entropy

MDPI

Article

Performance Improvement of Atmospheric Continuous-Variable Quantum Key Distribution with Untrusted Source

Qin Liao [1,2,*], Gang Xiao [1] and Shaoliang Peng [1,3,4,*]

[1] College of Computer Science and Electronic Engineering, Hunan University, Changsha 410082, China; hnuxg@hnu.edu.cn
[2] Center for Optoelectronic Information Engineering, Central South University, Changsha 410075, China
[3] School of Computer Science, National University of Defense Technology, Changsha 410073, China
[4] Peng Cheng Lab, Shenzhen 518000, China
* Correspondence: llqqlq@hnu.edu.cn (Q.L.); slpeng@hnu.edu.cn (S.P.)

Abstract: Atmospheric continuous-variable quantum key distribution (ACVQKD) has been proven to be secure theoretically with the assumption that the signal source is well protected by the sender so that it cannot be compromised. However, this assumption is quite unpractical in realistic quantum communication system. In this work, we investigate a practical situation in which the signal source is no longer protected by the legitimate parts, but is exposed to the untrusted atmospheric channel. We show that the performance of ACVQKD is reduced by removing the assumption, especially when putting the untrusted source at the middle of the channel. To improve the performance of the ACVQKD with the untrusted source, a non-Gaussian operation, called photon subtraction, is subsequently introduced. Numerical analysis shows that the performance of ACVQKD with an untrusted source can be improved by properly adopting the photon subtraction operation. Moreover, a special situation where the untrusted source is located in the middle of the atmospheric channel is also considered. Under direct reconciliation, we find that its performance can be significantly improved when the photon subtraction operation is manipulated by the sender.

Keywords: continuous-variable quantum key distribution; atmospheric channel; entanglement source; photon subtraction operation

check for updates

Citation: Liao, Q.; Xiao, G.; Peng, S. Performance Improvement of Atmospheric Continuous-Variable Quantum Key Distribution with Untrusted Source. *Entropy* **2021**, *23*, 760. https://doi.org/10.3390/e23060760

Academic Editor: Vladyslav Usenko

Received: 21 April 2021
Accepted: 13 June 2021
Published: 16 June 2021

1. Introduction

Continuous-variable quantum key distribution (CVQKD) [1–4] is a branch of quantum cryptography, it allows two distant legitimate partners (Alice and Bob) to share an identical secret key over an insecure quantum channel, its security is guaranteed by the laws of quantum mechanics [5,6]. Fiber-based CVQKD has been widely investigated over the past dozen years since the first CVQKD protocol, "GG02" was proposed [7]. According to the research, the theoretical security of fiber-based CVQKD has been proven in both an asymptotic limit [8] and finite-size regime [9]. Recently, the composable security proof for discrete-alphabet fiber-based CVQKD protocols have also been presented [10,11].

With the development of quantum communication technologies, especially after the first quantum satellite "Micius" is launched [12], CVQKD over free-space becomes another research hotspot [13,14]. CVQKD over free-space, especially in an atmospheric channel [15–17], can deliver a secret key to any place without the limitation of a fiber link, so that it is more flexible than fiber-based CVQKD. Therefore, investigating CVQKD over an atmospheric channel is beneficial for establishing global quantum communication systems. Recently, the ultimate limits and benchmarks have been established for ACVQKD [18], which provides comprehensive machinery for studying the composable finite-size security of CV-QKD protocols in free-space links (see also [19] for other investigations). However, due to the negative impact of transmission efficiency caused by atmospheric turbulence and the instability of the radiation source [20], the performance of CVQKD over an atmospheric channel is not desirable. The author of [21] suggested a tunable CVQKD scheme for the satellite-to-ground free space optical link using orthogonal frequency division multiplexing technology. Although it can theoretically improve the performance of ACVQKD in terms of the secret key rate, the complicated design is hard to implement with current technologies. The work of [22] proposed another improved approach for ACVQKD, showing that the performance of ACVQKD can be enhanced with the help of a proper non-Gaussian operation. However, all the above-mentioned works are based on an underlying assumption that the signal source cannot be compromised. This is actually quite unpractical in a real quantum system, since legitimate users may also be compromised in a realistic environment, let alone the signal source. Although this issue can be theoretically fixed by applying plug-and-play measurement-device-independent (PP MDI) configuration in which both the measurement device and signal source are integrated to the third untrusted party, Charlie [23], PP MDI-based DM CVQKD actually does not work well in a realistic communication system. This is because the most widely used amplitude modulators, e.g., $\mathrm{LiNbO_3}$ modulators, are polarization sensitive and features a polarizer, where the light can hardly be transmitted if its orientation is not perfectly aligned in PP configuration. Fortunately, Ref. [24] has proved the theoretical asymptotic security of CVQKD with a signal source in the middle of an insecure fiber link, thereby solving the issue of an untrusted entanglement source [25]. However, although security can be guaranteed, its performance is dramatically reduced.

In this work, we consider a practical configuration of ACVQKD in which a signal source is placed in an insecure atmospheric channel. With this configuration, we consider several situations where the signal source is placed at different positions of the atmospheric channel, and respectively analyze their performance. Unsurprisingly, we find that the performance of ACVQKD is dramatically reduced without the protection of legitimate parts, especially when the signal source is located in the middle of the atmospheric channel. In order to improve the performance of this practical ACVQKD system, photon subtraction [26] is introduced. Photon subtraction, which is a kind of non-Gaussian operation, has been demonstrated theoretically and experimentally to significantly enhance the maximal transmission distance of the CVQKD systems [27,28], and can be easily implemented with current technologies. Numerical simulation shows that the performance of ACVQKD with an untrusted source can be improved by properly adopting the photon subtraction operation. In particular, the performance of ACVQKD with an untrusted source in the middle of a channel can be significantly improved when the photon subtraction operation is applied to the import of the sender.

This paper is organized as follows. In Section 2, we demonstrate the design of the signal source in an untrusted channel, then, an improved ACVQKD by using photon subtraction is proposed. In Section 3, we show the security analysis of the improved ACVQKD. In Section 4, a model of transmission fluctuation in an atmospheric channel is introduced. Subsequently, we analyze the effect of the position of the signal source in an untrusted channel, and give the performance analysis of the ACVQKD with a photon subtraction operation through numerical simulation. Finally, a conclusion is given in Section 5.

2. ACVQKD with Untrusted Source and Its Improved Approach

In this section, we investigate a practical situation where the signal source is placed in an untrusted atmospheric channel, and detail the principle of a photon subtraction operation.

2.1. ACVQKD with Untrusted Source

In general, the signal source is used for generating a secure key and has to be protected by the trustworthy sender. However, the sender cannot guarantee the security of the signal source in the actual quantum system. In this view, we consider a practical configuration whereby the signal source is moved to the middle (or other location) of the untrusted atmospheric channel. In this configuration, the two-mode squeezed states (Einstein–Podolsky–Rosen (EPR) state) [29,30] serve as the signal source, and the corresponding Gaussian unitary is defined as $S(l) = \exp[\frac{l}{2}(\hat{a}\hat{b} - \hat{a}^{\dagger}\hat{b}^{\dagger})]$, where l is the squeezing parameter. The EPR state $|\Psi\rangle_{AB}$ is generated by combining two rotated squeezed vacuum states on a balanced beam splitter, and this process can be described as:

$$\gamma_{AB} = (Y^{BS})^T(\gamma_A \oplus \gamma_B)Y^{BS}, \tag{1}$$

where γ_A and γ_B are the covariance matrices of a squeezed and antisqueezed state, respectively, and Y^{BS} is the operation of the balanced beam splitter. The covariance matrices of γ_{AB} is written as:

$$\gamma_{AB} = \begin{pmatrix} VI & \sqrt{V^2-1}\mathbb{Z} \\ \sqrt{V^2-1}\mathbb{Z} & VI \end{pmatrix}, \tag{2}$$

where I represents the identity matrix diag(1,1), $\mathbb{Z}$ represents matrix $\begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$, and V is the modulation variance and its value can be calculated by $V = \frac{1}{2}(V_S + V_A)$. V_S is the variance for the squeezed state and V_A is for the antisqueezed state.

Once an EPR state is prepared, one half of the EPR state is transmitted to Alice through an atmospheric channel, and the other half is also transmitted to Bob through an atmospheric channel. Taking that the transmission of the channel fluctuates randomly and the signal source is moved to the atmospheric channel into consideration, the atmospheric channel is splitted into two halves, each half divided into N different subchannels with a constant attenuation. The transmission and possibility of each subchannel between Alice and the EPR source are $T_{1,i}(0\leq T_{1,i} \leq 1)$ and p_i, and those between the EPR source and Bob are $T_{2,i}(0\leq T_{2,i} \leq 1)$ and p_i. The relationship of subchannels is $\sum_{i=1}^{N} p_i = 1$, and schematic diagrams of the configuration is depicted in Figure 1.

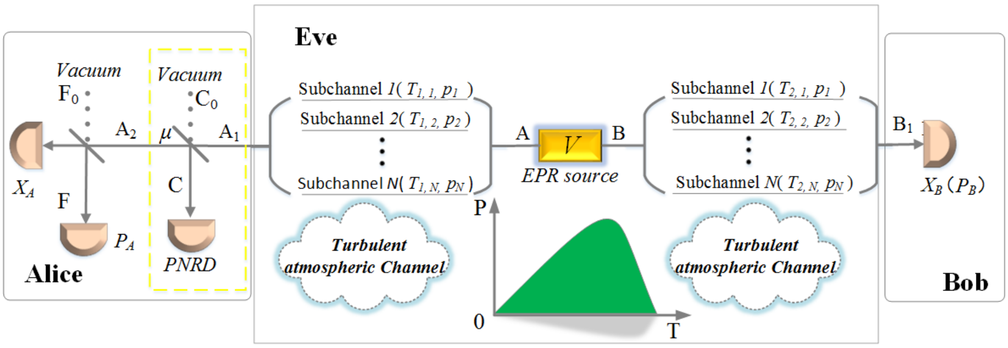

Eve
Vacuum
F_0
Vacuum
C_0
A_2
μ
A_1
X_A
F
C
P_A
PNRD
Alice
Subchannel 1($T_{1,1}$, p_1)
Subchannel 2($T_{1,2}$, p_2)
Subchannel N($T_{1,N}$, p_N)
A
V
B
EPR source
Subchannel 1($T_{2,1}$, p_1)
Subchannel 2($T_{2,2}$, p_2)
Subchannel N($T_{2,N}$, p_N)
B_1
X_B (P_B)
Turbulent atmospheric Channel
P
0
T
Turbulent atmospheric Channel
Bob

Figure 1. Schematic diagrams of the proposed ACVQKD with an untrusted source. The signal source (EPR) is located in the untrusted atmospheric channel. Each mode of EPR is sent to Alice and Bob respectively. The atmospheric channel is modeled by several subchannels, whose transmittance is fluctuating in time among T and occurrence probability P. Yellow dotted box presents the module of photon subtraction operation which is located on Alice's side.

The initial EPR state is represented in Equation (2). Therefore, the covariance matrix of the transmitted state in the certain ith subchannel can be described as:

$$\gamma_{A_1B_1,i} = \begin{pmatrix} V_{A_1X,i} & 0 & C_{X,i} & 0 \\ 0 & V_{A_1P,i} & 0 & C_{P,i} \\ C_{X,i} & 0 & V_{B_1X,i} & 0 \\ 0 & C_{P,i} & 0 & V_{B_1P,i} \end{pmatrix}, \tag{3}$$

where

$$\begin{aligned} V_{A_1X,i} &= V_{A_1P,i} = \frac{1}{2}T_{1,i}(V_A+V_S)+1-T_{1,i}+T_{1,i}\epsilon, \\ V_{B_1X,i} &= V_{B_1P,i} = \frac{1}{2}T_{2,i}(V_A+V_S)+1-T_{2,i}+T_{2,i}\epsilon, \\ C_{X,i} &= -C_{P,i} = \frac{1}{2}\sqrt{T_{1,i}T_{2,i}}(V_A-V_S). \end{aligned} \tag{4}$$

This convex mixture is a post-selected state, which is then used in security analysis. According to the Wigner function, it and its components can be represented by:

$$\begin{aligned} W(\mathbb{X},\mathbb{P}) &= \sum_i^N p_i W_i(\mathbb{X},\mathbb{P}), \\ W_i(\mathbb{X},\mathbb{P}) &= \frac{\exp(-\frac{1}{2}X_i^T V_{X,i}^{-1}X_i - \frac{1}{2}P_i^T V_{P,i}^{-1}P_i)}{4\pi^2\sqrt{detV_{X,i}detV_{P,i}}}, \end{aligned} \tag{5}$$

where $\mathbb{X}=(x_{A_1},x_{B_1}),\mathbb{P}=(p_{A_1},p_{B_1})$, and the matrices $V_{X,i}$ and $V_{P,i}$ are given by:

$$V_{X,i} = \begin{pmatrix} V_{A_1X,i} & C_{X,i} \\ C_{X,i} & V_{B_1X,i} \end{pmatrix}, V_{P,i} = \begin{pmatrix} V_{A_1P,i} & C_{P,i} \\ C_{P,i} & V_{B_1P,i} \end{pmatrix}. \tag{6}$$

From Equation (5), the second moments of the quadrature can be derived through integration:

$$\begin{aligned} \langle \hat{X},\hat{P} \rangle &= \int W(x_{A_1},x_{B_1},p_{A_1},p_{B_1})xpdx \\ &= \sum_i^N p_i \int W_i(x_{A_1},x_{B_1},p_{A_1},p_{B_1})xpdx \\ &= \sum_i^N p_i \langle \hat{X},\hat{P} \rangle_i. \end{aligned} \tag{7}$$

Since the mean value of the initial vacuum-squeezed state is null, the variances are directly governed by the second moments. According to Equation (7), the second moments of Equation (3) are linear combinations of the transmission factors $\sqrt{T_{1,i}}$, $\sqrt{T_{2,i}}$, $T_{1,i}$, and $T_{2,i}$. Therefore, we can use their expected values $\langle T_1 \rangle$, $\langle T_2 \rangle$, $\langle \sqrt{T_1} \rangle$, and $\langle \sqrt{T_2} \rangle$ to replace $T_{1,i}$, $T_{2,i}$, $\sqrt{T_{1,i}}$, and $\sqrt{T_{2,i}}$, respectively. The expected values can be calculated by:

$$\langle \sqrt{T_m} \rangle = \sum_i^N p_i \sqrt{T_{m,i}} \quad (m \in \{1,2\}) \tag{8}$$

and

$$\langle T_m \rangle = \sum_i^N p_i T_{m,i}. \tag{9}$$

2.2. Photon Subtraction Operation

As the signal source is no longer protected by the sender, the entanglement of EPR may be affected by an untrusted environment, resulting in a performance degeneration of the ACVQKD system. Fortunately, previous research has shown that the entanglement of EPR can be enhanced by a proper photon subtraction operation. To solve the above-mentioned issue, we therefore introduce a photon subtraction operation to improve the performance of ACVQKD with an untrusted source. According to the process ofa photon subtraction operation, the imporved Wigner function can be represented by:

$$W(x_{A_2},p_{A_2}) = \frac{1}{P_S(k)}\sum_{i=1}^N p_i P_{S,i}(k) W_i(x_{A_2},p_{A_2}), \tag{10}$$

where $P_S(k)$ is the total success probability of subtracting k photons. $P_S(k) = \sum_i^N p_i P_{S,i}(k)$, $P_{S,i}(k)$ is the success probability of subtracting k photons in the ith subchannel, which can be calculated by:

$$\begin{aligned} P_{S,i}(k) &= (1-\theta^2)\sum_{n=k}^{\infty}\theta^{2n}C_n^k\mu^{n-k}(1-\mu)^k \\ &= (1-\theta^2)(\frac{1-\mu}{\mu})^k\sum_{n=k}^{\infty}(\theta^2\mu)^n C_n^k \\ &= \frac{1-\theta^2}{1-\mu\theta^2}[\frac{\theta^2(1-\mu)}{1-\mu\theta^2}]^k, \end{aligned} \tag{11}$$

where C_n^k is the combinatorial number, μ is the transmittance of the balanced splitter (BS) in the photon subtraction operation, and the value of θ can be calculated by $V_{A_1X,i} = (1+\theta^2)/(1-\theta^2)$. The relationship between $P_{S,i}(k)$ and μ is shown in Figure 8.

For the photon subtraction operation on each subchannel, Alice uses a BS with transmittance μ to split $A_{1,i}$ and the vacuum state C_0 into modes $A_{2,i}$ and C, after that, we get a mixed tripartite state $\rho_{A_2CB_1,i}$, expressed as:

$$\rho_{A_2CB_1,i} = U_{BS}[|\psi\rangle_{A_1B_1,i}\langle\psi|_{A_1B_1,i}\otimes|0\rangle\langle 0|]U_{BS}^{\dagger}, \tag{12}$$

where $|\psi\rangle_{A_1B_1,i}$ is the output state in the ith subchannel before the photon-subtraction operation. Alice then uses the positive operator-valued measure (POVM)$\{\hat{\Pi}_0, \hat{\Pi}_1\}$ [31] to measure the state C in the photon number-resolving detector (PNRD), with states $A_{2,i}$ and $B_{1,i}$ kept only when the POVM element $\hat{\Pi}_1$ clicks. Therefore, the covariance matrix $\gamma_{A_2B_1,i}$ of the state $\rho_{A_2B_1,i}$ is obtained by:

$$\gamma_{A_2B_1,i} = \begin{pmatrix} V_{A_2X,i} & 0 & C'_{X,i} & 0 \\ 0 & V_{A_2P,i} & 0 & C'_{P,i} \\ C'_{X,i} & 0 & V'_{B_1X,i} & 0 \\ 0 & C'_{P,i} & 0 & V'_{B_1P,i} \end{pmatrix}, \tag{13}$$

where

$$\begin{aligned} V_{A_2X,i} = V_{A_2P,i} &= \frac{\sqrt{\mu}\theta(k+1)}{1-\mu\theta^2}, \\ V'_{B_1X,i} = V'_{B_1P,i} &= \frac{\mu\theta^2+2k+1}{1-\mu\theta^2}, \\ C'_{X,i} = -C'_{P,i} &= \frac{\mu\theta^2(2k+1)+1}{1-\mu\theta^2}. \end{aligned} \tag{14}$$

The detailed calculation can be found in [32].

After the analysis of the photon subtraction operation on each subchannel, the covariance matrix of the improved system A_2B_1 can be described as:

$$\gamma_{A_2B_1} = \begin{pmatrix} V_{A_2X} & 0 & C'_X & 0 \\ 0 & V_{A_2P} & 0 & C'_P \\ C'_X & 0 & V'_{B_1X} & 0 \\ 0 & C'_P & 0 & V'_{B_1P} \end{pmatrix}, \tag{15}$$

where the elements are given by:

$$\begin{aligned} V_{A_2X} = V_{A_2P} &= \frac{1}{P_S(k)}\sum_{i=1}^{N} p_i P_{S,i}(k) V_{A_2X,i}, \\ V'_{B_1X} = V'_{B_1P} &= \frac{1}{P_S(k)}\sum_{i=1}^{N} p_i P_{S,i}(k) V'_{B_1X,i}, \\ C'_X = -C'_P &= \frac{1}{P_S(k)}\sum_{i=1}^{N} p_i P_{S,i}(k) C'_{X,i}. \end{aligned} \tag{16}$$

In addition, the module of photon subtraction (the yellow dotted box in Figure 1) can also be deployed on Bob's side, so that we can obtain a different covariance matrix about the mixed state $\rho_{A_2B_1}$ due to the symmetry of the EPR source in the atmospheric channel CVQKD.

3. Calculation of the Secret Key Rate

In this section, we present the calculation of secret key rates of ACVQKD with an untrusted source under direct reconciliation [24]. Since the signal source is moved to the channel, there are two links in the whole ACVQKD system. In order to reduce the difficulty of analysis, we assume that the situation that occurs on these two links is identical, and the security analysis we considered is based on the case that the fading channel is only affected by constant attenuation, which means that the transmitted state still retains the Gaussian property. However, the attenuation of the quantum state is randomly fluctuating due to the environmental factors. Therefore, we use N subchannels to describe such a fluctuating channel on each link. In addition, after the photon subtraction operation on the Gaussian mixed state $\rho_{A_1B_1}$, the derived state $\rho_{A_2B_1}$ is no longer to hold the Gaussian property. Fortunately, the secret key rate of $\rho_{A_2B_1}$ is more than that of the Gaussian mixed state. Based on the above analysis, the calculation formula of secret key rate can be given by:

$$K = P_S(k)[\beta I(A_2 : B_1) - \chi_E], \tag{17}$$

where β is the reconciliation efficiency, $I(A_2 : B_1)$ is the Shannon mutual information between Alice and Bob, and χ_E is the Holevo bound of the mutual information between Alice and Eve. Subsequently, the atmospheric channel can be characterized by the covariance matrix $\gamma_{A_1B_1,i}$. Since the first moments of the squeezed state in both quadratures are zero, $\gamma_{A_1B_1,i}$ directly depends on the second moments. Therefore, the covariance matrix $\gamma_{A_1B_1}$ of the transmitted state is calculated by:

$$\gamma_{A_1B_1} = \begin{pmatrix} \langle T_1\rangle(V+H_1)I & \langle\sqrt{T_1}\rangle\langle\sqrt{T_2}\rangle\sqrt{(V^2-1)}\mathbb{Z} \\ \langle\sqrt{T_1}\rangle\langle\sqrt{T_2}\rangle\sqrt{(V^2-1)}\mathbb{Z} & \langle T_2\rangle(V+H_2)I, \end{pmatrix} \tag{18}$$

where $H_m = (1-\langle T_m\rangle)/\langle T_m\rangle + \epsilon$. The fluctuating channel can be regarded as a nonfading channel with transmittance $T_f = \langle\sqrt{T_1}\rangle^2$ and the channel-added noise can be estimated by $\epsilon_f = (\langle T_1\rangle - \langle\sqrt{T_1}\rangle^2)(V+\epsilon-1)$.

After the photon subtraction operation has been performed, the covariance matrix $\gamma_{A_1B_2}$ should be considered, as described in Equations (15) and (16). According to the standard form of the EPR state, some elements can be written as:

$$\begin{aligned} a &= V_{A_2X}, \\ b &= V'_{B_1X}, \\ c &= C'_X. \end{aligned} \tag{19}$$

Then the expression of the mutual information between Alice and Bob is represented by:

$$\begin{aligned} I(A_2 : B_1) &= \frac{1}{2} \log \frac{V_A + 1}{V_{A|B} + 1} \\ &= \frac{1}{2} \log \frac{a+1}{a+1-c^2/b}. \end{aligned} \tag{20}$$

As for the calculation of the Holevo quantity χ_E, assuming that Eve purifies the quantum system A_2B_1, so $\chi_E = S(E) - S(E \mid A_2)$, the calculation can be simplified as:

$$\chi_E = \sum_{i=1}^{2} G(\frac{\zeta_i - 1}{2}) - \sum_{i=3}^{4} G(\frac{\zeta_i - 1}{2}), \tag{21}$$

where

$$G(x) = (x+1)\log(x+1) - x \log x. \tag{22}$$

$S(E) = S(A_2B_1)$ is the function of the symplectic eigenvalues $\zeta_{1,2}$ of $\gamma^G_{A_2B_1}$, $\zeta^2_{1,2}$ can be calculated by:

$$\zeta^2_{1,2} = \frac{1}{2}[\Delta \pm \sqrt{\Delta^2 - 4D^2}], \tag{23}$$

with the denotations:

$$\begin{aligned} \Delta^2 &= a^2 + b^2 - 2c^2, \\ D^2 &= ab - c^2. \end{aligned} \tag{24}$$

$S(E \mid A_2) = S(B_1F \mid A_2)$ is the function of the symplectic eigenvalues $\zeta_{3,4}$, where F is Alice's auxiliary mode used for the heterodyne detection. The symplectic eigenvalues $\zeta^2_{3,4}$ can be calculated by:

$$\zeta^2_{3,4} = \frac{1}{2}[A_m \pm \sqrt{A_m^2 - 4B_m}], \tag{25}$$

with $A_m = (a + bD + \Delta)/(a+1)$ and $B_m = (D(b+D)/(a+1))$. Based on the above formula, the Holevo information bound χ_E for homodyne detection is estimated.

4. Performance Analysis and Disscussion

4.1. Fluctuating Loss Due to the Atmospheric Environment

The atmospheric channel is different from the fiber channel, thus it is necessary to consider the impact of transmission fluctuations caused by the atmospheric environment. In fact, the transmission fluctuation of the atmospheric channel is related to several factors, such as beam wandering, spreading, deformation, and scintillation [18,33,34], and these factors are usually caused by atmospheric turbulence and the instability of the radiation source. To simplify the analysis, here we only consider an important phenomenon of beam wandering [35,36], and the model of Figure 2 well describes the case of beam wandering.

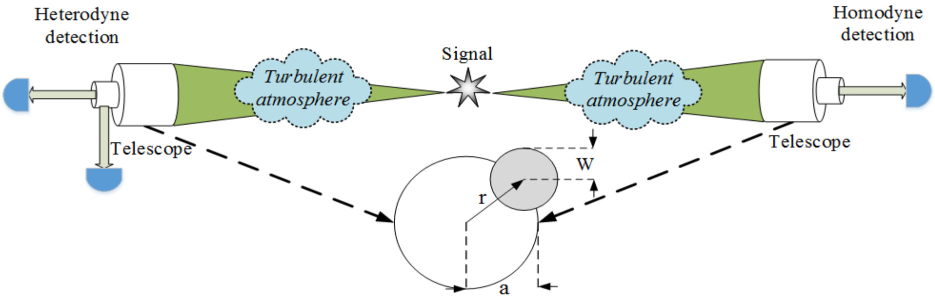


Figure 2. The signal is generated by the entanglement source placed in the atmospheric channel, and transmitted to Alice and Bob through the turbulent atmospheric channel, and finally detected with the help of a telescope. Note that the variation of the beam deflection distance *r* is the main reason for the fluctuation of transmittance.

Under this circumstance, the expression of the transmission efficiency is approximately given by:

$$H^2 = H_0^2 \exp\left[-(\frac{r}{R})^{\lambda}\right], \tag{26}$$

where r and R respectively represent the beam-deflection distance and scale parameter, and λ represents the shape. Parameter H_0 represents the maximal transmission coefficient, and has a relationship with the beam-spot radius W, calculated by:

$$H_0^2 = 1 - \exp(-2\frac{h^2}{W^2}), \tag{27}$$

where h represents the aperture radius. When the beam-deflection distance r equals zero, it is obvious that the transmission efficiency is determined by the ratio $\omega = h/W$ and cut at H_0 from Equations (26) and (27). For simplicity, we take some fixed values for ω, and then get the distribution of H^2 with respect to the beam-deflection distance r, as shown in Figure 3. We can find that the transmittance decreases with beam-deflection distance and has a lower maximum with a larger ratio ω.

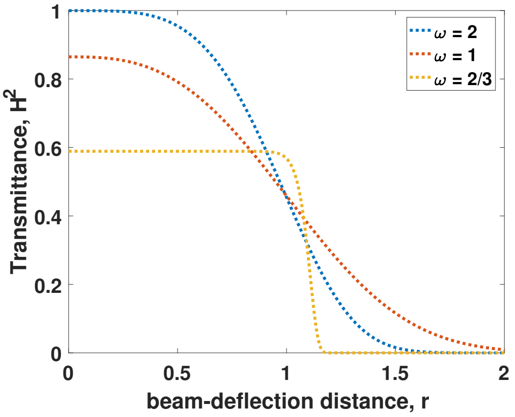


Figure 3. The relationship between transmittance squared and the beam deflection distance r for different values of the ratio ω.

According to Ref. [37], the beam-deflection distance r is decided by the Rice distribution [38], which is described as $P(H)$ by the variance δ^2 and the aperture center distance d. In addition, $P(H)$ will reduce to a log-negative Weibull distribution when the beam fluctuates around the center of the aperture (d = 0), and this distribution is written as:

$$P(H) = \frac{2R^2}{\lambda H \delta^2}(2\ln\frac{H_0}{H})^{\frac{2}{\lambda}-1} \exp[-\frac{R^2(2\ln\frac{H_0}{H})^{\frac{2}{\lambda}}}{2\delta^2}] \tag{28}$$

except for $H \in [0, H_0]$ and $P(H) = 0$.

Based on Ref. [39], the mean value of the transmission efficiency $\langle H^2 \rangle = \int_0^{H_0} H^2 P(H) dH$ and the mean of the square root of transmission efficiency $\langle H \rangle = \int_0^{H_0} HP(H)dH$. Note that the values of $\langle T_m \rangle$ and $\langle \sqrt{T_m} \rangle$ in Equation (18) can be calculated by $\langle H^2 \rangle$ and $\langle H \rangle$, respectively. In addition, according to the calculation of the Pirandola–Laurenza–Ottaviani–Banchi (PLOB) bound [40], one can bound the secret key capacity of the fading channel by means of the following free-space formula [18]:

$$K \leq \int_0^{H_0} H^2 P(H) \Phi(H^2) \frac{R^2}{\lambda H^2 \delta^2}(\ln\frac{H_0}{H^2})^{\frac{2}{\lambda}-1} \exp[-\frac{R^2(\ln\frac{H_0}{H^2})^{\frac{2}{\lambda}}}{2\delta^2}] dH, \tag{29}$$

where $\Phi(H) = -\log(1 - H^2)$.

4.2. Parameter Optimization

After analyzing the characteristics of the atmospheric channel, the parameters of ACVQKD system should be considered. The variance of the signal source is an important parameter since the effective fluctuation-induced noise is variance dependent, and its optimization is crucial for extending the secure distance in free-space link. In Figure 3, we obtain the relationship between beam-deflection distance r and transmission efficiency H^2, and find that transmission efficiency H^2 has the best performance with ratio $\omega = 2$. Therefore, we fix some parameters, such as $\omega = 2$, and then study the relationship between the signal source variance and secret key rate. In Figure 4, we show the relationship between V_S and the secret key rate of the different parameters δ^2 in case of the original protocol (without photon subtraction operation). We find that the secret key rate curves will rise sharply, no matter the value of parameter δ^2, the final infinity approaches 0. Which means that the applicable values of squeezing are sensitive to the fluctuating transmittance. The simulation shows that each of the curves is around Vs = 1/12, leading to the maximized secret key rate. All simulation parameters needed for simulation are presented in Table 1.

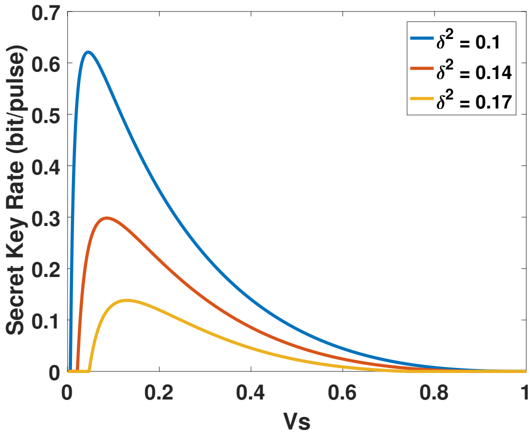


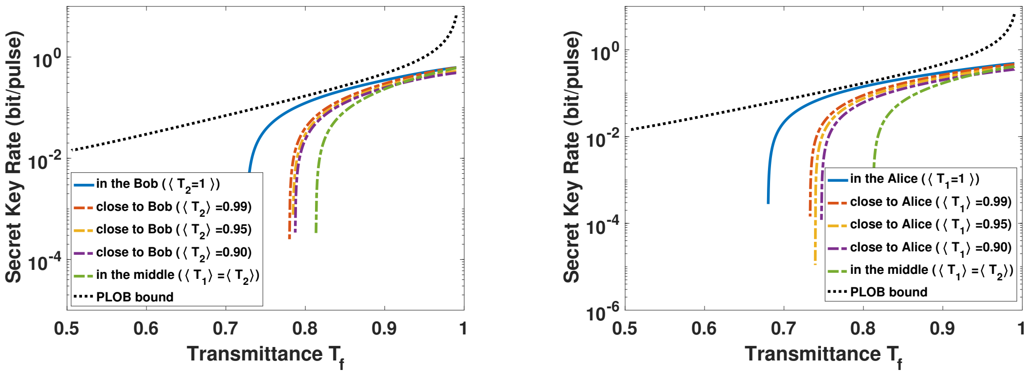
Figure 4. The effect of V_S on the secret key rate of CVQKD in the beam wandering case.

Table 1. Parameter settings for simulation of the secret key rate (all the variances and noises are in shot noise units).

V_S	β	h	W	ϵ
1/12	0.9	1	0.5	0.01

4.3. The Impact of Signal Source Location and Photon Subtraction Operation on ACVQKD

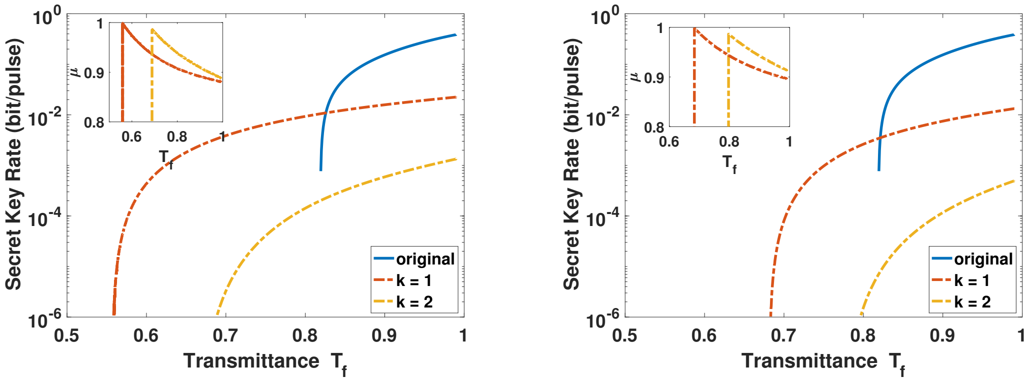
Since the signal source is moved to the atmospheric channel, the location of the signal source has an important effect on the performance of ACVQKD. We first consider the performance of ACVQKD with an untrusted signal source in three different situations: (1) The untrusted source is located close to Alice, (2) the untrusted source is located close to Bob, and (3) the untrusted source is located at the middle of channel. Figure 5 shows that the performance of ACVQKD (with a trusted source) outperforms the above three situations. This result matches with our expectation, as the untrusted source introduces extra noise. In addition, with the decrease of the channel transmittance $\langle T_2 \rangle$, the secret key rate is too difficult to exist in a lower channel transmittance, and it achieves the worst when the signal source is placed in the middle of the atmospheric channel. The same trend occurs when the signal source is placed close to Alice. The reason is that the system suffers more losses from the atmospheric environment due to the entanglement source being moved from the trusted legitimate party to the atmospheric channel, and the noise increases with the distance between the signal source and the legitimate party. Therefore, the photon subtraction operation is introduced to improve the performance of ACVQKD with the untrusted source.



(**a**) (**b**)

Figure 5. The secret key rate of the ACVQKD as a function of channel equivalent transmittance. (**a**) The untrusted source is located close to Bob, (**b**) the untrusted source is located close to Alice. The blue solid lines in (**a**,**b**) represent the signal source is generated by Bob whose security is trustworthy ($\langle T_2 \rangle$ = 1) and Alice whose security is trustworthy ($\langle T_1 \rangle$ = 1), respectively. All dash-dotted lines indicate that the signal source is placed close to Alice or Bob, the green dash-dotted lines represent the signal source is placed in the middle of atmospheric channel, and the black dotted lines represent the maximum secret key capacity on the beam wandering case.

In order to reduce the duplication and unnecessary work, we only focus on the worst case that the signal source is placed in the middle of the atmospheric channel. Note that the module of photon subtraction, the yellow box of Figure 1, can also be deployed to Bob's side. Therefore, there are two different ACVQKD configurations. In Figures 6 and 7, we optimize the μ of the BS in the photon subtraction operation to achieve the maximum key rate at different channel transmittance, and the insets represent the optimal transmittance μ of BS as a function of channel transmittance.



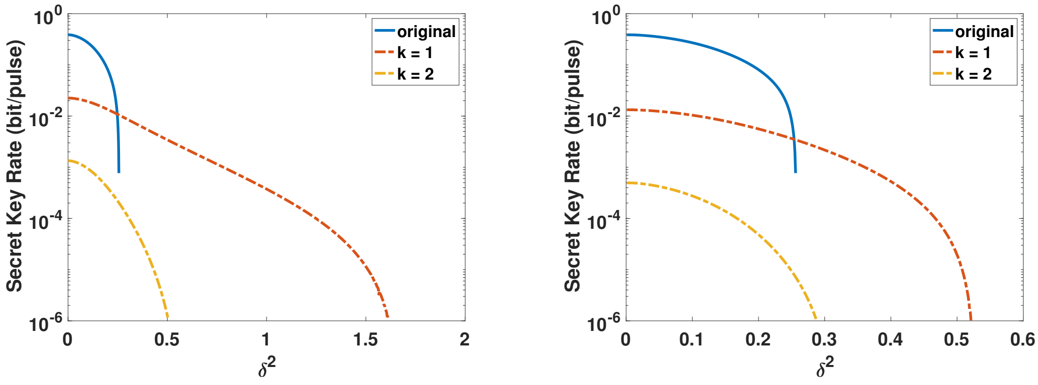
(**a**) (**b**)

Figure 6. The secret key rate of the ACVQKD as a function of equivalent transmittance T_f where the signal source is placed in middle of the atmospheric channel. (**a**) The photon-subtraction operation is deployed to Alice's side and (**b**) the photon-subtraction operation is deployed to Bob's side. The blue solid lines represent the case of the original ACVQKD without applying the photon-subtraction operation, the red dash-dotted lines represent the one-photon subtraction, and the yellow dash-dotted lines represent the two-photon subtraction.

In Figure 6, when transmittance T_f > 0.815, the original ACVQKD outperforms ACVQKD with the photon subtraction operation, no matter whether the photon subtraction operation is deployed on Alice's side or Bob's side. The reason is that the photon subtraction operation cannot improve the performance of ACVQKD on the low-loss channel.

Furthermore, since the success probability of the photon subtraction operation is relatively low, it further reduces the performance of ACVQKD. When transmittance $T_f < 0.815$, the secret key rate of original ACVQKD is reduced to 0, but there is still a relatively high secret key rate for the ACVQKD with the photon subtraction operation, which illustrates that the photon subtraction operation can tolerate lower channel transmittance with a relatively high secret key rate, so that it is more applicable in the real atmospheric environment. In addition, the performance of ACVQKD with one-photon subtraction operation is better than that of ACVQKD with two-photon subtraction operation, as shown in Figure 6a, it means that the success probability will be reduced and more noises will be introduced due to the risen number of subtracted photons, resulting in a worse performance. In Figure 6b, we can find that the effect of photon subtraction on Bob's side is not as good as that on Alice's side. The reason is that the module of the photon subtraction can be regarded as a trusted noise, which has a certain impact on the security of the key. When the photon subtraction operation is deployed to Bob's side, this trusted noise not only reduces the mutual information between Alice and Bob, but also increases the upper bound of Holevo, when compared to the photon subtraction operation deployed to Alice's side.

On the other hand, as the aperture center distance $d = 0$, the factors of the fluctuating channel depend on the variance δ^2. Figure 7 shows the relationship between the secret key rate and variance δ^2, and the photon subtraction operation cannot enhance the ability of channel to resist fluctuation when $\delta^2 < 0.256$, no matter whether the photon subtraction operation is deployed on Alice's side or Bob's side. However, when $0.256 < \delta^2$, the photon subtraction operation can really enhance the ability of the ACVQKD system to resist channel fluctuation.



(**a**) (**b**)

Figure 7. The secret key rate of the ACVQKD as a function of the variance of channel fluctuation δ^2 where the signal source is placed at the middle of the atmospheric channel. (**a**) The photon-subtraction operation is deployed to Alice's side and (**b**) the photon-subtraction operation is deployed to Bob's side. The blue solid lines represent the case of the original ACVQKD without photon subtraction, the reddash-dotted lines represent the one-photon subtraction, and the yellow dash-dotted lines represent the two-photon subtraction.

The other significant factor should be noted is the success probability of the photon subtraction operation. According to Equation (17), we find that it plays an important role in the calculation of secret key rates. Figure 8 shows that the success probability of the photon subtraction operation is reduced as the risen numbers of the subtracted photon, and the maximum success probability is less than 0.25. This means that a considerable amount of information will be discarded when performing the photon subtraction operation. In future, the performance and application of our scheme will be improved effectively if the success probability of the photon subtraction operation can be increased.

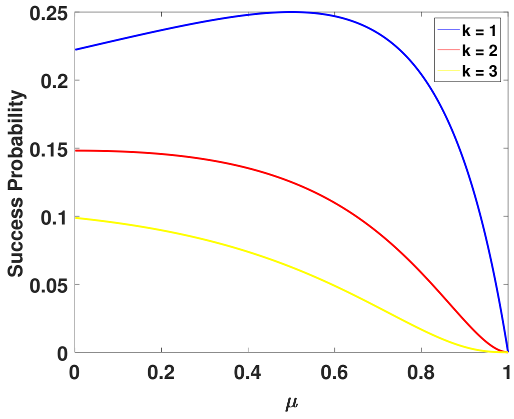


Figure 8. The success probability of subtracting k photons with different transmittances μ of BS. The curve surfaces from top to bottom represent one-photon subtraction, two-photon subtraction, three-photon subtraction respectively.

Now, we explore the reason as to why the introduction of the photon subtraction operation can improve the performance of the ACVQKD scheme. We consider the entanglement evolution of the two output modes of the two-mode squeezed state under the photon subtraction operation, and we use the logarithmic negativity as entanglement measures, which has known is an upper bound on the distillable entanglement. The logarithmic negativities of EPR state $|\Psi\rangle_{AB}$ and photon subtracted non-Gaussian state $|\Psi^{(1)}\rangle_{AB}$ can be calculated as:

$$E(|\Psi\rangle_{AB}) = -\log_2(1+\alpha^2) - 2\log_2(\sqrt{1+\alpha^2-\alpha}) \tag{30}$$

and

$$E(|\Psi^{(1)}\rangle_{AB}) = \frac{1+\alpha^2(1-\mu)}{\alpha\sqrt{\mu(1+\alpha^2)}} \sum_{n=1}^{\infty} \sqrt{n}(\frac{\alpha\sqrt{\mu}}{\sqrt{1+\alpha^2}})^n, \tag{31}$$

where $\alpha = \sinh l$. As shown in Figure 9, the photon-subtracted non-Gaussian state $|\Psi^{(1)}\rangle_{AB}$ has a larger amount of entanglement than the EPR state $|\Psi\rangle_{AB}$, and the gap extends with μ. In this sense, the photon subtraction operation has improved the correlation between the two modes of bipartite states. However, the photon subtraction operation can effectively improve the performance of ACVQKD based on if the channel attenuation factor being constant, if the attenuation factor is statistically fluctuating, its effect may be unsatisfactory.

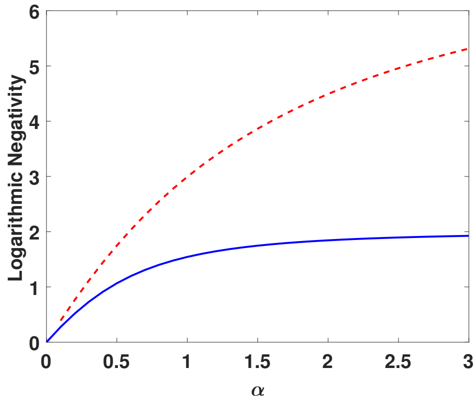


Figure 9. Comparison of the logarithmic negativity for state $|\Psi\rangle_{AB}$ [solid (blue) curve] and $|\Psi^{(1)}\rangle_{AB}$ for the photon subtraction operation [dashed (red) curve] as the function of α with μ = 0.95.

5. Conclusions

In this paper, we considered a practical situation of ACVQKD where the signal source is not protected by the legitimate parts, but is placed in an untrusted atmospheric channel. By removing the assumption that the signal source cannot be compromised, we found that the performance of ACVQKD with the untrusted source was dramatically degenerated especially when the signal source was placed at the middle of the atmospheric channel. Subsequently, a photon-subtraction operation, which is one of the non-Gaussian operations, was introduced. We showed that proper photon-subtraction operation could enhance the performance of ACVQKD with an untrusted source, especially when it was deployed to Alice's side. We thus provided a theoretical ground for applying ACVQKD to a realistic environment.

Author Contributions: Conceptualization, Q.L. and S.P.; methodology, Q.L. and G.X.; formal analysis, G.X. and Q.L.; investigation, G.X.; writing, G.X. and Q.L.; supervision, Q.L. and S.P. All authors have read and agreed to the published version of the manuscript.

Funding: This research was funded by the National Natural Science Foundation of China (Grant Nos. 61871407, 61772543), National Key R&D Project (Grant Nos. 2018YFB0704000, 2018YFC0910405), Hunan Provincial Natural Science Foundation of China (Grant No. 2020JJ5088), Science Foundation for Distinguished Young Scholars of Hunan Province (Grant No. 2020JJ2009) and the Fundamental Research Funds for the Central Universities (Grant No. 531118010371).

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

References

1. Pirandola, S.; Andersen, U.L.; Banchi, L.; Berta, M.; Bunandar, D.; Colbeck, R.; Englund, D.; Gehring, T.; Lupo, C.; Ottaviani, C.; et al. Advances in quantum cryptography. *Adv. Opt. Photon.* **2020**, *12*, 1012–1236. [CrossRef]
2. Liao, Q.; Xiao, G.; Zhong, H.; Guo, Y. Multi-label learning for improving discretely-modulated continuous-variable quantum key distribution. *New J. Phys.* **2020**, *22*, 083086. [CrossRef]
3. Liao, Q.; Liu, H.J.; Zhu, L.J.; Guo, Y. Quantum secret sharing using discretely modulated coherent states. *Phys. Rev. A* **2021**, *103*, 032410. [CrossRef]
4. Diamanti, E.; Leverrier, A. Distributing Secret Keys with Quantum Continuous Variables: Principle, Security and Implementations. *Entropy* **2015**, *17*, 6072–6092. [CrossRef]
5. Bang, J.Y.; Berger, M.S. Quantum mechanics and the generalized uncertainty principle. *Phys. Rev. D* **2006**, *74*, 125012. [CrossRef]
6. Wootter, W.K.; Zurek, W.H. A single quantum cannot be cloned. *Nature* **1982**, *299*, 802. [CrossRef]
7. Grosshans, F.; Grangier, P. Continuous Variable Quantum Cryptography Using Coherent States. *Phys. Rev. Lett.* **2002**, *88*, 057902. [CrossRef]
8. Grosshans, F. Collective Attacks and Unconditional Security in Continuous Variable Quantum Key Distribution. *Phys. Rev. Lett.* **2005**, *94*, 020504. [CrossRef]
9. Leverrier, A.; García-Patón, R.; Renner, R.; Cerf, N.J. Security of Continuous-Variable Quantum Key Distribution Against General Attacks. *Phys. Rev. Lett.* **2013**, *110*, 030502. [CrossRef]
10. Papanastasiou, P.; Pirandola, S. Continuous-variable quantum cryptography with discrete alphabets: Composable security under collective Gaussian attacks. *Phys. Rev. Res.* **2021**, *3*, 013047. [CrossRef]
11. Matsuura, T.; Maeda, K.; Sasaki, T.; Koashi, M. Finite-size security of continuous-variable quantum key distribution with digital signal processing. *Nat. Commun.* **2021**, *12*, 252. [CrossRef][PubMed]
12. Peng, C.Z.; Pan, J.W. Quantum Science Experimental Satellite "Micius". *Bull. Chin. Acad. Sci.* **2016**, *31*, 1096. [CrossRef]
13. Pirandola, S. Satellite Quantum Communications:Fundamental Bounds and Practical Security. *Phys. Rev. Res.* **2021**, *3*, 023130. [CrossRef]
14. Sidhu, J.S.; Joshi, S.K.; Gundogan, M.; Brougham, T.; Lowndes, D.; Mazzarella, L.; Krutzik, M.; Mohapatra, S.; Dequal, D.; Vallone, G.; et al. Advances in Space Quantum Communications. *IET Quantum Commun.* **2021**, under review. [CrossRef]
15. Hosseinidehaj, N.; Malaney, R. Erratum: Gaussian entanglement distribution via satellite. *Phys. Rev. A* **2016**, *93*, 069902. [CrossRef]
16. Derkach, I.; Usenko, V.C. Applicability of Squeezed- and Coherent-State Continuous-Variable Quantum Key Distribution over Satellite Links. *Entropy* **2021**, *23*, 55. [CrossRef]
17. Dequal, D.; Vidarte, L.T.; Rodriguez, V.R.; Vallone, G.; Villoresi, P.; Leverrier, A.; Diamanti, E. Feasibility of satellite-to-ground continuous-variable quantum key distribution. *NPJ Quantum Inf.* **2021**, *7*, 3. [CrossRef]
18. Pirandola, S. Limits and security of free-space quantum communications. *Phys. Rev. A* **2021**, *3*, 013279. [CrossRef]
19. Hosseinidehaj, N.; Walk, N.; Ralph, T.C. Composable finite-size effects in free-space continuous-variable quantum-key-distribution systems. *Phys. Rev. A* **2021**, *103*, 012605. [CrossRef]
20. Zunino, L.; Gulich, D.; Funes, G.; Perez, D.G. Turbulence-induced persistence in laser beam wandering. *Opt. Lett.* **2015**, *40*, 3145. [CrossRef]

21. Zhao, W.; Liao, Q.; Huang, D.; Guo, Y. Performance analysis of the satellite-to-ground continuous-variable quantum key distribution with orthogonal frequency division multiplexed modulation. *Quantum Inf. Process.* **2019**, *18*, 2147. [CrossRef]
22. Peng, Q.Q.; Liao, Q.; Guo, Y. Improving Continuous-Variable Quantum Key Distribution in a Turbulent Atmospheric Channel via Photon Subtraction. *Int. J. Theor. Phys.* **2019**, *19*, 4327. [CrossRef]
23. Liao, Q.; Guo, Y.; Wang, Y.; Huang, D. Dual-phase-modulated plug-and-play measurement-device-independent continuous-variable quantum key distribution. *Opt. Express.* **2018**, *26*, 019907. [CrossRef]
24. Weedbrook, C. Continuous-variable quantum key distribution with entanglement in the middle. *Phys. Rev. A* **2013**, *87*, 022308. [CrossRef]
25. Liao, Q.; Xiao, G.; Xu, C.G.; Xu, Y.; Guo, Y. Discretely modulated continuous-variable quantum key distribution with an untrusted entanglement source. *Phys. Rev. A* **2020**, *102*, 032604. [CrossRef]
26. Kim, M. S.; Park, E.; Knight, P.L.; Jeong, H. Nonclassicality of a photon-subtracted Gaussian field. *Phys. Rev. A* **2005**, *71*, 043805. [CrossRef]
27. Huang, P.; He, G.; Fang, J.; Zeng, G.H. Performance improvement of continuous-variable quantum key distribution via photon subtraction. *Phys. Rev. A* **2013**, *87*, 012317. [CrossRef]
28. Guo, Y.; Liao, Q.; Wang, Y.J.; Huang, D.; Huang, P.; Zeng, G.H. Performance improvement of continuous-variable quantum key distribution with an entangled source in the middle via photon subtraction. *Phys. Rev. A* **2017**, *95*, 032304. [CrossRef]
29. Duan, L.M.; Giedke, G.; Cirac, J.I.; Zoller, P. Inseparability Criterion for Continuous Variable Systems. *Phys. Rev. Lett.* **2000**, *84*, 2722. [CrossRef][PubMed]
30. Adhikari, S.; Majumdar, A.S.; Nayak, N. Teleportation of two-mode squeezed states. *Phys. Rev. A* **2008**, *77*, 012337. [CrossRef]
31. Eisaman, M.D.; Fan, J.; Migdall, A.; Polyakov, S.V. Invited Review Article: Single-photon sources and detectors. *Rev. Sci. Instrum.* **2011**, *82*, 071101. [CrossRef][PubMed]
32. Li, Z.; Zhang, Y.; Wang, X.; Xu, B.; Peng, X.; Guo, H. Non-Gaussian postselection and virtual photon subtraction in continuous-variable quantum key distribution. *Phys. Rev. A* **2016**, *93*, 012310. [CrossRef]
33. Zhang, S.J.; Xiao, C.; Zhou, C.; Wang, X.; Yao, J.S.; Zhang, H. L.; Bao, W.S. Performance analysis of the continuous-variable measurementdeviceindependent quantum key distribution under diverse weather conditions. *Chin. Phys. B* **2019**, *29*, 020301. [CrossRef]
34. Qian, X.M.; Zhu, W.Y.; Rao, R.Z. Intensity distribution properties of Gaussian vortex beam propagation in atmospheric turbulence. *Chin. Phys. B* **2015**, *24*, 044201. [CrossRef]
35. Vasylyev, D.Y.; Semenov, A.A.; Vogel, W. Toward Global Quantum Communication: Beam Wandering Preserves Nonclassicality. *Phys. Rev. Lett.* **2012**, *108*, 220501. [CrossRef][PubMed]
36. Zhang, S.L.; Jin, C.H.; Shi, J.H.; Guo, J.S.; Zou, X.B.; Guo, G.C. Continuous Variable Quantum Teleportation in Beam-Wandering Modeled Atmosphere Channel. *Chin. Phys. Lett.* **2017**, *34*, 040302. [CrossRef]
37. Jakeman, E.; Ridley, K.D. A Review Of “Modeling Fluctuations in Scattered Waves”. *Wave Random Complex* **2007**, *17*, 405–406. [CrossRef]
38. Berman, G.P.; Chumak, A.A.; Gorshkov, V.N. Beam wandering in the atmosphere: The effect of partial coherence. *Phys. Rev. E* **2007**, *76*, 056606. [CrossRef]
39. Usenko, V.C.; Heim, B.; Peuntinger, C.; Wittmann, C.; Marquardt, C.; Leuchs, G.; Filip, R. Entanglement of Gaussian states and the applicability to quantum key distribution over fading channels. *New J. Phys.* **2012**, *14*, 093048. [CrossRef]
40. Pirandola, S.; Laurenza, R.; Ottaviani, C.; Banchi, L. Fundamental limits of repeaterless quantum communications. *Nat. Commun.* **2017**, *8*, 150433. [CrossRef][PubMed]