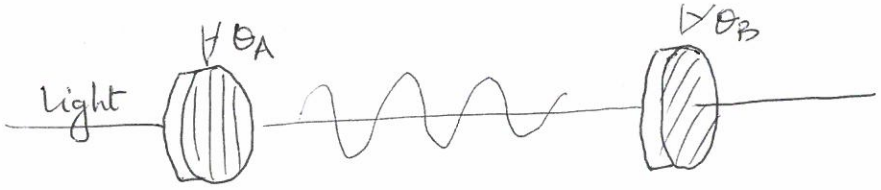
Guest Lecture: Quantum Cryptography

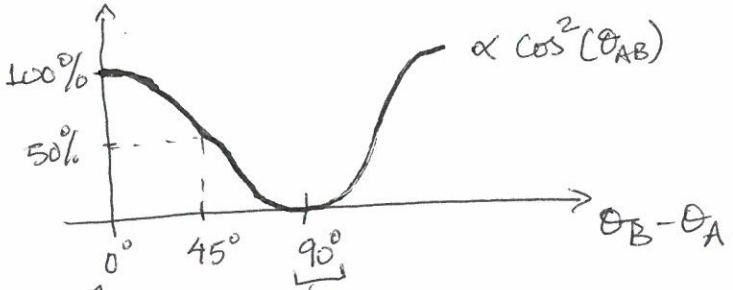
- Polarization of photon
- Qubits & quantum measurement
- QKD → BB84 Protocol

Polarization of light ← no Quantum mechanics



Class demo with a bunch of polarizers

Fraction getting through



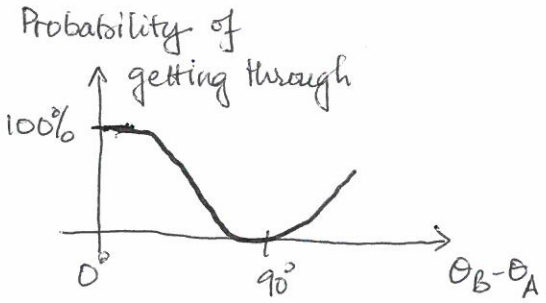
polarizers aligned ⇒ all light goes through

polarized orthogonal ⇒ no light goes through

Polarization of a photon

A photon = smallest unit of light

polariza



- polarizers aligned ⇒ photon goes through
- polarizers orthogonal ⇒ photon does not go through
- polarizers at 45° difference?
  half the photon goes through??

NOPE! because there is no such thing as half a photon

You can only have 0, 1, 2, ... photons

* sometimes (50% probability) the photon goes through
  & some other times (50%), it doesn't go through

- Is it random?
- Is it something a photon knows but we don't know?

Most physicists: Absolutely random, last minute decision by the photon

We will use this for key distribution!

Note: Polarization ~~can only~~ states ↕ vertical & horizontal ↔ are an orthogonal pair

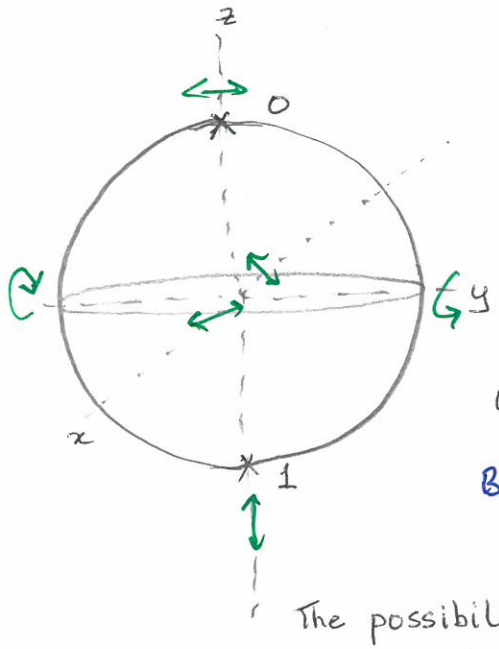
Use them as logic 1 and logic 0

But these are special quantum states

"Classical" bit

X 1

only 2 possibilities



Qubit lives on a Bloch Sphere

The possibilities are endless

Polarization

single photon qubit state

z-axis	+ basis	↔	horizontal	$\|0\rangle$
		↕	vertical	$\|1\rangle$
x-axis	X basis	⤢	diagonal up	$\frac{1}{\sqrt{2}}(\|0\rangle + \|1\rangle)$
		⤡	diagonal down	$\frac{1}{\sqrt{2}}(\|0\rangle - \|1\rangle)$
y-axis	ignore for now	↻	left circular	$\frac{1}{\sqrt{2}}(\|0\rangle + i\|1\rangle)$
		↺	right circular	$\frac{1}{\sqrt{2}}(\|0\rangle - i\|1\rangle)$

note that each one of these basis is an orthogonal pair spanning this vector space

Measuring qubit → only 0 or 1, just like a bit

collapse at north or south pole.

Just like making it go through a polarizer pair

Measuring qubit (contd...)

→ For a photon at the equator (recall 45° between polarizers), the photon randomly collapses to $\updownarrow$ or $\leftrightarrow$
1 0

(*) In this lecture, we will

- NOT do quantum computing i.e. using these qubits for information processing
- NOT use quantum signals to convey secret information,

Just use quantum signal to generate a secret crypto key. shared between 2 parties

Quantum Key Distribution

In general, ~~this~~ secret ⁊ crypto key:

- one-time pad
- generate via public-key cryptosystem like Diffie-Hellman or RSA

→ such public-key cryptosystem can ultimately be cracked by a quantum computer (eventually ∇.)

QKD systems are not vulnerable to attack by a q.c. because it's secured by the laws of nature and not computational complexity ∇.

Challenge: not transmission rate, but distance (photons do get absorbed!)

Recent experiments (2017) by Canadians & Chinese showed that this is no longer an issue.

Bennett - Brassard Protocol (BB84)

* Relies on the fact that quantum measurement is an invasive procedure, thus it will foil a potential ~~eves~~ eavesdropper.

* Lab implementations of BB84 always use photons
  - typically in fibers
  - In free space (2012)
  - Between satellites (2017)

check out Wiki for references

~~Imagine the ss~~

Alice + Bob want to generate a shared, random, secret key

Eavesdropper Eve wants to get info abt. this key without being detected.

→ Because Alice is sending quantum signals to Bob, Eve cannot measure these signals without causing disturbance.

⇒ Alice + Bob can detect her.

(but wait)

→ If Eve cannot measure signals w/out causing disturbance, then ~~so~~ Bob also cannot measure signals w/out changing them.

* So, protocol must be designed so that Bob gets the correct key in spite of the disturbance due to measurements.

BB84 solves this by letting Alice Bob know when Bob has made a measurement, so they can both discard that data.

Step 1: Alice generates 2 random binary strings

$A = (a_1, a_2, \cdots a_n)$ 0 & 1s

used to create secret key

$S = (s_1, s_2, \cdots s_n)$ $\{+ \text{ or } X\}$.

represents different basis for the state space of photons qubit

Step 2: Alice sends n photons to Bob.

Polarization of i-th photon is taken from basis s

$s_i = +$ then $(\updownarrow, \leftrightarrow)$

$|1\rangle \quad |0\rangle$

X then $(\nearrow, \searrow)$

$\left(\frac{|1\rangle + |0\rangle}{\sqrt{2}}, \frac{|1\rangle - |0\rangle}{\sqrt{2}}\right)$

Step 3: Before Bob receives photons, generates a random string.

$R = (r_1, r_2, \cdots r_n)$

from $\{+, X\}$

when he gets i-th photon, he measures it in r_i basis.

records 0 or 1s.

in $B = (b_1, b_2, \cdots b_n)$

$s_i \neq r_i$ in general

→ If $s_i = r_i$ then $b_i = a_i$ ideally.

→ If $s_i \neq r_i$ then no correlation b/w a_i & b_i

Step 4: After all photons are measured,
Alice & Bob tell each other S & R

→ they make note of all index i where the 2 sequences disagree

* no exchange of A & B *

→ Alice & Bob remove those bits from their A & B strings.

A' & B' left ← shorter

$\sim \frac{n}{2}$ long since 50% chance of Alice & Bob using same basis

Step 5: Transmission errors & how to estimate?

Alice sends some of her bits from A'

Bob measures them & compares to B'

they discard these bits.

Now smaller strings A''
B''

(missing quantum details & can be done w/out giving everything away)

Step 6: # of errors => max info Eve could obtain about remaining bits.

Replace $A'' \longrightarrow A'''$ shorter

$B'' \longrightarrow B'''$ shorter

so eavesdropper has no information whatsoever.