mathematics

IMPACT FACTOR 2.3

CITESCORE 4.0

Article

Practical Security of Continuous Variable Measurement- Device-Independent Quantum Key Distribution with Local Local Oscillator

Yewei Guo, Hang Zhang and Ying Guo

Special Issue

Quantum Cryptography and Applications

Edited by

Dr. Chun-Wei Yang, Dr. Chia-Wei Tsai and Dr. Jason Lin

MDPI

https://doi.org/10.3390/math12233732

mathematics

MDPI

Article

Practical Security of Continuous Variable Measurement-Device-Independent Quantum Key Distribution with Local Local Oscillator

Yewei Guo [1], Hang Zhang [2,*] and Ying Guo [2,*]

[1] BIT-BMSTU Joint School, Beijing Institute of Technology, Beijing 100086, China; bityewei@bit.edu.cn
[2] School of Automation, Central South University, Changsha 210056, China
* Correspondence: zhang22@csu.edu.cn (H.Z.); guoying@bupt.edu.cn (Y.G.)

Abstract: Continuous-variable (CV) measurement-device-independent (MDI) quantum key distribution (QKD) can remove the feasible side-channel attacks on detectors based on the accurate Bell-state measurement (BSM), where an optical amplitude modulator (AM) plays a crucial role in managing the intensity of the transmitted light pulse. However, the AM-involved practical security has remained elusive as the operating frequency of the AM usually determines the actual secret key rate of the CV-MDI-QKD system. We find that an imperfect pulse generated from the AM at high speed can lead to a challenge to the practical security as a minor intensity change of the light pulse can bring about a potential information leakage. Taking advantage of this flaw, we suggest an attack strategy targeting the embedded AM in CV-MDI-QKD without sending the local oscillator (LO). This attack can damage the AM and thus decrease the estimated secret key rate of the system even when the orthogonal local LO (LLO) scheme is carried out. To assess the practical security risk resulting from the leaked information from the AM, we conduct numerical simulations to demonstrate the influence of the AM on the CVMDI-QKD system.

Keywords: Bell-state measurement; quantum key distribution; quantum communication

MSC: 81P45

Citation: Guo, Y.; Zhang, H.; Guo, Y. Practical Security of Continuous Variable Measurement-Device-Independent Quantum Key Distribution with Local Local Oscillator. *Mathematics* **2024**, *12*, 3732. https://doi.org/10.3390/math12233732

Academic Editors: Chun-Wei Yang, Chia-Wei Tsai and Jason Lin

Received: 22 October 2024
Revised: 17 November 2024
Accepted: 20 November 2024
Published: 27 November 2024

1. Introduction

Quantum key distribution (QKD), which utilizes the physical characteristics of tangible particles as carriers to generate a secure one-time-pad (OTP), is a promising approach for transmitting secure messages [1]. There are many QKD protocols, which can be divided into two groups, i.e., discrete variable (DV) QKD and continuous variable (CV) QKD [2]. DVQKD employs the photons or weak coherent pulses encoded in discrete variables [3], whereas CVQKD encodes information on the quadratures x and p of light pulses, representing the amplitude and phase of an electromagnetic wave [4]. CVQKD offers an advantage in practicality: compatibility with the standard optical telecommunication network. It exhibits a tolerance to channel loss and noise; hence, it is much reliable than DVQKD [5]. However, the gap between experimental models and practical devices opens feasible loopholes in practical security, leading to the potential for attacks.

When implementing CVQKD, the sender may transmit quantum signals combined with a local oscillator (LO) to achieve a suitable phase reference for perfect detections [6]. The propagation of an LO between the sender and the receiver is a necessary factor to achieve the shot noise limit for the amplitude, phase, and timing measurements of optical signals, which is robust against noise photons in some kinds of quantum channels [7]. However, the transmitted LO (TLO) in a traditional scheme may have security loopholes as it must be brighter than quantum signals due to the shot-noise-limited demand for the homodyne detector [8], which may leak a considerable number of photons to quantum

signals. In order to solve the problem of the TLO problem, the local LO (LLO) [9], which is generated locally at the reception, has been suggested to shut the LO security loophole [10]. Then, TLO attacks are considered mitigated in an LLO-based scheme [11]. Consequently, the LLO has been widely exploited in both experiments and implementations to eliminate potential attacks [12,13]. However, the reliable photon leakage in source preparation is another challenge.

Inspired by the entanglement swapping in CV circumstances, MDI-QKD has been proposed to prevent the feasible issues related to the side channel attack of measurement apparatus [14]. This is an elegant modification of the CVQKD approach, introducing an untrusted third participant, Charlie, who conducts a joint measurement on the CV quantum signals transmitted by two participants, called Alice and Bob. They both ensure the security of the transmitted quantum signals by verifying the consistency of their datum according to Charlie's announcements. CV-MDI-QKD presents an advantage since it introduces device-independent security, eliminating trust of Charlie's detectors [15]. Because of the key negotiation being independent of measurement equipment, it can resist side channel attacks against measurement equipment [16]. Currently, the performance of the CV-MDI-QKD system has been improved [17,18]. However, practical devices such as the AM embedded in the transmitter for source preparation can still become a target of an assault, from which an attacker can achieve the secure key shared between Alice and Bob illicitly, thus jeopardizing practical security.

As a characterization describing the performance improvement of the CVQKD system, researchers have usually focused on increasing the secret key rate. The high-speed AM has been proven to be effective in implementations [19]; hence, it has been used as a promising and practical choice for conducting high-rate CVQKD [20]. However, we find the practical AM at high-speed modulation sometimes behaves different than anticipated from experiments, and hence a challenge may arise from the AM embedded in CV-MDI-QKD. For example, when the AM generates light pulses, the imperfect light pulses consist of leaked light with lower energy and information light with higher energy, which might produce extra noise, potentially providing additional information, thus potentially leading to information leakage [21]. If an attacker can understand the patterns or inefficiencies of the employed AM, they may take advantage of this side channel information to launch feasible attack strategies [22]. As an example, in a Trojan horse attack, the attacker sends a bright light pulse into the transmitter and analyzes the reflected light pulse to learn about the measurement settings [11,23]. This may enable an eavesdropper to perform a sophisticated attack to weaken the practical security. Regarding the feasibility of eavesdropping on CV-MDI-QKD, Eve mounts an assault on the laser beam of the AM, in which it causes a permanent change in its optical properties, but, overall, it leads to the optical attenuators within the system failing to meet the requirements of theoretical security [22]. Despite the theoretical security proof of CV-MDI-QKD, its practical implementation still exhibits such vulnerabilities. We find that the AM under the high-speed modulations may be susceptible to passive attacks when Eve intercepts information on quantum channels, eavesdropping on the secure key shared between Alice and Bob [18]. The success of this attack essentially exploits the imperfections of the AM within the participants, especially the nonideal characteristics under specific conditions [24,25]. It is more covert as it does not directly assault the devices embedded in CV-MDI-QKD, avoiding causing abnormal system features.

Motivated by the vulnerability of the AM together with the feasible attack strategy, this paper proposes an AM attack scheme taking into account the imperfect devices for quantum state preparation in CV-MDI-QKD. This scheme can cause legitimate participants to overestimate the secret key rate, thus creating an opportunity for the attacker to steal the leaked key information. We focused on the high-speed AM because it is crucial to elevating the secure key rate while keeping the distance constant. Our research indicates that the AM usually generates imperfect light pulses under high-speed modulations. The experimental result shows that these deviant light pulses from the output of the high-speed AM consist

of leaked light with lower energy and information light with higher energy. While the participants encode both types of light pulses and transmit them to Charlie, the leaked light could betray legitimate participants, enabling Eve to steal secure key information. To assess practical security, we conducted numerical simulations to examine the impact of the AM on the CV-MDI-QKD system. They indicate that in high-speed modulation, the risk of information leakage expands with the increase in the transmission distance.

This paper is organized as follows: In Section 2, we describe the structure of the LLO-based CV-MDI-QKD protocol and the orthogonal LLO scheme. In Section 3, we show the noise model and then the LLO structure in order to demonstrate an effect of the AM on the performance of the CV-MDI-QKD system. In Section 4, we show trhe performance of the LLO-based CV-MDI-QKD system. Moreover, we performed numerical simulations to demonstrate its implementation feasibility in experiments. Finally, the conclusions are drawn in Section 5.

2. LLO-Based CV-MDI-QKD

The LLO-based CV-MDI-QKD system was designed with the embedded AM for source preparations. The CV-MDI-QKD protocol is described at first, and then the LLO scheme is presented with the orthogonal transformation.

2.1. CV-MDI-QKD Embedded with AM

The configuration of CV-MDI-QKD embedded with an AM is shown in Figure 1. To begin, two participants, Alice and Bob, use their continuous-wave lasers together with the AM for pulse modulations to produce coherent state pulses $|\alpha_{sr}^{A}\rangle$ and $|\alpha_{sr}^{B}\rangle$, which are denoted by $|\alpha_{sr}^{\mu}\rangle$, $\forall\mu \in \{A, B\}$. Then, they use beam splitters (BSs) to split the resulting pulses into two portions, $|\alpha_{r}^{\mu}\rangle$ and $|\alpha_{s}^{\mu}\rangle$, $\forall\mu \in \{A, B\}$, respectively. One pulse, called the weak signal pulse $|\alpha_{s}^{\mu}\rangle$, is employed as an input of the other amplitude modulator (AM), which is then followed by the phase modulator (PM). The AM and the PM are both modulated according to the Gaussian distribution, with the optimized variances given by $V_{\mu}, \forall\mu \in \{A, B\}$. After using suitable variable optical attenuators (VOAs) to attenuate the intensity of the signal pulse, we obtain the resulting Gaussian-modulated coherent state (GMCS) $|X_{\mu} + iP_{\mu}\rangle$, $\forall\mu \in \{A, B\}$. The other pulse, called the strong reference pulse $|\alpha_{r}^{\mu}\rangle$, is delayed and separated from the weak signal pulse. This pulse is also suitably attenuated by the other VOA to generate an optimal intensity, which is then isolated from the weak signal pulse by using a polarization beam splitter (PBS). The combined pulses are all transmitted to Charlie.

Meanwhile, an intermediator Charlie produces another optical pulse $|\beta_{sr}\rangle$, which is the reference (LO) pulse split into two pulses $|\beta_{sr}^{\mu}\rangle$, i.e., $|\beta_{sr}^{A}\rangle$ and $|\beta_{sr}^{B}\rangle$, by using a 50:50 beam splitter (BS) to couple the received states from Alice and Bob. Subsequently, $|\beta_{sr}^{\mu}\rangle$ can be split into two pulses, $|\beta_{s}^{\mu}\rangle$ and $|\beta_{r}^{\mu}\rangle$. The signal pulse $|\alpha_{s}^{\mu}\rangle$ and the reference (LO) pulse $|\beta_{s}^{\mu}\rangle$, which are all delayed by using delay fibers, are simultaneously sent to a heterodyne detector, from which the raw key can be obtained. Meanwhile, the remaining $|\beta_{r}^{\mu}\rangle$ and $|\alpha_{r}^{\mu}\rangle$ are transmitted to another heterodyne detector for measurements, from which the phase drift can be estimated. After that, the derived phase is elegantly used for compensation of the transmitted quantum signals, from which the secret key is obtained.

As for the Bell-state measurement (BSM) of two independent quantum states, Charlie uses balanced homodyne detectors (BHDs) to measure the amplitude quadrature x_C and phase quadrature p_C, which can be derived as $x_C = (x_A - x_B)/\sqrt{2}$ and $p_C = (p_A + p_B)/\sqrt{2}$, respectively. Charlie announces the measurement results $(x_C + ip_C)/\sqrt{2}$. Subsequently, Alice and Bob displace their respective raw datum as $\hat{x}_{\mu} = x_A - d_{x}^{\mu}(r)$ and $\hat{p}_{\mu} = p_{\mu} - d_{p}^{\mu}(r)$, where $d^{\mu}(r)$ is a displacement operation.

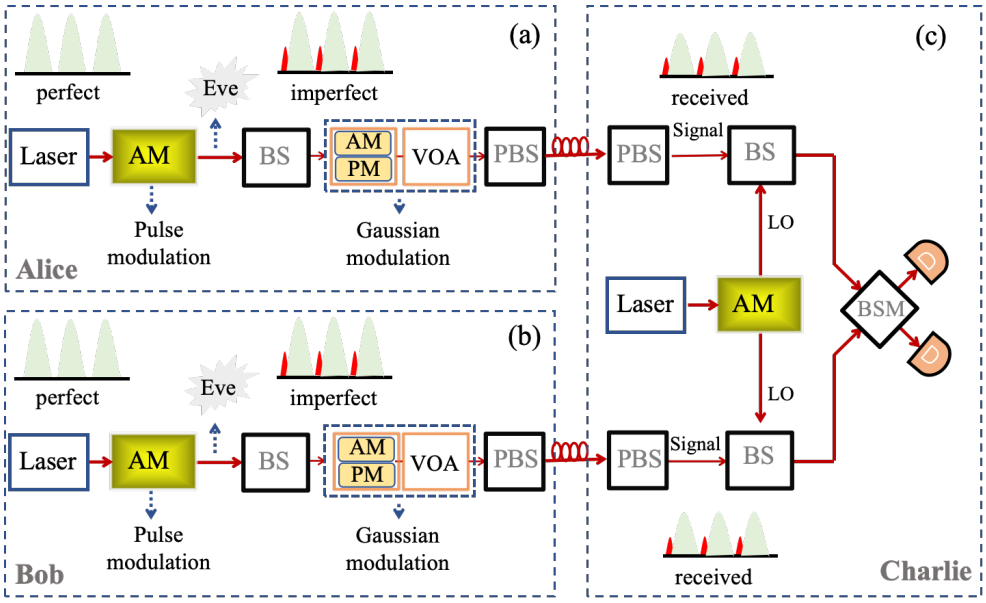

Figure 1. Configuration of CV-MDI-QKD embedded with an AM. (**a**) Procedure of the transmitter with high-speed modulation at Alice's station, (**b**) procedure of the transmitter with high-speed modulation at Bob's station, (**c**) procedure of the receiver at Charlie's station. PBS, polarizing beam splitter; AM, amplitude modulator; PM, phase modulator; BS, beam splitter; VOA, variable optical attenuator.

2.2. LLO Scheme with Orthogonal Block Transformation

A challenge with CV-MDI-QKD is coupling independent quantum signals while performing the BSM at Charlie's station, where the precise regulation of the relative phase between the received signal pulse and the locally produced reference pulse (LO) is required.

As shown in Figure 2, Alice (or Bob) generates a sequence of coherent states, which involves the signal pulse and pilot pulse with an interval given by $1/f$. The signal pulse is denoted by $S^{\mu_i}, \forall \mu \in \{A, B\}$, and $i \in \{1, 2, \cdots, M\}$, and the pilot pulse is represented by $R^{\mu_i}, \forall \mu \in \{A, B\}$, and $i \in \{1, 2, \cdots, M\}$, respectively. Both S^{μ_i} and R^{μ_i} are performed with the orthogonal block transformation, which is also called as the signal–pilotmultiplexed block scheme, before being transmitted. The orthogonal polarization channels are thus occupied to transmit the signal pulse and the pilot pulse simultaneously in order to resist phase noises.

At Charlie's station, the signal pulse and the pilot pulse are generated from the same coherent state pulse. Charlie generates a reference (LO) pulse with the same interval as that of Alice and Bob, given by $1/f$. The signal and pilot pulses can be simultaneously regulated, which are accurately aligned with the reference (LO) pulse. Subsequently, Charlie's reference (LO) pulse is split into two equivalent pulses, which are aligned with the respective signal pulse and pilot pulse of Alice (Bob). After performing the heterodyne detection, the raw key can be derived from the BSM of the interfered signal pulses, and the phase estimation is synchronously achieved from the BSM of the pilot pulses.

The proposed orthogonal signal–pilotscheme can be designed with the orthogonal block transformation. The signal–pilotsequence pulse, denoted by $\tau = (S_i^{\mu}, R_i^{\mu})$, can be encoded as follows:

$$\nu = H \cdot \tau, \tag{1}$$

where H denotes an orthogonal block transformation. For example, we take a Pauli matrix $\sigma_x = \left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)$ encoding the $(i-1)$-th and the i-th pulses, from which we have

$$\begin{pmatrix} S_{i-1}^{\mu} & S_i^{\mu} \\ R_{i-1}^{\mu} & R_i^{\mu} \end{pmatrix} = \sigma_x \cdot \begin{pmatrix} S_{i-1}^{\mu} & R_{i-1}^{\mu} \\ S_i^{\mu} & R_i^{\mu} \end{pmatrix}. \tag{2}$$

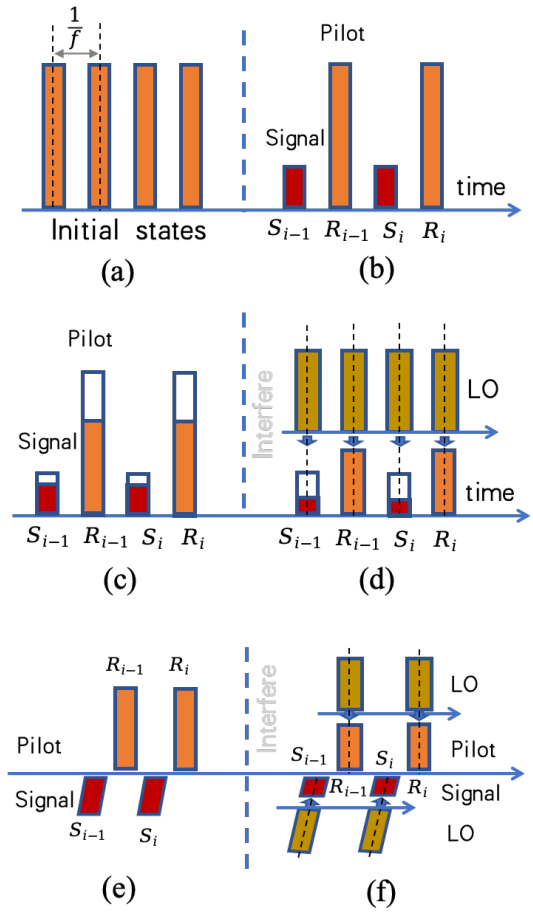

Figure 2. Procedure of the LLO scheme. (**a**) Preparation of the coherent state pulse, (**b**) splitting the coherent states into the signal pulse and the pilot pulse, (**c**) performance of the AM on the signal pulse and the pilot pulse, (**d**) reception of the signal pulse and the pilot pulse interfering with the LO pulse, (**e**) orthogonal transformation of the signal pulse and the pilot pulse, and (**f**) reception of the orthogonal signal pulse and pilot pulse when interfering with the LO pulse.

In this LLO scheme, since the signal pulse and the pilot pulse are all produced from the same laser at the same time, we can achieve the same phase θ_{sr}^{μ} for the signal pulse and the pilot pulse. After being modulated, the signal pulse has an optical phase θ_{m}^{μ}. However, we assume the signal pulse and the pilot pulse are both transmitted simultaneously through two different paths, even though they are orthogonal channels. The delayed pulse is dealt with using an accumulated phase θ_{μ}. As for the LO generated by Charlie, the adjacent LO pulses are generated simultaneously with the same optical phase θ_{sr}^{C}. Correspondingly, the LO path is delayed with the accumulated phase θ_{μ}^{D}. Consequently, the phase measurements of S_i^{μ} and R_i^{μ} are achieved, respectively, as

$$\begin{aligned} \theta_{s,i}^{\mu} &= \theta_{sr}^{\mu} + \theta_{m}^{\mu} - \theta_{sr}^{C}, \\ \theta_{r,i}^{\mu} &= \theta_{sr}^{\mu} + \theta_{m}^{\mu} + \theta_{\mu} - \theta_{sr}^{C} - \theta_{\mu}^{D}. \end{aligned} \tag{3}$$

The phase drift compensation is aimed at the phase drift between the two lasers of Alice and Bob. After performing this compensation, we obtain the corrected quadratures x_i' and p_i' that can be used for key distillation. As the phase θ_{m}^{μ} in Equation (3) is originally modulated for source preparation, we obtain the relative phase drift $\phi_{s,i}^{\mu}$ as follows:

$$\phi_{s,i}^{\mu} = \theta_{s,i}^{\mu} - \theta_{m}^{\mu} = \theta_{r,i}^{\mu} + \Delta\theta_{\mu}, \tag{4}$$

where $\Delta\theta_\mu$ is the difference between the accumulated phase of the related delay lines given by

$$\Delta\theta_\mu = \theta_\mu^D - \theta_\mu. \tag{5}$$

Because of the equivalent delay of both delay lines, we have the theoretical result $\theta_\mu^D = \theta_\mu$; thus, $\Delta\theta_\mu = 0$. Consequently, we can make use of $\theta_{s,i}^\mu$ to remap the quadratures x and p of the received quantum signal pulse due to the straightforward equivalence between $\phi_{s,i}^\mu$ and $\theta_{s,i}^\mu$.

In the initial phase, we obtain $\Delta\theta_\mu = 0$ in the theoretical derivation while adjusting the accuracy of the length of the delay lines of Alice (Bob) and Charlie. Unfortunately, it is difficult to prevent the optical path from fluctuating. Therefore, the parameter $\Delta\theta_\mu$ is kept a constant only for a short duration in a practical scenario, which needs a real-time calibration.

According the relative phase drift $\phi_{s,i}^\mu$ in Equation (4), we can obtain the phase drift, which can be divided into fast drift $\theta_{r,i}^\mu$ and slow drift $\Delta\theta_\mu$. The fast drift compensation can be performed with the fast drift between Alice's (Bob's) and Charlie's lasers. Subsequently, compensation of the phase of the pilot pulse $\theta_{r,i}^\mu$, which is used to monitor the fast drift of the signals, can be conducted as follows:

$$\hat{x}_{s,i}^\mu = x_{s,i}\cos\theta_{r,i}^\mu - p_{s,i}\sin\theta_{r,i}^\mu, \quad \hat{p}_{s,i}^\mu = x_{s,i}\sin\theta_{r,i}^\mu + p_{s,i}\cos\theta_{r,i}^\mu. \tag{6}$$

To estimate the slow drift $\Delta\theta_\mu$, Alice (Bob) transmits the signal pulse and the phase reference pulse that were generated with an identical optical phase. After Charlie performs the heterodyne detection and obtains the phase shift for each pulse from the amplitude quadrature $x_{r,i}^{\prime\mu}$ and the phase quadrature $p_{r,i}^{\prime\mu}$ of the M reference pulses, $i \in \{1, 2, \cdots, M\}$, corresponding to the initial quadrature $x_{r,i}^\mu$ and $p_{r,i}^\mu$, the parameter $\Delta\theta_\mu$ can be estimated as

$$\Delta\theta_\mu = \frac{1}{M}\sum_i [\arctan(\frac{p_{r,i}^\mu}{x_{r,i}^\mu}) - \arctan(\frac{p_{r,i}^{\prime\mu}}{x_{r,i}^{\prime\mu}})], \tag{7}$$

where M is the number of the revealed pairs. Then, the compensation based on the slow drift of the signal pulse is obtained as

$$\tilde{x}_{s,i}^\mu = x_{s,i}^\prime\cos\Delta\theta_\mu - p_{s,i}^\prime\sin\Delta\theta_\mu, \quad \tilde{p}_{s,i}^\mu = x_{s,i}^\prime\sin\Delta\theta_\mu + p_{s,i}^\prime\cos\Delta\theta_\mu. \tag{8}$$

Actually, Charlie can estimate the phase drift of the signal pulse with the adjacent pilot phase based on the interference measurements. As shown in Figure 2b, the ith signal pulse S_i^μ is located between two pilot pulses R_{i-1}^μ and R_i^μ, and thus the approximate phase drift of the signal pulse $\theta_{s,i}$ can be estimated from the phases of R_{i-1}^μ and R_i^μ as follows:

$$\hat{\theta}_{s,i}^\mu = \frac{\theta_{r,i-1}^\mu + \theta_{r,i}^\mu}{2}, \tag{9}$$

where $\hat{\theta}_{s,i}^\mu$ represents the phase drift estimator of the ith signal pulse, while $\theta_{r,i}^\mu$ denotes the phase of the reference pulse R_i^μ. Based on the derived estimator $\hat{\theta}_{s,i}^\mu$, the raw measurements of quadratures x and p can be described as [9]

$$\bar{x}_{s,i}^\mu = x_{s,i}\cos\hat{\theta}_{s,i}^\mu - p_{s,i}\sin\hat{\theta}_{s,i}^\mu, \quad \bar{p}_{s,i}^\mu = x_{s,i}\sin\hat{\theta}_{s,i}^\mu + p_{s,i}\cos\hat{\theta}_{s,i}^\mu. \tag{10}$$

After that, the obtained quadratures $x^\prime$ and $p^\prime$ can be used for distilling the secure keys.

3. Noise Analysis

The excess noise is a crucial parameter for the performance estimation of CV-MDI-QKD. As controlling excess noise can increase the performance of the system, the noise

model was established to show the effect of the AM on the LLO-based CV-MDI-QKD system. We considered the phase noise and the photon-leakage noise, because both of them may undermine the main performance of the CV-MDI-QKD system.

3.1. Phase Noise

According to the phase noise denoted by ε_θ in CV-MDI-QKD, we have [9]

$$\varepsilon_\theta = 2V_m^\mu \left(1 - e^{-\frac{V_\theta}{2}}\right), \tag{11}$$

where V_m^μ is the variance of modulation for $\forall \mu \in \{A, B\}$. In addition, V_θ is the variance of phase noise, which can be given by

$$V_\theta = \mathrm{var}\left(\theta_s - \hat{\theta}_s\right), \tag{12}$$

where θ_s is the initial phase, and $\hat{\theta}_s$ is the estimated phase of the quantum signal pulse.

In compensation, the derived data x_i and p_i are required to transform with the phase drift $\theta_{s,i}^\mu$. However, the derived estimator, such as $\hat{\theta}_{s,i}^\mu$ in Equation (9), has estimation error from time to time, leading to unavoidable phase noise in practice. Her, we treat this error as an imperfection of compensation.

In the orthogonal LLO-based CV-MDI-QKD, the signal pulse and the pilot pulse are simultaneous lytransmitted through the same orthogonal channels, thus avoiding the effect of phase noise on channel fluctuation. Based on the phase drift $V_{\Delta\theta}$ between the signal pulse and the pilot pulse, the phase noise is derived as

$$V_{\theta_{s,i}^\mu} = V_\phi + V_\epsilon, \tag{13}$$

where V_ϕ denotes the intrinsic phase noise, and V_ϵ represents the noise due to the measurement error of the pilot phase. Since the signal pulse is generated before the pilot pulse with a time $1/f$, the uncertainty of the relative phase drift causes an intrinsic phase noise given by

$$V_\phi = 2\pi(\delta v_\mu + \delta v_C)/f, \tag{14}$$

where δv_μ and δv_C correspond to the line width of the lasers. It implies that V_ϕ depends on the line width of the lasers when it comes to the pulse interval. As the pilot pulse and the signal pulse are generated simultaneously by Alice or Bob from the same laser, we have $V_\phi = 0$. Additionally, the pilot-involved LLO scheme suffers from measurement inaccuracy in the pilot phase, given by

$$V_\epsilon = (\chi + 1)/|\alpha|^2, \tag{15}$$

where $|\alpha|^2$ denotes the amplitude of the transmitted pilot pulse, and χ is the total noise resulting from the quantum system, which is given by

$$\chi = \frac{2 - \mu T}{\mu T} + \frac{2v_{\mathrm{el}}}{\mu T}. \tag{16}$$

Here, the foregoing part is the loss-involved vacuum noise, and the following part is the electronic noise resulting from the heterodyne detection.

Consequently, when we employ the intense pilot pulse to suppress the phase noise occurring in BSM with imperfect phase compensation, the phase noise can be estimated as follows:

$$\varepsilon_\theta \simeq V_m^\mu V_{\theta_{s,i}} = V_m^\mu V_\epsilon, \tag{17}$$

where the deviation of $\hat{\theta}_{s,i}^\mu$ is usually taken as a small value.

3.2. Photon Leakage Noise

Because the photons that come from the pilot pulse have the same frequency as that of the signal pulse, the leaked photons in CV-MDI-QKD may cause additional noise. As a result, we cannot ignore the effect of photon leakage on the CV-MDI-QKD system.

Taking the proposed LLO scheme into account, both Alice and Bob produce the pilot pulse and the signal pulse with Gaussian modulation, which are all transmitted to Charlie.

In the orthogonal LLO scheme, although the signal pulse and the pilot pulse are arranged in orthogonal directions, there are still some residual photons in the pilot pulse that may make incursions into the signal pulse. The resulting photon leakage noise is given by

$$\varepsilon_{\ln} = 2|\alpha|^2 / R_e, \tag{18}$$

where R_e is the finite extinction ratio. It is the ratio of the high level and the low level of the signal pulse, which is calculated as

$$R_e = I_1 / I_0, \tag{19}$$

where the optical power I_1 can be the transmitted signal pulse, and the optical power I_0 can be of lower power in an interval.

As for the photon-leakage noises at Alice and Bob's station, the signal pulse and the pilot pulse are rightly arranged in orthogonal directions, and thus there is no photon leakage happening in the orthogonal LLO scheme. The imperfect operation in this scheme lies in the polarization beam splitter (PBS), which can be used to recover the signal pulse and pilot pulse pulses received at Charile's station. Because of effect of the finite polarization extinction ratio R_p of the PBS, there are still a few residual photons leaked from the pilot pulse to the signal pulse. Therefore, in order to describe the photon-leakage noise in the orthogonal LLO scheme, we have to consider the the finite polarization extinction ratio R_p resulting from the pilot pulse. Namely, we obtain the derived photon leakage noise as follows

$$\varepsilon_{\ln} = 2|\alpha|^2 / (R_e + R_p). \tag{20}$$

4. Performance Analysis

The challenge of CV-MDI-QKD is obtaining the BSM of the received quantum signals at Charlie's station, where the precise regulation of the relative phase between the signal and reference pulses is necessary with the phase drift when considering the relation of Alice's (Bob's) signal pulse and Charlie's LO pulse. It involves fast phase drift and slow phase drift. Fast phase drift is caused by the frequency difference between the lasers, together with their channels from Alice (Bob) to Charlie. Slow phase drift comes from the BSM in time multiplexing. In what follows, we consider the performance of the system taking into account theeffect of the AM employed by Alice and Bob for pulse modulations.

4.1. AM Information Leakage

The secret key rate of CV-MDI-QKD often aligns with the lowest-frequency optical component involved in the encoding procedure. It is usually combined with the maximal quantum bit information that Alice and Bob can distill in a given unit of time. As an example, if Bob's detection frequency is in the gigahertz range, whereas Alice's modulation frequency is in the hundred-megahertz range, the overall system frequency is limited to the hundred-megahertz range. Therefore, all devices in the whole system should be properly designed to meet the exact requirements of the modulation frequency in the gigahertz range.

Unfortunately, the imperfect AM embedded in the transmitter may have a few security vulnerabilities due to the intrinsic defects of devices. In our experiments, we examined the modulation frequencies of the AM, as shown in Figure 1, for the pulse modulation before performing source preparation in CV-MDI-QKD.

In order to evaluate the effectiveness of the frequency, we observed the experimental results of the AM, which were modulated with the tunable frequencies for pulse modulations in CV-MDI-QKD. We found that for the low frequencies in pulse modulation of less than 1 GHz, the output pulse light appeared smooth and exhibited only a single peak. However, for the high frequency of 1 GHz, there were two adjacent pulses occurring in the output. According to the areas under the curves, the energy of the first red small pulse was close to half of the energy of the second green pulse. It is notable that in the high-speed AM-embedded CV-MDI-QKD system, the red pulse was still in a Gaussian-modulated coherent state (GMCS). Therefore, when conducting high-speed modulation for pulse modulation before source preparation, the appearance of the red pulse implies a risk of information leakage, opening up a potential security vulnerability in practical CV-MDI-QKD systems.

4.2. Security Analysis

The theoretical security of the system is usually analyzed using the entanglement-based (EB) scheme description, which is equivalent to the prepare-and-measure (PM) scheme used in an actual experiment [26]. In this section, we show the practical security of the AM-embedded CV-MDI-QKD system when considering the finite-size effects [27,28].

4.2.1. Derivation of the Secret Key Rate

Two legitimate participants, Alice and Bob, are expected to establish a secure key in CV-MDI-QKD. Each of them has a set of the AM-embedded equipment for preparing the GMCS. The AM can be used for the pulse modulations while attenuating the intensity of the light pulses before being split into the signal pulse and the reference pulse. It ensures the resulting light pulse meets the theoretically dictated safe intensity range of the system. There is an untrusted relay, Charlie, who performs a joint measurement on the received light pulses from Alice and Bob. In the EB scheme, both Alice and Bob generate a pair of dual-mode squeezed states with variances V_A and V_B, respectively. Unfortunately, an imperfect AM can become the target of Eve's attack because of pulse leakage. By combining the AM-involved attack with other attack strategies (such as the intercept-resend attack), Eve can steal the leaked information, jeopardizing the practical security of the CV-MDI-QKD system.

According to the finite-size effect, we have the secure key rate as follows [29]:

$$K = \frac{n}{N}[\beta I_{AB} - \chi_{BE} - \delta(n), \tag{21}$$

where n is the number of photons used for key distillation, N is the total size of the block, and β is the parameter for efficiency description in reverse reconciliation. Moreover, the first term I_{AB} is the Shannon mutual information between Alice and Bob, the second term χ_{BE} is the maximal value of the Holevo information, and the last term $\delta(n)$ depends on the privacy amplification. The derivation of the secret key rate under the finite-size effect is shown in Appendix A. In what follows, we delve into the attack strategy when considering the effect of information leakage on the secret key rate of the system.

Before starting the security analysis, we show the impact of the attack on the parameters of the above-derived secret key rate. In a scenario with Eve implementing an attack on the AM of the practical system, the decrease in the attenuation ability of the AM leads to a decrease in the intensity of the signal light pulse, which in turn results in a decrease in the variance of the transmitted GMCS. Let the modulation variance of Alice (or Bob) be changed from V_μ to $V_\mu^{'}$, $\forall \mu \in \{A, B\}$. However, during the derivation of the secret key rate for both participants, they do not notice the change in variance, and thus they use the incorrect modulation variances to estimate the secret key rate. In addition, during this process, because of the errors occurring in the variances, the transmittance $T_{\mu C}$ and the

excess noise ϵ of the quantum channel are also underestimated as $T_{\mu C}^{'}$ and $\epsilon^{'}$, respectively. Therefore, the secret key rate can be incorrectly estimated as

$$K_{\mathrm{e}} = K(V_A, V_B, T, \epsilon), \tag{22}$$

where the parameters T and ϵ are given by

$$\begin{aligned} T &= \frac{T_{AC} V_B}{T_{BC}(V_B + 2)} \\ \epsilon &= \frac{T_{BC}(\epsilon_{BC} - 2) + 2}{T_{AC}} + \epsilon_{AC}. \end{aligned} \tag{23}$$

However, the actual key rate using the correct parameters should be

$$K_{\mathrm{c}} = K(V_A^{'}, V_B^{'}, T^{'}, \epsilon^{'}), \tag{24}$$

where the parameters $V_A^{'}$, $V_B^{'}$, $T^{'}$, and ϵ' are given by

$$\begin{aligned} &V_A^{'} = gV_A, V_B^{'} = gV_B, \\ &T^{'} = \frac{gT_{AC} V_B}{T_{BC}(gV_B + 2)}, \\ &\epsilon^{'} = \frac{T_{BC}}{T_{AC}}\left(\frac{\epsilon_{BC}}{g} - 2\right) + \frac{\epsilon_{AC}}{g} + \frac{2}{gT_{AC}}. \end{aligned} \tag{25}$$

The above-derived parameters play a major role in influencing the practical security of the attacked CV-MDI-QKD system. Subsequently, we considered the effect of the leakage attack on the secret key rate through numerical simulations.

4.2.2. Numerical Simulations

The secret key rate can be obviously boosted by increasing the repetition rate of the system, where the embedded AM plays an important role in pulse modulations [9]. In what follows, we continue to demonstrate the practical security through simulating the effect of the AM on the system.

In order to illustrate the performance of the CV-MDI-QKD system when performing the AM-involved attack strategy, we set a series of parameters for numerical simulations. For example, we took the attenuation coefficient of a standard fiber link as 0.2 db/km, the detection efficiency $\eta = 0.5$, the electronic noise of the imperfect heterodyne detector $v_{el} = 0.05$, and the reconciliation efficiency $\beta = 0.95$. Moreover, we assumed the intensity of the phase reference $E_R^2 = 1000$, the number of the ADC quantization $n_{\mathrm{ADC}} = 10$, the AM dynamics d_{dB} = 40, and the finite extinction ratio R_e = 40 dB and R_p = 30 dB, respectively.

In Figure 3, we depict the relationship of the secret key rate and the transmission distance for the CV-MDI-QKD system under leaked information. The parameters for numerical simulations were set to $V_A = V_B = 4$, $\epsilon = 10^{-10}$, and $N = 7 \times 10^9$. The nonsecure region was derived from the differential equation $K_e - K_c$, where K_e is the theoretical key rate in Equation (22), and K_c is the actual key rate in Equation (24). This region is located between the red curve and the blue curve shown in Figure 3. It also indicates the leaked information that Eve could steal from the CV-MDI-QKD system without being discovered by legitimate participants. When the actual secret key rate falls under the insecure region, it is trustworthy, even in the presence of half of the information leakage due to the AM of 1 GHz. The secret key rate of the CV-MDI-QKD system falls within the not-secure region only when the leaked information is present and is not detected by the system. This implies that the leaked light pulse could open security vulnerabilities, allowing Eve to acquire the leaked key information.The upper region signifies that if the secret key rate falls within this area, the security of the secret key rate is compromised, irrespective of issues with the leaked light pulse. The unsecure region indicates the leaked information that Eve could use

to steal the secure key from the system without being discovered by legitimate participants. Moreover, it is noted that the misestimated secret key rate increases together with the degree of being misestimated as Eve's attack intensity increases, according to an increase in the area between the correct key rate curve and the misestimated key rate curve. It means that as the attack intensity increases, Eve can steal more key information, making the attack strategy much more effective.

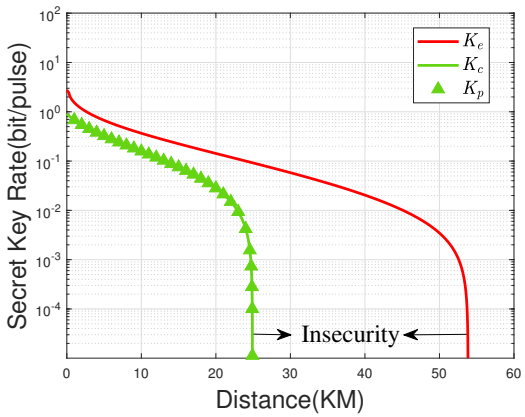

Figure 3. Secret key rate vs. the transmission distance of the CV-MDI-QKD system under an AM-involved attack. The red line represents the curve for the misestimated secret key rate, whereas the green line represents the curve for the correct secret key rate. The triangle line represents the curve for the actual secret key rate when Eve performs the AM-involved attack.

While considering effect of the LLO scheme on the system, we examined the secret key rate in a scenario while using the orthogonal LLO scheme (K_{OC}), which we compared with the sequential LLO scheme (K_{SC}) and the TLO scheme (K_{TC}), as shown in Figure 4. We found that the orthogonal LLO scheme performed better than the other schemes because of the impact of the excess noise of the channels. The effect of excess noise is shown in Figure 5 with the orthogonal LLO scheme with excess noises $\epsilon_{AC} = \epsilon_{BC} = 0.01$ or $\epsilon_{AC} = \epsilon_{BC} = 0.05$. Though the LLO scheme can be performed for the isolation of the signal pulse and the reference pulse through optical channels, there is still excess noise generated on Charlie's side. In the sequential LLO-involved system and the TLO-involved system, the increase in excess noise in the optical channels can enhance the effectiveness of the AM-involved attack, allowing Eve to steal more of the leaked information [27,28]. However, in the orthogonal LLO scheme, the increase in the excess noise in the optical channels has little effect on the secret key rate. Actually, the area of the space between the two curves does not change obviously with increasing excess noise.

When operating in practice, suitable appended apparatuses are usually expected to be equipped either for performance improvement or for protection of potential attacks. Fortunately, when performing the pulse modulation of the AM at high speed, the information leaked can be detected through experiments, which can be employed for detection of a potential attacker who attempts to steal the information from raw keys. As a countermeasure, one can make use of a fraction of the signal pulse before the AM to check the varied modulation variance V_μ. We show the relationship between the secret key rate and transmission distance while taking into account the effect of modulation variance in Figure 6. We found that the area of the space between the two solid lines is larger than that of the space between two dashed lines. Therefore, for a larger modulation variance, the attack is more effective because of the impact of the modulation variance on the secret key rate of the system.

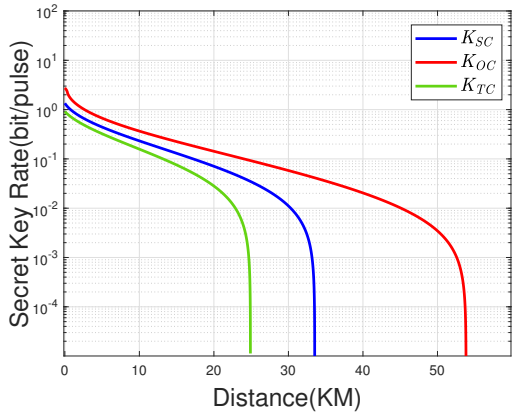

Figure 4. Secret key rate vs. the transmission distance of the CV-MDI-QKD system for the orthogonal LLO scheme (K_{OC}), the sequential LLO scheme (K_{SC}), and the traditional LLO scheme (K_{TC}). We set $\epsilon_{AC} = \epsilon_{BC} = 0.01$ in a symmetric case.

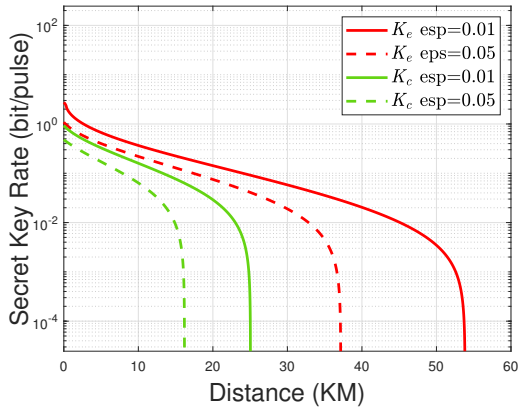

Figure 5. Secret key rate vs. the transmission distance of the CV-MDI-QKD system for $\epsilon_{AC} = \epsilon_{BC} = 0.01$ and $\epsilon_{AC} = \epsilon_{BC} = 0.05$. The solid-line curve represents the secret key rate of the symmetric system for $\epsilon_{AC} = \epsilon_{BC} = 0.01$, whereas the dashed-line curve represents the secret key rate of the symmetric system for $\epsilon_{AC} = \epsilon_{BC} = 0.05$.

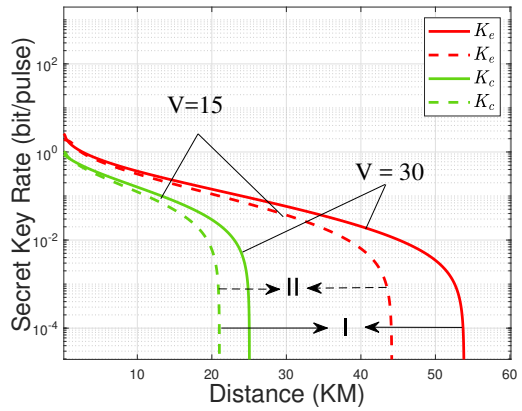

Figure 6. Secret key rate vs. the transmission distance of the CV-MDI-QKD system when considering effect of the tunable modulation variance for $V \in \{15, 30\}$. The solid line represents the secret key rate for $v = 30$, while the dashed line represents the secret key rate for $V = 15$.

Following the above analysis, Eve can obtain the leaked information resulting from the imperfect AM while performing an AM-involved attack in CV-MDI-QKD. Even a slight increase in the intensity of the prepared quantum states results in a substantial

overestimation of the secret key rate. Therefore, Eve may steal key information without being discovered by legitimate participants, which threatens the practical security of the system. As the intensity of the attacked light pulse increases, the effectiveness of the AM-involved attack becomes stronger, allowing Eve to steal more key information.

5. Conclusions

We proposed an LLO-based CV-MDI-QKD system with orthogonal block transformation, from which the signal pulse can be isolated from the reference pulse, and the access noise can hence be suppressed through the orthogonal channels. The noise mode in the LLO regime can be designed with the theoretical ability to analyze the performance of the CV-MDI-QKD system. In addition, we delved into the influence of the AM-induced leaked information in the CV- MDI-QKD system. The numerical simulations showed that the proposed orthogonal LLO scheme can outperform the previous LLO scheme. The findings also reveal that the leaked light pulse can result in deviations in the transmitted light pulse and thus underestimate the excess noise in optical channels. This effect causes an overestimation of the secret key rate, creating a security vulnerability to a feasible attack related to an imperfect AM. The result, particularly in the context of the high-speed modulation, contributes to understanding the AM-involved practical security and aids in the practical development of CV- MDI-QKD. Additionally, our assessment of the AM-involved leaked information shows that Alice and Bob can evaluate the parameters precisely, enabling the accurate analysis of the performance degradation in the CV-MDI-QKD system. This comprehensive understanding enhances the practical implementation ability of the CVQKD system.

Author Contributions: Conceptualization, writing—original draft preparation, Y.G. (Yewei Guo); validation and formal analysis, H.Z.; supervision, Y.G. (Ying Guo). All authors have read and agreed to the published version of this manuscript.

Funding: This work is supported was the Key Project of Scientific Research of Hunan Provincial Education Department (grant No. 22A0669), and the Hunan Provincial Natural Science Foundation of China (grant Nos. 2022GK2016, 2023JJ50268, 2023JJ50269).

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

Acknowledgments: Thanks to Dazu Huang for supporting the research in this article.

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

Appendix A. Secret Key Rate

Let us assume that Bob's state preparation and displacement operation are untrusted. Under this assumption, the proposed CV-MDI-QKD is equivalent to the traditional one-way CVQKD in which coherent states and heterodyne detection are used. In this context, the additional noise and the quantum channel transmittance between Alice (or Bob) and Charlie are denoted as ϵ_{AC} (or ϵ_{BC}) and T_{AC} (or T_{BC}) ,respectively. The Shannon mutual information between Alice and Bob becomes [26]

$$I_{AB} = \log_2 \left[\frac{1 + T(V_A + \chi_{line} + 1)}{1 + T(1 + \chi_{line})} \right], \tag{A1}$$

where $T = k^2 T_{AC}/2$, $\chi_{line} = 1/T + \epsilon - 1$, and $V_B = 1/2 + T(\chi_{line} + 1)/2$. In order to minimize ϵ, we assign $k = \sqrt{2V_B/T_{BC}(V_B + 2)}$, and hence the covariance matrix between Alice and Bob is described as

$$\gamma_{AB} = \begin{bmatrix} aI_2 & c\delta_z \\ c\delta_z & bI_2 \end{bmatrix}, \tag{A2}$$

where

$$\begin{aligned} a &= (V_A + 1), \quad b = T(V_A + \epsilon) + 1, \\ c &= \sqrt{T[(V_A + 1)^2 - 1]}, \quad \epsilon = \frac{T_{BC}(\epsilon_{BC} - 2) + 2}{T_{AC}} + \epsilon_{AC}. \end{aligned} \tag{A3}$$

Furthermore, the Holevo bound between Bob and Eve can be represented as

$$\chi_{BE} = \sum_{i=1}^{2} G(\frac{\lambda_i - 1}{2}) - G(\frac{\lambda_3}{2}), \tag{A4}$$

where $G(x)$ is the entropic function, and

$$\begin{aligned} \lambda_1^2 &= \frac{1}{2}(A + \sqrt{A^2 - 4B}), \\ \lambda_2^2 &= \frac{1}{2}(A - \sqrt{A^2 - 4B}), \\ \lambda_3 &= \frac{(T\epsilon + 2)(V_A + 1) - TV_A}{T(\epsilon + V_A) + 2}, \end{aligned} \tag{A5}$$

with notations $A = a^2 + b^2 - 2c^2$ and $B = ab - c^2$.

References

1. Weedbrook, C.; Pirandola, S.; Garcia-Patron, R.; Cerf, N.J.; Ralph, T.C.; Shapiro, J.H.; Lloyd, S. Gaussian quantum information. *Rev. Mod. Phys.* **2012**, *84*, 621. [CrossRef]
2. Notarnicola, M.N.; Olivares, S. Long-distance continuous-variable quantum key distribution with feasible physical noiseless linear amplifiers. *Phys. Rev. A* **2023**, *108*, 022404. [CrossRef]
3. Zhang, J.; Wang, X.; Xia, F.; Yu, S.; Chen, Z. Multiple-quadrature-amplitude-modulation continuous-variable quantum key distribution realization with a downstream-access network. *Phys. Rev. A* **2024**, *109*, 052429. [CrossRef]
4. Weedbrook, C. Continuous-variable quantum key distribution with entanglement in the middle. *Phys. Rev. A* **2013**, *87*, 022308. [CrossRef]
5. Pirandola, S.; Laurenza, R.; Ottaviani, C.; Banchi, L. Fundamental limits of repeaterless quantum communications. *Nat. Commun.* **2017**, *8*, 15043. [CrossRef]
6. Peng, Q.; Gao, B.; Wang, D.; Liao, Q.; Zuo, Z.; Zhong, H.; Huang, A.; Guo, Y. Defending against a laser-seeding attack on continuous-variable quantum key distribution using an improved optical power limiter. *Phys. Rev. A* **2023**, *108*, 052616. [CrossRef]
7. Wang, N.; Du, S.; Liu, W.; Wang, X.; Li, Y.; Peng, K. Long-distance continuous-variable quantum key distribution with entangled states. *Phys. Rev. Appl.* **2018**, *10*, 064028. [CrossRef]
8. Jouguet, P.; Kunz-Jacques, S.; Leverrier, A. Long-distance continuous-variable quantum key distribution with a Gaussian modulation. *Phys. Rev. A* **2011**, *84*, 062317. [CrossRef]
9. Wang, T.; Huang, P.; Zhou, Y.; Liu, W.; Zeng, G. Pilot-multiplexed continuous-variable quantum key distribution with a real local oscillator. *Phys. Rev. A* **2018**, *97*, 012310. [CrossRef]
10. Qi, B.; Lougovski, P.; Pooser, R.; Grice, W.; Bobrek, M. Generating the Local Oscillator Locally in Continuous-Variable Quantum Key Distribution Based on Coherent Detection. *Phys. Rev. X* **2015**, *5*, 041009. [CrossRef]
11. Huang, D.; Huang, P.; Wang, T.; Li, H.S.; Zhou, Y.M.; Zeng, G.H. Continuous-variable quantum key distribution based on a plug-and-play dual-phase-modulated coherent-states protocol. *Phys. Rev. A* **2016**, *94*, 032305. [CrossRef]
12. Pirandola, S.; Ottaviani, C.; Spedalieri, G.; Weedbrook, C.; Braunstein, S.L.; Lloyd, S.; Gehring, T.; Jacobsen, C.S.; Andersen, U.L. High-rate measurement-device-independent quantum cryptography. *Nat. Photon* **2015**, *9*, 397–402. [CrossRef]
13. Xu, F.; Ma, X.; Zhang, Q.; Lo, H.-K.; Pan, J.-W. Secure quantum key distribution with realistic devices. *Rev. Mod. Phys.* **2020**, *92*, 025002. [CrossRef]
14. 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. [CrossRef]
15. Lo, H.-K.; Curty, M.; Qi, B. Measurement-device-independent quantum key distribution. *Phys. Rev. Lett.* **2012**, *108*, 130503. [CrossRef]
16. Braunstein, S.L.; Pirandola, S. Side-channel-free quantum key distribution. *Phys. Rev. Lett.* **2012**, *108*, 130502. [CrossRef]
17. Patron, R.G.; Cerf, N.J. Unconditional optimality of Gaussian attacks against continuous-variable quantum key distribution. *Phys. Rev. Lett.* **2006**, *97*, 190503. [CrossRef]

18. Qin, H.; Kumar, R.; Makarov, V. Homodyne-detector-blinding attack in continuous-variable quantum key distribution. *Phys. Rev.* **2018**, *98*, 012312. [CrossRef]
19. Huang, D.; Lin, D.K.; Huang, P.; Zeng, G.H. Continuous-variable quantum key distribution with 1 Mbps secure key rate. *Opt. Lett.* **2015**, *40*, 3695. [CrossRef]
20. Leverrier, A.; Grangier, P. Unconditional security proof of long-distance continuous-variable quantum key distribution with discrete modulation. *Phys. Rev. Lett.* **2009**, *102*, 180504. [CrossRef]
21. Yang, J.; Xu, B.J.; Guo, H. Source monitoring for continuous-variable quantum key distribution. *Phys. Rev. A* **2012**, *86*, 042314. [CrossRef]
22. Huang, P.; Fang, J.; Zeng, G.H. State-discrimination attack on discretely modulated continuous-variable quantum key distribution. *Phys. Rev. A* **2014**, *89*, 042330. [CrossRef]
23. Inoue, K.; Honjo, T. Modified general individual attack against differential-phase-shift quantum key distribution. *Phys. Rev. A* **2024**, *110*, 042626. [CrossRef]
24. Zheng, Y.; Wang, Y.; Fang, C.; Shi, H.; Pan, W. Practical security of continuous-variable quantum key distribution with an optical amplifier. *Phys. Rev. A* **2024**, *109*, 022424. [CrossRef]
25. Huang, J.Z.; Weedbrook, C.; Yin, Z.Q.; Wang, S.; Li, H.W.; Chen, W.; Guo, G.C.; Han, Z.F. Quantum hacking of a continuous-variable quantum-key-distribution system using a wavelength attack. *Phys. Rev. A* **2013**, *87*, 062329. [CrossRef]
26. Liao, Q.; Wang, Y.; Huang, D.; Guo, Y. Dual-phase-modulated plug-and-play measurement-device-independent continuous-variable quantum key distribution. *Opt. Express* **2018**, *26*, 19907–19920. [CrossRef]
27. Ghalaii, M.; Pirandola, S. Continuous-variable measurement-device-independent quantum key distribution in free-space channels. *Phys. Rev. A* **2023**, *108*, 042621. [CrossRef]
28. Ma, H.-X.; Huang, P.; Bai, D.-Y.; Wang, T.; Wang, S.-Y.; Bao, W.-S.; Zeng, G.-H. Long-distance continuous-variable measurement-deviceindependent quantum key distribution with discrete modulation. *Phys. Rev. A* **2019**, *99*, 022322. [CrossRef]
29. Yang, H.; Liu, S.; Yang, S.; Lu, Z.; Li, Y.; Li, Y. High-efficiency rate-adaptive reconciliation in continuous-variable quantum key distribution. *Phys. Rev. A* **2024**, *109*, 012604. [CrossRef]