第 25 卷 第 3 期
2005 年 3 月

光 学 学 报
ACTA OPTICA SINICA

Vol. 25, No. 3
March, 2005

文章编号：0253-2239(2005)03-425-4

安全传送明文的量子直传实验方案设计*

王晓鑫[1] 刘 玉[2] 王长强[2]

(1 华中科技大学光电子工程系，武汉 430074
2 华中科技大学电子与信息工程系，武汉 430074)

摘要： 乒乓直传协议是一种新颖的量子直传通信协议。基于量子纠缠特性，乒乓协议允许绝对安全地进行明文直接通信和渐进地进行密钥安全分发，是一种绝对安全的即时通信协议。该量子直传协议将来有望成为安全稳定的光量子通信的主流方式。然而，目前还没有该协议的物理实现方案。分析了乒乓直传协议的工作原理，给出了该协议的流程图，进而分析了协议的物理实现机制，结合纠缠光子源、自由空间单光子路由控制和单光子检测技术，提出了在自由空间中实现乒乓直传协议的实验技术方案，并设计出了乒乓直传协议的实验装置。此实验技术方案为从实验角度进一步研究乒乓协议，以及未来此协议的商业化应用提供了参考。

关键词： 量子光学；量子信息；乒乓通信协议；实验方案

中图分类号：O431 文献标识码：A

Experimental Scheme of Secure Plaintext Transmission with Quantum Direct Communication

Wang Xiaoxin[1] Liu Yu[2] Wang Changqiang[2]

(1 *Department of Optoelectronic Engineering, Huazhong University of Science and Technology, Wuhan* 430074
2 *Department of Electronics and Information Engineering, Huazhong University of Science and Technology, Wuhan* 430074)

Abstract: "Ping-pong" protocol is a novel secure deterministic quantum communication protocol. Based on an entangled pair of qubit, it allows asymptotically secure key distribution and quasi-secure direct communication. Its absolute security has been proved. It is hoped that this kind of quantum deterministic communication will be a main trend of the future quantum optic communication. However, there is no experimental implement of this protocol reported so far. The working scheme of the ping-pong protocol is analyzed and its flow chart is presented. Then the scheme of physical realization of the ping-pong protocol is analyzed. Combining entangled photon resource technique with single photon routing control and single photon detecting technique, an experimental realization in freespace of this protocol and its equipment figure are then proposed. Based on this work, further research of the ping-pong protocol and some practical applications can be taken.

Key words: quantum optics; quantum information; ping-pong communication protocol; experimental scheme

1 引 言

经典密钥体系基于数学上的某些非确定性多项式算法(Non-polynomial，NP)问题(如大素数的因式分解)，其安全性依靠窃听者破解密钥需要的海量运算来保证。然而，对于量子计算而言，经典密钥体系相当脆弱。比如攻击数据加密标准(Data encryption standard，DES)体系，若以每秒 10^6 次搜索的运算速率操作，经典计算需要 1000 年。破解同样长度的密钥，采用 Grover 算法[1]的量子计算机只需要4 min。因此，人们急需找到新的密钥体系。

目前，量子密码通信是科学界公认的唯一能实现绝对安全的通信方式。它的安全性由量子力学中

* 湖北省自然科学基金(2003ABA008)资助课题。

作者简介：王晓鑫(1982～)，男，华中科技大学光电子工程系学生，主要从事量子信息方面的研究工作。E-mail：marswangxx@163.com。

收稿日期：2004-08-10；收到修改稿日期：2004-09-22

的海森堡不确定性原理、量子不可克隆定理以及量子不可分割性来保证，由于任何获取信息的操作都会因破坏量子态而被通信方发现，从而根本上杜绝了信道窃听存在。量子密码技术结合一次一密码技术可以做到无条件安全。

乒乓直传协议[2]是最近提出的一种量子直传通信协议，其特点是允许通信双方进行确定性通信。与其它的量子非确定性通信协议[3~6]相比，其通信具有即时性的特点，可直接传递明文或者密钥；没有协议原理自身造成的量子位丢弃，传输效率高。

2 乒乓协议的工作原理

乒乓直传协议的基本思想可追溯到 Bennett 和 Wiesner 提出的 E91 协议[7]，其基本原理是通过对爱因斯坦-玻多尔斯基-罗森(EPR)[8]纠缠对的局域操作和量子传送来传递保密信息。记光子的水平极化(沿 X 轴)和垂直极化(沿 Y 轴)态分别为 $|0\rangle$ 和 $|1\rangle$，则 Bell 基 $|\psi^{\pm}\rangle=(|01\rangle\pm|10\rangle)/\sqrt{2}$ 是处在 2 维 H 空间 $H=H_1\otimes H_2$ 里的最大纠缠态。单独测量 $|\psi^{\pm}\rangle$ 中任意一个光子的偏振态，得到的将是完全随机的结果，即仅测量一个光子，无法区分开 $|\psi^{+}\rangle$ 和 $|\psi^{-}\rangle$。另一方面，因为 $|\psi^{+}\rangle$ 和 $|\psi^{-}\rangle$ 彼此正交，则对纠缠光子对的联合测量可以区分开这两个态。乒乓协议正是利用这一性质，实现量子直传通信。

乒乓协议的工作流程如图 1 所示。记发送方为 Alice，接收方为 Bob。Bob 制备出纠缠光子对，纠缠态为 $|\psi^{+}\rangle$。Bob 保留其中的一个光子(光子 2)，把另一个光子(光子 1)发送给 Alice。

Alice 收到光子 1 后，以概率 C 转入消息模式(MM)。在消息模式下，Alice 可以对她接收到的光子 1 施加局域操作 $\sigma_z^{(1)}$(对应发送“1”)或者什么都不做(对应发送“0”)。由下式可知，局域操作 $\sigma_z^{(1)}$ 后，纠缠态由 $|\psi^{+}\rangle$ 变为 $|\psi^{-}\rangle$；若无作用，$|\psi^{+}\rangle$ 保持不变：

$$\hat{\sigma}_z\otimes I|\psi^{+}\rangle=\frac{1}{\sqrt{2}}(|0\rangle|1\rangle-|1\rangle|0\rangle)=|\psi^{-}\rangle,$$

操作完毕后，Alice 再把光子 1 发回给 Bob。Bob 对这两个量子位进行贝尔(Bell)基联合测量，区分系统处在 $|\psi^{+}\rangle$ 还是 $|\psi^{-}\rangle$，以提炼出 Alice 发送的是“1”还是“0”。

Alice 收到光子 1 后，另以概率 $1-C$ 转入控制模式(CM)，以侦测有无窃听。在控制模式下，Alice 不对光子 1 作么正变换，而是测量光子 1，并通过公共信道将结果发给 Bob。Bob 收到结果后，也对光子 2 进行测量，并与 Alice 发来的结果进行比较。按照量子力学的测量理论，对复合系统某一子系的测量将使系统塌缩到某一子项上，即 Alice 的测量使 $|\psi^{+}\rangle$ 等概率地塌缩到 $|01\rangle$ 或者 $|10\rangle$ 上，因而 Alice 和 Bob 测得的光子的偏振态必正交。若测得两个光子的偏振态相同(同为 $|0\rangle$ 或同为 $|1\rangle$)则必有 Eve 窃听，终止通信。由安全性证明[2]可知，对于每次攻击，若 Eve 获得的信息量 $I_0\geqslant 0$，则 Eve 被发现的概率 $d(I_0)\geqslant 0$。如果他想获得全部信息($I_0=1$)，被发现的概率为 $d(I_0=1)=1/2$。

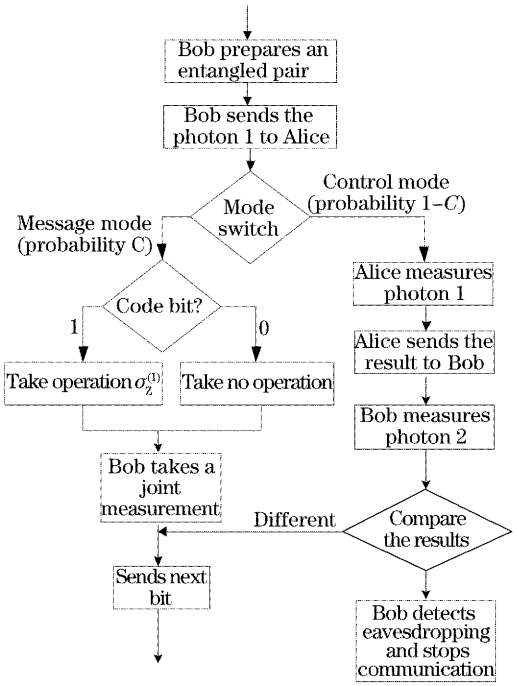

图 1 乒乓编码协议流程图

Fig. 1 Flow chart of ping-pong protocol

3 实验方案设计

根据乒乓协议的工作原理，Bob 制备并测量纠缠态，因此在 Bob 端需要有产生偏振纠缠光子对的纠缠源，以及能分辨开 $|\psi^{+}\rangle$ 和 $|\psi^{-}\rangle$ 的测量装置；在 Alice 端，为实现模式转换和信息处理，需要有对光子 1 进行模式切换和编码变换的装置。根据目前可实现的实验技术，我们设计了乒乓直传协议的实验装置(如图 2 所示)。

在图 2 中，钛宝石锁模激光器(Laser)、紫外半波片(UV-HWP)、索累补偿器(SC)、BG39 蓝色滤波片(BG)和 BBO 晶体组成偏振纠缠光子对生成源；光子 1 与光子 2 在分束器(BS)上发生干涉，BS、

偏振分束器(PBS1、PBS2)和单光子探测器(D3～D6)组成测量装置，联合测量光子的踪迹和偏振态；BS1、反射镜(M1)、压电换能器(PZT1)、BS2 和 BS3、M2、PZT2、BS4 组成两个级联的马赫-曾德尔干涉仪[9]，实现单光子 3 路路由；M3、M4、半波片(HWP1)组成变换装置，实现对的么正变换；合束器[10](BC)保证光子 1 由单路出射；反射棱镜(L)调整 Alice 和 Bob 两路的光程差(Δ)，保证光程差小于光子 1、2 的空间相干长度；控制器则实现噪声抑制、单光子复合计数与通信控制。

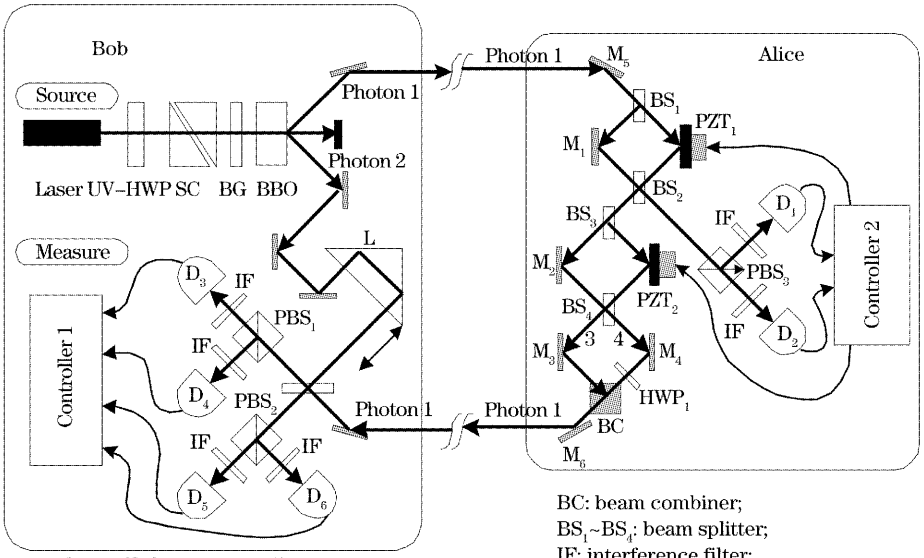

图 2　乒乓协议实验装置设计图

Fig. 2　Schematic of ping-pong protocol experiment

3.1　偏振纠缠光子对生成源

倍频钛蓝宝石锁模激光器的输出光，以得到波长 390 nm，半峰全宽(FWHM)3.5 nm，平均功率 16 mW，脉冲频率 78 MHz 的紫外脉冲抽运激光束。抽运激光依次通过紫外半波片(UV-HWP)、索累补偿器和 BG39 蓝色滤波片，再经过两块晶轴相互垂直的 BBO 晶体，发生Ⅱ型参量下转换非线性光学过程[11]，产生的自发辐射孪生光子对($\lambda=780$ nm，适合于自由空间传输)作为偏振纠缠光子源，光子处于最大纠缠态$|\psi^+\rangle=(|01\rangle+|10\rangle)/\sqrt{2}$。

3.2　消息模式下 Alice 端的操作

光子 1 被发送给 Alice，经过 M5 反射后，进入第一级马赫-曾德尔干涉仪[5]。Alice 通过控制压电换能器(PZT1)的驱动电压，改变马赫-曾德尔干涉仪两路的相位差，实现单光子的路由控制[9]。在消息模式(MM)下，光子 1 受控路由[5]从端口 1 出射，进入后续级联的马赫-曾德尔干涉仪；同样控制 PZT_2，可实现端口 3 与端口 4 间的路由。考虑半波片(HWP1)的变换作用，当半波片的快轴与 X 轴夹角为 0 时，其琼斯矩阵为

$$\boldsymbol{G}=\begin{bmatrix}1 & 0\\ 0 & -1\end{bmatrix}=\sigma_z=|0\rangle\langle 0|-|1\rangle\langle 1|,$$

光子 1 通过半波片(HWP1)，即实现局域操作 $\sigma_z^{(1)}$。若 Alice 传送“1”，则控制光子 1 从端口 4 出射，经 M4 反射后，通过半波片实现 $\sigma_z^{(1)}$ 操作；若欲传送“0”，则 Alice 控制光子 1 从端口 3 出射，不对光子作任何变换。然后，光子 1 经合束器(BC)发送到 Bob 端。

3.3　消息模式下 Bob 端的操作

理论上，通过对两粒子进行控制非门(Control-not)操作，再对单粒子施行哈达玛(Hadamard)操作，人们可以方便地进行贝尔态的测量。然而，到目前为止，还没有已实现的实验技术可用来区分所有的 4 个贝尔态。乒乓协议使用$|\psi^{\pm}\rangle$传递信息，目前，在已实现的实验上仅能利用干涉效应区分出$|\psi^+\rangle$和$|\psi^-\rangle$[12]。这对两光子的光程差提出了严格

要求，必须保证光子 1 和光子 2 的光程差小于两光子的空间相干长度。为了保证相干条件，可通过反射棱镜 L(或反射镜组)调整光子 2 的光程，使光子 2 到分束器(BS)的传输距离等于光子 1 从纠缠源经 Alice 再返回到分束器(BS)的传输距离。为解决光子 2 在 Bob 端的存储问题，可以让其通过两倍于 Alice 和 Bob 之间距离的光纤。待光子存储技术成熟后，即可采用光子存储技术代替现有方案中的长距离光纤。

光子 1 和 2 在分束器(BS)上发生干涉。因为光子是玻色子，服从玻色统计。这样，当两个全同光子在分束器上重叠干涉后，出射的末态整体波函数必须是交换对称的。如果光子 1 和 2 极化波函数处于反对称态 $|\psi^-\rangle$，则其空间波函数就必须也是反对称的。从而光子 1 和 2 将总是出现在分束器(BS)不同的输出端口上。如果光子处在对称极化态 $|\psi^+\rangle$，则相应的空间波函数也是交换对称的，也即光子 1 和 2 将总是同时出现在分束器的某一输出端口上。因此若探测器两路同时检测到光子，则知道光子处在反对称态 $|\psi^-\rangle$ 上，得到 Alice 发送的是“1”；若仅单路检测到光子，则处在 $|\psi^+\rangle$ 上，得到“0”。

3.4 控制模式

控制模式中，Alice 通过调节 PZT1 来调整马赫-曾德尔干涉仪两臂的相位差，使光子由端口 2 出射，通过偏振分束器(PBS_3)和单光子探测器(D1、D2)测量出光子 1 的偏振态，并将结果发送给 Bob。在 Bob 端，光子 2 在分束器(BS)处不再与光子 1 发生干涉，而是等概率地走上路或者下路，但是无论走哪一路，Bob 都可通过偏振分束器(PBS_1、PBS_2)和单光子探测器(D3～D6)测出其偏振态。Bob 将自己的测量结果和 Alice 发送的进行比较，即可根据偏振态是否正交，判断出有无窃听。

4 结 论

我们根据乒乓协议的工作原理，分析目前可行的实验机制，得到该协议在技术上可实现的实验方案：用级联的马赫-曾德尔干涉仪实现控制选择逻辑、用半波片实现编码变换、用双光子干涉效应实现逻辑检测，从而绘出了乒乓协议的实验装置，以期实现在自由空间中绝对安全地传送明文。上述方案中叙述的各项单元技术均可利用已有实验装置，实现简单。但是，现有的干涉测量方法，对光程差有严格要求，限制了协议在实际中的应用，因此迫切需要找到新的 Bell 基测量方法，打破原有的限制，以适应未来灵活多变的商业应用，笔者正对此问题进行进一步的研究。

参 考 文 献

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

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

3 C. H. Bennett, G. Brassard. Quantum cryptography: public key distribution and coin tossing[C]. *Proc. IEEE Int. Conf. on Computers, Systems and Signal Processing*, Bangalore, India (IEEE, New York, 1984). 175～179

4 A. K. Ekert. Quantum cryptography based on Bell's theorem[J]. *Phys. Rev. Lett.*, 1991, **67**(6): 661～663

5 C. H. Bennett, G. Brassard, N. D. Mermin. Quantum cryptography without Bell's theorem[J]. *Phys. Rev. Lett.*, 1992, **68**(5): 557～559

6 D. Brub. Optimal eavesdropping in quantum cryptography with six states[J]. *Phys. Rev. Lett.*, 1998, **81**(14): 3018～3021

7 C. H. Bennett, S. J. Wiesner. Communication via one- and two-particle operators on Einstein-Podolsky-Rosen states[J]. *Phys. Rev. Lett.*, 1992, **69**(20): 2881～2884

8 A. Einstein, B. Podolsky, N. Rosen. Can quantum-mechanical description of physical reality be considered complete? [J]. *Phys. Rev.*, 1935, **47**: 777～780

9 Xiong Li, Qin Xiaolin, Feng Mingming. Single-photon control with Mach-Zehner interferometer[J]. *Acta Optica Sinica*, 2004, **24**(3): 294～298 (in Chinese)
熊 利，秦小林，冯明明等. 基于马赫-曾德尔干涉仪的单个光子操控[J]. 光学学报，2004，**24**(3)：294～298

10 D. Haubrich, M. Dornseifer, R. Wynand. Lossless beam combiners for nearly equal laser frequencies[J]. *Rev. Sci. Instrum.*, 2000, **71**(2): 338～340

11 Y. H. Shih, C. O. Alley. New type of Einstein-Podolsky-Rosen-Bohm experiment using Pairs of light quanta produced by optical parametric down conversion[J]. *Phys. Rev. Lett.*, 1988, **61**(26): 2921～2924

12 K. Mattle, H. Weinfurter, P. G. Kwiat *et al.*. Dense coding in experimental quantum communication[J]. *Phys. Rev. Lett.*, 1996, **76**(25): 4656～4659