

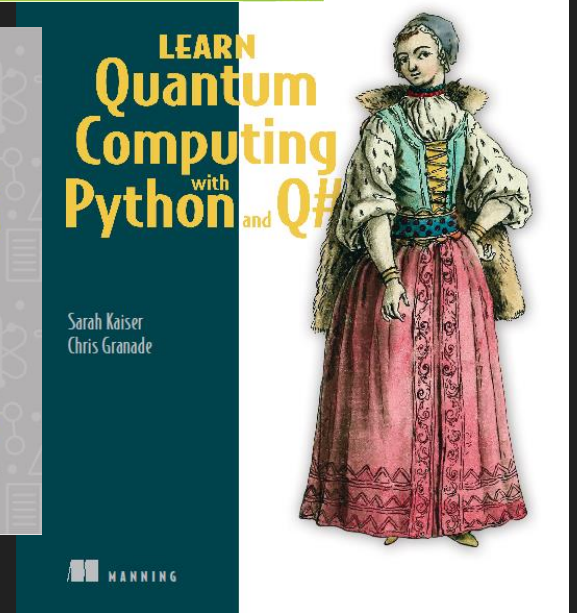
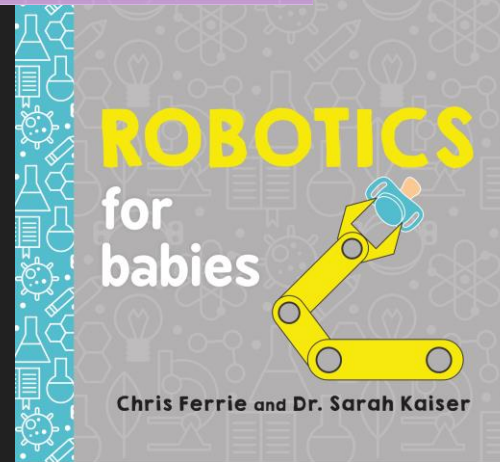
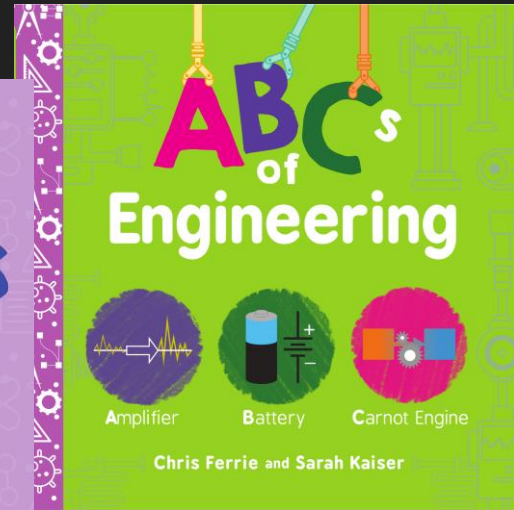
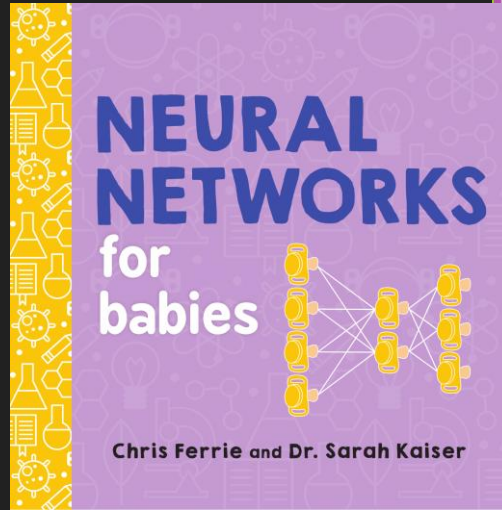


# Hacking Quantum Key Distribution Hardware

or How I Learned to Stop Worrying  
and Burn Things with Lasers

@crazy4pi314

about-me.md



# Quantum Technology

#bitcoin #buzzwords  
#FOMO #Blessed

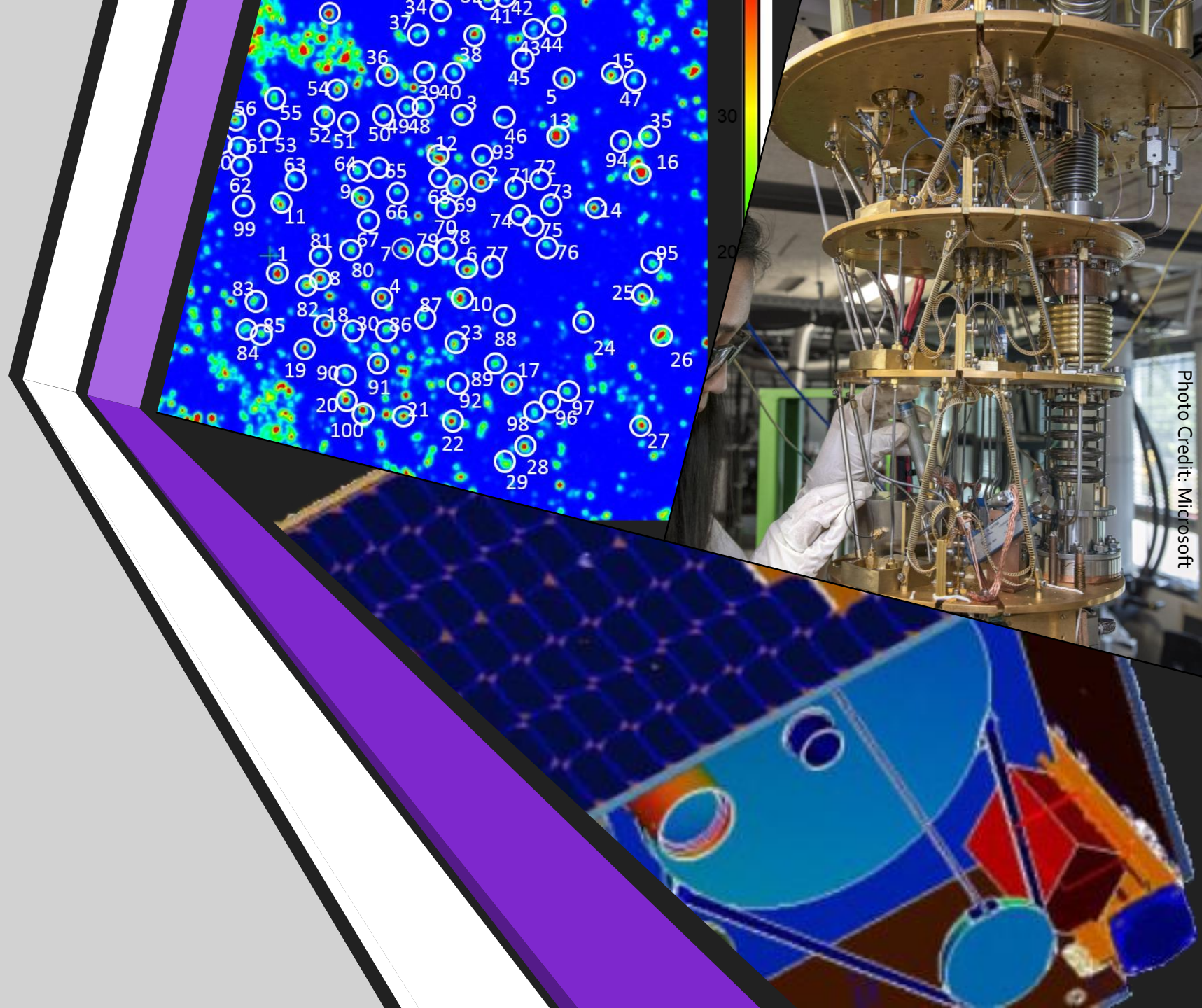


Photo Credit: Microsoft

What can  
quantum tech  
do for  
information  
security?

☹️ Factoring large  
numbers

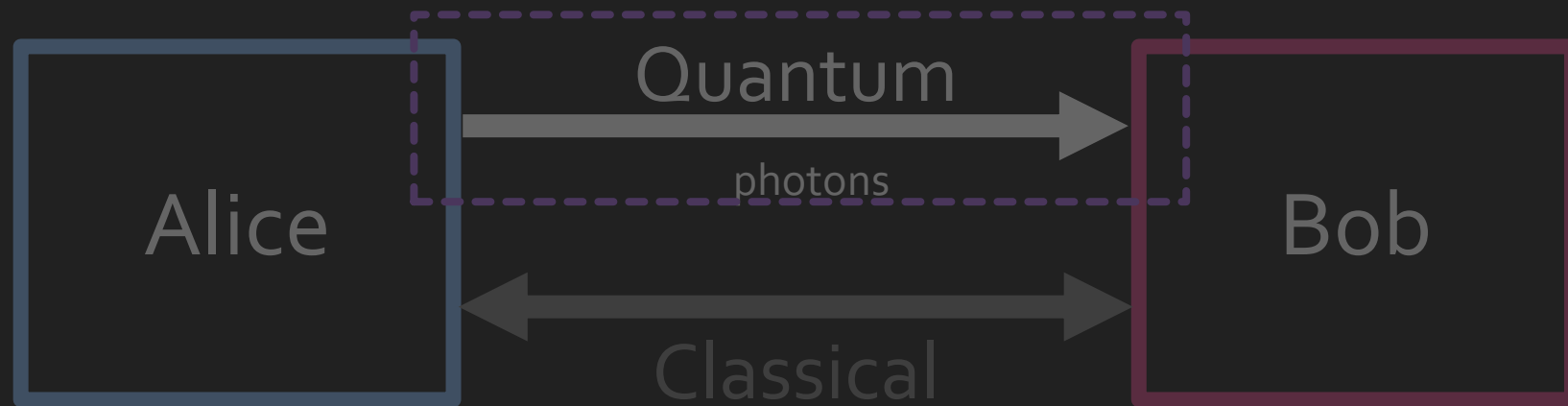
😊 Securely exchanging  
cryptographic keys

# Exchanging quantum keys



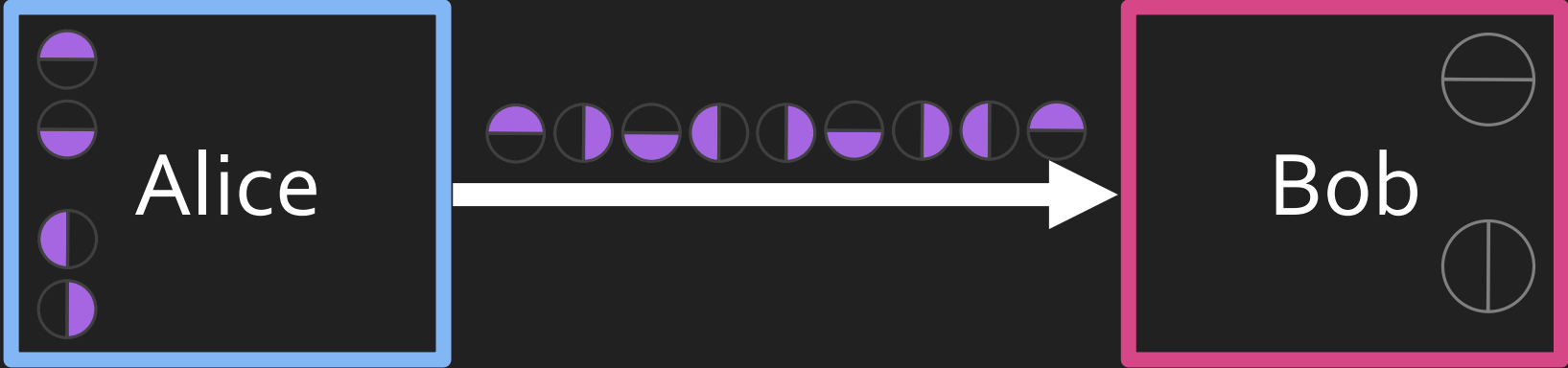
# Quantum Key Distribution (QKD)

- Objective: share a secret key between Alice and Bob



# PROVABLE SECURITY!

# QKD protocol : BB84



Alice sends



Bob measures



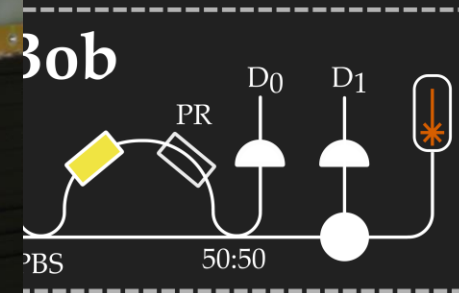
Matches?



# The ID Quantique QKD system



- Variable optical attenuator
- Phase modulator



- Laser diode
- Circulator
- Fiber coupler



A close-up photograph of a person's hand working on a complex electronic circuit board. The board is populated with various components, including integrated circuits, capacitors, and connectors. A prominent feature is a green ribbon cable connected to a multi-pin connector. Several red pushpins are used to hold wires in place. The background is dark and out of focus, suggesting a laboratory or workshop setting. The text "Quantum hacking" is overlaid in white, centered on the right side of the image.

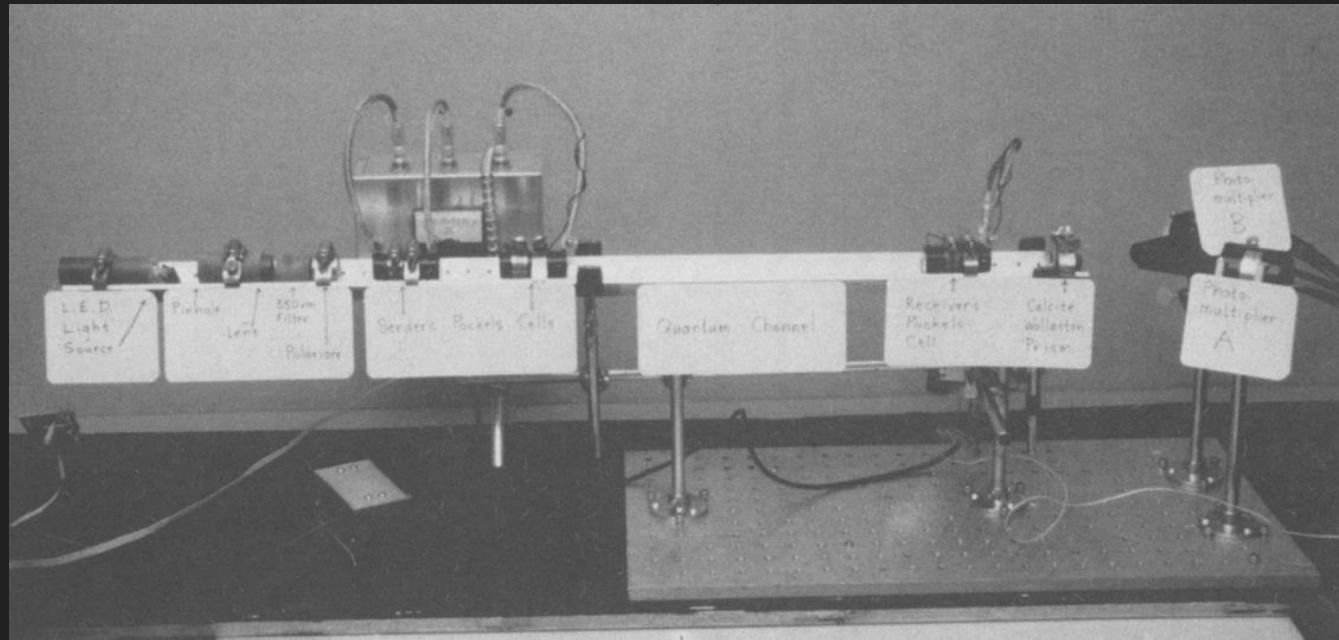
Quantum hacking

Provable security for QKD is...



<https://imgur.com/gallery/OPz1hjm>

# The IBM QKD proof of concept device (~1992)



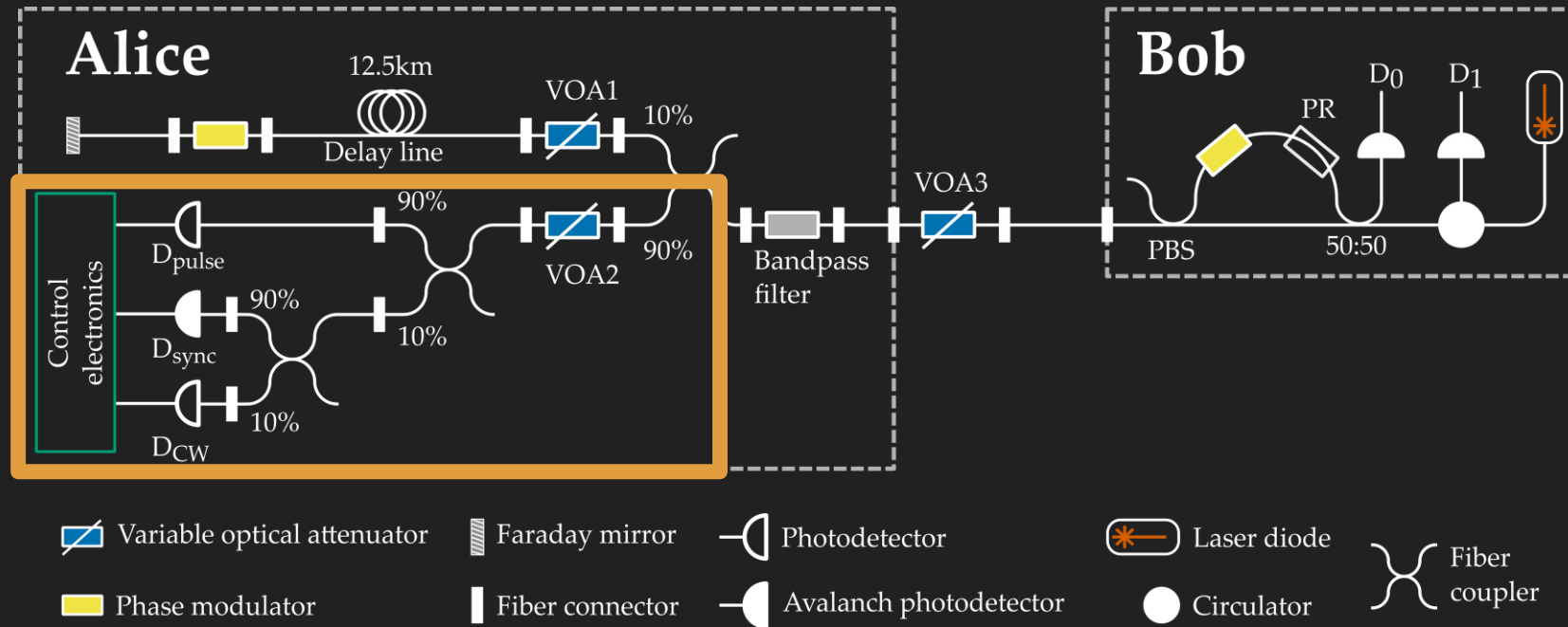
# Ways to break hardware assumptions

Known quantum attacks:

- Timing [doi:10/c97d7r](https://doi.org/10.1007/978-3-642-11221-1_10)
- Detector control [doi:10/d6cgxf](https://doi.org/10.1007/978-3-642-11221-1_11)
- Multi-wavelength [doi:10/fnqkhz](https://doi.org/10.1007/978-3-642-11221-1_12)

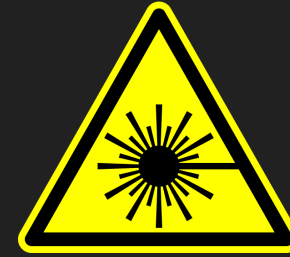


# The ID Quantique QKD system





GET THE LASERS!!!



<http://thirdmonk.net/high-culture/leslie-nielsen-gifs.html>

# Recipe for “disabling” the monitoring diodes

1. Test each optical fiber component to see how much power they can *really* handle
2. Characterize the behavior of the monitoring diodes
3. Determine ideal attack conditions
4. Profit! (try a full attack)

# FIRE THE LASERS



Experiment results

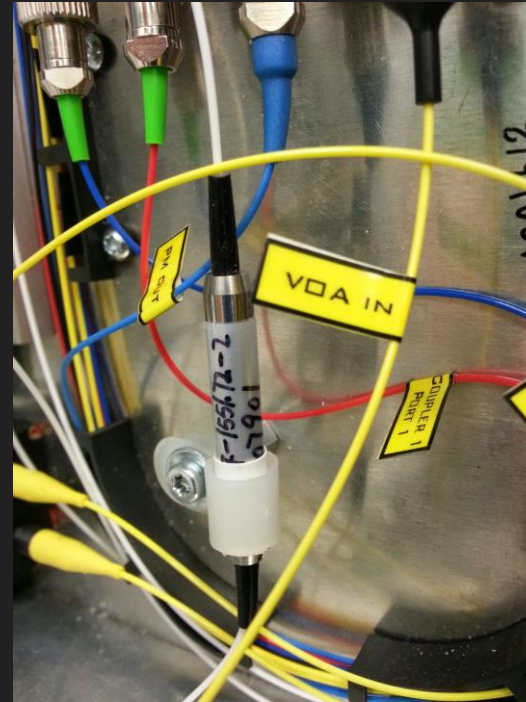


# Step 1. Test each optical fiber component

How much power can they handle?

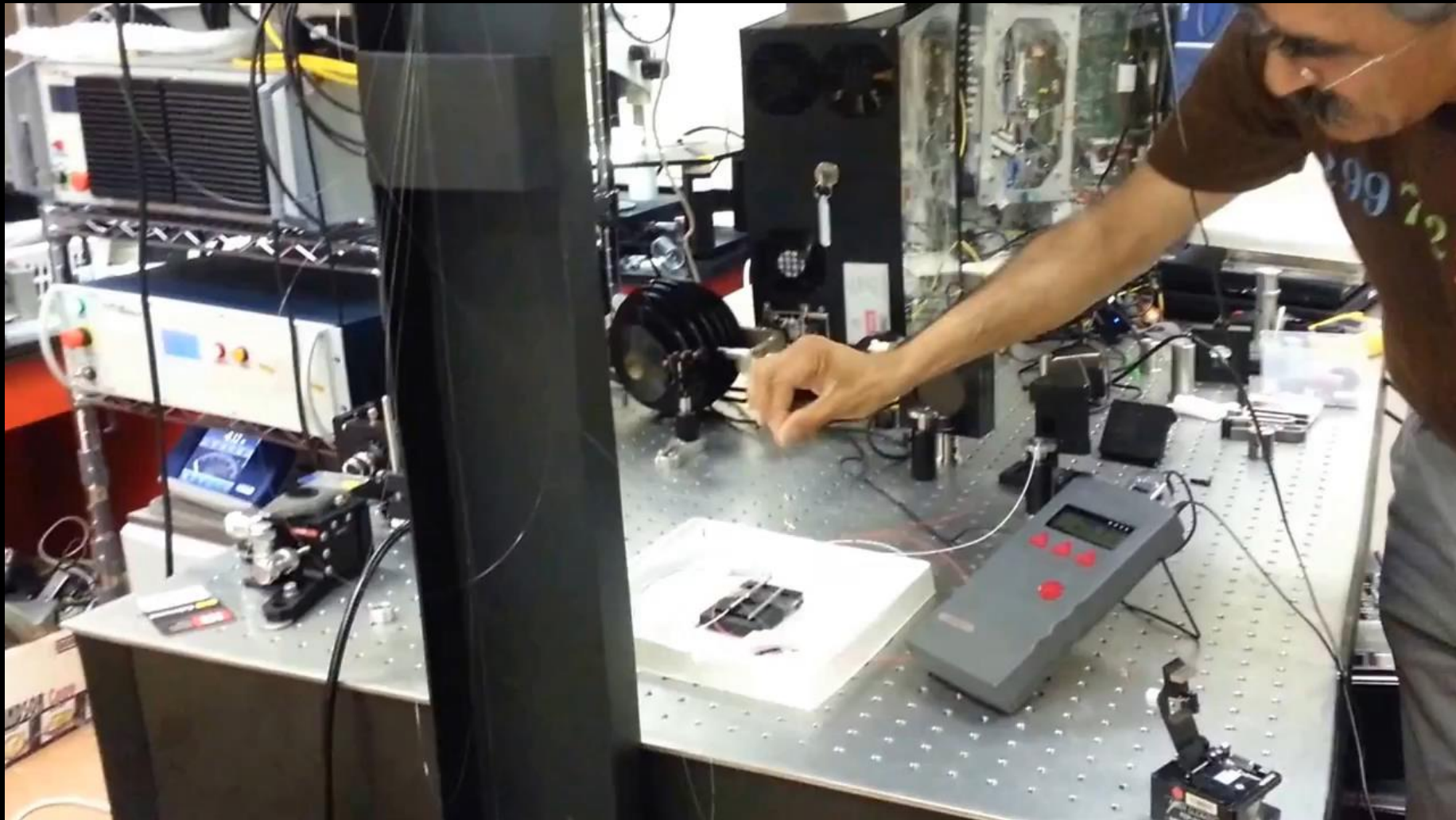
- Fiber + Splices
- Connectors
- Splitters
- Attenuators

Answer: All we could throw at them!  
(~15 W CW)

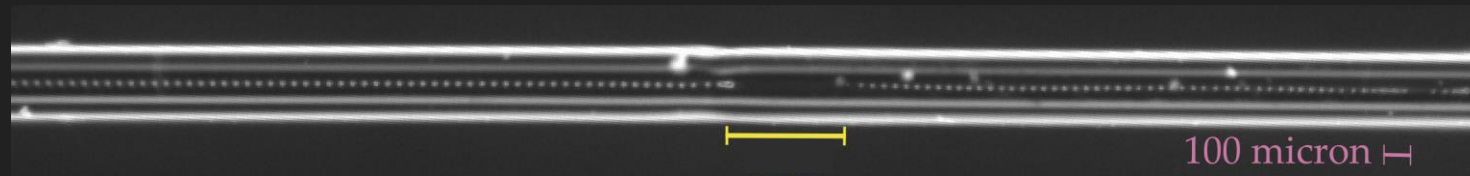


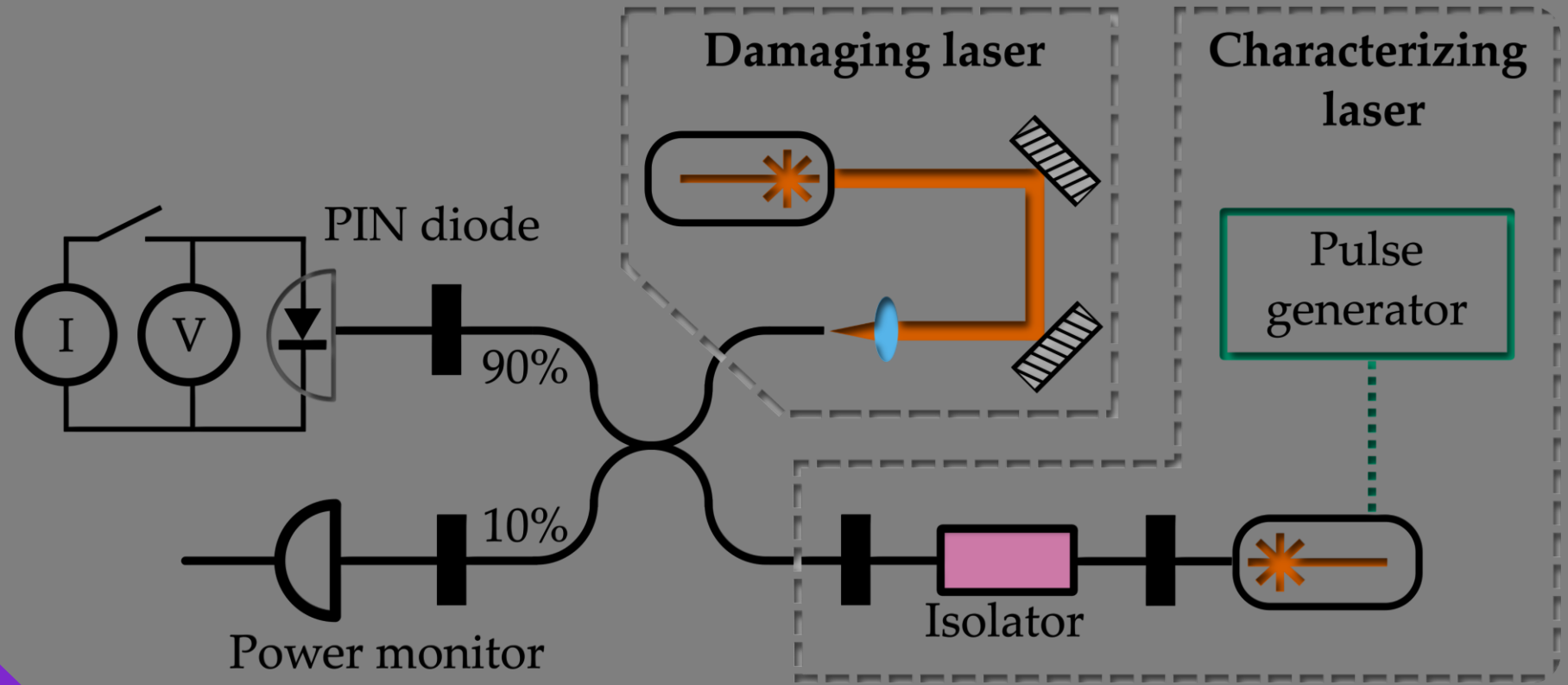
Sooooo much laser power....





# Side quest: Fiber Fusing

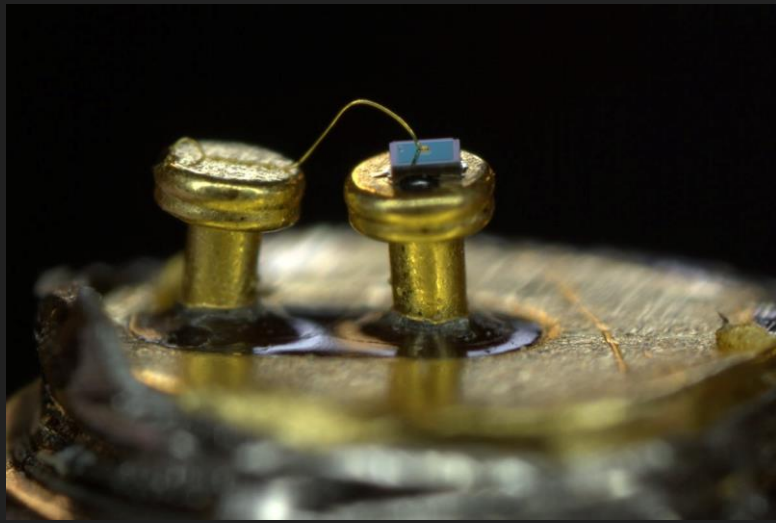




Step 2. Testing the monitoring diodes

# Investigating monitoring photodiode damage

New Detector



Post-attack detector



# SEM images of the photodiode



That will work!

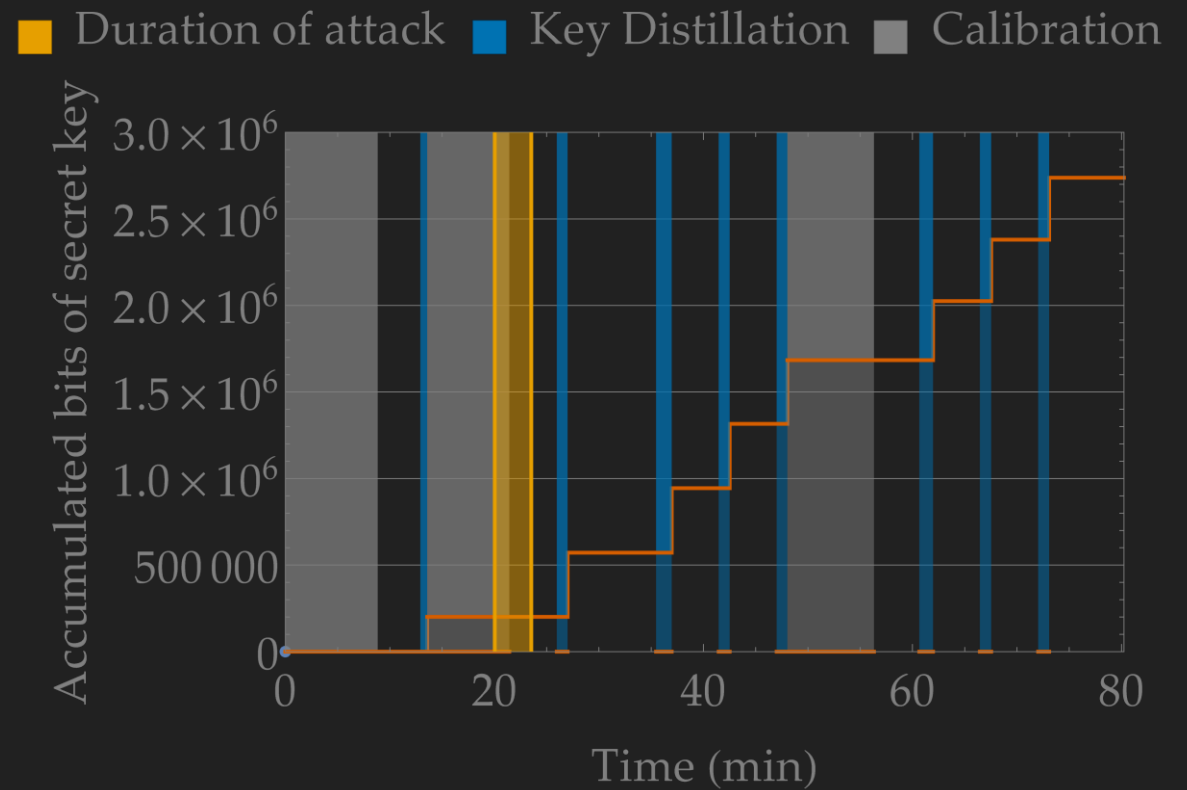
## Step 3. Attack paths found

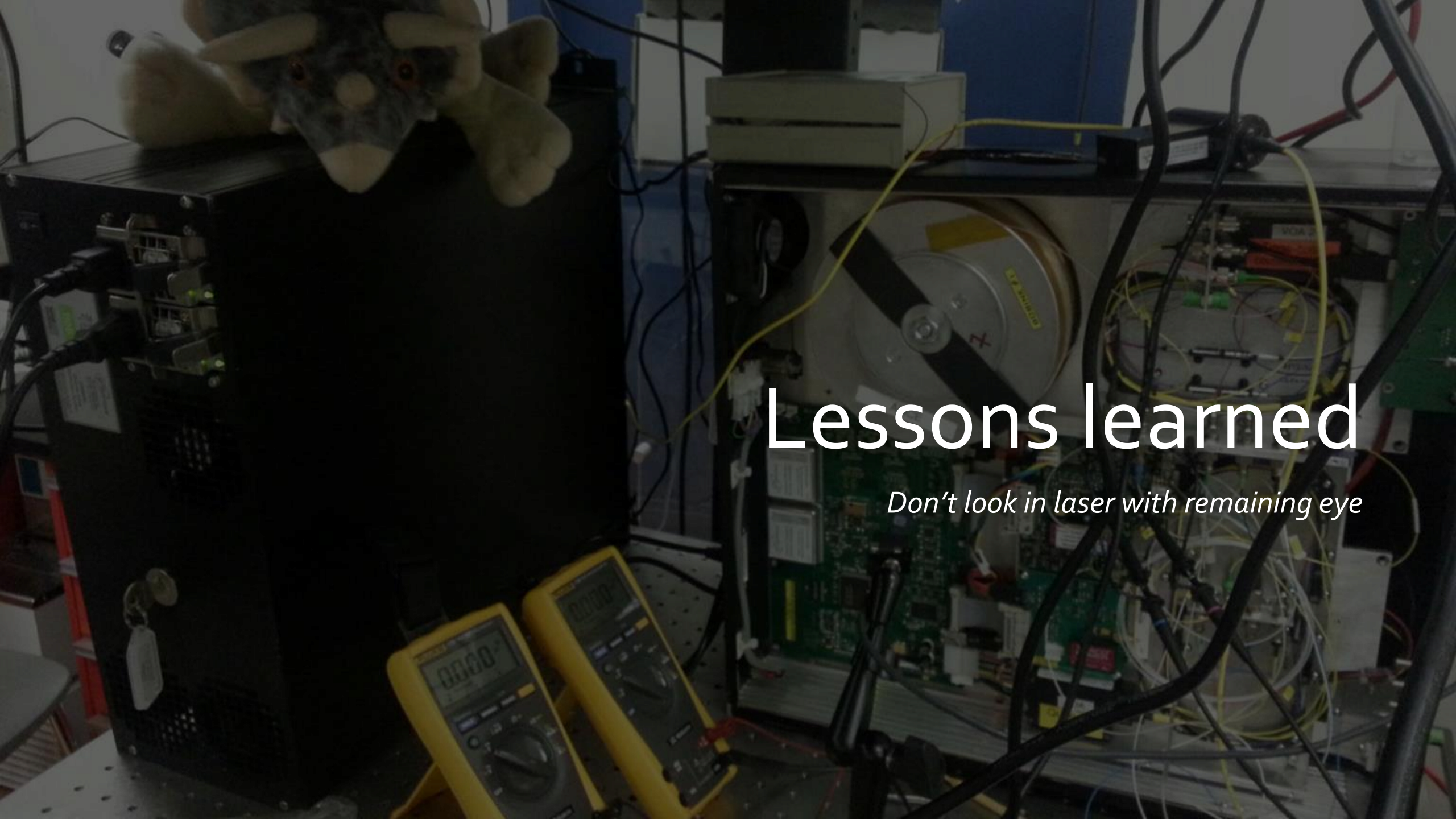
- **Full key:** Melt detector and it fails not in alarm mode (small but finite chance)
- **Partial key:** Decrease detector efficiency by 20-40%, which enables other attacks



# Step 4. Attack demo!

Full key attack on running system





# Lessons learned

*Don't look in laser with remaining eye*

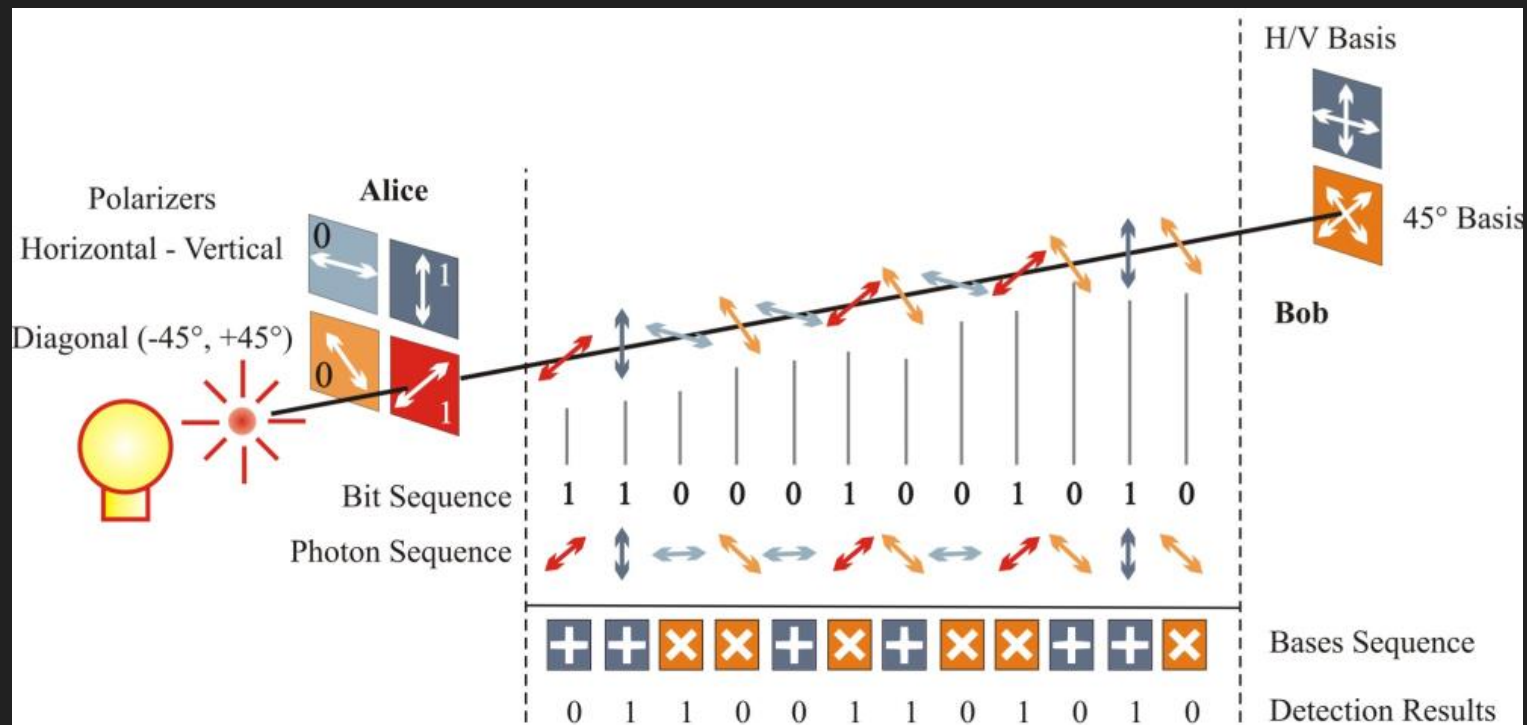
# I Learned to Stop Worrying and Burn Things with Lasers ♥

- Brute force sometimes is the best force
- Physical side channels can compromise even the best security
- Quantum hardware and software needs existing expertise!

Want to learn more about quantum tech or QKD?  
Find me on twitter @crazy4pi314



# BB84 protocol: quantum phase



# QKD protocol : BB84

