基于2体三维最大纠缠态的双向量子密集编码*

赵雨曦[1] 王 震[1] 骆 磊[2**]

(1. 辽宁师范大学物理与电子技术学院,辽宁 大连 116029; 2. 大连东软信息学院智能与电子工程学院,辽宁 大连 116023)

摘要:研究了1种基于2体三维最大纠缠态的双向密集编码,给出了2体三维最大纠缠态的具体形式,并构造了针对该最大纠缠态组的完备局域幺正变换集,给出了双向密集编码的解码公式,并进行了安全性分析.

关键词:2体三维最大纠缠态;双向量子密集编码

中图分类号:O413.1 **DOI**:10.19789/j.1004-9398.2020.04.006

0 引 言

量子纠缠是量子力学最显著的特征之一,也是一种有用的量子资源,在量子计算和量子通信中起着重要的作用. 基于2体二维体系最大纠缠态的量子通信技术被广泛应用于量子密钥分发[1-3]、量子隐形传态[4-6]、量子密集编码[7-8]、量子通信[9-10]等领域.

相对于二维量子位,高维量子位具有更大的信息容量,可以比量子比特荷载更多的信息. 人们首先研究了高维量子位在量子密钥分发中的应用. 2002年,Cerf等[11]在理论上提出利用d维量子态来实现量子密钥分发的理论方案,并证明了该方案的安全性;2007年,Khan等[12]提出利用多自由度光子来实现d维量子密钥分发并分析了该方案的实验可行性. 近年来也有研究基于2体三维最大纠缠态的量子信息过程:2019年,Zhang等[13]提出利用辅助纠缠实现高维Bell态的分析方法;同年,Luo等[14]在实验上实现了基于高维Bell态的高维量子隐形传态. 这些研究表明,高维量子位在量子信息过程中有着广泛的应用,但是针对高维最大量子纠缠态具体形式以及高维最大纠缠态的完备局域变换的种类,目前还没有具体给出. 此外,高维量子纠缠态还可以应用在哪些量子信息过程中也没有具体的结论,这些都有待于进一步的研究.

本文以2体三维最大纠缠态为载体进行量子通信,利用文献[15-16]引入的符号法以及文献[17]给出的一般2体最大纠缠态的方法构造2体三维最大纠缠态,以及最大纠缠态的完备局域幺正算符集. 在此基础上,通过改造量子密集编码方案,构造了双向量子密集编码的信息处理过程,并对通信过程的安全性进行了分析.

1 2体三维最大纠缠态

自1935年爱因斯坦等提出EPR佯谬之后,量子纠缠作为一种极具代表性的量子特性引起人们的注意,对量子纠缠的研究有助于更好地理解量子理论,拓广量子纠缠的应用. 量子纠缠是对多子系统量子系统而言,当对其中1个子系统进行测量的同时,测量结果会影响另1个系统的状态,具有纠缠现象的量子系统的量子态称为纠缠态. 纠缠态的定义较为复杂,对于2体纯态而言[18],其定义为:如果量子态$|\psi\rangle_{12}$不能写成如下直积形式,$|\psi\rangle_{12} \neq |\alpha\rangle_1 \otimes |\beta\rangle_2$(其中态$|\alpha\rangle_1$、$|\beta\rangle_2$分别为子系统1、2的量子态),则$|\psi\rangle_{12}$为2体纠缠态.

一般任意高维量子纠缠的结构还不是很清楚,但是对于确定维数的低维量子纠缠态形式和制备过程研究的较为清楚[19-20]. 本文取三维Hilbert空间的1组正交归一基矢量为$\{|1\rangle, |2\rangle, |3\rangle\}$,由文献[17]可知,2体三维Bell态有9个,可以写成如下形式

收稿日期:2019-08-10

*2018年度辽宁省普通高等学校本科教学改革研究项目,辽教函[2018]471号

** 通信作者:luolei@neusoft.edu.cn

$$|\phi_k\rangle_{12}=\Sigma_{ij}C_{ij}|i\rangle_1|j\rangle_2,\quad i,j\in\{1,2,3\}. \tag{1}$$

具体量子态可以表示为

$$\begin{cases}
|\phi_{11}\rangle_{12}=\frac{1}{\sqrt{3}}(|1\rangle_1|1\rangle_2+|2\rangle_1|2\rangle_2+|3\rangle_1|3\rangle_2),\\
|\phi_{22}\rangle_{12}=\frac{1}{\sqrt{3}}(|1\rangle_1|1\rangle_2+\omega|2\rangle_1|_2\rangle_2+\omega^2|3\rangle_1|3\rangle_2),\\
|\phi_{33}\rangle_{12}=\frac{1}{\sqrt{3}}(|1\rangle_1|1\rangle_2+\omega^2|2\rangle_1|2\rangle_2+\omega|3\rangle_1|3\rangle_2),\\
|\phi_{12}\rangle_{12}=\frac{1}{\sqrt{3}}(|1\rangle_1|2\rangle_2+|2\rangle_1|3\rangle_2+|3\rangle_1|1\rangle_2),\\
|\phi_{21}\rangle_{12}=\frac{1}{\sqrt{3}}(|1\rangle_1|2\rangle_2+\omega|2\rangle_1|3\rangle_2+\omega^2|3\rangle_1|1\rangle_2),\\
|\phi_{31}\rangle_{12}=\frac{1}{\sqrt{3}}(|1\rangle_1|2\rangle_2+\omega^2|2\rangle_1|3\rangle_2+\omega|3\rangle_1|1\rangle_2),\\
|\phi_{13}\rangle_{12}=\frac{1}{\sqrt{3}}(|1\rangle_1|3\rangle_2+|2\rangle_1|1\rangle_2+|3\rangle_1|2\rangle_2),\\
|\phi_{23}\rangle_{12}=\frac{1}{\sqrt{3}}(|1\rangle_1|3\rangle_2+\omega|2\rangle_1|1\rangle_2+\omega^2|3\rangle_1|2\rangle_2),\\
|\phi_{32}\rangle_{12}=\frac{1}{\sqrt{3}}(|1\rangle_1|3\rangle_2+\omega^2|2\rangle_1|1\rangle_2+\omega|3\rangle_1|2\rangle_2),
\end{cases} \tag{2}$$

式中 ω 为1的立方根,即 $\omega^3=1$. 容易验证,以上9个态也是2体三维系统的1组正交归一完备基. 记作

$$S_{|\phi\rangle_{12}}=\{|\phi_{11}\rangle_{12},|\phi_{22}\rangle_{12},|\phi_{33}\rangle_{12},|\phi_{12}\rangle_{12},|\phi_{21}\rangle_{12},|\phi_{13}\rangle_{12},|\phi_{31}\rangle_{12},|\phi_{23}\rangle_{12},|\phi_{32}\rangle_{12}\}. \tag{3}$$

对于2体纯态的量子纠缠度,一般采用部分熵纠缠度来衡量[21],其定义为

$$S(|\phi\rangle_{12})=-\mathrm{tr}_i\{\rho_i\log_2\rho_i\},\quad i\in\{1,2\},$$

式中 $\rho_i=\mathrm{tr}_j\{|\phi\rangle_{12}\langle\phi|\}$, $i\neq j\in\{1,2\}$. 由此容易计算出以上9个态部分熵均为

$$S(|\phi_k\rangle_{12})=\log_2 3\approx 1.442\,7. \tag{4}$$

所以,以上9个态为2体三维最大纠缠态. 针对以上9个纠缠态,相应的完备局域量子变换集为 $S=\{\boldsymbol{E}_0,\boldsymbol{E}_1,\boldsymbol{E}_2,\boldsymbol{E}_3,\boldsymbol{E}_4,\boldsymbol{E}_5,\boldsymbol{E}_6,\boldsymbol{E}_7,\boldsymbol{E}_8\}$,各操作具体形式分别为

$$\boldsymbol{E}_0=\begin{pmatrix}1&0&0\\0&1&0\\0&0&1\end{pmatrix},\quad \boldsymbol{E}_1=\begin{pmatrix}1&0&0\\0&\omega&0\\0&0&\omega^2\end{pmatrix},$$

$$\boldsymbol{E}_2=\begin{pmatrix}1&0&0\\0&\omega^2&0\\0&0&\omega\end{pmatrix},\quad \boldsymbol{E}_3=\begin{pmatrix}0&0&1\\1&0&0\\0&1&0\end{pmatrix},$$

$$\boldsymbol{E}_4=\begin{pmatrix}0&0&\omega^2\\1&0&0\\0&\omega&0\end{pmatrix},\quad \boldsymbol{E}_5=\begin{pmatrix}0&0&\omega\\1&0&0\\0&\omega^2&0\end{pmatrix},$$

$$\boldsymbol{E}_6=\begin{pmatrix}0&1&0\\0&0&1\\1&0&0\end{pmatrix},\quad \boldsymbol{E}_7=\begin{pmatrix}0&\omega&0\\0&0&\omega^2\\1&0&0\end{pmatrix},$$

$$\boldsymbol{E}_8=\begin{pmatrix}0&\omega^2&0\\0&0&\omega\\1&0&0\end{pmatrix}. \tag{5}$$

利用文献[17]方法容易验证,式(5)中任一操作,可以把式(2)中任意1个最大纠缠态唯一确定地变成另1个最大纠缠态(忽略态的整体因子). 例如

$$\begin{cases}\boldsymbol{E}_1(1)|\phi_{11}\rangle_{12}\rightarrow|\phi_{22}\rangle_{12},\\ \boldsymbol{E}_1(2)|\phi_{11}\rangle_{12}\rightarrow|\phi_{33}\rangle_{12}.\end{cases}$$

因此可以对该操作进行编码,然后进行量子通信. 对操作进行如下编码约定,即把式(5)中每个量子局域变换都对应为1个数字

$$\begin{cases}\boldsymbol{E}_0\rightarrow 1,\boldsymbol{E}_1\rightarrow 2,\boldsymbol{E}_2\rightarrow 3,\\ \boldsymbol{E}_3\rightarrow 4,\boldsymbol{E}_4\rightarrow 5,\boldsymbol{E}_5\rightarrow 6,\\ \boldsymbol{E}_6\rightarrow 7,\boldsymbol{E}_7\rightarrow 8,\boldsymbol{E}_8\rightarrow 9,\end{cases} \tag{6}$$

在式(6)编码的基础上进行通信.

2　具体方案

本文采用改进的双向密集编码方案,以 $|\phi_{11}\rangle_{12}$ 为例来说明该通信过程. 具体操作如下:通信双方Alice和Bob分别拥有粒子1和粒子2,双方采取式(2)的纠缠完备基和式(5)的完备局域幺正操作集,根据式(6)的编码约定进行如下操作:

(1)Alice和Bob分享处于纠缠态 $|\phi_{11}\rangle_{12}$ 的粒子1和2.

(2)假定Alice要把数字4发送给Bob,同时

Bob 要把数字 7 发送给 Alice. 依据式(6),数字 4 编码为量子局域变换 $\boldsymbol{E}_3$,数字 7 编码为量子局域变换 $\boldsymbol{E}_6$. 然后 Alice 对粒子 1 实施 $\boldsymbol{E}_3$ 操作,记作

$$\boldsymbol{E}_3(1)\,|\,\phi_{11}\rangle_{12} \rightarrow |\,\phi_{13}\rangle_{12}. \tag{7}$$

Bob 要对粒子 2 实施 $\boldsymbol{E}_6$ 操作,记作

$$\boldsymbol{E}_6(2)\,|\,\phi_{13}\rangle_{12} \rightarrow |\,\phi_{12}\rangle_{12}. \tag{8}$$

容易验证,Bob 与 Alice 的操作顺序不影响最后结果.

(3)Alice 把粒子 1 发送给 Bob,Bob 对粒子 1、2 进行式(2)所示的 2 体三维 Bell 基测量,并公布测量结果;或者,Bob 把粒子 2 发送给 Alice,Alice 进行相同的 Bell 基测量,并公布测量结果;也可以是 Alice 和 Bob 把粒子 1、2 发给一个共同的第三方 Carl,Carl 对粒子 1、2 根据式(2)所示的操作进行测量,并公布测量结果。这 3 种操作都可以完成量子通信过程,并且不影响该结果的安全性.

(4)Alice 对照初始态 $|\,\phi_{11}\rangle_{12}$,最终态 $|\,\phi_{12}\rangle_{12}$ 以及自己的局域操作 $\boldsymbol{E}_3(1)$,可以唯一确定地知道 Bob 的局域操作 $\boldsymbol{E}_6(2)$;同样,Bob 对照初始态 $|\,\phi_{11}\rangle_{12}$,最终态 $|\,\phi_{12}\rangle_{12}$ 以及自己的局域操作 $\boldsymbol{E}_6(2)$,可以唯一确定地知道 Alice 的局域操作 $\boldsymbol{E}_3(1)$.

具体解码方式可利用文献[17]中的符号,以及文献[22]中的类似公式给出整个通信过程的公式为

$$\boldsymbol{E}_3(1)\boldsymbol{T}(\phi_{11})_{12}\boldsymbol{E}_6^{\mathrm{T}}(2) = \boldsymbol{T}(\phi_{12})_{12}, \tag{9}$$

式中 $\boldsymbol{T}(\phi_{11})_{12}$、$\boldsymbol{T}(\phi_{12})_{12}$ 分别为初始态 $|\,\phi_{11}\rangle_{12}$ 和最终态 $|\,\phi_{12}\rangle_{12}$ 的符号矩阵,上标 T 表示矩阵的转置. 由上式可知,初始态与最终态是公开的信息,这样对于不知道 Alice 和 Bob 的局域操作,式(9)相当于 1 个二元一次方程

$$x \cdot a \cdot y = b, \tag{10}$$

x 与 y 是不可知的. 但是对于 Alice 来说,对粒子 1 所实施的局域操作是可知的,此时方程(9)对于 Alice 而言就是 1 个一元一次方程,可以唯一确定 Bob 的局域操作

$$\boldsymbol{E}_6(2) = [\boldsymbol{T}^{\dagger}(\phi_{11})_{12}\boldsymbol{E}_3(1)^{\dagger}\boldsymbol{T}(\phi_{12})_{12}]^{\mathrm{T}}. \tag{11}$$

同样,对于 Bob 可以得到解码公式

$$\boldsymbol{E}_3(1) = \boldsymbol{T}(\phi_{12})_{12}[\boldsymbol{E}_6^{\mathrm{T}}(2)]^{\dagger}\boldsymbol{T}^{\dagger}(\phi_{11})_{12}, \tag{12}$$

式中 † 表示矩阵的复共轭.

3 安全性分析

在通信过程中,信息的安全性十分重要. 依赖于纠缠的量子通信方案往往都要建立在纠缠粒子安全分享的基础上,利用文献[3]的操作很容易实现纠缠对的安全分享. 所以,本文的讨论均基于纠缠通道已经安全建立的情况下,在其他可能的窃听攻击下,通信的安全问题.

如果在步骤(3)中 Alice 发给 Bob 的粒子 1(或者 Bob 发给 Alice 的粒子 2)被窃听者截获并替换,因为信息是编码在纠缠态 $|\,\phi_{12}\rangle_{12}$ 上的,窃听者并不能从单个粒子 1(或粒子 2)中获得通信双方局域操作信息. 但这样做的后果会导致纠缠态 $|\,\phi_{12}\rangle_{12}$ 被破坏,形成一种类似截断通道的攻击,会被通信双方发现.

如果在步骤(3)通信双方把各自粒子发送给第三方时被窃听者全部截获替换,也就是窃听者获得最终态 $|\,\phi_{12}\rangle_{12}$,如果窃听者为了不被发现依旧正确公布测量结果,则通信过程依然成立,而由式(10)可知,窃听者依然无法知道通信双方的局域操作. 因此,此通信过程是安全的.

4 结 论

量子密集编码信息是发送者通过 1 个粒子传递 2 个粒子荷载信息的单向通信过程,本文推广到基于 2 体三维最大纠缠态的双向通信过程,并构造了完备的 2 体三维最大纠缠态形式,给出了针对该最大纠缠态的完备局域操作元素. 在此基础上,提出了基于 2 体三维最大纠缠态的双向量子密集编码方案,并分析指出该方案在安全分享了纠缠通道情况下是安全的. 此方法也可以推广到更高维的情况.

参 考 文 献

[1] EKERT A K. Quantum cryptography based on Bell′s theorem[J]. Phys Rev Lett,1991,67(6):661.

[2] BENNETT C H. Quantum cryptography using any two nonorthogonal states[J]. Phys Rev Lett, 1992, 68(21): 3121 - 3124.

[3] LI C, SONG H S, ZHOU L, et al. A random quantum key distribution by using Bell states[J]. Journal of Optics B Quantum and Semiclassical Optics,2003,5(2):155 - 157.

[4] BENNETT C H, BRASSARD G, CRÉPEAU C, et al. Teleporting an unknown quantum state via dual classical and

Einstein-Podolsky-Rosen channels[J]. Phys Rev Lett,1993,70(13):1895 – 1899.
[5] HUO M, QIN J L, CHENG J L,et al. Deterministic quantum teleportation through fiber channels[J]. Science Advances, 2018,4(10):eaas9401.
[6] REINDL M, HUBER D, SCHIMPF C, et al. All-photonic quantum teleportation using on-demand solid-state quantum emitters[J]. Science Advances, 2018, 4(12):eaau1255.
[7] BENNETT C H, WIESNER S J. Communication via one and two-particle operators on Einstein-Podolosky-Rosen states [J]. Phys Rev Lett,1992,69(20):2881 – 2884.
[8] BARREIRO J T, WEI T C, KWIAT P G. Beating the channel capacity limit for linear photonic superdense coding[J]. Nature Physics,2008,4(4):282 – 286.
[9] DENG F G, LONG G L, LIU X S. Two-step quantum direct communication protocol using the Einstein-Podolsky-Rosen pair block[J]. Phys Rev A, 2003,68(4):042317.
[10] DENG F G, LONG G L. Secure direct communication with a quantum one-time pad[J]. Phys Rev A, 2004, 69(5): 052319.
[11] CERF N J, BOURENNANE M, KARLSSON A, et al. Security of quantum key distribution using *d*-level systems[J]. Phys Rev Lett,2002, 88(12):127902.
[12] KHAN I A, BROADBENT C J, HOWELL J C. Large-alphabet quantum key distribution using energy-time entangled bipartite states[J]. Phys Rev Lett,2007,98(6):060503.
[13] ZHANG H, ZHANG C, HU X M, et al. Arbitrary two-particle high-dimensional Bell-state measurement by auxiliary entanglement[J]. Phys Rev A,2019, 99(5):052301.
[14] LUO Y H, ZHONG H S, ERHARD M, et al. Quantum teleportation in high dimensions[J]. Phys Rev Lett,2019,123(7):070505.
[15] LI C, SONG H S, LUO Y X. Criterion for general quantum teleportation[J]. Phys Lett A, 2002, 297(3 – 4): 121 – 125.
[16] LI C, WANG Z, SONG H S,et al. Alternative new notation for quantum information theory[J]. International Journal of Theoretical Physics, 2007, 46(7):1815 – 1822.
[17] WANG Z, TIAN L J, CAO W Z. Conditions for bipartite general Bell states[J]. International Journal of Quantum Information,2010, 8(7): 1213 – 1217.
[18] HORODECKI R, HORODECKI P, HORODECKI M, et al. Quantum entanglement[J]. Rev Mod Phys, 2009, 81(2): 865 – 942.
[19] 赵慧,张建峰. 一类高维量子态的生成纠缠[J]. 首都师范大学学报(自然科学版),2005,26(3):1 – 2 + 6.
[20] 张雅慈,曲艳玲,张凤阳. 混合固态量子信息处理器[J]. 首都师范大学学报(自然科学版),2017,38(2):41 – 46.
[21] HORODECKI R, HORODECKI P. Quantum redundancies and local realism[J]. Physics Letters A, 1994, 194(3): 147 – 152.
[22] WU Y H, ZHAI W D, CAO W Z, et al. Quantum secure direct communication by using general entangled states[J]. International Journal of Theoretical Physics,2011,50(2): 325 – 331.

Bidirectional Quantum Dense Coding Based on Two-particle Three-dimensional Maximal Entangled States

ZHAO Yuxi[1] WANG Zhen[1] LUO Lei[2]

(1. School of Physics and Electronic Technology, Liaoning Normal University, Dalian Liaoning 116029;
2. School of Intelligence and Electronic Engineering, Dalian Neusoft University of Information, Dalian Liaoning 116023)

Abstract: A Bidirectional quantum dense coding based on two-body three-dimensional maximally entangled states was studied, the concrete form of two-body three-dimensional maximally entangled state was given, the complete local unitary transformation set for the maximally entangled state group was constructed, the decoding formula of bidirectional dense coding was given, and the security was proven.

Keywords: two-body three-dimensional maximally entangled states; bidirectional quantum dense coding