Detecting quantum capacities of continuous-variable quantum channels

Ya-Dong Wu [1] and Giulio Chiribella [1,2,3,*]

[1] *QICI Quantum Information and Computation Initiative, Department of Computer Science, The University of Hong Kong, Pokfulam Road, Hong Kong*

[2] *Department of Computer Science, University of Oxford, Parks Road, Oxford OX1 3QD, United Kingdom*

[3] *Perimeter Institute for Theoretical Physics, Waterloo, Ontario N2L 2Y5, Canada*

(Received 25 October 2021; accepted 21 October 2022; published 30 November 2022)

Quantum communication channels and quantum memories are the fundamental building blocks of large-scale quantum communication networks. Estimating their capacity to transmit and store quantum information is crucial in order to assess the performance of quantum communication systems and to detect useful communication paths among the nodes of future quantum networks. However, the estimation of quantum capacities is a challenging task for continuous-variable systems, such as the radiation field, for which a complete characterization via quantum tomography is practically unfeasible. Here we introduce a method for detecting the quantum capacity of continuous-variable communication channels and memories without performing a full process tomography. Our method works in the general scenario where the devices are used a finite number of times, can exhibit correlations across multiple uses, and can change dynamically under the control of a malicious adversary. The method is experimentally friendly and can be implemented using only finitely squeezed states and homodyne measurements.

DOI: 10.1103/PhysRevResearch.4.043149

I. INTRODUCTION

Continuous-variable (CV) quantum systems are a promising platform for the realization of quantum technologies, including quantum communication [1–5], quantum computation [6–8], and the quantum internet [9]. An essential building block for all these quantum technologies is the realization of devices that reliably transmit or store quantum information [10–17]. An important performance measure for these devices is the quantum capacity [18–22], that is, the number of qubits that can be transmitted or stored with each use of the device under consideration. To assess the performance of realistic devices, one needs methods to estimate the capacity from experimental data. Such methods are important not only for the certification of new quantum hardware, but also as a way to monitor future quantum communication networks, in which the quality and availability of communication links may change dynamically due to fluctuations in the environment or to the amount of network traffic. In this setting, the estimation of the quantum capacity provides a way to assess how much information can be transmitted from one node to another during a given time frame, and to identify optimal paths for routing quantum information through the network.

Unfortunately, explicit expressions for the quantum capacity are only known for particularly simple noise models, under the assumption that the noise processes at different times are independent and identically distributed (i.i.d.) [23–26]. In realistic scenarios, however, the noise can change over time and can exhibit correlations across different uses of the same device [27]. Moreover, the calculation of the quantum capacity requires a classical description of the devices under consideration. To obtain such a description, one generally needs a full quantum process tomography [28–32], which, however, becomes practically unfeasible for devices acting on high-dimensional quantum systems.

A promising approach to circumvent the above difficulties is to search for lower bounds on the quantum capacity, and for experimental setups that estimate such lower bounds without requiring a full process tomography. In this way, one can detect a guaranteed amount of quantum information that can be transmitted or stored. For finite-dimensional systems, this approach has been explored in Refs. [33–35], which provided accessible lower bounds on the asymptotic quantum capacity under the i.i.d. assumption. For qubit channels, these results were extended in Ref. [36] to a broader scenario involving a finite number of uses of the device, possibly exhibiting correlations among different uses. However, the existing results do not apply to CV quantum channels due to the infinite dimensionality of input and output systems.

In this paper, we introduce two protocols for the detection of quantum capacities in the CV domain. The two protocols provide experimentally accessible lower bounds on the number of qubits that can be transmitted or stored with a finite number of uses of a given CV device. The first protocol works in the general scenario where the behavior of the device can change dynamically from one use to the next, can be under the control of a malicious adversary, and can exhibit

*giulio@cs.hku.hk

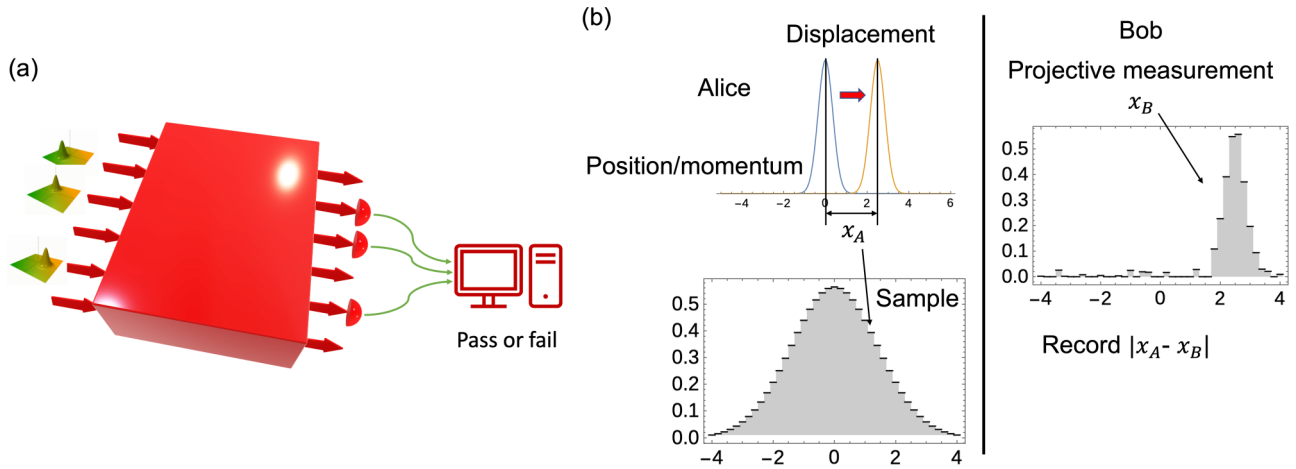

FIG. 1. (a) Capacity detection for continuous-variable quantum channels. The protocol deals with a completely unknown multimode quantum channel. A subset of the modes is randomly selected for testing the channel, while the remaining modes are kept for communication. For each testing mode, the sender prepares a single-mode Gaussian input state. At the corresponding output port, a receiver performs a Gaussian quantum measurement and sends the classical outcome to a classical computer for data analysis. If the test is passed, then the sender and receiver infer a lower bound on the quantum capacity of the channel acting on the communication modes. For each communication mode, the sender can feed one part of a two-mode squeezed state into the device, keeping the other part for a later quantum communication task. (b) Schematic diagram for Alice's and Bob's operations at each test mode in the first protocol.

correlations across different uses. The second protocol works in the less challenging setting where the different uses of the device are independent and identical. The protocol works for all phase-insensitive Gaussian channels [15] and requires only the preparation of coherent states. Both protocols can be implemented using current optical quantum technologies and provide a practically useful method to validate quantum communication channels and quantum memories.

Our protocols employ $k+n$ uses of the given quantum device and randomly select k uses for a test, as shown in Fig. 1(a). The test involves the preparation of single-mode input states (finitely squeezed states in the first protocol, coherent states in the second) and the execution of single-mode measurements on the output (homodyne measurements in the first protocol, heterodyne in the second). The result of the test is an estimated lower bound on the number of qubits that can be transmitted with the remaining n uses. Notably, the sender and receiver do not need to agree in advance on which uses of the device will be employed for testing and which ones for communication: the sender can make this decision locally and communicate it publicly after the transmission has taken place.

In both protocols, the lower bound on the capacity comes hand in hand with a lower bound on the amount of entanglement that can be established by sending halves of two-mode finitely squeezed vacuum states through the noisy channel under consideration. By using the resulting entangled state as a resource, the sender and receiver can then achieve practical quantum communication, e.g., using optimal CV teleportation [37,38]. The quantum capacity is a lower bound on the private capacity, that is, the number of secret bits that can be sent reliably per channel use [39]. For this reason, our estimated lower bound of the quantum capacity is also an estimated lower bound to the number of bits that can be sent privately through the channel. Another application of the protocol is to benchmark the performance of continuous-variable quantum error correction codes [17,40]. Detecting the lower bound on the quantum capacity of a quantum channel protected by quantum error correction codes and comparing it with the capacity of directly transmitting a physical quantum mode provides a way to assess the performance of quantum error correction codes.

II. BACKGROUND

A quantum process acting on a quantum system with Hilbert space $\mathcal{H}$ can be mathematically modeled by a quantum channel $\mathcal{E}:\mathcal{S}(\mathcal{H})\to\mathcal{S}(\mathcal{H})$, where $\mathcal{S}(\mathcal{H})$ denotes the set of density operators on the Hilbert space $\mathcal{H}$. The highest rate at which quantum information can be sent over a quantum channel $\mathcal{E}$ is quantified by its quantum capacity $Q(\mathcal{E})$ [28]. The definition of quantum capacity refers to the scenario where the channel is used an asymptotically large number of times, and the noisy processes in the various uses of the channel are identical and independently distributed. In this scenario, the quantum capacity is defined as the maximum number of qubits that can be transmitted per use of the channel with optimal encoding and decoding maps, under the condition that the error must vanish in the asymptotic limit.

Practical applications, however, often deviate from the asymptotic i.i.d. scenario. Noise can fluctuate in each run and correlations may arise between subsequent runs. Realistically, the number of uses of the quantum channel is always finite and it is reasonable to allow for a finite error tolerance, as in the task of approximate quantum error correction [12,41–44]. In these scenarios, it is convenient to adopt a one-shot version of the quantum capacity [45], denoted as $Q^{\epsilon}(\mathcal{E})$, where ϵ is the error tolerance. Explicitly, the one-shot quantum capacity is defined as

$$Q^{\epsilon}(\mathcal{E}) := \max\{\log_2 b | F(\mathcal{E},b)\geqslant 1-\epsilon\},$$

where b is the dimension of the subspace in which information is encoded, and

$$F(\mathcal{E}, b) := \max_{\overline{\mathcal{H}}\subset\mathcal{H},\dim(\overline{\mathcal{H}})=b} \max_{\mathcal{D}} \min_{|\phi\rangle\in\overline{\mathcal{H}}} \langle\phi|\mathcal{D}\circ\mathcal{E}(|\phi\rangle\langle\phi|)|\phi\rangle$$

is the maximum fidelity obtained by optimizing the choice of encoding subspace $\overline{\mathcal{H}}$ and the choice of a decoding channel $\mathcal{D}$, in the worst case over all possible input states. When the channel is of the form $\mathcal{E} = \Lambda^{\otimes n}$, corresponding to n i.i.d. uses of a channel Λ, the asymptotic quantum capacity $Q(\Lambda)$ is equal to the limit of the regularized one-shot capacity $Q^{\epsilon}(\Lambda^{\otimes n})/n$ when the number of uses goes to infinity and the error tolerance goes to zero. In summary, the one-shot quantum capacity includes as a special case the asymptotic quantum capacity.

For a generally correlated multipartite channel $\mathcal{E}_n : \mathcal{H}_{A'}^{\otimes n} \to \mathcal{H}_B^{\otimes n}$, the one-shot quantum capacity $Q^{\epsilon}(\mathcal{E}_n)$ can be bounded in terms of conditional entropies [36,45–48] as

$$Q^{\epsilon}(\mathcal{E}_n) \geqslant \max_{\sigma_A\in\mathcal{S}(\mathcal{H}_A^{\otimes n})} \sup_{\eta\in(0,\sqrt{\epsilon/2})} \times\Big[-H_{\max}^{\sqrt{\epsilon/2}-\eta}(A^n|B^n)_\rho + 4\log_2\eta - 2\Big], \quad (1)$$

where $\rho_{A^nB^n} := (\mathcal{I}_{A^n}\otimes\mathcal{E}_n)(|\Psi_\sigma\rangle\langle\Psi_\sigma|)$ is the state obtained by applying the channel $\mathcal{E}_n$ on a purification $|\Psi_\sigma\rangle_{A^nA'^n}$ of an input state σ_{A^n}, and $H_{\max}^{\epsilon}(A|B)_\rho := \min_{\rho'\in\mathcal{B}^{\epsilon}(\rho)} H_{\max}(A|B)_{\rho'}$ is the smooth max-entropy [49,50], defined as the minimum of the max-entropy $H_{\max}(A|B)_\rho$ in an ϵ-neighborhood $\mathcal{B}^{\epsilon}(\rho)$ of the state ρ, relative to the purified distance [51]. The max-entropy and its smoothed version were originally introduced in the finite-dimensional settings, and their infinite-dimensional extension was provided in [52,53].

The bound given by Eq. (1) can be relaxed by choosing a specific input σ_{A^n}. In the continuous-variable case, we choose the product state $\sigma_{A^n} = \rho_{\text{th}}^{\otimes n}$, where each of the n input systems is a bosonic mode in the thermal state with mean particle number $\bar{n}$, whose purification is a two-mode squeezed vacuum state. Hence, prediction of a lower bound on the one-shot quantum capacity is now reduced to estimating the smooth max-entropy of an unknown state resulting from the application of the channel to n two-mode squeezed states.

An indirect way to estimate $H_{\max}^{\sqrt{\epsilon/2}-\eta}(A^n|B^n)_\rho$ would be to perform a full quantum tomography of the state $\rho_{A^nB^n}$ [54]. However, full tomography is highly demanding for high-dimensional systems and convergence issues from the use of finite statistics arise in the CV case. Moreover, even if we knew ρ exactly, evaluating the smooth max-entropy by optimizing over a neighborhood of ρ is hard in general [49]. To circumvent these problems, we now propose two methods to estimate an upper bound on the smooth max-entropy without full tomography.

In the following, we will consider the situation where $\mathcal{E}$ acts on $n+k$ modes with Hilbert space $\mathcal{H}^{\otimes(n+k)}$. We will provide two protocols for experimentally estimating lower bounds to the one-shot capacity. In the first protocol, the channel $\mathcal{E}$ will be an arbitrary $(n+k)$-mode channel, corresponding to the situation where the $n+k$ uses of the device are generally correlated. In the second protocol, the channel will be assumed to be of the i.i.d. form $\mathcal{E} = \Lambda^{\otimes(n+k)}$, where Λ is a given single-mode channel, corresponding to the situation where the $n+k$ uses of the device are identical and independent.

III. PROTOCOL FOR ARBITRARY CORRELATED NOISES

This protocol provides an experimentally accessible lower bound on the number of qubits that can be transmitted with a completely unknown multimode channel. The protocol can be viewed as an infinite-dimensional generalization of the approach of Ref. [36]. A sender, Alice, prepares a quantum state of k modes, each of which is subject to a finite amount of squeezing and displacement. At the beginning, Alice randomly selects $k/2$ modes and initializes each of them in a single-mode position-squeezed vacuum state with finite amount of squeezing given by s dB. For the remaining $k/2$ modes, she initializes them in single-mode momentum-squeezed vacuum states with the same amount of squeezing. Practically, the amount of squeezing can be chosen by Alice depending on the experimental capabilities of her laboratory. Then, Alice performs a random displacement on each mode, displacing the position-squeezed states (momentum-squeezed states) in position (momentum). For each mode, the amount of displacement is chosen independently according to a zero-mean Gaussian distribution with variance $\sigma^2 = 10^{\frac{s}{10}}$. With this choice, the displaced squeezed states can also be obtained by applying a homodyne measurement on one side of a two-mode squeezed state with finite mean photon number $\bar{n} = (10^{\frac{s}{10}} - 1)/2$.

Notice that while the variance is finite, there is still a nonzero probability that the randomly chosen amount of displacement is too large to be implemented with Alice's devices. To take this experimental limitation into account, we introduce a cutoff parameter $\alpha > 0$ and allow Alice to repeat the randomization procedure until she gets a value in the interval $[-\alpha, \alpha]$. The probability that Alice does not need to repeat the randomization for a given mode is $p_{\alpha,s} := \text{erf}(\alpha\, 10^{-\frac{s}{20}}/\sqrt{2})$, where erf is the error function. Note that the probability $p_{\alpha,s}$ can be increased by increasing the amount of squeezing in the input states.

The receiver, Bob, performs homodyne detections on the k modes sent by Alice. Specifically, Bob performs position (momentum) measurements on the $k/2$ position-displaced (momentum-displaced) modes. Here we take into account that in a realistic setting, Bob's detectors will have a finite resolution and therefore the measurement outcomes will be discretized. We denote by d the width of the detector pixels in this discretization.

Finally, Alice and Bob perform a statistical test of the correlations between Alice's displacements and Bob's outcomes. For simplicity of analysis, we also apply the cutoff α to Bob's outcomes, and the discretization d also to Alice's displacements. In this way, both outcomes and displacements become discrete dimensionless random variables in the finite interval $\{0, 1, \ldots, \frac{2\alpha}{d} - 1\}$, having chosen $2\alpha/d$ to be an integer. In the following, we will denote by $\boldsymbol{x}_A$ ($\boldsymbol{x}_B$) the vector of Alice's displacements (Bob's outcomes). The test is passed if the condition

$$\frac{1}{k}\sum_{i=1}^{k} |x_{A,i} - x_{B,i}| \leqslant t \quad (2)$$

is satisfied, where t is a threshold value chosen by Alice and Bob. In the following, we will see that choosing smaller values of t results in higher values of the capacity guaranteed by the test. On the other hand, however, low values of t make the test harder to pass.

Theorem 1. If the test is passed on k randomly selected modes, then, with error probability no larger than $p_{\rm err}$, the one-shot quantum capacity of the channel corresponding to other n modes is lower bounded by

$$Q^\epsilon \geqslant \max\left\{0, \sup_{\eta\in(0,\sqrt{\epsilon/2}-\lambda)} f(\eta)\right\}, \tag{3}$$

where

$$\begin{aligned}
f(\eta) &= n\log_2\frac{2\pi}{d^2} - 2n\log_2\gamma\{t+\mu[\zeta(\eta)]\} - \Delta(\eta),\\
\lambda &= 8\sqrt{2\big(1-p^n_{\alpha,s}\big)}\left(3+\frac{5}{4p_{\rm err}}-\frac{1}{\sqrt{p_{\rm err}}}\right),\\
\gamma(x) &= (x+\sqrt{1+x^2})\left(\frac{x}{\sqrt{1+x^2}-1}\right)^x,\\
\mu(\zeta) &= \frac{2\alpha}{d}\sqrt{\frac{(k+n)(k+1)}{nk^2}\log_2\frac{1}{\zeta/4-2\sqrt{2\big(1-p^n_{\alpha,s}\big)}}},\\
\zeta(\eta) &= \left(\sqrt{\frac{\epsilon}{2}}-\eta+8\sqrt{\frac{2\big(1-p^n_{\alpha,s}\big)}{p_{\rm err}}}\right)\left(3+\frac{5}{4p_{\rm err}}\right)^{-1},\\
\Delta(\eta) &= 4\log_2\frac{1}{\eta}+2\log_2\frac{2}{\zeta(\eta)^2}+2.
\end{aligned} \tag{4}$$

Furthermore, the number of maximally entangled qubits that can be established with infidelity at most ϵ through the remaining n modes is lower bounded by

$$\sup_{\eta\in(0,\sqrt{\epsilon}-\epsilon')}\left[n\log_2\frac{2\pi}{d^2}-2n\log_2\gamma\{t+\mu[\zeta'(\eta)]\}-\Delta(\eta)+1\right], \tag{5}$$

where ζ' is defined in the same way as ζ, except that ϵ replaced by 2ϵ. This bound can be achieved by sending through each mode half of a two-mode squeezed state with average photon number $\bar n = (10^{\frac{t}{10}}-1)/2$.

The proof of the theorem is provided in the Appendix. Our main technical contribution is to reduce the estimation of the smooth max-entropy of the $2n$-partite joint state $\rho_{A^nB^n}$ to the estimation of the smooth max-entropy of a classical-quantum state $\omega_{X^nB^n}$ obtained by performing homodyne measurements on the n reference modes and by discretizing the outcomes in classical registers X^n. Our key result is the following bound:

$$H^{3\chi+5\chi'}_{\max}(A^n|B^n)_\rho \leqslant n\log_2\frac{d^2}{2\pi}+2H^{\chi'}_{\max}(X^n|B^n)_\omega-2\log_2\frac{2}{\chi^2} \tag{6}$$

for $d\ll 1$, and any $\chi,\chi'>0$. The derivation of the bound is provided in the Appendix. The strategy is to use a CV entropic uncertainty relation derived in [55,56], and adapt the result to practical homodyne measurements with a cutoff on the maximum values of the measured quadratures. $H^{\chi'}_{\max}(X^n|B^n)_\omega$ can be further bounded using t, if the correlation test in (2) is passed.

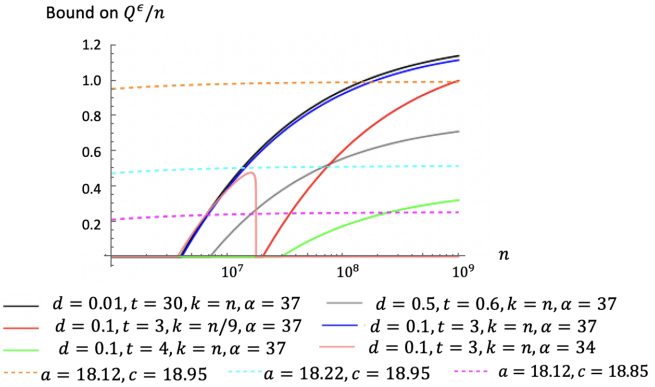

FIG. 2. Solid curves are the lower bounds on $\frac{Q^\epsilon}{n}$, with $\epsilon=0.02$, given by Eq. (3), as functions of n for different values of d, t, k, and α, and dashed curves are the lower bounds on $\frac{Q^\epsilon}{n}$, given by Eq. (10), as functions of n for different values of a and c. Other parameters are $p_{\rm err}=0.1$ and $\bar n=9.5$ for solid curves, and $k=n$ and $\bar n=9.5$ for dashed curves.

In Fig. 2, we show numerical plots of the bound (3) for different values of d, t, k/n, and α, setting $\bar n=9.5$, corresponding to 13 dB single-mode squeezing, achievable by state-of-the-art technology [57]. The figure shows that the lower bound (3) can be raised by increasing k/n, and/or by reducing d and/or by reducing t. Regarding the cutoff parameter α, it should be chosen to be large enough that the parameter λ defined in Eq. (4) does not exceed $\sqrt{\epsilon/2}$, for otherwise the bound (3) on the capacity Q^ϵ becomes trivially 0. As shown by Fig. 2, when $\alpha=34$, the protocol yields a trivial lower bound on the quantum capacity as n keeps increasing because for any given $p_{\alpha,s}$ there is an upper bound on adjustable n above which the lower bound (3) equals 0 due to the fact that $\sqrt{\epsilon/2}\leqslant\lambda$ and the set of adjustable η becomes empty.

The probability of success of our protocol depends on channel $\mathcal{E}$. For example, if $\mathcal{E}$ is a pure loss channel, obtained by sending each input mode through a beam splitter with transmissivity τ, the success probability is approximately $\frac{1}{2}+\frac{1}{2}\mathrm{erf}[\sqrt{\frac{k}{\pi-2}}(\frac{td\sqrt{\pi}}{2(\sqrt{\bar n+1}-\sqrt{\tau\bar n})}-1)]$.

IV. PROTOCOL FOR INDEPENDENT AND IDENTICAL NOISES

The previous protocol can be applied to all correlated noisy quantum channels. However, for some important i.i.d. noisy channels, the lower bound in Eq. (3) can be far from the optimal asymptotic lower bounds known in the literature [27]. To address this problem, we now introduce another protocol that works specifically for i.i.d. channels. Besides providing a better lower bound, our second protocol has the additional benefit that it does not require squeezing, but only the preparation of coherent states. Since the protocol works in the coherent state basis, the homodyne detection in the first protocol will be replaced by heterodyne detection, which is the canonical measurement in the coherent state basis.

The protocol works for phase-insensitive Gaussian channels, that is, Gaussian channels Λ satisfying the covariance condition $\Lambda\circ\mathcal{U}_\theta=\mathcal{U}_\theta\circ\Lambda$ for every $\theta\in[0,2\pi]$, where $\mathcal{U}_\theta$ is the unitary channel corresponding to the operator

$U_\theta = \exp[-i\theta a^\dagger a]$. This class of channels includes important examples in quantum optics and quantum communication, such as optimal parametric amplifiers [58,59], Gaussian additive channels, and Gaussian loss channels [60].

In the protocol, Alice prepares k coherent states, whose mean values $\boldsymbol{x} \in \mathbb{C}^k$ are random variables following a rotationally symmetric Gaussian distribution in the complex plane, with variance equal to $2\bar{n} + 3/2$. At the output, Bob applies a single-mode heterodyne measurement on each of the k modes, obtaining outcomes $\boldsymbol{y} \in \mathbb{C}^k$.

At this point, Alice and Bob can test the correlations between $\boldsymbol{x}$ and $\boldsymbol{y}$, as well as the amount of noise added by the channel. Specifically, they can estimate the variance of Bob's outcomes $\boldsymbol{y}$ and their cross correlation with Alice's inputs $\boldsymbol{x}$. The result of the estimates is two values in suitable confidence intervals, which contain the true values with probability $1 - \delta$. Here, the parameter δ can be chosen by Alice and Bob depending on how reliable they want their test to be. The results of the estimate are then used to infer a bound on the quantum capacity. The intuition is that higher cross correlations and lower added noise witness higher values of the capacity. To make this intuition rigorous, we consider the minimum value of the cross correlation and the largest value of the added noise in their respective confidence intervals. These two values, denoted by $\gamma_{\min}$ and $\sigma_{\max}$, are given by

$$\sigma_{\max} := \frac{||\boldsymbol{y}||^2}{2(k - \sqrt{2k \ln 1/\delta})} - 1/2, \tag{7}$$

$$\gamma_{\min} := \frac{||\boldsymbol{x}||^2 + ||\boldsymbol{y}||^2 + 2\langle \boldsymbol{x}, \boldsymbol{y}\rangle}{4(k + \sqrt{2k \ln 2/\delta} + \ln 2/\delta)} - \bar{n} - \frac{||\boldsymbol{y}||^2}{4(k - \sqrt{2k \ln 1/\delta})} - 3/4. \tag{8}$$

The conditions of high cross correlation and low added noise are then expressed as $\gamma_{\min} \geqslant c$ and $\sigma_{\max} \leqslant a$, respectively, where c and a are suitable thresholds that can be adjusted by Alice and Bob in the data analysis phase. The only constraint on c and a is that they need to be compatible with a quantum state, that is, that the matrix

$$\xi := \begin{pmatrix} (2\bar{n} + 1)\mathbb{1} & c\,\sigma_z \\ c\,\sigma_z & a\mathbb{1} \end{pmatrix} \tag{9}$$

satisfies the *bone fide* conditions for the covariance matrix of a quantum state [61].

Theorem 2. If both conditions $\gamma_{\min} \geqslant c$ and $\sigma_{\max} \leqslant a$ are satisfied, then, with error rate no larger than δ, the one-shot quantum capacity of the channel $\Lambda^{\otimes n}$ is lower bounded by

$$Q^\epsilon \geqslant n \max\left\{0, g(a) - g(\nu_1) - g(\nu_2) - \inf_{\eta \in (0, \sqrt{\epsilon/2})} \frac{h(\eta)}{k}\right\}, \tag{10}$$

where $g(x) := \frac{x+1}{2}\log_2 \frac{x+1}{2} - \frac{x-1}{2}\log_2 \frac{x-1}{2}$, ν_1 and ν_2 are the symplectic eigenvalues of the matrix ξ in Eq. (9), and $h(\eta) := \omega\sqrt{\log_2[2/(\sqrt{\epsilon/2} - \eta)^2]} - 4\log_2 \eta + 2$, with $\omega := 4\sqrt{k}\log_2(2\sqrt{1 + \bar{n}} + 2\sqrt{\bar{n}} + 1)$.

The proof of the theorem is given in the Appendix. In the i.i.d. scenario, the output state obtained when each mode is initialized in half of a two-mode squeezed state takes the form $\sigma_{AB}^{\otimes k}$ for a suitable two-mode state σ. In this setting, the property of quantum asymptotic equipartition (AEP) [62] implies that Q^ϵ can be bounded by $-nH(A|B)_\sigma$, plus an asymptotically vanishing term. When the noisy quantum channel is Gaussian and covariant with respect to any phase rotation operation, an upper bound on $H(A|B)_\sigma$ can be calculated from a confidence region of the covariance matrix of σ.

Similar to the second protocol for CV quantum channels, we develop a protocol, using single-qubit preparations and measurements, to estimate lower bounds on the one-shot quantum capacity of qubit channels with i.i.d. noise. Quantum AEP implies that a lower bound on one-shot quantum capacity can be obtained from estimating coherent information. To reliably estimate coherent information, we apply quantum process tomography, obtaining a confidence polytope [63] of the Choi state. By minimizing the coherent information within this polytope, we obtain a lower bound on the one-shot quantum capacity. This protocol for i.i.d. noise can be extended to a general non-i.i.d. scenario by utilizing the exponential de Finetti theorem [49,64], as shown in the Appendix.

V. COMPARISON OF LOWER BOUNDS IN THE i.i.d. ASYMPTOTIC LIMIT

In this section, we compare the lower bounds in Theorems 1 and 2 for particular i.i.d. noisy channels. When n grows linearly with k, Eq. (10) yields a lower bound on the asymptotic i.i.d. capacity $Q(\Lambda) = \lim_{\epsilon\to 0}\lim_{n\to\infty} Q^\epsilon/n$, which reads

$$Q(\Lambda) \geqslant B_{\text{iid}} := \max\{0, g(a) - g(\nu_1) - g(\nu_2)\}. \tag{11}$$

This asymptotic lower bound can be compared with the analogous lower bound obtained from Eq. (3), which reads

$$Q(\Lambda) \geqslant B := \max\left\{0, \log_2 \frac{2\pi}{d^2} - 2\log_2 \gamma(t)\right\}, \tag{12}$$

where $\gamma(t)$ is the function defined in Eq. (4). Here we compare both asymptotic lower bounds for a practically important type of channels, namely, Gaussian loss channels, corresponding to the transmission of the input through an arm of a beam splitter with transmissivity τ, with a thermal state with mean photon number $\bar{n}_{\text{th}}$ in the other arm. For our comparison, we choose the threshold values that maximize the asymptotic bounds under the condition that the probability to pass the test approaches 1 in the asymptotic limit.

We first consider the protocol in Sec. III for i.i.d. Gaussian loss channels in the asymptotic limit. For a Gaussian loss channel with transmissivity τ and mean photon number of thermal noise, $\bar{n}_{\text{th}}$, the random variable $x_A - x_B$ follows a Gaussian distribution with zero mean and standard deviation,

$$\sigma(x_A - x_B) := \sqrt{(\sinh\kappa - \sqrt{\tau}\cosh\kappa)^2 + (\cosh\kappa - \sqrt{\tau}\sinh\kappa)^2 + (1 - \tau)(2\bar{n}_{\text{th}} + 1)},$$

where κ is a squeezing parameter satisfying $\sinh^2\kappa = \bar{n}$.

Then $|x_A - x_B|$ simply follows a half-normal distribution with mean value $\sqrt{2/\pi}\sigma(x_A - x_B)$. From the central limit theorem, the sample mean $\frac{1}{k}\sum_{i=1}^{k}|x_{A,i} - x_{B,i}|$ approximately follows a Gaussian distribution with mean value $\sqrt{2/\pi}\sigma(x_A - x_B)$ and standard deviation $\sqrt{\frac{1-2/\pi}{k}}\sigma(x_A - x_B)$.

When k is asymptotically large, the averaged distance $1/k\sum_{i=1}^{k}|x_{A,i} - x_{B,i}|$ approaches a sharp distribution around its mean value. Thus, in the limit of the asymptotic limit, we can set

$$t = \frac{\sqrt{2/\pi}}{d}\sigma(x_A - x_B)$$
$$= \frac{2}{d}\sqrt{\frac{1}{\pi}}\sqrt{\bar{n}(1+\tau) + 1 + \bar{n}_{\rm th}(1-\tau) - 2\sqrt{\bar{n}(\bar{n}+1)\tau}},$$

where the second line comes from the fact that $\sinh^2\kappa = \bar{n}$. The correlation test will almost always be passed. Inserting the optimal threshold t into the expression (12) yields the lower bound of quantum capacity for the Gaussian loss channel given by the protocol in Sec. III.

Then we show the asymptotic lower bound of quantum capacity in Sec. IV for i.i.d. Gaussian loss channels. At the input side, the covariance matrix of a two-mode Gaussian state is

$$\begin{pmatrix} (2\bar{n}+1)\mathbb{1} & \sqrt{(2\bar{n}+1)^2-1}\sigma_z \\ \sqrt{(2\bar{n}+1)^2-1}\sigma_z & (2\bar{n}+1)\mathbb{1} \end{pmatrix}.$$

After applying a Gaussian loss channel, with transmissivity τ and thermal mean photon number $\bar{n}_{\rm th}$, on half of the two-mode squeezed vacuum state, the covariance matrix of this resulting two-mode Gaussian state becomes

$$\begin{pmatrix} 2(\bar{n}+1)\mathbb{1} & \sqrt{\tau}\sqrt{(2\bar{n}+1)^2-1}\sigma_z \\ \sqrt{\tau}\sqrt{(2\bar{n}+1)^2-1}\sigma_z & [\tau(2\bar{n}+1)+(1-\tau)(2\bar{n}_{\rm th}+1)]\mathbb{1} \end{pmatrix}.$$

The definitions of $\sigma_{\max}$ and $\gamma_{\min}$ indicate that when k is asymptotically large, $\sigma_{\max}$ approaches the variance $\tau(2\bar{n}+1)+(1-\tau)(2\bar{n}_{\rm th}+1)$ and $\gamma_{\min}$ approaches the covariance $\sqrt{\tau}\sqrt{(2\bar{n}+1)^2-1}$. As the statistical errors from finite sampling in estimators $\sigma_{\max}$ and $\gamma_{\min}$ asymptotically go to zero, we choose $a = \tau(2\bar{n}+1)+(1-\tau)(2\bar{n}_{\rm th}+1)$ and $c = \sqrt{\tau}\sqrt{(2\bar{n}+1)^2-1}$, which guarantees that the passing probability asymptotically approaches one. Inserting the optimal thresholds a and c into the expression of the asymptotic bound (11) for the Gaussian pure loss channel, we find the value $B_{\rm iid} = \max\{0, g[(1-\tau)(2\bar{n}+1)] - g[\tau(2\bar{n}+1)]\}$. Remarkably, this value is exactly equal to the energy-constrained quantum capacity of the channel [25,65]. In Fig. 3, we numerically compare both asymptotic lower bounds for Gaussian thermal loss channels and Gaussian pure loss channels.

VI. CONCLUSION

We have introduced two protocols for experimentally estimating lower bounds on quantum capacities of CV channels in the realistic scenario where the channel under consideration is used a finite number of times. The first protocol applies to arbitrarily correlated, dynamically changing channels, possibly under the control of a malicious attacker, while the second protocol is restricted to i.i.d. phase-insensitive Gaussian channels, and has a simpler experimental implementation. Both protocols can be implemented using current technologies on optical platforms. They provide a flexible method to validate practical quantum communication devices and quantum memories. In the longer term, they could be employed to discover useful quantum communication channels in quantum networks where the behavior of the transmission lines changes dynamically or adversarially. Similarly, they could be used to witness the presence of causal relations between quantum systems and to estimate the amount of quantum coherence between causally connected systems [66,67].

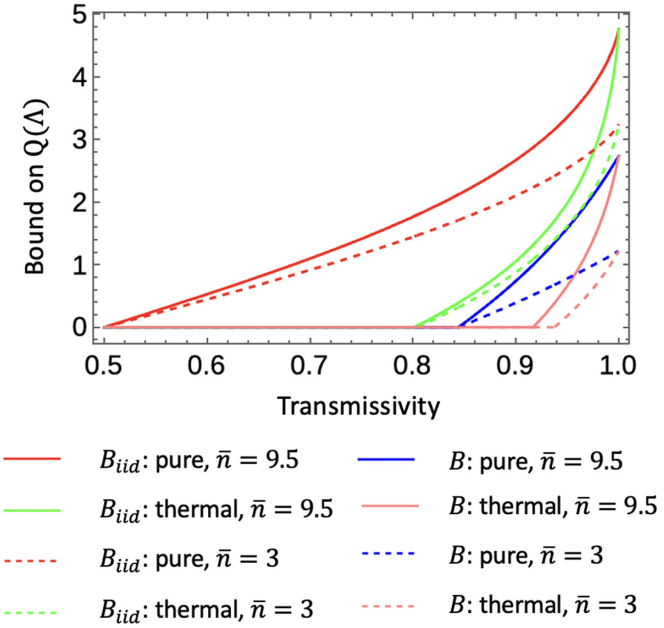

FIG. 3. Asymptotic lower bounds $B_{\rm iid}$ and B for i.i.d. Gaussian loss channels. Here we show the case of *pure* loss (corresponding to $\bar{n}_{\rm th} = 0$) and of *thermal* loss with $\bar{n}_{\rm th} = 1$. The bounds are shown as functions of transmissivity τ, for two values of input photon number $\bar{n} = 9.5$ and $\bar{n} = 3$. For the non-i.i.d. protocol, we set the discretization parameter to $d = 0.1$.

ACKNOWLEDGMENTS

We thank Chiara Macchiavello, Massimiliano F. Sacchi, Quntao Zhuang, Zheshen Zhang, Nana Liu, Kunal Sharma, Ge Bai, Yan Zhu, and Yuxiang Yang for the stimulating discussions. Y.D.W. and G.C. acknowledge funding from the Hong Kong Research Grant Council through Grants No. 17300918 and No. 17307520, through the Senior Research Fellowship Scheme SRFS2021-7S02, the Croucher Foundation, and the John Templeton Foundation through Grant No. 61466, The Quantum Information Structure of Spacetime. Research at the Perimeter Institute is supported by the Government of Canada through the Department of Innovation, Science and Economic Development Canada and by the Province of Ontario through the Ministry of Research, Innovation and Science. The opinions expressed in this publication are those of the authors and do not necessarily reflect the views of the John Templeton Foundation.

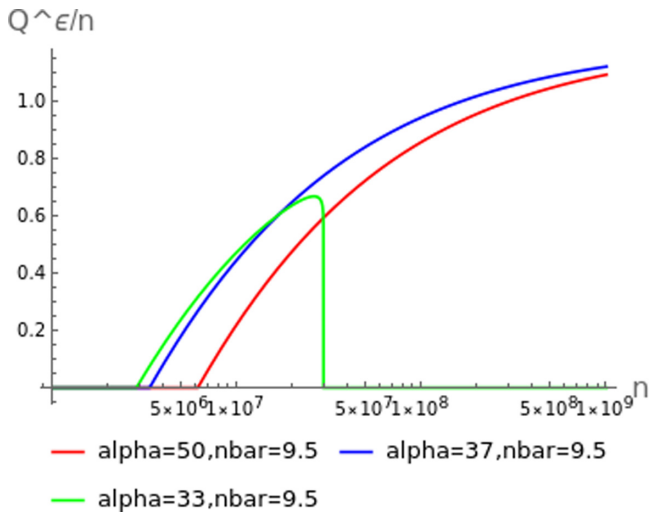

FIG. 4. Lower bound on $\frac{Q^\epsilon}{n}$, with $\epsilon = 0.02$, given by Theorem 1, as a function of n for different cutoff values $\alpha = 50$, $\alpha = 37$, and $\alpha = 33$, respectively. Other parameters are $d = 0.1$, $t = 3$, $k = n$, $p_{\text{err}} = 0.5$, and $\bar{n} = 9.5$.

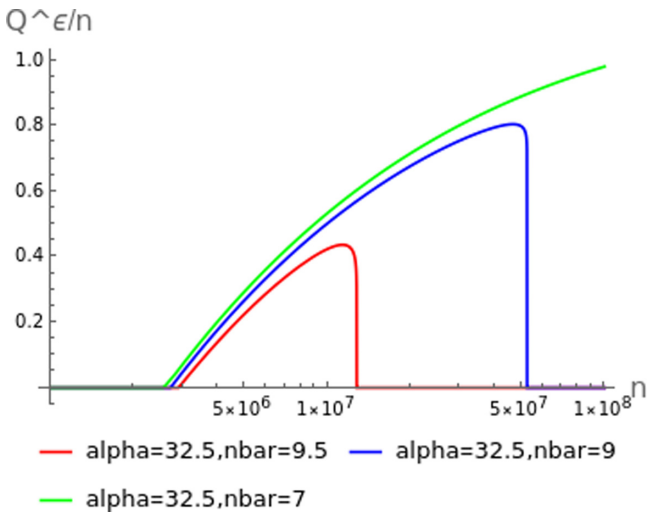

FIG. 5. Lower bound on $\frac{Q^\epsilon}{n}$, with $\epsilon = 0.02$, given by Theorem 1, as a function of n for different expected photon number $\bar{n} = 9.5$, $\bar{n} = 9$, and $\bar{n} = 7$, respectively. Other parameters are $d = 0.1$, $t = 3$, $k = n$, $p_{\text{err}} = 0.5$, and $\alpha = 32.5$.

APPENDIX

1. More numerical analysis

In this section, we present more numerical simulation results to analyze the dependence of the inferred lower bound of quantum capacity on those adjustable parameters in the protocols. We first study how the cutoff threshold α and the expected photon number $\bar{n}$ in the first protocol affect the lower bound in Theorem 1. As shown by Fig. 4, when we fix $\bar{n}$ while reducing the value of α, the protocol can fail to provide a nontrivial lower bound on the quantum capacity as n keeps increasing. This is because for any given $p_{\alpha,s}$, there is an upper bound on adjustable n, above which the lower bound in Theorem 1 does not work due to the fact that $\sqrt{\epsilon/2} - \lambda \leqslant 0$ and the set of adjustable η becomes empty. On the other hand, if we increase α, the lower bound is reduced in the region of positive bound. As shown by Fig. 5, when we fix α and increase $\bar{n}$, the protocol can fail to provide a nonzero bound as n increases. This is because of the same reason as we discussed above.

Then we investigate how different combinations of d and t affect the inferred lower bound while keeping dt fixed. By reducing d and fixing dt, we increase the number of bins within a fixed region of real numbers. As shown by Fig. 6, reducing d from 0.5 to 0.1, while keeping $dt = 0.3$, raises the lower bound significantly. However, when we further reduce d from 0.1 to 0.01, there is only a tiny increase in the lower bound. This phenomenon is reasonable because when we reduce d from 0.5 to 0.1, the estimation of correlation between input and output becomes more accurate, which statistically yields more information about the quantum channel under study. Given a fixed passing region given by dt, this additional information leads to an increase of the inferred lower bound on Q^ϵ. However, when we further reduce d, d no longer dominate the change of the lower bound. Similar phenomena are shown by Fig. 7 in the asymptotic limit.

Last, we study how the lower bound of Q^ϵ depends on the tolerable infidelity ϵ. As Fig. 8 suggests, increasing ϵ raises the lower bound, but this change is not quite significant.

2. Discussions on parameter choices

The adjustable parameters are either related to the limitation of the experimental setups available to Alice and Bob (e.g., the highest resolution of the detectors, the maximal amount of squeezing in the input states) or related to the required degree of confidence in their estimation procedure. Here we discuss the meanings of each parameter and how to choose those parameters.

In the first protocol, d, α and $\bar{n}$ depend on the practical quantum devices. Specifically, d represents the resolution

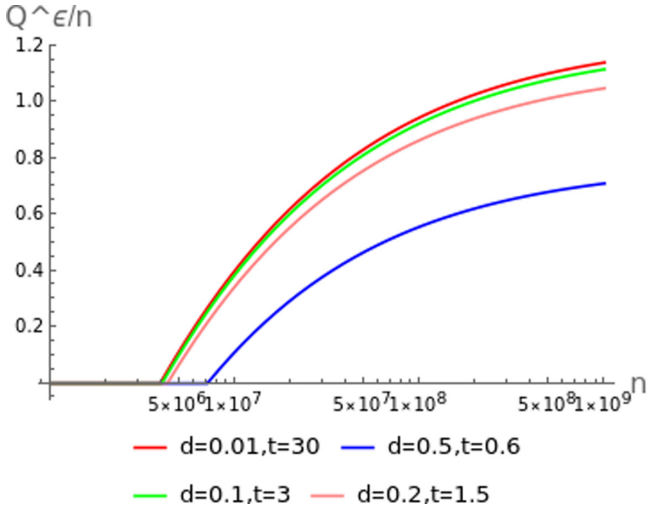

FIG. 6. Lower bound on $\frac{Q^\epsilon}{n}$, with $\epsilon = 0.02$, given by Theorem 1, as a function of n for different combinations of discretization widths d, while $dt = 0.3$ is kept. Other parameters are $k = n$, $p_{\text{err}} = 0.1$, $\alpha = 37$, and $\bar{n} = 9.5$.

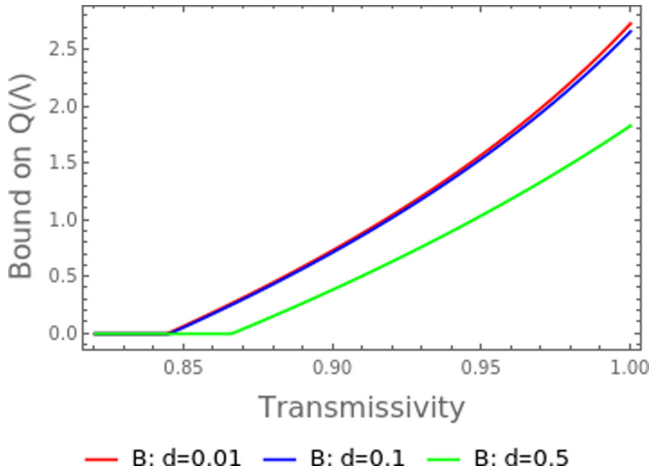

FIG. 7. Asymptotic lower bound B for Gaussian pure loss channel as a function of transmissivity τ for different values of discretization width d and threshold $t = \frac{1}{d}\sqrt{\frac{4}{\pi}}\sqrt{\bar{n}(1+\tau)+1-2\sqrt{\bar{n}(\bar{n}+1)\tau}}$.

of homodyne detections associated to the width of detector pixels. $(-\alpha, \alpha)$ is the maximal range of displacement that can be performed by Alice's quantum device. α must be large enough to make $\sqrt{\epsilon/2} - \lambda > 0$, otherwise the bound in Theorem 1 fails to give a nontrivial value. $\bar{n}$ denotes the expected photon number per input mode, which is limited by achievable squeezing. Any $\bar{n} \leqslant 13.6$ is achievable by current technology [57], corresponding to squeezing below 15 dB. $p_{\alpha,s} = \mathrm{erf}[\alpha/\sqrt{2(2\bar{n}+1)}]$ is determined by α and $\bar{n}$, denoting the probability that a sample from zero-mean Gaussian distribution with variance $2\bar{n}+1$ falls within $(-\alpha, \alpha)$, where erf is the error function.

Here, k is the number of modes Alice and Bob can sacrifice for performing the test and n is the number of modes which are demanded by Alice and Bob for later quantum communication. Both k and n are practically upper limited, and k, $n \leqslant 10^9$ are considered to be within the practical regime in CV quantum key distribution [68], whose setting is similar to ours. The ratio k/n, and other parameters t, p_{err}, and ϵ, can be chosen by the users of the channel, Alice and Bob. t is the threshold value in the test. Reducing t can increase the inferred lower bound on quantum capacity, but simultaneously reduce the probability to pass the test. $0 < p_{\mathrm{err}} < 1$ is the tolerable error probability in the inference. ϵ is introduced in the definition of one-shot quantum capacity and denotes the tolerable infidelity of quantum communication. In Fig. 2, we choose $\epsilon = 0.02$, which is acceptable considering the fact that the experimental fidelity of qubit teleportation over long distance is just above 0.9 [69].

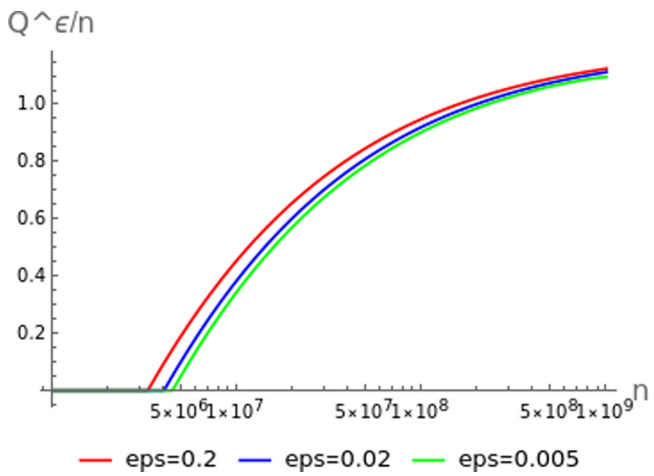

FIG. 8. Lower bounds on $\frac{Q^\epsilon}{n}$, given by Theorem 1, as functions of n for different maximal tolerable infidelities $\epsilon = 0.2$, $\epsilon = 0.02$, and $\epsilon = 0.005$. Other parameters are $d = 0.1$, $t = 3$, $k = n$, $p_{\mathrm{err}} = 0.1$, $\alpha = 37$, and $\bar{n} = 9.5$.

In the second protocol, k, n, and ϵ have the same meanings as those we have discussed in the first protocol. The threshold parameter a represents the maximal tolerable additional noise in $\boldsymbol{y}$ and the other threshold parameter c represents the minimal tolerable cross correlation between $\boldsymbol{x}$ and $\boldsymbol{y}$. a and c should be chosen to make matrix ξ (9) a viable covariance matrix, which is to satisfy the bona fide conditions [61]

$$\xi + i\Omega \geqslant 0 \text{ where } \Omega := \begin{pmatrix} 0 & 1 & 0 & 0 \\ -1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & -1 & 0 \end{pmatrix}.$$

Suitable a and c can be adjusted by Alice and Bob in the data analysis phase after obtaining measurement outcomes. Basically, Alice and Bob can pick the values that give them the best bound on the capacity of the channel under consideration. The optimal values of a and b generally depend on the channel itself.

3. Proof of Theorem 1

The one-shot quantum capacity is defined as

$$Q^\epsilon(\mathcal{E}) := \max\{\log_2 b | F(\mathcal{E}, b) \geqslant 1-\epsilon\}, \tag{A1}$$

where b is the dimension of the subspace in which information is encoded, and

$$F(\mathcal{E}, b) := \max_{\bar{\mathcal{H}} \subset \mathcal{H}, \dim(\bar{\mathcal{H}})=b} \max_{\mathcal{D}} \min_{|\phi\rangle \in \bar{\mathcal{H}}} \langle\phi|\mathcal{D}\circ\mathcal{E}(|\phi\rangle\langle\phi|)|\phi\rangle \tag{A2}$$

is the maximum fidelity obtained by optimizing the choice of encoding subspace $\bar{\mathcal{H}}$ and the choice of a decoding channel $\mathcal{D}$, in the worst case over all possible input states. When the channel is of the form $\mathcal{E} = \Lambda^{\otimes n}$, corresponding to n i.i.d. uses of a channel Λ, the asymptotic quantum capacity $Q(\Lambda)$ is equal to the limit of the regularized one-shot capacity $Q^\epsilon(\Lambda^{\otimes n})/n$ when the number of uses goes to infinity and the error tolerance goes to zero. In summary, the one-shot quantum capacity includes as a special case the asymptotic quantum capacity.

We then present all the related concepts of min- and max-quantum entropies [49,50], which are rigorously generalized into infinite dimensions [52]. The min-entropy of ρ_{AB} given σ_B is

$$H_{\min}(\rho_{AB}|\sigma_B) := -\log_2 \min\{\lambda | \lambda \mathbb{1} \otimes \sigma_B \geqslant \rho_{AB}\}, \tag{A3}$$

and the min-entropy of ρ_{AB} given system B is

$$H_{\min}(A|B)_\rho := \sup_{\sigma_B} H_{\min}(\rho_{AB}|\sigma_B). \tag{A4}$$

Given a purification ρ_{ABC} of ρ_{AB}, the max-entropy of ρ_{AB} given system B is

$$H_{\max}(A|B)_{\rho_{AB}} := -H_{\min}(A|C)_{\rho_{AC}}. \tag{A5}$$

Similarly, one can define the smooth min-entropy

$$H^\epsilon_{\min}(\rho_{AB}|\sigma_B) := \max_{\rho'_{AB}\in B^\epsilon(\rho_{AB})} H_{\min}(\rho'_{AB}|\sigma_B), \tag{A6}$$

where $B^\epsilon(\rho) := \{\rho' \geqslant 0 | \mathrm{tr}\rho' \leqslant 1, \mathcal{P}(\rho,\rho') \leqslant \epsilon\}$ is an ϵ-ball around ρ with $\mathcal{P}(\rho,\rho') := \sqrt{1-||\sqrt{\rho}\sqrt{\rho'}||_1^2}$ called purified distance, and

$$H^\epsilon_{\min}(A|B)_\rho := \max_{\rho'\in B^\epsilon(\rho)} H_{\min}(A|B)_{\rho'}. \tag{A7}$$

Given a purification ρ_{ABC} of ρ_{AB}, the smooth max-entropy of ρ_{AB} is

$$H^\epsilon_{\max}(A|B)_{\rho_{AB}} := -H^\epsilon_{\min}(A|C)_{\rho_{AC}}. \tag{A8}$$

Suppose we apply a channel $\mathcal{E}: \mathcal{H}_{A'}^{\otimes n} \to \mathcal{H}_B^{\otimes n}$ to an input state $\sigma_{A'^n}$, where n denotes the number of subsystems. The purification of $\sigma_{A'^n}$ is $|\Psi_\sigma\rangle_{A'^nA^n}$. Then the joint state at reference A^n and output B^n is $\rho_{A^nB^n} := \mathbb{1}\otimes\mathcal{E}(|\Psi_\sigma\rangle\langle\Psi_\sigma|)$.

Lemma 1. (lower bound on one-shot quantum capacity as optimization of max-entropy [36,45–48]). Given a quantum channel $\mathcal{E}$ from $\mathcal{H}_{A'}$ to $\mathcal{H}_B$, the one-shot quantum capacity of $\mathcal{E}$ is bounded by

$$Q^\epsilon(\mathcal{E}) \geqslant \sup_{\eta\in(0,\sqrt{\epsilon/2})} \max_{\sigma\in\mathcal{S}(\mathcal{H}_{A'}^{\otimes n})} \left[-H^{\sqrt{\epsilon/2}-\eta}_{\max}(A^n|B^n)_\rho + 4\log_2\eta\right] - 2. \tag{A9}$$

We can drop the maximization over all possible input states by choosing a specific input $\sigma_{A'}$. For an infinite-dimensional quantum system, we can further restrict the energy of each input mode to obtain a lower bound on the energy-constrained one-shot quantum capacity. In the following, we choose the input at each mode as a thermal state with mean photon number $\bar{n}$, i.e., $\rho_{\mathrm{th}}(\bar{n}) = \sum_{n=0}^\infty \frac{\bar{n}^n}{(\bar{n}+1)^{n+1}}|n\rangle\langle n|$, whose purification is a two-mode squeezed vacuum state $|\Psi_{\rho_{\mathrm{th}}(\bar{n})}\rangle := e^{\kappa/2(\hat{a}\hat{b}-\hat{a}^\dagger\hat{b}^\dagger)}|0\rangle|0\rangle$ with $\cosh(2\kappa) = 2\bar{n}+1$.

Below we present a lower bound, closely related to the above bound, on the maximal number of maximally entangled pairs, which can be established by applying entanglement distillation on $\rho_{A^nB^n}$.

Lemma 2. (lower bound on distillable entanglement [47,48,70]). For any state $\rho_{A^nB^n}$, a lower bound of its one-shot distillable entanglement is

$$\sup_{\eta\in(0,\sqrt{\epsilon})} \left[-H^{\sqrt{\epsilon}-\eta}_{\max}(A^n|B^n)_\rho + 4\log_2\eta\right] - 1. \tag{A10}$$

This Lemma shows that by estimating an upper bound of $H_{\max}(A^n|B^n)_\rho$, we can not only detect a lower bound on one-shot quantum capacity, but also obtain a lower bound on the amount of entanglement, which can be established by sending just halves of two-mode squeezed vacuum states.

Hence, prediction of a lower bound on one-shot quantum capacity is now reduced to estimating smooth max-entropy of an unknown state resulting from the application of the channel to n two-mode squeezed states. An indirect way to estimate $H^{\sqrt{\epsilon/2}-\eta}_{\max}(A^n|B^n)_\rho$ would be to perform a full quantum tomography of the state $\rho_{A^nB^n}$ [54]. However, full tomography is highly demanding for high-dimensional systems and convergence issues from the use of finite statistics arise in the CV case. Moreover, even if we knew ρ exactly, evaluating the smooth max-entropy by optimizing over a neighborhood of ρ is hard in general [49]. To circumvent these problems, we now propose a method to estimate an upper bound on the smooth max-entropy without full tomography.

Here we present the protocol for arbitrary unknown correlated noise in the entanglement-based formalism, instead of the one in the formalism of preparation and measurement shown in the main text. Given a $(k+n)$-mode input channel and $(k+n)$-mode output channel, Alice prepares $k+n$ copies of two-mode entangled states $|\psi\rangle$ and feeds one party of each to the channel. Through negotiation, Alice and Bob agree on k random pairs of modes. On these k pairs, Alice and Bob both apply homodyne detections at each of them in the same random bases $\boldsymbol{z}^k \in \{0,1\}^{\otimes k}$ (0 denotes position and 1 denotes momentum). Suppose the discretization distance when discretizing the outcomes is $d>0$ and the outcome cutoff is $(-\alpha+d, \alpha-d)$. Each measurement outcome is projected into one of the $2\alpha/d$ regions, $\{(-\infty,-\alpha+d], (-\alpha+d,-\alpha+2d], \ldots, (\alpha-d,\infty)\}$. Accordingly, each outcome is mapped to an integer in the set $\chi := \{0,1,\ldots,\frac{2\alpha}{d}-1\}$, where d and α are chosen to make $2\alpha/d \in \mathbb{N}^+$. $\boldsymbol{x}^{pe}_A \in \chi^{\otimes k}$ and $\boldsymbol{x}^{pe}_B \in \chi^{\otimes k}$ denote Alice's and Bob's discretized measurement outcomes at k modes, respectively. Alice and Bob pass the test at the k subsystems if the average distance

$$1/k\sum_{i=1}^k \left|x^{pe}_{A,i} - x^{pe}_{B,i}\right| \leqslant t. \tag{A11}$$

Otherwise, they abort the protocol.

Denote the state at the other n pairs of modes by $\rho_{A^nB^n}$, whose purification is denoted by $\rho_{A^nB^nE}$. Alice applies homodyne detections at the remaining n modes on random chosen bases $z_n \in \{0,1\}^{\otimes n}$ and $\boldsymbol{x}_A \in \chi^{\otimes n}$ denotes Alice's measurement outcomes at these n modes. Denote $\omega_{A^nX^nB^n}$ as the joint postmeasurement state at A^n, X^n, B^n, conditioned on the previous test being passed, where X^n denotes classical registers storing Alice's discretized measurement outcomes $\boldsymbol{x}_A$, and $\omega_{A^nX^nB^nE}$ as the purified state.

Now we present the proof of Theorem 1 by following the idea in [36] and using mainly the technical tools proven in Ref. [55]. Before we show the proof, we first present the following three useful lemmas.

Lemma 3. (chain rule of smooth max-entropy) Smooth max-entropy satisfies the following chain rule, for any $\epsilon>0$, $\epsilon', \epsilon'' \geqslant 0$, and any $\sigma \in \mathcal{S}(\mathcal{H}_A\otimes\mathcal{H}_B\otimes\mathcal{H}_C)$, where $\mathcal{H}_A$, $\mathcal{H}_B$, and $\mathcal{H}_C$ can be infinite-dimensional Hilbert spaces:

$$H^{\epsilon+\epsilon'+2\epsilon''}_{\max}(AB|C)_\sigma \leqslant H^{\epsilon'}_{\max}(A|BC)_\sigma + H^{\epsilon''}_{\max}(B|C)_\sigma + \log_2\frac{2}{\epsilon^2}. \tag{A12}$$

This lemma was first proven by Ref. [71] for finite-dimensional state σ. This result can be extended to an infinite-dimensional quantum system by combining the fact

that max-entropy on infinite-dimensional Hilbert spaces can be asymptotically approached by max-entropy on finite-dimensional Hilbert spaces [52] and the chain rule of smooth max-entropy in Ref. [71].

Lemma 4. (CV entropic uncertainty relation [55]) The post-measurement state ω, conditioned on the test at n modes being passed, satisfies the following entropic uncertainty relation:

$$H_{\min}^{\epsilon+2\epsilon'}(X^n|E)_\omega \geqslant -n\log_2 c(d) - H_{\max}^{\epsilon}(X^n|B^n)_\omega, \quad \text{(A13)}$$

where $c(d) = \frac{d^2}{2\pi} S_0^{(1)}(1, \frac{d^2}{4})^2$, $\epsilon' = \sqrt{\frac{2(1-(1-p_\alpha)^n)}{p_{\text{pass}}}}$, p_{pass} denotes the probability that the test is passed, and p_α is an upper bound of the probability that each x_A exceeds the region $(-\alpha, \alpha)$.

Here, $S_0^{(1)}(\cdot,\cdot)$ denotes the radial prolate spheroidal wave function of the first kind [56,72] and, when $d \ll 1$, we have $c(d) \approx d^2/(2\pi)$. If Alice's state preparation can be trusted, then the states in her possession are just copies of the thermal states. For a thermal state $\rho(\bar{n})$, the variances of both quadratures are $2\bar{n}+1$. We can obtain the value of p_α from the error function. For example, when $\alpha = 37$ and $\bar{n} = 9.5$, $p_\alpha = 1 - \text{erf}(6.17) \approx 1.11\times10^{-16}$.

Estimating $H_{\max}^{\sqrt{\epsilon/2}-\eta}(A^n|B^n)_\rho$ can be reduced to the estimation of $H_{\max}^{\zeta'}(X^n|B^n)$. At this point, the intuition is that if both Alice and Bob apply homodyne detections in the same basis at certain pairs of modes and their outcomes are highly correlated, then $H_{\max}^{\zeta'}(X^n|B^n)_\omega$ must be small because B^n contains much information about A^n. This intuition was made rigorous in Ref. [55], as given in the following lemma, which showed that if a suitable correlation test is passed, then $H_{\max}^{\zeta'}(X^n|B^n)_\omega$ can be bounded using the data of homodyne outcomes.

Lemma 5. (upper bound on max-entropy [55]) Conditioned on that $1/k\sum_{i=1}^k |X_{A,i}^{pe} - X_{B,i}^{pe}| \leqslant t$, the smooth max-entropy of Alice's measurement outcomes $\boldsymbol{x}_A$, given Bob's system B^n and measurement basis choices $\boldsymbol{z}_n$, are bounded by

$$H_{\max}^{\frac{\epsilon}{4p_{\text{pass}}} - \frac{2f(p_\alpha,n)}{\sqrt{p_{\text{pass}}}}}(X^n|B^n) \leqslant n\log_2 \gamma[t + \mu_0(\epsilon)], \quad \text{(A14)}$$

where $\gamma(t) := (t+\sqrt{1+t^2})(\frac{t}{\sqrt{1+t^2}-1})^t$, $\mu_0(\epsilon) = \frac{2\alpha}{d}\sqrt{\frac{(k+n)(k+1)}{nk^2}\log_2\frac{1}{\epsilon/4 - 2f(p_\alpha,n)}}$, and $f(p_\alpha,n) := \sqrt{2[1-(1-p_\alpha)^n]}$.

Now we are ready to present the result of the prediction of lower bounds on quantum capacities over n-mode quantum channels with general correlated noises.

Theorem 3. If the measurement outcomes at the k test modes pass the test, i.e., $1/k\sum_{i=1}^k |x_{A,i}^{pe} - x_{B,i}^{pe}| \leqslant t$, then either the probability to pass this test is lower than p_{pass} or the one-shot quantum capacity of the channel corresponding to the remaining n modes is bounded by

$$Q^\epsilon \geqslant \max\left(0, \sup_{\eta\in\left[0,\sqrt{\epsilon/2}-8f(p_\alpha,n)\left(3+\frac{5}{4p_{\text{pass}}}-\frac{1}{\sqrt{p_{\text{pass}}}}\right)\right]}\left\{n\log_2\frac{2\pi}{d^2} - 2n\log_2\gamma[t+\mu_0(\zeta)] - 4\log_2\frac{1}{\eta} - 2\log_2\frac{2}{\zeta^2} - 2\right\}\right), \quad \text{(A15)}$$

where $\zeta = (\sqrt{\epsilon/2} - \eta + \frac{8f(p_\alpha,n)}{\sqrt{p_{\text{pass}}}})/(3+\frac{5}{4p_{\text{pass}}})$, and the number of maximally entangled pairs, which can be established by sending halves of two-mode squeezed vacuum states, can be lower bounded by

$$\sup_{\eta\in\left[0,\sqrt{\epsilon}-8f(p_\alpha,n)\left(3+\frac{5}{4p_{\text{pass}}}-\frac{1}{\sqrt{p_{\text{pass}}}}\right)\right]}\left\{n\log_2\frac{2\pi}{d^2} - 2n\log_2\gamma[t+\mu_0(\zeta')] - 4\log_2\frac{1}{\eta} - 2\log_2\frac{2}{\zeta'^2} - 1\right\}, \quad \text{(A16)}$$

where $\zeta' = (\sqrt{\epsilon} - \eta + \frac{8f(p_\alpha,n)}{\sqrt{p_{\text{pass}}}})/(3+\frac{5}{4p_{\text{pass}}})$.

Proof. The proof closely follows the one in Ref. [36]. Denote $\{Q_x\}_{x\in\chi}$ as the positive operator-valued measure (POVM) measurement corresponding to homodyne detection in the position basis and the measurement outcome is discretized in the set of alphabets χ. Similarly, denote $\{P_x\}_{x\in\chi}$ as the POVM measurement corresponding to homodyne detection in the momentum basis and the measurement outcome is discretized in χ. For any random $\boldsymbol{z} \in \{0,1\}^{\otimes n}$, we define an isometry $V_{\boldsymbol{z}} : \mathcal{H}_{A^n} \to H_{A^n} \otimes H_{X^n} \otimes H_{X'^n}$ as an extension of the projective measurements on system A^n, where X'^n are classical registers copying the information in X^n,

$$V_{\boldsymbol{z}} : |\psi\rangle_{A^n} \to \sum_{\boldsymbol{x}\in\chi^{\otimes n}} \Lambda_{\boldsymbol{z},\boldsymbol{x}} |\psi\rangle_{A^n} |\boldsymbol{x}\rangle_{X^n} |\boldsymbol{x}\rangle_{X'^n}, \quad \text{(A17)}$$

where $\Lambda_{\boldsymbol{z},\boldsymbol{x}} = \otimes_{i=1}^n \Lambda_{z_i,x_i}$ and $\Lambda_{z,x} = \begin{cases} Q_x & \text{if } z=0 \\ P_x & \text{if } z=1. \end{cases}$

As $\omega_{A^nX^nX'^nB^nE}$ can be obtained by applying an isometry on $\rho_{A^nB^nE}$, we have

$$H_{\max}^{3\zeta+\zeta'+4\zeta''}(A^n|B^n)_\rho = H_{\max}^{3\zeta+\zeta'+4\zeta''}(A^nX^nX'^n|B^n)_\omega. \quad \text{(A18)}$$

Using Lemma 3, we get

$$H_{\max}^{\zeta+\zeta'+2(\zeta+2\zeta'')}(A^nX^nX'^n|B^n)_\omega \leqslant H_{\max}^{\zeta'}(X^n|A^nX'^nB^n)_\omega + H_{\max}^{\zeta+2\zeta''}(A^nX'^n|B^n)_\omega + \log_2\frac{2}{\zeta^2}. \quad \text{(A19)}$$

From the duality of min- and max-entropy (A8), we have

$$H_{\max}^{\zeta'}(X^n|A^nX'^nB^n)_\omega = -H_{\min}^{\zeta'}(X^n|E)_\omega. \quad \text{(A20)}$$

Using Lemma 3 again, we have

$$H_{\max}^{\zeta+2\zeta''}(A^nX'^n|B^n)_\omega \leqslant H_{\max}(A^n|X'^nB^n)_\omega + H_{\max}^{\zeta''}(X'^n|B^n)_\omega + \log_2\frac{2}{\zeta^2}. \tag{A21}$$

As X and X' stores the same information,

$$H_{\max}^{\zeta''}(X'^n|B^n)_\omega = H_{\max}^{\zeta''}(X^n|B^n)_\omega. \tag{A22}$$

Combining all of the above, we have, for any $\zeta > 0$ and $\zeta', \zeta'' \geqslant 0$,

$$H_{\max}^{3\zeta+\zeta'+4\zeta''}(A^n|B^n)_\rho \leqslant H_{\max}(A^n|X'^nB^n)_\omega + H_{\max}^{\zeta''}(X^n|B^n)_\omega - H_{\min}^{\zeta'}(X^n|E)_\omega + 2\log_2\frac{2}{\zeta^2}. \tag{A23}$$

We use the entropic uncertainty relation in Lemma 4 to obtain

$$-H_{\max}^{3\zeta+\zeta'+4\zeta''}(A^n|B^n)_\rho \geqslant -n\log_2 c(d) - H_{\max}^{\zeta''}(X^n|B^n)_\omega - H_{\max}^{\zeta'-2\frac{f(p_\alpha,n)}{\sqrt{p_{\text{pass}}}}}(X^n|B^n)_\omega - 2\log_2\frac{2}{\zeta^2}. \tag{A24}$$

By setting $\zeta' = \frac{\zeta}{4p_{\text{pass}}}$ and $\zeta'' = \zeta' - 2\frac{f(p_\alpha,n)}{\sqrt{p_{\text{pass}}}}$, using Lemma 5, we have

$$H_{\max}^{\zeta''}(X^n|B^n)_\omega = H_{\max}^{\zeta'-2\frac{f(p_\alpha,n)}{\sqrt{p_{\text{pass}}}}}(X^n|B^n)_\omega \leqslant n\log_2\gamma[t+\mu_0(\zeta)]. \tag{A25}$$

By setting the relation

$$3\zeta + \zeta' + 4\zeta'' = \sqrt{\epsilon/2} - \eta, \tag{A26}$$

we obtain

$$\zeta = \left(\sqrt{\epsilon/2} - \eta + \frac{8f(p_\alpha,n)}{\sqrt{p_{\text{pass}}}}\right)\Bigg/\left(3 + \frac{5}{4p_{\text{pass}}}\right). \tag{A27}$$

When $\frac{\zeta}{4} - 2f(p_\alpha,n) > 0$, i.e.,

$$0 < \eta < \sqrt{\epsilon/2} - 8f(p_\alpha,n)\left(3 + \frac{5}{4p_{\text{pass}}} - \frac{1}{\sqrt{p_{\text{pass}}}}\right), \tag{A28}$$

combining Lemma 1 and Eq. (A24), we get

$$Q^\epsilon \gtrsim \sup_{\eta\in\left[0,\sqrt{\epsilon/2}-8f(p_\alpha,n)\left(3+\frac{5}{4p_{\text{pass}}}-\frac{1}{\sqrt{p_{\text{pass}}}}\right)\right]} \left\{n\log_2\frac{2\pi}{d^2} - 2n\log_2\gamma[t+\mu_0(\zeta)] - 2\log_2\frac{2}{\zeta^2} + 4\log_2\eta - 2\right\}. \tag{A29}$$

Using Lemma 2, we obtain a lower bound on the number of maximally entangled pairs which can be established by sending halves of two-mode squeezed vacuum states. ■

4. Proof of Theorem 2

We first present the protocol for independent and identical noises in the entanglement-based formalism instead of in the preparation-and-measurement formalism as shown in the main text. Alice prepares n copies of two-mode squeezed vacuum states $|\Psi_{\rho_{\text{th}(\bar{n})}}\rangle$, feeds one party of each to a channel, and keeps the other party as reference modes. For each copy, Alice and Bob choose a random phase shift operation $U \in \mathbb{U}(1)$, and apply operation $U^\dagger \otimes U$ at the reference mode and output mode. After this symmetrization procedure, Alice and Bob both apply heterodyne measurements at the n pairs of modes. Their measurement outcomes are denoted by $\boldsymbol{x} \in \mathbb{C}^n$ and $\boldsymbol{y} \in \mathbb{C}^n$, respectively. Later, we show that if the i.i.d. noisy channel commutes with any phase rotation operation, then this symmetrization procedure is unnecessary to perform.

Based on the measurement outcomes $\boldsymbol{x}$ and $\boldsymbol{y}$ as well as error probability δ, Alice and Bob calculate

$$\sigma_{\max} := \frac{||\boldsymbol{y}||^2}{2(k-\sqrt{2k\ln 1/\delta})} - 1/2,$$

$$\gamma_{\min} := \frac{||\boldsymbol{x}||^2 + ||\boldsymbol{y}||^2 + 2\boldsymbol{x}^\top\boldsymbol{y}}{4(k+\sqrt{2k\ln 2/\delta}+\ln 2/\delta)} - \bar{n} - \frac{||\boldsymbol{y}||^2}{4(k-\sqrt{2k\ln 1/\delta})} - 3/4.$$

If the parameters satisfy $\sigma_{\max} \leqslant a$ and $\gamma_{\min} \geqslant c$, then Alice and Bob pass the test. Otherwise, they abort the protocol.

Before we prove Theorem 2, we present a useful lemma.

Lemma 6. (asymptotic equipartition property for CV states [52]) Let $\sigma \in \mathcal{H}_A \otimes \mathcal{H}_B$ such that the von Neumann entropy $H(A)_\sigma$ is finite. For any $\epsilon > 0$ and $n > \frac{8}{5}\log_2 \frac{2}{\epsilon^2}$, we have

$$H_{\max}^{\epsilon}(A^n|B^n)_{\sigma^{\otimes n}} \leqslant nH(A|B)_\sigma + 4\sqrt{n}\log_2 \nu\sqrt{\log_2 \frac{2}{\epsilon^2}},$$

where $H(A|B)_\sigma = H(AB)_\sigma - H(B)_\sigma$ and $\nu := \sqrt{2^{-H_{\min}(A|B)_\sigma}} + \sqrt{2^{H_{\max}(A|B)_\sigma}} + 1$.

For i.i.d. noisy channels, we suppose $\mathcal{E} = \Lambda^{\otimes n}$ and $\sigma = \Lambda \otimes \mathbb{1}(|\Psi_{\rho_{\text{th}(\bar{n})}}\rangle\langle\Psi_{\rho_{\text{th}(\bar{n})}}|)$. Using the fact that $H_{\min}(A|B)_\sigma \geqslant -2\log_2 \text{tr}(\sqrt{\sigma_A})$, $H_{\max}(A|B)_\sigma \leqslant 2\log_2 \text{tr}(\sqrt{\sigma_A})$, and $\sigma_A = \rho_{\text{th}}(\bar{n})$, we have $\nu \leqslant 2\sqrt{2^{2\log_2(\text{tr}\sqrt{\sigma_A})}} + 1 = 2\sqrt{2^{2\log_2(\sqrt{1+\bar{n}}+\sqrt{\bar{n}})}} + 1 = 2\sqrt{1+\bar{n}} + 2\sqrt{\bar{n}} + 1$. Using Lemma 6, we have

$$H_{\max}^{\epsilon}(A^n|B^n)_{\sigma^{\otimes n}} \leqslant nH(A|B)_\sigma + 4\sqrt{n}\log_2(2\sqrt{1+\bar{n}} + 2\sqrt{\bar{n}} + 1)\sqrt{\log_2 \frac{2}{\epsilon^2}}.$$

After the symmetrization procedure $\sigma \to \tilde{\sigma} := \int_{U\in\mathbb{U}(1)} dU U^\dagger \otimes U\sigma U \otimes U^\dagger$, the covariance matrix of $\tilde{\sigma}$ is

$$\begin{pmatrix} 2\bar{n}+1 & 0 & \Sigma_c & \Sigma_d \\ 0 & 2\bar{n}+1 & \Sigma_d & -\Sigma_c \\ \Sigma_c & \Sigma_d & \Sigma_b & 0 \\ \Sigma_d & -\Sigma_c & 0 & \Sigma_b \end{pmatrix}.$$

We find that the symplectic eigenvalues of the above matrix only depend on $\bar{n}$, Σ_b, and $\Sigma_c^2 + \Sigma_d^2$. Fixing $\bar{n}$, Σ_b, and Σ_c, $H(A|B)_{\tilde{\sigma}}$ is maximized by minimizing $\Sigma_c^2 + \Sigma_d^2$, which is achieved when $\Sigma_d = 0$. It is easy to find that $H(A|B)_{\tilde{\sigma}}$ keeps increasing when we raise Σ_b and reduce Σ_c because the noise within system B is increased, while the correlation between system A and system B decreases. Thus, an upper bound of Σ_b, together with a lower bound of Σ_c, yields an upper bound on $H(A|B)_{\tilde{\sigma}}$.

Suppose the channel $\Lambda(\cdot)$ commutes with any phase rotation operation $U \cdot U^\dagger$; then, $\tilde{\sigma} = \mathbb{1} \otimes \Lambda(\int_{U\in\mathbb{U}(1)} dU U^\dagger \otimes U\,|\Psi_{\rho_{\text{th}(\bar{n})}}\rangle\langle\Psi_{\rho_{\text{th}(\bar{n})}}|\,U \otimes U^\dagger)$. Note that any phase rotation $U^\dagger \otimes U$ keeps a two-mode squeezed vacuum state $|\Psi_{\rho_{\text{th}(\bar{n})}}\rangle$ invariant. Thus, $\tilde{\sigma} = \sigma$, which implies that the symmetrization procedure does not need to be performed.

Now we present how to obtain confidence intervals of variance Σ_b and covariance Σ_c from the finite measurement outcomes $\boldsymbol{x}$ and $\boldsymbol{y}$. To achieve this goal, we consider the random variables of Alice's and Bob's measurement outcomes as $\beta_A \in \mathbb{C}$ and $\beta_B \in \mathbb{C}$, respectively, which both follow Gaussian distributions. Then the covariance matrix of β_A together with β_B is

$$\begin{pmatrix} 2\bar{n}+3/2 & 0 & \Sigma_c & \Sigma_d \\ 0 & 2\bar{n}+3/2 & \Sigma_d & -\Sigma_c \\ \Sigma_c & \Sigma_d & \Sigma_b+1/2 & 0 \\ \Sigma_d & -\Sigma_c & 0 & \Sigma_b+1/2 \end{pmatrix}.$$

This is because of the fact that the heterodyne measurement combines the signal mode with a vacuum state by a balanced beam splitter and homodyne position and momentum of two resulting modes.

From the definition of chi-squared distribution, it is easy to see that $\frac{||\boldsymbol{y}||^2}{\Sigma_b+1/2}$ is a random variable following the chi-squared distribution with $2k$ degrees. Then, let us first introduce a concentration inequality for the chi-squared distribution.

Lemma 7. (concentration inequality of chi-squared distribution [73]) Suppose variable X follows the chi-squared distribution with n degrees. We have the following inequalities of probabilities, for any $x > 0$:

$$\Pr(X - n \geqslant 2\sqrt{nx} + 2x) \leqslant e^{-x},$$
$$\Pr(n - X \geqslant 2\sqrt{nx}) \leqslant e^{-x}.$$

By setting $\delta = e^{-x}$, the above inequalities are transformed to

$$\Pr(X \geqslant n + 2\sqrt{n\ln 1/\delta} + 2\ln 1/\delta) \leqslant \delta, \tag{A30}$$

$$\Pr(X \leqslant n - 2\sqrt{n\ln 1/\delta}) \leqslant \delta. \tag{A31}$$

Using (A31), we have

$$\Pr\left(\frac{||\boldsymbol{y}||^2}{\Sigma_b + 1/2} \leqslant 2k - 2\sqrt{2k\ln 1/\delta}\right) \leqslant \delta,$$

which is equivalent to

$$\Pr\left(\Sigma_b \geqslant \frac{||\boldsymbol{y}||^2}{2(k - \sqrt{2k\ln 1/\delta})} - 1/2\right) \leqslant \delta.$$

This is to say, with error probability of, at most, δ, the true variance satisfies

$$\Sigma_b \leqslant \frac{||\boldsymbol{y}||^2}{2(k-\sqrt{2k\ln 1/\delta})} - 1/2. \tag{A32}$$

On the other hand, we consider the combination $\bar{\beta}_A + \beta_B$. It can be seen that both the real and imaginary parts of $\bar{\beta}_A + \beta_B$ follow a Gaussian distribution with variance $2\bar{n} + 3/2 + \Sigma_b + 1/2 + 2\Sigma_c = 2\bar{n} + \Sigma_b + 2\Sigma_c + 2$. Hence, $\frac{||\bar{\boldsymbol{x}}+\boldsymbol{y}||^2}{2\bar{n}+\Sigma_b+2\Sigma_c+2}$ follows the chi-squared distribution with $2k$ degrees. Using (A30), we obtain

$$\Pr\left(\frac{||\bar{\boldsymbol{x}}+\boldsymbol{y}||^2}{2\bar{n}+\Sigma_b+2\Sigma_c+2} \geqslant 2k + 2\sqrt{2k\ln 1/\delta} + 2\ln 1/\delta\right) \leqslant \delta.$$

Using the relation $||\bar{\boldsymbol{x}}+\boldsymbol{y}||^2 = ||\boldsymbol{x}||^2 + ||\boldsymbol{y}||^2 + 2\boldsymbol{x}^\top\boldsymbol{y}$, the above inequality can be transformed to

$$\Pr\left(\Sigma_c \leqslant \frac{||\boldsymbol{x}||^2 + ||\boldsymbol{y}||^2 + 2\boldsymbol{x}^\top\boldsymbol{y}}{4(k+\sqrt{2k\ln 1/\delta}+\ln 1/\delta)} - \bar{n} - \Sigma_b/2 - 1\right) \leqslant \delta.$$

That is, with error probability of, at most, δ, the covariance is lower bounded by

$$\Sigma_c \geqslant \frac{||\boldsymbol{x}||^2 + ||\boldsymbol{y}||^2 + 2\boldsymbol{x}^\top\boldsymbol{y}}{4(k+\sqrt{2k\ln 1/\delta}+\ln 1/\delta)} - \bar{n} - \Sigma_b/2 - 1.$$

Combining the fact in (A32) and the union bound, we obtain both the upper bound of variance Σ_b the lower bound of covariance Σ_c with error probability of, at most, δ,

$$\begin{aligned}
\Sigma_b &\leqslant \frac{||\boldsymbol{y}||^2}{2(k-\sqrt{2k\ln 2/\delta})} - 1/2,\\
\Sigma_c &\geqslant \frac{||\boldsymbol{x}||^2 + ||\boldsymbol{y}||^2 + 2\boldsymbol{x}^\top\boldsymbol{y}}{4(k+\sqrt{2k\ln 2/\delta}+\ln 2/\delta)} - \bar{n} - \frac{||\boldsymbol{y}||^2}{4(k-\sqrt{2k\ln 2/\delta})} - 3/4.
\end{aligned}$$

Theorem 4. If the conditions $\sigma_{\max} \leqslant a$ and $\gamma_{\min} \geqslant c$ are satisfied, then with error probability of less than δ, the one-shot quantum capacity corresponding to each mode of the k channels uses is bounded by

$$\frac{Q^\epsilon}{k} \geqslant \max\left\{0, g(a) - g(\nu_1) - g(\nu_2) + \frac{1}{k}\sup_{\eta\in(0,\sqrt{\epsilon/2})}\left[-4\sqrt{k}\log_2(2\sqrt{1+\bar{n}}+2\sqrt{\bar{n}}+1)\sqrt{\log_2\frac{2}{(\sqrt{\epsilon/2}-\eta)^2}} + 4\log_2\eta - 2\right]\right\}.$$

Proof. Using Lemma 1, we have

$$Q^\epsilon \geqslant \sup_{\eta\in(0,\sqrt{\epsilon/2})}\left[-H_{\max}^{\sqrt{\epsilon/2}-\eta}(A^k|B^k)_{\sigma^{\otimes k}} + 4\log_2\eta - 2\right]. \tag{A33}$$

Using Lemma 6, we have

$$Q^\epsilon \geqslant \sup_{\eta\in(0,\sqrt{\epsilon/2})}\left[-kH(A|B)_\sigma - 4\sqrt{k}\log_2(2\sqrt{1+\bar{n}}+2\sqrt{\bar{n}}+1)\sqrt{\log_2\frac{2}{(\sqrt{\epsilon/2}-\eta)^2}} + 4\log_2\eta - 2\right].$$

If the conditions $\sigma_{\max} \leqslant a$ and $\gamma_{\min} \geqslant c$, then with probability of, at least, $1-\delta$, $H(A|B)_\sigma$ is upper bounded by the conditional entropy of a Gaussian state with covariance matrix $\left(\begin{smallmatrix}(2\bar{n}+1)\mathbb{1} & c\sigma_z\\ c\sigma_z & a\mathbb{1}\end{smallmatrix}\right)$. That is,

$$H(A|B)_\sigma \leqslant g(\nu_1) + g(\nu_2) - g(a), \tag{A34}$$

where $g(x) := \frac{x+1}{2}\log_2\frac{x+1}{2} - \frac{x-1}{2}\log_2\frac{x-1}{2}$, and ν_1 and ν_2 are the symplectic eigenvalues of covariance matrix $\left(\begin{smallmatrix}(2\bar{n}+1)\mathbb{1} & c\sigma_z\\ c\sigma_z & a\mathbb{1}\end{smallmatrix}\right)$. ■

5. Estimating lower bounds on quantum capacity of qubit channels

The protocol to estimate lower bounds on quantum capacities for i.i.d. qubit channels is first to prepare a maximally entangled state $|\Psi_+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$. Then Alice applies a quantum channel at one party of $|\Psi_+\rangle\langle\Psi_+|$ and keeps the other party as a reference qubit. At the output side, Bob randomly chooses to measure Pauli observable $\sigma_{B,i}\otimes\sigma_{A,j}$, where $i, j = 0, 1, 2, 3$ and $\sigma_{0,1,2,3} = \mathbb{1}, \sigma_x, \sigma_y, \sigma_z$. After n rounds of measurements, following the theorem below, Alice and Bob can calculate a lower bound on the quantum capacity.

Lemma 8. (fully quantum AEP [62]) For any σ_{AB},

$$H_{\max}^\epsilon(A^n|B^n)_{\sigma^{\otimes n}} \leqslant nH(A|B)_\sigma + 4\sqrt{n}\log_2\mu\sqrt{\log_2\frac{2}{\epsilon^2}} \tag{A35}$$

where $\mu \leqslant \sqrt{2^{H_{\min}(A|B)_\sigma}} + \sqrt{2^{-H_{max}(A|B)_\sigma}} + 1 \leqslant 2^{d_A/2+2}$.

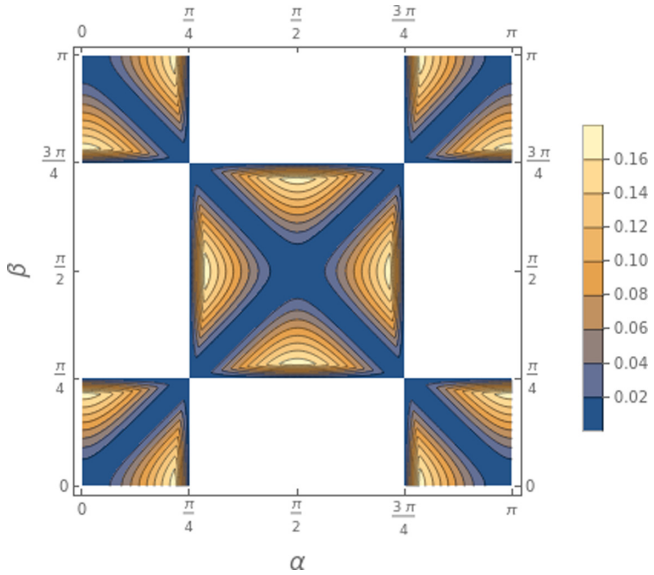

FIG. 9. The difference between the coherent information (A40) and the detectable lower bound of quantum capacity in Ref. [36] for quantum channels in Eq. (A39) within the region $\cos(2\alpha)/\cos(2\beta) > 0$.

Lemma 9. (confidence polytope of quantum tomography [63]) For the kth ($0 \leqslant k \leqslant d^4 - 1$) Pauli observable, denote the corresponding POVM by $\mathcal{M}_k := \{E_k^{(l)}\}_{l=0}^{d-1}$ on $\mathcal{H}_A \otimes \mathcal{H}_B$, where l denotes the measurement outcome. After the measurements $\otimes_{k=0}^{d^2-1} \mathcal{M}_k^{\otimes n_k}$, for each k, the number of rounds of measurements getting outcome l is n_k^l. The confidence interval of the state $\sigma \in \mathcal{S}(\mathcal{H}_A \otimes \mathcal{H}_B)$, with confidence level $1 - \delta$, where $\delta = \sum_{k=0}^{d^2-1} \sum_{l=0}^{d-1} \delta_k^l$, is $\Gamma = \cap_{0\leqslant k\leqslant d^2-1, 0\leqslant l\leqslant d-1} \Gamma_{kl}$, where

$$\Gamma_{kl} := \left\{ \rho \in \mathcal{S}(\mathcal{H}_A \otimes \mathcal{H}_B) : \frac{n_k}{n} \mathrm{tr}\left(\rho E_k^{(l)}\right) \leqslant \frac{n_k^l}{n} + \epsilon\left(n_k^l, \delta_k^l\right) \right\}. \tag{A36}$$

Here, $\epsilon(n_k^l, \delta_k^l)$ is the positive root of the equation

$$D\left(\frac{n_k^l}{n} \middle|\middle| \frac{n_k^l}{n} + \epsilon\right) = -\frac{1}{n} \log_2 \delta_k^l, \tag{A37}$$

where $D(x||y) = x \log_2 \frac{x}{y} + (1 - x) \log_2 \frac{1-x}{1-y}$.

Theorem 5. Suppose that by applying the quantum state tomography described above, we get a confidence region Γ. Then, we have

$$\frac{Q^\epsilon(\mathcal{E})}{n} \geqslant - \max_{\sigma_{AB} \in \Gamma} H(A|B)_\sigma + \sup_{\eta \in (0, \sqrt{\epsilon/2})} \frac{4}{n} \left[-(d_A/2 + 2)\sqrt{n} \sqrt{\log_2 \frac{2}{(\sqrt{\epsilon/2} - \eta)^2}} + \log_2 \eta \right] - \frac{2}{n}. \tag{A38}$$

One of our motivations to propose this protocol to estimate lower bounds on one-shot quantum capacities for i.i.d. noisy channels is that the previous lower bound obtained by the protocol in Ref. [36] can be far from the optimal lower bound for some practically important i.i.d. noisy channels. Particularly consider the following parametrized quantum channel:

$$\mathcal{E}(\rho) = \sum_{i=1}^{2} A_i \rho A_i^\dagger, \tag{A39}$$

where $A_1 = \cos\alpha\, |0\rangle\langle 0| + \cos\beta\, |1\rangle\langle 1|$ and $A_2 = \sin\beta\, |0\rangle\langle 1| + \sin\alpha\, |1\rangle\langle 0|$. When $\alpha = \beta$, the quantum channel is a dephasing channel, and when $\beta = 0$, the channel becomes an amplitude damping channel. Its quantum capacity is nonzero only when $\cos(2\alpha)/\cos(2\beta) > 0$.

The detectable lower bound in our protocol asymptotically approaches coherent information,

$$-H(A|B)_\sigma = h[(\cos^2\alpha + \sin^2\beta)/2] + h[(\sin^2\alpha + \sin^2\beta)/2]. \tag{A40}$$

Figure 9 shows the difference between the lower bound (A40) and the one obtained using the method in Ref. [36]. As it shows, for i.i.d. dephasing channels, our protocol, by estimating coherent information, provides the same lower bound on the quantum capacity in the asymptotic limit. However, for i.i.d. amplitude damping channels, our protocol outperforms the one in Ref. [36] asymptotically, providing a tighter lower bound on the quantum capacities.

In the following, we extend the above result to a general non-i.i.d. scenario by using the quantum de Finetti theorem. We suppose $\rho_{A^{n+k}B^{n+k}}$ is an arbitrary state jointly at A and B with $n+k$ pairs of qubits/qudits. As $\rho_{A^{n+k}B^{n+k}}$ is permutation invariant, there always exists a purification $\rho_{A^{n+k}B^{n+k}E^{n+k}} \in \mathcal{S}\{\mathrm{Sym}[(\mathcal{H}_A \otimes \mathcal{H}_B \otimes \mathcal{H}_E)]^{\otimes n+k}\}$, where $E \cong A \otimes B$.

Lemma 10. (exponential quantum de Finetti theorem [49]) The trace distance between $\rho_{A^nB^nE^n} := \mathrm{tr}_{A^kB^kE^k}\rho_{A^{n+k}B^{n+k}E^{n+k}}$ and a mixture of almost i.i.d. pure states $\tilde{\rho}^\theta \in \mathcal{S}[\mathrm{Sym}(\mathcal{H}_{ABE}^{\otimes n}, |\theta\rangle^{\otimes n-r})]$ can be bounded by

$$\left\| \rho_{ABE}^n - \int d\nu(\theta)\tilde{\rho}^\theta \right\|_1 \leqslant 2k^{d/2} e^{-\frac{k(r+1)}{2(n+k)}}, \tag{A41}$$

where ν is a probability measure on $\mathcal{H}_{ABE}$ and $d = \dim(\mathcal{H}_{ABE})$.

For qubits, $d = 2^4 = 16$ and the right-hand side of Eq. (A41) becomes $2k^8 e^{-\frac{k(r+1)}{2(n+k)}}$.

The quantum asymptotic equipartition property [62], shown in Lemma 8, can be generalized to almost i.i.d. states as follows:

Lemma 11. (fully quantum AEP for almost i.i.d. states) Given $\tilde{\rho}^\theta := |\Psi_\theta\rangle\langle\Psi_\theta|$ has an almost i.i.d. structure, i.e., $|\Psi_\theta\rangle_{ABE} \in \mathcal{S}ym(\mathcal{H}_{ABE}^{\otimes n}, |\theta\rangle^{\otimes n-r})$, from the asymptotic equipartition property, we have

$$-H_{\max}^\epsilon(A^n|B^n)_{\tilde{\rho}^\theta} \geqslant -(n-r)H(A|B)_{|\theta\rangle\langle\theta|} - 4\sqrt{n-r}\log_2\mu\sqrt{\log_2\frac{2}{\tilde{\epsilon}^2}} - nh(r/n) - r\log_2 d_A, \tag{A42}$$

where $\tilde{\epsilon} \geqslant \frac{\epsilon^2}{6\cdot 2^{n\cdot h(r/n)}}$, and $\mu \leqslant \sqrt{2^{-H_{\min}(A|E)_{|\theta\rangle\langle\theta|}}} + \sqrt{2^{H_{max}(A|E)_{|\theta\rangle\langle\theta|}}} + 1 \leqslant 2^{d_A/2+1} + 1$, where $d_A = \dim(\mathcal{H}_A)$. The above bound can be further simplified to

$$\begin{aligned} -H_{\max}^\epsilon(A^n|B^n)_{\tilde{\rho}^\theta} \geqslant{}& (n-r)[H(B)_{|\theta\rangle\langle\theta|} - H(AB)_{|\theta\rangle\langle\theta|}] \\ & - 4\sqrt{n-r}\log_2\mu\sqrt{2nh(r/n) - 4\log_2\epsilon + 2\log_2 6 + 1} - nh(r/n) - r\log_2 d_A. \end{aligned} \tag{A43}$$

The proof of this Lemma closely follows the idea in the proof of Theorem 4.4.1. in Ref. [49].

Proof. There exists a family of mutually orthonormal states $\{|\psi_s\rangle\}_{s\in S}$ on $\mathrm{Sym}(\mathcal{H}_{ABE}^{\otimes n}, |\theta\rangle^{\otimes n-r})$ with $|S| \leqslant 2^{nh(r/n)}$ such that $|\Psi_\theta\rangle = \sum_{s\in S}\gamma_s|\psi_s\rangle$ with $\sum_{s\in S}|\gamma_s|^2 = 1$. Then, the reduced state $\rho_{A^nE^n} = \mathrm{tr}_{B^n}(|\Psi_\theta\rangle\langle\Psi_\theta|)$ and $\tilde{\rho}^s_{A^nE^n} = \mathrm{tr}_{B^n}(|\psi_s\rangle\langle\psi_s|)$. Another state is defined, $\tilde{\rho}_{A^nE^nS} := \sum_{s\in S}|\gamma_s|^2\tilde{\rho}^s_{AE}\otimes|s\rangle\langle s|$. Then, it has been shown that

$$H_{\min}^\epsilon(A^n|E^n)_\rho \geqslant H_{\min}^{\tilde{\epsilon}}(A^n|E^nS)_{\tilde{\rho}} - H_{max}(\tilde{\rho}_S) \geqslant \min_{s\in S} H_{\min}^{\tilde{\epsilon}}(A^n|E^n)_{\tilde{\rho}^s} - nh(r/n),$$

where $\tilde{\epsilon} = \frac{\epsilon^2}{6|S|}$, and we have used the fact that $H_{\max}(\tilde{\rho}_S) = \log_2\mathrm{rank}(\tilde{\rho}_S) = nh(r/n)$.

Without loss of generality, $|\psi_s\rangle = |\theta\rangle^{n-r}\otimes|\hat{\psi}_s\rangle$ for some $|\hat{\psi}_s\rangle \in \mathcal{H}_{ABE}^{\otimes r}$. Then,

$$\tilde{\rho}^s_{A^nE^n} = \mathrm{tr}_{B^n}(|\theta\rangle\langle\theta|^{\otimes n-r}\otimes|\hat{\psi}_s\rangle\langle\hat{\psi}_s|) = (\mathrm{tr}_B|\theta\rangle\langle\theta|)^{\otimes n-r}\otimes\mathrm{tr}_{B^r}|\hat{\psi}_s\rangle\langle\hat{\psi}_s|.$$

Denote $\hat{\rho}^s_{A^rE^r} = \mathrm{tr}_{B^r}|\hat{\psi}_s\rangle\langle\hat{\psi}_s|$ and $\sigma_{AE} = \mathrm{tr}_B|\theta\rangle\langle\theta|$. By superadditivity of min-entropy, we have

$$H_{\min}^{\tilde{\epsilon}}(A^n|E^n)_{\tilde{\rho}^s} \geqslant H_{\min}^{\tilde{\epsilon}}(A^{n-r}|E^{n-r})_{\sigma^{\otimes n-r}} + H_{\min}(A^r|E^r)_{\hat{\rho}^s}.$$

Using the asymptotic equipartition property for i.i.d. states [62], that is, $H_{\min}^\epsilon(A^{n-r}|E^{n-r})_{\sigma^{\otimes n-r}} \geqslant (n-r)H(A|E)_\sigma - \sqrt{n-r}\delta(\epsilon,\mu)$, where $\delta(\epsilon,\mu) = 4\log_2\mu\sqrt{\log_2\frac{2}{\epsilon^2}}$, and $H_{\min}(A^r|E^r)_{\hat{\rho}^s} \geqslant -2\log_2\mathrm{tr}\sqrt{\hat{\rho}^s_{A^r}} \geqslant -r\log_2 d_A$, we obtain, for any s,

$$H_{\min}^{\tilde{\epsilon}}(A^n|E^n)_{\tilde{\rho}^s} \geqslant (n-r)H(A|E)_\sigma - \sqrt{n-r}\delta(\tilde{\epsilon},\mu) - r\log_2 d_A.$$

Hence, we have

$$H_{\min}^\epsilon(A|E)_{\rho_{AE}} \geqslant (n-r)H(A|E)_{\sigma_{AE}} - \sqrt{n-r}\delta(\tilde{\epsilon},\mu) - r\log_2 d_A - nh(r/n).$$

From the duality of smooth min- and max-entropy, we obtain the result. ∎

Lemma 12. (polytope confidence interval for almost i.i.d. state quantum tomography) $|\Psi_\theta\rangle \in \mathrm{Sym}(\mathcal{H}_{ABE}^{\otimes n}, |\theta\rangle^{\otimes n-r})$, where $r < n/2$. Suppose we apply local Pauli measurements at input A and output B. For the kth $(0 \leqslant k \leqslant d^2-1)$ Pauli observable, denote the corresponding POVM by $\mathcal{M}_k := \{E_k^{(l)}\}_{l=0}^{d-1}$ on $\mathcal{H}_A\otimes\mathcal{H}_B$, where l denotes the measurement outcome. After the measurements $\otimes_{k=0}^{d^2-1}\mathcal{M}_k^{\otimes n_k}$, for each k, the number of rounds of measurements getting outcome l is n_k^l. The confidence interval of state $\rho_{AB} = \mathrm{tr}_E|\theta\rangle\langle\theta|$, with confidence level $1-\delta$, where $\delta = \sum_{k=0}^{d^2-1}\sum_{l=0}^{d-1}\delta_k^l$, is $\Gamma = \cap_{0\leqslant k\leqslant d^2-1, 0\leqslant l\leqslant d-1}\Gamma_{kl}$, where

$$\Gamma_{kl} := \left\{ \rho \in \mathcal{S}(\mathcal{H}_{AB}) : \mathrm{tr}\left(\rho E_k^{(l)}\right) \leqslant \frac{n_k^l}{n_k} + \frac{n}{n_k}\sqrt{\frac{\log_2 1/\delta_k^l}{n} + h(r/n) + \frac{2}{n}\log_2(n/2+1)} \right\}. \tag{A44}$$

Proof. The proof combines the idea of confidence polytope in quantum tomography [63] with the statistical properties of almost i.i.d. states [49]. The POVM measurements at $\mathcal{H}_{AB}$ can be easily extended to $\mathcal{H}_{ABE}$ by denoting $\tilde{\mathcal{M}}_k := \{\tilde{E}_k^{(l)}\}_{l=0}^{d-1}$, where $\tilde{E}_k^{(l)} := E_k^{(l)}\otimes\mathbb{1}_E$. A renormalized POVM on $\mathcal{H}_{ABE}$ is $\tilde{\mathcal{M}} := \{\frac{n_k}{n}\tilde{E}_k^{(l)}\}_{k=0,l=0}^{d^2-1,d-1}$.

Then we consider POVM $\{\frac{n_k}{n}\tilde{E}_k^{(l)}, \mathbb{1}_{ABE} - \frac{n_k}{n}\tilde{E}_k^{(l)}\}$. Using Theorem 4.5.2 in Ref. [49], we obtain, for each k and l,

$$\Pr\left(\left|\langle\theta|\tilde{E}_k^{(l)}|\theta\rangle - \frac{n_k^l}{n_k}\right| > \frac{n}{n_k}\sqrt{\frac{\log_2\left(1/\delta_k^l\right)}{n_k} + h(r/n) + \frac{2}{n}\log_2(n_k/2+1)}\right) \leqslant \delta_k^l. \tag{A45}$$

By noting that $\mathrm{tr}[(\mathrm{tr}_E\,|\theta\rangle\langle\theta|)E_k^{(l)}] = \langle\theta|\tilde{E}_k^{(l)}|\theta\rangle$, we get

$$\Pr\left[\mathrm{tr}\left(\rho E_k^{(l)}\right) > \frac{n_k^l}{n_k} + \frac{n}{n_k}\sqrt{\frac{\log_2 1/\delta_k^l}{n} + h(r/n) + \frac{2}{n}\log_2(n/2+1)}\right] \leqslant \delta_k^l. \tag{A46}$$

Finally, the union bound indicates that $\sigma \in \cap_{0\leqslant k\leqslant d^2-1, 0\leqslant l\leqslant d-1}\Gamma_{kl}$, with probability at least $1 - \sum_{k=0}^{d^2-1}\sum_{l=0}^{d-1}\delta_k^l$. ■

Theorem 6. Suppose a quantum channel $\mathcal{E}^{n+k} : \mathcal{H}_{A'}^{\otimes n+k} \to \mathcal{H}_B^{\otimes n+k}$. We feed one party of the maximally entangled state at each input and keep the other party as a reference system. We randomly abandon k outputs and denote the channel corresponding to the other n inputs and n outputs by $\mathcal{E}^n$. For any error $\epsilon/2 > \epsilon' := 2k^{d/2}e^{-\frac{k(r+1)}{2(n+k)}}$, we have the lower bound of one-shot quantum capacity of $\mathcal{E}^n$,

$$\begin{aligned}Q^\epsilon(\mathcal{E}^n) \geqslant \max\Bigg\{0, \sup_{\eta\in(0,\sqrt{\epsilon/2}-\sqrt{\epsilon'})}\Big[-4\sqrt{n-r}\log_2(2\sqrt{2}+1)\sqrt{2nh(r/n) - 4\log_2(\sqrt{\epsilon/2}-\eta-\sqrt{\epsilon'}) + 2\log_2 6 + 1} + 4\log_2\eta\Big] \\ - nh(r/n) - r + (n-r)\min_{\sigma\in\Gamma}(H(B)_\sigma - H(AB)_\sigma) - 2\Bigg\}.\end{aligned} \tag{A47}$$

Proof. Lemma 1 tells us that $Q^\epsilon(\mathcal{E}^n)$ can be bounded below by a function of smooth max-entropy $H_{\max}^{\sqrt{\epsilon/2}-\eta}(A^n|B^n)_\rho$ optimized over $\eta \in (0, \sqrt{\epsilon/2})$, where ρ^n is the state at the n output qubits and the associated n ancillary qubits. The smooth max-entropy itself is a minimum value within a neighborhood $\mathcal{B}^{\sqrt{\epsilon/2}-\eta}(\rho_{A^nB^n})$. As Lemma 10, together with the fact that partial trace can only reduce trace distance, implies that $\rho_{A^nB^n}$ is close to an unknown almost i.i.d. state $\tilde{\rho}_{A^nB^n}$, we can use the minimum value over a smaller neighborhood around $\tilde{\rho}_{A^nB^n}$, which is a subset of $\mathcal{B}^{\sqrt{\epsilon/2}-\eta}(\rho_{A^nB^n})$, to obtain an upper bound on $H_{\max}^{\sqrt{\epsilon/2}-\eta}(A^n|B^n)_\rho$.

Using the triangle inequality of purified distance [51], we have, for any $\rho'_{A^nB^n} \in \mathcal{S}(\mathcal{H}_{A^nB^n})$,

$$\mathcal{P}(\rho_{A^nB^n}, \rho'_{A^nB^n}) \leqslant \mathcal{P}\left[\rho_{A^nB^n}, \int d\nu(\theta)\tilde{\rho}^\theta_{A^nB^n}\right] + \mathcal{P}\left[\rho'_{A^nB^n}, \int d\nu(\theta)\tilde{\rho}^\theta_{A^nB^n}\right]. \tag{A48}$$

To make sure $\mathcal{P}(\rho_{A^nB^n}, \rho'_{A^nB^n}) \leqslant \sqrt{\epsilon/2} - \eta$, as $\mathcal{P}[\rho_{A^nB^n}, \int d\nu(\theta)\tilde{\rho}^\theta_{A^nB^n}] \leqslant \sqrt{\lambda}$ with $\epsilon' := 2k^8e^{-\frac{k(r+1)}{2(n+k)}}$, we only need to set $\mathcal{P}[\rho'_{A^nB^n}, \int d\nu(\theta)\tilde{\rho}^\theta_{A^nB^n}] \leqslant \sqrt{\epsilon/2} - \eta - \sqrt{\epsilon'}$. Hence, using both Lemma 11 and Lemma 12, we get a lower bound, when $\eta < \sqrt{\epsilon/2} - \sqrt{\epsilon'}$,

$$\begin{aligned}-H_{\max}^{\sqrt{\epsilon/2}-\eta}(A^n|B^n)_\rho \geqslant -H_{\max}^{\sqrt{\epsilon/2}-\eta-\sqrt{\epsilon'}}(A^n|B^n)_{\tilde{\rho}} \geqslant -4\sqrt{n-r}\log_2(2\sqrt{2}+1)\sqrt{2nh(r/n) - 4\log_2(\sqrt{\epsilon/2}-\eta-\sqrt{\epsilon'}) + 2\log_2 6 + 1} \\ - nh(r/n) - r + (n-r)\min_{\sigma\in\Gamma}(H(B)_\sigma - H(AB)_\sigma),\end{aligned}$$

and hence, using Lemma 1, we get the result. ■

[1] S. L. Braunstein and H. J. Kimble, Teleportation of Continuous Quantum Variables, Phys. Rev. Lett. **80**, 869 (1998).

[2] A. Furusawa, J. L. Sørensen, S. L. Braunstein, C. A. Fuchs, H. J. Kimble, and E. S. Polzik, Unconditional quantum teleportation, Science **282**, 706 (1998).

[3] P. Jouguet, S. Kunz-Jacques, A. Leverrier, P. Grangier, and E. Diamanti, Experimental demonstration of long-distance continuous-variable quantum key distribution, Nat. Photon. **7**, 378 (2013).

[4] S. Pirandola, C. Ottaviani, G. Spedalieri, C. Weedbrook, S. L. Braunstein, S. Lloyd, T. Gehring, C. S. Jacobsen, and U. L. Andersen, High-rate measurement-device-independent quantum cryptography, Nat. Photon. **9**, 397 (2015).

[5] S. Pirandola, R. Laurenza, C. Ottaviani, and L. Banchi, Fundamental limits of repeaterless quantum communications, Nat. Commun. **8**, 15043 (2017).

[6] N. C. Menicucci, P. van Loock, M. Gu, C. Weedbrook, T. C. Ralph, and M. A. Nielsen, Universal Quantum Computation with Continuous-Variable Cluster States, Phys. Rev. Lett. **97**, 110501 (2006).

[7] M. Gu, C. Weedbrook, N. C. Menicucci, T. C. Ralph, and P. van Loock, Quantum computing with continuous-variable clusters, Phys. Rev. A **79**, 062318 (2009).

[8] B. Q. Baragiola, G. Pantaleoni, R. N. Alexander, A. Karanjai, and N. C. Menicucci, All-Gaussian Universality and Fault Tolerance with the Gottesman-Kitaev-Preskill Code, Phys. Rev. Lett. **123**, 200502 (2019).

[9] J. L. O'Brien, A. Furusawa, and J. Vučković, Photonic quantum technologies, Nat. Photon. **3**, 687 (2009).

[10] D. Gottesman, A. Kitaev, and J. Preskill, Encoding a qubit in an oscillator, Phys. Rev. A **64**, 012310 (2001).

[11] M. Mirrahimi, Z. Leghtas, V. V. Albert, S. Touzard, R. J. Schoelkopf, L. Jiang, and M. H. Devoret, Dynamically protected cat-qubits: A new paradigm for universal quantum computation, New J. Phys. **16**, 045014 (2014).

[12] M. H. Michael, M. Silveri, R. T. Brierley, V. V. Albert, J. Salmilehto, L. Jiang, and S. M. Girvin, New Class of Quantum Error-Correcting Codes for a Bosonic Mode, Phys. Rev. X **6**, 031006 (2016).

[13] V. V. Albert, K. Noh, K. Duivenvoorden, D. J. Young, R. T. Brierley, P. Reinhold, C. Vuillot, L. Li, C. Shen, S. M. Girvin, B. M. Terhal, and L. Jiang, Performance and structure of single-mode bosonic codes, Phys. Rev. A **97**, 032346 (2018).

[14] K. Noh, V. V. Albert, and L. Jiang, Quantum capacity bounds of Gaussian thermal loss channels and achievable rates with Gottesman-Kitaev-Preskill codes, IEEE Trans. Inf. Theory **65**, 2563 (2018).

[15] K. Sharma, M. M. Wilde, S. Adhikari, and M. Takeoka, Bounding the energy-constrained quantum and private capacities of phase-insensitive bosonic Gaussian channels, New J. Phys. **20**, 063025 (2018).

[16] K. Noh, S. Pirandola, and L. Jiang, Enhanced energy-constrained quantum communication over bosonic Gaussian channels, Nat. Commun. **11**, 457 (2020).

[17] K. Noh, S. M. Girvin, and L. Jiang, Encoding an Oscillator Into Many Oscillators, Phys. Rev. Lett. **125**, 080503 (2020).

[18] S. Lloyd, Capacity of the noisy quantum channel, Phys. Rev. A **55**, 1613 (1997).

[19] D. P. DiVincenzo, P. W. Shor, and J. A. Smolin, Quantum-channel capacity of very noisy channels, Phys. Rev. A **57**, 830 (1998).

[20] I. Devetak, The private classical capacity and quantum capacity of a quantum channel, IEEE Trans. Inf. Theory **51**, 44 (2005).

[21] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information* (Cambridge University Press, Cambridge, 2010).

[22] M. M. Wilde, *Quantum Information Theory* (Cambridge University Press, Cambridge, 2013).

[23] V. Giovannetti and R. Fazio, Information-capacity description of spin-chain correlations, Phys. Rev. A **71**, 032314 (2005).

[24] M. M. Wolf and D. Pérez-García, Quantum capacities of channels with small environment, Phys. Rev. A **75**, 012303 (2007).

[25] A. S. Holevo and R. F. Werner, Evaluating capacities of bosonic Gaussian channels, Phys. Rev. A **63**, 032312 (2001).

[26] M. M. Wolf, D. Pérez-García, and G. Giedke, Quantum Capacities of Bosonic Channels, Phys. Rev. Lett. **98**, 130501 (2007).

[27] F. Caruso, V. Giovannetti, C. Lupo, and S. Mancini, Quantum channels and memory effects, Rev. Mod. Phys. **86**, 1203 (2014).

[28] I. L. Chuang and M. A. Nielsen, Prescription for experimental determination of the dynamics of a quantum black box, J. Mod. Opt. **44**, 2455 (1997).

[29] J. F. Poyatos, J. I. Cirac, and P. Zoller, Complete Characterization of a Quantum Process: The Two-Bit Quantum Gate, Phys. Rev. Lett. **78**, 390 (1997).

[30] G. M. D'Ariano and P. Lo Presti, Quantum Tomography for Measuring Experimentally the Matrix Elements of an Arbitrary Quantum Operation, Phys. Rev. Lett. **86**, 4195 (2001).

[31] G. M. D'Ariano and P. Lo Presti, Imprinting Complete Information about a Quantum Channel on its Output State, Phys. Rev. Lett. **91**, 047902 (2003).

[32] J. B. Altepeter, D. Branning, E. Jeffrey, T. C. Wei, P. G. Kwiat, R. T. Thew, J. L. O'Brien, M. A. Nielsen, and A. G. White, Ancilla-Assisted Quantum Process Tomography, Phys. Rev. Lett. **90**, 193601 (2003).

[33] C. Macchiavello and M. F. Sacchi, Detecting Lower Bounds to Quantum Channel Capacities, Phys. Rev. Lett. **116**, 140501 (2016).

[34] C. Macchiavello and M. F. Sacchi, Witnessing quantum capacities of correlated channels, Phys. Rev. A **94**, 052333 (2016).

[35] Á. Cuevas, M. Proietti, M. A. Ciampini, S. Duranti, P. Mataloni, M. F. Sacchi, and C. Macchiavello, Experimental Detection of Quantum Channel Capacities, Phys. Rev. Lett. **119**, 100502 (2017).

[36] C. Pfister, M. A. Rol, A. Mantri, M. Tomamichel, and S. Wehner, Capacity estimation and verification of quantum channels with arbitrarily correlated errors, Nat. Commun. **9**, 27 (2018).

[37] S. Pirandola and S. Mancini, Quantum teleportation with continuous variables: A survey, Laser Phys. **16**, 1418 (2006).

[38] P. Liuzzo-Scorpo, A. Mari, V. Giovannetti, and G. Adesso, Optimal Continuous Variable Quantum Teleportation with Limited Resources, Phys. Rev. Lett. **119**, 120503 (2017).

[39] K. Horodecki, M. Horodecki, P. Horodecki, D. Leung, and J. Oppenheim, Unconditional Privacy over Channels which Cannot Convey Quantum Information, Phys. Rev. Lett. **100**, 110502 (2008).

[40] S. Lloyd and Jean-Jacques E. Slotine, Analog Quantum Error Correction, Phys. Rev. Lett. **80**, 4088 (1998).

[41] D. W. Leung, M. A. Nielsen, I. L. Chuang, and Y. Yamamoto, Approximate quantum error correction can lead to better codes, Phys. Rev. A **56**, 2567 (1997).

[42] Y. Yang, Y. Mo, J. M. Renes, G. Chiribella, and M. P. Woods, Covariant quantum error correcting codes via reference frames, Phys. Rev. Res. **4**, 023107 (2022).

[43] P. Faist, S. Nezami, V. V. Albert, G. Salton, F. Pastawski, P. Hayden, and J. Preskill, Continuous Symmetries and Approximate Quantum Error Correction, Phys. Rev. X **10**, 041018 (2020).

[44] S. Zhou, Z.-W. Liu, and L. Jiang, New perspectives on covariant quantum error correction, Quantum **5**, 521 (2021).

[45] F. Buscemi and N. Datta, The quantum capacity of channels with arbitrarily correlated noise, IEEE Trans. Inf. Theory **56**, 1447 (2010).

[46] H. Barnum, E. Knill, and M. A. Nielsen, On quantum fidelities and channel capacities, IEEE Trans. Inf. Theory **46**, 1317 (2000).

[47] C. Morgan and A. Winter, "Pretty strong" converse for the quantum capacity of degradable channels, IEEE Trans. Inf. Theory **60**, 317 (2013).

[48] M. Tomamichel, M. Berta, and J. M. Renes, Quantum coding with finite resources, Nat. Commun. **7**, 11419 (2016).

[49] R. Renner, Security of quantum key distribution, Intl. J. Quantum Inf. **06**, 1 (2008).

[50] R. Konig, R. Renner, and C. Schaffner, The operational meaning of min-and max-entropy, IEEE Trans. Inf. Theory **55**, 4337 (2009).

[51] A. Gilchrist, N. K. Langford, and M. A. Nielsen, Distance measures to compare real and ideal quantum processes, Phys. Rev. A **71**, 062310 (2005).

[52] F. Furrer, J. Åberg, and R. Renner, Min-and max-entropy in infinite dimensions, Commun. Math. Phys. **306**, 165 (2011).

[53] M. Berta, F. Furrer, and V. B. Scholz, The smooth entropy formalism for von Neumann algebras, J. Math. Phys. **57**, 015213 (2016).

[54] A. I. Lvovsky and M. G. Raymer, Continuous-variable optical quantum-state tomography, Rev. Mod. Phys. **81**, 299 (2009).

[55] F. Furrer, T. Franz, M. Berta, A. Leverrier, V. B. Scholz, M. Tomamichel, and R. F. Werner, Continuous Variable Quantum Key Distribution: Finite-Key Analysis of Composable Security against Coherent Attacks, Phys. Rev. Lett. **109**, 100502 (2012).

[56] F. Furrer, M. Berta, M. Tomamichel, V. B. Scholz, and M. Christandl, Position-momentum uncertainty relations in the presence of quantum memory, J. Math. Phys. **55**, 122205 (2014).

[57] H. Vahlbruch, M. Mehmet, K. Danzmann, and R. Schnabel, Detection of 15 dB Squeezed States of Light and their Application for the Absolute Calibration of Photoelectric Quantum Efficiency, Phys. Rev. Lett. **117**, 110801 (2016).

[58] N. J. Cerf, A. Ipe, and X. Rottenberg, Cloning of Continuous Quantum Variables, Phys. Rev. Lett. **85**, 1754 (2000).

[59] G. Chiribella and J. Xie, Optimal Design and Quantum Benchmarks for Coherent State Amplifiers, Phys. Rev. Lett. **110**, 213602 (2013).

[60] C. Weedbrook, S. Pirandola, R. García-Patrón, N. J. Cerf, T. C. Ralph, J. H. Shapiro, and S. Lloyd, Gaussian quantum information, Rev. Mod. Phys. **84**, 621 (2012).

[61] A. Serafini, Multimode Uncertainty Relations and Separability of Continuous Variable States, Phys. Rev. Lett. **96**, 110402 (2006).

[62] M. Tomamichel, R. Colbeck, and R. Renner, A fully quantum asymptotic equipartition property, IEEE Trans. Inf. Theory **55**, 5840 (2009).

[63] J. Wang, V. B. Scholz, and R. Renner, Confidence Polytopes in Quantum State Tomography, Phys. Rev. Lett. **122**, 190401 (2019).

[64] R. Renner, Symmetry of large physical systems implies independence of subsystems, Nat. Phys. **3**, 645 (2007).

[65] M. M. Wilde and H. Qi, Energy-constrained private and quantum capacities of quantum channels, IEEE Trans. Inf. Theory **64**, 7802 (2018).

[66] J.-P. W. MacLean, K. Ried, R. W. Spekkens, and K. J. Resch, Quantum-coherent mixtures of causal relations, Nat. Commun. **8**, 15149 (2017).

[67] G. Bai, Y.-D. Wu, Y. Zhu, M. Hayashi, and G. Chiribella, Quantum causal unravelling, npj Quantum Inf. **8**, 69 (2022).

[68] A. Leverrier, Security of Continuous-Variable Quantum Key Distribution via a Gaussian de Finetti Reduction, Phys. Rev. Lett. **118**, 200501 (2017).

[69] R. Valivarthi, S. I. Davis, C. Peña, S. Xie, N. Lauk, L. Narváez, J. P. Allmaras, A. D. Beyer, Y. Gim, M. Hussein, G. Iskander, H. L. Kim, B. Korzh, A. Mueller, M. Rominsky, M. Shaw, D. Tang, E. E. Wollman, C. Simon, P. Spentzouris *et al.*, Teleportation systems toward a quantum internet, PRX Quantum **1**, 020317 (2020).

[70] S. Khatri and M. M. Wilde, Principles of quantum communication theory: A modern approach, arXiv:2011.04672.

[71] A. Vitanov, F. Dupuis, M. Tomamichel, and R. Renner, Chain rules for smooth min-and max-entropies, IEEE Trans. Inf. Theory **59**, 2603 (2013).

[72] J. Kiukas and R. F. Werner, Maximal violation of Bell inequalities by position measurements, J. Math. Phys. **51**, 072105 (2010).

[73] B. Laurent and P. Massart, Adaptive estimation of a quadratic functional by model selection, Ann. Stat. **28**, 1302 (2000).