

Commun. Theor. Phys. **74** (2022) 035104 (8pp) https://doi.org/10.1088/1572-9494/ac5320

Photon subtraction-based continuous-variable measurement-device-independent quantum key distribution with discrete modulation over a fiber-to-water channel

Chao Yu[1], Yin Li[2], Jianzhi Ding[1], Yun Mao[2,*] and Ying Guo[2,3,*]

[1] School of Computer Science and Engineering, Central South University, Changsha 410083, China
[2] School of Automation, Central South University, Changsha 410075, China
[3] School of Computer Science, Beijing University of Posts and Telecommunications, Beijing 100876, China

E-mail: maoyun3106@csu.edu.cn and yingguo@csu.edu.cn

Received 27 October 2021, revised 22 January 2022
Accepted for publication 9 February 2022
Published 17 March 2022

Abstract

We propose a discrete-modulated continuous-variable measurement-device-independent quantum key distribution protocol over a fiber-to-water channel. Different from optical fibers, the underwater channel has more severe optical attenuation because of optical absorption and scattering, which reduces the maximum communication distance. To enhance the performance of the protocol, the photon subtraction operation is implemented at the modulator side. We carry out a performance simulation in two different kinds of seawater channel, and the result shows that the scheme with photon subtraction has a longer secure communication distance under certain conditions.

Keywords: measurement-device-independent, discrete modulation, fiber-to-water channel, continuous variable, quantum key distribution

(Some figures may appear in colour only in the online journal)

1. Introduction

Quantum key distribution (QKD) [1, 2] is one of the most important applications and rapidly developing technologies of quantum encryption. Whilst it is distinct from classic communication, the safety of QKD is built on the physical properties of photons and it can achieve unconditional security [3–5]. Generally, there are two types of QKD, discrete-variable QKD (DVQKD) and continuous-variable QKD (CVQKD) [6, 7]. Thanks to its simplicity in experiments and higher performance over short distances, CVQKD has become a research hotspot in recent years. In the Gaussian-modulated CVQKD (GM-CVQKD), the information follows Gaussian distribution so that it is more susceptible to noise than binary data, which limits the maximum communication distance [8, 9]. To solve this problem, discrete-modulated CVQKD (DM-CVQKD) was proposed [10]. In the DM-CVQKD, secret key data is binary, and it is modulated on two orthogonal components of the optical field [11], which shows better robustness to noise and better performance at long distances compared with GM-CVQKD.

In the one-way CVQKD scheme, there is an assumption that the hardware of QKD such as the detector is ideal, and most studies rely on this assumption. However, such a perfect device is difficult to achieve in reality, and this has led to numerous attacks on vulnerabilities caused by device imperfections, which include LO fluctuation attacks, wavelength attacks, detector saturation attack [12–14], etc. To solve the security loopholes caused by the imperfection of the measurement device, the continuous variable measurement-device-independent (MDI) quantum key distribution (CV-MDI-QKD) has been proposed [15–18]. In the CV-MDI-QKD protocol, there are three parties involved in the key distribution including the legitimate communication parties Alice,

* Authors to whom any correspondence should be addressed.

Bob and an additional untrusted third party, Charlie. Unlike traditional one-way QKD with only one sender, there are two signal senders, Alice and Bob in CV-MDI-QKD. In this protocol, Alice and Bob both send signals to Charlie, and Charlie performs Bell-State Measurement on the quantum signals that passed through the quantum channels [19]. Bob manipulates his quantum state according to the measurement result of Charlie, and then Alice and Bob receive a string of correlated data.

However, what is unfortunate is that the CV-MDI-QKD protocol has a shorter secure transmission distance compared with the traditional one-way CVQKD protocol [20]. Photon subtraction (PS) is one of the non Gaussian operations that have been proven to enhance the entanglement degree of quantum state and thereby improve the security distance [20–23]. This operation can be implemented with prior art and it has been applied in the experiment [24]. In order to extend the maximum communication distance, we apply the PS operation after signal modulation at Alice's side.

In the existing research, optical fiber is the primary channel of a CVQKD scheme. Nevertheless, underwater CVQKD has been widely concerned in recent years for its extensive application prospect, especially in the military field [25]. However, due to the attenuation and absorption of light, the maximum safe distance of quantum signal transmission in seawater is much shorter than that in optical fiber. Fortunately, underwater CVQKD still has important application scenarios. We consider that in some cases, a CV-MDI-QKD scheme may work in different channels. Optical fibers have much less impact on quantum signals than atmospheres. However, for one-way CVQKD, it is difficult to inject the quantum signal in the optical fiber directly into water, so we chose to use the MDI scheme to make Charlie a mediator to connect fiber and water channels. In this paper, we analyze the different channel medium of Alice and Bob to Charlie in a CV-MDI-QKD scheme. We also assessed the factors of seawater that affect the maximum distance and applied the PS operation to enhance the performance of the underwater CVQKD scheme.

This paper is structured as follows: In section 2, we discuss the CV-MDI-QKD scheme with PS. In section 3, we analyze the influence factors of seawater channel. In section 4, we show the performance of the proposed scheme with simulation. Finally, we draw the conclusion in section 5.

2. DM CV-MDI-QKD with photon subtraction

In this section, we first introduce the discrete modulation CV-MID-QKD protocol, including the prepare-and-measurement (PM) scheme and the entanglement-based (EB) scheme which is equivalent to the PM version in security. Afterwards we interpret the PS operation and its application in the discrete modulation CV-MDI-QKD.

2.1. Discrete modulation CV-MDI-QKD

The PM scheme of the discrete modulation CV-MDI-QKD is illustrated in figure 1. In the PM scheme, Alice and Bob prepare two coherent states A and B independently and send them to an untrusted third party named Charlie. Then Charlie measures the two states and the results are C and D. Afterwards, Charlie makes public the results and Bob manipulates his coherent state according to the published results to make it associated with Alice. Finally, Alice and Bob perform the post-processing steps to get the security key. The EB of our scheme is shown in figure 2. Here, we suppose that the channel between Alice and Charlie is called C_{AC}, and is called C_{BC} between Bob and Charlie. The length of channel C_{AC} and C_{BC} is represented by L_{AC} and L_{BC} respectively, and the transmittance of C_{AC} and C_{BC} is T_A and T_B respectively. To simplify the proof of security, we concentrate on the EB scheme and describe its process in detail.

(i) Alice and Bob prepare the two-mode squeezed state $|\psi_4^a\rangle_{A_1A_2}$ and $|\psi_4^b\rangle_{B_1B_2}$ in four-state modulation (or $|\psi_8^a\rangle_{A_1A_2}$ and $|\psi_8^b\rangle_{B_1B_2}$ in eight-state modulation) respectively.
(ii) The mode A_2 passes through the PS module, and then we obtain the mode A_2'. Alice and Bob send modes A_2' and B_2 to the untrusted third party Charlie through two quantum channels respectively.
(iii) The modes A_2' and B_2 interfere with the beamsplitter (BS), and the modes output from the BS are C and D. Charlie then measures the x quadrature of mode C and the p quadrature of D, which are marked as $\{X_C, P_D\}$ by homodyne detection.
(iv) Charlie announces the measurement result $\{X_C, P_D\}$ through the classic channel.
(v) Bob modifies the mode B_1 on the basis of $\{X_C, P_D\}$ by a displacement operation $D(\beta)$, specifically,

$$\rho_{B_1'} = D(\beta)\rho_{B_1}D^{\dagger}(\beta), \tag{1}$$

where ρ_{B_1} represents the density matrix of mode B_1 and $\beta = g(X_C + \mathrm{i}P_D)$ where g is the gain of the displacement operation [26]. After the displacement operation, mode A_1 and B_1' are entangled, and the secret key data of Alice and Bob are interrelated.
(vi) Alice and Bob perform the post-processing steps to share the secret key, which include data reconciliation, parameter estimation and privacy amplification.

After the above steps, Alice and Bob complete a key distribution process. However, due to the characteristics of the MDI protocol, the security transmission distance of key distribution is generally shorter than that of a one-way CVQKD protocol [27, 28]. So in the following section, we use PS to increase the security transmission distance.

2.2. PS-based discrete modulation CV-MDI-QKD

As shown in figure 2, the PS operation is modeled by a beamsplitter (BS) with transmittance μ and a photon number resolving detector(PNRD). The mode A_2 of the two mode squeezed state prepared by Alice intersects with vacuum state C_0 at the BS, and then they are split into two modes A_2' and C_1, where C_1 contains m subtracted photons. The PNRD could be applied to measure mode C_1 by using the positive operator-valued measurement(POVM) $\{\mathrm{I}\hat{\mathrm{I}}_0, \hat{\mathrm{I}}_1\}$ [29]. The

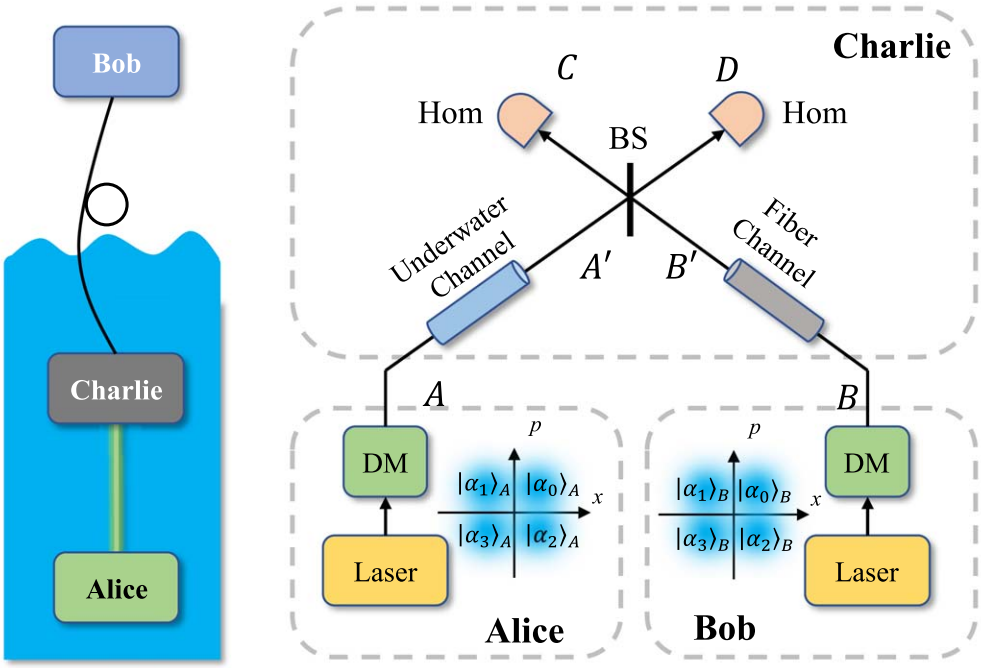

Figure 1. The PM scheme of discrete modulation CV-MDI-QKD. DM is the discrete modulation; Hom is the homodyne detection; BS is beamsplitter.

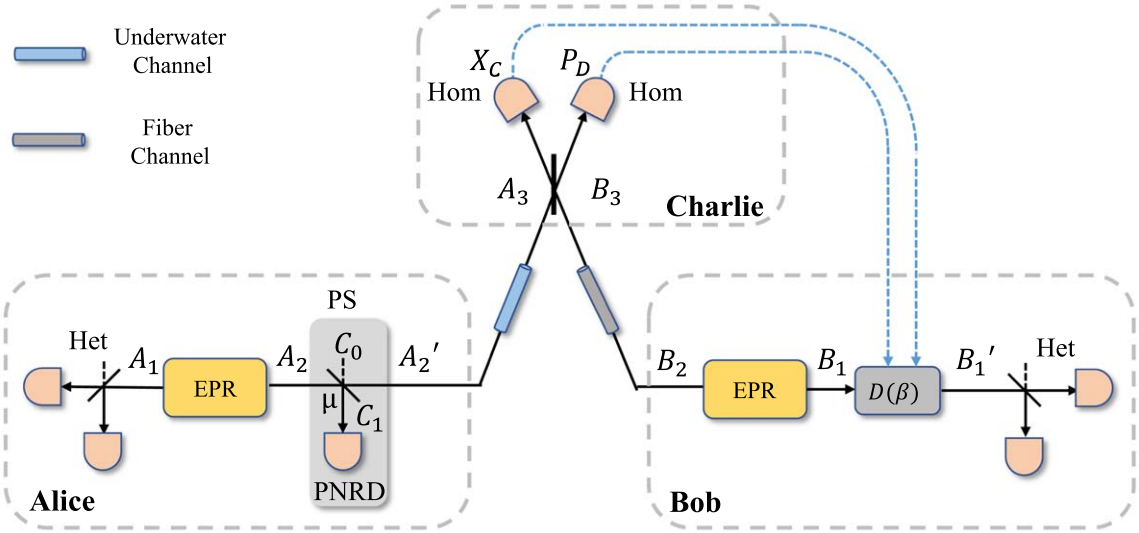

Figure 2. The EB scheme of PS-based discrete modulation CV-MDI-QKD. PNRD is the photon number resolving detector; $D(\beta)$ is the displacement operation; Het is the heterodyne detection; Hom is the homodyne detection.

subtracted photon number m depends on $\hat{\Pi}_1 = |m\rangle\langle m|$. Only when the POVM element $\hat{\Pi}_1$ clicks the PS operation succeeds, which means that Alice could keep state A_1 [30]. The PS operation can be expressed as

$$\rho_{A_1C_1A_2'} = U_{\mathrm{BS}}[|\psi\rangle_{A_1A_2}\langle\psi|_{A_1A_2} \otimes |0\rangle\langle 0|]U_{\mathrm{BS}}^{\dagger}. \tag{2}$$

After the PS, we obtain the triparite state $\rho_{A_1A_2'}^{\hat{\Pi}_1}$ that can be written as

$$\rho_{A_1A_2'}^{\hat{\Pi}_1} = \frac{\mathrm{tr}_{C_1}(\hat{\Pi}_1\rho_{A_1C_1A_2'})}{P_{(m)}^{\hat{\Pi}_1}}, \tag{3}$$

where the $\mathrm{tr}_X(Y)$ is the partial trace of multi-mode state and $P_{(m)}^{\hat{\Pi}_1}$ is the success rate of subtracting m photons which can be calculated by

$$\begin{aligned} P_{(m)}^{\hat{\Pi}_1} &= \mathrm{tr}_{A_1C_1A_2'}(\hat{\Pi}_1\rho_{A_1C_1A_2'}) \\ &= (1-\xi^2)\textstyle\sum_{n=m}^{\infty} C_n^m \xi^{2n}(1-\mu)^m\mu^{n-m} \\ &= (1-\xi^2)\left(\frac{1-\mu}{\mu}\right)^m \textstyle\sum_{n=m}^{\infty} C_n^m(\xi^2\mu)^n \\ &= (1-\xi^2)\xi^{2m}\frac{(1-\mu)^m}{(1-\xi^2\mu)^{m+1}}, \end{aligned} \tag{4}$$

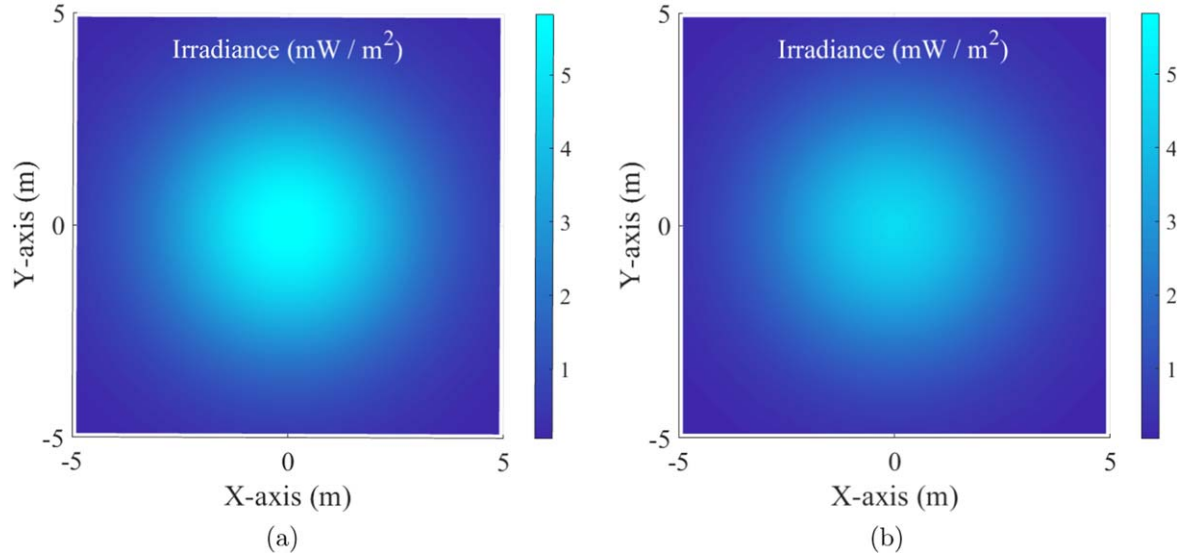

Figure 3. The light intensity distribution after transmitting in (a) pure sea water and (b) clean ocean water. The transmission distance is 2 meters and the power of source is 10 mW.

where C_n^m is the combination number ($n \geqslant m$) and $\xi = \frac{V_A - 1}{V_A + 1}$. The covariance matrix of photon-subtracted state $\rho^{\mathrm{ps}}_{A_1 A_2'}$ can be expressed as

$$\Gamma^{\mathrm{ps}}_{A_1 A_2'} = \begin{pmatrix} X\mathbb{I} & Z_d \sigma_z \\ Z_d \sigma_z & Y\mathbb{I} \end{pmatrix}, \tag{5}$$

where

$$X = \frac{\mu\zeta^2 + 2m + 1}{1 - \mu\zeta^2}, \tag{6}$$

$$Y = \frac{\mu\zeta^2(2m + 1) + 1}{1 - \mu\zeta^2}, \tag{7}$$

$$Z_d = \frac{\sqrt{\mu}\,\zeta(m + 1)}{1 - \mu\zeta^2}, \tag{8}$$

and the detailed calculation is shown in [31]. The asymptotical secret key rate of PS-based scheme against collective attacks is expressed as

$$K_{\mathrm{asym}} = P^{\hat{\Pi}_1}_{(m)}[\kappa I(A\colon B) - S(E\colon B)], \tag{9}$$

where κ is the reconciliation efficiency; $I(A\colon B)$ is the Shannon mutual information between Alice and Bob and $S(E\colon B)$ is the Holevo bound between Eve and Bob. We assume the excess noise of C_{AC} and C_{BC} is ε_A and ε_B and the normalized parameter $T = \frac{T_A g^2}{2}$ [32]. The total channel-added noise can be expressed as $\chi_{\mathrm{line}} = \frac{1 - T}{T} + \varepsilon^{\mathrm{th}}$. The variable $\varepsilon^{\mathrm{th}}$ is the equivalent excess noise of equivalent one-way protocol, which is given by

$$\varepsilon^{\mathrm{th}} = 1 + \chi_A + \frac{T_A}{T_B}(\chi_B - 1) + \frac{T_B}{T_A}\left(\sqrt{\frac{2}{T_B g^2}}\sqrt{V_M - 1} - \sqrt{V_M + 1}\right)^2, \tag{10}$$

where $\chi_A = 1/T_A - 1 + \varepsilon_A$ and $\chi_B = 1/T_B - 1 + \varepsilon_B$. To minimize the excess noise $\varepsilon^{\mathrm{th}}$, we set the value of g to

$$g = \sqrt{\frac{2(V_M - 1)}{T_B(V_M + 1)}}, \tag{11}$$

and then $\varepsilon^{\mathrm{th}}$ can be expressed as

$$\varepsilon^{\mathrm{th}} = \frac{T_B}{T_A}(\varepsilon_B - 2) + \varepsilon_A + \frac{2}{T_A}. \tag{12}$$

Details for the calculation of the secret key rate can be found in appendix A. After the PS operation, mode A_2' instead of A_2 will be sent to Charlie through the quantum channel, and the follow-up progress is the same as the original discrete modulation CV-MDI-QKD.

3. Underwater channel

In the most studies on QKD, researchers analyze the CV-QKD system in the fiber quantum channel. To explore the performance of our protocol, we first need to analyze the underwater channel.

Now we examine the influence of the seawater channel on the transmitted signal pulses. Due to the presence of water molecules, dissolved and suspended impurities (such as dissolved organic matter and chlorophyll molecules) in seawater [33], the transmission of light in the seawater channels is very difficult, resulting in the transmission distance being several orders of magnitude lower than the former. At the same time, the characteristics of seawater channels are also influenced by temperature and salinity. In figure 3, we show the light intensity distribution after transmitting in seawater [34–36], where the transmission distance is 2 meters and the power of the source is 10 mW. We have determined that after passing through the seawater channel, the light intensity is weakened and relatively serious scattering occurs. Since the transmission distance is short, we suppose that the channel is in the identical composition of seawater and hence it becomes a linear channel [25, 37–39]. Therefore, the transmittance of

Table 1. Attenuation coefficient of seawater at 520 nm wavelength.

Water Types	$a(\mathrm{m}^{-1})$	$b(\mathrm{m}^{-1})$	$c(\mathrm{m}^{-1})$
Pure sea water	0.0405	0.0025	0.043
Clean ocean water	0.114	0.037	0.151

seawater channel can be expressed as

$$T_{\mathrm{sea}} = \mathrm{e}^{-c(\lambda)\mathbb{D}}, \tag{13}$$

where $\mathbb{D}$ is the depth, λ is the wavelength of light and c is the total attenuation coefficient. There are two main factors that affect the light transmission in seawater: absorption and scattering. Absorption refers to the energy loss of light caused by the interaction between photons and particles in seawater, which leads to the reduction of light intensity. Scattering means the change of movement direction of photons when they interact with other particles. Consequently, the total attenuation coefficient can be written as [38]:

$$c(\lambda) = a(\lambda) + b(\lambda), \tag{14}$$

where $a(\lambda)$ denotes the absorption coefficient and $b(\lambda)$ denotes the scattering coefficient. The influence of temperature, salinity and chlorophyll concentration on the attenuation coefficient is shown in appendix A.

However, in practical terms, the model becomes more complex and even difficult to estimate, considering the effect of solutes, suspended solids, background light and others on the attenuation coefficient. Fortunately, some researchers have come up with valid parameters through underwater experiments, and we can use these data directly, which also makes our results more practical. Because the attenuation of light at different wavelengths is various, we choose the least attenuated blue-green light (520 nm) for communication purposes. The attenuation coefficient and corresponding sea water types are shown in table 1 [40].

4. Performance analysis

In this section, we discuss the performance of the proposed scheme in the asymptotic cases. Generally, four-state and eight-state modulation protocols are most often used in discrete modulation CVQKD. To simplify the analysis, for the PS operation we only consider its implementation in the four-state modulation scheme in the following.

The modulation variance V_M has a significant impact on performance. In figure 4, we show the relation between V_M and the secret key rate. The solid lines represent the eight-state protocol and the dash lines represent the four-state protocol. The black, red and blue lines represent $L_{\mathrm{AC}} = 0$ m, $L_{\mathrm{AC}} = 10$ m and $L_{\mathrm{AC}} = 20$ m in figure 4(a) and $L_{\mathrm{AC}} = 0$ m, $L_{\mathrm{AC}} = 5$ m and $L_{\mathrm{AC}} = 10$ m in figure 4(b) respectively. In order to make the security analysis method in Gauss-modulated CVQKD still applicable, the variance needs to be set in a small range ($V_m \leqslant 0.5$) [10]. At the same time, to facilitate the comparison with the original discrete modulation CV-MDI-QKD scheme, we set the constant variance with it in the following simulation.

The asymptotic secret key rate as a function of L_{AC} in different seawater channel is illustrated in figure 5. Compared with the original discrete modulation CV-MDI-QKD scheme, the one-photon subtracted (1-PS) scheme has higher secret key rate in the long distance when $L_{\mathrm{BC}} = 0$ m, 10 m and 20 m, although its performance is lower when the communication distance is short due to the low success rate of PS. Besides, the success rate of PS operation decreases with the rise of subtracted photon number m [21], resulting in that the secret key rate of m-PS ($m > 1$) scheme always lower than one-photon subtraction scheme. Therefore, we only discuss the one-photon subtraction scheme in the following.

According to [41], the impact of underwater turbulence on CVQKD system can be reflected in the transmittance. When the communication distance is long, in other words, when T is low, the PS-based scheme has a higher performance than the original scheme. That is, even in the presence of underwater turbulence, our PS-based CV-MDI-QKD scheme is still helpful for performance. However, we find from figure 6 that although the PS-based scheme has a longer secure transmission distance when the L_{BC} was short, the performance of PS-based scheme would be lower than the original four-state scheme when L_{BC} is greater than a certain value. The reason for this phenomenon may be that the total channel noise increases with the increase of L_{BC}, and the variance of the quantum state may decrease after PS.

5. Conclusion

We have suggested a method to enhance the performance of a fiber-to-water discrete modulation CV-MDI-QKD scheme by utilizing a PS operation and simulating it in two different fiber-to-water channels, and the PS operation was described in detail. We assessed the factors that affect the underwater light transmission and used the optimal parameters in the simulation. The influence of modulation variance is also considered, and for comparison we chose the same variance, which is $V_M = 0.5$, in the original and proposed protocol. The simulation results show that the proposed scheme has a longer transmission distance when L_{BC} is short, but lower performance than the original protocol in the long L_{BC} case. The transmission distance of the underwater channel is several orders of magnitude shorter than that of the optical fiber channel. However, it is still of great value in the construction of underwater communication networks.

Appendix A. Calculation of asymptotic secret key rate

In this section, we discuss the properties of the quantum states transmitted in the PS-based discrete modulation CV-MDI-QKD scheme and the calculation method of the secret key rate in the asymptotic scenario. We suppose that Alice employs heterodyne detection while Bob employs heterodyne

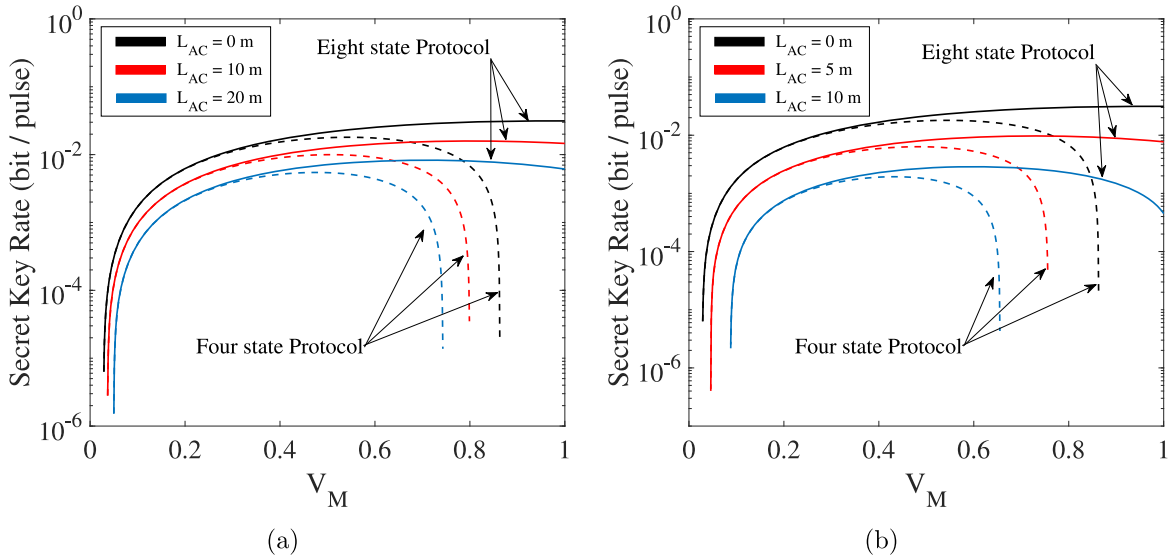

Figure 4. The secret key rate as a function of modulation variance V_M in (a) pure sea water and (b) clean ocean water. The solid lines represent the eight-state protocol and the dash lines represent the four-state protocol. The parameters are as follows: $\varepsilon_A = \varepsilon_B = 0.001$ and $L_{\mathrm{BC}} = 0$ m.

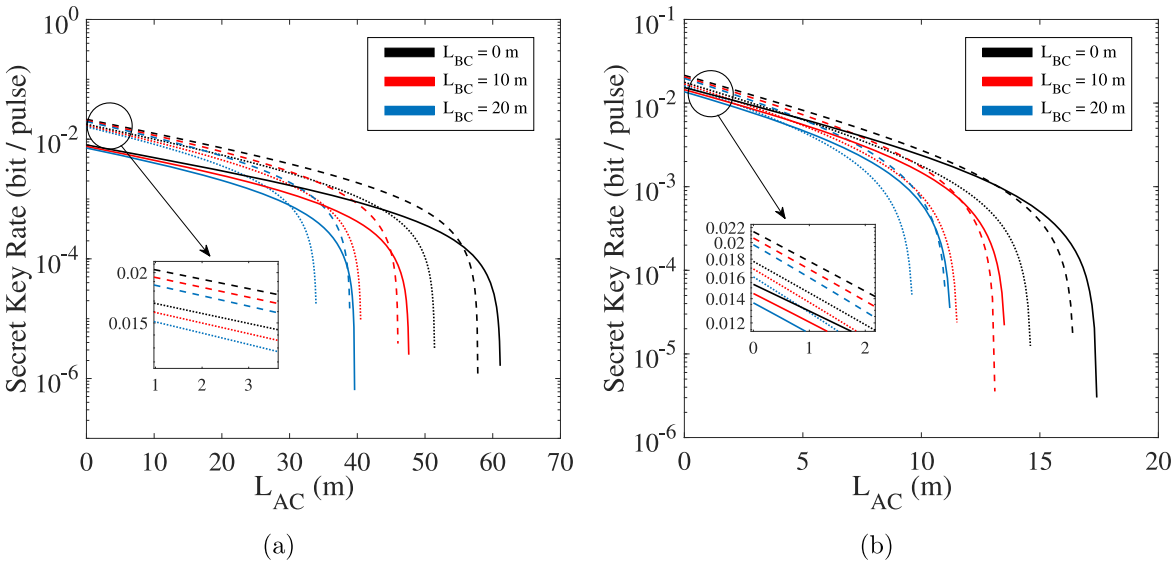

Figure 5. The secret key rate as a function of L_{AC} in (a) pure sea water and (b) clean ocean water. The solid lines represent the PS-based four-state CV-MDI-QKD protocol, the dash lines represent eight-state CV-MDI-QKD protocol and the dot lines represent the original four-state protocol. The color of lines black, red and blue represents $L_{\mathrm{BC}} = 0$ m, $L_{\mathrm{BC}} = 10$ m and $L_{\mathrm{BC}} = 20$ m respectively.

detection, and the postprocessing uses reverse reconciliation. The EPR state $|\psi\rangle$ prepared by Alice and Bob in the traditional DM-CVQKD can be written as

$$\begin{aligned}|\psi\rangle &= \textstyle\sum_{k=0}^{d-1}\sqrt{\lambda_k}|\phi_k\rangle|\phi_k\rangle \\ &= \frac{1}{2}\textstyle\sum_{k=0}^{d-1}|\psi_k\rangle|\alpha_k^d\rangle,\end{aligned} \tag{A.1}$$

where $d = 4$ for four-state protocol and $d = 8$ for eight-state protocol. Here,

$$|\psi_k\rangle = \frac{1}{2}\sum_{r=0}^{d-1} \mathrm{e}^{\mathrm{i}(1+\frac{d}{2}k)r\pi/8}|\phi_r\rangle, \tag{A.2}$$

and

$$|\phi_r\rangle = \frac{\mathrm{e}^{-\alpha^2/2}}{\lambda_r}\sum_{n=0}^{\infty}(-1)^n\frac{\alpha^{dn+r}}{\sqrt{(dn+r)!}}|dn+r\rangle, \tag{A.3}$$

where $r = 0, 1, \ldots, d-1$. For four-state protocol, λ_r is given as

$$\lambda_{0,2} = \frac{1}{2}\mathrm{e}^{-\alpha^2}[\cosh(\alpha^2) \pm \cos(\alpha^2)], \tag{A.4}$$

$$\lambda_{1,3} = \frac{1}{2}\mathrm{e}^{-\alpha^2}[\sinh(\alpha^2) \pm \sin(\alpha^2)], \tag{A.5}$$

and for eight-state protocol, λ_r is given as

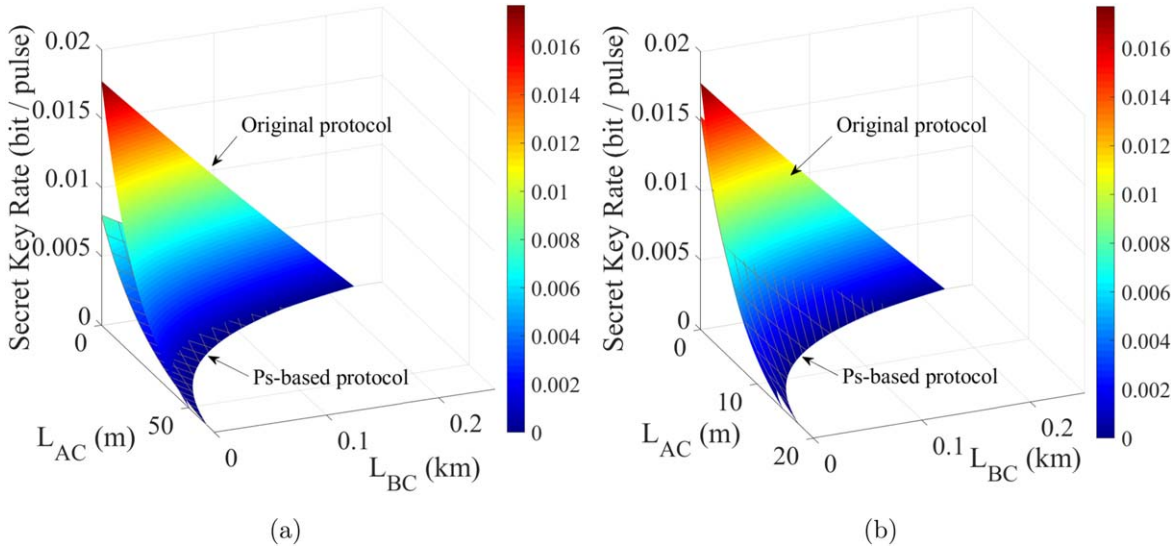

Figure 6. The secret key rate as a function of L_{AC} and L_{BC} in (a) pure sea water and (b) clean ocean water. The respectively. The smooth surfaces and the grid surfaces represent the original four-state CV-MDI-QKD and the corresponding PS-based scheme respectively.

$$\lambda_{0,4}=\frac{1}{4}\mathrm{e}^{-\alpha^2}[\cosh(\alpha^2)+\cos(\alpha^2)\pm 2\cos\left(\frac{\alpha^2}{\sqrt{2}}\right)\cosh\left(\frac{\alpha^2}{\sqrt{2}}\right)\Big], \tag{A.6}$$

$$\lambda_{1,5}=\frac{1}{4}\mathrm{e}^{-\alpha^2}[\sinh(\alpha^2)+\sin(\alpha^2)\pm\sqrt{2}\cos\left(\frac{\alpha^2}{\sqrt{2}}\right)\sinh\left(\frac{\alpha^2}{\sqrt{2}}\right)\pm\sqrt{2}\sin\left(\frac{\alpha^2}{\sqrt{2}}\right)\cosh\left(\frac{\alpha^2}{\sqrt{2}}\right)\Big], \tag{A.7}$$

$$\lambda_{2,6}=\frac{1}{4}\mathrm{e}^{-\alpha^2}[\sinh(\alpha^2)-\sin(\alpha^2)\pm 2\sin\left(\frac{\alpha^2}{\sqrt{2}}\right)\sinh\left(\frac{\alpha^2}{\sqrt{2}}\right)\Big], \tag{A.8}$$

$$\lambda_{3,7}=\frac{1}{4}\mathrm{e}^{-\alpha^2}[\sinh(\alpha^2)-\sin(\alpha^2)\mp\sqrt{2}\cos\left(\frac{\alpha^2}{\sqrt{2}}\right)\sinh\left(\frac{\alpha^2}{\sqrt{2}}\right)\pm\sqrt{2}\sin\left(\frac{\alpha^2}{\sqrt{2}}\right)\cosh\left(\frac{\alpha^2}{\sqrt{2}}\right)\Big]. \tag{A.9}$$

After the transmission of quantum channel and the detection of Charlie, the co-variance matrix of state $\rho^{\mathrm{ps}}_{A_1B_{1'}}$ can be represented as

$$\Gamma^{\mathrm{ps}}_{A_1B_{1'}}=\begin{pmatrix} a\mathbb{I} & c\sigma_z \\ c\sigma_z & b\mathbb{I}\end{pmatrix}=\begin{pmatrix} X\mathbb{I} & \sqrt{T}Z_d\sigma_z \\ \sqrt{T}Z_d\sigma_z & T(Y+\chi_{\mathrm{line}})\mathbb{I}\end{pmatrix}, \tag{A.10}$$

where X, Y and Z_d are given in equation (6)–(8). The Shannon mutual information between Bob and Alice is calculated by

$$I(A\colon B)=\log_2\frac{a+1}{a+1-c^2/(b+1)}, \tag{A.11}$$

and the Holevo bound $S(E\colon B)$ is

$$\begin{aligned} S(E\colon B)&=S(E)-S(E|B)\\ &=S(AB)-S(A|B)\\ &=G[(\gamma_1-1)/2]+G[(\gamma_2-1)/2]\\ &\quad -G[(\gamma_3-1)/2], \end{aligned} \tag{A.12}$$

where $G(x)=(x+1)\log_2(x+1)-x\log_2 x$, which denotes the Von Neumann entropy. Here, $\gamma_{1,2,3}$ are the symplectic eigenvalues derived from covariance matrix and they are calculated by

$$\gamma_{1,2}=\frac{1}{2}(A\pm\sqrt{A^2-4B^2}), \tag{A.13}$$

$$\gamma_3=\sqrt{a^2-\frac{ac^2}{b}}, \tag{A.14}$$

where $A=a^2+b^2-2c^2$ and $B=ab-c^2$. Then, we can calculate the secret key rate by equation (9).

Appendix B. Description of partial influencing factors of seawater channel

In this section we describe the effects of temperature, salinity and chlorophyll concentration on the marine channel. Assuming that the current channel is pure seawater, considering the influence of temperature and salinity, the absorption coefficient can be calculated as [42]:

$$a(\lambda,\Theta,S)=a(\lambda,\Theta_r,0)+\Psi_\Theta(\Theta-\Theta_r)+\Psi_S S, \tag{B.1}$$

where Θ is the temperature, Θ_r is a reference temperature, S is salinity and Ψ_Θ, Ψ_S is the linear temperature slope and salinity slope respectively (See [42] for detailed calculation). According to [43], the scattering coefficient can be further

expressed as

$$b(\lambda, \Theta, S) = b_d(\lambda, \Theta, S) + b_c(\lambda, \Theta, S). \tag{B.2}$$

Here, $b_d(\lambda, \Theta, S)$ and $b_c(\lambda, \Theta, S)$ can be calculated by

$$b_d(\lambda, \Theta, S) = \frac{8\pi^3}{\lambda^4}\left(\rho\frac{\partial n^2}{\partial \rho}\right)^2_{\Theta} k\Theta\beta_{\Theta}h(\delta), \tag{B.3}$$

$$b_c(\lambda, \Theta, S) = \frac{8\pi^3}{\lambda^4 N_A}\left(\frac{\partial n^2}{\partial S}\right)^2 \times\frac{M_w}{\rho}\frac{S}{-\partial \ln a_w/\partial S}h(\delta), \tag{B.4}$$

where k is the Boltzmann constant, N_A is the Avogadro number, ρ is the density, n is the refractive index in vacuum, β_{Θ} is the isothermal compressibility, δ is the depolarization ratio of the solution, and a_w and M_w are the activity and molecular weight of water in the solution respectively, which are detailed in [43].

The effect of chlorophyll on attenuation coefficient can be expressed as [37]:

$$a(\lambda) = [a_w(\lambda) + 0.06a_c(\lambda)C^{0.65}] \times[1 + 0.2e^{-0.014(\lambda-440)}], \tag{B.5}$$

$$b(\lambda) = 0.3\frac{550}{\lambda}C^{0.62}, \tag{B.6}$$

where $a_w(\lambda)$ is the absorption coefficient of pure water, $a_c(\lambda)$ is a nondimensional, statistically derived chlorophyll-specific absorption coefficient.

References

[1] Grosshans F, Van Assche G, Wenger J, Brouri R, Cerf N J and Grangier P 2003 *Nature* **421** 238–41
[2] Scarani V, Bechmann-Pasquinucci H, Cerf N J, Dušek M, Lütkenhaus N and Peev M 2009 *Rev. Mod. Phys.* **81** 1301
[3] Lo H K and Chau H F 1999 *Science* **283** 2050–6
[4] Lo H K, Curty M and Tamaki K 2014 *Nat. Photonics* **8** 595
[5] Li X H, Deng F G and Zhou H Y 2008 *Phys. Rev.* A **78** 022321
[6] Liao Q, Guo Y, Xie C, Huang D, Huang P and Zeng G 2018 *Quantum Inf. Process.* **17** 113
[7] Zhao W, Liao Q, Huang D and Guo Y 2019 *Quantum Inf. Process.* **18** 39
[8] Leverrier A and Grangier P 2009 *Phys. Rev. Lett.* **102** 180504
[9] Huang P, Fang J and Zeng G 2014 *Phys. Rev.* A **89** 042330
[10] Leverrier A and Grangier P 2010 arXiv:1002.4083
[11] Jouguet P, Kunz-Jacques S and Diamanti E 2013 *Phys. Rev.* A **87** 062313
[12] Wang T, Huang P, Zhou Y, Liu W, Ma H, Wang S and Zeng G 2018 *Opt. Express* **26** 2794–806
[13] Ma X C, Sun S H, Jiang M S and Liang L M 2013 *Phys. Rev.* A **88** 022339
[14] Ma X C, Sun S H, Jiang M S and Liang L M 2013 *Phys. Rev.* A **87** 052309
[15] Ma X C, Sun S H, Jiang M S, Gui M and Liang L M 2014 *Phys. Rev.* A **89** 042335
[16] Zhang Y C, Li Z, Yu S, Gu W, Peng X and Guo H 2014 *Phys. Rev.* A **90** 052325
[17] Pirandola S, Ottaviani C, Spedalieri G, Weedbrook C, Braunstein S L, Lloyd S, Gehring T, Jacobsen C S and Andersen U L 2015 *Nat. Photonics* **9** 397–402
[18] Wu Y, Zhou J, Gong X, Guo Y, Zhang Z M and He G 2016 *Phys. Rev.* A **93** 022325
[19] Ma H X, Huang P, Bai D Y, Wang T, Wang S Y, Bao W S and Zeng G H 2019 *Phys. Rev.* A **99** 022322
[20] Ma H X, Huang P, Bai D Y, Wang S Y, Bao W S and Zeng G H 2018 *Physical Review* A **97** 042329
[21] Guo Y, Liao Q, Wang Y, Huang D, Huang P and Zeng G 2017 *Phys. Rev.* A **95** 032304
[22] Liao Q, Guo Y, Huang D, Huang P and Zeng G 2018 *New J. Phys.* **20** 023015
[23] Yu C, Zou S, Mao Y and Guo Y 2020 *Applied Sciences* **10** 4175
[24] Huang P, He G, Fang J and Zeng G 2013 *Phys. Rev.* A **87** 012317
[25] Peng Q, Chen G, Li X, Liao Q and Guo Y 2019 *Entropy* **21** 1011
[26] Li Z, Zhang Y C, Xu F, Peng X and Guo H 2014 *Phys. Rev.* A **89** 052301
[27] Wu X, Wang Y, Li S, Zhang W, Huang D and Guo Y 2019 *Quantum Inf. Process.* **18** 1–16
[28] Wu X D, Wang Y J, Huang D and Guo Y 2020 *Frontiers of Physics* **15** 1–12
[29] Li F, Wang Y, Liao Q and Guo Y 2018 *Int. J. Theor. Phys.* **57** 2755–66
[30] Zhong H, Wang Y, Wang X, Liao Q, Wu X and Guo Y 2018 *Entropy* **20** 578
[31] Li Z, Zhang Y, Wang X, Xu B, Peng X and Guo H 2016 *Phys. Rev.* A **93** 012310
[32] Ye W, Guo Y, Zhang H, Zhong H, Mao Y and Hu L 2021 *J. Phys. B: At. Mol. Opt. Phys.* **54** 045501
[33] Prieur L and Sathyendranath S 1981 *Limnol. Oceanogr.* **26** 671–89
[34] Cochenour B M, Mullen L J and Laux A E 2008 *IEEE J. Oceanic Eng.* **33** 513–21
[35] Zeng Z 2015 A survey of underwater wireless optical communication *PhD Thesis* University of British Columbia (https://doi.org/10.14288/1.0220823)
[36] Saxena P and Bhatnagar M R 2019 *IEEE Access* **7** 105298 105298–313
[37] Xie C L, Guo Y, Wang Y J, Huang D and Zhang L 2018 *Chin. Phys. Lett.* **35** 090302
[38] Ruan X, Zhang H, Zhao W, Wang X, Li X and Guo Y 2019 *Applied Sciences* **9** 4956
[39] Li Z, Zhang H, Liao Q, Mao Y and Guo Y 2021 *Phys. Lett.* A **419** 127694
[40] Kong M, Wang J, Chen Y, Ali T, Sarwar R, Qiu Y, Wang S, Han J and Xu J 2017 *Opt. Express* **25** 21509–18
[41] Zuo Z, Wang Y, Mao Y, Ruan X and Guo Y 2021 *Phys. Rev.* A **104** 052613
[42] Pegau W S, Gray D and Zaneveld J R V 1997 *Appl. Opt.* **36** 6035–46
[43] Zhang X and Hu L 2010 Effects of temperature and salinity on light scattering by water *Proc. SPIE* **7678** 76780L