文章编号:1004-4213(2010)01-0156-4

四维二粒子超密编码的单向通信方案*

周锐[a],朱玉兰[a],聂义友[a,b,†]

(江西师范大学 a.物理与通信电子学院; b.江西省光电子与通信重点实验室,南昌 330022)

摘 要:根据超密编码原理,考虑到与经典的二进制编码相融合,提出了利用四维二粒子进行超密编码的单向通信方案.在该方案中,信息发送者在对其拥有的粒子进行幺正变换后,将粒子发送给信息接收者.然后信息接收者对二个粒子进行联合测量,根据测量结果,就可以推知信息发送者已作了那种幺正变换,每种幺正变换对应着 4 bits 经典信息,从而得知信息发送者要传送的信息.最后,对该通信方案进行了安全性分析.

关键词:量子通信;单向通信;超密编码;四维二粒子

中图分类号:O431.2;TN918 **文献标识码**:A **doi**:10.3788/gzxb20103901.0156

0 引言

量子通信是近年来迅速发展起来的研究领域,它是以量子态作为信息载体和通信信道进行通信的.量子通信为信息科学的发展提供了新的方法,它具有容量大、速度快、保密性强等优点,对信息的处理比经典方法具有更快的速度和更高的效率[1-5].因此量子通信的研究在世界范围内引起了极大的关注,各国都投入了巨大的人力财力资源来满足量子通信的需要.目前量子通信已经在实验领域取得了巨大突破,已验证了量子态的隐形传输、量子超密编码以及量子密钥的传输.

量子超密编码作为量子信息处理的研究领域之一,是 1993 年由 Bennett 和 Wiener 首次提出的[3],其特点是通信中只传送一个量子位即可完成传送二个经典位信息的任务.2002 年,我国的龙研究小组[6]和波兰的 Crudka 研究小组[7]分别将 Bennett 和 Wiener 提出的原始二维双方的量子超密编码方案推广至高维多方的情形.文献[6]提出了一种实现多体高维的量子超密编码方案.

实验上,二维量子超密编码过程,已经由 Mattle 等人[8]和方等人[9]分别在量子光学体系和核自旋体系中实现.

本文以超密编码[6]为基础,考虑到与经典的二进制编码相融合,提出利用四维二粒子进行超密编码的单向不对称通信方案.信息发送者 Bob 在对其拥有的粒子进行幺正变换后,将粒子发送给信息接收者 Alice.然后 Alice 对二个粒子进行联合测量,根据测量结果,就可以推知信息发送者已作了那种幺正变换,每种幺正变换对应着 4 bits 经典信息,从而得知信息发送者要传送的信息.该通信方案只需要传输一个粒子和一次测量就能获得 4 bits 的信息,具有较高的信息传送效力.

1 单向通信编码原理

对四维二粒子(粒子 A 和粒子 B)系统,其最大纠缠态函数的通式为

$$|\phi_{nm}\rangle_{AB}=\sum_j e^{i\pi jn/2}|j\rangle_A\otimes|j+m \bmod 4\rangle_B/2 \quad (n,m=0,1,2,3) \tag{1}$$

即四维二粒子系统共有 16 种态函数

$$|\phi_{00}\rangle_{AB}=\frac{1}{2}(|00\rangle_{AB}+|11\rangle_{AB}+|22\rangle_{AB}+|33\rangle_{AB})$$

$$|\phi_{01}\rangle_{AB}=\frac{1}{2}(|01\rangle_{AB}+|12\rangle_{AB}+|23\rangle_{AB}+|30\rangle_{AB})$$

$$|\phi_{02}\rangle_{AB}=\frac{1}{2}(|02\rangle_{AB}+|13\rangle_{AB}+|20\rangle_{AB}+|31\rangle_{AB})$$

$$|\phi_{03}\rangle_{AB}=\frac{1}{2}(|03\rangle_{AB}+|10\rangle_{AB}+|21\rangle_{AB}+|32\rangle_{AB})$$

……

$$|\phi_{32}\rangle_{AB}=\frac{1}{2}(|02\rangle_{AB}+e^{3\pi i/2}|13\rangle_{AB}+e^{\pi i}|20\rangle_{AB}+e^{\pi i/2}|31\rangle_{AB})$$

$$|\phi_{33}\rangle_{AB}=\frac{1}{2}(|03\rangle_{AB}+e^{3\pi i/2}|10\rangle_{AB}+e^{\pi i}|21\rangle_{AB}+e^{\pi i/2}|32\rangle_{AB})$$

这 16 个态构成一组正交完备集,称这 16 个态为四维二粒子系统的 Bell 基态.相应的有 16 个幺正操作

* 国家自然科学基金(60807014)、江西省自然科学基金(2009GZW0005)和江西省教育厅科研项目(GJJ09153)资助

† Tel:0791-8120376 Email:nieyiyou@163.com

收稿日期:2009-01-07 修回日期:2009-03-26

$$\boldsymbol{U}_{00}=\begin{pmatrix}1&0&0&0\\0&1&0&0\\0&0&1&0\\0&0&0&1\end{pmatrix},\boldsymbol{U}_{01}=\begin{pmatrix}0&0&0&1\\1&0&0&0\\0&1&0&0\\0&0&1&0\end{pmatrix},$$

$$\boldsymbol{U}_{02}=\begin{pmatrix}0&0&1&0\\0&0&0&1\\1&0&0&0\\0&1&0&0\end{pmatrix},$$

……

$$\boldsymbol{U}_{32}=\begin{pmatrix}0&0&\mathrm{e}^{\pi\mathrm{i}}&0\\0&0&0&\mathrm{e}^{\pi\mathrm{i}/2}\\1&0&0&0\\0&\mathrm{e}^{3\pi\mathrm{i}/2}&0&0\end{pmatrix},$$

$$\boldsymbol{U}_{33}=\begin{pmatrix}0&\mathrm{e}^{3\pi\mathrm{i}/2}&0&0\\0&0&\mathrm{e}^{\pi\mathrm{i}}&0\\0&0&0&\mathrm{e}^{\pi\mathrm{i}/2}\\1&0&0&0\end{pmatrix}$$

幺正操作矩阵元通式为

$$(\boldsymbol{U}_{mn})_{j'j}=\mathrm{e}^{\mathrm{i}\pi jn/2}\delta_{j',j+m \bmod 4}\quad(n,m=0,1,2,3)\tag{2}$$

当取出由式(2)所表示的 16 个幺正操作中的任意一个，把它作用于由式(1)所表示的 16 个四维二粒子系统的某一态函数中第二个粒子(B 粒子)上时，二粒子系统将唯一地转化成这 16 个系统态函数的另一个状态(例如 $U_{01}^{\mathrm{B}}|\phi_{32}\rangle_{\mathrm{AB}}=|\phi_{33}\rangle_{\mathrm{AB}}$)，其一般通式关系如下

$$U_{x_1y_1}^{\mathrm{B}}|\phi_{x_2,y_2}\rangle_{\mathrm{AB}}=|\phi_{xy}\rangle_{\mathrm{AB}}\tag{3}$$

式中

$$x=x_1+x_2 \bmod 4$$
$$y=y_1+y_2 \bmod 4\tag{4}$$

从关系式(3)～(4)中可以得出，在粒子 B 进行幺正变换后，再对二个粒子进行联合测量，只需测量一次，就能得出变换后二粒子系统所处的纠缠态，从而可以推算出已经对 B 粒子作了那种幺正变换.

为了进行通信，Bob 和 Alice 事先约定按下述幺正操作进行二进制编码，其对应关系为

$\boldsymbol{U}_{00}\rightarrow 0000,\boldsymbol{U}_{01}\rightarrow 0001,\boldsymbol{U}_{02}\rightarrow 0010,\boldsymbol{U}_{03}\rightarrow 0011,$

$\boldsymbol{U}_{10}\rightarrow 0100,\boldsymbol{U}_{11}\rightarrow 0101,\boldsymbol{U}_{12}\rightarrow 0110,\boldsymbol{U}_{13}\rightarrow 0111,$

$\boldsymbol{U}_{20}\rightarrow 1000,\boldsymbol{U}_{21}\rightarrow 1001,\boldsymbol{U}_{22}\rightarrow 1010,\boldsymbol{U}_{23}\rightarrow 1011,$

$\boldsymbol{U}_{30}\rightarrow 1100,\boldsymbol{U}_{31}\rightarrow 1101,\boldsymbol{U}_{32}\rightarrow 1110,\boldsymbol{U}_{33}\rightarrow 1111$

由此可见，每个幺正变换对应着 4 bits 经典信息.

2　单向通信方案

本文在超密编码的基础上，提出四维二粒子系统的单向通信方案. 具体协议为：

1)Alice 和 Bob 按上节的编码原理事先约定好幺正操作对应的二进制编码. 由 Alice 随机制备四维二粒子有序初态 $|\phi_{mn}\rangle_{\mathrm{AB}}$ 序列，并分成两个有序粒子序列(称为 A 系列和 B 系列)，把第二个粒子序列(B 粒子系列)传送给 Bob.

2)Alice 和 Bob 进行窃听检测，步骤为：(1) Bob 在 B 粒子序列中随机地选取一些粒子在四维正交基$\{|0\rangle,|1\rangle,|2\rangle,|3\rangle\}$下进行测量，并通过经典信道把测量结果告诉 Alice，同时还把这些被选取的粒子所对应的位置告诉 Alice；(2) Alice 在与 Bob 相同的测量基下测量 A 序列中相应的粒子，然后将她自己的测量结果和 Bob 的测量结果相比对. 如果在传送 B 序列的过程中没有任何窃听，那么他们的相应测量结果应该是相关联的. 如果他们俩人的测量结果是相关联的，Alice 和 Bob 可以确定没有窃听者窃听，继续进行下一步；否则，Alice 告诉 Bob 在传送过程中有窃听者，抛弃该粒子序列，重复上述过程，直到粒子序列安全传输为止.

3)当 Bob 有信息需要传送给 Alice 时，首先把信息用经典的二进制进行编码，再把编码好的字符串每四个分成一组，找出对应的幺正操作，对有序 B 粒子序列(进行窃听检测后的 B 粒子序列)按顺序执行幺正操作，并预留出检测窃听所需的粒子.

4)Bob 通过经典信道通知 Alice 作好接收准备. Alice 回复后，Bob 通过量子信道把已经编码的有序 B 粒子序列传给 Alice. 并进行窃听检测，检验窃听的步骤是：(1) Bob 通过经典信道把预留出检测窃听的粒子的位置告诉 Alice，(2) 然后，Alice 对预留的相对应的两个粒子分别在四维正交基$\{|0\rangle,|1\rangle,|2\rangle,|3\rangle\}$下进行测量，如果两次测量的结果是关联的，则没有窃听者窃听，通信成功，继续进行下一步；否则，有窃听者存在，放弃该序列粒子，从开始重来.

5)Alice 对已经得到的两个粒子在四维二粒子系统的 Bell 基下进行测量，得到末态 $|\phi_{n'm'}\rangle_{\mathrm{AB}}$. 根据上节的编码规则，Alice 可推算出 Bob 对第二个粒子(B 粒子)作了何种幺正操作，对应操作的编码就是 Bob 所要传输的信息.

3　安全性分析

协议的安全性要求是：在第一次传送 B 序列粒子和第二次传送携带信息序列粒子的过程中，窃听者 Eve 得不到任何有用的信息. 由于 Alice 和 Bob 是要求通信的当事双方，他们不可能自己把通信的秘密信息泄露给他人，因此，在整个通信过程是绝对可靠的. 下面对本协议的安全性进行具体分析.

首先，在第 1)步中涉及到粒子序列的分发，由

量子密钥分发的无条件安全性[10-16]，能够保证 B 序列粒子传输的安全，只要有窃听者存在，就能够被发现. 本协议中，第一次 B 序列粒子的传送和安全性检测过程类似于 BBM92QKD 协议[12]的过程. 在 BBM92QKD 协议中，EPR 对中的一个粒子被发送给 Alice，另一个被发送给 Bob. 本协议中，A 序列粒子被安全地保留在 Alice 手中. 在窃听检测前，窃听者 Eve 没有办法获得 A 序列中的粒子. 因此 B 序列传送的安全性简单地归结为 BBM92QKD 协议的安全性. 文献[13]给出了理想条件下 BBM92QKD 协议的安全性证明，文献[14]详细地给出了实际条件下 BBM92QKD 协议的安全性证明. 基于以上情况，说明本协议中 B 序列粒子的第一次传送是安全的，在此不再给出证明.

其次，由于 Alice 手中始终握有一个粒子(A 粒子)，因此，在通信过程中始终有一个粒子不能被窃听者截获，窃听者最多只能窃获一个粒子(B 粒子)，无法进行二个粒子联合测量，所以窃听者不能截获到有用的信息. 窃听者能获得信息的唯一途径就是猜测，而高维粒子的使用，使得量子态更为多样性. 这个方案中对每个粒子态猜测正确的几率只有 1/16，窃听者不能获得可靠的信息.

基于以上的分析，我们的协议是安全的.

4 结论

该文提出了利用四维二粒子进行超密编码的单向通信方案. Alice 随机制备四维二粒子有序初态序列，把第二个粒子序列(B 粒子系列)传送给 Bob. 信息发送者 Bob 在对其拥有的粒子进行幺正变换后，将粒子发送给信息接收者 Alice. 然后 Alice 对二个粒子进行联合测量，根据测量结果，就可以推知信息发送者已作了那种幺正变换，每种幺正变换对应着 4 bits 经典信息，从而得知信息发送者要传送的信息. 该通信方案只需要传输一个粒子和一次测量就能获得 4 bits 的信息，具有较高的信息传送效力. 该方法还可推广到 2 的幂次方维，其一次传送的信息量也按 2 的幂次方增长. 在该方案中，由于通信双方具有不对称的地位，适用于分散人员或机构向信息中心传递信息. 例如，记者向编辑部发送实时新闻等.

参考文献

[1] SHOR P. Polynomial-tim algorithm for prime factorization and discrete logarithms on a quantum[J]. *SIAMJ J Comput*, 1997, **26**(5): 1484-1509.

[2] GROVER L K. Quantum mechanics helps in searching for a needle in a haystack[J]. *Phys Rev Lett*, 1997, **79**(2): 325-328.

[3] BENNETT C H, WIESNER S J. Communication via one- and two-particle operators on Einstein-Podolsky-Rosen states[J]. *Phys Rev Lett*, 1993, **69**(20): 2881-2834.

[4] BENNETT C H BRASSARD G, CREPEAU C, *et al*. Teleporting an unknow quantum state via dual classical and Einstein-Podolsky-Rosen channels[J]. *Rhys Rev Lett*, 1993, **70**(13): 1895-1898.

[5] XIONG Xue-shi, FU Jie, SHEN Ke. Controlled teleportation of an unknown two-particle partly entangled state [J]. *Acta Photonica. Sin.*, 2006, **35**(5): 780-782.
熊学仕，付洁，沈柯. 二粒子部分纠缠未知态的量子受控传递[J]. 光子学报，2006，**35**(5)：780-782.

[6] LIU X S, LONG G L, TONG D M, *et al*. General scheme for superdense coding between multipaties[J]. *Phys Rev A*, 2002, **65**(2): 022304.

[7] CRUDKA A, WOJCIK A. Symmetric scheme for superdense coding between multipaties[J]. *Phys Rev A*, 2002, **66**(1): 014301.

[8] MATTLE K, WEINFURTER H, KWIAT P G, *et al*. Dense Coding in Experimental Quantum Communication [J]. *Phys Rev Lett*, 1996, **76**(25): 4656-4659.

[9] FANG X M, ZHU X W, FENG M, *et al*. Experimental implementation of dense coding using nuclear magnetic resonance[J]. *Phys Rev A*, 2006, **61**(2): 022307.

[10] BENNETT C H, BRASSARD G. Quantum cryptography: public-key distribution and coin tossing[A]. *Proceedings of the International Conference on Computers, systems and signal Processing*[C]. India: Bangalor Press, 1984, 175-179.

[11] EKERT A K. Quantum cryptography base on Bell's theorem [J]. *Phys Rev Lett*, 1991, **67**(6): 661-663.

[12] BENNETT C H, BRASSARD G, MERMIN N D. Quantum cryptography without Bells theorem[J]. *Phys Rev Lett*, 1992, **68**(5): 557-559.

[13] INAMORI H, RALLAN L, VEDRAL V. Security of EPR-based quantum cryptography againt incoherent symmetric attacks[J]. *J Phys A*, 2001, **34**(35): 6913-6918.

[14] WAKS E, ZEEVI A, YAMAMOTO Y. Security of quantum key distribution with entangled photons against individual attacks[J]. *Phys Rev A*, 2002, **65**(5): 052310.

[15] YI X J, NIE Y Y, ZHOU N R, *et al*. Secure Direct Communication Based on Non-Orthogonal Entangled Pairs and Local Measurement [J]. *International Journal of Theoretical Physics*, 2008, **47**(12): 3401-3407.

[16] CHEN Xia, WANG Fa-qiang, LU Yi-qun, *et al*. A differential phase shift key distribution QKD system combing with efficient BB84 scheme[J]. *Acta Photonica Sinica*, 2008, **37**(5): 1052-1056.
陈霞，王发强，路轶群，等. 结合高效 BB84 协议的差分密钥分发系统[J]. 光子学报，2008，**37**(5)：1052-1056.

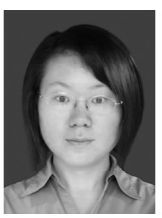
One-way Communication Scheme Based on Superdense Coding of Four Dimension Two Particles

ZHOU Rui[a]，ZHU Yu-lan[a]，NIE Yi-you[a,b]

(*a. Department of Physics；b. Key Laboratory of Photoelectronics & Telecommunication of Jiangxi Province，Jiangxi Normal University，Nanchang* 330022，*China*)

Abstract：A scheme of one-way communication is presented using four-dimension two-particle system，which is based on the superdense coding combined with the classical binary coding. The information sender performs a unitary operation on the particles，and sends the particles to the information receiver. Then information receiver performs a joint measurement on the two particles after receiving the sender's particles. The information receiver can know the information sent by the senter according to the joint measurement results and the encoding rules. In this scheme，four-bit classical information can be encoded after performing one unitary transformation. The security of the one-way communication scheme is also analysed.

Key words：Quantum communication；One-way communication；Superdense coding；Four-dimension two particles



ZHOU Rui　was born in 1974. Now she is studying for the M. S. degree at Jiangxi Normal University. Her research interests focus on quantum optics and quantum information.

NIE Yi-you　was born in 1963.　He is a professor at College of Physics and Communication Electronics，Jiangxi Normal University. His major research interests focus on quantum optics，quantum computation and quantum information.