量子密钥分发实验中的符合测量方法*

马海强[1,2]　符东浩[3]　冯凯峰[3]　姚德成[3]　吴令安[1,†]

（1　中国科学院物理研究所光物理开放实验室　北京　100080）

（2　东南大学　南京　210096）

（3　中国科学院研究生院　北京　100039）

摘　要　采用符合测量方法提高全光纤量子密钥分发系统的数据采集速度，寻求更高的密钥生成率. 主要论述了光路中的改进和符合测量的步骤、方法以及在密钥分发实验中的应用.

关键词　符合测量，量子密钥分发，马赫－曾德尔（Mach－Zehnder）干涉仪，时幅转换仪

APPLICATION OF COINCIDENCE MEASUREMENT TO BB84 QUANTUM KEY DISTRIBUTION

MA Hai-Qiang[1,2]　FU Dong-Hao[3]　FENG Kai-Feng[3]　YAO De-Cheng[3]　WU Ling-An[1,†]

（1　*Laboratory of Optical Physics, Institute of Physics, Chinese Academy of Sciences, Beijing* 100080, *China*）

（2　*South East University, Nanjing* 210096, *China*）

（3　*Graduate School, Chinese Academy of Sciences, Beijing* 100039, *China*）

Abstract　A coincidence measurement technique has been incorporated into our all-fiber BB84 quantum key distribution system which can improve the data acquisition and key generation rates.

Key words　coincidence measurement, quantum key distribution, Mach-Zehnder interferometer, time-amplitude converter

1　引言

量子信息科学是量子力学与信息科学相结合的新产物，是将会对人类社会产生重大影响的新型前沿科学. 量子密钥分发是量子信息科学中的重要分支，理论与实验研究已迅速展开，也是当前量子信息中最接近实用的领域. 早在20世纪70年代初期，美国哥伦比亚大学的Wiesner就提出了“共轭编码”的概念[1]，令人遗憾的是他的论文在1983年才得以发表，1984年，Bennett和Brassard基于他的思想提出第一个量子密钥分发方案（后来称之为BB84协议）[2]. 20世纪90年代初，量子计算理论发展起来了，尤其是Shor提出的大数质因子分解算法[3]，使人们认识到现在使用的依赖于数学复杂性的经典公钥密码体系存在着安全隐患，而由量子力学基本原理保证其安全性的量子密码通信，就成了解决这一问题的惟一途径. 通过量子密码技术[4]，在异地的通讯双方可随时建立绝对安全的真随机数密码本，并可察觉到窃听者.

量子密码通信的三大主流方案BB84协议、B92协议[5]、EPR协议[6]于1992年已经全部形成. 自1992年第一个原理性的量子密钥分发实验成功后，近十年来，实验方面的进展可以说是日新月异，由开始的几十厘米[7]，到现在的近70公里[8]，传播媒介包括自由空间和光纤，显示出巨大的应用潜力. 1995年，国内的第一个量子密钥分发实验在自由空间成功演示[9]，2000年，我们又在1.1km的光纤中完成量子密钥分发[10]. 本文介绍我们在数据采集方面的

*　国家自然科学基金（批准号：19974073，60178013）、国家科技部“九七三”（批准号：2001CB309301）、中国科学院知识创新工程“量子通信技术的研究”资助项目

2002－07－12收到初稿，2002－12－02修回

†　通讯联系人. E-mail：wula@aphy.iphy.ac.cn

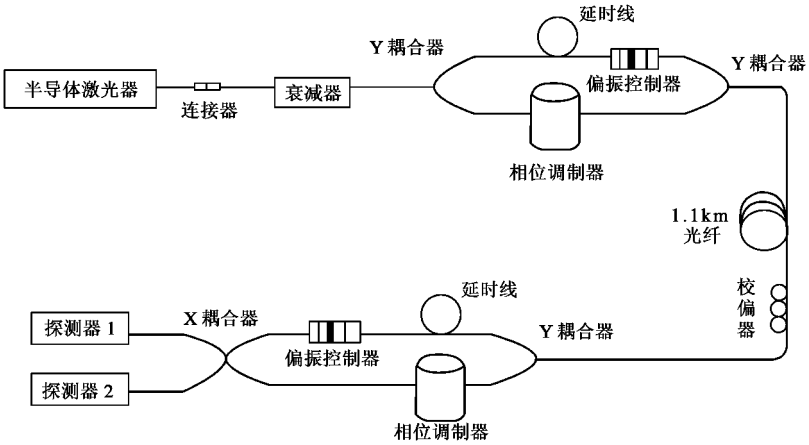

图1　实验中的光路简化图

一种新方法,用符合测量法来进行数据的采集,并随之介绍了光路中的改进和符合测量的步骤、方法. 最后,论述了符合测量的意义.

2　实验原理

采用 BB84 通信协议,基于不等臂马赫 – 曾德尔(Mach – Zehnder)(M – Z)光纤干涉仪(参见图1),Alice 从两个基中任选一个基矢对光子进行相位调制,Bob 从两个基中任选一个基矢进行检测,在 M – Z 干涉仪两个输出口分别放置单光子探测器用以检测相长干涉光子信号,探测器 1 或 2 响应分别代表 1 或 0 比特数. Alice 和 Bob 公开比较所选择的调制基之后,留下基相同时的比特数列为密码本.

单光子探测器采用工作于盖革模式下的雪崩光电二极管. 在实验中,为了减少噪声对计数的影响,通常采用门控电路打开硅雪崩二极管的高压,但采用符合计数技术,可用一般的无源抑制雪崩二极管探测器,省去门开关. 本文将介绍用无源抑制雪崩二极管进行信号探测,利用符合计数技术,借助多道分析仪与时幅转换仪的结合,测量和调试探测信号与激光器时钟信号的时间差,使它们同时到达符合计数器. 符合信号进入计算机,经采集程序的处理,分析比特序列从而确定量子密钥.

3　实验装置

3.1　光路部分

实验中的光路简化图如图 1 所示. 光源为中心波长 850nm 带尾纤半导体激光器,调节所加偏压,能够输出连续或脉冲的单模线偏振光,连续光功率和脉冲峰值功率均为 1mW,重复频率 1MHz,驱动电路、温控系统是我们自制的[10]. 为满足量子密钥分发所需光源的要求,即单光子源,激光器工作在脉冲状态下,再用衰减器将脉冲光衰减 90dB,每个脉冲中的平均光子数为 0.1 个,每次脉冲包含两个以上的光子概率仅为 0.5%. 衰减后的光脉冲经 50/50% 的分束器后进入 Alice 的 M – Z 干涉仪,其中一臂有相位调制器(压电陶瓷光纤调制器),另一臂有延时线和偏振控制器,随后经一 50/50% 的 Y 型耦合器进入到 1.1km 的光纤中. 到接收方 Bob 之后,首先用偏振控制器校偏,经分束器进入到 Bob 的 M – Z 干涉仪,再经一 X 型耦合器,最后到达两个(前 EG&G Canada 公司 C30902SQC – 02 型)硅雪崩光电二极管 (APD)[10]. 雪崩二极管采用无源抑制,工作在盖革模式下(工作电压超过雪崩电压),两探测器 APD1,APD2 探测概率分别为

$$P_1 = [1 + \cos(\Phi_a - \Phi_b)]/8, \qquad (1)$$

$$P_2 = [1 - \cos(\Phi_a - \Phi_b)]/8, \qquad (2)$$

其中 Φ_a 和 Φ_b 分别为 Alice 和 Bob 调制的相位角. 该光路的详细工作过程见参考文献[10].

3.2　符合测量电路

符合事件是指两个或两个以上同时发生的事件[11]. 图 2 是我们用于确定雪崩光二极管信号的符合测量原理图. 激光器在输出一个激光脉冲的同时也输出一个同步的 TTL 时钟信号,用它去和探测信号做符合,便可判断哪个探测器做出响应.

我们的 APD 无源抑制电路,尽量减小分布电容和分压电阻,工作在温度 – 50℃,偏压 – 170V(超过雪崩电压 2V)时暗计数为每秒 100 个左右,其雪崩信号即单光子峰高约为 50—60mV,半高全宽约为

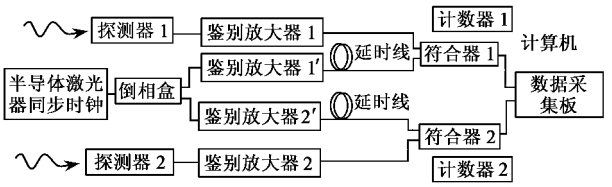

图 2　符合测量的电路简化图

5ns. 为使探测信号能被符合器所识别，必须将其转化为 NIM 信号（高电平为 0V，低电平为 −0.8V），于是又在 APD 后加了鉴别放大器，其功能是滤掉噪声，放大信号. 和探测信号作符合的是激光器的脉冲驱动电路所产生的同步时钟，频率 1MHz. 因为时钟信号是 TTL 信号，我们先将其转为负的脉冲信号，再经鉴别放大器和延时线输出为 NIM 信号. 用鉴别放大器 1 与鉴别放大器 1′作符合，用鉴别放大器 2 与鉴别放大器 2′作符合，信号进入前 EG&G 公司 CO 4020 型逻辑单元进行符合测量，其符合窗口为 8ns. 符合器的输出信号有两路，一路到计数器，随时观察两符合器的计数情况，另一输出为 TTL 信号，经接口电路板（PC − 1032T − N32 通道数据采集板）[10]，根据需要编写控制程序进行信号的采集和处理.

为了保证激光时钟脉冲与探测器脉冲信号同时到达符合器，必须调整好各光路、电路的长度. 为此，必须先精确地测量和纠正做符合的两路信号时间差.

3.3　时间差的标定与结果

实验中，我们使用时幅转换仪（TAC，前 EG&G 公司 567 型）和多道分析仪（MCA）的结合，来测量和控制两路的时间差. TAC 是将相对于同一个开始信号、不同时刻到来的结束信号的时间差转换为不同电压幅度输出. 可转换的时间差范围为 50ns 至 200μs 之间，我们的开始信号是 1MHz 的，选择的时间档就是 1μs，在这一档，输出的波形宽度为 2.5μs，重复频率 143kHz. 多道分析仪的作用是将不同的电压显示在不同的道址上，根据道址就能精确地区分不同的电压并由此推出时间差. 通道数有 4096，2048，1024，512 几档，根据所需精度选取恰当的道数，本实验中我们用的是 4096 通道数. 多道分析仪为北京核仪器厂 BH1224 型的接口电路板，将其插入计算机的 ISA 扩展槽中，在相应的驱动程序下，就能方便地读出峰的道址.

借助一个已标定的延时盒，标定出时间差与道址的关系式. 数据如表 1 所示.

表 1

延时/ns	42	52	56	63	67	71	75	78	84	87
道址	4	54	71	108	124	150	166	182	212	227
延时/ns	93	99	100	349	354	464	467	474	484	514
道址	254	284	287	1801	1831	2543	2562	2618	2688	2902

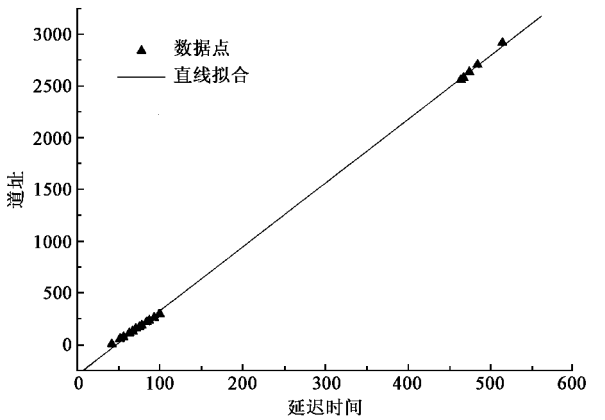

图 3　道址与延迟时间的关系图

道址与延迟时间的关系如图 3 所示. 经直线拟合得道址与延迟时间的关系式为：

$$X = 6.15t - 293.35, \qquad (3)$$

其中 X 为道址数，t 为延迟时间（单位 ns）. 也就是说，在这一档，两个道址相差 162.6ps. 为叙述简便，以作一路的时间标定为例加以说明. 在进行符合之前，将电路改为如图 4 所示.

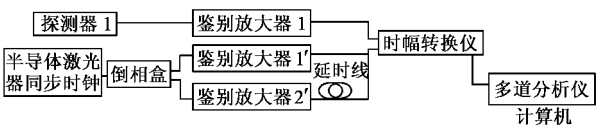

图 4　时间标定的电路简化图

在本实验中我们首先以鉴别放大器 1′做开始信号，以鉴别放大器 1 做结束信号时，观察到峰值出现在第 1832 道，利用（3）可求得开始与结束的时间差是

$$\Delta t = (1832 + 293.35)/6.15 = 345.58\text{ns}.$$

改变时间差有两种方法，一为加同轴电缆即电延时，另一种方法是在光路中加光纤即光延时. 因为加同轴电缆延时较为方便，我们采用的是前者. 经标定，同轴电缆的延时约为 4.91ns/m，因此应在鉴别放大器 1′后加长度为 70.38m 的同轴电缆.

将鉴别放大器 1′信号加了延时后，以鉴别放大器 2′信号作为开始信号，分别以鉴别放大器 1 和 1′的信号作为结束信号，测得各自道址见图 5. 从图 5

中的道址可看出鉴别放大器 1 信号和鉴别放大器 1′信号相对于同一起点和同一终点的时间差相同.

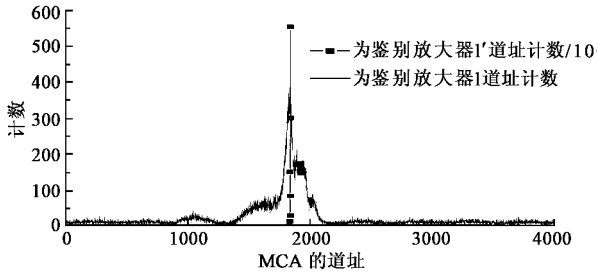

图 5　道址分布图

(横坐标是道址数,纵坐标是在 50s 的时间内各道址上的计数,注意鉴别放大器 1′信号的计数缩小了 100 倍)

从图 5 可看出,鉴别放大器 1′信号的峰很尖锐,出现在一个道址上,这是因为鉴别放大器 1′和 2′的信号都来自激光器时钟,时间差当然是很稳定的,经 TAC 输出的电压也是稳定的. 而鉴别放大器 1 信号的峰有一定的宽度,这是由于激光器所发的光脉冲有 100ns 的宽度造成的,而符合计数峰的半高全宽所占的道宽约是 600 个道,即时间约是 100ns,和脉冲宽度也是吻合的. 用这种读道址的方法,如果峰越窄即越尖锐,道址读得越准确,上述的(3)式就能和实验结果拟合得越好,误差就越小. 从图 5 中可读出两峰的道址,误差在 5 个道以内,这样获得的时间精度就能达到 0.81ns.

3.4　符合测量在量子密钥分发实验中的应用

根据 BB84 协议,Alice 从两个基中任选一个基矢,对发出的光子进行相位调制. Bob 在探测时,也是从两个基中任选一个基矢进行检测,只有当 Alice 和 Bob 选择相同的基时,并且同时也只有一个探测器探测到信号,这样的数据才为有效. 上述的(1),(2)式在具体的实验应用中为

$$P_1 = [1 + \cos(\Phi_0 + \Phi_a - \Phi_b)]/8, \quad (4)$$

$$P_2 = [1 - \cos(\Phi_0 + \Phi_a - \Phi_b)]/8, \quad (5)$$

其中 Φ_0 为初始相位. 在理想的情况下 Φ_0 应为 0,但由于环境的不稳定性,造成 Φ_0 实际上在不断地变动. 为此,实验中采取了分段测试.

我们用 C++ 嵌套汇编语言程序控制计算机进行数据的采集和处理. 在每次采集过程中分三步进行,先运行一段测试程序,测出 50 个数据,Alice 和 Bob 都不加调制,若 P_2 响应的次数多,则计初始相位为 π. 若两探测器响应的次数近乎相等,则计初始相位为 $\pi/2$. 然后以采集 100 个数据为一组,每组采集时间是 0.128s,每次采样 10 组,再将两个探测器都有信号或都没有信号的数据抛弃掉,将有效的数据记录到文件中. 作为例子,表 2 给出数据采集的一个片段.

表 2　实验中数据采集的一个片段

初相位	π						$\pi/2$				
采集序列	1	2	3	4	5	6	7	8	9	10	11
Φ_a	1	2	0	0	1	1	1	3	1	1	1
Φ_b	3	0	0	0	3	1	0	0	2	0	0
探测器 1	1	1	0	0	1	1	1	0	0	1	1
探测器 2	0	0	1	1	0	0	0	1	1	0	0
能否使用	Y	Y	Y	Y	Y	N	Y	Y	Y	Y	Y

将 Φ_a 和 Φ_b 的取值 $-\pi/2, 0, \pi/2, \pi$ 分别用 0,1,2,3 做标识. 探测器 1,2 测到符合信号,即测到光子时计 1,没有测到信号则计 0. 可看出前 6 个数据和后 5 个数据的初始相位的差别,前 6 个是 Φ_0 为 π 时,后 5 个是在 Φ_0 为 $\pi/2$ 时,其中第 6 个为误码,Y 表示测试结果可使用,N 表示测试结果有误,不能使用. 由于初始相位的漂移,基的组成也会变化. 本实验的误差来源主要是相位和偏振的漂移,前者为主要因素.

4　总结

在单光子光纤通信系统中有许多因素会影响测量精度,如探测器的暗噪声、环境对系统稳定性的干扰及光源的稳定性等等. 而且,这些因素常常很难准确地测定. 符合测量却能避开上述困难,起到门控开关的作用,方法简单,操作方便. 另外,符合逻辑电路中在电路制作方面也较容易实现.

我们的系统还处在实验阶段,波长为 850nm,相位调制器的频率只有 800Hz,若要满足系统的要求应在 MHz 以上,数据的采集与处理速度及探测器的量子效率都是影响我们最终结果的关键因素. 为使量子密钥分发走出实验室,我们的任务是,将光源改为普通的光通信波长 1.3μm 或 1.5μm 以增加通信距离,提高系统抗外界干扰能力,寻求适合 1.3μm 和 1.5μm 的单光子探测器,使通信双方的电路和光路控制集成化和模块化,以加快量子密钥分发技术向实用化发展的步伐.

参　考　文　献

[1] Bennett C H, Brassard G, Ekert A K. Scientific American, 1992, 10 27

[2] Bennett C H, Brassard G. Proc. IEEE Internat. Conf. Computers, Systems and Signal Processing, Bangalore, India. New York, IEEE, 1984

[3] Shor P W. Proc. 35th Annual Symposium on Foundations of Computer Science. New York, IEEE, 1994
[4] Hughes R J, Alde D M, Dyer P *et al*. Contemp. Phys., 1995,36:149; 吴令安. 物理,1998, 27:544 [Wu L A. Wuli(Physics), 1998, 27:544 (in Chinese)]
[5] Bennett C H. Phys. Rev. Lett., 1992, 68:3121
[6] Ekert A K. Phys. Rev. Lett.,1991, 67:661
[7] Bennett C H. J. Cryptol. , 1992, 5:3
[8] Hiskett P A, Bonfrate G, Buller G S *et al*. J. Mod. Optics, 2001,50:1957
[9] 邵进, 吴令安. 量子光学, 1995, 1:41 [Shao J, Wu L A. Quantum Optics, 1995,1:41 (in Chinese)]
[10] 梁创, 符东浩等. 物理学报, 2001,50:1429 [Liang C, Fu D H *et al*. Acta Physica Sinica, 2001,50:1429 (in Chinese)]
[11] 吴思诚, 王祖铨. 近代物理实验(第二版). 北京:北京大学出版社, 1995. 127 [Wu S C, Wang Z Q. Modern Physics Experiments (2nd ed.). Beijing: Peking University Press, 1995. 127 (in Chinese)]
[12] 丁慎训, 张孔时. 物理实验教程. 北京:清华大学出版社, 1993.10 [Ding S X, Zhang K S. Introduction to Physics Experiments. Beijing: Tsinghua University Press, 1993. 10 (in Chinese)]

·物理新闻与动态·

相互竞争下的最小化

自然界中存在着许多天然材料,它们具有多种相互竞争的性质,例如蜘蛛结的网,它将轻巧、富于弹性和不易断裂等性质集于一身. 而这类生物材料的特点总是由两种或更多的材料复合而成,从而使这类生物材料具有多种特殊的功能. 借鉴于这个思想,美国普林斯顿大学的 Torquato S 教授和他的同事们利用计算机模拟方法去计算合成材料的特性,他们希望新型的复合材料能具有多方面的优点,例如在力学性能、导电与导热、迅速地传输流体与粒子的功能方面都很有特色. 因此模拟工作要面对的是如何使单项性质得到优化. 简单地说,如果想要使一种材料具有保温特性,那就必需让这种材料以小气泡的形式悬浮在另一种材料中. 但现在还不太清楚是如何在混合材料中能使两种相互竞争的性质互不干扰地共存于同一结构中.

现在 Torquato S 教授的研究组采用了一种称为"拓扑优化(topology optimization)"的算法来模拟混合的两相,使新材料既能很好地导电,也能很好地导热;换句话说,也就是创造一种程序能使混合材料中的两种性能都达到最大值. 计算的结果出人意外,两种材料(或两相)间的界面是一种称为"双连续、三重周期的最小表面",这里的双连续是指一种相可以从样品的一端扩展到另一端的任何地点都不会发生中断,尽管该相是沉浸在另一相内. 而三重周期是指复合材料在三个方向上都会周期性地出现重复的花纹结构,最后的一点是两相的界面具有最小的表面积. 这个性质有点类似于在弯曲的铁丝框架下形成的肥皂泡膜,但肥皂膜的最小表面积是由于表面张力的作用,而复合材料的最小表面积是来自于两种不同物理特性的竞争,所以这种最小表面积的形成机理现在还不是很清楚. 除了上面所述的导电与导热性能的竞争机制外,拓扑优化算法还能应用于化学、力学以及光学特性间的竞争.

纽约大学的数学家 Kohn R 教授认为,从生物学的角度来看,为什么拓扑优化算法能使复合材料具有最小表面积的物理机理尚不清楚,但这个算法却是一个有力的工具,它能让我们去开启许多未知的领域,而寻找这些领域间的联系正是科学家们今后的艰巨任务.

(云中客摘自 Phys. Rev. Lett., 23 December 2002)

更　正

《物理》2002 年 12 期第 796 页的文章《激光等离子体推进在火箭推进技术领域的应用前景》的引言部分中关于液氢火箭的冲量耦合系数(即能量 – 动量转换效率)的计算有误,说明如下:

火箭喷出的是燃料燃烧后的产物,并非燃料本身. 液氢燃料火箭喷出的是水蒸气,而水蒸气中仅含有 1/9 质量的氢元素. 因此,在计算火箭的能量时用氢的燃烧热 ε 直接乘以喷气质量 dm 是不对的. 正确的算法是给 797 页的方程两边同时除以 $\varepsilon dm/9$,由此计算出的液氢火箭的冲量耦合系数应该比原文中的大 9 倍,即 29.7dyne/W. 由于笔者的疏忽导致文章出现无法挽回的错误,笔者在此向广大读者表示深深的歉意.

(中国科学院物理研究所　鲁　欣)