S. KIMMEL

Learning Goals

- Describe BB84 quantum crypto. protocol
- Describe quantum measurement

Crowd Notes! Introductions

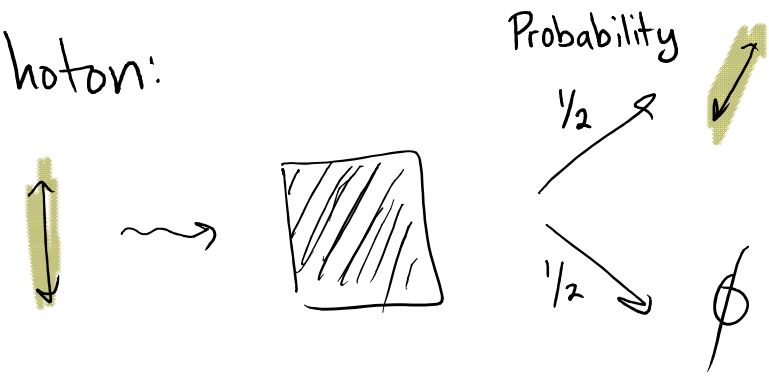
What is quantum computing?

- Use quantum bits to perform computational/informational tasks
- Because quantum bits follow different rules from Boolean bits, can do some tasks faster/better

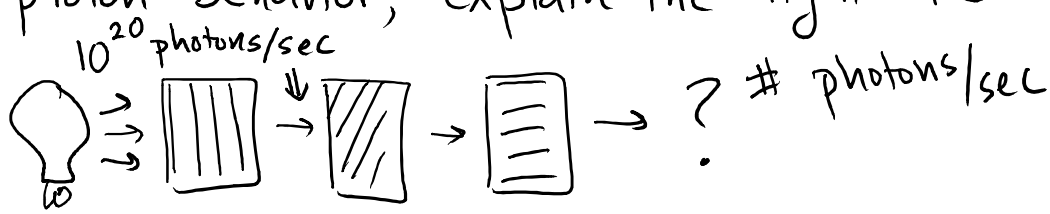
---

Goal: use photons to share secret key between Alice + Bob.

Single Photon:



Q: Given single photon behavior, explain the light bulb experiment



S.KIMMEL

Q: Given single photon behavior, explain the light bulb experiment

A. Half the vertically polarized photons make it through the diagonal filter, at which point they become diagonally polarized. Then half of those make it through the horizontal filter. Overall, 1/4 of photons that exit the first filter exit the final filter.

I said photon polarization is a qubit

BUT

Photon polarization doesn't seem like a 2-state system:

(more than 2 options)

BUT

When measure with filter, acts like only 2 options

S. KIMMEL

First Idea

Alice sends $\begin{cases} \updownarrow & \text{vertically polarized photon for } 0 \\ \leftrightarrow & \text{horizontally polarized photon for } 1 \end{cases}$

Bob:  , 

filter

Detector

light turns on if single photon hits

$\boxed{\text{Detector destroys photon}}$

1. How should Bob determine Alice's message?
2. What can Eve do to cheat?

S. KIMMEL

First Idea

Alice sends $\begin{cases} \updownarrow & \text{vertically polarized photon for } 0 \\ \leftrightarrow & \text{horizontally polarized photon for } 1 \end{cases}$

Bob:  , 

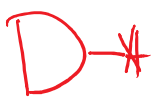
filter

Detector

light turns on if single photon hits

$\boxed{\text{Detector destroys photon}}$

1. How should Bob determine Alice's message?
2. What can Eve do to cheat?

Bob: vertical  

$\begin{cases} \text{light} \rightarrow 1 \\ \text{no light} \rightarrow 0 \end{cases}$

Eve: Sits between Alice + Bob. Does same as Bob. If detects, creates new $\updownarrow$ and sends to Bob. If no detection, creates new $\leftrightarrow$ and sends to Bob.

S.KIMMEL

BB84

Label states using bits

Basis	State	Polarization
0	0	↕
0	1	↔
1	0	↗↙
1	1	↖↘

1) Alice chooses $a, b \in \{0,1\}^n$

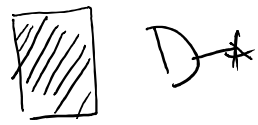
$a \Rightarrow$ basis, $b \Rightarrow$ state

ex:

$$\begin{array}{c} \\ a = \\ b = \end{array} \begin{array}{c} \begin{array}{cc} 1 & 2 \end{array} \\ \left.\begin{array}{cc} 0 & 1 \\ 1 & 1 \end{array} \cdots \right\} \end{array} \quad \underbrace{\begin{array}{cc} 1 & 2 \\ \leftrightarrow & \nwarrow\!\!\searrow \end{array} \cdots}_{\text{sends photons (in order, one at a time) to Bob}}$$

S.KIMMEL

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

- $c_i = 0 \implies$ 
- $c_i = 1 \implies$ 

} uses to detect i^{th} photon

$\boxed{a, b, c \text{ secret \& random (but not shared!)}}$

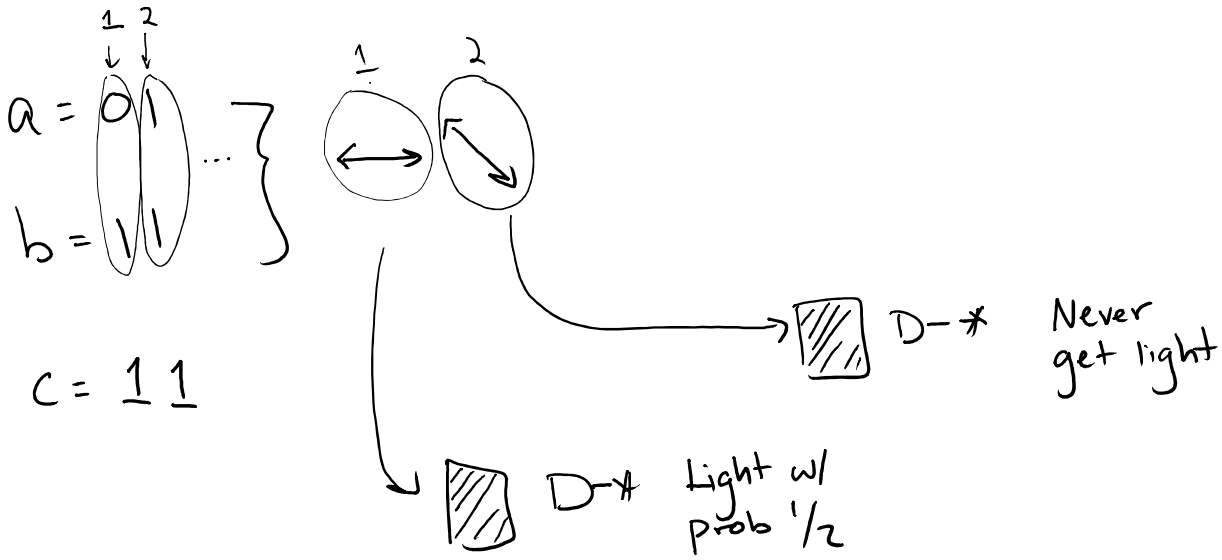
3. Bob records outcomes:

$$d \in \{0,1\}^n$$

$$d_i = \begin{cases} 0 & \text{if light on} \\ 1 & \text{if light off} \end{cases}$$

S.KIMMEL

ex:



$c = \underline{1}\,\underline{1}$

$d = 0\underline{1}$ or $\underline{1}\,\underline{1}$

4. Alice + Bob make public a, c.

Q

If $a_i = c_i$ A) $b_i = d_i \oplus 1$ B) $b_i = d_i$ C) $c_i = d_i$

D) $b_i \cdot d_i = 1$

If $a_i \neq c_i$ A) $b_i = d_i \oplus 1$ B) $b_i \cdot d_i = 1$

C) b_i and d_i match 1/2 of time

D) b_i and d_i match 1/4 of time

S.KIMMEL

Q

If $a_i = c_i$ A) $b_i = d_i \oplus 1$ $\boxed{\text{B) } b_i = d_i}$ C) $c_i = d_i$

D) $b_i \cdot d_i = 1$

Bob's choice of filter rotation means there is no probabilistic outcome, because he chose the <u>correct</u> rotation relative to Alice's preparation. Thus his measurement always matches Alice's preparation.

If $a_i \neq c_i$ A) $b_i = d_i \oplus 1$ B) $b_i \cdot d_i = 1$

$\boxed{\text{C) } b_i \text{ and } d_i \text{ match } 1/2 \text{ of time}}$

D) b_i and d_i match $1/4$ of time

Bob chose the <u>wrong basis</u> to measure, so

$\Updownarrow$

wrong rotation

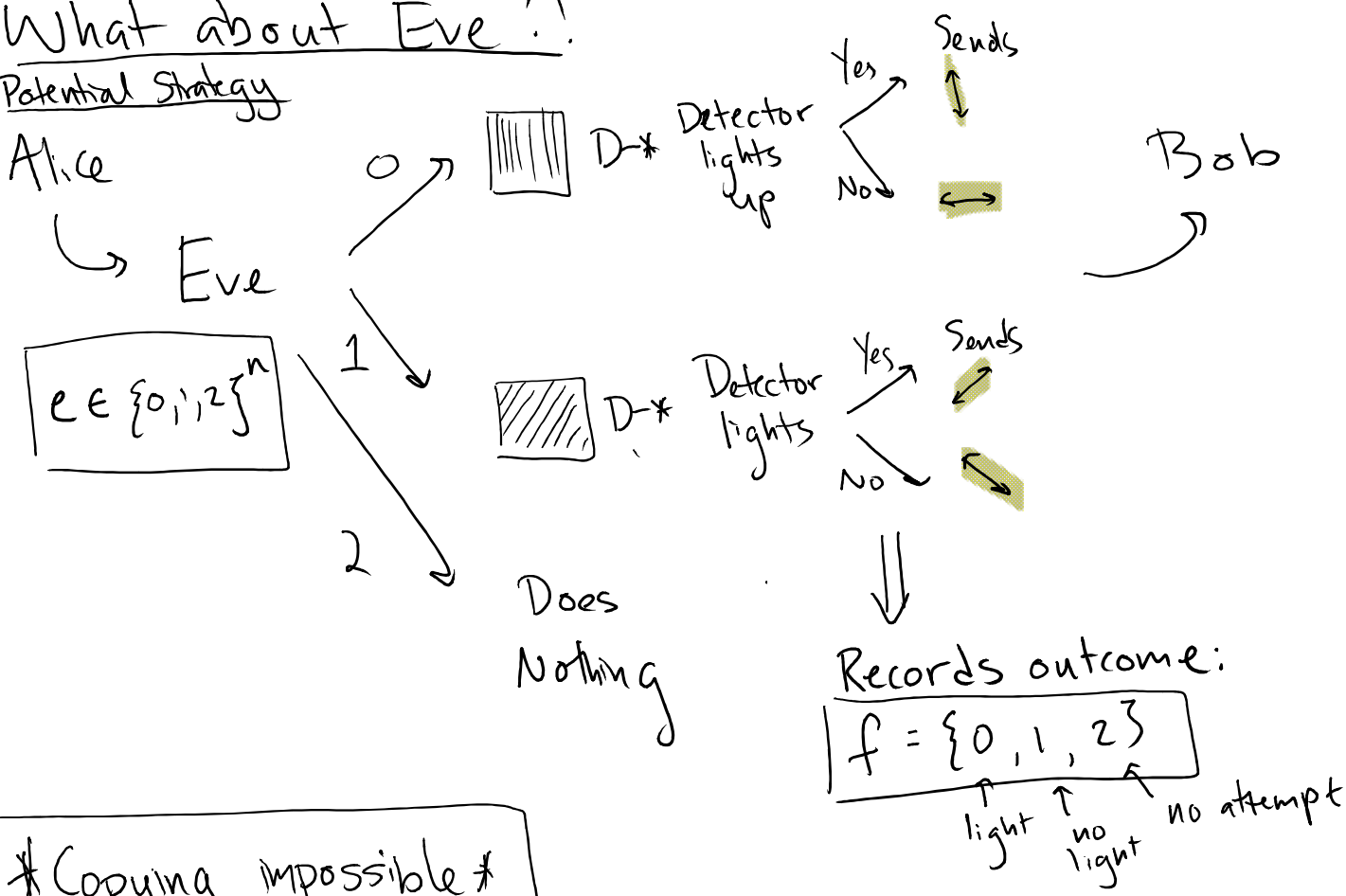
he gets a 0 or 1 with equal probability. Whatever Alice's bit is, his will match $1/2$ of time.

S.KIMMEL

5. Alice & Bob keep b', d' (bits of b, d where $a_i = c_i$).

What about Eve?!

Potential Strategy



Copying impossible

Group of 3: simulate Alice, Bob, Eve

(Eve happy whenever she chooses correct basis)