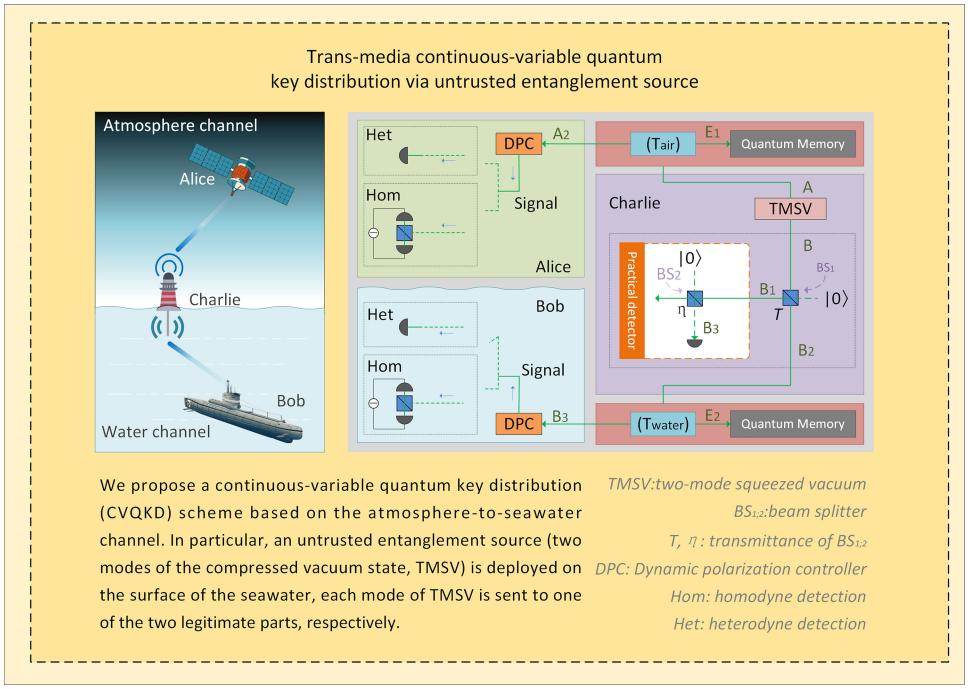
IEEE Photonics Journal
An IEEE Photonics Society Publication

Open Access

Trans-Media Continuous-Variable Quantum Key Distribution via Untrusted Entanglement Source

Volume 13, Number 2, April 2021

Ying Guo
Qingquan Peng
Qin Liao
Yijun Wang



DOI: 10.1109/JPHOT.2021.3064057

Trans-Media Continuous-Variable Quantum Key Distribution via Untrusted Entanglement Source

Ying Guo,[1] Qingquan Peng,[1] Qin Liao,[2] and Yijun Wang[1]

[1]School of Automation, Central South University, Changsha 410083, China
[2]College of Computer Science and Electronic Engineering, Hunan University, Changsha 410082, China

DOI:10.1109/JPHOT.2021.3064057

Manuscript received November 29, 2020; revised February 23, 2021; accepted March 2, 2021. Date of publication March 5, 2021; date of current version March 24, 2021. This work was supported in part by the National Natural Science Foundation of China under Grant 61871407, in part by the Hunan Provincial Natural Science Foundation of China under Grant 2020JJ5088, and in part by the Fundamental Research Funds for the Central Universities under Grant 531118010371. Corresponding author: Qin Liao (e-mail: llqqlq@hnu.edu.cn).

Abstract: We propose a continuous-variable quantum key distribution (CVQKD) scheme based on the atmosphere-to-seawater channel. In particular, an untrusted entanglement source (two modes of the compressed vacuum state, TMSV) is deployed on the surface of the seawater, each mode of TMSV is sent to one of the two legitimate parts, respectively. In this way, we can establish a trans-media CVQKD link between the atmosphere and the underwater. Meanwhile, a suitable non-Gaussian operation, namely photon subtraction, is introduced to enhance the performance of the trans-media CVQKD scheme. Security analysis shows that the proposed scheme can establish a trans-media quantum communication system on the atmosphere-to-seawater channel. Moreover, the maximum transmission distance can be further extended by using proper photon subtraction operation. Our scheme provides a guidance for applying CVQKD to trans-media channels.

Index Terms: Continuous variable quantum key distribution, trans-media channel, untrusted entanglement source, free-space quantum communication.

1. Introduction

Quantum key distribution (QKD) [1], [2] allows two legitimate parties, Alice, and Bob to remotely establish secure communication. Its security is guaranteed by the laws of quantum physics [3]. In general, there are two kinds of QKD technologies, i.e., discrete-variable quantum key distribution (DVQKD) [4] and continuous-variable quantum key distribution (CVQKD) [5], [6]. In CVQKD, the sender usually encodes key bits in the quadrature of the optical field, while the receiver can obtain the secret key bits by using high-speed and high-efficiency coherent detection techniques. This strategy usually has a repetition rate higher than that of single-photon detections so that CVQKD could potentially achieve higher secret key rates [7].

Based on the properties of quantum physics, it is theoretically proven that CVQKD is unconditionally secure in the fiber channel [8], [9]. At present, with people's research on communication channels, CVQKD has developed from fiber channel to free-space channel, and they have the same secret. For example, underwater quantum key distributions [10], atmosphere quantum key

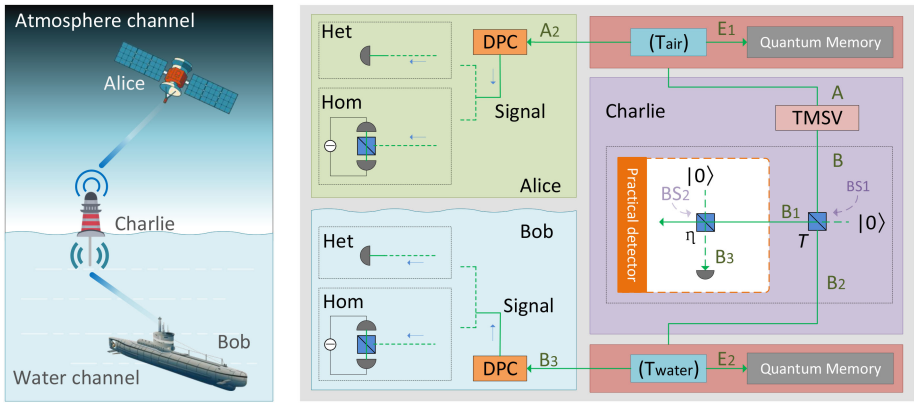


Fig. 1. (a) Trans-media CVQKD application scenario, (b) Trans-media CVQKD model diagram. TMSV: two-mode squeezed vacuum; DPC: Dynamic polarization controller; $BS_{1,2}$: beam splitter; T, η: transmittance of $BS_{1,2}$; Het: heterodyne detection; Hom: homodyne detection.

distributions [11], etc. However, these are all under a single media channel, and there is almost no CVQKD involving trans-media channels, so it is not suitable for the following scenarios, communication between satellite to submarine or ship to submarine-detector. Even so, the transmission performance of CVQKD is weaker than the fiber Channel [12]. This is mainly because the quantum signal is affected by absorption and scattering in free-space channels. Fortunately, non-Gaussian modulated photon subtraction technology [13] has been proven to effectively improve the performance of CVQKD by increasing the degree of entanglement between quantum.

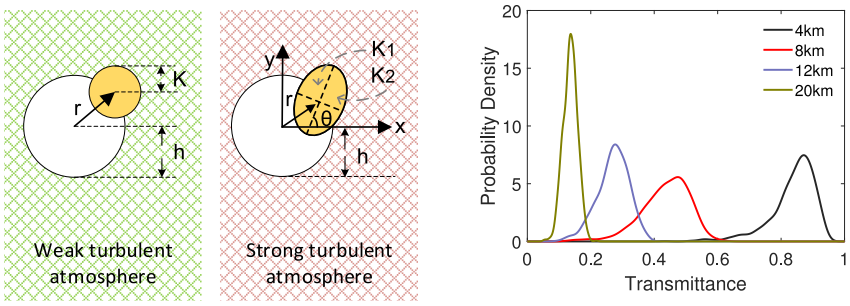
In this paper, we propose a trans-media CVQKD scheme and use photon subtraction technology to provide performance for this scheme. Specifically, we consider that the trans-media channel is composed of two parts, the atmosphere, and seawater. First, by placing an untrusted entanglement source (Charlie) [14] on the seawater surface, we have successfully constructed a trans-media CVQKD scheme from the atmosphere to the seawater. Security analysis shows that the proposed scheme can establish a trans-media quantum communication system in the atmosphere-to-seawater and generate a positive secret key rate. Among them, the effective transmission distance is 3885.15 m. Second, the performance of the scheme is further improved by Charlie using the photon subtraction operation. The effective transmission distance is increasing to 8693.73 m.

This paper is organized as follows: In Section 2, we introduce an untrusted entanglement source to establish a trans-media transmission model for CVQKD between atmosphere and seawater. In Section 3, we give a performance analysis of the trans-media CVQKD scheme and prove its security. In the end, the conclusions are drawn in Section 4.

2. Trans-Media CVQKD Scheme

In this work, we consider a situation where the quantum channel consists of multi-media and thus propose a trans-media CVQKD scheme based on the atmosphere-to-seawater channel to establish a trans-media quantum communication system.

Unlike the traditional CVQKD scheme, the sender Alice protects the source of entanglement. We place an untrusted entanglement source on the surface of the seawater and are controlled by third-party Charlie [15]. Charlie's participation enables us to build a quantum communication network involving trans-media transmission of atmosphere and seawater. Fig. 1 (a) shows this application scenario where Charlie is located on the surface of seawater. Alice is in the upper layer; Charlie's transmit quantum single to Alice through the atmosphere. Bob's is in the lower layer; Charlie's transmit quantum single to Bob through the seawater. Fig. 1 (b) shows the model diagram. First,



(a) Beam wandering case (b) Strong turbulence

Fig. 2. (a) Model diagram of the beam wandering case, (b) Distribution of transmission probabilities under strong springtime turbulence.

Charlie prepares the entanglement sources using a laser with a wavelength of 550 nm, half of which is transmitted to Alice through the atmospheric channel, and the other half is transmitted to Bob through the seawater channel after photon subtraction. Among them, quantum memory exists in the transmission of quantum single in the atmosphere or seawater. We regard the entire transmission process, then the signal loss can be expressed by the transmittance $T_{\text{air}} \in [0, 1]$. In the same way, the loss of quantum single in seawater can be expressed by the transmittance $T_{\text{water}} \in [0, 1]$. When Alice and Bob receive the quantum signal, they first perform a dynamic polarization control process on the signal and then perform homodyne detection or heterodyne detection. Finally, Alice and Bob respectively tell each other their detection results on the public channel and extract a string of secret keys by using parameter estimation, information reconciliation, and privacy amplification.

2.1 Atmospheric Channel

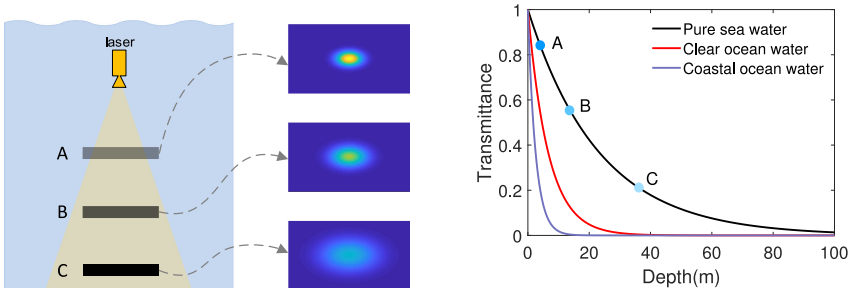
In a turbulent atmosphere, the transmission of quantum information can be affected by the beam, resulting from the unstable adjustment of the radiation source and insufficient coverage area at the receiver [16]. There are currently two atmospheric channel models, one is called fluctuating loss due to beam wandering [17] as shown in Fig. 2, and the other is randomly blocked quantum channel [18]. In this study, we found that the fluctuating loss due to beam wandering can better reflect the importance of photon subtraction. In a weak turbulent atmosphere, the beam-deflection distance r determines the transmittance of the atmospheric channel, whereas, in a strong turbulent atmosphere, atmospheric transmittance becomes complicated. It can also depend on the elliptical beam profile that includes the half axis K_1 and K_2 with an angle θ.

In a turbulent atmosphere case, atmospheric transmittance can be described as T_{air} [10], [18], as shown in Appendix B. The turbulence intensity, which affects the transmission efficiency of the CVQKD system, can be expressed by Rytov variance [19], given by

$$\sigma_R^2 = 1.23\mathbb{R}_n^2 N^{7/6} L^{11/9}, \tag{1}$$

where L is vertical propagation distance, N are optical wavenumber, and $\mathbb{R}_n^2$ is the refraction index structure parameters [20].

Without loss of generality, weak turbulence is usually regarded as a simplified model of strong turbulence. In this model, the atmospheric transmittance decreases as the beam deflection distance r and the beam spot radius k. We note that the fluctuation of the beam deflection distance r obeys Rice distribution [21]. When the distance between the Rytov variance $\mathbb{R}_n^2$ and the central aperture is reduced to zero, the resulting distribution can be simplified to the log-negative Weibull



(a) Beam-spread model diagram (b) Laser transmittance in seawater

Fig. 3. (a) Beam-spread model diagram for transmission in seawater, (b) Relationship of the transmittance and transmission depth.

distribution,

$$P(T_{\text{air}}) = \frac{2R^2}{\sigma^2 q T_{\text{air}}} \left(2In\frac{T_{\text{air}_0}}{T_{\text{air}}}\right)^{2/q-1} \exp\left[-\frac{R^2}{2\sigma^2}\left(2\log\frac{T_{\text{air}_0}}{T_{\text{air}}}\right)^{2/q}\right], \tag{2}$$

where $T_{\text{air}} \in [0, T_{\text{air}_0}]$, and $P(T_{\text{air}}) = 0$. The mean value of the fading probability distribution can be calculated by

$$\langle T_{\text{air}} \rangle = \int_0^{T_{\text{air}_0}} \sqrt{T_{\text{air}}} P(T_{\text{air}}) dT_{\text{air}}. \tag{3}$$

In Fig. 2(b), shows the transmission probability distribution at different distances in spring. This demonstrates the effect of weak turbulence on the transmission distance of communication system. In Appendix B, shows characteristics of the atmospheric transmittance with numerical simulations.

2.2 Seawater Channel

Quantum state transmission of seawater channel is weaker than that of atmospheric channel because of the absorption and scattering of light in seawater. The effect of light absorption is since the light intensity weakens sharply as the transmission distance, while the effect of light scattering is that the area radiated by light increases with the transmission distance. Both effects are irreversible thermal processes [22].

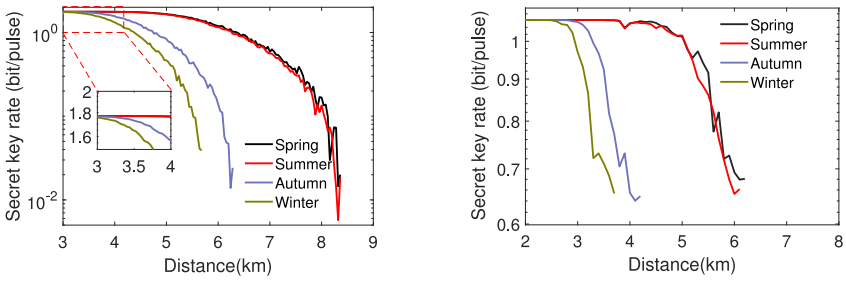
In Fig. 3(a), shows a beam-spread model diagram of the surface information when Bob is located at points A (3 m), B (11 m), and C (28 m), respectively. The brighter the yellow bright spot, the greater the light intensity, that is, the weaker the absorption effect, which can be calculated as

$$Q_{ab}(\iota) = \left[a_w(\iota) + 0.06 a_c(\iota)\mathbb{C}^{0.65}\right]\left[1 + 0.2e^{-0.014(\iota-440)}\right], \tag{4}$$

where ι is the wavelength, $\mathbb{C}$ represents chlorophyll concentration, and a_c is the chlorophyll-specific absorption coefficient obtained through statistics, and a_w is the absorption coefficient in seawater. Then, the smaller the halo radius, the more concentrated the light beam, that is, the weaker the scattering effect, which can be given by

$$Q_{sc}(\iota) = 0.3\frac{550}{\iota}\mathbb{C}^{0.62}. \tag{5}$$

The overall effect on the transmitted states can be derived $Q_{at}(\iota) = Q_{ab}(\iota) + Q_{sc}(\iota)$. The relevant values are given in Appendix C. Fig. 3(b) shows the relationship of the transmittance and depth in different seawaters, where A, B, and C correspond to the points in Fig. 3(a). We find that the transmittance decreases as the transmission depth increases.



(a) Weak turbulence (b) Strong turbulence

Fig. 4. Performance of the trans-media CVQKD scheme in turbulent atmosphere.

3. Security Analysis

In this section, we analyze the performance of CVQKD under the three quantum channel combinations of atmosphere-to-atmosphere, seawater-to-seawater, and atmosphere-to-water. We obtain the relationship between transmission distance and the secret key rate. The detailed calculation process is shown in Appendix D.

3.1 Atmosphere-to-Atmosphere

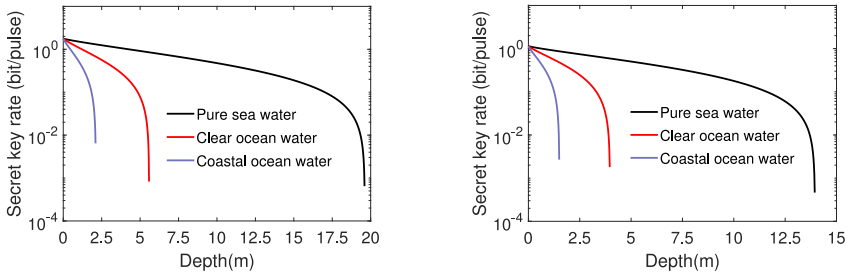
We assume that Alice and Bob are both deployed in the atmospheric channel to better analyze the atmospheric channel part of the trans-media CVQKD scheme. In this case, the two media channels of the trans-media CVQKD scheme are atmospheric channels.

Atmospheric information is a complex channel, and the transmission of quantum signals in the atmosphere is extremely susceptible to seasonal and strong turbulence. As shown in Fig. 4(a), the secret key rate of the trans-media CVQKD scheme is in the weak turbulent atmosphere. Spring and summer have the maximum transmission distance, which is related to the clean atmosphere, while the transmission distance in autumn and winter is short, which is related to the turbid atmosphere in these two seasons. Also, the maximum effective transmission distance is 8360 m in summer. However, when the quantum signal transmits in strong turbulence, the effective transmission distance will be further shortened. The secret key rate of the trans-media CVQKD scheme is in a strong turbulent atmosphere, as shown in Fig. 4(b). It can be seen from the figure that even in summer, the maximum effective transmission distance is only 6200 m. Through the above analysis, the CVQKD scheme can obtain the best performance only under the conditions of a clean atmosphere and weak turbulence, which means that the best season for quantum signal transmission is spring or summer.

3.2 Seawater-to-Seawater

We assume that Alice and Bob are both deployed in the seawater channel to better analyze the seawater channel part of the trans-media CVQKD scheme. In this case, the two media channels of the trans-media CVQKD scheme are seawater channels.

As shown in Fig. 5, the secret key rate of the trans-media CVQKD scheme for both homodyne and heterodyne measurements in the seawater channel. The pure seawater has the best performance, and the maximum transmission distance is 19.6 m. We can see that the better the water quality, the less the dissolved organic matter contained in the transmission medium, and the more conducive to the transmission of optical signals. Compare Fig. 5(a) and Fig. 5(b), it can be found that not only does the water quality affect performance, but also the measurement method affects performance. The maximum transmission distance of heterodyne detection is only 13.94 m, while that of homodyne detection is 19.62 m. Homodyne measurement is one of the conditions to



(a) Homodyne measurement (b) Heterodyne measurement

Fig. 5. Performance of the trans-media CVQKD scheme in seawater channel.

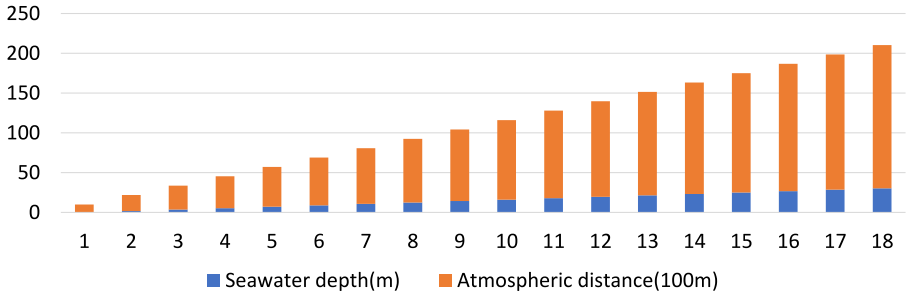


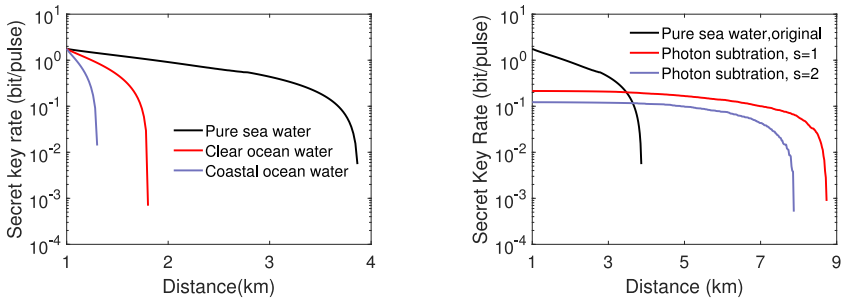
Fig. 6. Comparison of transmission distance between atmosphere and seawater in the trans-channel scheme.

obtain optimal performance in the CVQKD scheme. It is worth noting that although the transmission distance of the protocol in the seawater channel is less than that in the atmospheric channel, it provides a feasible method for the trans-media quantum communication between satellite and submarine.

3.3 Atmosphere-to-Seawater

Through the above security analysis, we know that the performance of the atmosphere and seawater in the trans-media CVQKD scheme is completely different. To optimize the performance of the trans-media CVQKD scheme, we define the distance $L_{distance}$ from Charlie to Alice and the distance L_{depth} from Charlie to Bob. As shown in Fig. 6, $L_{distance}$ and L_{depth} have the following relationship, orange represents the distance of $L_{distance}$, and blue represents the distance of L_{depth}.The initial value of $L_{distance}$ is 1Km. When $L_{distance}$ increases by 200 m, L_{depth} increases by 0.3575 m. For example, when the $L_{distance}$ is 5000 m, then the L_{depth} is 7.15 m.

We have established the relationship between the secret key rate and transmission distance of the trans-media CVKQD scheme, as shown in Fig. 7. Fig. 7(a) is a security analysis diagram of atmospheric-to-water CVQKD under the background of weak turbulence in summer. It is not difficult to find that the effective transmission distance of the multi-media channel is not as good as that of the atmospheric channel, but better than that of the seawater channel. This is because the attenuation coefficient of the atmospheric channel is smaller than that of the seawater channel, so the quantum signal can be transmitted in the atmosphere for a longer distance. The transmission of photons in the atmosphere is mainly limited by atmospheric turbulence. Turbulent eddies whose size is large compared to the size of the beam induce beam wandering [23]. But in water, photons inevitably interact with water molecules and other particulate matter in the water, where absorption and scattering seriously weaken the transmitted light signal. In the underwater environment,



(a) Original protocol (b) Photon Subtraction

Fig. 7. The performance of the trans-media CVQKD scheme involves the atmosphere and seawater channels. The ratio of atmospheric transmission distance to seawater transmission distance is 200 : 0.3575. (a) The performance of different water quality; (b) The performance of different photon subtraction operation for pure seawater.

substances such as chlorophyll can absorb blue and red light (Fig. C9). These substances and other colored dissolved organic matter increase the turbidity of the water, thereby reducing the distance of light travel. In addition, the concentration of colored dissolved organic matter will also change with the depth of the ocean, thereby changing the corresponding light attenuation coefficient [24]. For example, when Bob is placed in pure water, the trans-media CVQKD scheme maximum transmission distance is 4065.5 m. This transmission performance cannot meet the practicability of the trans-media CVQKD scheme. To further improve the performance of the trans-media CVQKD scheme, we will perform appropriate photon subtractions on Charlie's side. As shown in Fig. 7(b), the black line is the performance before improvement, red line and blue line are improved performance, where red line is a one-photon subtraction operation and the blue line is a two-photon subtraction operation. The simulation results show that the transmission performance of the trans-media CVQKD scheme can be effectively improved by using photon subtraction. It is worth noting that the trans-media CVQKD scheme achieves the best performance in one-photon subtraction operations. There are two main reasons for this phenomenon. One is that the success rate of one-photon subtraction is higher than that of two-photon subtraction [25]. Second, the photon reduction operation will cause the loss of quantum signals. Due to the loss of enough data, Alice and Bob cannot generate the secret key rate. The results also show that the improved scheme provides a feasible method to realize the actual trans-media transmission in the future.

4. Conclusion

We have proposed a novel scheme for trans-media CVQKD via untrusted entanglement source, thereby establishing secure quantum communications between the atmosphere and underwater. We have also improved the performance of the proposed scheme by taking advantage of suitable photon subtraction operation. Numerical simulations show that the proposed scheme can still establish secure communication through trans-media transmission, even if the entanglement source is untrusted. Moreover, photon subtraction can lengthen the maximal transmission distance of our system. This work provides guidance for applying CVQKD to trans-media channels.

Appendix A
Photon Subtraction

The TMSV state prepared by Charlie contains two modes A and B, which are sent to Alice and Bob, respectively. Then, Alice receive $\{\hat{a}, \hat{a}^{\dagger}\}$ and Bob receive $\{\hat{b}, \hat{b}^{\dagger}\}$. A covariance matrix of the TMSV

state can be written as

$$\gamma_{AB} = \begin{pmatrix} v\mathbb{I} & \sqrt{v^2-1}\mathbb{Z} \\ \sqrt{v^2-1}\mathbb{Z} & v\mathbb{I} \end{pmatrix}, \tag{A.1}$$

where $\mathbb{Z}$ is matrix diag $(1, -1)$, $\mathbb{I}$ is matrix diag (1,1), and $v = (v_a + v_s)/2$ is modulation variance.

As shown in Fig. 1(b), Charlie use a splitter (BS_1) to split mode B into modes B_1 and B_2 to obtain the tripartite state

$$\rho_{AB_1B_2} = U_{BS}[|\, TMSV\rangle \langle TMSV\, | \otimes |\, 0\rangle \langle 0\, |]U_{BS}^{\dagger}. \tag{A.2}$$

Thereafter, B_1 is measured with a positive operator's quantity. $\{\hat{\prod}_0, \hat{\prod}_1\}$ is saved only when the A and B_2 elements are clicked. The resulting TMSV after the photon subtraction operation can be described as

$$\rho_{AB_2}^{\hat{\prod}_1} = \frac{tr_{B_1}(\hat{\prod}_1 \rho_{AB_1B_2})}{tr_{AB_1B_2}(\hat{\prod}_1 \rho_{AB_1B_2})}, \tag{A.3}$$

where $tr_x(\cdot)$ is the partial trace of a multimode quantum state. The probability of element A being successfully clicked is calculated as

$$\begin{aligned} P_{(s)}^{\hat{\prod}_1} &= tr_{AB_1B_2}(\hat{\prod}_1 \rho_{AB_1B_2}) \\ &= (1-\nu^2)\sum_{n=s}^{\infty} \nu^{2n} C_n^s T^{n-s}(1-T)^s \\ &= \frac{(1-\nu^2)(1-T)^s \nu^{2s}}{(1-T\nu^2)^{s+1}}, \end{aligned} \tag{A.4}$$

where $\nu = \sqrt{(v-1)/(v+1)}$, s is the number of photons subtracted, and C_n^s is the combinatorial number and its relationship with the transmittance. Therefore, state γ_{AB_2} is no longer a Gaussian state [26], which can be derived as

$$\gamma_{AB_2}^{(s)} = \begin{pmatrix} a\mathbb{I} & c\mathbb{Z} \\ c\mathbb{Z} & b\mathbb{I} \end{pmatrix}, \tag{A.5}$$

with $a = \frac{T\nu^2+2s+1}{1-T\nu^2}$, $b = \frac{T\nu^2(2s+1)+1}{1-T\nu^2}$, and $c = \frac{2\sqrt{T}\nu(s+1)}{1-T\nu^2}$.

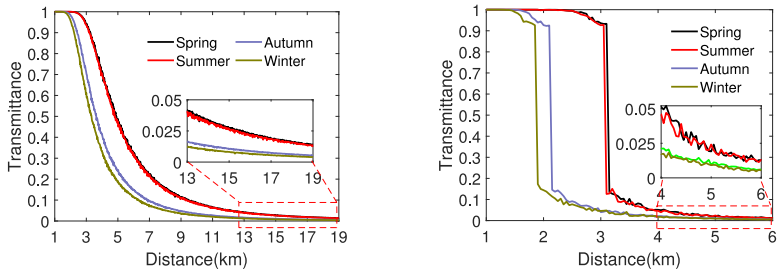
Appendix B
Parameter Derivation of the Atmospheric Channel

There are two kinds of atmospheric channels, i.e., weak turbulence and strong turbulence. In a weak turbulent atmosphere case, atmospheric transmittance can be calculated as T_{air}[10],

$$T_{\text{air}}^2 = T_{\text{air}_0}^2 \exp\left[-(r/R)^q\right], \tag{B.1}$$

where T_{air_0} is the maximum transmission coefficient given by $T_{\text{air}_0}^2 = 1 - \exp[-2(h/k)^2]$, R is the scale parameter, and q represent the shape, and r is the beam-deflection distance. In a strong turbulent atmosphere case, the elliptical beam model can use five parameters to describe the received light spot, i.e., $\{x_0, y_0, k_1, k_1, \theta\}$, where x_0 and y_0 partitions take the X-axis and Y-axis, which are used for reflecting the degree of the beam wandering, while the elliptical beam section half axis marked with k_1 and k_2, and the angle between the half-axis k_1 and the x-axis of the elliptical beam section is θ. According to the above-mentioned parameters, we obtain the transmittance of a strong turbulence atmosphere, which can be approximated as

$$T_{\text{air}} = T_{\text{air}_0} \exp\left\{-\left[\frac{r/h}{R\,(2/K_{\text{eff}}(\theta-\vartheta))}\right]^{q[2/K_{\text{eff}}(\theta-\vartheta)]}\right\}, \tag{B.2}$$



(a) Weak turbulence (b) Strong turbulence

Fig. B8. Simulation transmission distance and transmittance; beam radius 20 mm; receiver radius 60 mm.

TABLE B1
$\mathbb{R}_n^2$ Values in Four Seasons

	Spring	*Summer*	*Autumn*	*Winter*
$\mathbb{R}_n^2(m^{-2/3}\times 10^{-15})$	2.03	2.12	5.56	7.46

where $K_{\text{eff}}(\theta-\vartheta)$ represents the effective point radius. For $\Theta=\theta-\vartheta$, the parameter $K_{\text{eff}}(\Theta)$ can be calculated as

$$K_{\text{eff}}^2(\Theta)=4h^2\left\{\mathbb{W}\left(\frac{4h^2}{k_1k_2}\exp\left[\frac{h^2}{k_1^2}(1+2\cos^2(\Theta)\right]\times\exp\left[\frac{h^2}{k_2^2}(1+\sin^2(\Theta))\right]\right)\right\}^{-1}, \tag{B.3}$$

where $\mathbb{W}(\cdot)$ is the Lambert function. In addition, the maximum transmission coefficient is calculated as

$$T_{\text{air}_0}^2=1-I_0\left(h^2\frac{k_1^2-k_2^2}{k_1^2k_2^2}\right)\exp\left[-h^2\frac{k_1^2+k_2^2}{k_1^2k_2^2}\right]-2\left\{1-\exp\left[-\frac{h^2}{2}\left(\frac{1}{k_1}-\frac{1}{k_2}\right)^2\right]\right\}$$
$$\times\exp\left\{-\left[\frac{(k_1+k_2)^2/\left|k_1^2-k_2^2\right|}{R\left(1/k_1-1/k_2\right)}\right]^{q(1/k_1-1/k_2)}\right\}, \tag{B.4}$$

where I_0 is the modified Bessel functions.

Fig. B8 shows the relationship between transmission distance and transmittance. Table B1 shows that the $\mathbb{R}_n^2$-values of spring, summer, autumn and winter measured over a long period of time in Hefei, Anhui, China [20]. As shown in Fig. B8(a), since the atmosphere motion in weak turbulence is relatively stable, the change of the transmittance is not obvious. We find that it performs best in spring and summer, leading to a transmittance of 0.088 even at 10 km. However, the transmittance is only 0.026 when it becomes in autumn and winter at 10 km. It is worth noting that, under strong turbulence, due to the unstable atmosphere movement, the transmittance will drop sharply, as shown in Fig. B8(b). For example, when taking into account the transmission distances 3.1 km, 3 km, 2.1 km and 1.85 km in the spring, summer, autumn, and winter, respectively, the transmittance will approach around 0.1. Although there was no significant slump in winter, it was due to more severe shocks.

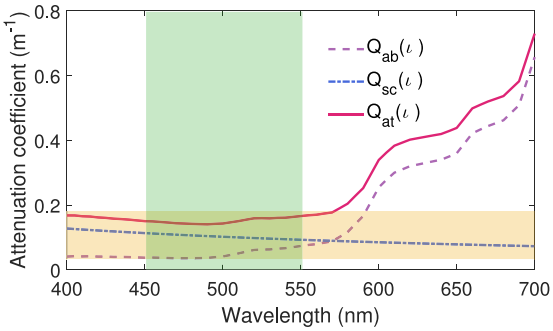


Fig. C9. Clear ocean water attenuation as a function of wavelength.

TABLE C2
Coefficient Values of Different Water Types At 520 nm

Water types	$Q_{ab}(m^{-1})$	$Q_{sc}(m^{-1})$	$Q_{at}(m^{-1})$
Pure sea water	0.0405	0.0025	0.043
Clear ocean water	0.114	0.037	0.151
Coastal ocean water	0.179	0.219	0.398

Appendix C
Parameter Derivation of the Seawater Channel

The total attenuation factor of light in seawater is Q_{at}, which is the sum of the absorption factor Q_{ab} and the scattering factor Q_{sc}. Both Qab and Qsc are associated with the wavelength l of the light. Fig. C9 shows the effect of clear seawater on shutdown at wavelengths between 400–700 nm, but with the least light attenuation at wavelengths between 450-55 nm, which coincides with the presence of a blue-green optical window in seawater. As shown in Table C2, the corresponding parameters for the effect of seawater of different water quality when the wavelength of the signal light is 520 nm. As shown in Table C2, the corresponding parameters for the effect of seawater of different water quality when the signal light wavelength is 520 nm [27].

Appendix D
The Secret Key Rate of the CVQKD System

When Eve performs a coherent attack [28], she can obtain the covariance matrix given by

$$\gamma_{E_1E_2} = \begin{pmatrix} W_A\mathbb{I} & \mathbb{G} \\ \mathbb{G} & W_B\mathbb{I} \end{pmatrix}, \tag{D.1}$$

where W_A is the variance corresponding to the link connecting Eve to Alice, and W_B is the variance corresponding to the link connecting Eve to Bob. In addition, $\mathbb{G}$ is matrix diag(g, g') given by Eve [29], which determines Eve's role in the whole link.

When it does not mean that $\mathbb{G}$ can take any value, from the actual situation [30], we have a constrain $|g| \leqslant \phi$ and $|g'| \leqslant \phi$ to a range [31], where

$$\phi := \min\{\sqrt{(W_A-1)(W_B+1)}, \sqrt{(W_A+1)(W_B-1)}\}. \tag{D.2}$$

Assuming Eve uses the same configuration for Alice and Bob, then $g = -g'$. In this case, the covariance matrix between Alice and Bob will be rewritten as

$$\gamma_{A_2B_3} = \begin{pmatrix} a'\mathbb{I} & c'\mathbb{Z} \\ c'\mathbb{Z} & b'\mathbb{I} \end{pmatrix}, \tag{D.3}$$

where $a' = T_1 a + (1 - T_1)W_A$, $b' = T_2 b + (1 - T_2)W_B$, and $c' = \sqrt{T_1}\sqrt{T_2}c + g\sqrt{1 - T_1}c$.

For the simplifying calculation of the model, we take the performance analysis with direct reconciliation, resulting in the secret key rate given by

$$k = I(A : B) - I(A : E), \tag{D.4}$$

where $I(A : B)$ is the mutual information between Alice and Bob, $I(A : E)$ is the mutual information between Alice and Eve. When Alice and Bob both use homodyne measurement, then the mutual information between them can be calculated as

$$I(A : B)_{\text{Hom}} = \frac{1}{2}\log_2\left(\frac{a'+1}{a'+1-c'^2/b'}\right). \tag{D.5}$$

If they use heterodyne measurement, the mutual information between them can be calculated as

$$I(A : B)_{\text{Het}} = \log_2\left(\frac{b'+1}{b'+1-c'^2/(a'+1)}\right). \tag{D.6}$$

The mutual information between Alice and Eve is $I(A : E) = S(E) - S(E|A)$, where $S(E)$ is information and $S(E|A)$ is conditional information. Considering that Eve can purify the CVQKD system, then $S(E) = S(AB)$. Therefore $S(AB)$ can be determined by the covariance matrix between Alice and Bob,

$$S(AB) = G[(\lambda_1 - 1)/2] + G[(\lambda_2 - 1)/2], \tag{D.7}$$

where $G(x) = (x + 1)\log_2(x + 1) - x\log_2 x$, and the symplectic can be calculated as

$$\lambda^2_{1,2} = \frac{1}{2}\left(\Delta \pm \sqrt{\Delta^2 - 4D^2}\right), \tag{D.8}$$

with $D = a'b' - c'^2$ and $\Delta = a'b' - c'^2$ [29]. In addition, we have $S(E|A) = S(B|A)$. Therefore, using Bob's covariance matrix, we get $S(B|A) = G[(\lambda_3 - 1)/2]$, where $\lambda^2_3 = a'(a' - c'^2/b')$. As Alice and Bob both use heterodyne measurement, we have $S(E|A) = S(BC|A)$. Similarly, conditional von Neumann entropy $S(BC|A)$ can be calculated as $S(BC|A) = G[(\lambda_4 - 1)/2]$, where $\lambda^2_4 = b' - c'^2/(a' + 1)$.

References

[1] M. A. Nielsen and I. Chuang, *Quantum Computation and Quantum Information*. Cambridge,U.K.: Cambridge Univ. Press, 2000.

[2] S. L. Braunstein and P. Van Loock, "Quantum information with continuous variables," *Rev. Modern Phys.*, vol. 77, no. 2, 2005, Art. no. 513.

[3] W. K. Wootters and W. H. Zurek, "A single quantum cannot be cloned," *Nature*, vol. 299, no. 5886, pp. 802–803, 1982.

[4] D. Elkouss, A. Leverrier, R. Alleaume, and J. J. Boutros, "Efficient reconciliation protocol for discrete-variable quantum key distribution," in *Proc. IEEE Int. Symp. Inf. Theory*, 2009, pp. 1879–1883.

[5] Q. Liao, G. Xiao, C. Xu, Y. Xu and Y. Guo, "Discretely modulated continuous-variable quantum key distribution with an untrusted entanglement source," *Phys. Rev. A*, vol. 102, no. 3, 2020, Art. no. 032604.

[6] D. Eleni and L. Anthony, "Distributing secret keys with quantum continuous variables: Principle security and implementations," *Entropy*, vol. 17, no. 9, pp. 6072–6092, 2015.

[7] Q. Liao, H. Liu, L. Zhu and Y. Guo, "Quantum secret sharing using discretely modulated coherent states," *Phys. Rev. A*, vol. 103, no. 3, 2021, Art. no. 032410.

[8] F. Fabian *et al.*, "Continuous variable quantum key distribution: Finite-key analysis of composable security against coherent attacks," *Phys. Rev. Lett.*, vol. 109, no. 10, 2012, Art. no. 100502.

[9] Q. Liao, G. Xiao, H. Zhong, and Y. Guo, "Multi-label learning for improving discretely-modulated continuous-variable quantum key distribution," *New J. Phys.*, vol. 22, no. 8, 2020, Art. no 0 83086.

[10] G. Ying *et al.*, "Channel-parameter estimation for satellite-to-submarine continuous-variable quantum key distribution," *Phys. Rev. A.*, vol. 97, no. 5, 2018, Art. no. 052326.

[11] S. Wang, P. Huang, T. Wang, and G. Zeng, "Atmospheric effects on continuous-variable quantum key distribution," *New J. Phys.*, vol. 20, no. 8, 2018, Art. no. 0 83037.

[12] A. Antonio, B. Nicolas, G. Nicolas, M. Serge, P. Stefano, and S. Valerio, "Device-independent security of quantum cryptography against collective attacks," *Phys. Rev. Lett.*, vol. 98, no. 23, 2007, Art. no. 230501.
[13] H. Peng, H. Guangqiang, F. Jian, and Z. Guihua, "Performance improvement of continuous-variable quantum key distribution via photon subtraction," *Phys. Rev. A.*, vol. 87, no. 1, 2013, Art. no. 0 12317.
[14] C. Weedbrook, "Continuous-variable quantum key distribution with entanglement in the middle," *Phys. Rev. A.*, vol. 87, no. 2, 2013, Art. no. 022308.
[15] Z. Zhaoyuan, S. Ronghua, and G. Ying, "Multipartite continuous variable quantum conferencing network with entanglement in the middle," *Appl. Sci.*, vol. 8, no. 8, 2018, Art. no. 1312.
[16] L. Zunino, D. Gulich, G. Funes, D. G. Pérez, "Turbulence-induced persistence in laser beam wandering," *Opt. Lett.*, vol. 40, no. 13, pp. 3145–3148, 2015.
[17] D. Y. Vasylyev, A. Semenov, and W. Vogel, "Toward global quantum communication: Beam wandering preserves nonclassicality," *Phys. Rev. Lett.*, vol. 108, no. 22, 2012, Art. no. 220501.
[18] G. Ying, X. Cailang, L. Qin, Z. Wei, Z. Guihua, and H. Duan, "Entanglement-distillation attack on continuous-variable quantum key distribution in a turbulent atmospheric channel," *Phys. Rev. A.*, vol. 96, no. 2, 2017, Art. no. 0 22320.
[19] A. Ishimaru, *Wave Propagation and Scattering in Random Media*, vol. 2, New York, NY, USA: Academic, 1978.
[20] P. Qingquan, C. Guojun, L. Xuan, L. Qin, and G. Ying, "Performance improvement of underwater continuous-variable quantum key distribution via photon subtraction," *Entropy*, vol. 21, no. 10, 2019, Art. no. 1011.
[21] E. Jakeman and K. Ridley, "A review of modeling fluctuations in scattered waves," *Waves in Random and Complex Media*, vol. 17, no. 3, pp. 405–406, 2007, doi: 10.1080/17455030701207491.
[22] X. Cailang, G. Ying, W. Yi-Jun, H. Duan, and Z. Ling, "Security simulation of continuous-variable quantum key distribution over air-to-water channel using Monte Carlo method," *Chin. Phys. Lett.*, vol. 35, no. 9, 2018, Art. no. 090302.
[23] C. Bonato, A. Tomaello, V. Da Deppo, G. Naletto, and P. Villoresi, "Feasibility of satellite quantum key distribution," *New J. Phys.*, vol. 11, no. 4, 2009, Art. no. 045017.
[24] D. Pompili and I. F. Akyildiz, "Overview of networking protocols for underwater wireless communications," *IEEE Commun. Mag.*, vol. 47, no. 1, pp. 97–102, Jan. 2009.
[25] L. Zhengyu, Z. Yichen, W. Xiangyu, X. Bingjie, P. Xiang, and G. Hong, "Non-gaussian postselection and virtual photon subtraction in continuous-variable quantum key distribution," *Phys. Rev. A.*, vol. 93, no. 1, 2016, Art. no. 012310.
[26] G. Ying, Y. Wei, Z. Hai, and L. Qin, "Continuous-variable quantum key distribution with non-gaussian quantum catalysis," *Phys. Rev. A.*, vol. 99, no. 3, 2019. doi: 10.1103/PhysRevA.99.032327.
[27] L. Jing, M. Yong, Z. Qunqun, Z. Bo, and W. Hongyuan, "Monte Carlo study on pulse response of underwater optical channel," *Opt. Eng.*, vol. 51, no. 6, 2012, Art. no. 066001.
[28] P. Stefano, "Entanglement reactivation in separable environments," *New J. Phys.*, vol. 15, no. 11, 2013, Art. no. 113046.
[29] C. Weedbrook *et al.*, "Gaussian quantum information," *Rev. Modern Phys.*, vol. 84, no. 2, 2012, Art. no. 621.
[30] P. Stefano, S. Alessio, and L. Seth, "Correlation matrices of two-mode bosonic systems," *Phys. Rev. A.*, vol. 79, no. 5, 2009, Art. no. 052327.
[31] S. Pirandola *et al.*, "High-rate measurement-device-independent quantum cryptography," *Nat. Photon.*, vol. 9, no. 6, pp. 397–402, 2015.