

Article

Impact of Imbalanced Modulation on Security of Continuous-Variable Measurement-Device-Independent Quantum Key Distribution

Wenyuan Liu ^{1,*}, Zehui Liu ¹, Jiandong Bai ¹ , Qi Jie ¹, Guangwei Zhang ¹, Yan Tian ² and Jingjing Jin ¹
¹ School of Semiconductor and Physics, North University of China, Taiyuan 030051, China; liu664586445@foxmail.com (Z.L.); jdbai@nuc.edu.cn (J.B.); jieqi@nuc.edu.cn (Q.J.); zhangguangw@foxmail.com (G.Z.); jingjingjin@nuc.edu.cn (J.J.)

² School of Information and Communication Engineering, North University of China, Taiyuan 030051, China; tianyan@nuc.edu.cn

* Correspondence: liuweny@nuc.edu.cn

Abstract: Continuous variable measurement-device-independent quantum key distribution (CV-MDI-QKD) removes all known or unknown side-channel attacks on detectors. However, it is difficult to fully implement assumptions in the security demonstration model, which leads to potential security vulnerabilities inevitably existing in the practical system. In this paper, we explore the impact of imbalanced modulation at transmitters on the security of the CV-MDI-QKD system mainly using a coherent state and squeezed state under symmetric and asymmetric distances. Assuming two different modulation topologies of senders, we propose a generalized theoretical scheme and evaluate the key parameter achievable of the protocol with the mechanism of imbalanced modulation. The presented results show that imbalanced modulation can achieve a relatively nonlinearly higher secret key rate and transmission distances than the previous protocol which is the balanced modulation variance used by transmitters. The advantage of imbalanced modulation is demonstrated for the system key parameter estimation using numerical simulation under different situations. In addition, the consequences indicate the importance of imbalanced modulation on the performance of CV-MDI-QKD protocol and provide a theoretical framework for experimental implementation as well as the optimal modulated mode.



Citation: Liu, W.; Liu, Z.; Bai, J.; Jie, Q.; Zhang, G.; Tian, Y.; Jin, J. Impact of Imbalanced Modulation on Security of Continuous-Variable Measurement-Device-Independent Quantum Key Distribution. *Photonics* **2024**, *11*, 649.

<https://doi.org/10.3390/photonics11070649>

photonics11070649

Received: 6 June 2024

Revised: 5 July 2024

Accepted: 8 July 2024

Published: 10 July 2024



Copyright: © 2024 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<https://creativecommons.org/licenses/by/4.0/>).

Keywords: quantum key distribution; imbalanced modulation mode; coherent state; squeezed state

1. Introduction

Quantum key distribution (QKD) can build the bridge between two legitimate communicating terminals (Alice and Bob), which are generally linked by a precariously quantum channel threaten by eavesdropper (Eve) and an authenticated classical channel [1–6]. Its unconditional security proof is guaranteed by primary principles of quantum mechanics with one-time pad protocol that any stealing activities for enciphered message using the shared secure keys by Eve can be detected by both sides of communication, even though the more powerful quantum computing is employed. Continuous-variable (CV) QKD is a major category of QKD protocol, which encodes information on the amplitude or phase quadratures of coherent or squeezed state, respectively, and receivers perform the homodyne or heterodyne detection. Owing to the advantage of promising potential high secure key rate at medium and short distances, as well as high compatibility with the current optical communication networks and simpler cost-effective practical implementations, CV-QKD systems have drawn scientists and engineer's attention over the past decade [7–24]. CV-QKD using a Gaussian quantum resource modulated state, such as the coherent state and squeezed state, has been demonstrated in their security level based on the procedure of parameter estimation, data reconciliation, and privacy amplification.

Based on the rapid progress in theory and experiment, the CV-QKD protocol has achieved tremendous advances in practical applications and optical networks [8,25–29].

At present, the theoretical security analyses of the Gaussian modulated coherent state (GMCS) and the modulated squeezed state-based CV-QKD protocol have been initially proved under the all possible attacks and later expanded to consider the finite-size effect and composable security [30–35]. However, the non-negligible gap between idealized hypothesis models and the process of practical experiment implementation for QKD, inevitably leads to some potential security vulnerabilities exploited by a variety of targeted attacks from Eve [4–6,36]. For the purpose of filling the gap between the theoretical models and practical experiments as soon as possible, the measurement-device-independent (MDI) QKD protocol has been proposed [37–42], in which both transmitting terminal Alice and Bob send modulation data to an untrusted third party, who are introduced to perform Bell-state measurement (BSM) and announce the result through an authenticated classical channel used for generating the secure keys. MDI-QKD can naturally eliminate all side-channel attacks against the detectors, whether we already know it or not.

In previous work [15,20,43–46], Alice and Bob generally perform a symmetry modulated coherent state or squeezed state during the process of theoretical analysis and experimental implementation based on the CV-MDI-QKD protocol. The results of the above literature indicate that when the distances from Alice to the untrusted third party are equal to the distances from Bob to the untrusted third party (the symmetric case), the performance of the protocol, in terms of both maximum secure transmission distances and secret key rate, is lower than in the asymmetric case, where these distances are different. Furthermore, the secure analysis of CV-MDI-QKD protocol is completed considering the worst-case scenario where the two links are subject to a two-mode Gaussian attack based on both sides utilizing balanced modulation. These results pave the way towards a quantum network and promote the progress of MDI security. Based on the theoretical analytical framework, the finite-key size effect is considered against general attacks with a rigorous security proof [46–49] that has shown the robustness security of MDI-QKD in asymmetric unstable channels. In addition, the secure bound of the ultimate secure key rate is acquired under the statistical fluctuations, which can provide practical guidance to threshold detectors with highly lossy channels and against environmental disturbances [50–52].

Motivated by [15,43–45], we mainly extend the advantages of the MDI framework and explore the impact of imbalanced modulation at both transmitting sides on the security of CV-MDI-QKD protocol in the paper. Both the asymmetric case and symmetric case have been demonstrated in the presence of an arbitrary two-mode Gaussian attack of the links, which has been proven to be the optimal attack for CV-MDI-QKD protocols [15]. Our results show that the imbalanced modulation can improve the performance of the protocol for both the secret key rate and transmission distances compared with the previous balanced modulation.

The rest of this paper is organized as follows. In Section 2, we describe the details of the CV-MDI-QKD protocol with imbalanced modulation using coherent state and squeezed state. In Sections 3 and 4, we present the simulation results under the case of symmetric and asymmetric transmitted distances respectively. In Section 5, we give a discussion, and in Section 6, we summarize our results.

2. CV-MDI-QKD Protocol with Imbalanced Modulated Using Squeezed State and Coherent State

In this section, we first review the conception of the CV-MDI-QKD protocol and theoretically establish equivalent entanglement-based (EB) scheme of the protocol using the coherent state and squeezed state [7,44,45,53]. We then present the influence of imbalanced modulation on key parameters against a two-mode Gaussian attack in the protocol under symmetric and asymmetric cases. We then elucidate the different performance between balanced modulation and imbalanced modulation.

In the case of CV-MDI-QKD with squeezed-state or coherent-state preparation, Alice and Bob independently generate randomly Gaussian-distributed values $x_A(p_A)$ and $x_B(p_B)$, satisfying the zero mean and variances V_A and V_B , respectively. During one of the crucial processes of the experimental realization of CV-MDI-QKD protocol for encoding the key information, the amplitude and phase modulator or IQ modulator are utilized to modulate x or p quadrature for the purpose of achieving various modulation types. In general, either coherent or squeezed state is prepared as the modulated source for the prepare-and-measure (PM) scheme. Then, these modulated-squeezed states or coherent states are transmitted through two different unsecured and loss standard quantum channels that can be controlled by the eavesdropper (Eve) to the third party (Charlie), respectively. The third party, Charlie, receives two independent quantum signals and mixes each of them with a 50:50 beam splitter (BS). The output port of the interfered mode signal is measured with $x(p)$ quadrature by two realistic homodyne detectors: one for amplitude quadrature and the other for phase quadrature, respectively. The detection results are publicly announced to Alice and Bob through an authenticated classical channel. The knowledge of public outcomes can enable each party (Alice or Bob) to infer the measurement results of the other party by data post-processing. In particular, the performance of the modulated-squeezed state can aggrandize the resistant capacity against a two-mode Gaussian attack when Alice and Bob generate an x or p quadrature-squeezed-state. If we assume that an x quadrature-squeezed state is prepared, the modulation variances V_{PM} and V_{AM} should satisfy the equation $s + V_{AM} = 1/s + \Delta V_0 + V_{PM}$, where s and $1/s + \Delta V_0$ denote the squeezing and anti-squeezing variances of the states, respectively. ΔV_0 is the excess noise of the anti-squeezing [45,53].

For convenience, to analyze the security of the protocol, an entanglement-based (EB) scheme is proposed to provide comprehensive proof and equivalent to the PM scheme even more important. The EB scheme of CV-MDI-QKD protocol equivalence to the PM scheme described above is presented in Figure 1.

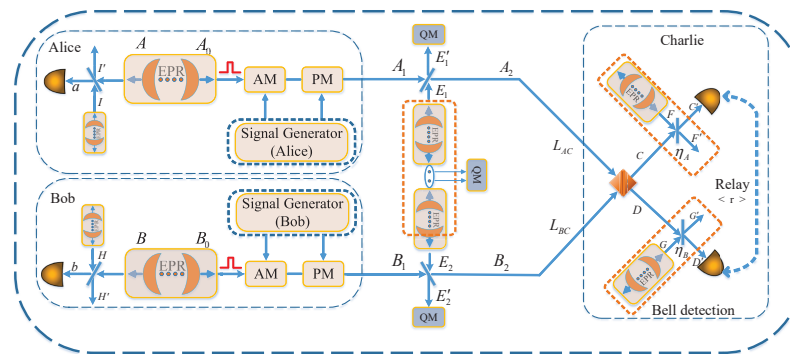


Figure 1. Entanglement-based scheme of CV-MDI-QKD protocol under imbalanced modulated quantum state. Both Alice and Bob prepare the same quantum state except for the modulation variance. Specifically, each side contacts the homodyne or heterodyne detection on one of the modes of the entangled state for different preparation quantum states and sends the other mode to an untrusted third party, Charlie, through a quantum channel with the length L_{AC} (L_{BC}), respectively. Furthermore, the thermal state V_N that simulates the electronic noise of the realistic detector and the BS with transmission efficiency η are utilized to represent the realistic detector.

Alice and Bob generate a two-mode squeezed vacuum state with the variance V_A and V_B independently (generally, $V_A = V_B$, but in this paper, the main analysis focuses on the case of $V_A \neq V_B$), and keep one of the modes on each side, another mode is sent to the third party through the two different quantum channels at the same time. Taking the modulated squeezed state as an example, an additional Einstein–Podolsky–Rosen (EPR) mode I is appended to the mode A through BS with a coupling ratio of 50:50, respectively. We can

implement the homodyne detection on mode A and the other mode A_0 is projected to the squeezed state. At the same time, Bob performs the same thing.

However, during primary studies [15,20,43–46], Alice and Bob keep the same operations, including squeezed parameters and modulated variance under two different conditions with symmetric and asymmetric transmission distances. This work emphasizes the point of imbalance modulation in the CV-MDI-QKD protocol using the coherent and squeezed state. The third-party, Charlie, performs a CV Bell-state measurement. On this station, the two received imbalanced modulated modes A_2 and B_2 are interfered at a 50:50 beam splitter, then the output two modes C and D are transformed into the modes C' and D' to model the realistic homodyne detector with detection efficiency η and electronic noise v_{el} . The measurement results are publicly announced to both sides, Alice and Bob, through the authenticated classical channel.

Next, based on the knowledge from the third party, Charlie, each party (Alice or Bob) can infer the measurement results from the other party. Finally, Alice and Bob can distill a common secret key over a quantum channel by implementing parameter estimation, information reconciliation, and privacy amplification procedures with the aid of an authenticated classical channel. We can calculate the secure key rate of the imbalance CV-MDI-QKD protocol based on the EB scheme. According to ref. [15], the asymptotic secret key rate against collective attacks is given by

$$R = \beta I_{ab} - \chi_E, \quad (1)$$

where β is reconciliation efficiency, I_{ab} is Shannon's mutual information between Alice and Bob after Charlie published the measurements. χ_E is the Holevo bound between Alice and Eve, representing the maximum information that Eve has stolen theoretically.

In this paper, we mainly consider a joint two-mode Gaussian attack. From the perspective way of eavesdropper, the "negative EPR attack" has proven to be an optimal correlated attack, which is the most general eavesdropping strategy for the CV-MDI-QKD protocol (see supplementary information of ref. [15] for more details). The main process of the eavesdropping program is appended two correlative ancillary modes E_1 and E_2 on each channel. Two ancillary modes have the covariance matrix of the form $\sigma_{E_1 E_2} = \begin{bmatrix} \omega_A \mathbf{I} & \mathbf{G} \\ \mathbf{G} & \omega_B \mathbf{I} \end{bmatrix}$, $\mathbf{G} = \begin{bmatrix} g & 0 \\ 0 & g' \end{bmatrix}$, $\mathbf{I} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$. Here, ω_A is the variance of the thermal noise introduced by E_1 in Alice's link, while ω_B is the variances of thermal noise introduced by E_2 in Bob's link. g and g' represent the quantum correlation between the two modes, and must satisfy a set of *bona-fide* conditions.

Then, the Shannon's mutual information between the trusted parties can be expressed as

$$I_{ab} = \frac{1}{2} \log_2 \frac{V_b}{V_b^a}, \quad (2)$$

where V_b and V_b^a denote the variance of the covariance matrices γ_b and γ_b^a , which can be calculated in CV-MDI-QKD protocol (see Appendix B of ref. [45] for more details), respectively.

The Holevo bound χ_E is given by

$$\chi_E = S(\rho_E) - S(\rho_E^a), \quad (3)$$

where $S(\rho)$ is the von Neumann entropy of the quantum state ρ . During the process of calculation, we assume that Eve has a capacity that can purify the whole system within the physical range. This means that the system ABE is pure after Charlie's measurement announcement. So, the equation between two Holevo bounds should satisfy the relation $S(\rho_E) = S(\rho_{AB})$. On account of these assumptions, the Holevo bound can be represented as

$$\chi_E = \sum_{i=1}^2 g\left(\frac{\lambda_i - 1}{2}\right) - \sum_{i=3}^5 g\left(\frac{\lambda_i - 1}{2}\right), \quad (4)$$

where λ_i is the symplectic eigenvalues of the corresponding covariance matrix and $g(x)$ should satisfy the relationship $g(x) = (x + 1)\log_2(x + 1) - x\log_2(x)$.

3. Imbalanced Modulation Influence on the Protocol under the Symmetric Distances

First, we consider the performances of the protocol under the symmetric distance, which means the transmittance distances $L_{AC} = L_{BC}$. The total transmission distance is $L = L_{AC} + L_{BC}$ (we assume that the channel loss is 0.2 dB per km hereafter). The secure key rate and maximum transmission distances using the imbalanced pure squeezed state and coherent state are demonstrated in this section respectively. Without loss of generality, we describe the performance of the protocol in the presence of an arbitrary two-mode Gaussian attack of the links.

We demonstrate the performance of the protocol using coherent state under symmetric distances. Figure 2 shows the contour of the secure key rate versus imbalanced modulation variance of V_A and V_B using the coherent state under symmetric distances and ideal detection. Different from the case of balanced modulation, we can obtain the same secure key rate by means of permutation and combination between V_A and V_B . Meanwhile, the consequence of protocol with balanced modulation is not optimal in comparison to the imbalanced modulation. Without loss of generality, the consequence of balanced modulation is a subset of the imbalanced modulation virtually. In the course of calculating the secret key rate, the equivalent excess noise due to the introduction of thermal noise from Eve in both quantum channels is not symmetric. If Alice is the encoder, Bob can modify his data while Alice keeps hers unchanged during the postprocessing step. This means that the symmetric case cannot result in an optimal system performance and imbalanced variance modulation cannot result in a symmetric secret key rate topological distribution. According to the actual experiment condition, imbalanced modulation variance can improve the performance of the protocol using coherent state. Based on the different modulated modes, we compare the consequence of coherent state protocol between optimal imbalanced modulation and optimal balanced modulation under ideal and practical detection efficiency. As illustrated in Figure 3, it is clear that the secure key rate and maximum transmission distances with imbalanced modulation are always larger than the balanced modulation under different detection efficiency even though just slightly. The dashed lines demonstrate that the imperfection of the detectors decreases the total transmission distances dramatically, but the imbalanced modulation mode is still better than the balanced modulation mode. These results reveal the advantages of the imbalanced modulation variance and provide a modulation method on the premise of guaranteeing the performance parameter.

For the purpose of comparing the performance of the coherent state preparation protocol, the pure squeezed-state protocol using balanced and imbalanced modulation is analyzed under the symmetric distance. As illustrated in Figure 4, we calculate the maximum transmission distance L_{max} , where the border region of secret key rate 10^{-4} bit per pulse is applied to the results as a function of imbalanced squeezed parameters s_A and s_B . We find that multiform arrangements and compositions between imbalanced squeezed parameters s_A and s_B can achieve the same maximum transmission distances. It is clear that the few squeezed-parameter states prepared can cause a more maximum distance of the protocol closer to the bound PLOB [54]. When squeezed parameter s tends to 1, the maximum transmission distances are close to the performance of coherent state protocol. Explicitly, the influence of squeezed parameters s_A and s_B on the secret key rate is nonlinear. In some certain regions, different imbalanced squeezed states have the same effect on maximum transmission distances and secret key rate. In order to achieve the purpose that is as far a distance as possible, Figure 4 also provides proof that as few squeezed parameters are applied to the experiment as possible. In the case of the secret key rate, there is a same similar conclusion, that different combinations of squeezed

parameters in both modulation terminals can obtain the same secret key rate, as shown in Figure 5. The solid and dashed lines represent different detection efficiency $\eta = 1, v_{el} = 0$ and $\eta = 0.97, v_{el} = 0.031$, respectively.

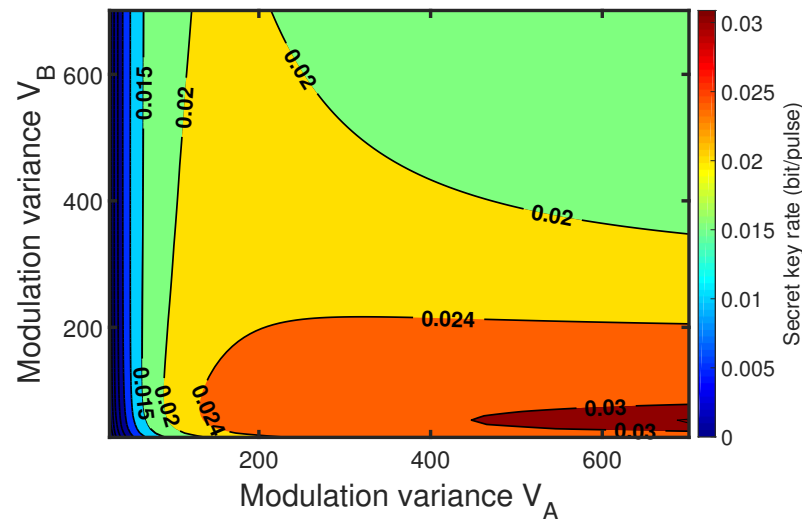


Figure 2. Behavior of the ideal secret key rate in terms of the modulation variance V_A and V_B under symmetric transmission distances ($L_{AC} = L_{BC} = 3$ km). The contour line shows the relationship between $R(V_A, V_B, \epsilon)$ and imbalanced modulation variance V_A and V_B . Here, the reconciliation efficiency $\beta = 0.99$, excess noise $\epsilon_A = \epsilon_B = 0.002$ shot noise units (SNUs), and ideal detection $\eta = 1, v_{el} = 0$.

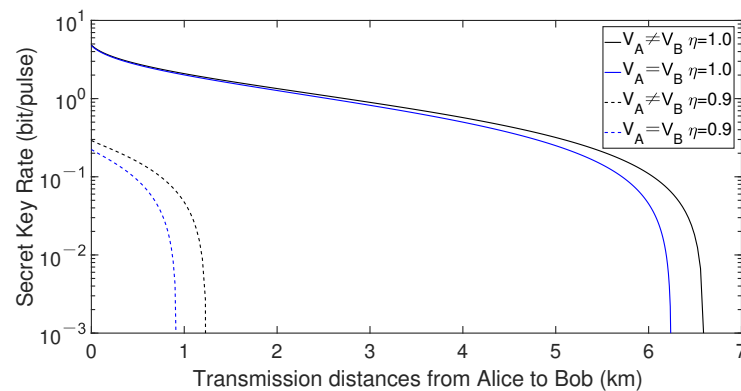


Figure 3. Secret key rate vs. transmission distances in the symmetric case for optimal balanced modulation variance with ideal detection (blue solid line) and optimal imbalanced modulation variance with ideal detection (black solid line), respectively. For comparing the ideal and practical detection efficiency, we set the $\eta = 0.9, v_{el} = 0.031$ (black dashed line) and $\eta = 0.9, v_{el} = 0.031$ (blue dashed line) corresponding to optimal imbalanced and balanced modulation modes, respectively. Here, we set the reconciliation efficiency $\beta = 0.99$, excess noise $\epsilon_A = \epsilon_B = 0.002$ shot noise units (SNUs).

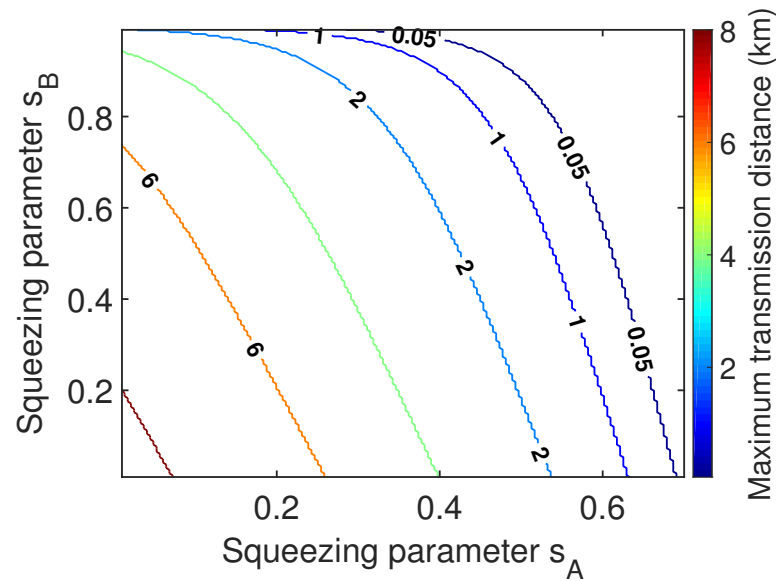


Figure 4. Contour line for maximum transmission distance in symmetric case versus imbalanced squeezed state prepared. Here, we set the reconciliation efficiency $\beta = 0.99$, excess noise $\varepsilon_A = \varepsilon_B = 0.002$ shot noise units (SNUs), and detection efficiency $\eta = 0.95, v_{el} = 0.031$.

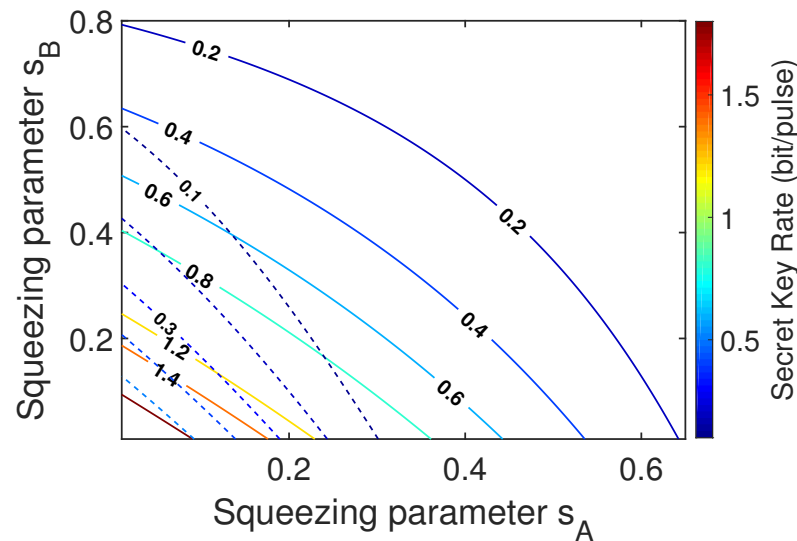


Figure 5. Contour line for secret key rate in symmetric case versus imbalanced squeezed state prepared. Solid lines and dashed lines represent ideal detectors with $\eta = 1, v_{el} = 0$ and imperfect detectors with $\eta = 0.90, v_{el} = 0.031$, respectively. Here, we set the reconciliation efficiency $\beta = 0.99$, symmetric distance is 1 km, excess noise $\varepsilon_A = \varepsilon_B = 0.002$ shot noise units (SNUs).

4. Imbalanced Modulation Influence on the Protocol under the Asymmetric Distances

In this section, we analyze the performance of the protocol using coherent state and squeezed state under the asymmetric distances, because it has been proved that the performance of asymmetric case ($L_{AC} \neq L_{BC}$) is superior to the symmetric case ($L_{AC} = L_{BC}$) [43]. If the terminal of Charlie located close to Alice, the total transmission distance L will increase significantly as L_{AC} decreases. The extreme asymmetric distance case, in which the two-mode Gaussian attack degenerates into two independent Gaussian attacks, is investigated using both the coherent state and squeezed state.

As depicted in Figure 6, we plot the secret key rate R as a function of the total transmission distances for the coherent state with optimal balanced modulation variance and

imbalanced modulation under the case of asymmetric distances. It is clear that the optimal imbalanced modulation variance is always larger than the optimal balanced modulation variance for the secret key rate. When the total distances are less than 15 km, the performance of optimal imbalanced modulation approaches the balanced modulation. As the total distances exceed the 20 km, the secret key rate under the optimal imbalanced modulation is always slightly larger than the balanced modulation. Explicitly, the total maximal transmission distances of imbalanced modulation increase by 2 km compared to the balanced modulation. Furthermore, these results provide proof that imbalanced modulation mode improves the performance of the protocol under the case of asymmetric distances. We can also observe the impact of imperfections of the detectors on the performance of the protocol. Figure 6 also shows that when L_{AC} increases, the transmission distance decreases dramatically. If the position of Charlie is located close to Alice, the total transmission distance can be a relatively longer distance. For instance, if the L_{AC} increases to 0.1 km, the total transmission distance decrease dramatically under both modulation mode. As a contrast, we consider a practical detector that has imperfections such as finite efficiency and electronic noise. These imperfections will increase the thermal noise, which reduces the detection efficiency of Bell state measurements. Thus, the secret key rate and total transmission distances will decrease when the detector is imperfect. For instance, the transmission distance reduces to 12 km when the detector's efficiency is setting to 0.90 depending on certain system parameters.

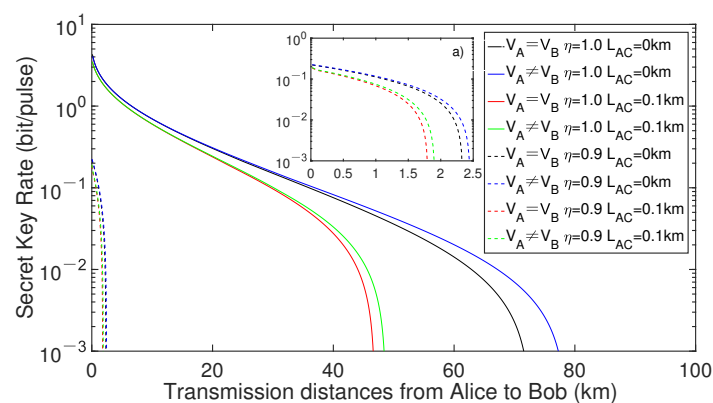


Figure 6. Secret key rate vs. transmission distances given different L_{AC} with ideal and practical detection efficiency under two modulation modes. The solid lines are under the same ideal conditions $\eta = 1, v_{el} = 0$. Optimal imbalanced and balanced modulation correspond to the blue solid line and black solid line in the most asymmetric case, respectively. When the L_{AC} increases to 0.1 km, the relationship between secret key rate and transmission distances are denoted by green solid line and red solid line under different modulation mode. The dash lines are under the same practical conditions $\eta = 0.9, v_{el} = 0.031$ on the inset part. (a) is an amplified graph with $\eta = 0.9, v_{el} = 0.031$. Here, we set the reconciliation efficiency $\beta = 0.99$, excess noise $\varepsilon_A = \varepsilon_B = 0.002$ shot noise units (SNUs).

As mentioned above, we also analyze the available key rate and maximum transmission distances with respect to the imbalanced squeezed degree prepared for the extreme asymmetric distances. The simulation results are shown in Figure 7, where we calculate the maximum transmission distances vs. the imbalanced squeezed state prepared for extreme asymmetric distances. It is clear that there are optimal maximum transmission distances by means of choosing different combinations between squeezed parameters. With the increase in s , the performance of the protocol is not better as the same traditional thinking method. In some tops of curve regions, different imbalanced squeezed degree states prepared can reach the same relatively longer distances. Even though there is a relatively larger difference between s_A and s_B , the maximum transmission distances are influenced slightly. Under the case of extreme asymmetric distances, different combinations of squeezed parameters can achieve different amounts of Shannon's mutual information and Holevo bound χ_E describing Eve's information obtained from the entangling cloner. Asymmetric combina-

tions between squeezed parameters s_A and s_B can obtain a relatively higher secret key rate and transmission distances comparing the commonly used symmetric modulation. The squeezed state reduces the quantum noise in one quadrature of the light field at the expense of increasing the noise in the orthogonal quadrature. By optimizing the squeezed parameters, we minimize the noise in the quadrature that is most sensitive to transmission losses. The chosen squeezed parameters represent an optimal balance between noise reduction and the loss of signal. This character provides a guide for the experiment for squeezed state, which is relatively difficult to prepare in comparison to the coherent state to achieve longer distances and a higher secure key rate. According to this result, we can establish the experiment scheme that compromises between the maximum transmission distances and the squeezed parameter, which is difficult to prepare for the experiment.

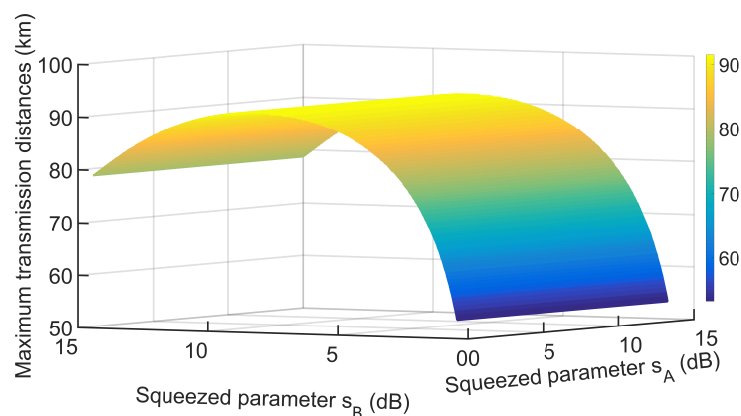


Figure 7. Secure key rate vs. squeezed parameter s_A and s_B in dB unit under the extreme asymmetric distances. Here, we set the reconciliation efficiency $\beta = 0.99$, excess noise $\varepsilon_A = \varepsilon_B = 0.002$ shot noise units (SNUs), and ideal detection $\eta = 1, v_{el} = 0$.

5. Discussion

As the theoretical analysis mentioned above, it may be insufficient to guarantee the realistic implement, which the practical device is imperfect for achieving the ideal protocol performance. Considering the detection noise and source noise, imperfect detector efficiency can be reformulated into quantum efficiency, vacuum electronic noise and source noise. According to the imperfect detector results, it has a guiding significance to experimental preparations. It is possible that these imperfections can be compensated by optical phase-sensitive amplifiers (PSA) [55]. Based on the simulation results for imbalanced modulation, the performance of the CV-MDI-QKD protocol with discrete modulation can be derived, taking the finite-size effect and composable security analysis into account at the same time.

6. Conclusions

In this paper, we have theoretically investigated and analyzed the performance of the protocol using coherent and squeezed states with balanced and imbalanced modulation. Security analysis shows that imbalanced modulation outperforms balanced modulation in both symmetric and extreme asymmetric distances against two-mode Gaussian attack. Furthermore, these simulation results show how to design the modulation mode of the experimental scheme for the purpose of reducing cost and complexity. It is found that there is slight enhancement in the transmission distances with imbalanced modulation using coherent state prepared. In terms of the imbalanced squeezed state prepared, there are optimal squeezed-parameter compositions for maximum transmission distances, and the advantage of the imbalanced state preparation is shown. In practice, imperfect detection efficiency and source noise can influence the performance of the protocol; nevertheless, PSA can be applied to the experiment procedure of the CV-MDI-QKD protocol.

Author Contributions: Conceptualization, W.L.; methodology and investigation, W.L. and Z.L.; software, W.L. and J.B.; validation, W.L. and J.J.; formal analysis, W.L. and Q.J.; resources and data curation, W.L. and J.B.; writing—original draft preparation, W.L.; writing—review and editing, Z.L. and J.J.; visualization, W.L. and Q.J.; supervision, W.L. and Y.T.; project administration, W.L. and G.Z.; funding acquisition, W.L. All authors have read and agreed to the published version of the manuscript.

Funding: This work is supported by the National Natural Science Foundation of China (NSFC) (Grants No. 12104419, No. 12104417 and No. 12104418); the Fundamental Research Program of Shanxi Province (Grants No. 20210302124689, Grants No. 20210302124161, Grants No. 20210302124025).

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: The data that support the findings of the study are available from the first author and the corresponding author upon reasonable request.

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

References

1. Gisin, N.; Ribordy, G.; Tittel, W.; Zbinden, H. Quantum cryptography. *Rev. Mod. Phys.* **2002**, *74*, 145–195.
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*, 1301–1350.
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.
4. Lo, H.K.; Curty, M.; Tamaki, K. Secure quantum key distribution. *Nat. Photon.* **2014**, *8*, 595–604.
5. 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.
6. 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.
7. 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.
8. Lance, A.M.; Symul, T.; Sharma, V.; Weedbrook, C.; Ralph, T.C.; Lam, P.K. No-switching quantum key distribution using broadband modulated coherent light. *Phys. Rev. Lett.* **2005**, *95*, 180503.
9. 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.
10. Lodewyck, J.; Bloch, M.; García-Patrón, R.; Fossier, S.; Karpov, E.; Diamanti, E.; Debuisschert, T.; Cerf, N.J.; McLaughlin, S.W.; Grangier, P.; et al. Quantum key distribution over 25 km with an all-fiber continuous-variable system. *Phys. Rev. A* **2007**, *76*, 042305.
11. Qi, B.; Zhu, W.; Qian, L.; Lo, H.K. Feasibility of quantum key distribution through a dense wavelength division multiplexing network. *New J. Phys.* **2010**, *12*, 103024.
12. Madsen, L.S.; Usenko, V.C.; Lassen, M.; Filip, R.; Andersen, U.L. Continuous variable quantum key distribution with modulated entangled states. *Nat. Commun.* **2012**, *3*, 1083.
13. 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.
14. Kumar, R.; Hao, Q.; Alléaume, R. Coexistence of continuous variable QKD with intense DWDM classical channels. *New J. Phys.* **2015**, *17*, 043027.
15. 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*, 397–403.
16. Walk, N.; Hosseini, S.; Geng, J.; Thearle, O.; Haw, J.Y.; Armstrong, S.J.; Assad, S.M.; Janousek, J.; Ralph, T.C.; Symul, T.; et al. Experimental demonstration of Gaussian protocols for one-sided device-independent quantum key distribution. *Optica* **2016**, *3*, 634–642.
17. Li, Y.M.; Wang, X.Y.; Bai, Z.L.; Liu, W.Y.; Yang, S.S.; Peng, K.C. Continuous variable quantum key distribution. *Chin. Phys. B* **2017**, *26*, 040303.
18. Liu, W.Y.; Wang, X.Y.; Wang, N.; Du, S.N.; Li, Y.M. Imperfect state preparation in continuous-variable quantum key distribution. *Phys. Rev. A* **2017**, *96*, 042312.
19. Liu, W.Y.; Cao, Y.X.; Wang, X.Y.; Li, Y.M. Continuous-variable quantum key distribution under strong channel polarization disturbance. *Phys. Rev. A* **2020**, *102*, 032625.
20. Tian, Y.; Wang, P.; Liu, J.Q.; Du, S.; Liu, W.Y.; Lu, Z.G.; Wang, X.Y.; Li, Y.M. Experimental demonstration of continuous-variable measurement-device-independent quantum key distribution over optical fiber. *Optica* **2022**, *9*, 492–500.

21. Karinou, F.; Brunner, H.H.; Fung, C.H.F.; Comandar, L.C.; Bettelli, S.; Hillerkuss, D.; Kuschnerov, M.; Mikroulis, S.; Wang, D.; Xie, C.S.; et al. Toward the Integration of CV Quantum Key Distribution in Deployed Optical Networks. *IEEE Photon. Tech. Lett.* **2018**, *30*, 650–653.
22. Huang, D.; Lin, D.K.; Wang, C.; Liu, W.Q.; Fang, S.H.; Peng, J.Y.; Huang, P.; Zeng, G.H. Continuous-variable quantum key distribution with 1 Mbps secure key rate. *Opt. Express* **2015**, *23*, 17511–17519.
23. Kleis, S.; Steinmayer, J.; Derksen, R.H.; Schaeffer, C.G. Experimental investigation of heterodyne quantum key distribution in the S-band or L-band embedded in a commercial C-band DWDM system. *Opt. Express* **2019**, *27*, 16540–16549.
24. Eriksson, T.A.; Hirano, T.; Puttnam, B.J.; Rademacher, G.; Luis, R.S.; Fujiwara, M.; Namiki, R.; Awaji, Y.; Takeoka, M.; Wada, N.; et al. Wavelength division multiplexing of continuous variable quantum key distribution and 18.3 Tbit/s data channels. *Commun. Phys.* **2019**, *2*, 9.
25. 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.
26. Huang, D.; Huang, P.; Li, H.S.; Wang, T.; Zhou, Y.M.; Zeng, G.H. Field demonstration of a continuous-variable quantum key distribution network. *Opt. Lett.* **2016**, *41*, 3511–3514.
27. Zhang, Y.C.; Li, Z.Y.; Chen, Z.Y.; Weedbrook, C.; Zhao, Y.J.; Wang, X.Y.; Huang, Y.D.; Xu, C.C.; Zhang, X.X.; Wang, Z.Y.; et al. Continuous-variable QKD over 50 km commercial fiber. *Quantum Sci. Technol.* **2019**, *4*, 035006.
28. Sun, S.H.; Xu, F.H. Security of quantum key distribution with source and detection imperfections. *New J. Phys.* **2021**, *23*, 023011.
29. Jain, N.; Chin, H.M.; Mani, H.; Lupo, C.; Nikolic, D.S.; Kordts, A.; Pirandola, S.; Pedersen, T.B.; Kolb, M.; Ömer, B.; et al. Practical continuous-variable quantum key distribution with composable security. *Nat. Commun.* **2022**, *13*, 4740.
30. García-Patrón, R.; Cerf, N.J. Unconditional optimality of Gaussian attacks against continuous-variable QKD. *Phys. Rev. Lett.* **2006**, *97*, 190503.
31. Navascués, M.; Grosshans, F.; Acín, A. Optimality of Gaussian attacks in continuous-variable quantum cryptography. *Phys. Rev. Lett.* **2006**, *97*, 190502.
32. Wolf, M.M.; Giedke, G.; Cirac, J.I. Extremality of Gaussian quantum states. *Phys. Rev. Lett.* **2006**, *96*, 080502.
33. 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.
34. Leverrier, A.; Grosshans, F.; Grangier, P. Finite-size analysis of a continuous-variable quantum key distribution. *Phys. Rev. A* **2010**, *81*, 062343.
35. Leverrier, A. Composable security proof for continuous-variable quantum key distribution with coherent states. *Phys. Rev. Lett.* **2015**, *114*, 070501.
36. Diamanti, E.; Lo, H.K.; Qi, B.; Yuan, Z.L. Practical challenges in quantum key distribution. *NPJ Quantum Inf.* **2016**, *2*, 16025.
37. Braunstein, S.L.; Pirandola, S. Side-channel-free quantum key distribution. *Phys. Rev. Lett.* **2012**, *108*, 130502.
38. Lo, H.K.; Curty, M.; Qi, B. Measurement-device-independent quantum key distribution. *Phys. Rev. Lett.* **2012**, *108*, 130503.
39. Wang, Q.; Wang, X.B. Efficient implementation of the decoy-state measurement-device-independent quantum key distribution with heralded single-photon sources. *Phys. Rev. A* **2013**, *88*, 052332.
40. Liu, Y.; Chen, T.Y.; Wang, L.J.; Liang, H.; Shentu, G.L.; Wang, J.; Cui, K.; Yin, H.L.; Liu, N.L.; Li, L.; et al. Experimental Measurement-Device-Independent Quantum Key Distribution. *Phys. Rev. Lett.* **2013**, *111*, 130502.
41. Hu, X.L.; Cao, Y.; Yu, Z.W.; Wang, X.B. Measurement-device-independent quantum key distribution over asymmetric channel and unstable channel. *Sci. Rep.* **2018**, *8*, 17634.
42. Liu, H.; Wang, W.Y.; Wei, K.J.; Fang, X.T.; Li, L.; Liu, N.L.; Liang, H.; Zhang, S.J.; Zhang, W.J.; Li, H.; et al. Experimental demonstration of high-rate measurement-device-independent quantum key distribution over asymmetric channels. *Phys. Rev. Lett.* **2019**, *122*, 160501.
43. Li, Z.Y.; Zhang, Y.C.; Xu, F.H.; Peng, X.; Guo, H. Continuous-variable measurement-device-independent quantum key distribution. *Phys. Rev. A* **2014**, *89*, 052301.
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.
45. Wang, P.; Wang, X.Y.; Li, Y.M. Continuous-variable measurement-device-independent quantum key distribution using modulated squeezed states and optical amplifiers. *Phys. Rev. A* **2019**, *99*, 042309.
46. Zheng, Y.; Shi, H.B.; Pan, W.; Wang, Q.T.; Mao, J.H. Security Analysis of Continuous-Variable Measurement-Device-Independent Quantum Key Distribution Systems in Complex Communication Environments. *Entropy* **2022**, *24*, 127.
47. Song, T.T.; Wen, Q.Y.; Guo, F.Z.; Tan, X.Q. Finite-key analysis for measurement-device-independent quantum key distribution. *Phys. Rev. A* **2012**, *86*, 022332.
48. Curty, M.; Xu, F.H.; Gui, W.; Lim, C.C.W.; Tamaki, K.; Lo, H.K. Finite-key analysis for measurement-device-independent quantum key distribution. *Nat. Commun.* **2014**, *5*, 3732.
49. Papanastasiou, P.; Ottaviani, C.; Pirandola, S. Finite-size analysis of measurement-device-independent quantum cryptography with continuous variables. *Phys. Rev. A* **2017**, *96*, 042332.
50. Ma, X.F.; Fung, C.H.F.; Razavi, M. Statistical fluctuation analysis for measurement-device-independent quantum key distribution. *Phys. Rev. A* **2012**, *86*, 052305.

51. Yu, Z.W.; Zhou, Y.H.; Wang, X.B. Statistical fluctuation analysis for measurement-device-independent quantum key distribution with three-intensity decoy-state method. *Phys. Rev. A* **2015**, *91*, 032318.
52. Wang, C.; Yin, Z.Q.; Wang, S.; Chen, W.; Guo, G.C.; Han, Z.F. Measurement-device-independent quantum key distribution robust against environmental disturbances. *Optica* **2017**, *4*, 1016–1023.
53. Zang, Y.C.; Li, Z.Y.; Yu, S.; Gu, W.Y.; Peng, X.; Guo, H. Continuous-variable measurement-device-independent quantum key distribution using squeezed states. *Phys. Rev. A* **2014**, *90*, 052325.
54. Pirandola, S.; Laurenza, R.; Ottaviani, C.; Banchi, L. Fundamental limits of repeaterless quantum communications. *Nat. Commun.* **2009**, *42*, 114014.
55. Fossier, S.; Diamanti, E.; Debuisschert, T. Improvement of continuous-variable quantum key distribution systems by using optical preamplifiers. *J. Phys. B At. Mol. Opt.* **2009**, *42*, 114014.

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.