第 59 卷 第 8 期 2010 年 8 月
1000-3290/2010/59(08)/5514-09

物 理 学 报
ACTA PHYSICA SINICA

Vol. 59, No. 8, August, 2010
©2010 Chin. Phys. Soc.

长程光纤传输的时间抖动对相位编码量子密钥分发系统的影响*

王金东[1)†] 魏正军[1)] 张 辉[2)] 张华妮[1)] 陈 帅[1)] 秦晓娟[3)]
郭健平[1)] 廖常俊[1)] 刘颂豪[1)]

1)(华南师范大学信息光电子科技学院光子信息技术广东普通高校重点实验室,广州 510006)

2)(中国人民解放军炮兵学院物理教研室,合肥 230031)

3)(广东广播电视大学工程技术系,广州 510091)

(2009 年 10 月 22 日收到;2009 年 11 月 24 日收到修改稿)

测量了光脉冲在不同传输距离和不同外界环境影响下基于差分相位编码和双不等臂 M-Z 相位编码系统的时间抖动,并根据时间抖动的分布情况建立了相位编码量子密钥分发系统中误码率和时间抖动关系的物理模型,给出了单光子脉冲一般波形函数和误码率之间的关系式,根据这个关系式可以得出确定波形单光子脉冲在确定时间抖动分布情况下系统误码率的结果.

关键词:量子密钥分发,相位编码,时间抖动,误码率

PACC:4250,0367,4230Q,9575K

1. 引 言

量子密码的最初思想是 1969 年 Wiesner 首先提出来的[1],并引入量子钞票(quantum bank notes)的概念.量子钞票是利用量子 bit 来储存金额,由于未知量子 bit 的不可克隆性,量子钞票具有物理上的无条件安全性.但是在 Wiesner 刚提出量子钞票的时候,通过光子技术实现量子 bit 的存储时间极短(小于 10 ns),实现量子钞票看起来几乎是不可能的.Bennett 和 Brassard 在 Wiesner 思想的启发下,意识到量子密码中量子 bit 的传输比量子 bit 的储存更为重要.基于这个考虑,Bennett 和 Brassard 于 1984 年提出了量子密钥分配的概念[2],这个概念的提出标志着量子密码的真正开始.

量子保密通信是基于物理学的基本原理来保证通信的安全性,利用单量子态进行密钥的传输,并将这种密钥分发方式和保密通信领域中唯一被证明是安全的等长度的一次一密私钥密码体制相结合,为保密通信领域提供了一种可行的,理论上被证明绝对安全的通信方式.量子力学的测不准原理和未知量子态不可克隆原理保证了单量子态用于密钥分配的理论安全性.自量子密钥分配的概念被提出以来,在短短 20 多年的时间中,该领域的理论、实验以及相关技术都取得了显著的进展[3—12],成为量子光学领域最接近实用的应用之一,其广泛的应用前景受到了包括军事、商业、外交、金融等各领域的普遍重视.

量子密钥分发系统常采用偏振编码或相位编码的方式,相比偏振编码来说,光子信号在光纤中传输时其相位信息更易保持,因此绝大多数现有的光纤量子密码系统都采用相位编码方案[13].对于相位编码系统,目前常见的系统有双不等臂 Mach-Zehnder(M-Z)相位编码系统和差分相位编码系统.

在图 1 所示的双不等臂 M-Z 相位编码系统中,Alice 首先将一个单光子脉冲通过一个不等臂的光纤延迟环(M-Z 干涉仪)分为两路,并在其中一路上插入相位调制器,按照协议约定进行随机相位调制

* 广州市科技支撑计划(批准号:2008Z1-D501),广东省工业攻关项目(批准号:2007B010400009),广东理工职业学院科研项目(批准号:0901)资助的课题.

† E-mail:jindongwakd@126.com

后，通过信道传输给 Bob，Bob 利用光学延迟的方法（M-Z 干涉仪）使这些单光子脉冲进行干涉，并在其中一臂上插入相位调制器进行随机相位调制，干涉输出的结果用单光子探测器进行记录，通信双方根据协议约定的编码规则，在公开信道交换了必要的信息后生成密钥 bit.

图 1　双不等臂 M-Z 相位编码系统

另外一种常见的相位编码系统是差分相位编码系统. 如图 2 所示，(a)是基于单光子脉冲的差分相位编码系统，(b)是基于连续激光进行强度调制产生弱相干激光脉冲的差分相位编码系统. 在基于弱相干光的差分相位编码系统中，Alice 将连续光经过强度调制后产生一列相干光脉冲，通过强衰减后对每个光脉冲进行 0 或 π 的随机相位调制，在 Bob 端，利用一个单比特延迟环进行延迟，这个单 bit 延迟环的两路臂长差引起的延时被设计成刚好等于 Alice 端发射的相邻两个光脉冲之间的时间差，因此，Alice 发送的相干光脉冲经过单比特延迟环后即可通过相邻两个单光子概率幅脉冲之间的干涉检出 Alice 调制的相位信息，同样经过必要的经典信息对照后，根据协议得到密钥 bit.

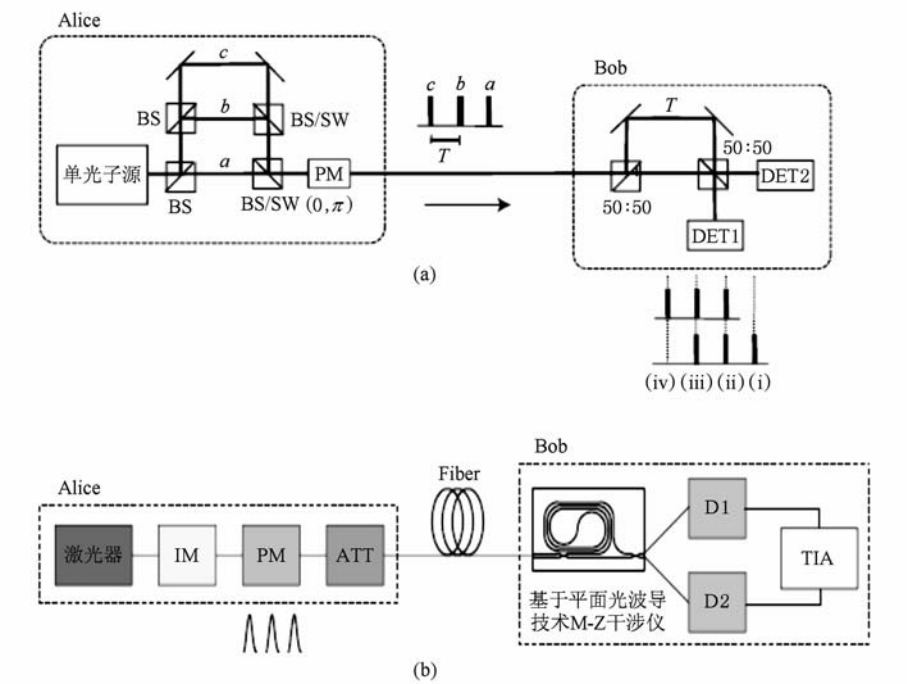

图 2　差分相位编码系统示意图[14,15]　(a)为基于单光子的差分相位编码系统；(b)为基于弱相干光的差分相位编码系统

以上常见的相位编码系统的特点是：首先将单光子脉冲通过时分的方式分裂为两个或多个单光子概率幅脉冲，并根据协议对这些单光子概率幅脉冲进行随机相位调制，然后经过长程光纤的传输，到达通信接收方后利用光学延迟的方法使这两个单光子概率幅脉冲重合并发生干涉叠加以检出被调制的相位信息. 然而，光脉冲在长程光纤中传输，会由于时间抖动的原因造成不能按照理想时刻到达通信接收机，那么由于长程传输时间抖动的存在，在 Bob 端采用光学延迟环进行检测时就会有不同重合度干涉情况的发生，给系统的密钥信息带来一定的误码率.

本文测量了光脉冲在不同传输距离和不同外界环境影响下基于差分相位编码和双不等臂 M-Z 相位编码系统的时间抖动,并根据时间抖动的分布情况建立了相位编码量子密钥分发系统中误码率和时间抖动关系的物理模型,给出了单光子脉冲一般波形函数和误码率之间的关系式,根据这个关系式可以得出确定波形在确定时间抖动分布情况下误码率的结果.

2. 光脉冲在长程光纤中传输延迟的测量

首先构建基于差分相位编码系统和双不等臂 M-Z 相位编码系统的光学结构并对 Alice 发送的光脉冲进行长程光纤传输时的时间抖动进行测量.

2.1. 基于弱相干光的差分相位编码系统时间抖动的测量

如图 3 所示,Alice 经过强度调制在时钟源的触发下产生弱相干光脉冲,经过随机相位调制后进行长程光纤的传输,相邻脉冲的时间间隔我们可以分别定义为 $t_1, t_2, t_3, \cdots$,理论上这些时间间隔都必须等于图 2 中 Bob 端的光学延迟单元所分裂光脉冲的时间间隔 t,但是在实际的实验系统和应用中,这些时间间隔并不是完全相同的,首先由于时钟精度的问题会使得这些时间间隔不可能完全相同,其次,这些光脉冲经过长程光纤传输时,会由于光纤受到外界环境的影响发生程度不同的时间延迟,这些因素造成了这些时间间隔之间会存在一个抖动分布,使得这些光脉冲在到达 Bob 端时相邻光脉冲的时间间隔并不严格等于 Bob 的延迟时间 t. 为了衡量任意两个相邻光脉冲时间间隔的变化有多大,采用对相邻光脉冲的时间间隔进行一阶差分运算得到相邻两个时间间隔的差值,并对这个时间差用示波器进行长时间的测量获得时间抖动分布的曲线. 显然,当图 3 中相邻两个光脉冲的时间间隔发生变化时,相邻两个光脉冲在干涉叠加时就不可能完全重合而造成干涉对比度的降低,增加了系统误码率.

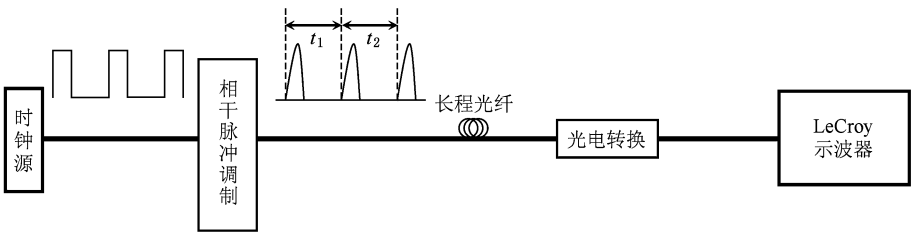

图 3 基于弱相干光差分相位编码系统的长程传输延迟时间分布的测量装置

采用一阶差分运算对时间抖动进行测量. 对任意相邻光脉冲进行采样,记录相邻光脉冲之间的时间间隔:$t_1, t_2, t_3, \cdots, t_n$ 等,因此可以得到 $t_2 - t_1, t_3 - t_2, \cdots, t_n - t_{n-1}$,通过示波器的大量采样,即可得出相邻光脉冲时间间隔差值的统计分布结果. 实验中采用力克示波器 104 MXi(带宽 1 GHz,采样率可达 10 Gbit/s)测量相邻光脉冲时间间隔抖动的统计分布,采样点选择为 10000,时间抖动测量精度为 5 ps. 以下是在不同传输距离和不同外界环境下时间抖动的分布曲线和漂移情况.

2.1.1. 实验室环境下不同传输距离时间抖动分布的测量

图 4 是采用图 3 的测试装置在实验室环境下对不同传输距离进行的时间抖动测量. 图中四条曲线峰值最高的是传输距离为 0 km 的分布曲线,向下依次为 25,50 和 75 km 的分布曲线. 对数据进行统计分析后,同时给出此时的时间抖动分布的相关数据比较,如表 1 所示.

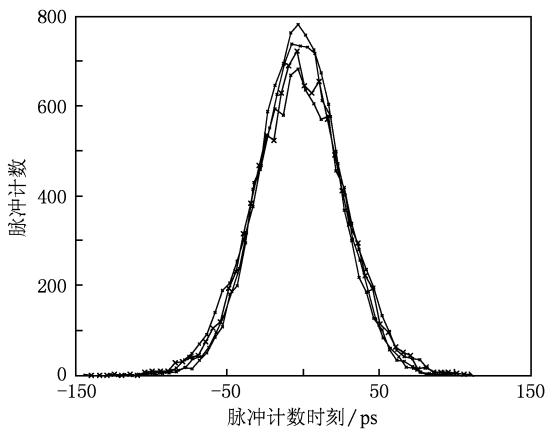

图 4 25 ℃时不同传输距离的时间抖动分布

表 1　实验室环境下不同传输距离时间抖动分布统计数据

光纤长度/km	全宽/ps	半宽/ps	最大计数
0	185	60	780
25	225	70	738
50	240	75	721
75	275	80	681

通过图 4 和表 1 可见：1）不管多长的传输距离，相邻两个光脉冲的时间间隔都不可能是长期确定的，都会存在一个随机分布；2）在实验室温度和振动相对保持稳定的情况下，随着传输距离的增加，时间抖动变大，这个现象可以通过抖动分布曲线的全宽，半宽等数据看出，并且随着抖动的变大，峰值点数（其物理意义是光脉冲干涉叠加时完全重合的最大概率）变小.

所以可以看出，随着传输距离的增加，时间抖动变大，并且在不同的传输距离，相邻两个光脉冲完全不能同时到达合束器进行干涉叠加的情况总是存在，会随着传输距离的增加而逐渐增多. 这样不同概率的干涉叠加的不完善性就造成了系统的误码，这种误码是由于长程光纤的传输延迟造成的，使量子密钥分发系统不可避免地出现一个误码率的极限，这个误码率不管如何改进探测器均会存在.

2.1.2. 75 km 传输距离户外光纤上的时间抖动分布测量

在实际应用中，除了传输距离对时间抖动的影响外，光纤在外界环境下受到温度的变化、震动等因素的影响都会改变光脉冲在长程光纤中的传输时间的抖动分布，以下是在户外 75 km 的长程光纤中，当温度在一昼夜发生变化时测量的时间抖动分布，并同时记录了测量时的温度，给出了时间抖动分布随外界实际应用环境的变化关系.

图 5 中，峰值最高曲线对应温度为 27 ℃时的统计分布曲线，向下依次为 32 和 40 ℃，整个测量是在温度由 27 向 40 ℃升温的过程中测量的. 我们仍旧对测量数据进行了相关统计数据的比较，如表 2 所示.

表 2　75 km 传输距离户外光纤时间抖动分布统计数据

温度/℃	全宽/ps	半宽/ps	最大计数
27	180	70	766
32	300	85	624
40	405	95	522

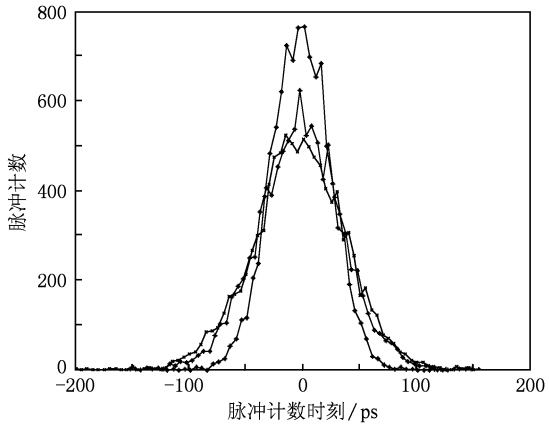

图 5　75 km 户外光纤传输时间抖动分布图

通过以上曲线和数据可以看出，周期间抖动分布除了会随着传输距离的增加而恶化，并且会随着外界环境的变化而恶化.

因为由于长程光纤的传输延时造成的时间抖动是一个慢过程，所以目前一般采用的方法是在一段时间后发现误码率增加就采用光纤检测环的光程调节来进行主动补偿[16—19]，但是采用在干涉环中进行相位主动补偿的原理仅仅是补偿由于传输延迟造成的相位不匹配引起的误码，通常都在一个相位周期内进行，对于时间抖动引起的不完全重合造成的误码并没有得到有效地补偿，并且在主动相位补偿的文献中，也并没有把时间抖动引起的不完全重合造成的误码考虑进来. 除了在一个相位周期内的主动补偿外，我们还可以通过光纤拉伸器等方法进行时间延迟的相对补偿，调节光纤环的臂长差以匹配最大概率的时间间隔的取值，那么最大概率的时间间隔的取值是否也会随着环境的变化以及传输距离的增加而变化呢？我们还利用这个实验平台测量了长时间的漂移情况，也就是图 6 中最大概

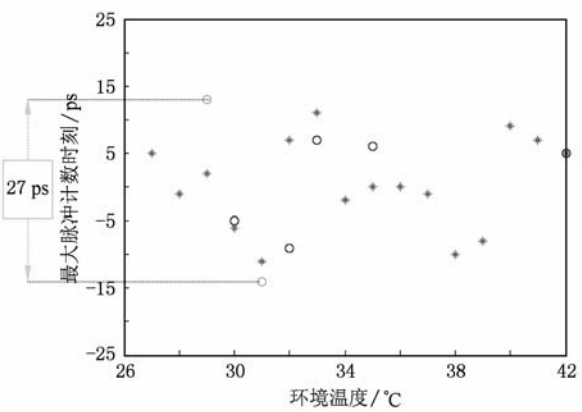

图 6　75 km 传输距离时间抖动随外界环境变化时的漂移

率的时间间隔取值的变化情况,也即图 4 和图 5 中分布曲线峰值所对应时间间隔的变化情况.

我们对户外光纤在一定温度变化(27—42 ℃)条件下进行了 75 km 传输距离时间抖动漂移的测量,如图 6 所示. 图中星点表示的数据是随温度升高进行的测量结果,圆点数据是在温度逐渐下降后进行的测量.

2.1.3. 实验结果分析

以上我们测量了基于弱相干光差分相位编码光学系统中光脉冲在不同条件下传输延迟造成的时间抖动的分布情况,以及时间抖动的缓慢漂移情况,通过这些数据可以清楚地看到,在 Alice 端注入长程光纤的相邻两个光脉冲在经历了长距离传输后,这两个脉冲之间的时间间隔发生了随机变化,在不同条件下变化的情况有所不同. 以上的测量是针对工作频率为 1 MHz 的差分相位编码系统进行的,之所以选择 1 MHz 的工作频率,是因为目前最常用的基于雪崩光电二极管的红外单光子探测器的工作频率一般为 1 MHz 的量级. 对于该工作频率,相邻两个光脉冲之间的时间间隔为 1 μs,经过长程光纤传输后,在实际应用环境的影响下,测量结果为几十 ps 的时间抖动,当然,由于在我们所采用的测量装置中存在由于光电转换和示波器本身造成的时间抖动,会使测量结果偏大,但是通过不同传输距离和不同外界环境影响的对比来看,这种时间抖动确实存在. 而基于弱相干激光脉冲的差分相位编码系统的时间抖动来自于所采用电时钟源的时间抖动和长程光纤传输带来的时间抖动,二者相比较,前者引起的时间抖动会大得多.

2.2. 基于双不等臂 M-Z 相位编码系统时间抖动的测量

目前文献中关于相邻很近的由 M-Z 光纤环分裂的两个光脉冲的干涉也没有考虑不完全重合引起的误码. 基于同样的考虑,我们也通过对 M-Z 光纤环分裂的两个光脉冲的时间间隔进行了统计测量,结果表明,这种影响依然存在,也同时决定了系统具有由随机时间抖动造成的误码率极限.

图 7 为测量 M-Z 系统光脉冲时间间隔抖动的装置图.

图 7 中,采用时钟源触发脉冲激光器(PDL820),经过自制的 M-Z 干涉环后分为两个间隔大约为 15ns 的一对光脉冲,在双不等臂 M-Z 相位编码系统中,这两个光脉冲通过 Bob 端的另一个对称的 M-Z 干涉检测环延迟后进行干涉叠加,输出到相应的单光子探测器,根据编码规则产生密钥信息. 利用具有统计测量功能的示波器对这两个光脉冲在长程光纤中的传输延迟进行测量.

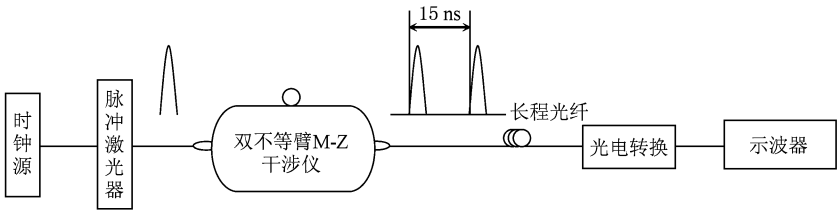

图 7 双不等臂 M-Z 相位编码系统光脉冲传输延迟抖动测量装置

2.2.1. 实验室环境下不同传输距离时间抖动分布的测量

图 8 是在实验室环境下两个相距 15 ns 的光脉冲之间的时间抖动分布.

取 10000 个采样点,测量不同传输距离时的传输延迟时间抖动. 图中,峰值最高的曲线为传输距离为 0 km 时的时间抖动曲线,向下依次为 25,50 和 75 km 时的时间抖动分布.

从图中可以看出,随着传输距离的增加,由于长程光纤的传输延迟造成的时间抖动也逐渐增加,对数据进行统计分析,相关数据如表 3 所示.

通过表 3 可以看出,基于双 M-Z 相位编码系统的光脉冲由于时间间隔较小,并且是由一个固定的 M-Z 光纤环产生的,因此可以较好地保持一对光脉冲之间的时间间隔,但是随着传输距离的增加,两个光脉冲之间的间隔也会发生一定的时间抖动,影响了长程传输时的误码率.

2.2.2. 75 km 传输距离户外光纤上的时间抖动分布测量

以下测量户外光纤 75 km 长距离传输的时间抖动分布变化情况. 图 9 为长程光纤置于户外,当温度在一定范围内变化时,时间抖动的分布变化情况.

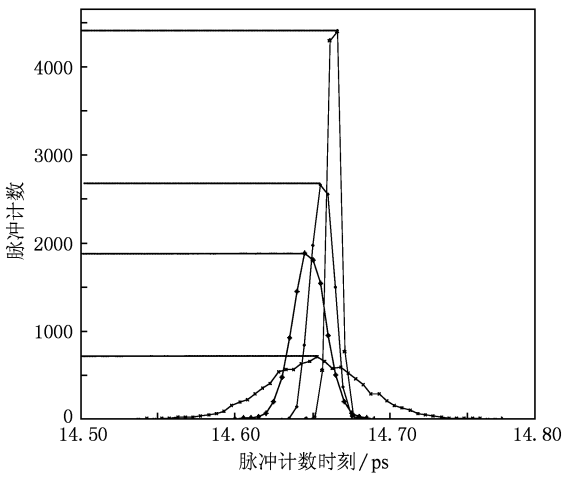

图 8　双 M-Z 相位编码系统长程光纤传输延迟时间抖动分布

表 3　实验室环境下不同传输距离的时间抖动分布

光纤长度/km	全宽/ps	半宽/ps	最大计数
0	25	10	4392
25	45	20	2651
50	50	25	1878
75	230	65	698

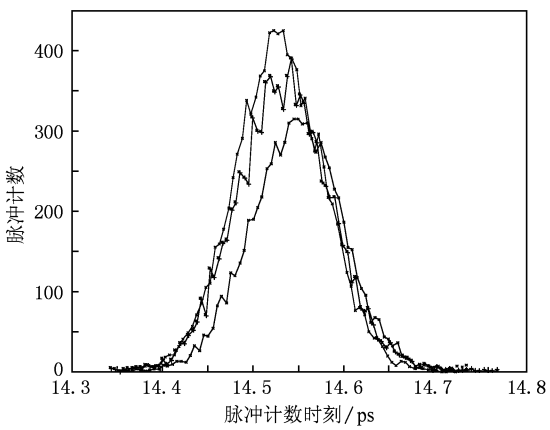

图 9　75 km 户外光纤传输时间抖动分布变化情况

图中，从左至右三条曲线分别为温度变化过程中在 23，28 和 36 ℃时采样得到的分布曲线. 将数据进行统计，列出表 4 所示的时间抖动的变化数据.

表 4　75 km 传输距离户外光纤时间抖动分布的统计数据

温度/℃	全宽/ps	半宽/ps	最大计数
23	300	115	424
28	355	125	397
36	385	140	340

从图 9 和表 4 可以看出，随着外界实际应用环境的变化，两个光脉冲在长程光纤传输的延迟时间也发生了时间抖动的变化，表现为抖动分布变宽，并且中心峰值的位置也在发生缓慢的漂移.

按照同样的方法测量了 M-Z 系统中，两个光脉冲的时间间隔最大概率取值的漂移情况.

图 10 为 75 km 户外光纤传输时间抖动漂移情况的变化，图 10 中，星点为温度缓慢上升时的测试数据，圆点为温度缓慢下降时的测试数据. 从以上两图可以看出，随着外界环境的变化，这两个光脉冲之间的时间间隔也在发生不同程度的变化，也就是说随着外界环境的变化，并不像目前文献中所提到的，将 Alice 和 Bob 端的 M-Z 光纤环的光程差设置成完全相同即可实现光脉冲的完全叠加，从 Alice 分裂出的两个光脉冲经过长程光纤传输延迟后，在实际应用环境下，对 Bob 光纤环臂长差的需求也在发生变化，如果固定 Bob 光纤环的光程差也无法得到理想的干涉，长程光纤传输的时间延迟在系统中和差分相位编码系统一样会造成系统的误码率上升.

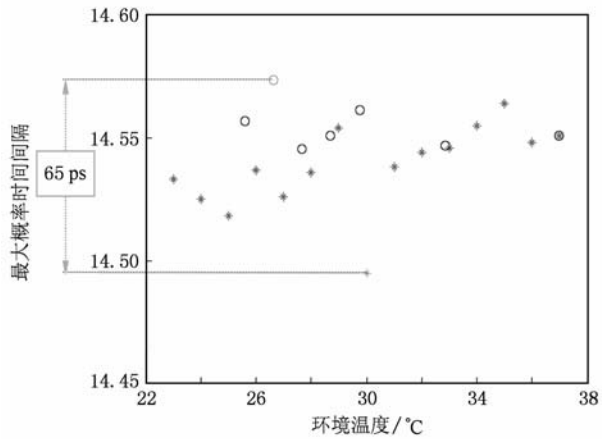

图 10　75 km 户外光纤传输时间抖动漂移的变化

2.2.3. 实验结果分析

以上的测量结果很明显比差分相位编码系统中的时间抖动要小得多，原因是基于双不等臂 M-Z 相位编码系统的时间抖动的原因不再包含像弱相干光差分相位编码系统中的时钟引起的时间抖动，从 Alice 端分裂的两个光脉冲的起始时间间隔的不同主要来自于 Alice 端光纤环随外界环境变化引起的时间间隔的变化，这个变化是非常小的，并且由于 Alice 端的光纤环放置在室内进行应用，受到外界环境的影响可以通过光纤环的被动补偿来进一

步减小,根据文献[20]的计算,光纤环引起的时间抖动相比较光脉冲的宽度来看是非常小的,对系统误码率的贡献也非常小. 实验结果中,同样由于受到了光电转换和示波器的时间抖动的影响,实际的两个光脉冲的时间间隔抖动会更小一些.

2.3. 讨 论

从以上基于弱相干光差分相位编码系统和双不等臂 M-Z 相位编码系统中光脉冲经过长程光纤传输延迟的测量,看出在长程光纤传输时会由于传输时间的随机分布造成光脉冲在合束器上可能发生非理想的干涉叠加而造成系统误码率的增大,使某些光子信息在密钥比特产生过程中进一步丢失. 实验结果由于受到电仪器的影响会使测得的时间抖动加大,但是通过不同传输距离和实际应用环境下在同样测量条件下的比较,看到光脉冲的传输延迟会随着传输距离的增加而增大,尤其是传输距离增大到近百公里时,这种传输延迟造成的时间抖动也会显著增加,从而影响系统的误码率. 这种时间抖动通过光脉冲传输进行统计测量具有一定的局限性,更适当的方法是根据时间抖动的现象建立误码率和时间抖动的物理模型,给出系统误码和时间抖动的关系,并根据系统误码的结果进一步估算时间抖动对于系统误码的影响. 在下一节内容中我们对这种时间抖动引起的不完全重合干涉对误码率的影响进行了理论分析,得出了相关的物理模型.

3. 长程光纤中传输延迟引起系统误码率的理论分析

通过时间抖动的分布曲线,可见两个光脉冲时间间隔为某一个 t 值时的概率,如果可以分析两个脉冲时间间隔为 t 时,由于不完全重合干涉叠加时的误码率,那么对这个误码率的结果进行随机分布的加权积分后即可得到系统在长程光纤传输时长时间的误码率结果.

如图 11 所示,假设光脉冲波形函数为 $f(t)$,两个光脉冲的时间间隔为 T,光脉冲的全宽为 τ_p,则可以根据干涉叠加的情况分为三个区域:一是 $t=0\rightarrow T$,这部分没有干涉叠加,如果在这段时间内探测到光子,那么从合束器输出的光子将等概率地从两个探测器输出,误码率为 50%;第二个区域是 $t=T\rightarrow\tau_p$,这个区域是两个脉冲发生干涉叠加的区域,在以下计算中,假设可以用主动相位补偿的方法使得这个区域发生干涉叠加的两个光脉冲具有理想的调制相位;第三个区域是 $t=\tau_p\rightarrow\tau_p+T$,这个区域也是没有发生干涉叠加的区域,如果在这段时间内探测到光子,那么在合束器上的输出也是等概率到达两个探测器,误码率为 50%.

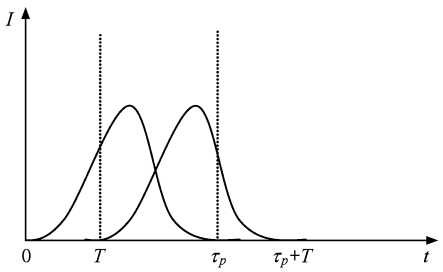

图 11 两个光脉冲不完全重合时的干涉叠加情况

下面计算当两个光脉冲不完全重合时干涉叠加的误码率. 根据干涉叠加的误码率公式

$$\mathrm{QBER}(T)=\frac{1-V}{2}. \tag{1}$$

将 QBER 写为 T 的函数,是因为计算的是两个光脉冲延时为 T 的误码率,其结果应该是 T 的函数. V 为干涉对比度,定义为

$$V=\frac{I_{\max}-I_{\min}}{I_{\max}+I_{\min}}, \tag{2}$$

式中,$I_{\max}$ 和 $I_{\min}$ 分别为干涉叠加时最大输出光强和最小输出光强.

根据(1)和(2)式得出

$$\mathrm{QBER}(T)=\frac{I_{\min}}{I_{\max}+I_{\min}}. \tag{3}$$

由于设光脉冲光强分布函数为 $f(t)$,则在图 11 坐标系中,第二个光脉冲光强分布函数可以表示为 $f(t-T)$,以下采用对上述三个区域进行积分,得出误码率和延时参数 T 之间的关系.

根据(3)式,可以得到

$$\mathrm{QBER}(T)=\frac{\int_0^T f(t)\,\mathrm{d}t+\int_{\tau_p}^{\tau_p+T} f(t-T)\,\mathrm{d}t+\int_T^{\tau_p}\left[f(t)+f(t-T)-2\sqrt{f(t)\cdot f(t-T)}\right]\mathrm{d}t}{2\int_0^T f(t)\,\mathrm{d}t+2\int_{\tau_p}^{\tau_p+T} f(t-T)\,\mathrm{d}t+\int_T^{\tau_p}\left[f(t)+f(t-T)-2\sqrt{f(t)\cdot f(t-T)}\right]\mathrm{d}t+\int_T^{\tau_p}\left[f(t)+f(t-T)+2\sqrt{f(t)\cdot f(t-T)}\right]\mathrm{d}t}. \tag{4}$$

将上式变形后可以得到

$$\mathrm{QBER}(T)=\frac{\int_0^T f(t)\,\mathrm{d}t+\int_{\tau_p}^{\tau_p+T} f(t-T)\,\mathrm{d}t+\int_T^{\tau_p}[f(t)+f(t-T)-2\sqrt{f(t)\cdot f(t-T)}]\,\mathrm{d}t}{2\int_0^T f(t)\,\mathrm{d}t+2\int_{\tau_p}^{\tau_p+T} f(t-T)\,\mathrm{d}t+2\int_T^{\tau_p}[f(t)+f(t-T)]\,\mathrm{d}t}$$

$$=\frac{1}{2}-\frac{\int_T^{\tau_p}\sqrt{f(t)\cdot f(t-T)}\,\mathrm{d}t}{\int_0^{\tau_p} f(t)\,\mathrm{d}t+\int_T^{\tau_p+T} f(t-T)\,\mathrm{d}t}. \tag{5}$$

(5)式为光强分布函数为一般形式 $f(t)$ 时不完全重合干涉叠加引起的误码率结果. 从这个结果可以看到当 $T=0$ 时,误码率 $\mathrm{QBER}(T)=0$,而当 $T>\tau_p$ 时,(5)式中第二项的分子所代表的干涉向将等于0,此时的误码率等于50%,和我们实际分析的物理模型是相符合的.

以上得到了任意两个相邻光脉冲在相对延时时间为 T 时的误码率公式,接下来根据脉冲之间相对延时的统计分布来计算系统长期工作的误码率.

可以设时间抖动的统计分布函数为 $\psi(T)$,这个分布函数表示了不同时延 T 的概率分布. 也就是说,延时时间为 T 的不完全干涉叠加的概率是 $\psi(T)$,那么系统长期工作的误码率表达式为

$$\int_{-\tau}^{\tau}\mathrm{QBER}(T)\cdot\psi(T)\,\mathrm{d}T. \tag{6}$$

如果 $\psi(T)$ 不是归一化函数,则上式的结果必须归一化

$$\frac{\int_{-\tau}^{\tau}\mathrm{QBER}(T)\cdot\psi(T)\,\mathrm{d}T}{\int_{-\tau}^{\tau}\psi(T)\,\mathrm{d}T}. \tag{7}$$

(7)式即为量子密钥分发系统在长期工作时由于时间抖动引起误码率的表达式.

4. 结　　论

通过以上的实验测量和相关理论分析可知,基于相位编码的量子密钥分配系统在实际应用中进行长程传输时,时间抖动会对系统误码率产生不同程度的影响. 对于双不等臂 M-Z 相位编码系统,主要是通信双方的光学延迟环和长程光纤引起的传输延迟对误码率有一定的影响,这种传输延迟造成的时间抖动在 M-Z 干涉仪分开的光脉冲时间间隔很小时取值也比较小,对误码率的影响相对于其他环节而言是比较小的,但是基于弱相干光的差分相位编码系统同时需要精密的时钟源,以减小 Alice 端发射的相邻两个光脉冲之间的时间间隔的抖动,但是再加上实际应用中户外商用光纤引起的光脉冲的传输延迟,造成光脉冲不完全重合引起的误码,这个误码在长程光纤传输的实际应用中是无法避免的. 从这个角度上来说,提高差分相位编码系统的工作频率以及减小双不等臂 M-Z 系统两个相干脉冲之间的时间间隔,对误码率将有改善作用. 同时,在工作频率较低的系统中,采用更短的光脉冲将造成更严重的误码率. 针对这个特点,采用一定方法(例如根据缓慢时间间隔漂移的特点对 Bob 端的光纤延迟环进行相应延迟时间的补偿)可以进一步减小误码率,减小光子调制密钥信息的丢失.

[1] Wiesner S 1983 *SIGACT News* **15** 78

[2] Bennett C H, Brassard G 1984 *Proceedings of the IEEE International Conference on Computers, Systems, and Signal Processing*, Bangalore, India, New York: IEEE 1984 p175

[3] Hwang W Y 2003 *Phys. Rev. Lett* **91** 057901

[4] Kurtsiefer C, Zarda P, Halder M, Weinfurter H, Gorman P, Tapster P R, Rarity J G 2002 *Nature* **419** 450

[5] Tobias S M, Henning W, Martin F, Rupert U, Felix T, Thomas S, Josep P, Zoran S, Christian K, John G R, Anton Z, Harald W 2007 *Phys. Rev. Lett.* **98** 010504

[6] Stucki D, Gisin N, Guinnard O, Ribordy G, Zbinden H 2002 *New J. Phys.* **4** 41

[7] Hiskett P A, Rosenberg D, Peterson C G, Hughes R J, Nam S W, Lita A E, Miller A J, Nordholt J E 2006 *New J. Phys.* **8** 193

[8] Elliott C, Colvin A, Pearson D, Pikalo O, Schlafer J, Yeh H 2005 *Proceedings of the SPIE*, May 25, p138

[9] Poppe Andreas, Peev M, Maurhart O 2008 *Int. J. Quantum Inf.* **6** 2

[10] Wang J D, Lu W, Zhao F, Liu X B, Guo B H, Zhang J, Huang Y X, Lu Y Q, Liu S H 2008 *Acta Phys. Sin.* **57** 4214 (in Chinese) [王金东、路 巍、赵 峰、刘小宝、郭邦红、张 静、黄宇娴、路轶群、刘颂豪 2008 物理学报 **57** 4214]

[11] Hu H P, Zhang J, Wang J D, Huang Y X, Lu Y Q, Liu S H, Lu W 2008 *Acta Phys. Sin.* **57** 5605 (in Chinese) [胡华鹏、张静、王金东、黄宇娴、路轶群、刘颂豪、路 巍 2008 物理学报 **57** 5605]

[12] Wang J D, Qin X J, Zhang H N, Wei Z J, Liao C J, Liu S H 2009 *Optics Communications* **282** 3379

[13] Gisin N, Ribordy G, Tittel W, Zbinden H 2002 *Rev. Mod. Phys.* **74** 145

[14] Inoue K, Waks E, Yamamoto Y, 2002 *Phys. Rev. Lett.* **89** 037902

[15] Takesue H, Diamanti E, Honjo T, Langrock C, Fejer M, Inoue K, Yamamoto Y 2005 arXiv: 0507110 [quant-ph]

[16] Townsend P D, Rarity J G, Tapster P R 1993 *Elect. Lett.* **29** 634

[17] Yuan Z L, Shields A J 2005 *Opt. Exp.* **13** 660

[18] Trifonov A, Zavriyev A, Denchev V, Leverrier A 2007 *J. Modern Opt.* **54** 305

[19] Makarov V, Brylevski A, Hjelme D R 2004 *Appl. Opt.* **43** 4385

[20] Chen W, Han Z F, Mo X F, Xu F X, Wei G, Guo G C 2008 *Chinese Science Bulletin* **53** 9

The influence of the time delay through long trunk fiber on the phase-coding quantum key distribution system*

Wang Jin-Dong[1)†] Wei Zheng-Jun[1)] Zhang Hui[2)] Zhang Hua-Ni[1)] Chen Shuai[1)]
Qin Xiao-Juan[3)] Guo Jian-Ping[1)] Liao Chang-Jun[1)] Liu Song-Hao[1)]

1) (*Key Laboratory of Photonic Information Technology of Guangdong Higher Education Institutes, School for Information and Optoelectronic Science and Engineering, South China Normal University, Guangzhou* 510006, *China*)

2) (*Physics Teaching and Research Section, Artillery Academy of Chinese People's Liberation Army, Hefei* 230031, *China*)

3) (*Guangdong Radio and TV University, Guangzhou* 510091, *China*)

(Received 22 October 2009; revised manuscript received 24 November 2009)

Abstract

Optical pulse will reach the receiver not at exact time instance due to the transmission through the long trunk fiber, and this phenomenon will effect on the bits error rate in the Quantum key distribution (QKD) system to some extend. The time jitter based on the differential phase shift quantum key distribution system and two asymmetric Mach-Zehnder interferometers is measured outdoors in different transmission distance and the physical model of the relationship between the time jitter and the quantum bit error rate is proposed. According to this relationship, the quantum bit error rate can be estimated for some optical pulse shape and some statistical distribution function.

Keywords: quantum key distribution, phase-encoding, time jitter, quantum bit error rate

PACC: 4250, 0367, 4230Q, 9575K

* Project supported by the Key Projects in the Guangzhou Science and Technology Pillar Program (Grant No. 2008Z1-D501), the Guangdong Key Technologies R and D Program (Grant No. 2007B010400009), the Guangdong polytechnic institute scientific research fund (Grant No. 0901)

† E-mail: jindongwqkd@126.com