

Article

Passive Continuous Variable Quantum Key Distribution through the Oceanic Turbulence

Yiwu Zhu, Lei Mao, Hui Hu and Yijun Wang *

School of Automation, Central South University, Changsha 410083, China

* Correspondence: xxywyj@csu.edu.cn

Abstract: Continuous variable quantum key distribution (CVQKD) can be potentially implemented through seawater channels, whereas the involved oceanic turbulence has a negative effect on the maximal transmission distance of quantum communication systems. Here, we demonstrate the effects of the oceanic turbulence on the performance of the CVQKD system and suggest an implementation feasibility of the passive CVQKD through the oceanic turbulence-based channel. We achieve the channel transmittance characterized by the transmission distance and depth of the seawater. Moreover, a non-Gaussian approach is used for performance improvement while counteracting the effects of excess noises on the oceanic channel. Numerical simulations show that the photon operation (PO) unit can bring reductions of excess noise when taking into account the oceanic turbulence, and hence results in performance improvement in terms of transmission distance and depth as well. The passive CVQKD explores the intrinsic field fluctuations of a thermal source without using an active scheme and hence has a promising application in chip integration for portable quantum communications.

Keywords: quantum key distribution; seawater channel; quantum communications



Citation: Zhu, Y.; Mao, L.; Hu, H.; Wang, Y. Passive Continuous Variable Quantum Key Distribution through the Oceanic Turbulence. *Entropy* **2023**, *25*, 307. <https://doi.org/10.3390/e25020307>

Academic Editor: Rosario Lo Franco

Received: 6 December 2022

Revised: 29 December 2022

Accepted: 6 January 2023

Published: 7 February 2023



Copyright: © 2023 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<https://creativecommons.org/licenses/by/4.0/>).

1. Introduction

Continuous variable quantum key distribution (CVQKD) is a branch of quantum communications [1,2], where two participants called Alice and Bob encode information symmetrically with quadratures ($\hat{x}$ and $\hat{p}$) of the optical field with Gaussian modulation and then establish a string of secret key through public channels. It can make use of continuous light for the source preparation and the homodyne detector or heterodyne detector for detection [3,4]. Consequently, it has an advantage that can be potentially implemented with the existing optical technology, which gives birth to perfect compatibility and usability in modern optical communications. In implementations of the traditional CVQKD, Gaussian-distributed random numbers x and p are generated and coherent states $|x + ip\rangle$ is prepared with amplitude and phase modulations. The security of practical CVQKD systems has been proved in theoretical and practical frameworks [5]. Moreover, it can be used for potential implementations in quantum computers [6] and quantum networks [7]. The adaptability of CVQKD is one of its great attractions while holding up the malicious invasion in modern communication systems [8]. However, the quantum random number generator (QRNG) is required so that high-speed CVQKD at the chip level may have some disadvantages in terms of performance and size parameter trade-offs in most integrated photonics circuits.

Currently, kinds of CVQKD protocols have been suggested in free space, such as satellite-to-satellite links, satellite-to-ground links, air-to-water channels, and so on [9]. Unfortunately, the transmission coefficient fluctuates due to the effects of turbulence in free space, where the coherent detection may be distorted, leading to the decreased performance of the quantum communication system [10,11]. To model the turbulence in free space, several scenarios of turbulence have already been proposed [12,13], including beam wandering and elliptic-beam model, which demonstrates the evolution of the receiving beam in weak and strong atmospheric turbulence. However, there is no suitable channel

model that can illustrate the effects of the turbulence on performance of the free-space CVQKD system.

To overcome the aforementioned disadvantages, a passive state preparation can be used for CVQKD with the thermal source, where the QRNG has been replaced by a thermal source, beam splitters, optical attenuators and homodyne detectors [14]. It offers a prospect of simple integration with low cost which is much more suitable for portable applications [15,16]. We will illustrate characteristics of the turbulence-modulated channel that can be used to describe the effect of oceanic turbulence on the performance of the passive CVQKD. We characterize the structure of the passive CVQKD through the seawater channel and demonstrate the effect of the oceanic turbulence on the performance of the system, which involves the intrinsic field fluctuations of a thermal source. Different from the traditional CVQKD, it does not require active modulations and hence has a potential application in chip integration and portable quantum communications. Moreover, we counteract the effect of the channel-added noise by employing a non-Gaussian photon operation (PO) unit at the receiver, which can efficiently compensate for the channel-added noise generated from the imperfect detector, leading to the performance improvement of the CVQKD system in the terahertz band.

This paper is organized as follows. In Section 2, we propose the scheme of PO-based passive CVQKD in terahertz band through oceanic turbulence in seawater channel. Given the oceanic turbulence, we illustrate the characteristics of the PO-embedded detector and demonstrate the effects of the PO unit on the CVQKD system in Section 3. In Section 4, we consider the performance analysis of the passive CVQKD system with numerical simulations. Finally, conclusions are drawn in Section 5.

2. Passive CVQKD through Seawater Channel

As mentioned in the traditional CVQKD [17–19], quantum states can be prepared actively, and hence usually called active CVQKD. It requires a highly precise modulator to meet the constraints of a complex modulation format while suppressing the modulation errors, making it difficult to lay a portable terminal device for practical implementations. In order to solve the above problems, we suggest an approach to the passive CVQKD through oceanic turbulence, which involves thermal states in the terahertz (THz) band, as shown in Figure 1.

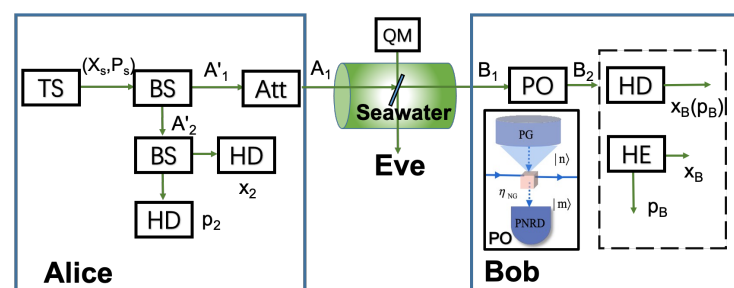


Figure 1. The schematic diagram of CVQKD with the passive state preparation. TS denotes thermal source, BS denotes beam splitter, Att is the optical attenuator, PO is photon operation involving photon generator (PG) with n input photons and m output photons, PNRD denotes photon number resolving detector, HD is the homodyne detector and HE is the heterodyne detector.

First of all, Alice splits the output of the thermal source (TS) with a beam splitter (BS), resulting in two spatial modes A'_1 and A'_2 . She chooses one mode A'_2 and measures with results (x_2, p_2) . Alice can get to know quadratures of A'_2 by scaling down the measurement results by using an optical attenuator. After that, she performs the suitable optical attenuation on another mode A'_1 , resulting in mode A_1 , which is transmitted to Bob through the seawater channel. Bob's actions on mode B_1 can be performed by using the PO unit, with input mode B_1 and output mode B_2 , as shown in Figure 1. There is a correlation between

the measurement results of Alice and Bob. Finally, they can generate a secret key after performing the data post-processing.

Different from the active CVQKD, which reduces the modulation deviation with the high extinction ratio modulators, the passive CVQKD makes full use of a thermal state for state preparation, rather than performing Gaussian modulation to a coherent state, and hence it simplifies implementations of the CVQKD system in practice. In Gaussian modulated coherent states (GMCS) CVQKD, the randomness comes from a true random number generator, whereas in the passive CVQKD, the randomness comes from the correlated thermal states that are split from a common thermal source. The former allows for the entanglement source that can be controlled by Eve while the latter requires a trusted source. In addition, Alice makes use of a high extinction ratio modulator to adjust the phase and amplitude of quantum states, which makes it difficult to realize in practice.

Moreover, due to the effects of the environmental thermal noise, the security threshold of the passive CVQKD is still high in terms of the secret key rate and the maximal transmission distance [20–22]. Fortunately, the turbulence under seawater can be efficiently compensated by deploying a suitable PO unit, such as photon catalysis, photon addition, and photon subtraction, to mitigate the turbulence wavefront aberrations of the received laser carrier signals. As shown in Figure 2, we find that zero photon catalysis (ZPC) performs better than others in terms of successful probability, and thus we select the ZPC-based OP unit for the performance improvement of the passive CVQKD system.

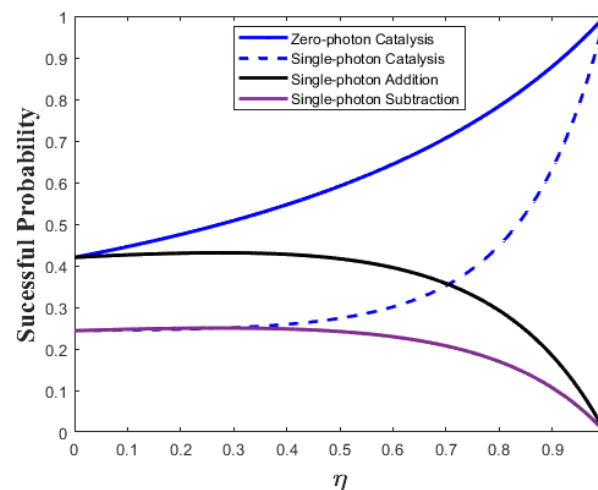


Figure 2. Successful probabilities of photon operations that involve photon catalysis, photon addition, and photon subtraction.

3. The PO Unit for Loss Compensation

To date, the passive CVQKD can be carried out with the PO-enabled unit through a seawater channel in terahertz (THz), and it turns out to be the potential to meet the needs of high-rate communications. In what follows, we will consider the effects of the PO unit on the passive CVQKD while taking into account the thermal source in the THz band.

The schematic diagram of the PO-embedded receiver for CVQKD can be shown in Figure 1. Alice prepares for the thermal states in the THz band. She performs the Gaussian modulation with two quadrature components, involving amplitude quadrature (x) and phase quadrature (p). The overall variance that includes the shot noise and modulation variance is given by $V = V_A + V_0$, where V_A is the zero-centered Gaussian distributed modulation variance and V_0 is the shot noise described as $V_0 = 2\bar{n}_0 + 1$. The parameter $\bar{n}_0$ is represented as

$$\bar{n}_0 = [\exp(h/\lambda\tau) - 1]^{-1}, \quad (1)$$

where λ denotes the wavelength of the THz thermal source, h is the temperature, and τ is Boltzmann's constant. The shot noise fluctuates due to thermal fluctuations and modulation.

Alice measures the coherent states projected on one mode, while she projects another mode, transmitting through the untrusted seawater channel.

At the receiver, Bob measures weak quantum signal with the local oscillator (LO) pulse in a shot-noise-limited homodyne detector (HD) or heterodyne detector (HE). Upon receiving the transmitted pulses, he demultiplexes signal and LO pulses, where an amplitude modulator is applied on the signal path to randomly attenuate the amplitude for the shot-noise estimation. Before performing detection, a suitable PO unit, such as zero photon catalysis (ZPC), is applied on the signal path and LO path to measure and correct wavefront distortions to restore signal quality by flattening the distorted wavefront. After that, Bob performs optical coherent detection to estimate the excess noise.

In Figure 3, we show that the PO unit can be regarded as a filter for attenuation in practice. The quantum signals follow Gaussian distribution mixed with excess noise for the seawater channel. Followed by the PO unit, we find that the weakened signals can be efficiently recovered while using the homodyne detector at the receiver. We note that in a PO unit, a wavefront sensor is applied to correct distorted wavefronts by physically distorting the reflective face sheet using mechanical actuators. The PO combining electronics with optics can realize the detection of distorted wavefront and then correct distorted wavefront in real-time. In addition, the PO unit will not start working until a very short period of time due to the characteristics of the transmission of the thermal source through oceanic turbulence in the seawater channel.

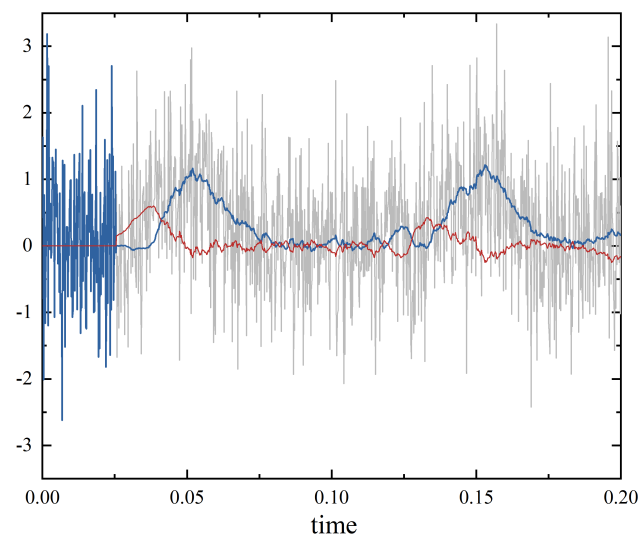


Figure 3. The effect of the ZPC-involved PO unit on the transmitted quantum signals through oceanic turbulence in the seawater channel. The gray line represents the waveform of the signal mixed with Gaussian-distributed noise. The blue line denotes the processed waveform of the signal mixed with Gaussian-distributed noise after using the PO unit. The red line denotes the signal error of the processed thermal source.

4. Performance Analysis

4.1. Parameter Evaluation of Seawater Channel

Before demonstrating the performance of the PO-enabled CVQKD through oceanic turbulence, we perform numerical simulations to show the characteristics of the seawater channel, which may have an effect on the performance of the CVQKD system.

A seawater channel can be modulated with the probability of transmittance distribution, which can be described with Beer's law [20,23]. When we ignore the multi-scattering of photons for the point-to-point propagation of signals, the deterministic losses caused by the ocean extinction have an effect on the transmittance with an estimation form [24]

$$T_B = \exp[-(a(\lambda, d) + b(\lambda, d))L], \quad (2)$$

where $a(\lambda, d)$ and $b(\lambda, d)$ denote the absorption coefficient and the scattering coefficient of light with wavelength λ , depth D and transmission distance L , which are shown in Figure 4a,b, respectively. Consequently, the transmittance can be described with Beer's law, as shown in Figure 4c. The transmittance decreases exponentially with the increase of transmission distance, and depth as well. In addition, we have the characteristics that illustrate the transmittance as a function of depth and transmission distance, which can be described with numerical simulation using the Monte-Carlo method in Figure 4d. It is interesting to find that, for the given transmission distance, there is a depth interval (from 50 m to 70 m) with better performance of the transmittance, due to the fact that the total attenuation is small for this interval. Therefore, we obtain the optimal depth that can be used for numerical simulations to illustrate the performance improvement of the passive CVQKD system.

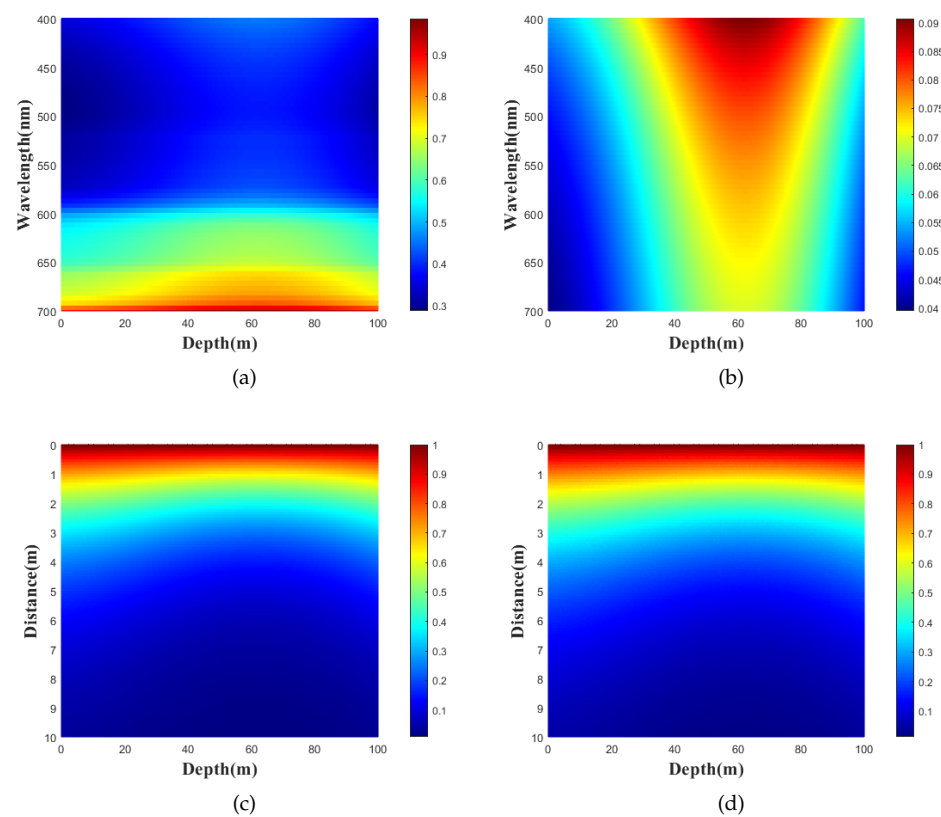


Figure 4. Parameters for transmittance in the seawater channel. (a) Variation of absorption coefficient $a(\lambda, d)$, (b) Variation of scattering coefficient $b(\lambda, d)$, (c) Transmittance T_B achieved with Beer method, (d) Transmittance T_B achieved with Monte-Carlo method.

4.2. Performance Analysis of the PO-Enabled CVQKD System

In what follows, we illustrate the performance of the PO-enabled CVQKD system with passive state preparation. We achieve performance improvement while comparing with the traditional scheme in terms of transmission distance and depth as well.

As shown in Figure 5, we demonstrate the secret key rate of the PO-enabled CVQKD system as a function of transmission distance for the oceanic turbulence model at the depths 80 m, 120 m and 200 m. We find that there is a decline in the secret key rate with the increasing transmission distance. Compared with the performance of the traditional scheme, the PO-embedded unit at the receiver, which serves as an attenuation in essence, enables the performance improvement of the CVQKD system.

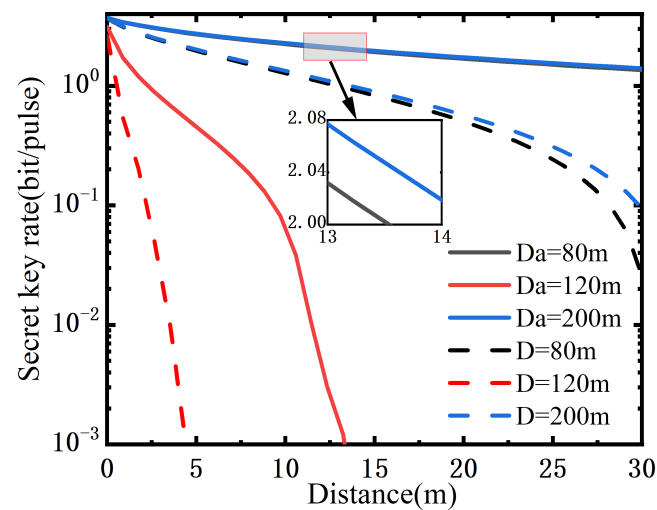


Figure 5. The secret key rate of the PO-enabled CVQKD system as a function of the transmission distance. The notation Da denotes the case of the PO-enabled scheme and the notation D denotes the traditional case.

As shown in Figure 6, we demonstrate the secret key rate of the PO-enabled CVQKD system as a function of the depth for the oceanic turbulence model at the transmission distances 1.65 m, 4.5 m and 6.5 m. Compared with the traditional scheme, the PO-embedded scheme performs better when considering the performance improvement of the CVQKD system. There is also a decline and then an increase in the secret key rate at the depth of 120 m, which is a particularly new phenomenon for both the PO-enabled CVQKD and the traditional CVQKD system. For the above-mentioned two cases, we find that the secret key rate is higher at depth 1.65 m than that at depths 4.5 m or 6.5 m. The reason is that the ocean absorption t_{abs} and the scattering factor t_{sca} increase rapidly at depths of 100 m to 140 m, which is shown in Figure 6b. We note that in actual situations, phytoplankton, particulate minerals and other extinction factors are usually enriched at this depth interval. In addition, we note the channel-added noise is relative to the transmission distance and the depth. For the given depth, the long transmission distance results in large channel-added noise. The reason is that when the turbulence gives rise to the fluctuation of the refractive index, the wavefront of the arriving beam is undermined, which degrades the performance of the transmission beam by contributing to beam wandering and redistribution of energy across the beam section (beam broadening and deformation).

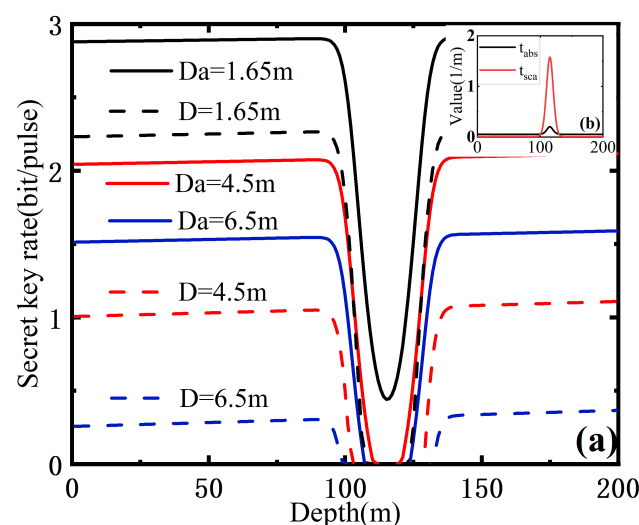


Figure 6. The secret key rate of the PO-enabled CVQKD system as a function of the depth. The notation Da denotes the case of the PO-enabled scheme and the notation D denotes the traditional case.

5. Conclusions

We have suggested an approach to performance improvement of the passive CVQKD through the oceanic turbulence in seawater channels, which can be improved by the embedded PO unit at the receiver. In addition, the characteristics of the seawater channel are illustrated with numerical simulations. We demonstrate the influences of the parameters of the seawater channel on the performance of the CVQKD system that involves the secret key rate, the transmission distance and the depth as well. We find that the embedded PO unit may have a positive effect on the performance of the passive CVQKD in free space. We illustrate the performance of the PO-enabled CVQKD through the seawater channel, which results in the increased secret key rate. It suggests an elegant approach to performance improvement of the practical CVQKD system in oceanic environments.

Author Contributions: Conceptualization, Y.Z.; writing—original draft preparation, L.M.; writing—review, H.H.; writing—editing, Y.W. All authors have read and agree to the published version of the manuscript.

Funding: This work was supported by the National Natural Science Foundation of China (Grant Nos. 61871407, 61801522), and the Key Research and Development Program of Hunan Province (Grant No. 2022GK2016).

Institutional Review Board Statement: The study did not require ethical approval.

Data Availability Statement: All data generated or analyzed during this study are included in this published article.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Grosshans, F.; Grangier, P. Continuous Variable Quantum Cryptography Using Coherent States. *Phys. Rev. Lett.* **2002**, *88*, 057902. [[CrossRef](#)] [[PubMed](#)]
2. Grosshans, F.; Assche, G.V.; Wenger, J.; Brouri, R.; Cerf, N.J.; Grangier, P. Quantum key distribution using gaussian-modulated coherent states. *Nature* **2003**, *421*, 238–241. [[CrossRef](#)] [[PubMed](#)]
3. Braunstein, S.L.; van Loock, P. Quantum information with continuous variables. *Rev. Mod. Phys.* **2005**, *77*, 513. [[CrossRef](#)]
4. Guo, Y.; Ye, W.; Zhong, H.; Liao, Q. Continuous-variable quantum key distribution with non-Gaussian quantum catalysis. *Phys. Rev. A* **2019**, *99*, 032327. [[CrossRef](#)]
5. Guo, Y.; Liao, Q.; Huang, D.; Zeng, G. Quantum relay schemes for continuous-variable quantum key distribution. *Phys. Rev. A* **2017**, *95*, 042326. [[CrossRef](#)]
6. Guo, Y.; Liao, Q.; Wang, Y.; Huang, D.; Huang, P.; Zeng, G. Performance improvement of continuous-variable quantum key distribution with an entangled source in the middle via photon subtraction. *Phys. Rev. A* **2017**, *96*, 032304. [[CrossRef](#)]
7. Chakraborty, K.; Rozpedek, F.; Dahlberg, A.; Wehner, S. Distributed Routing in a Quantum Internet. *arXiv* **2019**, arXiv:1907.11630.
8. Lira, E.R.; de Macêdo, H.B.; Lima, D.A.; Alt, L.; Oliveira, G. A reversible system based on hybrid toggle radius-4 cellular automata and its application as a block cipher. *arXiv* **2021**, arXiv:2106.04777.
9. Vasylyev, D.; Semenov, A.; Vogel, W. Magnon-squeezing as a niche of quantum magnonics. *Phys. Rev. Lett.* **2016**, *117*, 090501. [[CrossRef](#)]
10. Guo, Y.; Xie, C.; Liao, Q.; Zhao, W.; Zeng, G.; Huang, D. Entanglement-distillation attack on continuous-variable quantum key distribution in a turbulent atmospheric channel. *Phys. Rev. A* **2017**, *96*, 022320. [[CrossRef](#)]
11. Liao, Q.; Liu, H.; Gong, Y.; Wang, Z.; Peng, Q.; Guo, Y. Practical continuous-variable quantum secret sharing using plug-and-play dual-phase modulation. *Opt. Express* **2022**, *30*, 3876–3892. [[CrossRef](#)]
12. Zuo, Z.; Wang, Y.; Mao, Y.; Ye, W.; Hu, L.; Huang, D.; Guo, Y. Quantum catalysis-assisted attenuation for improving free-space continuous-variable quantum key distribution. *J. Phys. B At. Mol. Opt. Phys.* **2020**, *53*, 185501. [[CrossRef](#)]
13. Mao, Y.; Huang, W.; Zhong, H.; Wang, Y.; Qin, H.; Huang, D.; Guo, Y. Detecting quantum attacks: A machine learning based defense strategy for practical continuous-variable quantum key distribution. *New J. Phys.* **2020**, *22*, 083073. [[CrossRef](#)]
14. Wang, T.; Zuo, Z.; Li, L.; Huang, P.; Guo, Y.; Zeng, G. Continuous-Variable Quantum Key Distribution without Synchronized Clocks. *Phys. Rev. Appl.* **2022**, *18*, 014064. [[CrossRef](#)]
15. Jin, D.; Guo, Y.; Wang, Y.; Li, Y.; Huang, D. Key-sifting algorithms for continuous-variable quantum key distribution. *Phys. Rev. A* **2021**, *104*, 012616. [[CrossRef](#)]
16. Chen, Z.; Zhang, Y.; Wang, X.; Yu, S.; Guo, H. Improving Parameter Estimation of Entropic Uncertainty Relation in Continuous-Variable Quantum Key Distribution. *Entropy* **2019**, *21*, 652. [[CrossRef](#)] [[PubMed](#)]
17. Mao, Y.; Wang, Y.; Huang, W.; Qin, H.; Huang, D.; Guo, Y. Hidden-Markov-model-based calibration-attack recognition for continuous-variable quantum key distribution. *Phys. Rev. A* **2020**, *101*, 062320. [[CrossRef](#)]

18. Zuo, Z.; Wang, Y.J.; Mao, Y.; Ruan, X.; Guo, Y. Security of quantum communications in oceanic turbulence. *Phys. Rev. A* **2021**, *104*, 052613. [[CrossRef](#)]
19. Lo, H.-K.; Curty, M.; Qi, B. Measurement-Device-Independent Quantum Key Distribution. *Phys. Rev. Lett.* **2012**, *108*, 130503. [[CrossRef](#)]
20. Zuo, Z.; Wang, Y.J.; Liao, Q.; Guo, Y. Overcoming the uplink limit of satellite-based quantum communication with deterministic quantum teleportation. *Phys. Rev. A* **2021**, *104*, 022615; Erratum in *Phys. Rev. A* **2021**, *104*, 059901. [[CrossRef](#)]
21. Wang, Y.; Mao, Y.; Huang, W.; Huang, D.; Guo, Y. Optical frequency comb-based multichannel parallel continuous-variable quantum key distribution. *Opt. Express* **2019**, *27*, 25314. [[CrossRef](#)] [[PubMed](#)]
22. He, Y.; Mao, Y.; Huang, D.; Liao, Q.; Guo, Y. Indoor channel modeling for continuous variable quantum key distribution in the terahertz band. *Opt. Express* **2020**, *28*, 32386. [[CrossRef](#)] [[PubMed](#)]
23. Guo, Y.; Ding, J.; Mao, Y.; Ye, Y.; Liao, Q.; Huang, D. Quantum catalysis-based discrete modulation continuous variable quantum key distribution with eight states. *Phys. Lett. A* **2019**, *384*, 126340. [[CrossRef](#)]
24. Zhong, H.; Ye, W.; Zuo, Z.Y.; Huang, D.; Guo, Y. Kalman filter-enabled parameter estimation for simultaneous quantum key distribution and classical communication scheme over a satellite-mediated link. *Opt. Express* **2022**, *30*, 5981–6002. [[CrossRef](#)] [[PubMed](#)]

Disclaimer/Publisher’s Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.