DOI:10.11721/cqnuj20150225

基于 EPR 对的 Two-step QSDC 方案模拟研究*

曹 锟[1], 何国田[2,1], 李先忠[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:量子安全直接通信(Quantum secure direct communication,QSDC)协议是继 BB84 和 EPR 协议之后提出的关于量子通信的一个重要协议。自 2000 年龙桂鲁和刘晓曙提出第一个 QSDC 协议以来,得到了迅速发展。随后,邓富国等利用块传输思想,提出了基于 EPR 对的 Two-Step QSDC 方案。研究提出了光子的制备、光子通过偏振片前后的变化等算法,利用 AS 代码将量子通信过程中一些不可观察的过程可视化,并以 Flash 技术为载体,对基于 EPR 对的 Two-Step QSDC 方案进行了模拟仿真。模拟结果在直观展示出通信过程的基础上,证明了利用计算机对量子通信进行仿真的可行性。

关键词:EPR 对;量子通信;量子安全直接通信;模拟
中图分类号:TP391.41 **文献标志码**:A **文章编号**:1672-6693(2015)02-0133-05

量子通信[1]是 80 年代末发展起来的一门交叉学科,它是指利用量子态进行编码和携带信息,并对信息进行加工、处理、传输和提取的过程。量子通信的研究内容主要包括量子密码、量子直接通信(Quantum direct communication,QDC)和量子通信网络(Quantum communication network,QCN)等[2]。QDC 不同于传统的量子密钥分配(Quantum key distribution,QKD),通信双方不需要共享密钥就可以直接交换重要的信息,从而简化了量子密码通信的过程。按照量子通信是否需要经典辅助位的要求,将 QDC 分为两种类型:量子安全直接通信(QSDC)和确定型安全量子通信[3](DSQC)。

2000 年,Long 和 Liu 提出了第一个可以用于 QSDC 的物理模型,这个方案可以用于直接传输机密信息[4]。2003 年,Deng、Long 和 Liu 在 QSDC 的物理模型基础上,提出了高效的安全检测方法,给出了噪声下的常规处理和可能的实验实现方法,并给出了安全通信需要的条件。目前提出的 QSDC 协议按照信息载体可分为两类:一类是基于单光子系统的 QSDC,包括基于单光子的 QSDC 协议[5]、基于单光子顺序重排的 QSDC 协议[6]和基于单光子的单向 QSDC 协议[7]等;一类是基于纠缠系统的 QSDC,包括"Ping-Pong"协议[8]、基于 EPR 对的 Two-Step QSDC 方案[9]和基于超密集编码的 QSDC 方案[11]等。其中,基于 EPR 对的 Two-Step QSDC 方案是 Deng[9-10]等人在 2003 年提出的,该方案利用纠缠系统中只有对整个系统做联合测量才能读出操作信息的特性,在引进块传输思想的基础上,分步实现信息的直接传输。

本文以 Flash 为载体[12],对基于 EPR 对的 Two-Step QSDC 方案的主要传输过程进行了模拟。通过 Action Script 代码的设计和动画的演示,将一些不可观察的过程(例如:光子的制备,EPR 对的性质,检测和编码的过程等)直观地展示出来,并对其进行了分析和总结。

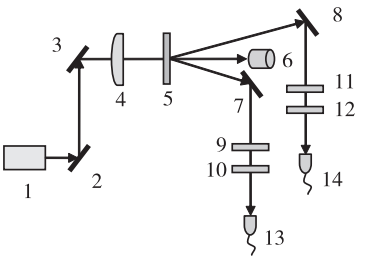
1 EPR 对的制备

量子纠缠指的是两个或多个量子系统之间存在非定域、非经典的强关联[13],是量子力学区别于经典物理学的重要特征之一。处在纠缠状态的两个粒子,无论其是否有距离的间隔,任一粒子状态的变化都会改变另一个粒子的状态。也就是说,两个粒子是相互联系的,不论它们相距多远。以极化的双光子纠缠态为例,假设$|0\rangle=\begin{bmatrix}1\\0\end{bmatrix}$和$|1\rangle=\begin{bmatrix}0\\1\end{bmatrix}$分别代表光子的量子态为水平和垂直偏振。如果对处于态$|\Psi^-\rangle_{AB}=\frac{1}{\sqrt{2}}(|01\rangle_{AB}-|10\rangle_{AB})$中的

* **收稿日期**:2013-11-01 **修回日期**:2014-12-08 **网络出版时间**:2015-01-22 11:56
资助项目:国家高新技术研究发展"863"计划资助项目(No. 2012AA040603)
作者简介:曹锟,男,研究方向为教学仪器与虚拟技术,E-mail: caokun77@126.com;**通讯作者**:何国田,教授,E-mail:289870966@qq.com
网络出版地址:http://www.cnki.net/kcms/detail/50.1165.N.20150122.1156.016.html

A光子进行测量,根据量子力学原理[14],每次测量的结果是确定的,也就是说每次的测量结果是$|0\rangle_A$或者是$|1\rangle_A$,并且这两种结果出现的概率是相等的。如果其中一个光子测量的结果是$|0\rangle_A$,则另外一个光子的结果必然为$|1\rangle_B$,反之亦然。

实验上纠缠光子对的产生方法有很多种,例如在腔QED、离子阱、核磁共振(NMR)系统等[15]。相比之下,利用晶体(如BBO)的非线性性质,通过自发参量下转换产生光子纠缠对具有效率高、容易操纵等优点。也是人们最为常用的一种方法。产生光子纠缠对的基本实验装置示意图如图1所示。



1.激光器 2,3,7,8.反射镜 4.凸透镜 5.BBO晶体 6.光学垃圾桶 9,11.半波片 10,12.偏振片 13,14.探测器

图1 纠缠对制备实验装置示意图

在光子的制备过程中,当光子通过BBO晶体后,遵循能量守恒和动量守恒定理。初始光子的能量$E=E1+E2$,在Flash模拟中,笔者用透明度来表示光子的能量。初始光子的动量$p=p1+p2$,遵循平行四边形法则。当光子通过偏振片后,遵循马吕斯定理,即:强度为Io的线偏振光,透过偏振片后,透射光的强度(不考虑吸收)为$I=Io(\cos(a))^2$。其中,a为线偏振光方向与偏振片方向的夹角。设偏振光的起始振幅为Eo,则从偏振片透出的光的振幅为$E=Eo\cos(a)$。核心语法实现如下:

```
mc.onEnterFrame=function(){
var m:Number=random(36); var n:Number=m*10;
  j=n;  setProperty(mc._rotation,n);//光子随机偏转n度数
    if(j>90 and j<270)
{mc._alpha=Math.abs(Math.cos((j/180)*Math.PI)*50);
setProperty(mc._rotation,180)} //角度在90到270之间时,通过偏振片后的能量和偏振方向
  if(j==90 or j==270){mc._alpha=0;} //角度等于90或270时,不会通过偏振片
k=j+90;
  if (j<=270){//设置两个光子始终处于正交状态
   setProperty(mc1._rotation,j+90); }
  if(j>270){setProperty(mc1._rotation,j-270); }
  }
```

2 Two-Step QSDC过程模拟

2.1 算法流程图

在此方案中,首先要对信道进行检测。当信道检测安全时,发送方Alice根据要传送的机密信息进行编码,然后将编码的信息通过量子信道传送给信息接收者Bob。Bob接收编码信息后,结合信道检测的序列进行Bell基联合测量,从而得到机密信息。算法流程图如图2所示。

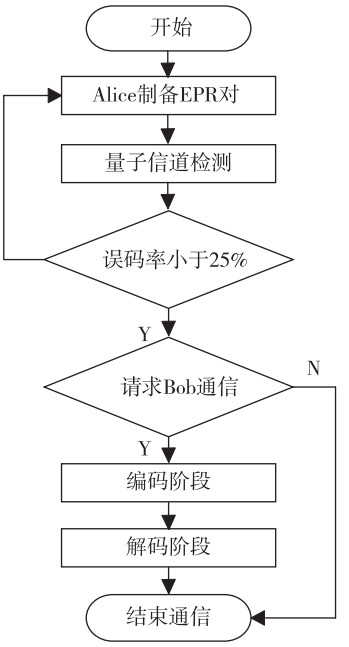


图2 算法流程图

2.2 误码率检测

首先由Alice(发送者)制备N对纠缠光子对,并且要使得纠缠光子对上的每个光子处于相同的量子态,比如说Bell态$|\Phi^+\rangle_{AB}=\frac{1}{\sqrt{2}}(|00\rangle_{AB}+|11\rangle_{AB})$,然后Alice挑出每对光子对中任意一个光子组成信息序列S_A,则剩下的光子自动组成检测序列S_B。

在测试的过程中,Alice自己保留信息序列S_A,将S_B传送给Bob(接收者)。等待S_B传输完成,Bob完全接受到检测序列后,从S_B中任意选择一些光子进行单光子测量[16],随机选用的两种测量基为Z基$\{|0\rangle,|1\rangle\}$或X基$\{|+\rangle,|-\rangle\}$。在对单光子进行测量的过程中,Bob要记录每个光子选用的测量基信息和对其测量所得到的结果。随后,Bob将记录的信息发送给Alice,Alice根据Bob每个光子的测量信息选用同样的测量基进行测量并记录。最后,Alice对比自己和Bob的测量结果,对信道的错误率进行分析:如果误码率比预先设定的安全阈值低很多,则表明在当前信道上传输的光子序列S_B是安全的;否则,该传输信道不安

全，需要重新选择纠缠资源进行测试。

模拟过程中信道误码率检测的核心语法实现：

```
on (release) {
  function rnd(min:Number, max:Number):Number {
    return int(Math.random() * (max−min+1))+min;}
    for (i=1; i<=100; i++) {
      title1.text+=rnd(0, 1)}
} //定义并随机获取 100 位二进制数
function replace(str, find,replace) { //定义替换函数
  var counter =random(10)+10;   //随机获取其中的二进制数
  C=random(30)+30;
  while (counter<C) {
    var start = str.indexOf(find, counter);
  if (start ==−1) { break; }
  else { var before=str.substr(0,start)
    var after=str.substr(start+find.length,str.length)
    str=before+replace+after
    var counter=before.length+replace.length
    i=counter;  A = substring(title1.text, i, 1);
 if (A==1){title3.text+="0";} //如果获取的二进制数为 1,则将其替换为 0 并存储
          title4.text=title3.length; //获取被改变的二进制数的个数
            title4.text+="%";
  if (title3.length<25){ title5.text="信道安全！可以进行下一步通信..."}
  else {title5.text="信道不安全！请结束通信!!!"}}}  return(str);}}
```

2.3 编码阶段

将 S_A 中除去检测使用外剩余的光子序列称为 S'_A，将 S_B 中除去检测使用外剩余的光子序列称为 S'_B。在量子信道的误码率检测为安全的情况下，Alice 将自己要传输的秘密信息与编码规则相对照，根据编码规则依次对序列 S'_A 进行编码（么正操作 U_0，U_1，U_2 或 U_3）。其中，U_0，U_1，U_2 或 U_3 四个么正操作要根据编码规则进行编码（表 1）。

表 1　编码规则

信息	原始量子态	么正操作	编码后量子态
00	$\|\Phi^+\rangle_{AB}$	$U_0=I\otimes\|\Phi^+\rangle_{AB}$	$\|\Phi^+\rangle_{AB}$
01	$\|\Phi^+\rangle_{AB}$	$U_1=\sigma_z\otimes\|\Phi^+\rangle_{AB}$	$\|\Phi^-\rangle_{AB}$
10	$\|\Phi^+\rangle_{AB}$	$U_2=\sigma_x\otimes\|\Phi^+\rangle_{AB}$	$\|\Psi^+\rangle_{AB}$
11	$\|\Phi^+\rangle_{AB}$	$U_3=\sigma_y\otimes\|\Phi^+\rangle_{AB}$	$\|\Psi^-\rangle_{AB}$

编码的核心语法实现：

```
on (release) {
  for (i = 1; i < 50; i = i +2){
  A = substring(title.text, i, 2); //依次提取信息序列的前两位
  if (A == 00)  //判断提取的信息,并按条件进行相应的变换
  {title1.text+= "00—执行 I 变换—|Φ+>\r";   title2.text+= "—|Φ+>—";}
  ……
  if (A == 11)
{ title1.text+= "11—执行 σz 变换—|Φ−>\r";   title2.text+= "—|Φ−> —";}}}
```

2.4 解码阶段

Alice 将编码后的信息序列 S'_A 通过量子信道发送给 Bob。Bob 对两个序列和 S'_B 中对应的纠缠光子对做 Bell 基联合测量[17]，读出 Alice 对光子序列中的每一个光子进行的么正操作信息。之后同编码规则表对照得出 Alice 所需传送的机密信息。解码的核心语法与编码类似。

3 模拟结果与分析

在纠缠光子的制备阶段,光子的起始偏振方向由随机偏转函数来控制。当光子通过非线性晶体(BBO)或偏振片后,其能量和偏振方向的变化遵循马吕斯定理,为了更清楚地观察这一变化,笔者用光子的透明度来表示改变前后的能量值。利用两个偏转函数与按钮控件建立关联,实现光子的纠缠性,即改变纠缠对中一个光子的偏振方向,另一个光子的偏振方向也随之改变,反之亦然。结果如图3所示。

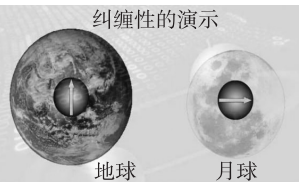


图3 光子的纠缠性

模拟信道误码率检测[18]的过程中,添加随机函数改变Bob测量结果(二进制序列)中的n个数值,从而得出误码率。其中,n的选取要随着Bob测量结果的不同而做出相应的变化。编码和解码的过程在现实实验中是不可观察的,作者利用动画对其进行模拟,便于学习者的理解,其模拟结果如图4和图5所示。

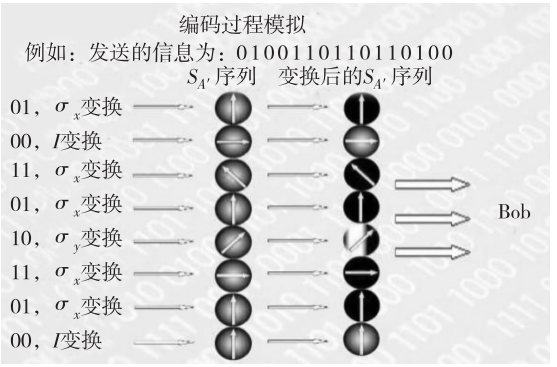


图4 编码的过程

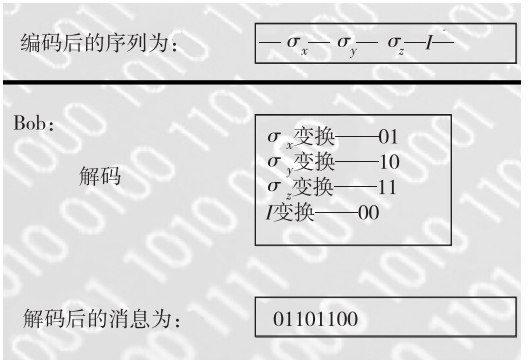


图5 获取信息结果

4 结语

本文介绍了基于EPR对的Two-Step QSDC方案的传输过程,并结合Flash技术,实现了对此方案的模拟。在量子通信的研究和教学中,利用Flash动画精确模拟一些不可观察的过程,加深了学习者的认识和理解,提高了教学的效率,同时也促进了量子通信的进一步发展。从简单的模拟实验到仿真实验再到虚拟现实实验,这个过程的实现还有待科学工作者的不懈努力。

参考文献:

[1] Bennett C H, Brassard D G, Crepeau 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.

[2] 权东晓. 量子通信协议研究[D]. 西安:西安电子科技大学, 2009.
Quan D X. Study on protocols for Quantum communication [D]. Xi'an: Xidian University, 2009.

[3] 任海鹏. 量子安全直接通信协议综述及展望[J]. 通信技术, 2013, 46(4): 31-33.
Ren H P. Review and development of Quantum secure direct communication[J]. Communications Technology, 2013, 46(4): 31-33.

[4] Long G L, Liu X S. Theoretically efficient high-capacity quantum-key-distribution scheme[J]. Phys Rev A, 2002, 65: 032302(1-3).

[5] Deng F G, Long G L. Secure direct communication with a quantum one-time pad[J]. Phys Rev A, 2004, 69: 052319(1-4).

[6] Wang J, Zhang Q, Tang C J. Quantum secure direct communication based on order rearrangement of single photons [J]. Phys Lett A, 2006, 358: 256-258.

[7] 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): 2493-2497.
Quan D X, Pei C X, Liu D, et al. One-way deterministic secure quantum communication protocol based on single photons[J]. China Phys, 2010, 59 (4): 2493-2497.

[8] Bostrom M K, Felbinger T. Deterministic secure direct communication using entanglement[J]. Phys Rev Lett, 2002, 89(18): 187902(1-4).

[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: 042317(1-4).

[10] 邓富国. 量子通信理论研究[D]. 北京:清华大学, 2004.

Deng F G. Study on the theory of Quantum communication[D]. Beijing: Tsinghua University, 2004.

[11] Wang C, Deng F G, Li Y S, et al. Quantum secure direct communication with high-dimension Quantum superdense coding[J]. Phys Rev A, 2005, 71: 044305(1-3).

[12] 陈冬. Flash action script 2.0 互动编程从基础到应用[M]. 北京: 人民邮电出版社, 2006.
Chen D. Flash action script 2.0 interactive programming from foundation to the application[M]. Beijing: Posts & Telecom Press, 2006.

[13] 曾谨言. 量子力学新进展[M]. 北京: 清华大学出版社, 2003.
Zeng J Y. New progress in Quantum mechanics[M]. Beijing: Tsinghua University Press, 2003.

[14] 曹海静. 量子通信的理论研究[D]. 大连: 大连理工大学, 2007.
Cao H J. Theoretical study of Quantum communication [D]. Dalian: Dalian University of Technology, 2007.

[15] 张强. 光子纠缠操纵及其应用[D]. 北京: 中国科学技术大学, 2006.
Zhang Q. Photonic entanglement manipulation and applications[D]. Beijing: University of Science and Technology of China, 2006.

[16] Bennett C H, Brassard G. Quantum cryptography: Public key distribution and coin tossing [C]//Proceedings of IEEE international conference on computers, system and signal processing. Bangalore, India: IEEE, 1984: 1 75-79.

[17] 黄大足. 量子安全通信理论及方案研究[D]. 长沙: 中南大学, 2010.
Huang D Z. Research on theories and schemes of Quantum secure communication[D]. Changsha: Central South University, 2010.

[18] 陈皇卿. 量子密码协议的仿真测试[D]. 北京: 国防科学技术大学, 2006.
Huang Q C. Simulation and test of Quantum cryptography protocol[D]. Beijing: National University, 2006.

Simulation Study of Two-step QSDC Scheme Based on EPR Pair Block

CAO Kun[1], HE Guotian[1,2], LI Xianzhong[1]

(1. Computer and Information Science, Chongqing Normal University, Chongqing 401331;
2. Institute of Green and Intelligent Technology, Chinese Academy of Sciences, Chongqing 401122, China)

Abstract: Quantum secure direct communication protocol is an important agreement on quantum communication after the BB84, EPR and six-state protocol. Since 2000, Quantum secure direct communication got rapid development. Soon afterwards, Deng F G and others was proposed Two-Step QSDC scheme based on EPR pair block using block transmission of ideas. This paper puts forward some algorithms about the preparation of photons, the changes of the photons through a Polarizer and so on, using the AS code to make some unobservable quantum communication progresses visualization, and take Flash technology as the carrier to simulate the Two-Step QSDC scheme based on the EPR Pair Block. On the basis of the visual display communication process, the simulation results proves the feasibility of using computer to simulate the quantum communication as well.

Key words: EPR pair block; quantum communication; QSDC; simulation

(责任编辑 游中胜)