CN43-1258/TP
ISSN 1007-130X

计算机工程与科学
COMPUTER ENGINEERING & SCIENCE

2011 年第 33 卷第 10 期
Vol. 33, No. 10, 2011

文章编号:1007-130X(2011)10-0057-03

全光纤分离调制连续变量量子密钥分发*

All Fiber Discrete Modulation Continuous-Variable Quantum Key Distribution

王旭阳,白增亮,李永民,彭堃墀

WANG Xu-yang, BAI Zeng-liang, LI Yong-min, PENG Kun-chi

(量子光学与光量子器件国家重点实验室山西大学光电研究所,山西 太原 030006)

(State Key Laboratory of Quantum Optics and Quantum Optics Devices, Institute of Opto-electronics, Shanxi University, Taiyuan 030006, China)

摘　要:本文给出了基于全光纤的分离调制连续变量量子密钥分发系统。首先介绍了四态分离调制方案及基于该方案的实验原理图;然后对关键器件时域脉冲平衡零拍探测器进行了介绍,并给出了性能测试结果;最后阐述了光脉冲信号的数据结构、编码规则和裸码的获取。

Abstract: In this paper, we give an all fiber discrete modulation continuous-variable quantum key distribution system. We introduce a quaternary discrete modulation protocol, and show the schematic of our experimental setup. The principle of the pulsed homodyne detector is analyzed and the test result about it is given. Finally we present the structure of pulses, the rules of encode, and the procedure to acquire a raw key.

关键词:全光纤;分离调制;连续变量;量子密钥分发

Key words: all fiber; discrete modulation; continuous-variable; quantum key distribution

doi: 10.3969/j.issn.1007-130X.2011.10.010

中图分类号:TP918.1　　**文献标识码**:A

1　引言

密码学是一门研究密码编制与破译的学科,是在编码与破译不断的斗争实践中发展起来的。随着现代科学技术的不断发展,它已成为与信息论、计算机科学、数学、电子学、语言学等有着密切联系的综合性尖端技术学科。目前广泛应用的密码体系有私钥(对称)和公钥(非对称)两种[1]。

RSA 是目前网络和银行广泛使用的公钥,其安全性是基于计算的复杂性(大数素数分解)。但迄今为止,并未证明在多项式时间内利用经典计算机完成大数的素数分解算法不存在。随着 shor 量子并行算法的提出,利用量子计算机可以在多项式时间内求解大数因子这类数学难题。因此,其安全性不能不令人担忧。

One Time Pad 是一种典型的私钥,其安全性早在 1949 由 Shannon 严格证明了。但是,由于其密钥分发过程比较困难,实际很少使用。基于量子力学基本原理的量子密钥分发(QKD)可以安全便捷地产生大量密钥,有着巨大的潜在应用价值。QKD 是量子信息领域内研究的热点之一,也是量

* **收稿日期**:2011-05-15;**修订日期**:2011-07-20
基金项目:国家自然科学基金资助项目(11074156);山西省高等学校优秀青年学术带头人支持计划资助项目;山西省回国留学人员科研资助项目
通讯地址:030006 山西省太原市坞城路 92 号山西大学光电研究所
Address: Institute of Opto-Electronics, Shanxi University, 92 Wucheng Rd, Taiyuan, Shanxi 030006, P. R. China

子信息领域内最接近实用的一个方向。根据编码所用的物理量的取值是连续谱还是分离谱分为离散变量量子密钥分发(DVQKD)和连续变量量子密钥分发(CVQKD)两大类协议。同 DVQKD 相比,CVQKD 不需要复杂的单光子探测器件,只需利用光通信领域已有的元器件及相干光通信的技术就可以构建起来。

根据对信息载体的调制方式不同,CVQKD 分为高斯调制方案[2]和分离调制方案[3]。相比高斯调制方案,分离调制方案具有通信距离长的优势。美国、德国等相关研究小组已对基于该方案的实验系统进行了报道[4,5];在国内,国防科技大学相关研究人员利用非光纤器件对该方案进行了初步的研究[6]。我们小组也开展了基于全光纤分离调制 CVQKD 的实验研究,并实现了裸码的获取。

2 实验方案及装置

2.1 四态分离调制方案

Leverrier A 等人于 2009 年提出四态分离调制方案,并对其安全性进行了严格证明。由于高斯调制在低信噪比时反向调和效率很低,使安全密钥速率接近为 0,限制了该方案的通信距离。分离调制方案在低信噪比时却有着较高的调和效率,经理论计算,当量子通道的额外噪声较低时,该方案可实现长达 250km 的量子密钥分发。

图 1 所示是该方案在相空间中的表示形式,X 和 Y 是光场的正交分量,相干态用误差圆来表示,其起伏方差为标准量子噪声极限 N_0。Alice 将相干态调制到如图 1a 所示的四个状态,经长距离传输后光强减弱,误差圆的中心向原点靠拢,同时由于额外噪声的引入,误差圆的半径变大,信噪比降低,如图 1b 所示。

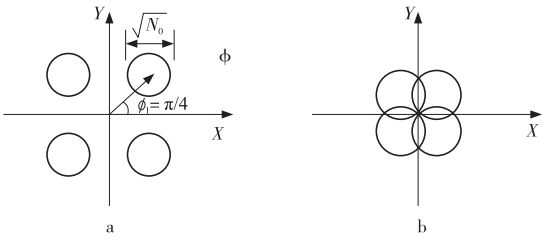

图 1 四态调制方案在相空间中的表示

2.2 实验原理图

实验原理如图 2 所示。在发送端 Alice 处,利用振幅调制器将光纤激光器产生的连续光斩成脉宽为 100ns,速率为 500kHz 的脉冲光;经耦合器后分为信号光和本地光。由计算机驱动的振幅调制器和相位调制器对信号光进行分离调制,其后连接的可变衰减器可将信号光衰减至需要的强度。

接收端 Bob 处,通过调制位于本地光路中的相位调制器,随机地选择光场的正交分量 X 或 Y 进行测量。两束光经耦合干涉后,由时域平衡零拍探测器进行探测,输出电压经数据采集卡采集后输出至计算机进行处理。本地光中接入的 50/50 耦合器,提取出部分 Local 光,用于获取同步时钟信号。为了避免 Bob 端用于干涉的 50/50 耦合器输出不平衡而导致探测器饱和,我们利用弯曲光纤导致损耗的原理自制了两个可实现精细衰减的光纤衰减器。

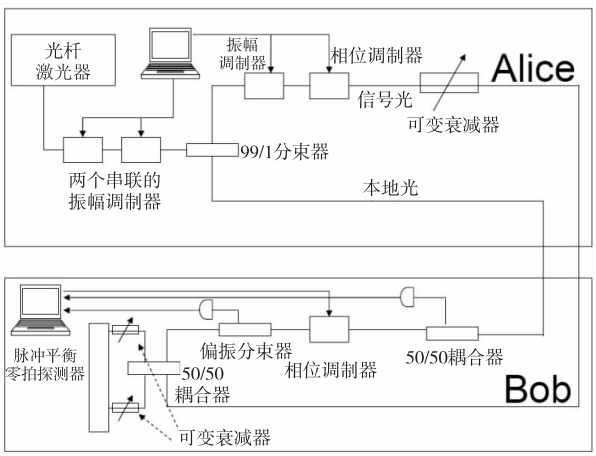

图 2 实验原理图

2.3 脉冲平衡零拍探测器

50/50 分束器输出的两束光被串联且相互匹配的光电二极管接收后,转化为电流信号。相减的电流信号经电荷放大器积分并转化为电压信号。再通过整形放大器对此电压信号进行放大,并整形为高斯形脉冲输出。输出脉冲电压的峰值与信号光场的正交分量成正比,如式(1)所示:

$$\hat{V}_{peak} = g|L|\hat{X}_{\phi} \tag{1}$$

其中 g 是探测器的增益,L 是本地光场的振幅。

探测器是整个系统的测量器件,其性能对安全密钥速率至关重要,我们采用如下方法对其进行了测试[7]。首先将信号光场置为真空场,然后连续均匀地改变本地光场的功率;对应不同的本地光场,对输出电压的峰值起伏方差进行测试,测试结果如图 3 所示。

图 3 中纵坐标为探测器输出电压峰值的起伏方差,横坐标为本地光场的功率,两者成线性关系,该结果与理论推导相符合。

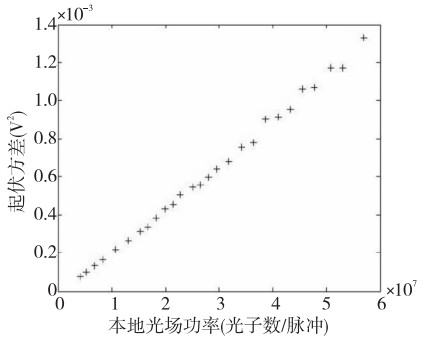

图 3　探测器的性能测试结果

3　数据的传送与裸码的获取

Alice 向 Bob 发送的脉冲以 Block 为一个实时的处理单元，每一个 Block 含有 100 个 Packet。Packet 由测试脉冲和数据脉冲两部分构成。测试脉冲可用于计算信号光的强度，信号光与本地光相对相位等，计算出的相位值可用于相对相位的锁定；数据脉冲可用于数据的传递和额外噪声的估算。由于要对裸码进行反向调和处理，数据经量子信道传输结束后，Bob 通过经典信道将其测量基发送给 Alice，Alice 依据编码规则（依据每个态的中心值在 X 或 Y 分量上投影的正负，将其编为 1 或 −1）对其所发送的态进行编码，编码后获得一组值为 1 和 −1 的数据。Bob 按编码规则（根据所测电压值的正负将其编为 1 或 −1）对其所测电压值进行编码，同样得到一组值为 1 和 −1 的数据。至此 Alice 和 Bob 将各自拥有一组裸码，其后展开的反向调和与私密放大将在这两组数据之间进行。

获取裸码结束后，Alice 将其随机产生的码字的一部分发送给 Bob，Bob 也将相应的每个码字所对应的电压值提取出来，可以得到图 4 中左图所示的分布图，图中相应于每个码字有一组呈高斯分布的电压值。

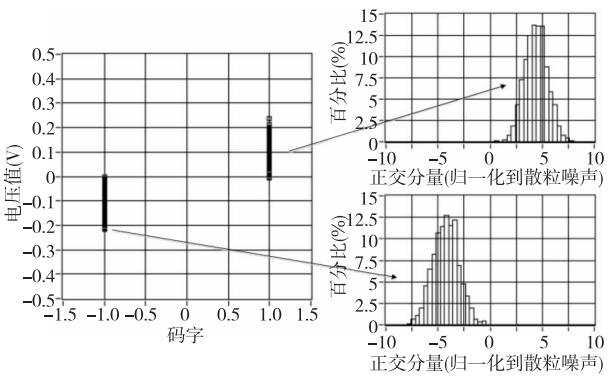

图 4　裸码的统计分析

将每组电压值进行展开后可得如图 4 中右边所示的两幅图，从图 4 中可以形象地看出其分布，横坐标是测量到的正交分量所对应的电压值，并将其归一化到散粒噪声，纵坐标是落在每个电压区间内的点数占总点数的百分比。从图 4 中可以看出，接收端 Bob 接收到的相干光平均光子数约为 8，其测量值呈高斯分布，通过该组数据还可以获取系统的通道效率和额外噪声，为下一步反向调和与私密放大提供必要的参数。

4　结束语

我们建立了全光纤分离调制连续变量量子密钥分发实验系统，并在该系统上实现了四态分离调制方案的裸码发送与接收。目前，我们正在进行后续的反向调和与私密放大的研究，以进一步从裸码中提取出最终的安全密钥。

参考文献：

[1] 郭光灿. 量子密码[J]. 物理与工程，2005，15(4)：1-8.

[2] Grosshans F，Assche G V，Wenger J，et al. Quantum Key Distribution Using Gaussian-Modulated Coherent States[J]. Nature，2003，421(16)：238-241.

[3] Leverrier A，Grangier P. Unconditional Security Proof of Long-Distance Continuous-Variable Quantum Key Distribution with Discrete Modulation[J]. Physical Review Letters，2009，102：180504.

[4] Xuan Q Y，Zhang Z S，Voss P L. A 24km Fiber-Based Discretely Signaled Continuous Variable Quantum Key Distribution System[J]. Optics Express，2009，17(26)：24244-24249.

[5] Wittmann C，Furst J，Wiechers C，et al. Witnessing Effective Entanglement over a 2km Fiber Channel[J]. Optics Express，2010，18(5)：4499-4509.

[6] Shen Y，Zou H X，Tian L，et al. Experimental Study on the Gaussian-Modulated Coherent-State Quantum Key Distribution over Standard Telecommunication Fi-Bers[J]. Physical Review A，2010，82：022317.

[7] Hansen H，Aichele T，Hettich C，et al. Ultrasensitive Pulsed，Balanced Homodyne Detector：Application to Time-Domain Quantum Measurements[J]. Opt Lett，2001，26(21)：1714-1716.

王旭阳(1984 -)，男，山西长治人，博士生，研究方向为量子信息。**E-mail**：200722607013@mail.sxu.cn

WANG Xu-yang，born in 1984，PhD candidate，his research interest includes quantum information.