Introduction to Qunatum Information Via the BB84 protocol

Nicholas Chancellor

Ph.D candidate University of Southern California

06/14/2012

What is Quantum Information?

Classical information:

- In principle measurements can be done without changing a system at all
- Ex. you looking at this slideshow doesn't change the content
- Measurements are said to "commute"

Quantum Information:

- Measuring a system necessarily changes it
- Ex. no light gets through 2 polarized sheets at 90^o to each other, but $\frac{1}{4}$ of the photons get though when another is inserted between them at 45^o
- Measurements do not "commute" in general
- One cannot know all information about a system (Heisenberg uncertainty)

Quantum Measurement Example: photon polarization

Photon can be prepared in any of 4 polarization states, $\downarrow\uparrow\leftarrow \text{or} \rightarrow$ can be measured in either the $\updownarrow$ or $\leftrightarrow$ direction, but not both[1] Consider a photon prepared in the ↑ state,, there are 3 potential options:

1. polarization is measured in the $\updownarrow$ direction, readout shows the photon in the ↑ state with 100% probability
2. polarization is measured in the $\leftrightarrow$ direction, readout randomly shows the photon in → or ← state with 50% probability the photon is now in this state
3. polarization is measured at some other angle, readout is $\nearrow$ with some probability 50% $< \mathrm{p} <$ 100% or $\swarrow$ with probability 1-p

[1] it can also be measured at some angle in between, but this doesn't really add anything new

Imagine the Following Situation (BB84 protocol)

Alice (A) prepares photons in random known (to her) states $\downarrow\uparrow\leftarrow \text{ or } \rightarrow$, She sends these photons to Bob (B), who randomly chooses to measure in the $\updownarrow$ or $\leftrightarrow$ direction, 2 possible cases:

1. Alice and Bob choose the same direction (i.e. Alice chooses $\uparrow$ and Bob measures in the $\updownarrow$ direction), in this case both know the direction of the polarization
2. Alice and Bob choose different directions (i.e. Alice chooses $\rightarrow$ and Bob measures in the $\updownarrow$ direction, in this case Bob gets polarization in a random direction $\downarrow \text{ or } \uparrow$) Bob thinks he knows the direction but is wrong

By comparing the direction that the photon was created and measured in, and throwing away every case where (2) occurs Bob and Alice can know the same random binary number if they call $\uparrow$ and $\rightarrow$ 1 and $\downarrow$ and $\leftarrow$ 0 (example on next slide)

Small Example (no Eavesdropper)

1. Alice randomly chooses and sends Bob photons with the polarizations ↓←↓↑→↓→ = 0001101
2. Bob decides randomly to measure in the directions ↔↔↕↔↔↕ and gets the following result →←↓→→←↓ = 1001100
3. Alice Publicly announces “I created the states in the ↕↔↕↕↔↕↔directions” and Bob announces “I measured in the ↔↔↕↔↔↕ directions”
4. Alice keeps $0\underline{00}1\underline{1}01 = 001$ and Bob keeps $1\underline{00}1\underline{1}00 = 001$ and they both know the same random number, and the public announcements give no clue to what this number is

No-Cloning Theorum

An unknown quantum state cannot be exactly copied:

- If copies could be made than one could measure the state of the system exactly by measuring many copies and taking averages over measurements
- Being able to do such measurements violates the Heisenberg uncertainty principle
- An eavesdropper who intercepts the photons must guess the state of the photon based on partial information, a new photon must be sent to avoid detection if it is wrong the eavesdropper can be caught
- Eve the eavesdropper can never be caught on a bit which is thrown away (50% chance)
- On a bit which is not thrown away Eve could happen to pick the same direction as Alice and Bob (50% chance)
- Even if Eve guesses the direction wrong Bob's measurement could randomly not show an error (50% chance)

What If there is an Eavesdropper (Eve)?

1. Alice randomly chooses and sends Bob photons with the polarizations $\downarrow\leftarrow\downarrow\uparrow\rightarrow\downarrow\rightarrow = 0001101$
2. Eve intercepts the photons and randomly chooses to measure in the $\updownarrow\updownarrow\leftrightarrow\updownarrow\leftrightarrow\leftrightarrow\leftrightarrow$ directions, gets the result $\downarrow\uparrow\leftarrow\uparrow\rightarrow\rightarrow\rightarrow$
3. Eve sends her states to Bob who again measures in the $\leftrightarrow\leftrightarrow\updownarrow\leftrightarrow\leftrightarrow\updownarrow$ directions this time getting $\rightarrow\rightarrow\downarrow\uparrow\leftarrow\rightarrow\uparrow = 1101111$
4. After publicly announcing directions Bob and Alice can compare (publicly) and see $1\underline{10}1\underline{1}11 = 101 \neq 001 = 0\underline{00}1\underline{1}01$, They are not the same, Bob and Alice know that there is an eavesdropper, hunt Eve down and have her tarred and feathered, the encryption key has been compromised and they must try again

BB84 Protocol: numbers

1. Bob and Alice end up with the same random string of binary numbers which can be used as a 1 time pad and is on average half the number of photons sent long
2. They can publicly compare (and throw away) part of this string to try and catch Eve spying on them
3. When Eve spies she has a probability of $\frac{1}{4}$ of being caught for each bit which is compared compared
4. If only 10 bits are compared the chance of Eve not being caught is $(\frac{3}{4})^{10} \approx \frac{1}{18}$, however if 50 bits are compared it is $(\frac{3}{4})^{50} \approx \frac{1}{1.8 \text{ million}}$, this probability keeps going down exponentially