多粒子纠缠态 QTDM 通信方案及 QMU 协议*

张天鹏[1]，聂敏[1,2]，裴昌幸[1]
（1 西安电子科技大学 综合业务网理论及关键技术国家重点实验室，西安 710071）
（2 西安邮电学院，西安 710061）

摘 要：分析了未知的三个三态粒子纠缠态的隐形传送过程，结合纠缠源的特性，提出了量子信道时分复用方案. 同时还提出了一种可传送多粒子纠缠态的量子时分多路通信方案和量子多用户协议. 研究结果表明，该方案与采用 BB84 协议的量子通信系统相比，不仅能够实现量子多用户安全保密通信，而且误码率低.

关键词：量子通信；多粒子纠缠；量子时分多路；量子多用户协议
中图分类号：TN914.52 **文献标识码**：A **文章编号**：1004-4213(2009)04-987-5

0 引言

根据量子态叠加原理和量子不可克隆定理，量子通信(Quantum Communication，QC)具有经典通信不可比拟的安全保密性和高效性，因而成为当前的研究热点. 量子通信是建立在量子力学的基础上，能够实现真正的绝对安全通信. Bennett 等人[1]在 1993 年提出了一种量子态隐形传输方案，其基本思想是：为实现某个物体未知态的传送，将原物的信息分为经典信息和量子信息两部分，分别由经典通道和量子通道传送给接收者. 经典信息是发送者对原物进行测量而获得的，而量子信息是发送者在测量中未提取的信息. 接收者在获得这两种信息后，就可以制备出原物的复制品. 在此过程中，原物并未被传送，传送的仅是原物的量子态，而发送者不一定预知该量子态. 这就是量子态的隐形传送.

迄今为止，最远的量子通信距离是 Gobby[2]等人在 2004 年实现的 122 km 光纤量子通信实验，自由空间的量子通信已达 23.4 km[3]. 中国潘建伟小组 2004 年首次实现了五光子量子纠缠，验证了“终端开放”的量子态隐形传输[4]. 这些都为基于多粒子纠缠[5]的多用户通信奠定了基础. 目前主要的量子通信方案是以 BB84 协议[6]为基础的量子密钥通信[7]，误码较大. 本文在 Bennet 提出的量子隐形传输方案的基础上，分析了多粒子的隐形传态，实现了多粒子传送，且误码率很低；还提出了量子信道的时分复用(Quantum Communication Time Multiplex，QCTM)和量子多用户通信方案，并给出了量子多用户(Quantum Multi-users，QMU)协议.

*国家自然科学基金(60572147，60672119)和陕西教育科学研究计划项目(08JK426)资助
Tel：029-88202514 Email：zhangtian909@163.com
收稿日期：2007-12-26

1 多粒子纠缠态隐形传送原理

目前，对多粒子纠缠态的研究[5,8,9]吸引了众多研究者. 从通信的角度看，量子隐形传态实际上完成了对量子信号的传输、调制与解调的过程，而纠缠粒子传输的通道就是量子信道. 隐形传态在误码率的控制上有良好的优势；多粒子不但可以传送更多的信息，而且也适合进行纠错编码.

多粒子纠缠态的隐形传送[10]原理如图 1. 在 Alice 处有三个三态粒子的纠缠态处于未知量子态，

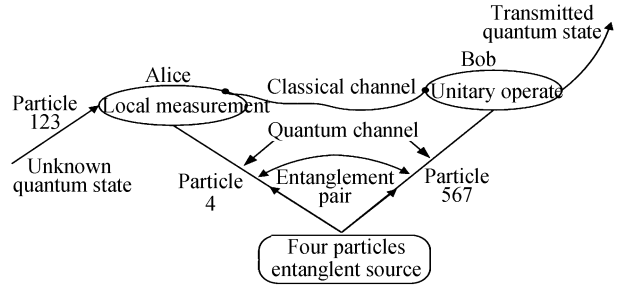

图 1 多粒子隐形传输原理
Fig. 1 Multi-particles teleportation scheme

可表示为

$$|\phi\rangle_{123}=x|000\rangle_{123}+y|111\rangle_{123}+z|222\rangle_{123} \quad (1)$$

式中 x、y、z 满足 $x^2+y^2+z^2=1$.

Alice 希望将这个未知量子态传给 Bob，但不传送粒子本身. 具体过程如下：

①在 Alice 和 Bob 之间制备四个处于最大纠缠态的三态粒子(纠缠粒子为 4567，其纠缠态可表示为式(2)). 由于纠缠粒子存在量子关联性，它们可作为 Alice 和 Bob 之间的量子信道.

$$|\phi\rangle_{4567}=\frac{1}{\sqrt{3}}(|0000\rangle_{4567}+|1111\rangle_{4567}+|2222\rangle_{4567}) \quad (2)$$

②将粒子 1、2、3、4 分发给 Alice，粒子 5、6、7 发给 Bob. 此时系统的量子态为

$$|\phi\rangle=|\phi\rangle_{123}|\phi\rangle_{4567}$$

③传输未知量子态时，Alice 先对粒子 1 和 4 进

行 Bell 基联合测量. Bell 基可表示为

$$|\phi_{mn}\rangle=\sum_j e^{2\pi ijn/3}|\phi\rangle\otimes|(j+m)mod3\rangle/\sqrt{3} \quad (3)$$

式中$(n,j,m)\in(0,1,2)$. 这时系统的量子态将塌缩为 $14\langle\varphi_{mn}|\phi\rangle$.

④Alice 对粒子 2 和 3 在基$\{|\pi_0\rangle,|\pi_1\rangle,|\pi_2\rangle\}$下进行单独测量,该基定义为

$$\begin{bmatrix}|\pi_0\rangle\\|\pi_1\rangle\\|\pi_2\rangle\end{bmatrix}=\frac{1}{\sqrt{3}}\begin{bmatrix}1&1&1\\1&\lambda&\lambda^2\\1&\lambda^2&\lambda\end{bmatrix}\begin{bmatrix}|0\rangle\\|1\rangle\\|2\rangle\end{bmatrix} \quad (4)$$

式中 $\lambda=e^{2\pi i/3}$. 此时粒子 5、6、7 的量子态塌缩为

$$|\phi\rangle_{567}=2\langle\pi_\alpha|\otimes 3\langle\pi_\beta|\otimes 14\langle\phi_{mn}|\phi\rangle \quad (5)$$

式中 α,β 可取 0、1 或 2.

⑤Alice 将测量结果通过经典信道通知 Bob. Bob 根据收到的测量结果对粒子 5、6 和 7 实施幺正变换(如式(6)),即可使粒子 567 的量子态与粒子 123 以前的量子态相同,这样就完成了对粒子 123 未知量子态的隐形传送.

$$U=U_{mn}^{\gamma}=\sum_j e^{2\pi in(n+\gamma)/3}|j\rangle\otimes|j\rangle\otimes|j\rangle\langle(j+m)\mathrm{mod}3|$$
$$\otimes\langle(j+m)\mathrm{mod}3|\otimes\langle(j+m)\mathrm{mod}3| \quad (6)$$

式中 n、m 与式(3)一致;γ 的取值与 β 和 α 有关. 若 $\alpha=\beta$,则 $\gamma=\alpha=\beta$;若 $\alpha\neq\beta$,则 γ 取 α 和 β 之外的第三个数(即 0、1、2 之一).

上述方案可推广到 N 个三态粒子隐形传送的情况,还可推广到 N 个 N 态粒子的隐形传输.

2 QCTM 方案

离散纠缠源(DES)每隔一定时间产生纠缠粒子对,本文利用该特性提出了量子信道时分复用方案. 具体思路是:将纠缠粒子产生的时间划分为不同的时隙,按时隙将产生的纠缠粒子对分发给不同的用户,以实现量子信道时分复用. 图 2 是单纠缠源量子时分复用系统原理.

量子纠缠源的输出是具有一定时隙的纠缠粒子流,要求具有高度稳定性. 发送的纠缠粒子与时隙一一对应,量子时分解复用器(Quantum Time Decomposition Multiplexer,QTDD)将量子复用信道(Quantum Multiplex Current,QMC)的纠缠粒子流分配给不同的单量子信道,按时隙和目的地址控制其输出. 量子信道时分复用原理如图 3.

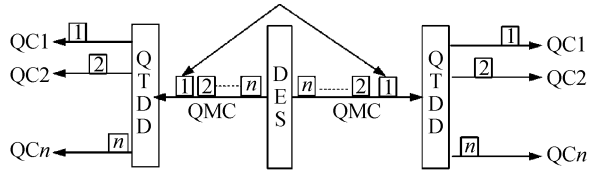

图 2 单纠缠源量子时分复用系统原理

Fig. 2 Scheme of QCTM system of mono-entanglement source

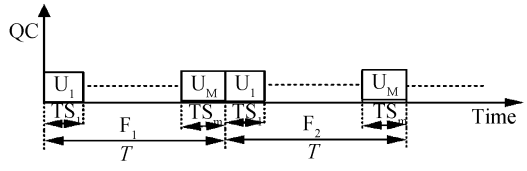

图 3 量子信道时分复用原理

Fig. 3 Scheme of QCTM channel

设帧周期为 T,每帧有 m 个时隙(TS). 每对用户通信时可得到指定的时隙. 这样保证 m 对用户同时通信. 由于单纠缠源仅能保证少数用户同时通信,为使系统容纳更多的用户,采用将多个不同频率的纠缠源同时时分复用方法,具体方案如图 4.

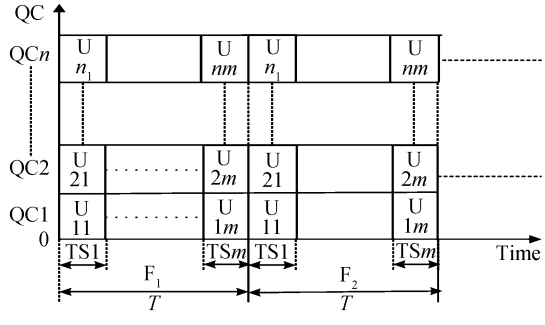

图 4 多纠缠源量子信道时分复用方案

Fig. 4 The scheme of multi-entanglement source quantum channel

图 4 中,n 是纠缠源的个数,它们的工作频率各不相同,这就保证了它们所产生的纠缠粒子是彼此独立的,以满足$(m\cdot n)$对用户同时通信的需要. 多纠缠源量子信道时分复用系统如图 5.

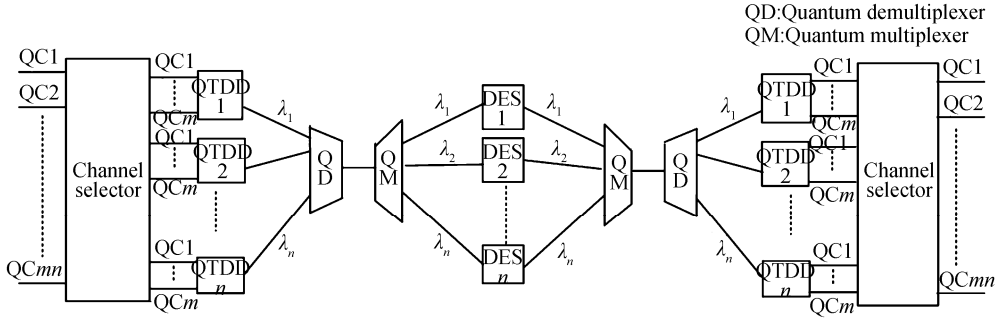

图 5 多纠缠源量子信道时分复用系统原理

Fig. 5 Scheme of QCTM system of multi-entanglement source

3　量子时分多路通信方案

基于上述对 QCTM 的分析，本文提出多用户量子时分多路通信方案（Quantum Time Division Multiplex，QTDM）如下：方案中，经典通信网为辅助信道，光纤为纠缠粒子对的分发信道，如图 6. QTDM 由四部分组成：量子信道复用系统（QCMS）、量子通信控制系统（QCCS）、用户网络、经典通信系统（CCS）. 具体实现过程如下：

①Alice 通过经典系统发出与 Bob 通信的请求. 若 Bob 空闲，则通知量子系统为 Alice 和 Bob 分配量子信道.

②量子系统收到请求后，查询是否有空闲时隙. 若有，则量子信道复用系统为 Alice 和 Bob 分配一个时隙，同时经典通信系统通知 Alice 和 Bob 准备接收纠缠粒子.

③Alice 和 Bob 在收到纠缠粒子后，Alice 发送量子信息，并进行 Bell 基联合测量，通过经典系统将测量结果通知 Bob.

④Bob 在收到测量结果后，通过幺正变换 U，恢复量子信息比特；

⑤量子信息传输完毕，释放 A 和 B 之间的量子信道和经典信道.

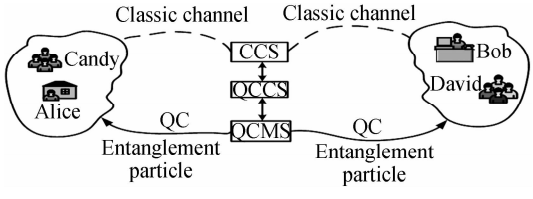

图 6　量子时分多用户通信方案

Fig. 6　QTDM multi-user communication scheme

4　QMU 协议及误码性能分析

为分析 QTDM 的系统性能，特做约定：①假定纠缠源的效率是 100%；②纠缠源频率为 f；③测量结果需用 m 个经典比特表示. ④帧长 T 取决于通信业务的种类.

4.1　QMU 协议

1）图 7 是量子多用户通信的复用帧格式. 其中 $n=T\cdot f$；0 和 1 时隙用于每帧的起始信号及目的地址编码，量子时分解复用器按该编码将不同时隙中的纠缠粒子输出到规定的单信道上；此帧由多粒子纠缠源生成，其中目的地址和时隙顺序是一一对应的.

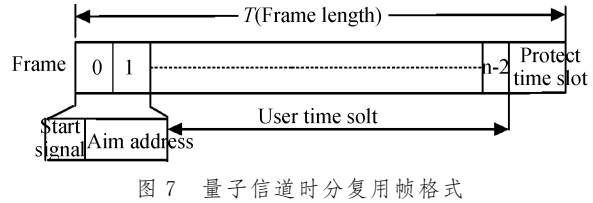

图 7　量子信道时分复用帧格式

Fig. 7　QTDM frame format

2）在通信开始时，用户先申请经典信道，若有空闲信道，再申请量子信道；若无空闲信道或无量子信道空闲，则用户通信失败. 若信道申请成功，用户开始占有该时隙，直到通信结束.

3）信道分配完成后，系统通知双方用户开始接收粒子，建立量子信道. 被叫在收到粒子后，向主叫发送确认信号. 终端用户有一个量子缓存器，存储接收的纠缠粒子，实现通信的同步. 用户将接收的粒子暂存，规定在开始接收后 Δt_0 内有一方未收到粒子，则通知对方，等待下一个时隙，并释放缓存器中的粒子.

4）主叫收到确认信号后，在自己也收到粒子时，Δt_0 过后开始测量，规定测量时间为 Δt. 当 Δt 时间到，同时分发给用户的经典时隙也达到，主叫通过经典时隙将测量结果发送给对方. 随后再等待 T 时间，重复进行 3）和 4）.

5）通信双方中，只要有一方结束通信，则系统释放信道.

4.2　系统误码性能分析

目前，在量子隐形传态方案中，量子信道以最大纠缠纯态的形式实现，可实现纠缠度和保真度均为 1 的量子态传输. 但是，由于实际环境中的温度和磁场对系统的影响，建立最大纠缠量子信道很困难. 海森堡模型研究[11-13]表明：在 Heisenberg 链中，量子热纠缠度只与外界温度有关，磁场无关；若温度、磁场一定，在平均保真度 $\overline{f}>\overline{f_0}$ 下仍可实现量子隐形传态. 本文仅考虑相位相干保持态和脆弱最大纠缠态两种特殊情况[14].

在实际量子通信中，量子纠缠态的储存时间远大于热力学时间尺度 ξ^{-1}，使脆弱最大纠缠态最终完全演变为经典混合态，而相位相干保持态纠缠度不变. 在测量量子信号时，产生了量子噪音，必然对被测系统产生影响，造成检测误码. 总误码率 p_Σ 包括脆弱最大纠缠态误码 p_s、量子信号检测误码 p_d 和经典通信系统误码 p_c 三部分，可表示为

$$p_\Sigma=1-(1-p_d)^2\cdot(1-p_c)\cdot(1-p_s) \tag{7}$$

在式（7）中，p_c 取决于经典系统，本文不做分析；p_d 取决于纠缠源，也不在本文研究之列. 下面主要分析 p_s.

在量子态测量中，测量基的偏差将导致误码. 本文采用三态粒子，如果测量基 (x,y,z) 与被测粒子的本征基 (X,Y,Z) 的方向有差别，如图 8. 设三个方向相差分别为 α、β 和 γ，测量算符为 U'，本征算符为 U，其关系可表示为

$$U'=f(U)=f(\alpha,\beta,\gamma) \tag{8}$$

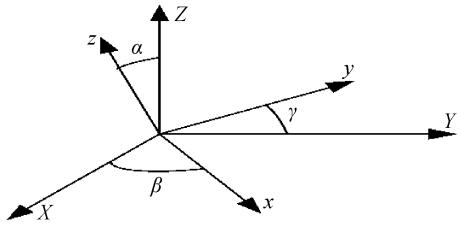

图 8 测量基(x,y,z)与被测粒子的本征基(X,Y,Z)不一致的情况

Fig. 8 The case in (x,y,z) different with eigenvalue base of measured particle of (X,Y,Z)

上述误差将引起测量的非正交性,导致测量误差,产生误码.下面仅分析 $\alpha=0$ 的情况.从误差角度来看,偏差角 β 和 γ 相关联,其概率密度函数服从高斯分布,所以每个量子比特的误码率为[15]

$$p_{\mathrm{d}}=\frac{1}{2}\{1-\cos\beta_0\exp\left(-\frac{\Delta^2}{4}\right)\} \tag{9}$$

式中 β_0 表示本征基和测量基方向之间有一个未被意识到的系统偏差,Δ 表示随机偏差随机涨落的均方根[15],所以

$$p_{\Sigma}=1-\frac{1}{4}\left(1+\cos\beta_0\exp\left(-\frac{\Delta^2}{4}\right)\right)^2\cdot(1-p_{\mathrm{c}})(1-p_{\mathrm{s}}) \tag{10}$$

式(10)表明,在 p_{c} 和 p_{s} 固定时,要达到很小的误码率,本征基和测量基方向间的误差必须很小,即系统误差 β_0 和随机误差 Δ 都必须控制在非常小的范围内.图 9 给出了 p_{Σ} 与 β_0、Δ 关系.

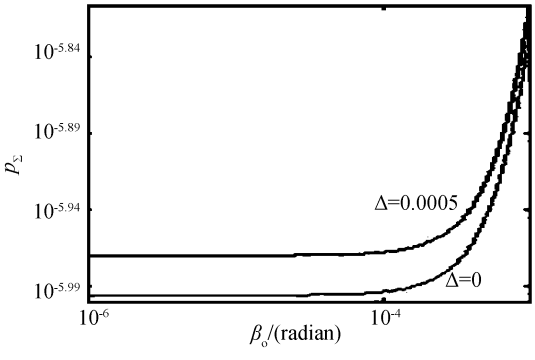

图 9 p_{Σ} 与 β_0 和 Δ 关系($p_{\mathrm{c}}=10^{-8}$,$p_{\mathrm{s}}=10^{-6}$)

Fig. 9 The relationship between p_{Σ} and $\beta_0\Delta$($p_{\mathrm{c}}=10^{-8}$,$p_{\mathrm{s}}=10^{-6}$)

由图 9 可以看出,当 p_{c} 和 p_{s} 固定时($p_{\mathrm{c}}=10^{-8}$,$p_{\mathrm{s}}=10^{-6}$),p_{Σ} 随 β_0 呈现准指数变化.在 $\Delta=0$ 和 $\Delta=0.000\,5$ 两种情况下,要实现极低的误码率 p_{Σ},要求测量基和本征基的方向高度一致.另外,BB84 协议的理论误码率最低为 0.25[16].因此,本方案比 BB84 协议方案具有更低的误码率.

5 结论

为实现多用户量子保密通信,本文提出了一种基于多粒子隐形传态和量子时分复用的通信方案.研究结果表明,该方案不仅可实现多用户同时通信,而且能够与传统的通信网相兼容.误码分析结果表明,要得到小于 1.76×10^{-6} 的误码率,测量基和本征基的方向误差要小于 10^{-3}.

参考文献

[1] BENNETT C H, BRASSARD G, CREPEAU C, *et al*. Teleporting an unknown quantum state via dual classical and Einstein Podolky-Rosen channels[J]. *Phy Rev Lett*, 1993, **70**(13): 1895-1899.

[2] GOBBY C, YUAN Z L, SHIELDS A J. Quantum key distribution over 122 km standard telecom fiber[J]. *Appl Phys Lett*. 2004, **84**(19): 3762-3764.

[3] KURTSIEFER C, ZARDA P, HALDER M, *et al*, A step towards global key distributions [J]. *Nature*, 2002, **419**(6906): 450.

[4] ZHAO Z, CHEN Y A, ZHANG A N, *et al*. Experimental demonstration of five-photon entanglement and opendestination teleportation[J]. *Nature*, 2004, **430**(6995): 54-58.

[5] CHEN Mei-feng, MA Song-she. Generation of w-type entangled coherent states of three-cavity field by raman interaction[J]. *Acta Photonica Sinica*. 2007, **36**(5): 950-953.

[6] BENNET C H , BRASSARD G. Quantum Cryptography: Public Key Distribution and Coin Tossing[C]. *Proceedings of the IEEE International Conference on Computers, Systems, and Signal Processing*. Bangalore: *IEEE*, 1984. 175-179.

[7] CHEN Zhi-xin, TANG Zhi-lie, LIAO Chang-jun, *et al*. Practical security problem of six states QKD protocol [J]. *Acta Photonica Sinica*, 2006, **35**(1): 126-129.
陈志新,唐志列,廖常俊,等. 实际量子密钥分配扩展 BB84 协议窃听下的安全性分析[J]. 光子学报. 2006, **35**(1): 126-129.

[8] CHEN Mei-feng, MA Song-she. A scheme for teleportation of an unknown multi-atom entangled state via raman interaction [J]. *Acta Photonica Sinica*, 2007, **36**(6): 1152-1155.

[9] ZHU Chang-hua, PEI Chang-xing, MA Huai-xin, *et al*. A scheme for quantum local area networks and performance analysis[J]. *Jouranl of Xidian University*, 2006, **33**(6): 839-843.
朱畅华,裴昌幸,马怀新,等. 一种量子局域网方案及其性能分析[J]. 西安电子科技大学学报, 2006, **33**(6)839-843.

[10] YU Li-zhi, GONG Ren-shan. Probabil istic teleportation of an unknown entangled state of three particles by a entangled state of four particles[J]. *Acta Sinica Quantum Optica*, 2005, **11**(1): 29-33.
于立志,龚仁山. 通过四个纠缠态粒子来实现未知的三个纠缠态粒子的量子几率隐形传输[J]. 量子光学学报, 2005, **11**(1): 29-33.

[11] ABLIZ A, GAO H J, XIE X C, *et al*. Entanglement control in an anisotropic two-qubit Heisenberg XYZ model with external magnetic fields[J]. *Phys Rev A*. 2006, **74**(5): 052105(5).

[12] XI Xiao-qiang, LIU Wu-ming. An important property of entanglement: pairwise entanglement that can onlybe transferred by an entangledpair [J]. *ChinesePhysics*.. 2007, **16**(07): 1858-1862.

[13] TANG Huang, FANG Jian-xing, QIAN Xue-min. Research on the quantun teleportation in Heisenberg model[J]. *Acta Sinia*

Quantum Optica. 2007，**11**(3)：109-113.
唐煌，方建兴，钱学旻. 海森堡模型中量子隐形传递的研究[J]. 量子光学学报. 2007，**11**(3)：109-113.

[14] XIANG Shao-hua，SONG Ke-hui. Entangle ment deco herence of two2p article entangled states in a noisy enviro nment[J]. *Acta Phys Sin*，2006，**55**(2)：529-533.
向少华，宋克慧. 噪音环境中两粒子纠缠态的纠缠消相干[J]. 物理学报，2006，**55**(02)：0529.

[15] LI Yi-feng，CHEN Jian-guo，FENG Guo-ying，*et al*. Analysis of basis direction deviation in quantum communication[J]. *Laser Journal*，2004，**25**(1)：43-44.
李义峰，陈建国，冯国英，等. 量子通信中的测量基方向问题[J]. 激光杂志，2004 ，**25**(1)：43-44.

[16] LIN Feng-zen. Introduction of BB84 Quantum cryptog-raphic protocols[EB/OL]. [2007-11-10]. http://ftlin. sam. pccu. edu. tw/QuantumLab/Cryptography/BB84_Intro. htm.

Research on Multi-particle Entangled State QTDM Communication Scheme and QMU Protocol

ZHANG Tian-peng，NIE Min，PEI Chang-xing
(1 *State Key Lab. of Integrated Service Networks*，*Xidian Univ. Xi'an* 710071，*China*)
(2 *Xi'an Institute of Post and Telecommunication*，*Xi'an* 710061，*China*)
Received date：2007-12-26

Abstract：The teleportation of three entangled states of three-state particles is analyzed. Aquantumchannel time multiplex scheme based on characteristics of entangled source is proposed. The quantum time division multiplexcommunication scheme capable of transmitting multi-particles entangled state is presented finally. The results show that the scheme above not only has a lower BER than BB84 protocol but can realize the multi-users secret communication.

Key words：Quantum Communication；Multiparticles entanglement；Quantum Time Division Multiplex；Quantum Multi-users protocol

ZHANG Tian-peng　was born in 1982. He obtained his the B. S degree from Xi'an Institute of Communication Engineering in 2005. He is studying for his M. S degree at Xidian University. His major is quantum communication system and quantum information processi.