连续变量量子密钥分发的参考脉冲相位攻击与探测

黄彪[1,2,3,4,5*]，黄永梅[1,2,3]，彭真明[4]

[1]中国科学院光束控制重点实验室，四川 成都 610209；
[2]中国科学院光电技术研究所，四川 成都 610209；
[3]中国科学院大学光电学院，北京 100049；
[4]电子科技大学信息与通信工程学院，四川 成都 610054；
[5]西南通信研究所，四川 成都 610041

摘要 针对基于本地本振光的连续变量量子密钥分发在不安全的量子信道中传输参考脉冲存在相位攻击的安全问题，提出一种窃听和篡改参考脉冲相位的攻击方法，该攻击方法可增大接收端的相位补偿误差，从而降低实际系统的安全密钥率。基于相位补偿噪声模型，实际系统在参考脉冲相位攻击下的安全密钥率被分析。同时，提出一种基于监听相位补偿噪声方差的相位攻击探测方法。仿真结果表明，通过训练信号估计得到的安全密钥率与理论分析结果一致，并且通过监听训练信号和参考脉冲的相位补偿噪声方差可以有效判断相位攻击是否存在。

关键词 量子光学；量子通信；连续变量；量子密钥分发；参考脉冲；相位攻击

中图分类号 O431.2 **文献标识码** A **doi**：10.3788/AOS201939.1127001

Attack and Detection on Reference-Pulse Phase of Continuous-Variable Quantum-Key Distribution

Huang Biao[1,2,3,4,5*], Huang Yongmei[1,2,3], Peng Zhenming[4]

[1] *Key Laboratory of Optical Engineering, Chinese Academy of Sciences, Chengdu, Sichuan* 610209, *China*;
[2] *Institute of Optics and Electronics, Chinese Academy of Sciences, Chengdu, Sichuan* 610209, *China*;
[3] *School of Optoelectronics, University of Chinese Academy of Sciences, Beijing* 100049, *China*;
[4] *School of Information and Communication Engineering, University of Electronic Science and Technology of China, Chengdu, Sichuan* 610054, *China*;
[5] *Southwest Communication Institute, Chengdu, Sichuan* 610041, *China*

Abstract Continuous-variable quantum-key distribution based on the local-oscillator approach has been encountered with new security issues due to reference pulses transmitted over insecure quantum channels. Herein, a attack method for eavesdropping and tampering with phases of reference pulses is proposed, allowing the phase-compensation error in the receiver to be increased and secure-key rate of practical systems to be decreased. The secure-key rate of a practical system under phase attack of reference pulses is analyzed using the phase-compensation noise model. Moreover, a method for detecting phase attack is proposed, wherein the phase-compensation-noise variances are monitored. Simulation results show that the secure-key rate estimated by training signals is consistent with its theoretical value, and phase attack can be detected by monitoring phase-compensation-noise variances of the training signals and reference pulses.

Key words quantum optics; quantum communication; continuous variable; quantum key distribution; reference pulse; phase attack

OCIS codes 270.5565; 270.5568; 270.5570

1 引 言

连续变量量子密钥分发(CVQKD)可使通信双方在不安全的量子信道中建立安全的共享密钥[1-2]。相比于单光子传输的离散变量量子密钥分发(DVQKD)[3-4]，CVQKD使用标准的光通信器件和

收稿日期：2019-05-27；**修回日期**：2019-06-23；**录用日期**：2019-07-15

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

* **E-mail**：1002970532@qq.com

光纤网络，可完成量子密钥的安全分发，避免单光子激光器与单光子探测器实现困难的问题，在实用性方面更具优势。在理论方面，CVQKD 在联合攻击和相干攻击下的无条件安全性已被理论证明[5-6]。在实验方面，CVQKD 实验系统的数据协调效率已超过 98%[7]，安全传输距离已超过 150 km[8-9]。

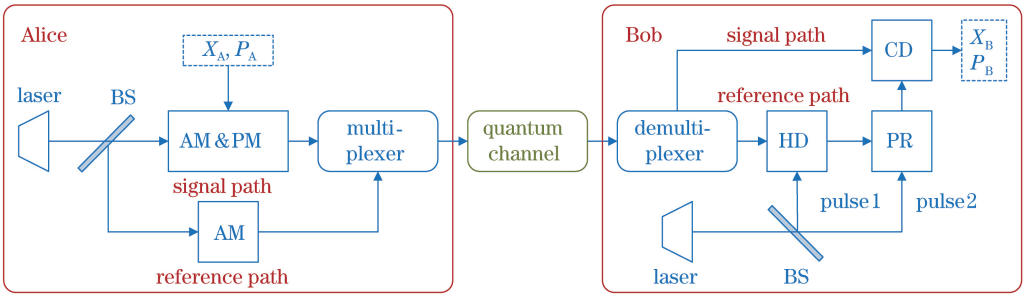
为完全解决传统 CVQKD 方案中由本振光传输带来的安全问题[10-16]，一种基于本地本振光（LLO）的 CVQKD 方案被提出[17-18]。在 LLO-CVQKD 方案中，本振光在接收端本地产生，不仅可完全避免由本振光传输带来的安全问题，而且还有利于实现散粒噪声受限的相干探测。另外，该方案还可利用时分复用和偏振复用技术，同步发送参考脉冲以补偿量子信号的相位漂移[19-21]。然而，在本振光传输所导致的问题被消除的同时，参考脉冲的传输可能会带来新的安全问题[22]。参考脉冲在不安全的量子信道中传输时，随时可能会被窃听者控制和篡改，其提供的相位信息不再准确可靠，最终可能导致 LLO-CVQKD 方案的安全密钥率降低。

本文提出一种参考脉冲相位攻击方法，在该攻击下参考脉冲的相位噪声可以被窃听者轻易地控制和篡改。基于相位补偿噪声模型，LLO-CVQKD 方案的实际安全性被分析。仿真结果表明，理论评估得到的安全密钥率与由实验参数估计得到的安全密钥率一致。此外，本文还提出一种相位攻击探测方法，通过实时监听训练信号和参考脉冲的相位补偿噪声方差，可以判断参考脉冲相位攻击是否存在。

2　相位攻击原理

2.1　系统描述

采用时分复用的 LLO-CVQKD 系统[17]如图 1 所示。发送端 Alice 使用标准化的商业激光器产生光脉冲，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，Alice 产生高斯随机数对（X_A，P_A），X_A 和 P_A 是两个独立服从均值为 0 方差的高斯随机变量。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 $\arctan(P_A/X_A)$，形成高斯调制相干态（GMCS）量子信号 $|X_A+\mathrm{i}P_A\rangle$。在参考路径，光脉冲经过另一个幅度调制器，形成强度固定的参考脉冲。随后，量子信号与参考脉冲经过时分复用后被发送出去，通过一个透传率为 T、过噪声为 ε_c 的量子信道传递给接收端 Bob。



BS: beam splitter　　HD: heterodyne detection
AM: amplitude modulator　　CD: coherent detection
PM: phase modulator　　PR: phase rotation

图 1　基于 LLO 的 CVQKD 模型图

Fig. 1　Model of CVQKD based on LLO

在接收端，接收信号经过时域解复用被分离到信号路径和参考路径。为准确补偿量子信号的相位偏移，接收端 Bob 使用激光器生成与发送端同频的光脉冲作为本振光，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。接收端利用子光脉冲 1 对参考路径上的参考脉冲信号进行外差探测（HD），测量出接收参考脉冲信号相对于 LLO 的相位偏移。基于参考脉冲的相位偏移测量结果，接收端再对子光脉冲 2 进行相位旋转（PR），以此作为对接收量子信号的相位补偿。最后，接收端将相位旋转后的光脉冲 2 与信号路径上的量子信号进行相干探测（CD）。在相干探测时，接收端 Bob 随机选择测量基，得到正交分量测量值 X_B 或 P_B。

在对接收参考脉冲信号进行外差探测时，由于接收参考脉冲信号与 LLO 的光频率相同，则外差探测的电压输出结果[23]为

$$v_{\mathrm{out}}=\alpha I_R I_L\cos\phi_R, \tag{1}$$

式中，α 是探测器响应因子，I_R 是接收参考脉冲的

光强，I_L 是 LLO 的光强，ϕ_R 是接收参考脉冲相对于 LLO 的相位偏移。由于 α 已知，而 I_R 和 I_L 可以在外差探测之前被测量，因此接收参考脉冲的相位偏移可以通过外差探测被估计。

2.2　相位补偿

为准确补偿量子信号的相位偏移，在量子信号与参考脉冲时域复用时，量子信号与参考脉冲依次占用 1 个时隙，于是接收端可以利用与量子信号相邻的两个参考脉冲去估计该量子信号的相位偏移，从而消除量子信道引入的慢漂移和激光器抖动引入的快漂移[17]。对于第 i 个接收量子信号，其相位偏移的估计值可以表示为

$$\hat{\phi}_{S,i}=\frac{1}{2}(\phi_{R,i}+\phi_{R,i+1}), \tag{2}$$

式中，$\phi_{R,i}$ 和 $\phi_{R,i+1}$ 分别为第 i 个和第 $i+1$ 个接收参考脉冲通过外差探测方式测得的相位偏移值。对于第 i 个接收量子信号，其相位补偿误差可表示为

$$\delta_{S,i}=\phi_{S,i}-\hat{\phi}_{S,i}, \tag{3}$$

式中，$\phi_{S,i}$ 为第 i 个接收量子信号相对于 Bob 本地本振光的实际相位偏移。假设量子信道和激光器引入的相位漂移在相邻两个参考脉冲之间线性变化，并且存在一个均值为 0 且方差为 V_{ch} 的相位噪声。根据(2)式和(3)式，相位补偿误差可进一步表示为

$$\delta_{S,i}=\varphi_{S,i}^{ch}-\frac{1}{2}(\varphi_{R,i}^{ch}+\varphi_{R,i+1}^{ch}), \tag{4}$$

式中，$\varphi_{S,i}^{ch}$ 为第 i 个接收量子信号的相位噪声，$\varphi_{R,i}^{ch}$ 和 $\varphi_{R,i+1}^{ch}$ 分别为第 i 个和第 $i+1$ 个接收参考脉冲的相位噪声。

2.3　相位攻击

篡改参考脉冲相位的攻击方法如图 2 所示。对于采用时分复用的 LLO-CVQKD 方案，窃听者 Eve 可以轻易地通过时域解复用器来分离发送信号中第 i 个量子信号 S_i、第 i 个参考脉冲 R_i 和第 $i+1$ 个参考脉冲 R_{i+1}。在量子信号路径，量子信号被量子存储器存储，从而维持量子态原有的信息。在参考脉冲路径，窃听者使用 BS 将参考脉冲分离为 2 个部分，其中一部分用于探测参考脉冲的强度，另一部分用于探测参考脉冲的相位。

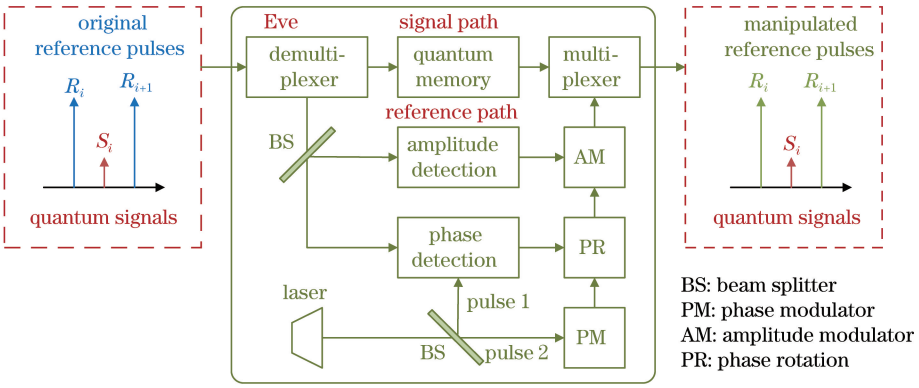


图 2　参考脉冲相位攻击示意图

Fig. 2　Diagram of phase attack on reference pulses

窃听者使用激光器产生与发送端同频的光脉冲，并通过 BS 将光脉冲分离为两个同相的子光脉冲。子光脉冲 1 对参考脉冲路径上的参考脉冲信号进行外差探测，测量得到参考脉冲的相位值。子光脉冲 2 先经过一个相位调制器(PM)，引入一个均值为 0 且方差为 V_{attack} 的相位噪声作为攻击干扰，再根据参考脉冲的相位测量结果进行 PR，使得子光脉冲 2 的相位是参考脉冲相位与攻击相位噪声之和。随后，经过 PR 的子光脉冲 2 通过一个幅度调制器(AM)，使得光强与 Alice 发送参考脉冲的强度相同。最后，被存储的量子信号与被篡改后的参考脉冲通过时分复用，被发送到量子信道中。

当 Eve 实施相位攻击后，Bob 对第 i 个接收参考脉冲的相位测量结果须改写为

$$\phi'_{R,i}=\phi_{R,i}+\varphi_{R,i}^{attack}, \tag{5}$$

式中，$\varphi_{R,i}^{attack}$ 为第 i 个接收参考脉冲上由窃听者 Eve 实施相位攻击所引入的攻击相位噪声。于是，接收端使用被篡改的参考脉冲对量子信号进行相位补偿时，第 i 个接收量子信号的相位补偿误差须改写为

$$\delta'_{S,i}=\varphi_{S,i}^{ch}-\frac{1}{2}(\varphi_{R,i}^{ch}+\varphi_{R,i+1}^{ch})-\frac{1}{2}(\varphi_{R,i}^{attack}+\varphi_{R,i+1}^{attack}). \tag{6}$$

因此，在参考脉冲相位攻击下的相位补偿噪声方差可表示为

$$V_S=\frac{3}{2}V_{ch}+\frac{1}{2}V_{attack}。 \tag{7}$$

3　安全性分析

3.1　协方差矩阵

发送端的高斯调制相干态量子信号$|X_{\mathrm{A}}+\mathrm{i}P_{\mathrm{A}}\rangle$经过一个透传率为$T$且过噪声为$\varepsilon_{\mathrm{c}}$的量子信道后，在非理想相位补偿情况下其正交分量的测量结果可表示为

$$X_{\mathrm{B}}=\sqrt{T}(X_{\mathrm{A}}\cos\delta'_{\mathrm{S}}-P_{\mathrm{A}}\sin\delta'_{\mathrm{S}})+N_X,\quad(8)$$

$$P_{\mathrm{B}}=\sqrt{T}(X_{\mathrm{A}}\sin\delta'_{\mathrm{S}}+P_{\mathrm{A}}\cos\delta'_{\mathrm{S}})+N_P,\quad(9)$$

式中，δ'_{S}是量子信号的相位补偿噪声，N_X和N_P分别是水平正交分量X和垂直正交分量P上的高斯噪声，它们独立服从均值为0且方差为$T\varepsilon_{\mathrm{c}}$的高斯分布。根据CVQKD相位补偿噪声模型[24-25]，Alice和Bob共享的混合量子态ρ_{AB}的协方差矩阵可表示为

$$\boldsymbol{\gamma}_{\mathrm{AB}}=\begin{pmatrix}V\boldsymbol{I}_2 & \sqrt{T_\kappa(V^2-1)}\boldsymbol{\sigma}_z\\ \sqrt{T_\kappa(V^2-1)}\boldsymbol{\sigma}_z & T_\kappa(V+\chi^\kappa_{\mathrm{tot}})\boldsymbol{I}_2\end{pmatrix},\quad(10)$$

式中：$\boldsymbol{I}_2$为二阶单位矩阵；$\boldsymbol{\sigma}_z$为泡利(Pauli)矩阵z分量，$\boldsymbol{\sigma}_z=\begin{pmatrix}1&0\\0&-1\end{pmatrix}$；$V$为相干态量子信号$|X_{\mathrm{A}}+\mathrm{i}P_{\mathrm{A}}\rangle$中水平正交分量$X$和垂直正交分量$P$的方差，$V=V_{\mathrm{A}}+1$，$V_{\mathrm{A}}$为高斯随机变量$X_{\mathrm{A}}$和$P_{\mathrm{A}}$的方差；$\chi^\kappa_{\mathrm{tot}}$为实际总噪声，$\chi^\kappa_{\mathrm{tot}}=\chi^\kappa_{\mathrm{line}}+\chi_{\mathrm{hom}}/T_\kappa$，$\chi^\kappa_{\mathrm{line}}$为实际线路噪声，$\chi^\kappa_{\mathrm{line}}=1/T_\kappa+\varepsilon^\kappa_{\mathrm{c}}-1$，$\chi_{\mathrm{hom}}$为接收端探测噪声，$\chi_{\mathrm{hom}}=(1-\eta+V_{\mathrm{el}})/\eta$，其中，$\eta$为探测器的探测效率，$V_{\mathrm{el}}$为探测器的电噪声。在不完美相位补偿情况下，实际透传率T_κ和实际过噪声$\varepsilon^\kappa_{\mathrm{c}}$的理论值[24]为

$$T_\kappa=\kappa T,\quad(11)$$

$$\varepsilon^\kappa_{\mathrm{c}}=\frac{1}{\kappa}[\varepsilon_{\mathrm{c}}+(1-\kappa)(V-1)],\quad(12)$$

式中，κ为相位补偿精度，$\kappa=[E(\cos\delta'_{\mathrm{S}})]^2$，其中$E(\cdot)$为随机变量的期望。当相位补偿噪声$\delta'_{\mathrm{S}}<5°$时，利用Talyor近似展开公式$\cos\delta'_{\mathrm{S}}\approx1-(\delta'_{\mathrm{S}})^2/2$，相位补偿精度可改写为

$$\kappa'=\left(1-\frac{1}{2}V_{\mathrm{S}}\right)^2,\quad(13)$$

式中，V_{S}为(7)式所表示的量子信号相位补偿噪声方差。

3.2　安全密钥率

数据反向协调的CVQKD在联合攻击下的安全密钥率[24]可表示为

$$K=\beta I_{\mathrm{AB}}-\chi_{\mathrm{BE}},\quad(14)$$

式中，β为数据协调效率，I_{AB}为Alice和Bob之间的香农互信息，χ_{BE}为Eve从Bob端获取的最大信息量，即Holevo界。若Bob使用平衡探测，香农互信息可表示为

$$I_{\mathrm{AB}}=\frac{1}{2}\mathrm{lb}\frac{V+\chi^\kappa_{\mathrm{tot}}}{1+\chi^\kappa_{\mathrm{tot}}}。\quad(15)$$

同时，根据(10)式描述的量子系统协方差矩阵，可求解出Holevo界为

$$\chi_{\mathrm{BE}}=\sum_{j=1}^{2}G\left(\frac{\lambda_j-1}{2}\right)-\sum_{j=3}^{5}G\left(\frac{\lambda_j-1}{2}\right),\quad(16)$$

式中，函数$G(x)=(x+1)\mathrm{lb}(x+1)-x\mathrm{lb}x$，而辛特征值$\lambda_j(j=1,2,\cdots,5)$表示为

$$\lambda^2_{1,2}=\frac{1}{2}(A\pm\sqrt{A^2-4B}),\quad(17)$$

$$\lambda^2_{3,4}=\frac{1}{2}(C\pm\sqrt{C^2-4D}),\quad(18)$$

$$\lambda_5=1,\quad(19)$$

式中，变量A为协方差矩阵$\boldsymbol{\gamma}_{\mathrm{AB}}$中所有子矩阵的行列式之和，$B$为协方差矩阵$\boldsymbol{\gamma}_{\mathrm{AB}}$的行列式，$C$为Bob完成测量后量子系统协方差矩阵的子矩阵行列式之和，D为Bob完成测量后量子系统协方差矩阵的行列式，取值分别为

$$A=V^2+2T_\kappa(1-V^2)+T^2_\kappa(V+\chi^\kappa_{\mathrm{line}})^2,\quad(20)$$

$$B=T^2_\kappa(1+V\chi^\kappa_{\mathrm{line}})^2,\quad(21)$$

$$C=\frac{A\chi_{\mathrm{hom}}+V\sqrt{B}+T_\kappa(V+\chi^\kappa_{\mathrm{line}})}{T_\kappa(V+\chi^\kappa_{\mathrm{line}})},\quad(22)$$

$$D=\frac{V\sqrt{B}+B\chi_{\mathrm{hom}}}{T_\kappa(V+\chi^\kappa_{\mathrm{line}})}。\quad(23)$$

3.3　参数估计

在实际系统中，实际透传率T_κ和实际过噪声$\varepsilon^\kappa_{\mathrm{c}}$需要通过训练信号来实时估计。当Bob接收到一定数量的量子信号后，Bob从中随机挑选M个接收量子信号作为训练信号，并随机选择测量基去测量这些训练信号，得到正交分量X或P的测量值$\{y_i\}(i=1,2,\cdots,M,M$为训练信号数量)。随后，Bob利用经典信道公布训练信号的位置和对应的测量基，Alice据此将对应的发送量子信号的正交分量值$\{x_i\}(i=1,2,\cdots,M)$通过经典信道传递给Bob。根据最大似然估计方法[16]，Bob估计出实际透传率和实际过噪声为

$$\hat{T}_\kappa=\left(\frac{\sum_{i=1}^{M}x_iy_i}{\sum_{i=1}^{M}x_i^2}\right)^2,\quad(24)$$

$$\hat{\varepsilon}_{\mathrm{c}}^{\kappa}=\frac{1}{M\hat{T}_{\kappa}}\sum_{i=1}^{M}\left(y_i-\sqrt{\hat{T}_{\kappa}}x_i\right)^2。\tag{25}$$

根据统计可知 $E(\hat{T}_{\kappa})=T_{\kappa}$ 和 $E(\hat{\varepsilon}_{\mathrm{c}}^{\kappa})=\varepsilon_{\mathrm{c}}^{\kappa}$，因此 Alice 和 Bob 可以准确估计安全密钥率。

4　相位攻击探测

Alice 和 Bob 根据参数估计结果来评估安全密钥率，从而在安全密钥率限定的速率下生成安全密钥，因此一般不用关注量子信道是否被窃听或被攻击。不过，探测窃听对实际系统而言仍然具有意义。例如，当 Alice 和 Bob 发现窃听后，可以采用其他更加安全的量子信道来通信，以获得更高的安全密钥率。针对参考脉冲相位攻击，一种探测相位攻击的方法被提出。该方法通过实时监听训练信号和参考脉冲的相位补偿噪声方差，判断出参考脉冲相位攻击是否存在。在硬件电路方面，接收端需要增加 2 个噪声监听器(noise monitor)，如图 3 所示。

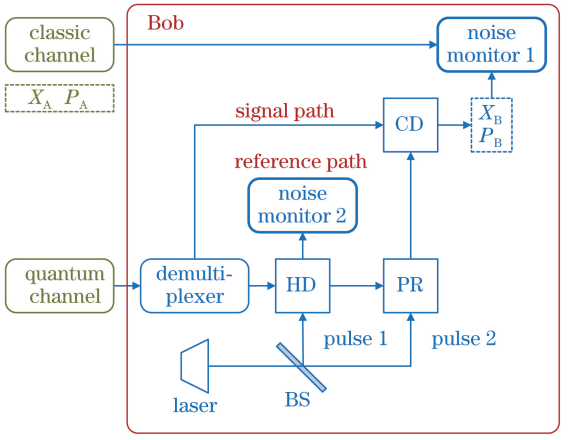


图 3　基于相位攻击探测的接收端模型图

Fig. 3　Model of receiver based on detection of phase attack

在噪声监听器 1 中，Bob 对训练信号的两个正交分量同时进行测量，并将测量结果(X_{B}，P_{B})与 Alice 通过经典信道公布的发送信号正交分量(X_{A}，P_{A})进行对比，从而估计出量子信号的相位补偿噪声方差[21]，即

$$\hat{V}_{\mathrm{S}}=\frac{1}{M}\sum_{i=1}^{M}\left(\arctan\frac{P_{\mathrm{A}}}{X_{\mathrm{A}}}-\arctan\frac{P_{\mathrm{B}}}{X_{\mathrm{B}}}\right)^2。\tag{26}$$

理论上，量子信号的相位补偿噪声方差估计值是无偏估计，即 $E(\hat{V}_{\mathrm{S}})=V_{\mathrm{S}}$。

在噪声监听器 2 中，当发送脉冲频率足够高时，三个相邻的参考脉冲上的相位偏移可近似为线性关系，于是 Bob 可以利用第 $i-1$ 个和第 $i+1$ 个接收参考脉冲去补偿第 i 个接收参考脉冲的相位偏移，从而估计出参考脉冲自身进行相位补偿后的相位补偿噪声方差。第 i 个接收参考脉冲的相位补偿噪声可表示为

$$\delta'_{\mathrm{R},i}=\phi'_{\mathrm{R},i}-\frac{1}{2}(\phi'_{\mathrm{R},i-1}+\phi'_{\mathrm{R},i+1}),\tag{27}$$

式中，$\phi'_{\mathrm{R},i-1}$，$\phi'_{\mathrm{R},i}$，$\phi'_{\mathrm{R},i+1}$分别是第 $i-1$ 个，第 i 个，第 $i+1$ 个接收参考脉冲在相位攻击下的相位测量结果。理论上，参考脉冲的相位补偿噪声方差为

$$V_{\mathrm{R}}=\frac{3}{2}V_{\mathrm{ch}}+\frac{3}{2}V_{\mathrm{attack}}。\tag{28}$$

当 Bob 接收到 L 个参考脉冲时，除首尾两个参考脉冲外，Bob 几乎可以利用所有的接收参考脉冲的相位测量结果去估计参考脉冲的相位补偿噪声方差，即

$$\hat{V}_{\mathrm{R}}=\frac{1}{L-2}\sum_{i=2}^{L-1}(\delta'_{\mathrm{R},i})^2。\tag{29}$$

理论上，参考脉冲的相位补偿噪声方差估计值是无偏估计，即 $E(\hat{V}_{\mathrm{R}})=V_{\mathrm{R}}$。最后，Bob 通过对比训练信号的相位补偿噪声方差和参考脉冲的相位补偿噪声方差是否一致，可以判断参考脉冲相位攻击是否存在。

5　仿真结果与分析

仿真实验中的系统参数根据实际 CVQKD 实验来确定[24]，参数取值如表 1 所示。仿真实验中，在量子信号和参考脉冲的相位上都叠加一个方差为 V_{ch}的高斯噪声作为信道的相位噪声，并且在参考脉冲相位上还叠加另外一个方差为 V_{attack}的高斯噪声作为 Eve 实施相位攻击的相位噪声。相位噪声方差和对应的相位补偿精度如表 2 所示。

表 1　实际 CVQKD 系统参数

Table 1　Parameters for practical CVQKD systems

Parameter	V_{A}	V_{el}	ε_{c}	β	η
Value	18.900	0.001	0.010	0.926	0.590

表 2　相位噪声与相位补偿精度

Table 2　Phase noise and phase compensation accuracy

Parameter	Group 1	Group 2	Group 3
V_{ch} /rad^2	0.0001	0.0001	0.0001
V_{attack} /rad^2	0	0.0009	0.0025
κ'	0.9998	0.9994	0.9986

在参考脉冲相位攻击下的 LLO-CVQKD 系统

安全密钥率仿真结果如图 4 所示。仿真结果中的实线、虚线和点横线为根据相位噪声方差计算得到的安全密钥率，而圆形、方形和三角形为根据 2000 个训练信号的测量结果估计得到的安全密钥率。仿真结果表明，理论评估得到的安全密钥率与实验参数估计得到的安全密钥率一致。因此，基于相位补偿噪声模型可以准确描述参考脉冲相位攻击对 LLO-CVQKD 安全密钥率的影响。

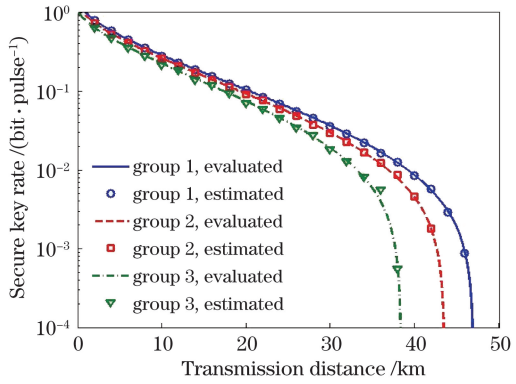


图 4　参考脉冲相位攻击下的 LLO-CVQKD 安全密钥率

Fig. 4　Secure-key rate of LLO-CVQKD under phase attack on reference pulses

在参考脉冲相位攻击下，量子信号(QS)和参考脉冲(RP)的相位补偿噪声方差如图 5 所示，其实验参数如表 3 所示。仿真实验中监听 50 个数据块，每个数据块包含 5000 对量子信号和参考脉冲，从量子信号中随机选择 2000 个作为训练信号，根据(26)式估计量子信号的相位补偿噪声方差，根据(29)式估计参考脉冲的相位补偿噪声方差。仿真结果表明，训练信号和参考脉冲的相位补偿噪声方差的估计值与理论值一致，通过监听训练信号和参考脉冲的相位补偿噪声方差是否一致，可以有效判断参考脉冲相位攻击是否存在。

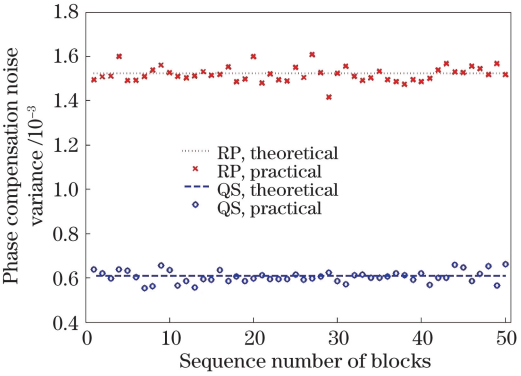


图 5　相位攻击下量子信号和参考脉冲的相位补偿噪声方差

Fig. 5　Phase compensation noise variances of quantum signals and reference pulses under phase attack

表 3　相位补偿噪声方差实验参数

Table 3　Experimental parameters of phase compensation noise variances

Parameter	V_{ch}	V_{attack}	V_S	V_R
Value /rad^2	0.0001	0.0009	0.0006	0.0015

6　结　　论

针对基于本地本振光的连续变量量子密钥分发的参考脉冲传输带来新的安全问题，提出一种篡改参考脉冲相位的攻击方法。利用相位补偿噪声模型，分析了基于本地本振光的连续变量量子密钥分发在参考脉冲相位攻击下的实际安全性。仿真结果表明，理论评估得到的安全密钥率与实验参数估计得到的安全密钥率一致，因此利用相位补偿噪声模型可以准确描述参考脉冲相位攻击对基于本地本振光的连续变量量子密钥分发安全密钥率的影响。另外，提出一种监听相位补偿噪声方差的相位攻击探测方法。仿真结果表明，通过实时监听训练信号和参考脉冲的相位补偿噪声方差，可以有效判断参考脉冲相位攻击是否存在。

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] Lo H K. Decoy state quantum key distribution[J]. International Journal of Quantum Information, 2005, 3(supp01): 143.

[4] Claudon J, Bleuse J, Malik N S, *et al*. A highly efficient single-photon source based on a quantum dot in a photonic nanowire[J]. Nature Photonics, 2010, 4(3): 174-177.

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

[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] Ma S T, Guo D B, Xue Z, *et al*. Multidimensional reconciliation for continuous-variable quantum key

distribution based on two-edge type low-density parity-check codes[J]. Acta Optica Sinica, 2019, 39(5): 0527001.
马识途, 郭大波, 薛哲, 等. 基于双边类型低密度奇偶校验码的连续变量量子密钥分发多维数据协调[J]. 光学学报, 2019, 39(5): 0527001.

[8] 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.

[9] Huang D, Huang P, Lin D K, *et al*. Long-distance continuous-variable quantum key distribution by controlling excess noise[J]. Scientific Reports, 2016, 6: 19201.

[10] 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.

[11] 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.

[12] Qin H, Kumar R, Alléaume R. Quantum hacking: saturation attack on practical continuous-variable quantum key distribution [J]. Physical Review A, 2016, 94(1): 012325.

[13] Ma X C, Sun S H, Jiang M S, *et al*. Enhancement of the security of a practical continuous-variable quantum-key-distribution system by manipulating the intensity of the local oscillator[J]. Physical Review A, 2014, 89(3): 032310.

[14] Liu W Q, Peng J Y, Huang P, *et al*. Monitoring of continuous-variable quantum key distribution system in real environment[J]. Optics Express, 2017, 25(16): 19429-19443.

[15] Jouguet P, Kunz-Jacques S, Diamanti E. Preventing calibration attacks on the local oscillator in continuous-variable quantum key distribution[J]. Physical Review A, 2013, 87(6): 062313.

[16] Huang P, Huang J Z, Wang T, *et al*. Robust continuous-variable quantum key distribution against practical attacks[J]. Physical Review A, 2017, 95(5): 052302.

[17] 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.

[18] 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.

[19] 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.

[20] 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.

[21] 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(1): 012310.

[22] 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.

[23] He Y. Phase matching of a heterodyne detection system[J]. Chinese Journal of Lasers, 1997, 24(10): 930-934.
何毅. 外差探测系统的相位匹配研究[J]. 中国激光, 1997, 24(10): 930-934.

[24] 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.

[25] 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.