S. KIMMEL

Goals

- Describe BB84 & why it works
- Use vectors to describe states + measurements

Self-Assessment

(Tutoring?)

- Rubric
- Find solutions
- Make comments

Big picture: goal is to share a secret random string (not to send a message, yet).

⇓

secret key

S. KIMMEL

BB84

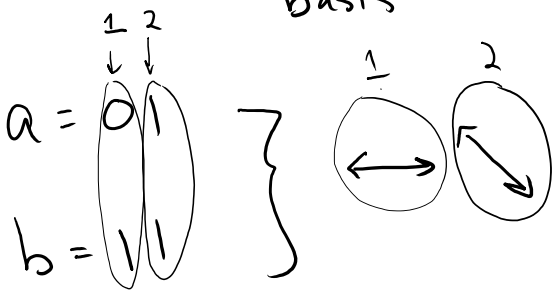
Label states with bits

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

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

basis state

ex:



She will send these photons in this order to Bob.

S. KIMMEL

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

- If $c_i = 0 \Rightarrow$  D→*
- If $c_i = 1 \Rightarrow$  D→*

} to detect i^{th} photon

a, b, c secret & random

3. Alice sends each photon, Bob tries to detect. Bob creates $d \in \{0,1\}^n$

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

ex: a = 01, b = 11, c = 00
d = 10 or d = 11

4. After Bob has made all measurements
Alice & Bob publicly announce a, c.

Q

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

D) $b_i \cdot d_i = 1$

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

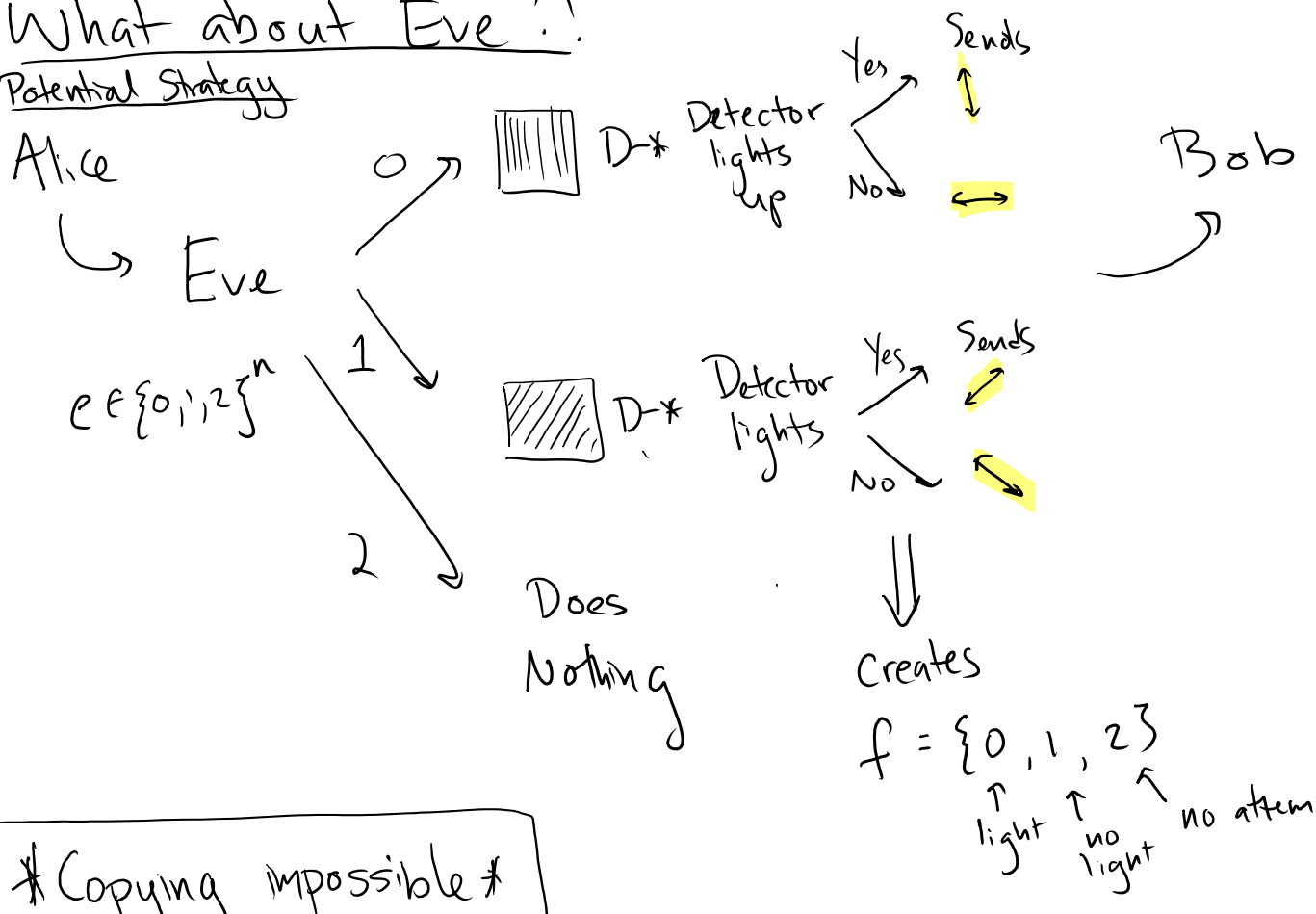
D) b_i and d_i match ½ of time

S. KIMMEL

4. Alice & Bob keep b', d' (bits of b, d where $a_i = c_i$). Start of secret key

What about Eve?!

Potential Strategy



Copying impossible

Group of 3: simulate Alice, Bob, Eve

(Eve happy whenever she chooses correct basis)

S. KIMMEL

5. Alice & Bob make public some random sample of bits of b', d'.

6. Based on fraction that disagree, Alice and Bob do ($b' \neq d'$)

If fraction small:
- Error Correction → $s = \tilde{b} = \tilde{d}$ — Eve still knows a bit about $\tilde{b}$
- Privacy Amplification $s \to s'$ (hash) — Eve doesn't know about s'

If fraction large: ABORT

Q: Go over steps of protocol as a group, explain what each step does.

Q: What is the quantum secret sauce?

A. If Eve wants info about key, she MUST disturb state. Alice & Bob can figure out how much she knows, and correct and amplify their privacy based on this info to ensure their key is private and identical.