

# 高速连续变量量子密钥分发系统同步技术研究

刘友明<sup>1</sup> 汪超<sup>2</sup> 黄端<sup>2</sup> 黄鹏<sup>2</sup> 冯晓毅<sup>1</sup> 彭进业<sup>3</sup> 曹正文<sup>1,3</sup> 曾贵华<sup>2,3</sup>

<sup>1</sup>西北工业大学电子信息学院, 陕西 西安 710129

<sup>2</sup>区域光纤通信网与新型光通信系统国家重点实验室, 上海 200240

<sup>3</sup>西北大学电子信息学院, 陕西 西安 710127

**摘要** 在高速连续变量量子密钥分发系统中,位帧同步技术是确保准确获取量子信号所携带有效信息的核心技术之一。结合平衡零差探测器测量相干态的正则分量数据,提出了一种简单高效的位帧同步理论方案。基于此理论方案,在重复频率为25MHz的高斯调制相干态连续变量量子密钥分发系统上进行了实验测试和性能分析。结果表明,所提出的位帧同步方案能有效克服量子信号在密钥分发中受到的环境因素影响,有效实现通信双方同步。

**关键词** 光通信;同步;高速连续变量量子密钥分发;位帧同步;相干态高斯调制

中图分类号 O436

文献标识码 A

doi: 10.3788/AOS201535.0106006

## Study of Synchronous Technology in High-Speed Continuous Variable Quantum Key Distribution System

Liu Youming<sup>1</sup> Wang Chao<sup>2</sup> Huang Duan<sup>2</sup> Huang Peng<sup>2</sup> Feng Xiaoyi<sup>1</sup> Peng Jinye<sup>3</sup>  
Cao Zhengwen<sup>1,3</sup> Zeng Guihua<sup>2,3</sup>

<sup>1</sup>School of Electronic and Information, Northwestern Polytechnical University, Xi'an, Shaanxi 710129, China

<sup>2</sup>State Key Laboratory of Advanced Optical Communication Systems and Networks, Shanghai 200240, China

<sup>3</sup>School of Electronic and Information, Northwest University, Xi'an, Shaanxi 710127, China

**Abstract** In high-speed continuous-variable quantum key distribution system, frame synchronous technology is one of the most important technologies to ensure accurate access to effective information carried by quantum signals. A simple and efficient frame synchronization theoretical method based on the measurement results of the quadratures of coherent states with balanced homodyne detector is proposed. This synchronous method in the continuous-variable quantum key distribution system is experimentally realized with repetition frequency of 25 MHz based on Gaussian modulation coherent states, and the performance of the proposed synchronous method is analyzed in detail. The results show that the proposed frame synchronization method can effectively overcome the disturbance from the environmental factor in the key distribution of quantum signals, and thus realizes efficient frame synchronization between the two communicators.

**Key words** optical communications; synchronization; continuous-variable quantum key distribution; frame synchronization; Gaussian modulated coherent state

**OCIS codes** 060.5565; 060.4785; 060.2920; 060.5060

收稿日期: 2014-07-24; 收到修改稿日期: 2014-08-21

基金项目: 国家自然科学基金(61170228, 61332019)、陕西省教育自然科学基金(12JK0497)、陕西省科技厅自然科学基金(2013JM8036)、中国博士后科学基金(2013M540365)、上海交通大学博士后研究基金(AE606203)

作者简介: 刘友明(1988—),男,硕士研究生,主要从事连续变量量子密码分发系统控制技术方面的研究。

E-mail: liuyouming88@sina.com

导师简介: 冯晓毅(1969—),女,教授,博士生导师,主要从事量子光通信、数据采集与处理、编码与安全监控技术等方面的研究。E-mail: fengxiao@nwpu.edu.cn(通信联系人)

本文电子版彩色效果请详见中国光学期刊网 [www.opticsjournal.net](http://www.opticsjournal.net)

## 1 引 言

量子密钥分发能使合法通信双方在不可信任的量子信道中安全共享密钥。与离散变量量子密钥分发协议不同,连续变量量子密钥分发能将信息编码在连续量子变量(相干态的正则位移和正则动量)上且使用高效低成本的零差或外差平衡检测技术,这种摒弃了单光子技术且具有更高的密钥分发速率的连续变量量子密钥分发系统已受到了学术界的密切关注<sup>[1-5]</sup>。目前,已经提出了很多连续变量量子密钥分发协议并且从理论上进行了安全性分析,给出了个体攻击和联合攻击的安全门限,特别是基于高斯调制的相干态量子密钥分发协议的无条件安全性得到了充分论证<sup>[6-11]</sup>。不仅在理论上获得了重要进展,在实验上也受到了人们的极大关注,基于高斯调制的相干态量子密钥分发通过使用先进的检测技术<sup>[12-14]</sup>和纠错算法<sup>[15-16]</sup>,使得近十年来连续变量系统在实验实现方面取得了很大的进步<sup>[17-21]</sup>。到目前为止,连续变量量子密钥分发在实验环境下已经能够实现 80 km 的安全距离传输<sup>[21]</sup>。

不过,已有实验系统都是针对低速连续变量量子密钥分发而开展的,其生成的最终安全码率不高。在很多实际应用诸如视频文件加密、大数据文件加密等需要大量数据传输的数据加密系统中,通常需要高速密钥分发技术。因此,如何实现高速连续变量量子密钥分发系统成为亟待解决的问题。在高速连续变量量子密钥分发系统中,许多技术与以往的低速连续变量量子密钥分发技术不同。例如,在低速系统中所应用的同步技术<sup>[19,22]</sup>就无法有效地移植到高速系统中。在连续变量量子密钥分发系统中,同步技术是一项至关重要的核心技术,因为在连续变量量子密钥分发系统中要想正确提取出最终密钥,通信双方必须首先共享一串相关数据,即接收方收到的数据与发送方发送的数据必须一一对应。要达到上述目的,通信双方必须进行同步,从而使接收方能准确的界定出数据传输过程中有效数据的起始位置和终止位置。然而,与传统光纤通信系统不同,连续变量量子密钥分发系统中传输的是微弱的量子信号,极易受到外部环境的影响,如光纤抖动、外部机械振动、湿度和温度等,这些环境因素都会影响系统中传输信号的量子相干态。因此,连续变量量子密钥分发系统不能简单地使用传统光纤通信系统的同步方案,必须使用具有符合量子传输特性的同步方案。

对此,构建了一种简单高效的位帧同步方案。在该方案中,发送方首先生成一组特殊的数据作为同步帧,然后通过量子信道把携带同步帧的量子信号发送给接收方,接收方使用平衡零差检测器测量相干态的正则分量,通过选择适合的参数来搜寻同步帧,继而界定出有效数据的起始位置,实现通信双方同步。基于所提出的位帧同步方案,在重复频率为 25 MHz 的高速连续变量量子密钥分发系统中进行了实验测试以及性能分析。结果表明位帧同步方案能有效克服同步信号在量子密钥分发过程中来自外界环境因素的干扰,实现通信双方同步。

## 2 高斯调制相干态协议下的位帧同步方案

为了清楚地描述位帧同步方案,先简单介绍一下高斯调制相干态连续变量量子密钥分发协议。

### 2.1 高斯调制相干态协议

相干态的高斯调制协议是由 Grosshans 和 Grangier 于 2002 年首次提出的协议,俗称 GG02 协议。GG02 协议为连续变量量子密钥分发带来了很好的发展前景,因为协议中使用的相干态在现实生活中非常容易制备,并且经过近些年的理论研究,它被证明是无条件安全的协议。GG02 协议可以描述为

- 1) 发送方 Alice 生成两组独立且服从均值为 0, 方差为  $V_A$  的高斯真随机数  $X_A, P_A$ , 同时接收方 Bob 生成一组随机数  $B$ ;
- 2) Alice 通过量子信道把中心为  $(X_A, P_A)$  的相干态发送给 Bob;
- 3) Bob 根据生成的随机数  $B$ , 随机选择测量基测量相干态的  $X_B$  或  $P_B$ ;
- 4) 当测量完所有数据后, Bob 通过经典信道公布自己的测量基;
- 5) Alice 根据 Bob 的测量基丢弃无用的  $X_A$  或  $P_A$ , 此时 Alice 和 Bob 共享了一串相关的数据;
- 6) 通过协商和保密增强, Alice 和 Bob 共享一串完全相同的密钥。

在实际的连续变量量子密钥分发系统中, Alice 通过相位和幅度调制器随机调制光脉冲的相位  $\varphi$  和幅度  $A$ , 同样可以达到相干态的高斯调制, 它们的转换关系为

$$X_A = A \cos \varphi, \quad (1)$$

$$P_A = A \sin \varphi. \quad (2)$$

## 2.2 位帧同步方案描述

在高速连续变量量子密钥分配系统中,为了保证系统最终分发密钥的速率,降低软件层算法复杂度,所构造的同步帧结构应该满足以下准则:

- 1) 同步帧在整个数据中的比例越小越好,即开销越少越好;
- 2) 帧结构越简单越好;
- 3) 接收方易于识别。

基于上述准则,针对高速连续变量量子密钥分发系统的特点,提出了如下的位帧同步方案:

- 1) Alice生成一组特殊数据  $\varphi_A$  (同步帧);
- 2) Alice通过量子信道把中心为  $(A \cos \varphi_A, A \sin \varphi_A)$  的相干态发送给 Bob,同时,Alice通过经典信道把数据  $\varphi_A$  的结构信息告知 Bob;
- 3) Bob使用零差检测器测量相干态的位移分量  $X_B$ ;
- 4) 根据步骤1)从经典信道获得的数据  $\varphi_A$  的结构信息,Bob选定合适的阈值  $\alpha$  和参数  $\beta$  来判定同步帧;
- 5) 若在规定的时间内,Bob都没有搜寻到同步帧,则同步失败,此时 Bob需要调整  $\alpha$  和  $\beta$  的取值,然后重新通信。

下面详细解释所提出的位帧同步方案及其所涉及的物理过程。构造的同步帧结构如图1所示。

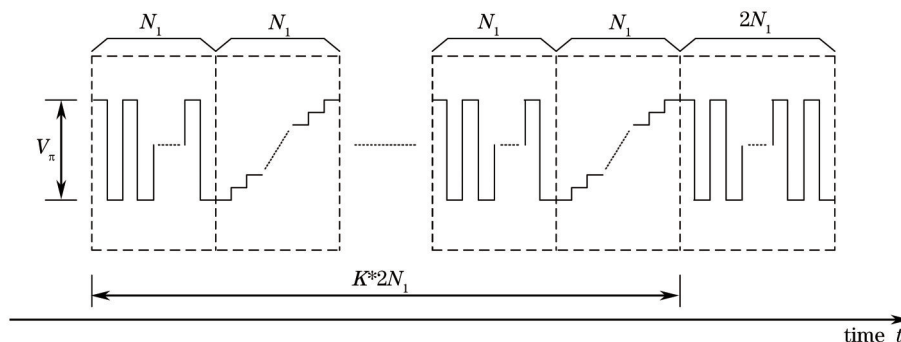


图1 构造的同步帧结构图

Fig.1 Structure of the proposed synchronization frame

所构造的同步帧包括两种类型:交替电压与阶梯电压。为了方便叙述,把同步帧分为两个部分:位同步段和帧同步段。其中,位同步段是由  $N_1$  个交替电压和  $N_1$  个阶梯电压构成,帧同步段是由  $2N_1$  个交替电压构成。实际通信过程中,Bob在知道同步帧结构的情况下对接收到的数据进行位同步段查找,当找到位同步段后,继而对帧同步段进行搜寻,当Bob成功找到帧同步段后,接下来就能准确的收到数据,从而实现了数据同步。由图1可知,构造的同步帧包含了  $K$  个位同步段和1个帧同步段。这是因为在实际系统运行中,由于各种环境因素如机械振动、温度以及湿度的影响,数据在底层物理层传输时会出现误码现象,为了尽可能地降低误码率让接收方Bob成功获取到同步帧,才把位同步段重复了  $K$  次。此时实现的具体算法为:Bob先寻找  $N_1$  个交替电压,紧接着寻找  $N_1$  个阶梯电压,如果当Bob寻找到的交替电压次数不够  $N_1$  或者阶梯电压的台阶数不够  $N_1$  时,则Bob重新寻找位同步段,若Bob寻找到了位同步段,则继续寻找帧同步段,如图2所示,假设Bob在左边的红色虚框里搜寻到了  $N_1$  个交替电压和  $N_1$  个阶梯电压后,Bob会以数量为  $2N_1$  的滑动窗口(图2红色窗口)向后查询帧同步段,直到当滑动窗口中出现交替电压的数目为  $N = \beta * 2N_1$  [步骤5)中提到的  $\beta$ ],则Bob找到了帧同步段,此时滑动窗口外的第一个数据即为有效的通信数据,同步功能实现。其中,参数  $\beta$  的取值范围为  $0.5 < \beta < 1$ 。这是由于底层物理线路的不可靠,  $2N_1$  个交替电压经光路传输后仍保持  $2N_1$  个交替特性的概率很小,若Bob还是以  $2N_1$  的交替电压为标准来衡量帧同步段的话,即  $\beta = 1$ ,Bob很有可能无法找到帧同步段,继而同步失败; $\beta$  取值大于0.5的原因是避免Bob把位同步段中的交替电压误当成帧同步段,造成同步失败。

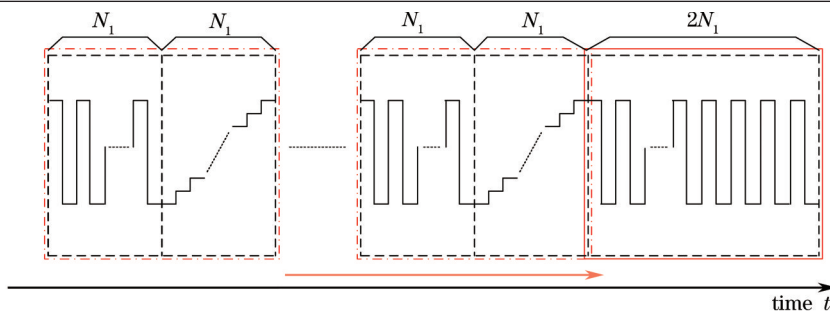


图2 搜寻帧同步段的示意图

Fig.2 Picture of searching frame synchronization

这里还需要说明的是,在图1同步帧结构中交替电压的差值和阶梯电压的最大值与最小值的差值均为  $V_\pi$ ,  $V_\pi$  是电光相位调制器的半波电压。在实际系统运行中,系统所用的交替电压用来调制脉冲光光场的相位,即把交替电压调制进脉冲光信号中,使得前后两个光脉冲信号的光场相位相差  $180^\circ$ , 这样可以让接收方 Bob 能够检测到差值很大的交替电压。

可以用二维相空间来描述这一过程,图3为相干量子态的二维相空间描述图,其中,坐标轴  $X$  和  $P$  分别代表了光场的正则位移和正则动量。假设  $a$  为脉冲光的初态,则态  $b$  和态  $c$  分别是态  $a$  经过电光相位调制器调制电压  $V_1$  和  $V_2$  后得到的态,它们的相位角相差  $180^\circ$ , 这里  $V_1 - V_2 = V_\pi$ , 即是构造同步帧的交替电压值。图3中  $x_1$  和  $x_2$  分别是态  $b$  和态  $c$  的正则位移分量,它们的绝对值都等于  $|x|$ 。此时 Bob 用零差检测器检测脉冲光的正则位移分量得到的电压值即为  $x_1$  和  $x_2$ , 刚好是易于判定的一正一负的高低电压值,然而,通信双方相距几十公里,由于外部环境的影响,系统会出现相位抖动现象。当 Alice 把初态  $a$  调制到图3中的态  $b$  和态  $c$  后,经过几十公里的光路达到 Bob, 此时 Bob 用检测器检测的相干态不一定是态  $b$  和态  $c$ , 而是态  $b'$  和态  $c'$ , 不过这两个态的相位差始终为  $180^\circ$ , 如图4所示。

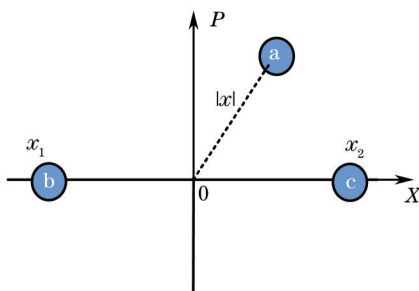


图3 量子态的二维相空间描述图

Fig.3 Two dimension phase space representation of quantum states

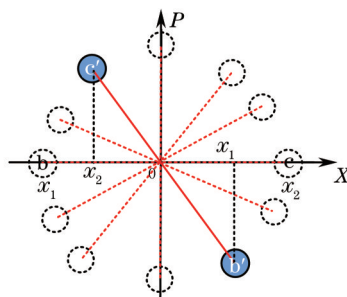


图4 Bob 收到的量子态的二维相空间图

Fig.4 Two dimension phase space representation of the detected quantum states by Bob

图4中各虚线圆圈的位置是 Bob 可能检测到的量子态,实线圆圈是假设的一种情况,此时检测器检测两个量子态的正则位移分量会得到  $x'_1$  和  $x'_2$ 。由此可知,假设 Alice 一直发送态  $b$  和态  $c$ , Bob 在不同时刻去检测量子态的正则位移分量会得到不同的值  $x'_1$  和  $x'_2$ , 其中包括  $x'_1 = x'_2 = 0$  的情况,即当 Alice 发送差值为  $V_\pi$  的交

替电压时, Bob用检测器检测得到的电压值不一定是差值最大( $2|x_1|$ )的交替电压, 甚至可能是一系列相等的值(在  $x_1' = x_2' = 0$  时)。所以, Alice把一串特殊的交替电压调制进光脉冲后, Bob很有可能检测不到这种交替结构或者电压差值很小的交替, 此时为了让 Bob尽可能地识别出 Alice发送的交替电压, 引入了参数  $\alpha$ , 只要 Bob检测到前后相邻电压差值  $\Delta V$  满足下列关系, 则 Bob认为自己检测到了这种交替结构, 关系如下:

$$\Delta V > \alpha \times 2|x_1|, \quad (3)$$

式中  $2|x_1| = |x_1 - x_2|$ ,  $\alpha$ 取值范围为  $0 < \alpha < 1$ 。

按照相同的思路, 构造的位同步段中的  $N_1$ 个阶梯电压, Alice通过电光相位调制器调制进脉冲光后, Bob经零差检测器检测后得到的是正余弦曲线, 相邻两个电压的差值很小, 小于 Bob设定的阈值  $\alpha \times 2|x_1|$ , 这样以来, Bob可以通过判定  $N_1$ 个相邻电压差值很小的电压来间接判断  $N_1$ 个阶梯电压, 简化了 Bob的软件算法。

### 3 位帧同步技术方案的实验实现

#### 3.1 连续变量量子密钥分发光路系统结构

在实验室已有的高速连续变量量子密钥分发光路系统上完成了上述位帧同步方案的实验验证与测试。高速连续变量量子密钥分发光路系统结构图如图5所示。Alice端有两个模块, 一个是用来产生信号光的光源模块, 一个是产生系统基准时钟信号的时钟模块。光源模块生成的脉冲光经过 1:99 的分束器(BS)分为量子信号光和本振光。分光比为 1 的光路输出量子信号, 经振幅调制器(AM)和相位调制器(PM)完成高斯随机数调制, 然后经偏振耦合器到达法拉第镜, 经法拉第镜使信号光的偏振旋转了  $90^\circ$ 再返回到偏振耦合器, 这条路径完成了两个操作: 量子信号光的传输延迟操作和偏振状态的改变, 这就可以让量子信号光与本振光通过时分复用和偏振复用在同一条光纤上传输。接着, 偏振耦合器的输出与时钟模块生成的时钟信号经波分复用器耦合进 30 km 的单模光纤中。

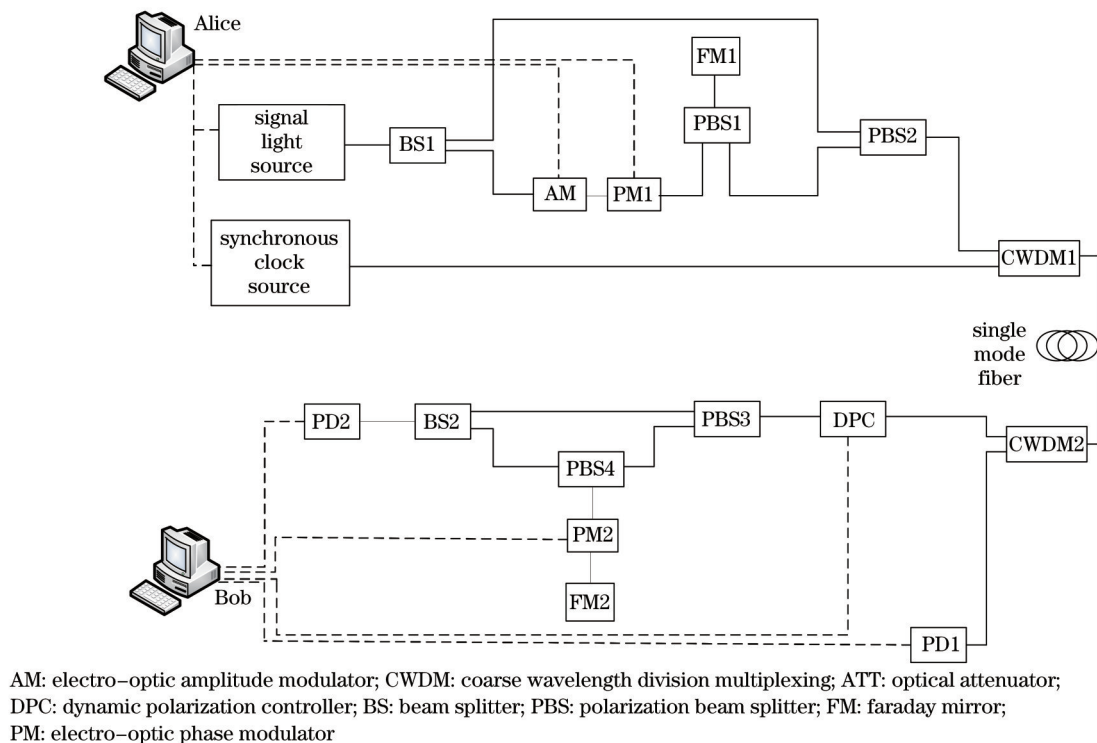


图5 量子密钥分发光路系统原理图

Fig.5 Schematic diagram of quantum key distribution optical system

Bob端用波分复用器逆复用得到信号光和时钟, 其中信号光经动态偏振控制器完成偏振态的补偿, 通过偏振分束器得到量子信号光和本振光, 本振光经 PM 和法拉第镜完成测量基选择和时间延迟, 使本振光与量子信号光的偏振态相同且能够同时到达分光比为 50:50 的 BS, 使其发生干涉。最后通过零差得到初始密

钥。图中的实线为光信号的传输路径,虚线为电信号的传输路径。

### 3.2 位帧同步技术方案实验验证

首先从实验的角度验证前面所提出的同步方案的可行性。所谓的同步就是通信双方的数据在通信过程中保持一定的相对关系,换句话说,Alice发出一串数据,经过信道传输给Bob,Bob能准确定位出数据串的起始位置并进行数据接收。因此,在测试方案中,制造了一种特殊的数据串,称之为测试数据。为了便于观测和分析,构造了一种简单的测试数据,数据量为2000的整数倍,其中每2000个数据中前1000个都为0,后1000个数据都为 $V_{\pi}$ (电光相位调制器的半波电压)。测试的系统光路为连续变量量子密钥分发系统光路,实验步骤如下:

- 1) Alice构造同步帧(图6)与一段测试数据(图7);
- 2) Alice把同步帧和测试数据调制进电光相位调制器中;
- 3) Bob使用零差检测器检测信号光的正则位移接收数据,包含同步帧(图8)和测试数据(图9)。

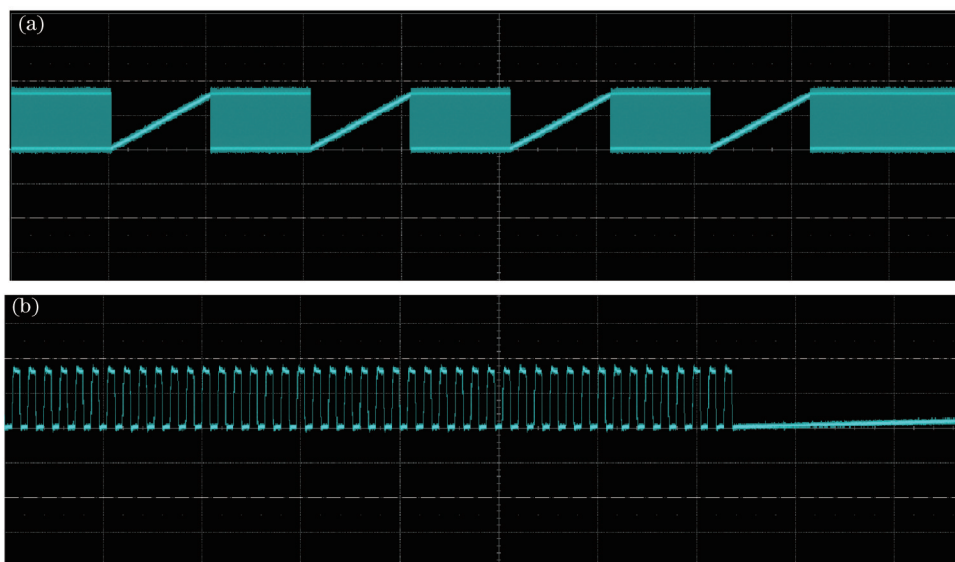


图6 (a) Alice构造的同步帧结构图;(b)局部放大位同步段显示图

Fig.6 (a) Structure of synchronization frame signal sent by Alice; (b) local-amplified synchronization frame signal display

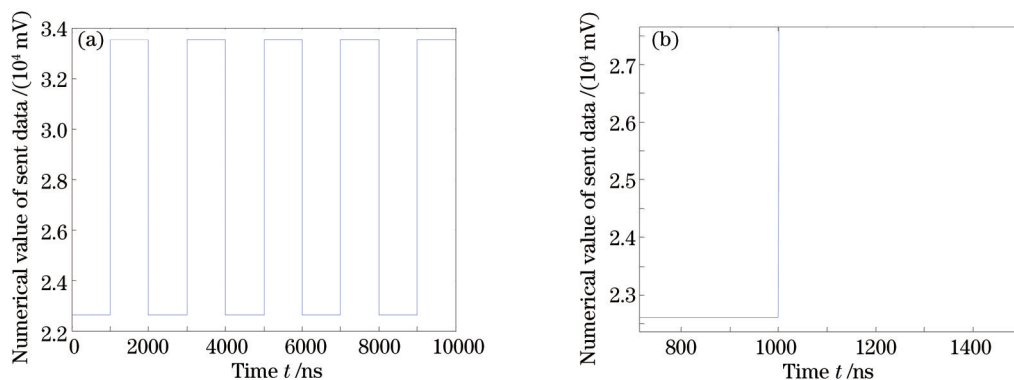


图7 (a) Alice构造的测试数据;(b)位置为1000附近的放大图

Fig.7 (a) Test data sent by Alice; (b) amplification image near 1000

图6(a)为Alice构造了位同步段为256个交替电压、256个阶梯电压和帧同步段为512个阶梯电压,以25 MHz的频率经数字模拟转换器(DA)推出,通过示波器观察到的原始同步帧结构。图6(b)为图6(a)中位同步段的放大图像。图7(a)为构造的测试数据,每一千个电压交替一次,交替电压的差值为 $V_{\pi}$ ,因为实际的模拟电压值是由DA推出得到的,所以图像中的纵坐标为模拟电压值所对应的数字值。图7(b)为位于1000附近的放大图像,目的是确认制造的测试数据是每1000交替一次。图8(a)为Alice把图5的同步帧调制进电光相位调制器,经过信

道传输到 Bob, Bob 检测器输出的波形图, 可以看到它就是 3.1 节提到的 Bob 检测到的位同步段为一段交替电压与一段正余弦曲线电压, 帧同步段为交替电压。图 8(b) 为放大图 8(a) 中交替电压部分, 其中白色虚线内的脉冲频率为 25 MHz。

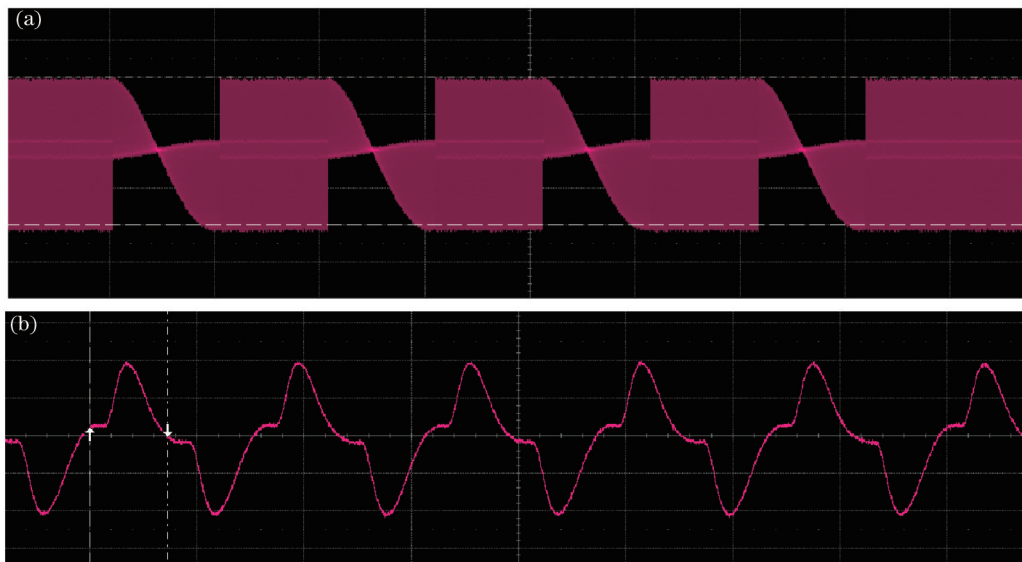


图 8 (a) Bob 检测到的数据图; (b) 放大交替电压显示图

Fig.8 (a) Data graph detected by Bob; (b) amplified alternate voltage signal display

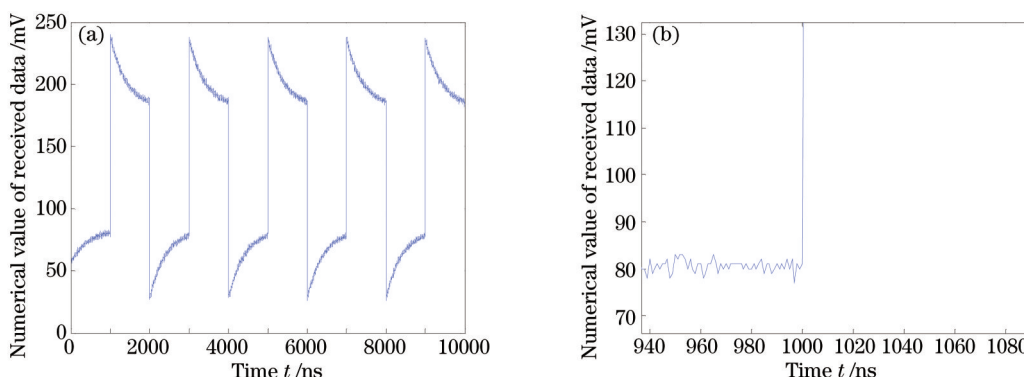


图 9 (a) Bob 接收到的测试数据; (b) 位置为 1000 附近的放大图

Fig.9 (a) Test data on received Bob; (b) amplification image near 1000

图 9(a) 为 Bob 使用所提出的同步方案收到的数据, 可以看到收到的数据也是呈周期性变化, 不过数据并不是像 Alice 构造的那样只有两个值 (0 和  $V_{\pi}$ ) 交替出现, 这是信道噪声导致的, 当然在实际的连续变量量子密钥分发系统中, 要对这种不理想的数据进行处理, 然而此时更注重同步方案的可行性, 对数据处理方面不做详细说明。图 9(b) 为位于 1000 附近的放大图像, 可以看到 Bob 收到的数据也是每 1000 点发送跳变, 这证明了提出的同步方案的可行性。

### 3.3 同步方案在实际系统中的实验测试及性能分析

结合相位补偿算法以及后处理反向协商低密度奇偶校验码 (LDPC) 算法, 运用高斯调制连续变量量子密钥分发协议在重复频率为 25 MHz 的高速连续变量量子密钥分发系统上, 成功的提取到最终密钥, 如图 10 所示。

图 10 中的协商监测窗口中显示的是系统密钥生成过程, 通信的数据量很大, 在后处理中把数据分成了很多 frame 来单独操作, success 为 1 表示对应的 frame 成功提取出密钥。实验中用到的参数: 系统重复频率为 25 MHz, 同步帧中  $N_1 = 256, K = 1000, \beta = 0.9, \alpha = 0.3$ 。以下对同步方案的性能进行详细分析。

同步方案的成功率是指通信双方能够成功同步的概率, 它的大小主要是由参数  $\alpha, \beta$  所决定。而同步所需要的理论时间  $t$  由参数  $K$  和  $N_1$  决定, 它们的关系可以表示为

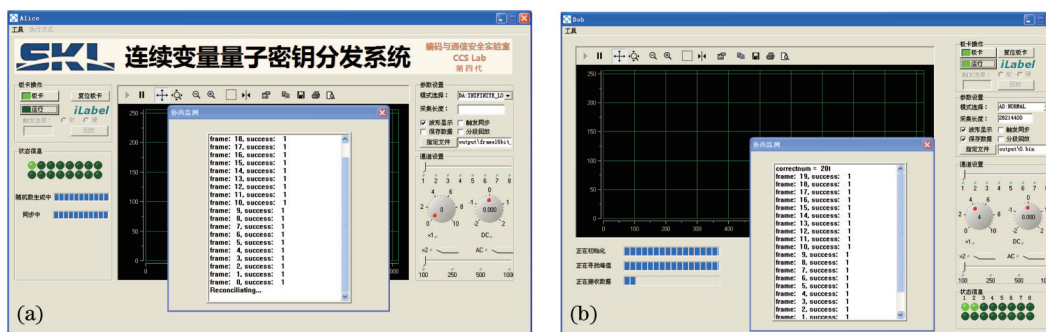


图 10 (a) Alice 成功提取密钥图; (b) Bob 成功提取密钥图

Fig.10 (a) Picture of successful extract secret key by Alice; (b) picture of successful extract secret key by Bob

$$t = \frac{2N_1(K+1)}{f}, \quad (4)$$

式中  $f$  为系统的重复频率,  $K$  为同步帧中位同步段的重复次数,  $N_1$  为位同步段中交替电压交替次数。同步所用参数的大小取值与实验具体所处环境以及所搭建的光路系统有关。在实验环境下, 为了得出  $\alpha$ 、 $\beta$  各自对同步的影响, 根据经验先取  $N_1 = 256, K = 1000$ 。

根据 1.2 节所阐述的同步原理, 可以知道  $\beta$  的取值范围为  $0.5 < \beta < 1$ , 在实验过程中, 首先取  $\beta = 0.75$ , 然后选取不同的  $\alpha$  值, 得出不同的  $\alpha$  值对应的同步成功率, 如图 11 所示。

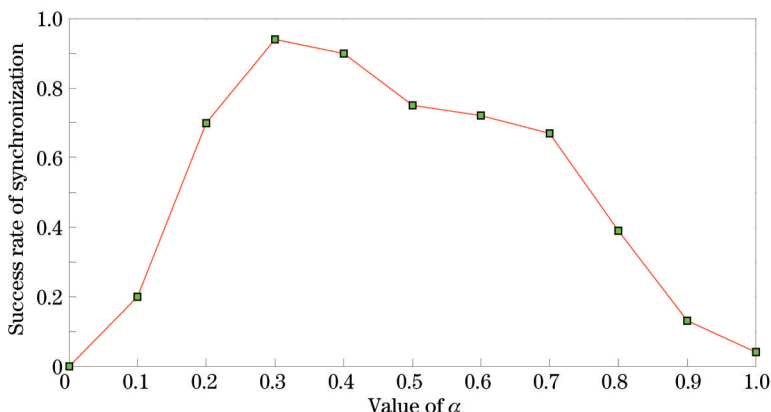


图 11 不同  $\alpha$  值对应的同步成功率

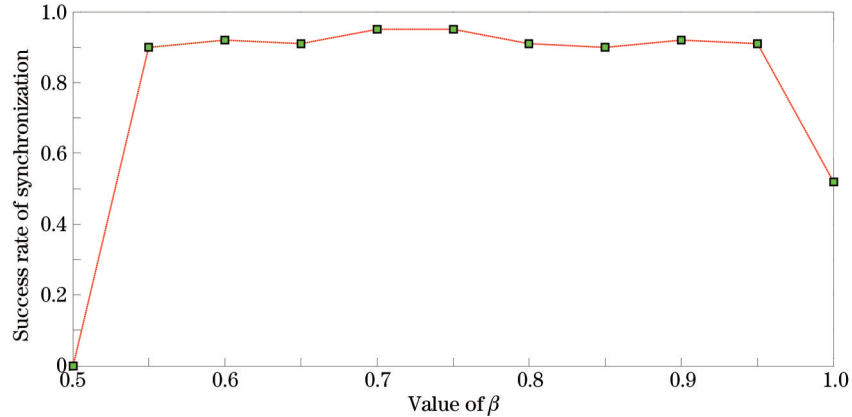
Fig.11 Success rate of synchronization corresponding to different values of  $\alpha$

对每个  $\alpha$  取值进行 100 次重复实验, 得到如图 11 所示概率曲线。从图中可以看到, 当  $\alpha = 0.3$  时, 在这 100 次实验中, 获得了 94 次同步成功的结果, 成功率达到实验中的最大值为 94%。如果  $\alpha$  的值越靠近 0 或者 1, 那么同步成功的概率越低。这是由于外部环境的影响, 系统出现相位漂移以及系统噪声引起误码导致  $\alpha$  取值过低或过高时, Bob 检测到满足 (3) 式的交替电压的概率降低, 甚至无法检测到。当  $\alpha$  的取值靠近 0 时, 由于  $\alpha$  过小,  $2\alpha|x|$  也就很小, 则 Bob 无法搜寻到阶梯电压的可能性增大, 从而导致同步成功率很低。当  $\alpha$  的取值靠近 1 时, 此时 Bob 判决交替电压的条件很苛刻, 就理想的无噪声的信道而言, 出现满足 (3) 式的交替电压的概率就不高, 所以此时同步成功率也就有所降低。当取  $\alpha = 0.3$ , 并选取不同的  $\beta$  值进行实验时, 得到了不同  $\beta$  值对应的同步成功率, 如图 12 所示。

同样, 图 12 是对每个  $\beta$  值进行 100 次重复实验而得出的图像。从图中可以看到, 除了  $\beta = 0.5$  和  $\beta = 1$  两种情况, 系统同步成功率均在 90% 以上。当  $\beta = 0.5$  时, Bob 会把位同步段的交替电压段误认为帧同步段, 导致同步失败, 实际上, Bob 能正确搜寻到帧同步段的概率是极低的。在实验中, 当  $\beta = 0.5$  时, 系统未出现同步成功的结果。当  $\beta = 1$  时, 系统同步成功率为 52%, 这是由于系统噪声的影响降低了 Bob 能够检测出交替次数为  $2N_1$  的帧同步段的概率。

由图 11 和图 12 可知, 影响同步成功率的主要因素为  $\alpha$ , 而  $\beta$  的大部分取值对同步的影响不大。上述实



图 12 不同  $\beta$  值对应的同步成功率Fig.12 Success rate of synchronization corresponding to different values of  $\beta$ 

验是在实验室环境下进行的,该环境相对稳定,如果在环境相对恶劣的情况下(如外场实验)进行实验,此时就需要考虑参数  $K$  和  $N_1$  对同步成功率的影响,因为不稳定的复杂环境可能会导致过大的噪声进而使系统在相对段的时间内无法找到位同步段,因此需要调整参数  $K$  和  $N_1$  来保证同步的成功率。在实验中,  $f=25$  MHz,  $N_1=256$ ,  $K=1000$ , 按照(4)式得到实验中的同步消耗时间为 21 ms。

## 4 结 论

结合平衡零差探测测量相干态的正则分量数据,提出了一种简单高效的位帧同步理论方案。在重复频率为 25 MHz 的高速连续变量量子密钥分发系统上对所提出的位帧同步方案进行了可行性实验验证。通过实验数据对位帧同步方案中的所有参数进行了实验分析,得出参数  $\alpha$  与  $\beta$  对同步成功率的影响,并且给出了同步所需的理论时间。所提出的同步方案能有效地克服量子信号受外界因素的影响,实现了量子密钥分发,并且其简单高效的特性适用于高速连续变量量子密钥分发系统中,对高速连续变量量子密钥分发系统的发展有着积极的作用。

## 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 G Zeng. Quantum Private Communication [M]. Berlin: Springer-Verlag, 2010.
- 3 F Grosshans, G Van Assche, J Wenger, *et al.*. Quantum key distribution using Gaussian-modulated coherent states [J]. Nature, 2003, 421(6920): 238-341.
- 4 F Grosshans, P Grangier. Continuous variable quantum cryptography using coherent states [J]. Phys Rev Lett, 2002, 88(5): 057902.
- 5 F Grosshans, N J Cerf, J Wenger, *et al.*. Virtual entanglement and reconciliation protocols for quantum cryptography with continuous variables [J]. Quantum Information and Computation, 2003.
- 6 F Grosshans. Collective attacks and unconditional security in continuous variable quantum key distribution [J]. Phys Rev Lett, 2005, 94(2): 020504.
- 7 M Navascués, A Acín. Security bounds for continuous variables quantum key distribution [J]. Phys Rev Lett, 2005, 94(2): 020505.
- 8 S Pirandola, R García-Patrón, S L Braunstein, *et al.*. Direct and reverse secret-key capacities of a quantum channel [J]. Phys Rev Lett, 2009, 102(5): 050503.
- 9 A Leverrier, E Karpov, P Grangier, *et al.*. Security of continuous-variable quantum key distribution: Towards a de Finetti theorem for rotation symmetry in phase space [J]. New Journal of Physics, 2009, 11(11): 115009.
- 10 P Jouguet, S Kunz-Jacques, E Diamanti, *et al.*. Analysis of imperfections in practical continuous-variable quantum key distribution [J]. Phys Rev A, 2012, 86(3): 032309.
- 11 P Huang, G Q He, G H Zeng. Bound on noise of coherent source for secure continuous-variable quantum key distribution [J]. International Journal of Theoretical Physics, 2013, 52(5): 1572-1582.

- 12 H Duan, F Jian, W Chao, *et al.*. A 300-MHz bandwidth balanced homodyne detector for continuous variable quantum key distribution [J]. *Chinese Phys Lett*, 2013, 30(11): 114209.
- 13 Guo Xueshi, Gao Kang, Liu Nannan, *et al.*. Differential detection system for measuring the quantum noise of pulsed light [J]. *Acta Optica Sinica*, 2013, 33(9): 0927002.  
郭学石, 高亢, 刘楠楠, 等. 适用于测量脉冲光量子噪声的差分探测系统[J]. *光学学报*, 2013, 33(9): 0927002.
- 14 Zheng Gongjue, Dai Dapeng, Fang Yinfei, *et al.*. Balanced homodyne detector based on two-stage amplification [J]. *Laser & Optoelectronics Progress*, 2014, 51(4): 040401.  
郑公爵, 戴大鹏, 方银飞, 等. 具有两级放大的平衡零拍光电探测器[J]. *激光与光电子学进展*, 2014, 51(4): 040401.
- 15 P Jouguet, S Kunz-Jacques. High performance error correction for quantum key distribution using polar codes [J]. *Quantum Information & Computation*, 2014, 14(3-4): 329-338.
- 16 Guo Dabo, Zhang Yanhuang, Wang Yunyan. Performance optimization for the reconciliation of Gaussian quantum key distribution [J]. *Acta Optica Sinica*, 2014, 34(1): 0127001.  
郭大波, 张彦煌, 王云艳. 高斯量子密钥分发数据协调的性能优化[J]. *光学学报*, 2014, 34(1): 0127001.
- 17 J Lodewyck, M Bloch, R García-Patrón, *et al.*. Quantum key distribution over 25 km with an all-fiber continuous-variable system [J]. *Phys Rev A*, 2007, 76(4): 042305.
- 18 S Fossier, E Diamanti, T Debuisschert, *et al.*. Field test of a continuous-variable quantum key distribution prototype [J]. *New Journal of Physics*, 2009, 11(4): 045023.
- 19 W C Dai, Y Lu, J Zhu, *et al.*. An integrated quantum secure communication system [J]. *Science China Information Sciences*, 2011, 54(12): 2578-2591.
- 20 P Jouguet, S Kunz-Jacques, T Debuisschert, *et al.*. Field test of classical symmetric encryption with continuous variables quantum key distribution [J]. *Opt Express*, 2012, 20(13): 14030-14041.
- 21 P Jouguet, S Kunz-Jacques, A Leverrier, *et al.*. Experimental demonstration of long-distance continuous-variable quantum key distribution [J]. *Nat Photonics*, 2013, 7(5): 378-381.
- 22 Shen Zeyuan, Fang Jian, He Guangqiang, *et al.*. Synchronous scheme and experimental realization in CV-QKD system [J]. *Chinese J Lasers*, 2013, 40(3): 0305004.  
申泽源, 房坚, 何广强, 等. 连续变量量子密钥分发系统中同步方案及实验实现 [J]. *中国激光*, 2013, 40(3): 0305004.

栏目编辑: 苏岑