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

PSet Self Assessment Process

Exit Tickets

- How photon polarization measured?
- Polarizer does heat up from blocking light, effectiveness can decrease
- Diagonal real or a probability?
- Polarizers a metaphor? Or really in computer?
- More photons? (One at a time?)

- Ket column?

Each photon "choice" independent?

Can you simulate a quantum computer w/ a classical?

Secret Key Protocol

Warm-Up (Day 2)

$m = 1 \quad s = 1$

$\bar{m} = ?$

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

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

Problem: How share secret key??

Current Solution: Public key cryptography

Looming Problem: 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

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.)

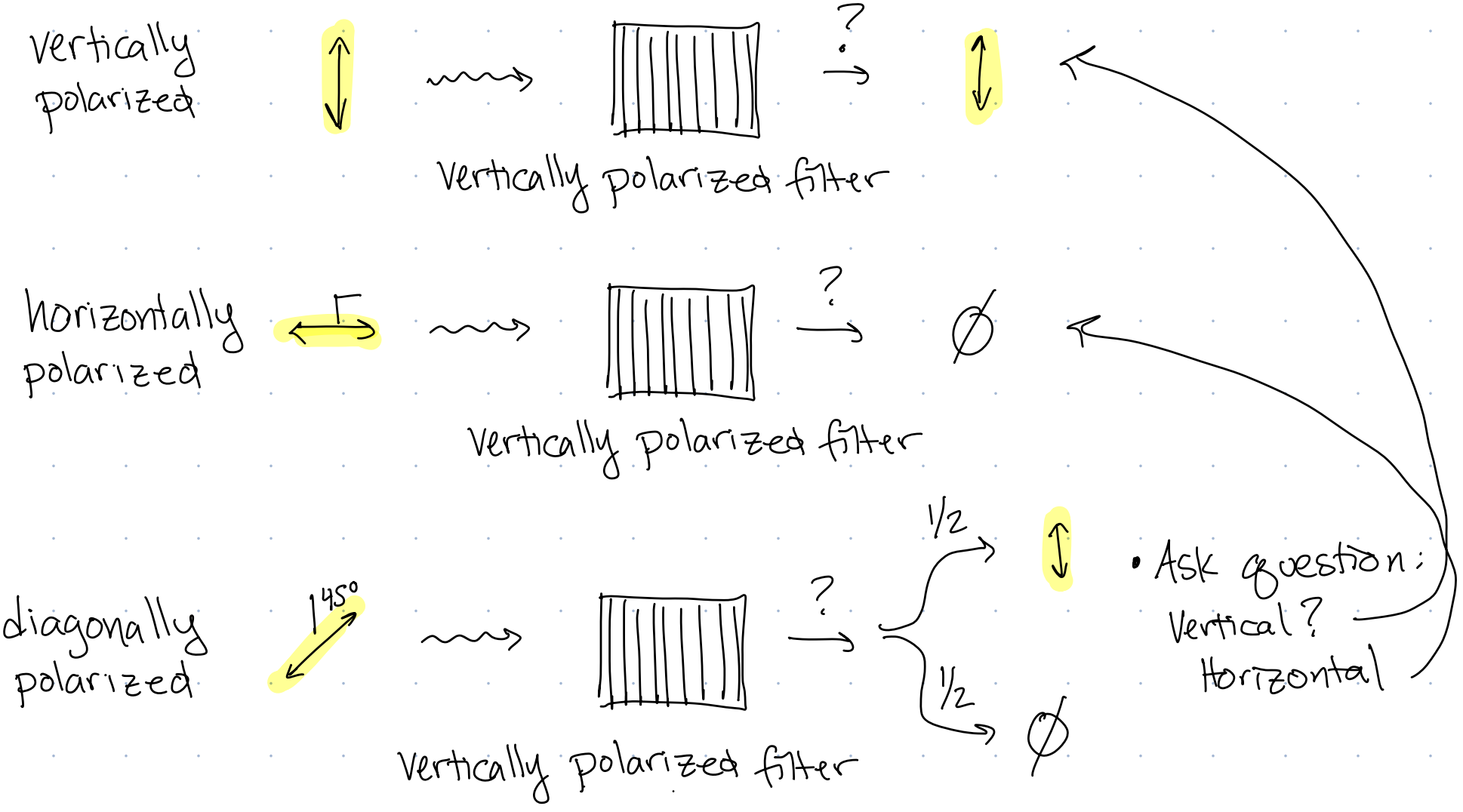
A. Same as no diag.

B. Less than Single filter

C. Same as Single filter

D. More than single filter

Photons + Polarizers

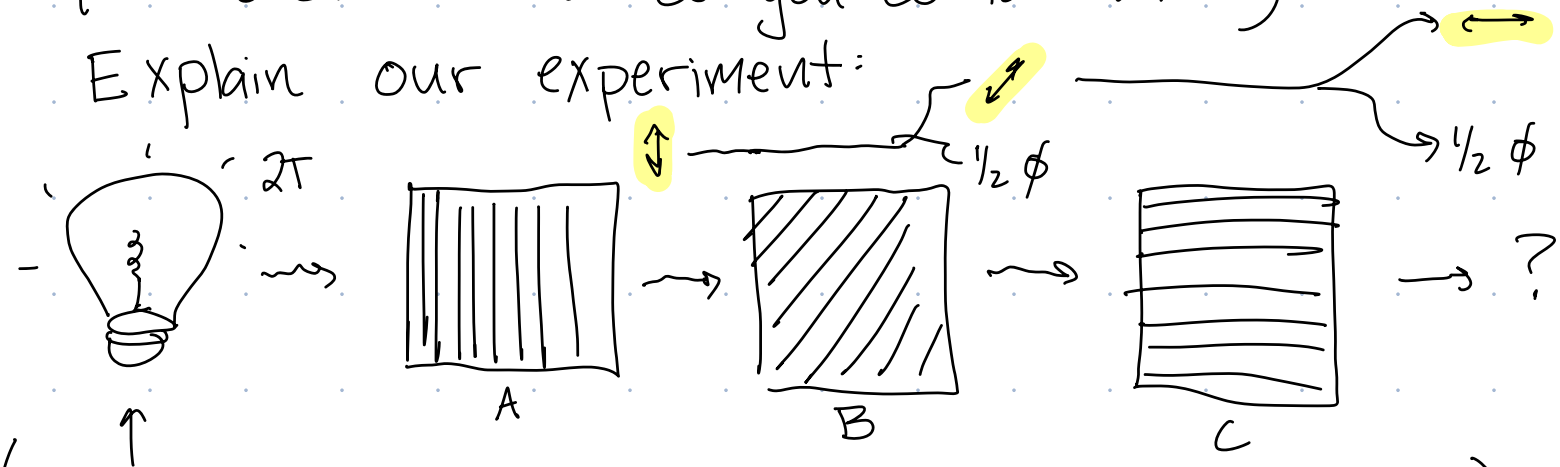


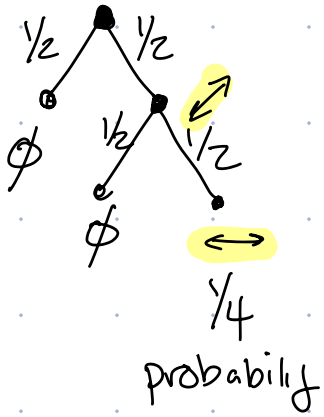
★ Behavior only depends on angle between photon polarization + polarizer

✓ Exiting photons have same polarization as filter

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

Explain our experiment:





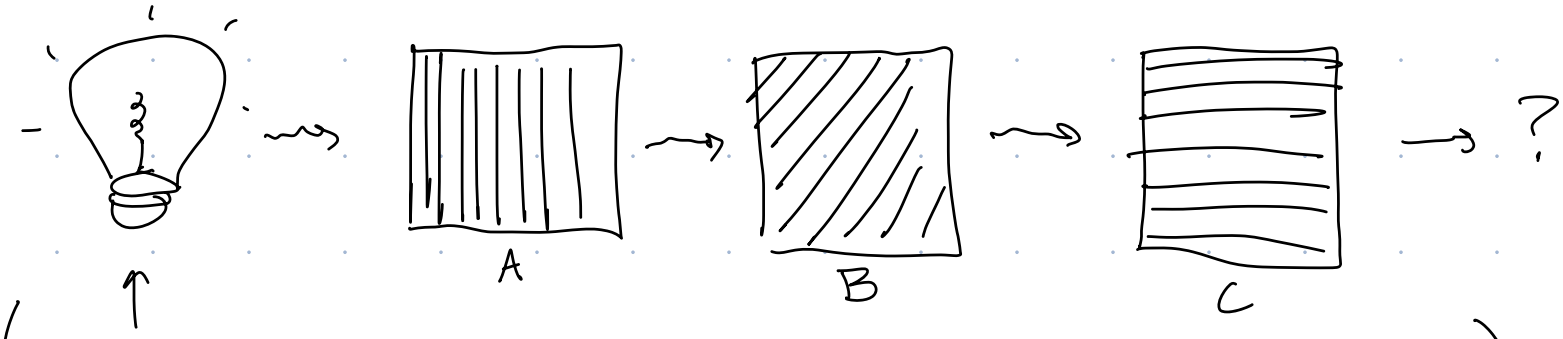
(lamp emits each photon with random polarization)

- 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:



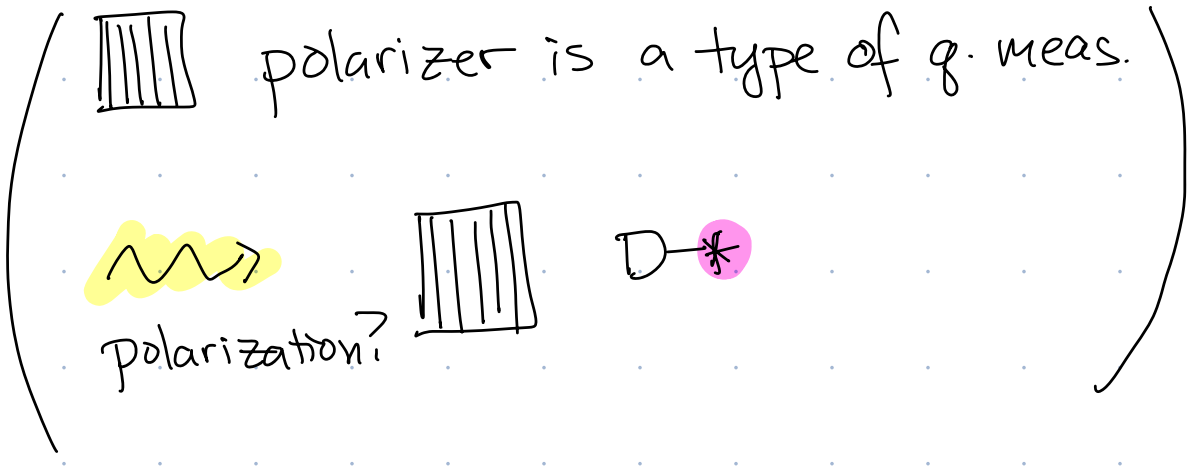
(lamp emits each photon with random polarization)

- 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)

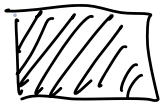
0. Alice + Bob pick $L \gg n$. (Eve knows L.)

	a (basis bit)	b (info bit)	photon	ket
vert/ hor. basis	0	0	↕	$\|0\rangle$
	0	1	↔	$\|1\rangle$
diag. basis	1	0	↗↙	$\|+\rangle$
	1	1	↖↘	$\|-\rangle$

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

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

↗ ↕ ↕ ↔ ↘ ⟶ Bob

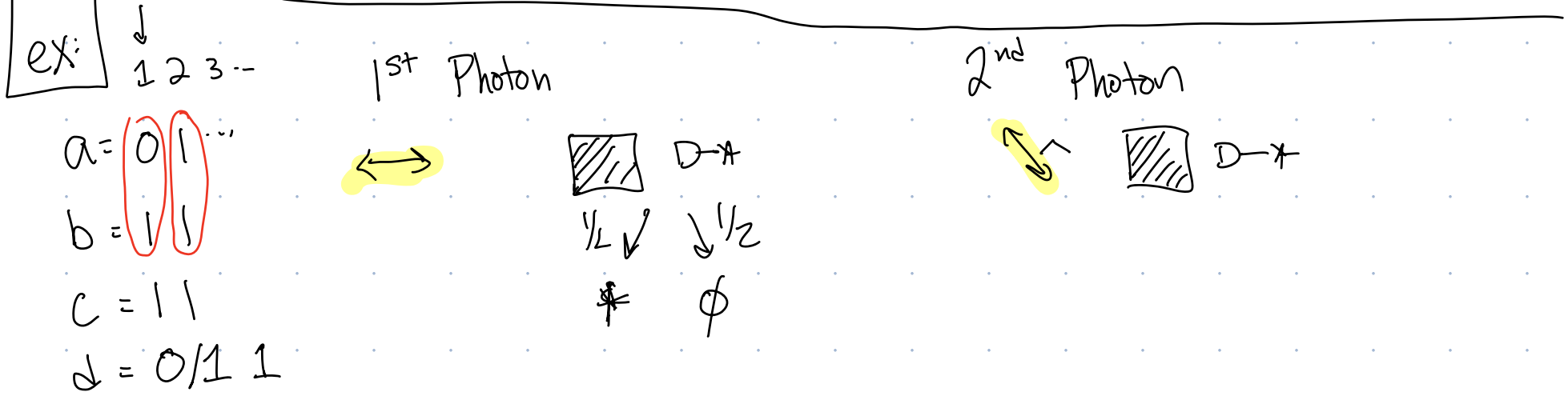
c (measurement basis bit)	Measurement	Ket
0	 D→*	$\{\|0\rangle, \|1\rangle\}$
1	 D→*	$\{\|+\rangle, \|-\rangle\}$

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

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

---

ex:



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

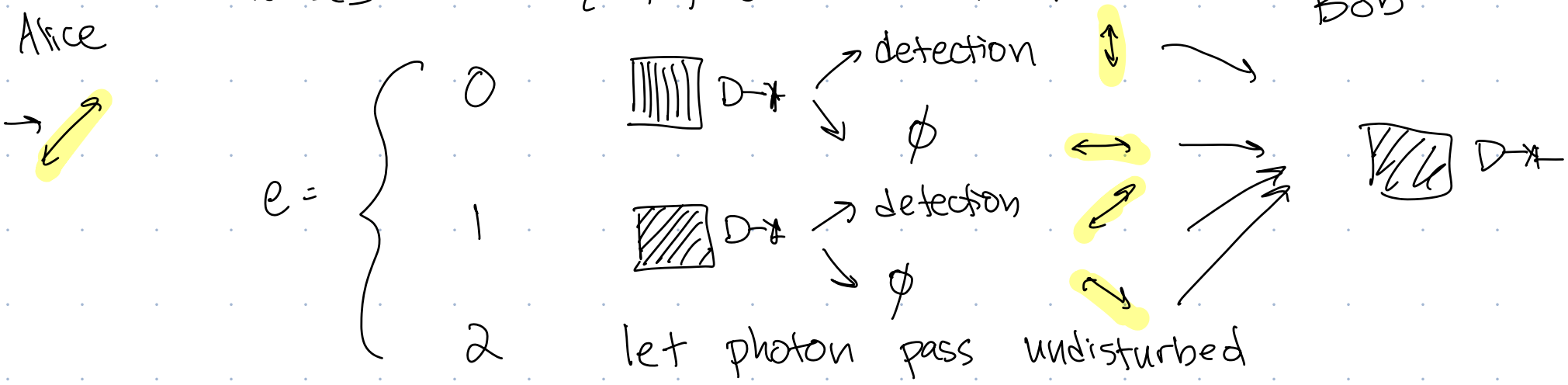
5. Alice and Bob throw out the bits of b, d corresponding to bits where $a \neq c$. Remaining bits of b, d match!

Secret key?!

What about Eve??

Possible strategy for Eve:

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



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

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

Simulate Eve's strategy.

What happens to Alice + Bob's secret key?

Bit	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
a	0	0	0	0	0	0	0	0	1	1	1	1	1	1	1	1	0	0	0	0
b	0	0	0	0	1	1	1	1	0	0	0	0	1	1	1	1	0	0	1	1
c	0	0	1	1	0	0	1	1	0	0	1	1	0	0	1	1	0	1	0	1
e	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	2	2	2	2
f	0	0/1		0/1	1	0/1	1	0/1	0/1	0	0/1	0		1	0/1		2	2		
d	0	0/1		0/1	1	0/1	0/1	0/1	0/1	0/1	0/1	0		0/1	0/1		0	0/1		

Bit	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
a	0	0	0	0	0	0	0	0	1	1	1	1	1	1	1	1	0	0	0	0
b	0	0	0	0	1	1	1	1	0	0	0	0	1	1	1	1	0	0	1	1
c	0	0	1	1	0	0	1	1	0	0	1	1	0	0	1	1	0	1	0	1
e	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	2	2	2	2
f	0	0/1		0/1		0/1	1	0/1	0/1	0		0		1	0/1		2	2		
d	0	0/1		0/1		0/1	0/1	0/1	0/1	0/1		0		0/1	0/1		0	0/1		

The more Eve interfers, the more $b' \neq d'$ (b', d' = remaining bits of b, d.) + the more Eve knows about b', d'

...

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

↓

+ then throw out those bits

↙ Lots of Mismatches

↓

Abort

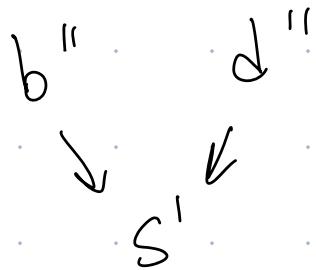
↘ Few mismatches

↓

Eve doesn't know very much about their key

Remaining strings: b'', d''

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



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

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

$s' \rightarrow s$

Outcome

- $|s| < |s'|$
- Eve knows nothing about s.

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?
- Play with go/BB84

Measurement disturbs the states