

# 光纤色散与损耗对光量子密钥分发系统的影响<sup>\*</sup>

郑力明<sup>1)†</sup> 王发强<sup>1)†</sup> 刘颂豪<sup>1)</sup>

1) 华南师范大学信息光电子科技学院 广州 510006)

2) 暨南大学电子工程系 广州 510632)

(2006 年 10 月 31 日收到 2007 年 1 月 23 日收到修改稿)

运用量子薛定谔方程,通过计算传输光场干涉强度和分析量子密钥分发系统的误码率,研究了光纤色散和损耗对量子密钥分发系统误码率的影响.研究表明,在目前的基于光纤的量子密钥分发系统中,选择色散位移光纤并以损耗最小波长  $1.55 \mu\text{m}$  为工作波长,同时缩短脉冲宽度,可以有效提高量子密钥系统的传输距离.

关键词:量子保密通信,量子密钥分发,光纤色散,光纤损耗

PACC: 4250, 4230Q, 4210J, 0365

## 1. 引言

量子保密通信是量子信息领域中一个重要的应用研究方向,人们已经对它进行了相当广泛的理论和实验研究,其中国内的同行也做出了相当多的工作<sup>[1-3]</sup>.2006 年,光纤量子保密通信的传输距离已经达到  $150 \text{ km}$ <sup>[4]</sup>,并逐步进入了商业化阶段.但是由于单光子探测器的暗计数和光纤传输线路上的随机应力等不理想因素的影响,实际光纤量子保密通信系统产生的密钥误码率一般为 8% 左右,需要进行纠错,这一过程将会进一步降低密钥的生成率<sup>[5]</sup>.因此,要提高传输距离或密钥生成率就必须降低误码率.

由于密钥误码率是与单光子探测的暗计数成正比,而与光纤通道的透射系数成反比,要进一步降低误码率必须降低光纤损耗或减少单光子探测器的暗计数.在  $1.5 \mu\text{m}$  处的光纤损耗是现有光纤损耗的最低值,难以进一步降低,因此,需要降低探测器的暗计数.现有的单光子探测器在  $-50 \text{ }^\circ\text{C}$  时暗计数水平已达到  $10^{-5}/\text{ns}$ ,要通过降低温度来抑制暗计数是困难的,

因为一般的制冷设备难以满足要求.对此,可以考虑使用更短的光脉冲源,并同时缩短门控雪崩光电探测器(APD)的门宽,以达到降低暗计数和误码率的目的.因为单光子探测器的暗计数在时间上是均匀分布的,与探测器的控制门宽是成正比的.

目前的光量子保密通信系统中的光脉冲宽度一般为  $500 \text{ ps}$  到  $1 \text{ ns}$ ,门宽为  $0.75\text{--}2 \text{ ns}$ <sup>[5]</sup>,因此,为降低误码率可以采用更窄的光脉冲.如目前德国产的用于量子保密通信的 PDL808 型脉冲光源,其脉冲宽度为  $10 \text{ ps}$ .但随着光脉冲的变窄,光纤的色散将逐渐起作用,对系统的脉冲宽度形成限制.本文将综合光纤色散和损耗的影响,对光纤量子保密通信系统中的光纤参数的影响进行研究和讨论.

## 2. 理论计算

由于本文的主要目的是研究光纤对量子密钥分发系统的影响,不失一般性,我们研究基于双 Mach-Zehnder (M-Z) 干涉仪的量子密钥分发系统(图 1)中的光纤色散和损耗对系统的影响.

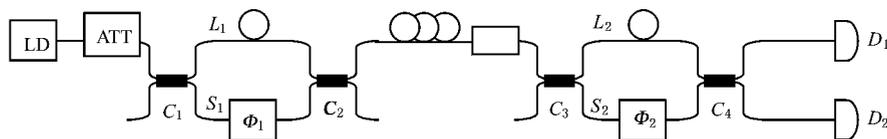


图 1 双 M-Z 干涉仪相位编码系统 LD 为脉冲激光器; $\Phi_1$  和  $\Phi_2$  为相位调制器;ATT 为衰减器; $C_1, C_2, C_3, C_4$  为耦合器; $D_1$  和  $D_2$  为单光子探测器

<sup>\*</sup> 国家自然科学基金(批准号:10404007)资助的课题.

<sup>†</sup> 通讯联系人. E-mail: fqwang98@sina.com

光场在光纤中传输的量子描述可以从光场与 Kerr 介质微观的哈密顿量出发, 通过绝热近似得到光在光纤中传输的量子非线性薛定谔方程, 然后运用 Bethe 近似或 Hartree 近似求解, 导出单粒子波函数所满足的经典方程<sup>[6]</sup>, 或者运用相干态路径积分方法从量子哈密顿量出发, 导出波函数所满足的经典方程<sup>[7]</sup>. 因为用于量子密钥分发的光脉冲是强度极其微弱的光脉冲, 其非空脉冲中只含一个光子的概率达 95% 以上, 且脉冲宽度在皮秒以上, 所以从文献 [6] 的 (34) 式出发, 忽略高阶非线性项, 同时考虑光场偏振<sup>[8]</sup>, 得到光场的量子传输方程

$$\begin{aligned} \frac{\partial A_x}{\partial Z} + \beta_{1x} \frac{\partial A_x}{\partial t} + \frac{i\beta_2}{2} \frac{\partial^2 A_x}{\partial t^2} + \alpha A_x &= 0, \\ \frac{\partial A_y}{\partial Z} + \beta_{1y} \frac{\partial A_y}{\partial t} + \frac{i\beta_2}{2} \frac{\partial^2 A_y}{\partial t^2} + \alpha A_y &= 0, \end{aligned} \quad (1)$$

式中  $A_x, A_y$  为  $x, y$  偏振的光场单粒子波函数, 其模方表示光子在时空中的概率密度分布;  $\beta_{1x}, \beta_{1y}$  分别是光场  $x$  和  $y$  偏振分量的一阶色散;  $\beta_2$  是光场的二阶色散;  $\alpha$  是光纤损耗参数;  $Z$  是光场传输距离.

当输入端输入高型脉冲

$$A_x = A_y = \exp\left(-\frac{t^2}{2T_0^2}\right),$$

其中  $T_0$  是脉冲宽度 (1) 式的解析解为

$$\begin{aligned} A_x &= \frac{T_0}{(T_0^2 - i\beta_2 Z)^2} \exp\left(-\frac{(t - \beta_{1x} Z)^2}{2(T_0^2 - i\beta_2 Z)}\right) \\ &\quad \times \exp(-\alpha Z), \\ A_y &= \frac{T_0}{(T_0^2 - i\beta_2 Z)^2} \exp\left(-\frac{(t - \beta_{1y} Z)^2}{2(T_0^2 - i\beta_2 Z)}\right) \\ &\quad \times \exp(-\alpha Z). \end{aligned} \quad (2)$$

因为本文只研究传输线路中光纤色散和损耗对系统的影响, 所以可假定发送端和接收端的 M-Z 干涉仪是完全理想的. 那么, 由 (2) 式便可以得到接收端的脉冲干涉结果如下:

$$\begin{aligned} I &= \frac{1}{4} \frac{T_0^2}{2\sqrt{T_0^4 + \beta_2^2 Z^2}} \left\{ \exp\left(-\frac{(t - \beta_{1x} Z)^2 T_0^2}{T_0^4 + \beta_2^2 Z^2}\right) \right. \\ &\quad \left. + \exp\left(-\frac{(t - \beta_{1y} Z)^2 T_0^2}{T_0^4 + \beta_2^2 Z^2}\right) \right\} \exp(-2\alpha Z). \end{aligned} \quad (3)$$

(3) 式对时间积分, 便得到在 Bob 端接收到光子的概率.

### 3. 分析及讨论

首先, 分析 (3) 式中各项的含义. (3) 式第一项中

的  $1/4$  是因为  $C_2$  和  $C_4$  两个耦合器的分光所引起的. (3) 式最后一项是光纤损耗引起的, 它说明光子到达接收端的概率将因损耗而随传输距离降低. (3) 式的其余各项则代表了光纤色散的影响. 通过该解析式, 我们可以看出光纤二阶色散将使脉冲在传输过程中的波形展宽, 使初始脉冲宽度  $T_0$  的展宽因子为  $T_0 \sqrt{1 + (Z|\beta_2|/T_0^2)^2}$ . 图 2 给出了不考虑光纤损耗和偏振色散时, 普通单模光纤传输初始脉冲宽度为 20 ps 的  $1.55 \mu\text{m}$  光脉冲展宽情况, 其中二阶色散  $\beta_2$  为  $-20 \text{ ps}^2/\text{km}$ <sup>[8]</sup>, 图中从上到下的 4 条曲线分别为传输距离为 0, 25, 50 和 75 km 时接收端的脉冲干涉强度曲线. 而光纤的一阶色散则影响两个偏振分量的到达时间, 由于光纤双折射变化是随机的, 所以两个偏振分量的到达时间差也将是随机的, 其方差与传输距离的关系为<sup>[7]</sup>

$$\sqrt{\Delta T^2} = \sqrt{(Z|\beta_x - \beta_y|)^2} = D_p Z^{1/2} \quad (4)$$

式中  $D_p$  是光纤二阶色散参数, 通常取为  $0.5 \text{ ps}/\text{km}^{1/2}$ . 图 3 给出了传输距离为 50 km 时,  $x$  方向偏振分量超前或落后时的接收端干涉强度曲线, 其中时间按 (4) 式取值, 初始脉冲宽度为 20 ps, 二阶色散  $\beta_2$  为  $-20 \text{ ps}^2/\text{km}$  对应于  $1.55 \mu\text{m}$  光脉冲在普通单模光纤中的传输情况. 由于两个偏振分量的到达时间差是满足麦克斯韦分布的随机量, 所以接收端光脉冲实际到达时间是不确定的, 随时间而缓慢变化, 但绝大多数到达脉冲处于图 3 所示的两脉冲之间.

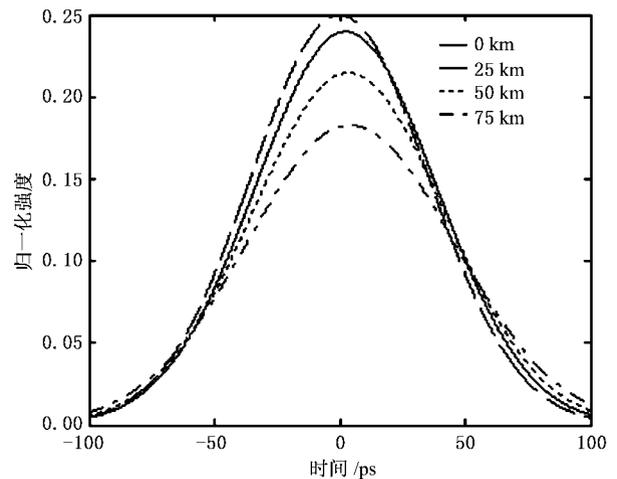


图 2 不同传输距离时的接收端脉冲干涉强度曲线

其次, 讨论光纤色散和损耗对量子密钥分发系统的量子比特误码率  $Q$  的影响. 对于采用弱相干光脉冲源的量子密钥分发系统, 其由雪崩光电二极

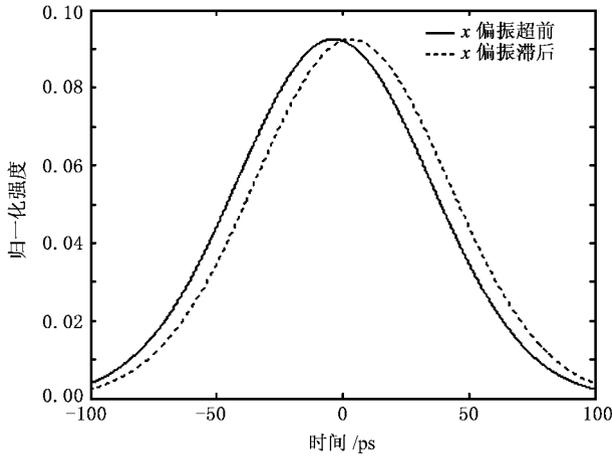


图3 存在偏振色散时的接收端脉冲干涉强度曲线

管暗电流引起的量子比特误码率由下式决定<sup>[5]</sup>：

$$Q = \frac{P_{\text{dark}} n}{2\mu T \eta}, \quad (5)$$

式中  $\mu$  为平均每脉冲内所含的光子数,一般取为 0.1;  $\eta$  为雪崩光电二极管的检测效率,如果不采用上转换技术,一般可达 15%;  $n$  为检测系统所采用的雪崩光电二极管个数,通常为 4<sup>[5]</sup>;  $T$  为光子到达接收端的传输系数,由(3)式中的因子  $\exp(-2\alpha Z)$  所确定;  $P_{\text{dark}}$  是雪崩光电二极管的暗计数概率,其与雪崩光电二极管的质量、环境温度、反向电压以及门宽有关。目前,在  $-50^\circ\text{C}$  时暗计数概率已达到  $10^{-5}/\text{ns}$ <sup>[5]</sup>。

在其他条件不变的情况下,雪崩光电二极管的暗计数概率与门宽成正比,如果采用较窄的弱脉冲源,则可以降低门宽,从而有效降低暗计数概率,以减小量子比特误码率。但是由于光纤色散,光脉冲将展宽。从(3)式可以看出,色散对光脉冲只影响光脉冲的形状和到达时间,又由于脉冲是高斯波形,所以只要像其他实验一样将探测器的门宽设为脉冲宽度的 2 倍<sup>[5]</sup>,就可以忽略波形对误码率的影响了。考虑到光纤一阶和二阶色散的影响,我们可以将探测器的门宽  $W$  设置如下：

$$W = 2\left\{T_0 \sqrt{1 + (Z|\beta_2|/T_0^2)^2} + D_p \sqrt{Z}\right\}. \quad (6)$$

从(6)式可以看出,偏振色散的影响与传输距离成 1/2 次方的关系,而二阶色散的影响近似与传输距离的一次方成正比。所以,在脉冲宽度为皮秒量级

且传输距离为几百公里以内,可以忽略偏振色散的影响。

采用前面所给出的参数,下面将分析普通单模光纤和色散位移光纤中分发量子密钥的误码率。对于普通单模光纤,其在  $1.3\ \mu\text{m}$  波长处二阶色散为零,损耗为  $0.35\ \text{dB/km}$ ,而在  $1.55\ \mu\text{m}$  波长处,二阶色散  $\beta_2$  为  $-20\ \text{ps}^2/\text{km}$ ,损耗为  $0.2\ \text{dB/km}$ 。利用这些参数可以进行计算:如果利用  $20\ \text{ps}$  脉冲宽度的  $1.3\ \mu\text{m}$  波长脉冲经过  $96\ \text{km}$  的光纤传输,系统量子比特误码率  $Q$  便达到了 15% (一般认为  $Q$  超过 15% 后,就很难通过单向的密性放大使窃听者的信息变为零而收发双方仍保留不为零的互信息<sup>[9,10]</sup>),而用  $500\ \text{ps}$  脉冲宽度的  $1.3\ \mu\text{m}$  波长脉冲传输  $58\ \text{km}$  时  $Q$  便达到 15%。如果利用  $20\ \text{ps}$  脉冲宽度  $1.55\ \mu\text{m}$  的光脉冲,须传输  $131\ \text{km}$  后  $Q$  才能达到 15%,用  $500\ \text{ps}$  脉冲宽度的  $1.55\ \mu\text{m}$  波长脉冲,在传输  $102\ \text{km}$  后  $Q$  便达到 15%。由此可以看出,使用  $1.55\ \mu\text{m}$  波长短脉冲有利于提高普通单模光纤中量子密钥传输距离。但是由于普通单模光纤在  $1.55\ \mu\text{m}$  波长处的色散较大,不利于探测器门宽的降低,影响了传输距离的提高。如果采用色散位移光纤(即 G653 光纤)和采用脉冲宽度为  $20\ \text{ps}$  的脉冲,传输距离将提高到  $166\ \text{km}$ 。如果脉冲宽度进一步减小到  $10\ \text{ps}$ ,则传输距离将达到  $177\ \text{km}$ 。

从以上的分析可以看出,通过选择合适的参数,包括光纤类型、工作波长和脉冲宽度,可以有效提高量子密钥系统的传输距离。

## 4. 结 论

本文通过理论计算和分析,研究了光纤色散和损耗对量子密钥分发系统误码率的影响。研究表明,在目前的基于光纤的量子密钥分发系统中,选择色散位移光纤并以损耗最小的波长( $1.55\ \mu\text{m}$ )为工作波长,同时缩短脉冲宽度,可以有效提高量子密钥系统的传输距离。

在实际的光纤线路中,由于环境振动和温度变化等随机因素将使接收端的干涉对比度下降,产生误码,但这并不影响本文的结论。关于随机因素对干涉对比度的影响,已超出本文的范围,我们将另文讨论。



- [ 1 ] Wu G , Zhou C Y , Chen X L *et al* 2005 *Acta Phys. Sin.* **54** 3622 ( in Chinese ) [ 吴 光、周春源、陈修亮等 2005 物理学报 **54** 3622 ]
- [ 2 ] Tang Z L , Li M , Wei Z J *et al* 2005 *Acta Phys. Sin.* **54** 2534 ( in Chinese ) [ 唐志列、李 铭、魏正军等 2005 物理学报 **54** 2534 ]
- [ 3 ] He G Q , Zeng G H 2006 *Chin. Phys.* **15** 1284
- [ 4 ] Tadamas K , Yoshihiro N , Takaaki H , Akihisa T , Hideo K , Kazuo N 2004 *Jpn. J. Appl. Phys.* **43** 1217
- [ 5 ] Ma R L 2006 *Quantum Cryptography Communication* ( Beijing : Science Press ) pp56—60 ( in Chinese ) [ 马瑞霖 2006 量子密码通信(北京 科学出版社)第 56—60 页 ]
- [ 6 ] Wen Y J , Yang X L , Zhang M D 1996 *Acta Phys. Sin.* **45** 394 ( in Chinese ) [ 温扬敬、杨祥林、张明德 1996 物理学报 **45** 394 ]
- [ 7 ] Deng L B , Chen W M 1989 *Chin. J. Quantum Electron.* **6** 173 ( in Chinese ) [ 邓履璧、陈未名 1989 量子电子学报 **6** 173 ]
- [ 8 ] Agrawal G P 2001 *Nonlinear Fiber Optics* ( 3rd ed ) New York : Elsevier ) Chap 1 , 6
- [ 9 ] Ekert A K , Huttner B , Palma G M 1994 *Phys. Rev. A* **50** 1047
- [ 10 ] Csizar I , Komer J 1978 *IEEE Trans. Inform. Theory* **24** 339

## The influence of dispersion and loss on quantum key distribution system<sup>\*</sup>

Zheng Li-Ming<sup>1,2)</sup> Wang Fa-Qiang<sup>1)†</sup> Liu Song-Hao<sup>1)</sup>

<sup>1)</sup> School for Information and Optoelectronic Science and Engineering , South China Normal University , Guangzhou 510006 , China )

<sup>2)</sup> Department of Electronic Engineering , Jinan University , Guangzhou 510632 , China )

( Received 31 October 2006 ; revised manuscript received 23 January 2007 )

### Abstract

The influence of dispersion and loss on quantum bit error rate of a quantum key distribution system is analytically studied via quantum Schrödinger equation. The results show that the haul of quantum key distribution system can be increased by using the dispersion shift fiber and weak pulse with short pulse width in wavelength of 1.55  $\mu\text{m}$ .

**Keywords :** quantum cryptography , quantum key distribution , fiber dispersion , fiber loss

**PACC :** 4250 , 4230Q , 4210J , 0365

<sup>\*</sup> Project supported by the National Natural Science Foundation of China ( Grant No. 10404007 ).

<sup>†</sup> Corresponding author. E-mail : fqwang98@sina.com