Learning Goals

- Predict outcome of (simple) quantum polarization measurements [QI1]
- Describe BB84 quantum crypto protocol and why it is secure [QI5]

Announcements

Exit Tickets

The Computer Science Department Presents

The 2026-27 LUNCHTIME SEMINAR SERIES

Join faculty and students to catch up over lunch and hear stories of what folks got up to this summer. All are welcome!

FREE PIZZA FOR ALL!

SESSIONS 1&2:

What I Did This Summer

9/18 & 9/25
12:20-1:20PM
75 SHANNON ST 102

Secret Key Cryptography

See PSet 1

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

Secret key
$s \in \{0,1\}^n$

Secret key
$\bar{m}$ s

m

Problem: How to share key?

Current Solution: Public key cryptography (Pset 1)

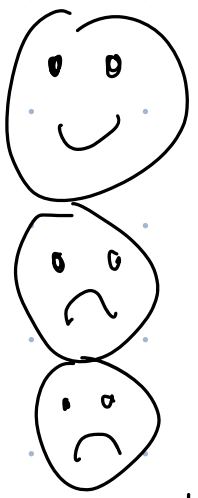
Looming Problem: Eve with large Q. computer can break

When one door closes, another door opens

Quantum Crypto

To do quantum crypto, need quantum particles:

photons ⇒ individual particles of light



Fast, infrastructure exists

Easily lost

Hard to create + detect (1 photon)

Polarizer Demo: 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.

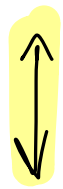
B. Less than single filter

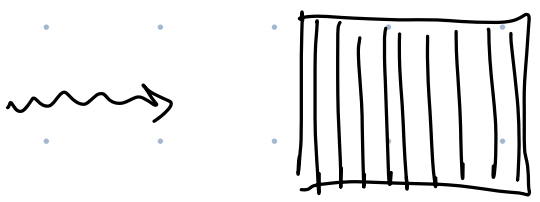
C. Same as single filter

D. More than single filter

Photons + Polarizers

vertical polarized

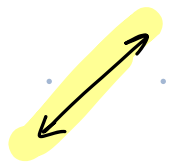


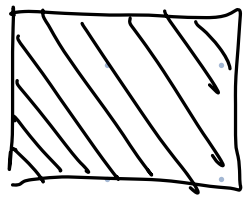


Filter with same polarization

?

diagonally polarized





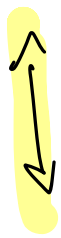
Filter with perpendicular polarization

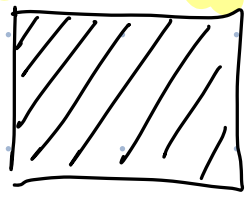
?

$\emptyset$

Filters are making a quantum measurement. causes "collapse" Forcing each photon to "choose" aligned or anti-aligned

horizontally polarized





Filter with 45° polarization

?

1/2

1/2

$\emptyset$

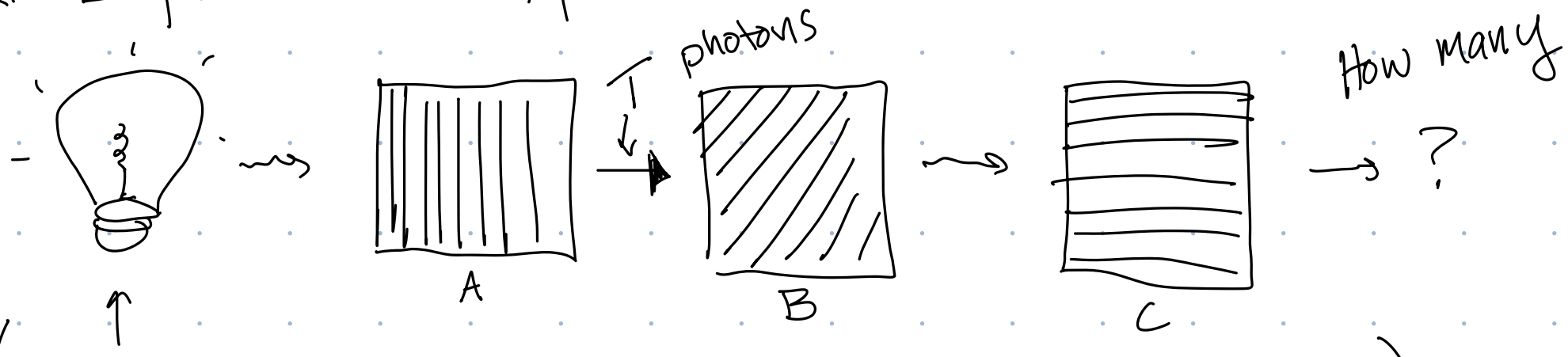
- ★ Behavior depends only on angle
- ♡ Outgoing polarization matches filter

Group Work: Helps you to learn by
- explaining thinking
- asking questions
- making mistakes

- In class only!
- No grade!
- I will provide solution!
- I won't always give you time to fully solve :(

Q: Name, pronouns (optional), what kind of group problem solver are you?

Q. Explain our experiment:



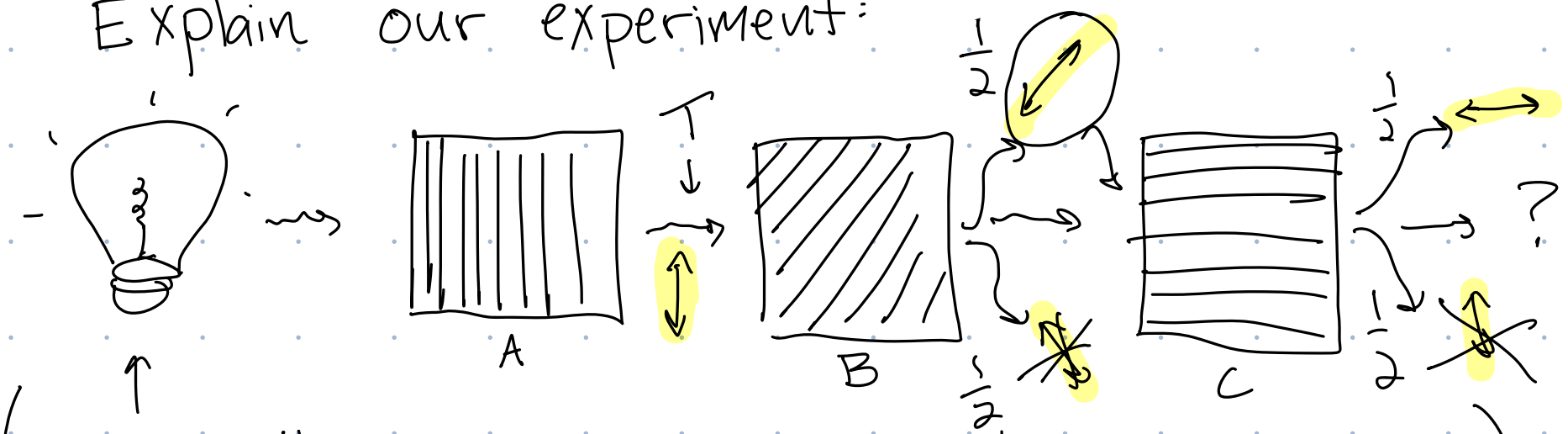
(lamp emits each photon with random polarization)

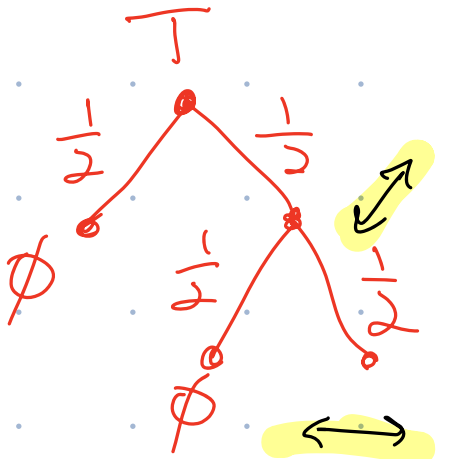
- What polarization(s) do exiting photons have?
- If T photons hit polarizer B, how many photons exit polarizer C?

(Learning target QI1 → Foundational)

Q:

Explain our experiment:

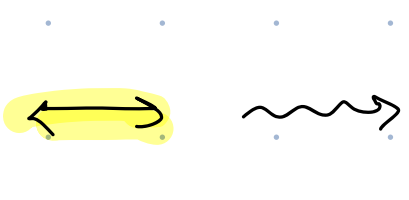


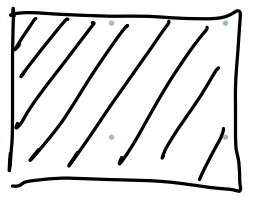


(lamp emits each photon with random polarization)

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

horizontally polarized



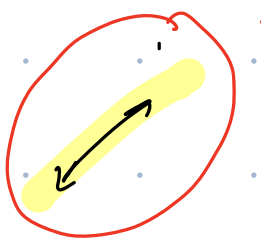


Filter with 45° polarization

?

50%

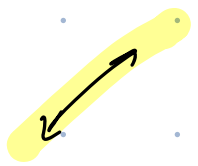
50%

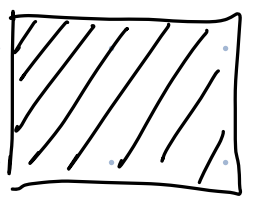


I

ϕ

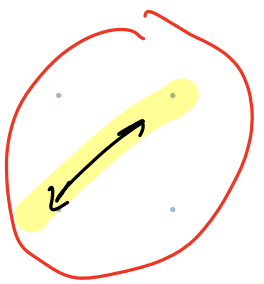
right diagonally polarized





Filter with same polarization

?



II

Which is true?

A) Photon I is brighter than II

B) Photon II is brighter than I

C) I and II are the same brightness

Quantum Crypto (BB84)

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

	a (basis bit)	b (info bit)	photon	qubit state
vert	0	0	↕	$\|0\rangle$
hor	0	1	↔	$\|1\rangle$
diag	1	0	↗↙	$\|+\rangle = \frac{1}{\sqrt{2}}\|0\rangle + \frac{1}{\sqrt{2}}\|1\rangle$
diag	1	1	↖↘	$\|-\rangle = \frac{1}{\sqrt{2}}\|0\rangle - \frac{1}{\sqrt{2}}\|1\rangle$

$a = 0\,0\,1\,0\,1\,1\,1\,0\,1 \ldots$ (L)

1. Alice chooses $a, b \in \{0,1\}^L$ ← Large number randomly. Secretly!
   At i^{th} second, sends photon a_i, b_i to Bob.

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

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

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

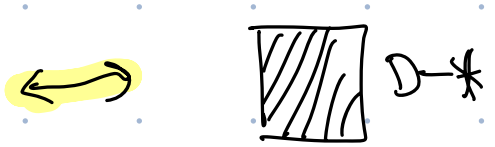
ex: Round 1 2 3 ...

$a = 0\ 1\ \cdots$

$b = 1\ 1$

$c = 1\ 1$

$d = 0/1\ 1$

1st Photon 

2nd Photon 

Q: If $a_i = c_i$ then

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) $b_i \neq d_i$ C) $b_i = d_i$ ½ the time

4. Alice + Bob publicly announce a, c strings after Bob has finished measuring all photons.

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

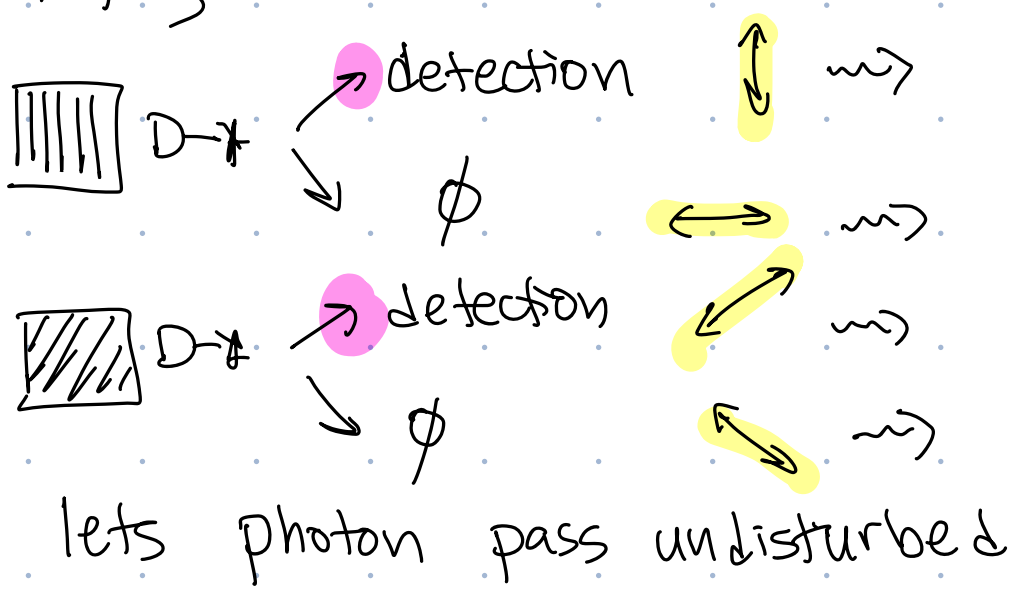
Secret key!?

What about Eve?? (She knows protocol, just not particular choices of a, b, c)

Possible strategy for Eve:

- Chooses $e \in \{0, 1, 2\}^L$ at random

$$e = \begin{cases} 0 \\ 1 \\ 2 \end{cases}$$



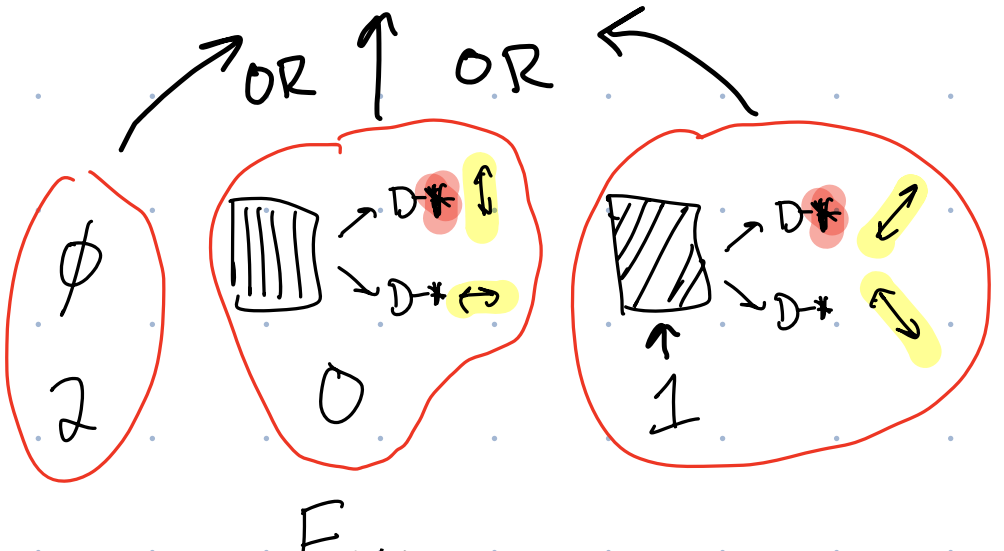
- Records $f = \begin{cases} 0 & \text{detection} \\ 1 & \text{no detection} \\ 2 & \text{no measurement} \end{cases}$

* Has to make their choice before a, c announced.

Ice breaker: what clubs/sports/activities do you do?

$a=0, b=0$

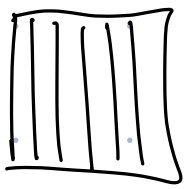
Alice ↕ ⇝



e:

Eve

$c=0$



Bob ↕ D*

d?

$f=0$

$f=1$

$f=2$ (no meas.)

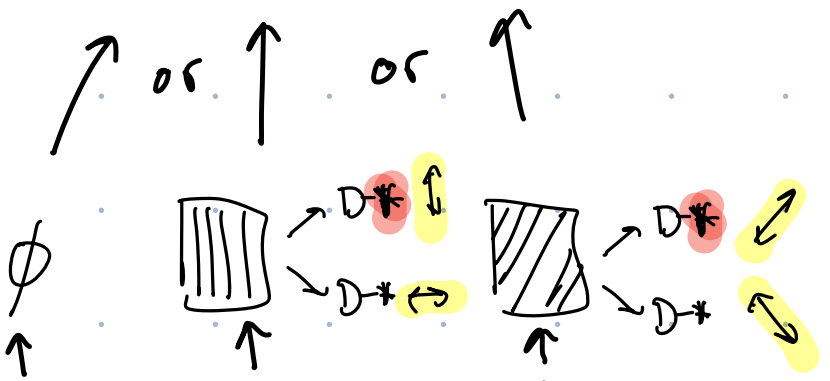
- What are d, f for each e?
- What does Eve learn about key?
- How does Eve's action affect key?
- Other cases where $a=c$?
- Why don't we care about cases where $a \neq c$?

Ice breaker: what clubs / sports / activities do you do?

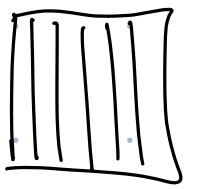
$a=0, b=0$

Alice  ⇝

Eve



$c=0$



Bob

d?

f?

e: 2 or 0 or 1

- What are d f for each e?
  - $e=0$ $f=0$ $d=0$
  - $e=1$: $f=0/1$ $d=0/1$
  - $e=2$ $f=2$ $d=0$

- $e=2$

- Other cases where $a = c$? See HW
- Why don't we care about cases where $a \neq c$?

The more Eve interfers, the more $b' \neq d'$ (b', d' = remaining bits)
+ the more Eve knows about b', d'.
Seems bad :(... actually ok.

6. A + B make public a random subset of bits of b', d' to detect Eve

Remaining strings: b'', d''

7. Alice + Bob error correct b", d" (parity checks)

b" d"

↘ ↙

s'

Outcome

- $|s'| < |b'|, |d'|$
- Eve learns extra info about s', b/c knows protocol
- A + B have matching s'

8. A + B do privacy amplification (hash function)

$s' \to s$

Outcome

- $|s| < |s'|$
- Eve knows nothing about s', even though she knows the hash function

As a group

- Review BB84 protocol
- Generate questions
- BB84 produces a secret key that is guaranteed secure from any eavesdropper. What is the quantum secret sauce?
- go! BB84