

QUANTUM CRYPTOGRAPHY

Learning Goals

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

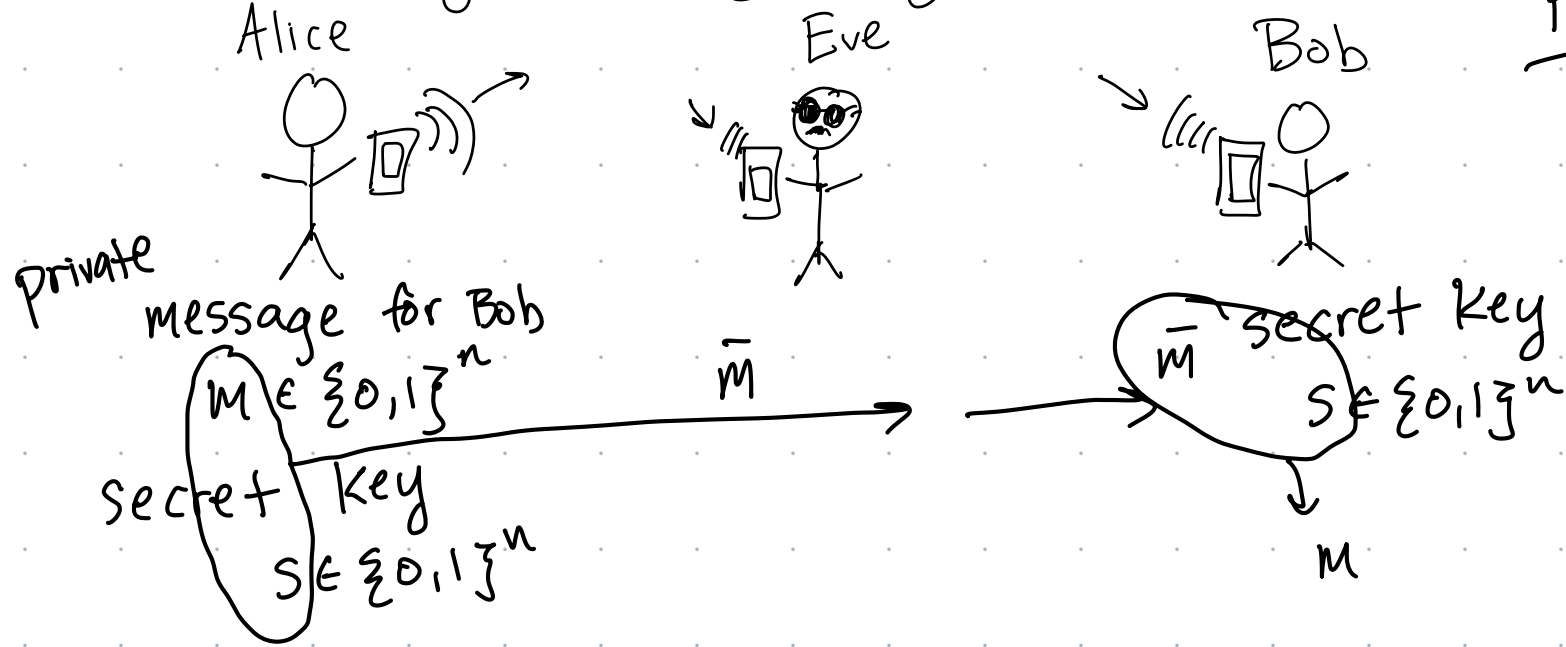
Announcements

What I Did This Summer, Fri 12:30-1:45, 755HS
PIZZA!
102

Exit Tickets

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

↓
Public Key
Crypto

↓
Quantum Crypto Protocol

To do quantum crypto, need quantum particles :

photons \Rightarrow individual particles of light



Fast, Fiberoptic infrastructure



Easily lost



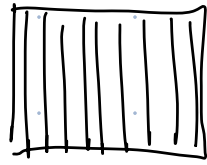
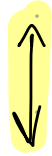
hard to create + detect (single photons)

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

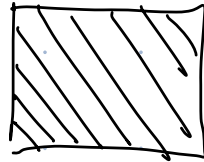
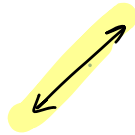
Photons + Polarizers

vertical
polarized



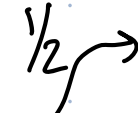
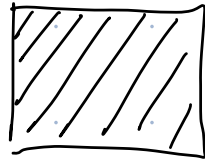
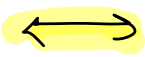
Filter with same
polarization

diagonally
polarized



Filter with perpendicular
polarization

horizontally
polarized



Filter with 45°
polarization

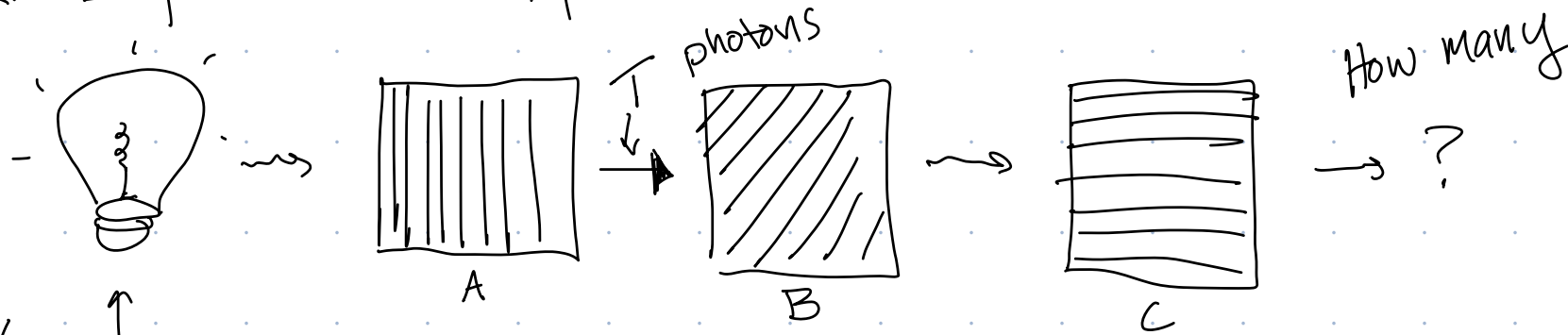
"collapse"

★ 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)

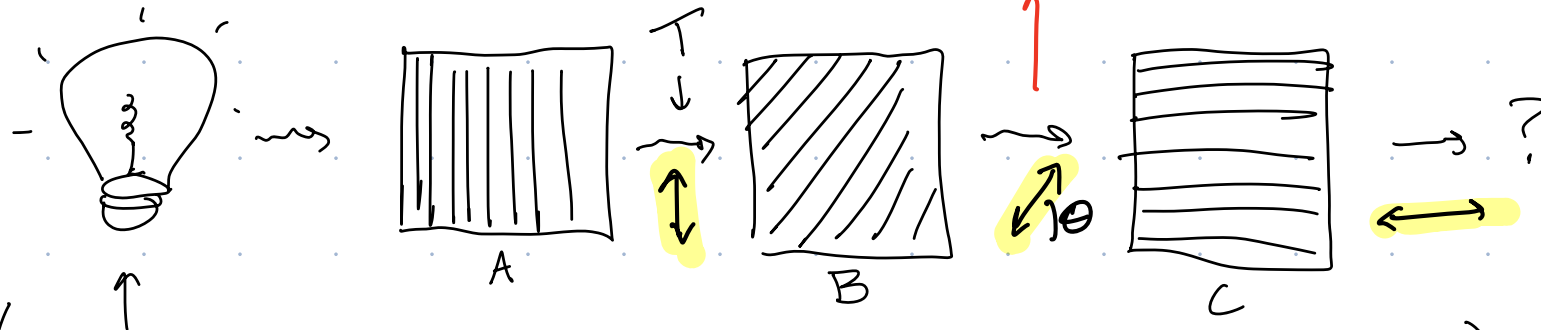
- What polarization(s) do exiting photons have? ↔
- If T photons hit polarizer B, how many photons exit polarizer C?

$T/4$

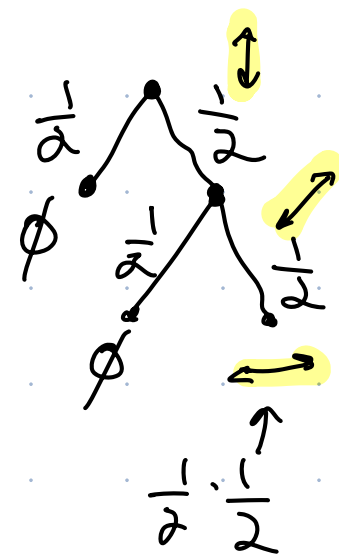
(Learning target QI1 → Foundational)

Q:

Explain our experiment:

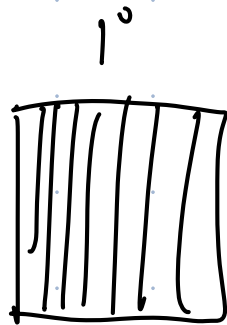
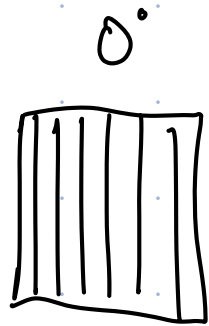


(lamp emits each photon with random polarization)

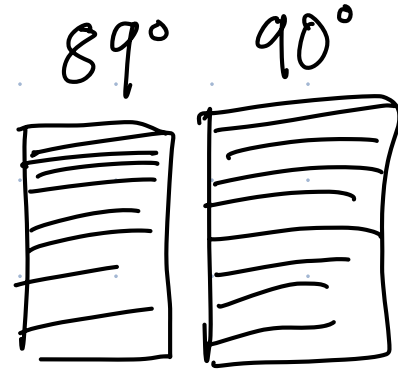


- What polarization(s) do exiting photons have? Horizontally polarized
- If T photons hit polarizer B, how many photons/sec exit polarizer C (on average)? $\frac{1}{4}$ chance of exiting
 $\frac{T}{4}$ photons exiting

Exit Tickets



...



?





• Filters → single photon?

- Syllabus
- PSETS - upcoming
- Exams

No video ñ

Quantum Crypto (BB84)

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

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

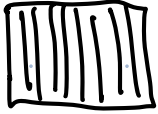

1. Alice chooses $a, b \in \{0, 1\}^L$ ← large number randomly.

a: 0 0 1 0 1 1
 b: 1 0 1 1 1
 i: 1 2 3

random,
keeps private

At i^{th} time step A sends $a_i b_i^{\text{th}}$ photon to Bob.







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

2. Bob chooses $c \in \{0, 1\}^L$ randomly

At i^{th} time step, sets up measurement c_i

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

ex:	Round	1st Photon	2nd Photon
	1 2 3 ...		
$a =$	0 1 ...	  $D-\ast$	  $D-\ast$
$b =$	1 1 ...		
$c =$	1 1 ...		
$d =$	0/1 1		

Q: If $a_i = c_i$ then

A) $b_i = d_i$ B) $b_i \neq d_i$ C) $b_i = d_i$ $\frac{1}{2}$ the time

Q: If $a_i \neq c_i$ then

A) $b_i = d_i$ B) $b_i \neq d_i$ C) $b_i = d_i$ $\frac{1}{2}$ the time

4. Alice + Bob publicly announce a, c strings
(Eve knows)

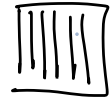
5. Alice + Bob throw out any bits of b, d
corresponding to bits where $a \neq c$. Remaining
bits of b, d match \Rightarrow call those strings b', d'
Secret Key?!

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

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



D

detection

\emptyset



D

detection

\emptyset

lets photon pass undisturbed



Bab

- Records

$f =$

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

detection

no detection

no measurement


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

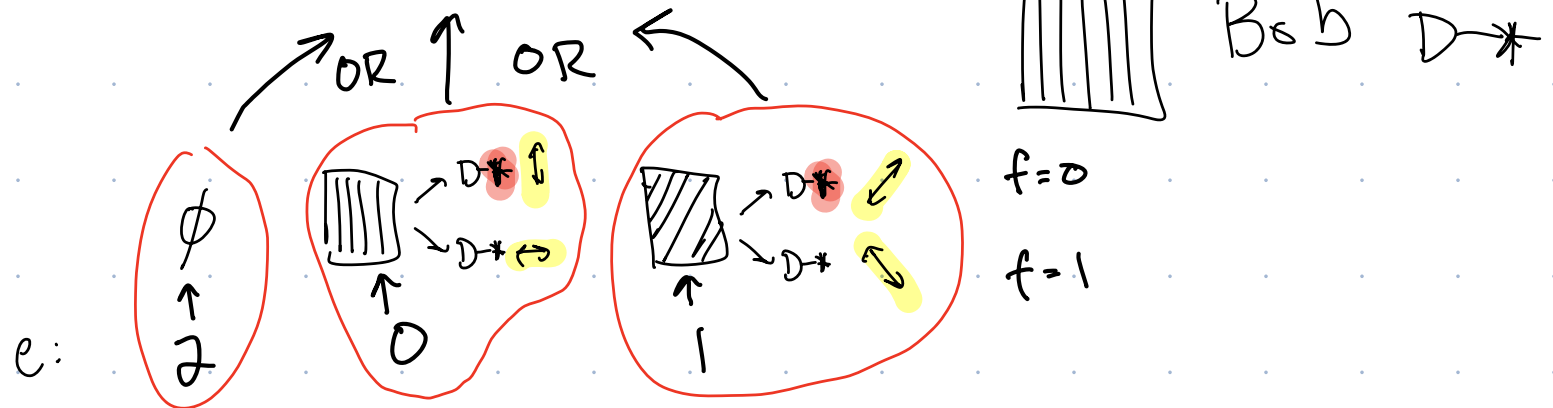
Ice breaker: what clubs/sports/activities do you do?

$a=0, b=0$

$c=0$

$d?$

Alice  \rightsquigarrow



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 $a \neq c$?

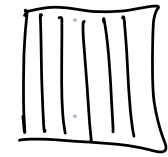
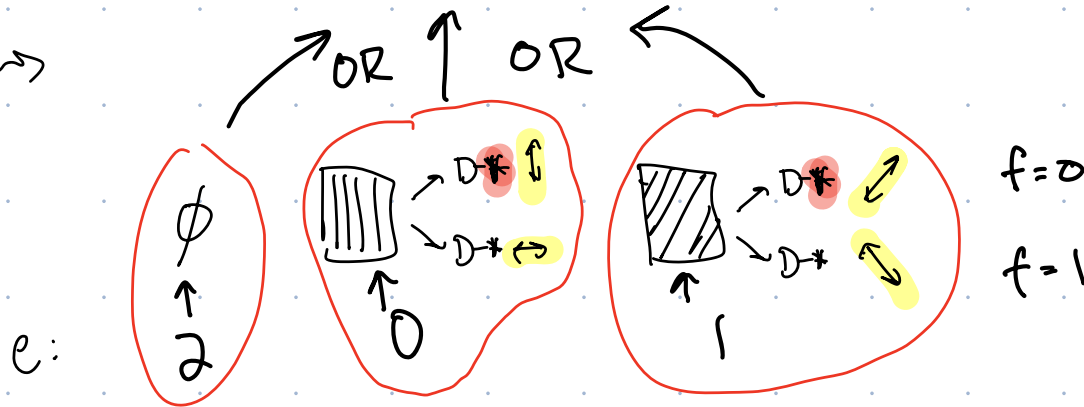
Ice breaker: what clubs/sports/activities do you do?

$a=0, b=0$

$c=0$

$d?$

Alice  \rightsquigarrow



Bob $D \rightarrow$

• What are d, f for each e ?

• $e=2:$

• $e=0:$

• $e=1$

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

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

Seems bad i ... 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)

Outcome

0

0

•

8. A + B do privacy amplification

Outcome

•

0

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