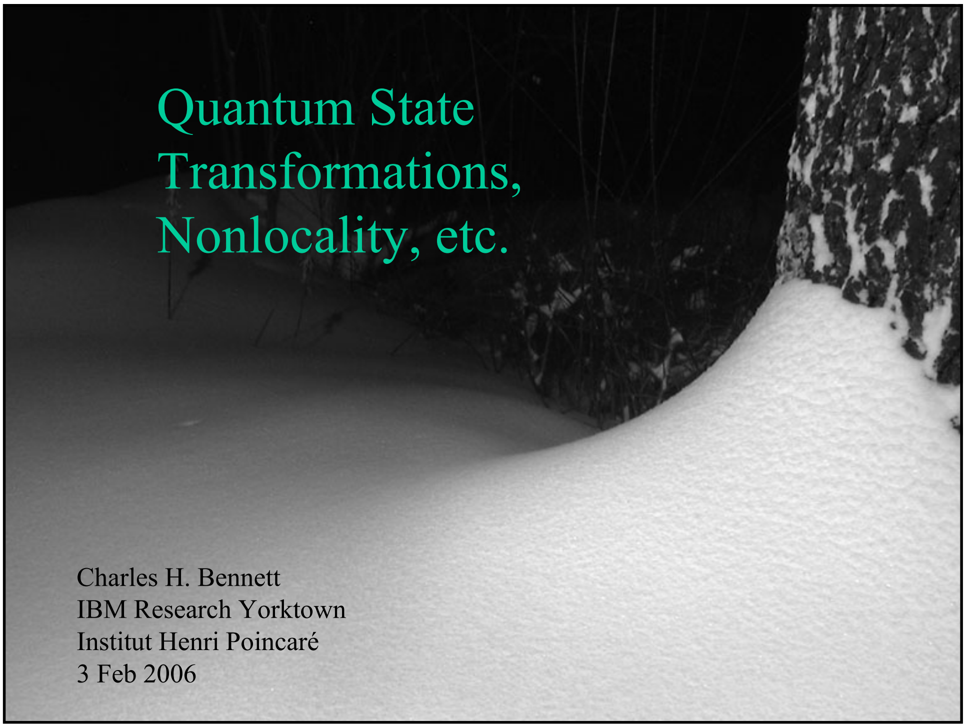


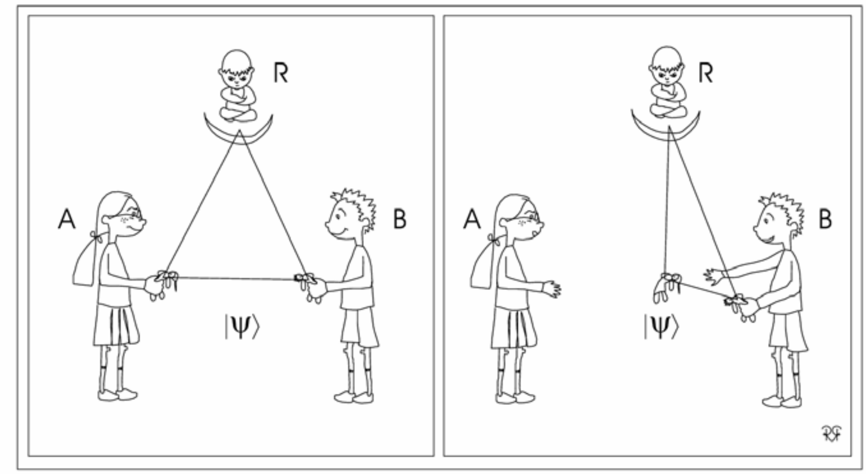
Quantum State Transformations, Nonlocality, etc.

Charles H. Bennett
IBM Research Yorktown
Institut Henri Poincaré
3 Feb 2006

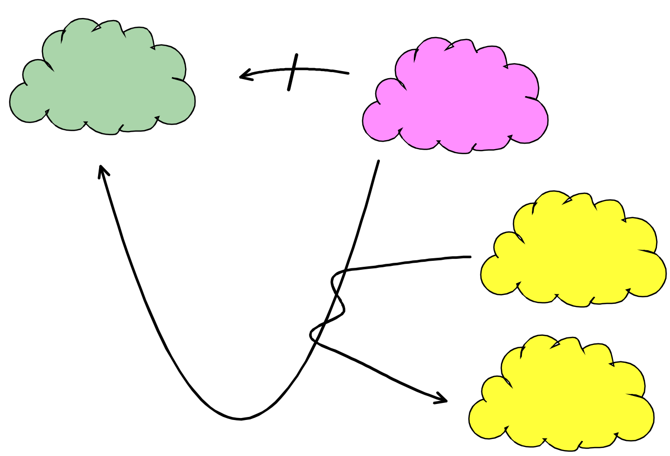
- More resource conversions
  - State Merging
  - Catalysis & Embezzling
- Degrees of knowledge of a quantum state
  - Impossibility of antiunitary transformation
  - Degrees of knowledge of a unitary transformation
  - Remote state preparation
  - When more words are needed to convey less information
- Nonlocal storage of classical information
  - Nonlocality without entanglement
  - Hiding classical data from LOCC prying
  - Unlocking classical correlations

- Publicity and Privacy in the Quantum world and the Real World

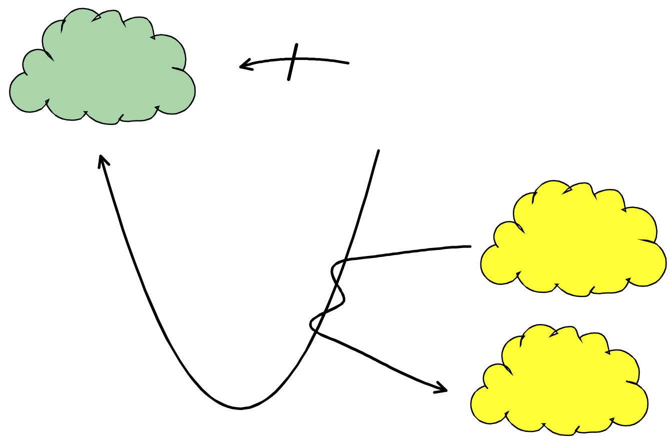
State Merging (HOW 0505062, 512127, cf also DH'W 0512015)



Asymptotically Alice can transfer her share of ψ to Bob using $I(A{:}B)=S(A)+S(B)-S(AB)$ classical bits communication and $S(A|B)=S(AB)-S(B)$ ebits. If the latter quantity is negative, the transfer can be effected while generating, instead of consuming, that many ebits. Reverse protocol can be used for state splitting.



Catalysis



Embezzling

“Entanglement Embezzling States”
(van Dam & Hayden quant-ph/0201041)

$$\mu_n = \sum_{j=1}^{n} |j\,j\rangle_{AB} /\sqrt{j}$$

have a very broad Schmidt spectrum.

Any bipartite pure state φ_{AB} on a d x d Hilbert space can be created, without communication, from an embezzling state, leaving the embezzling state almost unchanged.

$\mu_n \overset{\text{LO}}{\rightarrow} \mu_n\,\varphi$ with fidelity $>1-\varepsilon$ in the limit of large n.

How big an n is needed?
Approximately $d^{1/\varepsilon}$, so $\log n \approx (1/\varepsilon) \log d$

Embezzling states are a stronger entanglement resource than ordinary ordinary EPR pairs in the sense that one-way classical communication proportional to the square root of the embezzling state’s entropy of entanglement is required to create it from EPR pairs by entanglement dilution.

- More resource conversions
  - State Merging
  - Catalysis & Embezzling
- Degrees of knowledge of a quantum state
  - Impossibility of antiunitary transformation
  - Degrees of knowledge of a unitary transformation
  - Remote state preparation
  - When more words are needed to convey less information
- Nonlocal storage of classical information
  - Nonlocality without entanglement
  - Hiding classical data from LOCC prying
  - Unlocking classical correlations
- Publicity and Privacy in the Quantum world and the Real World

How much information does a single photon carry in its polarization?

• Infinitely much, since polarization state requires 2 real or one complex variable to describe.

• Even more, since N entangled photons require 2^N complex variables to describe their joint state.

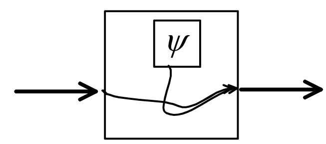
• Only 1 bit, because measuring a photon's polarization yields at most one bit about its polarization state.

• 2 bits, because a photon's state can be teleported using 2 bits and prior entanglement, and because in the presence of prior entanglement, a photon can carry 2 classical bits reliably.

Call a system $\mathcal{M}(\psi)$ a *mystification* of ψ if possession of $\mathcal{M}(\psi)$ enables one to predict the results of a measurement on ψ more accurately than one could if one had no information about ψ at all.

Examples of mystifications:

Complete classical description of ψ (the null mystification).



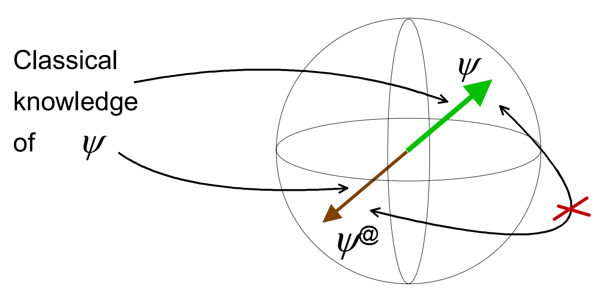
Two specimens of ψ

One specimen of ψ

One specimen of the state antipodal to ψ on the Bloch sphere.

A black box containing a specimen of ψ, a classical input port for a description of a measurement to be performed ψ, and a classical output port for the result of that measurement. The box can be used to simulate any measurement on on ψ, but cannot be reused to simulate further measurements, nor broken open to liberate the imprisoned specimen of ψ.

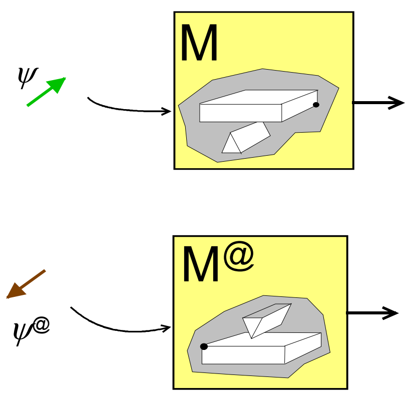
Classical knowledge of a qubit state ψ allows preparation of a specimen of ψ or of the antipodal state ψ@ (indeed arbitrarily many specimens of either). However, given a single specimen, or any finite number, ψ and ψ@ cannot be physically interconverted because it is an antiunitary transformation.



Indeed, Gisin and Popescu showed that a pair of antiparallel spins conveys more classical information about the unknown spin direction than a pair of parallel states (quant-ph/9902010).

Q. How does having a specimen of $\psi^{@}$ enable one to simulate a a measurement on ψ?

A. To simulate measurement M on ψ, just do an *antipodal measurement* (call it $M^{@}$) on $\psi^{@}$. The distribution of outcomes is the same as one would get by measuring M on ψ. True for von Neumann and generalized POVM measurements.



Same distri-bution of meas-uremen out-comes

(Given any classical measuring apparatus, an antipodal--- ie geometrically inverted--- measuring apparatus can always be built.)

$M \longleftrightarrow M^{@}$

but

$\psi \not\longleftrightarrow \psi^{@}$

Have a Classical Description of ψ =

Have infinitely many specimens of ψ =

Be able to simulate results of any number of von Neumann or generalized (POVM) measurements on ψ

⋮ ⋮

$\not\Uparrow\Downarrow$ $\not\Uparrow\Downarrow$

Have 2 specimens of ψ $\longrightarrow$ Be able to simulate any 2 POVM measurements on ψ

$\not\Uparrow\Downarrow$

Have 1 specimen of ψ $\not\longleftrightarrow$ Be able to simulate any 2 POVM measurements on ψ

$\not\Uparrow\Downarrow$ $\not\Uparrow\Downarrow$

Be able to simulate any 1 POVM measurement on ψ

$\not\Uparrow\Downarrow$

Be able to simulate any 1 von Neumann measurement on ψ

Classical knowledge or
infinitely many specimens ψ

. . .

Have 2 specimens of ψ

. . .

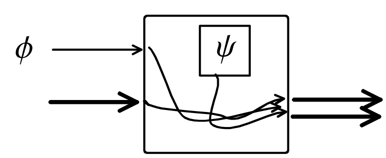
Be able to simulate any
2 measurements on ψ

Have 1 specimen of ψ

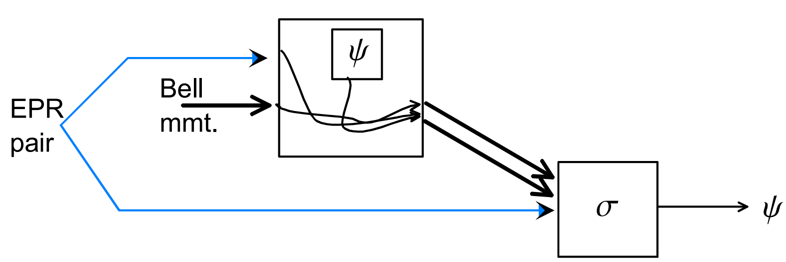
Be able to simulate 1 measurement on ψ

Be able to simulate
any 1 joint measurement on ψ and an arbitrary
other state ϕ of which one is given a single specimen

Black Box Mystification
for the ability to do a joint
measurement on ψ and
an external qubit input ϕ.



Ability to simulate any joint measurement on external qubit ϕ
and internal ψ implies ability to simulate a Bell measurement,
which can be used to *teleport* ψ *out of its prison*.



Asymptotic Equivalences and Reducibilities among Mystifications $\mathcal{M}$

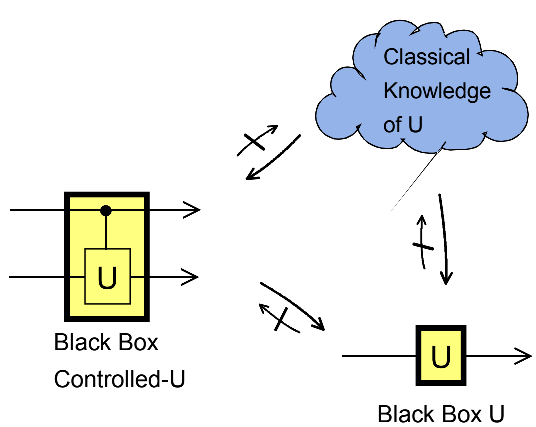
Say $\mathcal{M}_1(\psi) \preceq \mathcal{M}_2(\psi)$ if n copies of $\mathcal{M}_2(\psi)$ can be converted into m copies of $\mathcal{M}_1(\psi)$, with fidelity and efficiency (m/n) approaching 1 as $n \rightarrow \infty$

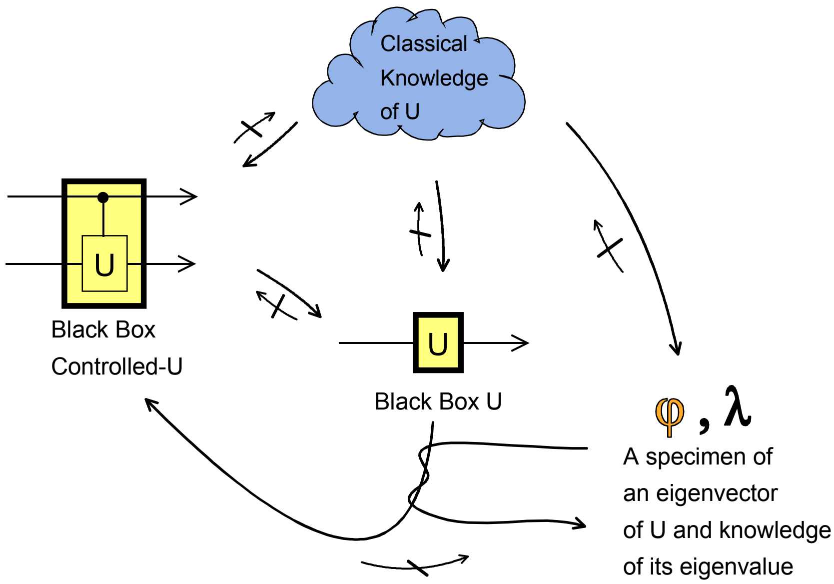
Let ρ be a labeled mixture of ψ and $\psi^{@}$ (ie a specimen of ψ or $\psi^{@}$, with an additional classical bit indicating which).

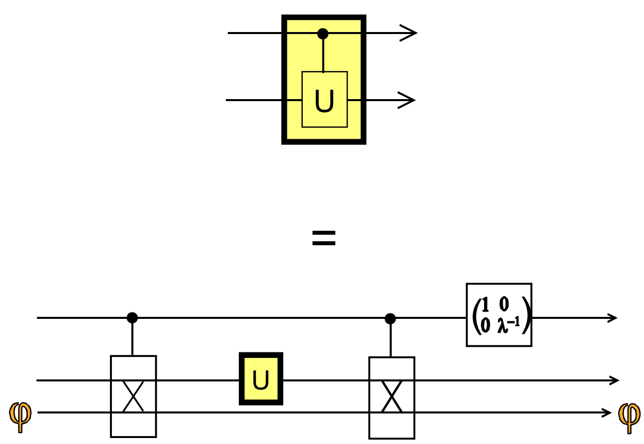
Then two copies of ρ are asymptotically equivalent to one copy each of ψ and $\psi^{@}$.

Degrees of Knowledge of Unitary Operations

(Knowledge is Power) Classical knowledge of a unitary U enables one to use it in a controlled fashion, but a simple black box for U does not.







(Hayden, Gottesman, Leung...)

Remote state preparation (RSP):

Classical description of ψ $\rightarrow$ Single specimen of ψ

Asymptotic cost of RSP is 1 ebit and 1 bit per qubit remotely prepared, ie half the classical communication cost of teleportation. (Not surprising, because sender starts with a more powerful resource)

But if we demand that RSP be exact and oblivious, leaking no extra information to the receiver besides that contained in a single specimen of the state prepared, then the cost rises to 2 bits per qubit, equal to teleportation.

More words are needed to convey less information. Like a politician who needs to use a lot of words to

Obliviousness and Remote State Preparation. In RSP Alice knows more about the quantum state than she wishes to convey to Bob.

Asymptotic cost of RSP is 1 ebit and 1 bit per qubit.

But if we demand that the protocol be perfectly oblivious, leaking no extra information to Bob besides what he could get from a single copy of the state, then the cost rises to 2 bits per qubit, like teleportation.

This tradeoff is reminiscent of a phenomenon in politics. When a politician wishes to communicate a vague idea exactly, without leaking extra information, a great many words are required, even when the idea itself is almost meaningless, like the distinction between autonomy and self-government.

• More resource conversions
    • State Merging
    • Catalysis & Embezzling
• Degrees of knowledge of a quantum state
    • Impossibility of antiunitary transformation
    • Degrees of knowledge of a unitary transformation
    • Remote state preparation
    • When more words are needed to convey less information
• Nonlocal storage of classical information
    • Nonlocality without entanglement
    • Hiding classical data from LOCC prying
    • Unlocking classical correlations

• Publicity and Privacy in the Quantum world and the Real World

---

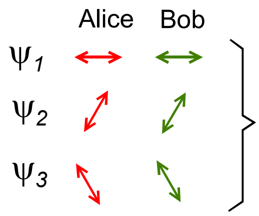
$$\Phi^+ = 00 + 11$$
$$\Phi^- = 00 - 11$$
$$\Psi^\pm = 01 \pm 10$$

Nonocal storage of information
The four Bell states are orthgonal and therefore distinguishable by a global measurement. Local operations and classical communication (LOCC) can distinguish any two Bell states but cannot distinguish all four.

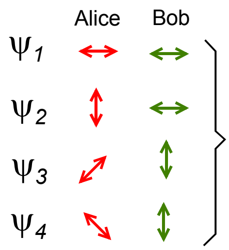
Is this imperfect local distinguishability a feature of entangled states only, or can product states exhibit it?

Are there states that are globally distinguishable, even though LOCC operations reveal *arbitrarily little* information about them?
If so, must the information-hiding states be entangled?

Early examples of unentangled states that are less distinguishable locally than globally

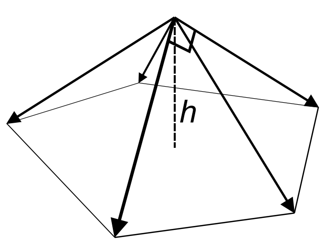


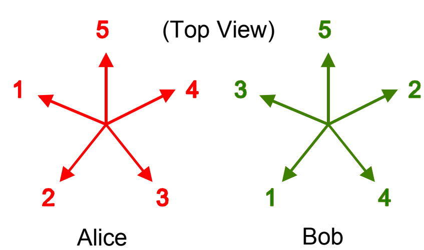
Peres-Wootters 3 trine states of 2 qubits: considered a dual to EPR, because these states are separately preparable, but more efficiently distinguishable by a joint measurement than by separate measurements.



Goldenberg - Vaidman (+Mor, Peres) interpretation BB84-type cryptography as a time-ordered presentation of two messages, the first of which must be read before the second (basis) is sent. This may be viewed as 4 orthogonal bipartite states, which cannot be distinguished if communication from Bob to Alice is forbidden.

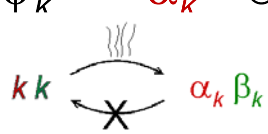
The 5 Pyramid States ψ_k of two qutrits, even though unentangled, are like Bell states in being orthogonal globally but not locally. If Alice and Bob are each given index k and told to prepare the k'th pyramid state, they can do so reliably, but the process is irreversible, generating waste heat if performed locally. If the preparation were carried out globally (by Alice and Bob getting together in the same lab) it would be thermodynamically reversible.





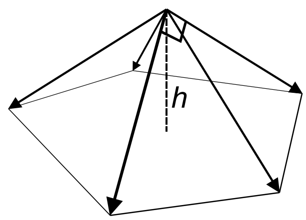
5 vectors in 3d real space form a regular pentagonal pyramid of such height such that every non-adjacent pair of vectors is orthogonal.

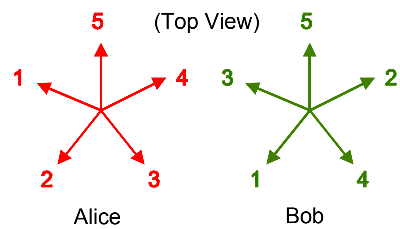
$$\psi_k = \alpha_k \otimes \beta_k$$



Nonlocality without Entanglement

The 5 Pyramid States ψ_k of two qutrits, even though unentangled, are like Bell states in being orthogonal globally but not locally. If Alice and Bob are each given index k and told to prepare the k'th pyramid state, they can do so without using entanglement or quantum communication, but the process is irreversible, generating waste heat if performed locally. If the preparation were carried out globally (by Alice and Bob getting together in the same lab) it would be reversible.

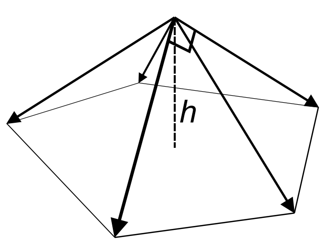


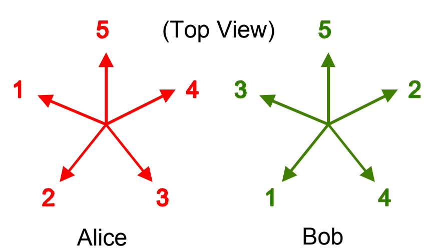


5 vectors in 3d real space form a regular pentagonal pyramid of such height such that every non-adjacent pair of vectors is orthogonal.

$$\psi_k = \alpha_k \otimes \beta_k$$

The 5 Pyramid States ψ_k form an "unextendible product basis", a set of 5 basis vectors in 9-dimensional Hilbert space, such that the complementary 4-dimensional subspace contains only entangled pure states, no product states. The mixed state uniformly distributed over this 4-dimensional subspace is a bound entangled sate, ie a mixed state from requiring entanglement to prepare, but from which no pure entanglement can be distilled.



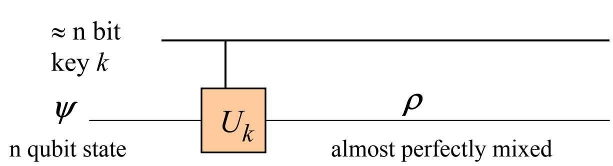


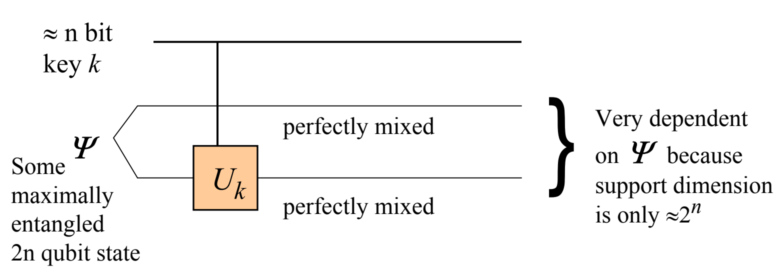
$$\psi_k = \alpha_k \otimes \beta_k$$

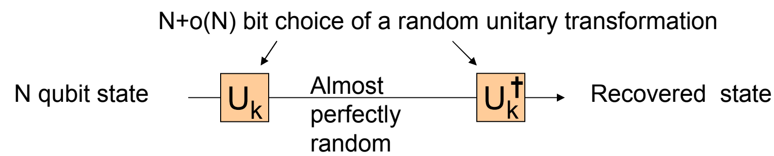
Walgate, Short, Hardy and Vedral (quant-ph/0007098) showed, remarkably, that *any two orthogonal pure states*, entangled or not, of *any number of parties* are reliably distinguishable by LOCC. Therefore, a classical bit cannot be even partly hidden from LOCC view in a choice between two pure states, however entangled. Mixed states must be used.

Quatum state tomography allows any state (pure or mixed, uni-partite or multipartite, product or entangled) to be identified by local measurements on a large n $\rightarrow \infty$ number of copies of the state. Therefore, globally distinct states cannot be made absolutely LOCC-indistinguishable. The best we can hope is to find globally distinguishable *mixed* states that are *arbitrarily close* to being LOCC-indistinguishable.

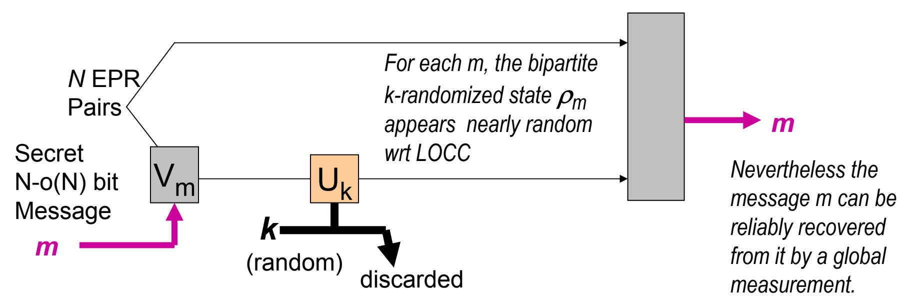
Approximate randomization, while hiding pure states almost perfectly, does not hide entangled states well at all. (Hayden, Leung, Shor, Winter 0307104)







This approximate randomization can be used for efficient data hiding

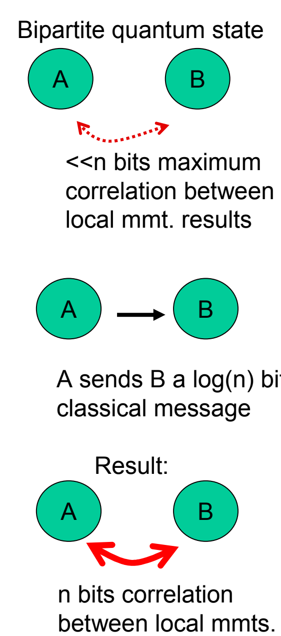


Unlocking Classical Correlations:

Alice and Bob share a mixed state ρ from which they can only recover a small amount of mutual classical information I by separate classical measurements on their parts (not full LOCC). The goal is for Alice to send Bob a small classical message that allows Bob to transform their joint state into another state ρ' from which a much larger amount of classical mutual information I' can be recovered by separate local measurements.

Such unlocking is classically impossible, but was found to hold for quantum states by DiVincenzo, M. Horodecki, Leung, Smolin, and Terhal quant-ph/0303088.

Using approximate randomization (0307100, 0307104) it can be made very efficient, obtaining simultaneously an arbitrarily large ratio of I' to I and to the size of the unlocking message.



Unlocking classical correlations using approximate randomization

$$\rho_{AB} = \frac{1}{dn} \sum_{i=1}^{d} \sum_{j=1}^{n} |ij\rangle\langle ij|_A \otimes (U_j|i\rangle\langle i|U_j^\dagger)_B$$

Alice takes a basis state $|\, \boldsymbol{i} >$ where $\boldsymbol{i}\ \varepsilon(1\ldots\boldsymbol{d})$, and locks it by applying a secret random unitary $\boldsymbol{U_j}$ where $\boldsymbol{j}\ \varepsilon\ (1\ldots\boldsymbol{n} \approx \log \boldsymbol{d})$, then sends the resulting randomized state $\boldsymbol{U_j}|\boldsymbol{i}>$ to Bob. But maybe it goes to Eve instead.

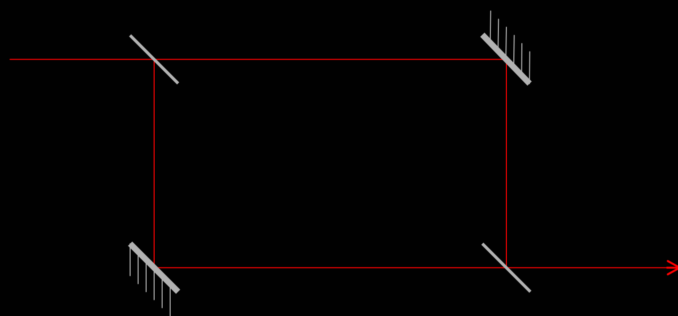
If Bob knows $\boldsymbol{j}$, he can discover $\boldsymbol{i}$ perfectly.

If Eve doesn't know $\boldsymbol{j}$, and also has no prior information on $\boldsymbol{i}$, she sees only the highly randomized state $\rho_{\boldsymbol{B}}$ from which she can recover only a little information about $\boldsymbol{i}$ by local measurement (0307104).

- More resource conversions
  - State Merging
  - Catalysis & Embezzling
- Degrees of knowledge of a quantum state
  - Impossibility of antiunitary transformation
  - Degrees of knowledge of a unitary transformation
  - Remote state preparation
  - When more words are needed to convey less information
- Nonlocal storage of classical information
  - Nonlocality without entanglement
  - Hiding classical data from LOCC prying
  - Unlocking classical correlations

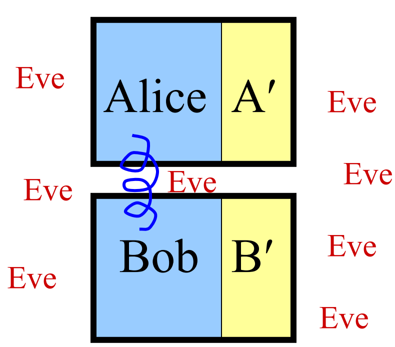
- Publicity and Privacy in the Quantum world and the Real World

Quantum information can be provisional



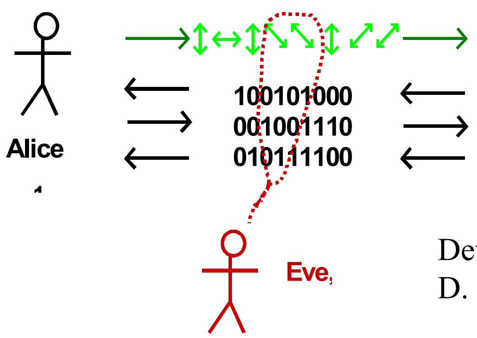
If no record is made of which path a photon follows through an interferometer, or if a record is made but then unmade, the photon will have followed a superposition of both paths.

An ebit of entanglement between Alice and Bob can be converted to a bit of shared secret key by local measurements.



but only if Alice and Bob can keep Eve out of their local environments A′ & B′

Conversely, standard non-EPR protocols for key distribution (eg BB84), when carried out coherently with the help of local environments well insulated from Eve, become protocols for entanglement sharing.



Devetak 0304127
D. & Winter 0306078

Private local environments can even help make key from non-distillable mixed states. To do so, Alice and Bob make local measurements but hold on to local "shield" subsystems which, if they fell into Eve's hands, would compromise the key.

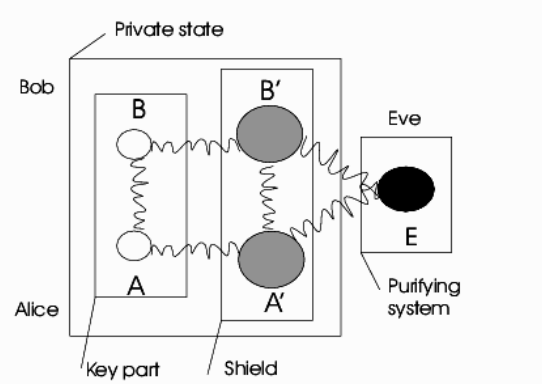


FIG. 1: A private state $\rho_{ABA'B'}$ with purifying system E. The "key part" (AB) after a complete von Neumann measurement gives an ideal key, which is secure due to the fact that Alice and Bob hold the "shield" part $(A'B')$.

Cf HHHO quant-ph/0309110, 0506189; HLLO 0510067

But as soon as Alice or Bob records a secret key bit generated by QKD in some macroscopic medium (eg hard disk or paper), it will begin to rapidly decohere relative to the environment outside their lab, just as Schrödinger's cat decoheres even before its box is opened.

This means the key is no longer absolutely secure. Eve might in principle learn it by doing an extremely difficult measurement on the surroundings of Alice’s or Bob’s lab.

Quantum test for the existence of God.

If someone (say Eve) comes to Alice and Bob claiming to be God, they should believe Her if She can repeatedly pass the following test:

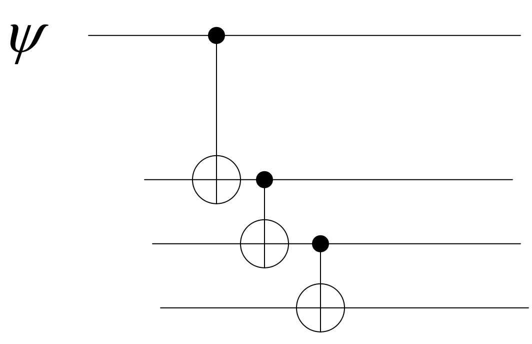
Alice and Bob each locally generate a random qubit, then ask “God” to predict which Bell state they hold. Alice and Bob then do a local or collective measurement to test whether the prediction is correct.

Thus there are 3 levels of privacy.

• **Quantum:** Information like the path taken in an interferometer, that exists only temporarily, and afterward can best be thought of as never having existed.

• **Classically Private:** Information that has been amplified to the point of becoming classical, and can recovered in principle, but not by humans with current technology. Humans can erase it, then lie about it with impunity, although perhaps not without guilt.

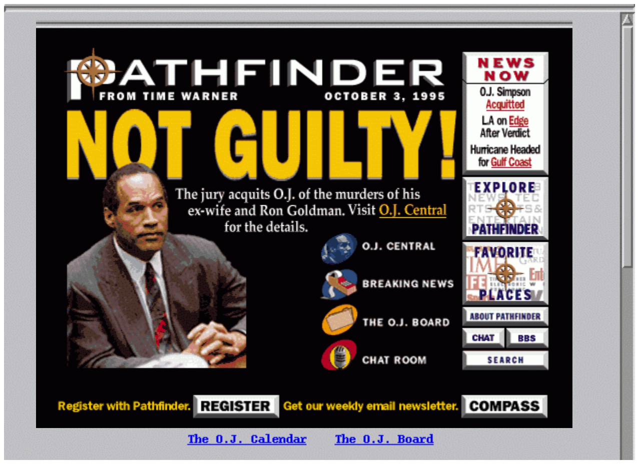
• **Public:** The cat is out of the bag. Trying to lie about it only makes you look foolish.



Environment: *Measured in 0/1 basis yields many redund-ant copies of system's infor-mation. In other bases it does not.*

Information becomes classical when it is replicated redund-antly throughout the environ-ment. "Quantum Darwinism"
B-K,Z quant-ph/0505031 etc.

The Internet has greatly increased the scope of public information, and helped make it impossible to retract.



In the practical tradeoff between Publicity and Privacy, digital technology has created a problem and an opportunity

Cheap, easy-to-use video cameras and cheap data storage leads to the temptation to record everything happening in public or even private places and save it forever, with ensuing loss of privacy, and potentially a loss of liberty if a latter-day J. Edgar Hoover gets hold of the data.

But these recordings are sometimes good, protecting human rights and promoting the rule of law. In many situations the bad guys want privacy for their misdeeds, while the good guys want publicity, with authenticity.

Maybe public policy should encourage citizens to make audiovisual recordings, but restrict how the recordings can legally be used (eg Yes for whistle blowing, No for blackmail).

Every citizen should carry a camera, not a gun.

It is tempting to believe that once information has become public, it can never be destroyed.

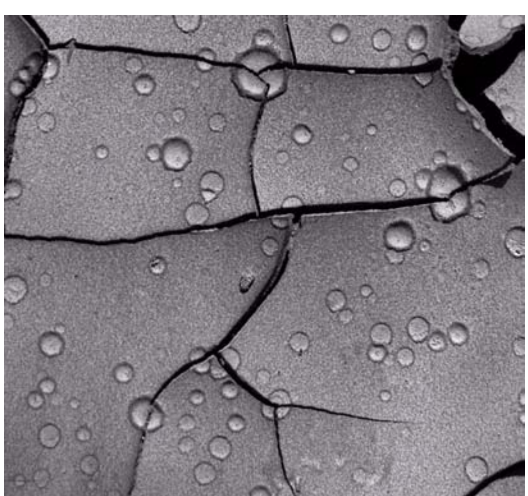
The modern world appears very different from ancient times, when major literary works once written down, performed, and widely known, were then lost.

"Since classical times, Sappho has been a source of fascination and romantic construction. The ancients, who had nine books of her poems at their disposal, were unstinting in their admiration…. It is difficult to judge her for ourselves when so little of her work remains. What we have consists on the one hand of quotations and more general references in ancient authors, and on the other hand of torn scraps from ancient papyrus and parchment copies…. Only twenty-one contain any complete stanzas; and only three – till now – gave us poems near enough complete to appreciate as literary structures.

"A recent find enables us to raise this number to four… This text, recovered from Egyptian mummy cartonnage, is the earliest manuscript of her work so far known. It was copied early in the third century bc, not much more than 300 years after she wrote."

[Martin West, Times Literary Supplement 24 June 2005]

But even in today's world, much macroscopic, publicly visible information is lost because no person, nor any natural process, happens to record it in a stable medium.



Raindrop marks in dried mud in a river bed in Las Vegas, USA in 1965.
A few days later these cracks and craters were washed away by a subsequent rain.

If no one had photographed them, would all record of them have been lost?

Still it is tempting to believe that such macroscopic information is not lost, just that it becomes so diffusely and complexly spread out as to be irrecoverable in practice but not in principle (just as when a book is burned its contents are in principle recoverable from the exact state of the smoke, ashes, and heat it generated).

Could it be that every major past phenomenon, say Sappho's other poems, or Jimmy Hoffa's murder, can be recovered from physical evidence in principle, if not in practice?

To believe otherwise is venturing dangerously close to the deconstructionist view, abhorred by most scientists, that history is not what "actually" happened, only what we think happened.

But I think some information is really lost, not from the universe but from the world (ie the planet Earth).

Why?

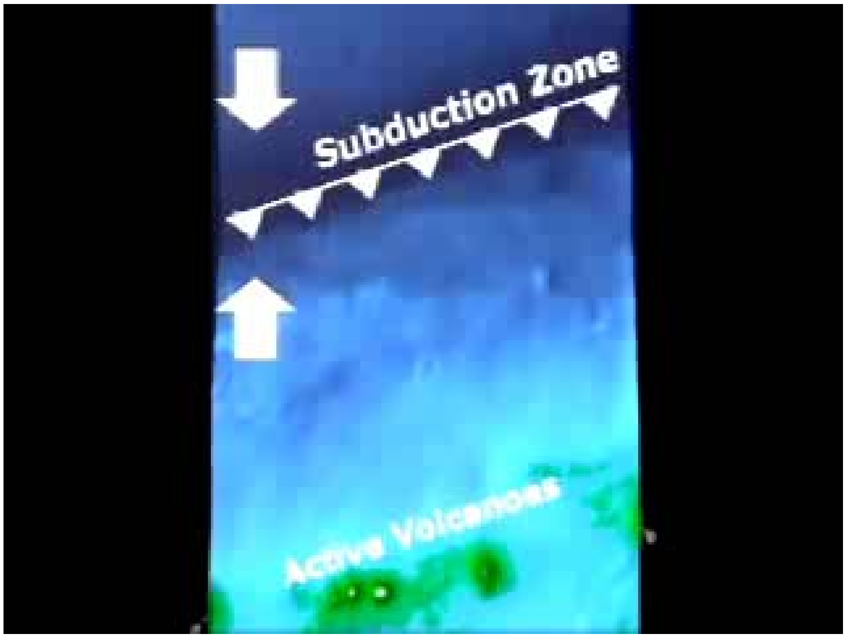
Because the world has finite memory capacity, but it exports a lot of randomness (generates a lot of entanglement with its environment, in the quantum way of speaking) in the form of thermal radiation into the sky.

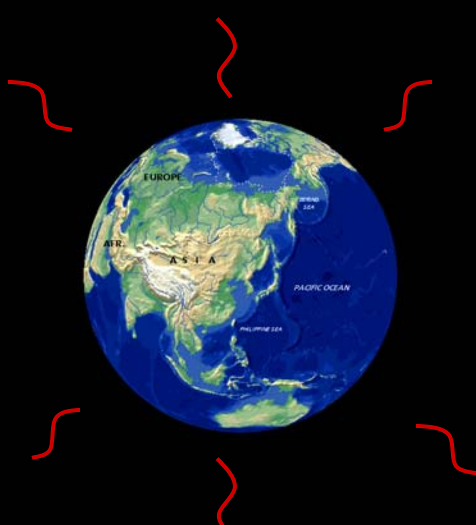
Thermal entropy export rate 100 watts/sq meter at 300K
= approx 10^{30} bits per square meter per year.

Geological information capture rate = crust thickness x rock information density / rock lifetime ≈ ≈ 10^{22} bits /square meter per year.

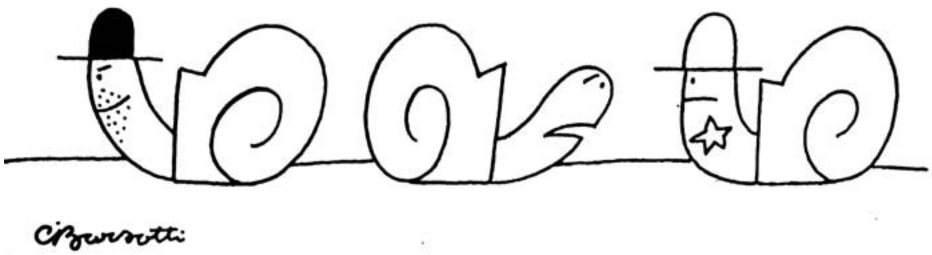
Human information capture rate in digital media ≈ ≈ 10^{21} bits per year

(for the whole world, not per sq meter)





To catch up with the thermal radiation leaving Earth, one would need to travel faster than light. So the information is still in the universe, but not recoverable by us, not even in principle.



"He's long gone, sheriff—you'll never catch him."

So now we add a new level of privacy.

- **Quantum:** Information like the path taken in an interferometer, that exists only temporarily, and afterward can best be thought of as never having existed.

- **Classical but Escaped:** Information that has been amplified to the point of becoming classical, but has escaped from Earth in thermal radiation. Humans have no way of recovering it even in principle.

- **Classically Private:** Information that has been amplified to the point of becoming classical, and still resides on earth in some form recoverable in principle, though not with current technology. Humans can erase it, then lie about it with impunity, although perhaps not without guilt.

- **Public and more or less permanent,** like quant-ph

Serious research needs to be done to better quantify these information flows, and especially to learn what determines the permanence or impermanence of various forms of macroscopic information

End