

星地量子密钥分发中的时间同步研究

任继刚¹, 印娟², 杨彬², 周飞¹, 易震环¹,
彭承志¹, 舒嵘³, 王建宇³

(1. 清华大学 物理系, 北京 100084; 2. 中国科学技术大学 微尺度物质科学国家实验室, 安徽 合肥 230027;
3. 中国科学院上海技术物理研究所, 上海 200083)

摘要:高精度的时间同步是星地量子密钥分发实验的关键. 给出了一种新型的时间同步方案, 该方案采用与量子信号光共光路的同步光脉冲, 采用单光子探测器对同步光脉冲进行探测, 通过基于时间标记型高精度时间测量插件对信号事例和同步事例进行精确的时间测量. 解决了星地量子密钥分发实验中星上同步光对卫星平台载荷和资源要求较高及同步光与量子信号光的隔离问题. 系统成功应用于 16 km 自由空间量子密钥分发实验中, 并达到 1.023 ns(1σ)的全系统时间同步精度, 量子密钥分发原始码成码率为 8.27 kHz.

关键词:量子密钥分发; 时间同步; 时间标志型 TDC

中图分类号: TN247 文献标识码: A

Time synchronization for quantum key distribution from ground to satellite

REN Ji-Gang¹, YIN Juan², YANG Bin², ZHOU Fei¹, YI Zhen-Huan¹,
PENG Cheng-Zhi¹, SHU Rong³, WANG Jian-Yu³

(1. Department of Physics, TsingHua University, Beijing 100084, China;

2. National Laboratory for Physical Sciences at Microscale, University of Science and Technology of China, Hefei, Anhui 230027, China;

3. Shanghai Institute of Technical Physics, Chinese Academy of Sciences, Shanghai 200083, China)

Abstract: High-resolution time synchronization is the crucial technology of quantum key distribution experiment from ground to satellite. A new scheme of time synchronization was presented. In this scheme, a synchronous pulse which has the same wavelength with the quantum signal was adopted and single photo detector was used to detect the synchronous pulse. High-resolution time measurement module was used to measure the instance of synchronous pulse and signal pulse. This scheme overcomes the problem that the synchronization laser requires much more resources of satellite and the isolation between the synchronization pulse and quantum single pulse. This system was successfully applied to the 16 km quantum key distribution in free space channel. Synchronous resolution of the system is 1.023 ns and bit rate of the raw key for the quantum key distribution is 8.27 kHz.

Key words: quantum key distribution; time synchronization; time stamp TDC

PACS: 03.67.Dd

引言

1984年 Bennett 和 Brassard 提出了量子密钥分发的概念(BB84 协议)^[1]. 利用单光子不可分割、不可克隆原理, 使用单光子量子态作为信息传递的载体, 通信双方之间可以建立相同的随机数序列, 外界

的窃听行为将会导致随机数序列误码率发生变化, 从而暴露窃听行为. 量子密钥分发为人们提供了一种能够从物理原理上^[2] 保证绝对安全的密钥分发方式, 尤其是星地量子密钥通信过程, 利用卫星平台中转, 可以有效地克服地面光纤信号与自由空间量子密钥分发^[3-5] 的距离限制, 成为实现覆盖全球量子

通信网络最切实可行的方案之一^[6].

量子密钥分发过程的目标就是利用单光子量子态作为信息载体,在相距遥远的两点间建立相同的随机数序列.为此如何准确判断接收到的单光子信号在发射单光子信号序列中的位置成为实现量子密钥分发过程的关键.时间同步技术正是为了解决这一问题而提出来的.

提出了一种用于星地量子密钥分发实验的时间同步方案,采用以量子信号共光路的小功率同步光,在接收端采用多个单光子探测器同时响应的方式分辨信号光与同步光,利用基于时间标志型时间测量插件进行高精度时间测量,从而实现高精度时间同步.该方案在地面 16 km 量子密钥分发实验中进行测试,达到了 1.023 ns 的时间同步精度.

1 星地量子密钥分发系统和时间同步原理

星地量子密钥分发系统如图 1 所示.星地量子密钥分发基本过程为:量子信源以一定重复频率随机发送处于水平偏振、竖直偏振、+45 度偏振、-45 度偏振四种状态的单光子光脉冲(规定光子处于竖直偏振与 +45 度偏振代表 1,水平偏振与 -45 度偏振代表 0).量子信号光脉冲经过自由空间量子信道传输后到达卫星接收端,接收端采用单光子探测器进行量子测量,测量时随机选择水平竖直基矢或 45 度基矢,记下所测的结果和所选的基矢.当传送了足够数量的光子比特之后,通信双方在经典通道上讨论测量时用的是哪组基,有 50% 的机会 Alice 和 Bob 所选的基不兼容,将不兼容基的结果全部扔掉.对于剩下的比特,在没有干扰的情况下, Alice 和 Bob 所得的结果应该完全相同.

由以上过程可见,完成量子密钥分发最重要的一步就是将接收端测量到的信号与发射端发射的原始数据进行基矢比对.由于量子信号处于单光子水平,在星地高损耗量子信道中传输,在接收端只能以很小

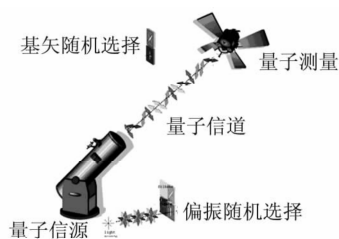


图 1 星地量子密钥分发系统示意图

Fig. 1 Diagram of the quantum key distribution from ground to satellite

的概率测量到量子信号,如何将探测到的这一小部分信号状态与发射端原始发射的状态一一对应起来就需要高精度的卫星轨道预报与时间同步系统.

时间同步系统除了能够完成发射段发射信号与接收端探测信号之间时序上的对准外,同时高精度的时间同步对于提高系统成码率、降低误码率也有重要的作用.

系统总误码率 ε 是指考虑到信源、信道、探测等各种不完美因素后的总误码率

$$\varepsilon = \varepsilon_s + \varepsilon_m + \varepsilon_q + \frac{A_N}{2(A_s + A_N)}, \quad (1)$$

其中 A_s 为量子信号增益(信道总传输效率),是指每 1bit 量子信号被量子测量系统所探测到的概率; A_N 为暗计数增益,是指系统各种背景光等造成的暗计数在测量系统上引发误计数的概率,考虑到系统时间分辨精度,位于分辨窗口外的暗计数将会被抛弃,不会引发误计数. A_N 的表达式为

$$A_N = (N_q + N_d)\Delta T. \quad (2)$$

从上面的推导来看,除了时间同步精度外,量子密钥分发中密钥的误码率主要和系统总暗计数及信道总传输效率相关,图 2 是在信道衰减 50 dB 的情况下,系统时间同步精度取 1 ns、5 ns 和 10 ns 时,系统误码率与系统总暗计数的水平关系图.

由上图可知,对于星地量子链路,信道总效率在 40 ~ 60 dB 之间,要实现 100 MHz 重复频率量子信号光发射,量子密钥误码率小于 10%,对时间同步精度的要求需在 ns 量级.

2 新型高精度时间同步方案

为了能够解决外同步方案中同步激光对卫星平台载荷要求较高以及同步光干扰量子信道的问题,提出了一种用于星地量子密钥分发实验的新型同步

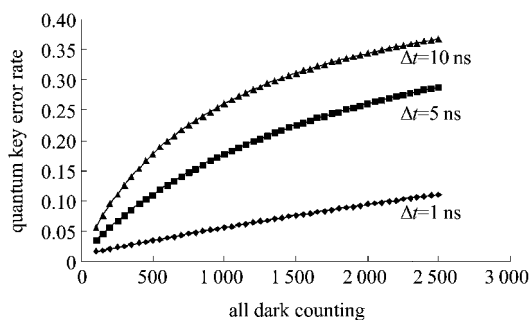


图 2 不同时间同步精度下量子密钥误码率与系统总暗计数关系图

Fig. 2 Diagram of the quantum key error rate vs. all dark counting under different time synchronization resolution

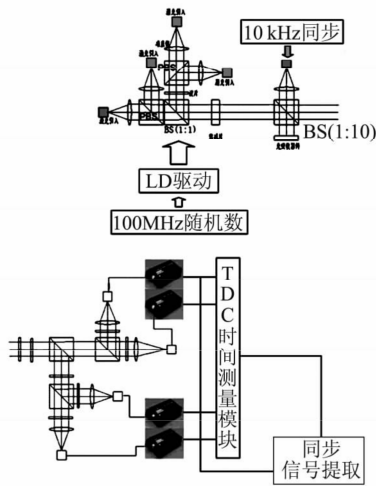


图3 量子密钥分发时间同步方案示意图
Fig.3 Time synchronization scheme of quantum key distribution

方案,如图3所示。

在发射端以一定重复频率(如100 MHz)随机驱动四个LD激光二极管发光产生量子信号;同时引入重复频率10 kHz的同步信号用于同步光LD激光二极管,量子信号光经衰减后处于单光子水平,而同步光脉冲不经衰减;同步光与量子信号光耦合至同一光路发射。

在接收端将同步光与量子信号光由单光子探测器进行探测,单光子探测器探测到的光子信号经甄别后需对其时间信息进行精确测量。目前高精度时间测量的方法有很多,如基于TDC-GP1芯片时间测量^[6]及基于TDC-GPX芯片时间测量^[7],本方案中采用时间标志型(time stamp)时间测量插件^[8](TDC,time-to-digital converter)。

2.1 同步信号的提取

接收端单光子探测到的事例中包含三个部分,信号光引起的触发、时间同步光引起的触发以及背景光等引起的暗计数。要完成时间同步过程,首先需要将同步信号提取出来。由于量子信号光在发射端发出时处于单光子水平,到达接收端后只会引起单个探测器响应,而时间同步光在发射端发射时每脉冲包含多个光子,到达接收端后将会有一定的概率引起多个探测器同时响应。背景光等因素造成的暗计数处于随机分布,同时在多个探测器上出现暗计数的概率很小,因此只需接收端任意两个单光子探测器在时间窗口内同时相应,那么该输出信号可以判断为时间同步信号。通过这样的方法,在接收端可以很容易区分量子光脉冲和同步光脉冲,探测到时间同步信号的位置将不再记入量子测量结果,解决

了同步光与信号光相互干扰的问题。

2.2 时基序列的恢复

由于接收端对时间同步信号的测量只是概率性测量,因此会有相当一部分时间无法被探测到同步信号,这样根据测量得到的时基序列并不是完整的,我们需要通过软件方法将时基序列恢复。

对于星地量子密钥分发实验,近地面卫星每秒的高度变化小于100 μs,同步光脉冲以10 kHz的重复频率发射,相邻两个时间同步光脉冲之间的间隔固定为100 μs,在这个时间间隔内接收端同步光脉冲间隔变化小于10 ns,因此假如某同步脉冲丢失,那么仅利用量子信号光参照其相邻同步脉冲(即相对此前最后一个同步光或此后第一个同步光)的时间间隔,来确定量子信息的随机数序列即可,就相当于恢复了该同步光信号。而在同步光连续丢失很多的情况下,为保证同步精度可以直接抛弃这段数据。

2.3 时间同步过程

发射端量子信号的时序以及与同步光的相对时序由驱动模块记录;在接收端由TDC时间测量模块测量接收信号的时间信息,量子信号的探测结果作为信号事例,同步信号的探测结果作为时基事例。

信号事例与时基事例的时序关系如图4所示。计算接收端的每一个信号事例相对于时基事例的时间间隔 $T = \frac{T_p}{T_i} \times \bar{T}_i$,其中 T_p 为信号事例距离上一个时基事例的时间间隔, T_i 为下一个时基事例与上一个时基事例之间的时间间隔, \bar{T}_i 为时基事例的平均时间间隔,程序设计中设置为一个固定值100 μs。将这个时间间隔除以标准时间间隔10 ns,如果所得余数在设定的符合窗口内,即判定为真实量子信号,并通过计算结果找到发射端相应的脉冲序列。

3 测试结果

时间测量插件的时间测量精度直接影响全系统时间同步精度,所用的时间测量插件由中国科学技

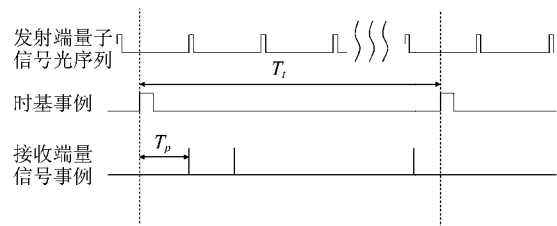


图4 信号事例的时间信息
Fig.4 Time information of quantum signal and synchronization signal

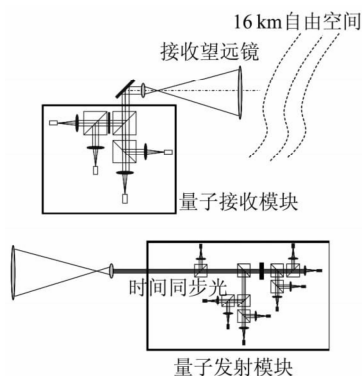


图5 16km 自由空间量子密钥分发示意图
Fig.5 Diagram of the 16km quantum key distribution in free space channel

术大学快电子学实验室提供,其时间测量精度可达到 100 ps.

将这种新型时间同步方案应用于 16 km 自由空间量子密钥分发实验中,对该方案所能达到的时间精度进行了测量,并验证了该方案在未来星地量子密钥分发实验中应用的可行性.实验装置如图 5 所示.

实验中发射端量子信源重复频率为 100 MHz,发射端的时间序列由 100 M 系统时钟精度保证,在接收端用 TDC 记录量子信息时刻和同步脉冲时刻,计算每个量子信号与相邻两个内同步信号之间的时间间隔,以相邻同步信号间隔 100 μ s 作归一化,将所得归一化相对时间间隔对 10 ns(量子信号时间间隔)取余并作统计,得出全系统的同步方差.

图 6 为全系统时间同步测量结果,其中纵坐标为计数值,横坐标为时间间隔(单位为 ns),从图中我们可以看出,目前时间同步的精度可以达到 1.023 ns(1σ),其中包括 TDC 测量精度 160 ps,单光子探测器的时间晃动 400 ps,以及同步光脉冲驱动以及电子学甄别系统所带来的全部时间误差.

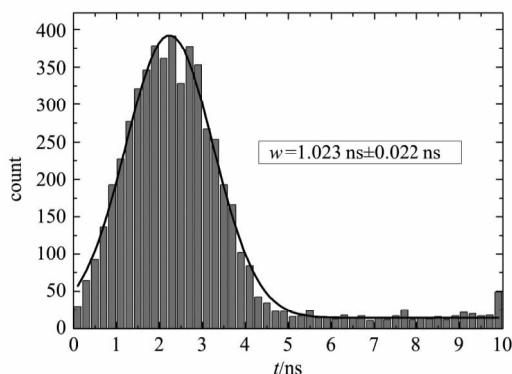


图6 时间同步精度示意图
Fig.6 Diagram of the time synchronous resolution

通过这套时间同步系统,我们在 16 km 自由空间信道中成功实现了量子密钥分发实验.下面给出一组典型实验结果,信源重复频率 100 MHz,信道损耗约 40 dB,实验时间 113.06 s,获得 1909782 个有效事例,经过基矢比对后得到原始码总量为 934577,误码率 3.56%.

4 结论

给出了一种可用于星地量子密钥分发实验的高精度时间同步方法.采用与量子信号同光路的小功率同步光脉冲在通信双方建立时序序列,采用基于时间标记型高精度时间测量插件(TDC)进行时间测量,有效解决了以往同步方案中星上载荷大功率激光器占用较多载荷资源以及时间同步光与量子信号之间的隔离问题.系统成功地应用于 16 km 自由空间量子密钥分发实验中,取得了 1.023 ns 的时间同步精度,量子密钥分发原始码成码率为 8.27 kHz,误码率为 3.56%,验证了该方案在未来星地量子密钥分发实验中的可行性.

REFERENCES

- [1] Bennett C H, Brassard G. Quantum cryptography: public key distribution and coin tossing [C]. In Proceeding of the IEEE International Conference on Computer, Systems and Signal Processing. 1984, 175 - 179.
- [2] Wootters W K, and Zurek W H, A single quantum cannot be cloned [J]. *Nature*, 1982, **299**: 802 - 803.
- [3] PENG C Z, ZHANG J, YANG D, *et al.* Experimental long-distance decoy-state quantum key distribution based on polarization encoding [J]. *Phys. Rev. Lett.*, 2007, **98**: 010505.
- [4] Schmitt-Manderbach T, Weier H, Furst M, *et al.* Experimental demonstration of free-space decoy-state quantum key distribution over 144km [J]. *Phys. Rev. Lett.*, 2007, **98** (1): 010504.
- [5] Rosenberg D J, Harrington W, Rice P R, *et al.* Long-distance decoy-state quantum key distribution in optical fiber [J]. *Phys. Rev. Lett.* 2007, **98** (1), 010503.
- [6] WU Gang, LI Chun-Lai, LIU Yin-Nian, *et al.* Study on high resolution time interval measurement module in pulsed laser ranging system [J]. *J. Infrared Millim. Waves* (吴刚, 李春来, 刘银年, 等. 脉冲激光测距系统中高精度时间间隔测量模块的研究. *红外与毫米波学报*), 2007, **26** (3): 213 - 216.
- [7] ZHU Lei, Huang Geng-Hua, OUYANG Jun-Hua, *et al.* Study on time interval measurement system in photon counting imaging lidar [J]. *J. Infrared Millim Waves* (朱磊, 黄庚华, 欧阳俊华, 等. 光子数成像激光雷达时间间隔测量系统研究. *红外与毫米波学报*), 2008, **27** (6): 461 - 464.
- [8] Song J, An Q, Liu S B. A high-resolution time-to-digital converter implemented in field-programmable-gate-arrays [J]. *IEEE Transactions on Nuclear Science*, 2006, **53** (1): 236 - 241.