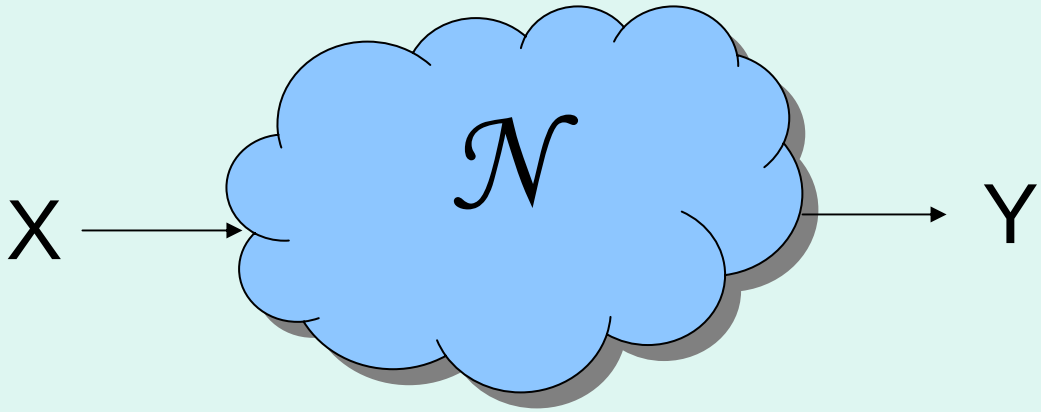
Sending Quantum Information with Zero Capacity Channels

Graeme Smith
IBM Research

KITP Quantum Information Science Program
November 5, 2009

Joint work with Jon and John

Noisy Channel Capacity



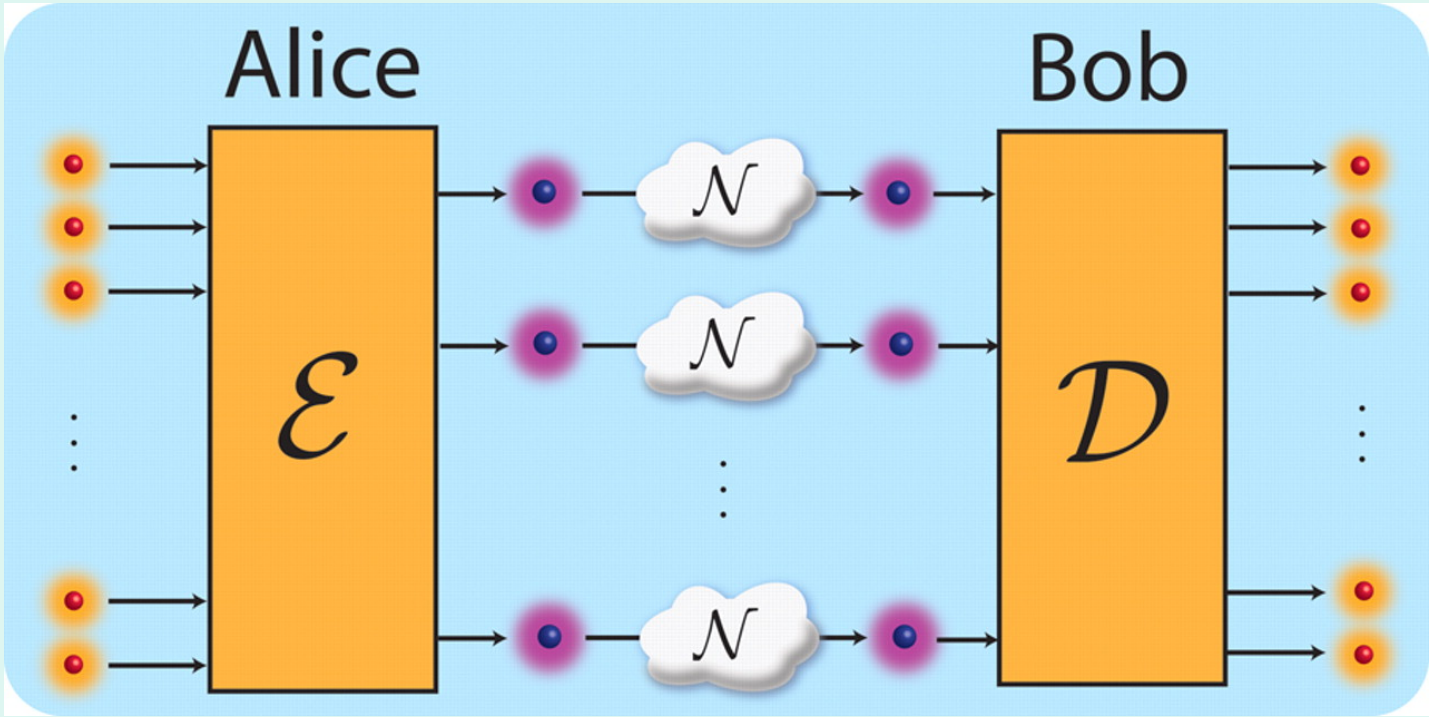
p(y|x)

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

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

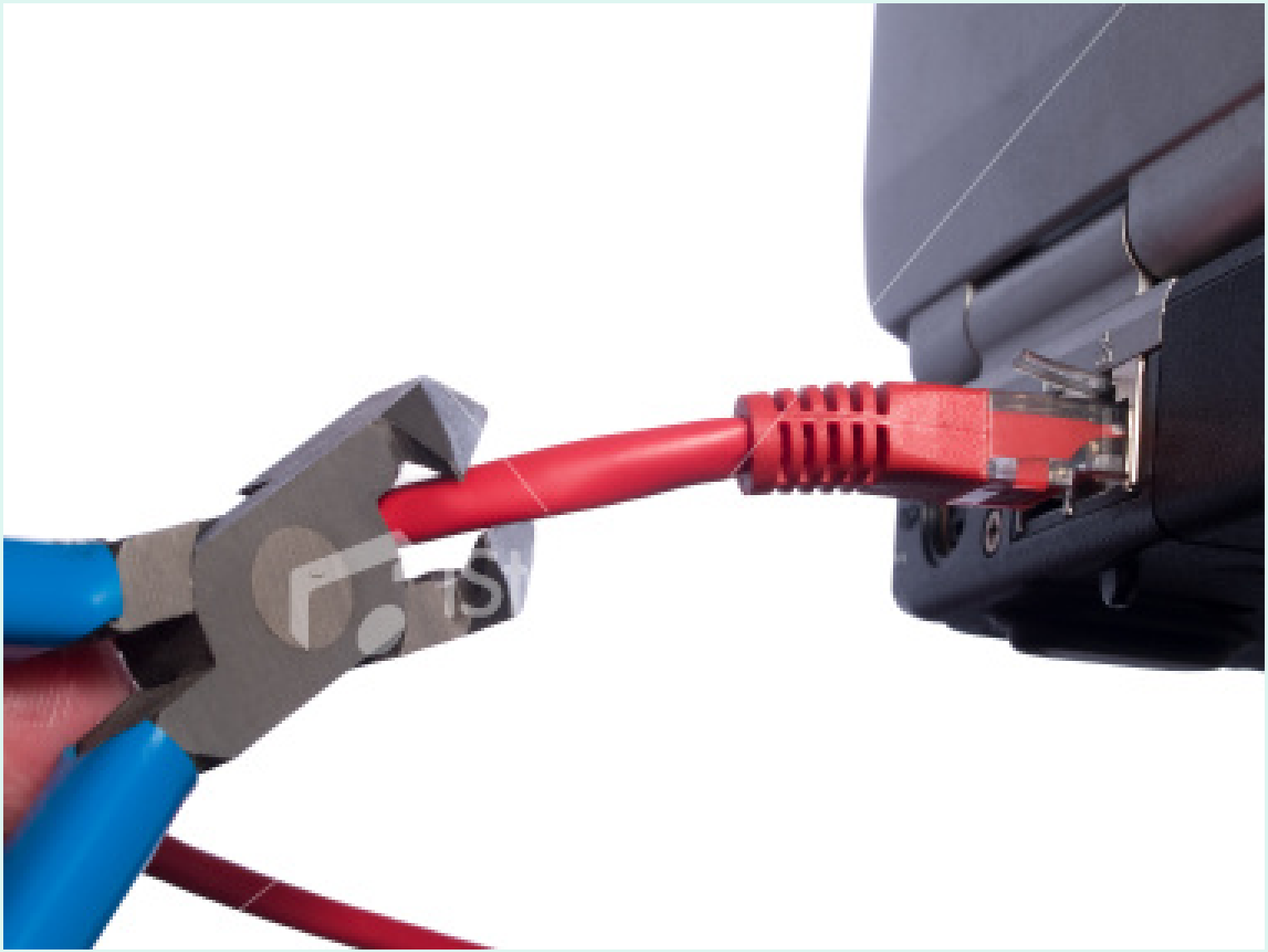
I(X;Y) is the mutual information

Quantum Communication

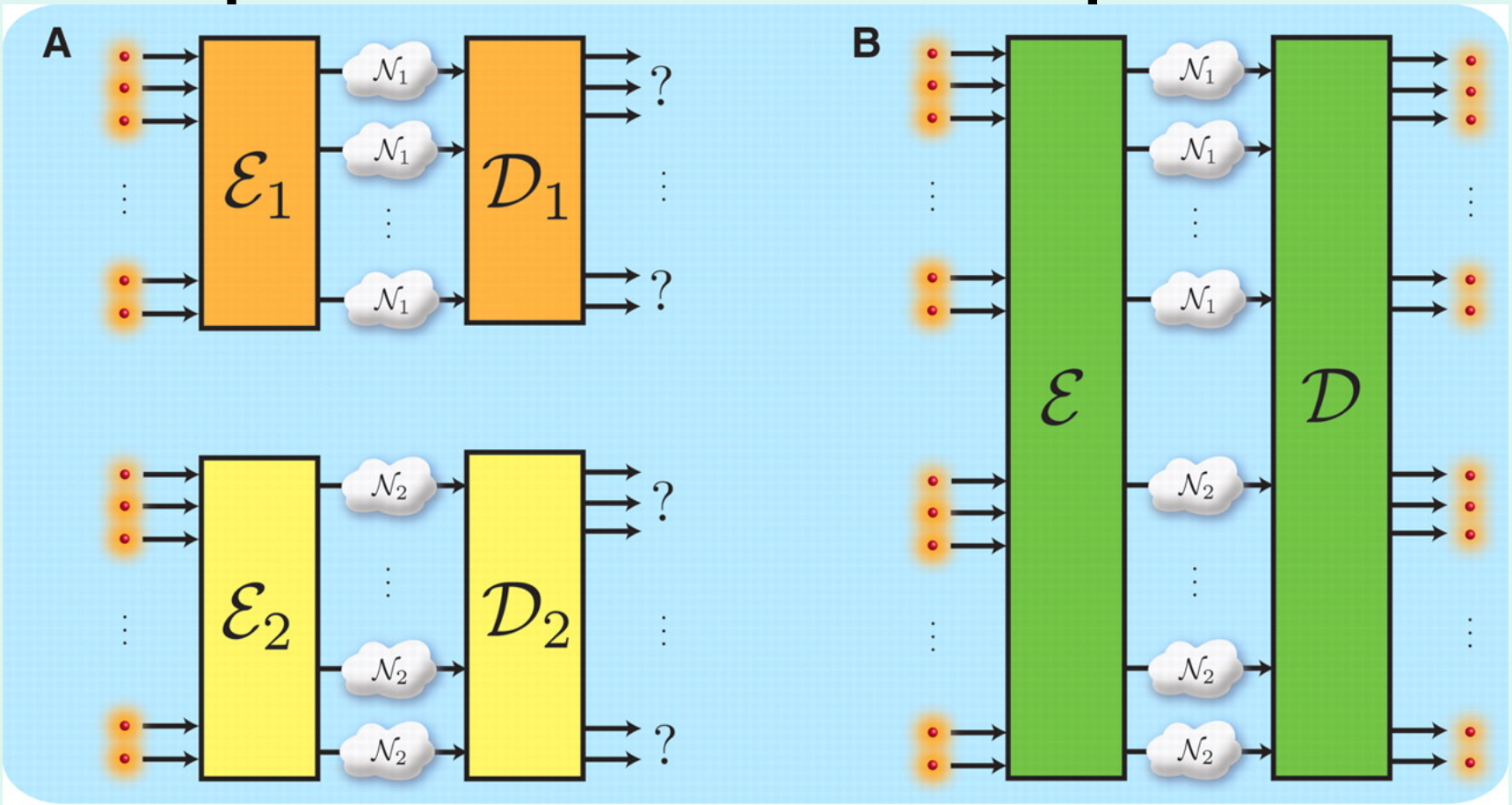


$$Q(\mathcal{N}) = \max\left(\frac{\#\text{ quantum bits sent}}{\#\text{ channel uses}}\right)$$

Quantum Capacity: the rate, in qubits per channel use, at which A can send high-fidelity quantum information to B.



Superactivation of Capacities



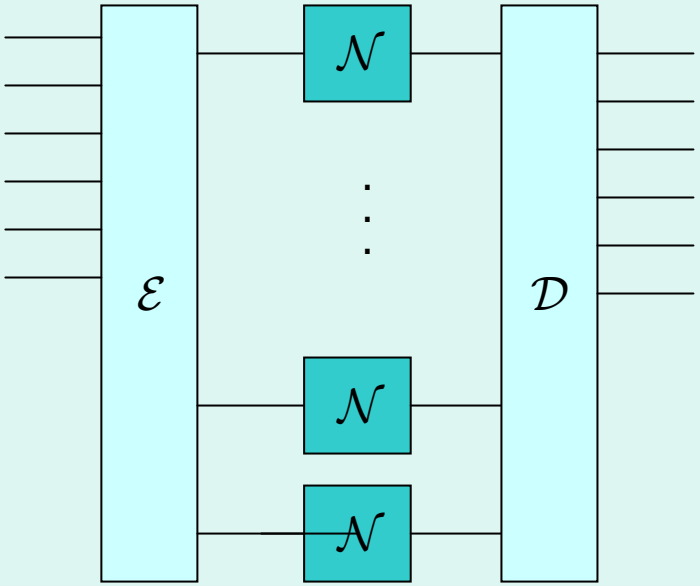
There are $\mathcal{N}_1$, $\mathcal{N}_2$ with zero quantum capacity but $Q(\mathcal{N}_1 \otimes \mathcal{N}_2) > 0$.

G. Smith and J. Yard, Science, 321, 1812-1815 (2008)

Outline

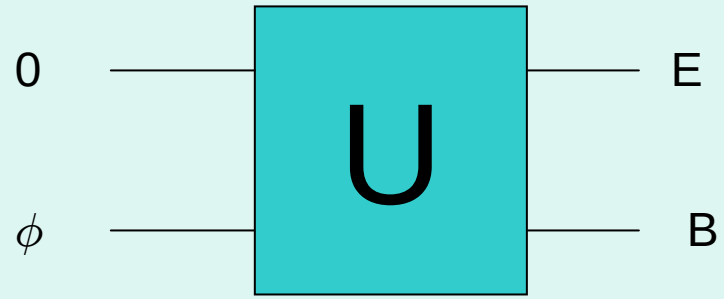
- Quantum and Private Capacities
- Channels with Zero Quantum Capacity
- Superactivation of Quantum Capacity
- Superadditivity of Private Capacity
- Applications

Quantum Capacity



- Want to encode qubits so they can be recovered after experiencing noise.
- Quantum capacity is the maximum rate, in qubits per channel use, at which this can be done.
- We'd like a formula for Q($\mathcal{N}$) in terms of $\mathcal{N}$.

Quantum Capacity



- Coherent Information:

  $Q^1(\mathcal{N}) = \max S(B)-S(E)$ (cf Shannon formula)
- $Q(\mathcal{N}) \geq Q^1(\mathcal{N})$ (Lloyd-Shor-Devetak)
- $Q(\mathcal{N}) = \lim_{n \to \infty}(1/n)\, Q^1(\mathcal{N} \otimes \ldots \otimes \mathcal{N})$
- $Q(\mathcal{N}) \neq Q^1(\mathcal{N})$ (DiVincenzo-Shor-Smolin ‘98)

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

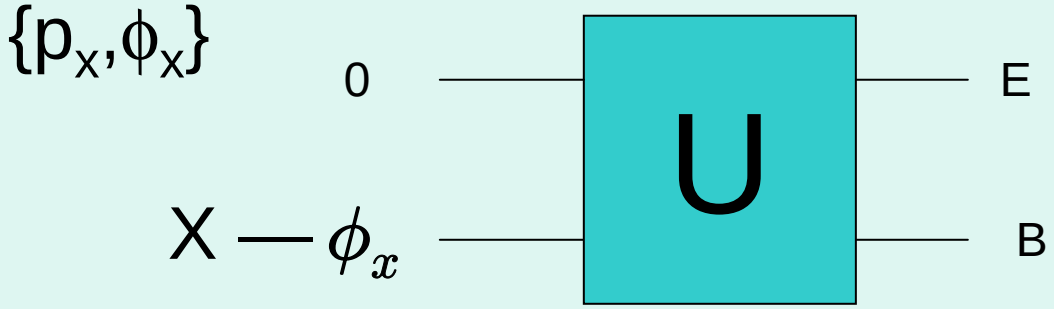
S(B) is how much information B has

S(E) is how much information E has

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

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

Private Capacity

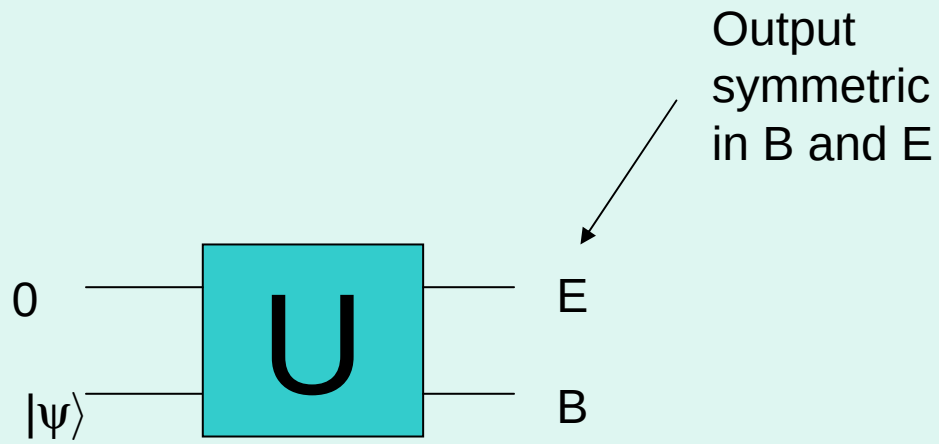


- Mutual Information: I(X;B) = S(X)+S(B)- S(XB)
- Private Information: $P^1(\mathcal{N})$ = max I(X;B)-I(X;E)
- $P(\mathcal{N}) \geq P^1(\mathcal{N})$ (Devetak)
- $P(\mathcal{N}) = \lim_{n \to \infty}(1/n)\, P^1(\mathcal{N} \otimes \ldots \otimes \mathcal{N})$
- $P(\mathcal{N}) \neq P^1(\mathcal{N})$ (Smith, Renes, Smolin ‘08)
- $P(\mathcal{N}) \geq Q(\mathcal{N})$

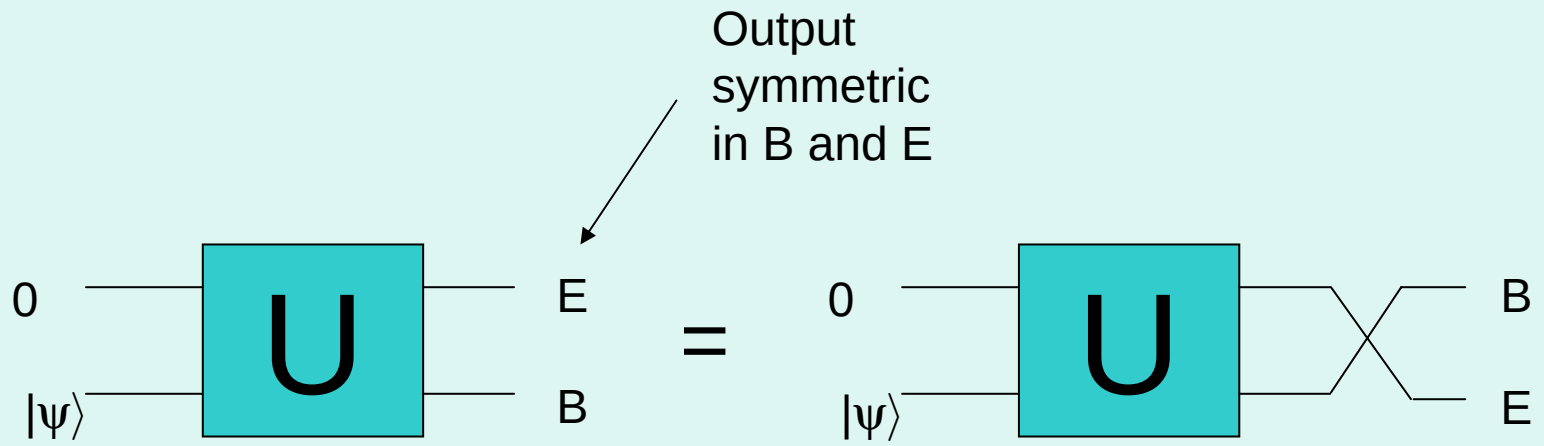
Outline

- ~~Quantum and Private Capacities~~
- Channels with Zero Quantum Capacity
- Superactivation of Quantum Capacity
- Superadditivity of Private Capacity
- Applications

Zero Quantum Capacity Channels: Symmetric Channels



Zero Quantum Capacity Channels: Symmetric Channels



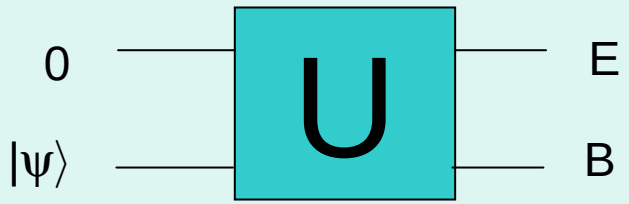
Example: 50% erasure channel:

$$|\psi\rangle \rightarrow \frac{1}{\sqrt{2}}(|\psi\rangle_B|e\rangle_E + |e\rangle_B|\psi\rangle_E)$$

Gives $\mathcal{N}(\rho) = \frac{1}{2}(\rho + |e\rangle\langle e|)$

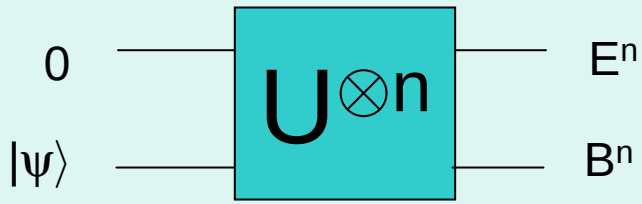
Zero Quantum Capacity Channels: Symmetric Channels

Suppose a symmetric channel had Q >0



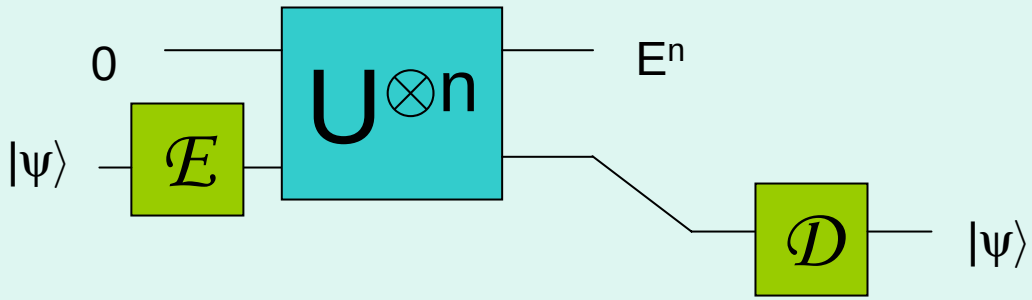
Zero Quantum Capacity Channels: Symmetric Channels

Suppose a symmetric channel had Q >0



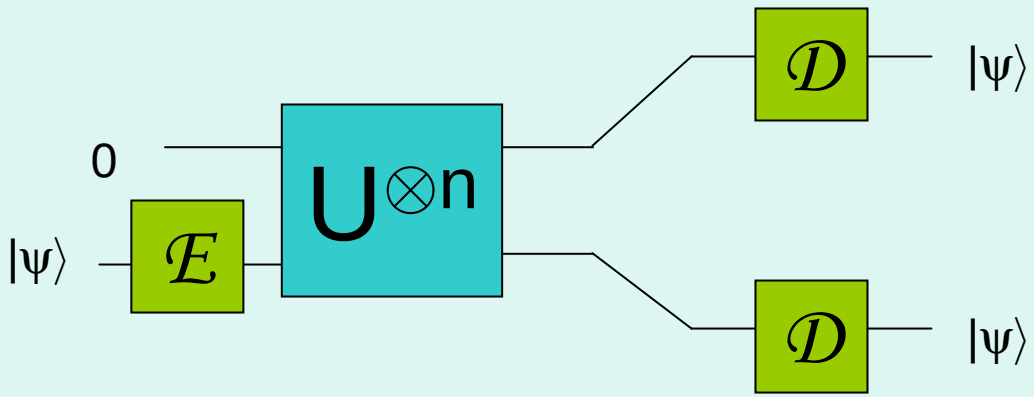
Zero Quantum Capacity Channels: Symmetric Channels

Suppose a symmetric channel had Q >0



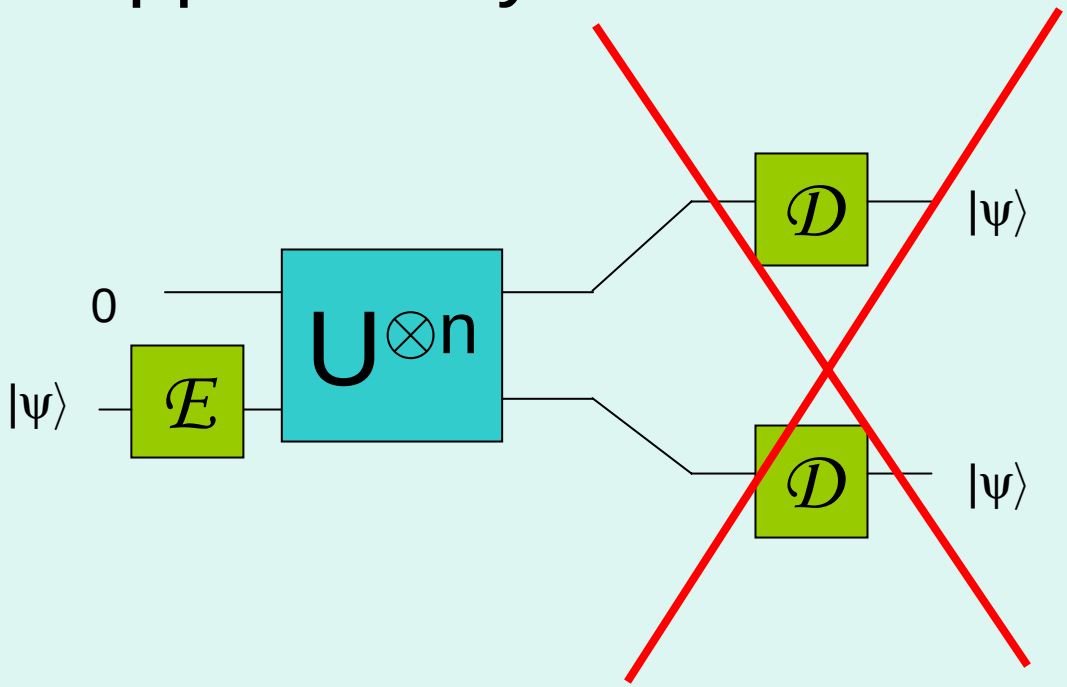
Zero Quantum Capacity Channels: Symmetric Channels

Suppose a symmetric channel had Q >0



Zero Quantum Capacity Channels: Symmetric Channels

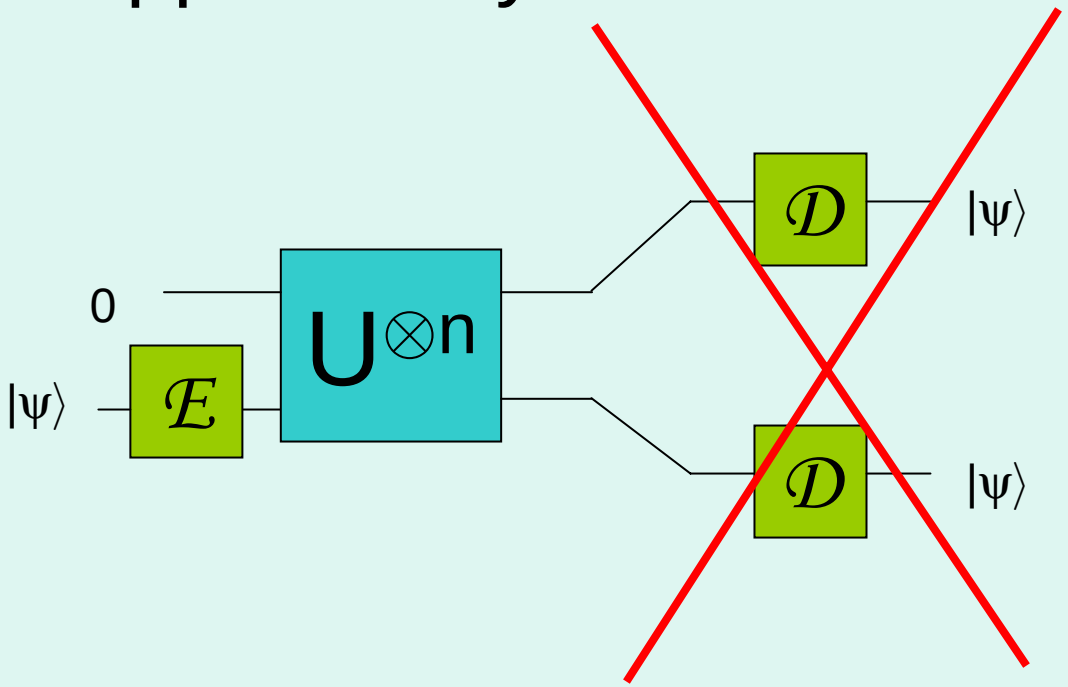
Suppose a symmetric channel had Q >0



IMPOSSIBLE!

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:
  $(|i\rangle\langle j|_A \otimes |k\rangle\langle l|_B)^\Gamma = |i\rangle\langle j|_A \otimes |l\rangle\langle k|_B$
- If $\rho_{AB}{}^\Gamma$ is not positive, then the state is entangled
- If $\rho_{AB}{}^\Gamma \geq 0$, 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:

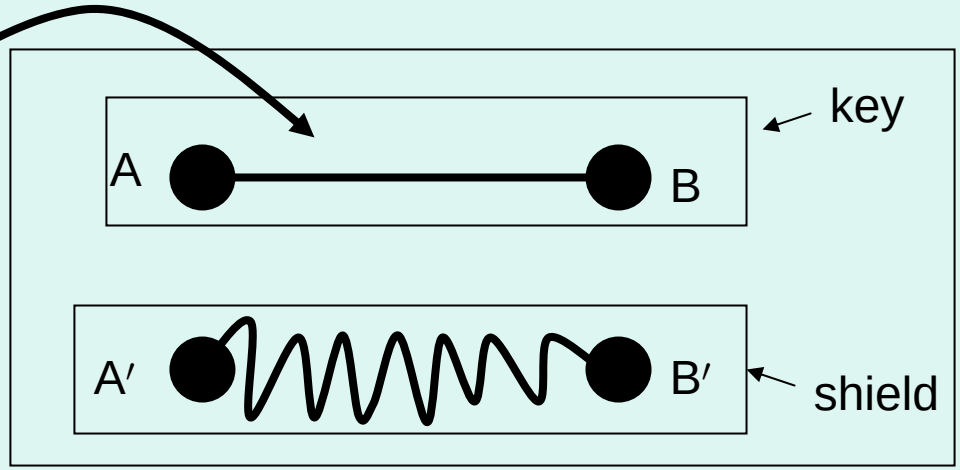
  $\rho_{AB} = I \otimes \mathcal{N}(\phi_{AB})$ is PPT
- Implies $Q(\mathcal{N}) = 0$, but can have $P(\mathcal{N}) > 0$

Conditions for Private Capacity

Channel with private classical capacity lets you make a “private state”.

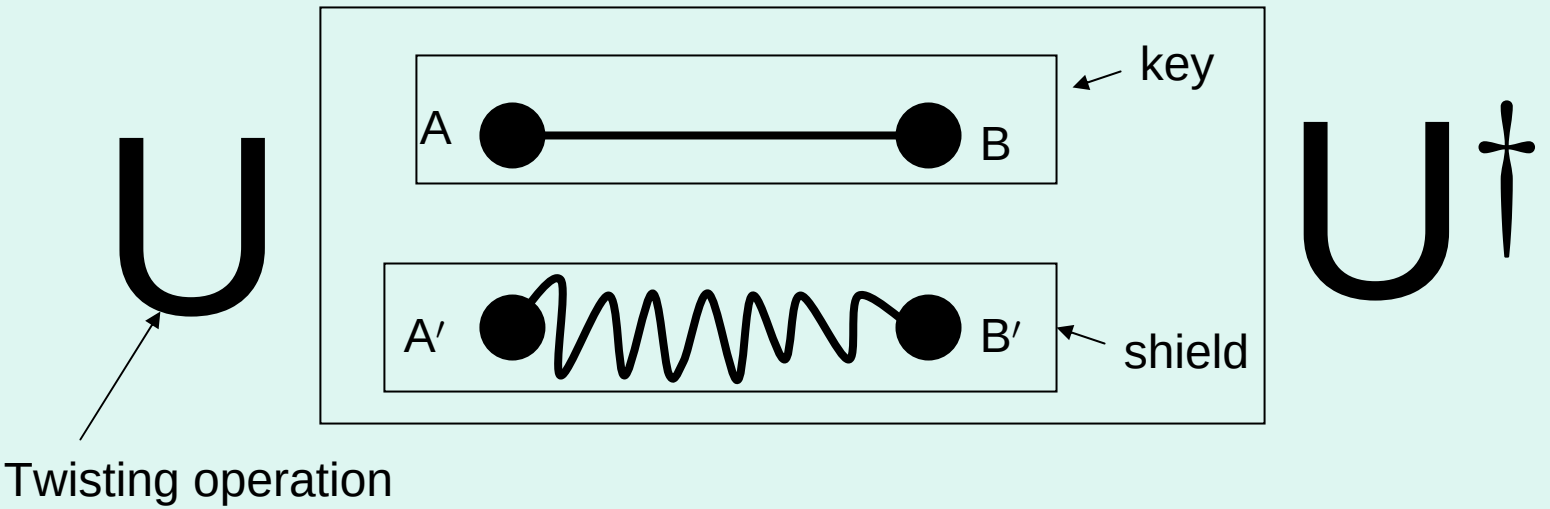
Straight line indicates Maximally Entangled state

$\frac{1}{\sqrt{2}}(|0\rangle|0\rangle + |1\rangle|1\rangle)$



Conditions for Private Capacity

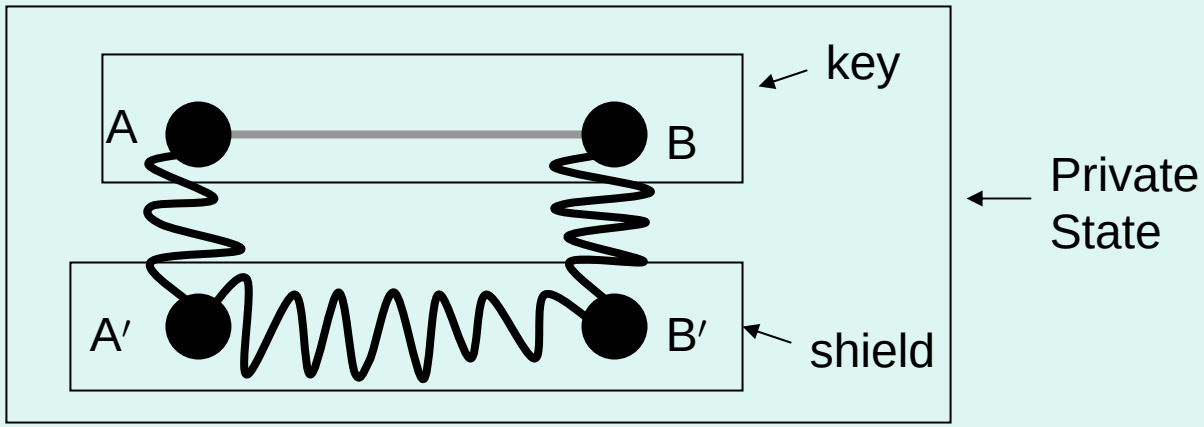
Channel with private classical capacity lets you make a “private state”.



$$U = \sum_{i,j} |i\rangle|j\rangle\langle i|\langle j|_{AB} \otimes U_{ij}^{A'B'}$$

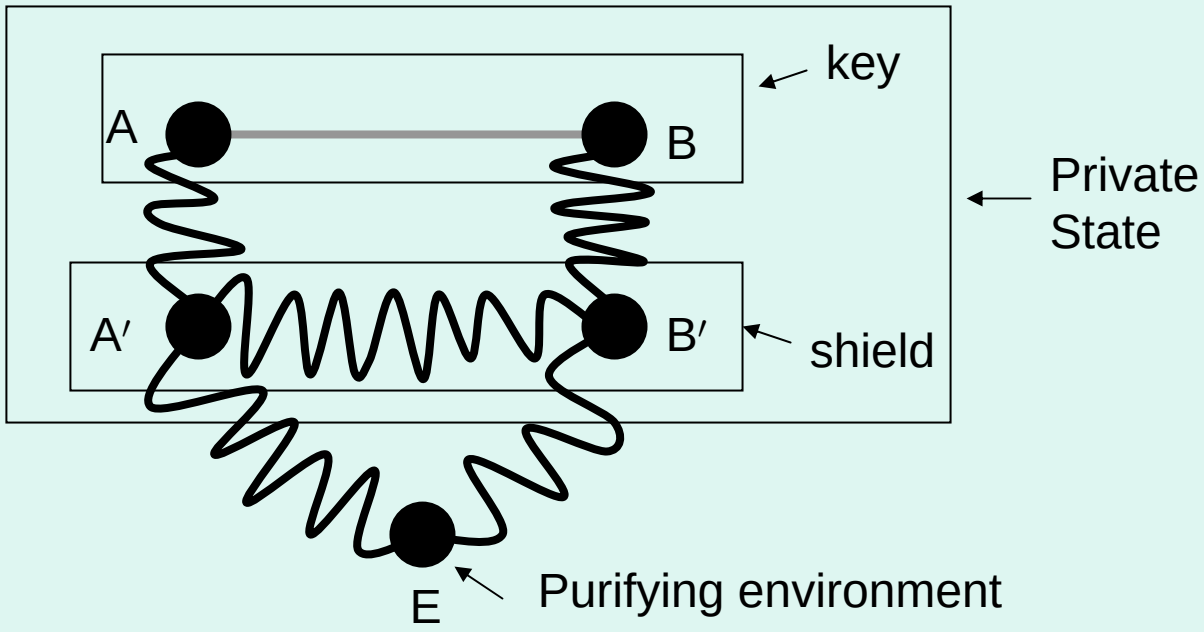
Conditions for Private Capacity

Channel with private classical capacity lets you make a “private state”.



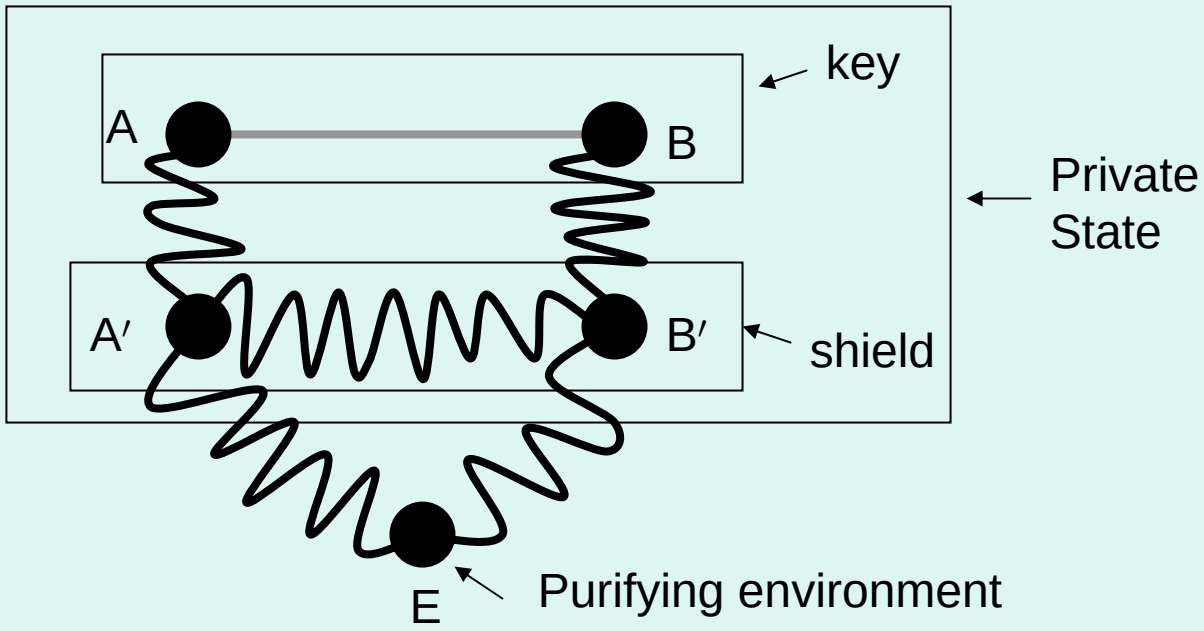
Conditions for Private Capacity

Channel with private classical capacity lets you make a “private state”.



Conditions for Private Capacity

Channel with private classical capacity lets you make a “private state”.



AB is conditionally independent of E:

Quantum Markov Chain: E—A’B’—AB

Zero Quantum Capacity Channels: PPT but Private

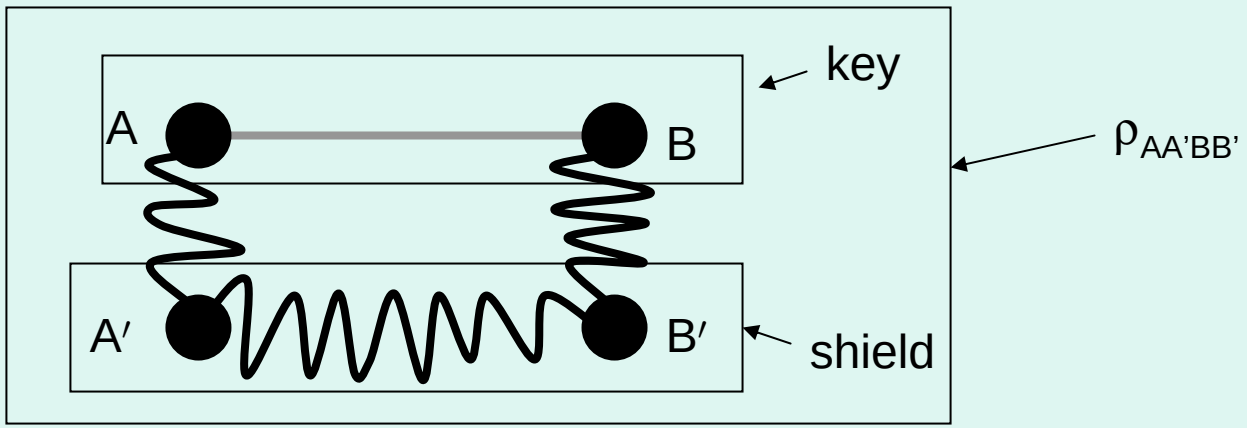
- Construction due to Oppenheim and several Horodeckis
- Let $|\phi_\pm\rangle = \frac{1}{\sqrt{2}}(|0\rangle|0\rangle \pm |1\rangle|1\rangle)$ and

$$\rho_{ABA'B'} = \frac{1}{2}\left(|\phi_+\rangle\langle\phi_+|_{AB} \otimes \tau_+^{A'B'} + |\phi_-\rangle\langle\phi_-|_{AB} \otimes \tau_-^{A'B'}\right)$$

- $\tau_\pm$ are "data-hiding states"--- separable, $\approx$ orthogonal but $\approx$ indistinguishable via LOCC
- $\rho_{ABA'B'}$ gives a full bit of secret key, but gives substantially less pure entanglement
- Proof: C'mon. To get at the EPRs, you'd have to distinguish the τ's, but you cant.

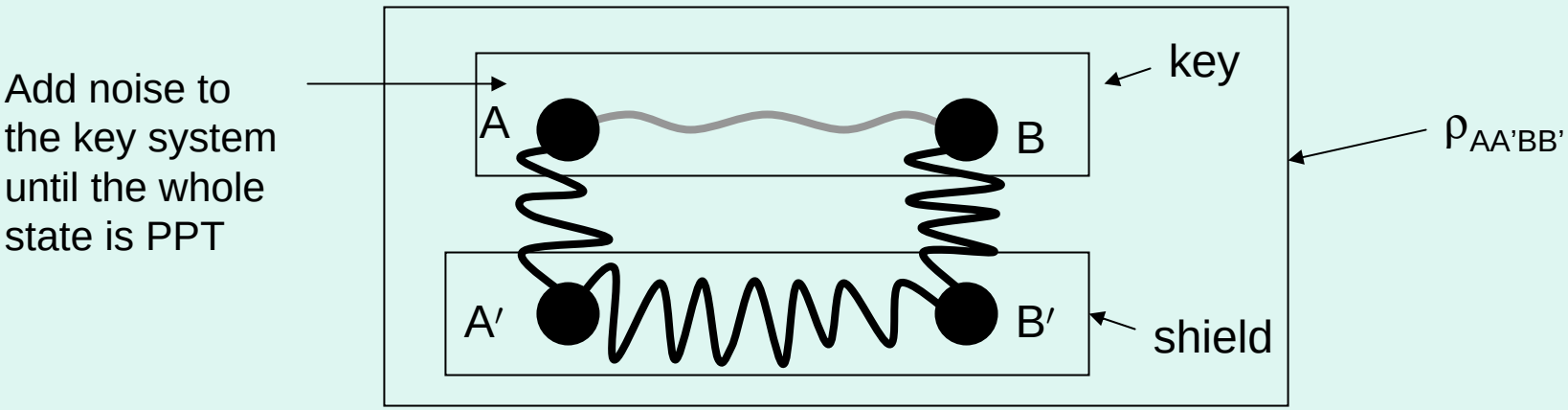
Zero Quantum Capacity Channels: PPT but Private

- Start with $\rho_{ABA'B'} = \frac{1}{2}\left(|\phi_+\rangle\langle\phi_+|_{AB} \otimes \tau_+^{A'B'} + |\phi_-\rangle\langle\phi_-|_{AB} \otimes \tau_-^{A'B'}\right)$



Zero Quantum Capacity Channels: PPT but Private

- Start with $\rho_{ABA'B'} = \frac{1}{2}\left(|\phi_+\rangle\langle\phi_+|_{AB} \otimes \tau_+^{A'B'} + |\phi_-\rangle\langle\phi_-|_{AB} \otimes \tau_-^{A'B'}\right)$



- Gives Q = 0 but P > 0

Outline

- ~~Quantum and Private Capacities~~
- ~~Channels with Zero Quantum Capacity~~
- Superactivation of Quantum Capacity
- Superadditivity of Private Capacity
- Applications

Superactivation of Quantum Capacity

Main Result

Theorem: Let $\mathcal{N}$ be any channel and $\mathcal{E}$ be a 50% erasure channel. Then

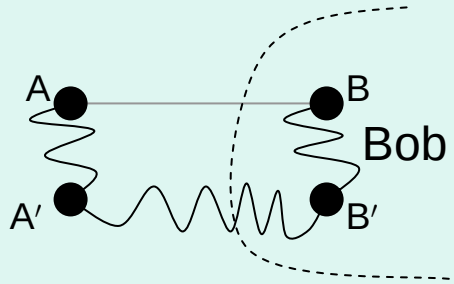
$$Q(\mathcal{N} \otimes \mathcal{E}) \geq (1/2)P(\mathcal{N}).$$

Corollary: There are $\mathcal{N}$ and $\mathcal{E}$ with $Q(\mathcal{N}) = Q(\mathcal{E}) = 0$ but $Q(\mathcal{N} \otimes \mathcal{E}) > 0$.

Reminder: $\mathcal{E}(\rho) = ½(\rho + |e\rangle\langle e|)$

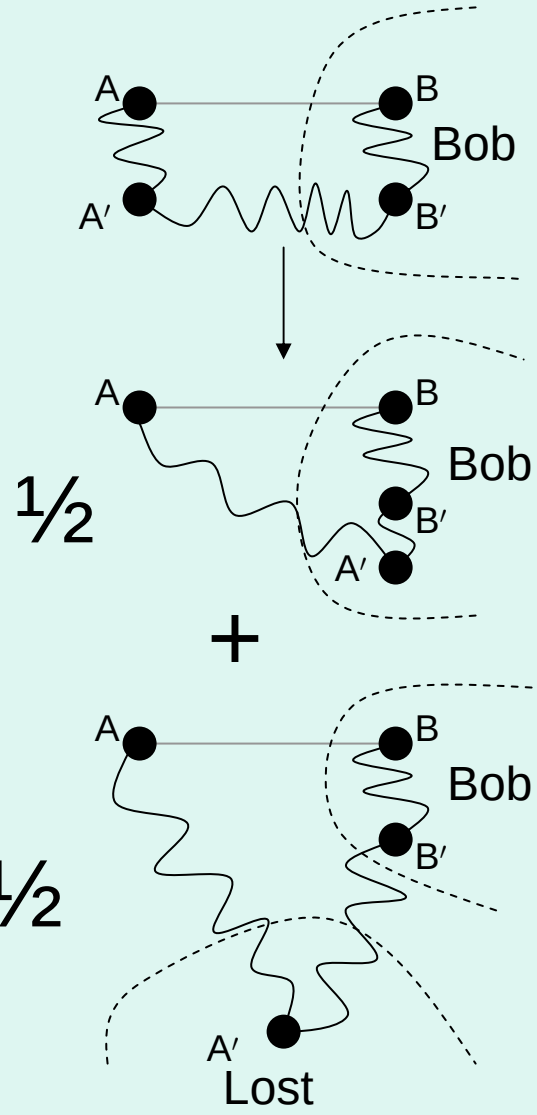
Superactivation of Quantum Capacity: Proof Ideas

- $\mathcal{N}$ has private capacity, so we can use it to make private states.
- Send the A' part of the shield system through the 50% erasure channel, $\mathcal{E}$.
- When the shield is transmitted (½ the time) they establish a maximally entangled state. Otherwise, the state is not too noisy.
- The resulting state has coherent information ½ P($\mathcal{N}$) + ½ 0 = ½ P($\mathcal{N}$), so the $\mathcal{N}$ and $\mathcal{E}$ can be used to transmit quantum information at this rate.



Superactivation of Quantum Capacity: Proof Ideas

- $\mathcal{N}$ has private capacity, so we can use it to make private states.
- Send the A' part of the shield system through the 50% erasure channel, $\mathcal{E}$.
- When the shield is transmitted (½ the time) they establish a maximally entangled state. Otherwise, the state is not too noisy.
- The resulting state has coherent information ½ P($\mathcal{N}$) + ½ 0 = ½ P($\mathcal{N}$), so the $\mathcal{N}$ and $\mathcal{E}$ can be used to transmit quantum information at this rate.



Interpretation

This superactivation effect is completely different from what happens in classical theory, and depends crucially on choosing inputs entangled between the channels. Somehow, each channel can transmit different sorts of quantum information---neither sort is sufficient on its own, but together they can be used for the usual noiseless variety.

What are the different kinds of information?

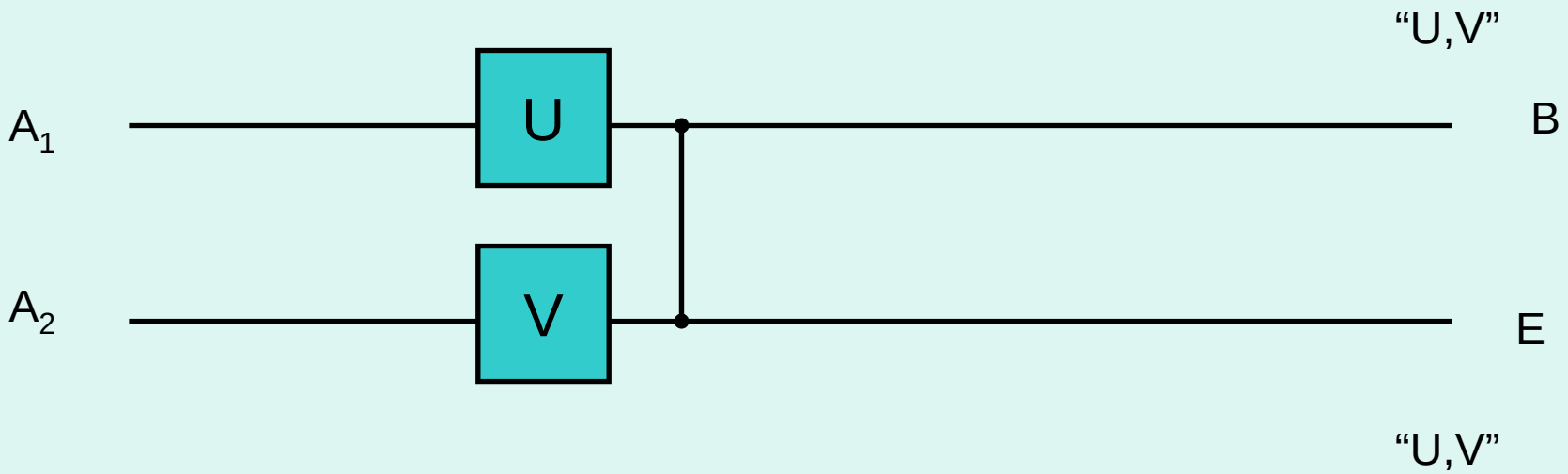
Is privacy important?

Outline

- ~~Quantum and Private Capacities~~
- ~~Channels with Zero Quantum Capacity~~
- ~~Superactivation of Quantum Capacity~~
- Superadditivity of Private Capacity
- Applications

Rocket Channels

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



This channel has classical capacity ≤ 2

Proof: C'mon!

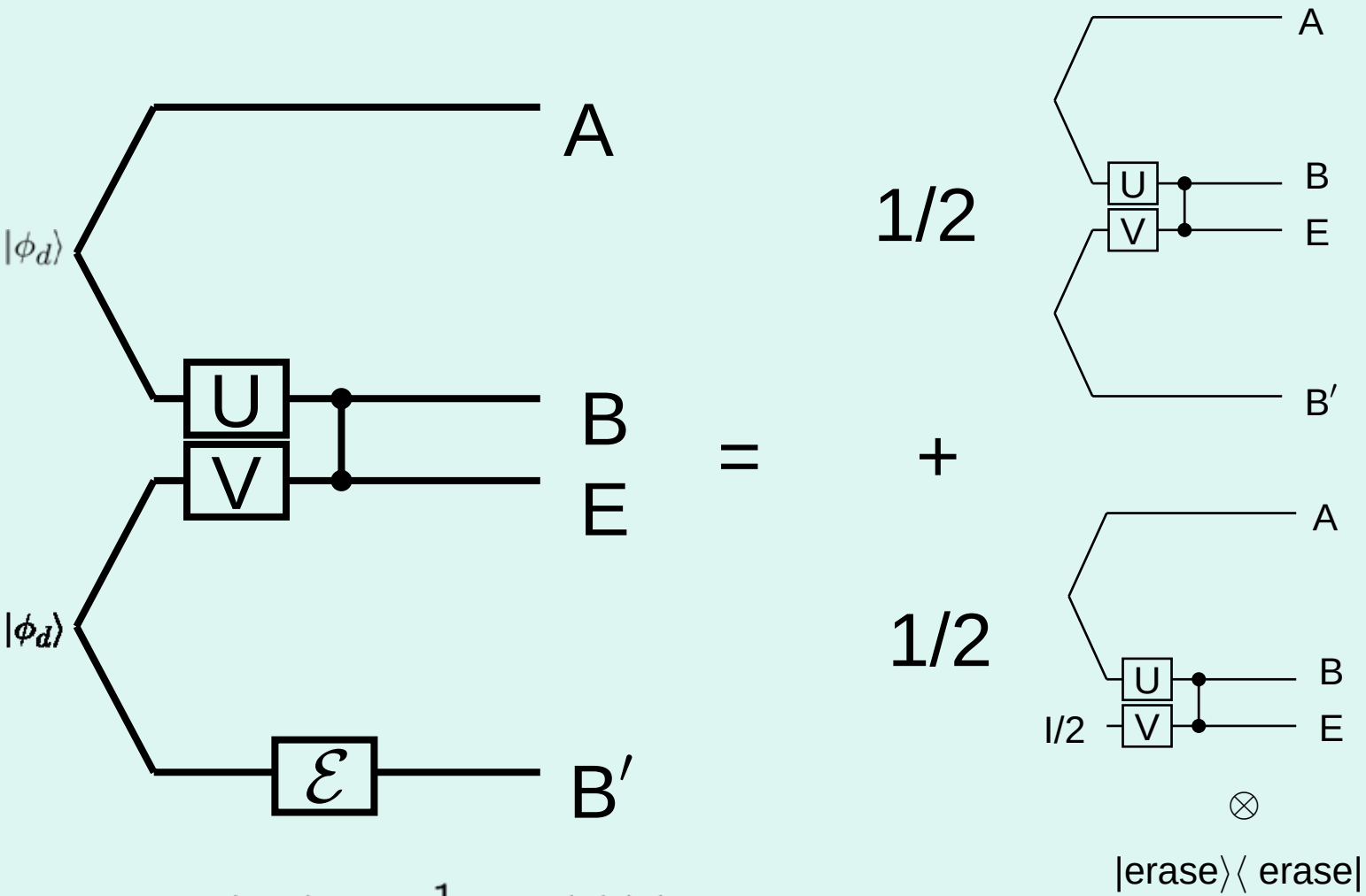
High Joint Capacity

- What channel should we use $\mathcal{R}_d$ with?
- We'll use a 50% erasure channel:

$$\mathcal{E}(\rho) = \tfrac{1}{2}\,\rho + \tfrac{1}{2}\,|\text{erase}\rangle\langle\text{erase}|$$

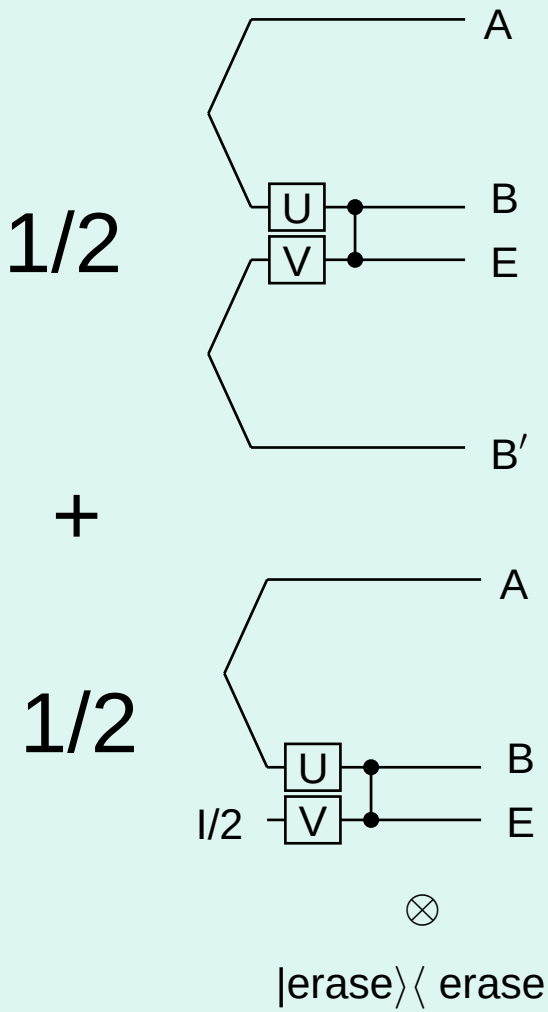
- How should we use it?

High Joint Capacity



$$|\phi_d\rangle = \frac{1}{\sqrt{d}} \sum_i |i\rangle|i\rangle$$

Coherent Information: average of two terms

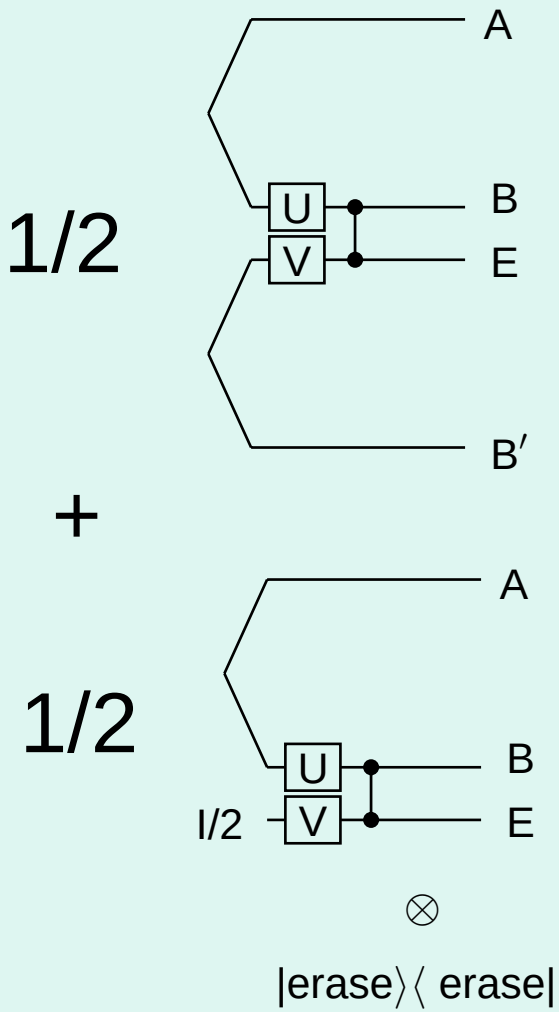


½ I^{coh}(not erased)

+

½ I^{coh}(erased)

Coherent Information: average of two terms



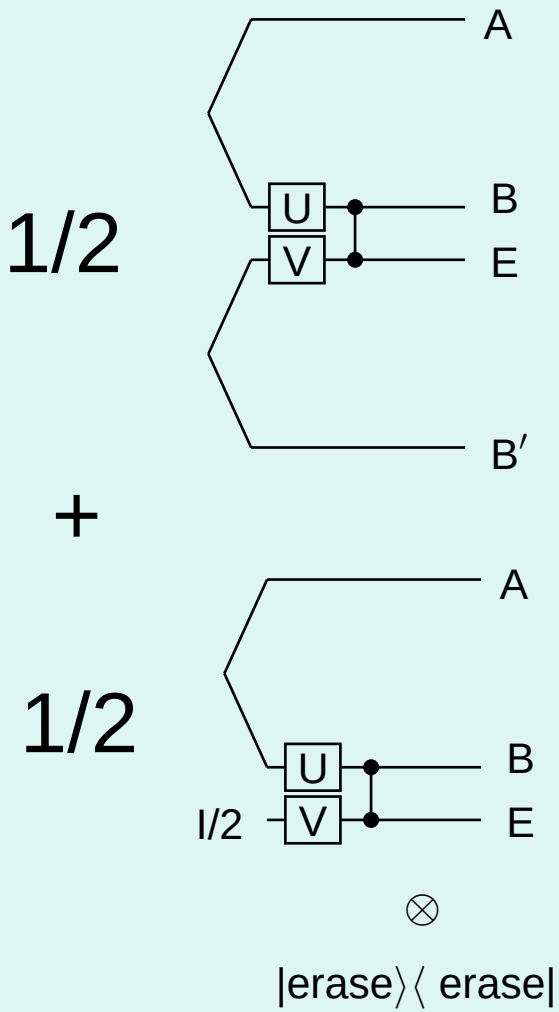
½ I^{coh}(not erased)

+

½ I^{coh}(erased)

This term is zero.

Coherent Information: average of two terms



½ I^{coh}(not erased)

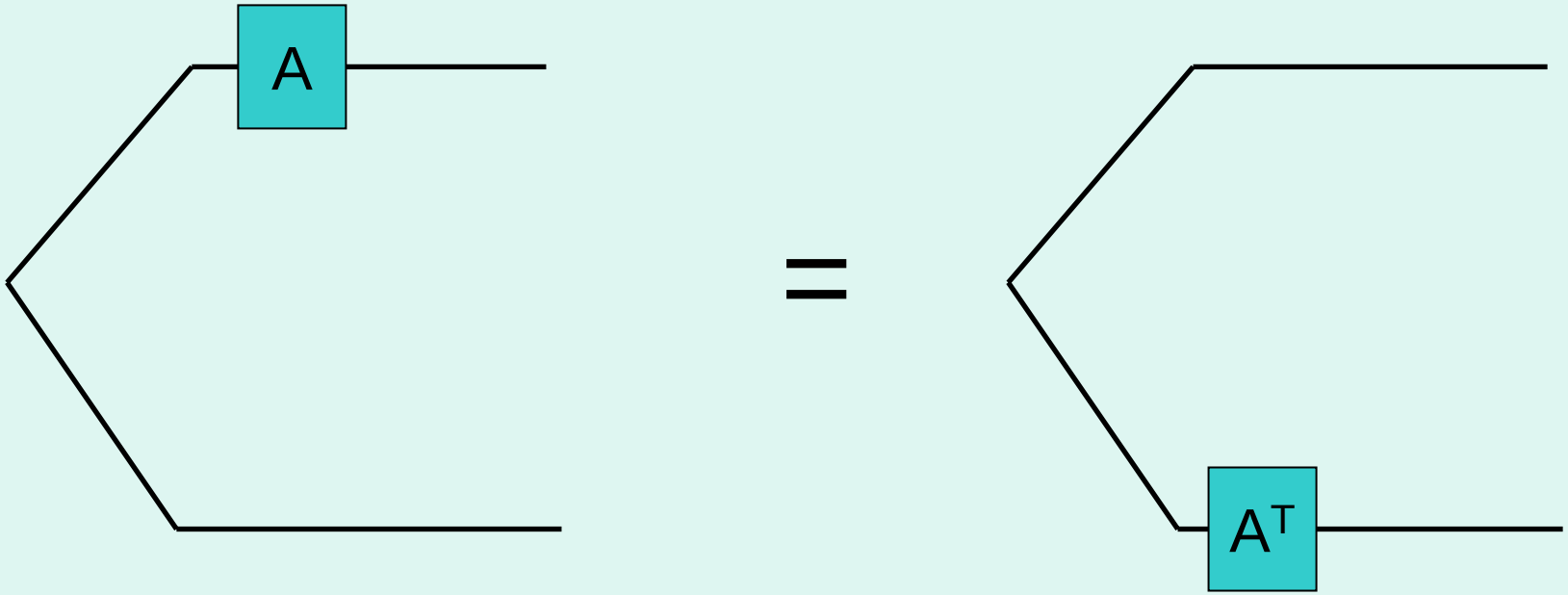
+

How big is this?

½ I^{coh}(erased)

This term is zero.

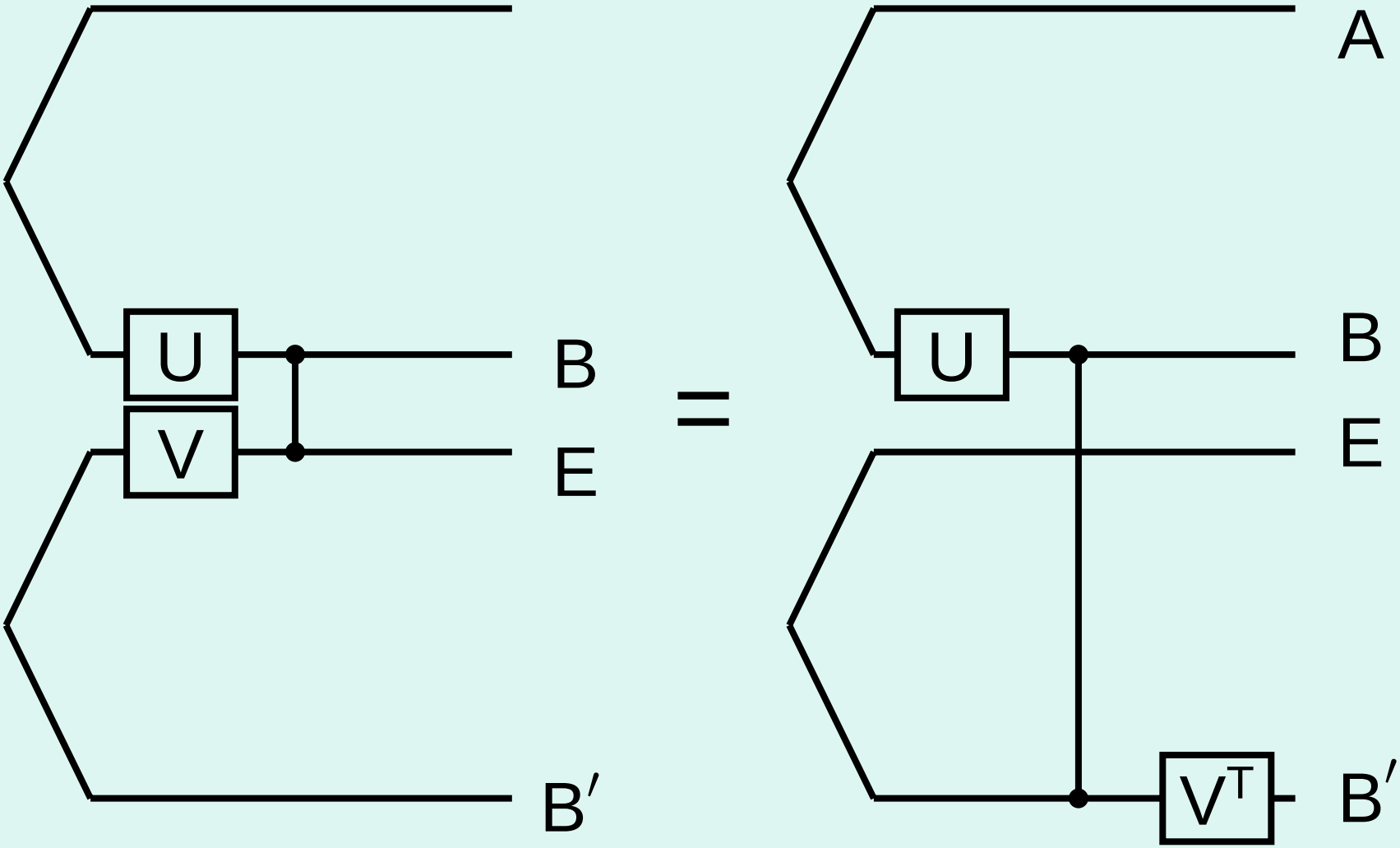
A nice identity



$$A \otimes I \, |\phi_d\rangle = \sum A_{i,j} \, |i\rangle \, |j\rangle \qquad I \otimes B \, |\phi_d\rangle = \sum B_{j,i} \, |i\rangle \, |j\rangle$$

$$|\phi_d\rangle = \sum |i\rangle \, |i\rangle$$

Bob can undo interaction



Bob can undo interaction

- Coherent information doesn't increase when Bob operates, so when there's no erasure, $I^{coh} = \log d$
- The overall coherent information, and therefore capacity satisfies

$$Q(\mathcal{R}_d \otimes \mathcal{E}) \geq I^{coh} \geq \tfrac{1}{2} \log d$$

Superadditivity of Privacy

- So, what we have is two channels, one with private capacity $P(\mathcal{E}) = 0$ and the other with $P(\mathcal{R}_d) \leq C(\mathcal{R}_d) \leq 2$
- The joint *quantum* capacity is

  $Q(\mathcal{R}_d \otimes \mathcal{E}) \geq ½ \log d$
- This tells us that the private capacity is strongly superadditive, but also that privacy was not the necessary component for superactivation of quantum capacity.
- We were beaten to the punch by Carl Li, Andreas Winter, etc.. Consoled ourselves by concentrating on the “simplicity” of our channels and “extensive” violations.

Outline

- ~~Quantum and Private Capacities~~
- ~~Channels with Zero Quantum Capacity~~
- ~~Superactivation of Quantum Capacity~~
- ~~Superadditivity of Private Capacity~~
- Applications

More implications

- The quantum capacity is not convex:

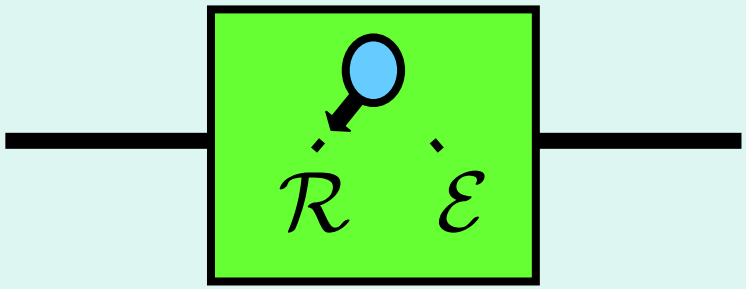
$$Q((1-p)\mathcal{N} + p\mathcal{M}) > (1-p)Q(\mathcal{M}) + pQ(\mathcal{N})$$

- Coherent information is a poor approximation to the quantum capacity (failure of random coding):

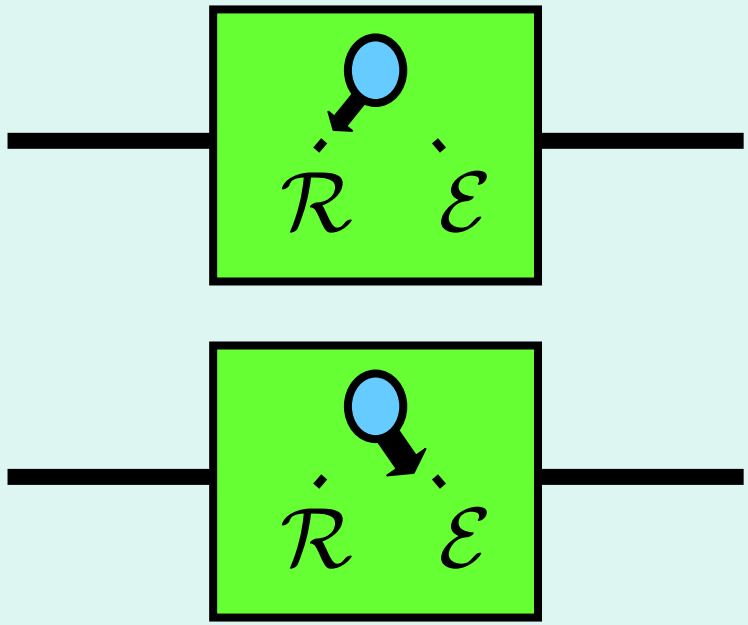
$$Q(\mathcal{N}) = \lim_{n\to\infty} \frac{1}{n} Q^1(\mathcal{N}^{\otimes n}) \geq \frac{1}{8} \log d$$

but $Q^1(\mathcal{N}) = 0$

Application: Big gap between Coherent Information and Capacity

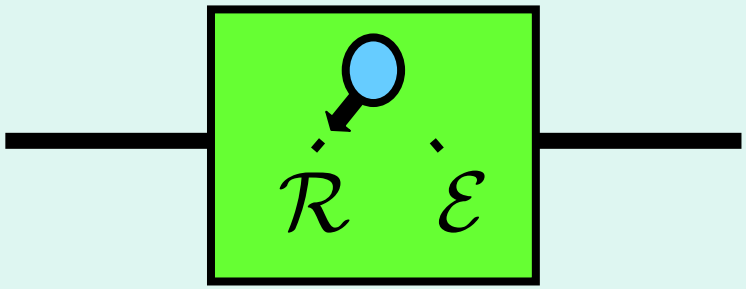


$Q^1(\mathcal{T}) \leq 2$ since it's no more than max $(Q^1(\mathcal{R}), Q^1(\mathcal{E}))$

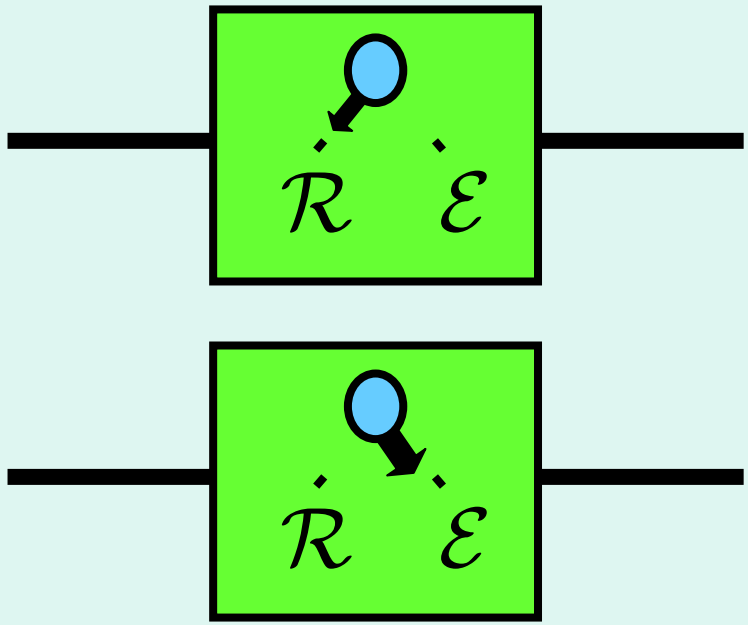


Make one channel $\mathcal{R}$ and the other $\mathcal{E}$ to get large $Q^1(\mathcal{T} \otimes \mathcal{T})$

Application: Big gap between Coherent Information and Capacity



$Q^1(\mathcal{T}) \leq 2$ since it's no more than max ($Q^1(\mathcal{R})$,$Q^1(\mathcal{E})$)



Make one channel $\mathcal{R}$ and the other $\mathcal{E}$ to get large $Q^1(\mathcal{T} \otimes \mathcal{T})$

Gives $Q^1(\mathcal{T}) \leq 2$ but

$Q(\mathcal{T}) \geq$ 1/8 log D_{in}

Summary

- The quantum capacity characterizes achievable rates of quantum transmission.
- There are different types of zero quantum capacity channels (PPT, symmetric)
- Taking one from each class leads us to superactivation of quantum capacity.
- This nonadditivity shows that the value of a channel for quantum transmission depends on the context in which it is used.
- Even though it looked like privacy was important, we can still get an effect with channels that have very little.

Questions

- When does superactivation occur?
- Quantify different types of information?
- Measure “Value Added” instead?
- What are the zero P and zero Q channels?
- Specifically, is there a zero P channel near the rocket channels? What resource do the rocket channels provide?
- Three-way interactions?

THANK YOU