(20) Quantum Key Distribution (≡ Quantum Encryption)

Many secure coding protocols use algorithms that require exchange of a key secretly between Alice and Bob

[eg. sending a credit card no. to an online shop
discussion always about paranoid twins Alice and Bob and an evil spy, Eve, who is trying to intercept their messages]
eavesdropper

For classical info, E can intercept info, read it and send on a copy quickly, thus evading detection. Security via coding protocols that require long calculations ($\sim 10^6$ yrs) to find the key.

[QC is a threat to this from the shear speed of such calculations → hours]

For quantum info,
E interception is a measurement
causing changes to the info via wavefnc collapse
allowing interception to be detected. (Gordon 1970s)

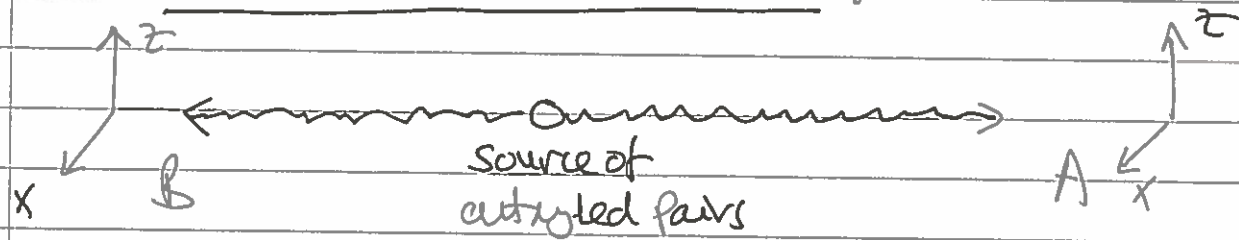
Here's one example of a QI protocol for exchanging a key, simplified E91 or Ekert protocol. (1991)
Read about BB84 in Rae or Miller. (1984)

Will be using: $\alpha_z = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$ $\beta_z = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$

$$\alpha_x = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 \\ 1 \end{pmatrix} \quad \beta_x = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 \\ -1 \end{pmatrix}$$

$$\begin{matrix} \alpha_z \\ \beta_z \end{matrix} = \frac{1}{\sqrt{2}}\left[\alpha_x \pm \beta_x\right] \quad \text{and} \quad \begin{matrix} \alpha_x \\ \beta_x \end{matrix} = \frac{1}{\sqrt{2}}\left[\alpha_z \pm \beta_z\right].$$

How do A and B determine their key?



A and B recieve one of a pair of entangled particles in a state, say, $\psi = \frac{1}{\sqrt{2}}\left[\alpha_z(1)\alpha_z(2) - \beta_z(1)\beta_z(2)\right]$

Each makes measurements using analysers S_z or S_x.

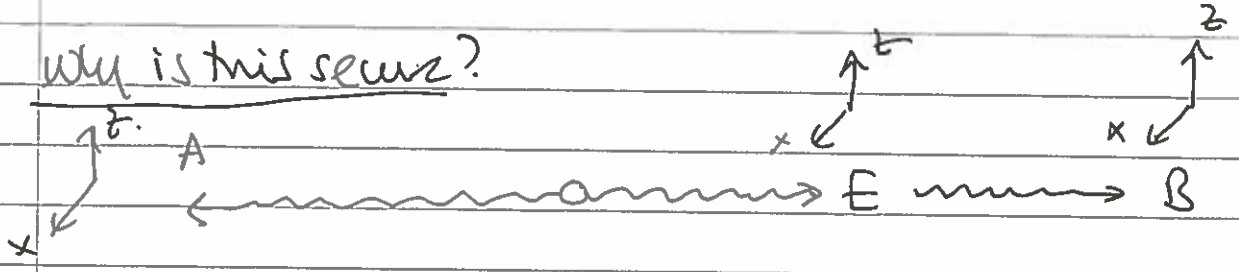
Agree to measure N events
Randomly switch between S_x and S_z
Along either axis $\alpha \equiv 1$, $\beta \equiv 0$ in biham.

If use same analyser, record same info.
eg. if A measures $+\hbar/2$, $\psi \to \alpha_z(1)\alpha_z(2)$
and B has to get $+\hbar/2$ as well.
both record a 1

If use different, don't have to have same info.
eg. if A measures with S_z and gets $+\hbar/2$
$\psi \to \alpha_z(1)\alpha_z(2) = \alpha_z(1)\frac{1}{\sqrt{2}}(\alpha_x(2) + \beta_x(2))$
if B measures with S_x
could get $\pm\hbar/2$ with 50% prob each. can't use these events. So....
(phone call)

A and B publically exchange knowledge of sequence of analysers (eg. $S_x, S_z, S_x S_x \ldots$) but not the measurements. Discard events where they used different axes.
Left with $\sim \frac{N}{2}$ events with same analysers, where QM tells them, unless nothing happened, they should have the same information $\Rightarrow$ use as their key.

why is this secure?



If E intercepts, particles going to B.
E needs to pass something onto B, otherwise noticed.
Best policy, send the info E measures.

But E doesn't know which analyser to use.
Best policy, switch randomly between S_x and S_y.

Consider just the $\frac{N}{2}$ ("key") events where A and B have same analyser.

Of these, by chance E uses same analyser } 50% of the
Steals info and sends correct copy to B } ie. $\frac{N}{4}$ events.

But 50% of time, the other $\frac{N}{4}$, E gets it wrong — So never easy to get the key!
eg. if A and B use S_z
E uses S_x.
E's measurement collapses the wavefunction to either
need to write all terms of eigenfunc of S_x since E measuring S_x.

$$\psi = \frac{1}{\sqrt{2}}\left[\alpha_z(1)\alpha_z(2) - \beta_z(1)\beta_z(2)\right]$$

$$= \frac{1}{\sqrt{2}}\left[\alpha_x(1)\beta_x(2) + \beta_x(1)\alpha_x(2)\right]$$ SHOW THIS.

so E measures $+\frac{\hbar}{2}$ or $-\frac{\hbar}{2}$ $\psi \to \alpha_x(1)\beta_x(2)$ or $\beta_x(1)\alpha_x(2)$

If the former, rewrite back in terms of z since A+B measure S_z.

$$\alpha_x(1)\beta_x(2) = \frac{1}{2}\left[\alpha_z(1) + \beta_z(1)\right]\left[\alpha_z(2) - \beta_z(2)\right]$$

$$= \frac{1}{2}\left(\underbrace{\alpha_z(1)\alpha_z(2) - \beta_z(1)\beta_z(2)}_{\text{A\&B agree}} + \underbrace{\beta_z(1)\alpha_z(2) - \alpha_z(1)\beta_z(2)}_{\text{A\&B disagree}}\right)$$

If collapses to $\beta_x(1)\alpha_x(2)$ same conclusion → SHOW THIS.

So E is not going to get the key – but disrupts info stream to B.

So if E is there, of the $\frac{N}{2}$ events where A&B should have the same info 25% of the time ie. $\frac{1}{4}N/8$ events the info will be different. ~~Compare to Schrödinger's cat.~~

A and B can find out by sharing publicly some of the N/2 events (ie. not whole key, just some bits) they should be the same; if not being intercepted ~~and~~ → search and destroy E.

Can use any type of entangled states: spin-1/2 pair (these 4 are Bell states for maximally entangled)

~~$\frac{1}{\sqrt{2}}[\alpha_z(1)\alpha_z(2) \pm \beta_z(1)\beta_z(2)]$~~

$\frac{1}{\sqrt{2}}[\alpha_z(1)\beta_z(2) \pm \alpha_z(2)\beta_z(1)]$

PRACTISE ARGUMENT WITH OTHERS!

in some cases the $\frac{N}{2}$ expect same info, others info is always inverted.

easier with photon polarisation.

Not sci-fi:

(2006) BB84 fibre optics over 150 km Los Alamos/NIST.

(2007) E91 across freespace 144 km between two Canary Islands (FMNS can be done via satellites)

four companies producing QKD systems.

2016 — 404 km using MDIQKD optical by fibre

2004 first bank transfer by QKD

21 Quantum teleportation and computing.

No-cloning theorem: in

It is impossible to transfer the quantum state of one reference system to another target system, without relying on prior knowledge of the ref state and without disturbing it in the process.
ie. $\psi(A)\psi(B) \not\Rightarrow \psi(A)\psi(B)$
~~without~~ CAN'T COPY STATES WITHOUT THOSE CAVEATS.

without relying on prior knowledge of the system

Same quantum mechan … with the … without alter the state of the init…

[Fairly easy proof ⇒ Rabl… clone large nos of copies that can… by the ensemble as a whole, could… by principle]

Quantum teleportation: … state of a reference system To … inevitably changing the state of reference system in the process.

[has been experimentally demonstrated for photons and atomic beams but a lay man STAR TREK as we can see]

For example, Alice has a reference state based on a spin-½ qbit: $\psi(3) = A\alpha(3) + B\beta(3)$
(implied z-axis: subscripts become untenable in a moment)
Wants to transfer A and B to ~~another Bobby~~ a tgt qbit (1) and send it to Bob.

(i) Make (1) part of an entangled pair with another qbit (2)
So system of three qbits:

$$\psi(1,2,3) = \frac{1}{\sqrt{2}}\left[A\alpha(3)+B\beta(3)\right]\left[\alpha(1)\beta(2)-\beta(1)\alpha(2)\right]$$

This is algebraically identical to:

$$\psi(1,2,3) = -\frac{1}{2}\left[A\alpha(1)+B\beta(1)\right]\psi_1(2,3) + \frac{1}{2}\left[A\alpha(1)-B\beta(1)\right]\psi_2(2,3)$$
$$-\frac{1}{2}\left[A\beta(1)+B\alpha(1)\right]\psi_3(2,3) - \frac{1}{2}\left[A\beta(1)-B\alpha(1)\right]\psi_4(2,3)$$

— Eqn (1)

where: $\psi_1(2,3) = 1/\sqrt{2}\,[\alpha(2)\beta(3) - \beta(2)\alpha(3)]$
$\psi_2(2,3) = 1/\sqrt{2}\,[\alpha(2)\beta(3) + \beta(2)\alpha(3)]$
$\psi_3(2,3) = 1/\sqrt{2}\,[\alpha(2)\alpha(3) - \beta(2)\beta(3)]$
$\psi_4(2,3) = 1/\sqrt{2}\,[\alpha(2)\alpha(3) + \beta(2)\beta(3)]$

} so-called Bell's states maximally entangled spin-½ states.

so rewritten in terms of entangled states of 2+3 rather than 1+2.

(ii) Alice sends qbit(1) to Bob

(iii) Alice performs a "Bell state measurement" on (2) and (3). ie. represented by an operator whose eigenfunctions are the Bell states

And $\Psi(1,2,3)$ collapses into the appropriate term in eqn (1)

(iv) Alice phones Bob and tells him result of measurement.

If answer was $\psi_1(2,3)$ $\quad \Psi = [A\alpha(1) + B\beta(1)]\,\psi_1(2,3)$

(1) has same props as ref ✓

If answer was one of the others, then Bob uses a magnetic field to rotate the spins.

Eg. if $\psi_2(2,3)$

$$\psi(1) = A\alpha(1) - B\beta(1)$$

induce unitary evolution

Turn on magnetic field perp to quantisation axis

$e^{-i\omega t}$ $\quad e^{i\omega t}$

Problem sheet 6:

By on a state α_z evolves $\alpha_z \to \alpha_x \to \beta_z \to -\beta_x \to -\alpha_z$
$\omega t = 0 \quad \pi/4 \quad \pi/2$ etc.

on a state β_z evolves $\beta_z \to -\alpha_x \to -\alpha_z \to \beta_z$

So if $\omega t = \pi$

$\psi(1)$ evolves from $A\alpha_z(1) - B\beta_z(1)$

to $-(A\alpha_z(1) + B\beta_z(1))$

$\omega = \frac{g\mu_B B}{2\hbar} = \frac{eg}{4m} B$

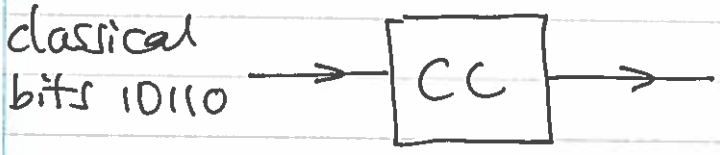
Now to make a measurement of which Bell state (2) and (3) are in? ie. a simultaneous measure on (1) and (2).

Clever ways with half-silvered mirrors and photons → RAE 12.3

VB // Phone call important: if transmit info by entanglement alone then in trouble with relativity → EPR paradox and hidden vars

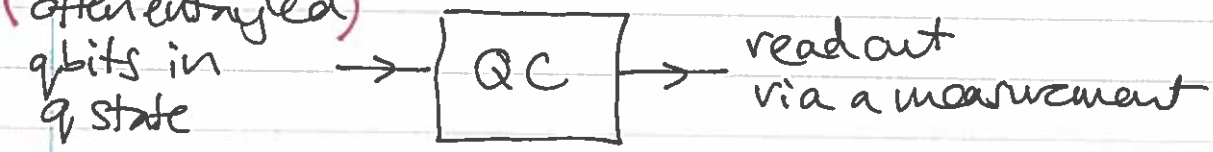
Quantum computing

Classical computer (CC):



↳ set of rules for operating on a bit; may depend on state of other bits.

Quantum computer (QC):



↳ evolution of q state by TDSE (unitary evol^{n}) under specific conditions

In principle, all CC ops can be done by QC
In practise, really hard so why bother?

Example of simple gate: NOT i.e. Input 0 → output 1
1 → 0

$0 \equiv \alpha_z$ $\quad$ Apply mag. field in y dir. state will evolve. Chose right time interval switch off $\quad$ $\beta_z \equiv 1$

$1 \equiv \beta_z$ $\quad$ $wt = \frac{\pi}{2}$ QNOT $\quad$ $-\alpha_z \equiv 0$ ↳ phase factor

If used an initial state: $A\alpha_z + B\beta_z \Rightarrow A\beta_z - B\alpha_z$

ie. can do the two basic operations in only one calculation with QC.

1 qbit has two coeff in superposition.

Two entangled qbits have four: $a_1\alpha(1)\alpha(2) + a_2\alpha(1)\beta(2) + a_3\beta(1)\alpha(2) + a_4\beta(1)\beta(2)$

N entangled qbits have: 2^N

eg. N=300 stores 2^{300} ie. a # bigger than # atoms in Universe !!

So for computing problems that scale rapidly with size, QC has an advantage over CC: superposition of 2^N calculations generated in a single operation.

But in QC, the readout involves measurement. In simple 1 qbit NOT operation, if measure can only get out one of the answers from the 2 ops.

So QC often has no advantage, except where aim is a small # of pieces of info that would require a long and complex CC.

eg. a database search
or factorising into prime #s

} both proved to be better on QC [even if not built].

↓ see example in Rae 12.4
see article on link on web page.

Many ways of trying:
B field precessing of spin-1/2
manipulation of photon polarisation
μwave flipping of molecular spins.

Major issues, esp isolation of qbit from environment
eg. stray fields that rotate spins.
— some systems more immune
— or perform quantum error correction.
entangled states of 2 qbits — routine.
— a few — difficult
many — seems impossible?
└ but who knows. (WATCH THIS SPACE)

Current example as of 2014, first expt test of advantage of QC in optical system using 6 qbits.
in Simon's problem:
for a function $f(x)$ is it one-to-one (one input has a unique output)
or do inputs share the same output eg. $f(x_1) = f(x_2)$
PRL 113, 200501 (2014).