连续变量量子密钥分发系统中同步方案及实验实现

申泽源 房 坚 何广强 曾贵华

(上海交通大学电子工程系,区域光纤通信网与新型光通信系统国家重点实验室,
北斗导航与位置服务上海市重点实验室,上海 200240)

摘要 基于连续变量量子密钥分发系统,提出了一种自发同步的方案。这种方案能有效地克服连续变量量子在光通信过程中受到环境因素的影响,实现连续变量量子密钥分发端和接收端系统之间的同步。从理论上介绍了这种同步方案的机制,并在连续变量量子密钥分发系统上对这种同步方案的可行性进行了验证。在实验所得数据的基础上分析了这种同步方案所需时间和成功率等关键性能指标。

关键词 光通信;自发同步;连续变量量子密钥分发系统;字符同步帧;握手帧

中图分类号 O431.2 **文献标识码** A **doi**: 10.3788/CJL201340.0305004

Synchronous Scheme and Experimental Realization in Continuous Variable Quautum Key Distribution System

Shen Zeyuan Fang Jian He Guangqiang Zeng Guihua

(*State Key Laboratory of Advanced Optical Communication Systems and Networks, Key Laboratory on Navigation and Location-Based Service, Department of Electronic Engineering, Shanghai Jiaotong University, Shanghai* 200240, *China*)

Abstract A method of spontaneous synchronization based on a continuous variable quantum key distribution (CV-QKD) system is proposed. This method can effectively overcome the disturbance effects which are generated by the environment in the transmission process of continuous variable quantum. The scheme realizes the synchronization between the sending terminal and the receiving tevminal. The mechanism of this synchronization scheme is introduced theoretically, and then the feasibility of this synchronization scheme is verified based on a continuous variable quantum key distribution system. Based on the experimental data, the key performance indicators for this synchronization scheme such as required time and successful probability are analyzed.

Key words optical communications; spontaneous synchronization; continuous variable quantum key distribution system; character synchronization frame; handshake frame

OCIS codes 060.5565; 060.4785; 060.2920; 060.5060

1 引 言

连续变量量子密钥分发(CV-QKD)近年来引起了学术界很大的关注[1~4],特别是在 Grosshans 等[5]提出了基于相干态高斯调制的连续变量量子密钥分发方案后,这种不涉及光场的非经典性质的量子密钥分发(QKD)方案具有极大的意义。该方案采用零差检测器来检测量子态,不需要使用单光子探测器。实验表明,在无损耗的量子信道上,密钥传输速率为 1.7 M/s;当信道损耗为 3.1 dB 时,密钥传输速率为 75 k/s。实验采用的量子信号是平均光子数为 250 个的相干光脉冲。由于相干光的产生比较容易,因此该实验方案的可重复性较高,也是目前

收稿日期: 2012-10-12; **收到修改稿日期**: 2012-11-07

基金项目: 国家自然科学基金(61170228、60970109 和 61102053)资助课题。

作者简介: 申泽源(1987—),男,硕士研究生,主要从事连续变量量子密钥分发方面的研究。
E-mail: zeyuanshen@126.com

导师简介: 曾贵华(1966—),男,教授,博士生导师,主要从事量子密码、量子光通信、编码与安全监控技术等方面的研究。
E-mail: ghzeng@sjtu.edu.cn(通信联系人)

各个研究机构重视和采用最多的一种方案[6,7]。基于相干态高斯调制的连续变量量子密钥分发的安全性证明相继被提出[8~11]，连续变量量子密钥分发也被越来越多的人认为是无条件安全的。无论是离散变量量子密钥分发还是连续变量量子密钥分发，探测器性能对系统整体的性能有着决定性作用，因而在探测器方面和密钥的随机性上，受到各个研究机构越来越多的重视[12~16]。

连续变量量子信号是由相干激光脉冲经过衰减后产生，基本上在1个相干光脉冲内，光子数小于250个。由于相干光脉冲衰减到了量子级别，在光通信过程中，特别容易受到环境和系统噪声的影响，例如温度、湿度的变化引入的小幅噪声，系统的电噪声、震动及实验周边的声音能带来更大的干扰。这些环境因素造成的影响主要作用在光脉冲相位上，使得光脉冲的相位变化速率是随机不定的。从通信的角度看，这些环境因素使得传输误码率大大地增加。然而，传统的强光通信中，这些问题对光通信系统的影响基本上可以忽略不计。传统的强光通信中两种同步方式——异步传输和同步传输，无论哪一种方式都是建立在误码率很小的基础上。这些传统的光通信方面的一系列协议、流程设计在连续变量量子密钥分发系统中并不实用，因此必须另辟蹊径，设计出一个符合连续变量量子传输特性的同步方案。

CV-QKD系统已经有了一个成熟的相位补偿方案来克服环境对系统的影响[17]，但任何一个相位补偿方案的前提是需要通信双方之间的载波同步、位同步(码元同步)、帧同步(群同步)等。从通信层面上来看，一个系统需要通信，必须实现同步，在连续变量量子密钥分发系统中，同步问题也是必须首要解决的问题。

本文主要研究了在连续变量量子密钥分发系统上同步实现的方案，简要介绍了相干态高斯协议量子密钥分发，提出了同步实现的理论方案，介绍了连续变量量子密钥分发系统，并在实验上验证同步方案，对其性能进行分析，简要总结了自发同步实现方案的意义。

2　相干态高斯协议QKD和同步实现的理论方案

2.1　相干态高斯协议QKD

在本文中，连续变量量子密钥发送端称为Alice，接收端称为Bob，以方便描述。

基于相干态高斯调制量子密钥分发协议描述如下：

1) Alice先准备好高斯分布的真随机数集合R_d。

2) Alice制备宏观相干态$|\phi_0\rangle$，然后通过光学元器件[一般来说是一个1∶99的光学分束器(BS)]将宏观相干态分成量子信号和本振信号。其中本振信号直接送给接收方，而量子信号需要进行高斯调制。

3) Alice根据随机数集合R_d中的元素，通过强度调制器与相位调制器对信号光的正则位置与正则动量进行编码，编码后的相干态为$|X_A+\mathrm{j}P_A\rangle$。

4) Alice已经将完成编码的相干态信号$|X_A+\mathrm{j}P_A\rangle$从Alice端传输到Bob，同样，本振光信号也要同时的传给Bob端，Bob采用平衡零差检测器来测量收到的量子信号的两个分量，选择性的测量$\langle X\rangle$或$\langle P\rangle$，舍弃那些没有经过测量的值。

5) 通过经典信道的协助，Alice和Bob两方共享了一串具有关联性的符号值。Alice和Bob分别对自己的符号串进行量化，得到相关比特串，并通过公开信道进行密钥协商和保密增强，最终得到量子密钥。

连续变量具体在物理上是指光场的复振幅的位置分量X和动量分量P，若Alice得到高斯随机数X,P后，那么通过坐标变化，得到幅度调制器的电压值A和相位调制器的需调制的角度值φ，变化公式如下：

$$A=\sqrt{X^2+P^2},\tag{1}$$

$$\varphi=\arctan\frac{P}{X}.\tag{2}$$

要使得连续变量量子密钥分发协议具体实现，第一步工作就需要通信系统之间的同步，然而由于量子级别的信号特别容易受到环境因素的干扰，传统的通信同步方案并不能在此利用，所以需要一个全新的同步实现方案来实现系统间的同步。

2.2　同步实现的理论方案

1) Alice产生一种特殊的比特串——字符同步帧，并在连续变量量子信号相位上进行调制。

2) Alice在量子信道上以固定的频率循环发送字符同步帧，并且通过经典信道告诉Bob字符同步帧的结构和发送重复频率。

3) Bob让零差检测器一直检测X分量上的投影，然后收集光脉冲数据。

4) Bob从光脉冲中取出携带的信息值——光

脉冲的峰值。

5) Bob 选定合适的门限值 Thr 来确定是否收到字符同步帧信号。当确认收到字符同步帧后，告诉 Alice。

6) Alice 收到 Bob 信号后，停止发送字符同步帧，发送另一种特殊的比特串——握手帧，然后开始密钥分发。

7) Bob 选定合适的判定值 T_{num} 来辨别是否收到握手同步帧。当确认收到握手帧后，开始进入密钥分发阶段。同步方案成功结束。

8) Bob 若在 T_1 时间之内一直没找到字符同步帧或者是握手帧，通信失败，对应的修改 T_{hr}，T_{num} 的值，重新开始。

方案提到的字符同步帧结构如图 1 所示，握手帧结构如图 2 所示。其中，V_1 表示的是 Alice 端中相位调制器件当调制光信号到 90°时所需的电压值。同步字符帧一共有 $10N_1$ 个点，每 N_1 个点作为 1 节，第一节中前 N_2 个点设计为 0、$+V_1$ 的交替数据，后面(N_1-N_2)个点的数据值为 0，即不加调制。后面 9 节数据值为 0。握手帧的数据个数为 $10N_1$，分为 10 节，每一节的数据个数是 N_1，第一节和第二节选用 0、$+V_1$ 的交替数据，即交替数据的个数为 $2N_1$，后面 8 节数据为 0。

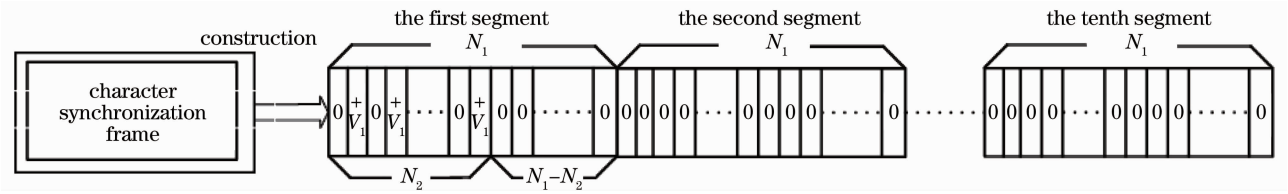

图 1 字符同步帧结构图

Fig. 1 Structure of character synchronization frame

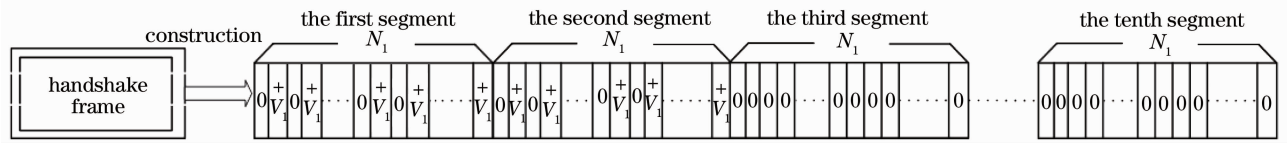

图 2 握手帧结构图

Fig. 2 Structure of handshake frame

在同步方案中门限值 T_{hr} 和判定值 T_{num} 的选取至关重要，门限值 T_{hr} 是用来判断是否为交替数组的标准，取值如下：

$$T_{hr} = |\alpha(V_3 - V_4)|, \tag{3}$$

其中 V_3、V_4 是对应接收端检测调制信号 0、$+V_1$ 时零差检测器的理想输出值。而 α 为系统噪声涨落水平，根据实际情况选取，$\alpha \in (0.15 \sim 0.6)$。

T_{num} 是用来辨别是否收到握手同步帧。判决值 T_{num} 取值如下：

$$T_{num} = \beta(2N_1), \tag{4}$$

式中 β 的取值与通信系统环境有关，$\beta \in (0.6 \sim 0.9)$。

在步骤 5) 中，Bob 选定 T_{hr} 值后，计算一帧里面连续的交替数据个数 n_1。如果 n_1 的值等于 N_2，那么就找到了字符的开始时刻，字符同步成功，通过经典信道向 Alice 发送帧同步成功信号。如果 n_1 的值不等于 N_2，那么继续计算下一个字符同步帧，直到字符同步成功为止，若在 T_1 时间之内一直都没找到，则进入步骤 8)。

在步骤 7) 中，Bob 选定 T_{num} 值后，计算一帧里面的交替数据个数 n_2。若 n_2 值大于等于 T_{num}，则确定此帧为标志帧，那么这帧结束后开始密钥分发。若 n_2 值小于 T_{num}，那么此帧不是标志帧，继续检测。若在 T_1 时间之内一直都没找到，则进入步骤 8)。

3 方案的实验验证和分析

3.1 连续变量量子密钥分发系统

连续变量量子密钥分发系统实验结构如图 3 所示，Alice 发送端光源部分是由两个激光器组成，一个激光器的中心波长是 1550 nm，用来生成本振光和连续变量量子信号。另一个激光器的中心波长是 1310 nm，用来传输系统基准时钟。1550 nm 波段激光脉冲经过放大器、滤波器和衰减器后进入 1∶99 的分束器，分束器分光比为 1 的那一路输出连续变量量子信号，传送到幅度调制器中进行振幅调制，然后信号脉冲将经过可调延迟线，为信号光一路增加长度，意味着信号光将比本振光延迟 40 ns，这样在后面的偏振分光棱镜(PBS)耦合时就利用了时分复用原理。信号光经过相位调制器进行相位调制，再通

过一个法拉第镜，法拉第镜将信号光脉冲的偏振偏转 90°，这样，信号光和本振光就产生了偏振隔离，可利用偏振复用在同一条光纤上传输，连续变量量子信号光和载波信号通过 PBS 合成一路信号。接着与1310 nm波段的基准时钟信号利用波分复用器耦合成一路光信号进入 25 km 传输光纤。

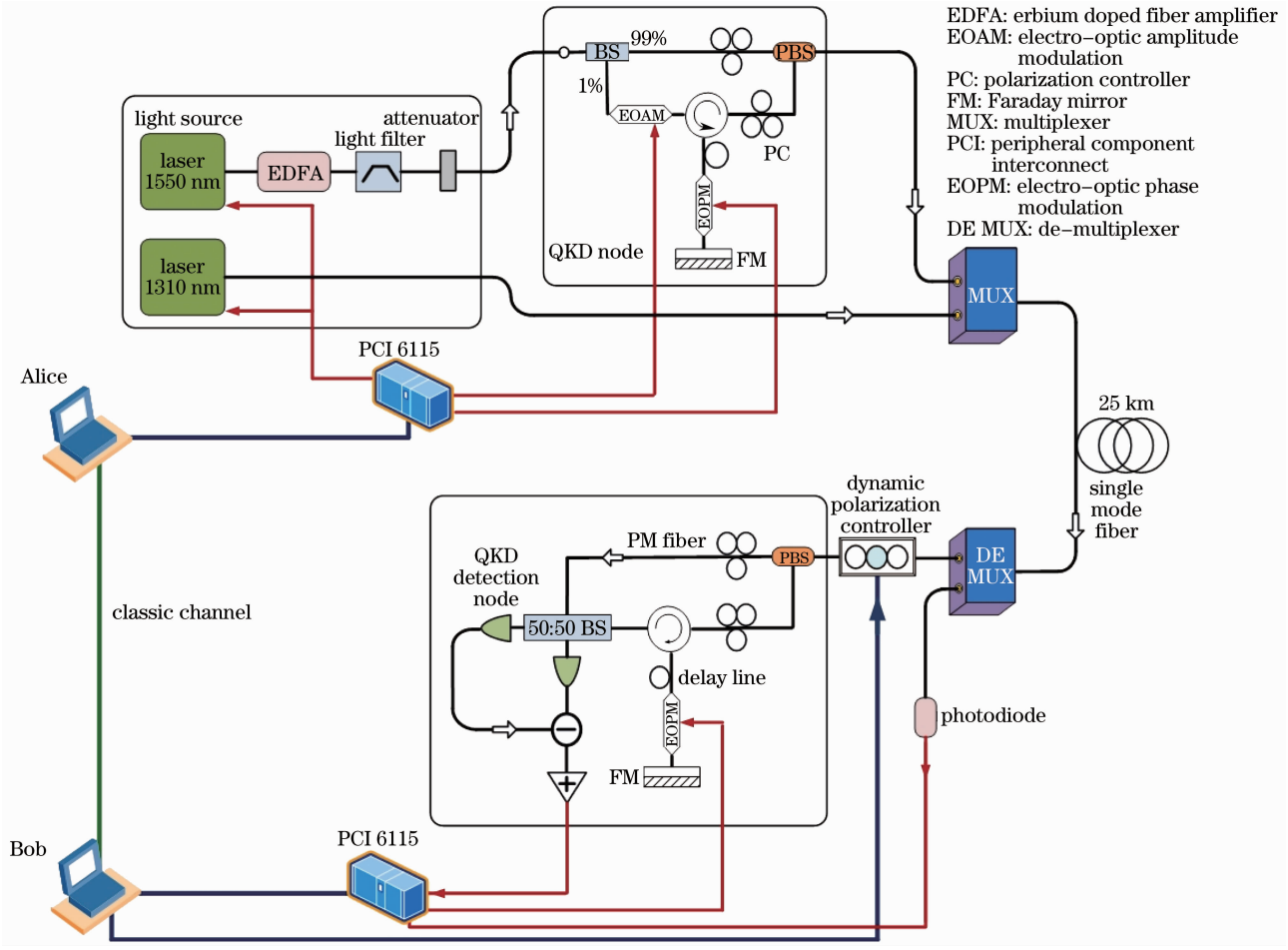

图 3　连续变量量子密钥分发系统实验结构图

Fig. 3　Experimental scheme of CV-QKD system

在 Bob 接收端，1310/1550 波分解复用器把两路波分复用耦合信号分开，1550 nm 波段的信号输入动态偏振控制器中，矫正在传输过程中产生的偏振偏移，然后输出到偏振分束器中，把载波信号和连续变量量子信号分开，载波信号通过延时光纤、相位调制器和法拉弟镜后与信号光在 50∶50 分束器处发生干涉，然后通过零差检测得到原始密钥。

系统的电路控制部分主要由 PCI6115 板卡完成，Alice 端的两个激光光源的触发时钟由 PCI6115 板卡发送的，振幅和相位调制器的调制信号也由板卡控制输出。电脑直接控制动态偏振器，Bob 端的偏振控制器由 PCI6115 板卡控制，零差检测器输出的模拟信号由 PCI6115 采集成数字信号输出到 Bob 端电脑中处理。

3.2　实验验证

同步方案具体实现措施：

1) Alice 端开始一直向相位调制器上加字符同步帧(如图 4 所示)。

2) Bob 端从零差检测输出中提取信号值[如图 5(a)所示]。

3) Bob 检测字符同步帧，当检测到后，字符同步帧指示灯亮，并向 Alice 端发送信号。

4) Alice 检测到 Bob 发送的信号后，发送握手帧，然后进去密钥分发阶段。

5) Bob 检测到握手帧后，指示灯亮，并且开始接受开始密钥分发[如图 5(b)所示]。

图 4(a)是 3 个字符同步帧在示波器上面的显示图；图 4(b)是字符同步帧第一节数据在示波器上的显示图。图 5(a)模拟采样监视器显示的是 Bob 端从零差检测器中接受的光脉冲数据；图 5(b)数据扫描样点监视器显示的是同步实现后密钥分发数据。

在实验验证中，实验环境：温度23.5 ℃，相对湿

度 40.8%。同步方案中参数设定为：$N_1=1000$，$N_2=1000$，$V_1=5$ V，$V_3=0$，$V_4=1$，$\alpha=0.2$，$\beta=0.675$。

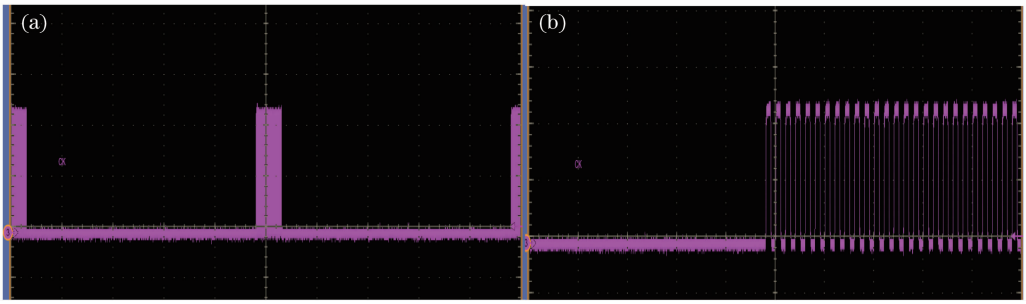

图 4 (a)字符同步帧信号；(b)放大第一节的显示图

Fig. 4 (a) Character synchronization frame signal on a oscilloscope; (b) amplified first section display

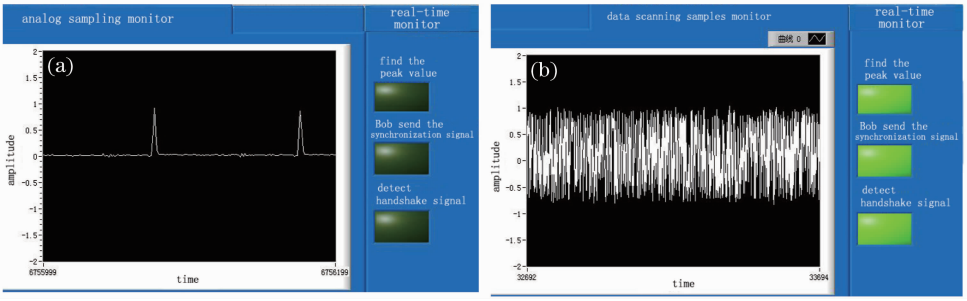

图 5 (a)零差检测器输出的光脉冲信号；(b)通过同步阶段后，原始密钥分发结果

Fig. 5 (a) Light pulse signal of homodyne detector; (b) results of original key distribution after the synchronization stage

3.3 同步方案性能分析

同步方案成功完成同步所需要的时间由检测出字符同步帧所用的时间决定的，同步方案成功率由检测出握手帧的概率决定的。

α 的不同选值(也就是不同门限值 T_{hr})，对于 Bob 端检测出字符同步帧所用的时间有着决定性的影响，如图 6 所示。

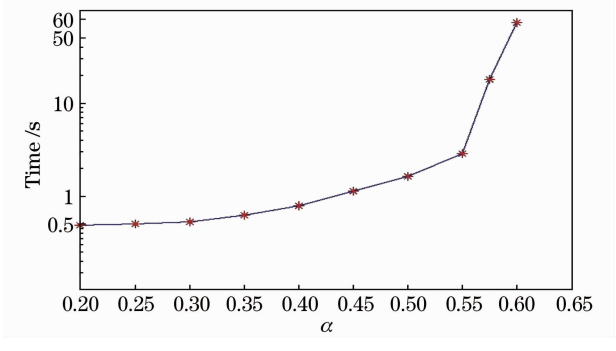

图 6 不同 α 值对应的找字符同步帧的时间

Fig. 6 Time of detecting the character synchronization frame signal corresponding to different values of α

图 6 中，每一个 α 值对应的所需时间是一个平均值，记录找到同步字符帧所需的时间并重复 100 次后求平均所得。可以看出，如果 α 的取值在0.2～0.4 之间，那么找到字符同步帧所需时间不会超过 1 s，当 α 取 0.6 时，所用时间激增到 74.126 s，α 取值再往上所需时间更多，以致于无法检测出字符同步帧。

α 的取值决定着同步方案所需要的时间，合适的 α 值可以使得同步所需时间不超过1 s。

不同的 β 值(不同的判决值 T_{num})对应的检测出握手帧的概率如图 7 所示。

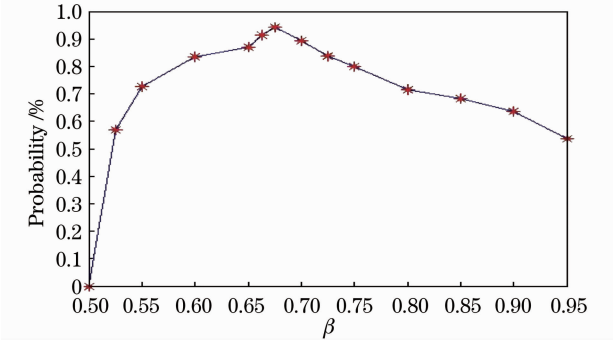

图 7 不同 β 值对应的检测出握手帧的概率

Fig. 7 Probability of detect the handshake frame signal corresponding to different values of β

图 7 中所有数据是在 α 取值 0.4 基础上测得的，从图中可以看出，当 β 取 0.675 时，可以得到最大的概率检测到握手帧 0.9456。如果 β 越接近 0.5 或者 1 时，那么检测出握手帧的概率就越小。这是因为环境等因素引入较大的误码率造成的，β 越接近 0.5 时，容易把字符同步帧当成握手帧，因此容易

判断错误，而 β 越接近 1 的时候，容易检测不到握手帧，从而系统超时，通信失败。β 的取值决定着同步方案成功率，合适的 β 值可以使得同步成功率超过 0.94。

上述讨论 β 的情况是基于 α 为 0.4 的前提下而言的。根据(3)式，α 取值决定了门限值 T_{hr} 的大小，T_{hr} 大小的选取会影响到步骤 7）中 n_2 的值。根据(4)式，β 的取值决定了判决值 T_{num} 的大小，而同步方案是否成功是看 n_2 的值是否大于 T_{num} 的值。因此，α 取值对于同步方案成功率有一定的影响，但不是决定性因素，β 的取值对同步方案成功率起着决定性影响。

在实验验证中，α 的取值在 0.2～0.45 之间，不同 β 值对应的检测出握手帧的概率于图 7 没有多大变化，但是当 α 的取值在 0.45～0.6 之间，不仅 β 值对应的检测出握手帧的概率大幅下降，而且同步所需时间过长，所以在讨论 β 的取值时仅仅考虑 α 取 0.4。

4　结　论

基于连续变量量子密钥分发系统，提出了一种自发同步系统方案，并且在实验上验证了同步实现方案的可行性。针对方案中的参数 α 和 β 对同步性能的影响做了具体的分析，发现合适的 α 和 β 的值可以使得同步方案具有极佳的性能。该同步方案能有效地克服光通信过程中连续变量量子受到环境的影响，对连续变量量子密钥分发系统的发展有着积极的推进作用。

参　考　文　献

1 Zeng Guihua. Quantum Cryptography [M]. Beijing: Science Press, 2006
曾贵华. 量子密码学[M]. 北京：科学出版社，2006

2 Zeng G. H.. Quantum Private Communication [M]. Berlin: Springer-Verlag, 2010

3 Cheng Lei, Lu Yuan, Zeng Guihua. Quantum key agreement development system on embedded Linux [J]. *Acta Sinica Quantum Optics*, 2010, **16**(1): 36～40
程　磊，陆　鸢，曾贵华. 嵌入式 Linux 环境下的量子密钥协商系统开发[J]. 量子光学学报，2010，**16**(1)：36～40

4 Leverrier A.. Continuous-variable quantum-key-distribution protocols with a non-Gaussian modulation[J]. *Phys. Rev. A*, 2011, **83**(4): 042312

5 F. Grosshans, G. Van Assche, J. Wenger *et al*.. Quantum key distribution using Gaussian-modulated coherent states [J]. *Nature*, 2003, **421**: 238～341

6 Weedbrook C., Lance A. M., Bowen W. P. *et al*.. Quantum cryptography without switching[J]. *Phys. Rev. Lett.*, 2004, **93**(17): 170504

7 Luo Hui. Zeng Guihua. System scheme of high-speed CV-QKD based on FPGA[J]. *Acta Sinica Quantum Optics*, 2012, **18**(1): 16～22
罗　辉，曾贵华. 基于 FPGA 的高速 CV-QKD 系统方案[J]. 量子光学学报，2012，**18**(1)：16～22

8 Grosshans F., Cerf N. J.. Continuous-variable quantum cryptography is secure against non-Gaussian attacks[J]. *Phys. Rev. Lett.*, 2004, **92**(4): 047905

9 Grosshans F.. Collective attacks and unconditional security in continuous variable quantum key distribution[J]. *Phys. Rev. Lett.*, 2005, **94**(2): 020504

10 Navascues M., Grosshans F., Acin A.. Optimality of Gaussian attacks in continuous-variable quantum cryptography[J]. *Phys. Rev. Lett.*, 2006, **97**(19): 190502

11 J. Sudjana, L. Magnin, R. García-Patrón *et al*.. Tight bounds on the eavesdropping of a continuous-variable quantum cryptographic protocol with no basis switching[J]. *Phys. Rev. A*, 2006, **76**(5): 052301

12 Wang Jinjing, Jia Xiaojun, Peng Kunchi. Improvement of balanced homodyne detector [J]. *Acta Optica Sinica*, 2012, **32**(1): 0127001
王金晶，贾晓军，彭堃墀. 平衡零拍探测器的改进[J]. 光学学报，2012，**32**(1)：0127001

13 Liang Xiaolei, Jiang Wenhao, Liu Jianhong *et al*.. A 1.25 GHz InGaAs/InP single-photon detector for high-speed quantum cryptography[J]. *Chinese J. Lasers*, 2012, **39**(8): 0818001
梁晓磊，蒋文浩，刘建宏 等. 用于高速量子密码系统的 1.25 GHz InGaAs/InP 单光子探测器的研制[J]. 中国激光，2012，**39**(8)：0818001

14 Lü Liang, Zhang Yinchao, Lin Yandong. Research on absolute calibration of photodetector quantum-efficiency using entangled photons[J]. *Acta Optica Sinica*, 2012, **32**(1): 0112004
吕　亮，张寅超，林延东. 纠缠光子法绝对定标光电探测器量子效率的研究[J]. 光学学报，2012，**32**(1)：0112004

15 Zhao Guhao, Zhao Shanghong, Yao Zhoushi *et al*.. Effect of the pulse broadening caused by atmosphere on satellite based quantum key distribution[J]. *Acta Optica Sinica*, 2012, **32**(11): 1127001
赵顾颢，赵尚弘，幺周石 等. 大气导致的脉冲展宽对星载量子密钥分发的影响[J]. 光学学报，2012，**32**(11)：1127001

16 Yan Qiurong, Zhao Baosheng, Liu Yongan *et al*.. Optical quantum random number generator based on the time randomness of single-photon pulse[J]. *Acta Optica Sinica*, 2012, **32**(3): 0327001
鄢秋荣，赵宝升，刘永安 等. 基于单光子脉冲时间随机性的光量子随机源[J]. 光学学报，2012，**32**(3)：0327001

17 Dai Wenchao, Lu Yuan, Zhu Jun *et al*.. An integrated quantum secure communication system [J]. *Science China Information Sciences*, 2011, **54**(12): 2578～2591

栏目编辑：李文喆