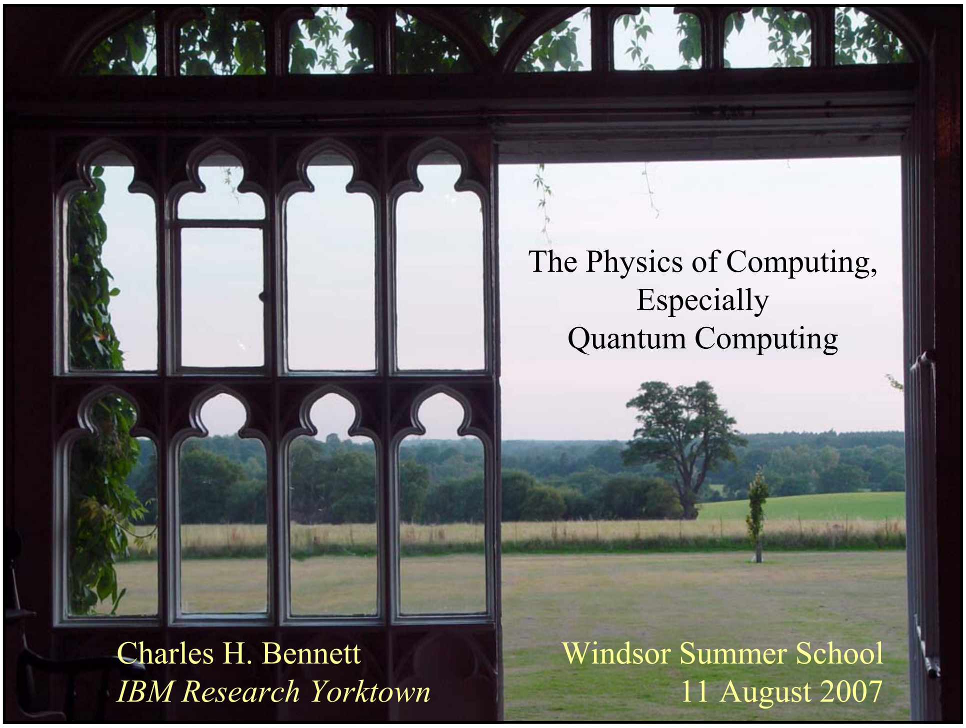
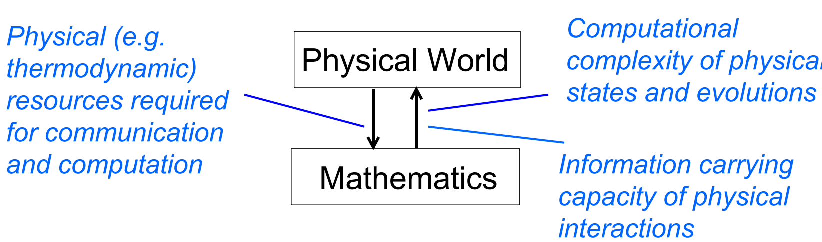


"Information is Physical" Rolf Landauer

"It from bit" John Archibald Wheeler



When Turing, Shannon, von Neumann and their contemporaries formalized the notions of information and computation, they forgot about the reversibility and the superposition principle

reversibility => thermodynamics of computation

superposition => quantum information/computation theory.

Information = Distinguishability,
considered as an abstract property separate from the physical information carrier.
(Using a pencil, a piece of paper can be put into various states distinguishable at a later time.)

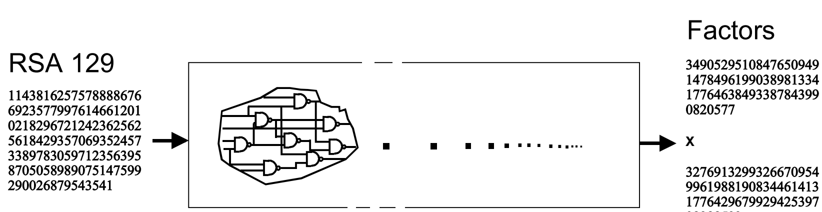
- Information is reducible to bits (**0** ,**1**)

- Information processing, to reveal implicit truths, can be reduced to logic gates (**NOT**, **AND**)

- bits and gates are *fungible*, independent of physical embodiment, making possible Moore's law

We take for granted that information
- can be copied without disturbing it
- cannot travel faster than light
- can be erased when no longer wanted

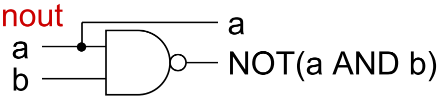
Classical Computation Theory shows how to reduce all computations to a sequence of NANDs and Fanouts. It classifies problems into solvable and unsolvable, and among the solvable ones classifies them by the resources (e.g. time, memory, luck) required to solve them. Complexity classes P, NP, PSPACE…



Some computations require a great many intermediate steps to get to the answer. Factoring large integers is in NP but believed not to be in P.

Conventional computer logic uses irreversible gates, eg NAND, but these can be simulated by reversible gates. Toffoli gate is universal.

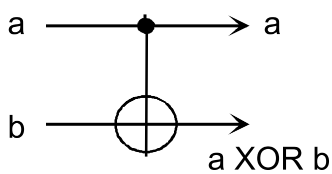
Fanout



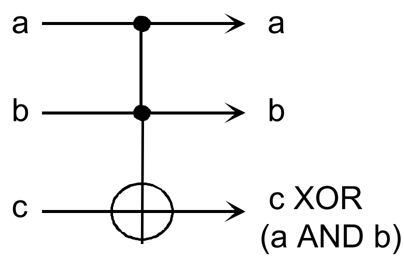
NAND gate

no inverse

Reversible logic was used to show that computation is thermodynamically reversible in principle. Now it is needed for quantum computation.



XOR gate



Toffoli gate

self-inverse

Logical Reversibility and Thermodynamics

• Landauer Principle: each erasure of a bit, or other logical 2:1 mapping of the state of a physical computer, increases the entropy of its environment by k log 2.

• Reversible computers, which by their hardware and programming avoid these logically irreversible operations, can in principle operate with arbitrarily little energy dissipation per step.

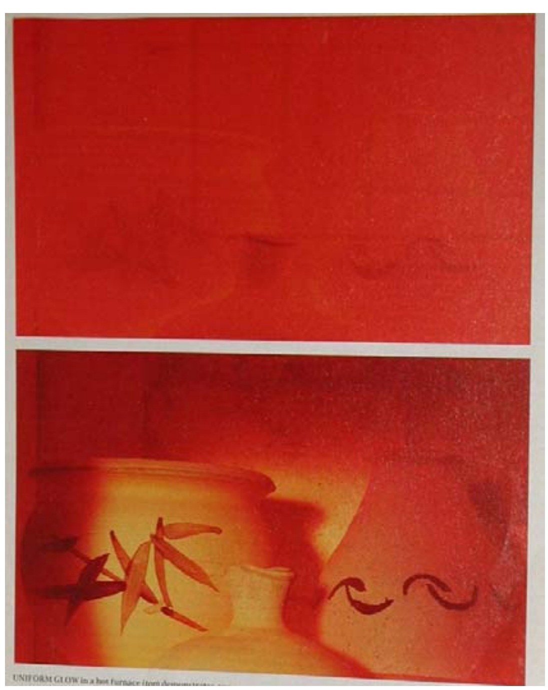
Avatars of the Second Law of Thermodynamics:

No physical process has as its sole result is the conversion of heat into work.

It is impossible to extract work from a gas at constant volume if all parts are initially at the same temperature and pressure.

It is impossible to see anything inside a uniformly hot furnace by the light of its own glow.

No process has as its sole result the erasure of information.



Ordinary irreversible computation can be viewed as an approximation or idealization, often quite justified, in which one considers only the evolution of the computational degrees of freedom and neglects the cost of exporting entropy to the environment.

We will return to this later.

A bigger change of mindset: Quantum Information

Information in microsopic bodies such as photons or nuclear spins obeys quantum laws. Such information

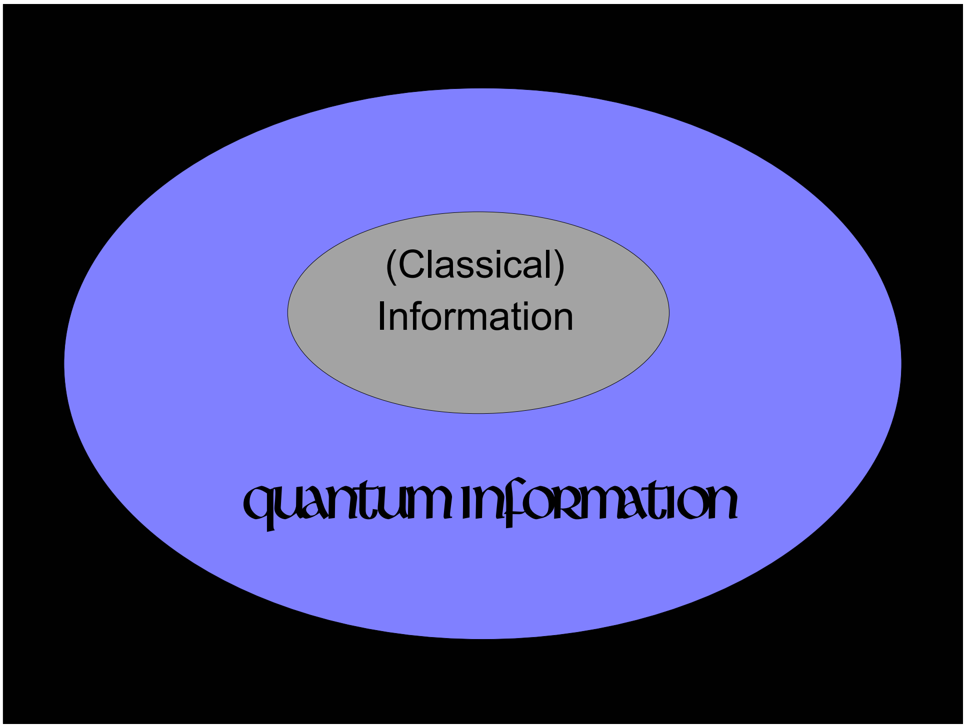
- cannot be read or copied without disturbance.

- can connect two spacelike separated observers by a correlation too strong to be explained by classical communication. However, this "entanglement" cannot be used to send a message faster than light or backward in time.

Quantum information is reducible to **qubits** i.e. two-state quantum systems such as a photon's polarization or a spin-1/2 atom.

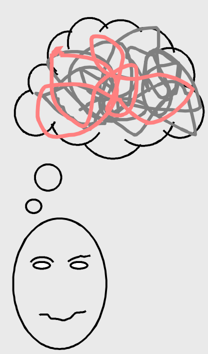
Quantum information processing is reducible to one- and two-qubit gate operations.

Qubits and quantum gates are fungible among different quantum systems



Ordinary classical information, such as one finds in a book, can be copied at will and is not disturbed by reading it.

Quantum information is more like the information in a dream



• Trying to describe your dream changes your memory of it, so eventually you forget the dream and remember only what you've said about it.

• You cannot prove to someone else what you dreamed.

• You can lie about your dream and not get caught.

But unlike dreams, quantum information obeys well-known laws.

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.

quantum laws

I. To each physical system there corresponds a Hilbert space **1** of dimensionality equal to the system's maximum number of reliably distinguishable 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 --

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 $\leftrightarrow\nearrow$ 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 $\mathbf{P}_j$.

superposition principle

Between any two reliably distinguishable states of a quantum system

(for example vertically and horizontally polarized single photons)

there exists other states that are not reliably distinguishable from either original state

(for example diagonally polarized photons)

A historical question:

Why didn't the founders of information and computation theory (Turing, Shannon, von Neumann, et al) develop it on quantum principles from the beginning?

Maybe because they unconsciously thought of information and information processing devices as macroscopic. They did not have before them the powerful examples of the genetic code, the transistor, and the continuing miniaturization of electronics.

But even in the 19th Century, some people thought of information in microscopic terms
(Maxwell's Demon 1875)

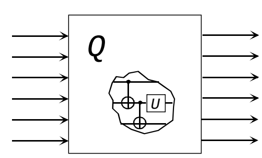
Perhaps more important (Nicolas Gisin)

Until recently, most people, under the influence of Bohr and Heisenberg, thought of quantum mechanics in terms of the uncertainty principle and unavoidable limitations on measurement. Schroedinger and Einstein understood early on the importance of entanglement, but most other people failed to notice, thinking of the EPR paradox as a question for philosophers. Meanwhile engineers thought of quantum effects as a nuisance, causing tiny quantum devices to function unreliably. The appreciation of the positive application of quantum effects to information processing grew slowly.

First: Quantum cryptography - use of uncertainty to prevent undetected eavesdropping

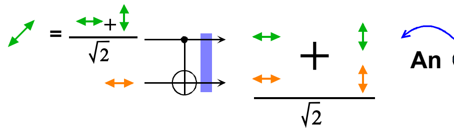
Now: Fast quantum computation, teleportation, quantum channel capacity, quantum distributed computation, quantum game theory, quantum learning theory, quantum economics, quantum voting…

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

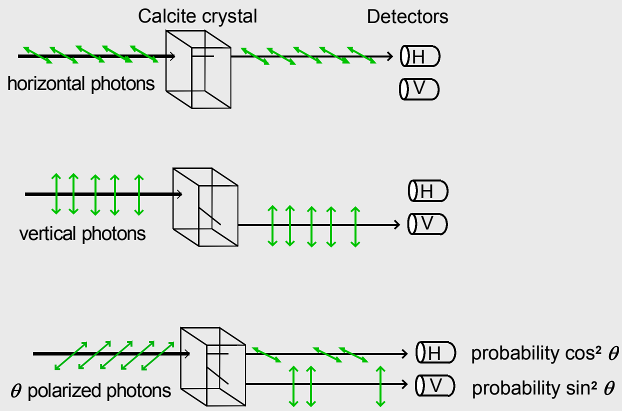


The 2-qubit XOR or "controlled-NOT" gate flips its 2nd input if its first input is 1, otherwise does nothing.

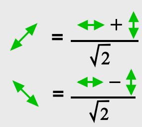
A superposition of inputs gives a superposition of outputs.



An entangled or EPR state

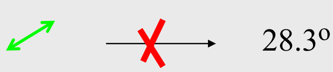


(Mathematically, a superposition is a weighted sum or difference, and can be pictured as an intermediate *direction* in space)

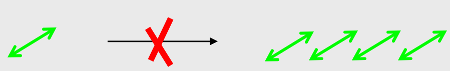


Non-orthogonal states like ↔ and ⤢ are in principle imperfectly distinguishable. ↔ always behaves somewhat like ⤢ and vice versa. This is the basis of quantum cryptography.

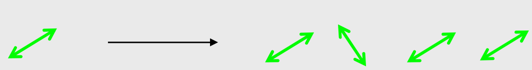
Measuring an unknown photon’s polarization exactly is impossible (no measurement can yield more than 1 bit about it).



Cloning an unknown photon is impossible. (If either cloning or measuring were possible the other would be also).

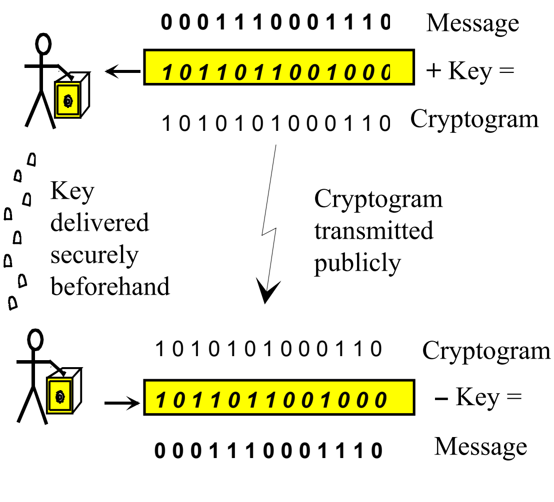


If you try to amplify an unknown photon by sending it into an ideal laser, the output will be polluted by just enough noise (due to spontaneous emission) to be no more useful than the input in figuring out what the original photon’s polarization was.

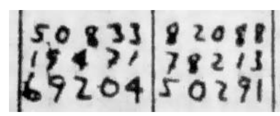


Cryptography: the One Time Pad

allows messages to be transmitted in absolute privacy over public channels, but requires the sender and receiver to have shared secret random data ("key") beforehand. One key digit is used up for each message digit sent. The key cannot be reused. If it, system becomes insecure.

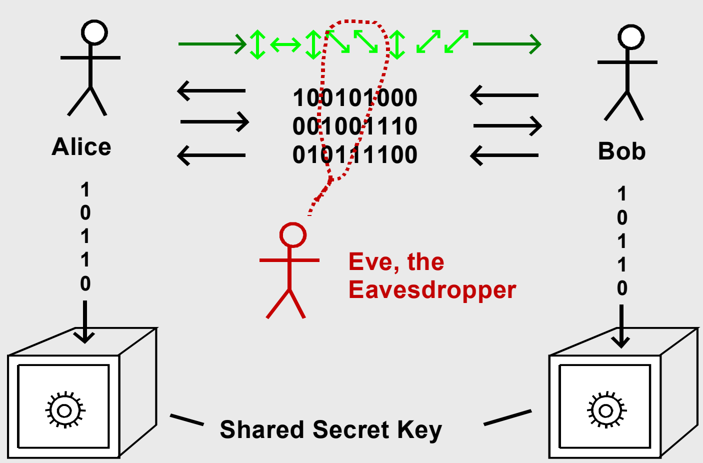


One time pad worksheet used by Che Guevara

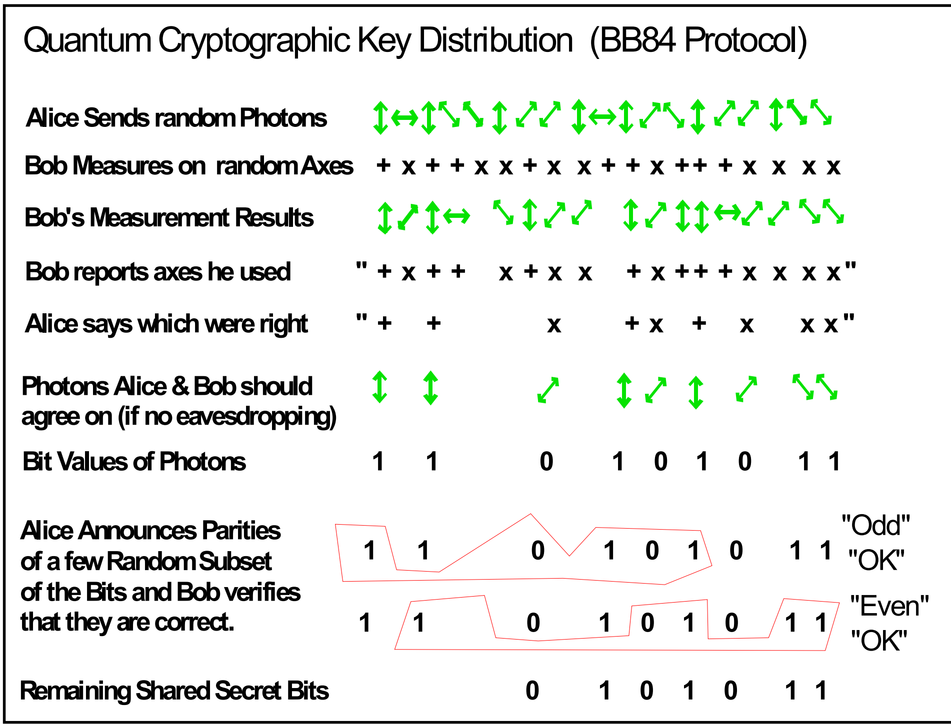


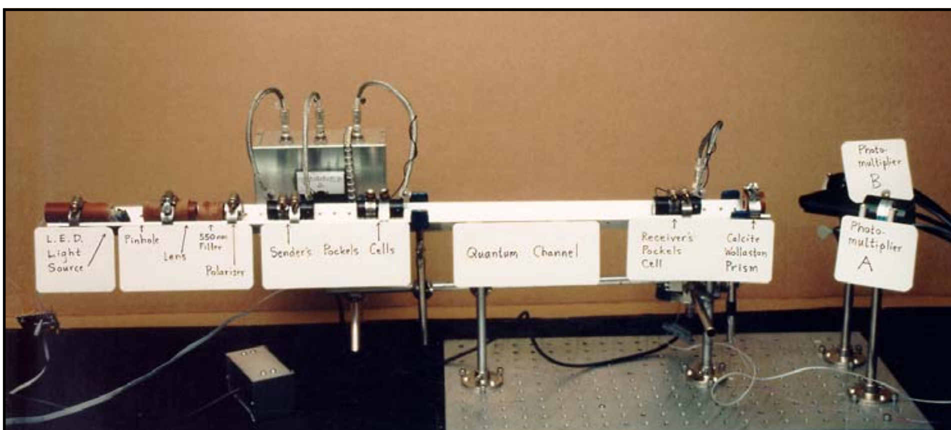
message
key
cryptogram

Quantum Cryptography avoids the need to hand-deliver the key.



In the end, Alice and Bob will either agree on a shared secret key, or else they will detect that there has been too much eavesdropping to do so safely. They will not, except with exponentially low probability, agree on a key that is not secret.



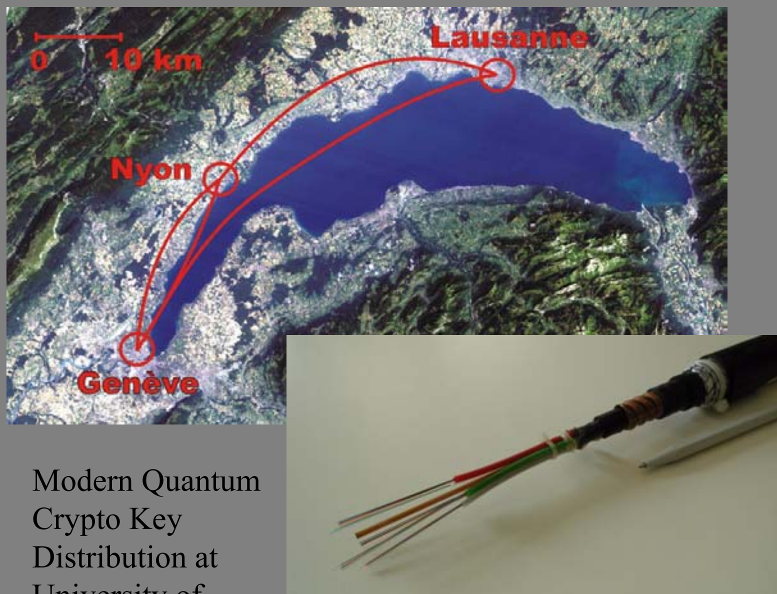


Original Quantum Cryptographic Apparatus built in 1989 transmitted information secretly over a distance of about 30 cm.

Sender's side produces very faint green light pulses of 4 different polarizations.

Quantum channel is an empty space about 30 cm long. There is no Eavesdropper, but if there were she would be detected.

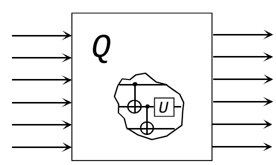
Calcite prism separates polarizations. Photomultiplier tubes detect single photons.



Modern Quantum Crypto Key Distribution at University of Geneva

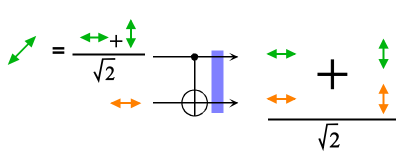
Also experiments at several other labs, and at least 3 commercial systems.

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.

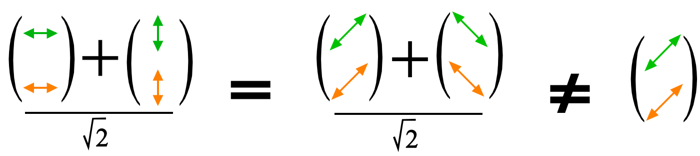
A superposition of inputs gives a superposition of outputs.



or EPR state

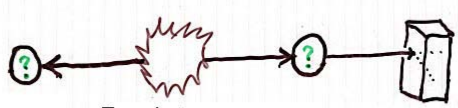
An entangled or EPR tate.

an entangled state is a state of a whole system that is not expressible in terms of states of its parts.



The two photons may be said to be in a definite state of ***sameness*** of polarization even though neither photon has a polarization of its own.

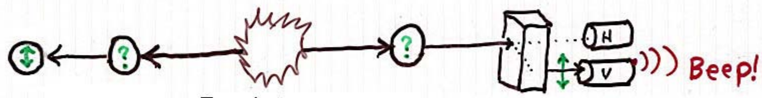
Einstein Podolsky Rosen Effect



Two photons are created in an "entangled" state.

Measuring either one, along any axis, gives a random result...

Einstein Podolsky Rosen Effect



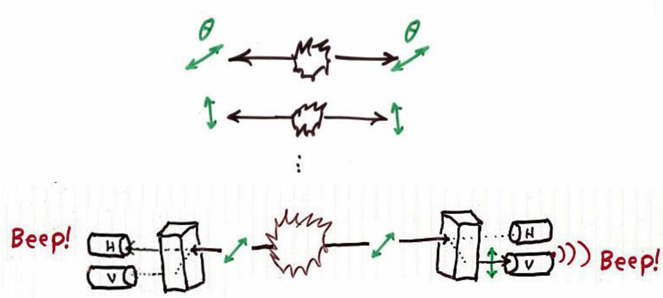
Two photons are created in an "entangled" state.

Measuring either one, along any axis, gives a random result...

And simultanteously causes the other photon to acquire the same polarization.

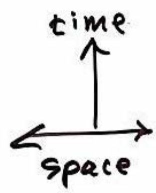
Alternative Explanations of EPR effect.

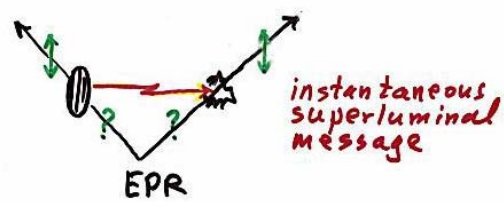
1. At each shot, source emits 2 photons with the same random polarization.



This explanation fails. Sometimes the source would emit 2 digonal photons, and if these were both measured on the V/H axis, sometimes one would behave V and the other H. In fact, they always behave the same, both V or both H.

2. Instantaneous Action at a Distance

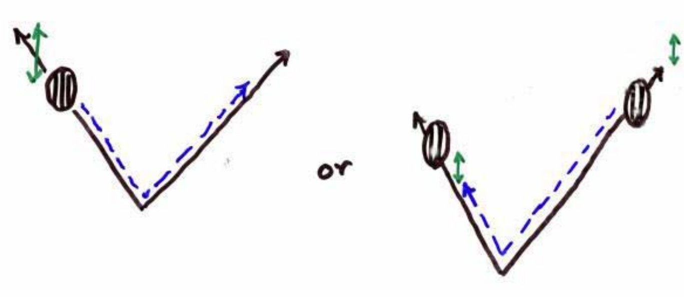


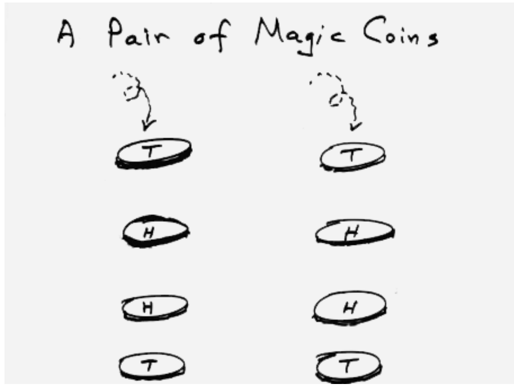


No. Violates special relativity and besides, how does the first particle know where to send the message to?

3. Quantum Mechanics - the right answer

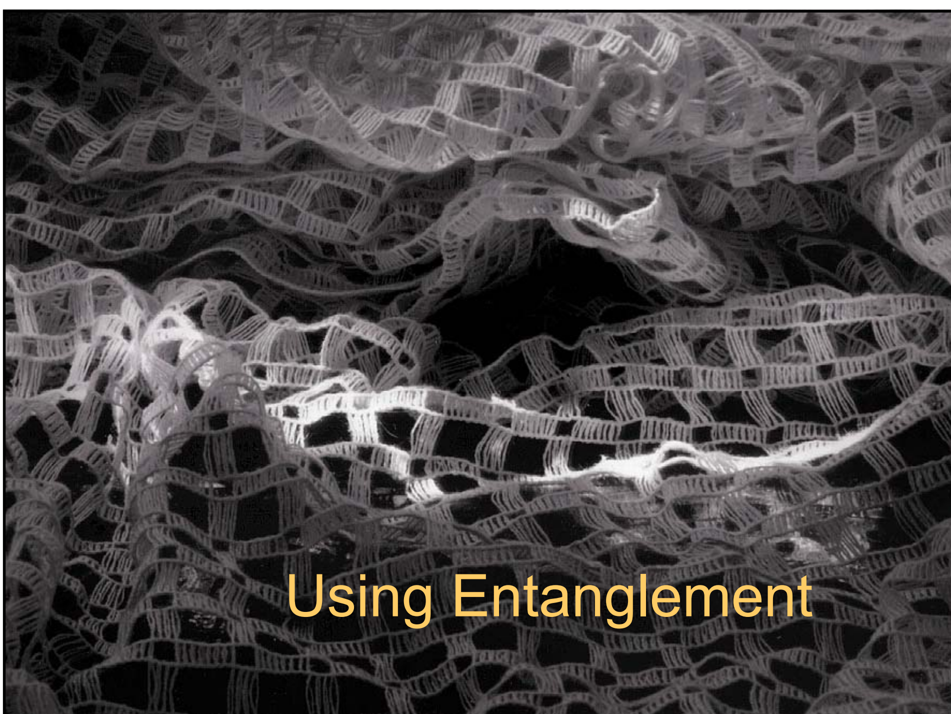
4. Random Uncontrollable Message Backward in time





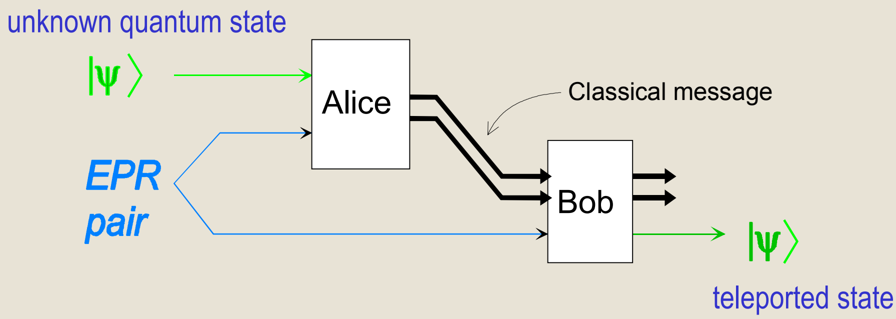
A "message" backward in time is safe from paradox under two conditions, either of which frustrates your ability to advise your broker what stocks to buy or sell yesterday:

1. Sender can't control message (EPR effect) OR
2. Receiver disregards message (Cassandra myth).



Entanglement is useful for Quantum Teleportation,

a way to transmit quantum information when no quantum channel is available.



Prior sharing of an EPR pair allows Alice to disembody an unknown qubit into a 2-bit classical message and preexisting entanglement. When Bob receives the classical message, he can reconstruct the unknown state exactly, but cannot copy it. The EPR link from Alice to Bob goes backward in time, but cannot by itself carry any meaningful message.

Alice's and Bob's roles in teleportation

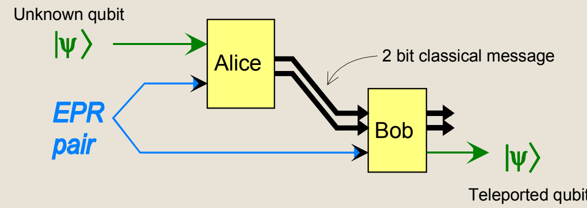
Alice performs a joint measurement of the unknown input qubit ψ and her half of the shared EPR pair in the so-called Bell basis

According to Alice's result, Bob performs one of four unitary transformations, the Pauli operations `I, X, Y, and Z,` on his half of the EPR pair.

|00> +|11>	I (do nothing)	$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$
|00> -|11>	Z phase shift	$\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$
|01> +|10>	X bit flip	$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$
|01> -|10>	Y flip & shift	$\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$

Result: Bob's qubit is left in the same state as Alice's was in before teleportation. If Alice's qubit was itself entangled with some other system, then Bob's will be when the teleportation is finished.

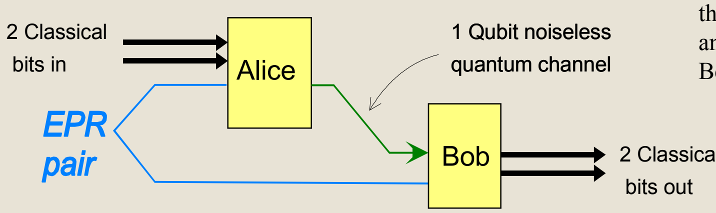
Quantum Teleportation



A dual process
to teleportation

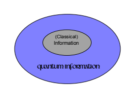
Quantum Superdense Coding

Here Alice does the Pauli rotation and Bob does the Bell measurement.



doubles the classical capacity of any noiseless quantum channel

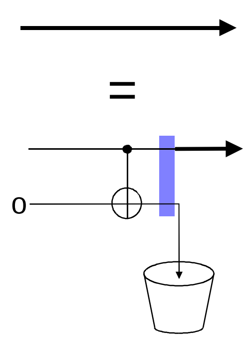
Expressing classical data processing in quantum terms.



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**.

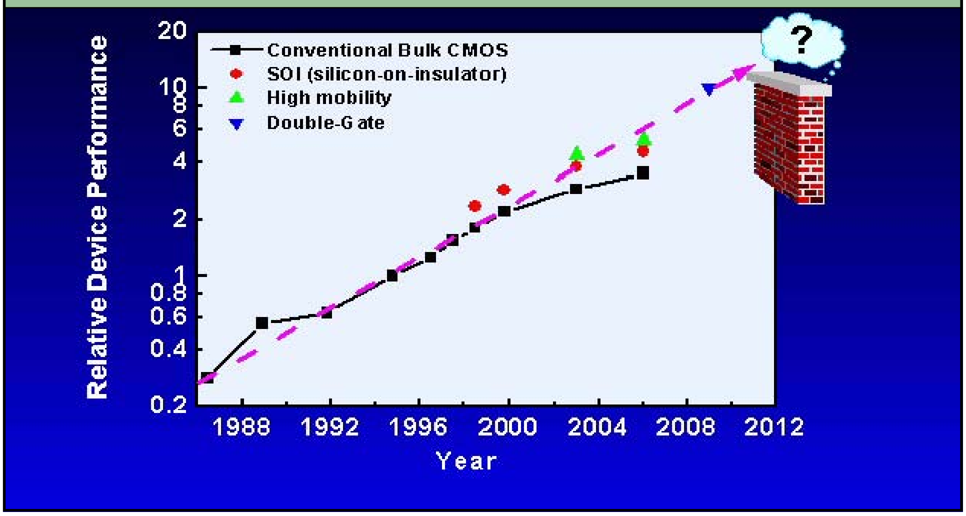
(This occurs because the data passing through the wire interacts with its environment, causing the environment to learn the value of the data, if it was **0** or **1**, and otherwise become entangled with it.)



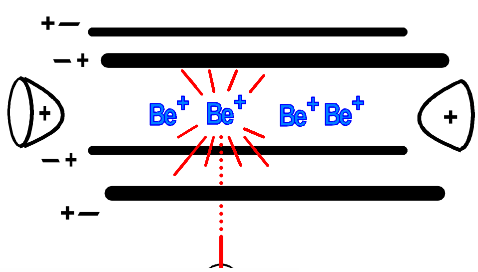
A classical channel is a quantum channel with an eavesdropper.

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

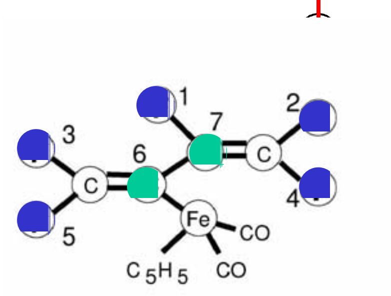
Computer performance has been increasing exponentially for several decades (Moore's law). But this can't go on for ever. Can quantum computers give Moore's law a new lease on life? If so, how soon will we have them?



Some proposed physical implementations of quantum computing



Ion trap: scalable in principle, existing experiments have reached only about ~~2~~ 4 qubits.



Liquid State NMR: used to implement most complicated computations so far, on several qubits. Significant obstacles to scaling above about 10 qubits.

This 7 qubit molecule was used to factor 15

Physical systems actively considered for quantum computer implementation

- **Liquid-state NMR**
- **NMR spin lattices**
- **Linear ion-trap spectroscopy**
- **Neutral-atom optical lattices**
- **Cavity QED + atoms**
- **Linear optics with single photons**
- **Nitrogen vacancies in diamond**
- **Topological defects in fractional quantum Hall effect systems**
- **Electrons on liquid helium**
- **Small Josephson junctions**
  - **"charge" qubits**
  - **"flux" qubits**
- **Spin spectroscopies, impurities in semiconductors**
- **Coupled quantum dots**
  - **Qubits: spin, charge, excitons**
  - **Exchange coupled, cavity coupled**

Executive Summary

• A Quantum computer can probably be built eventually, but not right away. Maybe in 20 years. We don't know yet what it will look like.

• It would exponentially speed up a few computations like factoring, thereby breaking currently used digital signatures and public key cryptography. (Shor algorithm)

• It would speed up many important optimization problems like the traveling salesman, but only quadratically, not exponentially. (Grover algorithm)

• There would be no speedup for many other problems. For these computational tasks, Moore's law would still come to an end, even with quantum computers.

But quantum information is good for many other things besides speeding up computation.

- Quantum cryptography. Practical today and secure even against eventual attack by a quantum computer. Quantum cryptography brings back part of the security that is lost because of quantum computers, but does not fully restore public key infrastructure.

- Speeding up the simulation of quantum physics, with applications to chemistry and materials science.

- Communication and Distributed Computing

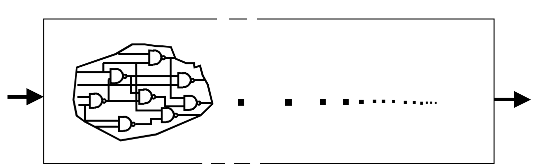
- Metrology, precision measurement and time standards.

- New quantum information phenomena are continually being discovered. An exciting area of basic science.

Classical Computation Theory shows how to reduce all computations to a sequence of NANDs and Fanouts. It classifies problems into solvable and unsolvable, and among the solvable ones classifies them by the resources (e.g. time, memory, luck) required to solve them.   Complexity classes P, NP, PSPACE…

RSA 129

1143816257578888676
6923577997614661201
0218296721242362562
5618429357069352457
3389783059712356395
8705058989075147599
290026879543541



Factors

3490529510847650949
1478496199038981334
1776463849338784399
0820577

x

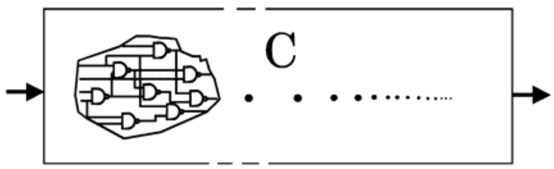
3276913299326670954
9961988190834461413
1776429679929425397
98288533

Some computations require a great many intermediate steps to get to the answer. Factoring large integers is an example. This factoring job took 8 months on hundreds of computers. It could be done much faster on a quantum computer, if one existed.

(For a classical computer, factoring appears to be exponentially harder than multiplication, by the best known algorithms.)

RSA 129

1143816257578888676
6923577997614661201
0218296721242362562
5618429357069352457
3389783059712356395
8705058989075147599
290026879543541



Factors

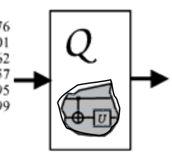
3490529510847650949
1478496199038981334
1776463849338784399
0820577

x

3276913299326670954
9961988190834461413
1776429679929425397
98288533

Same Input and Output, but Quantum processing of intermediate data gives

1143816257578888676
6923577997614661201
0218296721242362562
5618429357069352457
3389783059712356395
8705058989075147599
290026879543541



3490529510847650949
1478496199038981334
1776463849338784399
0820577

x

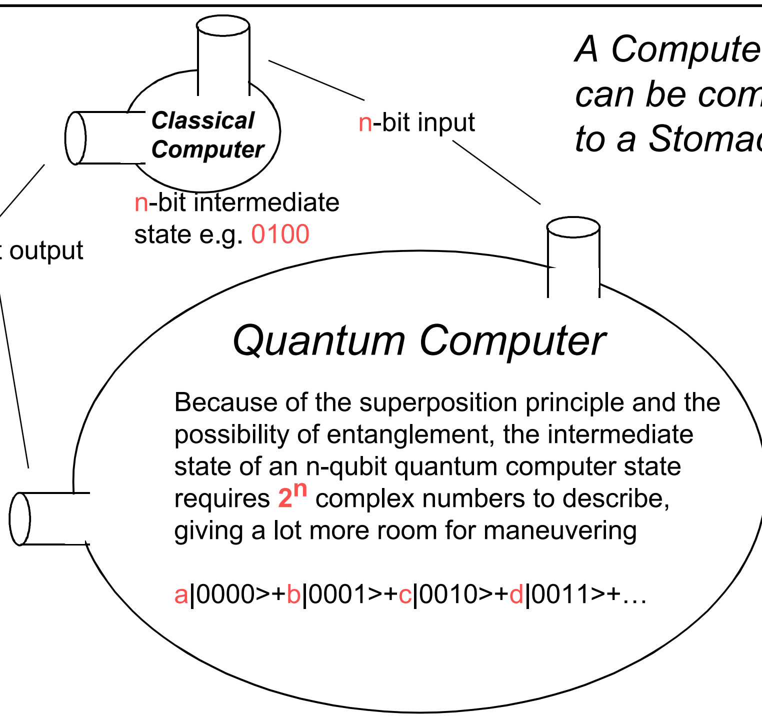
3276913299326670954
9961988190834461413
1776429679929425397
98288533

Exponential speedup for Factoring (Shor algorithm)

Quadratic speedup for Search (Grover algorithm)

(For a quantum computer, factoring is about as easy as multiplication, due to the availability of **entangled** intermediate states.)

A Computer can be compared to a Stomach



How Much Information is "contained in" n qubits, compared to n classical bits, or n analog variables?

	Digital	Analog	Quantum
Information required to specify a state	n bits	n real numbers	2^n complex numbers
Information extractable from state	n bits	n real numbers	n bits
Good error correction	yes	no	yes

The Downside of Entanglement

Quantum data is exquisitely sensitive to decoherence, a randomization of the quantum computer's internal state caused by entangling interactions with the quantum computer's environment.

Fortunately, decoherence can be prevented, in principle at least, by quantum error correction techniques developed since 1995, including

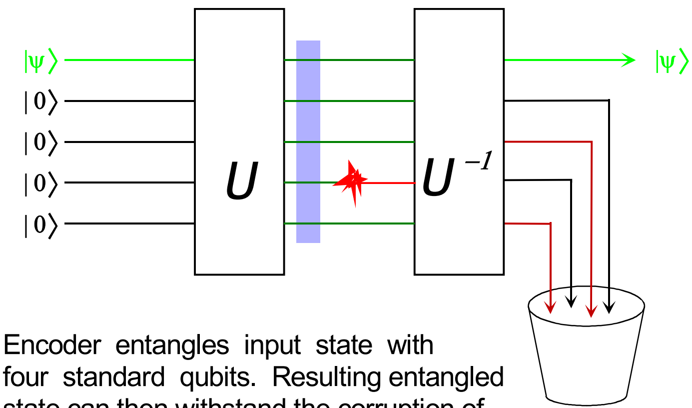
Quantum Error Correcting Codes

Entanglement Distillation

Quantum Fault-Tolerant Circuits

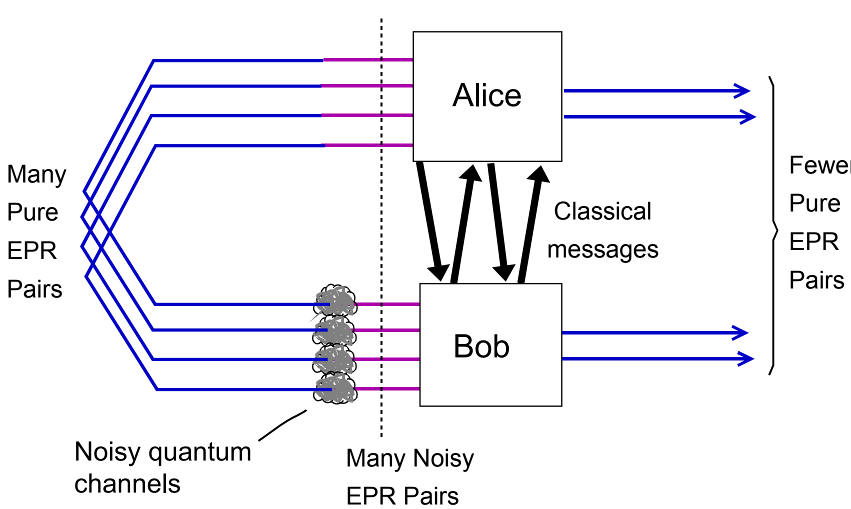
These techniques, combined with hardware improvements, will probably allow practical quantum computers to be built, but not any time soon.

The Simplest Quantum Error-Correcting Code

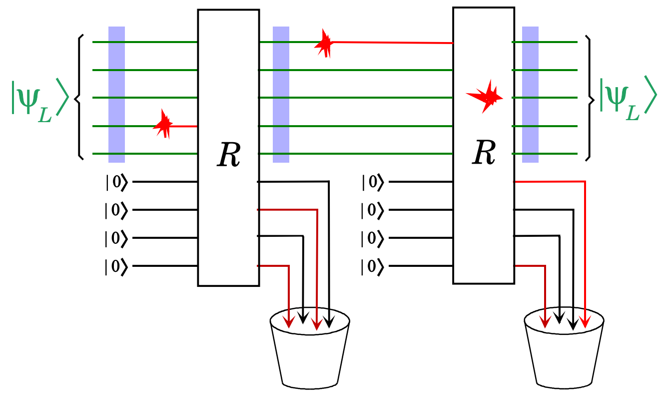


Encoder entangles input state with four standard qubits. Resulting entangled state can then withstand the corruption of any one of its qubits, and still allow recovery of the exact initial state by a decoder at the receiving end of the channel

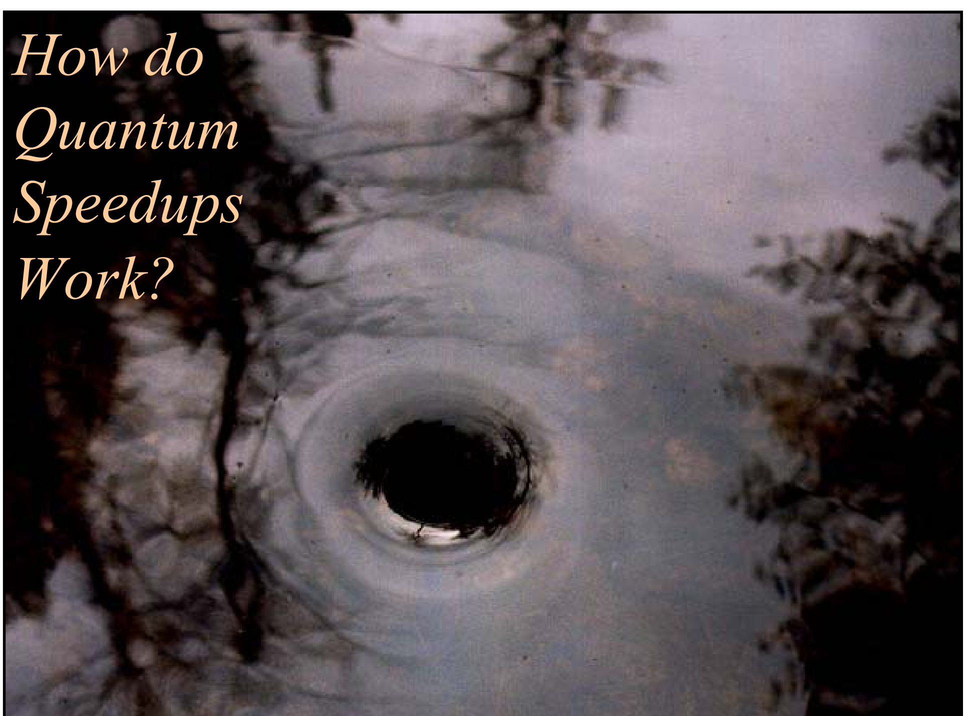
Entanglement Distillation



Quantum Fault Tolerant Computation



Clean qubits are brought into interaction with the quantum data to siphon off errors, even those that occur during error correction itself.



Shor's algorithm – exponential speedup of factoring – Depends on fast quantum technique for finding the period of a periodic function

Grover's algorithm – quadratic speedup of search – works by gradually focusing an initially uniform superposition over all candidates into one concentrated on the designated element. Speedup arises from the fact that a linear growth of the amplitude of the desired element in the superposition causes a quadratic growth in the element's probability.

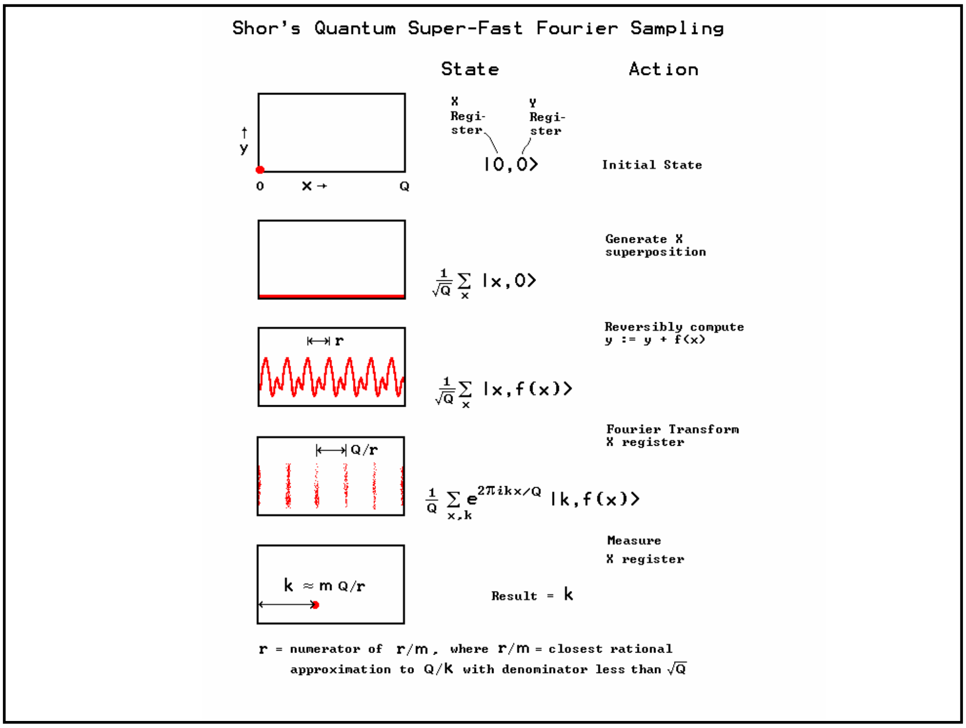
Well-known facts from number theory.

Let N be a number we are trying to factor.

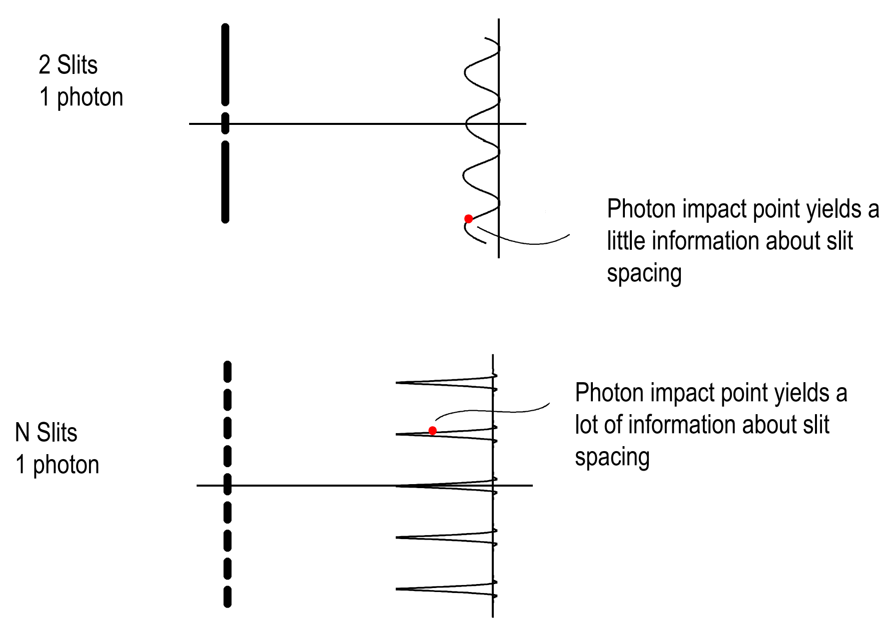
For each $a<N$, the function $f_a(x) = a^x \bmod N$ is periodic with period at most N. Moreover it is easy to calculate. Let its period be r_a. All known classical ways of finding r_a from a are hard.

Any algorithm for calculating r_a from a can be converted to an algorithm for factoring N.

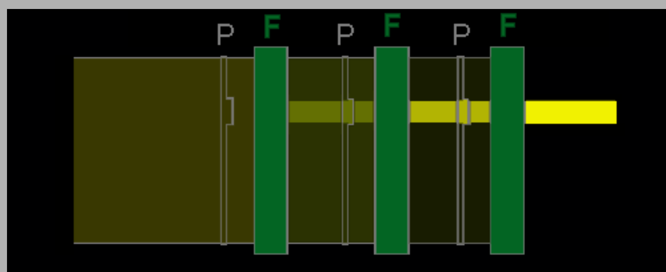
Quantum mechanics makes this calculation easy.



Shor algorithm uses interference to find unknown period of periodic function.



Grover's quantum search algorithm uses about $\sqrt{N}$ steps to find a unique marked item in a list of N elements, where classically N steps would be required. In an optical analog, phase plates with a bump at the marked location alternate with fixed optics to steer an initially uniform beam into a beam wholly concentrated at a location corresponding to the bump on the phase plate.
If there are N possible bump locations, about $\sqrt{N}$ iterations are required.

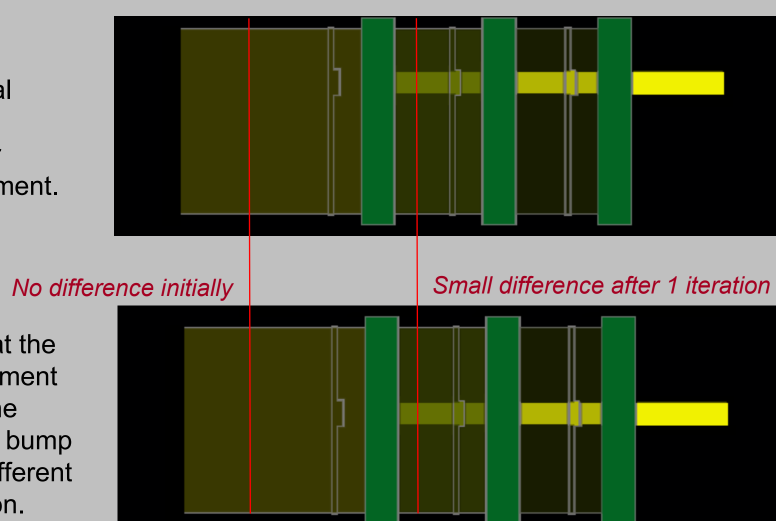


P = phase plate
F = fixed optics

Same optical setup works even with a single photon, so after about $\sqrt{N}$ iterations it would be directed to the right location.

Optimality of Grover's Algorithm: Why can't it work in 1 iteration?

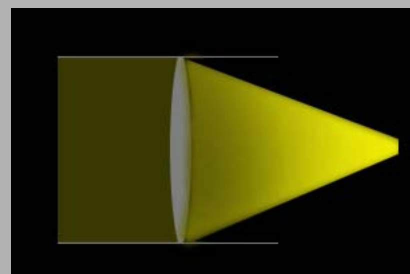
Original optical Grover experiment.



Repeat the experiment with the phase bump in a different location.

Because most of the beam misses the bump in either location, the difference between the two light fields can increase only slowly. About $\sqrt{N}$ iterations are required to get complete separation. (BBBV quant-ph/9701001)

Non-iterative ways to aim a light beam.

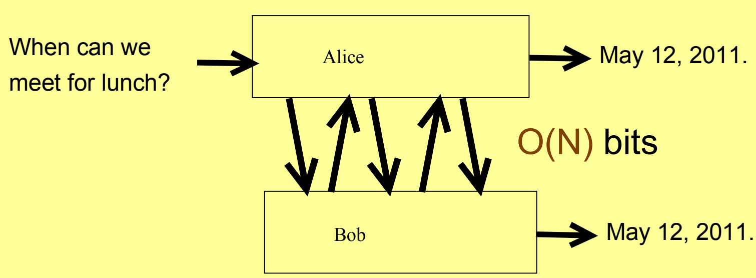


Mask out all but desired area. Has disadvantage that most of the light is wasted. Like classical trial and error. If only 1 photon used each time, N tries would be needed.

Lens: Concentrates all the light in one pass, but to use a lens is cheating. Unlike a Grover iteration or a phase plate or mask, a lens steers all parts of the beam, not just those passing through the distinguished location.

What else is quantum information good for?

1. Quantum Savings in *Communication Complexity*



Quantum communication cost is only **O(sqrt(N) log N)** bits.

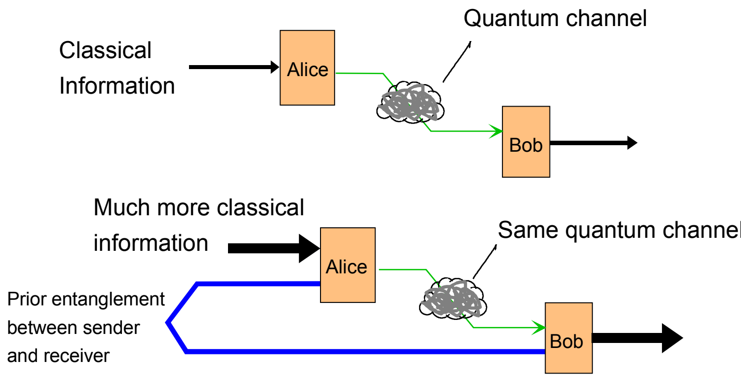
(Buhrman, Cleve and Wigderson, subsequently improved to O(sqrt(N) by Razborov)

Fast quantum protocol for the lunch scheduling problem is a distributed form of Grover's algorithm.

A register of log N qubits, initially containing a uniform superposition of all dates, is passed back and forth between the two parties about $\sqrt{N}$ times, gradually building up amplitude on a conflict-free date.

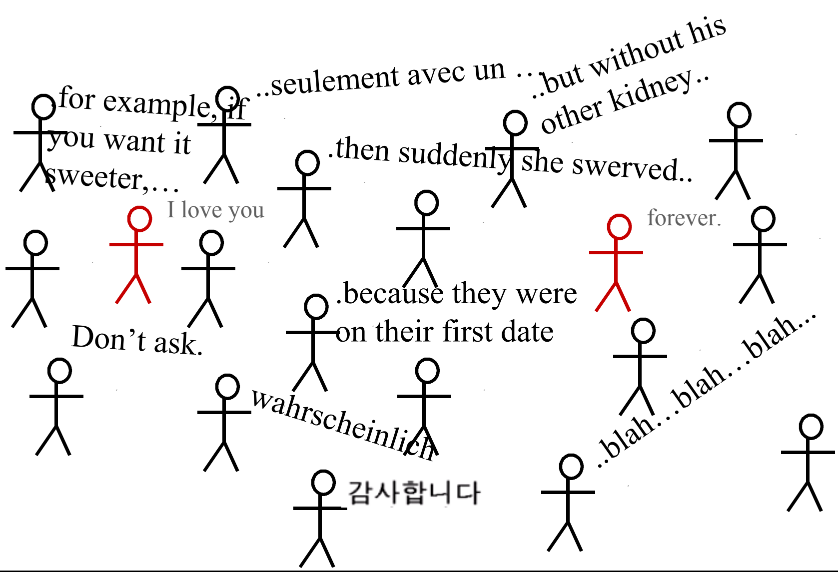
2. Entanglement Enhanced Classical Capacity:

By itself, entanglement itself cannot be used for classical communication (otherwise we would have faster-than-light communication) but it can increase the classical capacity of an existing quantum channel, in some cases by a large factor.

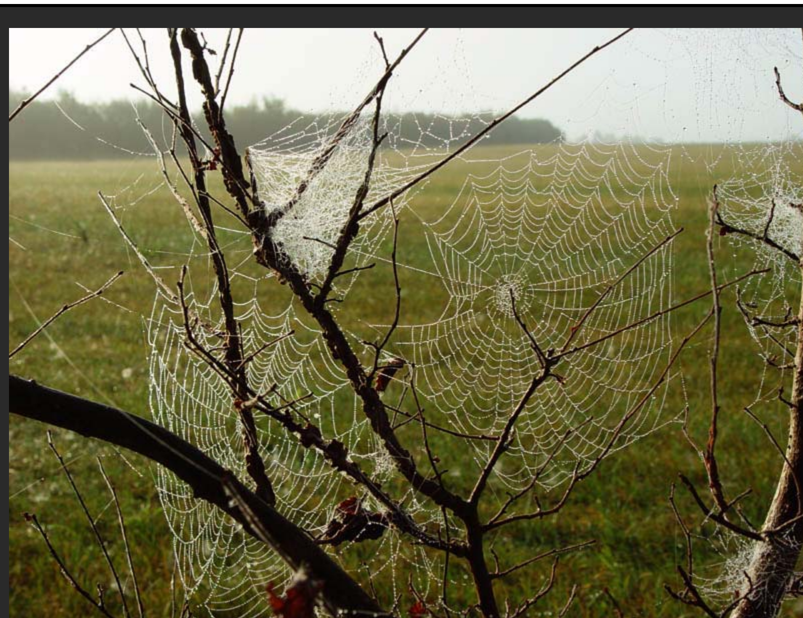


Enhancement factor = 2 for noiseless channels, can be arbitrarily large for noisy channels

Prior shared entanglement helps a good deal if Alice and Bob are trying to hold a quiet conversation in a room full of noisy strangers (Gaussian channel in low signal, high noise, low-attenuation limit)



But it doesn't help much if they are far apart in an empty room (high attenuation)



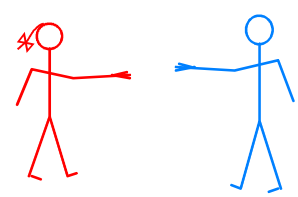
Quantum Laws & the Universality of Interaction

One way in which quantum laws are simpler than classical is the universality of interaction.

Classically, there are distinct kinds of interaction that cannot be substituted for one another. For example, if I'm a speaker and you're a member my audience, no amount of talking by me enables you to ask me a question.

Quantumly, interactions are intrinsically bidirectional. Indeed there is only one kind of interaction, in the sense that any interaction between two systems can be used to simulate any other.

A quantum love story, based on the classic tale of Pyramus and Thisbe.



Alice and Bob are young and in love.

Unfortunately, their parents oppose their relationship, and have forbidden them to visit, or talk, or exchange email.

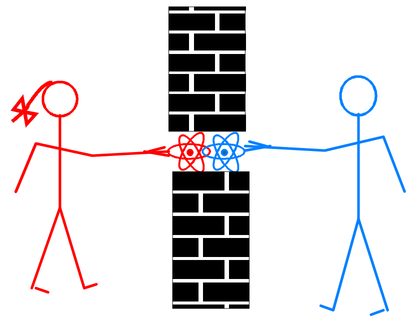
Fortunately, they live next door to one another.

Unfortunately, there's a wall between their two houses.

Fortunately, there's a hole in the wall.

-- more --

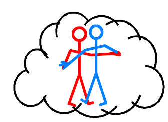
Unfortunately, the hole is only big enough for one atom of Alice to interact with one atom of Bob, via an interaction ***H'*** **.**



Fortunately, Alice and Bob know quantum mechanics. They know that any interaction can be used to create entanglement, and that interactions are intrinsically bidirectional and private: A cannot affect B without B affecting A. If C interferes or eavesdrops, the joint state of A and B will be degraded and randomized.

-- more --

The young lovers wish to experience the life they would have had if they had been allowed to interact not by the one-atom interaction **H'** but by the many-atom interaction **H**, which is a physicist's way of saying always being in each other's arms.



How can they use the available **H'** to simulate the desired **H** ?

They can of course separately prepare their respective interacting atoms in any initial states, and thereafter alternate through-the-wall interactions under H' with local operations among their own atoms, each on his/her own side of the wall.

Using the hole in the wall, they can prepare entangled states. We assume each has a quantum computer in which to store and process this entanglement. Whenever they need to communicate classically, to coordinate their operations, they can use the interaction **H'** to do that too. Thus the joint states they can experience are all those that can be achieved by shared entanglement and classical communication. Of course it will take a lot of time and effort.

-- more --

The joint states they can experience are all those that can be achieved by shared entanglement and classical communication.

But this is *all* quantum states of A and B!

If their parents had only plugged the hole in the wall and allowed them unlimited email, their future would have been much bleaker.

They could never have become entangled, and their relationship would have remained Platonic and classical. In particular, it would have had to develop with the circumspection of knowing that everything they said might be overheard by a third party.

As it is, with the hole remaining open, by the time they get to be old lovers, they can experience exactly what it would have been like to be young lovers (if they are still foolish enough to want that).

-- The End --

Some relevant papers, mostly available online

On Thermodynamics of Computation and Reversible Computation:

C.H. Bennett "The Thermodynamics of Computation-- a Review" Internat. J. Theoret. Phys. 21, pp. 905-940 (1982).
http://www.research.ibm.com/people/b/bennetc/bennettc1982666c3d53.pdf

Bennett, C.H., "Logical Reversibility of Computation" IBM J. Res. Develop. 17, 525 (1973).
http://www.research.ibm.com/people/b/bennetc/bennettc19734c533842.pdf

On Logical Depth and physical complexity

Charles H. Bennett, "How to Define Complexity in Physics, and Why," in Complexity, Entropy, and the Physics of Information (Wojciech H. Zurek, Editor), Addison-Wesley, 1990 pp 137-148.
http://www.research.ibm.com/people/b/bennetc/bennettc19903b272b10.pdf

Charles H. Bennett "Logical Depth and Physical Complexity" in The Universal Turing Machine– a Half-Century Survey, edited by Rolf Herken Oxford University Press 227-257, (1988)
http://www.research.ibm.com/people/b/bennetc/UTMX.pdf

Quantum Information and Computation

C.H. Bennett and D.P. DiVincenzo; "Quantum Information and Computation" Nature 404:6775, 247-255 (2000).

Report to US National Science Foundation on Quantum Information Science
http://www.nsf.gov/pubs/2000/nsf00101/nsf00101.htm