

Title: An introduction to quantum channels and their capacities

Date: Nov 07, 2012 02:00 PM

URL: <http://pirsa.org/12110066>

Abstract: <span>A quantum communication channel can be put to many uses: it can transmit classical information, private classical information, or quantum information.

It can be used alone, with shared entanglement, or together with other channels. For each of these settings there is a capacity that quantifies a channel's fundamental potential for communication. &nbsp;In this introductory talk, I will discuss what we know about the various capacities of a quantum channel, including a discussion of synergies between different channels and related additivity questions.</span>

$$N(P) = T E U \rho \otimes \rho \otimes U^T$$

$A \rightarrow B$



# Introduction to quantum channel capacities

Graeme Smith  
IBM TJ Watson Research Center

Perimeter Institute Colloquium  
November 7<sup>th</sup> 2012

# Information



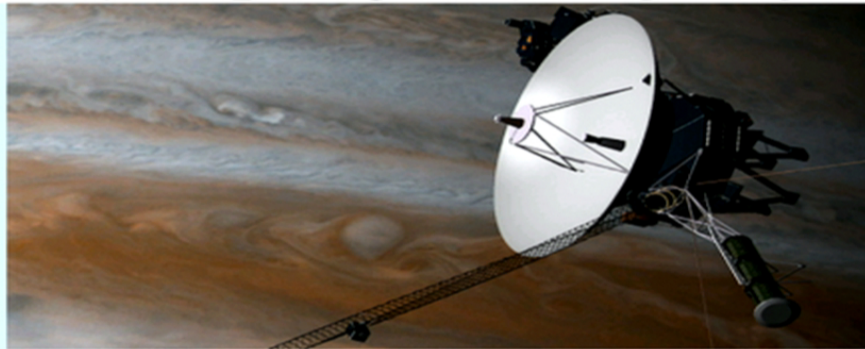
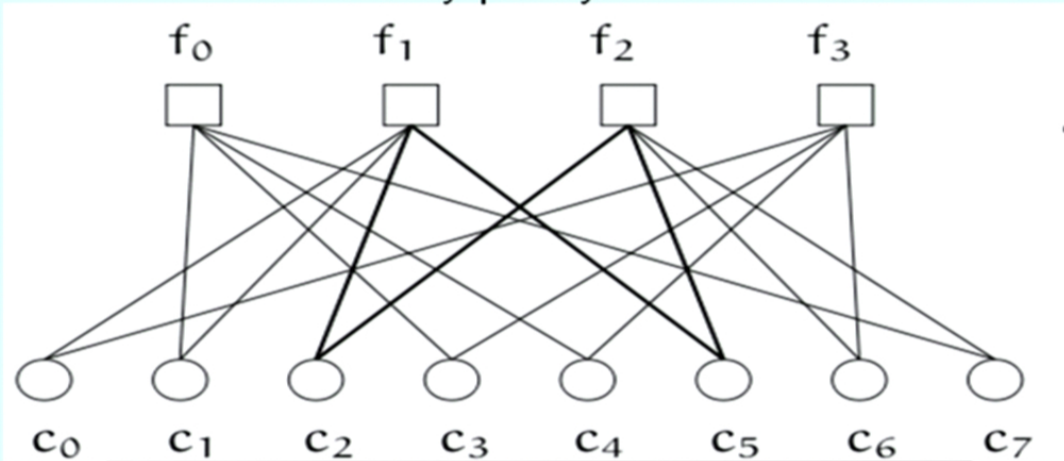
**“The most valuable commodity I know of is information.” -Gordon Gekko, Wall Street (1987)**

# Information Theory

- “A Mathematical Theory of Communication”, C.E. Shannon, 1948
- Lies at the intersection of Electrical Engineering, Mathematics, and Computer Science
- Concerns the reliable and efficient storage and transmission of information.

# Information Theory: Some Hits

Low density parity check codes



Voyager (Reed Solomon codes)



Cell Phones



Lempel-Ziv compression (gunzip, winzip, etc)

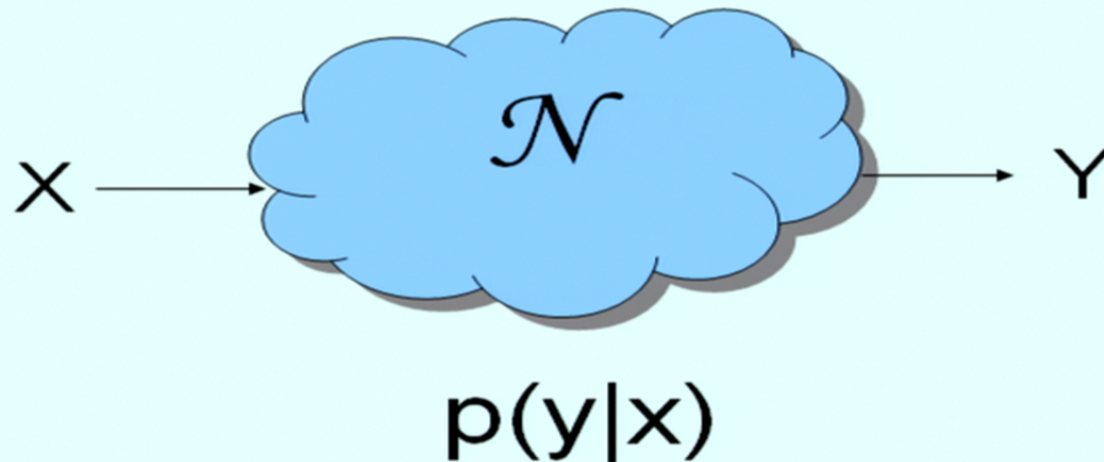
# Quantum Shannon Theory

When we include quantum mechanics (which was there all along!) things get much more interesting!

Secure communication, entanglement enhanced communication, sending quantum information,...

Capacity, error correction, compression, entropy..

# Channel Capacity



Capacity: bits per channel use in the limit of many channels

$$C = \max_x I(X;Y)$$

$I(X;Y) = H(X)+H(Y)-H(XY)$  is the mutual information



# Outline

- Quantum capacity of quantum channel
- Sketch coherent information achievability
- Additivity and superadditivity (quantum synergy!)
- Classical and private capacities
- Gaussian quantum channels
- Open questions

# Quantum Capacities

There are several kinds of information you can try to send with a quantum channel:

- Classical Information
- Private Classical Information
- Quantum Information

There are different capacities for each of these. Actually, there are even more: I might give you free entanglement or free two-way classical communication to help.

# Quantum Capacities

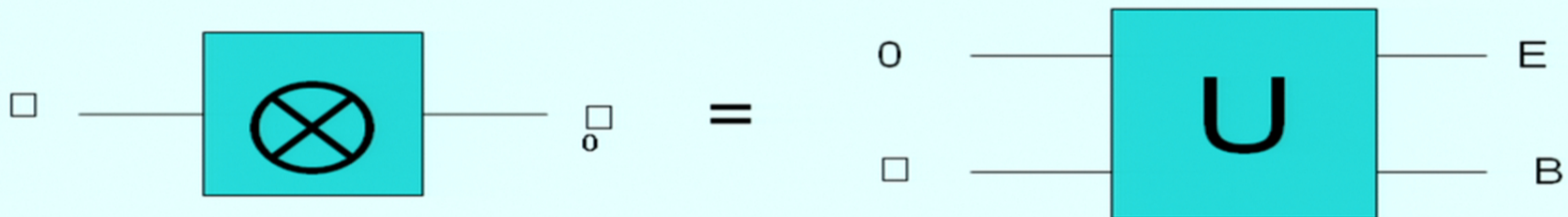
There are several kinds of information you can try to send with a quantum channel:

- Classical Information
- Private Classical Information
- **Quantum Information**

There are different capacities for each of these. Actually, there are even more: I might give you free entanglement or free two-way classical communication to help.

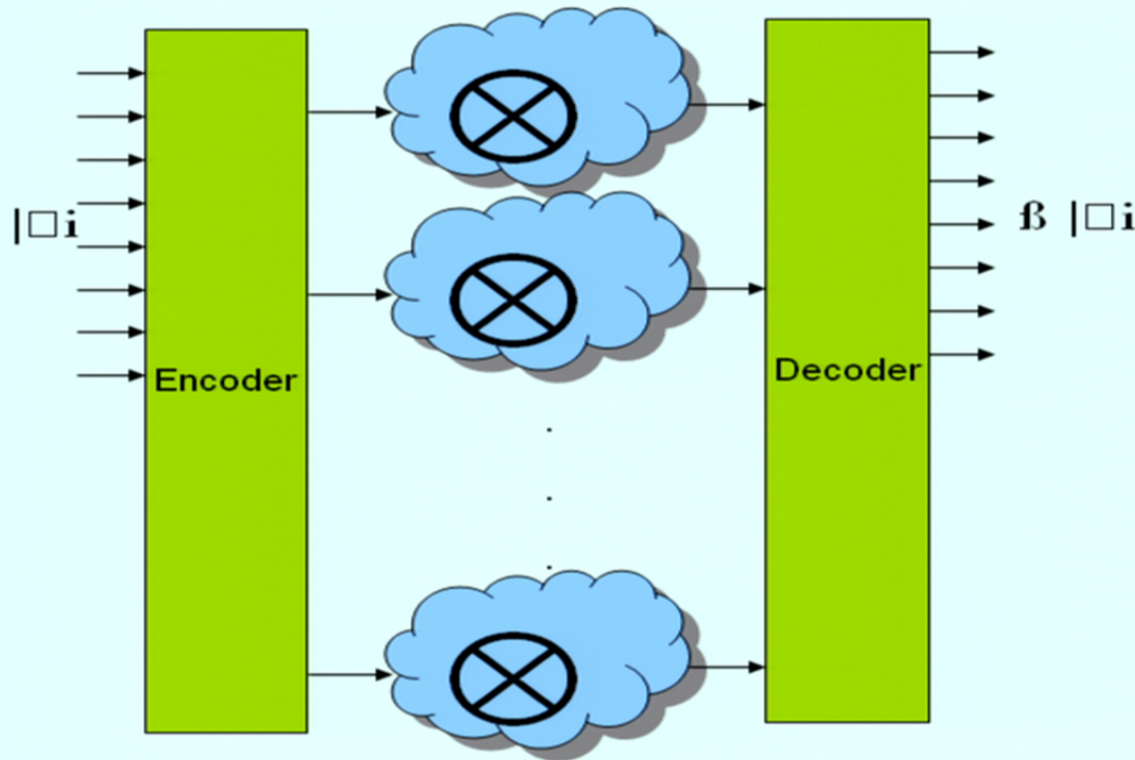
# Noisy Quantum Channels

- Noiseless quantum evolution:  $\rho \rightarrow U\rho U^\dagger$   
Unitary satisfies  $U^\dagger U = I$
- Noisy quantum evolution: unitary interaction with inaccessible environment



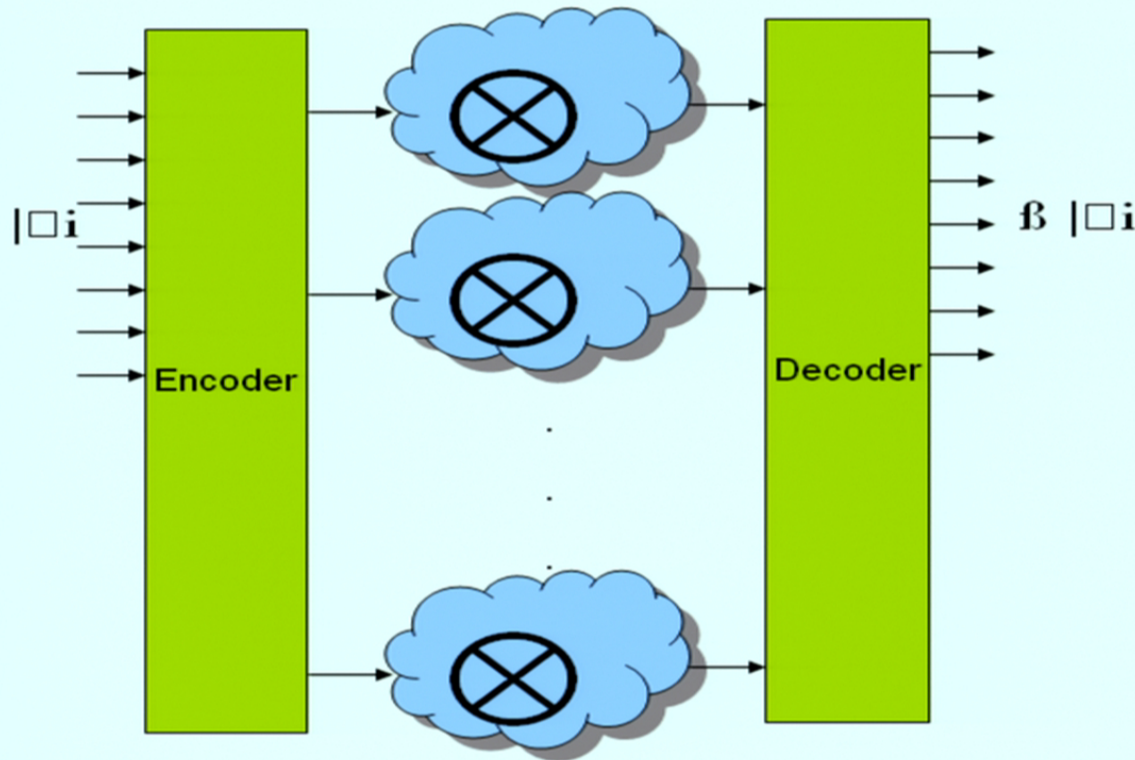
$$\rho_B = \text{Tr}_E U(\rho_B \otimes |0\rangle\langle 0|_E) U^\dagger$$

# Quantum Capacity



- If we try to transmit an arbitrary quantum state, we arrive at the quantum capacity,  $Q(\mathcal{N})$ .
- The quantum capacity, measured in qubits per channel use, characterizes the ultimate limit on quantum error correction.

# Quantum Capacity



Define the coherent information:

$$Q^1(\mathcal{N}) = \max_{\phi} H(B) - H(E),$$

with entropies evaluated on  $U_{\phi}U^{\dagger}$ . Then, we can show that  $Q^1(\mathcal{N})$  is an achievable rate for quantum communication, so

$$Q(\mathcal{N}) \geq Q^1(\mathcal{N})$$

Furthermore,

$$Q(\mathcal{N}) =$$

$$\lim_{n \rightarrow \infty} (1/n) Q^1(\mathcal{N} \otimes \dots \otimes \mathcal{N})$$

See Lloyd 97, Shor 02, Devetak 03

$$N(P) = T E U \rho \otimes \rho \otimes U^T$$

$A \rightarrow B$



# Coherent Information and no-cloning

- **No cloning:** there is no physical operation that copies an unknown quantum state.
- Basically, because  $|\psi\rangle \rightarrow |\psi\rangle|\psi\rangle$  isn't linear

$H(B)$  is how much information B has

$H(E)$  is how much information E has

$Q^1 = H(B) - H(E)$  is how much more Bob knows than Eve.

$\approx$  how much secret information we can send to Bob



# Outline

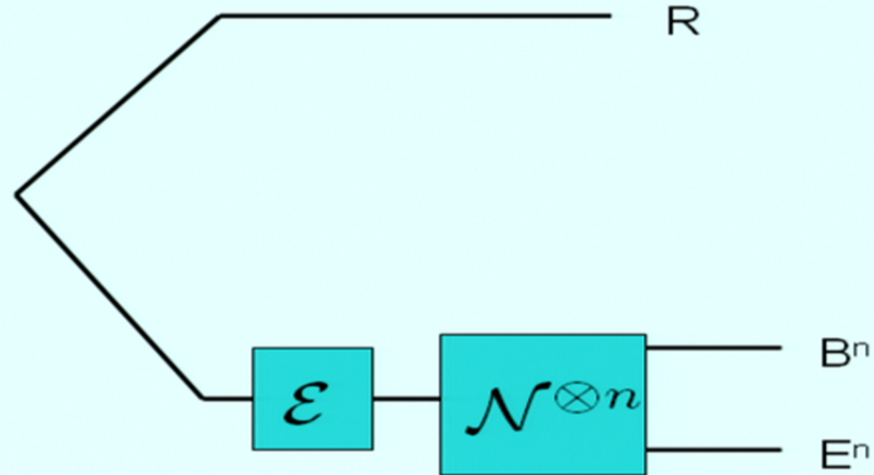
- ~~Quantum capacity of quantum channel~~
- Quantum coding theorem
- Additivity and superadditivity (quantum synergy!)
- classical and private capacities
- Gaussian quantum channels
- Open questions

# Sketch of Achievability of Coherent Information

- Step 1: If you can transmit half of a maximally entangled state reliably, then you can transmit a quantum state.
- Step 2: If you can decouple your reference system from the environment, then you have a pure entangled state.

Hayden, Horodecki, Yard, Winter '08

# Decoupling

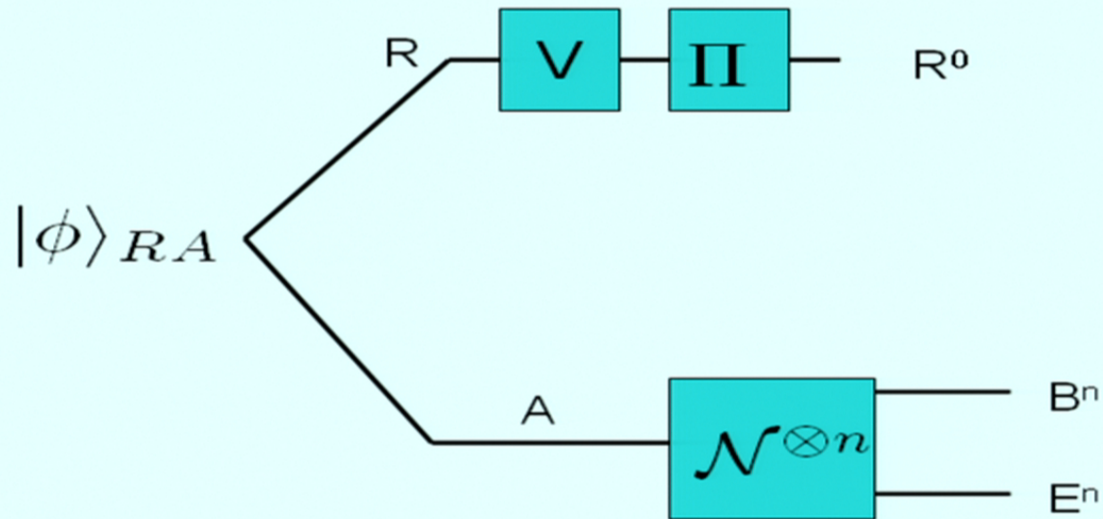


If  $\rho_{RE^n} \approx \rho_R \otimes \rho_{E^n}$ , then  $\rho_{RB_1B_2E^n} = |\varphi\rangle_{RB_1} |\psi\rangle_{B_2E^n}$

# Entropy and Typical Spaces

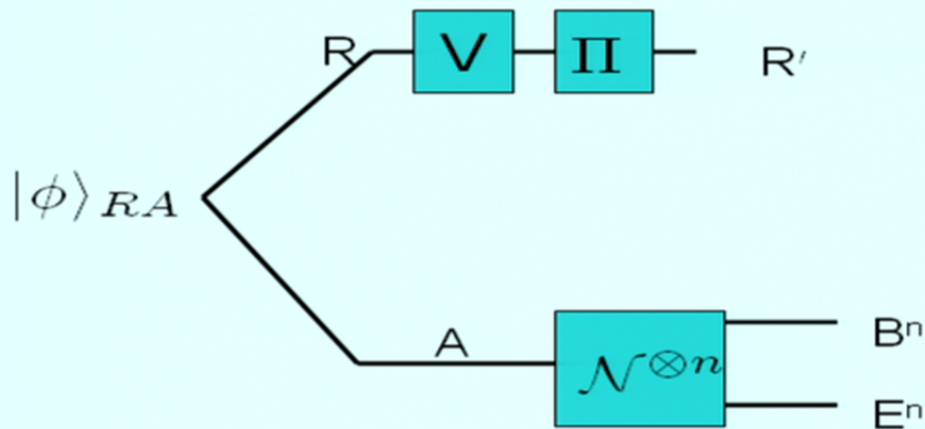
- Any  $\rho_B = \text{Tr}_A |\psi\rangle\langle\psi|_{AB}$
- $H(\rho_B) = -\text{Tr} \rho_B \log \rho_B$  is the entropy
- It measures the uncertainty in B
- Given n copies of  $|\psi\rangle_{AB}$ , we can reversibly map B to a space of dimension  $2^{n H(\rho_B)}$ . This is the “typical space.”

# Decoupling with Random encoding



$$|\phi\rangle_{RA} = \frac{1}{\sqrt{|R|}} \sum_{i=1}^{|R|} |i\rangle |i\rangle$$

# Decoupling with Random encoding



Choose  $V$  randomly.

Consider the state this circuit generates on  $R'E^n$ .

$$\left( \int dV \|\sigma_{R'E^n}(V) - \sigma_{R'}^{\max} \otimes \sigma_{E^n}\|_1 \right)^2 \leq |R'E^n| (\text{Tr}(\sigma_{RE^n}))^2$$

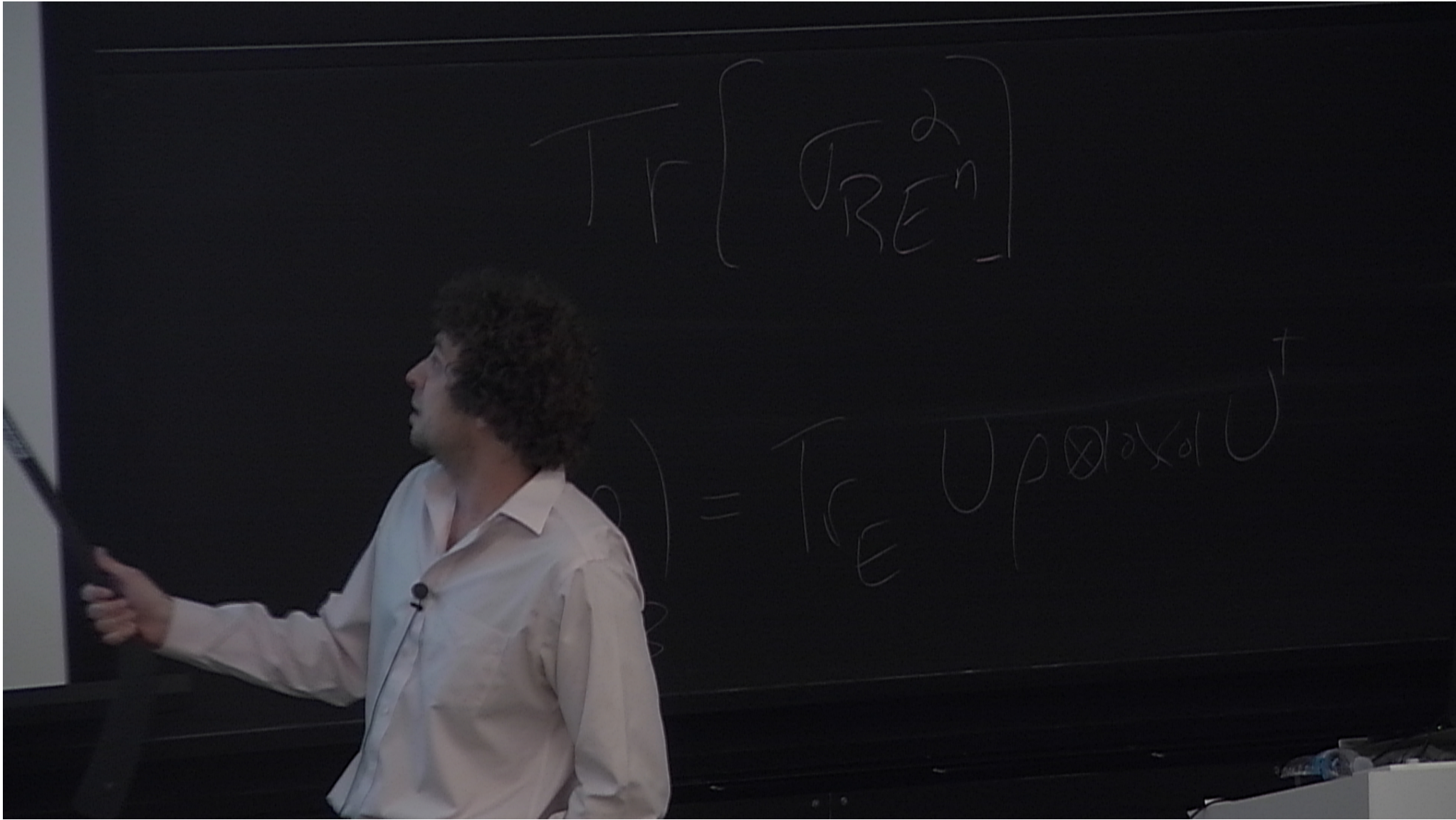
Estimate:  $|R'| = 2^{n(\text{rate})}$

$|E^n| \approx 2^{n H(E)}$

Spectrum of  $RE$  is same as spectrum of  $B$ . When iid, this is maximally mixed with dimension  $2^{nH(B)}$ . This gives  $(\text{Tr}(\sigma_{RE^n}))^2 \approx \frac{1}{2^{nH(B)}}$

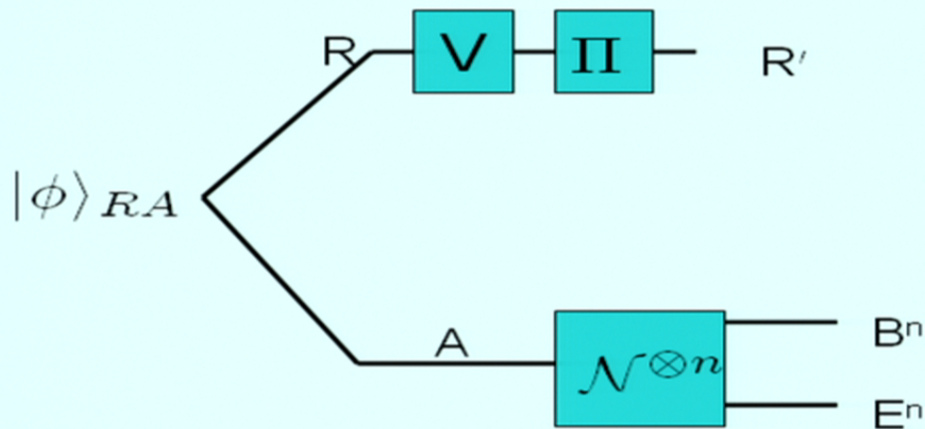
$$\text{Tr} \left[ \sqrt{\rho} \right]$$

$$= \text{Tr} \left[ U \rho U^\dagger \right]$$





# Decoupling with Random encoding



So, as long as  $\text{rate} < S(B) - S(E)$ , the deviation from a product state between  $R'$  and  $E^n$  becomes arbitrarily small. Which enables transmission.

Choose  $V$  randomly.

Consider the state this circuit generates on  $R'E^n$ .

$$\left( \int dV \|\sigma_{R'E^n}(V) - \sigma_{R'}^{\max} \otimes \sigma_{E^n}\|_1 \right)^2 \leq |R'E^n| (\text{Tr}(\sigma_{RE^n})^2)$$

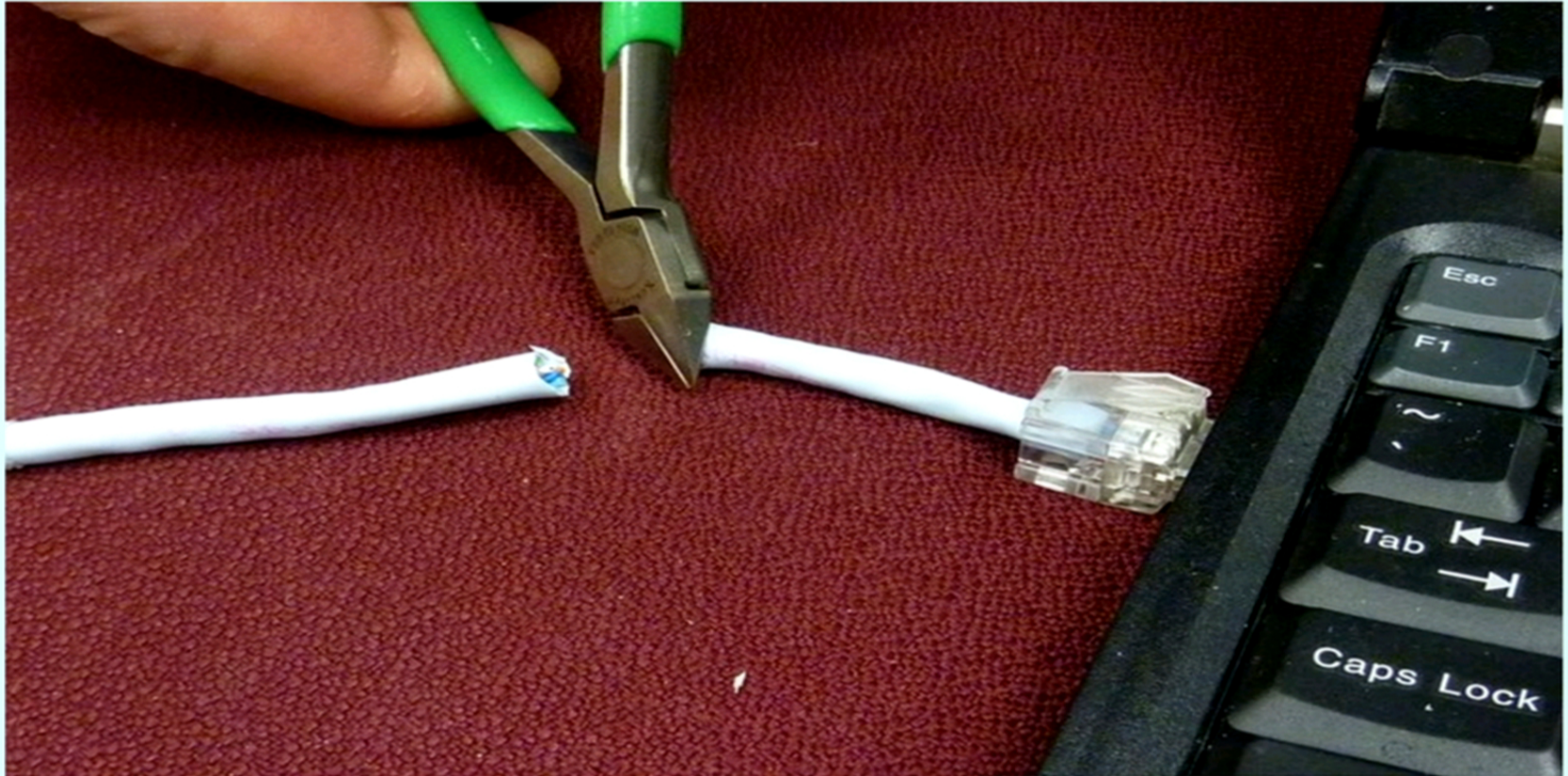
Estimate:  $|R'| = 2^{n(\text{rate})}$

$|E^n| \approx 2^{n H(E)}$

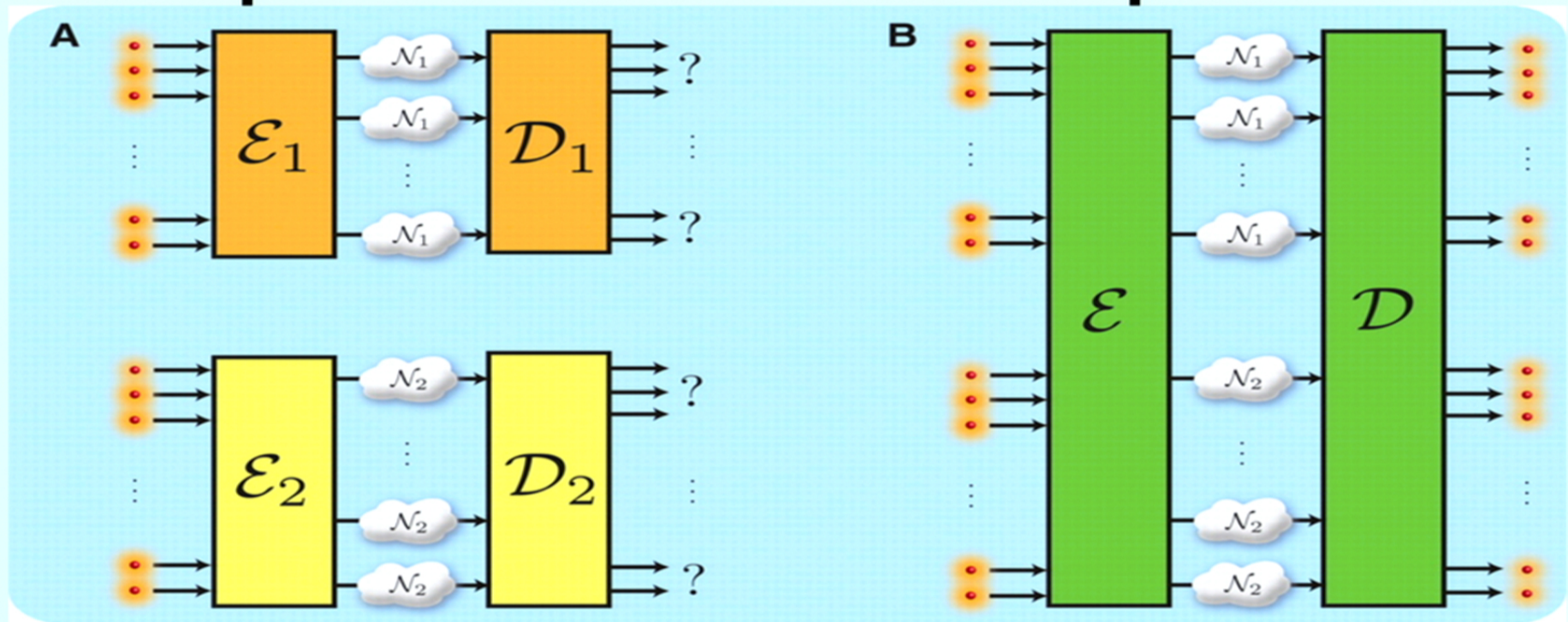
Spectrum of  $RE$  is same as spectrum of  $B$ . When iid, this is maximally mixed with dimension  $2^{nH(B)}$ . This gives  $(\text{Tr}(\sigma_{RE^n})^2) \approx \frac{1}{2^{nH(B)}}$

# Outline

- ~~Quantum capacity of quantum channel~~
- ~~Quantum coding theorem~~
- Zero Quantum capacity channels and Superactivation (quantum synergy!)
- Classical and private capacities
- Additivity in general
- Gaussian quantum channels
- Open questions

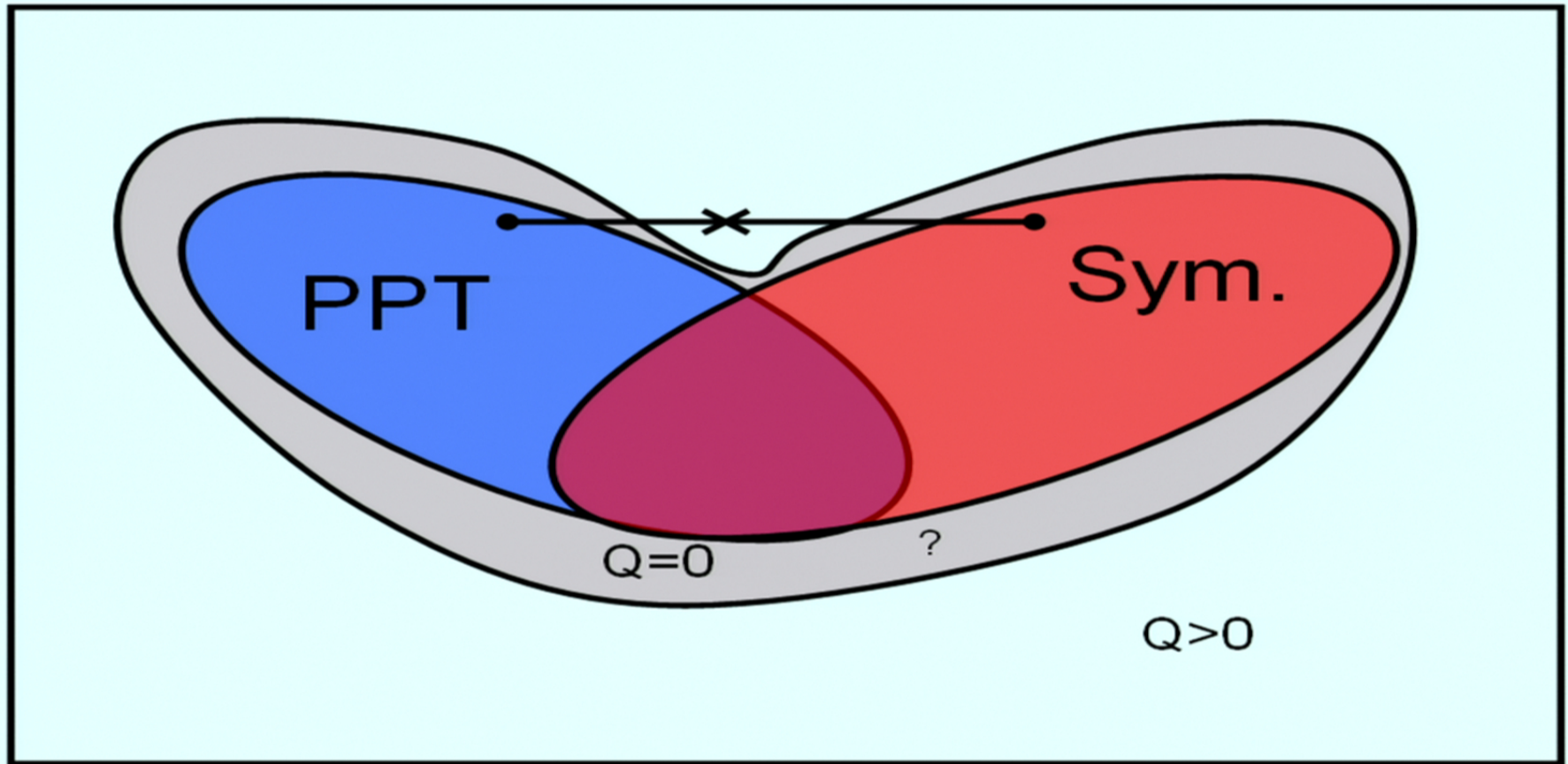


# Superactivation of Capacities

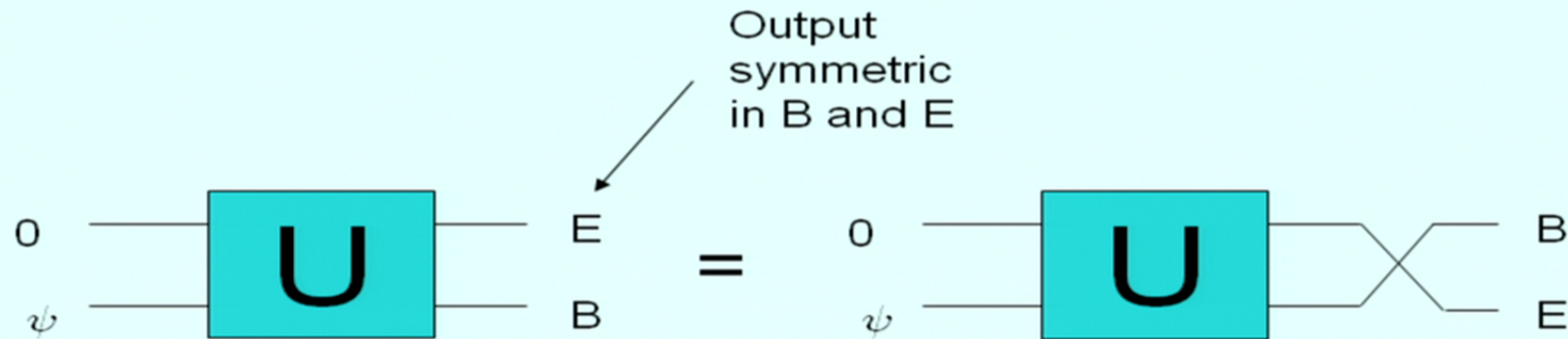


There are  $\mathcal{N}_1, \mathcal{N}_2$  with zero quantum capacity but  $Q(\mathcal{N}_1 \otimes \mathcal{N}_2) > 0$ .  
G. Smith and J. Yard, Science, 321, 1812-1815 (2008)

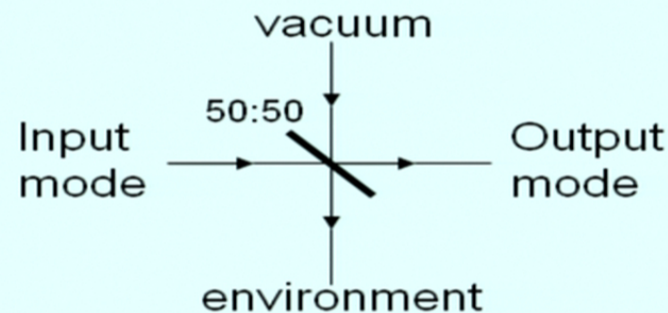
# Zero-quantum-capacity channels



# Zero Quantum Capacity Channels: Symmetric Channels



Example: 50% attenuation channel



# Zero Quantum Capacity Channels: Symmetric Channels

Suppose a symmetric channel had  $Q > 0$



# Zero Quantum Capacity Channels: Symmetric Channels

Suppose a symmetric channel had  $Q > 0$





# Zero Quantum Capacity Channels: Symmetric Channels

Suppose a symmetric channel had  $Q > 0$



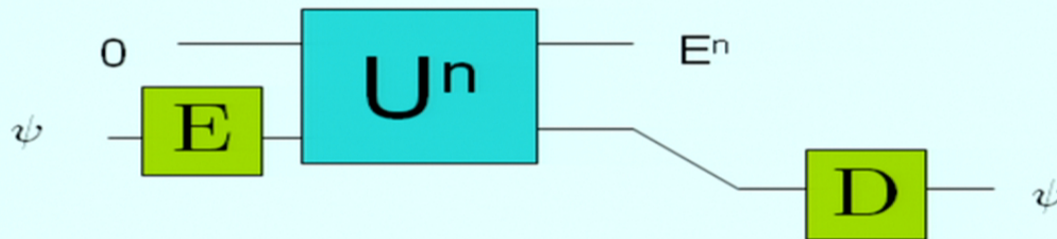
# Zero Quantum Capacity Channels: Symmetric Channels

Suppose a symmetric channel had  $Q > 0$



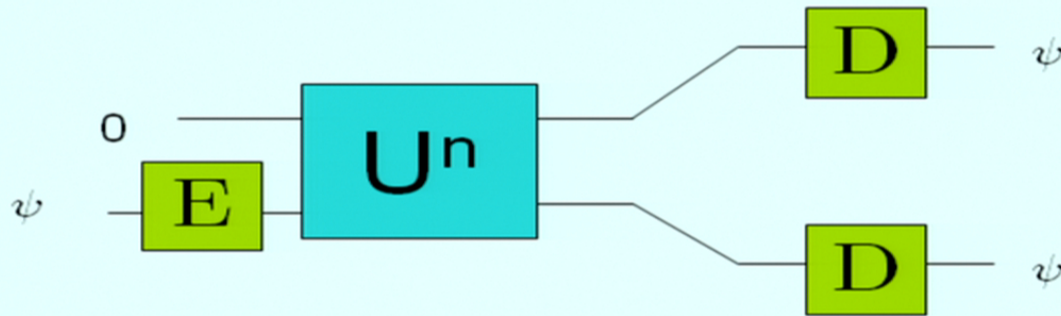
# Zero Quantum Capacity Channels: Symmetric Channels

Suppose a symmetric channel had  $Q > 0$



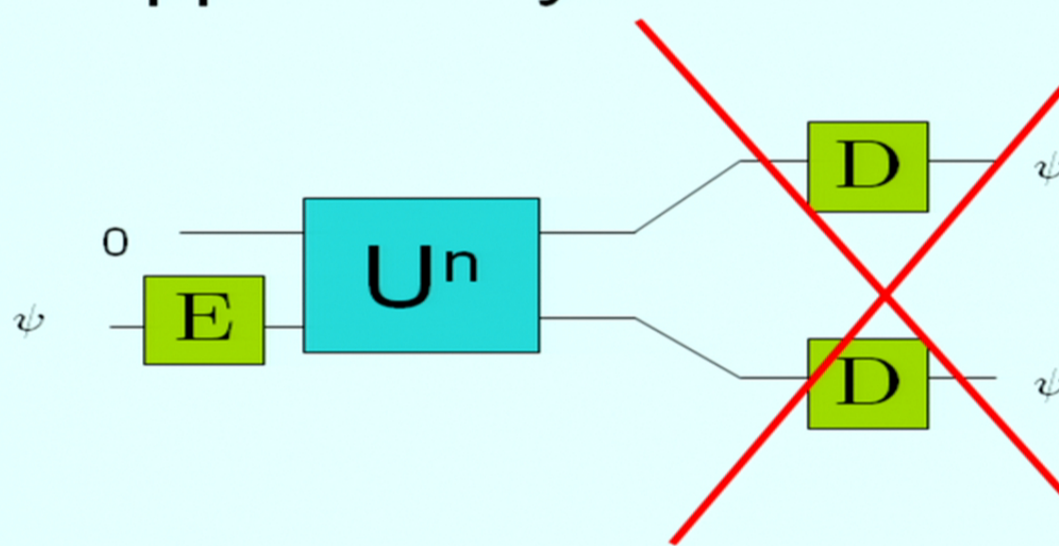
# Zero Quantum Capacity Channels: Symmetric Channels

Suppose a symmetric channel had  $Q > 0$



# Zero Quantum Capacity Channels: Symmetric Channels

Suppose a symmetric channel had  $Q > 0$



So, symmetric channels must have zero quantum capacity. Specifically, the 50% erasure channel has zero capacity. It will be one of our two zero quantum capacity channels.

## IMPOSSIBLE!

# Zero Quantum Capacity Channels: Positive Partial Transpose

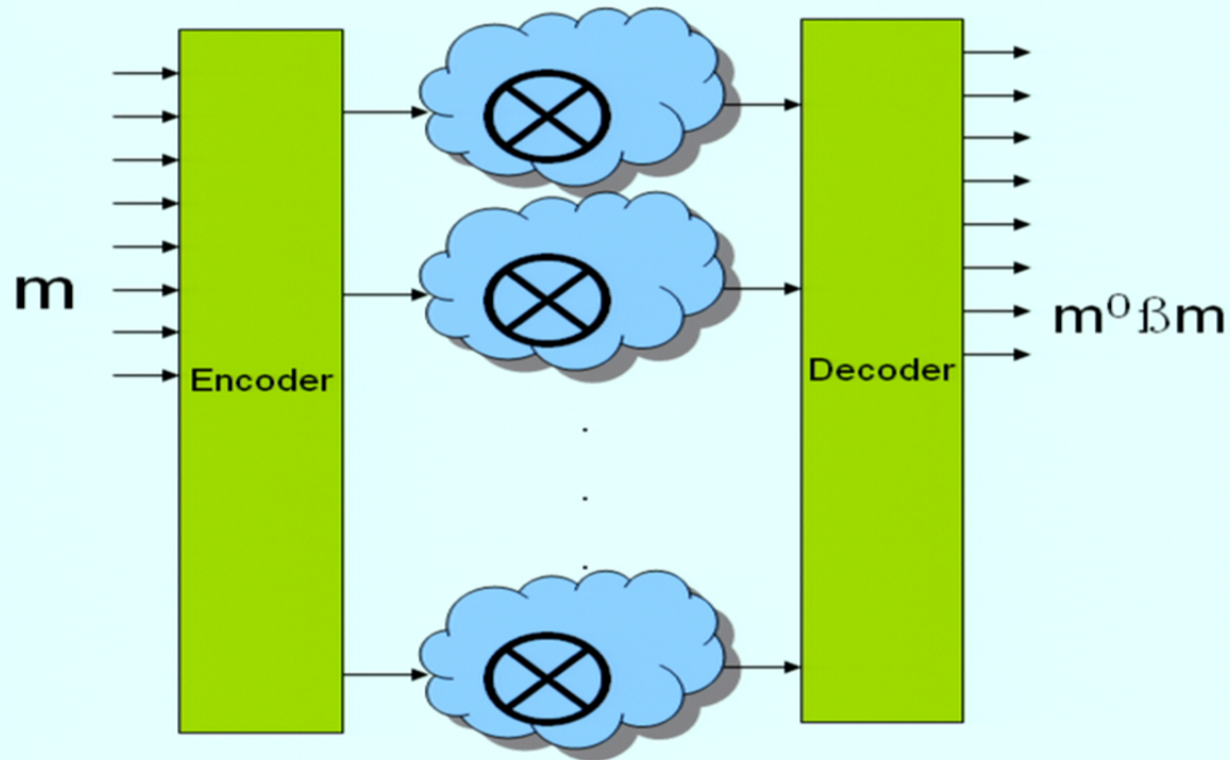
- Partial transpose:  
 $(|i\rangle\langle j|_A \otimes |k\rangle\langle l|_B)^T = |i\rangle\langle j|_A \otimes |l\rangle\langle k|_B$
- If  $\rho_{AB}^T$  is not positive, then the state is entangled
- If  $\rho_{AB}^T \geq 0$ , it may be entangled, but then it is *very noisy*. Bound entanglement---can't get any pure entanglement from it.
- A PPT-channel enforces PPT between output and purification of the input:  
 $\rho_{AB} = I \otimes \mathcal{N}(\phi_{AB})$  is PPT
- Implies  $Q(\mathcal{N}) = 0$

Peres, Horodeckis '96

# Outline

- ~~Quantum capacity of quantum channel~~
- ~~Quantum coding theorem~~
- ~~Zero Quantum capacity channels and Superactivation (quantum synergy!)~~
- Classical and private capacities
- Additivity in general
- Gaussian quantum channels
- Open questions

# Classical Capacity of Quantum Channel



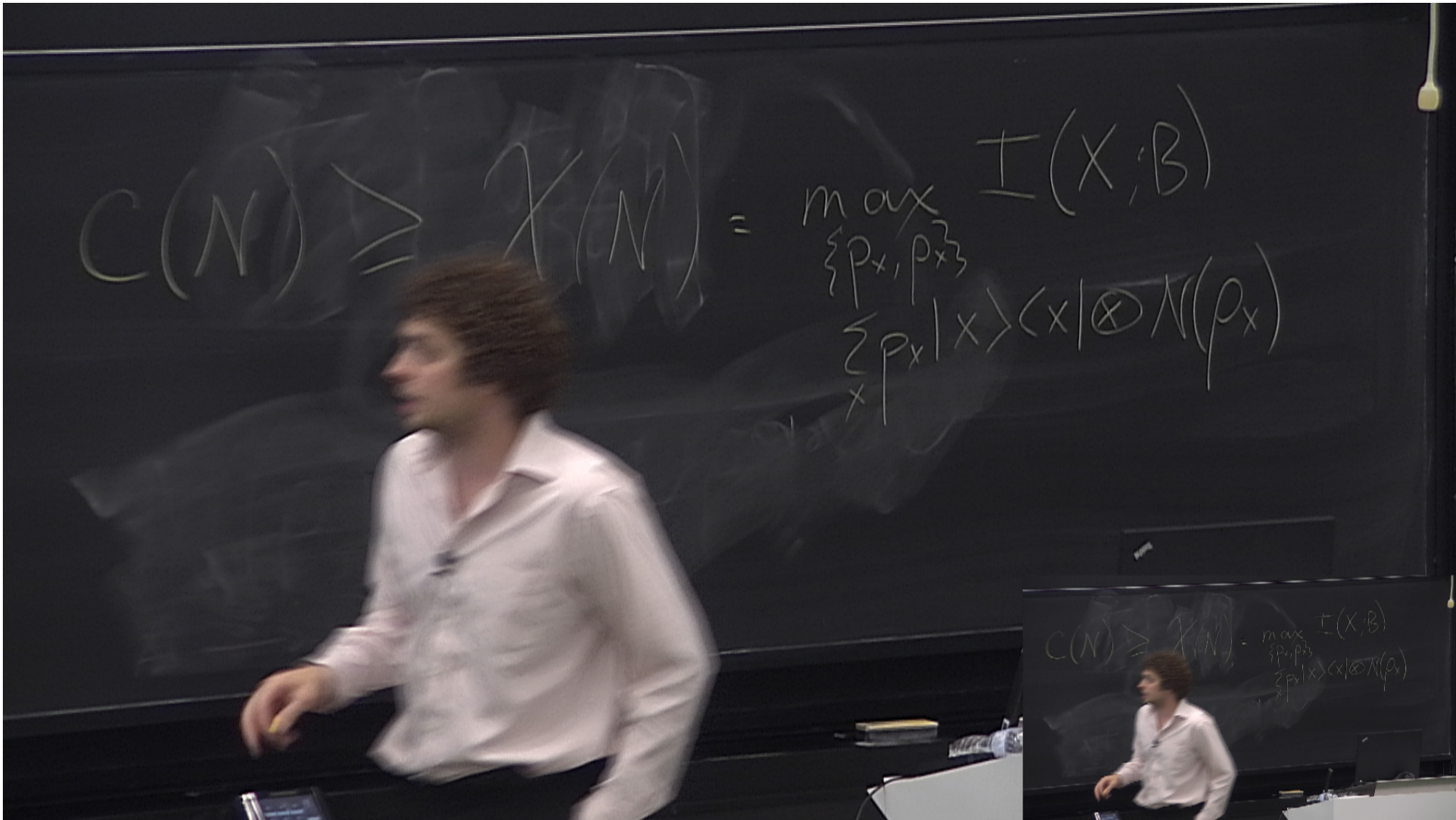
Send a classical message over a quantum message using a code

$$m \rightarrow \rho_m$$

such that all  $\rho_m$  can be distinguished at the channel output.

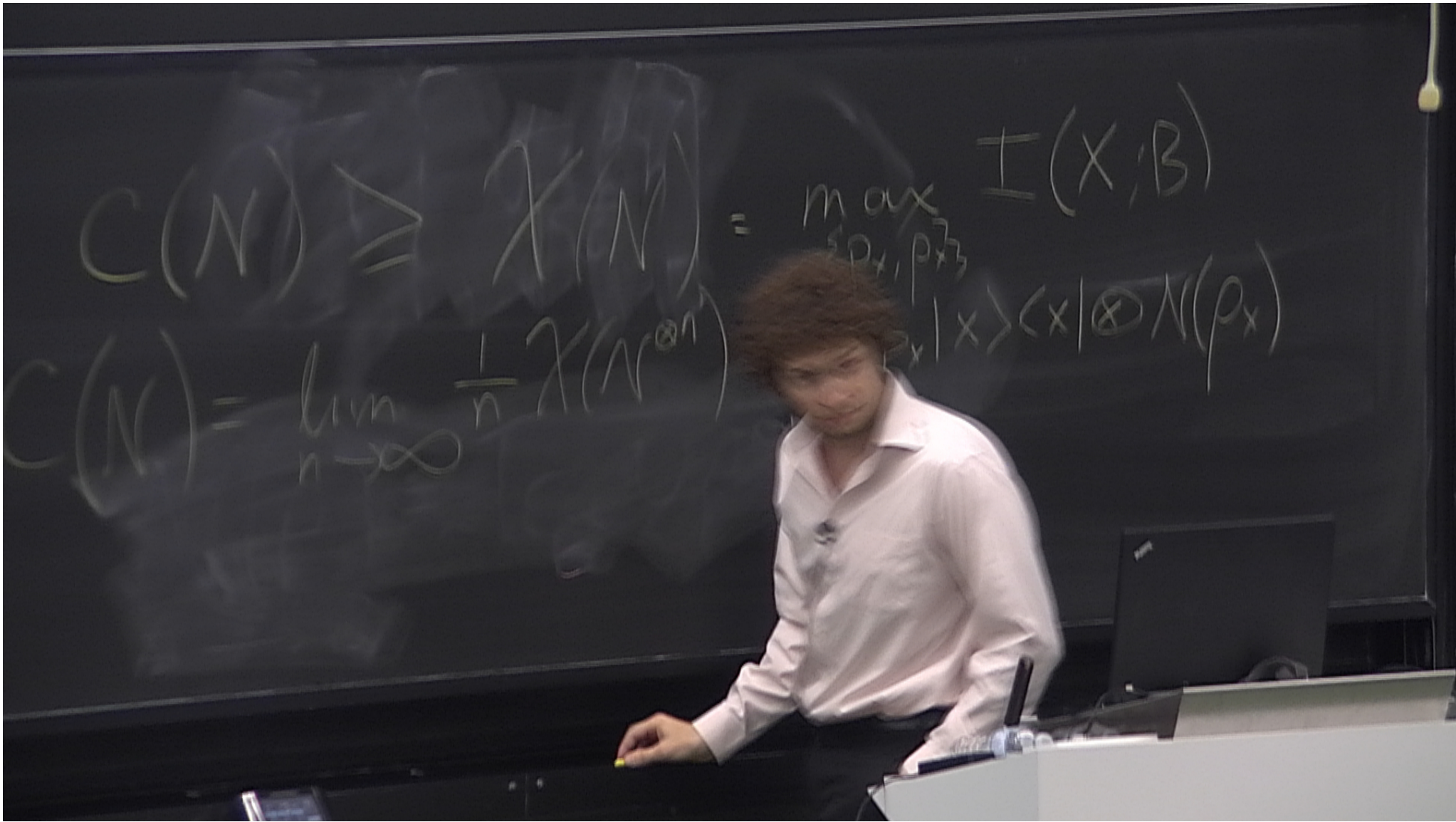
$C(\chi)$  is the capacity



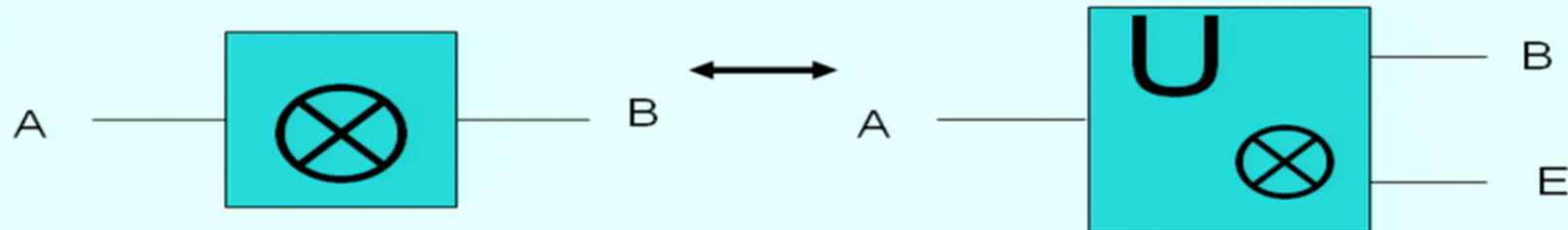


$$C(N) \geq I(N) = \max_{\{p_x, p_{x^3}\}} I(X; B)$$
$$\sum_x p_x |x\rangle \langle x| \otimes \mathcal{N}(p_x)$$

$$C(N) \geq I(N) = \max_{\{p_x, p_{x^3}\}} I(X; B)$$
$$\sum_x p_x |x\rangle \langle x| \otimes \mathcal{N}(p_x)$$

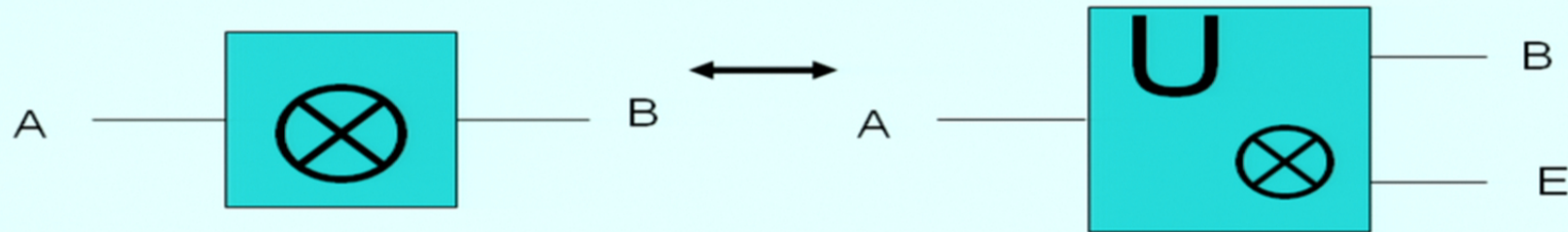


# Private Classical Capacity



- Quantum channel looks like a broadcast channel---one sender, two receivers.
- Best rate for classical messages from A to B while E learns nothing = private capacity. Call it  $P(\mathcal{N})$ .
- Related to quantum key distribution---the fact that by analysing the map from A to B we can infer the map from A to E allows unconditional security that is impossible classically.

# Private Classical Capacity



- Let  $P^1(\mathcal{N}) = \max_{p_v, \phi_v} I(V;B) - I(V;E)$ , with mutual informations evaluated on  $\sum_v p_v |v\rangle\langle v| \otimes U\phi_v U^\dagger$
- Random coding and privacy amplification shows  $P(\mathcal{N}) \geq P^1(\mathcal{N})$  and, in fact we can get

$$P(\mathcal{N}) = \lim_{n \rightarrow \infty} (1/n) P^1(\mathcal{N} \otimes \dots \otimes \mathcal{N})$$

See Devetak IEEE IT 03

n uses

# Classical Capacity of Quantum Channel

We can understand coding schemes for classical information in terms of the Holevo Information:

$$\chi(\mathcal{N}) = \max_{\{p_x, \rho_x\}} I(X;B)$$

where  $I(X;B) = H(X) + H(B) - H(XB)$  uses von Neumann entropy and is evaluated on the state  $\sum_x p_x |x\rangle\langle x| \otimes \mathcal{N}(\rho_x)$

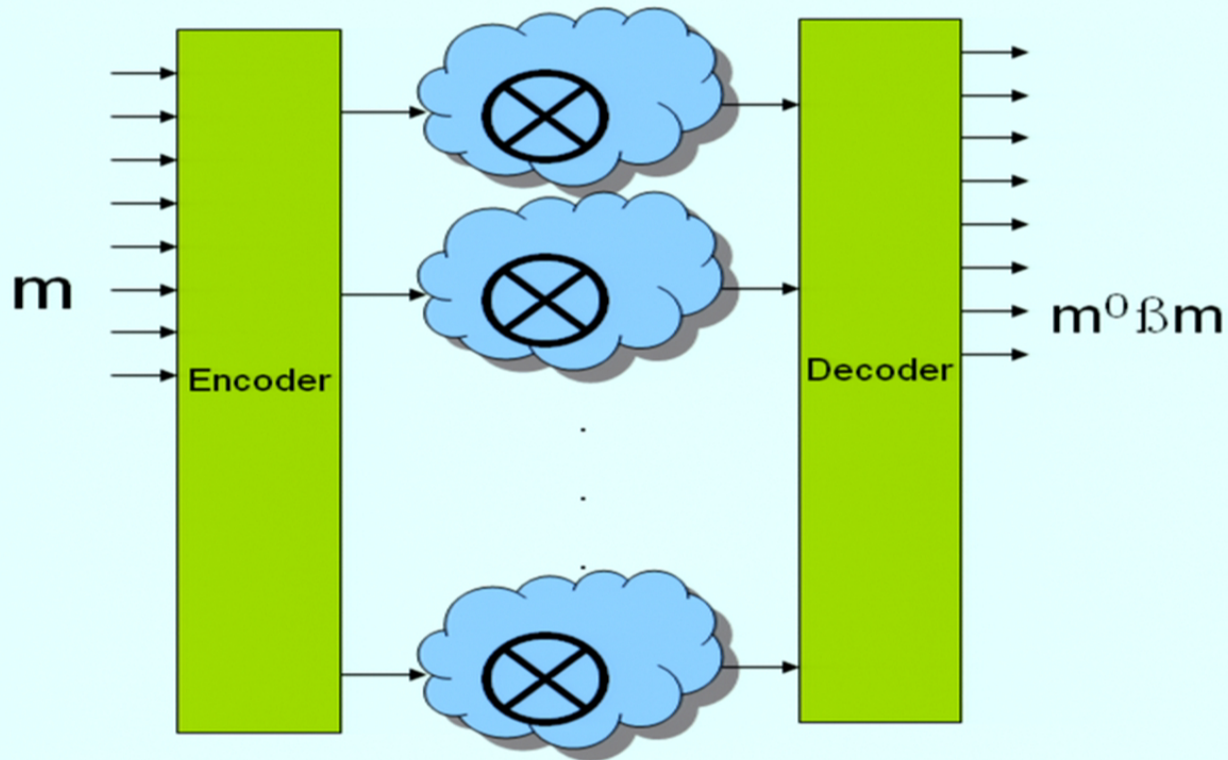
Random coding arguments show that  $\chi(\mathcal{N})$  is an achievable rate, so  $C(\mathcal{N}) \geq \chi(\mathcal{N})$ . Furthermore,

$$C(\mathcal{N}) = \lim_{n \rightarrow \infty} (1/n) \chi(\mathcal{N} \otimes \dots \otimes \mathcal{N})$$

n uses

(see Holevo 73, 79, 98, Schumacher-Westmoreland 97)

# Classical Capacity of Quantum Channel



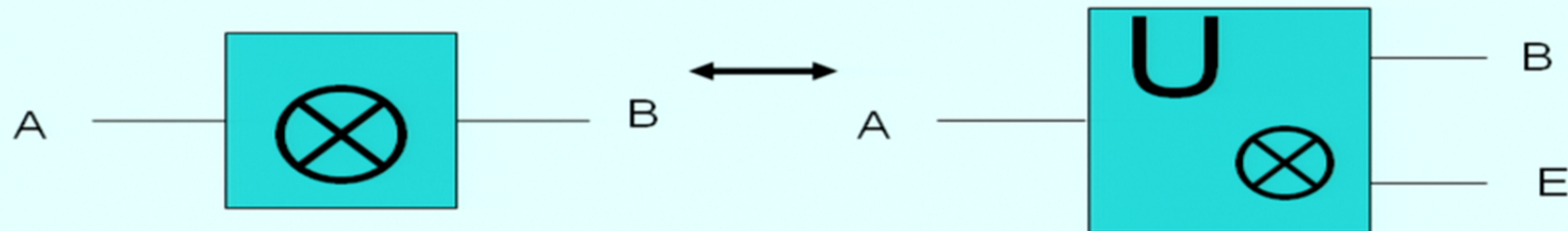
Send a classical message over a quantum message using a code

$$m \rightarrow \rho_m$$

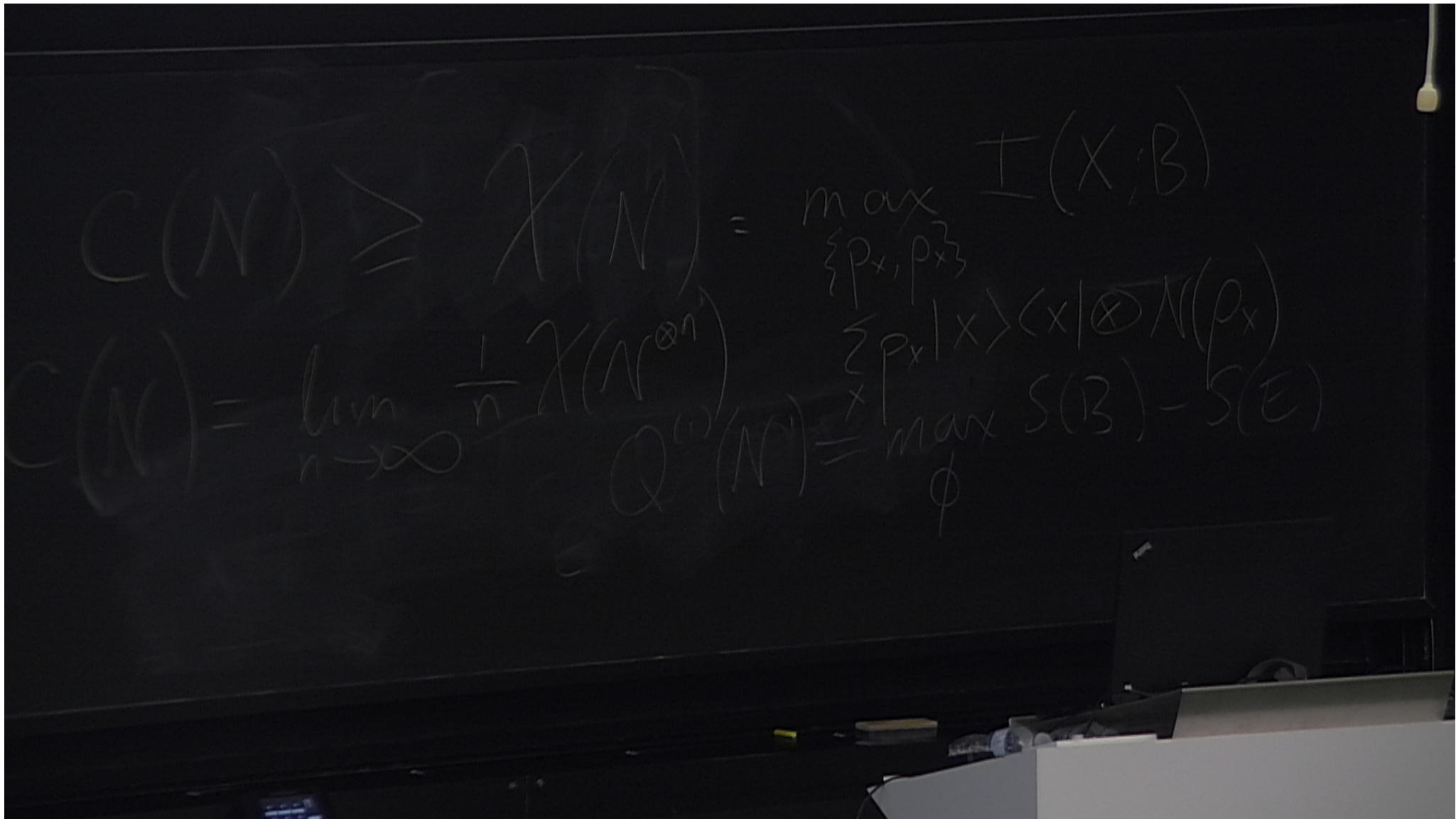
such that all  $\rho_m$  can be distinguished at the channel output.

$C(\text{channel})$  is the capacity

# Private Classical Capacity



- Quantum channel looks like a broadcast channel---one sender, two receivers.
- Best rate for classical messages from A to B while E learns nothing = private capacity. Call it  $P(\mathcal{N})$ .
- Related to quantum key distribution---the fact that by analysing the map from A to B we can infer the map from A to E allows unconditional security that is impossible classically.



$$C(N) \geq X(N)$$

$$X(N) = \max_{\{p_x, p_x\}} I(X; B)$$

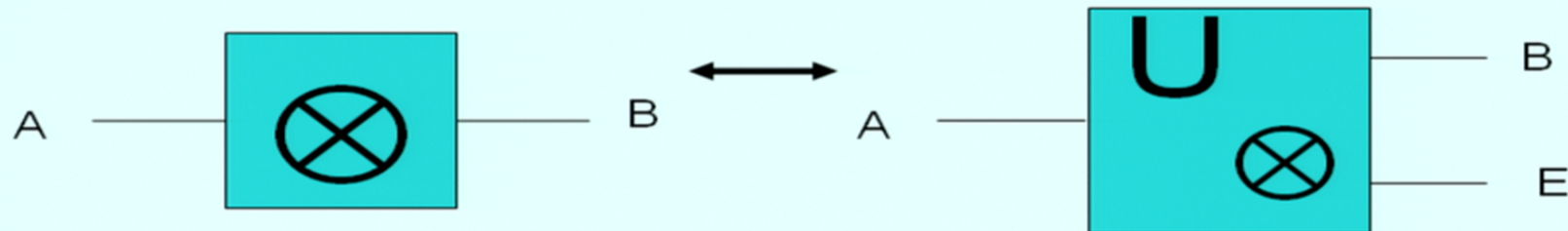
$$I(X; B) = \sum p_x |x\rangle \langle x| \otimes \Lambda(\rho_x)$$

$$C(N) = \lim_{n \rightarrow \infty} \frac{1}{n} X(N^{\otimes n})$$

$$Q(N) = \max_{\phi} S(B) - S(E)$$



# Private Classical Capacity



- Let  $P^1(\mathcal{N}) = \max_{p_v, \phi_v} I(V;B) - I(V;E)$ , with mutual informations evaluated on  $\sum_v p_v |v\rangle\langle v| \otimes U\phi_v U^\dagger$
- Random coding and privacy amplification shows  $P(\mathcal{N}) \geq P^1(\mathcal{N})$  and, in fact we can get

$$P(\mathcal{N}) = \lim_{n \rightarrow \infty} (1/n) P^1(\mathcal{N} \otimes \dots \otimes \mathcal{N})$$

See Devetak IEEE IT 03

n uses

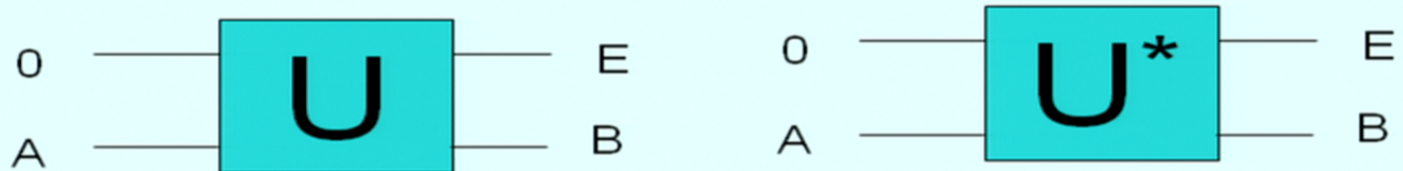
# Outline

- ~~Quantum capacity of quantum channel~~
- ~~Quantum coding theorem~~
- ~~Zero Quantum capacity channels and Superactivation (quantum synergy!)~~
- ~~Classical and private capacities~~
- Additivity in general
- Gaussian quantum channels
- Open questions

# Additivity: definition and motivation

- A function on channels is called additive if  $f(\mathcal{N} \otimes \mathcal{M}) = f(\mathcal{N}) + f(\mathcal{M})$
- Recall that  $Q(\mathcal{N}) = \lim_{n \rightarrow \infty} (1/n) Q^1(\mathcal{N}^{\otimes n})$ . If we could show that  $Q^1$  was additive, we'd have  $Q(\mathcal{N}) = Q^1(\mathcal{N})$ .
- Similarly,  $C(\mathcal{N}) = \lim_{n \rightarrow \infty} (1/n) \chi(\mathcal{N}^{\otimes n})$  and  $P(\mathcal{N}) = \lim_{n \rightarrow \infty} (1/n) P^1(\mathcal{N}^{\otimes n})$ , so if  $\chi$  and  $P^1$  were additive, we'd have single-letter capacities for classical and private communication.

# Nonadditivity of $\chi$



Choose  $U$  randomly and you get

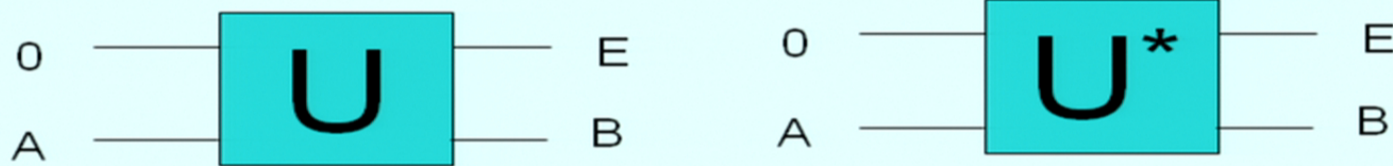
$$\chi(\mathcal{N}_U \otimes \mathcal{N}_{U^*}) > \chi(\mathcal{N}_U) + \chi(\mathcal{N}_{U^*})$$

Hastings, Nat. Phys. '09

# Additivity: definition and motivation

- A function on channels is called additive if  $f(\mathcal{N} \otimes \mathcal{M}) = f(\mathcal{N}) + f(\mathcal{M})$
- Recall that  $Q(\mathcal{N}) = \lim_{n \rightarrow \infty} (1/n) Q^1(\mathcal{N}^{\otimes n})$ . If we could show that  $Q^1$  was additive, we'd have  $Q(\mathcal{N}) = Q^1(\mathcal{N})$ .
- Similarly,  $C(\mathcal{N}) = \lim_{n \rightarrow \infty} (1/n) \chi(\mathcal{N}^{\otimes n})$  and  $P(\mathcal{N}) = \lim_{n \rightarrow \infty} (1/n) P^1(\mathcal{N}^{\otimes n})$ , so if  $\chi$  and  $P^1$  were additive, we'd have single-letter capacities for classical and private communication.

# Nonadditivity of $\chi$



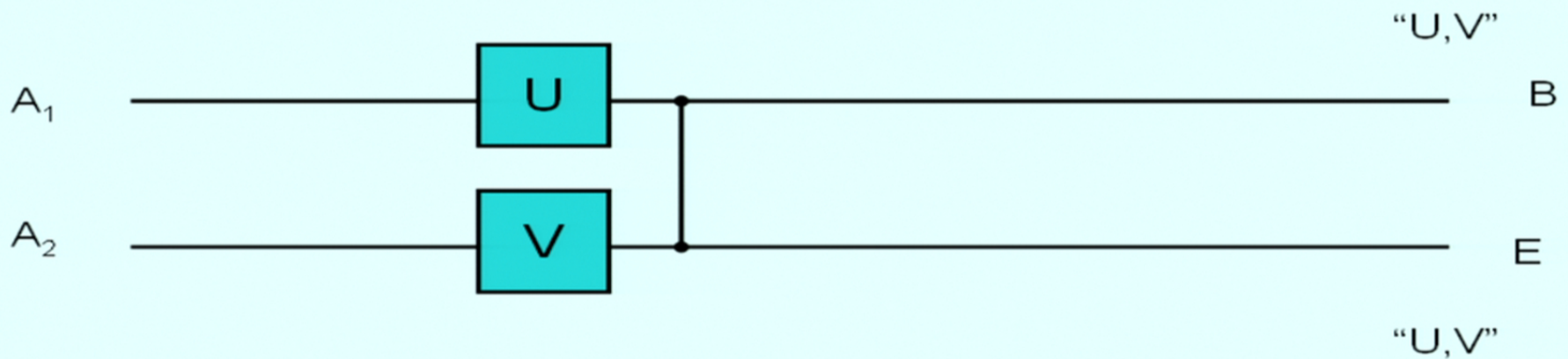
Choose  $U$  randomly and you get

$$\chi(\mathcal{N}_U \otimes \mathcal{N}_{U^*}) > \chi(\mathcal{N}_U) + \chi(\mathcal{N}_{U^*})$$

Hastings, Nat. Phys. '09

# Nonadditivity of Privacy

$$\mathcal{R}_d = E(\mathcal{R}^{U,V}_d \otimes |UV\rangle\langle UV|)$$



This channel has very little classical capacity, but used together with a 50% erasure channel, it can generate lots of private capacity

Li-Winter-Zuo-Guo '09, Smith-Smolin '09

# Most things aren't additive

- $Q^1$  is not additive for the very noisy depolarizing channel (Shor-Smolin '96)
- $P^1$  isn't additive for BB84 channel (Smith-Renes-Smolin, '08)
- $\chi$  is nonadditive for high-dimensional random channel (Hastings '09)
- $Q^1$  and  $P^1$  can both be extremely nonadditive (Smith-Smolin 08, 09)



# But sometimes they are

- $\chi$  is additive for depolarizing, erasure, and entanglement breaking channels.
- $Q^1$  and  $P^1$  are additive for degradable channels,  $Q^1$  is for PPT channels.

See King, Shor, Ruskai, Devetak-Shor, Horodecki, ...

# Additivity Questions

Information \ Quantity	Capacity	Correlation Measure
<b>Classical</b>	Classical Capacity ?	Holevo Information $\chi = \max I(X;B)$ <b>No</b> (Hastings '09)
<b>Private</b>	Private Capacity <b>No</b> (Li-Winter-Zou-Guo '09 Smith-Smolin-08/09)	Private Information $\max I(X;B) - I(X;E)$ <b>No</b> (Smith-Renes-Smolin '08)
<b>Quantum</b>	Quantum Capacity <b>No</b> (Smith-Yard '08)	Coherent Information $\max S(B) - S(E)$ <b>No</b> (Div-Shor-Smolin '98)
Entanglement assisted	Entanglement assisted classical capacity <b>Yes</b> (Bennett-Shor-Smolin-Thapliyal '99)	Quantum Mutual Information <b>Yes</b> (Bennett-Shor-Smolin-Thapliyal '99)

# Outline

- ~~Quantum capacity of quantum channel~~
- ~~Quantum coding theorem~~
- ~~Zero Quantum capacity channels and Superactivation (quantum synergy!)~~
- ~~Classical and private capacities~~
- ~~Additivity in general~~
- Gaussian quantum channels
- Open questions

# Gaussian Quantum Channels

- Classical Additive White Gaussian Noise:

$$X \rightarrow aX + N$$

- Quantum Generalization:

$$\gamma \rightarrow A\gamma A^T + N$$

- $\gamma$  contains all information about the EM field
- Generated by quadratic interactions between input signal and vacuum environment

# Additive White Gaussian Noise

Input  $X$  is a real variable (eg, component of EM field)

$$X \rightarrow X + bN = Y$$

$N$  is normally distributed with variance 1, and mean zero, so

$$Pr(y|x) = \frac{1}{\sqrt{2\pi}b} e^{-(x-y)^2/2b^2}$$

Capacity of this channel is infinite, but makes sense if we introduce a power constraint:  $E[X^2] \leq P$ . Then the capacity becomes

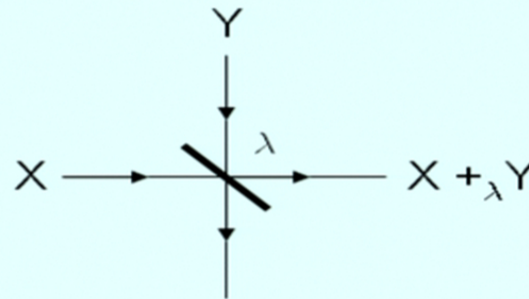
$$C = \frac{1}{2} \log(1 + SNR)$$

Where  $SNR = P/b^2$  is the ratio of max signal power to noise power

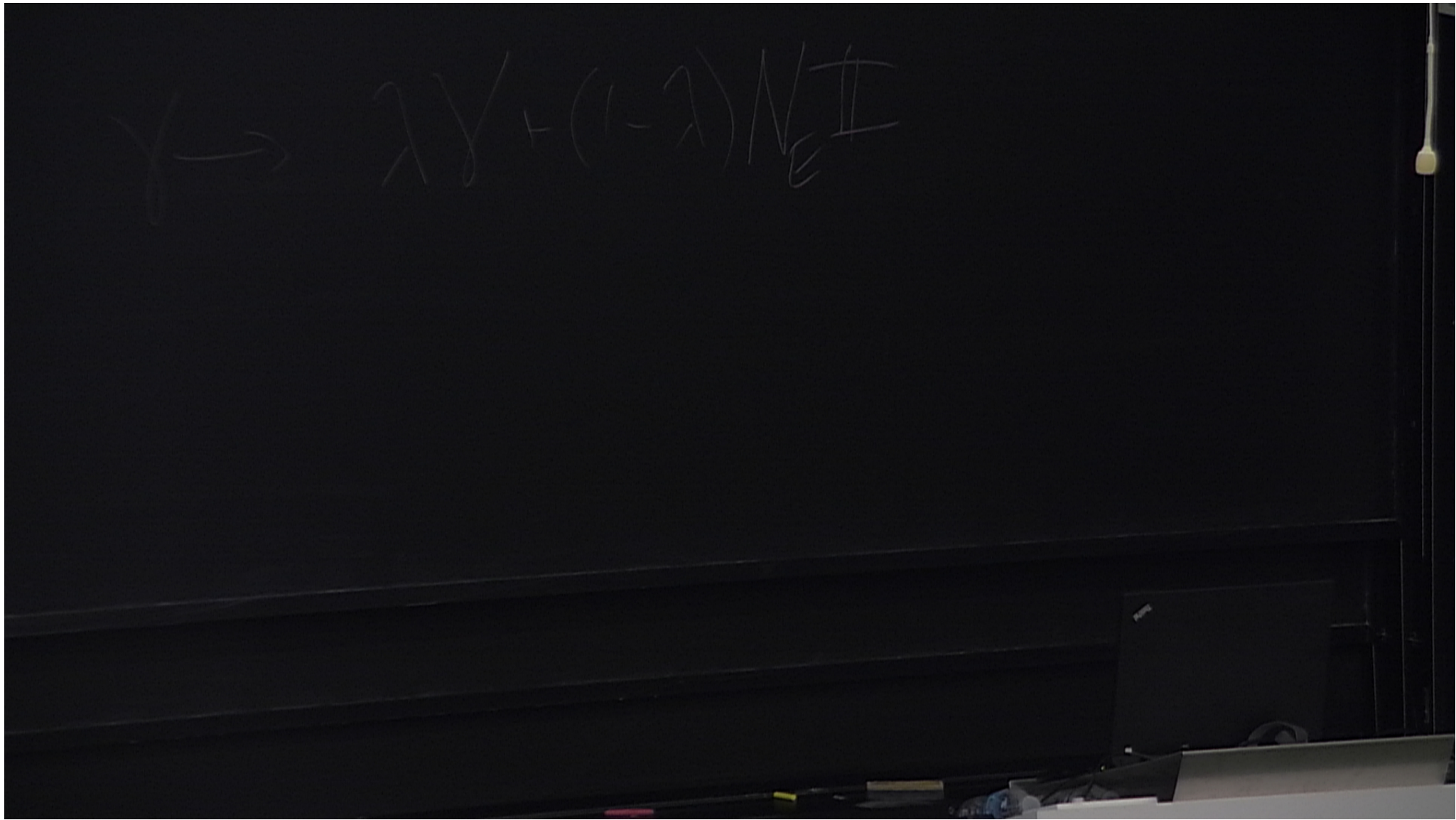
# Classical Capacity of gaussian thermal noise channel

- Evolution:  $\gamma \rightarrow (1 - \lambda)\gamma + \lambda N_E I$
- Models combination of attenuation and amplification present in optical fiber
- LB:  $C_N \geq g(\lambda N + (1 - \lambda)N_E) - g((1 - \lambda)N_E)$
- Good upper bds from quantum entropy power inequality:

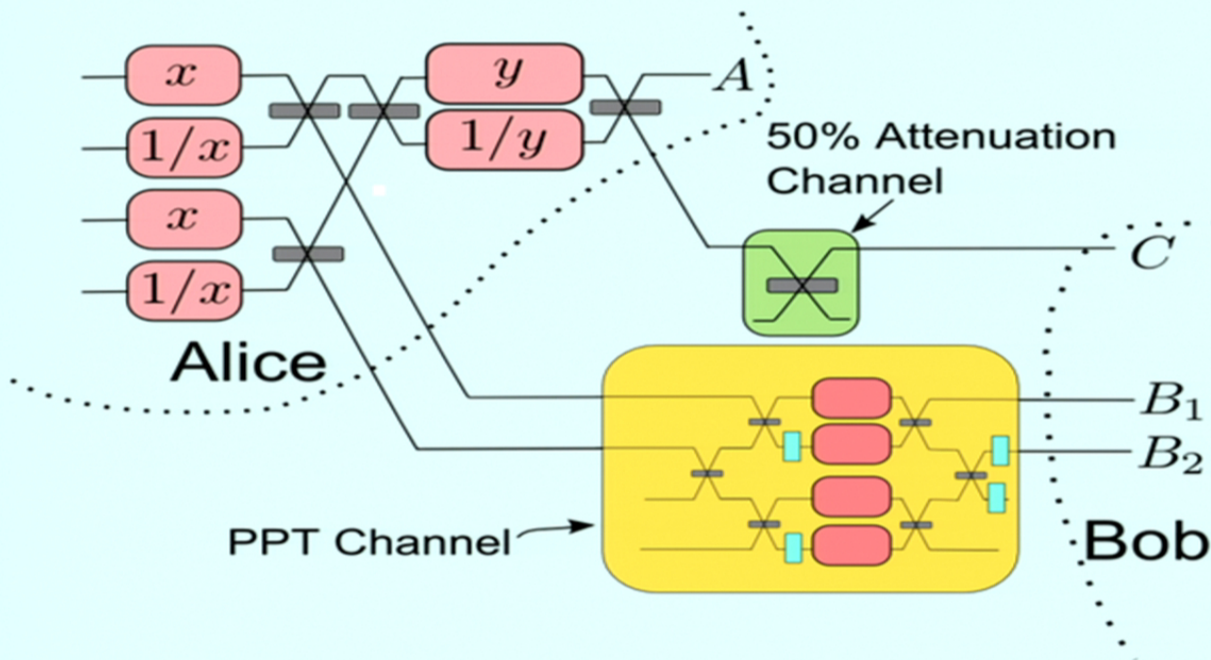
$$H(X +_{\lambda} Y) \geq \lambda H(X) + (1 - \lambda)H(Y)$$



Koenig-Smith '12



# Gaussian Superactivation



- Combining the 50% attenuation channel with a PPT channel lets us make a state that we use to generate coherent information.
- The strategy on the left can get around 0.06 bits of coherent information.

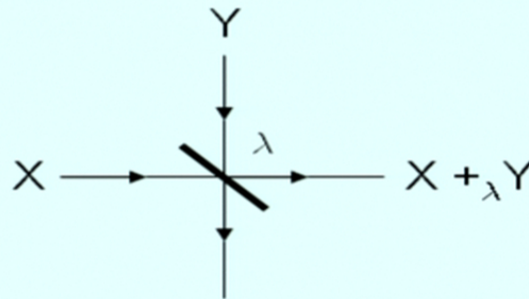
Smith-Smolín-Yard Nat. Photon. '11 Squeezing required: Lercher-Giedke-Wolf '12



# Classical Capacity of gaussian thermal noise channel

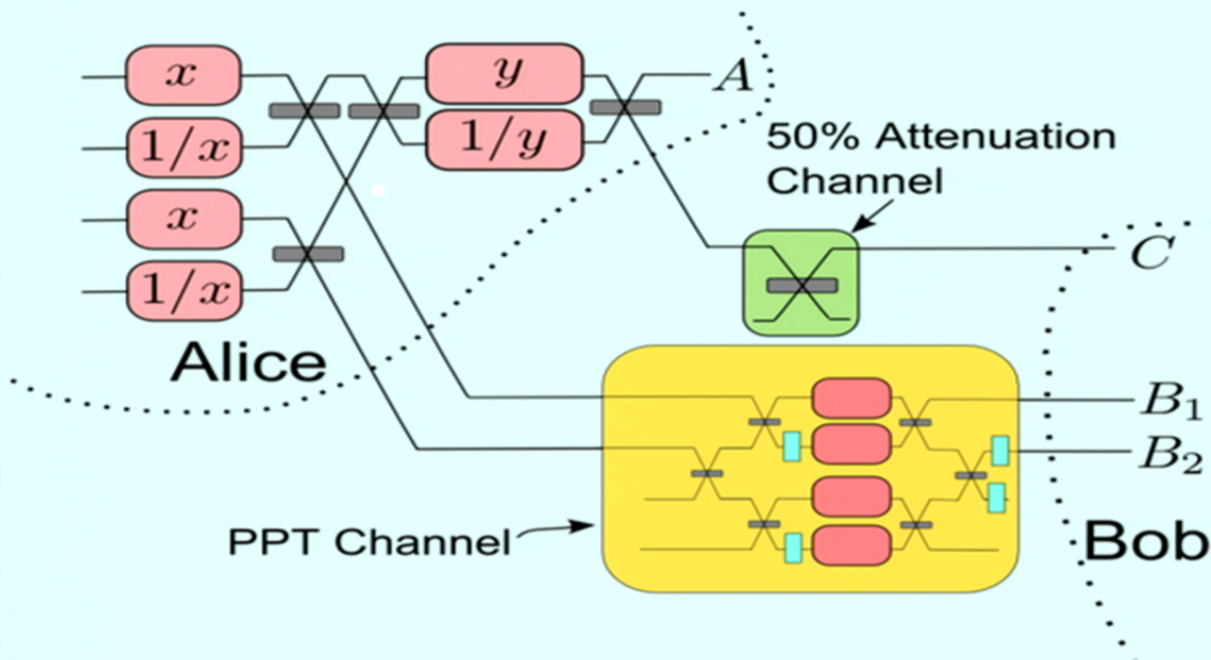
- Evolution:  $\gamma \rightarrow (1 - \lambda)\gamma + \lambda N_E I$
- Models combination of attenuation and amplification present in optical fiber
- LB:  $C_N \geq g(\lambda N + (1 - \lambda)N_E) - g((1 - \lambda)N_E)$
- Good upper bds from quantum entropy power inequality:

$$H(X +_{\lambda} Y) \geq \lambda H(X) + (1 - \lambda)H(Y)$$



Koenig-Smith '12

# Gaussian Superactivation



- Combining the 50% attenuation channel with a PPT channel lets us make a state that we use to generate coherent information.
- The strategy on the left can get around 0.06 bits of coherent information.

Smith-Smolín-Yard Nat. Photon. '11 Squeezing required: Lercher-Giedke-Wolf '12

# Summary

- The capacities of a quantum channel characterize its capability for transmitting information: classical, private classical, quantum
- There are random coding theorems for each of these cases, whose rates are characterized by some entropic functions.
- In general these functions are superadditive, so we don't get single-letter formulas. This is **good**, since it means we get higher rates!
- In special cases (degradable, entanglement breaking, PPT), we can show additivity.
- There are a million simple questions that nobody knows how to answer!

# What Next?

- We have very few (computable) upper bounds on the capacities of a quantum channel. Sometimes calculating the information measures is (complexity theoretically) hard.
- Important special case: bosonic gaussian channels (quantum version of AWGN). Unsolved (even for single mode), with the exception of pure loss. Tight bounds for thermal noise, but can we find nonadditivity here?
- There are ad hoc techniques for showing additivity of  $\chi$  but no general guide for when to expect it.
- Is there a non-degradable, non-PPT channel for which we can find the quantum capacity? When is  $Q = 0$ ?  $P=0$ ? What do the zero-capacity sets look like?
- Is there a general mapping between quantum channels and classical broadcast channels that lets you get the capacity of one from that of the other?

# Some things I haven't mentioned

- Multiple access channels, broadcast channels, etc.
- How do we actually achieve these rates?
- Coding theory, fault-tolerance, etc.
- Pure-state source coding (aka “data compression”) is actually solvable.
- Two-way capacities and relationship to entanglement and LOCC.
- PPT criterion and NPT bound entanglement?
- $P \neq Q$
- Connections between Quantum Key Distribution and private capacities (tomography, non-iid, etc.).
- Beyond i.i.d. (symmetrization and de Finetti arguments)
- Identification capacity, environment assisted capacity, capacity of unitary interactions, symmetric side channels, commitment capacity, reverse Shannon theorem, embezzling states, entanglement measures, zero-error...

THANK YOU