Quantum secret sharing using discretely modulated coherent states

Qin Liao,[1,2,*] Haijie Liu,[1] Lingjin Zhu,[3] and Ying Guo[2,†]

[1] *College of Computer Science and Electronic Engineering, Hunan University, Changsha 410082, China*
[2] *Institute of Advanced Photoelectric Detection and Quantum System, Central South University, Changsha 410083, China*
[3] *Hunan Institute of Metrology and Test, Changsha 410014, China*

(Received 25 October 2020; accepted 1 March 2021; published 12 March 2021)

Point-to-point quantum privacy communication over a standard telecommunication fiber link can be implemented by continuous-variable quantum key distribution (CV QKD). However, as communication networks develop, the two-party CV QKD system may hardly meet the requirements of secret key sharing of multiple users (at least three users). In this paper, we consider a protocol called quantum secret sharing (QSS) which allows a legitimate user, a so-called dealer, to share a secret key with multiple remote users through an insecure quantum channel. These users can correctly recover the dealer's secret key only when they work cooperatively. We carry out QSS with discretely modulated coherent states (DMCSs) because they are easy to prepare and resilient to losses. An asymptotic security proof for the proposed DMCS-based QSS protocol against both eavesdroppers and dishonest users is presented. Numerical simulation based on a linear bosonic channel shows that the maximal transmission distance of the DMCS-based QSS protocol reaches more than 100 km, and it can be further lengthened by exploiting a higher-dimensional discrete modulation strategy. Moreover, the composable security of the DMCS-based QSS protocol is also presented.

DOI: 10.1103/PhysRevA.103.032410

I. INTRODUCTION

Continuous-variable quantum key distribution (CV QKD) [1] is designed to implement point-to-point secret key distribution over an insecure quantum channel; its security is guaranteed by the laws of quantum physics [2]. Specifically, the sender, Alice, usually encodes secret key bits in the phase space of coherent states, and the receiver, Bob, measures the incoming signal states using coherent detection techniques. After postprocessing, Alice and Bob can share an identical string of a secret key. One of the advantages of CV QKD is that it is compatible with most state-of-the-art commercial telecommunication technologies [3]; therefore, one may apply the CV QKD system to current practical communication links in use.

In general, CV QKD can be further divided into two types according to the different modulation approaches, i.e., Gaussian-modulated CV QKD [4,5] and discretely modulated CV QKD [6,7]. The first type has been widely studied; since the repetition rate in Gaussian-modulated CV QKD is usually higher, it might potentially obtain a higher secret key rate. It is worth noticing that the first protocol of CV QKD ("GG02" protocol presented in Ref. [8]) belongs to the Gaussian-modulated CV QKD, and it has been proven to be secure in both the asymptotic limit [9] and the finite-size regime [10]. Moreover, the composable security proof for Gaussian-modulated CV QKD was presented in [11], which showed that the theoretical security issue of Gaussian-modulated CV QKD is completely solved. For the second type, discretely modulated CV QKD prepares several nonorthogonal states and encodes secret key bits in the sign of the quadrature of each state. This modulation approach is probably more suitable for long-distance transmission because the sign of the quadrature is already discrete, so most existing error-correcting codes might work well even at a low signal-to-noise ratio. The preliminary security proof for discretely modulated CV QKD was suggested in [12], which showed that discretely modulated CV QKD is secure against Gaussian attacks for any linear quantum channel. After that, Ref. [13] showed that discretely modulated CV QKD with decoy states is secure against arbitrary collective attacks, which implies the unconditional security of discretely modulated CV QKD in the asymptotic limit. Very recently, the asymptotic security of discretely modulated CV QKD (without decoy states) against arbitrary collective attacks was proven. Reference [14] established a lower bound on the asymptotic secret key rate of discretely modulated CV QKD. This bound is obtained by formulating the problem as a semidefinite program, while Ref. [15] applied a numerical method to analyze the security of discretely modulated CV QKD, paving the way for a full security proof with finite-size effects. The latest security proof for discretely modulated CV QKD was presented in [16]; it provides a composable security analysis in the finite-size regime assuming the realistic, but restrictive, hypothesis of collective Gaussian attacks.

However, with the rapid development of communication networks, the point-to-point CV QKD system may hardly meet the specific requirements of multiple users (at least three users). Imagine a scenario in which a legitimate user, a so-called dealer, wants to share a secret key with two remote users through an insecure quantum channel. The dealer knows one of them may not be entirely honest. The dealer therefore

[*] llqqlq@hnu.edu.cn
[†] yingguo@csu.edu.cn

splits the secret key into two parts and individually sends each user a part. Consequently, no one can obtain the whole secret key unless they collaborate. Such situations widely exist in business, the military, and politics. To achieve this goal, single-qubit sequential secret sharing was suggested and experimentally demonstrated in Ref. [17], but some tough security issues have not been completely resolved yet, especially for Trojan horse attacks in which a malicious eavesdropper could send multiphoton signals to the polarization rotation device of the targeted party and unambiguously determine the corresponding polarization rotation by measuring the output signals [18].

Considering the growing demand for securely sharing a secret key with multiple users, in this paper, we extend two-party CV QKD, which has been proven to be secure, to at least three users and thus consider a protocol called quantum secret sharing (QSS). QSS, which is a kind of secret-sharing protocol using quantum-based technology, can securely deliver multiple secret keys to a group of remote users; these users can jointly share an identical secret key with the dealer only when they cooperatively work together. That is to say, a single user or even part of the users in the group cannot recover the correct secret key without the whole group's knowledge. In particular, we implement the QSS protocol with discretely modulated coherent states (DMCSs); the nonorthogonal nature of coherent states is the basis for many of these applications, particularly those involving communication security [19]. DMCSs are ideal for quantum communications because they are easy to prepare and measure, and they are resilient to losses, so they can maximize the information transmitted over the long-distance communication channel. We then present a theoretical security proof for the proposed DMCS-based QSS protocol against both eavesdroppers and dishonest users. Numerical simulation based on the linear bosonic channel shows that the maximal transmission distance of the DMCS-based QSS protocol reaches more than 100 km, and it can be further lengthened by exploiting a higher-dimensional discrete modulation strategy. Moreover, the composable security of the DMCS-based QSS protocol against collective Gaussian attacks is also presented.

This paper is structured as follows. In Sec. II, we detail the proposed DMCS-based QSS protocol. In Sec. III, we derive the calculations of the secret key rate of the proposed protocol. Performance analysis and discussion are presented in Sec. IV, and final conclusions are drawn in Sec. V.

II. DMCS-BASED QSS PROTOCOL

Since our protocol is extended by CV QKD, it is necessary to show the principles of CV QKD. To make the derivation self-contained, we first introduce coherent states and show how they work in discretely modulated CV QKD with quadrature-phase-shift keying (QPSK). After that, we detail the proposed DMCS-based QSS protocol and consider its security.

A. Coherent states in discretely modulated CV QKD

In general, coherent states can be generalized to one with N quantum states $|\alpha_k^N\rangle = |\alpha e^{i2k\pi/N}\rangle$, where $k \in \{0, 1, \dots, N-1\}$ and α is a positive number related to the modulation variance of the quantum state as $V_M = 2\alpha^2$ [20].

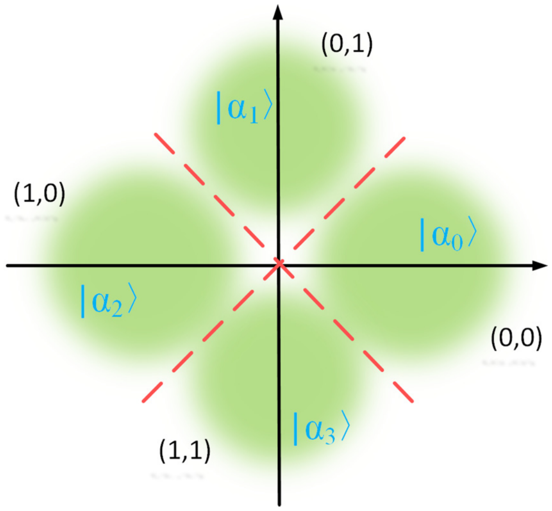

FIG. 1. Description of coherent states with QPSK and the partition of phase space in four quadrants.

In the prepare-and-measure (PM) version of discretely modulated CV QKD, Alice first selects a random bit string $\mathbf{a} = (a_0, a_1, \dots, a_{2L-1})$ of length $2L$; the coherent states are subsequently encoded according to the successive pairs of bit strings $\mathbf{a}$ with the form $|\alpha_k^N\rangle$, where $k_l = 2a_{2l} + a_{2l+1}$. Alice sends these modulated coherent states to remote Bob through a lossy and noisy quantum channel. When Bob receives these states, he can apply a heterodyne detector to measure each output mode. The mixture state that Bob receives can be expressed by the following form:

$$\rho_N = \frac{1}{N}\sum_{k=1}^{N} |\alpha_k^N\rangle\langle\alpha_k^N|. \tag{1}$$

Note that the discrete modulation strategy of QPSK requires four nonorthogonal coherent states so that we have $N = 4$; the presentation of QPSK in phase space is depicted in Fig. 1. After the measurement, Bob obtains a $2L$ string $\mathbf{c} = (c_0, c_1, \dots, c_{2L-1}) \in \mathbb{R}^{2L}$. This string can be transformed into a raw key of $2L$ bits $\mathbf{b} = (b_0, b_1, \dots, b_{2L-1})$, given by [14]

$$(b_{2l}, b_{2l+1}) = \begin{cases} (0,0) & \text{if } c_{2l+1} < c_{2l},\ c_{2l+1} \geqslant -c_{2l}, \\ (0,1) & \text{if } c_{2l+1} \geqslant c_{2l},\ c_{2l+1} > -c_{2l}, \\ (1,0) & \text{if } c_{2l+1} > c_{2l},\ c_{2l+1} \leqslant -c_{2l}, \\ (1,1) & \text{if } c_{2l+1} \leqslant c_{2l},\ c_{2l+1} < -c_{2l}. \end{cases} \tag{2}$$

Bob then broadcasts the absolute values of $c_{2l} \pm c_{2l+1}$ through a classical authenticated channel. This side information allows Alice and Bob to turn the information reconciliation problem into a well-studied channel coding problem for the binary-input additive white-noise Gaussian channel (see Ref. [21] for how it works). After several postprocessing steps such as parameter estimation, reconciliation, and privacy amplification, Alice and Bob can establish a correlated sequence of a random secure key.

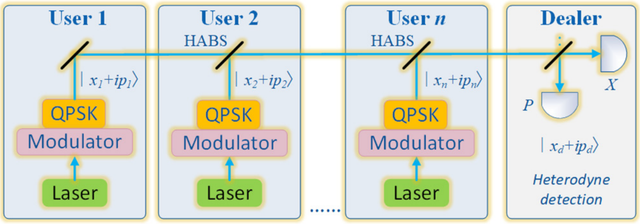

FIG. 2. The proposed DMCS-based QSS protocol, which can distribute multiple parts of a security key to different users, thereby allowing them to cooperatively share a security key with the dealer. Each user can also individually send DMCSs to achieve the purpose of point-to-point CV QKD with the dealer. HABS denotes highly asymmetric beam splitter.

B. DMCS-based QSS and its security

Inspired by the principle of discretely modulated CV QKD [12] and single-qubit sequential quantum secret sharing [17], we propose a DMCS-based QSS protocol using a QPSK modulation strategy. It allows the dealer to share a string of a secret key with a group of remote users over a long-distance commercial fiber-link transmission. As shown in Fig. 2, a dealer is connected to n users through a single communication fiber channel. The procedure of our protocol is detailed as follows.

Step 1. For each quantum transmission, the user who is farthest away from the dealer (user 1) prepares a DMCS with the QPSK format $|x_1 + ip_1\rangle$ and sends it to his nearest neighbor (user 2).

Step 2. User 2 also independently prepares a DMCS with the QPSK format and couples it to the same spatiotemporal mode as the incoming signal state prepared by user 1 via a highly asymmetric beam splitter (HABS). The mixed signal is then sent to the next user.

Step 3. All other users who connected to the link perform similar operations, so that they can inject their locally prepared DMCSs into the spatiotemporal mode corresponding to the signal from user 1.

Step 4. Since each user can introduce displacement of (x_j, p_j) by carefully controlling the modulation variance and having knowledge of the reflectivity of its HABS, the arriving signal state from the dealer's station can be expressed as $|\sum_{j=1}^{n}\sqrt{T_j}x_j + i\sum_{j=1}^{n}\sqrt{T_j}p_j\rangle$, where T_j denotes the channel transmittance that the signal experiences between the jth user and the dealer. The dealer then measures both the amplitude and phase quadratures of the received signal state using heterodyne detection, thereby obtaining the measurement result (x_d, p_d).

Step 5. After many rounds of the above steps, the dealer and users hold sufficient related raw data.

Note that steps 1–5 belong to a quantum operation which aims to generate the related data by taking advantage of quantum optics. The remaining steps address these data with classical postprocessing technologies.

Step 6. The dealer and all users disclose a group of related data to estimate the respective channel transmittance T_j [18]. Note that these disclosed data have to be discarded after this step.

Step 7. Assume the jth user is honest and the remaining $n-1$ users are dishonest. The dealer further picks another group of raw data and requests all users except user j disclose their corresponding values. This operation allows the dealer to displace his measurement results of the group to $x_{b_j} = x_d - \sum_{s\neq j}^{n}\sqrt{T_s}x_s$ and $p_{b_j} = p_d - \sum_{s\neq j}^{n}\sqrt{T_s}p_s$, where $s = 1, 2, \ldots, n$. By doing so, a point-to-point CV QKD link between the dealer and user j is actually established. Therefore, we can estimate a lower bound of the secure key rate R_j using the security analysis technology of QPSK-modulated CV QKD [12]. After that, all participants discard the disclosed data.

Step 8. By performing step 7 n times, the dealer establishes n CV QKD links to each user and obtains the estimated secret key rates $\{R_1, R_2, \ldots, R_n\}$. For security reasons, the dealer should choose the smallest value among $\{R_1, R_2, \ldots, R_n\}$ as the final secret key rate R of the QSS protocol.

Step 9. If the value of R is positive, the dealer can share different secret keys with each user using the rest of the undisclosed data. For each CV QKD link, the dealer converts the raw data into bit strings according to Eq. (2) and then broadcasts the values of $|x_{b_j} \pm p_{b_j}|$ [14]. These absolute values are used for the reverse reconciliation in which classical information goes from the dealer to the users [21]. Note that this process can be finished without users' cooperation. After the standard postprocessing procedures in CV QKD, the dealer shares an independent secret key K_j with each user.

Step 10. Finally, the dealer generates a new key according to the formula $K = K_1 \oplus K_2 \oplus \cdots \oplus K_n$ and subsequently encodes the message M via the expression $E = M \oplus K$. The dealer then announces the encrypted message E to all users. As a result, the encrypted message E can be decoded by the whole group of users only when they work cooperatively.

Directly analyzing the security of the proposed DMCS-based QSS protocol is intuitively complicated because there are multiple participants and we actually do not know how many users are untrusted and how powerful an attack suffered during the transmission could be. Fortunately, by tactfully exploiting the well-established security proof of discretely modulated CV QKD, the security of the DMCS-based QSS protocol can be proven. Let us address the problem of dishonest users first. As mentioned in step 7, a point-to-point CV QKD link between the dealer and user j is actually established. This statement is based on the assumption that the jth user is the only user who can be trusted. This is the most pessimistic assumption since the protocol is useless if all users are dishonest. Therefore, this two-party link can be deemed a model of CV QKD involving two legitimate users, i.e., the sender, Alice (user j), and the receiver, Bob (the dealer). Now the problem is whether the remaining $n-1$ dishonest users can gain the information between Alice and Bob and thereby recover the secret key shared by Alice and Bob. Note that the dealer requests all users except user j to publicly disclose their corresponding values in this CV QKD transmission, so that user j holds the complete information of all users, while the remaining $n-1$ users cannot deduce the information between user j and the dealer by knowing only the revealed information. Therefore, Alice and Bob can share a secret key regardless of the existence of $n-1$ dishonest users (the worst situation). As for eavesdroppers, it is reasonable to consider the quantum attack in each CV QKD link separately. This suggests that we can use the existing security proof for QPSK-modulated CV QKD to evaluate the security key rate R_j. As we mentioned in Sec. I, the security of discretely modulated CV QKD was investigated in several works. For simplicity, the main tools we chose for solving the eavesdropper issue is the method presented in [12], so a linear bosonic channel assumption is necessary. Note that the proposed QSS protocol should be secure for any honest user, so the dealer is required to evaluate the secret key rate of each CV QKD link and selects the smallest one as the lower bound of the final secret key rate of the QSS protocol. Therefore, the security of the DMCS-based QSS protocol against collaborative attacks launched by the eavesdropper and any $n-1$ (or fewer) dishonest users can be guaranteed if the final secret key rate is positive. Moreover, by injecting locally prepared DMCSs into the circulating optical mode, the modulators within the secure stations cannot be reached by the probing signals from the eavesdropper. That is to say, the user who is assumed to be honest can prevent eavesdroppers from accessing the signal state preparation process, thereby making our protocol immune to Trojan horse attacks [18].

III. CALCULATION OF THE SECRET KEY RATE

As the carrier of the secret key, the derivation of DMCSs is the first issue to be considered. Remember that the received DMCS in the PM version of discretely modulated CV QKD is expressed as Eq. (1); this form, however, is not suitable for security analysis [22]. Fortunately, the PM version is equivalent to the entanglement-based (EB) version, which is more convenient for security analysis [23–25]. In what follows, we first consider the EB version of DMCSs with the QPSK format and then present the calculation of the secret key rate of the proposed DMCS-based QSS protocol.

In the EB version, a DMCS with the QPSK format can be deem a pure state, defined as [13]

$$\begin{aligned}|\Psi_4\rangle &= \sum_{k=0}^{3}\sqrt{\lambda_k}\big|\phi_k^4\big\rangle\big|\phi_k^4\big\rangle\\ &= \frac{1}{2}\sum_{k=0}^{3}\big|\psi_k^4\big\rangle\big|\alpha_k^4\big\rangle,\end{aligned} \tag{3}$$

where the states

$$\big|\psi_k^4\big\rangle = \frac{1}{2}\sum_{m=0}^{3} e^{i(1+2k)m\pi/4}\big|\phi_m^4\big\rangle \tag{4}$$

are the non-Gaussian states and the state $|\phi_m^4\rangle$ is given by

$$\big|\phi_k^4\big\rangle = \frac{e^{-\alpha^2/2}}{\sqrt{\lambda_k}}\sum_{n=0}^{\infty}(-1)^n\frac{\alpha^{4n+k}}{\sqrt{(4n+k)!}}|4n+k\rangle, \tag{5}$$

with

$$\lambda_{0,2} = \tfrac{1}{2}e^{-\alpha^2}[\cosh(\alpha^2)\pm\cos(\alpha^2)], \tag{6}$$

$$\lambda_{1,3} = \tfrac{1}{2}e^{-\alpha^2}[\sinh(\alpha^2)\pm\sin(\alpha^2)]. \tag{7}$$

Consequently, the mixture state ρ_4 can be expressed by

$$\begin{aligned}\rho_4 &= \mathrm{Tr}(|\Psi_4\rangle\langle\Psi_4|)\\ &= \sum_{k=0}^{3}\lambda_k\big|\phi_k^4\big\rangle\big\langle\phi_k^4\big|.\end{aligned} \tag{8}$$

Let A and B respectively denote the two output modes of the bipartite state $|\Psi_4\rangle$ and $\hat{a}$ and $\hat{b}$ denote the annihilation operators applicable to modes A and B, respectively. We have a covariance matrix Γ_{AB}^4 of the bipartite state $|\Psi_4\rangle$ with the following form:

$$\Gamma_{AB}^4 = \begin{pmatrix} X\mathbb{I} & Z_4\sigma_z\\ Z_4\sigma_z & Y\mathbb{I}\end{pmatrix}, \tag{9}$$

where $\mathbb{I}$ and σ_z represent diag(1, 1) and diag(1, −1), respectively, and

$$\begin{aligned}X &= \langle\Psi_4|1+2a^\dagger a|\Psi_4\rangle = 1+2\alpha^2,\\ Y &= \langle\Psi_4|1+2b^\dagger b|\Psi_4\rangle = 1+2\alpha^2,\\ Z_4 &= \langle\Psi_4|ab+a^\dagger b^\dagger|\Psi_4\rangle = 2\alpha^2\sum_{k=0}^{3}\lambda_{k-1}^{3/2}\lambda_k^{-1/2}.\end{aligned} \tag{10}$$

Note that the addition arithmetic should be operated with modulo 4.

According to step 8, the final secret key rate R of the DMCS-based QSS protocol has to be the smallest secret key rate of two-party CV QKD between the dealer and each user. Assuming that each user introduces an equal amount of noise ξ_0, obviously, the smallest CV QKD key rate can be obtained when the distance of the CV QKD link is the longest. Nevertheless, it is worth noticing that the smallest CV QKD key rate in a practical QSS system must be estimated from realistic data, so it may not belong to the farthest CV QKD link. For theoretical analysis, we consider only the situation in which the introduced noise of each user is identical. Let Alice be the farthest user and Bob be the dealer (their distance is denoted as L), and all the other $n-1$ users are located between them at equal intervals; the secret key rate of the proposed QSS protocol can be estimated by reasonably exploiting the security analysis technology of the discretely modulated CV QKD between Alice and Bob. Therefore, the lower bound of the asymptotic secret key rate of the QSS protocol can be given by [12]

$$R = \beta I_{AB} - \chi_{BE}, \tag{11}$$

where β is the reverse reconciliation efficiency, I_{AB} is the Shannon mutual information between Alice and Bob, and χ_{BE} is the maximum information available to the dishonest users and eavesdroppers on Bob's measurement. Assuming that the transmittance of HABS at each user's station is $t \cong 1$, the channel transmittance of the jth user can be expressed as

$$T_j = 10^{\frac{-\delta l_j}{10}}, \tag{12}$$

where $l_j = \frac{n-j+1}{n}L$ is the distance between the dealer and the jth user and δ is the attenuation coefficient of the fiber link. Therefore, the excess noise contributed by the jth user, when referred to the channel input, can be calculated by [18]

$$\xi_j = \frac{T_j}{T_1}\xi_0, \tag{13}$$

so that the channel-added noise, referred to as the channel input, can be given by

$$\chi_{\text{line}} = \frac{1}{T_1} - 1 + \sum_{j=1}^{n}\xi_j, \tag{14}$$

and the noise added by Bob's heterodyne detector (referred to as Bob's input) is given by

$$\chi_{\text{het}} = (2 - \mu + 2v_{el})/\mu, \tag{15}$$

where μ is the detection efficiency and v_{el} is the electronics noise of the imperfect detector. Hence, the overall noise, referred to as the channel input, can be expressed as

$$\chi_{\text{tot}} = \chi_{\text{line}} + \frac{\chi_{\text{het}}}{T_1}. \tag{16}$$

We now can calculate the Shannon mutual information between Alice and Bob using the following equation [9]:

$$I_{AB} = \log_2\frac{V + \chi_{\text{tot}}}{1 + \chi_{\text{tot}}}, \tag{17}$$

where $V = 1 + V_M$.

The term χ_{BE} in Eq. (11) is bounded by the Holevo quantity [26],

$$\chi_{BE} = S(\rho_E) - \int dx_B, p_B P(x_B, p_B) S\big(\rho_E^{x_B, p_B}\big), \tag{18}$$

where x_B, p_B denotes Bob's measurement result. $P(x_B, p_B)$ is the probability density of the measurement, $\rho_E^{x_B, p_B}$ is the eavesdropper's state conditional on Bob's measurement result, and S is the von Neumann entropy of the quantum state ρ_4. Assuming that the loss and noise of Bob's detector are trusted and cannot be accessed by the eavesdropper, Eq. (18) can be further expressed as [27]

$$\chi_{BE} = \sum_{j=1}^{2} G\left(\frac{\xi_j - 1}{2}\right) - \sum_{j=3}^{5} G\left(\frac{\xi_j - 1}{2}\right), \tag{19}$$

where $G(x) = (x+1)\log_2(x+1) - x\log_2 x$ and $\xi_{1,2}$ are symplectic eigenvalues of the covariance matrix,

$$\Gamma_{AB'}^{4} = \begin{pmatrix} X\mathbb{I} & \sqrt{T_1}Z_4\sigma_z \\ \sqrt{T_1}Z_4\sigma_z & T_1(Y + \chi_{\text{line}})\mathbb{I} \end{pmatrix}. \tag{20}$$

As is known, the Holevo information χ_{BE} is maximized if state ρ_4 shared by Alice and Bob is Gaussian. Therefore, χ_{BE} can be bound by a function of the covariance matrix (20) in which Z_4 would be replaced by the correlation of a two-mode squeezed vacuum $Z_{EPR} = \sqrt{V^2 - 1}$. The correlation of Z_4 for state $|\Psi_4\rangle$ does not take such a simple mathematical form but turns out to be almost equal to Z_{EPR} for small variance [12]. Hence, for a sufficiently low modulation variance, the bound on χ_{BE} is almost identical to the one obtained for a Gaussian modulation. So we have

$$\xi_{1,2}^2 = \frac{1}{2}[A \pm \sqrt{A^2 - 4B}], \tag{21}$$

with

$$A = V^2 + T_1^2(V + \chi_{\text{line}})^2 - 2T_1Z_4^2 \tag{22}$$

and

$$B = T_1^2\big(V^2 + V\chi_{\text{line}} - Z_4^2\big)^2. \tag{23}$$

The calculation of $\xi_{3,4,5}$ using the security analysis technology of CV QKD is quit redundant; we here present only the final equations, and a detailed derivation can be found in our previous work [28]. So we have

$$\xi_{3,4}^2 = \frac{1}{2}[C \pm \sqrt{C^2 - 4D}], \quad \xi_5 = 1, \tag{24}$$

where

$$C = \frac{1}{T^2(V + \chi_{\text{tot}})^2}\Big\{A\chi_{\text{het}}^2 + B + 1 + 2\chi_{\text{het}}\big[V\sqrt{B} + T(V + \chi_{\text{line}}) + 2TZ_4^2\big]\Big\}, \tag{25}$$

$$D = \left(\frac{V + \sqrt{B}\chi_{\text{het}}}{T(V + \chi_{\text{tot}})}\right)^2. \tag{26}$$

For now, we can evaluate the performance of the proposed DMCS-based QSS protocol.

IV. PERFORMANCE ANALYSIS AND DISCUSSION

In this section, we discuss the performance of the proposed DMCS-based QSS protocol in terms of both the asymptotic limit and finite-size regime. Before performing the numerical simulation, several global parameters have to be assigned according to the realistic experimental environment [9]. Therefore, we set the attenuation coefficient of a standard fiber link to $\delta = 0.2$ dB/km, the detection efficiency and electronics noise of the imperfect heterodyne detector to $\mu = 0.6$ and $v_{el} = 0.05$, the reconciliation efficiency to $\beta = 0.98$, and excess noise to $\xi_0 = 0.001$. Figure 3 shows the asymptotic performance of the DMCS-based QSS protocol; these results are optimized by considering the optimal modulation variance in each transmission distance (shown in the inset). Note that the optimal modulation variances are very small (ranging from 0.35 to 0.75) because the established security proof of discretely modulated CV QKD [12] has shown that small modulation variance is beneficial for preventing information from being overheard by Eve. The maximal transmission distance of the DMCS-based QSS protocol reaches more than 100 km (blue line) when only two users cooperatively work in the QSS network. However, the performance decreases as the number of users increases; especially, when the number of users is 40 (green line), the transmission distance is reduced to less than 20 km. This is actually to be expected; as we mentioned in Sec. II, the secret key rate of the QSS protocol has to be the smallest secret key rate among all two-party CV QKD links. For security, the other $n-1$ dishonest users in each CV QKD link are deemed to be untrusted, thereby introducing amounts of noise. That is to say, the more untrusted users that exist, the more noise will be introduced. To verify the above inference, we plot (Fig. 4), for the proposed DMCS-based QSS protocol (solid lines) and point-to-point CV QKD protocol (black dashed line), the resistance to noise as a

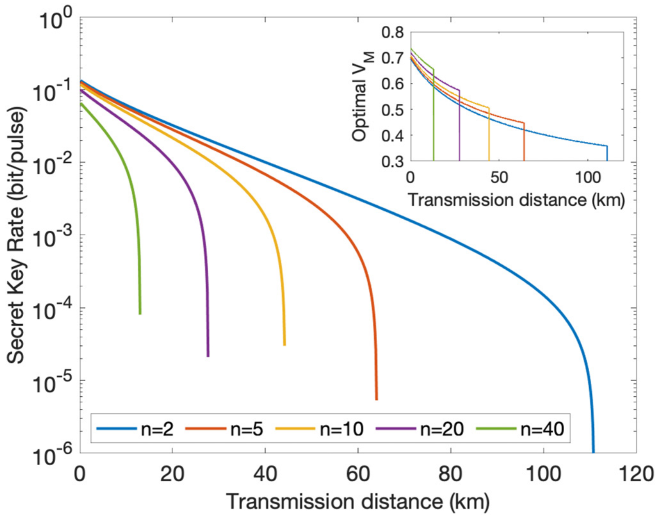

FIG. 3. Asymptotic secret key rate of the DMCS-based QSS protocol as a function of transmission distance. Inset: Optimal modulation variance of the DMCS-based QSS protocol as a function of the transmission distance. From right to left in both the main figure and inset, the solid lines denote the number of users: $n = 2$, $n = 5$, $n = 10$, $n = 20$, and $n = 40$.

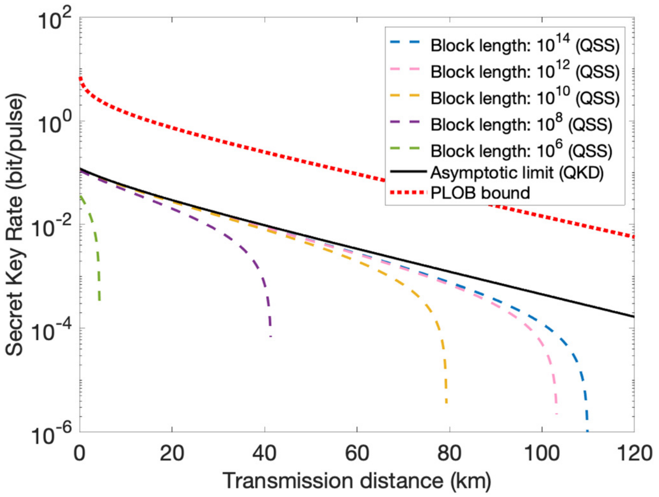

FIG. 5. Secret key rate as a function of the transmission distance. Dashed lines denote the composable secret key rate of the DMCS-based QSS protocol (the number of users $n = 2$). For comparison, the black solid line denotes the asymptotic secret key rate of point-to-point discretely modulated CV QKD (the number of users $n = 1$). The red dotted line denotes the Piradola-Laurenza-Ottaviani-Banchi (PLOB) bound [29]. From right to left, dashed lines correspond to block lengths of 10^{14}, 10^{12}, 10^{10}, 10^8, and 10^6.

function of the channel losses, which gives the excess noise ξ_0 given a null secret key for a given channel of transmittance. We observe that the best resistance can be obtained when $n = 1$; this situation represents the point-to-point CV QKD where only one user and the dealer share a random secret key over an insecure quantum channel, while the resistance continuously degenerates as the number of users increases. Actually, the ability of the proposed DMCS-based QSS protocol to resist the channel-added noise caused by the channel should be identical if each newly added untrusted user does not introduce any excess noise; this, obviously, is impossible. The introduced excess noise caused by an untrusted user will, to some degree, influence the protocol's resistance capacity. Therefore, having in mind the results of Fig. 4, it is not a surprise that the proposed DMCS-based QSS protocol gives the maximal transmission distance when n has the smallest value of 2.

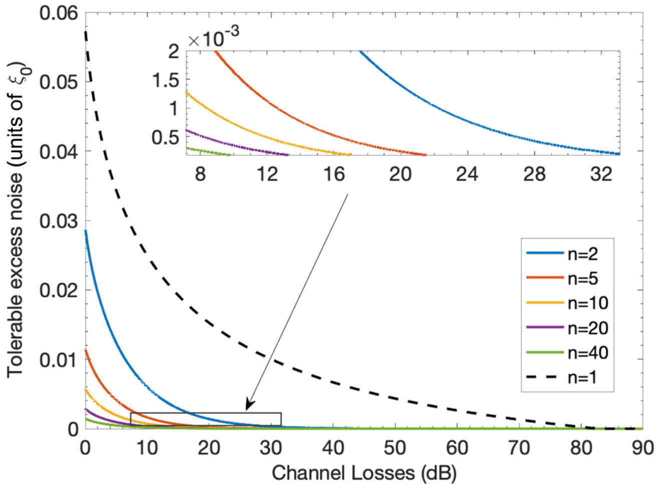

FIG. 4. Tolerable excess noise ξ_0 of the DMCS-based QSS protocol as a function of the channel losses (measured in decibels). The black dashed line (the number of users $n = 1$) denotes point-to-point CV QKD where only one user and the dealer share a random secret key. From top to bottom, the solid lines denote $n = 2$, $n = 5$, $n = 10$, $n = 20$, and $n = 40$.

The above performance analysis is based on an assumption that one considers the security of the QSS protocol in the asymptotic regime of infinitely many signals exchanged by users and the dealer. However, the practical security of QSS implementations is, in fact, jeopardized due to the finite length of the data blocks. Therefore, it is necessary to consider the impact of the finite-size effect on the proposed DMCS-based QSS protocol. Thanks to the recently established composable security proof for discretely modulated CV QKD [16], we therefore can further derive its composable security under the finite-size effect. The calculation for the composable security key rate of the proposed QSS protocol is presented in Appendix A. As an example, the dashed lines in Fig. 5 depict the composable secret key rates of the DMCS-based QSS protocol in the situation in which only two users cooperatively communicate with the dealer. This situation belongs to the simplest QSS network, thereby maximizing the performance of the QSS protocol in theory. We find that the maximal transmission distance increases as the data block length increase, and it will be infinitely close to the asymptotic secret key rate shown by the blue line in Fig. 3. A similar trend also occurs when the number of users increases. That is to say, the data block length is a crucial parameter that would dramatically impact the performance of a realistic DMCS-based QSS system. It is worth noticing that this composable security of the DMCS-based QSS protocol is restricted to the hypothesis of

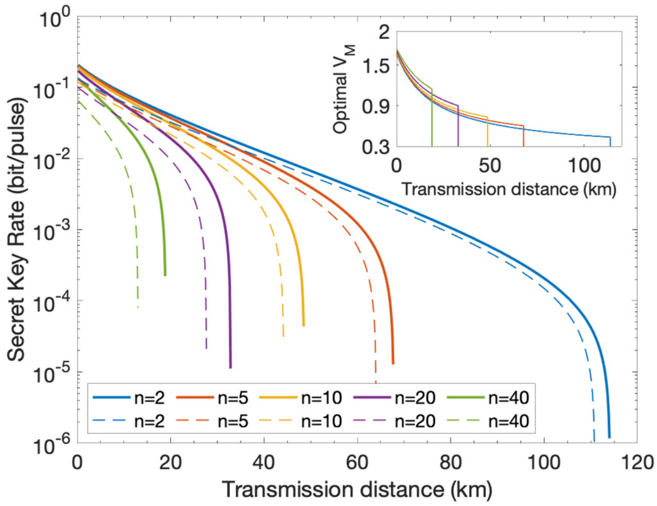

FIG. 6. Asymptotic secret key rates of the 8PSK-modulated QSS protocol (solid lines) and the QPSK-modulated QSS protocol (dashed lines) as a function of transmission distance. Inset: Optimal modulation variance of the 8PSK-modulated QSS protocol as a function of the transmission distance. From right to left in both the main figure and inset, the solid lines and dashed lines denote the number of users $n = 2$, $n = 5$, $n = 10$, $n = 20$, and $n = 40$.

collective Gaussian attacks. Under this assumption, we can efficiently estimate the parameters of the channel via maximum likelihood estimators and bound the corresponding error in the final secret key rate.

In addition, it is worth noting that the modulation strategy of DMCSs used for the above analysis is QPSK. Actually, there exist higher-dimensional discrete modulation strategies for DMCSs, such as eight-phase-shift keying (8PSK). Compared with QPSK, 8PSK allows each coherent state to carry three bits of information, thereby improving the transmission efficiency. Therefore, it will be valuable to investigate the proposed QSS protocol using the 8PSK-modulated state. A detailed derivation of the 8PSK-modulated state is presented in Appendix B. We do not present the whole process of the 8PSK-modulated QSS protocol here since it is very similar to QPSK-modulated QSS protocol described in Sec. II B. Now the question is whether the 8PSK-modulated QSS protocol is secure or not. As we analyzed before, the theoretical security of the QSS protocol depends on its longest two-party CV QKD link. That is to say, if we could find a way to prove the security of this CV QKD link, the 8PSK-modulated QSS protocol would be secure. Fortunately, the eight-state protocol, which exploits 8PSK-modulated coherent states as an information carrier in CV QKD, has been proven to be secure in the asymptotic limit [30]. Therefore, the security of the 8PSK-modulated QSS protocol can be proven by taking advantage of the security analysis technology of the eight-state protocol. Figure 6 depicts the asymptotic performance of the 8PSK-modulated QSS protocol and its optimal modulation variance at each transmission distance. For comparison, we also plot the asymptotic performance of the QPSK-modulated QSS protocol, shown by dashed lines. As expected, the 8PSK-modulated QSS protocol outperforms the QPSK-modulated QSS protocol in terms of both secret key rate and transmission distance when they have the same number of users. Therefore, the performance of the DMCS-based QSS protocol can be enhanced by adopting a higher-dimensional discrete modulation strategy.

V. CONCLUSION

In this work, we considered a quantum secret-sharing protocol which enables remote users to cooperatively share a secret key with the dealer. In particular, we implemented this protocol with discretely modulated coherent states. By tactfully exploiting the well-established security analysis technology of discretely modulated CV QKD, we proved the theoretical security of the proposed DMCS-based QSS protocol against both eavesdroppers (collective Gaussian attacks) and dishonest users. Mainly, the QPSK-modulated QSS protocol was analyzed; we showed that its maximal transmission distance in the asymptotic limit reaches more than 100 km but will be reduced when we consider its composable security. We also investigated the performance of the 8PSK-modulated QSS protocol; the result showed that the proposed QSS protocol can be enhanced by using a higher-dimensional discrete modulation strategy.

In summary, the proposed DMCS-based QSS protocol can meet the requirement of metropolitan quantum key sharing between multiple users. In a possible future study, we will introduce some non-Gaussian operations, such as photon subtraction and quantum catalysis, to further enhance the performance of the QSS protocol.

ACKNOWLEDGMENTS

Q. Liao would like to thank S. Pirandola and A. Leverrier for helpful discussions. We would also like to thank the anonymous referees for their constructive suggestions. This work is supported by the National Natural Science Foundation of China (Grant No. 61871407), the Hunan Provincial Natural Science Foundation of China (Grant No. 2020JJ5088), and the Fundamental Research Funds for the Central Universities (Grant No. 531118010371).

APPENDIX A: CALCULATION OF THE COMPOSABLE SECRET KEY RATE FOR THE DMCS-BASED QSS PROTOCOL

As we analyzed in the main text, the security of the DMCS-based QSS protocol can be guaranteed if the lowest secret key rate in all CV QKD links remains positive. Therefore, to consider the composable security of the proposed QSS protocol, we need to calculate the composable secret key rate of the longest CV QKD link in theory.

Let M be the total number of transmitted signals and m be the number of signals that are taken advantage of by parameter estimation with failure probability ϵ_{PE}. Setting $r = m/M$, the composable secret key rate of this link can be expressed as

$$R_{\text{comp}} \geqslant (1-r)p\Bigg[R_{\epsilon_{PE}} - \frac{\Delta_{AEP}\big(p\epsilon_s^2/3, |\mathcal{L}|\big)}{\sqrt{M(1-r)}} + \frac{\log_2\big[p\big(1-\epsilon_s^2/3\big)\big] + 2\log_2\sqrt{2}\epsilon_h}{M(1-r)}\Bigg], \quad \text{(A1)}$$

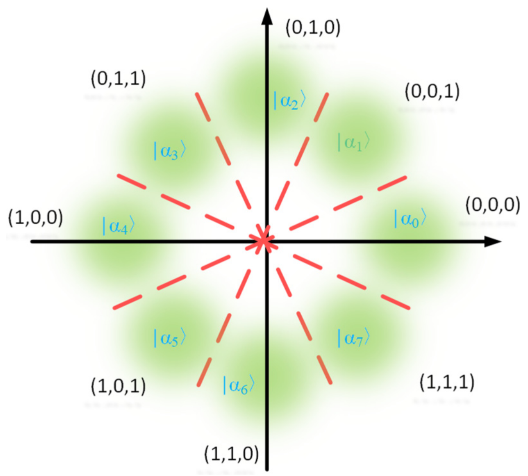

FIG. 7. Description of nonorthogonal states with the 8PSK format and the partition of phase space in four quadrants.

where p denotes the success probability of error correction and $R_{\epsilon_{PE}}$ is the finite-size expression of the key rate R of Eq. (11) which accounts for the imperfect parameter estimation and the reduced number of signals. This is given by replacing

$$R \rightarrow (1-r)R_{\epsilon_{PE}}. \tag{A2}$$

We have

$$\Delta_{AEP}(\epsilon_s, |\mathcal{L}|) := 4\log_2(2\sqrt{|\mathcal{L}|}+1)\sqrt{\log(2/\epsilon_s^2)}, \tag{A3}$$

where the parameter $|\mathcal{L}|$ is the cardinality of Bob's outcome; it is equal to 4 for QPSK. In our numerical simulation, the related parameters in Fig. 5 are set to $r = 0.01$, $p = 0.9$, and $\epsilon_s = \epsilon_h = \epsilon_{PE} = 10^{-10}$.

It is noteworthy that the above-mentioned parameter estimation, which is a crucial step for CV QKD, was detailed in both Refs. [12,16]; however, the former is designed for Gaussian-modulated protocols, while the latter is for protocols with discrete alphabets assuming a Gaussian channel. As our proposed DMCS-based QSS is based on discretely modulated CV QKD, our calculation is derived from Ref. [16].

APPENDIX B: DERIVATION OF THE 8PSK-MODULATED NONORTHOGONAL STATE

As we presented in Sec. II A, DMCSs can be generalized to the one with N quantum states $|\alpha_k^N\rangle = |\alpha e^{i2k\pi/N}\rangle$. One can consequently infer $|\alpha_k^8\rangle = |\alpha e^{i2k\pi/8}\rangle$ in the 8PSK modulation strategy. Figure 7 depicts a diagram of DMCSs using 8PSK modulation in phase space.

Similarly, DMCSs using 8PSK modulation can be deemed a pure state which defined as

$$|\Psi_8\rangle = \frac{1}{4}\sum_{k=0}^{7}|\psi_k^8\rangle|\alpha_k^8\rangle, \tag{B1}$$

where the states

$$|\psi_k^8\rangle = \frac{1}{2}\sum_{m=0}^{7}e^{i(1+4k)m\pi/4}|\phi_m^8\rangle \tag{B2}$$

are orthogonal non-Gaussian states. State $|\phi_m^8\rangle$ can be described as follows:

$$|\phi_k^8\rangle = \frac{e^{-\alpha^2/2}}{\sqrt{\lambda_k}}\sum_{n=0}^{\infty}e^{\frac{\alpha^{(8n+k)}}{\sqrt{(8n+k)!}}}|8n+k\rangle, \tag{B3}$$

with

$$\lambda_{0,4} = \frac{1}{4}e^{-\alpha^2}\bigg[\cosh(\alpha^2)+\cos(\alpha^2) \pm 2\cos\left(\frac{\alpha^2}{\sqrt{2}}\right)\cosh\left(\frac{\alpha^2}{\sqrt{2}}\right)\bigg], \tag{B4}$$

$$\lambda_{1,5} = \frac{1}{4}e^{-\alpha^2}\bigg[\sinh(\alpha^2)+\sin(\alpha^2) \pm\sqrt{2}\cos\left(\frac{\alpha^2}{\sqrt{2}}\right)\sinh\left(\frac{\alpha^2}{\sqrt{2}}\right) \pm\sqrt{2}\sin\left(\frac{\alpha^2}{\sqrt{2}}\right)\cosh\left(\frac{\alpha^2}{\sqrt{2}}\right)\bigg], \tag{B5}$$

$$\lambda_{2,6} = \frac{1}{4}e^{-\alpha^2}\bigg[\cosh(\alpha^2)-\cos(\alpha^2)\pm 2\sin\left(\frac{\alpha^2}{\sqrt{2}}\right)\sinh\left(\frac{\alpha^2}{\sqrt{2}}\right)\bigg], \tag{B6}$$

$$\lambda_{3,7} = \frac{1}{4}e^{-\alpha^2}\bigg[\sinh(\alpha^2)-\sin(\alpha^2) \mp\sqrt{2}\cos\left(\frac{\alpha^2}{\sqrt{2}}\right)\sinh\left(\frac{\alpha^2}{\sqrt{2}}\right) \pm\sqrt{2}\sin\left(\frac{\alpha^2}{\sqrt{2}}\right)\cosh\left(\frac{\alpha^2}{\sqrt{2}}\right)\bigg]. \tag{B7}$$

The sender prepares bipartite state $|\Psi_8\rangle$ with variance $V = V_M + 1$, where $V_M = 2\alpha^2$. The sender implements projective measurements on one of the set $|\psi_k^8\rangle\langle\psi_k^8|$ for $k \in \mathbb{Z}$ to the first half of $|\Psi_8\rangle$ and projects the second half of the set $|\psi_k^8\rangle\langle\psi_k^8|$ on one of the eight nonorthogonal states $|\alpha_k^8\rangle$. The modulated state is subsequently sent through an untrusted quantum channel. The covariance matrix of the modulated state can be expressed by

$$\Gamma_{AB}^8 = \begin{pmatrix} X\mathbb{I} & Z_8\sigma_z \\ Z_8\sigma_z & Y\mathbb{I} \end{pmatrix}, \tag{B8}$$

where

$$X = Y = 1+2\alpha^2,$$

$$Z_8 = 2\alpha^2\sum_{k=0}^{7}\lambda_{k-1}{}^{3/2}\lambda_k{}^{-1/2}. \tag{B9}$$

Here the addition arithmetic should be operated with modulo 8, and the remaining calculations are the same as for the QPSK-modulated state.

[1] S. Pirandola, U. L. Andersen, L. Banchi, M. Berta, D. Bunandar, R. Colbeck, D. Englund, T. Gehring, C. Lupo, C. Ottaviani, J. Pereira, M. Razavi, J. S. Shaari, M. Tomamichel, V. C. Usenko, G. Vallone, P. Villoresi, and P. Wallden, Adv. Opt. Photon **12**, 1012 (2020).

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

[3] Y. Zhang, Z. Li, Z. Chen, C. Weedbrook, Y. Zhao, X. Wang, Y. Huang, C. Xu, X. Zhang, Z. Wang, M. Li, X. Zhang, Z. Zheng, B. Chu, X. Gao, N. Meng, W. Cai, Z. Wang, G. Wang, S. Yu, and H. Guo, Quantum Sci. Technol. **4**, 035006 (2019).

[4] A. M. Lance, T. Symul, V. Sharma, C. Weedbrook, T. C. Ralph, and P. K. Lam, Phys. Rev. Lett. **95**, 180503 (2005).

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

[6] Q. Liao, G. Xiao, C.-G. Xu, Y. Xu, and Y. Guo, Phys. Rev. A **102**, 032604 (2020).

[7] Q. Liao, G. Xiao, H. Zhong, and Y. Guo, New J. Phys. **22**, 083086 (2020).

[8] F. Grosshans and P. Grangier, Phys. Rev. Lett. **88**, 057902 (2002).

[9] S. Fossier, E. Diamanti, T. Debuisschert, R. Tualle-Brouri, and P. Grangier, J. Phys. B **42**, 114014 (2009).

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

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

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

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

[14] S. Ghorai, P. Grangier, E. Diamanti, and A. Leverrier, Phys. Rev. X **9**, 021059 (2019).

[15] J. Lin, T. Upadhyaya, and N. Lütkenhaus, Phys. Rev. X **9**, 041064 (2019).

[16] P. Papanastasiou and S. Pirandola, Phys. Rev. Research **3**, 013047 (2021).

[17] C. Schmid, P. Trojek, M. Bourennane, C. Kurtsiefer, M. Żukowski, and H. Weinfurter, Phys. Rev. Lett. **95**, 230505 (2005).

[18] W. P. Grice and B. Qi, Phys. Rev. A **100**, 022339 (2019).

[19] F. E. Becerra, J. Fan, G. Baumgartner, J. Goldhar, J. T. Kosloski, and A. Migdall, Nat. Photonics **7**, 147 (2013).

[20] P. Huang, J. Fang, and G. Zeng, Phys. Rev. A **89**, 042330 (2014).

[21] A. Leverrier, Theoretical Study of Continuous-Variable Quantum Key Distribution, Ph.D thesis, Télécom ParisTech, 2009.

[22] R. García-Patrón and N. J. Cerf, Phys. Rev. Lett. **97**, 190503 (2006).

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

[24] M. Curty, M. Lewenstein, and N. Lütkenhaus, Phys. Rev. Lett. **92**, 217903 (2004).

[25] A. Ferenczi and N. Lütkenhaus, Phys. Rev. A **85**, 052310 (2012).

[26] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information* (Cambridge University Press, Cambridge, 2000).

[27] J. Lodewyck, M. Bloch, R. García-Patrón, S. Fossier, E. Karpov, E. Diamanti, T. Debuisschert, N. J. Cerf, R. Tualle-Brouri, S. W. McLaughlin, and P. Grangier, Phys. Rev. A **76**, 042305 (2007).

[28] Q. Liao, Y. Guo, D. Huang, P. Huang, and G. Zeng, New J. Phys. **20**, 023015 (2018).

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

[30] Y. Guo, R. Li, Q. Liao, J. Zhou, and D. Huang, Phys. Lett. A **382**, 372 (2018).