QM I Lecture # 27 Phys 651

Intro to Quantum Information

classically:
"bits" - 0 or 1
"off" "on"
Voltage "low" "high"

$\boxed{\text{Quantum cryptography} \\ \text{Quantum computing} \\ \text{Quantum teleportation}}$

QM:
QM superpositions;
entanglement;
wave function collapse
⇓
quantum information

Quantum cryptography

Use "randomness" for
secure distribution of information

Conventional cryptography:
- if we do not have the key ⇒ can't decode the message (takes too long to do calculations)
- other people may find a way to do them faster

Quantum cryptography:
- relies on fundamental properties of QM ⇒ exchange of info with security & no amount of calculation can crack the code

Important: no-cloning theorem

Quantum cryptography is secure because no one can guarantee to make an exact replica of an arbitrary QM state of the system.

Examples of systems
- e^- with a particular spin state
- photon with a particular polarization

can one clone?

(~~make~~ another e^- or photon in exactly the same state without changing the state of the original e^- or photon)

Let's say our initial state is $|\Psi_a\rangle_1 |\Psi_s\rangle_2$

two-particle

particle 1 is in the state Ψ_a

particle 2 is in some "starting" state

$$\left(\underbrace{|\Psi_a\rangle_1 |\Psi_s\rangle_2}_{\in \mathcal{E} = \mathcal{E}_1 \otimes \mathcal{E}_2} = \underset{\in \mathcal{E}_1}{|\Psi_a\rangle_1} \otimes \underset{\in \mathcal{E}_2}{|\Psi_s\rangle_2} \right)$$

Consider $|\Psi_a\rangle_1$ to be some sort of a basis state

For example:
- polariz. of a photon can be described as $c_1|H\rangle + c_2|V\rangle$, so $|H\rangle$ & $|V\rangle$ would be "basis" states
- for e^- : $|+\rangle, |-\rangle$ are basis states

Consider a unitary linear operator (3)

$$\hat{U} = e^{-\frac{i}{\hbar}\hat{H}(t-t_0)}$$

↑ e.g. time evolution

such that $\hat{U}|\psi_a\rangle_1|\psi_s\rangle_2 = |\psi_a\rangle_1|\psi_a\rangle_2$

leaves particle 1 in the original state but changes the "standby" state of particle 2 to the "clone" of that of particle 1

Let's say we are able to do it with another basis state as well:

$$\hat{U}|\psi_b\rangle_1|\psi_s\rangle_2 = |\psi_b\rangle_1|\psi_b\rangle_2$$

Now let's try to do the same if the state we are attempting to clone is a superposition:

$$|\psi\rangle_1 = \frac{1}{\sqrt{2}}(|\psi_a\rangle_1 + |\psi_b\rangle_1)$$

Then, the initial state for a 2-particle system is

$$\frac{1}{\sqrt{2}}(|\psi_a\rangle_1 + |\psi_b\rangle_1)|\psi_s\rangle_2 = \frac{1}{\sqrt{2}}(|\psi_a\rangle_1|\psi_s\rangle_2 + |\psi_b\rangle_1|\psi_s\rangle_2)$$

QM operators are <u>linear</u> so

$$\hat{U}\left(\frac{1}{\sqrt{2}}(|\psi_a\rangle_1|\psi_s\rangle_2 + |\psi_b\rangle_1|\psi_s\rangle_2)\right) =$$

$$= \frac{1}{\sqrt{2}}(|\psi_a\rangle_1|\psi_a\rangle_2 + |\psi_b\rangle_1|\psi_b\rangle_2)$$

but for cloning we wanted ⇒

$$\frac{1}{2}\left(|\psi_a\rangle_1 + |\psi_b\rangle_1\right)\left(|\psi_a\rangle_2 + |\psi_b\rangle_2\right)$$

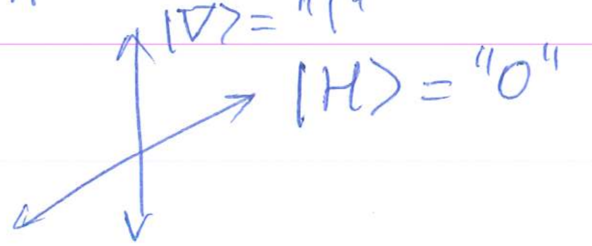
So even if we could clone basis states, we can't clone an arbitrary quantum state $\Rightarrow$ backup of quantum states is impossible!

A simple quantum encryption scheme

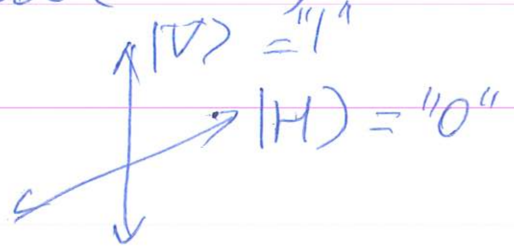
Bennett & Brassard 1984 $\Rightarrow$ use single photons

- demonstrated over 48 km optical fiber network
- — " — through atmosphere over 1,6 km (2000)

Alice (sender)



Bob (receiver)

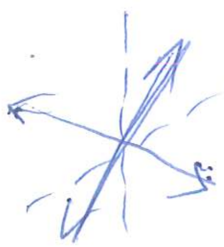


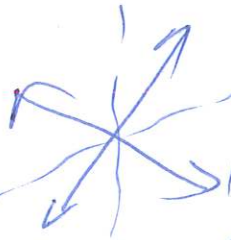
Alice sends a vertically polarized photon ("1")

Bob has a polarizer & separates polarizations onto two detectors $\Rightarrow$ when he gets a photon in a vertically polarized detector $\Rightarrow$ "1"

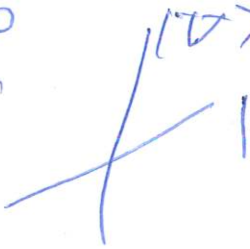
Problem: scheme is not secure

If Eve ("eavesdropper") inserts a detection system like Bob's, intercepts a photon, and re-sends the photon like Alice, no one will know!

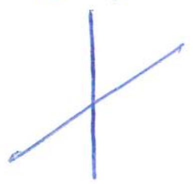




$|\pm 45\rangle = \frac{1}{\sqrt{2}}(|H\rangle \pm |V\rangle)$ $\Rightarrow$ Bob still gets info



If Eve still has her detectors
she will have 50% prob.
to detect "0" or "1" $\Rightarrow$
no info (and Bob will know to look for intercepts!)



and vice versa
$\Rightarrow$ no meaningful transmission

(Eve's error rate would be 50% and since she can't clone $\Rightarrow$ Bob would notice)

To secure the communication:
Alice & Bob each randomly choose between $|H\rangle - |V\rangle$ & $|45\rangle - |-45\rangle$ configuration to communicate a bit $\Rightarrow$
so 2 configurations $\Rightarrow$ meaningful
2 — " — $\Rightarrow$ not meaningful
and then call (public phone) to confirm which bits were meaningful.

Current research:

- develop quantum cryptographic techniques with security against sophisticated attacks
- monitor error rates & exclude consequences from partial interception of messages

Quantum computing

$\Downarrow$

Operate on a quantum state rather than classical

N two-level QM systems as inputs $\Rightarrow 2^N$ numbers

classical machine can't do it $\Rightarrow$ operation in parallel

For $N = 300$ binary inputs

$\Downarrow$

not enough atoms to store 2^{300} numbers at 1 atom/number

classical computer: $\xrightarrow[\text{bits}]{\text{input}}$ black box $\xrightarrow[\text{bits}]{\text{output}}$

"0" or "1"

"Clock" (trigger quantum operations)

$\Uparrow$

unitary evolution

quantum computer: $\xrightarrow{\text{qubits}}$ black box "oracle" $\Rightarrow$ readout (measurement process)

any QM system that can exist in a two-state superposition (e⁻ spin, photon polarization, atom in a superpos. of two states)

necessarily throw away some of the info about the final state

$\Uparrow$

loss is one of the major issues

$|\psi\rangle = c_0|0\rangle + c_1|1\rangle \doteq \begin{bmatrix} c_0 \\ c_1 \end{bmatrix}$

$|0\rangle, |1\rangle \Rightarrow |H\rangle, |V\rangle$

$|+\rangle, |-\rangle$

$|g\rangle, |e\rangle$

logical "0"

Basic operations: (to act on a qubit)

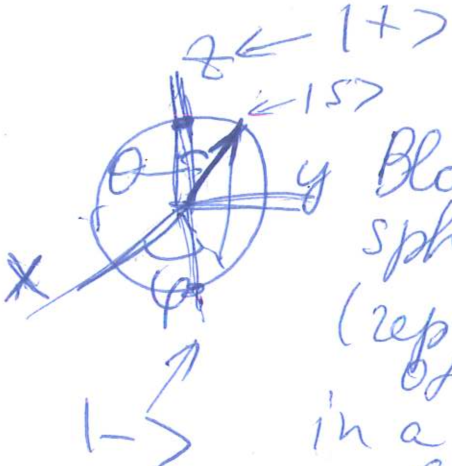
$U_H \doteq \frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$ — Hadamard operator

$U_Z \doteq \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$ — Z operator

⑦

$U_{NOT\,X} \doteq \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$

NOT X operator



Bloch sphere (representation of a state in a two-state basis)

$|S\rangle = \cos\frac{\theta}{2}\,|+\rangle + e^{i\varphi}\sin\frac{\theta}{2}\,|-\rangle$

θ, φ on Bloch sphere characterise the spin state & geometrical x, y, z directions $\Rightarrow$ direction of the eigenvectors of the corresponding spin operators

So $\Rightarrow$ U's perform rotations of the vector (qubit) on the Bloch sphere

In practice: B-fields for spin qubits
EM fields pulses for atomic states qubits
polarisation components for photon-based qubits

Another operation:
interaction between 2 qubits $\Rightarrow$ Controlled-NOT (C-NOT)

2-qubit state is a vector in a 4D Hilbert space

$|\Psi\rangle = C_{00}|0\rangle_{control}|0\rangle_{target} + C_{01}|0\rangle_{control}|1\rangle_{target} + C_{10}|1\rangle_{control}|0\rangle_{target} + C_{11}|1\rangle_{control}|1\rangle_{target} \doteq \begin{bmatrix} C_{00} \\ C_{01} \\ C_{10} \\ C_{11} \end{bmatrix}$

Quantum teleportation

Transfer a quantum state from one place to another w/o actually transferring the specific carrier of the state

↑ note: can't clone

⇓ "share entanglement"

Entangled states: e.g. two photons (EPR pair)

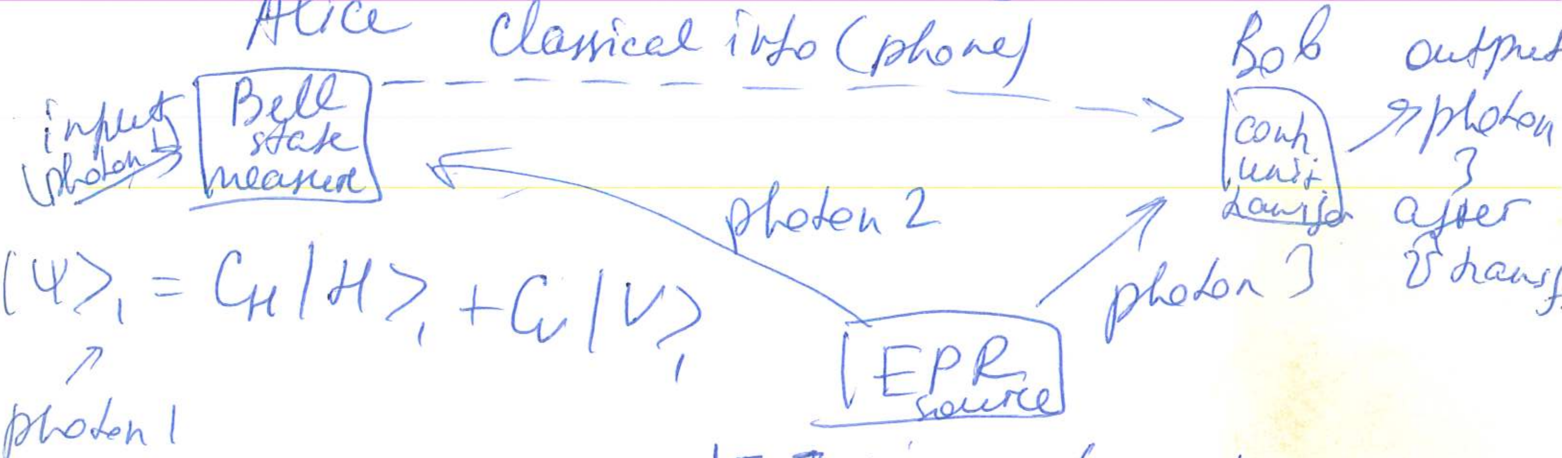
$$|\Phi^\pm\rangle_{12} = \frac{1}{\sqrt{2}}\left(|H\rangle_1|H\rangle_2 \pm |V\rangle_1|V\rangle_2\right)$$

$$|\Psi^\pm\rangle_{12} = \frac{1}{\sqrt{2}}\left(|H\rangle_1|V\rangle_2 \pm |V\rangle_1|H\rangle_2\right)$$

Bell states

Expt. realization: spont. optical parametric down-conversion ⇒ generate EPR pairs

$$\omega = \omega_1 + \omega_2$$
$$\vec{k} = \vec{k}_1 + \vec{k}_2$$



$$|\psi\rangle_1 = c_H|H\rangle_1 + c_V|V\rangle_1$$

↑ photon 1

$$|\Psi^-\rangle_{23} = \frac{1}{\sqrt{2}}\left(|H\rangle_2|V\rangle_3 - |V\rangle_2|H\rangle_3\right)$$

↑ entangled photons 2, 3

core trick

$$|\Psi\rangle_{123} = |\psi\rangle_1|\Psi^-\rangle_{23} = \frac{1}{2}\Big[|\Phi^+\rangle_{12}\left(c_H|V\rangle_3 - c_V|H\rangle_3\right) +$$

↑ show

$$+ |\Phi^-\rangle_{12}\left(c_H|V\rangle_3 + c_V|H\rangle_3\right) + |\Psi^+\rangle_{12}\left(-c_H|H\rangle_3 + c_V|V\rangle_3\right) -$$

$- |\Psi^{+}\rangle_{12} \left(C_H |H\rangle_3 + C_V |V\rangle_3\right)\Big]$ (10)

So $|\Psi\rangle_{123}$ is presented as a superposition of Bell states for photons 1 & 2

Now Alice makes a measurement of the Bell state and, say, gets $|\Phi^-\rangle_{12} \Rightarrow$ then

$$|\Psi\rangle_{123} = \frac{1}{2} |\Phi^-\rangle_{12} \left(C_H |V\rangle_3 + C_V |H\rangle_3\right)$$

after the measurement

Alice tells Bob over the phone the result ($|\Phi^-\rangle_{12}$) and so Bob knows that photon 3 is in the state $C_H|V\rangle_3 + C_V|H\rangle_3$.

Not the same as original $C_H|H\rangle_1 + C_V|V\rangle_1$ but easily fixed by polarization components ($|V\rangle \to |H\rangle$, $|H\rangle \to |-V\rangle$)

Then photon 3 is in the same state as photon 1 without Alice or Bob ever knowing what the state was (i.e. C_H & C_V)

(For other Alice's measurement results $\Rightarrow$ choose different polarization components) $\Leftarrow$ equivalent of a unitary transformation

Note: measurements of photons 1 & 2 by Alice affect the state of photon 3 $\Rightarrow$ EPR paradox