Non-Gaussian operations in measurement-device-independent quantum key distribution

Jaskaran Singh[*] and Soumyakanti Bose[†]
Department of Physical Sciences, Indian Institute of Science Education and Research (IISER) Mohali, Sector 81 SAS Nagar, Manauli, Punjab 140306, India

(Received 20 July 2021; revised 6 October 2021; accepted 27 October 2021; published 11 November 2021)

Non-Gaussian operations in continuous variable (CV) quantum key distribution (QKD) have been limited to photon subtraction on squeezed vacuum states only. This is mainly due to the ease of calculating the covariance matrix representation of such states. In this paper we study the effects of general non-Gaussian operations corresponding to photon addition, catalysis, and subtraction on squeezed coherent states on CV measurement-device-independent (MDI) QKD. We find that non-Gaussianity coupled with coherence can yield significantly longer transmission distances than without. Particularly we observe that zero photon catalysis on the two-mode squeezed coherent state (TMSC) is an optimal choice for CV MDI QKD, while single photon subtraction is also a good candidate; both of them offer nearly 70 km of transmission distances. We also derive a single generalized covariance matrix for the aforementioned states which will be useful in several other aspects of CV quantum information processing.

DOI: 10.1103/PhysRevA.104.052605

I. INTRODUCTION

Quantum key distribution (QKD) [1,2] is one of the most widely known and commercially available applications of quantum information theory. It provides a measure of security that is not possible to achieve using classical key distribution schemes. While the latter protocols are traditionally deemed secure by virtue of some computationally hard to solve mathematical problem, the security of the former is based on a principle of nature like the Heisenberg uncertainity principle [3,4], the no-cloning theorem [5–8], and Bell's theorem [9–11]. Ideally, QKD protocols are unconditionally secure [12–15], but noise in the measurement and preparation devices may cause the security to be entirely compromised. For this purpose certain assumptions and pre-conditions have to be imposed on all the devices available to the parties, Alice and Bob. However, in order for the protocol to be practical, it is desirable for the assumptions to be minimal. For example, the standard BB84 protocol assumes that the parties share a single qubit state and have access to dichotomic measurements only.

Among all, measurement device independent (MDI) is a prominent class of QKD protocols [16–22], based on entanglement swapping, which work under the assumption that the state preparation devices with Alice and Bob are well characterized such that an eavesdropper, Eve, has no access to any side channels, while the measurement devices are uncharacterized and untrusted. With this, continuous variable (CV) MDI QKD protocols [23–28] further boast of longer transmission distances that can encompass a small metropolitan city, in comparison to the discrete variable counterparts [29,30].

While CV MDI QKD has been well studied using Gaussian states like the two-mode squeezed vacuum (TMSV), few recent studies have shown that non-Gaussianity [31–39] and coherence [40] can have a major impact on maximizing the transmission distances. It might be noted that the desired non-Gaussianity could be induced in many ways such as photon subtraction, photon addition, catalysis, etc. While the case of photon subtraction has been studied in full depth, the process of photon catalysis has been explored to some extent. Furthermore, the impact of coherence on CV MDI QKD protocols has only been made possible in the case of photon subtraction, where it was shown to be quite advantageous [40]. However, a general treatment of these non-Gaussian processes along with fiducial coherence has not been attempted due to the difficulty in obtaining a closed form solution for the covariance matrix—a primary ingredient in Gaussian-modulated CV QKD.

In this paper we derive a generalized covariance matrix for processes corresponding to photon addition, photon subtraction, and catalysis on two-mode squeezed coherent states (PATMSC, PSTMSC, and CTMSC, respectively), which to the best of our knowledge has not been attempted before. The covariance matrix takes into account the number of photons added, subtracted, or catalyzed as parameters which can be chosen arbitrarily. Furthermore, we introduce displacement (coherence) as a parameter, too, which can also be chosen arbitrarily. Coupled with all the parameters, our covariance matrix is the most general one attempted to date and apart from its immediate application in QKD, it is expected to be of immense interest in other non-Gaussian information processing tasks such as quantum teleportation, entanglement swapping [41,42], quantum internet [43], etc.

We provide a detailed discourse on the impact of non-Gaussianity coupled with small displacements on CV MDI QKD protocols. Such a discourse would be of immense in-

[*] jsinghiiser@gmail.com
[†] soumyakanti.bose09@gmail.com

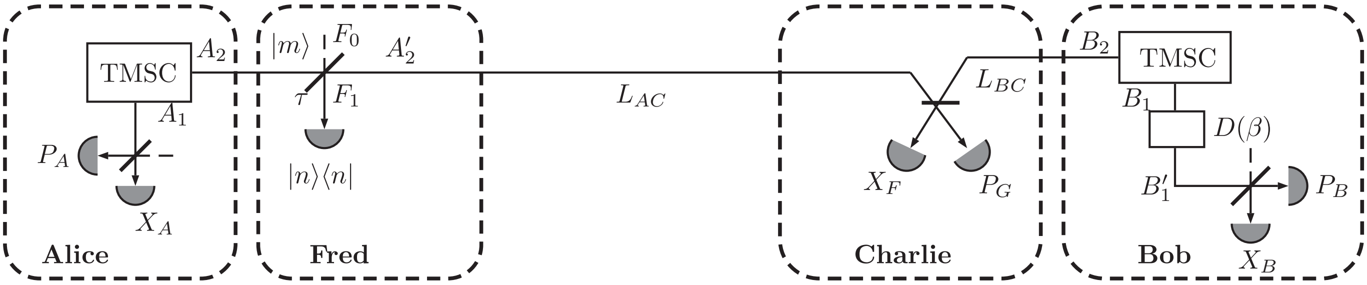

FIG. 1. Scheme to implement CV MDI QKD using non-Gaussian states. Two trusted parties Alice and Bob produce TMSC states while a third untrusted party Fred performs photon addition, subtraction, or catalysis. A fourth untrusted party Charlie performs homodyne measurements on the two modes obtained from Fred and Bob after mixing them via a BS. The results of Charlie's measurements are declared publicly.

terest to experimentalists in selecting the most optimal state for QKD based on transmission distances, noise robustness, and/or coherence. While it has already been shown that a small amount of coherence is an actually helpful process in the case of photon subtraction [40], we find that it is true for photon addition and catalysis, too. This reinforces the idea that non-Gaussianity coupled with coherence leads to better performance in CV MDI QKD. Particularly, we find that the CTMSC state outperforms the other states in both the aforemetioned criterion allowing transmission distances of almost 70 Km, while photon subtraction is equivalently a good candidate, too. We also find that addition of photons is not an adequate process to introduce non-Gaussianity in CV MDI QKD protocols as it does not lead to any significant increase in transmission distances.

The paper is organized as follows: In Sec. II we provide a brief idea of CV MDI QKD with Gaussian states followed by corresponding cases with non-Gaussian operations such as photon subtraction, addition, and catalysis. In this section we also discuss the process to calculate secure key rates. Section III presents our simulation results on experimentally obtainable key rates. In Sec. IV we summarize our results.

II. CV MDI QKD USING CTMSC, PATMSC, AND PSTMSC

In this section we first provide a brief overview of CV MDI QKD using Gaussian states. We then describe the scenario where non-Gaussian states can be utilized. We then elucidate how secure key rates are to be computed.

A. Gaussian CV MDI QKD

Consider two parties Alice and Bob who wish to share a secure key. Each party prepares a TMSV state with quadrature variances $V_A = V_B$, respectively. The two modes with each party are labeled as A_1, A_2 and B_1, B_2, respectively. Alice and Bob transmit the modes A_2 and B_2 to a third untrusted party, Charlie, while retaining the modes A_1 and B_1 with themselves. These modes are transmitted via quantum channels of length L_{AC} and L_{BC} respectively. The total transmission distance between Alice and Bob is then $L = L_{AC} + L_{BC}$.

Charlie interferes the two modes with the help of a 50:50 beam splitter (BS) which has two output modes C and D. He then performs a homodyne measurement of x quadrature on C and p quadrature on D to obtain outcomes X_C and P_D, respectively. The obtained outcomes $\{X_C, P_D\}$ are then publicly announced by Charlie. Subsequently, Bob performs a displacement operation $D(\alpha)$ on his retained mode B_1 to get B_1', where $\alpha = g(X_C + iP_D)$ and g is the gain factor.

After these operations, the modes A_1 and B_1' are found to be entangled. Alice and Bob then perform heterodyne measurements on their entangled modes to obtain the outcomes $\{X_A, P_A\}$ and $\{X_B, P_B\}$ which are correlated. The scheme is given in Fig. 1 with the exception of Fred.

Finally, both the parties perform information reconciliation and privacy amplification to obtain a secure key.

B. CV MDI QKD using non-Gaussian states

The scenario of CV MDI QKD which utilizes non-Gaussian states is quite similar to the Gaussian CV MDI QKD, with the exception of an additional untrusted party Fred who acts on the mode A_2 as shown in Fig. 1. We also assume that Bob performs reverse reconciliation (RR), which implies that his outcomes are taken to be as a reference for Alice to reconcile with.

We describe the basic scheme of our protocol with relevant calculations done in the Appendix. We make use of phase space methods (particularly Wigner functions) to perform the calculations. The protocol proceeds as follows:

Step 1. Alice prepares a TMSC state $|\psi\rangle_{A_1A_2}$ with quadrature variance $V_A = \cosh(2r)$. Such a state can be achieved by using a nonlinear optical downconverter and the process is described as

$$|\psi\rangle_{A_1A_2} = S_{12}(r)D_1(d)D_2(d)|00\rangle, \qquad (1)$$

where $S_{12}(r) = \exp[r(\hat{a}^\dagger_{A_1}\hat{a}^\dagger_{A_2} - \hat{a}_{A_1}\hat{a}_{A_2})]$ is the squeezing operator with parameter r while $D_i(d) = \exp[d(\hat{a}^\dagger_{A_i} - \hat{a}_{A_i})]$ is the displacement operator displacing mode A_i only along the x quadrature with magnitude d.

Step 2. Alice then transmits the mode A_2 to the untrusted party Fred, who mixes it with the mode F_0 through a BS with transmittivity τ. The mode F_0 is initialized in the state $|m\rangle\langle m|$. The corresponding transformation $\mathcal{U}^{\mathrm{BS}}_{A_2F_0}$ is described as

$$\mathcal{U}^{\mathrm{BS}}_{A_2F_0} : |\psi\rangle_{A_1A_2}|m\rangle_{F_0} \to |\Psi\rangle_{A_1A_2'F_1}. \qquad (2)$$

Using a photon number resolving detector (PNRD), Fred then performs a projective measurement $\{|n\rangle\langle n|, \mathbb{1} - |n\rangle\langle n|\}$ on the mode F_1, where $|n\rangle\langle n|$ corresponds to n photons being detected. As a consequence, for the modes A_1 and A_2',

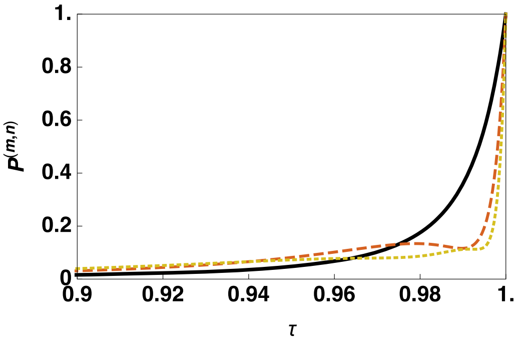

FIG. 2. Probability of photon catalysis as a function of BS transmittance τ. The parameters are fixed as $V_A = 50$ and displacement $d = 2$. Various plots correspond to (0, 0)-CTMSC (black solid), (1, 1)-CTMSC (red dashed), and (2, 2)-CTMSC (yellow tiny dashed). Plotted parameters are dimensionless.

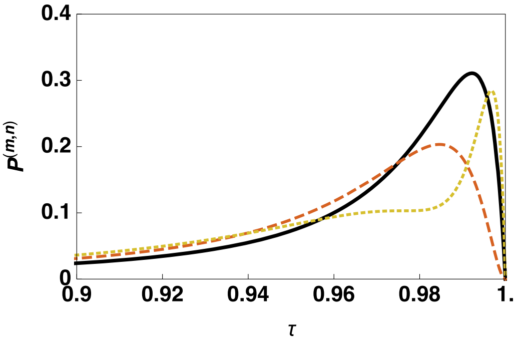

FIG. 3. Probability of photon addition as a function of BS transmittance τ. The parameters are fixed as $V_A = 50$ and displacement $d = 2$. Various plots correspond to (1, 0)-PATMSC (black solid), (2, 0)-PATMSC (red dashed), and (2, 1)-PATMSC (yellow tiny dashed). Plotted parameters are dimensionless.

we call the resultant two-mode state (m, n)-TMSC and it is given by the unnormalized state $|\Psi\rangle^{(m,n)}_{A_1A'_2} = {}_{F_1}\langle n|\Psi\rangle_{A_1A'_2F_1}$. The normalization is the probability of n photon detections and is given as

$$P^{(m,n)} = \sum_r \sum_s \left|{}_{A_1}\langle r|_{A'_2}\langle s|\Psi\rangle^{(m,n)}_{A_1A'_2}\right|^2. \quad (3)$$

At this stage one may consider various cases by choosing different combinations of m and n. Here we broadly classify all these cases into three categories.

$m = n$: In this case, the number of input photons is equal to the number of detected photons in the mode F_1. This case is popularly known as photon catalysis [44] and leads to non-Gaussian states even for $m = n = 0.m < n$: In this case the number of photons detected in the mode F_1 is more than the input number of photons in the mode F_0. This leads to an overall deduction in the number of photons in the original TMSC state leading to a photon subtracted state. Hence the name photon subtraction. The resultant state is a non-Gaussian state.$m > n$: In this case, the number of photons detected in the mode F_1 is less than the number of photons input in the mode F_0. This way we can add to the total number of photons in the original TMSC state, with the resultant state being non-Gaussian.

We denote these cases as photon catalyzed TMSC (CTMSC), photon subtracted TMSC (PSTMSC), and photon added TMSC (PATMSC), respectively. The latter has been studied in depth in Ref. [40]. The probability of n photon detections as a function of τ is plotted in Figs. 2, 3 and 4 corresponding to CTMSC, PATMSC, and PSTMSC. It should be noted that the value of τ used throughout the paper is optimized to maximize the transmission distance and not photon detection.

Fred has to publicly announce when the required (m, n)-TMSC state has been prepared. Thus, it is natural to assume that any and all modes of Fred can be accessed by an eavesdropper Eve. This also allows us to have the device with Fred to be fully uncharacterized such that there may exist information side channels to Eve. Thus, for the remainder of this paper we assume that Fred is an untrusted party and separate from Alice.

The position of Fred plays also plays an important role in non-Gaussian CV MDI QKD. Fred can either be placed only on Alice's side (before Charlie), on Bob's side (after Charlie), or on both sides. However, placing Fred between Bob and Charlie will not offer any advantage as the parties will apply classical reverse reconciliation techniques to extract a secure correlated key rate. In this case, Bob will try to align his bits to that of Alice's. It is therefore the case that Alice's source prepares the information that is sent to Bob, while Bob's state is only used to guess the bit of Alice. Therefore, placing Fred between Bob and Charlie will not provide any benefit. Moreover, placing Fred at both the locations (between Alice-Charlie and Bob-Charlie) will eventually be extremely detrimental as the probability of detecting n photons simultaneously on modes A_2, B_2 is very low. Consequently, we have considered the case where Fred lies between Alice and Charlie.

The location of Fred can be further chosen to be either close to Alice, in between Alice and Charlie, or close to Charlie. The main purpose of Fred is to increase the entanglement between the modes A_1 and A'_2 by performing non-Gaussian operations through photon detection on the Gaussian TMSC state. Therefore, if Fred is close to Charlie, he will be per-

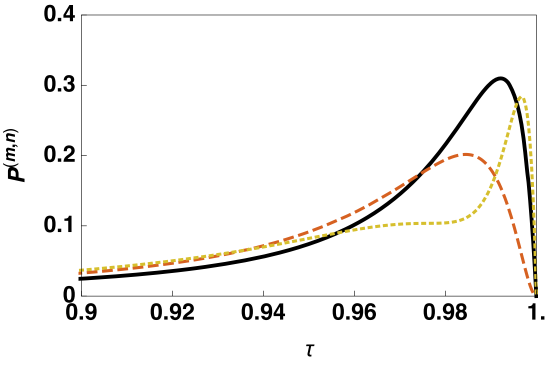

FIG. 4. Probability of photon subtraction as a function of BS transmittance τ. The parameters are fixed as $V_A = 50$ and displacement $d = 2$. Various plots correspond to (0, 1)-PSTMSC (black solid), (0, 2)-PSTMSC (red dashed), and (1, 2)-PSTMSC (yellow tiny dashed). Plotted parameters are dimensionless.

forming photon detections on a state which has already passed through a lossy channel and undergone noise. The state that he receives is a mixed state with less entanglement than the initial TMSC state. Therefore, photon detections on this state will result in a final state with lower entanglement content than the final state generated if he were located close to Alice. This, in turn, can lead to lesser key rate or transmission distance. Thus in the rest of this paper we assume that Fred is located close to Alice.

We calculate the covariance matrix of (m, n)-TMSC in terms of moment generating functions and is given as

$$\Sigma_{A_1A_2'} = \begin{pmatrix} V_A^x & 0 & V_C^x & 0 \\ 0 & V_A^p & 0 & V_C^p \\ V_C^x & 0 & V_B^x & 0 \\ 0 & V_C^p & 0 & V_B^p \end{pmatrix}, \tag{4}$$

where V_i^ξ, $i \in \{A, B, C\}$ and $\xi \in \{x, p\}$ is interpreted as variance of ξ quadrature for the i^{th} party (see Appendix C). Fred announces when the (m, n)-TMSC state has been successfully prepared and consequently the mode A_2' is transmitted to Charlie via a quantum channel.

Step 3. Bob also prepares a TMSC state with variance $V_B = V_A$ and transmits the mode B_2 to Charlie.

Step 4. Charlie mixes the two modes A_2' and B_2 via a BS with output modes C and D. He then performs a homodyne measurement of x and p quadrature on C and D, respectively. The outcomes to these measurements are then declared publicly.

Step 5. Based on the publicly declared results, Bob displaces his mode B_1 to B_1' by applying $D(\alpha)$. As a consequence the modes A_1 and B_1' are entangled.

Step 6. Alice and Bob perform heterodyne measurements on the entangled modes A_1 and B_1' to get correlated outcomes.

Step 7. Alice and Bob perform information reconciliation and privacy amplification to obtain a secure key. Here we follow reverse reconciliation [45] (from Bob to Alice) as it is more secure and is known to perform better [46].

C. Eavesdropping, channel parameters, and secure key rate

In this subsection we describe several parameters which will be useful in simulating the secure key rates obtained by Alice and Bob in the presence of an eavesdropper Eve. While most of the terminology has been set up in Ref. [40], we recap it here for brevity of the reader.

The CV MDI QKD protocol detailed above comprises two quantum channels between Alice, Bob, and Charlie and a single classical channel between Alice and Bob. We assume that Eve can perform independent one-mode collective attacks [19,25,47] on each channel and the maximum information that can be obtained is then quantified by the Holevo bound χ_{BE} between Bob and Eve.

We assume that the two channels have transmittance T_A and T_B, given as

$$T_A = 10^{-l\frac{L_{\text{AC}}}{10}} \quad \text{and} \quad T_B = 10^{-l\frac{L_{\text{BC}}}{10}}, \tag{5}$$

where $l = 0.2$ dB/Km is the channel loss. Furthermore, we only consider the asymmetric case in which $L_{\text{BC}} = 0$, implying Bob and Charlie are at the same place. The total transmission length is then $L = L_{\text{AC}} = L_{\text{AB}}$ with $T_B = 1$. The symmetric case in which Charlie is midway between Alice and Bob has been found to be more subpar than the asymmetric one in several previous results [34,40].

We define a normalized parameter T associated with channel transmittance in terms of T_A as

$$T = \frac{T_A g^2}{2}, \tag{6}$$

where g is the gain of Bob's displacement operation. Total added noise in the channel can then be defined as

$$\chi_{\text{line}} = \frac{1 - T}{T} + \varepsilon_{th}, \tag{7}$$

where ε_{th} is the thermal excess noise in the equivalent one-way protocol [34] which can be written as

$$\varepsilon_{th} = \frac{T_B}{T_A}(\varepsilon_B - 2) + \varepsilon_A + \frac{2}{T_A}, \tag{8}$$

where ε_A and ε_B correspond to thermal excess noise in the respective quantum channels. The gain is then taken as

$$g = \sqrt{\frac{2(V_A - 1)}{T_B(V_A + 1)}}, \tag{9}$$

in order to minimize ε_{th}.

We also assume that Charlie's homodyne detectors are noisy, with excess noise given as

$$\chi_{\text{homo}} = \frac{v_{el} + 1 - \eta}{\eta}, \tag{10}$$

where, v_{el} is the electric noise of the detectors and η is the efficiency. Therefore, the total noise added because of the channel and detectors is

$$\chi_{\text{tot}} = \chi_{\text{line}} + \frac{2\chi_{\text{homo}}}{T_A}. \tag{11}$$

The secure key rate obtained by Alice and Bob is given as

$$K = P^{(m,n)}(\beta I_{\text{AB}} - \chi_{\text{BE}}), \tag{12}$$

where $P^{(m,n)}$ is the probability to obtain the (m, n)-TMSC state given in Eq. (3), I_{AB} is the mutual information between Alice and Bob and χ_{BE} is the Holevo bound between Bob and Eve. The factor $P^{(m,n)}$ appears in Eq. (12) because the final (m, n)-TMSC state is obtained probabilistically depending on the detection of n photons. Thus the final resource is a fraction of the initial TMSC state.

The covariance matrix corresponding to the state $\rho_{A_1B_1'}$ which is obtained after Step 5 of the protocol is

$$\Sigma_{A_1B_1'} = \begin{pmatrix} V_A^x & 0 & \sqrt{T}V_C^x & 0 \\ 0 & V_A^p & 0 & \sqrt{T}V_C^p \\ \sqrt{T}V_C^x & 0 & TV_B'^x & 0 \\ 0 & \sqrt{T}V_C^p & 0 & TV_B'^p \end{pmatrix}, \tag{13}$$

where $V_B'^\xi = V_B^\xi + \chi_{\text{tot}} I_2$ and V_B^ξ is the variance of $\xi \in \{x, p\}$ quadrature for Bob's state.. The mutual information between Alice and Bob, I_{AB} can then be calculated as

$$I_{\text{AB}} = \frac{1}{2}\log_2\left(\frac{V_{A_M}^x}{V_{A_M|B_M}^x}\right) + \frac{1}{2}\log_2\left(\frac{V_{A_M}^p}{V_{A_M|B_M}^p}\right), \tag{14}$$

such that

$$V_{A_M}^{\xi} = \frac{V_A^{\xi} + 1}{2}, \tag{15}$$

where $V_{A_M|B_M}^{\xi}$ is the conditional variance of Alice's outcome conditioned on Bob's outcome of his heterodyne measurement given by

$$V_{A_M|B_M}^{\xi} = \frac{V_{A|B}^{\xi} + 1}{2}, \tag{16}$$

where

$$V_{A|B}^{\xi} = V_A^{\xi} - V_C^{\xi}\left(V_B^{\xi} + I_2\right)^{-1}\left(V_C^{\xi}\right)^T. \tag{17}$$

In order to calculate the Holevo bound χ_{BE}, we assume that Eve also has access to Fred's mode F and her state is then given by ρ_{EF}. We also assume that she can purify $\rho_{A_1B_1'\mathrm{EF}}$. The Holevo bound χ_{BE} between Bob and Eve can then be calculated as

$$\begin{aligned}\chi_{\mathrm{BE}} &= S(\rho_{\mathrm{EF}}) - \int dm_B\, p(m_B) S\left(\rho_{\mathrm{EF}}^{m_B}\right)\\ &= S\left(\rho_{A_1B_1'}\right) - S\left(\rho_{A_1}^{m_{B_1'}}\right),\end{aligned} \tag{18}$$

where $S(\rho)$ is the von-Neumann entropy of the state ρ, m_B represents measurement outcomes of Bob with probability density $p(m_B)$, and $\rho_{\mathrm{EF}}^{m_B}$ is the state of Eve conditioned on Bob's outcome. The covariance matrices corresponding to the states $\rho_{A_1B_1'}$ and $\rho_{A_1}^{m_{B_1'}}$ are represented by $\Sigma_{A_1B_1'}$ and $\Sigma_{A_1}^{m_{B_1'}}$, respectively. The von-Neumann entropy $S(\rho_{A_1B_1'})$ and $S(\rho_{A_1}^{m_{B_1'}})$ are functions of symplectic eigenvalues λ_1, λ_2 of $\Sigma_{A_1B_1'}$, and λ_3 of $\Sigma_{A_1}^{m_{B_1'}}$ which are given as

$$S(\rho_{A_1B_1'}) = G\left[\frac{\lambda_1 - 1}{2}\right] + G\left[\frac{\lambda_2 - 1}{2}\right], \tag{19}$$

and

$$S\left(\rho_{A_1}^{m_{B_1'}}\right) = G\left[\frac{\lambda_3 - 1}{2}\right], \tag{20}$$

with

$$G(x) = (x+1)\log_2(x+1) - x\log_2 x \tag{21}$$

the von-Neumann entropy of the thermal state.

III. SIMULATION RESULTS

In this section we provide numerical results corresponding to the aforementioned non-Gaussian operations on a TMSC state. For each case we analyze the effects of coherence and non-Gaussianity on key rate and transmission distances.

A. Effect of displacement for a fixed key rate

In this subsection we analyze the effect of displacement on transmission distances for a fixed key rate corresponding to CTMSC, PATMSC, and PSTMSC.

As is evident from Fig. 5, in the case of CTMSC, transmission distance decreases monotonically with increased displacement, with a maximum distance of 70 km achieved for $K = 10^{-4}$ bits/pulses. Therefore, catalysis on TMSC or TMSV yields equivalent results with no increase in transmission distances and it is therefore preferable to use minimal or no displacement. On the other hand, photon addition on the TMSC state is more advantageous than TMSV as is evident from Fig. 6. Photon subtraction on the TMSC state also offers a significant improvement in transmission distances over TMSV as shown in Fig. 7. It is seen that transmission

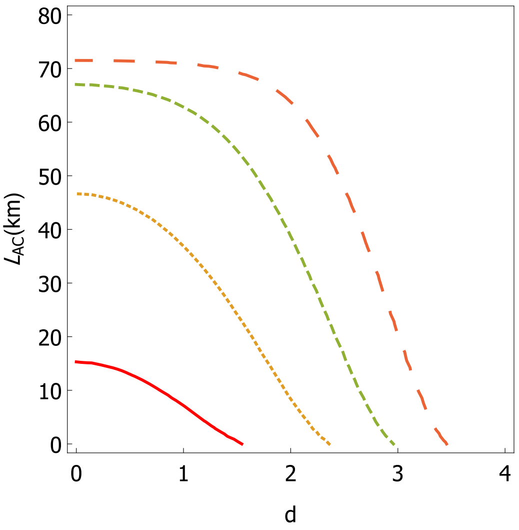

FIG. 5. Contour plot of displacement d (dimensionless) and transmission distance L_{AC} (km) in the extreme asymmetric case as a function of key rate (bits/pulses) for the case of (0, 0)-CTMSC. The parameters are fixed as $V_A = 50$, $\tau = 0.9$, $\epsilon_A^{th} = 0.002 = \epsilon_B^{th}$, $\beta = 96\%$. Various curves correspond to different values of fixed key rate $K = 10^{-1}$ (red solid), $K = 10^{-2}$ (tiny dashed), $K = 10^{-3}$ (dashed), and $K = 10^{-4}$ (large dashed).

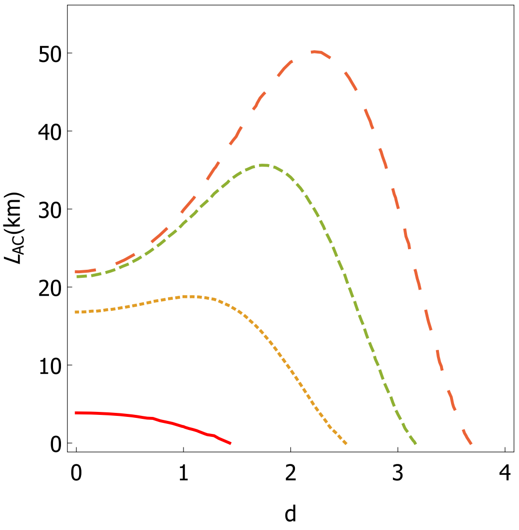

FIG. 6. Contour plot of displacement d (dimensionless) and transmission distance L_{AC} (km) in the extreme asymmetric case as a function of key rate (bits/pulses) for the case of (1, 0)-PATMSC. The parameters are fixed as $V_A = 50$, $\tau = 0.9$, $\epsilon_A^{th} = 0.002 = \epsilon_B^{th}$, $\beta = 96\%$. Various curves correspond to different values of fixed key rate $K = 10^{-1}$ (red solid), $K = 10^{-2}$ (tiny dashed), $K = 10^{-3}$ (dashed), and $K = 10^{-4}$ (large dashed).

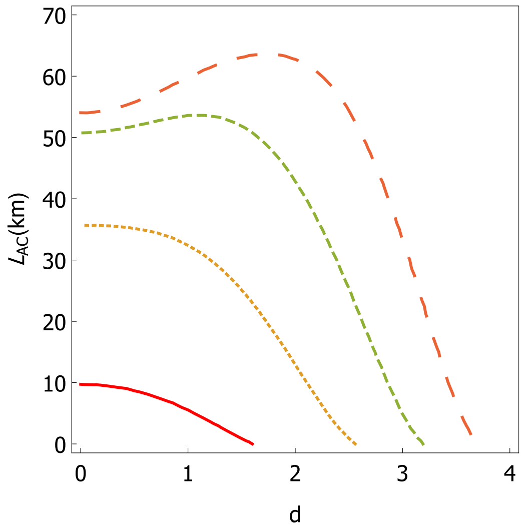

FIG. 7. Contour plot of displacement d (dimensionless) and transmission distance $L_{\rm AC}$ (km) in the extreme asymmetric case as a function of key rate (bits/pulses) for the case of (0, 1)-PSTMSC. The parameters are fixed as $V_A = 50$, $\tau = 0.9$, $\epsilon_A^{th} = 0.002 = \epsilon_B^{th}$, $\beta = 96\%$. Various curves correspond to different values of fixed key rate $K = 10^{-1}$ (red solid), $K = 10^{-2}$ (tiny dashed), $K = 10^{-3}$ (dashed), and $K = 10^{-4}$ (large dashed).

distances increase drastically with increasing displacement. However, we also note that displacement cannot be increased indefinitely as it begins to have detrimental effects on the transmission distance. A maximum distance of 50 km can be achieved with $K = 10^{-4}$ for $d \approx 2$.

The apparent nonmonotonic behavior of the key rate with displacement could be understood in terms of the interplay between the success probability ($P^{(m,n)}$) and the difference between mutual information and Holevo information ($I_{\rm AB} - \chi_{\rm BE}$). Here, we explain for the case of single photon subtracted TMSC-(0, 1)−PSTMSC. As can be seen in Fig. 8, for a fixed BS transmittivity τ, with an increase in the displacement amplitude (d), the probability of photon subtraction drops, while simultaneously, the difference between $I_{\rm AB}$ and $\chi_{\rm BE}$ increases. This results in an increase in the key rate ($K = P^{(m,n)}(\beta I_{\rm AB} - \chi_{\rm BE})$) up to $d \approx 2$. However, for larger displacement ($d > 2$), while the difference between $I_{\rm AB}$ and $\chi_{\rm BE}$ saturates the success probability falls drastically. As a consequence, the overall key rate falls beyond the optimal displacement which in our case is $d = 2$.

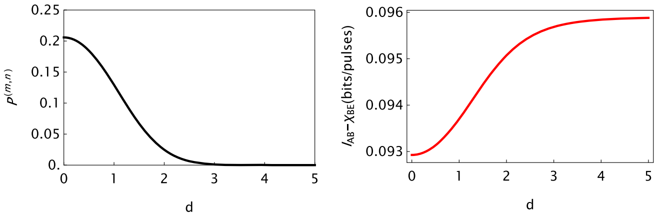

FIG. 8. Plot of probability $P^{(m,n)}$ and $I_{\rm AB} - \chi_{\rm BE}$ (bits/pulse) with displacement d for the case of $(0, 1) -$ PSTMSC with parameters $V_A = 50$, $\tau = 0.9$, $\epsilon_A^{th} = 0.002 = \epsilon_B^{th}$, $\beta = 100\%$, and $L_{\rm AC} = L_{\rm AB} =$ 50 km. The latter plot shows a gradual increase up to a certain maximum value with increasing d, while the former reaches zero just before $d = 3$.

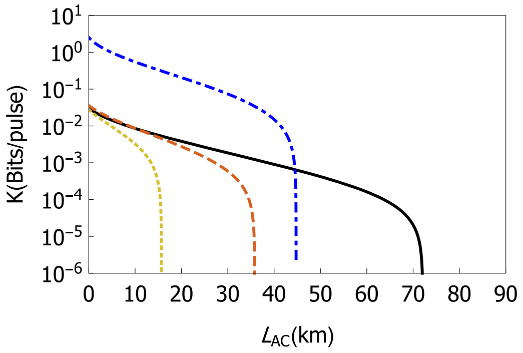

FIG. 9. Secret key rate as a function of $L_{\rm AC}$ in the extreme asymmetric case. The parameters are fixed as $V_A = 50$, $\tau = 0.9$, $\epsilon_A^{th} = 0.002 = \epsilon_B^{th}$, $\beta = 96\%$, and displacement $d = 2$. Various plots correspond to TMSV (blue dash dotted), (0, 0)-CTMSC (black solid), (1, 1)-CTMSC (red dashed), and (2, 2)-CTMSC (yellow tiny dashed).

Photon subtraction on TMSC has been studied extensively in a previous study [40]. For the sake of completion we reproduce the same results, albeit using the generalized covariance matrix as derived in this paper. From Fig. 7, we conclude that displacement can effectively increase the transmission distances of CV-MDI QKD protocols.

B. Effect of length on key rate

In this subsection we analyze the available key rate with respect to transmission distances in the extreme asymmetric case.

From Fig. 9 we find that the (0, 0)-CTMSC state offers a dramatic increase in transmission distances as compared to the (1, 1)-, (2, 2)-CTMSC and TMSV states. A maximum distance of more than 70 km can be achieved using the same. However, (1, 1) and (2, 2)-CTMSC fare more poorly than even the TMSV state.

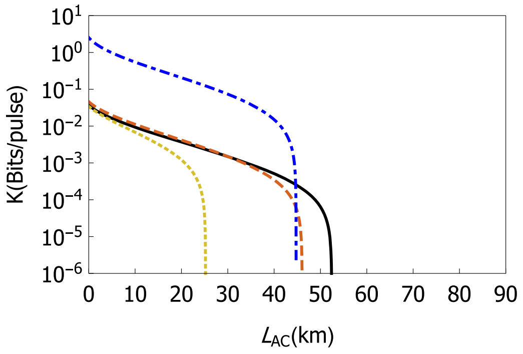

FIG. 10. Secret key rate as a function of $L_{\rm AC}$ in the extreme asymmetric case. The parameters are fixed as $V_A = 50$, $\tau = 0.9$, $\epsilon_A^{th} = 0.002 = \epsilon_B^{th}$, $\beta = 96\%$, and displacement $d = 2$. Various plots correspond to TMSV (blue dash dotted), (1, 0)-PATMSC (black solid), (2, 0)-PATMSC (red dashed), and (2, 1)-PATMSC (yellow tiny dashed).

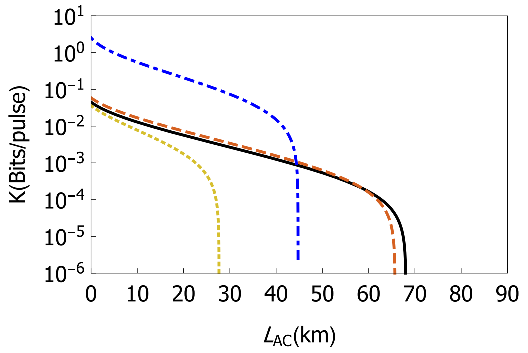

FIG. 11. Secret key rate as a function of L_{AC} in the extreme asymmetric case. The parameters are fixed as $V_A = 50$, $\tau = 0.9$, $\epsilon_A^{th} = 0.002 = \epsilon_B^{th}$, $\beta = 96\%$, and displacement $d = 2$. Various plots correspond to TMSV (blue dash dotted), (0, 1)-PSTMSC (black solid), (0, 2)-PSTMSC (red dashed), and (1, 2)-PSTMSC (yellow tiny dashed).

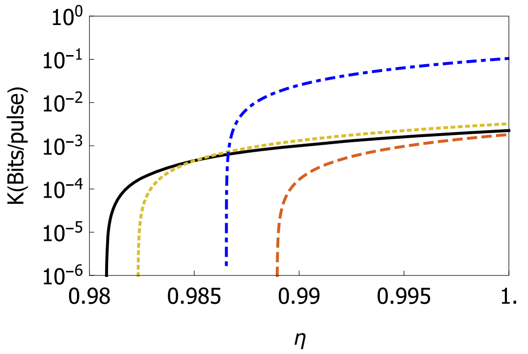

FIG. 12. Secret key rate as a function of detection inefficiency η (dimensionless) in the extreme asymmetric case. The parameters are fixed as $L_{AC} = 20$ km, $\tau = 0.9$, $\epsilon_A^{th} = 0.002 = \epsilon_B^{th}$, $\beta = 96\%$, and displacement $d = 2$. Various plots correspond to TMSV (blue dash dotted), (0, 0)-CTMSC (black solid), (1, 0)-PATMSC (red dashed), and (0, 1)-PSTMSC (yellow tiny dashed).

As is evident from Fig. 10, the (1, 0)-PATMSC state offers better transmission distances than the (2, 0)-, (2, 1)-PATMSC, and TMSV states. However, the distances are still comparatively smaller than what was observed for the (0, 0)-CTMSC state.

From Fig. 11, it is clear that (0, 1) and (0, 2)-PSTMSC states offer equally good key rates for large transmission distances than either the (1, 2)-PSTMC or TMSV state. It should also be noted that photon subtraction is the only case (considered so far) that offers a substantial improvement in transmission distances for single as well as two-photon operations.

From the above analysis it is clear that the (0, 0)-CTMSC state offers the highest transmission distance. However, (0, 1)- and (0, 2)-PSTMSC states offer a similar performance. Since the experimental implementation of both is more or less the same, these states should be preferred for CV MDI QKD.

One of the major factors limiting transmission distances (and equivalently the secure key rate) is the noise added to the channel and how it affects each state correspondingly. More noise will imply smaller transmission distances and vice versa. The channel parameters that we have chosen in our plots are achievable in the laboratory while detection inefficiency with Charlie is assumed to zero. In the next subsection we look at the effect of noisy homodyne detections with Charlie, which results in added noise in the channel between Alice and Bob.

C. Noisy homodyne detection

In this subsection we analyze the key rate under noisy homodyne detectors with Charlie. We observe that under noise the transmission distances are affected greatly.

From Fig. 12, we see that (0, 0)-CTMSC state is the most robust under detector noise, while photon addition has the worst response. Photon subtraction is also seen to perform adequately as compared to others. It should also be noted that the key rate for all cases except TMSV is quite low around approximately $K \approx 10^{-3}$ bits/pulses.

The total transmission distance is also seen to suffer under detector noise in Fig. 13. A maximum distance of approximately 29 km can be achieved by using (0, 0)-CTMSC, while (0, 1)-PSTMSC is not far behind. It is again observed that the photon added state performs even worse than the TMSV state.

IV. CONCLUSION

In this paper we derived a generalized covariance matrix for non-Gaussian states comprising CTMSC, PATMSC, and PSTMSC. The number of photons to be catalyzed, added, or subtracted as well as squeezing and displacement are taken as parameters to this covariance matrix. Using the generalized covariance matrix we analyze performance of the aforementioned non-Gaussian states in CV MDI QKD. We find that the (0, 0)-CTMSC state offers the best possible choice of state as it affords a longer transmission distance and is robust against white noise. However, (0, 1)-PSTMSC is also equivalently good. We found that PATMSC states are not an optimal choice in CV MDI QKD, but are still better than standard Gaussian states in some cases.

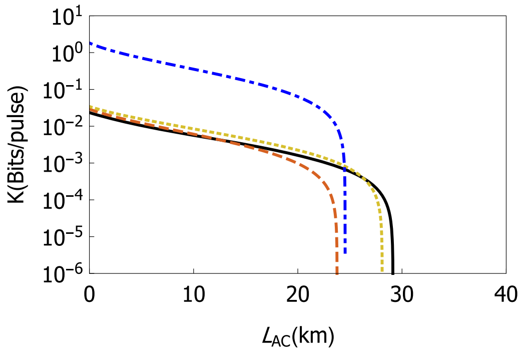

FIG. 13. Secret key rate as a function of L_{AC} in the extreme asymmetric case. The parameters are fixed as $\eta = 0.995$, $\tau = 0.9$, $\epsilon_A^{th} = 0.002 = \epsilon_B^{th}$, $\beta = 96\%$, and displacement $d = 2$. Various plots correspond to TMSV (blue dash dotted), (0, 0)-CTMSC (black solid), (1, 0)-PATMSC (red dashed), and (0, 1)-PSTMSC (yellow tiny dashed).

We also reinforce the fact that coherence is a useful phenomena in increasing the total transmission distances in CV MDI QKD protocols. While the effect of displacement has been studied extensively in Ref. [40] for the case of photon subtraction, we further generalize it to photon addition and catalysis too. In comparison to the earlier studies on quantum catalysis on TMSV [33,37,38,48], here we show that additional coherence boosts the performance further. However, it must be noted that all these non-Gaussian operations are probabilistic and subject to the finesse of the experimental setup.

The efficacy of photon catalysis operation with displacement could further be cherished under realistic conditions such as imperfect state preparation [49] that is abundant in any practical setup. Moreover, in recent years, there have been several new proposals for tweaking the modulation to further optimize the key-rate-vs-transmission distance, such as discrete modulation [50,51], simultaneous classical communication [52], phase-modulation [53], etc. These render, to the current work, immediate relevance and immense interest in the present context as well as in other areas of continuous variable quantum information processing [54].

ACKNOWLEDGMENTS

Both the authors wish to thank Prof. Arvind for helpful discussions regarding non-Gaussian operations on coherent states.

APPENDIX A: WIGNER DISTRIBUTION OF (*m*, *n*)-TMSC

In Fig. 14, we portray the generation of (m, n)-TMSC pictorially. Now we present stepwise calculation of the Wigner function for (m, n)-TMSC and the corresponding probability in shot noise unit (SNU).

1. Wigner Distribution for TMSC

Let's consider a two-mode coherent state, $\rho^C_{A_1A_2} = |d, d\rangle\langle d, d|$, represented by the Wigner distribution,

$$W^C_{A_1A_2}(\xi) = \frac{\exp[-(1/2)(\xi - \bar{\xi})^T V^{-1}(\xi - \bar{\xi})]}{(2\pi)^2\sqrt{\det V}}, \tag{A1}$$

where $\xi = (x_1, p_1, x_2, p_2)^T$ is the column vector with mode quadratures as its components, $\bar{\xi} = (d, 0, d, 0)^T$ denotes the corresponding displacement vector, and $V = \mathbb{1}_2 \bigoplus \mathbb{1}_2$ is the covariance matrix corresponding to the vacuum state. Here, $\mathbb{1}_2$ denotes the 2×2 identity matrix. Thus Eq. (A1) can be explicitly written as

$$W^C_{A_1A_2}(\xi) = \frac{1}{4\pi^2} e^{-\frac{1}{2}((x_1-d)^2+p_1^2+(x_2-d)^2+p_2^2)}. \tag{A2}$$

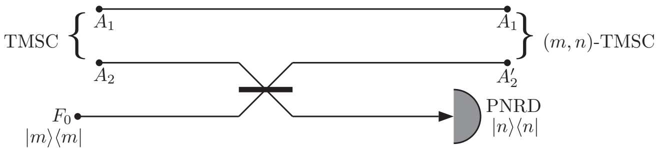

FIG. 14. Schematic diagram of generation of the (m, n)-TMSC state.

Now the two-mode squeezing transformation is given by

$$S_{12}(r) = \begin{pmatrix} \cosh r\, \mathbb{1}_2 & \sinh r\, \mathbb{Z}_2 \\ \sinh r\, \mathbb{Z}_2 & \cosh r\, \mathbb{1}_2 \end{pmatrix}, \tag{A3}$$

where $\mathbb{Z}_2 = \left(\begin{smallmatrix} 1 & 0 \\ 0 & -1 \end{smallmatrix}\right)$. Under the transformation $S_{12}(r)$, Wigner distribution changes as $S_{12}(r) : W^C_{A_1A_2}(\xi) \rightarrow W_{A_1A_2}(\xi) = W^C_{A_1A_2}(S^{-1}_{12}(r)\xi)$, i.e.,

$$\begin{aligned} W_{A_1A_2}(\xi) = \frac{1}{4\pi^2} \exp\bigg[-\frac{1}{2}((x_1 \cosh\, r - x_2 \sinh\, r - d)^2 \\ + (p_1 \cosh\, r + p_2 \sinh\, r)^2 \\ + (x_2 \cosh\, r - x_1 \sinh\, r - d)^2 \\ + (p_1 \sinh\, r + p_2 \cosh\, r)^2) \bigg]. \end{aligned} \tag{A4}$$

2. Wigner Distribution for (*m*, *n*)-TMSC

Fred mixes the ancilla mode F_0 in number state $|m\rangle$ with mode A_2 of TMSC using a beam splitter of transmittivity τ, represented by the transformation matrix,

$$B(\tau) = \begin{pmatrix} \sqrt{\tau}\mathbb{1}_2 & \sqrt{1-\tau}\mathbb{1}_2 \\ -\sqrt{1-\tau}\mathbb{1}_2 & \sqrt{\tau}\mathbb{1}_2 \end{pmatrix}. \tag{A5}$$

This introduces the transformation,

$$S_{\text{BS}} = \mathbb{1}_2 \bigoplus B(\tau), \tag{A6}$$

on the three-mode quadrature vector $\tilde{\xi} = (x_1, p_1, x_2, p_2, x_3, p_3)^T$ for the input state described by the Wigner distribution $W_{A_1A_2F_0}(\tilde{\xi}) = W_{A_1A_2}(\xi) \otimes W^{|m\rangle}_{F_0}(\xi_3) = W_{A_1A_2}(\xi_1, \xi_2) \otimes W^{|m\rangle}_{F_0}(\xi_3)$, where $\xi_i = (x_i, p_i)^T\, (i = 1, 2, 3)$ and $W^{|m\rangle}(\xi_3)$ is the Wigner distribution for number state $|m\rangle$ given as

$$\begin{aligned} W^{|m\rangle}(x_3, p_3) = \frac{(-1)^m}{2\pi} e^{-\frac{x_3^2+p_3^2}{2}} \partial_s^n \partial_t^n \\ \times (e^{st+s(x_3+ip_3)-t(x_3-ip_3)})\Big|_{s=t=0}. \end{aligned} \tag{A7}$$

Consequently, the BS input three-mode Wigner distribution changes as $S_{\text{BS}} : W_{A_1A_2F_0}(\tilde{\xi}) \rightarrow W_{A_1A_2'F_1}(\tilde{\xi}) = W_{A_1A_2F_0}(S^{-1}_{\text{BS}}\tilde{\xi}) = W_{A_1A_2}(\xi_1, \xi_2')W^{|m\rangle}_{F_0}(\xi_3')$.

After a successful detection of n photons, i.e., when $\Pi = |n\rangle\langle n|$ clicks, the unnormalized Wigner distribution for (m, n)-TMSC becomes

$$\begin{aligned} W^{(m,n)}_{A_1A_2'}(\xi_1, \xi_2) = 4\pi \int dx_3 dp_3\, W_{A_1A_2}(\xi_1, \xi_2')W^{|m\rangle}_{F_0}(\xi_3'), \\ \times W^{|n\rangle}_{F_0}(\xi_3). \end{aligned} \tag{A8}$$

As we shall see, we do not need to explicitly calculate the Wigner distribution for (m, n)-TMSC in our probability and covariance matrix calculation.

APPENDIX B: CALCULATION OF PROBABILITY OF (*m*, *n*)-TMSC

The probability of n-photon detection is obtained by integrating $W^{(m,n)}_{A_1A'_2}(\xi_1,\xi_2)$ as

$$\begin{aligned} P^{(m,n)} &= \int \xi_1\xi_2\, W^{(m,n)}_{A_1A'_2}(\xi_1,\xi_2) \\ &= 4\pi \int d^6\tilde{\xi}\; W_{A_1A_2}(\xi_1,\xi'_2) W^{|m\rangle}_{F_0}(\xi'_3) W^{|n\rangle}_{F_0}(\xi_3). \end{aligned} \tag{B1}$$

Now, using the generating function of the Laguerre polynomial,

$$\partial_s^k\partial_t^k\big(e^{st+s(q+ip)-t(q-ip)}\big)\Big|_{s=t=0} = k!L_k(q^2+p^2), \tag{B2}$$

we get the probability of n-photon detection as

$$\begin{aligned} P^{(m,n)} &= \frac{(-1)^{m+n}}{4\pi^3}\frac{1}{m!n!}e^{-d^2}\partial_u^m\partial_v^m\partial_s^n\partial_t^n e^{st+uv} \\ &\times n \int d^6\tilde{\xi}\,\exp(-\tilde{\xi}^T M\tilde{\xi} + N^T\tilde{\xi})\Big|_{u=v=s=t=0}, \end{aligned} \tag{B3}$$

with

$$M = \begin{pmatrix} m_1\mathbb{1}_2 & m_4\mathbb{Z}_2 & m_5\mathbb{Z}_2 \\ m_4\mathbb{Z}_2 & m_2\mathbb{1}_2 & m_6\mathbb{1}_2 \\ m_5\mathbb{Z}_2 & m_6\mathbb{1}_2 & m_3\mathbb{1}_2 \end{pmatrix} \;\&$$

$$N = \begin{pmatrix} -dn_1 \\ 0 \\ (u-v)\sqrt{1-\tau} - dn_1\sqrt{\tau} \\ i(u+v)\sqrt{1-\tau} \\ s-t+(u-v)\sqrt{\tau} + dn_1\sqrt{1-\tau} \\ i(s+t)+i(u+v)\sqrt{\tau} \end{pmatrix}, \tag{B4}$$

where $m_1 = -(1+2\alpha^2)/2$, $m_2 = -(1+2\alpha^2\tau)/2$, $m_3 = -(1+\alpha^2(1-\tau))$, $m_4 = \alpha\sqrt{(1+\alpha^2)\tau}$, $m_5 = -\alpha\sqrt{(1+\alpha^2)(1-\tau)}$, $m_6 = \alpha^2\sqrt{\tau(1-\tau)}$ and $n_1 = \alpha - \sqrt{1+\alpha^2}$, and $\alpha = \sinh r$. This form facilitates the use of the multidimensional Gaussian integral formula,

$$\int_{\mathbb{R}^n} \exp(-X^T MX + N^T X)dX = \sqrt{\frac{\pi^n}{\det M}}\exp\left(\frac{N^T M^{-1}N}{4}\right). \tag{B5}$$

Consequently the expression of probability reduces to

$$\begin{aligned} P^{(m,n)} &= \frac{(-1)^{m+n}}{m!n!}\frac{1}{1+\alpha^2(1-\tau)}e^{-i_1}\partial_u^m\partial_v^m\partial_s^n\partial_t^n e^{-a_1st+b_1s+c_1t-d_1uv+e_1u+f_1v+g_1tu+h_1sv}\Big|_{u=v=s=t=0} \\ &= \frac{(-1)^{m+n}}{m!n!}\frac{1}{1+\alpha^2(1-\tau)}e^{-i_1}\partial_u^m\partial_v^m\partial_s^n\partial_t^n \sum_{l=0}^{\infty}\frac{(g_1tu)^l}{l!}\sum_{k=0}^{\infty}\frac{(h_1sv)^k}{k!}e^{-a_1st+b_1s+c_1t}e^{-d_1uv+e_1u+f_1v}\Big|_{u=v=s=t=0} \\ &= \frac{(-1)^{m+n}}{m!n!}\frac{1}{1+\alpha^2(1-\tau)}e^{-i_1}\partial_u^m\partial_v^m\partial_s^n\partial_t^n \sum_{l=0}^{\infty}\sum_{k=0}^{\infty}\frac{g_1^l}{l!}\frac{h_1^k}{k!}\partial_{c_1}^l\partial_{b_1}^k\partial_{e_1}^l\partial_{f_1}^k e^{-a_1st+b_1s+c_1t}e^{-d_1uv+e_1u+f_1v}\Big|_{u=v=s=t=0}, \end{aligned} \tag{B6}$$

where

$$\begin{aligned} a_1 &= \frac{\alpha^2}{1+\alpha^2}d_1 = \frac{\alpha^2(1-\tau)}{1+\alpha^2(1-\tau)}, & g_1 = h_1 &= \frac{-\sqrt{\tau}}{1+\alpha^2(1-\tau)}, \\ c_1 &= -b_1 = \frac{a_1(\alpha+\sqrt{1+\alpha^2})\sqrt{1-\tau}}{2(1+\alpha^2(1-\tau))}, & i_1 &= \frac{d^2(1+2\alpha(\alpha+\sqrt{1+\alpha^2}))(1-\tau)}{4(1+\alpha^2(1-\tau))}. \\ e_1 &= -f_1 = \frac{a_1(\alpha+\sqrt{1+\alpha^2})\sqrt{\tau(1-\tau)}}{2(1+\alpha^2(1-\tau))}, \end{aligned} \tag{B7}$$

Now we recall the following identities for the two-variable Hermite polynomial,

$$H_{m,n}(x,y) = \partial_s^m \partial_t^n \exp(-st+sx+ty)\big|_{s=t=0} \sum_{j=0}^{\min(m,n)} \frac{(-1)^j m!n!x^{m-j}y^{n-j}}{j!(m-j)!(n-j)!} \quad \&$$

$$\partial_x^k \partial_y^l H_{m,n}(x,y) = \frac{m!n!}{(m-k)!(n-l)!} H_{m-k,n-l}(x,y). \tag{B8}$$

These identities reduce Eq. (B6):

$$\begin{aligned} P^{(m,n)} &= \frac{(-1)^{m+n}}{m!n!}\frac{1}{1+\alpha^2(1-\tau)}e^{-i_1}\sum_{l=0}^{\infty}\sum_{k=0}^{\infty}\frac{g_1^l}{l!}\frac{h_1^k}{k!}\partial_{c_1}^l\partial_{b_1}^k\partial_{e_1}^l\partial_{f_1}^k a_1^m H_{m,m}\left[\frac{b_1}{\sqrt{a_1}},\frac{c_1}{\sqrt{a_1}}\right]d_1^n H_{n,n}\left[\frac{e_1}{\sqrt{d_1}},\frac{f_1}{\sqrt{d_1}}\right] \\ &= \frac{(-1)^{m+n}}{m!n!}\frac{1}{1+\alpha^2(1-\tau)}e^{-i_1}\sum_{l=0}^{\min(m,n)}\sum_{k=0}^{\min(m,n)}\frac{g_1^l}{l!}\frac{h_1^k}{k!}a_1^m d_1^n\frac{1}{\sqrt{a_1}^{k+l}}\frac{1}{\sqrt{d_1}^{k+l}}\frac{m!m!n!n!}{(m-k)!(n-k)!(m-l)!(n-l)!}, \\ &\quad \times H_{m-k,m-l}\left[\frac{b_1}{\sqrt{a_1}},\frac{c_1}{\sqrt{a_1}}\right]H_{n-l,n-k}\left[\frac{e_1}{\sqrt{d_1}},\frac{f_1}{\sqrt{d_1}}\right]. \end{aligned} \tag{B9}$$

APPENDIX C: CALCULATION OF COVARIANCE MATRIX

Here we provide a general expression for the moment generating function defined as $\mathscr{F}_M = \frac{1}{2}\langle\{\hat{x_1}^{r_1}\hat{p_1}^{s_1}\hat{x_2}^{r_2}\hat{p_2}^{s_2}\}_{\rm sym}\rangle$. Any particular moment, i.e., the elements of the covariance matrix could be easily obtained from this generating function as special cases, e.g., $\frac{1}{2}\langle\{\hat{x_1}\hat{p_1}\}_{\rm sym}\rangle = \frac{1}{2}\langle\{\hat{x_1},\hat{p_1}\}\rangle = \lim_{\substack{r_1\to 1,\, s_1\to 1\\ r_2\to 0,\, s_2\to 0}}\mathscr{F}_M$, where "{, }" denotes the anticommutator. In terms of this normalized Wigner distribution of (m,n)-TMSC, $\tilde{W}_{A_1A_2'}^{(m,n)}(\xi_1,\xi_2) = \frac{1}{P^{(m,n)}}W_{A_1A_2'}^{(m,n)}(\xi_1,\xi_2)$, the moment generating function $\mathscr{F}_M$ could be easily evaluated by using parametric differentiation techniques as

$$\begin{aligned} \mathscr{F}_M &= \int d^4\xi\, x_1^{r_1}p_1^{s_1}x_2^{r_2}p_2^{s_2}\tilde{W}_{A_1A_2'}^{(m,n)}(\xi_1,\xi_2) \\ &= \frac{1}{P^{(m,n)}}\frac{(-1)^{m+n}}{m!n!}\frac{1}{1+\alpha^2(1-\tau)}\sum_{k,l=0}^{\min(m,n)}\frac{g_1^l}{l!}\frac{h_1^k}{k!}a_1^{m-\frac{k+l}{2}}d_1^{n-\frac{k+l}{2}}\frac{m!m!n!n!}{(m-k)!(n-k)!(m-l)!(n-l)!} \\ &\quad \times \partial_{u_1}^{r_1}\partial_{v_1}^{s_1}\partial_{u_2}^{r_2}\partial_{v_2}^{s_2}e^{g_2u_1+h_2u_2+i_2(u_1^2+v_1^2+u_2^2+v_2^2)-j_2(u_1u_2-v_1v_2)+k_2} \\ &\quad \times H_{m-k,m-l}\left[\frac{-a_2(u_1-iv_1)-b_2(u_2+iv_2)-c_2}{\sqrt{a_1}},\frac{a_2(u_1+iv_1)+b_2(u_2-iv_2)+c_2}{\sqrt{a_1}}\right] \\ &\quad \times H_{n-l,n-k}\left[\frac{-d_2(u_1+iv_1)-e_2(u_2-iv_2)-f_2}{\sqrt{d_1}},\frac{d_2(u_1-iv_1)+e_2(u_2+iv_2)+f_2}{\sqrt{d_1}}\right]\Bigg|_{u_1=v_1=u_2=v_2=0}, \end{aligned} \tag{C1}$$

where

$$\begin{aligned} &a_2 = \frac{d_2}{\sqrt{\tau}} = \frac{\alpha\sqrt{(1+\alpha^2)(1-\tau)}}{1+\alpha^2(1-\tau)}, \quad b_2 = \frac{\alpha^2\sqrt{\tau(1-\tau)}}{1+\alpha^2(1-\tau)}, \quad c_2 = \frac{f_2}{\sqrt{\tau}} = \frac{d(\alpha+\sqrt{1+\alpha^2})\sqrt{1-\tau}}{2(1+\alpha^2(1-\tau))}, \\ &e_2 = \frac{(1+\alpha^2)\sqrt{1-\tau}}{1+\alpha^2(1-\tau)}, \quad g_2 = -\frac{d(\sqrt{1+\alpha^2}+\alpha\tau)}{1+\alpha^2(1-\tau)}, \quad h_2 = -\frac{d(\alpha+\sqrt{1+\alpha^2})\sqrt{\tau}}{1+\alpha^2(1-\tau)}, \\ &i_2 = -\frac{1+\alpha^2(1+\tau)}{2(1+\alpha^2(1-\tau))}, \quad j_2 = \frac{2\alpha\sqrt{(1+\alpha^2)\tau}}{1+\alpha^2(1-\tau)}, \quad k_2 = \frac{d^2(1+2\alpha(\alpha+\sqrt{1+\alpha^2}))(1-\tau)}{4(1+\alpha^2(1-\tau))}. \end{aligned} \tag{C2}$$

By suitably choosing values of r_1, s_1, r_2, s_2 in Eq. (C1), one can calculate all the elements of the covariance matrix that takes the following form:

$$\Sigma = (V_{ij}) \equiv \begin{pmatrix} V_A^x & 0 & V_C^x & 0 \\ 0 & V_A^p & 0 & V_C^p \\ V_C^x & 0 & V_B^x & 0 \\ 0 & V_C^p & 0 & V_B^p \end{pmatrix}. \tag{C3}$$

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

[2] S. Pirandola, U. L. Anderson, 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. Usenko, G. Vallone, P. Villoresi, and P. Wallden, Adv. Opt. Photon **12**, 1012 (2020).

[3] C. H. Bennett and G. Brassard, Quantum cryptography public key distribution and coin tossing, in *Proceedings of IEEE International Conference on Computers, Systems, and Signal Processing* (IEEE Press, New York, 1984), pp. 175–179.

[4] P. W. Shor and J. Preskill, Phys. Rev. Lett. **85**, 441 (2000).

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

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

[7] N. J. Cerf, M. Lévy, and G. Van Assche, Phys. Rev. A **63**, 052311 (2001).

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

[9] A. K. Ekert, Phys. Rev. Lett. **67**, 661 (1991).

[10] A. Acín, N. Gisin, and L. Masanes, Phys. Rev. Lett. **97**, 120405 (2006).

[11] M. Pawłowski, Phys. Rev. A **82**, 032313 (2010).

[12] R. Renner and J. I. Cirac, Phys. Rev. Lett. **102**, 110504 (2009).

[13] A. Leverrier, R. García-Patrón, R. Renner, and N. J. Cerf, Phys. Rev. Lett. **110**, 030502 (2013).

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

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

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

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

[18] M. Curty, F. Xu, W. Cui, C. C. W. Lim, K. Tamaki, and H.-K. Lo, Nat. Commun. **5**, 3732 (2014).

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

[20] A. Rubenok, J. A. Slater, P. Chan, I. Lucio-Martinez, and W. Tittel, Phys. Rev. Lett. **111**, 130501 (2013).

[21] T. Ferreira da Silva, D. Vitoreti, G. B. Xavier, G. C. do Amaral, G. P. Temporão, and J. P. von der Weid, Phys. Rev. A **88**, 052303 (2013).

[22] Y. Liu, T.-Y. Chen, L.-J. Wang, H. Liang, G.-L. Shentu, J. Wang, K. Cui, H.-L. Yin, N.-L. Liu, L. Li, X. Ma, J. S. Pelc, M. M. Fejer, C.-Z. Peng, Q. Zhang, and J.-W. Pan, Phys. Rev. Lett. **111**, 130502 (2013).

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

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

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

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

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

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

[29] T. Gehring, V. Händchen, J. Duhme, F. Furrer, T. Franz, C. Pacher, R. F. Werner, and R. Schnabel, Nat. Commun. **6**, 8795 (2015).

[30] F. Xu, M. Curty, B. Qi, L. Qian, and H.-K. Lo, Nat. Photonics **9**, 772 (2015).

[31] S. L. Zhang and P. van Loock, Phys. Rev. A **82**, 062316 (2010).

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

[33] Y. Guo, W. Ye, H. Zhong, and Q. Liao, Phys. Rev. A **99**, 032327 (2019).

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

[35] P. Huang, G. He, J. Fang, and G. Zeng, Phys. Rev. A **87**, 012317 (2013).

[36] Z. Li, Y. Zhang, X. Wang, B. Xu, X. Peng, and H. Guo, Phys. Rev. A **93**, 012310 (2016).

[37] W. Ye, H. Zhong, X. Wu, L. Hu, and Y. Guo, Quant. Info. Proc. **19**, 346 (2020).

[38] Y. Wang, S. Zou, Y. Mao, and Y. Guo, Entropy **22**, 571 (2020).

[39] L. Hu, M. Al-amri, Z. Liao, and M. S. Zubairy, Phys. Rev. A **102**, 012608 (2020).

[40] C. Kumar, J. Singh, S. Bose, and Arvind, Phys. Rev. A **100**, 052329 (2019).

[41] K. Marshall and C. Weedbrook, Entropy **17**, 3152 (2015).

[42] F. Dell'anno, D. Buono, G. Nocerino, S. D. Siena, and F. Illuminati, Quantum Inf. Process. **18**, 20 (2019).

[43] X. Su, M. Wang, Z. Yan, X. Jia, C. Xie, and K. Peng, Science China Information Sciences **63**, 180503 (2020).

[44] R. J. Birrittella, M. E. Baz, and C. C. Gerry, J. Opt. Soc. Am. B **35**, 1514 (2018).

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

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

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

[48] L. Hu, Z. Liao, and M. S. Zubairy, Phys. Rev. A **95**, 012310 (2017).

[49] P. Wang, X. Wang, and Y. Li, Phys. Rev. A **102**, 022609 (2020).

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

[51] W. Ye, Y. Guo, H. Zhang, H. Zhong, Y. Mao, and L. Hu, J. Phys. B: At., Mol. Opt. Phys. **54**, 045501 (2021).

[52] X.-D. Wu, Y.-J. Wang, D. Huang, and Y. Guo, Front. Phys. **15**, 31601 (2020).

[53] Q. Liao, Y. Wang, D. Huang, and Y. Guo, Opt. Express **26**, 19907 (2018).

[54] F. Flamini, N. Spagnolo, and F. Sciarrino, Rep. Prog. Phys. **82**, 016001 (2018).