补充材料 (2025 *Acta Phys. Sin.* **74** 160303)

《基于卡尔曼滤波的本地本振连续变量量子秘密共享》的补充材料

廖骁[1)]　费焯迎[1)]　王一军[2)†]

1) (湖南大学信息科学与工程学院, 长沙　410082)

2) (中南大学自动化学院, 长沙　410083)

补充材料A　矢量KF滤波流程

矢量KF系统状态方程为

$$\theta(k)=\theta(k-1)+T_{\mathrm{s}}\varphi(k)+\omega(k), \tag{S1}$$

$$\varphi(k)=\varphi(k-1)+\nu(k), \tag{S2}$$

其中T_{s}为脉冲间隔, $\omega(k)$和$\varphi(k)$代表相位快、慢漂移, 它们为相互独立的零均值高斯噪声, 各自方差$\sigma_{\mathrm{w}}^2=2\pi f_{\mathrm{AB}}T_{\mathrm{S}}$和$\sigma_{\mathrm{v}}^2=(2\pi f_{\mathrm{AB}})^2$均与发射端和接收端激光器总谱线宽度$f_{\mathrm{AB}}$相关. 用户2和Dealer参考相位为输入信号, 其测量方程为

$$y(k)=\theta(k)+n(k), \tag{S3}$$

其中$n(k)$为方差σ_{n}^2的测量噪声.

状态方程和测量方程写成矩阵形式分别为

$$\boldsymbol{s}(k)=\boldsymbol{A}\boldsymbol{s}(k-1)+\boldsymbol{\omega}(k), \tag{S4}$$

$$y(k)=\boldsymbol{C}\boldsymbol{s}(k-1)+n(k), \tag{S5}$$

其中$\boldsymbol{A}=\begin{bmatrix}1 & T_{\mathrm{s}}\\ 0 & 1\end{bmatrix}$, $\boldsymbol{C}=\begin{bmatrix}1 & 0\end{bmatrix}$. 状态噪声和测量噪声的协方差矩阵相应地写为

$$\boldsymbol{Q}=E\left[\omega(k)\omega^{\mathrm{T}}(k)\right]=\begin{bmatrix}\sigma_{\mathrm{w}}^2 & 0\\ 0 & \sigma_{\mathrm{v}}^2\end{bmatrix}, \tag{S6}$$

$$\boldsymbol{R}=E\left[n^2(k)\right]=\sigma_n^2. \tag{S7}$$

1) 初始化

初始状态和初始估计误差可由前两个参考相位分别计算得到

$$\hat{\boldsymbol{s}}(2)=\begin{bmatrix}y(2)\\ \dfrac{y(2)-y(1)}{T_{\mathrm{s}}}\end{bmatrix}, \tag{S8}$$

$$P(2)=E\left\{[\boldsymbol{s}(2)-\hat{\boldsymbol{s}}(2)][\boldsymbol{s}(2)-\hat{\boldsymbol{s}}(2)]^{\mathrm{T}}\right\}=\begin{bmatrix}\sigma_{\mathrm{n}}^2 & \dfrac{\sigma_n^2}{T_s}\\ \dfrac{\sigma_n^2}{T_{\mathrm{s}}} & \dfrac{2\sigma_n^2+\sigma_{\mathrm{w}}^2}{T_{\mathrm{s}}^2}\end{bmatrix} \tag{S9}$$

为获得σ_n^2, 用户2和Dealer取部分参考相位估计, 公式如下:

$$E\left\{[y(k+1)+y(k-1)-2y(k)]^2\right\}=6\sigma_{\mathrm{n}}^2+2\sigma_{\mathrm{w}}^2, \tag{S10}$$

之后用户2和Dealer披露所取相位位置, 所有参与方需丢弃相应数据.

2) 预测

根据前一参考相位得到后一参考相位的预测值, 预测状态和预测估计误差分别为

$$\hat{\boldsymbol{s}}(k)=\boldsymbol{A}\hat{s}(k-1), \tag{S11}$$

$$\bar{P}(k)=\boldsymbol{A}\bar{P}(k-1)\boldsymbol{A}^{\mathrm{T}}+\boldsymbol{Q} \tag{S12}$$

至此, 可以得到卡尔曼增益

$$\boldsymbol{K}(k)=\bar{P}(k)\boldsymbol{C}^{\mathrm{T}}\left[\boldsymbol{C}\bar{P}(k)\boldsymbol{C}^{\mathrm{T}}+\boldsymbol{R}\right]^{-1} \tag{S13}$$

3) 估计

对其余参考相位, 结合卡尔曼增益, 当前状态和当前估计误差可推导为

$$\hat{\boldsymbol{s}}(k)=\bar{s}(k)\ +\boldsymbol{K}(k)[y(k)-\boldsymbol{C}\bar{s}(k)], \tag{S14}$$

$$\boldsymbol{P}(k)=[\boldsymbol{I}-\boldsymbol{K}(k)\boldsymbol{C}]\bar{\boldsymbol{P}}(k), \tag{S15}$$

其中$\boldsymbol{I}$为二阶单位矩阵. 之后根据当前状态补偿量子信号相位漂移, 完成本次迭代. 估计误差μ由稳态$\boldsymbol{P}$的矩阵元素得到, 即解矩阵Riccati方程[28]:

$$\boldsymbol{AP}+\boldsymbol{PA}^{\mathrm{T}}-\boldsymbol{PC}^{\mathrm{T}}\boldsymbol{R}^{-1}\boldsymbol{CP}+\boldsymbol{Q}=0 \tag{S16}$$

由于矩阵$\boldsymbol{Q}$和$\boldsymbol{R}$是对角矩阵, 且矢量KF能够消除慢漂移影响, 矩阵Riccati 方程可简化为应用于标量KF的代数Riccati, 此时均方误差满足方程$\mu^2+\sigma_{\mathrm{w}}^2\mu-\sigma_{\mathrm{w}}^2\sigma_{\mathrm{n}}^2=0$.

补充材料B　CVQSS密钥率计算

如第2节所述, CVQSS密钥率为各CVQKD链路密钥率最小值, 其下界可表示为

$$R=\beta I_{\mathrm{AB}}-\chi_{\mathrm{BE}}, \tag{S17}$$

其中, β为反向协商效率, I_{AB}为该链路用户与Dealer之间的Shannon 互信息, χ_{BE}为窃听者和不诚实用户根据Dealer测量可获取的最大信息量. 结合第4节给出的系统过噪声, 信道输入端附加噪声为

$$\chi_{\mathrm{line}}=\frac{1}{T}-1+\varepsilon, \tag{S18}$$

Dealer输入端探测噪声为

$$\chi_{\mathrm{het}} = \frac{2-\eta+2v_{\mathrm{el}}}{\eta}, \tag{S19}$$

其中η为检测效率, v_{el}为不完善检测仪的电子噪声. 因此, 信道输入端总噪声可以表示为

$$\chi_{\mathrm{tot}} = \chi_{\mathrm{line}} + \frac{\chi_{\mathrm{het}}}{T}. \tag{S20}$$

Shannon互信息计算公式为

$$I_{\mathrm{AB}} = \log_2 \frac{V+\chi_{\mathrm{tot}}}{1+\chi_{\mathrm{tot}}}, \tag{S21}$$

其中$V = V_{\mathrm{A}} + 1$. χ_{BE}则可以计算为[57]

$$\chi_{\mathrm{BE}} = \sum_{j=1}^{2} G\left(\frac{\lambda_j - 1}{2}\right) - \sum_{j=3}^{5} G\left(\frac{\lambda_j - 1}{2}\right), \tag{S22}$$

其中$G(x) = (x+1)\log_2(x+1) - x\log_2 x$和辛特征值:

$$\lambda_{1,2}^2 = \frac{1}{2}\left[A \pm \sqrt{A^2 - 4B}\right], \tag{S23}$$

$$\lambda_{3,4}^2 = \frac{1}{2}\left[C \pm \sqrt{C^2 - 4D}\right], \tag{S24}$$

$$\lambda_5 = 1, \tag{S25}$$

其中:

$$A = V^2(1-2T) + 2T + T^2(V+\chi_{\mathrm{line}})^2, \tag{S26}$$

$$B = T^2(V\chi_{\mathrm{line}} + 1)^2, \tag{S27}$$

$$C = \frac{A\chi_{\mathrm{het}}^2 + B + 1 + 2\chi_{\mathrm{het}}\left[V\sqrt{B} + T(V+\chi_{\mathrm{line}})\right] + 2T\left(V^2-1\right)}{\left[T(V+\chi_{\mathrm{tot}})\right]^2}, \tag{S28}$$

$$D = \left[\frac{V+\sqrt{B}\chi_{\mathrm{het}}}{T(V+\chi_{\mathrm{tot}})}\right]^2 \tag{S29}$$