

Capacity of the Bosonic Wiretap Channel and the Entropy Photon-Number Inequality

Saikat Guha

Research Laboratory of Electronics
MIT, Cambridge, MA 02139
saikat@MIT.edu

Jeffrey H. Shapiro

Research Laboratory of Electronics
MIT, Cambridge, MA 02139
jhs@MIT.edu

Baris I. Erkmen

Research Laboratory of Electronics
MIT, Cambridge, MA 02139
erkmen@MIT.edu

Abstract—Determining the ultimate classical information carrying capacity of electromagnetic waves requires quantum-mechanical analysis to properly account for the bosonic nature of these waves. Recent work has established capacity theorems for bosonic single-user and broadcast channels, under the presumption of two minimum output entropy conjectures. Despite considerable accumulated evidence that supports the validity of these conjectures, they have yet to be proven. In this paper, it is shown that the second conjecture suffices to prove the classical capacity of the bosonic wiretap channel, which in turn would also prove the quantum capacity of the lossy bosonic channel. The preceding minimum output entropy conjectures are then shown to be simple consequences of an Entropy Photon-Number Inequality (EPnI), which is a conjectured quantum-mechanical analog of the Entropy Power Inequality (EPI) from classical information theory.

I. MOTIVATION AND HISTORY

The performance of communication systems that rely on electromagnetic wave propagation are ultimately limited by noise of quantum-mechanical origin. Moreover, high-sensitivity photodetection systems have long been close to this noise limit. Hence determining the ultimate capacities of lasercom channels is of immediate relevance. The most famous channel capacity formula is Shannon's result for the classical additive white Gaussian noise channel. For a complex-valued channel model in which we transmit a and receive $c = \sqrt{\eta}a + \sqrt{1-\eta}b$, where $0 < \eta < 1$ is the channel's transmissivity and b is a zero-mean, isotropic, complex-valued Gaussian random variable that is independent of a , Shannon's capacity is

$$C_{\text{classical}} = \ln[1 + \eta\bar{N}/(1-\eta)N] \text{ nats/use}, \quad (1)$$

with $E(|a|^2) \leq \bar{N}$ and $E(|b|^2) = N$. In the quantum version of this channel model, we control the state of an electromagnetic mode with photon annihilation operator \hat{a} at the transmitter, and receive another mode with photon annihilation operator $\hat{c} = \sqrt{\eta}\hat{a} + \sqrt{1-\eta}\hat{b}$, where \hat{b} is the annihilation operator of a noise mode that is in a zero-mean, isotropic, complex-valued Gaussian state. For lasercom, if quantum measurements corresponding to ideal optical homodyne or heterodyne detection are employed at the receiver, this quantum channel reduces to a real-valued (homodyne) or complex-valued (heterodyne) additive Gaussian noise channel, from which the following capacity formulas (in nats/use)

follow:

$$C_{\text{homodyne}} = 2^{-1} \ln[1 + 4\eta\bar{N}/(2(1-\eta)N + 1)] \quad (2)$$

$$C_{\text{heterodyne}} = \ln[1 + \eta\bar{N}/((1-\eta)N + 1)]. \quad (3)$$

The +1 terms in the noise denominators are quantum contributions, so that even when the noise mode \hat{b} is unexcited these capacities remain finite, unlike the situation in Eq. (1).

The classical capacity of the pure-loss bosonic channel—in which the \hat{b} mode is unexcited ($N = 0$)—was shown in [1] to be $C_{\text{pure-loss}} = g(\eta\bar{N})$ nats/use, where $g(x) \equiv (x+1)\ln(x+1) - x\ln(x)$ is the Shannon entropy of the Bose-Einstein probability distribution with mean x . This capacity exceeds the $N = 0$ versions of Eqs. (2) and (3), as well as the best known bound on the capacity of ideal optical direct detection. The ultimate capacity of the thermal-noise ($N > 0$) version of this channel is bounded below as follows, $C_{\text{thermal}} \geq g(\eta\bar{N} + (1-\eta)N) - g((1-\eta)N)$, and this bound was shown to be the capacity if the thermal channel obeyed a certain minimum output entropy conjecture [2]. This conjecture states that the von Neumann entropy at the output of the thermal channel is minimized when the \hat{a} mode is in its vacuum state. Considerable evidence in support of this conjecture has been accumulated [3], but it has yet to be proven. Nevertheless, the preceding lower bound already exceeds Eqs. (2) and (3) as well as the best known bounds on the capacity of direct detection.

More recently, a capacity analysis of the bosonic broadcast channel led to an inner bound on the capacity region, which was shown to be the capacity region under the presumption of a second minimum output entropy conjecture [4]. Both conjectures have been proven if the input states are restricted to be Gaussian, and they have been shown to be equivalent under this input-state restriction. In this paper, we show that the second conjecture will establish the privacy capacity of the lossy bosonic channel, as well as its ultimate quantum information carrying capacity.

The Entropy Power Inequality (EPI) from classical information theory is widely used in coding theorem converse proofs for Gaussian channels. By analogy with the EPI, we conjecture its quantum version, viz., the Entropy Photon-number Inequality (EPnI). In this paper we show that the two minimum output entropy conjectures cited above are

simple corollaries of the EPnI. Hence, proving the EPnI would immediately establish key results for the capacities of bosonic communication channels.

II. QUANTUM WIRETAP CHANNEL

The term ‘‘wiretap channel’’ was coined by Wyner [5] to describe a communication system, in which Alice wishes to communicate classical information to Bob, over a point-to-point discrete memoryless channel that is subjected to a wiretap by an eavesdropper Eve. Alice’s goal is to reliably and securely communicate classical data to Bob, in such a way that Eve gets no information whatsoever about the message. Wyner used the conditional entropy rate of the signal received by Eve, given Alice’s transmitted message, to measure the secrecy level guaranteed by the system. He gave a single letter characterization of the rate-equivocation region under a limiting assumption, that the signal received by Eve is a degraded version of the one received by Bob. Csiszár and Körner later generalized Wyner’s results to the case in which the signal received by Eve is not a degraded version of the one received by Bob [6]. These classical-channel results were later extended by Devetak [7] to encompass classical transmission over a quantum wiretap channel.

A quantum channel \mathcal{N}_{A-B} from Alice to Bob is a trace-preserving completely positive map that transforms Alice’s single-use density operator $\hat{\rho}^A$ to Bob’s, $\hat{\rho}^B = \mathcal{N}_{A-B}(\hat{\rho}^A)$. The quantum wiretap channel \mathcal{N}_{A-BE} is a quantum channel from Alice to an intended receiver Bob and an eavesdropper Eve. The quantum channel from Alice to Bob is obtained by tracing out E from the channel map, i.e., $\mathcal{N}_{A-B} \equiv \text{Tr}_E(\mathcal{N}_{A-BE})$, and similarly for \mathcal{N}_{A-E} . A quantum wiretap channel is degraded if there exists a degrading channel $\mathcal{N}_{B-E}^{\text{deg}}$ such that $\mathcal{N}_{A-E} = \mathcal{N}_{B-E}^{\text{deg}} \circ \mathcal{N}_{A-B}$.

The wiretap channel describes a physical scenario in which for each successive n uses of \mathcal{N}_{A-BE} Alice communicates a randomly generated classical message $m \in W$ to Bob, where m is a classical index that is uniformly distributed over the set, W , of 2^{nR} possibilities. To encode and transmit m , Alice generates an instantiation $k \in K$ of a discrete random variable, and then prepares n -channel-use states that after transmission through the channel, result in bipartite conditional density operators $\{\hat{\rho}_{m,k}^{B^n E^n}\}$. A $(2^{nR}, n, \epsilon)$ code for this channel consists of an encoder, $x^n : (W, K) \rightarrow \mathcal{A}^n$, and a positive operator-valued measure (POVM) $\{\Lambda_m^{B^n}\}$ on \mathcal{B}^n such that the following conditions are satisfied for every $m \in W$.¹

- 1) Bob’s probability of decoding error is at most ϵ , i.e.,

$$\text{Tr}\left(\hat{\rho}_{m,k}^{B^n} \Lambda_m^{B^n}\right) > 1 - \epsilon, \quad \forall k, \quad \text{and} \quad (4)$$

- 2) For any POVM $\{\Lambda_m^{E^n}\}$ on \mathcal{E}^n , no more than ϵ bits of information is revealed about the secret message m . Using $j \equiv (m, k)$, this condition can be expressed, in terms of the Holevo information [8], as follows,

$$\chi\left(p_j, \mathcal{N}_{A-E}^{\otimes n}(\rho_j^{A^n})\right) \leq \epsilon. \quad (5)$$

¹ \mathcal{A}^n , \mathcal{B}^n , and \mathcal{E}^n are the n -channel-use alphabets of Alice, Bob and Eve.

Here, $\chi(p_j, \hat{\sigma}_j) \equiv S(\sum_j p_j \hat{\sigma}_j) - \sum_j p_j S(\hat{\sigma}_j)$, is the Holevo information, where $\{p_j\}$ is a probability distribution associated with the density operators $\hat{\sigma}_j$, and $S(\hat{\rho}) \equiv -\text{Tr}(\hat{\rho} \log \hat{\rho})$ is the von Neumann entropy of the density operator $\hat{\rho}$.²

Because Holevo information may not be additive, the classical privacy capacity C_p of the quantum wiretap channel must be computed by maximizing over successive uses of the channel, i.e., for n being the number of uses of the channel,

$$\begin{aligned} C_p(\mathcal{N}_{A-BE}) &= \sup_n \max_{p_T(i), \sum_j p_{A|T}(j|i) \hat{\rho}_j^{B^n}} \left[\chi(p_T(i), \sum_j p_{A|T}(j|i) \hat{\rho}_j^{B^n})/n \right. \\ &\quad \left. - \chi(p_T(i), \sum_j p_{A|T}(j|i) \hat{\rho}_j^{E^n})/n \right]. \end{aligned} \quad (6)$$

The probabilities $\{p_i\}$ form a distribution over an auxiliary classical alphabet \mathcal{T} , of size $|\mathcal{T}|$. The ultimate privacy capacity is computed by maximizing the expression specified in (6) over $\{p_T(i)\}$, $\{p_{A|T}(j|i)\}$, $\{\hat{\rho}_j^{A^n}\}$, and n , subject to a cardinality constraint on $|\mathcal{T}|$. For a degraded wiretap channel, the auxiliary random variable is unnecessary, and Eq. (6) reduces to

$$C_p(\mathcal{N}_{A-BE}) = \sup_n \max_{p_A(j)} [\chi(p_A(j), \hat{\rho}_j^{B^n})/n - \chi(p_A(j), \hat{\rho}_j^{E^n})/n]. \quad (7)$$

III. NOISELESS BOSONIC WIRETAP CHANNEL

The noiseless bosonic wiretap channel consists of a collection of spatial and temporal bosonic modes at the transmitter that interact with a minimal-quantum-noise environment and split into two sets of spatio-temporal modes en route to two independent receivers, one being the intended receiver and the other being the eavesdropper. The multi-mode bosonic wiretap channel is given by $\bigotimes_s \mathcal{N}_{A_s-B_s E_s}$, where $\mathcal{N}_{A_s-B_s E_s}$ is the wiretap-channel map for the s th mode, which can be obtained from the Heisenberg evolutions

$$\hat{b}_s = \sqrt{\eta_s} \hat{a}_s + \sqrt{1 - \eta_s} \hat{f}_s, \quad (8)$$

$$\hat{e}_s = \sqrt{1 - \eta_s} \hat{a}_s - \sqrt{\eta_s} \hat{f}_s, \quad (9)$$

where the $\{\hat{a}_s\}$ are Alice’s modal annihilation operators, and $\{\hat{b}_s\}$, $\{\hat{e}_s\}$ are the corresponding modal annihilation operators for Bob and Eve, respectively. The modal transmissivities $\{\eta_s\}$ satisfy $0 \leq \eta_s \leq 1$, and the environment modes $\{\hat{f}_s\}$ are in their vacuum states. We will limit our treatment here to the single-mode bosonic wiretap channel, as the privacy capacity of the multi-mode channel can in principle be obtained by summing up capacities of all spatio-temporal modes and maximizing the sum capacity subject to an overall input-power budget using Lagrange multipliers, cf. [2], where this was done for the multi-mode single-user lossy bosonic channel.

Theorem — Assuming the truth of minimum output entropy conjecture 2 (see Sec. V), the ultimate privacy capacity of the

²A density operator is Hermitian, with eigenvalues that form a probability distribution. Thus, the von Neumann entropy of a density operator $\hat{\rho}$ is the Shannon entropy of its eigenvalues.

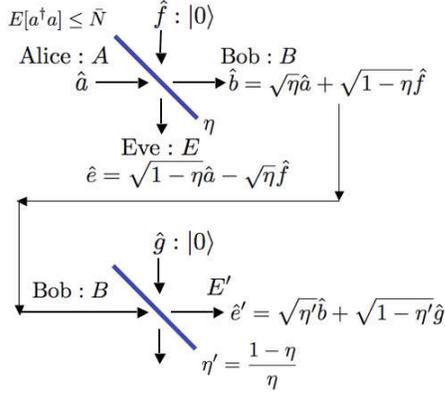


Fig. 1. Schematic diagram of the single-mode bosonic wiretap channel. The transmitter Alice (A) encodes her messages to Bob (B) in a classical index j , and over n successive uses of the channel, thus preparing a bipartite state $\hat{\rho}_j^{B^n E^n}$ where E^n represents n channel uses of an eavesdropper Eve (E). For $\eta > 1/2$, this channel is degraded, as Eve's state can be recreated by passing Bob's state through a beamsplitter of transmissivity $(1 - \eta)/\eta$.

single-mode noiseless bosonic wiretap channel (see Fig. 1) with mean input photon-number constraint $\langle \hat{a}^\dagger \hat{a} \rangle \leq \bar{N}$ is

$$C_p(\mathcal{N}_{A-BE}) = g(\eta\bar{N}) - g((1-\eta)\bar{N}) \text{ nats/use}, \quad (10)$$

for $\eta > 1/2$ and $C_p = 0$ for $\eta \leq 1/2$. This capacity is additive and achievable with single-channel-use coherent-state encoding with a zero-mean isotropic Gaussian prior distribution $p_A(\alpha) = \exp(-|\alpha|^2/\bar{N})/\pi\bar{N}$.

Proof — Devetak's result for the privacy capacity of the degraded quantum wiretap channel in Eq. (7) requires finite-dimensional Hilbert spaces. Nevertheless, we will use this result for the bosonic wiretap channel, which has an infinite-dimensional state space, by extending it to infinite-dimensional state spaces through a limiting argument.³ Furthermore, it was recently shown that the privacy capacity of a degraded wiretap channel is additive, and equal to the single-letter quantum capacity of the channel from Alice to Bob [9], i.e.,

$$C_p(\mathcal{N}_{A-BE}) = C_p^{(1)}(\mathcal{N}_{A-BE}) = Q^{(1)}(\mathcal{N}_{A-B}), \quad (11)$$

where the superscript (1) denotes single-letter capacity. It is straightforward to show that if $\eta > 1/2$, the bosonic wiretap channel is a degraded channel, in which Bob's is the less-noisy receiver and Eve's is the more-noisy receiver. The degraded nature of the bosonic wiretap channel has been depicted in

³When $|\mathcal{T}|$ and $|\mathcal{A}|$ are finite and we are using coherent states in Eq. (7), there will be a finite number of possible transmitted states, leading to a finite number of possible states received by Bob and Eve. Suppose we limit the auxiliary-input alphabet (\mathcal{T})—and hence the input (\mathcal{A}) and the output alphabets (\mathcal{B} and \mathcal{E})—to truncated coherent states within the finite-dimensional Hilbert space spanned by the Fock states $\{|m\rangle : 0 \leq m \leq M\}$, where $M \gg \bar{N}$. Applying Devetak's theorem to the Hilbert space spanned by these truncated coherent states then gives us a lower bound on the privacy capacity of the bosonic wiretap channel when the entire, infinite-dimensional Hilbert space is employed. By taking M sufficiently large, while maintaining the cardinality condition for \mathcal{T} , the rate-region expressions given by Devetak's theorem will converge to Eq. (10).

Fig. 1, where the quantum states $\hat{\rho}^{E'}$ of the constructed system E' are identical to the quantum states $\hat{\rho}^E$ for a given input quantum state $\hat{\rho}^A$. Using Eq. (11) for the bosonic wiretap channel, we have

$$\begin{aligned} C_p(\mathcal{N}_{A-BE}) &= \max_{\langle \hat{a}^\dagger \hat{a} \rangle \leq \bar{N}} [S(\hat{\rho}^B) - S(\hat{\rho}^E)] \\ &= \max_{\langle \hat{a}^\dagger \hat{a} \rangle \leq \bar{N}} [S(\hat{\rho}^B) - S(\hat{\rho}^{E'})] \\ &= \max_{0 \leq K \leq g(\eta\bar{N})} \{ \max_{\langle \hat{a}^\dagger \hat{a} \rangle \leq \bar{N}, S(\hat{\rho}^B) = K} [S(\hat{\rho}^B) - S(\hat{\rho}^{E'})] \} \\ &= \max_{0 \leq K \leq g(\eta\bar{N})} \{ K - \min_{\langle \hat{a}^\dagger \hat{a} \rangle \leq \bar{N}, S(\hat{\rho}^B) = K} [S(\hat{\rho}^{E'})] \} \\ &= \max_{0 \leq K \leq g(\eta\bar{N})} \{ K - g[(1-\eta)g^{-1}(K)/\eta] \} \\ &= g(\eta\bar{N}) - g((1-\eta)\bar{N}) \text{ nats/use} \\ &= Q^{(1)}(\mathcal{N}_{A-B}). \end{aligned} \quad (12)$$

The first equality above follows from Lemma 3 of [9]. The second equality follows from \mathcal{N}_{A-BE} being a degraded channel. The restriction to $0 \leq K \leq g(\eta\bar{N})$ in the third equality is permissible because $\max_{\langle \hat{a}^\dagger \hat{a} \rangle \leq \bar{N}} S(\hat{\rho}^B) = g(\eta\bar{N})$. The fifth equality follows⁴ from minimum output entropy conjecture 2 (see Sec. V). The $\hat{\rho}^B$ that achieves this equality is a thermal state, which is realized when Alice employs coherent-state encoding with a zero-mean isotropic Gaussian prior distribution $p_A(\alpha) = (1/\pi K) \exp(-|\alpha|^2/K)$. The sixth equality now follows from $g(x) - g(cx)$ being a monotonically increasing function of $x \geq 0$, for c a constant satisfying $0 \leq c < 1$, and the equality to the single-letter quantum capacity follows from Eq. (11). Note that the privacy capacity of this channel is zero when $\eta \leq 1/2$. It is straightforward to show that in the limit of high input photon number \bar{N} ,

$$C_p(\mathcal{N}_{A-BE}) = Q^{(1)}(\mathcal{N}_{A-B}) = \max\{0, \ln(\eta) - \ln(1-\eta)\},$$

a result that Wolf et. al. [10] independently derived by a different approach without use of an unproven output entropy conjecture.

IV. THE ENTROPY PHOTON-NUMBER INEQUALITY (EPNI)

A. The Entropy Power Inequality

Let \mathbf{X} and \mathbf{Y} be statistically independent, n -dimensional, real-valued random vectors that possess differential (Shannon) entropies $h(\mathbf{X})$ and $h(\mathbf{Y})$ respectively. Because a real-valued, zero-mean Gaussian random variable U has differential entropy given by $h(U) = \ln(2\pi e \langle U^2 \rangle)$, where the mean-squared value, $\langle U^2 \rangle$, is considered to be the *power* of U , the entropy powers of \mathbf{X} and \mathbf{Y} are taken to be

$$P(\mathbf{X}) \equiv \frac{e^{h(\mathbf{X})/n}}{2\pi e} \quad \text{and} \quad P(\mathbf{Y}) \equiv \frac{e^{h(\mathbf{Y})/n}}{2\pi e}. \quad (13)$$

⁴Here, $g^{-1}(S)$ is the inverse of the function $g(N)$. Because $g(N)$ for $N \geq 0$ is a non-negative, monotonically increasing, concave function of N , it has an inverse, $g^{-1}(S)$ for $S \geq 0$, that is non-negative, monotonically increasing, and convex.

In this way, an n -dimensional, real-valued, random vector $\tilde{\mathbf{X}}$ comprised of independent, identically distributed (i.i.d.), real-valued, zero-mean, variance- $P(\mathbf{X})$, Gaussian random variables has differential entropy $h(\tilde{\mathbf{X}}) = h(\mathbf{X})$. We can similarly define an i.i.d. Gaussian random vector $\tilde{\mathbf{Y}}$ with differential entropy $h(\tilde{\mathbf{Y}}) = h(\mathbf{Y})$. We define a new random vector by the convex combination

$$\mathbf{Z} \equiv \sqrt{\eta} \mathbf{X} + \sqrt{1-\eta} \mathbf{Y}, \quad (14)$$

where $0 \leq \eta \leq 1$. This random vector has differential entropy $h(\mathbf{Z})$ and entropy power $P(\mathbf{Z})$. Furthermore, let $\tilde{\mathbf{Z}} \equiv \sqrt{\eta} \tilde{\mathbf{X}} + \sqrt{1-\eta} \tilde{\mathbf{Y}}$. Three equivalent forms of the Entropy Power Inequality (EPI), see, e.g., [11], are then:

$$P(\mathbf{Z}) \geq \eta P(\mathbf{X}) + (1-\eta)P(\mathbf{Y}) \quad (15)$$

$$h(\mathbf{Z}) \geq h(\tilde{\mathbf{Z}}) \quad (16)$$

$$h(\mathbf{Z}) \geq \eta h(\mathbf{X}) + (1-\eta)h(\mathbf{Y}). \quad (17)$$

B. The Entropy Photon-Number Inequality

Let $\hat{\mathbf{a}} = [\hat{a}_1 \hat{a}_2 \cdots \hat{a}_n]$ and $\hat{\mathbf{b}} = [\hat{b}_1 \hat{b}_2 \cdots \hat{b}_n]$ be vectors of photon annihilation operators for a collection of $2n$ different electromagnetic field modes of frequency ω [12]. The joint state of the modes associated with $\hat{\mathbf{a}}$ and $\hat{\mathbf{b}}$ is given by the product-state density operator $\hat{\rho}_{ab} = \hat{\rho}_a \otimes \hat{\rho}_b$, where $\hat{\rho}_a$ and $\hat{\rho}_b$ are the density operators associated with the $\hat{\mathbf{a}}$ and $\hat{\mathbf{b}}$ modes, respectively. The von Neumann entropies of the $\hat{\mathbf{a}}$ and $\hat{\mathbf{b}}$ modes are $S(\hat{\rho}_a) = -\text{tr}[\hat{\rho}_a \ln(\hat{\rho}_a)]$ and $S(\hat{\rho}_b) = -\text{tr}[\hat{\rho}_b \ln(\hat{\rho}_b)]$.

The thermal state of a mode with annihilation operator \hat{a} has two equivalent definitions:

$$\hat{\rho}_T = \int d^2\alpha \frac{e^{-|\alpha|^2/N}}{\pi N} |\alpha\rangle\langle\alpha|, \quad (18)$$

and

$$\hat{\rho}_T = \sum_{i=0}^{\infty} \frac{N^i}{(N+1)^{i+1}} |i\rangle\langle i|, \quad (19)$$

where $N = \langle \hat{a}^\dagger \hat{a} \rangle$ is the average photon number. In Eq. (18), $|\alpha\rangle$ is the coherent state of amplitude α , i.e., it satisfies $\hat{a}|\alpha\rangle = \alpha|\alpha\rangle$, for α a complex number. In Eq. (19), $|i\rangle$ is the i -photon state, i.e., it satisfies $\hat{N}|i\rangle = i|i\rangle$, for $i = 0, 1, 2, \dots$, with $\hat{N} \equiv \hat{a}^\dagger \hat{a}$ being the photon number operator. Physically, Eq. (18) says that the thermal state is an isotropic Gaussian mixture of coherent states. Equation (19), on the other hand, says that the thermal state is a Bose-Einstein mixture of number states. From Eq. (19) we immediately have that $S(\hat{\rho}_T) = g(N)$, because the photon-number states are orthonormal.⁵

The entropy photon-numbers of the density operators $\hat{\rho}_a$ and $\hat{\rho}_b$ are defined as follows:

$$N(\hat{\rho}_a) \equiv g^{-1}(S(\hat{\rho}_a)/n) \text{ and } N(\hat{\rho}_b) \equiv g^{-1}(S(\hat{\rho}_b)/n). \quad (20)$$

Thus, if $\hat{\rho}_{\hat{\mathbf{a}}} \equiv \bigotimes_{i=1}^n \hat{\rho}_{T_{a_i}}$ and $\hat{\rho}_{\hat{\mathbf{b}}} \equiv \bigotimes_{i=1}^n \hat{\rho}_{T_{b_i}}$, where $\hat{\rho}_{T_{a_i}}$ is the thermal state of average photon number $N(\hat{\rho}_{a_i})$ for

the \hat{a}_i mode and $\hat{\rho}_{T_{b_i}}$ is the thermal state of average photon number $N(\hat{\rho}_{b_i})$ for the \hat{b}_i mode, then we have $S(\hat{\rho}_{\hat{\mathbf{a}}}) = S(\hat{\rho}_a)$ and $S(\hat{\rho}_{\hat{\mathbf{b}}}) = S(\hat{\rho}_b)$. We define a new vector of photon annihilation operators, $\hat{\mathbf{c}} = [\hat{c}_1 \hat{c}_2 \cdots \hat{c}_n]$, by the convex combination

$$\hat{\mathbf{c}} \equiv \sqrt{\eta} \hat{\mathbf{a}} + \sqrt{1-\eta} \hat{\mathbf{b}}, \quad \text{for } 0 \leq \eta \leq 1, \quad (21)$$

and use $\hat{\rho}_{\hat{\mathbf{c}}}$ to denote its density operator. This is equivalent to saying that \hat{c}_i is the output of a lossless beam splitter whose inputs, \hat{a}_i and \hat{b}_i , couple to that output with transmissivity η and reflectivity $1-\eta$, respectively.

We can now state two equivalent forms of our conjectured Entropy Photon-Number Inequality (EPnI) [13]:

$$N(\hat{\rho}_{\hat{\mathbf{c}}}) \geq \eta N(\hat{\rho}_a) + (1-\eta)N(\hat{\rho}_b) \quad (22)$$

$$S(\hat{\rho}_{\hat{\mathbf{c}}}) \geq S(\hat{\rho}_{\hat{\mathbf{c}}}), \quad (23)$$

where $\hat{\rho}_{\hat{\mathbf{c}}} \equiv \bigotimes_{i=1}^n \hat{\rho}_{T_{c_i}}$ with $\hat{\rho}_{T_{c_i}}$ being the thermal state of average photon number $\eta N(\hat{\rho}_a) + (1-\eta)N(\hat{\rho}_b)$ for \hat{c}_i .

V. MINIMUM OUTPUT ENTROPY CONJECTURES

By analogy with the classical EPI, we might expect there to be a third equivalent form of the quantum EPnI, viz.,

$$S(\hat{\rho}_{\hat{\mathbf{c}}}) \geq \eta S(\hat{\rho}_a) + (1-\eta)S(\hat{\rho}_b). \quad (24)$$

It is easily shown that (22) implies (24) [14], but we have not been able to prove the converse. Indeed, we suspect that the converse might be false. More important than whether or not (24) is equivalent to (22) and (23), is the role of the EPnI in proving classical information capacity results for bosonic channels. In particular, the EPnI provides simple proofs of the following two minimum output entropy conjectures. These conjectures are important because proving minimum output entropy conjecture 1 also proves the conjectured capacity of the thermal-noise channel [2], and proving minimum output entropy conjecture 2 also proves the conjectured capacity region of the bosonic broadcast channel [4]. Furthermore, as we have shown above, proving minimum output entropy conjecture 2 also establishes the privacy capacity of the bosonic wiretap channel and the single-letter quantum capacity of the lossy bosonic channel.

Minimum Output Entropy Conjecture 1 — Let \mathbf{a} and \mathbf{b} be n -dimensional vectors of annihilation operators, with joint density operator $\hat{\rho}_{ab} = (|\psi\rangle_{\mathbf{a}\mathbf{a}}\langle\psi|) \otimes \hat{\rho}_{\mathbf{b}}$, where $|\psi\rangle_{\mathbf{a}}$ is an arbitrary zero-mean-field pure state of the \mathbf{a} modes and $\hat{\rho}_{\mathbf{b}} = \bigotimes_{i=1}^n \hat{\rho}_{T_{b_i}}$ with $\hat{\rho}_{T_{b_i}}$ being the \hat{b}_i mode's thermal state of average photon number K . Define a new vector of photon annihilation operators, $\hat{\mathbf{c}} = [\hat{c}_1 \hat{c}_2 \cdots \hat{c}_n]$, by the convex combination (21) and use $\hat{\rho}_{\hat{\mathbf{c}}}$ to denote its density operator and $S(\hat{\rho}_{\hat{\mathbf{c}}})$ to denote its von Neumann entropy. Then choosing $|\psi\rangle_{\mathbf{a}}$ to be the n -mode vacuum state minimizes $S(\hat{\rho}_{\hat{\mathbf{c}}})$.

Minimum Output Entropy Conjecture 2 — Let \mathbf{a} and \mathbf{b} be n -dimensional vectors of annihilation operators with joint density operator $\hat{\rho}_{ab} = (|\psi\rangle_{\mathbf{a}\mathbf{a}}\langle\psi|) \otimes \hat{\rho}_{\mathbf{b}}$, where $|\psi\rangle_{\mathbf{a}} = \bigotimes_{i=1}^n |0\rangle_{a_i}$ is the n -mode vacuum state and $\hat{\rho}_{\mathbf{b}}$ has von

⁵The coherent states, $\{|\alpha\rangle\}$, are *not* orthonormal, but rather overcomplete.

Neumann entropy $S(\hat{\rho}_b) = ng(K)$ for some $K \geq 0$. Define a new vector of photon annihilation operators, $\hat{c} = [\hat{c}_1 \hat{c}_2 \cdots \hat{c}_n]$, by the convex combination (21) and use $\hat{\rho}_c$ to denote its density operator and $S(\hat{\rho}_c)$ to denote its von Neumann entropy. Then choosing $\hat{\rho}_b = \bigotimes_{i=1}^n \hat{\rho}_{T_{b_i}}$ with $\hat{\rho}_{T_{b_i}}$ being the \hat{b}_i mode's thermal state of average photon number K minimizes $S(\hat{\rho}_c)$.

To see that the EPnI encompasses both of the preceding minimum output entropy conjectures is our final task in this paper. We begin by using the premise of conjecture 1 in (22). Because the \hat{a} modes are in a pure state, we get $S(\hat{\rho}_a) = 0$ and hence the EPnI tells us that

$$N(\hat{\rho}_c) \geq (1 - \eta)N(\hat{\rho}_b) = (1 - \eta)K. \quad (25)$$

Taking $g(\cdot)$ on both sides of this inequality, we get $S(\hat{\rho}_c)/n \geq g[(1 - \eta)K]$. But, if $|\psi\rangle_a$ is the n -mode vacuum state, we can easily show that $\hat{\rho}_c = \bigotimes_{i=1}^n \hat{\rho}_{T_{c_i}}$, with $\hat{\rho}_{T_{c_i}}$ being the \hat{c}_i mode's thermal state of average photon number $(1 - \eta)K$. Thus, when $|\psi\rangle_a$ is the n -mode vacuum state we get $S(\hat{\rho}_c) = ng[(1 - \eta)K]$, which completes the proof.

Next, we apply the premise of conjecture 2 in (22). Once again, the \hat{a} modes are in a pure state, so we get

$$N(\hat{\rho}_c) \geq (1 - \eta)N(\hat{\rho}_b) = (1 - \eta)K, \quad (26)$$

and hence $S(\hat{\rho}_c)/n \geq g[(1 - \eta)K]$. But, taking $\hat{\rho}_b = \bigotimes_{i=1}^n \hat{\rho}_{T_{b_i}}$, with $\hat{\rho}_{T_{b_i}}$ being the \hat{b}_i mode's thermal state of average photon number K , satisfies the premise of minimum output entropy conjecture 2 and implies that $\hat{\rho}_c = \bigotimes_{i=1}^n \hat{\rho}_{T_{c_i}}$, with $\hat{\rho}_{T_{c_i}}$ being the \hat{c}_i mode's thermal state of average photon number $(1 - \eta)K$. In this case we have $S(\hat{\rho}_c) = ng[(1 - \eta)K]$, which completes the proof.

VI. CONCLUSION

We conjectured a quantum version of the classical entropy power inequality, which subsumes two minimum output entropy conjectures that prior work has shown to be sufficient to prove the capacity of the point-to-point thermal-noise lossy bosonic channel, and the bosonic broadcast channel respectively [2], [4]. Even though proving this more general inequality—the Entropy Photon-number Inequality (EPnI)—might seem harder than the two minimum output entropy conjectures, there is a possibility of drawing parallels from the proofs of the classical entropy power inequality [11]. In this paper, we have also shown that the EPnI also implies the proof of the privacy capacity of the bosonic wiretap channel. Furthermore, using a result from [9], we have that the degraded nature of the bosonic wiretap channel implies that its privacy capacity equals the single-letter quantum capacity of the lossy bosonic channel. Moreover, both of these capacities are achieved by coherent-state encoding using an isotropic Gaussian prior.

ACKNOWLEDGEMENTS

This research was supported by the W. M. Keck Foundation Center for Extreme Quantum Information Theory.

REFERENCES

- [1] V. Giovannetti, S. Guha, S. Lloyd, L. Maccone, J. H. Shapiro, and H. P. Yuen, "Classical capacity of lossy bosonic channels: the exact solution," *Phys. Rev. Lett.* **92**, 027902 (2004).
- [2] V. Giovannetti, S. Guha, S. Lloyd, L. Maccone, J. H. Shapiro, B. J. Yen, and H. P. Yuen, "Classical capacity of free-space optical communication," in O. Hirota, ed., *Quantum Information, Statistics, Probability*, (Rinton Press, New Jersey, 2004) pp. 90–101.
- [3] V. Giovannetti, S. Guha, S. Lloyd, L. Maccone, and J. H. Shapiro, "Minimum output entropy of bosonic channels: a conjecture," *Phys. Rev. A* **70**, 032315 (2004).
- [4] S. Guha, J. H. Shapiro, and B. I. Erkmen, "Classical capacity of bosonic broadcast communication and a minimum output entropy conjecture," *Phys. Rev. A* **76**, 032303 (2007).
- [5] A. D. Wyner, "The wiretap channel," *Bell. Sys. Tech. Jour.* **54**, 1355–1387 (1975).
- [6] I. Csiszár and J. Körner, "Broadcast channels with confidential messages," *IEEE Trans. Inform. Theory* **23**, 339–348, (1978).
- [7] I. Devetak, "The private classical capacity and quantum capacity of a quantum channel," arXiv:quant-ph/0304127v6.
- [8] A. S. Holevo, "The capacity of a quantum channel with general input states," *IEEE Trans. Inform. Theory* **44**, 269–273 (1998); P. Hausladen, R. Jozsa, B. Schumacher, M. Westmoreland, and W. K. Wootters, "Classical information capacity of a quantum channel," *Phys. Rev. A* **54**, 1869–1876 (1996); B. Schumacher and M. D. Westmoreland, "Sending classical information via noisy quantum channels," *Phys. Rev. A* **56**, 131–138 (1997).
- [9] G. Smith, "The private classical capacity with a symmetric side channel and its application to quantum cryptography," arXiv:quant-ph/0705.3838.
- [10] M. M. Wolf, D. Pérez-García, G. Giedke, "Quantum capacities of bosonic channels," arXiv:quant-ph/0606132.
- [11] O. Rioul, "Information theoretic proofs of entropy power inequalities," arXiv:cs.IT/07041751.
- [12] L. Mandel and E. Wolf, *Optical Coherence and Quantum Optics*, (Cambridge University Press, Cambridge, 1995).
- [13] To show that (22) implies (23), assume (22) is true:

$$N(\hat{\rho}_c) \geq \eta N(\hat{\rho}_a) + (1 - \eta)N(\hat{\rho}_b) \quad (27)$$

$$= \eta N(\hat{\rho}_{\bar{a}}) + (1 - \eta)N(\hat{\rho}_{\bar{b}}) \quad (28)$$

Now, if $\hat{\rho}_{\bar{a}\bar{b}} = \hat{\rho}_{\bar{a}} \otimes \hat{\rho}_{\bar{b}}$ is the joint density operator of the \hat{a} and \hat{b} modes, we find that the state of the \hat{c} modes is $\hat{\rho}_{\bar{c}} \equiv \bigotimes_{i=1}^n \hat{\rho}_{T_{c_i}}$, where $\hat{\rho}_{T_{c_i}}$ is a thermal state with average photon number given by $N(\hat{\rho}_{\bar{c}}) = \eta N(\hat{\rho}_{\bar{a}}) + (1 - \eta)N(\hat{\rho}_{\bar{b}})$, so that $S(\hat{\rho}_{\bar{c}}) = ng[N(\hat{\rho}_{\bar{c}})]$. Thus, from (28) we get $N(\hat{\rho}_c) \geq N(\hat{\rho}_{\bar{c}}) = g^{-1}(S(\hat{\rho}_{\bar{c}})/n)$. Taking $g(\cdot)$ of both sides of this inequality completes the proof.

To show that (23) implies (22), assume (23) is true:

$$\begin{aligned} N(\hat{\rho}_c) &= g^{-1}(S(\hat{\rho}_c)/n) \\ &\geq g^{-1}(S(\hat{\rho}_{\bar{c}})/n) = g^{-1}[g(\eta N(\hat{\rho}_{\bar{a}}) + (1 - \eta)N(\hat{\rho}_{\bar{b}}))] \\ &= \eta N(\hat{\rho}_{\bar{a}}) + (1 - \eta)N(\hat{\rho}_{\bar{b}}) \\ &= \eta N(\hat{\rho}_a) + (1 - \eta)N(\hat{\rho}_b), \end{aligned} \quad (29)$$

where the inequality is due to $g^{-1}(S)$ being a monotonically increasing function of S , and the proof is complete.

- [14] Assume that (22) is true. We then have that $N(\hat{\rho}_c) \geq \eta N(\hat{\rho}_a) + (1 - \eta)N(\hat{\rho}_b)$, so that

$$S(\hat{\rho}_c) = ng[N(\hat{\rho}_c)] \geq ng[\eta N(\hat{\rho}_a) + (1 - \eta)N(\hat{\rho}_b)] \quad (30)$$

$$\geq \eta ng[N(\hat{\rho}_a)] + (1 - \eta)ng[N(\hat{\rho}_b)] \quad (31)$$

$$= \eta S(\hat{\rho}_a) + (1 - \eta)S(\hat{\rho}_b), \quad (32)$$

where the second inequality follows from $g(N)$ being concave, and the proof is complete.