharing with five-qubit absolutely maximally entangled state. Int J Theor Phys, 2021, 60: 2583–2591

68 Zhang Z, Zhang L, Zhuge B, et al. Four-party deterministic quantum operation sharing with a generalized seven-qubit Brown state. Laser Phys Lett, 2021, 18: 055202

69 Zhang Z. Tripartite quantum operation sharing with six-qubit highly entangled state. Mod Phys Lett A, 2021, 36: 2150034

70 Peng J Y, Xiang Y. Multiparty quantum rotation operation sharing. Int J Theor Phys, 2021, 60: 3771–3782

71 Zhang Z, Yuan H. Deterministic tripartite sharing of an arbitrary single-qubit operation with the five-qubit cluster state in a given entanglement structure. Quantum Inf Process, 2021, 20: 3

72 Zhang Z, Deng L, Zhang L, et al. Efficient tripartite quantum operation sharing with five-qubit absolutely maximally entangled state. Int J Theor Phys, 2021, 60: 2583–2591

73 Zhang Z J, Zhang L, Zhuge B, et al. Tripartite quantum operation sharing with a six-qubit absolutely maximally entangled state. Int J Theor Phys, 2021, 60: 2520–2530

74 Zhang Z J, Yuan H, Xie C M, et al. Four-party quantum operation sharing with 7-qubit mixing state (in Chinese). Sci Sin-Phys Mech Astron, 2022, 52: 120313 [张战军, 袁好, 谢传梅, 等. 基于一种七量子比特混态的四方量子操作分享. 中国科学: 物理学 力学 天文学, 2022, 52: 120313]

75 Peng J Y, Wu F, Tang J G, et al. Quantum multicast, multi-output protocols of quantum state sharing and quantum operation sharing via

six-particle cluster state. Quantum Inf Process, 2023, 22: 424

76 Shi W M, Bai M X, Zhou Y H, et al. Hierarchical quantum rotation operation sharing with multiparty users. Quantum Inf Process, 2024, 23: 196

77 Markham D, Sanders B C. Graph states for quantum secret sharing. Phys Rev A, 2008, 78: 042309

78 Keet A, Fortescue B, Markham D, et al. Quantum secret sharing with qudit graph states. Phys Rev A, 2010, 82: 062315

79 Qiu X Y, Chen L. Controlled Remote Implementation of Operations via Graph States. Ann Phys (Berl), 2023, 535: 2300320

80 Boschi D, Branca S, de Martini F, et al. Experimental realization of teleporting an unknown pure quantum state via dual classical and EinsteinPodolsky-Rosen channels. Phys Rev Lett, 1998, 80: 1121–1125

81Ikram M, Zhu S Y, Zubairy M S. Quantum teleportation of an entangled state. Phys Rev A, 2000, 62: 022307

82 Solano E, Cesar C L, de Matos Filho R L, et al. Reliable teleportation in trapped ions. Eur Phys J D, 2001, 13: 121–128

83 Riebe M, Häffner H, Roos C F, et al. Deterministic quantum teleportation with atoms. Nature, 2004, 429: 734–737

84 Barrett M D, Chiaverini J, Schaetz T, et al. Deterministic quantum teleportation of atomic qubits. Nature, 2004, 429: 737–739

85 Sheng Y B, Deng F G, Long G L. Complete hyperentangled-Bell-state analysis for quantum communication. Phys Rev A, 2010, 82: 032318

86 Ren B C, Wei H R, Hua M, et al. Complete hyperentangled-Bell-state analysis for photon systems assisted by quantum-dot spins in optical microcavities. Opt Express, 2012, 20: 24664

87 Zhou L, Sheng Y B. Complete logic Bell-state analysis assisted with photonic Faraday rotation. Phys Rev A, 2015, 92: 042314

88 Wang G Y, Ai Q, Ren B C, et al. Error-detected generation and complete analysis of hyperentangled Bell states for photons assisted by quantum dot spins in double-sided optical microcavities. Opt Express, 2016, 24: 28444

# Six-party (3,5)-threshold quantum operation sharing with 8-qubit graph state

**JI ShiYu[1], YUAN Hao[2], YU JinHua[1], LI Bo[3] & ZHANG ZhanJun[1*]**

[1]*School of Information & Electronic Engineering (Sussex Artificial Intelligence Institute), Zhejiang Gongshang University, Hangzhou 310018, China*

[2]*School of Physics and Optoelectric Engineering, Anhui University, Hefei 230601, China ;*

[3]*School of Computer and Computing Science, Hangzhou City University, Hangzhou 310015, China*

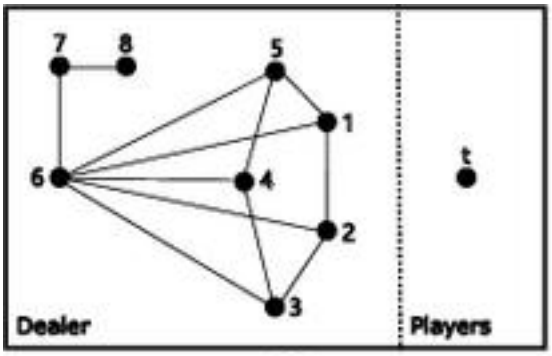
**Corresponding author (email: zhangzhanjun@zjgsu.edu.cn)*

Quantum operation sharing (QOS) is an important quantum remote control technique, which can be used for remotely encrypting or decrypting quantum information. To date, all the sharers should collaborate together to conclusively share the remote quantum operation in all the existing QOS schemes, which are the so-called (n,n)-threshold ones. In this paper, a six-party (3,5)-threshold QOS scheme is put forward by utilizing a 8-qubit graph state, where 3 sharers among the 5 ones are able to achieve the sharing of the remote initial owner's arbitrary operation. We investigated the symmetry and the limitation of the sharers who can reach the achievement, success probability and its underlying physics, scheme security, and scheme feasibility. The scheme is observed to be secure, including that the quantum remote operation can be safely shared successfully by any sharer with whose two neighboring partners or two non-neighboring partners; moreover, the scheme is feasible in terms of the current technologies.

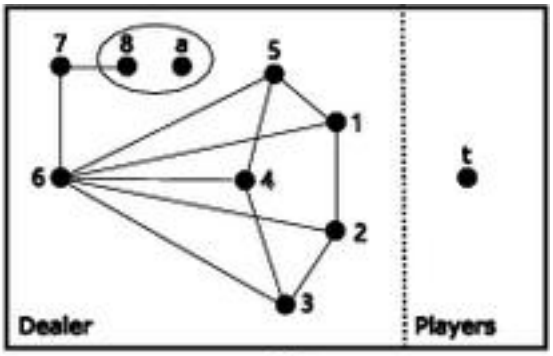
**Keywords:(3,5)-threshold, quantum operation sharing, six-party, 8-qubit graph state**

**PACS:** 03.67.Hk, 03.67.Dd, 03.65.Ud

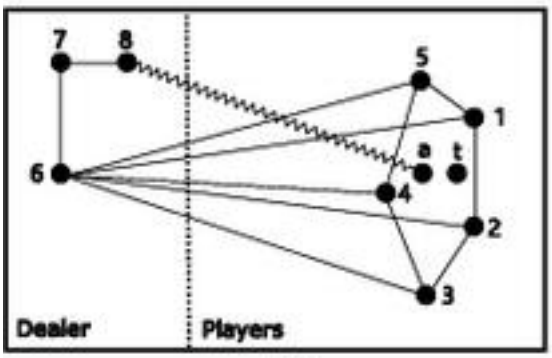
**doi:** 10.1360/SSPMA2016-00000



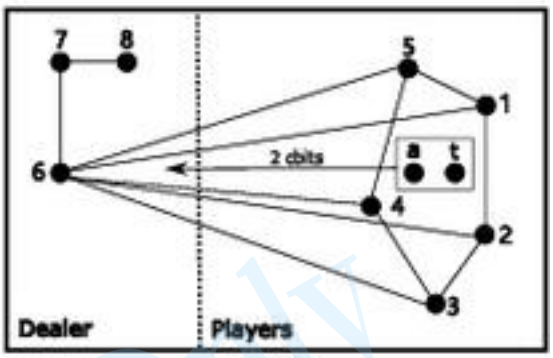

(a)



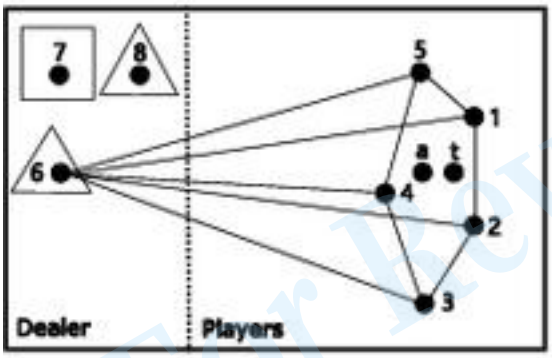

(b)



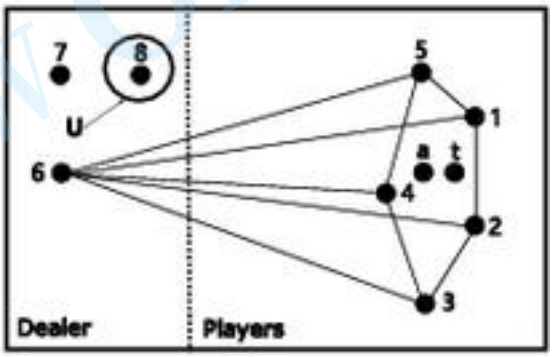

(c)



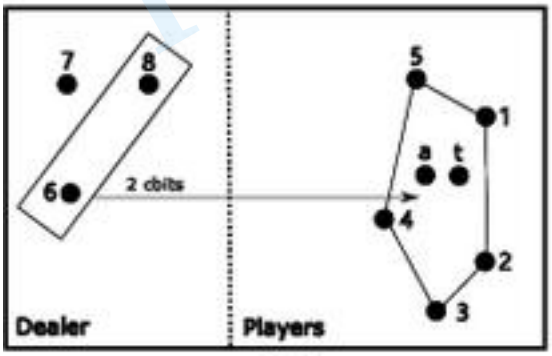

(d)



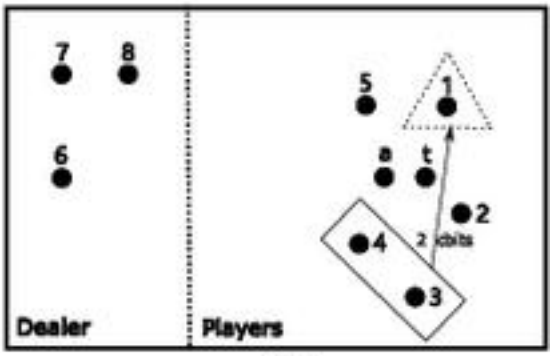

(e)




(f)




(g)




(h)

505×653