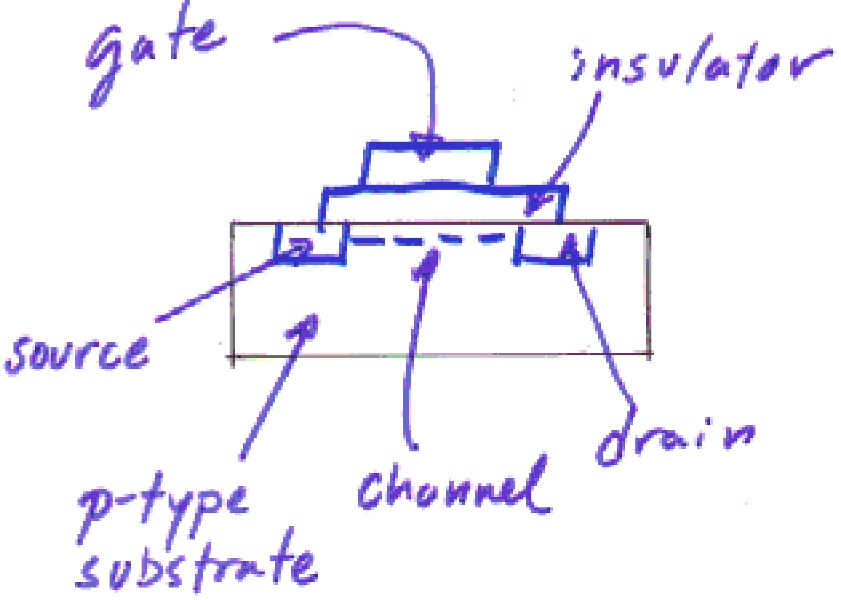
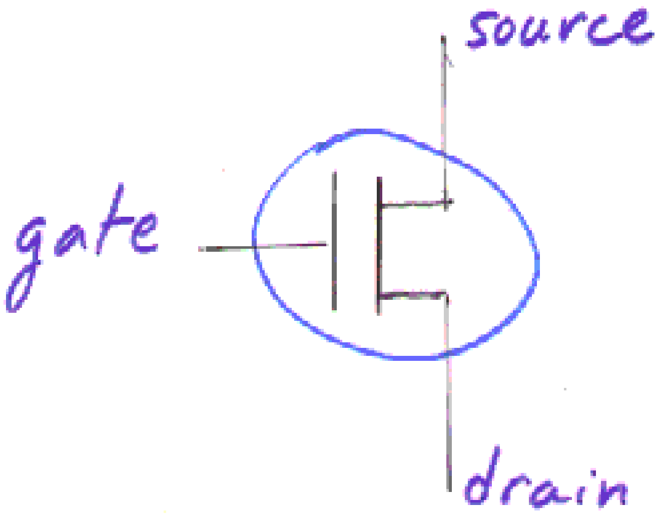
6/13/01

Putting Quantum Weirdness to Work: An Introduction to Quantum Computing

Nick Bonesteel, FSU Physics

At the heart of the information age is... **The Transistor**



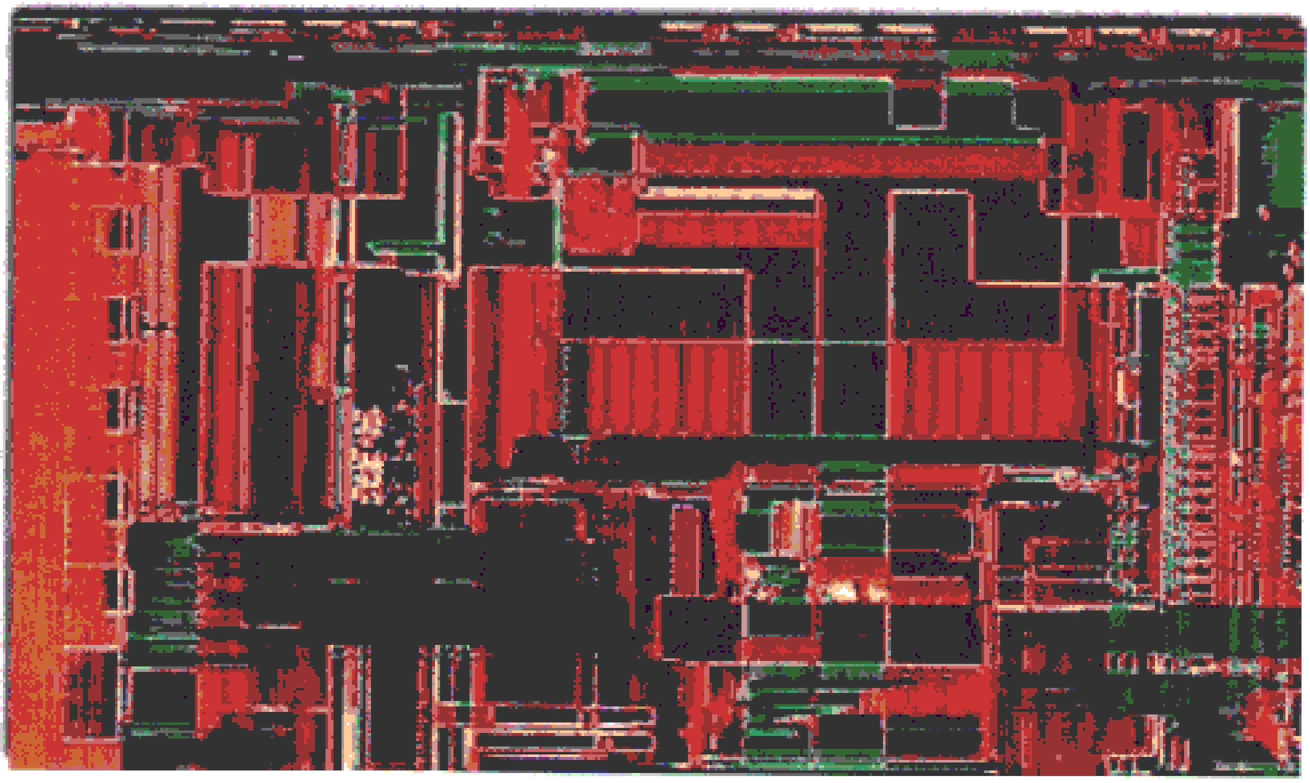


Applying a voltage V_{gate} to the gate allows current to flow from source to drain.

$$\begin{array}{l} V_{gate} > V_T \longrightarrow 1 \\ V_{gate} < V_T \longrightarrow \underbrace{0}_{\text{1 bit of information}} \end{array}$$

The Transistor + Lithography

= The Integrated Circuit

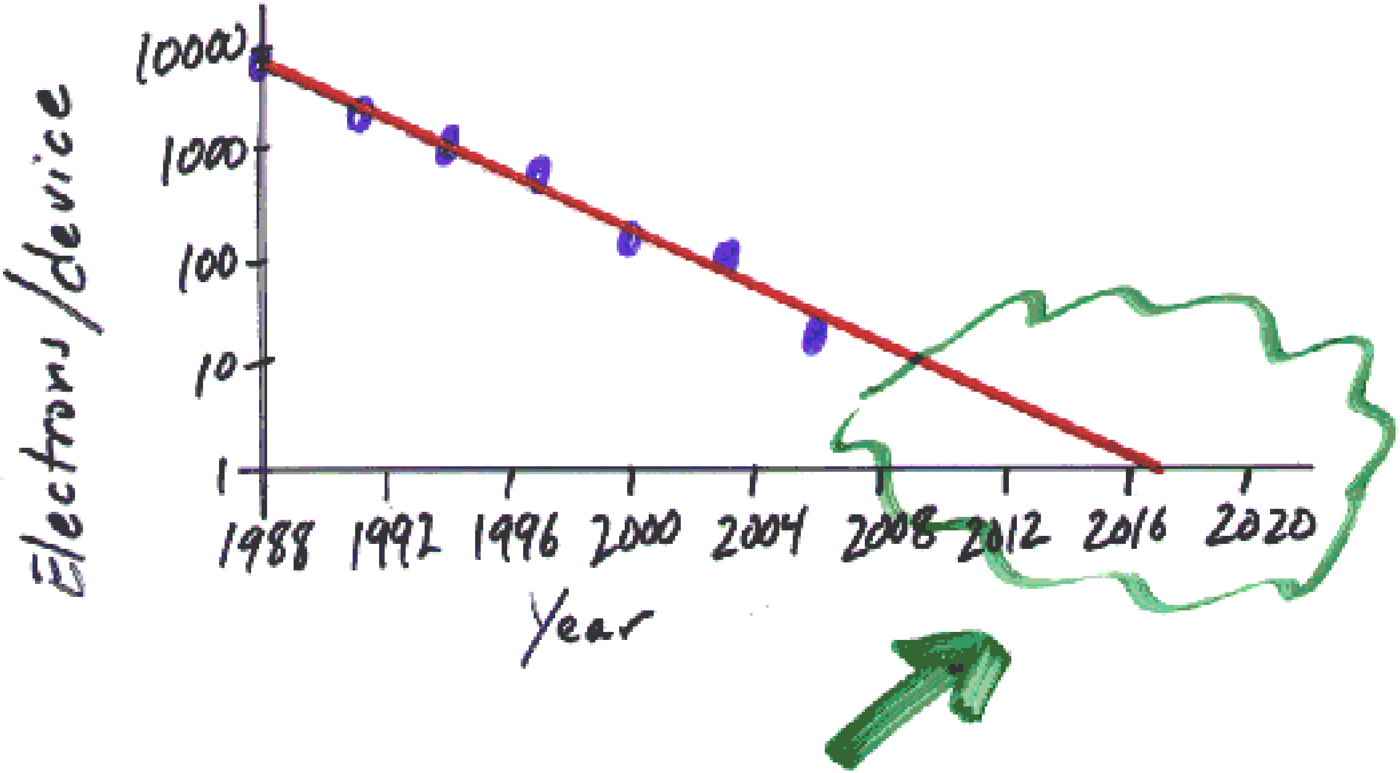


Chip features ~ 0.35 microns

The Pentium III Chip

- 28,000,000 transistors.
- Difference between a 0 and a 1 is ~ 10,000 electrons.

Moore's law



The Quantum World !

From Bits to Qubits

- Qubit = Quantum bit.
- Simplest example: A spin-$\frac{1}{2}$ particle, (e.g. electron, neutron, ...)

Two Quantum States

Up spin: $\uparrow \rightarrow |0\rangle$

Down spin: $\downarrow \rightarrow |1\rangle$

Unlike a bit, a qubit can be placed in a quantum superposition of $|0\rangle$ and $|1\rangle$.

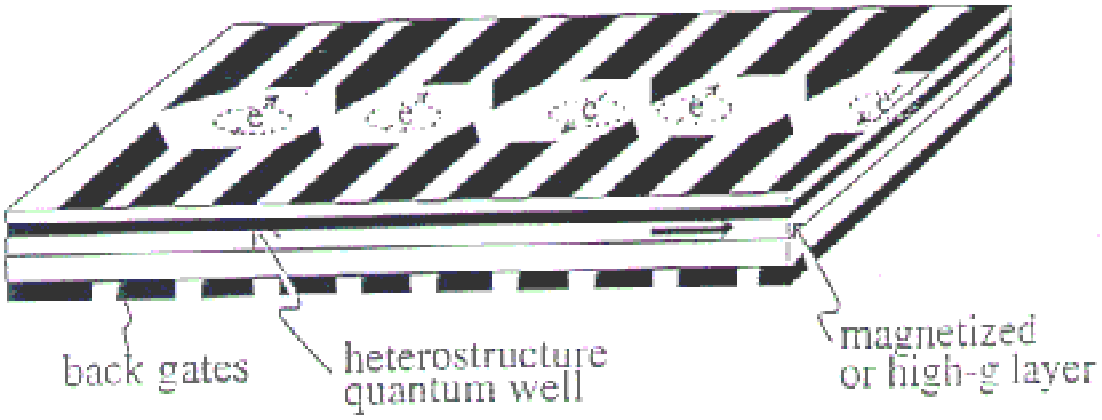
$$\rightarrow \boxed{|\psi\rangle = \alpha|0\rangle + \beta|1\rangle}$$

The Quantum Computer

A computer which manipulates qubits according to the laws of quantum mechanics.

One possible realization,

Quantum Dot Computer



Other proposals

- Trapped ions
- Nuclear spins (NMR)

⋮

Quantum Computing "Weirdness"

A single qubit in the state

$$|0\rangle$$

can be "rotated" into the state

$$|0\rangle + |1\rangle$$

If each of two qubits initially in the state

$$|0\rangle|0\rangle$$

are rotated to $|0\rangle + |1\rangle$ the final state is

$$(|0\rangle + |1\rangle)(|0\rangle + |1\rangle)$$

$$= |0\rangle|0\rangle + |0\rangle|1\rangle + |1\rangle|0\rangle + |1\rangle|1\rangle$$

The N qubit state

$$\underbrace{|0\rangle|0\rangle|0\rangle\cdots}_{N \text{ qubits}}$$

becomes

$$(|0\rangle+|1\rangle)(|0\rangle+|1\rangle)(|0\rangle+|1\rangle)\cdots$$

$$\underline{\text{binary rep. of } k}$$

$$= |0\rangle|0\rangle|0\rangle\cdots \rightarrow k=0$$

$$+ |1\rangle|0\rangle|0\rangle\cdots \rightarrow k=1$$

$$+ |0\rangle|1\rangle|0\rangle\cdots \rightarrow k=2$$

$$+ |1\rangle|1\rangle|0\rangle\cdots \rightarrow k=3$$

$$\vdots \qquad\qquad \vdots$$

$$\boxed{= \sum_{k=0}^{2^N-1} |k\rangle}$$

For $N=100$,

$$\underline{2^N \simeq 10^{30}}\;!!$$

Massive Quantum Parallelism

Let F be a subroutine which calculates the function $f(k)$.

$$F\left[\sum_{k=0}^{2^N-1} |k\rangle\right] \Rightarrow \sum_{k=0}^{2^N-1} |f(k)\rangle$$

In a single run of F the function f has been evaluated for 2^N inputs !!!

But... Measurement collapses the wave function;

$$\sum_{k=0}^{2^N-1} |f(k)\rangle \xrightarrow[\text{measure qubits}]{} |f(k_0)\rangle$$

No free lunch!

However... In 1994 Peter Shor found a free lunch hidden in this state.

Prime factorization

Given two prime numbers p and q,

$p \times q = C$ Easy

$C \rightarrow p, q$ Hard

Best known factorization algorithm scales as,

$$\# \text{ of steps} \sim \exp(\# \text{ of digits})$$

→ Mathematical basis of public-key cryptography.

Quantum Factoring

$$|0\rangle\otimes|0\rangle \rightarrow \sum_{k=0}^{Q-1}|k\rangle\otimes|0\rangle$$

$Q=2^N$

$$U_A\left(\sum_{k=0}^{Q-1}|k\rangle\otimes|0\rangle\right)=\sum_{k=0}^{Q-1}|k\rangle\otimes|x^k \bmod \underline{C}\rangle$$

$x<C$

measure left register

$$U_{FT}\left(\sum_{m=0}^{M-1}|l+mr\rangle\right)=\sum_{m=0}^{r}\left|m\frac{Q}{r}\right\rangle$$

measure

$$m\frac{Q}{r}\longrightarrow r$$

Can show $x^{r/2}\pm 1$ shares a common factor with C,

→ Prime Factors

Classical Factoring

$$\#\text{ of steps} \sim \exp(\#\text{ of digits})$$

Quantum Factoring

$$\#\text{ of steps} \sim (\#\text{ of digits})^3$$

➜ **Exponential Quantum Speed Up!**

Other algorithms?

- Grover's search algorithm searches an N item database in $\sqrt{N}$ steps.

Other free lunches? Unknown

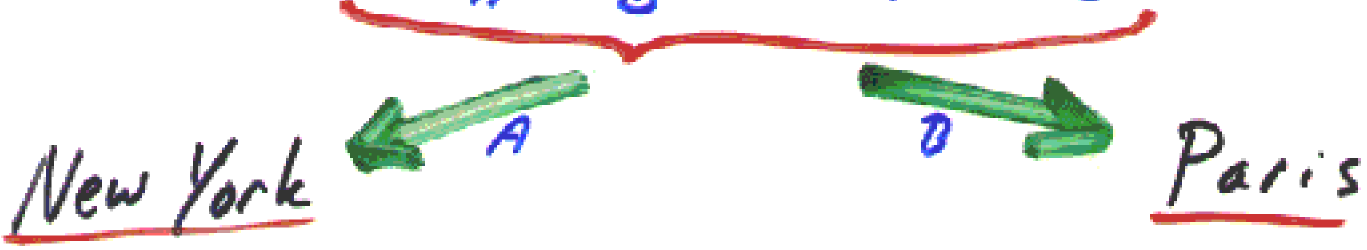
Q: Where do quantum computers get their power?

A: We don't know, but part of the story is...

Entanglement

Two qubits can be placed in the state,

$$|0\rangle_A |1\rangle_B - |1\rangle_A |0\rangle_B$$



New York

Paris

Einstein was very upset that measuring a qubit in New York could instantly collapse the state of a qubit in Paris.

Bell's Inequality

- Inequality on correlations in entangled states required by local realism, but violated by quantum mechanics.
- Experiments confirm quantum theory.

While carrying out Shor's algorithm the state of a quantum computer becomes highly entangled. Somehow the algorithm exploits the quantum "weirdness" of entangled states to factor integers.

PHYSICAL REVIEW LETTERS

VOLUME 81 7 DECEMBER 1998 NUMBER 23

Violation of Bell's Inequality under Strict Einstein Locality Conditions

Gregor Weihs, Thomas Jennewein, Christoph Simon, Harald Weinfurter, and Anton Zeilinger
Institut für Experimentalphysik, Universität Innsbruck, Technikerstraße 25, A-6020 Innsbruck, Austria

(Received 6 August 1998)

We observe strong violation of Bell's inequality in an Einstein-Podolsky-Rosen-type experiment with independent observers. Our experiment definitely implements the ideas behind the well-known work by Aspect *et al.* We for the first time fully enforce the condition of locality, a central assumption in the derivation of Bell's theorem. The necessary spacelike separation of the observations is achieved by sufficient physical distance between the measurement stations, by ultrafast and random setting of the analyzers, and by completely independent data registration. [S0031-9007(98)07901-0]

PACS numbers: 03.65.Bz

The stronger-than-classical correlations between entangled quantum systems, as first discovered by Einstein, Podolsky, and Rosen (EPR) in 1935 [1], have ever since occupied a central position in the discussions of the foundations of quantum mechanics. After Bell's discovery [2] that EPR's implication to explain the correlations using hidden parameters would contradict the predictions of quantum physics, a number of experimental tests have been performed [3–5]. All recent experiments confirm the predictions of quantum mechanics. Yet, from a strictly logical point of view, they don't succeed in ruling out a local realistic explanation completely, because of two essential loopholes. The first loophole builds on the fact that all experiments so far detect only a small subset of all pairs created [6]. It is therefore necessary to assume that the pairs registered are a fair sample of all pairs emitted. In principle this could be wrong and once the apparatus is sufficiently refined the experimental observations will contradict quantum mechanics. Yet we agree with Bell [7] that "*... it is hard for me to believe that quantum mechanics works so nicely for inefficient practical set-ups and is yet going to fail badly when sufficient refinements are made. Of more importance, in my opinion, is the complete absence of the vital time factor in existing experiments. The analyzers are not rotated during the flight of the particles.*"

This is the second loophole which so far has only been encountered in an experiment by Aspect *et al.* [4] where the directions of polarization analysis were switched after the photons left the source. Aspect *et al.*, however, used periodic sinusoidal switching, which is predictable into the future. Thus communication slower than the speed of light, or even at the speed of light [8], could in principle explain the results obtained. Therefore this second loophole is still open.

The assumption of locality in the derivation of Bell's theorem requires that the individual measurement processes of the two observers are spacelike separated (Fig. 1). We define an individual measurement to last from the first point in time which can influence the choice of the analyzer setting until the final registration of the photon. Such an individual measurement then has to be so quick that it is impossible for any information about it to travel via any (possibly unknown) channel to the other observer before he, in turn, finishes his measurement [9]. Selection of an analyzer direction has to be completely unpredictable, which necessitates a physical random number generator. A pseudo-random-number generator cannot be used, since its state at any time is predetermined. Furthermore, to achieve complete independence of both observers, one should avoid any common context as would be conventional registration of coincidences as in all previous experiments [10]. Rather the individual events should be registered on both sides independently and compared only after the measurements are finished. This requires independent and highly accurate time bases on both sides.

Experimental quantum teleportation

Dik Bouwmeester, Jian-Wei Pan, Klaus Mattle, Manfred Eibl, Harald Weinfurter & Anton Zeilinger

Institut für Experimentalphysik, Universität Innsbruck, Technikerstr. 25, A-6020 Innsbruck, Austria

Quantum teleportation—the transmission and reconstruction over arbitrary distances of the state of a quantum system—is demonstrated experimentally. During teleportation, an initial photon which carries the polarization that is to be transferred and one of a pair of entangled photons are subjected to a measurement such that the second photon of the entangled pair acquires the polarization of the initial photon. This latter photon can be arbitrarily far away from the initial one. Quantum teleportation will be a critical ingredient for quantum computation networks.

The dream of teleportation is to be able to travel by simply reappearing at some distant location. An object to be teleported can be fully characterized by its properties, which in classical physics can be determined by measurement. To make a copy of that object at a distant location one does not need the original parts and pieces—all that is needed is to send the scanned information so that it can be used for reconstructing the object. But how precisely can this be a true copy of the original? What if these parts and pieces are electrons, atoms and molecules? What happens to their individual quantum properties, which according to the Heisenberg's uncertainty principle cannot be measured with arbitrary precision?

Bennett *et al.*[1] have suggested that it is possible to transfer the quantum state of a particle onto another particle—the process of quantum teleportation—provided one does not get any information about the state in the course of this transformation. This requirement can be fulfilled by using entanglement, the essential feature of quantum mechanics[2]. It describes correlations between quantum systems much stronger than any classical correlation could be.

The possibility of transferring quantum information is one of the cornerstones of the emerging field of quantum communication and quantum computation[3]. Although there is fast progress in the theoretical description of quantum information processing, the difficulties in handling quantum systems have not allowed an equal advance in the experimental realization of the new proposals. Besides the promising developments of quantum cryptography[4] (the first provably secure way to send secret messages), we have only recently succeeded in demonstrating the possibility of quantum dense coding[5], a way to quantum mechanically enhance data compression. The main reason for this slow experimental progress is that, although there exist methods to produce pairs of entangled photons[6], entanglement has been demonstrated for atoms only very recently[7] and it has not been possible thus far to produce entangled states of more than two quanta.

Here we report the first experimental verification of quantum teleportation. By producing pairs of entangled photons by the process of parametric down-conversion and using two-photon interferometry for analysing entanglement, we could transfer a quantum property (in our case the polarization state) from one photon to another. The methods developed for this experiment will be of great importance both for exploring the field of quantum communication and for future experiments on the foundations of quantum mechanics.

The problem

To make the problem of transferring quantum information clearer, suppose that Alice has some particle in a certain quantum state $|\psi\rangle$ and she wants Bob, at a distant location, to have a particle in that state. There is certainly the possibility of sending Bob the particle directly. But suppose that the communication channel between Alice and Bob is not good enough to preserve the necessary quantum coherence or suppose that this would take too much time, which could easily be the case if $|\psi\rangle$ is the state of a more complicated or massive object. Then, what strategy can Alice and Bob pursue?

As mentioned above, no measurement that Alice can perform on $|\psi\rangle$ will be sufficient for Bob to reconstruct the state because the state of a quantum system cannot be fully determined by measurements. Quantum systems are so evasive because they can be in a superposition of several states at the same time. A measurement on the quantum system will force it into only one of these states—this is often referred to as the projection postulate. We can illustrate this important quantum feature by taking a single photon, which can be horizontally or vertically polarized, indicated by the states $|\leftrightarrow\rangle$ and $|\updownarrow\rangle$. It can even be polarized in the general superposition of these two states

$$|\psi\rangle = \alpha|\leftrightarrow\rangle + \beta|\updownarrow\rangle \qquad (1)$$

where α and β are two complex numbers satisfying $|\alpha|^2 + |\beta|^2 = 1$. To place this example in a more general setting we can replace the states $|\leftrightarrow\rangle$ and $|\updownarrow\rangle$ in equation (1) by $|0\rangle$ and $|1\rangle$, which refer to the states of any two-state quantum system. Superpositions of $|0\rangle$ and $|1\rangle$ are called qubits to signify the new possibilities introduced by quantum physics into information science[8].

If a photon in state $|\psi\rangle$ passes through a polarizing beamsplitter—a device that reflects (transmits) horizontally (vertically) polarized photons—it will be found in the reflected (transmitted) beam with probability $|\alpha|^2$ ($|\beta|^2$). Then the general state $|\psi\rangle$ has been projected either onto $|\leftrightarrow\rangle$ or onto $|\updownarrow\rangle$ by the action of the measurement. We conclude that the rules of quantum mechanics, in particular the projection postulate, make it impossible for Alice to perform a measurement on $|\psi\rangle$ by which she would obtain all the information necessary to reconstruct the state.

The concept of quantum teleportation

Although the projection postulate in quantum mechanics seems to bring Alice's attempts to provide Bob with the state $|\psi\rangle$ to a halt, it was realised by Bennett *et al.*[1] that precisely this projection postulate enables teleportation of $|\psi\rangle$ from Alice to Bob. During teleportation Alice will destroy the quantum state at hand while Bob receives the quantum state, with neither Alice nor Bob obtaining information about the state $|\psi\rangle$. A key role in the teleportation scheme is played by an entangled ancillary pair of particles which will be initially shared by Alice and Bob.

For years, she shared recipes with her friend in Osaka.

She showed him hundreds of ways to use paprika.

He shared his secret recipe for sukiyaki.

One day Margit e-mailed Shinji,

"Stand by. I'll teleport you some goulash."

Margit is a little premature, but we are working on it.

An IBM scientist and his colleagues have discovered a way to make an object disintegrate in one place and reappear intact in another.

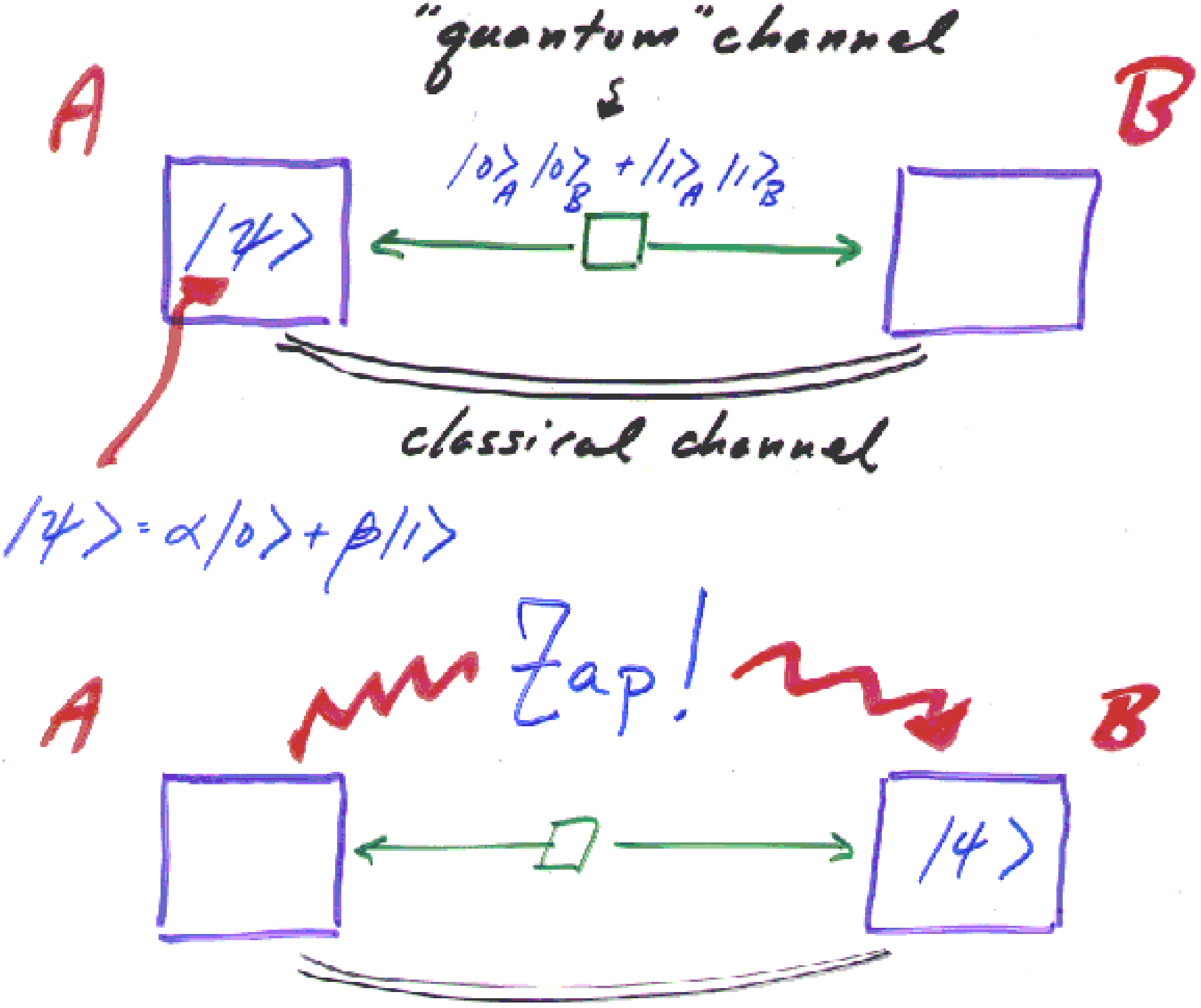
It sounds like magic. But their breakthrough could affect everything from the future of computers to our knowledge of the cosmos.

Smart guys. But none of them can stuff a cabbage. Yet.

IBM

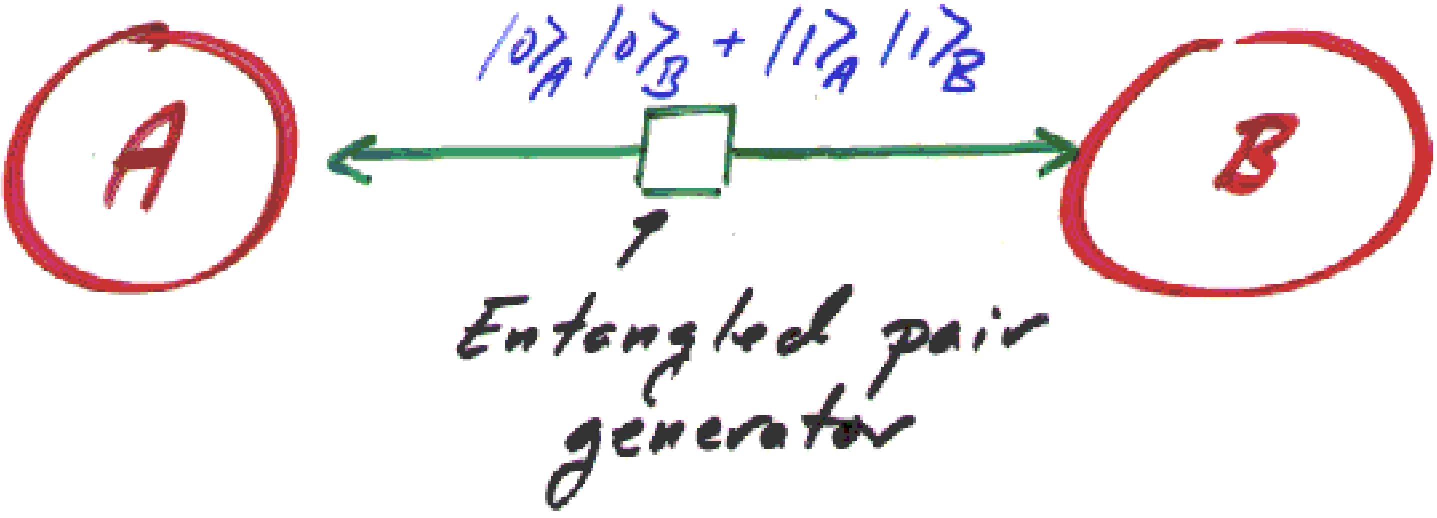
Solutions for a small planet

Quantum Teleportation


"quantum" channel
A
B
$|0\rangle_A|0\rangle_B + |1\rangle_A|1\rangle_B$
$|\psi\rangle$
classical channel
$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$
Zap!
A
B
$|\psi\rangle$

★ Shared entanglement & classical communication can be used to "teleport" a quantum state from A to B.

Quantum Cryptography



A : 0 1 1 0 1 1 1 0 . . .

B : 0 1 1 0 1 1 1 0 . . .

Message: HI → 89 → $\overbrace{0100}^{8}\ \overbrace{0101}^{9}$

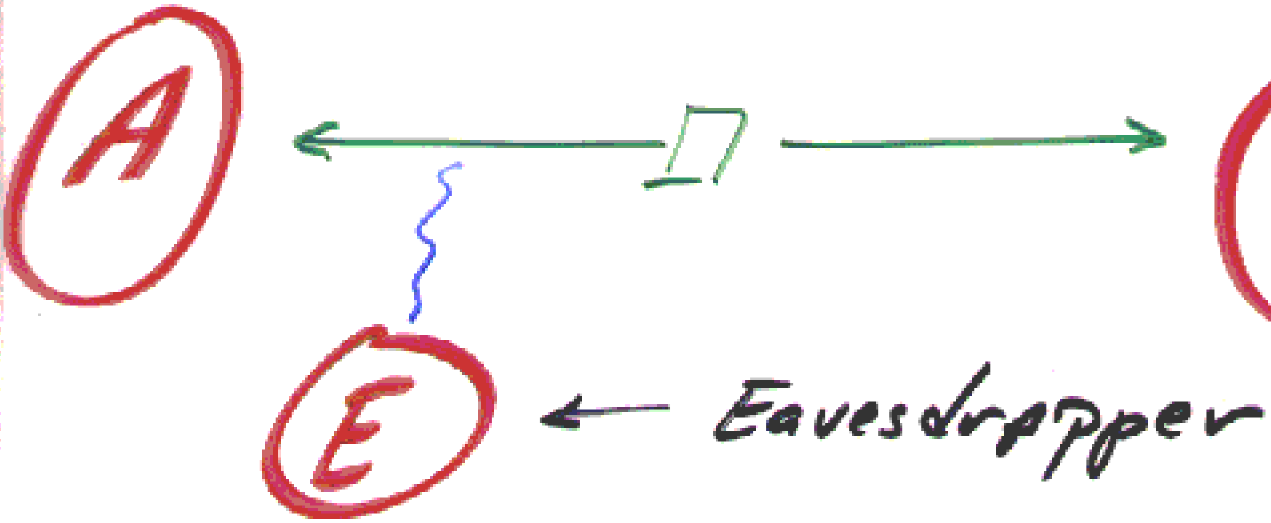
A encodes ⟶ 01101110 ⊕

00101011

B decodes ⟶ 01101110 ⊕

HI ⟵ 01000101

★ Eavesdropping can be detected because quantum states cannot be measured without disturbing them.



A:	0	0	1	1	0	0	1	1	0	...
B:	0	1	1	1	0	1	1	1	0	.

→ E can be detected!

Note: I have simplified things a bit, but this is the general idea.

Quantum Cryptography with Entangled Photons

Thomas Jennewein,[1] Christoph Simon,[1] Gregor Weihs,[1] Harald Weinfurter,[2] and Anton Zeilinger[1]

[1] *Institut für Experimentalphysik, Universität Wien, Boltzmanngasse 5, A-1090 Wien, Austria*

[2] *Sektion Physik, Universität München, Schellingstrasse 4/III, D-80799 München, Germany*

(Received 24 September 1999)

By realizing a quantum cryptography system based on polarization entangled photon pairs we establish highly secure keys, because a single photon source is approximated and the inherent randomness of quantum measurements is exploited. We implement a novel key distribution scheme using Wigner's inequality to test the security of the quantum channel, and, alternatively, realize a variant of the BB84 protocol. Our system has two completely independent users separated by 360 m, and generates raw keys at rates of 400–800 bits/s with bit error rates around 3%.

PACS numbers: 03.67.Dd, 42.79.Sz, 89.80.+h

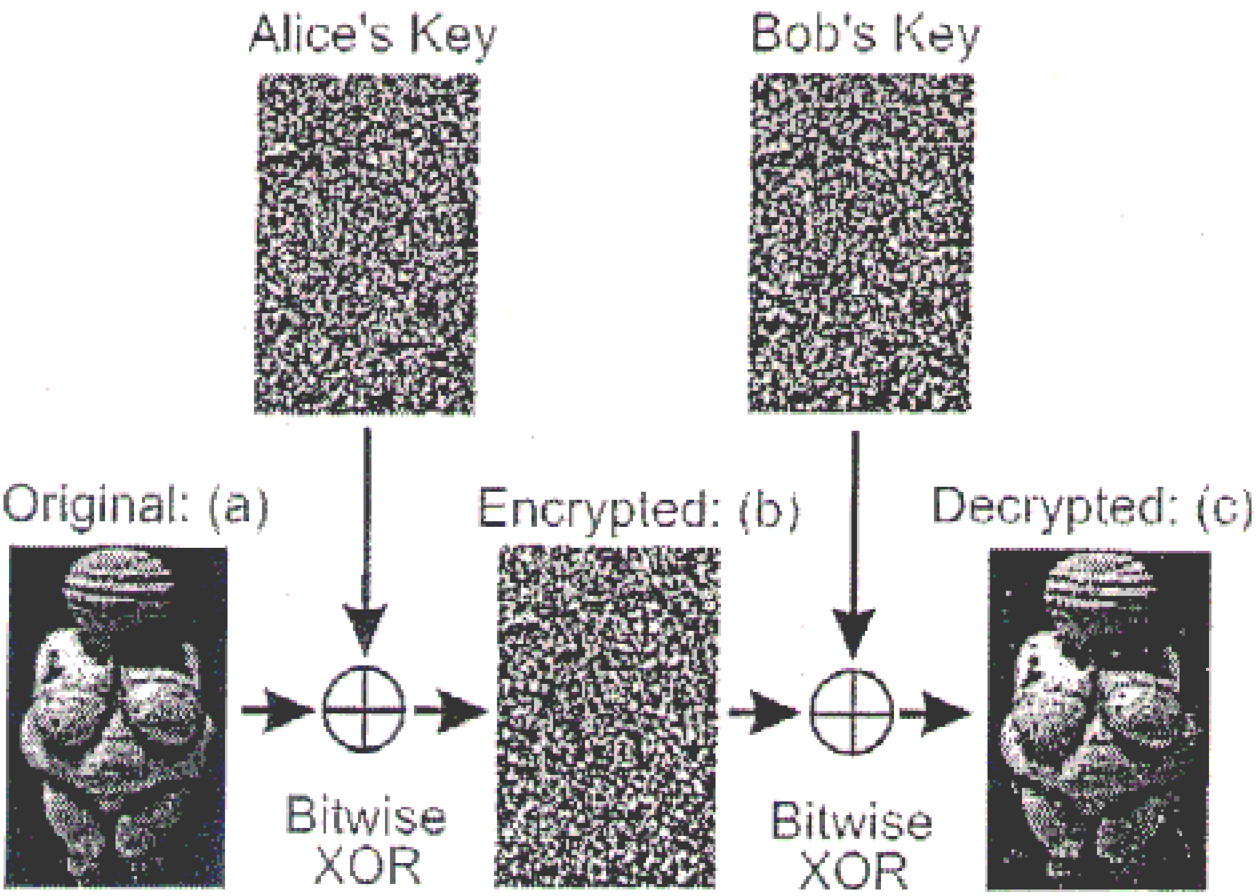
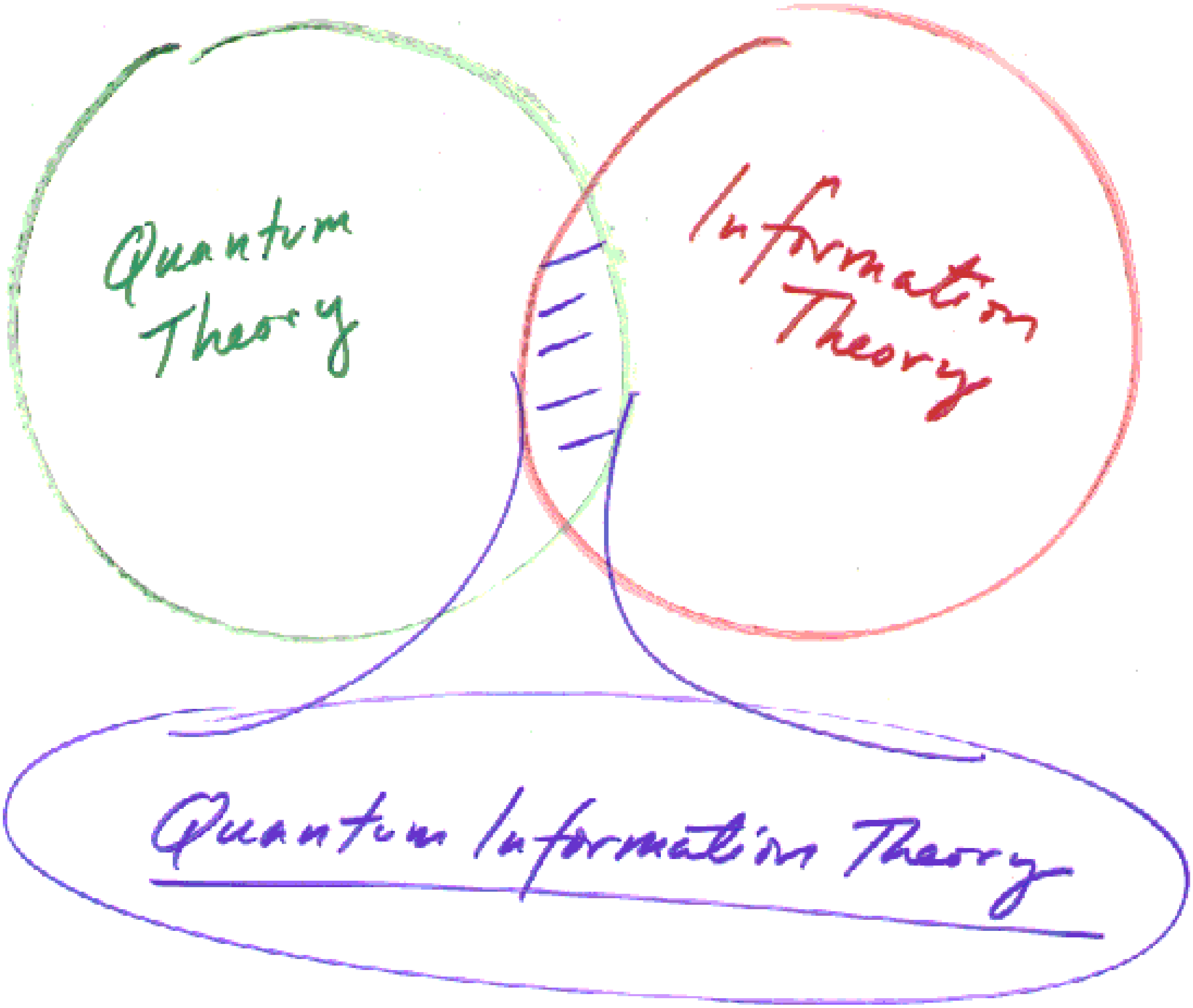


FIG. 3 (color). The 49984 bit large keys generated by the BB84 scheme are used to securely transmit an image [23] (a) of the "Venus von Willendorf" [24] effigy. Alice encrypts the image via bitwise XOR operation with her key and transmits the encrypted image (b) to Bob via the computer network. Bob decrypts the image with his key, resulting in (c) which shows only a few errors due to the remaining bit errors in the keys.



On paper, a qualitatively new kind of technology appears to be possible. Is it possible in practice?

“Where a calculator on the Eniac is equipped with 18000 vacuum tubes and weighs 30 tons, computers in the future may have only 1000 tubes and weigh only 1 1/2 tons”

Popular Mechanics, March 1949