一种基于确定性量子密钥分发误码判据的相位调制器半波电压的精确测定方法*

魏正军[1)] 万 伟[2)] 王金东[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省高校重点实验室,广州 510006)

2)(广东广播电视大学,广州 510091)

(2011 年 2 月 4 日收到;2011 年 4 月 1 日收到修改稿)

基于相位编码的量子密钥分发系统需要对信息加载的相位调制器的半波电压进行精确的测定以减小量子密钥的误码率,相位调制器半波电压的测量精度直接影响到了量子密钥分发系统的最终误码. 本文提出了一种基于确定性量子密钥分发误码率判据的相位调制器半波电压的精确测定方法,所采用相位调制器的半波电压的测量精度达到了 2 mV,实验结果表明这种方法可以用于量子密钥分发实际应用系统中实时获得不同条件下的行波相位调制器的半波电压以最大程度地减小由于相位信息不准确加载而带来的系统误码.

关键词: 量子保密通信, 相位编码, 半波电压, 误码率

PACS: 42. 50. Ar,03. 67. – a,42. 79. Sz,95. 75. Kk

1. 引 言

量子密码的最初思想是 1969 年 Wiesner 首先提出来的[1]. Bennett 和 Brassard 在 Wiesner 思想的启发下,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.

量子保密通信系统的安全性是基于物理学的基本原理,利用单量子作为密钥传输的载体,并和经典保密通信领域中唯一被证明是安全的等长度的一次一密的密码体制相结合,为信息安全领域提供了一种可行的,理论上被证明绝对安全的通信机理. 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,在近 30 年的时间里,该领域无论从理论、实验,还是相关关键技术方面都取得了显著的进展[3—13],成为量子光学领域最接近实际应用的方向之一,其广泛的应用前景也普遍受到了包括军事、商业、外交、金融等各领域的重视.

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[14]. 对于相位编码系统,目前常见的系统有双不等臂 Mach – Zehnder 相位编码系统和差分相位编码系统. 无论是采用 BB84 协议的相位编码系统,还是采用差分协议的相位编码系统,密钥信息的加载以及实际系统中的随环境漂移的相位跟踪和主动补偿都需要用到系统所采用相位调制器的半波电压[15—17],而半波电压的准确程度直接决定了单光子干涉的相位误差,进而影响了获得量子密钥的误码率. 如果同时需要针对外界环境引起的相位漂移进行主动相位补偿,那么主动补偿的过程也需要不断进行加载相位电压的溢出处理[15—17]. 相位电压的溢出处理指的是当所加载的相位电压大于驱动电路所能提供的电压时,需要将预加载的相位电压减小两倍半波电压以防止相位电压的溢出出错,那么每做一次溢出处理就叠加一倍的半波电压的测量误差,尤其是针对弱相干光的差分相位编码系统的主动相位补偿则需要不断累加相位电压和进行溢出处理,那么半波电压的准确程度就非常关键. 另一方面,在目前

* 广州市科技支撑计划(批准号:2008Z1 – D501)和广东省工业攻关项目(批准号:2007B010400009)资助的课题.

† 通讯联系人. E-mail:jindongwqkd@126. com

的相位编码量子密钥分发系统中一般都采用铌酸锂行波相位调制器,这种行波相位调制器在不同的条件下半波电压的数值稍有差别,即使可以采用某些方法高精度测定半波电压,但是当量子密钥分发系统的某些条件发生变化时(如单光子脉冲发射速率变化,相位调制器半波长期工作半波电压的不稳定性等),半波电压的数据仍旧不能满足系统的需要,因此在量子密钥分发系统的实际应用中,寻找一种能够实时、高精度测定半波电压的方法以进行量子密钥信息加载和检测具有较大的实用价值.

本文提出了一种可以应用在量子密钥分发实际应用系统中的可以实时、高精度测定相位调制器半波电压的方法,该方法通过单光子干涉曲线等待法阈值判断后进行确定性量子密钥分发,并通过该确定性密钥分发[18,19]的误码率来测定相位调制器的半波电压,实验采用的测量精度为 2 mV,并给出了根据误码率确定半波电压的方案. 这种方法由于采用了单光子干涉计数的方法来测定半波电压,所以可以在不增加任何硬件的条件下直接应用于量子密钥分发的实际应用系统实时获得精确度高的半波电压以减小系统的误码率.

2. 基于确定性量子密钥分发误码判据的相位调制器半波电压的测定方法

该方法的基本思想是当相位调制器不加载任何驱动电压时,外界环境变化导致的干涉系统的相位漂移将导致单光子计数结果在最大值和最小值之间来回变化. 通过计算机程序实时判断外界相位漂移为 π 的整数倍的时刻,一旦外界相位漂移为 π 的整数倍,则其中一个单光子探测器的计数结果将达到最小,另一个单光子探测器的计数结果将达到最大,此时 Bob 端通知 Alice 端加载始终为 1 的确定性密钥信息(即每相邻两个单光子脉冲的相位差总为 π)并开始进行密钥信息的检测,一旦当 Alice 加载了始终为 1 的确定性密钥信息,那么在理想条件下输出口的两个单光子探测器的计数结果将发生突变,即计数结果为最大值的探测器的计数结果将变为最小,计数结果为最小值的探测器的计数结果将变为最大. 我们根据这两个探测器的计数结果按照协议的密钥规则可以得到确定性密钥分发的误码率,当在相位调制器上加载的半波电压的误差越小时,系统的误码率也越小,我们在粗测相位调制器的半波电压得到大致数据后,按照该方法即可得到使得系统误码率最小的半波电压的数据,该数据即为最优化的半波电压的结果.

2.1. 测量方案

以下我们采用基于弱相干光的差分相位编码系统来说明利用确定性量子密钥分发误码判据来测定相位调制器半波电压的测定方法.

图 1 是基于弱相干光差分相位编码量子密钥分发系统的示意图[20]. 1550 nm 的窄线宽连续激光器发射的连续激光经过强度调制器(IM, JDSU-2.5 GHz)调制成矩形激光脉冲,每个激光脉冲经过相位调制器(PM, Sumitomo-2.5G-1550)加载相位信息,之后通过衰减器(ATT, Exfo-FVA-3100)进行强衰减,衰减为安全密钥生成率最优化的平均每脉冲 0.2 个光子[21],通过传输光纤发送到 Bob 端. Bob 端通过一个单比特 M-Z 干涉环进行干涉检测后获得密钥信息. 在密钥分发过程中,Alice 端的相位调制器随机调制 0 或 π 的相位,在 Bob 端则根据所调制的相位差从单光子探测器 SPD1 (ID Quantique, ID201)或 SPD2(ID Quantique, ID201)输出,形成光子计数.

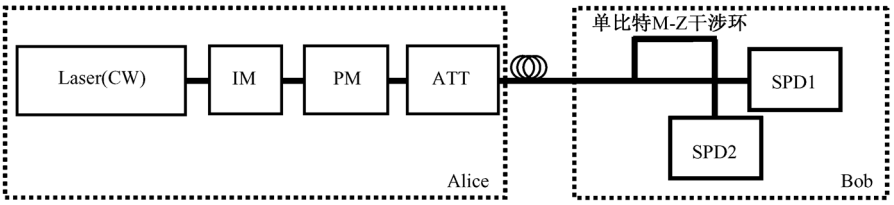

图 1 基于弱相干光差分相位编码量子密钥分发系统的示意图

Alice 端加载 π 的相位对应相位调制器加载相应工作条件下的半波电压,如果半波电压的测量数值不准确,则在 Bob 端的干涉结果就有一定的概率从另外一个单光子探测器输出,从而形成系统误码. 同时由于 Bob 端的干涉环存在外界环境影响的相位漂移,因此需要进行动态相位漂移参数的跟踪

补偿以使得系统可以长期稳定工作,而在主动相位补偿的过程中同样需要准确的半波电压数据,差分相位编码系统的特点使得在主动相位补偿过程中,半波电压的测量误差被快速叠加,使得系统误码急剧增加,甚至无法进行密钥分发.

当 Alice 端的相位调制器不加载任何相位(即相位调制器加载电压始终为零)时,由于 M-Z 干涉仪受到外界环境的影响,其固有相位差将不断发生变化,此时 Bob 端干涉仪后的单光子探测器的计数值将随着相位差的变化而进行正弦曲线的变化,不断交替出现计数的最大值和最小值,且两个单光子探测器的计数输出完全互补,光子计数输出满足下式[17]:

$$N_1 = (N_{\max} - N_{\min})\sin^2\left(\frac{\phi_{\rm pm} + \phi_{\rm h}}{2}\right) + N_{\min}, \quad (1)$$

$$N_2 = (N_{\max} - N_{\min})\sin^2\left(\frac{\phi_{\rm pm} + \phi_{\rm h} + \pi}{2}\right) + N_{\min}, \quad (2)$$

其中,$N_{\max}$ 为干涉输出的最大光子计数值,$N_{\min}$ 为干涉输出的最小光子计数值,在不考虑光路中的其他因素(如干涉叠加时两路光子概率不等,偏振变化等因素)时等于单光子探测器的暗计数. 干涉环的附加相位 $\phi_{\rm h}$ 除了光纤环制作过程中长度差引起的固定相位差以外,还会由于外界环境的影响随时间发生不断变化,这种随机的相位变化使得干涉输出也会发生改变,进而影响相位编码信息的检测. 每个单光子探测器输出的最小值是该点干涉相消的计数输出,我们通过仔细控制干涉仪两臂的偏振状态使得最小计数的输出尽量小,在 260 kHZ 的工作频率和计入单光子探测器暗计数的情况下,干涉对比度可达 97.3%.

利用确定性量子密钥分发误码判据精确测定相位调制器半波电压的第一步是控制系统对每 4×10^3 个单光子脉冲的干涉结果进行计数,之所以选择 4×10^3 个单光子脉冲进行干涉结果的计数处理,是因为光子统计的特征一般要选择在 1×10^3 以上才能够体现出来[15]. 4×10^3 个单光子脉冲的干涉结果的计数结果正像(1)式和(2)式一样随着外界环境引起的相位变化呈现正余弦变化规律,我们可以在较长周期(大于外界环境引起相位变化量为 2π 的时间)内对两个单光子探测器计数后得到 4×10^3 个单光子干涉脉冲输出的计数值,这些计数值中肯定会出现最大值和最小值,分别记为 $N_{1,\max}N_{2,\max}$, $N_{1,\min}$ 和 $N_{2,\min}$.

第二步是控制系统利用计数结果实时判断随外界引起相位变化的数值为 π 的整数倍的时刻. 具体方法是,累计 4×10^3 个单光子干涉脉冲的输出形成一个计数点,控制系统得到计数点的数据后进行实时判断,判断条件为

$$N_1 < N_{1,\max}\times3\% \quad \text{或者} \quad N_2 < N_{2,\max}\times3\%.$$

在理想情况下,相位差为 π 的整数倍时,N_1 或 N_2 应该达到零,但是由于系统中单光子探测器暗计数的影响和光学元器件不理想的特性等原因,得到的计数结果是不可能等于零的. 我们调节判断条件为 3% 倍的计数最大值,主要是在实验中最大值的 3% 倍略大于暗计数的值,在实际系统中这个参数可以根据系统性能选择,例如在传输距离较长或所用单光子探测器暗计数较高时可以提高这个参数的数值,其原则是判断参数($N_{\max}\times3\%$)略大于在考虑单光子探测器暗计数情况下系统能够达到的最小干涉计数输出. 例如,我们调节每脉冲光子数为 0.2,两个单光子探测器得到的 4×10^3 个单光子脉冲的累计最大计数值为 100 左右,选择判断条件为 3%,即当 4×10^3 个单光子脉冲的累计计数达到小于 3 时,即认为满足了相位条件.

第三步是当外界环境引起的相位漂移满足上述相位条件时,Bob 通知 Alice 马上进行确定性量子密钥分发. 当 Bob 端的控制系统判断 4×10^3 个单光子脉冲的累计计数结果小于判断阈值,马上向 Alice 发出一个信号,告知 Alice 开始进行确定性量子密钥分发过程,这个确定性量子密钥分发过程指的是在差分相位编码系统中逐次在单光子脉冲上加载 0 和 π 的相位调制,即在相位调制器上交替加载 0 和 V_π 的调相电压,按照密钥规则这种调制方式为全 1 的确定性量子密钥分发. 由于系统存在单光子探测器暗计数等因素的影响,为了提高误码率判据的数据可靠性,我们在统计确定性量子密钥分发的误码率时,将全 1 量子密钥分发的单光子脉冲的数量提高到 42 kHz.

第四步是根据确定性量子密钥分发的误码率来精确测定相位调制器的半波电压. 在 Alice 进行了全 1 的确定性量子密钥分发后,Bob 端根据接收到的单光子探测结果计算误码率,当相位调制器的 V_π 误差越小时,得到的量子密钥的误码率也越小. 系统采用了住友公司的 2.5 GHz 带宽的铌酸锂行波相位调制器,我们利用强光赛格纳克环的方法测得该调制器在 260 kHz 时半波电压为 3.8 V. 在确定性量子密钥分发的过程中,当满足相位条件时我们改

变加载的半波电压得到对应的确定性密钥分发的误码率数据如图 2,相位调制器加载电压的变化精度为 2 mV,根据图 2 我们可以得到在 2 mV 的精度下,当加载电压为 3.26 V 时,扣除阈值判断引起的误码,相位调制器相位电压加载不准确引起的误码最小为 1.22%,该电压即为精度为 2 mV 的半波电压的精确数据.

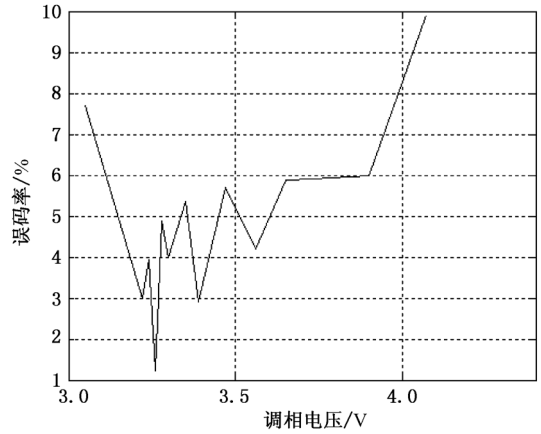

图 2 相位调制器调相电压和确定性量子密钥分发误码率之间的关系

2.2. 实验结果分析

以上我们通过确定性量子密钥分发误码判据精确地测定了系统所用相位调制器的半波电压,得到了精度为 2 mV 的对应工作频率下的半波电压的数据. 从图 2 可以看出,当所加载的调相电压和准确的半波电压差距越大时,系统密钥分发的误码率也越大,而准确的半波电压所对应的系统误码率应该是最低的,所测试的误码率曲线也呈现明显的趋势. 假设半波电压测量数据和最优化半波电压数据之间的偏差为 ΔV, 则由于此偏差产生的相位偏差为: $\Delta\varphi = \dfrac{\Delta V}{V_\pi}\pi$. 在差分相位量子密钥分发系统中,从光学系统的角度考虑,如果两个相干涉的单光子概率幅脉冲之间的相位差为 π,则干涉输出的单光子会全部从对应的单光子探测器输出并形成密钥信息. 如果存在相位偏差,则发送端调制的相位信息会有一定概率进入另外一个探测器形成误码,系统误码 QBER 和相位偏差 $\Delta\varphi$ 之间的关系为[17]

$$\mathrm{QBER}_{\Delta\varphi} = \sin^2\left(\frac{\Delta\varphi}{2}\right). \tag{3}$$

如果不考虑由于电路问题引起的加载电压的偏差,则由于半波电压的偏差 ΔV 与系统误码率之间的关系为

$$\mathrm{QBER}_{\Delta V} = \sin^2\left(\frac{\Delta V\pi}{2V_\pi}\right). \tag{4}$$

图 2 中的实验数据充分说明了以上定量关系,同时这个特征可以使得我们能够有效利用本文提出的方法获得高精度的相位调制器的半波电压数据. 在实验数据中,也有一些特别的数据,这些数据显示在更接近半波电压时,误码率反而出现小范围的减小,这种减小和总的变化趋势有所差别,其原因应该来自于光子计数和暗计数的统计起伏,通过在密钥分发过程中增加量子密钥分发的误码统计脉冲数可以在一定程度上减小这种现象.

3. 结 论

通过以上的分析和实验数据可以看到,在相位调制器不加载任何相位信息时,外界环境引起的相位变化使得单光子脉冲干涉计数的输出呈现正余弦变化的规律,我们利用这种规律找到相位差为 π 的整数倍的时刻,然后在该时刻进行全 1 的确定性量子密钥分发,如果调相电压不准确时,将给系统的量子密钥带来附加的误码,而当附加误码最小时,对应的调相电压即为半波电压. 本文基于差分相位编码系统通过该方法精确测定了精度在 2 mV 范围内的相位调制器半波电压的数据,并得到了小到 4.22% 的系统总误码,考虑阈值引起的判断误码,调相电压加载不准确所引入的误码仅为 1.22%.

利用这种方法得到的半波电压的数据在量子密钥分发的相位调制、检测以及主动相位补偿等各个环节将得到最小的系统误码. 在实际应用的量子密钥分发系统中,铌酸锂行波相位调制器会随着工作频率等条件的变化而有所差别,我们可以将以上的方法通过计算机控制系统设置为工作条件改变后的初始化程序的一部分,这样当系统工作条件改变时就可以保证系统仍旧能够有效地运行.

[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, 2005 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、路铁群、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、路铁群、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] Wang J D, Wei Z J, Zhang H, Xiao J Q, Liu X B, Zhang Z M, Liao C J, Liu S H 2010 *J. Phys.* B: *At. Mol. Opt. Phys.* **43** 095504

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

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

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

[17] Wang J D, Qin x J, Liu X B, Liao C J, Liu S H 2010 *Acta Phys. Sin.* **59** 281 (in Chinese) [王金东、秦晓娟、刘小宝、廖常俊、刘颂豪 2010 物理学报 **59** 281]

[18] Zhou N R, Wang L J, Ding J, Gong L H 2010 *Physica Scripta.* **81** 045009

[19] Zhou N R, Wang L J, Ding J, Gong L H 2010 *International Journal of Theoretical Physics* **49** 2035

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

[21] Takesue H, Sae W N, Qiang Z, Robert H, Toshimori H, Kiyoshi T, Yamamoto Y 2007 *Nat. Photonics* **1** 343

A new method to acquire the half-wave voltage by the quantum bit error rate in the deterministic quantum key distribution system*

Wei Zheng-Jun[1)] Wan Wei[2)] Wang Jin-Dong[1)†] Liao Chang-Jun[1)] Liu Song-Hao[1)]

1) (*Laboratory of Photonic Information Technology SIPSE & LQIT, South China Normal University, Guangzhou* 510006, *China*)

2) (*Guangdong Radio&TV University, Guangzhou* 510091, *China*)

(Received 4 February 2011; revised manuscript received 1 April 2011)

Abstract

The value of the half-wave voltage of the phase modulator must be measured with high accuracy to reduce the quantum bit error rate (QBER) in a quantum key distribution system based the phase-coding scheme. A new method to measure the half-wave voltage of the phase modulator in an accuracy of 2 mV by adjusting the quantum bit error rate (QBER) of the deterministic quantum key distribution is proposed experimentally to increase the accuracy of the half-wave voltage and reduce the error rate of the quantum key distribution system. The experimental results show that this method can be used to acquire efficiently the half-wave voltage of the phase modulator in a high accuracy which can make the error rate from adding the inaccurate voltage to the phase modulator decrease to the greatest extent.

Keywords: quantum cryptography, phase-encoding, half-wave voltage, quantum bit error rate

PACS: 42.50.Ar, 03.67-A, 42.79.Sz, 95.75.Kk

* Project supported by the Key Projects in the Guangzhou Science & Technology Pillar Program (Grant No. 2008Z1-D501) and by the Guangdong Key Technologies R&D Program (Grant No. 2007B010400009).

† Corresponding author. E-mail: jindongwqkd@126.com