How Alice Should Balance the Photon Budget in Quantum Communication

Mark M. Wilde

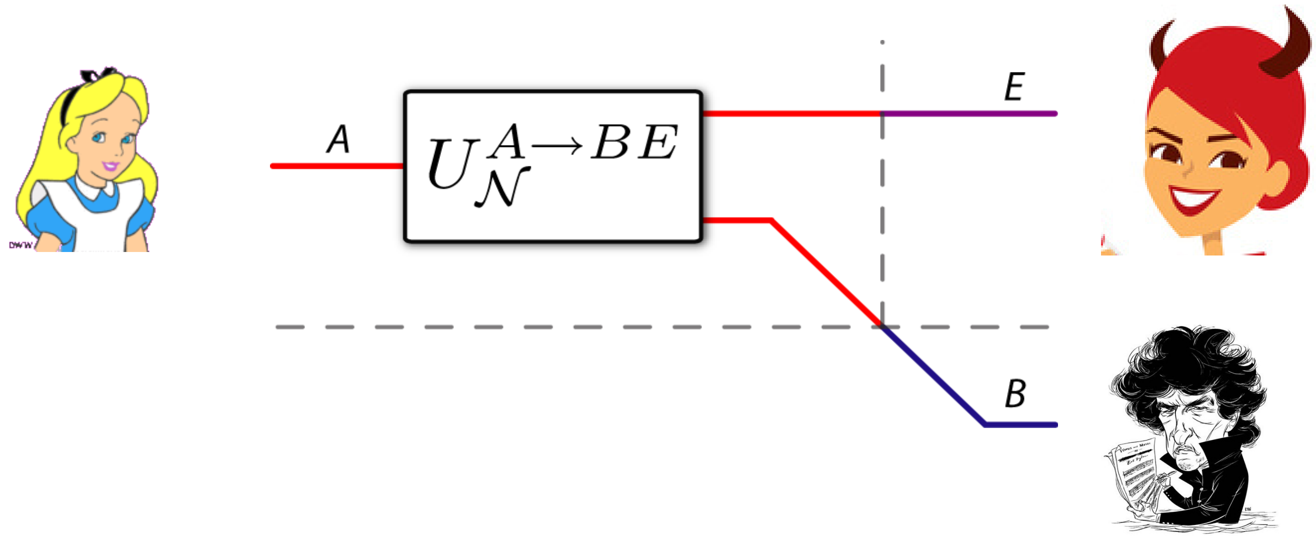
School of Computer Science
McGill University

In collaboration with
Patrick Hayden and Saikat Guha

arXiv:1105.0119

Seminar for the Disruptive Information Processing Technologies Group,
Raytheon BBN Technologies, May 6, 2011

The Many Uses of a Quantum Channel



Classical Data – Alice wishes to send “I love you” or “I don't love you”

Quantum Data – Alice sends $\frac{1}{\sqrt{2}}\left(|\text{“I love you”}\rangle + |\text{“I don't love you”}\rangle\right)$

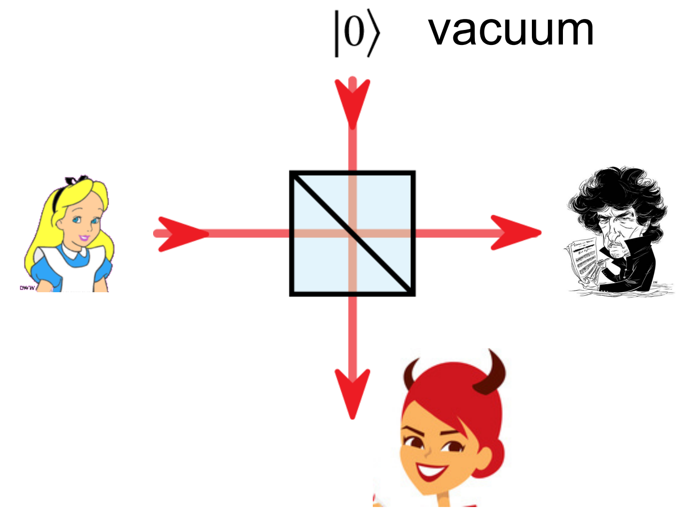
Private Classical Data – A concerned Alice sends “I love you” or “I don't love you” and doesn't want Eve to know

Assisting Resources – If Alice and Bob share any assisting resources such as entanglement or secret key, this can help

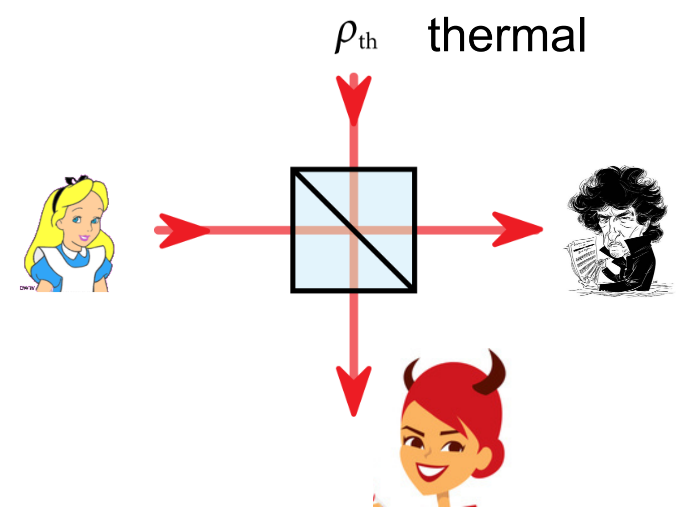
Can also **consume** or **generate** these resources in addition to using a quantum channel

Bosonic Channels

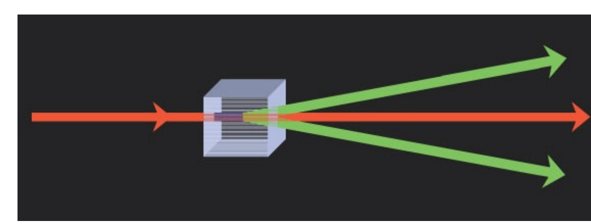
Lossy Bosonic Channel
(*models fiber optic or free space transmission*)



Thermalizing Channel
(similar model with background radiation)



Amplifier Channel
(models amplifier noise, Hawking-Unruh radiation)



Weedbrook *et al*., Gaussian Quantum Information, *Reviews of Modern Physics* (2011).

Sending Classical Information over a Quantum Channel

Coding Strategy

(similar to that for classical case)

Use a quantum channel many times so that law of large numbers comes into play

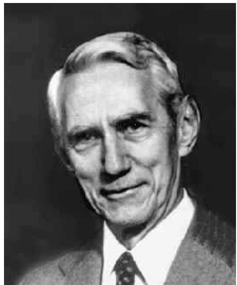
Code randomly with an ensemble of the following form:

$$\{p(x), \rho_x^{A'}\}_{x \in \mathcal{X}}$$

Channel input states are **product states**

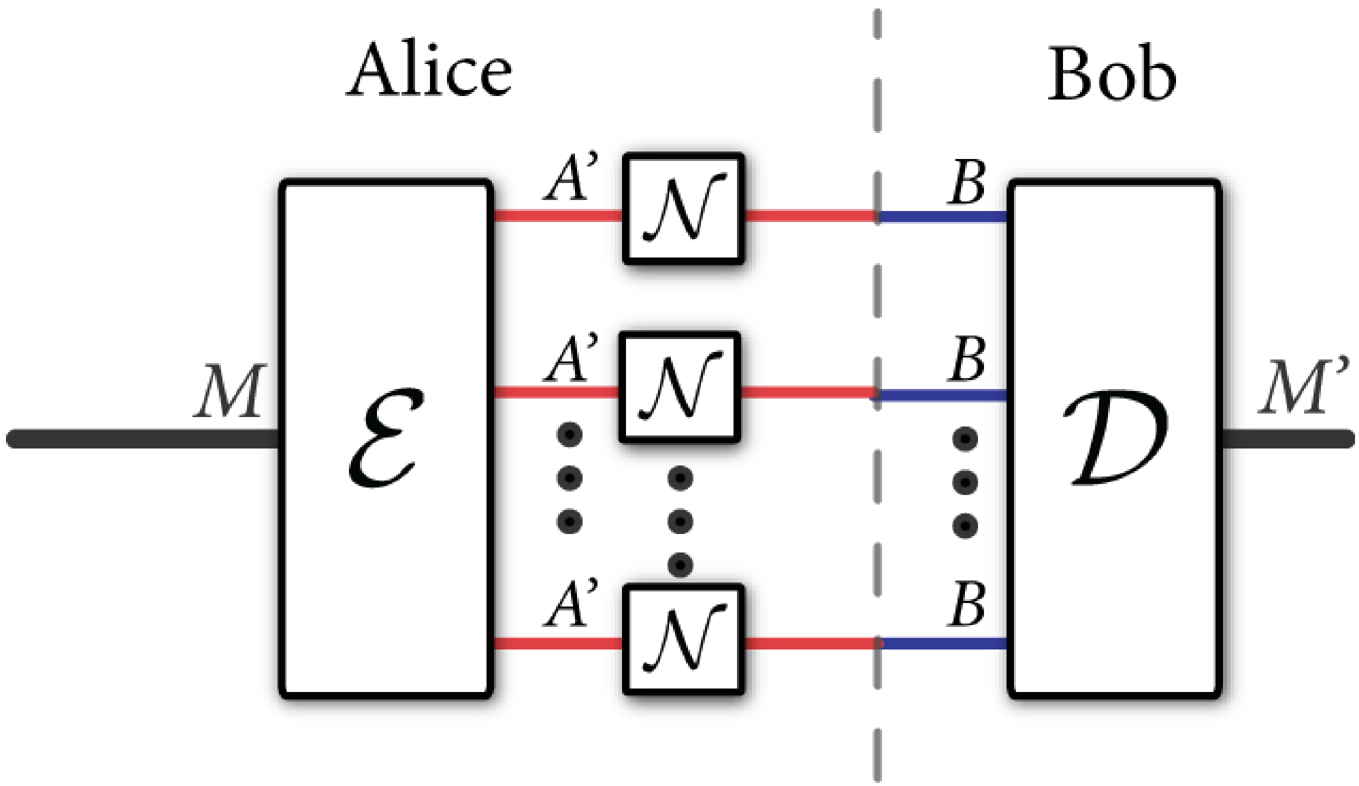
Hey, that's my idea!!!!

Allow for small error but show that the error vanish large block length



Holevo, IEEE Trans. Inf. Theory, 44, 269-273 (1998).
Schumacher & Westmoreland, PRA, 56, 131-138 (1997).

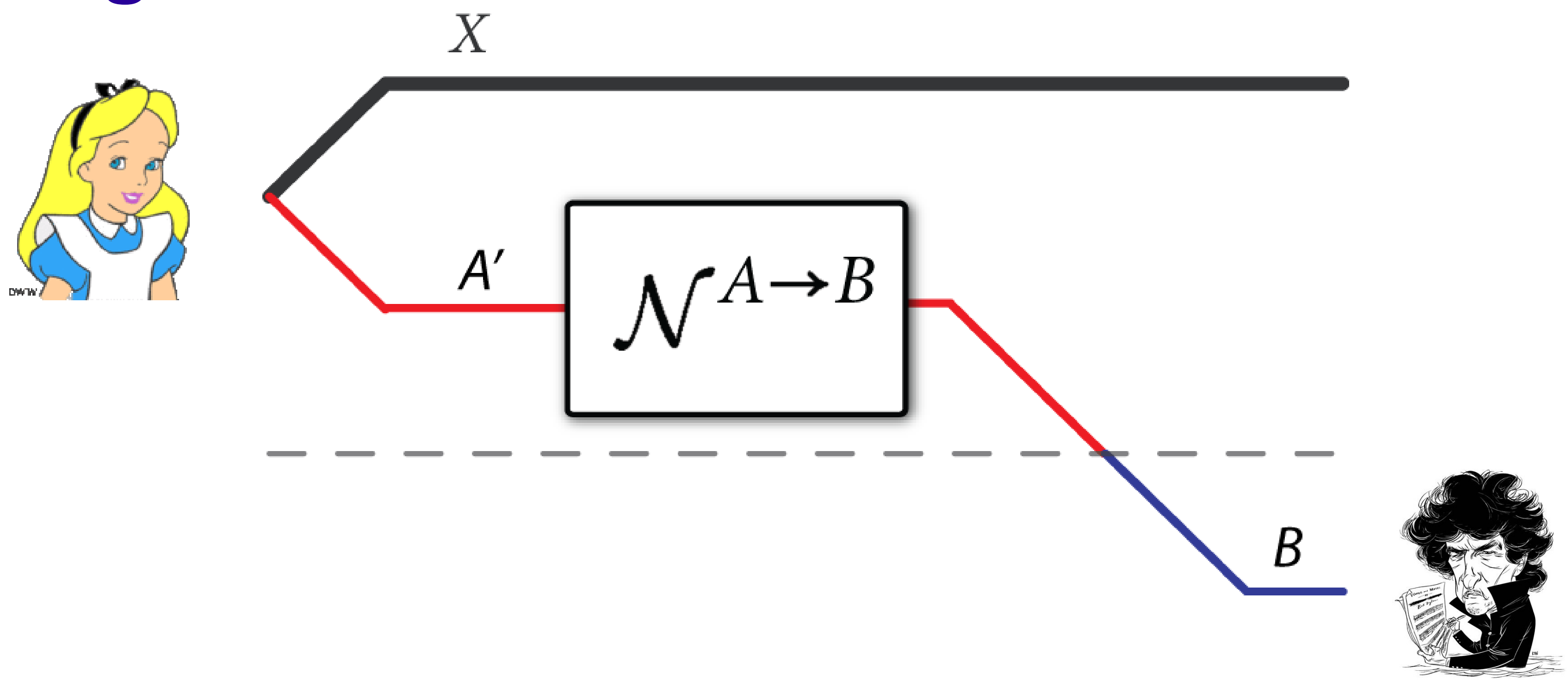
Sending Classical Information over a Quantum Channel (ctd.)



Encoder just maps classical signal to a **tensor product state**

Decoder performs a measurement over all the output states to determine transmitted classical signal

Sending Classical Data over Quantum Channels



Correlate classical data with quantum states:

$$\sum_x p_X(x)|x\rangle\langle x|^X \otimes \mathcal{N}^{A'\to B}(\phi_x^{A'})$$

Holevo information of a quantum channel:

$$\chi(\mathcal{N}) \equiv \max_{\{p_X(x),\phi_x\}} I(X;B)$$

Holevo (1998), Schumacher and Westmoreland (1997)

Sending Classical Data over Bosonic Channels

Classical capacity of **lossy bosonic channel** is exactly

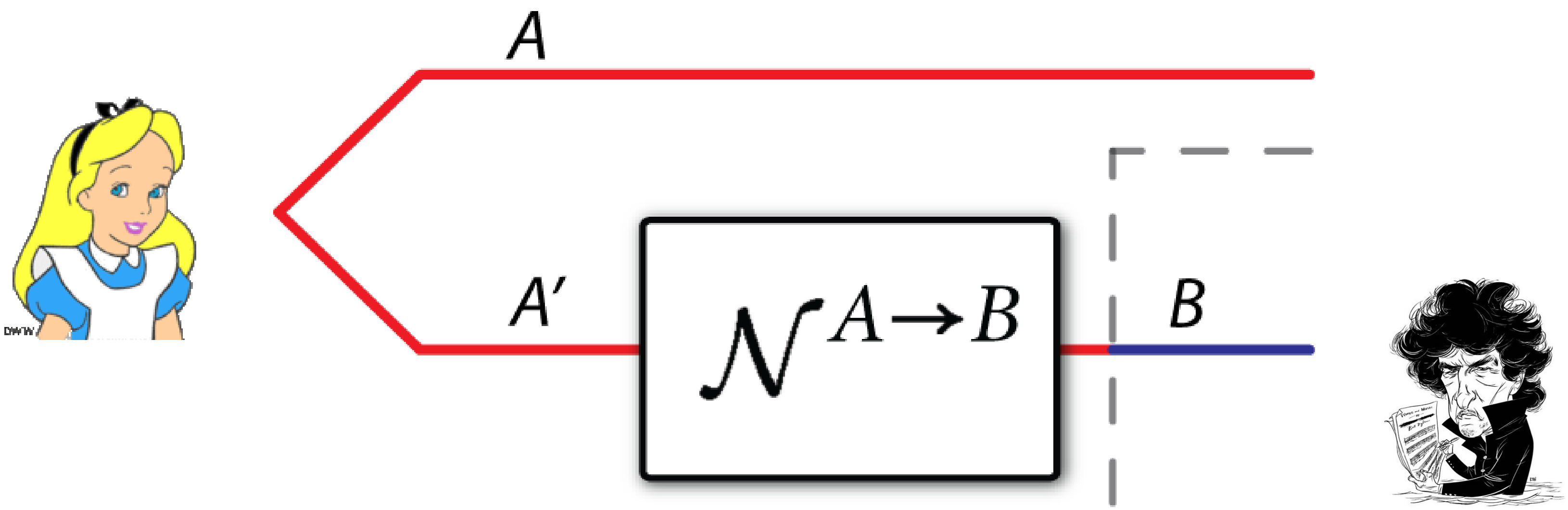
$$g(\eta N_S)$$

where η is **transmissivity** of channel,
N_S is the **mean input photon number**,
and $g(x) = (x+1) \log(x+1) - x \log x$
is the **entropy** of a **thermal state**
with photon number x

Can **achieve** this capacity by selecting **coherent states** randomly according to a complex, isotropic Gaussian prior with variance N_S

Giovannetti *et al.*, *Physical Review Letters* 92, 027902 (2004)

Sending Quantum Data over Quantum Channels



Preserving entanglement is the same as transmitting quantum data

$$\mathcal{N}^{A'\to B}(\phi^{AA'})$$

Coherent information of a quantum channel:

$$Q(\mathcal{N}) \equiv \max_{\phi} I(A\rangle B)$$

where $I(A\rangle B) \equiv H(B) - H(AB)$

Lloyd (1997), Shor (2002), Devetak (2005)

Sending Quantum Data over Bosonic Channels

Quantum capacity of lossy bosonic channel is

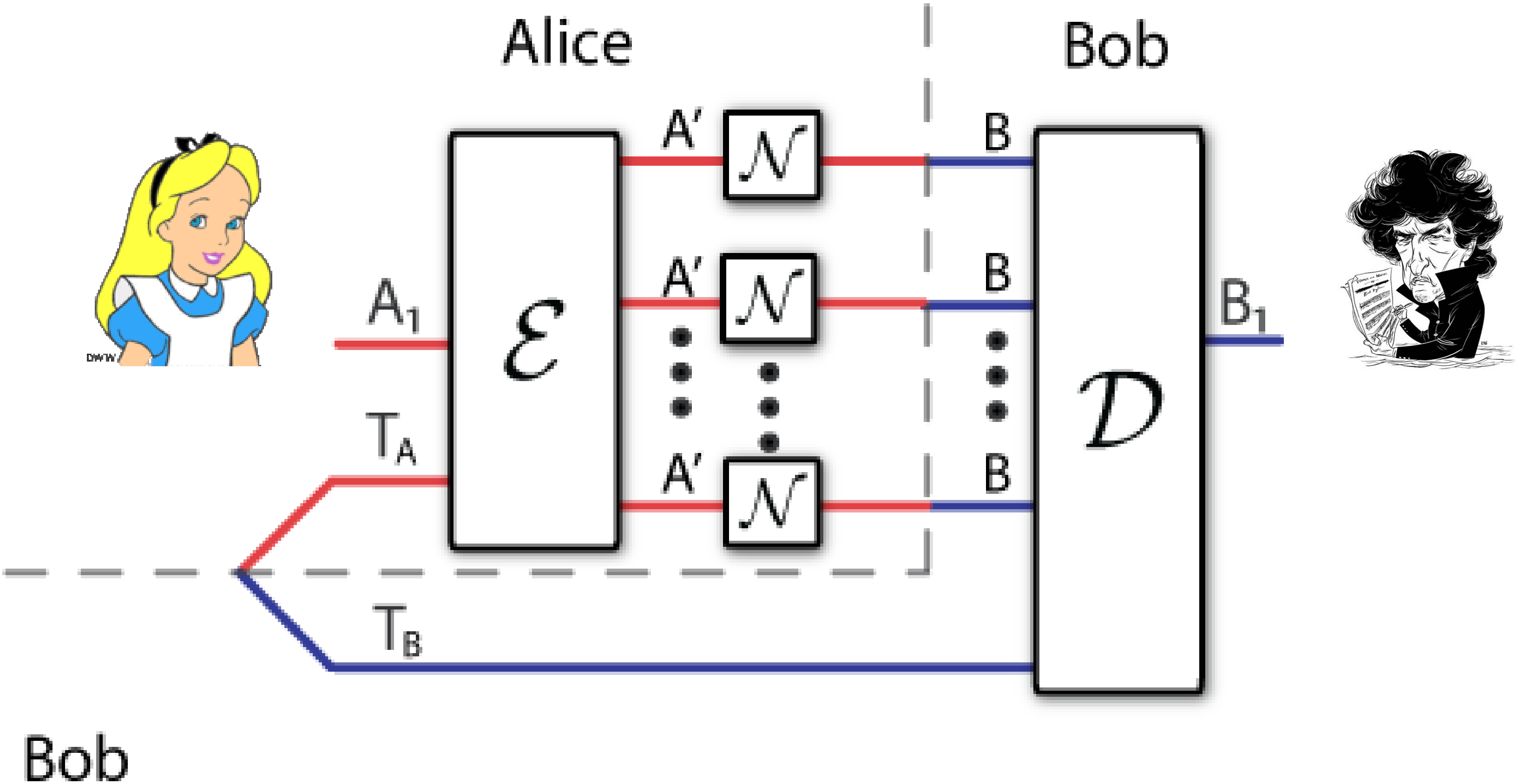
$$g(\eta N_S) - g((1-\eta)N_S)$$

Interpretation: Generate **random** quantum codes from a **thermal state** distribution

An **achievable rate** is the *difference* of Bob and Eve's entropy

Holevo and Werner, *Physical Review A* 63, 032312 (2001)
Wolf *et al*., *Physical Review Letters* 98, 130501 (2007)
Guha *et al*., ISIT 2008, arXiv:0801.0841

Sending Quantum Data with Entanglement Assistance



Encoder is a random unitary mapping

Decoder decouples from Eve the quantum information Alice would like to protect

Devetak, Harrow, Winter, IEEE Trans. Information Theory vol. 54, no. 10, pp. 4587-4618, Oct 2008
Devetak, Harrow, Winter, Phys. Rev. Lett., 93, 230504 (2004).

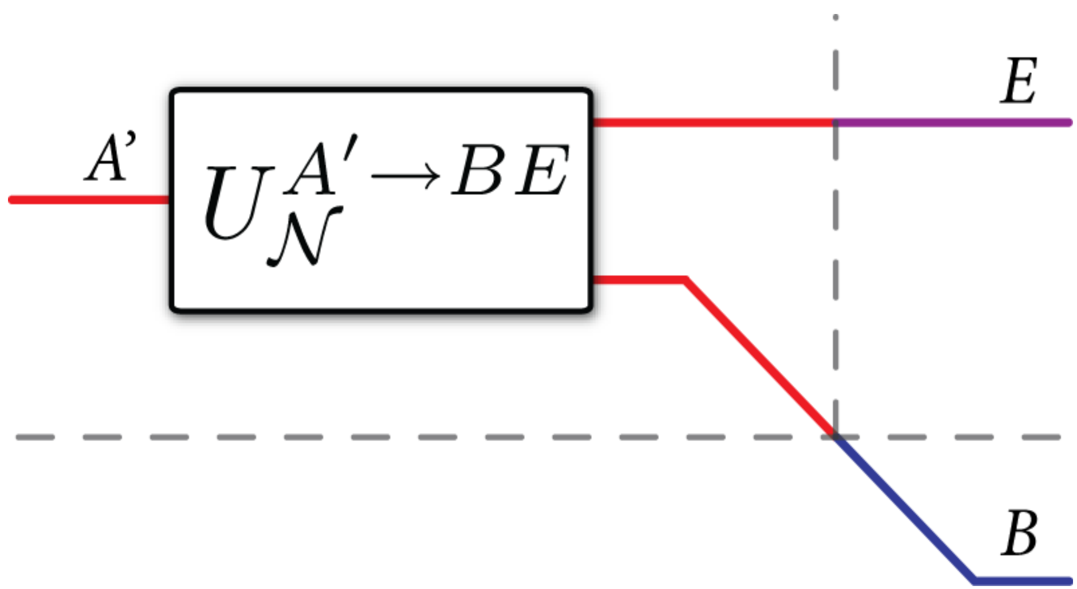
Father Protocol

Can achieve the following resource inequality:

$$\langle \mathcal{N}^{A' \to B} \rangle + \frac{1}{2} I(A;E)_\psi [qq] \geq \frac{1}{2} I\left(A;B\right)_\psi \left[q \to q\right]$$

where

$|\psi\rangle^{AA'}$



$|\psi\rangle^{ABE}$

Devetak, Harrow, Winter, IEEE Trans. Information Theory vol. 54, no. 10, pp. 4587-4618, Oct 2008
Devetak, Harrow, Winter, Phys. Rev. Lett., 93, 230504 (2004).

Entanglement-Assisted Quantum Transmission over Bosonic Channels

Entanglement-Assisted Quantum Capacity:

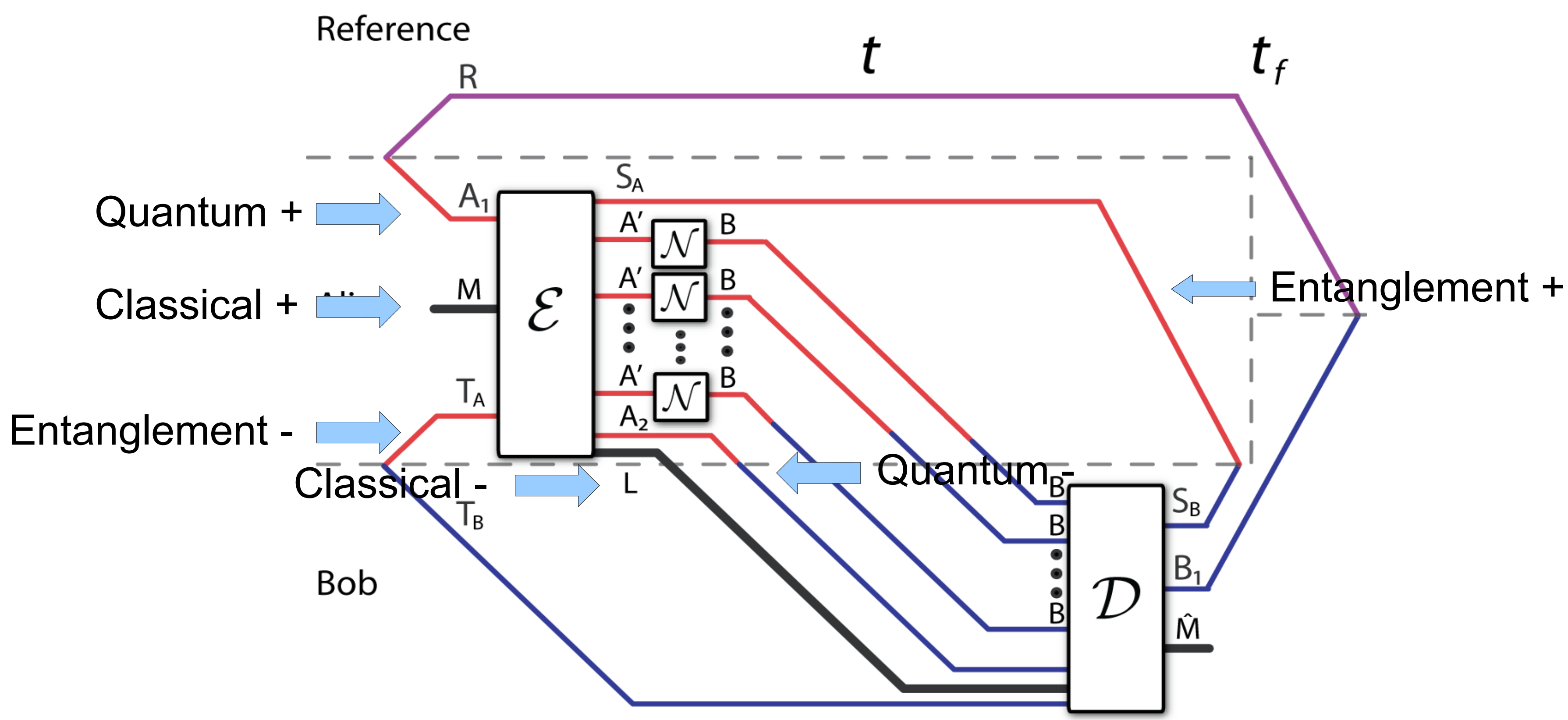
$$1/2 \quad g(\eta N_S) + g(N_S) - g((1-\eta)N_S)$$

Again generate **random** quantum codes from a **thermal state** distribution

Prior shared entanglement boosts capacity

Giovannetti et al., Physical Review Letters 91, 047901 (2003)
Wilde, Hayden, Guha. arXiv:1105.0119

First Setting: The CQE Setting



$$nC = \log|M| - \log|L|$$

$$nQ = \log|A_1| - \log|A_2|$$

$$nE = \log|S_A| - \log|T_A|$$

[1] Hsieh and Wilde. arXiv:0901.3038. *IEEE Transactions on Information Theory*, September 2010.
[2] Wilde and Hsieh. arXiv:1004.0458. The quantum dynamic capacity formula of a quantum channel.

Quantum Dynamic Capacity Theorem

The dynamic capacity region $\mathcal{C}_{CQE}(\mathcal{N})$ is

$$\mathcal{C}_{CQE}(\mathcal{N}) = \overline{\bigcup_{k=1}^{\infty} \frac{1}{k} \mathcal{C}^{(1)}_{CQE}(\mathcal{N}^{\otimes k})}. \tag{1}$$

The "one-shot" region $\mathcal{C}^{(1)}_{CQE}(\mathcal{N})$ is

$$\mathcal{C}^{(1)}_{CQE}(\mathcal{N}) \equiv \bigcup_{\sigma} \mathcal{C}^{(1)}_{CQE,\sigma}(\mathcal{N}).$$

The "one-shot, one-state" region $\mathcal{C}^{(1)}_{CQE,\sigma}(\mathcal{N})$ is the set of all rates C, Q, and E, such that

$$C + 2Q \leq I(AX;B)_{\sigma}, \tag{2}$$
$$Q + E \leq I(A\rangle BX)_{\sigma}, \tag{3}$$
$$C + Q + E \leq I(X;B)_{\sigma} + I(A\rangle BX)_{\sigma}. \tag{4}$$

The above entropic quantities are with respect to a classical-quantum state σ^{XAB} where

$$\sigma^{XAB} \equiv \sum_{x} p(x) \left|x\right\rangle \left\langle x\right|^{X} \otimes \mathcal{N}^{A' \to B}(\phi_x^{AA'}). \tag{5}$$

One should consider states on A'^k instead of A' when taking the regularization.

Achievability

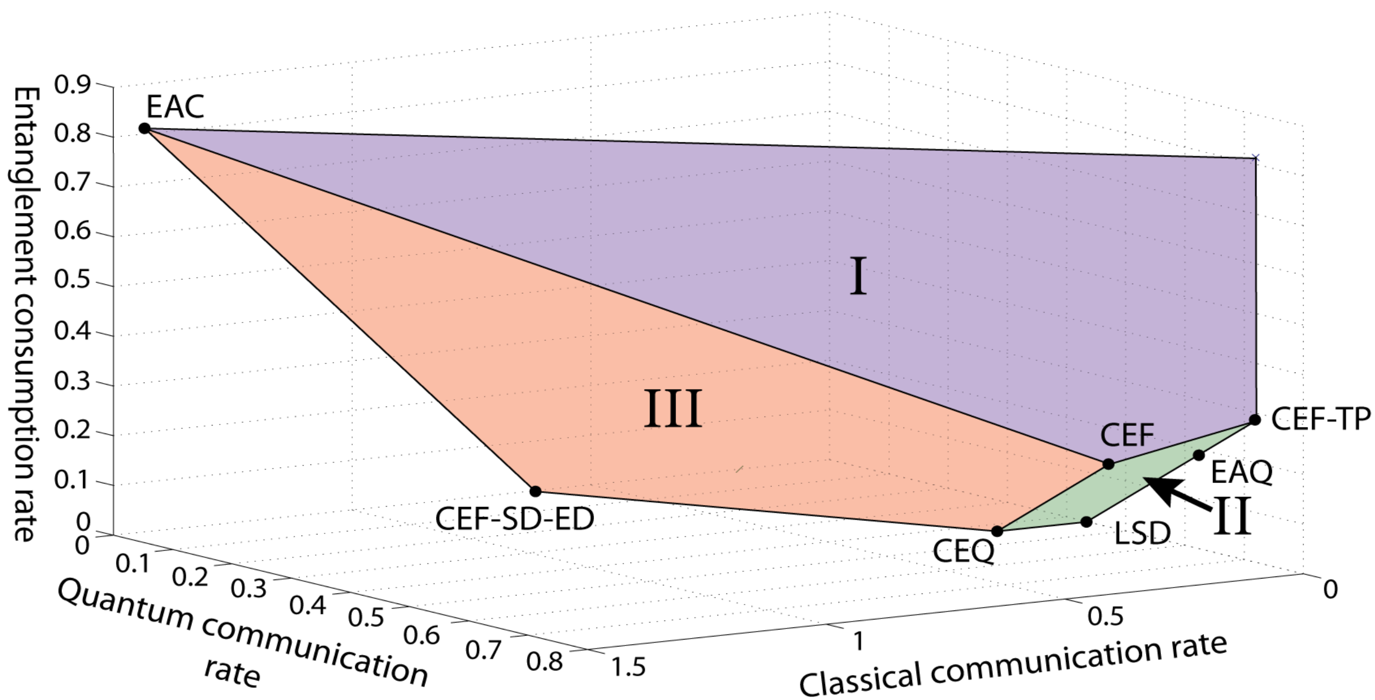
There exists a protocol for

entanglement-assisted classical and quantum communication

that achieves the following rates:

$$\langle \mathcal{N}^{A' \to B} \rangle + \frac{1}{2} I(A;E|X)_\sigma [qq] \geq \frac{1}{2} I(A;B|X)_\sigma [q \to q] + I(X;B)_\sigma [c \to c]$$

Combine this with teleportation, dense coding, and entanglement distribution...



Hsieh and Wilde. arXiv:0811.4227. *IEEE Transactions on Information Theory*, September 2010.

Converse Proof

Can prove using just the simplest tools:

Assume the existence of a good catalytic protocol

(The actual state is close to the ideal state)

Alicki-Fannes' inequality for continuity of entropic terms

(Entropies are close if states are close)

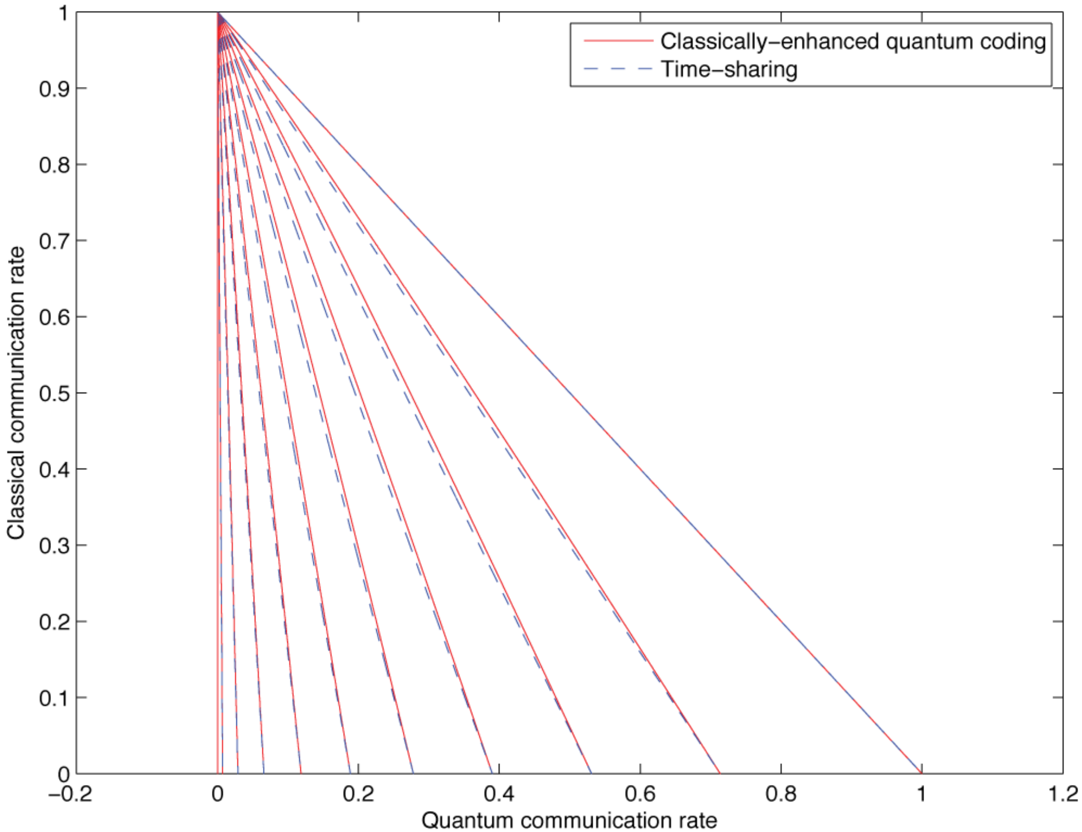
Quantum data processing inequality

(Data processing cannot increase classical or quantum correlations)

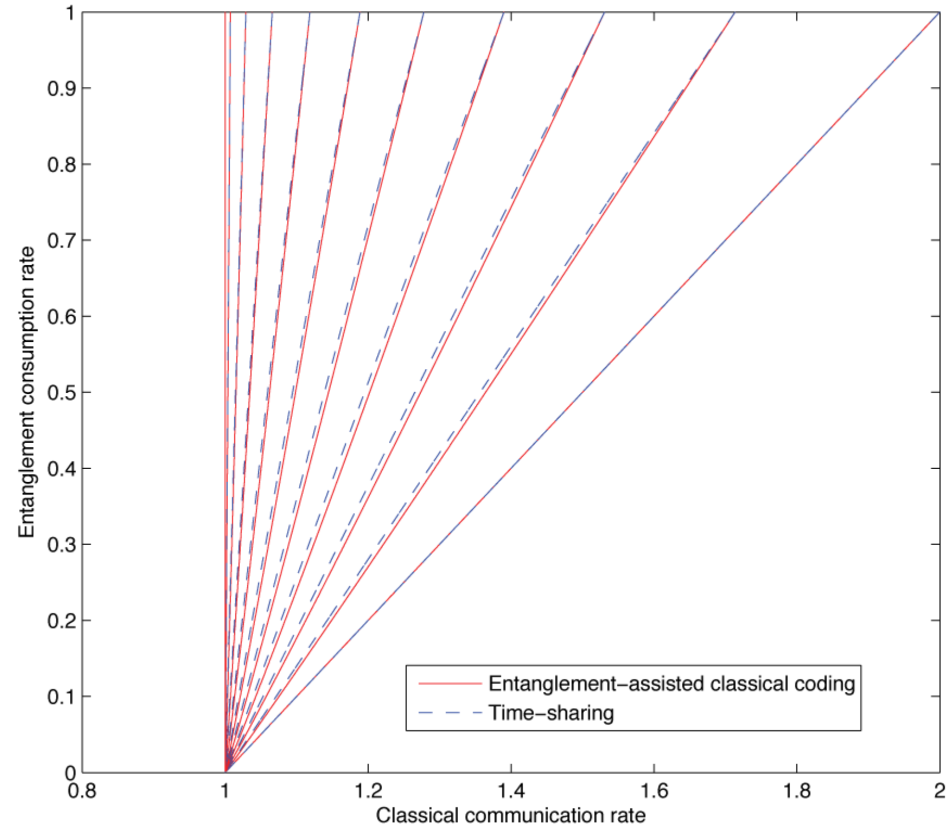
Chain rule for quantum mutual information

Wilde and Hsieh. The quantum dynamic capacity formula of a quantum channel. arXiv:1004.0458.

Trade-off Coding for Dephasing Channels



Classical-Quantum Trade-off



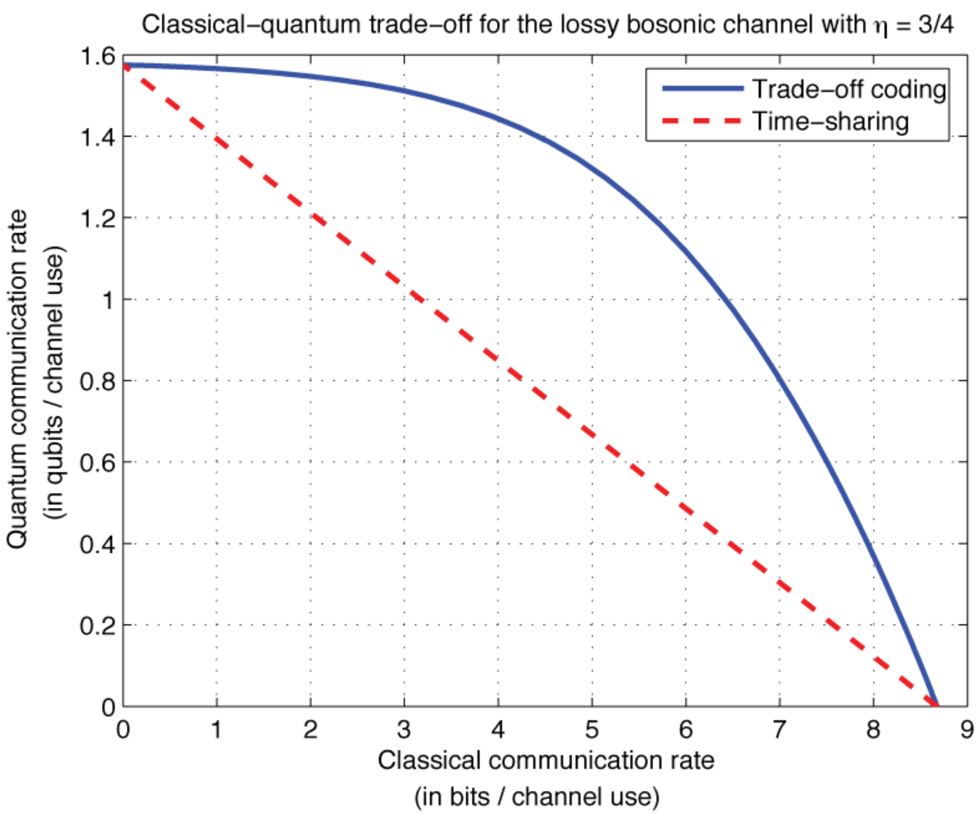
Classical-Ent. Trade-off

Trade-offs for a **qubit dephasing channel** with various noise levels *just barely* beat time-sharing

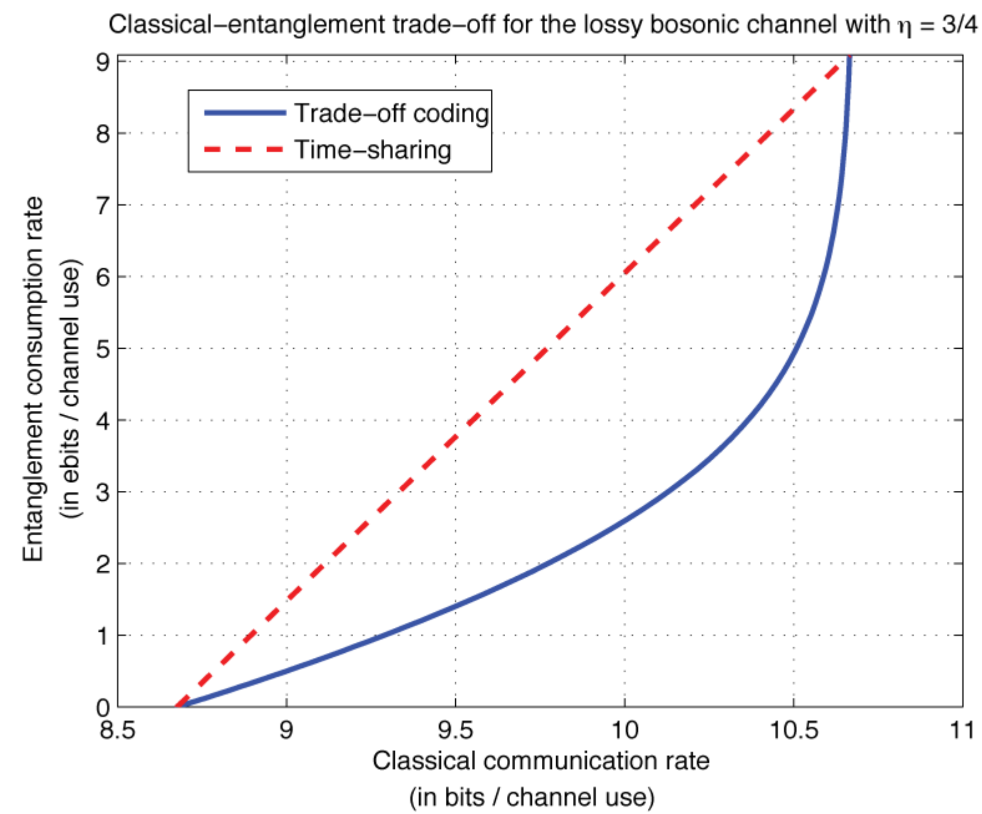
Why then would you implement a trade-off coding strategy in practice?

Bradler, Hayden, Touchette, Wilde. Physical Review A 81, 062312 (2010)

Trade-off Coding for Bosonic Channels



Classical-Quantum Trade-off



Classical-Ent. Trade-off

Trade-off is *so strong* for **bosonic channels**
that it would be **silly** not to use such a strategy

Wilde, Hayden, Guha. arXiv:1105.0119

Power-Sharing Coding Strategy

Coding Ensemble:

$$\left\{ p_{(1-\lambda)N_S}\left(\alpha\right), D^{A'}\left(\alpha\right)\left|\psi_{\text{TMS}}\right\rangle^{AA'} \right\}.$$

where

$$p_{(1-\lambda)N_S}\left(\alpha\right) \equiv \frac{1}{\pi(1-\lambda)N_S} \exp\left\{ -\left|\alpha\right|^2 / (1-\lambda)N_S \right\}$$

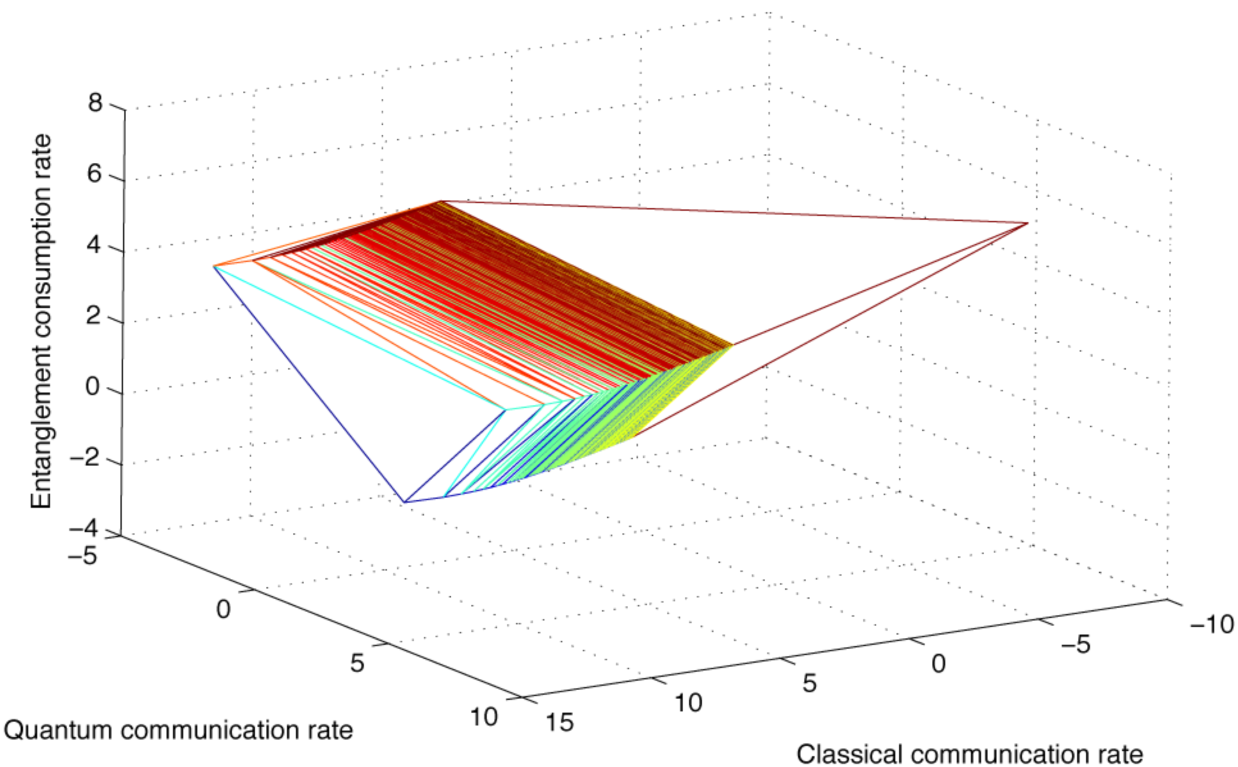
$$\left|\psi_{\text{TMS}}\right\rangle^{AA'} \equiv \sum_{n=0}^{\infty} \sqrt{\frac{\left[\lambda N_S\right]^n}{\left[\lambda N_S + 1\right]^{n+1}}} \left|n\right\rangle^{A} \left|n\right\rangle^{A'}$$

Wilde, Hayden, Guha. arXiv:1105.0119

Achievable Rate Region for Lossy Channel

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

λ is a **power-sharing parameter** between zero and one



Wilde, Hayden, Guha. arXiv:1105.0119

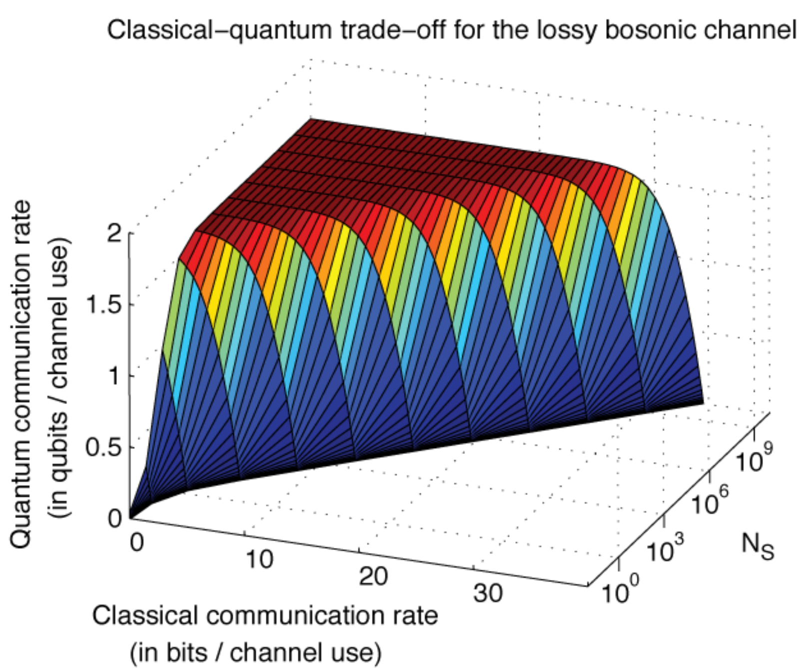
Rule of Thumb for Trade-off Coding

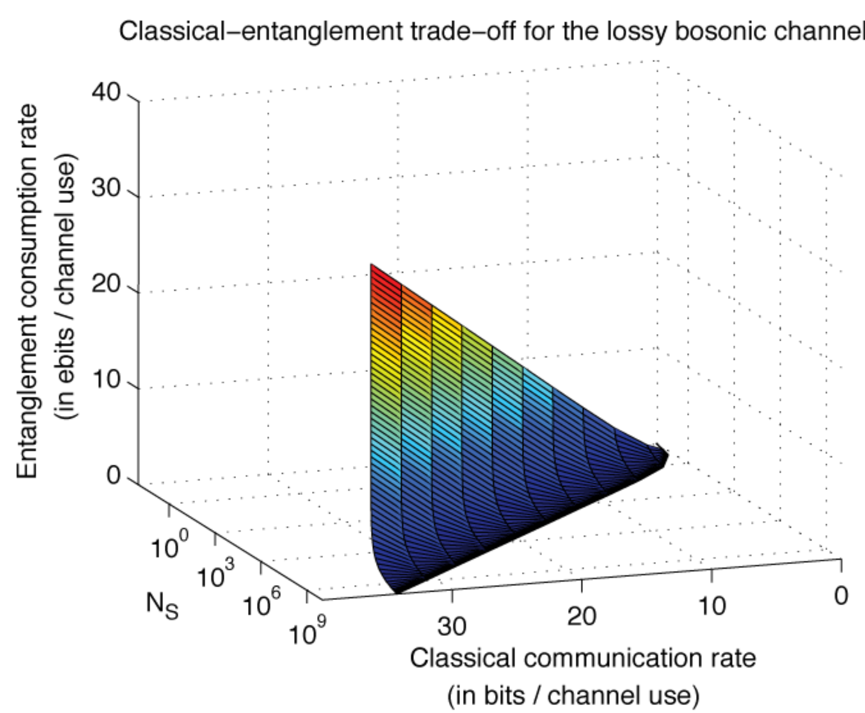
To be within ϵ bits of quantum capacity, choose

$$\lambda = 1/\left[\eta\left(1-\eta\right)\epsilon N_S \ln 2\right]$$

To be within ϵ bits of EA capacity, choose

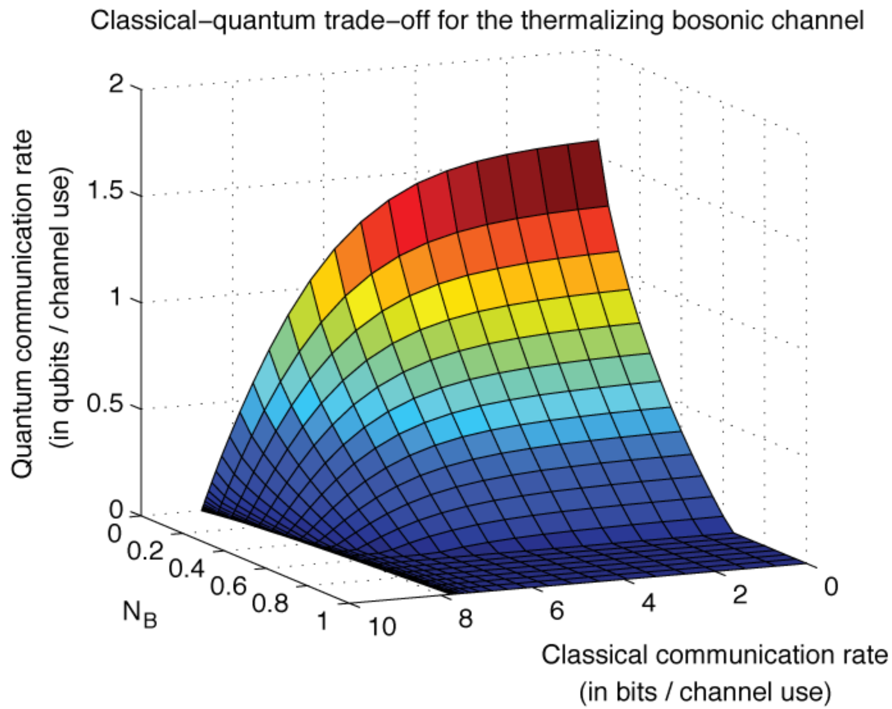
$$\lambda = 5/\left[6\epsilon N_S\left(1-\eta\right)\ln 2\right]$$

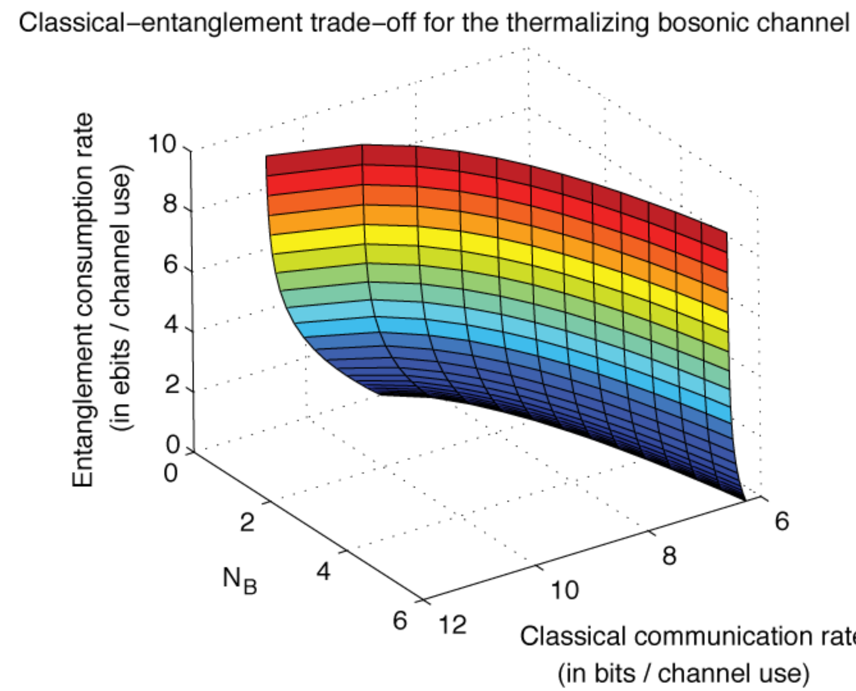




Wilde, Hayden, Guha. arXiv:1105.0119

Thermal Channel Trade-offs

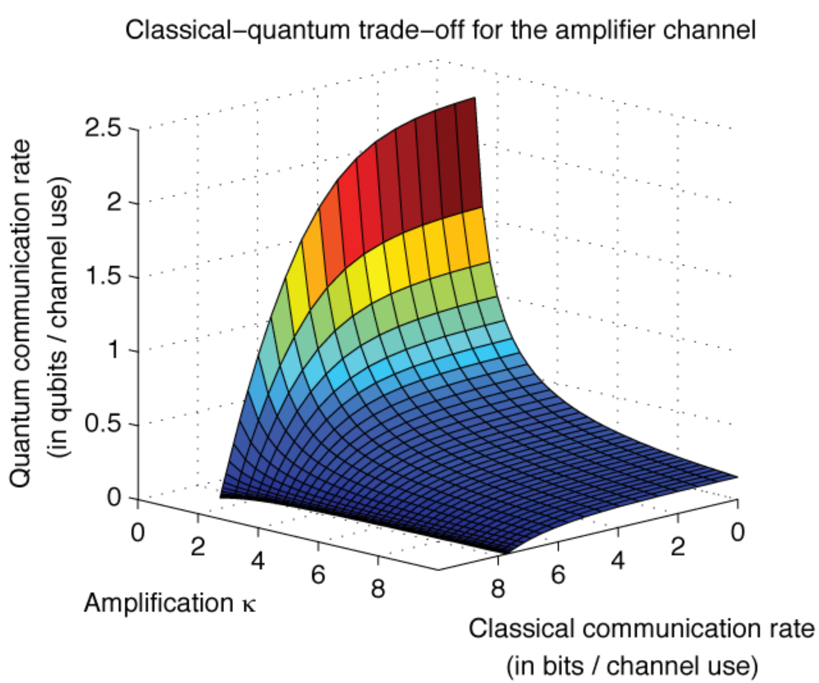


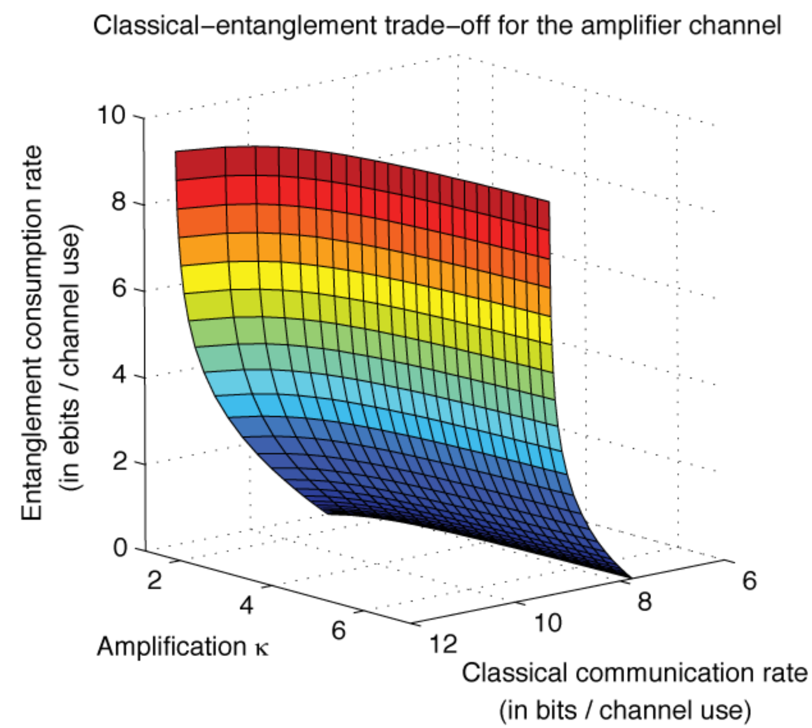


Thermal noise destroys **quantum correlations** more easily than it does **classical correlations**

Wilde, Hayden, Guha. arXiv:1105.0119

Amplifier Channel Trade-offs





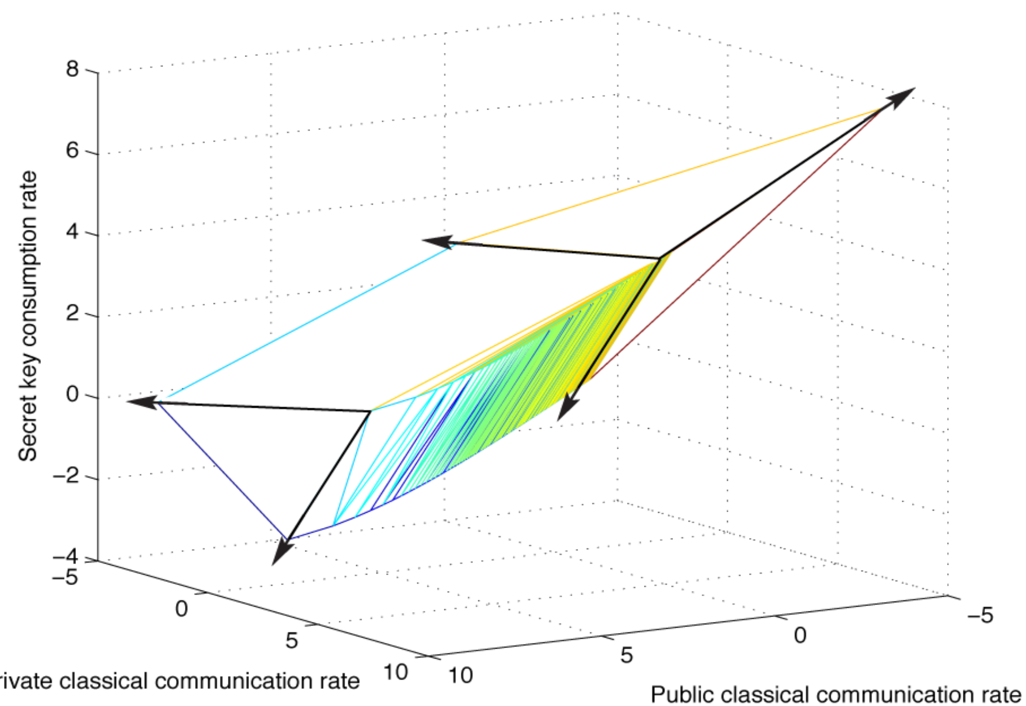
Amp noise destroys **quantum correlations** more easily than it does **classical correlations**

Wilde, Hayden, Guha. arXiv:1105.0119

Trading Public and Private Resources

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

Coding ensemble: $\left\{ p_{\overline{\lambda} N_S}(\alpha)\, p_{\lambda N_S}(\beta), |\alpha + \beta\rangle \right\}$



Wilde, Hayden, Guha. arXiv:1105.0119

Conclusion

Power-sharing significantly outperforms
time-sharing between the best known protocols

Is this region *optimal*?

Do there exist structured encoders and decoders
to achieve these rates?