基于非理想测量基选择的水下连续变量量子密钥分发方案*

吴晓东[1)] 黄端[2)†]

1) (福建理工大学管理学院, 福州 350118)

2) (中南大学电子信息学院, 长沙 410083)

(2024 年 6 月 6 日收到; 2024 年 8 月 27 日收到修改稿)

在基于零差探测的水下连续变量量子密钥分发系统中, 测量基选择是必不可少的步骤. 然而在实际中, 接收端数模转换器的带宽有限, 这会导致测量基选择出现缺陷, 即接收方无法在相位调制器上精确地调制出相应的相位角来进行测量基选择以实施零差探测. 非理想测量基选择会引入额外的过噪声, 影响水下连续变量量子密钥分发方案的安全性. 针对这个问题, 本文提出基于非理想测量基选择的水下连续变量量子密钥分发方案, 详细分析非理想测量基选择对水下连续变量量子密钥分发系统性能的影响. 研究结果表明, 由非理想测量基选择所引入的过噪声能够降低水下高斯调制量子密钥分发的密钥率与最大传输距离, 因而降低系统的安全性. 为了实现可靠的水下连续变量量子密钥分发, 本文对非理想测量基选择所引入的额外过噪声进行定量分析并获得其安全界限, 并且考虑不同海水深度对所提出方案安全界限的影响, 有效地解决由非理想测量基选择所带来的安全隐患. 此外, 对所提出的方案, 本文不仅考虑了其渐近安全性, 也考虑了其组合安全性, 后者能够获得比前者更紧的性能曲线. 本文所提出的方案旨在推动水下连续变量量子密钥分发系统的实用化进程, 为全球量子通信网络的水下通信中水信道参数的准确评估提供理论指导.

关键词: 非理想测量基选择, 连续变量量子密钥分发, 海水信道, 海水深度

PACS: 03.67.Dd, 03.67.Hk **DOI:** 10.7498/aps.73.20240804

CSTR: 32037.14.aps.73.20240804

1 引 言

水下无线通信技术在海洋探测系统的实用化进程中发挥着重要作用, 主要原因在于该技术能够满足水下航行器与传感器之间进行可靠的数据传输的需求[1,2]. 其中, 水下无线光通信 (underwater wireless optical communication, UWOC) 技术由于能够在短距离范围内实现高速数据传输而备受关注[3]. UWOC 通常被认为是比声学通信和射频通信更安全的通信技术[1,3]. 为了进一步提升其传输距离和数据传输速率, UWOC 系统已得到广泛的研究与论证[4]. 然而, 对于 UWOC 系统的安全性问题很少有相关研究. 2017 年, Kong 等[3] 研究验证了 UWOC 系统随着传输距离的增加或水信道浑浊程度的加剧, 信息泄漏的可能性大大增加, 对 UWOC 系统的安全性构成巨大威胁.

幸运的是, 量子密钥分发 (quantum key distribution, QKD)[5,6] 技术基于量子力学的基本定律, 能够保证信息传输的无条件安全, 是解决 UWOC 信息安全问题的一种有效方法. 通常, QKD 主要可分为离散变量 (discrete variable, DV)QKD[7–10]

* 福建省自然科学基金 (批准号: 2023J01940) 和福建理工大学科研启动基金 (批准号: GY-Z22042) 资助的课题.

† 通信作者. E-mail: duanhuang@csu.edu.cn

与连续变量 (continuous variable, CV) QKD[11–16]. 相比于 DV-QKD, CV-QKD 易融于现有光通信系统, 无需使用造价高昂的单光子探测器, 而是采用成本更低的相干探测器, 具有更大的密钥率以及更高的探测效率. 作为 CV-QKD 应用最广泛的一种类型, 高斯调制相干态 (Gaussian modulated coherent state, GMCS) 方案在理论安全性 [17–21] 和实验 [22–29] 方面都已取得显著进展. 此外, GMCS 方案也被应用于其他连续变量量子通信方案中, 比如量子秘密共享方案 [30,31], 量子数字签名方案 [32] 等.

由于地球约 71% 的表面积被海洋所覆盖, 因此海水也是一种非常重要的信息传输信道. 水下 QKD 技术能够用于提升水下信息传输的安全性, 对构建全球量子通信网络至关重要. 因此近年来, 研究人员对水下 QKD 技术的可行性进行了理论 [33,34] 和实验 [35–39] 研究. 然而, 上述研究均是基于 DV-QKD 方案. 最近, 水下 CV-QKD 技术由于自身独特的优势而备受关注, 并且已进行了相关的理论研究 [40–44] 以及实验研究 [45]. 在水下 CV-QKD 方案的实际部署中, 接收方通常会对所接收到的信息进行零差或外差探测. 在执行零差探测时, 由于只对正则分量 X 和 P 的其中之一进行测量, 因此测量基的选择是必不可少的步骤. 然而, 在实际系统的接收端, 由于所采用的数模转换器 (digital-to-analog convertor, DAC) 其带宽有限, 使得测量基在选择过程中会产生角度偏差 [46]. 这会导致合法通信方在评估海水信道透过率和过噪声时与真实值发生偏差, 影响方案的安全性.

基于上述分析, 本文提出基于非理想测量基选择的水下 CV-QKD 方案, 并且在实际海水信道条件下对所提出的方案进行安全性分析. 为了对非理想测量基选择所引入的额外过噪声进行定量分析并获得其安全界限, 本文引入对应于 DAC 中运算放大器环路增益的参数, 构建水下 CV-QKD 方案的综合安全性框架. 仿真结果表明, 由非理想测量基选择所引入的额外过噪声能够降低水下 CV-QKD 方案的密钥率与最大传输距离, 影响其安全性. 但所提出的安全性分析框架模型能够有效地解决由非理想测量基选择所带来的安全隐患, 有助于推动水下 CV-QKD 系统的实用化进程. 本文第 2 节详细描述了所提出的基于非理想测量基选择的水下 CV-QKD 方案; 第 3 节对所提出的方案的安全性进行分析, 包括其渐近安全性与组合安全性; 第 4 节总结全文.

2 基于非理想测量基选择的水下 CV-QKD 方案

本节首先介绍基于非理想测量基选择的水下 CV-QKD 方案, 之后对海水信道的光传播特性进行详细分析.

2.1 基于非理想测量基选择的水下 CV-QKD 方案描述

图 1 给出了基于非理想测量基选择的水下 CV-QKD 制备-测量 (prepare-and-measure, PM) 方案图. 发送方 Alice 采用随机数发生器生成两个

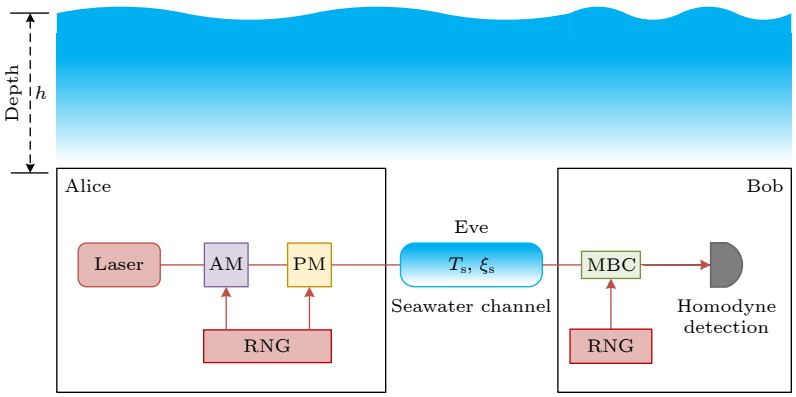

图 1 基于非理想测量基选择的水下 CV-QKD 制备-测量方案图. RNG 为随机数发生器, AM 为振幅调制器, PM 为相位调制器, MBC 表示测量基选择, T_s 表示海水信道的透过率, ξ_s 表示海水信道过噪声

Fig. 1. Prepare-and-measure version of underwater continuous variable quantum key distribution scheme based on imperfect measurement basis choice. RNG, random number generator; AM, amplitude modulator; PM, phase modulator; MBC, measurement basis choice; T_s , the transmittance of seawater channel; ξ_s , the excess noise of seawater channel.

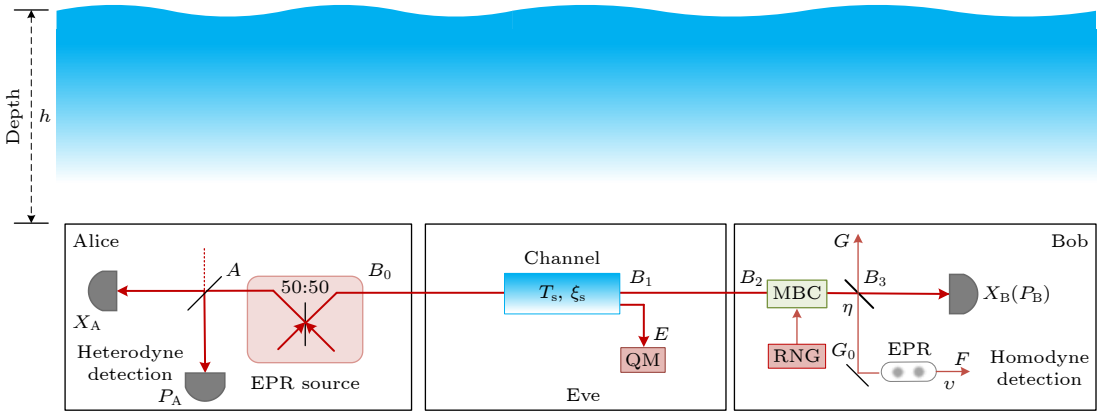

图 2 基于非理想测量基选择的水下 CV-QKD 纠缠模型原理图 (QM 为量子存储器)

Fig. 2. Schematic diagram of the entanglement-based model of underwater continuous variable quantum key distribution scheme based on imperfect basis choice (QM, quantum memory).

高斯随机数 X_A 与 P_A, 两者的均值为 0, 方差为 V_A. 之后, Alice 利用振幅调制器和相位调制器将密钥信息加载到散粒噪声为 $(\Delta X_A,\ \Delta P_A)$ 的初始相干态中, 并经海水信道发送给接收方 Bob. 海水信道的透过率与过噪声分别为 T_s 与 ξ_s, 此处过噪声可以理解为由于 Eve 的窃听所引入的噪声. 当 Bob 接收到由 Alice 发送的信息后, 采用零差探测器随机对所接收到的相干态其中一个正则分量进行测量. 由于平衡零差探测器能够通过调节量子信号与本振光之间的差分相位 ψ 来测量正则分量 X_B 或 P_B. 因此, Bob 可以通过采用相位调制器来进行测量基选择, 即 Bob 通过在相位调制器上选择 0 或 $\pi/2$ 来执行测量基选择流程.

图 2 给出了与 PM 方案等价的纠缠模型方案. 在图 2 中, Alice 相干态的制备等价为对双模压缩态 (Einstein-Podolsky-Rosen, EPR) 其中一个模 A 进行外差探测, 而另一个模 B_0 则经过海水信道后转换为模 B_1, 并以模 B_2 发送给接收方 Bob 进行测量, Bob 通过在相位调制器上选择 0 或 $\pi/2$ 来执行测量基选择流程. 此外, 模 E 表示 Eve 所收集的辅助模, 利用量子存储器对其进行存储. 在 Bob 端, 用透过率为 η 的分束器表示 Bob 实际探测器的量子效率, 而探测器电噪声 υ_{el} 则等价于方差为 υ 的辅助 EPR 态 ρ_{FG_0} 其中一个模 G_0 经分束器后引入的噪声. 模 G_0 与模 B_2 经分束器相互作用后得到模 B_3 和模 G, 辅助 EPR 态另一个模为 F.

零差探测器的探测原理图如图 3 所示. 在图 3 中, 当量子信号光与本征光 (LO) 经分束器进行干涉后, 每束出射光束都被引导到光子探测器用于测量光电流 $I_1(t)$ 和 $I_2(t)$, 之后进行电子化处理, 并将 $I_1(t)$ 和 $I_2(t)$ 相减. 为了简化分析, 此处假定所测量的光电流 $I_1(t)$ 与光子数 n_1 成正比, 并且 $I_2(t)$ 与光子数 n_2 成正比. 50∶50 分束器的两个输出光场模的湮灭算符分别为 $\hat{a}_1$ 与 $\hat{a}_2$, 其表达式为

$$\begin{aligned}\hat{a}_1 &= (\hat{a}_S + \mathrm{i}\hat{a}_{LO})/\sqrt{2},\\ \hat{a}_2 &= (\hat{a}_{LO} + \mathrm{i}\hat{a}_S)/\sqrt{2},\end{aligned} \tag{1}$$

其中 $\hat{a}_S$ 与 $\hat{a}_{LO}$ 分别表示信号光模与本征光模. 则平衡零差探测的输出结果 I_t (光电流差), 其表达式为[46]

$$\begin{aligned}I_t &= I_1(t) - I_2(t) \propto \langle\hat{n}_1\rangle - \langle\hat{n}_2\rangle\\ &\propto X_B\cos\psi + P_B\sin\psi,\end{aligned} \tag{2}$$

其中 ψ 表示信号光与本征光之间的差分相位. 由 (2) 式可知, 零差探测器的测量值 I_t 取决于本振光的相位, 即所采用的平衡零差探测器可以通过调整信号光与本征光之间的差分相位 ψ 来选择是测量正则分量 X_B 还是正则分量 P_B. 因此, 图 3 中所采

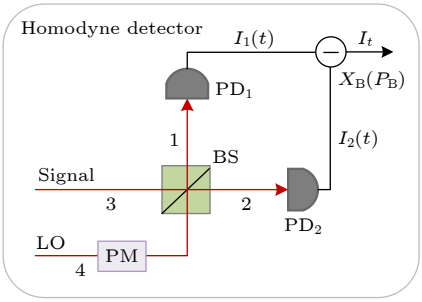

图 3 零差探测器的探测原理图 (LO 为本振光, PM 为相位调制器, BS 为分束器, $PD_{1(2)}$ 为光电探测器)

Fig. 3. Principle of balanced homodyne detector. LO, local oscillator; PM, phase modulator; BS, beam splitter; $PD_{1(2)}$, photodetector.

用的相位调制器用于实现连续变量测量基的选择. 换言之, 当接收方 Bob 利用相位调制器令差分相位 $\psi=0$ 时, 则表明 Bob 测量的是正则分量 X_{B}; 当接收方 Bob 利用相位调制器令差分相位 $\psi=\pi/2$ 时, 则表明 Bob 测量的是正则分量 P_{B}. 因此, 在本文所提出的方案中, 连续变量的测量基指的是正则分量 X_{B} 或 P_{B}, 测量基选择指的是正则分量 X_{B} 或 P_{B} 的选取.

由于相位调制器的调制相位与调制电压线性相关, 因此差分相位 ψ 的表达式可写为

$$\psi=\frac{\Omega}{\Omega_{\pi}}\pi, \tag{3}$$

式中 Ω_{π} 表示 Bob 端相位调制器的半波电压, 并且其调制电压 Ω 的表达式为

$$\Omega=2S\Omega_{\pi}, \tag{4}$$

其中参数 S 表示支持测量基选择的随机数, 可由 DAC 导出. 此外, Alice 端的相关数据 P_{A} 表达式为 $P_{\mathrm{A}}=I_{\mathrm{A}}\sin\phi$, 其中 I_{A} 表示极坐标下量子信号的强度, ϕ 表示极坐标下量子信号的相位. 假设方案中所采用的 DAC 是完美的, 并且在实际环境下进行理想测量基选择所得到的测量结果为 P_{B}, 其表达式可写为

$$P_{\mathrm{B}}=\sqrt{T_{\mathrm{s}}}\left[I_{\mathrm{A}}\sin\left(\phi+\varpi\right)+\xi_{\mathrm{s}}\right], \tag{5}$$

其中 ϖ 表示相位漂移. 此外, 假定 Alice 端的另外一个数据为 $P_{\mathrm{A}}^{*}=I_{\mathrm{A}}\sin\left(\phi+\vartheta\right)$, 其中 ϑ 为已知相位. 对 $P_{\mathrm{A}}P_{\mathrm{B}}$ 与 $P_{\mathrm{A}}^{*}P_{\mathrm{B}}$ 的期望进行计算, 可得[46]

$$\begin{aligned}&E\left[P_{\mathrm{A}}P_{\mathrm{B}}\right]\\&=E\left[I_{\mathrm{A}}\sin\phi\left(\sqrt{T_{\mathrm{s}}}I_{\mathrm{A}}\sin\left(\phi+\varpi\right)+\sqrt{T_{\mathrm{s}}}\xi_{\mathrm{s}}\right)\right]\\&=\sqrt{T_{\mathrm{s}}}V_{\mathrm{A}}\cos\varpi,\end{aligned} \tag{6}$$

$$\begin{aligned}&E\left[P_{\mathrm{A}}^{*}P_{\mathrm{B}}\right]\\&=E\left[I_{\mathrm{A}}\sin\left(\phi+\vartheta\right)\left(\sqrt{T_{\mathrm{s}}}I_{\mathrm{A}}\sin\left(\phi+\varpi\right)+\sqrt{T_{\mathrm{s}}}\xi_{\mathrm{s}}\right)\right]\\&=\sqrt{T_{\mathrm{s}}}V_{\mathrm{A}}\cos\left(\vartheta-\varpi\right)\ .\end{aligned} \tag{7}$$

然而, 当 DAC 的带宽有限时, 这表明此时调制电压 Ω 和调制相位 ψ 与它们的真实值发生偏离, 则有

$$\psi^{*}=\frac{\Omega\left|\Xi\right|}{\Omega_{\pi}\left(1+\left|\Xi\right|\right)}\pi=\frac{\left|\Xi\right|}{1+\left|\Xi\right|}\psi, \tag{8}$$

其中 Ξ 表示 DAC 中运算放大器的环路增益, 并且与运算放大器的增益带宽成比例[46]. 此处, ψ^{*} 的实际值将会与预期值产生差异. 将 ψ^{*} 代入 (5) 式, 则有

$$P_{\mathrm{B}}^{*}=\sqrt{T_{\mathrm{s}}}\left[I_{\mathrm{A}}\sin\left(\phi+\varpi\right)\sin\psi^{*}+\xi_{\mathrm{s}}\right]. \tag{9}$$

将 (9) 式和 (5) 式进行比较可以发现, 此时所获得的测量基 P_{B}^{*} 与实际测量基 P_{B} 存在偏差. 在这种情况下, 无论所选择的测量基是 X_{B}^{*} 或 P_{B}^{*}, 都与实际测量基 X_{B} 或 P_{B} 存在偏差, 即由于 DAC 带宽限制而导致的非理想测量基选择. 则

$$\begin{aligned}&E\left[P_{\mathrm{A}}P_{\mathrm{B}}^{*}\right]\\&=E\left[I_{\mathrm{A}}\sin\phi\left(\sqrt{T_{\mathrm{s}}}I_{\mathrm{A}}\sin\left(\phi+\varpi\right)\sin\psi^{*}+\sqrt{T_{\mathrm{s}}}\xi_{\mathrm{s}}\right)\right]\\&=\sqrt{T_{\mathrm{s}}}V_{\mathrm{A}}\cos\varpi E\left[\sin\psi^{*}\right],\end{aligned} \tag{10}$$

$$\begin{aligned}E\left[P_{\mathrm{A}}^{*}P_{\mathrm{B}}^{*}\right]\ &=E\Big[I_{\mathrm{A}}\sin\left(\phi+\vartheta\right)\\&\quad\times\left(\sqrt{T_{\mathrm{s}}}I_{\mathrm{A}}\sin\left(\phi+\varpi\right)\sin\psi^{*}+\sqrt{T_{\mathrm{s}}}\xi_{\mathrm{s}}\right)\Big]\\&=\sqrt{T_{\mathrm{s}}}V_{\mathrm{A}}\cos\left(\vartheta-\varpi\right)E\left[\sin\psi^{*}\right].\end{aligned} \tag{11}$$

因此, 当考虑非理想测量基选择的情况时, 海水信道透过率与过噪声的表达式可重新写为

$$\begin{aligned}&T_{\mathrm{s}}^{*}=T_{\mathrm{s}}(E\left[\sin\psi^{*}\right])^{2},\\&\xi_{\mathrm{s}}^{*}=\left[T_{\mathrm{s}}\xi_{\mathrm{s}}+\left(T_{\mathrm{s}}-T_{\mathrm{s}}^{*}\right)V_{\mathrm{A}}\right]/T_{\mathrm{s}}^{*}.\end{aligned} \tag{12}$$

2.2 海水信道的光传播特性

在实际情况下, 不同地区海水所呈现的衰减特性存在差异, 主要原因在于不同地区海水其成分构成不同. 即使在同一地区, 其衰减效应也会随着海水深度和气候等多种因素的变化而变化. 因此, 为了简化分析, 此处假定气候等外部环境不变, 只考虑海水深度和波长在水下 CV-QKD 系统中对海水信道光吸收和光散射效应的影响. 吸收系数 $\gamma\left(\lambda,h\right)$ 作为波长 λ 与海水深度 h 的函数, 其表达式为[47]

$$\begin{aligned}\gamma\left(\lambda,h\right)=&\gamma_{0}\left(\lambda\right)+\gamma_{1}\left(\lambda\right)U_{1}(h)^{0.602}\\&+\gamma_{2}U_{2}\left(h\right)\exp\left(-\alpha_{2}\lambda\right)\\&+\gamma_{3}U_{3}\left(h\right)\exp\left(-\alpha_{3}\lambda\right)\\&+\gamma_{4}\exp\left(-\alpha_{4}\lambda\right),\end{aligned} \tag{13}$$

其中 (13) 式中所涉及的具体参数计算和设定见附录 A. 而散射系数 $\kappa\left(\lambda,h\right)$ 同样作为波长 λ 与海水深度 h 的函数, 其表达式可写为[48]

$$\kappa\left(\lambda,h\right)=\kappa_{\mathrm{w}}\left(\lambda\right)+\kappa_{\mathrm{s}}\left(\lambda\right)U_{\mathrm{s}}\left(h\right)+\kappa_{\mathrm{b}}\left(\lambda\right)U_{\mathrm{b}}\left(h\right), \tag{14}$$

其中 (14) 式中所涉及的具体参数计算和设定见附录 B. 根据 (13) 式与 (14) 式, 总信道衰减系数 $\sigma(\lambda,h)$ 其表达式为

$$\sigma(\lambda,h)=\gamma(\lambda,h)+\kappa(\lambda,h). \tag{15}$$

根据 Ruan 等报道 [42] 可知, 在海水的“光传输窗口”中, 即在 450—550 nm 的波长范围内, 光传输效果最好. 因此, 此处选择波长为 520 nm 的光来研究水下 CV-QKD 的系统性能.

由上述分析可知, 不同深度的海水对光的传播特性存在差异, 变化过程是非线性的. 因此, 为了方便分析, 此处只考虑信号光在具有相同深度的水平面中传播的情况. 不失一般性, 假定光的传播特性在短距离传输的情况下以及在同一水平面内保持不变. 则海水信道透过率 $T_{\rm s}$ 的表达式可写为

$$T_{\rm s}=\mathrm{e}^{-\sigma(\lambda,h)L}, \tag{16}$$

其中 $\sigma(\lambda,h)$ 为信道总衰减系数, L 为水平传输距离.

需要指出的是, 水下 CV-QKD 与自由空间大气 CV-QKD 两者作为全球安全通信网络不可或缺的一部分, 具有一些相似之处, 即两者性能均会受到光吸收和光散射的影响. 但水下 CV-QKD 与自由空间大气 CV-QKD 又有本质区别: 在水下连续变量 QKD 方案中, 光吸收系数和光散射系数与波长和海水深度有关, 并且信号光在水中传播存在一个透过率窗口, 其波长范围在 450—550 nm, 称为蓝绿光, 波长在窗口范围内的光透过率较大 [42]; 而在自由空间大气 CV-QKD 方案中, 信号光在大气信道中传输同样会受到传输介质的吸收和散射作用, 但该种信道对信号光的吸收和散射作用主要由大气分子与气溶胶粒子的存在而产生, 这与海水信道对信号光的吸收和散射作用机理具有本质区别.

3 方案安全性分析

本节在渐近情况 [17] 以及组合安全性情况 [20] 下对基于非理想测量基选择的水下 CV-QKD 方案进行安全性分析.

3.1 方案的渐近安全性

此处考虑方案的渐近安全性, 即在集体攻击下, 水下 CV-QKD 方案在不考虑实际数据量的情况下所进行的安全密钥率分析计算. 因此, 所提出的方案在反向协商下其渐近密钥率的计算式为 [49]

$$K_{\rm asy}=\beta I_{\rm AB}-\chi_{\rm BE}, \tag{17}$$

其中 $I_{\rm AB}$ 表示 Alice 与 Bob 的互信息量, $\chi_{\rm BE}$ 表示 Eve 从 Bob 密钥中所窃取的信息量的 Holevo 界, β 表示反向协商效率. 互信息量 $I_{\rm AB}$ 的表达式为

$$I_{\rm AB}=\frac{1}{2}\log_2\frac{V+\chi_{\rm tot}}{1+\chi_{\rm tot}}. \tag{18}$$

这里 $V=V_{\rm A}+1$, $V_{\rm A}$ 为调制方差. $\chi_{\rm tot}$ 表示归结为信道输入的总噪声, 其表达式为

$$\chi_{\rm tot}=\chi_{\rm line}+\frac{\chi_{\rm hom}}{T_{\rm s}}, \tag{19}$$

式中 $\chi_{\rm hom}=[(1-\eta)+\upsilon_{\rm el}]/\eta$, η 和 $\upsilon_{\rm el}$ 分别表示零差探测器量子效率和电噪声; $\chi_{\rm line}$ 表示归结于信道输入的总信道附加噪声,

$$\chi_{\rm line}=\frac{1}{T_{\rm s}}-1+\xi_{\rm s}, \tag{20}$$

其中参数 $T_{\rm s}$ 与 $\xi_{\rm s}$ 分别表示海水信道的透过率与过噪声.

为了计算参数 $\chi_{\rm BE}$, 此处假设攻击者 Eve 无法对 Bob 系统中的非理想器件进行攻击. 此种噪声评估模型已被广泛应用于 CV-QKD 实验中 [22,23]. 基于该噪声评估模型, $\chi_{\rm BE}$ 的表达式可写为

$$\chi_{\rm BE}=\sum_{i=1}^{2}G\left(\frac{\omega_i-1}{2}\right)-\sum_{i=3}^{5}G\left(\frac{\omega_i-1}{2}\right), \tag{21}$$

式中 $G(x)=(x+1)\log_2(x+1)-x\log_2 x$;

$$\omega_{1,2}^2=\frac{1}{2}\left(\Delta\pm\sqrt{\Delta^2-4D}\right), \tag{22}$$

其中

$$\begin{aligned}&\Delta=V^2-2T_{\rm s}\left(V^2-1\right)+T_{\rm s}^2(V+\chi_{\rm line})^2,\\&D=T_{\rm s}^2(1+V\chi_{\rm line})^2;\end{aligned} \tag{23}$$

$\omega_{3,4}$ 表达式可写为

$$\omega_{3,4}^2=\frac{1}{2}\left(A\pm\sqrt{A^2-4B}\right), \tag{24}$$

其中

$$\begin{aligned}&A=\frac{1}{T_{\rm s}(V+\chi_{\rm tot})}\left[\Delta\chi_{\rm hom}+V\sqrt{D}+T_{\rm s}\left(V+\chi_{\rm line}\right)\right],\\&B=\frac{\sqrt{D}V+D\chi_{\rm hom}}{T_{\rm s}(V+\chi_{\rm tot})};\quad\omega_5=1.\end{aligned} \tag{25}$$

接下来分析基于非理想测量基选择的水下 CV-QKD 方案在渐近情况下的方案性能. 涉及的仿真系统参数分别设定为 $V_{\rm A}=3$, $\eta=0.6$, $\upsilon_{\rm el}=0.05$.

根据 2.1 节的分析, 如果调制相位不正确并且 Alice 与 Bob 都没意识到这一点, 则他们将会获得偏离正确值的参数 $T_{\rm s}^{*}$ 与 $\xi_{\rm s}^{*}$. 根据 (12) 式, 设 $\mu=(E[\sin\psi^{*}])^{2}$, 即由非理想测量基选择所引入的额外过噪声用参数 μ 进行衡量. 则所提出方案的渐近密钥率与传输距离在不同参数 $\mu=0.990$, 0.993, 0.995, 0.997, 1 下的关系如图 4 所示, 其中协商效率 $\beta=0.95$, 海水深度 $h=30\,\text{m}$, 海水信道过噪声 $\xi_{\rm s}=0.01$, $\mu=1$ 表示理想测量基选择. 在所提出的方案中, 不同的参数 μ 对应于 DAC 中运算放大器的不同环路增益. 由图 4 可知, 所提出方案的渐近密钥率随参数 μ 的减小而降低, 并且在海水信道的最大传输距离也随之减小. 比如当参数 $\mu=1$ 时, 所提出方案的最大传输距离为 53.46 m; 而当参数 $\mu=0.993$ 时, 所提出方案的最大传输距离为 41.76 m.

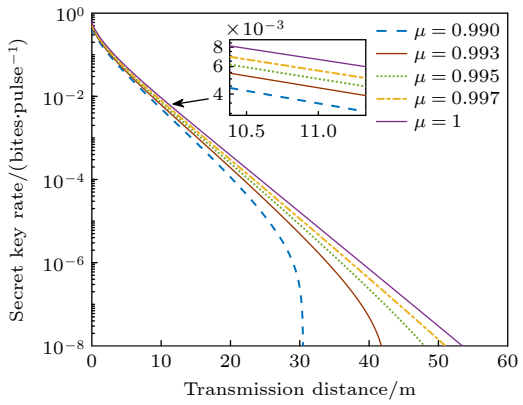

图 4 所提出方案的渐近密钥率与传输距离在不同参数 μ 下的关系

Fig. 4. Relationship between the asymptotic secret key rate of the proposed scheme and the transmission distance under different parameters μ.

图 5 给出了所提出方案的渐近密钥率与协商效率 β 在不同参数 $\mu=0.990$, 0.993, 0.995, 0.997, 1 下的关系, 其中深度 h=30 m, 传输距离 L=10 m, 信道过噪声 $\xi_{\rm s}=0.01$. 由图 5 可知, 对于所提出的方案, 协商效率 β 的可使用范围随着参数 μ 的减小而压缩. 例如当 $\mu=1$ 时, 所提出方案的协商效率 β 的可使用范围为 [0.784, 1], 即在此种情况下当 $\beta<0.784$ 时, 所提出的方案无法获得密钥; 而当 $\mu=0.993$ 时, 所提出方案的协商效率 β 的可使用范围则压缩至 [0.838, 1], 即在此种情况下当 $\beta<0.838$ 时, 所提出的方案无法获得密钥.

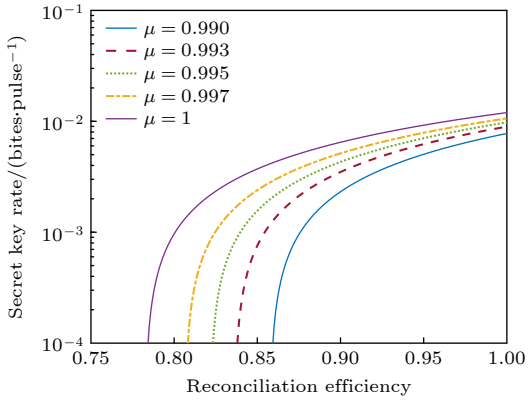

图 5 所提出方案的渐近密钥率与协商效率在不同参数 μ 下的关系

Fig. 5. Relationship between the asymptotic secret key rate of the proposed scheme and the reconciliation efficiency under different parameters μ.

图 6 给出了所提出方案的密钥率与参数 μ 在不同海水深度 $h=10$, 30, 50 m 下的关系, 其中协商效率 $\beta=0.95$, 过噪声 $\xi_{\rm s}=0.01$, 传输距离 $L=10$ m. 在图 6 中, 将渐近密钥率 $K_{\rm asy}=0$ 的水平虚线与不同海水深度 $h=10$, 30, 50 m 所对应的性能曲线相交, 分别得到纵坐标均为 0 的点 P_1, P_2 与 P_3, 三个点对应的坐标分别为 $(0.9738,0)$、$(0.9761,0)$ 与 $(0.978,0)$. 基于此, 可得到海水深度 $h=10$, 30, 50 m 时所对应的参数 μ 的阈值下界限, 即 $\hat{\mu}_{\rm th}=0.9738, 0.9761, 0.978$. 由图 6 可以观察到, 随着海水深度 h 的增加, 参数 μ 的阈值下界限也随之增大. 这表明深度 h 的值越大, 为保证所提出方案的密钥率为正所需要的参数 μ 的最小值也越大. 例如当 $h=10$ m 时, 参数 μ 的阈值下界限为 $\hat{\mu}_{\rm th}=0.9738$; 而

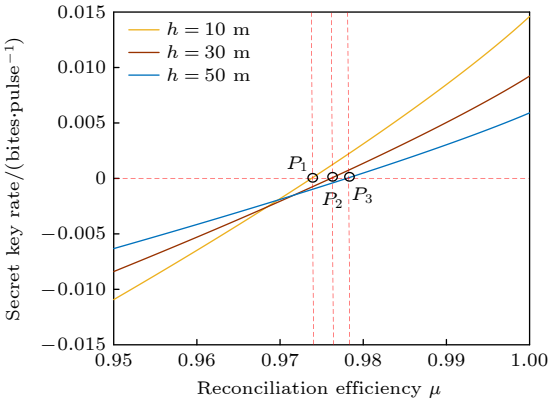

图 6 所提出方案的密钥率与参数 μ 在不同海水深度 h 下的关系

Fig. 6. Relationship between the asymptotic secret key rate of the proposed scheme and the parameter μ under different seawater depths h.

当 h =50 m 时, 参数 μ 的阈值下界限为 $\hat{\mu}_{\rm fh}=0.978$, 显然 $\hat{\mu}_{\rm th}<\hat{\mu}_{\rm fh}$.

图 7 给出了非理想测量基选择情况下所提出的方案与基于 Beer's law(BL) 模型的水下 CV-QKD 方案性能比较, 基于 BL 模型的水下 CV-QKD 方案其密钥率计算详见 Ruan 等[42] 的报道, 其中深度 $h=30$ m(本文所提出的方案), β=0.95, μ=0.993, 信道过噪声 $\xi_{\rm s}=0.01$. 从图 7 可以发现, 基于 BL 模型的纯净海水 (pure sea water) 信道以及清澈海水信道 (clear ocean water) 信道的 CV-QKD 其渐近密钥率和传输距离要优于本文所提出方案的渐近密钥率和传输距离. 这在我们的意料之中, 主要原因在于 Ruan 等[42] 所采用的 BL 海水信道模型基于这样的假设, 即在短距离传输的情况下, 海水信道可视为线性信道. 由于该模型只是简单将海水信道在短距离传输的情况下等同于线性信道, 这意味着在 BL 模型中海水对光的衰减系数是固定的, 并没有考虑包括海水深度、海水中叶绿素浓度、有色溶解有机物以及非藻类颗粒等因素对水下 CV-QKD 方案性能的影响, 因此面对实际情况复杂的海水信道, 该模型并不适用. 而本文所提出的方案其水下信道模型采用叶绿素 a 浓度模型, 在计算海水信道参数时 (吸收和散射系数) 充分考虑了海水深度、海水中叶绿素浓度、有色溶解有机物以及非藻类颗粒等因素 (计算过程详见附录 A 与附录 B), 更符合实际情况. 因此, 在图 7 中, 本文所提出方案其性能曲线相比基于 BL 模型的纯净海水信道以及清澈海水信道的 CV-QKD 方案的性能曲线更符合实际.

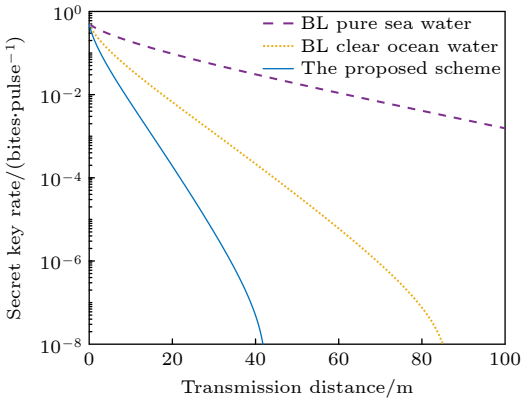

图 7 非理想测量基选择情况下所提出的方案与基于 BL 模型的水下 CV-QKD 方案性能比较

Fig. 7. Performance comparison between the proposed scheme and the underwater CV-QKD scheme based on BL model under imperfect measurement basis choice.

3.2 方案的组合安全性

在上述渐近安全性分析中, 对于所提出方案的渐近密钥率计算的前提是假定 Alice 和 Bob 可以采用无限多的信号进行互换交流. 然而这在实验中是无法实现的, 主要原因是实际安全密钥的长度是有限的. 由于组合安全性是有限长效应[18] 的不确定性安全的增强, 在集体攻击下, 通过详细分析水下 CV-QKD 系统中的每一个步骤, 可以获得一条理论上的最紧安全界限[20]. 因此本节主要研究所提出的方案在组合安全框架下的性能表现.

在考虑组合安全性的情况下, 所提出方案的密钥率其表达式为[20]

$$K_{\rm comp}=(1-\varepsilon_{\rm rob})\left[\beta I_{\rm AB}-F(\Theta_a^{\max},\Theta_b^{\max},\Theta_c^{\min})-\frac{1}{R}\left(\Delta_{\rm AEP}+\Delta_{\rm ent}+2\log_2\frac{1}{2\bar{\varepsilon}}\right)\right], \tag{26}$$

其中 $\varepsilon_{\rm rob}$ 表示协议的鲁棒性. $F(\Theta_a^{\max},\Theta_b^{\max},\Theta_c^{\min})$ 表示计算 Bob 与 Eve 之间 Holevo 界的函数, 其表达式为

$$F(\Theta_a^{\max},\Theta_b^{\max},\Theta_c^{\min})=G\left(\frac{\nu_1-1}{2}\right)+G\left(\frac{\nu_2-1}{2}\right)-G\left(\frac{\nu_3-1}{2}\right), \tag{27}$$

其中 ν_1 与 ν_2 为协方差矩阵 $\begin{bmatrix}\Theta_a^{\max}I_2 & \Theta_c^{\min}\sigma_z\\ \Theta_c^{\min}\sigma_z & \Theta_b^{\max}I_2\end{bmatrix}$ 的辛特征值, $I_2=\mathrm{diag}(1,1)$, $\sigma_z=\mathrm{diag}(1,-1)$, 另一个辛特征值 $\nu_3=\Theta_a^{\max}-(\Theta_c^{\min})^2/(1+\Theta_b^{\max})$. 具体而言, 有

$$\begin{aligned}&\nu_1^2+\nu_2^2=(\Theta_a^{\max})^2+(\Theta_b^{\max})^2-2(\Theta_c^{\min})^2,\\ &\nu_1^2\nu_2^2=\left[\Theta_a^{\max}\Theta_b^{\max}-(\Theta_c^{\min})^2\right]^2.\end{aligned} \tag{28}$$

此外, R 表示用于交换的有效脉冲总数, 参数 $\Delta_{\rm AEP}$ 与 $\Delta_{\rm ent}$ 的表达式分别为

$$\Delta_{\rm AEP}=\sqrt{R}\left[(z_0+1)^2+4(z_0+1)\log_2\left(\frac{2}{\varepsilon_{\rm sm}^2}\right)+2\log_2\left(\frac{2}{\varepsilon_{\rm sm}\varepsilon^2}\right)\right]+\frac{4z_0\varepsilon_{\rm sm}}{\varepsilon}, \tag{29}$$

$$\Delta_{\rm ent}=\log_2\left(\frac{1}{\varepsilon}\right)+\sqrt{2R\log_2^2(R)\log_2\left(\frac{2}{\varepsilon_{\rm sm}}\right)}, \tag{30}$$

其中 z_0 表示离散化参数, 方案的总体安全参数 $\varepsilon=\sqrt{\varepsilon_{\rm ent}+\varepsilon_{\rm PE}+\varepsilon_{\rm cor}}+2\varepsilon_{\rm sm}+\bar{\varepsilon}$. 根据 Leverrier[20]

的研究结果, 这些参数的值可取 $\varepsilon_{\rm sm}=\bar{\varepsilon}=10^{-21}$, $\varepsilon_{\rm ent}=\varepsilon_{\rm PE}=\varepsilon_{\rm cor}=10^{-41}$, $z_0=5$. 需要指出的是当执行参数估计这一步骤的概率至少为 0.99 时, 本方案的鲁棒性参数 $\varepsilon_{\rm rob}\leqslant 10^{-2}$. 基于此, 则与本方案相关的 3 个随机变量 $\|X\|$, $\|Y\|$ 和 $\langle X,Y\rangle$ 的值满足以下 3 个约束条件:

$$\begin{aligned}\|X\|^2 &\leqslant R(V_{\rm A}+1)+3\sqrt{2R(V_{\rm A}+1)},\\ \|Y\|^2 &\leqslant R(T_{\rm s}V_{\rm A}+T_{\rm s}\xi_{\rm s}+1)\\ &\quad +3\sqrt{2R(T_{\rm s}V_{\rm A}+T_{\rm s}\xi_{\rm s}+1)},\\ \langle X,Y\rangle &\geqslant R\sqrt{T_{\rm s}(V^2-1)}\\ &\quad -3\sqrt{(V-1)(\eta T_{\rm s}\chi_{\rm tot}+1)R/2}.\end{aligned}\tag{31}$$

根据 (31) 式, 可以得到

$$\begin{aligned}\Theta_a^{\max}&=\frac{1}{R}\left[1+2\sqrt{\frac{\log(36/\varepsilon_{\rm PE})}{R/2}}\right]\|X\|^2-1,\\ \Theta_b^{\max}&=\frac{1}{R}\left[1+2\sqrt{\frac{\log(36/\varepsilon_{\rm PE})}{R/2}}\right]\|Y\|^2-1,\\ \Theta_c^{\min}&=\frac{1}{R}\langle X,Y\rangle-5\sqrt{\frac{\log(8/\varepsilon_{\rm PE})}{(R/2)^3}}\\ &\quad\times\left(\|X\|^2+\|Y\|^2\right),\end{aligned}\tag{32}$$

其中 $\varepsilon_{\rm PE}$ 表示参数估计失败的最大概率.

接下来分析所提出的基于非理想测量基选择的水下 CV-QKD 方案在考虑组合安全性的情况下方案的性能. 涉及全局的仿真系统参数与渐近情情况下所采用的仿真系统参数相同. 图 8 给出了在组合密钥率与用于交换的有效脉冲总数在不同参数 $\mu=0.985,\ 0.990,\ 0.995,\ 1$ 下的关系, 其中 $\beta=0.95$, 深度 $h=30$ m, 传输距离 $L=15$ m, 信道过噪声 $\xi_{\rm s}=0.01$, 并且水平虚线表示相对应的渐近密钥率. 从图 8 可以观察到, 所提出方案的组合密钥率随着参数 μ 的减小而降低, 这表明所提出的基于非理想测量基选择的水下 CV-QKD 方案的组合密钥率会因 DAC 的有限带宽而降低. 此外, 所提出方案的组合密钥率总是低于其渐近密钥率. 因此, 相比于渐近安全性分析, 采用组合安全性分析可以获得更紧的密钥率曲线.

图 9 给出了非理想测量基选择情况下所提出的方案与基于 BL 模型的水下 CV-QKD 方案组合密钥率比较, 其中深度 $h=30$ m(本文所提出的方案), $\beta=0.95$, $\mu=0.993$, 传输距离 $L=15$ m, 信道过噪声 $\xi_{\rm s}=0.01$. 从图 9 可以发现, 在用于交换的有效脉冲总数 R 相同的情况下, 所提出方案的组合密钥率低于基于 BL 模型的纯净海水信道以及清澈海水信道 CV-QKD 方案的组合密钥率, 其原因已在上述分析中给出, 并且三者的组合密钥率均低于各自的渐近密钥率 (水平虚线). 由于本文所提出的方案其水下信道模型采用叶绿素 a 浓度模型, 在计算海水信道参数时 (吸收和散射系数) 充分考虑了海水深度、海水中叶绿素浓度、有色溶解有机物以及非藻类颗粒等因素. 因此, 在图 9 中, 本文所提出方案其组合密钥率曲线相比基于 BL 模型的纯净海水信道以及清澈海水信道的 CV-QKD 方案的组合密钥率曲线更符合实际.

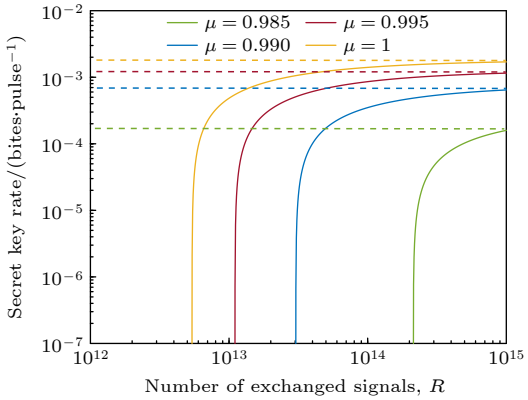

图 8 所提出方案的组合密钥率与用于交换的有效脉冲总数在不同参数 μ 下的关系

Fig. 8. Relationship between the composable secret key rate of the proposed scheme and the number of exchanged signals under different parameters μ.

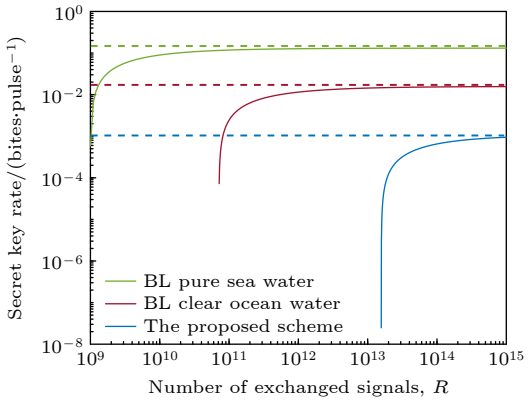

图 9 非理想测量基选择情况下所提出的方案与基于 BL 模型的水下 CV-QKD 方案组合密钥率比较

Fig. 9. Composable secret key rate comparison between the proposed scheme and the underwater CV-QKD scheme based on BL model under imperfect measurement basis choice.

4 结 论

本文提出基于非理想测量基选择的水下 CV-QKD 方案, 考虑水下 CV-QKD 系统的接收端由于 DAC 的有限带宽所引起的非理想测量基选择对系统性能的影响. 经过研究分析, 发现 DAC 的有限带宽使得测量基在选择过程中会产生角度偏差, 从而导致合法通信方对海水信道透过率和过噪声的错误估计. 为了对非理想测量基选择所引入的额外过噪声进行定量分析并获得其安全界限, 本方案引入对应于 DAC 中运算放大器环路增益的参数 μ. 仿真结果表明由非理想测量基选择所引入的额外过噪声能够降低水下 CV-QKD 方案的性能. 此外, 考虑不同海水深度对所提出方案安全界限的影响, 即随着海水深度的增加, 为保证方案安全性所需要的参数 μ 的阈值下界限也随之增大. 因此, 本文所提出的方案可以在不改变水下 CV-QKD 框架结构的前提下, 有效地解决由接收端 DAC 带宽限制导致的非理想测量基选择所带来的安全隐患. 此外, 在对所提出的方案进行安全性分析时, 不仅考虑了其渐近安全性, 也考虑了其组合安全性, 因而能够获得更紧的性能曲线.

附录A 吸收系数公式中涉及的具体参数计算及设定

根据 Gilerson 等[47] 报道, 可通过采用叶绿素模型来表征吸收系数 $\gamma(\lambda,h)$, 即

$$\gamma(\lambda,h)=\gamma_0(\lambda)+\gamma_{\rm acp}(\lambda)+\gamma_{\rm CDOM}(\lambda)+\gamma_{\rm NAP}(\lambda). \tag{A1}$$

这里 $\gamma_0(\lambda)$ 表示纯净海水的吸收系数并且其值可参考 Prieur 和 Sathyendranath [50] 研究结果. $\gamma_{\rm acp}(\lambda)$ 表示浮游植物的吸收系数, 其中叶绿素 a 起主要作用, 其表达式为

$$\gamma_{\rm acp}(\lambda)=\gamma_1(\lambda)U_1(h)^{0.602}, \tag{A2}$$

式中 $\gamma_1(\lambda)$ 表示 400 nm 参考波长下叶绿素浓度的光谱吸收系数并且其值可参考 Prieur 和 Sathyendranath [50] 的研究结果; $U_1(h)$ 表示深度为 h 的叶绿素 a 的浓度,

$$U_1(h)=\tilde{U}_Z\left(U_k-\frac{qh}{D_{\rm e}}+U_{\max}\exp\frac{-(h/D_{\rm e}-\Upsilon_{\max})^2}{\Delta\Upsilon^2}\right), \tag{A3}$$

其中 $\tilde{U}_Z=0.250\ {\rm mg\cdot m^{-3}}$ 表示透光层内的总叶绿素 a 的平均柱集成含量, $U_k=0.570$ 表示表层叶绿素 a 的背景浓度, $q=0.173\ m^{-1}$ 表示垂直梯度, $D_{\rm e}=80.2$ 表示透光层深度, $U_{\max}=0.766$ 表示最大浓度, $\Upsilon_{\max}=U_{\max}/D_{\rm e}$, $\Delta\Upsilon=0.814$ 表示高斯峰的宽度. 上述固定参数的取值都是基于 Uitz 等[51] 报道. $\gamma_{\rm CDOM}(\lambda)$ 表示有色溶解有机物的吸收系数, 主要包括腐殖酸和黄腐酸对光的吸收, 其表达式为

$$\gamma_{\rm CDOM}(\lambda)=\gamma_2U_2(h)\exp(-\alpha_2\lambda)+\gamma_3U_3(h)\exp(-\alpha_3\lambda), \tag{A4}$$

其中参数 $\gamma_2=35.959\ {\rm m^2/mg}$ 与 $\gamma_3=18.828\ {\rm m^2/mg}$ 分别表示黄腐酸和腐殖酸在 400 nm 参考波长下的光谱吸收系数; 参数 $\alpha_2=0.0189\ {\rm nm^{-1}}$ 与 $\alpha_3=0.01105\ {\rm nm^{-1}}$ 分别表示黄腐酸和腐殖酸的吸收斜率系数; $U_2(h)$ 与 $U_3(h)$ 分别表示黄腐酸和腐殖酸的浓度, 其表达式可分别写为

$$\begin{aligned}U_2(h)&=1.74098U_1(h)\exp[0.12327U_1(h)],\\ U_3(h)&=0.19334U_1(h)\exp[0.12343U_1(h)].\end{aligned} \tag{A5}$$

$\gamma_{\rm NAP}(\lambda)$ 表示非藻类颗粒 (nonalgal particulates, NAP) 的吸收系数, 其表达式为

$$\gamma_{\rm NAP}(\lambda)=\gamma_4\exp(-\alpha_4\lambda), \tag{A6}$$

其中 $\gamma_4=9.721\ {\rm m^2/mg}$ 表示 NAP 在 400 nm 参考波长下的光谱吸收系数, $\alpha_4=0.012\ {\rm nm^{-1}}$ 表示 NAP 的吸收斜率系数.

附录B 散射系数公式中涉及的具体参数计算及设定

由于海水对光的散射作用主要是由纯净海水和 NAP 的散射引起的, 因此散射系数 $\kappa(\lambda,h)$ 的表达式可写为[48]

$$\kappa(\lambda,h)=\kappa_{\rm w}(\lambda)+\kappa_{\rm NAP}(\lambda,h). \tag{B1}$$

这里 $\kappa_{\rm w}(\lambda)$ 表示纯净海水的散射系数, 其表达式为

$$\kappa_{\rm w}(\lambda)=0.005826(400/\lambda)^{4.3222}. \tag{B2}$$

$\kappa_{\rm NAP}(\lambda,h)$ 表示 NAP 的散射系数, 包括小颗粒和大颗粒, 其表达式为

$$\kappa_{\rm NAP}(\lambda,h)=\kappa_{\rm s}(\lambda)U_{\rm s}(h)+\kappa_{\rm b}(\lambda)U_{\rm b}(h), \tag{B3}$$

其中 $\kappa_{\rm s}(\lambda)$ 与 $\kappa_{\rm b}(\lambda)$ 分别表示小颗粒与大颗粒的散射光谱; $U_{\rm s}(h)$ 与 $U_{\rm b}(h)$ 分别表示小颗粒与大颗粒在海水深度为 h 时的浓度, 它们的表达式分别为

$$\begin{aligned}\kappa_{\rm s}(\lambda)&=1.1513(400/\lambda)^{1.7},\\ \kappa_{\rm b}(\lambda)&=0.3411(400/\lambda)^{0.3},\\ U_s(h)&=0.01739U_1(h)\exp[0.11631U_1(h)],\\ U_{\rm b}(h)&=0.76284U_1(h)\exp[0.03092U_1(h)].\end{aligned} \tag{B4}$$

参考文献

[1] Zeng Z, Fu S, Zhang H, Dong Y, Cheng J 2017 *IEEE Commun. Surv. Tutorials* **19** 204

[2] Hanson F, Radic S 2008 *Appl. Opt.* **47** 277

[3] Kong M, Wang J, Chen Y, Ali T, Sarwar R, Qiu Y, Wang S, Han J, Xu J 2017 *Opt. Express* **25** 21509

[4] Wang J, Lu C, Li S, Xu Z 2019 *Opt. Express* **27** 12171

[5] Xu F, Ma X, Zhang Q, Lo H K, Pan J W 2020 *Rev. Mod. Phys.* **92** 025002

[6] Pirandola S, Andersen U L, Banchi L, Berta M, Bunandar D, Colbeck R, Englund D, Gehring T, Lupo C, Ottaviani C, Pereira J L, Razavi M, Shaari J S, Tomamichel M, Usenko V C, Vallone G, Villoresi P, Wallden P 2020 *Adv. Opt. Photonics* **12** 1012

[7] Liu Y, Zhang W J, Jiang C, Chen J P, Zhang C, Pan W X, Ma D, Dong H, Xiong J M, Zhang C J, Li H, Wang R C, Wu J, Chen T Y, You L, Wang X B, Zhang Q, Pan J W 2023 *Phys. Rev. Lett.* **130** 210801

[8] Li W, Zhang L, Tan H, Lu Y, Liao S K, Huang J, Li H, Wang Z, Mao H K, Yan B, Li Q, Liu Y, Zhang Q, Peng C Z, You L, Xu F, Pan J W 2023 *Nat. Photonics* **17** 416

[9] Zahidy M, Mikkelsen M T, Müller R, Lio B D, Krehbiel M, Wang Y, Bart N, Wieck A D, Ludwig A, Galili M, Forchhammer S, Lodahl P, Oxenløwe L K, Bacco D, Midolo L 2024 *npj Quantum Inf.* **10** 2

[10] Zhu H T, Huang Y, Liu H, Zeng P, Zou M, Dai Y, Tang S, Li H, You L, Wang Z, Chen Y A, Ma X, Chen T Y, Pan J W 2023 *Phys. Rev. Lett.* **130** 030801

[11] Grosshans F, Grangier P 2002 *Phys. Rev. Lett.* **88** 057902

[12] Laudenbach F, Pacher C, Fung C H F, Poppe A, Peev M, Schrenk B, Hentschel M, Walther P, Hübel H 2018 *Adv. Quantum Technol.* **1** 1800011

[13] Zhang Y, Bian Y, Li Z, Yu S, Guo H 2024 *Appl. Phys. Rev.* **11** 011318

[14] Wu X D, Huang D 2023 *Acta Phys. Sin.* **72** 050303 (in Chinese) [吴晓东, 黄端 2023 物理学报 **72** 050303]

[15] Wu X D, Wang Y J, Zhong H, Liao Q, Guo Y 2019 *Front. Phys.* **14** 41501

[16] Weedbrook C, Pirandola S, García-Patrón R, Cerf N J, Ralph T C, Shapiro J H, Lloyd S 2012 *Rev. Mod. Phys.* **84** 621

[17] Renner R, Cirac J I 2009 *Phys. Rev. Lett.* **102** 110504

[18] Leverrier A, Grosshans F, Grangier P 2010 *Phys. Rev. A* **81** 062343

[19] Leverrier A, García-Patrón R, Renner R, Cerf N J 2013 *Phys. Rev. Lett.* **110** 030502

[20] Leverrier A 2015 *Phys. Rev. Lett.* **114** 070501

[21] Leverrier A 2017 *Phys. Rev. Lett.* **118** 200501

[22] Grosshans F, Assche G V, Wenger J, Brouri R, Cerf N J, Grangier P 2003 *Nature* **421** 238

[23] Jouguet P, Kunz-Jacques S, Leverrier A, Grangier P, Diamanti E 2013 *Nat. Photonics* **7** 378

[24] Huang D, Lin D, Wang C, Liu W, Fang S, Peng J, Huang P, Zeng G 2015 *Opt. Express* **23** 17511

[25] Huang D, Huang P, Lin D , Zeng G 2016 *Sci. Rep.* **6** 19201

[26] Zhang G, Haw J Y, Cai H, Xu F, Assad S M, Fitzsimons J F, Zhou X, Zhang Y, Yu S, Wu J, Ser W, Kwek L C, Liu A Q 2019 *Nat. Photonics* **13** 839

[27] Zhang Y, Chen Z, Pirandola S, Wang X, Zhou C, Chu B, Zhao Y, Xu B, Yu S, Guo H 2020 *Phys. Rev. Lett.* **125** 010502

[28] Williams B P, Qi B, Alshowkan M, Evans P G, Peters N A 2024 *Phys. Rev. Appl.* **21** 014056

[29] Hajomer A A E, Derkach I, Jain N, Chin H M, Andersen U L, Gehring T 2024 *Sci. Adv.* **10** eadi9474

[30] Grice W P, Qi B 2019 *Phys. Rev. A* **100** 022339

[31] Wu X D, Huang D 2024 *Acta Phys. Sin.* **73** 020304 (in Chinese) [吴晓东, 黄端 2024 物理学报 **73** 020304]

[32] Zhao W, Shi R, Wu X, Wang F, Ruan X 2023 *Opt. Express* **31** 17003

[33] Shi P, Zhao S C, Gu Y J, Li W D 2015 *J. Opt. Soc. Am. A:* **32** 349

[34] Zhao S C, Han X H, Xiao Y, Shen Y, Gu Y J, Li W D 2019 *J. Opt. Soc. Am. A:* **36** 883

[35] Ji L, Gao J, Yang A L, Feng Z, Lin X F, Li Z G, Jin X M 2017 *Opt. Express* **25** 19795

[36] Feng Z, Li S, Xu Z 2021 *Opt. Express* **29** 8725

[37] Zhao S, Li W, Shen Y, Yu Y H, Han X H, Zeng H, Cai M, Qian T, Wang S, Wang Z, Xiao Y, Gu Y 2019 *Appl. Opt.* **58** 3902

[38] Hu C Q, Yan Z Q, Gao J, Li Z M, Zhou H, Dou J P, Jin X M 2021 *Phys. Rev. Appl.* **15** 024060

[39] Li D D, Shen Q, Chen W, Li Y, Han X, Yang K X, Xu Y, Lin J, Wang C Z, Yong H L, Liu W Y, Cao Y, Yin J, Liao S K, Ren J G 2019 *Opt. Commun.* **452** 220

[40] Guo Y, Xie C L, Huang P, Li J W, Zhang L, Huang D, Zeng G H 2018 *Phys. Rev. A* **97** 052326

[41] Xie C L, Guo Y, Wang Y J, Huang D, Zhang L 2018 *Chin. Phys. Lett.* **35** 090302

[42] Ruan X, Zhang H, Zhao W, Wang X, Li X, Guo Y 2019 *Appl. Sci.* **9** 4956

[43] Mao Y, Wu X, Huang W, Liao Q, Deng H, Wang Y, Guo Y 2020 *Appl. Sci.* **10** 5744

[44] Xiang Y, Wang Y, Ruan X, Zuo Z, Guo Y 2021 *Phys. Scr.* **96** 065103

[45] Tang X, Chen Z, Zhao Z, Kumar R, Dong Y 2022 *Opt. Express* **30** 32428

[46] Liu W, Peng J, Qi J, Cao Z, He C 2020 *Laser Phys. Lett.* **17** 055203

[47] Gilerson A, Zhou J, Hlaing S, Ioannou I, Schalles J, Gross B, Moshary F, Ahmed S 2007 *Opt. Express* **15** 15702

[48] Gariano J, Djordjevic I B 2019 *Opt. Express* **27** 3055

[49] Fossier S, Diamanti E, Debuisschert T, Tualle-Brouri R, Grangier P 2009 *J. Phys. B: At. Mol. Opt. Phys.* **42** 114014

[50] Prieur L, Sathyendranath S 1981 *Limnol. Oceanogr.* **26** 671

[51] Uitz J, Claustre H, Morel A, Hooker S B 2006 *J. Geophys. Res. Oceans.* **111** C08005

Underwater continuous variable quantum key distribution scheme based on imperfect measurement basis choice*

Wu Xiao-Dong [1)] Huang Duan [2)†]

1) (*School of Management, Fujian University of Technology, Fuzhou* 350118 , *China*)

2) (*School of Electronic Information, Central South University, Changsha* 410083, *China*)

(Received 6 June 2024; revised manuscript received 27 August 2024)

Abstract

Measurement basis choice is an essential step in the underwater continuous variable quantum key distribution system based on homodyne detection. However, in practice, finite bandwidth of analog-to-digital converter on the receiver's side is limited, which can result in defects in the measurement basis choice. That is, the receiver cannot accurately modulate the corresponding phase angle on the phase modulator for measurement basis choice to implement homodyne detection. The imperfect measurement basis choice will introduce extra excess noise, which affects the security of underwater continuous variable quantum key distribution scheme. To solve this problem, we propose an underwater continuous variable quantum key distribution scheme based on imperfect measurement basis choice, and analyze the influence of imperfect measurement basis choice on the performance of underwater continuous variable quantum key distribution system in detail. The research results indicate that the extra excess noise introduced by imperfect measurement basis choice can reduce the secret key rate and maximum transmission distance of the underwater Gaussian modulated quantum key distribution, thus reducing the security of the system. In order to achieve reliable underwater continuous variable quantum key distribution, we quantitatively analyze the extra excess noise introduced by choosing the imperfect measurement basis and obtain its security limit. Besides, we also consider the influence of different seawater depths on the security limit of the proposed scheme, effectively solving the security risks caused by the imperfect measurement basis choice. Furthermore, for the proposed scheme, we consider not only its asymptotic security case but also its composable security case, and the performance curves obtained in the latter are tighter than that achieved in the former. The proposed scheme aims to promote the practical process of underwater continuous variable quantum key distribution system and provide theoretical guidance for accurately evaluating the water channel parameters in underwater communication of global quantum communication networks.

Keywords: imperfect measurement basis choice, continuous variable quantum key distribution, seawater channel, seawater depth

PACS: 03.67.Dd, 03.67.Hk **DOI:** 10.7498/aps.73.20240804

CSTR: 32037.14.aps.73.20240804

* Project supported by the Fujian Provincial Natural Science Foundation of China (Grant No. 2023J01940) and the Scientific Research Initiation Fund of Fujian University of Technology, China (Grant No. GY-Z22042).

† Corresponding author. E-mail: duanhuang@csu.edu.cn

物理学报 Acta Physica Sinica
Chinese Physical Society
Institute of Physics, CAS

基于非理想测量基选择的水下连续变量量子密钥分发方案

吴晓东　黄端

Underwater continuous variable quantum key distribution scheme based on imperfect measurement basis choice

Wu Xiao-Dong　Huang Duan

引用信息 Citation: Acta Physica Sinica, 73, 210302 (2024)　DOI: 10.7498/aps.73.20240804
在线阅读 View online: https://doi.org/10.7498/aps.73.20240804
当期内容 View table of contents: http://wulixb.iphy.ac.cn
