

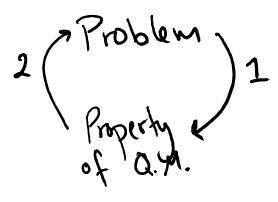
Quantum Cryptography

Goals:

- Build excitement
- Qualitative understanding of QM

Announce: Pickers
 Questionnaire
 Prequiz
 HW on go/cs333
 Signup

Structure

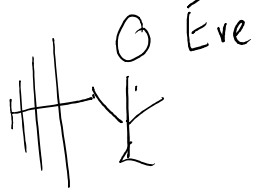


Cryptography

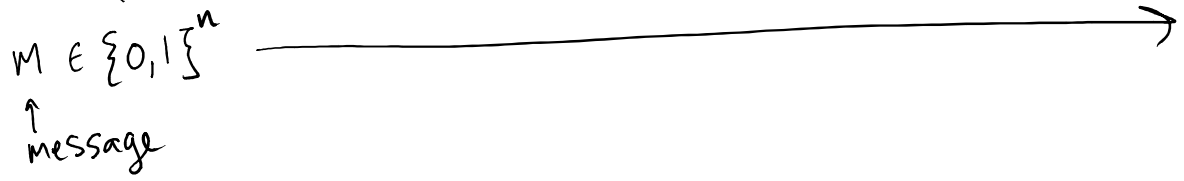
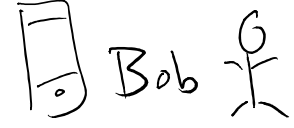
Message Sender



Eavesdropper



Message Receiver



(Notation: $\{0,1\}^n$ = the set of n-bit strings $\{0,1\}^1 = \{0,1\}$, $\{0,1\}^2 = \{00,01,10,11\}$)

Best Crypto Method: secret key $s \in \{0,1\}^n$

- s randomly chosen
- s known only to Alice & Bob

Secret Key Protocol

1. Using secret key $s \in \{0,1\}^n$ and message $m \in \{0,1\}^n$, Alice creates encrypted message \bar{m} , where $\bar{m}_i = m_i \oplus s_i$
2. Alice sends \bar{m} to Bob
3. Bob decrypts \bar{m} by setting $m_i = \bar{m}_i \oplus s_i$

XOR
 addition mod 2

\uparrow m_i bit of string

x	y	$x \oplus y$
0	0	0
0	1	1
1	0	1
1	1	0

(See HW for security)

Secret Key Problem:

- How to share between A & B in first place

Use quantum!

Quantum Bit (qubit)

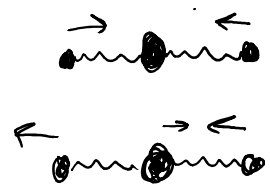
2-state system

2-state quantum system

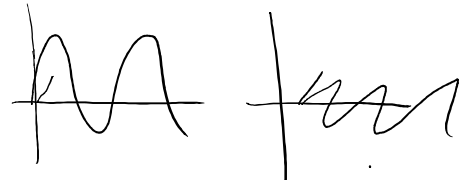
ex:



s, p electron orbitals



Vibrational modes of a molecule with 3 atoms



Single photon polarization vertically or horizontally

We'll use photon polarization for crypto

- Fast (speed of light)
- Easy to send (fiber optic cable)

Polarizer Demo

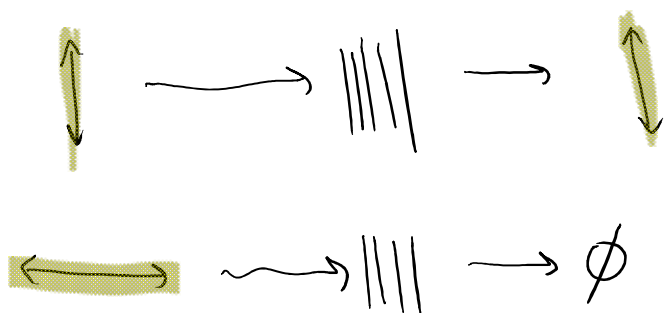
10^{20} photons/sec from a lightbulb

Q: If insert diagonal between vertical and horizontal polarizers, how much light will come through?

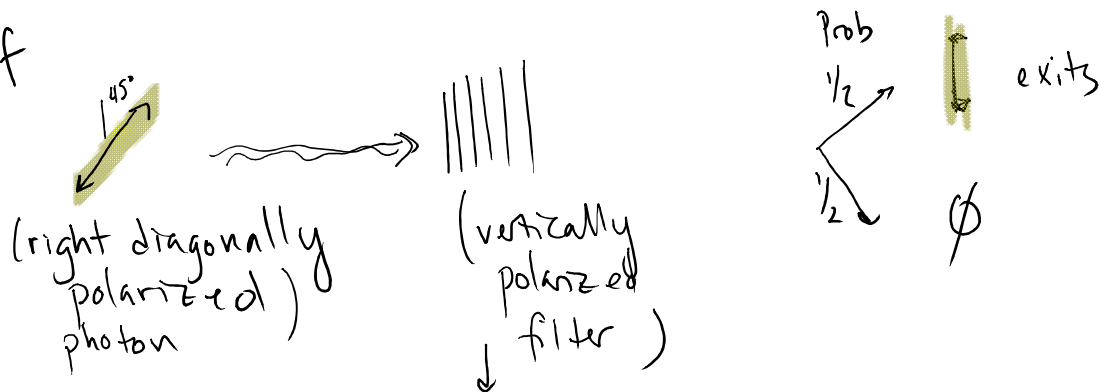
- A. None B. A little C. A lot



Single Photon :



What happens if prepare



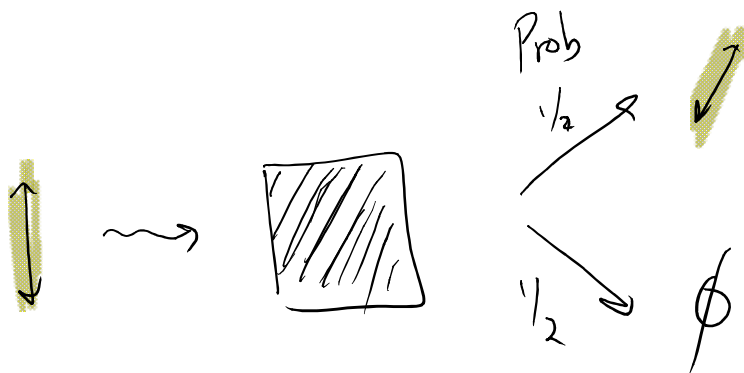
- A) A vertically polarized photon appears with $\frac{1}{2}$ energy
- B) A right diagonally polarized photon appears with $\frac{1}{2}$ energy
- C) A right diagonally polarized or left diagonally photon appears with equal probability
- \Rightarrow D) A vertically polarized photon appears w/prob $\frac{1}{2}$, and no photon exits w/ prob $\frac{1}{2}$

"Are you vertical or horizontal? You MUST choose"

We'll take advantage of this for crypto!

Same effect for any photon @ 45° to polarizer

Also:





Q: Given single photon picture, explain the lightbulb experiment.

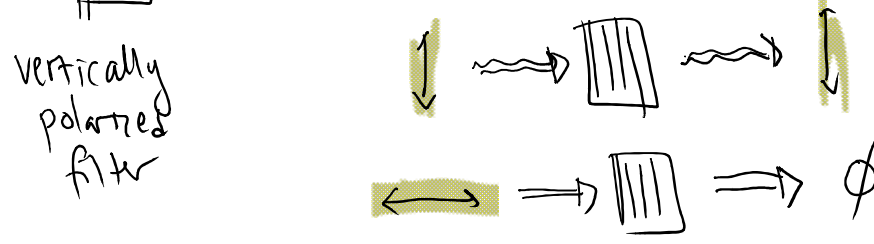
A: Half the vertically polarized photons make it through diagonal filter. Then half of those make it through the horizontal filter. So overall, $\frac{1}{4}$ of the photons that make it through the first filter exit. (But more than none!)

First idea

Alice sends \downarrow (vertically polarized) photon for 0
Alice sends \leftrightarrow (horizontally polarized) photon for 1



Bob puts  in front of detector

 light turns on if any photon hits



Light with polarization perpendicular to polarization filter won't pass.





Detector destroys photon

How can Eve eavesdrop? (Assume she can create $\downarrow, \leftrightarrow$, has  & )

Eve's strategy: do same thing as Bob. If detection, creates a new \downarrow photon, sends to Bob. If no detection, creates new \leftrightarrow photon, sends to Bob

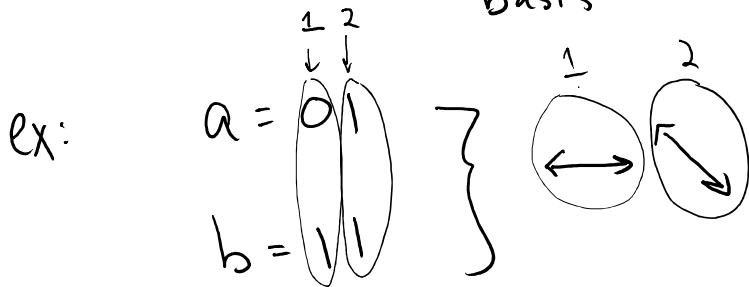
BB84

Label states with bits

Basis	State	Polarization
0	0	
0	1	
1	0	
1	1	

1) Alice chooses

$a, b \in \{0, 1\}^n$
 ↙ basis ↘ state



She will send these photons in this order to Bob.

2) Bob chooses $c \in \{0,1\}^n$

• If $c_i = 0 \implies$



D

• If $c_i = 1 \implies$



D

} to detect i^{th} photon

a, b, c secret & random

3. Alice sends each photon, Bob tries to detect. Bob creates $d \in \{0,1\}^n$

$d_i = 0$ if light on

$d_i = 1$ if light off

ex: $a=01, b=11, c=00$

$d=10$ or $d=11$

4. After Bob has made all measurements

Alice & Bob publicly announce a, c .

If $c_i = a_i$:

A) $b_i = d_i \oplus 1$ B) $b_i = d_i$ C) $b_i \oplus a_i = 1$

D) $b_i \cdot d_i = 1$ 