mathematics

Article

Suppression of Fading Noise in Satellite-Mediated Continuous-Variable Quantum Key Distribution via Clusterization

Zhiyue Zuo, Wenqi Peng, Hui Xian, Wenqi Jiang, Hao Luo, Sha Xiong and Ying Guo

MDPI

https://doi.org/10.3390/math11163584

mathematics

Article

Suppression of Fading Noise in Satellite-Mediated Continuous-Variable Quantum Key Distribution via Clusterization

Zhiyue Zuo [1], Wenqi Peng [2], Hui Xian [1], Wenqi Jiang [1], Hao Luo [1], Sha Xiong [1,*] and Ying Guo [1,3]

[1] School of Automation, Central South University, Changsha 410083, China
[2] College of Physics and Information Engineering, Fuzhou University, Fuzhou 350108, China
[3] School of Computer Science, Beijing University of Posts and Telecommunications, Beijing 100876, China
* Correspondence: xiongsha@csu.edu.cn

Abstract: The satellite-mediated continuous-variable quantum key distribution (CV-QKD) protocol, which relies on off-the-shelf telecommunication components, has the potential for a global quantum communication network with all-day operation. However, the transmittance fluctuation of satellite-mediated links leads to the arriving quantum state showing non-Gaussian property, introducing extra fading noise in security analysis and limiting the secret key rate of the protocol. Here, we consider the clusterization method for data post-processing to suppress the fading noise in both downlink and uplink scenarios, where the measurement data are divided into several clusters, and we perform security analysis separately. In particular, we set the optimal upper and lower bounds of each cluster in terms of the probability distribution of transmittance (PDT), while finding an optimal cluster number for the trade-off between fading noise and the composable finite-size effect. Numerical analysis shows that the proposed method can improve the composable finite-size rate when the fading noise is large enough, even with only two clusters. Moreover, a high-speed CV-QKD system with a higher frequency of signal preparation and detection can extend the proposed method to work in the case of lower fading noise.

Keywords: clusterization; continuous-variable quantum key distribution; fading noise; satellite

MSC: 81P45

check for updates

Citation: Zuo, Z.; Peng, W.; Xian, H.; Jiang, W.; Luo, H.; Xiong, S.; Guo Y. Suppression of Fading Noise in Satellite-Mediated Continuous-Variable Quantum Key Distribution via Clusterization. *Mathematics* **2023**, *11*, 3584. https://doi.org/10.3390/math11163584

Academic Editor: Jonathan Blackledge

Received: 12 July 2023
Revised: 31 July 2023
Accepted: 16 August 2023
Published: 18 August 2023

1. Introduction

Over the past 40 years, considerable attention has been paid to quantum key distribution (QKD) for its ability to realize unconditional secure communication between two legal users over insecure channels [1]. To date, QKD has been well explored in both theory and experiments in fiber links, and the time is ripe to begin transitioning toward a global quantum communications network [2]. However, point-to-point QKD via optical fiber succeeds only within a limited distance due to huge fiber losses, and the no-cloning theorem [3] leads to the inability to perfectly clone a quantum state. One solution to this problem is the use of quantum repeaters for a global network [4]. These repeaters divide the transmission path into several segments, where errors and losses are corrected using entanglement swapping and entanglement purification. Unfortunately, the realization of mature quantum repeaters remains a challenge due to factors such as quantum memory technology, the limited brightness of entanglement sources, and technological restrictions associated with distillation protocols.

A promising solution with current technology is to build a satellite-mediated network, which connects widely separated ground stations using quantum satellites [5]. Although the quantum state suffers atmospheric attenuation, the feasibility of satellite-mediated QKD has been verified by several applications such as the *Micius* quantum satellite in

China [6]. This is because the layer around the Earth with a thickness of 20 km contains, on average, 95% of the total mass of the atmosphere, while above this layer is approximately a vacuum [7]. To date, most of the investigations into satellite-mediated QKD have been based on a discrete-variable (DV) protocol [8], which uses discrete quantum degrees of freedom to encode information, e.g., the polarization of a single photon. However, the entanglement of the DV protocol relies on probabilistic generation, which results in non-deterministic communication. Moreover, background noise due to sunlight presents a serious limitation for the achievable performance of the DV protocol, limiting most of the experiments obtained so far to nighttime [9]. Unlike the DV protocol, the continuous-variable (CV) protocol [10–13], which can generate deterministic entanglement using off-the-shelf telecommunication components, offers effective resistance against background noise for all-day operation. This is because only the contribution of the background noise mode-matching with the local oscillator (LO) will survive in the output of the CV protocol [14–17]. Additionally, the LO can be used as the frequency reference of the signal so that the CV protocol is not affected by the space-time curvature [18].

However, the achievable performance of the CV protocol is limited by finite entanglement [19], especially in a fading channel. To date, the longest transmission distance of fiber-based CV-QKD is 202.81 km [20], which is far from the goal of a global network. Bohmann et al. discussed the evolution of bipartite Gaussian entanglement in a fading channel [21] and showed that Gaussian entanglement transmission is related to the probability distribution of transmittance (PDT). The transmittance fluctuation leads to the total arriving quantum state becoming a non-Gaussian mixture of Gaussian states. This non-Gaussian property introduces extra fading noise, which reduces the secret key rate. To suppress fading noise, Usenko et al. proposed a postselection method [22], which sets a transmittance threshold and then selects the data from the sub-channels above this threshold for data post-processing. Since the total state after postselection has high transmittance and a more Gaussian nature, the fading noise is reduced. The postselection method was extended to the satellite-mediated case in [23]; however, it needs to discard measurement data, which reduces the data size for parameter estimation and key generation. Note that this is a challenging issue for space systems, as the satellite can only communicate with ground stations over very precise time windows, such that the systems may not gather enough measurement data in short time intervals.

Recently, Ruppert et al. proposed a clusterization method for suppressing fading noise without the need to discard measurement data [24]. In detail, the clusterization method reduces fading noise by dividing the measurement data into different clusters and performing security analysis for each cluster separately. Since each cluster contains data with relatively similar transmittance, its fading noise is reduced. Then, Hosseinidehaj et al. discussed the optimal cluster number in the horizontal link case based on the uniform binning of the probability distribution, which is not the optimal binning [25]. Motivated by the previous idea, in this work, we extend the clusterization method to satellite-mediated cases for suppressing fading noise, both downlink and uplink scenarios. We consider the Gaussian-modulated coherent state (GMCS) protocol with homodyne detection [26,27], while the security analysis is performed under Gaussian collective attacks [28]. To balance the trade-off between the fading noise and the composable finite-size effect, the number of clusters is optimized in terms of the PDT. Numerical analysis shows that the clusterization method can increase the secret key rate when the fading noise is large enough. Our solution does not require an increase in hardware equipment, and will not increase the burden of satellite space and energy.

This paper is organized as follows. In Section 2, we introduce the GMCS protocol over the satellite-mediated link and show its asymptotic key rate. In Section 3, we analyze the distribution of fading noise in the downlink and uplink scenarios and propose a clusterization scheme to suppress this noise. The security analysis in the composable finite-size regime is shown in Section 4, and Section 5 concludes this paper.

2. System Description

In this section, we describe the GMCS protocol over the satellite-mediated links based on its entanglement-based (EB) representation for the convenience of security analysis. Note that one usually uses the equivalent prepare-measure (PM) scheme instead of the EB scheme for the experimental setup because the PM scheme uses 'virtual' entanglement without requiring a real entangled state [29]. However, Eve is assumed to hold the purification of the system between Alice and Bob when one uses the EB scheme for security analysis. Therefore, the EB scheme is not convenient for security analysis with a trusted-loss or trusted-noise detector. In our manuscript, we assume an untrusted detector, where both the detector loss and setup noise are controlled by Eve. The security analysis with a trusted-loss or trusted-noise detector can be found in [30], which is based on the PM scheme. Moreover, the notation used for noise analysis is the equivalent number of thermal photons due to it being more appropriate for free-space channels compared to excess noise [30]. In addition, the wavelength of the protocol is set to $\lambda = 800$ nm. A higher frequency case, such as microwave frequency, exhibits higher loss and increased noise [30] and holds potential feasibility for short-range communication or inter-satellite communication, which are beyond the scope of this work.

Figure 1a shows the EB scheme of the GMCS protocol. Alice first prepares an Einstein–Podolsky–Rosen (EPR) state as the entangled source, which can be characterized by its covariance matrix [31]

$$\mathrm{V}_{AB} = \begin{bmatrix} \mu \mathrm{I} & \sqrt{\mu^2 - 1}\mathrm{Z} \\ \sqrt{\mu^2 - 1}\mathrm{Z} & \mu \mathrm{I} \end{bmatrix}, \tag{1}$$

where $\mathrm{Z} = \mathrm{diag}(1, -1)$, $\mathrm{I} = \mathrm{diag}(1, 1)$, and the signal variance $\mu = \sigma_x^2 + 1$, with a modulation variance of σ_x^2. Then, mode A of the EPR state is kept locally for heterodyne detection while another mode, B, is sent to Bob over the satellite-mediated (fading) link, which is characterized by the random transmittance η_{ch} and the mean number of background thermal photons $\bar{n}_B$. Note that Alice performing heterodyne detection on mode A will collapse mode B into a coherent state, which reveals the equivalence between the PM scheme and the EB scheme [29]. In terms of the Glauber–Sudarshan P function, the evolution of the quantum state in a fading link can be described by [32]

$$P_{\mathrm{out}}(\alpha) = \int_0^1 d\eta_{\mathrm{ch}} \mathcal{P}(\eta_{\mathrm{ch}}) \frac{1}{\eta_{\mathrm{ch}}} P_{\mathrm{in}}(\frac{\alpha}{\sqrt{\eta_{\mathrm{ch}}}}), \tag{2}$$

where $\mathcal{P}(\eta_{\mathrm{ch}})$ is the PDT, and $P_{\mathrm{in}}(\alpha)$ and $P_{\mathrm{out}}(\alpha)$ are the P functions of the input state and output state, respectively. According to Equation (2), the evolution of the quantum state is characterized by the statistics $\mathcal{P}(\eta_{\mathrm{ch}})$. Therefore, we treat the fading link using the statistical mean as in [22], where the link is divided into K stable sub-links, with a constant transmittance $\{\eta_{\mathrm{ch}}^j\}_{j=1,\ldots,K}$ $(0 \leq \eta_{\mathrm{ch}}^j \leq 1)$ and corresponding probability $\{\mathcal{P}^j\}_{j=1,\ldots,K}$ (note that $\Sigma_{j=1}^K \mathcal{P}^j = 1$). Then, the arriving quantum state is a mixture of the results in each sub-link, weighted by corresponding probability, whose total covariance matrix is given by

$$\mathrm{V}_{AB_1} = \begin{bmatrix} \mu \mathrm{I} & \langle\sqrt{\tau}\rangle\sqrt{\mu^2 - 1}\mathrm{Z} \\ \langle\sqrt{\tau}\rangle\sqrt{\mu^2 - 1}\mathrm{Z} & [\langle\tau\rangle(\mu - 1) + 2\bar{n} + 1]\mathrm{I} \end{bmatrix}, \tag{3}$$

where $\langle\tau\rangle = \sum_{j=1}^K \mathcal{P}^j \tau^j$, $\langle\sqrt{\tau}\rangle = \Sigma_{j=1}^K \mathcal{P}^j \sqrt{\tau^j}$, and $\bar{n}$ is the total number of thermal photons due to the various sources of noise. Note that the above covariance matrix takes the detector efficiency η_{eff} (considered constant) into account, i.e., $\tau^j = \eta_{\mathrm{eff}}\eta_{\mathrm{ch}}^j$. Finally, Bob performs shot-noise limited homodyne detection (or heterodyne detection) on mode B_1 and shares secret keys with Alice through classical data post-processing (i.e., parameter estimation, error correction, and privacy amplification).

Next, we derive the asymptotic key rate of the protocol under Gaussian collective attacks. Here, we use reverse reconciliation (RR) in data post-processing, which is more robust against channel attenuation compared to direct reconciliation [26]. In terms of the Csiszar–Korner theorem, the asymptotic key rate under RR is given by [31,33]

$$R_{\text{asy}}\left(\langle\tau\rangle,\langle\sqrt{\tau}\rangle,\bar{n}\right)=\beta I_{AB}-\chi_{BE},\tag{4}$$

where β denotes the reconciliation efficiency, I_{AB} is the Shannon mutual information between Alice and Bob, and χ_{BE} represents the Holevo bound. The values of I_{AB} and χ_{BE} can be derived from the covariance matrix in Equation (3). Therefore, we first need to know the values of $\langle\tau\rangle$, $\langle\sqrt{\tau}\rangle$, and $\bar{n}$. In our manuscript, we use the model in [23] to describe the PDT of satellite-mediated links, which takes the diffraction, atmospheric extinction, turbulence, and pointing errors into account. Moreover, $\bar{n}$ is considered to originate from background light, i.e., $\bar{n}=\eta_{\text{eff}}\bar{n}_B$, while the setup noises on both Alice's and Bob's side are ignored (see [29] for a discussion of setup noise). Once we determine $\langle\tau\rangle$, $\langle\sqrt{\tau}\rangle$, and $\bar{n}$, the derivation of I_{AB} and χ_{BE} can be found (refer to [22]). Note that our manuscript considers Eve's active attack on the channel to establish a lower bound on the secret key rate. However, the satellite-mediated link can be treated as a line-of-sight (LOS) link, as Eve would find it hard to tamper with the middle channel between the ground station and the moving satellite, and would likely only conduct passive attacks. The LOS security is discussed in [30], where it is shown that LOS scenarios can achieve higher secret key rates than cases involving active attacks.

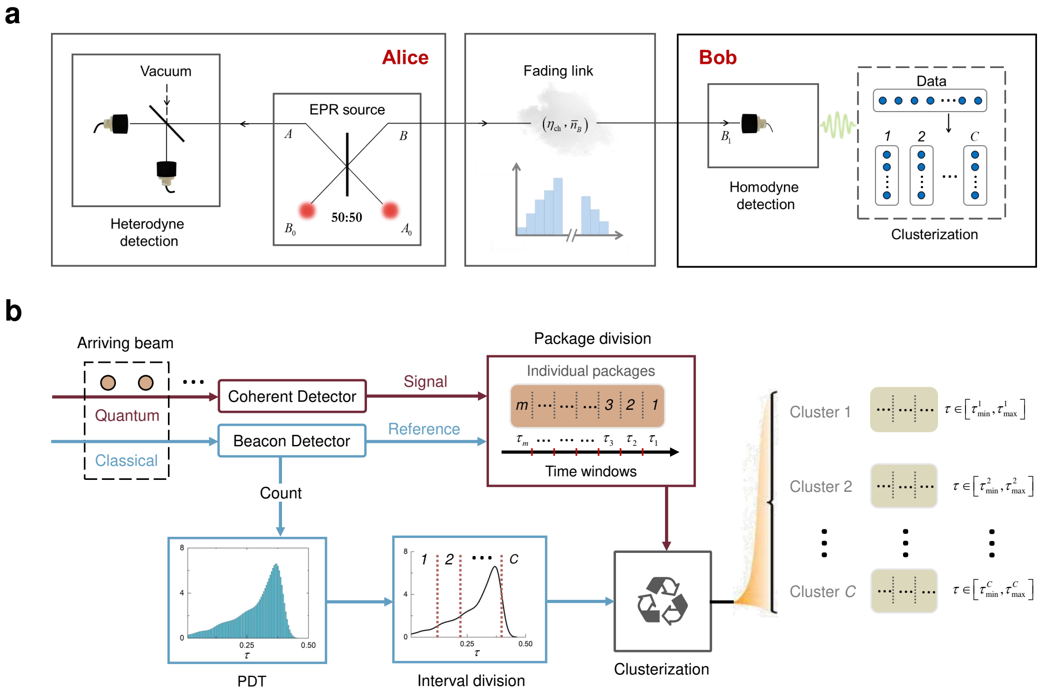
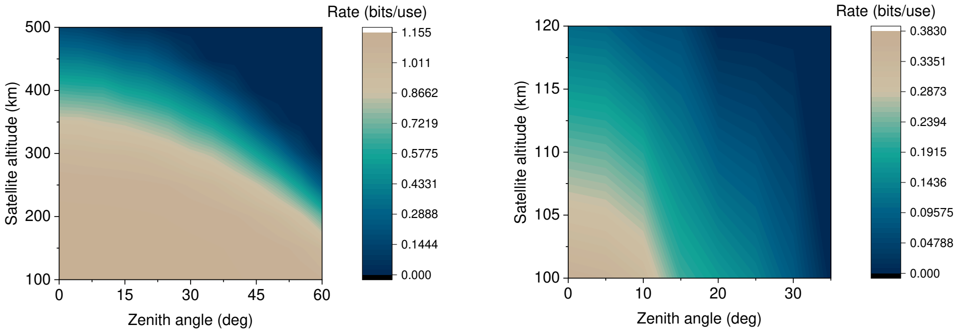


Figure 1. (**a**) EB scheme of GMCS protocol over a satellite-mediated (fading) link. Note that Bob can also use heterodyne detection instead of homodyne detection. (**b**) Demonstration of the clusterization method. EPR: Einstein–Podolsky–Rosen; PDT: probability distribution of transmittance; η_{ch}: channel transmittance; $\bar{n}_B$: mean number of background thermal photons; C: cluster number; τ: real-time transmittance including detector efficiency; $\tau^k_{\max}$ ($\tau^k_{\min}$): the upper (lower) bound of the k-th cluster, $k=1,\ldots,C$.

Figure 2 shows the asymptotic key rate, R_{asy}, of the GMCS protocol over the satellite-mediated links versus the satellite altitude h and the zenith angle θ. The simulation parameters are shown in Table 1. Here, we consider the nighttime situation with an atmospheric parameter of $A_0=1.7\times10^{-14}\ \text{m}^{-2/3}$ and a windspeed of $v=21\ \text{m/s}$, which is commonly known as the H-V$_{5/7}$ model. Moreover, $\bar{n}_{\text{B}}$ is set to 0.02 for both the downlink and uplink scenarios, as our focus is primarily on the effects caused by channel fading instead of background noise. In fact, the background noise shows a difference between the downlink and uplink scenarios due to variations in the source of background light [23]. We find that the downlink geometry is favorable for the CV-QKD task. This is because the optical beam in the downlink geometry starts to propagate in a vacuum until it enters the atmosphere, while the atmospheric influence appears in the early stages of beam transmission in the uplink geometry. Note that the layer around the Earth with a thickness of 20 km contains, on average, 95% of the total mass of the atmosphere [7]. Therefore, the downlink geometry is more favorable for optical signal transmission. However, the uplink geometry is important for a satellite-mediated network between ground stations because the ground station first generates the keys and needs to send them to a satellite via the uplink. In addition, the uplink geometry has the following advantages: the simple design of the satellite, variability of quantum light sources, and accessibility for maintenance or repair.



(a) (b)

Figure 2. The asymptotic key rate of the GMCS protocol over the satellite-mediated links versus satellite altitude and zenith angle: (**a**) downlink scenario, (**b**) uplink scenario.

Table 1. Physical parameters.

Physical Parameter	Notation	Value
Wavelength	λ	800 nm
Beam curvature	R_0	∞
Beam spot size	ω_0	0.4 m
Receiver aperture	a_R	1 m
Detector efficiency	η_{eff}	0.7
Atmospheric parameter [1]	A_0	1.7×10^{-14} m$^{-2/3}$
Windspeed	v	21 m/s
Mean number of background thermal photons	$\bar{n}_B$	0.02
Pointing error	σ_{p}^2	1 μrad
Sea-level value (λ = 800 nm)	α_0	5×10^{-6} m^{-1}
Modulation variance	σ_x^2	6
Reconciliation efficiency	β	0.98
Satellite altitude	h	100~500 km
Zenith angle	θ	0~60 deg
Detector shot-noise (homodyne)	v_{det}	1

[1] A_0 describes the relative strength of the turbulence near the ground level.

3. Improvement via Clusterization

In this section, we consider the clusterization method to improve the secret key rate of the satellite-mediated protocol by suppressing the fading noise. We first analyze the additional fading noise caused by transmittance fluctuation in both downlink and uplink scenarios. Then, a clusterization method is suggested to suppress the fading noise for improvement.

3.1. Fading Noise in Satellite-Mediated Protocol

From the form of Equation (3), γ_{AB_1} can be equivalently parameterized as originating from a stable link with fixed parameters, which can be rewritten as

$$\mathrm{V}_{AB_1} = \begin{bmatrix} \mu \mathrm{I} & \sqrt{\eta(\mu^2-1)}\mathrm{Z} \\ \sqrt{\eta(\mu^2-1)}\mathrm{Z} & [\eta(\mu-1)+2\bar{n}_{\mathrm{eff}}+1]\mathrm{I} \end{bmatrix}, \tag{5}$$

with effective transmittance

$$\eta = \langle\sqrt{\tau}\rangle^2, \tag{6}$$

and effective noise

$$\bar{n}_{\mathrm{eff}} = \frac{\langle\tau\rangle - \langle\sqrt{\tau}\rangle^2}{2}(\mu-1) + \bar{n}. \tag{7}$$

We find that the effect of transmittance fluctuation is the increase in thermal noise by the additional term

$$\bar{n}_{\mathrm{fad}} = \bar{n}_{\mathrm{eff}} - \bar{n} = \frac{\langle\tau\rangle - \langle\sqrt{\tau}\rangle^2}{2}(\mu-1). \tag{8}$$

It is clear that the fading thermal noise $\bar{n}_{\mathrm{fad}}$ is related to the statistics $\mathrm{Var}(\sqrt{\tau}) = \langle\tau\rangle - \langle\sqrt{\tau}\rangle^2$. Additionally, the fading noise will decrease if the signal variance μ is decreased.

Figure 3 shows the distribution of fading noise, $\bar{n}_{\mathrm{fad}}$, versus the satellite altitude h and the zenith angle θ. The simulation parameters are shown in Table 1. We find that the fading noise in the uplink is generally more significant than that in the downlink. A joint analysis of Figures 2 and 3 shows that the asymptotic key rate drops rapidly in the area where $\bar{n}_{\mathrm{fad}}$ is on the rise. Therefore, we consider improving the secret key rate by suppressing the fading noise in the following. Note that the uplink $\bar{n}_{\mathrm{fad}}$ in Figure 3b decreases in the area with higher satellite altitude and a larger zenith angle, where the atmospheric effects are more severe. This can be attributed to the further decrease in transmittance (near zero), leading to a more 'stable' channel.

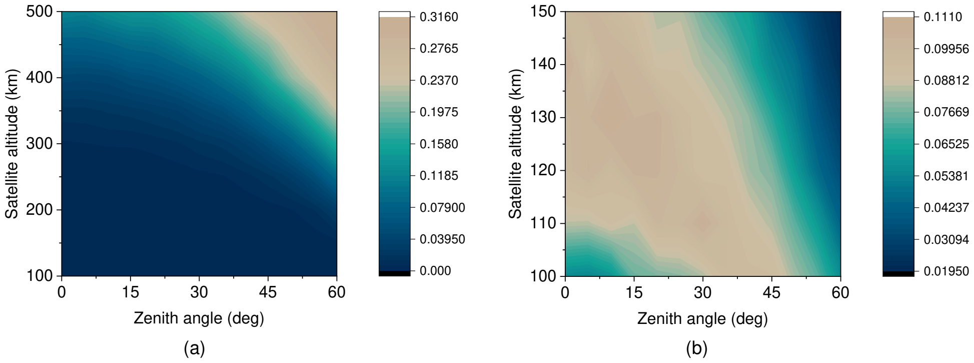


Figure 3. Distribution of fading noise versus the satellite altitude and zenith angle: (**a**) downlink scenario, (**b**) uplink scenario.

3.2. Suppressing Fading Noise via Clusterization

As mentioned above, the fading noise, $\bar{n}_{\mathrm{fad}}$, is related to the statistics $\mathrm{Var}(\sqrt{\tau})$. However, we cannot change the channel statistics but only the method of data post-processing. In a practical setting, the frequency of signal preparation and detection ν_s (reached GHz in a recent study [34]) is much higher than the fluctuation frequency of the atmospheric channel ν_f (usually $\sim$1 KHz [10]). In other words, for a small time window, each transmitted pulse can be considered as passing through a stable channel with constant transmittance. Therefore, we can divide the arrived N pulses into m individual packages based on time windows (i.e., each package has $n = N/m$ pulses), and each package has no transmittance fluctuation. In detail, as shown in Figure 1b, by detecting the intensity of the multiplexing beacon, we can monitor the real-time transmittance and the total PDT as the reference for package division [10,35]. Then, we calculate the secret key rate of each package individually and the final result is their average. Since there is no transmittance fluctuation in each package, the fading noise is zero.

However, there is a negative impact of the individual package scheme when considering composable finite-size effects [36]. In a practical setting, users do not know all the parameters of the protocol, so they need to use part of the measurement data for parameter estimation. The asymptotic key rate in Figure 2 assumes that users can use the quantum communication channel an infinite number of times, thus having enough measurement data for perfect parameter estimation. This is impossible in a practical setting, where users can only use the quantum channel a finite number of times. Here, we assume that Alice knows the signal modulation μ, while Bob monitors the quantum efficiency η_{eff}, thus only τ and $\bar{n}$ need to be estimated. In the composable finite-size regime, the secret key rate of an individual package can be expressed as [36]

$$R^i_{\text{com}} = \mathcal{P}_{\text{ec}} r \left[R_{\text{asy}}\left(\tau^i_{\text{min}}, \bar{n}_{\text{max}}\right) - \frac{\Delta_{\text{aep}}}{\sqrt{r \cdot n}} + \frac{\log_2\left(2\varepsilon^2_{\text{h}}\varepsilon_{\text{cor}}\right)}{r \cdot n} \right], \tag{9}$$

with the higher-order terms

$$\Delta_{\text{aep}} = 4\log_2\left(\sqrt{d} + 2\right)\sqrt{\log_2(2/\varepsilon^2_{\text{s}})}, \tag{10}$$

where $i = 1, \ldots, m$ is the label of an individual package, r is the proportion of measured data used for secret key generation, $\mathcal{P}_{\text{ec}}$ is the success probability of error correction, d is digitalization, ε_{h} is the hashing parameter, ε_{s} is the smoothing parameter, and ε_{cor} is the ε-correctness, which bounds the probability that Alice's and Bob's local strings are different after error correction and successful verification of their hashes. The estimated values τ^i_{min} and $\bar{n}^i_{\text{max}}$ are calculated using the maximum-likelihood estimators, which yield the results

$$\tau^i_{\text{min}} \simeq \tau^i - w\sqrt{\frac{2\tau^i + \tau^i(2\bar{n} + v_{\text{det}})/\sigma^2_x}{(1-r)n}}, \tag{11}$$

$$\bar{n}_{\text{max}} \simeq \bar{n} + w\frac{2\bar{n} + v_{\text{det}}}{\sqrt{2(1-r)n}}, \tag{12}$$

where $w = \sqrt{2}\text{erf}^{-1}(1 - 2\varepsilon_{\text{pe}})$ with the failing probability of parameter estimation ε_{pe} and inverse error function erf^{-1}, and the detector shot-noise $v_{\text{det}} = 1$ ($v_{\text{det}} = 2$) for homodyne (heterodyne) detectors. Finally, the total composable finite-size rate is the packages' average given by

$$R_{\text{com}} = \frac{1}{m}\sum_{i=1}^{m} R^i_{\text{com}}. \tag{13}$$

In our manuscript, we assume that ν_s =1 GHz and ν_f =1 KHz. During a run of 1 s, $N = 10^9$ pulses were transmitted between Alice and Bob, while the measurement data can be divided into $m = 1/\nu_f = 1000$ packages based on the time windows. Correspondingly, the size of each package is $n = 10^6$. For the individual package scheme, the measurement data for parameter estimation in each package ($r \cdot n < 10^6$) are significantly low, which introduces a composable finite-size effect.

Therefore, we consider the clusterization scheme to balance the trade-off between the fading noise and the composable finite-size effect. We divide all the individual packages into C groups (clusters), whereas the transmittance of the packages in the k-th cluster satisfies $\tau \in [\tau^k_{\text{min}}, \tau^k_{\text{max}}]$. Here, τ^k_{min} and τ^k_{max} are the upper and lower bounds of the k-th clusters, respectively. We determine the values of τ^k_{min} and τ^k_{max} according to the total PDT for an optimal division, where each group has an almost equal package number. Finally, we perform a security analysis for each cluster independently, and the final composable finite-size rate is their average, given by

$$R_{\text{com}} = \mathcal{P}_{\text{ec}} r \sum_{k=1}^{C} \mathcal{P}^k \left[R_{\text{asy}}\left(\eta^k_{\text{min}}, \bar{n}^k_{\text{max}}\right) - \frac{\Delta_{\text{aep}}}{\sqrt{r \cdot N/C}} + \frac{C \cdot \log_2\left(2\varepsilon_{\text{h}}^2 \varepsilon_{\text{cor}}\right)}{r \cdot N} \right], \tag{14}$$

where $\mathcal{P}^k$ denotes the probability of the package falling in the k-th cluster, and η^k_{min} and $\bar{n}^k_{\text{max}}$ are the estimators of effective parameters in the k-th cluster. In detail, the covariance matrix of the k-th cluster can be expressed as

$$\gamma^k_{AB_1} = \begin{bmatrix} \mu \mathrm{I} & \sqrt{\eta^k(\mu^2-1)}\mathrm{Z} \\ \sqrt{\eta^k(\mu^2-1)}\mathrm{Z} & \left[\eta^k(\mu-1) + 2\bar{n}^k_{\text{eff}} + 1\right]\mathrm{I} \end{bmatrix}, \tag{15}$$

with the effective parameters

$$\eta^k = \left[\int_{\tau^k_{\text{min}}}^{\tau^k_{\text{max}}} \sqrt{\tau} \mathcal{P}(\tau) d\tau \right]^2, \tag{16}$$

$$\bar{n}^k_{\text{eff}} = \frac{\int_{\tau^k_{\text{min}}}^{\tau^k_{\text{max}}} \tau P(\tau) d\tau - \eta^k}{2}(\mu - 1) + \bar{n}. \tag{17}$$

Note that each cluster retains fading noise, as the packages within each cluster have relatively similar but not identical transmittance. Fortunately, the optimal clusterization based on the total PDT can control the composable finite-size effects within a suitable range while reducing $\bar{n}_{\text{fad}}$. Moreover, the cluster number cannot be too large, as the case of $C = 1000$ is equivalent to the individual package scheme with a heavy composable finite-size effect. The optimal cluster number is discussed in the following section.

4. Security Analysis in Composable Finite-Size Regime

In this section, we perform a security analysis in the composable finite-size regime. In the satellite-mediated scenario, we need to consider the effect of the instantaneous zenith angle between the moving satellite and the ground station. For a 1 GHz system, it takes 1 s to collect 10^9 data, whereas the satellite has moved a certain distance during this time. Therefore, the total 10^9 data are transferred through multiple links with different zenith angles. This leads to a problem in the theoretical analysis, as it is difficult to provide a formula describing the irregular PDT related to the instantaneous zenith angle, or equivalently, the flight time of the satellite. Note that the transmittance data in the theoretical analysis are generated using the Monte Carlo method in terms of the PDT formula. However, it is not a problem in a practical setting since we can obtain the irregular PDT using the measurement data of the beacon light. For the sake of simplicity, we divide the satellite orbit into several intervals based on the flight time of the satellite while using the PDT at the end time of each interval to investigate the whole interval. Moreover, we only consider the flight area where the zenith angle increases from zero to maximum, so the simulation results of the rate represent the lower bound of each interval. In our manuscript, we divide the orbit into steps of 60 s, and the relationship between the flight time and the instantaneous zenith angle is shown in Appendix A.

4.1. Without Clusterization

We first perform a security analysis without clusterization, i.e., $C = 1$. Figure 4 shows the composable finite-size rate R_{com} with no clusterization versus the satellite altitude h and the zenith angle θ. The simulation parameters related to composable finite-size security are shown in Table 2. Here, we ignored the effect of the instantaneous zenith angle to show the gap between the composable finite-size rate and the asymptotic key rate through a joint analysis of Figures 2 and 4. The block size of each simulation point is set to $N = 10^7$.

Table 2. Parameters related to composable finite-size security.

Parameter	Notation	Value
Digitalization	d	2^5
Hashing parameter	ε_{h}	10^{-10}
Smoothing parameter	ε_{s}	10^{-10}
ε-correctness	$\varepsilon_{\mathrm{cor}}$	10^{-10}
Failing probability of PE [1]	$\varepsilon_{\mathrm{pe}}$	10^{-10}
EC [2] success probability	$\mathcal{P}_{\mathrm{ec}}$	0.9
Proportion of PE data	r	0.9
Frequency of signal preparation and detection	ν_s	1 GHz, 10 GHz
Frequency of channel fluctuation	ν_f	1 KHz
Total pulses (one minute)	N	$60 \cdot \nu_s$
Individual package number	m	$N/(\nu_s \cdot \nu_f)$
Pulses of an individual package	n	N/m
Cluster number	C	1~10

[1] PE denotes parameter estimation. [2] EC denotes error correction.

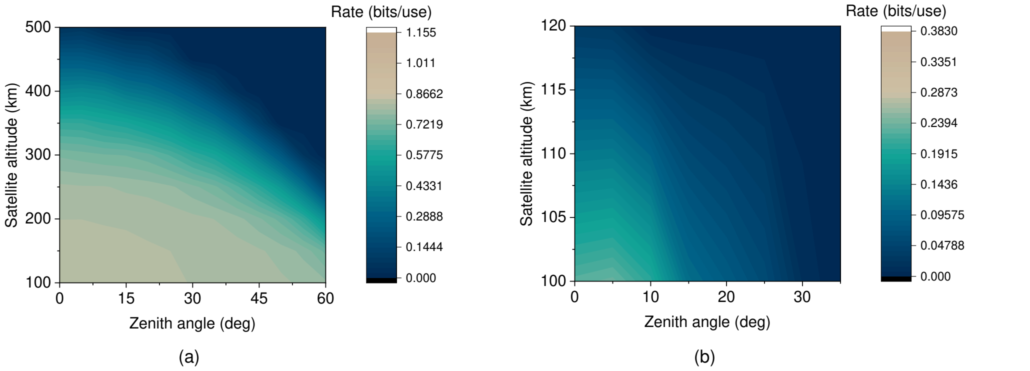
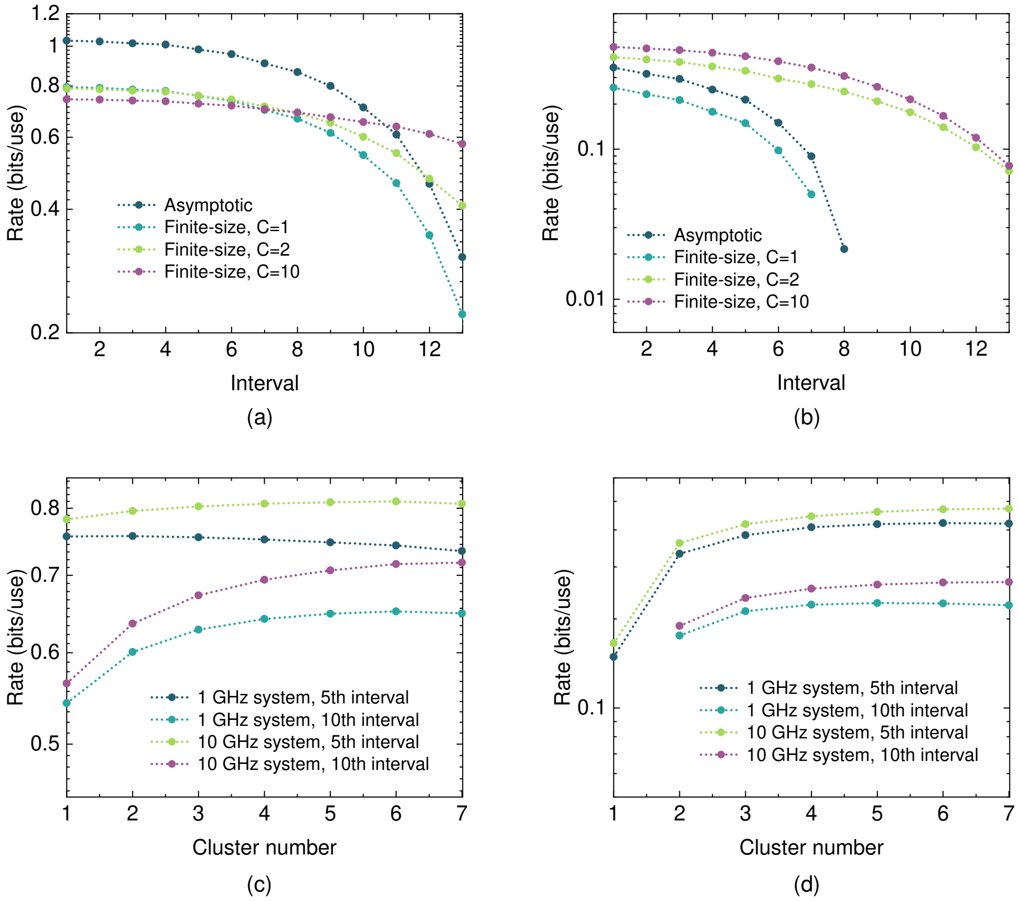


Figure 4. The composable finite-size rate with no clusterization versus the satellite altitude and zenith angle: (**a**) downlink scenario, (**b**) uplink scenario. The color bars are the same as those in Figure 2.

4.2. With Clusterization

In this subsection, we discuss the performance of the clusterization method. Figure 5 shows the composable finite-size rate R_{com} with clusterization versus the cluster number, C, and the intervals. The satellite altitudes of the downlink and uplink scenarios are 300 km and 100 km, respectively. Figure 5a shows the rate of the downlink scenario versus the interval with various cluster numbers. Here, we also provide the corresponding asymptotic key rate for comparison, where $C = 1$ denotes the case without clusterization. We find that the clusterization method can improve the composable finite-size rate after the seventh interval, even with only two clusters. Moreover, the composable finite-size rates of $C = 2$ and $C = 10$ surpass the asymptotic key rate after the 12th and 11th intervals, respectively. This is because a bigger interval number means a larger zenith angle and thus a higher $\bar{n}_{\mathrm{fad}}$ (see Table 3), while the proposed clusterization method can suppress it. In other words, more cluster numbers lead to less fading noise. However, having more cluster numbers means a more serious composable finite-size effect. Take $C = 10$ as an example: the clusterization method damages the rate before the sixth interval, where $\bar{n}_{\mathrm{fad}}$ is at a relatively low level. In these intervals, the added composable finite-size effect becomes the main effect, and the improvement caused by clusterization is overshadowed by this effect. When the fading noise is large enough, the rate of the clusterization method is consistently higher than that of no clusterization, as shown in Figure 5b and Table 3.



(a)

(b)

(c)

(d)

Figure 5. The composable finite-size rate with clusterization versus the cluster number and interval. (**a**,**c**) are downlink scenarios with a satellite altitude of $h = 300$ km, (**b**,**d**) are uplink scenarios with a satellite altitude of $h = 100$ km. The value of $\bar{n}_{\text{fad}}$ in each interval refers to the information in Table 3.

Table 3. The value of $\bar{n}_{\text{fad}}$ in each interval.

Downlink	$\bar{n}_{\textbf{fad}}$	Uplink	$\bar{n}_{\textbf{fad}}$
1st	0.0039	1st	0.0406
2nd	0.0042	2nd	0.0435
3rd	0.0047	3rd	0.0450
4th	0.0048	4th	0.0484
5th	0.0062	5th	0.0503
6th	0.0075	6th	0.0551
7th	0.0102	7th	0.0590
8th	0.0125	8th	0.0632
9th	0.0168	9th	0.0652
10th	0.0232	10th	0.0652
11th	0.0313	11th	0.0651
12th	0.0450	12th	0.0591
13th	0.0613	13th	0.0526

Figure 5c shows the downlink rate versus the cluster number at specific intervals. Here, we also provide the results of $\nu_s = 10$ GHz for comparison. In the 1 GHz case, we find that increasing the number of clusters reduces the rate in the fifth interval since its fading noise is relatively low. For the 10th interval, there is an optimal cluster number of $C_{\text{opt}} = 6$. Beyond this number, the increase in clusters cannot further improve performance since the composable finite-size effect increases. However, the results show a difference when ν_s increases from 1 GHz to 10 GHz. In the 10 GHz case, the composable finite-size effect is mitigated due to the total measurement data, or equivalently, the data for the parameter estimation of each interval, being increased. Correspondingly, increasing the cluster number improves the rate in the 10th interval, whereas the 5th interval has an optimal cluster number of $C_{\mathrm{opt}} = 6$. Figure 5d shows the uplink rate versus the cluster number. We find that the 10th interval cannot generate the secret key without the support of clusterization, even when ν_s =10 GHz.

5. Conclusions

We have proposed a clusterization method to suppress fading noise in the satellite-mediated GMCS protocol. In detail, the measurement data are divided into several clusters for separate security analysis, of which the data have relatively similar transmittance. The optimal upper and lower bounds of each cluster are based on the link's total PDT, whereas the optimal cluster number should balance the reduction in fading noise and increase the composable finite-size effect caused by the clusterization method. We found that the clusterization method can improve the composable finite-size rate when the fading noise is large enough, but may damage the performance by increasing the composable finite-size effect if the fading noise is at a relatively low level. Moreover, increasing the frequency of the signal preparation and detection of the system can suppress the composable finite-size effect, thereby allowing the proposed method to work effectively in a lower fading noise case.

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

Funding: This work was supported by the key research and development project in Hunan Province (Grant No. 2022GK2016), the Scientific Research Fund of Hunan Provincial Education Department (Grant No. 22C0446), Key project of Scientific Research of Hunan Provincial Education Department (Grant No. 21A0470 and 22A0669), and the Natural Science Foundation of Hunan Province (Grant No. 2023JJ50268 and 2023JJ50269).

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

Acknowledgments: We would like to thank Stefano Pirandola, Masoud Ghalaii, D. Vasylyev, Neda Hosseinidehaj, and Xinchao Ruan for their helpful discussions.

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

Appendix A

To divide the orbit into several flight intervals based on time windows, we first need to calculate the speed of a satellite. According to Newton's second law, the satellite speed v can be written as a function of the satellite altitude h, which is given by

$$v = \sqrt{\frac{G_0 M}{R_E + h}}, \tag{A1}$$

where G_0 is the universal gravitation, $M = 5.965 \times 10^{24}$ kg denotes the Earth's mass, and $R_E = 6371$ km represents the Earth's radius. Figure A1 shows the basic geometry for satellite-mediated quantum communications. Here, we only consider the right-hand side with the zenith angle $\theta \in [0, 60]$, whereas G is a sea-level ground station. The relationship between the flight distance and the instantaneous zenith angle is given by

$$D = \frac{\theta}{180}\pi(R_E + h). \tag{A2}$$

Then, we can obtain the relationship between the flight time and the instantaneous zenith angle as

$$t = \frac{\theta}{180} \frac{\pi(R_E + h)^{3/2}}{\sqrt{G_0 M}}. \tag{A3}$$

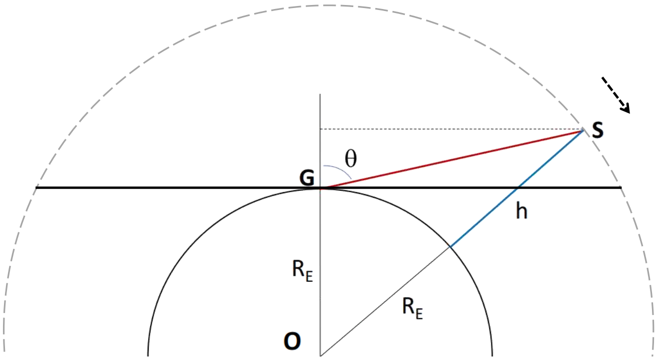


Figure A1. Basic geometry for satellite-mediated quantum communications. R_E: earth radius; G: ground station; S: quantum satellite; h: satellite altitude; O: Earth's center; θ: zenith angle.

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. Photonics* **2020**, *12*, 1012–1236.
2. Xu, F.; Ma, X.; Zhang, Q.; Lo, H.-K.; Pan, J.-W. Secure Quantum Key Distribution with Realistic Devices. *Rev. Mod. Phys.* **2020**, *92*, 025002. [CrossRef]
3. Wootters, W.K.; Zurek, W.H. A Single Quantum Cannot Be Cloned. *Nature* **1982**, *299*, 802–803. [CrossRef]
4. Briegel, H.-J.; Dür, W.; Cirac, J.I.; Zoller, P. Quantum Repeaters: The Role of Imperfect Local Operations in Quantum Communication. *Phys. Rev. Lett.* **1998**, *81*, 5932–5935. [CrossRef]
5. Liao, S.-K.; Cai, W.-Q.; Handsteiner, J.; Liu, B.; Yin, J.; Zhang, L.; Rauch, D.; Fink, M.; Ren, J.-G.; Liu, W.-Y.; et al. Satellite-Relayed Intercontinental Quantum Network. *Phys. Rev. Lett.* **2018**, *120*, 030501. [CrossRef] [PubMed]
6. Lu, C.-Y.; Cao, Y.; Peng, C.-Z.; Pan, J.-W. Micius Quantum Experiments in Space. *Rev. Mod. Phys.* **2022**, *94*, 035001. [CrossRef]
7. Liorni, C.; Kampermann, H.; Bruß, D. Satellite-Based Links for Quantum Key Distribution: Beam Effects and Weather Dependence. *New J. Phys.* **2019**, *21*, 093055. [CrossRef]
8. Lim, C.C.-W.; Xu, F.; Pan, J.-W.; Ekert, A. Security Analysis of Quantum Key Distribution with Small Block Length and Its Application to Quantum Space Communications. *Phys. Rev. Lett.* **2021**, *126*, 100501. [CrossRef]
9. Sidhu, J.S.; Joshi, S.K.; Gündoğan, 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**, *2*, 182–217. [CrossRef]
10. Dequal, D.; Trigo Vidarte, L.; Roman Rodriguez, V.; 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]
11. Zuo, Z.; Wang, Y.; Huang, D.; Guo, Y. Atmospheric Effects on Satellite-Mediated Continuous-Variable Quantum Key Distribution. *J. Phys. A: Math. Theor.* **2020**, *53*, 465302. [CrossRef]
12. Xu, S.; Li, Y.; Wang, Y.; Mao, Y.; Zuo, Z.; Ruan, X.; Guo, Y. Noiseless Attenuation for Continuous-Variable Quantum Key Distribution over Ground-Satellite Uplink. *Appl. Sci.* **2021**, *11*, 11289. [CrossRef]
13. Günthner, K.; Khan, I.; Elser, D.; Stiller, B.; Bayraktar, Ö.; Müller, C.R.; Saucke, K.; Tröndle, D.; Heine, F.; Seel, S.; et al. Quantum-Limited Measurements of Optical Signals from a Geostationary Satellite. *Optica* **2017**, *4*, 611. [CrossRef]
14. Pirandola, S. Limits and Security of Free-Space Quantum Communications. *Phys. Rev. Res.* **2021**, *3*, 013279. [CrossRef]
15. Zuo, Z.; Wang, Y.; Liao, Q.; Guo, Y. Overcoming the Uplink Limit of Satellite-Based Quantum Communication with Deterministic Quantum Teleportation. *Phys. Rev. A* **2021**, *104*, 022615. [CrossRef]
16. 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]
17. Wang, S.; Huang, P.; Wang, T.; Zeng, G. Feasibility of All-Day Quantum Communication with Coherent Detection. *Phys. Rev. Appl.* **2019**, *12*, 024041. [CrossRef]
18. Bruschi, D.E.; Ralph, T.C.; Fuentes, I.; Jennewein, T.; Razavi, M. Spacetime Effects on Satellite-Based Quantum Communications. *Phys. Rev. D* **2014**, *90*, 045041. [CrossRef]
19. Andersen, U.L.; Neergaard-Nielsen, J.S.; van Loock, P.; Furusawa, A. Hybrid Discrete- and Continuous-Variable Quantum Information. *Nat. Phys.* **2015**, *11*, 713–719. [CrossRef]
20. Zhang, Y.; Chen, Z.; Pirandola, S.; Wang, X.; Zhou, C.; Chu, B.; Zhao, Y.; Xu, B.; Yu, S.; Guo, H. Long-Distance Continuous-Variable Quantum Key Distribution over 202.81 Km of Fiber. *Phys. Rev. Lett.* **2020**, *125*, 010502. [CrossRef]

21. Bohmann, M.; Semenov, A.A.; Sperling, J.; Vogel, W. Gaussian Entanglement in the Turbulent Atmosphere. *Phys. Rev. A* **2016**, *94*, 010302. [CrossRef]
22. 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]
23. Pirandola, S. Satellite Quantum Communications: Fundamental Bounds and Practical Security. *Phys. Rev. Res.* **2021**, *3*, 023130. [CrossRef]
24. Ruppert, L.; Peuntinger, C.; Heim, B.; Günthner, K.; Usenko, V.C.; Elser, D.; Leuchs, G.; Filip, R.; Marquardt, C. Fading Channel Estimation for Free-Space Continuous-Variable Secure Quantum Communication. *New J. Phys.* **2019**, *21*, 123036. [CrossRef]
25. 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]
26. Grosshans, F.; Van Assche, G.; Wenger, J.; Brouri, R.; Cerf, N.J.; Grangier, P. Quantum Key Distribution Using Gaussian-Modulated Coherent States. *Nature* **2003**, *421*, 238–241. [CrossRef]
27. 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]
28. García-Patrón, R.; Cerf, N.J. Unconditional Optimality of Gaussian Attacks against Continuous-Variable Quantum Key Distribution. *Phys. Rev. Lett.* **2006**, *97*, 190503. [CrossRef]
29. Laudenbach, F.; Pacher, C.; Fung, C.-H.F.; Poppe, A.; Peev, M.; Schrenk, B.; Hentschel, M.; Walther, P.; Hübel, H. Continuous-Variable Quantum Key Distribution with Gaussian Modulation-The Theory of Practical Implementations. *Adv. Quantum Technol.* **2018**, *1*, 1800011. [CrossRef]
30. Pirandola, S. Composable Security for Continuous Variable Quantum Key Distribution: Trust Levels and Practical Key Rates in Wired and Wireless Networks. *Phys. Rev. Res.* **2021**, *3*, 043014. [CrossRef]
31. Weedbrook, C.; Pirandola, S.; García-Patrón, R.; Cerf, N.J.; Ralph, T.C.; Shapiro, J.H.; Lloyd, S. Gaussian Quantum Information. *Rev. Mod. Phys.* **2012**, *84*, 621–669. [CrossRef]
32. Vasylyev, D.; Semenov, A.A.; Vogel, W. Atmospheric Quantum Channels with Weak and Strong Turbulence. *Phys. Rev. Lett.* **2016**, *117*, 090501. [CrossRef]
33. Zuo, Z.; Wang, Y.; Mao, Y.; Ruan, X.; Guo, Y. Security of Quantum Communications in Oceanic Turbulence. *Phys. Rev. A* **2021**, *104*, 052613. [CrossRef]
34. Hajomer, A.A.E.; Bruynsteen, C.; Derkach, I.; Jain, N.; Bomhals, A.; Bastiaens, S.; Andersen, U.L.; Yin, X.; Gehring, T. Continuous-Variable Quantum Key Distribution at 10 GBaud Using an Integrated Photonic-Electronic Receiver. *arXiv* **2023**, arXiv:2305.19642.
35. Vallone, G.; Marangon, D.G.; Canale, M.; Savorgnan, I.; Bacco, D.; Barbieri, M.; Calimani, S.; Barbieri, C.; Laurenti, N.; Villoresi, P. Adaptive Real Time Selection for Quantum Key Distribution in Lossy and Turbulent Free-Space Channels. *Phys. Rev. A* **2015**, *91*, 042320. [CrossRef]
36. Pirandola, S.; Papanastasiou, P. Improved Composable Key Rates for CV-QKD. *arXiv* **2023**, arXiv:2301.10270.

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.