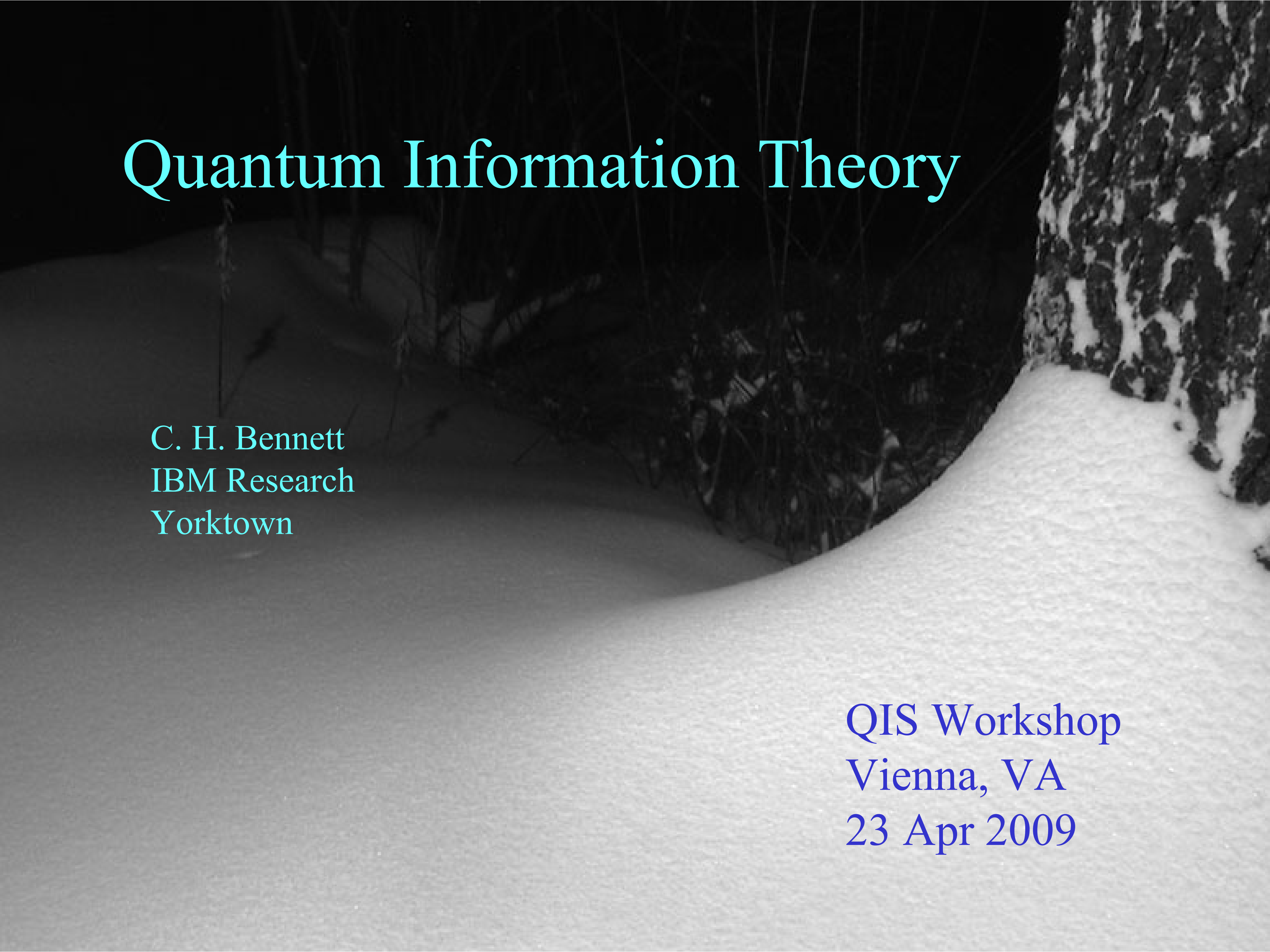


Quantum Information Theory

C. H. Bennett
IBM Research
Yorktown

QIS Workshop
Vienna, VA
23 Apr 2009

Nature and importance of Information

Distinctive features of Quantum Information

- Superposition principle, imperfect distinguishability, no-cloning
- Entanglement—an intense ***monogamous*** kind of correlation
- Multiple distinct channel capacities: quantum, private, classical, entanglement-assisted…

Feats and Achievements, Challenges and Puzzles

Importance as basic science and for science education

Nature and Importance of Information

Information and Computation Theory was developed by considering bits and logic gates abstractly, ignoring the nature of the information carriers and the mechanisms of their interaction.

Our information society is built on the success of this abstraction

(**Information Theory** | Computation Theory)

distributed computation

cf Broadbent, Watrous talks

But the correct arena for making this abstraction is ***quantum, not classical***

Recasting the classical theory in this way yields

- Dramatic speedups of some classically hard computations

- New kinds of communication and measurement

- New encryption techniques and breaking of some old ones.

- An exciting area of basic science

superposition principle

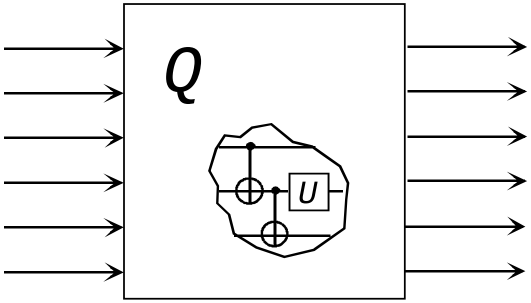
Between any two reliably distinguishable states of a quantum system

(for example horizontally and vertically polarized single photons)

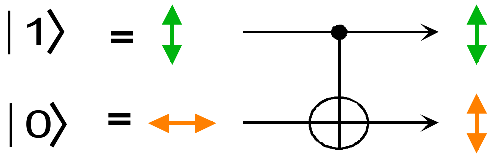
there exists a continuum of intermediate states (representable as complex linear combinations of the original states) that in principle cannot be reliably distinguished from either original state.

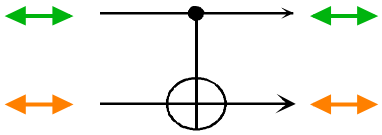
(for example diagonal polarizations)

Any quantum data processing can be done by 1- and 2-qubit gates acting on qubits.

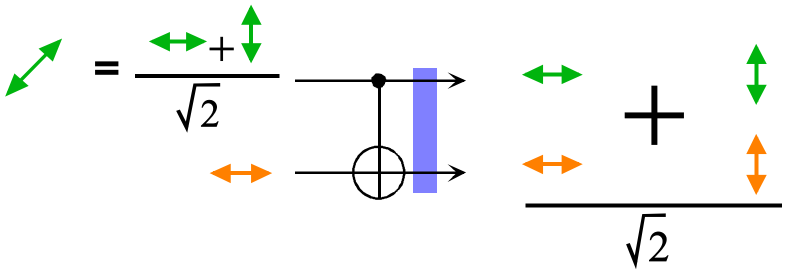


The 2-qubit XOR or "controlled-NOT" gate flips its 2nd input if its first input is 1, otherwise does nothing.





A superposition of inputs gives a superposition of outputs.



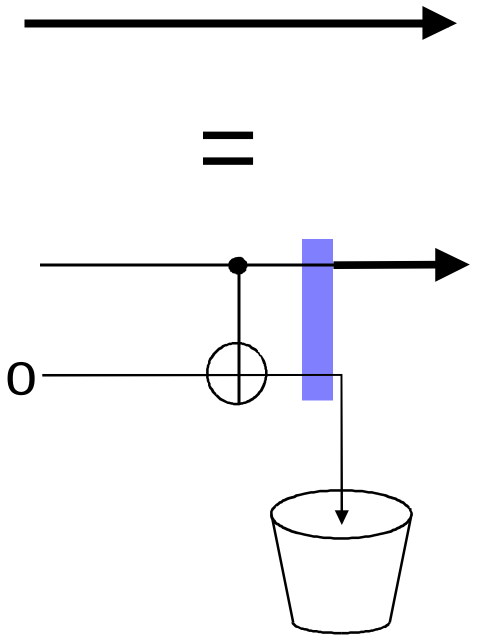
An entangled or EPR tate.

Expressing classical data processing in quantum terms.

A classical bit is just a qubit with one of the Boolean values **0** or **1**.

A classical wire is a quantum channel that conducts **0** and **1** faithfully, but randomizes superpositions of **0** and **1**.

(This occurs because the data passing through the wire interacts with its environment, causing the environment to learn the value of the data, if it was **0** or **1**, and otherwise become entangled with it.)



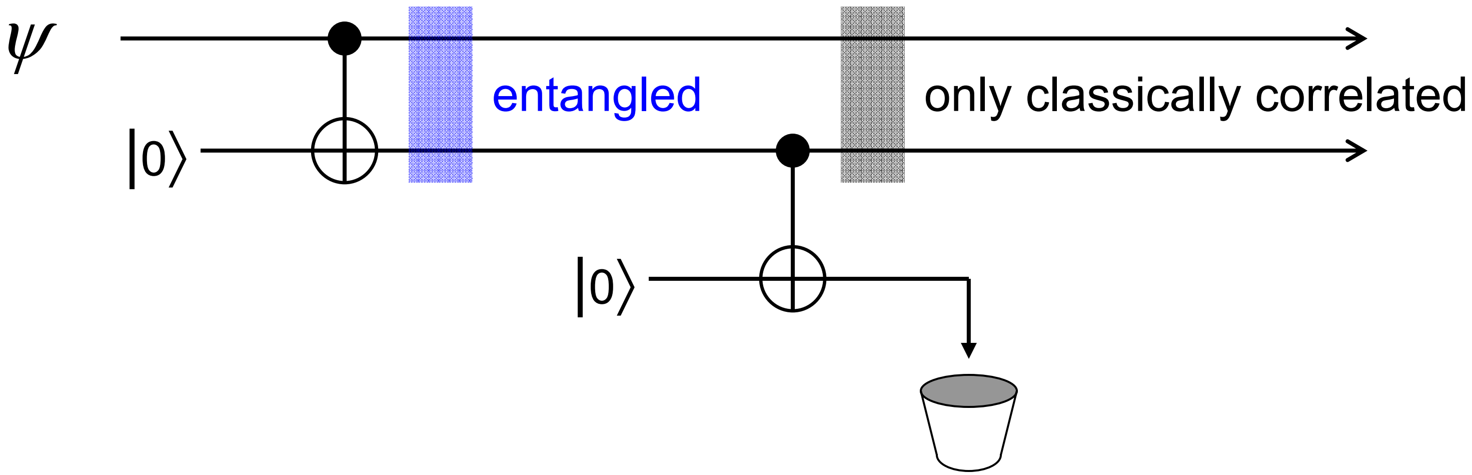
A classical channel is a quantum channel with an eavesdropper.

A classical computer is a quantum computer handicapped by having eavesdroppers on all its wires.

Entanglement is an intense and private kind of correlation

- A pure quantum whole can have impure parts, whereas classically a whole can be no purer than its most impure part.
- Monogamy: If A and B are maximally entangled with each other, they cannot be even classically correlated with anything else.
- Indeed classical correlation typically arises from unsuccessful attempts to clone entanglement.

Two is a couple, three is a crowd.



Entanglement is a quantifiable nonlocal resource that can be harvested from physical systems, distilled into standard form (“ebits”) and used for various purposes such as entanglement-assisted communication.

Though having no communication capacity of its own, entanglement can

- allow quantum information to be transmitted through a classical channel

- increase a quantum channel’s capacity for transmitting classical information.

- improve the precision of measurement

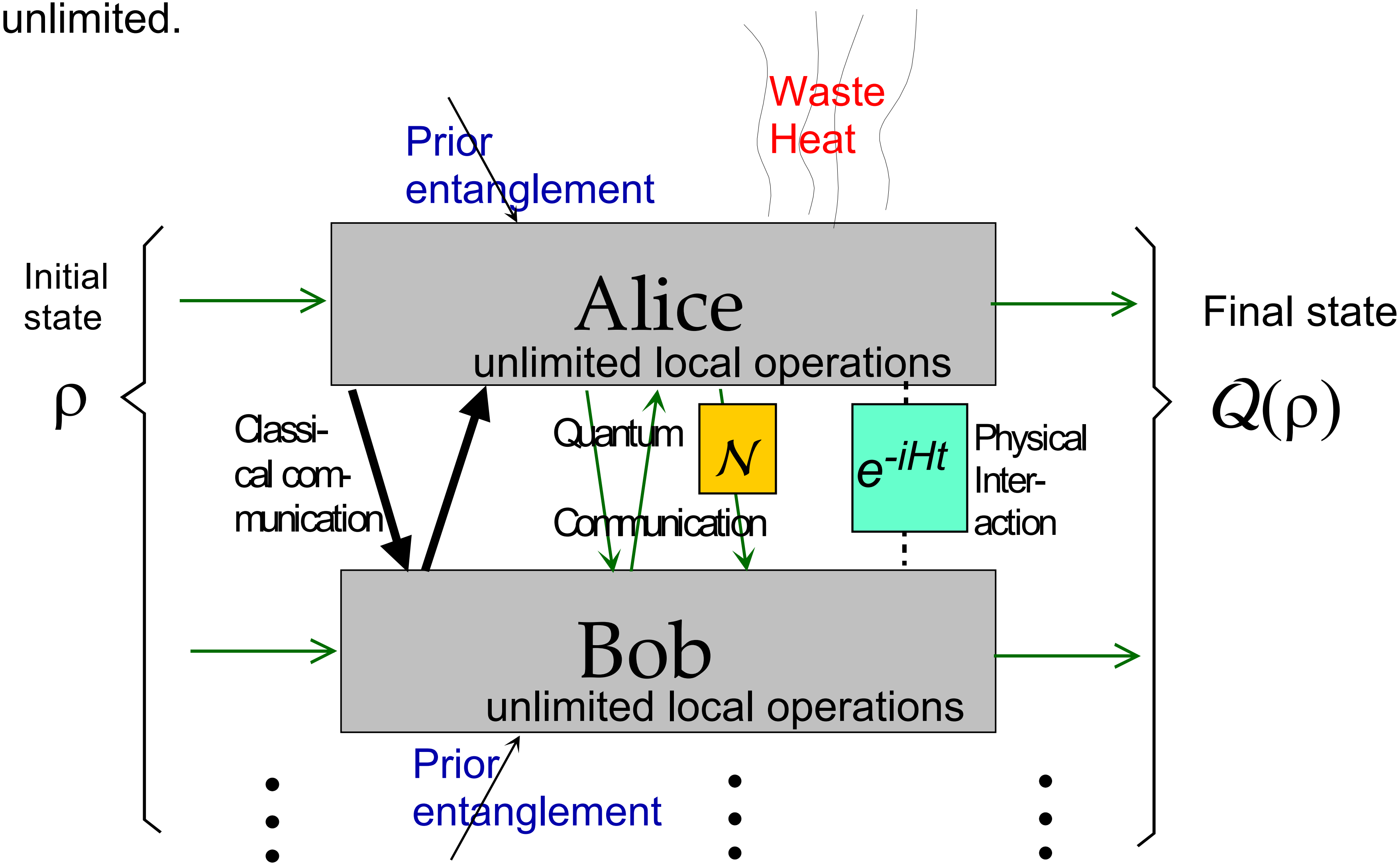
In classical information theory, a channel has a single capacity, and its capacity is not increased by auxiliary resources such as shared randomness between sender and receiver, or back communication (feedback) from receiver to sender

$$C_R=C_B=C$$

(However shared randomness, in the form of a one-time pad, makes it possible to communicate ***secretly*** over a public channel. Back communication, though it doesn't increase capacity, reduces encoding/decoding effort and latency.)

Moreover (for memoryless channels) the classical capacity is given by a simple single-letter formula, being the maximum, over source distributions, of the Shannon mutual information between input and output.

An important goal of quantum information theory is to understand the nonlocal resources, and tradeoffs among them, needed to transform one state of a multipartite system into another, when local operations are unlimited.



These questions can be asked in an exact setting

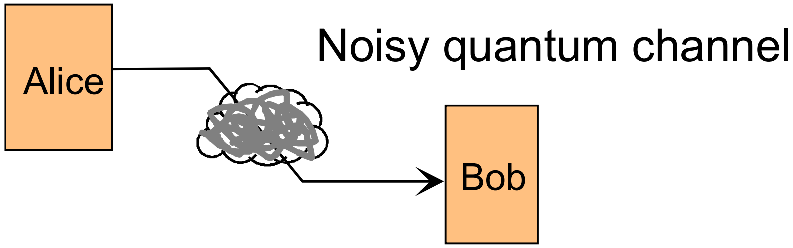
$$\rho \longrightarrow \mathcal{Q}(\rho)$$

or in the regularized IID setting characteristic of information theory, where one seeks to transform many copies of the input state into a high-fidelity approximation to many copies of the desired output state

$$\rho^{\otimes n} \longrightarrow \approx \mathcal{Q}(\rho)^{\otimes n}$$

By appropriate choice of the transformation $\mathcal{Q}$ which one seeks to implement (a completely positive trace preserving map on multipartite states), one can define state properties like distillable entanglement, and many sorts of channel capacity

Multiple capacities of Quantum Channels



Q plain quantum capacity = qubits faithfully trasmitted per channel use,

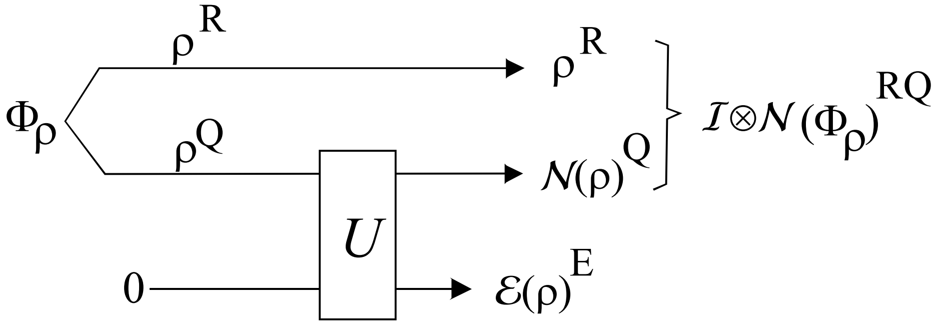
P capacity for sending classical bits ***privately*** when Eve holds Environment

C plain classical capacity = bits faithfully trasmitted per channel use $\boldsymbol{Q \leq P \leq C}$

$\boldsymbol{Q_B}$ quantum capacity assisted by classical back communication
$\boldsymbol{Q_2}$ quantum capacity assisted by classical two-way communication

$\boldsymbol{C_E}$ entanglement assisted classical capacity i.e. bit capacity in the presence of unlimited prior entanglement between sender and receiver.

For quantum channels, these assisted capacities can be greater than the corresponding unassisted capacities.



Mostly Frustrating Search for Simple Expressions for the various Capacities

C = Holevo cap. = $\lim_{n\to\infty} \max_{\{p_x,\rho_x\}} (S(\mathcal{N}^{\otimes n}(\rho)) - \Sigma p_x S(\mathcal{N}^{\otimes n}(\rho_x)))/n$
regularized

Regularization needed---Hastings 2008

P = Private cap. = $\lim_{n\to\infty} \max_{\{p_x,\rho_x\}} (I(X;\mathcal{N}^{\otimes n}(\rho_x)) - I(X;\mathcal{E}^{\otimes n}(\rho_x)))/n$

Devetak quant-ph/0304127

Q = Coherent Info. = $\lim_{n\to\infty} \max_{\rho} (S(\mathcal{N}^{\otimes n}(\rho)) - S(\mathcal{E}^{\otimes n}(\rho)))/n$ LSD
regularized

C_E = Quantum Mutual Info. = $\max_{\rho}\ S(\rho) + S(\mathcal{N}(\rho)) - S(\mathcal{E}(\rho))$
(reg. not needed)

BSST01

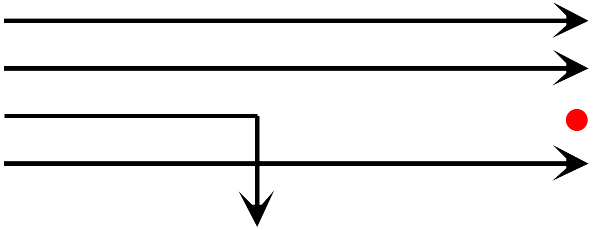
No good expressions for Q_2 , Q_B

Superactivation: $\exists \mathcal{M},\mathcal{N}$ $Q(\mathcal{M})=Q(\mathcal{N})=0$ but $Q(\mathcal{M}\otimes\mathcal{N})>0$ SY08

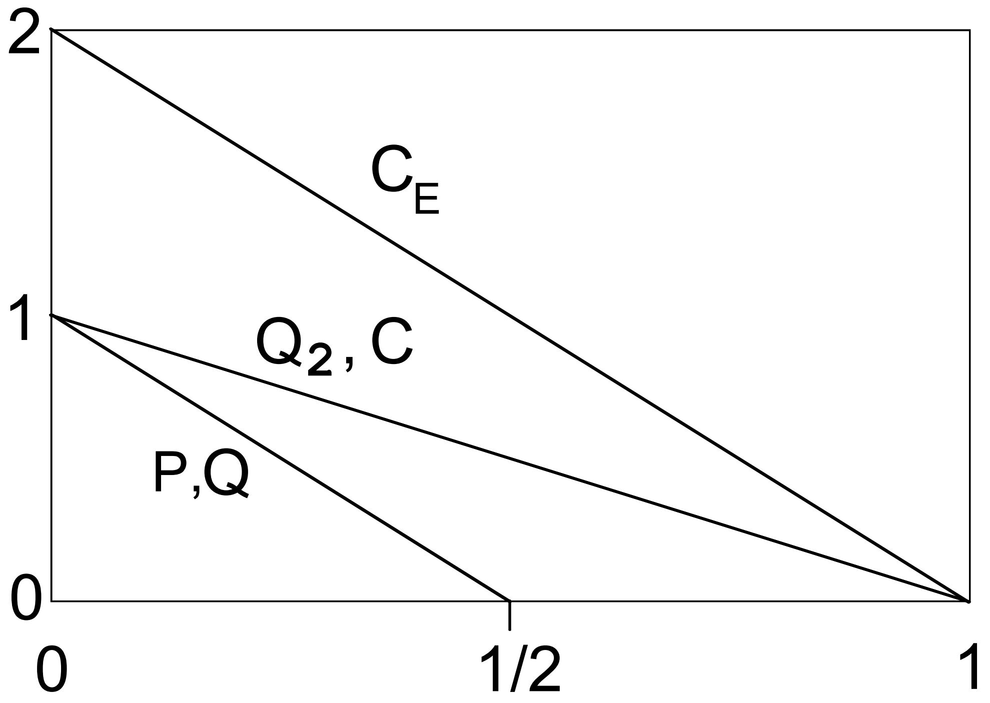
Simple illustrative example

Quantum Erasure Channel

input qubit sometimes lost



Capacities of Quantum Erasure Channel

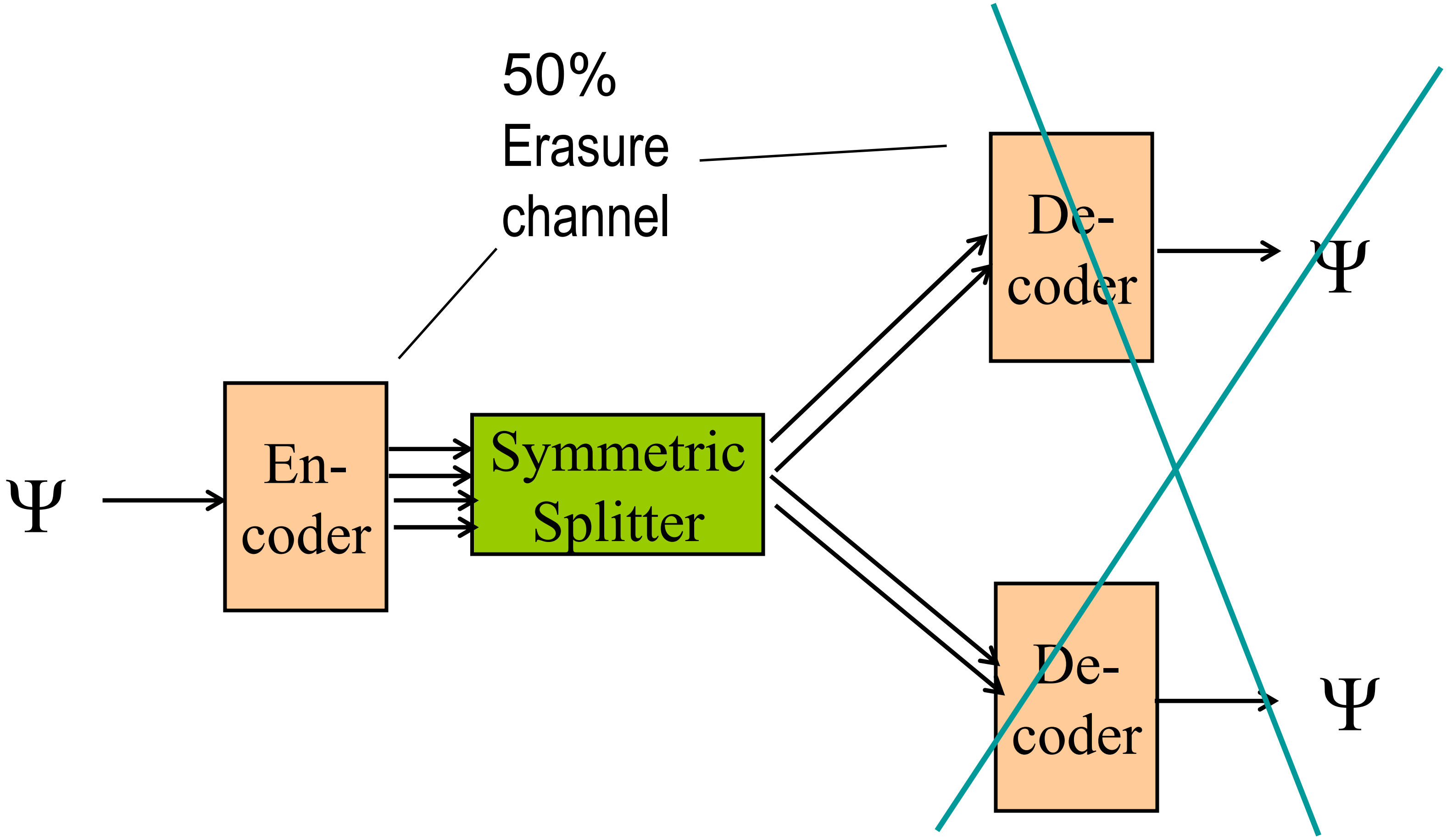


Erasure Probability

A 50% erasure channel can be viewed as one output of a symmetric splitter.

Because of this its unassisted quantum capacity Q must be zero.

If this were not the case, the splitter could be used together with an encoder and two decoders to clone unknown quantum states.



But when assisted by classical communication or shared entanglement, the 50% erasure channel acquires a nonzero quantum capacity:

With Classical 2-way communication

- Alice uses the erasure channel to send Bob halves of EPR pairs.
- Bob reports back classically which ones arrived successfully.
- Alice uses these and forward classical communication to teleport the quantum input to Bob

With Shared Entanglement

- With the help of ordinary Shannon coding, Alice uses the erasure channel's forward classical capacity (50%) to send Bob the classical bits needed for teleportation. They already have the other resource required, viz Alice-Bob entanglement.

With Classical Back Communication alone

- Combine the two constructions above

Another Useful Assistive Resource: the 50% Quantum Erasure Channel itself, or more generally, “symmetric side channels”, viz any channel that can be viewed as one output of a symmetric splitter. Such channels have no quantum capacity Q, so one can define the assisted capacity

$\boldsymbol{Q_{ss}}$ = Symmetric side channel-assisted Quantum Capacity
(G.Smith, J.Smolin, A.Winter IEEE-IT, quant-ph/0607039)

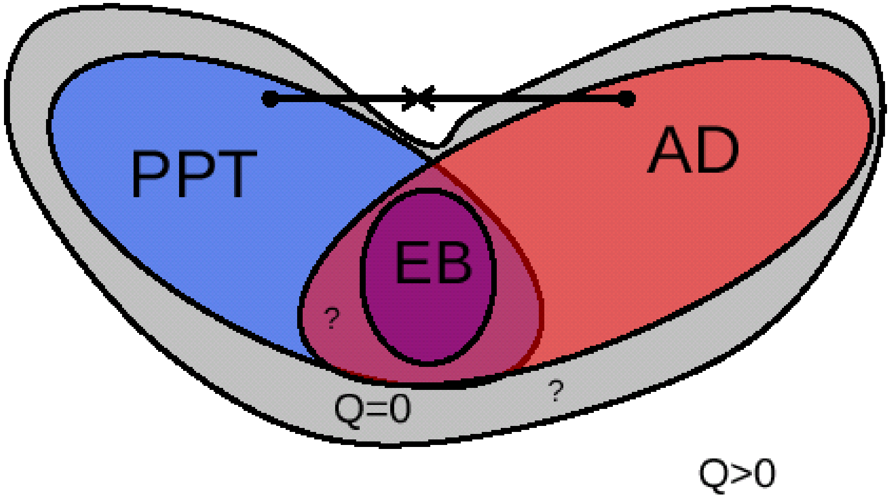
Smith and Yard (arXiv/0807.4935) showed a nice relation between private classical capacity and this assisted quantum capacity, namely that for all channels, $\boldsymbol{P} \leq 2\boldsymbol{Q_{ss}}$

K.,M.and P.Horodecki and J.Oppenheim had previously (quant-ph/0506189) found channels with $\boldsymbol{Q} = 0$ but $\boldsymbol{P} > 0$. Combining these facts Smith and Yard obtained the surprising result:

There exist pairs of channels, each with no quantum capacity, which have positive quantum capacity when used together:

$Q(\mathcal{M})=Q(\mathcal{N})=0$ but $Q(\mathcal{M}\otimes\mathcal{N})>0$

The set of Zero-Quantum-Capacity channels is not convex



PPT = Positive Partial Transpose-enforcing channels (e.g. Horodecki)
EB = Entanglement-breaking channels
AD = Antidegradable channels, such as the 50% erasure channel

- Is privacy necessary for superactivation of quantum capacity?
- Is there a third sex, i.e. a third incomparable kind of zero-quantum capacity channel that can superactivate one or more of the other kinds?
- Is private capacity superactivatible? (Need nontrivial upper bound on P)

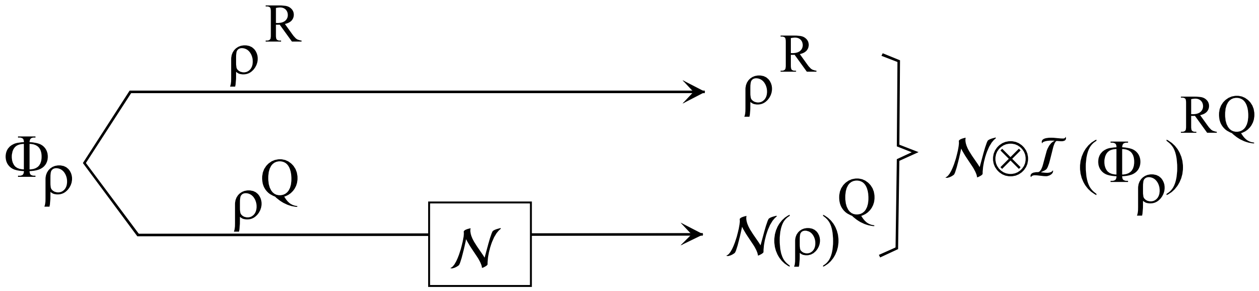
Additivity Status of Some Capacities and Single-Letter Correlation Measures

Information \ Quantity	Capacity	Correlation Measure
Classical	?	Holevo Information $\chi = \max I(X;B)$ No [Hastings Nat. Phys. '09]
Private	No [S-Smolin PRL'09] [Li-Winter-Zou-Guo '09]	Private Information $\max I(X;B) - I(X;E)$ No [S-Renes-Smolin PRL'08]
Quantum	No [S-Yard Science'08]	Coherent Information $\max S(B) - S(E)$ No [Div-Shor-Smolin PRA'96]
Entanglement assisted	Yes	Yes Quantum Mutual Information max $S(B)+S(BE) - S(E)$ [BSST 01]

With all these capacities, complicated formulas, and especially the ability of zero-quantum-capacity channels to superactivate one another, quantum capacity theory is beginning to look ugly.

But there are also some results that make it begin to look simple again.

- Entanglement-assisted capacity
- Approximate Randomization and Data Hiding
- Reversible State Redistribution



(entangled
purification
of ρ)

$$C_E(\mathcal{N}) \;=\; \max_\rho \quad S(\rho) \;+ S(\mathcal{N}(\rho)) - S(\mathcal{N}\otimes\mathcal{I}(\Phi_\rho))$$

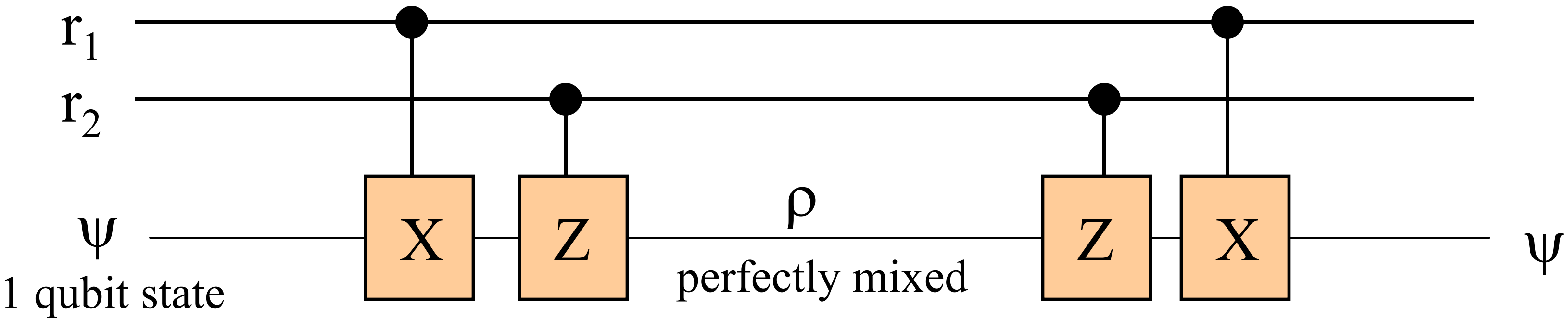
Entanglement-Assisted capacity C_E of a quantum channel $\mathcal{N}$ is equal to the maximum, over channel inputs ρ, of the input (von Neumann) entropy plus the output entropy minus their "joint" entropy (more precisely the joint entropy of the output and a reference system entangled with the late input) (BSST 0106052, Holevo 0106075).

In retrospect, ***entanglement-assisted capacity***, not plain classical capacity, is the natural quantum generalization of the classical capacity of a classical channel. What Shannon actually found in 1948 was a nice formula for the entanglement-assisted capacity of a classical channel.

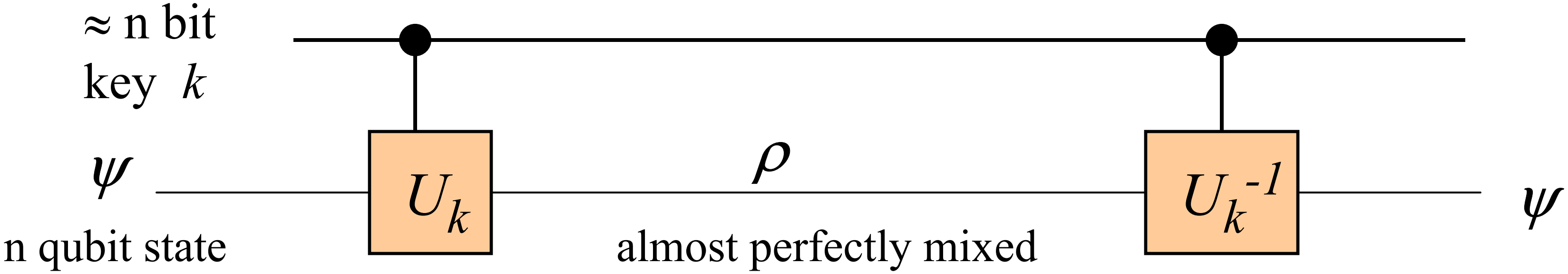
$Q_E = C_E / 2$ for all channels, by teleportation & superdense coding.

Private Quantum Channels and Approx. Randomization

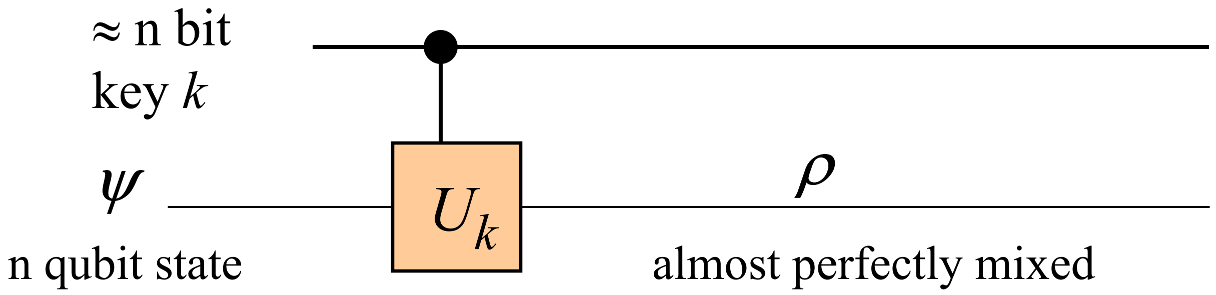
It is well known that two random key bits are necessary and sufficient to perfectly encrypt a qubit, so that regardless of the input ψ, the intermediate "ciphertext" looks completely mixed.



But if we are willing to settle for asymptotically perfect encryption, then in the limit of large block size, only half as much key is needed.



Curiously, this encryption, while hiding pure states almost perfectly, does not hide entangled states well at all. (Hayden, Leung, Shor, Winter 0307104)



≈ n bit key k

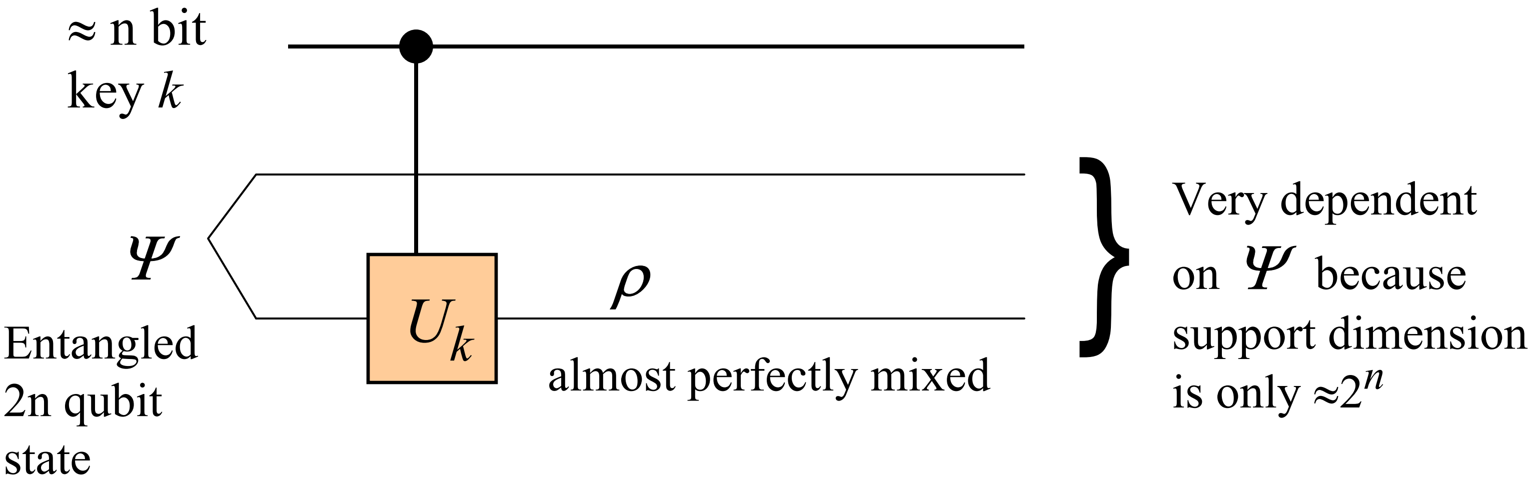
ψ

n qubit state

U_k

ρ

almost perfectly mixed



≈ n bit key k

Ψ

Entangled 2n qubit state

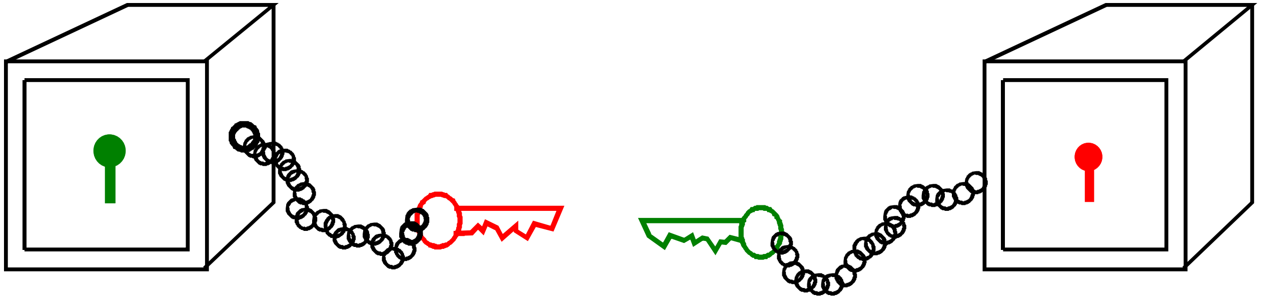
U_k

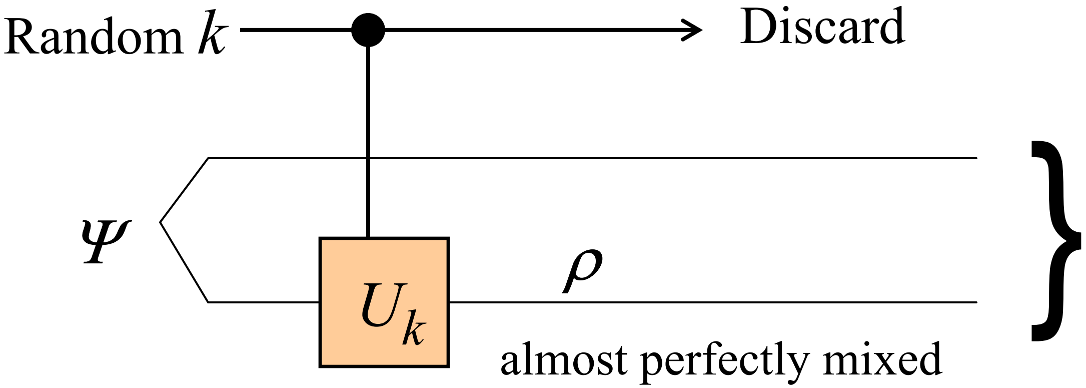
ρ

almost perfectly mixed

Very dependent on Ψ because support dimension is only ≈2^n

Data Hiding: A multipartite state which stores classical data that can be recovered by a joint measurement, but not by any sequence of local measurements and classical communication. Like 2 locked boxes each chained to the other's key .

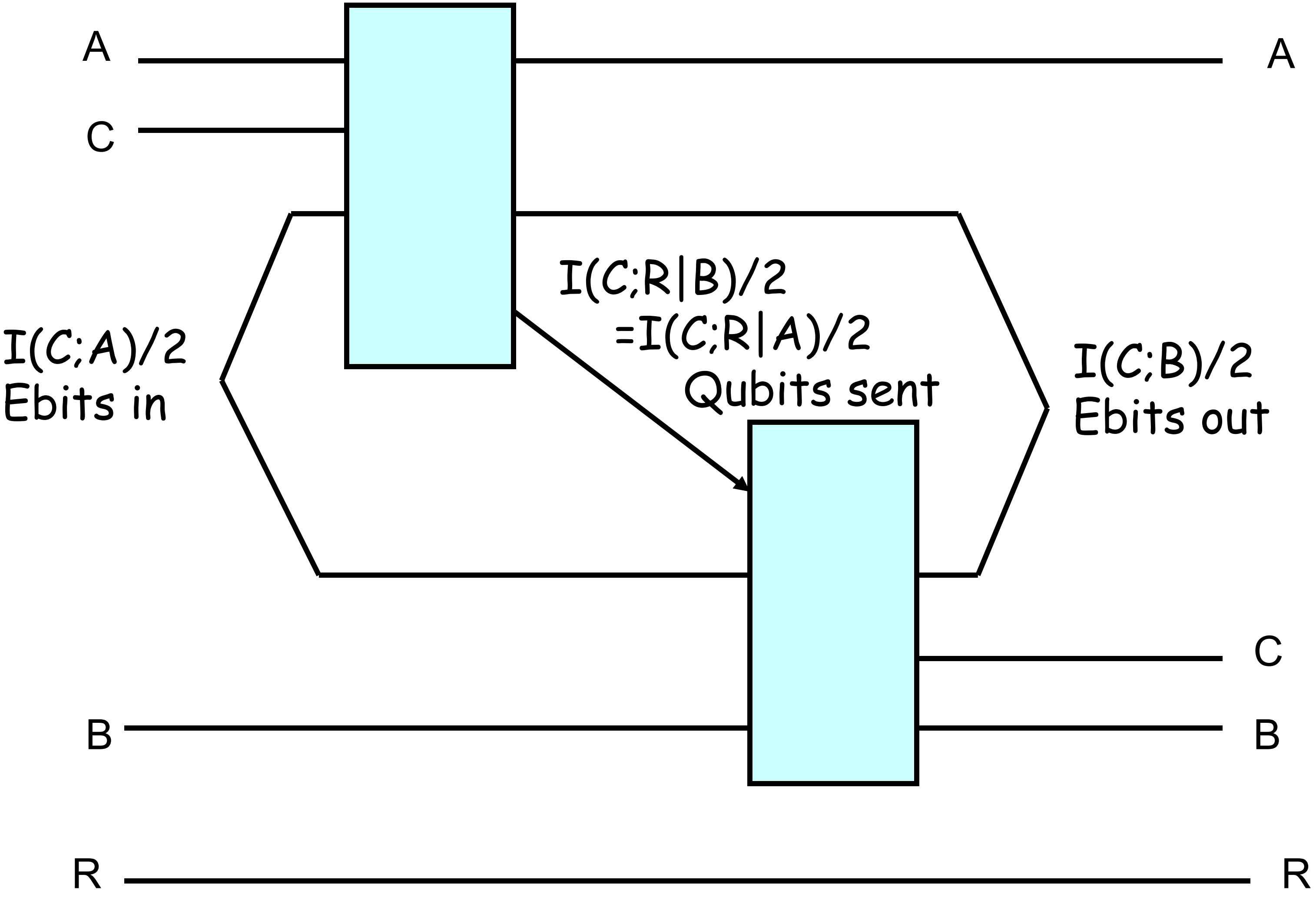




Resulting $2n$ qubit bipartite mixed state

Hides nearly n bits of classical data

Quantum State Redistribution: Reversibly transforming iid tripartite pure state (AC | B | R) into (A | CB | R) by local actions, quantum communication, and shared entanglement. R is a passive reference system. (recent work by Devetak & Yard, Oppenheim)



Some Quantum Information Feats and Successes

- Quantum Cryptography
  - Quantum Key Distribution (Lütkenhaus talk)
  - No-go theorem for bit commitment and post-cold-war cryptography (but can do it with limits on q memory)

- Quantum Error Correction
  - Quantum Error Correcting Codes
  - Entanglement Distillation Protocols
  - Fault Tolerant computation (Preskill talk)

- Entanglement-assisted protocols
  - teleportation and superdense coding
  - entangled illumination (Lloyd, Shapiro cf. e.g. 0904.2490)
  - entanglement-assisted measurement (Wineland talk)

Quantum Information as Basic Science

A simpler view of information, interaction, and correlation, applicable to computer science, physics, and education

- Classically there are many incomparable kinds of interaction; quantumly there is only one kind, which can generate entanglement or communicate in either direction.

- Quantum origin of classical behavior (3 is a crowd)

- Entanglement and black hole thermodynamics (e.g. Hayden, Preskill)

- QIS is a subject undergraduates are excited about, challenging teachers to dispel the mystery and guide their enthusiasm

Some Quantum Information Theory Challenges

- Additivity and Superactivation Questions – How many sexes?

- Alternatives to LOCC (local operations and classical communication) as a possibly simpler regime for a resource-based theory of quantum communication

- Understand Capacities better, especially the most poorly characterized ones like Q_2 and P.

- Multipartite Communication and Entanglement Theory: Quantum Multiple Access and Broadcast Channels.

- Better Error correction and distillation protocols, especially as enablers for fault tolerant quantum computation.