quantum laws

I. To each physical system there corresponds a Hilbert space [1] of dimensionality equal to the system's maximum number of reliably distinguishablee states. [2]

2. Each direction (ray) in the Hilbert space corresponds to a possible state of the system. [3]

3. Spontaneous evolution of an unobserved system is a unitary [4] transformation on its Hilbert space.

-- more --

1. A linear vector space with complex coefficients and inner product $<\phi|\psi> = \Sigma \phi_i^* \psi_i$

2. For polarized photons two, e.g. vertical and horizonal

$\leftrightarrow = \begin{pmatrix} 0 \\ 1 \end{pmatrix} \updownarrow = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$

3. E.g. for photons, other polarizations

$\nearrow = \begin{pmatrix} 1 \\ 1 \end{pmatrix} \searrow = \begin{pmatrix} +1 \\ -1 \end{pmatrix}$

$\circlearrowright = \begin{pmatrix} i \\ 1 \end{pmatrix} \circlearrowleft = \begin{pmatrix} i \\ -1 \end{pmatrix}$

4. Unitary = Linear and inner-product preserving.

4. The Hilbert space of a composite sysem is the tensor product of the Hilbert spaces of its parts. 1

5. Each possible measurement 2 on a system corresponds to a resolution of its Hilbert space into orthogonal subspaces $\{ \mathbf{P}_j \}$, where $\Sigma\, \mathbf{P}_j = 1$. On state ψ the result j occurs with probability $|\mathbf{P}_j\ \psi|^2$ and the state after measurement is

$$\frac{\mathbf{P}_j\, |\psi>}{|\mathbf{P}_j\, |\psi>|}$$

1. Thus a two-photon system can exist in "product states" such as $\leftrightarrow\leftrightarrow$ and $\leftrightarrow\ \swarrow\!\!\!\nearrow$ but also in "entangled" states such as

$$\frac{\leftrightarrow\leftrightarrow\ -\ \updownarrow\updownarrow}{\sqrt{2}}$$

in which neither photon has a definite state even though the pair together does

2 Believers in the "many worlds interpretation" reject this axiom as ugly and unnecessary. For them measurement is just a unitary evolution producing an entangled state of the system and measuring apparatus. For others, measurement causes the system to behave probabilistically and forget its pre-measurement state, unless that state happens to lie entirely within one of the subspaces $\mathbf{P}_j$.

Mixed States and Density Matrices

The quantum states we have been talking about so far, identified with rays in Hilbert space, are called *pure states.* They represent situations of minimal ignorance, where there is nothing more to know about the system. Pure states are fundamental in the sense that the quantum mechanics of any closed system can be completely described as a unitary evolution of pure states, without need of further notions. However, a very useful notion, the *mixed state*, has been introduced to deal with situations of greater ignorance, in particular

an ensemble $\mathcal{E}$ in which the system in question may be in any of several pure states ψ_1, ψ_2 ... with probabilities p_1, p_2....

a situation in which the system in question (call it *A*) is part of larger system *AB*, which itself is in an entangled pure state $\Psi(AB)$.

In open systems, a pure state may naturally evolve into a mixed state (which can also be described as a pure state of a larger system comprising the original system and its environment)

A mixed state is represented by a Hermitian, positive-semidefinite, unit-trace *density matrix*

$$\rho = \sum_i p_i \, | \psi_i \rangle\langle \psi_i | \qquad \text{for an ensemble}$$

$$\rho(A) = \mathrm{Tr}_B \, | \Psi(AB) \rangle\langle \Psi(AB) |$$

for a subsystem

($\rho = | \psi \rangle\langle \psi |$ for a pure state)

Different ensembles can have the same density matrix. For example any equal mixture of two orthogonal polarizations has

$\rho = \begin{pmatrix} 1/2 & 0 \\ 0 & 1/2 \end{pmatrix}$ What common feature does ρ represent?

Meaning of the Density Matrix

The density matrix represents *all and only* that information which can be learned by sampling the ensemble or observing the *A* part of the compound system. Ensembles with the same ρ are indistinguishable. Pure states $\Psi(AB)$ with the same $\rho(A)$ are indistinguishable by observing the *A* part.

If Alice and Bob share a system in state $\Psi(AB)$, then, for any ensemble $\mathcal{E}$ compatible with $\rho(A)$, there is a measurement Bob can do on his subsystem alone, which generates the ensemble, in the sense that the measurement yields outcome i with probability p_i , and, conditionally on that outcome having occurred, Alice's subsystem will be left in pure state ψ_i .

(Hughston-Jozsa-Wootters/Schroedinger theorem)

Schmidt Decomposition

Any pure state $\Psi(AB)$ of a bipartite system is expressible as

$$\Psi(AB) \;=\; \Sigma_i \;\lambda^{1/2} \,|\,\alpha_i\,\rangle\,|\,\beta_i\,\rangle\,,$$

where $|\,\alpha_i\,\rangle$ and$_i$ $|\,\beta_i\,\rangle$ are (orthogonal) eigenvectors

and λ_i the common eigenvalues of the density matrices $\rho(A)$ and $\rho(B)$ obtained by tracing out subsystem B or A respectively. (Not generally true for tripartite and higher)

Corollary: any two pure states of the *AB* system having the same $\rho(B)$ are interconvertible by a unitary transformation acting on system *A* alone. (important for Bit Commitment No-Go theorem)

The degree of ignorance embodied in a mixed state is represented by its

von Neumann entropy

$$S(\rho) \;=\; -\,\mathrm{Tr}\;\rho\;\log\rho.$$

= Shannon entropy of eigenvalues of ρ

For an ensemble $\{\,p_i\,,\,\psi_i\}$ the von Neumann entropy is $\leq$ the Shannon entropy of the probabilities p_i, equality holding iff the states are orthogonal.

When a pure state ψ is degraded by noise, the result is a mixed state ρ. The degree resemblence or *fidelity* of ψ to ρ is

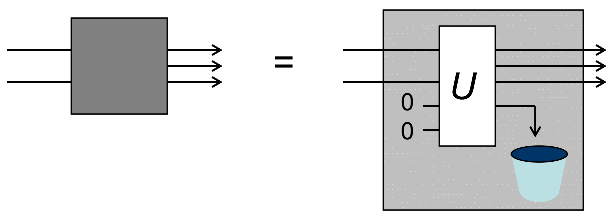
$$F \;=\; <\psi\,|\,\rho\,|\psi>$$

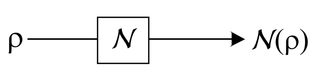
Unitary evolution is reversible, preserving distinguishability.

But quantum systems in interaction with an environment can undergo irreversible loss of distinguishability.

- noisy or lossy channels, which lose classical information
- classical wires, which spoil superpositions
- erasure, which destroys distinguishability completely

Any physically possible evolution of an open quantum system can be modeled as a unitary interaction with an environment, initially in a standard 0 state.



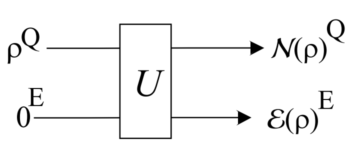


$$\mathcal{N}(\rho) = \Sigma_k\ A_k\ \rho\ A_k^\dagger$$

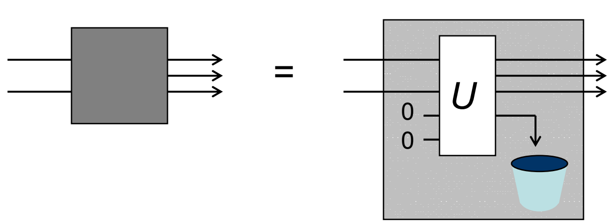
where A_k are matrices such that

$$\Sigma_k A_k^\dagger A_k = 1$$

Kraus representation.



Unitary representation.

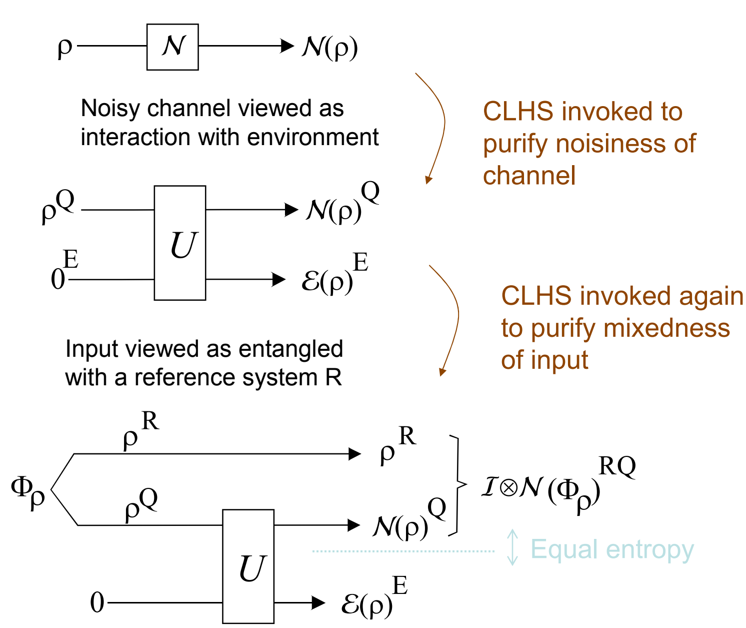


The Church of the Larger Hilbert Space

This is the name given by John Smolin to the habit of always thinking of a mixed state as a pure state of some larger system; and of any nonunitary evolution as being embedded in some unitary evolution of a larger system: No one can stop us from thinking this way; and Church members find it satisfying and helpful to their intuition:

This doctrine only makes sense in a quantum context, where because of entanglement a pure whole can have impure parts: Classically; a whole can be no purer than its most impure part.

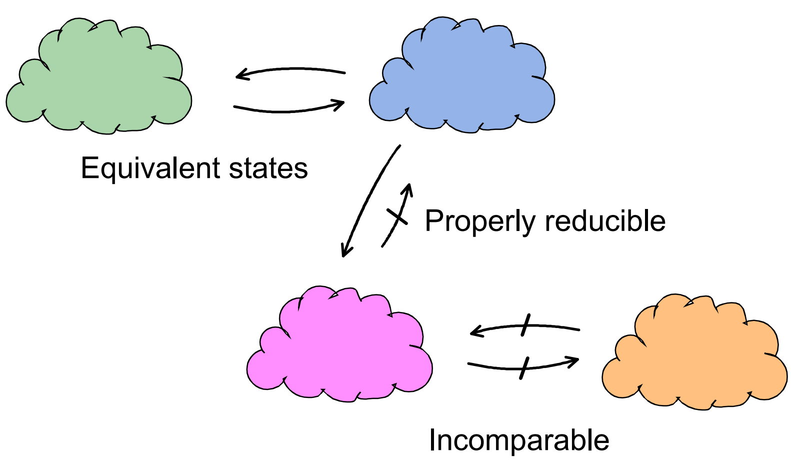
Cf. Biblical view of impurity (Matthew 18:8)
If thy hand or thy foot offend thee, cut them off, and cast them from thee: it is better for thee to enter into life halt or maimed, rather than having two hands or two feet to be cast into everlasting fire.



Church of the Larger Hilbert Space

Its teachings were anticipated by those of the actual Unitarian Church, as expressed in an unofficial but well known poem and logo.

He drew a circle that shut me out,
Heretic, rebel, a thing to flout.
But love and I had the wit to win.
We drew a circle that took him in.
--Edwin Markham (1852-1940)



Reversible and irreversible transformations of quantum states (eg under Local Operations and Classical Communication) (entanglement is sexy) $\wedge$ (sex is risky) $\Rightarrow$

Entanglement Gambling, ie

Sometimes getting a good EPR pair out of a slightly entangled pair (but sometimes losing it)

HH + VV

HH + vv

HH + vv

HH + VV

HH

Alice tries to pass her (red) photon through a Brewster window (which selectively reflects H photons with some probability). If the photon gets through, both parties are left with the desired HH+VV ; otherwise they are left with the unentangled state HH.

Measures of entanglement of bipartite pure state Ψ

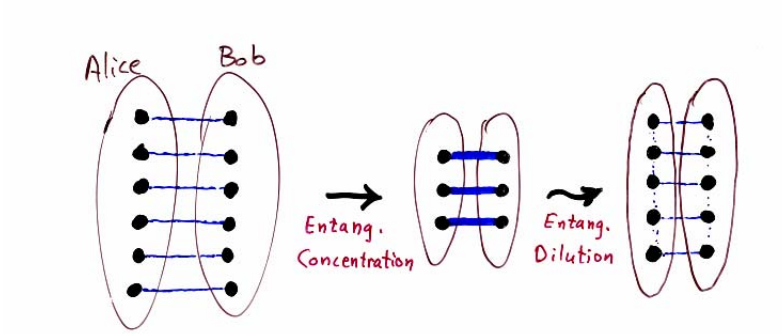
- Schmidt Rank (the number of nonzero Schmidt coefficients) is conserved by gambling, when it succeeds.

- Entropy of Entanglement $E(\Psi)$, the local entropy of either party, is asymptotically conserved in entanglement concentration and dilution

E.g. for $\Psi = \alpha HH + \beta VV$, $\quad E(\Psi) = H(|\alpha|^2, |\beta|^2)$.

For large n, n copies of Ψ can be created from $n\,E(\Psi) + o(n)$ EPR pairs, and can be converted into $n\,E(\Psi) - o(n)$ EPR pairs.

Entanglement Concentration and Dilution



Entanglement Concentration (the large *n* limit of entanglement gambling) is exact and requires no communication.

Entanglement Dilution requires $O(\sqrt{n})$ one way classical communication, and yields the desired diluted state in the limit of large *n.*

Entanglement Concentration

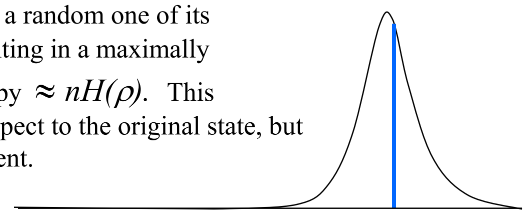
Let $\Psi^n=(HH+vv)^n$ be shared between Alice & Bob

Alice measures how many H's she has, but not in which positions. Suppose she gets the result k. This result will be binomially distributed. (If Bob measured, he would get the same k, through the magic of entanglement.) The residual state after measuring k is a maximally entangled state with (n choose k) equal terms, which can be converted into about $nE(\Psi)$ EPR pairs.

Entanglement Dilution: Alice makes the state Ψ^n locally in her lab. She Schumacher-compresses one side of it and teleports it to Bob using about $nE(\Psi)$ EPR pairs. He then decompresses it. Other techniques use less classical communication.

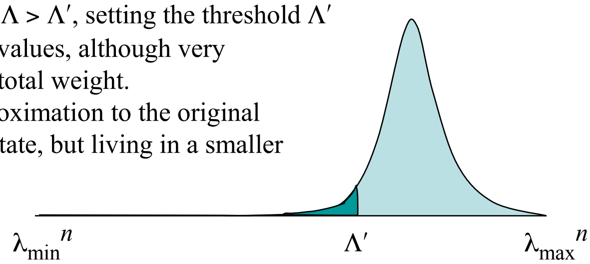
Entanglement Concentration

Projects local state $\rho^{\otimes n}$ into a random one of its degenerate eigenspaces, resulting in a maximally entangled state of local entropy $\approx nH(\rho)$. This state has low fidelity with respect to the original state, but retains most of its entanglement.

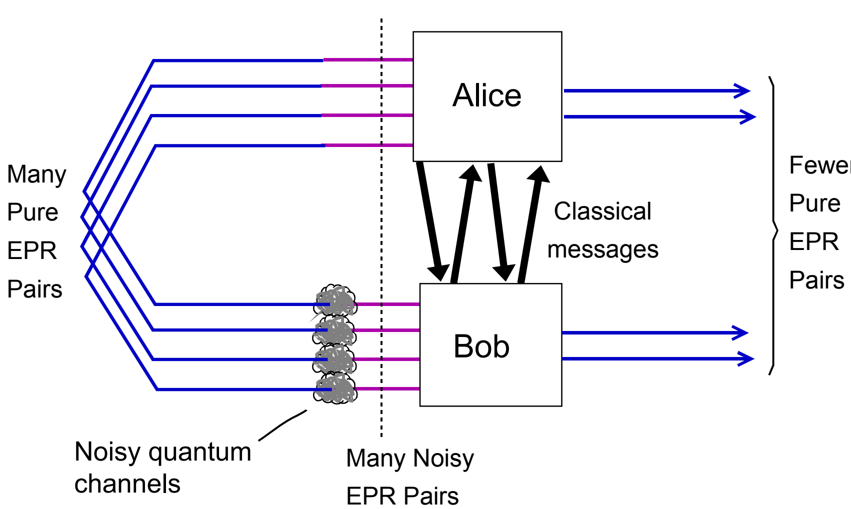


Schumacher Compression

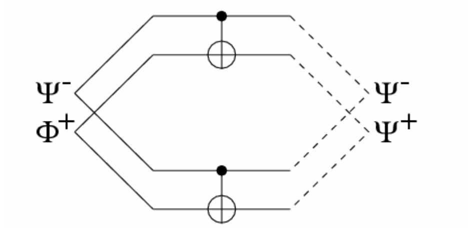
Projects state $\rho^{\otimes n}$ into subspace spanned by its Schmidt eigenvectors of eigenvalue $\Lambda > \Lambda'$, setting the threshold Λ' so that the remaining eigenvalues, although very numerous, have negligible total weight.
Result: a high-fidelity approximation to the original non-maximally entangled state, but living in a smaller Hilbert space of dimension
$\approx 2^{nH(\rho)}$



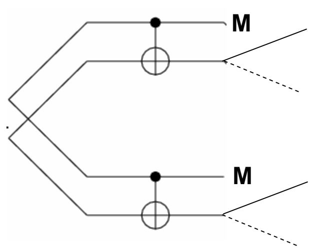
Entanglement Distillation



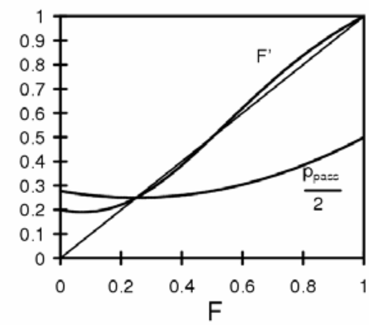
Two-way distillation for Bell pairs “recurrence method”



Phase (Ψ/Φ) gets XORed upward
Amplitude (–/+) gets XORed down

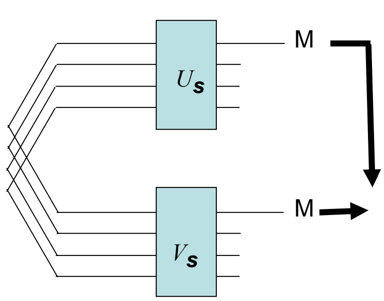


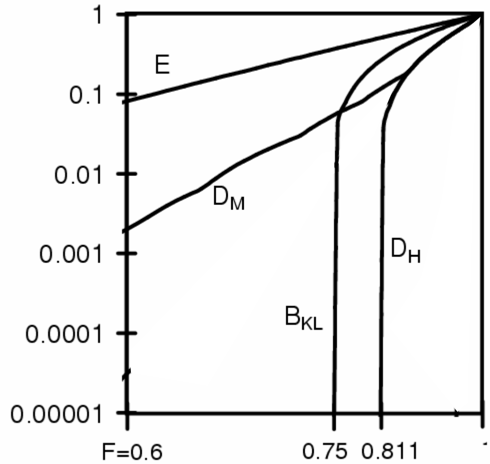
Keep remaining pair if measurement results agree; discard it if they disagree



One-way distillation by random Hashing

An unknown state of N Bell pairs is characterized by a distribution over 2N bit strings ***x***.
To get a random subset parity ***s.x*** of this string, local operations are performed, then a single pair is measured, and from the results of the measurement, half the candidates for the remaining unmeasured pairs can be excluded. Method gives positive yield if initial Bell mixture has entropy less than 1 bit.





Entanglement Measures for Mixed States

Entanglement Cost or asymptotic entanglement of formation E_C
The asymptotic efficiency with which singlets can be converted into the state in question, using LOCC.

Distillable Entanglement E_D
The asymptotic efficiency with which the state in question can be converted into singlets, using LOCC.

For Pure Bipartite States, $E_D = E_C$, and the amount of classical communication per state prepared tends to zero in the limit of large *n*.

For Mixed States, E_D can be less than E_C. Indeed some mixed states (called **bound entangled** states) have zero distillable entanglement but positive entanglement of formation.

Recognizing Entanglement

$$\rho \longrightarrow \boxed{\mathcal{N}} \longrightarrow \mathcal{N}(\rho)$$

Channels map density matrices onto density matrices in a linear fashion.

Are all such positive maps physically possible?

No. Consider the transpose. It maps density matrices onto density matrices, but when applied to part of a bipartite system, in an entangled state, produces a nonphysical matrix with negative eigenvalues.

$$\begin{matrix} 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 \end{matrix} \quad \text{partial transpose} \Rightarrow \quad \begin{matrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{matrix}$$

EPR state with eigenvalues (1,0,0,0)

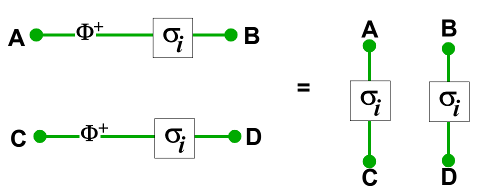
Nonphysical eigenvalues (-1/2,1/2,1/2,0)

Negativity of partial transpose is a *sufficient* condition for a mixed state to be entangled (Peres-Horodecki condition).

Strange Things you can do with Multipartite Entanglement

"Unlock able" 4 party BE state ρ (Smolin 0001001)

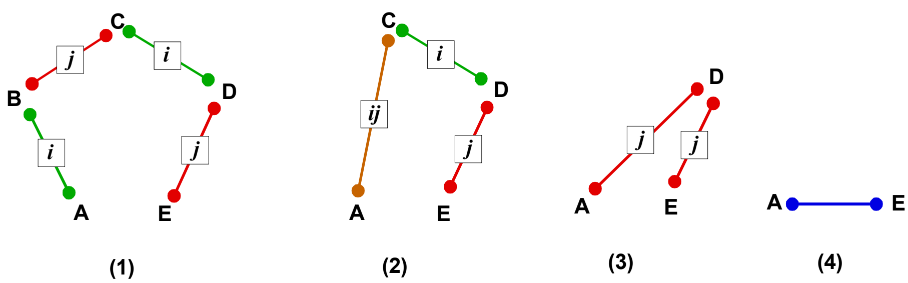
A & **B** share a random Bell state; **C** & **D** share the same random Bell state



(ρ is symmetric among all 4 parties. Therefore it is not distillable across any 2:2 boundary, and certainly not distillable in its original 1:1:1:1 form)

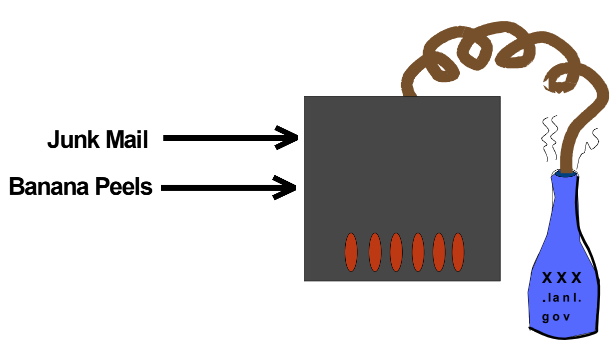
To **unlock** the state, **A** and **B** get together in the same lab, measure their Bell state, and tell **C** the result i. **C** then performs σ_i thereby restoring the Bell state between **C** and **D** to standard Φ^+ form. This shows the original state ρ must have had at least 1 ebit of entanglement of formation across the **ABC:D** boundary (otherwise **A, B,** and **C,** even by coming together, could not have distilled an ebit between themselves and **D**). Similarly for all other 3:1 boundaries.

"Superactivation" of Bound Entanglement: two non-distillable states ρ^{ABCD} and ρ^{BCDE} can be combined to form a distillable state $\rho^{ABCD} \otimes \rho^{BCDE}$.

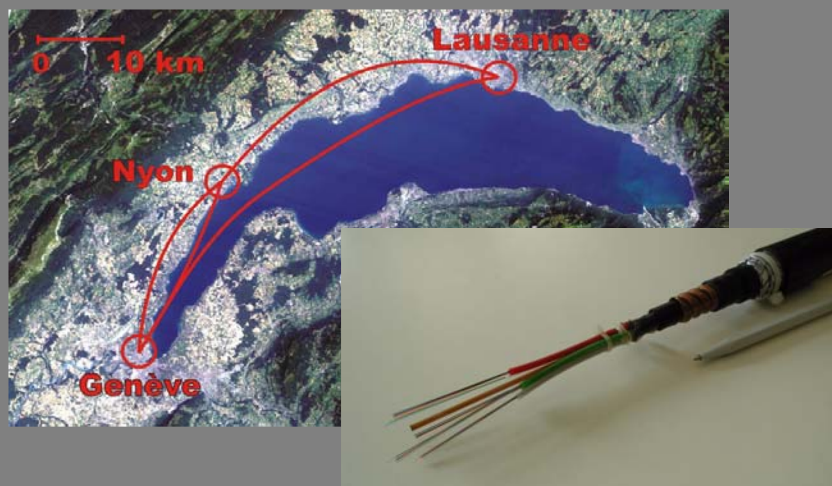


Starting state $\rho^{ABCD} \otimes \rho^{BCDE}$ is shown in **(1)**.
To distill an ebit from this state**, B** uses the **BC** EPR pair to teleport his half of the **AB** pair to **C.** This results in configuration **(2),** where **B** is gone and **AC** share a new ij-rotated EPR pair (brown). Next **C** uses the **CD** pair (green) to teleport her end of this new AC pair to **D.** This cancels the i rotation, leaving only a j rotation in the resulting **AD** pair **(3)**. Finally **D** teleports his half of the **AD** pair to **E**, resulting in an **AE** pair in which all rotations have been canceled (4)
(Smolin, Shor, Thapliyal 0005117).

This shows that distillable entanglement is not *additive.* In fact it is not even *convex,* since one can mix two nondistillable states and get a distillable state as the result. Let $\mu_0 = |0\rangle\langle 0| \otimes \rho^{ABCD}$ and $\mu_1 = |1\rangle\langle 1| \otimes \rho^{BCDE}$, and let μ be an equal mixture of μ_0 and μ_1. Here the first tensor factor is an extra flag qubit (wlog given to Alice), which enables her to determine (and tell the other parties) which of μ_0 or μ_1 is present in a given specimen of μ. By measuring the flag qubit on several specimens of μ, the parties can, with high probability accumulate a known specimen each of ρ^{ABCD} and ρ^{BCDE}, from which a pure ebit can be distilled by LOCC.



Quantum Cryptography



Quantum Cryptographic Key Distribution (BB84 Protocol)

Alice Sends random Photons	↕ ↔ ↕ ⤡ ⤡ ↕ ⤢ ⤢ ↕ ↔ ↕ ⤢ ⤡ ↕ ⤢ ⤢ ↕ ⤡ ⤡
Bob Measures on random Axes	+ x + + x x + x x + + x ++ + x x x x
Bob's Measurement Results	↕ ⤢ ↕ ↔ ⤡ ↕ ⤢ ⤢ ↕ ⤢ ↕ ↕ ↔ ⤢ ⤢ ⤡ ⤡
Bob reports axes he used	" + x + + x + x x + x ++ + x x x x"
Alice says which were right	" + + x + x + x x x"
Photons Alice & Bob should agree on (if no eavesdropping)	↕ ↕ ⤢ ↕ ⤢ ↕ ⤢ ⤡ ⤡
Bit Values of Photons	1 1 0 1 0 1 0 1 1
Alice Announces Parities of a few Random Subset of the Bits and Bob verifies that they are correct.	1 1 0 1 0 1 0 1 1 "Odd" "OK" 1 1 0 1 0 1 0 1 1 "Even" "OK"
Remaining Shared Secret Bits	0 1 0 1 0 1 1

Data Reconciliation
Alice and Bob start with *N* bit strings $\boldsymbol{x}_A$, $\boldsymbol{x}_B$
which agree in most positions

They publicly chooses a random index string $\boldsymbol{s}$

They calculate and publicly compare parities $\boldsymbol{s}\cdot\boldsymbol{x}_A$, $\boldsymbol{s}\cdot\boldsymbol{x}_B$

Each comparison gives Bob and Eve 1 bit of information about Alice's string $\boldsymbol{x}_A$.

Privacy amplification
When Bob thinks he knows $\boldsymbol{x}_A$ they do a few more comparisons, they estimate Eve's partial knowledge, including what she may have gained from eavesdropping, pulse-splitting, and listening to the reconciliation. Suppose it is estimated to be less than *K* bits. They calculate *N-K-m* further random subsets as their final key. Eve expected information on it is exponentially small in the security parameter *m*.

Sources of information for Eve

Eavesdropping

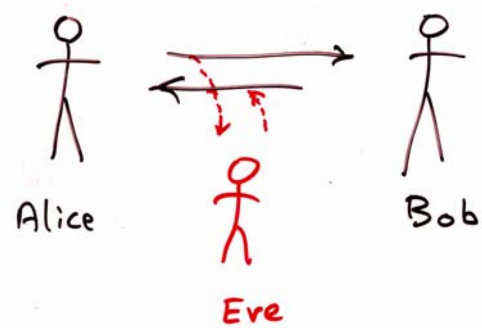
Pulse-splitting or photon number splitting PNS

Listening to reconciliation

Remedies for Pulse Splitting:

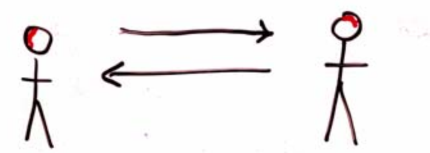
Single Photon Sources
Bright/Dim coherent pulse method
Decoy states

Key Distribution is
Cold War era
cryptography.
The good guys trust
each other and know
who the bad guy is.

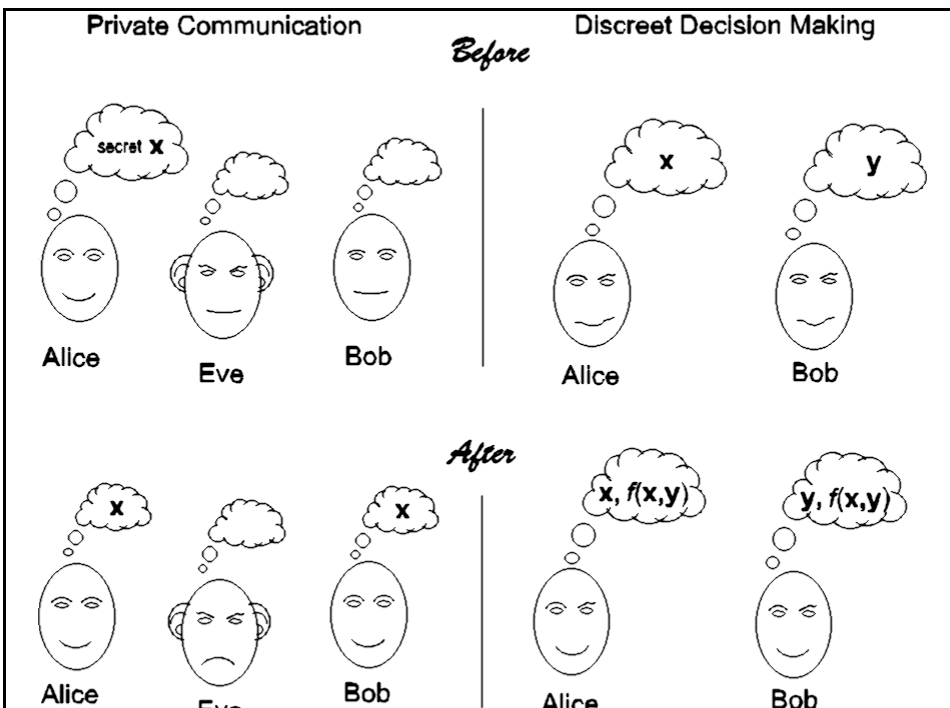


2 Good Guys and 1 Bad Guy

Often today, especially in the business world, there is no bad guy per se. But, human nature being what it is, the good guys don't trust each other. Nevertheless they must cooperate and make joint decisions. But they wish to do so circumspectly, as if they were dealing through a trusted intermediary. Of course there is no one they trust well enough to hire for that job. What to do? .



2 Good Guys who don't trust each other



Simple examples of Discreet 2-Party Tasks

Dating problem = Logical AND of Alice's bit x and Bob's bit y. Alice and Bob want to go out together if both are willing, while minimizing the hurt feelings in case only one is willing. If they use a trusted intermediary, and only Alice is willing, the date is off, but Alice is spared the embarrassment of having Bob learn that she wanted it. Of course there is no way to spare her the disappointment of learning that Bob didn't want it, since she can infer that from her input and the common output.

Bit Commitment: Alice wishes to send Bob a bit of her choosing but in a form he cannot read. Then, later, at a time of her choosing, she wishes to enable Bob to read the bit. Between these two times, Bob should be unable to read the bit, and Alice should be unable to change it. A concrete example would be sending Bob a locked box containing the bit, then later sending the key. Mayers and Yao showed that a secure bit commitment, if it existed, could be combined with other quantum primitives to calculate any function of two inputs discreetly. Unfortunately there is no secure bit commitment..

BB84 Bit Commitment, and how to Cheat

To commit to 0(1) Alice sends *n* random +(x) photons	↕ ↔ ↕ ↕ ↔ ↔ ↕ ↕ ↔ ↕ ↕ ↕
Bob measures in random bases, getting results:	x + + x + x x + x x + +
	⤡ ↔ ↕ ⤢ ↔ ⤢ ⤢ ↕ ⤡ ⤢ ↕ ↕

To open her commitment, Alice announces all her polarizations	“ ↕ ↔ ↕ ↕ ↔ ↔ ↕ ↕ ↔ ↕ ↕ ↕ ”

Bob thinks she's telling the truth, because her photons agree with all his + measurement results, and are uncorrelated with his x measurement results.

Instead of + or x photons, Alice actually sent n halves of EPR pairs, saving the other halves in her laboratory.

Bob measures in random bases, getting random results:

x + + x + x x + x x + +

⤢ ↕ ↔ ⤢ ↕ ⤢ ⤢ ↕ ⤡ ⤡ ↕ ↔

To open her "commitment" as a 0, Alice measures the saved halves in the + basis, obtaining data perfectly correlated with the Bob's + measurements. She announces, e.g.

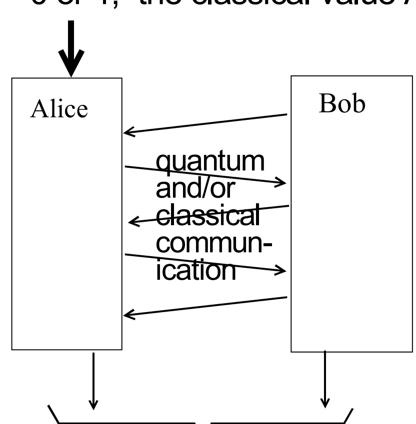
"⤢ ↕ ↔ ⤡ ↕ ⤢ ⤡ ↕ ⤡ ⤢ ↕ ↔"

To open her "commitment" as a 1, Alice measures the saved halves in the x basis, obtaining data perfectly correlated with the x measurements. She announces, e.g.

"⤢ ↔ ↕ ⤢ ↕ ⤢ ⤢ ↕ ⤡ ⤡ ↔ ↕"

Mayers' No-Go theorem for quantum bit commitment

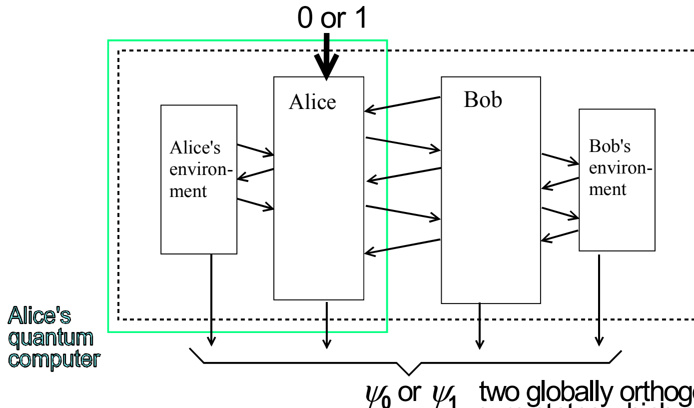
0 or 1, the classical value Alice commits to



Stage at which commitment has been made but not yet opened

ρ_0 or ρ_1 two globally orthogonal joint states which should look the same to Bob.

Go to the "Church of the Larger Hilbert Space" by including Alice's and Bob's environments.
Now all operations are unitary, all communications are quantum and all states are pure.



Honest protocol is a global unitary known to both parties.

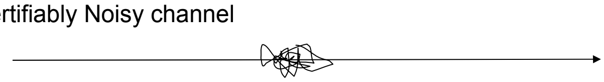
two globally orthogonal pure states which are known to both parties and which look the same to Bob.

Honest protocol outcomes are therefore related by a unitary transformation on Alice's side alone, so if Bob plays honestly, Alice can initially make a "commitment" to ψ_0 and then later unilaterally change it to ψ_1 without Bob's knowledge or cooperation!

Other ways of obtaining bit commitment

Adrian Kent's relativistic method quant-ph/9906013 v6

Certifiably Noisy channel



Reference Frame uncertainty HOT'05