Simultaneous two-way classical communication and measurement-device-independent quantum key distribution with coherent states

Dong Pan,[1,2] Soon Xin Ng,[2] Dong Ruan,[1] Liuguo Yin,[3] Guilu Long,[1,4,5] and Lajos Hanzo[2]

[1]*State Key Laboratory of Low-dimensional Quantum Physics and Department of Physics, Tsinghua University, Beijing 100084, China*
[2]*School of Electronics and Computer Science, University of Southampton, Southampton SO17 1BJ, United Kingdom*
[3]*School of Information Science and Technology, Tsinghua University, Beijing 100084, China*
[4]*Tsinghua National Laboratory for Information Science and Technology, Beijing 100084, China*
[5]*Collaborative Innovation Center of Quantum Matter, Beijing 100084, China*

(Dated: October 31, 2019)

Simultaneous quantum and classical communication integrates both continuous variable quantum key distribution and classical coherent optical communication by using the same communication infrastructure. Given its compelling benefits, we proposed a protocol relying on both two-way classical communication and on measurement-device-independent quantum key distribution, in which the superposition modulation based coherent states depend on the information bits of both the secret key and on the classical communication ciphertext, which are measured by an untrusted relay node. The proposed scheme strikes a beneficial balance between its level of security and its grade of practicability. Explicitly, on the one hand, the secret key obtained is secure against all attacks on the detectors, and it is eminently suitable for bidirectional classical communication in the metropolitan network as a benefit of its relay-based configuration. Our results show a convincing bit error rate vs. secret key rate trade-off for transmission over dozens of kilometers in the quantum channel, hence striking an excellent integrity (bit error rate) vs. security trade-off.

I. INTRODUCTION

Quantum key distribution (QKD) [1] and quantum secure direct communication [2–4] are popular secure information transmission schemes for the future hybrid quantum-classical network environment [5], regardless of the capability of the eavesdropper who is restricted by the laws of quantum mechanics. Specifically, QKD takes charge of distributing the cryptographic keys, thus it is integrated into classical communication for ciphertext transmission after one-time pad encryption. By contrast, quantum secure direct communication transmits messages directly over the quantum channel, while the associated classical communication is invoked for eavesdropping detection.

The implementation of discrete variable based quantum communication [6], relying for example on the BB84 protocol [1], calls for some high-cost devices, such as single-photon source and single-photon detector, which increases the challenge of constructing the quantum layer in a communication network [7]. To mitigate this challenge, continuous variable (CV) schemes have been designed [8, 9]. The quadrature components of the optical field may be modulated for conveying the secret key, which are then detected by a homodyne or heterodyne detector. As a benefit, a high secret key rate can be achieved by off-the-shelf optical hardware. As for the attainable grade of security, it has been proved theoretically that the Gaussian-modulated CV QKD relying on coherent states is secure both against collective attacks [10, 11] as well as coherent attacks [12], even in the context of finite-size analysis [13, 14] or composable security [15]. The transmission distance record of experimental CV-QKD was improved to 150 km [16], and soon afterwards the field test was extended to a network in [17]. Satellite-based CV quantum communication is also attracting substantial research attention [18, 19].

Recently, a simultaneous quantum and classical communication (SQCC) scheme was proposed in [20], where both the bits of classical communication and the cryptographic key are mapped to the same coherent state and then detected by the receiver. The SQCC protocol amalgamated both the classical coherent optical communication and QKD schemes in the same communication infrastructure for different purposes. For achieving long-distance transmission in the face of hostile phase noise, a true local oscillator was used by the SQCC protocol in [21]. The classical carrier phase estimation algorithm was proved to be capable of recovering the phase and to extract the data [22]. If an optical amplifier is incorporated in the plug-and-play SQCC configuration, the secret key rate can be further improved [23].

However, the proof of security was provided for CV QKD under some idealized simplifying assumptions, which are however hard to satisfy by using practical devices. The gap between the ideal devices and the imperfect ones could lead to security loopholes. The side-channel attacks targeting the detector, such as saturation attacks [24, 25] and blinding attacks [26] are the most popular eavesdropping strategies targeting imperfect detectors. Some known attacks have been investigated and eliminated, as shown in [27]. However, it is quite a challenge to characterize all loopholes caused by imperfect devices. In order to tackle this challenge, the measurement-device-independent (MDI) QKD philosophy was proposed in the discrete variable domain [28, 29], which was then also soon extended to its CV counterpart [30–33]. Let us consider a pair of legitimate users, Alice and Bob, who are not connected to each other directly but through a relay Charlie who controls the detectors. The relay is typically assumed to be untrusted, because it can be accessed by the eavesdropper Eve. Alice and Bob prepare the quantum states and send them to Charlie for measurement. Then the correlated data (i.e. the secret key) between Alice and Bob will be established according to the measurement results after reconciliation. No third-parties can obtain the secret information, even though the measurement results are published, thus all side-channel attacks targeted at the detectors are eliminated. This form of communication works well for striking a balance between the grade of security [34, 35] and practicability, and it is particularly suitable for long-distance transmission [36] and for multiuser communication across a star topology network [37, 38].

Against this background, we proposed a protocol for simultaneous two-way classical communication and measurement-device-independent quantum key distribution, where the communication performance is characterized by practical system parameters. The end-users can exchange independent messages at the same time whilst relying on classical communication, which is more beneficial than the one-way SQCC protocol [20], since most practical communication links are bidirectional. The secret key is distributed, whilst being immune to all detection-related security loopholes. Furthermore, this configuration can also be readily embedded into classical base station aided multi-user networks.

The paper is structured as follows. In Sec. II, we introduce the details of the protocol conceived. In Sec. III, we provide our associated bit error rate and secret key rate analysis in the face of a specific noise model. In Sec. IV, we provide simulation results under a range of practical system parameters and discuss the associated performance trends. Finally, the conclusions and outlook are presented in Sec. V.

II. DETAILS OF THE PROTOCOL

We have a choice of numerous simultaneous two-way classical communication and CV MDI QKD protocols, which can be categorized according to the specific modulation methods used both in classical communication and in CV MDI QKD. For example, we may opt for phase-shift keying [39] or for quadrature amplitude modulation [40] in classical communication, and either for Gaussian or for non-Gaussian modulation in CV QKD [41]. Taking the associated implementation into consideration, we adopt quadrature phase-shift keying modulated classical communication in conjunction with Gaussian-modulated coherent-state based QKD for our protocol. The feasibility of other modulation schemes will also be discussed.

A. Protocol description

The prepare-and-measure description of the new protocol shown in Fig. 1 (a) is described as follows.

Step 1. State preparation: Alice and Bob prepare the coherent states formulated as

$$|\alpha e^{i\frac{\pi}{4}(2n_\star+1)} + [x_\star(k) + ip_\star(k)]\rangle, \tag{1}$$

where $\star$ represents either A or B, while α is the amplitude of the quadrature phase-shift keying signal. More specifically, $n_A, n_B \in \{0,1,2,3\}$ is mapped to the classical bits $\{00, 01, 10, 11\}$, while $\{x_A(k), p_A(k), x_B(k), p_B(k)\}$ is the quadrature set representing the cryptographic keys. Explicitly, two layers of bits are mapped to the same coherent state, where $n_\star$ is encoded by either Alice or Bob to convey the classical ciphertext bits and they choose the data pair from two independent Gaussian-distributions, usually for $\{x_A, p_A\}$ associated with $N \sim \mathcal{N}(0, V_A)$ and $\{x_B, p_B\}$ with $N \sim \mathcal{N}(0, V_B)$, by modulating their coherent states for distributing the secret key bits. Then, they send their coherent states to Charlie, respectively.

Step 2. Measurement: The coherent states arriving from Alice and Bob will be combined by the balanced beam splitter of Fig. 1 (a) for the CV Bell detection [30] at Charlie's station. The measurement results $\{X_C, P_C\}$ of Charlie will then be published via a classical authenticated channel, which can be written as

$$X_C = \frac{X_A - X_B}{\sqrt{2}}, P_C = \frac{P_A + P_B}{\sqrt{2}}, \tag{2}$$

where X_A, P_A, X_B and P_B are the quadrature components of the coherent states of Alice or Bob $|X_\star + iP_\star\rangle$, which can be rewritten in the simple form of Eq. (1).

Step 3. Decoding: Alice and Bob deduce the classical information transmitted by each other according to the specific quadrant of the measurement results and their own $n_\star$ value. Then the Gaussian data associated with the secret key will be obtained by removing the displacement of classical communication.

Step 4. Parameter estimation and data processing: Alice and Bob complete the parameter estimation related to both the channel transmissions and the excess noises. Finally, error correction and privacy amplification are employed for generating the final secret key, as in the Gaussian-modulated coherent state based CV MDI QKD of [42].

In a detailed realization, there needs time synchronization of the two states. However, for the proposed protocol, we can ignore this for simplicity. Here, we have followed the notation of Ref. [30], where we have $\left[\hat{X}, \hat{P}\right] = 2i$ (i.e., $\hbar$=2). Then the vacuum noise becomes 1.

B. Characteristics of the protocol

On the one hand, this protocol has the ability to distribute the secret key using the Gaussian-modulated coherent states, as in [30–32]. On the other hand, a pair of communicating parties can transmit information to each other at the same time with the aid of a relay. In Fig. 2, there are different colors for each row and column. Alice or Bob can infer the bits sent by the other side under the premise that they know their own bits. For example, if Alice sends "10" and the measurement results are those shown in red, then she will know that Bob has sent "11", and vice versa for Bob. Eve aims for inferring both the common secret key sequence as it will be discussed later in Sec. III B and the classical bit sequence Alice transmits to Bob as well as that of Bob transmitted to Alice.

Observe that the classical bits of the individual users do not become readily available for an illegal third party in the process of two-way classical communication despite the fact that all measurement results are published. The reasons for this are

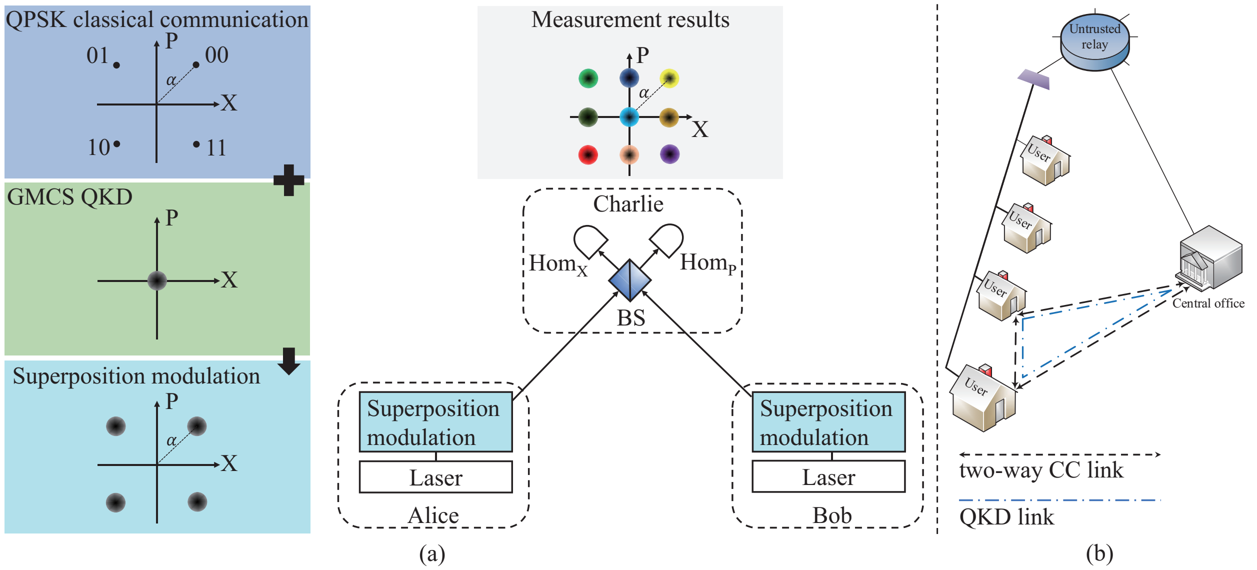
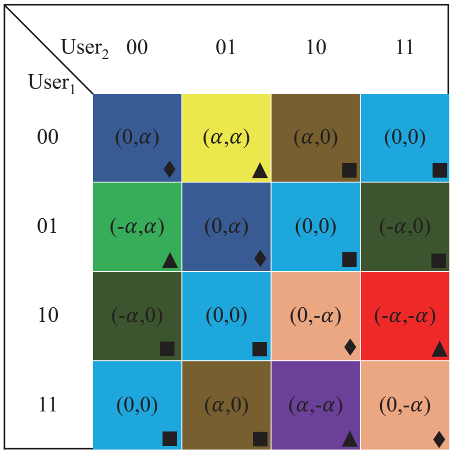


Figure 1. (Color online) (a) Prepare-and-measure scheme of simultaneous two-way classical communication and CV MDI QKD. QPSK: quadrature phase-shift keying, GMCS: Gaussian modulated coherent state, BS: beam splitter, $\mathrm{Hom_X}$, $\mathrm{Hom_P}$: homodyne detector. (b) A star topology network based on our simultaneous two-way classical communication and CV MDI QKD: the two-way classical communication (CC) link and the QKD link can be achieved between any pair of users across this network.



User$_1$ \ User$_2$	00	01	10	11
00	(0,α) ♦	(α,α) ▲	(α,0) ■	(0,0) ■
01	(-α,α) ▲	(0,α) ♦	(0,0) ■	(-α,0) ■
10	(-α,0) ■	(0,0) ■	(0,-α) ♦	(-α,-α) ▲
11	(0,0) ■	(α,0) ■	(α,-α) ▲	(0,-α) ♦

Figure 2. (Color online) Encoding the bits of two users in terms of the CV Bell-measurement results in the two-way classical communication considered. Alice (Bob) could be either User$_1$ or User$_2$. For the sake of simplicity, the measurement results $\{X_C, P_C\}$ have omitted the term of Gaussian data $\left\{\frac{1}{2}(x_A - x_B), \frac{1}{2}(p_A + p_B)\right\}$ as well as the factor $\frac{\sqrt{2}}{2}$ in front of α. The different measurement results are labeled with different colors, which can also be seen using the same color in Fig. 1. The diamonds, squares, and triangles mark three different scenarios according to Eve's inference process.

Table I. The examples of Eve's specific inference process, which selected from three different scenarios.

Measurement results	Inferring process	
	Stage 1 Transmitted combination?	Stage 2 Specific bits of each user?
.5 ♦ (0, α)	{00,00}	Alice$\overset{00}{\underset{00}{\rightleftarrows}}$Bob
	{01,01}	Alice$\overset{01}{\underset{01}{\rightleftarrows}}$Bob
.9 ■ ($-\alpha$, 0)	.5 {10,00}	Alice$\overset{10}{\underset{00}{\rightleftarrows}}$Bob
		Alice$\overset{00}{\underset{10}{\rightleftarrows}}$Bob
	.5 {01,11}	Alice$\overset{01}{\underset{11}{\rightleftarrows}}$Bob
		Alice$\overset{11}{\underset{01}{\rightleftarrows}}$Bob
.5 ▲ (α, α)	.5 {00,01}	Alice$\overset{00}{\underset{01}{\rightleftarrows}}$Bob
		Alice$\overset{01}{\underset{00}{\rightleftarrows}}$Bob

three-fold, (♦), (■) and (▲), depending on Eve's specific inference process. (♦) Firstly, the transmission of different bits may lead to the same measurement results, depending on the information of the other party. Eve would have to guess the specific transmission combinations correctly. In the example of Table I, the observation (0, α)-dark-blue may have resulted by the transmission combinations $\{00, 00\}$ or $\{01, 01\}$. (■) Secondly, similarly to (♦), the same measurement results may accrue from different transmission combinations. However, in contrast to (♦), Eve would have to guess not only the specific transmission combinations correctly, but also the particular transmitted bits of the individual users. There are two ($-\alpha$, 0)-dark-green labels in Fig. 2. Hence, Eve has the probability of 50% to guess the transmission combination correctly. If Eve guesses that the transmission combination is "{10,00}", as shown in Table I, she has to further guess whether Alice has transmitted “10” or “00” to Bob. (▲) Thirdly, some unique and unambiguous measurement results also exist in Fig. 2. Hence, although Eve can unambiguously infer the transmission combinations when these measurement results are revealed, she still has to guess the specific transmitted bits of the individual users. The corresponding transmission combination of the observation (α, α)-yellow must be $\{00, 01\}$, but the specific transmitted bits of Alice could be "00" or "01", as seen in the example of Table I.

We would like to mention that the above statement of "the particular transmitted bits of the individual users" is important during the process when Eve wants to infer the transmitted bit sequence in the second and third scenarios related to Fig. 2. For example, if the pair of consecutive measurement results are yellow-red, the possible transmitted bits of Alice may be “0010”, “0110”, “0011”, and “0111”, provided that Bob’s corresponding bits are “0111”, “0011”, “0110’, and “0010”, respectively.

Furthermore, the security of two-way classical communication is unequivocally guaranteed by the one-time pad encryption that has been proved to be information-theoretically secure [43]. Explicitly, the transmitted ciphertext bits of the individual users are not readily available for Eve and the employment of one-time pad encryption guarantees the security of the associated two-way classical communication. This beneficial characteristic is also retained for eight-level phase-shift keying, but not for binary phase-shift keying [44], which can be readily deduced from Eq. (2) using the relevant coherent encoded states [20].

III. PERFORMANCE ANALYSIS

In this section, both the bit error rate and the secret key rate are derived for analyzing the performance of our proposed protocol based on the following noise sources: (1) the vacuum noise with variance of 1; (2) the electronic noise of the detector having a variance of $\nu_{\rm el}$; (3) the Gaussian modulation used by Alice and Bob in the CV MDI QKD have a variance of V_{MA} and V_{MB}, respectively; (4) the excess noise $\varepsilon_{t\star}$ imposed by the two quantum channels is expressed by $\varepsilon_{t\star} = \varepsilon_p + \varepsilon_{0\star}$, where $\varepsilon_p = \frac{\alpha^2 \sigma_\phi}{N_0}$ [20] is the excess noise caused by phase instability under the condition of $\alpha^2 \geqslant (V_{MA}+1)N_0$ (in which σ_ϕ is the phase-noise variance and $N_0 = \frac{1}{4}$ quantifies the shot-noise-variance), and ε_0 is the excess noise independent of the amplitude α; (5) the interference between the classical communication signal and quantum communication signal. All the noise sources are characterized by their power in terms of shot-noise units [45].

A. Bit error rate of two-way classical communication

The bit error rate of two-way classical communication using quadrature phase-shift keying signalling is given by [39]

$$e_c = \frac{1}{2}\mathrm{erfc}\left(\sqrt{\frac{C_{\rm SNR}}{2}}\right), \tag{3}$$

where $\mathrm{erfc}(*)$ stands for the complementary error function, while $C_{\rm SNR}$ is the signal-noise-ratio of the carrier in two-way classical communication, which can be evaluated by using the ratio of the carrier power and the noise power at Charlie’s node, when the CV Bell-measurement is carried out using homodyne detectors. Hence, we may rewrite Eq. (3) as

$$e_c = \frac{1}{2}\mathrm{erfc}\left(\sqrt{\frac{T_A\eta_{\rm hom}\alpha^2 + T_B\eta_{\rm hom}\alpha^2}{4N_tN_0}}\right), \tag{4}$$

where T_A and T_B are the channel transmittance in the Alice-to-Charlie and Bob-to-Charlie links, respectively. Furthermore, $\eta_{\rm hom}$ is the detection efficiency of homodyne detectors, while $N_{\rm t}$ denotes the overall noise variance at Charlie’s node, and the factor $\frac{1}{4}$ under the sqrt function is introduced by the factor $\frac{1}{2}$ due to the balanced beam splitter and the other factor $\frac{1}{2}$ is owing to Eq. (3). According to the noise sources mentioned above, the overall noise variance is given by

$$\begin{aligned} N_t = {} & 2\ (1+\nu_{\rm el}) + T_A\eta_{\rm hom}V_{MA} + T_B\eta_{\rm hom}V_{MB} \\ & + T_A\eta_{\rm hom}\varepsilon_{tA} + T_B\eta_{\rm hom}\varepsilon_{tB}, \end{aligned} \tag{5}$$

where ε_{tA} and ε_{tB} are the excess noise imposed by the Alice-to-Charlie and Bob-to-Charlie quantum channel, respectively. Since the optical homodyne phase-shift keying communication system has achieved a bit error rate of 10^{-9} [46] in experimental implementation, with this goal in mind, the specific modulated signal amplitude α of two-way classical communication can be expressed as:

$$\alpha = \omega\sqrt{\frac{2\,(1+\nu_{\rm el}) + T_A\eta_{\rm hom}V_{MA} + T_B\eta_{\rm hom}V_{MB} + T_A\eta_{\rm hom}\varepsilon_{0A} + T_B\eta_{\rm hom}\varepsilon_{0B}}{T_A\eta_{\rm hom} + T_B\eta_{\rm hom} - \omega^2 T_A\eta_{\rm hom}\frac{\sigma_\phi}{N_0} - \omega^2 T_B\eta_{\rm hom}\frac{\sigma_\phi}{N_0}}}, \tag{6}$$

where ε_{0A} and ε_{0B} denotes the excess noise independent of α and imposed by the Alice-to-Charlie and Bob-to-Charlie quantum channel, and $\omega = \mathrm{erfc}^{-1}(2e_c) = \mathrm{erfc}^{-1}(2\times 10^{-9})$ in which $\mathrm{erfc}^{-1}(*)$ is the inverse complementary error function.

B. Secret key rate of CV MDI QKD

The equivalent entanglement-based model of the prepare-and-measure protocol is commonly adopted to analyze the security of CV QKD [47]. As seen in Fig. 3, the equivalent entanglement-based version of our proposed protocol comprises the following steps: The two-mode squeezed states are prepared by Alice and Bob independently and they send one of the modes to Charlie for CV Bell-measurement. The measurement results will be announced both to Alice and Bob. Then Bob applies a displacement operation with the gain of g on his retained mode according to the data announced, while the mode of Alice remains unchanged. Finally, Alice and Bob use the heterodyne detector to measure their own mode for establishing the secret key. If we assume furthermore that the two-mode squeezed states prepared by Bob and the displacement operation are untrusted, the entanglement-based version of the proposed protocol is converted into a common one-way CV QKD model. Thus, the secret key rate deduced from the common one-way CV QKD qualifies the lower bound key rate of CV MDI QKD.

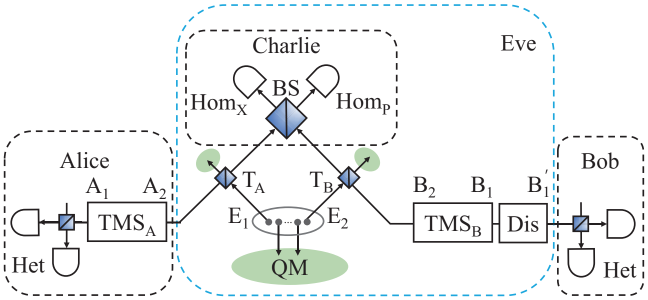


Figure 3. (Color online) The equivalent entanglement-based scheme of simultaneous two-way classical communication and MDI QKD. $\mathrm{TMS_A}$ and $\mathrm{TMS_B}$ represent the two-mode squeezed state prepared by Alice and Bob, respectively. BS: beam splitter, Dis: displacement operation, QM: quantum memory, Het: heterodyne detector, $\mathrm{Hom_X}$ and $\mathrm{Hom_P}$: homodyne detector.

In this work, we mainly consider the secret key rate that is guaranteed to remain secure against arbitrary collective attacks, where Eve interacts individually with each mode sent from Alice and Bob by using her ancillary states, and she stores these ancillary states in the quantum memory to infer the secret key by performing an optimal collective measurement on the ensemble of stored ancilla at any later time. Depending on Eve's specific strategy concerning the two quantum channels, the collective attacks encountered in CV MDI QKD can be divided into two types : (1) one-mode attack, where Eve performs entangling cloner on the two quantum channels independently. She interacts with Alice's and Bob's modes with her half of each EPR pair, respectively, as detailed in [32]; (2) two-mode attack, in which Eve applies a correlated two-mode coherent Gaussian attack by injecting the quantum correlations $\{\mathrm{E}_1, \mathrm{E}_2\}$ in both the quantum channels [30], as shown in Fig. 3. Further related discussions are provided in Refs. [48, 49] on the same subject under different attacks. The correlation between the two quantum channels is weak, hence the two-mode attack has effectively degenerated into the one-mode attack. The related composable security analysis [35] shows that these two types of attacks are equivalent in the extremely asymmetric case, where Bob is very close to Charlie, as discussed later in Sec. IV B. Furthermore, the higher the geographic symmetry in the three communication parties' position, namely when Eve is closer to the mid-point between Alice and Bob, the stronger the impact of the two-mode attack on the secret key rate becomes. This reduces the key rate, but it will not influence the security analysis under the one-mode attack. In view of the above, we may adopt the one-mode attack for our security analysis, as seen in numerous theoretical contributions on CV QKD [31, 32, 49]. However, the two-mode attack was shown to be the optimal attack in [30], which hence results in the minimum secret key rate [50]. Hence, our secret key rate will be derived under the premise of two-mode attack.

In the two-mode attack, the optimal correlated attack has been proven to be "negative EPR attack", and the covariance matrix of the injected pair of correlated modes E_1 and E_2 is given by [50]

$$\gamma_{E_1E_2} = \begin{pmatrix} V_{E_1}I_2 & -\sqrt{V_E^2-1}\sigma_z \\ -\sqrt{V_E^2-1}\sigma_z & V_{E_1}I_2 \end{pmatrix}, \tag{7}$$

where $I_2 = \mathrm{diag}(1,1)$, $\sigma_z = \mathrm{diag}(1,-1)$, and the variances are assumed to be $V_{E_1} = V_{E_2} = V_E$ for the sake of achieving maximum correlation between two modes.

Assuming that the attenuation of both quantum channels is l=0.2 dB/km, then the channel transmittance can be expressed as $T_A = 10^{-\frac{lL_{AC}}{10}}$ and $T_B = 10^{-\frac{lL_{BC}}{10}}$. The equivalent excess noise in the one-way model is given by

$$\begin{aligned}\varepsilon = 1 &+ \chi_A + \frac{1}{T_A}\left[T_B\left(\chi_B - 1\right) - C_E\right] \\ &+ \frac{T_B}{T_A}\left(\sqrt{\frac{2}{T_B}}\sqrt{\frac{V_B-1}{g^2}} - \sqrt{V_B+1}\right)^2,\end{aligned} \tag{8}$$

where

$$\chi_A = \frac{1}{T_A} - 1 + \varepsilon_{tA} + \frac{\alpha^2}{N_0}e_c \tag{9}$$

and

$$\chi_B = \frac{1}{T_B} - 1 + \varepsilon_{tB} + \frac{\alpha^2}{N_0}e_c \tag{10}$$

represent the channel-added noise referred to the channel inputs, while C_E is the noise contribution induced by the correlation of Eve's two modes. Furthermore, C_E can be deduced from the quadrature components of Eve's two modes, namely,

$$C_E = \frac{2}{T_A}\sqrt{(1-T_A)(1-T_B)}\left\langle E_{1X}E_{2X}\right\rangle \tag{11}$$

or

$$C_E = -\frac{2}{T_A}\sqrt{(1-T_A)(1-T_B)}\left\langle E_{1P}E_{2P}\right\rangle, \tag{12}$$

where $\langle E_{1_X} E_{2_X} \rangle = -\langle E_{1_P} E_{2_P} \rangle = -\sqrt{V_E^2 - 1} = -\sqrt{(1 + \frac{T_A}{1-T_A}\varepsilon_{tA})^2 - 1}$ [35, 48]. The excess-noise imposed by the classical communication is quantified by the last terms in Eq. (9) and Eq. (10), respectively. As it may be observed from Eq. (11) and Eq. (12), the correlation of Eve's two modes will disappear when $L_{BC} \approx 0$ ($T_B \approx 1$), which is the reason why the two-mode attack is degenerated to a one-mode attack in the extremely asymmetric case. If the displacement gain defined in [31] is set to $g = \sqrt{\frac{2}{T_B}}\sqrt{\frac{V_B-1}{V_B+1}}$, the equivalent excess noise can be further minimized, yielding

$$\varepsilon' = \frac{2}{T_A} + \varepsilon_{tA} + \frac{\alpha^2}{N_0}e_c + \frac{T_B}{T_A}\left(\varepsilon_{tB} - 2 + \frac{\alpha^2}{N_0}e_c\right) - \frac{C_E}{T_A}. \tag{13}$$

Consequently, the total channel-added noise in the one-way model, which consists of the equivalent excess noise and the detection induced noise can be expressed as:

$$\chi_t = \frac{1}{T} - 1 + \varepsilon' + \frac{2\chi_{\text{hom}}}{T_A}, \tag{14}$$

where $T = \frac{g^2 T_A}{2}$ [31] is the total quantum channel transmittance between Alice and Bob, while $\chi_{\text{hom}} = \frac{1-\eta_{\text{hom}}}{\eta_{\text{hom}}} + \frac{\nu_{\text{el}}}{\eta_{\text{hom}}}$ is the detection noise. Both the electronic noise variance ν_{el} and detection efficiency η_{hom} have been assumed to be inaccessible to Eve.

The secret key rate K of the CV MDI QKD is given by

$$K = \beta I_{AB} - \chi_{BE}, \tag{15}$$

where β is the reconciliation efficiency, I_{AB} is the Shannonian mutual information, and the Holevo bound χ_{BE} is the maximum accessible information of Eve. The calculation of I_{AB} and χ_{BE} can be found in the Appendix, thus the secret key rate K is written as

$$\begin{aligned} K = {} & \beta \log_2 \left[\frac{T\left(V_{MA} + 1 + \chi_t\right) + 1}{T\left(1 + \chi_t\right) + 1}\right] \\ & - G\left(\frac{\lambda_1 - 1}{2}\right) - G\left(\frac{\lambda_2 - 1}{2}\right) + G\left(\frac{\lambda_3 - 1}{2}\right), \end{aligned} \tag{16}$$

where λ_1, λ_2, and λ_3 are the symplectic eigenvalues of the specific covariance matrices of the Appendix. Furthermore, we have $G(*) = (* + 1)\log_2(* + 1) - (*)\log_2(*)$. The secret key remains secure in the face of the collective attacks, provided that K in Eq. (16) remains positive.

IV. PERFORMANCE RESULTS AND DISCUSSIONS

In this section, we will characterize the performance of our protocol in two different application scenarios. In the first scenario, Charlie is placed right in the middle of two legitimate parties ($L_{AC} = L_{BC}$). This so-called symmetric scheme is suitable for a star topology, where two users are nearly equidistant to a public server. The second scenario is an asymmetric one, where Charlie is closer to one of the legitimate parties ($L_{AC} \neq L_{BC}$), which may find employment in metropolitan point-to-point communications. It has been shown that the asymmetric CV MDI QKD scenario has superior performance over the symmetric one, when employing the same parameters, especially when Charlie is extremely close to Bob [30–33]. The following simulations characterize these two cases. The key parameters that affect both the bit error rate and the secret key rate are the amplitude of the classical communication, the variance of the two parties' modulated signal ($V_{MA} = V_{MB}$), the channel transmittance, the reconciliation efficiency β, the excess noise derived from the noise model, as well as the imperfect homodyne detection factor, such as the detector efficiency η_{hom} and the electronic noise variance ν_{el}.

A. Performance in the symmetric scenario

The interaction between classical communication and quantum communication in the proposed protocol has been investigated in Sec. III. The bit error rate of classical communication is degraded by the total channel-added noise, while the modulation variance of CV MDI QKD also affects the bit error rate. Our goal is to achieve two-way classical communication at a low bit error rate of 10^{-9} and simultaneously maintain a positive secret key rate. The amplitude required for attaining a bit error rate of 10^{-9} over a certain transmission distance has been formulated in Eq. (6), which depends on the modulation variance, that in turn fundamentally affects the secret key rate of CV MDI QKD. Therefore, we plot the secret key rate and amplitude of classical communication as a function of the modulation variance at different distances for the sake of finding the optimal modulation variance, which is presented in Fig. 4.

Observe in Fig. 4 that the optional range of near-optimal modulation variance becomes narrow and the secret key rate is significantly reduced upon increasing the transmission distance. The secret key rate tends to reach its peak, when the modulation variance is about 35. Accordingly, the concomitant amplitude value of the optimal modulation variance that meets the required bit error rate target is about 26, as shown in the inset graph of Fig. 4. Additionally, the amplitude α is increased, when the modulation variance is increased, but the curves are almost overlapped for different transmission distances. The reason for amplitude α to be the same regardless of the distance is justified by Eq. (6), because the channel transmittances appear in both of in the numerator and the denominator of Eq. (6). The pair of optimal parameters $V_{MA} = 35$ and $\alpha = 26$ are selected for the performance characterization of the symmetric case.

Figure 5 shows the simulation results characterizing the proposed protocol, while the Pirandola-Laurenza-Ottaviani-Banchi (PLOB) bound [51] of the secret key rates of direct transmission over lossy bosonic channels and the secret key rates of the original Gaussian CV MDI QKD [31] are also considered for comparison. In the symmetric case, the secret key rate of the proposed SQCC scheme decreases as the transmission distance increases, where the maximum transmission distance is about 3.84 km. It can be seen that the secret key

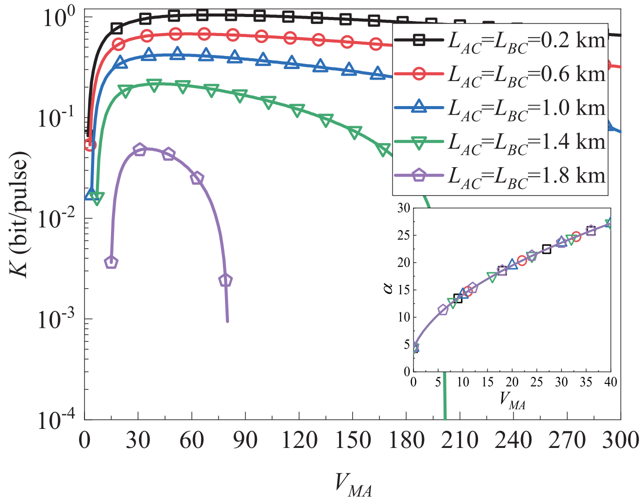


Figure 4. (Color online) Secret key rate (main graph) and amplitude of the classical signal (inset) as a function of V_{MA} under the condition of a bit error rate lower than 10^{-9} in the symmetric case, where $L_{AC} = L_{BC}$. The curves with markers represent the data over different transmission distances. The remaining parameters are set as follows: reconciliation efficiency $\beta = 0.98$, phase-noise variance $\sigma_\phi = 10^{-6}$, electronic noise $\nu_{\rm el} = 0.01$, detector efficiency $\eta_{\rm hom} = 0.98$, and the excess noise independent of the classical signal amplitude of two channels $\varepsilon_{0A} = \varepsilon_{0B} = 0.002$.

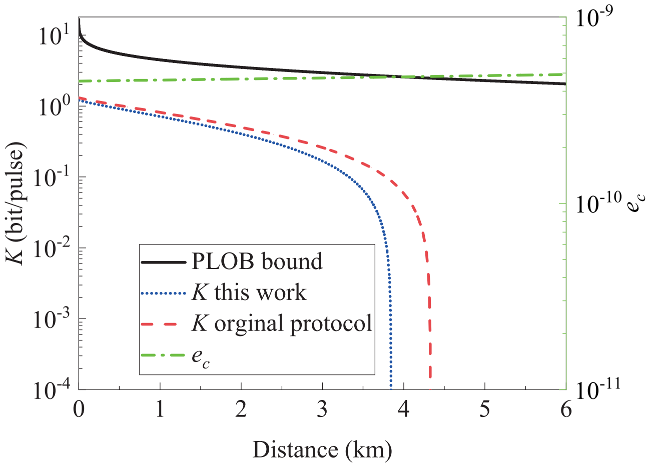


Figure 5. (Color online). Secret key rate and bit error rate performance of the proposed protocol in the symmetric case. The blue dotted curve and green dash-dotted curve denote the secret key rate and bit error rate of this work, respectively. For comparison, the secret key rate of the Pirandola-Laurenza-Ottaviani-Banchi (PLOB) bound [51] and of the original Gaussian modulated CV MDI QKD [31] are computed based on the same parameters, which are represented by the black solid curve and red dashed curve, respectively. In the simulations, the modulation variance is $V_{MA} = 35$ and the classical signal amplitude is $\alpha = 26$, which are optimal. The remaining system parameters are fixed as follows: reconciliation efficiency $\beta = 0.98$, phase-noise variance $\sigma_\phi = 10^{-6}$, electronic noise $\nu_{\rm el} = 0.01$, detector efficiency $\eta_{\rm hom} = 0.98$, and $\varepsilon_{0A} = \varepsilon_{0B} = 0.002$.

rate of the proposed SQCC scheme and that of the original CV MDI QKD protocol are almost identical for distances below 1.5 km. However, the gap between them becomes larger when the transmission distance approaches the maximum distance of 3.84 km, where the original protocol operates closer to the PLOB bound. Additionally, the maximum transmission distance of the proposed protocol is slightly shorter than that of the original protocol. As seen in Fig. 5, there is only a small degradation of about 0.48 km in terms of the maximum distance at $K = 10^{-4}$ bit/pulse between the proposed protocol and the original CV MDI QKD protocol. However, the proposed protocol is capable of supporting simultaneous two-way classical communication and CV MDI QKD at a modest performance erosion. The bit error rate increases slowly as the distance increases, but it is always below our target of bit error rate 10^{-9}, which means that the optimal parameters V_{MA} and α have played an active role in appropriately configuring the proposed protocol.

B. Performance in the extremely asymmetric scheme

In this subsection, the performance is analyzed when the proposed protocol is utilized in the extremely asymmetric scenario, where Charlie is very close to Bob ($L_{BC} \approx 0$). We will discuss some similar simulation results to those of the symmetric scheme, and focus our attention on the comparison between these two cases.

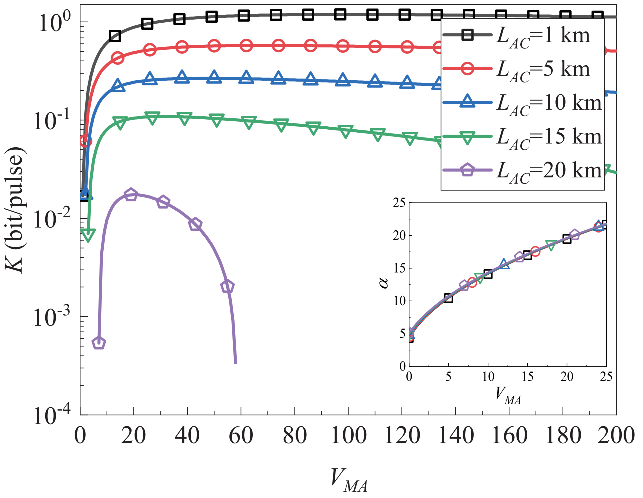


Figure 6. (Color online). Secret key rate (main graph) and amplitude of the classical signal (inset) as a function of V_{MA} under the condition of a bit error rate lower than 10^{-9} in the extremely asymmetric scheme, where $L_{BC} \approx 0$. The curves with markers are the results simulated under different transmission distances. The remaining parameters are fixed the same as Fig. 4.

The main graph in Fig. 6 shows the secret key rate as a function of Alice's modulation variance. Analogously, we can obtain the optimal modulation variance V_{MA}, which is about 20 and the concomitant classical signal amplitude also has to be 20 according to the inset. The difference is that the suitable modulation variance range is wider in the extremely asymmetric scenario than that of the symmetric scheme, when their transmission distances are identical, as shown in Fig. 7. Thus the extremely asymmetric scheme is more stable and flexible due to its larger optional distance range of near-optimal modulation variance. Moreover, the secret key rate is also higher than that of the symmetric case. These two characteristics explain the superiority of the extremely asymmetric scheme over the symmetric scheme. Furthermore, the optimal modulation variance and classical signal amplitude are about 35 and 26, respectively. In Fig. 7, these two optimal parameters match well in two different scenarios. The reason why we opted for $V_{MA} = 20$ and $\alpha = 20$ as the optimal parameters in the extremely asymmetric case is that these are the optimal values for long-distance communication, while the change of secret key rate at a short distance is relatively smooth in a certain range of modulation variance, as seen in Fig. 7.

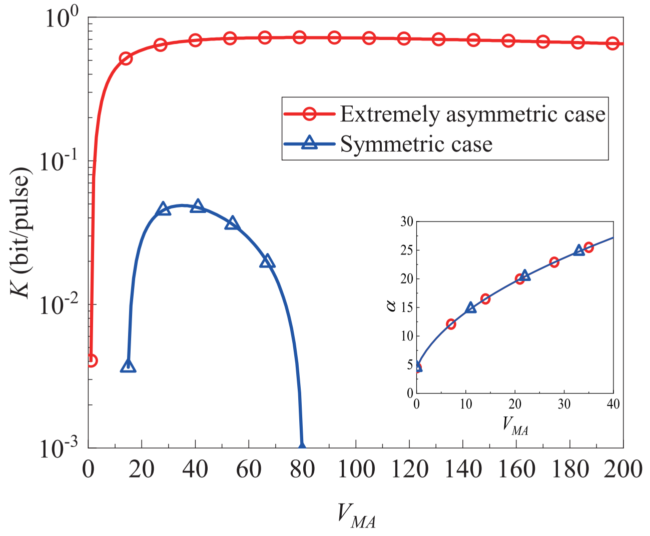


Figure 7. (Color online) Comparision of secret key rate (main graph) and classical signal amplitude (inset) as a function of modulation variance between the extremely asymmetric (L_{AC}=3.6 km, $L_{BC} \approx 0$) and symmetric scheme ($L_{AC} = L_{BC}$ =1.8 km). The remaining parameters are as same as in Fig. 4.

Again, the proposed protocol supports classical communication and CV MDI QKD running simultaneously in the same communication infrastructure at the cost of a slightly reduced transmission-distance compared to the original CV MDI QKD scheme. When relying on imperfect reconciliation and detection, a distance of 21 km is feasible for SQCC in the extremely asymmetric scheme ($L_{BC} \approx 0$), as shown in Fig. 8. It is a practically acceptable distance for communications in metropolitan areas. Observe that the bit error rate of classical communication seen in both Fig. 5 and Fig. 8 have not changed much, which means that the bit error rate is only sensitive to long-distance transmission, but it is stable under the optimal parameters settings. This insensitivity to the distance can also be concluded from the insets, since the α versus V_{MA} curves are indistinguishable for different transmission distances.

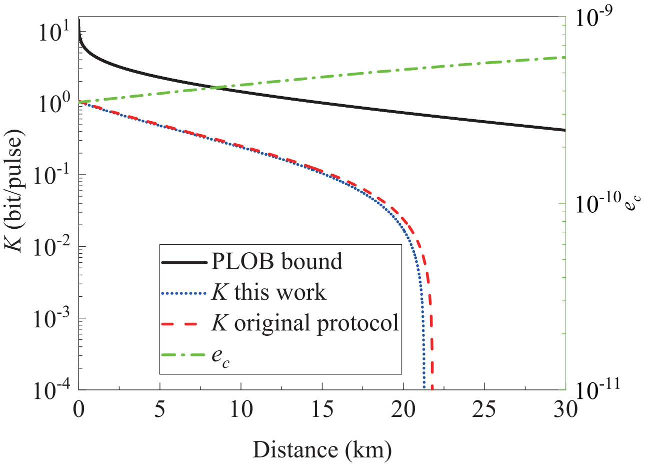


Figure 8. (Color online). Secret key rate and bit error rate in the extremely asymmetric scheme, where $L_{BC} \approx 0$. The blue dotted curve and green dash-dotted curve denote the secret key rate and bit error rate of this work, respectively. Pirandola-Laurenza-Ottaviani-Banchi (PLOB) bound [51] (black solid curve) and original Gaussian modulated CV MDI QKD [31] (red dashed curve) are plotted with the same parameters for the comparison. The curves are obtained using the optimal modulation variance $V_{MA} = 20$ (its concomitant classical signal amplitude $\alpha = 20$) and the remaining parameters which are as same as those have mentioned in Fig. 5.

It is also worth mentioning that we have also tried to introduce discrete modulation [52] that proved to be suitable for long-distance CV MDI QKD into our SQCC protocol. However, we have found that no practical secret key rate can be realized for the extremely asymmetric scenario by using a four-state modulation scheme [53] in conjunction with the optimal modulation variance and the associated amplitude, when the remaining system parameters are the same as those used in this treatise, unless almost perfect detectors ($\eta_{\text{hom}} = 0.99$, $\nu_{\text{el}} = 0.001$) and perfect reconciliation $\beta = 1$ are employed. This trend is probably caused by the lower variance of the quantum communication signal. However, a discrete modulation scheme associated with 256-modes was found to be capable of obtaining the same secret key rate as Gaussian modulation in [54]. Therefore, the feasibility of employing the so-called hierarchical modulation technique of [55] (a basic constellation for discrete-modulation CV MDI QKD) to extend the transmission distance of our SQCC protocol should be further investigated.

Note that the secret key rate above is obtained in the asymptotic regime, namely under the idealized simplifying conditions of having an infinite number of signals exchanged by a pair of legitimate users. More explicitly, this would correspond to the assumption that the quantum channel is perfectly known. Naturally, the number of exchanged signals cannot be unlimited in practice, which implies that the length of the secret key is finite. To elaborate a little further, when considering our security analysis in the practical finite-key length scenario [13, 23, 56, 57], then a part of the exchanged signals has to be used for parameter estimation, rather than for secret key generation, since the characteristics of the quantum channel are actually not known. They have to be estimated. In reality, both the secret key rate and the maximum transmission distance of our proposed protocol will be reduced by different amounts associated with different block sizes.

V. CONCLUSIONS AND OUTLOOK

We proposed a protocol for simultaneously supporting both two-way classical communication and measurement-device-independent quantum key distribution, where a pair of terminals are not directly connected to each other via a quantum channel, but through an untrusted relay. They transmit their information carriers to the untrusted relay for measurement. Despite the fact that all measurement results are published, the specific transmitted ciphertext is not directly available to an illegal third party in the bidirectional classical coherent optical communication. As a further benefit, the secret key bits can be simultaneously distributed under guaranteed security of withstanding all attacks of the detectors. This enables both communication modalities to operate concurrently based on the same communication infrastructure, which can be conveniently applied in a star topology network. To evaluate the performance of our proposed protocol, the secret key rate attainable in the face of collective attacks is calculated for both the symmetric and the extremely asymmetric case, while ensuring that the classical communication has a low bit error rate of 10^{-9}. Our simulation results show that even when considering various noise sources and imperfect implementation parameters, the proposed SQCC scheme only sacrifices a little bit of transmission distance, despite integrating CV MDI QKD protocol with bidirectional classical coherent optical communication.

Simultaneous transmission and detection of classical and quantum signals has been demonstrated to be feasible over a 25 km optical fiber section by using superposition modulation [58], showing an excellent prospect for the point-to-point SQCC protocol [20]. As for the future experimental implementation of the proposed SQCC protocol, the high-speed homodyne detectors have to be developed [59, 60] (at the time of writing 1 GHz available), if the detection rate close to the repetition rate of classical communication systems (generally ~ 100 GHz), these two kinds of communication would match well and more efficient. Since both two-way coherent optical classical communication and CV MDI QKD are suitable for free-space communications [30], it promising to extend the proposed SQCC protocol into free-space optical scenarios for establishing station-based wireless multi-user networks. Then the coherent states will be inevitably contaminated by the air turbulence [61–63], which has to be further investigated. Our hope is that this solution could offer a feasible scheme for secure communication in hybrid quantum-classical networks.

ACKNOWLEDGMENTS

We acknowledge the helpful discussions with H. X. Ma, P. Huang, and Z. Chen. D. Pan, D. Ruan, L. G. Yin, and G. L. Long are supported by the National Basic Research Program of China (2015CB921001 and 2017YFA0303700), the National Natural Science Foundation of China (61726801,11474168 and 11474181), and the Beijing Advanced Innovation Center for Future Chip (ICFC). D. Pan also supported by the China Scholarship Council (CSC NO. 201806210237). S. X. Ng and L. Hanzo would like to acknowledge the financial support of the Engineering and Physical Sciences Research Council projects EP/Noo4558/1, EP/PO34284/1, COALESCE, of the Royal Society's Global Challenges Research Fund Grant as well as of the European Research Council's Advanced Fellow Grant QuantCom.

Appendix: Calculation of the secret key rate

Considering the channel properties in the entanglement-based scheme, the modes $\rho_{A_1B_1'}$ after CV Bell-measurement and displacement are uniquely and unambiguously determined by the covariance matrices $\gamma_{A_1B_1'}$, which has the form of

$$\gamma_{A_1B_1'} = \begin{pmatrix} VI_2 & \sqrt{T\left(V^2-1\right)}\sigma_z \\ \sqrt{T\left(V^2-1\right)}\sigma_z & T\left(V+\chi_t\right)I_2 \end{pmatrix} = \begin{pmatrix} aI_2 & c\sigma_z \\ c\sigma_z & bI_2 \end{pmatrix}, \tag{A.1}$$

where we have assumed that the variances obey $V = V_A = V_B = V_{MA}+1 = V_{MB}+1$ without loss of generality. Assuming that both the x and p quadrature components are used for generating the secret key, the Shannonian mutual information between Alice's and Bob's heterodyne measurements is given by

$$\begin{aligned} I_{AB} &= 2\times\frac{1}{2}\log_2\left(\frac{a+1}{a+1-\frac{c^2}{b+1}}\right) \\ &= \log_2\left[\frac{V_{MA}+2}{V_{MA}+2-\frac{T\left[(V_{MA}+1)^2-1\right]}{T(V_{MA}+1+\chi_t)+1}}\right] \\ &= \log_2\left[\frac{T\left(V_{MA}+1+\chi_t\right)+1}{T\left(1+\chi_t\right)+1}\right]. \end{aligned} \tag{A.2}$$

The Holevo bound χ_{BE} can be obtained from [64] as follows:

$$\chi_{BE} = S(\rho_E) - \int dx_B' dp_B' p\left(x_B',p_B'\right) S\left(\rho_E^{x_B',p_B'}\right), \tag{A.3}$$

where $p\left(x_B',p_B'\right)$ is the probability distribution of the measurement results of Bob related to $\{x_B',p_B'\}$, $\rho_E^{x_B',p_B'}$ is Eve's state conditioned on Bob's measurement result, and $S(\rho)$ is the von Neumann entropy of the quantum state ρ. For the Gaussian state, we can write [65]

$$S(\rho) = \sum_i G\left(\frac{\lambda_i - 1}{2}\right), \tag{A.4}$$

where λ_i is the generic symplectic eigenvalue of the covariance matrices characterizing ρ. Based on the fact that Eve is capable of purifying the whole system $\rho_{A_1 B_1'}$ [30] and that the projected results of heterodyne detection are given by pure states, we have $S\left(\rho_E\right) = S\left(\rho_{A_1 B_1'}\right)$ and $S\left(\rho_E^{x_B', p_B'}\right) = S\left(\rho_{A_1}^{x_B', p_B'}\right)$. The Holevo bound becomes

$$\chi_{BE} = S\left(\rho_{A_1 B_1'}\right) - S\left(\rho_{A_1}^{x_B', p_B'}\right). \tag{A.5}$$

The required symplectic eigenvalues of $\gamma_{A_1 B_1'}$ are given by [66]

$$\lambda_{1,2}^2 = \frac{1}{2}\left(\Delta \pm \sqrt{\Delta^2 - 4D^2}\right), \tag{A.6}$$

with

$$\begin{aligned} \Delta &= a^2 + b^2 - 2c^2, \\ D &= ab - c^2. \end{aligned} \tag{A.7}$$

Correspondingly, we can obtain the covariance matrices of the state $\rho_{A_1}^{x_B', p_B'}$ as:

$$\begin{aligned} \gamma_{A_1}^{x_B', p_B'} &= aI_2 - c\sigma_z \left(bI_2 + I_2\right)^{\mathrm{MP}} c\sigma_z \\ &= \left(a - \frac{c^2}{b+1}\right) I_2, \end{aligned} \tag{A.8}$$

where MP represents the Moore Penrose inverse of a matrix [67], and its symplectic eigenvalue is given by

$$\lambda_3 = a - \frac{c^2}{b+1}. \tag{A.9}$$

Hence the Holevo bound can be written as

$$\chi_{BE} = G\left(\frac{\lambda_1 - 1}{2}\right) + G\left(\frac{\lambda_2 - 1}{2}\right) - G\left(\frac{\lambda_3 - 1}{2}\right). \tag{A.10}$$

Finally, the secret key rate can be derived by combining Eq. (15), Eq. (A.2), and Eq. (A.10).

[1] C. H. Bennett and G. Brassard, in *Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing, Bangalore, India* (IEEE, New York, 1984) pp. 175-179.

[2] G.-L. Long and X.-S. Liu, Phys. Rev. A **65**, 032302 (2002).

[3] F.-G. Deng, G. L. Long, and X.-S. Liu, Phys. Rev. A **68**, 042317 (2003).

[4] F.-G. Deng and G. L. Long, Phys. Rev. A **69**, 052319 (2004).

[5] L. Hanzo, H. Haas, S. Imre, D. O'Brien, M. Rupp, and L. Gyongyosi, Proc. IEEE **100**, 1853 (2012).

[6] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, Rev. Mod. Phys. **74**, 145 (2002).

[7] M. Sasaki, M. Fujiwara, H. Ishizuka, W. Klaus, K. Wakui, M. Takeoka, S. Miki, T. Yamashita, Z. Wang, A. Tanaka, et al., Opt. Express **19**, 10387 (2011).

[8] T. C. Ralph, Phys. Rev. A **61**, 010303 (1999).

[9] M. Hillery, Phys. Rev. A **61**, 022309 (2000).

[10] F. Grosshans, Phys. Rev. Lett. **94**, 020504 (2005).

[11] M. Navascués, F. Grosshans, and A. Acin, Phys. Rev. Lett. **97**, 190502 (2006).

[12] F. Furrer, T. Franz, M. Berta, A. Leverrier, V. B. Scholz, M. Tomamichel, and R. F. Werner, Phys. Rev. Lett. **109**, 100502 (2012).

[13] A. Leverrier, F. Grosshans, and P. Grangier, Phys. Rev. A **81**, 062343 (2010).

[14] A. Leverrier, Phys. Rev. Lett. **118**, 200501 (2017).

[15] A. Leverrier, Phys. Rev. Lett. **114**, 070501 (2015).

[16] D. Huang, P. Huang, D. Lin, and G. Zeng, Sci. Rep. **6**, 19201 (2016).

[17] D. Huang, P. Huang, H. Li, T. Wang, Y. Zhou, and G. Zeng, Opt. Lett. **41**, 3511 (2016).

[18] N. Hosseinidehaj and R. Malaney, Phys. Rev. A **91**, 022304 (2015).

[19] N. Hosseinidehaj, Z. Babar, R. Malaney, S. X. Ng, and L. Hanzo, IEEE Commun. Surv. Tut. **21**, 881 (2018).

[20] B. Qi, Phys. Rev. A **94**, 042340 (2016).

[21] B. Qi and C. C. W. Lim, Phys. Rev. Appl. **9**, 054008 (2018).

[22] T. Wang, P. Huang, S. Wang, and G. Zeng, Phys. Rev. A **99**, 022318 (2019).

[23] X. Wu, Y. Wang, Q. Liao, H. Zhong, and Y. Guo, Entropy **21**, 333 (2019).

[24] H. Qin, R. Kumar, and R. Alléaume, Proc. SPIE **8899**, 88990N (2013).

[25] H. Qin, R. Kumar, and R. Alléaume, Phys. Rev. A **94**, 012325 (2016).

[26] H. Qin, R. Kumar, V. Makarov, and R. Alléaume, Phys. Rev. A **98**, 012312 (2018).

[27] P. Jouguet, S. Kunz-Jacques, and E. Diamanti, Phys. Rev. A **87**, 062313 (2013).

[28] S. L. Braunstein and S. Pirandola, Phys. Rev. Lett. **108**, 130502 (2012).

[29] H.-K. Lo, M. Curty, and B. Qi, Phys. Rev. Lett. **108**, 130503 (2012).

[30] S. Pirandola, C. Ottaviani, G. Spedalieri, C. Weedbrook, S. L. Braunstein, S. Lloyd, T. Gehring, C. S. Jacobsen, and U. L. Andersen, Nat. Photonics **9**, 397 (2015).

[31] Z. Li, Y.-C. Zhang, F. Xu, X. Peng, and H. Guo, Phys. Rev. A **89**, 052301 (2014).

[32] X.-C. Ma, S.-H. Sun, M.-S. Jiang, M. Gui, and L.-M. Liang, Phys. Rev. A **89**, 042335 (2014).

[33] Y.-C. Zhang, Z. Li, S. Yu, W. Gu, X. Peng, and H. Guo, Phys. Rev. A **90**, 052325 (2014).

[34] C. Lupo, C. Ottaviani, P. Papanastasiou, and S. Pirandola, Phys. Rev. A **97**, 052327 (2018).

[35] Z. Chen, Y. Zhang, G. Wang, Z. Li, and H. Guo, Phys. Rev. A **98**, 012314 (2018).

[36] M. Lucamarini, Z. L. Yuan, J. F. Dynes, and A. J. Shields, Nature **557**, 400 (2018).

[37] X. Ma and M. Razavi, Phys. Rev. A **86**, 062319 (2012).

[38] O. Elmabrok, M. Ghalaii, and M. Razavi, J. Opt. Soc. Am. B **35**, 487 (2018).

[39] K. Kikuchi, J. Lightwave Technol. **34**, 157 (2015).

[40] L. Hanzo, W. Webb, and T. Keller, Single-and Multi-carrier Quadrature Amplitude Modulation: Principles and Applications for Personal Communications, WATM and Broadcasting: 2nd (IEEE Press-John Wiley, 2000).

[41] A. Leverrier and P. Grangier, Phys. Rev. A **83**, 042312 (2011).

[42] F. Grosshans, G. Van Assche, J. Wenger, R. Brouri, N. J. Cerf, and P. Grangier, Nature **421**, 238 (2003).

[43] C. E. Shannon, Bell Syst. Tech. J. **28**, 656 (1949).

[44] P. V. Trinh, T. V. Pham, H. V. Nguyen, S. X. Ng, and A. T. Pham, in *2016 IEEE Globecom Workshops (GC Wkshps)* (IEEE, 2016) pp. 1-6.

[45] F. Laudenbach, C. Pacher, C.-H. F. Fung, A. Poppe, M. Peev, B. Schrenk, M. Hentschel, P.Walther, and H. Hübel, Adv. Quantum Technol. **1**, 1800011 (2018).

[46] M. Stevens, D. Caplan, B. Robinson, D. Boroson, and A. Kachelmyer, Opt. Express **16**, 10412 (2008).

[47] F. Grosshans, N. J. Cerf, J. Wenger, R. Tualle-Brouri, and P. Grangier, Quantum Inf. Comput. **3**, 535 (2003).

[48] Y. Zhao, Y. Zhang, B. Xu, S. Yu, and H. Guo, Phys. Rev. A **97**, 042328 (2018).

[49] H.-X. Ma, P. Huang, D.-Y. Bai, S.-Y. Wang, W.-S. Bao, and G.-H. Zeng, Phys. Rev. A **97**, 042329 (2018).

[50] C. Ottaviani, G. Spedalieri, S. L. Braunstein, and S. Pirandola, Phys. Rev. A **91**, 022320 (2015).

[51] S. Pirandola, R. Laurenza, C. Ottaviani, and L. Banchi, Nat. Commun. **8**, 15043 (2017)

[52] A. Leverrier and P. Grangier, Phys. Rev. Lett. **102**, 180504 (2009).

[53] H.-X. Ma, P. Huang, D.-Y. Bai, T. Wang, S.-Y. Wang, W.-S. Bao, and G.-H. Zeng, Phys. Rev. A **99**, 022322 (2019).

[54] Z. Li, Y.-C. Zhang, and H. Guo, arXiv:1805.04249 (2018).

[55] H. Jiang and P. A. Wilford, IEEE Trans. Broadcast. **51**, 223 (2005).

[56] P. Papanastasiou, C. Ottaviani, and S. Pirandola, Phys. Rev. A **96**, 042332 (2017).

[57] X. Zhang, Y. Zhang, Y. Zhao, X. Wang, S. Yu, and H. Guo, Phys. Rev. A **96**, 042334 (2017).

[58] R. Kumar, A. Wonfor, R. Penty, T. Spiller, and I. White, Sci. Rep. **9**, 11190 (2019).

[59] D. Huang, P. Huang, D. Lin, C. Wang, and G. Zeng, Opt. Lett. **40**, 3695 (2015).

[60] X. Zhang, Y. Zhang, Z. Li, S. Yu, and H. Guo, IEEE Photon. J. **10**, 1 (2018).

[61] A. Semenov, F. Töppel, D. Y. Vasylyev, H. Gomonay, and W. Vogel, Phys. Rev. A **85**, 013826 (2012).

[62] D. Vasylyev, A. Semenov, andW. Vogel, Phys. Rev. Lett. **117**, 090501 (2016).

[63] Y. Guo, C. Xie, Q. Liao, W. Zhao, G. Zeng, and D. Huang, Phys. Rev. A **96**, 022320 (2017).

[64] A. S. Holevo, Probl. Inf. Transm. **9**, 3 (1973).

[65] A. S. Holevo, M. Sohma, and O. Hirota, Phys. Rev. A **59**, 1820 (1999).

[66] A. Serafini, F. Illuminati, and S. De Siena, J. Phys. B **37**, L21 (2003).

[67] R. A. Horn and C. R. Johnson, *Matrix analysis* (Cambridge university press, 2012).