Infinite-fold enhancement in communications capacity using pre-shared entanglement

Saikat Guha

July 21, 2020
College of Optical Sciences,
Department of Electrical and Computer Engineering
University of Arizona, Tucson AZ (USA)

THE UNIVERSITY OF ARIZONA

arXiv:2001.03934 (2020)

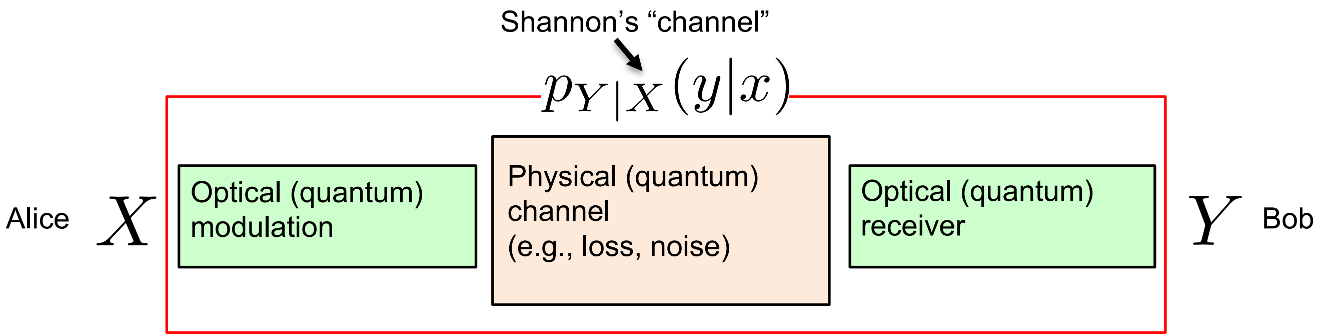
Outline

- Background
  - Quantum limit of classical communications
  - Joint detection receivers for superadditive capacity
- Entanglement assisted communications over the bosonic channel
  - Transmitter-receiver design
  - Infinite-fold capacity enhancement with pre-shared entanglement
- Conclusions and ongoing work

Outline

- Background
  - **Quantum limit of classical communications**
  - Joint detection receivers for superadditive capacity
- Entanglement assisted communications over the bosonic channel
  - Transmitter-receiver design
  - Infinite-fold capacity enhancement with pre-shared entanglement
- Conclusions and ongoing work

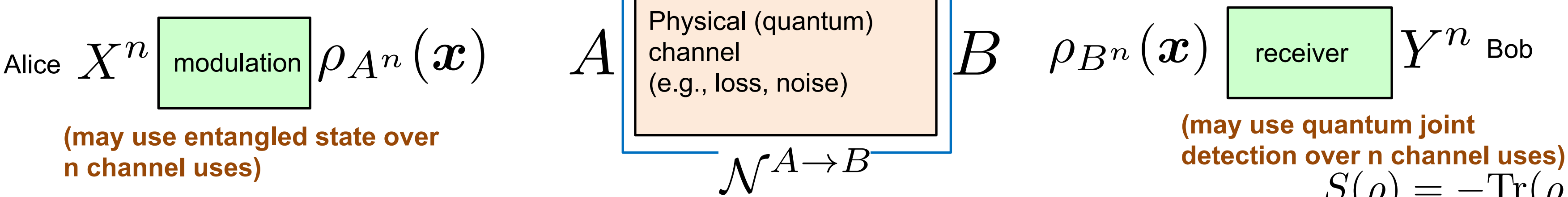
Quantum limit of classical communications



Shannon, 1948

Shannon capacity, $C_{\text{Shannon}} = \max_{p_X} I(X;Y)$

Holevo, 1996
Schumacher, Westmoreland, 1997

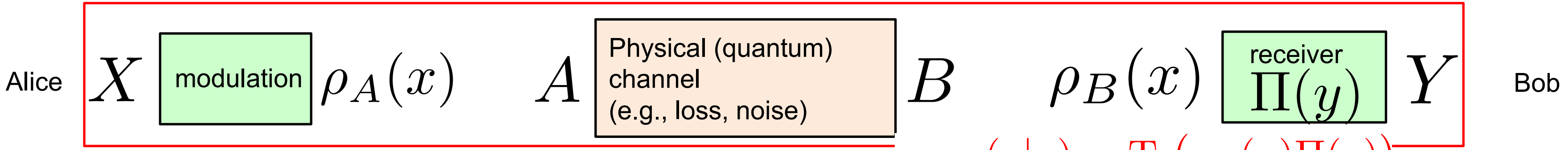


$$S(\rho) = -\text{Tr}(\rho \log \rho)$$

Holevo capacity, $C = \sup_n \dfrac{\max_{p_{X^n}(\boldsymbol{x}),\rho_{A^n}(\boldsymbol{x})} S\left(\sum p_{X^n}(\boldsymbol{x})\rho_{B^n}(\boldsymbol{x})\right) - \sum p_{X^n}(\boldsymbol{x}) S\left(\rho_{B^n}(\boldsymbol{x})\right)}{n}$

“Superadditivity” on the transmitter and receiver side

- Superadditivite capacity
  - **Transmitter side:** Using entangled states help achieve higher capacity
  - **Receiver side:** Quantum joint detection receiver helps achieve higher capacity
- Channel not transmitter-side superadditive, it can still be receiver-side
  - Product state modulation is optimal (entanglement at transmitter doesn’t help)
  - Holevo Capacity, $C = \max_{p_X} S\left(\sum p_X(x)\rho_B(x)\right) - \sum p_X(x) S\left(\rho_B(x)\right)$



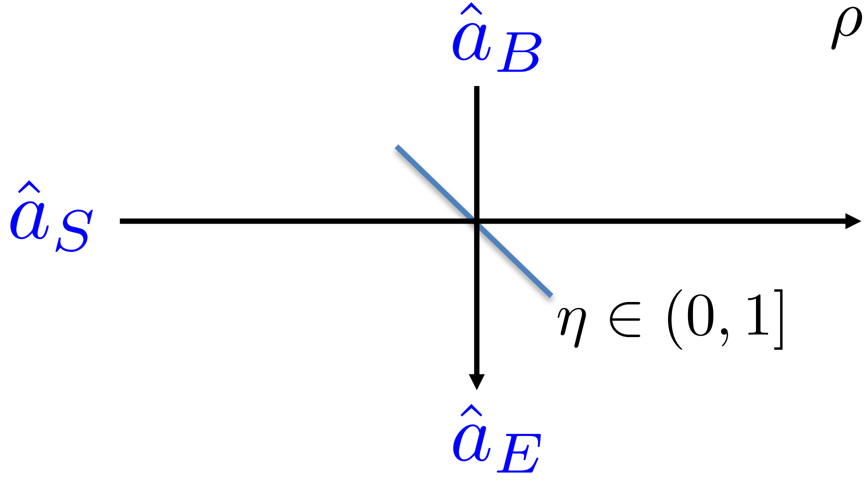
$$p_{Y|X}(y|x) = \mathrm{Tr}\left(\rho_B(x)\Pi(y)\right)$$

  - Shown : receiver uses symbol by symbol detection; Shannon capacity $C_1 < C$
  - Joint detection receiver (JDR) required, unless $\rho_B(x)$ orthogonal pure states
  - Calculation of C does not need receiver. Finding receiver achieving C is hard

The single-mode bosonic channel

- Mean photon number per mode constraint at transmitter $\langle \hat{a}_S^\dagger \hat{a}_S \rangle \leq N_S$
- Environment mode in thermal state, mean photon number $\langle \hat{a}_B^\dagger \hat{a}_B \rangle = N_B$

$$\rho_B = \int \frac{1}{\pi N_B} e^{-|\beta|^2/N_B} |\beta\rangle\langle\beta| d^2\beta$$



$$\hat{a}_R = \sqrt{\eta}\,\hat{a}_S + \sqrt{1-\eta}\,\hat{a}_B$$

- Any linear lossy propagation medium can be decomposed into a collection of single mode bosonic channels

Holevo capacity of the single-mode bosonic channel

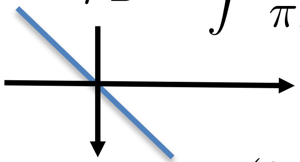
$$C = g(\eta N_S + (1-\eta)N_B) - g((1-\eta)N_B)$$ bits per mode

- C > Shannon capacity of all known standard optical receivers
- Product coherent state modulation achieves capacity
- Need joint detection receiver (collective measurement over codeword)

$$\rho_B = \int \frac{1}{\pi N_B} e^{-|\beta|^2/N_B} |\beta\rangle\langle\beta| d^2\beta$$

$$p(\alpha) = \frac{1}{\pi N_S} e^{-|\alpha|^2/N_S}$$

$|\alpha\rangle$



$$\rho_R = \int \frac{1}{\pi(1-\eta)N_B} e^{-|\beta-\sqrt{\eta}\alpha|^2/(1-\eta)N_B} |\beta\rangle\langle\beta| d^2\beta$$

$\eta \in (0, 1]$

$$g(N) = (1+N)\log(1+N) - N\log(N)$$

V. Giovannetti, SG, S. Lloyd, L. Maccone, J. H. Shapiro, and H. P. Yuen, Phys. Rev. Lett. 92, 027902 (2004)

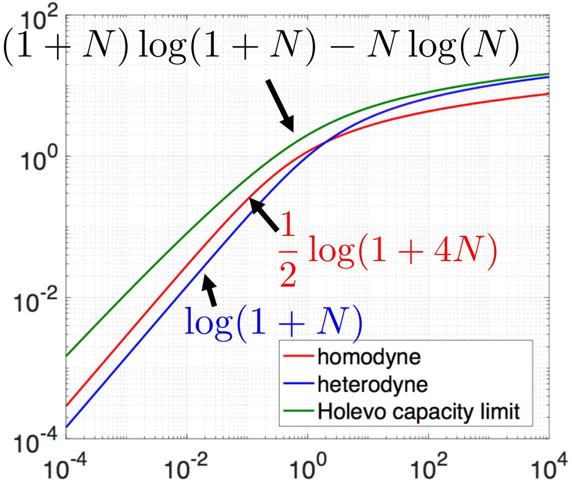
V. Giovannetti, SG, S. Lloyd, L. Maccone, and J. H. Shapiro, Phys. Rev. A (2004)

V. Giovannetti, R. García-Patrón, N. J. Cerf, and A. S. Holevo, Nat. Photonics 8, 796 (2014)

Quantum limit of classical (optical) communications over a lossy channel, with an input mean photon number constraint

$$N_B = 0$$

$$g(N) = (1 + N)\log(1 + N) - N\log(N)$$



$$N = \eta N_S$$

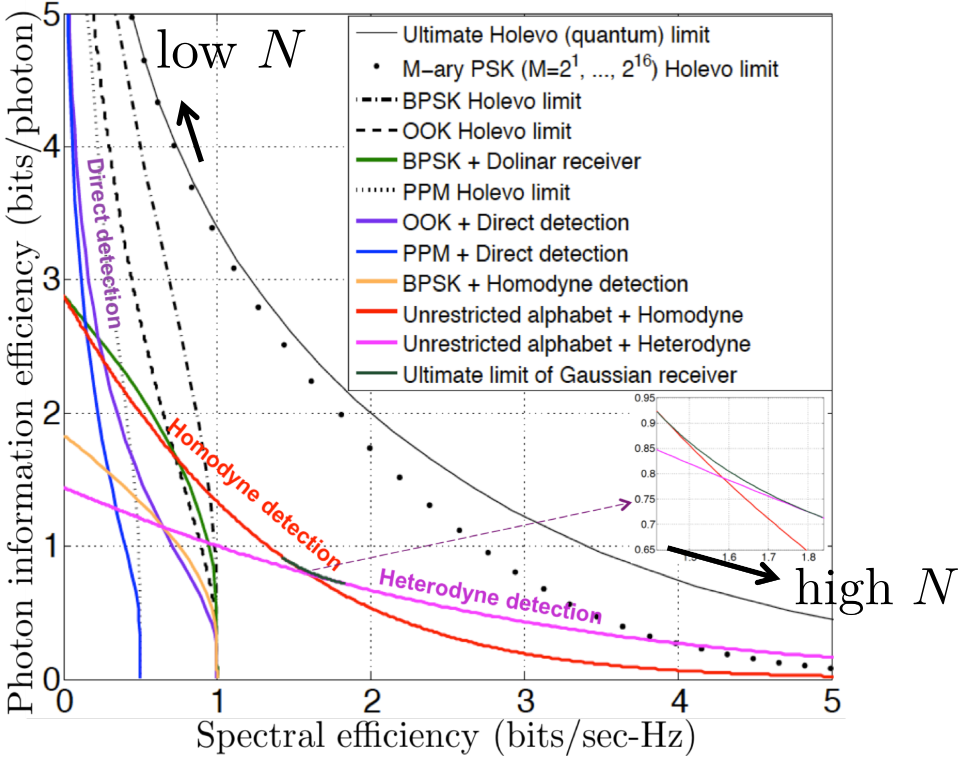
$\eta \sim e^{-\alpha L}$ fiber

$\eta \sim 1/L^2$ free-space

η : Transmissivity

N_S : Mean photon number transmitted per mode

$$\frac{C(N)}{N}$$



$$C(N)$$

Giovannetti, SG, Lloyd, Maccone, Shapiro, & Yuen, PRL (2004)

Takeoka and SG, Physical Review A 89, 042309 (2014)

Outline

- Background
  - Quantum limit of classical communications
  - **Joint detection receivers for superadditive capacity**
- Entanglement assisted communications over the bosonic channel
  - Transmitter-receiver design
  - Infinite-fold capacity enhancement with pre-shared entanglement
- Conclusions and ongoing work

Binary hypothesis test: $|\psi_1\rangle$ (hypothesis H_1) vs. $|\psi_2\rangle$ (hypothesis H_2)

$$\text{Prior probabilities: } p_1 = p,\ p_2 = 1-p$$

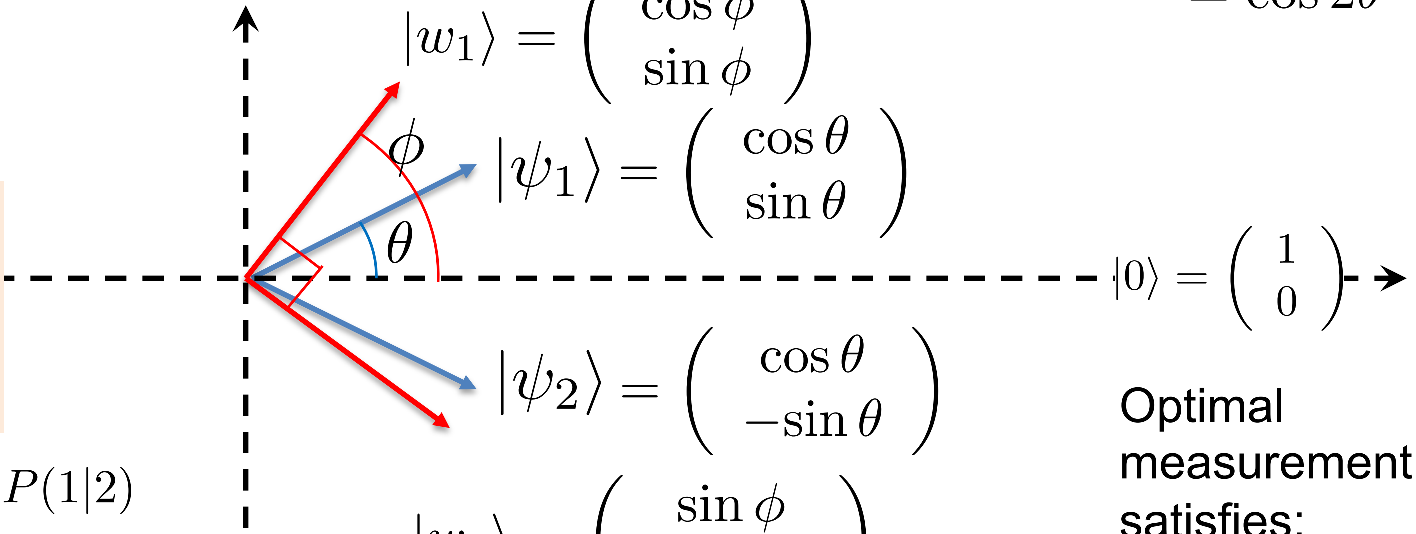
Inner product between the two states

$$\langle\psi_1|\psi_2\rangle = \sigma = \cos 2\theta$$

$$|1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

$$|w_1\rangle = \begin{pmatrix} \cos\phi \\ \sin\phi \end{pmatrix}$$

$$|\psi_1\rangle = \begin{pmatrix} \cos\theta \\ \sin\theta \end{pmatrix}$$



$$|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$$

$$|\psi_2\rangle = \begin{pmatrix} \cos\theta \\ -\sin\theta \end{pmatrix}$$

$$|w_2\rangle = \begin{pmatrix} \sin\phi \\ -\cos\phi \end{pmatrix}$$

Helstrom bound
(for minimum probability of error state discrimination)

$$P_e = pP(2|1) + (1-p)P(1|2)$$

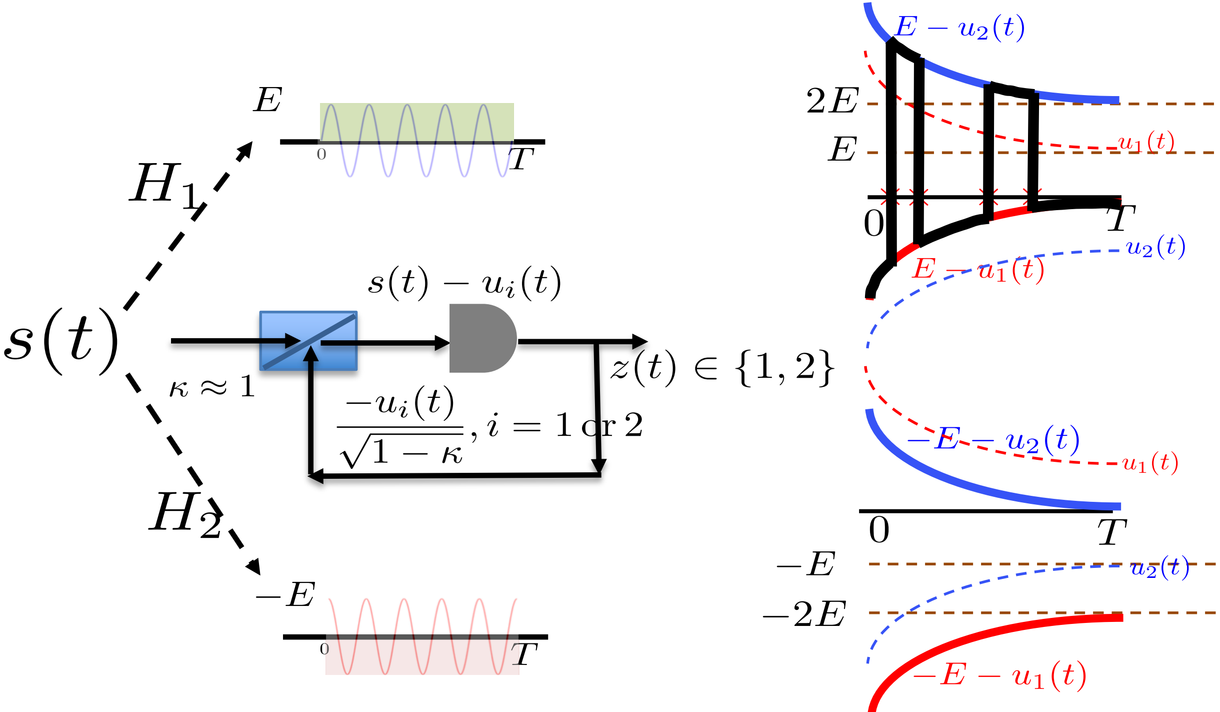
$$P_{e,\min} = \frac{1}{2}\left[1 - \sqrt{1 - 4p(1-p)\sigma^2}\right]$$

Optimal measurement satisfies:

$$\tan 2\phi = \frac{\tan 2\theta}{2p-1}$$

Binary phase shift keying (BPSK) modulation

- Consider BPSK modulation, $\{|\alpha\rangle, |-\alpha\rangle\}$, priors $(p, 1-p)$, $N = |\alpha|^2$



$$\langle \alpha | -\alpha \rangle = e^{-2N}$$

Minimum error probability:

$$P_{e,\min} = \frac{1}{2}\left[1 - \sqrt{1 - 4p(1-p)e^{-4N}}\right]$$

Sam Dolinar, MIT Ph.D. Thesis, 1973

Example of receiver-side superadditive capacity

- Maximum capacity with the optimal symbol-by-symbol measurement

$$C_1 = 1 - h_2(p), \quad p = \frac{1}{2}[1 - \sqrt{1 - e^{-4N}}]$$ bits per mode

- Holevo capacity (joint detection over infinite-length modulated block)

$$C_\infty = S\left(\frac{|\alpha\rangle\langle\alpha| + |-\alpha\rangle\langle-\alpha|}{2}\right) = h_2\left(\frac{1 + e^{-2N}}{2}\right)$$ bits per mode

- The joint-detection gain most pronounced at low photon number

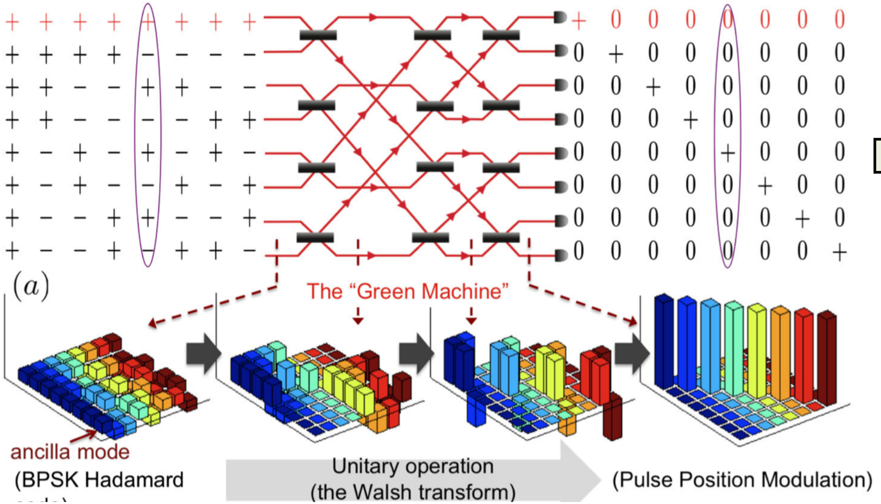
$$\lim_{N \to 0} \frac{C_\infty}{C_1} = \infty$$

We do not know, $C_2, C_3, \ldots, C_n, \ldots$

Joint detection receiver (JDR) for superadditive capacity

n-mode input, n-mode output (n=8 shown)

$$\begin{bmatrix} \alpha \\ -\alpha \\ \alpha \\ -\alpha \\ \alpha \\ -\alpha \\ \alpha \\ -\alpha \end{bmatrix} \Rightarrow$$



$$\Rightarrow \begin{bmatrix} 0 \\ 0 \\ 0 \\ 0 \\ \sqrt{8}\alpha \\ 0 \\ 0 \\ 0 \end{bmatrix} \quad n = 8$$

Mean photon number in the n-mode Hadamard codeword (input and output), $n|\alpha|^2 = nN$

$$X \in \{1, 2, \ldots, n\} \rightarrow p_{Y|X}(y|x) = \begin{cases} 1 - e^{-nN}, & \text{if } y = x \\ 0, & \text{if } y \neq x \\ e^{-nN}, & \text{if } y = n+1 \end{cases} \rightarrow Y \in \{1, 2, \ldots, n, n+1\}$$

SG, Phys. Rev. Lett. 106, 240502 (2011)

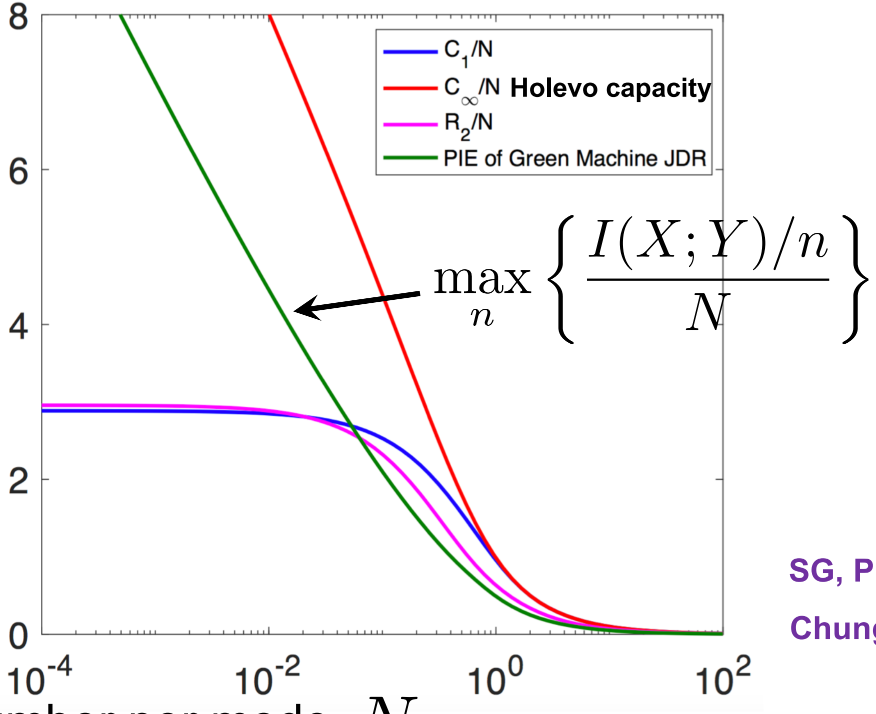
Superadditive capacity

Bridging the remaining gap to the Holevo capacity requires JDRs that use **quantum optical** effects

- Plotting photon information efficiency, C(N)/N

$$\frac{C(N)}{N}$$

bits per photon



mean photon number per mode, N

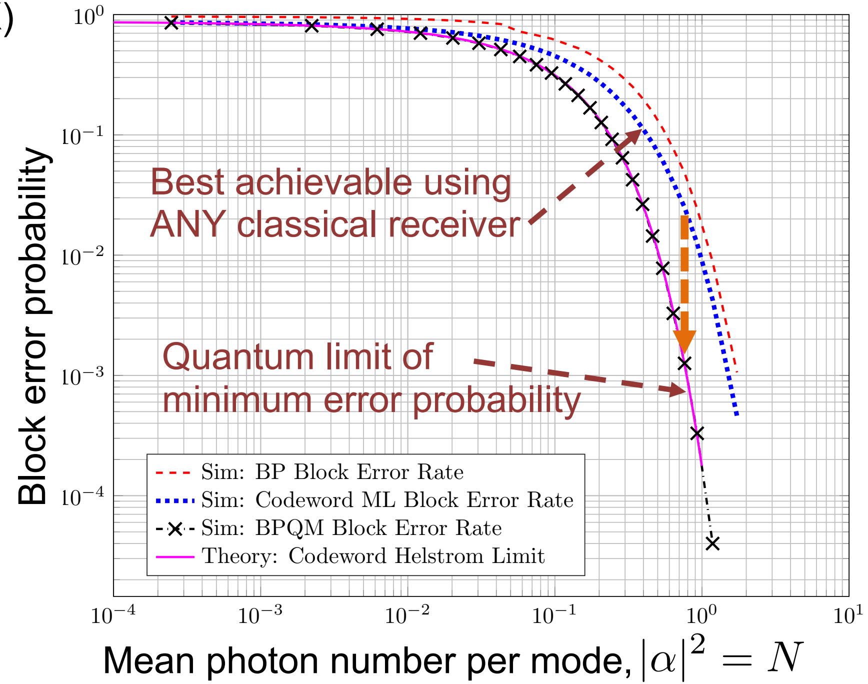
SG, Phys. Rev. Lett. 106, 240502 (2011)

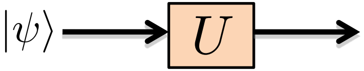
Chung, SG, Zheng, PRA 96, 012320 (2017)

A receiver (based on quantum "belief propagation" to achieve the Holevo capacity

Coherent state binary-phase shift keyed (BPSK) codebook, with eight 5-mode codewords

$$\left\{ \begin{array}{l} |-\alpha\rangle|-\alpha\rangle|\alpha\rangle|-\alpha\rangle|\alpha\rangle \\ |\alpha\rangle|\alpha\rangle|\alpha\rangle|\alpha\rangle|\alpha\rangle \\ |-\alpha\rangle|-\alpha\rangle|\alpha\rangle|\alpha\rangle|-\alpha\rangle \\ |\alpha\rangle|\alpha\rangle|\alpha\rangle|-\alpha\rangle|-\alpha\rangle \\ |\alpha\rangle|-\alpha\rangle|-\alpha\rangle|\alpha\rangle|\alpha\rangle \\ |\alpha\rangle|-\alpha\rangle|-\alpha\rangle|-\alpha\rangle|-\alpha\rangle \\ |-\alpha\rangle|\alpha\rangle|-\alpha\rangle|\alpha\rangle|-\alpha\rangle \\ |-\alpha\rangle|\alpha\rangle|-\alpha\rangle|-\alpha\rangle|\alpha\rangle \end{array} \right\}$$





$$|\psi_\pm\rangle = \sqrt{\frac{1+x}{2}}|0\rangle \pm \sqrt{\frac{1-x}{2}}|1\rangle$$

$|\psi\rangle \in \{|\alpha\rangle, |-\alpha\rangle\}$

$\langle\alpha|-\alpha\rangle = e^{-2N} \equiv x$

$\langle\psi_+|\psi_-\rangle = x$

Narayanan, Seshadreesan, SG, Pfister, arXiv:2003.04356 (2020)

Outline

- Background
  - Quantum limit of classical communications
  - Joint detection receivers for superadditive capacity
- Entanglement assisted communications over the bosonic channel
  - **Transmitter-receiver design**
  - Entanglement assisted covert communications
- Conclusions and ongoing work

Entanglement assisted classical communications

- Communication capacity, when Alice and Bob pre-share (unlimited amount of) entanglement, $C_E = \max_{\rho_A \in \mathcal{H}_A} I(\mathcal{N}^{A \to B}, \rho_A)$

$$I(\mathcal{N}^{A \to B}, \rho_A) = S(\rho_A) + S(\mathcal{N}^{A \to B}(\rho_A)) - S\big((\mathcal{N}^{A \to B} \otimes \mathbb{I})[\Phi]\big)$$

  - where, Φ is a purification of ρ_A

C. H. Bennett, P. W. Shor, J. A. Smolin, and A. V. Thapliyal, IEEE Trans. Inform. Theory 48, 2637 (2002)

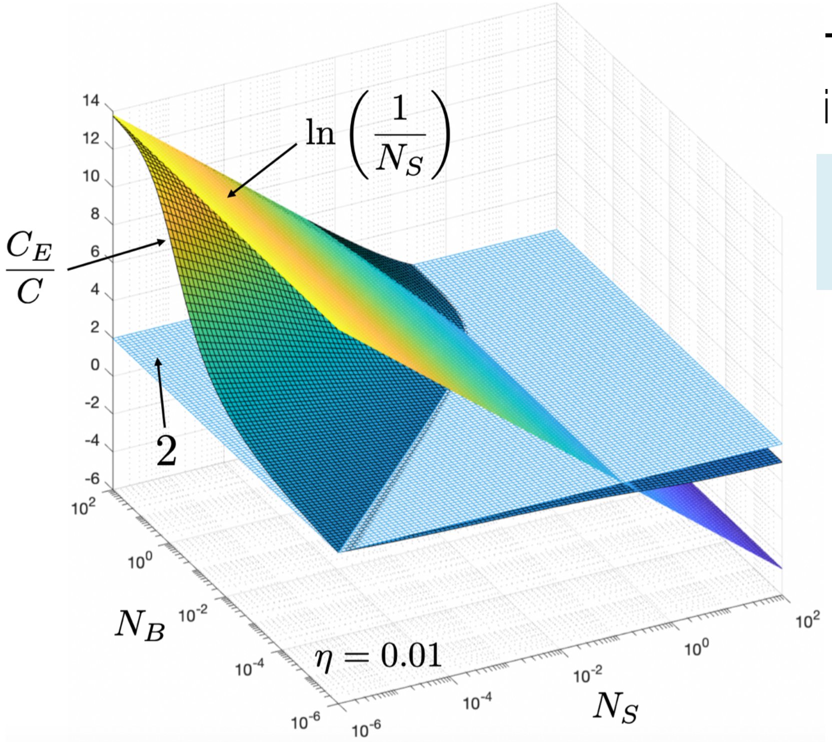
Entanglement assisted capacity of the bosonic channel

- Mean photon number constraint, N_S
- Take, $\rho_A = \int \frac{1}{\pi N_S} e^{-|\alpha|^2} |\alpha\rangle\langle\alpha| d^2\alpha$
- Purification, $|\Phi\rangle = \sum_{n=0}^{\infty} \sqrt{\frac{N_S^n}{(1+N_S)^{1+n}}} |n\rangle_S |n\rangle_I$
- Capacity, $C_E(\eta, N_S, N_B) = g(N_S) + g(N_S') - g(A_+) - g(A_-)$
  - $A_\pm = (D - 1 \pm (N_S' - N_S))/2$
  - $D = \sqrt{(N_S + N_S' + 1)^2 - 4\eta N_S (N_S + 1)}$

Vittorio Giovannetti, Seth Lloyd, Lorenzo Maccone, Peter W. Shor, Phys. Rev. A 68, 062323 (2003)

Comparison of C_E with C

Shi, Zhang, Zhuang, arXiv:1909.11112 (2019)
SG, Zhuang, Bash, arXiv:2001.03934 (2020)



The entanglement assistance is most pronounced, i.e., $C_E/C \sim \ln(1/N_S)$ when $N_S \ll 1, N_B \gg 1$

Low brightness transmitter
Long center wavelength (high noise)

Taylor series expansion at $N_S = 0$ yields:

$$C_E = -N_S \ln N_S + o(N_S)$$

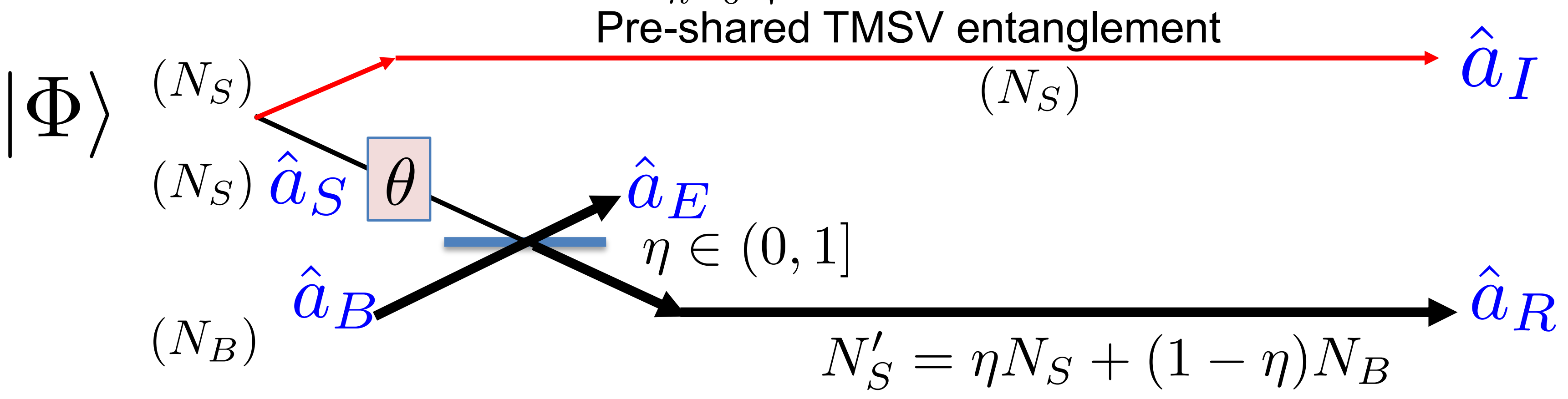
$$C = N_S \ln\left(1 + [(1-\eta)N_B]^{-1}\right) + o(N_S)$$

$$\lim_{N_S \to 0} \frac{C_E}{C \ln(1/N_S)} = \frac{1}{(1+(1-\eta)N_B)\ln\left(1+[(1-\eta)N_B]^{-1}\right)}$$

Achieving C_E for the bosonic channel

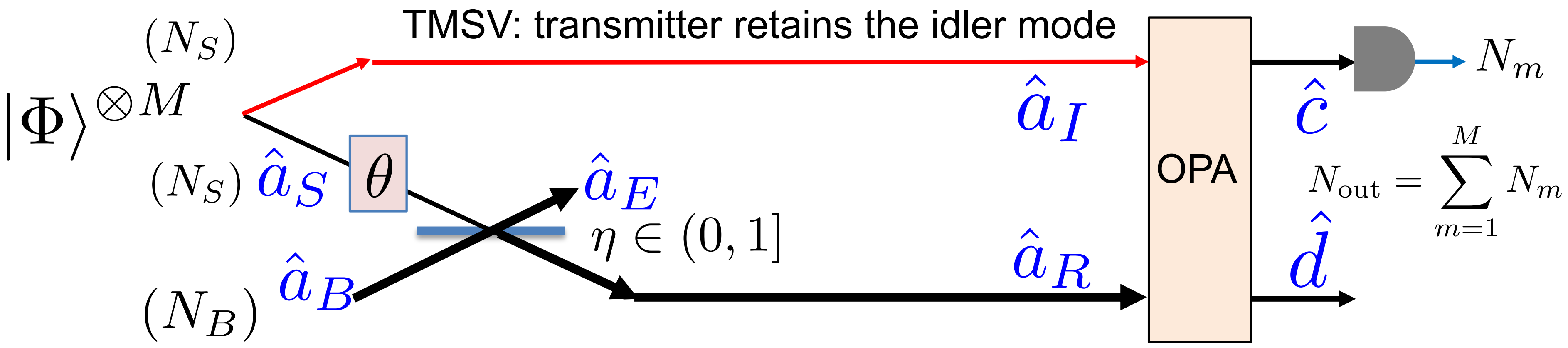
- A two-mode squeezed vacuum (TMSV) source, and phase modulation achieves the entanglement assisted capacity C_E, when $N_S \ll 1, N_B \gg 1$
  - In general, active modulation (squeezing, displacement) of TMSV maybe necessary
  - binary phase modulation suffices

$$|\Phi\rangle = \sum_{n=0}^{\infty} \sqrt{\frac{N_S^n}{(1+N_S)^{1+n}}} |n\rangle_S |n\rangle_I$$



Shi, Zhang, Zhuang, arXiv:1909.11112 (2019)

The Optical Parametric Amplifier (OPA) based receiver



$$\langle \hat{a}_R \hat{a}_I \rangle = \sqrt{\eta N_S (N_S + 1)}$$

$$\frac{C_E}{C} \to 2$$

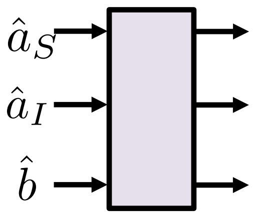
$$\hat{c}^{(m)} = \sqrt{G}\hat{a}_I^{(m)} + \sqrt{G-1}\hat{a}_R^{\dagger(m)}$$
$$\hat{d}^{(m)} = \sqrt{G}\hat{a}_R^{(m)} + \sqrt{G-1}\hat{a}_I^{\dagger(m)}$$

$$E[N_m] = \langle \hat{c}^\dagger \hat{c} \rangle = G N_S + (G-1)(1 + (1-\eta)N_B + \eta N_S)$$
$$\pm 2\sqrt{G(G-1)}\sqrt{\eta N_S (N_S + 1)}$$

SG and B. I. Erkmen, Phys. Rev. A (2009)

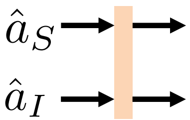
Receiver based on sum frequency generation (SFG)

$$\hat{H}_I = \hbar g \sum_{m=1}^{M} \left(\hat{b}^\dagger \hat{a}_{S_m} \hat{a}_{I_m} + \hat{b} \hat{a}^\dagger_{S_m} \hat{a}^\dagger_{I_m} \right)$$ SFG



$t = \pi / 2\sqrt{M} g$

OPA



The SF ($\hat{b}_k$) modes are in displaced thermal states:

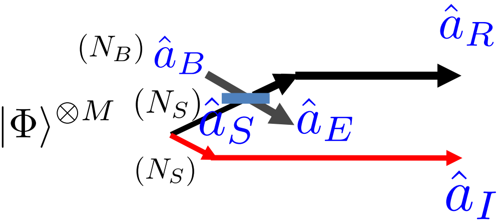
$$\hat{\rho}_{\rm th}(\alpha^{(k)}, N_T) = \int_{\mathbb{C}} \frac{1}{\pi N_T} e^{-|\beta - \alpha^{(k)}|^2 / N_T} |\beta\rangle\langle\beta| d^2\beta$$

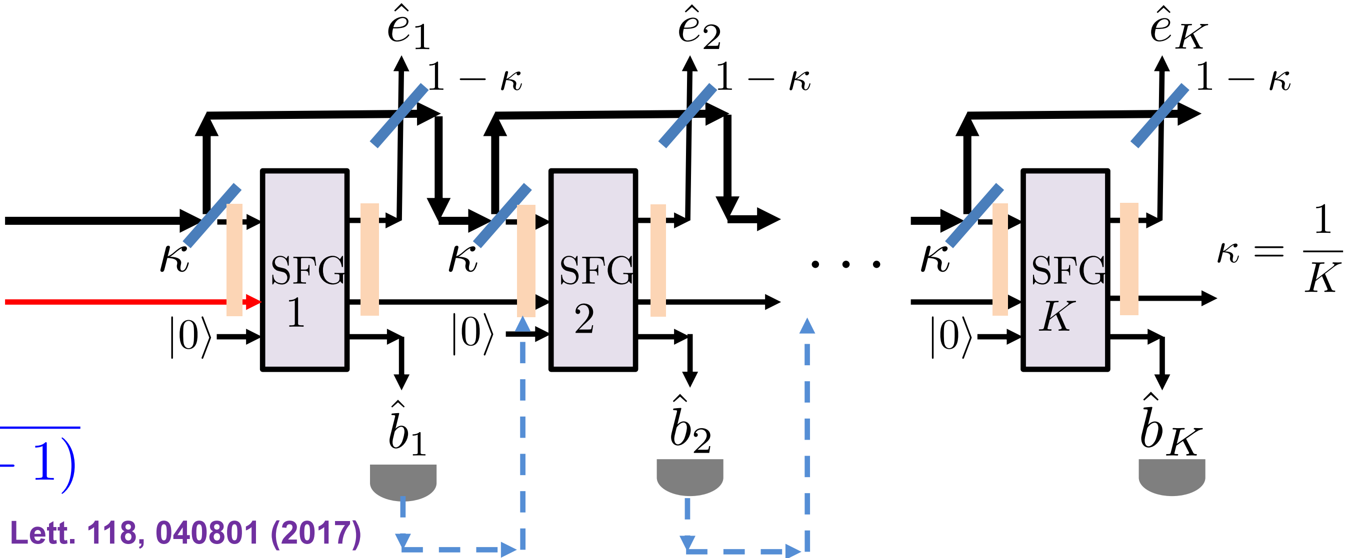
$$\alpha^{(k)} = \sqrt{M \kappa \eta N_S (1 + N_S) \mu^{k-1}}$$

$$\mu = \left(1 - \kappa(1 + N_S')\right)^2$$

$$N_T = \kappa N_S N_S'$$

Feed-Forward SFG

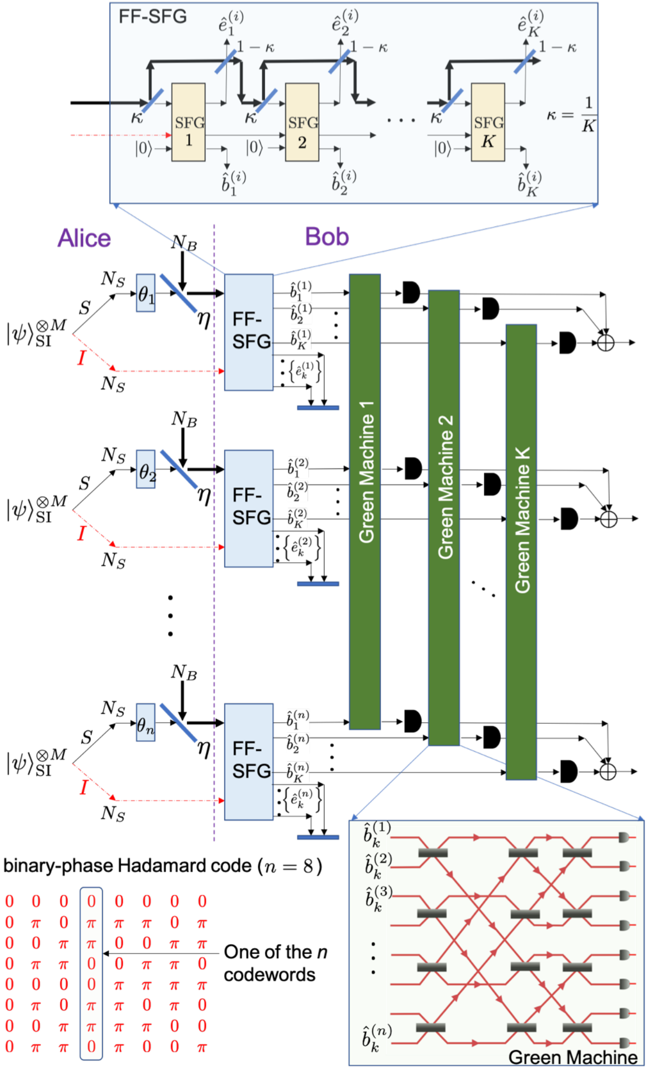




$$\langle \hat{a}_R \hat{a}_I \rangle = \sqrt{\eta N_S (N_S + 1)}$$

Zhuang, Zhang, Shapiro, Phys. Rev. Lett. 118, 040801 (2017)

Transmitter and joint-detection receiver for entanglement assisted communication



k-th Green Machine's inputs:

$$\hat{\rho}_{\rm th}(\pm\alpha^{(k)}, N_T)$$

k-th Green Machine's outputs (one of them has this mean, others have zero mean)

$$\hat{\rho}_{\rm th}(\sqrt{n}\,\alpha^{(k)}, N_T)$$

$$\langle 0|\hat{\rho}_{\rm th}(\alpha, N_T)|0\rangle = (1/(N_T+1))e^{-|\alpha|^2/(N_T+1)}$$

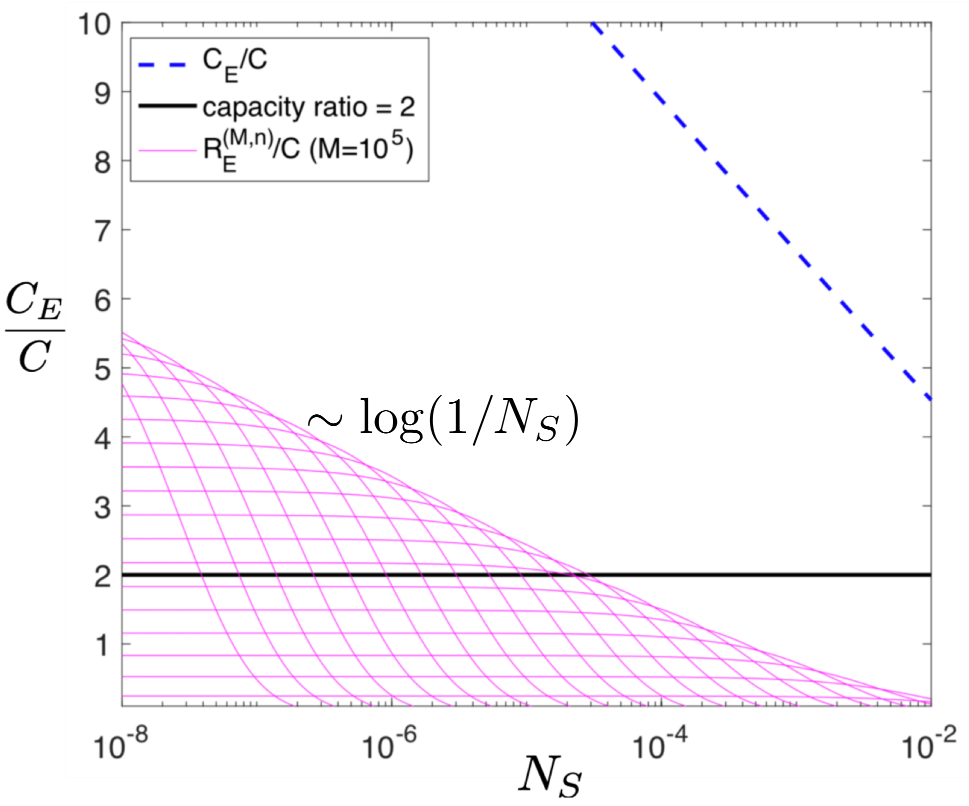
$$\alpha^{(k)} = \sqrt{M\kappa\eta N_S(1+N_S)\mu^{k-1}}$$

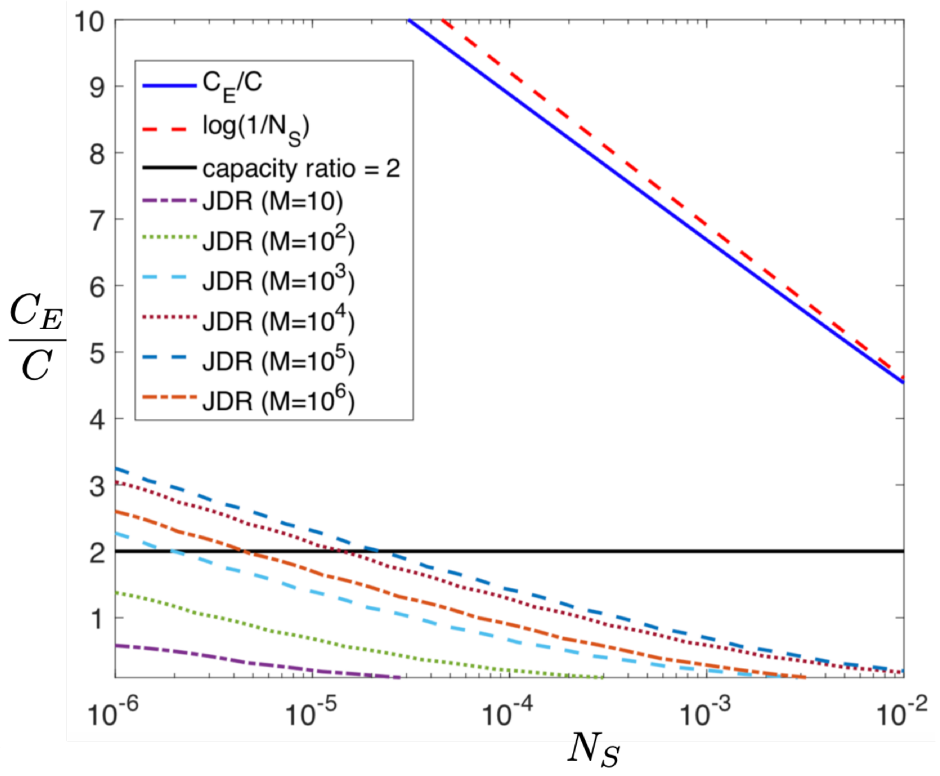
$$\mu = \left(1-\kappa(1+N_S')\right)^2$$

$$N_T = \kappa N_S N_S'$$

SG, Zhuang, Bash, arXiv:2001.03934 (2020)

Superadditivity in entanglement assisted communication rate





SG, Zhuang, Bash, arXiv:2001.03934 (2020)

Outline

- Background
  - Quantum limit of classical communications
  - Joint detection receivers for superadditive capacity
- Entanglement assisted communications over the bosonic channel
  - Transmitter-receiver design
  - **Entanglement assisted covert communications**
- Conclusions and ongoing work

Covert communications

- Provably covert communications needs $N_S = O(1/\sqrt{n})$, resulting in:

$$O(\sqrt{n}) \quad \text{bits in} \quad n \quad \text{modes}$$

B. A. Bash, A. H. Gheorghe, M. Patel, J. L. Habif, D. Goeckel, D. Towsley, and SG, Nat. Commun. 6, 8626 (2015)

- Entanglement assisted covert communications: the $\log(1/N_S)$ enhancement in capacity results in:

$$O(\sqrt{n}\log n) \quad \text{bits in} \quad n \quad \text{modes}$$

Gagatsos, Bullock, Bash, arXiv:2002.06733 [quant-ph] (2020)

Outline

- Background
  - Quantum limit of classical communications
  - Joint detection receivers for superadditive capacity
- Entanglement assisted communications over the bosonic channel
  - Transmitter-receiver design
  - Entanglement assisted covert communications
- Conclusions and ongoing work

Conclusions and ongoing work

- **Holevo capacity, C:** Quantum limit of classical communications
  - (product) coherent state, i.e., laser light modulation is capacity optimal
  - Attaining ultimate limit of classical communications needs quantum (joint detection) receivers
- **Entanglement assisted capacity, C_E:** highest gain when the transmitter is low brightness and thermal noise is high
  - TMSV pre-shared entanglement and SFG receiver front end translates the problem back to receiver design for coherent states to achieve Holevo capacity
  - Covert communications: shared entangled breaks the "square root law"
- Find better transmitter modulation, codes, and receivers to fully achieve C_E: explore **resource theories** of non-Gaussian components
- Connection with **quantum illumination radar**

Thank you!

Quntao Zhuang
Boulat Bash
Jeffrey Shapiro
Baris Erkmen
Kaushik Seshadreesan
Narayanan Rengaswamy
Henry Pfister
Lizhong Zheng
Hye-Won Chung
Christos Gagatsos

Office of Naval Research Science & Technology
DARPA
U.S. DEPARTMENT OF ENERGY | Office of Science
NSF
Raytheon
Army Research Office
ARL
GENERAL DYNAMICS