Quantum Interference

Andrew M. Sessler

Lawrence Berkeley Laboratory

Some Remarks

It is a delight to be here once again-- I have fond memories of my first visit to Novosibirsk in 1965 and of subsequent visits In later years.

My subject, today, is not chaos theory (you know much more about that than do I), but rather a topic that should interest Boris -- and all of you -- a great deal (and, hopefully, you don't know more about it than do I).

Actually, I have not published in this area, but I have spent much time studying the subject and like to think I even understand it and can present it rather effectively. We shall see.

Table of Contents

Table of Contents (Continued)

Some Curious Consequences of Quantum Interference

How to Always Win at Coin Tossing

Based on David Meyer, Phys Rev Letters 82, 1052

How to *Always* Win at Coin Tossing

- Classical-Quantum Penny Flip-Over
- 1. Put penny H up in a box
- 2. Q turns the box over or not
- 3. C turns the box over or not
- 4. Q turns it over or not
- 5. If H turns up (not T) then Q (you are Q) wins

Classical Analysis

		NN	FN	FN	FF
Q options across	N	H	T	H	T
C options down	F	T	H	T	H

N is no flip
F is flip
H is heads
T is tails

Check: Second column, first row: Q goes first and N, C goes second and N, Q goes last and F Result should be T

Strategy:
No fixed strategy (or other guy will find out)
Best just flip, or not, with probability 1/2
Payoff: Zero on the average

Quantum Analysis

$$H:\begin{pmatrix}1\\0\end{pmatrix} \quad T:\begin{pmatrix}0\\1\end{pmatrix}$$

$$N:\begin{pmatrix}1 & 0\\0 & 1\end{pmatrix} \quad F:\begin{pmatrix}0 & 1\\1 & 0\end{pmatrix}$$

Check: $$FH=\begin{pmatrix}0 & 1\\1 & 0\end{pmatrix}\begin{pmatrix}1\\0\end{pmatrix}=\begin{pmatrix}0\\1\end{pmatrix}=T$$

Now Q does a very clever thing. He applies U to H, where

$$U=\frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\\1 & -1\end{pmatrix}$$

Quantum Analysis (Continued)

He can do that ! A unitary operator describes some Hamiltonian
And vice versa.

$$U^T = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

Note that $UU^T = I$

Now: $UH = \frac{1}{\sqrt{2}}(H + T) = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 1 \end{pmatrix}$

This is clearly invariant under either F or N !!

Quantum Analysis (Completed)

It doesn't matter what C does. Then Q applies U^T

Then Q gets back H and always wins.

$$U^T(F(UH)) = \frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix}\begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix}\frac{1}{\sqrt{2}}\begin{pmatrix}1\\ 1\end{pmatrix} = \frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\\ -1 & 1\end{pmatrix}\frac{1}{\sqrt{2}}\begin{pmatrix}1\\ 1\end{pmatrix} =$$

$$\frac{1}{2}\begin{pmatrix}2\\ 0\end{pmatrix} = \begin{pmatrix}1\\ 0\end{pmatrix} = H$$

Some Curious Consequences of Quantum Interference

Interaction Free Measurements

Based on the work of A. Elitzur and L. Vaidman,
Foundations of Physics 23, 987 (1993)

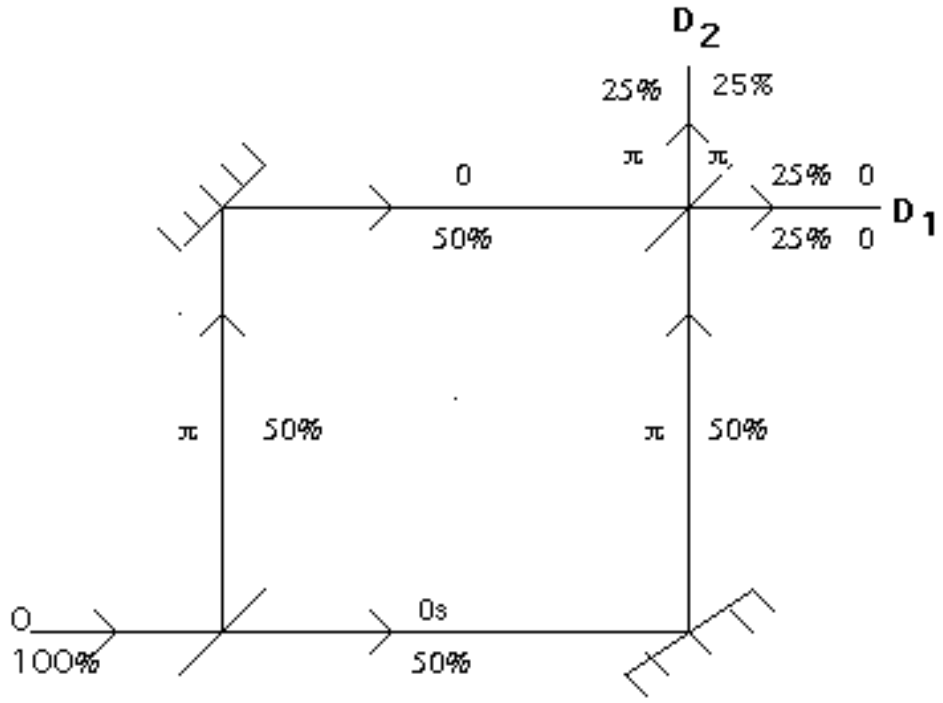
Quantum Mechanical Interaction-Free Measurements

- Classically it is impossible, but quantum
- Mechanically possible. We shall determine whether or not something is there without ever looking at it!

Interaction-Free (Continued)

- Suppose you know something is in one of two boxes and we look at one box and find nothing. Then we know the object is in the other box (without ever looking at it).
- Suppose we have an Einstein-Podolsky-Rosen state and we measure one particle and find it is “up”. Then the other must be down (and we never looked at it).
- Both examples of PRIOR knowledge.
- The scheme shown here requires NO prior knowledge

The Max-Zehnder Interferometer



Interaction Free (continued)

Adjust lengths so that beams at D_2 interfere. 100% goes to D_1

Now put an object in the upper arm. What happens as we send one photon at a time through the interferometer ?

A). No clicks (P=1/2) No information
B). Detector D_1 clicks (P=1/4) No information
C). Detector D_2 clicks (P=1/4) Yes information !

We have determined that an object is there and we never touched it !
The photon clearly went on the lower path (otherwise it would have hi
the object and been scattered away). Yet D_2 only gives a click if the
upper arm is obstructed.

Interaction Free (Continued)

You might think a photon has been split (remember only one photon at a time is going through the interferometer), but that never happens. (In an experiment with detectors just after the first beam splitter, both detectors never go off.)

Can one test a bomb without exploding it ?

We have a stock of bombs with a new, and very sensitive, sensor that explodes the bomb if even a single photon hits the sensor.

Some of the bombs are broken and a small part of the sensor is missing so a photon just passes through and the bomb is not exploded.

Interaction Free (Continued)

Is it possible to determine which bombs are still working without blowing up the bomb (i.e., still having it for use) ?

Impossible in classical physics, but perfectly possible quantum mechanically.

Put the bomb on the upper path. Send through one photon at a time. Keep doing that until
A). The bomb goes off, or
B). Detector D_2 clicks.

When D_2 gives a click we have achieved what we desired: We know that the bomb is good and we haven't set it off !

Interaction Free (Continued)

Probabilities: (A good bomb is used)

P=1/2 to explode the bomb (Half the photons go on the upper path)

P=1/4 to have detector D_1 click and that tells us nothing
(Actually D_1 could be eliminated)

P=1/4 to have D_2 click and we learn the bomb is good

So probability of finding a good bomb is 1/4 + 1/4*1/4
+1/4*1/4*1/4+..
or 1/3. Can get this up to 1/2 by not using half-silvered mirrors.

Interaction Free (Completed)

1.All this can be done with state vectors, but the formalism adds nothing (except confusion).
2. Notice that Planck's constant never appeared and yet this is a purely quantum mechanical phenomena.
2.Why is this of interest ? At least two reasons (beyond the interest of terrorists):
A). Gravity wave detectors (Future generations, as right now other sources of noise are dominant).
B). Quantum computers (They are based on this sort of thing)

Some Curious Consequences of Quantum Interference

One Photon and Two Slits

(Quantum Erasers and Delayed Choice)

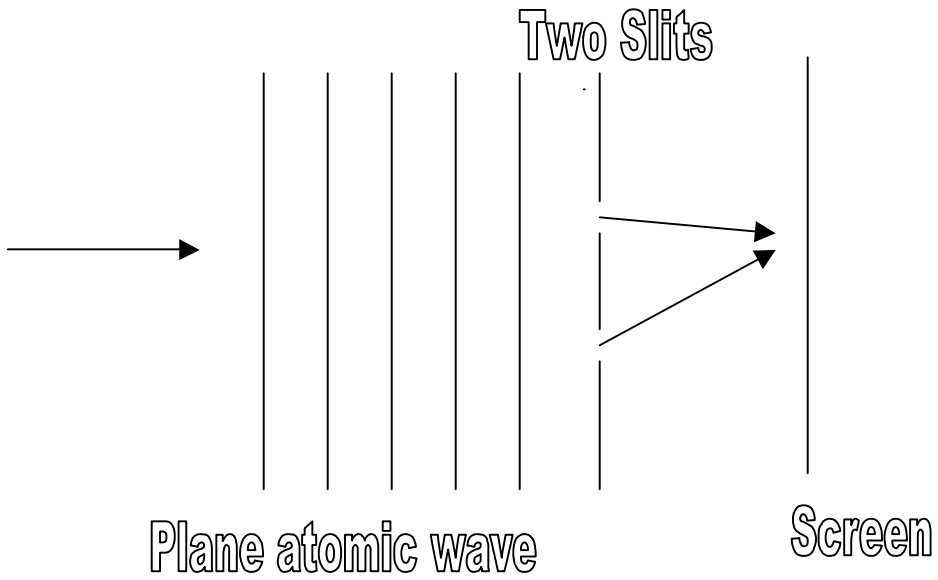
Based on the work of:

Marlan Scully and Herbert Walther, Found. Of Physics 28, 39 (1998)

M. Scully, B-G Engbert and H. Walther, Nature 351, 111 (1991) and

Am. J. of Phys 67, 325 (1995)

One Photon, Two Slits (Continued)



Slits far apart: Diffraction
Close one slit: Diffraction
Slits close together: Interference

One Photon, Two Slits (Continued)

Send through one atom at a time.
Do you get an interference pattern? Yes
(One can think of the atom as a wave as it goes through the slits, but as a particle as it hits the screen.

Einstein said one could measure the recoil of the slits and thus tell which slit the atom went through. But that was wrong, as Bohr showed, for if the measurement of transverse momentum is precise enough to tell which slit the atom went through, then the slit's position is unknown enough to not be able to tell which slit was used.

One Photon, Two Slits (Continued)

Suppose there is a cloud chamber that allows one to tell which slit the atom went through. Interference pattern? No

Suppose one has a cloud chamber but doesn't look. Interference pattern? No

The analysis of cloud chambers, and Bohr's uncertainty principle seem to depend upon modifying the motion of the center of mass. (That is what I learned in school)

But it isn't true at all !

One Photon, Two Slits (Continued)

An atomic interference experiment (we need an atom for this)
An atomic beam is in an excited state and gives up a photon in going through the cavity. We can look at the cavity(after the atom has gone by) and see if there is a photon in #1 or #2. Interference pattern?
{Notice we have had *no* effect, by the observation, on the center of mass motion.}
No

Let us do some analysis:

The Set-Up

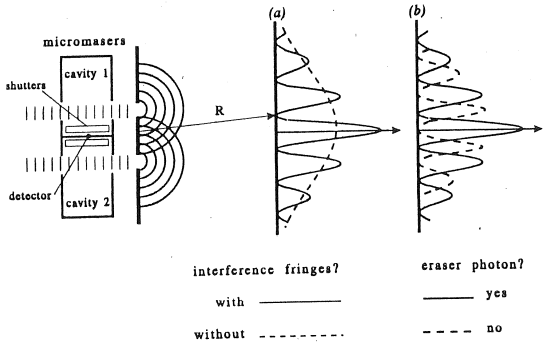


Fig. 1. Quantum eraser overview. (a) Electro-optic shutters separate microwave photons in two cavities. (b) Detector wall absorbs microwave photons and acts as a photodetector. Plot is density of particles on the screen depending upon whether a photocount is observed in the detector wall ("yes") or not ("no"), demonstrating that correlations between the event on the screen and the eraser photocount are necessary to retrieve the interference pattern.

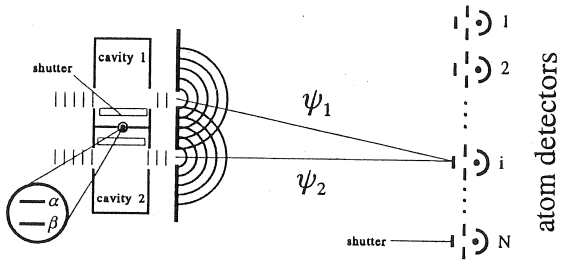


Fig. 2. Quantum eraser detector array. The photon detector in Fig. 1 is represented by a two-level system which is excited upon absorption of a photon. The screen consists of an array of atom detectors.

The Set-Up

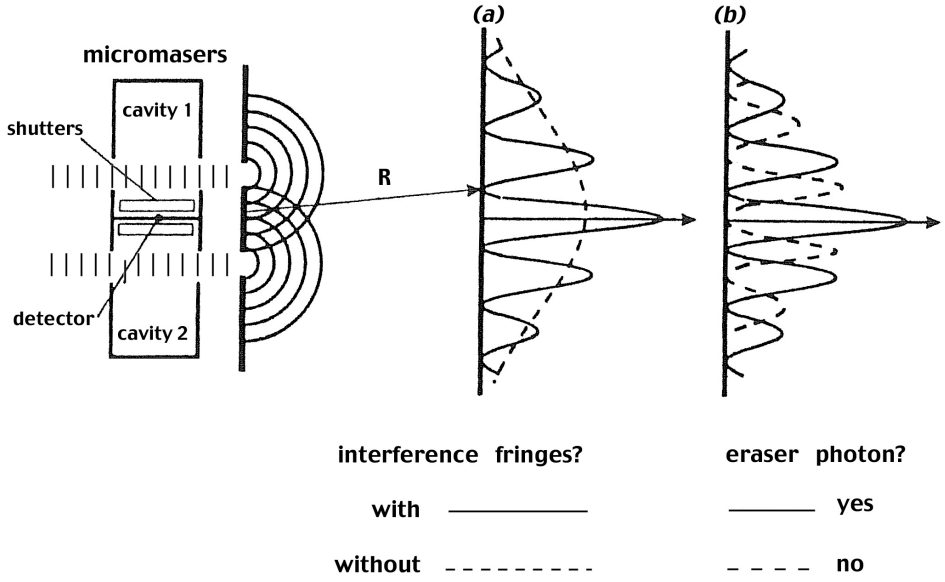


Fig. 1. Quantum eraser overview. (a) Electro-optic shutters separate microwave photons in two cavities. (b) Detector wall absorbs microwave photons and acts as a photodetector. Plot is density of particles on the screen depending upon whether a photocount is observed in the detector wall ("yes") or not ("no"), demonstrating that correlations between the event on the screen and the eraser photocount are necessary to retrieve the interference pattern.

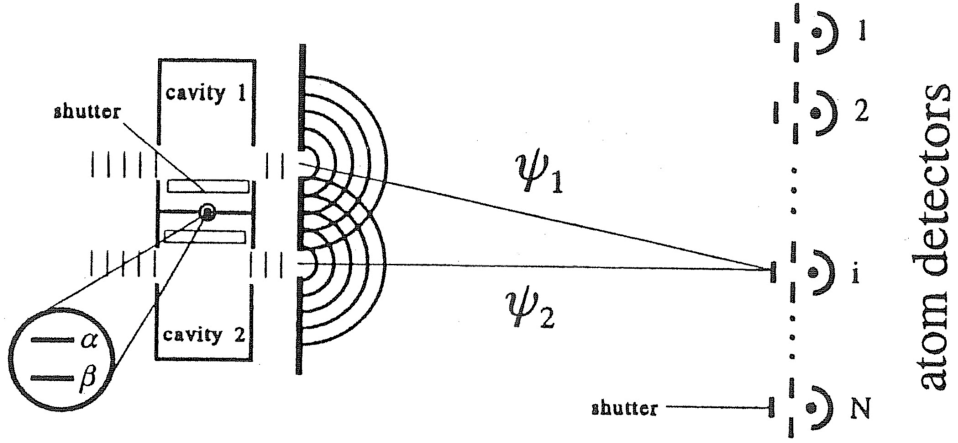


Fig. 2. Quantum eraser detector array. The photon detector in Fig. 1 is represented by a two-level system which is excited upon absorption of a photon. The screen consists of an array of atom detectors.

One slit, Two cavities (continued)

If there are no cavities:

$$\psi = \frac{1}{\sqrt{2}}[\psi_1(r) + \psi_2(r)]|i\rangle$$

#1 and #2 indicates the slit through which it passes

The i indicates the internal state of the atom

$$P(r) = \frac{1}{2}\left(|\psi_1(r)^2| + |\psi_2(r)^2| + \psi_1{}^*\psi_2 + \psi_1\psi_2{}^*\right)\langle i|i\rangle$$

We see the interference term

One slit, Two cavities (Continued)

Now suppose there are the two cavities:

$$\psi = \frac{1}{\sqrt{2}}[\psi_1(r)|1_1,0_2\rangle + \psi_2(r)|0_1,1_2\rangle]$$

This indicates a photon in #1 and no photon in #2 for the Atom going though slit #1 and the same for #2. Entangled !

$$P(r) = \frac{1}{2}\left(|\psi_1(r)^2| + |\psi_2(r)^2| + \psi_1{}^*\psi_2\langle 1_1 0_2|0_1 1_2\rangle + \psi_1\psi_2{}^*\langle 0_1 1_2|1_1 0_2\rangle\right)$$

But the brackets are zero and there is *no* interference
Even if we don't look !

One photon, Two slits (continued)

So, in this case we get no interference not to uncertainty in position, but due to the entanglement.

Now let us go onto what is called a quantum eraser The detector is (say) an atom in its lowest state d and it can get excited to state e.

Introduce symmetric and anti-symmetric states of the photons in cavities #1 and #2. (We are going to open the shutter so this is convenient.)Equally good to the above description.

One photon, Two slits (Continued)

$$|\pm\rangle = \frac{1}{\sqrt{2}}\left(|1_1, 0_2\rangle \pm |0_1, 1_2\rangle\right)$$

Do the same for atoms:

$$\psi_{\pm} = \frac{1}{\sqrt{2}}[\psi_1(r)|1_1, 0_2\rangle \pm \psi_2(r)|0_1, 1_2\rangle]$$

Consider our previous expression:

$$\psi = \frac{1}{\sqrt{2}}[\psi_1(r)|1_1, 0_2\rangle + \psi_2(r)|0_1, 1_2\rangle]|d\rangle$$

One photon, Two slits (Continued)

The d just indicates the detector in the ground state
Equivalently becomes:

$$\psi = \frac{1}{\sqrt{2}}\left[\psi_{+}|+\rangle + \psi_{-}|-\rangle\right]$$

Now the eraser ! Long after the atom has gone through the device, we open the shutters and mix up the photons. We have erased the information about which Cavity the atom went through.Will we see an interference pattern? Yes (when correlated with the detector; not otherwise).

One photon, Two slits (continued)

When the shutter is open (eraser system), we have
The state:

$$\psi = \frac{1}{\sqrt{2}}\left[\psi_+ |+\rangle |e\rangle + \psi_- |-\rangle |d\rangle\right]$$

(Because only the symmetric state excites the detector)
Now:

$$P(r) = \frac{1}{2}\left(|\psi_+|^2 + |\psi_-|^2\right) = \frac{1}{2}\left(|\psi_1|^2 + |\psi_2|^2\right)$$

No interference

One photon, Two slits (Continued)

However, if we ask that the detector is excited (and the atom has long since hit the screen), then:

$$P(r) = (\psi_+)^2 = \frac{1}{2}\left(|\psi_1|^2 + |\psi_2|^2 + R(\psi_1^* \psi_2)\right)$$

And now there is interference !

Similarly if the detector is not excited:

$$P(r) = [\psi_+]^2 = \frac{1}{2}\left(|\psi_1|^2 + |\psi_2|^2 - R(\psi_1^* \psi_2)\right)$$

The sum of these two interference patterns is a pure diffraction pattern.

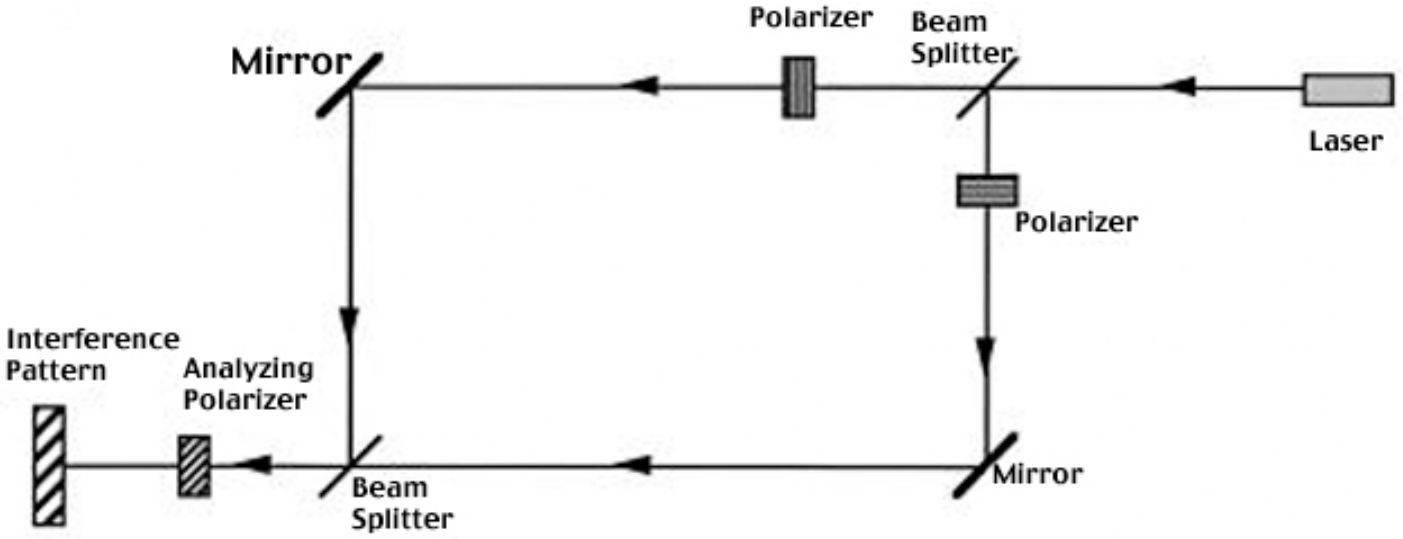
One photon, Two slits (Continued)

So; long after the atom has gone by (delayed choice) we can destroy the information about which slit the atom went through, but recover an interference by making a correlation.

A Simple Interference Experiment

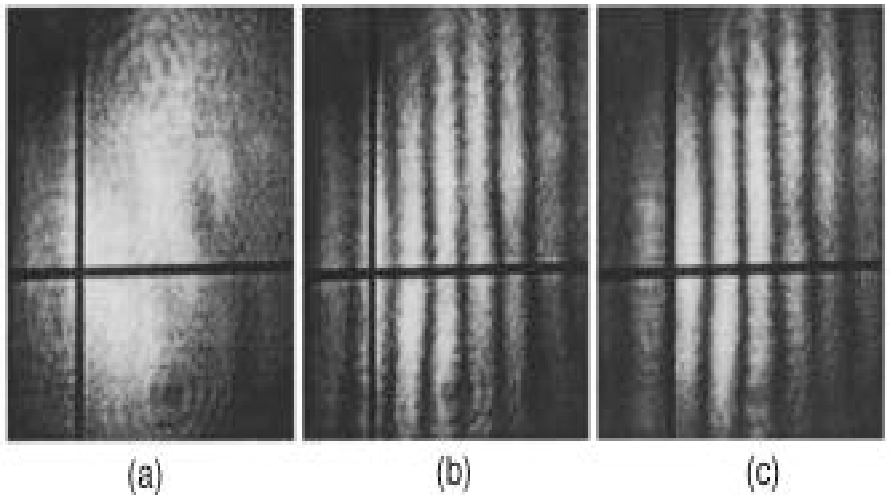
Having a which-way detector and a quantum eraser (But not "delayed")

Based upon the work of M. Scneider and I. La Puma,
Am.J. of Phys 70, 266 (2002)



Schematic view of the interferometer. Note the direction (now right to left) and the polarizers.

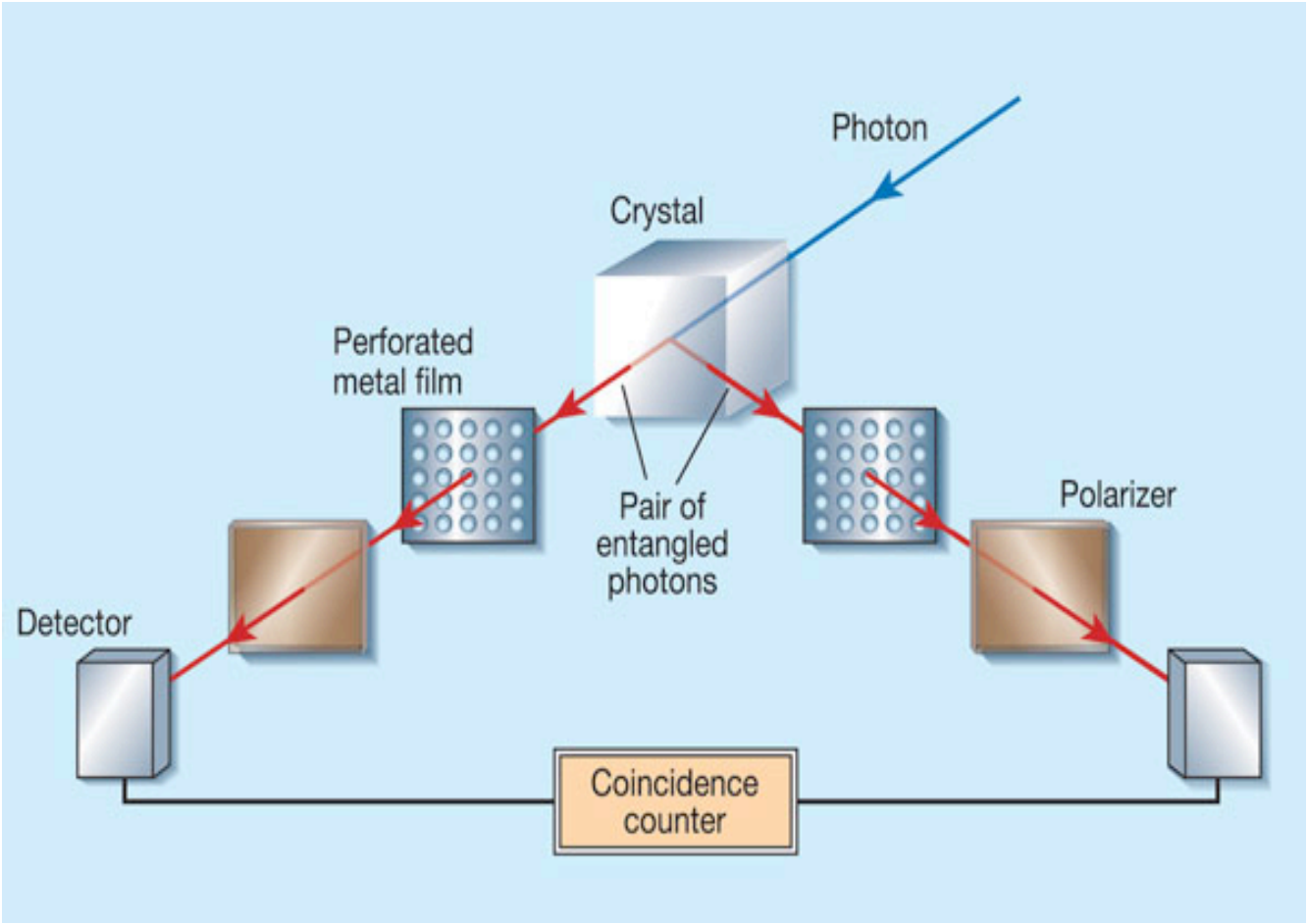
A Simple Interferometer Experiment



Photographs of the interference patterns projected on a white screen. (a) The pattern resulting when which-way information is encoded in the polarization; (b) the pattern given after a final analysis by a 45° polarizer; (c) analyzed with a–45° polarizer. The black cross is only to allow comparison of registration between figures. Note that (b) and (c) are complementary.

Quantum Interference (Even through perforated metal foils)

Altewischer et al Nature 418, 304 (2002)



Some Curious Consequences of Quantum Interference

Two Photons and Two Slits

(More magic)

Anton Zellinger

Rev. of Modern Phys. 71,
S288 (1999)

Two photons, Two slits (continued)

We now show that the picture of a photon travelling as a wave through slits and then detected as a particle, is hopelessly wrong.

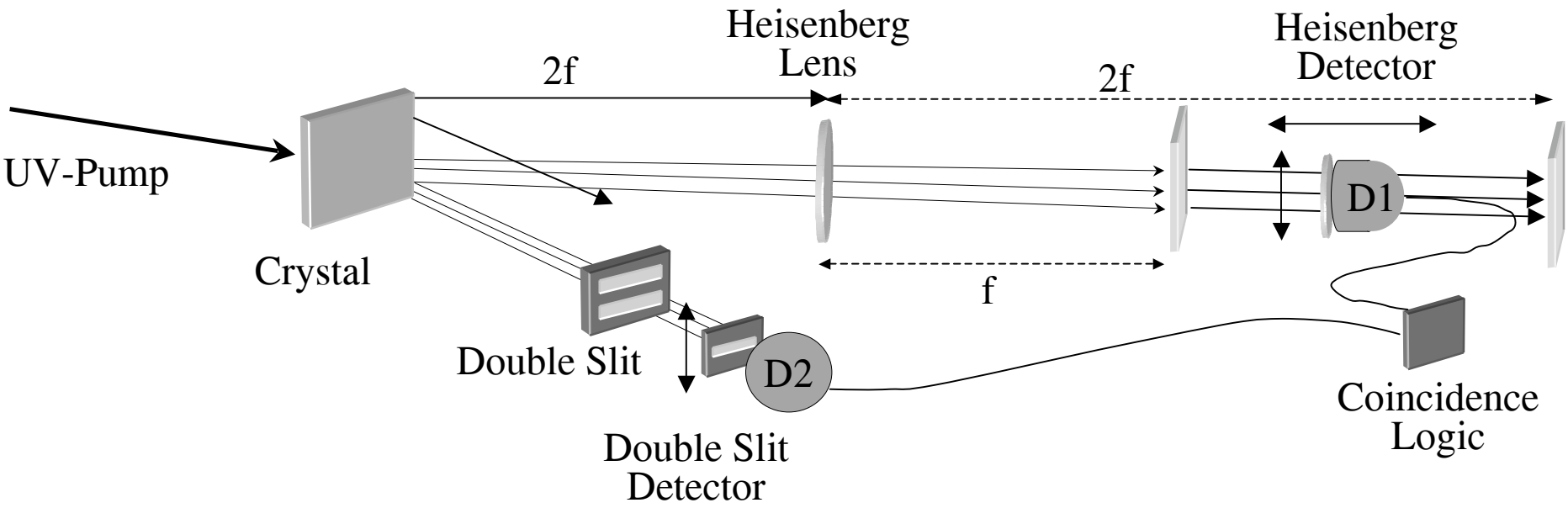
We saw previously that ψ_1 and ψ_2 are complimentary to ψ_+ and ψ_-. We had a choice which to measure (use as a basis), but that we couldn't measure both (complimentarity).

Here it is shown that we can decide, long after registration of the photon whether a "wave feature" or a "particle feature" manifests itself.

Two photons, Two slits (continued)

- Realistic pictures for quantum phenomena just don't work. As Roger Penrose said, "Quantum theory makes absolutely no sense".
- Consider the following set-up (actually done by Dopfer, but here generalized a bit).

Two photons, two slits (continued)



Two photons, two slits (continued)

Two entangled photons

#2 goes through the double slit
#1 goes to “Heisenberg detector”

The Heisenberg detector can be far away so it is effective only long after photon #2 has gone through the double slit and hit detector #2

Two photons, two slits (continued)

If detector D1 is in the focal plane then it registers the transverse momentum of the photon before it enters the lens. Hence we know the momentum of photon #2 and nothing about its position. We *do* get an interference pattern.

If detector D1 is in the imaging plane then we can tell which slit photon #2 went through and the interference pattern is *gone*.

Two photons, two slits (continued)

Some curious aspects:

1. By varying D1 we can go continuously from only diffraction to interference (Fringes get sharper and sharper)

2. Note that we do things on photon #1 and that effects what photon #2 does !!

3. Note that what we do to photon #1 can be done long after photon #2 hits D2 !!

Two photons, two slits (continued)

(In the next version of he experiment they will choose position of D1 after the fact by random choice.)

4. If don't look at photon #1 then photon #2 makes a diffraction pattern (because the information to determine which slit photon #1 went through could be extracted).

5. Only when photon #1 is registered in the focal plane of the lens does one see an interference pattern in photon #2.

Two photons, two slits (continued)

6. Put D1 in the focal plane of the lens. Move it laterally. Make a coincidence with photon #2 getting to D2. What does one see? A pure diffraction pattern of photon #1 (even though it never passed through any slits!!)

Measuring photon #1 simultaneously in the focal plane and the image plane is impossible. They are complimentary. Our choice which to do. The whole apparatus must be considered. It is not possible to ascribe reality to one photon.

The No-Cloning Theorem

W.K. Wooters and W. H.Zurak, Nature 299, 802 (1982)
D. Dicks, Pys. Rev. Lett. A92, 271 (1982)

A. Steane has said, “Even though one can clone a sheep, one cannot clone a single photon”

Consequences of the theorem:
1. Cryptography is possible
2. Quantum computers only produce very limited information
3. Error correction is hard (but not impossible)
4. Teleportation is hard (but not impossible)

The No-Cloning Theorem (continued)

Theorem: It is impossible to build a machine that will take an arbitrary quantum state, preserve it and make an exact copy of the state.

Proof: Describe the "machine" as a unitary transformation U that works on the arbitrary state ψ. Assume the theorem is true and show a contradiction.

$$U(|\psi\rangle|0\rangle) = |\psi\rangle|\psi\rangle$$

The symbol 0 is the input state we want to convert.

The No-cloning Theorem (continued)

Consider another state φ. Clearly, U working on this state must give

$$U(|\varphi\rangle|0\rangle) = |\varphi\rangle|\varphi\rangle$$

However, by linearity we must have:

$$U(|a\psi + b\varphi\rangle|0\rangle) = a|\psi\rangle|\psi\rangle + b|\varphi\rangle|\varphi\rangle$$

But, if U clones arbitrary states then:

$$U(|a\psi + b\varphi\rangle|0\rangle) = |a\psi + b\varphi\rangle|a\psi + b\varphi\rangle$$

$$= a^2|\psi\rangle|\psi\rangle + b^2|\varphi\rangle|\varphi\rangle + ab|\psi\rangle|\varphi\rangle + ba|\varphi\rangle|\psi\rangle$$

The No Cloning theorem (continued)

Which differs, so there is a contradiction with the assumption that U exists.

Thus the theorem is proved.

Quantum Teleportation

C.H. Bennett et al, Phys. Rev. A54, 3824 (1996)
Lots of experimental work by Anton Zelinger (26 PRL in the last 3 years)
See Phys. Rev. Lett. 86, 4435 (2001) for a start
(Presentation based on an article by Richard Jozsa)

First we need to discuss entanglement as that is at the heart of teleportation and quantum computers. There are
thousands of papers on the subject.

First, consider a single qubit. Define an ortho-normal basis 0❭ and 1❭. (Like spin up and down.)
Then a qubit is:

$|\psi\rangle = \cos\theta\,|0\rangle + e^{i\phi}\sin\theta\,|1\rangle$

Quantum Teleportation (continued)

A qubit carries lots of information, namely all the digits needed to specify θ and ϕ. (A classical bit is simply on or off; a qubit is much more.)

Now, consider two qubits. We can entangle them. Call then A (Alice) and B (Bob) and they are often physically far apart. For example (there are other ways to entangle, but this is one):

$$|\psi\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle_A|1\rangle_B - |1\rangle_A|0\rangle_B\right)$$

In the direct product the first state will always be qubit A and the second state qubit B.

Quantum Teleportation (continued)

Consider four special states that span the two qubit space. They are called Bell States and they are very convenient. They are:

$$|\psi^-\rangle = \frac{1}{\sqrt{2}}(|0\rangle_A|1\rangle_B - |1\rangle_A|0\rangle_B)$$

$$|\psi^+\rangle = \frac{1}{\sqrt{2}}(|0\rangle_A|1\rangle_B + |1\rangle_A|0\rangle_B)$$

$$|\varphi^-\rangle = \frac{1}{\sqrt{2}}(|0\rangle_A|0\rangle_B - |1\rangle_A|1\rangle_B)$$

$$|\varphi^+\rangle = \frac{1}{\sqrt{2}}(|0\rangle_A|0\rangle_B + |1\rangle_A|1\rangle_B)$$

Alice alone -- only acting on her qubit -- can go from one of these states to the other.

Quantum Teleportation (continued)

Consider the four 1-qubit unitary operators:

$$U_{00} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

$$U_{01} = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$$

$$U_{10} = \begin{bmatrix} 0 & -1 \\ -1 & 0 \end{bmatrix}$$

$$U_{11} = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}$$

U_{00} takes $0\rangle$ into $0\rangle$ and $1\rangle$ into $1\rangle$

U_{01} takes $0\rangle$ into $0\rangle$ and $1\rangle$ into $-1\rangle$

U_{10} takes $0\rangle$ into $-1\rangle$ and $1\rangle$ into $-0\rangle$

U_{11} takes $0\rangle$ into $1\rangle$ and $1\rangle$ into $-0\rangle$

One can easily see that the U operators take the Bell states into each other.

Now, on to teleportation !

Quantum Teleportation (continued)

Suppose Alice is given a qubit $|\psi\rangle$ and desires to send it to Bob. How can she do that? (Of interest, for example, in quantum computers where she might be half-way through a calculation and desire that Bob complete it.)

A) She can put $|\psi\rangle$ in a box that shields it from the noisy environment and send it to him.
B) If she knows $|\psi\rangle$ (if not measurement will destroy much of it) then she can send, classically, the values of *a* and *b* in $|\psi\rangle = a|0\rangle_C + b|1\rangle_C$, but that takes lots and lots of bits in order just to transfer one qubit.

Quantum Teleportation (continued)

But, remarkably enough, Alice can send $\psi\rangle$ to Bob !
The no cloning theorem would seem to make this impossible, but not so ! (Alice will not "look at" $\psi\rangle$, not try to clone it, but simply "send it on" to Bob.)

But, Alice and Bob need to be sharing entangled qubits.
Suppose $\psi^-\rangle_{AB}$ is the entangled pair (in Bell State ψ^-).
And the state to transfer is $\psi\rangle = a\,0\rangle_C + b\,1\rangle_C = \psi\rangle_C$.

Alice has A and C; Bob has B

Quantum Teleportation (continued)

$$|\Psi\rangle_{ABC} = |\psi\rangle_C |\psi^-\rangle_{AB}$$

$$|\Psi\rangle_{ABC} = \frac{1}{\sqrt{2}}\left(a|0\rangle_C + b|1\rangle_C\right)\left(|0\rangle_A|1\rangle_B - |1\rangle_A|0\rangle_B\right)$$

$$|\Psi\rangle_{ABC} = \frac{1}{2}\left\{\begin{array}{l}|\psi^-\rangle_{CA}\left(-a|0\rangle_B - b|1\rangle_B\right) + |\psi^+\rangle_{CA}\left(-a|0\rangle_B + b|1\rangle_B\right) + \\ |\varphi^-\rangle_{CA}\left(b|0\rangle_B + a|1\rangle_B\right) + |\varphi^+\rangle_{CA}\left(-b|0\rangle_B + a|1\rangle_B\right)\end{array}\right\}$$

Now Alice performs a Bell measurement on C and A (and regardless of $\psi\rangle_C$ each comes out with probability 1/4 so she learns nothing about $\psi\rangle_C$).

Quantum Teleportation (continued)

Because of the measurement Bob's qubit is:

$$(-a|0\rangle_B - b|1\rangle_B) = -U_{00}|\psi\rangle_B$$
$$(-a|0\rangle_B + b|1\rangle_B) = -U_{01}|\psi\rangle_B$$
$$(b|0\rangle_B + a|1\rangle_B) = -U_{10}|\psi\rangle_B$$
$$(-b|0\rangle_B + a|1\rangle_B) = U_{11}|\psi\rangle_B$$

All Alice needs to do is tell Bob the outcome of her measurement; namely *i* and *j*. Bob now applies the inverse of U_{ij} to his qubit and it becomes $\psi\rangle$.

Quantum Teleportation (continued)

So, only two classical bits are required to transfer the full quantum information. Information flows backwards
in time !

This idea is the basis for error correcting codes in quantum computers. (Essentially making such computers a real possibility.)

Quantum teleportation

Jozca

Figure 2: Quantum teleportation. The figure shows a spacetime diagram just as in Fig. 1 with the EPR pair created at t_0. Alice also has input qubit. At time t_1 Alice performs a Bell measurement on the joint state of her input qubit and her EPR particle and sends the outcome *ij* to Bob. On reception at t_2 Bob applies -U*ij* to his particle which is then guaranteed to be in the same state as Alice's original input qubit.

Quantum Money

Stephen Wiesner, Sigact News 15, 78 (1983)

Really these are quantum checks, not cash, for the bank is needed to confirm its validity at each
transaction.

The importance of this early work was not appreciated at the time.

It is impossible, in principle, to counterfeit this money.

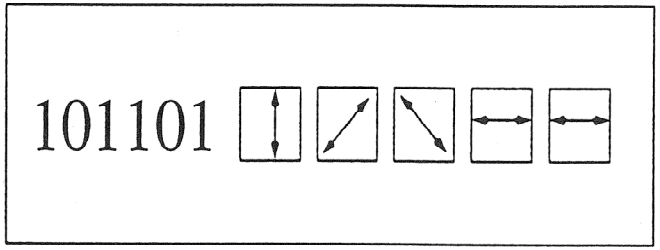
Quantum Money (continued)

On each note there is a serial number and trapped photons of various polarizations (not so easy to do in practice !).

The bank has a record of the polarization basis and of the actual polarization.

The bank can easily check that the polarization hasn't been messed up.

Quantum Money (continued)



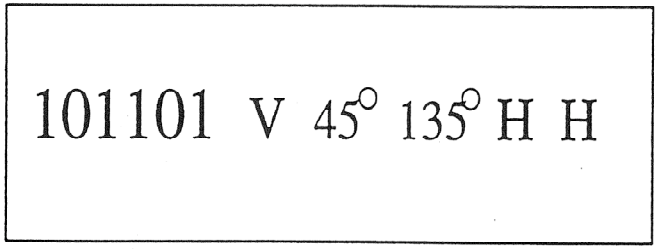


Figure 2: In addition to a serial number, a sequence of single photons are kept in a bank note. The polarizations of those photons are a secret which is kept in the bank record.

Quantum money (continued)

But a counterfeiter is ignorant of the polarization basis and 1/2 the time he will get it wrong. Of the wrong ones, 1/2 will get by the banks test. So he has

A chance = 1/2 +1/2 x1/2 = 3/4 of success. If there are

N photons then only $(3/4)^N$ chance of success; i.e., only an exponentially small chance (N large) of success.

Quantum money (continued)

One sees how for this to work -- and exactly the same principle makes quantum cryptography possible -- the no-cloning theorem is vital.

(Otherwise one just clones the state many times and tries different orientations of the polarization until one gets the same answer every time.)

Quantum Cryptography

Benett and Brussard, IEEE Int. Conf. On Computers, p.175 (1984)

I will only describe the BB84 scheme.(Many others exist.)

The system is absolutely secure. Therefore it is of great interest to the military, the banks, etc.

It is real. That is, it has already been done over tens of kilometers and Los Alamos is gearing up to transmit to satellite.

Cryptography accounts for the money supporting the whole field of teleportation and quantum computers.

Quantum Cryptography (continued)

Two channels are needed:

1. Classical: public and unjammable.
   (Anyone can read, no one can alter.
   Like the NY Times).
2. Quantum: Insecure.
   (Eavesdroppers can play around as they desire.)

Quantum Cryptography (continued)

Hoi-Kwong Lo

(1) Alice sends Bob a sequence of photons, each of which is chosen randomly and independently to be in one of the four polarization (horizontal, vertical, 45 degrees and 135 degrees). (Fig. 5, Step 1.)

(2) For each photon, Bob randomly chooses either the rectilinear or diagonal bases to perform a measurement. (Fig. 5, Step 2.)

(3) Bob records his bases used and the results of the measurements. (Fig. 5, Step 3.)

(4) Subsequently, Bob announces his bases (but *not* the results) publicly through the public unjammable channel that he shares with Alice. (Fig. 5, Step 4.)

Notice that it is crucial that Bob publicly announces his basis of measurement only *after* the measurement is made. This ensures that the eavesdropper, Eve, does not know the right basis during eavesdropping. If Bob were to announce his basis before the measurement, Eve could simply eavesdrop along the announced basis without being detected.

(5) Alice tells Bob which measurements are done in the correct bases. (Fig. 5, Step 5.)

Quantum Cryptography (continued)

Hoi-Kwong Lo

(6) Alice and Bob divide up their polarization data into four classes according to the bases used by them. See Fig. 7. In cases (a) and (b), Bob has performed the wrong type of measurement (i.e., Alice and Bob have used difference bases). They should throw away those polarization data. On the other hand, in cases (c) and (d), Bob has performed the correct type of measurement (i.e., Alice and Bob have used the same bases).

Notice that if no eavesdropping has occurred, all the photons that are measured by Bob in the correct bases should give the same polarization as prepared by Alice. Bob can determine those polarizations by his own detector without any communications from Alice. Therefore, Alice and Bob can use those polarization data as their raw key. Of course, before they proceed any further, they should sacrifice a small number of those photons to test for eavesdropping. For instance, they can do the following:

(7) Alice and Bob randomly pick a fixed number say m_1 photons from case (c) and compute its experimental error rate, e_1. Similarly, they randomly pick m_2 photons from case (d) and compute its experimental error rate, e_2.[n]

If either e_1 or e_2 is larger than the maximal tolerable error rate e_{max}, either substantial eavesdropping has occurred or the channel is unexpectedly noisy. Alice and Bob should, therefore, discard all the data and start with a fresh batch of photons. On the other hand, if both e_1 and e_2 are smaller than e_{max}, they proceed to step 8.

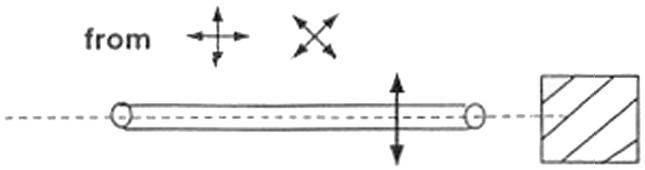
(8) Reconciliation and privacy amplification: Alice and Bob and independently convert the polarizations of the remaining photons into a raw key by, for example, regarding a horizontal or 45-degree photon as denoting a ‘0’ and a vertical or 135-degree photon a ‘1’.

The Scheme

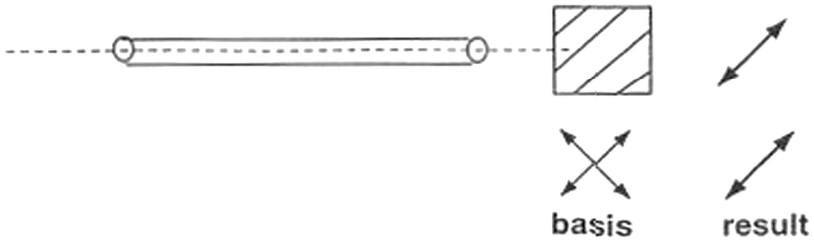
Lo

Step 1: Alice picks polarization randomly from

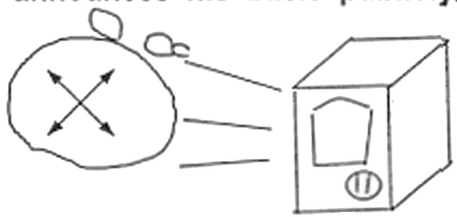
Step 2: Bob picks basis randomly from



Step 3: Bob records his basis and measurement results.



Step 4: Bob announces his basis publicly.



Step 5: Alice tells Bob if he has chosen the correct basis.

Step 6: Test for tampering, error correction and privacy amplification.

Figure 5: Procedure of the BB84 scheme for quantum key distribution.

In Detail

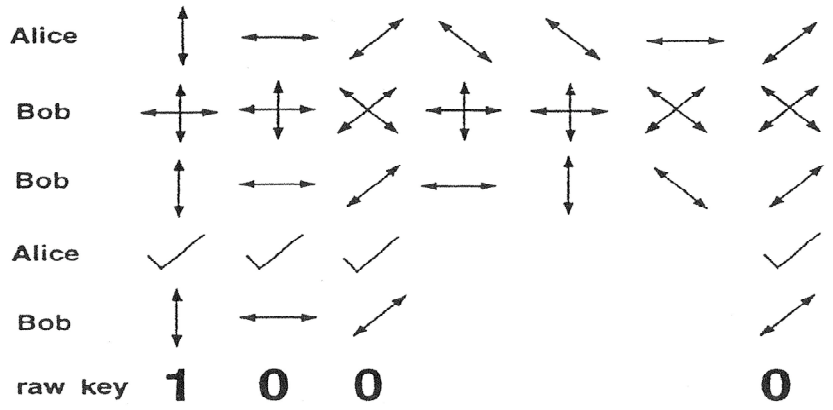


Figure 6: A sequence of photons are sent by the BB84 scheme. For each photon, Alice chooses its polarizations randomly from horizontal, vertical, 45-degree and 135-degree. Bob then randomly chooses the rectilinear or diagonal basis to perform a measurement. He writes down the result of his measurement. Alice and Bob public compare their basis. Whenever they have used the same basis, they can convert their polarization data into a single raw bit. Of course, they need to test for tampering and go through error correction and privacy amplification as described in the text.

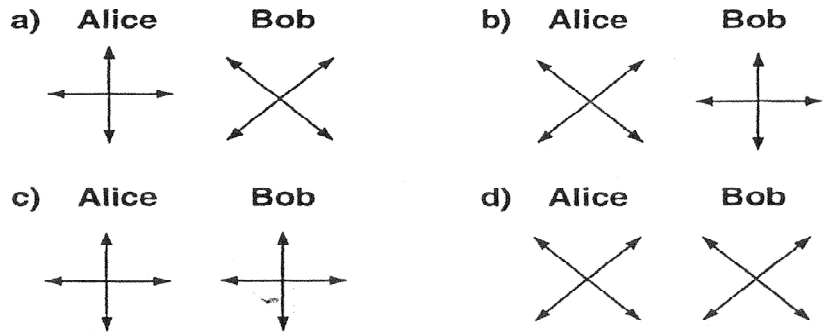


Figure 7: Alice and Bob divide their polarization data into four cases according to the bases used by them.

Los Alamos Quantum Encryption

Hughes et al,
New J. of Physics 4, 43 (2002)

Signals sent 10 km
through the air

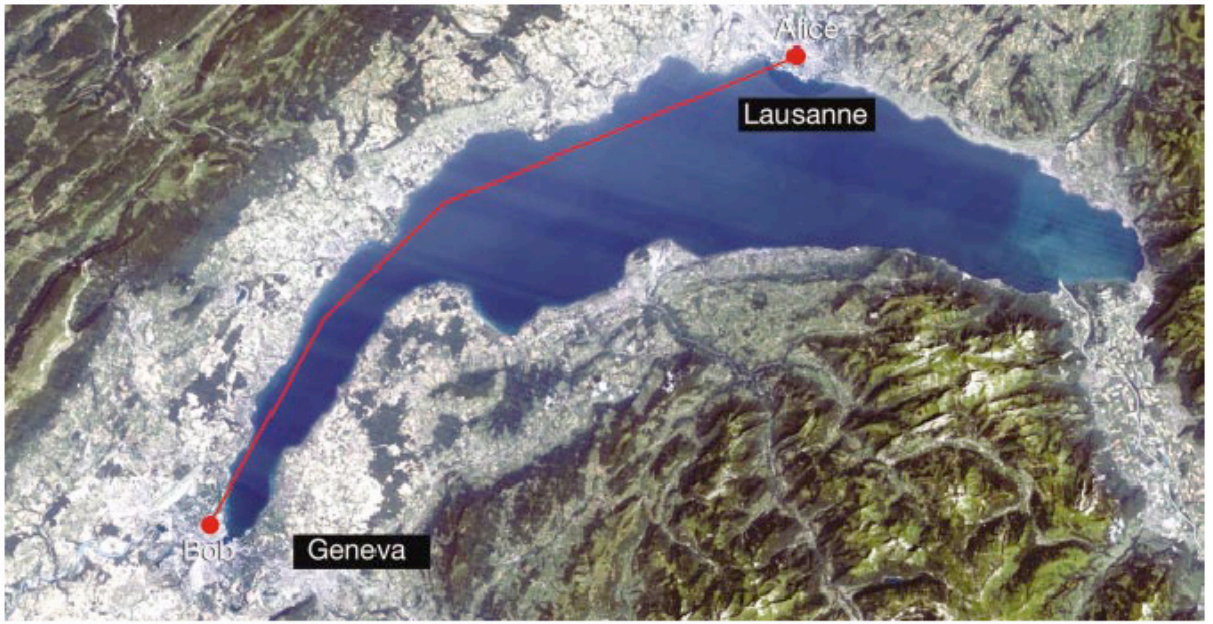
In the air: Richard Hughes has sent a photon-encrypted code from a laser source (circled, inset) to a receiver.

Univ. of Geneva Encryption

Stucki et al
New J. Phys
4, 41 (2002)

Signal sent 67 km though commercial optical cable

Light work: keys encoded using polarized photons have been sent between Alice and Bob (left) through 67 km of fibre-optic cable under Lake Geneva.



Quantum Computing

Quantum computers can do nothing that classical computers can't do. But they can do it with more efficient use of storage and the can do it faster.

It is the speed that has really caught attention. Most particularly, Shor's lemma which demonstrates that factoring large numbers, which is exponentially difficult on a classical computer, and is the basis of the public encryption system in wide use, can be easily accomplished on a quantum computer !

Quantum computing (continued)

We shall not go into the many details of quantum computing. Whole books exist on the subject.

I would like, however, to comment upon the two basic features:

1. Compact storage (due to the use of qubits)
2. Parallel computing (due to quantum interference)

One should note that Quantum Computers are far from being realized. (But much work is going on.)