中国科学 : 物理学 力学 天文学 2025 年 第 55 卷 第 4 期 : 240315
SCIENTIA SINICA Physica, Mechanica & Astronomica physcn.scichina.com
《中国科学》杂志社 SCIENCE CHINA PRESS
论 文 量子密码和量子计算专题

受控型非局域CNOT量子门的设备无关验证

黎一宁, 宫能飞, 田悦含, 王铁军*

北京邮电大学理学院, 北京 100876
*联系人, E-mail: wangtiejun@bupt.edu.cn

收稿日期: 2024-11-26; 接受日期: 2025-01-02; 网络出版日期: 2025-02-24
分布式量子计算网络物理性质的研究(编号: 62471058)和北京邮电大学信息光子学与光通信全国重点实验室自主课题项目(编号: IPOC2022ZT10)资助

摘要 受控非局域量子门操作揭示了量子网络中控制方与非局域门操作方之间的合作与控制关系, 是构建多方量子计算网络的关键, 其安全性保证来源于量子纠缠资源. 针对供应商以经典-量子混合资源代替量子纠缠资源的行为, 本文提出了一种受控非局域CNOT量子门的设备无关验证方案, 并在Svetlichny不等式不适用的情况下设计了Svetlichny-type不等式, 有效检验了非局域门操作中纠缠资源利用情况. 我们的方案为未来构建安全的分布式量子计算网络提供了理论基础.

关键词 分布式量子计算, 受控非局域量子门, 设备无关验证

PACS: 03.67.-a, 03.67.Ac, 03.67.Dd, 03.67.Lx

1 引言

量子计算[1]是一种基于量子力学规律调控量子信息单元进行高性能计算的新型计算技术[2]. 理论上, 量子系统的叠加性使得量子计算机拥有进行高度并行计算的能力[3]. 如果能实现成百上千位容错量子位的有效计算[4], 那么量子计算将有望突破经典算力瓶颈[5–8], 成为人工智能和新质生产力的“引擎”[9–11]. 目前, 最具有实现量子计算潜质的物理系统有中性原子系统[12,13]、超导量子比特系统[14–16]、半导体量子点系统[17,18]、离子阱系统[19]、光量子系统[20,21]等. 其中, 基于中性原子系统的量子处理器拥有目前最多的量子比特数. 然而, 由于噪声的存在, 量子比特还需要进行纠错和避错才能进行有效的计算. 一个逻辑比特需要很多个物理比特通过纠错码表示, 在实际计算问题中实现0.1%的门错误率至少需要成千上万个物理比特[22,23]. 以目前的技术手段, 大规模扩展量子比特的数目仍是量子计算机发展所面临的巨大挑战. 进一步地, 随着量子比特数量的增加, 如何控制、互连和保存量子比特, 也成为实现大规模量子计算的技术难点[24]. 在此背景下, 分布式量子计算(Distributed Quantum Computing, DQC)[25]成为实现大规模量子计算的有效途径之一.

根据DQC范式, 大型量子计算任务由多个空间分离的、具有有限量子位的量子处理模块(量子节点)协同完成[26]. DQC 网络中不同量子节点通常需要完成

引用格式: 黎一宁, 宫能飞, 田悦含, 等. 受控型非局域CNOT量子门的设备无关验证. 中国科学: 物理学 力学 天文学, 2025, 55: 240315
Li Y N, Gong N F, Tian Y H, et al. Device-independent verification of controlled non-local CNOT quantum gate (in Chinese). Sci Sin-Phys Mech Astron, 2025, 55: 240315, doi: 10.1360/SSPMA-2024-0575

不同的计算任务, 这些任务需要通过逻辑操作进行关联以形成大规模的计算任务. 由于单个节点所需要处理的量子计算任务复杂度低、量子电路深度浅, DQC具有显著的降噪优势[27], 为容错量子计算提供了新的解决思路.

DQC网络中的不同子任务之间可以通过非局域的量子门操作进行任务关联, 不同节点间的非局域双量子位逻辑门操作可由量子门隐形传输(Quantum Gate Teleportation, QGT)协议[28]实现. 根据QGT协议, 双方事先共享一对EPR纠缠粒子, 各自持有一个纠缠粒子以及一个待执行门操作的量子比特. 随后, 他们局域地对手中的两个比特执行相应的操作与测量, 并通过经典信道向对方传输测量结果. 最终, 双方基于这些测量结果对手中的粒子执行相应的局域幺正操作, 从而完美实现非局域量子门的操作. 早在2004年, 郭光灿院士团队[29]已经实现了原型CNOT量子门隐形传输的实验演示. 2018年, Chou等人[30]通过实验实现了一个远程传输的CNOT量子门, 并通过实时自适应控制使其具有确定性, 传输保真度达到0.79. 2024 年, 郭光灿院士团队[31]展示了在空间上相隔7.0 km的两个节点之间的非局域光子量子门, 实现了量子门在城域尺度距离上的原理验证演示. 基于量子纠缠独特的非局域性[32], QGT可以完成计算任务的关联, 且此过程中不需要传输任何实际参与局域计算任务的物理比特, 具有更高的安全性[33].

安全、完美地执行QGT协议的关键在于以量子纠缠作为量子信道[34]. 然而, 量子纠缠在信道中传输时容易受到噪声影响导致退相干[35–37], 且高质量分发量子纠缠资源的成本相对较高, 在实际量子网络中设备供应商很有可能利用经典资源或经典-量子混合资源模拟量子隐形传态(Quantum Teleportation, QT)及QGT的执行过程[38–42], 以达到节约量子纠缠资源、降低成本的目的. 通常, 平均保真度是衡量量子信息处理协议性能的重要指标. 然而, Popescu[43]证明在Alice和Bob没有共享纠缠态的情况下, 量子隐形传态的平均保真度最高可达$\bar{F}=\frac{2}{3}$. Gisin[41]提出的经典模型可以模拟隐形传态的保真度达0.87. 2014年, Ho等人[44]还提出了保真度高达0.97的经典模拟QT的方案. 2023年, Wang等人[42]提出了保真度为0.9545的经典模拟QGT方案. 因此, 仅分析协议实现的平均保真度并不可靠[45], 需要额外的判据作为补充.

设备无关(Device-Independent, DI)[46,47]框架提供了一种在设备完全不可信的情况下认证协议安全性的有效后验手段. DI框架以输入-输出的概率分布描述黑盒设备中所执行的任务, 而不需要关注设备内部的构造和具体操作细节, 其验证方案基于量子非局域相关性[32]. 1964年, 针对EPR (Einstein-Podolsky-Rosen Paradox的简称)佯谬[48], Bell从定域实在论及隐变量理论出发推导出了Bell不等式[49], 满足贝尔不等式的关联为经典关联, 违背贝尔不等式的关联为贝尔非局域相关. 对于给定的量子态及基于该量子态所执行的量子过程, 这样的不等式违背是无法被经典模型模拟的[50], 因此DI验证可作为检验量子信息处理协议真实性的有效方法. 2006年, Acín等人[51]首先提出了一个基于CHSH不等式的设备无关量子密钥分发(Device-independent Quantum Key Distribution, DI-QKD)方案, 正式奠定了DI-QKD的思想; 此后, 针对多方DI-QKD(也称为DI-Conference Key Agreement, DI-CKA)[52]的研究也在理论上展开了探索. 在此启发之下, 有研究者将DI框架应用于检验基于信道的功能实现中纠缠资源的使用情况. 然而, 人们发现针对于信道的DI验证操作在检验基于相同信道的非局域量子功能操作是否还具有量子性时失效了, 因此需要结合非局域量子功能的具体过程定制相应的DI验证方案来进行验证. 2013 年, Ho等人[44]首先提出针对QT的DI验证方案; 2023年, Wang等人[42]研究了基于黑盒模型的CNOT门隐形传输DI验证方案, 在基于Bell态的噪声信道中, 若非局域CNOT门的实现保真度大于97.53%且检测到CHSH不等式违背, 则可以证明非局域CNOT门传输协议是可信的. 这些成功的探索表明了DI验证手段应用于检验基于信道的功能实现的可行性.

除了二方通信外, 多方之间的监督、合作和控制也是量子网络中需要实现的基本功能[53–56]. 特别是当一个普通用户连接到一个量子网络来实现一些计算功能时, 用户需要监控网络中量子服务器的运行状态, 并在发生潜在危机时控制并制止计算的实现. 同时, 用户有必要具备调节网络资源、提高网络效率的能力[57]. 受控型量子信息处理协议成为了实际量子网络中用户安全入网的有效途径之一, 其安全性检验方案也成为了重要的研究方向. 2022 年, Gangopadhyay等人[58]设计了受控量子隐形传态(Controlled Quantum Teleporta-

tion, CQT)的DI验证方案, 有效地实现了多方QT的安全性检验. 然而, 目前尚未提出针对受控型非局域量子门的DI验证方案.

针对未来供应商以经典资源或经典-量子混合资源替代量子纠缠资源的行为, 本文给出了基于黑盒模型的受控型非局域CNOT量子门DI验证方案. 在黑盒模式下[59], 当供应商以经典-量子混合资源$\frac{1}{2}(|\phi^+\rangle_{ab}\langle\phi^+||+\rangle_c\langle+|+|\phi^-\rangle_{ab}\langle\phi^-||-\rangle_c\langle-|)$替代量子纠缠资源$\frac{1}{\sqrt{2}}(|000\rangle+|111\rangle)_{abc}$时, 通过控制力的测量无法发现供应商的欺骗行为, 并且无法基于Svetlichny不等式直接对信道资源进行检验. 基于此, 我们提出了Svetlichny-type不等式作为验证手段, 其可在受控非局域CNOT量子门实施过程中进行DI验证, 对量子信道态进行区分, 以发现供应商的欺骗行为. 此工作为分布式量子网络的安全性保障提供了理论基础.

2 标准受控CNOT量子门隐形传输协议

2.1 受控CNOT量子门隐形传输过程

用户Charlie希望通过非局域CNOT量子门操作使得两个空间分离的量子处理器Alice和Bob之间实现信息(qubit A和qubit B)的远程关联. 为了完成上述目标, 他们执行以GHZ态[60]为量子信道的标准受控CNOT量子门隐形传输(Controlled CNOT Quantum Gate Teleportation, 受控CNOT-QGT)协议, 具体内容如下.

(1) 三方共享GHZ态为量子信道:

$$|\mathrm{GHZ}\rangle_{abc}=\frac{1}{\sqrt{2}}(|000\rangle+|111\rangle)_{abc}, \tag{1}$$

记其密度矩阵形式为$\rho_{abc}^{\mathrm{GHZ}}=|\mathrm{GHZ}\rangle_{abc}\langle\mathrm{GHZ}|$, 其中纠缠粒子$a$, b, c分别分发给Alice, Bob, Charlie. 此外, 他们彼此可以通过经典信道交流测量结果.

(2) 设Charlie对纠缠粒子c执行沿X方向的投影测量M_c^γ并输出测量结果γ,

$$M_c^\gamma=\frac{I_2+\gamma\cdot\sigma_x}{2},\gamma\in\{-1,+1\}, \tag{2}$$

测量后, Alice和Bob间的量子信道ab塌缩至ρ_{ab}^γ,

$$\rho_{ab}^\gamma=\frac{\mathrm{Tr}^c\left[(I_2\otimes I_2\otimes M_c^\gamma)\rho_{abc}^{\mathrm{GHZ}}\right]}{\mathrm{Tr}\left[(I_2\otimes I_2\otimes M_c^\gamma)\rho_{abc}^{\mathrm{GHZ}}\right]}=|\phi^\gamma\rangle\langle\phi^\gamma|, \tag{3}$$

当$\gamma=\pm1$时, $\left|\phi^{\pm1}\right\rangle=\frac{1}{\sqrt{2}}(|00\rangle\pm|11\rangle)_{ab}$. 此时, 将Alice和Bob间的量子信道为$\rho_A\otimes\rho_{ab}^\gamma\otimes\rho_B$.

(3) 以qubit A和qubit B为执行非局域CNOT量子门操作U_B^A的初始输入态, 则初始量子系统AB为$\rho_{AB}^{\mathrm{initial}}=\rho_A\otimes\rho_B$, ρ_A和ρ_B分别代表qubit A和qubit B 的密度矩阵, 对应的目标输出态为$\rho_{AB}^{\mathrm{CNOT}}=U_B^A\rho_{AB}^{\mathrm{initial}}U_B^{A\dagger}$, 其中

$$U_B^A=\begin{pmatrix}1&0&0&0\\0&1&0&0\\0&0&0&1\\0&0&1&0\end{pmatrix}. \tag{4}$$

设$\rho_{AB}^{\mathrm{initial}}$, $\rho_{AB}^{\mathrm{CNOT}}$所对应的Bloch向量分别为$\boldsymbol{m}$, $\boldsymbol{n}$, 根据高维量子系统的密度矩阵与高维Bloch向量间的关系[61,62], 有

$$\begin{aligned}\rho_{AB}^{\mathrm{initial}}&=\frac{1}{4}\mathbb{I}_4+\frac{1}{2}\boldsymbol{m}\cdot\boldsymbol{\lambda},\\ \rho_{AB}^{\mathrm{CNOT}}&=\frac{1}{4}\mathbb{I}_4+\frac{1}{2}\boldsymbol{n}\cdot\boldsymbol{\lambda},\end{aligned} \tag{5}$$

其中, $\mathbb{I}_n$为n维单位矩阵, $\boldsymbol{\lambda}=(\lambda_1,...,\lambda_{15})$是代数$SU(4)$群的生成元算子, 具体表达式见附录.

(4) Alice对所持有的qubit A和纠缠粒子a执行一个以A为控制比特, a为受控比特的局域CNOT门U_a^A. 为了将A与a间的量子门关系传输到A和B上, Bob对其持有的qubit B和纠缠粒子b执行一个以b为控制比特, B为受控比特的局域CNOT门U_B^b. 此时联合系统$AabB$的量子态为

$$\rho_{AabB}^\gamma=(U_a^A\otimes U_B^b)(\rho_A\otimes\rho_{ab}^\gamma\otimes\rho_B)(U_a^A\otimes U_B^b)^\dagger. \tag{6}$$

为了确定此时系统AB的具体状态, Alice和Bob分别沿Z和X方向测量纠缠粒子a和b, 并输出结果s_0, s_1. 设他们的投影测量算子分别为

$$M_{a,z}^{s_0}=\frac{\mathbb{I}_2+s_0\cdot\sigma_z}{2},\qquad M_{b,x}^{s_1}=\frac{\mathbb{I}_2+s_1\cdot\sigma_x}{2}, \tag{7}$$

其中, $\sigma_z(\sigma_x)$为泡利$Z(X)$矩阵, $s_0(s_1)\in\{-1,+1\}$.

为便于处理数据, 此处将$s_0(s_1)$的取值范围映射到$\{0,1\}$. 令$\tilde{s}_i=-\frac{1}{2}(s_i-1)$ $(i\in\{0,1\})$, 则基于输出结果$(\tilde{s}_0\tilde{s}_1\gamma)$的联合系统$AB$为

$$\rho_{AB}^{\tilde{s}_0\tilde{s}_1\gamma}=\mathrm{Tr}^{ab}\left[\frac{(M_{a,z}^{s_0}\otimes M_{b,x}^{s_1})\rho_{AabB}^\gamma(M_a^{s_0}\otimes M_{b,x}^{s_1})^\dagger}{\mathrm{Tr}(M_{a,z}^{s_0}\otimes M_{b,x}^{s_1})\rho_{AabB}^\gamma(M_{a,z}^{s_0}\otimes M_{b,x}^{s_1})^\dagger}\right]. \tag{8}$$

设$\rho_{AB}^{\tilde{s}_0\tilde{s}_1\gamma}$对应的15维Bloch向量为$\boldsymbol{n}'$, 则有

$$\rho_{AB}^{\tilde{s}_0\tilde{s}_1\gamma}=\frac{1}{4}\mathbb{I}_4+\frac{1}{2}\boldsymbol{n}'\cdot\boldsymbol{\lambda}. \tag{9}$$

(5) 当Charlie许可时, 他向Alice和Bob传输γ, Alice和Bob根据$(\tilde{s}_0\tilde{s}_1\gamma)$分别对qubit A和qubit B执行正确的幺正操作$R_{\tilde{s}_0\tilde{s}_1\gamma}$ (见附录), 并得到系统AB的最终输出态ρ_{AB}^{final}. 在式(9)的基础上, ρ_{AB}^{final}可以明确表示为

$$\rho_{AB}^{\text{final}}=\frac{1}{4}\mathbb{I}_4+\frac{1}{2}(R_{\tilde{s}_0\tilde{s}_1\gamma}\cdot\boldsymbol{n}')\cdot\boldsymbol{\lambda}, \tag{10}$$

此时, 有$(R_{\tilde{s}_0\tilde{s}_1\gamma}\cdot\boldsymbol{n}')=\boldsymbol{n}$, 即$\rho_{AB}^{\text{final}}=\rho_{AB}^{\text{CNOT}}$.

2.2 Charlie的控制力

Charlie的控制力定义为, 他许可时实施非局域CNOT量子门的平均保真度F_C与他不许可时的平均保真度F_{NC}的差值, 即

$$CP=F_C-F_{NC}. \tag{11}$$

平均保真度定义为, 执行幺正操作后的量子系统ρ_{AB}^{final}与目标量子系统ρ_{AB}^{CNOT}的接近程度, 即

$$F=\int_S\langle n|\rho_{AB}^{\text{final}}|n\rangle\frac{\mathrm{d}\boldsymbol{n}}{S}, \tag{12}$$

其中, $\boldsymbol{n}$为ρ_{AB}^{CNOT}所对应的15维Bloch向量, $|n\rangle$为沿$\boldsymbol{n}$的基矢, $\langle n|$为其共轭形式, $S=\iint\mathrm{d}\boldsymbol{A}\mathrm{d}\boldsymbol{B}=16\pi^2$. 根据式(10)进一步计算, 得到

$$F=\int_S\frac{1}{4}+\frac{\boldsymbol{n}\cdot(R_{\tilde{s}_0\tilde{s}_1\gamma}\cdot\boldsymbol{n}')}{2}\frac{\mathrm{d}\boldsymbol{n}}{S}. \tag{13}$$

当Charlie许可时, ρ_{AB}^{final}能够完美地恢复到目标态ρ_{AB}^{CNOT}, 因此F_C表示为

$$F_C=\int_S\frac{1}{4}+\frac{\boldsymbol{n}\cdot\boldsymbol{n}}{2}\frac{\mathrm{d}\boldsymbol{n}}{S}=1. \tag{14}$$

当Charlie不许可时, 他保留自己的测量结果γ. 由于缺少了Charlie的信息, Alice和Bob只能猜测Charlie的输出为γ' (他们有1/2的概率猜对), 并以幺正旋转$R_{\tilde{s}_0\tilde{s}_1\gamma'}$代替$R_{\tilde{s}_0\tilde{s}_1\gamma}$. 因此$F_{NC}$表示为

$$\begin{aligned}F_{NC}=\int_S\sum_{\gamma,\gamma'\in\{-1,+1\}}\sum_{\tilde{s}_0\tilde{s}_1\in\{0,1\}}P(\tilde{s}_0\tilde{s}_1\gamma\gamma')\\ \times\left(\frac{1}{4}+\frac{\boldsymbol{n}\cdot R_{\tilde{s}_0\tilde{s}_1\gamma'}\boldsymbol{n}'}{2}\right)\frac{\mathrm{d}\boldsymbol{n}}{S}=\frac{2}{3},\end{aligned} \tag{15}$$

其中, $P(\tilde{s}_0\tilde{s}_1\gamma\gamma')=\frac{1}{16}$, 表示执行$R_{\tilde{s}_0\tilde{s}_1\gamma'}$的概率. 根据式(11), Charlie对非局域CNOT量子门的控制力为

$$CP=F_C-F_{NC}=\frac{1}{3}. \tag{16}$$

3 受控CNOT-QGT的设备无关验证方案

在实际场景中, 设备往往由外部的供应商提供. 为了节约成本, 供应商可能会采用经典-量子混合资源来替代真多方量子纠缠资源作为设备内部的信道. 这些设备虽然能够执行标准协议, 但其可能与外部的其他系统存在隐含的关联, 从而给潜在的窃听者和攻击者提供了可乘之机. 这一行为极大地增加了协议执行中被非法窃听和恶意干扰的风险, 从而对分布式量子计算的整体安全性构成严峻挑战.

如以某些具有类似于GHZ态结构的特定混态$\rho_{abc}^{\text{Classic}}$ [63]为信道执行协议时, 根据第2.1节, Charlie沿X方向测量自己的系统后, Alice和Bob之间仍旧以Bell态为信道执行标准的两方非局域门传输过程, 最终Charlie的控制力为$CP=\frac{1}{3}$, 具有与标准协议一致的效果.

$$\rho_{abc}^{\text{Classic}}=\frac{1}{2}\left(|\phi^+\rangle_{ab}\langle\phi^+||+\rangle_c\langle+|+|\phi^-\rangle_{ab}\langle\phi^-||-\rangle_c\langle-|\right). \tag{17}$$

若将$\rho_{abc}^{\text{Classic}}$掺杂至设备中, 则此时信道为

$$\rho=p\rho_{abc}^{\text{GHZ}}+(1-p)\rho_{abc}^{\text{Classic}}, \tag{18}$$

其中, p为信道态中包含ρ_{abc}^{GHZ}的概率, $(1-p)$为$\rho_{abc}^{\text{Classic}}$的掺杂概率. 那么, Charlie所具有的真实控制力(Real Control Power, RCP)应为RCP $=\frac{1}{3}p$.

RCP更准确可靠地给出了以经典-混合量子资源为信道时Charlie所具有的真实控制力, 为了进一步完善协议安全性的认证方案, 我们设计了基于黑盒模型的受控CNOT-QGT的DI验证方案. DI验证方案基于量子非定域性, 量子非定域性可以通过对Bell不等式及其变体形式的违背来度量[32], 由于此过程仅依赖于实验中各观测结果之间的统计相关性, 因此可以在设备完全不受信的情况下完成认证. 并且, 这样的违背无法以经典的方式解释, 故DI验证结果可以作为区分量子信息处理和经典信息处理的特征之一[42,44]. 结合RCP和DI验证结果, 能够更可靠地检验受控CNOT-QGT执行过程的安全性.

3.1 DI验证场景

假设输入态均为纯态. 基于黑盒模型及标准受控CNOT-QGT协议, 我们提出如下DI验证场景.

(1) Alice, Bob和Charlie分别持有一个黑盒设备, 不假设任何关于设备的先验情况.

(2) Charlie的黑盒从$\boldsymbol{c}_l \in \{\boldsymbol{c}_0, \boldsymbol{c}_1\}$中接收其一作为测量纠缠粒子$c$的测量方向, 并在测量后输出$\gamma \in \{0,1\}$. 根据第2.1节, Charlie测量后使得Alice和Bob以两方最大纠缠态执行标准CNOT-QGT过程, 因此我们检验当Charlie的两种测量设置分别为$\boldsymbol{c}_0 = (1,0,0)$和$\boldsymbol{c}_1 = (0,-1,0)$时执行DI验证的结果. Charlie测量后得到结果γ的概率为$P_c(\gamma|l) = \frac{1}{2}$.

(3) Alice (Bob)随机向黑盒输入$\boldsymbol{A}_0$或$\boldsymbol{A}_1$ ($\boldsymbol{B}_0$或$\boldsymbol{B}_1$)作为qubit A (B)的输入态. 在DI验证中, 挑选初始输入组合$\{\boldsymbol{A}_0, \boldsymbol{B}_0\}$及$\{\boldsymbol{A}_1, \boldsymbol{B}_1\}$构成执行CNOT-QGT的两粒子体系AB的输入态$\boldsymbol{m}_j \in \{\boldsymbol{m}_0, \boldsymbol{m}_1\}$, 则对应的目标态为$\boldsymbol{n}_j \in \{\boldsymbol{n}_0, \boldsymbol{n}_1\}$.

注入输入态后, Alice (Bob)的黑盒执行局域CNOT门U_a^A (U_B^b), 并以$M_{a,z}$ ($M_{b,x}$)测量纠缠粒子a (b), 输出$\tilde{s}_0$ ($\tilde{s}_1$) $\in \{0,1\}$. 为了适应DI验证框架, 对$(\tilde{s}_0, \tilde{s}_1)$作如下映射:

$$\alpha = 2\tilde{s}_j - 1, j \in \{0,1\}. \tag{19}$$

(4) 完成(3)后, Alice和Bob随机输入关于qubit A和B的局域测量设置. 挑选$\{z_{A_0}, z_{B_0}\}$及$\{z_{A_1}, z_{B_1}\}$构成对系统AB的联合测量基$\boldsymbol{z}_k \in \{\boldsymbol{z}_0, \boldsymbol{z}_1\}$. 测量完成后, Alice和Bob的黑盒输出$(c_0, c_1)$ $(c_0, c_1 \in \{-1, +1\})$, 我们将其进一步编码为$\beta$[42]:

$$\beta = \begin{cases} +1, & c_0, c_1 = +1, \\ -1, & \text{others}. \end{cases} \tag{20}$$

(5) 每一方在完成几轮相同的实验后同时公开自己的输入和测量结果.

图图 1展示了DI验证方案的执行过程. 由于每个黑盒里发生的事件均不影响其他空间分离的黑盒中发生的事件[45], 即黑盒之间无主动补偿, 因此该DI验证场景满足无信号原则[64]; 各黑盒的输出均独立地取决于各自的输入, 因此该DI验证场景满足自由意志假设[65].

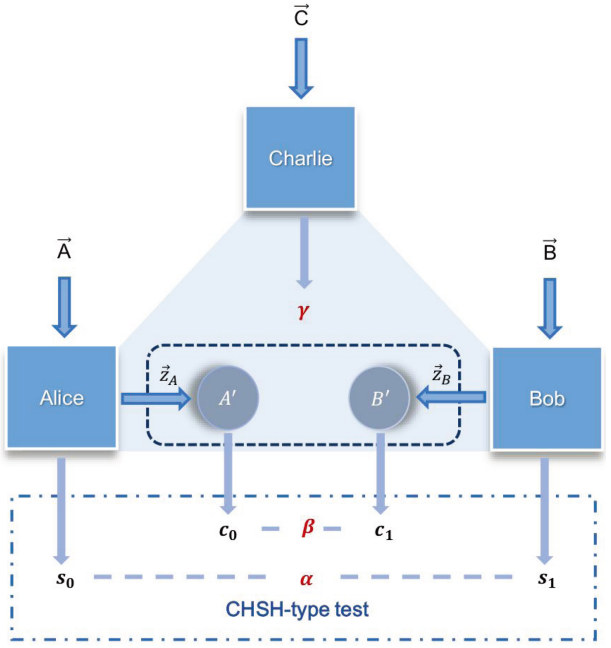

图 1 (网络版彩图)受控非局域CNOT量子门的DI验证方案. 此方案中, $\boldsymbol{C}$和γ分别代表Charlie黑盒的输入和输出. $\boldsymbol{A}$ ($\boldsymbol{B}$), s_0 (s_1)分别代表Alice (Bob)黑盒的初始输入、完成门传输基本过程后的输出. 随后, Alice (Bob)的黑盒接收$\boldsymbol{Z}_A$ ($\boldsymbol{Z}_B$)为输入, 并输出c_0 (c_1). 在Alice和Bob间的CHSH-type测试中, s_0和s_1被重新编码为α, c_0和c_1被重新编码为β

Figure 1 (Color online) DI verification scheme for controlled nonlocal CNOT quantum gate. In this scheme, $\boldsymbol{C}$ and γ represent the input and output of Charlie's black box respectively. $\boldsymbol{A}$ and s_0 ($\boldsymbol{B}$ and s_1) represent the initial input and output of Alice's (Bob's) black box after the basic process of gate transmission, respectively. Subsequently, Alice's (Bob's) black box receives $\boldsymbol{Z}_A(\boldsymbol{Z}_B)$ as input and outputs c_0 (c_1). In the CHSH-type test between Alice and Bob's black boxes, s_0 and s_1 are recoded as α, c_0 and c_1 are recoded as β.

3.2 基于DI场景的Svetlichny-type不等式

针对第3.1节的DI验证场景, 我们首先以Svetlichny不等式[66]进行检验, 计算结果表明不论基于$\rho_{abc}^{\text{Classic}}$还是$\rho_{abc}^{\text{GHZ}}$执行该DI验证方案得到的Svetlichny值均为2. 为了解决这一问题, 我们提出了一个Svetlichny-type函数, 其值为Alice与Bob之间基于(γ, l)的CHSH-type测试值的加权平均, 权重为$P_c(\gamma|l) = \frac{1}{2}$,

$$\begin{aligned} S =& P_C(\gamma = +1|l = 0)\text{CHSH}_{\gamma=+1,l=0} \\ &- P_C(\gamma = -1|l = 0)\text{CHSH}'_{\gamma=-1,l=0} \\ &+ P_C(\gamma = +1|l = 1)\text{CHSH}_{\gamma=+1,l=1} \\ &- P_C(\gamma = -1|l = 1)\text{CHSH}'_{\gamma=-1,l=1}. \end{aligned} \tag{21}$$

$\mathrm{CHSH}_{\gamma=+1,l}$及其对称形式$\mathrm{CHSH}'_{\gamma=-1,l}$为对应于$(\gamma, l)$的CHSH-type 测试, 具体的表达式为

$$\begin{aligned}\mathrm{CHSH}_{\gamma=+1,l} &= E_{00}^{(+1)l} + E_{01}^{(+1)l} + E_{10}^{(+1)l} - E_{11}^{(+1)l},\\ \mathrm{CHSH}'_{\gamma=-1,l} &= -E_{00}^{(-1)l} - E_{01}^{(-1)l} + E_{10}^{(-1)l} - E_{11}^{(-1)l},\end{aligned} \quad (22)$$

其中, 期望值$E_{jk}^{\gamma l} = P(\alpha = \beta|\boldsymbol{n}_j, \boldsymbol{z}_k, \boldsymbol{c}_l, \gamma) - P(\alpha \neq \beta|\boldsymbol{n}_j, \boldsymbol{z}_k, \boldsymbol{c}_l, \gamma)$.

在遍历所有Alice和Bob的输入设置的情况下, 若信道为完美的GHZ态, 则Svetlichny-type函数最大值S-type$_{\mathrm{GHZ}} \approx 4.494$; 若信道为完全的$\rho_{abc}^{\mathrm{Classic}}$, 则Svetlichny-type 函数最大值为S-type$_{\mathrm{Classic}} \approx 4.265$.

由图图 2可知, 在信道态ρ下, Svetlichny-type不等式的值S-type随GHZ态的含量p单调递增, 且Charlie对受控非局域CNOT门的真实控制力RCP与p呈正比. 当$p = 1$时, 信道为完美的GHZ态, 此时RCP与标准协议下的理想控制力$\frac{1}{3}$相等; $p = 0$时, 信道为完全的经典-量子混合态$\rho_{abc}^{\mathrm{Classic}}$, 此时控制方的真实控制力应为0.

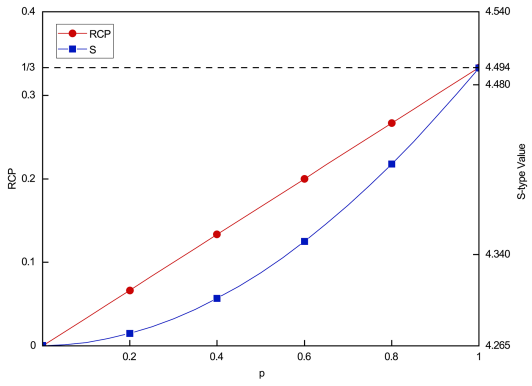

图 2 (网络版彩图)真实控制力RCP及Svetlichny-type函数值S-type. 以方块、实心圆标记的两条线分别代表RCP及S-type. 根据式(16), 虚线表示信道为GHZ态时Charlie所具有的理想控制力

Figure 2 (Color online) Real control power RCP and Svetlichny-type function value S-type. The two lines marked by square and solid circle respectively represent RCP and S-type. The dotted line represents the ideal control power that Charlie has when the GHZ state is quantum channel according to eq. (16).

4 结论

本文提出了一个基于黑盒模型的受控CNOT-QGT设备无关验证方案及对应的Svetlichny-type不等式, 并分析了控制方的真实控制力. 根据该DI验证方案, DI验证结果的获取仅仅依赖于设备的输入及输出统计数据, 而没有任何针对于设备的假设, 因此能够在不可信设备中检验受控非局域门执行过程中纠缠资源的利用情况, 且这一验证过程具备一定的防窃听能力. 在Svetlichny不等式不适用的情况下, 本文提出的Svetlichny-type不等式能够区分受控非局域CNOT门的执行是基于经典-量子混合资源还是真多方量子纠缠资源, 理论上保证了该量子过程的安全性.

针对于信道资源的DI验证方案通常以Bell不等式及其各类变体形式作为检验工具. 更实际地, 这些信道资源最终需要应用在执行具体的量子信息处理过程、实现具体的功能之中. 然而, 根据目前的研究成果, 我们发现检验信道的DI操作手段及不等式并不一定能够直接迁移到检验基于信道的功能实现中. 本文所提出的DI验证方案及Svetlichny-type不等式仍然从量子非局域性的角度出发, 或许未来能够在检验量子非局域性发挥作用. 我们的DI验证方案是设备无关框架应用于验证多方量子过程的一种有效扩展, 是未来分布式量子计算网络安全性检验的有效工具.

参考文献

1 Steane A. Quantum computing. Rep Prog Phys, 1998, 61: 117–173
2 Nielsen M A, Chuang I L. Quantum Computation and Quantum Information: 10th Anniversary Edition. Cambridge: Cambridge University Press, 2010. 12–60
3 Moore C, Nilsson M. Parallel quantum computation and quantum codes. SIAM J Comput, 2001, 31: 799–815
4 Wang S B, Dou M H, Wu Y C, et al. Research progress of distributed quantum computing (in Chinese). Chin J Quantum Electron, 2024, 41: 1–25 [王升斌, 窦猛汉, 吴玉椿, 等. 分布式量子计算研究进展. 量子电子学报, 2024, 41: 1–25]
5 Deutsch D, Jozsa R. Rapid solution of problems by quantum computation. Proc R Soc Lond A, 1992, 439: 553–558
6 Huang H L, Xu X Y, Guo C, et al. Near-term quantum computing techniques: Variational quantum algorithms, error mitigation, circuit compila-

tion, benchmarking and classical simulation. Sci China-Phys Mech Astron, 2023, 66: 250302
7 Li Z H, Yu G F, Wang Y X, et al. Experimental demonstration of deterministic quantum search algorithms on a programmable silicon photonic chip. Sci China-Phys Mech Astron, 2023, 66: 290311
8 Zheng Q, Yu M, Zhu P, et al. Solving the subset sum problem by the quantum Ising model with variational quantum optimization based on conditional values at risk. Sci China-Phys Mech Astron, 2024, 67: 280311
9 Hou X, Zhou G, Li Q, et al. A duplication-free quantum neural network for universal approximation. Sci China-Phys Mech Astron, 2023, 66: 270362
10 Song Y, Wu Y, Wu S, et al. A quantum federated learning framework for classical clients. Sci China-Phys Mech Astron, 2024, 67: 250311
11 Li L, Li J, Song Y, et al. An efficient quantum proactive incremental learning algorithm. Sci China-Phys Mech Astron, 2025, 68: 210313
12 Young C B, Safari A, Huft P, et al. An architecture for quantum networking of neutral atom processors. Appl Phys B, 2022, 128: 151
13 Covey J P, Weinfurter H, Bernien H. Quantum networks with neutral atom processing nodes. npj Quantum Inf, 2023, 9: 90
14 Huang H L, Wu D, Fan D, et al. Superconducting quantum computing: A review. Sci China Inf Sci, 2020, 63: 180501
15 Castelvecchi D. IBM releases first-ever 1000-qubit quantum chip. Nature, 2023, 624: 238
16 Zeng Y, Dong Z, Wang H, et al. A general quantum minimum searching algorithm with high success rate and its implementation. Sci China-Phys Mech Astron, 2023, 66: 240315
17 Zhang X, Li H O, Cao G, et al. Semiconductor quantum computation. Natl Sci Rev, 2019, 6: 32–54
18 García de Arquer F P, Talapin D V, Klimov V I, et al. Semiconductor quantum dots: Technological progress and future challenges. Science, 2021, 373: eaaz8541
19 Qiao M, Cai Z, Wang Y, et al. Tunable quantum simulation of spin models with a two-dimensional ion crystal. Nat Phys, 2024, 20: 623–630
20 O'Brien J L, Furusawa A, Vučković J. Photonic quantum technologies. Nat Photon, 2009, 3: 687–695
21 Wang J, Sciarrino F, Laing A, et al. Integrated photonic quantum technologies. Nat Photon, 2020, 14: 273–284
22 Breuckmann N P, Eberhardt J N. Quantum low-density parity-check codes. PRX Quantum, 2021, 2: 040101
23 Bravyi S, Cross A W, Gambetta J M, et al. High-threshold and low-overhead fault-tolerant quantum memory. Nature, 2024, 627: 778–782
24 de Leon N P, Itoh K M, Kim D, et al. Materials challenges and opportunities for quantum computing hardware. Science, 2021, 372: eabb2823
25 Cacciapuoti A S, Caleffi M, Tafuri F, et al. Quantum internet: Networking challenges in distributed quantum computing. IEEE Netw, 2019, 34: 137–143
26 Caleffi M, Amoretti M, Ferrari D, et al. Distributed quantum computing: A survey. Comput Netws, 2024, 254: 110672
27 Avron J, Casper O, Rozen I. Quantum advantage and noise reduction in distributed quantum computing. Phys Rev A, 2021, 104: 052404
28 Gottesman D, Chuang I L. Demonstrating the viability of universal quantum computation using teleportation and single-qubit operations. Nature, 1999, 402: 390–393
29 Huang Y F, Ren X F, Zhang Y S, et al. Experimental teleportation of a quantum controlled-NOT gate. Phys Rev Lett, 2004, 93: 240501
30 Chou K S, Blumoff J Z, Wang C S, et al. Deterministic teleportation of a quantum gate between two logical qubits. Nature, 2018, 561: 368–373
31 Liu X, Hu X M, Zhu T X, et al. Nonlocal photonic quantum gates over 7.0 km. Nat Commun, 2024, 15: 8529
32 Brunner N, Cavalcanti D, Pironio S, et al. Bell nonlocality. Rev Mod Phys, 2014, 86: 419–478
33 Gong N F, Wang T J, Ghose S. Control power of a high-dimensional controlled nonlocal quantum computation. Phys Rev A, 2021, 103: 052601
34 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
35 Hu X M, Huang C X, Sheng Y B, et al. Long-distance entanglement purification for quantum communication. Phys Rev Lett, 2021, 126: 010503
36 Schlosshauer M. Quantum decoherence. Phys Rep, 2019, 831: 1–57
37 Yan P S, Zhou L, Zhong W, et al. Advances in quantum entanglement purification. Sci China-Phys Mech Astron, 2023, 66: 250301
38 Massar S, Bacon D, Cerf N J, et al. Classical simulation of quantum entanglement without local hidden variables. Phys Rev A, 2001, 63: 052305
39 Fu J, Si Z, Tang S, et al. Classical simulation of quantum entanglement using optical transverse modes in multimode waveguides. Phys Rev A, 2004, 70: 042313
40 Georgescu I M, Ashhab S, Nori F. Quantum simulation. Rev Mod Phys, 2014, 86: 153–185
41 Gisin N. Nonlocality criteria for quantum teleportation. Phys Lett A, 1996, 210: 157–159
42 Wang Z Q, Wang T J. Verification of quantum-gate teleportation based on Bell nonlocality in a black-box scenario. Phys Rev A, 2023, 108: 012434
43 Popescu S. Bell's inequalities versus teleportation: What is nonlocality? Phys Rev Lett, 1994, 72: 797–799
44 Ho M, Bancal J D, Scarani V. Device-independent certification of the teleportation of a qubit. Phys Rev A, 2013, 88: 052318

45 Clifton R, Pope D. On the nonlocality of the quantum channel in the standard teleportation protocol. Phys Lett A, 2001, 292: 1–11
46 Chiribella G, Yuan X. Bridging the gap between general probabilistic theories and the device-independent framework for nonlocality and contextuality. Inf Comput, 2016, 250: 15–49
47 Chen G, Zhang W H, Yin P, et al. Device-independent characterization of entanglement based on Bell nonlocality. Fundam Res, 2021, 1: 27–42
48 Einstein A, Podolsky B, Rosen N. Can quantum-mechanical description of physical reality be considered complete? Phys Rev, 1935, 47: 777–780
49 Bell J S. On the Einstein Podolsky Rosen paradox. Phys Phys Fiz, 1964, 1: 195–200
50 Pironio S, Scarani V, Vidick T. Focus on device independent quantum information. New J Phys, 2016, 18: 100202
51 Acín A, Gisin N, Masanes L. From Bell's theorem to secure quantum key distribution. Phys Rev Lett, 2006, 97: 120405
52 Holz T, Kampermann H, Bruß D. Genuine multipartite Bell inequality for device-independent conference key agreement. Phys Rev Res, 2020, 2: 023251
53 Shen A, Cao X Y, Wang Y, et al. Experimental quantum secret sharing based on phase encoding of coherent states. Sci China-Phys Mech Astron, 2023, 66: 260311
54 Li H W, Hao C P, Chen Z J, et al. Security of quantum key distribution with virtual mutually unbiased bases. Sci China-Phys Mech Astron, 2024, 67: 270313
55 Huang C, Chen Y, Luo T, et al. A cost-efficient quantum access network with qubit-based synchronization. Sci China-Phys Mech Astron, 2024, 67: 240312
56 Lv M Y, Hu X M, Gong N F, et al. Demonstration of controlled high-dimensional quantum teleportation. Sci China-Phys Mech Astron, 2024, 67: 230311
57 Mannalath V, Pathak A. Multiparty entanglement routing in quantum networks. Phys Rev A, 2023, 108: 062614
58 Gangopadhyay S, Wang T, Mashatan A, et al. Controlled quantum teleportation in the presence of an adversary. Phys Rev A, 2022, 106: 052433
59 Ljung L. Black-box models from input-output measurements. In: Proceedings of the 18th IEEE Instrumentation and Measurement Technology Conference. Budapest: IEEE, 2001. 138–146
60 Greenberger D M, Horne M A, Shimony A, et al. Bell's theorem without inequalities. Am J Phys, 1990, 58: 1131–1143
61 Jakóbczyk L, Siennicki M. Geometry of Bloch vectors in two-qubit system. Phys Lett A, 2001, 286: 383–390
62 Bertlmann R A, Krammer P. Bloch vectors for qudits. J Phys A-Math Theor, 2008, 41: 235303
63 Barasiński A, Černoch A, Lemr K. Demonstration of controlled quantum teleportation for discrete variables on linear optical devices. Phys Rev Lett, 2019, 122: 170501
64 Masanes L, Acin A, Gisin N. General properties of nonsignaling theories. Phys Rev A, 2006, 73: 012112
65 Gebhart V, Pezzè L, Smerzi A. Genuine multipartite nonlocality with causal-diagram postselection. Phys Rev Lett, 2021, 127: 140401
66 Svetlichny G. Distinguishing three-body from two-body nonseparability by a Bell-type inequality. Phys Rev D, 1987, 35: 3066–3069

附录A $SU(4)$生成元及量子门系统的Bloch向量表示

对于N维量子系统, 其密度矩阵ρ由(N^2-1)维的Bloch向量$\boldsymbol{m}=(m_1,...,m_k)$表示为

$$\rho=\frac{1}{N}\mathbb{I}_N+\frac{1}{2}(\boldsymbol{m}\cdot\boldsymbol{\lambda})=\frac{1}{N}\mathbb{I}_N+\frac{1}{2}\sum_{k=1}^{N^2-1}m_k\cdot\lambda_k, \tag{1}$$

其中, $\boldsymbol{\lambda}=(\lambda_1,...,\lambda_{N^2-1})$为代数$SU(N)$的生成元. 当$N=4$时, 15维Bloch向量满足$\|\boldsymbol{m}\|_2=\frac{3}{2}$ [62], $SU(4)$群生成元分别为

$$\lambda_1=\begin{pmatrix}0&1&0&0\\1&0&0&0\\0&0&0&0\\0&0&0&0\end{pmatrix},\ \lambda_2=\begin{pmatrix}0&-\mathrm{i}&0&0\\\mathrm{i}&0&0&0\\0&0&0&0\\0&0&0&0\end{pmatrix},\ \lambda_3=\begin{pmatrix}1&0&0&0\\0&-1&0&0\\0&0&0&0\\0&0&0&0\end{pmatrix},\ \lambda_4=\begin{pmatrix}0&0&1&0\\0&0&0&0\\1&0&0&0\\0&0&0&0\end{pmatrix},\ \lambda_5=\begin{pmatrix}0&0&-\mathrm{i}&0\\0&0&0&0\\\mathrm{i}&0&0&0\\0&0&0&0\end{pmatrix},$$

$$\lambda_6=\begin{pmatrix}0&0&0&0\\0&0&1&0\\0&1&0&0\\0&0&0&0\end{pmatrix},\ \lambda_7=\begin{pmatrix}0&0&0&0\\0&0&-\mathrm{i}&0\\0&\mathrm{i}&0&0\\0&0&0&0\end{pmatrix},\ \lambda_8=\frac{1}{\sqrt{3}}\begin{pmatrix}1&0&0&0\\0&1&0&0\\0&0&-2&0\\0&0&0&0\end{pmatrix},\ \lambda_9=\begin{pmatrix}0&0&0&1\\0&0&0&0\\0&0&0&0\\1&0&0&0\end{pmatrix},\ \lambda_{10}=\begin{pmatrix}0&0&0&-\mathrm{i}\\0&0&0&0\\0&0&0&0\\\mathrm{i}&0&0&0\end{pmatrix},$$
$$\lambda_{11}=\begin{pmatrix}0&0&0&0\\0&0&0&1\\0&0&0&0\\0&1&0&0\end{pmatrix},\ \lambda_{12}=\begin{pmatrix}0&0&0&0\\0&0&0&-\mathrm{i}\\0&0&0&0\\0&\mathrm{i}&0&0\end{pmatrix},\ \lambda_{13}=\begin{pmatrix}0&0&0&0\\0&0&0&0\\0&0&0&1\\0&0&1&0\end{pmatrix},\ \lambda_{14}=\begin{pmatrix}0&0&0&0\\0&0&0&0\\0&0&0&-\mathrm{i}\\0&0&\mathrm{i}&0\end{pmatrix},\ \lambda_{15}=\frac{1}{\sqrt{6}}\begin{pmatrix}1&0&0&0\\0&1&0&0\\0&0&1&0\\0&0&0&-3\end{pmatrix}. \tag{2}$$

根据第2.1节, 初始量子门系统$\rho_{AB}^{\mathrm{initial}}$为2-qubit可分量子系统, 其对应的15维Bloch向量$\boldsymbol{m}$可以由ρ_A, ρ_B所对应的3维Bloch向量$\boldsymbol{A}=(A_1,A_2,A_3)$, $\boldsymbol{B}=(B_1,B_2,B_3)$及$SU(4)$生成元计算得到. 根据文献[61], $\boldsymbol{m}$的各分量$m_k(k=1,...,15)$分别为

$$\begin{aligned}
&m_1=\frac{B_1}{2}(1+A_3),\ m_2=\frac{B_2}{2}(1+A_3),\ m_3=\frac{B_3}{2}(1+A_3),\ m_4=\frac{A_1}{2}(1+B_3),\ m_5=\frac{A_2}{2}(1+B_3),\\
&m_6=\frac{1}{2}(A_1B_1+A_2B_2),\ m_7=\frac{1}{2}(A_2B_1-A_1B_2),\ m_8=\frac{1}{2\sqrt{3}}(A_3B_3+2A_3-B_3),\ m_9=\frac{1}{2}(A_1B_1-B_3),\\
&m_{10}=\frac{1}{2}(A_1B_2+A_2B_1),\ m_{11}=\frac{A_1}{2}(1-B_3),\ m_{12}=\frac{A_2}{2}(1-B_3),\ m_{13}=\frac{B_1}{2}(1-A_3),\ m_{14}=\frac{B_2}{2}(1-A_3),\\
&m_{15}=\frac{1}{\sqrt{6}}(A_3+B_3-A_3B_3).
\end{aligned} \tag{3}$$

设目标系统$\rho_{AB}^{\mathrm{CNOT}}$对应的15维Bloch向量为$\boldsymbol{n}$, 经计算得到其分量$n_k(k=1,...15)$分别为

$$\begin{aligned}
&n_1=\frac{B_1}{2}(1+A_3),\ n_2=\frac{B_2}{2}(1+A_3),\ n_3=\frac{B_3}{2}(1+A_3),\ n_4=\frac{1}{2}(A_1B_1-A_2B_2),\ n_5=\frac{1}{2}(A_1B_2+A_2B_1),\\
&n_6=\frac{A_1}{2}(1-B_3),\ n_7=\frac{A_2}{2}(1-B_3),\ n_8=\frac{1}{2\sqrt{3}}(2A_3+B_3-A_3B_3),\ n_9=\frac{A_1}{2}(1+B_3),\ n_{10}=\frac{A_2}{2}(1+B_3),\\
&n_{11}=\frac{1}{2}(A_1B_1+A_2B_2),\ n_{12}=\frac{1}{2}(A_2B_1-A_1B_2),\ n_{13}=\frac{B_1}{2}(1-A_3),\ n_{14}=\frac{B_2}{2}(A_3-1),\ n_{15}=\frac{1}{\sqrt{6}}(A_3-B_3+A_3B_3).
\end{aligned} \tag{4}$$

附录B 标准受控CNOT-QGT协议中的恢复性操作

设Alice和Bob对量子比特A和B执行的局域幺正操作分别为R_A, R_B, 则对联合系统AB的幺正操作为$\tilde{R}_{\tilde{s}_0\tilde{s}_1\gamma}=R_A\otimes R_B$, 其中$R_A,R_B\in\{I_2,\delta_x,\delta_y,\delta_z\}$. 于是, 有$\tilde{R}_{\tilde{s}_0\tilde{s}_1\gamma}\rho_{AB}^{\tilde{s}_0\tilde{s}_1\gamma}\tilde{R}_{\tilde{s}_0\tilde{s}_1\gamma}^{\dagger}=(R_A\otimes R_B)\rho_{AB}^{\tilde{s}_0\tilde{s}_1\gamma}(R_A\otimes R_B)^{\dagger}$, 其中$\tilde{R}_{\tilde{s}_0\tilde{s}_1\gamma}$以及幺正操作之间的等价关系分别为

$$\begin{aligned}
&\tilde{R}_{00(+1)}=I_2\otimes I_2,\ \tilde{R}_{01(+1)}=\delta_z\otimes I_2,\ \tilde{R}_{10(+1)}=I_2\otimes\delta_x,\ \tilde{R}_{11(+1)}=\delta_z\otimes\delta_x,\\
&\tilde{R}_{00(-1)}=\delta_z\otimes I_2,\ \tilde{R}_{01(-1)}=I_2\otimes I_2,\ \tilde{R}_{10(-1)}=\delta_z\otimes\delta_x,\ \tilde{R}_{11(-1)}=I_2\otimes\delta_x.\\
&\tilde{R}_{00(+1)}=\tilde{R}_{01(-1)},\ \tilde{R}_{01(+1)}=\tilde{R}_{00(-1)},\ \tilde{R}_{10(+1)}=\tilde{R}_{11(-1)},\ \tilde{R}_{11(+1)}=\tilde{R}_{10(-1)}.
\end{aligned} \tag{1}$$

在第2.1节中, $R_{\tilde{s}_0\tilde{s}_1\gamma}$作用于$\rho_{AB}^{\tilde{s}_0\tilde{s}_1\gamma}$所对应的15维Bloch向量. 根据测量结果$(\tilde{s}_0\tilde{s}_1\gamma)$将$\tilde{R}_{\tilde{s}_0\tilde{s}_1\gamma}$转换为$R_{\tilde{s}_0\tilde{s}_1\gamma}$, 其中部分表示为

$$R_{00(+1)}=\begin{pmatrix}
1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1
\end{pmatrix},R_{01(+1)}=\begin{pmatrix}
1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&-1&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&-1&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&-1&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&-1&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&-1&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&-1&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&-1&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&-1&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&-1&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1
\end{pmatrix},$$

$$R_{10(+1)}=\begin{pmatrix}
1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&-1&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&-1&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0\\
0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0\\
0&0&0&0&0&0&\frac{1}{3}&0&0&0&0&0&0&0&\frac{2\sqrt{2}}{3}&0\\
0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0\\
0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&-1&0&0&0\\
0&0&0&0&0&0&\frac{2\sqrt{2}}{3}&0&0&0&0&0&0&0&-\frac{1}{3}&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1
\end{pmatrix},$$

$$R_{11(+1)}=\begin{pmatrix}
1&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&-1&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&-1&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&-1&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&-1&0&0\\
0&0&0&0&0&0&0&0&-1&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&-1&0&0&0&0\\
0&0&0&0&0&0&0&\frac{1}{3}&0&0&0&0&0&\frac{2\sqrt{2}}{3}\\
0&0&0&0&0&-1&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&-1&0&0&0&0&0&0&0\\
0&0&0&-1&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&-1&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&1&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&-1&0\\
0&0&0&0&0&0&0&\frac{2\sqrt{2}}{3}&0&0&0&0&0&-\frac{1}{3}
\end{pmatrix}.$$

$R_{\tilde{s}_0\tilde{s}_1\gamma}$间的等价关系同样为

$$R_{00(+1)}=R_{01(-1)},\quad R_{01(+1)}=R_{00(-1)},\quad R_{10(+1)}=R_{11(-1)},\quad R_{11(+1)}=R_{10(-1)}. \tag{2}$$

Device-independent verification of controlled non-local CNOT quantum gate

LI YiNing, GONG NengFei, TIAN YueHan & WANG TieJun*

School of Science, Beijing University of Posts and Telecommunications, Beijing 100876, China
**Corresponding author (email: wangtiejun@bupt.edu.cn)*

Controlled non-local quantum gate operations reveal the cooperative and supervisory relationships of the controller and the non-local gate operators in a quantum networks, which is an essential feature for building multi-party quantum computing networks, and their security relies on quantum entanglement resources. To understand the behavior of vendors who substitute quantum entanglement resources with classical-quantum hybrid resources, this paper proposes a device-independent verification scheme for controlled non-local CNOT quantum gates. Moreover, it formulates a Svetlichny-type inequality to conduct an effective verification of the utilization of entanglement resources in nonlocal gate operations, particularly in instances where the Svetlichny inequality is not applicable. Our scheme offers a theoretical foundation for constructing secure distributed quantum computing networks in the future.

distributed quantum computing, controlled non-local quantum gate, device-independent verification

PACS: 03.67.-a, 03.67.Ac, 03.67.Dd, 03.67.Lx

doi: 10.1360/SSPMA-2024-0575