

CIS 3362 11/28/22

11/28 - Quantum Cryptography

11/30 - Hash Functions

12/2 - Final Exam Review

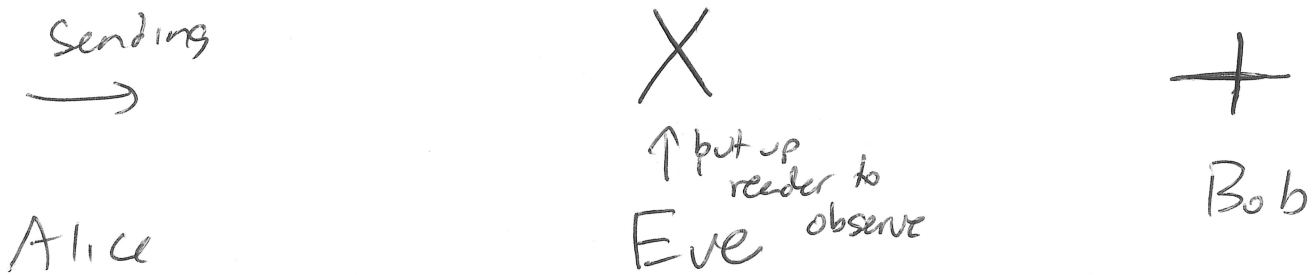
↳ Summarize last chpt in Code Book  
Demonstration - Crypt Tool

photons - to know their orientation, you need  
to use a "reader"

+ | = 1      - = 0  
                photon

X \ = 1      / = 0  
                photon

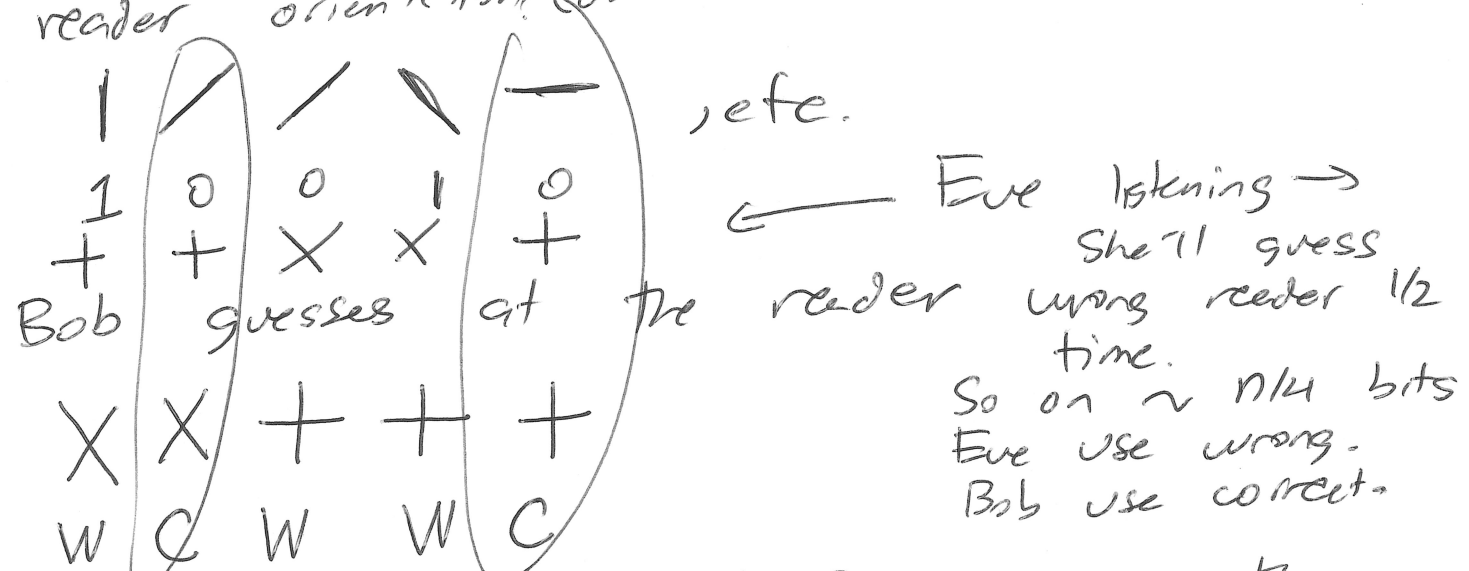
What happens when \ but read + ?  
50%  $\Rightarrow$  read 1, 50%  $\Rightarrow$  read 0.



It's near impossible for Eve to observe what's going on w/o being detected, because her presence affects the qubits.

Goal: for Alice + Bob to exchange a stream of bits for either a time pad or a private key scheme knowing that no one else has that stream of bits.

Alice sends Bob  $n$  bits, randomly choosing the reader orientation. (doesn't share w/Bob)



Afterwards, ~~we~~ ~~share~~ ~~the~~ Bob's guesses, throw out all wrong guesses. (left  $n/2$  bits ...)

Imagine Alice shares info about the bits w/Bob.  $n/4$  bits where Eve guessed wrong,  $1/2$  time Bob's answer he's read will disagree w/what Alice sent.  $\sim n/8$  bits Bob will get wrong.

$\left(\frac{7}{8}\right)^n$  where we use  $n$  bits is probability that Eve goes undetected.

We send more than  $n$  bits

Sample  $n$  bits this way randomly.

If no error is detected among all the bits where Alice + Bob used the same reader, then we assume Eve wasn't on the line!

$$\left(\frac{7}{8}\right)^{100} \sim 10^{-6}$$

If we chose  $n=400 \rightarrow \sim 10^{-24}$  (small!)

Example  $\rightarrow$  send 2000 bits  
sample 400  $\Rightarrow$  if all ok  
~~the~~ exchange into 1600 readers  
keep all bits w/ the correct reader.

In theory would be unbreakable.

Issues: extremely costly + time consuming  
probably issues w/ reliability over  
distances.