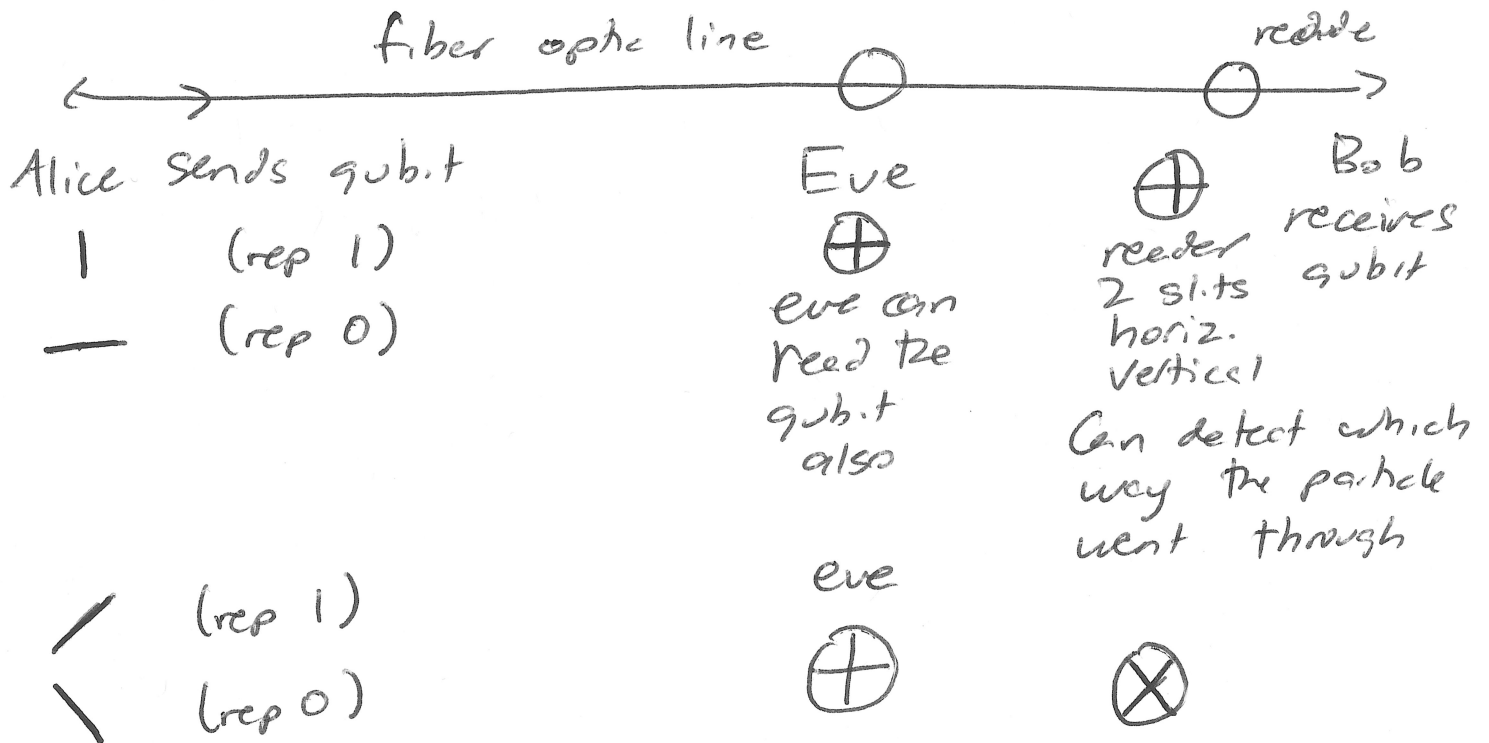


CIS 3362 - 11/6/23

Quantum Crypto - based on Code Book Chapter 8.

qubit (quantum bit)

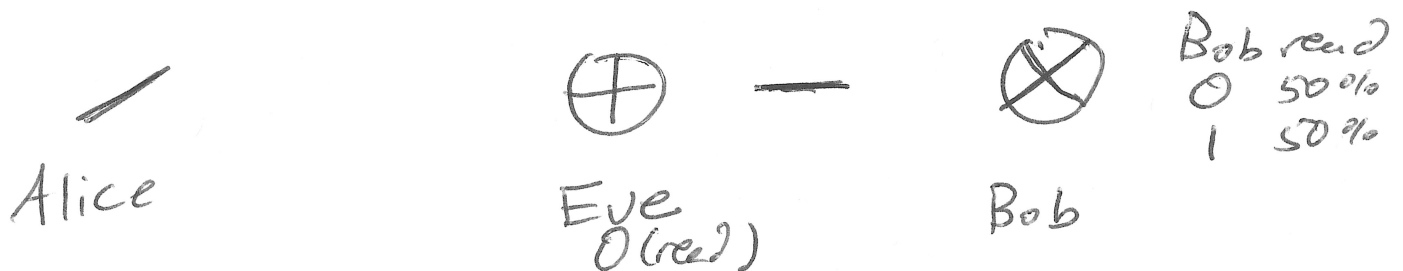


If eve KNOWS which reader Bob is using she can accurately read the bits

What happen if Eve uses the wrong reader?

- ① 50% time she reads the correct ans
50% = she reads wrong ans

- ② Particle CHANGES orientation to one of the slit openings in Eve's reader

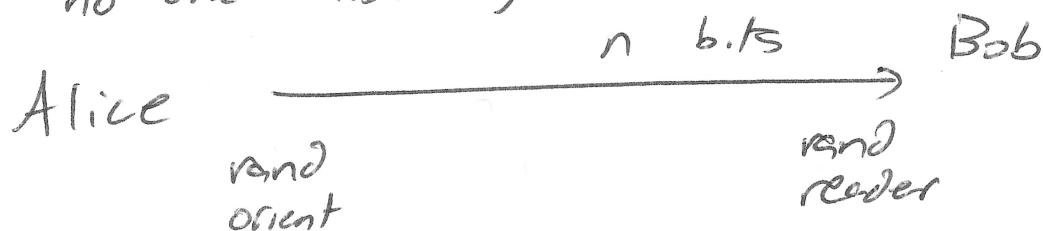


Unlike regular internet where lots of people can observe w/o clear detection, over this line, an eavesdropper can accidentally change a qubit and be detected.

Idea

Alice sends n qubits randomly choosing a reader for each one.

Bob will guess for each bit + choose a reader
If no one listening



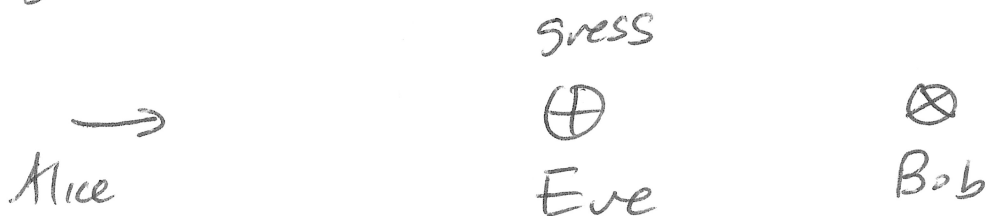
50% time Bob guesses correct reader.

But doesn't know WHEN he guessed correct.
Afterwards Alice could tell Bob which orientation she used on each one.

If no one was listening, Alice + Bob could use the bits that Bob used the correct reader on for a secret key.

How do we know if no one was listening?

Sample k bits ($k \ll n$), decide not to use these
Alice tells Bob on insecure line both orientation AND bit she sent.



Of k bits sampled, Bob probably used the correct reader on $\frac{k}{2}$ of them.

If Eve was there, she used a correct reader on $\frac{1}{2}$ of these ($\frac{k}{4}$) and an incorrect reader on the other $\frac{1}{2}$ ($\frac{k}{4}$).

Out of $\frac{k}{4}$ bits where Eve was wrong, Bob right, $\frac{1}{2}$ will be read incorrectly by Bob + detected.

on avg $\frac{k}{8}$ bits will be incorrectly read

prob eve undetected is $\left(\frac{7}{8}\right)^k$.

$\frac{1}{2}$ bob wrong reader

$\frac{1}{4}$ eve + bob right reader

$\frac{1}{8}$ eve W, bob R but lucky match

$\frac{1}{8}$ eve W, bob R no match

512

$$100 + \frac{100}{2} + 512 = 1124$$

sample bob d
 wrong need

if I wanted 512 bits key I would probably send 1300 bits, sample 100.

if any mismatch $\rightarrow$ throw out whole transaction

if no mismatch $\rightarrow$ good proof no one was on the line, so bits were exchanged securely.