**AFRL-RI-RS-TM-2008-11**
**Final Technical Memorandum**
**March 2008**

# INFORMATION TRANSMISSION AND ENTANGLEMENT DISTRIBUTION OVER BOSONIC CHANNELS

**Massachusetts Institute of Technology**

**Sponsored by**
**Defense Advanced Research Projects Agency**
**DARPA Order No. AE14**



**AIR FORCE RESEARCH LABORATORY**
**INFORMATION DIRECTORATE**
**ROME RESEARCH SITE**
**ROME, NEW YORK**

# NOTICE AND SIGNATURE PAGE



AFRL-RI-RS-TM-2008-11 HAS BEEN REVIEWED AND IS APPROVED FOR PUBLICATION IN ACCORDANCE WITH ASSIGNED DISTRIBUTION STATEMENT.

FOR THE DIRECTOR:

| | |
|---|---|
| /s/ | /s/ |
| DONALD J. NICHOLSON<br>Work Unit Manager | JAMES A. COLLINS, Deputy Chief<br>Advanced Computing Division<br>Information Directorate |

| REPORT DOCUMENTATION PAGE | *Form Approved* **OMB No. 0704-0188** |
|---|---|



| **1. REPORT DATE** *(DD-MM-YYYY)* | **2. REPORT TYPE** | **3. DATES COVERED** *(From - To)* |
|---|---|---|
| MAR 2008 | Final | Sep 06 – Sep 07 |

**4. TITLE AND SUBTITLE**

INFORMATION TRANSMISSION AND ENTANGLEMENT DISTRIBUTION OVER BOSONIC CHANNELS

**5a. CONTRACT NUMBER**

**5b. GRANT NUMBER** FA8750-06-2-0069

**5c. PROGRAM ELEMENT NUMBER** 62304E

**6. AUTHOR(S)**

Jeffrey H. Shapiro

**5d. PROJECT NUMBER** INFO

**5e. TASK NUMBER** TR

**5f. WORK UNIT NUMBER** AN

**7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)**
Massachusetts Institute of Technology
77 Massachusetts Avenue
Cambridge MA 02139-4301

**8. PERFORMING ORGANIZATION REPORT NUMBER**

**9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)**

| | |
|---|---|
| AFRL/RITC | Defense Advanced Research Projects Agency |
| 525 Brooks Rd | 3701 North Fairfax Drive |
| Rome NY 13441-4505 | Arlington VA 22203-1714 |

**10. SPONSOR/MONITOR'S ACRONYM(S)**

**11. SPONSORING/MONITORING AGENCY REPORT NUMBER**
AFRL-RI-RS-TM-2008-11

**12. DISTRIBUTION AVAILABILITY STATEMENT**
*APPROVED FOR PUBLIC RELEASE; DISTRIBUTION UNLIMITED. PA# WPAFB 08-0942*

**13. SUPPLEMENTARY NOTES**

**14. ABSTRACT**
High-sensitivity photdetection systems have long been limited by noises of quantum-mechanical origin. Nevertheless, analyses and designs of optical communication systems have seldom employed fully quantum treatments. As a result, these works do not establish the ultimate limits on optical communication performance. This program established an inner bound on the capacity region for the Bosonic broadcast channel, and showed that this inner bound is in fact the capacity region if a new minimum output entropy conjecture is true. Evidence supporting this minimum output entropy conjecture was obtained, and its relation to a previous minimum output entropy conjecture — used in the capacity theorem for the single-user thermal-noise channel — was investigated. The Entropy Photon-Number Inequality, which is the quantum generalization of the classical Entropy Power Inequality, was posed and evidence supporting its validity was obtained. In other work, entanglement assistance was shown to be of no benefit in classical information transmission under a photon-number constraint unless burst-mode communication is considered.

**15. SUBJECT TERMS**
Optical communication, channel capacity, quantum information, minimum output entropy

| **16. SECURITY CLASSIFICATION OF:** | | | **17. LIMITATION OF ABSTRACT** | **18. NUMBER OF PAGES** | **19a. NAME OF RESPONSIBLE PERSON** Donald J. Nicholson |
|---|---|---|---|---|---|
| **a. REPORT** | **b. ABSTRACT** | **c. THIS PAGE** | | | **19b. TELEPHONE NUMBER** (*Include area code*) |
| U | U | U | UU | 9 | N/A |

**Standard Form 298 (Rev. 8-98)**
**Prescribed by ANSI Std. Z39.18**

## Introduction

Ubiquitous, reliable, high data rate communication, carried by electromagnetic waves at optical frequencies, is an essential ingredient of our technological age. Information theory seeks to delineate the ultimate limits on reliable communication that arise from the presence of noise and other disturbances, and to establish the means by which these limits can be approached. Because electromagnetic fields are quantum mechanical, and high-sensitivity photodetection systems have long been limited by noises of quantum mechanical origin, information theory for optical communication channels should be couched in fully quantum terms. Yet, this has seldom been the case for channel capacity studies and communication system designs for realistic, or even quasi-realistic, optical channels. Thus, the main thrust of this program was to remedy this deficiency by putting information theory of important single-user and multiple-user optical channels on firm, quantum-mechanical foundations.

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 $c = \eta^{1/2}a + (1-\eta)^{1/2}b$, 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

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

with $E(|a|^2) \leq N_s$ 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 $\mathbf{a}$ at the transmitter, and receive another mode with photon annihilation operator $\mathbf{c} = \eta^{1/2}\mathbf{a} + (1-\eta)^{1/2}\mathbf{b}$, where $\mathbf{b}$ 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:

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

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

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

The classical capacity of the pure-loss bosonic channel — in which the $\mathbf{b}$ mode is unexcited ($N = 0$) — was shown in [1] to be $C_{\text{pure-loss}} = g(\eta N_s)$ nats/use, where $g(x) = (x+1)\ln(x+1) - x\ln(x)$ 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, $C_{\text{thermal}} \geq g(\eta N_s + (1-\eta)N) - g((1-\eta)N)$, 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 **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. A principal goal of the research program "Information Transmission and Entanglement Distribution over Bosonic Channels," Contract Number FA8750-06-2-0069, was to seek further evidence in support of — and perhaps a complete proof for — this minimum output entropy conjecture and the capacity formula for the thermal-noise channel. A second major goal of this program was to extend the single-user capacity theory to a multi-user broadcast scenario, as could be encountered in optical networking. A third goal of the program was to evaluate the capacity when classical communication over a bosonic channel was augmented by the availability of shared entanglement between the sender and receiver when the entanglement distribution and the classical communication were both subject to a constraint on the total average photon number used at the transmitter. In this report we briefly summarize the results that we have obtained in pursuit of the preceding goals. Additional information on research under this program can be obtained from the documents listed in the publications section at the end of this report.

## Bosonic Broadcast Channel

A broadcast channel is the congregation of communication media connecting a single transmitter to two or more receivers. In general, the transmitter encodes and sends out independent information to each receiver in a way that each receiver can reliably decode its respective information. The two-user, lossless bosonic broadcast channel takes the following form. The transmitter (Alice) controls a single-mode electromagnetic field with photon annihilation operator **a**. Alice's objective is to reliably communicate independent information streams to two receivers — Bob and Charlie — that observe single-mode electromagnetic fields whose photon annihilation operators are $\mathbf{b} = \eta^{1/2}\mathbf{a} + (1-\eta)^{1/2}\mathbf{e}$ and $\mathbf{c} = -(1-\eta)^{1/2}\mathbf{a} + \eta^{1/2}\mathbf{e}$, respectively, where **e** is the photon annihilation operator of an environmental mode that is in its vacuum state. We first showed [4] that when coherent-state encoding is employed in conjunction with coherent detection, the bosonic broadcast channel is equivalent to a classical degraded Gaussian broadcast channel whose capacity region is known, and known to be dual to that of the classical Gaussian multiple-access channel [5]. Thus, under these coding and detection assumptions, the capacity region of the bosonic broadcast channel is dual to that of the multiple-access bosonic channel with coherent-state encoding and coherent detection. To treat more general transmitter and receiver conditions, we used a limiting argument to apply the degraded quantum broadcast-channel coding theorem for finite-dimensional state spaces [6] to the infinite-dimensional bosonic channel with an average photon-number constraint. For the two-user lossless case, with $\eta>1/2$, we showed [5] that

$$R_B \leq g(\eta\beta N_s) \quad \text{and} \quad R_C \leq g((1-\eta)N_s) - g((1-\eta)\beta N_s), \text{ for } 0 \leq \beta \leq 1, \qquad (4)$$

is an inner bound on the capacity region, and that this inner bound specifies the capacity region if a new minimum output entropy conjecture is satisfied. Interestingly, this capacity region is *not* dual to that of the bosonic multiple-access channel with coherent-state encoding and optimum measurement that was found in [7].

The two minimum output entropy conjectures — one that establishes the capacity of the lossy bosonic channel with thermal noise and the other that establishes the capacity region of the bosonic broadcast channel — appear to be duals. We showed that they were equivalent when the input states are restricted to be Gaussian [5]. We also proved that the second minimum output entropy conjecture is true when Wehrl entropy is used in lieu of von Neumann entropy [5]. As yet, however, a full proof of the second minimum output entropy conjecture has not been obtained.

**The Entropy Photon-Number Inequality**

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 conjectured [8] its quantum version, viz., the Entropy Photo-number Inequality (EPnI). The EPI states that if $\mathbf{X}$ and $\mathbf{Y}$ are statistically independent, $n$-dimensional, continuous random vectors with differential Shannon entropies $h(\mathbf{X})$ and $h(\mathbf{Y})$, respectively, and associated entropy powers defined by

$$P(\mathbf{X}) = [\exp(h(\mathbf{X})/n)]/2\pi e] \quad \text{and} \quad P(\mathbf{Y}) = [\exp(h(\mathbf{Y})/\mathrm{n})]/2\pi e], \qquad (5)$$

where $e$ is the base for natural logarithms, then all of the following are true [9]:

$$P(\mathbf{Z}) \geq \eta P(\mathbf{X}) + (1\text{-}\eta)P(\mathbf{Y}) \qquad (6)$$

$$h(\mathbf{z}) \geq \mathrm{h}(\mathbf{Z}) \qquad (7)$$

$$h(\mathbf{Z}) \geq \eta h(\mathbf{X}) + (1\text{-}\eta)h(\mathbf{Y}). \qquad (8)$$

In these expressions, $0 \leq \eta \leq 1$ and

$$\mathbf{Z} = \eta\mathbf{X} + (1\text{-}\eta)\mathbf{Y} \quad \text{and} \quad \mathbf{z} = \eta\mathbf{x} + (1\text{-}\eta)\mathbf{y}, \qquad (9)$$

where $\mathbf{x}$ and $\mathbf{y}$ are statistically independent, $n$-dimensional, Gaussian random vectors with independent identically-distributed components of variances $P(\mathbf{X})$ and $P(\mathbf{Y})$, respectively.

Our conjectured Entropy Photon-number Inequality is as follows. Let $\boldsymbol{a}$ and $\boldsymbol{b}$ be $n$-dimensional column vectors of photon annihilation operators that are in a product state, i.e., their joint density operator satisfies $\rho_{\boldsymbol{ab}} = \rho_{\boldsymbol{a}} \otimes \rho_{\boldsymbol{b}}$. Define a new vector of photon annihilation operators by the beam splitter relation $\boldsymbol{c} = \eta^{1/2}\boldsymbol{a} + (1-\eta)^{1/2}\boldsymbol{b}$, where $0 \le \eta \le 1$. The entropy photon-numbers associated with the density operators $\rho_{\boldsymbol{a}}$ and $\rho_{\boldsymbol{b}}$ are

$$N(\rho_{\boldsymbol{a}}) = g^{-1}(S(\rho_{\boldsymbol{a}})/n) \quad \text{and} \quad N(\rho_{\boldsymbol{b}}) = g^{-1}(S(\rho_{\boldsymbol{b}})/n), \qquad (10)$$

where $S(\rho)$ is the von Neumann entropy of the state specified by the density operator $\rho$ and $g^{-1}$ is the inverse of the monotonically increasing function $g(x)$. The two equivalent forms of our conjectured EPnI are [8]:

$$N(\rho_{\boldsymbol{c}}) \ge \eta N(\rho_{\boldsymbol{a}}) + (1-\eta)N(\rho_{\boldsymbol{b}}) \qquad (11)$$

$$S(\rho_{\boldsymbol{ç}}) \ge S(\rho_{\boldsymbol{c}}), \qquad (12)$$

where $\boldsymbol{ç}$ is an n-dimensional column vector of photon annihilation operators whose joint density operator, $\rho_{\boldsymbol{ç}}$, is the product of $n$ thermal states each with average photon number $\eta N(\rho_{\boldsymbol{a}}) + (1-\eta)N(\rho_{\boldsymbol{b}})$. So far we have shown that the minimum output entropy conjectures needed to prove the capacity of the lossy bosonic channel with thermal noise and the bosonic broadcast channel are simple consequences of the EPnI. Thus, if the proof techniques employed for the EPI can be extended to apply to the EPnI, we will have established the capacities of the lossy bosonic channel with thermal noise and the bosonic broadcast channel. Furthermore, in very recent work [10], we have shown that our second minimum output entropy 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. Hence, proving the EPnI would have the immediate consequence of establishing those capacities as well.

**Entanglement-Assisted Capacity**

Previous work [11] had shown that the entanglement-assisted capacity of the lossy bosonic channel exceeded what could be accomplished without such nonclassical help. That work imposed an average photon number constraint on the classical information transmission, but no such constraint was imposed on the entanglement distribution. We have shown that when both the classical communication and the entanglement distribution are subject to a constraint on the total average photon number employed for both processes, then there is no benefit — in classical communication capacity — to be gained from entanglement distribution. However, such benefit might accrue in a continuous-time (multi-mode) setting wherein the classical information is bursty and there are both average and peak photon-flux constraints.

## 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] N. Jindal, S. Vishwanath, and A. Goldsmith, "On the duality of Gaussian multiple-access and broadcast channels," IEEE Trans. Inform. Theory **50,** 768 (2004).

[6] J. Yard, P. Hayden, and I. Devetak, "Quantum broadcast channels," arXiv:quant-ph/0603098.

[7] B. J. Yen and J. H. Shapiro, "Multiple-access bosonic communications," Phys. Rev. A **72,** 062312 (2005).

[8] S. Guha, B. I. Erkmen, and J. H. Shapiro, "The entropy photon-number inequality and its consequences," to be presented at 2008 Information Theory and Applications Workshop, San Diego, CA, January 2008, arXiv:quant-ph/0710.5666.

[9] O. Rioul, "Information theoretic proofs of entropy power inequalities," arXiv:cs.IT/07041751.

[10] S. Guha, J. H. Shapiro, and B. I. Erkmen, "Capacity of the bosonic wiretap channel and the entropy photon-number inequality,'' arXiv:quant-ph/0801.0841.

[11] V. Giovannetti, S. Lloyd, L. Maccone, and P. W. Shor, "Entanglement assisted capacity of the broadband lossy channel," Phys. Rev. Lett. **91,** 047901 (2003).

## Personnel

The research under this program was performed by:

Professor Jeffrey H. Shapiro — Principal Investigator

Dr. Stewart D. Personick — Consultant

Mr. Saikat Guha — Graduate Research Assistant

## Publications

The research under this program resulted in the following publications:


1. S. Guha and J. H. Shapiro, "Bosonic broadcast channel capacity and a new minimum output entropy conjecture," in O. Hirota, J. H. Shapiro, and M. Sasaki, eds., *Proceedings of the 8th International Conference on Quantum Communication, Measurement and Computing* (NICT Press, 2007) pp. 299-302.

2. 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).

3. S. Guha, B. I. Erkmen, and J. H. Shapiro, "The entropy photon-number inequality and its consequences," to be presented at 2008 Information Theory and Applications Workshop, San Diego, CA, January 2008, arXiv:quant-ph/0710.5666.