entropy

Article

Security Analysis of Continuous-Variable Measurement-Device-Independent Quantum Key Distribution Systems in Complex Communication Environments

Yi Zheng *, Haobin Shi, Wei Pan, Quantao Wang and Jiahui Mao

School of Computer Science, Northwestern Polytechnical University, Xi'an 710129, China; shihaobin@nwpu.edu.cn (H.S.); panweihh@163.com (W.P.); wqt@nwpu.mail.edu.cn (Q.W.); maojiahui@nwpu.mail.edu.cn (J.M.)

* Correspondence: yizheng@nwpu.edu.cn; Tel.: +86-029-8843-1517

Abstract: Continuous-variable measure-device-independent quantum key distribution (CV-MDI QKD) is proposed to remove all imperfections originating from detection. However, there are still some inevitable imperfections in a practical CV-MDI QKD system. For example, there is a fluctuating channel transmittance in the complex communication environments. Here we investigate the security of the system under the effects of the fluctuating channel transmittance, where the transmittance is regarded as a fixed value related to communication distance in theory. We first discuss the parameter estimation in fluctuating channel transmittance based on these establishing of channel models, which has an obvious deviation compared with the estimated parameters in the ideal case. Then, we show the evaluated results when the channel transmittance respectively obeys the two-point distribution and the uniform distribution. In particular, the two distributions can be easily realized under the manipulation of eavesdroppers. Finally, we analyze the secret key rate of the system when the channel transmittance obeys the above distributions. The simulation analysis indicates that a slight fluctuation of the channel transmittance may seriously reduce the performance of the system, especially in the extreme asymmetric case. Furthermore, the communication between Alice, Bob and Charlie may be immediately interrupted. Therefore, eavesdroppers can manipulate the channel transmittance to complete a denial-of-service attack in a practical CV-MDI QKD system. To resist this attack, the Gaussian post-selection method can be exploited to calibrate the parameter estimation to reduce the deterioration of performance of the system.

Keywords: continuous-variable; quantum key distribution; measure-device-independent; fluctuating channel transmittance; security analysis

check for updates

Citation: Zheng, Y.; Shi, H.; Pan, W.; Wang, Q.; Mao, J. Security Analysis of Continuous-Variable Measurement-Device-Independent Quantum Key Distribution Systems in Complex Communication Environments. *Entropy* **2022**, *24*, 127. https://doi.org/10.3390/e24010127

Academic Editors: Durdu Guney and David Petrosyan

Received: 24 December 2021
Accepted: 12 January 2022
Published: 14 January 2022

1. Introduction

Quantum key distribution (QKD) offers an unconditionally secure communication scheme to establish secret keys between the sender Alice and the receiver Bob through an insecure quantum channel in the presence of potential eavesdropper Eve, where the two remote partners are authenticated [1–5]. The security of the scheme is guaranteed by the basic laws of quantum mechanics [6–8]. At present, there are two kinds of QKD protocols: discrete-variable quantum key distribution (DVQKD) and continuous-variable quantum key distribution (CVQKD). In particular, CVQKD scheme based on the Gaussian-modulated coherent states (GMCS) can be well compatible with the classical optical communication systems, which has been fully proven to be secure against general attacks (e.g., the collective and coherent attacks) based on some ideal assumptions [8–12]. It has been experimentally implemented by many research groups in laboratories and in field environments [13–18]. In addition, the system has also been optimized by researchers from different aspects [19–25]. However, practical security problems seriously hinder the commercial development of CVQKD, where this obstacle is caused by the security loopholes opened by the gaps between the theoretical model and the practical system because the behavior of real devices typically deviates from that considered in the security proofs [26,27]. This problem also limits the application of DVQKD, which has been investigated by many researchers [28–30].

In a practical CVQKD system, Eve can exploit the above imperfections to successfully obtain secret key information without being detected, which is an effective quantum hacking strategy. For example, Eve can control the transmitted local oscillator (LO) to perform the LO fluctuation attack [31], LO calibration attack [32], and wavelength attack [33,34]. In addition, the imperfect linearity of homodyne detector can be exploited by Eve to launch saturation attack [35] and homodyne detector blinding attack [36]. Apart from this, laser damage attack against optical attenuator and laser seeding attack in light source have been proposed [37–42]. The security loopholes involved by these attacks can be closed by the corresponding countermeasures, which makes the system complicated. Moreover, there are some unknown attacks in practical CVQKD systems, which cannot be effectively resisted by the above schemes. Therefore, the researchers propose the continuous-variable measure-device-independent quantum key distribution (CV-MDI QKD) protocol to close all loopholes opened by imperfect detection [43–53]. In CV-MDI QKD, the measurement is performed by an untrusted third party, which is immune to all quantum hacking on detection. The research of CV-MDI QKD can promote the application of CVQKD.

According to the framework of CV-MDI QKD, the source and channel become the final battlefield between the authorized communication parties and Eve. Recently, the imperfections on source in practical CV-MDI QKD systems have been gradually researched [54–56]. In particular, the channel transmittance in theoretical model is considered to be a fixed value, which can be acquired based on the communication distance. However, practical communication environments are complex, which may result in the time-varying transmittance. In this work, we investigate the effects of the fluctuating channel transmittance for the security of practical CV-MDI QKD systems. Specifically, CV-MDI QKD in fluctuating channel transmittance is first described. Based on the model, we then show the difference of parameter estimation between this case and the stable channel case. To clearly quantify this difference, we discuss the specific parameter estimation when the channel transmittance respectively obeys the two-point distribution and the uniform distribution. Here, Eve can easily manipulate the channel to make the transmittance obey the above distributions. Subsequently, we analyze the secret key rate of the system based on the estimated parameter in different channel distributions. We observe that the fluctuating channel transmittance make the performance of the system deteriorated obviously, which may make communication interrupted. This impact is even greater in the extreme asymmetric case. These analyses indicate that the channel transmittance can be easily manipulated by Eve to launch a denial-service attack in a practical CV-MDI QKD system, which is different from the quantum hacking attack originating from security loopholes. Finally, the Gaussian post-selection technology can be exploited to calibrate the estimated parameters to prevent this attack.

The paper is organized as follows. In Section 2, parameter estimation in complex communication environments is shown for a practical CV-MDI QKD system, where these two theoretical channel models are established. Then, based on these models, we analyze the security of the system in the fluctuating channel transmittance when the channel transmittance respectively obeys the two-point distribution and the uniform distribution in Section 3. Finally, conclusions are presented in Section 4.

2. Channel Models and Parameter Estimation in Complex Communication Environments

Figure 1 shows the entanglement-based (EB) model of a GMCS CV-MDI-QKD protocol, which is fully equivalent to the standard prepare and measure (PM) model [45,46]. It is important to note that this equivalence is the core of security proofs for GMCS CVQKD protocols. In the EB model, one two-mode squeezed state with variance $V_A + 1(V_B + 1)$ is first prepared by Alice (Bob), where the mode $A_1(B_1)$ is measured by a heterodyne detector and the other mode $A_2(B_2)$ is sent to an unauthenticated third party, Charlie, through the quantum channel. The channel distance between Alice (Bob) and Charlie is $L_{AC}(L_{BC})$, and the total transmission distance L_{AB} should be $L_{AC}+L_{BC}$. Subsequently, Charlie interferes the received modes A' and B' at a beam splitter (BS) and obtains two output modes C and D. Then, two homodyne detectors are exploited by Charlie to measure the quadrature variable x_C of mode C and quadrature variable p_D of mode D, and the detection results x_C, p_D are immediately announced through a public channel. Finally, the mode B_1 is modified to B_1' by Bob through displacement operation $D(\beta)$. Here $\beta = g_m(x_C + ip_D)$, and g_m indicates the gain of the displacement operation. It is believed that the mode A_1 and B_1' become entangled after through these above steps. Therefore, Alice and Bob will share a group correlated vectors $X = \{(x_{A,i}, x_{B,i})|i = 1,2,...,N\}$ or $P = \{(p_{A,i}, p_{B,i})|i = 1,2,...,N\}$. These data can be used to estimate the channel transmittance $T_{AC}(T_{BC})$ and the excess noise $\varepsilon_{AC}(\varepsilon_{BC})$. In addition, key reconciliation and privacy amplification are exploited to further guarantee the security of the system.

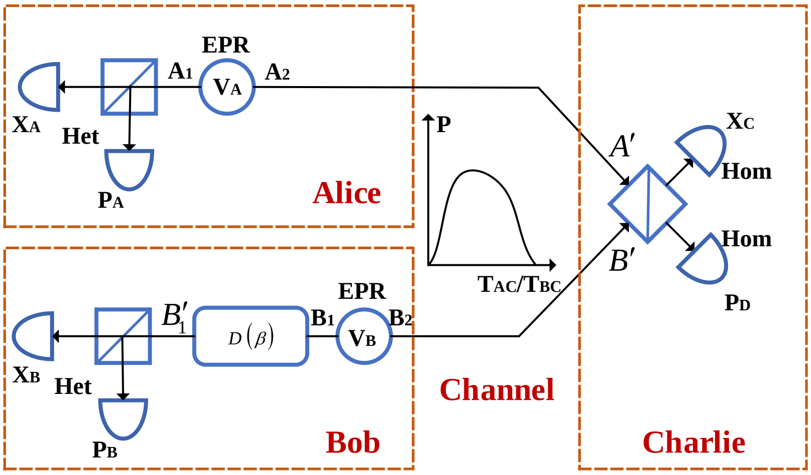

Figure 1. EB model of a practical GMCS CV-MDI-QKD system running in complex environments. Here, channel transmittance T_{AC} and T_{BC} are modeled to obey a certain distribution, which may be easily controlled by Eve.

According to the above analysis, there are two quantum channels in a practical CV-MDI-QKD system, i.e., C_{AC} and C_{BC}, which are assumed to be a normal linear model with the following relations:

$$\begin{aligned} x_{A'} &= t_{AC}x_A + z_{AC}, \\ p_{A'} &= t_{AC}p_A + z_{AC}, \\ x_{B'} &= t_{BC}x_B + z_{BC}, \\ p_{B'} &= t_{BC}p_B + z_{BC}, \end{aligned} \tag{1}$$

where $x_A(p_A)$, $x_{A'}(p_{A'})$, $x_B(p_B)$ and $x_{B'}(p_{B'})$ represent the corresponding quadrature variables of the mode A_2, A', B_2 and B', $t_{AC} = \sqrt{T_{AC}}$, $t_{BC} = \sqrt{T_{BC}}$, z_{AC} and z_{BC} indicate the total noises in the aforementioned quantum channels. Here, z_{AC} and z_{BC} respectively obey two centered normal distributions with variance $\sigma^2_{AC} = T_{AC}\xi_{AC} + N_0$ and $\sigma^2_{BC} = T_{BC}\xi_{BC} + N_0$, where $\xi_{AC} = \varepsilon_{AC}N_0$, $\xi_{BC} = \varepsilon_{BC}N_0$, and N_0 is the shot-noise variance. Therefore, t_{AC} and σ^2_{AC} can be calculated as

$$\begin{aligned} t_{AC} &= \frac{E(x_A x_{A'})}{E(x_A^2)}, \\ \sigma^2_{AC} &= E[(x_{A'} - t_{AC}x_A)^2]. \end{aligned} \tag{2}$$

It is no doubt that t_{AC} and σ^2_{AC} can also be acquired using p_A and $p_{A'}$. In addition, t_{BC} and σ^2_{BC} can be similarly calculated. In the following analysis, we only discuss the relevant calculation about channel C_{AC}. Based on the Eqs. (1) and (2), T_{AC} and ε_{AC} can be expressed by

$$\begin{aligned} T_{AC} &= t_{AC}^2 = [\frac{E(x_A x_{A'})}{E(x_A^2)}]^2, \\ \varepsilon_{AC} &= \frac{\sigma_{AC}^2 - N_0}{N_0 t_{AC}^2} \\ &= \frac{E[(x_{A'} - t_{AC} x_A)^2] - N_0}{N_0 T_{AC}}. \end{aligned} \tag{3}$$

In security proofs, the channel transmittance is assumed to be stable. Therefore, it is reasonably regarded as a fixed value related to transmission distance. However, practical communication environments are complex, which may result in a time-varying transmittance. In particular, the potential Eve may control the channel transmittance. To analyze the effects of the deviation, based on the phase space, x_A and x'_A can be written as

$$\begin{aligned} x_A &= |\alpha_A| \cos\theta_A, \\ x_{A'} &= \sqrt{T_{AC}}\{|\alpha_A| \cos(\theta_A + \Delta\varphi) + x_{\varepsilon_{AC}}\} + x_{N_0}, \end{aligned} \tag{4}$$

where $|\alpha_{\mathrm{A}}|$ is the amplitude of the coherent states prepared by Alice, θ_A is the phase of these states, $\Delta\varphi$ is the phase shift caused by complex channel environments. In particular, $x_{\varepsilon_{AC}}$ and x_{N_0} are the additional values of quadratures variable x_{A}, which are caused by the channel excess noise ε_{AC} and shot-noise N_0, respectively. We can further obtain

$$\begin{aligned} E(x_A x_{A'}) &= E(\sqrt{T_{AC}}|\alpha_{\mathrm{A}}|^2 \cos^2\theta_A) = E(\sqrt{T_{AC}})V_{x_A}, \\ E(x_A^2) &= E(|\alpha_{\mathrm{A}}|^2 \cos^2\theta_A) = V_{x_A}, \\ E(x_{A'}^2) &= V_{x_A} E(T_{AC}) + \xi_{AC} E(T_{AC}) + N_0, \end{aligned} \tag{5}$$

where $V_{x_A} = V_A N_0$, V_A is the modulation variance at Alice's side. It is important to note that T_{AC}, $|\alpha_A| \cos\theta_A$, N_0 and ξ_{AC} are totally independent. In addition, it is reasonable that $\Delta\varphi$ is approximated to zero in the above analyses, because the phase noise can be extremely constrained by the high-precision phase compensation technique. Eventually, based on Equations (3) and (5), the estimated channel parameters $\hat{T}_{AC}$ and $\hat{\varepsilon}_{AC}$ in fluctuating channel transmittance should satisfy

$$\begin{aligned} \hat{T}_{AC} &= [\frac{E(x_A x_{A'})}{E(x_A^2)}]^2 = [E(\sqrt{T_{AC}})]^2, \\ \hat{\varepsilon}_{AC} &= \frac{V_{\mathrm{A}} E(T_{AC}) + \varepsilon_{AC} E(T_{AC}) - V_{\mathrm{A}}[E(\sqrt{T_{AC}})]^2}{[E(\sqrt{T_{AC}})]^2}. \end{aligned} \tag{6}$$

Similarly, the estimated channel parameters $\hat{T}_{BC}$ and $\hat{\varepsilon}_{BC}$ in fluctuating channel transmittance also obey the above relations. There are some clear deviations between the estimated channel parameters in fluctuating channel transmittance and ideal values, which is closely related to the distribution of the fluctuating channel transmittance. Therefore, we need to quantify the distribution to analyze the effects of the fluctuating channel transmittance. However, the channel transmittance may irregularly change, which cannot be described using a specific formula. In particular, Eve may actively control the channel to disturb the transmittance. According to Ref. [57], the channel transmittance may be easily manipulated by Eve to obey the two-point distribution or the uniform distribution. Then, we discuss the estimated channel parameters when the channel transmittance obeys the two distributions.

Figure 2 describes the probability density function when the channel transmittance obeys the two-point distribution, where the channel transmittance can vary between 0 and

T_0 under the control of Eve. Therefore, $T_{AC}/T_0 \sim (1, P)$, where $T_0 = 10^{-0.02L_{AC}}$ represents the ideal channel transmittance and L_{AC} is the transmission distance between Alice and Charlie. Correspondingly, we can obtain $E(T_{AC}) = PT_0$, $E(\sqrt{T_{AC}}) = P\sqrt{T_0}$. Eventually, based on Equation (6), the channel parameters can be evaluated as

$$\hat{T}_{AC,1} = P^2 T_0, \hat{\varepsilon}_{AC,1} = \frac{1}{P}V_A - V_A + \frac{1}{P}\varepsilon_{AC}, \tag{7}$$

where P is the probability when the channel transmittance T_{AC} equals to T_0, ε_{AC} is the true channel excess noise, the number 1 indicates the two-point distribution. It is no doubt that the estimated channel parameters $\hat{T}_{BC,1}$ and $\hat{\varepsilon}_{BC,1}$ also satisfy Equation (7).

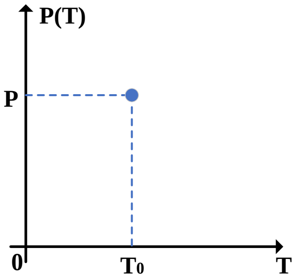

Figure 2. The probability density function of the channel transmittance when it obeys the two-point distribution, where T represents T_{AC} or T_{BC}.

Figure 3 shows the probability density function of the channel transmittance when it obeys the uniform distribution. Here, T_{AC} is a uniform distributed random number between $gT_0 (0 < g < 1)$ and T_0, i.e., $T_{AC} \sim U(gT_0, T_0)$, where T_0 also represents the ideal channel transmittance. Therefore, $E(T_{AC})$ and $E(\sqrt{T_{AC}})$ can be calculated as

$$\begin{aligned} E(T_{AC}) &= \int_{gT_0}^{T_0} \frac{1}{T_0 - gT_0} T_{AC} dT_{AC} \\ &= \frac{(1+g)T_0}{2}, \\ E(\sqrt{T_{AC}}) &= \int_{gT_0}^{T_0} \frac{1}{T_0 - gT_0} \sqrt{T_{AC}} dT_{AC} \\ &= \frac{2(1-g^{\frac{3}{2}})\sqrt{T_0}}{3(1-g)}. \end{aligned} \tag{8}$$

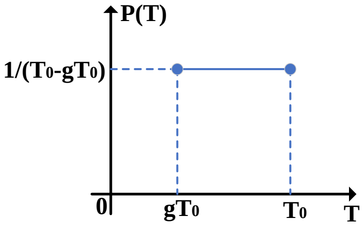

Figure 3. The probability density function of the channel transmittance when it obeys the uniform distribution, where T represents T_{AC} or T_{BC}.

According to Equations (6) and (8), the estimated values of the channel parameters can be expressed as

$$\begin{aligned} \hat{T}_{AC,2} &= \frac{4(1-g^{\frac{3}{2}})^2 T_0}{9(1-g)^2}, \\ \hat{\varepsilon}_{AC,2} &= \\ &\frac{(1-9g+16g^{\frac{3}{2}}-9g^2+g^3)V_A+9(1-g-g^2+g^3)\varepsilon_{AC}}{8(1-g^{\frac{3}{2}})^2}, \end{aligned} \tag{9}$$

where ε_{AC} also represents the true excess noise, the number 2 indicates the uniform distribution. Similarly, $\hat{T}_{BC,2}$ and $\hat{\varepsilon}_{BC,2}$ also obey Equation (9). In the following analysis, the two-point and uniform distributions are considered to be common channel distribution models to investigate the effects of the fluctuating channel transmittance.

In addition, fiber dispersion and imperfect polarization compensation in a practical system may affect the accuracy of measurement, which makes the estimated channel parameters deviate from the practical values. Therefore, these imperfections can indirectly lead to the fluctuation of the channel transmittance. Here, this variation may be not regular, which is difficulty expressed by a mathematical formula. However, according to the above analysis, Eve may actively control channel to disturb the communication environments. She can easily manipulate the channel to make it obeys the above distributions. To facilitate security analysis, the two-point distribution and the uniform distribution can be considered to be common channel distribution models, which does not affect our conclusion.

3. Security Analysis

Secret key rate is a key parameter for the security and performance of a practical CV-MDI-QKD system. Here, we focus on the secret key rate of the system under one-mode collective Gaussian attack, where reverse reconciliation is performed by Bob. It is important to note that the one-mode attack is not the optimal strategy. At present, the two-mode attack has been proven to be optimal. To be specific, the correlated two-mode coherent Gaussian attack are performed on two quantum channels, where the interactions of the two channels are used by Eve. However, in practical CV-MDI-QKD systems, the above correlation can become very weak when these channels come from different directions. Therefore, to facilitate analysis, the quantum channels of CV-MDI-QKD can be reduced to one-mode channel, where the one-mode attack can be efficiently performed. In particular, this simplification does not affect the results of the analysis of this article.

According to Ref. [45],the CV-MDI-QKD protocols are equivalent to the one-way CVQKD schemes using coherent states and heterodyne detection when the EPR states prepared by Bob and the displacement operation are assumed to be untrusted, which indicates that the calculation of the secret key rate of CV-MDI-QKD is the same with the standard one-way GMCS CVQKD. In the following analysis, the heterodyne detection is assumed to be perfect, and the finite-size effect is not considered. First, the Shannon mutual information between Alice and Bob can be calculated as [45,46,48]

$$\begin{aligned} I_{AB}^{het} &= 2 \times \frac{1}{2} \log_2 \frac{V_{B_m}^{het}}{V_{B_m|A_m}^{het}} \\ &= \log_2 \frac{T_m(V_A+1+\chi_{\text{line},m})+1}{T_m(1+\chi_{\text{line},m})+1}, \end{aligned} \tag{10}$$

where

$$\begin{aligned}V_{A_m}^{het} &= V_A/2+1,\\ V_{B_m}^{het} &= [T_m(V_A+1+\chi_{\text{line},m})+1]/2,\\ V_{B_m|A_m}^{het} &= V_{B_m}^{het} - \frac{T_m[(V_A+1)^2-1]}{V_{A_m}^{het}}\\ &= [T_m(1+\chi_{\text{line},m})+1]/2,\\ \chi_{\text{line},m} &= 1/T_m - 1 + \varepsilon_m.\end{aligned} \tag{11}$$

Then, the covariance matrix Γ_{AB}^m between Alice and Bob can be written as

$$\Gamma_{AB}^m = \begin{bmatrix} a\mathbb{I} & b\sigma_Z \\ b\sigma_Z & c\mathbb{I} \end{bmatrix}, \tag{12}$$

where

$$\begin{aligned}a &= V_A+1,\\ b &= \sqrt{T_m[(V_A+1)^2-1]},\\ c &= T_mV_A+1+T_m\varepsilon_m.\end{aligned} \tag{13}$$

Here,

$$\begin{aligned}T_m =&\frac{T_{AC}}{2}k^2,\\ \varepsilon_m =&1+\frac{1}{T_{AC}}[2+T_{BC}(\varepsilon_{BC}-2)+T_{AC}(\varepsilon_{BC}-1)]\\ &+\frac{1}{T_{AC}}\left(\frac{\sqrt{2}}{k}\sqrt{V_B}-\sqrt{T_{BC}}\sqrt{V_B+2}\right)^2.\end{aligned} \tag{14}$$

In particular, $k=\sqrt{\frac{2V_B}{T_{BC}(V_B+2)}}$ is adopted to minimize ε_m. Based on this condition, we can obtain

$$\begin{aligned}T_m &= \frac{T_{AC}V_B}{T_{BC}(V_B+2)},\\ \varepsilon_m &= \frac{T_{BC}}{T_{AC}}(\varepsilon_{BC}-2)+\varepsilon_{AC}+\frac{2}{T_{AC}}.\end{aligned} \tag{15}$$

In the following simulation analysis, these above channel parameters should be replaced by the estimated values in Equations (7) or (9). Then, the Holevo bound can be calculated as

$$\chi_{BE} = G(\frac{\lambda_{m,1}-1}{2})+G(\frac{\lambda_{m,2}-1}{2})-G(\frac{\lambda_{m,3}-1}{2}). \tag{16}$$

Here,

$$\begin{aligned}\lambda_{m,1,2}^2 &= \frac{1}{2}(A_m \pm \sqrt{A_m^2-4B_m}),\\ \lambda_{m,3} &= \frac{(T_m\varepsilon_m+2)(V_A+1)-T_mV_A}{T_m(\varepsilon_m+V_A)+2},\end{aligned} \tag{17}$$

where

$$\begin{aligned}A_m =&(V_A+1)^2-2T_m(V_A^2+2V_A)+(T_mV_A\\ &+T_m\varepsilon_m+1)^2,\\ B_m =&[(T_m\varepsilon_m+1)(V_A+1)-T_mV_A]^2.\end{aligned} \tag{18}$$

Finally, the secret key rate of the system can be acquired as

$$K_m = \beta I_{AB}^{het} - \chi_{BE}. \tag{19}$$

Based on Equations (7), (9)–(11) and (15)–(19), the secret key rate of a CV-MDI-QKD system can be analyzed when the channel transmittance obeys the two-point distribution or the uniform distribution.

Figure 4 describes the secret key rate versus transmission distance in the symmetric case when the channel transmittance obeys the two-point distribution. Here, the fixed parameters for the simulation are set as $\beta = 0.95$, $V_A = V_B = 40$, and $\varepsilon_{AC} = \varepsilon_{BC} = 0.05$. The simulation results show that the fluctuating channel make the performance of the system dramatically, where $P = 1$ represents the ideal case. It is important to note that even though the secure transmission distance is limited compared with a standard one-way CVQKD system, the demand of high-efficiency homodyne detection is removed.

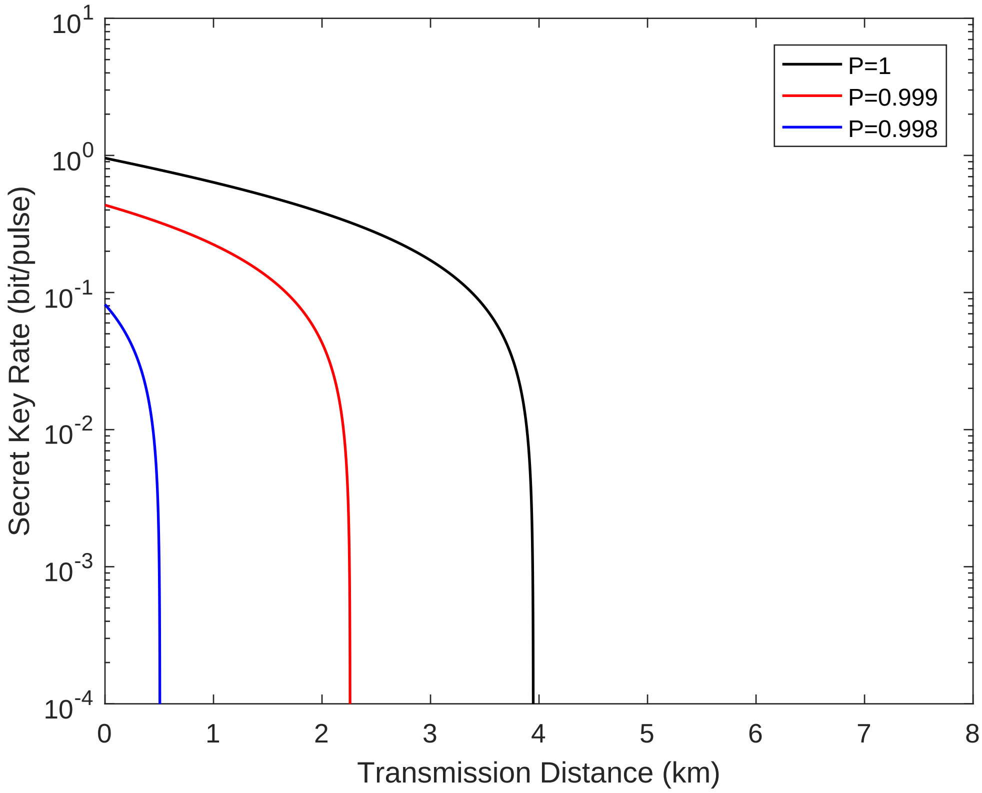

Figure 4. Secret key rate as a function of the transmission distance from Alice to Bob in the symmetric case when the channel transmittance obeys the two-point distribution, where $L_{AC} = L_{BC}$. The fiber loss is 0.2 dB/km.

Figure 5 reveals the secret key rate of the system as a function of the transmission distance from Alice to Bob in the extreme asymmetric case when the channel transmittance obeys the two-point distribution. The fixed parameters for simulation are the same as the symmetric case. It is obvious that the performance of the system also deteriorate under the effects of the fluctuating channel transmittance. In particular, the deterioration in the extreme asymmetric case is even worse than the symmetric case.

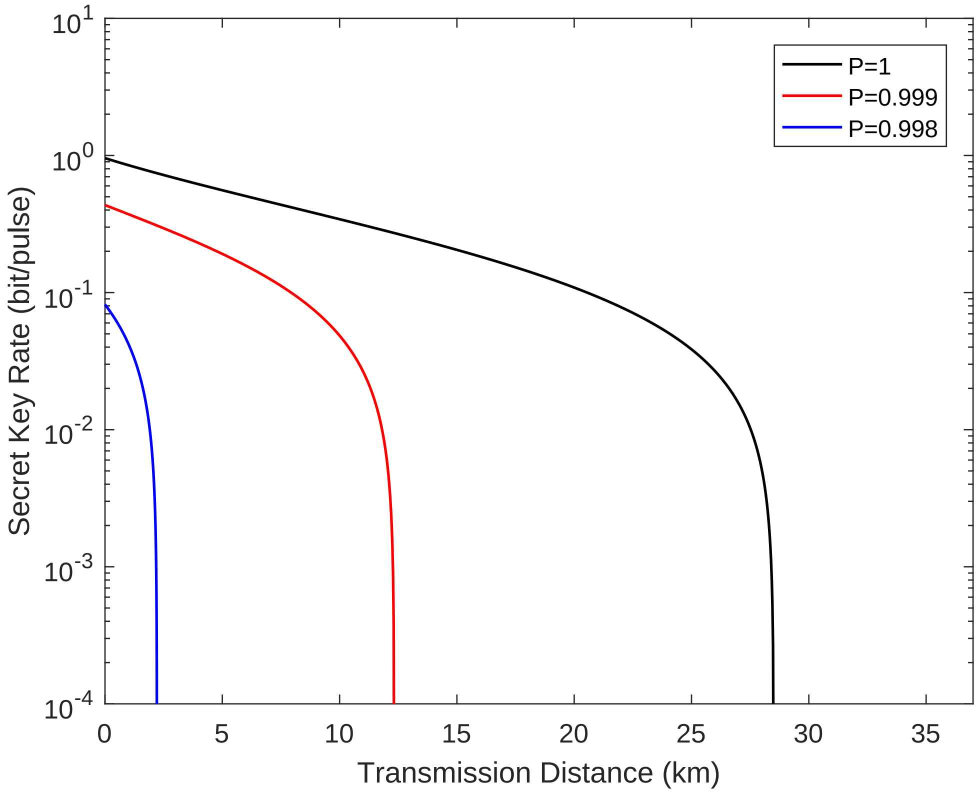

Figure 5. Secret key rate vs the transmission distance from Alice to Bob in the extreme asymmetric case when the channel transmittance obeys the two-point distribution, where $L_{BC} = 0$.

Figure 6 shows the secret key rate of the system versus transmission distance in the symmetric case when the channel transmittance obeys the uniform distribution, where g reflects the degree of channel jitter. Here, the fixed simulation parameters remain unchanged. We observe that the deterioration of the performance of the system increases with the degree of channel jitter.

Figure 7 depicts the secret key rate of the system as a function of the transmission distance from Alice to Bob in the extreme asymmetric case when the channel transmittance obeys the uniform distribution. The fixed parameters for simulation analysis also remain unchanged. It is clear that the dynamic trend of the performance of the system is consistent with the results shown in Figure 5.

These above simulation analyses indicate that the fluctuating channel transmittance may introduce an extra excess noise that can seriously deteriorate the performance of the practical CV-MDI-QKD systems. Correspondingly, the communication service between Alice, Bob and Charlie may be interrupted. Therefore, in a practical CV-MDI QKD systems, the potential Eve can launch a denial-service attack by manipulating the channel transmittance. To resist this attack, the Gaussian post-selection technology can be used to effectively improve the performance of the system. Specifically, Charlie first judge whether the $x_{A'}$ and $x_{B'}$ meet the Gaussian distribution. If the channel transmittance is manipulated, the normal linear model of the channel is destroyed. Therefore, Charlie can then extract a set of (almost) Gaussian-distributed data among the raw measurement data to calibrate the estimated values of these channel parameters to improve the performance of the system [35,57]. For example, if the channel transmittance obeys the two-point distribution, Charlie can first filter out the data when the transmittance is zero, and then complete parameter estimation. If the channel transmittance obeys the uniform distribution, Charlie can extract a set of Gaussian-distributed data when the transmittance is the low bound gT_0 to complete parameter estimation [57].

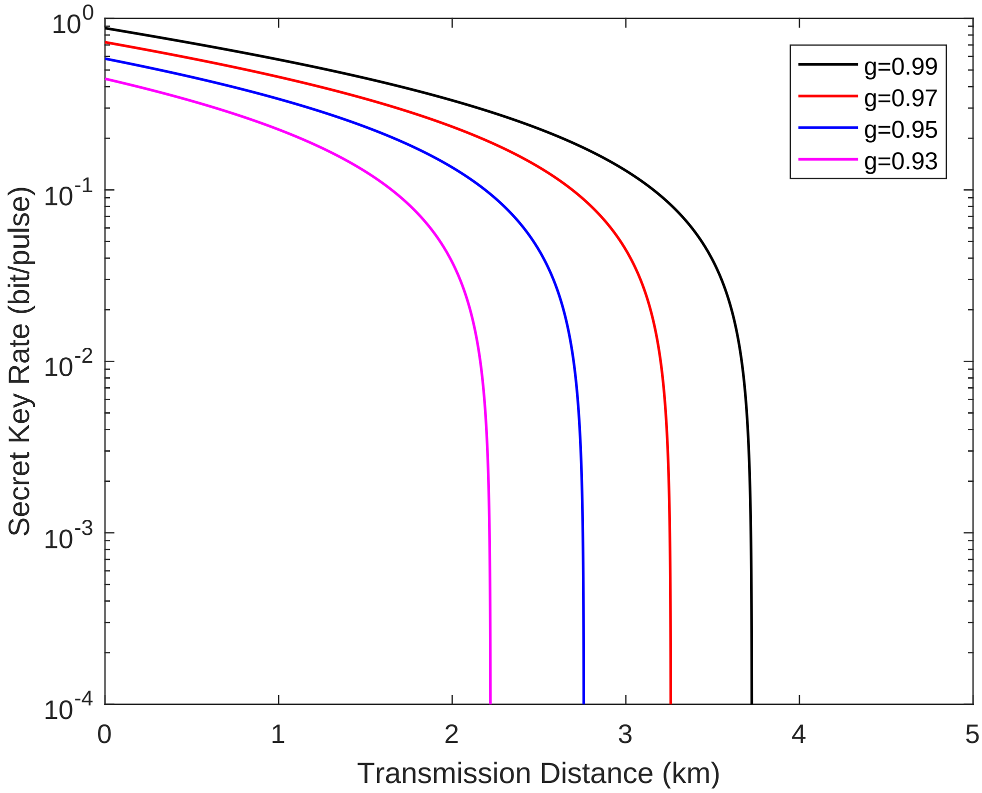

Figure 6. Secret key rate as a function of the transmission distance from Alice to Bob in the symmetric case when the channel transmittance obeys the uniform distribution, where $L_{AC} = L_{BC}$.

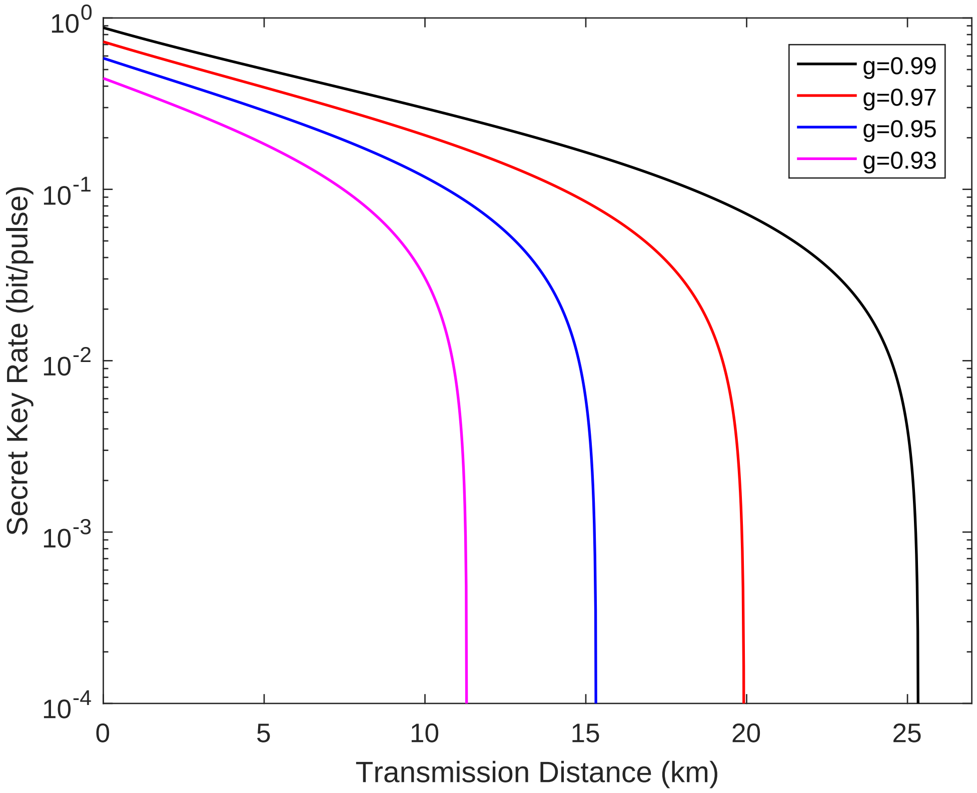

Figure 7. Secret key rate vs the transmission distance from Alice to Bob in the extreme asymmetric case when the channel transmittance obeys the uniform distribution, where $L_{BC} = 0$.

4. Conclusions

We have investigated the security of a practical CV-MDI-QKD system under the effects of the fluctuating channel transmittance caused by complex communication environments. We first model the fluctuating channel transmittance based on the EB scheme, and revel the deviation of parameter estimation between the fluctuating channel case and the ideal case. Furthermore, we show the parameter estimation when the channel transmittance respectively obey the two-point distribution and the uniform distribution. Based on the estimated parameters, we analyze the practical performance of the system. We observe that there is an obvious decline for the performance of the system under the impact of the fluctuating channel transmittance, especially in the extreme asymmetric case. The simulation results indicate that the fluctuating channel transmittance can produce an extra excess noise to deteriorate the system performance, which may interrupt the communication service between Alice, Bob and Charlie. This impact is more profound in the extreme asymmetric case. Therefore, a denial-service attack can be launched by Eve through manipulating the channel transmittance. To prevent this attack, the Gaussian post-selection technology is exploited to improve the performance of the system.

Author Contributions: Y.Z. designed the conception of the study, accomplished the formula derivation and numerical simulations, and drafted the article. H.S. gave the general idea of the study, checked the draft and provided feasible suggestions and critical revision of the manuscript. W.P. reviewed relevant studies and literature, conceived of and designed the study and performed critical revision of the manuscript. Q.W. conceived of the study and reviewed relevant studies. J.M. gave feasible advice and helped with the calculation. All authors have read and agreed to the published version of the manuscript.

Funding: This research was funded by National Natural Science Foundation of China (Grants No. 61976178, 62076202), and Fundamental Research Funds for the Central Universities (Grants No. D5000210764).

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Not applicable.

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

References

1. Ekert, A.K. Quantum cryptography based on Bell's theorem. *Phys. Rev. Lett.* **1991**, *67*, 661. [CrossRef]
2. Gisin, N.; Ribordy, G.; Tittel, W.; Zbinden, H. Quantum cryptography. *Rev. Mod. Phys.* **2002**, *74*, 145–195. [CrossRef]
3. 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]
4. Takesue, H.; Nam, S.W.; Zhang, Q.; Hadfield, R.H.; Honjo, T.; Tamaki, K.; Yamamoto, Y. Quantum key distribution over a 40-dB channel loss using superconducting single-photon detectors. *Nat. Photon.* **2007**, *1*, 343–348. [CrossRef]
5. 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] [PubMed]
6. Shor, P.W.; Preskill, J. Simple proof of security of the BB84 quantum key distribution protocol. *Phys. Rev. Lett.* **2000**, *85*, 441. [CrossRef] [PubMed]
7. Lo, H.K.; Chau, H.F. Unconditional Security of Quantum Key Distribution over Arbitrarily Long Distances. *Science* **1999**, *283*, 2050–2056. [CrossRef] [PubMed]
8. Grosshans, F.; Cerf, N.J. Continuous-variable quantum cryptography is secure against non-Gaussian attacks. *Phys. Rev. Lett.* **2004**, *92*, 047905. [CrossRef]
9. Navascués, M.; Grosshans, F.; Acin, A. Optimality of Gaussian attacks in continuous-variable quantum cryptography. *Phys. Rev. Lett.* **2006**, *97*, 190502. [CrossRef] [PubMed]
10. Garcia-Patron, R.; Cerf, N.J. Unconditional optimality of Gaussian attacks against continuous-variable quantum key distribution. *Phys. Rev. Lett.* **2006**, *97*, 190503. [CrossRef]
11. Leverrier, A.; García-Patrón, R.; Renner, R.; Cerf, N.J. Security of continuous-variable quantum key distribution against general attacks. *Phys. Rev. Lett.* **2013**, *110*, 030502. [CrossRef] [PubMed]
12. Leverrier, A. Composable security proof for continuous-variable quantum key distribution with coherent states. *Phys. Rev. Lett.* **2015**, *114*, 070501. [CrossRef]

13. Qi, B.; Huang, L.L.; Qian, L.; Lo, H.K. Experimental study on the Gaussian-modulated coherent-state quantum key distribution over standard telecommunication fibers. *Phys. Rev. A* **2007**, *76*, 052323. [CrossRef]
14. Fossier, S.; Diamanti, E.; Debuisschert, T.; Villing, A.; Tualle-Brouri, R.; Grangier, P. Field test of a continuous-variable quantum key distribution prototype. *New J. Phys.* **2009**, *11*, 045023. [CrossRef]
15. Jouguet, P.; Kunz-Jacques, S.; Leverrier, A.; Grangier, P.; Diamanti, E. Experimental demonstration of long-distance continuous-variable quantum key distribution. *Nat. Photon.* **2013**, *7*, 378–381. [CrossRef]
16. Huang, D.; Huang, P.; Li, H.; Wang, T.; Zhou, Y.; Zeng, G. Field demonstration of a continuous-variable quantum key distribution network. *Opt. Lett.* **2016**, *41*, 3511–3514. [CrossRef] [PubMed]
17. Zhang, Y.; Li, Z.; Chen, Z.; Weedbrook, C.; Zhao, Y.; Wang, X.; Huang, Y.; Xu, C.; Zhang, X.; Wang, Z.; others. Continuous-variable QKD over 50 km commercial fiber. *Quantum Sci. Technol.* **2019**, *4*, 035006. [CrossRef]
18. 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 fiber. *Phys. Rev. Lett.* **2020**, *125*, 010502. [CrossRef]
19. DiMario, M.; Kunz, L.; Banaszek, K.; Becerra, F. Optimized communication strategies with binary coherent states over phase noise channels. *NPJ Quantum Info.* **2019**, *5*, 65. [CrossRef]
20. Sabuncu, M.; Filip, R.; Leuchs, G.; Andersen, U.L. Environment-assisted quantum-information correction for continuous variables. *Phys. Rev. A* **2010**, *81*, 012325. [CrossRef]
21. Sabuncu, M.; Mišta, L., Jr.; Fiurášek, J.; Filip, R.; Leuchs, G.; Andersen, U.L. Nonunity gain minimal-disturbance measurement. *Phys. Rev. A* **2007**, *76*, 032309. [CrossRef]
22. Lassen, M.; Sabuncu, M.; Huck, A.; Niset, J.; Leuchs, G.; Cerf, N.J.; Andersen, U.L. Quantum optical coherence can survive photon losses using a continuous-variable quantum erasure-correcting code. *Nat. Photon.* **2010**, *4*, 700–705. [CrossRef]
23. Lassen, M.; Madsen, L.S.; Sabuncu, M.; Filip, R.; Andersen, U.L. Experimental demonstration of squeezed-state quantum averaging. *Phys. Rev. A* **2010**, *82*, 021801. [CrossRef]
24. Huang, P.; He, G.; Fang, J.; Zeng, G. Performance improvement of continuous-variable quantum key distribution via photon subtraction. *Phys. Rev. A* **2013**, *87*, 012317. [CrossRef]
25. Blandino, R.; Leverrier, A.; Barbieri, M.; Etesse, J.; Grangier, P.; Tualle-Brouri, R. Improving the maximum transmission distance of continuous-variable quantum key distribution using a noiseless amplifier. *Phys. Rev. A* **2012**, *86*, 012327. [CrossRef]
26. Jouguet, P.; Kunz-Jacques, S.; Diamanti, E.; Leverrier, A. Analysis of imperfections in practical continuous-variable quantum key distribution. *Phys. Rev. A* **2012**, *86*, 032309. [CrossRef]
27. 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]
28. Fei, Y.Y.; Meng, X.D.; Gao, M.; Wang, H.; Ma, Z. Quantum man-in-the-middle attack on the calibration process of quantum key distribution. *Sci. Rep.* **2018**, *8*, 4283. [CrossRef]
29. Jain, N.; Wittmann, C.; Lydersen, L.; Wiechers, C.; Elser, D.; Marquardt, C.; Makarov, V.; Leuchs, G. Device calibration impacts security of quantum key distribution. *Phys. Rev. Lett.* **2011**, *107*, 110501. [CrossRef] [PubMed]
30. Wang, X.B. Beating the photon-number-splitting attack in practical quantum cryptography. *Phys. Rev. Lett.* **2005**, *94*, 230503. [CrossRef] [PubMed]
31. Ma, X.C.; Sun, S.H.; Jiang, M.S.; Liang, L.M. Local oscillator fluctuation opens a loophole for Eve in practical continuous-variable quantum-key-distribution systems. *Phys. Rev. A* **2013**, *88*, 022339. [CrossRef]
32. Jouguet, P.; Kunz-Jacques, S.; Diamanti, E. Preventing calibration attacks on the local oscillator in continuous-variable quantum key distribution. *Phys. Rev. A* **2013**, *87*, 062313. [CrossRef]
33. Huang, J.Z.; Weedbrook, C.; Yin, Z.Q.; Wang, S.; Li, H.W.; Chen, W.; Guo, G.C.; Han, Z.F. Quantum hacking of a continuous-variable quantum-key-distribution system using a wavelength attack. *Phys. Rev. A* **2013**, *87*, 062329. [CrossRef]
34. Ma, X.C.; Sun, S.H.; Jiang, M.S.; Liang, L.M. Wavelength attack on practical continuous-variable quantum-key-distribution system with a heterodyne protocol. *Phys. Rev. A* **2013**, *87*, 052309. [CrossRef]
35. Qin, H.; Kumar, R.; Alléaume, R. Quantum hacking: Saturation attack on practical continuous-variable quantum key distribution. *Phys. Rev. A* **2016**, *94*, 012325. [CrossRef]
36. Qin, H.; Kumar, R.; Makarov, V.; Alléaume, R. Homodyne-detector-blinding attack in continuous-variable quantum key distribution. *Phys. Rev. A* **2018**, *98*, 012312. [CrossRef]
37. Zheng, Y.; Huang, P.; Huang, A.; Peng, J.; Zeng, G. Practical security of continuous-variable quantum key distribution with reduced optical attenuation. *Phys. Rev. A* **2019**, *100*, 012313. [CrossRef]
38. Zheng, Y.; Huang, P.; Huang, A.; Peng, J.; Zeng, G. Security analysis of practical continuous-variable quantum key distribution systems under laser seeding attack. *Opt. Express* **2019**, *27*, 27369–27384. [CrossRef]
39. Huang, A.; Navarrete, Á.; Sun, S.H.; Chaiwongkhot, P.; Curty, M.; Makarov, V. Laser-seeding attack in quantum key distribution. *Phys. Rev. Appl.* **2019**, *12*, 064043. [CrossRef]
40. Huang, A.; Li, R.; Egorov, V.; Tchouragoulov, S.; Kumar, K.; Makarov, V. Laser-damage attack against optical attenuators in quantum key distribution. *Phys. Rev. Appl.* **2020**, *13*, 034017. [CrossRef]
41. Bugge, A.N.; Sauge, S.; Ghazali, A.M.M.; Skaar, J.; Lydersen, L.; Makarov, V. Laser damage helps the eavesdropper in quantum cryptography. *Phys. Rev. Lett.* **2014**, *112*, 070503. [CrossRef]

42. Makarov, V.; Bourgoin, J.P.; Chaiwongkhot, P.; Gagné, M.; Jennewein, T.; Kaiser, S.; Kashyap, R.; Legré, M.; Minshull, C.; Sajeed, S. Creation of backdoors in quantum communications via laser damage. *Phys. Rev. A* **2016**, *94*, 030302. [CrossRef]
43. Pirandola, S.; Ottaviani, C.; Spedalieri, G.; Weedbrook, C.; Braunstein, S.L.; Lloyd, S.; Gehring, T.; Jacobsen, C.S.; Andersen, U.L. High-rate measurement-device-independent quantum cryptography. *Nat. Photon.* **2015**, *9*, 397–402. [CrossRef]
44. Ma, X.C.; Sun, S.H.; Jiang, M.S.; Gui, M.; Liang, L.M. Gaussian-modulated coherent-state measurement-device-independent quantum key distribution. *Phys. Rev. A* **2014**, *89*, 042335. [CrossRef]
45. Li, Z.; Zhang, Y.C.; Xu, F.; Peng, X.; Guo, H. Continuous-variable measurement-device-independent quantum key distribution. *Phys. Rev. A* **2014**, *89*, 052301. [CrossRef]
46. Zhang, X.; Zhang, Y.; Zhao, Y.; Wang, X.; Yu, S.; Guo, H. Finite-size analysis of continuous-variable measurement-device-independent quantum key distribution. *Phys. Rev. A* **2017**, *96*, 042334. [CrossRef]
47. Papanastasiou, P.; Ottaviani, C.; Pirandola, S. Finite-size analysis of measurement-device-independent quantum cryptography with continuous variables. *Phys. Rev. A* **2017**, *96*, 042332. [CrossRef]
48. Ma, H.X.; Huang, P.; Bai, D.Y.; Wang, S.Y.; Bao, W.S.; Zeng, G.H. Continuous-variable measurement-device-independent quantum key distribution with photon subtraction. *Phys. Rev. A* **2018**, *97*, 042329. [CrossRef]
49. Zhang, Y.C.; Li, Z.; Yu, S.; Gu, W.; Peng, X.; Guo, H. Continuous-variable measurement-device-independent quantum key distribution using squeezed states. *Phys. Rev. A* **2014**, *90*, 052325. [CrossRef]
50. Ma, H.X.; Huang, P.; Bai, D.Y.; Wang, T.; Wang, S.Y.; Bao, W.S.; Zeng, G.H. Long-distance continuous-variable measurement-device-independent quantum key distribution with discrete modulation. *Phys. Rev. A* **2019**, *99*, 022322. [CrossRef]
51. Wang, P.; Wang, X.; Li, Y. Continuous-variable measurement-device-independent quantum key distribution using modulated squeezed states and optical amplifiers. *Phys. Rev. A* **2019**, *99*, 042309. [CrossRef]
52. Lupo, C.; Ottaviani, C.; Papanastasiou, P.; Pirandola, S. Continuous-variable measurement-device-independent quantum key distribution: Composable security against coherent attacks. *Phys. Rev. A* **2018**, *97*, 052327. [CrossRef]
53. Chen, Z.; Zhang, Y.; Wang, G.; Li, Z.; Guo, H. Composable security analysis of continuous-variable measurement-device-independent quantum key distribution with squeezed states for coherent attacks. *Phys. Rev. A* **2018**, *98*, 012314. [CrossRef]
54. Wang, P.; Wang, X.; Li, Y. Continuous-variable measurement-device-independent quantum key distribution with source-intensity errors. *Phys. Rev. A* **2020**, *102*, 022609. [CrossRef]
55. Ma, H.X.; Huang, P.; Wang, T.; Wang, S.Y.; Bao, W.S.; Zeng, G.H. Security of continuous-variable measurement-device-independent quantum key distribution with imperfect state preparation. *Phys. Lett. A* **2019**, *383*, 126005. [CrossRef]
56. Zheng, Y.; Huang, P.; Peng, J.; Zhu, Y.; Zeng, G. Performance analysis of practical continuous-variable quantum key distribution systems with weak randomness. *J. Phys. B At. Mol. Opt. Phys.* **2020**, *53*, 095501. [CrossRef]
57. Li, Y.; Huang, P.; Wang, S.; Wang, T.; Li, D.; Zeng, G. A denial-of-service attack on fiber-based continuous-variable quantum key distribution. *Phys. Lett. A* **2018**, *382*, 3253–3261. [CrossRef]