第 58 卷 第 11 期/2021 年 6 月/激光与光电子学进展 研究论文

激光与光电子学进展

连续变量量子密钥分发中的最小二乘相位估计算法

黄彪[1,2,3,4]，麻甜甜[4]，黄永梅[1,3*]，彭真明[2]

[1]中国科学院光电技术研究所光束控制重点实验室，四川 成都 610209；

[2]电子科技大学信息与通信工程学院，四川 成都 610054；

[3]中国科学院大学，北京 100049；

[4]西南通信研究所基础平台事业部，四川 成都 610041

摘要 为了提高连续变量量子密钥分发的参考相位估计精度，提出了基于最小二乘的参考相位估计方案。利用相位慢漂移的二阶相关特性和最小二乘估计原理，在接收端对多个参考脉冲的相位测量结果进行二次多项式拟合估计，从而抑制相位噪声的影响。仿真结果表明，相比于块平均估计法，基于最小二乘的参考相位估计算法能够更好地适应相位漂移变化，降低参考相位估计的均方误差，从而提高系统的安全密钥率。

关键词 量子光学；量子通信；连续变量；量子密钥分发；参考相位；最小二乘估计

中图分类号 O431.2 **文献标志码** A **doi**：10.3788/LOP202158.1127001

Least Square Algorithm for Phase Estimation in Continuous-Variable Quantum Key Distribution

Huang Biao[1,2,3,4], Ma Tiantian[4], Huang Yongmei[1,3*], Peng Zhenming[2]

[1]*Key Laboratory of Optical Engineering, Institute of Optics and Electronics, Chinese Academy of Sciences, Chengdu, Sichuan* 610209, *China*;

[2]*School of Information and Communication Engineering, University of Electronic Science and Technology of China, Chengdu, Sichuan* 610054, *China*;

[3]*University of Chinese Academy of Sciences, Beijing* 100049, *China*;

[4]*Department of Basic Platform, Southwest Communication Institute, Chengdu, Sichuan* 610041, *China*

Abstract To improve the accuracy of reference phase estimation in the continuous-variable quantum key distribution, a scheme of reference phase estimation is proposed, which is based on the least square method. Utilizing the second-order correlation characteristics of slow phase drift and the least-square estimation theory, the phase measurement results for a group of reference pulses are fitted by a quadratic polynomial at the receiver to suppress the effect of phase noise. The simulation results show that the least square phase estimation algorithm, compared with the block-averaging estimation algorithm, is better adapted to phase drift variation, so that the mean square error of reference phase estimation can be reduced and the secret key rate of the practical system can be improved significantly.

收稿日期：2020-11-05；**修回日期**：2020-11-16；**录用日期**：2020-12-02

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

*E-mail：huangym@ioe.ac.cn

Key words　quantum optics; quantum communication; continuous variable; quantum key distribution; reference phase; least square estimation

OCIS codes　270.5565; 270.5568

1　引　　言

连续变量量子密钥分发(CVQKD)[1]是一种在公共信道中建立安全共享密钥的技术。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[2-5],因而具有极大的应用价值。

虽然GMCS-CVQKD协议在理论上早已被证明是无条件安全的[6-7],但是实际系统的安全性仍在不断研究和改进。近年来,为了解决传统GMCS-CVQKD系统中本振光(LO)传输而导致的漏洞攻击问题[8-10],一种基于本地本振光(LLO)的CVQKD方案被提出[11]。接收端在本地产生本振光,并利用参考脉冲提供的相位信息对接收到的量子信号进行相位补偿,从而有效避免本振光传输带来的安全问题。随后,一些改进的LLO-CVQKD协议被提出并得到实验验证[12-15]。

在LLO-CVQKD系统中,参考脉冲相位估计的准确度对系统实际安全性十分重要[16-19]。由于信道干扰、参考脉冲光子泄露以及探测器误差的影响,参考脉冲的相位测量结果不可避免地叠加了相位噪声,导致参考相位估计误差增加。在现有的LLO-CVQKD实验系统中,一般采用块平均参考相位估计算法来抑制参考脉冲的相位噪声[20-21],即对连续多个参考脉冲的相位测量结果取平均值来估计参考相位。然而,由于收发端激光器自发辐射噪声和中心频率抖动的影响,参考脉冲的相位漂移并非是线性变化的[22],因此块平均估计法对相位噪声的抑制效果不够理想。

为了提高LLO-CVQKD系统中参考脉冲相位估计的准确度,本文利用参考脉冲的相位漂移在时域上的低阶相关性,提出了基于最小二乘(LS)的参考相位估计算法,采用二次多项式对连续多个参考脉冲的相位测量结果进行曲线拟合。仿真结果表明,最小二乘估计法的相位估计均方误差显著低于块平均估计法,该方法能够更好地适应相位漂移的非线性变化特性,从而有效提高实际系统的安全密钥率。

2　系统模型

基于导频延迟方案的LLO-CVQKD系统如图1所示。发送端Alice用激光器产生符号周期为T_s的光脉冲序列,并利用光分束器(BS)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产生高斯随机数对(x_A, p_A),通过幅度调制器(AM)和相位调制器(PM)将光脉冲的强度和相位分别调制为$\sqrt{x_A^2+p_A^2}$和$\arctan(p_A/x_A)$,从而得到高斯调制相干态量子信号$|x_A+ip_A\rangle$,其正则分量x_A和p_A独立服从调制方差为V_A的高斯分布。在参考路径,光脉冲经过一个延迟器(DL)后被延迟半个符号周期,然后经过一个光衰减器(OA)形成指定强度的参考脉冲。随后,量子信号与参考脉冲经偏振合束器(PBC)合束后被发送出去,经量

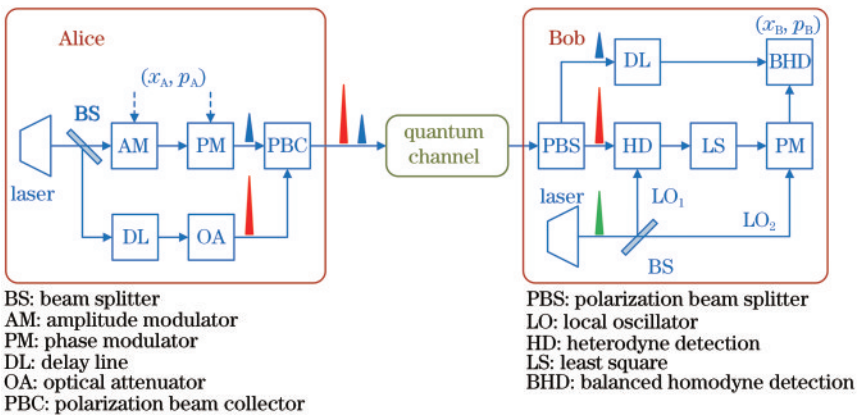

图1　基于导频延迟的LLO-CVQKD模型图

Fig. 1　Schematic of LLO-CVQKD model based on pilot-delay design

子信道传递给接收端Bob。

在接收端，量子信号和参考脉冲被偏振分束器(PBS)分离到信号路径和参考路径。接收端Bob使用激光器生成与发送端同频的光脉冲，并使用光分束器将光脉冲分离成两个相位相同的子光脉冲，分别作为探测参考脉冲的本振光LO_1和探测量子信号的本振光LO_2。接收端先利用LO_1对参考路径上的参考脉冲进行外差探测(HD)，得到参考脉冲的相位测量结果，接着再利用最小二乘估计算法对参考脉冲的相位测量结果进行滤波估计，得到最佳的参考相位估计值，并以此对LO_2进行相位调制，以补偿对应量子信号的相位漂移。最后，接收端使用经过相位调制后的LO_2对信号路径上延迟了半个符号周期的量子信号进行平衡零差探测(BHD)，通过随机选择测量基，得到正则分量的测量结果x_B或p_B。

3 最小二乘估计

在接收端使用本振光对参考脉冲进行外差探测时，假设接收端本振光与参考脉冲之间的初始相位差为零，那么后续测量得到的相位差可以表示为相位漂移和相位噪声之和。从时域局部来看，相位漂移的变化存在一定的相关性，其中一阶相关性和二阶相关性为主导因素，因此连续多个参考脉冲之间的相位漂移变化可以用一个二阶多项式来逼近。那么对于连续接收到的L个参考脉冲，若它们的相位测量结果为$y_k(k=1,2,\ldots,L)$，那么观测方程可以表示为

$$y_k=a_0+a_1k+a_2k^2+w_k+n_k, \tag{1}$$

式中：a_0,a_1,a_2为待估计的二阶多项式系数；w_k为相位漂移高阶变化引入的模型误差；n_k为相位噪声。连续L个参考脉冲的观测方程可以采用矢量和矩阵形式表示，即

$$\boldsymbol{y}=\boldsymbol{H}\boldsymbol{a}+\boldsymbol{w}+\boldsymbol{n}, \tag{2}$$

式中：$\boldsymbol{y}=[y_1,y_2,\ldots,y_L]^{\mathrm{T}}$为观测矢量；$\boldsymbol{a}=[a_0,a_1,a_2]^{\mathrm{T}}$为待估矢量；$\boldsymbol{w}=[w_1,w_2,\ldots,w_L]^{\mathrm{T}}$为模型误差矢量；$\boldsymbol{n}=[n_1,n_2,\ldots,n_L]^{\mathrm{T}}$为相位噪声矢量；$\boldsymbol{H}$为观测矩阵，具体表示为

$$\boldsymbol{H}=\begin{bmatrix}1 & 1 & 1\\ 1 & 2 & 4\\ \vdots & \vdots & \vdots\\ 1 & L & L^2\end{bmatrix}。 \tag{3}$$

根据最小二乘原理[23]，假设模型误差和相位噪声独立服从高斯分布，那么使$(\boldsymbol{y}-\boldsymbol{H}\boldsymbol{a})^{\mathrm{T}}(\boldsymbol{y}-\boldsymbol{H}\boldsymbol{a})$最小的待估矢量$\boldsymbol{a}$的最优估计为

$$\hat{\boldsymbol{a}}=(\boldsymbol{H}^{\mathrm{T}}\boldsymbol{H})^{-1}\boldsymbol{H}^{\mathrm{T}}\boldsymbol{y}。 \tag{4}$$

为了与块平均估计法进行对比，在得到最优估计矢量$\hat{\boldsymbol{a}}$后，我们用$\hat{\boldsymbol{a}}$去重新估计这L个参考脉冲中处于中间位置的那个参考脉冲的参考相位。设定L的取值为奇数，即$L=2m+1$，那么中间位置的参考脉冲的参考相位估计为

$$\hat{\varphi}=\hat{a}_0+\hat{a}_1(m+1)+\hat{a}_2(m+1)^2, \tag{5}$$

式中：$\hat{a}_0$、$\hat{a}_1$和$\hat{a}_2$分别为二次多项式系数a_0,a_1,a_2的估计值。

在参考脉冲接收和测量过程中，当接收到L个参考脉冲后就开始执行最小二乘估计，用一个长度为L的滑动窗口去估计处于窗口中间位置的参考脉冲的相位漂移。当接收到下一个参考脉冲后就移动窗口，并重新执行最小二乘估计，随后以此类推。

4 安全性分析

发送端的高斯调制相干态量子信号$\left|x_A+\mathrm{i}p_A\right\rangle$经过一个透传率为$T$且过噪声为$\varepsilon$的量子信道之后，接收端在非理想相位补偿情况下使用平衡零差探测器得到的正则分量测量结果[24]可表示为

$$\begin{pmatrix}x_B\\ p_B\end{pmatrix}=\sqrt{\eta T}\left[\begin{pmatrix}\cos\theta & \sin\theta\\ -\sin\theta & \cos\theta\end{pmatrix}\begin{pmatrix}x_A\\ p_A\end{pmatrix}+\begin{pmatrix}x_N\\ p_N\end{pmatrix}\right]+\begin{pmatrix}x_{el}\\ p_{el}\end{pmatrix}, \tag{6}$$

式中：η为探测效率；x_N和p_N是方差为ε的信道过噪声分量；x_{el}和p_{el}是方差为V_{el}的电噪声分量；θ是相位补偿噪声，其方差记为V_θ。假设相位补偿噪声主要来自于参考相位估计，那么V_θ可以利用参考相位估计的均方误差来直接进行描述。本文考虑的三种常用的参考相位估计方案为：1)直接估计法(Direct)，即使用单个参考脉冲的相位测量值作为参考相位估计值；2)块平均估计法(Average)，即对多个参考脉冲的相位测量结果取平均值并将其作为参考相位估计值；3)最小二乘估计法，即根据最小二乘估计原理对多个参考脉冲的相位测量结果进行多项式拟合估计。

根据非理想相位补偿噪声模型[25]，实际透传率T'和实际过噪声ε'的估计值分别为$T'=\kappa T$和$\varepsilon'=[\varepsilon+(1-\kappa)V_A]/\kappa$，其中$\kappa=(1-V_\theta/2)^2$为相位补偿精度。最终，LLO-CVQKD在联合攻击下的安全密钥率为

$$K=\beta I_{AB}(T',\varepsilon')-\chi_{BE}(T',\varepsilon'), \tag{7}$$

式中：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 端获取的量子互信息。

5　仿真结果与分析

根据现有实验测定[26]，系统参数取值如下：调制方差 $V_A=18.9$，电噪声方差 $V_{el}=0.001$，过噪声 $\varepsilon=0.01$，协调效率 $\beta=0.92$，探测器效率 $\eta=0.59$，相位噪声方差 $V_\theta=4.0\times10^{-4}$ rad^2，收发端激光器线宽之和 $\upsilon_{AB}=3.8$ kHz，参考脉冲的重复频率 $f_R=100$ MHz。基于这些参数，相位漂移可以建模成一个参数为 $2\pi\upsilon_{AB}/f_R$ 的维纳过程[22]。

直接估计法、块平均估计法和最小二乘估计法的均方误差随块长度 L 的变化情况如图 2 所示。直接估计法只与相位噪声方差相关，因此均方误差不随块长度的变化而改变。当块长度取值较小时，少量参考脉冲之间的相位漂移以线性变化为主，此时块平均估计法的相位估计均方误差较小。随着块长度的增加，相位漂移逐渐呈现出非线性变化，此时块平均估计法的相位估计均方误差逐渐增大，而最小二乘估计法的相位估计均方误差逐渐减小。另外，块平均估计法对最优块长度的取值十分敏感。为了保持最优估计效果，块平均估计法只能在较窄的块长度取值范围内进行取值，而最小二乘估计法则具有较宽的最优块长度取值范围。

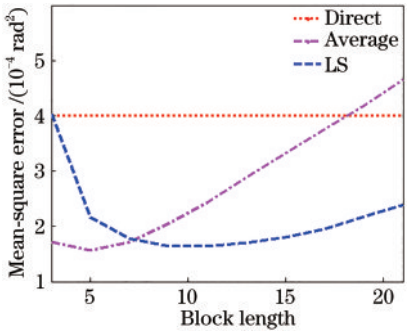

图 2　均方误差随块长度的变化

图 3 比较了几种参考相位估计算法的估计性能，此时块长度取值为 11。在仿真中，我们先根据相位漂移的维纳过程参数生成了 500 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 500 个服从高斯分布的相位噪声序列，并将其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。随后使用直接估计法、块平均估计法和最小二乘估计法来估计相位漂移，并实时统计相位估计的均方误差。图 3(a)给出了相位漂移变化序列和参考相位的估计结果，容易看出，最小二乘估计法得到的相位漂移估计曲线比块平均估计法更接近理想情况(Perfect)下的相位漂移曲线。图 3(b)对比了均方误差的实时统计结果。在参考脉冲样本个数到达 100 后，直接估计法、块平均估计法和最小二乘估计法的均方误差趋于稳定，分别约为 4.0×10^{-4}，2.6×10^{-4}，1.8×10^{-4} rad^2。

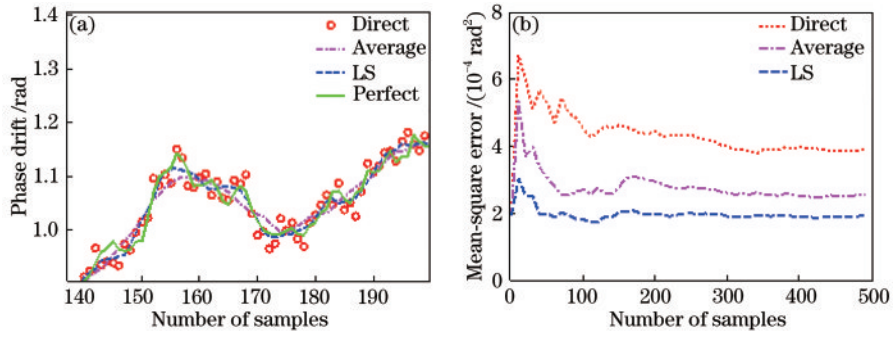

图 3　不同参考相位估计算法的估计性能比较。(a)相位漂移的估计结果；(b)均方误差实时统计结果

Fig. 3　Comparison of estimation performances of different reference phase estimation algorithms. (a) Estimated results of phase drifts; (b) real-time statistical results of mean square errors

图 4 比较了 LLO-CVQKD 系统在不同估计算法下的安全密钥率。当块长度为 11 时，直接估计法、块平均估计法和最小二乘估计法的相位补偿精度分别为 0.9996，0.9997 和 0.9998。根据相位补偿精度参数，可以修正系统的实际透传率和实际过噪声，并根据(7)式计算安全密钥率。仿真结果表明，相比于块平均估计法，最小二乘估计法具有更高的相位补偿精度，因此能够进一步提高 LLO-CVQKD 系统的安全密钥率和安全通信距离。

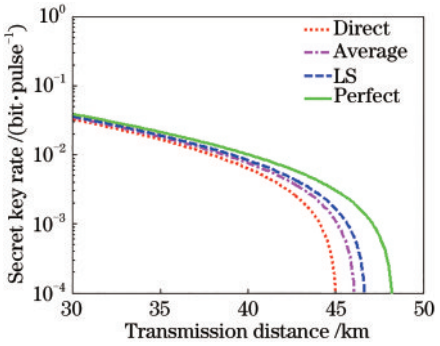

图 4　LLO-CVKQD 系统的安全密钥率

Fig. 4　Secret key rate of LLO-CVQKD system

6　结　　论

为了提高连续变量量子密钥分发的参考相位估计精度，提出了一种基于最小二乘的参考相位估计方案。通过最小二乘估计法，在接收端对参考脉冲的相位测量结果进行了实时滤波估计，有效降低了相位估计的均方误差。仿真结果表明，相比于块平均估计法，最小二乘估计法能够更好地适应相位漂移的非线性变化，从而有效提高系统的安全密钥率。

参　考　文　献

[1] Weedbrook C, Pirandola S, García-Patrón R, et al. Gaussian quantum information[J]. Reviews of Modern Physics, 2012, 84(2): 621-669.

[2] Grosshans F, van Assche G, Wenger J, et al. Quantum key distribution using Gaussian-modulated coherent states[J]. Nature, 2003, 421(6920): 238-241.

[3] Lodewyck J, Bloch M, García-Patrón R, et al. Quantum key distribution over 25 km with an all-fiber continuous-variable system[J]. Physical Review A, 2007, 76(4): 042305.

[4] Dai W C, Lu Y, Zhu J, et al. An integrated quantum secure communication system[J]. Science China Information Sciences, 2011, 54(12): 2578-2591.

[5] Jouguet P, Kunz-Jacques S, Leverrier A, et al. Experimental demonstration of long-distance continuous-variable quantum key distribution[J]. Nature Photonics, 2013, 7(5): 378-381.

[6] Leverrier A, García-Patrón R, Renner R, et al. Security of continuous-variable quantum key distribution against general attacks[J]. Physical Review Letters, 2013, 110(3): 030502.

[7] Leverrier A. Composable security proof for continuous-variable quantum key distribution with coherent states[J]. Physical Review Letters, 2015, 114(7): 070501.

[8] 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[J]. Physical Review A, 2013, 88(2): 022339.

[9] Huang J Z, Weedbrook C, Yin Z Q, et al. Quantum hacking of a continuous-variable quantum-key-distribution system using a wavelength attack[J]. Physical Review A, 2013, 87(6): 062329.

[10] Qin H, Kumar R, Alléaume R, et al. Quantum hacking: saturation attack on practical continuous-variable quantum key distribution[J]. Physical Review A, 2016, 94: 012325.

[11] 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.

[12] Soh D B, Brif C, Coles P J, et al. Self-referenced continuous-variable quantum key distribution protocol[J]. Physical Review X, 2015, 5(4): 041010.

[13] Marie A, Alléaume R. Self-coherent phase reference sharing for continuous-variable quantum key distribution[J]. Physical Review A, 2017, 95: 012316.

[14] Wang T, Huang P, Zhou Y M, et al. High key rate continuous-variable quantum key distribution with a real local oscillator[J]. Optics Express, 2018, 26(3): 2794-2806.

[15] Gong F, Yang X, Wang T Y, et al. Improvement of self-referenced continuous variable quantum key distribution using optical amplifier[J]. Laser & Optoelectronics Progress, 2019, 56(21): 212702.
龚峰, 杨鑫, 王天一, 等. 利用光放大器改进自参考连续变量量子密钥分发[J]. 激光与光电子学进展, 2019, 56(21): 212702.

[16] Qi B, Lim C C W. Noise analysis of simultaneous quantum key distribution and classical communication scheme using a true local oscillator[J]. Physical Review Applied, 2018, 9(5): 054008.

[17] Ren S J, 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.

[18] Zhao W, Shi R H, Huang D, et al. Practical security analysis of reference pulses for continuous-variable quantum key distribution[J]. Scientific

Reports, 2019, 9: 18155.

[19] Wang T, Huang P, Zhou Y M, et al. Pilot-multiplexed continuous-variable quantum key distribution with a real local oscillator[J]. Physical Review A, 2018, 97: 012310.

[20] Huang B, Huang Y, Peng Z, et al. Practical security of the continuous-variable quantum key distribution with real local oscillators under phase attack[J]. Optics Express, 2019, 27(15): 20621-20631.

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

[22] Bilal S M, Fludger C, Bosco G, et al. Carrier phase estimation in multi-subcarrier coherent optical systems [J]. IEEE Photonics Technology Letters, 2016, 28 (19): 2090-2093.

[23] Zhao S J, Zhao J X. Signal detection and estimation theory[M]. 2nd ed. Beijing: Publishing House of Electronics industry, 2013: 215-217.
赵树杰, 赵建勋. 信号检测与估计理论[M]. 2 版. 北京: 电子工业出版社, 2013: 215-217.

[24] Jouguet P, Kunz-Jacques S, Diamanti E, et al. Analysis of imperfections in practical continuous-variable quantum key distribution[J]. Physical Review A, 2012, 86(3): 032309.

[25] Huang B, Huang Y, Peng Z M, et al. Attack and detection on reference-pulse phase of continuous-variable quantum-key distribution[J]. Acta Optica Sinica, 2019, 39(11): 1127001.
黄彪, 黄永梅, 彭真明, 等. 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.

[26] 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.