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

Exit Tickets

Secret Key Protocol

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 $\underbrace{\text{door}}$ opens

closes ↓ Public key crypto

door ↓ Quantum Crypto Prot.

To do quantum crypto, need quantum particles :

photons ⇒ individual particles of light

☺ Fast

☹ Easily lost

☹ Hard to create + to detect

<u>Polarizer Demo</u>: 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