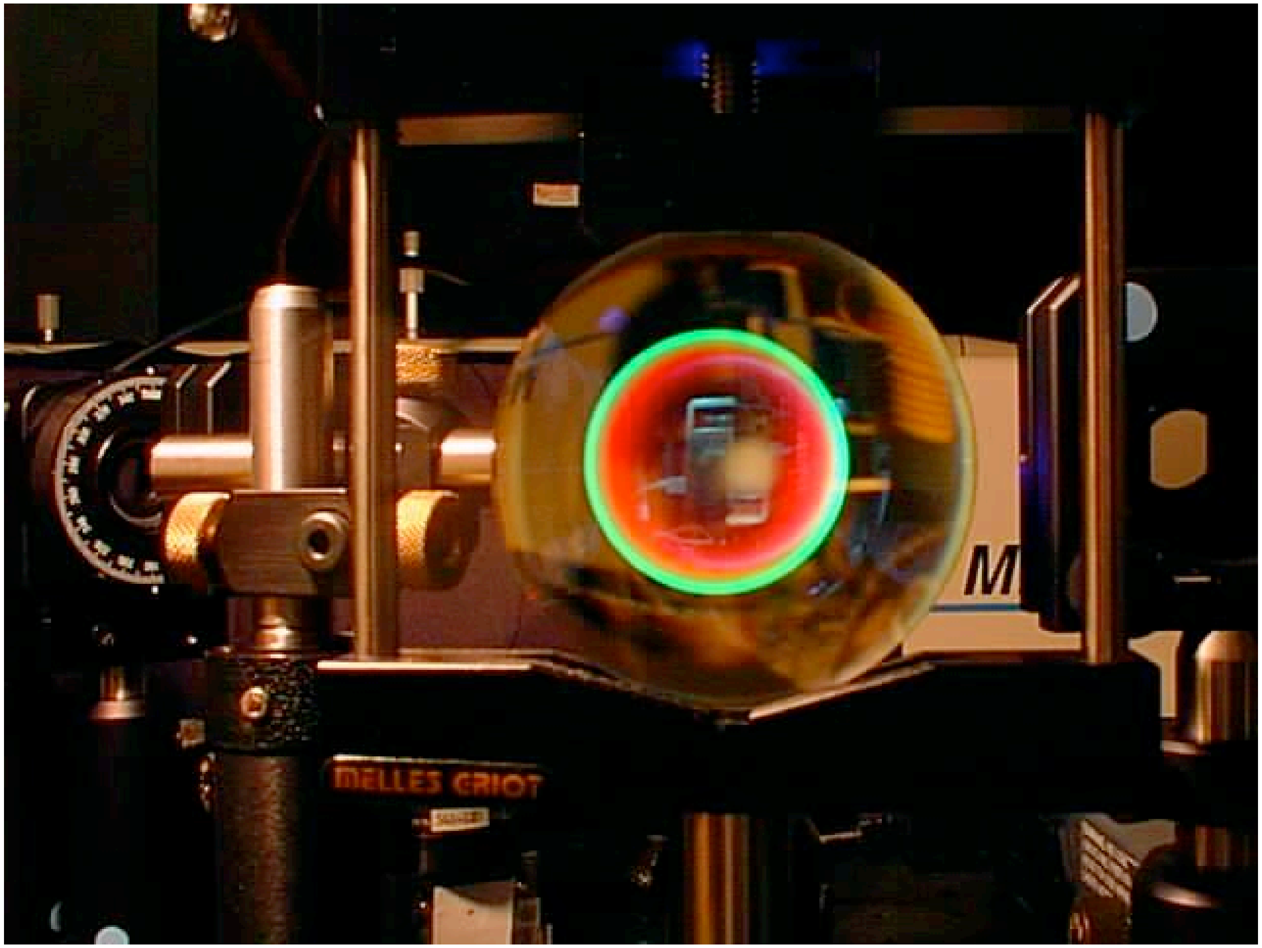
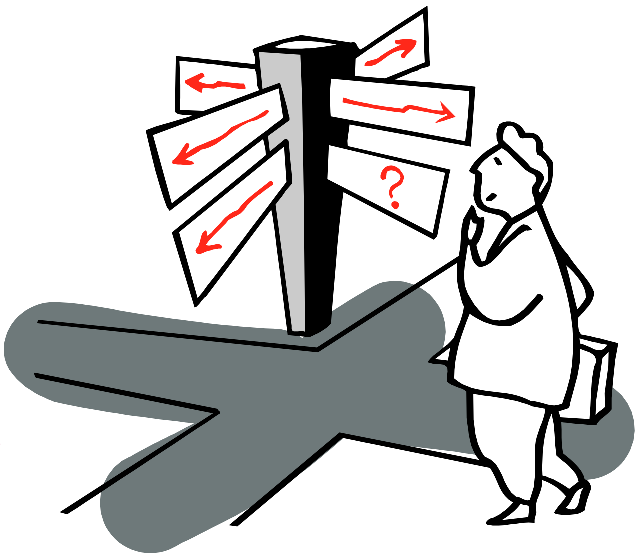
God's Dice: Quantum Mechanics from Einstein to the Internet



Aephraim Steinberg
University of Toronto

PASU + EngSci
24 Nov 2009

Just so you know where we're going...

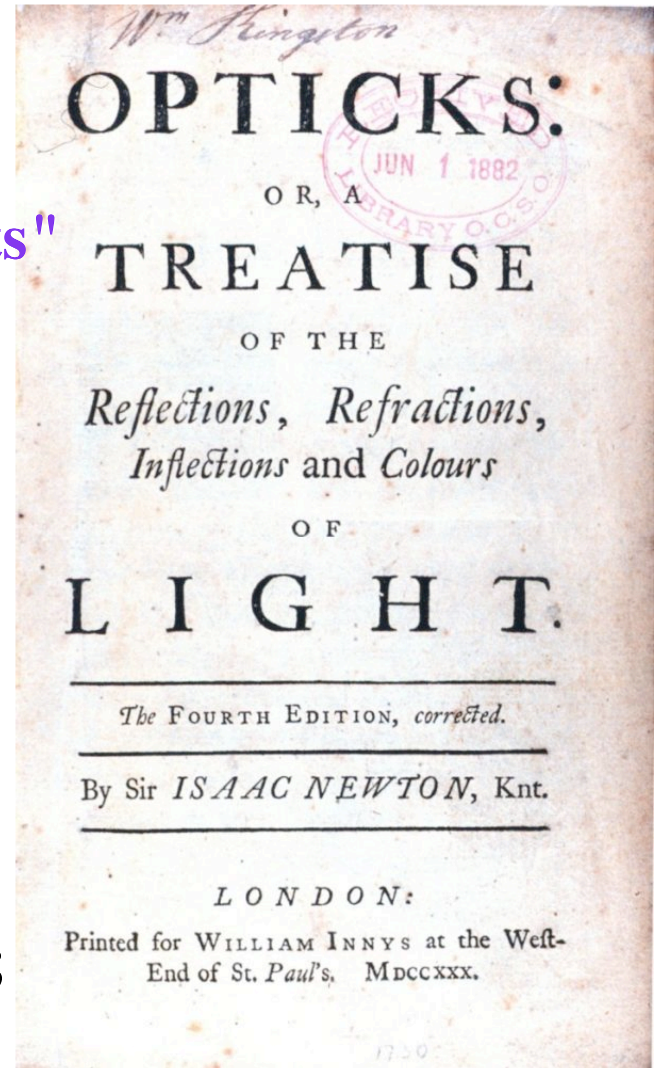


- What is light?
    - Particle or wave or particle or ...?
- Quantum mechanics
    - Uncertainty and complementarity
- The Einstein-Podolsky-Rosen "paradox"
    - Spooky actions at a distance
- Faster-than-light communications, cloning, and information
    - What does "information" have to do with physics?
- Quantum cryptography
    - Using quantum uncertainty for ... the internet?
- Quantum computers, Quantum teleportation, ...

Long before 1905...

What is light?

The greatest thinkers of all time wanted to understand how we see, and what light is. They moved from "thought experiments" to real experiments... but remained confused!

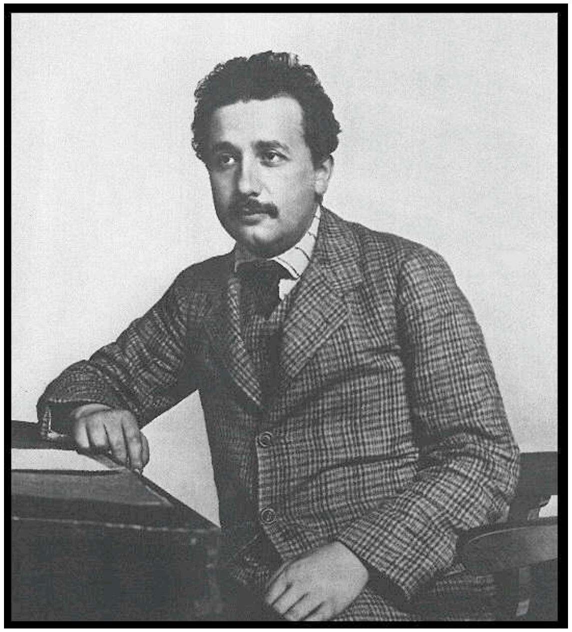


Newton: light is a particle

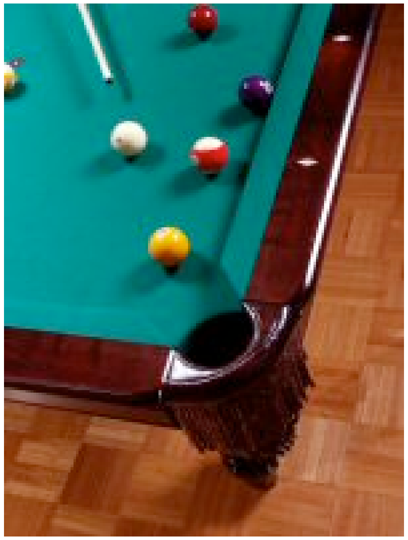
Fresnel, Poisson/Arago: it's a wave
Maxwell: it's an *em* wave

Planck: well, it's *emitted* as a particle
Einstein: it's also *absorbed* as a particle; in some sense, I guess it *is* a particle...

us: so, what the *$&@ is it?



Particle or Wave?



Einstein:

Light may well travel as a wave, interfering & all that, but when you detect it, it appears one particle at a time.

A particle of light ("photon") is incredibly small – a normal light bulb gives off about 1,000,000,000,000,000,000,000 of them every second – this is why (even though in the dark, the eye is sensitive to 3 or 4 photons) we never realized this.

An upcoming lecture...

2009 Boris P. Stoicheff Lecture

From Einstein's photon to Wheeler's delayed choice experiment: wave particle duality brought to light

by

Professor Alain Aspect

Laboratoire Charles Fabry de l'Institut d'Optique, Palaiseau, France

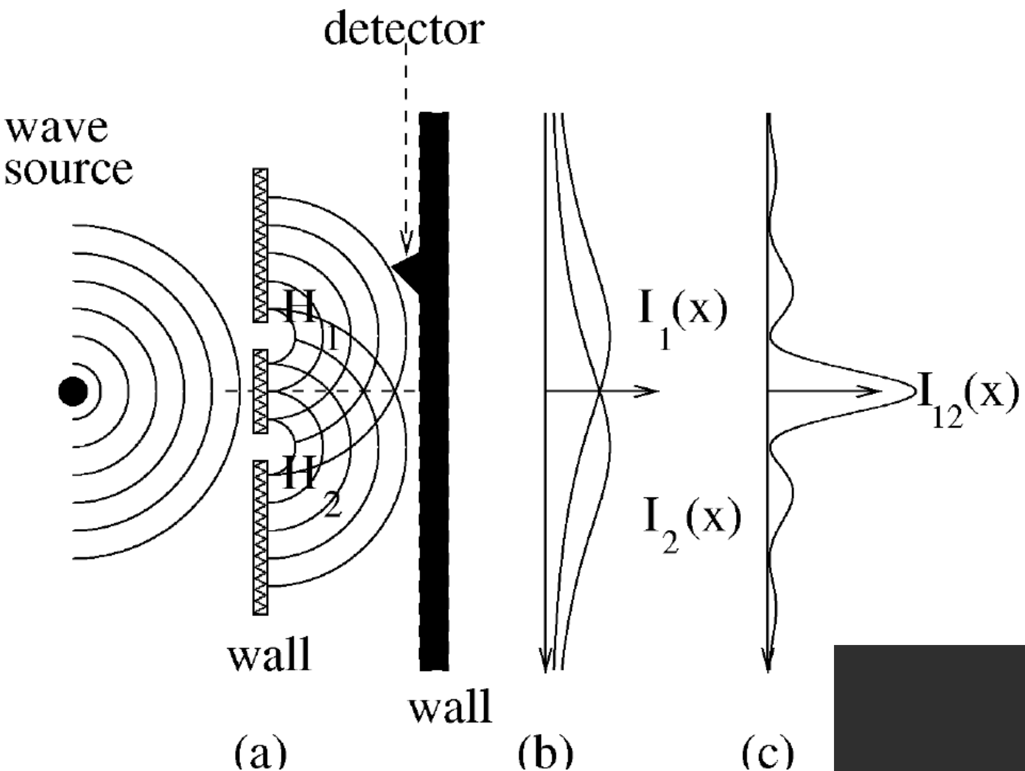
Sunday, December 6, 2009, 3:00 PM

Public Lecture - All are welcome
Free admission and refreshments

J. J. R Macleod Auditorium
Medical Sciences Building
University of Toronto
1 King's College Circle

Click here for a campus map with the lecture location highlighted in purple.

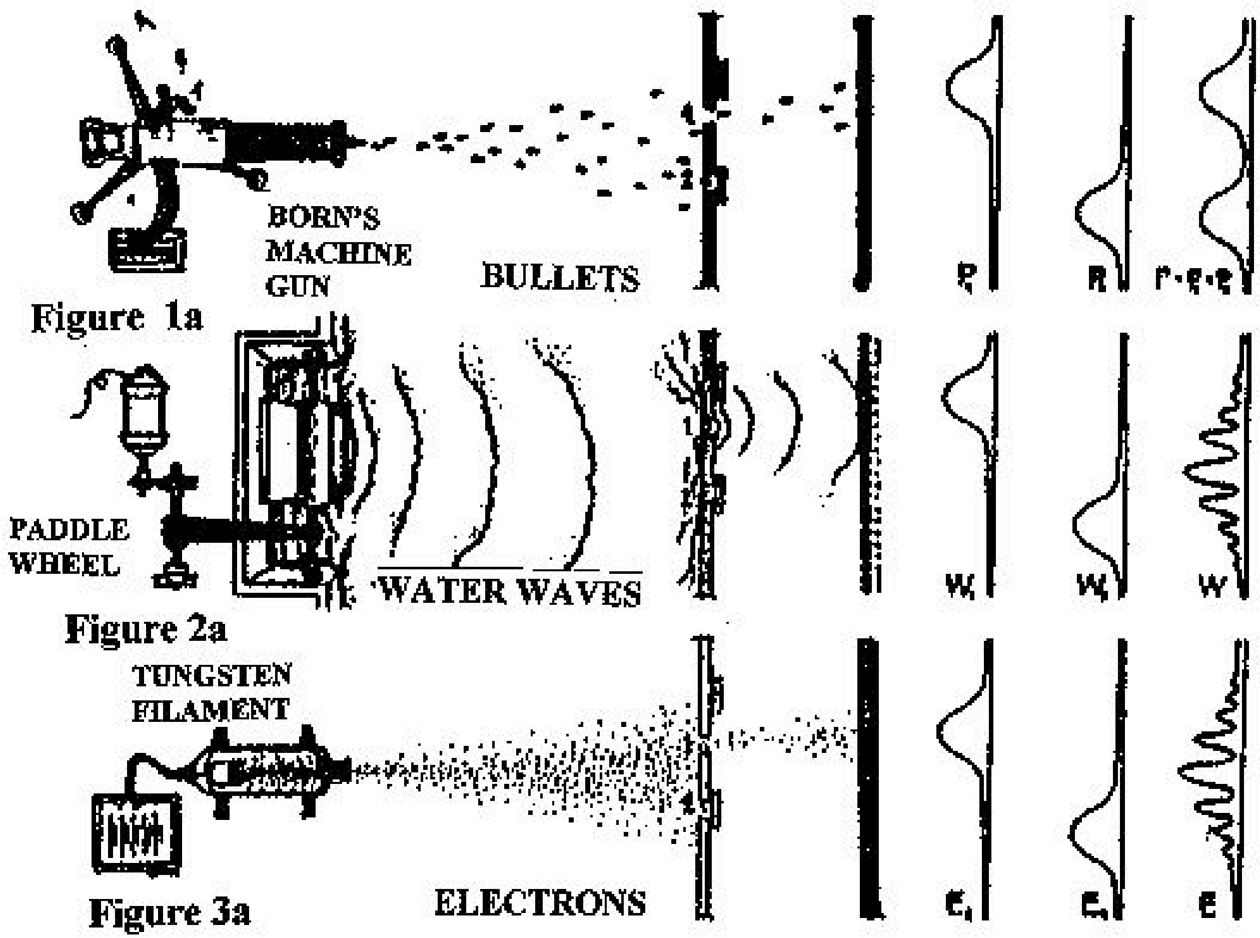
Interference: a property of waves



"Real world" examples:
the coloured stripes of
oil slicks
butterfly wings
CDs

Prince Louis de Broglie:

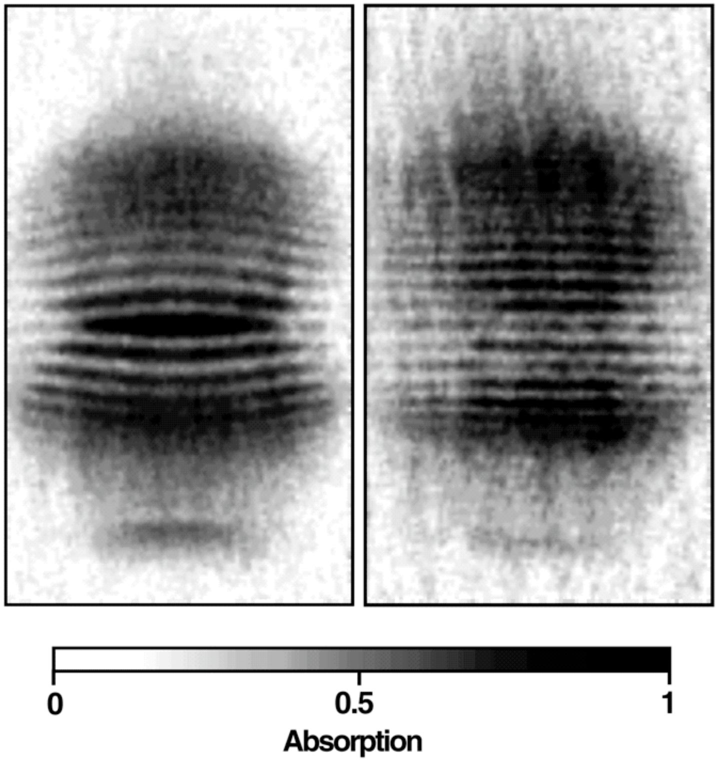
If light waves act like particles sometimes, then maybe particles of matter also act like waves sometime.



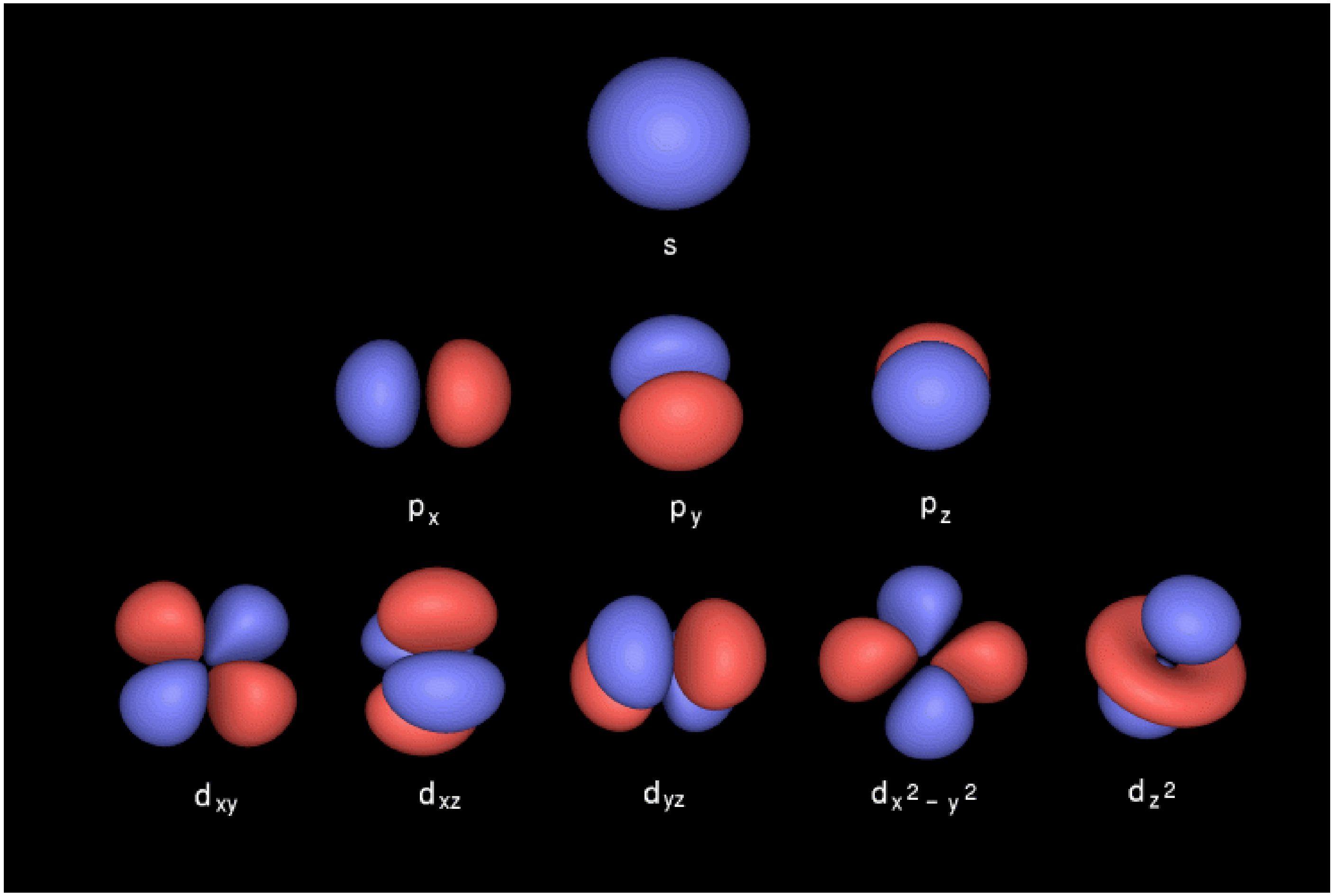
Quantum mechanics

Waves of light are also particles...
and particles of matter are also waves!

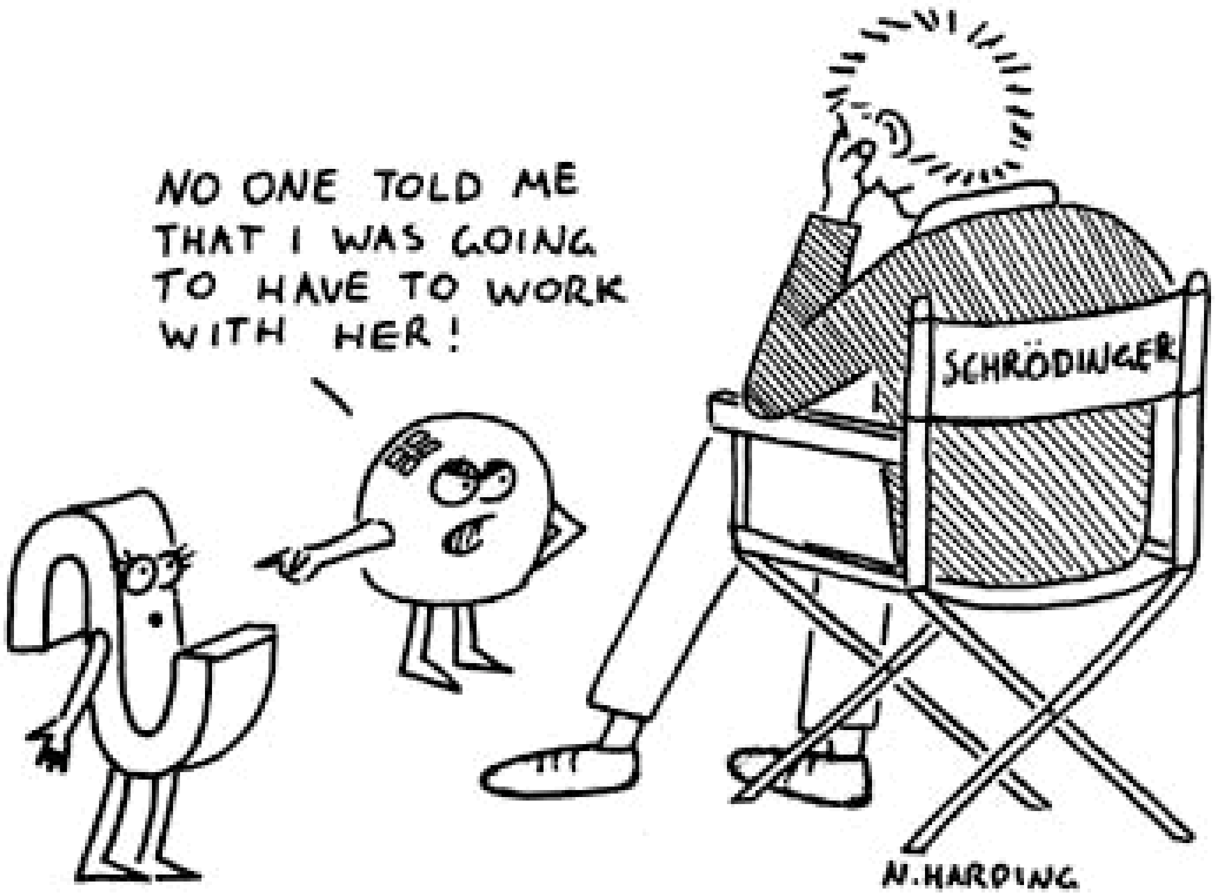
MIT photo of atoms interfering!
(Relying on lasers and on
Bose-Einstein condensation,
two more of Einstein's contributions...)



Is this what an atom “looks” like?



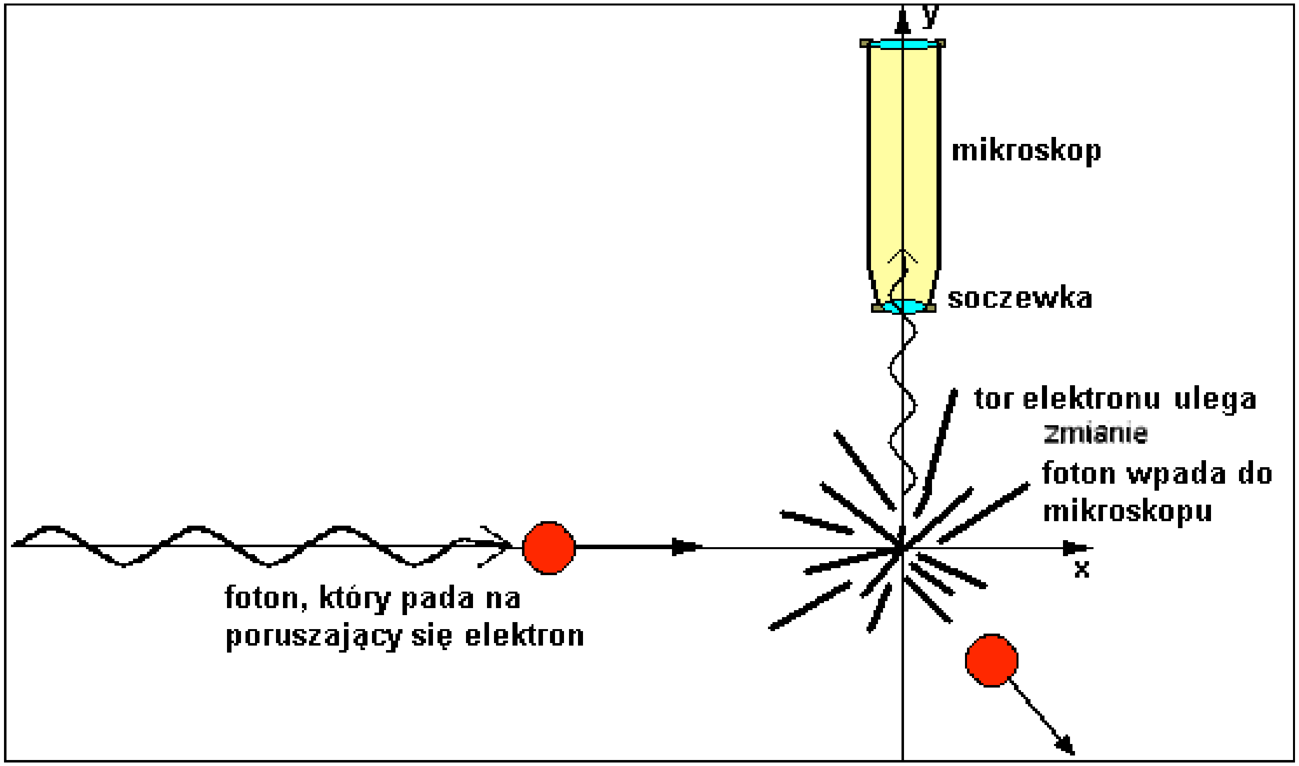
Schrödinger: If I'd known, I would never have started the darned thing.



Bohr-Einstein debates

How can a particle go through both slits at once?
If I measured which one it went through, how could interference occur between the two of them?

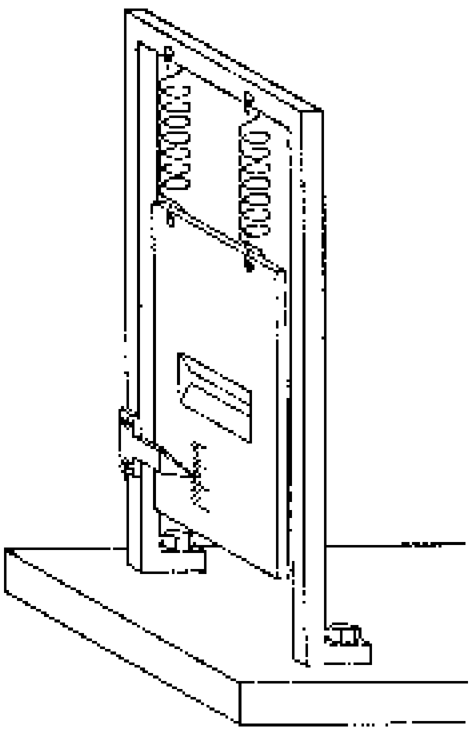
Heisenberg's uncertainty principle

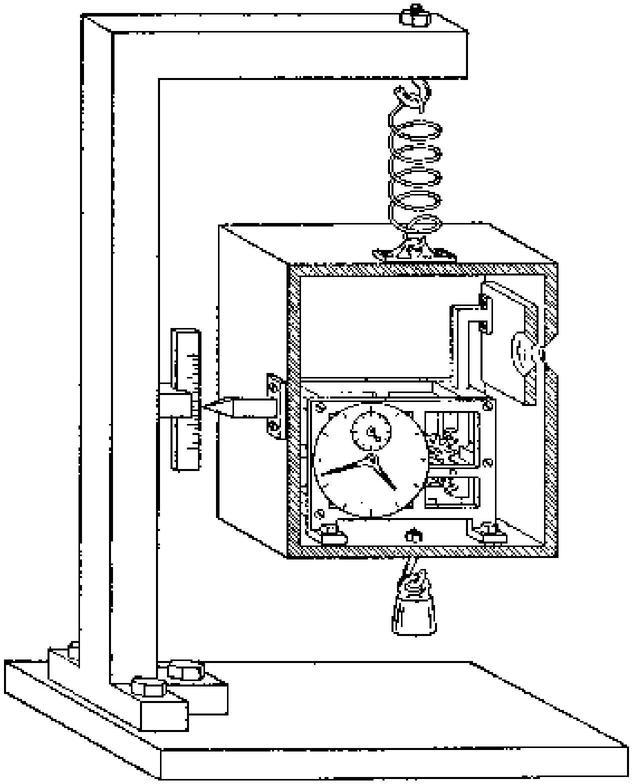


Przykład działania zasady Heisenberga - foton padający na elektron pozwala dokonać pomiaru, ale jednocześnie zmienia układ, który mierzymy.

You can't measure anything without disturbing it!
...it's impossible to figure out where something is
***and* how fast/which way it's going, at the same time!**
(Position and "momentum"[speed/direction] must be uncertain.)

More and more schemes to measure Welcher Weg (which way) the particle goes...

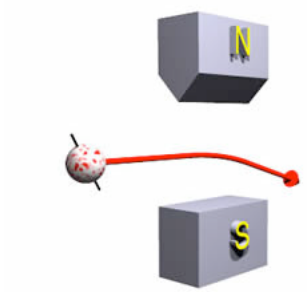


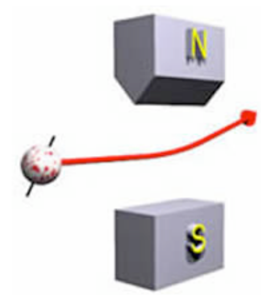


So what happens when I measure something?

The position and velocity couldn't have both been known, but I get an answer whichever one I measure... and even if I measure position, where will it be a minute later??

The problem we're still arguing about today:
What does it mean that it's "impossible" to know both?

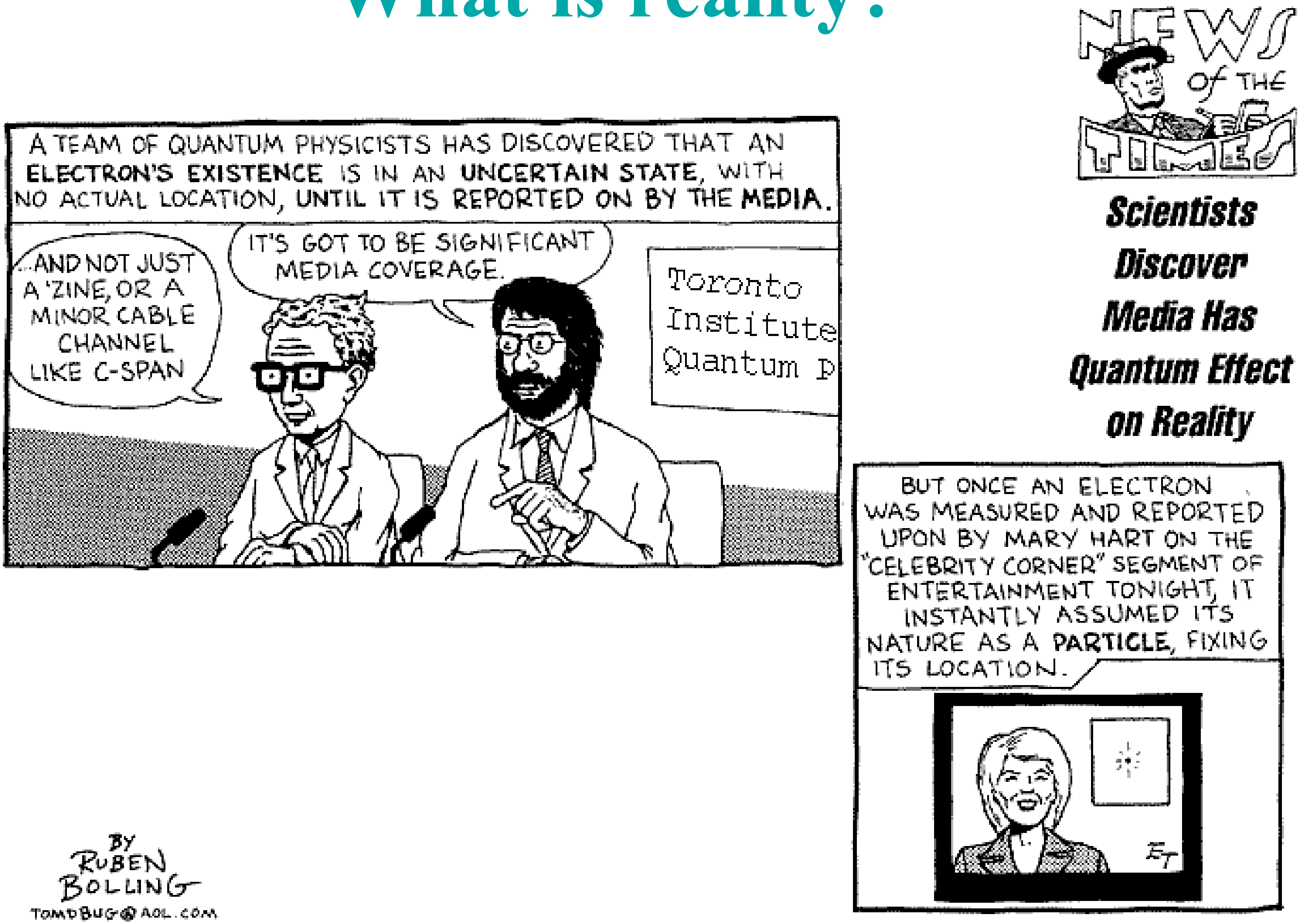




- **Particles really have definite positions & momenta,** **but we don't know how to measure them? And QM is just a theory of the "big picture," like thermodynamics?**
- **Particles don't actually have definite positions & momenta?** **(or any other definite properties, for that matter?)**

The quantum state "collapses" randomly when we look at it?

What is reality?



More Bohr-Einstein debates

Einstein:
I can't believe God plays dice with the universe.

Bohr:
Albert, stop telling God what to do.

Einstein, Podolsky, & Rosen (1935)

Source

Alice Bob

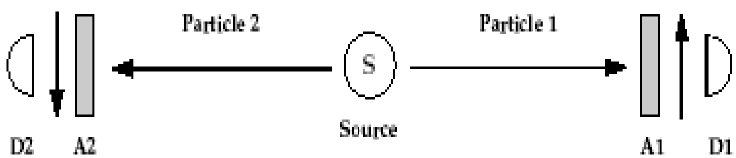


FIG. 1. Bohm's version of the EPR Gedankenexperiment

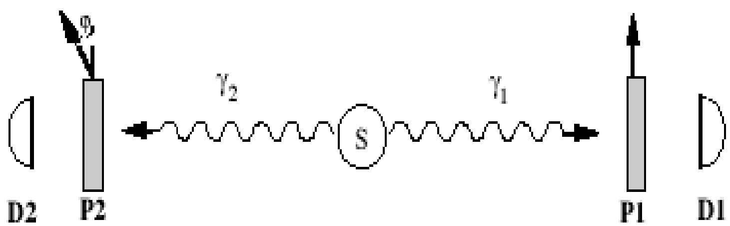


FIG. 2. Optical version of EPR experiment

2 particles emitted together at the same time with opposite speeds.

If Alice measures her particle's position, she knows Bob's. But if she measures her particle's momentum, she knows Bob's.

Did her measurement "affect" Bob's particle instantaneously?

Spooky action at a distance

Or did Bob's particle already have both?

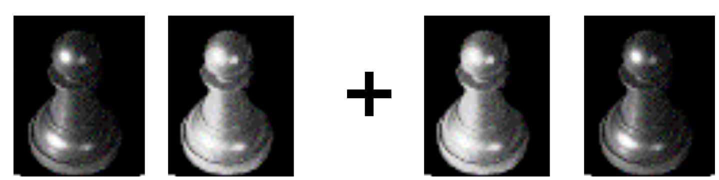
Hidden variables (QM "incomplete")

Schrödinger 1935:

"entanglement"

"Verschränkung" (SP?!)

$$|\psi\rangle = |B\rangle_L |W\rangle_R + |W\rangle_L |B\rangle_R$$

= 

Hidden variables?

Einstein seems to have thought the particles "knew" what they were going to do, even if we didn't: QM not wrong but "incomplete".

John Bell's example, "Bertlmann's socks":

"Spontaneous parametric down-conversion"

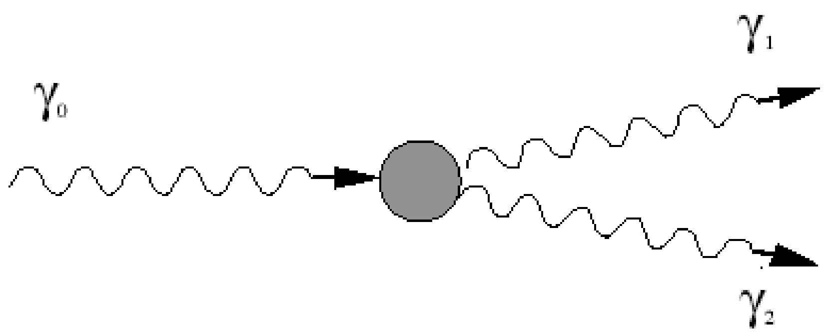


FIG. 3. Two-photon decay from one photon

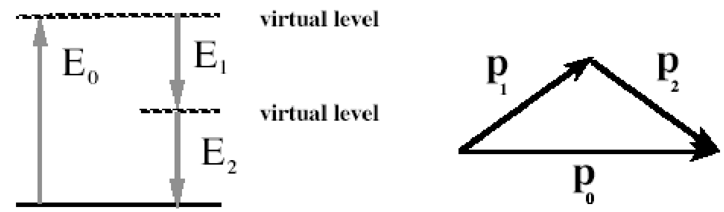
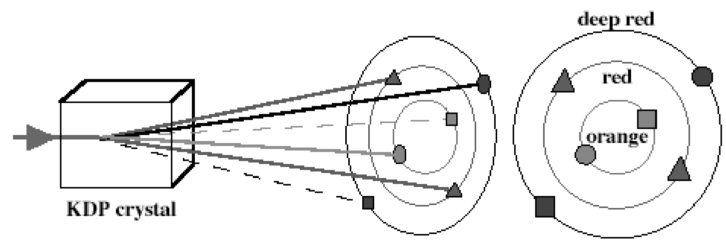


FIG. 5. Energy level diagram; momentum conservation triangle



"Spontaneous parametric down-conversion"

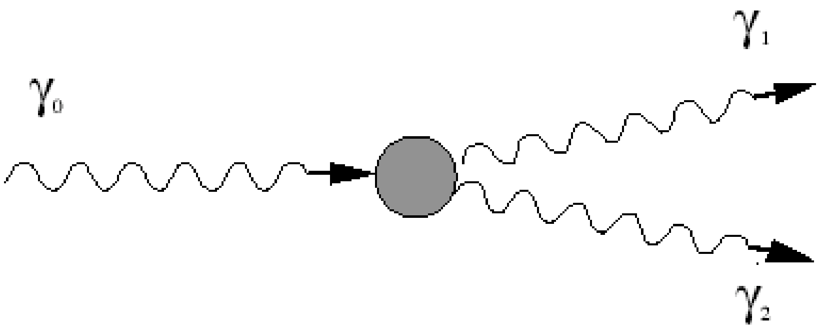


FIG. 3. Two-photon decay from one photon

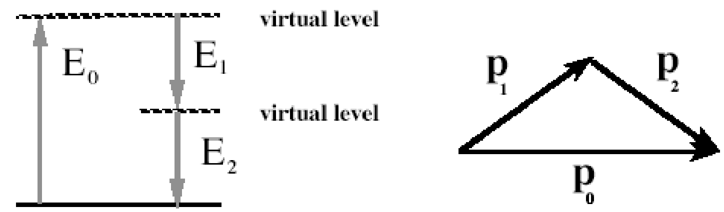
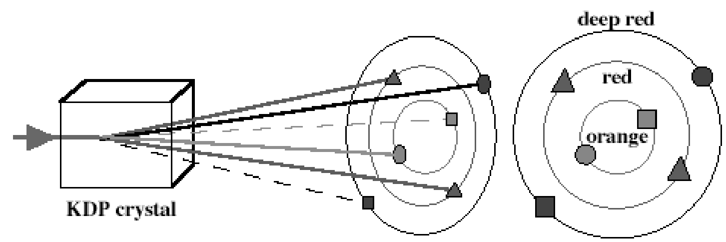
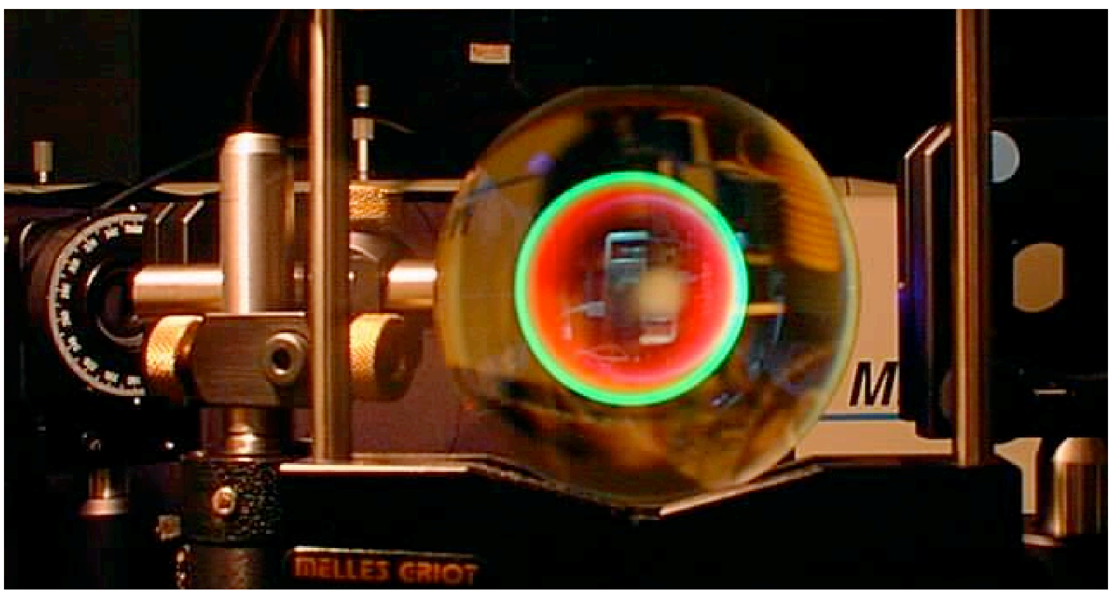
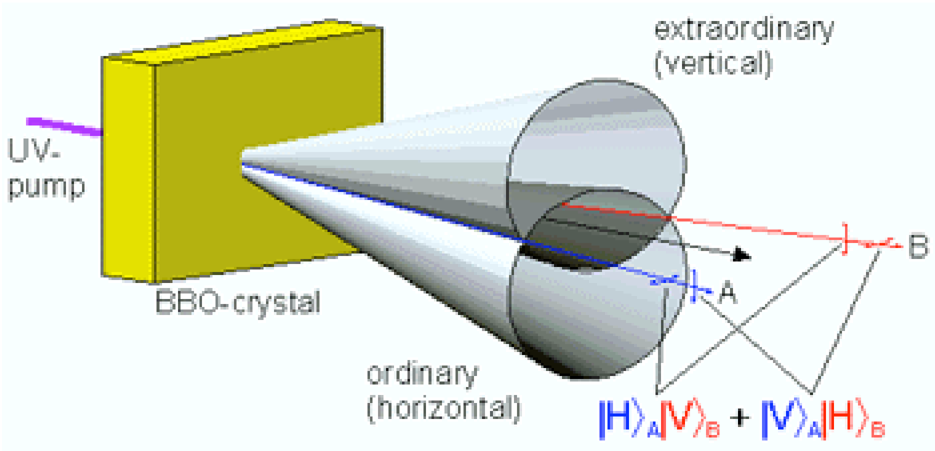


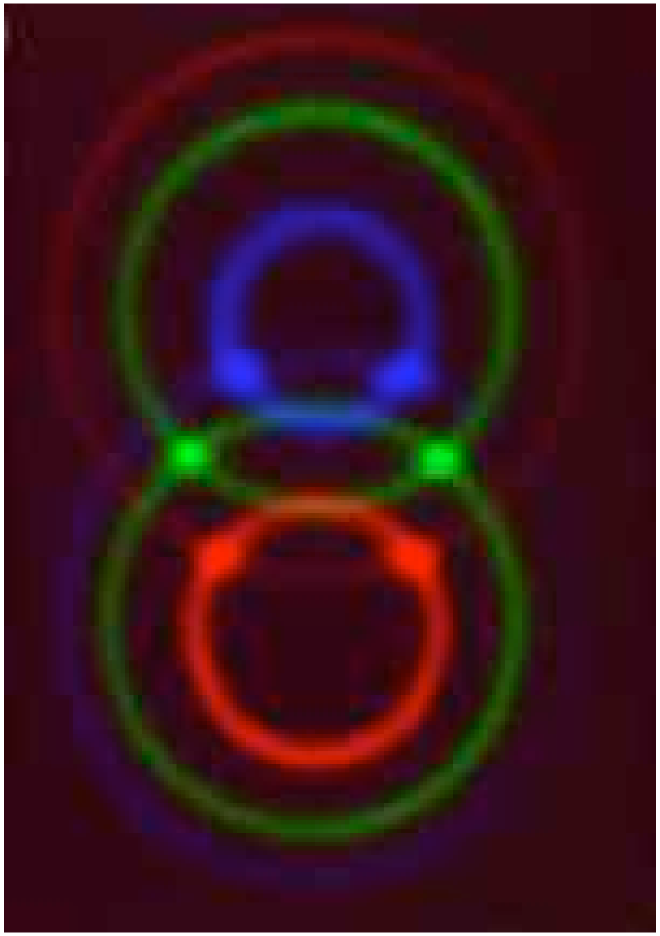
FIG. 5. Energy level diagram; momentum conservation triangle





More sophisticated "sources of entangled photons"

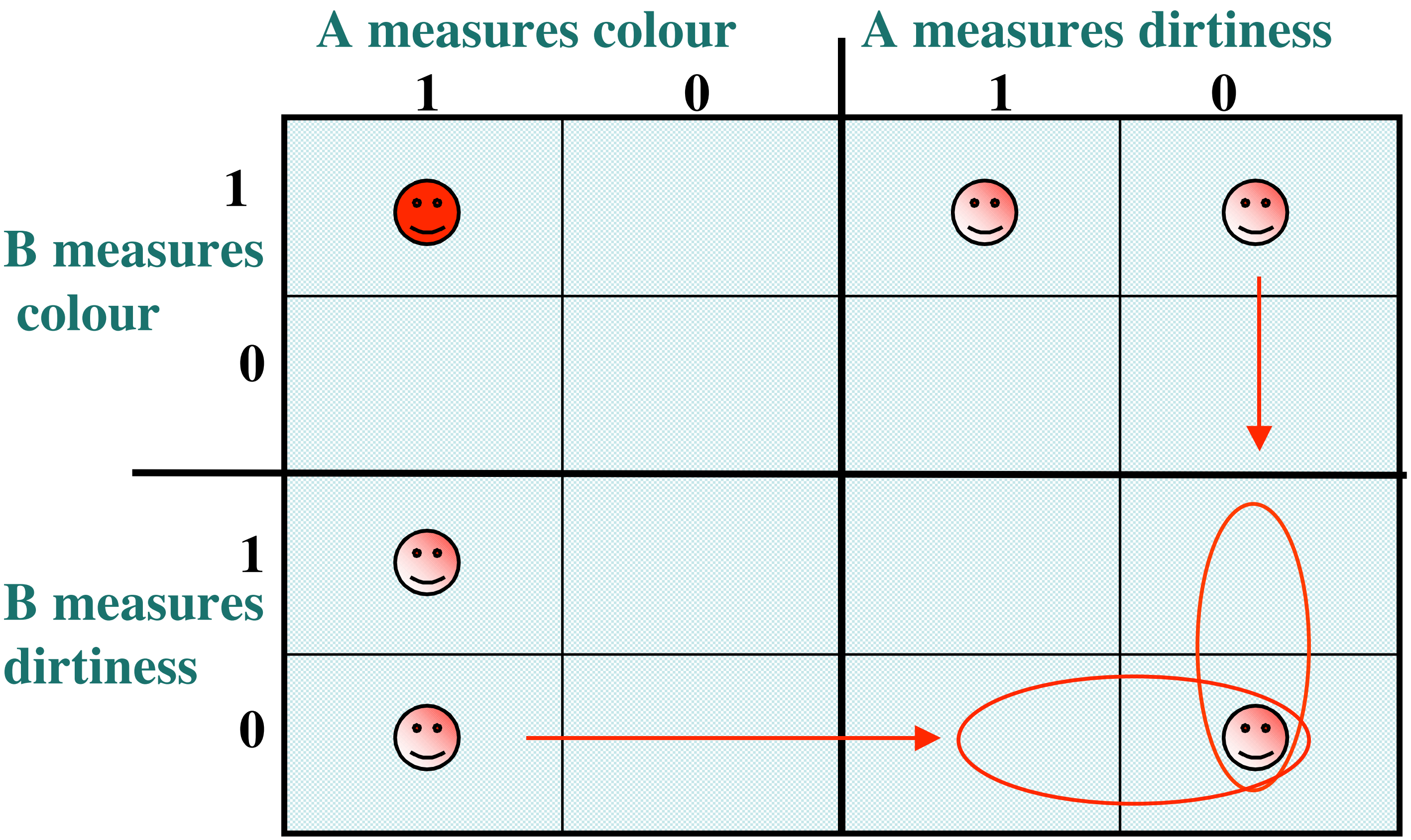




Bell's Theorem

Forget Quantum Mechanics.

Suppose you've got two particles, and A & B can choose what to measure on each of them – "color" or "dirtiness", for example. For each measurement, they either get "1" or "0". If there are "hidden variables," then A's choice doesn't affect B, and vice versa – from this alone, you can prove something.



The HVs must tell me what would happen for any choice of measurement: i.e., which box of *each quadrant* the particle is "in."

$$P(cc \Rightarrow 11) \leq P(cd \Rightarrow 11) + P(dc \Rightarrow 11) + P(dd \Rightarrow 00)$$

An example of an EPR ("Bell inequality") experiment

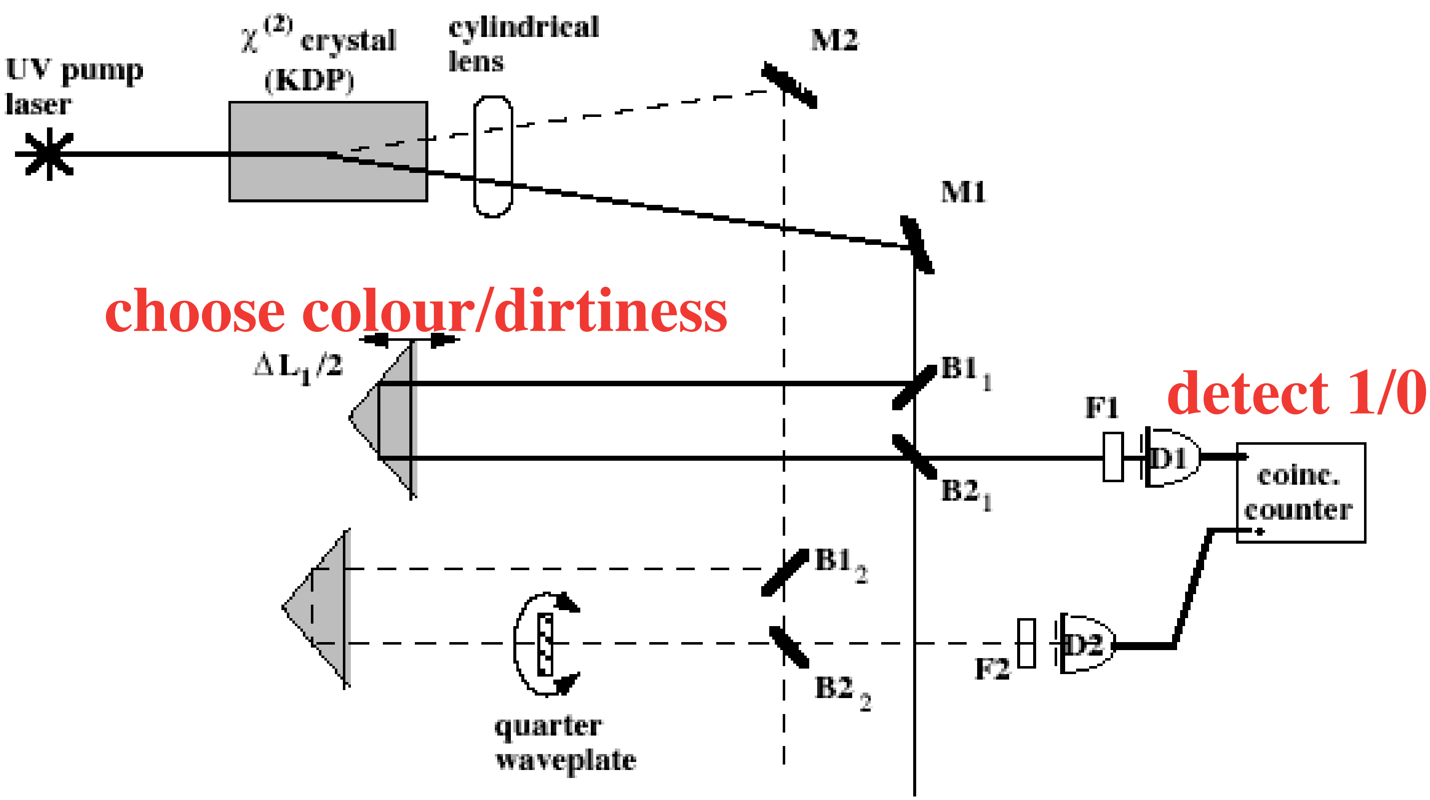
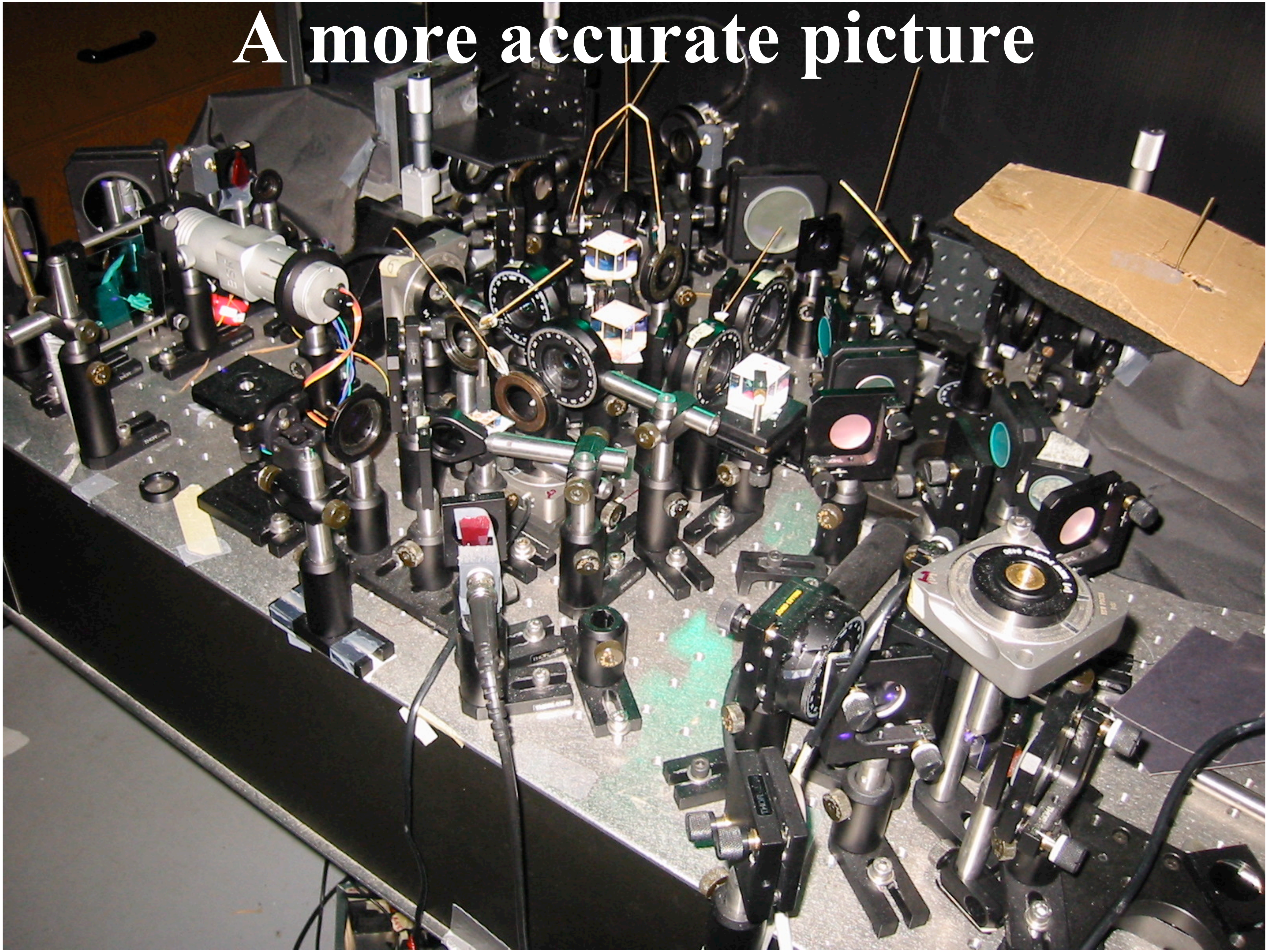
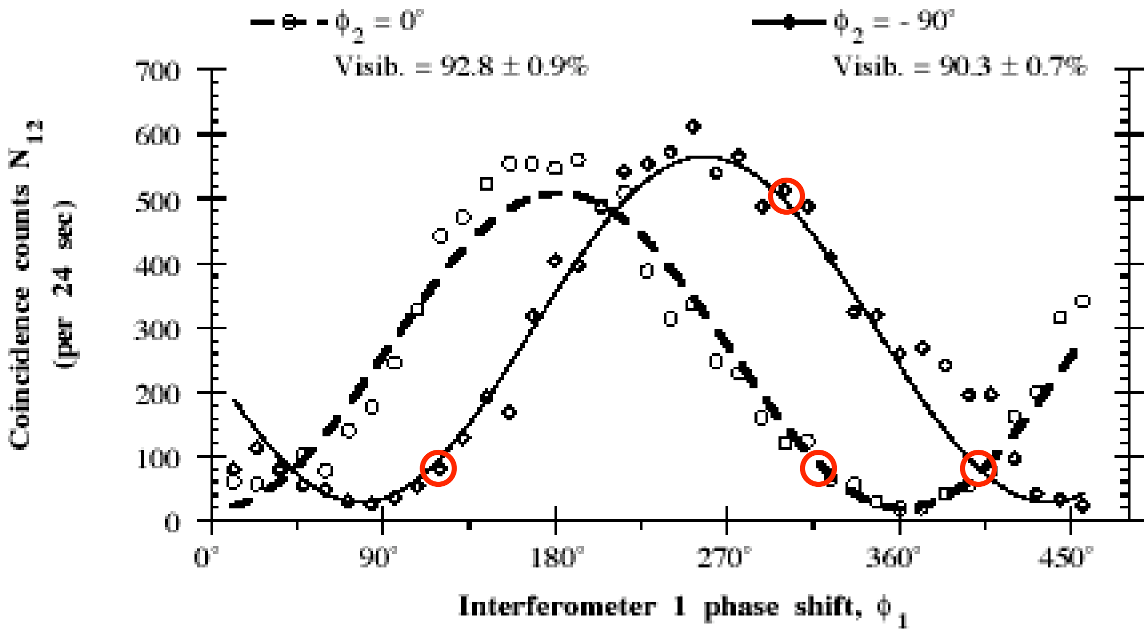


FIG. 7. Apparatus used at Berkeley to perform the Franson experiment

A more accurate picture

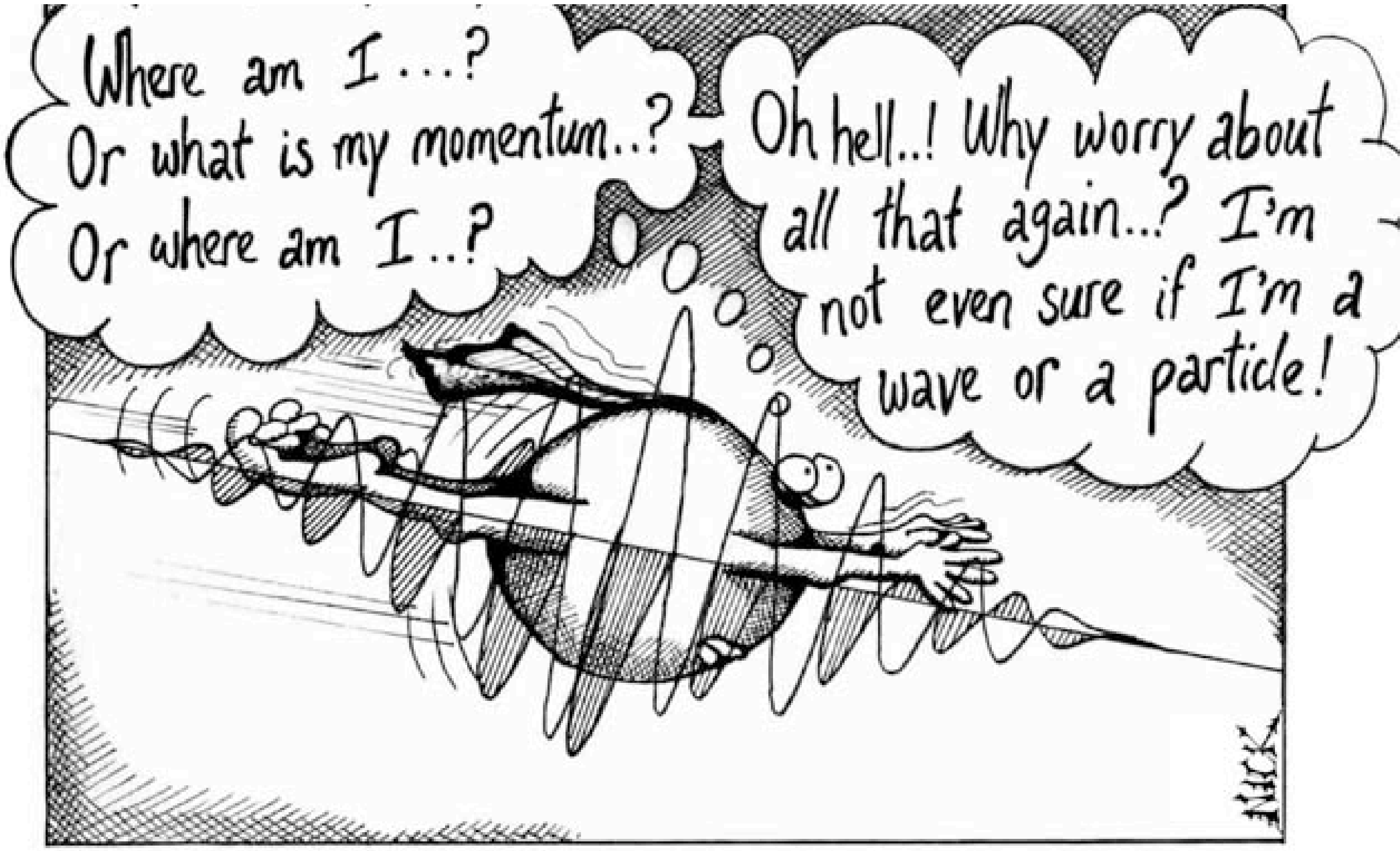


The "colour/dirtiness" curve for a photon pair



Bell's inequality is violated – in other words, whether or not quantum mechanics is right, this experiment can't be explained by "local hidden variables."

Somehow, we know that the particles don't know what they're doing!



Photon self-identity problems.

"FLASH" !?

So, does Bob immediately know what Alice chose to measure?

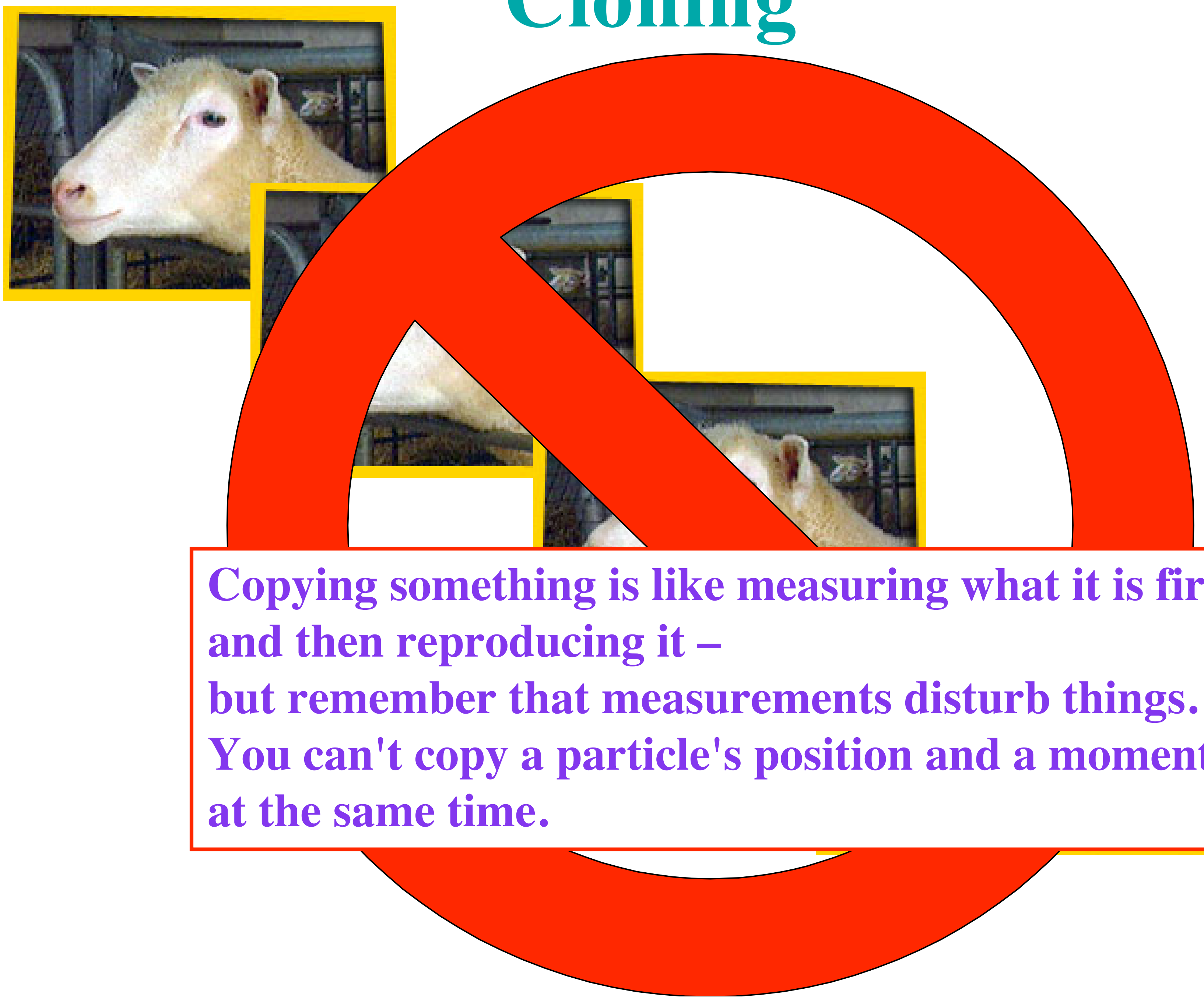
NO! If she chose "dirtiness," she already knows whether his is clean or dirty – but the answer was random.
If she chose "colour," then she knows whether his is pink or not pink – so its "dirtiness" is undetermined.

Bob gets a random answer no matter what... but was the random answer known before he made his measurement?

Nick Herbert: if he made 100 copies ("clones") of his photon before measuring, then he could see whether they all have the same dirtiness (because Alice already knew it), or whether each one was random (because Alice measured "colour").

They could communicate faster than light!

Cloning

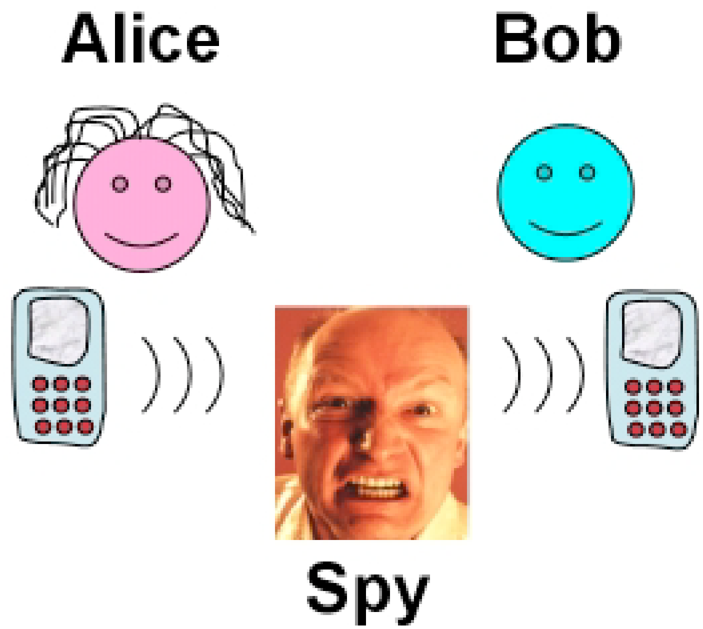


Copying something is like measuring what it is first, and then reproducing it –
but remember that measurements disturb things.
You can't copy a particle's position and a momentum at the same time.

Quantum Cryptography

"We don't need to worry about information security or message encryption. Most of our communications are impossible to understand in the first place."

The foundations of cryptography



The only provably secure way to send secrets:

the "one-time pad." Alice and Bob share a *random* "key", which is AS LONG AS THE ENTIRE MESSAGE.

They never reuse it. (Soviets made this mistake.)

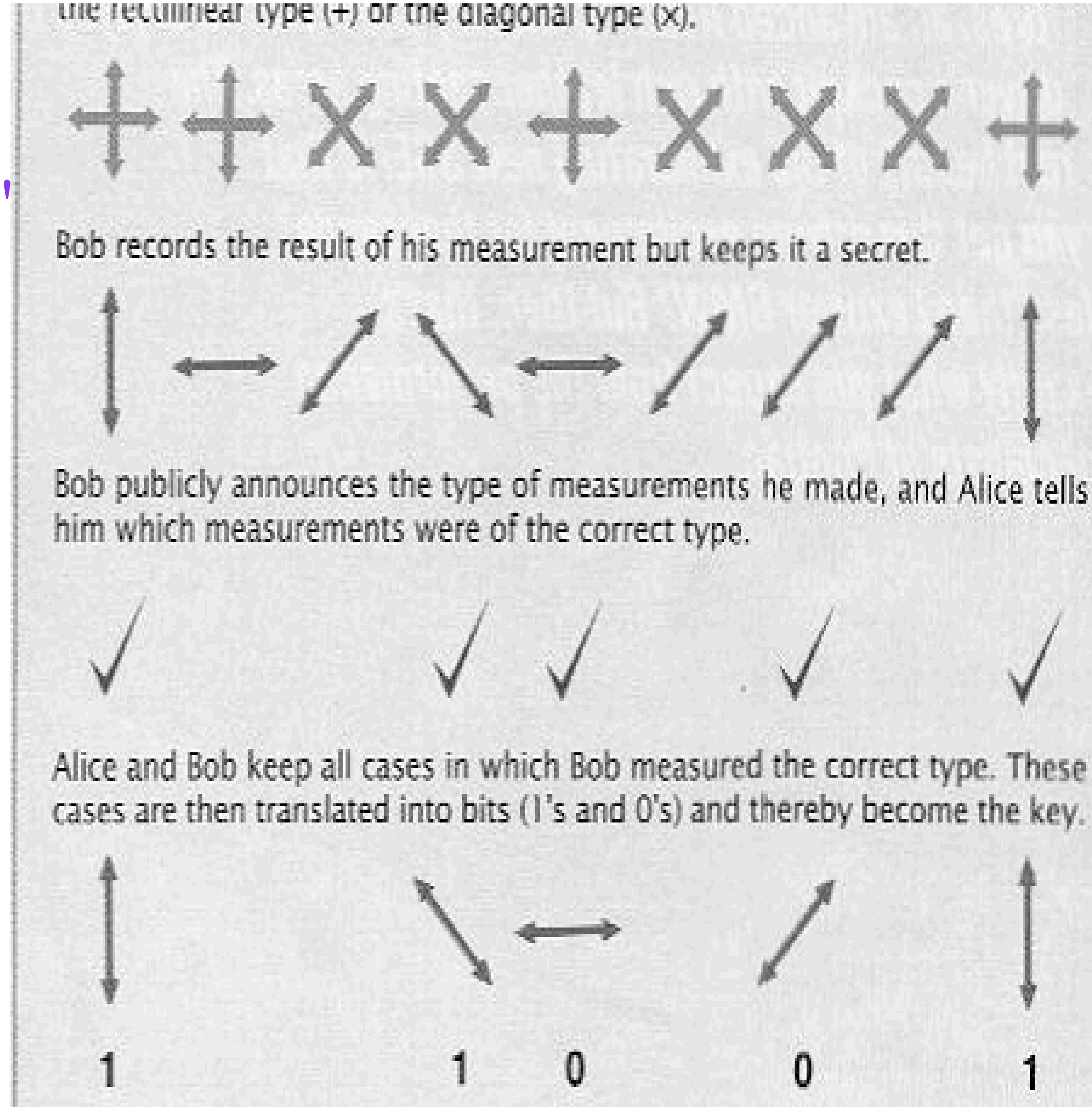
Problem: How to be sure "Eve" didn't get a copy of the key?

The Bennett-Brassard Protocol (1984)

Heisenberg to the rescue!
Photons have "polarisation"

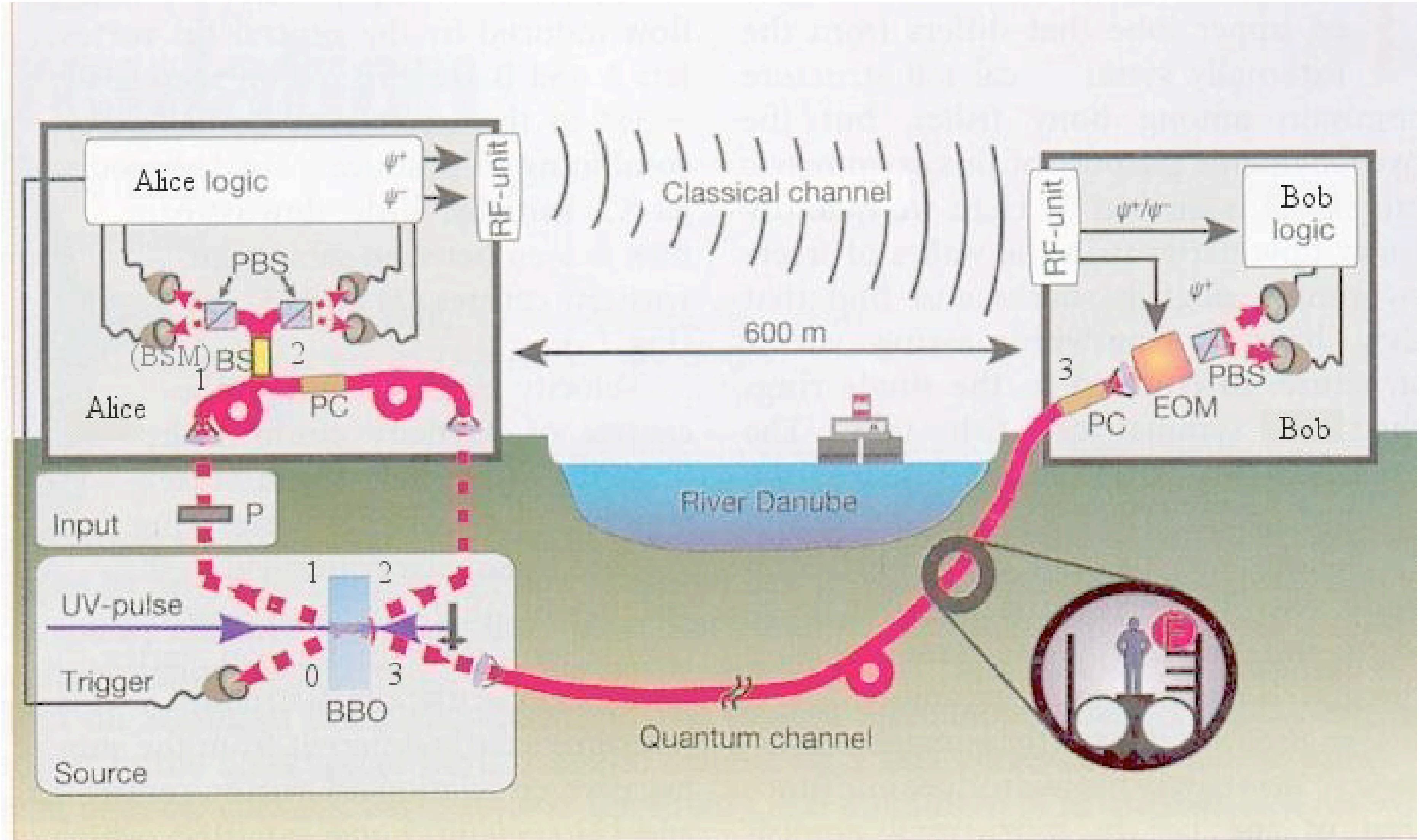
You can measure whether one is ↕ or ↔
OR you can measure whether it's ↘ or ↗

But if it's ↘
and you measure HV, the result is random; and vice versa.

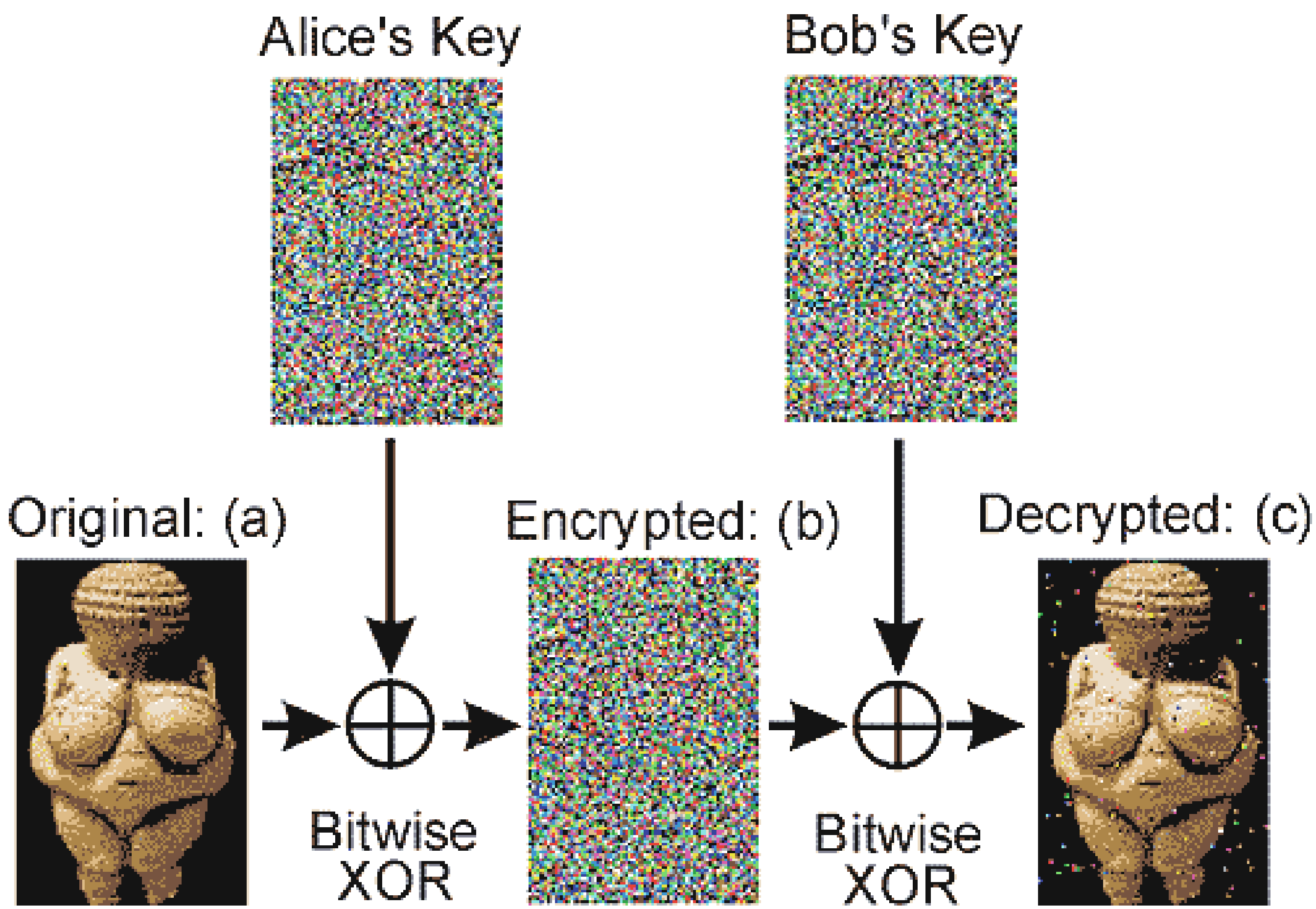


Eve can't know in advance which axis to measure along... and if she guesses wrong, she destroys the correlations Alice & Bob test.

The Blue Danube



This random string of bits can be used as a secret key...



Quantum Computation?

Some problems (like factoring large numbers) are "exponentially hard" on classical computers [as far as we know] – this means that every time you make the number one digit longer, the problem takes twice [for example] as long for a computer to solve.

This is why your credit card # is (maybe) secure when you send it over the internet!

But there are countless examples throughout history of people who thought their codes were secure, but learned otherwise (see Simon Singh's "The Code Book").

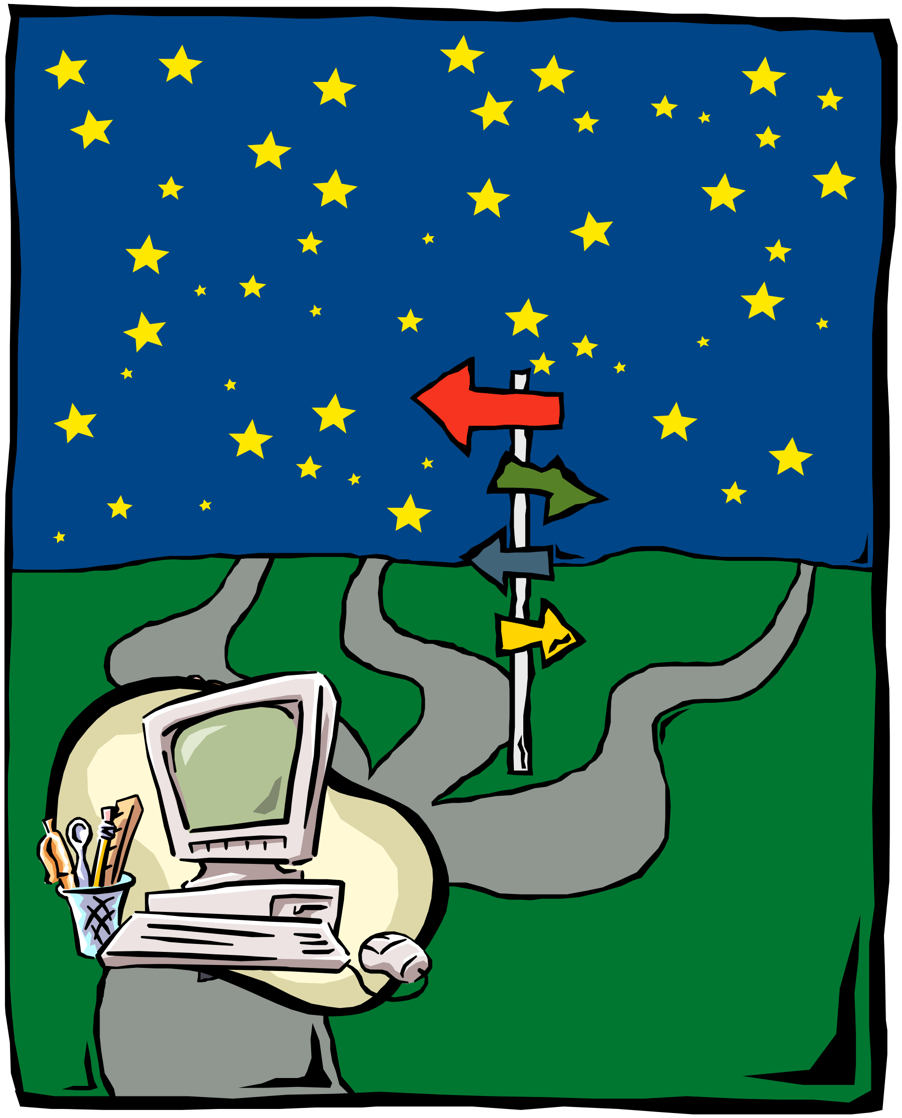
Peter Shor showed about ten years ago that if a computer were in a *quantum* state (completely uncertain), it could break this classical code.

No solution but quantum cryptography!

How in the world...?

People like Richard Feynman and David Deutsch realized that the "uncertain" state of a quantum computer could actually be useful...
If it doesn't know what state it's in, maybe it can be in all of them at the same time... and then solve many possible problems all at once?!

(Yes and no, but Deutsch – and later Shor – showed there were at least some clever things to do.)



Quantum Information

What's so great about it?

If a classical computer takes input |n> to output |f(n)>, an analogous quantum computer takes a state |n>|0> and maps it to |n>|f(n)> (unitary, reversible).

By superposition, such a computer takes Σ_n |n>|0> to Σ_n |n>|f(n)>; it calculates f(n) for every possible input simultaneously.

A clever measurement may determine some global property of f(n) even though the computer has only run once...

A not-clever measurement "collapses" n to some random value, and yields f(that value).

The rub: any interaction with the environment leads to "decoherence," which can be thought of as continual unintentional measurement of n.

What makes a computer quantum?

(One partial answer...)

If a quantum "bit" is described by two numbers:

$$|\Psi\rangle = c_0|0\rangle + c_1|1\rangle,$$

then n quantum bits are described by 2^n coeff's:

$$|\Psi\rangle = c_{00..0}|00..0\rangle + c_{00..1}|00..1\rangle + ... c_{11..1}|11..1\rangle;$$

this is exponentially more information than the 2n coefficients it would take to describe n independent (e.g., classical) bits.

We need to understand the nature of quantum information itself.

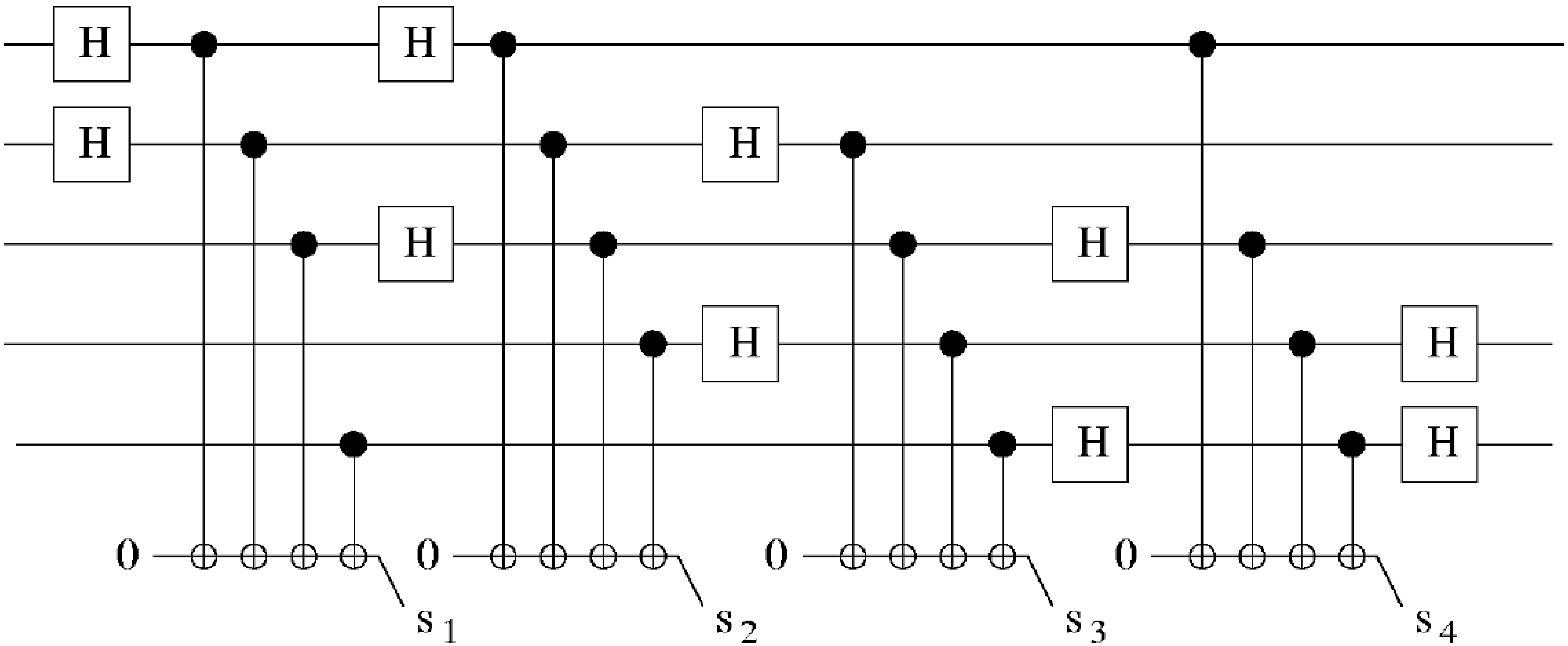
How to characterize and compare quantum states?
How to most fully describe their evolution in a given system?
How to manipulate them?

The danger of errors & decoherence grows exponentially with system size.

The only hope for QI is quantum error correction.

We must learn how to *measure* what the system is doing, and then correct it.

Quantum computing so far...



This is a small fragment of the "quantum logic circuit" which was used a few years ago to prove 15 $= 3 \cdot 5$!

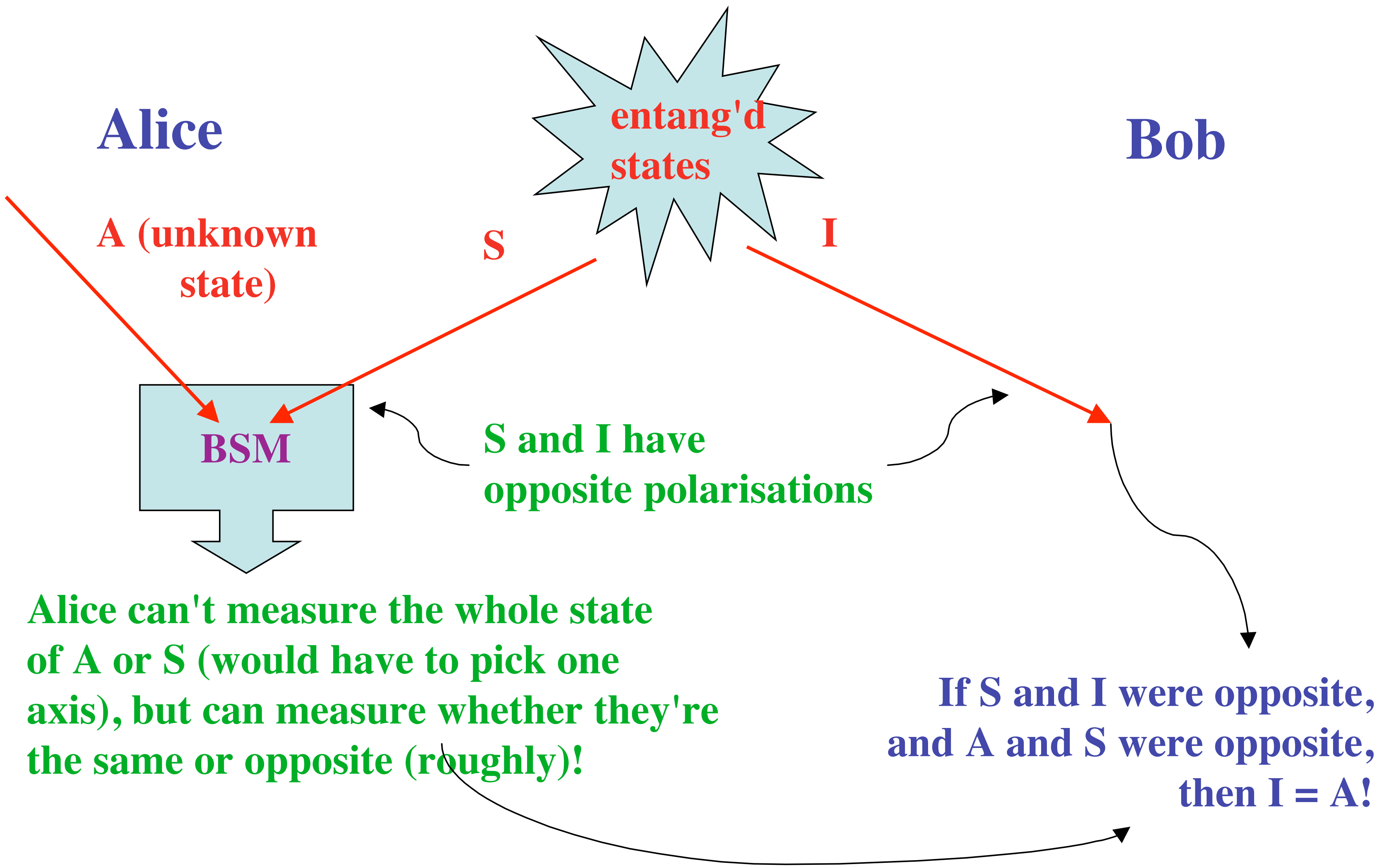
N.B.: More recently, Daniel James of U of T was part of a collaboration that says they did this *right*...

Quantum teleportation...

If I can't completely *measure* Kirk, and I can't make a *clone*, can I just send him somewhere else?

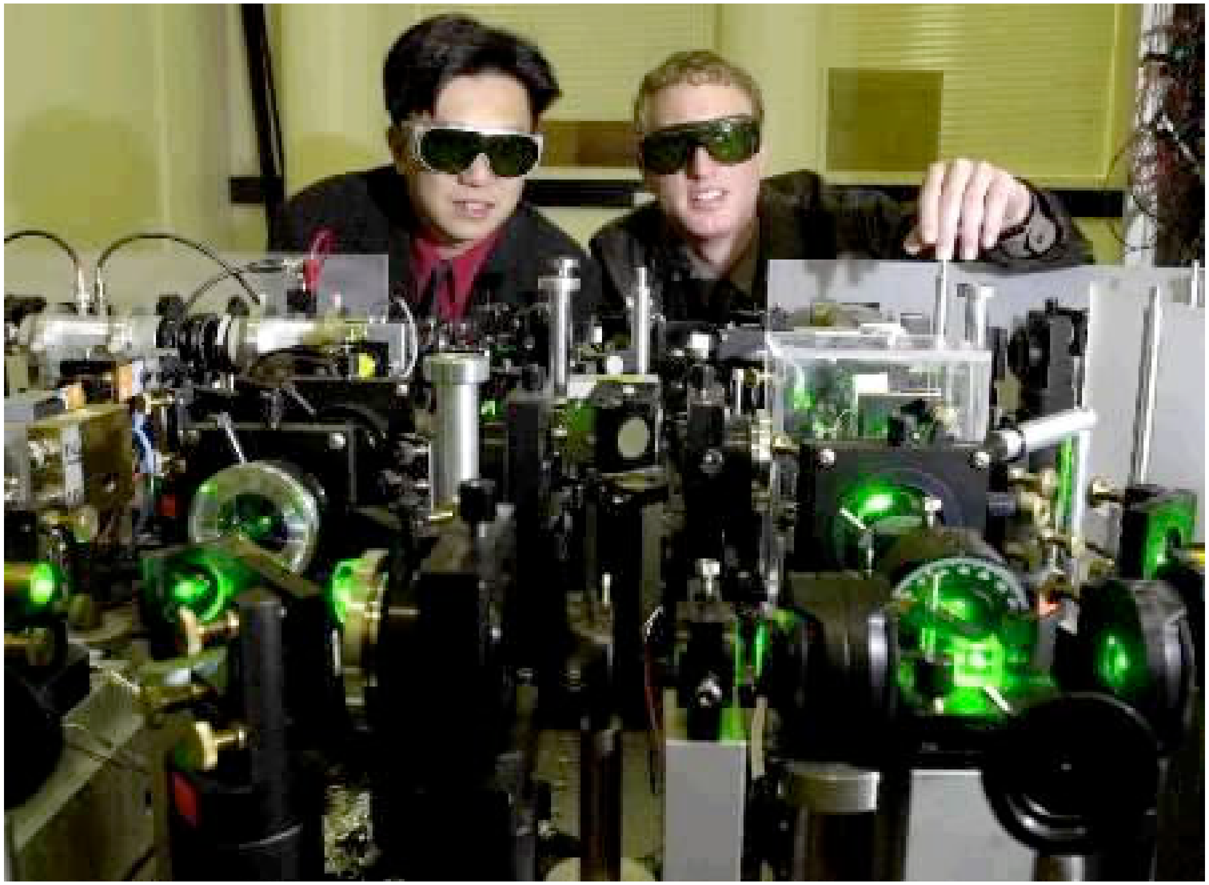
Quantum Teleportation

Bennett *et al*., Phys. Rev. Lett. 70, 1895 (1993)

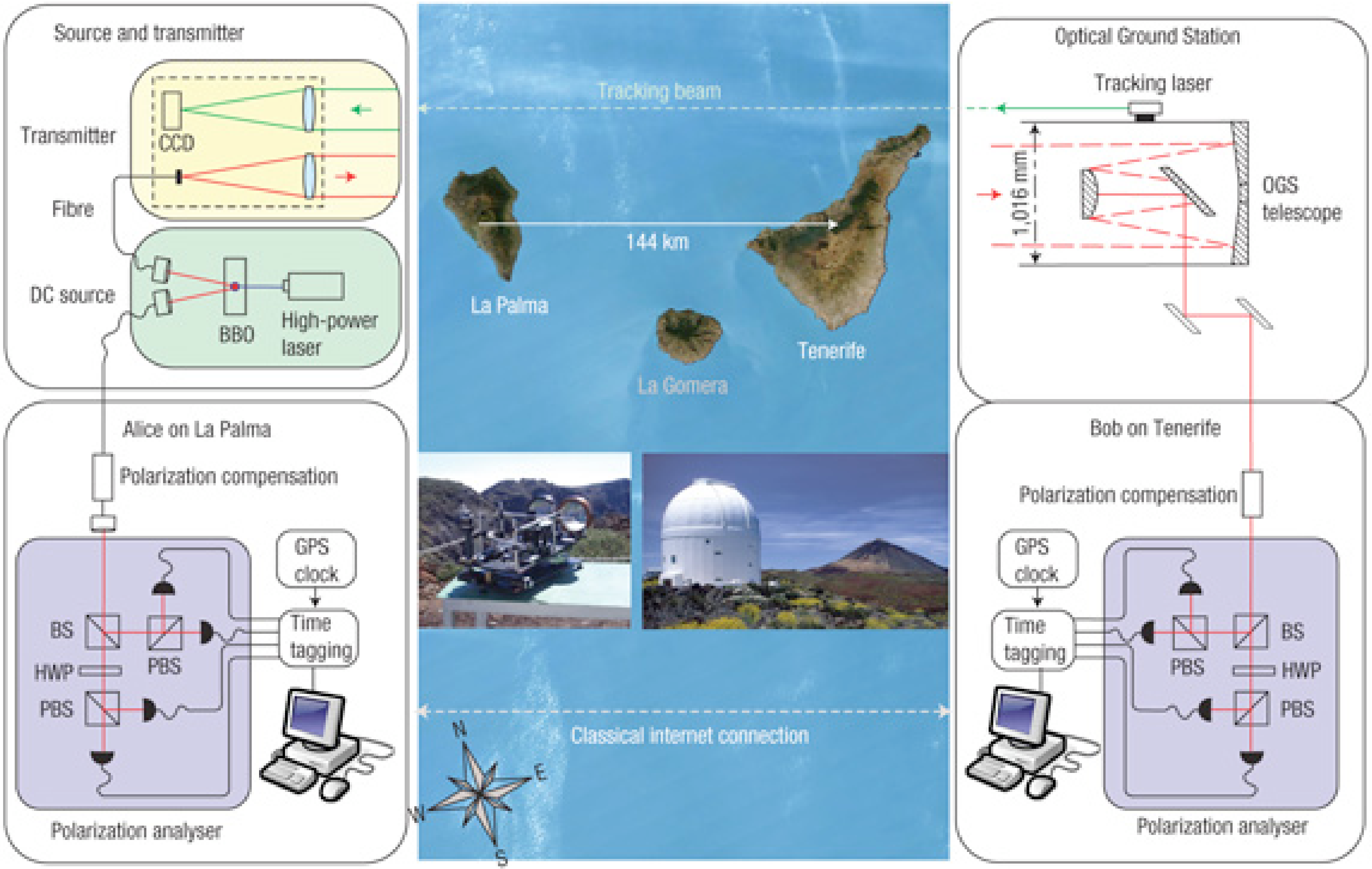


(Bob now has state A – but it's not cloning, because Alice's copy was destroyed!)

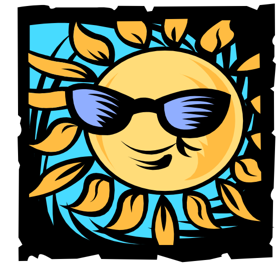
Scotty and his assistant



A good excuse for a junket!
(light teleported over 144 km)



Highly number-entangled states ("3003" experiment).



M.W. Mitchell *et al.*, Nature **429**, 161 (2004)

States such as |n,0> + |0,n> ("noon" states) have been proposed for high-resolution interferometry – related to "spin-squeezed" states.

Important factorisation:

$$\left(a^{\dagger 3} + b^{\dagger 3}\right) = \left(a^{\dagger} + b^{\dagger}\right)\left(a^{\dagger} + e^{2\pi i/3} b^{\dagger}\right)\left(a^{\dagger} + e^{-2\pi i/3} b^{\dagger}\right)$$

A really odd beast: one 0^o photon, one 120^o photon, and one 240^o photon... but of course, you can't tell them apart, let alone combine them into one mode!

Theory: H. Lee *et al.*, Phys. Rev. A 65, 030101 (2002); J. Fiurásek, Phys. Rev. A 65, 053818 (2002)

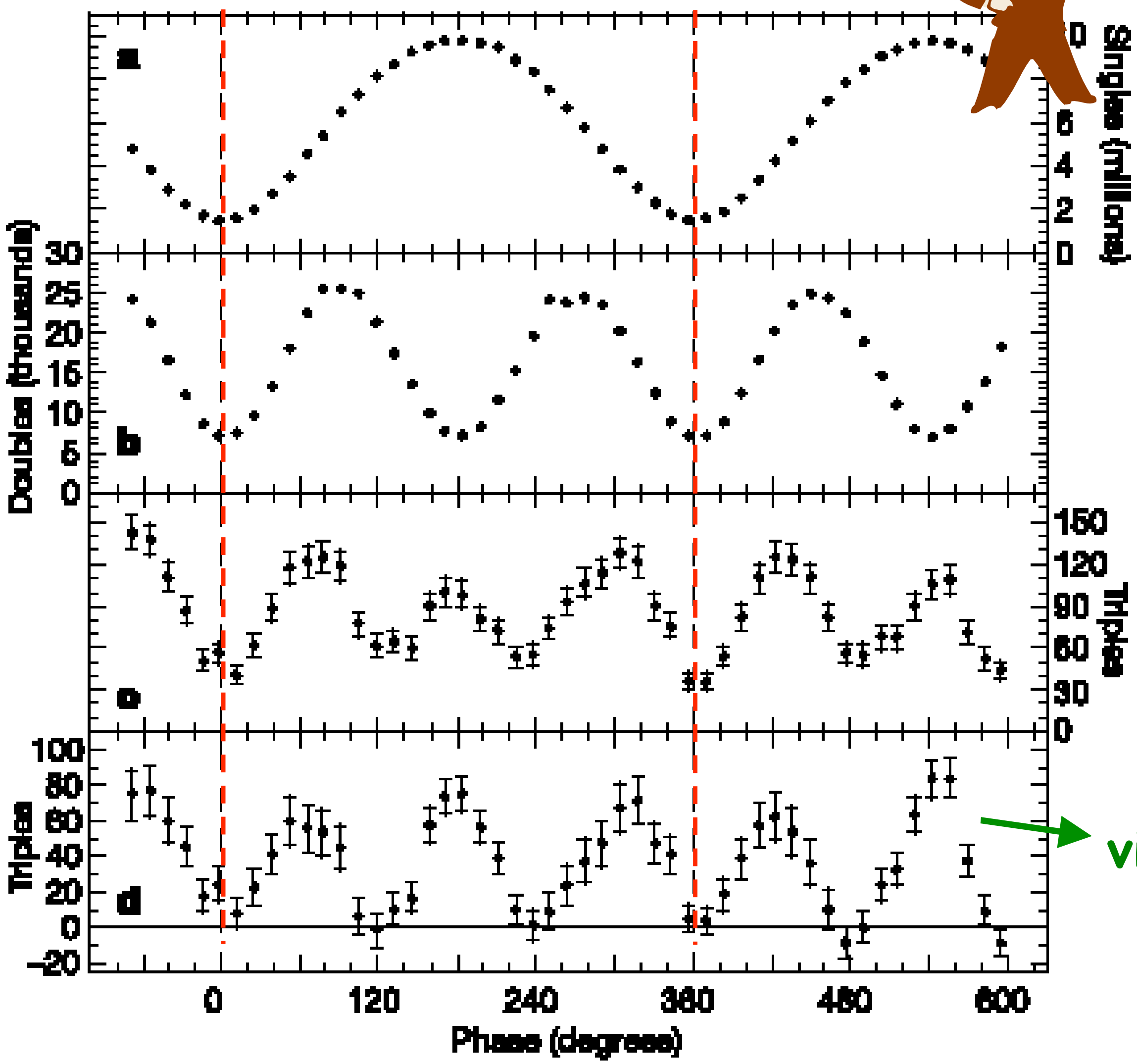
It works!

Singles:

Coincidences:

Triple coincidences:

Triples (bg subtracted):



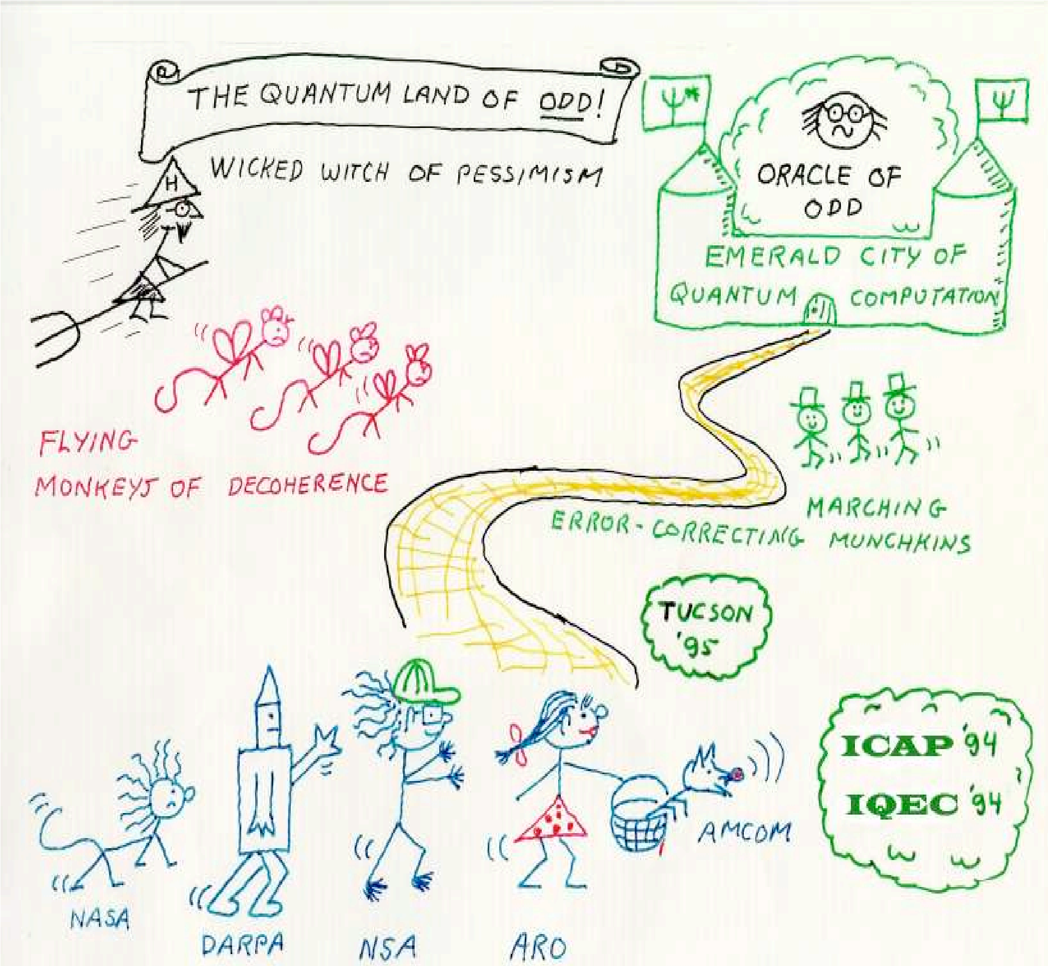
vis > 100% !

M.W. Mitchell, J.S. Lundeen, and A.M. Steinberg, Nature 429, 161 (2004)

Summary

- Light is neither a wave or a particle
- Nor is anything else
- Everything is uncertain – not just unknown to us, but actually unknowable!
- You can't always talk about what one particle is doing without thinking about what others it's "entangled" with are doing too
- Information stored in quantum systems may allow us to do things we could never do classically – faster computers, unbreakable codes, quantum dating game, et cetera...

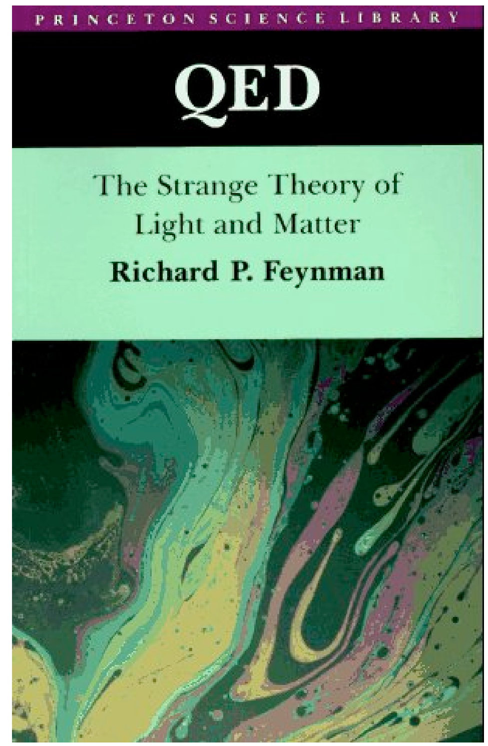
THE END



(Cartoon stolen from Jonathan Dowling)

For more info...

Nick Herbert's "Quantum Reality"
John Gribbin's "Schrödinger's Kittens"
and many more



Links: http://faraday.physics.utoronto.ca/PVB/GeneralInterest.html
http://faraday.physics.utoronto.ca/PVB/Harrison/Flash/index.html