

基于十量子比特团簇态的多量子双向链式 受控量子隐形传态

范萍^{1,2}, 杨国旺¹

(1. 华东交通大学信息工程学院, 南昌 330013; 2. 闽江学院计算机与控制工程学院, 福州 350108)

摘要: 为了在多参与者之间实现链式量子通信, 采用十量子比特团簇态作为量子信道 (quantum channel, QC), 提出一种在4方之间进行多量子比特初始态的双向链式受控量子隐形传态 (bidirectional-chain controlled quantum teleportation, BCCQT) 协议. 在通信参与者 Alice、Bob、Charlie 和通信控制者 David 之间进行量子通信, 并且在量子通信过程中的安全性由控制者的权限和 QC 的纠缠特性予以保证的情况下, 经过多量子比特初始态的复单转换、顺序通信、逆序通信、单重塑和复重塑等一系列复杂的过程和方法来重塑多量子比特初始态, 实现了链式量子通信. 结果证明该协议是可行的, 同时, 在此基础上对 $n+1$ 方量子隐形传态和 QC 之间的关系提出了猜想.

关键词: 双向链式量子隐形传态; 十量子比特团簇态; 多量子比特初始态; 量子态转换; H 门操作; 幺正操作 (unitary operation, UO); 重塑量子态

中图分类号: U 461; TP 308

文献标志码: A

文章编号: 0254-0037(2023)06-0684-10

doi: 10.11936/bjtu2022110010

Bidirectional-chain Controlled Quantum Teleportation of Multiple Quantum Based on a Ten-qubit Cluster State

FAN Ping^{1,2}, YANG Guowang¹

(1. School of Information Engineering, East China Jiaotong University, Nanchang 330013, China;

2. College of Computer and Control Engineering, Minjiang University, Fuzhou 350108, China)

Abstract: To realize chained quantum communication between multiple actors, a bidirectional-chain controlled quantum teleportation (BCCQT) protocol that provided multi-qubit initial states between four parties was proposed using the ten-qubit cluster state as the quantum channel (QC). Quantum communication was carried out between communication participants Alice, Bob, Charlie and communication controller David, and the security of quantum communication process was guaranteed by the authority of the controller and the entanglement characteristics of QC. After a series of complex processes and methods such as complex single transformation of multi-qubit states, sequential communication, reverse communication, single remodeling and complex remodeling, the initial state of multi-qubit was reconstructed, and the chain quantum communication was finally achieved. Results show that the protocol is feasible. Meanwhile, based on this, a conjecture about the relationship between $n+1$ square quantum teleportation and QC was proposed.

Key words: bidirectional-chain quantum teleportation; ten-qubit cluster state; multi-qubit initial states; quantum state conversion; H gate operation; unitary operation (UO); reshape quantum state

近年来,随着各种信息安全问题的层出不穷,传统的加密算法保护能力日渐趋弱,量子通信^[1]作为保密的通信技术应运而生,量子通信基于量子力学的测不准原理、不可克隆原理和纠缠态^[2]原理可以确保信息的传输安全.目前,在量子通信方面主要有两大应用分支:一是量子密钥分发^[3],二是量子隐形传态.本文研究的量子隐形传态属于量子通信的范畴,是未来实现全球量子通信网络的核心要素,其基础原理是发送方和接收方之间在非局域的环境中共享一个量子信道(quantum channel, QC)来进行初始量子态的重塑.基于量子通信技术的高速发展,各种形式的量子隐形传态协议也纷纷被提出,包括简单的标准量子隐形传态协议^[4]、双向量子隐形传态(bidirectional quantum teleportation, BQT)协议^[5]、循环量子隐形传态协议^[6]以及更加复杂的量子隐形传态协议^[7]等.量子隐形传态协议主要通过3个方面展开:一是QC的多样性;二是量子隐形传态方式的复杂性;三是拟重塑的量子态数量级.本文协议不考虑在量子比特纠缠态制备等实验下的真实情形,例如:在关联噪声^[8]影响下的QC只会发生部分纠缠,QC自身的退相干导致保真度下降等诸多不利因素.基于QC的多样性研究,可分为两量子比特Bell纠缠态^[9-10]、三量子比特W纠缠态或GHZ(Greenberger-Horne-Zeilinger)纠缠态^[11-12]、四量子比特G纠缠态^[13]以及多量子比特团簇态^[14],如四量子比特团簇态^[15]、五量子比特团簇态^[16-18]、八量子比特团簇态^[19]以及这些状态衍生出来的各种多量子比特初始态^[20-22].量子隐形传态方式的复杂性可以从以下2个方面分析:第一,从量子隐形传态重塑方式角度分析,可分为信道中的通信双方中一方只负责重塑另一方的量子态的单向量子隐形传态、信道中通信双方均可以重塑对方量子态的BQT^[23]、信道中多方之间进行循环重塑量子态的循环量子隐形传态以及空间立体式多方量子隐形传态等情况.第二,从量子态^[24]所受约束的角度分析,根据不同情况可分为在局域环境下通信多方进行量子态重塑、信道中通信一方隔一段时间分发量子比特的连续分发约束、通信方需要达到一定条件才可以对量子态重塑的催化^[25]约束、需要重塑的量子态分为不同权限或者优先级进行的分层^[13]约束、通信过程中有第三方帮助重塑量子态的可控^[26]约束、通信多方各自重塑的量子态数量一致的对称约束和通信多方各自重塑的

量子态数量不一致的非对称^[27-28]约束等.拟重塑的量子态数量级可分为单量子比特数量级、双量子比特数量级以及复杂的多量子比特数量级等.

传统的BQT是同时且双向的通信过程,本文协议的通信过程是链式双向传输,将传输流程化为顺逆序通信,在宏观上是同时进行的,在微观具体测量步骤上是分布式的,这并不影响最后多量子比特初始态的重塑,反而使原本复杂的过程更加简洁.

本协议流程不同于以往的BQT流程,其灵感源于双向链表.双向链表结构灵活,分为3个部分:首结点、尾结点和指针.本文将协议流程和数据结构双向链表进行对比,以便于对量子通信流程进行理解.协议分为参与者和控制者,相当于链表中的结点和指针.参与者既是发送方,同时也是接收方,从首结点顺序通信到尾结点,再转换方向进行逆序通信,从而形成环路.控制者充当指针的作用,在结点(参与者)之间进行经典信息告知,并且控制者的数量可以增加量子通信的安全性.

目前,研究表明量子隐形传态中重塑的量子态处在有限的数量级.本文提出一种多量子比特初始态的双向链式受控量子隐形传态(bidirectional-chain controlled quantum teleportation, BCCQT)协议,采用一个十量子比特团簇态作为QC,在Alice、Bob、Charlie和David之间进行多量子比特初始态的重塑,最终完成了量子安全通信,协议信息量多、层级高,过程比较复杂.

1 总流程及准备

假设有4方要实现量子通信,其中分为参与者和控制者,参与者是Alice、Bob、Charlie,控制者是David,并且预先在4方之间共享了一个完美的十量子比特团簇态.本文协议总流程类似于双向链表,Alice是首结点,Charlie是尾结点,Bob是中间结点.参与者持有的多量子比特初始态分别为 $|X\rangle$ 、 $|Y\rangle$ 、 $|Z\rangle$ 、 $|W\rangle$,是 x 、 y 、 z 、 w 未知位量子态,其优势在于多量子比特初始态的数目始终大于参与者的数目,而且双向链式通信链是可以扩展的,因此,能传递更多信息.参与者要达成的目的是在通信过程中实现这4个多量子比特初始态的传递和重塑工作,其中各方系数均满足归一化条件,即 $|a_0|^2 + |a_1|^2 = 1$, $|b_0|^2 + |b_1|^2 = 1$, $|c_0|^2 + |c_1|^2 = 1$, $|d_0|^2 + |d_1|^2 = 1$,各自的多量子比特初始态表示为

$$\begin{aligned}
 |X\rangle &= (a_0 |00\dots 0\rangle + a_1 |11\dots 1\rangle)_{A_1 A_2 \dots A_x} \\
 |Y\rangle &= (b_0 |00\dots 0\rangle + b_1 |11\dots 1\rangle)_{B_1 B_2 \dots B_y} \quad (1) \\
 |Z\rangle &= (c_0 |00\dots 0\rangle + c_1 |11\dots 1\rangle)_{C_1 C_2 \dots C_z} \\
 |W\rangle &= (d_0 |00\dots 0\rangle + d_1 |11\dots 1\rangle)_{D_1 D_2 \dots D_w}
 \end{aligned}$$

协议采用1个十量子比特团簇态作为QC,该团簇态中10个量子比特通过量子纠缠作用可以实现彼此之间的信息共享,QC由3个三量子比特GHZ纠缠态加1个单量子比特构成,可表示为

$$\begin{aligned}
 |\varphi\rangle_{1,2,3,4,5,6,7,8,9,10} = & \\
 \frac{1}{4}(& |0000000000\rangle + |0000000111\rangle + \\
 & |0000111000\rangle + |0000111111\rangle + \\
 & |0111000000\rangle + |0111000111\rangle + \\
 & |0111111000\rangle + |0111111111\rangle + \\
 & |1000000000\rangle + |1000000111\rangle + \\
 & |1000111000\rangle + |1000111111\rangle + \\
 & |1111000000\rangle + |1111000111\rangle + \\
 & |1111111000\rangle + |1111111111\rangle)_{1,2,3,4,5,6,7,8,9,10} \quad (2)
 \end{aligned}$$

量子隐形传态总流程如图1所示,其中红色实线为量子通信过程,箭头指向为量子通信方向,黑色虚线为经典通信,蓝色小球代表参与者本身的量子比特,黑色小球代表从QC共享的量子比特。

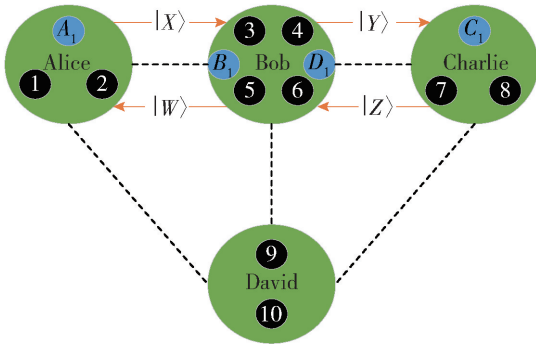


图1 量子隐形传态总流程

Fig. 1 General flow of quantum teleportation

2 BCCQT协议的实现和分析

2.1 多量子比特初始态的复单转换

首先,对4个多量子比特初始态 $|X\rangle$ 、 $|Y\rangle$ 、 $|Z\rangle$ 、 $|W\rangle$ 进行CNOT操作,CNOT操作的原理是当量子比特是0时,其后面的量子比特保持不变,而当量子比特是1时,其后面的量子比特全部取反.复单转换的任务就是先将多量子比特初始态各自的第1位置量子比特 A_1 、 B_1 、 C_1 、 D_1 作为控制量子比特,各自

剩余的 $x-1$ 、 $y-1$ 、 $z-1$ 、 $w-1$ 位置量子比特作为目标量子比特,操作完成后的状态表示为

$$\begin{aligned}
 |X_1\rangle &= (a_0 |0\rangle + a_1 |1\rangle)_{A_1} |00\dots 0\rangle_{A_2 A_3 \dots A_x} \\
 |Y_1\rangle &= (b_0 |0\rangle + b_1 |1\rangle)_{B_1} |00\dots 0\rangle_{B_2 B_3 \dots B_y} \quad (3) \\
 |Z_1\rangle &= (c_0 |0\rangle + c_1 |1\rangle)_{C_1} |00\dots 0\rangle_{C_2 C_3 \dots C_z} \\
 |W_1\rangle &= (d_0 |0\rangle + d_1 |1\rangle)_{D_1} |00\dots 0\rangle_{D_2 D_3 \dots D_w}
 \end{aligned}$$

经过上述操作,协议就变成了由4个单量子比特加上各自拥有的 $x-1$ 、 $y-1$ 、 $z-1$ 、 $w-1$ 位置量子态组合而成的复合态在一个十量子比特团簇态的信道下完成BCCQT.为实现多量子比特初始态的重塑目标,分为以下2个步骤来实施.

第1步 在通信参与方之间进行4个单量子比特的量子态重塑目标.

第2步 在通信参与方之间进行 $x-1$ 、 $y-1$ 、 $z-1$ 、 $w-1$ 位置量子态的重塑目标.通信方需要拥有额外的信道量子比特来完成通信过程中的信息交互,根据图1,十量子比特团簇态的信道中1、2量子比特属于Alice,3、4、5、6量子比特属于Bob,7、8量子比特属于Charlie,9、10量子比特属于David,如此,便完成了通信方量子比特的分配.整个量子系统组合状态表示为

$$\begin{aligned}
 |E\rangle_{A_1,1,2,B_1,3,D_1,4,5,6,C_1,7,8,9,10} = & \\
 |\varphi\rangle_{1,2,3,4,5,6,7,8,9,10} \otimes & |X_1\rangle \otimes |Y_1\rangle \otimes |Z_1\rangle \otimes |W_1\rangle \quad (4)
 \end{aligned}$$

式中: $|\varphi\rangle$ 是十量子比特团簇态; $|X_1\rangle$ 、 $|Y_1\rangle$ 、 $|Z_1\rangle$ 、 $|W_1\rangle$ 是完成多量子比特初始态的复单转换后的复合态; $|X_1\rangle$ 属于Alice; $|Y_1\rangle$ 和 $|W_1\rangle$ 属于Bob; $|Z_1\rangle$ 属于Charlie.

2.2 顺序量子隐形传态

根据图1,先进行顺序量子隐形传态,按Alice→Bob→Charlie顺序进行链式量子通信,具体可分为以下3个过程.

2.2.1 Alice→Bob阶段的通信

第1步 Alice将拥有的量子比特 A_1 和1组成量子比特对,其中, A_1 作为控制量子比特,1作为目标量子比特来进行CNOT操作.通过该操作, $(A_1, 1)$ 组成的量子比特对将会产生4种结果,结果集为 $\{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$.

第2步 Alice单独对拥有的量子比特 A_1 进行H门操作,H门操作的原理是可将基态变为叠加态的量子逻辑门,其是量子态自身的逆操作,因此,经过2次H门操作后量子态恢复到原来的状态,相当于中间没有经过任何测量操作.通过该操作,量子

比特 A_1 相当于将量子态转换为另一种量子比特状态,并传输给 Bob,在通信过程中起到了过渡的作用,为测量和重塑量子态做准备.

第3步 将 Alice 要传输给 Bob 的 $|X_1\rangle$ 复合态的非单量子比特部分 $|00\dots 0\rangle_{A_2A_3\dots A_x}$ 和后面可用来重塑 A_1 和 D_1 的量子比特 5 和 2 进行量子矢量计算,以此重塑 $|X_1\rangle$,完成 Alice \rightarrow Bob 阶段的通信. 此时,量子系统局部状态表示为

$$|E\rangle = |E_1\rangle \otimes |Y_1\rangle \otimes |Z_1\rangle \otimes |W_1\rangle = \frac{1}{8} [|00\dots 0\rangle_{A_2A_3\dots A_x} \otimes \{ |00\rangle_{A_1,1}(a_0|0\rangle \pm a_1|1\rangle)_2 \otimes (b_0|0\rangle \pm b_1|1\rangle)_5 + |00\rangle_{A_1,1}(a_0|1\rangle \pm a_1|0\rangle)_2 \otimes (b_0|1\rangle \pm b_1|0\rangle)_5 + |01\rangle_{A_1,1}(a_0|0\rangle \pm a_1|1\rangle)_2 \otimes (b_0|0\rangle \pm b_1|1\rangle)_5 + |01\rangle_{A_1,1}(a_0|1\rangle \pm a_1|0\rangle)_2 \otimes (b_0|1\rangle \pm b_1|0\rangle)_5 + |10\rangle_{A_1,1}(a_0|0\rangle \pm a_1|1\rangle)_2 \otimes (b_0|0\rangle \pm b_1|1\rangle)_5 + |10\rangle_{A_1,1}(a_0|1\rangle \pm a_1|0\rangle)_2 \otimes (b_0|1\rangle \pm b_1|0\rangle)_5 + |11\rangle_{A_1,1}(a_0|0\rangle \pm a_1|1\rangle)_2 \otimes (b_0|0\rangle \pm b_1|1\rangle)_5 + |11\rangle_{A_1,1}(a_0|1\rangle \pm a_1|0\rangle)_2 \otimes (b_0|1\rangle \pm b_1|0\rangle)_5 \} | \pm \rangle_9] \otimes |Y_1\rangle \otimes |Z_1\rangle \otimes |W_1\rangle \quad (5)$$

式中:量子比特 9 表示控制者 David 第 1 次单量子比特测量(single quantum measurement, SQM)可能出现的结果之一,后续也会把结果告知其他参与者;量子比特 5 和 2 表示的状态分别对应 A_1 和 D_1 可能出现的量子比特状态,其状态为结果集的 1/16.

2.2.2 Bob \rightarrow Charlie 阶段的通信

第1步 Bob 同样将拥有的量子比特 B_1 和 3 组成量子比特对,其中, B_1 作为控制量子比特, 3 作为目标量子比特来进行 CNOT 操作. 此时,产生 4 种结果,结果集为 $\{ |00\rangle, |01\rangle, |10\rangle, |11\rangle \}$.

第2步 Bob 将单独对其所拥有的量子比特 B_1 进行 H 门操作, H 门操作会将其要传输给 Charlie 的 B_1 量子比特状态转换为另一种状态,便于量子比特初始态的重塑.

第3步 将 Bob 要传输给 Charlie 的 $|Y_1\rangle$ 复合态的非单量子比特部分 $|00\dots 0\rangle_{B_2B_3\dots B_y}$ 进行整体的量子矢量计算,以此重塑 $|Y_1\rangle$,完成 Bob \rightarrow Charlie 阶段的通信. 此时,顺序阶段量子系统总状态表示为

$$|E\rangle = |E_2\rangle \otimes |Z_1\rangle \otimes |W_1\rangle = \frac{1}{16} [|00\dots 0\rangle_{A_2A_3\dots A_x} |00\dots 0\rangle_{B_2B_3\dots B_y} \otimes \{ |00\rangle_{A_1,1}(a_0|0\rangle \pm a_1|1\rangle)_2 \otimes (b_0|0\rangle \pm b_1|1\rangle)_5 + |00\rangle_{A_1,1}(a_0|1\rangle \pm a_1|0\rangle)_2 \otimes (b_0|1\rangle \pm b_1|0\rangle)_5 +$$

$$|01\rangle_{A_1,1}(a_0|0\rangle \pm a_1|1\rangle)_2 \otimes (b_0|0\rangle \pm b_1|1\rangle)_5 + |01\rangle_{A_1,1}(a_0|1\rangle \pm a_1|0\rangle)_2 \otimes (b_0|1\rangle \pm b_1|0\rangle)_5 + |10\rangle_{A_1,1}(a_0|0\rangle \pm a_1|1\rangle)_2 \otimes (b_0|0\rangle \pm b_1|1\rangle)_5 + |10\rangle_{A_1,1}(a_0|1\rangle \pm a_1|0\rangle)_2 \otimes (b_0|1\rangle \pm b_1|0\rangle)_5 + |11\rangle_{A_1,1}(a_0|0\rangle \pm a_1|1\rangle)_2 \otimes (b_0|0\rangle \pm b_1|1\rangle)_5 + |11\rangle_{A_1,1}(a_0|1\rangle \pm a_1|0\rangle)_2 \otimes (b_0|1\rangle \pm b_1|0\rangle)_5 \} | + \rangle_9 + \{ |00\rangle_{B_1,3}(a_0|0\rangle \mp a_1|1\rangle)_2 \otimes (b_0|0\rangle \mp b_1|1\rangle)_5 + |00\rangle_{B_1,3}(a_0|1\rangle \mp a_1|0\rangle)_2 \otimes (b_0|1\rangle \mp b_1|0\rangle)_5 + |01\rangle_{B_1,3}(a_0|0\rangle \mp a_1|1\rangle)_2 \otimes (b_0|0\rangle \mp b_1|1\rangle)_5 + |01\rangle_{B_1,3}(a_0|1\rangle \mp a_1|0\rangle)_2 \otimes (b_0|1\rangle \mp b_1|0\rangle)_5 + |10\rangle_{B_1,3}(a_0|0\rangle \mp a_1|1\rangle)_2 \otimes (b_0|0\rangle \mp b_1|1\rangle)_5 + |10\rangle_{B_1,3}(a_0|1\rangle \mp a_1|0\rangle)_2 \otimes (b_0|1\rangle \mp b_1|0\rangle)_5 + |11\rangle_{B_1,3}(a_0|0\rangle \mp a_1|1\rangle)_2 \otimes (b_0|0\rangle \mp b_1|1\rangle)_5 + |11\rangle_{B_1,3}(a_0|1\rangle \mp a_1|0\rangle)_2 \otimes (b_0|1\rangle \mp b_1|0\rangle)_5 \} | - \rangle_9] \otimes |Z_1\rangle \otimes |W_1\rangle \quad (6)$$

式(6)主要是在顺序链式传输的阶段通过量子矢量计算的结果重塑 A_1 和 D_1 的量子比特初始态. 因为之前对量子比特 A_1 和量子比特 B_1 都进行了 H 门操作,状态变化了 2 次,所以量子比特 9 的结果有 2 种,即控制者 David 第 1 次测量产生的 2 种结果,状态为测量结果中的 1/2.

2.2.3 量子态的测量

一个量子态被测量后会坍缩成另一个本征态,此时状态就已经固定不变了,会是预期结果集中的情况,因此,测量结果是一个概率性问题. 量子态在此阶段进行测量代表着整个顺序量子隐形传态的结束,根据协议流程的对称性,一半结果将产生. 测量主要分为以下 2 个步骤.

1) 控制者的测量.

David 用测量基 $\{ | + \rangle, | - \rangle \}$ 对量子比特 9 进行第 1 次 SQM, 其中 $| \pm \rangle = \frac{1}{\sqrt{2}}(|0\rangle \pm |1\rangle)$, 测量

基的选取和 Alice、Bob 传输的多量子比特初始态的单量子比特部分个数一致. 量子比特 9 的测量结果为 $| + \rangle_9$ 或者 $| - \rangle_9$, 概率各为 1/2, David 把测量的结果通过经典信道告知所有参与者.

2) 参与者的测量.

Alice 和 Bob 对其所拥有的量子比特对 $(A_1, 1)$ 和 $(B_1, 3)$ 经过 CNOT 操作和单独对各自的量子比特 A_1 和 B_1 执行 H 门操作后的量子比特 A_1 和 B_1 用测量基 $\{ |00\rangle, |01\rangle, |10\rangle, |11\rangle \}$ 进行第 1 次贝尔态测量(Bell state measurement, BSM). 经过测量后,

量子态分别坍缩成式(6)中量子比特5和2的可能结果,概率为1/16,并且Alice和Bob同样将测量的结果通过经典信道告知其他参与者。

2.3 逆序量子隐形传态

进行逆序量子隐形传态,与前面的过程同理,按Charlie→Bob→Alice顺序进行链式量子通信,具体可分为以下3个过程。

2.3.1 Charlie→Bob阶段的通信

第1步 Charlie将拥有的量子比特 C_1 和7组成量子比特对,其中, C_1 作为控制量子比特,7作为目标量子比特来进行CNOT操作。通过该操作后,同样 $(C_1,7)$ 组成的量子比特对将会产生4种结果,结果集为 $\{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$ 。

第2步 Charlie将单独对拥有的量子比特 C_1 进行H门操作,经过这个操作后, C_1 变成另一种量子态,并将信息传递给Bob,为量子态重塑做准备。

第3步 Charlie将要传输给Bob的 $|Z_1\rangle$ 复合态的非单量子比特部分 $|00\dots0\rangle_{c_2c_3\dots c_z}$ 和后面用来重塑 B_1 和 C_1 的信道量子比特8和6进行量子矢量计算,以此达到重塑 $|Z_1\rangle$,完成Charlie→Bob阶段的通信。量子比特8和6表示的状态分别对应 B_1 和 C_1 可能出现的量子初始状态,并且 B_1 和 C_1 总状态结果分别有16种,概率为1/16。此时,量子系统局部状态表示为

$$|E\rangle = |E_3\rangle \otimes |W_1\rangle = \frac{1}{32} [|00\dots0\rangle_{c_2c_3\dots c_z} \otimes \{ |00\rangle_{c_1,7} (c_0 |0\rangle \pm c_1 |1\rangle)_8 \otimes (d_0 |0\rangle \pm d_1 |1\rangle)_6 + |00\rangle_{c_1,7} (c_0 |1\rangle \pm c_1 |0\rangle)_8 \otimes (d_0 |1\rangle \pm d_1 |0\rangle)_6 + |01\rangle_{c_1,7} (c_0 |0\rangle \pm c_1 |1\rangle)_8 \otimes (d_0 |0\rangle \pm d_1 |1\rangle)_6 + |01\rangle_{c_1,7} (c_0 |1\rangle \pm c_1 |0\rangle)_8 \otimes (d_0 |1\rangle \pm d_1 |0\rangle)_6 + |10\rangle_{c_1,7} (c_0 |0\rangle \pm c_1 |1\rangle)_8 \otimes (d_0 |0\rangle \pm d_1 |1\rangle)_6 + |10\rangle_{c_1,7} (c_0 |1\rangle \pm c_1 |0\rangle)_8 \otimes (d_0 |1\rangle \pm d_1 |0\rangle)_6 + |11\rangle_{c_1,7} (c_0 |0\rangle \pm c_1 |1\rangle)_8 \otimes (d_0 |0\rangle \pm d_1 |1\rangle)_6 + |11\rangle_{c_1,7} (c_0 |1\rangle \pm c_1 |0\rangle)_8 \otimes (d_0 |1\rangle \pm d_1 |0\rangle)_6 \} | \pm \rangle_{10}] \otimes |W_1\rangle \quad (7)$$

式(7)中量子比特10表示控制者David进行第2次SQM可能出现的结果之一,同时,David把结果告知其他参与者。

2.3.2 Bob→Alice阶段的通信

第1步 Bob同样也将拥有的量子比特 D_1 和4组成量子比特对,其中, D_1 作为控制量子比特,4作为目标量子比特来进行CNOT操作,此时也将产生4种结果,结果集为 $\{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$ 。

第2步 Bob将单独对其拥有的量子比特 D_1 进行H门操作,通过该操作, D_1 将会以另一种量子态的形式传输给Alice,这步操作为后面量子态的重塑提供保证。

第3步 Bob把要传输给Alice的 $|W_1\rangle$ 复合态的非单量子比特部分 $|00\dots0\rangle_{d_2d_3\dots d_w}$ 进行量子矢量计算,以此重塑 $|W_1\rangle$,完成Bob→Alice阶段的通信。此时,逆序通信完成,也标志着整个协议总流程全部完成,2条链路形成一个环路,协议分为2条单向链路来执行流程,这样做使流程更加清晰。逆序通信阶段量子系统总状态表示为

$$|E\rangle = \frac{1}{64} [|00\dots0\rangle_{c_2c_3\dots c_z} |00\dots0\rangle_{d_2d_3\dots d_w} \otimes \{ |00\rangle_{c_1,7} (c_0 |0\rangle \pm c_1 |1\rangle)_8 \otimes (d_0 |0\rangle \pm d_1 |1\rangle)_6 + |00\rangle_{c_1,7} (c_0 |1\rangle \pm c_1 |0\rangle)_8 \otimes (d_0 |1\rangle \pm d_1 |0\rangle)_6 + |01\rangle_{c_1,7} (c_0 |0\rangle \pm c_1 |1\rangle)_8 \otimes (d_0 |0\rangle \pm d_1 |1\rangle)_6 + |01\rangle_{c_1,7} (c_0 |1\rangle \pm c_1 |0\rangle)_8 \otimes (d_0 |1\rangle \pm d_1 |0\rangle)_6 + |10\rangle_{c_1,7} (c_0 |0\rangle \pm c_1 |1\rangle)_8 \otimes (d_0 |0\rangle \pm d_1 |1\rangle)_6 + |10\rangle_{c_1,7} (c_0 |1\rangle \pm c_1 |0\rangle)_8 \otimes (d_0 |1\rangle \pm d_1 |0\rangle)_6 + |11\rangle_{c_1,7} (c_0 |0\rangle \pm c_1 |1\rangle)_8 \otimes (d_0 |0\rangle \pm d_1 |1\rangle)_6 + |11\rangle_{c_1,7} (c_0 |1\rangle \pm c_1 |0\rangle)_8 \otimes (d_0 |1\rangle \pm d_1 |0\rangle)_6 \} | + \rangle_{10} + \{ |00\rangle_{d_1,4} (c_0 |0\rangle \mp c_1 |1\rangle)_8 \otimes (d_0 |0\rangle \mp d_1 |1\rangle)_6 + |00\rangle_{d_1,4} (c_0 |1\rangle \mp c_1 |0\rangle)_8 \otimes (d_0 |1\rangle \mp d_1 |0\rangle)_6 + |01\rangle_{d_1,4} (c_0 |0\rangle \mp c_1 |1\rangle)_8 \otimes (d_0 |0\rangle \mp d_1 |1\rangle)_6 + |01\rangle_{d_1,4} (c_0 |1\rangle \mp c_1 |0\rangle)_8 \otimes (d_0 |1\rangle \mp d_1 |0\rangle)_6 + |10\rangle_{d_1,4} (c_0 |0\rangle \mp c_1 |1\rangle)_8 \otimes (d_0 |0\rangle \mp d_1 |1\rangle)_6 + |10\rangle_{d_1,4} (c_0 |1\rangle \mp c_1 |0\rangle)_8 \otimes (d_0 |1\rangle \mp d_1 |0\rangle)_6 + |11\rangle_{d_1,4} (c_0 |0\rangle \mp c_1 |1\rangle)_8 \otimes (d_0 |0\rangle \mp d_1 |1\rangle)_6 + |11\rangle_{d_1,4} (c_0 |1\rangle \mp c_1 |0\rangle)_8 \otimes (d_0 |1\rangle \mp d_1 |0\rangle)_6 \} | - \rangle_{10}] \quad (8)$$

式(8)主要是在逆序链式传输的阶段通过量子矢量计算产生的结果,目的是来重塑 B_1 和 C_1 的量子比特初始态。因为之前对量子比特 C_1 和量子比特 D_1 都进行了H门操作,状态变化了2次,并且经过了2次阶段通信,所以量子比特10的结果也有2种,即控制者David进行第2次SQM产生的2种结果,其状态的结果共有2种,概率为1/2。

2.3.3 量子态的测量

量子态在该阶段的测量代表着整个逆序量子隐形传态的结束,同时也代表着协议总流程的结束,通信4方至此便完成了所有量子态的传输。量子态的测量主要分为以下2个步骤。

1) 控制者的测量。

David仍用测量基 $\{|+\rangle, |-\rangle\}$ 对量子比特

10 进行第 2 次 SQM, 测量结果为 $|+\rangle_{10}$ 或者 $|-\rangle_{10}$, 概率为 1/2, 并且把测量的所有结果通过经典信道告知所有参与者.

2) 参与者的测量.

Charlie 和 Bob 对其所拥有的量子比特对 ($C_1, 7$) 和 ($D_1, 4$) 经过 CNOT 操作和单独对各自的量子比特 C_1 和 D_1 执行 H 门操作后的量子比特 C_1 和 D_1 , 同样用测量基 $\{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$ 进行第 2 次 BSM. 经过测量后量子态分别坍缩成式 (8) 中量子比特 8 和 6 的可能结果, 概率为 1/16, 最后, Charlie 和 Bob 同样将测量的结果通过经典信道告知其他参与者.

经过前面的顺序和逆序量子隐形传态中参与者的第 1 次测量和第 2 次测量, 得到的结果如表 1 所示.

2.4 多量子比特初始态的单重塑

经过前面的复单转换、顺序通信和逆序通信操作后, 实现了 4 个单量子比特加上各自拥有的 $x-1, y-1, z-1, w-1$ 位置量子态组合而成的复合态在 3 个参与者之间的通信. 然后, 对 Alice 所剩的量子比特 2、Bob 所剩的量子比特 5 和 6 及 Charlie 所剩的量子比特 8 进行么正操作 (unitary operation, UO), 以重塑 D_1, A_1, C_1, B_1 的单量子比特状态信息. 具体 UO 如表 2 所示. 其中: 符号 I 表示恒等操作; σ_x 表示非门; σ_z 表示 z 操作. UO 后的状态都表示为 0 和 1 的组合, 概率为 1/16, 对应的量子线路如图 2 所示.

2.5 多量子比特初始态的复重塑和可行性分析

经过对多量子比特初始态的重塑操作, 完成了单量子比特部分. 然后, 则是在通信完成后进行 $x-1, y-1, z-1, w-1$ 位置量子态的重塑操作. 在重塑多量子比特初始态 $|X\rangle, |Y\rangle, |Z\rangle, |W\rangle$ 的情况下, 虽然 x, y, z, w 的个数都是不确定的, 但总体上, 量子的约束仍分为对称和非对称量子隐形传态.

2.5.1 对称量子隐形传态

当 3 个参与者之间进行的是对称量子隐形传态, 即 $x=y=z=w$ 时, Alice 以量子比特 2 为控制量子比特, $D_2 D_3 \dots D_w$ 为目标量子比特, Bob 分别以量子比特 5 和 6 为控制量子比特, $A_2 A_3 \dots A_x$ 和 $C_2 C_3 \dots C_z$ 为目标量子比特, Charlie 则以量子比特 8 为控制量子比特, $B_2 B_3 \dots B_y$ 为目标量子比特, 全部进行 CNOT 操作, 相当于取各自的已经重塑了的首位单量子比特部分 D_1, A_1, C_1, B_1 进行反向控制操作, 最终完成

表 1 测量结果
Table 1 Measurement results

Alice 的 BSM1	Bob 的 BSM1	Charlie 的 BSM2	Bob 的 BSM2
$ 00\rangle_{A_1,1}$	$ 00\rangle_{B_1,3}$	$ 00\rangle_{C_1,7}$	$ 00\rangle_{D_1,4}$
$ 00\rangle_{A_1,1}$	$ 01\rangle_{B_1,3}$	$ 00\rangle_{C_1,7}$	$ 01\rangle_{D_1,4}$
$ 00\rangle_{A_1,1}$	$ 10\rangle_{B_1,3}$	$ 00\rangle_{C_1,7}$	$ 10\rangle_{D_1,4}$
$ 00\rangle_{A_1,1}$	$ 11\rangle_{B_1,3}$	$ 00\rangle_{C_1,7}$	$ 11\rangle_{D_1,4}$
$ 01\rangle_{A_1,1}$	$ 00\rangle_{B_1,3}$	$ 01\rangle_{C_1,7}$	$ 00\rangle_{D_1,4}$
$ 01\rangle_{A_1,1}$	$ 01\rangle_{B_1,3}$	$ 01\rangle_{C_1,7}$	$ 01\rangle_{D_1,4}$
$ 01\rangle_{A_1,1}$	$ 10\rangle_{B_1,3}$	$ 01\rangle_{C_1,7}$	$ 10\rangle_{D_1,4}$
$ 01\rangle_{A_1,1}$	$ 11\rangle_{B_1,3}$	$ 01\rangle_{C_1,7}$	$ 11\rangle_{D_1,4}$
$ 10\rangle_{A_1,1}$	$ 00\rangle_{B_1,3}$	$ 10\rangle_{C_1,7}$	$ 00\rangle_{D_1,4}$
$ 10\rangle_{A_1,1}$	$ 01\rangle_{B_1,3}$	$ 10\rangle_{C_1,7}$	$ 01\rangle_{D_1,4}$
$ 10\rangle_{A_1,1}$	$ 10\rangle_{B_1,3}$	$ 10\rangle_{C_1,7}$	$ 10\rangle_{D_1,4}$
$ 10\rangle_{A_1,1}$	$ 11\rangle_{B_1,3}$	$ 10\rangle_{C_1,7}$	$ 11\rangle_{D_1,4}$
$ 11\rangle_{A_1,1}$	$ 00\rangle_{B_1,3}$	$ 11\rangle_{C_1,7}$	$ 00\rangle_{D_1,4}$
$ 11\rangle_{A_1,1}$	$ 01\rangle_{B_1,3}$	$ 11\rangle_{C_1,7}$	$ 01\rangle_{D_1,4}$
$ 11\rangle_{A_1,1}$	$ 10\rangle_{B_1,3}$	$ 11\rangle_{C_1,7}$	$ 10\rangle_{D_1,4}$
$ 11\rangle_{A_1,1}$	$ 11\rangle_{B_1,3}$	$ 11\rangle_{C_1,7}$	$ 11\rangle_{D_1,4}$
$ 00\rangle_{A_1,1}$	$ 00\rangle_{B_1,3}$	$ 00\rangle_{C_1,7}$	$ 00\rangle_{D_1,4}$
$ 00\rangle_{A_1,1}$	$ 01\rangle_{B_1,3}$	$ 00\rangle_{C_1,7}$	$ 01\rangle_{D_1,4}$
$ 00\rangle_{A_1,1}$	$ 10\rangle_{B_1,3}$	$ 00\rangle_{C_1,7}$	$ 10\rangle_{D_1,4}$
$ 00\rangle_{A_1,1}$	$ 11\rangle_{B_1,3}$	$ 00\rangle_{C_1,7}$	$ 11\rangle_{D_1,4}$
$ 01\rangle_{A_1,1}$	$ 00\rangle_{B_1,3}$	$ 01\rangle_{C_1,7}$	$ 00\rangle_{D_1,4}$
$ 01\rangle_{A_1,1}$	$ 01\rangle_{B_1,3}$	$ 01\rangle_{C_1,7}$	$ 01\rangle_{D_1,4}$
$ 01\rangle_{A_1,1}$	$ 10\rangle_{B_1,3}$	$ 01\rangle_{C_1,7}$	$ 10\rangle_{D_1,4}$
$ 01\rangle_{A_1,1}$	$ 11\rangle_{B_1,3}$	$ 01\rangle_{C_1,7}$	$ 11\rangle_{D_1,4}$
$ 10\rangle_{A_1,1}$	$ 00\rangle_{B_1,3}$	$ 10\rangle_{C_1,7}$	$ 00\rangle_{D_1,4}$
$ 10\rangle_{A_1,1}$	$ 01\rangle_{B_1,3}$	$ 10\rangle_{C_1,7}$	$ 01\rangle_{D_1,4}$
$ 10\rangle_{A_1,1}$	$ 10\rangle_{B_1,3}$	$ 10\rangle_{C_1,7}$	$ 10\rangle_{D_1,4}$
$ 10\rangle_{A_1,1}$	$ 11\rangle_{B_1,3}$	$ 10\rangle_{C_1,7}$	$ 11\rangle_{D_1,4}$
$ 11\rangle_{A_1,1}$	$ 00\rangle_{B_1,3}$	$ 11\rangle_{C_1,7}$	$ 00\rangle_{D_1,4}$
$ 11\rangle_{A_1,1}$	$ 01\rangle_{B_1,3}$	$ 11\rangle_{C_1,7}$	$ 01\rangle_{D_1,4}$
$ 11\rangle_{A_1,1}$	$ 10\rangle_{B_1,3}$	$ 11\rangle_{C_1,7}$	$ 10\rangle_{D_1,4}$
$ 11\rangle_{A_1,1}$	$ 11\rangle_{B_1,3}$	$ 11\rangle_{C_1,7}$	$ 11\rangle_{D_1,4}$

$|W\rangle, |X\rangle, |Z\rangle, |Y\rangle$ 多量子比特初始态的重塑.

2.5.2 非对称量子隐形传态

当 3 个参与者之间进行的是非对称量子隐形传态, 即 x, y, z, w 只要有一个不相等时, 具体的量子隐形传态可分以下 2 个过程.

1) Alice 与 Bob 的 BQT 过程.

当 Alice 传输给 Bob 的 $|X\rangle$ 量子比特数不等于

表 2 么正操作

Table 2 Unitary operation

Alice 的 UO	Bob 的 UO1	Bob 的 UO2	Charlie 的 UO	Alice 的 UO	Bob 的 UO1	Bob 的 UO2	Charlie 的 UO
I_2	I_5	I_6	I_8	σ_{x2}	σ_{x5}	σ_{x6}	σ_{x8}
σ_{x2}	I_5	σ_{x6}	I_8	I_2	σ_{x5}	I_6	σ_{x8}
σ_{z2}	I_5	σ_{z6}	I_8	$\sigma_{x2}\sigma_{x2}$	σ_{x5}	$\sigma_{x6}\sigma_{x6}$	σ_{x8}
$\sigma_{z2}\sigma_{x2}$	I_5	$\sigma_{z6}\sigma_{x6}$	I_8	I_2	σ_{x5}	I_6	σ_{x8}
I_2	σ_{x5}	I_6	σ_{x8}	$\sigma_{x2}\sigma_{x2}$	$\sigma_{x5}\sigma_{x5}$	σ_{x6}	$\sigma_{x8}\sigma_{x8}$
σ_{x2}	σ_{x5}	σ_{x6}	σ_{x8}	$\sigma_{x2}\sigma_{x2}$	$\sigma_{x5}\sigma_{x5}$	$\sigma_{x6}\sigma_{x6}$	$\sigma_{x8}\sigma_{x8}$
σ_{z2}	σ_{x5}	σ_{z6}	σ_{x8}	I_2	$\sigma_{x5}\sigma_{x5}$	I_6	$\sigma_{x8}\sigma_{x8}$
$\sigma_{z2}\sigma_{x2}$	σ_{x5}	$\sigma_{z6}\sigma_{x6}$	σ_{x8}	$\sigma_{z2}\sigma_{x2}\sigma_{z2}$	$\sigma_{x5}\sigma_{x5}$	$\sigma_{z6}\sigma_{x6}\sigma_{z6}$	$\sigma_{x8}\sigma_{x8}$
I_2	σ_{x5}	I_6	σ_{x8}	σ_{z2}	I_5	σ_{z6}	I_8
σ_{x2}	σ_{x5}	σ_{x6}	σ_{x8}	$\sigma_{x2}\sigma_{x2}$	I_5	$\sigma_{x6}\sigma_{x6}$	I_8
σ_{z2}	σ_{x5}	σ_{z6}	σ_{x8}	I_2	I_5	I_6	I_8
$\sigma_{z2}\sigma_{x2}$	σ_{x5}	$\sigma_{z6}\sigma_{x6}$	σ_{x8}	$\sigma_{z2}\sigma_{x2}\sigma_{z2}$	I_5	$\sigma_{z6}\sigma_{x6}\sigma_{z6}$	I_8
I_2	σ_{x5}	I_6	$\sigma_{x8}\sigma_{x8}$	σ_{z2}	$\sigma_{x5}\sigma_{x5}\sigma_{x5}$	σ_{z6}	$\sigma_{x8}\sigma_{x8}\sigma_{x8}$
σ_{x2}	σ_{x5}	σ_{x6}	$\sigma_{x8}\sigma_{x8}$	$\sigma_{x2}\sigma_{x2}$	$\sigma_{x5}\sigma_{x5}\sigma_{x5}$	$\sigma_{x6}\sigma_{x6}$	$\sigma_{x8}\sigma_{x8}\sigma_{x8}$
σ_{z2}	$\sigma_{x5}\sigma_{x5}$	σ_{z6}	$\sigma_{x8}\sigma_{x8}$	I_2	$\sigma_{x5}\sigma_{x5}\sigma_{x5}$	I_6	$\sigma_{x8}\sigma_{x8}\sigma_{x8}$
$\sigma_{z2}\sigma_{x2}$	$\sigma_{x5}\sigma_{x5}$	$\sigma_{z6}\sigma_{x6}$	$\sigma_{x8}\sigma_{x8}$	$\sigma_{z2}\sigma_{x2}\sigma_{z2}$	$\sigma_{x5}\sigma_{x5}\sigma_{x5}$	$\sigma_{z6}\sigma_{x6}\sigma_{z6}$	$\sigma_{x8}\sigma_{x8}\sigma_{x8}$

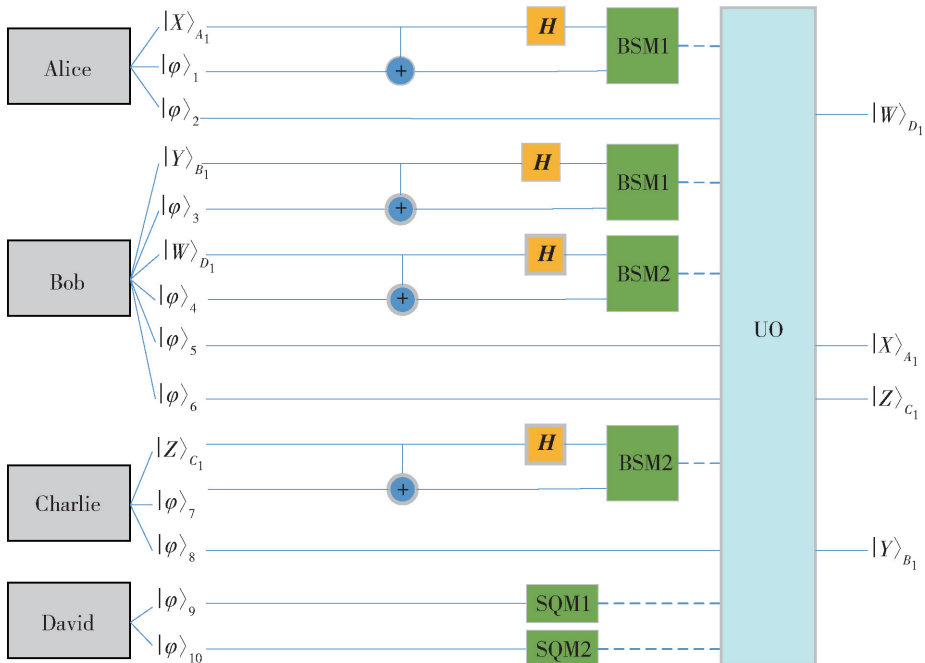


图 2 量子线路

Fig. 2 Quantum circuit

Bob 传输给 Alice 的 $|W\rangle$ 量子比特数时, 即 $x \neq w$, 具体地, 分为以下 2 种情况来进行讨论.

① 当 Alice 传输给 Bob 的 $|X\rangle$ 量子比特数大于 Bob 传输给 Alice 的 $|W\rangle$ 量子比特数时, 即 $x > w$, 因

为要满足对称的情况, 所以 Bob 需要添加 $x - w$ 个辅助量子比特, 并且以量子比特 5 为控制量子比特, $D_2 D_3 \dots D_w, Q_1 Q_2 \dots Q_{x-w}$ 为目标量子比特进行 $x - 1$ 次 CNOT 操作来重塑 $|X\rangle$, Alice 以量子比特 2 为控

制量子比特, $D_2 D_3 D_4 \cdots D_w$ 为目标量子比特进行 $w-1$ 次 CNOT 操作, 由于 Bob 传输的数量少, Alice 只需要进行 $w-1$ 次操作来重塑 $|W\rangle$ 。

② 当 Alice 传输给 Bob 的 $|X\rangle$ 量子比特数小于 Bob 传输给 Alice 的 $|W\rangle$ 量子比特数时, 即 $x < w$, 因为要满足对称的情况, 所以 Alice 需要添加 $w-x$ 个辅助量子比特, 并且以量子比特 2 为控制量子比特, $A_2 A_3 \cdots A_x, Q_1 Q_2 \cdots Q_{w-x}$ 为目标量子比特进行 $w-1$ 次 CNOT 操作来重塑 $|W\rangle$, Bob 以量子比特 5 为控制量子比特, $A_2 A_3 \cdots A_x$ 为目标量子比特进行 $x-1$ 次 CNOT 操作, 由于 Alice 传输的数量少, Bob 只需要进行 $x-1$ 次操作来重塑 $|X\rangle$ 。

2) Bob 与 Charlie 的 BQT 过程。

当 Bob 传输给 Charlie 的 $|Y\rangle$ 量子比特数不等于 Charlie 传输给 Bob 的 $|Z\rangle$ 量子比特数时, 即 $y \neq z$, 具体地, 分为以下 2 种情况进行讨论。

① 当 Bob 传输给 Charlie 的 $|Y\rangle$ 量子比特数大于 Charlie 传输给 Bob 的 $|Z\rangle$ 量子比特数时, 即 $y > z$, 因为要满足对称的情况, 所以 Charlie 需要添加 $y-z$ 个辅助量子比特, 并且以量子比特 8 为控制量子比特, $C_2 C_3 \cdots C_z, Q_1 Q_2 \cdots Q_{y-z}$ 为目标量子比特进行 $y-1$ 次 CNOT 操作来重塑 $|Y\rangle$, Bob 以量子比特 6 为控制量子比特, $C_2 C_3 \cdots C_z$ 为目标量子比特进行 $z-1$ 次 CNOT 操作, 由于 Charlie 传输的数量少, Bob 只需要进行 $z-1$ 次操作来重塑 $|Z\rangle$ 。

② 当 Bob 传输给 Charlie 的 $|Y\rangle$ 量子比特数小于 Charlie 传输给 Bob 的 $|Z\rangle$ 量子比特数时, 即 $y < z$, 因为要满足对称的情况, 所以 Bob 需要添加 $z-y$ 个辅助量子比特, 并且以量子比特 6 为控制量子比特, $B_2 B_3 \cdots B_y, Q_1 Q_2 \cdots Q_{z-y}$ 为目标量子比特进行 $z-1$ 次 CNOT 操作来重塑 $|Z\rangle$, Charlie 以量子比特 8 为控制量子比特, $B_2 B_3 \cdots B_y$ 为目标量子比特进行 $y-1$ 次 CNOT 操作, 由于 Bob 传输的数量少, Charlie 只需要进行 $y-1$ 次操作来重塑 $|Y\rangle$ 。

通过上述步骤和过程, 通信 4 方在 QC 中完成了量子隐形传态, 并且实现了多量子比特初始态的重塑。因此, 本文提出的十量子比特团簇态的多量子 BCCQT 协议是可行的。

2.6 协议的安全性分析

本文的 BCCQT 中, 参与者 Alice、Bob 和 Charlie 要进行安全的量子通信, 必须在控制者 David 的协助下进行, 因此, 控制者主要有以下 2 个权限来保证信息的安全传输。

第 1 权限: 协议中控制者 David 允许 Alice、

Bob、Charlie 之间进行通信, 并且 David 在测量基 $\{|+\rangle, |-\rangle\}$ 下进行 SQM, 同时, 参与者在测量后基 $\{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$ 下进行 BSM, 从而实现通信。如果 David 不允许参与者通信, 并且没有进行测量, 则该通信过程都无从谈起, 因此, 控制者 David 决定通信安全的第 1 个权限就是通信过程的有无。

第 2 权限: 通信过程中控制者 David 允许参与者 Alice、Bob、Charlie 之间进行通信, 控制者 David 在测量基测量下发生量子坍塌, 得到测量结果, 并且通过经典信道将其测量结果公布给参与者, 参与者完成测量后将结果公布, 从而通信过程完成, 参与者可以根据结果进行 UO 来重塑量子比特初始态。如果此时控制者 David 选择不公布测量结果, 那么参与者就无法只根据自己的测量结果完成通信过程, 并且不能通过 UO 重塑量子初始态, 因此, 控制者 David 决定通信安全的第 2 个权限就是是否公布其测量结果。

量子通信过程中的安全性除了控制者发挥关键作用外, 还有 QC 的纠缠特性。多量子比特初始态的重塑则依赖十量子比特团簇态的量子纠缠特性, 由通信方 Alice、Bob、Charlie 和 David 的非局域关联以及经典信道和 UO 等共同完成的。QC 的纠缠特性保证不会受到窃听, 通信方共享了一个完美的十量子比特团簇态后, 它们彼此之间不受空间噪声的干扰, 并且如果经典信道也是一种稳定环境, 那么量子安全通信能够顺利完成。因此, 完善通信过程中的 QC 对于量子安全通信是必须的。

3 协议的对比讨论

量子隐形传态协议中重塑的多量子比特初始态比较多, 并且通信过程较为复杂, 可以根据协议^[16]中的公式 $\mu = q_s / (q_u + q_s + q_a + b)$ 来计算量子隐形传态协议的内在效率 μ 。其中: q_u 表示 QC 的量子比特数; q_s 表示未知的量子比特总数目; q_a 表示辅助量子比特的数目; b 表示经典信道消耗的比特数。不同协议之间 μ 的对比如表 3 所示, 传输量表示双方传输的量子比特数, 信道表示使用的 QC。

当参数满足 $x = w = y = z$ 时, 该协议是一个对称量子隐形传态协议, 反之, 则是非对称协议。本文主要考虑对称的情况, 因为协议传输的是多量子比特初始态, 所以不考虑加入辅助量子比特。本文协议和文献[18]中的相比, 若都是在 $1 \leftrightarrow 1$ 的情况下, $\mu = 15.38\%$, 效率高于以五量子比特团簇态为 QC

表3 协议对比

Table 3 Protocol comparison

协议	传输量	信道	b	$\mu/\%$
文献[18]	1↔1	5	10	13.33
文献[16]	2↔2	5	6	30.76
文献[21]	1↔1	10	8	11.11
文献[22]	3↔3	11	9	30.00
文献[7]	3↔3	13	15	17.65
本文	$x↔w$	10	12	$\frac{2(x+w)}{2(x+w)+22} \times 100$

的情况;与文献[21]中的协议相比,若都是在1↔1的情况下,并且也是以一个十量子比特团簇态作为QC,尽管经典信道所消耗比特数更高,但由于Alice和Bob及Bob和Charlie之间通信的对称性,本文协议内在效率也高于文献[21]中的协议的11.11%;文献[16]中的协议在2↔2的情况下,采取了一个五量子比特团簇态作为QC且经典信道所耗比特数只需要6个, $\mu=30.76\%$,虽然本文在此情况下 $\mu=2 \times 4 / (2 \times 4 + 22) = 26.66\%$,略微低于其效率,但是传输的量子比特总数多,在对称的情况下,总共为8个,是其2倍,单从量子比特数目来说,效率也还不错;文献[22]中的协议在3↔3的情况下,采用了一个十一量子比特团簇态作为QC,此情况下,本文协议 $\mu=35.29\%$,效率更高;文献[7]中的协议同样是在3↔3的情况下,采用一个十三量子比特团簇态作为QC且都是BQT,但其内在效率低于本文协议,凸显了本协议的优势。综上,通过以上对比预估,在理想情况下,BCCQT随着参与者的增多,通信链可以向右无限延伸,并且随着双方传输的量子比特数增加,协议的内在效率也逐渐提高,无限接近于1。

通过系统性地阐述多量子BCCQT协议,发现协议有规律可循。其中,以十量子比特团簇态作为QC,这是根据结点数即参与者数量和多量子比特初始态综合考虑的,双向链式意味着这个通信链和双向链表一样,通过加结点可以向右进行延伸。假设总结点数为 n ,首先考虑参与者,中间结点数是 $n-2$,首尾结点数分别恒定为1,中间结点消耗的总量子比特数为 $4(n-2)$,首尾结点共消耗4个量子比特;然后,考虑控制者,因为控制者可以告知其他参与者测量结果,所以它必须存在,并且数量只可能是1或2,控制者作为指针,大大增加了通信过程的安全性,当控制者唯一时消耗的量子比特数为2,则协议

总消耗量子比特(QC的比特数)为 $4n-2$ 。

4 结论

1) 以十量子比特团簇态作为QC的BCCQT协议在理论上是可行和安全的,该协议在量子比特和经典比特的消耗上相互协调,随着总量子比特数的相对增加,协议的内在效率也随之提高。

2) 将协议流程和双向链表进行对比,发现QC的量子比特数与参与者、控制者数量之间存在规律,并且通信链可以无限延伸,以此提出基于 $4n-2$ 量子比特团簇态的链式 $n+1$ 方BCQT协议范式。

参考文献:

- [1] 吴华, 王向斌, 潘建伟. 量子通信现状与展望[J]. 中国科学: 信息科学, 2014, 44(3): 296-311.
WU H, WANG X B, PAN J W. Current situation and prospect of quantum communication[J]. Science China: Information Science, 2014, 44(3): 296-311. (in Chinese)
- [2] 赵慧, 郭莎. 三体量子态的纠缠性质[J]. 北京工业大学学报, 2015, 41(5): 797-800.
ZHAO H, GUO S. Entanglement properties of the tripartite quantum states[J]. Journal of Beijing University of Technology, 2015, 41(5): 797-800. (in Chinese)
- [3] 刘洋. 远距离量子密钥分发系统的相关研究[D]. 合肥: 中国科学技术大学, 2012.
LIU Y. Research on long-distance quantum key distribution system[D]. Hefei: University of Science and Technology of China, 2012. (in Chinese)
- [4] 苏晓琴, 郭光灿. 量子隐形传态[J]. 物理学进展, 2004, 24(3): 259-273.
SU X Q, GUO G C. Quantum teleportation[J]. Progress in Physics, 2004, 24(3): 259-273. (in Chinese)
- [5] FU H Z, TIAN X L, HU Y. A general method of selecting quantum channel for bidirectional quantum teleportation[J]. International Journal of Theoretical Physics, 2014, 53: 1840-1847.
- [6] CHEN Y X, DU J, LIU S Y, et al. Cyclic quantum teleportation[J]. Quantum Information Processing, 2017, 16(8): 201.
- [7] SUN S Y, ZHANG H S. Quantum double-direction cyclic controlled communication via a thirteen-qubit entangled state[J]. Quantum Information Processing, 2020, 19(9): 120.
- [8] FAHIMEH Z, HOSSEIN K M, DARIUSH A M, et al. Efficient circular controlled quantum teleportation and broadcast schemes in the presence of quantum noises[J].

- Quantum Information Processing, 2021, 20(5): 175.
- [9] 赵慧, 张兴华. 三体 Bell 对角态的纠缠[J]. 北京工业大学学报, 2011, 37(2): 306-313.
ZHAO H, ZHANG X H. Entanglement of tripartite Bell diagonal states [J]. Journal of Beijing University of Technology, 2011, 37(2): 306-313. (in Chinese)
- [10] WANG M T, LI H S. Bidirectional controlled quantum teleportation via two pairs of Bell states[J]. International Journal of Theoretical Physics, 2021, 60: 2262-2267.
- [11] VIKRAM V. Cyclic quantum teleportation via GHZ-like state[J]. Modern Physics Letters A, 2020, 35(40): 2050333.
- [12] DU Z L, LI X L, LIU X J. Bidirectional quantum teleportation with GHZ states and EPR pairs via entanglement swapping [J]. International Journal of Theoretical Physics, 2020, 59: 622-631.
- [13] VIKRAM V. Bidirectional quantum teleportation and cyclic quantum teleportation of multi-qubit entangled states via G-state [J]. International Journal of Modern Physics B, 2020, 34(28): 2050261.
- [14] LIU X F, LI D F, DENG Y D. Experimental realization of quantum controlled teleportation of arbitrary two-qubit state via a five-qubit entangled state[J]. Chinese Physics B, 2022, 31(5): 127-132.
- [15] LI D F, ZHENG Y D, LIU X F, et al. Hierarchical quantum teleportation of arbitrary single-qubit state by using four-qubit cluster state[J]. International Journal of Theoretical Physics, 2021, 60: 1911-1919.
- [16] VIKRAM V. Bidirectional controlled quantum teleportation of multi-qubit entangled states via five-qubit entangled state [J]. Physica Scripta, 2021, 96(3): 035105.
- [17] WANG M T, LI H S. Bidirectional quantum teleportation using a five-qubit cluster state as a quantum channel[J]. Quantum Information Processing, 2022, 21(2): 44.
- [18] ZHA X W. Bidirectional quantum controlled teleportation via five-qubit cluster state [J]. International Journal of Theoretical Physics, 2013, 52(6): 1740-1744.
- [19] PAYMAN K. Asymmetric bidirectional controlled quantum teleportation using eight qubit cluster state[J]. International Journal of Theoretical Physics, 2022, 61: 17.
- [20] ZHOU R G, LING C P. Asymmetric cyclic controlled quantum teleportation by using nine-qubit entangled state [J]. International Journal of Theoretical Physics, 2021, 60: 3435-3459.
- [21] WANG J W, SHU L. Bidirectional quantum controlled teleportation of qudit state via partially entangled GHZ-type states [J]. International Journal of Modern Physics B, 2015, 29(18): 1550122.
- [22] JIANG Y L, ZHOU R G, HAO D Y, et al. Bidirectional controlled quantum teleportation of three-qubit state by a new entangled eleven-qubit state [J]. International Journal of Theoretical Physics, 2021, 60: 3618-3630.
- [23] YUAN H, LIU X Y, PAN G Z. Analyses and optimizing of bidirectional quantum teleportation using a five-qubit cluster state as quantum channel [J]. Laser Physics Letters, 2022, 19(12): 4632-4639.
- [24] 赵慧, 赵静云. 多体量子系统中 2 类特殊图的可分性 [J]. 北京工业大学学报, 2018, 44(8): 1152-1156.
ZHAO H, ZHAO J Y. Separability of two classes of special graphs in multipartite quantum systems [J]. Journal of Beijing University of Technology, 2018, 44(8): 1152-1156. (in Chinese)
- [25] PATRYK L B, PAUL S. Catalytic quantum teleportation [J]. Physical Review Letters, 2021, 127(8): 080502.
- [26] WU F, BAI M Q, ZHANG Y C, et al. Cyclic and cyclic controlled quantum teleportation in a high-dimension system [J]. International Journal of Quantum Information, 2020, 18(4): 2050012.
- [27] 邵忠良, 龙银香. 基于真七粒子纠缠态实现受控双向非对称量子隐形传态 [J]. 量子电子学报, 2020, 37(1): 34-42.
SHAO Z L, LONG Y X. Controlled-bidirectional asymmetric quantum teleportation based on true seven-particle entanglement [J]. Journal of Quantum Electronics, 2020, 37(1): 34-42. (in Chinese)
- [28] FENG Z Y. Asymmetric bidirectional controlled quantum teleportation of three-qubit and four-qubit states [J]. Advance in Mathematical Physics, 2022, 2022(13): 3828446.

(责任编辑 梁洁)