Quantum trade-off coding for bosonic communication

Mark M. Wilde and Patrick Hayden
School of Computer Science, McGill University, Montreal, Québec, Canada H3A 2A7

Saikat Guha
Quantum Information Processing Group, Raytheon BBN Technologies, Cambridge, Massachusetts, 02138 USA
(Received 17 July 2012; published 6 December 2012)

The trade-off capacity region of a quantum channel characterizes the optimal net rates at which a sender can communicate classical, quantum, and entangled bits to a receiver by exploiting many independent uses of the channel, along with the help of the same resources. Similarly, one can consider a trade-off capacity region when the noiseless resources are public, private, and secret-key bits. We identified [see Wilde, Hayden, and Guha, Phys. Rev. Lett. **108**, 140501 (2012)] these trade-off rate regions for the pure-loss bosonic channel and proved that they are optimal provided that a long-standing minimum-output entropy conjecture is true. Additionally, we showed that the performance gains of a trade-off coding strategy when compared to a time-sharing strategy can be quite significant. In this paper, we provide detailed derivations of the results announced there, and we extend the application of these ideas to thermal-noise and amplifying bosonic channels. We also derive a "rule of thumb" for trade-off coding, which determines how to allocate photons in a coding strategy if a large mean photon number is available at the channel input. Our results on the amplifying bosonic channel also apply to the "Unruh channel" considered in the context of relativistic quantum information theory.

DOI: 10.1103/PhysRevA.86.062306 PACS number(s): 03.67.Hk, 03.67.Pp, 04.62.+v

I. INTRODUCTION

One of the great scientific accomplishments of the last century was Shannon's formulation of information theory and his establishment of its two fundamental theorems [1]. Shannon's first theorem states that the entropy of an information source is the best rate at which it can be compressed, in the limit where many copies of the source are available. His second theorem states that the maximum mutual information of a classical channel is the highest rate at which information can be transmitted error free over such a channel, again in a limit where many independent uses of the channel are available.

Shannon's theory is certainly successful in a world obeying the laws of classical physics, but as we know, quantum mechanics is necessary in order to describe the true physical nature of many communication channels. In particular, a quantum-mechanical model is especially important for the case of optical communication over free space or fiber-optic channels (the name for a simple model of this channel is the *pure-loss bosonic channel* [2]). As such, we should also revise Shannon's theory of information in order to account for quantum-mechanical effects, and Holevo, Schumacher, and Westmoreland (HSW) [3,4] were some of the first to begin this effort by proving that a quantity now known as the Holevo information is an achievable rate for classical communication over a quantum channel. Revising Shannon's information theory is not merely a theoretical curiosity (the promise of quantum information theory is that communication rates can be boosted by doing so [5,6]), and recent experiments have improved the state of the art in approaching the limits on communication given by quantum information theory [7].

The task of communicating classical data is certainly important, but the communication of quantum data could be just as important, given the advent of quantum computation [8] and given the possibility that distributed quantum computation might one day become a reality [9]. Lloyd [10], Shor [11], and Devetak [12] (LSD) gave increasingly rigorous proofs that a quantity known as the coherent information of a quantum channel is an achievable rate for quantum communication, after Schumacher and others identified that this quantity would be relevant for quantum data transmission [13–16].

In future communication networks, it is likely that a sender and receiver will not be using communication channels to transmit either classical data alone or quantum data alone, but rather that the data being transmitted will be a mix of these data types. Additionally, it could be that the sender and receiver might share some entanglement before communication begins, and it is well known that entanglement can boost transmission rates [17,18]. A simple strategy for simultaneously communicating classical and quantum data would be for the sender and receiver to use the best HSW classical code for a fraction of the time and to use the best LSD quantum code for the other fraction of the time (this simple strategy is known as time sharing). Devetak and Shor, however, demonstrated that this is not the optimal strategy in general and that a trade-off coding strategy can outperform a time-sharing strategy [17]. In short, a trade-off coding strategy is one in which the sender encodes classical information into the many different ways of permuting quantum error-correcting codes. After obtaining the channel outputs, the receiver first performs a measurement to identify which permutation the sender employed, and as long as the total number of permutations is not too large, it is possible to identify the permutation with arbitrarily high probability (and thus recovering the classical data that the sender transmitted). Since this measurement is successful, it causes a negligible disturbance to the state [19], and the receiver can then decode the quantum information encoded in the quantum codes.

We showed recently [20] that the performance gains can be very significant for a pure-loss bosonic channel when employing a trade-off coding strategy rather than a time-sharing strategy. (In this case, the trade-off coding strategy amounts to a power-sharing strategy, like those considered in classical information theory [21].) We briefly summarize the main results of Ref. [20]. Suppose that a sender and receiver are allowed access to many independent uses of a pure-loss bosonic channel with transmissivity parameter $\eta \in [0,1]$ (so that η is the average fraction of photons that make it to the receiver). Suppose further that the sender is power constrained to input N_S photons to the channel on average per channel use. Let C be the net rate of classical communication (in bits per channel use), Q the net rate of quantum communication (in qubits per channel use), and E the net rate of entanglement generation (in ebits per channel use). If a given rate is positive, then it means the protocol generates the corresponding resource at the given rate, whereas if a given rate is negative, then the protocol consumes the corresponding resource at the given rate. The first main result of Ref. [20] is that the following rate region is achievable:

$$\begin{aligned} C + 2Q &\leqslant g(\lambda N_S) + g(\eta N_S) - g((1-\eta)\lambda N_S), \\ Q + E &\leqslant g(\eta\lambda N_S) - g((1-\eta)\lambda N_S), \\ C + Q + E &\leqslant g(\eta N_S) - g((1-\eta)\lambda N_S), \end{aligned} \tag{1}$$

where $g(x) \equiv (x+1)\log_2(x+1) - x\log_2 x$ is the entropy of a thermal distribution with mean photon number x and $\lambda \in [0,1]$ is a photon-number-sharing parameter, determining the fraction of photons the code dedicates to quantum communication (so that $1-\lambda$ is the fraction of photons that the code dedicates to classical communication). The full region is the union over all of the three-faced polyhedra given by the above inequalities, as the photon-number-sharing parameter λ increases from zero to one. This region is optimal whenever $\eta \geqslant \frac{1}{2}$ provided that a long-standing minimum output entropy conjecture is true [22–25], which remains unproven but towards which proving there has been some good recent progress [26,27].

The second main result of Ref. [20] applies to a different though related setting. The sender and receiver are again given access to many independent uses of a pure-loss bosonic channel, but this time, the trade-off is between the rate R of public classical communication, the rate P of private classical communication, and the rate S of secret key. We showed that the following region is achievable:

$$\begin{aligned} R + P &\leqslant g(\eta N_S), \\ P + S &\leqslant g(\lambda\eta N_S) - g(\lambda(1-\eta)N_S), \\ R + P + S &\leqslant g(\eta N_S) - g(\lambda(1-\eta)N_S), \end{aligned} \tag{2}$$

where the parameter $\lambda \in [0,1]$ is again a photon-number-sharing parameter, determining the fraction of photons the code dedicates to private communication (so that $1-\lambda$ is the fraction of photons that the code dedicates to public communication). Optimality of this region whenever $\eta \geqslant \frac{1}{2}$ is again subject to the same long-standing minimum-output entropy conjecture. This result has a practical relevance for a quantum key distribution protocol executed using a pure-loss bosonic channel and forward public classical communication only.

In this paper, we provide detailed derivations of the above results announced in Ref. [20], and we extend the ideas there to thermal-noise and amplifying bosonic channels. Section II recasts known results on trade-off coding [28–31] into a form more suitable for the bosonic setting. Section III proves that the regions in Eqs. (1) and (2) are achievable and that they are the capacity regions provided a long-standing minimum-output entropy conjecture is true [32]. Section III also gives expressions for special cases of the regions in Eqs. (1) and (2), demonstrates that trade-off coding always beats time sharing whenever $0 < \eta < 1$, rigorously establishes a "rules of thumb" for trade-off coding outlined in Ref. [20], and considers the high-photon-number limit for some special cases. Sections IV and V give achievable rate regions for the thermal-noise and amplifier bosonic channels, respectively. Finally, Sec. VI demonstrates that an encoding with a fixed mean photon budget can beat the rates achieved with a single-excitation encoding for the "Unruh channel." We summarize our results in the conclusion and suggest interesting lines of inquiry for future research.

II. REVIEW OF TRADE-OFF REGIONS

In recent work, Wilde and Hsieh have synthesized all known single-sender single-receiver quantum and classical communication protocols over a general noisy quantum channel into a three-way dynamic capacity region that they call the "triple-trade-off" region [28–30]. They consider a three-dimensional region whose points (C,Q,E) correspond to rates of classical communication, quantum communication, and entanglement generation (or consumption), respectively. Let us illustrate a few simple examples of such triple trade-offs. In the *qubit teleportation* protocol [33], communication (consumption) of two classical bits and communication (consumption) of one ebit of shared entanglement is used to communicate (generate) one noiseless qubit, giving a rate triple $(-2,1,-1)$, where a minus sign indicates the consumption of a resource and a plus sign indicates the generation of a resource. Similarly, the superdense coding protocol consumes a noiseless qubit channel and an ebit to generate two classical bits [33]. It corresponds to the rate triple $(2,-1,-1)$. Another simple protocol is entanglement distribution, which communicates one noiseless qubit to generate one ebit of shared entanglement, thereby yielding the rate triple $(0,-1,1)$. Wilde and Hsieh have shown that when a communication channel is noisy, the above three unit-resource protocols, in conjunction with the *classically enhanced father protocol* [28,34], can be used to derive the ultimate (C,Q,E) trade-off space for any noisy quantum channel. The dynamic capacity region's formulas are regularized over multiple channel uses, and hence the triple trade-off region may in general be superadditive. Another dynamic capacity region that Wilde and Hsieh characterize is the trade-off between private communication rate P (generation or consumption), public communication rate R (generation or consumption), and secret-key rate S (distribution or consumption) [31]. We should clarify that these public and private rates are for forward communication (generation or consumption).

A. Quantum dynamic region

Proposition 1. The quantum dynamic capacity region of a quantum channel $\mathcal{N}$ is the regularization of the union of regions of the form

$$C + 2Q \leqslant H(\mathcal{N}(\rho)) + \sum_x p_X(x)[H(\rho_x) - H(\mathcal{N}^c(\rho_x))], \tag{3}$$

$$Q + E \leqslant \sum_x p_X(x)[H(\mathcal{N}(\rho_x)) - H(\mathcal{N}^c(\rho_x))], \tag{4}$$

$$C + Q + E \leqslant H(\mathcal{N}(\rho)) - \sum_x p_X(x) H(\mathcal{N}^c(\rho_x)), \tag{5}$$

where $H(\sigma) \equiv -\text{Tr}(\sigma \ln \sigma)$, $\{p_X(x),\rho_x\}$ is an ensemble with expected density operator $\rho \equiv \sum_x p_X(x)\rho_x$ and $\mathcal{N}^c$ is the channel complementary to the channel $\mathcal{N}$.

Proof. The above proposition is just a rephrasing of the results from Refs. [28–30]. First recall that the quantum mutual information of a bipartite state ρ^{AB} is defined as follows:

$$I(A;B)_\rho \equiv H(A)_\rho + H(B)_\rho - H(AB)_\rho,$$

the conditional entropy is defined as

$$H(A|B)_\rho \equiv H(AB)_\rho - H(B)_\rho,$$

and the coherent information is

$$I(A\rangle B)_\rho \equiv -H(A|B)_\rho.$$

Reference [30] derived that the quantum dynamic capacity region is the regularization of the union of regions of the form

$$C + 2Q \leqslant I(AX;B)_\rho, \tag{6}$$

$$Q + E \leqslant I(A\rangle BX)_\rho, \tag{7}$$

$$C + Q + E \leqslant I(X;B)_\rho + I(A\rangle BX)_\rho, \tag{8}$$

where the union is over all classical-quantum states ρ^{XAB} of the following form:

$$\rho^{XAB} \equiv \sum_x p_X(x)\,|x\rangle\,\langle x|^X \otimes \mathcal{N}^{A'\to B}(\phi_x^{AA'}), \tag{9}$$

and each $\phi_x^{AA'}$ is a pure, bipartite state [28–30]. The convention in the above formulas is that a rate for a resource is positive when the communication protocol generates that resource, and the rate for a resource is negative when the communication protocol consumes that resource. The above characterization is the full triple trade-off, including both positive and negative rates. A simple strategy for achieving the above capacity region is to combine the "classically enhanced father protocol" [28,34] with teleportation [33], superdense coding [35], and entanglement distribution. The classically enhanced father protocol is a coding strategy that can communicate both classical and quantum information with the help of shared entanglement. It generalizes both of the trade-off coding strategies from Refs. [36,37].

We should clarify that the converse theorem from Ref. [30] applies even for the case of an infinite-dimensional channel. Without loss of generality, the sender's systems storing the shared entanglement, classical and quantum data to be transmitted can be assumed to be finite dimensional, as can the receiver's systems after the decoding operation. If not, the sender and receiver can isometrically transfer their information to finite-dimensional systems with negligible loss of fidelity. This is because finite numbers of perfect cbits, qubits, and ebits occupy only finite-dimensional subspaces of an infinite-dimensional Hilbert space. The converse theorem still holds in the infinite-dimensional case because all of the proofs begin by reasoning about the amount of information shared between a reference system and the decoded systems, which are finite dimensional by the above assumption. Thus, applying continuity of entropy (as is done as a first step in all of the proofs) is not problematic. The proofs then make use of quantum data processing from the outputs of the infinite-dimensional channel to the decoded systems, and it is well known that quantum data processing follows from monotonicity of quantum relative entropy [34], an inequality which is robust in the infinite-dimensional case [38]. (This is the essential ingredient behind the Yuen-Ozawa proof of the infinite-dimensional variation of the Holevo bound [6].) Thus, the converse theorem from Ref. [30] still holds for the infinite-dimensional case. (A similar statement applies to the converse theorem from Ref. [31], which we employ later on in Sec. II B.)

Due to the particular form of the state in Eq. (9), we can rewrite the inequalities in Eqs. (6)–(8) as

$$C + 2Q \leqslant H(A|X)_\rho + H(B)_\rho - H(E|X)_\rho, \tag{10}$$

$$Q + E \leqslant H(B|X)_\rho - H(E|X)_\rho, \tag{11}$$

$$C + Q + E \leqslant H(B)_\rho - H(E|X)_\rho, \tag{12}$$

where the entropies are now with respect to the classical-quantum state

$$\rho^{XABE} \equiv \sum_x p_X(x)|x\rangle\langle x|^X \otimes U_{\mathcal{N}}^{A'\to BE}(\phi_x^{AA'}), \tag{13}$$

and $U_{\mathcal{N}}^{A'\to BE}$ is an isometric extension of the channel $\mathcal{N}^{A'\to B}$. We can also think of the information quantities as being with respect to the following input ensemble [isomorphic to the input classical-quantum state in Eq. (13)]:

$$\{p_X(x),\phi_x^{AA'}\}. \tag{14}$$

Let $\rho_x \equiv \text{Tr}_A\{\phi_x^{AA'}\}$ and let $\rho \equiv \sum_x p_X(x)\rho_x$. We then obtain the inequalities in the statement of the proposition by substituting into Eqs. (10)–(12). ∎

Observe that it suffices to calculate just four entropies in order to determine the achievable rates (C,Q,E) associated to particular input ensemble:

$$H(\mathcal{N}(\rho)), \tag{15}$$

$$\sum_x p_X(x)H(\rho_x), \tag{16}$$

$$\sum_x p_X(x)H(\mathcal{N}(\rho_x)), \tag{17}$$

$$\sum_x p_X(x)H(\mathcal{N}^c(\rho_x)). \tag{18}$$

B. Private dynamic region

The private dynamic capacity region of a quantum channel captures the trade-off between public classical communication, private classical communication, and secret key [31].

Proposition 2. The private dynamic capacity region of a degradable quantum channel $\mathcal{N}$ is the regularization of the union of regions of the form

$$R + P \leqslant H(\mathcal{N}(\rho)) - \sum_{x,y} p_X(x) p_{Y|X}(y|x)\, H(\mathcal{N}(\psi_{x,y})), \tag{19}$$

$$P + S \leqslant \sum_x p_X(x)[H(\mathcal{N}(\rho_x)) - H(\mathcal{N}^c(\rho_x))], \tag{20}$$

$$R + P + S \leqslant H(\mathcal{N}(\rho)) - \sum_x p_X(x) H(\mathcal{N}^c(\rho_x)), \tag{21}$$

where $\{p_X(x)p_{Y|X}(y|x), |\psi_{x,y}\rangle\}$ is an ensemble of pure states, $\rho_x \equiv \sum_y p_{Y|X}(y|x)\psi_{x,y}$, $\rho \equiv \sum_x p_X(x)\rho_x$, and $\mathcal{N}^c$ is the channel complementary to $\mathcal{N}$.

Proof. This proposition is a rephrasing of the results in Ref. [31]. For a degradable quantum channel $\mathcal{N}$, Lemma 6 of Ref. [31] states that the private dynamic region is as follows:

$$R + P \leqslant I(YX;B)_\omega,$$
$$P + S \leqslant H(B|X)_\omega - H(E|X)_\omega,$$
$$R + P + S \leqslant H(B)_\omega - H(E|X)_\omega,$$

where R is the rate of public classical communication, P is the rate of private classical communication, S is the rate of secret-key generation or consumption, the state ω^{XYBE} is a state of the following form:

$$\omega^{XYBE} \equiv \sum_{x,y} p_X(x) p_{Y|X}(y|x) |x\rangle\langle x|^X \otimes |y\rangle\langle y|^Y \otimes U_{\mathcal{N}}^{A\to BE}\left(\psi_{x,y}^A\right),$$

$U_{\mathcal{N}}^{A\to BE}$ is an isometric extension of the channel $\mathcal{N}^{A\to B}$, and $\psi_{x,y}^A$ are pure states. The register X is associated to the public information of the code, and the register Y is associated to the code's private information. The method for achieving the above capacity region is to combine the "publicly enhanced private father" protocol with the one-time pad, private-to-public communication, and secret-key distribution [31] . The "publicly enhanced private father" protocol exploits shared secret key and the channel to communicate public and private classical information [39].

We can also think about this capacity region from the ensemble point of view. Let the input ensemble be

$$\{p_X(x)p_{Y|X}(y|x), \psi_{x,y}\}.$$

Let $\rho_x \equiv \sum_y p_{Y|X}(y|x)\psi_{x,y}$ and $\rho \equiv \sum_x p_X(x)\rho_x$. Then, we get the characterization in the statement of the proposition by substitution. ■

The above proposition also gives an achievable rate region if we restrict the input states to be pure (pure states are sufficient to achieve the boundary of the region for degradable channels, but a general channel might need an optimization over all mixed states). Observe that it suffices to consider the following four entropies in order to calculate the private dynamic capacity region:

$$H(\mathcal{N}(\rho)), \tag{22}$$

$$\sum_{x,y} p_X(x) p_{Y|X}(y|x) H(\mathcal{N}(\psi_{x,y})), \tag{23}$$

$$\sum_x p_X(x) H(\mathcal{N}(\rho_x)), \tag{24}$$

$$\sum_x p_X(x) H(\mathcal{N}^c(\rho_x)). \tag{25}$$

III. LOSSY BOSONIC CHANNEL

Consider now the case of a single-mode lossy bosonic channel. The transformation that this channel induces on the input annihilation operators is

$$\hat{a} \to \sqrt{\eta}\,\hat{a} + \sqrt{1-\eta}\,\hat{e}, \tag{26}$$

$$\hat{e} \to -\sqrt{1-\eta}\,\hat{a} + \sqrt{\eta}\,\hat{e}, \tag{27}$$

where $\hat{a}$ is the input annihilation operator for the sender, $\hat{e}$ is the input annihilation operator for the environment, and η is the transmissivity of the channel. Let $\mathcal{N}$ denote the Kraus map induced by this channel, and let $\mathcal{N}^c$ denote the complementary channel. In the case where the environmental input is the vacuum state, the complementary channel is just a lossy bosonic channel with transmissivity $1-\eta$ [40]. We place a photon-number constraint on the input mode to the channel, such that the mean number of photons at the input can not be greater than N_S.

A. Quantum dynamic achievable rate region

The proof of the theorem below justifies achievability of the region in Eq. (1) in the main text.

Theorem 3. An achievable quantum dynamic region for a lossy bosonic channel with transmissivity η is the union of regions of the form

$$C + 2Q \leqslant g(\lambda N_S) + g(\eta N_S) - g((1-\eta)\lambda N_S), \tag{28}$$

$$Q + E \leqslant g(\eta\lambda N_S) - g((1-\eta)\lambda N_S), \tag{29}$$

$$C + Q + E \leqslant g(\eta N_S) - g((1-\eta)\lambda N_S), \tag{30}$$

where $\lambda \in [0,1]$ is a photon-number-sharing parameter and $g(N)$ is the entropy of a thermal state with mean photon number N.

Proof. We pick an input ensemble of the form in Eq. (14) as follows, from which we will generate random codes:

$$\left\{p_{\bar{\lambda}N_S}(\alpha), D^{A'}(\alpha)|\psi_{\rm TMS}\rangle^{AA'}\right\}. \tag{31}$$

The distribution $p_{\bar{\lambda}N_S}(\alpha)$ is an isotropic Gaussian distribution with variance $\bar{\lambda}N_S$:

$$p_{\bar{\lambda}N_S}(\alpha) \equiv \frac{1}{\pi\bar{\lambda}N_S}\exp\{-|\alpha|^2/\bar{\lambda}N_S\}, \tag{32}$$

where $\bar{\lambda} \equiv 1-\lambda$, $\lambda \in [0,1]$ is a photon-number-sharing parameter, indicating how many photons to dedicate to the quantum part of the code, while $\bar{\lambda}$ indicates how many photons to dedicate to the classical part. In Eq. (31), $D^{A'}(\alpha)$ is a displacement operator acting on mode A', and $|\psi_{\rm TMS}\rangle^{AA'}$ is a two-mode squeezed (TMS) vacuum state of the following form [41,42]:

$$|\psi_{\rm TMS}\rangle^{AA'} \equiv \sum_{n=0}^{\infty} \sqrt{\frac{[\lambda N_S]^n}{[\lambda N_S+1]^{n+1}}}\,|n\rangle^A |n\rangle^{A'}. \tag{33}$$

Let θ denote the state resulting from tracing over the mode A:

$$\theta \equiv \text{Tr}_A\{|\psi_{\text{TMS}}\rangle\langle\psi_{\text{TMS}}|^{AA'}\} = \sum_{n=0}^{\infty} \frac{[\lambda N_S]^n}{[\lambda N_S + 1]^{n+1}} |n\rangle \langle n|^{A'}.$$

Observe that the reduced state θ is a thermal state with mean photon number λN_S [41]. Let $\overline{\theta}$ denote the state resulting from taking the expectation of the state θ over the choice of α with the prior $p_{\bar{\lambda}N_S}(\alpha)$:

$$\overline{\theta} \equiv \int d\alpha\ p_{\bar{\lambda}N_S}(\alpha)\ D(\alpha)\theta D^{\dagger}(\alpha).$$

The state $\overline{\theta}$ is just a thermal state with mean photon number N_S [41]. Thus, the state input to the channel on average has a mean photon number N_S, ensuring that we meet the photon-number constraint on the channel input.

It is worth mentioning the two extreme cases of the ensemble in Eq. (31). When the photon-number-sharing parameter $\lambda = 0$, the ensemble reduces to an ensemble of coherent states with a zero-mean Gaussian prior of variance N_S:

$$\{p_{N_S}(\alpha), |0\rangle^A \otimes |\alpha\rangle^{A'}\}.$$

This ensemble achieves the classical capacity of the lossy bosonic channel [6]. When the photon-number-sharing parameter $\lambda = 1$, the input state is always the two-mode squeezed state in Eq. (33) with $\lambda = 1$, from which random codes are then constructed. This input state achieves both the entanglement-assisted classical and quantum capacities of the lossy bosonic channel [18,43–45] and the channel's quantum capacity [40]. For the latter statement about quantum capacity, the result holds if the mean input photon number is sufficiently high [so that $g(\eta N_S) - g((1-\eta)N_S) \approx \log_2(\eta) - \log_2(1-\eta)$] and, otherwise, the statement depends on a long-standing minimum-output entropy conjecture [22,23,40].

We can now calculate the various entropies in Eqs. (15)–(18). For our case, they are respectively as follows:

$$H(\mathcal{N}(\overline{\theta})), \tag{34}$$

$$\int d\alpha\ p_{\bar{\lambda}N_S}(\alpha)\ H(D(\alpha)\theta D^{\dagger}(\alpha)), \tag{35}$$

$$\int d\alpha\ p_{\bar{\lambda}N_S}(\alpha)\ H(\mathcal{N}(D(\alpha)\theta D^{\dagger}(\alpha))), \tag{36}$$

$$\int d\alpha\ p_{\bar{\lambda}N_S}(\alpha)\ H(\mathcal{N}^c(D(\alpha)\theta D^{\dagger}(\alpha))). \tag{37}$$

The above entropies are straightforward to calculate for the case of the lossy bosonic channel. We proceed in the above order. The state $\mathcal{N}(\overline{\theta})$ is a thermal state with mean photon number ηN_S (the lossy bosonic channel attenuates the mean photon number of the transmitted thermal state), and so its entropy is

$$H(\mathcal{N}(\overline{\theta})) = g(\eta N_S).$$

Entropy is invariant under the application of a unitary transformation, and so the second entropy is just

$$\int d\alpha\ p_{\bar{\lambda}N_S}(\alpha)\ H(D(\alpha)\theta D^{\dagger}(\alpha)) = \int d\alpha\ p_{\bar{\lambda}N_S}(\alpha)\ H(\theta) = H(\theta) = g(\lambda N_S).$$

Both the channel $\mathcal{N}$ and the complementary channel $\mathcal{N}^c$ are covariant with respect to a displacement operator $D(\alpha)$ whenever the input state is thermal. Thus, we can compute the last two entropies as

$$\begin{aligned}\int d\alpha\ p_{\bar{\lambda}N_S}(\alpha)\ H(\mathcal{N}(D(\alpha)\theta D^{\dagger}(\alpha))) &= \int d\alpha\ p_{\bar{\lambda}N_S}(\alpha)\ H(D(\sqrt{\eta}\alpha)\mathcal{N}(\theta)D^{\dagger}(\sqrt{\eta}\alpha)) \\ &= H(\mathcal{N}(\theta)) = g(\eta\lambda N_S)\end{aligned} \tag{38}$$

and

$$\begin{aligned}\int d\alpha\ p_{\bar{\lambda}N_S}(\alpha)\ H(\mathcal{N}^c(D(\alpha)\theta D^{\dagger}(\alpha))) &= \int d\alpha\ p_{\bar{\lambda}N_S}(\alpha)\ H(D(\sqrt{\bar{\eta}}\alpha)\mathcal{N}^c(\theta)D^{\dagger}(\sqrt{\bar{\eta}}\alpha)) \\ &= H(\mathcal{N}^c(\theta)) = g((1-\eta)\lambda N_S),\end{aligned} \tag{39}$$

where $\overline{\eta} \equiv 1 - \eta$.

We can now specify our characterization of an achievable rate region for trade-off communication over the lossy bosonic channel simply by plugging in our various entropies into the characterization of the region in Eqs. (3)–(5). We can justify this approach by means of a limiting argument similar to that which appears in Refs. [24,40]. Suppose that we truncate the Hilbert space at the channel input so that it is spanned by the Fock number states $\{|0\rangle, |1\rangle, \ldots, |K\rangle\}$ where $K \gg N_S$. Thus, all coherent states, squeezed states, and thermal states become truncated to this finite-dimensional Hilbert space. Also, it is only necessary to consider an alphabet $\mathcal{X}$ that is finite because the input Hilbert space is finite (this follows from Caratheodory's theorem [28,36]). Applying Proposition 1 to the ensemble of the form in Eq. (31) in this truncated Hilbert space gives a quantum dynamic region which is strictly an inner bound to the region in Eqs. (28)–(30). As we let K grow without bound, the entropies given by Proposition 1 converge to the entropies in Eqs. (28)–(30). A similar argument applies to the private dynamic regions and the other regions throughout this paper. ∎

In order to obtain the full region, we take the union of all the above regions by varying the photon-number-sharing parameter λ from 0 to 1. When λ is one, we are dedicating all of the photons to quantum resources without the intent of sending any classical information. In the other case when λ is equal to zero, we are dedicating all of the photons to sending classical information without any intent to send quantum information. Figure 1 plots this triple-trade-off region for $\eta = \frac{3}{4}$ and $N_S = 100$.

B. Special cases of the quantum dynamic trade-off

A first special case of the quantum dynamic achievable rate region is the trade-off between classical and quantum communication (first explored by Devetak and Shor in Ref. [36]).

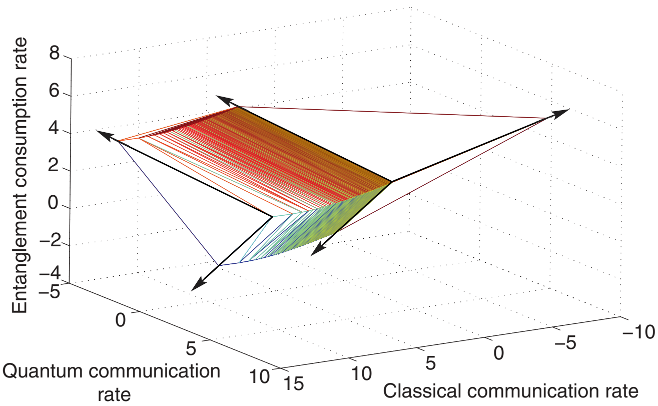

FIG. 1. (Color online) The full triple-trade-off region for the lossy bosonic channel with transmissivity $\eta = \frac{3}{4}$ and mean input photon number $N_S = 100$. Units for classical communication, quantum communication, and entanglement consumption are bits per channel use, qubits per channel use, and ebits per channel use, respectively.

The region in Eqs. (28)–(30) reduces to the following set of inequalities for this special case:

$$Q \leqslant g(\eta\lambda N_S) - g((1-\eta)\lambda N_S), \quad (40)$$

$$C + Q \leqslant g(\eta N_S) - g((1-\eta)\lambda N_S). \quad (41)$$

Figure 2(a) in the main text displays a plot of this region for a lossy bosonic channel with transmissivity $\eta = \frac{3}{4}$ and mean input photon number $N_S = 200$. Trade-off coding for this channel can give a dramatic improvement over a time-sharing strategy. More generally, Fig. 2(a) demonstrates that trade-off coding beats time sharing for all η such that $\frac{1}{2} < \eta < 1$ (there is no trade-off for $\eta \leqslant \frac{1}{2}$ because the quantum capacity vanishes for these values of η).

Another special case of the quantum dynamic capacity region is when the sender and receiver share prior entanglement and the sender would like to transmit classical information to the receiver (a trade-off first explored by Shor in Ref. [37]). The region in Eqs. (28)–(30) reduces to the following set of inequalities for this special case:

$$C \leqslant g(\lambda N_S) + g(\eta N_S) - g((1-\eta)\lambda N_S), \quad (42)$$

$$C \leqslant g(\eta N_S) - g((1-\eta)\lambda N_S) + E, \quad (43)$$

where we now take the convention that positive E corresponds to the consumption of shared entanglement. Figure 2(b) in the main text displays a plot of this region for the case where $\eta = \frac{3}{4}$ and $N_S = 200$. The figure demonstrates that trade-off coding can give a dramatic improvement over time sharing. More generally, Fig. 2(b) demonstrates that trade-off coding beats time sharing for all η such that $0 < \eta < 1$.

C. Limit of high mean input photon number

We now briefly describe what happens to the above special cases when the mean input photon number becomes high. We begin with the classical-quantum trade-off. Recall from Ref. [43] that the classical capacity of the lossy bosonic channel can be infinite if the input photon number is unlimited. But, the quantum capacity is fundamentally limited even if an infinite number of photons are available [43,46]. The threshold on quantum capacity for the lossy bosonic channel with transmissivity η is

$$\lim_{N_S\to\infty} g(\eta N_S) - g((1-\eta)N_S) = \ln(\eta) - \ln(1-\eta). \quad (44)$$

Let N_T denote the approximate number of photons needed to reach the above limit on quantum capacity. This limit has implications for trade-off coding. Given a large input photon number $N_S > N_T$, it is possible to exploit an amount N_T

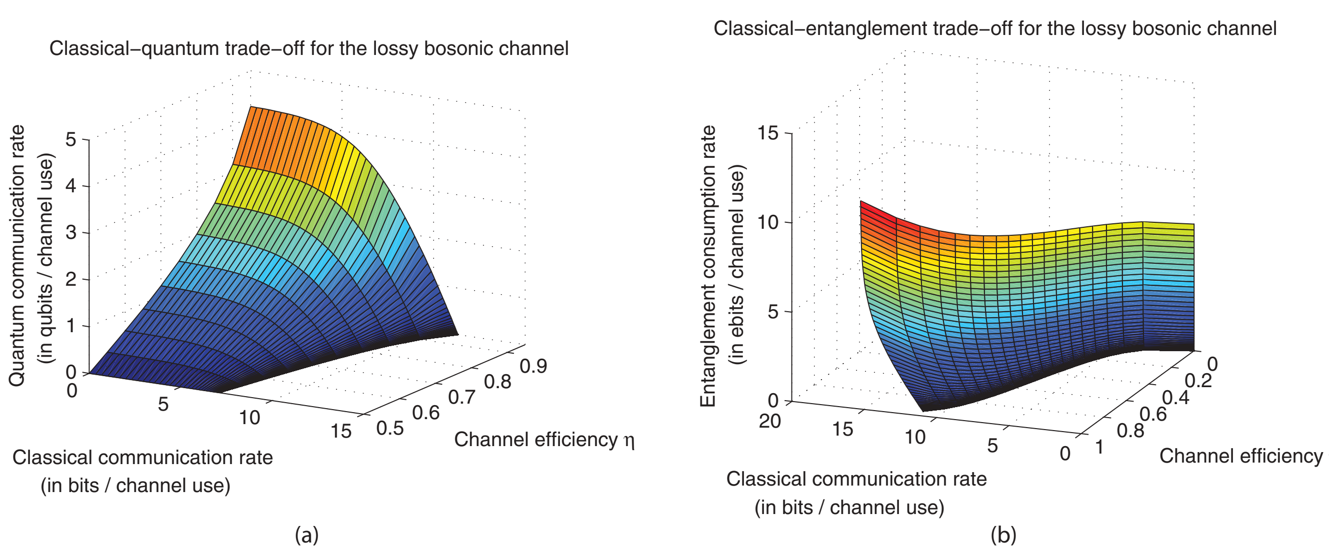

FIG. 2. (Color online) (a) The trade-off between classical and quantum communication for all $\eta \in (1/2,1)$, with the result that trade-off coding always beats time sharing by a significant margin. We assume that the mean input photon number $N_S = 50/(1-\eta)$ so that there are a sufficient number of photons to reach the quantum capacity of $\ln(\eta) - \ln(1-\eta)$ if the trade-off code dedicates all of the available photons to quantum communication. (b) The trade-off between entanglement-assisted and unassisted classical communication for all $\eta \in (0,1)$, with the result that trade-off coding always beats time sharing. For consistency with (a), we again assume that $N_S = 50/(1-\eta)$.

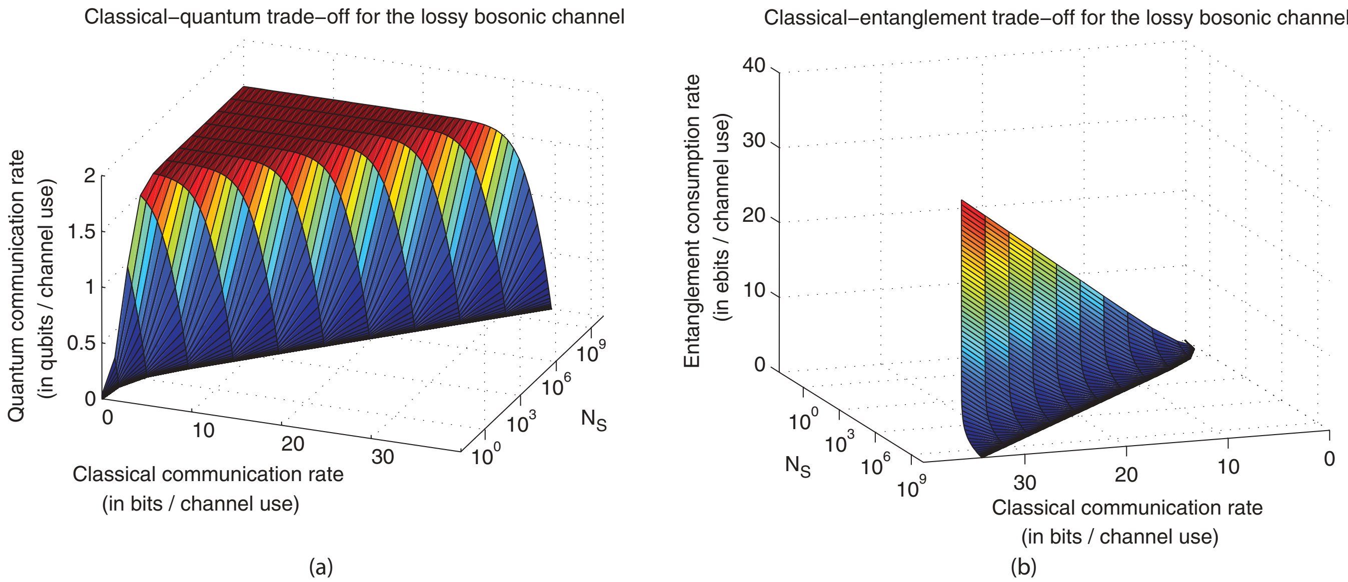

FIG. 3. (Color online) (a) The trade-off between classical and quantum communication for a lossy bosonic channel with transmissivity $\eta = \frac{3}{4}$ as the mean input photon number N_S increases on a logarithmic scale from 0.01 to 10^{10}. The quantum capacity can never be larger than $\ln(\eta) - \ln(1-\eta)$, but the classical capacity is unbounded as $N_S \to \infty$. Thus, the best option for a trade-off code is to abide by the rule of thumb given in the main text and dedicate only a small fraction $\lambda \approx 50/[(1-\eta)N_S]$ of the available photons to quantum resources. This ensures that the quantum data rate is near maximal while also maximizing the rate of classical communication. (b) The trade-off between entanglement-assisted and unassisted classical communication for the same lossy bosonic channel as N_S increases logarithmically from 0.01 to 10^{10}. Abiding by a similar rule of thumb and dedicating a fraction $\lambda \approx 50/[(1-\eta)N_S]$ of the available photons to shared entanglement ensures that the classical data rate is near maximal while minimizing the entanglement consumption rate. Observe that trade-off protocols operating at these near-maximal data rates given by the rule of thumb consume about the same amount of entanglement for all of the trade-off curves depicted.

for the quantum part of the transmission and $N_S - N_T$ for the classical part of the transmission, so that the classical part of the transmission can become arbitrarily large in the limit of infinite mean input photon number (this leads to our rule of thumb pointed out in the main text). Figure 3(a) depicts the classical-quantum trade-off for a lossy bosonic channel with $\eta = \frac{3}{4}$ as the mean input photon number N_S increases on a logarithmic scale from 0.01 to 10^{10}.

An interesting effect occurs with the trade-off between assisted and unassisted classical communication. In the limit of infinite photon number, the difference between the entanglement-assisted classical capacity and the classical capacity approaches $\ln[1/(1-\eta)]$:

$$\begin{aligned}
&\lim_{N_S\to\infty} g(N_S) + g(\eta N_S) - g((1-\eta)N_S) - g(\eta N_S) \\
&\quad = \lim_{N_S\to\infty} g(N_S) - g((1-\eta)N_S) \\
&\quad = \lim_{N_S\to\infty} \ln(N_S) - \ln[(1-\eta)N_S] = \ln[1/(1-\eta)].
\end{aligned}$$

Since both capacities diverge, this implies, in particular, that their ratio approaches one in the same limit. This is an indication that entanglement becomes less useful in the high-photon-number limit. Figure 3(b) depicts the classical-entanglement trade-off for a lossy bosonic channel with transmissivity $\eta = \frac{3}{4}$ and mean input photon number N_S increasing on a logarithmic scale from 0.01 to 10^{10}.

D. "Rules of thumb" for trade-off coding

Here, we derive two propositions to support the claims in the main text regarding two different "rules of thumb" for trade-off coding.

Lemma 4. The thermal entropy function $g(N)$ admits the following power series expansion whenever $N \geqslant 1$:

$$g(N) = \ln(N) + 1 + \sum_{j=1}^{\infty} \frac{(-1)^{j+1}}{j(j+1)N^j}.$$

Proof. Consider the following chain of equalities:

$$\begin{aligned}
g(N) &= (N+1)\ln(N+1) - N\ln(N) \\
&= (N+1)\ln\left(1+\frac{1}{N}\right) - 1 + \ln(N) + 1. \quad (45)
\end{aligned}$$

Now consider the following Taylor series expansion of $\ln(1 + 1/N)$ which is valid for all $N \geqslant 1$:

$$\ln\left(1+\frac{1}{N}\right) = \sum_{j=1}^{\infty} \frac{(-1)^{j+1}}{jN^j}. \quad (46)$$

We can use this expansion to manipulate the expression $(N+1)\ln(1+1/N) - 1$:

$$(N+1)\left(\sum_{j=1}^{\infty} \frac{(-1)^{j+1}}{jN^j}\right) - 1 = \sum_{j=1}^{\infty} \frac{(-1)^{j+1}}{j(j+1)N^j}. \quad (47)$$

Combining Eqs. (45)–(47) gives the statement of the lemma. ■

Proposition 5. A lower bound on the achievable rate for the lossy bosonic channel is as follows:

$$g(\eta N_S) - g((1-\eta)N_S) \geqslant \ln(\eta) - \ln(1-\eta) - \frac{1}{\eta(1-\eta)N_S},$$

provided that $(1-\eta)N_S \geqslant 2$ and $\eta \geqslant 1-\eta$. Thus, in a trade-off coding strategy, it suffices to choose the photon-number-sharing parameter $\lambda = 1/[\eta(1-\eta)\epsilon N_S \ln 2]$ whenever $\lambda(1-\eta)N_S \geqslant 2$ and $\eta \geqslant 1-\eta$ in order to be within ϵ bits of the quantum capacity (expressed in units of qubits per channel use).

Proof. The first step is to use the expansion from Lemma 4. Substituting in gives

$$\begin{aligned} g(\eta N_S) &- g((1-\eta)N_S) \\ &\geqslant \ln\eta - \ln(1-\eta) + \frac{1}{2\eta N_S} - \frac{1}{6\eta^2 N_S^2} + \cdots \\ &\quad - \frac{1}{2(1-\eta)N_S} + \frac{1}{6(1-\eta)^2 N_S^2} - \cdots \\ &\geqslant \ln\eta - \ln(1-\eta) - \frac{2\eta-1}{2\eta(1-\eta)N_S} \\ &\quad - \sum_{j=2}^{\infty} \frac{1}{j(j+1)} \frac{1}{[(1-\eta)N_S]^j}, \end{aligned}$$

where in the last line the order $1/N_S$ term is exact. The error term was estimated by keeping only the negative terms in the expansion for orders $1/N_S^2$ and higher, in addition to applying the inequality $1-\eta \leqslant \eta$. Let $R = (1-\eta)N_S$. We can then bound

$$\sum_{j=2}^{\infty} \frac{1}{j(j+1)R^j} \leqslant \frac{1}{6}\sum_{j=2}^{\infty} \frac{1}{R^j} = \frac{1}{6(R^2-R)}$$

using the formula for the sum of a geometric series. So, if $R = (1-\eta)N_S \geqslant 2$, then $R \leqslant R^2/2$ and we get that

$$\begin{aligned} g(\eta N_S) &- g((1-\eta)N_S) \\ &\geqslant \ln\eta - \ln(1-\eta) - \frac{2\eta-1}{2\eta(1-\eta)N_S} - \frac{1}{3}\frac{1}{(1-\eta)N_S} \\ &= \ln\eta - \ln(1-\eta) - \frac{8\eta/3-1}{2\eta(1-\eta)N_S} \\ &\geqslant \ln\eta - \ln(1-\eta) - \frac{1}{\eta(1-\eta)N_S}, \end{aligned}$$

using in the last line that $\eta < 1$.

The statement in the proposition about trade-off coding follows by analyzing the above bound. An achievable rate for quantum data transmission with a trade-off coding strategy is $g(\lambda\eta N_S) - g(\lambda(1-\eta)N_S)$, and the above development gives the following lower bound on this achievable rate (in units of qubits per channel use):

$$\log_2(\eta) - \log_2(1-\eta) - \frac{1}{\eta(1-\eta)\lambda N_S \ln 2}.$$

Thus, if we would like to be within ϵ bits of the maximum quantum capacity $\log_2(\eta) - \log_2(1-\eta)$, then it suffices to choose the photon-number-sharing parameter λ as given in the statement of the proposition. ■

Proposition 6. An upper bound on the difference between the entanglement-assisted classical capacity with maximal entanglement and that for limited entanglement trade-off coding is as follows:

$$\frac{5}{6\lambda N_S(1-\eta)},$$

provided that $\lambda(1-\eta)N_S \geqslant 2$. Thus, in order to be within ϵ bits of the entanglement-assisted classical capacity, it suffices to choose the photon-number-sharing parameter $\lambda = 5/[6\epsilon N_S(1-\eta)\ln 2]$ whenever $\lambda(1-\eta)N_S \geqslant 2$.

Proof. Consider the difference between the entanglement-assisted classical capacity $g(N_S) + g(\eta N_S) - g((1-\eta)N_S)$ and the limited entanglement classical data rate $g(\lambda N_S) + g(\eta N_S) - g((1-\eta)\lambda N_S)$:

$$\begin{aligned} g(N_S) &+ g(\eta N_S) - g((1-\eta)N_S) \\ &\quad - [g(\lambda N_S) + g(\eta N_S) - g((1-\eta)\lambda N_S)] \\ &= g(N_S) - g(\lambda N_S) - [g((1-\eta)N_S) - g((1-\eta)\lambda N_S)] \\ &= \sum_{j=1}^{\infty} \frac{(-1)^{j+1}}{j(j+1)}\left[\frac{1}{N_S^j} - \frac{1}{(\lambda N_S)^j}\right] \\ &\quad - \sum_{j=1}^{\infty} \frac{(-1)^{j+1}}{j\,(j+1)\,N_S^j}\left[\frac{1}{(1-\eta)^j} - \frac{1}{[\lambda(1-\eta)]^j}\right] \\ &= \frac{1}{2N_S}[1 - \lambda^{-1} - (1-\eta)^{-1} + [\lambda(1-\eta)]^{-1}] \\ &\quad + \sum_{j=2}^{\infty} \frac{(-1)^{j+1}}{j(j+1)}\left[\frac{1}{N_S^j} - \frac{1}{(\lambda N_S)^j}\right] \\ &\quad - \sum_{j=2}^{\infty} \frac{(-1)^{j+1}}{j(j+1)N_S^j}\left[\frac{1}{(1-\eta)^j} - \frac{1}{[\lambda(1-\eta)]^j}\right]. \end{aligned}$$

The second equality follows by expanding the thermal entropy functions with Lemma 4 and by canceling terms. The third equality follows by taking out the first term in the summation. Continuing,

$$\begin{aligned} &\leqslant \frac{1}{2N_S}\left(\frac{\eta}{1-\eta}\right)\left(\frac{1-\lambda}{\lambda}\right) \\ &\quad + \sum_{j=2}^{\infty} \frac{2}{j\,(j+1)\,[\lambda(1-\eta)N_S]^j} \\ &\leqslant \frac{1}{2\lambda N_S(1-\eta)} + \sum_{j=2}^{\infty} \frac{2}{j\,(j+1)\,[\lambda(1-\eta)N_S]^j}. \end{aligned}$$

The first inequality follows by realizing that $1 - \lambda^{-1} - (1-\eta)^{-1} + [\lambda(1-\eta)]^{-1} = [\eta/(1-\eta)](1-\lambda)/\lambda$, by keeping only the positive terms in the series, and by realizing that $\lambda(1-\eta)N_S \leqslant (1-\eta)N_S$, $\lambda(1-\eta)N_S \leqslant \lambda N_S$, and $\lambda(1-\eta)N_S \leqslant N_S$. The next inequality follows because $\eta, 1-\lambda \leqslant 1$.

Continuing,

$$\leqslant \frac{1}{2\lambda N_S(1-\eta)} + \frac{2}{6}\sum_{j=2}^{\infty}\frac{1}{[\lambda(1-\eta)N_S]^j}$$
$$= \frac{1}{2\lambda N_S(1-\eta)} + \frac{2}{6}\left(\frac{1}{[\lambda(1-\eta)N_S]^2-\lambda(1-\eta)N_S}\right)$$
$$\leqslant \frac{1}{2\lambda N_S(1-\eta)} + \frac{2}{6}\frac{1}{\lambda(1-\eta)N_S}$$
$$= \frac{5}{6\lambda N_S(1-\eta)}.$$

The first inequality follows because $1/j(j+1) \leqslant \frac{1}{6}$ for $j \geqslant 3$. The first equality follows from the formula for a geometric series. The second inequality is true whenever $\lambda(1-\eta)N_S \geqslant 2$, and the final equality follows from simple addition.

The statement about trade-off coding follows from the above bound on the difference between the entanglement-assisted classical capacity and the limited entanglement data rate. If we would like the error to be within ϵ bits of capacity, then the bound in the statement of the proposition should hold. ■

E. Private dynamic achievable rate region

The proof of the theorem below justifies achievability of the region in Eq. (3) in the main text.

Theorem 7. An achievable private dynamic region for a lossy bosonic channel with transmissivity η is the union of regions of the form

$$R + P \leqslant g(\eta N_S), \tag{48}$$
$$P + S \leqslant g(\lambda\eta N_S) - g(\lambda(1-\eta)N_S), \tag{49}$$
$$R + P + S \leqslant g(\eta N_S) - g(\lambda(1-\eta)N_S), \tag{50}$$

where $\lambda \in [0,1]$ is a photon-number-sharing parameter and $g(N)$ is defined in Eq. (2).

Proof. This channel is degradable whenever $\eta \geqslant \frac{1}{2}$ [40], and antidegradable otherwise. For simplicity, we study the case where the channel is degradable (Lemma 5 of Ref. [31] demonstrates that the region is somewhat trivial for the case of an antidegradable channel). We choose the input ensemble to be a mixture of coherent states

$$\{p_{\overline{\lambda}N_S}(\alpha)p_{\lambda N_S}(\beta), |\alpha+\beta\rangle\}, \tag{51}$$

where the distributions $p_{\overline{\lambda}N_S}(\alpha)$ and $p_{\lambda N_S}(\beta)$ are isotropic Gaussian priors of the form in Eq. (32). The parameter λ is again a photon-number-sharing parameter where $\overline{\lambda} = 1-\lambda$ is the fraction of photons that the code dedicates to public resources and λ is the fraction that it dedicates to private resources. Let θ_α denote the state resulting from averaging over the variable β:

$$\theta_\alpha \equiv \int d\beta\ p_{\lambda N_S}(\beta)\ |\alpha+\beta\rangle\langle\alpha+\beta| = D(\alpha)\theta D^\dagger(\alpha), \tag{52}$$

where θ is a thermal state with mean photon number λN_S. Let $\overline{\theta}$ denote the state resulting from averaging over all states in the ensemble:

$$\overline{\theta} \equiv \iint d\alpha\ d\beta\ p_{\overline{\lambda}N_S}(\alpha)p_{\lambda N_S}(\beta)\ |\alpha+\beta\rangle\langle\alpha+\beta|$$
$$= \int d\alpha\ p_{\overline{\lambda}N_S}(\alpha)\ D(\alpha)\theta D^\dagger(\alpha). \tag{53}$$

Observe that $\overline{\theta}$ is just a thermal state with mean photon number N_S, so that the mean number of photons entering the channel meets the constraint of N_S.

We remark on the two extreme cases of the ensemble in Eq. (51). If the photon-number-sharing parameter $\lambda = 0$, then the coding scheme devotes all of its photons to public classical communication. The ensemble is an isotropic distribution of coherent states, which is the ensemble needed to achieve the capacity of the lossy bosonic channel for public classical communication [6]. If the photon-number-sharing parameter $\lambda = 1$, then the coding scheme devotes all of its photons to private classical communication. The ensemble is again an isotropic mixture of coherent states, which is the ensemble needed to achieve the private classical capacity of the lossy bosonic channel [40], up to the aforementioned minimum-output entropy conjecture [22,23].

The four entropies in Eqs. (22)–(25) become the following four entropies for our case:

$$H(\mathcal{N}(\overline{\theta})), \tag{54}$$
$$\iint d\alpha\ d\beta\ p_{\overline{\lambda}N_S}(\alpha)p_{(\lambda)N_S}(\beta)\ H(\mathcal{N}(|\alpha+\beta\rangle\langle\alpha+\beta|)), \tag{55}$$
$$\int d\alpha\ p_{\overline{\lambda}N_S}(\alpha)\ H(\mathcal{N}(\theta_\alpha)), \tag{56}$$
$$\int d\alpha\ p_{\overline{\lambda}N_S}(\alpha)\ H(\mathcal{N}^c(\theta_\alpha)). \tag{57}$$

The first entropy is equal to the entropy of an attenuated thermal state:

$$H(\mathcal{N}(\overline{\theta})) = g(\eta N_S).$$

The second entropy is equal to zero because a lossy bosonic channel does not change the purity of a coherent state. We calculate the final two entropies in the same way as we did in Eqs. (38) and (39), respectively. ■

Figure 4 plots the private dynamic capacity region for a lossy bosonic channel with transmissivity $\eta = \frac{3}{4}$ and the mean input photon number $N_S = 100$.

F. Special case of the private dynamic region

An interesting special case of the private dynamic region is the trade-off between public and private classical communication. Lemma 3 of Ref. [31] proves that the classical-quantum trade-off from Sec. III B is the same as the public-private trade-off whenever the channel is degradable (recall that the lossy bosonic channel is degradable whenever $\eta \geqslant \frac{1}{2}$). Thus, the formulas in Eqs. (40) and (41) characterize this trade-off as

$$P \leqslant g\,(\eta\lambda N_S) - g((1-\eta)\lambda N_S), \tag{58}$$
$$R + P \leqslant g(\eta N_S) - g((1-\eta)\lambda N_S) \tag{59}$$

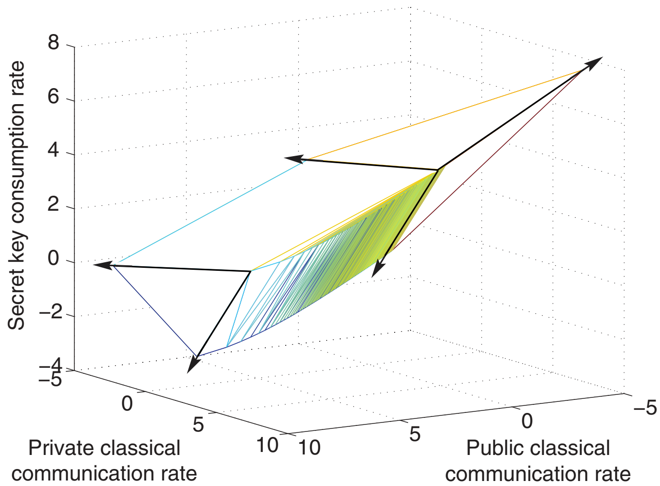

FIG. 4. (Color online) The private dynamic capacity region for a lossy bosonic channel with transmissivity $\eta = \frac{3}{4}$ and mean input photon number $N_S = 100$. The units for each kind of resource are bits per channel use.

and Fig. 2(a) serves as a plot of it. We should note that the trade-off between public classical communication and secret-key generation is the same as that between public and private classical communication, found simply by replacing P with S in the above formulas.

G. Converse for the quantum dynamic region

We now prove that the characterization in Eqs. (28)–(30) is the capacity region corresponding to the trade-off between classical communication, quantum communication, and entanglement. Our converse proof exploits the same ideas used in Refs. [24,25] to prove optimality of the bosonic broadcast channel region and, as such, it is optimal only if the minimum-output entropy conjecture is true (in particular, the second strong version from Refs. [24,25]). Some evidence has been collected suggesting that this conjecture should be true, but a full proof remains elusive. References [24,25], however, have shown that the conjecture is true if the input states are restricted to be Gaussian, and thus our region is optimal if the input states are restricted to be Gaussian.

Proof. Proposition 1 states that the regularization of the region in Eqs. (3)–(5) is the quantum dynamic capacity region for any quantum channel. We prove here that the region in Eqs. (28)–(30) is equivalent to the capacity region for a lossy bosonic channel $\mathcal{N}$ with transmissivity parameter $\eta > \frac{1}{2}$ and mean input photon number N_S, up to a minimum-output entropy conjecture. We do so by proving the following upper bounds:

$$\sum_x p_X(x) H(\rho_x) \leqslant n g(\lambda N_S), \tag{60}$$

$$H(\mathcal{N}^{\otimes n}(\rho)) \leqslant n g(\eta N_S), \tag{61}$$

$$\sum_x p_X(x) H(\mathcal{N}^{\otimes n}(\rho_x)) \leqslant n g\left(\eta \lambda N_S\right), \tag{62}$$

and the following lower bound:

$$\sum_x p_X(x) H((\mathcal{N}^c)^{\otimes n}(\rho_x)) \geqslant n g((1-\eta)\lambda N_S), \tag{63}$$

so that for all n-letter ensembles $\{p_X(x),\rho_x\}$ with $\rho_x \in \mathcal{B}(\mathcal{H}^{\otimes n})$ and $\rho \equiv \sum_x p_X(x)\rho_x$, there exists some $\lambda \in [0,1]$ such that the above bounds hold. The above bounds immediately imply that the region in Eqs. (28)–(30) is the quantum dynamic capacity region.

The second bound in Eq. (61) follows because the quantum entropy is subadditive and the entropy of a thermal state gives the maximum entropy for a bosonic state with mean photon number ηN_S (if the input mean photon number is N_S, then the output mean photon number is ηN_S for a lossy bosonic channel with transmissivity η).

Recall that the thermal entropy function $g(x)$ is monotonically increasing and concave in its input argument. The proof from Refs. [24,25] makes use of these facts and we can do so as well. Let us begin by bounding the term in Eq. (60). Supposing that the mean number of photons for the jth symbol of ρ_x is N_{S,x_j}, we have the following bound:

$$\begin{aligned} 0 &\leqslant H(\rho_x) && (64a)\\ &\leqslant \sum_{j=1}^{n} H\left(\rho_x^j\right) && (64b)\\ &\leqslant \sum_{j=1}^{n} g\left(N_{S,x_j}\right) && (64c)\\ &\leqslant n g(N_{S,x}), && (64d)\end{aligned}$$

where $N_{S,x} \equiv \sum_{j=1}^{n} \frac{1}{n} N_{S,x_j}$. The second inequality exploits the subadditivity of quantum entropy, the third inequality exploits the fact that the maximum quantum entropy of a bosonic system with mean photon number N is $g(N)$, and the last inequality exploits concavity of $g(x)$. Thus, for all $x \in \mathcal{X}$, there exists some $\lambda'_x \in [0,1]$ such that

$$H(\rho_x) = n g(\lambda'_x N_{S,x}) \tag{65}$$

because $g(x)$ is a monotonically increasing function of x for $x \geqslant 0$. Also, we have that

$$\begin{aligned} 0 &\leqslant \sum_x p_X(x) H(\rho_x) && (66a)\\ &\leqslant H(\rho) && (66b)\\ &\leqslant n g(N_S), && (66c)\end{aligned}$$

where the second inequality follows from concavity of quantum entropy, and the last follows from the fact that the maximum entropy for a bosonic state of mean photon number N is $g(N)$. Thus, there exists some $\lambda' \in [0,1]$ such that

$$\sum_x p_X(x) H(\rho_x) = n g(\lambda' N_S) \tag{67}$$

because $g(x)$ is a monotonically increasing function of x for $x \geqslant 0$. We then have that

$$\sum_x p_X(x) g(\lambda'_x N_{S,x}) = g(\lambda' N_S) \tag{68}$$

by combining Eqs. (65) and (67). Alice can simulate Bob's state by passing her system through one input port of a beam-splitter with transmissivity η while passing the vacuum through the other port. Assuming the truth of Strong Conjecture 2 from Refs. [24,25], we have that

$$H(\mathcal{N}^{\otimes n}(\rho_x)) \geqslant n g(\lambda'_x \eta N_{S,x}).$$

(We should point out that Strong Conjecture 2 holds if the entropy photon-number inequality is true [25].) Using the relation in Eq. (68) and concavity of $g(x)$, we can apply a slightly modified version of Corollary A.4 from Guha's thesis [25] to show that

$$\sum_x p_X(x) g(\lambda'_x \eta N_{S,x}) \geqslant g(\lambda' \eta N_S),$$

giving the lower bound

$$\sum_x p_X(x) H(\mathcal{N}^{\otimes n}(\rho_x)) \geqslant g(\lambda' \eta N_S). \quad (69)$$

(Corollary A.4 of Ref. [25] is stated for a uniform distribution, but the argument only relies on a concavity argument and thus applies to an arbitrary distribution.)

With a similar development as in Eqs. (64a)–(64d), we can bound the entropy $H(\mathcal{N}^{\otimes n}(\rho_x))$ because the mean number of photons for the jth symbol of $\mathcal{N}^{\otimes n}(\rho_x)$ is $\eta N_{S,x_j}$:

$$0 \leqslant H(\mathcal{N}^{\otimes n}(\rho_x)) \leqslant \sum_{j=1}^{n} H\big(\mathcal{N}^{\otimes n}(\rho_x^j)\big) \leqslant \sum_{j=1}^{n} g\big(\eta N_{S,x_j}\big) \leqslant n g(\eta N_{S,x}).$$

Thus, for all $x \in \mathcal{X}$, there exists some $\lambda_x \in [0,1]$ such that

$$H(\mathcal{N}^{\otimes n}(\rho_x)) = n g(\lambda_x \eta N_{S,x}) \quad (70)$$

because $g(x)$ is a monotonically increasing function of x for $x \geqslant 0$. We also have that

$$0 \leqslant \sum_x p_X(x) H(\mathcal{N}^{\otimes n}(\rho_x)) \leqslant H(\mathcal{N}^{\otimes n}(\rho)) \leqslant n g(\eta N_S),$$

for reasons similar to those in Eqs. (66a)–(66c). Thus, there exists some $\lambda \in [0,1]$ such that

$$\sum_x p_X(x) H(\mathcal{N}^{\otimes n}(\rho_x)) = n g(\lambda \eta N_S) \quad (71)$$

because $g(x)$ is a monotonically increasing function of x for $x \geqslant 0$. This gives us our third bound in Eq. (62). Combining Eqs. (71) and (69) gives us the following bound:

$$g(\lambda \eta N_S) \geqslant g(\lambda' \eta N_S),$$

which in turn implies that

$$g(\lambda N_S) \geqslant g(\lambda' N_S)$$

because $g(x)$ and its inverse $g^{-1}(y)$ (defined on positive reals) are both monotonically increasing. This gives us our first bound in Eq. (60) by combining with Eq. (67).

Combining Eqs. (70) and (71), we have

$$\sum_x p_X(x) n g(\lambda_x N_{S,x}) = n g(\eta \lambda N_S).$$

We are assuming that the lossy bosonic channel has $\eta \geqslant \frac{1}{2}$ so that it is degradable and Bob can simulate Eve's state by passing his state through one input port of a beamsplitter with transmissivity $(1-\eta)/\eta$ while passing the vacuum through the other port. Assuming the truth of Strong Conjecture 2 from Refs. [24,25], we have that

$$H((\mathcal{N}^c)^{\otimes n}(\rho_x)) \geqslant n g(\lambda_x (1-\eta) N_{S,x}).$$

Using the above relation, concavity of $g(x)$, and the fact that $\eta \geqslant \frac{1}{2}$, we can apply the modified version of Corollary A.4 from Ref. [25] to show that

$$\sum_x p_X(x) g(\lambda_x (1-\eta) N_{S,x}) \geqslant g(\lambda (1-\eta) N_S).$$

This gives our final bound in Eq. (63):

$$\sum_x p_X(x) H((\mathcal{N}^c)^{\otimes n}(\rho_x)) \geqslant \sum_x p_X(x) g(\lambda_x (1-\eta) N_{S,x}) \geqslant g(\lambda(1-\eta) N_S). \quad ■$$

1. Special cases of the quantum dynamic region

A similar proof can be used to show that our characterization of the classical-entanglement (CE) trade-off curve is optimal for all $\eta \in [0,1]$ and that our characterization of the classical-quantum (CQ) trade-off curve is optimal for all $\eta \in [1/2,1]$. Of course, both proofs require Strong Conjecture 2 from Refs. [24,25] (which holds if the entropy photon-number inequality is true).

We also can completely characterize the trade-off between quantum communication and entanglement consumption for a lossy bosonic channel with $\eta \geqslant 1/2$.

Theorem 8. The trade-off between entanglement assistance and quantum communication (when $C = 0$, $Q \geqslant 0$, and $E \leqslant 0$) given by Eqs. (28)–(30) is optimal for the lossy bosonic channel with $\eta \geqslant 1/2$.

Proof. Recall from Ref. [47] that the characterization of the entanglement-assisted quantum capacity region for any channel $\mathcal{N}$ is the regularization the union of the following regions:

$$2Q \leqslant I(A;B)_\rho, \quad Q \leqslant I(A\rangle B)_\rho + |E|,$$

where the entropies are with respect to a state $\rho^{AB} \equiv \mathcal{N}^{A'\to B}(\phi^{AA'})$, the union of the above regions is over pure, bipartite states $\phi^{AA'}$, Q is the rate of quantum communication, and E is the rate of entanglement consumption. Characterizing the boundary of the region is equivalent to optimizing the following function [47]:

$$\max_\rho I(A;B)_\rho + \mu I(A\rangle B)_\rho,$$

where μ is a positive number playing the role of a Lagrange multiplier. We can rewrite the above function in the following form:

$$\max_\rho H(A)_\rho + (\mu+1) I(A\rangle B)_\rho$$

because $I(A;B) = H(A) + I(A\rangle B)$. It is straightforward to show that the above formula is additive for degradable channels [36], and furthermore, we can rewrite the coherent information $I(A\rangle B)_\rho$ as a conditional entropy $H(F|E)$, whenever the channel is degradable [36] (let F be the environment of the degrading map). Then, from the extremality of Gaussian states for entropy and conditional entropy [48,49], it suffices to perform the above optimization over only Gaussian states. Recall that $I(A\rangle B) = H(B) - H(E)$ where E is the environment of the channel. For a lossy bosonic channel with $\eta \geqslant \frac{1}{2}$ with mean input photon number N_S, the following bounds hold:

$$0 \leqslant H(A)_\rho \leqslant g(N_S),$$
$$0 \leqslant H(B)_\rho \leqslant g(\eta N_S).$$

Thus, there exist some $\lambda',\lambda \in [0,1]$ such that $H(A)_\rho = g(\lambda' N_S)$ and $H(B)_\rho = g(\eta\lambda N_S)$ from the monotonicity of $g(x)$. Also, we have that $g(\eta\lambda N_S) \geqslant g(\eta\lambda' N_S)$ from the same reasoning as in the above proof, although Strong Conjecture 2 from Refs. [24,25] is known to hold for Gaussian states. This then implies that $g(\lambda N_S) \geqslant g(\lambda' N_S)$ by the same reasoning as in the above proof. Also, we have the following lower bound from Strong Conjecture 2 (which holds for Gaussian states):

$$H(E)_\rho \geqslant g((1-\eta)\lambda N_S),$$

by the same reasoning as in the above proof. Thus, we have the following upper bound for a particular state ρ:

$$H(A)_\rho + (\mu+1)I(A\rangle B)_\rho \leqslant g(\eta\lambda N_S) + (\mu+1)[g(\eta\lambda N_S) - g((1-\eta)\lambda N_S)].$$

It is straightforward to show that $g(\eta x) - g((1-\eta)x)$ is a monotonically increasing function in x whenever $\eta \geqslant \frac{1}{2}$, by considering that $g(\eta x) = g((1-\eta)x) = 0$ for $x = 0$, $g(\eta x) \geqslant g((1-\eta)x)$, and $\frac{\partial}{\partial x} g(\eta x) \geqslant \frac{\partial}{\partial x} g((1-\eta)x)$ whenever $\eta \geqslant \frac{1}{2}$. Thus, we obtain our final upper bound by setting $\lambda = 1$. These rates are achievable simply taking the input state $\phi^{A'}$ to be thermal with mean photon number N_S. ■

H. Converse for the private dynamic region

We can prove the converse for the private dynamic capacity region similarly to how we did for the quantum dynamic capacity region. Proposition 2 states that the regularization of the region in Eqs. (19)–(21) is equivalent to the private dynamic capacity region. We prove that the region in Eqs. (48)–(50) is equivalent to the capacity region for a lossy bosonic channel with transmissivity parameter $\eta > \frac{1}{2}$ and mean input photon number N_S, up to a minimum-output entropy conjecture. We do so by proving the following upper bounds:

$$H(\mathcal{N}^{\otimes n}(\rho)) \leqslant n g(\eta N_S), \tag{72}$$

$$\sum_x p_X(x) H(\mathcal{N}^{\otimes n}(\rho_x)) \leqslant n g(\eta\lambda N_S), \tag{73}$$

and the following lower bounds (the first up to the minimum-output entropy conjecture):

$$\sum_x p_X(x) H((\mathcal{N}^c)^{\otimes n}(\rho_x)) \geqslant n g((1-\eta)\lambda N_S),$$

$$\sum_{x,y} p(x)p(y|x) H(\mathcal{N}^{\otimes n}(\rho_{x,y})) \geqslant 0 \tag{74}$$

so that for all n-letter ensembles $\{p_X(x)p_{Y|X}(y|x),\rho_{x,y}\}$ with $\rho_{x,y} \in \mathcal{B}(\mathcal{H}^{\otimes n})$, $\rho_x \equiv \sum_y p_{Y|X}(y|x)\rho_{x,y}$, and $\rho \equiv \sum_x p_X(x)\rho_x$, there exists some $\lambda \in [0,1]$ such that the above bounds hold. The above bounds immediately imply that the region in Eqs. (48)–(50) is the private dynamic capacity region of the lossy bosonic channel.

Proof. The last bound in Eq. (74) follows simply because the quantum entropy is always positive. The other bounds follow by the same method given in the converse of the quantum dynamic capacity region for the lossy bosonic channel. ■

IV. THERMAL-NOISE CHANNEL

The thermal-noise channel is the same map as in Eqs. (26) and (27), with the exception that the environment is in a thermal state with mean photon number N_B.

A. Quantum dynamic region

Theorem 9. An achievable quantum dynamic region for the thermal-noise channel with transmissivity η and mean thermal photon number N_B is as follows:

$$C + 2Q \leqslant g(\lambda N_S) + g(\eta N_S + (1-\eta)N_B) - g_E^\eta(\lambda,N_S,N_B),$$
$$Q + E \leqslant g(\eta\lambda N_S + (1-\eta)N_B) - g_E^\eta(\lambda,N_S,N_B),$$
$$C + Q + E \leqslant g(\eta N_S + (1-\eta)N_B) - g_E^\eta(\lambda,N_S,N_B),$$

where $\lambda \in [0,1]$ is a photon-number-sharing parameter, $g(N)$ is defined in Eq. (2), and

$$g_E^\eta(\lambda,N_S,N_B) \equiv g([D + \lambda(1-\eta)N_S - (1-\eta)N_B - 1]/2) + g([D - \lambda(1-\eta)N_S + (1-\eta)N_B - 1]/2),$$
$$D^2 \equiv [\lambda(1+\eta)N_S + (1-\eta)N_B + 1]^2 - 4\eta\lambda N_S(\lambda N_S + 1).$$

Proof. We use the same coding strategy as in Eq. (31) and then simply need to calculate the four entropies in Eqs. (34)–(37) for this case. The average output state is a thermal state with mean number of photons $\eta N_S + (1-\eta)N_B$, implying that the first entropy in Eq. (34) is

$$H(\mathcal{N}(\overline{\theta})) = g(\eta N_S + (1-\eta)N_B).$$

The second entropy in Eq. (35) is the same as before because it is the entropy of the half of the state not transmitted through the channel:

$$\int d\alpha\ p_{\overline{\lambda}N_S}(\alpha)\ H(D(\alpha)\theta D^\dagger(\alpha)) = g(\lambda N_S).$$

The state of the output conditioned on the displacement operator applied is a thermal state with mean photon number $\eta\lambda N_S + (1-\eta)N_B$. Thus, the third entropy in Eq. (36) is

$$\int d\alpha\ p_{\overline{\lambda}N_S}(\alpha)\ H(\mathcal{N}(D(\alpha)\theta D^\dagger(\alpha))) = g(\eta\lambda N_S + (1-\eta)N_B).$$

We calculate the fourth entropy in Eq. (37) in a different way, along the lines presented in Refs. [43,45]. The displacement operator does not affect the correlation matrix of the two-mode squeezed state, and thus the entropy of this state does not change under such a transformation. In this case, the entropy is

$$g_E^\eta(\lambda,N_S,N_B) \equiv g([D + \lambda(1-\eta)N_S - (1-\eta)N_B - 1]/2) + g([D - \lambda(1-\eta)N_S + (1-\eta)N_B - 1]/2), \tag{75}$$

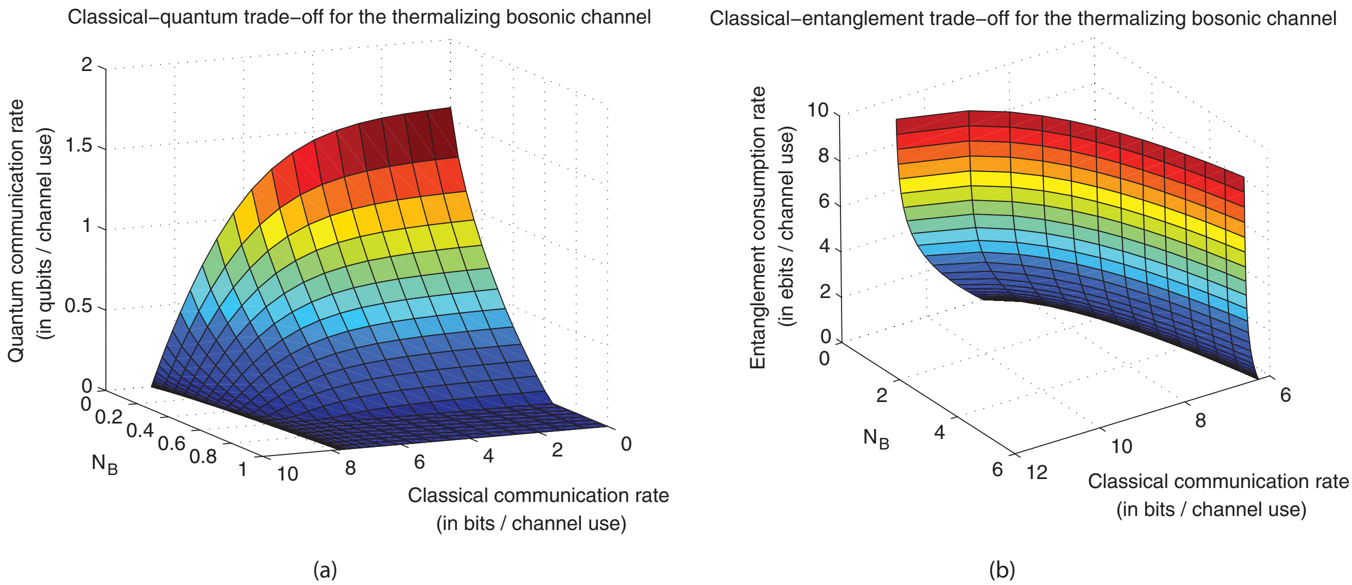

FIG. 5. (Color online) This figure displays the effect of increasing thermal noise (parametrized by N_B) on the trade-off between (a) classical and quantum communication and (b) entanglement-assisted and unassisted classical communication. We can not say whether any points in these regions are optimal because the capacity of the thermal channel is unknown (though, they are known if the minimum-output entropy conjecture is true [22,23]).

where

$$D^2 \equiv [\lambda\,(1+\eta)\,N_S + (1-\eta)N_B + 1]^2 - 4\eta\lambda N_S\,(\lambda N_S + 1)\,.$$

Plugging in the entropies gives us the statement of the proposition. ■

The trade-off region for classical and quantum communication is

$$Q \leqslant g(\eta\,(\lambda)\,N_S + (1-\eta)N_B) - g_E^{\eta}(\lambda, N_S, N_B), \quad (76)$$

$$C + Q \leqslant g(\eta N_S + (1-\eta)N_B) - g_E^{\eta}(\lambda, N_S, N_B). \quad (77)$$

The trade-off region for assisted and unassisted classical communication is

$$C \leqslant g((\lambda)N_S) + g(\eta N_S + (1-\eta)N_B) - g_E^{\eta}(\lambda, N_S, N_B),$$
$$C \leqslant g(\eta N_S + (1-\eta)N_B) - g_E^{\eta}(\lambda, N_S, N_B) + E,$$

where above our convention changes so that positive E corresponds to the consumption of entanglement. Figure 5(a) depicts the trade-off between classical and quantum communication for a thermal-noise channel, and Fig. 5(b) depicts the trade-off between assisted and unassisted classical communication.

B. Private dynamic region

Theorem 10. An achievable private dynamic region for the thermal-noise channel with transmissivity η and mean thermal photon number N_B is as follows:

$$R + P \leqslant g(\eta N_S + (1-\eta)N_B) - g((1-\eta)N_B),$$
$$P + S \leqslant g(\eta\lambda N_S + (1-\eta)N_B) - g_E^{\eta}(\lambda, N_S, N_B),$$
$$R + P + S \leqslant g(\eta N_S + (1-\eta)N_B) - g_E^{\eta}(\lambda, N_S, N_B),$$

where $\lambda \in [0,1]$ is a photon-number-sharing parameter, $g(N)$ is defined in Eq. (2), and g_E^{η} is defined in Eq. (75).

Proof. We can obtain an expression for a private dynamic achievable rate region of the thermal-noise channel. If we use the same ensemble for coding as in Eq. (51), then the resulting private dynamic achievable rate region is slightly different from that in Eqs. (48)–(50). A thermal channel does not preserve the purity of coherent states transmitted through it. Thus, the entropy in Eq. (55) is no longer equal to zero, but it is instead equal to

$$\int\!\!\int d\alpha\, d\beta\; p_{\bar{\lambda}N_S}(\alpha)p_{(\lambda)N_S}(\beta)\;\; H(\mathcal{N}(|\alpha+\beta\rangle\langle\alpha+\beta|))$$
$$= g((1-\eta)N_B)$$

because Bob's state is a displaced thermal state with mean photon number $(1-\eta)N_B$ (the amount of noise that the environment injects into the state). Thus, the expression for the private dynamic achievable rate region is as stated in the theorem. ■

This region is generally smaller than the full quantum dynamic achievable rate region for the same values of N_S, N_B, and η because there is no analog of the superdense coding effect with the resources of public classical communication, private classical communication, and secret key [31,50]. Although, the trade-off between public and private communication with this coding strategy is the same as that between classical and quantum communication in Eqs. (76) and (77).

V. AMPLIFYING CHANNEL

The amplifying channel is another bosonic channel important in applications, modeling any kind of amplification process that can occur in bosonic systems. These applications range from cavities coupled with Josephson junctions [51], to nondegenerate parametric amplifiers in quantum optics [52], to the Unruh effect from relativistic quantum mechanics [53].

The amplifying channel corresponds to the following transformation of the input annihilation operator:

$$\hat{a} \rightarrow \sqrt{\kappa}\, \hat{a} + \sqrt{\kappa - 1}\, \hat{e}^{\dagger}, \tag{78}$$

$$\hat{e}^{\dagger} \rightarrow \sqrt{\kappa - 1}\, \hat{a} + \sqrt{\kappa}\, \hat{e}^{\dagger}, \tag{79}$$

where $\kappa \geqslant 1$ is the amplifier gain and $\hat{e}$ is now an auxiliary mode associated with the amplification process. If the state of the auxiliary mode is a vacuum state, then this auxiliary mode injects the minimum possible noise into the signal mode. We can consider the auxiliary mode more generally to be in a thermal state with mean photon number N_B.

A. Achievable quantum and private dynamic regions

Theorem 11. An achievable quantum dynamic region for the amplifying channel with gain $\kappa \geqslant 1$ and mean thermal photon number N_B is as follows:

$$\begin{aligned} C + 2Q &\leqslant g(\lambda N_S) + g(\kappa N_S + (\kappa - 1)(N_B + 1)) \\ &\quad - g_E^{\kappa}(\lambda, N_S, N_B), \\ Q + E &\leqslant g(\kappa \lambda N_S + (\kappa - 1)(N_B + 1)) \\ &\quad - g_E^{\kappa}(\lambda, N_S, N_B), \\ C + Q + E &\leqslant g(\kappa N_S + (\kappa - 1)(N_B + 1)) \\ &\quad - g_E^{\kappa}(\lambda, N_S, N_B), \end{aligned}$$

where $\lambda \in [0,1]$ is a photon-number-sharing parameter, $g(N)$ is defined in Eq. (2), and

$$\begin{aligned} &g_E^{\kappa}(\lambda, N_S, N_B) \\ &\quad \equiv g([D + (\kappa - 1)[\lambda N_S + N_B + 1] - 1]/2) \\ &\qquad + g([D - (\kappa - 1)[\lambda N_S + N_B + 1] - 1]/2), \\ &D^2 \equiv [\lambda(1 + \kappa) N_S + (\kappa - 1)(N_B + 1) + 1]^2 \\ &\qquad - 4\kappa \lambda N_S (\lambda N_S + 1). \end{aligned}$$

Theorem 12. An achievable private dynamic region for the amplifying channel with gain $\kappa \geqslant 1$ and mean thermal photon number N_B is as follows:

$$\begin{aligned} R + P &\leqslant g(\kappa N_S + (\kappa - 1)(N_B + 1)) \\ &\quad - g((\kappa - 1)(N_B + 1)), \\ P + S &\leqslant g(\kappa \lambda N_S + (\kappa - 1)(N_B + 1)) \\ &\quad - g_E^{\kappa}(\lambda, N_S, N_B), \\ R + P + S &\leqslant g(\kappa N_S + (\kappa - 1)(N_B + 1)) \\ &\quad - g_E^{\kappa}(\lambda, N_S, N_B), \end{aligned}$$

where $\lambda \in [0,1]$ is a photon-number-sharing parameter, $g(N)$ is defined in Eq. (2), and g_E^{κ} is defined in Eq. (80).

Proof (of Theorems 11 and 12). The trade-off coding scheme for both the quantum dynamic and private dynamic trade-off settings is the same as we used before in Eqs. (31) and (51), respectively. Thus, we only need to calculate the various entropies associated with the amplifying channel. We consider the quantum dynamic setting first and calculate the four entropies in Eqs. (34)–(37).

The state resulting from transmitting a thermal state with mean photon number N_S through the amplifying channel is a thermal state with mean photon number $\kappa N_S + (\kappa - 1)(N_B + 1)$. Thus, it follows that

$$H(\mathcal{N}(\overline{\theta})) = g(\kappa N_S + (\kappa - 1)(N_B + 1)).$$

By the same argument as before, we have that

$$\int d\alpha\ p_{\overline{\lambda} N_S}(\alpha)\ H(D(\alpha)\theta D^{\dagger}(\alpha)) = g(\lambda N_S).$$

The displacement operators acting on a thermal state are again covariant with respect to the amplifying channel so that

$$\begin{aligned} &\int d\alpha\ p_{\overline{\lambda} N_S}(\alpha)\ H(\mathcal{N}(D(\alpha)\theta D^{\dagger}(\alpha))) \\ &\quad = g(\kappa \lambda N_S + (\kappa - 1)(N_B + 1)). \end{aligned}$$

Finally, we can make use of the Holevo-Werner results in Sec. V A of Ref. [43] to show that

$$\int d\alpha\ p_{\overline{\lambda} N_S}(\alpha)\ H(\mathcal{N}^c(D(\alpha)\theta D^{\dagger}(\alpha))) = g_E^{\kappa}(\lambda, N_S, N_B),$$

where

$$\begin{aligned} &g_E^{\kappa}(\lambda, N_S, N_B) \\ &\quad \equiv g([D + (\kappa - 1)(\lambda N_S + N_B + 1) - 1]/2) \\ &\qquad + g([D - (\kappa - 1)(\lambda N_S + N_B + 1) - 1]/2) \end{aligned} \tag{80}$$

and

$$\begin{aligned} D^2 &\equiv [\lambda\,(1 + \kappa)\, N_S + (\kappa - 1)\,(N_B + 1) + 1]^2 \\ &\quad - 4\kappa \lambda N_S\,(\lambda N_S + 1)\,. \end{aligned}$$

Thus, the expression for the quantum dynamic capacity region of an amplifying channel is as stated in Theorem 11 above.

We can also use a similar coding scheme as in Eq. (51) for the private dynamic setting. The only other entropy that we need to calculate for this setting is the one in Eq. (55):

$$\begin{aligned} &\iint d\alpha\, d\beta\ p_{\overline{\lambda} N_S}(\alpha) p_{(\lambda) N_S}(\beta)\ H(\mathcal{N}(|\alpha + \beta\rangle\langle\alpha + \beta|)) \\ &\quad = g((\kappa - 1)(N_B + 1)) \end{aligned}$$

because Bob's state is a displaced thermal state with mean photon number $(\kappa - 1)\,(N_B + 1)$ (the amount of noise that the environment injects into the state). Thus, the expression for the private dynamic achievable rate region is as stated in Theorem 12 above. ■

Figure 6 plots the classical-quantum and classical-entanglement trade-off curves for an amplifying channel with $N_S = 200$, $N_B = 0$, and increasing values of the amplification parameter κ. The figures demonstrate that increased amplification decreases performance, but the upshot is that both trade-off settings still exhibit a remarkable improvement over time sharing.

VI. UNRUH CHANNEL

Brádler *et al.* studied the information-theoretic consequences of the Unruh effect in a series of papers [54–59]. They dubbed "the Unruh channel" as the channel induced by the Unruh effect when an observer encodes a qubit into a single-excitation subspace of Unruh modes and a uniformly accelerating Rindler observer detects this state (by single-excitation encoding, we mean a dual-rail encoding

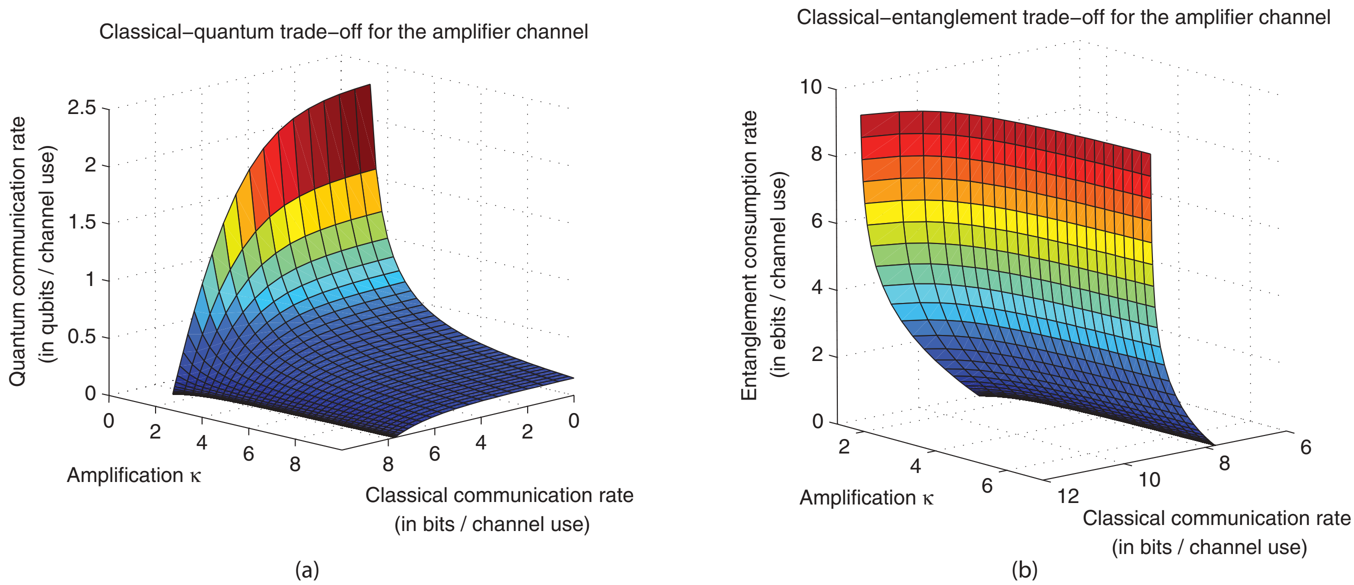

FIG. 6. (Color online) (a) Trade-off between classical and quantum communication for the bosonic amplifying channel with $N_S = 200$ and $N_B = 0$ for increasing values of the amplification parameter κ. (b) Trade-off between entanglement-assisted and unassisted classical communication for the same channel. For both trade-offs, more amplification degrades performance because it introduces too much noise.

with $|0_L\rangle \equiv |01\rangle$ and $|1_L\rangle \equiv |10\rangle$). It is well known that the transformation corresponding to the Unruh effect is equivalent to the transformation in Eqs. (78) and (79) for an amplifying bosonic channel [60]. The results of Brádler *et al.* demonstrate that "the Unruh channel" has a beautiful structure as a countably infinite direct sum of universal cloning machine channels [54], and this property implies that both the quantum dynamic and private dynamic capacity regions are single letter [30,31,57]. More generally, their results with single-excitation encodings of course apply to amplifying bosonic channels.

In spite of these analytical results, one might question calling this channel *the* Unruh channel because the encoding has a specific form as a dual-rail encoding. More generally, we could study the capacities of the transformation corresponding to the Unruh effect by imposing a mean-photon-number constraint at the input, rather than restricting the form of the encoding. In this way, we can relate the achievable rates in Sec. V to the capacity results of Brádler *et al.* In order to make a fair comparison, we should restrict the mean number of photons at the input to be $\frac{1}{2}$ because this is the mean number of photons when sending a dual-rail maximally mixed state of the form $(|01\rangle\langle 01| + |10\rangle\langle 10|)/2$, but we should then multiply all rates by two because the Unruh channel of Brádler *et al.* exploits two uses of the Unruh transformation for one use of the

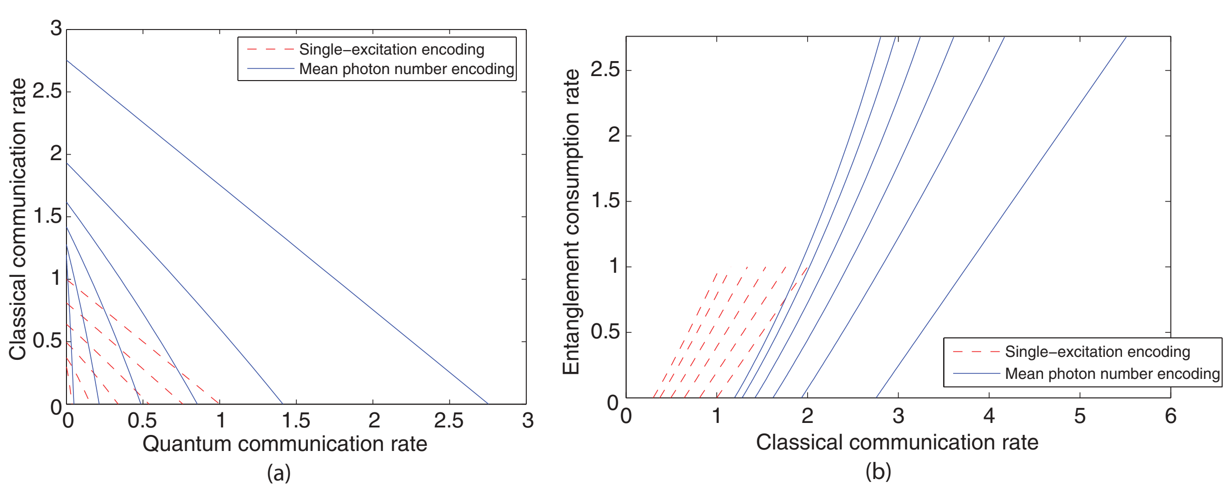

FIG. 7. (Color online) Trade-off curves between (a) classical and quantum communication and (b) entanglement-assisted and unassisted classical communication. Units for classical communication, quantum communication, and entanglement consumption are bits per channel use, qubits per channel use, and ebits per channel use, respectively. Each figure plots a trade-off curve (rightmost to leftmost) for increasing values of the acceleration parameter $z \in \{0,0.2,0.4,0.6,0.8,0.95\}$. The dotted curves are the trade-off curves from Ref. [57] when the encoding is restricted to a single-excitation subspace. The solid lines are achievable rates with a mean-photon-number constraint of $1/2$. The result is that the mean-photon-number constrained encoding always outperforms single-excitation encoding.

Unruh channel. It is fair to consider the maximally mixed state as input because this is the state that achieves the boundary of the various capacity regions when tracing over all other systems not input to the channel [57]. Furthermore, note that the acceleration parameter z of Brádler *et al.* in Refs. [54,57] is related to the amplification parameter κ for the amplifying bosonic channel via $z = (\kappa - 1)/\kappa$.

Figure 7 compares the trade-off curves for the "Unruh channel" with the trade-off curves for the Unruh transformation with a mean-photon-number constraint. The result is that the latter outperforms the former for all depicted values of the acceleration parameter z (although note that the quantum rates become comparable as the acceleration parameter z increases to 0.95). The result in the figure is unsurprising because an encoding with a mean-photon-number constraint has access to more of Fock space than does a restricted encoding. A similar result occurs when comparing the amplitude damping channel with the lossy bosonic channel [61] (the amplitude damping channel results from sending a superposition of the vacuum state and a single-photon state through the lossy bosonic channel).

VII. CONCLUSION

In summary, we have provided detailed derivations of the main results announced in our previous paper [20]. In particular, we have shown that the rate regions given in Eqs. (1) and (2) characterize the classical-quantum-entanglement trade-off and the public-private secret-key trade-off, respectively, for communicating over a pure-loss bosonic channel. We have argued for a "rule of thumb" for trade-off coding, so that a sender and receiver can make the best use of photon-number sharing if a large number of photons are available on average for coding. We have also argued that the regions in Eqs. (1) and (2) for $\eta \geqslant \frac{1}{2}$ are optimal, provided that a long-standing minimum-output entropy conjecture is true. Finally, we have generalized the achievable rate regions in Eqs. (1) and (2) to the case of thermal-noise and amplifying bosonic channel, with the latter results applying to the Unruh channel studied in previous work.

There are certainly some interesting questions to consider for future work. First, it would be great to lay out explicit encoding-decoding architectures that come close to achieving the rate regions given in Eqs. (1) and (2). Progress along these lines is in Refs. [62–66] for the case of classical or quantum communication alone, but more generally, there might be some way to leverage these results for a trade-off coding architecture. It would also be good to investigate whether the recent bounds derived in Ref. [27] could be used to determine true outer bounds on the regions given here. Finally, it would be good to go beyond the single-mode approximation for the Unruh channel, as recent work has demonstrated that this approximation is not sufficient for modeling the Unruh effect in general quantum information-theoretic applications [67]. References [68,69] identify the communication conditions under which effective single-mode Unruh channels can be identified.

ACKNOWLEDGMENTS

We thank J. H. Shapiro for reminding us of relevant results [24] and N. Menicucci for a useful discussion. M.M.W. acknowledges the MDEIE (Québec) PSR-SIIRI international collaboration grant. P.H. acknowledges the hospitality of the Stanford Institute for Theoretical Physics as well as funding from the Canada Research Chairs program, the Perimeter Institute, CIFAR, FQRNT's INTRIQ, NSERC, ONR through Grant No. N000140811249, and QuantumWorks. S.G. acknowledges the DARPA Information in a Photon program, Contract No. HR0011-10-C-0159.

[1] C. E. Shannon, Bell Syst. Tech. J. **27**, 379 (1948).

[2] C. Weedbrook, S. Pirandola, R. Garcia-Patron, N. J. Cerf, T. C. Ralph, J. H. Shapiro, and S. Lloyd, Rev. Mod. Phys. **84**, 621 (2012).

[3] A. S. Holevo, IEEE Trans. Inf. Theory **44**, 269 (1998).

[4] B. Schumacher and M. D. Westmoreland, Phys. Rev. A **56**, 131 (1997).

[5] H. P. Yuen and M. Ozawa, Phys. Rev. Lett. **70**, 363 (1993).

[6] V. Giovannetti, S. Guha, S. Lloyd, L. Maccone, J. H. Shapiro, and H. P. Yuen, Phys. Rev. Lett. **92**, 027902 (2004).

[7] J. Chen, J. L. Habif, Z. Dutton, R. Lazarus, and S. Guha, Nat. Photonics **6**, 374 (2012).

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

[9] S. Barz, E. Kashefi, A. Broadbent, J. F. Fitzsimons, A. Zeilinger, and P. Walther, Science **335**, 303 (2012).

[10] S. Lloyd, Phys. Rev. A **55**, 1613 (1997).

[11] P. W. Shor, Lecture Notes, MSRI Workshop on Quantum Computation, 2002 (unpublished).

[12] I. Devetak, IEEE Trans. Inf. Theory **51**, 44 (2005).

[13] B. Schumacher and M. A. Nielsen, Phys. Rev. A **54**, 2629 (1996).

[14] B. Schumacher and M. D. Westmoreland, Phys. Rev. Lett. **80**, 5695 (1998).

[15] H. Barnum, E. Knill, and M. A. Nielsen, IEEE Trans. Inf. Theory **46**, 1317 (2000).

[16] H. Barnum, M. A. Nielsen, and B. Schumacher, Phys. Rev. A **57**, 4153 (1998).

[17] C. H. Bennett, P. W. Shor, J. A. Smolin, and A. V. Thapliyal, Phys. Rev. Lett. **83**, 3081 (1999).

[18] C. H. Bennett, P. W. Shor, J. A. Smolin, and A. V. Thapliyal, IEEE Trans. Inf. Theory **48**, 2637 (2002).

[19] A. Winter, IEEE Trans. Inf. Theory **45**, 2481 (1999).

[20] M. M. Wilde, P. Hayden, and S. Guha, Phys. Rev. Lett. **108**, 140501 (2012).

[21] T. M. Cover and J. A. Thomas, *Elements of Information Theory* (Wiley, New York, 1991).

[22] V. Giovannetti, S. Guha, S. Lloyd, L. Maccone, and J. H. Shapiro, Phys. Rev. A **70**, 032315 (2004).

[23] V. Giovannetti, A. S. Holevo, S. Lloyd, and L. Maccone, J. Phys. A: Math. Theor. **43**, 415305 (2010).
[24] S. Guha, J. H. Shapiro, and B. I. Erkmen, Phys. Rev. A **76**, 032303 (2007).
[25] S. Guha, Ph.D. thesis, Massachusetts Institute of Technology, 2008.
[26] R. Koenig and G. Smith, arXiv:1205.3409.
[27] R. Koenig and G. Smith, arXiv:1205.3407.
[28] M.-H. Hsieh and M. M. Wilde, IEEE Trans. Inf. Theory **56**, 4682 (2010).
[29] M.-H. Hsieh and M. M. Wilde, IEEE Trans. Inf. Theory **56**, 4705 (2010).
[30] M. M. Wilde and M.-H. Hsieh, Quantum Inf. Process. **11**, 1431 (2012).
[31] M. M. Wilde and M.-H. Hsieh, Quantum Inf. Process. **11**, 1465 (2012).
[32] The simplest version of the minimum-output entropy conjecture is stated as follows. Suppose that a thermal state is injected into one input port of a beamsplitter. What state should we inject into the other input port to minimize the entropy at one of the output ports? The conjecture is that the state should just be the vacuum, but this question has been open for some time [22–25,40]. See Refs. [26,27] for recent progress.
[33] C. H. Bennett, G. Brassard, C. Crépeau, R. Jozsa, A. Peres, and W. K. Wootters, Phys. Rev. Lett. **70**, 1895 (1993).
[34] M. M. Wilde, arXiv:1106.1445.
[35] C. H. Bennett and S. J. Wiesner, Phys. Rev. Lett. **69**, 2881 (1992).
[36] I. Devetak and P. W. Shor, Commun. Math. Phys. **256**, 287 (2005).
[37] P. W. Shor, *Quantum Information, Statistics, Probability* (Rinton, Paramus, NJ, 2004), pp. 144–152.
[38] A. Uhlmann, Commun. Math. Phys. **54**, 21 (1977).
[39] M.-H. Hsieh and M. M. Wilde, Phys. Rev. A **80**, 022306 (2009).
[40] S. Guha, J. H. Shapiro, and B. I. Erkmen, in Proceedings of the IEEE International Symposium on Information Theory, Toronto, Ontario, Canada, 2008 (unpublished).
[41] C. Gerry and P. Knight, *Introductory Quantum Optics* (Cambridge University Press, Cambridge, UK, 2004).
[42] S. L. Braunstein and P. van Loock, Rev. Mod. Phys. **77**, 513 (2005).
[43] A. S. Holevo and R. F. Werner, Phys. Rev. A **63**, 032312 (2001).
[44] V. Giovannetti, S. Lloyd, L. Maccone, and P. W. Shor, Phys. Rev. Lett. **91**, 047901 (2003).
[45] V. Giovannetti, S. Lloyd, L. Maccone, and P. W. Shor, Phys. Rev. A **68**, 062323 (2003).
[46] M. M. Wolf, D. Pérez-García, and G. Giedke, Phys. Rev. Lett. **98**, 130501 (2007).
[47] I. Devetak, A. W. Harrow, and A. Winter, IEEE Trans. Inf. Theory **54**, 4587 (2008).
[48] J. Eisert and M. M. Wolf, *Quantum Information with Continous Variables of Atoms and Light* (Imperial College Press, London, 2007), pp. 23–42.
[49] M. M. Wolf, G. Giedke, and J. I. Cirac, Phys. Rev. Lett. **96**, 080502 (2006).
[50] D. Collins and S. Popescu, Phys. Rev. A **65**, 032321 (2002).
[51] A. A. Clerk, M. H. Devoret, S. M. Girvin, F. Marquardt, and R. J. Schoelkopf, Rev. Mod. Phys. **82**, 1155 (2010).
[52] C. M. Caves, Phys. Rev. D **26**, 1817 (1982).
[53] W. G. Unruh, Phys. Rev. D **14**, 870 (1976).
[54] K. Brádler, P. Hayden, and P. Panangaden, J. High Energy Phys. 09 (2009) 074.
[55] K. Brádler, IEEE Trans. Inf. Theory **57**, 5497 (2011).
[56] K. Brádler, N. Dutil, P. Hayden, and A. Muhammad, J. Math. Phys. **51**, 072201 (2010).
[57] K. Brádler, P. Hayden, D. Touchette, and M. M. Wilde, Phys. Rev. A **81**, 062312 (2010).
[58] K. Brádler, P. Hayden, and P. Panangaden, Commun. Math. Phys. **312**, 361 (2012).
[59] T. Jochym-O'Connor, K. Brádler, and M. M. Wilde, J. Phys. A: Math. Theor. **44**, 415306 (2011).
[60] P. D. Nation, J. R. Johansson, M. P. Blencowe, and F. Nori, Rev. Mod. Phys. **84**, 1 (2012).
[61] V. Giovannetti and R. Fazio, Phys. Rev. A **71**, 032314 (2005).
[62] M. M. Wilde, S. Guha, S.-H. Tan, and S. Lloyd, in *Proceedings of the 2012 International Symposium on Information Theory, 2012* (IEEE, New York, 2012), pp. 551–555, arXiv:1202.0518.
[63] M. M. Wilde and S. Guha, arXiv:1109.2591 [IEEE Trans. Inf. Theory (to be published)].
[64] M. M. Wilde and S. Guha, arXiv:1109.5346.
[65] M. M. Wilde and J. M. Renes, in *Proceedings of the 2012 International Symposium on Information Theory* (IEEE, New York, 2012), pp. 334–338, arXiv:1201.2906.
[66] M. M. Wilde and J. M. Renes, arXiv:1203.5794.
[67] D. E. Bruschi, J. Louko, E. Martin-Martinez, A. Dragan, and I. Fuentes, Phys. Rev. A **82**, 042332 (2010).
[68] T. G. Downes, T. C. Ralph, and N. Walk, arXiv:1203.2716.
[69] A. Dragan, J. Doukas, E. Martin-Martinez, and D. E. Bruschi, arXiv:1203.0655.