doi:10.11959/j.issn.1000-436x.2015221

多方控制量子通信协议

常利伟[1,2]，郑世慧[1,2]，谷利泽[1,2]，雷敏[1,2]，杨义先[1,2]
(1.北京邮电大学 信息安全中心，北京 100876；2.北京邮电大学 灾备技术国家工程实验室，北京 100876)

摘 要：为了满足远距离多节点量子网络的需求，分别利用最大纠缠信道和部分纠缠信道构造了 2 个多方控制量子通信协议。最大纠缠信道时，利用投影测量实现多方控制四粒子 χ-态远程制备；部分纠缠信道时，利用联合酉操作和最优 POVM 实现多方控制四粒子 χ-态远程制备。理论推导表明，第一个协议的效率达到 100%且优于其他协议，第二协议的效率被有效提高且 2 种测量方法的构造方法可被用于同类协议。

关键词：多方控制协议；四粒子 χ-态；联合酉操作；最优 POVM 测量
中图分类号：TN911 **文献标识码**：A

Multi-party controlled quantum communication protocol

CHANG Li-wei[1,2], ZHENG Shi-hui[1,2], GU Li-ze[1,2], LEI Min[1,2], YANG Yi-xian[1,2]
(1. Information Security Research Center, Beijing University of Posts and Telecommunications, Beijing 100876, China;
2. National Engineering Laboratory for Disaster Backup and Recovery,
Beijing University of Posts and Telecommunications, Beijing 100876, China)

Abstract: In order to satisfy the requirements of long-distance multi-node quantum networks，two multi-party controlledquantum communication protocols are put forward via maximally and partially entangled quantum channels. For the maximally entangled channels, projective measurements are used to realizemulti-party controlled joint remote preparation of an arbitrary four-qubitχ-state. For the partially entangled channels, collective unitary operations and optimal positive operator-valued measures are used to realize multi-party controlled joint remote preparation of an arbitrary four-qubitχ-state.The theoretical analysis shows that the efficiency of the first scheme can be up to 100% which is suprior to that of others. In addition, the efficiency of the second scheme is effectively improved and the way to be used to construct two kinds of measurement methods can be utilized in the similar protocols.

Key words: multiparty controlled protocol; four-qubit χ-state; joint unitary operation; optimal positive operator-valued measure

1 引言

近几年，随着量子技术的快速发展，量子通信引起了社会各界的广泛关注。量子通信协议研究成为一个研究热点。量子远程态制备被认为是量子通信的重要组成部分。最初是由一些学者们同时提出[1~3]，量子远程态制备允许一个发送者在局域操作和经典通信的帮助下发送一个已知量子态给远方接收者。到目前为止，随着大量相关协议被提出，量子远程态制备获得深入的发展[4~8]。

为了防止目标态的全部信息泄露，包含多个发送者的远程量子态制备协议被研究人员提出，称为联合远程量子态制备。一般而言，联合远程量子态制备协议包含 2 个或更多位于不同地方的参与者。目标态被秘密地分割成许多份以确保其安全。在过去 10 年间，研究人员从不同的角度深入研究了联

收稿日期：2014-08-07；**修回日期**：2015-04-10
基金项目：国家自然科学基金资助项目(61370194, 61202082, 61121061)；中央高校基金资助项目(BUPT2012RC0219, BUPT 2013RC0311)
Foundation Items: The National Natural Science Foundation of China (61370194, 61202082, 61121061); Fundamental Research Funds for the Central Universities (BUPT2012RC0219, BUPT2013RC0311)

合远程量子态制备[9~13]。

众所周知，目前控制信息处理是量子通信研究的一个热点。因此，一个新概念——控制远程态制备被提出[14]。控制者参与整个协议执行过程却无需知道目标态的任何信息。控制者监督整个执行过程、决定协议是否成功且控制者采用的测量算符往往较简单，使控制远程态制备适合被用于远距离多节点的量子网络。随后，王等人给出一个一粒子和两粒子任意量子态控制远程制备协议[15]，陈等人提出一个两粒子和三粒子任意量子态控制远程制备协议[16]。由于一粒子态、两粒子态和三粒子态远程制备已经被学者们广泛研究，四粒子χ-态研究较少，因此，本文介绍 2 个任意四粒子 χ-态多方控制远程制备协议。本文的研究成果可能有助于量子网络的发展[17,18]。

2 利用 GHZ 类态构造多方控制四粒子 χ-态远程制备协议

本节利用 GHZ 类态作为量子信道给出一个任意四粒子 χ-态控制远程制备协议。该协议非常有意义，因为该协议的成功率达到百分之百。

协议中，有 $N+1$ 个合法参与者通常称为 Alice、Bob、Dick 和 $N-2$ 个控制者，简记为 C_1，C_2，…，C_{N-2}，其中 Alice 和 Bob 是 2 个位于不同地方的发送者，他们分别拥有量子态的振幅信息和相位信息。控制者 C_l $(1,\cdots,N-2)$ 无需拥有目标态的任何信息，但他们参与整个协议的执行过程。

Dick 是一个远方的接收者(注意控制者的数目可以根据实际需求随时调整)。

如图 1 所示，发送者 Alice 和 Bob 需要做的是在控制者 C_l $(1,\cdots,N-2)$ 监督下帮助远方的接收者 Dick 制备一个任意四粒子 χ-态。目标态被表示如下

$$\begin{aligned}|\Phi\rangle = {} & \lambda_0|0000\rangle + \lambda_1 e^{i\theta_1}|0011\rangle + \lambda_2 e^{i\theta_2}|0101\rangle + \\ & \lambda_3 e^{i\theta_3}|0110\rangle + \lambda_4 e^{i\theta_4}|1001\rangle + \lambda_5 e^{i\theta_5}|1010\rangle + \\ & \lambda_6 e^{i\theta_6}|1100\rangle + \lambda_7 e^{i\theta_7}|1111\rangle \end{aligned} \quad (1)$$

其中，λ_i 和 $\phi_i \in [0,2\pi](i=0,1,\cdots,7)$ 是实数，所有参数满足归一化条件 $\sum_{i=0}^{7}\lambda_i^2 = 1$。$|\Phi\rangle$ 所携带信息为 $S=\{\lambda_i,\phi_i\}$，它被分割成 2 个子集 $S_1=\{\lambda_i\}$ 和 $S_2=\{\phi_i\}$，满足从 S_1 或 S_2 中不能推导出 S。这里假设 S_1 仅被 Alice 知道，S_2 仅被 Bob 知道。然而控制者 C_l 不拥有任何有关目标态的信息。

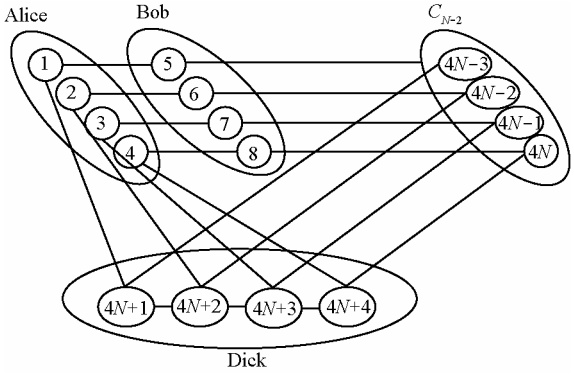

图 1 多方控制 χ-态远程制备协议

所有合法参与者共享 4 个 GHZ 类态作为量子信道，具体如下

$$\begin{aligned}|\Psi\rangle_{1,5,9,\cdots,4N+1} &= \frac{1}{\sqrt{2}}\sum_{j}^{0,1}|j\rangle^{\otimes N+1} \\ |\Psi\rangle_{2,6,10,\cdots,4N+2} &= \frac{1}{\sqrt{2}}\sum_{j}^{0,1}|j\rangle^{\otimes N+1} \\ |\Psi\rangle_{3,7,11,\cdots,4N+3} &= \frac{1}{\sqrt{2}}\sum_{j}^{0,1}|j\rangle^{\otimes N+1} \\ |\Psi\rangle_{4,8,12,\cdots,4N+4} &= \frac{1}{\sqrt{2}}\sum_{j}^{0,1}|j\rangle^{\otimes N+1} \end{aligned} \quad (2)$$

发送者 Alice 拥有粒子 $(1,2,3,4)$，Bob 拥有粒子 $(5,6,7,8)$，且每个控制者 C_l 控制 4 个粒子 $(4(l+1)+1,4(l+1)+2,4(l+1)+3,4(l+1)+4)$, $(l=1,2,\cdots,N-2)$。粒子 $(4N+1,4N+2,4N+3,4N+4)$ 属于接收者 Dick。

如图 2 所示，协议需要以下 4 步完成，其中每个黑点表示一个量子态，纠缠态被实线连接；P_A、P_B 和 P_{C_l} 表示一些合适的投影测量，U_D 表示一些泡利操作。

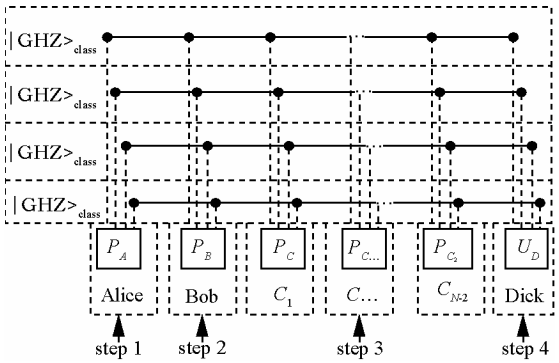

图 2 最大纠缠信道多方控制 χ-态远程制备实现

step1 Alice 需要做的是对自己拥有的 4 个粒子 $(1,2,3,4)$ 实施一个投影测量。测量完成后，她通过经典信道公布她的测量结果。不妨假设 Alice 和

Dick 预先约定好经典信息"0000"对应于测量结果$|\alpha_0\rangle$("0001" 对应于$|\alpha_1\rangle$，…，"1111"对应于$|\alpha_{15}\rangle$)。

Alice 选取一组正交基$\{|\alpha_i\rangle, i=0,1,\cdots,15\}$作为测量基，该测量基具体表示为

$$\begin{pmatrix}|\alpha_0\rangle\\|\alpha_1\rangle\\|\alpha_2\rangle\\|\alpha_3\rangle\\|\alpha_4\rangle\\|\alpha_5\rangle\\|\alpha_6\rangle\\|\alpha_7\rangle\end{pmatrix}=\boldsymbol{H}\begin{pmatrix}|0000\rangle\\|0011\rangle\\|0101\rangle\\|0110\rangle\\|1001\rangle\\|1010\rangle\\|1100\rangle\\|1111\rangle\end{pmatrix},\quad\begin{pmatrix}|\alpha_8\rangle\\|\alpha_9\rangle\\|\alpha_{10}\rangle\\|\alpha_{11}\rangle\\|\alpha_{12}\rangle\\|\alpha_{13}\rangle\\|\alpha_{14}\rangle\\|\alpha_{15}\rangle\end{pmatrix}=\boldsymbol{H}\begin{pmatrix}|0001\rangle\\|0010\rangle\\|0100\rangle\\|0111\rangle\\|1000\rangle\\|1011\rangle\\|1101\rangle\\|1110\rangle\end{pmatrix}\tag{3}$$

其中，

$$\boldsymbol{H}=\begin{pmatrix}\lambda_0&\lambda_1&\lambda_2&\lambda_3&\lambda_4&\lambda_5&\lambda_6&\lambda_7\\\lambda_1&-\lambda_0&\lambda_3&-\lambda_2&\lambda_5&-\lambda_4&\lambda_7&-\lambda_6\\\lambda_2&-\lambda_3&-\lambda_0&\lambda_1&-\lambda_6&\lambda_7&\lambda_4&-\lambda_5\\\lambda_3&\lambda_2&-\lambda_1&-\lambda_0&\lambda_7&\lambda_6&-\lambda_5&-\lambda_4\\\lambda_4&-\lambda_5&\lambda_6&-\lambda_7&-\lambda_0&\lambda_1&-\lambda_2&\lambda_3\\\lambda_5&\lambda_4&-\lambda_7&-\lambda_6&-\lambda_1&-\lambda_0&\lambda_3&\lambda_2\\\lambda_6&-\lambda_7&-\lambda_4&\lambda_5&\lambda_2&-\lambda_3&-\lambda_0&\lambda_1\\\lambda_7&\lambda_6&\lambda_5&\lambda_4&-\lambda_3&-\lambda_2&-\lambda_1&-\lambda_0\end{pmatrix}\tag{4}$$

因此初始量子信道可以被重写为

$$\begin{aligned}|q\rangle&=\frac{1}{4}[(|0\rangle^{N+1}+|1\rangle^{N+1})\otimes(|0\rangle^{N+1}+|1\rangle^{N+1})\otimes\\&(|0\rangle^{N+1}+|1\rangle^{N+1})\otimes(|0\rangle^{N+1}+|1\rangle^{N+1})]\\&=\frac{1}{4}[|\alpha_0\rangle(\lambda_0|0000\rangle^N+\lambda_1|0011\rangle^N+\lambda_2|0101\rangle^N+\\&\lambda_3|0110\rangle^N+\lambda_4|1001\rangle^N+\lambda_5|1010\rangle^N+\lambda_6|1100\rangle^N+\\&\lambda_7|1111\rangle^N)+|\alpha_8\rangle(\lambda_0|0001\rangle^N+\lambda_1|0010\rangle^N+\\&\lambda_2|0100\rangle^N+\lambda_3|0111\rangle^N+\lambda_4|1000\rangle^N+\lambda_5|1011\rangle^N+\\&\lambda_6|1101\rangle^N+\lambda_7|1110\rangle^N)+|\alpha_1\rangle(\lambda_1|0000\rangle^N-\\&\lambda_0|0011\rangle^N+\lambda_3|0101\rangle^N-\lambda_2|0110\rangle^N+\lambda_5|1001\rangle^N-\\&\lambda_4|1010\rangle^N+\lambda_7|1100\rangle^N-\lambda_6|1111\rangle^N)+\\&|\alpha_9\rangle(\lambda_1|0001\rangle^N-\lambda_0|0010\rangle^N+\lambda_3|0100\rangle^N-\\&\lambda_2|0111\rangle^N+\lambda_5|1000\rangle^N-\lambda_4|1011\rangle^N+\lambda_7|1101\rangle^N-\\&\lambda_6|1110\rangle^N)+|\alpha_2\rangle(\lambda_2|0000\rangle^N-\lambda_3|0011\rangle^N-\\&\lambda_0|0101\rangle^N+\lambda_1|0110\rangle^N-\lambda_6|1001\rangle^N+\\&\lambda_7|1010\rangle^N+\lambda_4|1100\rangle^N-\lambda_5|1111\rangle^N)+\\&|\alpha_{10}\rangle(\lambda_2|0001\rangle^N-\lambda_3|0010\rangle^N-\lambda_0|0100\rangle^N+\\&\lambda_1|0111\rangle^N-\lambda_6|1000\rangle^N+\lambda_7|1011\rangle^N+\lambda_4|1101\rangle^N-\\&\lambda_5|1110\rangle^N)+|\alpha_3\rangle(\lambda_3|0000\rangle^N+\lambda_2|0011\rangle^N-\\&\lambda_1|0101\rangle^N-\lambda_0|0110\rangle^N+\lambda_7|1001\rangle^N+\lambda_6|1010\rangle^N-\\&\lambda_5|1100\rangle^N-\lambda_4|1111\rangle^N)+|\alpha_{11}\rangle(\lambda_3|0001\rangle^N+\\&\lambda_2|0010\rangle^N-\lambda_1|0100\rangle^N-\lambda_0|0111\rangle^N+\lambda_7|1000\rangle^N+\\&\lambda_6|1011\rangle^N-\lambda_5|1101\rangle^N-\lambda_4|1110\rangle^N)+\\&|\alpha_4\rangle(\lambda_4|0000\rangle^N-\lambda_5|0011\rangle^N+\lambda_6|0101\rangle^N-\\&\lambda_7|0110\rangle^N-\lambda_0|1001\rangle^N+\lambda_1|1010\rangle^N-\lambda_2|1100\rangle^N+\\&\lambda_3|1111\rangle^N)+|\alpha_{12}\rangle(\lambda_4|0001\rangle^N-\lambda_5|0010\rangle^N+\\&\lambda_6|0100\rangle^N-\lambda_7|0111\rangle^N-\lambda_0|1000\rangle^N+\lambda_1|1011\rangle^N-\\&\lambda_2|1101\rangle^N+\lambda_3|1110\rangle^N)+|\alpha_5\rangle(\lambda_5|0000\rangle^N+\\&\lambda_4|0011\rangle^N-\lambda_7|0101\rangle^N-\lambda_6|0110\rangle^N-\lambda_1|1001\rangle^N-\\&\lambda_0|1010\rangle^N+\lambda_3|1100\rangle^N+\lambda_2|1111\rangle^N)+\\&|\alpha_{13}\rangle(\lambda_5|0001\rangle^N+\lambda_4|0010\rangle^N-\lambda_7|0100\rangle^N-\\&\lambda_6|0111\rangle^N-\lambda_1|1000\rangle^N-\lambda_0|1011\rangle^N+\lambda_3|1101\rangle^N+\\&\lambda_2|1110\rangle^N)+|\alpha_6\rangle(\lambda_6|0000\rangle^N-\lambda_7|0011\rangle^N-\\&\lambda_4|0101\rangle^N+\lambda_5|0110\rangle^N+\lambda_2|1001\rangle^N-\lambda_3|1010\rangle-\\&\lambda_0|1100\rangle^N+\lambda_1|1111\rangle^N)+|\alpha_{14}\rangle(\lambda_6|0001\rangle^N-\\&\lambda_7|0010\rangle^N-\lambda_4|0100\rangle^N+\lambda_5|0111\rangle^N+\lambda_2|1000\rangle^N-\\&\lambda_3|1011\rangle^N-\lambda_0|1101\rangle^N+\lambda_1|1110\rangle^N)+\\&|\alpha_7\rangle(\lambda_7|0000\rangle^N+\lambda_6|0011\rangle^N+\lambda_5|0101\rangle^N+\\&\lambda_4|0110\rangle^N-\lambda_3|1001\rangle^N-\lambda_2|1010\rangle^N-\\&\lambda_1|1100\rangle^N-\lambda_0|1111\rangle^N)+|\alpha_{15}\rangle(\lambda_7|0001\rangle^N+\\&\lambda_6|0010\rangle^N+\lambda_5|0100\rangle^N+\lambda_4|0111\rangle^N-\\&\lambda_3|1000\rangle^N-\lambda_2|1011\rangle^N-\lambda_1|1101\rangle^N-\lambda_0|1110\rangle^N)]\end{aligned}\tag{5}$$

step2　根据 Alice 的测量结果，Bob 从基$\{|\beta_j^{(k)}\rangle, j=0,1,\cdots,15\}$中选取一组正交基对自己的粒子(5,6,7,8)实施四粒子投影测量。注意 Alice 的测量结果和 Bob 所选测量基的对应关系满足如下形式

$$\begin{aligned}&|\alpha_i\rangle_{1234}\rightarrow\{|\beta_j^{(k)}\rangle_{5678},(k=i,i<8,j=0,1,\cdots,7)\};\\&|\alpha_i\rangle_{1234}\rightarrow\{|\beta_{j+8}^{(k)}\rangle_{5678},(k=i\ mod\ 8,i\geqslant 8,j=0,1,\cdots,7)\}\end{aligned}\tag{6}$$

可供 Bob 选取的测量基总共有 16 组正交基，具体如下

$$\begin{pmatrix}|\beta_0^{(k)}\rangle\\|\beta_1^{(k)}\rangle\\|\beta_2^{(k)}\rangle\\|\beta_3^{(k)}\rangle\\|\beta_4^{(k)}\rangle\\|\beta_5^{(k)}\rangle\\|\beta_6^{(k)}\rangle\\|\beta_7^{(k)}\rangle\end{pmatrix}=\frac{1}{2\sqrt{2}}\boldsymbol{G}^{(k)}\begin{pmatrix}|0000\rangle\\|0011\rangle\\|0101\rangle\\|0110\rangle\\|1001\rangle\\|1010\rangle\\|1100\rangle\\|1111\rangle\end{pmatrix},$$

$$\begin{pmatrix}|\beta_8^{(k)}\rangle\\|\beta_9^{(k)}\rangle\\|\beta_{10}^{(k)}\rangle\\|\beta_{11}^{(k)}\rangle\\|\beta_{12}^{(k)}\rangle\\|\beta_{13}^{(k)}\rangle\\|\beta_{14}^{(k)}\rangle\\|\beta_{15}^{(k)}\rangle\end{pmatrix}=\frac{1}{2\sqrt{2}}\boldsymbol{G}^{(k)}\begin{pmatrix}|0001\rangle\\|0010\rangle\\|0100\rangle\\|0111\rangle\\|1000\rangle\\|1011\rangle\\|1101\rangle\\|1110\rangle\end{pmatrix} \tag{7}$$

其中，每个 $\boldsymbol{G}^{(k)}$ 是一个 8×8 的矩阵。

$$\begin{cases}\boldsymbol{G}^{(0)}=\boldsymbol{G}_{(1,\ r_1,\ r_2,\ r_3,\ r_4,\ r_5,\ r_6,\ r_7)},\boldsymbol{G}^{(1)}=\boldsymbol{G}_{(r_1,\ 1,\ r_3,\ r_2,\ r_5,\ r_4,\ r_7,\ r_6)},\\ \boldsymbol{G}^{(2)}=\boldsymbol{G}_{(r_2,\ r_3,\ 1,\ r_1,\ r_6,\ r_7,\ r_4,\ r_5)},\boldsymbol{G}^{(3)}=\boldsymbol{G}_{(r_3,\ r_2,\ r_1,\ 1,\ r_7,\ r_6,\ r_5,\ r_4)},\\ \boldsymbol{G}^{(4)}=\boldsymbol{G}_{(r_4,\ r_5,\ r_6,\ r_7,\ 1,\ r_1,\ r_2,\ r_3)},\boldsymbol{G}^{(5)}=\boldsymbol{G}_{(r_5,\ r_4,\ r_7,\ r_6,\ r_1,\ 1,\ r_3,\ r_2)},\\ \boldsymbol{G}^{(6)}=\boldsymbol{G}_{(r_6,\ r_7,\ r_4,\ r_5,\ r_2,\ r_3,\ 1,\ r_1)},\boldsymbol{G}^{(7)}=\boldsymbol{G}_{(r_7,\ r_6,\ r_5,\ r_4,\ r_3,\ r_2,\ r_1,\ 1)}\end{cases} \tag{8}$$

其中，$r_j=\mathrm{e}^{-\mathrm{i}\theta_j}(j=0,1,\cdots,7)$ 和 $\theta_0=0$。为了清楚地认识 $\boldsymbol{G}^{(k)}$，不妨令 $\boldsymbol{G}=\boldsymbol{G}_{(a_1,a_2,a_3,a_4,a_5,a_6,a_7,a_8)}$，有如下通式

$$\boldsymbol{G}=\begin{pmatrix}a_1&a_2&a_3&a_4&a_5&a_6&a_7&a_8\\a_1&-a_2&a_3&-a_4&a_5&-a_6&a_7&-a_8\\a_1&-a_2&-a_3&a_4&-a_5&a_6&a_7&-a_8\\a_1&a_2&-a_3&-a_4&a_5&a_6&-a_7&-a_8\\a_1&-a_2&a_3&-a_4&-a_5&a_6&-a_7&a_8\\a_1&a_2&-a_3&-a_4&-a_5&-a_6&a_7&a_8\\a_1&-a_2&-a_3&a_4&a_5&-a_6&-a_7&a_8\\a_1&a_2&a_3&a_4&-a_5&-a_6&-a_7&-a_8\end{pmatrix} \tag{9}$$

当 Bob 测量完成时，Bob 通过经典信道广播他的测量结果。假设 Bob 和 Dick 预先约定经典比特串 000, 001, 010, 011, 100, 101, 110 和 111 分别表示测量结果 $|\beta_0^{(k)}\rangle(|\beta_8^{(k)}\rangle)$，$|\beta_1^{(k)}\rangle(|\beta_9^{(k)}\rangle)$，$|\beta_2^{(k)}\rangle(|\beta_{10}^{(k)}\rangle)$，$|\beta_3^{(k)}\rangle(|\beta_{11}^{(k)}\rangle)$，$|\beta_4^{(k)}\rangle(|\beta_{12}^{(k)}\rangle)$，$|\beta_5^{(k)}\rangle(|\beta_{13}^{(k)}\rangle)$，$|\beta_6^{(k)}\rangle(|\beta_{14}^{(k)}\rangle)$ 和 $\beta_7^{(k)}\rangle(|\beta_{15}^{(k)}\rangle)$。

不失一般性，假设 Alice 的测量结果为 $|\alpha_2\rangle_{1234}$，Bob 选取相应测量基 $\{|\beta_j^{(2)}\rangle,j=0,1,\cdots,7\}$ 测量自己手中的粒子 (5,6,7,8)，于是剩下的量子信道表示为

$$\begin{aligned}&\frac{1}{4}(\lambda_2|0000\rangle^N-\lambda_3|0011\rangle^N-\lambda_0|0101\rangle^N+\lambda_1|0110\rangle^N-\\&\lambda_6|1001\rangle^N+\lambda_7|1010\rangle^N+\lambda_4|1100\rangle^N-\lambda_5|1111\rangle^N)\\&=\frac{1}{8\sqrt{2}}[|\beta_0^{(2)}\rangle(\lambda_2\mathrm{e}^{\mathrm{i}\theta_2}|0000\rangle^{N-1}-\lambda_3\mathrm{e}^{\mathrm{i}\theta_3}|0011\rangle^{N-1}-\\&\lambda_0\mathrm{e}^{\mathrm{i}\theta_0}|0101\rangle^{N-1}+\lambda_1\mathrm{e}^{\mathrm{i}\theta_1}|0110\rangle^{N-1}-\lambda_6\mathrm{e}^{\mathrm{i}\theta_6}|1001\rangle^{N-1}+\\&\lambda_7\mathrm{e}^{\mathrm{i}\theta_7}|1010\rangle^{N-1}+\lambda_4\mathrm{e}^{\mathrm{i}\theta_4}|1100\rangle^{N-1}-\lambda_5\mathrm{e}^{\mathrm{i}\theta_5}|1111\rangle^{N-1})+\\&|\beta_1^{(2)}\rangle(\lambda_2\mathrm{e}^{\mathrm{i}\theta_2}|0000\rangle^{N-1}+\lambda_3\mathrm{e}^{\mathrm{i}\theta_3}|0011\rangle^{N-1}-\\&\lambda_0\mathrm{e}^{\mathrm{i}\theta_0}|0101\rangle^{N-1}-\lambda_1\mathrm{e}^{\mathrm{i}\theta_1}|0110\rangle^{N-1}-\lambda_6\mathrm{e}^{\mathrm{i}\theta_6}|1001\rangle^{N-1}-\\&\lambda_7\mathrm{e}^{\mathrm{i}\theta_7}|1010\rangle^{N-1}+\lambda_4\mathrm{e}^{\mathrm{i}\theta_4}|1100\rangle^{N-1}+\lambda_5\mathrm{e}^{\mathrm{i}\theta_5}|1111\rangle^{N-1})+\\&|\beta_2^{(2)}\rangle(\lambda_2\mathrm{e}^{\mathrm{i}\theta_2}|0000\rangle^{N-1}+\lambda_3\mathrm{e}^{\mathrm{i}\theta_3}|0011\rangle^{N-1}+\\&\lambda_0\mathrm{e}^{\mathrm{i}\theta_0}|0101\rangle^{N-1}+\lambda_1\mathrm{e}^{\mathrm{i}\theta_1}|0110\rangle^{N-1}+\lambda_6\mathrm{e}^{\mathrm{i}\theta_6}|1001\rangle^{N-1}+\\&\lambda_7\mathrm{e}^{\mathrm{i}\theta_7}|1010\rangle^{N-1}+\lambda_4\mathrm{e}^{\mathrm{i}\theta_4}|1100\rangle^{N-1}+\lambda_5\mathrm{e}^{\mathrm{i}\theta_5}|1111\rangle^{N-1})+\\&|\beta_3^{(2)}\rangle(\lambda_2\mathrm{e}^{\mathrm{i}\theta_2}|000\rangle^{N-1}-\lambda_1\mathrm{e}^{\mathrm{i}\theta_1}|0110\rangle^{N-1}+\\&\lambda_6\mathrm{e}^{\mathrm{i}\theta_6}|1001\rangle^{N-1}-\lambda_7\mathrm{e}^{\mathrm{i}\theta_7}|1010\rangle^{N-1}-\lambda_3\mathrm{e}^{\mathrm{i}\theta_3}|0011\rangle^{N-1}+\\&\lambda_0\mathrm{e}^{\mathrm{i}\theta_0}|0101\rangle^{N-1}-\lambda_4\mathrm{e}^{\mathrm{i}\theta_4}|1100\rangle^{N-1}+\lambda_5\mathrm{e}^{\mathrm{i}\theta_5}|1111\rangle^{N-1})+\\&|\beta_4^{(2)}\rangle(\lambda_2\mathrm{e}^{\mathrm{i}\theta_2}|0000\rangle^{N-1}+\lambda_3\mathrm{e}^{\mathrm{i}\theta_3}|0011\rangle^{N-1}-\\&\lambda_0\mathrm{e}^{\mathrm{i}\theta_0}|0101\rangle^{N-1}-\lambda_1\mathrm{e}^{\mathrm{i}\theta_1}|0110\rangle^{N-1}+\lambda_6e^{\mathrm{i}\theta_6}|1001\rangle^{N-1}+\\&\lambda_7\mathrm{e}^{\mathrm{i}\theta_7}|1010\rangle^{N-1}-\lambda_4\mathrm{e}^{\mathrm{i}\theta_4}|1100\rangle^{N-1}-\lambda_5e^{\mathrm{i}\theta_5}|1111\rangle^{N-1})+\\&|\beta_5^{(2)}\rangle(\lambda_2\mathrm{e}^{\mathrm{i}\theta_2}|0000\rangle^{N-1}-\lambda_3\mathrm{e}^{\mathrm{i}\theta_3}|0011\rangle^{N-1}+\\&\lambda_0\mathrm{e}^{\mathrm{i}\theta_0}|0101\rangle^{N-1}-\lambda_1\mathrm{e}^{\mathrm{i}\theta_1}|0110\rangle^{N-1}+\lambda_6\mathrm{e}^{\mathrm{i}\theta_6}|1001\rangle^{N-1}-\\&\lambda_7\mathrm{e}^{\mathrm{i}\theta_7}|1010\rangle^{N-1}+\lambda_4\mathrm{e}^{\mathrm{i}\theta_4}|1100\rangle^{N-1}-\lambda_5\mathrm{e}^{\mathrm{i}\theta_5}|1111\rangle^{N-1})+\\&|\beta_6^{(2)}\rangle(\lambda_2\mathrm{e}^{\mathrm{i}\theta_2}|0000\rangle^{N-1}+\lambda_3\mathrm{e}^{\mathrm{i}\theta_3}|0011\rangle^{N-1}+\\&\lambda_0\mathrm{e}^{\mathrm{i}\theta_0}|0101\rangle^{N-1}+\lambda_1\mathrm{e}^{\mathrm{i}\theta_1}|0110\rangle^{N-1}-\lambda_6\mathrm{e}^{\mathrm{i}\theta_6}|1001\rangle^{N-1}-\\&\lambda_7\mathrm{e}^{\mathrm{i}\theta_7}|1010\rangle^{N-1}-\lambda_4\mathrm{e}^{\mathrm{i}\theta_4}|1100\rangle^{N-1}-\lambda_5\mathrm{e}^{\mathrm{i}\theta_5}|1111\rangle^{N-1})+\\&|\beta_7^{(2)}\rangle(\lambda_2\mathrm{e}^{\mathrm{i}\theta_2}|0000\rangle^{N-1}-\lambda_3\mathrm{e}^{\mathrm{i}\theta_3}|0011\rangle^{N-1}-\\&\lambda_0\mathrm{e}^{\mathrm{i}\theta_0}|0101\rangle^{N-1}+\lambda_1\mathrm{e}^{\mathrm{i}\theta_1}|0110\rangle^{N-1}+\lambda_6\mathrm{e}^{\mathrm{i}\theta_6}|1001\rangle^{N-1}-\\&\lambda_7\mathrm{e}^{\mathrm{i}\theta_7}|1010\rangle^{N-1}-\lambda_4\mathrm{e}^{\mathrm{i}\theta_4}|1100\rangle^{N-1}+\lambda_5\mathrm{e}^{\mathrm{i}\theta_5}|1111\rangle^{N-1})\end{aligned} \tag{10}$$

step3 每个控制者 C_l 利用测量基 $\{|\gamma_0\rangle,|\gamma_1\rangle,|\gamma_2\rangle,|\gamma_3\rangle\}$ 依次实施两粒子投影测量。测量完成时，控制者 C_l 公布他的测量结果。前 2 个粒子和后 2 个粒子的测量结果依次记为 ξ_1^l 和 ξ_2^l，特别注意 $\xi_i^l(i=1,2)\in\{00,01,10,11\}$。每个控制者选取的测量基都是正交基

$$\begin{cases}|\gamma_0\rangle=\frac{1}{2}(|00\rangle+|01\rangle+|10\rangle+|11\rangle)\\|\gamma_1\rangle=\frac{1}{2}(|00\rangle-|01\rangle-|10\rangle+|11\rangle)\\|\gamma_2\rangle=\frac{1}{2}(|00\rangle-|01\rangle+|10\rangle-|11\rangle)\\|\gamma_3\rangle=\frac{1}{2}(|00\rangle+|01\rangle-|10\rangle-|11\rangle)\end{cases}. \tag{11}$$

不失一般性，假设 Alice 的测量结果为

$|\alpha_2\rangle_{1234}$，Bob 的测量结果为$|\beta_3^{(2)}\rangle_{5678}$，所有控制者 C_l 的测量结果为 $\xi_i^l(i=1,2)$。令 $m_i=\bigoplus_{l=1}^{N-2}\xi_i^l$，如果 $m_1=01$，$m_2=10$，接收者拥有的 4 个粒子塌缩为

$$|\Phi'\rangle=\frac{1}{2^{2N-1}\sqrt{2}}(\lambda_2 e^{i\theta_2}|0000\rangle+\lambda_3 e^{i\theta_3}|0011\rangle+\lambda_0 e^{i\theta_0}|0101\rangle+\lambda_1 e^{i\theta_1}|0110\rangle-\lambda_6 e^{i\theta_6}|1001\rangle-\lambda_7 e^{i\theta_7}|1010\rangle-\lambda_4 e^{i\theta_4}|1100\rangle-\lambda_5 e^{i\theta_5}|1111\rangle) \quad (12)$$

step4　根据发送者 Alice、Bob 和控制者 $C_l(l=1,2,\cdots,N-2)$的测量结果，接收者 Dick 通过对自己手中的粒子分别实施合适的酉操作可以得到目标态即获得所传递的信息。

如表 1 所示，Dick 对自己手中的粒子实施酉操作 $\sigma_{4N+1}^z\otimes\sigma_{4N+2}^x\otimes I_{4N+3}\otimes\sigma_{4N+4}^x$，他可以得到目标态

$$|\Phi\rangle=\frac{1}{2^{2N-1}\sqrt{2}}(\lambda_0 e^{i\theta_0}|0000\rangle+\lambda_1 e^{i\theta_1}|0011\rangle+\lambda_2 e^{i\theta_2}|0101\rangle+\lambda_3 e^{i\theta_3}|0110\rangle+\lambda_4 e^{i\theta_4}|1001\rangle+\lambda_5 e^{i\theta_5}|1010\rangle+\lambda_6 e^{i\theta_6}|1100\rangle+\lambda_7 e^{i\theta_7}|1111\rangle) \quad (13)$$

表 1　接收者 Dick 应实施的恢复操作

m_1	m_2	U_D
00	00	$I_{4N+1}\otimes\sigma_{4N+2}^x\sigma_{4N+2}^z\otimes I_{4N+3}\otimes\sigma_{4N+4}^x\sigma_{4N+4}^z$
00	01	$\sigma_{4N+1}^z\otimes\sigma_{4N+2}^x\otimes I_{4N+3}\otimes\sigma_{4N+4}^x\sigma_{4N+4}^z$
00	10	$I_{4N+1}\otimes\sigma_{4N+2}^x\sigma_{4N+2}^z\otimes I_{4N+3}\otimes\sigma_{4N+4}^x$
00	11	$\sigma_{4N+1}^z\otimes\sigma_{4N+2}^x\otimes I_{4N+3}\otimes\sigma_{4N+4}^x$
01	00	$\sigma_{4N+1}^z\otimes\sigma_{4N+2}^x\otimes I_{4N+3}\otimes\sigma_{4N+4}^x\sigma_{4N+4}^z$
01	01	$I_{4N+1}\otimes\sigma_{4N+2}^x\sigma_{4N+2}^z\otimes I_{4N+3}\otimes\sigma_{4N+4}^x\sigma_{4N+4}^z$
01	10	$\sigma_{4N+1}^z\otimes\sigma_{4N+2}^x\otimes I_{4N+3}\otimes\sigma_{4N+4}^x$
01	11	$I_{4N+1}\otimes\sigma_{4N+2}^x\sigma_{4N+2}^z\otimes I_{4N+3}\otimes\sigma_{4N+4}^x$
10	00	$I_{4N+1}\otimes\sigma_{4N+2}^x\otimes I_{4N+3}\otimes\sigma_{4N+4}^x\sigma_{4N+4}^z$
10	01	$I_{4N+1}\otimes\sigma_{4N+2}^x\otimes\sigma_{4N+3}^z\otimes\sigma_{4N+4}^x$
10	10	$I_{4N+1}\otimes\sigma_{4N+2}^x\otimes I_{4N+3}\otimes\sigma_{4N+4}^x$
10	11	$\sigma_{4N+1}^z\otimes\sigma_{4N+2}^x\sigma_{4N+2}^z\otimes I_{4N+3}\otimes\sigma_{4N+4}^x$
11	00	$I_{4N+1}\otimes\sigma_{4N+2}^x\otimes\sigma_{4N+3}^z\otimes\sigma_{4N+4}^x$
11	01	$I_{4N+1}\otimes\sigma_{4N+2}^x\otimes I_{4N+3}\otimes\sigma_{4N+4}^x\sigma_{4N+4}^z$
11	10	$\sigma_{4N+1}^z\otimes\sigma_{4N+2}^x\sigma_{4N+2}^z\otimes I_{4N+3}\otimes\sigma_{4N+4}^x$
11	11	$I_{4N+1}\otimes\sigma_{4N+2}^x\otimes I_{4N+3}\otimes\sigma_{4N+4}^x$

总之，对所有 Alice、Bob 和控制者 C_l 的 $16\times8\times16^{N-2}$ 种测量结果，接收者 Dick 所拥有的粒子总塌缩为下列 2 种量子态之一

$$\frac{1}{2^{2N-1}\sqrt{2}}(\lambda_{i_0}e^{i\theta_{i_0}}|0000\rangle\circ\lambda_{i_1}e^{i\theta_{i_1}}|0011\rangle\circ\lambda_{i_2}e^{i\theta_{i_2}}|0101\rangle\circ\lambda_{i_3}e^{i\theta_{i_3}}|0110\rangle\circ\lambda_{i_4}e^{i\theta_{i_4}}|1001\rangle\circ\lambda_{i_5}e^{i\theta_{i_5}}|1010\rangle\circ\lambda_{i_6}e^{i\theta_{i_6}}|1100\rangle\circ\lambda_{i_7}e^{i\theta_{i_7}}|1111\rangle) \quad (14)$$

或者

$$\frac{1}{2^{2N-1}\sqrt{2}}(\lambda_{i_0}e^{i\theta_{i_0}}|0001\rangle\circ\lambda_{i_1}e^{i\theta_{i_1}}|0010\rangle\circ\lambda_{i_2}e^{i\theta_{i_2}}|0100\rangle\circ\lambda_{i_3}e^{i\theta_{i_3}}|0111\rangle\circ\lambda_{i_4}e^{i\theta_{i_4}}|1000\rangle\circ\lambda_{i_5}e^{i\theta_{i_5}}|1011\rangle\circ\lambda_{i_6}e^{i\theta_{i_6}}|1101\rangle\circ\lambda_{i_7}e^{i\theta_{i_7}}|1110\rangle) \quad (15)$$

其中，$(\lambda_{i_0},\lambda_{i_1},\lambda_{i_2},\lambda_{i_3},\lambda_{i_4},\lambda_{i_5},\lambda_{i_6},\lambda_{i_7})$ 是式(4)中矩阵 $\boldsymbol{H}$ 的行向量，$(e^{i\theta_{i_0}},e^{i\theta_{i_1}},e^{i\theta_{i_2}},e^{i\theta_{i_3}},e^{i\theta_{i_4}},e^{i\theta_{i_5}},e^{i\theta_{i_6}},e^{i\theta_{i_7}})$ 是式(8)中对应于 Bob 所选取的测量基转换矩阵 $\boldsymbol{G}^{(k)}$ 对应共轭转置矩阵的列向量。式(14)和式(15)中总是有 4 个“+”和 4 个“−”。接收者 Dick 总能利用合适的酉操作恢复目标态，并得到发送者传送的信息，也就是说这个协议的成功率为

$$16\times8\times16^{N-2}\times\left(\frac{1}{2^{2N-1}\sqrt{2}}\right)^2=1 \quad (16)$$

如表 1 所示，当发送者 Alice 和 Bob 的测量结果分别为$|\alpha_2\rangle_{1234}$和$|\beta_3^{(2)}\rangle_{5678}$时，控制者 C_l 测量结果和接收者 Dick 所实施酉操作的关系。

3　利用非最大纠缠信道构造多方控制四粒子 χ-态远程制备协议

由于最大纠缠态不稳定，将拓展上述协议到更一般的情形——非最大纠缠态作为量子信道。

不失一般性，假设连接所有合法参与者之间的量子信道为

$$|\Psi\rangle_{1,5,9,\cdots,4N+1}=\sum_j^{0,1}a_j|j\rangle^{\otimes N+1}$$
$$|\Psi\rangle_{2,6,10,\cdots,4N+2}=\sum_j^{0,1}b_j|j\rangle^{\otimes N+1}$$
$$|\Psi\rangle_{3,7,11,\cdots,4N+3}=\sum_j^{0,1}c_j|j\rangle^{\otimes N+1}$$
$$|\Psi\rangle_{4,8,12,\cdots,4N+4}=\sum_j^{0,1}d_j|j\rangle^{\otimes N+1} \quad (17)$$

其中，a_j、b_j、c_j 和 d_j 都是实数，且满足归一化条件 $a_0^2+a_1^2=1$，$b_0^2+b_1^2=1$，$c_0^2+c_1^2=1$ 和 $d_0^2+d_1^2=1$。

粒子 $(1,2,3,4)$ 属于发送者 Alice，粒子 $(5,6,7,8)$ 属于发送者 Bob，且 4 个粒子 $(4(l+1)+1,\ 4(l+1)+2,\ 4(l+1)+3, 4(l+1)+4)$, 被控制者 C_l 控制 $(l=1,2,\cdots,N-2)$。接收者 Dick 拥有 4 个粒子 $(4N+1,\ 4N+2,\ 4N+3,\ 4N+4)$。

假设发送者 Alice 和 Bob 在控制者 C_l 监督下帮助接收者 Dick 制备的仍然是四粒子 χ-态。和前面的协议一样，发送者 Alice 和 Bob 分别知道目标态的振幅信息和相位信息，控制者不知道任何目标态信息。

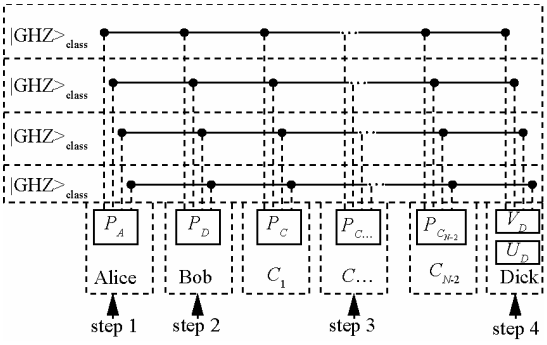

图 3 部分纠缠信道多方控制 χ-态远程制备实现

如图 3 所示，每个黑点表示一个量子态，纠缠态被实线连接；P_A、P_B 和 P_{C_l} 表示一些合适的投影测量，U_D 表示一些泡利操作，V_D 表示最优 POVM 测量或一个特定恢复联合酉操作。首先发送者 Alice 对自己手中的粒子 $(1,2,3,4)$ 实施一个四粒子投影测量并通过经典信道公布她的测量结果。其次发送者 Bob 根据 Alice 的测量结果，选择对应的测量基测量自己手中的粒子 $(5,6,7,8)$ 并通过经典信道公布测量结果。然后每个控制者利用测量基 $\{|\gamma_0\rangle,|\gamma_1\rangle,|\gamma_2\rangle,|\gamma_3\rangle\}$ 依次对自己手中的 4 个粒子实施两粒子投影测量并通过经典信道将自己的测量结果 $\xi_i^l\in\{00,01,10,11\}$ 告诉接收者 Dick。最后接收者 Dick 根据 Alice、Bob 和控制者 C_l 的测量结果，选取合适的酉操作恢复目标态 $|\Phi\rangle$。

为清楚地理解本文协议，不失一般性，给出一个具体的例子。当 Alice 的测量结果为 $|\alpha_2\rangle_{1234}$，Bob 选择对应的测量基 $\{|\beta_j^{(2)}\rangle,\ j=0,1,\cdots,7\}$ 测量他手中的粒子 $(5,6,7,8)$ 并得到测量结果 $|\beta_3^{(2)}\rangle_{5678}$。如果所有控制者 C_l 的测量结果为 $m_1=01$ 和 $m_2=10$，则接收者 Dick 手中的粒子塌缩为

$$|\Phi'\rangle=\frac{1}{2^{2N-3}\sqrt{2}}(a_0b_0c_0d_0\lambda_2\mathrm{e}^{\mathrm{i}\theta_2}|0000\rangle+a_0b_0c_1d_1\lambda_3\mathrm{e}^{\mathrm{i}\theta_3}|0011\rangle+a_0b_1c_0d_1\lambda_0\mathrm{e}^{\mathrm{i}\theta_0}|0101\rangle+a_0b_1c_1d_0\lambda_1\mathrm{e}^{\mathrm{i}\theta_1}|0110\rangle-a_1b_0c_0d_1\lambda_6\mathrm{e}^{\mathrm{i}\theta_6}|1001\rangle-a_1b_0c_1d_0\lambda_7\mathrm{e}^{\mathrm{i}\theta_7}|1010\rangle-a_1b_1c_0d_0\lambda_4\mathrm{e}^{\mathrm{i}\theta_4}|1100\rangle-a_1b_1c_1d_1\lambda_5\mathrm{e}^{\mathrm{i}\theta_5}|1111\rangle) \tag{18}$$

接下来，接收者 Dick 将使用 2 种不同的方法恢复目标态。

方法 1 为了恢复目标态，接收者 Dick 引入一个辅助粒子 A 其初始态为 $|0\rangle_A$，他对自己手中的粒子 $(4N+1,\ 4N+2,\ 4N+3,\ A)$ 实施联合酉变换 U'。有序测量基为 $\{|0000\rangle,\ |0010\rangle,\ |0100\rangle,\ |0110\rangle,\ |1000\rangle,\ |1010\rangle,\ |1100\rangle,\ |1110\rangle,\ |0001\rangle,\ |0011\rangle,\ |0101\rangle,\ |0111\rangle,\ |1001\rangle,\ |1011\rangle,\ |1101\rangle,\ |1111\rangle\}$。不失一般性，假设 $|a_1b_1c_1d_1|$ 是集合 $\{|a_0b_0c_0d_0|,\ |a_0b_0c_1d_1|,\ |a_0b_1c_0d_1|,\ |a_1b_0c_0d_1|,\ |a_0b_1c_1d_0|,\ |a_1b_0c_1d_0|,\ |a_1b_1c_0d_0|,\ |a_1b_1c_1d_1|\}$ 中的最大值。U' 有如下形式

$$U'=\begin{pmatrix}\boldsymbol{D}_1 & \boldsymbol{D}_2\\ \boldsymbol{D}_2 & -\boldsymbol{D}_1\end{pmatrix} \tag{19}$$

其中，$\boldsymbol{D}_i(i=1,2)$ 是一个矩阵且可表示为如下形式

$$\begin{aligned}\boldsymbol{D}_1&=diag(d_0,d_1,d_2,d_3,d_4,d_5,d_6,d_7)\\ \boldsymbol{D}_2&=diag(\sqrt{1-d_0^2},\sqrt{1-d_1^2},\sqrt{1-d_2^2},\sqrt{1-d_3^2},\sqrt{1-d_4^2},\\ &\qquad\sqrt{1-d_5^2},\sqrt{1-d_6^2},\sqrt{1-d_7^2})\end{aligned} \tag{20}$$

满足

$$d_0=\frac{a_1b_1c_1d_1}{a_0b_0c_0d_0},d_1=\frac{a_1b_1c_1d_1}{a_0b_0c_1d_1},d_2=\frac{a_1b_1c_1d_1}{a_0b_1c_0d_1},d_3=\frac{a_1b_1c_1d_1}{a_0b_1c_1d_0},$$
$$d_4=\frac{a_1b_1c_1d_1}{a_1b_0c_0d_1},d_5=\frac{a_1b_1c_1d_1}{a_1b_0c_1d_0},d_6=\frac{a_1b_1c_1d_1}{a_1b_1c_0d_0},d_7=1$$

因此 Dick 手中的粒子将演化为

$$\begin{aligned}U'(|\Phi'\rangle\otimes|0\rangle_A)=&\frac{1}{2^{2N-3}\sqrt{2}}[a_1b_1c_1d_1(\lambda_2\mathrm{e}^{\mathrm{i}\theta_2}|0000\rangle+\\ &\lambda_3\mathrm{e}^{\mathrm{i}\theta_3}|0011\rangle+\lambda_0\mathrm{e}^{\mathrm{i}\theta_0}|0101\rangle+\lambda_1\mathrm{e}^{\mathrm{i}\theta_1}|0110\rangle-\\ &\lambda_6\mathrm{e}^{\mathrm{i}\theta_6}|1001\rangle-\lambda_7e^{i\theta_7}|1010\rangle-\lambda_4\mathrm{e}^{\mathrm{i}\theta_4}|1100\rangle-\\ &\lambda_5\mathrm{e}^{\mathrm{i}\theta_5}|1111\rangle)\otimes|0\rangle_A+(\sqrt{1-d_0^2}\lambda_2\mathrm{e}^{\mathrm{i}\theta_2}|0000\rangle+\\ &\sqrt{1-d_1^2}\lambda_3\mathrm{e}^{\mathrm{i}\theta_3}|0011\rangle+\sqrt{1-d_2^2}\lambda_0\mathrm{e}^{\mathrm{i}\theta_0}|0101\rangle+\\ &\sqrt{1-d_3^2}\lambda_1\mathrm{e}^{\mathrm{i}\theta_1}|0110\rangle-\sqrt{1-d_4^2}\lambda_6\mathrm{e}^{\mathrm{i}\theta_6}|1001\rangle-\\ &\sqrt{1-d_5^2}\lambda_7\mathrm{e}^{\mathrm{i}\theta_7}|1010\rangle-\sqrt{1-d_6^2}\lambda_4\mathrm{e}^{\mathrm{i}\theta_4}|1100\rangle)\otimes|1\rangle_A]\end{aligned} \tag{21}$$

最后 Dick 利用测量基 $\{|0\rangle,|1\rangle\}$ 测量辅助粒子 A，如果态 $|1\rangle$ 被测得，他手中的粒子将塌缩为错

误态，也就是协议失败；否则 Dick 手中的粒子能够成功演化为目标态$|\Phi\rangle$。因此 Dick 获得成功的概率为

$$p=(\frac{1}{2^{2N-3}\sqrt{2}})^2\times|a_1b_1c_1d_1|^2=\frac{1}{2\times4^{2N-3}}|a_1b_1c_1d_1|^2 \quad (22)$$

方法 2　为了恢复目标态，接收者 Dick 引入 3 个辅助粒子 A、B 和 C，它们处于初始态 1000〉，并实施 3 个受控非操作，其中粒子 $4N+1, 4N+2$ 和 $4N+3$ 为控制比特，而粒子 A、B 和 C 为目标比特。3 个受控非操作完成后，量子态$|\Phi'\rangle$变为

$$\begin{aligned}|\Phi''\rangle=&a_0b_0c_0d_0\lambda_2e^{i\theta_2}|0000000\rangle+\\&a_0b_0c_1d_1\lambda_3e^{i\theta_3}|0011001\rangle+\\&a_0b_1c_0d_1\lambda_0e^{i\theta_0}|0101010\rangle+\\&a_0b_1c_1d_0\lambda_1e^{i\theta_1}|0110011\rangle-\\&a_1b_0c_0d_1\lambda_6e^{i\theta_6}|1001100\rangle-\\&a_1b_0c_1d_0\lambda_7e^{i\theta_7}|1010101\rangle-\\&a_1b_1c_0d_0\lambda_4e^{i\theta_4}|1100110\rangle-\\&a_1b_1c_1d_1\lambda_5e^{i\theta_5}|1111111\rangle\end{aligned} \quad (23)$$

为了方便，不妨令 $\alpha=a_0b_0c_0d_0$，$\beta=a_0b_0c_1d_1$，$\gamma=a_0b_1c_0d_1$，$\delta=a_0b_1c_1d_0$，$\varepsilon=a_1b_0c_0d_1$，$\varsigma=a_1b_0c_1d_0$，$\zeta=a_1b_1c_0d_0$ 和 $\eta=a_1b_1c_1d_1$。量子态$|\Phi''\rangle$进一步可以被表示为

$$|\Phi''\rangle=\frac{1}{8}\sum_{j=1}^{8}|\Phi_j\rangle_{4N+1,4N+2,4N+3,4N+4}|H_j\rangle_{ABC} \quad (24)$$

其中，

$$\begin{aligned}|\Phi_1\rangle=&\lambda_2e^{i\theta_2}|0000\rangle+\lambda_3e^{i\theta_3}|0011\rangle+\lambda_0e^{i\theta_0}|0101\rangle+\\&\lambda_1e^{i\theta_1}|0110\rangle-\lambda_6e^{i\theta_6}|1001\rangle-\lambda_7e^{i\theta_7}|1010\rangle-\\&\lambda_4e^{i\theta_4}|1100\rangle-\lambda_5e^{i\theta_5}|1111\rangle\end{aligned}$$

$$\begin{aligned}|H_1\rangle=&(\alpha|000\rangle+\beta|001\rangle+\gamma|010\rangle+\delta|011\rangle-\\&\varepsilon|100\rangle-\varsigma|101\rangle-\zeta|110\rangle-\eta|111\rangle)\end{aligned}$$

$$\begin{aligned}|\Phi_2\rangle=&\lambda_2e^{i\theta_2}|0000\rangle-\lambda_3e^{i\theta_3}|0011\rangle+\lambda_0e^{i\theta_0}|0101\rangle-\\&\lambda_1e^{i\theta_1}|0110\rangle-\lambda_6e^{i\theta_6}|1001\rangle+\lambda_7e^{i\theta_7}|1010\rangle-\\&\lambda_4e^{i\theta_4}|1100\rangle+\lambda_5e^{i\theta_5}|1111\rangle\end{aligned}$$

$$\begin{aligned}|H_2\rangle=&(\alpha|000\rangle-\beta|001\rangle+\gamma|010\rangle-\delta|011\rangle-\\&\varepsilon|100\rangle+\varsigma|101\rangle-\zeta|110\rangle+\eta|111\rangle)\end{aligned}$$

$$\begin{aligned}|\Phi_3\rangle=&\lambda_2e^{i\theta_2}|0000\rangle-\lambda_3e^{i\theta_3}|0011\rangle-\lambda_0e^{i\theta_0}|0101\rangle+\\&\lambda_1e^{i\theta_1}|0110\rangle+\lambda_6e^{i\theta_6}|1001\rangle-\lambda_7e^{i\theta_7}|1010\rangle-\\&\lambda_4e^{i\theta_4}|1100\rangle+\lambda_5e^{i\theta_5}|1111\rangle\end{aligned}$$

$$\begin{aligned}|H_3\rangle=&(\alpha|000\rangle-\beta|001\rangle-\gamma|010\rangle+\delta|011\rangle+\\&\varepsilon|100\rangle-\varsigma|101\rangle-\zeta|110\rangle+\eta|111\rangle)\end{aligned}$$

$$\begin{aligned}|\Phi_4\rangle=&\lambda_2e^{i\theta_2}|0000\rangle+\lambda_3e^{i\theta_3}|0011\rangle-\lambda_0e^{i\theta_0}|0101\rangle-\\&\lambda_1e^{i\theta_1}|0110\rangle-\lambda_6e^{i\theta_6}|1001\rangle-\lambda_7e^{i\theta_7}|1010\rangle+\\&\lambda_4e^{i\theta_4}|1100\rangle+\lambda_5e^{i\theta_5}|1111\rangle\end{aligned}$$

$$\begin{aligned}|H_4\rangle=&(\alpha|000\rangle+\beta|001\rangle-\gamma|010\rangle-\delta|011\rangle-\\&\varepsilon|100\rangle-\varsigma|101\rangle+\zeta|110\rangle+\eta|111\rangle)\end{aligned}$$

$$\begin{aligned}|\Phi_5\rangle=&\lambda_2e^{i\theta_2}|0000\rangle-\lambda_3e^{i\theta_3}|0011\rangle+\lambda_0e^{i\theta_0}|0101\rangle-\\&\lambda_1e^{i\theta_1}|0110\rangle+\lambda_6e^{i\theta_6}|1001\rangle-\lambda_7e^{i\theta_7}|1010\rangle+\\&\lambda_4e^{i\theta_4}|1100\rangle-\lambda_5e^{i\theta_5}|1111\rangle\end{aligned}$$

$$\begin{aligned}|H_5\rangle=&(\alpha|000\rangle-\beta|001\rangle+\gamma|010\rangle-\delta|011\rangle+\\&\varepsilon|100\rangle-\varsigma|101\rangle+\zeta|110\rangle-\eta|111\rangle)\end{aligned}$$

$$\begin{aligned}|\Phi_6\rangle=&\lambda_2e^{i\theta_2}|0000\rangle+\lambda_3e^{i\theta_3}|0011\rangle-\lambda_0e^{i\theta_0}|0101\rangle-\\&\lambda_1e^{i\theta_1}|0110\rangle+\lambda_6e^{i\theta_6}|1001\rangle+\lambda_7e^{i\theta_7}|1010\rangle-\\&\lambda_4e^{i\theta_4}|1100\rangle-\lambda_5e^{i\theta_5}|1111\rangle\end{aligned}$$

$$\begin{aligned}|H_6\rangle=&(\alpha|000\rangle+\beta|001\rangle-\gamma|010\rangle-\delta|011\rangle+\\&\varepsilon|100\rangle+\varsigma|101\rangle-\zeta|110\rangle-\eta|111\rangle)\end{aligned}$$

$$\begin{aligned}|\Phi_7\rangle=&\lambda_2e^{i\theta_2}|0000\rangle-\lambda_3e^{i\theta_3}|0011\rangle-\lambda_0e^{i\theta_0}|0101\rangle+\\&\lambda_1e^{i\theta_1}|0110\rangle-\lambda_6e^{i\theta_6}|1001\rangle+\lambda_7e^{i\theta_7}|1010\rangle+\\&\lambda_4e^{i\theta_4}|1100\rangle-\lambda_5e^{i\theta_5}|1111\rangle\end{aligned}$$

$$\begin{aligned}|H_7\rangle=&(\alpha|000\rangle-\beta|001\rangle-\gamma|010\rangle+\delta|011\rangle-\\&\varepsilon|100\rangle+\varsigma|101\rangle+\zeta|110\rangle-\eta|111\rangle)\end{aligned}$$

$$\begin{aligned}|\Phi_8\rangle=&\lambda_2e^{i\theta_2}|0000\rangle+\lambda_3e^{i\theta_3}|0011\rangle+\lambda_0e^{i\theta_0}|0101\rangle+\\&\lambda_1e^{i\theta_1}|0110\rangle+\lambda_6e^{i\theta_6}|1001\rangle+\lambda_7e^{i\theta_7}|1010\rangle+\\&\lambda_4e^{i\theta_4}|1100\rangle+\lambda_5e^{i\theta_5}|1111\rangle\end{aligned}$$

$$\begin{aligned}|H_8\rangle=&(\alpha|000\rangle+\beta|001\rangle+\gamma|010\rangle+\delta|011\rangle+\\&\varepsilon|100\rangle+\varsigma|101\rangle+\zeta|110\rangle+\eta|111\rangle)\end{aligned} \quad (25)$$

显然，如果非正交态$|H_j\rangle_{ABC}$ $(j=1,2,\cdots,8)$能够被区分，则接收者 Dick 能够准确知道态$|\Phi_j\rangle(j=1,2,\cdots,8)$。为了区分态$|H_j\rangle_{ABC}$，Dick 对粒子 A、B 和 C 实施最优 POVM[19,20]。POVM 具体为如下形式

$$P_i=\frac{1}{x}|M_i\rangle\langle M_i|(i=1,2,\cdots,8),\ \boldsymbol{P}_9=I-\frac{1}{x}\sum_{i=1}^{8}|M_i\rangle\langle M_i| \quad (26)$$

其中，

$$|M_1\rangle=\frac{1}{\sqrt{\xi}}(\frac{1}{\alpha}|000\rangle+\frac{1}{\beta}|001\rangle+\frac{1}{\gamma}|010\rangle+\frac{1}{\delta}|011\rangle-\frac{1}{\varepsilon}|100\rangle-\frac{1}{\varsigma}|101\rangle-\frac{1}{\zeta}|110\rangle-\frac{1}{\eta}|111\rangle)$$

$$|M_2\rangle=\frac{1}{\sqrt{\xi}}(\frac{1}{\alpha}|000\rangle-\frac{1}{\beta}|001\rangle+\frac{1}{\gamma}|010\rangle-\frac{1}{\delta}|011\rangle-\frac{1}{\varepsilon}|100\rangle+\frac{1}{\varsigma}|101\rangle-\frac{1}{\zeta}|110\rangle+\frac{1}{\eta}|111\rangle)$$

$$|M_3\rangle=\frac{1}{\sqrt{\xi}}(\frac{1}{\alpha}|000\rangle-\frac{1}{\beta}|001\rangle-\frac{1}{\gamma}|010\rangle+\frac{1}{\delta}|011\rangle+\frac{1}{\varepsilon}|100\rangle-\frac{1}{\varsigma}|101\rangle-\frac{1}{\zeta}|110\rangle+\frac{1}{\eta}|111\rangle),$$

$$|M_4\rangle=\frac{1}{\sqrt{\xi}}(\frac{1}{\alpha}|000\rangle+\frac{1}{\beta}|001\rangle-\frac{1}{\gamma}|010\rangle-\frac{1}{\delta}|011\rangle-\frac{1}{\varepsilon}|100\rangle-\frac{1}{\varsigma}|101\rangle+\frac{1}{\zeta}|110\rangle+\frac{1}{\eta}|111\rangle)$$

$$|M_5\rangle=\frac{1}{\sqrt{\xi}}(\frac{1}{\alpha}|000\rangle-\frac{1}{\beta}|001\rangle+\frac{1}{\gamma}|010\rangle-\frac{1}{\delta}|011\rangle+\frac{1}{\varepsilon}|100\rangle-\frac{1}{\varsigma}|101\rangle+\frac{1}{\zeta}|110\rangle-\frac{1}{\eta}|111\rangle)$$

$$|M_6\rangle=\frac{1}{\sqrt{\xi}}(\frac{1}{\alpha}|000\rangle+\frac{1}{\beta}|001\rangle-\frac{1}{\gamma}|010\rangle-\frac{1}{\delta}|011\rangle+\frac{1}{\varepsilon}|100\rangle+\frac{1}{\varsigma}|101\rangle-\frac{1}{\zeta}|110\rangle-\frac{1}{\eta}|111\rangle),$$

$$|M_7\rangle=\frac{1}{\sqrt{\xi}}(\frac{1}{\alpha}|000\rangle-\frac{1}{\beta}|001\rangle-\frac{1}{\gamma}|010\rangle+\frac{1}{\delta}|011\rangle-\frac{1}{\varepsilon}|100\rangle+\frac{1}{\varsigma}|101\rangle+\frac{1}{\zeta}|110\rangle-\frac{1}{\eta}|111\rangle)$$

$$|M_8\rangle=\frac{1}{\sqrt{\xi}}(\frac{1}{\alpha}|000\rangle+\frac{1}{\beta}|001\rangle+\frac{1}{\gamma}|010\rangle+\frac{1}{\delta}|011\rangle+\frac{1}{\varepsilon}|100\rangle+\frac{1}{\varsigma}|101\rangle+\frac{1}{\zeta}|110\rangle+\frac{1}{\eta}|111\rangle),$$

$$\xi=\frac{1}{\alpha^2}+\frac{1}{\beta^2}+\frac{1}{\gamma^2}+\frac{1}{\delta^2}+\frac{1}{\varepsilon^2}+\frac{1}{\varsigma^2}+\frac{1}{\zeta^2}+\frac{1}{\eta^2} \tag{27}$$

其中，I 表示单位操作，且系数 x、α、β、γ、δ、ε、ς、ζ 和 η 相关，必须确保测量算符 $\boldsymbol{P}_9$ 为正定算符。为了准确确定 x，根据式(26)和式(27)，将算符 $\boldsymbol{P}_1\sim\boldsymbol{P}_8$ 写成矩阵的形式。容易发现算符 $\boldsymbol{P}_9$ 为一个如下对角矩阵

$$\boldsymbol{P}_9=\begin{pmatrix}1-\frac{8}{x\xi\alpha^2} & 0 & 0 & 0 & 0 & 0 & 0 & 0\\ 0 & 1-\frac{8}{x\xi\beta^2} & 0 & 0 & 0 & 0 & 0 & 0\\ 0 & 0 & 1-\frac{8}{x\xi\gamma^2} & 0 & 0 & 0 & 0 & 0\\ 0 & 0 & 0 & 1-\frac{8}{x\xi\delta^2} & 0 & 0 & 0 & 0\\ 0 & 0 & 0 & 0 & 1-\frac{8}{x\xi\varepsilon^2} & 0 & 0 & 0\\ 0 & 0 & 0 & 0 & 0 & 1-\frac{8}{x\xi\varsigma^2} & 0 & 0\\ 0 & 0 & 0 & 0 & 0 & 0 & 1-\frac{8}{x\xi\zeta^2} & 0\\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1-\frac{8}{x\xi\eta^2}\end{pmatrix} \tag{28}$$

显然，因为算符 $\boldsymbol{P}_9$ 是一个正定算符，容易计算得到 x 满足不等式 $x\geqslant\frac{8}{\xi\mu^2}$，设 μ^2 为集合 $\{\alpha^2,\beta^2,\gamma^2,\delta^2,\varepsilon^2,\varsigma^2,\zeta^2,\eta^2\}$ 中最小元素。实施完 POVM 测量，接收者 Dick 以如下概率得到量子态 $\boldsymbol{\Phi}_i$

$$p_i=\langle\Phi''|P_i|\Phi''\rangle={}_{ABC}\langle H_i|P_i|H_i\rangle_{ABC}/64=\frac{1}{x\xi} \tag{29}$$

然而将以概率 $1-\frac{8}{x\xi}$ 得到算符 $\boldsymbol{P}_9$ 的测量结果，此时接收者 Dick 不能将自己手中的粒子恢复为目

标态。只有接收者 Dick 能够区分态$|H_j\rangle$，则接收者能将自己手中的粒子恢复为目标态。当$x=\frac{8}{\xi\mu^2}$时，接收者将以最大概率$p_{\max}$恢复目标态

$$p_{\max}=\frac{1}{2\times4^{2N-3}}\times8\times\frac{\mu^2}{8}=\frac{\mu^2}{2\times4^{2N-3}} \tag{30}$$

对于所有$16\times8\times16^{N-2}$中情形每一种情况，接收者 Dick 实施合适的酉操作以概率$\frac{\mu^2}{2\times4^{2N-3}}$将自己手中的粒子恢复为目标态。因此，采用这种方法该协议的成功率为$16\mu^2$。采用方法 1，协议的成功率为$16|a_1b_1c_1d_1|^2$。

表 2　　2 种方法效果比较

方法	恢复操作维数	辅助粒子个数	协议成功效率
方法 1	16	1	$16\|a_1b_1c_1d_1\|^2$
方法 2	8	3	$16\mu^2$

4　协议的实验可行性

现在分析协议的实验可行性。本文方案以多粒子 GHZ 态为量子信道资源。Zou 等人利用单光子源、线性光学元件和光子探测器理论上给出一个多光子 GHZ 态生成方案[21]，随后 Yao 和 Monz 等实验实现了 8 光子 GHZ 态和 14 离子 GHZ 态[22,23]。此外，2 种方案实现的关键是四粒子投影测量，三粒子 POVM 测量和五粒子特定联合酉操作。到目前为止，对投影测量的研究已经取得一定成果。已经证明投影测量能够分解为一系列弱测量，仅引起初始态较小变化[24, 25]。其次 POVM 测量已经被学者和专家通过光学的方式解释[26, 27]，最近学者们进一步通过光学方式和研究 POVM 测量的兼容性实现 POVM 测量[28, 29]。最后专家已经证明任何联合酉操作都能分解成单粒子旋转操作和受控非门操作。其中单粒子旋转操作实现已经被大量文献研究[30, 31]，且受控非操作通过光学的方式已经被成功实现[32~35]。因此有理由相信本文方案在现有技术条件下能够实现。

5　结束语

为了进一步丰富量子网络通信的发展，研究怎样构造一些多方控制量子通信协议——任意四粒子 χ-态控制远程制备协议。利用 2 种不同的信道构造了 2 种方案。

在第一种方案中，最大纠缠态被作为量子信道，接收者只需实施简单的泡利操作就能够恢复目标态，获得发送者们传送的信息。此外，协议的成功率为百分之百。在第二种方案中，将第一种情形拓展为更一般的情形——非最大纠缠态作为量子信道。同时采用现存的 2 种方法恢复目标态，并从恢复操作维数、辅助粒子个数和协议成功率 3 个方面比较这 2 种方法。纵观上述 2 种方案不难发现，此类协议的共同特点为信道参数和测量方法决定协议的成功率，而控制者的个数影响协议的安全性。控制者越多协议的安全性越强，但是控制增多也会增大协议的通信资源消耗。

参考文献：

[1] LO H K. Classical-communication cost in distributed quantum information processing: a generalization of quantum communication complexity[J]. Phys Rev A, 2000, 62: 012313.

[2] PATI A K, Minimum classical bit for remote preparation and measurement of a qubit[J]. Phys Rev A, 2000, 63: 014302.

[3] BENNETT C H, VINCENZO D P, SHOR P W, *et al*. Remote state preparation[J]. Phys Rev Lett, 2001, 87: 077902.

[4] DEVETAK I, BERGER T. Low-entanglement remote state preparation[J]. Phys Rev Lett, 2001, 87: 197901.

[5] ZENG B, ZHANG P. Remote-state preparation in higher dimension and the parallelizable manifold [J]. Phys Rev A, 2002, 65:022316.

[6] DENG L, CHEN A X, XU Y Q. High efficient scheme for remote state preparation with cavity QED[J]. Chin Phys B, 2008, 17: 3725 -3728.

[7] MA S Y, TANG P, CHEN X B, *et al*. Schemes for remotely preparing a six-particle entangled cluster-type state[J]. Int J of Theor Phys, 2013, 52: 968-979.

[8] MA S Y, LUO M X, CHEN X B, *et al*. Schemes for remotely preparing an arbitrary four-qubit χ-state[J]. Quantum Inf Process, 2014, 13: 1951-965.

[9] WANG Y, JI X. Deterministic joint remote state preparation of arbitrary two- and three-qubit states[J]. Chin Phys B, 2013, 22: 020306.

[10] LUO M X, DENG Y. Joint remote preparation of an arbitrary 4-qubit *x*-state[J]. Int J Theor Phys, 2012, 51:3027-3036.

[11] MA S Y, TANG P, LUO M X. Schemes for remotely preparing Brown-type entangled state[J]. Int J of Quant Inf, 2013,11:1350042.

[12] CHANG L W, ZHENG S H, GU L Z, *et al*. Joint remote preparation of an arbitrary five-qubit Brown state via non-maximally entangled channels[J]. Chin Phys B, 2014, 23:090307.

[13] ZHOU N R, CHENG H L, TAO X Y, *et al*. Three-party remote state preparation schemes based on entanglement[J]. Quantum Inf Process, 2014, 13: 513-526.

[14] WANG Z Y, LIU Y M, ZUO X Q, *et al*. Controlled remote state preparation[J]. Commun Theor Phys, 2009, 52: 235-240.

[15] WANG D, YE L. Multiparty-controlled joint remote state prepara-

tion[J]. Quantum Inf Process, 2013, 12: 3223-3237.

[16] CHEN X B, MA S Y, SU Y, *et al*. Controlled remote state preparation of arbitrary two and three qublt states via the Brown state[J]. Quantum Inf Process, 2012, 11: 1653-1667.

[17] HAYASHI M, IWAMA K, NISHIMURA H, *et al*. Quantum Network Coding[R]. Lecture Notes in Computer Science, 2007.610-621.

[18] GONG L H, LIU Y, ZHOU N R. Novel quantum virtual private network scheme for PON via quantum secure direct communication[J]. Int J Theor Phys, 2013, 52: 3260-3268.

[19] HELSTROM C W. Quantum Dectection and Estimation Theory[M]. Academic Press New York, 1976.

[20] MAR T, HORODECKI P. Teleportation via generalized measurements and conclusive teleportation[EB/OL].http://arxiv.org/abs/quant-ph/9906039.

[21] ZOU X B, PAHLKE K, MATHIS W. Generation of a multi-photon Greenberger-horne-zeilinger state with linear optical elements and photon detectors[J]. J Opt B: Quantum Semiclass, 2005, 7 : 119-121.

[22] YAO X C, WANG T X, HE P X, *et al*. Observation of eight-photon entanglement[J]. Nature (London), 2012, 6: 224-228.

[23] MONZ T, SCHINDLER P. 14-qubit entanglement: creation and coherences[J]. Phys Rev L, 2011, 106: 130506 .

[24] AHARONOV Y, VAIDMAN L. Properties of a quantum system during the time interval between two measurements[J]. Phys Rev A, 1990, 41:11-20.

[25] JOHANSEN L M. Quantum theory of successive projective measurements[J]. Phys Rev A, 2007, 76: 012119.

[26] AHNERT S E, PAYNE M C. General implementation of all possible positive-operator-value measurements of single-photon polarization states[J]. Phys Rev A, 2005, 71: 012330.

[27] ZIMAN M, BUZEK V. Realization of positive-operator-valued measures using measurement-assisted programmable quantum processors[J]. Phys Rev A, 2005, 72: 022343.

[28] HAN Y, WU W, WU C W, *et al*. Realization of arbitrary positive-operator-value measurement of single atomic qubit via cavity QED[J]. Chin Phys Lett, 2008, 25: 4195-4198.

[29] KUNJWAL R, HEUNEN C, FRITZ T. Quantum realization of arbitrary joint measurability structures[J]. Phys Rev A, 2014, 89: 052126.

[30] RECK M, ZEILINGER A. Experimental realization of any discrete unitary operator[J]. Phys Rev L,1994,73:58-61.

[31] KNILL E, LAFLAMME R, MILBURN G J. A scheme for efficient quantum computation with linear optics[J]. Nature (London), 2001, 409: 46-52.

[32] PITTMAN T B, FITCH M J, JACOBS B C, FRANSON J D. Experimental controlled-NOT logic gate for single photons in the coincidence basis[J]. Phys Rev A, 2003, 68: 032316.

[33] OBRIEN J L, PRYDE G J, WHITE A G, *et al*. Demonstration of an all-optical quantum controlled-NOT gate[J]. Nature (London), 2004, 426:264-267.

[34] GAO W B, XU P, YAO X C. Experimental realization of a controlled-NOT gate with four-photon six-qubit cluster states[J]. Phys Rev L, 2010,104:020501.

[35] BISWAS K K, SAJEED S. Design and realization of a quantum controlled NOT gate using optical implementation[J]. International Journal of Advancements in Research & Technology, 2012,1: 2278-7763.

作者简介：

常利伟（1986-），男，山西朔州人，北京邮电大学博士生，主要研究方向为密码学。

郑世慧（1979-），女，山东日照人，北京邮电大学讲师，主要研究方向为密码分析与设计。

谷利泽（1965-），男，辽宁营口人，北京邮电大学副教授、硕士生导师，主要研究方向为信息安全和网络完全。

雷敏（1979-），男，江西瑞昌人，北京邮电大学博士生，主要研究方向为信息隐藏与隐写分析。

杨义先（1961-），男，四川盐亭人，北京邮电大学教授，博士生导师，主要研究方向为编码理论、密码学、信息安全、信号与信息处理。