

# Information is Quantum

Charles H. Bennett  
IBM Research Yorktown  
IBM Research Hawthorne, 7 July 2006



Information



(Classical)  
Information

A Venn diagram consisting of two nested ellipses. The outer ellipse is light blue and contains the text 'quantum information' at the bottom. The inner ellipse is light gray and is centered within the blue one, containing the text '(Classical) Information'.

*quantum information*

A Venn diagram illustrating the relationship between classical and quantum information. It features a large light blue oval representing the total space. Inside this oval is a smaller gray oval. The gray oval contains the text "(Classical) Information". At the bottom of the gray oval is a red rectangular box containing the text "Information Technology". Below the gray oval, within the light blue oval, is the text "quantum information".

(Classical)  
Information

Information Technology

quantum information

Information = Distinguishability.

(Using a pencil, a piece of paper can be put into a 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

It is natural to assume that information

- can be copied at will without disturbing it
- cannot travel faster than light or backward in time
- can be erased when it is no longer wanted

## *But chemists and physicists have long known that*

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

- cannot be read or copied without disturbance.
- can connect two isolated parties by a correlation too strong to be explained by imputing a separate, perhaps unknown, state to each. 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

$$\langle \phi | \psi \rangle = \sum \phi_i^* \psi_i$$

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

$$\longleftrightarrow = \begin{pmatrix} 0 \\ 1 \end{pmatrix} \quad \updownarrow = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$$

3. E.g. for photons, other polarizations

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

$$\curvearrowright = \begin{pmatrix} i \\ 1 \end{pmatrix} \quad \curvearrowleft = \begin{pmatrix} i \\ -1 \end{pmatrix}$$

4. Unitary = Linear and inner-product preserving.

## quantum laws

1. To each physical system there corresponds a Hilbert space <sup>1</sup> of dimensionality equal to the system's maximum number of reliably distinguishable states. <sup>2</sup>

2. Each direction (ray) in the Hilbert space corresponds to a possible state of the system. <sup>3</sup>

3. Spontaneous evolution of an unobserved system is a unitary transformation on its Hilbert space. <sup>4</sup>

-- more --



4. The Hilbert space of a composite system 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  $\{P_j\}$ , where  $\sum P_j = 1$ . On state  $\psi$  the result  $j$  occurs with probability  $|P_j \psi|^2$  and the state after measurement is

$$\frac{P_j |\psi\rangle}{|P_j \psi|}$$

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

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

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  $P_j$ .

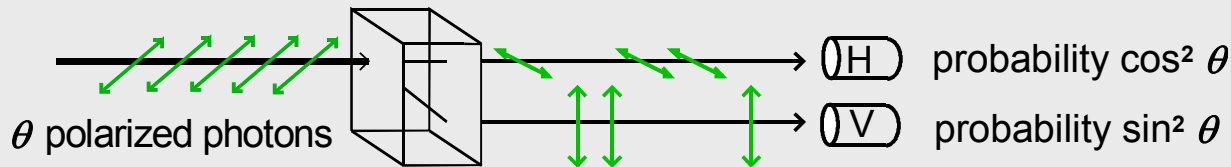
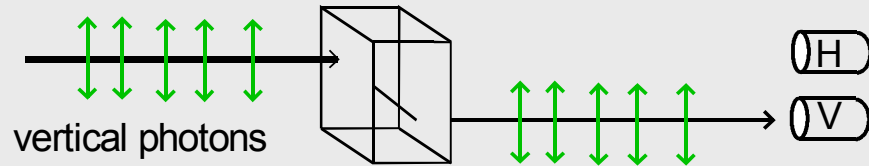
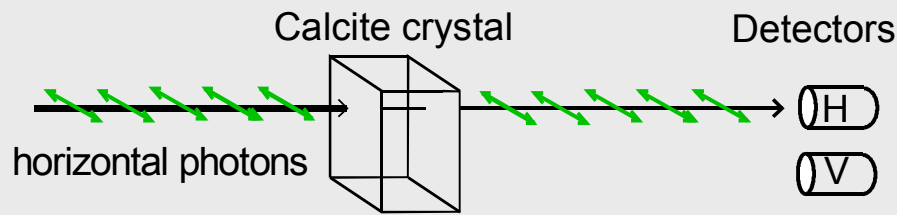
# superposition principle

*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)*



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

$$\begin{aligned} \nearrow &= \frac{\leftrightarrow + \updownarrow}{\sqrt{2}} \\ \nwarrow &= \frac{\leftrightarrow - \updownarrow}{\sqrt{2}} \end{aligned}$$

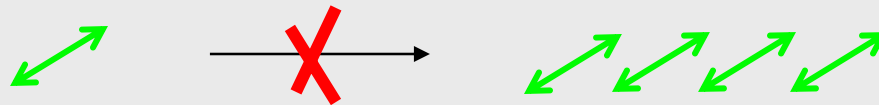
Non-orthogonal states like  $\leftrightarrow$  and  $\nearrow$  are in principle imperfectly distinguishable.

$\leftrightarrow$  always behaves somewhat like  $\nearrow$  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).

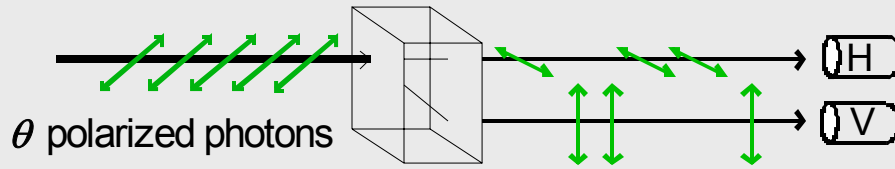


Cloning an unknown photon is impossible. (If either cloning or measuring were possible the other would be also).



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.





Like a pupil confronting a strict teacher, a quantum system being measured is forced to choose among a set of distinguishable states (here 2) characteristic of the measuring apparatus.

*Teacher:* Is your polarization vertical or horizontal?

*Pupil:* Uh, I am polarized at about a 55 degree angle from horizontal.

*Teacher:* **I believe I asked you a question.** Are you vertical or horizontal?

*Pupil:* Horizontal, sir.

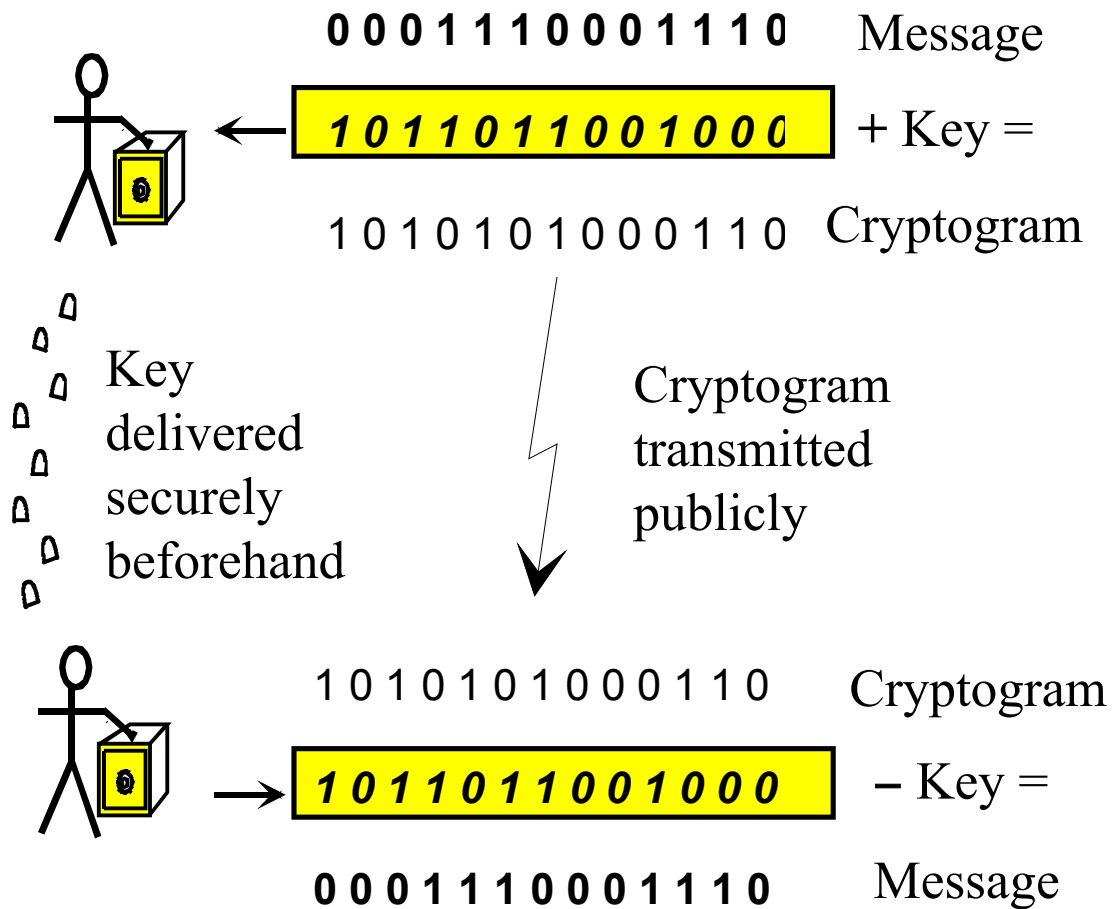
*Teacher:* Have you ever had any other polarization?

*Pupil:* No, sir. I was always horizontal.

# 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

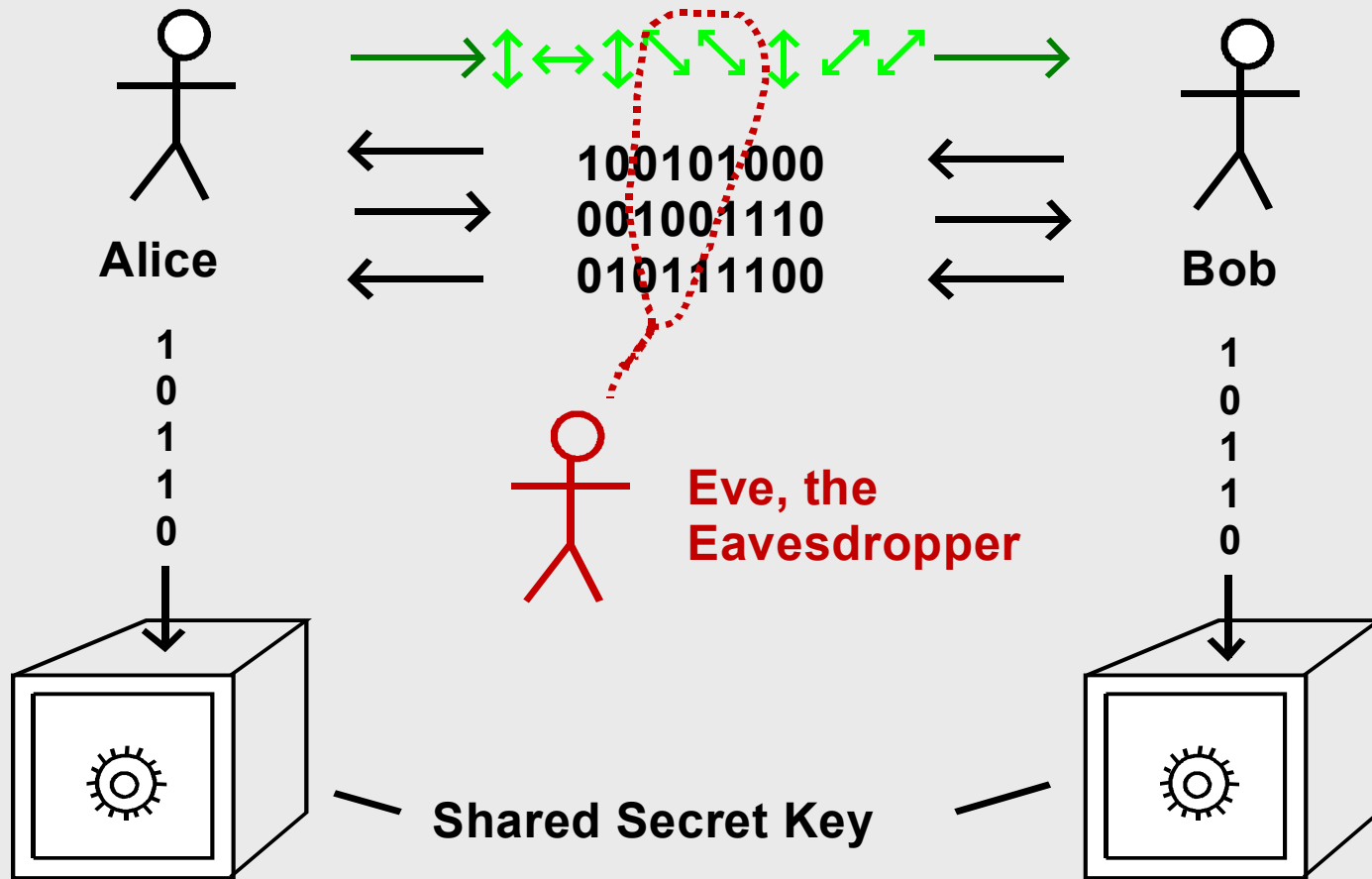


|   |   |   |   |   |
|---|---|---|---|---|
| 5 | 0 | 8 | 3 | 3 |
| 1 | 8 | 4 | 7 | 1 |
| 6 | 9 | 2 | 0 | 4 |

|   |   |   |   |   |
|---|---|---|---|---|
| 8 | 2 | 0 | 8 | 8 |
| 7 | 8 | 2 | 1 | 3 |
| 5 | 0 | 2 | 9 | 1 |

message  
key  
cryptogram

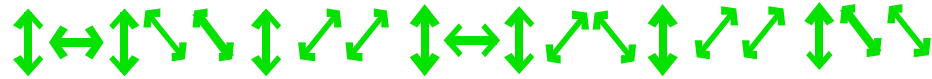
# Quantum Cryptographic Key Distribution



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.

# 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 "

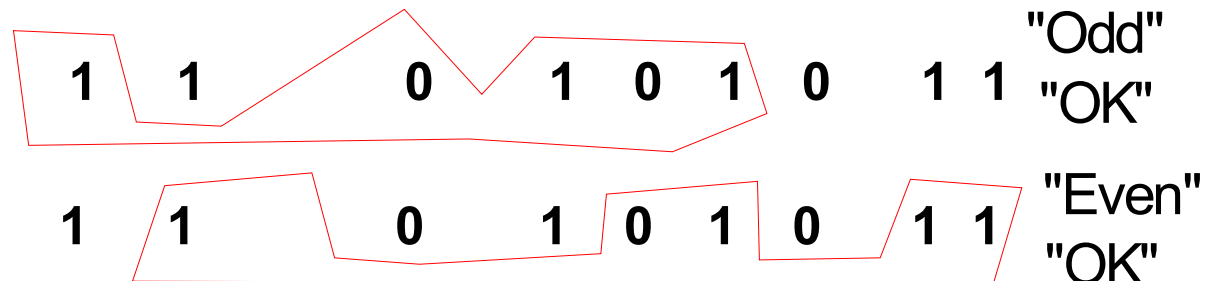
Photons Alice & Bob should agree on (if no eavesdropping)



Bit Values of Photons

1 1 0 1 0 1 0 1 1

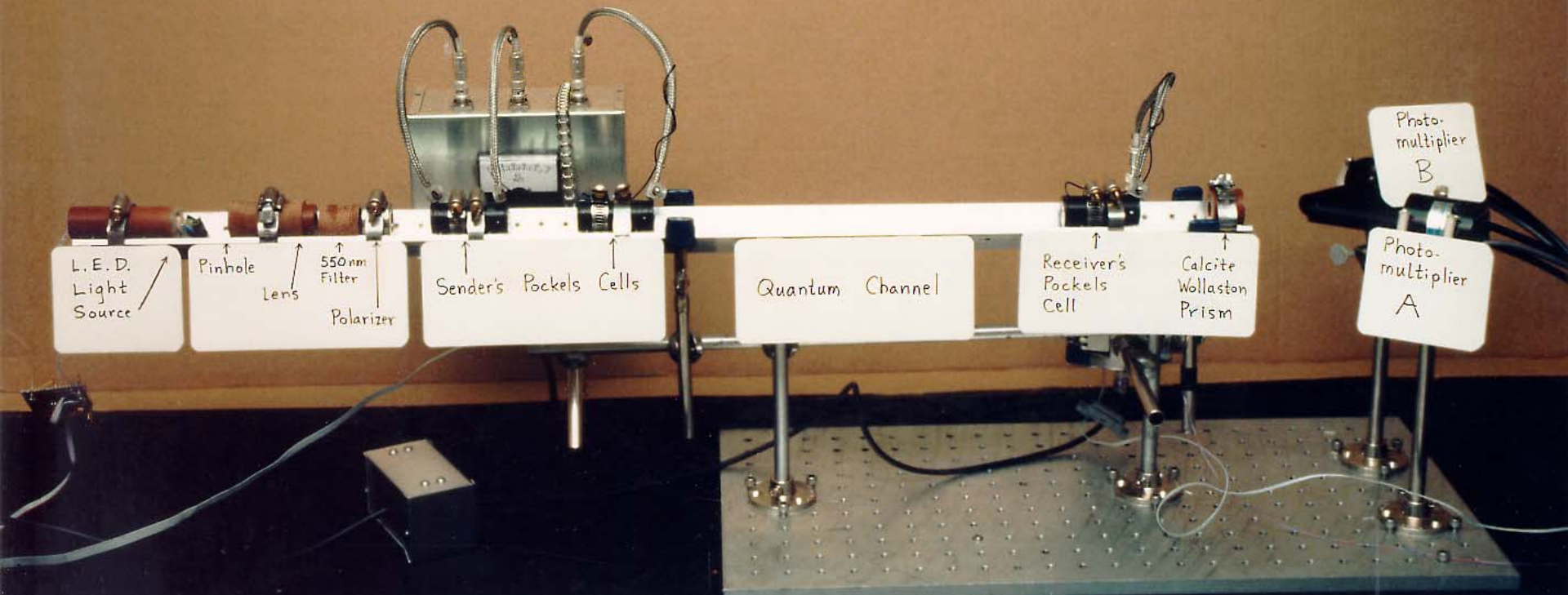
Alice Announces Parities of a few Random Subset of the Bits and Bob verifies that they are correct.



Remaining Shared Secret Bits

0 1 0 1 0 1 1





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.



Quantum  
Crypto Key  
Distribution at  
University of  
Geneva



Also experiments at Los Alamos, Almaden,  
and other labs in US, Europe & Japan.



# Commercial Quantum Key Distribution systems



ID-Quantique

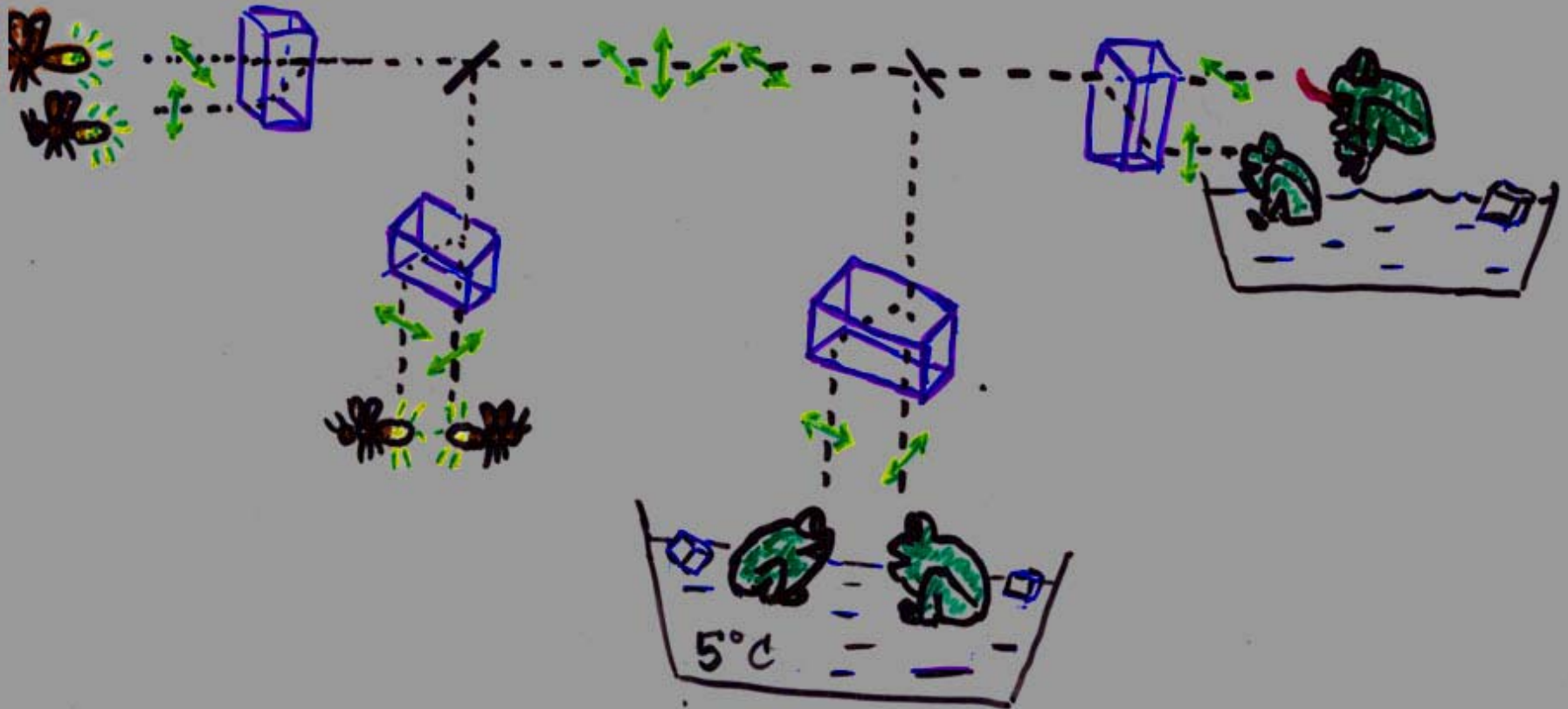


MagiQ Technologies

So far, all commercial QKD equipment has taken the form of boring rectangular metal boxes.

Sales have been less than anticipated. Perhaps some new ideas are needed.

Frogs, if cooled to  $5^{\circ}\text{C}$  to reduce dark counts, can see and respond to single photons. This raises the possibility of an all-natural quantum cryptography system, “Green QKD”.



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)

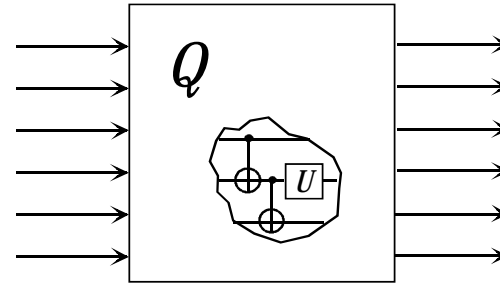
*Perhaps more important* (Nicolas Gisin)

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.

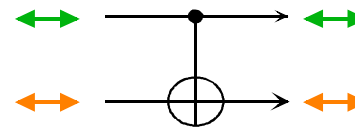
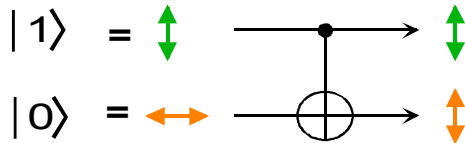
First: Quantum cryptography—use of uncertainty to prevent undetected eavesdropping

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

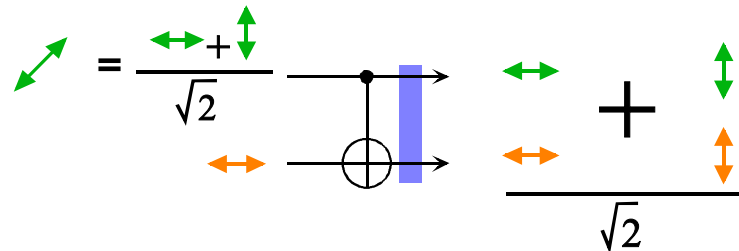
Any quantum data processing can be done by 1- and 2-qubit gates acting on qubits.



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



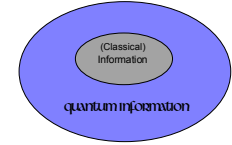
A superposition of inputs gives a superposition of outputs.



An **entangled** or EPR state

# Expressing classical data processing in quantum terms.

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

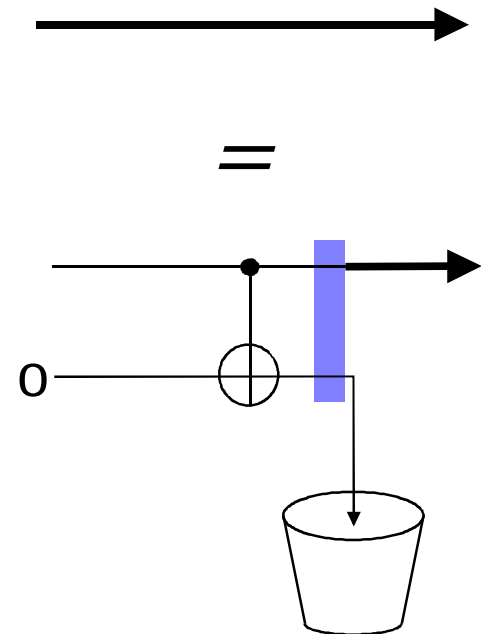


A classical wire is a quantum channel that conducts **0** and **1** faithfully, but randomizes superpositions of **0** and **1**.

(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.*





**Bit** (< binary digit) n.

1. (math) One of the digits 0 and 1 used in binary arithmetic.
2. (information theory)
  - a) Any system with two reliably distinguishable states.
  - b) The amount of information carried by a such a system.

**Qubit** (< quantum bit) n.

1. (math) A ray in a 2 dimensional complex Hilbert space.
2. (quantum information theory)
  - a) Any system capable of existing in two reliably distinguishable states and arbitrary superpositions of them.
  - b) The amount of quantum information carried by such a system.

(proposed dictionary definition)

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

$$\frac{\begin{pmatrix} \text{green} \leftrightarrow \\ \text{orange} \leftrightarrow \end{pmatrix} + \begin{pmatrix} \text{green} \updownarrow \\ \text{orange} \updownarrow \end{pmatrix}}{\sqrt{2}} = \frac{\begin{pmatrix} \text{green} \nearrow \\ \text{orange} \searrow \end{pmatrix} + \begin{pmatrix} \text{green} \nwarrow \\ \text{orange} \swarrow \end{pmatrix}}{\sqrt{2}} \neq \begin{pmatrix} \text{green} \nearrow \\ \text{orange} \searrow \end{pmatrix}$$

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.



During the hippie era, it was common to find people who individually knew nothing, but nevertheless felt perfectly in tune with each other.



1967

Pedagogic analog of entanglement:

Twin pupils Remus and Romulus, who are each completely ignorant of all subjects, answering randomly, but always give the same answer, even when questioned separately.

Teacher A: Remus, what color is growing grass?

Remus: Pink, sir.

Teacher B (in another classroom): Romulus, what color is growing grass?

Romulus: Pink, ma'am.

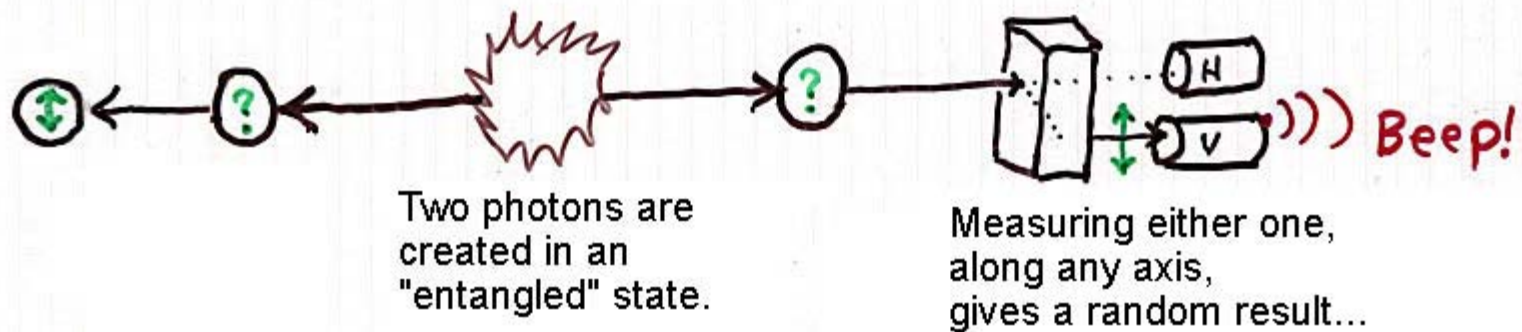
# Einstein Podolsky Rosen Effect



Two photons are  
created in an  
"entangled" state.

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

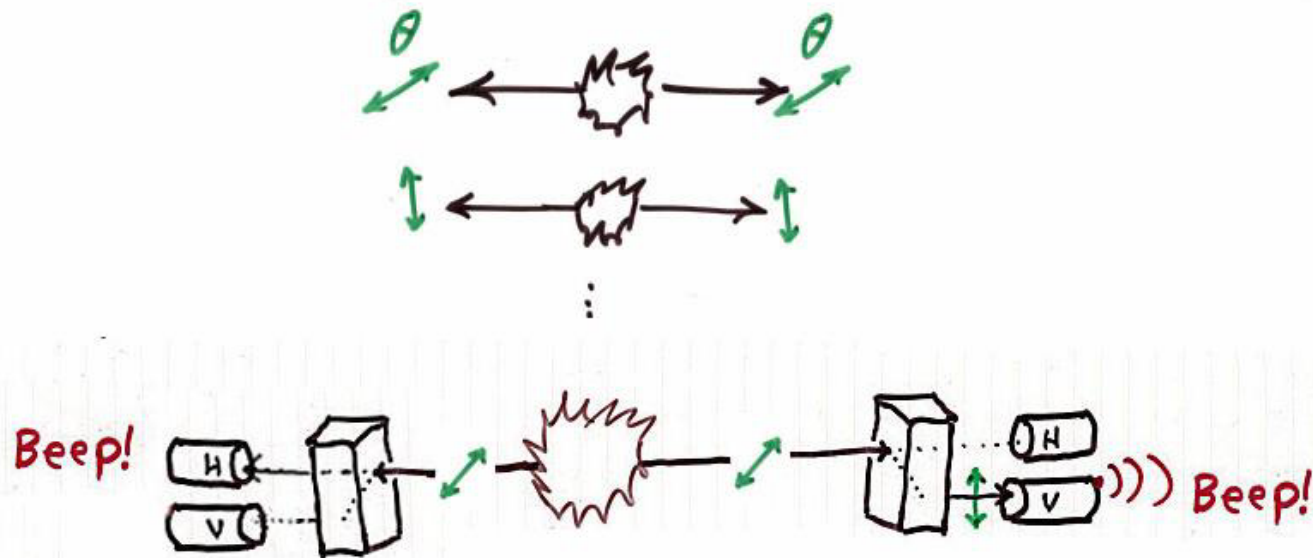
# Einstein Podolsky Rosen Effect



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

## Alternative Explanations of EPR effect.

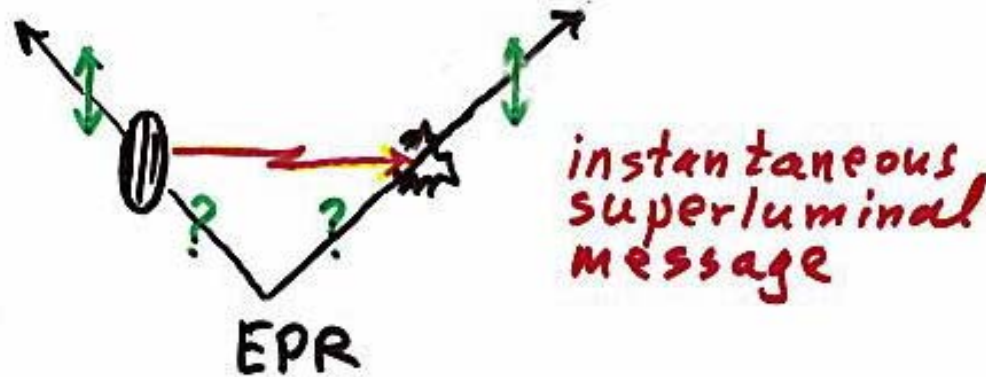
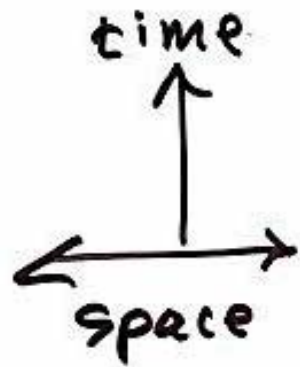
1. At each shot, source emits 2 photons with the same random polarization.



This explanation fails. Sometimes the source would emit 2 diagonal 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?

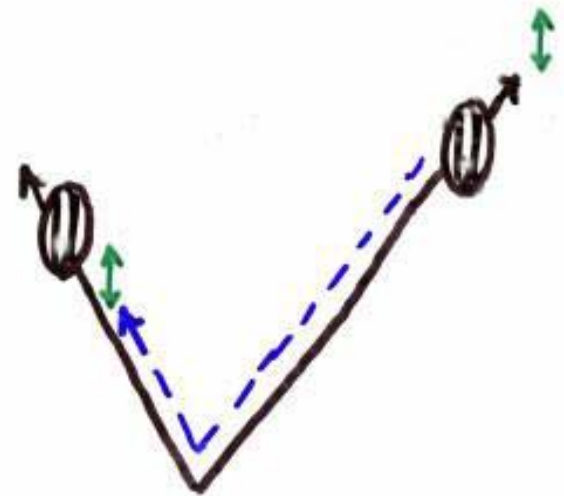


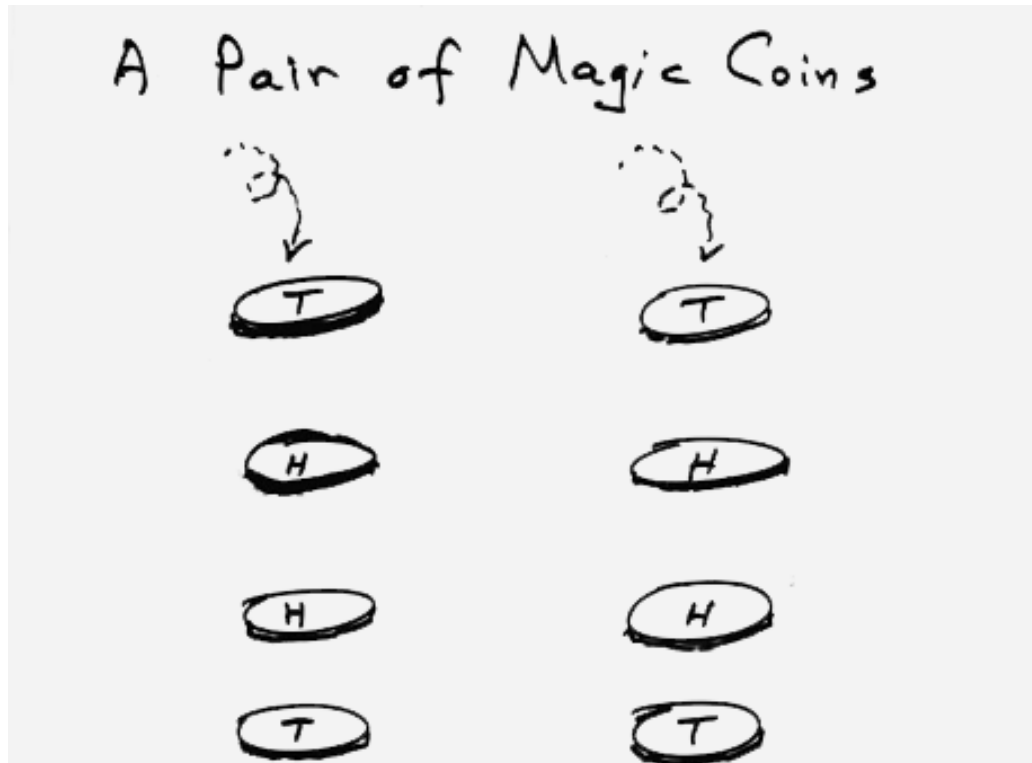
3. Quantum Mechanics - the right answer

4. Random Uncontrollable Message  
Backward in time



or

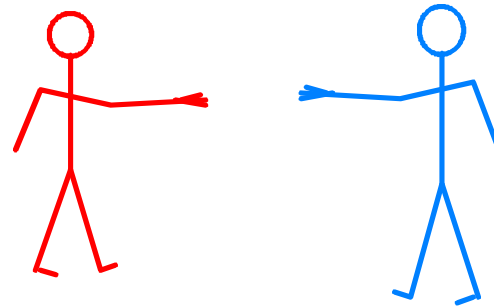




A “message” backward in time is safe from paradox under two conditions, either of which frustrate your ability to advise your broker what stocks to buy or sell yesterday:

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

# Personification of Entanglement



Some physical interaction is needed to create entanglement. You can't get entangled with someone simply by talking on the telephone.

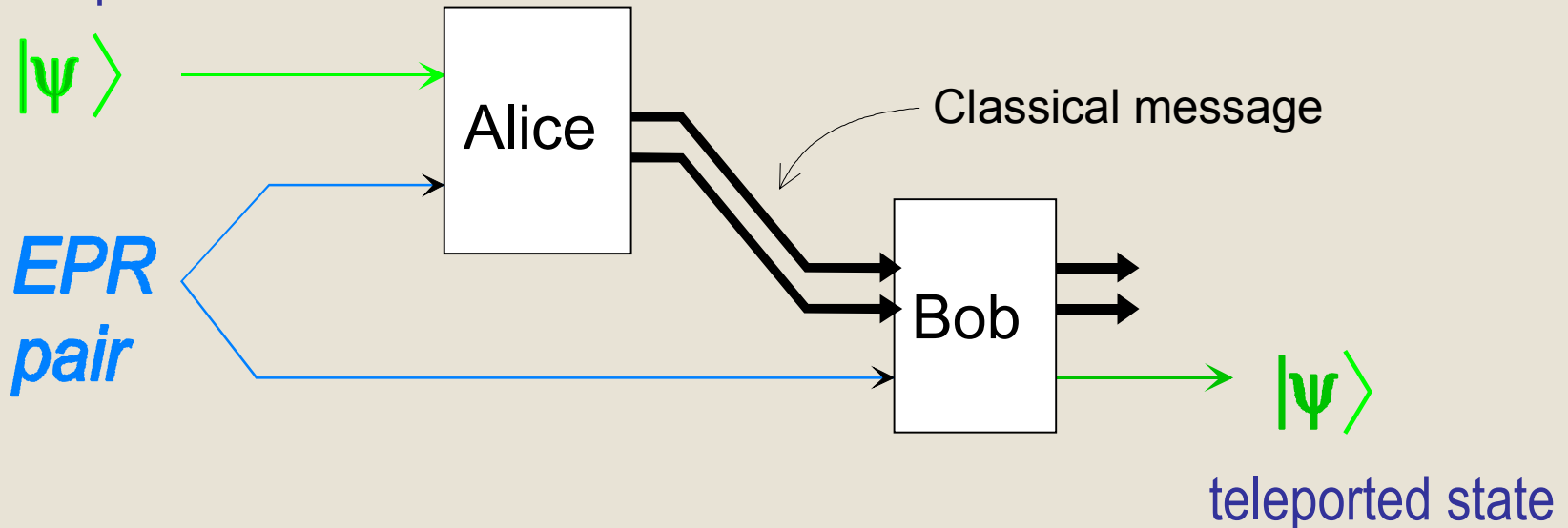
Entanglement is monogamous —  
the more entangled Bob is with Alice,  
the less entangled he can be with anyone else.

(The hippies failed to intuit this feature of entanglement. If they had, their revolution might have been more successful.)

# *Using Entanglement*

Entanglement is useful for Quantum Teleportation,  
a way to transmit quantum information when no quantum channel is available.

unknown quantum state



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.

## Human analog of quantum teleportation, or How entangled twins Remus and Romulus can assist the police with their investigations

Suppose Alice has witnessed a complicated crime with possible terrorist implications where she lives, in Boston. The police are aware that her perception of the crime is in a fragile form. They don't want to ask her questions that might distort her memory. They especially don't want to leave the investigation to the local authorities, who will ask her stupid questions and confuse her. They propose to have her travel to FBI headquarters in Washington, where people will ask just the right questions and not spoil her memory. But Alice is busy, and cannot make the trip. The local authorities will have to do the investigation after all.

Then the FBI comes up with a compromise. They know of a pair of twins, Remus and Romulus. The twins don't know anything about the crime, or anything else for that matter, but they are entangled: whatever one feels, the other feels. "So here's the deal," says the FBI. "We want Alice and Remus to sit down together and decide whether they like each other. We don't want them to talk about the crime. We just want them to tell us how they get on."

Remus goes to Boston to meet Alice. The meeting is a sort of speed-date, with the parties instructed not to talk about anything substantive, just to decide whether they like each other. Alice emerges at the end saying, "I hate him, and for some reason, this has been so stressful that now I don't remember anything about the crime "

The Boston police thank her and tell her she can go home.

Then they phone Washington and tell the FBI that Alice and Remus don't get on. The FBI officers go to Romulus and say, "Well, it seems that Alice and your brother don't get on. So any question we would have asked Alice, we can ask you. We know that whenever you say yes, she would have said no." They proceed with their careful questioning, reversing every one of Romulus' answers to get what Alice would have answered."

# Alice's and Bob's roles in teleportation

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

$$\begin{aligned} &|00\rangle + |11\rangle \\ &|00\rangle - |11\rangle \\ &|01\rangle + |10\rangle \\ &|01\rangle - |10\rangle \end{aligned}$$

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

|                |   |
|----------------|---|
| I (do nothing) | $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$  |
| Z phase shift  | $\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$ |
| X bit flip     | $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$  |
| 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.



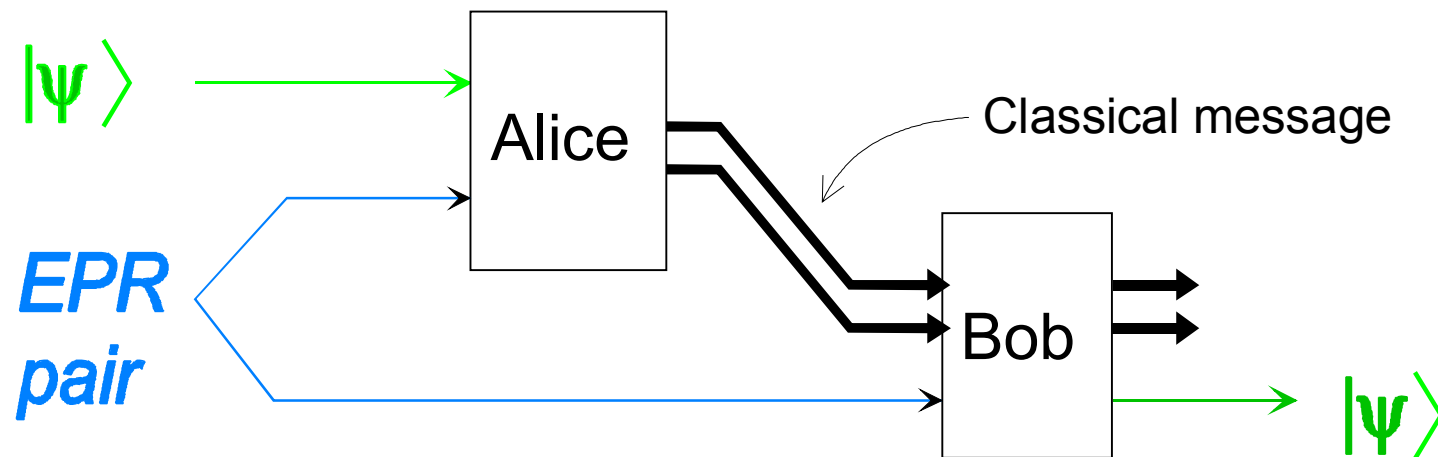
# Partial analogy between teleportation & 1-time pad encryption

Private  $\approx$  Quantum

Public  $\approx$  Classical

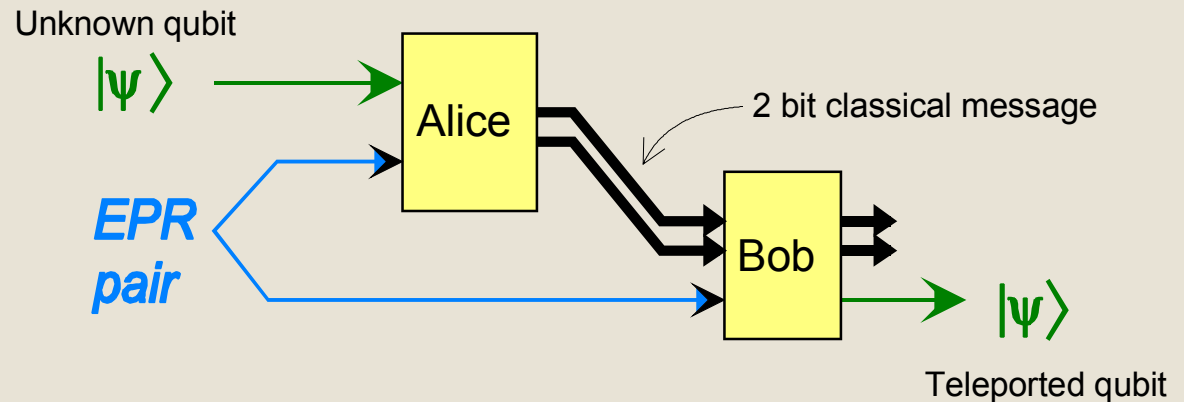
Key  $\approx$  Entanglement

Ciphertext  $\approx$  Classical message in teleportation



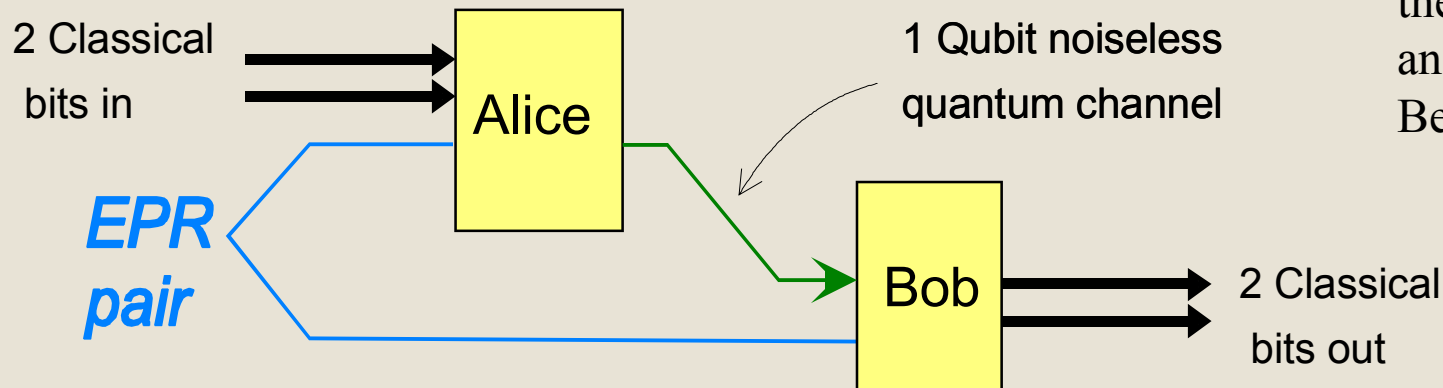
But analogy is not exact, since for example  
classical message in teleportation has 2 bits, not 1

## Quantum Teleportation



A dual process  
to teleportation

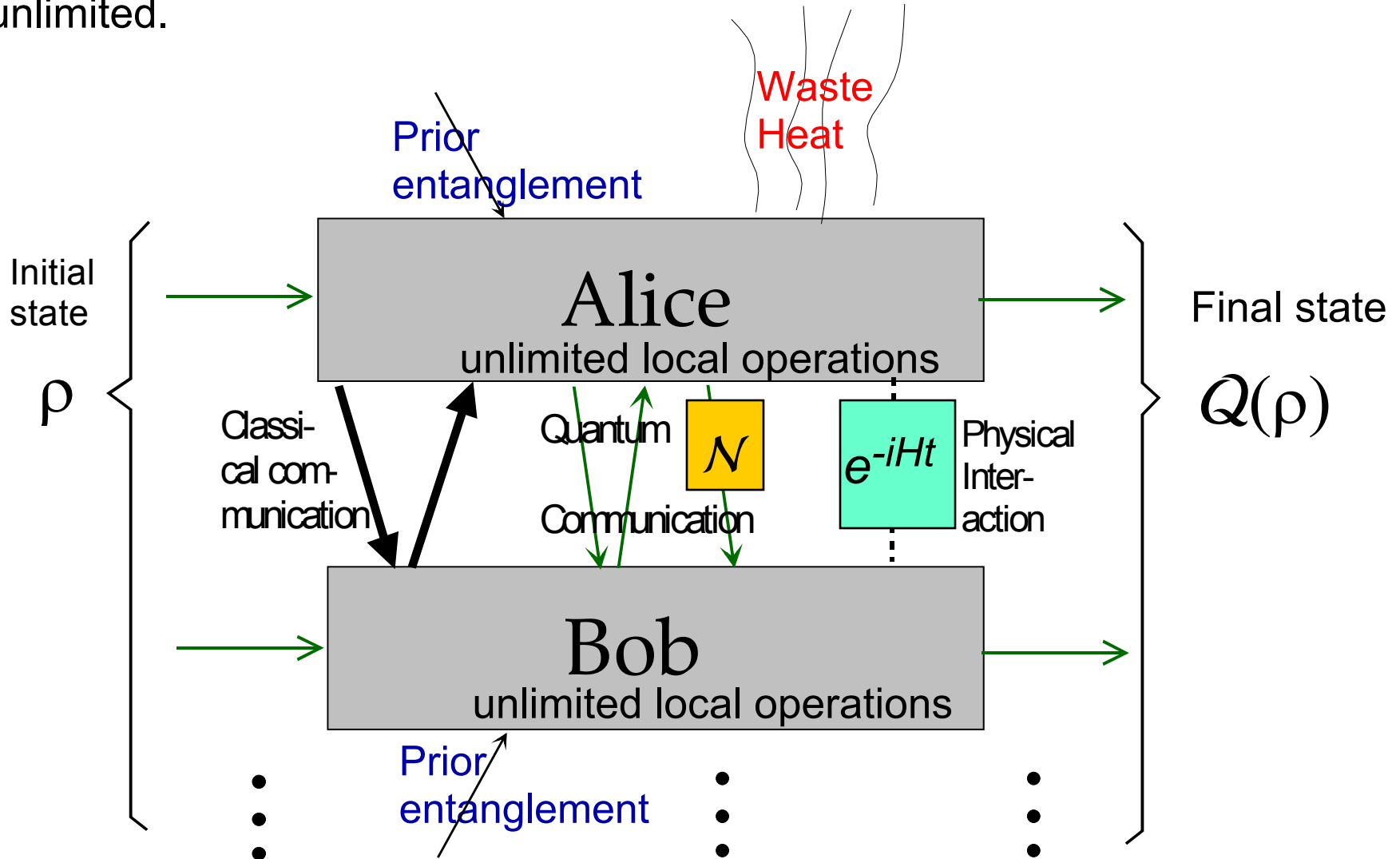
## Quantum Superdense Coding Wiesner, BW92



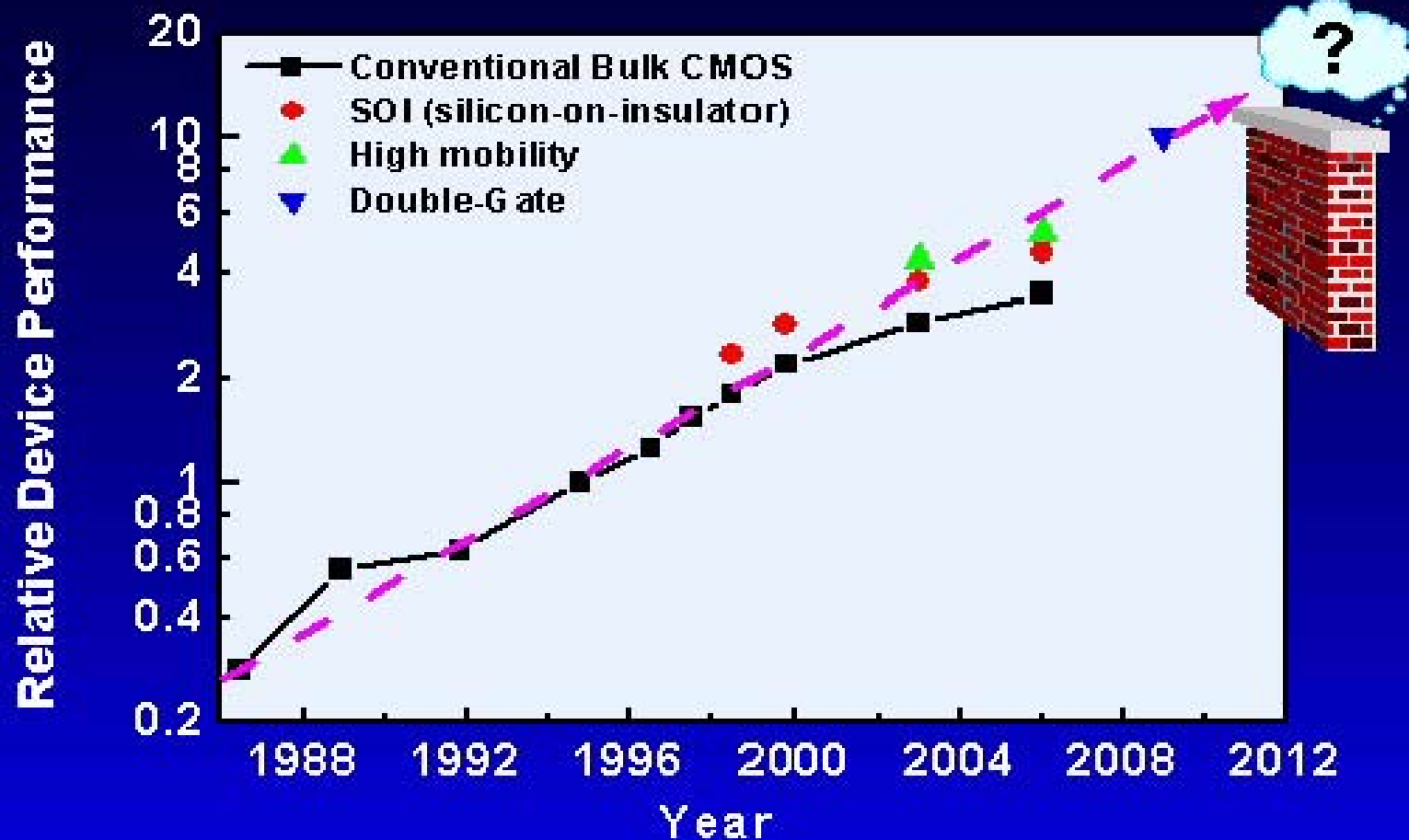
Here Alice does  
the Pauli rotation  
and Bob does the  
Bell measurement.

doubles the classical capacity of any noiseless quantum channel

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



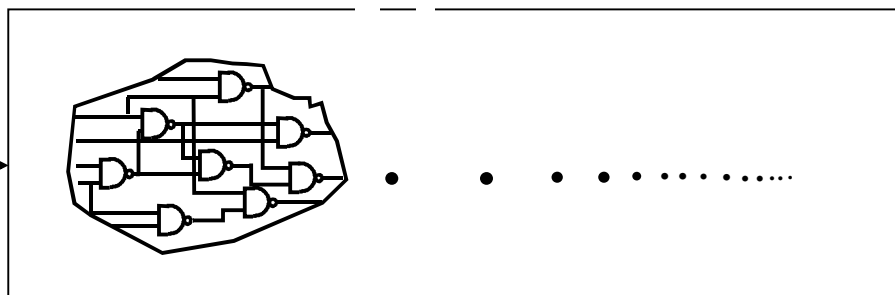
*Computer performance has been increasing exponentially for several decades (Moore's law). But this can't go on for ever. Can quantum computers give Moore's law a new lease on life? If so, how soon will we have them?*



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

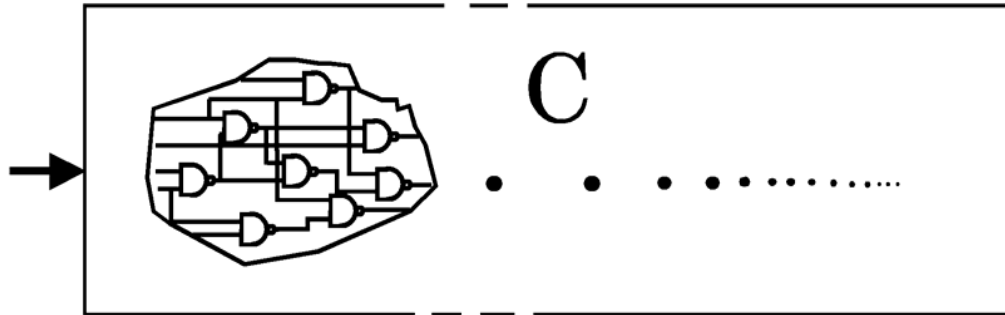
3276913299326670954  
9961988190834461413  
1776429679929425397  
98288533

Some computations require a great many intermediate steps to get to the answer. Factoring large integers is in NP but believed not to be in P. This factoring job took 8 months on hundreds of computers.

(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

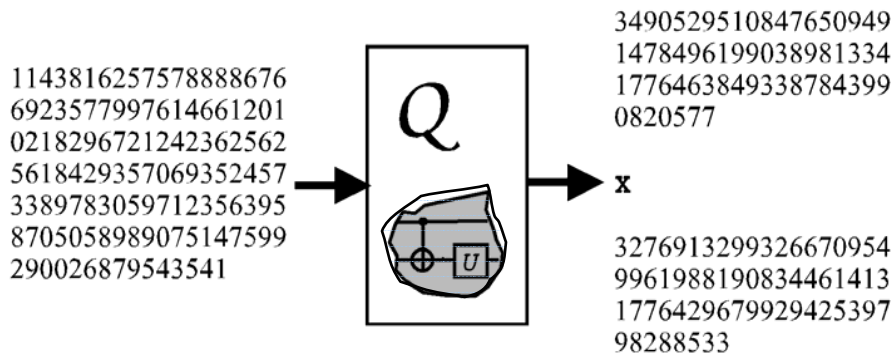


## Factors

3490529510847650949  
1478496199038981334  
1776463849338784399  
0820577

**x**  
3276913299326670954  
9961988190834461413  
1776429679929425397  
98288533

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

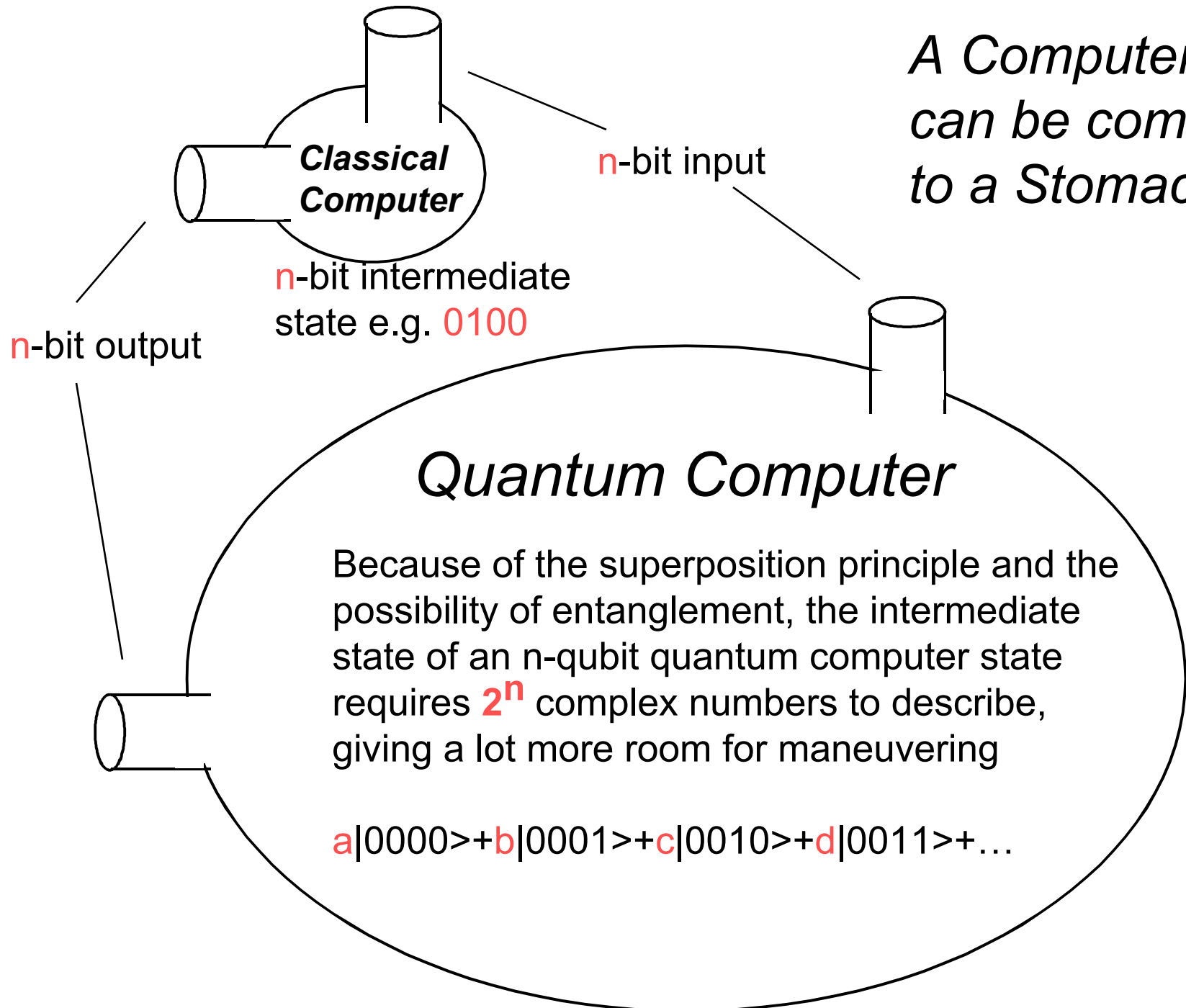


Exponential speedup  
for Factoring (Shor algorithm)

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<br>required<br>to specify<br>a state | $n$ bits | $n$ real<br>numbers | $2^n$ complex<br>numbers |
| Information<br>extractable<br>from state         | $n$ bits | $n$ real<br>numbers | $n$ bits                 |
| Good error<br>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

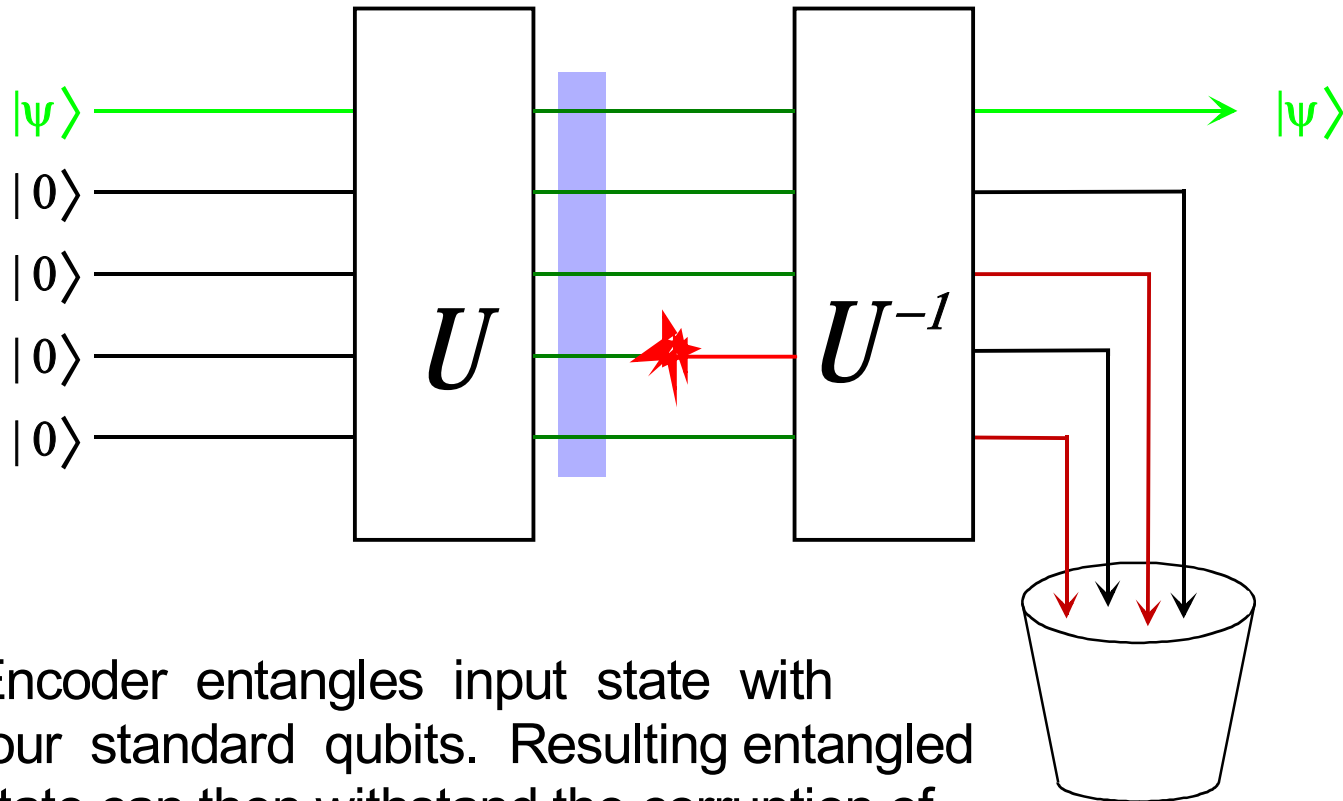
**Quantum Error Correcting Codes**

**Entanglement Distillation**

**Quantum Fault-Tolerant Circuits**

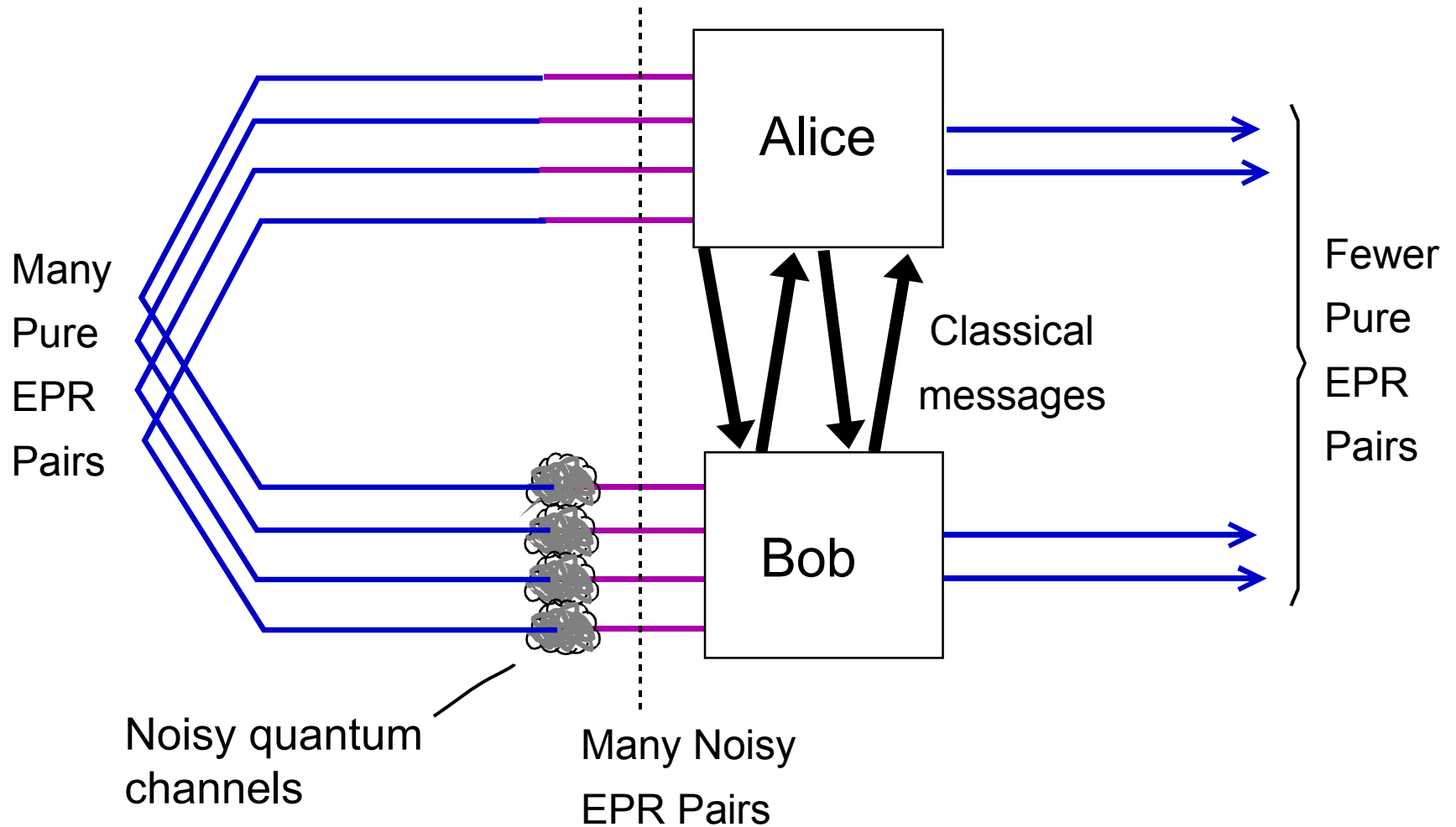
These techniques, combined with hardware improvements, will probably allow practical quantum computers to be built, but not any time soon.

# The Simplest Quantum Error-Correcting Code

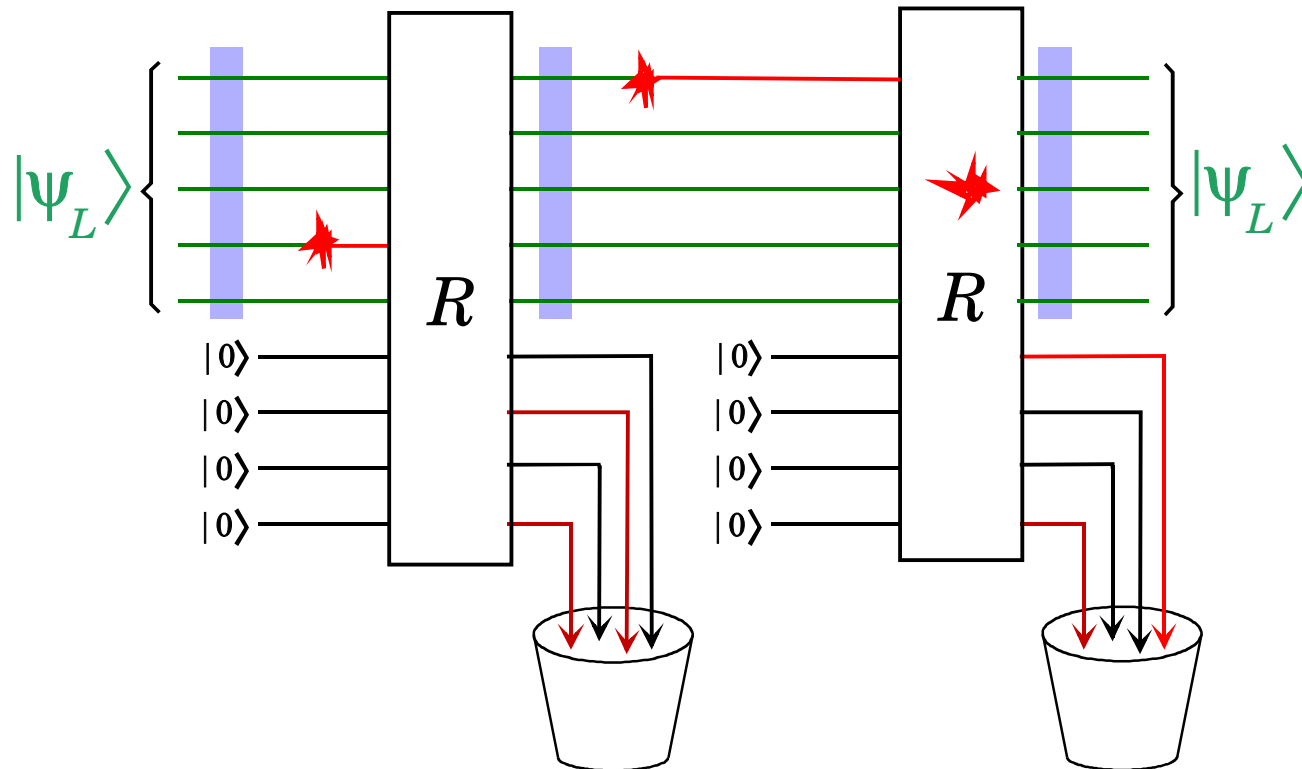


Encoder entangles input state with four standard qubits. Resulting entangled state can then withstand the corruption of any one of its qubits, and still allow recovery of the exact initial state by a decoder at the receiving end of the channel

# Entanglement Distillation

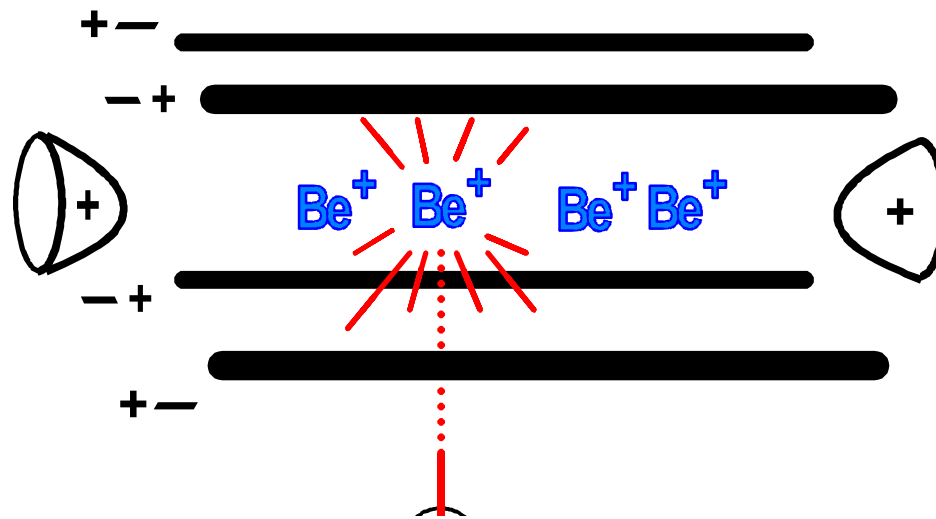


# Quantum Fault Tolerant Computation



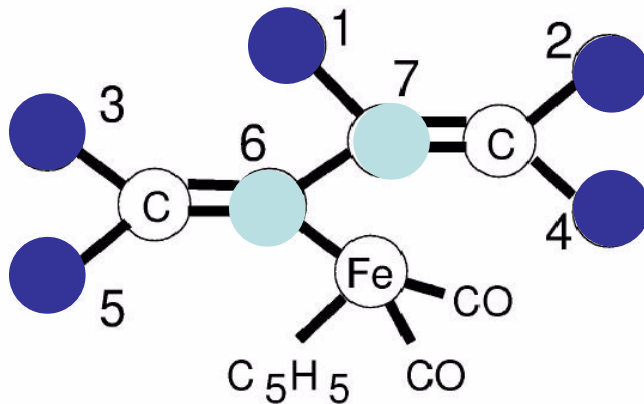
Clean qubits are brought into interaction with the quantum data to siphon off errors, even those that occur during error correction itself.

# Some proposed physical implementations of quantum computing



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

~~4~~  
5



**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

# Five Criteria for physical implementation of a quantum computer

---

1. Well defined extendible qubit array -stable memory
2. Preparable in the “000...” state
3. Long decoherence time ( $> 10^4$  operation time)
4. Universal set of gate operations
5. Single-quantum measurements

D. P. DiVincenzo, in Mesoscopic Electron Transport, eds. Sohn, Kowenhoven, Schoen (Kluwer 1997), p. 657, cond-mat/9612126; “The Physical Implementation of Quantum Computation,” quant-ph/0002077.

## *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.



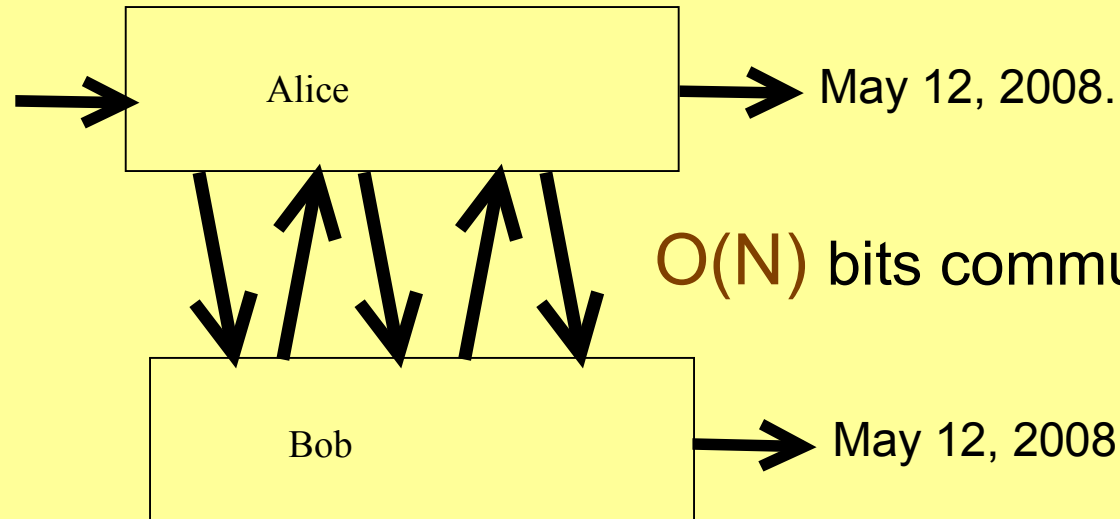
But quantum information is good for many other things besides speeding up computation.

- 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.

Other things quantum information good for, besides speeding up some computations and guaranteeing privacy:

## Reducing Communication Complexity, as in the lunch scheduling problem

When can we  
meet for lunch?



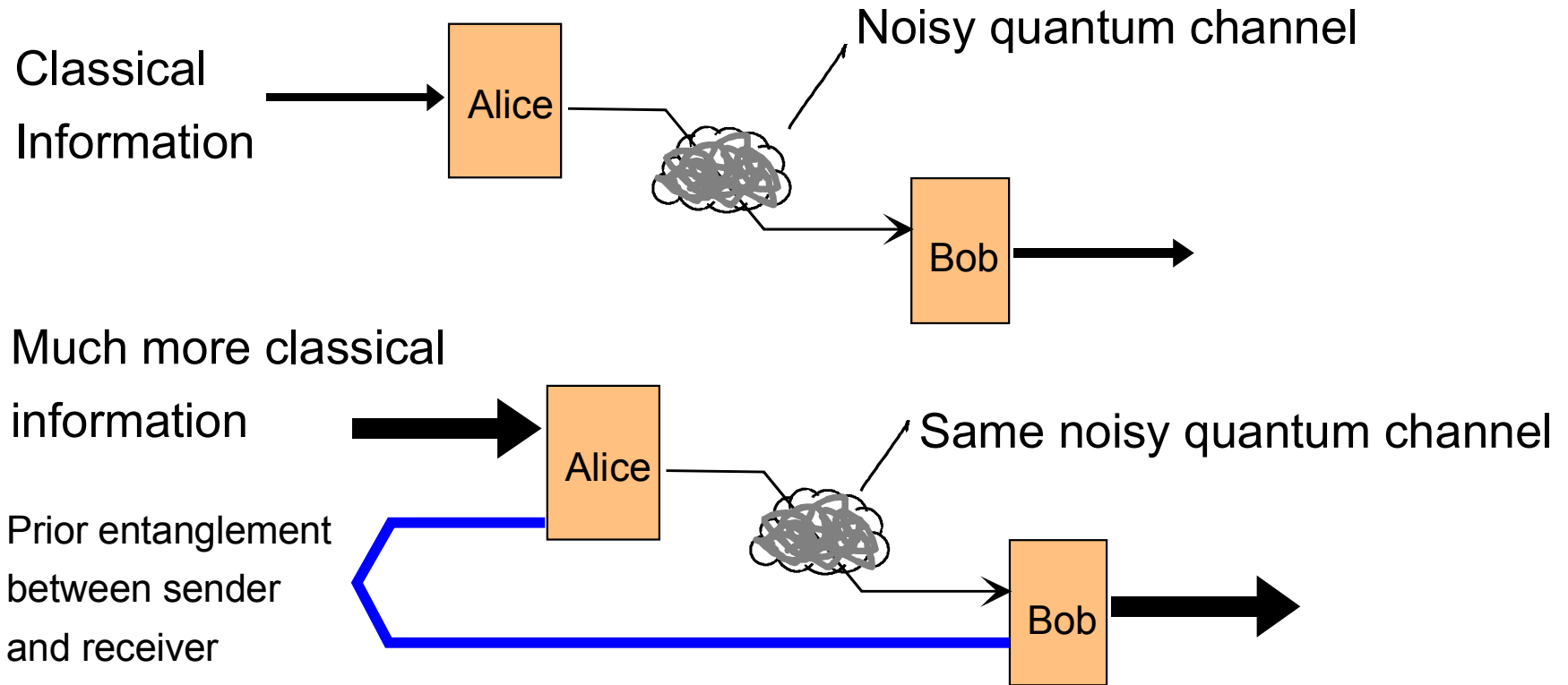
$O(N)$  bits communication

Quantum communication cost is only  $O(\sqrt{N})$  bits.

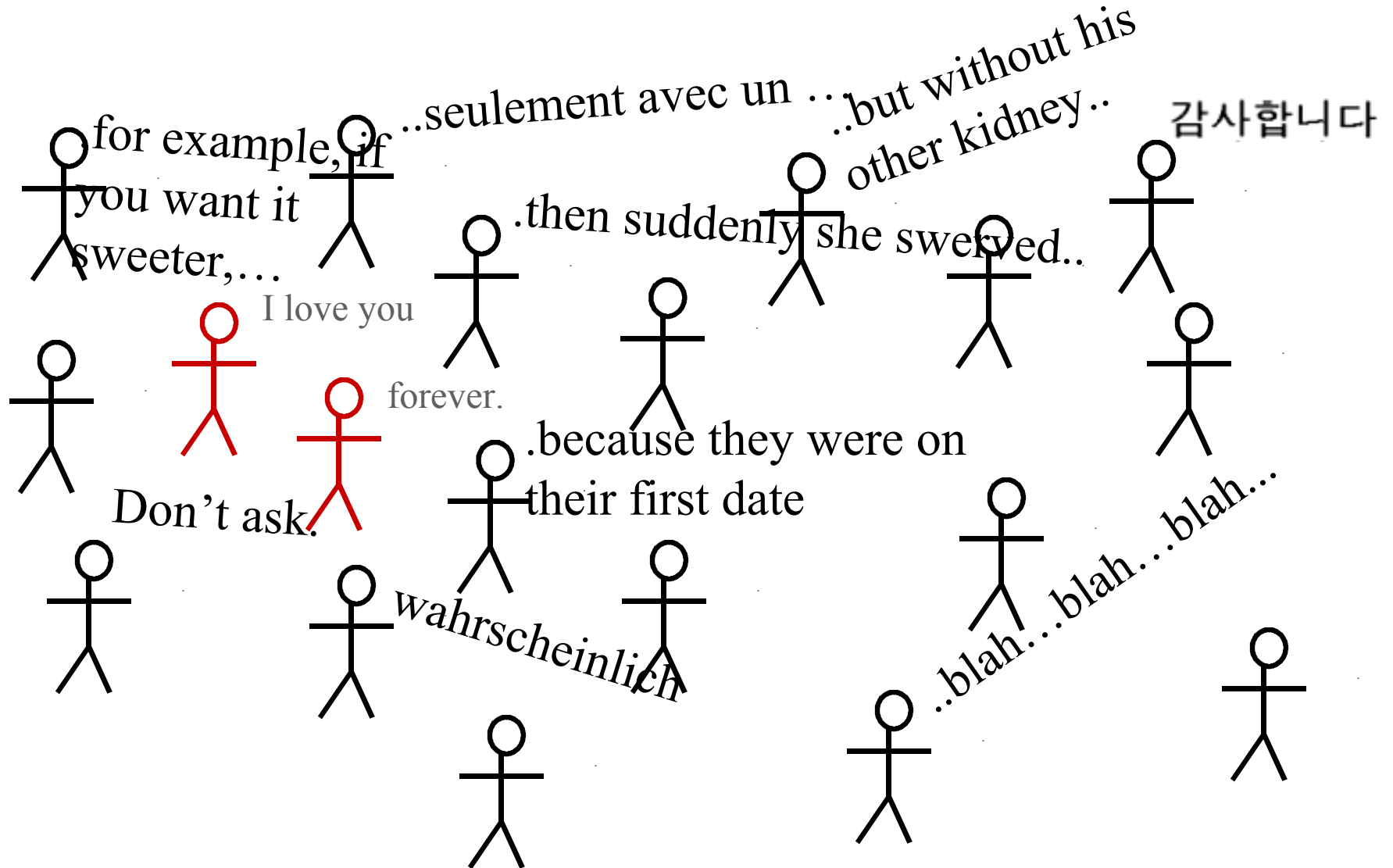
(Buhrman, Cleve and Wigderson)

# Entanglement Assisted Communication

Entanglement cannot itself be used to communicate, but it increases the amount of classical information that can be sent through some noisy quantum channels, and allows quantum information to be sent through classical channels.

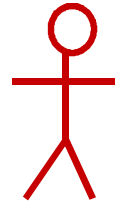


Prior shared entanglement helps a good deal if Alice and Bob are trying to hold a quiet conversation in a room full of noisy strangers (Gaussian channel in low signal, high noise, low-attenuation limit)

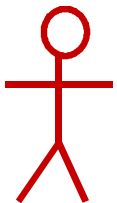


But it doesn't help much if they are far apart in an empty room  
(attenuation)

What?



I love you

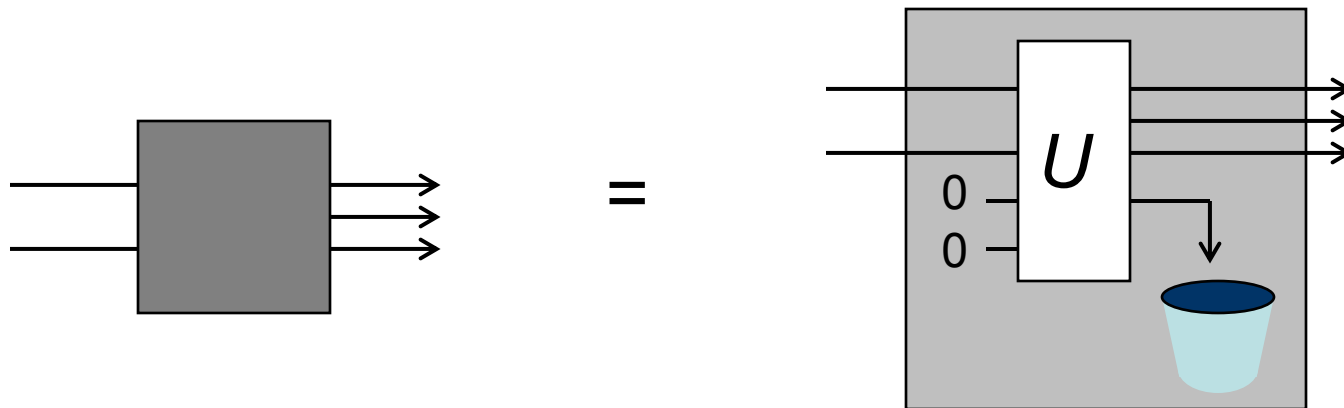


*Quantum Religion:  
Entanglement and  
the origin of  
Randomness*

Unitary evolution of an isolated quantum system is deterministic and reversible, preserving distinguishability.

But quantum systems undergoing measurement or other interactions with an environment can behave randomly, and undergo irreversible loss of distinguishability.

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.



# *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  $\psi_1, \psi_2 \dots$  with probabilities  $p_1, p_2 \dots$

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*

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

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

for a subsystem

$$(\rho = |\psi\rangle\langle\psi| \quad \text{for a pure state})$$

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

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

# ***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  $\rho$  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  $\psi_i$ .

(Hughston-Jozsa-Wootters/Schroedinger theorem)

## *Schmidt Decomposition*

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

$$\Psi(AB) = \sum_i \lambda_i^{1/2} |\alpha_i\rangle |\beta_i\rangle,$$

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

and  $\lambda_i$  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*

$$S(\rho) = -\text{Tr } \rho \log \rho.$$

= Shannon entropy  
of eigenvalues of  $\rho$

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  $\psi$  is degraded by noise,  
the result is a mixed state  $\rho$ . The degree  
resemblance or *fidelity* of  $\psi$  to  $\rho$  is

$$F = \langle \psi | \rho | \psi \rangle$$

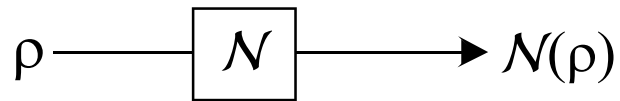
# The Church of the Larger Hilbert Space

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:

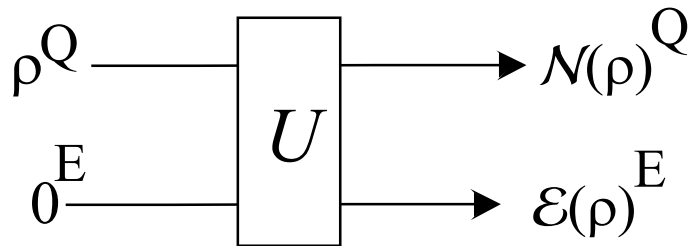
This doctrine only makes sense in a quantum context, where because of entanglement a pure whole can have impure parts: Classically; a whole can be no purer than its most impure part.

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.



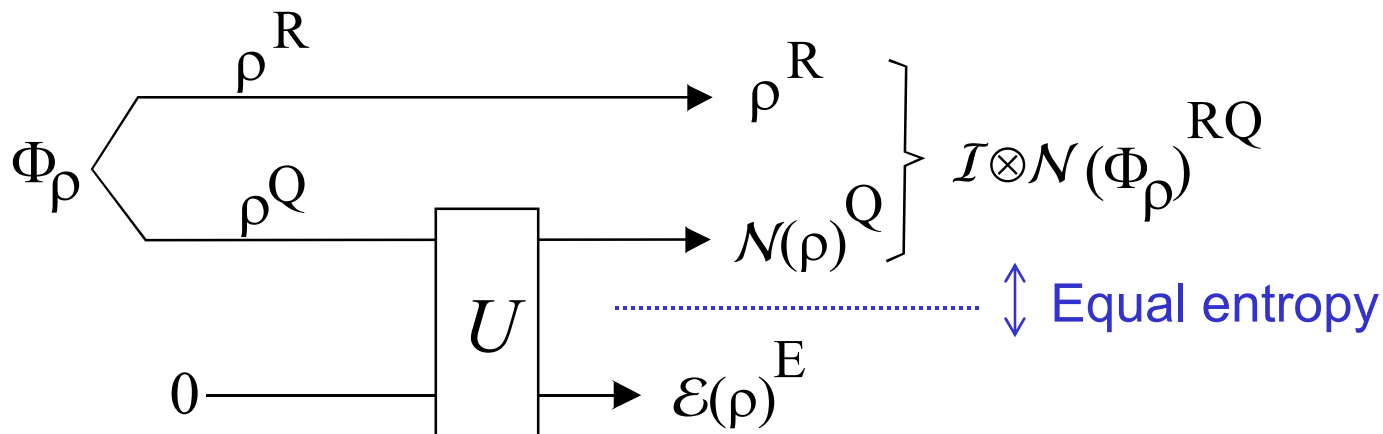
Noisy channel viewed as interaction with environment



Input viewed as entangled with a reference system R

CLHS invoked to purify noisiness of channel

CLHS invoked again to purify mixedness of input



# 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)

*Quantum Laws and  
the Universality of  
Interaction*

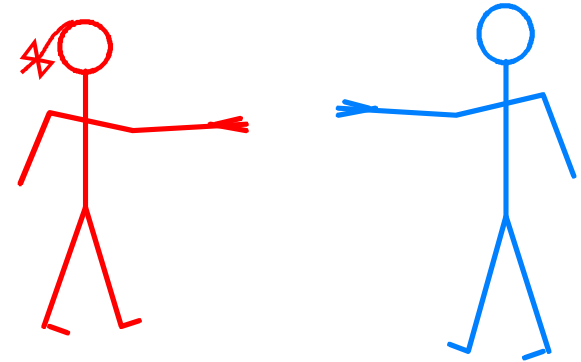


One way in which quantum laws are simpler than classical is the universality of interaction.

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.

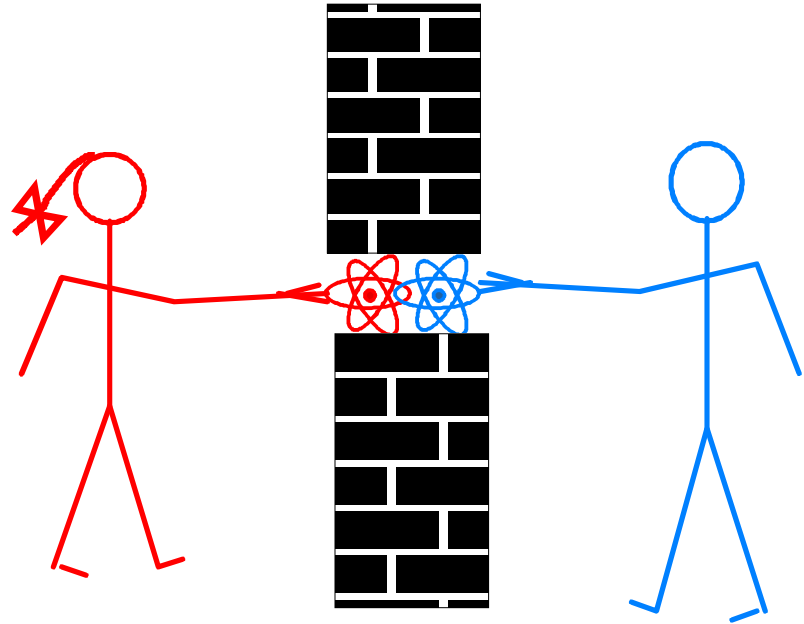
*Fortunately*, they live next door to one another.

*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  $H'$ .

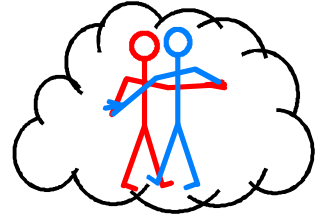


*Fortunately*, Alice and Bob know quantum mechanics. They know that any interaction can be used to create entanglement, and that interactions are intrinsically bidirectional and private: A cannot affect B without B affecting A. If C interferes or eavesdrops, the joint state of A and B will be degraded 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  $\mathbf{H}'$  but by the many-atom interaction  $\mathbf{H}$ , which is a physicist's way of saying always being in each other's arms.

How can they use the available  $\mathbf{H}'$  to simulate the desired  $\mathbf{H}$  ?



They can of course separately prepare their respective interacting atoms in any initial states, and thereafter alternate through-the-wall interactions under  $\mathbf{H}'$  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  $\mathbf{H}'$  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.

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 --

*How do  
Quantum  
Speedups  
Work?*

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 denoted  $r_a$ .



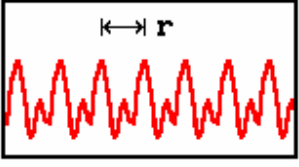
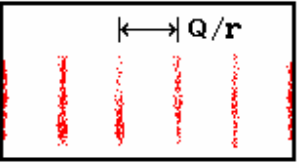
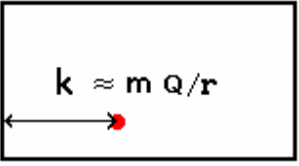
Any algorithm for calculating  $r_a$  from  $a$  can be converted to an algorithm for factoring  $N$ .

All known classical ways of finding  $r_a$  from  $a$  are hard.

But it can be done easily on a quantum computer.



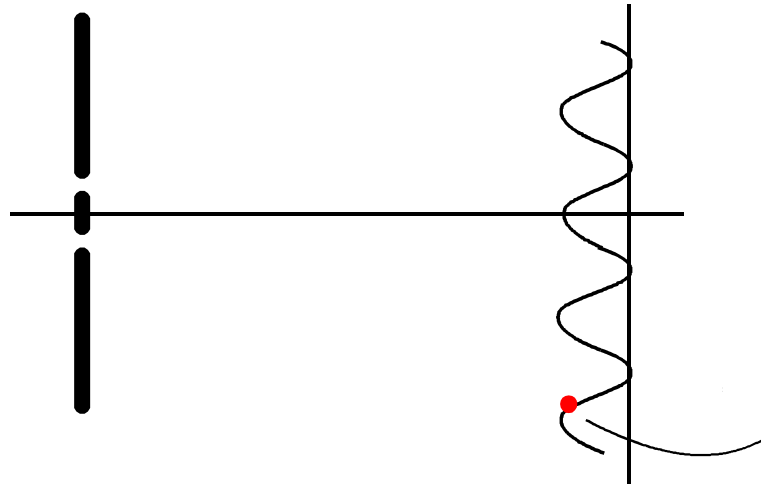
# Shor's Quantum Super-Fast Fourier Sampling

|   | State   | Action                                |
|---|---|---------------------------------------|
|    | $x$ Register<br>$y$ Register<br>$ 0, 0\rangle$                            | Initial State                         |
|    | $\frac{1}{\sqrt{Q}} \sum_x  x, 0\rangle$                                  | Generate $x$ superposition            |
|    | $\frac{1}{\sqrt{Q}} \sum_x  x, f(x)\rangle$                               | Reversibly compute<br>$y := y + f(x)$ |
|   | $\frac{1}{Q} \sum_{x,k} e^{2\pi i k x / Q}  k, f(x)\rangle$               | Fourier Transform<br>$x$ register     |
|  | <p>Measure<br/><math>x</math> register</p> <p>Result = <math>k</math></p> |                                       |

$r$  = numerator of  $r/m$ , where  $r/m$  = closest rational approximation to  $Q/K$  with denominator less than  $\sqrt{Q}$

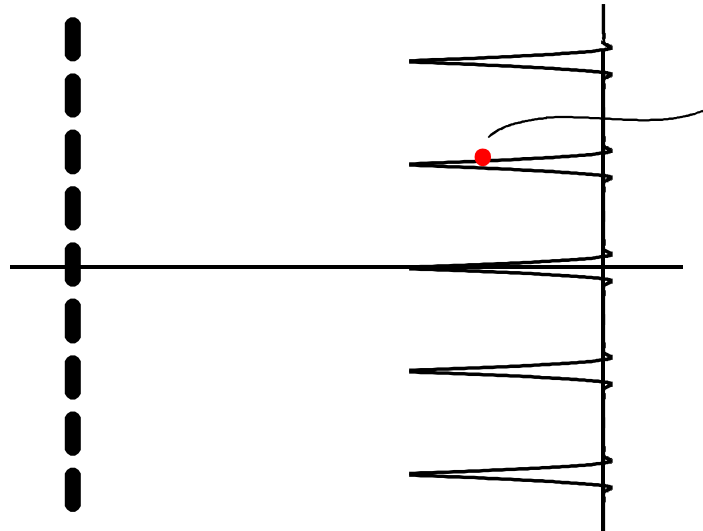
Shor algorithm uses interference to find unknown period of periodic function.

2 Slits  
1 photon



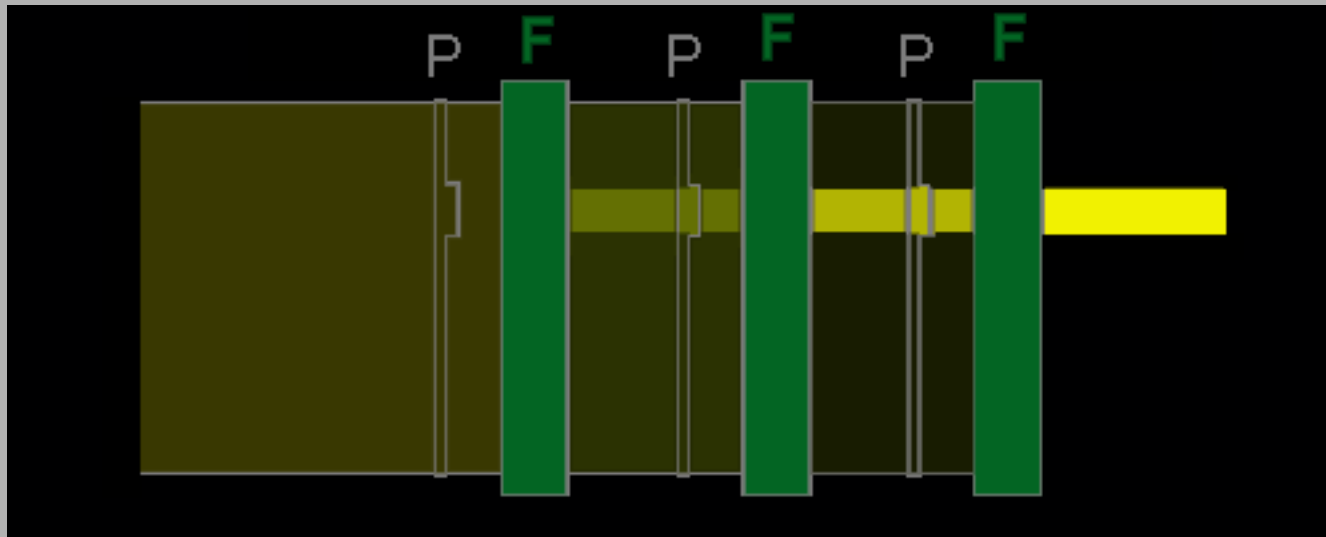
Photon impact point yields a  
little information about slit  
spacing

N Slits  
1 photon



Photon impact point yields a  
lot of information about slit  
spacing

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.

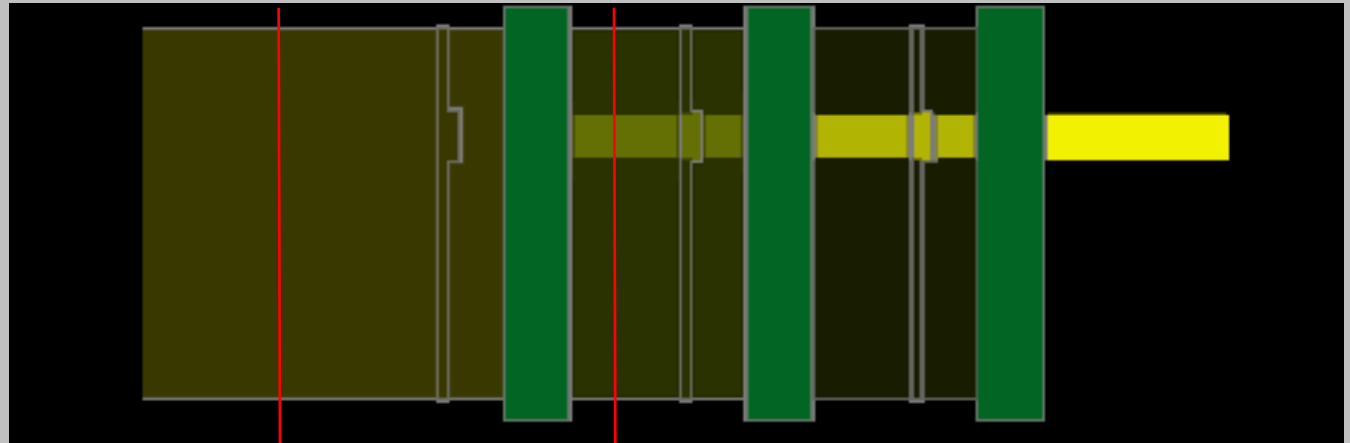


P = phase plate  
F = fixed optics

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?

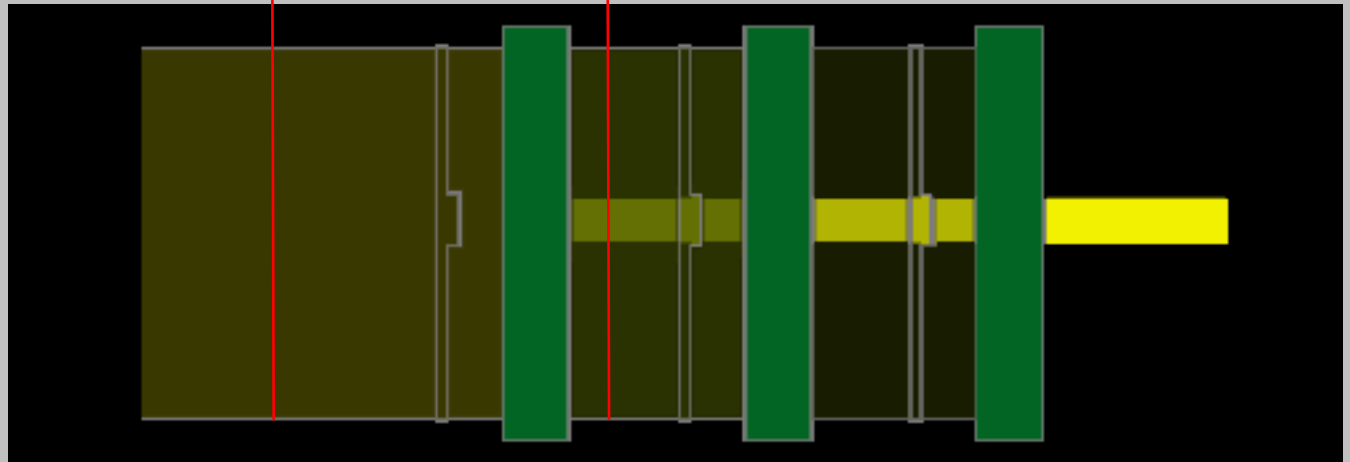
Original optical Grover experiment.



*No difference initially*

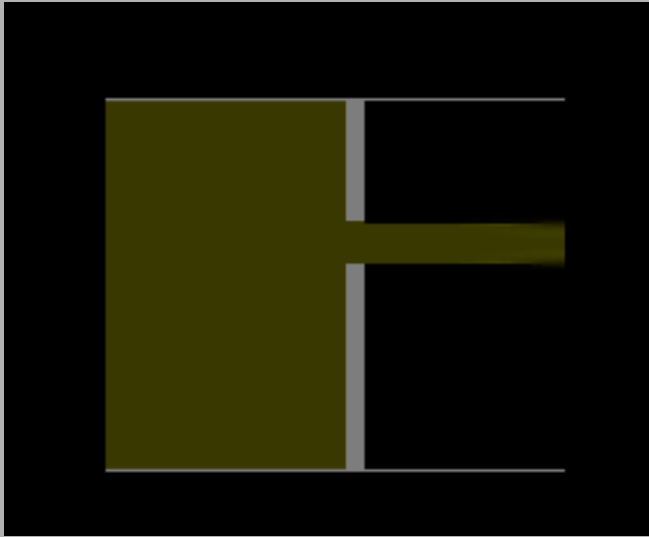
*Small difference after 1 iteration*

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

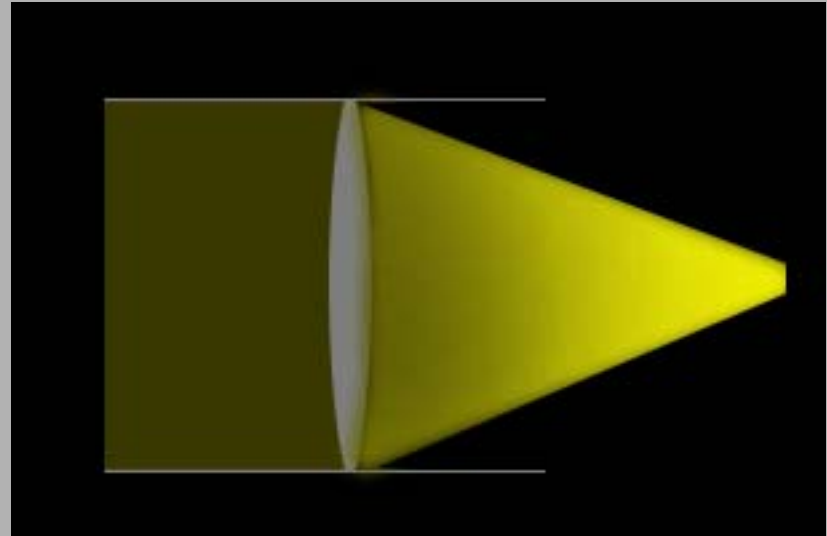


Because most of the beam misses the bump in either location, the difference between the two light fields can increase only slowly. About  $\sqrt{N}$  iterations are required to get complete separation. (BBBV quant-ph/9701001)

## 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.