entropy

MDPI

Article

Security Analysis of a Passive Continuous-Variable Quantum Key Distribution by Considering Finite-Size Effect

Shengjie Xu [1,2,†], Yin Li [1,†], Yijun Wang [1], Yun Mao [1,*], Xiaodong Wu [1,*] and Ying Guo [1,*]

[1] School of Automation, Central South University, Changsha 410083, China; 206166@csu.edu.cn (S.X.); liyin@csu.edu.cn (Y.L.); xxywyj@csu.edu.cn (Y.W.)
[2] School of Economics and Mangement, Beihua University, Jilin 132013, China
* Correspondence: maoyun3106@csu.edu.cn (Y.M.); wuxiaodong2018@foxmail.com (X.W.); yingguo@csu.edu.cn (Y.G.)
† These authors contribute equally.

Abstract: We perform security analysis of a passive continuous-variable quantum key distribution (CV-QKD) protocol by considering the finite-size effect. In the passive CV-QKD scheme, Alice utilizes thermal sources to passively make preparation of quantum state without Gaussian modulations. With this technique, the quantum states can be prepared precisely to match the high transmission rate. Here, both asymptotic regime and finite-size regime are considered to make a comparison. In the finite-size scenario, we illustrate the passive CV-QKD protocol against collective attacks. Simulation results show that the performance of passive CV-QKD protocol in the finite-size case is more pessimistic than that achieved in the asymptotic case, which indicates that the finite-size effect has a great influence on the performance of the single-mode passive CV-QKD protocol. However, we can still obtain a reasonable performance in the finite-size regime by enhancing the average photon number of the thermal state.

Keywords: passive; continuous-variable quantum key distribution; finite-size effect

Citation: Xu, S.; Li, Y.; Wang, Y.; Mao, Y.; Wu, X.; Guo, Y. Security Analysis of a Passive Continuous-Variable Quantum Key Distribution by Considering Finite-Size Effect. *Entropy* **2021**, *23*, 1698. https://doi.org/10.3390/e23121698

Academic Editor: Xiang-Bin Wang, Cong Jiang, Leong Chuan Kwek

Received: 2 November 2021
Accepted: 17 December 2021
Published: 19 December 2021

1. Introduction

Quantum key distribution (QKD) solves the problem of sharing secure keys between two distant authenticated users (Alice and Bob). These two users can perform secure communications when such keys are established [1–4]. QKD has been divided into two main categories: one is discrete-variable (DV)QKD protocols [5,6], and the other is continuous-variable (CV) QKD schemes [7–10]. CV-QKD takes advantage of the quadrature components of the optical field to perform the key information distribution. Compared with DV-QKD, CV-QKD has better compatibility with existing optical communication systems and employs lower-cost light sources and detectors.

The Gaussian-modulated CV-QKD protocol making use of coherent states has attracted much attention because of its theoretical security [11–18] and its practicality [19–22]. In this protocol, the quantum state is traditionally prepared in an active manner: Gaussian distributed random numbers are firstly generated by Alice with the help of a true random number generator, then Alice can perform preparation of a coherent state and transmit it to Bob. The modulation method used in the Gaussian-modulated CV-QKD protocol is that Alice modulates the output of a laser by taking advantage of high-speed amplitude and phase modulators with requisite high extinction ratio. Because the modulation format of the Gaussian-modulated CVQKD scheme is relatively complex and the tolerable modulation error is small, it is necessary to make use of high extinction ratio modulators with good stability in this protocol [23].

However, the use of high extinction ratio modulators may present evident enhancement in cost, especially, creating an important challenge in the chip-integration in view of cost-effective silicon photonics technology [24]. The authors of [25] demonstrated on-chip

modulators with high extinction ratio over 65 dB. The high-speed on-chip modulators needed in active QKD encoding schemes bring about significant cost, manufacturing time, and complexity. Consequently, it is important to study the potential of removing the modulators, which, when taken advantage of for encoding, may yield obvious reductions in cost and manufacturing time.

Recently, a passive-state preparation scheme in view of single-mode thermal source rather than high extinction ratio modulators has been proposed, whose aim is to simplify the implementation of CV-QKD [26]. By assuming that Alice's QKD transmitter is trusted, it can take advantage of the well-established security proofs directly for Gaussian-modulated CV-QKD into passive CV-QKD protocol. This passive-state preparation scheme has been applied in CV quantum secret sharing [27] and measurement-device-independent CV-QKD [28,29]. More recently, an experimental study of the passive-state preparation protocol [30] and the local-oscillator-based passive CV-QKD scheme [31] have been proposed, which demonstrate the feasibility of passive CV-QKD in practical implementation. The practical implementations of a thermal source can be realized by employing a broadband-amplified spontaneous emission (ASE) source, which contains many spectral–temporal modes of independent thermal states [30,31]. Compared to a direct Gaussian modulation CV-QKD protocol, the passive CV-QKD scheme with practical implementations of a thermal source has its own advantages, namely, this protocol waives the necessity of utilizing high-extinction ratio amplitude and phase modulators, which may yield significant reductions in cost. The interesting extension of this work may be found in quantum algorithms [32,33], quantum computational speed [34], and quantum communication networks [35]. The security analysis of single-mode passive CV-QKD in asymptotic scenarios has been presented [26]. Nevertheless, the utility of single-mode passive CV-QKD protocol in finite-size regimes has never been analyzed.

In this paper, we perform security analysis of single-mode passive CV-QKD protocol by considering finite-size effect. Here, only the reverse reconciliation scheme is taken into consideration, since the direct reconciliation scheme can be analyzed in a similar way. The numerical simulations of the scheme are conducted by employing block lengths between 10^7 and 10^{11}. When the amount of data samples taken advantage of to perform parameter estimation is large, the performance of single-mode passive CV-QKD protocol in a finite-size regime will approach that in the asymptotic scenario.

The paper is structured as follows. In Section 2, we introduce the main idea of the single-mode passive CV-QKD protocol. In Section 3, we perform the security analysis with numerical simulations by considering an asymptotic case and the finite-size effect. Finally, conclusions are drawn in Section 4.

2. Passive CV-QKD Protocol

The setup of the passive CV-QKD is shown in Figure 1. This scheme makes use of the intrinsic field fluctuations of a thermal source to generate a secure quantum key [26]. As illustrated in Figure 1, Alice makes use of a balanced beam splitter to split the output of a thermal source into two spatial modes. One mode is locally measured by Alice with the help of conjugate homodyne detection, then the other mode is transmitted to Bob through an optical attenuator. In order to make an estimate of the quadrature values of the outgoing mode, it is necessary to achieve the Gaussian-distributed random numbers (x_A, p_A). Therefore, the local measurement owned by Alice is scaled down numerically via a factor of λ_A, which can obtain Alice's desired modulation variance value V_A with a proper combination of source intensity and optical attenuation. Besides, it has been proved that the passive CV-QKD protocol is equivalent to the GMCS QKD protocol in terms of security [26].

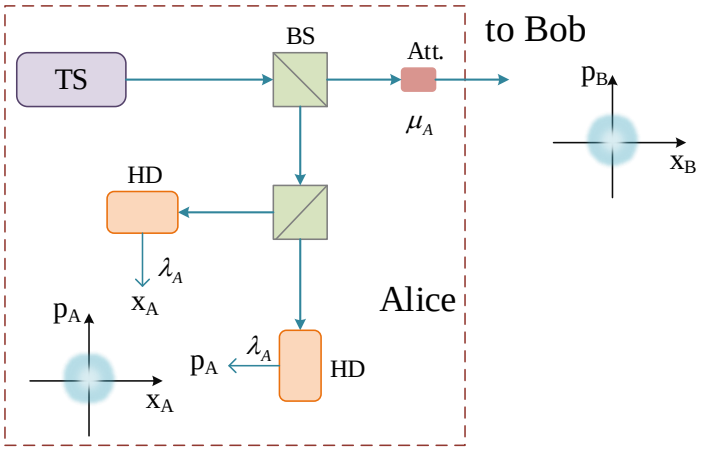

Figure 1. Single-mode passive CV-QKD protocol [26]. HD, homodyne detector; BS, beam splitter; Att., optical attenuator. Here, we employ a beam splitter with a transmittance of ω_M to model the efficiency of the homodyne detector.

It is noteworthy that the excess noise caused by the quantum state preparation has an important effect on the performance of the passive CV-QKD protocol; the mutual information between Alice and Bob is associated with Alice's uncertainties on the quadrature of the outgoing mode. According to the uncertainty principle in quantum mechanics, the minimum uncertainty on either quadrature value of the outgoing mode (equal to 1) can be achieved by Alice. In the passive CV-QKD protocol (illustrated in Figure 1), Alice's uncertainty on the outgoing mode is given by [26]

$$\Lambda_A = \frac{2\mu_A}{\omega_M}(1 - \frac{\omega_M}{2} + \nu_{el}) + 1, \tag{1}$$

where μ_A represents the transmittance of the optical attenuator, and ω_M and ν_{el} stand for the efficiency and noise variance of detector owned by Alice, respectively. According to Equation (1), the excess noise caused by the passive state preparation can be calculated as

$$\xi_A = \Lambda_A - 1 = \frac{2\mu_A}{\omega_M}(1 - \frac{\omega_M}{2} + \nu_{el}). \tag{2}$$

Making use of the relation $V_A = \mu_A m_0$, Equation (2) is revised as

$$\xi_A = \frac{2V_A}{\omega_M m_0}(1 - \frac{\omega_M}{2} + \nu_{el}), \tag{3}$$

where m_0 represents an average photon number of a thermal source owned by Alice.

Considering the fact that the excess noise due to the passive state preparation ξ_A always exists in the single-mode passive CV-QKD protocol, it is necessary to analyze the excess noise ξ_A to achieve desired performance. The excess noise ξ_A as a function of the average photon number m_0 with different modulation variance values V_A is shown in Figure 2. One can find that the larger the average photon number m_0 is, the smaller the excess noise ξ_A is, especially for the low value of modulation variance. Besides, the reduction of modulation variance V_A can also effectively restrain the excess noise ξ_A. According to [26], a typical value of V_A=1 can be satisfied by a practical broadband thermal source. Therefore, the modulation variance value of V_A used in the following simulations is set to V_A=1.

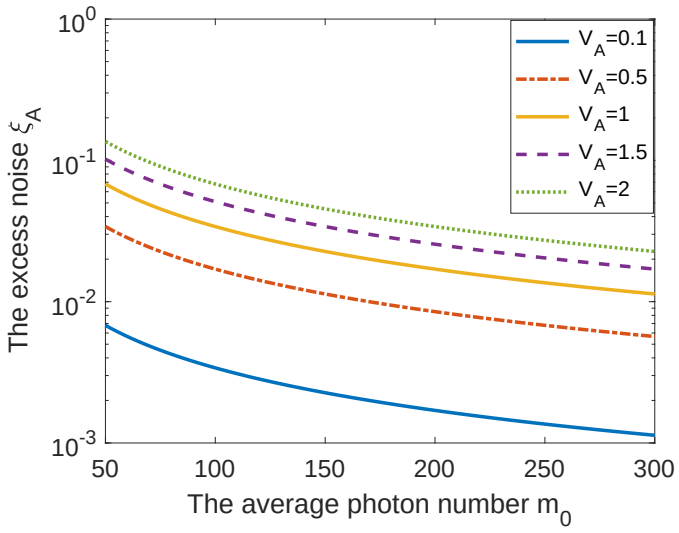

Figure 2. The excess noise ξ_A as a function of the average photon number m_0 with different modulation variance values V_A. Simulation parameters are $\omega_M = 0.5$, $\nu_{el} = 0.1$ [26].

It is necessary to point out that [30,31] employ broadband-amplified spontaneous emission source, which contains many spectral–temporal modes of independent thermal states, and is different from the single-mode thermal source. In [30,31], the excess noise caused by the passive state preparation using multimode thermal source is related with the mode-overlap coefficient. However, it is not necessary to consider the relationship between the excess noise caused by the passive state preparation and the mode-overlap coefficient with the use of single-mode thermal source shown in our protocol.

3. Security Analysis

In this section, we perform security analysis of passive CV-QKD protocol by taking both asymptotic case [15] and finite-size regime [16] into consideration.

3.1. Asymptotic Security of Passive CV-QKD Protocol

Here, we calculate the asymptotic secure key rate of the passive CV-QKD protocol with reverse reconciliation, which is given by [13,36]

$$K_{asy} = \beta I(A:B) - \chi(E), \tag{4}$$

where β represents the reconciliation efficiency, $I(A:B)$ represents the Shannon mutual information between Alice and Bob, and $\chi(E)$ represents the Holevo bound of the information owned by Eve. Here, channel losses is assumed as $\alpha = 0.2$ dB/km. The transmittance is given by

$$T = 10^{\frac{-\alpha L}{10}}, \tag{5}$$

where L represents the fiber length in kilometers.

We now calculate the noise added by Bob's detector for conjugate homodyne detection, which is expressed as [36]

$$\chi_{het} = [1 + (1 - \omega_M) + 2\nu_{el}]/\omega_M, \tag{6}$$

where we have made an assumption that the performance of Bob's detector is the same as that of Alice's.

For the channel-added noise referred to the channel input, it can be calculated as

$$\chi_{line} = \frac{1}{T} - 1 + \xi_A + \xi_0, \tag{7}$$

where ξ_A stands for the excess noise caused by Alice's passive state preparation (shown in Equation (3)). ξ_0 stands for other sources of untrusted noise.

Based on the above analysis, we can present the overall noise referred to the channel input, which is given by

$$\chi_{tot} = \chi_{line} + \frac{\chi_{het}}{T}. \tag{8}$$

Considering that both quadratures can be taken advantage of to make the generation of the secure key, we can thus determine the mutual information between Alice and Bob, which is given by

$$I(A:B) = log_2 \frac{V + \chi_{tot}}{1 + \chi_{tot}}, \tag{9}$$

where $V = V_A + 1$.

Since we adopt a reverse reconciliation scheme to calculate the secret key rate of the passive CV-QKD protocol, the parameter $\chi(E) = \chi(B:E)$. Here, $\chi(B:E)$ stands for the Holevo bound between Eve and Bob. In order to make an estimation of parameter $\chi(B:E)$, the realistic noise mode shown in [10] was adopted, which has been utilized widely in CV-QKD experiments [10,13,19,37,38]. Based on this model, we can calculate the parameter $\chi(B:E)$ as

$$\chi(B:E) = \sum_{i=1}^{2} G(\frac{\rho_i - 1}{2}) - \sum_{i=3}^{5} G(\frac{\rho_i - 1}{2}), \tag{10}$$

where $G(x) = (x+1)\log_2(x+1) - x\log_2 x$.

$$\rho_{1,2}^2 = \frac{1}{2}(\Delta \pm \sqrt{\Delta^2 - 4D}), \tag{11}$$

where

$$\Delta = V^2(1-2T) + 2T + T^2(V + \chi_{line})^2, \tag{12}$$

$$D = T^2(V\chi_{line} + 1)^2. \tag{13}$$

$$\rho_{3,4}^2 = \frac{1}{2}(A \pm \sqrt{A^2 - 4B}), \tag{14}$$

where

$$A = \frac{1}{[T(V + \chi_{tot})]^2}\{\Delta\chi_{het}^2 + D + 1 + 2\chi_{het}[V\sqrt{D} + T(V + \chi_{line})] + 2T(V^2 - 1)\}, \tag{15}$$

$$B = [\frac{V + \sqrt{D}\chi_{het}}{T(V + \chi_{tot})}]^2, \tag{16}$$

$$\rho_5 = 1. \tag{17}$$

In the following, we illustrate the relationship between the asymptotic secret key rate and the transmission distance under four different average photon numbers m_0 = 70, m_0 = 100, m_0 = 150, and m_0 = 200. The Pirandola–Laurenza–Ottaviani–Banchi (PLOB) bound is also plotted in Figure 3, which illustrates the ultimate limit of repeaterless quantum communication [39]. From Figure 3, we can observe that the performance of the passive CV-QKD protocol in terms of asymptotic secret key rate and transmission distance is enhanced by increasing the average output photon number m_0. As a matter of course, the performance of the single-mode passive CV-QKD protocol becomes more and more close to the PLOB bound with the increase of m_0. We can find the reason from Equation (3), namely, with a desired V_A, the larger average output photon number m_0, the smaller the excess noise ξ_A introduced by Alice. In addition, one can find that the maximum transmission distance is over 100 km when m_0 = 100. That is to say, we can perform efficient implementation of the passive CV-QKD protocol with m_0 above 100.

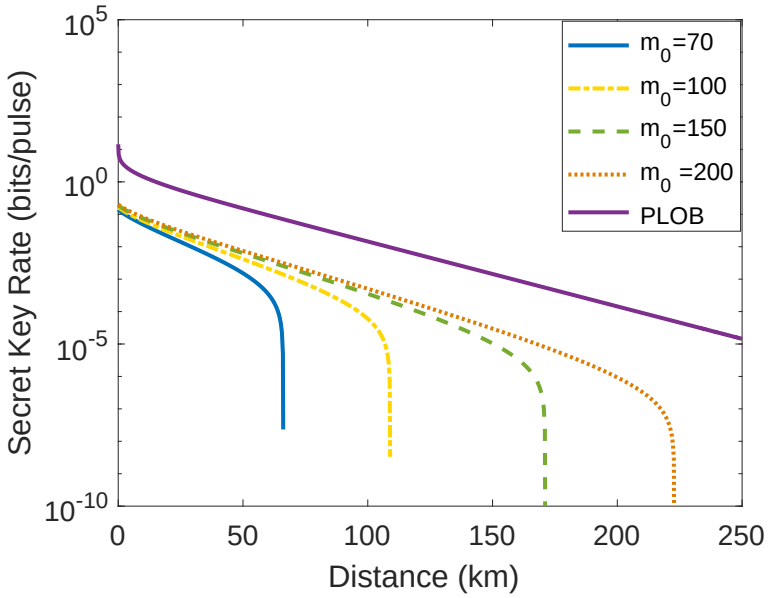

Figure 3. The relationship between the asymptotic secret key rate and the distance under four different average photon numbers: $m_0 = 70$, $m_0 = 100$, $m_0 = 150$, and $m_0 = 200$. Simulation parameters are $V_A = 1$, $\xi_0 = 0.01$, $\omega_M = 0.5$, $\nu_{el} = 0.1$, and reconciliation efficiency $\beta = 0.95$ [26].

Figure 4 illustrates the asymptotic secret key rate as a function of average photon number m_0 under different distances. From Figure 4, one can observe that the asymptotic secret key rate of the single-mode passive CV-QKD protocol grows fast in the interval $[60, 200]$; nevertheless, it enhances slowly in the interval $[200, 500]$. This indicates that when the average photon number m_0 reaches a certain value, the performance improvement is inapparent with continuing increase of average photon number m_0.

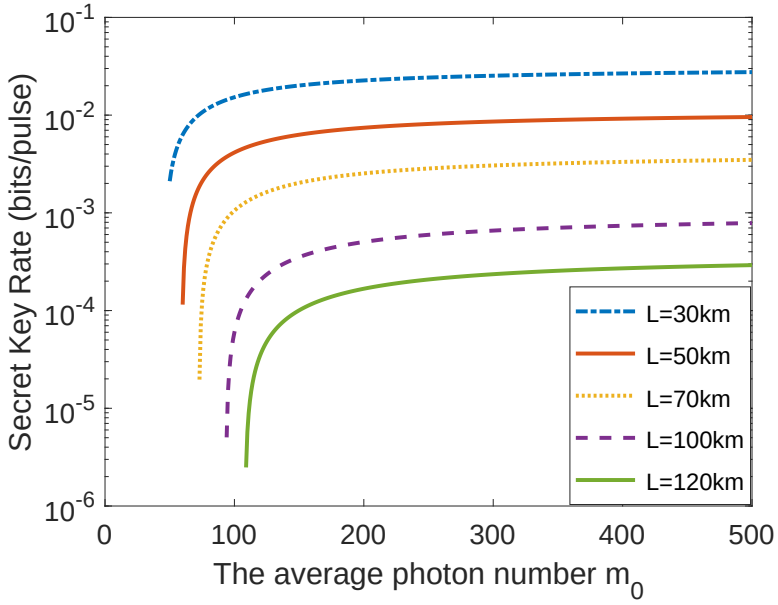

Figure 4. The asymptotic secret key rate as a function of average photon number m_0 under different distances. Simulation parameters are $V_A = 1$, $\xi_0 = 0.01$, $\omega_M = 0.5$, $\nu_{el} = 0.1$, reconciliation efficiency $\beta = 0.95$ [26].

3.2. Security of Passive CV-QKD in Finite-Size Scenario

In the above analysis, we show the calculation of the asymptotic secret key rate of the passive CV-QKD protocol based on an assumption that Alice and Bob can take advantage

of infinitely many signals to make the exchange. Nevertheless, it is impossible to achieve in practice, as the length of the practical secure key is limited. Consequently, it is necessary to perform security analysis of the passive CV-QKD scheme by considering the finite-size effect. The finite-size secret key rate of the single-mode passive CV-QKD protocol with reverse reconciliation is given by [16]

$$K_{fini} = \frac{f}{F}[\beta I(A:B) - \chi_{\epsilon_{PE}}(B:E) - \Delta(f)], \tag{18}$$

where the meanings of β and $I(A:B)$ are shown above. F represents the total exchanged signals and f is the number of signals which are used to generate secure key, and the leftover signal $P = F - f$ is taken advantage of to perform parameter estimation. ϵ_{PE} stands for the failure probability of parameter estimation, and $\Delta(f)$ is associated with the security of the privacy amplification, which is given by

$$\Delta(f) = (2dim\Psi_B + 3)\sqrt{\frac{\log_2(2/\bar{\epsilon})}{f}} + \frac{2}{f}\log_2(1/\epsilon_{PB}), \tag{19}$$

where $\bar{\epsilon}$ is assumed to be the smoothing parameter, ϵ_{PB} represents the failure probability that exists in the privacy amplification procedure, and Ψ_B stands for the Hilbert space corresponding to the raw key owned by Bob. Here, $dim\Psi_B = 2$ because the raw key is encoded on binary bits.

In order to perform the security analysis of the single-mode passive CV-QKD protocol in a finite-size regime, it is important to make calculation of $\chi_{\epsilon_{PE}}(B:E)$ by employing a covariance matrix assumed as $\Upsilon_{\epsilon_{PE}}$, which makes the secret key rate of the single-mode passive CV-QKD protocol minimum exist under a probability of $1 - \epsilon_{PE}$. Through using P couples of correlated variables $(x_i, y_i)_{i=1,2,\cdots,P}$, we can achieve the covariance matrix $\Upsilon_{\epsilon_{PE}}$. To perform analysis of these correlated variables, we adopt a normal model, which is shown as follows:

$$y = tx + z, \tag{20}$$

where $t = \sqrt{T}$ and z follow a centered normal distribution with variance $\vartheta^2 = 1 + T(\xi_A + \xi_0)$. According to Equation (20), the data owned by Alice and Bob can be connected. The covariance matrix $\Upsilon_{\epsilon_{PE}}$ is given by

$$\Upsilon_{\epsilon_{PE}} = \begin{pmatrix} (V_A + 1)I_2 & t_{min}Z\sigma_z \\ t_{min}Z\sigma_z & (t_{min}^2 V_A + \vartheta_{max}^2)I_2 \end{pmatrix}, \tag{21}$$

where t_{min} and ϑ_{max}^2 stand for the minimum of t and maximum of ϑ^2 compatible with sampled couples, except with probability $\epsilon_{PE}/2$, and $Z = \sqrt{V_A^2 + 2V_A}$. After that, we can obtain the maximum-likelihood estimators $\hat{t}$ and $\hat{\vartheta}^2$, which are calculated as

$$\hat{t} = \frac{\sum_{i=1}^{P} x_i y_i}{\sum_{i=1}^{P} x_i^2} \quad and \quad \hat{\vartheta}^2 = \frac{1}{P}\sum_{i=1}^{P}(y_i - \hat{t}x_i)^2. \tag{22}$$

Distributions followed by the maximum-likelihood estimators $\hat{t}$ and $\hat{\vartheta}^2$ are, respectively, given by

$$\hat{t} \sim N(t, \frac{\vartheta^2}{\sum_{i=1}^{P} x_i^2}) \quad and \quad \frac{P\hat{\vartheta}^2}{\vartheta^2} \sim \chi^2(P-1), \tag{23}$$

which indicate that $\hat{t}$ and $\hat{\vartheta}^2$ are independent for each other. In view of [16], we respectively show the expressions of t_{min} and ϑ_{max}^2, which are given by

$$t_{min} \approx \hat{t} - z_{\epsilon_{PE}/2}\sqrt{\frac{\hat{\vartheta}^2}{PV_A}}, \qquad \vartheta^2_{max} \approx \hat{\vartheta}^2 + z_{\epsilon_{PE}/2}\frac{\sqrt{2}\hat{\vartheta}^2}{\sqrt{P}}, \tag{24}$$

where $z_{\epsilon_{PE}/2}$ is such that $1 - \mathrm{erf}(z_{\epsilon_{PE}/2}/\sqrt{2})/2 = \epsilon_{PE}/2$, and $\mathtt{erf}$ represents the error function defined as $\mathtt{erf}(x) = \frac{2}{\sqrt{\pi}}\int_0^x e^{-t^2}dt$. Making use of the expected values of $\hat{t}$ and $\hat{\vartheta}^2$, which are $\mathtt{E}[\hat{t}] = \sqrt{T}$ and $\mathtt{E}[\hat{\vartheta}^2] = 1 + T(\xi_A + \xi_0)$, one can perform calculation of t_{min} and ϑ^2_{max} as

$$t_{min} \approx \sqrt{T} - z_{\epsilon_{PE}/2}\sqrt{\frac{1 + T(\xi_A + \xi_0)}{PV_A}}, \qquad \vartheta^2_{max} \approx 1 + T(\xi_A + \xi_0) + z_{\epsilon_{PE}/2}\frac{\sqrt{2}[1 + T(\xi_A + \xi_0)]}{\sqrt{P}}. \tag{25}$$

It is noteworthy that the error probabilities shown above are set to [16]

$$\bar{\epsilon} = \epsilon_{PE} = \epsilon_{PB} = 10^{-10}. \tag{26}$$

Making use of the derived bound t_{min} and ϑ^2_{max}, the finite-size secret key rate of single-mode passive CV-QKD protocol can be calculated.

Figure 5 illustrates the relationship between the finite-size secret key rate and the transmission distance under four different average photon numbers m_0. It is worth mentioning that the average output photon number m_0 we set in Figure 5a–d are 70, 100, 150, and 200. From left to right, the lines shown in Figure 5 correspond to block lengths of 10^7, 10^8, 10^9, 10^{10}, and the asymptotic case. Here, we plot the PLOB bound in all four subgraphs to make a detailed comparison. As shown in Figure 5, one can observe that the performance of the single-mode passive CV-QKD protocol in the finite-size regime is more pessimistic than that obtained in the asymptotic limit. This is in line with our expectations because a part of the exchanged signals needs to be made use of to perform parameter estimation instead of generating the secure key in the finite-size regime. Nevertheless, the performance of passive CV-QKD protocol in terms of secret key rate and maximum transmission distance in the finite-size regime becomes more and more close to that in the asymptotic case and the PLOB bound with the increase of the number of total exchanged signals. In addition, we can still achieve a reasonable performance in the finite-size scenario by improving the average photon number of the thermal state.

The relationship between the finite-size secret key rate and the average photon number m_0 with different distances is shown in Figure 6. Here, the block size $F = 10^9$ is used as an example to perform analysis since other block size cases can be analyzed in the same way. It can be seen that the finite-size secret key rate of the single-mode passive CV-QKD protocol grows fast in the interval $[30, 200]$; however, it increases slowly in the interval $[200, 500]$. The results make it clear that when the average photon number m_0 reaches a certain value, the finite-size secret key rate enhancement is inapparent with continuing increase of the average photon number m_0.

The plot of Figure 7 shows the relations of the finite-size secret key rate and the reconciliation efficiency. Similar to Figure 6, here, we take the block size $F = 10^9$ as an example to perform analysis since other block size cases can be analyzed in the same way. It can be seen that the usable range of the reconciliation efficiency β of the passive CV-QKD protocol in the finite-size regime expands with the enhancement of the average photon number m_0. For example, when $m_0 = 70$, the usable range of β is $[0.96, 1]$. However, when $m_0 = 100$, the usable range of β is $[0.88, 1]$.

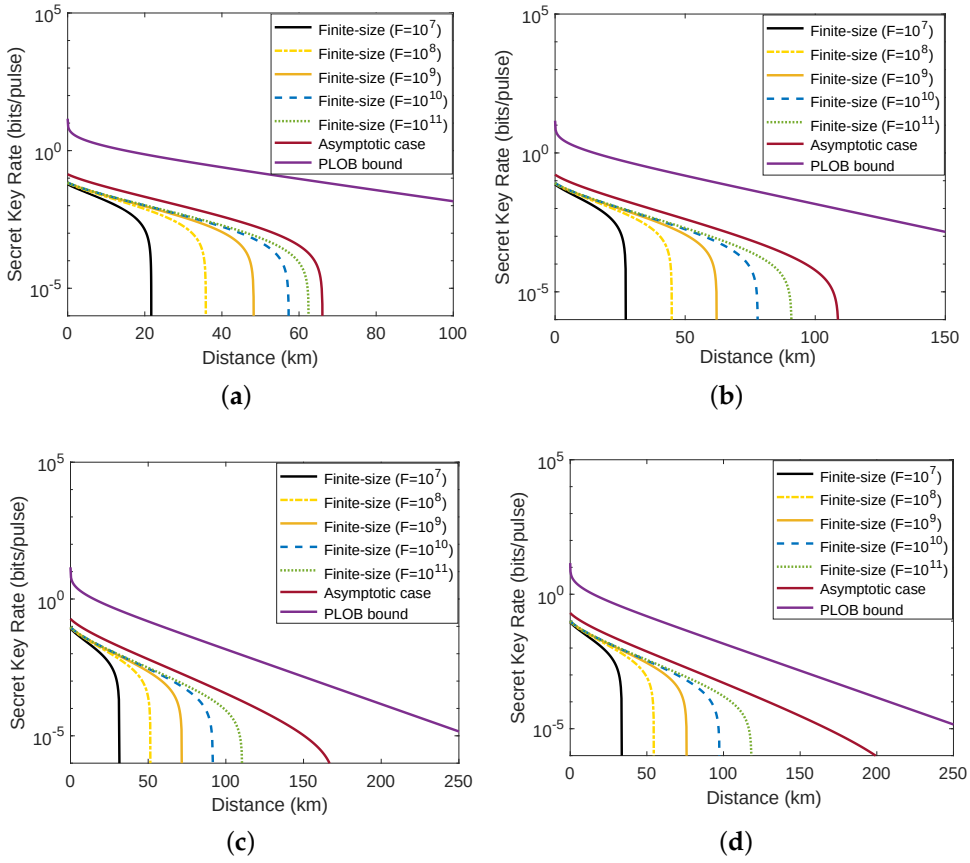

Figure 5. The relationship between the finite-size secret key rate of single-mode passive CV-QKD protocol and the distance: (**a**) $m_0 = 70$; (**b**) $m_0 = 100$; (**c**) $m_0 = 150$; (**d**) $m_0 = 200$. From left to right, the lines correspond to block lengths of $F = 10^7$, 10^8, 10^9, 10^{10}, and 10^{11}. Other parameters are set to be the same as Figure 3.

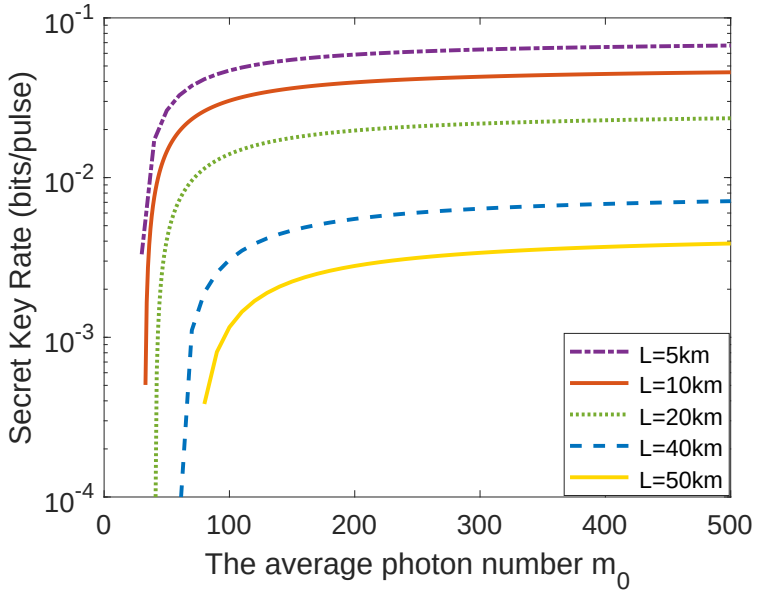

Figure 6. The relationship between the finite-size secret key rate and the average photon number m_0 with different distances. The block size is set to $F = 10^9$. Other parameters are set to be the same as Figure 4.

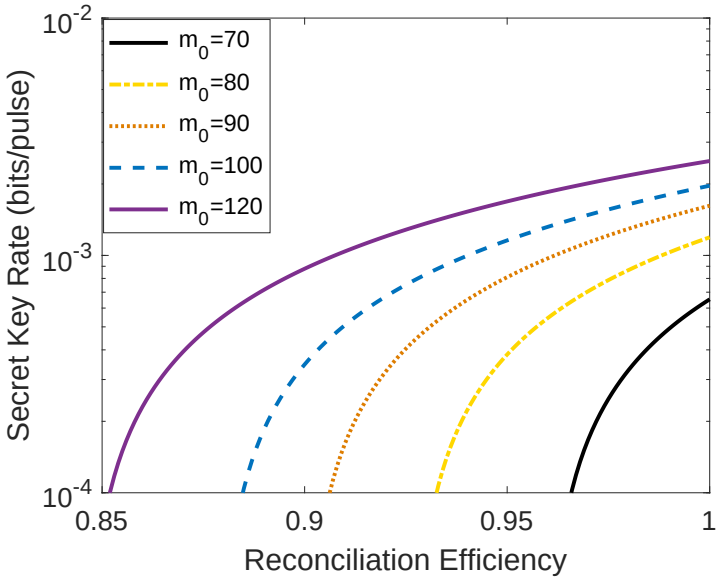

Figure 7. The relationship between the finite-size secret key rate of single-mode passive CV-QKD protocol and the reconciliation efficiency β. The block size is set to $F = 10^9$. Other parameters are set to be the same as Figure 3.

4. Conclusions

We performed the security analysis of single-mode passive CV-QKD protocol by considering the finite-size effect under collective attack. By taking advantage of the single-mode passive CV-QKD protocol in the finite-size regime of the secret key rate formula for numerical simulation, one can find the secret key rate and maximum transmission distance under the influence of the finite-size effect. Therefore, the performance of the single-mode passive CV-QKD protocol in a finite-size regime is more pessimistic than those achieved in asymptotic case. However, with the enhancement of the number of total exchanged signals, the secret key rate and maximum transmission distance in the finite-size regime becomes more and more close to those in asymptotic case and the PLOB bound. Our work focuses on the influence of the finite-size effect on the single-mode passive CV-QKD protocol, which shows more practical results than those achieved in asymptotic case.

Author Contributions: Y.W. and X.W. gave the general idea of the study, designed the conception of the study, and performed critical revision of the manuscript. S.X. and Y.L. accomplished the formula derivation and numerical simulations and drafted the article. Y.M. provided feasible advice and critical revision of the manuscript. Y.G. provided critical revision of the manuscript. All authors have read and approved the final manuscript.

Funding: This work was supported by the National Natural Science Foundation of China (Grant Nos. 61871407, 61572529).

Institutional Review Board Statement: Not Applicable.

Informed Consent Statement: Not Applicable.

Data Availability Statement: Data sharing not Applicable.

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

References

1. Gisin, N.; Ribordy, G.; Tittel, W.; Zbinden, H. Quantum cryptography. *Rev. Mod. Phys.* **2002**, *74*, 145. [CrossRef]
2. Scarani, V.; Bechmann-Pasquinucci, H.; Cerf, N.J.; Dušek, M.; Lütkenhaus, N.; Peev, M. The security of practical quantum key distribution. *Rev. Mod. Phys.* **2009**, *81*, 1301. [CrossRef]
3. 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]

4. Xu, F.H.; Ma, X.F.; Zhang, Q.; Lo, H.K.; Pan, J.W. Secure quantum key distribution with realistic devices. *Rev. Mod. Phys.* **2020**, *92*, 025002. [CrossRef]
5. Takeda, S.; Fuwa, M.; Van Loock, P.; Furusawa, A. Entanglement swapping between discrete and continuous variables. *Phys. Rev. Lett.* **2015**, *114*, 100501. [CrossRef]
6. Gessner, M.; Pezzè, L.; Smerzi, A. Efficient entanglement criteria for discrete, continuous, and hybrid variables. *Phys. Rev. A* **2016**, *94*, 020101. [CrossRef]
7. Braunstein, S.L.; Van Loock, P. Quantum information with continuous variables. *Rev. Mod. Phys.* **2005**, *77*, 513. [CrossRef]
8. 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. [CrossRef]
9. Wu, X.D.; Wang, Y.J.; Zhong, H.; Liao, Q.; Guo, Y. Plug-and-play dual-phase-modulated continuous-variable quantum key distribution with photon subtraction. *Front. Phys.* **2019**, *14*, 41501. [CrossRef]
10. 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. [CrossRef]
11. Garcia-Patron, R.; Cerf, N.J. Unconditional optimality of Gaussian attacks against continuous-variable quantum key distribution. *Phys. Rev. Lett.* **2006**, *97*, 190503. [CrossRef]
12. Navascués, M.; Grosshans, F.; Acin, A. Optimality of Gaussian attacks in continuous-variable quantum cryptography. *Phys. Rev. Lett.* **2006**, *97*, 190502. [CrossRef]
13. Lodewyck, J.; Bloch, M.; García-Patrón, R.; Fossier, S.; Karpov, E.; Diamanti, E.; Debuisschert, T.; Cerf, N.J.; Tualle-Brouri, R.; McLaughlin, S.W.; et al. Quantum key distribution over 25 km with an all-fiber continuous-variable system. *Phys. Rev. A* **2007**, *76*, 042305. [CrossRef]
14. Pirandola, S.; Braunstein, S.L.; Lloyd, S. Characterization of collective Gaussian attacks and security of coherent-state quantum cryptography. *Phys. Rev. Lett.* **2008**, *101*, 200504. [CrossRef]
15. Renner, R.; Cirac, J.I. de Finetti Representation Theorem for Infinite-Dimensional Quantum Systems and Applications to Quantum Cryptography. *Phys. Rev. Lett.* **2009**, *102*, 110504. [CrossRef]
16. Leverrier, A.; Grosshans, F.; Grangier, P. Finite-size analysis of a continuous-variable quantum key distribution. *Phys. Rev. A* **2010**, *102*, 110504. [CrossRef]
17. Leverrier, A. Composable security proof for continuous-variable quantum key distribution with coherent states. *Phys. Rev. Lett.* **2015**, *114*, 070501. [CrossRef]
18. Leverrier, A. Security of continuous-variable quantum key distribution via a Gaussian de Finetti reduction. *Phys. Rev. Lett.* **2017**, *118*, 200501. [CrossRef] [PubMed]
19. 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. [CrossRef]
20. Huang, D.; Huang, P.; Lin, D.K.; Zeng, G.H. Long-distance continuous-variable quantum key distribution by controlling excess noise. *Sci. Rep.* **2016**, *6*, 19201. [CrossRef]
21. Huang, D.; Huang, P.; Li, H.; Wang, T.; Zhou, Y.; Zeng, G.H. Field demonstration of a continuous-variable quantum key distribution network. *Opt. Lett.* **2016**, *41*, 3511–3514. [CrossRef]
22. 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] [PubMed]
23. 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]
24. Zhang, G.; Haw, J.Y.; Cai, H.; Xu, F.; Assad, S.; Fitzsimons, J.F.; Zhou, X.; Zhang, Y.; Yu, S.; Wu, J.; et al. An integrated silicon photonic chip platform for continuous-variable quantum key distribution. *Nat. Photon.* **2019**, *13*, 839–842. [CrossRef]
25. Liu, S.; Cai, H.; DeRose, C.T.; Davids, P.; Pomerene, A.; Starbuck, A.L.; Trotter, D.C.; Camacho, R.; Urayama, J. High speed ultra-broadband amplitude modulators with ultrahigh extinction> 65 dB. *Opt. Express* **2017**, *25*, 11254. [CrossRef] [PubMed]
26. Qi, B.; Evans, P.G.; Grice, W.P. Passive state preparation in the Gaussian-modulated coherent-states quantum key distribution. *Phys. Rev. A* **2018**, *97*, 012317. [CrossRef]
27. Wu, X.; Wang, Y.; Huang, D. Passive continuous-variable quantum secret sharing using a thermal source. *Phys. Rev. A* **2020**, *101*, 022301. [CrossRef]
28. Bai, D.; Huang, P.; Ma, H.; Wang, T.; Zeng, G. Passive-state preparation in continuous-variable measurement-device-independent quantum key distribution. *J. Phys. B* **2019**, *52*, 135502. [CrossRef]
29. Wu, X.; Wang, Y.; Li, S.; Zhang, W.; Huang, D.; Guo, Y. Security analysis of passive measurement-device-independent continuous-variable quantum key distribution with almost no public communication. *Quantum Inf. Process.* **2019**, *18*, 372. [CrossRef]
30. Qi, B.; Gunther, H.; Evans, P.G.; Williams, B.P.; Camacho, R.M.; Peters, N.A. Experimental passive-state preparation for continuous-variable quantum communications. *Phys. Rev. Appl.* **2020**, *13*, 054065. [CrossRef]
31. Wu, X.; Wang, Y.; Guo, Y.; Zhong, H.; Huang, D. Passive continuous-variable quantum key distribution using a locally generated local oscillator. *Phys. Rev. A* **2021**, *103*, 032604. [CrossRef]
32. Zidan, M.; Aldulaimi, S.; Eleuch, H. Analysis of the Quantum Algorithm based on Entanglement Measure for Classifying Boolean Multivariate Function into Novel Hidden Classes: Revisited. *Appl. Math.* **2021**, *15*, 643–647.

33. Zidan, M.; Abdel-Aty, A.H.; Nguyen, D.M.; Mohamed, A.S.; Al-Sbou, Y.; Eleuch, H.; Abdel-Aty, M. A quantum algorithm based on entanglement measure for classifying Boolean multivariate function into novel hidden classes. *Results Phys.* **2019**, *15*, 102549. [CrossRef]
34. Obada, A.S.; Abo-Kahla, D.; Metwally, N.; Abdel-Aty, M. The quantum computational speed of a single Cooper-pair box. *Phys. E Low Dimens. Syst. Nanostruct.* **2011**, *43*, 1792–1797. [CrossRef]
35. Farouk, A.; Batle, J.; Elhoseny, M.; Naseri, M.; Lone, M.; Fedorov, A.; Alkhambashi, M.; Ahmed, S.H.; Abdel-Aty, M. Robust general N user authentication scheme in a centralized quantum communication network via generalized GHZ states. *Front. Phys.* **2018**, *13*, 130306. [CrossRef]
36. Fossier, S.; Diamanti, E.; Debuisschert, T.; Tualle-Brouri, R.; Grangier, P. Improvement of continuous-variable quantum key distribution systems by using optical preamplifiers. *J. Phys. B* **2009**, *42*, 114014. [CrossRef]
37. 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]
38. Kumar, R.; Qin, H.; Alléaume, R. Coexistence of continuous variable QKD with intense DWDM classical channels. *New J. Phys.* **2015**, *17*, 043027. [CrossRef]
39. Pirandola, S.; Laurenza, R.; Ottaviani, C.; Banchi, L. Fundamental limits of repeaterless quantum communications. *Nat. Commun.* **2017**, *8*, 15043. [CrossRef]