Learning Goals

- Predict outcome of (simple) quantum polarization measurements ✓
- Describe classical secret key protocol
- Understand key terms: encode/encrypt, decode/decrypt, secret key, encoded message
- Describe BB84 quantum crypto protocol and why it is secure

Announcements / Logistics

Announcement on Canvas

Rough Draft Submit → Hints (Otherwise on Wed)

Syllabus questions

Exit Tickets

Quantum Crypto really exists?

Working quantum computer now?

Secret Key Protocol

Warm-Up (Day 2)

$m = 1 \quad s = 1$

$\bar{m} = ?$

$\bar{m} \oplus s = ?$ $\quad m?$

Secret message $m \in \{0,1\}^n$

Eve knows everything about protocol, except m, s

1. A + B sharing a secret random key $s \in \{0,1\}^n$
2. A creates an encoded message $\bar{m} = s \oplus m$
3. A sends $\bar{m}$ (encrypted message) to B (Open channel, so Eve learns $\bar{m}$.)
4. B decrypts $\bar{m}$ by computing $\bar{m} \oplus s$ to gets m.

$\oplus$ = bit-wise addition mod 2. = XOR

<u>Problem</u>: How share secret key??

<u>Current Solution</u>: Public key cryptography

<u>Looming Problem</u>: Eve with quantum computer can break

When one door closes, another door opens

↓ Public key crypto

↓ Quantum Crypto Prot.

To do quantum crypto, need quantum particles :

photons ⇒ individual particles of light

 Fast

 Easily lost

 Hard to create + to detect

<u>Polarizer Demo:</u> If insert diagonal filter between horizontal and vertical polarizers, how much light will come through? (Bulb produces 10^{20} photons/sec each with random polarization.)

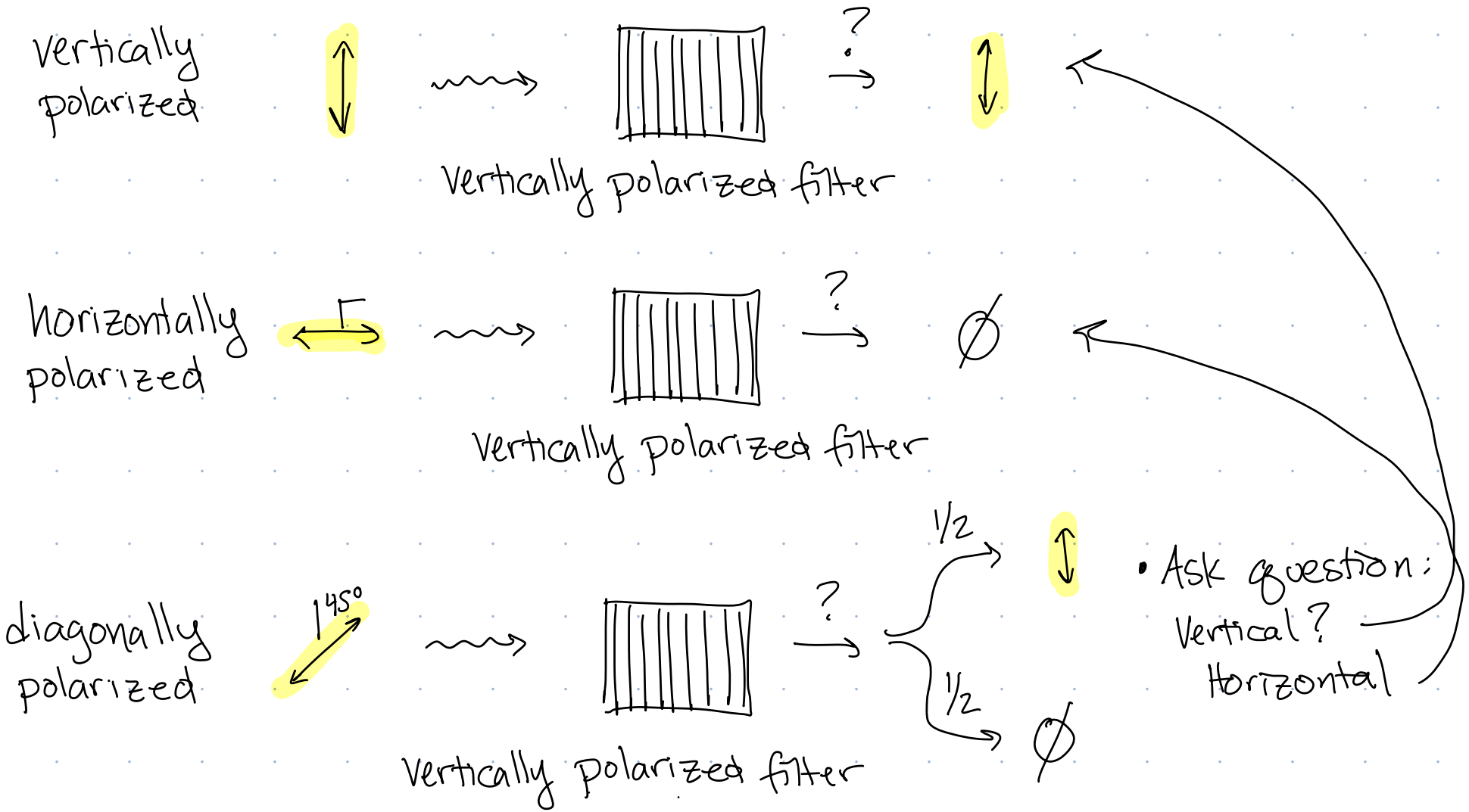
A. Same as no diag.

B. Less than single filter

C. Same as single filter

D. More than single filter

Photons + Polarizers

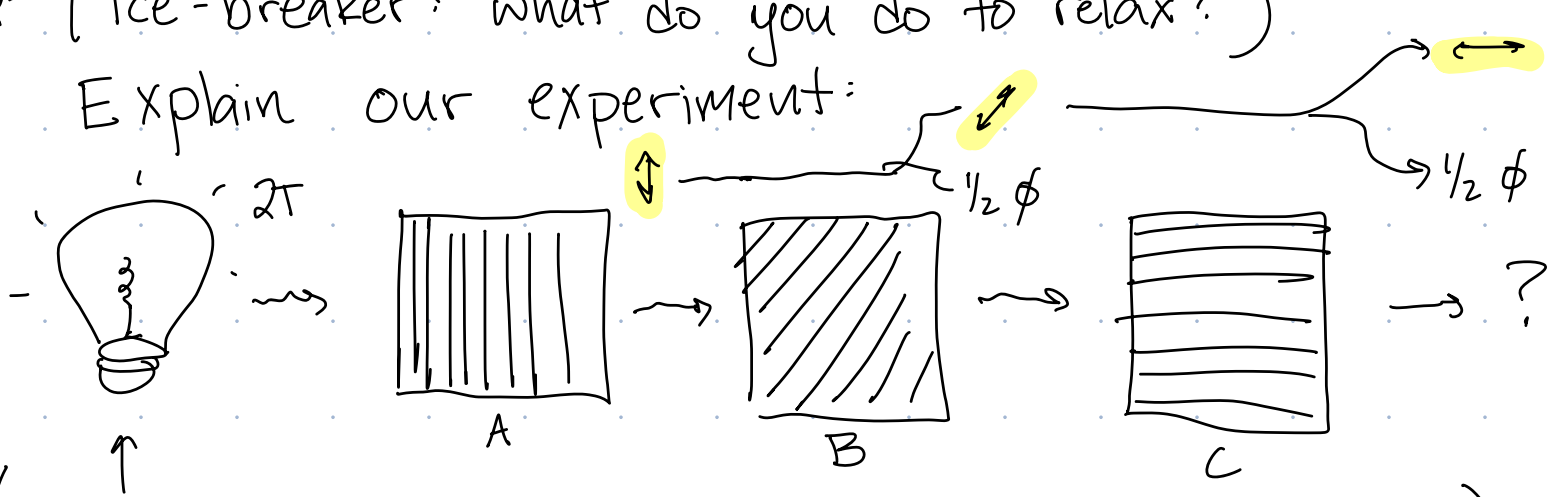


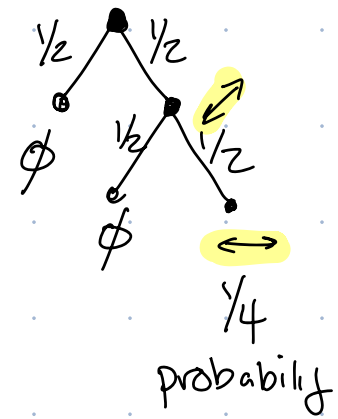
★ Behavior only depends on angle between photon polarization + polarizer

♡ Exiting photons have same polarization as filter

Q: (Ice-breaker: what do you do to relax?)

Explain our experiment:





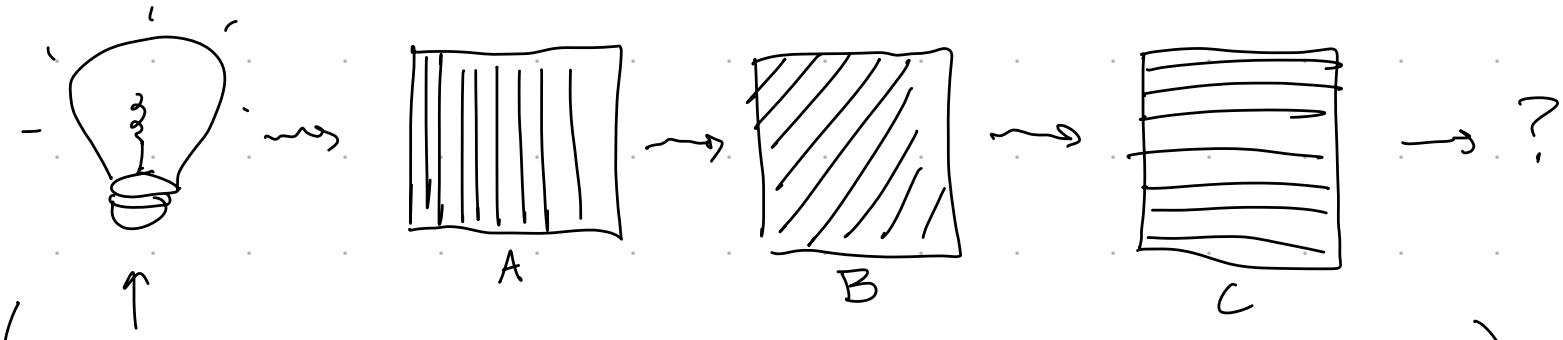
(lamp emits each photon with random polarization)

- What polarization(s) do exiting photons have?
- If T photons/sec hit polarizer B, how many photons/sec exit polarizer C? T/4 photons/sec exiting.

All photons exiting A, are vertically polarized. Since angle between photons + B is 45° ½ of time → blocked, ½ time → ~~emerge with~~ collapses to a diagonal polarization. Similarly ½ get blocked by C, ½ ~~emerge with~~ collapses to horizontal polarization.

Q: (Ice-breaker: what do you do to relax?)

Explain our experiment:



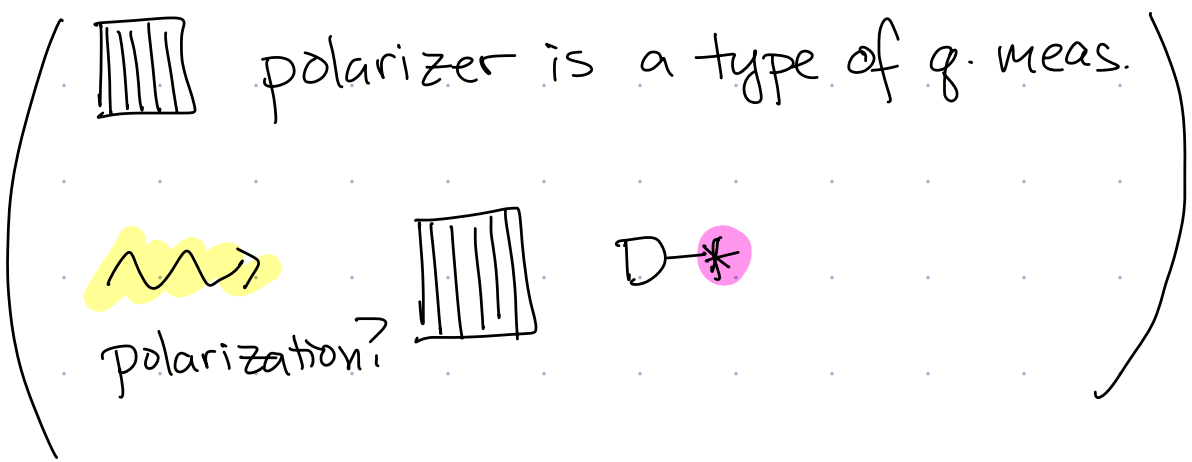
(lamp emits each photon with random polarization)

- What polarization(s) do exiting photons have? ↔
- If T photons hit polarizer B, how many photons/sec exit polarizer C (on average)? T/4 photons

Quantum Measurements

- Particle to be measured is changed by measurement

- Call this change "collapse"
- Measurement outcomes are possible results of a measurement



Quantum Crypto (BB84)

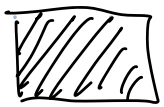
0. Alice + Bob pick $L \gg n$. (Eve knows L.)

	a (basis bit)	b (info bit)	photon	ket
vert/hor. basis	0	0	$\updownarrow$	$\lvert 0\rangle$
	0	1	$\leftrightarrow$	$\lvert 1\rangle$
diag. basis	1	0	$\nearrow\swarrow$	$\lvert +\rangle$
	1	1	$\nwarrow\searrow$	$\lvert -\rangle$

1. Alice chooses $a, b \in \{0,1\}^L$ randomly. ← Large number

At i^{th} second, sends photon a_i, b_i to Bob.

$\nearrow\swarrow \quad \updownarrow \quad \updownarrow \quad \leftrightarrow \quad \nwarrow\searrow \longrightarrow$ Bob

c (measurement basis bit)	Measurement	Ket
0		$\{\|0\rangle, \|1\rangle\}$
1		$\{\|+\rangle, \|-\rangle\}$

2. Bob chooses $c \in \{0,1\}^L$ randomly
   At i^{th} second, sets up measurement c_i

3. Records outcome $d_i = \begin{cases} 0 & \text{if detection} \\ 1 & \text{if no detection} \end{cases}$

$\boxed{\text{ex:}}$

	1st Photon	2nd Photon
$a = 0\ 1 \ldots$		
$b = 1\ 1$		
$c = 1\ 1$		
$d = 0/1\ 1$		

4. Alice + Bob publicly announce a, c strings

Q: If $a_i = c_i$ then

$\boxed{\text{A) } b_i = d_i}$ B) $b_i \neq d_i$ C) $b_i = d_i$ ½ the time

Q: If $a_i \neq c_i$ then

A) $b_i = d_i$ B) $b_i \neq d_i$ $\boxed{\text{C) } b_i = d_i \text{ ½ the time}}$

5. Alice and Bob throw out the bits of b, d corresponding to bits where $a \neq c$.