将量子隐形传态看作量子信道的通信方式

贺转玲[1*]，孙苗[2]，曾晗[1]，贺岳星[1]

[1]国防科技大学信息通信学院，陕西 西安 710106；

[2]重庆师范大学计算机与信息科学学院，重庆 401331

摘要 一次一密经典通信方式存在密钥丢失的风险，在传输大量数据时密钥会很快消耗完，不适于大数据经典通信，同时量子隐形传态由于要区分四个 Bell 态，实现起来比较困难。考虑到量子信道不仅能传输量子信息，还可以传输经典信息，提出将量子隐形传态看作量子信道，进而传输经典信息序列。在传输的过程中将待传输的信息 0 和 1 分别编码为计算基矢态|0〉和|1〉，这样在保证安全性的基础上可以不停地生成密钥，适用于大数据通信，同时此方案只需区分两种 Bell 态，实现起来比较容易。

关键词 量子光学；量子隐形传态；Bell 基测量；量子信道；线性量子光学

中图分类号 O436 **文献标识码** A **doi**：10.3788/LOP56.232602

Communication Method Regarding Quantum Teleportation as Quantum Channel

He Zhuanling[1*], Sun Miao[2], Zeng Han[1], He Yuexing[1]

[1] *College of Information and Communication, National University of Defense Technology, Xi'an, Shaanxi* 710106, *China*;

[2] *College of Computer and Information Science, Chongqing Normal University, Chongqing* 401331, *China*

Abstract The classical one-time-pad communication method exhibits the disadvantage of key loss and the shortcoming that the key will be quickly exhausted when a large amount of data is transmitted, making it unsuitable for classical big data communication. Further, it is difficult to distinguish the four Bell states in quantum teleportation. This study considers quantum teleportation as a quantum channel that transmits classical information sequences because quantum channels not only transmit quantum information but also classical information. The transmitted data 0 and 1 are encoded as quantum states |0〉 and |1〉, respectively. The proposed scheme can continuously ensure security and generate keys, which is suitable for big data communication. Furthermore, this scheme only needs to distinguish between two kinds of Bell states, which can be easily implemented.

Key words quantum optics; quantum teleportation; Bell state measurement; quantum channel; linear quantum optics

OCIS codes 270.5565; 270.5585; 270.5568

1 引 言

人们的日常生活与通信有着密切的关系，随着科技的进步，通信的安全性越来越受到大家的关注。量子通信基于量子力学基本理论，在安全性上比微波经典通信好，于是成为信息科学的研究热点。量子通信是量子信息学的主要分支，主要包括量子隐形传态、密集编码、量子密钥分发等[1]，其中量子隐形传态是量子信息领域最引人注目的研究课题之一，它是一种结合经典通信和量子纠缠，实现远程信息传输的技术。自 1993 年美国科学家 Bennett 等[2]提出量子隐形传态的概念以来，国内外学者进

收稿日期：2019-04-12；**修回日期**：2019-05-15；**录用日期**：2019-06-03

基金项目：国家自然科学基金(11704412)、国防科大校内科研重点项目(zk17-02-09)、陕西省重点研发计划(2019ZDLGY09-01)

* **E-mail**：hezhuanling0612@126.com

行了大量的理论[3-5]和实验[6-10]研究。1997 年,潘建伟与波密斯特首次实现未知量子态的远程传输[11]。1998 年,Karlsson 等[12]提出可控量子隐形传态,以 GHZ 纠缠态作为量子信道,在控制者的协助下实现未知量子态的传送。清华大学和中国科学技术大学联合研究小组于 2009 年在北京八达岭与河北怀来之间实现了长达 16 km 的自由空间的量子隐形传态。潘建伟小组于 2012 年实现了百千米量级的自由空间量子隐形传态和纠缠分发。量子隐形传态也经历了多种方式的改变,由最初的二粒子最大纠缠态到多粒子最大纠缠态,由单向隐形传态到双向隐形传态[13-14]及可控隐形传态[15-16]等。

在实际过程中,要想成功实现量子隐形传态比较困难,同时考虑到一次一密经典通信方案会存在密钥丢失的风险,当需要传输的数据量比较大时,双方携带的密钥会很快消耗完。鉴于此需将量子隐形传态看作量子信道,传输由 0 和 1 组成的随机经典信息序列,这种方式一方面在保证安全性的基础上可以不停地生成密钥,另一方面在接收端 Bob 处只需区分两种 Bell 态,降低了 Bell 基测量的难度,实现起来比较容易。

2 张量表示的量子隐形传态

随着高维量子态的量子位的增加,穷举法显得无能为力,为了使隐形传态的表示简洁明了,常用张量表示量子隐形传态[17]。在量子隐形传态方案中,待传送的粒子表示为

$$|\varphi\rangle_{\mathrm{a}}=R^{i}|i\rangle=R^{0}|0\rangle+R^{1}|1\rangle,\tag{1}$$

式中:$|\varphi\rangle_{\mathrm{a}}$ 为粒子 a 的状态;i 为只能取 0 和 1 的变量;R^{i} 为取值 i 的几率幅。R^{i} 满足归一化条件,$R^{i}R_{i}^{*}=1$,其中 R_{i}^{*} 为 R^{i} 的共轭复数。

量子信道可表示为

$$|\varphi\rangle_{\mathrm{AB}}=X^{jk}|jk\rangle=X^{00}|00\rangle+X^{01}|01\rangle+X^{10}|10\rangle+X^{11}|11\rangle,\tag{2}$$

式中:X^{jk} 为取值为 $|jk\rangle$ 的几率幅;j、k 为只能取 0 和 1 的变量。X^{jk} 满足归一化条件,$X^{jk}X_{jk}^{*}=1$ 且 $X^{00}X^{11}\neq X^{01}X^{10}$,其中 X_{jk}^{*} 为 X^{jk} 的共轭复数。

则整个系统的量子态为

$$|\varphi\rangle_{\mathrm{tot}}=|\varphi\rangle_{\mathrm{a}}\otimes|\varphi\rangle_{\mathrm{AB}}=R^{i}X^{jk}|ijk\rangle_{\mathrm{aAB}},\tag{3}$$

式中:⊗为张量积。粒子 a 与 A 被分配给发送端 Alice 手中,粒子 B 被分配给接收端 Bob 手中。接下来 Alice 对粒子 a 和 A 进行 Bell 态测量,Bell 基的量子态可表示为

$$|\phi^{1}\rangle=\frac{1}{\sqrt{2}}(|00\rangle+|11\rangle),\tag{4}$$

$$|\phi^{2}\rangle=\frac{1}{\sqrt{2}}(|00\rangle-|11\rangle),\tag{5}$$

$$|\phi^{3}\rangle=\frac{1}{\sqrt{2}}(|01\rangle+|10\rangle),\tag{6}$$

$$|\phi^{4}\rangle=\frac{1}{\sqrt{2}}(|01\rangle-|10\rangle)。\tag{7}$$

在 $|\varphi\rangle_{\mathrm{tot}}$ 中粒子 a 和 A 是通过计算基矢表示的,这时需要通过变换矩阵将其用 Bell 基表示,计算基矢 $|00\rangle$,$|01\rangle$,$|10\rangle$,$|11\rangle$ 与 Bell 基 $|\phi^{1}\rangle$,$|\phi^{2}\rangle$,$|\phi^{3}\rangle$,$|\phi^{4}\rangle$ 之间的变换矩阵为

$$\boldsymbol{T}=\begin{pmatrix}T_{00}^{1}&T_{01}^{1}&T_{10}^{1}&T_{11}^{1}\\T_{00}^{2}&T_{01}^{2}&T_{10}^{2}&T_{11}^{2}\\T_{00}^{3}&T_{01}^{3}&T_{10}^{3}&T_{11}^{3}\\T_{00}^{4}&T_{01}^{4}&T_{10}^{4}&T_{11}^{4}\end{pmatrix}=\frac{1}{\sqrt{2}}\begin{pmatrix}1&0&0&1\\1&0&0&-1\\0&1&1&0\\0&1&-1&0\end{pmatrix}。\tag{8}$$

在 Bell 基的表示下,整个系统的量子态可以表示为 $|\varphi\rangle_{\mathrm{tot}}=R^{i}X^{jk}T_{ij}^{\alpha}|\alpha\rangle|k\rangle$,其中 T_{ij}^{α} 是 $\boldsymbol{T}$ 的元素,α 为 4 个 Bell 态中的一种。若令 $\sigma_{i}^{(\alpha)k}=X^{jk}T_{ij}^{\alpha}$,则 $|\varphi\rangle_{\mathrm{tot}}=R^{i}\sigma_{i}^{(\alpha)k}|\alpha\rangle|k\rangle$,记 $\sigma_{i}^{(\alpha)k}$ 为矩阵 $\boldsymbol{\sigma}^{\alpha}$ 的元素,则

$$\boldsymbol{\sigma}^{\alpha}=\boldsymbol{X}\boldsymbol{T}^{\alpha}=\begin{pmatrix}\sigma_{0}^{\alpha0}&\sigma_{1}^{\alpha0}\\\sigma_{0}^{\alpha1}&\sigma_{1}^{\alpha1}\end{pmatrix}=\begin{pmatrix}X^{00}&X^{10}\\X^{01}&X^{11}\end{pmatrix}\begin{pmatrix}T_{00}^{\alpha}&T_{10}^{\alpha}\\T_{01}^{\alpha}&T_{11}^{\alpha}\end{pmatrix},\tag{9}$$

式中:$\boldsymbol{X}$ 与量子信道参数有关,定义为通道参数矩阵;$\boldsymbol{\sigma}^{\alpha}$ 定义为变换矩阵;$\boldsymbol{T}^{\alpha}$ 对应不同的测量基,定义为测量矩阵。$\boldsymbol{T}^{\alpha}$ 可用单位矩阵 $\boldsymbol{\sigma}_{0}$ 和泡利矩阵 $\boldsymbol{\sigma}_{x}$,$\boldsymbol{\sigma}_{y}$,$\boldsymbol{\sigma}_{z}$ 表示为

$$\begin{aligned}&\boldsymbol{T}^{1}=\frac{1}{\sqrt{2}}\boldsymbol{\sigma}_{0},\boldsymbol{T}^{2}=\frac{1}{\sqrt{2}}\boldsymbol{\sigma}_{z}\\&\boldsymbol{T}^{3}=\frac{1}{\sqrt{2}}\boldsymbol{\sigma}_{x},\boldsymbol{T}^{4}=-\frac{1}{\sqrt{2}}\boldsymbol{\sigma}_{y}\end{aligned},\tag{10}$$

则此时 $\boldsymbol{\sigma}^{\alpha}$ 表示为

$$\boldsymbol{\sigma}^{1}=\frac{\boldsymbol{X}\boldsymbol{\sigma}_{0}}{\sqrt{2}}=\begin{pmatrix}X^{00}&X^{10}\\X^{01}&X^{11}\end{pmatrix},\tag{11}$$

$$\boldsymbol{\sigma}^{2}=\frac{\boldsymbol{X}\boldsymbol{\sigma}_{z}}{\sqrt{2}}=\begin{pmatrix}X^{00}&-X^{10}\\X^{01}&-X^{11}\end{pmatrix},\tag{12}$$

$$\boldsymbol{\sigma}^{3}=\frac{\boldsymbol{X}\boldsymbol{\sigma}_{x}}{\sqrt{2}}=\begin{pmatrix}X^{10}&X^{00}\\X^{11}&X^{01}\end{pmatrix},\tag{13}$$

$$\boldsymbol{\sigma}^4=\frac{-\mathrm{i}\boldsymbol{X}\boldsymbol{\sigma}_y}{\sqrt{2}}=\begin{pmatrix}X^{10} & -X^{00}\\ X^{11} & -X^{01}\end{pmatrix}。\tag{14}$$

当 Alice 完成 Bell 基测量后，整个系统的量子态$|\varphi\rangle_{\mathrm{tot}}=R^i\sigma_i^{(\alpha)k}|\alpha\rangle|k\rangle$坍缩为$|\varphi^\alpha\rangle_{\mathrm{B}'}=R^i\sigma_i^{(\alpha)k}|k\rangle$。为完成量子隐形传态，这时需 Alice 通过经典信道将测量的结果告诉 Bob，随后 Bob 将相应的$(\boldsymbol{\sigma}^\alpha)^{-1}$作用到$|\varphi^\alpha\rangle_{\mathrm{B}'}$上便能成功实现量子隐形传态。

上述部分从理论角度分析了量子隐形传态的原理，但是在实际量子隐形传态的过程中，要准确区分 4 个 Bell 态比较困难。考虑到量子信道不仅能传输量子信息，还可以传输经典信息[18]，而经典信息只有 0 和 1 两个状态，则需将量子隐形传态作为量子信道，传输由 0 和 1 组成的随机经典信息序列，这样接收端 Bob 测量时只需区分两个 Bell 态，这样降低了操作难度，更容易实现相关操作。

3 量子隐形传态传输单比特信息

当传输的信息为经典比特 0 或 1 时，可用计算基矢态$|0\rangle$和$|1\rangle$分别表示经典比特 0 和 1。这时可将第 2 节中待传送的粒子态$|\varphi\rangle_a=R^i|i\rangle=R^0|0\rangle+R^1|1\rangle$进行特殊化处理，即满足$R^0=0$，$R^1=1$或$R^0=1$，$R^1=0$。因此，$\pm R^0|0\rangle\pm R^1|1\rangle$表示同一个态，$\pm R^0|1\rangle\pm R^1|0\rangle$也表示同一个态，这样对坍缩态$|\varphi^\alpha\rangle_{\mathrm{B}'}=R^i\sigma_i^{(\alpha)k}|k\rangle$的单粒子操作，只需执行$\boldsymbol{\sigma}_x$或$\boldsymbol{I}$(单位矩阵)操作，由原来的四种操作变为两种操作。进行 Bell 基测量后，坍缩态为$|\varphi^1\rangle_{\mathrm{B}'}$或$|\varphi^2\rangle_{\mathrm{B}'}$时，对其执行$\boldsymbol{\sigma}_x$操作；坍缩态为$|\varphi^3\rangle_{\mathrm{B}'}$或$|\varphi^4\rangle_{\mathrm{B}'}$时，对其执行$\boldsymbol{I}$操作，便可成功实现单比特信息的传输。在信息传输过程中，由于要传输的是$|0\rangle$态或$|1\rangle$态，在进行 Bell 基测量时不需要区别四个 Bell 态，只需区分两类 Bell 态即可。线性量子光学技术[19]相对容易实现，但是其只能区分四个 Bell 态的两种[20-21]，这正好满足量子隐形传态传输经典信息方案的需求，因此本方案可通过线性量子光学技术实现。

4 量子隐形传态传输经典信息序列

当要传输的信息是由 0 和 1 组成的随机序列时，首先发送端 Alice 和接收端 Bob 共享 N 个 EPR 对$|\varphi\rangle_{\mathrm{AB}}=X^{jk}|jk\rangle=X^{00}|00\rangle+X^{01}|01\rangle+X^{10}|10\rangle+X^{11}|11\rangle$，EPR 对有 4 种表示方式，这里取$|\varphi^4\rangle_{\mathrm{AB}}=\frac{1}{\sqrt{2}}(|01\rangle-|10\rangle)_{\mathrm{AB}}$。具体操作过程为：Alice 制备 N 个处于量子态$|\varphi^4\rangle_{\mathrm{AB}}=\frac{1}{\sqrt{2}}(|01\rangle-|10\rangle)_{\mathrm{AB}}$的纠缠对，并从每个纠缠对中挑出一个粒子组成序列 S_{A}，余下粒子组成序列 S_{B}，并通过块传输技术经量子信道发送给 Bob。

为保证序列 S_{B} 在传输过程的安全性，Bob 在接收到的序列 S_{B} 中随机抽取一部分以 z 基($|0\rangle$，$|1\rangle$)或 x 基($|+\rangle$，$|-\rangle$)进行单粒子测量，并将所选的测量基矢和测量结果通过经典信道告知 Alice，Alice 也取相同的测量基矢对序列 S_{A} 中相应的粒子进行单粒子测量，并与 Bob 的测量结果进行比对，以判断传输过程有没有遭到窃听，从而保证量子纠缠对的安全分发。

0 对应$|0\rangle$态，1 对应$|1\rangle$态，Alice 将待传输的经典信息序列编码为量子状态序列 S_{C}，这里需要注意的是，量子状态序列 S_{C} 中粒子的个数与序列 S_{A} 中经单粒子测量后所剩的粒子个数相同；然后 Alice 让量子状态序列 S_{C} 与 S_{A} 中的粒子两两对应执行 Bell 基测量，这时 Bob 手中的序列 S_{B} 相应的粒子态发生坍缩；Alice 将测量结果通过公开信道通知给 Bob，这时 Bob 执行相应的酉操作便可得到待传送的粒子态。重复操作，直到量子状态序列 S_{C} 中的粒子都操作完为止，这样就完成了量子隐形传态传输经典信息。

5 安全性及可行性分析

发送端 Alice 和接收端 Bob 共享 EPR 对序列时，Alice 制备 N 个纠缠对，并从每个纠缠对中挑出一个粒子组成序列 S_{A}，剩下的粒子组成序列 S_{B}，并经量子信道发送给 Bob。这一过程采用块传输技术来实现，这与量子安全直接通信的安全性一致，这一过程的安全性已被证明。纠缠分发完成后，发送者 Alice 对序列 S_{A} 和序列 S_{C} 进行 Bell 基测量，量子态的坍缩分别发生在发送端 Alice 处和接收端 Bob 处，这一过程窃听者根本没有机会窃听，随后 Alice 通过公开信道将测量结果告知 Bob，在这一过程中，窃听者虽然可以窃听到测量结果，但得不到任何信息。同时，将量子隐形传态看作量子信道，通过编码将 0 和 1 分别编为$|0\rangle$和$|1\rangle$，就可实现由 0 和 1 组成的随机经典信息序列的传输，在进行 Bell 基测量时不需要区别四个 Bell 态，只需区分两类 Bell 态，这种通信方式可以通过线性量子光学技术实现。

6 结 论

针对一次一密经典通信方式存在密钥丢失的风

险和传输大量数据时密钥会很快消耗完的缺点，提出将量子隐形传态看作量子信道，这种通信方式在保证安全性的基础上可以不停地生成密钥，满足大数据通信的需求。同时在该方案中将待传输的经典信息序列编码为计算基矢态，这样在接收端 Bob 处只需区分两种 Bell 态，相比经典量子隐形传态，本方案降低了 Bell 基测量的难度，实现起来比较容易。线性量子光学技术可以区分两类 Bell 态，理论上本方案可以通过线性量子光学技术实现，具体实现过程是下一步工作的研究内容。

参 考 文 献

[1] Su X Q, Guo G C. Quantum communication and quantum computation [J]. Chinese Journal of Quantum Electronics, 2004, 21(6): 706-718.
苏晓琴, 郭光灿. 量子通信与量子计算[J]. 量子电子学报, 2004, 21(6): 706-718.

[2] Bennett C H, Brassard G, Crépeau C, *et al*. Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels [J]. Physical Review Letters, 1993, 70(13): 1895-1899.

[3] Nandi K, Mazumdar C. Quantum teleportation of a two qubit state using GHZ-like state [J]. International Journal of Theoretical Physics, 2014, 53(4): 1322-1324.

[4] Sun X M, Zha X W. A scheme of bidirectional quantum controlled teleportation via six-qubit maximally entangled state[J]. Acta Photonica Sinica, 2013, 42(9): 1052-1056.
孙新梅, 查新未. 基于六粒子最大纠缠态的双向控制隐形传态方案[J]. 光子学报, 2013, 42(9): 1052-1056.

[5] Lu H, Chen L B, Huang C Q, *et al*. Teleportation of an entangled state via the W states [J]. Chinese Journal of Quantum Electronics, 2004, 21(6): 730-733.
路洪, 陈立冰, 黄纯青, 等. 用 W 态作量子信道实现纠缠态的隐形传送[J]. 量子电子学报, 2004, 21(6): 730-733.

[6] Ye L, Yao C M, Guo G C. Teleportation of a two-particle entangled state[J]. Chinese Physics, 2001, 10(11): 1001-1003.

[7] Dyer S, Takesue H, Verma V, *et al*. Polarization-insensitive superconducting nanowire single-photon detectors[C]//CLEO: 2015, May 10-15, 2015, San Jose, California, United States. Washington, D. C.: OSA, 2015: FF2A. 4.

[8] Xia X X, Sun Q C. The latest developments of fiber quantum teleportation [J]. Journal of Information Security Research, 2017, 3(1): 36-43.
夏秀秀, 孙启超. 光纤量子隐形传态技术最新进展[J]. 信息安全研究, 2017, 3(1): 36-43.

[9] Sun Q C, Mao Y L, Chen S J, *et al*. Quantum teleportation with independent sources and prior entanglement distribution over a network[J]. Nature Photonics, 2016, 10(10): 671-675.

[10] Valivarthi R, Puigibert M L G, Zhou Q, *et al*. Quantum teleportation across a metropolitan fibre network[J]. Nature Photonics, 2016, 10(10): 676-680.

[11] Bouwmeester D, Pan J W, Mattle K, *et al*. Experimental quantum teleportation [J]. Nature, 1997, 390(6660): 575-579.

[12] Karlsson A, Bourennane M. Quantum teleportation using three-particle entanglement [J]. Physical Review A, 1998, 58(6): 4394-4400.

[13] Yang Y F, Ye Z Q. Scheme of two-way quantum teleportation and security[J]. Acta Photonica Sinica, 2013, 42(5): 619-622.
杨幼凤, 叶志清. 双向隐形传态方案及安全性分析[J]. 光子学报, 2013, 42(5): 619-622.

[14] Zou X, Ye Z Q. Two-way quantum teleportation controlled by a third party [J]. Chinese Journal of Quantum Electronics, 2012, 29(6): 683-687.
邹昕, 叶志清. 基于第三方控制的量子双向传态[J]. 量子电子学报, 2012, 29(6): 683-687.

[15] Yang C P, Chu S I, Han S Y. Efficient many-party controlled teleportation of multiqubit quantum information via entanglement [J]. Physical Review A, 2004, 70(2): 022329.

[16] Zou X, Ye Z Q. Based on four-qubit cluster state secretly shared by three parties to realize controlled teleportation of three-qubit state [J]. Journal of Jiangxi Normal University(Natural Science Edition), 2012, 36(3): 263-266.
邹昕, 叶志清. 基于三方秘密共享 4 粒子团簇态实现三比特量子态的可控隐形传态[J]. 江西师范大学学报(自然科学版), 2012, 36(3): 263-266.

[17] Tian X L, Hu Y, Fu H Z. Research on tensor representation of quantum teleportation[J]. Journal of Xi'an University of Posts and Telecommunications, 2014, 19(4): 1-8.
田秀劳, 胡洋, 符洪姿. 张量表示的量子隐形传态研究[J]. 西安邮电大学学报, 2014, 19(4): 1-8.

[18] He Z L, Guo D B, Wang X K. Security capacity of

compound wiretap channel [J]. Laser & Optoelectronics Progress, 2015, 52(11): 112701.
贺转玲, 郭大波, 王晓凯. 复合窃听信道的安全容量[J]. 激光与光电子学进展, 2015, 52(11): 112701.

[19] Zhai S Q, Zhang Y. Duplex hybrid entanglement manipulation based on linear optics [J]. Chinese Journal of Lasers, 2016, 43(11): 1112002.
翟淑琴, 张姚. 基于线性光学的双通道混合纠缠操控[J]. 中国激光, 2016, 43(11): 1112002.

[20] van Houwelingen J A W, Brunner N, Beveratos A, *et al*. Quantum teleportation with a three-Bell-state analyzer[J]. Physical Review Letters, 2006, 96(13): 130502.

[21] Xia X X, Sun Q C. The latest developments of fiber quantum teleportation [J]. Journal of Information Security Research, 2017, 3(1): 36-43.
夏秀秀, 孙启超. 光纤量子隐形传态技术最新进展[J]. 信息安全研究, 2017, 3(1): 36-43.