Continuous-variable measurement-device-independent multipartite quantum communication via a fast-fading channel

Runbo Zhao,[1] Jian Zhou,[1,*] Ronghua Shi,[2] Jinjing Shi,[2] and Guangqiang He[3]

[1]*College of Computer and Mathematics, Central South University of Forestry and Technology, Changsha, Hunan 410004, People's Republic of China*

[2]*School of Electronic Information, Central South University, Changsha 410083, People's Republic of China*

[3]*State Key Laboratory of Advanced Optical Communication Systems and Networks, Department of Electronic Engineering, Shanghai Jiao Tong University, Shanghai 200240, People's Republic of China*

(Received 21 October 2024; accepted 3 January 2025; published 13 January 2025)

This study investigates the implementation of measurement-device-independent multiparty quantum communication using continuous-variable Greenberger-Horne-Zeilinger (CV GHZ) states under the fast fading channel. The communication parties are connected through free space, and factors such as atmospheric turbulence cause beam drift, resulting in variations in channel transmittance according to specific probability distributions. We assume a worst-case scenario in which an eavesdropper has complete control over the channel, forcing the communicators to estimate the channel based on this probability distribution. The protocol employs CV GHZ states to achieve secure communication through quantum cryptographic conference and quantum secret sharing. For the aspect of security, independent entangling cloner attack and coherent attack are analyzed. Simulation results demonstrate that the protocol can withstand advantageous attacks from eavesdroppers.

DOI: 10.1103/PhysRevA.111.012613

I. INTRODUCTION

Quantum communication [1] is first proposed to ensure the absolute security of transmitted information based on the quantum properties of microscopic particles. Quantum communication is divided into two branches based on the encoding scheme: continuous quantum information [2] and discrete quantum information techniques [3]. On the other hand, quantum information can be classified to quantum key distribution [4] and multipartite quantum communication [5] based on the number of users participating in the communication. The latter involves quantum secret sharing (QSS) [6] and quantum cryptography conference (QCC) [7]. Every legal participant gets the identical and complete message in QCC while all users can recover the full message together in QSS.

It is worth noting that quantum communication can guarantee the security of communication in principle, but the actual communication environment will have an impact on the security of communication. The attacks on detection device are huge threat to quantum communications. Fortunately, physicists have developed the measurement-device-independent (MDI) [8–10] method to defend the attacks on the detection devices where the signals are detected by the untrusted third party [11]. In this approach, all communicators connect to an untrusted party, eliminating detector side channels, representing a significant advancement bridging the gap between QKD theory and practice.

Research has explored multiparty continuous-variable quantum communication, utilizing Greenberger-Horne-Zeilinger (GHZ) states for information sharing [12]. GHZ states have been realized in several optical experiments, demonstrating the feasibility of theoretical quantum communication through multipartite entanglement [13,14]. However, on the other hand, in realistic implementations, one should also consider the possibility of temporal variations of the communication line between two remote users as modeled by the so-called fading channel. Fast-fading channel describes connections between communicators through free space, where adverse propagation conditions, such as atmospheric turbulence [15,16], cause fluctuations in phase and amplitude. Consequently, the channel's projection rate varies according to mathematical probabilities, leading to data corruption. In such complex environments, the rapid signal changes significantly degrade communication performance [17]. In this case, the transmissivity of the link between the two parties is not constant and may take values according to some probability distribution.

To achieve quantum encrypted communication in challenging real-world environments, this paper presents a continuous-variable measurement-device-independent (CV MDI) multiparty quantum communication system via fast-fading channel. It extends the implementation of CV MDI multipartite quantum communication, based on GHZ states with uniformly reduced channel loss, to free-space links affected by atmospheric turbulence, making it more suitable for practical applications. It employs two types of protocols: QCC and QSS, addressing both individual and collaborative decryption scenarios to ensure communication security. In a nutshell, the continuous variable GHZ states, which can be used to implement QCC and QSS, are generated by MDI technique. Then the proposed continuous-variable MDI multiparty quantum communication via fast-fading channel can defend the attacks on detection devices. Moreover, in the proposed protocol, it is assumed that the eavesdropper has full control of the fast-fading process. Under this circumstance, the eavesdropper

*Contact author: 13142153489@163.com

can choose the instantaneous transmissivity of the channel while the legal participants can only detect the mean statistical process. The performance of the continuous-variable MDI multiparty quantum communication protocols in the worst-case scenario are studied. It is also enhanced from a utility point of view, demonstrating that the protocol is still well available in harsh environments, contributing to the real-world implementation of quantum communication.

The organization of this paper is as follows. In Sec. II, we provide a detailed explanation of how to utilize CV GHZ states to implement multiparty quantum communication protocols, highlighting both the prepare-and-measure (PM) and entanglement-based (EB) schemes. In Sec. III, we examine the implementation of multiparty quantum communication via fast-fading channel and provide a brief overview of the postselection (PS) scheme. In Sec. IV, we analyze how QCC and QSS protocols withstand independent entangling cloner and coherent attacks. Section V presents simulations and performance analyses of the QCC and QSS protocols, testing their performance based on actual parameters. Finally, the conclusion is drawn in Sec. VI.

II. CONTINUOUS-VARIABLE GREENBERGER-HORNE-ZEILINGER STATES

This section will detail the implementation of QCC and QSS schemes using CV GHZ states. CV GHZ states are quantum states formed by the entanglement of multiple modes, typically three or more. These states resemble the originally proposed discrete-variable GHZ states and are described in continuous-variable systems by the orthogonal components of the light field, such as phase and amplitude.

The QCC scheme [7,18] is designed for a group of users who need to conduct a secure conference. In this scenario, each member must be able to decrypt any encrypted public information broadcasted by other members, while ensuring that external parties cannot access this information. Although a straightforward approach would involve assigning a separate key for each pair of users through simple two-user encryption, this method is inefficient. A more effective solution is for users within the group to share particles, with measurement results used to establish a common key known to all group members.

Conversely, the QSS scheme [6,19,20] is applicable in situations where the entire group must collaborate to decrypt a message. This is achieved by using GHZ states to divide the published quantum information into multiple parts, each of which does not contain the original information. Only by combining these parts can the original information be restored. This approach significantly simplifies the complexity associated with information splitting required for secret sharing in classical key systems.

CV GHZ states have been realized and confirmed in various optical experiments [13,14]. Here, we demonstrate how to implement the PM scheme [21] and EB scheme [22] for QCC and QSS using CV GHZ states. The three parties involved in the communication (Alice, Bob, and Charlie) are connected to an untrusted party, David, to eliminate potential attacks from the detector side. The security of the communication relies on

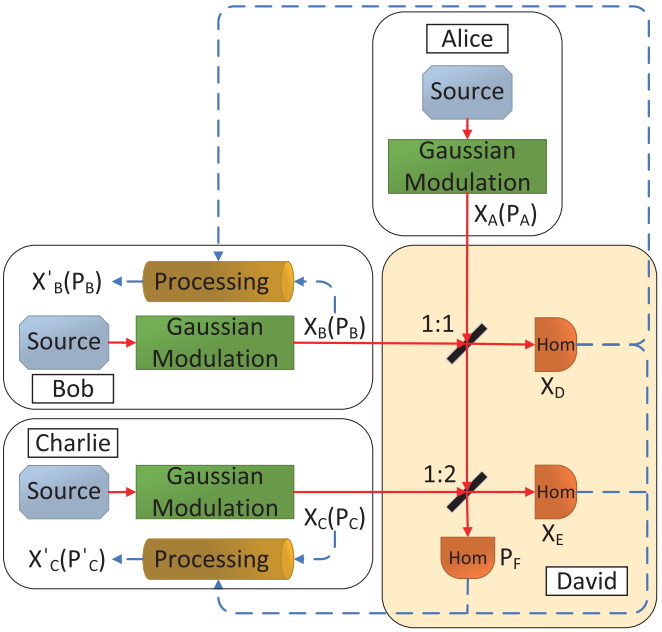

FIG. 1. PM scheme of the multipartite measurement-device-independent quantum communication. The measurement is completed by the relay.

David's operations and measurement data. We first present the PM scheme illustrated in Fig. 1.

PM scheme.

Step 1: Alice, Bob, and Charlie generate random numbers using their respective signal sources and then apply Gaussian modulation to the squeezed states. In the QCC scheme, the position of the squeezed vacuum state is modulated, with X_A, X_B, and X_C obeying Gaussian distribution. In the QSS scheme, the momentum of the squeezed vacuum state is modulated, yielding an average momentum that follows a Gaussian distribution represented by random numbers P_A, P_B, and P_C.

Step 2: These three parties involved in the communication send the modulation results to the untrusted party, David. David then mixes the various states using two beam splitters he has prepared and detects the output results with three homodyne detectors. He subsequently broadcasts the measurement results to Alice, Bob, and Charlie.

Step 3: Alice, Bob, and Charlie need to perform data post-processing [23] to further analyze and manipulate the acquired data. In the QCC scheme, Bob modifies X_B using $X'_B = X_B + \sqrt{2}X_D$, while Charlie modifies X_C with $X'_C = X_C + (\sqrt{\frac{1}{2}}X_D - \sqrt{\frac{3}{2}}X_E)$, leaving Alice unchanged. This results in the construction of a GHZ state that satisfies the relationships $X_A - X'_B \to 0$ and $X'_B - X'_C \to 0$. In the QSS scheme, Charlie changes P_C to $P'_C = P_C + \sqrt{3}P_F$, while Alice and Bob remain unchanged, thereby satisfying $P_A + P_B + P'_C \to 0$ [12].

Step 4: Finally, these participants can implement QCC or QSS with these data they kept.

The PM scheme is normally used to guide experiment. For the sake of analyzing the security of the proposed schemes, the equivalent EB scheme is also proposed. The specific steps of the EB scheme are illustrated in Fig. 2.

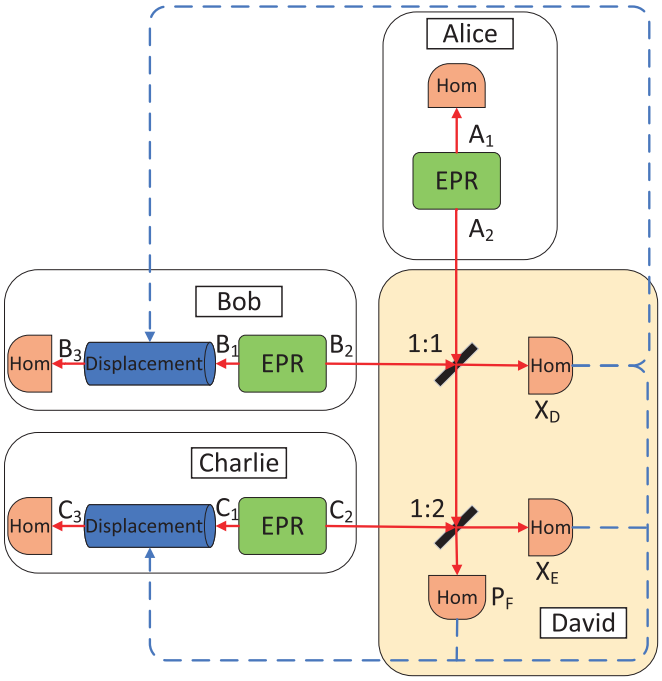

FIG. 2. EB scheme of the multipartite measurement-device-independent quantum communication. The legitimate users displace their own states based on the measurement result announced by the relay. The GHZ states shared by the users can be used to share keys.

EB scheme.

Step 1: Alice, Bob, and Charlie each prepare an EPR pair, keeping one mode for themselves while sending the other mode to the untrusted party, David.

Step 2: David prepared two specific beam splitters. First, he used a 1:1 beam splitter to combine the modes sent by Alice and Bob. One of the two new output modes was measured using a homodyne detector and obtained the position quadrature $\hat{X}_D$, while the other was sent to a 1:2 beam splitter. This second mode was mixed with the mode from Charlie and then the position quadrature $\hat{X}_E$ and momentum quadrature $\hat{P}_F$ were measured by two homodyne detectors. Subsequently, David broadcasted these measurement results X_D, X_E, and P_F [24].

Step 3: These participants proceed these data with post-processing operation. Bob modifies the position quadrature with $\hat{X}_{B_1} = \sqrt{2}X_D$ after receiving X_D, while Charlie modifies the position quadrature by $\hat{X}_{C_1} = (\sqrt{\frac{1}{2}}X_D - \sqrt{\frac{3}{2}}X_E)$ and momentum quadrature by $\hat{P}_{C_1} = \sqrt{3}P_F$. Then, the modes A_1, B_3, and C_3 held by them form a set of GHZ states. In the QCC scheme, they satisfy the conditions $\hat{X}_{A_1} - \hat{X}_{B_3} \to 0$ and $\hat{X}_{B_3} - \hat{X}_{C_3} \to 0$. the condition $\hat{P}_{A_1} + \hat{P}_{B_3} + \hat{P}_{C_3} \to 0$ can be used to implement QSS [12].

Step 4: At least two of the three parties in the communication must disclose their private results to recover the secret.

III. PROTOCOLS OF MULTIPARTITE QUANTUM COMMUNICATION via FAST-FADING CHANNEL

The protocol via fast-fading channel is illustrated in Fig. 3. Alice, Bob, and Charlie send their states to David through this channel, forming the CV GHZ state described in the previous section, and then engage in encrypted communication using QCC or QSS. In real-world scenarios, strong atmospheric turbulence leads to rapid fluctuations in channel transmittance, causing effects such as beam spreading, absorption, and scattering [25]. Consequently, their transmitted signals experience significant interference, resulting in a decreased secure key rate and potential communication disruption under sufficiently strong interference. This paper discusses the worst-case scenario, utilizing the most pessimistic estimated transmittance, $\eta^{\min}_{A(B,C)}$, for the channels of Alice, Bob, and Charlie. This is achieved through a postselection (PS) scheme.

The complexity of fast-fading channel influenced by atmospheric conditions is significant. In our analysis, we often consider the postselection (PS) scheme [26]. Typically, the volatility of atmospheric channels falls within the kilohertz range, while modulation and detection rates are usually in the megahertz range. This disparity allows for the transmission of thousands of signals or detection states during the stable time of atmospheric channel attenuation, with each measurement reflecting a relatively stable transmittance. We categorize the channel into multiple subchannels, where the collective state of these subchannels represents a mixture of their individual states, described by the overall channel's probability transmittance. By selecting subchannels with lower attenuation, we can achieve higher key rates or stronger entanglement. In practical experiments, operations are conducted based on this categorization. The estimated channel transmittance by the communicators is faster than the fluctuations of the channel, enabling them to assess the actual transmission conditions (P_η). The PS scheme has been shown to ensure the security of Gaussian protocols and the recovery of entangled states. In our approach, communicators perform postselection by choosing a subset of the actual transmittance distribution $\{\eta_i\}$ for subsequent statistical analysis and key rate calculations. We consider the worst-case scenario to be the most pessimistic selection within the chosen subset.

The diagram on the right side of Fig. 3 illustrates the transmission probability of the subchannel PS principle. The green shaded area represents the cumulative interval of reliable transmittance within the subchannel. To increase the overall success probability, this interval must be expanded by shifting $\eta_{\min}$ downward, thereby allowing more data contributions from the subchannels to enhance security.

IV. SECURITY ANALYSIS

Since the safety levels of the PM and EB schemes are equivalent, but the EB scheme offers greater robustness in complex scenarios, we focus on analyzing the EB scheme. We will address two aspects: independent entangling cloner attack and coherent attack [27].

A. Independent entangling cloner attack

In this section, we focus on the independent entangling cloner attacks on each channel, as illustrated in Fig. 4.

Before the attack, Eve prepares three EPR pairs. Using beam splitters with transmittances $\eta_{A(B,C)}$, Eve injects one mode of each EPR pair into a fast-fading channel. The output after the attack, denoted as $\hat{E}_{A1(B1,C1)}$, and the other mode of the EPR pair, denoted as $\hat{E}_{A2(B2,C2)}$, are stored in a quantum

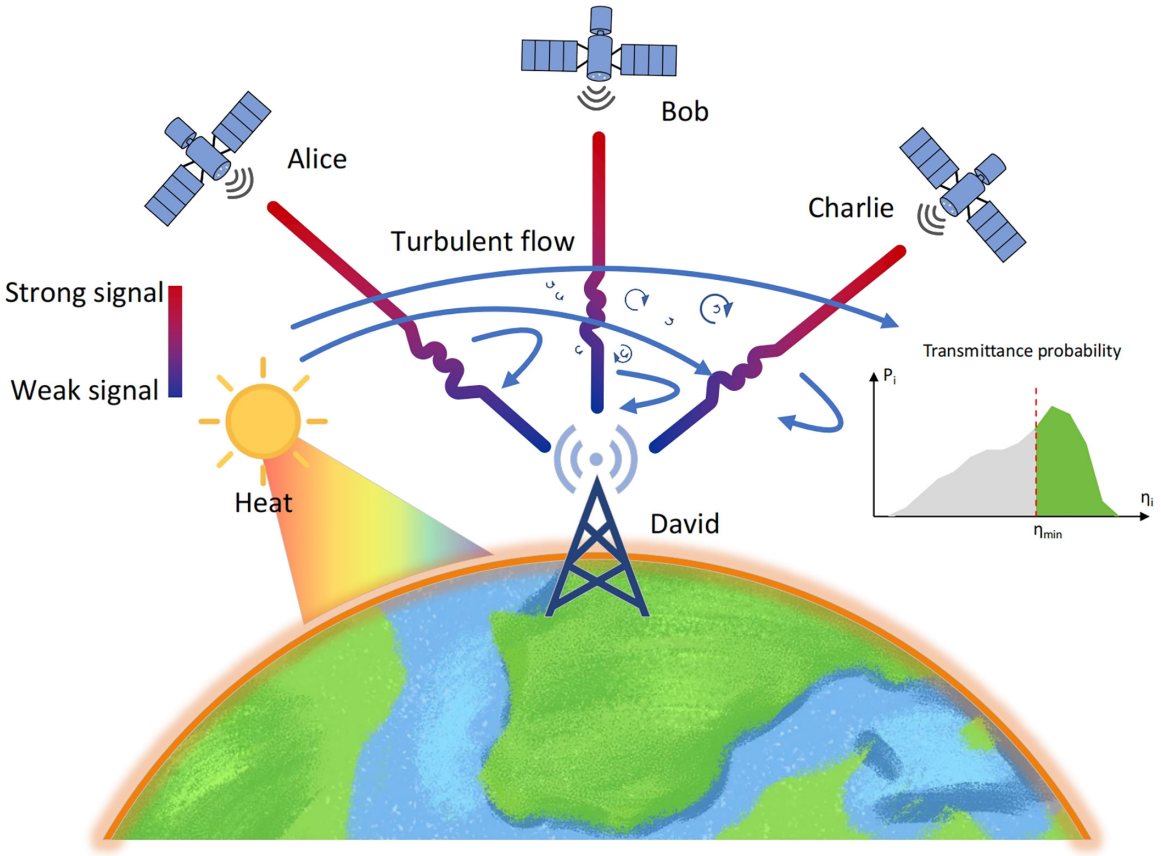

FIG. 3. Scheme of the continuous-variable measurement-device-independent multipartite quantum communication via fast-fading channel.

memory (QM). The initial state ρ_{A,E_A,B,E_B,C,E_C} consists of six independent tensor products of TMSS, forming a covariance matrix, which can be expressed as

$$V_{A,E_A,B,E_B,C,E_C} = \bigoplus_{k=1}^{3} V, \tag{1}$$

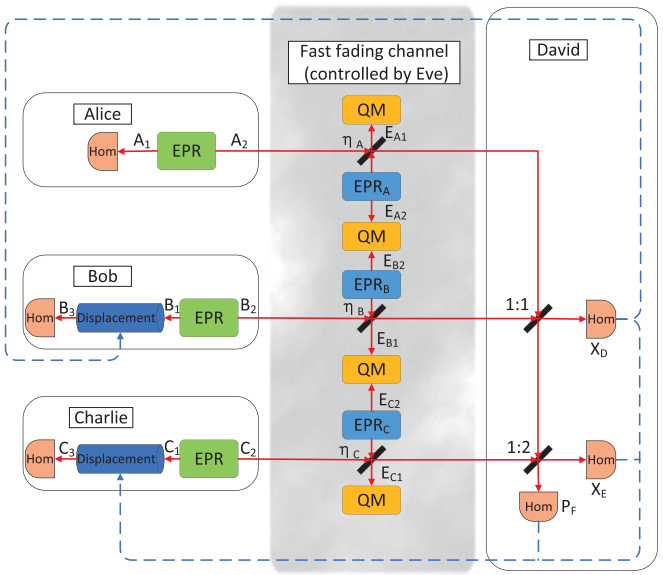

FIG. 4. EB Scheme for independent entangling cloner attack via fast-fading channel.

where

$$V = \begin{pmatrix} VI & \sqrt{V^2-1}Z & 0 & 0 \\ \sqrt{V^2-1}Z & VI & 0 & 0 \\ 0 & 0 & V_E I & \sqrt{V_E^2-1}Z \\ 0 & 0 & \sqrt{V_E^2-1}Z & V_E I \end{pmatrix}. \tag{2}$$

$V(V \geqslant 1)$ represents the variance of Alice's (Bob's, Charlie's) two-mode squeezed state (TMSS) [28], $V_E(V_E \geqslant 1)$ represents the variance of Eve's TMSS, I is the identity matrix, 0 is the zero matrix, and Z is the Pauli Z matrix. In each channel, the communicators (Alice, Bob, or Charlie) transmit patterns through beam splitters with transmittance $\eta_{A(B,C)}$. Eve injects an attack into this process, denoted as

$$U_{\text{Eve}} = BS_A \oplus BS_B \oplus BS_C, \tag{3}$$

where

$$BS_{A(B,C)} = \begin{pmatrix} I & 0 & 0 & 0 \\ 0 & \sqrt{\eta_{A(B,C)}}I & \sqrt{1-\eta_{A(B,C)}}I & 0 \\ 0 & -\sqrt{1-\eta_{A(B,C)}}I & \sqrt{\eta_{A(B,C)}}I & 0 \\ 0 & 0 & 0 & I \end{pmatrix}. \tag{4}$$

In this study, we examine the worst-case scenario where the eavesdropper, Eve, has complete control over the transmission channel. This means that Eve can manipulate the instantaneous transmittance. Consequently, honest communicators can only obtain the probability distribution of channel fading at the end of the communication. To extract the key, honest users assume the minimum transmittance, denoted as $\eta_{\min}$, based on this distribution [29]. At this point, Eq. (4) becomes

$$BS'_{A(B,C)} = \begin{pmatrix} I & 0 & 0 & 0 \\ 0 & \sqrt{\eta^{\min}_{A(B,C)}}I & \sqrt{1-\eta^{\min}_{A(B,C)}}I & 0 \\ 0 & -\sqrt{1-\eta^{\min}_{A(B,C)}}I & \sqrt{\eta^{\min}_{A(B,C)}}I & 0 \\ 0 & 0 & 0 & I \end{pmatrix}. \tag{5}$$

The transmittance rate $\eta_{A(B,C)}$ is not a constant and must be estimated probabilistically. In the most random scenarios, the transmittance rate is uniformly distributed between two extremes, $\eta^{\min}_{A(B,C)}$ and $\eta^{\max}_{A(B,C)}$, and they satisfy

$$\eta^{\max}_{A(B,C)} = \eta^{\min}_{A(B,C)} + \Delta\eta_{A(B,C)}. \tag{6}$$

After receiving the hybrid mode, which has been contaminated by attackers, David mixed these three received modes using two splitters [30]

$$U_{\text{David}} = BS_2 BS_1, \tag{7}$$

where

$$BS_1 = \begin{pmatrix} W_1 & W_2 & 0 \\ -W_2 & W_1 & 0 \\ 0 & 0 & I \end{pmatrix}, \quad BS_2 = \begin{pmatrix} W_3 & 0 & W_4 \\ 0 & I & 0 \\ -W_4 & 0 & W_3 \end{pmatrix},$$

$$W_1 = \begin{pmatrix} I & 0 & 0 & 0 \\ 0 & \frac{1}{\sqrt{2}}I & 0 & 0 \\ 0 & 0 & I & 0 \\ 0 & 0 & 0 & I \end{pmatrix}, \quad W_2 = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & \frac{1}{\sqrt{2}}I & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix},$$

$$W_3 = \begin{pmatrix} I & 0 & 0 & 0 \\ 0 & \sqrt{\frac{2}{3}}I & 0 & 0 \\ 0 & 0 & I & 0 \\ 0 & 0 & 0 & I \end{pmatrix}, \quad W_4 = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & \frac{1}{\sqrt{3}}I & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}. \tag{8}$$

Prior to homodyne measurement, the entire state $\rho_{A_1,F,E_{A1},E_{A2},B_1,D,E_{B1},E_{B2},C_1,E,E_{C1},E_{C2}}$ evolves with its covariance matrix. It is

$$V_{A_1,F,E_{A1},E_{A2},B_1,D,E_{B1},E_{B2},C_1,E,E_{C1},E_{C2}} = U_{\text{David}} U_{\text{Eve}} V_{A,E_A,B,E_B,C,E_C} U^T_{\text{Eve}} U^T_{\text{David}}. \tag{9}$$

Next, rewrite the covariance matrix in the order of A_1, B_1, C_1, Eve, D, E, F, is

$$V_{A_1,B_1,C_1,\text{Eve},D,E,F} = \begin{pmatrix} V_{A_1,B_1,C_1,\text{Eve},D,E} & C \\ C^T & V_F \end{pmatrix}. \tag{10}$$

In this context, C denotes the covariance submatrix, and Eve encompasses all patterns related to Eve, including $E_{A1}, E_{A2}, E_{B1}, E_{B2}, E_{C1}$, and E_{C2}. Simplify the covariance matrix $V_{A_1,B_1,C_1,\text{Eve},D,E}$ using homodyne measurement $\hat{P}_F$

$$V_{A_1,B_1,C_1,\text{Eve},D,E} = V_{A_1,B_1,C_1,\text{Eve},D,E|P_F} + C \begin{pmatrix} 0 & 0 \\ 0 & \frac{1}{V(\hat{P}_F)} \end{pmatrix} C^T. \tag{11}$$

The variance of $\hat{P}_F$, denoted as $V(\hat{P}_F)$, is provided in the matrix V_F [31].

After iteratively computing the covariance matrix of the state following partial Gauss measurements [32,33], it is evident from Eq. (11) that this process is independent of the measurement outcomes, and the covariance matrix remains constant. Because the displacement operation maintains the variance and covariance of $\hat{X}$ and $\hat{P}$ unchanged while only altering their means, partial state ρ_{A_1,B_3,C_3} have the same covariance matrix as $\rho_{A_1,B_1,C_1|X_D,X_E,P_F}$ [12]. Therefore, we can obtain the state $\rho_{A_1,B_3,C_3,Eve}$ in the covariance matrix $V_{A_1,B_3,C_3,Eve}$. The key rate is calculated as the difference between the mutual information of the communicating parties and Eve's mutual information. Under this circumstance, we have

$$K(\eta_{A(B,C)}) = I_{AB(AC,BC)} - I_E. \tag{12}$$

where $I_{AB(AC,BC)}$ are the mutual information between Alice, Bob, and Charlie, respectively, and I_E is the valid information stolen by eavesdropper Eve.

Via fast-fading channel, communication parties rely on the PS scheme to estimate the channel conditions. We consider the worst-case scenario where Eve has complete control over the transmission channel, allowing her to arbitrarily specify the instantaneous pass rate for each transmission. The transmittance rate fluctuates randomly within a range in the communicator's perception. We select the optimal estimated boundary $\eta_{\min}$ to estimate the eavesdropper's average mutual information $\widetilde{I}_E$, the key rate becomes

$$K_{\text{fast}} = \beta I^{\eta_{\min}}_{AB(AC,BC)} - \widetilde{I}_E, \tag{13}$$

where correction efficiency coefficient $\beta \in [0, 1]$ [34].

Alice, Bob, and Charlie only know that the minimum transmittance, $\eta_{\min}$, follows a specific distribution P_η. We consider a scenario where only one user is in a fast-fading channel. When they estimate using the worst-case scenario, denoted as $I^{\eta_{\min}}_{AB(AC,BC)} := I_{AB(AC,BC)}(\eta^{\min}_{A(B,C)})$, the eavesdropper's accessible information is determined by the average Holevo quantity [35], is

$$\widetilde{I}_E = \int \mathrm{d}\eta P_\eta \chi(E:\gamma). \tag{14}$$

Under the circumstance, Eq. (13) becomes

$$K_{\text{fast}} = \beta I_{AB(AC,BC)}\left(\eta^{\min}_{A(B,C)}\right) - \frac{1}{\Delta\eta}\int_{\eta^{\min}_{A(B,C)}}^{\eta^{\max}_{A(B,C)}} \mathrm{d}\eta \chi(E:\gamma). \tag{15}$$

$\chi(E:\gamma)$ represents the mutual information of Eve.

In the QCC scheme, let us assume that Alice intends to share the secret key with Bob and Charlie, key rate is

$$K_{\text{QCC}} = \min\{K_{\text{AB}}, K_{\text{AC}}\}. \tag{16}$$

The reverse reconciliation [36] key rates are given by

$$K_{\mathrm{AB}}^{\mathrm{RR}} = \beta I\left(X_{A_1} : X_{B_3}\right) - \frac{1}{\Delta\eta}\int_{\eta_{\min}}^{\eta_{\max}} d\eta I\left(X_{A_1} : X_{E_{A1}}, X_{E_{A2}}\right), \tag{17}$$

$$K_{\mathrm{AC}}^{\mathrm{RR}} = \beta I\left(X_{A_1} : X_{C_3}\right) - \frac{1}{\Delta\eta}\int_{\eta_{\min}}^{\eta_{\max}} d\eta I\left(X_{A_1} : X_{E_{A1}}, X_{E_{A2}}\right). \tag{18}$$

The direct reconciliation key rates are given by

$$K_{\mathrm{AB}}^{\mathrm{DR}} = \beta I\left(X_{A_1} : X_{B_3}\right) - \frac{1}{\Delta\eta}\int_{\eta_{\min}}^{\eta_{\max}} d\eta I\left(X_{B_3} : X_{E_{B1}}, X_{E_{B2}}\right), \tag{19}$$

$$K_{\mathrm{AC}}^{\mathrm{DR}} = \beta I\left(X_{A_1} : X_{C_3}\right) - \frac{1}{\Delta\eta}\int_{\eta_{\min}}^{\eta_{\max}} d\eta I\left(X_{C_3} : X_{E_{C1}}, X_{E_{C2}}\right), \tag{20}$$

where

$$I\left(X_{A_1} : X_{B_3(C_3)}\right) = \frac{1}{2}\log_2 \frac{V\left(\hat{X}_{B_3(C_3)}\right)}{V\left(\hat{X}_{B_3(C_3)}\middle|X_{A_1}\right)}, \tag{21}$$

and

$$I\left(X_{A_1(B_3,C_3)} : X_{E_{A1(B1,C1)}}, X_{E_{A2(B2,C2)}}\right) = \frac{1}{2}\log_2 \frac{V\left(\hat{X}_{A1(B1,C1)}\right)}{V\left(\hat{X}_{A1(B1,C1)}\middle|X_{E_{A1(B1,C1)}}, X_{E_{A2(B2,C2)}}\right)}. \tag{22}$$

The condition variance of $\hat{X}_{B_3(C_3)}$ after homodyne detection $\hat{X}_{A_1}$ is represented by $V(\hat{X}_{B_3(C_3)}|X_{A_1})$ and can be obtained from the covariance matrix $V_{B_3C_3|X_{A_1}}$ [12]. After homodyne detection for $\hat{X}_{E_{A1}(B1,C1)}$ and $\hat{X}_{E_{A2(B2,C2)}}$, the variance of $\hat{X}_{A1(B1,C1)}$ can be obtained from a simplified covariance matrix $V_{A_1(B_3,C_3)|X_{E_{A1(B1,C1)}},X_{E_{A2(B2,C2)}}}$, recorded as $V(\hat{X}_{A1(B1,C1)}|X_{E_{A1(B1,C1)}}, X_{E_{A2(B2,C2)}})$.

For the QSS scheme, we assume that Charlie holds the key, and the reverse reconciliation key rates are defined as

$$K_{\mathrm{QSS}}^{\mathrm{RR}} = \beta I\left(P_{A_1}, P_{B_3} : P_{C_3}\right) - \frac{1}{\Delta\eta}\int_{\eta_{\min}}^{\eta_{\max}} d\eta I\left(P_{C_3} : P_{E_{C1}}, P_{E_{C2}}\right), \tag{23}$$

the direct reconciliation key rates are defined as

$$K_{\mathrm{QSS}}^{\mathrm{DR}} = \beta I\left(P_{A_1}, P_{B_3} : P_{C_3}\right) - \frac{1}{\Delta\eta}\int_{\eta_{\min}}^{\eta_{\max}} d\eta\left[I\left(P_{A_1} : P_{E_{A1}}, P_{E_{A2}}\right) + I\left(P_{B_3} : P_{E_{B1}}, P_{E_{B2}}\right)\right]. \tag{24}$$

For Eq. (23), we obtain mutual information from the covariance matrix, as

$$I\left(P_{A_1}, P_{B_3} : P_{C_3}\right) = \frac{1}{2}\log_2 \frac{V\left(\hat{P}_{C_3}\right)}{V\left(\hat{P}_{C_3}\middle|P_{A_1}, P_{B_3}\right)}, \tag{25}$$

and

$$I(P_{C_3} : P_{E_{C1}}, P_{E_{C2}}) = \frac{1}{2}\log_2 \frac{V\left(\hat{P}_{C_3}\right)}{V\left(\hat{P}_{C_3}\middle|P_{E_{C1}}, P_{E_{C2}}\right)}. \tag{26}$$

In Eq. (24), the maximum mutual information between Eve's measurement data and those of Alice and Bob is

$$I\left(P_{A_1} : P_{E_{A1}}, P_{E_{A2}}\right) + I\left(P_{B_3} : P_{E_{B1}}, P_{E_{B2}}\right) = \frac{1}{2}\log_2 \frac{V\left(\hat{P}_{A_1}\right)}{V\left(\hat{P}_{A_1}\middle|P_{E_{A1}}, P_{E_{A2}}\right)} + \frac{1}{2}\log_2 \frac{V\left(\hat{P}_{B_3}\right)}{V\left(\hat{P}_{B_3}\middle|P_{E_{B1}}, P_{E_{B2}}\right)}. \tag{27}$$

In contrast, under slow fading channel, the channel transmittance remains constant after a sufficient number of uses, enabling remote users to estimate its actual value. At this point, the key rate is averaged over the transmittance distribution, and the mutual information of the communicating parties and Eve needs to be averaged as well [29]. Therefore, Eq. (15) transforms to

$$K_{\mathrm{slow}} = \frac{1}{\Delta\eta}\int_{\eta_{A(B,C)}^{\min}}^{\eta_{A(B,C)}^{\max}} d\eta\left[\beta I_{AB(AC,BC)}\left(\eta_{A(B,C)}^{\min}\right) - \chi(E:\gamma)\right]. \tag{28}$$

In symmetric scenarios, all users experience interference via fast-fading channels, and the transmittance for each channel $\eta_{A(B,C)}^{\min}$ follows the same probability distribution. Consequently, the key rate becomes

$$K_{\mathrm{fast}}^{\mathrm{symmetric}} = \beta I_{AB(AC,BC)}\left(\eta_{A(B,C)}^{\min}\right) - \frac{1}{(\Delta\eta)^3} \times \int_{\eta_A^{\min}}^{\eta_A^{\max}}\int_{\eta_B^{\min}}^{\eta_B^{\max}}\int_{\eta_C^{\min}}^{\eta_C^{\max}} d\eta_A d\eta_B d\eta_C \chi(E:\gamma). \tag{29}$$

B. Coherent attack

In this section, we will investigate the security of a more general case in coherent attacks. Based on the de Finetti theorem [37–39], a Gaussian-modulation protocol is secure against general attack when it is secure against collective attack. But in the actual security analysis, coherent attack is more threaten to the protocol than collective attack when more than one channel is used. This study focuses on multiparty communication via fast-fading channel, in such scenarios, coherent attacks pose a greater threat to secure communication than collective attacks due to the correlation between quantum states across different channels. Consequently, the key rate is reduced. Therefore, it is essential to reassess the impact of coherent attacks on protocol security to demonstrate higher security requirements [26]. This process is illustrated in Fig. 5. Eve extracts three quantum modes in the auxiliary quantum modes and injects them into three fast-fading channels. The fourth quantum mode and one of the outcomes from each channel's beam splitter are stored in the QM. Eve measures these quantum modes to obtain maximum information.

The reduced state ρ_{E_A,E_B,E_C} of Eve can be determined in the covariance matrix below

$$V_{E_A,E_B,E_C} = \begin{pmatrix} V_A & G_1 & G_2 \\ G_1 & V_B & G_3 \\ G_2 & G_3 & V_C \end{pmatrix}, \tag{30}$$

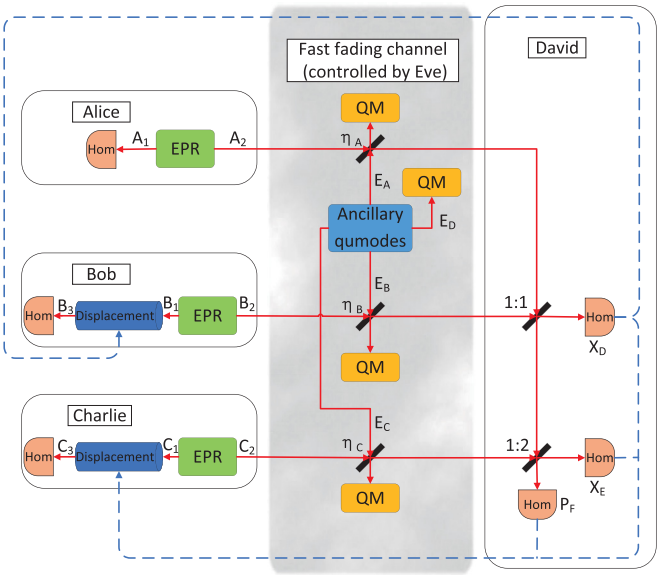

FIG. 5. EB Scheme for coherent attack via fast-fading channel.

where

$$V_{E_A} = V_{E_A} I, V_{E_B} = V_{E_B} I, V_{E_C} = V_{E_C} I,$$

$$G_1 = \begin{pmatrix} g_1 & 0 \\ 0 & g_1' \end{pmatrix}, \quad G_2 = \begin{pmatrix} g_2 & 0 \\ 0 & g_2' \end{pmatrix}, \quad G_3 = \begin{pmatrix} g_3 & 0 \\ 0 & g_3' \end{pmatrix}. \tag{31}$$

The variances V_{E_A}, V_{E_B}, and V_{E_C} represent the thermal noise injected by Eve into each channel. The correlations between the noise added by Eve in the three channels are denoted as g_1, g_2, and g_3. Thus, the covariance matrix of the whole system can be expressed as:

$$V_{A,B,C,\text{Eve}} = \bigoplus_{k=1}^{3} V' \oplus V_{E_A,E_B,E_C}, \tag{32}$$

where

$$V' = \begin{pmatrix} VI & \sqrt{V^2-1}Z \\ \sqrt{V^2-1}Z & VI \end{pmatrix}. \tag{33}$$

Rearranging the covariance matrix in Eq. (32) in the order of A, E_A, B, E_B, C, E_C, and applying the conjugate unitary operation yields the full modal covariance matrix, which includes A_1, B_1, C_1, and Eve, is

$$U'_{\text{David}} U'_{\text{Eve}} V_{A,E_A,B,E_B,C,E_C} U'^{T}_{\text{Eve}} U'^{T}_{\text{David}}. \tag{34}$$

In this process, U'_{David} and U'_{Eve} must remove the seventh and eighth rows and columns of matrix $BS'_{A(B,C)}$ from Eq. (5) and $W_{I(2,3,4)}$ from Eq. (8) to match the dimensions with V_{A,E_A,B,E_B,C,E_C}. Next, we should delete the rows and columns related to Eve in Eq. (34) and rearrange according to A_1, B_1, C_1, D, E, F to obtain the covariance matrix $V_{A_1,B_1,C_1,D,E,F}$. Performing the same operations as in Eq. (11), the displacement operation will not alter the covariance matrix, resulting in covariance matrix $V_{A_1,B_3,C_3|X_D,X_E,P_F}$.

Once the covariance matrix is obtained, the calculation of the key rate can commence. In the case of a fast-fading channel, the key rate for the QCC scheme is given by

$$\begin{aligned} K_{\text{AB}}^{\text{RR}} &= \beta I(X_{A_1} : X_{B_3}) - H(\rho_{\text{Eve}} : X_{A_1}), \\ K_{\text{AC}}^{\text{RR}} &= \beta I(X_{A_1} : X_{C_3}) - H(\rho_{\text{Eve}} : X_{A_1}). \end{aligned} \tag{35}$$

$H(\rho_{\text{Eve}} : X_{A_1})$ represents the Holevo quantity of the quantum state ρ, indicating the maximum information that Eve can obtain during an attack, calculated as follows:

$$H(\rho_{\text{Eve}} : X_{A_1}) = S(\rho_{A_1,B_3,C_3}) - S(\rho_{B_3,C_3|X_{A_1}}). \tag{36}$$

$S(\rho_{A_1,B_3,C_3})$ is calculated from the covariance matrix V_{A_1,B_3,C_3} as

$$S(\rho_{A_1,B_3,C_3}) = h(\nu_1) + h(\nu_2) + h(\nu_3). \tag{37}$$

Here, ν_1, ν_2, and ν_3 are the symplectic eigenvalues of a matrix [40]. Moreover,

$$h(x) := \frac{x+1}{2}\log_2\frac{x+1}{2} - \frac{x-1}{2}\log_2\frac{x-1}{2}. \tag{38}$$

Similarly, it can be concluded that

$$S(\rho_{B_3,C_3|X_{A_1}}) = h(\nu_4) + h(\nu_5). \tag{39}$$

In this context, ν_4 and ν_5 represent the symplectic eigenvalues of the covariance matrix $V_{B_3,C_3|X_{A_1}}$. For QSS schemes via fast-fading channel, the key rate is

$$K_{\text{QSS}}^{\text{RR}} = \beta I(P_{A_1}, P_{B_3} : P_{C_3}) - \frac{1}{\Delta\eta}\int_{\eta_{\min}}^{\eta_{\max}} H(\rho_{\text{Eve}} : P_{C_3}), \tag{40}$$

where

$$\begin{aligned} H(\rho_{\text{Eve}} : P_{C_3}) &= S(\rho_{\text{Eve}}) - S(\rho_{\text{Eve}|P_{C_3}}) \\ &= S(\rho_{A_1,B_3,C_3}) - S(\rho_{A_1,B_3|P_{C_3}}). \end{aligned} \tag{41}$$

$S(\rho_{A_1,B_3|P_{C_3}})$ can be calculated from $h(\nu_6) + h(\nu_7)$, where ν_6 and ν_7 are the symplectic eigenvalues of the covariance matrix $V_{A_1,B_3|P_{C_3}}$.

V. SIMULATION AND PERFORMANCE ANALYSIS

To demonstrate higher security requirements, this section primarily discusses coherent attacks. We denote the transmittance of the channel between Alice (Bob, Charlie) and David as $\eta_{A(B,C)} = 10^{-\frac{L_{A(B,C)}}{10}}$, where $L_{A(B,C)}$ represents their respective transmission distances. Each channel connected to an untrusted third party, David, can be considered a fast-fading channel. Both in the QCC and QSS schemes, these three participants Alice, Bob, and Charlie are in the same status. In order to analyze the performance of the protocol when the distance between three users is asymmetrical, we set $L_A \neq L_B$ [41]. On the other hand, in order to simplify the analysis, we assume that Bob and Charlie are equidistant from David $L_B = L_C$. The QCC and QSS schemes are analyzed independently.

A. Quantum cryptographic conference

We examine Eve's symmetric attack on the channels between Bob and Charlie, which prevents Alice from

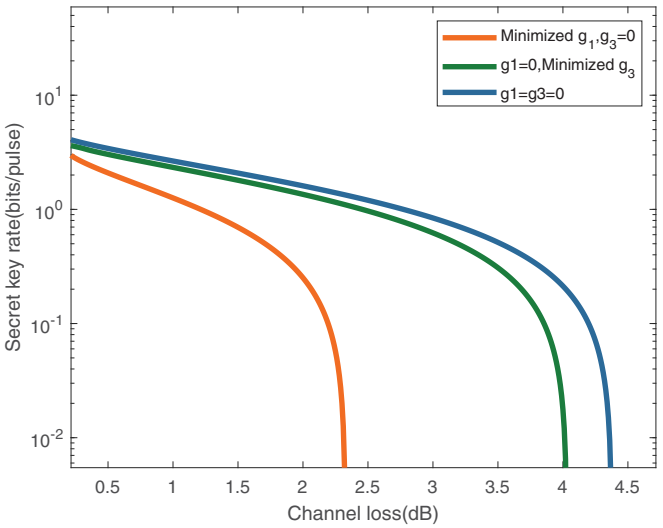

FIG. 6. The relationship between the key rate K and the transmittance η under varying noise correlations.

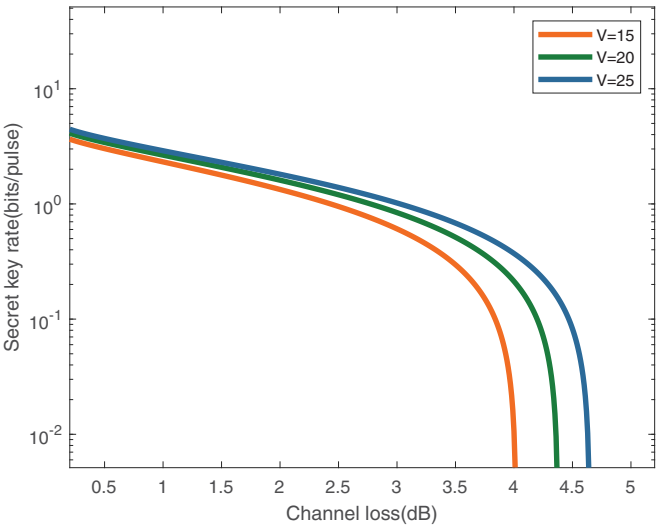

FIG. 7. The relationship between key rate K and transmittance η under different TMSS variances V.

establishing secure communication with either party, necessitating the fulfillment of conditions $V_{E_B} = V_{E_C}$ and $g_1 = g_2$. To maximize the attack while minimizing the key rate, Eve must increase the negative correlation of noise in each channel as much as possible. In Fig. 6, we analyze two types of entanglement attacks that maximize their effectiveness: one where g_1 is minimized and g_3 is set to 0 (orange line), and another where g_1 is set to 0 and g_3 is minimized (green line). The other parameters are set as follows: $\Delta\eta = 0.05$, $V_{E_C} = 1.02$, $V = 20$, $L_B = L_C = 0.3$, and $\beta = 0.98$. Compared to the independent attack with $g_1 = g_3 = 0$ (blue line), the entanglement attacks demonstrate greater aggressiveness, with the attack where g_1 is minimized and g_3 is set to 0 showing the best results. Also, it is not hard to find that the secret key rate can exceed 1 when the channel loss is low. Different from discrete variable quantum communication protocols, the key rate of continuous variable quantum key distribution protocols can exceed 1 due to the advantage of Gaussian modulation. This is also one of the merits of CV QKD.

For MDI CV-QKD via fast-fading channel, we assume that Eve employs the aforementioned independent attack. As the variance V of Alice's (Bob's, Charlie's) initial two-mode squeezed state increases, improved modulation leads to higher key rates. In Fig. 7, we illustrate the key rates for $V = 15$ (orange line), $V = 20$ (green line), and $V = 25$ (blue line), with the following parameters set: $\Delta\eta = 0.05$, $V_{E_C} = 1.02$, $L_B = L_C = 0.3$ km, and $\beta = 0.98$. In fact, Alice, Bob, and Charlie may all experience interference in fast-fading channel. Assuming that the channels used by all three follow the same fading distribution, denoted as $\eta^{\max}_{A(B,C)} = \eta^{\min}_{A(B,C)} + \Delta\eta$, Fig. 8 illustrates the key rate curves for varying numbers of interfered users. The orange line represents one user (Alice) experiencing interference, the green line indicates two users (Alice and Bob), and the blue line shows all three users affected simultaneously. The other parameters are held constant at $\Delta\eta = 0.05$, $V_{E_A} = V_{E_B} = V_{E_C} = 1.02$, $V = 20$, $\beta = 0.98$, and $g_1 = g_2 = g_3 = 0$. Interference experienced by each user results in a further decline in the key rate.

B. Quantum secret sharing

We also consider a symmetric scenario similar to the QCC scheme, where Eve simultaneously attacks the channels of Alice and Bob, satisfying the conditions $V_{E_A} = V_{E_B}$ and $g_2 = g_3$. We proceed to analyze the impact of other variables on communication. As the variance of the thermal noise injected by Eve increases, the effect on the communicators intensifies, leading to a decrease in the key rate. Other parameters are set to $\Delta\eta = 0.05$, $g_1 = 0$, $g_2 = -\sqrt{\frac{V_{E_C}^2 - 1}{2}}$, $V = 10$, and $L_B = L_C = 0.3$ km, $\beta = 0.98$. The results are illustrated for $V_{E_C} = 1.9$ (yellow line), $V_{E_C} = 2$ (purple line), and $V_{E_C} = 2.1$ (red line) in Fig. 9.

Via fast-fading channel, an important metric is the probability distribution of transmittance changes $\Delta\eta$. Greater fluctuations in the channel in more significant losses for honest users. Figure 10 illustrates the impact of different

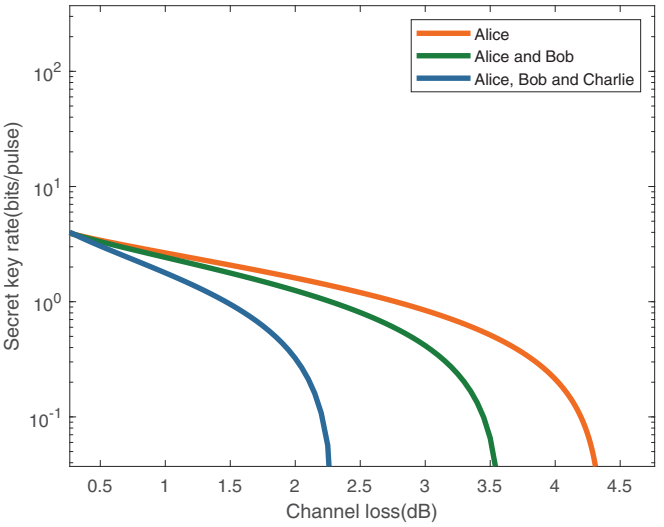

FIG. 8. The impact of the number of users affected by interference on the key rate K.

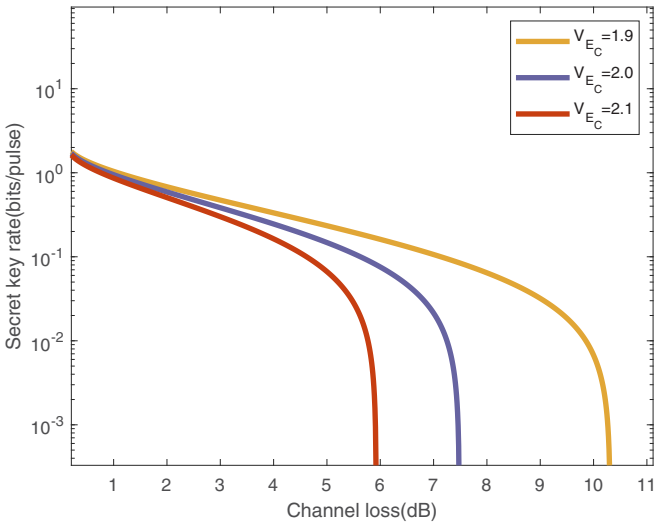

FIG. 9. The impact of different thermal noise variances V_{E_C} on the relationship between key rate K and transmittance η.

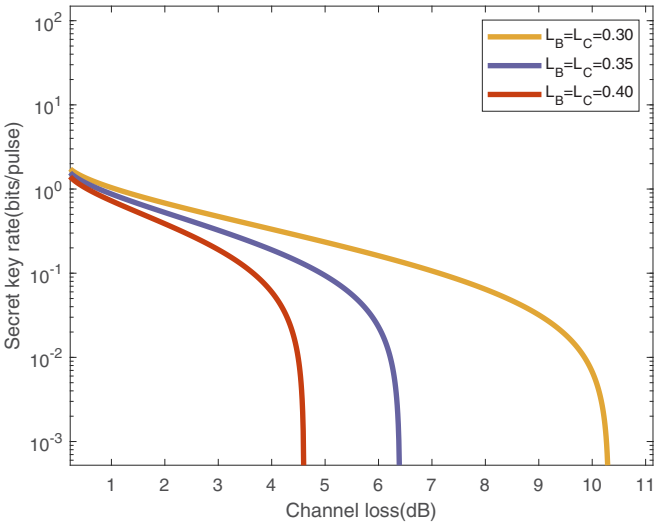

FIG. 11. Connection between transmission distance L and key rate K.

probability distribution of transmittance changes $\Delta\eta$ on the key rate, for $\Delta\eta = 0.05$ (yellow line), $\Delta\eta = 0.10$ (purple line), $\Delta\eta = 0.15$ (red line), and $\Delta\eta = 0.20$ (green line). The other parameters are set as follows: $g_1 = 0$, $g_2 = -\sqrt{\frac{V_{E_C}^2 - 1}{2}}$, $V = 10$, $L_B = L_C = 0.3$ km, $\beta = 0.98$, and $V_{E_C} = 1.9$. As $\Delta\eta$ increases, the intensified channel fluctuations lead to a rapid decrease in the key rate.

In symmetric attacks, the use of reverse reconciliation, to achieve a comparable key rate, Alice must reduce her secure transmission distance as Bob and Charlie move farther away from David (i.e., as L_B and L_C increase). This adjustment increases the transmittance, allowing Eve to obtain less information from Alice's measurement data. Figure 11 illustrates the scenarios for $L_B = L_C = 0.30$ km (yellow line), $L_B = L_C = 0.35$ km (purple line), and $L_B = L_C = 0.40$ km (red line), with the following parameters set: $\Delta\eta = 0.05$, $g_1 = 0$, $g_2 = -\sqrt{\frac{V_{E_C}^2 - 1}{2}}$, $V = 10$, $\beta = 0.98$, and $V_{E_C} = 1.9$.

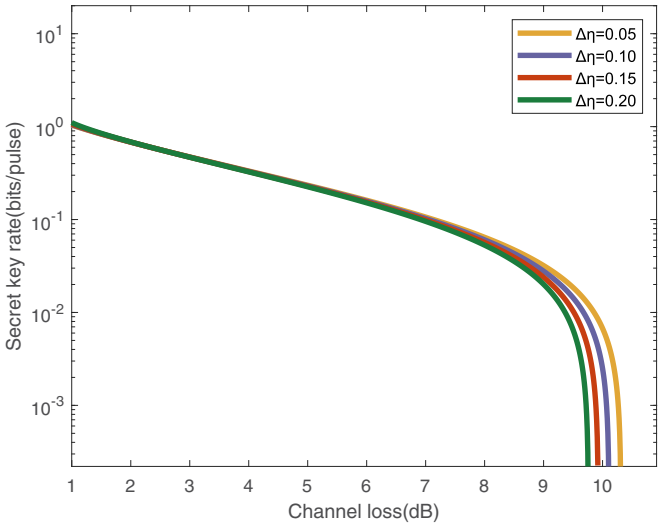

FIG. 10. The relationship between the probability distribution of transmittance changes $\Delta\eta$ and the key rate K.

VI. CONCLUSION

This work investigates the implementation of measurement-device-independent multiparty quantum communication using CV GHZ states via fast-fading channel. In such channels, the transmittance fluctuates due to various complex factors, including atmospheric absorption and geometric losses. We specifically consider a worst-case scenario in which an eavesdropper fully controls the fast-fading channel, with the transmittance randomly varying within a certain range. We demonstrate that the postselection scheme can serve as a reasonable estimation model for the channel under appropriate conditions, making it a viable subject for research in free space. Additionally, we eliminate detector-side attack interference and optimize under the worst channel conditions, proving that both the quantum cryptographic conference scheme and the quantum secret sharing scheme can withstand attacks from untrusted parties in adverse propagation environments, thereby maintaining robustness.

It is worth pointing out that the proposed multipartite quantum communication protocol is based on CV GHZ states. For the QSS scheme, (2, 3) QSS can be supported. Further, the GHZ-state QSS only support (n-1, n) threshold QSS when scaling to more users. For the implementation of arbitrary (k, n) threshold QSS, cluster state-based CV-QSS is a possible solution, which needs further study. The differences among the GHZ-states QSS, coherent-state-based QSS, and cluster-state based QSS is given. For coherent-state-based CV-QSS, it can be regarded as two or more continuous variable quantum key distribution protocols. In the GHZ state, each pair of particles is entangled. For cluster-state-based CV-QSS, the three-particle GHZ state is in accordance with cluster state as only one arrangement mode exists. For the cases of more than three modes, cluster states have more arrange modes. As to whether they can implement QSS, further study is needed.

ACKNOWLEDGMENTS

The research was funded by the National Natural Science Foundation of China Grants No. 62075129 and No. 62272483, the Science Fund for Distinguished Young Scholars of Hunan Province Grant No. 2023JJ10078, the Outstanding Youth Program of Education Department of Hunan Province Grant No. 22B0267, the Open Project Program of the SJTU-Pinghu Institute of Intelligent Optoelectronics Grant No. 2022SPIOE204.

[1] N. Gisin and R. Thew, Quantum communication, Nat. Photon. **1**, 165 (2007).

[2] S. L. Braunstein and P. van Loock, Quantum information with continuous variables, Rev. Mod. Phys. **77**, 513 (2005).

[3] F. Xu, X. Ma, Q. Zhang, H.-K. Lo, and J.-W. Pan, Secure quantum key distribution with realistic devices, Rev. Mod. Phys. **92**, 025002 (2020).

[4] R. Wolf, Quantum key distribution, Lect. Notes Phys. **988**, 1 (2021).

[5] S. K. Joshi, D. Aktas, S. Wengerowsky, M. Lončarić, S. P. Neumann, B. Liu, T. Scheidl, G. C. Lorenzo, Ž. Samec, L. Kling *et al.*, A trusted node–free eight-user metropolitan quantum communication network, Sci. Adv. **6**, eaba0959 (2020).

[6] M. Hillery, V. Bužek, and A. Berthiaume, Quantum secret sharing, Phys. Rev. A **59**, 1829 (1999).

[7] S. Bose, V. Vedral, and P. L. Knight, Multiparticle generalization of entanglement swapping, Phys. Rev. A **57**, 822 (1998).

[8] Y. Tian, P. Wang, J. Liu, S. Du, W. Liu, Z. Lu, X. Wang, and Y. Li, Experimental demonstration of continuous-variable measurement-device-independent quantum key distribution over optical fiber, Optica **9**, 492 (2022).

[9] G.-J. Fan-Yuan, F.-Y. Lu, S. Wang, Z.-Q. Yin, D.-Y. He, Z. Zhou, J. Teng, W. Chen, G.-C. Guo, and Z.-F. Han, Measurement-device-independent quantum key distribution for nonstandalone networks, Photon. Res. **9**, 1881 (2021).

[10] J. Li, W. Wang, and H.-K. Lo, Fully passive measurement-device-independent quantum key distribution, Phys. Rev. Appl. **21**, 064056 (2024).

[11] H. Liu, W. Wang, K. Wei, X.-T. Fang, L. Li, N.-L. Liu, H. Liang, S.-J. Zhang, W. Zhang, H. Li *et al.*, Experimental demonstration of high-rate measurement-device-independent quantum key distribution over asymmetric channels, Phys. Rev. Lett. **122**, 160501 (2019).

[12] Y. Wu, J. Zhou, X. Gong, Y. Guo, Z.-M. Zhang, and G. He, Continuous-variable measurement-device-independent multipartite quantum communication, Phys. Rev. A **93**, 022325 (2016).

[13] Y. Qin, J. Ma, D. Zhao, J. Cheng, Z. Yan, and X. Jia, Continuous variable quantum conference network with a Greenberger–Horne–Zeilinger entangled state, Photon. Res. **11**, 533 (2023).

[14] M. S. Alam, F. A. Wudarski, M. J. Reagor, J. Sud, S. Grabbe, Z. Wang, M. Hodson, P. A. Lott, E. G. Rieffel, and D. Venturelli, Practical verification of quantum properties in quantum-approximate-optimization runs, Phys. Rev. Appl. **17**, 024026 (2022).

[15] M. Ghalaii and S. Pirandola, Quantum communications in a moderate-to-strong turbulent space, Commun. Phys. **5**, 38 (2022).

[16] B. J. Rollick, G. Siopsis, and B. Qi, Dynamic attenuation scheme in measurement-device-independent quantum key distribution over turbulent channels, Phys. Rev. A **106**, 032405 (2022).

[17] Y. Cao, Y.-H. Li, K.-X. Yang, Y.-F. Jiang, S.-L. Li, X.-L. Hu, M. Abulizi, C.-L. Li, W. Zhang, Q.-C. Sun *et al.*, Long-distance free-space measurement-device-independent quantum key distribution, Phys. Rev. Lett. **125**, 260503 (2020).

[18] M. Proietti, J. Ho, F. Grasselli, P. Barrow, M. Malik, and A. Fedrizzi, Experimental quantum conference key agreement, Sci. Adv. **7**, eabe0395 (2021).

[19] S. Liu, Z. Lu, and Y. Wang, X. Li, Experimental demonstration of multiparty quantum secret sharing and conference key agreement, npj Quantum Inf. **9**, 92 (2023).

[20] Q. Liao, H. Liu, L. Zhu, and Y. Guo, Quantum secret sharing using discretely modulated coherent states, Phys. Rev. A **103**, 032410 (2021).

[21] M. Ioannou, P. Sekatski, A. A. Abbott, D. Rosset, J.-D. Bancal, and N. Brunner, Receiver-device-independent quantum key distribution protocols, New J. Phys. **24**, 063006 (2022).

[22] Y.-H. Zhou, S.-F. Qin, W.-M. Shi, and Y.-G. Yang, Measurement-device-independent continuous variable semi-quantum key distribution protocol, Quantum Info. Proc. **21**, 303 (2022).

[23] X.-Q. Jiang, P. Huang, D. Huang, D. Lin, and G. Zeng, Secret information reconciliation based on punctured low-density parity-check codes for continuous-variable quantum key distribution, Phys. Rev. A **95**, 022318 (2017).

[24] P. van Loock and A. Furusawa, Detecting genuine multipartite continuous-variable entanglement, Phys. Rev. A **67**, 052315 (2003).

[25] S.-K. Liao, W.-Q. Cai, W.-Y. Liu, L. Zhang, Y. Li, J.-G. Ren, J. Yin, Q. Shen, Y. Cao, Z.-P. Li *et al.*, Satellite-to-ground quantum key distribution, Nature (London) **549**, 43 (2017).

[26] V. C. Usenko, B. Heim, C. Peuntinger, C. Wittmann, C. Marquardt, G. Leuchs, and R. Filip, Entanglement of Gaussian states and the applicability to quantum key distribution over fading channels, New J. Phys. **14**, 093048 (2012).

[27] J. Zhou and Y. Guo, Continuous-variable measurement-device-independent multipartite quantum communication using coherent states, J. Phys. Soc. Jpn. **86**, 024003 (2017).

[28] F. R. Cardoso, D. Z. Rossatto, G. P. L. M. Fernandes, G. Higgins, and C. J. Villas-Boas, Superposition of two-mode squeezed states for quantum information processing and quantum sensing, Phys. Rev. A **103**, 062405 (2021).

[29] P. Papanastasiou, C. Weedbrook, and S. Pirandola, Continuous-variable quantum key distribution in uniform fast-fading channels, Phys. Rev. A **97**, 032311 (2018).

[30] M. Żukowski, A. Zeilinger, and M. A. Horne, Realizable higher-dimensional two-particle entanglements via multiport beam splitters, Phys. Rev. A **55**, 2564 (1997).

[31] J. Eisert, S. Scheel, and M. B. Plenio, Distilling Gaussian states with Gaussian operations is impossible, Phys. Rev. Lett. **89**, 137903 (2002).

[32] C. Weedbrook, S. Pirandola, R. García-Patrón, N. J. Cerf, T. C. Ralph, J. H. Shapiro, and S. Lloyd, Gaussian quantum information, Rev. Mod. Phys. **84**, 621 (2012).

[33] G. Adesso, D. Girolami, and A. Serafini, Measuring Gaussian quantum information and correlations using the Rényi entropy of order 2, Phys. Rev. Lett. **109**, 190502 (2012).

[34] Y. Feng, R. Qiu, K. Zhang, X.-Q. Jiang, M. Zhang, P. Huang, and G. Zeng, Secret key rate of continuous-variable quantum key distribution with finite codeword length, Sci. China Inf. Sci. **66**, 180511 (2023).

[35] R. Zhao, J. Zhou, R. Shi, and J. Shi, Unidimensional continuous variable quantum key distribution via fast-fading channel, Ann. Phys. (NY) **536**, 2300401 (2024).

[36] Y. Feng, Y.-J. Wang, R. Qiu, K. Zhang, H. Ge, Z. Shan, and X.-Q. Jiang, Virtual channel of multidimensional reconciliation in a continuous-variable quantum key distribution, Phys. Rev. A **103**, 032603 (2021).

[37] O. Fawzi, R. Kueng, D. Markham, and A. Oufkir, Learning properties of quantum states without the IID assumption, Nat. Commun. **15**, 9677 (2024).

[38] A. Leverrier, Security of continuous-variable quantum key distribution via a Gaussian de Finetti reduction, Phys. Rev. Lett. **118**, 200501 (2017).

[39] R. Renner, Security of quantum key distribution, Int. J. Quantum Inf. **6**, 1 (2008).

[40] Y.-C. Zhang, Z. Li, S. Yu, W. Gu, X. Peng, and H. Guo, Continuous-variable measurement-device-independent quantum key distribution using squeezed states, Phys. Rev. A **90**, 052325 (2014).

[41] D. Pan, S. X. Ng, D. Ruan, L. Yin, G. Long, and L. Hanzo, Simultaneous two-way classical communication and measurement-device-independent quantum key distribution with coherent states, Phys. Rev. A **101**, 012343 (2020).