引用本文：黄彪，韩贺松，黄永梅，等. CVQKD 中块平均参考相位估计算法的性能优化[J]. 光通信技术，2021，45(6)：18-21.

CVQKD 中块平均参考相位估计算法的性能优化

黄 彪[1-5]，韩贺松[4]，黄永梅[1, 3, 5*]，彭真明[2]

（1. 中国科学院 光电技术研究所，成都 610209；2. 电子科技大学，成都 610054；3. 中国科学院大学，北京 100049；
4. 西南通信研究所，成都 610041；5. 中国科学院 光束控制重点实验室，成都 610209）

摘要：块平均参考相位估计算法能够有效降低连续变量量子密钥分发的相位补偿噪声方差。为了使块平均参考相位估计算法的性能达到最优，根据相位漂移变化的数学模型，从理论上分析了该算法的均方误差特性，并得到最优的块长度取值。仿真结果表明：最优相位估计可使系统的相位补偿噪声方差降低 72%，从而最大化提升安全密钥的成码距离。

关键词：量子密钥分发；连续变量；参考脉冲；相位估计；相位补偿

中图分类号：TN256　**文献标志码**：A　**文章编号**：1002-5561(2021)06-0018-04

DOI：10.13921/j.cnki.issn1002-5561.2021.06.005　**开放科学(资源服务)标识码(OSID)**：

Performance optimization of the block-averaging reference phase estimating algorithm in CVQKD

HUANG Biao[1-5], HAN Hesong[4], HUANG Yongmei[1, 3, 5*], PENG Zhenming[2]

(1. Institute of Optics and Electronics, Chinese Academy of Sciences, Chengdu 610209, China; 2. University of Electronic Science and Technology of China, Chengdu 610054, China; 3. University of Chinese Academy of Sciences, Beijing 100049, China; 4. Southwest Communication Institute, Chengdu 610041, China; 5. Key Laboratory of Optical Engineering, Chinese Academy of Sciences, Chengdu 610209, China)

Abstract: The block-averaging reference phase estimating algorithm is able to reduce the variance of phase compensation noise effectively in the continuous-variable quantum key distribution. In order to optimize the performance of the block-averaging reference phase estimating algorithm, according to the mathematical model of phase drift variation, the mean square error characteristics of the algorithm are analyzed theoretically, and the optimal block length is obtained. Simulation results show that the variance of phase compensation noise can be reduced by 72% under the optimal phase estimation, so that the distance for generating secure key can be improved most significantly.

Key words: quantum key distribution; continuous variable; reference pulse; phase estimation; phase compensation

0 引言

连续变量量子密钥分发(CVQKD)是一种在公共信道中建立安全共享密钥的技术[1]。在 CVQKD 技术中，基于高斯调制相干态(GMCS)的 CVQKD 协议仅需使用标准的光通信器件就可以实现相干态量子信号的制备和探测[2]，因而具有极大的应用价值。近年来，为了解决传统 GMCS-CVQKD 系统中由于本振光传输而导致的漏洞攻击问题[3]，一种基于本地本振光(LLO)的 CVQKD 方案被提出[4]。由于接收端产生的本振光不会被窃听者控制，因此该方案可以完全避免因本振光传输而带来的安全问题。随后，一些改进的 LLO-CVQKD 协议被提出并得到实验验证[5-7]。

准确估计参考相位对提高 LLO-CVQKD 方案的实际安全性十分重要[8-11]。由于信道干扰、参考脉冲光子泄露以及探测器误差的影响，参考相位测量结果不可避免地叠加了一个相位噪声，导致参考相位估计误差的增加。现有的实验系统一般采用块平均参考相位估计方案，即对连续多个参考脉冲的相位测量结果取平均值来抑制参考脉冲的相位噪声[12]。然而，现有的实

收稿日期：2020-09-08。

基金项目：国家自然科学基金(U1738204、61775030、61571096)资助；中国科学院光束控制重点实验室基金(2017LBC003)资助。

作者简介：黄彪(1986—)，男，四川成都人，电子科技大学、中国科学院大学联合培养博士研究生，西南通信研究所高级工程师，主要研究方向为保密通信技术和量子通信技术，长期从事各类通信平台的嵌入式软件开发和量子密钥系统的研制工作。

*** 通信作者**：黄永梅(1968—)，女，博士，研究员，主要研究方向为空间量子激光通信。

验系统在选择块长度时忽略了相位漂移随机变化的特性，于是未能取得最优的估计结果。为了最优化块平均参考相位估计算法的估计性能，本文根据相位漂移变化的数学模型，从理论上分析块平均参考相位估计算法的均方误差随块长度变化的曲线特性，从而得到最优的块长度取值。

1 系统模型

基于导频延迟方案[13]的 LLO-CVQKD 系统如图 1 所示。发送端 Alice 以重复频率 f_{rep} 产生光脉冲序列，并利用分束器将光脉冲分离到信号路径和参考路径，使得信号路径与参考路径上的每一对光脉冲具有相同的光源相位。在信号路径中，Alice 产生调制方差为 V_A 的高斯随机数对 (x_A,p_A)，通过幅度调制器和相位调制器将光脉冲调制为 GMCS 量子信号 $|x_A+ip_A\rangle$。在参考路径，光脉冲经过延迟器被延迟半个符号周期，然后经过一个光衰减器形成指定强度的参考脉冲。随后，量子信号与参考脉冲通过偏振合束器合并，并通过量子信道传递给接收端 Bob。

在接收端，量子信号和参考脉冲通过偏振分束器后被分离到信号路径和参考路径。接收端 Bob 以相同的重复频率产生光脉冲，并使用分束器将光脉冲分离成 2 个具有相同光源相位的本振光，分别用于探测参考脉冲和量子信号。接收端先利用其中一个本振光对参考路径上的参考脉冲进行外差探测，得到参考相位测量结果；接着再使用块平均参考相位估计算法对连续多个参考相位测量结果取平均值，得到参考相位估计结果；然后结合随机选择的测量基对另一个本振光进行相位调制，生成用于探测量子信号的真实本振光；最后，接收端使用真实本振光对信号路径上被延迟一定时间的量子信号进行零差平衡探测，得到正则分量测量结果 x_B 或 p_B。

2 参考相位估计

收发端激光器之间的相位漂移通常采用维纳过程来描述[14]。假设初始时刻的相位漂移为零，收发端激光器线宽之和为 f_{AB}，那么第 k 个参考脉冲的相位测量结果可以表示为：

$$\varphi_k=w_k+v_k \tag{1}$$

其中，w_k 是参数为 $\sigma_w^2=2\pi f_{AB}/f_{rep}$ 的维纳过程，v_k 是均值为零、方差为 σ_v^2 的相位噪声。维纳过程参数 σ_w^2 描述了相位漂移的变化程度，该值越大则相位漂移变化越显著。相位噪声方差 σ_v^2 描述了参考相位测量结果的误差程度，该误差包含了信道干扰、参考脉冲光子泄漏以及探测器误差的影响。

为了抑制相位噪声，块平均参考相位估计算法通过对前后相邻的 $2m+1$ 个参考相位测量结果取平均值来估计当前时刻的参考相位，于是第 k 个量子信号的参考相位估计可表示为：

$$\hat{\varphi}_k=\frac{1}{l}\sum_{n=-m}^{m}\hat{\varphi}_{k+n} \tag{2}$$

其中，m 为块半径，$l=2m+1$ 为块长度。由于块平均参考相位估计算法需要用到前后多个时刻的参考相位测量结果，因此量子信号的探测时间需要被适当地延迟。

为了使块平均参考相位估计算法的估计性能达到最优，本文需要对参考相位估计的均方误差特性进行量化分析。根据式(1)和式(2)，并利用平方求和公式 $\sum_{n=1}^{m}n^2=m(m+1)\times(2m+1)$，可以得到块平均参考相位估计算法的均方误差理论值为：

$$\delta=\frac{m(m+1)}{3l}\sigma_w^2+\frac{1}{l}\sigma_v^2 \tag{3}$$

式(3)表明：块平均参考相位估计算法的均方误差特性与块长度、相位漂移的维纳过程参数和相位噪声方差有直接的关联。合理选择块长度，可以使块平均参考相位估计算法的均方误差达到最小，从而最大化地降低相位补偿噪声方差。

3 安全密钥率

发送端的高斯调制相干态量子信号 $|x_A+ip_A\rangle$ 经过一个透传率为 T、过噪声为 ε 的量子信道后，接收端在非理想相位补偿情况下使用平衡探测器得到正则分

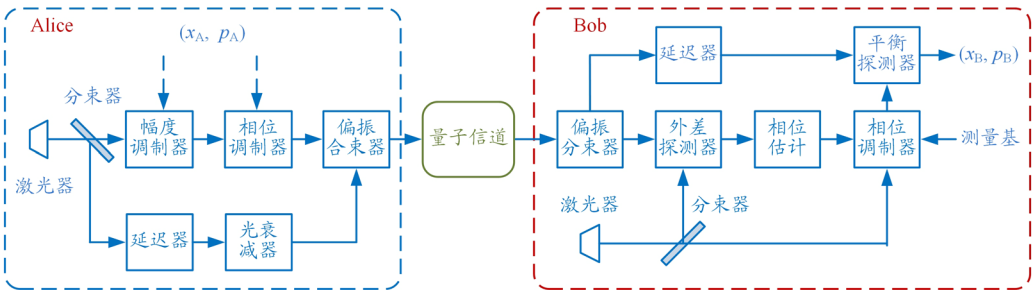


图 1 基于导频延迟方案的 LLO-CVQKD 系统模型图

量测量结果为:

$$\begin{pmatrix} x_B \\ p_B \end{pmatrix}=\sqrt{\eta T}\left[\begin{pmatrix} \cos\theta_k & \sin\theta_k \\ -\sin\theta_k & \cos\theta_k \end{pmatrix}\begin{pmatrix} x_A \\ p_A \end{pmatrix}+\begin{pmatrix} x_N \\ p_N \end{pmatrix}\right]+\begin{pmatrix} x_{el} \\ p_{el} \end{pmatrix} \quad (4)$$

其中,η 为探测器效率,x_N 和 p_N 是 ε 的加性高斯噪声,x_{el} 和 p_{el} 是方差为 V_{el} 的电噪声,θ_k 是第 k 个量子信号的相位补偿噪声,其方差记为 V_θ。在理想相位补偿情况下 $V_\theta=0$,而在块平均相位估计情况下 $V_\theta=\delta$。在使用单个参考相位测量结果进行相位估计时有 $\theta_k=\sigma_v^2$,此时等价于块长度为 1 的块平均相位估计。

根据非理想相位补偿噪声模型[15],实际透传率和实际过噪声的理论值分别为 $T'=\kappa T$ 和 $\varepsilon'=[\varepsilon+(1-\kappa)\times V_A]/\kappa$,其中 $\kappa=(1-V_\theta/2)^2$ 为相位补偿精度,V_A 为调制方差。于是,LLO-CVQKD 在联合攻击下的安全密钥率为:

$$K=\beta I_{AB}(T',\varepsilon')-\chi_{BE}(T',\varepsilon') \quad (5)$$

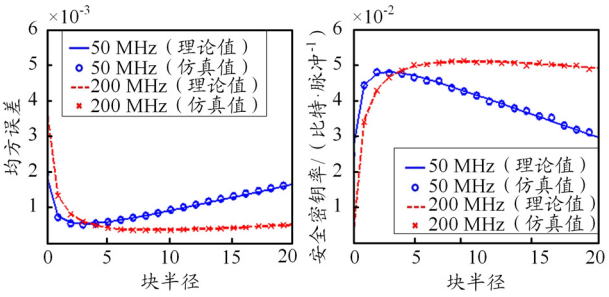
其中,β 为数据协调效率,$I_{AB}(T',\varepsilon')$ 为 Alice 和 Bob 之间的香农互信息,$\chi_{BE}(T',\varepsilon')$ 为 Eve 从 Bob 端获取的最大信息量。

4 仿真结果与分析

根据现有实验测定[16],系统参数取值如下:$V_A=18.9$,$V_{el}=0.001$,$\varepsilon=0.01$,$\beta=0.92$,探测器效率 $\eta=0.59$,收发端激光器线宽之和为 3.8 kHz,参考脉冲的重复频率分别取 50 MHz 和 200 MHz,于是相位漂移的 σ_w^2 分别为 4.8×10^{-4} rad^2 和 1.2×10^{-4} rad^2,同时 σ_v^2 分别为 2.0×10^{-3} rad^2 和 4.0×10^{-3} rad^2。

在仿真中,本文先根据相位漂移的维纳过程参数生成了 2000 个参考脉冲的相位漂移变化序列,然后根据相位噪声方差产生了 2000 个服从高斯分布的相位噪声序列,并依次叠加在参考脉冲的相位漂移变化序列之上,从而得到含有相位噪声的相位漂移变化序列。随后,使用块平均参考相位估计算法估计这些参考脉冲的相位值,并统计相位估计的均方误差,得到均方误差随块半径取值变化的性能曲线如图 2(a)所示。可以看出,块平均参考相位估计算法的均方误差理论曲线与仿真统计结果一致,50 MHz 和 200 MHz 系统的均方误差最小值分别在块半径为 3(即块长度为 7)和块半径为 10(即块长度为 21)时取得,此时相位补偿噪声方差可以分别减小 72%和 90%。

当通信距离为 25 km 时,系统安全密钥率随块半径变化的性能曲线如图 2(b)所示,其中仿真值是通过 $M=20000$ 个训练量子信号来测量实际透传率

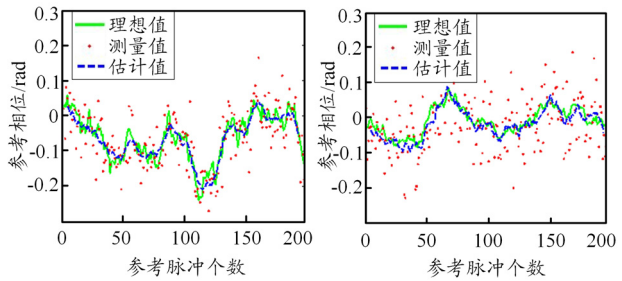


(a) 均方误差性能　　(b) 安全密钥率性能

图 2 均方误差和安全密钥率随块半径取值变化的性能曲线

和实际过噪声后评估所得到的。本文根据 V_A 产生符合高斯分布的正则分量序列 $\{x_i\}$ 和 $\{p_i\}$,然后根据 ε 和 V_{el} 产生高斯噪声序列,并由式(4)生成训练量子信号正则分量的测量结果。假设 Bob 只测量 x 分量,其测量结果序列记为 $\{y_i\}$。由于 Alice 可以将训练量子信号的正则分量信息 $\{x_i\}$ 通过经典信道告知 Bob,于是 Bob 可以通过统计量 $\hat{T}'=\left(\sum_{i=1}^{M}x_iy_i/\sum_{i=1}^{M}x_i^2\right)^2$ 和 $\hat{T}'\hat{\varepsilon}'=\sum_{i=1}^{M}\left(y_i-\sqrt{\hat{T}'}x_i\right)^2/M\hat{T}'$ 来估计实际透传率和实际过噪声,然后根据式(5)评估安全密钥率。从图 2(b)可以看出,安全密钥率随块长度变化的理论曲线与仿真曲线一致,安全密钥的最大值也分别在块半径为 3 和块半径为 10 时取得;相比于使用单个参考相位测量结果进行相位估计的情况(即块半径为 0 时),50 MHz 系统的安全密钥率几乎提高了 1 倍,而 200 MHz 系统的安全密钥率更是从 0 提高至 5×10^{-2} 比特/脉冲。

50 MHz 和 200 MHz 系统在最优块长度取值下(分别为 7 和 21)的参考相位估计效果如图 3 所示。其中,理想值是不含相位噪声时的参考脉冲相位值,测量值是叠加了相位噪声时的参考脉冲相位测量结果,而估计值是在最优块长度取值下使用块平均参考相位估计算法对参考相位的估计结果。可以看出,测量值由于

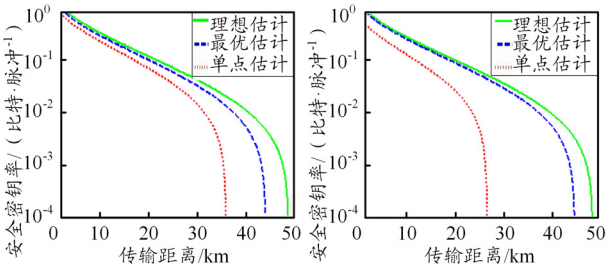


(a) 重复频率为 50 MHz,最优块长度=7　　(b) 重复频率为 200 MHz,最优块长度=21

图 3 最优块长度取值下的参考相位估计效果

相位噪声的影响，与理想值之间存在比较明显的偏差，而经过块平均参考相位估计算法处理后得到的估计值变得更平滑且更接近理想值，因此块平均参考相位估计算法起到了降噪的作用。由于相位噪声的影响显著大于相位漂移的变化，所以块平均参考相位估计算法能够有效地提高参考相位估计精度。

50 MHz 和 200 MHz 系统在 3 种相位估计情况下的安全密钥率随传输距离的变化情况如图 4 所示。其中，理想估计是指不含相位噪声的情况，此时相位补偿精度为 1。单点估计是指直接使用单个参考脉冲的相位测量结果作为相位估计，此时 2 种系统的相位估计均方误差分别为 2.0×10^{-3} rad^2 和 4.0×10^{-3} rad^2，相位补偿精度分别为 0.9980 和 0.9960。最优估计是指在最优块长度取值下采用块平均参考相位估计算法估计参考相位，此时 2 种系统的相位估计均方误差分别为 5.6×10^{-4} rad^2 和 4.0×10^{-4} rad^2，相位补偿精度分别为 0.9994 和 0.9996。通过相位补偿精度参数，可以评估系统的实际透传率和实际过噪声，再根据式(5)计算安全密钥率。从图 4 可以看出，在单点估计情况下，相位噪声对相位补偿的影响较大，安全密钥率随传输距离的增加而迅速下降；在最优相位估计情况下，相位噪声被有效抑制，系统可在更远距离(接近理想估计距离)的情况下生成安全密钥。



(a) 重复频率为 50 MHz　　(b) 重复频率为 200 MHz

图 4　系统安全密钥率随传输距离的变化

5 结束语

块平均参考相位估计算法可以有效降低 LLO-CVQKD 系统的相位补偿噪声方差。本文根据相位漂移的数学模型，从理论上分析了块平均参考相位估计算法的均方误差随块长度的变化特性。仿真结果表明：在实际系统中，为了确定最优块长度的取值，需要实时测定相位噪声方差。相位噪声方差的大小和估计误差可能导致最优块长度取值存在一定的偏差。因此，下一步工作是分析实际系统中相位噪声方差的大小和估计误差对最优块长度取值的灵敏度影响，设计高效准确的相位噪声方差测量方案。另外，研究更加有效的相位估计方案也是未来的工作重点。

参考文献：

[1] GISIN N, RIBORDY G, TITTEL W, et al. Quantum cryptography[J]. Reviews of Modern Physics, 2001, 74(1): 145–195.

[2] GROSSHANS F, GILLES V A, WENGER J, et al. Quantum key distribution using gaussian-modulated coherent states[J]. Nature, 2003, 421: 238–241.

[3] MA X C, SUN S H, JIANG M S, et al. Local oscillator fluctuation opens a loophole for Eve in practical continuous-variable quantum-key-distribution systems [EB/OL]. [2020–09–08]. https://journals.aps.org/pra/abstract/10.1103/PhysRevA.88.022339.

[4] QI B, LOUGOVSKI P, POOSER R, et al. Generating the local oscillator "locally" in continuous-variable quantum key distribution based on coherent detection[J]. Physical Review X, 2015, 5(4): 041009-1–041009-12.

[5] SOH D B S, BRIF C, COLES P J, et al. Self-referenced continuous-variable quantum key distribution protocol[J]. Physical Review X, 2015, 5(4): 041010-1–041010-15.

[6] MARIE A, ROMAIN A. Self-coherent phase reference sharing for continuous-variable quantum key distribution [EB/OL]. [2020–09–08]. https://journals.aps.org/pra/abstract/10.1103/PhysRevA.95.012316.

[7] WANG T, HUANG P, ZHOU Y, et al. High key rate continuous-variable quantum key distribution with a real local oscillator[J]. Optics Express, 2018, 26(3): 2794-2806.

[8] QI B, LIM C C W. Noise analysis of simultaneous quantum key distribution and classical communication scheme using a true local oscillator [EB/OL]. [2020–09–08]. https://arxiv.org/abs/1708.08742v2.

[9] REN S, KUMAR R, WONFOR A, et al. Reference pulse attack on continuous variable quantum key distribution with local local oscillator under trusted phase noise [J]. Journal of the Optical Society of America B, 2019, 36(3): B7–B15.

[10] ZHAO W, SHI R, HUANG D. Practical security analysis of reference pulses for continuous-variable quantum key distribution [EB/OL]. [2020–09–08]. https://www.nature.com/articles/s41598-019-54249-0.

[11] HUANG B, HUANG Y, PENG Z. Practical security of the continuous-variable quantum key distribution with real local oscillators under phase attack[J]. Optics Express, 2019, 27(15): 20621–20631.

[12] HUANG D, HUANG P, LIN D, et al. High-speed continuous-variable quantum key distribution without sending a local oscillator [J]. Optics Letters, 2015, 40(16): 3695–3698.

[13] WANG T, HUANG P, ZHOU Y, et al. Pilot-multiplexed continuous-variable quantum key distribution with a real local oscillator [J]. Physical Review A, 2018, 97(1): 012310-1–012310-11.

[14] BILAL S M, FLUDGER C, BOSCO G. Carrierphase estimation in multi-subcarrier coherent optical systems [J]. IEEE Photonics Technology Letters, 2016, 28(19): 2090–2093.

[15] 黄彪，黄永梅，彭真明. 连续变量量子密钥分发的参考脉冲相位攻击与探测[J]. 光学学报，2019，39(11)：1127001-1–1127001-7.

[16] HUANG P, LIN D K, HUANG D, et al. Security of continuous-variable quantum key distribution with imperfect phase compensation[J]. International Journal of Theoretical Physics, 2015, 54(8): 2613–2622.