Article

# Phase-Matching Continuous-Variable Measurement-DeviceIndependent Quantum Key Distribution 

Peng Huang ${ }^{1,2, *(D)}$, Tao Wang ${ }^{1,2}$, Duan Huang ${ }^{3}$ and Guihua Zeng ${ }^{1,2, *}$<br>1 State Key Laboratory of Advanced Optical Communication Systems and Networks, Center for Quantum Sensing and Information Processing, Shanghai Jiao Tong University, Shanghai 200240, China; tonystar@sjitu.edu.cn<br>2 Shanghai Research Center for Quantum Sciences, Shanghai 201315, China<br>3 School of Computer Science and Engineering, Central South University, Changsha 410083, China; duanhuang@csu.edu.cn<br>* Correspondence: huang.peng@sjtu.edu.cn (P.H.); ghzeng@sjtu.edu.cn (G.Z.)

Citation: Huang, P.; Wang, T.; Huang D.; Zeng, G. Phase-Matching Continuous-Variable Measurement-Device-Independent Quantum Key Distribution. Symmetry 2022, 14, 568.
https://doi.org/10.3390/ sym14030568

Academic Editor: Alexander Shelupanov

Received: 12 February 2022
Accepted: 11 March 2022
Published: 13 March 2022
Publisher's Note: MDPI stays neutral with regard to jurisdictional claims in published maps and institutional affiliations.


Copyright: © 2022 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/).


#### Abstract

Continuous-variable measurement-device-independent quantum key distribution (CV-MDI-QKD) allows remote parties to share information-theoretical secure keys while defending all the side-channel attacks on measurement devices. However, the secure transmission distance and the secret key rate are quite limited due to the high untrusted equivalent excess noise in the Gaussian modulation. More particularly, extremely high-efficiency homodyne detections are required for even non-zero secure transmission distances, which directly restrict its practical realization. Here, we propose a CV-MDI-QKD protocol by encoding the key information into matched discrete phases of two groups of coherent states, which decreases the required detection efficiency for ideally asymmetric cases, and makes it possible to practically achieve secure key distribution with current low-efficiency homodyne detections. Besides, a proof-of-principle experiment with a locally generated oscillator is implemented, which, for the first time, demonstrates the realizability of CV-MDI-QKD using all fiber-based devices. The discrete-modulated phase-matching method provides an alternative direction of an applicable quantum key distribution with practical security.


Keywords: continuous-variable; measurement-device-independent; quantum key distribution; phase-matching

## 1. Introduction

Continuous-variable quantum key distribution (CV-QKD) [1-5] allows two remote authenticated users to establish a secure key through untrusted quantum channels, and authenticated classical channels, by using coherent detection. In particular, the secret keys are always encoded by Alice on the quadrature values [2,6,7] and the quadrature choices [8] of the quantized electronmagnetic field of coherent states, while they are distilled by homodyne or heterodyne detection in Bob's side and the cooperative postprocessing procedure. The CV-QKD protocols have inherent features of high transmission capacity, simple hardware implementation, and effective compatibility with already deployed classical optical communication systems. In addition, the ideal implementation of CVQKD can nearly approximate the ultimate limit of the secret key capacity of repeaterless quantum communication, i.e., the PLOB bound [9]. Since the ideal assumptions in the theoretical security proof of the CV-QKD protocol may be compromised in realistic implementations [10-14], eavesdroppers can exploit the security vulnerabilities arising from the imperfect implementations to capture the key information [15-22].

In order to thoroughly eliminate the practical security vulnerabilities at the measurement side, the Gaussian-modulated coherent-state (GMCS) continuous-variable measurement-device-independent quantum key distribution (CV-MDI-QKD) protocols are proposed [23-26]. In these CV-MDI-QKD schemes, two legitimate parties, Alice and Bob,
are both senders, and an untrusted third party, Charlie, is employed to perform Bell-State Measurement (BSM) and broadcast the outcomes to help to create the secret correlations between Alice and Bob. Despite the possibility that Charlie's station can be fully tampered with, the legitimate parties can still extract the secure keys under optimal coherent attacks via insecure quantum channels. Therefore, CV-MDI-QKD protocols can eliminate all sidechannel attacks against detections. In recent years, some breakthroughs have been made in the theoretical security study of CV-MDI-QKD [27-30].

Unfortunately, the theoretical performance, including the secret key rate and secure transmission distance of the GMCS CV-MDI-QKD, are quite limited because of the induced high equivalent excess noise [23,25]. In particular, almost perfect detections are required even for a non-zero secure transmission distance, which restricts its practical implementations $[14,23]$. In order to improve the performance and develop the practical realization, many efforts are currently being dedicated, such as developing the parameter estimation [31], employing photon subtraction [32], employing non-Gaussian postselection [33], and employing discrete modulation [34]. Recently, the concept of optimized communication strategies to enhance the information transfer over a non-Gaussian noisy channel is also proposed [35]. However, the practical realization remains a challenge issue, especially since extremely high-efficiency homodyne detection is still required even against individual attacks. So far, the only experimentally confirmed CV-MDI-QKD is the one based on the free-space transmission and the advanced detection techniques with an efficiency about $98 \%$ [23,36]. Practically, the overall efficiency of fiber-based homodyne detection is around $60 \%$ at telecom wavelengths [37-41]. Therefore, the full implementation of CV-MDI-QKD with practical lengths of optical fibers has not been reported on in the literature yet [14]. However, there are efforts to extend the robustness of CV-MDI-QKD by resorting to postselection, such as in [42].

In this paper, we propose a realizable CV-MDI-QKD protocol by encoding the key information into some discrete specific phases. When Alice and Bob's discrete encoding phases match each other, the correlation between them can be established after Charlie publicly announces the outcomes of the two homodyne detectors. When comparing the conventional GMCS CV-MDI-QKD schemes, the proposed discrete-modulated phase-matching (DMPM) CV-MDI-QKD protocol can theoretically achieve secure key distribution with current low-efficiency detections for the ideally asymmetric case, against a typical and powerful non-Gaussian individual attack, which could reach the quantum limit of the discrimination of the discrete encoded quantum states. Moreover, we demonstrate the realizability of the proposed scheme by performing a proof-of-principle experiment with a local oscillator (LO) and realistic homodyne detection over standard single-mode fiber (SMF) spools. The proposed protocol can be applied in an access network for cryptography communications.

For simplicity, we start by introducing the DMPM protocol. We then analyze the security of the proposed scheme under the SD attacks and show the corresponding numerical simulation performances. Finally, the experimental realizability of the proposed phase-matching scheme under realistic conditions is demonstrated.

## 2. DMPM CV-MDI-QKD Protocol

The proposed DMPM CV-MDI-QKD protocol, which is illustrated in Figure 1, can be described as follows.

Step 1. Alice and Bob prepare four coherent states: $\left|\alpha e^{k \pi i / 2}\right\rangle$ with $k \in\{0,1,2,3\}$, respectively. The states $|\alpha\rangle$ and $\left|\alpha e^{\pi i}\right\rangle$ with encoded binary values 0 and 1, respectively, are called X-basis states, while $\left|\alpha e^{\pi i / 2}\right\rangle$ and $\left|\alpha e^{3 \pi i / 2}\right\rangle$ with encoded binary values of 0 and 1 , respectively, are called P-basis states.

Step 2. According to the binary random values, Alice and Bob choose the corresponding encoded coherent states randomly from X- or P-basis states, respectively. Then they simultaneously send them to Charlie through two different channels after adjusting for the intensities by VOAs.

Step 3. The received two modes ( $A_{1}$ and $B_{1}$ ) interfere at a 50:50 BS with two output modes $A_{1}^{\prime}$ and $B_{1}^{\prime}$ on Charlie's side. Then, both the X quadrature of $A_{1}^{\prime}$ and the P quadrature of $B_{1}^{\prime}$ are measured by homodyne detections, and the measurement results $\left\{X_{A_{2}}, P_{B_{2}}\right\}$ are broadcasted by Charlie.

Step 4. Alice and Bob publicly announce their bases. And according to Charlie's measurement results, they collect the corresponding binary RNG values with the same bases as strings $K_{A}$ and $K_{B}$, respectively, for the $X$-basis case $\left\{X_{A_{2}} \in \mathbb{R}:-\delta_{A} \leq X_{A_{2}} \leq \delta_{A}\right\}$ and for the P-basis case $\left\{P_{B_{2}} \in \mathbb{R}:-\delta_{B} \leq P_{B_{2}} \leq \delta_{B}\right\}$. Besides, they preserve the quadratures of the prepared inconsistent-basis states $\left\{X_{a}^{p}, P_{a}^{p}\right\}$ and $\left\{X_{b}^{p}, P_{b}^{p}\right\}$ as strings $K_{A}^{p}$ and $K_{B}^{p}$, respectively.

Step 5. Alice keeps her binary string $K_{A}$ unchanged, and Bob generates a modified binary string $K_{A}^{\prime}$ by flipping the bits in $K_{B}$ when the corresponding encoding states are P-basis states. After these operations, Alice and Bob share a set of correlated binary raw keys $\left\{K_{A}, K_{A}^{\prime}\right\}$.

Step 6. Alice and Bob perform a parameter estimation based on strings $K_{A}^{p}, K_{B}^{p}$ and the corresponding broadcasted results $\left\{X_{A_{2}}^{p}, P_{B_{2}}^{p}\right\}$, and then further distill a string of secret keys from $\left\{K_{A}, K_{A}^{\prime}\right\}$ with information reconciliation and privacy amplification processes through an authenticated public channel.


Figure 1. (Color online). The phase-matching CV-MDI-QKD scheme. RNG is random number generator, QM is quadrature phase-shift keying (QPSK) modulator, VOA is variable optical attenuator, BS is beam splitter, $\mathrm{Hom}_{0}$ is homodyne detection of measuring the X quadrature, $\mathrm{Hom}_{1}$ is homodyne detection of measuring the P quadrature, $T_{A(B)}$ and $\epsilon_{A(B)}$ are the transmission efficiency and excess noise of quantum channel between Alice (Bob) and Charlie, respectively.

In the proposed protocol, Alice and Bob prepare, independently, the coherent states, and the measurements are performed by a totally untrusted third party, Charlie. Here, Alice and Bob can optimize their amplitudes $\alpha$ and the phase-matching thresholds $\delta_{A}, \delta_{B}$ to maximize the evaluated secret key rate. The phase-matching conditions in step 4 and the decoding rules in step 5 give four effective secret key generation cases, as shown in Table 1.

Table 1. Key generation cases for Alice and Bob in DMPM CV-MDI-QKD protocol.

| Encoded States | Encoded Bits | Decoded Bits |
| :---: | :---: | :---: |
| $(\|\alpha\rangle,\|\alpha\rangle)$ | $(0,0)$ | $(0,0)$ |
| $\left(\left\|\alpha e^{\pi i}\right\rangle,\left\|\alpha e^{\pi i}\right\rangle\right)$ | $(1,1)$ | $(1,1)$ |
| $\left(\left\|\alpha e^{\pi i / 2}\right\rangle,\left\|\alpha e^{3 \pi i / 2}\right\rangle\right)$ | $(0,1)$ | $(0,0)$ |
| $\left(\left\|\alpha e^{3 \pi i / 2}\right\rangle,\left\|\alpha e^{\pi i / 2}\right\rangle\right)$ | $(1,0)$ | $(1,1)$ |

## 3. Eavesdropping and Simulations

Here, we exemplify the security of the proposed protocol under a typical and powerful non-Gaussian individual attack, i.e., the beam-splitting (BS) and partial intercept-resend (IR) attacks, combined with the SD attacks [43], which are constructed by a SD receiver [44-47] and a heralded noiseless linear amplifier (NLA) [48-51]. Specifically, Eve can apply SD receivers to directly capture the discrete-encoded secret key with low average error probability, which has two lower bounds, i.e., the standard quantum limit (SQL) $P_{\text {SQL }}$ and the quantum limit (QL) $P_{\mathrm{QL}}$ [44-47], respectively. Here, SQL defines the minimum average error probability with which the nonorthogonal states can be distinguished by directly measuring the encoded physical observable coherent states, such as the intensity and phase, with conventional receivers. The QL is a lower bound which is fundamentally allowed in quantum mechanics, and it is shown in [43] that for the discrete-modulated types of CVQKD schemes, the SD attacks are powerful and can be almost close to optimal levels when combined with the NLA in some specific conditions.In practical scenarios, the phase-matching thresholds $\delta_{A}, \delta_{B}$ should be set according to the parameter estimation of the two quantum channels. Here, we will consider two typical cases, i.e, the symmetric case that the transmission efficiencies and excess noises of the two quantum channels are both $T$ and $\varepsilon_{c}$, and the ideally asymmetric case has a transmission efficiency $T_{B}=1$ and excess noises $\varepsilon_{B}=0, \varepsilon_{A}=\varepsilon_{c}$, respectively. For the symmetric or asymmetric cases, Alice and Bob can adjust their VOAs to balance the total transmission efficiencies to optimize the performance.

For the BS-combined SD attacks, Eve first performs a standard BS attack on the transmitted signals, then she takes SD attacks on the split photons to directly capture the secret key information after the announcement of bases and Charlie's measurement outcomes. Thus, she can decrease the discrimination error probability by just discriminating the nonorthogonal coherent states in a binary phase-shift keying (BPSK) format, other than QPSK. For the symmetric case, Eve will directly discriminate Bob's states for eavesdropping when using reverse reconciliation. While for the ideally asymmetric case, Eve needs to judge Bob's encoded keys according to Charlie's measurement outcomes and the results of the SD attacks on Alice's states. It should be mentioned that Eve will amplify the split coherent states with a heralded NLA to further lower the discriminating error probability, but with a probability of success. In this way, when the legitimate parities set the suitable intensity of coherent states and phase-matching thresholds, Eve can not obtain the secret key for both symmetric and ideally asymmetric cases. See the Appendixes A and B for further details about the calculation of the secret key rate under BS-combined SD attacks.

For the IR attacks, Eve intercepts the transmitted quantum states from both Alice and Bob's stations (for symmetric or, ideally, asymmetric cases). In particular, Eve will control the untrusted party, Charlie, and intercept the transmitted states from Alice and Bob to perform perfect heterodyne detections. However, she will not resend the reproduced quantum state here, but will directly resend the forged broadcasted measurement results. Moreover, she can capture the secret key by using the measurement results of the intercepted quantum state through the channel between Bob and Charlie. In this way, Eve can obtain the secret key for both symmetric and, ideally, asymmetric cases. See the Appendix C for further details about the calculation of the secret key rate under the complete IR attacks.However, the error discrimination will induce extra excess noise, which could be
found by the legitimate parties in the parameter estimation. So, she will use the channel excess noise to cover her eavesdropping to try her best to capture the secret key.

Here, we evaluate the secret key rate under Eve's specific attack strategy for the symmetric and, ideally, asymmetric cases. In particular, if the total channel excess noise $\varepsilon_{c}^{t}$ is equal to, or larger than, the total extra excess noise $\varepsilon_{c}^{e}$ induced by the complete IR attacks, Alice and Bob cannot share the secure secret key, since Eve can replace the quantum channels with noiseless ones to cover the induced extra excess noise and capture all the secret keys by performing complete IR attacks. When $\varepsilon_{c}^{t}<\varepsilon_{c}^{e}$, Eve will perform partial IR attacks with the probability $\mu=\frac{\varepsilon_{c}^{t}}{\varepsilon_{c}^{c_{c}}}$ and will perform BS-combined SD attacks for other cases. Here, both the quantum channels are replaced with noiseless ones to cover Eve's induced extra excess noise. In this state, the secret key rate can be calculated as

$$
\begin{equation*}
R^{s(a)}=\beta I_{A B}^{s(a)}-I_{B E}^{s(a)}, \tag{1}
\end{equation*}
$$

where $I_{A B}^{s(a)}$ is the classical mutual information between Alice and Bob, $I_{B E}^{s(a)}$ is the leaked information to Eve, and $\beta$ is the reconciliation efficiency. Here, all the superscripts $s$ and $a$ denote the symmetric and asymmetric cases, respectively. See the Appendix D for further details about the evaluation of the secret key rate of the proposed protocol under the non-Gaussian individual attack.

As shown in Figure 2, the proposed CV-MDI-QKD protocol can achieve secure key distribution with a realistic low-efficiency homodyne detector for the ideally asymmetric case. The scheme is also sensitive to channel excess noise for both symmetric and, ideally, asymmetric cases. Moreover, there exists an optimal amplitude $\alpha$ and a threshold of $\delta_{A}\left(\delta_{B}\right)=\kappa \alpha$ for the given transmission distance and channel excess noise. Therefore, one can optimize the amplitude and thresholds to maximize the secret key rate and the secure transmission distance. It should be mentioned that the secure transmission distances for both the symmetric and, ideally, asymmetric cases are limited to the access network, since the direct IR attack utilizes the untrusted property of the measurement party, Charlie. Moreover, it restricts the required detection efficiency (RDE) (at least larger than 0.5, in theory) to guarantee a positive secret key rate for both the symmetric and, ideally, asymmetric cases. However, due to the restriction of the direct access to the encoded states from Bob's station in the BS-combined SD attacks, the demand of extremely high-efficiency homodyne detection is removed for the ideally asymmetric case.

The RDE for the different transmission distances in an ideally asymmetric case are depicted in Figure 3. The results show that the proposed protocol exhibits the capability of low RDE, which can be well implemented in realistic conditions. Compared to the conventional GMCS CV-MDI-QKD protocol [25] under the general individual attacks [52] with similar parameters (the modulation variance is set under the practical condition $V_{A}=V_{B}=39$ [25]) for the ideally asymmetric case, the RDEs of the proposed scheme are lower for most of the reachable secure transmission distances when the SD receivers reach SQL and QL. Specifically, the RDEs are 0.5344 and 0.5342 for the non-zero secure transmission distance when the SD receivers reach SQL and QL without the consideration of finite-size effects, respectively. While the RDEs are $0.6722,0.7837$, and 0.8870 for conventional GMCS CV-MDI-QKD protocols under the same type of non-Gaussian individual, as well as the general individual and collective attacks, respectively. However, for the symmetric case, the RDEs of the proposed DMPM CV-MDI-QKD are similar to the ones of conventional GMCS CV-MDI-QKD protocols, which are all approximately 0.7 for the same parameters.


Figure 2. (Color online). The secret key rates for different channel excess noises when the SD receivers reach QL and SQL, respectively. The results are compared to the PLOB bound [9]. The other parameters are set as $\eta=0.9, \alpha=1.1, \kappa=0.25 \sqrt{2 \eta T}$ (for symmetric case), $\eta=0.6, \alpha=2.5$, $\kappa=0.5 \sqrt{2 \eta T}$ (for ideally asymmetric case), $v_{e l}=0.04, \beta=0.98, g=1$.


Figure 3. (Color online). The RDEs as a function of transmission distance for ideally asymmetric case when the SD receivers reach QL and SQL. The other parameters are set as $\alpha=2.5, \varepsilon_{c}=0.02$, $v_{e l}=0.04, \beta=0.98, g=1, \kappa=0.5 \sqrt{2 \eta T}$.

## 4. Proof-of-Principle Experiment

For the realistic implementation of the proposed DMPM CV-MDI-QKD scheme, the key issues are the interference and random phase drifts between the two remote independent lasers. By using frequency-locking and phase-reference techniques, the latest experiments $[53,54]$ show the feasibilities of this kind of interference and phase compensation, with even weaker optical signals and a much longer transmission distance. Recently, an alternative method was proposed and demonstrated experimentally by using carrier synchronization to compensate the frequency offsets and phase drifts for the similar interference of continuous-variable quantum states with the local-LO implementation [55]. These methods pave the way for the realistic implementation of the proposed scheme.

Inspired by the method proposed in [55], a proof-of-principle experiment for the ideally asymmetric case of the DMPM CV-MDI-QKD protocol is designed here with the local-LO. It should be mentioned that the local-LO realization shows the superiority of the compatibility of the continuous-variable technique with classical optical communication, which is a promising direction for high-speed, high-integration, and low-cost applications. The schematic diagram is shown in Figure $4 . L_{1}$ is a narrow linewidth frequency-stabilized laser with a center wavelength of 1542.38 nm and a linewidth around 150 kHz , which is employed to generate both Alice and Bob's signal states. The generated continuous-wave light (Wavelength Reference, Clarity-NLL-1542-HP) is split into two beams used as the carriers from Alice and Bob. The emission power of $L_{1}$ is controlled at -40 dbm , which meets the requirements of modulation variance in the theoretical protocol. Two VOAs are applied to control the intensities of the optical signals, where the signal includes $M$ consecutive pilot signals and cascaded $N$ consecutive data signals. The pilot signals are used for the cursory estimation of the frequency offset between the signals and the local-LO, and some of the data signals are used for further estimations of frequency offset and phase drifts caused by the fluctuations in the path length.


Figure 4. (Color online). The schematic diagram of the proof-of-principle experiment of the proposed phase-matching CV-MDI-QKD scheme. $L_{1}, L_{2}$ : the lasers with stabilized frequencies, BS: beamsplitter, VOA: variable optical attenuator, SMF: single mode fiber, PC: polarization controller, PM: phase modulator, Hom: homodyne detector, PD: photoelectric detector, OSC: oscilloscope.

Since the state of polarization (SOP) in the single-mode fiber will change independently due to the birefringence effect, the SOP cannot be kept the same. After being transmitted through two $5-\mathrm{km}$ SMF spools with a measured loss of $0.2 \mathrm{~dB} / \mathrm{km}$ at 1542.38 nm , it is adjusted by the manual PCs to ensure that the polarization directions of the coherent states transmitted by Alice and Bob are consistent to interfere by a $50: 50 \mathrm{BS}$ at the receiver.Here, we consider the ideally asymmetric case, where one SMF spool is served as the quantum channel and the other is used as a the delay line to synchronize the two signals in Bob's station, which cannot be intercepted by Eve. The quantum channel between Bob and Charlie can be seen as the one with $T_{B}=1$ and $\varepsilon_{B}=0$. Here, the actual fiber coupling efficiency and the natural loss of the fiber are all attributed to the attenuation of the quantum channel, which has been analyzed in the theoretical analysis. Another frequency stabilized laser $L_{2}$ is used as the local-LO, which is the same type as $L_{1}$ and is also divided into two beams. The optical power of $L_{2}$ is controlled by a VOA at 5 dbm to meet the shot noise
detection requirement. Specifically, the power is adjusted while it is monitored in real-time by a power meter. Each of the LOs are mixed with one interference output followed by a homodyne detector with a $350-\mathrm{MHz}$ bandwidth to measure the quadratures $X_{A_{2}}$ and $P_{B_{2}}$, which contain the pilot segments $X_{P A_{2}}, P_{P B_{2}}$, and the data segments $X_{D A_{2}}, P_{D B_{2}}$. An oscilloscope with a $1 \mathrm{GS} / \mathrm{s}$ sampling rate is used to acquire the output results from the two homodyne detectors.

It should be mentioned that since we use a continuous-wave mode of the quantum signal, the bandwidth of the whole system mainly depends on the bandwidth of the homodyne detectors. Here, the cursory frequency offset estimation is firstly performed by using the acquired outputs from the pilot segments $X_{P A_{2}}$. In our experiment, this frequency offset $\delta f$ mainly originates from the phase noise caused by the spontaneous emission in two lasers, which is related to the linewidth and is around 15 MHz in this experiment. In order to perform a further estimate of the frequency offset and phase drift, some data signals should be revealed. To monitor the phase drift in the quantum channel, here, the interference output power is directly detected by a PD through port 2 , which reflects the phase drift of two optical fields after passing through their respective channels. The output is sampled as $2 \mathrm{kS} / \mathrm{s}$ and the result is shown in Figure 5a, and the average phase drift rate is $0.6541 \mathrm{rad} / \mathrm{ms}$. By using these values, Alice and Bob will modify their prepared values $\left\{X_{a(b)}, P_{a(b)}\right\}$ and $\left\{X_{a(b)}^{p}, P_{a(b)}^{p}\right\}$ with frequency their offset recovery and phase drift compensation algorithms. A parameter estimation can then be performed, just like in the original protocol. See the Appendix E for further details about the method of the frequency offset recovery and phase drift compensation.


Figure 5. (Color online). (a) Phase drift angle and phase drift rate change with time. (b) The excess noise and corresponding secret key rates for the ideally asymmetric case as a function of the size of frame. The other parameters are set as $\eta=0.6, v_{e l}=0.04, \beta=0.98, g=1, \kappa=0.5 \sqrt{2 \eta T}$.

For simplicity, here we don't perform modulation on the signal state and therefore random number generators are omitted, but measure the quadratures of the carrier signal, i.e., the quadratures $X_{A_{2}}$ and $P_{B_{2}}$ of pilot segments, and then perform communication simulations with constructed key data and the measured quadratures and monitored phase drifts for the same simulation model [55]. The result reflects the phase drift situation in the actual optical fiber channel and its influence on the theoretical performance. By adopting the algorithm we proposed in Ref. [55], the phase misalignment problem can be solved, and the practical realization of the proposed protocol can be guaranteed.

Especially, we evaluate the excess noise for different frame sizes, where the first symbol is used to compensate the phase of the next four symbols. It can be seen from Figure 5b that the excess noise increases with the frame sizes. The reason is that when the phase drift rate is specified, shorter frame can be used to track the phase drift more accurately, which reducing the excess noise caused by the phase deviation. More detailedly, the frame length affects the accuracy of phase compensation. Specifically, the designed phase compensation algorithm for phase drift is to make an overall compensation for each frame. If the length of a frame is longer, then the symbol phase drift in one frame is not consistent and has a significant difference, and the residual phase noise will become more prominent after the compensation. The secret key rates are also shown in Figure 5b, which are evaluated under the conditions that the length of the SMF spool served as the quantum channel is 2 km with the channel loss $0.2 \mathrm{~dB} / \mathrm{km}$ and $|\alpha|=2.5$. We can find that the frame size should be controlled smaller enough to guarantee secure key distribution.

## 5. Conclusions

We propose a realizable CV-MDI-QKD scheme by encoding the key information into some discrete and matched specific phases, where the correlation between the legitimate parities can be established after Charlie publicly announces the results of the homodyne detections. The eavesdropping analysis is provided under a typical non-Gaussian attack, which is constructed by an SD receiver and a heralded NLA, when combined with the BS and partial IR attacks. The simulation results show that the two legitimate parties can obtain a secure secret key at relatively short distances against the strongest SD attacks, even with the currently low-efficiency homodyne detections for an ideally asymmetric case. For the symmetric case, the demand of the high-efficiency homodyne detection remains.

Different from the conventional discrete-modulated CV-MDI-QKD and CVQKD protocols, the encoding of secret keys here is based on the choices of discrete-distributed matched specific phases, but not directly encoding the secret information on continuous-distributed quadrature values with further judgments. This encoding way efficiently decreases the RDE and weakens the effect of the channel's excess noise on the secret key rate, especially for the ideally asymmetric case, which is similar to the basis of the encoding for the QKD scheme [8] where the secret keys are encoded on the quadrature choices, i.e., the discretedistributed measurement bases of the Gaussian-modulated coherent states. However, the discrete modulation and phase-matching encoding lead to a low utilization efficiency and a low capacity of the quantum channel, thus restricting the secret key rate to a relatively low level. The proof-of-principle experiment, with a locally-generated LO, demonstrates, for the first time, that CV-MDI-QKD can be currently well implemented using fiber-based devices under realistic conditions, which also shows the potentiality to be further integrated with low-cost classical optical communications.

From the security analysis, we found that the proposed DMPM CV-MDI-QKD protocol is not able to overcome the PLOB bound. However, for the discrete-variable (DV) PM QKD protocol proposed in [56], it is shown that the secret key rate can overcome the PLOB bound. The fundamental reason may be that they have different physical principles of implementations, which leads to different security analyses frameworks. In the DV case, the PM QKD protocol executes based on single-photon interference, where the unfolding of the used Mach-Zehnder interferometer doubles the transmission distance. In the CV case, the proposed CV-MDI-QKD protocol is based on the first-order interference of the light
field quadratures of the multiphoton quantum states. The optical structure is the same as the one in the known Gaussian-modulated CV-MDI-QKD protocol, but it instead uses the phase-matching method with discrete-encoding. Thus, the performances of this protocol are also fundamentally restricted by the security framework of CV-QKD, and it is not able to overcome the PLOB bound. However, the introduction of the phase-matching method with discrete-encoding relatively increases the correlation between the legitimated parties, which, to some extent, relieves the required detection efficiency.

Here, the analysed non-Gaussian individual attack against the proposed scheme are realistic and important attacks for cryptography communication, which has been thoroughly studied in theory and in experiments [57,58]. Moreover, it is shown in [43] that for the discrete-modulated four-state CV-QKD schemes, the leaked information under the SD attacks can be larger than the Holevo bound that is calculated directly with the estimated parameters from the reconstructed covariance matrix under the linear channel assumption [7], when combining with the NLA in some specific conditions. Actually, the asymptotic security of the discrete-modulated CV-QKD against the collective attacks has only recently been proven [59]. The security has also been proven, in a composable finite-size way, against the collective Gaussian attacks [60]. In particular, a lower bound of the secret key rate is given for the four-state protocol, which is also lower than the one while assuming a linear channel [59]. This proof shows that the SD attacks are powerful and close to optimal, since the proposed protocol also performs essentially discrete modulations. Nevertheless, the security should be further developed against more general attacks. Under realistic conditions, the discrete modulation can achieve a high symbol rate to GHz , and the secret key rate with practical security can reach applicable levels for accessing networks in cryptography communications.

It should be mentioned here that the fiber chromatic dispersion and polarization mode dispersion will not affect the current theoretical protocols and experiments. It is because the symbol rate of the discrete-modulation, currently, is not high, less than G Baud. Therefore, under a single-mode fiber, chromatic dispersion and polarization mode dispersion will not cause inter-symbol crosstalk. However, if the operation symbol rate exceeds G Baud in the future, the influence of fiber dispersion needs to be further considered. Moreover, the protocol can be also applied in the case of the free-space quantum channel [61-63] and the encoding may be extended to the squeezed states [64] with discrete-modulation.

Author Contributions: P.H. and G.Z. conceived the research. T.W. carried out the proof-of-principle experiment. P.H. performed the security analysis. P.H. and D.H. analyzed the data and wrote the manuscript. All authors contributed to the data collection, discussed the results and reviewed the manuscript. All authors have read and agreed to the published version of the manuscript.
Funding: This work was supported by the National key research and development program (Grant No. 2016YFA0302600), the National Natural Science Foundation of China (Grants No. 61971276, 61631014), Shanghai Municipal Science and Technology Major Project (Grant No. 2019SHZDZX01), and the Key R\&D Program of Guangdong province (Grant No. 2020B030304002).
Institutional Review Board Statement: Not applicable.
Informed Consent Statement: Not applicable.
Data Availability Statement: Not applicable.
Conflicts of Interest: The authors declare no conflict of interest.

## Appendix A. Secret Key Rate under BS-Combined SD Attacks

For BS-combined SD attacks, Eve first performs a beam-splitting (BS) attack on the transmitted signals, i.e., Eve replaces the quantum channel with a perfect lossless and noiseless one, connecting a beam splitter with the transmission efficiency $T_{A}$ and $T_{B}$. Then, she performs SD attacks to directly capture the secret key information. We will first calculate the mutual information $I_{A B}^{B S}$ between Alice and Bob, then evaluate the mutual information
$I_{B E}^{B S}$ between Eve and Bob, and, finally, we will show the simulations of the secret key rate under the BS-combined SD attacks.

(a)

Figure A1. (Color online). (a) The description of the SD attack strategy on the phase-matching CV-MDI-QKD scheme. BS is beam splitter, PIA is phase-insensitive amplifier, $\mathrm{Hom}_{0}$ is homodyne detection of measuring the $X$ quadrature, $\mathrm{Hom}_{1}$ is homodyne detection of measuring the $P$ quadrature, $T$ is the transmission efficiency of quantum channel between Alice (Bob) and Charlie; (b) the construction of SD attack, NLA is noiseless linear amplifier.

## Appendix A.1. The Mutual Information $I_{A B}^{B S}$ between Alice and Bob

We first consider the symmetric case, i.e., the transmission efficiencies and excess noises of the two quantum channels, which are are both $T$ and $\varepsilon_{c}$. Here, Eve can directly discriminate Bob's states for reverse reconciliation to capture the secret key, or Eve can use both the results of the SD attack, through Alice and Bob's channels, to judge the encoded secret key. However, Eve's BS-combined SD attacks do not change the parameters of the quantum channels between Alice and Charlie, and Bob and Charlie. Therefore, Eve's operations will not affect the mutual information between Alice and Bob.

Here, the output intensities of Alice and Bob's states are a set equivalent. After the beam splitting and amplification operations, the quadratures of the output modes $A_{1}$ and $B_{1}$, in Figure A1, can be expressed as

$$
\begin{align*}
X_{A_{1}} & =\sqrt{T} X_{A_{0}}+\sqrt{1-T} X_{e}^{a}  \tag{A1}\\
P_{A_{1}} & =\sqrt{T} P_{A_{0}}+\sqrt{1-T} P_{e}^{a} \\
X_{B_{1}} & =\sqrt{T} X_{B_{0}}+\sqrt{1-T} X_{e}^{b} \\
P_{B_{1}} & =\sqrt{T} P_{B_{0}}+\sqrt{1-T} P_{e}^{b}
\end{align*}
$$

where $X_{e}^{a}\left(P_{e}^{a}\right)$ and $X_{e}^{b}\left(P_{e}^{b}\right)$ are the equivalent extra input quadratures of the thermal states controlled by Eve, and they satisfy $\left\langle\left(X_{e}^{a}\right)^{2}\right\rangle=\left\langle\left(P_{e}^{a}\right)^{2}\right\rangle=\left\langle\left(X_{e}^{b}\right)^{2}\right\rangle=\left\langle\left(P_{e}^{b}\right)^{2}\right\rangle=1+\frac{T}{1-T} \varepsilon_{c}$ in the shot noise unit (SNU). For a noisy channel, Eve can use a beam splitter and a cascaded phase-insensitive amplifier (PIA) with total transmission efficiencies $T=T_{1} g^{\prime}$ to split the photons as much as possible, thus reducing the error probability of her SD attacks. Here, $T_{1}$ is the transmission efficiency of the renewed beam splitter and $g^{\prime} \geqslant 1$ is the gain of the PIA (shown in Figure A8). This restricts the largest quantity of the mean photon number captured by Eve for the SD attacks to $\frac{2-2 T+T \varepsilon_{c}}{2+T \varepsilon_{c}}|\alpha|^{2}$ (see Appendix B for details).

After the interference, the quadratures of the output modes $A_{1}^{\prime}$ and $B_{1}^{\prime}$ in Charlie's side are given by

$$
\begin{align*}
X_{A_{1}^{\prime}} & =\frac{1}{\sqrt{2}}\left[\sqrt{T}\left(X_{A_{0}}-X_{B_{0}}\right)+\sqrt{1-T}\left(X_{e}^{a}-X_{e}^{b}\right)\right]  \tag{A2}\\
P_{A_{1}^{\prime}} & =\frac{1}{\sqrt{2}}\left[\sqrt{T}\left(P_{A_{0}}-P_{B_{0}}\right)+\sqrt{1-T}\left(P_{e}^{a}-P_{e}^{b}\right)\right] \\
X_{B_{1}^{\prime}} & =\frac{1}{\sqrt{2}}\left[\sqrt{T}\left(X_{A_{0}}+X_{B_{0}}\right)+\sqrt{1-T}\left(X_{e}^{a}+X_{e}^{b}\right)\right] \\
P_{B_{1}^{\prime}} & =\frac{1}{\sqrt{2}}\left[\sqrt{T}\left(P_{A_{0}}+P_{B_{0}}\right)+\sqrt{1-T}\left(P_{e}^{a}+P_{e}^{b}\right)\right] .
\end{align*}
$$

Then, we can get

$$
\begin{align*}
X_{A_{2}} & =\frac{1}{\sqrt{2}}\left[\sqrt{\eta T}\left(X_{A_{0}}-X_{B_{0}}\right)+\sqrt{\eta(1-T)}\left(X_{e}^{a}-X_{e}^{b}\right)\right]+\sqrt{1-\eta} X_{v}^{a}+X_{e l}  \tag{A3}\\
P_{B_{2}} & =\frac{1}{\sqrt{2}}\left[\sqrt{\eta T}\left(P_{A_{0}}+P_{B_{0}}\right)+\sqrt{\eta(1-T)}\left(P_{e}^{a}+P_{e}^{b}\right)\right]+\sqrt{1-\eta} P_{v}^{a}+P_{e l}
\end{align*}
$$

where $X_{v}^{a}\left(P_{v}^{b}\right)$ and $X_{e l}\left(P_{e l}\right)$ are the quadratures of the vacuum states and the electronic noise induced from the imperfect homodyne detection, respectively, and they satisfy $\left\langle\left(X_{v}^{a}\right)^{2}\right\rangle=\left\langle\left(P_{v}^{b}\right)^{2}\right\rangle=1$, and $\left\langle\left(X_{e l}\right)^{2}\right\rangle=\left\langle\left(P_{e l}\right)^{2}\right\rangle=v_{e l}$ in the SNU, respectively. Moreover, we have

$$
\begin{align*}
X_{A_{0}} & =X_{a}+X_{v, e}^{a}, P_{A_{0}}=P_{a}+P_{v, e r}^{a}  \tag{A4}\\
X_{B_{0}} & =X_{b}+X_{v, e}^{b}, P_{B_{0}}=P_{b}+P_{v, e}^{b}
\end{align*}
$$

where $X_{a(b)}, P_{a(b)}$ are the fixed values from the set $\{\alpha, 0,-\alpha\}$, where $\alpha$ is assumed to be a real and positive value, and $X_{v, e}^{a(b)}, P_{v, e}^{a(b)}$ are the quadratures of the vacuum states induced in the encoding step.

According to Alice and Bob's public basis announcements, they will discard one half of the measurement results with inconsistent bases. For the other half of the outcomes with consistent bases, $X_{a}=X_{b}$ for the X-basis case and $P_{a}=-P_{b}$ for the P-basis case, respectively, Alice and Bob can perform correct and effective decodings after basis reconciliation. For these two cases, one can always find that

$$
\begin{align*}
X_{A_{2}} & =X_{A_{2}}^{c}  \tag{A5}\\
& =\frac{1}{\sqrt{2}}\left[\sqrt{\eta T}\left(X_{v, e}^{a}-X_{v, e}^{b}\right)+\sqrt{\eta(1-T)}\left(X_{e}^{a}-X_{e}^{b}\right)\right]+\sqrt{1-\eta} X_{v}^{a}+X_{e l}, \\
P_{B_{2}} & =P_{B_{2}}^{c} \\
& =\frac{1}{\sqrt{2}}\left[\sqrt{\eta T}\left(P_{v, e}^{a}+P_{v, e}^{b}\right)+\sqrt{\eta(1-T)}\left(P_{e}^{a}+P_{e}^{b}\right)\right]+\sqrt{1-\eta} P_{v}^{a}+P_{e l},
\end{align*}
$$

and they follow the normal distribution as

$$
\begin{equation*}
X_{A_{2}}^{c}, P_{B_{2}}^{c} \sim \mathcal{N}\left(0,1+\eta T \varepsilon_{c}+v_{e l}\right) . \tag{A6}
\end{equation*}
$$

Because of the symmetry of the two bases, we assume $\delta_{A}=\delta_{B}$, and the correct and effective decoding probability can then be calculated as

$$
\begin{align*}
P_{\mathrm{BS}}^{c} & =\operatorname{Pr}\left(-\delta_{A}<X_{A_{2}}^{c}<\delta_{A}\right)=\operatorname{Pr}\left(-\delta_{B}<P_{B_{2}}^{c}<\delta_{B}\right)  \tag{A7}\\
& =\operatorname{Pr}\left(-\kappa \alpha<X_{A_{2}}^{c}<\kappa \alpha\right)=\operatorname{Pr}\left(-\kappa \alpha<P_{B_{2}}^{c}<\kappa \alpha\right) \\
& =\operatorname{erf}\left(\frac{\kappa \alpha}{\sqrt{2\left(1+\eta T \varepsilon_{c}+v_{e l}\right)}}\right)
\end{align*}
$$

where $\kappa \in \mathbb{R}$ is the decoding threshold, and $\operatorname{erf}(x)=\frac{2}{\sqrt{\pi}} \int_{0}^{x} e^{-t^{2}} d t$.
While $X_{a}=-X_{b}$ for the X-basis case and $P_{a}=P_{b}$ for the P-basis case, respectively, Alice and Bob will perform incorrect but effective decodings. For these two cases, one can find that

$$
\begin{align*}
X_{A_{2}} & =X_{A_{2}}^{w}  \tag{A8}\\
& =\frac{1}{\sqrt{2}}\left[\sqrt{\eta T}\left(2 X_{a}+X_{v, e}^{a}-X_{v, e}^{b}\right)+\sqrt{\eta(1-T)}\left(X_{e}^{a}-X_{e}^{b}\right)\right]+\sqrt{1-\eta} X_{v}^{a}+X_{e l}, \\
P_{B_{2}} & =P_{B_{2}}^{w} \\
& =\frac{1}{\sqrt{2}}\left[\sqrt{\eta T}\left(2 P_{a}+P_{v, e}^{a}+P_{v, e}^{b}\right)+\sqrt{\eta(1-T)}\left(P_{e}^{a}+P_{e}^{b}\right)\right]+\sqrt{1-\eta} P_{v}^{a}+P_{e l},
\end{align*}
$$

and they follow the normal distribution as

$$
\begin{align*}
X_{A_{2}}^{w} & \sim \mathcal{N}\left(\sqrt{2 \eta T} X_{a}, 1+\eta T \varepsilon_{c}+v_{e l}\right),  \tag{A9}\\
P_{B_{2}}^{w} & \sim \mathcal{N}\left(\sqrt{2 \eta T} P_{a}, 1+\eta T \varepsilon_{c}+v_{e l}\right),
\end{align*}
$$

where $X_{a}\left(P_{a}\right)$ values $\alpha$ or $-\alpha$ have the same probability. Similarly, we assume $\delta_{A}=\delta_{B}$, and the incorrect but effective decoding probability can be calculated as

$$
\begin{align*}
P_{\mathrm{BS}}^{w} & =\operatorname{Pr}\left(-\delta_{A}<X_{A_{2}}^{w}<\delta_{A}\right)  \tag{A10}\\
& =\operatorname{Pr}\left(-\delta_{B}<P_{B_{2}}^{w}<\delta_{B}\right) \\
& =\operatorname{Pr}\left(-\kappa \alpha<X_{A_{2}}^{w}<\kappa \alpha\right)=\operatorname{Pr}\left(-\kappa \alpha<P_{B_{2}}^{w}<\kappa \alpha\right) \\
& =\frac{1}{2}\left[\operatorname{erf}\left(\frac{\sqrt{2 \eta T} \alpha+\kappa \alpha}{\sqrt{2\left(1+\eta T \varepsilon_{c}+v_{e l}\right)}}\right)-\operatorname{erf}\left(\frac{\sqrt{2 \eta T} \alpha-\kappa \alpha}{\sqrt{2\left(1+\eta T \varepsilon_{c}+v_{e l}\right)}}\right)\right] .
\end{align*}
$$

Therefore, the key distribution channel between Alice and Bob can be seen as a binary symmetric channel (BSC) with utilization efficiency $P_{A B}^{\mathrm{BS}}=\frac{1}{4}\left(P_{\mathrm{BS}}^{c}+P_{\mathrm{BS}}^{w}\right)$, and quantum bit error rate (QBER) $P_{A B, e}^{\mathrm{BS}}=P_{\mathrm{BS}}^{w} /\left(4 P_{A B}^{\mathrm{BS}}\right)$. Thus, the mutual information between Alice and Bob under the BS-combined SD attack is given by

$$
\begin{equation*}
I_{A B}^{\mathrm{BS}}=P_{A B}^{\mathrm{BS}}\left[1-\mathrm{H}\left(P_{A B, e}^{\mathrm{BS}}\right)\right] . \tag{A11}
\end{equation*}
$$

While, for the asymmetric case (the total channel excess noise of two channels is the same as $2 \varepsilon_{c}$ ), Bob will adjust the VOA in his station, where the attenuation efficiency will be equivalent to the quantum channel between Alice and Charlie, such that the decoding procedures in Equations (A5) and (A8) can be guaranteed. Therefore, the mutual information between Alice and Bob under the BS-combined SD attack for the asymmetric case can be also given by the Equation (A11).

## Appendix A.2. The Mutual Information $I_{B E}^{B S}$ between Eve and Bob

Now, we turn to Eve's information from the BS-combined SD attack. We first consider the symmetric case. The detailed construction of the SD attack is shown in Figure A1b. Here, Eve can use both the results of the SD attack through Alice and Bob's channels to judge the encoded secret key. However, Eve just needs to discriminate Bob's states for reverse reconciliation. Since the legitimate parties will discard the ineffective results according to Charlie's measurement results, Eve will also optimize her eavesdropping to capture the secret key according to Charlie's measurement results.

Specifically, she will reserve the split photons in the beam splitting stage and will perform the SD attack after the announcement of the bases. Thus, she can decrease the discrimination error probability by just discriminating the nonorthogonal coherent states in a BPSK format other than a QPSK one. Moreover, Eve will amplify the split coherent states with a heralded NLA to further lower the discriminating error probability with a
success probability $P_{s} \leqslant \frac{1-\exp \left(-|\gamma|^{2}\right)}{1-\exp \left(-|g \gamma|^{2}\right)}$, where $g \geqslant 1$ is the gain of the NLA and $\gamma$ is the input amplitude of the coherent states. Moreover, according to Alice and Bob's public basis announcements, Eve will discard one half of the split states with the inconsistent bases. For the other half of the coherent states with consistent bases, we also consider the two cases, i.e., $X_{a}=X_{b}$ and $X_{a}=-X_{b}$ for the $X$-basis case and $P_{a}=-P_{b}$ and $P_{a}=P_{b}$ for the P-basis case. Because of symmetric encoding, we just consider the $X$-basis case in the following equations.

We suppose that when Eve fails in the implementation of the NLA, she will randomly choose one of the two coherent states, which will induce a $\frac{1}{2}\left(1-P_{s}\right)$ error probability in the decoding. Moreover, if Eve performs an incorrect discrimination of a coherent state sent from Alice or Bob's stations after the successful implementation of the NLA, it will induce a $P_{S} P_{\mathrm{SD}}^{b}$ error probability in decoding, where $P_{\mathrm{SD}}^{b}$ is the average error probability of Eve's SD receiver, which has two lower bounds, i.e., the standard quantum limit (SQL) $P_{\text {SQL }}$ and the quantum limit (QL) $P_{\mathrm{QL}}$ [44-47], respectively. In particular, the SQL defines the minimum average error probability with which the nonorthogonal states can be distinguished by directly measuring the encoded physical observable coherent states, such as the intensity and phase, with conventional receivers. The QL is a lower bound which is fundamentally allowed in quantum mechanics. The SQL for the discrimination of the amplified BPSK coherent states is given by [44]

$$
\begin{equation*}
P_{\mathrm{SQL}}^{g, b}=\frac{1}{2}[1-\operatorname{erf}(\sqrt{2} g \gamma)], \tag{A12}
\end{equation*}
$$

where $g \gamma$ is the amplified amplitude. The QL for the amplified signal in the BPSK format is expressed as

$$
\begin{equation*}
P_{\mathrm{QL}}^{g, b}=\frac{1}{2}\left[1-\sqrt{1-\exp \left(-4|g \gamma|^{2}\right)}\right] . \tag{A13}
\end{equation*}
$$

It should be mentioned that Eve will also discard the ineffective results according to Charlie's measurement results. Here, we consider the first case, i.e., $X_{a}=X_{b}\left(P_{a}=-P_{b}\right)$, and Alice and Bob perform correct and effective decodings with the probability $P_{\mathrm{BS}}^{c}$. There are two scenarios when referring to the SD attack results on Bob's states. Firstly, considering the successful probability of the implementation of the NLA and when Eve performs the incorrect discrimination of the state sent from Bob's station, the overall incorrect decoding probability will be

$$
\begin{equation*}
P_{\mathrm{BS}}^{1,1}=\frac{1}{2}-\frac{1}{2} P_{s}+P_{s} P_{\mathrm{SD}}^{b} . \tag{A14}
\end{equation*}
$$

Secondly, when Eve correctly discriminates the state sent from Bob's station, she will then capture the distributed secret information. Considering the successful probability of the implementation of the NLA, the overall probability of the information leakage will be

$$
\begin{equation*}
P_{\mathrm{BS}}^{1,2}=\frac{1}{2}+\frac{1}{2} P_{S}-P_{S} P_{\mathrm{SD}}^{b} . \tag{A15}
\end{equation*}
$$

Now, we consider the second case, i.e., $X_{a}=-X_{b}\left(P_{a}=P_{b}\right)$, where Alice and Bob perform effective decodings with the probability $P_{\mathrm{BS}}^{w}$, which also includes two scenarios. Firstly, considering the successful probability of the implementation of the NLA, and when Eve performs the incorrect discrimination of the state sent from Bob's station, the overall incorrect decoding probability will be $P_{\mathrm{BS}}^{2,1}=P_{\mathrm{BS}}^{1,1}$. Secondly, when Eve correctly discriminates the state sent from Bob's station, she will capture the secret key. Considering the successful probability of the implementation of the NLA, the overall probability of information leakage will be $P_{\mathrm{BS}}^{2,2}=P_{\mathrm{BS}}^{1,2}$.

Therefore, the key distribution channel between Bob and Eve, for the symmetric case, can also be seen as a BSC with a utilization efficiency of $P_{B E}^{\mathrm{BS}, \mathrm{s}}=\frac{1}{4}\left(P_{\mathrm{BS}}^{c} \sum_{i=1}^{2} P_{\mathrm{BS}}^{1, i}+\right.$ $\left.P_{\mathrm{BS}}^{w} \sum_{i=1}^{2} P_{\mathrm{BS}}^{2, i}\right)=\frac{1}{4}\left(P_{\mathrm{BS}}^{w}+P_{\mathrm{BS}}^{c}\right)$, and QBER is $P_{\mathrm{BE}, e}^{\mathrm{BS}, \mathrm{s}}=P_{\mathrm{BS}}^{1,1}\left(P_{\mathrm{BS}}^{w}+P_{\mathrm{BS}}^{c}\right) /\left(P_{\mathrm{BS}}^{w}+P_{\mathrm{BS}}^{c}\right)=P_{\mathrm{BS}}^{1,1}$.

Thus, the mutual information between Bob and Eve, under the BS-combined SD attack, is given by

$$
\begin{equation*}
I_{B E}^{\mathrm{BS}, \mathrm{~s}}=P_{B E}^{\mathrm{BS}, \mathrm{~s}}\left[1-\mathrm{H}\left(P_{B E, e}^{\mathrm{BS}, \mathrm{~s}}\right)\right] . \tag{A16}
\end{equation*}
$$

For the ideally asymmetric case, i.e, the transmission efficiency between Bob and Charlie is $T_{B}=1$, and the excess noise is $\varepsilon_{B}=0$. Moreover, we suppose that $\varepsilon_{A}$ is the same as the total channel excess noises of both channels in the symmetric case, i.e., $\varepsilon_{A}=2 \varepsilon_{c}$. In this case, Eve can not directly capture the secret key information by splitting the photons from the quantum channel between Bob and Charlie. The feasible way is that Eve performs SD attacks on the split photons from the quantum channel between Alice and Charlie to guess the secret key encoded in Bob's states. In particular, Eve will use the same decoding criterion as the legitimate parities in the protocol to judge Bob's encoding states. Eve will also discard one half of the split states with inconsistent bases. For the other half of coherent states with consistent bases, we also consider the two cases, i.e., $X_{a}=X_{b}$ and $X_{a}=-X_{b}$ for the X-basis case and $P_{a}=-P_{b}$ and $P_{a}=P_{b}$ for the P-basis case. Because of symmetric encoding, we just consider the X -basis case in the following equations.

We also suppose that when Eve fails in the implementation of the NLA, she will randomly choose one of the two coherent states, which will induce a $\frac{1}{2}\left(1-P_{s}\right)$ error probability in decoding. Moreover, if Eve performs an incorrect discrimination of a coherent state sent from Alice or Bob's stations after the successful implementation of the NLA, it will induce a $P_{S} P_{\mathrm{SD}}^{b}$ error probability in decoding. It should be mentioned that Eve will also discard the ineffective results according to Charlie's measurement outcomes.

Here, we consider the first case, i.e., $X_{a}=X_{b}\left(P_{a}=-P_{b}\right)$, and Alice and Bob perform the correct and effective decodings with the probability $P_{\mathrm{BS}}^{c}$. Since Eve can not split photons from the channel between Bob and Charlie to directly capture the secret key information, she will use the result of the SD attack, through Alice's channels and Charlie's announced outcomes, to guess Bob's encoded secret key. Since the legitimate parties will discard the ineffective results according to Charlie's measurement outcomes, Eve will also optimize her eavesdropping to capture the secret key according to Charlie's measurement results. There are two scenarios when referring to the SD attack results on Alice's states. Firstly, considering the successful probability of the implementation of the NLA and when Eve performs the incorrect discrimination of the state sent from Alice's station, the overall incorrect decoding probability will be $P_{\mathrm{BS}}^{1,1}$. In this case, Eve will also get the incorrect encoded key on Bob's state. Secondly, when Eve correctly discriminates the state sent from Alice's station, she will then capture Alice's encoded secret information and also correctly guess the encoded key in Bob's side. Considering the successful probability of the implementation of the NLA, the overall probability of information leakage will be $P_{\mathrm{BS}}^{1,2}$.

Now, we consider the second case, i.e., $X_{a}=-X_{b}\left(P_{a}=P_{b}\right)$. Alice and Bob perform effective decodings with the probability $P_{\mathrm{BS}}^{w}$, which also includes two scenarios. Firstly, the successful probability of the implementation of the NLA when Eve performs the incorrect discrimination of the state sent from Alice's station is considered.However, Eve's incorrect decoding will lead to a correct judgment of Bob's encoded key. Therefore, the overall correct decoding probability will be $P_{\mathrm{BS}}^{2,1}=P_{\mathrm{BS}}^{1,1}$. Secondly, when Eve correctly discriminates the state sent from Alice's station, she will capture the encoded secret key but will incorrectly guess the secret key encoded on Bob's state. Considering the successful probability of the implementation of the NLA, the overall incorrect decoding probability will be $P_{\mathrm{BS}}^{2,2}=P_{\mathrm{BS}}^{1,2}$.

Thus, the key distribution channel between Bob and Eve for the ideally asymmetric case can also be seen as a BSC with utilization efficiency $P_{B E}^{\mathrm{BS}, \mathrm{a}}=P_{B E}^{\mathrm{BS}, \mathrm{s}}=\frac{1}{4}\left(P_{\mathrm{BS}}^{w}+P_{\mathrm{BS}}^{c}\right)$, and QBER is $P_{B E, e}^{\mathrm{BS}, \mathrm{a}}=\left(P_{\mathrm{BS}}^{1,1} P_{\mathrm{BS}}^{c}+P_{\mathrm{BS}}^{1,2} P_{\mathrm{BS}}^{w}\right) /\left(P_{\mathrm{BS}}^{w}+P_{\mathrm{BS}}^{c}\right)=\left[P_{\mathrm{BS}}^{w}+\left(P_{\mathrm{BS}}^{c}-P_{\mathrm{BS}}^{w}\right) P_{B E, e}^{\mathrm{BS}, \mathrm{s}}\right] /\left(4 P_{A B}^{\mathrm{BS}}\right)$. Therefore, the mutual information between Bob and Eve under the BS-combined SD attack is given by

$$
\begin{equation*}
I_{B E}^{\mathrm{BS}, \mathrm{a}}=P_{B E}^{\mathrm{BS}, \mathrm{a}}\left[1-\mathrm{H}\left(P_{B E, e}^{\mathrm{BS}, \mathrm{a}}\right)\right] \tag{A17}
\end{equation*}
$$

When the asymmetric case is not ideal, i.e., for the cases where the transmission efficiencies $T_{A} \neq T_{B}<1$ and/or excess noise $\varepsilon_{A} \neq \varepsilon_{B} \neq 0$, Eve will choose the optimal
strategy to capture the secret key information. In particular, she will compare the secret key information captured from the channel between Alice and Charlie by using the BScombined SD attack with the one captured directly from the channel between Bob and Charlie, and will then choose the way to maximize the leaked secret key information. Therefore, the mutual information between Bob and Eve, in this case, will be changed to

$$
\begin{equation*}
I_{B E}^{\mathrm{BS}, \mathrm{a}} \rightarrow \max \left\{I_{B E}^{\mathrm{BS}, \mathrm{~s}}, I_{B E}^{\mathrm{BS}, \mathrm{a}}\right\} . \tag{A18}
\end{equation*}
$$

## Appendix A.3. Simulations of Secret Key Rate under BS-Combined SD Attacks

The secret key rate of the proposed protocol under the BS-combined SD attacks can be calculated as

$$
\begin{equation*}
R_{\mathrm{BS}}=\beta I_{A B}^{\mathrm{BS}}-I_{B E}^{\mathrm{BS}, \mathrm{~s}(\mathrm{a})}, \tag{A19}
\end{equation*}
$$

where $I_{A B}^{\mathrm{BS}}$ is the classical mutual information between Alice and Bob for both symmetric and asymmetric cases, $I_{B E}^{\mathrm{BS}, s(\mathrm{a})}$ is the leaked information to Eve for the symmetric or asymmetric cases, and $\beta$ is the reconciliation efficiency.

We first consider the symmetric case. We find that $g=1$ is optimal for Eve, which corresponds to the lowest estimation of the secret key rate for the BS-combined SD attacks. The secret key rates, as a function of the transmission distance against the BS-combined SD attacks for different channel excess noises are shown in Figure A2. It can be seen that the proposed CV-MDI-QKD protocol is sensitive to the channel's excess noise. Specifically, there exists an optimal amplitude $\alpha$ for the given transmission distance, which is shown in Figure A3. We also explore the dependence of the phase-matching threshold $\delta_{A}\left(\delta_{B}\right)=\kappa \alpha$ on the secret key rate. Figure A4 shows that the threshold does not obviously affect the secure transmission distance, but rather the quantity of the secret key rate. Therefore, one can appropriately choose a relatively large threshold to increase the secret key rate without decreasing the transmission distance.


Figure A2. (Color online). The secret key rates for different channel excess noises against the BScombined SD attacks for the symmetric case when the SD receivers reach SQL (thick curves) and QL (thin curves), respectively. Solid, dashed, dotted, and dash-dotted curves represent the channel excess noise $\varepsilon_{c}=0.02,0.05,0.08$, and 0.1 , respectively. The other parameters are set as $\alpha=3.3, \eta=0.6$, $v_{e l}=0.04, \beta=0.98, g=1, \kappa=0.01 \sqrt{2 \eta T}$.


Figure A3. (Color online). The secret key rates as a function of amplitude $\alpha$ against the BS-combined SD attacks with transmission distance of 3 km of the standard single mode fiber for the symmetric case, when the SD receivers reach QL and SQL, respectively. The other parameters are set as $\varepsilon_{c}=0.03$, $\eta=0.6, v_{e l}=0.04, \beta=0.98, g=1, \kappa=0.01 \sqrt{2 \eta T}$.


Figure A4. (Color online). The secret key rates for different $\kappa$ against the BS-combined SD attacks for the symmetric case when the SD receivers reach QL and SQL, respectively. The solid, dashed, dotted, and dash-dotted curves represent $\kappa=0.1 \sqrt{2 \eta T}, 0.01 \sqrt{2 \eta T}, 0.005 \sqrt{2 \eta T}$ and $0.001 \sqrt{2 \eta T}$, respectively. The other parameters are set as $\varepsilon_{c}=0.03, \eta=0.6, v_{e l}=0.04, \beta=0.98, g=1, \alpha=3.3$.

For the ideally asymmetric case, we also find that $g=1$ is optimal for Eve. The secret key rates, as a function of the transmission distance against the BS-combined SD attacks for different channel excess noises, in this case, are shown in Figure A5. It can be seen that the proposed CV-MDI-QKD protocol is quite insensitive to channel excess noises (the curves are overlapping with each other for different excess noises). Specifically, there exists an optimal amplitude $\alpha$ for a given transmission distance, which is shown in Figure A6. We also explore the dependence of the phase-matching threshold $\delta_{A}\left(\delta_{B}\right)=\kappa \alpha$ on the secret key rate. Figure A7 shows that the threshold does not obviously affect the secure transmission
distance, but rather the quantity of the secret key rate. Therefore, one can appropriately choose a relatively large threshold to increase the secret key rate, without decreasing the transmission distance.


Figure A5. (Color online). The secret key rates for different channel excess noises against the BScombined SD attacks for the ideally asymmetric case when the SD receivers reach QL (thick curves) and SQL (thin curves), respectively. Solid, dashed, dotted, and dash-dotted curves represent the channel excess noise $\varepsilon_{c}=0.02,0.05,0.08$, and 0.1 , respectively. The other parameters are set as $\alpha=0.8$, $\eta=0.6, v_{e l}=0.04, \beta=0.98, g=1, \kappa=\sqrt{2 \eta T}$.


Figure A6. (Color online). The secret key rates as a function of amplitude $\alpha$ against the BS-combined SD attacks with transmission distance of 50 km of standard single mode fiber for the ideally asymmetric case. The black dashed and red solid curves denote the secret key rates when the SD receivers reach QL and SQL, respectively. The other parameters are set as $\varepsilon_{c}=0.03, \eta=0.6, v_{e l}=0.04$, $\beta=0.98, g=1, \kappa=\sqrt{2 \eta T}$.

We find that the legitimate parties can obtain the secure secret key for both symmetric and, ideally, asymmetric cases, if they only consider Eve performing the BS-combined SD attacks. Moreover, it shows that the BS-combined SD attacks are stronger for the symmetric case than the ideally asymmetric case.


Figure A7. (Color online). The secret key rates for different $\kappa$ against the BS-combined SD attacks for the ideally asymmetric case when the SD receivers reach QL and SQL, respectively. The solid, dashed, dotted, and dash-dotted curves represent $\kappa=2 \sqrt{2 \eta T}, \sqrt{2 \eta T}, 0.1 \sqrt{2 \eta T}$ and $0.01 \sqrt{2 \eta T}$, respectively. The other parameters are set as $\varepsilon_{c}=0.03, \eta=0.6, v_{e l}=0.04, \beta=0.98, g=1, \alpha=0.8$.

## Appendix B. Eve's BS-Combined SD Attack Strategy

The equivalent beam-splitting operation with the transmission efficiency $T$ for Eve's SD attack in Figure A1 are realized by a beam splitter with transmission efficiencies $T_{1}$ and a cascaded PIA with the gain of amplification $g^{\prime} \geqslant 1$. We will show below that this operation can be equivalently realized by a virtual beam splitter with the transmission efficiency $T=T_{1} g^{\prime}$ to fully consider the ability of Eve's SD attacks.


SD attack

Figure A8. (Color online). Equivalent realization of beam splitting and amplification operation for Eve's optimized SD attack.

The quadratures of the output modes $A_{0}^{\prime}$ and $B_{0}^{\prime}$ in Figure A8 can be expressed as

$$
\begin{align*}
X_{A_{0}}^{\prime} & =\sqrt{T_{1}} X_{A_{0}}+\sqrt{1-T_{1}} X_{v^{\prime}}^{a}  \tag{A20}\\
P_{A_{0}}^{\prime} & =\sqrt{T_{1}} P_{A_{0}}+\sqrt{1-T_{1}} P_{v^{\prime}}^{a} \\
X_{B_{0}}^{\prime} & =\sqrt{T_{1}} X_{B_{0}}+\sqrt{1-T_{1}} X_{v^{\prime}}^{b} \\
P_{B_{0}}^{\prime} & =\sqrt{T_{1}} P_{B_{0}}+\sqrt{1-T_{1}} P_{v^{\prime}}^{b}
\end{align*}
$$

where $X_{v^{\prime}}^{a}\left(P_{v^{\prime}}^{a}\right)$ and $X_{v^{\prime}}^{b}\left(P_{v^{\prime}}^{b}\right)$ are the quadratures of the induced vacuum states. The split quantum state for the output mode $A_{s}\left(B_{s}\right)$ will be a coherent state with the mean photon number $\left(1-T_{1}\right) \alpha^{2}$. Thus, Eve can directly discriminate between the nonorthogonal coherent states and can capture the secret information with an extremely low error rate, which can be below the SQL and can reach the Helstrom bound (QL). The value of $T_{1}$ is directly related to the performance of Eve's SD attacks.

After transmission through the amplifier, the quadratures of the output modes $A_{1}$ and $B_{1}$ are given by

$$
\begin{align*}
X_{A_{1}} & =\sqrt{g^{\prime} T_{1}} X_{A_{0}}+\sqrt{1-g^{\prime} T_{1}} X_{e}^{a}  \tag{A21}\\
P_{A_{1}} & =\sqrt{g^{\prime} T_{1}} P_{A_{0}}+\sqrt{1-g^{\prime} T_{1}} P_{e}^{a} \\
X_{B_{1}} & =\sqrt{g^{\prime} T_{1}} X_{A_{0}}+\sqrt{1-g^{\prime} T_{1}} X_{e}^{b} \\
P_{B_{1}} & =\sqrt{g^{\prime} T_{1}} P_{A_{0}}+\sqrt{1-g^{\prime} T_{1}} P_{e}^{b}
\end{align*}
$$

where $T_{1}=T / g^{\prime}$, and

$$
\begin{align*}
X_{e}^{a} & =\frac{1}{\sqrt{1-g^{\prime} T_{1}}}\left(\sqrt{g^{\prime}\left(1-T_{1}\right)} X_{v^{\prime}}^{a}+\sqrt{g^{\prime}-1} X_{I}^{a}\right)  \tag{A22}\\
P_{e}^{a} & =\frac{1}{\sqrt{1-g^{\prime} T_{1}}}\left(\sqrt{g^{\prime}\left(1-T_{1}\right)} P_{v^{\prime}}^{a}+\sqrt{g^{\prime}-1} P_{I}^{a}\right) \\
X_{e}^{b} & =\frac{1}{\sqrt{1-g^{\prime} T_{1}}}\left(\sqrt{g^{\prime}\left(1-T_{1}\right)} X_{v^{\prime}}^{b}+\sqrt{g^{\prime}-1} X_{I}^{b}\right) \\
P_{e}^{b} & =\frac{1}{\sqrt{1-g^{\prime} T_{1}}}\left(\sqrt{g^{\prime}\left(1-T_{1}\right)} P_{v^{\prime}}^{b}+\sqrt{g^{\prime}-1} P_{I}^{b}\right)
\end{align*}
$$

are the equivalent extra input quadratures of the thermal states controlled by Eve in Figure A1a, and satisfy $\left\langle\left(X_{e}^{a}\right)^{2}\right\rangle=\left\langle\left(P_{e}^{a}\right)^{2}\right\rangle=\left\langle\left(X_{e}^{b}\right)^{2}\right\rangle=\left\langle\left(P_{e}^{b}\right)^{2}\right\rangle=1+\frac{T}{1-T} \varepsilon_{c}$ in the SNU. Moreover, $\left(X_{I}^{a(b)}, P_{I}^{a(b)}\right)$ are the quadratures of the idler mode for Eve's PIA. When the idler mode is ideally in a vacuum state, one can get

$$
\begin{equation*}
\frac{1}{1-T}\left[\left(g^{\prime}-T\right)+g^{\prime}-1\right]=1+\frac{T}{1-T} \varepsilon_{c} . \tag{A23}
\end{equation*}
$$

Thus, we can get a lower bound of $T_{1}=T / g^{\prime}$ as $\frac{2 T}{2+T \varepsilon_{c}}$. It should be mentioned that the channel excess noise $\varepsilon_{c}$ is attributed to the induced excess noises by the beams splitting and amplification operations.

## Appendix C. Secret Key Rate under Complete IR Attacks

For CV-MDI-QKD, the measurement procedure is performed by a third untrusted party. Thus, Eve can directly intercept the quantum signals without resending the real quantum states, but can just broadcast the measurement outcomes without introducing extra excess noises in state reproduction procedure.


Figure A9. (Color online). The description of the IR attack on the symmetric case of DMPM CV-MDIQKD scheme. BS is the 50:50 beam splitter, Hom is homodyne detection of measuring the $X$ or $P$ quadrature with quantum efficiency $\eta_{e}=1$. These components are all controlled by Eve without reproduction of quantum states. Eve will guess Bob's encoding state to capture the secret key.

For the symmetric or, ideally, asymmetric cases, the complete IR attacks are some of the optimal attacks on the proposed protocol, which can be depicted in Figure A9. While Charlie is untrusted, Eve can control Charlie's station. After Alice and Bob send the quantum states, Eve will simultaneously perform two standard IR attacks on the two quantum channels between Alice and Charlie, and Bob and Charlie. In particular, Eve will replace the quantum channels between Alice and Charlie, and Bob and Charlie, and the two heterodyne detections, with two perfect channels and two 50:50 beam splitters connecting two perfect heterodyne detections, i.e., $\eta_{e}=1$, respectively. The outputs of Charlie's two heterodyne detections can be expressed as

$$
\begin{align*}
X_{A_{1}} & =\frac{1}{\sqrt{2}}\left(X_{a}+X_{v, e}^{a}-X_{v}^{a}\right)  \tag{A24}\\
P_{A_{1}} & =\frac{1}{\sqrt{2}}\left(P_{a}+P_{v, e}^{a}-P_{v}^{a}\right) \\
X_{B_{1}} & =\frac{1}{\sqrt{2}}\left(X_{b}+X_{v, e}^{b}+X_{v}^{b}\right) \\
P_{B_{1}} & =\frac{1}{\sqrt{2}}\left(P_{b}+P_{v, e}^{b}+P_{v}^{b}\right)
\end{align*}
$$

Charlie will use the above outcomes to forge the broadcasted results $X_{A_{2}}, P_{B_{2}}$ as

$$
\begin{align*}
X_{A_{2}} & =X_{A_{1}}-X_{B_{1}}  \tag{A25}\\
& =\frac{1}{\sqrt{2}}\left[\sqrt{\eta T}\left(X_{a}-X_{b}\right)+\sqrt{\eta T}\left(X_{v, e}^{a}-X_{v, e}^{b}\right)-\sqrt{\eta T}\left(X_{v}^{a}+X_{v}^{b}\right)\right] \\
P_{B_{2}} & =P_{A_{1}}+P_{B_{1}} \\
& =\frac{1}{\sqrt{2}}\left[\sqrt{\eta T}\left(P_{a}+P_{b}\right)+\sqrt{\eta T}\left(P_{v, e}^{a}+P_{v, e}^{b}\right)-\sqrt{\eta T}\left(P_{v}^{a}-P_{v}^{b}\right)\right] .
\end{align*}
$$

Alice and Bob cannot judge whether these values are forged or are practical measurement results. Here, Eve can capture the secret key encoded in Bob's quantum state by using the measurement results after Alice and Bob's announcements of the bases, when $X_{a}=X_{b}$ is
for the X-basis and $P_{a}=-P_{b}$ is for the P-basis case, respectively, Alice and Bob can perform correct and effective decodings after basis reconciliation. For these two cases, one can get

$$
\begin{align*}
X_{A_{2}} & =X_{A_{2}, I R}^{c}=\frac{1}{\sqrt{2}}\left[\sqrt{\eta T}\left(X_{v, e}^{a}-X_{v, e}^{b}\right)-\sqrt{\eta T}\left(X_{v}^{a}+X_{v}^{b}\right)\right]  \tag{A26}\\
P_{B_{2}} & =P_{A_{2}, I R}^{c}=\frac{1}{\sqrt{2}}\left[\sqrt{\eta T}\left(P_{v, e}^{a}+P_{v, e}^{b}\right)-\sqrt{\eta T}\left(P_{v}^{a}-P_{v}^{b}\right)\right],
\end{align*}
$$

and they follow the normal distribution as

$$
\begin{equation*}
X_{A_{2}, I R}^{c}, P_{B_{2}, I R}^{c} \sim \mathcal{N}(0,2 \eta T) . \tag{A27}
\end{equation*}
$$

Because of the symmetry of the two bases, we assume $\delta_{A}=\delta_{B}$, and the correct and effective decoding probability can then be calculated as

$$
\begin{equation*}
P_{\mathrm{IR}}^{c}=\operatorname{erf}\left(\frac{\kappa \alpha}{\sqrt{4 \eta T}}\right) \tag{A28}
\end{equation*}
$$

where $\kappa \in \mathbb{R}$ is the decoding threshold.
While $X_{a}=-X_{b}$ is for the X-basis case and $P_{a}=P_{b}$ is for the P-basis case, respectively, Alice and Bob will perform incorrect but effective decodings. For these two cases, one can find that

$$
\begin{align*}
X_{A_{2}} & =X_{A_{2}, I R}^{w}=\frac{1}{\sqrt{2}}\left[\sqrt{\eta T}\left(2 X_{a}+X_{v, e}^{a}-X_{v, e}^{b}\right)-\sqrt{\eta T}\left(X_{v}^{a}+X_{v}^{b}\right)\right]  \tag{A29}\\
P_{B_{2}} & =P_{B_{2}, I R}^{w}=\frac{1}{\sqrt{2}}\left[\sqrt{\eta T}\left(2 P_{a}+P_{v, e}^{a}-P_{v, e}^{b}\right)-\sqrt{\eta T}\left(P_{v}^{a}+P_{v}^{b}\right)\right]
\end{align*}
$$

and they follow the normal distribution as

$$
\begin{align*}
X_{A_{2}, I R}^{w} & \sim \mathcal{N}\left(\sqrt{2 \eta T} X_{a}, 2 \eta T\right),  \tag{A30}\\
P_{B_{2}, I R}^{w} & \sim \mathcal{N}\left(\sqrt{2 \eta T} P_{a}, 2 \eta T\right),
\end{align*}
$$

where $X_{a}\left(P_{a}\right)$ values $\alpha$ or $-\alpha$ with the same probability. Similarly, we assume $\delta_{A}=\delta_{B}$, and the incorrect but effective decoding probability can be calculated as

$$
\begin{equation*}
P_{\mathrm{IR}}^{w}=\frac{1}{2}\left[\operatorname{erf}\left(\frac{\sqrt{2 \eta T} \alpha+\kappa \alpha}{\sqrt{4 \eta T}}\right)-\operatorname{erf}\left(\frac{\sqrt{2 \eta T} \alpha-\kappa \alpha}{\sqrt{4 \eta T}}\right)\right] . \tag{A31}
\end{equation*}
$$

We will first calculate the mutual information $I_{A B}^{I R}$ between Alice and Bob, and the mutual information $I_{B E}^{I R}$ between Eve and Bob. Then, we will evaluate the induced extra excess noise under Eve's IR attacks, which will be used for the further consideration of Eve's optimal attack strategy. Finally, we will show the simulations of the secret key rate under the complete IR attacks.

## Appendix C.1. The Mutual Information between Alice and Bob

It should be noted that whenever Eve's judgments on Bob's encoded states in the IR attacks are correct or incorrect, Alice and Bob will discard one half of the measurement results with inconsistent bases according to their public basis announcements. For the other half of the outcomes with consistent bases, we consider two cases, $X_{a}=X_{b}$ and $X_{a}=-X_{b}$ for the X-basis case and $P_{a}=-P_{b}$ and $P_{a}=P_{b}$ for the P-basis case. We also need to consider the $X$-basis case here, because of the symmetric encoding. After Eve's IR attacks, the measurement outcomes in Charlie's side can also be expressed as Equation (A25).

We consider the first case, i.e., $X_{a}=X_{b}\left(P_{a}=-P_{b}\right)$. The effective detections for this case will be regarded as correct decodings after Alice and Bob's announcements of bases
with the probability $P_{\text {IR }}^{c}$. For $X_{a}=-X_{b}\left(P_{a}=P_{b}\right)$, the effective detections for inconsistent bases will be regarded as incorrect decodings with the probability $P_{\text {IR }}^{w}$. Thus, the key distribution channel between Alice and Bob under Eve's IR attacks can be seen as a BSC with utilization efficiency $P_{A B}^{\mathrm{IR}}=\frac{1}{4}\left(P_{\mathrm{IR}}^{c}+P_{\mathrm{IR}}^{w}\right)$, and QBER $P_{A B, e}^{\mathrm{IR}}=P_{\mathrm{IR}}^{w} /\left(4 P_{A B}^{\mathrm{IR}}\right)$. Therefore, the mutual information between Alice and Bob under the BS-combined SD attack for the symmetric case is given by

$$
\begin{equation*}
I_{A B}^{\mathrm{IR}}=P_{A B}^{\mathrm{IR}}\left[1-\mathrm{H}\left(P_{A B, e}^{\mathrm{IR}}\right)\right] . \tag{A32}
\end{equation*}
$$

## Appendix C.2. The Mutual Information between Eve and Bob

Now, we turn to Eve's information from the IR attack. According to Alice and Bob's public basis announcements, Eve will discard one half of the intercepted states with the inconsistent bases. Here, the total probability of the efficient decoding will be $P_{B E}^{\mathrm{IR}}=P_{A B}^{\mathrm{IR}}$. Since Eve will not reproduce the quantum states intercepted from Alice and Bob, she will instead perform the discrimination operation with the measurement result from Bob to capture the encoded secret key. In this case, whether Alice and Bob send the matched states, i.e., $X_{a}=X_{b}$ and $P_{a}=-P_{b}$ or not, i.e, $X_{a}=-X_{b}$ and $P_{a}=P_{b}$, the QBER can be bound by the SQL for the discrimination of the BPSK coherent states with the amplitude $\alpha$.

Therefore, the key distribution channel between Bob and Eve can be seen as a BSC with a utilization efficiency of $P_{B E}^{\mathrm{IR}}=P_{A B}^{\mathrm{IR}}$, and QBER is $P_{B E, e}^{\mathrm{IR}}=P_{B E, e}^{\mathrm{IR}}=P_{\mathrm{SQL}}^{g, b}$ with $g=1$. Here, $g=1$ corresponds to the unamplified BPSK signal, which is optimal when considering the successful probability of the implementation of the NLA. Thus, the mutual information between Alice and Bob, under the SD attack, is given by

$$
\begin{equation*}
I_{B E}^{\mathrm{IR}}=P_{B E}^{\mathrm{IR}}\left[1-\mathrm{H}\left(P_{B E, e}^{\mathrm{IR}}\right)\right] . \tag{A33}
\end{equation*}
$$

## Appendix C.3. The Evaluation of Extra Excess Noise

As shown in the protocol procedure, the excess noise will be evaluated with the broadcasted measurement results $\left\{X_{A_{2}}, P_{B_{2}}\right\}$ and the quadratures of the prepared inconsistentbasis states $\left\{X_{a}^{p}, P_{a}^{p}\right\}$ and $\left\{X_{b}^{p}, P_{b}^{p}\right\}$. In particular, Alice and Bob will first get the prepared values as

$$
\begin{equation*}
X^{p}=X_{a}^{p}-X_{b}^{p}, P^{p}=P_{a}^{p}+P_{b}^{p} . \tag{A34}
\end{equation*}
$$

We suppose that the quadrature of the prepared states $X^{p}\left(P^{p}\right)$ and the measurement results $X_{A_{2}}\left(P_{B_{2}}\right)$ are linked through the following relation

$$
\begin{equation*}
y=t x+z \tag{A35}
\end{equation*}
$$

which is a normal linear model. Moreover, $t=\sqrt{\eta T} \in \mathbb{R}$ is the total transmission efficiency, $z$ follows a centered normal distribution with an unknown variance $\sigma^{2}=1+\eta T \varepsilon_{c}+v_{e l}$ for the phase-matched outcomes, and $\varepsilon_{c}$ is the average channel excess noise for the two quantum channels between Alice and Charlie, and Bob and Charlie. For the ineffective decoding cases, the centers will shift. When the measurement outcomes meet the phasematching condition, there may be error decodings. Because of the symmetric encoding, we need to consider the X-basis case here.

For this normal linear model, the known maximum-likelihood estimator can be expressed as

$$
\begin{equation*}
\hat{t}=\frac{\sum_{i=1}^{m} x_{i} y_{i}}{\sum_{i=1}^{m} x_{i}^{2}}, \hat{\sigma}^{2}=\frac{1}{m} \sum_{i=1}^{m}\left(y_{i}-\hat{t} x_{i}\right)^{2} . \tag{A36}
\end{equation*}
$$

Therefore, in the parameter estimation, if no IR attacks exist, $z$ will follow a centered normal distribution with the variance $\sigma^{2}=1+\eta T \varepsilon_{c}+v_{e l}$. If Eve performs complete IR attacks, according to the output in Equation (A25), the induced total excess noise in the two quantum channels will change to $\varepsilon_{c}^{e}=\frac{2 \eta T-v_{e l}-1}{\eta T}$.

Since the evaluated excess noise reflects the total one from both quantum channels, Eve will try her best to lower the total induced extra excess noise. One simple way is to
replace the channels with the noiseless ones. Therefore, in a practical security analysis, considering Eve's strongest attacks, the legitimate parties will attribute the evaluated total excess noise to Eve's eavesdropping from the attacked quantum channels.

## Appendix C.4. Simulations of Secret Key Rate under Complete IR Attacks

The secret key rate of the proposed protocol under the IR attacks can be calculated as

$$
\begin{equation*}
R_{\mathrm{IR}}=\beta I_{A B}^{\mathrm{IR}}-I_{B E}^{\mathrm{IR}}, \tag{A37}
\end{equation*}
$$

where $I_{A B}^{\mathrm{IR}}$ is the classical mutual information between Alice and Bob, $I_{B E}^{\mathrm{BS}}$ is the leaked information to Eve, and $\beta$ is the reconciliation efficiency.

We find that $g=1$ is optimal for Eve, which corresponds to the lowest estimation of the secret key rate. The secret key rate, as a function of the transmission distance and state amplitude against the IR attacks, are shown in Figure A10. It can be seen that Eve can always capture the secret key by using the complete IR attacks, whatever the transmission distance and state amplitude are for the specified threshold and homodyne detections, if ignoring the disturbance of the channel excess noise. We can see that Eve will optimize her eavesdropping strategy by first considering the use of the IR attacks. However, Eve's IR attacks will inevitably introduce extra excess noise. Thus, she will try to find an optimal eavesdropping strategy to cover her IR attacks.


Figure A10. (Color online). The secret key rates under the complete IR attacks. The other parameters are set as $\varepsilon_{c}=0.03, \eta=0.6, v_{e l}=0.04, \beta=0.98, \kappa=0.01 \cdot(2 \eta T)$.

## Appendix D. Secret Key Rate of the Phase-Matching Protocol

The secret key rate of the proposed protocol under the non-Gaussian individual attacks, i.e., the one based on the SD attacks, combined with BS and partial IR attacks, can be evaluated as

$$
\begin{equation*}
R^{s(a)}=\beta I_{A B}^{s(a)}-I_{B E}^{s(a)}, \tag{A38}
\end{equation*}
$$

where $I_{A B}^{s(a)}$ is the classical mutual information between Alice and Bob for the symmetric or, ideally, asymmetric case, $I_{B E}^{s(a)}$ is the leaked information to Eve for the symmetric or, ideally, asymmetric case, and $\beta$ is the reconciliation efficiency.

We first consider eavesdropping in the symmetric case, and we suppose the transmission efficiencies and excess noises of the quantum channels between Alice and Charlie, and

Bob and Charlie, are both $T$ and $\varepsilon_{c}$, respectively. Eve will preferentially perform IR attacks on two quantum channels and the whole measurement station due to its effectiveness. However, she should use the channel excess noise to cover her eavesdropping. In particular, if the total channel excess noise $\varepsilon_{c}^{t}$ is equal to, or larger than, the total evaluated excess noise $\varepsilon_{c}^{e}=\frac{2 \eta T-v_{e l}-1}{\eta T}$ induced by the complete IR attacks, Eve can replace the quantum channels with noiseless ones to cover the induced extra excess noise and capture all the secret keys by performing complete IR attacks. When $\varepsilon_{c}^{t}<\varepsilon_{c}^{e}$, she will perform IR attacks on a fraction $\mu=\frac{\varepsilon_{c}^{t}}{\varepsilon_{c}^{c}}$ of the states, and will performs BS-combined SD attacks on the remaining fraction $1-\mu$ of the states. Here, both the quantum channels are replaced with noiseless ones to cover Eve's induced extra excess noise.

Thus, the mutual information between Alice and Bob for the proposed protocol can be calculated as

$$
\begin{equation*}
I_{A B}^{s}=\mu I_{A B}^{\mathrm{IR}}\left(\varepsilon_{c}=0\right)+(1-\mu) I_{A B}^{\mathrm{BS}}\left(\varepsilon_{c}=0\right), \tag{A39}
\end{equation*}
$$

where $I_{A B}^{\mathrm{BS}}=P_{A B}^{\mathrm{BS}}\left[1-\mathrm{H}\left(P_{A B, e}^{\mathrm{BS}}\right)\right], I_{A B}^{\mathrm{IR}}=P_{A B}^{\mathrm{IR}}\left[1-\mathrm{H}\left(P_{A B, e}^{\mathrm{IR}}\right)\right]$. The mutual information between Bob and Eve will be

$$
\begin{equation*}
I_{B E}^{S}=\mu I_{B E}^{\mathrm{IR}}\left(\varepsilon_{c}=0\right)+(1-\mu) I_{B E}^{\mathrm{BS}, \mathrm{~s}}\left(\varepsilon_{c}=0\right), \tag{A40}
\end{equation*}
$$

where $I_{B E}^{\mathrm{BS}, \mathrm{s}}=P_{B E}^{\mathrm{BS}, \mathrm{s}}\left[1-\mathrm{H}\left(P_{B E, e}^{\mathrm{BS}, \mathrm{s}}\right)\right], I_{B E}^{\mathrm{IR}}=P_{B E}^{\mathrm{IR}}\left[1-\mathrm{H}\left(P_{B E, e}^{\mathrm{IR}}\right)\right]$. We find $g=1$ is optimal for Eve.

For the ideally asymmetric case, Eve can access the channel between Alice and Charlie. She will preferentially perform IR attacks due to their effectiveness, and to capture the secret key. Moreover, she will use the channel excess noise to cover her eavesdropping. If the total channel excess noise $\varepsilon_{c}^{t}$ is equal to, or larger than, the total extra excess noise $\varepsilon_{c}^{e}$ induced by the complete IR attacks, Eve can capture all the secret keys by performing complete IR attacks. While $\varepsilon_{c}^{t}<\varepsilon_{c}^{e}$, she will perform IR attacks on a fraction $\mu=\frac{\varepsilon_{c}^{t}}{\varepsilon_{c}^{e}}$ of the states, and will perform BS-combined SD attacks on the remaining fraction $1-\mu$ of the states. We can, similarly, obtain the mutual information between Alice and Bob as

$$
\begin{equation*}
I_{A B}^{a}=I_{A B}^{s} . \tag{A41}
\end{equation*}
$$

Moreover, the leaked information to Eve will be

$$
\begin{equation*}
I_{B E}^{a}=\mu I_{B E}^{\mathrm{IR}}\left(\varepsilon_{c}=0\right)+(1-\mu) I_{B E}^{\mathrm{BS}, \mathrm{a}}\left(\varepsilon_{c}=0\right), \tag{A42}
\end{equation*}
$$

where $I_{B E}^{\mathrm{BS}, \mathrm{a}}=P_{B E}^{\mathrm{BS}, \mathrm{a}}\left[1-\mathrm{H}\left(P_{B E, e}^{\mathrm{BS}, \mathrm{a}}\right)\right]$. We find $g=1$ is also optimal for Eve.

## Appendix E. Frequency Offset Recovery and Phase Drift Compensation

Before the frequency offset recovery, we should firstly perform the frequency offset estimation. The purpose is to accurately evaluate the frequency offset $\delta f_{A(B) L}$ between Alice's (Bob's) laser and the local-LO laser (here, the frequency offsets for Alice and Bob are all $\delta f$ in the proof-of-principle experiment). The annihilation operator of Alice and Bob's pilots after transmitting through the quantum channel, which consist of some classical unmodulated signals, can be expressed as

$$
\begin{align*}
& \hat{E}_{P A_{1}} \rightarrow A_{P A_{1}} \exp \left[-i\left(\omega_{A} t+\phi_{P A}\right)\right]  \tag{A43}\\
& \hat{E}_{P B_{1}} \rightarrow A_{P B_{1}} \exp \left[-i\left(\omega_{B} t+\phi_{P B}\right)\right],
\end{align*}
$$

where $A_{P A(B)_{1}}=X_{P A(B)_{1}}+i P_{P A(B)_{1}}$ is the constant complex amplitude of the pilot, $\omega_{A(B)}=$ $2 \pi f_{A(B)}$ is the center frequency of Alice's (Bob's) laser, and $\phi_{P A(B)}$ is the phase drift of the pilot. Moreover, since LO is a classical signal, its annihilation operator can be also expressed as

$$
\begin{equation*}
\hat{E}_{L} \rightarrow A_{L} \exp \left[-i\left(\omega_{L} t+\phi_{L}\right)\right] \tag{A44}
\end{equation*}
$$

where $\omega_{L}=2 \pi f_{L}, \phi_{L}$ are the center frequencies and the initial phases of $L O$, respectively. The pilot signals are then sent by Alice and Bob simultaneously to Charlie for interference through the BS, and are detected by homodyne detectors the same as the quantum signals. Here, $\phi_{L}=0$ and $\phi_{L}=\pi / 2$ are set to get the quadratures $X_{A_{2}}$ and $P_{B_{2}}$, respectively. The photocurrent signals of the pilots obtained from the homodyne detectors can be expressed as

$$
\begin{align*}
I_{P A_{2}}(t)= & \frac{\sqrt{2} q A_{L}}{T_{d}}\left[A_{P A_{1}} \cos \left(2 \pi \delta f_{A L} t+\phi_{P A_{1}}\right)\right.  \tag{A45}\\
& \left.+A_{P B_{1}} \cos \left(2 \pi \delta f_{B L} t+\phi_{P B_{1}}\right)+n_{C}(t)\right] \\
I_{P B_{2}}(t)= & \frac{\sqrt{2} q A_{L}}{T_{d}}\left[A_{P A_{1}} \sin \left(2 \pi \delta f_{A L} t+\phi_{P A_{1}}\right)\right. \\
& \left.-A_{P B_{1}} \sin \left(2 \pi \delta f_{B L} t+\phi_{P B_{1}}\right)+n_{D}(t)\right]
\end{align*}
$$

where $q$ is the electron charge, $T_{d}$ is the signal duration, and $\delta f_{A L}=f_{A}-f_{L}$ and $\delta f_{B L}=$ $f_{B}-f_{L}$, and $n_{C(D)}(t)$ represent the shot noise in detections. Since the signal-to-noise ratio (SNR) of the pilots is relatively high in comparison to the quantum signal, classic frequency offset estimation algorithms [65] can be adopted here. We can see the output signals are good indicators for the estimation of the frequency offset. The peak points in the spectrum of the signals will show the frequency offsets $\delta \tilde{f}_{A L}$ and $\delta \tilde{f}_{B L}$, which can be directly realized via fast Fourier transform (FFT) on the received quadrature signals $I_{P A_{2}}(t)$ and $I_{P B_{2}}(t)$. The peaks can still appear clearly at a low SNR, which is demonstrated in [55].

In practical scenarios, the intensity of the pilot should be reasonably designed based on the channel loss, such that Charlie can distinguish them. It should be mentioned that although we estimate the absolute value $\left|\delta \tilde{f}_{A(B) L}\right|$, the sign is not confirmed. A method is proposed in [65] that one can try out the positive and negative values to verify the correctness. However, in the proposed CV-MDI-QKD protocol, since only one quadrature is detected for the output modes $A_{2}$ and $B_{2}$, phase compensation cannot be performed at the receiver's site. Therefore, the frequency offset can only be compensated at the senders' sites. Here, the correlation coefficient can be used to determine the sign of the frequency offset.

Specifically, Alice and Bob first disclose a part of the modulated data $X_{a}^{p}, P_{a}^{p}$ and $X_{b}^{p}, P_{b}^{p}$, which are used for parameter estimations. Then, they perform frequency offset recovery on them. Since the sign of the offset is not known, one will try four cases. Supposing that the phase drifts through the transmission are $\phi_{1}$ and $\phi_{2}$, one can get

$$
\begin{align*}
\tilde{\alpha}_{a}^{P} & =\exp \left( \pm i 2 \pi \delta \tilde{f}_{A L} t+\phi_{1}\right) \cdot\left(X_{a}^{p}+i P_{a}^{p}\right)  \tag{A46}\\
\tilde{\alpha}_{b}^{P} & =\exp \left( \pm i 2 \pi \delta \tilde{f}_{B L} t+\phi_{2}\right) \cdot\left(X_{b}^{p}+i P_{b}^{p}\right)
\end{align*}
$$

It should be noted that the added shot noise in the state preparation and transmission and the electronic noise of detection will not affect the evaluation of the correlation coefficient, and the channel loss and detection inefficiency will just affect the whole correlation coefficient value. Therefore, we will simplify the following processing without considering the transmission and detection inefficiency and the induced shot noise and electronic noise. Thus, the quadrature components $X_{A_{2}}$ and $P_{B_{2}}$ can be evaluated by the homodyne detection results as

$$
\begin{align*}
\tilde{X}_{A_{2}} & \sim \operatorname{Re}\left[\left(\tilde{\alpha}_{a}^{P}+\tilde{\alpha}_{b}^{P}\right) / \sqrt{2}\right]  \tag{A47}\\
\tilde{P}_{B_{2}} & \sim \operatorname{Im}\left[\left(\tilde{\alpha}_{a}^{P}-\tilde{\alpha}_{b}^{P}\right) / \sqrt{2}\right] .
\end{align*}
$$

One can then calculate the cross-correlation coefficient between $\tilde{X}_{A_{2}}\left(\tilde{P}_{B_{2}}\right)$ and the real measurement results $X_{A_{2}}\left(P_{B_{2}}\right)$ for different signs of frequency offsets. In each case, the phase angles $\phi_{1(2)}$ are traversed from 0 to $2 \pi$ to calculate the corresponding value of correlation coefficient. We will find that only one frequency offset sign has the highest peak value of the correlation coefficient with specified phase angles $\phi_{1}=\tilde{\phi}_{A}$ and $\phi_{2}=\tilde{\phi}_{B}$.

Therefore, the signs of frequency offsets can be determined, and the phase angles $\tilde{\phi}_{A}$ and $\tilde{\phi}_{B}$ are just the estimated drifted phases in Alice and Bob's data segments, respectively.

Finally, the frequency offset recovery and phase drift compensation can be implemented on Alice and Bob's preparation values, according to the estimated frequency offset and phase drift, as

$$
\begin{align*}
& \tilde{X}_{a(b)}+i \tilde{P}_{a(b)}=\exp \left(2 \pi \delta \tilde{f}_{A(B) L} t+\tilde{\phi}_{A(B)}\right) \cdot\left(X_{a(b)}+i P_{a(b)}\right),  \tag{A48}\\
& \tilde{X}_{a(b)}^{P}+i \tilde{P}_{a(b)}^{P}=\exp \left(2 \pi \delta \tilde{f}_{A(B) L} t+\tilde{\phi}_{A(B)}\right) \cdot\left(X_{a(b)}^{P}+i P_{a(b)}^{P}\right),
\end{align*}
$$

where $\tilde{X}_{a(b)}, \tilde{P}_{a(b)}$ and $\tilde{X}_{a(b)}^{P}, \tilde{P}_{a(b)}^{P}$ represent the recovered data in Alice and Bob's sites. Based on these, Alice and Bob can perform parameter estimations and data reconciliations, just like the original protocol. We should note that the phase drifts in one frame are assumed constant. In practical scenarios, the size of one frame should be determined according to the realistic rate of phase drifts, such that the phase drift estimation algorithm can track the fluctuation of phase drifts in real time.

## References

1. Ralph, T.C. Continuous variable quantum cryptography. Phys. Rev. A 1999, 61, 010303(R). [CrossRef]
2. Grosshans, F.; Grangier, P. Continuous variable quantum cryptography using coherent states. Phys. Rev. Lett. 2002, 88, 057902. [CrossRef]
3. Grosshans, F.; Grangier, P. Quantum key distribution using gaussian-modulated coherent states. Nature 2003, 421, 238. [CrossRef] [PubMed]
4. 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]
5. Pirandola, S.; Andersen, U.L.; Banchi, L.; Berta, M.; Bunandar, D.; Colbeck, R.; Englund, D.; Gehring, T.; Lupo, C.; Ottaviani, C.; et al. Advances in quantum cryptography. Adv. Opt. Photonics 2020, 12, 1012-1236. [CrossRef]
6. Pirandola, S.; Mancini, S.; Lloyd, S.; Braunstein, S.L. Continuous-variable quantum cryptography using two-way quantum communication. Nat. Phys. 2008, 4, 726-730. [CrossRef]
7. Leverrier, A.; Grangier, P. Unconditional Security Proof of Long-Distance Continuous-Variable Quantum Key Distribution with Discrete Modulation. Phys. Rev. Lett. 2009, 102, 180504; Erratum in Phys. Rev. Lett. 2011, 106, 259902. [CrossRef]
8. Huang, P.; Huang, J.; Zhang, Z.; Zeng, G. Quantum key distribution using basis encoding of Gaussian-modulated coherent states. Phys. Rev. A 2018, 97, 042311. [CrossRef]
9. Pirandola, S.; Laurenza, R.; Ottaviani, C.; Banchi, L. Fundamental limits of repeaterless quantum communications. Nat. Commun. 2017, 8, 15043. [CrossRef]
10. Brassard, G.; Lütkenhaus, N.; Mor, T.; Sanders, B.C. Limitations on practical quantum cryptography. Phys. Rev. Lett. 2000, 85, 1330. [CrossRef]
11. Filip, R. Continuous-variable quantum key distribution with noisy coherent states. Phys. Rev. A 2008, 77, 022310. [CrossRef]
12. Jouguet, P.; Kunz-Jacques, S.; Diamanti, E.; Leverrier, A. Analysis of imperfections in practical continuous-variable quantum key distribution. Phys. Rev. A 2012, 86, 032309. [CrossRef]
13. Diamanti, E.; Lo, H.-K.; Qi, B.; Yuan, Z. Practical challenges in quantum key distribution. NPJ Quantum Inf. 2016, 2, 16025. [CrossRef]
14. Xu, F.; Ma, X.; Zhang, Q.; Lo, H.; Pan, J. Secure quantum key distribution with realistic devices. Rev. Mod. Phys. 2020, 92, 025002. [CrossRef]
15. Ma, X.-C.; Sun, S.-H.; Jiang, M.-S.; Liang, L.-M. Local oscillator fluctuation opens a loophole for Eve in practical continuousvariable quantum-key-distribution systems. Phys. Rev. A 2013, 88, 022339. [CrossRef]
16. Jouguet, P.; Kunz-Jacques, S.; Diamanti, E. Preventing calibration attacks on the local oscillator in continuous-variable quantum key distribution. Phys. Rev. A 2013, 87, 062313. [CrossRef]
17. Ma, X.-C.; Sun, S.-H.; Jiang, M.-S.; Liang, L.M. Wavelength attack on practical continuous-variable quantum-key-distribution system with a heterodyne protocol. Phys. Rev. A 2013, 87, 052309. [CrossRef]
18. 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 continuousvariable quantum-key-distribution system using a wavelength attack. Phys. Rev. A 2013, 87, 062329. [CrossRef]
19. Qin, H.; Kumar, R.; Alléaume, R. Quantum hacking: Saturation attack on practical continuous-variable quantum key distribution. Phys. Rev. A 2016, 94, 012325. [CrossRef]
20. Wang, C.; Huang, P.; Huang, D.; Lin, D.; Zeng, G. Practical security of continuous-variable quantum key distribution with finite sampling bandwidth effects. Phys. Rev. A 2016, 93, 022315. [CrossRef]
21. Zheng, Y.; Huang, P.; Huang, A.; Peng, J.; Zeng, G. Practical security of continuous-variable quantum key distribution with reduced optical attenuation. Phys. Rev. A 2019, 100, 012313. [CrossRef]
22. Zheng, Y.; Huang, P.; Huang, A.; Peng, J.; Zeng, G. Security analysis of practical continuous-variable quantum key distribution systems under laser seeding attack. Opt. Express 2019, 27, 27369. [CrossRef]
23. 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. Photonics 2015, 9, 397-402. [CrossRef] [PubMed]
24. Ma, X.-C.; Sun, S.-H.; Jiang, M.-S.; Gui, M.; Liang, L.-M. Gaussian-modulated coherent-state measurement-device-independent quantum key distribution. Phys. Rev. A 2014, 89, 042335. [CrossRef]
25. Li, Z.; Zhang, Y.-C.; Xu, F.; Peng, X.; Guo, H. Continuous-variable measurement-device-independent quantum key distribution. Phys. Rev. A 2014, 89, 052301. [CrossRef]
26. Ottaviani, C.; Spedalieri, G.; Braunstein, S.L.; Pirandola, S. Continuous-variable quantum cryptography with an untrusted relay: Detailed security analysis of the symmetric configuration. Phys. Rev. A 2015, 91, 022320. [CrossRef]
27. 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]
28. Zhang, X.; Zhang, Y.; Zhao, Y.; Wang, X.; Yu, S.; Guo, H. Finite-size analysis of continuous-variable measurement-deviceindependent quantum key distribution. Phys. Rev. A 2017, 96, 042334. [CrossRef]
29. Lupo, C.; Ottaviani, C.; Papanastasiou, P.; Pirandola, S. Continuous-variable measurement-device-independent quantum key distribution: Composable security against coherent attacks. Phys. Rev. A 2018, 97, 052327. [CrossRef]
30. Chen, Z.; Zhang, Y.; Wang, G.; Li, Z.; Guo, H. Composable security analysis of continuous-variable measurement-deviceindependent quantum key distribution with squeezed states for coherent attacks. Phys. Rev. A 2018, 98, 012314. [CrossRef]
31. Lupo, C.; Ottaviani, C.; Papanastasiou, P.; Pirandola, S. Parameter Estimation with Almost No Public Communication for Continuous-Variable Quantum Key Distribution. Phys. Rev. Lett. 2018, 120, 220505. [CrossRef]
32. Ma, H.-X.; Huang, P.; Bai, D.-Y.; Wang, S.-Y.; Bao, W.-S.; Zeng, G.-H. Continuous-variable measurement-device-independent quantum key distribution with photon subtraction. Phys. Rev. A 2018, 97, 042329. [CrossRef] [PubMed]
33. Zhao, Y.; Zhang, Y.; Xu, B.; Yu, S.; Guo, H. Continuous-variable measurement-device-independent quantum key distribution with virtual photon subtraction. Phys. Rev. A 2018, 97, 042328. [CrossRef]
34. Ma, H.-X.; Huang, P.; Bai, D.-Y.; 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]
35. DiMario, M.T.; Kunz, L.; Banaszek, K.; Becerra, F.E. Optimized communication strategies with binary coherent states over phase noise channels. NPJ Quantum Inf. 2019, 5, 65. [CrossRef]
36. Pirandola, S.; Ottaviani, C.; Spedalieri, G.; Weedbrook, C.; Braunstein, S.L.; Lloyd, S.; Gehring, T.; Jacobsen, C.S.; Andersen, U.L. Reply to 'Discrete and continuous variables for measurement-device-independent quantum cryptography'. Nat. Photonics 2015, 9, 773-775. [CrossRef]
37. Jouguet, P.; Kunz-Jacques, S.; Leverrier, A.; Grangier, P.; Diamanti, E. Experimental demonstration of long-distance continuousvariable quantum key distribution. Nat. Photonics 2013, 7, 378. [CrossRef]
38. Xu, F.; Curty, M.; Qi, B.; Qian, L.; Lo, H.-K. Discrete and continuous variables for measurement-device-independent quantum cryptography. Nat. Photonics 2015, 9, 772-773. [CrossRef]
39. Huang, D.; Huang, P.; Lin, D.; Zeng, G. Long-distance continuous-variable quantum key distribution by controlling excess noise. Sci. Rep. 2016, 6, 19201. [CrossRef]
40. Zhang, Y.; Li, Z.; Chen, Z.; Weedbrook, C.; Zhao, Y.; Wang, X.; Huang, Y.; Xu, C.; Zhang, X.; Wang, Z.; et al. Continuous-variable QKD over 50 km commercial fiber. Quantum Sci. Technol. 2019, 4, 035006. [CrossRef]
41. 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]
42. Wilkinson, K.N.; Papanastasiou, P.; Ottaviani, C.; Gehring, T.; Pirandola, S. Long-distance continuous-variable measurement-device-independent quantum key distribution with postselection. Phys. Rev. Res. 2020, 2, 033424. [CrossRef]
43. Huang, P.; Fang, J.; Zeng, G. State-discrimination attack on discretely modulated continuous-variable quantum key distribution. Phys. Rev. A 2014, 89, 042330. [CrossRef]
44. Tsujino, K.; Fukuda, D.; Fujii, G.; Inoue, S.; Fujiwara, M.; Takeoka, M.; Sasaki, M. Quantum Receiver beyond the Standard Quantum Limit of Coherent Optical Communication. Phys. Rev. Lett. 2011, 106, 250503. [CrossRef]
45. Becerra, F.E.; Fan, J.; Baumgartner, G.; Polyakov, S.V.; Goldhar, J.; Kosloski, J.T.; Migdall, A. M-ary-state phase-shift-keying discrimination below the homodyne limit. Phys. Rev. A 2011, 84, 062324. [CrossRef]
46. Becerra, F.E.; Fan, J.; Baumgartner, G.; Goldhar, J.; Kosloski, J.T.; Migdall, A. Experimental demonstration of a receiver beating the standard quantum limit for multiple nonorthogonal state discrimination. Nat. Photonics 2013, 7, 147-152. [CrossRef] [PubMed]
47. Müller, C.R.; Usuga, M.A.; Wittmann, C.; Takeoka, M.; Marquardt, C.; Andersen, U.L.; Leuchs, G. Quadrature phase shift keying coherent state discrimination via a hybrid receiver. New J. Phys. 2012, 14, 083009. [CrossRef]
48. Ferreyrol, F.; Barbieri, M.; Blandino, R.; Fossier, S.; Tualle-Brouri, R.; Grangier, P. Implementation of a Nondeterministic Optical Noiseless Amplifier. Phys. Rev. Lett. 2010, 104, 123603. [CrossRef]
49. Zavatta, A.; Fiurasek, J.; Bellini, M. A high-fidelity noiseless amplifier for quantum light states. Nat. Photonics 2011, 5, 52-56. [CrossRef]
50. Xiang, G.Y.; Ralph, T.C.; Lund, A.P.; Walk, N.; Pryde, G.J. Heralded noiseless linear amplification and distillation of entanglement. Nat. Photonics 2010, 4, 316. [CrossRef]
51. Usuga, M.A.; Muller, C.R.; Wittmann, C.; Marek, P.; Filip, R.; Marquardt, C.; Leuchs, G.; Andersen, U.L. Noise-powered probabilistic concentration of phase information. Nat. Phys. 2010, 6, 767-771. [CrossRef]
52. Lodewyck, J.; Grangier, P. Tight bound on the coherent-state quantum key distribution with heterodyne detection. Phys. Rev. A 2007, 76, 022332. [CrossRef]
53. Chen, J.-P.; Zhang, C.; Liu, Y.; Jiang, C.; Zhang, W.; Hu, X.-L.; Guan, J.-Y.; Yu, Z.-W.; Xu, H.; Lin, J.; et al. Sending-or-Not-Sending with Independent Lasers: Secure Twin-Field Quantum Key Distribution over 509 km . Phys. Rev. Lett. 2020, 124, 070501. [CrossRef]
54. Fang, X.-T.; Zeng, P.; Liu, H.; Zou, M.; Wu, W.; Tang, Y.-L.; Sheng, Y.-J.; Xiang, Y.; Zhang, W.; Li, H.; et al. Implementation of quantum key distribution surpassing the linear rate-transmittance bound. Nat. Photonics 2020, 14, 422-425. [CrossRef]
55. Wang, T.; Huang, P.; Ma, H.; Wang, S.; Zeng, G. Carrier synchronization for continuous-variable measurement-device-independent quantum key distribution with a real local oscillator. Phys. Rev. A 2021, 104, 022606. [CrossRef] [PubMed]
56. Ma, X.; Zeng, P.; Zhou, H. Phase-matching quantum key distribution. Phys. Rev. X 2018, 8, 031043. [CrossRef] [PubMed]
57. Grosshans, F.; Grangier, P. Continuous-variable quantum cryptography is secure against non-Gaussian attacks. Phys. Rev. Lett. 2004, 92, 047905. [CrossRef]
58. Lodewyck, J.; Debuisschert, T.; García-Patrón, R.; Tualle-Brouri, R.; Cerf, N.J.; Grangier, P. Experimental Implementation of Non-Gaussian Attacks on a Continuous-Variable Quantum-Key-Distribution System. Phys. Rev. Lett. 2007, 98, 030503. [CrossRef]
59. 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]
60. Papanastasiou, P.; Pirandola, S. Continuous-variable quantum cryptography with discrete alphabets: Composable security under collective Gaussian attacks. Phys. Rev. Res. 2021, 3, 013047. [CrossRef]
61. Sabuncu, M.; Filip, R.; Leuchs, G.; Andersen, U.L. Environment-assisted quantum-information correction for continuous variables. Phys. Rev. A 2010, 81, 012325. [CrossRef]
62. Sabuncu, M.; Mišta, L., Jr.; Fiurášek, J.; Filip, R.; Leuchs, G.; Andersen, U.L. Nonunity gain minimal-disturbance measurement. Phys. Rev. A 2007, 76, 032309. [CrossRef]
63. Wang, S.; Huang, P.; Wang, T.; Zeng, G. Environment-assisted quantum-information correction for continuous variables. New J. Phys. 2018, 20, 083037. [CrossRef]
64. Lassen, M.; Madsen, L.S.; Sabuncu, M.; Filip, R.; Andersen, U.L. Experimental demonstration of squeezed-state quantum averaging. Phys. Rev. A 2010, 82, 021801(R). [CrossRef]
65. Cao, Y.; Yu, S.; Shen, J.; Gu, W.; Ji, Y. Frequency Estimation for Optical Coherent MPSK System without Removing Modulated Data Phase. IEEE Photonics Technol. Lett. 2010, 22, 691-693. [CrossRef]
