Multimode non-Gaussian secure communication under mode mismatch

Soumyakanti Bose[*] and Hyunseok Jeong[†]

Department of Physics and Astronomy, Seoul National University, Gwanak-ro 1, Gwanak-gu, Seoul 08826, Korea

(Received 6 July 2022; accepted 22 September 2023; published 12 October 2023)

In this paper we analyze entanglement-based (EB) continuous-variable (CV) quantum-key distribution (QKD) with bright multimode non-Gaussian light. Our analysis is centered around the role of non-Gaussianity in mitigating the excess noise arising due to the mismatch between the signal modes and the local oscillators used for measurements. To be specific, we consider the non-Gaussian resources generated by single-photon subtraction and zero-photon catalysis applied on a two-mode squeezed vacuum (TMSV) state. We show that, at a given strength of the mode-mismatch noise, zero-photon catalysis leads to the maximum transmission distance, compared to the TMSV. However, considering the unavoidable issue of photon loss in the linear optical scheme for implementing zero-photon catalysis, our results hints at the single-photon-subtracted TMSV being the optimal choice for maximizing the transmission distance in EB CV QKD.

DOI: 10.1103/PhysRevA.108.042412

I. INTRODUCTION

Encryption and decryption of messages between two distant parties have been of great interest over a long period in modern scientific endeavors [1,2]. While classical prescriptions are secure up to technical limitations in obtaining prime divisors of a large number [3], quantum protocols rely upon the fundamental laws of nature [4–9]. Moreover, recent advances indicate the vulnerability of classical cryptography further [10], thereby pointing towards the indispensability of quantum cryptography, which provides security beyond the scope of classical physics with both asymptotic [11–17] and finite resources [18–23].

Over the past three decades there have been extensive studies on cryptographic aspects of quantum systems, in particular generating and distributing a quantum key or password known as quantum key distribution (QKD) [24]. Communication protocols involving quantum systems could be broadly classified into two groups, discrete variable (DV) QKD [4,5] and continuous variable (CV) QKD [6–9]. While DV QKD requires expensive single-photon sources, CV QKD protocols are readily implementable within the current technology. Nonetheless, CV protocols have been proved to be unconditionally secure against the most general collective attack and have been experimentally implemented [25–32].

Although quantum optical entangled states with low energy are the ideal choices for performing QKD, it is always challenging to control and manipulate such microscopic systems in practice. On the other hand, classical light beams are generally multimode, bright (intense), and easy to operate but are devoid of quantum character. This often sets off a trade-off between quantumness and macroscopicity of physical systems [33], two practical concerns for performing tasks outside the classical domain. In recent times, there have been numerous findings revealing interesting quantum features of such macroscopic systems [34–40].

Another compelling factor of such multimode light is that for such light fields all the modes do not always match the local oscillators used for the quadrature measurements. As a consequence, the excess unmatched signal modes yield additional undesired noise in the quadrature value. One can still perform QKD using such multimode light fields under this type of mode mismatch if the field energy is low, i.e., it contains a small number of photons as in that case the additional noise could be suppressed by making the local oscillators very intense [41]. However, when the source light becomes bright (high average photon number) additional noise due to mode mismatch plays a significant role in reducing key length [42,43] as well as serving as a security concern [44]. However, it must be noted that previous analyses in this context were primarily restricted to the Gaussian premises only.

On the other hand, over the past decade, authors have pointed out the efficiency of various non-Gaussian operations in CV QKD [45–54]. In particular, non-Gaussianity induced by photon subtraction [45,47,48,52] or catalysis [51,53,54] enhances the distance between the parties and provides robustness against the detector inefficiency. However, it remains an open question whether such non-Gaussian operations have any practical impact on the macroscopic optical systems that play an important role in quantum information processing with optical resources [55]. It is quite interesting to analyze such non-Gaussian aspects of CV QKD with macroscopic light.

In the present paper we analyze the QKD with multimode non-Gaussian light under mode mismatch between the source and the detectors. We consider the entanglement-based protocol for key distribution with no-switching assumption [56] as it yields more distance [57]. In this protocol, two parties generate a key by performing heterodyne (instead of homodyne) measurements on the shared entangled state of light. Although

[*] soumyakanti.bose09@gmail.com

[†] h.jeong37@gmail.com

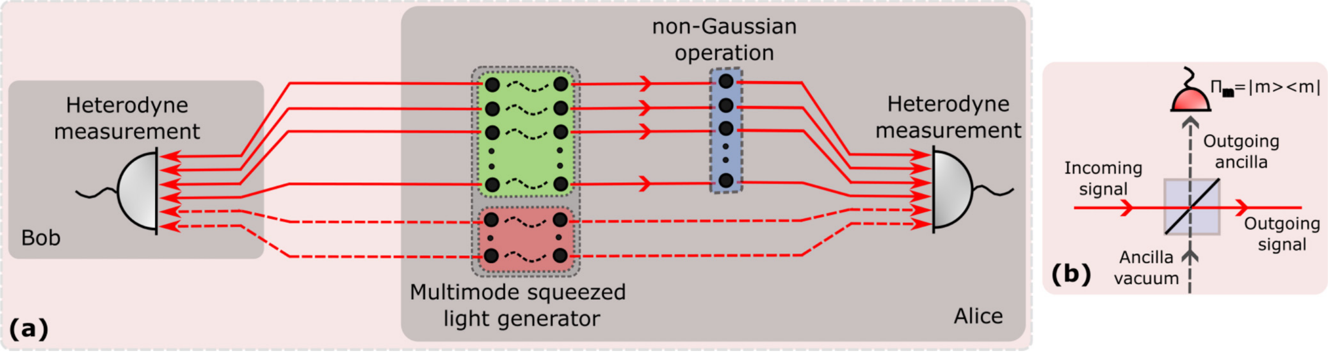

FIG. 1. (a) Schematic of the EB QKD protocol with multimode non-Gaussian light under mode mismatch. The matched (unmatched) signal modes are represented by red solid (dashed) lines coming out of the green (red) box of the multimode-squeezed-light generator. First, the desired non-Gaussian operations (blue box) are performed only on the matched signal modes (green box) at on Alice's side. Subsequently, both Alice and Bob follow the rest of the QKD protocol (as discussed in the text) using balanced heterodyne measurements that use a balanced (50:50) beam splitter and two homodyne detectors (with efficiency η). (b) Description of the non-Gaussian operations for a single signal mode. First the incoming signal is mixed with an ancilla vacuum in an unbalanced beam splitter (with transmittivity T). The T needs to be chosen suitably to optimize the performance. Subsequent projection of the outgoing ancilla onto a photon-number state yields the desired non-Gaussian operation on the outgoing signal mode. Projection along $|0\rangle\langle 0|$ leads to zero-photon catalysis, while projection along $|1\rangle\langle 1|$ yields single-photon subtraction on the outgoing signal.

there are many ways of introducing non-Gaussianity to a two-mode squeezed vacuum (TMSV) state, here we consider only single-photon subtraction and zero-photon catalysis as they appear to yield optimal results [58]. We show that both the single-photon-subtracted TMSV (1PSTMSV) and zero-photon-catalyzed TMSV (ZPCTMSV) states considerably enhance the transmission distance, compared to the Gaussian case (TMSV), at all strengths of noise due to mode mismatch. In particular, the ZPCTMSV yields the maximum transmission distance of approximately 160 km. However, considering the effect of photon loss, a very natural phenomenon in zero-photon catalysis, we find that the 1PSTMSV appears to be the optimal non-Gaussian resource in entanglement-based CV QKD with a maximum distance of approximately 70 km.

Our paper is organized as follows. In Sec. II we discuss the basic protocol for the entanglement-based (EB) scheme for CV QKD. We also discuss the generation of non-Gaussian resources. In Sec. III we briefly describe the multimode-homodyne measurement under mode mismatch and its ramifications in the case of heterodyne measurements. We also provide a brief description of the choice of mode-mismatch noise. Section IV provides a concise description of the effect of mode mismatch on the entanglement for a Gaussian state. Section V contains an analysis of the secured key rate for both the Gaussian and the non-Gaussian cases. We first discuss the role of non-Gaussianity in maximizing the transmission distance followed by an analysis of the dependence of key rate upon detector inefficiency. In Sec. VI we discuss a physical situation where the performance of the ZPCTMSV could be compromised. We summarize our observations in Sec. VII.

II. PROTOCOL

In Fig. 1 we describe the schematic for the entanglement-based scheme for generating a quantum key with multimode non-Gaussian bright light under mode mismatch (when some of the source modes do not match the local oscillators). The protocol could be understood in the following way.

Step 1. Alice first generates multiple pairs (numbers $M+N$) of the TMSV state. She keeps one mode from each pair to herself (solid line) and she sends the other mode to a distant party Bob (dashed line). Of all the modes only M modes match the local oscillators and the remaining N modes do not match.

Step 2. Alice then performs the desired non-Gaussian operations, i.e., the zero-photon catalysis and single-photon subtraction on each of the M matching modes (the vertical rectangular box) while the other N modes remain intact.

Step 3. Subsequently, Alice performs heterodyne measurement (measuring both x and p quadratures) on the incoming modes. The data set corresponding to the M matching modes leads to the quadrature value. However, the N remaining unmatched modes lead to the additional noise (see Sec. III A).

Step 4. Bob also performs heterodyne measurement on all the modes he receives in a similar fashion, where M modes match the local oscillators and N modes do not match.

Step 5. After generating the data set (measurement outcomes), both Alice and Bob go for the postprocessing. Here they perform privacy amplification and then evaluate the final secured key rate.

We also elaborate a simple linear optical model for performing the desired non-Gaussian operations for a single signal mode [Fig. 1(b)]. The schematic is described as follows.

(i) Each of the incoming signal modes is fed to one of the inputs of a passive beam splitter (BS) with transmittivity $T_{\rm BS}$ while the other input is left in the vacuum (ancilla mode). The transmittivity $T_{\rm BS}$ describes how much light is passed through the BS. For example, $T_{\rm BS} = 0.9$ stands for 90% transmission and 10% reflection.

(ii) On the outgoing ancilla mode, Alice performs a photon-detection measurement using a photon-number-resolving detector; the measurements are described in terms of the set of projective operators $\{\Pi_k = |k\rangle\langle k| : k = 0, 1, \ldots, \infty\}$.

(iii) Upon detection of k photons in the ancilla mode, the outgoing signal mode becomes k-photon subtracted. We consider two particular choices of k that give rise to single-photon subtraction and zero-photon catalysis [45,47,48,51–54]. Our aim is to analyze these cases to understand the role of these de-Gaussification operations in the present context. These cases are as follows.

Case $k = 0$. In this case the outgoing ancilla is projected along the state $|0\rangle\langle 0|$. This could be seen as if no actual photon is taken from or added to the signal mode. This is referred to as zero-photon catalysis [51,53,54].

Case $k = 1$. In this case the outgoing ancilla is projected along the state $|1\rangle\langle 1|$. In a similar way this could be seen as a single unit of the photon being taken out of the signal mode, which is known as single-photon subtraction [45,47,48,52].

(iv) The process of photon subtraction is probabilistic where the probability of k photon subtraction is given by $P(k) = \frac{1}{\mu^2}\frac{\tau^{2k}(1-T_{\rm BS})^k}{(1-\tau^2 T_{\rm BS})^{k+1}}$, where $\mu = \cosh r$ and $\tau = \tanh r$. The variance matrix for the k-photon-subtracted TMSV is given by (Appendix B) $V^{(k)} = \begin{pmatrix} x^{(k)}\mathbf{I} & z^{(k)}\sigma_3 \\ z^{(k)}\sigma_3 & y^{(k)}\mathbf{I}\end{pmatrix}$, where $\mathbf{I}$ is the 2×2 identity matrix, $\sigma_3 = \mathrm{diag}(1, -1)$ is the Pauli matrix, $x^{(k)} = \frac{2(1+k)}{1-\tau^2 T_{\rm BS}} - 1$, $y^{(k)} = \frac{2(1+k\tau^2 T_{\rm BS})}{1-\tau^2 T_{\rm BS}} - 1$, and $z^{(k)} = \frac{2\sqrt{T_{\rm BS}}\tau(1+k)}{1-\tau^2 T_{\rm BS}}$. However, the coefficient $z^{(k)}$ as shown here differs from that of Ref. [48].[1]

III. MULTIMODE QUADRATURE MEASUREMENT UNDER MODE MISMATCH

A. Multimode homodyning under mode mismatch

Let us first consider the basic outline of homodyne detection of a multimode light with the mode mismatch elaborated in a simple diagram as in Fig. 2. Suppose the emitter emits M signal modes a_i that match the M local oscillators α_i ($i = 1, 2, \dots, M$). It also emits N signal modes b_j, which are mixed with N vacuum modes V_j ($j = 1, 2, \dots, N$) in the BS. For the sake of simplicity, we consider balanced homodyne detection, i.e., we use a 50:50 BS.

We consider that the detectors can detect the additional modes with efficiency ϵ, i.e., the detector D$_1$ can register the average photon number as $n_1 = \sum_k a'^\dagger_k a'_k + \epsilon \sum_l b'^\dagger_l b'_l$, where primed operators correspond to the respective output modes of the BS. In a simple and straightforward manner it could be shown that in the presence of this mode mismatch the measured quadrature for the signal modes changes as [42] $R_i \rightarrow R_i + \frac{\epsilon}{\alpha_i}\sum_j (b^\dagger_j V_j + b_j V^\dagger_j)$, leading to the variance $\Delta R_i \rightarrow \Delta R_i + \frac{\epsilon^2}{\alpha^2}\sum_j \langle b^\dagger_j b_j\rangle$. Since there are M matched modes, the normalized variance per mode is obtained by dividing the measured result by the factor M. Furthermore, for the sake of simplicity, we consider that the additional (unmatched) modes are equally strong, i.e., $\langle b^\dagger_j b_j\rangle = \langle b^\dagger_k b_k\rangle = \bar{n}\,\forall\, j, k$. As a consequence, the normalized variance becomes [42]

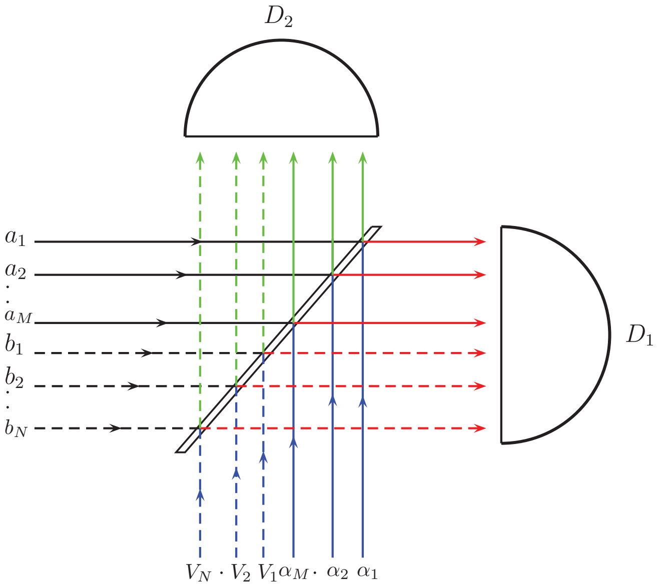

FIG. 2. Schematic of homodyne measurement of a multimode light with mode mismatch. Various lines correspond to incoming light, i.e., signal modes (black lines) and local oscillators (blue lines), and outgoing light, i.e., the signal to D_1 (red lines) and the signal to D_2 (green lines). Solid and dotted lines correspond to the matched modes and the unmatched modes, respectively. Here D_1 and D_2 are the photon-number-resolving detectors. The BS (slanted narrow rectangular box) is considered to be balanced (50:50).

$$v_i \rightarrow v_i + \frac{N\epsilon^2}{M\alpha^2}\bar{n} = v_i + \delta, \tag{1}$$

where δ is the mode-mismatch noise (Appendix A).

B. Multimode heterodyning under mode mismatch

Here we consider heterodyne measurement instead of homodyne measurement. In Fig. 3 we present the schematic difference between homodyne and heterodyne measurements.

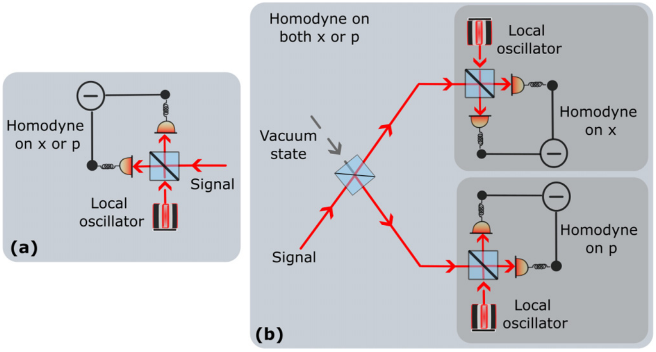

FIG. 3. Schematic of (a) homodyne measurement and (b) heterodyne measurement of the signal source. In the case of heterodyning, two homodyne measurements are performed after splitting the signal at a 50:50 beam splitter.

[1] We note that in the expression of z^k in [48], a factor of 2 is missing. This additional factor of 2, as shown here, could be easily appreciated by a comparison with the variance of the TMSV in the shot-noise unit (the ground-state quadrature variance is unity). The case of the TMSV could be obtained within the present setup by choosing $T_{\rm BS} \rightarrow 1$ and $k \rightarrow 0$. Detailed and explicit results are presented in Appendix B.

In contrast to the homodyne measurement [Fig. 3(a)], in the case of heterodyne measurement [Fig. 3(b)] first the signal mode is split into two equal halves at a 50:50 BS. Subsequently, two individual homodyne measurements are performed on each of the halves.

In line with the standard procedure for heterodyne measurement, the present protocol is as follows. First, each of the incoming signal modes is split into two parts by using a 50:50 beam splitter. Then we proceed with the multimode homodyne measurement under mode mismatch (as discussed in Fig. 2) on both parts for each of the signal modes. This completes the procedure for multimode heterodyne measurement under mode mismatch. The effect of this multimode heterodyne measurement under mode mismatch could be mathematically summarized in the following way. Let us consider any particular signal mode with variance matrix $V_{\text{in}} = \begin{pmatrix} v_{xx} & v_{xp} \\ v_{xp} & v_{pp} \end{pmatrix}$. Due to heterodyne measurement, the diagonal entries acquire one additional unit of contribution arising from the splitting at the 50:50 beam splitter. Then the same diagonal entries acquire an additional contribution in the form of noise due to the mode mismatch. As a consequence, the final measured variance matrix becomes $V_{\text{out}} = \begin{pmatrix} v_{xx}+1+\delta & 0 \\ 0 & v_{pp}+1+\delta \end{pmatrix}$, which can be obtained by a straightforward calculation.

C. Choice of mode-mismatch noise

It might be interesting to discuss the physical limits of δ. There could be several ways of tuning the value of δ such as changing the ratio of M and N and the strength of unmatched modes ($\bar{n}$). In the present work we are interested in understanding the role non-Gaussianity in mitigating this additional noise. Consequently, for the sake of simplicity, we consider a scenario where the number of modes matching the local oscillators is equal to the number of modes that do not match, i.e., $M = N$. We also assume that the heterodyne detectors used in Alice's and Bob's laboratories do not differentiate between the matched and the unmatched modes. In other words, the detectors detect the unmatched modes with complete efficiency, i.e., $\epsilon = 1.0$. As a consequence, the additional noise appearing in the quadrature measurements (mode-mismatch noise) is essentially $\delta = \bar{n}/|\alpha|^2$. As discussed in [43], the average strength of the local oscillators is varied between 10^5 and 2×10^6. If we consider the local oscillators to be as strong as $|\alpha|^2 = 10^5$, then the source light could be made as bright as $\bar{n} \sim 10^3$ to yield the mode-mismatch noise $0.01 \leqslant \delta \leqslant 0.05$. However, by reducing the efficiency of detecting the excess unmatched modes with a better apparatus, i.e., making $\epsilon < 1$, one can further increase the brightness of the signal modes.

IV. MODE MISMATCH VS ENTANGLEMENT FOR GAUSSIAN STATES

In any EB QKD protocol the first step is to check for the nonzero mutual information between the distant parties that separates it from non-EB protocols. As described in the preceding section, the mismatch between the modes generated and the available modes for heterodyning yields additional noise on the measured quadrature. Consequently, before presenting the results on the key rate, here we discuss the impact of this mode mismatch on the entanglement of the initial Gaussian resource, i.e., the TMSV. A TMSV is given by

$$|\psi\rangle = S_{ab}(r)|0,0\rangle, \tag{2}$$

where $S_{ab}(r) = \exp[r(a^\dagger b^\dagger - ab)]$ is the two-mode squeezing operator and r is the squeezing strength. It could be efficiently described in terms of the variance matrix $V = \begin{pmatrix} \mathbf{A} & \mathbf{C} \\ \mathbf{C} & \mathbf{B} \end{pmatrix}$, where $\mathbf{A} = \mathbf{B} = \operatorname{diag}(\zeta, \zeta)$ correspond to the individual subsystems and $\mathbf{C} = \operatorname{diag}(c, -c)$ represents the intermode correlation with $\zeta = \cosh 2r$ and $c = \sinh 2r$. Due to mode mismatch, the measured quantities for the subsystems ζ would acquire an additional contribution while the intermode terms c would be unaffected. As a consequence, under multimode heterodyning with mode mismatch, the measured variance matrix for the TMSV becomes

$$V_{\text{meas}} = \begin{pmatrix} \zeta+\delta & 0 & c & 0 \\ 0 & \zeta+\delta & 0 & -c \\ c & 0 & \zeta+\delta & 0 \\ 0 & -c & 0 & \zeta+\delta \end{pmatrix}, \tag{3}$$

where $\delta = \frac{N\epsilon^2}{M\alpha^2}\bar{n}$.

It could be easily checked that the mode mismatch introduces mixedness in the variance matrix as $\det V_{\text{meas}} > 1$. As a consequence, we consider the logarithmic negativity as the check for entanglement. Logarithmic negativity for a bipartite Gaussian state with variance matrix $V = \begin{pmatrix} \mathbf{A} & \mathbf{C} \\ \mathbf{C} & \mathbf{B} \end{pmatrix}$ is given in terms of its minimum symplectic eigenvalue (under partial transposition) $l_{\min}$ as [59] $\mathbf{E_N} = \max\{0, -\log_2 l_{\min}\}$, where

$$l_{\min} = \sqrt{\frac{\Delta - \sqrt{\Delta^2 - 4\det V}}{2}}. \tag{4}$$

Here Δ is given as $\Delta = \det A + \det B - 2\det C$. Consequently, in the present case of macroscopic heterodyne detection with mode mismatch, logarithmic negativity for the variance matrix V_{meas} (3) is given by

$$\mathbf{E_N} = -\tfrac{1}{2}\log_2[-1 + \delta^2 + 2(\delta+\mu)(\mu-\nu)], \tag{5}$$

which is a strictly decreasing function of the noise δ introduced solely due to the macroscopic nature of the source, where $\mu = \cosh 2r$ and $\nu = \sinh 2r$. In a simple and straightforward calculation it could be shown that for V_{meas} the condition of nonzero logarithmic negativity $\Delta_{\text{meas}} > \det V_{\text{meas}} + 1$ yields

$$\delta < 1 - \cosh 2r + \sinh 2r. \tag{6}$$

For $\delta \geqslant 1 - \cosh 2r + \sinh 2r$, V_{meas} represents a separable state. Moreover, for $\delta = 1$, the state is always separable, i.e., for $\delta = 1$ there is no entanglement.

V. ANALYSIS OF KEY RATE: GAUSSIAN VS NON-GAUSSIAN RESOURCES

In this section we analyze the role of non-Gaussianity in mitigating the effect of mode mismatch in obtaining a secured key over distance. To be specific, we compare the attainable secured key rate for the TMSV, 1PSTMSV, and ZPCTMSV for various values of mode-mismatch noise. A brief account of the other channel parameters and evaluation of key rate could be found in Appendix C. It is important to note the operating

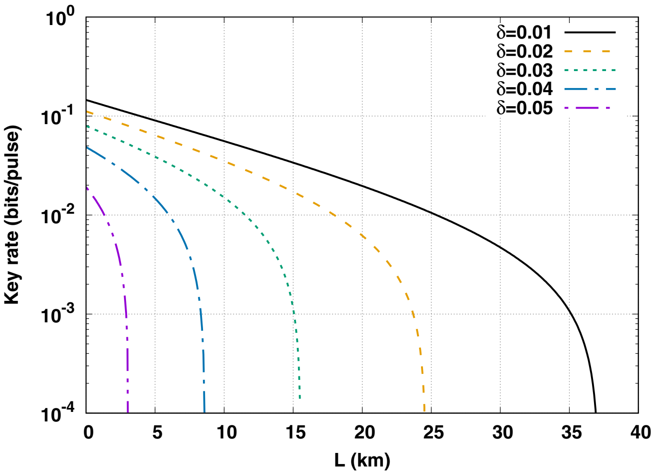

FIG. 4. Key rate vs length for the TMSV for different values of the noise parameter δ and $\eta = 1.0$.

parameter region for the squeezing strength at which CV QKD is performed. In line with [47,48,51–54,58], throughout the paper we consider $\cosh 2r = 50$.

A. Key rate vs transmission distance with an ideal detector

To ascertain the effectiveness of non-Gaussian operations, in Figs. 4–6 we plot the dependence of key rate on the distance L with ideal detectors ($\eta = 1$) for the TMSV, 1PSTMSV, and ZPCTMSV, respectively. In the case of the lowest value of mode-mismatch noise considered, i.e., $\delta = 0.01$, the ZPCTMSV yields the maximum attainable transmission distance of approximately 150 km, while it is limited to approximately 75 km and approximately 45 km for 1PSTMSV and TMSV, respectively. However, as it is evident from the figures, for all three resources, the maximum transmission distance uniformly decreases as the mode-mismatch noise increases. This implies that zero-photon catalysis appears to be highly efficient in the optimizing key rate vs transmission distance at a given noise strength.

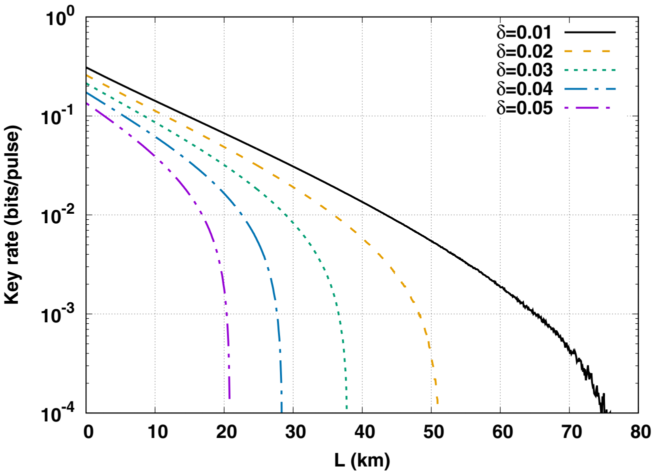

FIG. 5. Key rate vs length for the 1PSTMSV for different values of the noise parameter δ and $\eta = 1.0$.

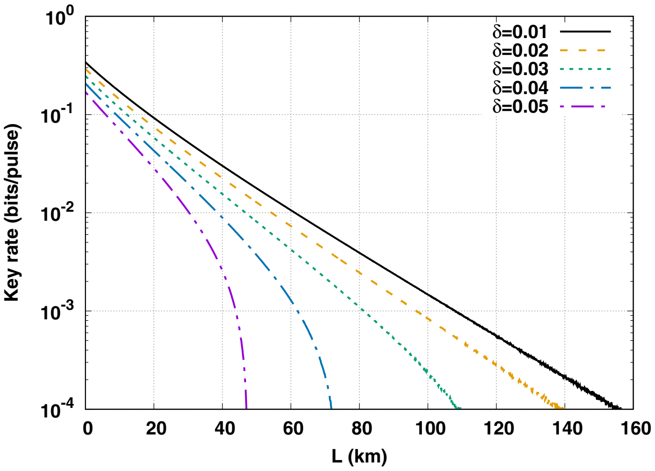

FIG. 6. Key rate vs length for the ZPCTMSV for different values of the noise parameter δ and $\eta = 1.0$.

B. Key rate vs transmission distance with a nearly perfect detector

From Figs. 4–6 it is evident that with an ideal detector ($\eta = 1.0$), one can attain a maximum transmission distance of approximately 150 km with the ZPCTMSV. However, in a realistic setup, detection efficiency is limited by the photon loss. Here we consider a case of 1% photon loss at the detector, leading to a detection efficiency of $\eta = 0.99$. In Fig. 7 we plot the secured key rate as a function of transmission distance for the TMSV, 1PSTMSV, and ZPCTMSV for $\eta = 0.99$. Compared to the case of an ideal detector, here the maximum transmission distance is reduced greatly for all three resources. To be specific, at $\delta = 0.01$, the ZPCTMSV yields a maximum distance of approximately 22 km, while it is limited to below 20 km for the 1PSTMSV and TMSV.

C. Key rate vs detection inefficiency

Figure 7 naturally poses the question of whether non-Gaussian resources are useful in obtaining robustness against the detector inefficiencies in CVQKD. To apprehend the situation better, in Fig. 8 we plot the dependence of the key rate K on the detector efficiency η for the TMSV, 1PSTMSV and ZPCTMSV at $L = 10$ km. As it is evident from the figure that even when two laboratories are separated by a distance of 10 km, below 98% detection efficiency ($\eta = 0.98$) there is hardly any obtainable secured key.

VI. PHOTON LOSS AS A LIMITING FACTOR FOR ZPS TMSV

Before we conclude, it is important to look at the practical concern of photon loss in generating the zero-photon-catalyzed TMSV. As described in Sec. II, a zero-photon-catalyzed TMSV is generated when the detector at the outgoing ancilla mode registers no photon or, in other words, the detector does not click. Under ideal conditions or, say, a perfect experimental setup, no click in the detector means collapse of the state in the $|0\rangle\langle 0|$ state, yielding zero-photon catalysis. However, in reality, there is an intrinsic technical

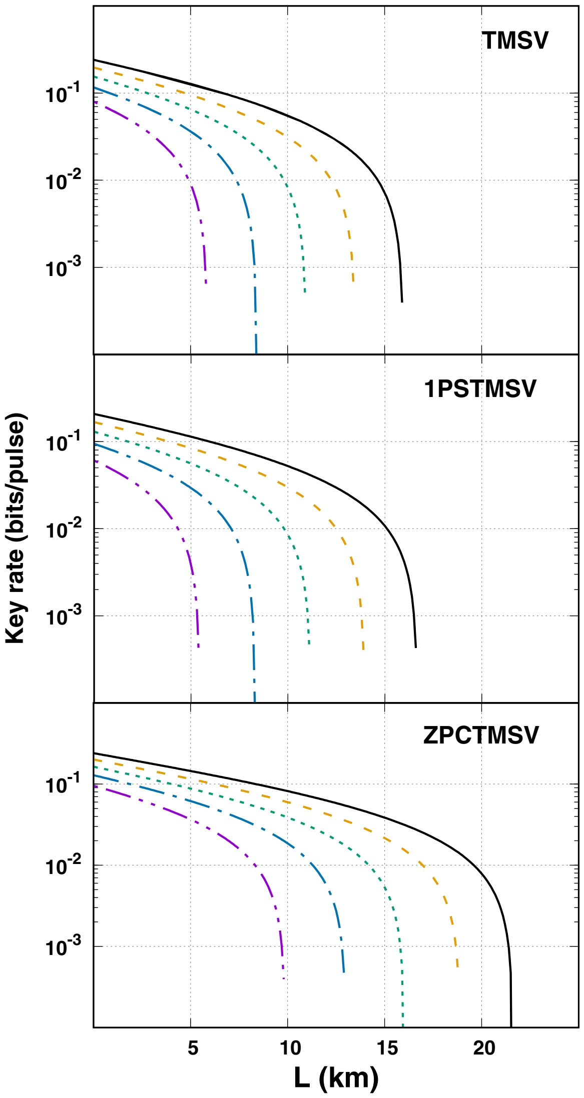

FIG. 7. Key rate vs length for the TMSV, 1PSTMSV, and ZPCTMSV at $\eta = 0.99$. Different curves correspond to $\delta = 0.01$ (black solid line), $\delta = 0.02$ (yellow dashed line), $\delta = 0.03$ (green dotted line), $\delta = 0.04$ (blue dash-dotted line), and $\delta = 0.05$ (magenta dash–double-dotted line).

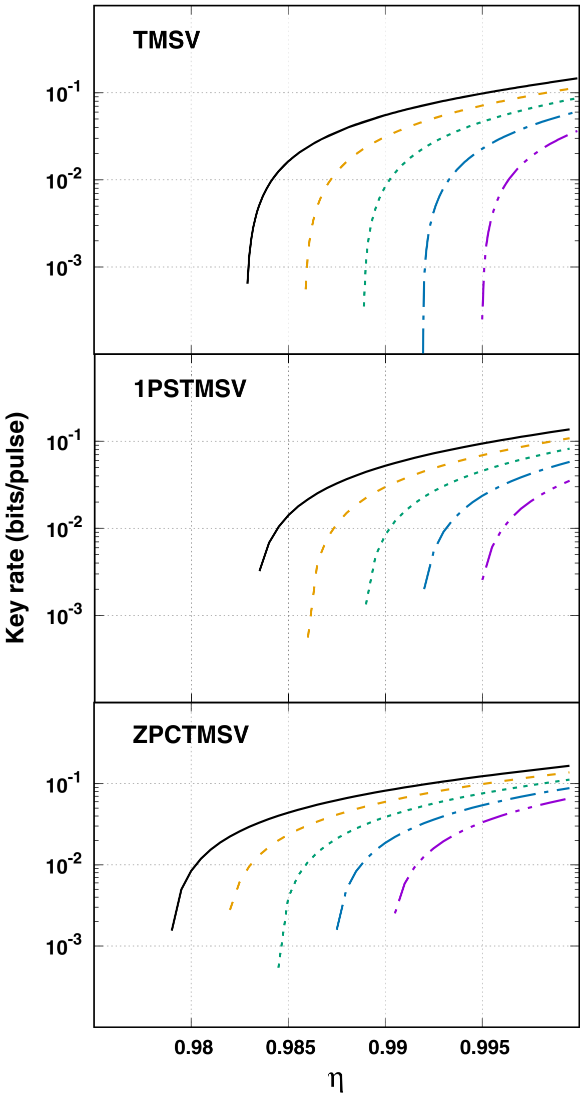

FIG. 8. Key rate vs detection efficiency for the TMSV, 1PSTMSV, and ZPCTMSV at $L = 10$ km. Different curves correspond to $\delta = 0.01$ (black solid line), $\delta = 0.02$ (yellow dashed line), $\delta = 0.03$ (green dotted line), $\delta = 0.04$ (blue dash-dotted line), and $\delta = 0.05$ (magenta dash–double-dotted line).

issue in generating a zero-photon-catalyzed TMSV using this method, as discussed below.

The no-click condition can appear in two characteristically different situations: when the photon in the outgoing ancilla mode is (a) collapsed in the $|0\rangle\langle 0|$ state or (b) lost. As a consequence, the effective variance matrix between Alice and Bob becomes

$$V_{AB} = pV_{\text{lost}} + (1-p)V_{\text{ZPC}}, \tag{7}$$

where p is the probability of losing the outgoing ancilla photon and V_{ZPC} is the variance matrix for the zero-photon-catalyzed TMSV. The variance matrix for the photon-loss case (V_{lost}) is given by $V_{\text{lost}} = \begin{pmatrix}\cosh 2r\mathbf{I} & \mathbf{0}\\ \mathbf{0} & \mathbf{I}\end{pmatrix}$, where $\mathbf{I}$ and $\mathbf{0}$ are the 2×2 identity and null matrices, respectively.

To illustrate the effect of photon loss in the generation of a zero-photon-catalyzed TMSV, in Fig. 9 we plot the maximum transmission distance as a function of probability of photon loss at different key rates for two different choices of mode-mismatch-noise strength, i.e., $\delta = 0.01$ and 0.02. As it is evident from the figure, as the probability increases the maximum attainable distance drops drastically. For a photon-loss probability as low as 0.5% ($p = 0.005$) there is no available key for any transmission distance. This may be interpreted as follows. The variance matrix for the photon-loss case (7) essentially represents a Gaussian lossy channel. Now, at the operating parameter region $\cosh 2r = 50$, the additional noise pV_{lost} in the variance matrix V_{AB} is significantly high to reduce the effective correlation and thus the key rate between Alice and Bob.

In Fig. 10 we further show the dependence of the secured key rate as a function of the transmission distance for the 0.2% probability of photon loss, i.e., $p = 0.002$, for different values of mode-mismatch noise. Compared to the no-photon-loss

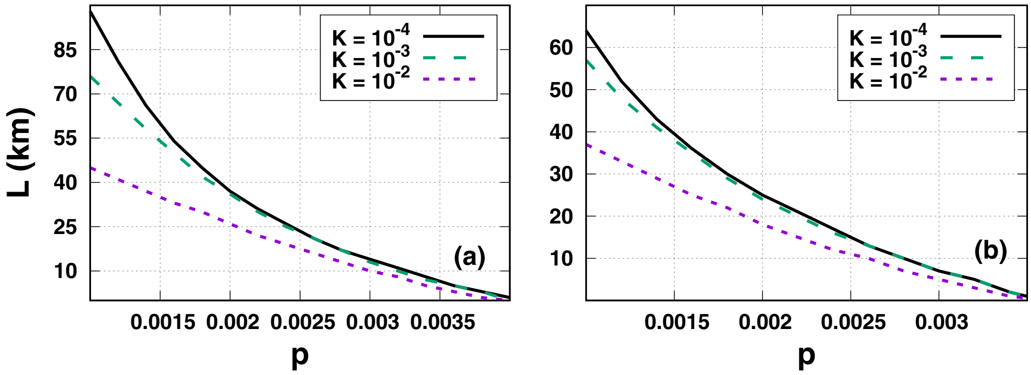

FIG. 9. Maximum transmission distance vs probability of photon loss for the ZPCTMSV at different key rates for (a) $\delta = 0.01$ and (b) $\delta = 0.02$. The other parameters are $T_{\mathrm{BS}} = 0.85$ and $\eta = 1.0$.

case (Fig. 6), even for such a small probability, the transmission distance is reduced significantly, from approximately 150 km to approximately 35 km.

VII. CONCLUSION

In this paper we have analyzed the role of non-Gaussianity in CV QKD with macroscopic light under mode mismatch. We have shown that non-Gaussian operations are helpful in mitigating the detrimental presence of unmatched modes and improve the overall performance reasonably well in comparison to the Gaussian case. To be specific, with the ideal detectors ($\eta = 1.0$) and low mode-mismatch noise ($\delta = 0.01$), the zero-photon catalysis and the single-photon subtraction lead to maximum transmission distances of approximately 150 km and approximately 70 km, while it is limited to approximately 45 km with the TMSV. The apparent superiority of the 1PSTMSV and ZPCTMSV over the TMSV could possibly be understood in terms of the entanglement-vs-loss relation for a state undergoing photon loss.

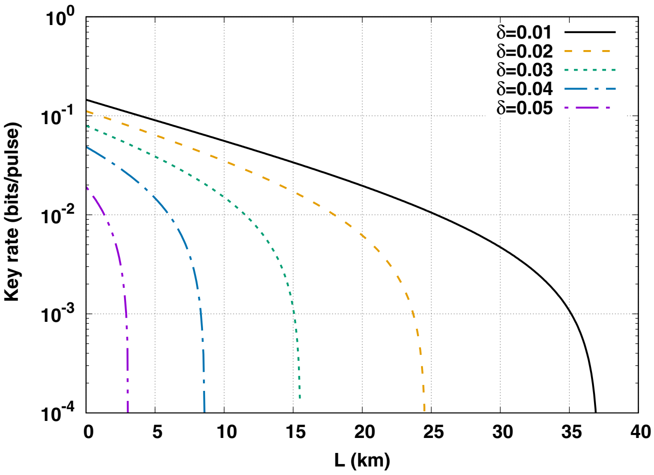

FIG. 10. Key rate vs transmission distance for the ZPCTMSV under the effect of photon loss for different δ. The photon loss probability is kept very low at $p = 0.002$. The other parameters are $T_{\mathrm{BS}} = 0.85$ and $\eta = 1.0$. Different curves correspond to $\delta = 0.01$ (black solid line), $\delta = 0.02$ (yellow dashed line), $\delta = 0.03$ (green dotted line), $\delta = 0.04$ (blue dash-dotted line), and $\delta = 0.05$ (purple dash–double-dotted line).

Transmission through a noisy channel (here optical fiber) could be seen as the state undergoing an effective photon loss, where the loss percentage is proportional to the transmission distance. In the case of the 1PSTMSV, photon subtraction leads to the excitation of higher-energy levels, which in turn increases the average energy of the initial TMSV. We believe that, due to this additional energy, it takes a longer transmission distance for the 1PSTMSV to lose the entanglement compared to the TMSV. On the other hand, zero-photon catalysis could be seen as a noiseless attenuation [53] that preserves the quantum coherence at a lower amplitude. This implies that the ZPCTMSV, at a fixed squeezing strength, experiences less loss compared to the TMSV, which in turn allows the ZPCTMSV to maintain the entanglement over a longer distance.

It is also intriguing to consider the fact that physical systems with higher mean energy, in general, are more fragile under noise, which is a well-known limiting factor in performing quantum tasks with macroscopic systems. In the case of the 1PSTMSV, while excitation of higher-energy levels contributes to more entanglement, their fragility under noise limits maximum attainable transmission distance. However, for the ZPCTMSV such a situation of competition between the fragility and mean energy is less dominant. We believe that this interplay between more mean energy and more fragility at higher energy plays a crucial role in improving the transmission distance with the non-Gaussian operations.

However, the practical concerns in performing zero-photon catalysis using linear optical setup limits the efficacy of the ZPCTMSV. In a realistic setup, zero-photon catalysis yields a maximum transmission distance of approximately 35 km, which is lower than the case of the TMSV. From this point of view, single-photon subtraction appears to be the optimal non-Gaussian operation, contrary to the result in [58].

Nonetheless, the non-Gaussian operations fail to offer improvement in resistance against the inefficiency of the homodyne detectors. It could be inferred from Fig. 7 that with a near-perfect detector, the maximum transmission distance decreases drastically Even for just 1% photon loss at the detector ($\eta = 0.99$), the maximum transmission distance becomes limited to approximately 22 km for the ZPCTMSV. In the case of the 1PSTMSV and TMSV it is further reduced to below 20 km. Furthermore, Fig. 7 indicates that below an almost ideal detection condition ($\eta \sim 98\%$) there is no secured key, irrespective of the mode-mismatch noise. This could in general be considered a common issue with the CV QKD protocols [29,60,61].

In the present work we have considered a simple model of additional noise that is present in the communication channel. We considered symmetric mode mismatch, i.e., the noise arising due mode mismatch in all the detectors is same. Although it serves as the primary motivation of the analysis, in practice, this is a serious restriction. Under a realistic setup the mode mismatch at different detectors could be different. Thus, for a comprehensive analysis one can consider different mode mismatch in different detectors. In addition, there may be am additional factor such as gain of the homodyne measurement or electronic noise of the detector that further reduces the key rate as well as the maximum transmission distance [48]. Moreover, our work was limited to the linear regime of the detectors. If the brightness of the signal is increased arbitrarily it may lead to the nonlinear response regime of the detectors. In that case there will be contributions from the additional modes which may in turn introduce additional noises. One can also extend the analysis on the role of non-Gaussianity in CV QKD with a different kind of noise such as state-preparation error [62–64] where the initial state suffers from side-channel loss prior to modulation. Nonetheless, compared to the simplistic entanglement-based protocol, one may further go for a more theoretically motivated model, such as a measurement-device-independent protocol, which is more promising from the point of view of ensuring security [48,49,52,54].

It may be noted that earlier analysis of CV QKD with macroscopic Gaussian light around mitigating the effect of mode mismatch by considering bright light [42] as well as rearranging the multiple modes [41]. The present work offers a different perspective in terms of enhancement in the performance of CV QKD with bright multimode light under mode mismatch by using non-Gaussianity as a resource. Here we have shown that certain non-Gaussian operations, in particular single-photon subtraction, can significantly enhance the transmission distance compared to the Gaussian case. Moreover, here we considered a key distribution protocol with both quadratures unlike the earlier works [41–43], where only one of the quadratures was taken into account. In view of the recent advances on the non-Gaussian operations [65,66], we believe that our work provides further understanding of non-Gaussianity as a resource in CV QKD with bright multimode light under the practical concern of mismatch between the signal and local oscillator modes.

ACKNOWLEDGMENTS

This work was supported by National Research Foundation of Korea grants funded by the Korean government (Grants No. 2023R1A2C1006115 and No. NRF-2022M3E4A1076099) via the Institute of Applied Physics at Seoul National University and by the Institute of Information & Communications Technology Planning & Evaluation grant funded by the Korea government (MSIT) (Grants No. IITP-2021-0-01059 and No. IITP-2023-2020-0-01606).

APPENDIX A: QUADRATURE MEASUREMENT OF MULTIMODE LIGHT UNDER MODE MISMATCH

In standard homodyne detection of a single-mode incoming light field, the mode is mixed with a local oscillator with a well-defined phase. This local oscillator is considered classical as its intensity is very high compared to the signal and it is described by the laser light with coherent amplitude α. In the case of multimode homodyne measurement or detection, one uses multiple local oscillators in different modes described by the set of coherent states $\{\alpha_i\}$, where $i = 1, 2, \ldots, K$, with K the total number of modes in the signal.

Let us consider that there is a total of $M + N$ incoming modes of light, out of which only M modes a_k match the local oscillators and the remaining N modes b_l do not match. For reference, consider Fig. 2. In the measurement setup M modes are mixed with the local oscillators in coherent states $\{\alpha_i\}$ and the rest of the N modes are mixed with the vacuum states V_j. Consequently, the output numbers $M + N$ of signal modes of the balanced BS (transmission is 50%) are given as

$$a^{\rm out}_{{\rm hor},i} = \frac{1}{\sqrt{2}}(a_i + \alpha_i), \quad b^{\rm out}_{{\rm hor},i} = \frac{1}{\sqrt{2}}(b_i + V_i),$$
$$a^{\rm out}_{{\rm ver},i} = \frac{1}{\sqrt{2}}(-a_i + \alpha_i), \quad b^{\rm out}_{{\rm ver},i} = \frac{1}{\sqrt{2}}(-b_i + V_i), \qquad \text{(A1)}$$

where hor and ver stand for horizontal and vertical, respectively. Horizontal light fields go to detector D_1 and the vertical light fields go to detector D_2. For the sake of simplicity, we further consider that all the coherent states have the same amplitude, i.e., $\alpha_i = \alpha \, \forall \, i = 1, 2, \ldots, M$.

If we assume that the detectors are identical and they detect the unmatched modes with efficiency ϵ, then the photons detected in detectors D_1 (n_1) and D_2 (n_2) are given as

$$\begin{aligned} n_1 &= \sum_{i=1}^{M} \left(a^{\rm out}_{{\rm hor},i}\right)^\dagger a^{\rm out}_{{\rm hor},i} + \epsilon \sum_{j=1}^{N} \left(b^{\rm out}_{{\rm hor},i}\right)^\dagger b^{\rm out}_{{\rm hor},i} \\ &= \frac{1}{2} \sum_{i=1}^{M} \{a_i^\dagger a_i + (a_i^\dagger \alpha + a_i \alpha^*) + \alpha^* \alpha\} \\ &\quad + \frac{\epsilon}{2} \sum_{j=1}^{N} \{b_j^\dagger b_j + (b_j^\dagger V_j + b_j V_j^\dagger) + V_j^\dagger V_j\}, \\ n_2 &= \sum_{k=1}^{M} \left(a^{\rm out}_{{\rm ver},k}\right)^\dagger a^{\rm out}_{{\rm ver},k} + \epsilon \sum_{l=1}^{N} \left(b^{\rm out}_{{\rm ver},l}\right)^\dagger b^{\rm out}_{{\rm ver},l} \\ &= \frac{1}{2} \sum_{k=1}^{M} \{a_k^\dagger a_k - (a_k^\dagger \alpha + a_k \alpha^*) + \alpha^* \alpha\} \\ &\quad + \frac{\epsilon}{2} \sum_{l=1}^{N} \{b_l^\dagger b_l - (b_l^\dagger V_l + b_l V_l^\dagger) + V_l^\dagger V_l\}. \end{aligned} \qquad \text{(A2)}$$

Let us consider $\alpha = |\alpha| e^{{\rm i}\phi}$. This leads to the photon-number difference Δ ($n_1 - n_2$) as

$$\Delta = |\alpha| \sum_{i=1}^{M} (a_i^\dagger e^{{\rm i}\phi} + a_i e^{-{\rm i}\phi}) + \epsilon \sum_{j=1}^{N} (b_j^\dagger V_j + b_j V_j^\dagger). \qquad \text{(A3)}$$

As it is quite explicit from Eq. (A3), by setting the phase of the local oscillators (ϕ), we can measure the quadrature. For example, $\phi = 0$ and $\phi = \pi/2$ yield x and p quadratures, respectively. Let us consider the specific case of $\phi = 0$. This yields

$$\Delta = |\alpha| \sum_{i=1}^{M} x_i + \epsilon \sum_{j=1}^{N} (b_j^\dagger V_j + b_j V_j^\dagger). \tag{A4}$$

The variance of an operator A is given as $\text{Var}(A) = \langle A^2 \rangle - \langle A \rangle^2$. In consideration of the fact that in the present case of multimode homodyne measurement all the modes are identical, we obtain the variance of Δ [Eq. (A4)] as

$$\begin{aligned}\text{Var}(\Delta) &= |\alpha|^2 \sum_{i=1}^{M} \text{Var}(x_i) + \epsilon^2 \sum_{j=1}^{N} \langle b_j^\dagger b_j \rangle \\ &= M|\alpha|^2 \text{Var}(x) + N\epsilon^2 \bar{n},\end{aligned} \tag{A5}$$

where $\bar{n}$ is the average photon number in the signal modes. However, this measurement result needs to be normalized. In the absence of the signal, the effective variance is given by $M|\alpha|^2$, arising solely due to the presence of local oscillators. Thus the normalized variance of the x quadrature for a multimode light under mode mismatch is obtained by dividing $\text{Var}(\Delta)$ by the zero-signal count $M|\alpha|^2$ as

$$\text{Var}(x)_{\text{norm}} = \text{Var}(x) + \frac{N\epsilon^2 \bar{n}}{M|\alpha|^2}. \tag{A6}$$

Similarly, we can write for p the quadrature also by setting $\phi = \pi/2$. As a consequence, we can write for both quadratures in a compact form

$$v_i \to v_i + \frac{N\epsilon^2 \bar{n}}{M|\alpha|^2} = v_i + \delta, \tag{A7}$$

where $v_i = \{\text{Var}(x), \text{Var}(p)\}$.

APPENDIX B: VARIANCE MATRIX FOR A *k*-PHOTON SUBTRACTED TMSV

Here we work with the Wigner function description for convenience. The Wigner functions for the TMSV and a single-mode photon-number state $|n\rangle$, in the shot-noise unit, are given as

$$\begin{aligned} W_{\text{TMSV}}(R_1, R_2) &= 4 \exp\left(-\frac{\mu^2 + \nu^2}{2}\left(x_1^2 + p_1^2 + x_2^2 + p_2^2\right) + 2\mu\nu(x_1x_2 - p_1p_2)\right), \\ W_{|n\rangle}(R) &= \frac{2(-1)^n}{n!} e^{-(x^2+p^2)/2} \mathscr{L}_n(x^2 + p^2) = \frac{2(-1)^n}{n!} e^{-(x^2+p^2)/2} \partial_\eta^n \partial_\zeta^n \left(e^{\eta\zeta + (x+\mathrm{i}p)\eta - (x-\mathrm{i}p)\zeta}\right)_{\eta,\zeta \to 0}, \end{aligned} \tag{B1}$$

where $R_i = \{x_i, p_i\}$ $(i = 1, 2)$, $R = (x, p)$, and $\mathscr{L}_n(x)$ is the nth-order Laguerre polynomial.

Let us now consider Fig. 1, where the linear optical model for photon subtraction is discussed (Sec. II A). In the very first step of photon subtraction, we mix one of the modes of the TMSV (say, mode 2) with the vacuum of an ancilla (say, mode 3) through a passive BS with transmittivity T_{BS}, leading to the three-mode Wigner function

$$\begin{aligned} W_{\text{TMSV}}(R_1, R_2) W_{|0\rangle}(R_3) &\xrightarrow{\text{BS}} W_{\text{out}}(R_1, R_2, R_3) \\ &= 8 \exp\left(-\frac{\mu^2 + \nu^2}{2}\left(x_1^2 + p_1^2\right)\right) \exp\left(-\frac{\mu^2 - (1 - 2T_{\text{BS}})\nu^2}{2}\left(x_2^2 + p_2^2\right) + 2\mu\nu\sqrt{T_{\text{BS}}}(x_1x_2 - p_1p_2)\right) \\ &\quad \times \exp\left(-\frac{\mu^2 + (1 - 2T_{\text{BS}})\nu^2}{2}\left(x_3^2 + p_3^2\right) + [2\nu\sqrt{1 - T_{\text{BS}}}(\nu\sqrt{T_{\text{BS}}}x_2 - \mu x_1)]x_3 \right. \\ &\qquad \left. + 2\nu\sqrt{1 - T_{\text{BS}}}(\nu\sqrt{T_{\text{bs}}}p_2 + \mu p_1)p_3\right). \end{aligned} \tag{B2}$$

Consequently, the Wigner function for the reduced state after projecting the ancilla mode on the number state $|n\rangle$ becomes

$$\begin{aligned} W_{\text{red}} &= \int \frac{dx_3 dp_3}{4\pi} W_{\text{out}}(R_1, R_2, R_3) W_{|n\rangle}^k(R_3) \\ &= 16\frac{(-1)^k}{k!} \exp\left(-\frac{\mu^2 + \nu^2}{2}\left(x_1^2 + p_1^2\right)\right) \exp\left(-\frac{\mu^2 - (1 - 2T_{\text{BS}})\nu^2}{2}\left(x_2^2 + p_2^2\right) + 2\mu\nu\sqrt{T_{\text{BS}}}(x_1x_2 - p_1p_2)\right) \\ &\quad \times \partial_\eta^k \partial_\zeta^k \left[e^{\eta\zeta} \int \frac{dx_3 dp_3}{4\pi} \exp\left\{-(\mu^2 - T_{\text{BS}}\nu^2)\left(x_3^2 + p_3^2\right) + [(\eta - \zeta) + 2\nu\sqrt{1 - T_{\text{BS}}}(\nu\sqrt{T_{\text{BS}}}x_2 - \mu x_1)]x_3 \right.\right. \\ &\qquad \left.\left. + [i(\eta + \zeta) + 2\nu\sqrt{1 - T_{\text{BS}}}(\nu\sqrt{T_{\text{BS}}}p_2 + \mu p_1)]p_3 \right\} \right]_{\substack{\eta=0 \\ \zeta=0}} \\ &= \frac{4(-1)^k}{k!(\mu^2 - T_{\text{BS}}\nu^2)} \exp\left(-\frac{\mu^2 + \nu^2}{2}\left(x_1^2 + p_1^2\right)\right) \exp\left(-\frac{\mu^2 - (1 - 2T_{\text{BS}})\nu^2}{2}\left(x_2^2 + p_2^2\right) + 2\mu\nu\sqrt{T_{\text{BS}}}(x_1x_2 - p_1p_2)\right) \end{aligned}$$

$$
\begin{aligned}
&\times \partial_\eta^k \partial_\zeta^k \bigg[e^{\eta\zeta} \exp\bigg(\frac{1}{4(\mu^2 - T_{\mathrm{BS}}\nu^2)} \{[(\eta-\zeta) + 2\nu\sqrt{1-T_{\mathrm{BS}}}(\nu\sqrt{T_{\mathrm{BS}}}x_2 - \mu x_1)]^2 + [i(\eta+\zeta) \\
&\qquad + 2\nu\sqrt{1-T_{\mathrm{BS}}}(\nu\sqrt{T_{\mathrm{BS}}}p_2 + \mu p_1)]^2\} \bigg) \bigg]_{\substack{\eta=0\\ \zeta=0}} \\
&= \frac{4(-1)^k}{k!(\mu^2 - T_{\mathrm{BS}}\nu^2)} \exp\left(-\frac{\mu^2+\nu^2}{2}(x_1^2 + p_1^2) \right) \exp\left(-\frac{\mu^2 - (1-2T_{\mathrm{BS}})\nu^2}{2}(x_2^2+p_2^2) + 2\mu\nu\sqrt{T_{\mathrm{BS}}}(x_1x_2 - p_1p_2) \right) \\
&\times \exp\left(\frac{\nu^2(1-T_{\mathrm{BS}})}{\mu^2 - T_{\mathrm{BS}}\nu^2}[(\nu\sqrt{T_{\mathrm{BS}}}x_2 - \mu x_1)^2 + (\nu\sqrt{T_{\mathrm{BS}}}p_2 + \mu p_1)^2] \right) \\
&\times \partial_\eta^k \partial_\zeta^k \bigg[\exp\bigg(\frac{\nu^2(1-T_{\mathrm{BS}})}{\mu^2 - T_{\mathrm{BS}}\nu^2}\eta\zeta + \frac{\sqrt{1-T_{\mathrm{BS}}}}{\mu^2 - T_{\mathrm{BS}}\nu^2}[\nu^2\sqrt{T_{\mathrm{BS}}}(x_2 + \mathrm{i}p_2) - \mu\nu(x_1 - \mathrm{i}p_1)]\eta \\
&\qquad - \frac{\sqrt{1-T_{\mathrm{BS}}}}{\mu^2 - \tau\nu^2}[\nu^2\sqrt{T_{\mathrm{BS}}}(x_2 - \mathrm{i}p_2) - \mu\nu(x_1 + \mathrm{i}p_1)]\zeta \bigg) \bigg]_{\substack{\eta=0\\ \zeta=0}} \\
&= (-A)^k W_0(R_1, R_2)\, \mathscr{L}_k\left(\frac{|R_{12}|^2}{\nu^2(\mu^2 - T_{\mathrm{BS}}\nu^2)} \right), \qquad \text{(B3)}
\end{aligned}
$$

where

$$
\begin{aligned}
A &= \frac{\nu^2(1-T_{\mathrm{BS}})}{(\mu^2 - T_{\mathrm{BS}}\nu^2)}, \quad R_{12} = \nu^2\sqrt{T_{\mathrm{BS}}}(x_2 + ip_2) - \mu\nu(x_1 - ip_1), \\
W_0(R_1, R_2) &= \frac{4}{\mu^2 - T_{\mathrm{BS}}\nu^2} \exp\left(-\frac{\mu^2+\nu^2}{2}(x_1^2+p_1^2) \right) \exp\left(-\frac{\mu^2 - (1-2T_{\mathrm{BS}})\nu^2}{2}(x_2^2+p_2^2) + 2\mu\nu\sqrt{T_{\mathrm{BS}}}(x_1x_2 - p_1p_2) \right) \\
&\quad \times \exp\left(\frac{1-T_{\mathrm{BS}}}{\mu^2 - T_{\mathrm{BS}}\nu^2}|R_{12}|^2 \right). \qquad \text{(B4)}
\end{aligned}
$$

The probability of obtaining the k TMSV is given as

$$
P_k = \int \frac{dx_1dp_1}{4\pi} \int \frac{dx_2dp_2}{4\pi} W_{\mathrm{red}}(R_1, R_2) = \frac{A^k}{\mu^2 - T_{\mathrm{BS}}\nu^2}, \qquad \text{(B5)}
$$

leading to the normalized Wigner function for the k TMSV,

$$
W^k_{\mathrm{TMSV}}(R_1, R_2) = \frac{1}{P_k} W_{\mathrm{red}}(R_1, R_2) = (\mu^2 - T_{\mathrm{BS}}\nu^2)(-1)^k W_0(R_1, R_2)\, \mathscr{L}_k\left(\frac{|R_{12}|^2}{\nu^2(\mu^2 - T_{\mathrm{BS}}\nu^2)} \right). \qquad \text{(B6)}
$$

To evaluate the variance matrix for the k TMSV, we first derive the general expression for the moment generating function as

$$
\begin{aligned}
C^{k,l}_{i,j} &= \langle x_1^i p_1^j x_2^k p_2^l \rangle = \int \frac{dx_1dp_1}{4\pi} \int \frac{dx_2dp_2}{4\pi} W^k_{\mathrm{TMSV}}(R_1, R_2) x_1^i p_1^j x_2^k p_2^l \\
&= \partial_a^i \partial_b^j \partial_c^k \partial_d^l \left(\int \frac{dx_1dp_1}{4\pi} \int \frac{dx_2dp_2}{4\pi} W^k_{\mathrm{TMSV}}(R_1, R_2) e^{ax_1 + bp_1 + cx_2 + dp_2} \right)_{\substack{a=0,b=0\\ c=0,d=0}} \\
&= \frac{1}{P_k} \frac{(-1)^k}{k!(\mu^2 - T_{\mathrm{BS}}\nu^2)} \partial_a^i \partial_b^j \partial_c^k \partial_d^l \Bigg\{ \exp\left(\frac{\mu^2 + T_{\mathrm{BS}}\nu^2}{2(\mu^2 - T_{\mathrm{BS}}\nu^2)}(a^2+b^2+c^2+d^2) + \frac{2\mu\nu\sqrt{T_{\mathrm{BS}}}}{\mu^2 - T_{\mathrm{BS}}\nu^2}(ac - bd) \right) \\
&\qquad \times \partial_\eta^k \partial_\zeta^k \left[\exp\left(-\frac{\nu^2(1-T_{\mathrm{BS}})}{\mu^2 - T_{\mathrm{BS}}\nu^2}\eta\zeta \right) \exp\left(-\frac{Z\sqrt{1-T_{\mathrm{BS}}}}{2(\mu^2 - T_{\mathrm{BS}}\nu^2)}\eta + \frac{Z^*\sqrt{1-T_{\mathrm{BS}}}}{2(\mu^2 - T_{\mathrm{BS}}\nu^2)}\zeta \right) \right]_{\substack{\eta=0\\ \zeta=0}} \Bigg\}_{\substack{a=0,b=0\\ s=0,t=0}} \\
&= \partial_a^i \partial_b^j \partial_c^k \partial_d^l \left[\exp\left(\frac{\mu^2 + T_{\mathrm{BS}}\nu^2}{2(\mu^2 - T_{\mathrm{BS}}\nu^2)}(a^2+b^2+c^2+d^2) + \frac{2\mu\nu\sqrt{T_{\mathrm{BS}}}}{\mu^2 - T_{\mathrm{BS}}\nu^2}(ac - bd) \right) \mathscr{L}_k\left(-\frac{|Z|^2}{4\nu^2(\mu^2 - T_{\mathrm{BS}}\nu^2)} \right) \right]_{\substack{a=0,b=0\\ c=0,d=0}}, \\
&\qquad \text{(B7)}
\end{aligned}
$$

where $Z = 2\mu\nu(a - ib) + 2\sqrt{\tau}\nu^2(c + id)$. By considering the symmetry of the state in a straightforward but tedious calculation, it could be shown that the variance matrix for the k TMSV is of the form $\begin{pmatrix} X\mathbf{I} & Z\sigma_3 \\ Z\sigma_3 & Y\mathbf{I} \end{pmatrix}$, where $\mathbf{I}$ and σ_3 are the 2×2 identity matrix and the Pauli Z matrix, respectively. The coefficients are given as

$$\begin{aligned} X = C^{0,0}_{2,0} = C^{0,0}_{0,2} &= \frac{\mu^2 + T_{\mathrm{BS}}\nu^2}{\mu^2 - T_{\mathrm{BS}}\nu^2} + \frac{2\mu^2}{\mu^2 - T_{\mathrm{BS}}\nu^2}\frac{L^1_{k-1}(0)}{L_k(0)} \\ &= \frac{\mu^2(2k+1) + T_{\mathrm{BS}}\nu^2}{\mu^2 - T_{\mathrm{BS}}\nu^2} = \frac{2(k+1)}{1 - T_{\mathrm{BS}}\tau^2} - 1, \end{aligned} \tag{B8}$$

$$\begin{aligned} Y = C^{2,0}_{0,0} = C^{0,2}_{0,0} &= \frac{\mu^2 + T_{\mathrm{BS}}\nu^2}{\mu^2 - T_{\mathrm{BS}}\nu^2} + \frac{2\nu^2 T_{\mathrm{BS}}}{\mu^2 - T_{\mathrm{BS}}\nu^2}\frac{L^1_{k-1}(0)}{L_k(0)} \\ &= \frac{\mu^2 + T_{\mathrm{BS}}\nu^2(2k+1)}{\mu^2 - T_{\mathrm{BS}}\nu^2} = \frac{2(1 + kT_{\mathrm{BS}}\tau^2)}{1 - T_{\mathrm{BS}}\tau^2} - 1, \end{aligned} \tag{B9}$$

and

$$\begin{aligned} Z = C^{1,0}_{1,0} = -C^{0,1}_{0,1} &= \frac{2\mu\nu\sqrt{T_{\mathrm{BS}}}}{\mu^2 - T_{\mathrm{BS}}\nu^2}\left(1 + \frac{L^1_{k-1}(0)}{L_k(0)}\right) \\ &= \frac{2\mu\nu\sqrt{T_{\mathrm{BS}}}(1+k)}{\mu^2 - T_{\mathrm{BS}}\nu^2}. \end{aligned} \tag{B10}$$

APPENDIX C: CHANNEL PARAMETERS AND KEY RATE

In the entanglement-based scheme, one of the parties, say, Alice, generates a two-mode entangled resource and sends one of the modes to a distant party, say, Bob, through optical cables which are lossy in general. The transmittance loss of the channel is quantified as $T = \frac{1}{2}10^{-lL/10}$, where $l = 0.2$ (dB/km) is the loss per kilometer and L is the distance between Alice and Bob. This transmittance through lossy channel leads to the line noise given as $\chi_{\mathrm{line}} = \frac{1-T}{T}$. On the other hand, the homodyne detectors, used by Alice and Bob, are not perfect, in general. The imperfection in the detector further leads to homodyne noise as $\chi_{\mathrm{homo}} = \frac{1-\eta}{\eta}$, where η is the efficiency of the detectors. Under these assumptions, the total additional noise, introduced in the variance matrix, due to channel transmission and a noisy detector, could be written as

$$\chi_{\mathrm{tot}} = \chi_{\mathrm{line}} + \frac{2\chi_{\mathrm{homo}}}{T}. \tag{C1}$$

Let us consider the variance matrix generated by Alice given as $V = \begin{pmatrix} V_A & V_C \\ V_C^{\mathsf{T}} & V_B \end{pmatrix}$, where V_A and V_B correspond to the subsystems of Alice and Bob, while V_C is the correlation between them. Under the effect of channel transmission and noisy detectors, the final variance matrix becomes $V' = \begin{pmatrix} V'_A & V'_C \\ V'^{\mathsf{T}}_C & V'_B \end{pmatrix} = \begin{pmatrix} V_A & \sqrt{T}V_C \\ \sqrt{T}V_C^{\mathsf{T}} & T(V_B + \chi_{\mathrm{tot}}\mathbf{I}_2) \end{pmatrix}$, where $\mathbf{I}_2$ is the 2×2 identity matrix. Here T stands for transposition.

It is natural to think of an adversary, say, Eve, trying to hack and obtain information about the communication or quantum state between Alice and Bob. We assume that Eve can perform independent one-mode collective attacks on each channel. In this scenario, the secured raw key rate is given by [67]

$$K = \beta I_{AB} - \chi_{\mathrm{Hol}}, \tag{C2}$$

where I_{AB} is the mutual information between Alice and Bob and χ_{Hol} is the maximum information available to Eve which is given by the Holevo bound [68]. Here we have considered reverse reconciliation, i.e., Bob tallies his measurement data with Alice, as it offers a better key rate and it is more robust than the direct reconciliation where Alice tallies her results with Bob. As a consequence, χ_{Hol} is given by the maximum information bound on Eve due to Bob's data and is denoted by χ_{BE}. We now consider the transmitted variance matrix between Alice and Bob, V', to evaluate the key rate.

In any CV QKD protocol, the key rate is obtained by considering the equivalent prepare-and-measure (P&M) protocol. Moreover, we consider the no-switching protocol, i.e., instead of homodyne measurements (measuring either of x and p), we consider heterodyne measurement (measuring both x and p). Consequently, the mutual information between Alice and Bob is given by

$$I_{AB} = \frac{1}{2}\log_2\left(\frac{V'^x_{A_m}}{V'^x_{A_m|B_m}}\right) + \frac{1}{2}\log_2\left(\frac{V'^p_{A_m}}{V'^p_{A_m|B_m}}\right), \tag{C3}$$

with a contribution coming from the measurements of both x and p quadratures. Here $V'^\zeta_{A_m}$ and $V'^\zeta_{A_m|B_m}$ ($\zeta = x, p$) are the measured quadratures for Alice's subsystem and Alice's conditional subsystem based on Bob's measurement. These are mathematically described as $V'^\zeta_{A_m} = (V'^\zeta_A + 1)/2$ and $V'^\zeta_{A_m|B_m} = (V'^\zeta_{A|B} + 1)/2$, where

$$V'_{A|B} = V'_A - V'^{\mathsf{T}}_C(V'_B + I)^{-1}V'_C. \tag{C4}$$

On the other hand, the Holevo bound between Bob and Eve is defined as [68]

$$\begin{aligned} \chi_{BE} &= S(\rho_{BE}) - \int dm_B P(m_B) S(\rho^{m_B}_{BE}) \\ &= S(\rho_{AB}) - S(\rho_{A|B}), \end{aligned} \tag{C5}$$

where $S(\rho)$ denotes the von Neumann entropy of the state ρ, m_B is Bob's measurement outcome with probability $P(m_B)$, and $\rho^{m_B}_{BE}$ is Eve's state conditioned on Bob's corresponding measurement. In terms of the total variance matrix between Alice and Bob (V') and Alice's conditional variance matrix based on Bob's measurement ($V'_{A|B}$), we can easily obtain the Holevo bound as

$$\begin{aligned} S(\rho_{AB}) &= G\left(\frac{\lambda_1 - 1}{2}\right) + G\left(\frac{\lambda_2 - 1}{2}\right) \\ S(\rho_{A|B}) &= G\left(\frac{\lambda_3 - 1}{2}\right), \end{aligned} \tag{C6}$$

where $G(x) = (x+1)\log_2(x+1) - x\log_2 x$, and $\{\lambda_1, \lambda_2\}$ and λ_3 are the symplectic eigenvalues of V' and $V'_{A|B}$, respectively.

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

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

[3] R. Rivest, A. Shamir, and L. Adleman, Commun. ACM **21**, 120 (1978).

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

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

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

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

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

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

[10] M. Agrawal, N. Kayal, and N. Saxena, Ann. Math. **160**, 781 (2004).

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

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

[13] M. Pawlowski, Phys. Rev. A **82**, 032313 (2010).

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

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

[16] I. Kogias, Y. Xiang, Q. He, and G. Adesso, Phys. Rev. A **95**, 012315 (2017).

[17] K. Bradler and C. Weedbrook, Phys. Rev. A **97**, 022310 (2018).

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

[19] A. Leverrier, R. Garcia-Patron, R. Renner, and N. J. Cerf, Phys. Rev. Lett. **110**, 030502 (2013).

[20] L. Ruppert, V. C. Usenko, and Radim Filip, Phys. Rev. A **90**, 062310 (2014).

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

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

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

[24] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dusek, N. Lutkenhaus, and M. Peev, Rev. Mod. Phys. **81**, 1301 (2009).

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

[26] J. Lodewyck, M. Bloch, R. Garcia-Patron, 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).

[27] P. Jouguet, S. Kunz-Jacques, A. Leverrier, P. Grangier, and E. Diamanti, Nat. Photon. **7**, 378 (2013).

[28] J.-Y. Wang, B. Yang, S.-K. Liao, L. Zhang, Q. Shen, X.-F. Hu, J.-C. Wu, S.-J. Yang, H. Jiang, Y.-L. Tang *et al.*, Nat. Photon. **7**, 387 (2013).

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

[30] C. S. Jacobsen, T. Gehring, and U. L. Andersen, Entropy **17**, 4654 (2015).

[31] D. Huang, D. Lin, C. Wang, W. Liu, S. Fang, J. Peng, P. Huang, and G. Zeng, Opt. Express **23**, 17511 (2015).

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

[33] C. W. Lee and H. Jeong, Phys. Rev. Lett. **106**, 220401 (2011).

[34] J. Hald, J. L. Sørensen, C. Schori, and E. S. Polzik, Phys. Rev. Lett. **83**, 1319 (1999).

[35] T. Fernholz, H. Krauter, K. Jensen, J. F. Sherson, A. S. Sorensen, and E. S. Polzik, Phys. Rev. Lett. **101**, 073601 (2008).

[36] T. Iskhakov, M. V. Chekhova, and G. Leuchs, Phys. Rev. Lett. **102**, 183602 (2009).

[37] G. Toth and M. W. Mitchell, New J. Phys. **12**, 053007 (2010).

[38] T. S. Iskhakov, I. N. Agafonov, M. V. Chekhova, and G. Leuchs, Phys. Rev. Lett. **109**, 150502 (2012).

[39] N. Behbood, F. M. Ciurana, G. Colangelo, M. Napolitano, G. Tóth, R. J. Sewell, and M. W. Mitchell, Phys. Rev. Lett. **113**, 093601 (2014).

[40] G. Vasilakis, H. Shen, K. Jensen, M. Balabas, D. Salart, B. Chen, and E. S. Polzik, Nat. Phys. **11**, 389 (2015).

[41] V. C. Usenko, L. Ruppert, and R. Filip, Phys. Rev. A **90**, 062326 (2014).

[42] V. C. Usenko, L. Ruppert, and R. Filip, Opt. Express **23**, 31534 (2015).

[43] O. Kovalenko, K. Y. Spasibko, M. V. Chekhova, V. C. Usenko, and R. Filip, Opt. Express **27**, 36154 (2019).

[44] I. Derkach, V. C. Usenko, and R. Filip, Phys. Rev. A **93**, 032309 (2016).

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

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

[47] Y. Guo, Q. Liao, Y. Wang, D. Huang, P. Huang, and G. Zeng, Phys. Rev. A **95**, 032304 (2017).

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

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

[50] W. Ye, H. Zhong, Q. Liao, D. Huang, L. Hu, and Y. Guo, Opt. Express **27**, 17186 (2019).

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

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

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

[54] W. Ye, H. Zhong, X. Wu, L. Hu, and Y. Guo, Quantum Inf. Process. **19**, 346 (2020).

[55] U. L. Andersen, G. Leuchs, and C. Silberhorn, Laser Photon. Rev. **4**, 337 (2010).

[56] C. Weedbrook, A. M. Lance, W. P. Bowen, T. Symul, T. C. Ralph, and P. K. Lam, Phys. Rev. Lett. **93**, 170504 (2004).

[57] Y. Zhang, S. Yu, and H. Guo, Quantum Inf. Process. **14**, 4339 (2015).

[58] J. Singh and S. Bose, Phys. Rev. A **104**, 052605 (2021).

[59] G. Adesso and F. Illuminati, Phys. Rev. A **72**, 032334 (2005).

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

[61] S. Pirandola, C. Ottaviani, G. Spedalieri, C. Weedbrook, S. L. Braunstein, S. Lloyd, T. Gehring, C. S. Jacobsen, and U. L. Andersen, Nat. Photon. **9**, 773 (2015).

[62] I. Derkach, V. C. Usenko, and R. Filip, Phys. Rev. A **96**, 062309 (2017).

[63] W. Zhang, R. Li, Y. Wang, X. Wang, L. Tian, and Y. Zheng, Opt. Express **29**, 22623 (2021).

[64] N. Jain, I. Derkach, H.-M. Chin, R. Filip, U. L. Andersen, V. C. Usenko, and T. Gehring, Quantum Sci. Technol. **6**, 045001 (2021).

[65] H. Zhong, Y. Guo, Y. Mao, W. Ye, and D. Huang, Sci. Rep. **10**, 17526 (2020).

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

[67] I. Devetak and A. Winter, Proc. R. Soc. London A **461**, 207 (2005).

[68] A. S. Holevo, Probl. Peredachi Inf. **9**, 3 (1973); Probl. Inf. Transm. **9**, 177 (1973).