Information Trade-Offs for Optical Quantum Communication

Mark M. Wilde,[1] Patrick Hayden,[1] and Saikat Guha[2]

[1]School of Computer Science, McGill University, Montreal, Québec H3A 2A7, Canada

[2]Disruptive Information Processing Technologies Group, Raytheon BBN Technologies, Cambridge, Massachusetts 02138, USA

(Received 26 September 2011; revised manuscript received 24 January 2012; published 2 April 2012)

Recent work has precisely characterized the achievable trade-offs between three key information processing tasks—classical communication (generation or consumption), quantum communication (generation or consumption), and shared entanglement (distribution or consumption), measured in bits, qubits, and ebits per channel use, respectively. Slices and corner points of this three-dimensional region reduce to well-known protocols for quantum channels. A trade-off coding technique can attain any point in the region and can outperform time sharing between the best-known protocols for accomplishing each information processing task by itself. Previously, the benefits of trade-off coding that had been found were too small to be of practical value (viz., for the dephasing and the universal cloning machine channels). In this Letter, we demonstrate that the associated performance gains are in fact remarkably high for several physically relevant bosonic channels that model free-space or fiber-optic links, thermal-noise channels, and amplifiers. We show that significant performance gains from trade-off coding also apply when trading photon-number resources between transmitting public and private classical information simultaneously over secret-key-assisted bosonic channels.

DOI: 10.1103/PhysRevLett.108.140501 PACS numbers: 03.67.Hk, 03.67.Pp, 04.62.+v

Shannon's classical information theory found the capacity of a classical channel, which quantifies the channel's ability to transmit information [1]. The capacity serves as a benchmark against which communication engineers can test the performance of any practical scheme. Despite the success of Shannon's theory, it fails to identify the true capacity for physical channels such as free-space or fiber-optic links because the quantum physical properties of the optical-frequency electromagnetic waves—the carriers of information—must be accounted for within a full quantum framework in order to assess the ultimate limits on reliable communication [2]. A major revision of Shannon's information theory, dubbed quantum Shannon theory, has emerged in recent years in an attempt to determine the ultimate physical limits on communications [3]. This theory has provided a successful quantum theory of information in many special cases [4–8], but recent developments have indicated that there is much more to understand regarding the nature of information transmission over quantum channels [9,10].

Quantum channels support a richer variety of information processing tasks than do classical channels. A sender can transmit classical information, such as "on" or "off" [11–13], or she can transmit quantum information, such as the quantum state of a photon [14–16]. Additionally, if the sender and receiver have prior shared entanglement, this resource can boost the rate of information transmission [17], generalizing the superdense coding effect [18]. The sender might also want to transmit classical and quantum information simultaneously to the receiver [6], or even limit the amount of entanglement consumed in the entanglement-assisted transmission of classical and/or quantum information [19]. The sender and receiver could further specify whether they would like the classical information to be public or private [20].

In a "trade-off" communication problem, such as that of simultaneous classical-quantum communication, a naive strategy of time sharing would have the sender and receiver use a classical communication protocol for some fraction of the time (say, the best Holevo-Schumacher-Westmoreland (HSW) classical code and a joint-detection receiver on long code word blocks [11–13]), while operating with a quantum communication protocol for the other fraction of the time (say, the best Lloyd-Shor-Devetak (LSD) quantum code and a joint-detection receiver on quantum code words [14–16]). Trade-off coding is a more complex strategy, in which—simply stated—the sender encodes classical information into the many different ways of permuting quantum codes. Its performance can beat that of time sharing for certain channels such as dephasing and universal cloning machine channels, for which it is even provably optimal [6,21–23]. The original [3,6,19] and subsequent developments [22,24] on trade-off coding have greatly enhanced our understanding of communication over quantum channels. However, the pay-off of trade-off coding for the channels studied previously was too small to be worthwhile in a practical setting, given the increased encoding and decoding complexity over time sharing.

In this Letter, we show that trade-off coding yields remarkable gains over time sharing for the single-mode lossy bosonic channel, which can model free-space optical communication. These single-mode results are sufficient to construct trade-off capacity results for any physical optical

communication channel that modulates multiple degrees of freedom of the photon, such as spatial and polarization modes of light. Our results also apply more generally to thermal-noise and amplifying bosonic channels, which can model systems as diverse as superconducting transmission lines in the microwave range [25] or hybrid quantum memories that store both classical and quantum information in the collective degrees of freedom of atomic ensembles [26]. We determine an achievable rate region for the lossy bosonic channel using a transmitter that modulates the two-mode squeezed vacuum—an entangled light state that can be generated using parametric down-conversion—and prove that this rate region is optimal, assuming that a long-standing minimum-output entropy conjecture is true [27–30]. Even if the conjecture is not true, our achievable trade-off region beats time sharing between the best-known quantum communication protocols by huge margins. The same holds for the thermal and amplifying channels.

Trading quantum and classical resources.—Our first result concerns the transmission of classical and quantum information over a single-mode lossy bosonic channel of input-output power transmissivity $\eta \in (0, 1]$, with a constraint on the mean photon number N_S per mode at the transmitter. Recall that this channel has the following input-output Heisenberg-picture specification: $\hat{b} = \sqrt{\eta}\hat{a} + \sqrt{1-\eta}\hat{e}$, where $\hat{a}$, $\hat{b}$, and $\hat{e}$ are the respective bosonic annihilation operators representing the sender's input mode, the receiver's output mode, and an environmental input in the vacuum state. Transmission over this channel can also be used to generate shared entanglement between the sender and the receiver, or this resource might assist transmission if they share it beforehand. We let C be the rate of classical communication, Q be the rate of quantum communication, and E be the rate of entanglement generation (or consumption). If the rate of a resource is positive, then the interpretation is that the protocol generates that resource. Otherwise, the protocol consumes that resource.

Hsieh and Wilde described a general-purpose protocol for entanglement-assisted communication of classical and quantum information over many independent uses of *any* noisy quantum channel [24] and subsequently found the full (C, Q, E) triple trade-off region [21,31]. The Hsieh-Wilde protocol is constructed from a particular ensemble $\{p_X(x), \rho_x\}$ and the channel $\mathcal{N}$. Let $|\phi_x\rangle$ denote a purification of ρ_x, let $\rho \equiv \sum_x p_X(x)\rho_x$ be the average density operator of the ensemble, let $\mathcal{N}^c$ be the channel complementary to $\mathcal{N}$ [32], and let $H(\sigma) \equiv -\mathrm{Tr}(\sigma \log_2 \sigma)$ be the von Neumann entropy. Then, the Hsieh-Wilde protocol generates $H[\mathcal{N}(\rho)] - \sum_x p_X(x) H(\rho_x)$ bits per channel use and $\sum_x p_X(x)\{H(\rho_x) + H[\mathcal{N}(\rho_x)] - H[\mathcal{N}^c(\rho_x)]\}/2$ qubits per channel use by consuming $\sum_x p_X(x)\{H(\rho_x) + H[\mathcal{N}^c(\rho_x)] - H[\mathcal{N}(\rho_x)]\}/2$ ebits per channel use [24]. This protocol is a trade-off coding protocol, in the sense that encoded classical and quantum data can be fed into the same channel input, rather than into separate channel inputs, as is the case in a time sharing protocol that allocates a portion of the channel uses solely for classical data transmission and the other portion solely for quantum data transmission. Figure 1 depicts an example operation of this protocol in the case where there is no entanglement assistance. Combining the Hsieh-Wilde protocol with teleportation, superdense coding, and entanglement distribution (while keeping track of net rates) gives the following achievable rate region [21]:

$$\begin{aligned} C + 2Q &\leq H[N(\rho)] + \sum_x p(x)\{H(\rho_x) - H[\mathcal{N}^c(\rho_x)]\}, \\ Q + E &\leq \sum_x p(x)\{H[N(\rho_x)] - H[\mathcal{N}^c(\rho_x)]\}, \\ C + Q + E &\leq H[\mathcal{N}(\rho)] - \sum_x p(x) H[\mathcal{N}^c(\rho_x)]. \end{aligned} \tag{1}$$

Hsieh and Wilde also proved a multiletter converse, so that the above region's regularization is optimal [21,31].

For the lossy bosonic channel, the Hsieh-Wilde protocol and rate region translate to the following. The protocol is constructed from an ensemble of Gaussian-distributed phase-space displacements of two-mode squeezed vacuum

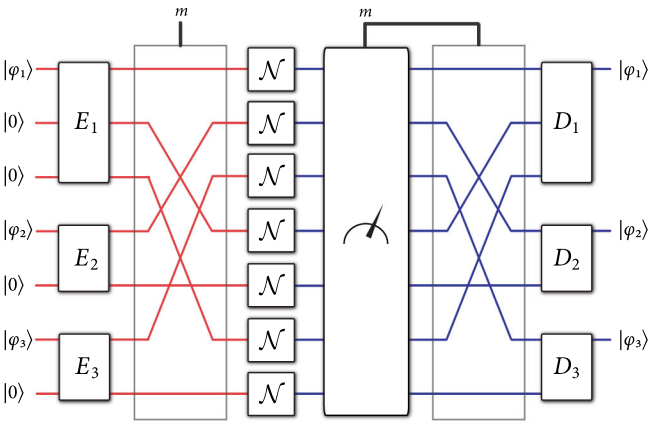

FIG. 1 (color online). A sketch of the trade-off coding protocol for communication of classical and quantum information without any entanglement assistance (this case is the Devetak-Shor protocol [6]). The sender begins by encoding qubits $|\varphi_1\rangle$, $|\varphi_2\rangle$, and $|\varphi_3\rangle$ into different quantum error-correcting codes, each constructed from a particular state $|\phi_x\rangle$ and the channel $\mathcal{N}$. To encode classical information, the sender permutes the quantum systems emerging from the outputs of the encoders according to some classical message m. The sender then transmits these systems through many independent uses of the noisy channel $\mathcal{N}$. The receiver obtains the outputs of channels and performs an HSW measurement to determine the classical message m. If the success probability of the measurement is asymptotically close to 1, then it causes an asymptotically negligible disturbance to the state on which it acts. The receiver then knows the permutation, unpermutes the quantum systems, and exploits the decoders of the quantum error-correcting codes to decode the qubits $|\varphi_1\rangle$, $|\varphi_2\rangle$, and $|\varphi_3\rangle$. The Wilde-Hsieh protocol [31] extends this idea by permuting entanglement-assisted quantum codes in a similar way.

(TMSV) states: $\{p_{\bar{\lambda}N_S}(\alpha), D^{A'}(\alpha)|\psi_{\mathrm{TMSV}}\rangle^{AA'}\}$, where A' is a system sent into the channel input and A is a system that purifies A'. [In the above, the distribution $p_{\bar{\lambda}N_S}(\alpha)$ replaces $p_X(x)$, and the state $D^{A'}(\alpha)|\psi_{\mathrm{TMSV}}\rangle^{AA'}$ replaces $|\phi_x\rangle$.] The distribution $p_{\bar{\lambda}N_S}(\alpha) \equiv \frac{1}{\pi\bar{\lambda}N_S}\exp\{-|\alpha|^2/\bar{\lambda}N_S\}$ is an isotropic Gaussian distribution with variance $\bar{\lambda}N_S$, where $\bar{\lambda} \equiv 1-\lambda$ and $\lambda \in [0,1]$ is a photon-number-sharing parameter. The state $|\psi_{\mathrm{TMSV}}\rangle^{AA'}$ is a two-mode squeezed vacuum [33,34]:

$$|\psi_{\mathrm{TMSV}}\rangle^{AA'} \equiv \sum_{n=0}^{\infty}\sqrt{[\lambda N_S]^n/[\lambda N_S+1]^{n+1}}\,|n,n\rangle^{AA'}. \quad (2)$$

Evaluating the entropies in (1) for this ensemble and the lossy bosonic channel gives the following achievable rate region:

$$\begin{aligned} C+2Q &\le g(\lambda N_S)+g(\eta N_S)-g[(1-\eta)\lambda N_S],\\ Q+E &\le g(\eta\lambda N_S)-g[(1-\eta)\lambda N_S],\\ C+Q+E &\le g(\eta N_S)-g[(1-\eta)\lambda N_S], \end{aligned} \quad (3)$$

where N_S is the input mean photon number per mode (per channel use) and $g(N)$ is the entropy of a single-mode thermal state with mean photon number N: $g(N) \equiv (N+1)\log_2(N+1)-N\log_2 N$. The photon-number-sharing parameter λ is the fraction of photons the code dedicates to quantum resources as compared to classical resources. This allocation, however, is done within a single channel use (as a power-sharing strategy), whereas, in a time sharing strategy, each channel use is dedicated to only one task at a time. The above result extends to other important bosonic channels such as the thermal-noise and amplifier channels [35].

Note that $Q=0$ for $\eta<1/2$, thereby making the (C,Q) trade-off region trivial for $\eta<1/2$. However, for the (C,E) trade-off with $C\ge 0$ and $E\le 0$, trade-off coding with the Hsieh-Wilde protocol outperforms time sharing for all values of η.

If $\eta \ge 1/2$ and the minimum-output entropy conjecture is true, then the rate region defined by (3) is the actual capacity region [35]. Our proof of optimality is similar to the optimality proof for the bosonic broadcast channel [29], a setting in which a sender, at one input port of a beam splitter, transmits classical data to two receivers at the two output ports. For the noiseless broadcast channel, the second beam splitter input is in the vacuum state. In the broadcast setting, there is always one receiver whose output is less noisy than the other's (whichever receiver has the output for which $\eta \ge 1/2$). The techniques for proving optimality of rates to the less noisy receiver readily apply when analyzing our setting [35], but we require $\eta \ge 1/2$ in order to apply them because there is only one receiver in our setting.

Figure 2 depicts two important special cases of the region in (3): (a) the trade-off between classical and quantum communication without entanglement assistance and (b) the trade-off between entanglement-assisted and unassisted classical communication. The figure indicates the remarkable improvement over time sharing that trade-off coding achieves for the lossy bosonic channel. If N_S is high enough to achieve close to the maximum quantum capacity $\log_2(\eta)-\log_2(1-\eta)$, then the achievable rates in (3) are much better than those achievable by time sharing between its quantum capacity [8], its classical capacity [7], and its entanglement-assisted classical and quantum capacities [17,36,37].

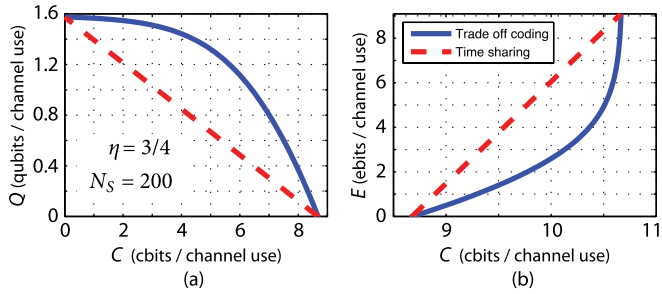

FIG. 2 (color online). (a) The (C,Q) trade-off: A lossy bosonic channel with transmissivity $\eta = 3/4$ can reliably transmit a maximum of $\log_2(3/4)-\log_2(1/4) \approx 1.58$ qubits per channel use [8], and $N_S = 200$ photons per mode at the channel input is sufficient to nearly achieve this quantum capacity. A trade-off coding strategy that lowers the quantum data rate to about 1.4 qubits per use while retaining the same mean photon budget allows the transmission of an additional 4.5 classical bits per channel use, while time sharing would only allow for an additional 1 classical bit per channel use with this photon budget. (b) The (C,E) trade-off: The sender and the receiver share entanglement, and the sender would like to transmit classical information while minimizing the consumption of entanglement. With a mean photon budget of $N_S = 200$ photons per channel use, the sender can reliably transmit a maximum of about 10.7 classical bits per channel use while consuming entanglement at a rate of about 9.1 entangled bits per channel use [17,36,37]. With trade-off coding, the sender can significantly reduce the entanglement consumption rate to about 5 entangled bits per channel use while still transmitting about 10.5 classical bits per channel use, i.e., only a 0.08 dB decrease in the rate of classical communication for a 2.6 dB decrease in the entanglement consumption rate.

A rule of thumb for trade-off coding.—The quantum capacity of a lossy bosonic channel with transmissivity η and mean photon number per mode N_S is given by $Q(\eta,N_S) = \max\{0, g(\eta N_S)-g[(1-\eta)N_S]\}$ [8,36,38]. Note that $Q(\eta,N_S)=0$, $\forall\ \eta \le 1/2$, and $\lim_{N_S\to\infty} Q(\eta,N_S) = \log_2(\eta)-\log_2(1-\eta) \equiv Q_{\max}(\eta)$. In the context of trade-off coding, the achievable rate becomes $Q(\eta,\lambda N_S)$, where λ is the fraction of photons dedicated to quantum resources. A Taylor series expansion yields $Q(\eta,\lambda N_S) \ge Q_{\max}(\eta)-[\eta(1-\eta)\lambda N_S \ln 2]^{-1}$ when N_S is sufficiently high [35]. Thus, in order to reach the quantum capacity to within ϵ bits, a trade-off code should dedicate no more than a fraction

$\lambda^* = 1/[\eta(1-\eta)\epsilon N_S \ln 2]$ to the quantum part of the code. If the trade-off code dedicates a higher fraction of the photons than λ^* to quantum resources, then it is effectively wasting photons which could instead be used to get a significant amount of classical communication "for free." As N_S increases, the fraction of available photons needed for the quantum rate to saturate at $Q_{\max}(\eta)$ becomes smaller and smaller. So, if a trade-off code abides by the above rule of thumb, it will nearly saturate $Q_{\max}(\eta)$, while achieving a high classical data rate, as well—something that is *not* possible by merely time sharing between classical (HSW) and quantum (LSD) communication. A similar rule of thumb applies for entanglement-assisted classical communication; i.e., it is not necessary to dedicate a large fraction of the photons to shared entanglement when the photon budget increases [35].

Trading public and private classical resources.—Analogous trade-off coding results hold for another notable setting, where a sender would like to transmit both public and private classical information to a receiver over a bosonic channel (perhaps even with the assistance of a secret key). These results constitute a relevant benchmark for satellite-to-satellite (far-field free-space) links, which might be used for both public communication and quantum key distribution [39]. We let R denote the rate of public communication, P the rate of private communication, and S the rate of secret key generation/consumption. An achievable rate region for the lossy bosonic channel with $\eta \in [0, 1]$ is

$$\begin{aligned} R + P &\leq g(\eta N_S), \\ P + S &\leq g(\eta\lambda N_S) - g[(1-\eta)\lambda N_S], \\ R + P + S &\leq g(\eta N_S) - g[(1-\eta)\lambda N_S], \end{aligned} \tag{4}$$

where $\lambda \in [0, 1]$, a photon-number-sharing parameter, is the fraction of photons dedicated to private classical resources and N_S is the mean input photon number per mode. If $\eta \geq 1/2$ and the minimum-output entropy conjecture is true, then this region is the capacity region [35]. We were able to prove optimality here again by appealing to the optimality results from the bosonic broadcast channel [38]. For $\eta < 1/2$, the above region remains achievable. The strategy for achieving the above rate region is to combine the general-purpose Hsieh-Wilde protocol for secret-key-assisted communication of public and private classical information [20] and combine it with the one-time pad, secret key distribution, and private-to-public transmission (the ideas here are similar to those for the CQE trade-off). For the lossy bosonic channel, coherent-state code words with each symbol selected according to an isotropic Gaussian distribution suffice to achieve the above region [35].

An interesting special case of the above achievable region is the trade-off between public and private classical communication. Lemma 3 of Ref. [20] proves that the classical-quantum trade-off region is the same as the public-private trade-off whenever the channel is degradable, which applies here since the lossy bosonic channel is degradable whenever $\eta \geq 1/2$ [8,38]. These special cases coincide because ensembles of pure states suffice for achieving the private classical capacity of degradable channels [20], further implying in such a case that the private information is equivalent to the coherent information. Thus, Fig. 2(a) doubles as a plot of the public-private trade-off ($C \to R$, $Q \to P$). Furthermore, note that the trade-off between public classical communication and secret key generation is the same as that between public and private classical communication, respectively.

Discussion.—We might attempt to understand why trade-off coding between classical and quantum communication performs so well for bosonic channels in the high photon-number regime by making an analogy with qubit dephasing channels. It is well-known that, for every $\eta < 1$, the lossy bosonic channel has a finite quantum capacity even when an infinite number of photons are available [36]. Here, we have seen that we can approach this quantum capacity with just a small fraction of the total photon number dedicated to the quantum part of the code. Thus, one can think loosely of the lossy bosonic channel as being "composed of" a few channels that are good for quantum transmission while the rest are good for classical transmission. The analogy is that we can combine many strongly dephasing channels that are only good for classical data transmission with just a few weakly dephasing channels that are good for quantum data transmission in order to approximate the lossy bosonic classical-quantum trade-off. References [6,22,24] prove that the trade-off capacity region of any dephasing channel is additive, and so the resulting region for the combined dephasing channel is simply the Minkowski sum of those of the individual channels. However, this understanding is only satisfying in the very high photon-number regime, when the available number of photons is much larger than that needed to saturate the quantum capacity.

Conclusion.—We have shown that achievable rates with trade-off coding over bosonic channels can be significantly higher than those achievable from time sharing between conventional quantum protocols, suggesting that quantum communication engineers should try to take advantage of these gains in a practical coding scheme. Our trade-off regions are optimal for a lossy bosonic channel that transmits on average over half of the photons input to it, assuming that the minimum-output entropy conjecture is true. This Letter does not discuss specific codes and structured optical receivers to attain reliable communications at rate triples predicted by our achievable trade-off region. In future work, it would be interesting to lay out the full transmitter-coding-receiver architecture for optical trade-off coding.

We thank J. H. Shapiro for reminding us of relevant results [29]. 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] J. H. Shapiro, IEEE J. Sel. Top. Quantum Electron. **15**, 1547 (2009).
[3] C. H. Bennett and P. W. Shor, Science **303**, 1784 (2004).
[4] J. Harrington and J. Preskill, Phys. Rev. A **64**, 062301 (2001).
[5] C. King, IEEE Trans. Inf. Theory **49**, 221 (2003).
[6] I. Devetak and P. W. Shor, Commun. Math. Phys. **256**, 287 (2005).
[7] V. Giovannetti, S. Guha, S. Lloyd, L. Maccone, J. H. Shapiro, and H. P. Yuen, Phys. Rev. Lett. **92**, 027902 (2004).
[8] M. M. Wolf, D. Pérez-García, and G. Giedke, Phys. Rev. Lett. **98**, 130501 (2007).
[9] G. Smith and J. Yard, Science **321**, 1812 (2008).
[10] M. B. Hastings, Nature Phys. **5**, 255 (2009).
[11] P. Hausladen, R. Jozsa, B. Schumacher, M. Westmoreland, and W. K. Wootters, Phys. Rev. A **54**, 1869 (1996).
[12] B. Schumacher and M. D. Westmoreland, Phys. Rev. A **56**, 131 (1997).
[13] A. S. Holevo, IEEE Trans. Inf. Theory **44**, 269 (1998).
[14] S. Lloyd, Phys. Rev. A **55**, 1613 (1997).
[15] P. W. Shor, MSRI, 2002 (unpublished).
[16] I. Devetak, IEEE Trans. Inf. Theory **51**, 44 (2005).
[17] C. H. Bennett, P. W. Shor, J. A. Smolin, and A. V. Thapliyal, IEEE Trans. Inf. Theory **48**, 2637 (2002).
[18] C. H. Bennett and S. J. Wiesner, Phys. Rev. Lett. **69**, 2881 (1992).
[19] P. W. Shor, Quantum Inf. Comput. **4**, 537 (2004).
[20] M. M. Wilde and M.-H. Hsieh, Quant. Info. Proc. (in press).
[21] M. M. Wilde and M.-H. Hsieh, Quant. Info. Proc. (in press).
[22] K. Brádler, P. Hayden, D. Touchette, and M. M. Wilde, Phys. Rev. A **81**, 062312 (2010).
[23] T. Jochym-O'Connor, K. Brádler, and M. M. Wilde, J. Phys. A **44**, 415306 (2011).
[24] M.-H. Hsieh and M. M. Wilde, IEEE Trans. Inf. Theory **56**, 4682 (2010).
[25] A. Wallraff, D. I. Schuster, A. Blais, L. Frunzio, R.-S. Huang, J. Majer, S. Kumar, S. M. Girvin, and R. J. Schoelkopf, Nature (London) **431**, 162 (2004).
[26] T. Chaneliere, D. N. Matsukevich, S. D. Jenkins, S.-Y. Lan, T. A. B. Kennedy, and A. Kuzmich, Nature (London) **438**, 833 (2005).
[27] V. Giovannetti, S. Guha, S. Lloyd, L. Maccone, and J. H. Shapiro, Phys. Rev. A **70**, 032315 (2004).
[28] V. Giovannetti, A. S. Holevo, S. Lloyd, and L. Maccone, J. Phys. A **43**, 415305 (2010).
[29] S. Guha, J. H. Shapiro, and B. I. Erkmen, Phys. Rev. A **76**, 032303 (2007).
[30] S. Guha, Ph.D. thesis, Massachusetts Institute of Technology, 2008.
[31] M.-H. Hsieh and M. M. Wilde, IEEE Trans. Inf. Theory **56**, 4705 (2010).
[32] Every quantum channel $\mathcal{N}$ has an isometric extension to a larger Hilbert space [6]. One could imagine this isometric extension arising operationally from a unitary interaction between the sender's input system and an environment initialized in some pure state. After the unitary acts on the joint state, one obtains the original noisy channel to the receiver by tracing over the environment system, and one obtains the complementary channel to the environment by tracing over the receiver's system.
[33] C. Gerry and P. Knight, *Introductory Quantum Optics* (Cambridge University Press, Cambridge, England, 2004).
[34] S. L. Braunstein and P. van Loock, Rev. Mod. Phys. **77**, 513 (2005).
[35] M. M. Wilde, P. Hayden, and S. Guha, arXiv:1105.0119 [Phys. Rev. A (to be published)].
[36] A. S. Holevo and R. F. Werner, Phys. Rev. A **63**, 032312 (2001).
[37] V. Giovannetti, S. Lloyd, L. Maccone, and P. W. Shor, Phys. Rev. Lett. **91**, 047901 (2003).
[38] S. Guha, J. H. Shapiro, and B. I. Erkmen, in *Proceedings of the IEEE International Symposium on Information Theory, Toronto, Ontario, Canada, 2008* (IEEE Xplore, Piscataway, NJ, 2008), p. 91.
[39] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dušek, N. Lütkenhaus, and M. Peev, Rev. Mod. Phys. **81**, 1301 (2009).