photonics

MDPI

Article

Continuous-Variable Measurement-Device-Independent Quantum Key Distribution in the Terahertz Band

Haoxin Liu [1,2], Zhe Yang [1,2,*], Shuoyu Yang [1], Dongyun Sun [1,2] and Cunlin Zhang [1,2,*]

[1] Department of Physics, Capital Normal University, Beijing 100048, China; 2210602067@cnu.edu.cn (H.L.); 1200603025@cnu.edu.cn (S.Y.); 2220602055@cnu.edu.cn (D.S.)
[2] Key Laboratory of Terahertz Optoelectronics (MoE), Capital Normal University, Beijing 100048, China
* Correspondence: yangzhe7010@cnu.edu.cn (Z.Y.); cunlin_zhang@cnu.edu.cn (C.Z.)

Abstract: We have introduced, for the first time, a protocol for Continuous-Variable Measurement-Device-Independent Quantum Key Distribution (CV-MDI-QKD) in the terahertz (THz) frequency band. We have conducted a secret key rate analysis against collective attacks. The proposed THz CV-MDI-QKD is immune to all detector attacks, significantly enhancing the security assurance of practical THz CVQKD implementations. Furthermore, we investigated the impact of finite key length (the finite-size effect) and finite reconciliation efficiency on the performance of practical THz CV-MDI-QKD systems. Our findings reveal that by employing a large number of keys or signals and optimizing the modulation variance, the detrimental effects arising from the finite-size effect and suboptimal reconciliation efficiency can be notably mitigated. These insights play a crucial role in advancing the feasibility of THz CVQKD technology towards practical applications.

Keywords: terahertz communication; continuous variable; measurement device independent; quantum key distribution

check for updates

Citation: Liu, H.; Yang, Z.; Yang, S.; Sun, D.; Zhang, C. Continuous-Variable Measurement-Device-Independent Quantum Key Distribution in the Terahertz Band. *Photonics* **2024**, *11*, 367. https://doi.org/10.3390/photonics11040367

Received: 6 October 2023
Revised: 5 November 2023
Accepted: 7 November 2023
Published: 15 April 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/).

1. Introduction

Quantum key distribution (QKD) enables the establishment of theoretically unconditionally secure keys between legitimate communicating parties, Alice and Bob [1,2], even in the presence of an eavesdropper (Eve) on the channel. Due to the substantial demand for secure communication, the development of quantum key distribution has rapidly progressed and entered practical stages [3,4]. QKD can be implemented using continuous-variable quantum systems (such as optical field quadratures) or discrete variable systems (such as discrete polarization or phase of light), known as CVQKD and DVQKD [5–8], respectively. Notably, the CVQKD protocol represented by GG02 does not require single-photon sources or detectors, making it compatible with existing optical communication devices and thus highly practical [9,10].

CVQKD has achieved significant progress in both theory and experiments [11–16]. In the theory of CVQKD, Ghorai S. et al. established a lower bound on the asymptotic secret key rate of CVQKD with a discrete modulation of coherent states in 2019 [11]. In 2019, Lin J. et al. analyzed the security of discrete-modulation protocols against collective attacks in the asymptotic limit [12]. In 2021, Liu W. B. et al. proposed a homodyne detection protocol using the quadrature phase shift keying technique which enhances excess noise tolerance to a high level [13]. In 2023, Kanitschar F. et al. presented a composable finite-size security proof against independently and identically distributed collective attacks for a general Discrete-Modulated CVQKD protocol [14]. And in an experiment, Zhang Y. et al. reported two different field tests of a CVQKD system through commercial fiber networks in Xi'an and Guangzhou over distances of 30.02 km (12.48 dB) and 49.85 km (11.62 dB) in 2019 [15]. In 2020, Zhang Y. et al. reported a 202.81 km optical fiber CVQKD experiment [16].

Terahertz (THz) waves generally refer to electromagnetic waves with frequencies ranging from 0.1 THz (wavelength 3000 μm) to 10 THz (wavelength 30 μm) [17–19]. Compared

to free-space optical communication, THz waves are less affected by atmospheric conditions such as dust, smoke, fog, and turbulence [20–24], making THz QKD a subject of extensive scientific interest [25–34]. Due to the immature development of single-photon detectors in the THz range [35], THz CVQKD holds more promise for experimental verification compared to THz DVQKD [25,26]. Currently, there has been substantial research on THz CVQKD in both ground-based atmospheric environments [36] and space environments [37]. THz CVQKD achieves transmission distances of up to 200 m in ground-based atmospheric environments [38] and several hundred kilometers in space [39].

Although THz CVQKD is theoretically unconditionally secure, the imperfections in experimental devices, resulting in a mismatch between actual devices and ideal models, lead to gaps between practical THz CVQKD systems and ideal protocols. This exposes the security of practical THz QKD systems to significant challenges, as Eve can exploit the gaps between devices and theoretical models to launch attacks on the protocol. Among these attacks, attacks on detectors play a major role, including local oscillator attacks, wavelength attacks, detector blinding attacks [40–44], and so on. To address the security vulnerabilities of detectors of the practical THz CVQKD, inspired by optical-waveband measurement-device-independent (MDI) QKD [45–49], we introduce THz CV-MDI-QKD. MDI-QKD is a protocol immune to detector attacks, where Alice and Bob send unrelated quantum states to an untrusted third party, Charlie. Charlie measures the received quantum states and discloses the measurement results. Alice and Bob process their respective data based on the disclosed measurement results to obtain secure keys [48,49].

However, due to the unique characteristics of the THz range, where THz QKD key rates are significantly affected by noise photons generated by environmental temperature [27,28], the analysis results of the THz band are significantly different from those of the optical band. This paper presents the first theoretical analysis of THz CV-MDI-QKD and thoroughly investigates the relationship between the protocol's key rate and transmission distance. Considering the finite-size effect in practical QKD systems is essential, as the number of keys (signals) sent by the practical system is finite, while theoretical analysis assumes infinite key length. The limited signal number leads to biases in estimating channel transmittance and excess noise between legitimate communicating parties in the practical QKD system, resulting in an overestimation of secure key rates and causing security vulnerabilities [50–53]. The solution involves estimating the channel transmittance and excess noise under adverse conditions for the practical THz CV-MDI-QKD system, in order to prevent the overestimation of secure key rates. We analyze the relationship between the THz CV-MDI-QKD key rate and transmission distance under the finite-size effect, aligning our analysis more closely with the operational state of the THz CV-MDI-QKD protocol. Additionally, due to the impact of limited reconciliation efficiency ($\beta < 1$), the maximum secure transmission distance of THz CV-MDI-QKD keys decreases. Fortunately, we demonstrate that selecting optimal modulation variances can enhance both key rates and transmission distances.

In conclusion, this paper emphasizes the enhancement of security and practicality in THz CVQKD systems. Our proposed THz CV-MDI-QKD protocol addresses detector vulnerabilities in THz CVQKD. We also study optimal modulation variances in THz CV-MDI-QKD, which partially resolve the decrease in key transmission distance caused by finite reconciliation efficiency in practical THz CV-MDI-QKD systems. Our work contributes to advancing THz QKD towards practical applications.

2. THz Continuous-Variable Measurement-Device-Independent QKD Protocol

2.1. Basic Principles of THz CV-MDI-QKD

The prepare-and-measure (PM) model of THz CV-MDI-QKD is illustrated in Figure 1a. The protocol proceeds as follows: Alice (Bob) prepares N Gaussian coherent states $|q_A + ip_A >$ ($|q_B + ip_B >$), where q_A (q_B) and p_A (p_B) are Gaussian distributions with modulation variances V_{AS} (V_{BS}), and sends them through the quantum channel to Charlie.

The state $|q_A + ip_A>$ is denoted as A, and the state $|q_B + ip_B>$ is denoted as B. The channel lengths are L_{AC} (for Alice to Charlie) and L_{BC} (for Bob to Charlie).

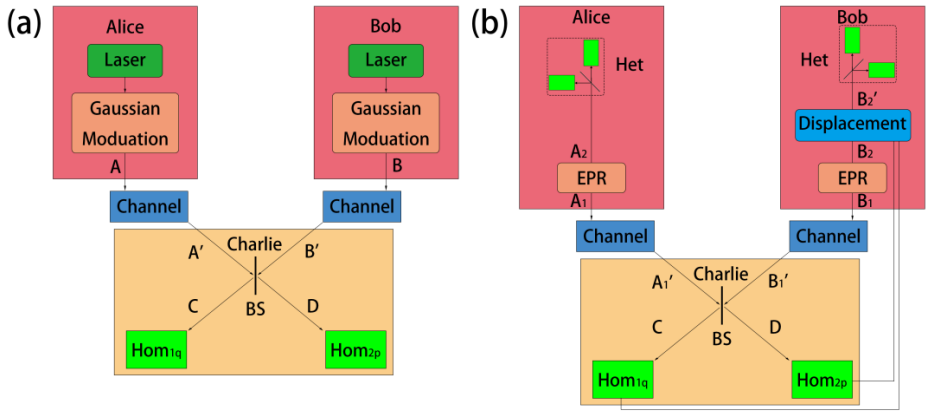

Figure 1. (**a**) The prepare-and-measure (PM) model of THz CV-MDI-QKD. BS: beam splitter, Hom: homodyne detections; (**b**) the entanglement-based (EB) model of THz CV-MDI-QKD, Het: heterodyne detections.

Upon receiving the coherent states from Alice and Bob, Charlie employs a 50:50 beam splitter (BS) to interfere with the received Gaussian states A' and B', creating two output modes, C and D. Charlie then measures both the q-quadrature of mode C and the p-quadrature of mode D using homodyne detections (Hom) and subsequently announces the measurement results $\{Q_C, P_D\}$ to Alice and Bob. Following this, Bob applies a displacement operation to his data, $Q_B = q_B + sQ_C$, $P_B = p_B - sP_D$, based on Charlie's announced measurement results. In quantum optics, the displacement operator can shift a coherent state from one position in phase space to another, thereby obtaining another coherent state. Specifically, a coherent state is typically defined as a state obtained by applying the corresponding displacement operator to the quantum vacuum state. The amplification coefficient s in the PM scheme is described as follows:

$$s = \frac{g}{\sqrt{\frac{V_B - V_0}{V_B + V_0}}}, \tag{1}$$

where the variable g represents the gain of the displacement. Meanwhile, Alice retains her data unchanged: $Q_A = q_A$, $P_A = p_A$.

When Alice and Bob gather sufficient correlated data, they perform parameter estimation through the public channel. Subsequently, through steps such as data reconciliation and privacy amplification, Alice and Bob can share a secure key.

As shown in Figure 1b, the entanglement-based (EB) model of CV-MDI-QKD is as follows: Alice (Bob) prepares N entangled two-mode squeezed states (EPR states) with modulation variances V_A (V_B). Keeping one mode A_2 (B_2), Alice (Bob) sends the other mode A_1 (B_1) to a third party, Charlie. Subsequently, Charlie combines two received modes $A_1{}'$ and $B_1{}'$ using a 50:50 BS and measures the q-quadrature of mode C and the p-quadrature of mode D with homodyne detections, publicly announcing the measurement results $\{Q_C, P_D\}$ to Alice and Bob through classical channels.

Subsequently, Alice directly performs heterodyne detections on the retained mode A_2 to obtain the data $\{Q_A, P_A\}$. Bob applies a displacement operation $\hat{D}(\beta)$ to mode B_2 and obtains $\hat{\rho}_{B_2{}'} = \hat{D}(\beta)\hat{\rho}_{B_2}\hat{D}^{\dagger}(\beta)$, where $\hat{\rho}_{B_2}$ represents the density matrix of mode B_2, $\beta = g(Q_C + iP_D)$. Then, Bob performs heterodyne detections to mode $B_2{}'$ and obtains the data $\{Q_B, P_B\}$. Finally, Alice and Bob perform parameter estimation, data reconciliation, and privacy amplification on the measured data, ultimately sharing a secure key.

It has been proven that the PM model of CV-MDI-QKD is equivalent to the EB model of CV-MDI-QKD [48]. In quantum communication, the PM model is experimentally

feasible, while the EB model is commonly used for theoretical analysis and security proofs. Therefore, for the security analysis of THz CV-MDI-QKD, we employ the EB model. In fact, if Bob's EPR state preparation and displacement operation are untrusted, the EB scheme of CV-MDI-QKD is essentially equivalent to coherent-state-based one-way CVQKD with heterodyne detections [48,53].

2.2. Terahertz Parameter

The key distinction between THz QKD and standard QKD lies in the fact that THz QKD cannot neglect the impact of thermal photon noise caused by environmental temperature. According to the blackbody radiation formula, the average number of noise photons $\overline{n}$ generated by temperature is:

$$\overline{n} = \frac{1}{e^{hf/k\tau} - 1}, \tag{2}$$

where h represents the Planck constant, τ stands for temperature, k denotes the Boltzmann constant, and f represents communication frequency. It can be observed that, at the same temperature, a lower frequency f corresponds to a larger $\overline{n}$. For instance, at a temperature of 288 K, with $f = 300$ GHz, $\overline{n}$ is 19.5; for $f = 1$ THz, $\overline{n}$ is 5.5; and for $f = 193.5$ THz (wavelength of 1550 nm), $\overline{n}$ is 10^{-14}.

The thermal noise variance V_0, which is called the 'terahertz parameter' [38], can be described using $\overline{n}$:

$$V_0 = 2\overline{n} + 1. \tag{3}$$

The THz parameter V_0 plays a significant role in THz CV-MDI-QKD. When Alice (Bob) prepares coherent states $|q_A + ip_A >$ ($|q_B + ip_B >$), the modulation variance is $V_{AS}(V_{BS})$, but in reality, the overall variance of the coherent state is $V_A = V_{AS} + V_0(V_B = V_{BS} + V_0)$. This is because environmental thermal noise photons introduce additional quantum shot noise on the modulated coherent state [28].

In the visible light range or near-infrared range (1550 nm), $\overline{n}$ is extremely small, and the parameter V_0 is assumed to be 1 SNU (Standard Noise Unit). Therefore, in optical research papers of CVQKD, the value of V_0 is usually set to 1 [48,54]. However, in the THz range, due to the non-negligible value of $\overline{n}$, V_0 in THz CVQKD is greater than 1. Therefore, special attention is required for this parameter, and it will severely impact the secure key rate of THz CV-MDI-QKD.

To provide a clearer illustration of how the THz parameter V_0 changes with frequency f at room temperature (288 K), we have plotted Figure 2. It can be seen that in the optical range (the typical optical QKD band ranges from 800 nm to 1650 nm), V_0 approaches 1, while for the Thz band with lower frequencies, the numerical values of V_0 are larger than 1. A larger V_0 represents higher thermal photon noise, providing Eve with more opportunities to conceal her activities [27].

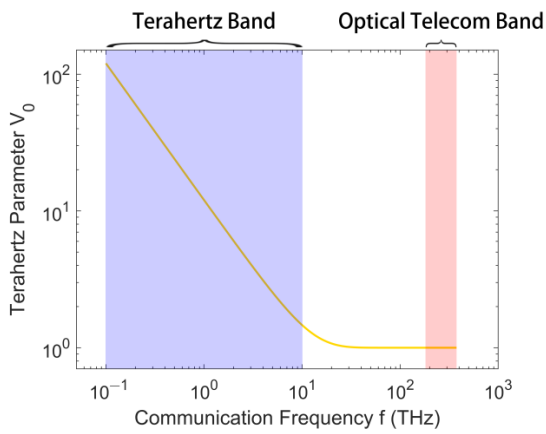

Figure 2. Terahertz parameter (V_0) changes with communication frequency (f).

2.3. Channel Analysis for THz CV-MDI-QKD

The path loss experienced by the THz wave in the atmospheric environment is primarily due to three factors [55–57]: free-space path loss (L_{FS}), atmospheric molecular absorption loss (L_{AL}), and miscellaneous loss (L_{ML}). The miscellaneous loss is caused by the reflection and scattering of matter along the path and can usually be neglected in THz CVQKD. The free-space path loss (L_{FS}) can be expressed as:

$$L_{FS} = 20lg\left(\frac{4\pi d}{\lambda}\right) - G_{TX} - G_{RX}, \tag{4}$$

where G_{TX} and G_{RX} represent the gains of the transmitter and receiver antennas, respectively, and λ is the wavelength. It can be observed that we can compensate for the signal loss caused by free-space path loss by adjusting the gains of the transmitting and receiving antennas. Consequently, in this paper, we will focus on the impact of atmospheric molecular absorption loss on THz CV-MDI-QKD systems.

The channel characteristics of THz CV-MDI-QKD are determined by the channel transmittance function T and the channel excess noise ξ. The channel transmittance function T is given by:

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

where α represents the channel's attenuation coefficient, with its primary contribution being atmospheric absorption loss, and L denotes the transmission distance. In atmospheric channels, different frequencies are associated with distinct α values. Figure 3 provides the attenuation coefficients of electromagnetic waves at different frequencies under various atmospheric conditions.

This paper primarily focuses on the atmospheric attenuation coefficients corresponding to different THz frequencies under standard conditions. In this paper, we analyzed frequencies of 200 GHz (0.2 THz), 900 GHz (0.9 THz), and 10 THz, corresponding to α values of 1.2 dB/km, 100 dB/km, and 1000 dB/km, respectively [38]. Also, we analyzed 30 THz corresponding to α of 50 dB/km, which is often considered in extended THz QKD research [38].

In the THz CVQKD protocol, the noise in the channel from Alice to Charlie is represented as χ_1:

$$\chi_1 = (1 - T_1)/T_1 + \xi_1, \tag{6}$$

where T_1 and ξ_1 are the transmittance and channel excess noise of the channel from Alice to Charlie, respectively.

Similarly, the noise in the channel from Bob to Charlie is represented as χ_2, while T_2 and ξ_2 are the transmittance and excess noise of the channel from Bob to Charlie, respectively. In this paper, both ξ_1 and ξ_2 are set to 0.002.

It is important to note that the total channel of the THz CV-MDI-QKD system includes both the channel from Alice to Charlie (L_{AC}) and the channel from Bob to Charlie (L_{BC}). Upon the work of Li Z. Y. et al. in 2014 [48], the equivalent transmittance of the protocol channel needs to be calculated:

$$T = \frac{T_1}{2}g^2. \tag{7}$$

Additionally, the equivalent excess noise of the total channel in the THz frequency range is denoted as ξ':

$$\xi' = 1 + \frac{1}{T_1}[T_2(\chi_2 - 1) + T_1\chi_1] + \frac{1}{T_1}\left(\frac{\sqrt{2}}{g}\sqrt{V_B - V_0} - \sqrt{T_2}\sqrt{V_B + V_0}\right)^2. \tag{8}$$

It should be noted that the THz parameter V_0 significantly affects ξ', yielding a different form of Equation (8) from that in the optical band [48].

To minimize the above equivalent excess noise, it is easy to derive the value of g as:

$$g = \sqrt{\frac{2}{T_2}}\sqrt{\frac{V_B - V_0}{V_B + V_0}}. \tag{9}$$

According to Equation (9), the equivalent excess noise ξ' is given by:

$$\xi' = \xi_1 + \frac{1}{T_1}[T_2(\xi_2 - 2) + 2]. \tag{10}$$

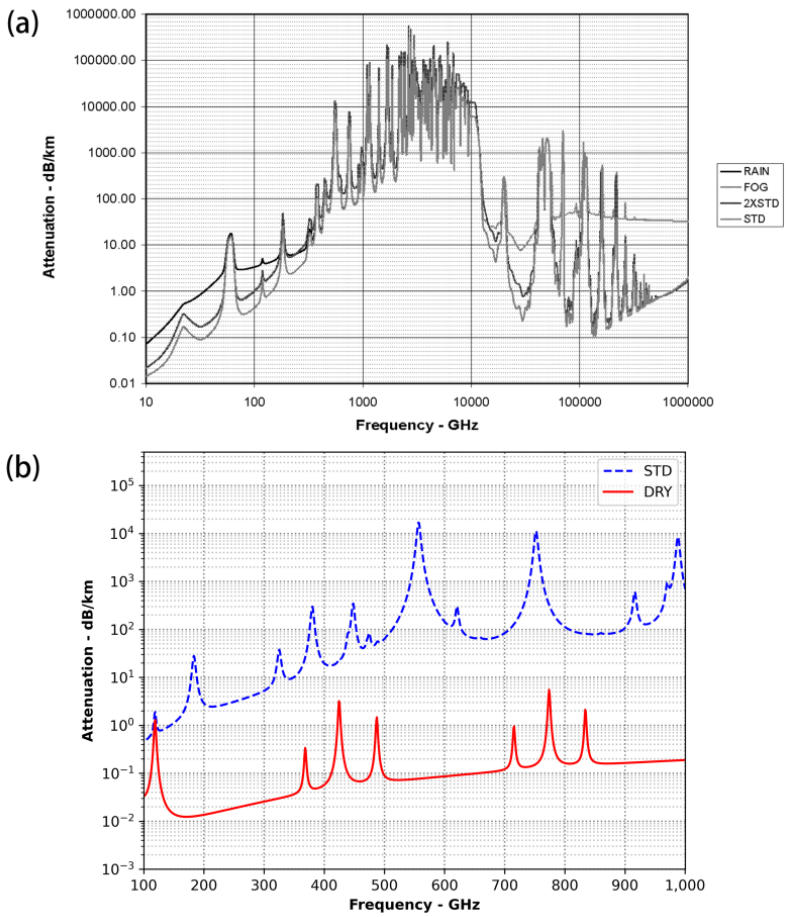

Figure 3. (**a**) Atmospheric attenuation across the electromagnetic spectrum at sea level based on currently accepted models. Atmospheric pressure P is 1013.25 hPa. Rain = 4 mm/h, fog = 100 m visibility, STD (standard atmosphere) = 7.5 g/m^3 water vapor, and 2XSTD = 15 g/m^3 water vapor (excerpted from Rosker M. L. et al. [58]). (**b**) Atmospheric attenuation in the frequency range of 100 GHz to 1 THz (drawn according to ITU-R P.676-12 [59,60])). STD means standard atmosphere with 7.5 g/m^3 water vapor, 15 °C temperature (288 K), and 1013.25 hPa atmospheric pressure. DRY means dry atmosphere.

3. Analysis of Secure Key Rates for THz CV-MDI-QKD

Based on the EB model, we analyzed the relationship between the secure key rate and distance of THz CV-MDI-QKD under Gaussian collective attacks [61–63]. In the EB model, it is assumed that the channels from Alice to Charlie and from Bob to Charlie are subjected to two independent entanglement-cloning attacks. Charlie conducts the standard CV entanglement swapping process as required by the EB model. Therefore, the formula for the secure key rate of THz CV-MDI-QKD under Gaussian collective attacks is given by [54]:

$$R = \beta I(A:B) - S(B:E), \tag{11}$$

where $I(A:B)$ represents the mutual information between Alice and Bob, β is the reconciliation efficiency in the post-processing, and $S(B:E)$ stands for the von Neumann entropy between Bob and Eve.

Next, we will analyze the specific forms of each term in Equation (11). It is worth noting that the THz parameter V_0 will significantly impact the two terms in Equation (11).

In the first part of Equation (11), the mutual information between Alice and Bob in THz CV-MDI-QKD is given by [28,48,53]:

$$I(A:B) = log_2\left[\frac{T(V_A+\chi)+1}{T(V_0+\chi)+1}\right]. \tag{12}$$

According to Williamson's theorem [64], von Neumann entropy $S(B:E)$ is given by:

$$S(B:E) = G[(\lambda_1-1)/2] + G[(\lambda_2-1)/2] - G[(\lambda_3-1)/2], \tag{13}$$

where $G(X) = (x+1)log_2(x+1) - xlog_2x$.

Specifically, in the first two terms of Equation (13), λ_1 and λ_2 are the symplectic eigenvalues of the covariance matrix $\gamma_{A_1B_1'}$ between Alice and Bob [48]. The matrix $\gamma_{A_1B_1'}$ is defined as:

$$\gamma_{A_1B_1'} = \begin{pmatrix} aI & c\delta_z \\ c\delta_z & bI \end{pmatrix}, \tag{14}$$

where the symplectic eigenvalues λ_1 and λ_2 are:

$$\lambda_{1,2} = \sqrt{\frac{1}{2}\left[a \pm \sqrt{a^2-4b^2}\right]}. \tag{15}$$

The values of the matrix elements in Equations (14) and (15) are as follows:

$$I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \qquad \delta_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \tag{16}$$

$$a = V_A = V_{AS} + V_0, \tag{17}$$

$$b = T(V_A+\chi) = t^2(V_{AS}+V_0-1)+\delta^2, \tag{18}$$

$$c = \sqrt{T\left({V_A}^2-1\right)} = t\sqrt{(V_{AS}+V_0)^2-1}, \tag{19}$$

where the definitions of the channel transmittance coefficient t and the variance of channel excess noise δ^2 are given by:

$$t = \sqrt{T}, \tag{20}$$

$$\delta^2 = 1 + T\xi'. \tag{21}$$

For the eigenvalues λ_3 in Equation (13), considering the essence of the EB model of THz CV-MDI-QKD and its equivalence to coherent-state-based heterodyne detection CVQKD [48,53], we can derive:

$$\lambda_3 = a - c^2/(b+1). \tag{22}$$

Combining Equations (11)–(13), (15) and (22), we can calculate the secure key rate for THz CV-MDI-QKD.

Finally, it can be observed that in previous optical QKD research [48,54], all the V_0 mentioned above were directly replaced with the number 1, resulting in significant distinctions with THz QKD. In conclusion, the THz QKD and optical QKD theories have significant differences because of the THz parameter V_0.

As depicted in Figure 4, we show the secure key rates R of THz CV-MDI-QKD with the transmission distance L at different THz frequencies. In this case, we consider the scenario where both channels have equal lengths, i.e., $L_{AC} = L_{BC}$, resulting in a total channel length of $L = L_{AC} + L_{BC}$. The reconciliation efficiency β is set to 1, and the modulation variances $V_{AS} = V_{BS} = 100,000$.

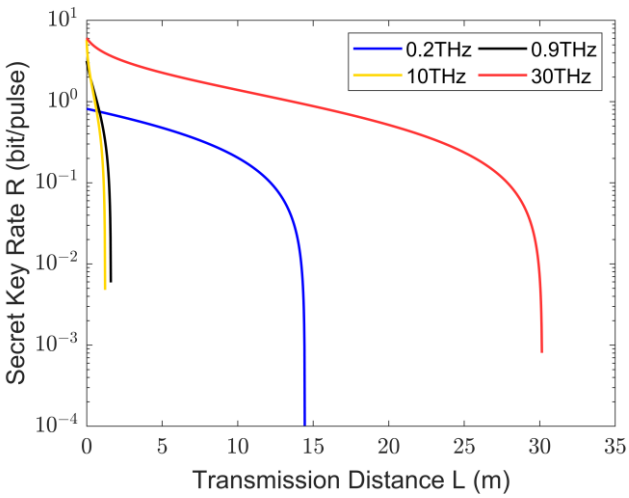

Figure 4. Secure key rates of THz CV-MDI-QKD change with transmission distances L at equal lengths of L_{BC} and L_{AC} for different THz frequencies.

Another important scenario arises when Charlie's interferometric measurement setup is placed adjacent to Bob's. In this case, $L_{BC} = 0$, indicating that the total channel length is $L = L_{AC}$. The key rates and transmission distances for different THz frequencies of CV-MDI-QKD in this case are shown in Figure 5.

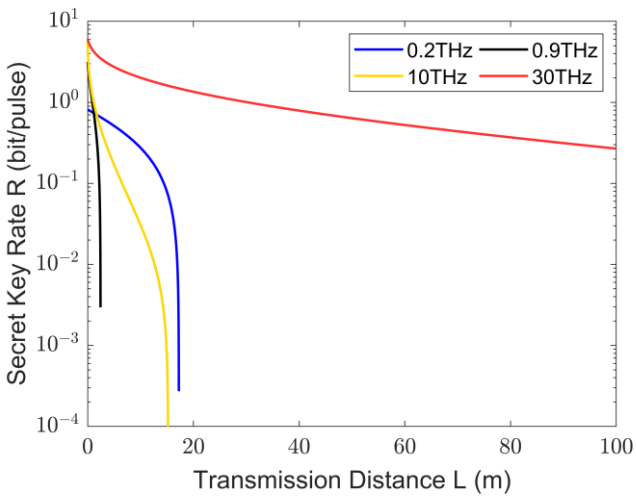

Figure 5. Secure key rates of THz CV-MDI-QKD changes with transmission distances when $L_{BC} = 0$ and $L = L_{AC}$ for different THz frequencies.

Comparing Figures 4 and 5 reveals that the transmission distance of THz CV-MDI-QKD is significantly longer when Charlie's interferometric measurement setup is placed adjacent to Bob than that in the case of equal-length channels. In practical applications, this asymmetric arrangement of THz CV-MDI-QKD can be leveraged to enhance the key rate and secure the transmission distance.

To illustrate the differences between THz CVQKD and THz CV-MDI-QKD, we present the key rates and transmission distances of THz CVQKD in Figure 6. Considering the equivalence of MDI-QKD and the coherent-state heterodyne detection CVQKD (with

reverse reconciliation) [48], we selected the reverse reconciliation coherent-state heterodyne detection THz CVQKD for comparison.

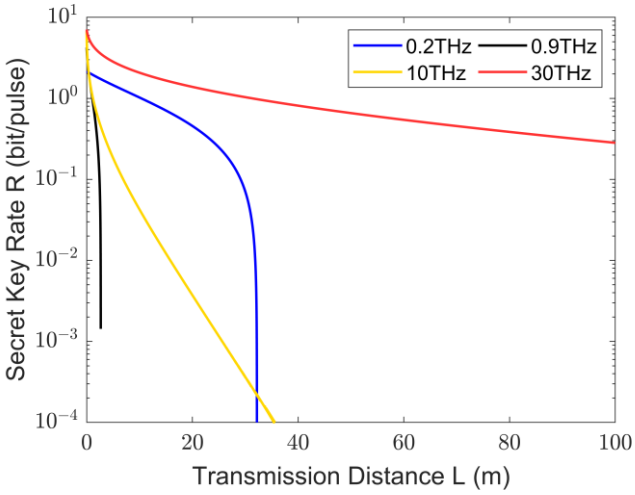

Figure 6. Secure key rates of THz CVQKD change with transmission distances when $L_{BC} = 0$ and $L = L_{AC}$ for different THz frequencies.

The important parameters for them are the same: $L_{BC} = 0$; the reconciliation efficiency $\beta = 1$; the modulation variance $V_{AS} = V_{BS} = 100,000$; and frequencies of 0.2 THz, 0.9 THz, 10 THz, and 30 THz.

By comparing Figures 5 and 6, we can conclude that THz CV-MDI-QKD offers lower distance but higher security, whereas THz CVQKD provides greater distance at the cost of lower practical security. This is due to the design of the MDI protocol; the communication between Charlie and Bob inevitably introduces extra quantum noise, resulting in a reduction in the secure key rate.

4. The Finite-Size Effect and Suboptimal Reconciliation Efficiency for THz CV-MDI-QKD

4.1. Impact of the Finite-Size Effect

The preceding section analyzed the theoretical model and theoretical transmission efficiency of THz CV-MDI-QKD under collective Gaussian attacks, assuming an infinite amount of data. However, in practical QKD systems, the number of transmitted keys and the amount of data employed by both Alice and Bob for parameter estimation are finite. To bring the analysis of the THz CV-MDI-QKD protocol closer to practical scenarios, in this section, we delve into the discussion of the relationship between key rate and transmission distance in THz CV-MDI-QKD under the finite-size effect [50]:

$$R = \frac{n}{N}[\beta I(A:B) - S_{\epsilon_{PE}}(B:E) - \Delta(n)], \tag{23}$$

where N represents the total length of data exchanged between the communicating parties; $n = N - m$, where m signifies the data length used for estimating the parameters t and δ^2 mentioned earlier. In this study, m is set to be half of N. Actually, the values of N and m are always finite. Consequently, the estimation of t and δ^2 through limited samples is not accurate, leading to incorrect assessments of the amount of information Eve can potentially intercept, resulting in security vulnerabilities.

Therefore, it is necessary to adjust the conditional entropy $S(B:E)$ in Equation (11) to $S_{\epsilon_{PE}}(B:E)$, which, considers the probability of errors occurring during the parameter estimation process. The ϵ_{PE} is the failure probability of parameter estimation, with ϵ_{PE} taking 10^{-10}. The adjustment approach involves estimating parameter t with a minimum value assumption and estimating parameter δ^2 with a maximum value assumption, thus correcting the impact of the finite-size effect on the key rate.

Specifically, it is necessary to adjust Equations (20) and (21) by substituting t with t_{min} and δ^2 with, respectively:

$$t_{min} = \sqrt{T} - Z_{\epsilon_{PE}/2}\sqrt{\frac{\delta^2}{mV_{AS}}}, \tag{24}$$

$$\delta^2_{max} = 1 + T\xi' + Z_{\epsilon_{PE}/2}\frac{\sqrt{2}\delta^2}{\sqrt{m}}, \tag{25}$$

where $Z_{\epsilon_{PE}/2}$ is $2 - erf\left(0.5Z_{\epsilon_{PE}/2}\right) = \epsilon_{PE}$, and when ϵ_{PE} takes 10^{-10}, its value is about 6.5.

And the third part of Equation (23) $\Delta(n)$ is related to the security of private key amplification:

$$\Delta(n) = (2dimH_X + 3)\sqrt{\frac{log_2(2/\overline{\epsilon})}{n}} + \frac{2}{n}log_2\frac{1}{\epsilon_{PA}}, \tag{26}$$

Among them, H_x represents the Hilbert space corresponding to the variable x used in the original key, and the value of $dimH_x$ is 2.

The post-processing procedure of THz CV-MDI-QKD comprises three stages, namely parameter estimation, data reconciliation, and privacy amplification. The global security parameters for these three stages are defined as follows:

$$\epsilon = \epsilon_{PE} + \epsilon_{EC} + \overline{\epsilon} + \epsilon_{PA}, \tag{27}$$

Among them, ϵ_{PE} is the failure probability of parameter estimation, ϵ_{EC} represents the probability of data reconciliation failures, $\overline{\epsilon}$ is a smoothing parameter, and ϵ_{PA} represents the failure probability of the privacy amplification procedure. The post-processing procedure is essentially a data processing step and is unrelated to the wavelength in the communication process. Therefore, when discussing the finite-size effects of CVQKD [41,50] and THz CVQKD [30], optimized parameters can be applied. In this paper, ϵ_{PE}, ϵ_{EC}, $\overline{\epsilon}$, and ϵ_{PA} are all taken as 10^{-10}, which is consistent with other related works.

The relationship between the key rate and distance of THz CV-MDI-QKD under the finite-size effect calculated according to Equation (23) is shown in Figure 7. For the convenience of comparison, we set the important parameters in Figure 7 to be consistent with Figure 5, namely $L_{BC} = 0$ (Charlie's measuring equipment is placed at Bob's end), modulation variance $V_{AS} = V_{BS} = 100000$, and coordination efficiency $\beta = 1$. We investigated the relationship between the CV-MDI-QKD key rate and transmission distance under four different THz frequencies (values of 0.2 THz, 0.9 THz, 10 THz, and 30 THz, respectively) at different data lengths.

From Figure 7, it can be seen that due to the finite-size effect, the secure key rate of the system decreases compared to the case where N is infinite, as shown by the black dashed line (as shown in Figure 5). Therefore, the finite-size effect cannot be ignored in THz CV-MDI-QKD. Of course, it can also be seen that when the N value reaches 10^{12}, the protocol key rate and the farthest transmission distance are close to the infinite data length, which is also the reason why many QKD experimental systems have key lengths ranging from 10^{12} to 10^{14} [4,16].

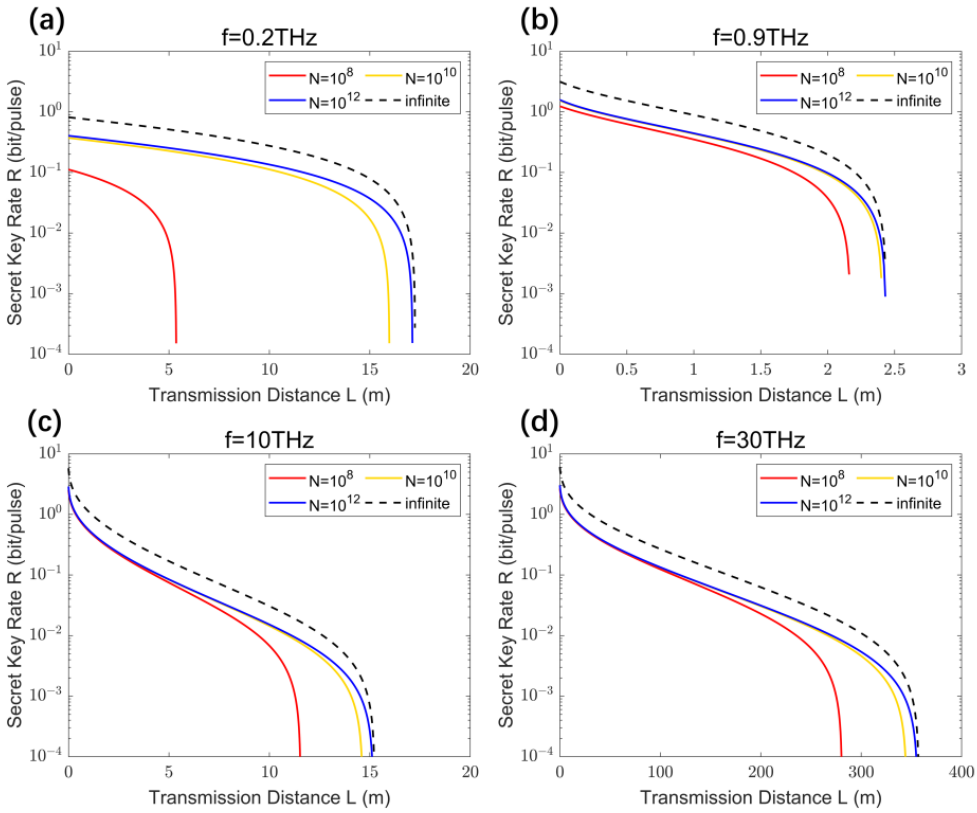

Figure 7. Secure key rates of THz CV-MDI-QKD change with transmission distances considering the finite-size effect using default modulation variance at different THz frequencies: (**a**) 0.2 THz; (**b**) 0.9 THz; (**c**) 10 THz; (**d**) 30 THz.

4.2. Impacts of the Reconciliation Efficiency

The previous discussion was based on the case of the reconciliation efficiency $\beta = 1$. Considering that the reconciliation efficiency of the practical QKD system is generally less than 1, we set the reconciliation efficiency $\beta = 0.96$ in Figure 8, and the secure key rate of THz CV-MDI-QKD under the finite-size effect varies with signal number N and transmission distance L. The important parameters are the same as in Figure 7, except for the reconciliation efficiency.

Comparing Figures 7 and 8, it can be seen that when β is less than 1, the secure key rate R and transmission distance L of THz CV-MDI-QKD are reduced regardless of whether the finite-size effect is considered. Therefore, improving the reconciliation efficiency is of great significance for practical THz CV-MDI-QKD systems.

Please note that in Figure 8a, the red curve's disappearance signifies that under conditions of limited reconciliation efficiency and a room-temperature atmospheric environment, and taking finite-size effects into account for $N = 10^8$, achieving secure 0.2 THz CV-MDI-QKD becomes unattainable. This is primarily due to the substantial influence of statistical errors on parameters like channel transmittance and excess noise when the data length is insufficient. Fortunately, when the data length is scaled up to $N = 10^{10}$, the 0.2 THz CV-MDI-QKD protocol can operate effectively and facilitate secure key transmission, as illustrated by the yellow curve in Figure 8a.

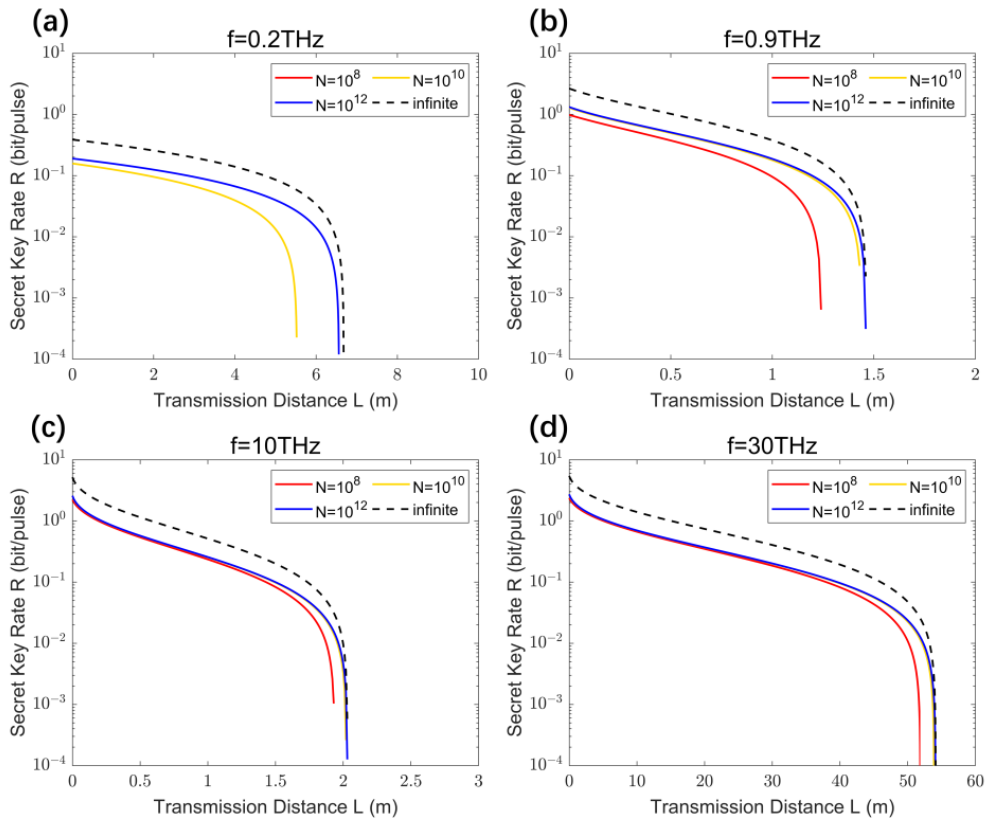

Figure 8. Secure key rates of THz CV-MDI-QKD change with transmission distances considering the finite-size effect and limited reconciliation efficiency $\beta = 0.96$ at different THz frequencies: (**a**) 0.2 THz; (**b**) 0.9 THz; (**c**) 10 THz; and (**d**) 30 THz.

4.3. Optimal Modulation Variances

Although many studies have improved the reconciliation efficiency β, the efficiency in practical CVQKD systems still remains below 1 [4,65]. To address the issue of suboptimal reconciliation efficiency β causing a decrease in key rate and transmission distance in THz CV-MDI-QKD, we investigated the relationship between modulation variances and transmission distances. In CVQKD experiments, the values of V_{AS} and V_{BS} can be adjusted according to practical considerations [16,66]. In THz CVQKD, when $\beta = 1$, larger values of modulation variance for both Alice and Bob lead to higher key rates. Therefore, we set the default modulation variance to 100,000 in the case of $\beta = 1$.

However, when the reconciliation efficiency is less than 1, larger modulation variances do not necessarily yield better results. Referring to Equation (23), we studied the impact of different modulation variance values on the farthest secure transmission distance under the conditions of $N = 10^{12}$ and N approaching infinity, with $L_{BC} = 0$ and modulation variance values $V = V_{AS} = V_{BS}$. As shown in Figure 9, each subgraph displays the farthest transmission distances changes with different modulation variances for different THz frequencies, with the red circles indicating the extremum points of the respective curves. The farthest transmission distance refers to the distance at which the protocol's key rate becomes zero, signifying that beyond this distance, the THz CV-MDI-QKD protocol will be unable to generate a secure key.

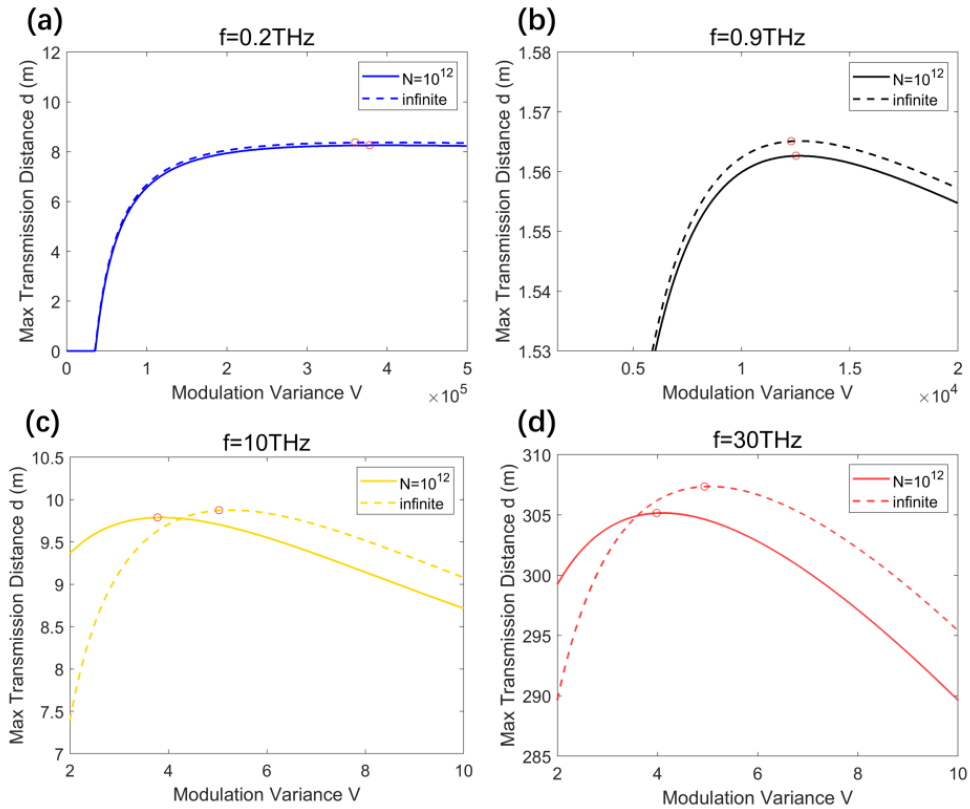

Figure 9. The influence of modulation variances on max transmission distances of (**a**) 0.2 THz, (**b**) 0.9 THz, (**c**) 10 THz, and (**d**) 30 THz CV-MDI-QKD ($V = V_{AS} = V_{BS}$). The red circles represent the maximum transmission distances achieved by THz CV-MDI-QKD with different THz frequencies and data sizes under the optimal modulation variance.

Based on Figure 9, we determined the optimal modulation variances for different THz frequencies at $N = 10^{12}$ and when N approaches infinity. We selected the optimal modulation variances and default modulation variances for various THz frequencies to depict the relationship between the secure key rate and transmission distance, as shown in Figure 10. The solid lines represent the comparison of key rate variation with transmission distance between the default and optimal modulation variance conditions when $N = 10^{12}$. Correspondingly, the dashed lines represent the comparison of key rate variation with transmission distance between the default and optimal modulation variance conditions when N approaches infinity.

For practical THz QKD systems, achieving $V_{AS}(V_{BS})$ values exceeding 10,000 in experimental implementations is challenging. Therefore, when considering scenarios at 0.2 THz and 0.9 THz, the choice of modulation variance must take into account the constraints of practical conditions.

By comparing the variations in key rates under these two conditions, it can be observed that THz CV-MDI-QKD with the optimal modulation variance achieves a greater maximum transmission distance. As depicted in Figure 10a,b, employing the optimal modulation variances has a positive impact on extending the maximum transmission distance for frequencies of 0.2 THz and 0.9 THz. From Figure 10c,d, it is evident that using the optimal modulation variances significantly improves the extension of the maximum transmission distance for frequencies of 10 THz and 30 THz.

Additionally, in Figure 10, the maximum transmission distances achieved after optimizing the modulation variances align with the optimization outcomes obtained by selecting the optimal modulation variances for different THz frequencies, as shown in Figure 9. From the analysis in this section, it is apparent that careful planning is necessary when determining the modulation variance for practical THz CV-MDI-QKD systems.

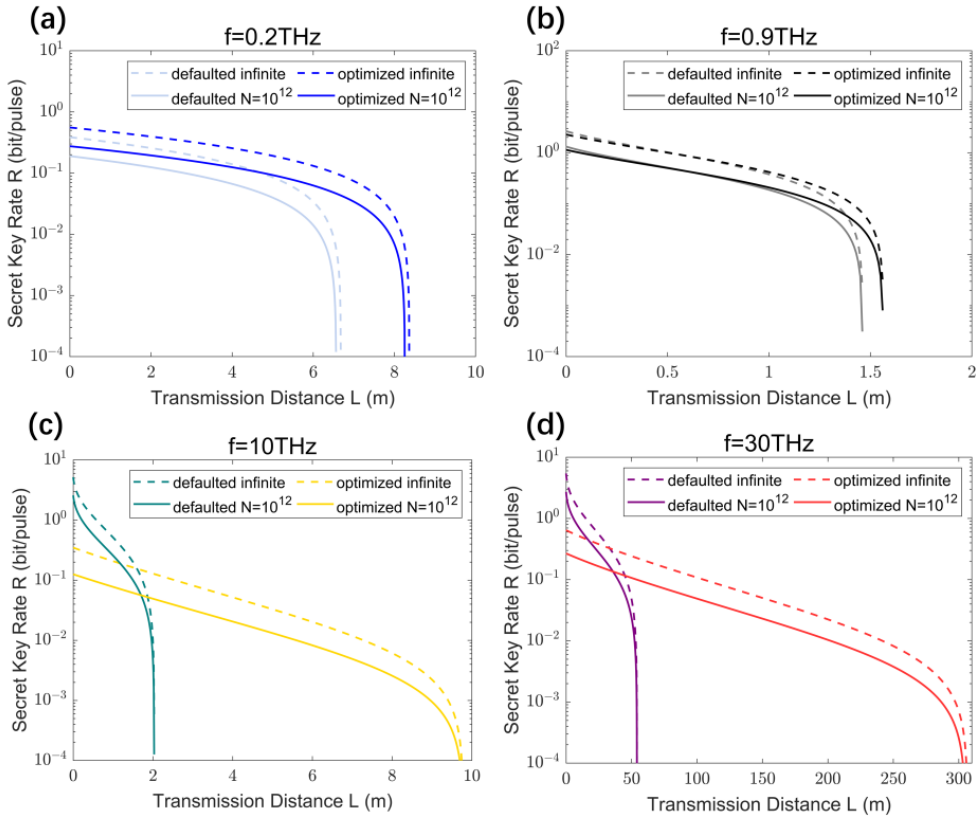

Figure 10. Secure key rates of (**a**) 0.2 THz, (**b**) 0.9 THz, (**c**) 10 THz, and (**d**) 30 THz CV-MDI-QKD change with transmission distances with the optimal modulation variances and defaulted modulation variances, as for $N = 10^{12}$ and when N approaches infinity.

4.4. Low-Temperature THz CV-MDI-QKD

The theoretical analysis of CVQKD is primarily based on large modulation variances ($V_S = 100,000$ [41,48], $V_S = 1000$ [30]). The practical modulation variances reported in CVQKD experimental work are typically around 40 [67–69]. Based on the previous analysis, it is evident that the optimal modulation variances for 0.2 THz and 0.9 THz CV-MDI-QKD are much greater than 100, making experimental implementation quite challenging. This situation can be addressed through cryogenic methods.

Figure 11 illustrates that even when not using the optimal modulation variances, and instead using typical modulation variances, the asymmetric scheme of THz CV-MDI-QKD can transmit over several meters. At a temperature of 18.6 K, the optimal modulation variance for 0.2 THz CV-MDI-QKD is 481. As shown in Figure 11a, when the modulation variance (V) is set to 30 and $N = 10^{12}$, a transmission distance of 15 m can be achieved. At a temperature of 77 K, the optimal modulation variance for 0.9 THz CV-MDI-QKD is 364. As depicted in Figure 11b, with a modulation variance of 30 ($V = 30$) and when $N = 10^{12}$, a transmission distance of 2 m is attainable.

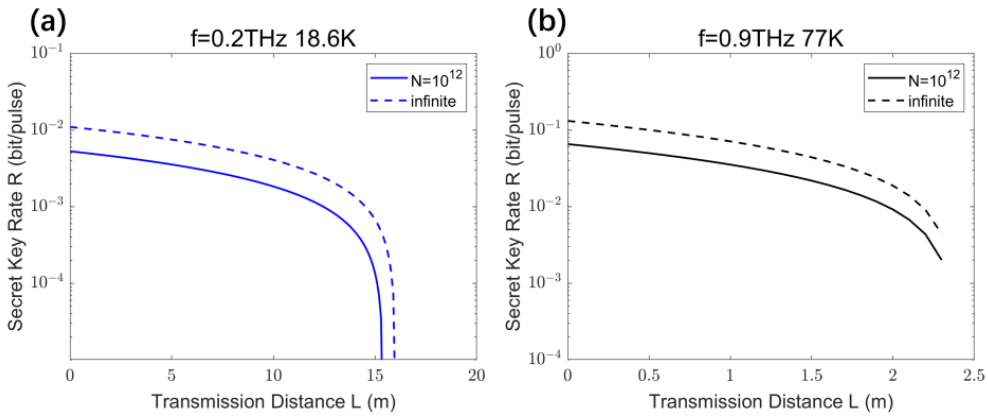

Figure 11. Secure key rates for (**a**) 0.2 THz and (**b**) 0.9 THz CV-MDI-QKD vary with transmission distances at low temperatures.

5. Discussion

We investigated the relationship between the key rate and transmission distance of THz CV-MDI-QKD at four different THz frequencies in atmospheric environments. We found that in the asymmetric configuration (with Charlie's detection setup placed adjacent to Bob's end), the protocol achieves longer key transmission distances.

Considering the finite-size effect in practical THz CV-MDI-QKD systems, we studied the impact of different numbers of signals on the key rate. Furthermore, in the context of practical THz CV-MDI-QKD systems, the issue of reconciliation efficiency being less than 1 greatly affects the key rate and transmission distance. We have demonstrated that by searching for the optimal modulation variance, the protocol's transmission distance can be significantly extended.

It is worth noting that the THz CV-MDI-QKD proposed here primarily addresses vulnerabilities in the detection equipment. Addressing deficiencies at the source end can be achieved through the CV source-device-independent (SDI) QKD protocol [70]. However, the THz CV-SDI-QKD protocol frequency range still requires further research and exploration.

5.1. Compared with Optical QKD

Optical QKD has seen rapid development [9,10,48], and THz QKD has also garnered significant attention from researchers [35,38,39]. In comparison to optical QKD, THz waves exhibit a reduced susceptibility to atmospheric factors, such as dust, smoke, fog, and turbulence (scintillation) [20–24]. These atmospheric conditions pose challenges for optical QKD but can be effectively addressed by THz QKD, thereby enhancing the reliability of secure communication systems. It is worth noting that THz QKD faces its own challenges, as it is more sensitive to environmental noise photons and experiences significant atmospheric attenuation. Therefore, THz QKD is better suited for short-distance secure communication scenarios.

In addition, the space environment offers unique advantages for THz QKD, as it is free from atmospheric losses and features lower temperatures, enabling long-distance THz QKD over hundreds of kilometers [39].

5.2. Experimental Implementation of THz CV-MDI-QKD

This paper primarily focuses on a theoretical analysis and numerical simulation for the THz CV-MDI-QKD. The required experimental instruments for THz CV-MDI-QKD are similar to those for THz CVQKD (as outlined in ref. [30]). Of course, the arrangement of these experimental instruments should adhere to the PM model, as depicted in Figure 1. These instruments mainly include THz light sources, THz detectors, as well as THz intensity and phase modulators.

The advancement of THz CV-MDI-QKD experimental systems requires several key aspects of work:

1. Advances in the main components of THz QKD, which encompass THz light sources, THz detectors, and THz intensity and phase modulators, are expected to significantly promote the development of THz QKD technology.
2. The maturity of THz single-photon detectors will greatly advance THz DVQKD, as the majority of current research, including our work, has been focused on THz CVQKD.
3. Developments in THz optical waveguides, akin to how optical fiber advancements have greatly promoted optical QKD, can lead to significant improvements in THz wired channel QKD by reducing losses. This can help circumvent issues associated with wireless channel attenuation and obstacles.

6. Conclusions

In conclusion, we propose THz CV-MDI-QKD to address challenges faced by THz QKD in real-world applications, including detector attacks, the finite-size effect, and sub-optimal reconciliation efficiency. We also provide insights into the relationship between the secure key rate and transmission distance for THz CV-MDI-QKD under the optimal modulation variance. Our work contributes to the practical implementation of THz QKD systems.

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

Funding: This research was funded by The National Natural Science Foundation of China grant number (12104251, 61875140), and the Beijing Natural Science Foundation Project grant number (4181001).

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: All data can be obtained from the authors under reasonable request.

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

References

1. Bennett, C.H.; Brassard, G. Quantum cryptography: Public key distribution and coin tossing. In Proceedings of the International Conference on Computers, Systems and Signal Processing, Bangalore, India, 10–12 December 1984; pp. 175–179.
2. Bennett, C.H.; Brassard, G. Experimental quantum cryptography: The dawn of a new era for quantum cryptography: The experimental prototype is working. *ACM Sigact News* **1989**, *20*, 78–80. [CrossRef]
3. Wang, S.; Yin, Z.; He, D.; Chen, W.; Wang, R.; Ye, P.; Zhou, Y.; Fan-Yuan, G.; Wang, F.; Chen, W.; et al. Twin-field quantum key distribution over 830-km fibre. *Nat. Photonics* **2022**, *16*, 154–161. [CrossRef]
4. Liu, Y.; Zhang, W.; Jiang, C.; Chen, J.; Zhang, C.; Pan, W.; Ma, D.; Dong, H.; Xiong, J.; Zhang, C.; et al. Experimental Twin-Field Quantum Key Distribution Over 1000 km Fiber Distance. *Phys. Rev. Lett.* **2023**, *130*, 210801. [CrossRef]
5. Ralph, T.C. Security of continuous-variable quantum cryptography. *Phys. Rev. A* **2000**, *62*, 062306. [CrossRef]
6. Huang, D.; Liu, S.; Zhang, L. Secure Continuous-Variable Quantum Key Distribution with Machine Learning. *Photonics* **2021**, *8*, 511. [CrossRef]
7. Li, D.D.; Tang, Y.L.; Zhao, Y.K.; Zhou, L.; Zhao, Y.; Tang, S.B. Security of Optical Beam Splitter in Quantum Key Distribution. *Photonics* **2022**, *9*, 527. [CrossRef]
8. Zhou, L.; Lin, J.; Xie, Y.M.; Lu, Y.S.; Jing, Y.; Yin, H.L.; Yuan, Z. Experimental quantum communication overcomes the rate-loss limit without global phase tracking. *Phys. Rev. Lett.* **2023**, *130*, 250801. [CrossRef]
9. Grosshans, F.; Grangier, P. Continuous Variable Quantum Cryptography Using Coherent States. *Phys. Rev. Lett.* **2002**, *88*, 057902. [CrossRef]
10. Williams, B.P.; Qi, B.; Alshowkan, M.; Evans, P.G.; Peters, N.A. Continuous-variable quantum key distribution with true local oscillator. In Proceedings of the Conference on Lasers and Electro-Optics (CLEO) 2023, San Jose, CA, USA, 7–12 May 2023; p. FF1A.2.

11. Ghorai, S.; Grangier, P.; Diamanti, E.; Leverrier, A. Asymptotic security of continuous-variable quantum key distribution with a discrete modulation. *Phys. Rev. X* **2019**, *9*, 021059. [CrossRef]
12. Lin, J.; Upadhyaya, T.; Lütkenhaus, N. Asymptotic security analysis of discrete-modulated continuous-variable quantum key distribution. *Phys. Rev. X* **2019**, *9*, 041064. [CrossRef]
13. Liu, W.B.; Li, C.L.; Xie, Y.M.; Weng, C.X.; Gu, J.; Cao, X.Y.; Lu, Y.S.; Li, B.H.; Yin, H.L.; Chen, Z.B. Homodyne detection quadrature phase shift keying continuous-variable quantum key distribution with high excess noise tolerance. *PRX Quantum* **2021**, *2*, 040334. [CrossRef]
14. Kanitschar, F.; George, I.; Lin, J.; Upadhyaya, T.; Lütkenhaus, N. Finite-Size Security for Discrete-Modulated Continuous-Variable Quantum Key Distribution Protocols. *PRX Quantum* **2023**, *4*, 040306. [CrossRef]
15. Zhang, Y.; Li, Z.; Chen, Z.; Weedbrook, C.; Zhao, Y.; Wang, X.; Huang, Y.; Xu, C.; Zhang, X.; Wang, Z. Continuous-variable QKD over 50 km commercial fiber. *Quantum Sci. Technol.* **2019**, *4*, 035006. [CrossRef]
16. 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]
17. Sakda, N.; Chitaree, R.; Rahman, B.M.A. Reflective Terahertz Metasurfaces Based on Non-Volatile Phase Change Material for Switchable Manipulation. *Photonics* **2022**, *9*, 508. [CrossRef]
18. Kiwa, T.; Tonouchi, M. Special Issue "Terahertz (THz) Science in Advanced Materials, Devices and Systems". *Photonics* **2023**, *10*, 1024. [CrossRef]
19. Shiramizu, T.; Seiki, N.; Matsumoto, R.; Masutomi, N.; Mikami, Y.; Ueda, Y.; Kato, K. Feasibility Demonstration of THz Wave Generation/Modulation Based on Photomixing Using a Single Wavelength-Tunable Laser. *Photonics* **2023**, *10*, 369. [CrossRef]
20. Ma, J.; Vorrius, F.; Lamb, L.; Moeller, L.; Federici, J.F. Comparison of experimental and theoretical determined terahertz attenuation in controlled rain. *J. Infrared Millim. Terahertz Waves* **2015**, *36*, 1195–1202. [CrossRef]
21. Ma, J.; Vorrius, F.; Lamb, L.; Moeller, L.; Federici, J.F. Experimental comparison of terahertz and infrared signaling in laboratory-controlled rain. *J. Infrared Millim. Terahertz Waves* **2015**, *36*, 8856–8865. [CrossRef]
22. Su, K.; Moeller, L.; Barat, R.B.; Federici, J.F. Experimental comparison of terahertz and infrared data signal attenuation in dust clouds. *J. Opt. Soc. Am. A* **2012**, *29*, 2360–2366. [CrossRef]
23. Su, K.; Moeller, L.; Barat, R.B.; Federici, J.F. Experimental comparison of performance degradation from terahertz and infrared wireless links in fog. *J. Opt. Soc. Am. A* **2012**, *29*, 179–184. [CrossRef] [PubMed]
24. Ma, J.; Lamb, L.; Moeller, L.; Federici, J.F. Experimental comparison of terahertz and infrared signaling in controlled atmospheric turbulence. *J. Infrared Millim. Terahertz Waves* **2015**, *36*, 130–143. [CrossRef]
25. Ramos, R.V. A Proposal for Single-Photon Detection in Millimeter-Wave and THz Regions. In Proceedings of the 2021 SBMO/IEEE MTT-S International Microwave and Optoelectronics Conference (IMOC), Fortaleza, Brazil, 24–27 October 2021; pp. 1–3.
26. Guedes, V.F.; Mendonca, F.A.; Silva, J.B.R.; Ramos, R.V. Discrete Variable Quantum Key Distribution in Millimeter-Wave and THz Regions. *TechRxiv* **2021**, preprint. [CrossRef]
27. Weedbrook, C.; Pirandola, S.; Lloyd, S.; Ralph, T.C. Quantum cryptography approaching the classical limit. *Phys. Rev. Lett.* **2010**, *105*, 110501. [CrossRef] [PubMed]
28. Weedbrook, C.; Pirandola, S.; Ralph, T.C. Continuous-variable quantum key distribution using thermal states. *Phys. Rev. A* **2012**, *86*, 022318. [CrossRef]
29. Weedbrook, C.; Ottaviani, C.; Pirandola, S. Two-way quantum cryptography at different wavelengths. *Phys. Rev. A* **2014**, *89*, 219–228. [CrossRef]
30. Liu, X.; Zhu, C.; Chen, N.; Pei, C. Practical aspects of terahertz wireless quantum key distribution in indoor environments. *Quantum Inf. Process.* **2018**, *17*, 1–20. [CrossRef]
31. Liu, C.; Zhu, C.; Nie, M.; Yang, H.; Pei, C. FL-QKD based on optical-THz biphotons generated by spontaneous parametric downconversion in inter-satellite wireless communication. *Appl. Opt.* **2021**, *60*, 7362–7370. [CrossRef]
32. Kundu, N.K.; Dash, S.P.; McKay, M.R.; Mallik, R.K. MIMO terahertz quantum key distribution. *IEEE Commun. Lett.* **2021**, *25*, 3345–3349. [CrossRef]
33. Liu, C.; Zhu, C.; Liu, X.; Nie, M.; Yang, H.; Pei, C. Multicarrier multiplexing continuous-variable quantum key distribution at terahertz bands under indoor environment and in inter-satellite links communication. *IEEE Photonics J.* **2021**, *13*, 1–13.
34. Liu, C.; Zhu, C.; Li, Z.; Nie, M.; Yang, H.; Pei, C. Continuous-variable quantum secret sharing based on thermal terahertz sources in inter-satellite wireless links. *Entropy* **2021**, *23*, 1223. [CrossRef] [PubMed]
35. Echternach, P.M.; Pepper, B.J.; Reck, T.; Bradford, C.M. Single photon detection of 1.5 THz radiation with the quantum capacitance detector. *Nat. Astron.* **2018**, *2*, 90–97. [CrossRef]
36. He, Y.; Mao, Y.; Huang, D.; Liao, Q.; Guo, Y. Indoor channel modeling for continuous variable quantum key distribution in the terahertz band. *Opt. Express* **2020**, *28*, 32386–32402. [CrossRef] [PubMed]
37. Wang, Z.; Malaney, R.; Green, J. Inter-Satellite Quantum Key Distribution at Terahertz Frequencies. In Proceedings of the 2019 IEEE International Conference on Communications (ICC), Shanghai, China, 20–24 May 2019; pp. 1–7.
38. Ottaviani, C.; Woolley, M.J.; Erementchouk, M.; Federici, J.F.; Mazumder, P.; Pirandola, S.; Weedbrook, C. Terahertz Quantum Cryptography. *IEEE J. Sel. Areas Commun.* **2020**, *38*, 483–495. [CrossRef]
39. Liu, C.; Zhu, C.; Nie, M.; Yang, H.; Pei, C. Composable security for inter-satellite continuous-variable quantum key distribution in the terahertz band. *Opt. Express* **2022**, *30*, 14798–14816. [CrossRef] [PubMed]

40. Curty, M.; Xu, F.; Cui, W.; Lim, C.; Tamaki, K.; Lo, H.K. Finite-key analysis for measurement-device-independent quantum key distribution. *Nat. Commun.* **2014**, *5*, 3732. [CrossRef]
41. 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]
42. Zhao, Y.; Fung, C.; Qi, B.; Chen, C.; Lo, H.K. Quantum hacking: Experimental demonstration of time-shift attack against practical quantum key distribution systems. *Phys. Rev. A* **2008**, *78*, 042333. [CrossRef]
43. Makarov, V.; Hjelme, D. Faked states attack on quantum cryptosystems. *J. Mod. Opt.* **2005**, *52*, 691–705. [CrossRef]
44. Makarov, V. Controlling passively quenched single photon detectors by bright light. *New J. Phys.* **2009**, *11*, 065003. [CrossRef]
45. Lo, H.K.; Curty, M.; Qi, B. Measurement-device-independent quantum key distribution. *Phys. Rev. Lett.* **2012**, *108*, 130503. [CrossRef] [PubMed]
46. Vorontsova, I.O.; Goncharov, R.K.; Tarabrina, A.D.; Tupyakov, D.V.; Bolychev, E.A.; Smirnov, S.V.; Kiselev, F.D.; Egorov, V.I. Theoretical analysis of measurement-device-independent quantum key distribution systems integrated into fiber-optic communication lines using dense wavelength division multiplexing. *J. Opt. Technol.* **2022**, *89*, 424–429. [CrossRef]
47. Sun, Z.; Pan, D.; Ruan, D.; Long, G. One-Sided Measurement-Device-Independent Practical Quantum Secure Direct Communication. *J. Light. Technol.* **2023**, *41*, 4680–4690. [CrossRef]
48. Li, Z.; Zhang, Y.; Xu, F.; Peng, X.; Guo, H. Continuous-variable measurement-device-independent quantum key distribution. *Phys. Rev. A* **2014**, *89*, 052301. [CrossRef]
49. Peng, Q.; Guo, Y.; Liao, Q.; Ruan, X. Satellite-to-submarine quantum communication based on measurement-device-independent continuous-variable quantum key distribution. *Quantum Inf. Process.* **2022**, *21*, 61. [CrossRef]
50. Leverrier, A.; Grosshans, F.; Grangier, P. Finite-size analysis of a continuous-variable quantum key distribution. *Phys. Rev. A* **2010**, *81*, 062343. [CrossRef]
51. Wang, P.; Wang, X.; Li, J.; Li, Y. Finite-size analysis of unidimensional continuous-variable quantum key distribution under realistic conditions. *Opt. Express* **2017**, *25*, 27995–28009. [CrossRef]
52. 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]
53. Weedbrook, C.; Lance, A.M.; Bowen, W.P.; Symul, T.; Ralph, T.C.; Lam, P.K. Quantum Cryptography Without Switching. *Phys. Rev. Lett.* **2004**, *93*, 170504. [CrossRef]
54. Devetak, I.; Winter, A. Distillation of secret key and entanglement from quantum states. *Proc. R. Soc. A Math. Phys. Eng. Sci.* **2005**, *461*, 207–235. [CrossRef]
55. Sheikh, F.; Zarifeh, N.; Kaiser, T. Terahertz band: Channel modelling for short-range wireless communications in the spectral windows. *IET Microw. Antennas Propag.* **2016**, *10*, 1435–1444. [CrossRef]
56. Schneider, T.; Wiatrek, A.; Preussler, S.; Grigat, M.; Braun, R.P. Link budget analysis for terahertz fixed wireless links. *IEEE Trans. Terahertz Sci. Technol.* **2012**, *2*, 250–256. [CrossRef]
57. Han, C.; Wang, Y.; Li, Y.; Chen, Y.; Abbasi, N.A.; Kürner, T.; Molisch, A.F. Terahertz wireless channels: A holistic survey on measurement, modeling, and analysis. *IEEE Commun. Surv. Tutor.* **2022**, *24*, 1670–1707. [CrossRef]
58. Rosker, M.J.; Wallace, H.B. Imaging through the atmosphere at terahertz frequencies. In Proceedings of the 2007 IEEE/MTT-S International Microwave Symposium, Honolulu, HI, USA, 3–8 June 2007; pp. 773–776.
59. Sector, I.R. *Recommendation ITU-R p. 676–12, Attenuation by Atmospheric Gases*; International Telecommunications Union: Geneva, Switzerland, 2019.
60. Portillo, I. ITU-Rpy: A python Implementation of the ITU-R P. Recommendations to Compute Atmospheric Attenuation in Slant and Horizontal Paths. GitHub, 2017. Available online: https://github.com/inigodelportillo/ITU-Rpy (accessed on 5 October 2023).
61. Navascués, M.; Grosshans, F.; Acín, A. Optimality of Gaussian attacks in continuous-variable quantum cryptography. *Phys. Rev. Lett.* **2006**, *97*, 190502. [CrossRef]
62. García-Patrón, R.; Cerf, N.J. Unconditional optimality of Gaussian attacks against continuous-variable quantum key distribution. *Phys. Rev. Lett.* **2006**, *97*, 190503. [CrossRef]
63. 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]
64. 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]
65. Wang, H.; Li, Y.; Pi, Y.; Pan, Y.; Shao, Y.; Ma, L.; Zhang, Y.; Yang, J.; Zhang, T.; Huang, W.; et al. Sub-Gbps key rate four-state continuous-variable quantum key distribution within metropolitan area. *Commun. Phys.* **2022**, *5*, 162. [CrossRef]
66. Jain, N.; Chin, H.; 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. [CrossRef]
67. Grosshans, F.; Assche, V.G.; Wenger, J.; Brouri, R.; Cerf, N.J.; Grangier, P. Quantum key distribution using gaussian-modulated coherent states. *Nature* **2003**, *421*, 238–241. [CrossRef]
68. Jouguet, P.; Kunz-Jacques, S.; Leverrier, A.; Grangier, P.; Diamanti, E. Experimental demonstration of long-distance continuous-variable quantum key distribution. *Nat. Photonics* **2013**, *7*, 378–381. [CrossRef]

69. Soh, D.B.S.; Brif, C.; Coles, P.J.; Lütkenhaus, N.; Camacho, R.M.; Urayama, J.; Sarovar, M. Self-referenced continuous-variable quantum key distribution protocol. *Phys. Rev. X* **2015**, *5*, 041010. [CrossRef]
70. Zhang, Y.; Chen, Z.; Weedbrook, C.; Yu, S.; Guo, H. Continuous-variable source-device-independent quantum key distribution against general attacks. *Sci. Rep.* **2020**, *10*, 6673. [CrossRef] [PubMed]

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.