npj | Quantum Information

www.nature.com/npjqi

Corrected: Publisher Correction

ARTICLE OPEN

Quantum non-Gaussianity and secure quantum communication

Jaehak Lee[1], Jiyong Park[2] and Hyunchul Nha[1]

No-cloning theorem, a profound fundamental principle of quantum mechanics, also provides a crucial practical basis for secure quantum communication. The security of communication can be ultimately guaranteed if the output fidelity via the communication channel is above the no-cloning bound (NCB). In quantum communications using continuous-variable (CV) systems, Gaussian states, more specifically, coherent states have been widely studied as inputs, but less is known for non-Gaussian states. We aim at exploring quantum communication covering CV states comprehensively with distinct sets of unknown states properly defined. Our main results here are (i) to establish the NCB for a broad class of quantum non-Gaussian states, including Fock states, their superpositions, and Schrodinger-cat states and (ii) to examine the relation between NCB and quantum non-Gaussianity (QNG). We find that NCB typically decreases with QNG. Remarkably, this does not mean that QNG states are less demanding for secure communication. By extending our study to mixed-state inputs, we demonstrate that QNG specifically in terms of Wigner negativity requires more resources to achieve output fidelity above NCB in CV teleportation. The more non-Gaussian, the harder to achieve secure communication, which can have crucial implications for CV quantum communications.

npj Quantum Information (2019)5:49 ; https://doi.org/10.1038/s41534-019-0164-9

INTRODUCTION

No-cloning theorem is one of the fundamental quantum principles also providing a crucial practical basis for quantum communication—an eavesdropper cannot gain information without disturbing the quantum state carrying information. Numerous works studied an approximate cloning scheme, making clones with imperfect quality[1–4] and rigorously established as a security benchmark the no-cloning bound (NCB), above which the output fidelity of two clones cannot reach.[4–9] If a receiver obtains an output state with fidelity higher than NCB, he can be assured of no better copy existing elsewhere and extract more information than Eve—an ultimate security of communication. Such a connection was specifically made between the optimal cloning and the security of quantum cryptographic protocols.[4,6,10–12]

The NCB varies with the set of input states and it is of crucial importance to identify it for different input states to address communication security relevant to various protocols. In quantum communication using continuous variables (CVs), coherent states are readily available information carriers and have been mostly employed as input states to many protocols, e.g., quantum cryptography[12] and quantum teleportation.[13] Furthermore, it was recently proved that coherent states are the optimal input states achieving the ultimate classical capacity of bosonic Gaussian channels.[14,15] The NCB of coherent states was well studied with some extension to other Gaussian (squeezed) states.[7,8,16] On the other hand, quantum non-Gaussian (QNG) states have recently drawn much attention as an essential ingredient for quantum information processing, due to the limited capability of Gaussian states and operations in some crucial tasks, e.g., entanglement distillation,[17] quantum computation,[18] and error correction.[19] However, little is known about non-Gaussian states, particularly their NCBs and the critical role played by their quantum non-Gaussianity (QNG) in quantum communications. QNG here refers to the characteristic of non-Gaussian states that cannot be represented as a mixture of Gaussian states, with its measure rigorously quantifying distinction between those two sets of states.[20] For instance, some studies investigated several non-Gaussian input states for CV teleportation,[21–23] which however lacks the analysis of performance in view of ultimate security, with no access to the NCB benchmark. We need to extend our approach to deal with a broad class of QNG states and to rigorously identify NCB and its relation to QNG in quantum communications. By doing so, we may address some important issues, e.g., comparing performance and security conditions between Gaussian and non-Gaussian states in CV quantum information protocols.[24–31]

Our objective is twofold. First, we intend to establish NCB for QNG states broadly to gain insight into the non-Gaussian regime. Second, we intend to identify the role played by QNG for CV quantum communications. There has recently been a growing interest in studying QNG as a resource under the framework of resource theories,[20,32,33] with its operational significance largely unexplored.[34] We here find a strong correlation between QNG and NCB—NCB overall decreases with QNG. Importantly, this does not mean that achieving ultimate security becomes easier with QNG states. We show that non-Gaussian input states require more resources to achieve secure teleportation,[13,35,36] even though NCB is smaller. This implies that the security of CV teleportation can be most readily attained when employing Gaussian input states.

[1]Department of Physics, Texas A & M University at Qatar, P.O. Box 23874, Doha, Qatar and [2]School of Basic Sciences, Hanbat National University, Daejeon 34158, Korea
Correspondence: Hyunchul Nha (hyunchul.nha@qatar.tamu.edu)

Received: 15 October 2018 Accepted: 15 May 2019
Published online: 14 June 2019

RESULTS

To address CV states comprehensively and systematically, we first define a set of states as $S_{|\psi\rangle} \equiv \{\hat{D}(\alpha)|\psi\rangle \ \forall \alpha \in C\}$, where each set $S_{|\psi\rangle}$ consists of a pure state $|\psi\rangle$ arbitrarily displaced in phase space $\hat{D}(\alpha) \equiv e^{\alpha a^\dagger - \alpha^* a}$ (Fig. 1a). The set of coherent states is a special case with $|\psi\rangle = |0\rangle$ (vacuum). In generalizing CV states this way, we may examine QNG states comprehensively varying the state $|\psi\rangle$ for each set. Furthermore, displacement operation provides an important protocol of information encoding for CV communications. Quantum teleportation of coherent states corresponds to transmitting information on the unknown displacement in phase space for a given seed state $|0\rangle$. In addition, the ultimate classical capacity under Gaussian channels uses encoding based on displacement as an optimal scheme.[14,15] A full displacement in phase space can represent an increasingly large amount of information.

Covariant cloning machine

We first investigate the cloning of Fock states (prominently QNG) under displacement, i.e., the sets $S_{|\psi\rangle=|n\rangle}$, which will be extended to other non-Gaussian states, like superposition of Fock states and Schrodinger-cat states later. Our goal is to maximize the output fidelity averaged over all input displacements α for a given set $S_{|n\rangle}$. For simplicity, we assume that the distribution of unknown α is uniform in the whole phase space. For a 1-to-M cloning map T, the fidelity of the ith clone is expressed as

$$F^{(i)} = Tr\left[T(\rho_{\text{in}})\rho_{\text{in}}^{(i)}\right], \tag{1}$$

where $\rho^{(i)} \equiv 1 \otimes \cdots \otimes 1 \otimes \rho \otimes 1 \otimes \cdots \otimes 1$ has its component ρ on the ith system, whereas others are given by identity operator 1. Let us consider a symmetric cloner with identical fidelity for each i. The optimal cloner can then be given by a covariant cloner,[9,37] with the covariance property $T(\rho) = T_\beta(\rho)$ regardless of β (see the "Methods" section), where

$$T_\beta(\rho) = \hat{D}^{\dagger\otimes M}(\beta) T\left[\hat{D}(\beta)\rho\hat{D}^\dagger(\beta)\right]\hat{D}^{\otimes M}(\beta) \tag{2}$$

is a shifted cloner. If an input state is displaced by β, each output state is also displaced by the same β. With this covariance, input and output states must satisfy the relation in terms of the characteristic function $\chi(\xi) = tr[\rho\hat{D}(\xi)]$[38] as[9,37]

$$\chi_{\text{out}}(\boldsymbol{\xi}) = \chi_T(\Omega\boldsymbol{\xi})\chi_{\text{in}}\left(\sum_i \xi_i\right). \tag{3}$$

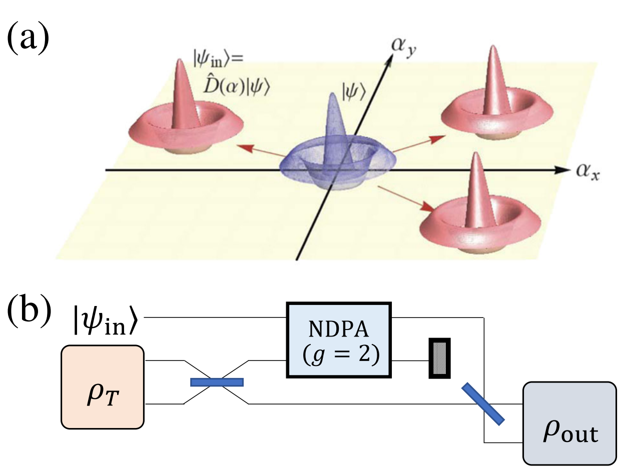

Fig. 1 **a** A quantum state $|\psi\rangle$ is displaced by an unknown amplitude in phase space, which defines a set of states $S_{|\psi\rangle} \equiv \{\hat{D}(\alpha)|\psi\rangle \ \forall\alpha \in C\}$. An example of a non-Gaussian state $|\psi\rangle = |2\rangle$ is shown. **b** Optimal $1 \to 2$ cloner can be implemented by a nondegenerate parametric amplifier (NDPA) and 50/50 beamsplitters with an ancilla state ρ_T optimized

Here, Ω is a linear transformation acting as $\xi_{i,p} \to \xi_{i,x}$ and $\xi_{i,x} \to \sum_{j\neq i} \xi_{j,p}$ with $\boldsymbol{\xi} = (\xi_{1,x}, \ \xi_{1,p}, \ \ldots, \ \xi_{M,x}, \ \xi_{M,p})$ and $\chi_T(\boldsymbol{\xi})$ is the characteristic function of a certain M-mode state ρ_T. That is, our problem is reduced to finding an optimal state ρ_T giving a maximal fidelity through Eq. (1). This ρ_T can be utilized as a resource state to construct the optimal cloner[9] and the equivalent telecloning protocol.[39] For instance, the optimal $1 \to 2$ cloner can be realized using a scheme in Fig. 1b.

Using Eq. (3), the fidelity in Eq. (1) for each n is given, with details in Supplementary Section 1, by

$$F_n^{(i)} \equiv \left\langle \hat{f}_n^{(i)} \right\rangle_{\rho_T} = \left\langle [L_n(\hat{O}_i)]^2 e^{-\hat{O}_i} \right\rangle_{\rho_T}, \tag{4}$$

where $\hat{O}_i \equiv \frac{1}{2}\left[\hat{x}_i^2 + (\sum_{j\neq i}\hat{p}_j)^2\right]$ with $\hat{x}_i$ and $\hat{p}_i$ being position and momentum operators of the ith mode, respectively, and L_n the Laguerre polynomial of order n. NCB of our interest is given by considering the case of two clones ($M = 2$), with the average fidelity $\frac{1}{2}(F_n^{(1)} + F_n^{(2)})$ optimized over a resource state ρ_T. That is, NCB corresponds to the maximum eigenvalue of the operator $\frac{1}{2}(\hat{f}_n^{(1)} + \hat{f}_n^{(2)})$ [see Supplementary Section 1]. For instance, the NCB~0.6826 for coherent-state inputs ($n = 0$) is given by the maximum eigenvalue of $\frac{1}{2}(e^{-\frac{1}{2}(\hat{x}_1^2+\hat{p}_2^2)} + e^{-\frac{1}{2}(\hat{x}_2^2+\hat{p}_1^2)})$.[9,37]

Invariance under Gaussian unitaries. Remarkably, NCB is invariant under Gaussian unitary operations. Namely, NCBs for the two sets $S_{|\psi\rangle}$ and $S_{\hat{U}_G|\psi\rangle}$ are identical, where $\hat{U}_G$ is an arbitrary Gaussian unitary (Methods). Thus, all pure Gaussian states attain the same NCB, which was mentioned for the Gaussian cloners, using only Gaussian resource states,[7,8] but the same is true with general covariant cloners using non-Gaussian resources for any input state. For instance, the Fock states and the squeezed Fock states have the same NCBs, which make our result encompass non-Gaussian states more broadly.

Gaussian no-cloning bound

Before we deal with the ultimate cloning limit, it is worth investigating NCB under the constraint of Gaussian operations, because Gaussian operations are highly feasible in the laboratory.[16] ρ_T in Eq. (2) is then a Gaussian state with $\chi_T(\Omega\boldsymbol{\xi}) = \exp\left(-\frac{1}{2}\boldsymbol{\xi}^T\gamma_t\boldsymbol{\xi}\right)$ and $\gamma_t = a1_M \otimes 1_2 + b(\mathbb{E}_M - 1_M) \otimes 1_2$ for a symmetric covariant cloner [see Supplementary Section 3] (1_d: $d \times d$ identity matrix, $\mathbb{E}_d$: $d \times d$ matrix with $(\mathbb{E}_d)_{i,j} = 1$ for all i, j). The positivity of the cloning transformation is fulfilled if and only if $a - b \geq 1$ and $a + (M-1)b \geq M - 1$. We find that the maximum fidelity is achieved, interestingly regardless of Fock states, at $a = \frac{2M-2}{M}$ and $b = \frac{M-2}{M}$, with details in Supplementary Section 3. For $M = 2$, we obtain the Gaussian NCB $F_0^{(G)\text{nc}} = \frac{2}{3} \simeq 0.6667$, $F_1^{(G)\text{nc}} = \frac{10}{27} \simeq 0.3704$, $F_2^{(G)\text{nc}} = \frac{22}{81} \simeq 0.2716$, and $F_3^{(G)\text{nc}} = \frac{490}{2187} \simeq 0.2241$, which rapidly decreases with n.

Ultimate no-cloning bound

Although Gaussian NCB is a useful benchmark, the ultimate NCB must be obtained by optimizing over all possible physical operations. The problem is to find the maximum value of $\frac{1}{2}\left\langle \hat{f}_n^{(1)} + \hat{f}_n^{(2)} \right\rangle_{\rho_T}$ over all quantum states ρ_T. We examine the largest eigenvalue of the corresponding operator in the truncated Fock-state basis $|n_1, n_2\rangle$ with $0 \leq n_1, n_2 \leq N_{\text{trunc}}$. The density matrix elements of Eq. (4) can be evaluated using position(momentum) representation of Fock states [see Supplementary Section 1]. We numerically obtain the ultimate NCB decreasing with n as $F_0^{\text{nc}} \simeq 0.6826$, $F_1^{\text{nc}} \simeq 0.5449$, $F_2^{\text{nc}} \simeq 0.5145$, and $F_3^{\text{nc}} \simeq 0.5033$ with $N_{\text{trunc}} = 300$. We have checked that our results are stable with a negligible change over varied N_{trunc} [see Supplementary Fig. 1].

Our method also gives the same known NCB for the coherent-state inputs in ref. [9]

For non-Gaussian states, there is a substantial difference between the ultimate NCB and the Gaussian NCB, whereas the difference is quite small for Gaussian states. For the coherent-state input, while each component operator $\hat{f}_0^{(i)}$ to determine fidelity is Gaussian, the sum of those two operators $\frac{1}{2}(\hat{f}_0^{(1)} + \hat{f}_0^{(2)}) = \frac{1}{2}(e^{-\frac{1}{2}(\hat{x}_1^2+\hat{p}_2^2)} + e^{-\frac{1}{2}(\hat{x}_2^2+\hat{p}_1^2)})$ is non-Gaussian, which makes the non-Gaussian cloning an optimal cloner. For non-Gaussian input states, on the other hand, each component operator $\hat{f}_n^{(i)}$ itself is already non-Gaussian, not to mention their sum. While Gaussian states also require non-Gaussian resources for optimal cloning,[9] our result clearly shows that non-Gaussian resources are more essential to optimally clone non-Gaussian inputs.

Secure teleportation and QNG

We now demonstrate that the smaller NCB does not merely mean "easy to achieve" by examining an important communication protocol—CV quantum teleportation.[13] The output state of CV teleportation can be described by $\chi_{\text{out}}(\xi) = \chi_{\text{in}}(\xi)\chi_{AB}(\xi^*, \xi)$ where $\chi_{AB}(\xi_1, \xi_2)$ is the characteristic function of the two-mode resource state.[30,40] Let us consider a typical resource, i.e., two-mode squeezed state (TMSV) to illustrate a general trend. The teleportation fidelity is then given by $F = \frac{1}{\pi}\int d^2\xi \chi_{\text{in}}(-\xi)\chi_{\text{in}}(\xi)e^{-e^{-2r}|\xi|^2}$ with an r-squeezing parameter. Both the mean photon number and the entanglement of TMSV increase with r, which can be used as a measure of the required resource. We investigate the critical value of r to achieve secure teleportation above the NCB for each case.

(i) *Fock-state inputs*—interestingly, the output fidelity above the Gaussian NCB can be achieved with the same squeezing $r = \tanh^{-1}\frac{1}{3}$ regardless of Fock states $|n\rangle$. In this case, the correlated quadratures of TMSV become $\left\langle \Delta^2\left(\frac{\hat{x}_A - \hat{x}_B}{\sqrt{2}}\right)\right\rangle = \left\langle \Delta^2\left(\frac{\hat{p}_A + \hat{p}_B}{\sqrt{2}}\right)\right\rangle = \frac{1}{2}V_0$, where V_0 is the vacuum fluctuation. This result reflects the feature of Gaussian cloners,[7] where the optimal cloning is achieved when the added noise is the half of vacuum fluctuation. To achieve the fidelity corresponding to the ultimate NCB, resource requirement r is of course higher than that for the Gaussian NCB. In Fig. 2, we see that higher squeezing r is needed for a larger n, even though the NCB itself is smaller.

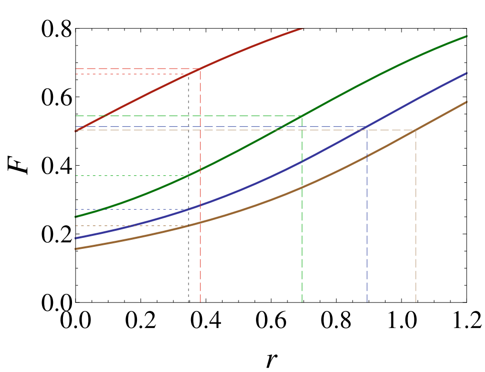

Fig. 2 Teleportation fidelity using TMSV as a resource [Supplementary Eq. (32)] and squeezing requirement to achieve NCB. Solid curves represent the fidelity for $n = 0$ (red), 1 (green), 2 (blue), and 3 (brown) from top to bottom. Horizontal dashed (dotted) lines represent the ultimate (Gaussian) NCB and the vertical dashed (dotted) lines, the required squeezing to achieve each NCB

One may wonder if our finding varies with the type of resource state used for teleportation, as we have used a Gaussian resource, TMSV, even for the teleportation of non-Gaussian states. It was shown that the teleportation fidelity can be improved by employing non-Gaussian resources under the energy constraint for coherent-state inputs.[31] In Supplementary Section 6, we perform a similar analysis for non-Gaussian input states to draw the same conclusion, i.e., teleportation of non-Gaussian input states requires more resources to overcome the NCB, even when optimal non-Gaussian entangled resources are employed.

As a remark, the output state via teleportation with TMSV is given by $\chi_{\text{out}}(\xi) = \chi_{\text{in}}(\xi)e^{-e^{-2r}|\xi|^2}$, which is equivalent to the output under Gaussian noise-added channels. Thus, our result also represents the robustness of security under Gaussian channels, which is the strongest when Gaussian input states are employed.

It is also an interesting issue how Alice and Bob can actually confirm security in teleportation, as the output fidelity above NCB should be verified with respect to unknown input states. In a typical teleportation experiment,[41] there exists a third party who provides an input state to Alice and who also checks the output fidelity afterward to assess the performance quality. On the other hand, if Alice and Bob themselves want to do the security analysis, they may execute a trial teleportation for a subset of sample states. That is, Alice herself prepares some states (selected from the set of unknown states they are supposed to teleport) and performs the teleportation protocol with Bob who can check the fidelity with the information Alice gives. This procedure is somewhat similar to the security test in quantum key distribution,[10–12] using sample data out of raw correlated data established between Alice and Bob, which enables them to analyze the properties of the channel they use and bound the information Eve possesses.

(ii) *General pure-state inputs*—We now want to discuss the relation between QNG and NCB for secure quantum communication more rigorously. A faithful measure of QNG was introduced in ref. [20] using a convex-roof extension of non-Gaussianity defined by the relative entropy $\delta(\rho) \equiv S(\rho|\tau) = S(\tau) - S(\rho)$[42,43] for a given state ρ with respect to its reference Gaussian state τ having the same first and second moments (S: von Neumann entropy). For a pure state, QNG is simply given by the entropy of the reference Gaussian state $S(\tau)$. We here consider two general non-Gaussian states, a superposition of Fock states and cat states, with the results in Fig. 3a showing NCB versus QNG. The procedures to obtain NCB for general input states are described in Supplementary Section 1. For superposition states $c_0|0\rangle + c_1|1\rangle$, $c_0|0\rangle + c_2|2\rangle$, and $c_1|1\rangle + c_2|2\rangle$, we have calculated each quantity by changing the coefficients gradually. For a comprehensive analysis, we have also generated the superposition of $|0\rangle$, $|1\rangle$, and $|2\rangle$ randomly 9×10^3 times (gray dots). For an even or odd cat state, $\mathcal{N}_\alpha^\pm(|\alpha\rangle \pm |-\alpha\rangle)$ with $\mathcal{N}_\alpha^\pm = \left(2 \pm 2e^{-2\alpha^2}\right)^{-1/2}$ normalization factor, we obtain NCB and QNG by changing α from 0 to 2.

For a fixed QNG, different input states show a very close value of NCB and we find an overall trend—NCB decreases with QNG. We also note that the NCBs for all non-Gaussian states are below that of Gaussian states, 0.6826.

We also plot the critical squeezing r_c required to achieve NCB in Fig. 3b. r_c varies with a class of input states at a fixed QNG, however, it shows a monotonic behavior within the same class. The difference might be further reduced when one employs resource states optimized for each input state. Our result shows that it becomes more demanding to achieve secure teleportation with a larger

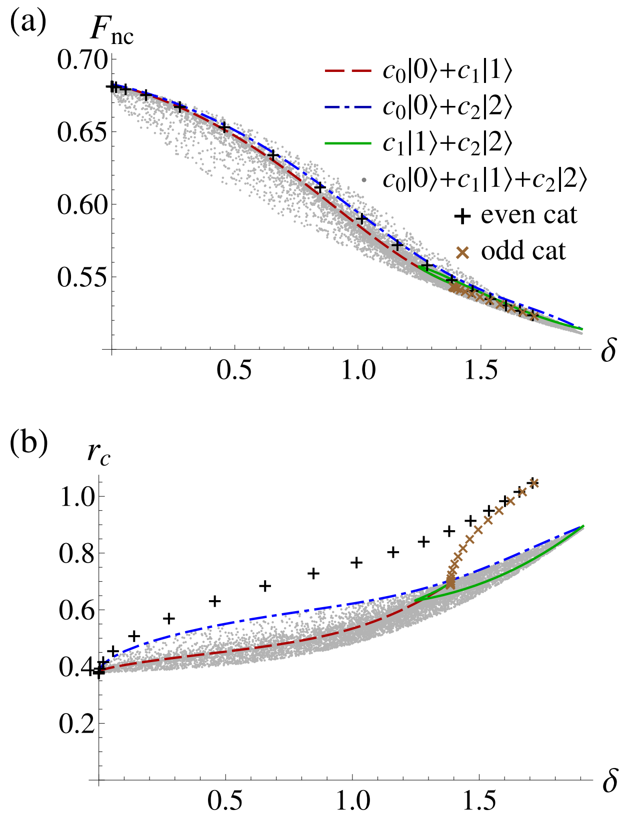

Fig. 3 **a** QNG in terms of δ (main text) versus NCB for quantum non-Gaussian states. **b** QNG versus critical squeezing to achieve secure quantum teleportation

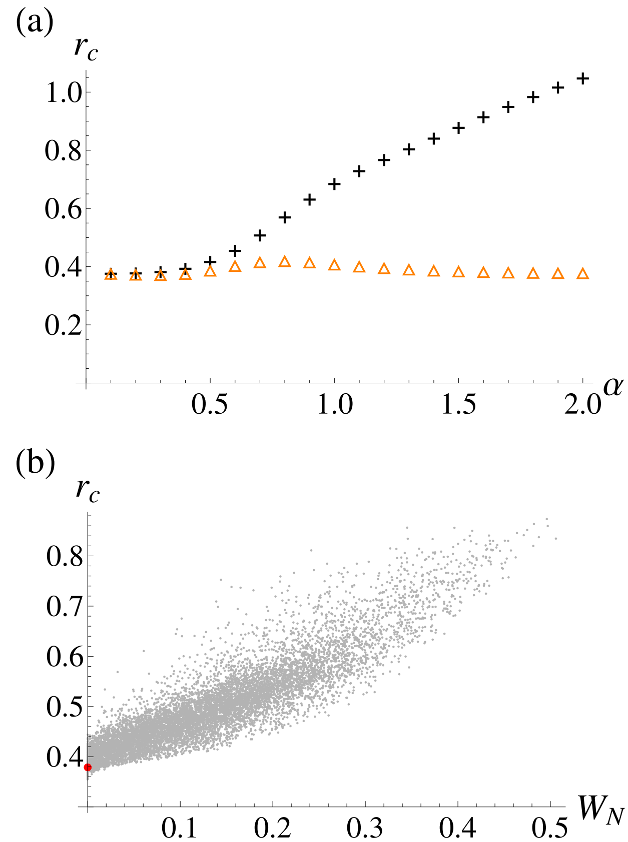

Fig. 4 **a** Critical squeezing r_c to achieve secure quantum teleportation with respect to α for even-cat states (black crosses) and for coherent-state mixtures (orange triangles). **b** Critical squeezing r_c versus logarithmic Wigner negativity W_N. Each point corresponds to a randomly chosen mixed state in the Fock space $|0\rangle$, $|1\rangle$, and $|2\rangle$ (red dot: vacuum state)

QNG of input states. We recall that the NCB is invariant under Gaussian unitaries, which means our result covers a broader class of non-Gaussian states, including squeezed non-Gaussian states. QNG δ is also invariant under Gaussian unitaries,[20] which supports our conclusion in relation to QNG and NCB more broadly.

(iii) *Mixed-state inputs*—So far, we have considered pure-state inputs as an ideal information carrier. We intend to further extend this approach to mixed-state inputs to more rigorously identify which source of QNG is a critical factor affecting secure communication. For mixed-state inputs, we adopt a trace method to quantify the overlap of two states in Eq. (1) instead of the usual fidelity measure. The overlap Tr$\{\rho\tau\}$ may be operationally interpreted as the expectation value of the output state τ over the *observable* ρ.[44] In another perspective, it represents the overlap of the Wigner functions in phase space, i.e., $\mathrm{Tr}\{\rho\tau\} = \pi\int d^2\alpha W_\rho(\alpha)W_\tau(\alpha)$. This quasi-probability overlap can also be readily measured experimentally by mixing two states ρ and τ at a 50:50 beam splitter and then observing the number parity of one output state. That is, $W_\rho(\alpha_1)W_\tau(\alpha_2) \xrightarrow{\mathrm{BS}} W'_{12}(\alpha_1,\alpha_2) = W_\rho(\frac{\alpha_1+\alpha_2}{\sqrt{2}})W_\tau(\frac{\alpha_1-\alpha_2}{\sqrt{2}})$, from which the parity of mode 2 is given by $\frac{\pi}{2}W'_2(\alpha_2=0) = \frac{\pi}{2}\int d^2\alpha_1 W'_{12}(\alpha_1,0) = \pi\int d^2\alpha W_\rho(\alpha)W_\tau(\alpha)$. This method was used, e.g., to detect entanglement by measuring local and global purities Tr$\{\rho^2\}$ after preparing two identical states.[45] This overlap measure applied to mixed states may involve an undesirable feature. For instance, given $\rho = 0.75|0\rangle\langle 0| + 0.25|1\rangle\langle 1|$, a different state $\tau = 0.9|0\rangle\langle 0| + 0.1|1\rangle\langle 1|$ may yield a higher overlap than ρ itself, i.e., $\mathrm{Tr}\{\rho\tau\} > \mathrm{Tr}\{\rho^2\}$, an issue related to mixedness of each state. Nevertheless, with more details in Supplementary Section 7, our overlap measure is relevant to capture the essence of quantum cloning and the related problems.

Importantly, when both of the NCB and the performance quality of teleportation are assessed and compared using the same measure (fidelity or state overlap), our analysis is fair: by its construction, the NCB derived in terms of trace in Eq. (1) (state overlap in phase space) indicates that no pair of two cloned copies can possess the value above the bound in terms of the same measure. Therefore, for a given mixed-input state ρ_{in}, if the condition $\mathrm{Tr}\{\rho_{\mathrm{tele}}\rho_{\mathrm{in}}\} > \mathrm{Max}\frac{1}{2}[\mathrm{Tr}\{\rho_{\mathrm{clone1}}\rho_{\mathrm{in}}\} + \mathrm{Tr}\{\rho_{\mathrm{clone2}}\rho_{\mathrm{in}}\}]$, where the latter maximum is our NCB benchmark, is verified importantly in ensemble sense averaged over unknown amplitudes α in the entire phase space, we can say that there does not exist a copy possessing better state overlap than the teleported state with the original state.

To begin with, we need to make a distinction between QNG and simple non-Gaussianity. Even a finite mixture of Gaussian states can be a non-Gaussian state, which however is not regarded as genuinely quantum non-Gaussian.[46–53] To illustrate that our conclusion only refers to QNG, not simply non-Gaussianity, we compare the even-cat state $\mathcal{N}_\alpha^+(|\alpha\rangle + |-\alpha\rangle)$ and the coherent-state mixture $\frac{1}{2}(|\alpha\rangle\langle\alpha| + |-\alpha\rangle\langle-\alpha|)$. Figure 4a shows the resource requirement to beat NCB for those two cases. The QNG for a pure-cat state increases with α, whereas the mixed-cat state has no QNG, regardless of α. The critical squeezing for even-cat states increases with QNG, while that for coherent-state mixtures hardly changes.

To understand the critical source of QNG more deeply, we investigate mixed-input states residing in the Hilbert space spanned by $|0\rangle$, $|1\rangle$, and $|2\rangle$, which cover positive and nonpositive Wigner functions. We then compare the logarithmic Wigner negativity $\mathrm{W_N} \equiv \log[\int d^2\alpha |W(\alpha)|]$[32,33] of the input state with its resource requirement $\mathrm{r_c}$ to beat NCB in Fig. 4b. We find an overall monotonic relation between $\mathrm{r_c}$ and $\mathrm{W_N}$. We also note that the critical squeezing is not substantially varied among states when $\mathrm{W_N}$ is absent (values along the y axis in Fig. 4b). We thus draw the conclusion that QNG in terms of $\mathrm{W_N}$ critically determines the resource requirement to beat NCB. This tendency is somewhat related to the point that higher Fock-state components in the resource state are needed to better teleport the non-Gaussian structure of the Wigner function. For those states with a positive Wigner function, such a non-Gaussian structure is much simpler, leading to a less-demanding resource requirement.

DISCUSSION

Our study reveals that QNG is an important characteristic to consider for secure quantum communication. Overall, the NCB benchmark decreases with QNG, while the resource requirement to achieve secure communication becomes more demanding with QNG. To draw our conclusion, we have extensively investigated QNG states, both pure and mixed, and remarkably found that the role of QNG is prominent when Wigner function is nonpositive, pointing out the $\mathrm{W_N}$ as a critical factor.

While more detailed investigation, e.g., distribution of input states with a finite variance,[54] will be necessary in the future, our finding already has a crucial implication for CV quantum communication. For instance, if our goal is to send information securely in the form of continuous amplitudes, our result shows that the resource requirement is minimal with coherent-state inputs. So far, coherent states have been mostly used, because they are readily available CV states. Our result demonstrates that they actually have a merit for secure communication in a rigorous sense. In addition, the NCB studied here can be importantly used for the security analysis of communication for a broad class of QNG states. There are other interesting and critical issues to address for CV quantum informatics, and we hope our work could provide a useful insight into future works.

METHODS

Optimality of a covariant cloner

We here prove the optimality of covariant cloners by showing that, for an arbitrary cloner T, one can always construct a covariant cloner $\tilde{T}$ resulting in the same fidelity. Let us define a cloning map $\tilde{T}$ by averaging over shifted cloners T_β of the given T, defined in Eq. (2), in the whole phase space, i.e., $\tilde{T}(\rho) = \int d^2\beta p(\beta) T_\beta(\rho)$ with a flat distribution $p(\beta)$. Obviously, $\tilde{T}$ is a covariant map satisfying invariance under shifting $\tilde{T} = \tilde{T}_\gamma$ for all γ. The fidelity of the ith clone in Eq. (1) under $\tilde{T}$, with an average over all input states $|\psi_\alpha\rangle \equiv \hat{D}(\alpha)|\psi\rangle$, is expressed as

$$\begin{aligned}
&\int d^2\alpha p(\alpha) \mathrm{Tr}\left[\tilde{T}(|\psi_\alpha\rangle\langle\psi_\alpha|)|\psi_\alpha\rangle\langle\psi_\alpha|^{(i)}\right] \\
&= \int d^2 a d^2\beta p(\alpha) p(\beta) \\
&\times \mathrm{Tr}\left[T\left(\hat{D}(\beta)|\psi_\alpha\rangle\langle\psi_\alpha|\hat{D}^\dagger(\beta)\right)\hat{D}_i(\beta)|\psi_\alpha\rangle\langle\psi_\alpha|^{(i)}\hat{D}_i^\dagger(\beta)\right] \\
&= \int d^2 a d^2\beta p(\alpha) p(\beta) \\
&\times \mathrm{Tr}\left[T\left(|\psi_{\alpha+\beta}\rangle\langle\psi_{\alpha+\beta}|\right)|\psi_{\alpha+\beta}\rangle\langle\psi_{\alpha+\beta}|^{(i)}\right] \\
&= \int d^2\alpha\prime p(\alpha\prime) \mathrm{Tr}\left[T(|\psi_{\alpha\prime}\rangle\langle\psi_{\alpha\prime}|)|\psi_{\alpha\prime}\rangle\langle\psi_{\alpha\prime}|^{(i)}\right],
\end{aligned} \tag{5}$$

which is identical with the average fidelity under a given cloner T. Thus, the optimal cloning fidelity can always be obtained by considering covariant cloners only.

Gaussian invariance

We here demonstrate the invariance of NCB under Gaussian unitary operations $\hat{U}_G$ including displacement, squeezing, and phase rotation. For any cloner T on the set of states $\mathcal{S}_{|\psi\rangle}$, we can find a cloner T_{U_G} on the set of states $\mathcal{S}_{\hat{U}_G|\psi\rangle}$ yielding the same average fidelity, which is given by $T_{U_G}(\rho) = \hat{U}_G^{\otimes M} T(\hat{U}_G^\dagger \rho \hat{U}_G)\hat{U}_G^{\dagger\otimes M}$. Operationally, T_{U_G} first performs the inverse Gaussian unitary $\hat{U}_G^\dagger$ on an input and then applies the same cloning map T followed by the Gaussian operation $\hat{U}_G$ on the cloned copies.

The same fidelity under the two cloners can be shown as follows. An arbitrary $\hat{U}_G$ makes a linear transformation between input and output operators (Bogoliubov transformation), which yields $\hat{U}_G^\dagger \hat{D}(\alpha)\hat{U}_G = \hat{D}(\tilde{\alpha})$, i.e., a displacement operator is transformed into another displacement operator. This gives a variant covariance property of the map T_{U_G} as $T_{U_G}\left(\hat{D}(\alpha)\hat{U}_G\rho\hat{U}_G^\dagger\hat{D}^\dagger(\alpha)\right) = (\hat{D}(\alpha)\hat{U}_G)^{\otimes M} T(\rho)(\hat{U}_G^\dagger\hat{D}^\dagger(\alpha))^{\otimes M}$, where we have used the covariance property of the map T. We then find

$$\begin{aligned}
&\mathrm{Tr}\left[T_{U_G}\left(\hat{D}(\alpha)\hat{U}_G\rho\hat{U}_G^\dagger\hat{D}^\dagger(\alpha)\right)\hat{D}^{(i)}(\alpha)\hat{U}_G^{(i)}\rho^{(i)}\hat{U}_G^{\dagger(i)}\hat{D}^{\dagger(i)}(\alpha)\right] \\
&\quad = \mathrm{Tr}\left[T(\rho)\rho^{(i)}\right],
\end{aligned} \tag{6}$$

using the invariance of trace under operator reordering and $\hat{U}^\dagger\hat{U} = I$. That is, finding an optimal cloner T on $\mathcal{S}_{|\psi\rangle}$ is equivalent to finding an optimal T_{U_G} on $\mathcal{S}_{\hat{U}G|\psi\rangle}$. In Fig. 1b, the cloning scheme for T_{U_G} corresponds to that for T by additionally implementing $\hat{U}_G^\dagger$ on the input state and $\hat{U}_G$ on the output clones, respectively.

DATA AVAILABILITY

The data that support the findings of this study are available from the corresponding author upon reasonable request.

ACKNOWLEDGEMENTS

This work is supported by an NPRP grant 8-751-1-157 from Qatar National Research Fund. J.P. acknowledges support by the National Research Foundation of Korea (NRF) grant funded by the Korea government (MSIT) (NRF-2019R1G1A1002337). The calculations were performed with the RAAD supercomputer at Texas A&M University at Qatar.

AUTHOR CONTRIBUTIONS

J. L. and H. N. conceived the project and made theoretical developments. All authors contributed to discussion of results and writing of the paper. H. N. supervised all procedures for the project.

ADDITIONAL INFORMATION

Supplementary information accompanies the paper on the *npj Quantum Information* website (https://doi.org/10.1038/s41534-019-0164-9).

Competing interests: The authors declare no competing interests.

Publisher's note: Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

REFERENCES

1. Bužek, V. & Hillery, M. Quantum copying: beyond the no-cloning theorem. *Phys. Rev. A* **54**, 1844–1888 (1996).
2. Braunstein, S. L., Cerf, N. J., Iblisdir, S., van Loock, P. & Massar, S. Optimal cloning of coherent states with a linear amplifier and beam splitters. *Phys. Rev. Lett.* **86**, 4938–4941 (2001).
3. Fiurášek, J. Optical implementation of continuous-variable quantum cloning machines. *Phys. Rev. Lett.* **86**, 4942–4945 (2001).
4. Scarani, V., Iblisdir, S., Gisin, N. & Acín, A. Quantum cloning. *Rev. Mod. Phys.* **77**, 1225–1256 (2005).
5. Gisin, N. & Massar, S. Optimal quantum cloning machines. *Phys. Rev. Lett.* **79**, 2153–2156 (1997).
6. Bruß, D., Cinchetti, M., D'Ariano, G. M. & Macchiavello, C. Phase-covariant quantum cloning. *Phys. Rev. A* **62**, 012302 (2000).

7. Cerf, N. J., Ipe, A. & Rottenberg, X. Cloning of continuous quantum variables. *Phys. Rev. Lett.* **85**, 1754–1757 (2000).
8. Cerf, N. J. & Iblisdir, S. Optimal N-to-M cloning of conjugate quantum variables. *Phys. Rev. A* **62**, 040301(R) (2000).
9. Cerf, N. J., Krüger, O., Navez, P., Werner, R. F. & Wolf, M. M. Non-Gaussian cloning of quantum coherent states is optimal. *Phys. Rev. Lett.* **95**, 070501 (2005).
10. Acín, A., Gisin, N. & Scarani, V. Coherent-pulse implementations of quantum cryptography protocols resistant to photon-number-splitting attacks. *Phys. Rev. A* **69**, 012309 (2004).
11. Grosshans, F. & Grangier, P. Continuous variable quantum cryptography using coherent states. *Phys. Rev. Lett.* **88**, 057902 (2002).
12. Cerf, N. J. & Grangier, P. From quantum cloning to quantum key distribution with continuous variables: a review. *J. Opt. Soc. Am. B* **24**, 324–334 (2007).
13. Braunstein, S. L. & Kimble, H. J. Teleportation of continuous quantum variables. *Phys. Rev. Lett.* **80**, 869 (1998).
14. Giovannetti, V., García-Patrón, R., Cerf, N. J. & Holevo, A. S. Ultimate classical communication rates of quantum optical channels. *Nat. Photonics* **8**, 796–800 (2014).
15. Mari, A., Giovannetti, V. & Holevo, A. S. Quantum state majorization at the output of bosonic Gaussian channels. *Nat. Commun.* **5**, 3826 (2014).
16. Weedbrook, C. et al. Gaussian quantum information. *Rev. Mod. Phys.* **84**, 621 (2012).
17. Fiurášek, J. Gaussian transformations and distillation of entangled Gaussian states. *Phys. Rev. Lett.* **89**, 137904 (2002).
18. Menicucci, N. C. et al. Universal quantum computation with continuous-variable cluster states. *Phys. Rev. Lett.* **97**, 110501 (2006).
19. Niset, J., Fiurášek, J. & Cerf, N. J. No-Go theorem for Gaussian quantum error correction. *Phys. Rev. Lett.* **102**, 120501 (2009).
20. Park, J., Lee, J., Baek, K., Ji, S.-W. & Nha, H. Faithful measure of Quantum non-Gaussianity via quantum relative entropy, Preprint at arXiv:1809.02999.
21. Ide, T., Hofmann, H. F., Furusawa, A. & Kobayashi, T. Gain tuning & fidelity in continuous-variable quantum teleportation. *Phys. Rev. A* **65**, 062303 (2002).
22. DellAnno, F., De Siena, S., Albano, L. & Illuminati, F. Continuous-variable quantum teleportation with non-Gaussian resources. *Phys. Rev. A* **76**, 022301 (2007).
23. Farias, L. A. & Stephany, J. Optimization of the transmission of observable expectation values and observable statistics in continuous-variable teleportation. *Phys. Rev. A* **82**, 062322 (2010).
24. Allegra, M., Giorda, P. & Paris, M. G. A. Role of initial entanglement and non-Gaussianity in the decoherence of photon-number entangled states evolving in a noisy channel. *Phys. Rev. Lett.* **105**, 100503 (2010).
25. Lee, J., Kim, M. S. & Nha, H. Comment on "role of initial entanglement and non-Gaussianity in the decoherence of photon-number entangled states evolving in a noisy channel". *Phys. Rev. Lett.* **107**, 238901 (2011).
26. Sabapathy, K. K., Ivan, J. S. & Simon, R. Robustness of non-Gaussian entanglement against noisy amplifier and attenuator environments. *Phys. Rev. Lett.* **107**, 130501 (2011).
27. Lee, J. & Nha, H. Entanglement distillation for continuous variables in a thermal environment: effectiveness of a non-Gaussian operation. *Phys. Rev. A* **87**, 032307 (2013).
28. Opatrný, T., Kurizki, G. & Welsch, D.-G. Improvement on teleportation of continuous variables by photon subtraction via conditional measurement. *Phys. Rev. A* **61**, 032302 (2000).
29. Lee, S.-Y., Ji, S.-W., Kim, H.-J. & Nha, H. Enhancing quantum entanglement for continuous variables by a coherent superposition of photon subtraction and addition. *Phys. Rev. A* **84**, 012302 (2011).
30. Nha, H., Lee, S.-Y., Ji, S.-W. & Kim, M. S. Efficient entanglement criteria beyond Gaussian limits using Gaussian measurements. *Phys. Rev. Lett.* **108**, 030503 (2012).
31. Lee, J., Park, J. & Nha, H. Optimal continuous-variable teleportation under energy constraint. *Phys. Rev. A* **95**, 052343 (2017).
32. Albarelli, F., Genoni, M. G., Paris, M. G. A. & Ferraro, A. Resource theory of quantum non-Gaussianity and Wigner negativity, *Phys. Rev. A* **98**, 052350 (2018).
33. Takagi, R. & Zhuang, Q. Convex resource theory of non-Gaussianity, *Phys. Rev. A* **97**, 062337 (2018).
34. Takagi, R., Regula, B., Bu, K., Liu, Z.-W. & Adesso, G. Operational advantage of quantum resources in subchannel discrimination, *Phys. Rev. Lett*. **122**, 140402 (2019).
35. He, Q., Rosales-ZáÃ¡rate, L., Adesso, G. & Reid, M. D. Secure continuous variable teleportation and Einstein–Podolsky–Rosen Steering. *Phys. Rev. Lett.* **115**, 180502 (2015).
36. Liuzzo-Scorpo, P. & Adesso, G. Optimal secure quantum teleportation of coherent states of light. *Proc. SPIE Opt. Photon.* **10358**, 103580V (2017).
37. Krüger, O. *Quantum Information Theory with Gaussian Systems* (Ph. D. thesis, Technische Universität, Braunschweig, Germany, 2006).
38. Barnett, S. M. & Radmore, P. M. *Methods in Theoretical Quantum Optics* (Oxford University Press, New York, US, 2003).
39. Lee, J., Ji, S.-W., Park, J. & Nha, H. Monogamy relation in multipartite continuous-variable quantum teleportation. *Phys. Rev. A* **94**, 062318 (2016).
40. Marian, P. & Marian, T. A. Continuous-variable teleportation in the characteristic-function description. *Phys. Rev. A* **74**, 042306 (2006).
41. Furusawa, A. & Takei, N. Quantum teleportation for continuous variables and related quantum information processing. *Phys. Rep.* **443**, 97 (2007).
42. Genoni, M. G. & Paris, M. G. A. Quantifying non-Gaussianity for quantum information. *Phys. Rev. A* **82**, 052341 (2010).
43. Marian, P. & Marian, T. A. Relative entropy is an exact measure of non-Gaussianity. *Phys. Rev. A* **88**, 012322 (2013).
44. Owari, M., Plenio, M. B., Polzik, E. S., Serafini, A. & Wolf, M. M. Squeezing the limit: quantum benchmarks for the teleportation and storage of squeezed states. *New J. Phys.* **10**, 113014 (2008).
45. Islam, R. et al. Measuring entanglement entropy in a quantum many-body system. *Nature* **528**, 77 (2015).
46. Filip, R. & Mišta, L. Jr. Detecting quantum states with a positive Wigner function beyond mixtures of Gaussian states. *Phys. Rev. Lett.* **106**, 200401 (2011).
47. Ježek, M. et al. Experimental test of the Quantum non-Gaussian character of a heralded single-photon state. *Phys. Rev. Lett.* **107**, 213602 (2011).
48. Genoni, M. G. et al. Detecting quantum non-Gaussianity via the Wigner function. *Phys. Rev. A* **87**, 062104 (2013).
49. Hughes, C., Genoni, M. G., Tufarelli, T., Paris, M. G. A. & Kim, M. S. Quantum non-Gaussianity witnesses in phase space. *Phys. Rev. A* **90**, 013810 (2014).
50. Park, J. et al. Testing nonclassicality and non-Gaussianity in phase space. *Phys. Rev. Lett.* **114**, 190402 (2015).
51. Park, J. & Nha, H. Demonstrating nonclassicality and non-Gaussianity of single-mode fields: bell-type tests using generalized phase-space distributions. *Phys. Rev. A* **92**, 062134 (2015).
52. Happ, L., Efremov, M. A., Nha, H. & Schleich, W. P. Sufficient condition for a quantum state to be genuinely quantum non-Gaussian. *New J. Phys.* **20**, 023046 (2018).
53. Straka, I. et al. Quantum non-Gaussian multiphoton light. *npj Quantum Inf.* **4**, 4 (2018).
54. Cochrane, P. T., Ralph, T. C. & Dolińska, A. Optimal cloning for finite distributions of coherent states. *Phys. Rev. A* **69**, 042313 (2004).