

# 基于半波片的偏振跟踪理论分析

马 晶<sup>1)</sup> 张光宇<sup>1)2)</sup> 戎亦文<sup>1)</sup> 谭立英<sup>1)</sup>

1) 哈尔滨工业大学可调谐激光技术国家级重点实验室 哈尔滨 150001)

2) 哈尔滨理工大学应用科学学院 哈尔滨 150080)

(2005 年 3 月 18 日收到 2005 年 6 月 8 日收到修改稿)

分析了卫星量子密钥分配中采用半波片进行偏振跟踪的原理,通过旋转半波片实现对偏振“零”方向的跟踪.针对 BB84 协议和 B92 协议,给出了三组共轭基六个光子偏振态的变换关系式,分析了基于偏振跟踪的量子密钥编码原理.

关键词:量子密钥分配,偏振跟踪,半波片

PACC:0365,0760

## 1. 引 言

自从 Bennett 等人<sup>[1]</sup>完成第一个量子密钥分配演示性实验以来,基于自由空间量子信道的量子密钥分配实验取得了很大进展.目前,国外研究主要集中在地面点对点大气光路的量子密钥分配实验和卫星量子密钥分配的可行性分析<sup>[2-6]</sup>,国内研究主要集中在实验室内的量子密钥分配实验<sup>[7-9]</sup>.量子密钥分配具有绝对安全性,这由量子力学的不确定原理和量子不可克隆原理来保证.在已经进行的地面点对点大气光路实验中,量子密钥分配协议采用 BB84 协议和 B92 协议<sup>[10,11]</sup>,以光子偏振态作为量子信息态.为实现全球任意两点间保密通信,需要通过卫星进行量子密钥分配.偏振跟踪技术是卫星量子密钥分配的关键技术之一.在卫星量子密钥分配中,由于采用偏振编码,对发射信号的方向性要求很高,通信双方需要具有跟踪偏振方向改变的能力.而在太空中,卫星的姿态控制不可能与地面完全相对静止,所以需要定期对偏振基准进行及时地修正,否则会造成密钥分配的困难. Nordholt 等人<sup>[12]</sup>提出采用半波片进行偏振跟踪,但并没有给出相关理论分析.

本文首先分析了卫星量子密钥分配中采用半波片进行偏振跟踪的原理,然后给出了 BB84 协议和 B92 协议中光子偏振态的变换关系,最后对基于偏振跟踪的量子密钥编码原理进行了分析.

## 2. 偏振跟踪原理

在卫星量子密钥分配中,由于发射机或接收机运动而产生光子偏振方向的改变.为完成量子密钥分配协议,需要通信双方具有跟踪偏振方向改变的能力.偏振方向的改变相当于对光子偏振态进行了某种操作,这种操作可以用算符来表示.一般地,偏振跟踪可以表示为

$$F_1 F_2 |\psi\rangle = |\psi\rangle, \quad (1)$$

式中,  $|\psi\rangle$  为光子偏振态,  $F_1$  和  $F_2$  是两个算符.其中,  $F_2$  表示光子偏振态的改变,  $F_1$  表示对光子偏振态进行补偿,实现偏振跟踪.

对于卫星量子密钥分配,偏振跟踪可以通过半波片来实现.以负单轴晶体为例,半波片工作原理如图 1 所示.假设线偏振光垂直入射到晶面上,且光轴的方向平行于晶片表面.由于双折射效应,入射线偏振光将分解为相互垂直的 o 光和 e 光,其折射率分别为  $n_o$  和  $n_e$ .由于二光的折射率不同,它们通过厚度为  $d$  的晶片后,将产生一定的相位差  $\delta$ ,且

$$\delta = \frac{2\pi}{\lambda} |n_o - n_e| d, \quad (2)$$

式中,  $\lambda$  为光在真空中的波长.半波片使 o 光和 e 光产生的相位差为

$$\delta = (2m + 1)\pi, \quad (3)$$

式中,  $m$  为整数.设入射线偏振光的振动面和光轴成角度  $\alpha$ ,在透过半波片之后,线偏振光的振动面转过  $2\alpha$ .若右旋圆偏振光入射,则透过半波片之后变

为左旋圆偏振光,左旋圆偏振光入射则变为右旋圆偏振光.

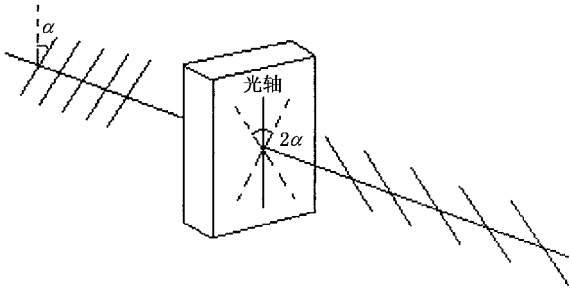


图1 半波片工作原理

在实现量子密钥分配过程中,通信双方需要确定共同的偏振基准即偏振“零”方向,这由通信双方发射偏振信标光进行定义.在偏振跟踪中,通过旋转半波片进行校正,使得偏振“零”方向得到补偿.记“零”方向偏振态为 $|0\rangle$ ,其琼斯矢量为

$$|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}. \quad (4)$$

假设偏振“零”方向改变角度 $\theta$ ,用算符 $D$ 表示,其琼斯矩阵为

$$D = \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}, \quad (5)$$

则

$$D|0\rangle = |\theta\rangle, \quad (6)$$

即为 $\theta$ 方向偏振态,其琼斯矢量为

$$|\theta\rangle = \begin{pmatrix} \cos\theta \\ \sin\theta \end{pmatrix}. \quad (7)$$

采用半波片进行偏振跟踪,假设半波片光轴与偏振“零”方向夹角为 $\theta/2$ ,半波片操作算符 $H_{\lambda/2}$ 表示,其琼斯矩阵为

$$H_{\lambda/2} = \begin{pmatrix} \cos\theta & \sin\theta \\ \sin\theta & -\cos\theta \end{pmatrix}, \quad (8)$$

则

$$H_{\lambda/2}D|0\rangle = H_{\lambda/2}|\theta\rangle = |0\rangle. \quad (9)$$

这是“零”方向偏振态,从而实现了对偏振“零”方向的补偿.

总之,在实现卫星量子密钥分配过程中,通信双方首先需要进行偏振基准校准即确定偏振“零”方向,然后在已知 $D$ 的情况下进行偏振跟踪,以完成量子密钥分配协议.

### 3. 光子偏振态变换

基于光子偏振态编码,对于 BB84 协议和 B92 协议,主要涉及六个光子偏振态:水平偏振态、垂直偏振态、45 度偏振态、135 度偏振态、左旋圆偏振态和右旋圆偏振态,分别记为 $|H\rangle, |V\rangle, |\pi/4\rangle, |3\pi/4\rangle, |L\rangle$ 和 $|R\rangle$ .它们分属于三组共轭基:线偏振基 $\{|H\rangle, |V\rangle\}$ , $\{|\pi/4\rangle, |3\pi/4\rangle\}$ 和圆偏振基 $\{|L\rangle, |R\rangle\}$ .将水平偏振态记为偏振态“零”方向,即

$$|H\rangle = |0\rangle, \quad (10)$$

则 $|H\rangle, |V\rangle, |\pi/4\rangle, |3\pi/4\rangle, |L\rangle$ 和 $|R\rangle$ 的琼斯矢量分别为

$$|H\rangle = |0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \quad (11)$$

$$|V\rangle = \left| \frac{\pi}{2} \right\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}, \quad (12)$$

$$\left| \frac{\pi}{4} \right\rangle = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 1 \end{pmatrix}, \quad (13)$$

$$\left| \frac{3}{4}\pi \right\rangle = \frac{1}{\sqrt{2}} \begin{pmatrix} -1 \\ 1 \end{pmatrix}, \quad (14)$$

$$|L\rangle = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ i \end{pmatrix}, \quad (15)$$

$$|R\rangle = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ -i \end{pmatrix}. \quad (16)$$

在实现量子密钥分配协议过程中,光子偏振态要发生改变.对于 $\varphi$ 方向线偏振态 $|\varphi\rangle$ ,算符 $D$ 作用相当于偏振方向偏转角度 $\theta$ ,即

$$\begin{aligned} D|\varphi\rangle &= \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix} \begin{pmatrix} \cos\varphi \\ \sin\varphi \end{pmatrix} \\ &= \begin{pmatrix} \cos(\varphi + \theta) \\ \sin(\varphi + \theta) \end{pmatrix} = |\varphi + \theta\rangle. \end{aligned} \quad (17)$$

根据(17)式得

$$D|H\rangle = D|0\rangle = |\theta\rangle, \quad (18)$$

$$D|V\rangle = D\left| \frac{\pi}{2} \right\rangle = \left| \frac{\pi}{2} + \theta \right\rangle, \quad (19)$$

$$D\left| \frac{\pi}{4} \right\rangle = \left| \frac{\pi}{4} + \theta \right\rangle, \quad (20)$$

$$D\left| \frac{3}{4}\pi \right\rangle = \left| \frac{3}{4}\pi + \theta \right\rangle. \quad (21)$$

对于圆偏振态,算符 $D$ 作用对偏振态没有影响,即

$$D|L\rangle = |L\rangle, \quad (22)$$

$$D|R\rangle = |R\rangle. \quad (23)$$

采用半波片进行偏振跟踪.对于线偏振态,半波

片作用相当于对称操作,使偏振方向以光轴作镜像变换.假设半波片光轴位于  $\theta/2$  则

$$H_{\lambda/2} D |\varphi\rangle = H_{\lambda/2} |\varphi + \theta\rangle = |-\varphi\rangle. \quad (24)$$

根据(24)式得

$$H_{\lambda/2} D |H\rangle = H_{\lambda/2} D |0\rangle = H_{\lambda/2} |\theta\rangle = |0\rangle = |H\rangle, \quad (25)$$

$$\begin{aligned} H_{\lambda/2} D |V\rangle &= H_{\lambda/2} D \left| \frac{\pi}{2} \right\rangle = H_{\lambda/2} \left| \frac{\pi}{2} + \theta \right\rangle \\ &= \left| -\frac{\pi}{2} \right\rangle = \left| \frac{\pi}{2} \right\rangle = |V\rangle, \end{aligned} \quad (26)$$

$$\begin{aligned} H_{\lambda/2} D \left| \frac{\pi}{4} \right\rangle &= H_{\lambda/2} \left| \frac{\pi}{4} + \theta \right\rangle = \left| -\frac{\pi}{4} \right\rangle \\ &= \left| \frac{3}{4} \pi \right\rangle, \end{aligned} \quad (27)$$

$$\begin{aligned} H_{\lambda/2} D \left| \frac{3}{4} \pi \right\rangle &= H_{\lambda/2} \left| \frac{3}{4} \pi + \theta \right\rangle = \left| -\frac{3}{4} \pi \right\rangle \\ &= \left| \frac{\pi}{4} \right\rangle. \end{aligned} \quad (28)$$

对于圆偏振态,有

$$H_{\lambda/2} D |L\rangle = H_{\lambda/2} |L\rangle = |R\rangle, \quad (29)$$

$$H_{\lambda/2} D |R\rangle = H_{\lambda/2} |R\rangle = |L\rangle. \quad (30)$$

从以上分析可以看出,经过算符  $D$  和  $H_{\lambda/2}$  作用后,线偏振基  $\{|H\rangle, |V\rangle\}$  的两个基矢态没有发生改变,即实现了偏振跟踪.而线偏振基  $\{|\pi/4\rangle, |3\pi/4\rangle\}$  和圆偏振基  $\{|L\rangle, |R\rangle\}$  的两个基矢态之间发生了相互转变,但算符  $D$  对  $|L\rangle$  和  $|R\rangle$  并不产生影响.

#### 4. 基于偏振跟踪的量子密钥编码原理

在卫星量子密钥分配中,采用光子偏振态进行量子密钥编码,量子密钥分配协议采用 BB84 协议和 B92 协议. BB84 协议基于四个非正交态,且这四个态分属于两组共轭基,每组共轭基中的两个态是相互正交的.两组共轭基可以选择线偏振基  $\{|H\rangle, |V\rangle\}$ ,  $\{|\pi/4\rangle, |3\pi/4\rangle\}$  和圆偏振基  $\{|L\rangle, |R\rangle\}$  中的任意两个. B92 协议基于任何两个非正交量子态编码,两个非正交态可以从基  $\{|H\rangle, |V\rangle\}$ ,  $\{|\pi/4\rangle, |3\pi/4\rangle\}$  和  $\{|L\rangle, |R\rangle\}$  的基矢态中选择.下面针对 BB84 协议和 B92 协议,对基于偏振跟踪的量子密钥编码原理进行分析.

对于 BB84 协议,若发射机采用基  $\{|H\rangle, |V\rangle\}$  的两个基矢态  $|H\rangle$  和  $|V\rangle$  编码,以  $|H\rangle$  代表二进制数 1,以  $|V\rangle$  代表二进制数 0,即

$$|H\rangle \leftrightarrow 1, \quad (31)$$

$$|V\rangle \leftrightarrow 0, \quad (32)$$

则经算符  $D$  和  $H_{\lambda/2}$  作用后向基  $\{|H\rangle, |V\rangle\}$  投影,得

$$\begin{aligned} P_H H_{\lambda/2} D |H\rangle &= P_H |H\rangle = |H\rangle \langle H | H\rangle \\ &= |H\rangle, \end{aligned} \quad (33)$$

$$\begin{aligned} P_V H_{\lambda/2} D |V\rangle &= P_V |V\rangle = |V\rangle \langle V | V\rangle \\ &= |V\rangle, \end{aligned} \quad (34)$$

式中  $P_H$  和  $P_V$  为投影算符.所以,接收机的编码方式为

$$|H\rangle \leftrightarrow 1, \quad (35)$$

$$|V\rangle \leftrightarrow 0. \quad (36)$$

若发射机采用基  $\{|\pi/4\rangle, |3\pi/4\rangle\}$  的两个基矢态  $|\pi/4\rangle$  和  $|3\pi/4\rangle$  编码,即

$$\left| \frac{\pi}{4} \right\rangle \leftrightarrow 1, \quad (37)$$

$$\left| \frac{3}{4} \pi \right\rangle \leftrightarrow 0, \quad (38)$$

则经算符  $D$  和  $H_{\lambda/2}$  作用后向基  $\{|\pi/4\rangle, |3\pi/4\rangle\}$  投影,得

$$\begin{aligned} P_{3\pi/4} H_{\lambda/2} D \left| \frac{\pi}{4} \right\rangle &= P_{3\pi/4} \left| \frac{3}{4} \pi \right\rangle = \left| \frac{3}{4} \pi \right\rangle \langle \frac{3}{4} \pi | \frac{3}{4} \pi \rangle \\ &= \left| \frac{3}{4} \pi \right\rangle, \end{aligned} \quad (39)$$

$$\begin{aligned} P_{\pi/4} H_{\lambda/2} D \left| \frac{3}{4} \pi \right\rangle &= P_{\pi/4} \left| \frac{\pi}{4} \right\rangle = \left| \frac{\pi}{4} \right\rangle \langle \frac{\pi}{4} | \frac{\pi}{4} \rangle \\ &= \left| \frac{\pi}{4} \right\rangle, \end{aligned} \quad (40)$$

式中  $P_{3\pi/4}$  和  $P_{\pi/4}$  为投影算符.所以,接收机的编码方式为

$$\left| \frac{3}{4} \pi \right\rangle \leftrightarrow 1, \quad (41)$$

$$\left| \frac{\pi}{4} \right\rangle \leftrightarrow 0. \quad (42)$$

若发射机采用基  $\{|L\rangle, |R\rangle\}$  的两个基矢态  $|L\rangle$  和  $|R\rangle$  编码,即

$$|L\rangle \leftrightarrow 1, \quad (43)$$

$$|R\rangle \leftrightarrow 0, \quad (44)$$

则经算符  $D$  和  $H_{\lambda/2}$  作用后向基  $\{|L\rangle, |R\rangle\}$  投影,得

$$\begin{aligned} P_R H_{\lambda/2} D |L\rangle &= P_R |R\rangle = |R\rangle \langle R | R\rangle \\ &= |R\rangle, \end{aligned} \quad (45)$$

$$\begin{aligned} P_L H_{\lambda/2} D |R\rangle &= P_L |L\rangle = |L\rangle \langle L | L\rangle \\ &= |L\rangle, \end{aligned} \quad (46)$$

式中  $P_R$  和  $P_L$  为投影算符.所以,接收机的编码方式为

$$|R\rangle \leftrightarrow 1, \quad (47)$$

$$|L\rangle \leftrightarrow 0. \quad (48)$$

对于 B92 协议,若发射机采用  $|H\rangle$  和  $|\pi/4\rangle$  编码,即

$$|H\rangle \leftrightarrow |1\rangle, \quad (49)$$

$$\left| \frac{\pi}{4} \right\rangle \leftrightarrow |0\rangle, \quad (50)$$

则经算符  $D$  和  $H_{\lambda/2}$  作用后向  $|V\rangle$  和  $|\pi/4\rangle$  投影, 得

$$\begin{aligned} P_{\pi/4} H_{\lambda/2} D |H\rangle &= P_{\pi/4} |H\rangle = \left| \frac{\pi}{4} \right\rangle \left| \frac{\pi}{4} \right\rangle |H\rangle \\ &= \left| \frac{\pi}{4} \right\rangle / \sqrt{2}, \end{aligned} \quad (51)$$

$$\begin{aligned} P_V H_{\lambda/2} D \left| \frac{\pi}{4} \right\rangle &= P_V \left| \frac{3\pi}{4} \right\rangle = |V\rangle \left| \frac{3\pi}{4} \right\rangle \\ &= |V\rangle / \sqrt{2}. \end{aligned} \quad (52)$$

所以, 接收机的编码方式为

$$\left| \frac{\pi}{4} \right\rangle \leftrightarrow |1\rangle, \quad (53)$$

$$|V\rangle \leftrightarrow |0\rangle. \quad (54)$$

若发射机采用  $|H\rangle$  和  $|L\rangle$  编码, 即

$$|H\rangle \leftrightarrow |1\rangle, \quad (55)$$

$$|L\rangle \leftrightarrow |0\rangle, \quad (56)$$

则经算符  $D$  和  $H_{\lambda/2}$  作用后向  $|V\rangle$  和  $|L\rangle$  投影, 得

$$\begin{aligned} P_L H_{\lambda/2} D |H\rangle &= P_L |H\rangle = |L\rangle \left| \frac{\pi}{4} \right\rangle |H\rangle \\ &= |L\rangle / \sqrt{2}, \end{aligned} \quad (57)$$

$$\begin{aligned} P_V H_{\lambda/2} D |L\rangle &= P_V |R\rangle = |V\rangle \left| \frac{3\pi}{4} \right\rangle |R\rangle \\ &= |V\rangle / \sqrt{2}, \end{aligned} \quad (58)$$

所以, 接收机的编码方式为

$$|L\rangle \leftrightarrow |1\rangle, \quad (59)$$

$$|V\rangle \leftrightarrow |0\rangle. \quad (60)$$

若发射机采用  $|\pi/4\rangle$  和  $|L\rangle$  编码, 即

$$\left| \frac{\pi}{4} \right\rangle \leftrightarrow |1\rangle, \quad (61)$$

$$|L\rangle \leftrightarrow |0\rangle, \quad (62)$$

则经算符  $D$  和  $H_{\lambda/2}$  作用后向  $|\pi/4\rangle$  和  $|L\rangle$  投影, 得

$$\begin{aligned} P_L H_{\lambda/2} D \left| \frac{\pi}{4} \right\rangle &= P_L \left| \frac{3\pi}{4} \right\rangle = |L\rangle \left| \frac{3\pi}{4} \right\rangle \\ &= |L\rangle / \sqrt{2}, \end{aligned} \quad (63)$$

$$\begin{aligned} P_{\pi/4} H_{\lambda/2} D |L\rangle &= P_{\pi/4} |R\rangle = \left| \frac{\pi}{4} \right\rangle \left| \frac{\pi}{4} \right\rangle |R\rangle \\ &= \left| \frac{\pi}{4} \right\rangle / \sqrt{2}, \end{aligned} \quad (64)$$

所以, 接收机的编码方式为

$$|L\rangle \leftrightarrow |1\rangle, \quad (65)$$

$$\left| \frac{\pi}{4} \right\rangle \leftrightarrow |0\rangle. \quad (66)$$

从上述分析可以看出, 对于 BB84 协议和 B92 协议, 由于基  $\{|\pi/4\rangle, |3\pi/4\rangle\}$  和  $\{|L\rangle, |R\rangle\}$  的基矢态经过算符  $D$  和  $H_{\lambda/2}$  作用后发生了改变, 所以接收机在进行量子测量投影和量子密钥编码时也要进行相应改变, 这与未采用偏振跟踪时的量子密钥编码原理是不同的。

## 5. 结 论

本文分析了卫星量子密钥分配中采用半波片进行偏振跟踪的原理, 通过旋转半波片实现对偏振“零”方向的跟踪. 通过分析 BB84 协议和 B92 协议中三组共轭基六个光子偏振态的变换关系, 得到基  $\{|H\rangle, |V\rangle\}$  的两个基矢态可实现偏振跟踪, 而基  $\{|\pi/4\rangle, |3\pi/4\rangle\}$  和  $\{|L\rangle, |R\rangle\}$  的两个基矢态之间发生了相互转变. 在此基础上, 通过调整接收机的量子测量投影, 给出了基于偏振跟踪的量子密钥编码原理, 从而实现了 BB84 协议和 B92 协议。

[1] Bennett C H, Bessette F, Brassard G, Salvail L 1992 *J. Crypto.* **5** 3

[2] Hughes R J, Buttler W T, Kwiat P G, Lamoreaux S K, Morgan G L, Nordholt J E, Peterson C G 2000 *Proc. SPIE* **3932** 117

[3] Buttler W T, Hughes R J, Lamoreaux S K, Morgan G L, Nordholt J E, Peterson C G 2000 *Phys. Rev. Lett.* **84** 5652

[4] Rarity J G, Gorman P M, Tapster P R 2001 *Electron. Lett.* **37** 512

[5] Kurtsiefer C, Zarda P, Halder M, Gorman P M, Tapster P R, Rarity J G, Weinfurter H 2002 *Proc. SPIE* **4917** 25

[6] Hughes R J, Nordholt J E, Derkacs D, Peterson C G 2002 *New J. Phys.* **4** 43.1

[7] Shao J, Wu L A 1995 *Acta Sin. Quant. Opt.* **1** 41 (in Chinese) [邵 进、吴令安 1995 量子光学学报 **1** 41]

[8] Wu W, Liu W T, Feng S H, Ou B Q, Liang L M, Li C Z 2004 *Acta Sin. Quant. Opt.* **10** 135 (in Chinese) [吴 伟、刘伟涛、冯少晖、欧保全、梁林梅、李承祖 2004 量子光学学报 **10** 135]

[9] Miao E L, Mo X F, Gui Y Z, Han Z F, Guo G C 2004 *Acta Phys. Sin.* **53** 2123 (in Chinese) [苗二龙、莫小范、桂有珍、韩正甫、郭光灿 2004 物理学报 **53** 2123]

[10] Bennett C H, Brassard G 1984 *Proc. of IEEE Int. Conf. on Comp., Sys. and Sig. Proc.* (India: Bangalore) pp 175—179

[11] Bennett C H 1992 *Phys. Rev. Lett.* **68** 3121

[12] Nordholt J E, Hughes R J, Morgan G L, Peterson C G, Wipf C C 2002 *Proc. SPIE* **4635** 116

# Theoretical analysis of polarization tracking based on half-wave plate

Ma Jing<sup>1)</sup> Zhang Guang-Yu<sup>1)2)</sup> Rong Yi-Wen<sup>1)</sup> Tan Li-Ying<sup>1)</sup>

1) ( *National Key Laboratory of Tunable Laser Technology, Harbin Institute of Technology, Harbin 150001, China* )

2) ( *College of Applied Sciences, Harbin University of Science and Technology, Harbin 150080, China* )

( Received 18 March 2005 ; revised manuscript received 8 June 2005 )

## Abstract

The polarization tracking principle is analyzed by using a half-wave plate in satellite quantum key distribution and the polarization " zero " direction can be corrected by rotation of the half-wave plate. The transforms of six photon polarization states in three conjugative bases are given and the quantum key coding principle based on the polarization tracking is analyzed for the BB84 protocol and B92 protocol.

**Keywords** : quantum key distribution , polarization tracking , half-wave plate

**PACC** : 0365 , 0760