QC3

Wednesday, February 5, 2025 4:18 PM

Qubits: One Qubit case

- Classical Bits enter 0 or 1
  Can be represented by anything that has two mutually exclusive states:
  switch < on / off
- Classical Computers — measurement of bit does not enter in the picture
- Qubit any quantum state with two ordered orthonormal basis vects
  say $|q_0\rangle$ $|q_1\rangle$
  $|q_0\rangle$ ← collapsed state of 0
  $|q_1\rangle$ ← collapsed state of 1
- Qubit $|V\rangle = \alpha_0|q_0\rangle + \alpha_1|q_1\rangle$
- after we measure, its state will jump to $|q_0\rangle$ α_0^2 - p.
  or $|q_1\rangle$ - with α_1^2 - prob.
- Measurement is an important part of dealing with Qubits

⇒ Alice, Bob, Eve

- Alice wants to send conf. message to Bob
- Eve wants to eavesdrop
- how should Alice encrypt her messages so that Bob can read them but Eve can't.
  (Cryptography)

- Alice is sending Bob stream of qubits

(1) She measures them using her orthonormal Basis $|q_0\rangle, |q_1\rangle$

(2) Bob measures the qubits that Alice

Sends using his orth. Basis
$(|e_0\rangle, |e_1\rangle)$

– Suppose Alice wants to send 0

(I) Measures at her basis
when gets 0 → collapse → $|e_0\rangle$
Sends $|e_0\rangle$ to Bob

(II) Bob gets it and measures with his basis

$|e_0\rangle = \beta_0^B |f_0\rangle + \beta_1^B |f_1\rangle$

Two outcomes 0 – with $\beta_0^{B\,2}$
1 – with $\beta_1^{B\,2}$

Why Bob is not choosing $|e_0\rangle$ $|e_1\rangle$
since then he will get equally 0

– But then Eve can eavesdrop without A and B knowing about it

⇒ To be specific let's choose

A $\left(\begin{bmatrix}1\\0\end{bmatrix}, \begin{bmatrix}0\\1\end{bmatrix}\right)$ $B = \left(\begin{bmatrix}\frac{1}{\sqrt{2}}\\ \frac{1}{\sqrt{2}}\end{bmatrix}, \begin{bmatrix}\frac{1}{\sqrt{2}}\\ \frac{1}{\sqrt{2}}\end{bmatrix}\right)$
0 1 0 1

Remember:

$$D(-\theta, n_z) = \begin{pmatrix} \cos\frac{\theta}{2} & \sin\frac{\theta}{2} \\ -\sin\frac{\theta}{2} & \cos\frac{\theta}{2} \end{pmatrix}$$

$$|\nearrow_\theta\rangle = \begin{pmatrix} \cos\theta/2 \\ -\sin\theta/2 \end{pmatrix} \quad |\swarrow_\theta\rangle = \begin{pmatrix} \sin\frac{\theta}{2} \\ \cos\frac{\theta}{2} \end{pmatrix}$$

A B E BB84 Protocol

How to send a secure message in Classical Encription

– Long string of binary digits
– Both should have same key
– if 3rd party knows the key – he can decode too without A and B

knocking about it.

— Charles Bennett Gilles Brassard
1984

— Two sets of O. Bases $\left(\begin{bmatrix}1\\0\end{bmatrix}, \begin{bmatrix}0\\1\end{bmatrix}\right)$ - standard
V-basis

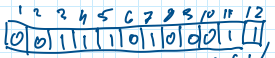
and $\left(\begin{bmatrix}\frac{1}{\sqrt{2}}\\ \frac{1}{\sqrt{2}}\end{bmatrix}, \begin{bmatrix}\frac{1}{\sqrt{2}}\\ -\frac{1}{\sqrt{2}}\end{bmatrix}\right)$
H-basis

1. A chooses the key that she wants to send Bob

— String of classical bits
00110001...

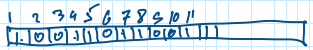
— for each bit she chooses V or H randomly

— says for 0 measured at V she will send $\begin{bmatrix}1\\0\end{bmatrix}$, measured verify if she sends $\left\{\begin{bmatrix}\frac{1}{\sqrt{2}}\\ -\frac{1}{\sqrt{2}}\end{bmatrix}\right.$



recording V H H V V H V V H H V V

— Bob chooses his V and H bases randomly



Recording H H V H V V H V

— A and B choosing there bases randomly
$\frac{1}{2}$ time they will choose same basis
$\frac{1}{2}$ time different basis

— If they are using same basis their reading should be the same (unless Eve did not eavesdropped)

— compare their HHVs (over unencripted line) 2n coincidae of Basis choice

→ they keep the bits corresponding to the times they chose same basis 2n times

— If Eve is not evesdroping they will end up with the same binary digits (2n length)

— If Eve evesdrops/intercepts she needs to measure it and then send her measurement forward to Bob (clone it)

so she will choose again one of the basis V or H

- $\frac{1}{2}$ times she will get same basis of Alice will measure and send to Bob Bob will not know about interceptor

A	E	B
V	V	V
1	1	1

A	E	B
V	H	V
1	50%	1 50%
	0 50%	0 50%

- When Alice and Bob agree in their Basis that will be half the time 50%
  - Eve will agree half of the time of Alices and Bob's agreed basis

A: H V V H V H | B: H V V H V H
1 1 0 1 0 1 | 1 1 0 1 0 1

No Eve

With Eve

A: H V V H V H | E: H V V H V H
1 1 0 1 0 1 → 0 1 1
V A V H H H

- A and B combaring their 2n strings that have same basis
  - if Eve did not intercepted their digits should be the same
  - if Eve intercepted the 50% time they will be different

- A and B compare half of $2n - n$ by open line
  - if they agree → no eavesdroping and can use other n as a key
  - if they disagree → eavesdroped should stop communicating