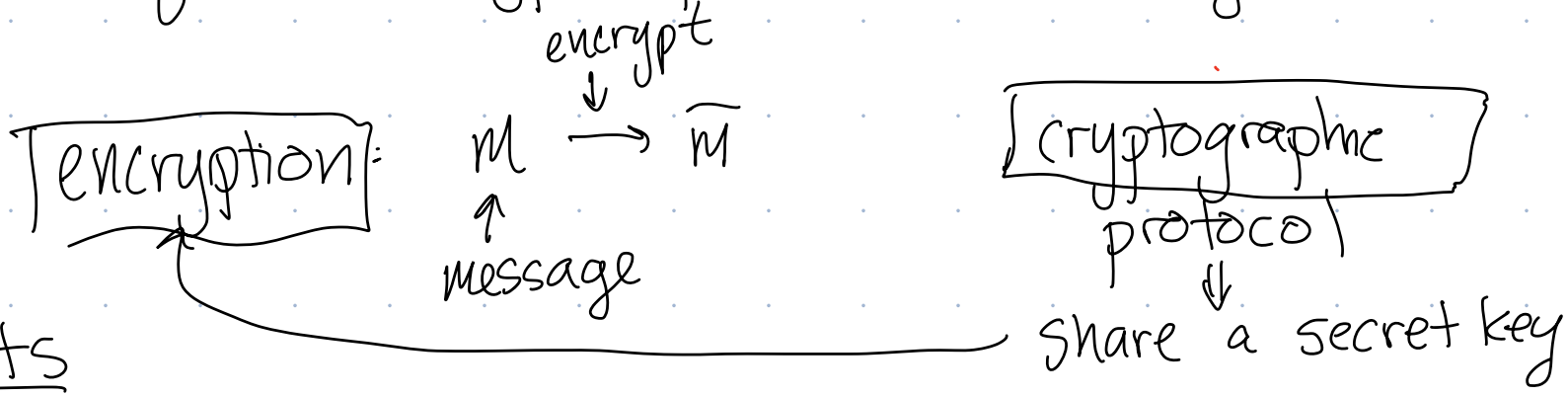
QUANTUM CRYPTOGRAPHY

Learning Goals

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



Announcements

What I Did This Summer, Fri 12:30-1:45, 75SH5 102

PIZZA!

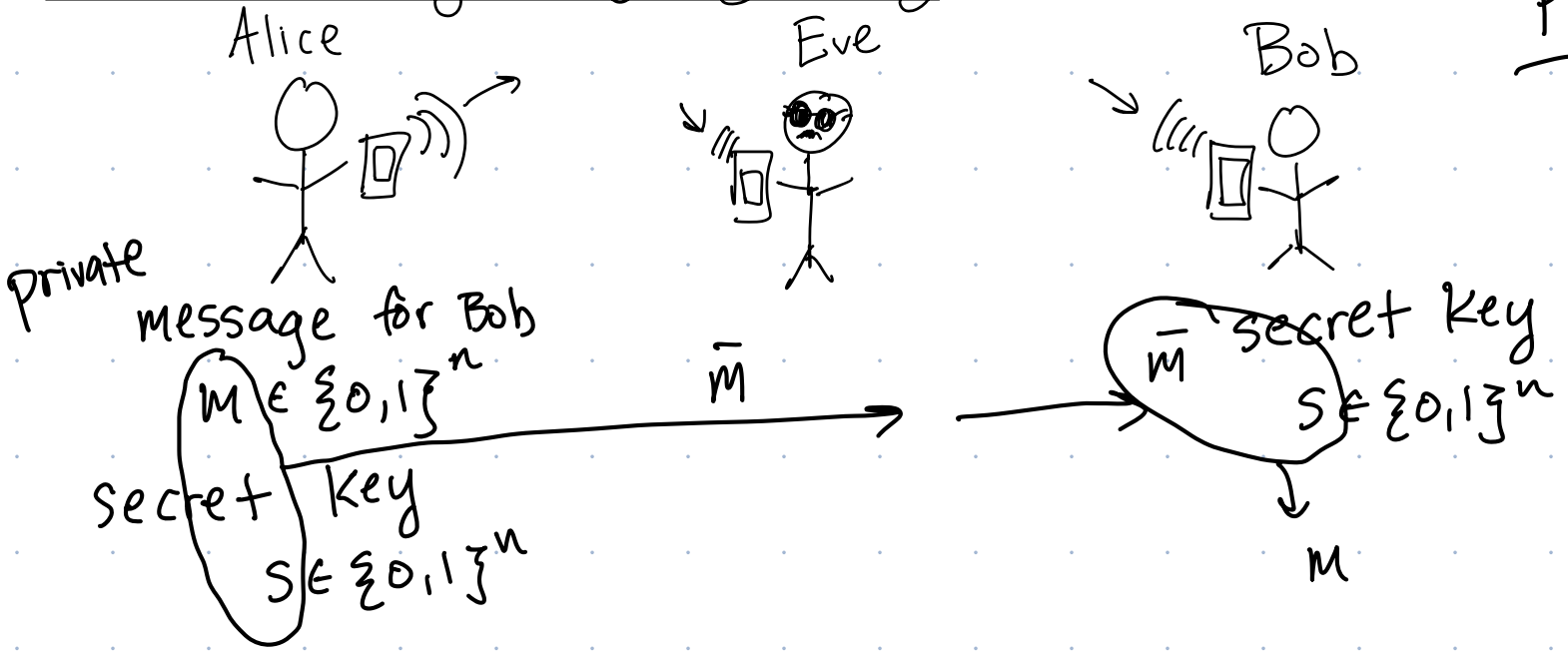
Exit Tickets

Review Alice + Bob BB84.

- Length of b/d after throwing out?
- Why do they publicly announce a, c?

Secret Key Cryptography

PS1



Problem: How to share secret key?!

Current Solution: Public Key Cryptography (PS1)

Looming Problem: Eve with a quantum computer can crack PKC

When one door closes, another door opens

door → Public Key Crypto

door → Quantum Crypto Protocol

To do quantum crypto, need quantum particles:

photons ⇒ individual particles of light

Fast, Fiberoptic infrastructure

Easily lost

Hard to create + detect (single photons)

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

A. Same as no diag.

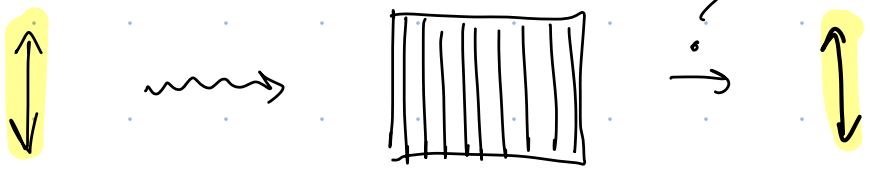
B. Less than Single filter

C. Same as single filter

D. More than single filter

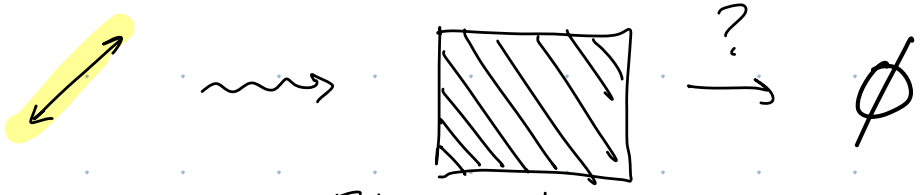
Photons + Polarizers

vertical polarized



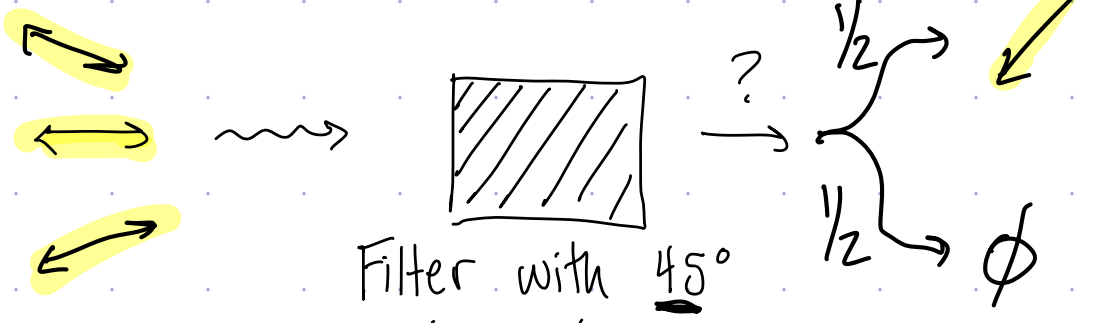
Filter with same polarization

diagonally polarized



Filter with perpendicular polarization

horizontally polarized



Filter with 45° polarization

"collapse"

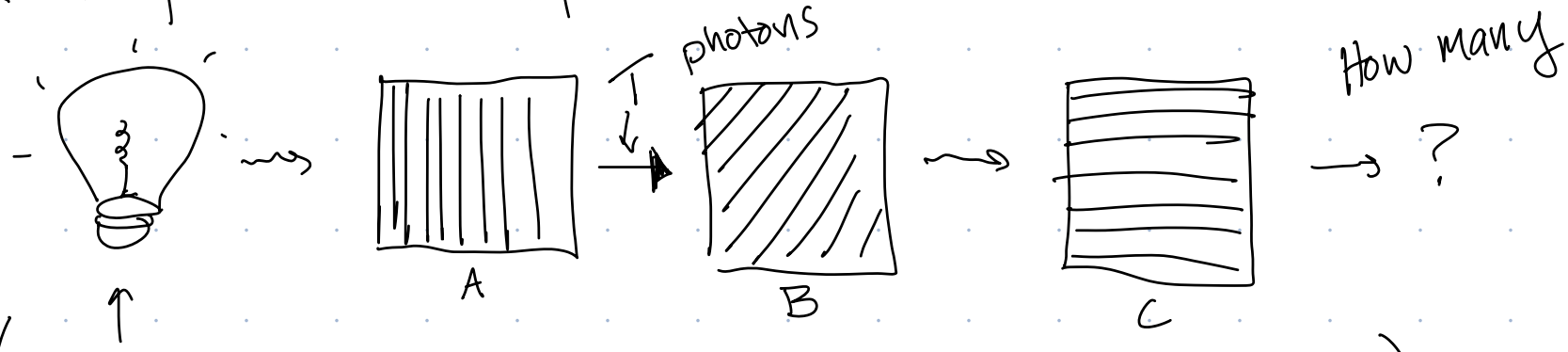
★ Behavior only depends on angle between photon polarization + polarizer

✓ Exiting photons have same polarization as filter

Group Work:

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

Q. Explain our experiment:



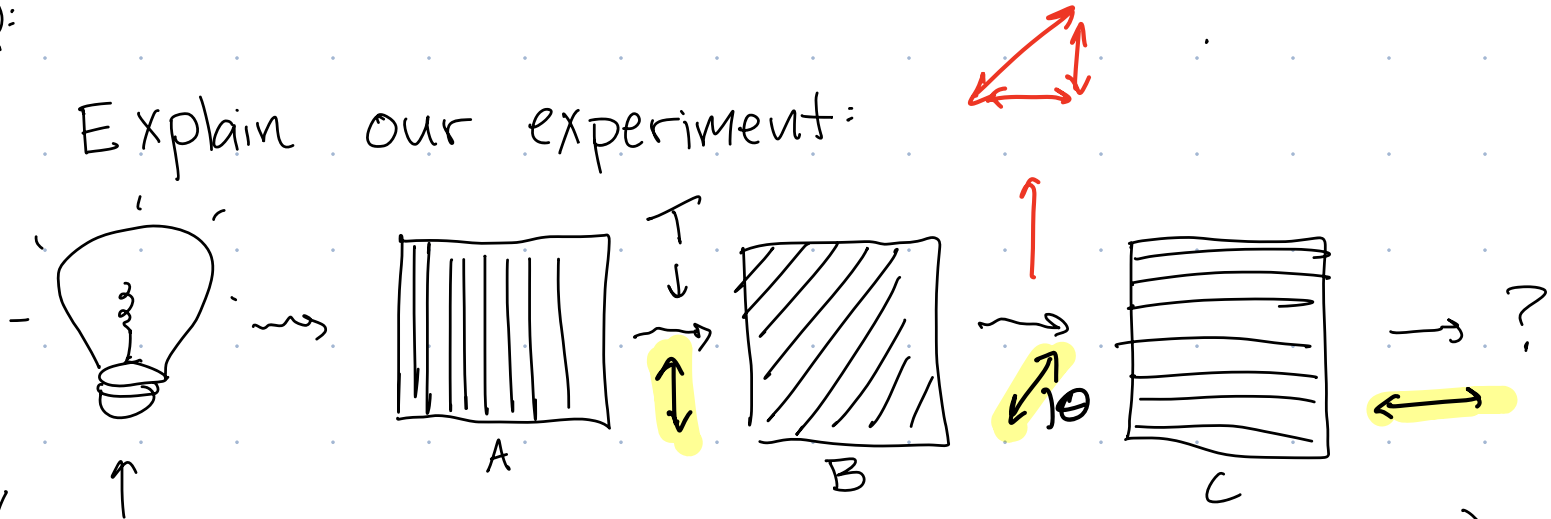
(lamp emits each photon with random polarization)

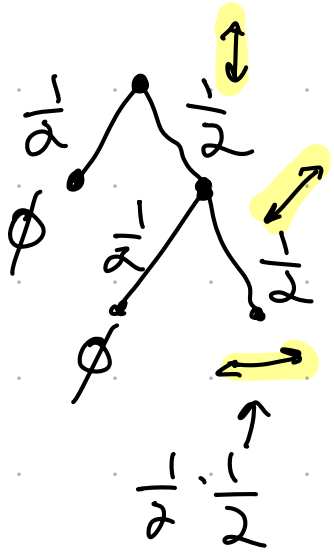
- What polarization(s) do exiting photons have? ⟷
- If T photons hit polarizer B, how many photons exit polarizer C? T/4

(Learning target QI1 → Foundational)

Q:

Explain our experiment:



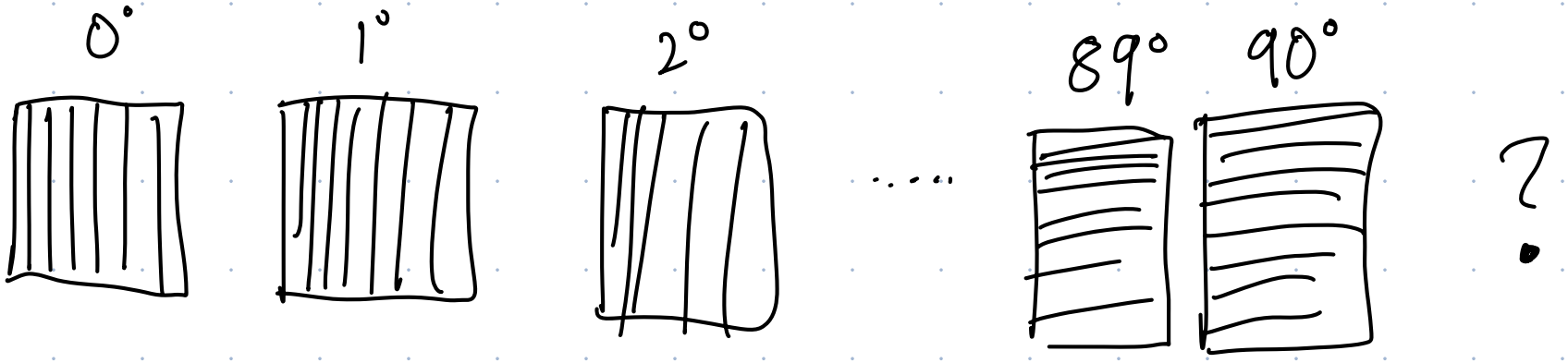


(lamp emits each photon with random polarization)

- What polarization(s) do exiting photons have? Horizontally polarized
- If T photons hit polarizer B, how many photons/sec exit polarizer C (on average)? $\frac{1}{4}$ chance of exiting

  $\frac{T}{4}$ photons exiting

Exit Tickets



- Filters → single photon?

- Syllabus
- PSETS - upcoming
- Exams

No video :

Quantum Crypto (BB84)

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

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

random, keeps private

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

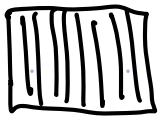
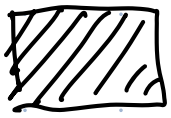
a: 0 0 1 0 1 1

b: 1 0 1 1 1

i: 1 2 3

↔

At i^{th} time step A sends a_i b_i^{th} photon 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} time step, 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 ...

$a = 0\ 1 \ldots$

$b = 1\ 1 \ldots$

$c = 1\ 1 \ldots$

$d = 0/1\ 1$

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 (Eve knows)

5. Alice + Bob throw out any bits of b, d corresponding to bits where $a \neq c$. Remaining bits of b, d match ⇒ call those strings b', d'!

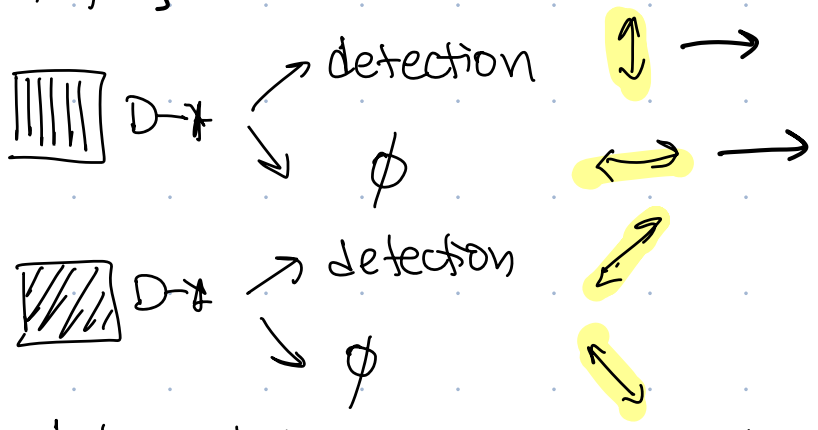
Secret Key?!

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

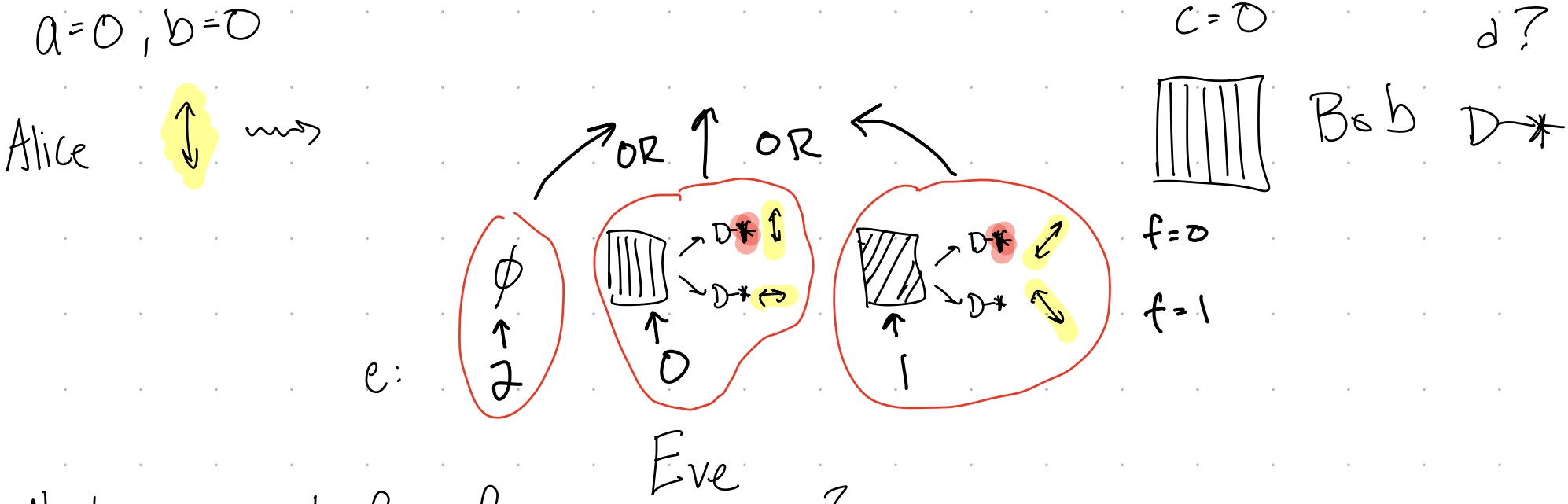
* Has to make their choice before a, c announced.

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

$a=0, b=0$

$c=0$

d?

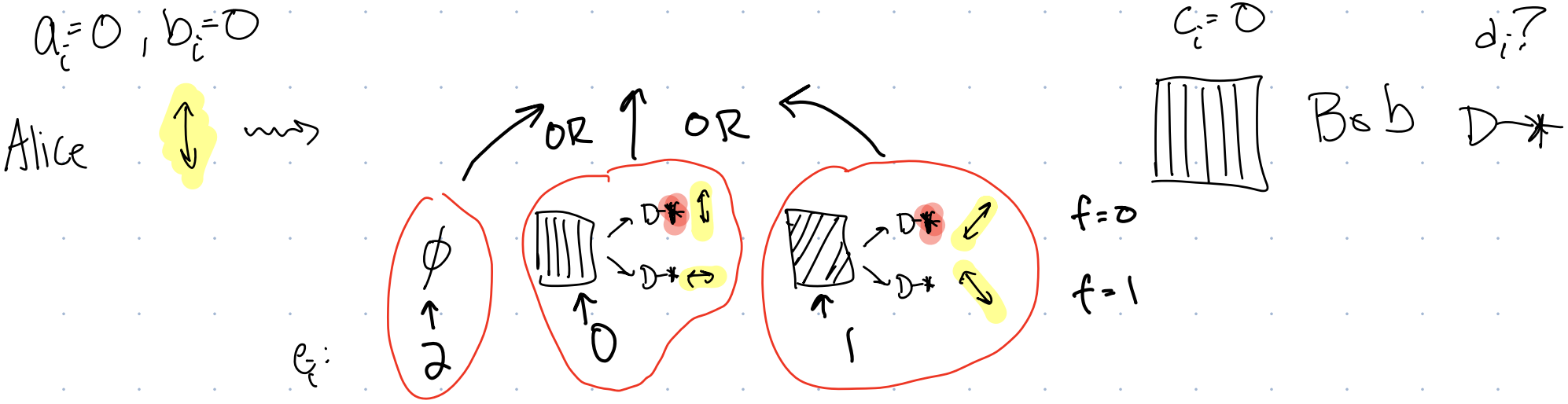


- What are d, f for each e?
- What does Eve learn about key?
- How does Eve's action affect key?
- Other cases where $a = c$?
- Why don't we care about cases where $a \neq c$?

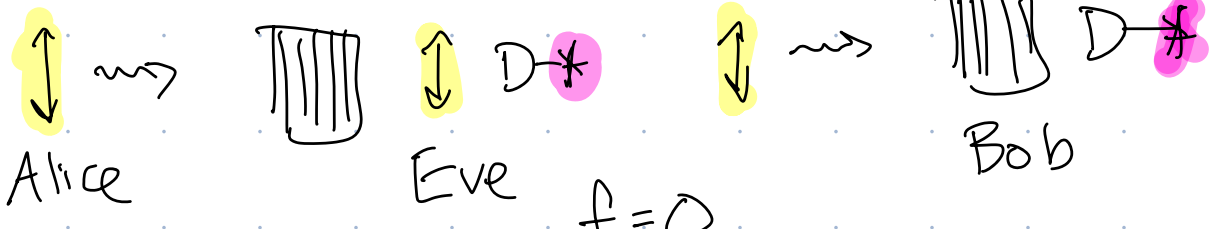
Ice breaker: what clubs/sports/activities do you do?

$a_i = 0, b_i = 0$

$c_i = 0$ d_i?

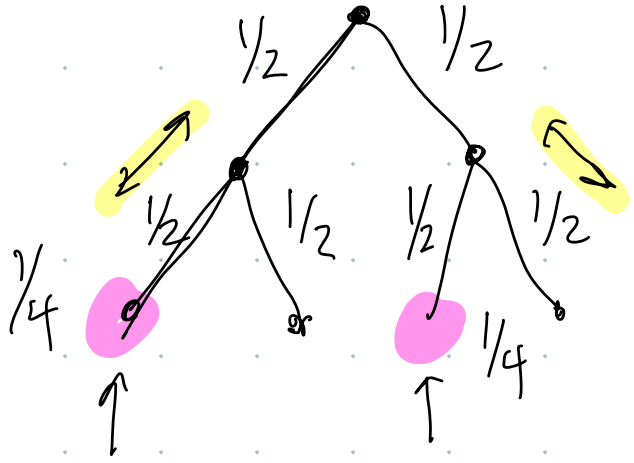


- What are d, f for each e?
  - $e_i = 2$: $b_i = d_i = 0$ $f_i = 2$
  - $e_i = 0$:



$f_i = 0$ $d_i = 0$

  - $e_i = 1$

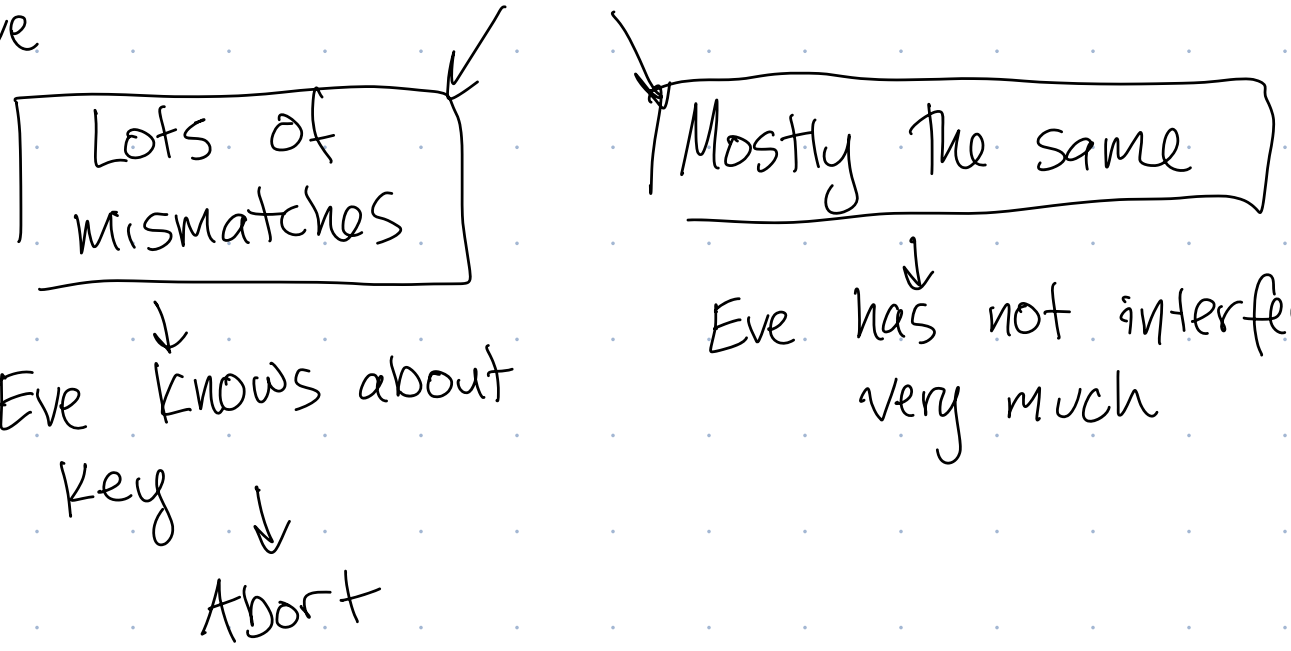


1/2 chance of detection

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

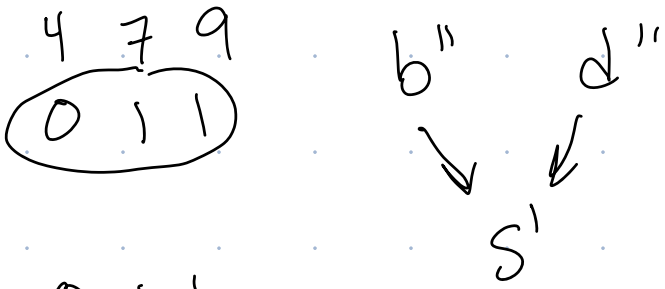
The more Eve interfers, the more $b' \neq d'$ (b', d' = remaining bits)
+ the more Eve knows about b', d'.
Seems bad :(... actually ok.

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



Remaining strings: b'', d''

7. Alice + Bob <u>error correct</u> b", d" (parity checks)



<u>Outcome</u>

- $|s'| < |b''|, |d''|$
- Eve learn extra info about s'
- A+B have matching s'

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

$s' \rightarrow s$

<u>Outcome</u>

- $|s| < |s'|$
- Eve know nothing about s even though she knew a little about s', know hash

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

measurement disturbs state