基于四粒子团簇态的量子安全直接通信协议仿真*

李先忠[1], 何国田[1,2], 张 欣[1]
(1. 重庆师范大学 计算机与信息科学学院, 重庆 401331; 2. 中国科学院重庆绿色智能技术研究院, 重庆 401122)

摘 要: 随着量子通信在近年来的不断发展,量子安全直接通信成为了量子通信的一大重要分支。但目前的实验设备很难满足量子通信实验,导致通信协议的正确性和安全性无法得到验证。针对这一问题,提出了一种协议仿真算法。在 Microsoft Visual C ++6.0 平台上利用 C ++ 语言编写了量子安全直接通信协议的仿真程序,最终实现了发送方和接收方之间的有效安全通信。仿真结果体现了量子通信的高效性和绝对安全性。实验结果与理论结果相吻合,进一步验证了协议是安全、正确的,也证明了用计算机对量子计算进行仿真的可行性。

关键词: 量子态; 量子通信; 量子安全直接通信; 仿真
中图分类号: TP391.9;TP393 **文献标志码**: A **文章编号**: 1001-3695(2013)12-3705-03
doi:10.3969/j.issn.1001-3695.2013.12.048

Simulation of quantum secure direct communication protocol based on four-qubit cluster state

LI Xian-zhong[1], HE Guo-tian[1,2], ZHANG Xin[1]
(1. *College of Computer & Information Science, Chongqing Normal University, Chongqing* 401331, *China*; 2. *Chongqing Institute of Green & Intelligent Technology, Chinese Academy of Sciences, Chongqing* 401122, *China*)

Abstract: With the development if quantum communication, quantum secure direct communication has become a very important branch of quantum communication. But the current experiment equipment is difficult to meet the quantum communication experiment, which leads to correctness and safety of the communication protocol cannot be verified. In order to solve this problem, this paper proposed a protocol simulation algorithm. In Microsoft Visual C ++ 6.0 platform using C ++ language to write the simulation program of quantum secure direct communication protocol, finally achieved effective and safe communication between sender and receiver. Simulation result reflects the high efficiency and absolute security features of quantum communication, in addition, consistent with the theoretical results further verify the correctness of the proposed agreement, also proves the feasibility of quantum computing simulation with computers.

Key words: quantum state; quantum communication; quantum secure direct communication protocol; simulation

0 引言

量子通信和量子计算[1,2]是近年迅速发展的热门学科,是量子力学理论、计算机通信和数学相结合的新型交叉学科。1984 年,第一个量子密钥分配方案(quantum key distribution, QKD)BB84 协议[3]由 Bennett 和 Brassard 提出,由此迎来了通信时代的新局面,更为密码学带来了新方向。该协议在量子不可克隆原理的基础上利用两组正交的量子基实现密钥分配,完成密钥的共享,首次实现了通信的绝对安全。但是标准 QKD 传输效率比较低,大量的量子比特不能被有效利用。为了提高传输效率,研究人员又提出了量子安全直接通信(QSDC)[4,5]。QSDC 和 QKD 的通信原理不同,它可以实现秘密消息的直接传送而无须事先共享经典密钥再对秘密消息进行加密。

目前提出的量子安全直接通信协议按信息载体可分为两类,即基于单光子系统的 QSDC 和基于纠缠系统的 QSDC。2005 年,Man 等人[6]提出了基于纠缠交换和局域幺正操作的安全直接通信协议。2006 年,Lee 等人[7]提出了基于 GHZ 态的带认证的量子安全直接通信协议;Cao 等人[8]提出了一种基于四粒子 W 态的安全直接通信协议;之后,杨新元等人[9]对该协议提出了改进。王剑等人[10]提出一种基于纯纠缠态的量子安全直接通信协议,发送方通过控制非操作和 von Neumann 测量,将秘密消息编码在纯纠缠态上并发送给接收方,该协议具有较高的量子比特效率。徐红云等人[11]提出一种新的带认证的三方量子安全直接通信协议,该方案利用共享的三粒子部分纠缠态和 CNOT 门来编码和译码,两方可同时向第三方传递秘密消息。权东晓等人[12]提出了基于单光子的单向量子安全通信方案。刘晓芬等人[13]提出了一个可抵抗旋转噪声的双向量子安全直接通信协议,消息分发者直接将 1 bit 秘密信息编码到对应的相干保持态,接收者执行确定的测量来解码消息。曹正文等人[14]提出了一种新的基于一类 W 态密集编码的量子安全直接通信方案,协议用到了安全检测粒子和传输粒子,大大提高了通信效率。2001 年,Briegel和 Raussendorf 提出了一种当粒子数不小于 4 时才能体

收稿日期: 2013-03-30; **修回日期**: 2013-06-05 **基金项目**: 国家高技术研究发展计划资助项目(2012AA040603)

作者简介:李先忠(1986-),男,山东菏泽人,硕士,主要研究方向为量子通信与信息安全(493402719@qq.com);何国田(1968-),男,四川人,教授,博士,主要研究方向为纳米精度光学干涉测量、磁流变机理及其应用、机器人技术;张欣(1989-),女,重庆北碚人,硕士,主要研究方向为教育技术学.

现出某种特殊性质的新量子,即团簇态。它不仅包含了 GHZ 态[15]和 W 态[16]的纠缠态性质 ,而且还具有最大连通性和纠缠顽固性[17,18],其持续纠缠性也更强。本文要仿真的协议选用了四粒子团簇态[19]作为信息载体,提高了通信效率及安全性。

目前对 QSDC 的研究主要体现在理论创新和科学实验上。做量子通信实验时,用现有设备和仪器制备并保存量子态比较困难,对量子态的测量和操作比较复杂且昂贵。很多量子通信协议只是在理论上进行论证。Gottesman-Knill 定理[20,21]为在计算机上进行量子通信仿真提供了可能。该定理表明,若量子通信建立于计算基组上,且只使用 Clifferd 群(如 Hadamard 门、相位门、CNOT 门和 Pauli 门)在计算基组上测量,则可以用计算机有效地仿真。结合以上问题,本文对一种 QSDC 协议在 Microsoft Visual C ++6.0 平台上进行了模拟仿真,主要研究量子通信安全性以及仿真可行性。QSDC 协议的仿真可以为量子通信的研究提供一种新的研究手段,借此,还可以为量子通信的实现和量子加密提供一定的辅助作用。

1 量子安全直接通信协议

通信协议用到 Z 基$\{|0\rangle,|1\rangle\}$、X 基$\{|+\rangle,|\rightarrow\}$、4 个 Bell 态、3 个 Pauli 算子、一个 Hadamard 门(H 门)。它们分别为

$$|+\rangle=\frac{1}{\sqrt{2}}(|0\rangle+|1\rangle),|\rightarrow=\frac{1}{\sqrt{2}}(|0\rangle-|1\rangle)$$

$$|\beta_{00}\rangle=\frac{1}{\sqrt{2}}(|00\rangle+|11\rangle),|\beta_{01}\rangle=\frac{1}{\sqrt{2}}(|01\rangle+|10\rangle)$$

$$|\beta_{10}\rangle=\frac{1}{\sqrt{2}}(|00\rangle-|11\rangle),|\beta_{11}\rangle=\frac{1}{\sqrt{2}}(|01\rangle-|10\rangle)$$

$$\sigma_0=I=\begin{bmatrix}1&0\\0&1\end{bmatrix},\sigma_x=\begin{bmatrix}0&1\\1&0\end{bmatrix},\sigma_z=\begin{bmatrix}1&0\\0&-1\end{bmatrix};H=\frac{1}{\sqrt{2}}\begin{bmatrix}1&1\\1&-1\end{bmatrix}$$

四粒子团簇态记为

$$|\psi\rangle_{1234}=\frac{1}{2}(|0000\rangle+|0011\rangle+|1100\rangle-|1111\rangle)$$

首先,Alice 制备 $2n$ 个四粒子团簇态,随机选出 n 个态作为校验态,对量子信道进行安全性检测,并判断量子信道中是否有窃听者 Eve 窃听。检测阶段用到两个算子:

$$U_I=\sigma_I\otimes\sigma_I\otimes\sigma_I\otimes\sigma_I$$

$$U_x=\sigma_x\otimes\sigma_x\otimes\sigma_x\otimes\sigma_x$$

Alice 对 n 个校验态随机进行或操作,随后 Alice 将校检态中粒子 1、2 组成序列 Q_A,粒子 3、4 组成 Q_B,其中:

$$Q_A=\{P_1(1)\otimes P_1(2),P_2(1)\otimes P_2(2),\cdots,P_n(1)\otimes P_n(2)\}$$

$$Q_B=\{P_1(3)\otimes P_1(4),P_2(3)\otimes P_2(4),\cdots,P_n(3)\otimes P_n(4)\}$$

然后把 Q_B 发送给 Bob,双方对校检序列进行测量,Alice 比较双方测量结果得出误码率。若误码率高于 25% 则认为有 Eve 在窃听;低于 25% 认为通信环境安全。若量子信道安全,则可以通信。Alice 把余下的 n 个态作为编码序列对消息编码。发送 0(1),则对粒子 2 执行 σ_0(σ_x)变换。同时对粒子 1 随机执行 σ_0 或 σ_z 变换,目的在于使译码阶段公布的测量结果等概率出现$|\beta_{00}\rangle$、$|\beta_{01}\rangle$、$|\beta_{10}\rangle$和$|\beta_{11}\rangle$,从而可以防止 Eve 从测量结果中获取信息。编码方案如表 1 所示。编码完成后,双方分别对手中的粒子进行 Bell 基测。Alice 把测量结果发送给 Bob,Bob 对比测量结果译码获得消息。译码规则如表 2 所示。

表 1 编码方案

消息	粒子 1	粒子 2	编码后的四粒子团簇态
0	σ_0	σ_0	$\sigma_0\otimes\sigma_0\otimes\sigma_0\otimes\sigma_0|\psi\rangle_{1234}$
0	σ_z	σ_0	$\sigma_z\otimes\sigma_0\otimes\sigma_0\otimes\sigma_0|\psi\rangle_{1234}$
1	σ_0	σ_x	$\sigma_0\otimes\sigma_x\otimes\sigma_0\otimes\sigma_0|\psi\rangle_{1234}$
1	σ_z	σ_x	$\sigma_z\otimes\sigma_x\otimes\sigma_0\otimes\sigma_0|\psi\rangle_{1234}$

表 2 译码方案

	$\|\beta_{00}\rangle$	$\|\beta_{01}\rangle$	$\|\beta_{10}\rangle$	$\|\beta_{11}\rangle$		$\|\beta_{00}\rangle$	$\|\beta_{01}\rangle$	$\|\beta_{10}\rangle$	$\|\beta_{11}\rangle$
$\|\beta_{00}\rangle$	0	×	0	×	$\|\beta_{10}\rangle$	0	×	0	×
$\|\beta_{01}\rangle$	1	×	1	×	$\|\beta_{11}\rangle$	1	×	1	×

注:×表示不会出现相应组合。

2 仿真实验

2.1 算法流程

根据协议的通信过程编写仿真程序。算法流程如图 1 所示。

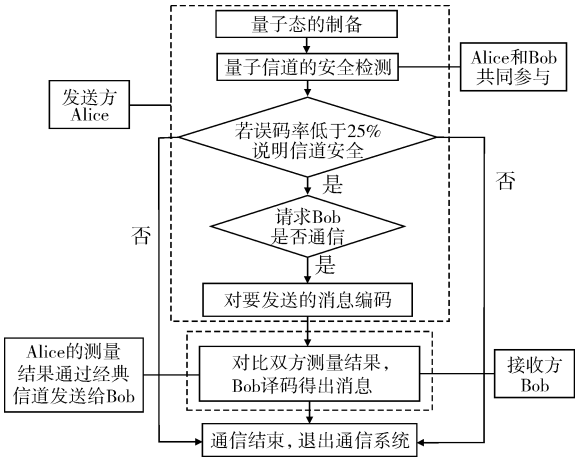

图 1 算法流程

2.2 协议仿真

2.2.1 量子态的表示

协议中用到了不同的量子态,在算法中用矩阵来表示它们。算法中矩阵的构造函数如下:

```
Matrix:Matrix(int r,int c)
{   ++MatrixCount;
    Row=r;   Col=c;
    size=Row*Col;
    ptr=new Complex[size];
    for(int m=0;m<Row;m++)
      for(int n=0;n<Col;n++)
      {   ptr[m+n*Row]=m;   }
}
```

例如,Z 基中的$|1\rangle$可以定义为 Matrix one_state(2,1)。其余量子态均可类似表示。为方便灵活表示,在算法中又加入了设置矩阵元素值的函数 Complex Set(int i,Complex j),此函数可以随意更改矩阵元素值,其具体实现如下:

```
Complex Matrix:Set(int i,Complex j)
{   if(i>=Row*Col)
    { cout <<"错误: 越界!" <<endl;   return 0;}
    else
    { ptr[i]=j;    return ptr[i];}
}
```

启动可视化程序后,首界面如图 2 所示。

2.2.2 安全检测阶段

量子态制备完成后,协议进入量子信道安全检测阶段。该阶段要对量子态作幺正变换,会用到矩阵之间的加减乘除以及张量积(也称为直积)。这些运算中最复杂的是张量积,用符

号⊗表示,设有矩阵 $A=(a_{ij})_{p\times q}$ 和 B,那么:

$$A\otimes B=\begin{bmatrix} a_{11}B & a_{12}B & \cdots & a_{1q}B \\ a_{21}B & a_{22}B & \cdots & a_{2q}B \\ \vdots & \vdots & & \vdots \\ a_{p1}B & a_{p2}B & \cdots & a_{pq}B \end{bmatrix}$$

在算法中运用运算符重载张量积 Matrix operator^(Matrix &),其具体实现如下:

```
Matrix Matrix:operator^(Matrix &mat)
{Matrix temp(Row * mat. Row,Col * mat. Col);
int i,j,k,l,a,b;
for(i=0;i<Row;i++)
  for(j=0;j<Col;j++)
    for(k=0;k<mat. Row;k++)
      for(l=0;l<mat. Col;l++)
      {
a=(i-1) * mat. Row+k+mat. Row;
b=(j-1) * mat. Col+l+mat. Col;
temp. ptr[a+b * Row * mat. Row]=ptr[i+j * Row] * mat. ptr[k+l * mat. Row];
      }
return temp;
}
```

对量子态作幺正变换后,量子态并非完全按照理论值变化,而是会出现一定程度的塌缩现象,为模拟这种不确定的塌缩现象,编写程序时引用 C ++ 语言中 srand((unsigned)time(NULL)随机函数。在程序中对 n 个态中逐次使用随机函数得到实际测量值,然后再与理论值逐一比较,得出发生塌缩现象的量子态的个数,然后计算出误码率。根据误码率的高低决定是否进行通信。以下是统计塌缩个数的函数。

```
if((cs1[a](b+1,1))! =(cs2[a](b+1,1)))
{ErrorNumber=ErrorNumber+1;
}
```

在图 2 界面点击“开始检测”按钮开始信道安全检测,如果误码率低于 25%,则弹出图 3 所示界面。

如果误码率高于 25%,则弹出图 4 所示界面,此消息表明信道存在窃听者,通信将泄密,系统默认不进行通信,这时请点击“结束通信”或“退出检测”退出。

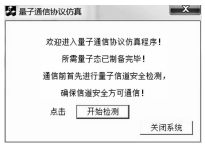

图 2　启动界面

图 3　信道安全

图 4　信道不安全

2.2.3　编码和译码阶段

如果检测后出现如图 3 所示界面,就说明量子信道是安全的。Bob 同意通信,点击“开始通信”对消息序列进行编码。例如对消息 0 进行编码,实现如下:

```
if(message[i]=='0')
{if(i%2==0)
  {cs[i]=UI&cluster_state;}
  else if(i%2==1)
  {cs[i]=ZI&cluster_state;}
}
```

一个团簇态发送一位消息,编码完成后,消息发送成功,等待对方提取,如图 5、6 所示。提取过程如下:

```
for(int f=0;f<strlen(message);f++)
{if((cs[f]==NewState1)||cs[f]==NewState2))
    {  cout<<0;  }
  if((cs[f]==NewState3)||(cs[f]==NewState4))
    {  cout<<1;  }
}
```

3　仿真结果与分析

根据量子安全直接通信协议的过程设计出仿真算法的流程,利用 Microsoft Visual C ++ 6.0 平台对协议进行仿真。图 7 是模拟通信前对信道安全 20 次检测的统计情况。可以看出,在通信前协议总能检测出信道是否安全,这为协议提供了安全保障。图中虚线是安全警戒线,安全警戒线以上表示信道不安全。此外,由于量子具有不可克隆的特点,在信道安全的条件下进行通信时,第三方也不可能窃取到任何有用的消息。实验结果同样也证明了协议是安全的。在信道安全的情况下进行模拟通信,通过多次实验和分析得到表 3,不难看出该协议通信完全可行。

图 5　发送消息

图 6　获取消息

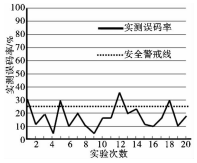

图 7　信道安全检测实验结果

表 3　发送、接收消息对比

Alice 发送消息	Bob 接收消息	Alice 发送消息	Bob 接收消息
101	101	001	001
1111	1111	0101	0101
0001	0001	1101	1101
00101	00101	11001	11001
111101	111101	011010	011010
0000011	0000011	1010111	1010111
1001001	1001001	1110000	1110000
1010101	1010101	1010101	1010101

通过以上仿真数据和实验结果可以看出,量子安全直接通信协议是安全高效的,协议的正确与否和在计算机上进行仿真的可行性都得到了有力的证明。

4　结束语

在计算机上设计了基于四粒子团簇态的量子安全直接通信协议的算法,并用 C ++ 语言在 Microsoft Visual C ++ 6.0 平台上实现了通信的仿真过程。仿真平台得到的结果与量子安全直接通信协议的理论结果在数值是上一致的,这不仅表明了协议的正确性和安全性,也表明了在计算机上仿真量子通信过程是可行的。计算机仿真能有效验证量子计算、量子通信的正确性和安全性,可以把它视为研究量子计算和量子通信的一种新手段,可为量子通信的研究和发展起到推波助澜的作用。

参考文献:

[1] 郑建国,覃朝勇. 量子计算进展与展望[J]. 计算机应用研究, 2008,25(3):641-645.

[2] 陈晖,徐兵杰,王运兵. 量子信息技术及其应用探讨[J]. 中国电子科学研究院学报, 2012, 7(5): 441-445.

[3] BENNETT C H, BRASSARD G. Quantum cryptography: public key distribution and coin tossing[C]//Proc of IEEE International Conference on Computers, Systems, and Signal Processing. 1984:175-179.

[4] 杨静. 量子安全直接通信的理论研究[D]. 北京:北京邮电大学, 2012.

[5] 龙桂鲁, 王川, 李岩松,等. 量子安全直接通信[J]. 中国科学:物理学 力学 天文学, 2011, 41(4): 332-342.　(下转第 3715 页)

资源 2 中得出真正均衡的节点数不超过 10 个。图 3(b)却保证节点查询请求负载与节点能力保持一致。图 4 中虽然单重资源 1 和多重资源的常规负载节点都可以达到 950 个以上,但单重资源 1 却并不能真实地代表节点的负载情况。

实验结果最终表明,在网络中同时存在两种瓶颈资源的情况下,若只考虑一种资源的负载均衡,将忽视节点的其他瓶颈资源的能力。而 MRLB 算法能确保节点承担的每个资源的负载与自身能力值基本保持一致,也就是实验中存储负载和处理请求负载都随着对应资源能力的上升而增加。理论上 MRLB 算法适用于任意数目的瓶颈资源,但随着瓶颈资源数目的增加,相应计算量也将增加,节点上每个资源同时达到负载均衡的难度也将增加。

5　结束语

本文通过相似度模型和转移代价函数,设计出了 MRLB 算法。该算法运用令牌环轮询机制来收集全局信息,并使用管理节点负责虚拟服务器的转移,最终实现了任意结构化 P2P 网络下多种资源的负载均衡问题。仿真实验表明,MRLB 算法使网络中节点各尽其能,最优化地利用了网络资源,避免了瓶颈节点的产生。如何使 MRLB 算法更好地适应 Churn 情形,满足网络的动态环境,以及在转移虚拟服务器时考虑拓扑一致性,尽可能降低转移开销,这些问题是今后研究的重点。

参考文献:

[1] STOICA I, MORRIS R, KARGER D, *et al*. Chord: a scalable peer-to-peer lookup service for Internet applications [C]//Proc of Conference on Application, Technologies, Architectures, and Protocols for Computer Communications. New York: ACM Press, 2001: 149-160.

[2] ROWSTRON A, DRUSCHEL P. Pastry: scalable, decentralized object location, and routing for large-scale peer-to-peer systems [C]// Proc of IFIP/ACM International Conference on Distributed Systems Platforms. Berlin: Springer, 2001: 329-350.

[3] RATNASAMY S, FRANCIS P, HANDLEY M, *et al*. A scalable content-addressable network [C]//Proc of Conference on Application, Technologies, Architectures, and Protocols for Computer Communications. New York: ACM Press, 2001: 161-172.

[4] RAO A, LAKSHMINARAYANAN K, SURANA S, *et al*. Load balancing in structured P2P systems [C]//Proc of International Workshop on Peer-To-Peer Systems. Berkely: Springer, 2003: 68-79.

[5] GODFREY B, LAKSHMINARAYANAN K, SURANA S, *et al*. Load balancing in dynamic structured P2P systems [C]//Proc of IEEE INFOCOM. Washington DC: IEEE Computer Society, 2004: 2253-2262.

[6] ZHU Y. Load balancing in structured P2P networks [M]//Handbook of Peer-to-Peer Networking. Berlin: Springer, 2009: 1149-1164.

[7] ZHU Y, HU Y. Efficient, proximity-aware load balancing for DHT-based P2P systems [J]. IEEE Trans on Parallel and Distributed Systems, 2005, 16(4): 349-361.

[8] HSIAO H C, LIAO H, CHEN S T, *et al*. Load balance with imperfect information in structured peer-to-peer systems [J]. IEEE Trans on Parallel and Distributed Systems, 2011, 22(4): 634-649.

[9] HAUTAKORPI J, MÄENPÄÄ J. Load balancing for structured P2P networks using the advanced finger selection algorithm (AFSA) [C]//Proc of ACM Symposium on Applied Computing. New York: ACM Press, 2010: 655-662.

[10] 张宇翔, 张宏科. 一种层次结构化 P2P 网络中的负载均衡方法 [J]. 计算机学报, 2010, 33(9): 1580-1590.

[11] AGHBARI Z A, KAMEL I, MUSTAFA A. Dynamic storage and access load balancing for answering range queries in peer-to-peer networks [J]. Peer-to-Peer Networking and Applications, 2009, 4(4): 391-409.

[12] TOMIMOTO T, TACHIBANA T, SUGIMOTO K. Capability-aware object management based on skip list in large-scale heterogeneous P2P networks [J]. WSEAS Trans on Communications, 2010, 9(5): 312-321.

[13] MI W, ZHANG C H, QIU X F. SLBA: a security load-balancing algorithm for structured P2P systems [J]. Journal of Computational Information Systems, 2012, 8(7): 2751-2760.

(上接第 3707 页)

[6] MAN Zhong-xiao, ZHANG Zhan-jun, LI Yong. Deterministic secure direct communication by using swapping quantum entanglement and local unitary operations[J]. Chinese Physics Letters, 2005, 22(1): 18-21.

[7] LEE H, LIM J, YANG H. Quantum direct communication with authentication[J]. Physical Review A, 2006, 73(4):042305-1-5.

[8] CAO Hai-jing, SONG He-shan. Quantum secure direct communication with W state[J]. Chinese Physics Letters, 2006, 23(2): 290-292.

[9] 杨新元,马智,吕欣. 基于 W 态的量子安全直接通信协议[J]. 计算机科学, 2009, 36(10):68-71.

[10] 王剑,张盛,张守林,等. 基于纯纠缠态的量子安全直接通信协议[J]. 国防科技大学学报, 2009, 31(2): 51-54.

[11] 徐红云,杨新元,马智,等. 基于部分纠缠态的量子安全直接通信协议[J]. 计算机工程, 2010, 36(2): 170-172.

[12] 权东晓,裴昌幸,刘丹,等. 基于单光子的单向量子安全通信协议[J]. 物理学报, 2010, 59(4): 2493-2496.

[13] 刘晓芬,潘日晶. 集体旋转噪声信道上的量子安全直接通信[J]. 福建师范大学学报:自然科学版, 2011, 27(5): 117-119.

[14] 曹正文,冯晓毅,康维宏,等. 基于一类 W 态密集编码的量子安全直接通信方案[J]. 光电子·激光, 2012, 23(6): 1152-1158.

[15] 王晓芹,逯怀新,赵加强. 广义 GHZ 态的纠缠与非定域性[J]. 物理学报, 2011, 60(11): 110301-1-5.

[16] 王晓芹,逯怀新,赵加强. 三体 W 态的纠缠与非定域性[J]. 量子电子学报, 2012, 29(5): 542-546.

[17] SALEMIAN S, MOHAMMADNEJAD S. An error-free protocol for quantum entanglement distribution in long-distance quantum communication[J]. Chinese Science Bulletin, 2011, 56(7):618-625.

[18] HAO Xiang, SHA Jin-qiao, SUN Jian, *et al*. Dynamics of quantum entanglement in reservoir with memory effects [J]. Communications in Theoretical Physics, 2012, 57(1):29-33.

[19] LIU Zhi-hao, CHEN Han-wu, LIU Wen-jie, *et al*. Quantum secure direct communication with optimal quantum superdense coding by using general four-qubit states[J]. Quantum Information Processing, 2013, 12(1):587-599.

[20] NIELSEN M A, CHUANG I L. Quantum computation and quantum information [M]. Cambridge, UK: Cambriage University Press, 2000: 464-465.

[21] MAURICIO, GUTIÉRREZ, LUKAS, *et al*. Approximation of realistic errors by Clifford channels and Pauli measurements [J]. Physical Review A, 2013, 87(3): 030302(R)1-5.