第 57 卷 第 5 期 2008 年 5 月
1000-3290/2008/57(05)/3016-06

物 理 学 报
ACTA PHYSICA SINICA

Vol.57, No.5, May, 2008

基于光子轨道角动量的密码通信方案研究*

苏志锟 王发强† 路轶群 金锐博 梁瑞生 刘颂豪

(华南师范大学信息光电子科技学院,光子信息技术广东省高校重点实验室,广州 510006)

(2007 年 6 月 18 日收到;2007 年 8 月 21 日收到修改稿)

设计了一个基于两个正交的光子轨道角动量态的量子密码通信方案.在该方案中,Alice 使用具有独特设计的激光器,随机发送有确定轨道角动量的光子;Bob 采用由两个达夫棱镜组成的光束旋转器,对光子的轨道角动量态进行测量.对系统安全性的讨论表明,Eve 采用截获重发、攻击单臂等攻击手段,其窃听行为都会被发现.理论证明,该方案不需要通信双方实时监测和调整参考系,同时避免了 BB84,B92 协议因发送基和测量基不一致而丢弃一半信息的问题,从而提高了密钥生成效率.

关键词:量子保密通信,轨道角动量

PACC:4281,4280F

1. 引 言

1992 年,Allen 及其同事从理论上证明:当光束的振幅函数含有方位角相位项 $\exp(\mathrm{i}l\phi)$ 时,光束中的每个光子,在传播方向上具有确定轨道角动量 $l\hbar$[1].1995 年,He 等采用计算全息的方法产生了 $l=3$ 的光束,利用此光束实现了对微米量级 CuO 粒子的囚禁,实验表明轨道角动量的大小与 l 成正比,但这种光束携带了多少轨道角动量的问题仍未解决[2].随后,Simpson 及其同事于 1997 年巧妙地测量了含有 $\exp(\mathrm{i}\phi)$ 相位项的圆偏振光具有 $\hbar$ 的轨道角动量和 $\hbar$ 的自旋角动量[3].之后,光子轨道角动量越来越引起人们的关注[4,5].

光子轨道角动量态可作为量子密码通信的信息载体[6].量子密码通信是近年发展起来的一种绝对安全的密钥分配技术.目前,量子密码通信系统多采用 BB84 和 B92 这两种协议,而这两种协议在对比发送基和测量基的时候,不可避免地遇到丢掉一半信息的问题,因而降低了密钥生成效率.本文在 Lior 等人提出的正交态编码协议[7]的基础上,设计了一个利用两正交的轨道角动量态传递信息的量子密码通信方案,该方案具有如下两个明显的优点:第一,不需要通信双方实时监测、调整参考系;第二,避免了非正交态系统因发送基和测量基不一致而丢弃一半信息的问题,从而提高了密钥生成效率.

2. 轨道角动量密码通信方案

2.1. 光束旋转器对拉盖尔-高斯光束的作用

Jonathan 等人把两个达夫棱镜组合成一个光束旋转器[8],如图 1(a)所示,达夫棱镜 DP_1,DP_2 分别位于干涉仪的两臂,当这两个棱镜的相对角度为 $\alpha/2$ 时,达夫棱镜 DP_1,DP_2 的作用等效于在其中一臂加入旋转角为 α 的光束旋转器 BR,从而使含有相位项 $\exp(\mathrm{i}l\phi)$ 的拉盖尔-高斯光束在干涉仪两臂产生 $\delta=l\alpha$ 的相位差[9],见图 1(b).利用 Allen 等人提出的光束轨道角动量传输矩阵[10],下面分析本密码通信方案中所用到的光束旋转器对一阶、二阶拉盖尔-高斯光束的作用,根据文献[10],一阶、二阶光束旋转器的作用可用矩阵形式表达为

* 国家重点基础研究发展计划(973)项目(批准号:2007CB307001)资助的课题.

† 通讯联系人. E-mail:tq_wang@163.com

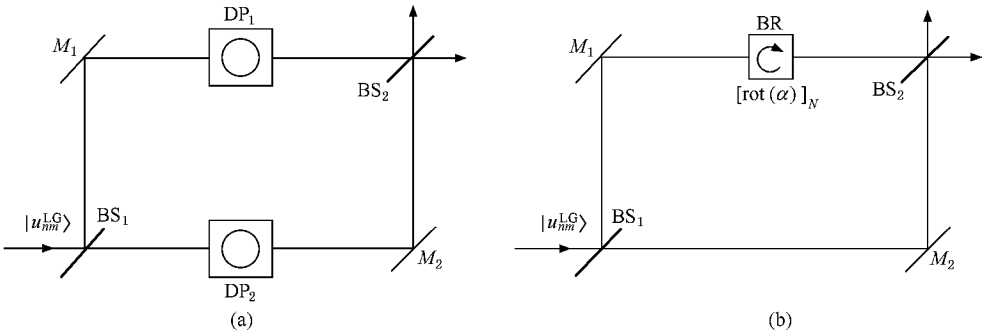

图 1　在干涉仪中光束旋转器的(a)结构示意图和(b)等效图

$$[\mathrm{rot}(\alpha)]_{N=1}=\begin{bmatrix}\cos\alpha & \sin\alpha\\ -\sin\alpha & \cos\alpha\end{bmatrix}, \tag{1}$$

$$[\mathrm{rot}(\alpha)]_{N=2}=\begin{bmatrix}\cos^2\alpha & \dfrac{\sin 2\alpha}{\sqrt{2}} & \sin^2\alpha\\ \dfrac{-\sin 2\alpha}{\sqrt{2}} & \cos 2\alpha & \dfrac{\sin 2\alpha}{\sqrt{2}}\\ \sin^2\alpha & \dfrac{-\sin 2\alpha}{\sqrt{2}} & \cos^2\alpha\end{bmatrix}, \tag{2}$$

其中，$N=n+m=2p+|l|$ 为厄米-高斯模式或拉盖尔高斯模式的阶，m，n 是表征厄米-高斯光束 $u_{nm}^{\mathrm{HG}}(x,y,z)$ 的任意整数，$l=|n-m|$，$p=\min(m,n)$ 是表征拉盖尔-高斯光束 $u_{nm}^{\mathrm{LG}}(x,y,z)$ 的整数. N 阶拉盖尔-高斯光束模式可以分解为 $(N+1)$ 个厄米-高斯光束模式的和[11]：

$$u_{nm}^{\mathrm{LG}}(x,y,z)=\sum_{k=0}^{N}a(n,m,k)\,u_{N-k,k}^{\mathrm{HG}}(x,y,z). \tag{3}$$

用矢量形式表示为

$$|u_{nm}^{\mathrm{LG}}\rangle=\begin{bmatrix}a(n,m,0)\\ a(n,m,1)\\ \\ a(n,m,N-1)\\ a(n,m,N)\end{bmatrix}, \tag{4}$$

其中，

$$a(n,m,k)=\mathrm{i}^k\left(\frac{(N-k)!k!}{2^N n!m!}\right)^{1/2}\times\frac{1}{k!}\frac{d^k}{dt^k}[(1-t)^n(1+t)^m]_{t=0}.$$

在该方案中用于编码的两个正交轨道角动量态分别对应 $l=1,p=0$ 和 $l=2,p=0$ 的拉盖尔-高斯光束，它们的列向量形式可分别写为

$$|u_{l=1,p=0}^{\mathrm{LG}}\rangle=|u_{n=1,m=0}^{\mathrm{LG}}\rangle=\begin{bmatrix}\dfrac{1}{\sqrt{2}}\\ \dfrac{-\mathrm{i}}{\sqrt{2}}\end{bmatrix}, \tag{5}$$

$$|u_{l=2,p=0}^{\mathrm{LG}}\rangle=|u_{n=2,m=0}^{\mathrm{LG}}\rangle=\begin{bmatrix}\dfrac{1}{2}\\ \dfrac{-\mathrm{i}}{\sqrt{2}}\\ \dfrac{-1}{2}\end{bmatrix}. \tag{6}$$

经旋转角为 α 的光束旋转器作用后，(5)，(6)式表示的态将变为

$$\begin{aligned}|u'^{\mathrm{LG}}_{l=1,p=0}\rangle&=[\mathrm{rot}(\alpha)]_{N=1}|u_{l=1,p=0}^{\mathrm{LG}}\rangle\\&=\mathrm{e}^{-\mathrm{i}\alpha}|u_{l=1,p=0}^{\mathrm{LG}}\rangle,\end{aligned} \tag{7}$$

$$\begin{aligned}|u'^{\mathrm{LG}}_{l=2,p=0}\rangle&=[\mathrm{rot}(\alpha)]_{N=2}|u_{l=2,p=0}^{\mathrm{LG}}\rangle\\&=\mathrm{e}^{-2\mathrm{i}\alpha}|u_{l=2,p=0}^{\mathrm{LG}}\rangle.\end{aligned} \tag{8}$$

由此可见，当干涉仪的入射光子态为 $|u_{l=1,p=0}^{\mathrm{LG}}\rangle$ 时，干涉仪两臂将产生 $\delta=\alpha$ 的相位差；当干涉仪的入射光子态为 $|u_{l=2,p=0}^{\mathrm{LG}}\rangle$ 时，干涉仪两臂将产生 $\delta=2\alpha$ 相位差.

2.2. 量子密钥分配方案

图 2 是基于轨道角动量的量子保密通信系统的结构示意图，它的原型是一个马赫-曾德干涉仪. 分束器 BS_1，BS_2 的分束比都是 50∶50，脉冲激光器 LD_1，LD_2 能分别直接输出轨道角动量为 $\hbar$，$2\hbar$ 的光子[12]，激光脉冲经过光混合器 LM 混合、衰减器 A 衰减后进入量子通道. 由达夫棱镜 DP_1，DP_2 组成的光束旋转器的旋转角 $\alpha=\pi$. 延时器 Delay_1，Delay_2 分别位于干涉仪的两臂，其作用是防止窃听者 Eve 同时截获干涉仪两臂的小脉冲，这是正交编码方案的最核心内容[7]. t_s，t_r 分别是 Alice 发送光子和 Bob 接收到光子的瞬时时刻，τ 是延时器延时的时间，t_1 是光子在量子通道中传输的时间，使 $\tau>t_1$.

在图 2 Alice 控制的区域中，Alice 随机发送轨道角动量为 $\hbar$ 或 $2\hbar$ 的光子. 输入态 $|\mathrm{in}\rangle_{\mathrm{BS}_1}=|0\rangle|1\rangle$

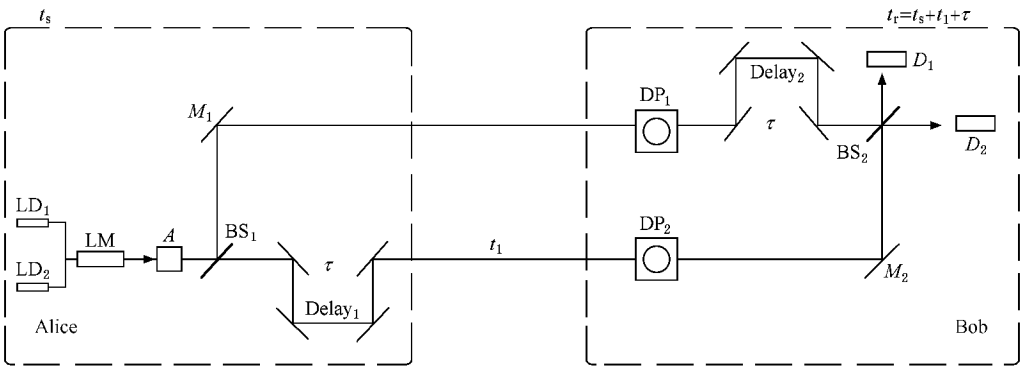

图 2 轨道角动量保密通信系统的组成

经分束器 BS_1 作用后,输出态

$$|\mathrm{out}\rangle_{BS_1}=\frac{1}{\sqrt{2}}(|0\rangle|1\rangle+\mathrm{i}|1\rangle|0\rangle), \tag{9}$$

(9)式表明光子从分束器透射端和反射端输出的概率都是 50%,但从反射端输出时附加了$\frac{\pi}{2}$的相位跃变,其中,$|0\rangle$,$|1\rangle$分别表示真空态和单光子态,以下相同.光子离开量子通道,进入 Bob 控制的区域,经过达夫棱镜 DP_1,DP_2 作用后,两臂产生了 $\delta=\pi$ 或 2π 的相位差,则分束器 BS_2 的输入态

$$|in\rangle_{BS_2}=\frac{1}{\sqrt{2}}(|0\rangle|1\rangle+\mathrm{i}\mathrm{e}^{\mathrm{i}\delta}|1\rangle|0\rangle). \tag{10}$$

分束器 BS_2 有转换形式

$$|0\rangle|1\rangle\xrightarrow{BS_2}\frac{1}{\sqrt{2}}(|0\rangle|1\rangle+\mathrm{i}|1\rangle|0\rangle),$$

和

$$|1\rangle|0\rangle\xrightarrow{BS_2}\frac{1}{\sqrt{2}}(|1\rangle|0\rangle+\mathrm{i}|0\rangle|1\rangle),$$

其中直积态的第一、二个态分别表示光子向着探测器 D_1,D_2 传播的态.那么,$|in\rangle_{BS_2}$ 经过分束器 BS_2 后变为

$$|\mathrm{out}\rangle_{BS_2}=\frac{1}{2}(1-\mathrm{e}^{\mathrm{i}\delta})|0\rangle|1\rangle+\frac{\mathrm{i}}{2}(1+\mathrm{e}^{\mathrm{i}\delta})|1\rangle|0\rangle). \tag{11}$$

对(11)式作如下讨论:第一,当 $\delta=\pi$,即 $l=1$ 时,有

$$\frac{1}{2}(1-\mathrm{e}^{\mathrm{i}\delta})|0\rangle|1\rangle+\frac{\mathrm{i}}{2}(1+\mathrm{e}^{\mathrm{i}\delta})|1\rangle|0\rangle\xrightarrow{BS_2}|0\rangle|1\rangle,$$

这表明当入射光子的轨道角动量为 $\hbar$ 时,探测器 D_1 没有响应,探测器 D_2 有响应;第二,当 $\delta=2\pi$,即 $l=2$ 时,有

$$\frac{1}{2}(\mathrm{e}^{\mathrm{i}\delta}+1)|1\rangle|0\rangle+\frac{\mathrm{i}}{2}(\mathrm{e}^{\mathrm{i}\delta}-1)|0\rangle|1\rangle\xrightarrow{BS_2}\mathrm{i}|1\rangle|0\rangle,$$

这表明当入射光子的轨道角动量为 $2\hbar$ 时,探测器 D_1 有响应,探测器 D_2 无响应.

根据以上分析,可以设计如下的量子密钥分配方案:首先,根据轨道角动量为 $\hbar$,$2\hbar$ 的光子态分别代表二进制的‘0’和‘1’的规则,Alice 随机地发送这两种光子态,并记录发送光子的瞬时时刻 t_s;然后,Bob 记录下探测器响应的时刻 t_r 和哪个探测器有响应;最后,Alice 和 Bob 公开一部分二进制位用于对比瞬时时刻和位值.

2.3. 系统安全性的分析

Eve 将 Alice 随机发送的、轨道角动量为 $\hbar$ 或 $2\hbar$ 的光子全部截获,并用与 Bob 一样的装置对所截获的光子进行测量,根据对(11)式的讨论知,Eve 能正确测出 Alice 所发送光子的量子态,接着,Eve 根据测量结果用与 Alice 一样的装置给 Bob 重发一个相同量子态的光子.然而,Bob 接收到光子的瞬时时刻 t_r 将从 $t_{r1}=t_s+t_1+\tau$ 变为 $t_{r2}=t_s+\tau+\tau$(忽略了 t_1),由 $\tau>t_1$,知 $t_{r1}\neq t_{r1}$,即 Bob 不能在预定的瞬时时刻接收到光子,Eve 的窃听行为会被发现.因此,Eve 可以在还没测出结果前,先给 Alice 发送一个光子,测量出结果后,再用相位调制器 PM 补偿相位 Φ,如图 3 所示.设 Eve 先给 Bob 发送轨道角动量为 $\hbar$ 的光子,则输入态 $|in'\rangle_{BS_4}=|0\rangle|1\rangle$经分束器 BS_4、调制器 PM 和达夫棱镜 DP_1,DP_2 的作用后,得到分束器 BS_2 的输入态

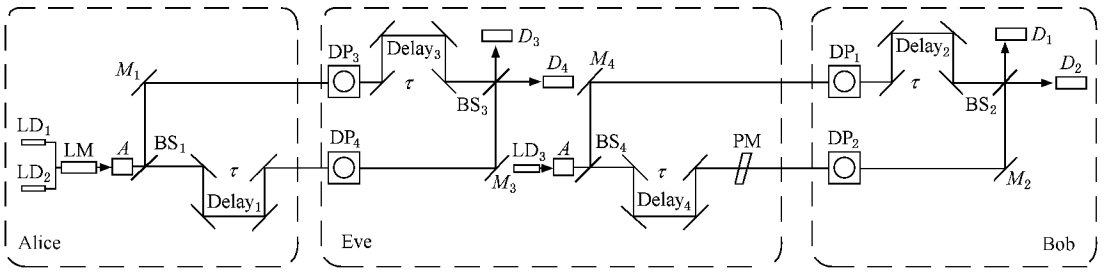

图 3　Eve 采用截获重发的方法对轨道角动量保密通信系统进行窃听

$$|\mathrm{i}n'\rangle_{\mathrm{BS}_2} = \frac{1}{\sqrt{2}}(|0\rangle|1\rangle + \mathrm{i}\mathrm{e}^{\mathrm{i}(\pi+\Phi)}|1\rangle|0\rangle). \quad (12)$$

与(11)式同理，可得分束器 BS_2 的输出态

$$|\mathrm{out}'\rangle_{\mathrm{BS}_2} = \frac{1}{2}(1 - \mathrm{e}^{\mathrm{i}(\pi+\Phi)})|0\rangle|1\rangle + \frac{\mathrm{i}}{2}(1 + \mathrm{e}^{\mathrm{i}(\pi+\Phi)})|1\rangle|0\rangle. \quad (13)$$

由(13)式，得探测器 D_2 有响应的概率是

$$P_2 = \frac{1}{2}[1 - \cos(\pi + \Phi)]. \quad (14)$$

由(14)式知，若 Eve 经测量得 Alice 发送的光子的轨道角动量是 $\hbar$，则通过让 $\Phi = 0$，就可以使探测器 D_1 没有响应，探测器 D_2 有响应，即 Eve 的窃听行为不被发现；若 Eve 经测量得 Alice 发送的光子的轨道角动量是 $2\hbar$，则通过让 $\Phi = \pi$，就可以使探测器 D_1 有响应，D_2 没有响应，即 Eve 的窃听行为不被发现．然而，在本文提出的方案中 Alice 发送光子的瞬时时刻是随机的，即 Eve 不能预先知道应该什么时刻先发送光子给 Bob．

除了截获重发的方法外，Eve 还可以采用攻击单臂的方法，见图 4，Eve 用与 Bob 相似(去掉了延时器)的测量装置只测量干涉仪中没经过延时的路径 I 的光子态，测量后再用与 Alice 一样的装置给 Bob 发送光子．光子选择路径 I 和 II 各有 50% 的概率，光子选择路径 I 时，Eve 的测量装置有响应，有响应时测量结果是正确的，Eve 的窃听行为不引入错误；当光子选择路径 II 时，Eve 对 Alice 发送光子的瞬时时刻是无知的，Eve 的窃听行为引入错误．可见，Eve 采用攻击单臂的方法进行窃听将引入误码率 $D = 0.5$，Alice，Bob 和 Eve 两两之间的互信息分别为 $I(A,B) = 0.5$，$I(A,E) = 0.5$，$I(E,B) = 1$，Eve 的窃听行为会被发现．

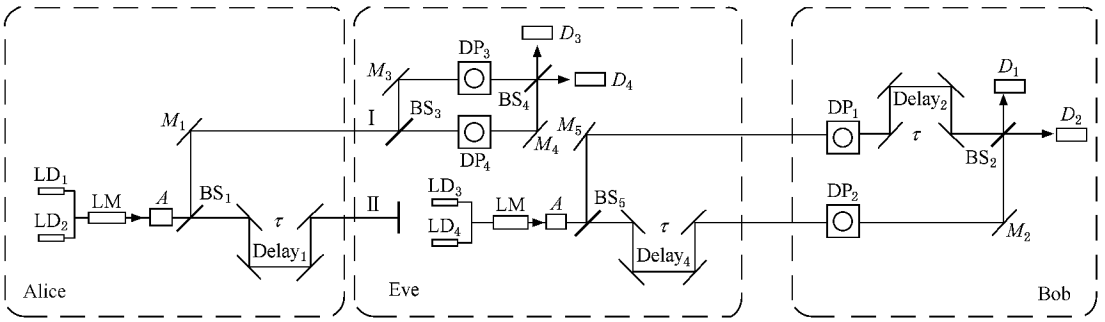

图 4　Eve 采用攻击单臂的方法对轨道角动量保密通信系统进行窃听

3. 轨道角动量保密通信系统的优点

3.1. 不需要调整参考系

轨道角动量态能用含有相位因子 $\exp(\mathrm{i}l\phi)$ 的波函数表示，在柱坐标系中，设光波沿 z 轴传播，则函数表达式可表示为

$$u_{lp}^{\mathrm{LG}}(r,z,\varphi) = \frac{A(r,z)}{\sqrt{2\pi}}\exp(\mathrm{i}l\phi). \quad (15)$$

沿 z 轴方向的轨道角动量算符在柱坐标系下可表示为

$$\hat{L}_z = -\mathrm{i}\frac{\partial}{\partial\phi}. \quad (16)$$

当 Bob 的测量系绕传播轴旋转了 θ，如图 5 所示.轨道角动量态 $|u_{lp}^{LG}\rangle$ 进入 Bob 控制的区域后，光子态保持不变，因为

$$e^{i\theta\hat{L}_z}|u_{lp}^{LG}\rangle = \left[1 + i\theta\hat{L}_z + \frac{(i\theta)^2(\hat{L}_z)^2}{2!} + \cdots + \frac{(i\theta)^n(\hat{L}_z)^n}{n!}\right]|u_{lp}^{LG}\rangle = e^{il\theta}|u_{lp}^{LG}\rangle, \quad (17)$$

由(17)式可知，当 Bob 的测量系绕传播轴旋转 θ 后，光子态 $|u_{lp}^{LG}\rangle$ 发生的变化仅仅是多了一个常数项因子 $e^{il\theta}$，而 $|u_{lp}^{LG}\rangle$ 和 $e^{il\theta}|u_{lp}^{LG}\rangle$ 所描述的光子态是完全相同的，所以，在轨道角动量保密通信系统中，通信双方在传播轴上不需要实时监测、调整参考系.

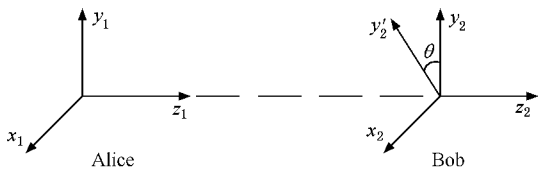

图 5 Alice 和 Bob 的测量系

3.2. 不用丢弃一半信息

由对(11)式的讨论，可知：当 Alice 发送轨道角动量为 $\hbar$ 的光子时，探测器 D_1 没有响应，探测器 D_2 有响应；当 Alice 发送轨道角动量为 $2\hbar$ 的光子时，探测器 D_1 有响应，探测器 D_2 没有响应，Bob 通过记录探测器的响应情况，就可以知道 Alice 所发送光子的态，避免了非正交态方案对比测量基时，因发送基和测量基不一致而丢弃一半信息的问题，有效地提高了密钥生成效率.

4. 结 论

在正交态编码协议的基础上，设计了一个利用光子轨道角动量态进行保密通信的实验方案.该实验方案，Alice 使用的激光器能直接产生具有确定轨道角动量的光子；Bob 采用光束旋转器对光子轨道角动量态进行测量.对系统安全性的讨论表明，Eve 采取截获重发、攻击单臂等攻击手段，都会给系统引入不小于 50% 的误码率，其窃听行为会被发现.理论分析显示，该方案在光子传播方向上不需要调整参考系，解决了偏振编码需要实时调整参考系的困难；同时，该方案利用两个正交的轨道角动量态传递信息，避免了利用非正交态传递信息时，因发送基和测量基不一致而丢弃一半信息的问题，从而提高了密钥生成效率.

[1] Allen L, Beijersbergen M W, Spreeuw R J C, Woerdman J P 1992 *Phys. Rev.* A **45** 8185

[2] He H, Friese M E J, Heckenberg N R, Rubinsztein-Dunlop H 1995 *Phys. Rev.* L **75** 826

[3] Simpson N B, Dholakia K, Allen L, Padgett M J 1997 *Opt. Lett.* **22** 52

[4] Ye F W, Li Y P 2003 *Acta Phys. Sin.* **52** 328 (in Chinese) [叶芳伟、李永平 2003 物理学报 **52** 328]

[5] Wu J Z, Li Y J 2007 *Chin. Phys.* **16** 1334

[6] Spedalieri F M 2006 *Opt. Comm.* **260** 340

[7] Lior G, Lev V 1995 *Phys. Rev.* L **75** 1239

[8] Jonathan L, Miles J P, Stephen M B, Sonja F A, Johannes C 2002 *Phys. Rev.* L **88** 257901

[9] Wei H Q, Xue X, Jonathan L, Miles J P, Stephen M B, Sonja F A, Eric Y, Johannes C 2003 *Opt. Comm.* **223** 117

[10] Allen L, Johannes C, Padgett M J 1999 *Phys. Rev.* E **60** 7497

[11] Beijersbergen M W, Allen L, Veen H E L O V D, Woerdman J P 1993 *Opt. Comm.* **96** 123

[12] Oron R, Davidson N, Friesem A A, Hasman E 2000 *Opt. Comm.* **182** 205

Study on quantum cryptography using orbital angular momentum states of photons *

Su Zhi-Kun Wang Fa-Qiang† Lu Yi-Qun Jin Rui-Bo Liang Rui-Sheng Liu Song-Hao

(*Laboratory of Photonic Information Technology, School for Information and Optoelectronic Science and Engineering, South China Normal University, Guangzhou* 510006, *China*)

(Received 18 June 2007; revised manuscript received 21 August 2007)

Abstract

We present a simple quantum cryptographic scheme that encodes information in two orthogonal orbital angular momentum states. The states used in this scheme are invariant under rotations of the propagation direction, making this implementation independent of the alignment between the reference frames of Alice and Bob. Besides, since the two orbital angular momentum states are orthogonal, 100% use of the photons is attained, which increases the key generation rate of the protocol.

Keywords: quantum crytography, orbital angular momentum

PACC: 4281, 4280F

* Project supported by the State Key Development Program for Basic Research of China (Grant No. 2007CB307001).

† Corresponding author. E-mail: fq_wang@163.com