Received 21 March 2023; revised 17 August 2023; accepted 28 September 2023; date of publication 9 October 2023;
date of current version 6 November 2023.

Digital Object Identifier 10.1109/TQE.2023.3322171

Continuous-Variable Quantum Secret Sharing in Fast-Fluctuating Channels

FANGLI YANG[1,2], DAOWEN QIU[1,2,3,4], AND PAULO MATEUS[4]

[1]Institute of Quantum Computing and Computer Theory, School of Computer Science and Engineering, Sun Yat-sen University, Guangzhou 510006, China
[2]The Guangdong Key Laboratory of Information Security Technology, Sun Yat-sen University, Guangzhou 510006, China
[3]QUDOOR Technologies Inc., Guangzhou 510006, China
[4]Instituto de Telecomunicações, Departamento de Matemática, Instituto Superior Técnico, 1049-001 Lisbon, Portugal

Corresponding author: Daowen Qiu (e-mail: issqdw@mail.sysu.edu.cn).

This work was supported in part by the National Natural Science Foundation of China under Grant 61876195 and Grant 61572532 and in part by Fundação para a Ciência e Tecnologia, Instituto de Telecomunicações Research Unit under Grant UIDB/50008/2020 and Grant UIDP/50008/2020.

ABSTRACT Recently, several continuous-variable quantum secret sharing (CV-QSS) protocols were proposed, while most of them are limited to the fiber channel systems with a relatively stable transmissivity. However, by means of complex channels, the transmissivity fluctuates dramatically in time with a probability distribution, which will lead to a fast-fluctuating attack. Therefore, the security analysis of CV-QSS in fiber channels may not apply to CV-QSS in complex channels. In this article, we study the CV-QSS protocol in the absence of uniform fast-fluctuating channels whose transmissivity changes with respect to a uniform probability distribution. We give a lower bound of secret key rate to provide security analysis against the fast-fluctuating attack for the CV-QSS protocol. In particular, the realistic highly asymmetric beam splitter (HABS) in CV-QSS protocol is investigated in detail here for the first time, and numerical simulation shows that the security bound is overestimated when the HABS is treated as the perfect device.

INDEX TERMS Continuous-variable (CV), quantum key distribution, quantum secret sharing (QSS).

I. INTRODUCTION

Quantum key distribution (QKD) [1], [2] is the most important part of quantum cryptography communication. It can distribute a secret key between two legitimate parties, Alice and Bob, over an insecure quantum channel eavesdropped by a third party (Eve). QKD using the continuous-variable (CV) quantum system was first introduced by Ralph [3]. In [4], Cerf, Levy, and Assche proposed a squeezed state protocol using Gaussian modulation. On this basis, Grosshans and Grangier [5] proposed the famous GG02 CV-QKD protocol, in which Alice prepared the coherent states of Gaussian modulation. The protocol showed that the CV-QKD may have a better compatibility with optical communication networks in comparison to DV-QKD, due to the utilization of coherent states and the balanced homodyne detector. Since then, efforts have been made to improve the CV-QKD system, such as two-way communication [6], measurement device independence [7] and free-space quantum channels [8].

With the rapid development of the communication network, the point-to-point CV-QKD may hardly meet the requirements of a multiple-party network. In 2019, Grice et al. [9] extended the point-to-point CV-QKD protocol to a multiparty secret key distribution protocol, called continuous-variable qauntum secret sharing (CV-QSS). Generally, secret sharing refers to the (k, n) threshold scheme [10], [11], which has important application in E-Business, banking business, and politics. Namely, the dealer encrypts the message into n parts to n participants, respectively. The condition for decoding this secret message is that at least $k \leq n$ participants have to work together. Because it is difficult to study the (k, n) quantum threshold scheme, and the general results have been given in the literature [12], the current research on QSS mainly focuses on the (n, n) scheme. In a QSS based on the (n, n)-threshold scheme, the dealer first generates an independent secure key K_i ($i = 1, 2, \ldots, n$) with each participant where the length of each key is the same as that of the message, then obtains a new key $K = K_1 \oplus K_2 \oplus \cdots \oplus K_n$ to encode message M resulting in encrypted message $E = K \oplus M$, where $\oplus$ is addition modulo 2. If participants want to decode message M from E, all participants have to work together. The CV-QSS studied in [9] is based on coherent states and heterodyne detector. In this CV-QSS, each participant injects a locally prepared coherent state into a circulating optical mode using a highly asymmetric beam splitter (HABS). Since the quantum state preparation process is independent of the eavesdropper, the scheme is resilient to Trojan horse attacks. Ref. [13] proposed a CV-QSS by using a thermal source and achieved a tighter bound of QSS distance under the finite-size effect. The authors in [14] showed a CV-QSS by using discrete modulated coherent states that are easy to be prepared and resilient to losses. However, these contributions usually consider the protocols under the fiber channels, and the impact of HABS on security analysis is not discussed in detail.

The practical implementation of CV-QKD in the fiber channel is still restricted by the limitations of the birefringence effect and the inherent losses. In fact, these limitations will also have negative impact on the actual implementation of CV-QSS with the fiber channel. An alternative channel model for quantum cryptography is the fast-fluctuating channel, such as the free-space channel, in which there is virtually nonexistent birefringence effect, thus it may preserve nonclassical effects. In such type of channel, the transmissivity T fluctuates rapidly according to some probability distribution. This fast fluctuation will make the honest users suffer a fast-fluctuating attack [15], where the eavesdropper is able to control the channel fluctuating process, but the users can only access the probability distribution of fluctuating at the end of the quantum communication.

In this article, we establish a security analysis for CV-QSS under fast-fluctuating attack, by proving the lower bound of key rate. Here, we discuss the most random channel model where the transmissivity is uniformly distributed over some interval. This type of channel was first studied in CV-QKD system by Papanastasiou et al. [15], who have shown that the CV-QKD protocol can still achieve high rates within reasonable parameters associated with the probability distribution, even if the eavesdropper controls the channel fluctuating process.

The rest of this article is organized as follows. In Section II, we describe the CV-QSS under fast-fluctuating channel in detail. In Section III, we analyze the security of the CV-QSS protocol against collaborating attack and fast-fluctuating attack. In Section IV, we discuss the secret key rates of CV-QSS protocol under fast-fluctuating channel by simulations and comparisons. Finally, Section V concludes the article.

II. CV-QSS IN FAST-FLUCTUATING CHANNEL

We propose the QSS protocol using the fast-fluctuating channels. The structure of the protocol is shown in Fig. 1(a), where a dealer is connected to n participants called as $U_1, U_2, \ldots, U_n$ through the fast-fluctuating channel. The procedure of the protocol is detailed as follows.

- *Step 1:* The participant U_1 prepares a Gaussian modulated coherent state centered on $\mathbf{x_1} = (q_1, p_1)$ in phase space. Then, she sends the state to his nearest neighbor participant U_2 through a fluctuating channel.
- *Step 2:* Using a telescope, each participant U_j ($j = 2, \ldots, n$) collects the signal from the previous participant, adds its locally coherent state centered on $\mathbf{x_j} = (q_j, p_j)$ with the HABS of transmissivity T_H, and then send it to the following participant, where q_j and p_j are random real numbers according to the independent Gaussian distributions of variance V_A.
- *Step 3:* The dealer uses a telescope to collect the signal (including n participants' Gaussian information) and measures it by performing heterodyne detector. The measurement results $\{q_B, p_B\}$ are kept as raw data.
- *Step 4:* Repeat the above steps N ($N > 2n$) times to generate a set of raw data $A_N = \{\{q_{B_1}, p_{B_1}\}, \ldots, \{q_{B_i}, p_{B_i}\}, \ldots, \{q_{B_N}, p_{B_N}\}\}$, where subscript i indicates the ith repetition.
- *Step 5:* The dealer randomly selects n pairs from A_N, i.e., a subset $B_n = \{\{q_{B_{h(1)}}, p_{B_{h(1)}}\}, \ldots, \{q_{B_{h(m)}}, p_{B_{h(m)}}\}, \ldots, \{q_{B_{h(n)}}, p_{B_{h(n)}}\}\}$ of A_N, where $h(m) \in [1, N]$. The dealer requests all the participants to announce their corresponding Gaussian random numbers. This step is to estimate the n channel transmissivities $\{T_1, T_2, \ldots, T_n\}$ between participants and the dealer. Note that all the participants discard the disclosed data.
- *Step 6:* The participant U_j is considered to be honest and all the other participants are considered to be dishonest.
- *Step 7:* The dealer randomly picks a pair $\{q_{B_i}, p_{B_i}\}$ of remaining raw dataset A_N/B_n and requests all the participants except U_j to announce their corresponding random numbers. Using the announced data and $\{T_1, T_2, \ldots, T_n\}$, the dealer can calculate the pair $\{q'_{i_j}, p'_{i_j}\}$. From $\{q'_{i_j}, p'_{i_j}\}$ and U_j's raw data $\{q_{i_j}, p_{i_j}\}$, we can estimate a lower bound of secure key rate R_j of two-party QKD between the dealer and the participant U_j in fast-fluctuating channel. Similarly, all the disclosed data should be discarded.
- *Step 8:* Steps 6–7 are repeated n times to establish the n secure QKD between the dealer and each participant, resulting in n key rates $\{R_1, R_2, \ldots, R_n\}$. In each run, a different participant is picked as the honest one.
- *Step 9:* For security requirements, the minimum one of n key rates in step 8 should be determined as the final secret key rate R^f of the CV-QSS, i.e., $R^f = \min\{R_1, R_2, \ldots, R_n\}$. By using the standard CV-QKD protocol [16], the dealer shares the corresponding security key K_j with each participant U_j from the remaining undisclosed data, where $j = 1, \ldots, n$.
- *Step 10:* Finally, the dealer generates a new key $K = K_1 \oplus K_2 \oplus \cdots \oplus K_n$ and encrypts the message M via $E = M \oplus K$.

In the procedure, steps 1–4 are in the quantum stage which involves quantum states and quantum operations, and the remaining steps belong to the classical postprocessing stage.

In step 7, the participant U_j and the dealer actually establish a point-to-point CV-QKD depicted in Fig. 1(b), where them can be regarded as trusted parties Alice and Bob. The

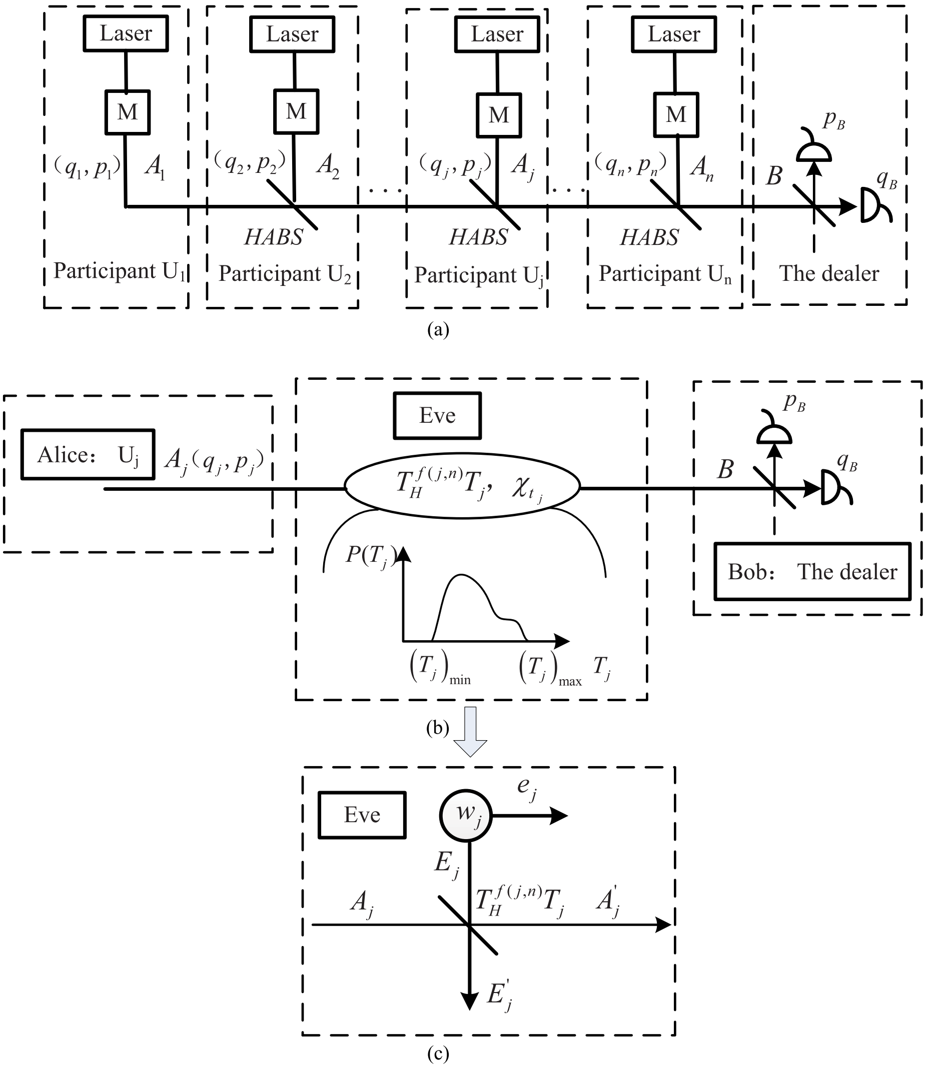

FIGURE 1. **(a) CV-QSS protocol under fast-fluctuating channels with n participants and a dealer. (b) The point-to-point QKD between the participant U_j (Alice) and the dealer (Bob). (c) The equivalent channel (controlled by Eve) using a BS with transmissivity $T_{e_j} = T_H^{f(j,n)} T_j$ and a TMSV state (described by modes E_j and e_j) of variance w_j.**

locally coherent state prepared by U_j is described as mode A_j. The channel in this CV-QKD can be characterized by the equivalent transmissivity $T_{e_j} = T_H^{f(j,n)} T_j$, where

$$f(j,n) = \begin{cases} n-j, & j=1 \quad (1) \\ n-j+1, & j=2,\ldots,n \quad (2) \end{cases}$$

and the total noise χ_{t_j}, where T_j represents the random fast-fluctuating channel transmissivity, which is in probability $P(T_j)$ within a range of $[(T_j)_{\min}, (T_j)_{\max}]$.

For each use of the channel, Eve prepares a two-mode squeezed vacuum (TMSV) state (described by modes E_j and e_j) of variance w_j. Then, modes E_j and A_j are fed into a beam splitter (BS) with transmissivity T_{e_j}. The output mode e_j' is stored in a quantum memory, and the other mode A_j' transmitted to the dealer is given by $A_j' = \sqrt{T_{e_j}} A_j + \sqrt{1-T_{e_j}} E_j$, where E_j centered on $\mathbf{x_{E_j}} = (0,0)$. The detailed process is shown in Fig. 1(c).

Since each A_j prepared by U_j will go through the above process, the central position of mode B that the dealer gets in phase space can be described by

$$\mathbf{x_B} = \sum_{j=1}^{n} \left[\sqrt{T_{ej}} \mathbf{x_j} + \sqrt{1 - T_{ej} T_j} \mathbf{x_{E_j}} \right]$$
$$= \sum_{j=1}^{n} \sqrt{T_H^{f(j,n)} T_j} \mathbf{x_j}. \tag{3}$$

In other words, the quantum state that arrives at the dealer can be described by $|q_B + i p_B\rangle$, where

$$q_B = \sqrt{T_H^{n-1} T_1} q_1 + \sum_{j=2}^{n} \sqrt{T_H^{n-j+1} T_j} q_j \tag{4}$$

and

$$p_B = \sqrt{T_H^{n-1} T_1} p_1 + \sum_{j=2}^{n} \sqrt{T_H^{n-j+1} T_j} p_j. \tag{5}$$

III. SECURITY ANALYSIS OF THE CV-QSS PROTOCOL

In this section, we first briefly analyze the security of CV-QSS protocol against collaborating attack, which is an attack strategy implemented by multiparty cooperation.

Note that in steps 6–7 of the CV-QSS protocol, the participant U_j and the dealer can be regarded as trusted parties (Alice and Bob) of a point-to-point CV-QKD, where the collaborating attacks come from eavesdroppers including the $n-1$ dishonest participants and potential eavesdroppers in the channel. This indicates the security proof for CV-QKD in fast-fluctuating channel can be used to evaluate the security key rate R_j. By implementing step 8, the dealer establishes n secure QKD links and obtains n secure key rates. The smallest one will be used as the secure key rate for QSS to ensure that the key remains secure against the collaborating attacks.

Then, let us focus on the discussion of the security against the fast-fluctuating attack by proving a lower bound of the secret key rate.

As mentioned above, when we assume participant U_j is honest and all the other $n-1$ participants are dishonest, the CV-QSS protocol is equivalent to a point-to-point CV-QKD, where the participant U_j and the dealer can be regarded as two trusted parties Alice and Bob, respectively. Under this circumstance, the security proof of the CV-QKD against the fast-fluctuating attack can be applied to the CV-QSS protocol. In this section, by means of [16] and [17], we first have Lemma 1 concerning the lower bound of the key rate of the CV-QKD protocol based on Gaussian modulation of Gaussian states.

Lemma 1 [16], [17]: Let a CV-QKD protocol based on Gaussian modulation of coherent states, use a lossy and noise channel, with channel transmissivity T and the excess noise ε. Let Alice and Bob perform reverse reconciliation. Then, the secret key rate of the CV-QKD is lower-bounded by

$$R_{qkd}(T, \varepsilon) = \eta I_{AB}(T, \varepsilon) - \chi_{B:E}(T, \varepsilon) \tag{6}$$

where $I_{A:B}(T, \varepsilon)$ is the Shannon mutual information between Alice and Bob, and $\chi_{B:E}(T, \varepsilon)$ is the Holevo bound, which is the maximum information that Eve can obtain based on Bob's variable, $\eta \in [0, 1]$ is the reconciliation parameter.

The (1) of [15] describes a lower bound of the secret key rate for the CV-QKD in the fast-fluctuating channels, on which we show and prove Lemma 2.

Lemma 2 [15]: Let a reverse reconciliation CV-QKD protocol based on Gaussian modulation of coherent states, suffers a fast-fluctuating attack where Eve completely controls the whole channel fluctuating process with a probability density distribution $P(T)$ of transmissivity $T \in [T_{\min}, T_{\max}]$, with an excess noise ε. Then, the secret key rate of the CV-QKD in the fast-fluctuating channel is lower-bounded by

$$R^f_{qkd}(T, \varepsilon) = \eta I_{AB}(T_{\min}, \varepsilon) - \int_{T_{\min}}^{T_{\max}} d_T P(T) \chi_{B:E}(T, \varepsilon). \tag{7}$$

Proof: When Eve performs the fast-fluctuating attack, she will completely control the whole channel fluctuating process described by a probability density distribution $P(T)$ of transmissivity $T \in [T_{\min}, T_{\max}]$. In other words, she may control instantaneous values of the transmissivity for each use of the channel. Therefore, the information that Eve can obtain on Bob's variable is given by the averaged Holevo bound $\int_{T_{\min}}^{T_{\max}} d_T P(T) \chi_{B:E}(T, \varepsilon)$. For Alice and Bob, this transmissivity is changed too rapidly to estimate its instantaneous value at each transmission. More specifically, Alice and Bob can only access the probability distribution of fluctuating at the end of the quantum communication. Assume the value of the transmissivity that Alice and Bob can access is $T \in [T_{\min}, T_{\max}]$. Using Lemma 1, the lower-bounded secret key rate is written as

$$R^{f_0}_{qkd}(T, \varepsilon) = \eta I_{AB}(T, \varepsilon) - \int_{T_{\min}}^{T_{\max}} d_T P(T) \chi_{\alpha E}(T, \varepsilon) \tag{8}$$

where

$$I_{AB}(T, \varepsilon) = \log_2 \frac{V + \chi_t(T)}{1 + \chi_t(T)} = \log_2 \left(\frac{V - 1}{1 + \chi_t(T)} + 1 \right) \tag{9}$$

and

$$\chi_t(T, \varepsilon) = \frac{1 + \chi_h}{T} + \varepsilon - 1. \tag{10}$$

The noise χ_h caused by Bob's detection is a constant independent of the channel transmissivity T. As for the excess noise ε, it is a given constant or a parameter satisfying $\varepsilon = \frac{(w-1)(1-T)}{T}$ in CV-QKD systems, where w is the thermal noise. Then, it is clear that the lower bound of the mutual information between Alice and Bob is $I_{A:B}(T_{\min}, \varepsilon)$. For all $T \in [T_{\min}, T_{\max}]$, there is

$$R^{f_0}_{qkd}(T, \varepsilon) = \eta I_{AB}(T, \varepsilon) - \int_{T_{\min}}^{T_{\max}} d_T P(T) \chi_{\alpha E}(T, \varepsilon) \geq$$
$$R^f_{qkd}(T, \varepsilon) = \eta I_{AB}(T_{\min}, \varepsilon) - \int_{T_{\min}}^{T_{\max}} d_T P(T) \chi_{\alpha E}(T, \varepsilon). \tag{11}$$

So, we complete the proof. □

Lapidoth and Shamai [18] studied the robustness of the communication scheme under fading channels. Dequal et al. [19] showed the feasibility of establishing secret keys in a satellite-to-ground fading channel using continuous-variable encoding. In both references, the mean value is used for estimating the amount of mutual information I_{AB}. In this article, we consider the other extreme case where the system is subject to a fast-fluctuating attack, where Alice and Bob can only access the transmissivity at the end of the communication, thus they treat this value as the constant transmissivity for the whole communication process. Therefore, the mutual information corresponding to this transmissivity is used in the estimation of the key rate, instead of the average value of the corresponding mutual information in the interval of $[T_{\min}, T_{\max}]$.

Furthermore, for a uniform fast-fluctuating channel, where the probability density distribution of the transmissivity is $P(T) = \frac{1}{\triangle T}$ with $\triangle T = T_{\max} - T_{\min}$, we can show that the lower bound of the key rate $R^f_{qkd}(T)$ estimated by using the mutual information corresponding to $T_{\min}$ is a tighter bound than the lower bound on the key rate $R^a_{qkd}(T)$ estimated by using the mean value of the mutual information in the interval $[T_{\min}, T_{\max}]$. In particular, this can be expressed as

$$R^f_{qkd}(T) = \eta I_{AB}(T_{\min}) - \frac{1}{\triangle T}\int_{T_{\min}}^{T_{\max}} d_T\, \chi_{\alpha E}(T) \leq$$
$$R^a_{qkd}(T) = \frac{1}{\triangle T}\int_{T_{\min}}^{T_{\max}} d_T(\eta I_{AB}(T) - \chi_{\alpha E}(T)). \quad (12)$$

Here, we give a simple proof of the (12). From (9) and (10), the mutual information $I_{AB}(T)$ is a monotonically increasing function with respect to T. Moreover, the value of $I_{AB}(T)$ is greater than zero. Combining the definition of the integral, we can obtain

$$(T_{\max} - T_{\min}) I_{AB}(T_{\min}) \leq \int_{T_{\min}}^{T_{\max}} d_T I_{AB}(T). \quad (13)$$

In turn, (12) is proved.

For the CV-QSS protocol based on Gaussian modulation of coherent states, we discuss the case that participant U_j is honest and all the other $n-1$ participants are dishonest.

Theorem 1: Let the transmissivity of each HABS be T_H, and let the thermal noise introduced by Eve in the channel between the participant U_j $(j = 1, 2, \ldots, n)$ and the dealer be $w_j = w$. Then, the lower bound of secret key rate for reverse reconciliation CV-QKD between the participant U_j $(j = 1, 2, \ldots, n)$ and the dealer under fast-fluctuating attack is given by

$$R^f_j(T_j, w) = \eta I_{U_jB}\left(T_H^{f(j,n)} (T_j)_{\min}, w\right) - \int_{(T_j)_{\min}}^{(T_j)_{\max}} d_{T_j} P(T_j)\, \chi_{\alpha E}\left(T_H^{f(j,n)} T_j, w\right). \quad (14)$$

Therefore, the lower bound of secret key rate for the CV-QSS under fast-fluctuating attack is

$$R^f(T, w) = \min\left\{R^f_1(T_1, w), R^f_2(T_2, w), \ldots, R^f_n(T_n, w)\right\}. \quad (15)$$

Proof: When the effect of the HABS is considered, the channel transmissivity between the participant U_j and the dealer is $T_{e_j} = T_H^{f(j,n)} T_j$, and the total noise becomes

$$\chi_{t_j}(T_j, w) = \frac{1 + \chi_h}{T_H^{f(j,n)} T_j} + \sum_{i=1}^{n} \varepsilon_i(T_i, w) - 1 \quad (16)$$

where $\varepsilon_j(T, w)$ denotes the equivalent excess noise introduced by jth participant, which is given by

$$\varepsilon_j(T_j, w) = \frac{[w-1][1 - T_H^{f(j,n)} T_j]}{T_H^{f(j,n)} T_j}. \quad (17)$$

Clearly, the total noise $\chi_{t_j}(T_j, w)$ is a monotonically decreasing function of T_j, so the mutual information $I_{U_jB}(T_H^{f(j,n)} T_j, w) = \log_2 \frac{V_j + \chi_{t_j}(T_j, w)}{1 + \chi_{t_j}(T_j, w)}$ is a monotonically increasing function of T_j within $[(T_j)_{\min}, (T_j)_{\max}]$. According to Lemma 2, the lower bound of secret key rate between the participant U_j and the dealer is obtained by (14). According to step 9 of the protocol, the lower bound of the key rate of CV-QSS is the minimum value among n lower bounds of key rates $\{R^f_1(T_1, w), R^f_2(T_2, w), \cdots, R^f_n(T_n, w)\}$, i.e., $R^f(T, w) = \min\{R^f_1(T_1, w), R^f_2(T_2, w), \cdots, R^f_n(T_n, w)\}$. So, the theorem is proven. □

A positive value of $R^f(T, w)$ guarantees security of the CV-QSS protocol against fast-fluctuating attack.

Similar to the previous analysis, when considering a uniformly fluctuating channel in CV-QSS, the lower bound of secret key rate $R^a_j(T_j)$ according to the mean value of the mutual information is given by

$$R^a_j(T_j) = \frac{1}{\triangle T_j}\int_{(T_j)_{\min}}^{(T_j)_{\max}} d_T \eta I_{U_j:B}(T_H^{f(j,n)} T_j) - \frac{1}{\triangle T_j}\int_{(T_j)_{\min}}^{(T_j)_{\max}} d_T\, \chi_{\alpha E}(T_H^{f(j,n)} T_j). \quad (18)$$

Since mutual information $I_{U_jB}(T_H^{f(j,n)} T_j)$ is a monotone increasing function of T_j within $[(T_j)_{\min}, (T_j)_{\max}]$, it follows that $R^f_j(T_j)$ is less than $R^a_j(T_j)$. From Theorem 1, the lower bound of the key rate for CV-QSS is the smallest key rate among n CV-QKD links established by U_j and the dealer, and thus in CV-QSS with the uniform fluctuating channel, the bound of key rate $R^f(T)$ based on the mutual information by using $T_{\min}$ is lower than the bound of key rate $R^a(T)$ by using the average mutual information. In the following numerical simulation, we also verify the conclusion.

IV. SECRET KEY RATES

In order to make the security analysis of the CV-QSS protocol under fast-fluctuating channel more complete and intuitive, in this section we will mainly carry out numerical simulation of key rate based on realistic system parameters.

We assume that the difference of the channel loss between any two adjacent participants is the same. The dealer's channel loss is zero, and U_j's channel loss is $d(j, n) = \frac{n-j+1}{n} D$, where $j = 1, \ldots, n$. Notice that the relevant parameters will be rewritten as the function of j and n to discuss the properties of the total noise in detail. The effect of HABS will be considered, and the channel transmittance is $T_e(j, n) = T_H^{f(j,n)} T(j, n)$, where $T(j, n) = 10^{-0.1 d(j,n)}$ [20]. Note that $T_e(j, n) = T(j, n)$, if we ignore the effect of HABS, i.e,

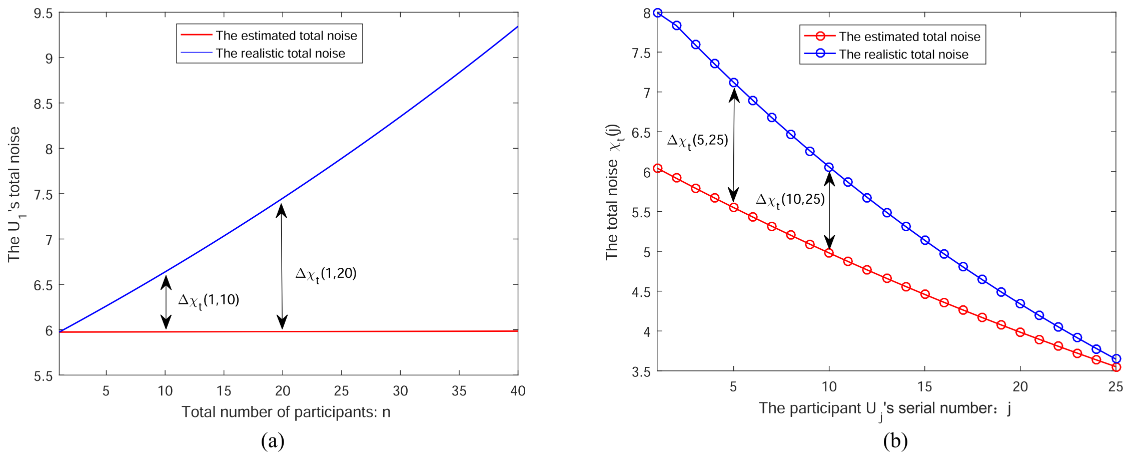

FIGURE 2. Comparisons of realistic total noise $\chi_t(j,n)$ and the estimated total noise $\tilde{\chi}_t(j,n)$ with $w = 1.001$. (a) U_1's total noises (blue line) $\chi_t(1,n)$ and (red line) $\tilde{\chi}_t(1,n)$ versus the total number of participants n. (b) U_j's total noises (blue line) $\chi_t(j,25)$ and (red line) $\tilde{\chi}_t(j,25)$ with the total number of participants $n = 25$.

$T_H = 1$. The excess noise is

$$\varepsilon(j,n) = \frac{[w-1][1-T_e(j,n)]}{T_e(j,n)}. \tag{19}$$

The total noise between the participant U_j (Alice) and the dealer (Bob) is given by

$$\chi_t(j,n) = \chi_l(j,n) + \frac{\chi_h}{T_e(j,n)} \tag{20}$$

where the channel input is written as $\chi_l(j,n) = \frac{1}{T_e(j,n)} - 1 + \sum_{i=1}^{n} \varepsilon(i,n)$, and the noise caused by Bob's heterodyne detection is $\chi_h = \frac{2-\eta_e+2v_{el}}{\eta_e}$, where the symbol η_e is the detection efficiency and v_{el} is the electronics noise of the homodyne detection.

In this article, we consider a more practical case, namely, the precise consideration of the impact of HABS on QSS protocol. Theoretically, we provide a simple theorem to describe the effect of HABS on the total noise χ_t.

Theorem 2: Assume that the size of the CV-QSS protocol is n. The channel loss of participant U_j is $d(j,n) = \frac{n-j+1}{n}D$, where $j = 1,\ldots,n$. If we take into account precisely the effects of HABS, i.e., setting $0 < T_H < 1$, then the total noise $\chi_t(j,n)$ between the participant U_j and the dealer has the following properties.

I: It is a monotonically increasing function on n.

II: It is a monotonically decreasing function on j.

III: The error between the realistic total noise $\chi_t(j,n)$ ($0 < T_H < 1$) and the estimated one $\tilde{\chi}_t(j,n)$ ($T_H = 1$), denoting as $\Delta\chi_t(j,n) = \chi_t(j,n) - \tilde{\chi}_t(j,n)$, is a monotonically increasing function on n and a monotonically decreasing function on j.

We give the mathematical proof of Theorem 2 in Appendix A. This theorem reveals that as the number of participants n increases, for each participant U_j, his total noise $\chi_t(j,n)$ and error noise $\Delta\chi_t(j,n)$ are both increased. This fact shows that with the increase of the number of participants, ignoring the influence of HABS will increase the error in terms of the noise, which will affect the secret key rate of QSS protocol. In Fig. 2(a), we visually present the first participant's realistic total noise $\chi_t(1,n)$ with $T_H = 0.99$ (blue line) and the estimated total noise $\tilde{\chi}_t(1,n)$ (red line) as the functions of the number of participants n. Obviously, the simulation results verify the conclusions of Theorem 2 about n.

TABLE 1. Default Parameters of CV-QSS in Key Rates Analysis

Symbol	Quantity	Value (The variances and noises are in shot noise units.)
η	Reconciliation parameter	0.98
η_e	The efficiency of the dealer's detector	0.5
v_{el}	The noise variance of the dealer's detector	0.1
V_A	U_j's modulation variance	1

Theorem 2 shows that for a fixed size (n fixed) QSS protocol, with the increase of serial number j, the corresponding total noise $\chi_t(j,n)$ and error noise $\Delta\chi_t(j,n)$ gradually decrease. According to this property, ignoring the influence of HABS has the most negative impact on the noise of the first participant. The reason is that the number of HABS passed by the signals prepared by U_j decreases with the increase of j, so the impact of HABS on noise is reduced. These properties of Theorem 2 are verified by numerical simulations shown in Fig. 2(b).

By analyzing the total noise $\chi_t(j,n)$, we prove that it is a monotone decreasing function on j. The conclusion reveals that the first participant U_1 experiences a stronger channel noise than any other participant in this protocol. Besides, U_1 has the maximum channel loss with the dealer. Therefore, the minimum one of n key rates between the dealer and each participant may be the secret key rate R_1^f between the first participant U_1 and the dealer. Based on the parameters in Table I, we will verify this point in the following key rate analysis.

We discuss the security of the protocol with a basic model of fluctuating channel, where the transmissivity is uniformly distributed over a interval $[T_{\min}, T_{\max}]$, i.e., the

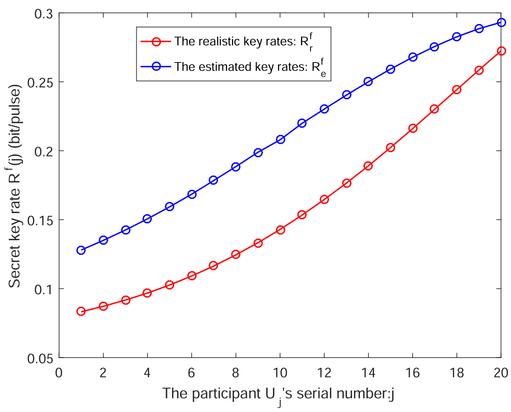

FIGURE 3. Realistic secret key rates ($0 < T_H < 1$, blue line) and the estimated key rates ($T_H = 1$, red line) shared between the participant U_j and the dealer with $n = 20$, $w = 1.001$.

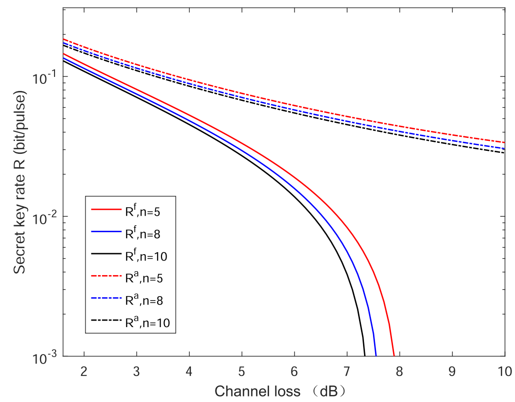

FIGURE 5. (Solid lines) Secret key rates $R^f(T)$ and (dashed lines) the secret key rates $R^a(T)$ with $w = 1.001$, and different $n = \{5, 8, 10\}$. Note that curves start from nonzero dBs, which is due to the fact that the fading channels must satisfy $T_{\min} + \triangle T \leq 1$.

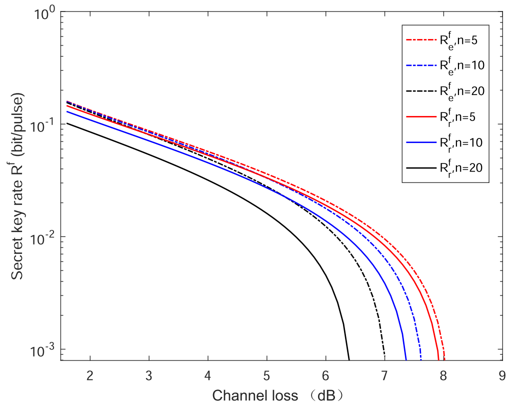

FIGURE 4. Realistic secret key rates R_r ($0 < T_H < 1$, solid lines) and the estimated secret key rates R_e ($T_H = 1$, dashed lines) as the functions of $T_{\min}$ with $w = 1.001$, and different $n = \{5, 10, 20\}$. Note that curves start from nonzero dBs, which is due to the fact that the fading channels must satisfy $T_{\min} + \triangle T \leq 1$.

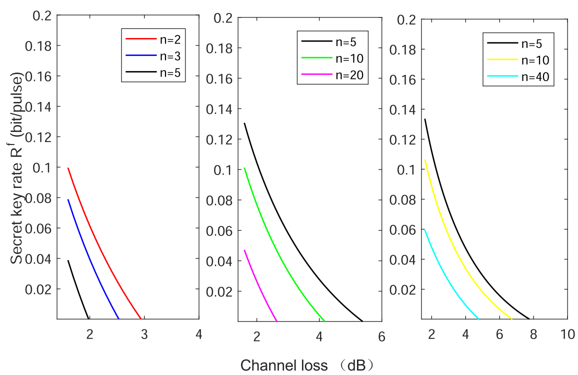

FIGURE 6. Relationship between the secret key rates for different thermal noise $w = 1.1, 1.01, 1.001$. Note that curves start from nonzero dBs, which is due to the fact that the fading channels must satisfy $T_{\min} + \triangle T \leq 1$.

probability density distribution of the transmissivity is $P(T) = \frac{1}{\triangle T}$, where $\triangle T = T_{\max} - T_{\min}$.

In this part, we present a comparison among n key rates $\{R^f_1, R^f_2, \ldots, R^f_n\}$. In addition, the calculation method of the secret key rate between an arbitrary participant U_j (Alice) and the dealer (Bob) is shown in Appendix B in detail. As shown in Fig. 3, a comparison among n (fixed $n = 20$) key rates is displayed, and the figure shows that the key rate R^f_j increases with the increase of j, and R^f_1 is the smallest of them. According to the aforementioned protocol, the smallest R^f_1 can be thought of as the key rate of the QSS in the fast-fluctuating channel.

First, we focus on the effects of the HABS on the security bound of the QSS protocol in uniform fast-fluctuating channel. In Fig. 4, we compare the realistic key rates R^f_r ($0 < T_H < 1$, solid lines) and the estimated key rates R^f_e ($T_H = 1$, dashed lines) under different n. Note that curves start from nonzero dBs, which is due to the fact that the fading channels must satisfy $T_{\min} + \triangle T \leq 1$, where we set $\triangle T = 0.3$. As shown in this figure, the security key rate bound is overestimated when the HABS is treated as the perfect device ($T_H = 1$), and the degree of influence increases with the increase of the total number of the participants n. When $n = 20$, the errors in terms of the maximum channel loss and the key rate become obvious. Therefore, simply equating the transmissivity of HABS to 1 will lead to a large error. In the security analysis, considering the factor of realistic HABS will eliminate this error. In the following analysis, we proceed on the premise that HABS is realistic with transmissivity $T_H = 0.99$.

Second, we verify the conclusion that in CV-QSS under uniform fast-fluctuating channels, the bound on the key rate $R^f(T)$ computed by using the mutual information corresponding to $T_{\min}$ is tighter than the bound $R^a(T)$ by using the average mutual information through numerical simulations. As shown in Fig. 5, when the number of participants is the same (such as $n = 5$), the key rate curve of $R^f(T)$ (red solid line) is below the curve of $R^a(T)$ (red dashed line). Clearly, the simulation result is in accord with the theoretical analysis.

Fig. 6 shows the effect of the thermal noise w introduced by each participant on the performance of QSS protocol.

Note that the w we set in Fig. 6 are 1.1, 1.01, and 1.001, respectively. In fact, with the same number of participants, the smaller the thermal noise is, the higher the key rate and the tolerable channel loss will be. From another perspective, the number of participants n can be increased by reducing the thermal noise w introduced by each participant.

Moreover, Figs. 4 and 6 illustrate the fact that as the number of participants n increases, the key rate and the maximum tolerable channel loss (threshold channel loss for which keys can be generated) decrease. The phenomenon is derived from the fact that an increase in the number of participants can result in more excess noise.

V. CONCLUSION

In this article, we have presented a feasible CV-QSS protocol in fast-fluctuating channels. Unlike the protocol using the fiber channel, this CV-QSS protocol is exposed to the fast-fluctuating attack in which Eve has the ability to fully control the process of transmissivity fluctuations, while the users only have access to the transmissivity that occurs at the end of the quantum communication.

First, we have offered the lower bound of the key rate for the QKD link between any participant U_j and the dealer under the fast-fluctuating attack. Then, on this basis, we have established an security lower bound of key rate for CV-QSS by presenting the Theorem 1. In particular, we have discussed a more practical CV-QSS, where the effects of the realistic HABS were investigated in terms of the total noise and secret key rate.

In the key-rate simulation analysis, we have provided one typical channel model: The uniform fluctuating channel. Numerical simulations have shown that simply considering perfect HABS, the total noise will be underestimated and the key rate will be overestimated. Furthermore, the performance of CV-QSS in terms of the key rate and he maximum tolerable channel loss decreases as the number of participants n and the noise w introduced by each participant increases.

It would be meaningful to further explore the feasibility and performance of CV-QSS in some more complex channels in practice, such as atmospheric fluctuating channels with nonuniform fluctuating transmissivity. Moreover, as for the Holevo bound, there is no consensus on how to calculate it under the fast-fluctuating channels. In [15], the Holevo bound is calculated by averaging the bounds for the different channel transmittances, while in [19], the bound is calculated on the average covariance matrix. In this article, we use the first method, and we will try to compare the key rates under the two methods theoretically and experimentally to find a tighter lower bound of the key rate in future studies.

APPENDIX

A. PROOF OF THEOREM 2

Proof 1: The total noise can be written as

$$\chi_t(j,n) = \frac{1+\chi_h}{T_e(j,n)} + \sum_{i=1}^{n} \varepsilon(i,n) - 1. \tag{21}$$

The derivative of $T_e(n)$ according to n is

$$T_e'(n) = \begin{cases} T_H^{n-1} * \ln(T_H) * 10^{-0.1D}, & j=1 \quad (22)\\ T_e(j,n) g(j,n), & j=2,\ldots,n \quad (23) \end{cases}$$

where

$$g(j,n) = \left[\ln(T_H) - \ln(10) * 0.1D * (j-1) * n^{-2}\right]. \tag{24}$$

Obviously, when $0 < T_H < 1$, we obtain $T_e'(n) < 0$ and thus $T_e(j,n)$ decreases as n increases. Moreover, the excess noise $\varepsilon(j,n)$ for each participant U_j is increses as n increases. Naturally, the sum of excess noises: $\sum_{i=1}^{n} \varepsilon(i,n)$ increases with the number of participants. In combination with (21), the noise $\chi_t(j,n)$ is a monotonically increasing function as n increases.

Proof 2: The derivative with respect to j of the total noise $\chi_t(j,n)$ is written as

$$\chi_t'(j) = -\frac{1+\chi_h}{T_e^2(j)} T_e'(j) \tag{25}$$

where

$$T_e'(j) = T_e(j,n)[\ln(10) * 0.1 * D * n^{-1} - \ln(T_H)] \tag{26}$$

is the derivative of $T_e(j)$ with respect to $j (j = 2,\ldots,n)$. When $0 < T_H < 1$, there is $T_e(j=2) > T_e(j=1)$, and according to the (26), we obtain $T_e'(j) > 0$ $(j=1,\ldots,n)$. Combined with (25), the total noise $\chi_t(j)$ is a monotone decreasing function on j.

Proof 3: The deviation between the realistic total noise $\chi_t(j,n)$ and the estimated total noise $\tilde{\chi}_t(j,n)$ can be written as

$$\begin{aligned} \Delta\chi_t(j,n) &= \chi_t(j,n) - \tilde{\chi}_t(j,n) \\ &= \frac{(1+\chi_h)(1-T_H^{f(j,n)})}{T_e(j,n)} \\ &\quad + \sum_{i=1}^{n} \frac{(w-1)(1-T_H^{f(i,n)})}{T_e(i,n)}. \end{aligned} \tag{27}$$

Let item $\frac{(1+\chi_h)(1-T_H^{f(j,n)})}{T_e(j,n)} = \Delta\chi_{t1}(j,n)$. When $0 < T_H < 1$, we find its derivative according to n is positive, thus the item $\Delta\chi_{t1}(j,n)$ is a monotone increasing function with respect to n. As for $\Delta\varepsilon(j,n) = \frac{(w-1)(1-T_H^{f(j,n)})}{T_e(j,n)}$, it increases as n increases. Naturally, the sum: $\sum_{i=1}^{n} \Delta\varepsilon(j,n)$ increases as n increases. Therefore, according to (27), the $\Delta\chi_t(j,n)$ is a monotone increasing function with respect to n.

The derivative with respect to j of the deviation noise $\Delta\chi_t(j,n)$ is written as

$$\begin{aligned} \Delta\chi_t'(j) = &-\frac{(1+\chi_h)(1-T_H^{f(j,n)})}{T_e^2(j)} T_e'(j) \\ &+ \frac{(1+\chi_h) T_H^{f(j,n)} \ln(T_H)}{T_e^2(j)} \end{aligned} \tag{28}$$

where we have obtained $T_e'(j) > 0$ and $\ln(T_H) < 0$ with $\chi_h \geq 0$, so the derivative $\Delta\chi_t'(j) < 0$. Therefore, the deviation noise $\Delta\chi_t(j, n)$ is a monotone decreasing function on j.

B. CALCULATION METHOD OF SECRET KEY RATE

Our purpose is to give a calculation method of secret key rate distributed between an arbitrary participant U_j (Alice) and the dealer (Bob) in 9. The mutual information between Alice and Bob is given by

$$I_{AB}(j,n) = \log_2 \frac{V(j,n) + \chi_t(j,n)}{1 + \chi_t(j,n)} \tag{29}$$

where the variance $V(j, n) = V_A + 1$. Since reverse reconciliation in Alice and Bob can overcome the 3-dB limit, we consider this reconciliation in our QSS protocol. In order to estimate the secure key rate, we should obtain the Holevo bound $\chi_{B:E} = S(E) - S(E|B)$ between Eve and Bob, where $S(E)$ is Eve's von Neumann entropy and $S(E|B)$ is the conditional von Neumann entropy. By using the model introduced in [17], the expression of $\chi_{B:E}$ can be further simplified as

$$\chi_{B:E}(j,n) = \sum_{i=1}^{2} G(\nu_i(j,n)) - \sum_{i=3}^{5} G(\nu_i(j,n)) \tag{30}$$

where $G(\nu) = \frac{\nu+1}{2}\log_2\frac{\nu+1}{2} - \frac{\nu-1}{2}\log_2\frac{\nu-1}{2}$. The symplectic eigenvalues can be given by

$$\nu_{1,2}(j,n) = \frac{1}{2}[A(j,n) \pm \sqrt{A^2(j,n) - 4B(j,n)}] \tag{31}$$

$$\nu_{3,4}(j,n) = \frac{1}{2}\left[C(j,n) \pm \sqrt{C^2(j,n) - 4D(j,n)}\right] \tag{32}$$

and $\nu_5 = 1$, where

$$A(j,n) = V^2(j,n)(1 - 2T_e(j,n)) + 2T_e(j,n) + [T_e(j,n)(V + \chi_l(j,n))]^2 \tag{33}$$

$$B(j,n) = [T_e(j,n)(V(j,n) + \chi_l(j,n))]^2 \tag{34}$$

$$C(j,n) = \frac{A(j,n)\chi_h^2 + 2\chi_h[V(j,n)\sqrt{B(j,n)} + E(j,n)]}{E^2(j,n)} + \frac{B(j,n) + 1 + 2T_e(j,n)(V^2(j,n) - 1)}{E^2(j,n)} \tag{35}$$

$$D(j,n) = \left[\frac{V(j,n) + \sqrt{B(j,n)}\chi_h}{E^2(j,n)}\right] \tag{36}$$

$$E(j,n) = T_e(j,n)\left(V(j,n) + \chi_t(j,n)\right). \tag{37}$$

ACKNOWLEDGMENT

The authors would like to thank the anonymous referees and editor for important suggestions that help us improve the quality of the article.

REFERENCES

[1] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, "Quantum cryptography," *Rev. Modern Phys.*, vol. 74, no. 1, Art. no. 145, 2002, doi: 10.1103/RevModPhys.74.145.

[2] F. Xu, X. Ma, Q. Zhang, H.-K. Lo, and J.-W. Pan, "Secure quantum key distribution with realistic devices," *Rev. Modern Phys.*, vol. 92, no. 2, 2020, Art. no. 025002, doi: 10.1103/RevModPhys.92.025002.

[3] T. C. Ralph, "Continuous variable quantum cryptography," *Phys. Rev. A*, vol. 61, no. 1, 1999, Art. no. 010303, doi: 10.1103/PhysRevA.61.010303.

[4] N. J. Cerf, M. Levy, and G. Van Assche, "Quantum distribution of Gaussian keys using squeezed states," *Phys. Rev. A*, vol. 63, no. 5, 2001, Art. no. 052311, doi: 10.1103/PhysRevA.63.052311.

[5] F. Grosshans and P. Grangier, "Continuous variable quantum cryptography using coherent states," *Phys. Rev. Lett.*, vol. 88, no. 5, 2002, Art. no. 057902, doi: 10.1103/PhysRevLett.88.057902.

[6] S. Pirandola, S. Mancini, S. Lloyd, and S. L. Braunstein, "Continuous-variable quantum cryptography using two-way quantum communication," *Nature Phys.*, vol. 4, no. 9, pp. 726–730, 2008, doi: 10.1038/nphys1018.

[7] S. Pirandola et al., "High-rate measurement-device-independent quantum cryptography," *Nature Photon.*, vol. 9, no. 6, pp. 397–402, 2015, doi: 10.1038/nphoton.2015.83.

[8] G. Chai, Z. Cao, W. Liu, S. Wang, P. Huang, and G. Zeng, "Parameter estimation of atmospheric continuous-variable quantum key distribution," *Phys. Rev. A*, vol. 99, no. 3, 2019, Art. no. 032326, doi: 10.1103/PhysRevA.99.032326.

[9] W. P. Grice and B. Qi, "Quantum secret sharing using weak coherent states," *Phys. Rev. A*, vol. 100, no. 2, 2019, Art. no. 022339, doi: 10.1103/PhysRevA.100.022339.

[10] A. Shamir, "How to share a secret," *Commun. ACM*, vol. 22, no. 11, pp. 612–613, 1979, doi: 10.1145/359168.359176.

[11] C. Schmid, P. Trojek, M. Bourennane, C. Kurtsiefer, M. Żukowski, and H. Weinfurter, "Experimental single qubit quantum secret sharing," *Phys. Rev. Lett.*, vol. 95, no. 23, 2005, Art. no. 230505, doi: 10.1103/PhysRevLett.95.230505.

[12] D. Gottesman, "Theory of quantum secret sharing," *Phys. Rev. A*, vol. 61, no. 4, 2000, Art. no. 042311, doi: 10.1103/PhysRevA.61.042311.

[13] X. Wu, Y. Wang, and D. Huang, "Passive continuous-variable quantum secret sharing using a thermal source," *Phys. Rev. A*, vol. 101, no. 2, 2020, Art. no. 022301, doi: 10.1103/PhysRevA.101.022301.

[14] Q. Liao, H. Liu, L. Zhu, and Y. Guo, "Quantum secret sharing using discretely modulated coherent states," *Phys. Rev. A*, vol. 103, no. 3, 2021, Art. no. 032410, doi: 10.1103/PhysRevA.103.032410.

[15] P. Papanastasiou, C. Weedbrook, and S. Pirandola, "Continuous-variable quantum key distribution in uniform fast-fading channels," *Phys. Rev. A*, vol. 97, no. 3, 2018, Art. no. 032311, doi: 10.1103/PhysRevA.97.032311.

[16] F. Grosshans, G. Van Assche, J. Wenger, R. Brouri, N. J. Cerf, and P. Grangier, "Quantum key distribution using Gaussian-modulated coherent states," *Nature*, vol. 421, no. 6920, pp. 238–241, 2003, doi: 10.1038/nature01289.

[17] J. Lodewyck et al., "Quantum key distribution over 25 km with an all-fiber continuous-variable system," *Phys. Rev. A*, vol. 76, no. 4, 2007, Art. no. 042305, doi: 10.1103/PhysRevA.76.042305.

[18] A. Lapidoth and S. Shamai, "Fading channels: How perfect need "perfect side information" be?," *IEEE Trans. Inf. Theory*, vol. 48, no. 5, pp. 1118–1134, May 2002, doi: 10.1109/18.995552.

[19] D. Dequal et al., "Feasibility of satellite-to-ground continuous-variable quantum key distribution," *npj Quantum Inf.*, vol. 7, no. 1, 2021, Art. no. 3, doi: 10.1038/s41534-020-00336-4.

[20] C. Weedbrook et al., "Gaussian quantum information," *Rev. Modern Phys.*, vol. 84, no. 2, 2012, Art. no. 621, doi: 10.1103/RevModPhys.84.621.

[21] D. Y. Vasylyev, A. Semenov, and W. Vogel, "Toward global quantum communication: Beam wandering preserves nonclassicality," *Phys. Rev. Lett.*, vol. 108, no. 22, 2012, Art. no. 220501, doi: 10.1103/PhysRevLett.108.220501.

[22] Y. Guo, C. Xie, Q. Liao, W. Zhao, G. Zeng, and D. Huang, "Entanglement-distillation attack on continuous-variable quantum key distribution in a turbulent atmospheric channel," *Phys. Rev. A*, vol. 96, no. 2, 2017, Art. no. 022320, doi: 10.1103/PhysRevA.96.022320.

[23] S. Pirandola, R. Laurenza, C. Ottaviani, and L. Banchi, "Fundamental limits of repeaterless quantum communications," *Nature Commun.*, vol. 8, no. 1, 2017, Art. no. 15043, doi: 10.1038/ncomms15043.