Learning Goals

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

Announcements

Exit Tickets

Secret Key Cryptography

See PSet 1

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

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

Secret key
S

Problem:

Current Solution:

Looming Problem:

When one door closes, another door opens

To do quantum crypto, need quantum particles:

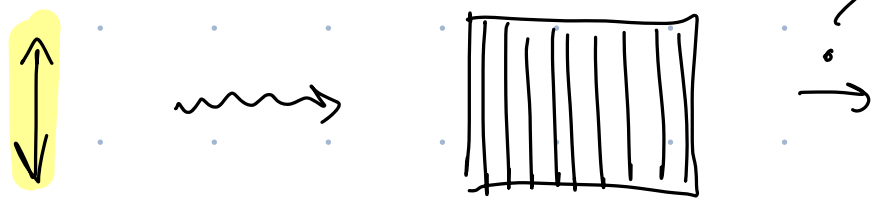
photons ⇒ individual particles of light

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

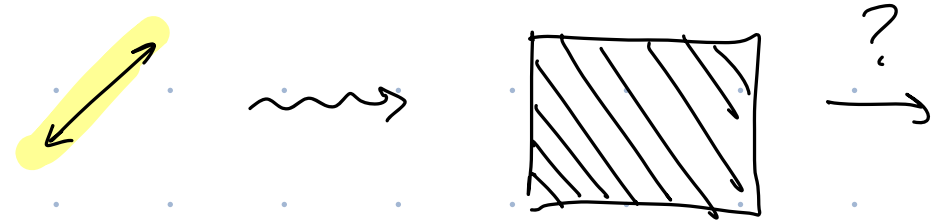
Photons + Polarizers

vertical polarized



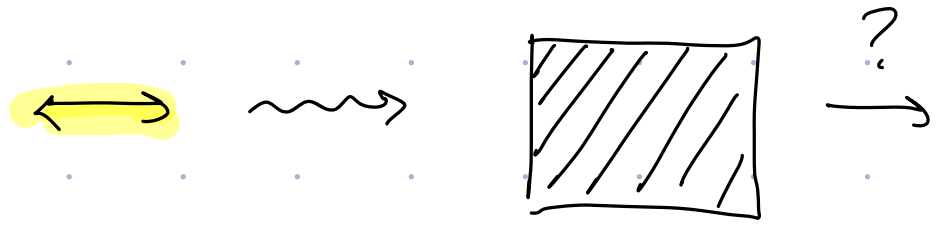
Filter with same polarization

diagonally polarized



Filter with perpendicular polarization

horizontally polarized



Filter with 45° polarization

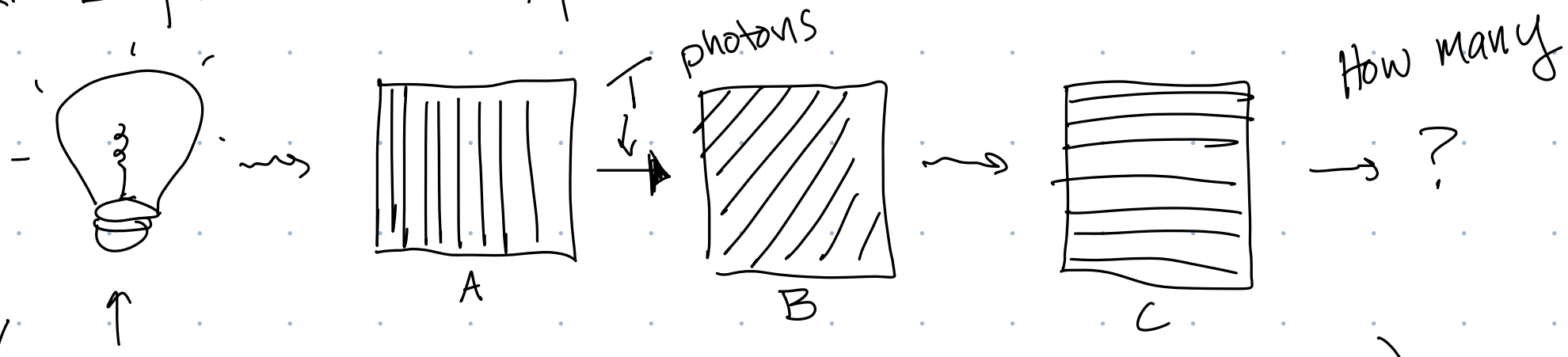
i-er

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:



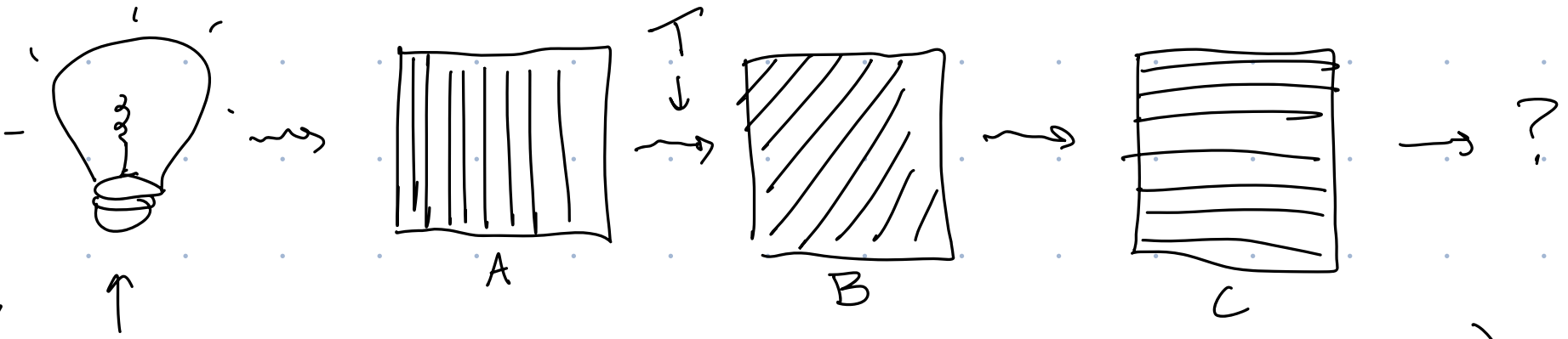
(lamp emits each photon with random polarization)

- 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)

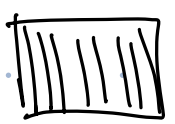
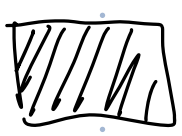
- What polarization(s) do exiting photons have?
- If T photons hit polarizer B, how many photons/sec exit polarizer C (on average)?

Quantum Crypto (BB84)

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

	a (basis bit)	b (info bit)	photon	qubit state
vert	0	0		
hor	0	1		
diag	1	0		
	1	1		

1. Alice chooses $a, b \in \{0,1\}^L$ ← Large number randomly.
   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
   At i^{th} second, sets up measurement c_i

3. Records outcome $d_i = \{$

ex:	Round	1st Photon	2nd Photon
a =	0 1 ⋯		
b =	1 1		
c =	1 1		
d =			

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.

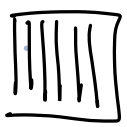
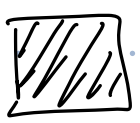
5. Alice and Bob throw out the bits of b, d corresponding to bits where $a \neq c$. Remaining bits of b, d match!

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

$$e = \begin{cases} 0 & \text{  } \\ 1 & \text{  } \\ 2 & \text{lets photon pass undisturbed} \end{cases}$$

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

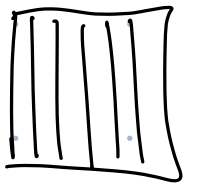
* Has to make their choice before a, c announced.

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

a=0, b=0

Alice 

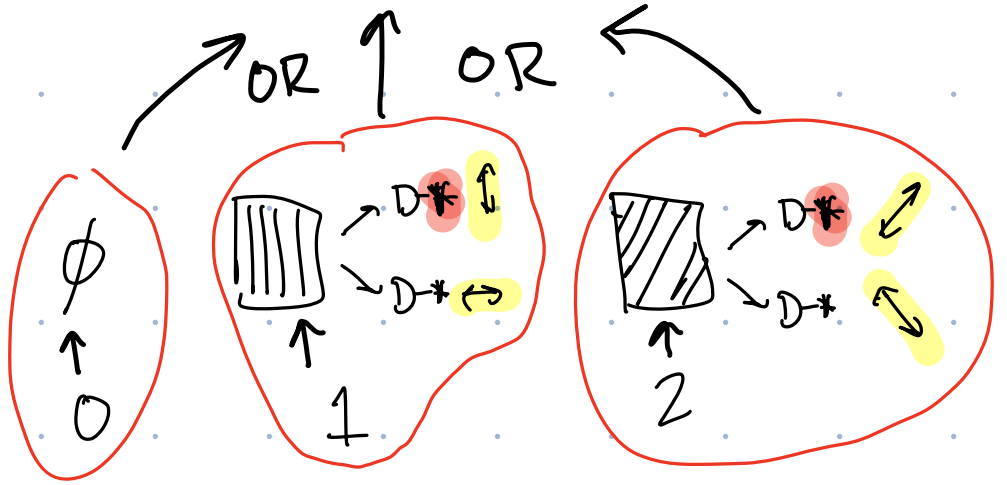
c=0



Bob

d?

D→*

e: 

f=0

f=1

Eve

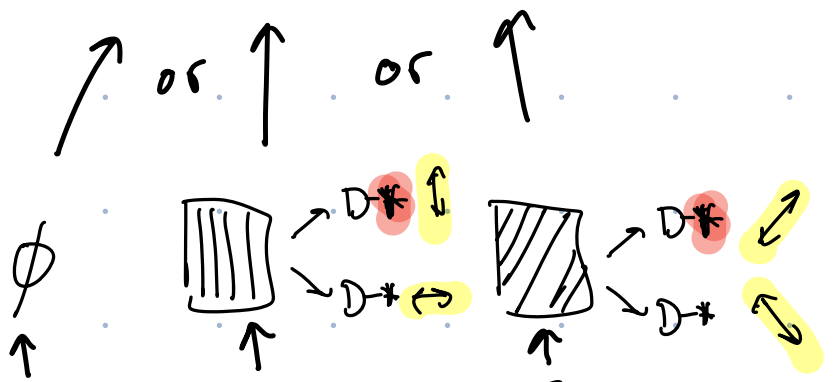
- What are d, f for each e?
- What does Eve learn about key?
- How does Eve's action affect key?
- Other cases where a = c?
- Why don't we care about cases where a ≠ c?

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

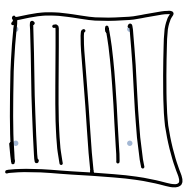
a=0, b=0

Alice  ⇝

Eve



c=0



Bob

d?

D→*

f?

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