时间抖动对相位编码量子密钥分发系统量子误码率的影响

陈 帅 王金东 钟平平 魏正军 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,广东 广州 510631)

摘要 就时间抖动对相位编码量子密钥分发(QKD)系统量子误码率(QBER)的影响进行了系统的分析,建立了相位编码 QKD 系统量子误码率和时间抖动关系的物理模型,给出了单光子脉冲的一般波形函数和量子误码率之间的关系。针对高斯脉冲分布,导出了时间抖动引起的相位编码 QKD 系统的量子误码率与脉冲宽度和时间抖动分布参数之间的定量关系。得出高斯分布的单光子脉冲在确定的时间抖动分布的情况下系统的量子误码率。提出了通过控制系统抖动参数和单光子脉冲宽度来减小系统量子误码率的方法。

关键词 量子密钥分发;相位编码;量子误码率;时间抖动

中图分类号 O431.2 **文献标识码** A **doi**: 10.3788/AOS201131.0727001

Influence of Time Jitter on Quantum Bit Error Rate of Phase-Coding Quantum Key Distribution System

Chen Shuai Wang Jindong Zhong Pingping Wei Zhengjun Liu Songhao

(*Key Laboratory of Photonic Information Technology of Guangdong Higher Education Institutes, School of Information and Optoelectronic Science and Engineering, South China Normal University, Guangzhou, Guangdong* 510631, *China*)

Abstract The quantum bit error rate (QBER) caused by time jitter in the phase-coding quantum key distribution (QKD) system is analysed. The physical model of the relation between the QBER and the time jitter in the phase-coding QKD is proposed. The formula between the general waveform function of the single photon pulses and QBER is given. Based on the distribution of Gaussian pulse, the quantitative relation among QBER, the pulse width and the distribution of the time jitter is educed, based on which the QBER of a certain time jitter distribution can be calculated in the Gaussian single photon pulse. The method of reducing the QBER by the control of the system′s time jitter and the width of single photon pulse is proposed.

Key words quantum key distribution; phase coding; quantum bit error rate; time jitter

OCIS codes 270.5568; 270.5565; 060.5060; 060.2330

1 引 言

量子密钥分发(QKD)是为通信的双方,即发送端(Alice)和接收端(Bob),在窃听者(Eve)面前提供了一种安全地分享密钥的方法[1~3],其安全性是由量子力学基本原理来保障的[4]。因为一个未知的量子态不能被完美克隆[5,6],任何试图窃听的行为都有可能扰乱量子态。因此,在对传输量子态的误码率(BER)进行评估之后,就可以判断出通信程中是否存在窃听者。

QKD 系统的编码方式有偏振编码、相位编码、时间编码、频率编码和混合编码等,其中比较常用是偏振编码和相位编码。由于光子信号在光纤中传输时其相位信息比偏振信息更容易保持,因此绝大多数现有的光纤量子密码系统都采用相位编码方案[4]。就相位编码系统而言,目前常用的是双不等臂马赫-曾德尔(M-Z)干涉仪的相位编码系统和差分相位编码系统等。而这些相位编码系统的特点是:首先在发送端将单光子脉冲通过时分的方式分

收稿日期: 2011-01-17; **收到修改稿日期**: 2011-02-25

基金项目: 广州市科技支撑计划(2008Z1-D501)、广东省工业攻关项目(2007B010400009)和中国科学院量子信息技术国家重点实验室开放资助课题。

作者简介: 陈 帅(1985—),男,硕士研究生,主要从事量子保密通信方面的研究。E-mail: chenshuai3639@163.com

导师简介: 王金东(1974—),男,博士,副研究员,主要从事量子保密通信方面的研究。E-mail: jindongwqkd@126.com

裂为两个或多个单光子概率幅脉冲，并根据协议对这些单光子概率幅脉冲进行随机相位调制。然后经过长程的光纤传输，到达通信接收方后利用光学延迟的方法使这两个单光子概率幅脉冲重合并发生干涉叠加以检出被调制的相位信息。然而，光脉冲由于器件和光纤传输引入了时间抖动，会造成不能按照理想时刻到达通信接收机，由于存在时间抖动，在接收端采用光学延迟环进行检测时就会有不同重合度干涉情况的发生，给系统的密钥信息带来一定的误码率。

在相位编码 QKD 系统中，影响光脉冲干涉叠加的时间抖动主要来源于以下几个方面：1）双不等臂 M-Z 干涉仪系统中的两个不等臂 M-Z 干涉仪带来的不同传输路径之间的抖动，该抖动由于干涉环的臂长一般很小，所以对干涉叠加引起的误码贡献不大[7,8]；2）采用强度调制器产生弱相干光脉冲的差分相位系统中，由于强度调制器驱动电脉冲的时间精度有限而造成发送端发送的弱相干光脉冲本身存在的时间抖动[9]，该抖动为 10～30 ps 量级[10]。无论接收端的单比特延迟环如何选取，都会由于该时间抖动引入一定的系统误码，特别是当系统采用的光脉冲宽度小到可以和时间抖动的量级可以相比拟时，由时间抖动影响而产生的系统误码尤其显著[11,12]；3）所有相位编码系统均采用时分的方式在信道中传输，在接收端采用响应延迟的方法进行相位检测，因此长程传输信道中引起的光脉冲抖动也在一定程度上影响了系统误码的大小[9,13～16]。

文献[7]对基于弱相干光的差分相位编码系统和基于双不等臂 M-Z 相位编码系统的时间抖动进行了测量，同时建立了相位编码 QKD 系统量子误码率和时间抖动关系的物理模型，给出了单光子脉冲的一般波形函数和量子误码率之间的关系式。本文在文献[7]的基础上，针对具体的光脉冲高斯形状对时间抖动引起的系统量子误码率进行了理论计算和模拟。针对时间抖动的统计分布是高斯分布的情况，导出了时间抖动引起的相位编码 QKD 系统的量子误码率与脉冲宽度和时间抖动分布参数之间的定量关系，提出了通过控制系统抖动参数和单光子脉冲宽度来减小系统量子误码率的方法，可以进一步有效降低系统的实际量子误码率。

2　源于时间抖动的系统误码率

图 1 和图 2 分别为常见的基于双不等臂 M-Z 干涉仪的 QKD 系统和强度调制弱相干光的差分相位编码 QKD 系统。其中 LD 表示脉冲激光光源，CW 表示连续激光光源，ATT 表示衰减器，PM 表示相位调制器，IM 表示强度调制器，DET 表示探测器，L_1 表示 M-Z 干涉仪的长臂，L_2 表示 M-Z 干涉仪的短臂。在这两个典型的相位编码系统中，发送端通过不等臂的 M-Z 干涉仪或强度调制器产生在时域上分开的光脉冲，到达接收端后利用一个单比特延迟环进行干涉并检测出相位差信息。如果这些时分的单光子脉冲不能在理想的时刻到达通信接收端并进行干涉，接收端进行相位检测时光脉冲的叠加干涉情况就会出现完全干涉叠加、部分干涉叠加和完全不干涉叠加的三种情况，如图 3 所示。

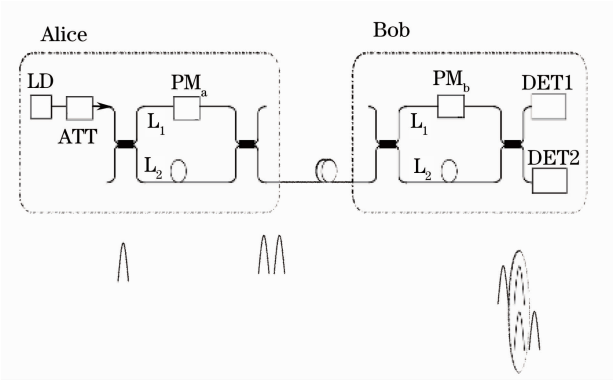

图 1　基于双不等臂 M-Z 干涉仪相位编码系统

Fig. 1　Phase-coding system based on the double unequal-arm Mach-Zehnder interferometers

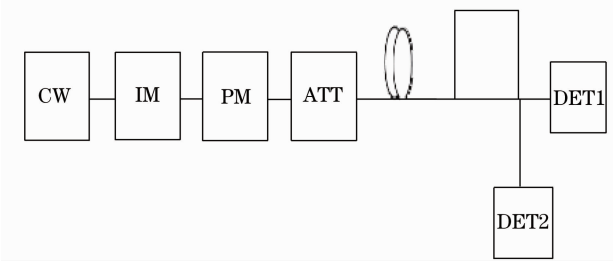

图 2　弱相干光的差分相位编码 QKD 系统

Fig. 2　Differential-phase-coding QKD system based on weak coherent light

对源于时间抖动而引起的系统量子误码率进行计算如图 4 所示，假设两个光脉冲的时间间隔为 τ，光脉冲延时为 t，光脉冲光强函数分别为 $I(t)$ 和 $I(t-\tau)$，光脉冲的全宽为 T，则可以根据干涉叠加的情况分为 3 个区域：1）$t=0\sim\tau$，没有干涉叠加，如果在这段时间内探测到光子，那么光子将会被等概率地从耦合器输出到两个探测器上，量子误码率为 50%；2）$t=\tau\sim T$，这是两个脉冲发生干涉叠加的区域，假设可以用主动相位补偿的方法使得这个区域发生干涉叠加的两个脉冲具有理想的调制相位；3）$t=$

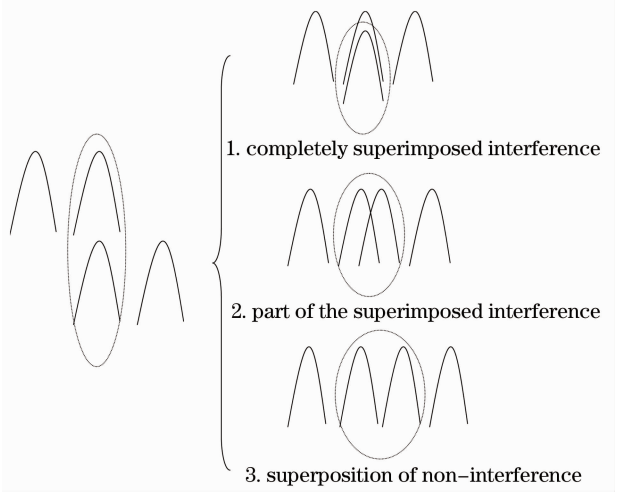

图 3　在接收端光脉冲干涉时可能出现的三种情况

Fig. 3　Three possibilities of optical pulse interference occurring at the Bob′s side

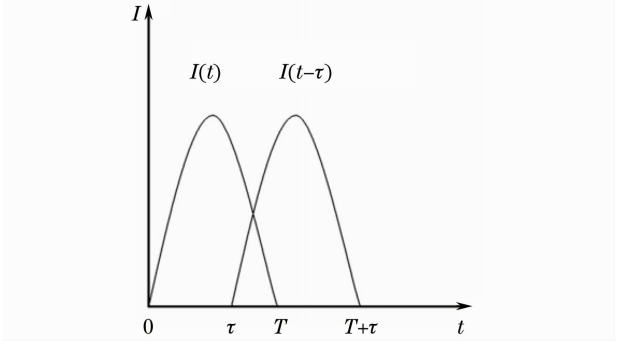

图 4　两个光脉冲不完全重合时的干涉叠加示意图

Fig. 4　Sketch of interference superposition of the incomplete overlap of two optical pulses

$T\sim T+\tau$，没有发生干涉叠加，如果在这段时间内探测到光子，那么光子将会被等概率地从耦合器输出到两个探测器上，量子误码率为 50%。

计算当两个光脉冲部分叠加干涉时的量子误码率，根据光的干涉叠加原理，干涉光强 I 为

$$I=\int(I_1+I_2+2\sqrt{I_1I_2}\cos\alpha)\mathrm{d}t,\tag{1}$$

式中 I_1 和 I_2 分别代表这两叠加干涉的光脉冲光强；α 代表这两个干涉光脉冲之间的相位差。干涉叠加的量子误码率为

$$R_{\mathrm{QBE}}(t)=\frac{1-V}{2},\tag{2}$$

式中 V 为干涉对比度：

$$V=\frac{I_{\max}-I_{\min}}{I_{\max}+I_{\min}},\tag{3}$$

式中 $I_{\max}$ 和 $I_{\min}$ 分别代表干涉叠加时出现的最大和最小输出光强。在图 4 的坐标系中，设第一个光脉冲光强分布函数为 $I(t)$，则在经过了 τ 延时后第二个光脉冲光强分布函数为 $I(t-\tau)$，对三个干涉区域进行积分，则 $I_{\max}$ 和 $I_{\min}$ 为

$$I_{\max}=\int_0^{\tau}I(t)\mathrm{d}t+\int_T^{T+\tau}I(t-\tau)\mathrm{d}t+\int_{\tau}^{T}\left[I(t)+I(t-\tau)+2\sqrt{I(t)I(t-\tau)}\right]\mathrm{d}t,\tag{4}$$

$$I_{\min}=\int_0^{\tau}I(t)\mathrm{d}t+\int_T^{T+\tau}I(t-\tau)\mathrm{d}t+\int_{\tau}^{T}\left[I(t)+I(t-\tau)-2\sqrt{I(t)I(t-\tau)}\right]\mathrm{d}t.\tag{5}$$

将(2)～(5)式合并化简得

$$R_{\mathrm{QBE}}(t)=\frac{1}{2}-\frac{\int_{\tau}^{T}\sqrt{I(t)I(t-\tau)}\mathrm{d}t}{\int_0^{T}I(t)\mathrm{d}t+\int_{\tau}^{\tau+T}I(t-\tau)\mathrm{d}t}.\tag{6}$$

(6)式是光脉冲光强分布函数为一般形式时部分叠加干涉引起的量子误码率结果。由(6)式可见当抖动时间 $t=0$ 时，量子误码率 $R_{\mathrm{QBE}}(t)=0$；当抖动时间大于脉宽，即 $t>T$ 时，(6)式中第二项的分子项代表的干涉项将为 0，这时的量子误码率为 50%，符合对物理模型的分析。光脉冲形状一般为高斯分布，所以假设在干涉端的两个单光子概率幅度脉冲为高斯脉冲。其复振幅分布为

$$E(t)=A\exp\left(\mathrm{i}\varphi-\frac{t^2}{2\sigma^2}\right),\tag{7}$$

式中 A 为光脉冲的振幅，σ 为高斯脉冲的标准方差，φ 为高斯脉冲的相位。光脉冲光强分布函数 $I(t)$ 和 $I(t-\tau)$ 分别为

$$I(t)=|E(t)|^2=\left|A\exp\left[\mathrm{i}\varphi_1-\frac{(t-T/2)^2}{2\sigma^2}\right]\right|^2=A^2\exp^2\left[-\frac{(t-T/2)^2}{2\sigma^2}\right],\tag{8}$$

$$I(t-\tau)=|E^2(t-\tau)|^2=\left|A\exp\left[\mathrm{i}\varphi_2-\frac{(t-T/2-\tau)^2}{2\sigma^2}\right]\right|^2=A^2\exp^2\left[-\frac{(t-T/2-\tau)^2}{2\sigma^2}\right].\tag{9}$$

假设理想的高斯脉冲的脉宽 $T=8\sigma$。将(8)，(9)式代入(6)式并化简得

$$R_{\mathrm{QBE}}(t)=1/2+\frac{\exp(-8\tau^2/T^2)\mathrm{erf}[2\sqrt{2}(-1+\tau/T)]}{2\mathrm{erf}(2\sqrt{2})},\tag{10}$$

式中 erf 是误差函数。令 x 为 τ/T，将 x 代入(10)式

得到 R_{QBE} 随 x 变化的曲线图，如图 5 所示。

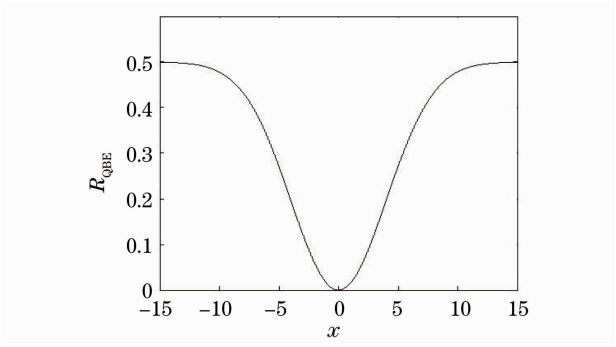

图 5　R_{QBE} 随任意两个相邻光脉冲的 x 的变化曲线

Fig. 5　R_{QBE} versus x from any two adjacent optical pulses

根据图 5 的曲线分布对曲线的表达式重新模拟，简化(10)式为

$$R_{\mathrm{QBE}}(t) = 0.50 - 0.50\exp\left[-\frac{(\tau/T+7.79635\mathrm{e}-4)^2}{0.124161}\right]. \quad (11)$$

其中按照(11)式和(10)式做出的曲线完全重合，如图 5 所示，同时(10)式和(11)式中的变量还都是 τ/T，可以说模拟结果(11)式是正确。由(11)式可以得到任意两个相邻光脉冲量子误码率 R_{QBE} 与脉宽 T、时间抖动 t 的三维分布图，如图 6 所示。

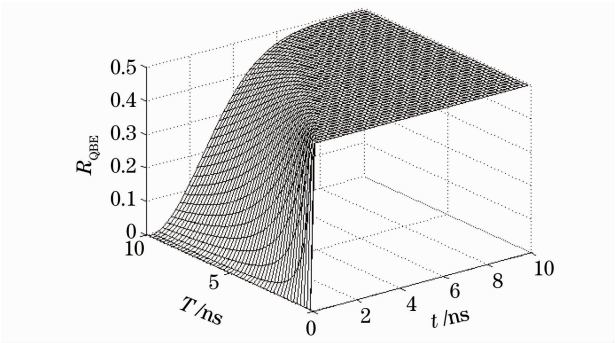

图 6　任意两个相邻光脉冲 R_{QBE} 与 T、t 的三维分布图

Fig. 6　Relation between R_{QBE}, T and t from any two adjacent optical pulses in three-dimensional coordinates

根据脉冲之间相对延时的统计分布来计算系统长期工作时由时间抖动而产生的量子误码率。文献[17]的研究发现时钟频率抖动的统计分布是一个高斯函数；同时文献[18,19]对光脉冲在光纤里面传输的时间抖动研究发现这些时间抖动的统计分布也是高斯函数。而这两个因素是 QKD 系统中由于时间抖动引起误码的最主要的因素，因此假设强度调制弱相干光的 QKD 系统的时间抖动统计分布函数为高斯函数 $\eta(t)$，它是不同抖动时间 t 的概率分布，抖动时间为 t 的部分叠加干涉的概率是 $\eta(t)$：

$$\eta(t) = \frac{1}{\sigma'\sqrt{2\pi}}\exp\left(-\frac{2t^2}{\sigma'^2}\right), \quad (12)$$

式中 σ' 为统计分布的标准方差，t 为抖动时间。

系统在长期工作时由于时间抖动引起误码率的表达式：

$$R = \int_{-\infty}^{\infty} R_{\mathrm{QBE}}(t)\times\eta(t)\mathrm{d}t = \int_{-\infty}^{\infty}\left\{0.5-0.5\exp\left[-\frac{(t/T+7.79635\mathrm{e}-4)^2}{0.124161}\right]\right\}\times\frac{1}{\sigma'\sqrt{2\pi}}\exp\left(-\frac{t^2}{\sigma'^2}\right)\mathrm{d}t = 0.25-0.19947\exp\left[\frac{0.0000394287}{2\times(T/\sigma')^2+8.05406}\right]\times\frac{1}{\sqrt{2.5369\times(\sigma'/T)+2/\pi}}. \quad (13)$$

根据(13)式得到相位编码的 QKD 系统长期工作时由于时间抖动引起误码率 R、脉宽 T 和时间抖动统计分布的标准方差 σ' 的三维分布，如图 7 所示。还可以得到时间抖动引起误码率 R 与 T/σ' 比率的二维分布图，如图 8 所示。由图 8 可见，当时间抖动的量级远小于脉冲宽度时，由时间抖动引起的系统量子误码率也会很小；而当时间抖动的量级可以和脉冲宽度相比拟时，由时间抖动引起的系统量子误码率就会尤其显著。

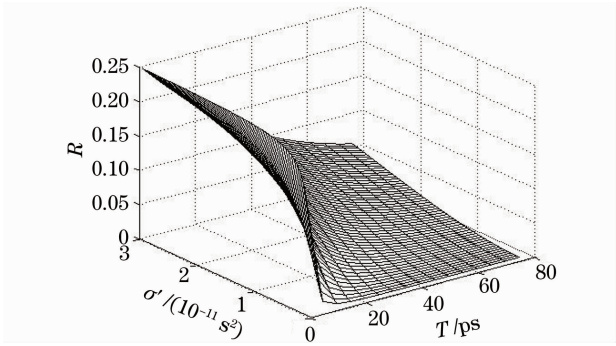

图 7　误码率 R 随脉宽 T 和时间抖动统计分布的标准方差 σ' 变化

Fig. 7　Bit error rate R versus pulse width T and the standard variance σ' of time jitter statistical distribution

3　讨　论

系统各部分的时间抖动会给系统引入误码，且源于时间抖动的系统误码随时间抖动参数减小而减小或在一定的时间抖动参数下随单光子脉冲宽度增

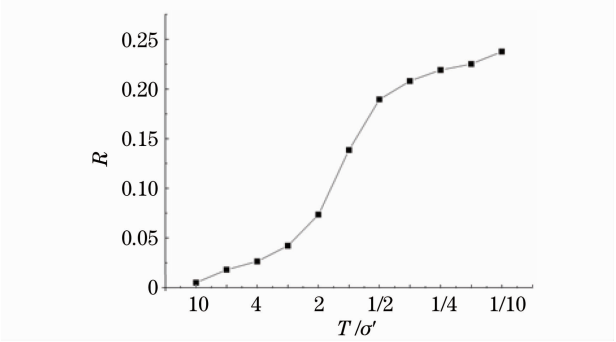

图 8　误码率 R 随 T/σ' 变化

Fig. 8　Bit error rate R versus T/σ'

大而减小。基于双不等臂 M-Z 干涉仪的系统，两个不等臂干涉仪带来的时间抖动很小，对误码的影响也很小，其主要的时间抖动来自于长程传输信道带来的时间抖动[9]。基于强度调制的弱相干光的差分相位编码系统的时间抖动主要源于强度调制器驱动电脉冲的时间精度带来的抖动和长程传输信道带来的抖动。当系统采用的单光子脉冲的宽度不断减小时，例如文献[12]采用 10 ps 的单光子脉冲，源于时间抖动的系统误码会在一定程度上增加，尤其当单光子脉冲宽度和时间抖动量级可以相比拟时，时间抖动的系统误码会显著增加；另一方面，采用较小宽度的单光子脉冲有助于提高单光子的探测性能[20~22]，因此在选择光脉冲宽度时，应同时考虑时间抖动对量子误码率的影响以及脉冲宽度对单光子探测器的影响，以获得最佳的系统性能。所以减小长程传输的时间抖动和改善驱动电脉冲的时间抖动参数将在一定程度上减小系统的量子误码率。

4　结　　论

通过对源于时间抖动的系统量子误码率的分析，给出了源于时间抖动的系统量子误码率和系统各部分抖动参数以及所采用单光子脉冲宽度之间的物理模型和定量关系。由理论分析可知，采用时间抖动参数较小的精密驱动电脉冲可以进一步减小基于强度调制弱相干光相位编码系统的量子误码率，而采用相关方法减小长程传输引起的时间抖动也可以在一定程度上减小系统的量子误码率。在同等时间抖动参数情况下，采用较宽的单光子脉冲可以减小系统量子误码率，但采用较窄的单光子脉冲有助于提高单光子探测的性能，因此，一方面尽量采用相关技术减小时间抖动参数，另一方面应在保证单光子脉冲宽度远大于时间抖动参数的情况下尽量减小单光子脉冲宽度以提高系统的整体性能。

参　考　文　献

1 C. H. Bennett, G. Brassard. Quantum cryptography: public key distribution and coin tossing[J]. *IEEE*, 1984, **175**: 175～179

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

3 H.-K. Lo, Y. Zhao. Quantum cryptography [J]. *Enc. of Complexity and Systems Science*, 2009, **8**: 7265～7289

4 N. Gisin, G. Ribordy, W. Tittel *et al.*. Quantum cryptography [J]. *Rev. Mod. Phys.*, 2002, **74**(1): 145～195

5 W. K. Wootters, W. Zurek. A single quantum cannot be cloned [J]. *Nature*, 1982, **299**(5886): 802～803

6 D. Dieks. Communication by EPR devices[J]. *Phys. Lett. A*, 1982, **92**(6): 271～271

7 Wang Jindong, Wei Zhengjun, Zhang Hui *et al.*. The influence of the time delay through long trunk fiber on the phase-coding quantum key distribution system[J]. *Acta Physica Sinica*, 2010, **59**(8): 5514～5522
王金东，魏正军，张　辉 等. 长程光纤传输的时间抖动对相位编码量子密钥分发系统的影响[J]. 物理学报，2010，**59**(8)：5514～5522

8 Liu Xiaobao, Tang Zhilie, Liao Changjun *et al.*. Study on quantum bit error rate of quantum key distribution system based on the double Mach-Zehnder interferometers [J]. *Chinese J. Quant. Electron.*, 2006, **23**(2): 191～196
刘小宝，唐志列，廖常俊 等. 双非对称 Mach-Zehnder 干涉仪量子密钥分发系统误码率的研究[J]. 量子电子学报，2006，**23**(2)：191～196

9 D. Stucki, C. Barreiro, H. Zbinden *et al.*. Continuous high speed coherent one-way quantum key distribution [J]. *Opt. Express*, 2009, **17**(16): 13326～13334

10 B. Mesgarzadeh, M. Hansson, A. Alvandpour. Jitter characteristic in resonant clock distribution [J]. *IEEE*, 2006, **42**(44): 464～467

11 H. Takesue, E. Diamanti, T. Honjo *et al.*. Differential phase shift quantum key distribution experiment over 105 km fibre[J]. *New J. Phys.*, 2005, **7**(1): 232～232

12 H. Takesue, E. Diamanti, C. Langrock *et al.*. 10-GHz clock differential phase shift quantum key distribution experiment[J]. *Opt. Express*, 2006, **14**(20): 9522～9530

13 S. M. Foreman, K. W. Holman, D. H. Darren *et al.*. Remote transfer of ultrastable frequency references via fiber networks[J]. *Rev. Sci., Instrum.*, 2007, **78**(2): 021101

14 N. R. Newbury, P. A. Williams, W. C. Swann. Coherent transfer of an optical carrier over 251 km[J]. *Opt. Lett.*, 2007, **32**(21): 3056～3057

15 L. S. Ma, P. Jungner, J. Ye *et al.*. Delivering the same optical frequency at two places: accurate cancellation of phase noise introduced by an optical fiber or other time-varying path[J]. *Opt. Lett.*, 1994, **19**(21): 1777～1779

16 Pei Changxing, Han Baobin, Zhao Nan *et al.*. QBER Modeling and simulation of QKD in optical fiber with force [J]. *Acta Photonica Sinica*, 2009, **38**(2): 422～424
裴昌幸，韩宝彬，赵　楠 等. 光纤信道压力作用下量子密钥分发误码率建模与仿真[J]. 光子学报，2009，**38**(2)：422～424

17 Huang Jiunlang, Huang Juijer, Liu Yuanshuang. A low-cost jitter measurement technique for BIST applications [J]. *J. Electron. Testing: Theor. Appl.*, 2006, **22**(3): 219～228

18 V. S. Grigoryan, C. R. Menyuk, R.-M. Mu. Calculation of timing and amplitude jitter in dispersion-managed optical fiber communications using linearization[J]. *J. Lightwave Technol.*, 1999, **17**(8): 1347～1356

19 A. N. Pinto, G. P. Agrawal, J. Ferreira da Rocha. Effect of

soliton interaction on timing jitter in communication systems[J]. *J. Lightwave Technol.*, 1998, **16**(4): 515～519

20 Fang Junbin, Liao Changjun, Wei Zhengjun *et al*.. Influence of ultra-short laser pulse shapes on gate-mode single photon detection[J]. *Acta Photonica Sinica*, 2009, **38**(9): 2192～2195
方俊彬, 廖常俊, 魏正军 等. 超短光脉冲波形对门模单光子探测的影响[J]. 光子学报, 2009, **38**(9): 2192～2195

21 You Lixing, Shen Xiaofang. Shaping the response pulse of superconducting nanowire single photon detection with a snubber [J]. *Appl. Phys. Lett.*, 2009, **95**(15): 152514

22 You Lixing, Shen Xiaofang, Yang Xiaoyan. Single photon response of superconducting nanowire single photon detector[J]. *Chin. Sci. Bull.*, 2010, **55**(4-5): 441～445