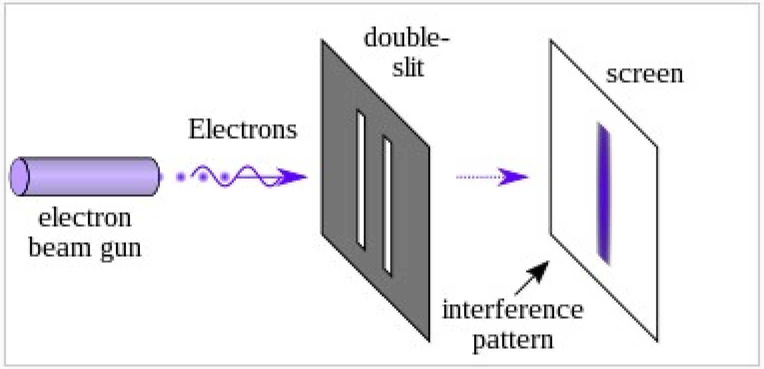
# Brief overview of post-quantum cryptography
CSE 468 Fall 2023

jedimaestro@asu.edu

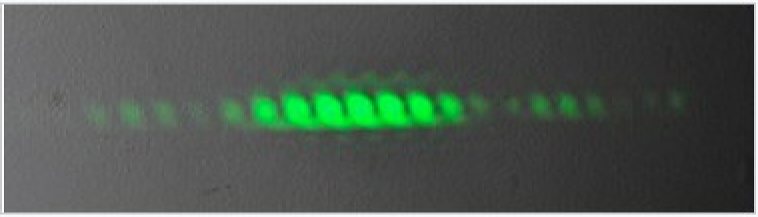
# To prepare for this lecture…

- https://www.youtube.com/watch?v=_C5dkUiiQnw
- https://www.youtube.com/watch?v=QDdOoYdb748
- https://www.youtube.com/watch?v=K026C5YaB3A

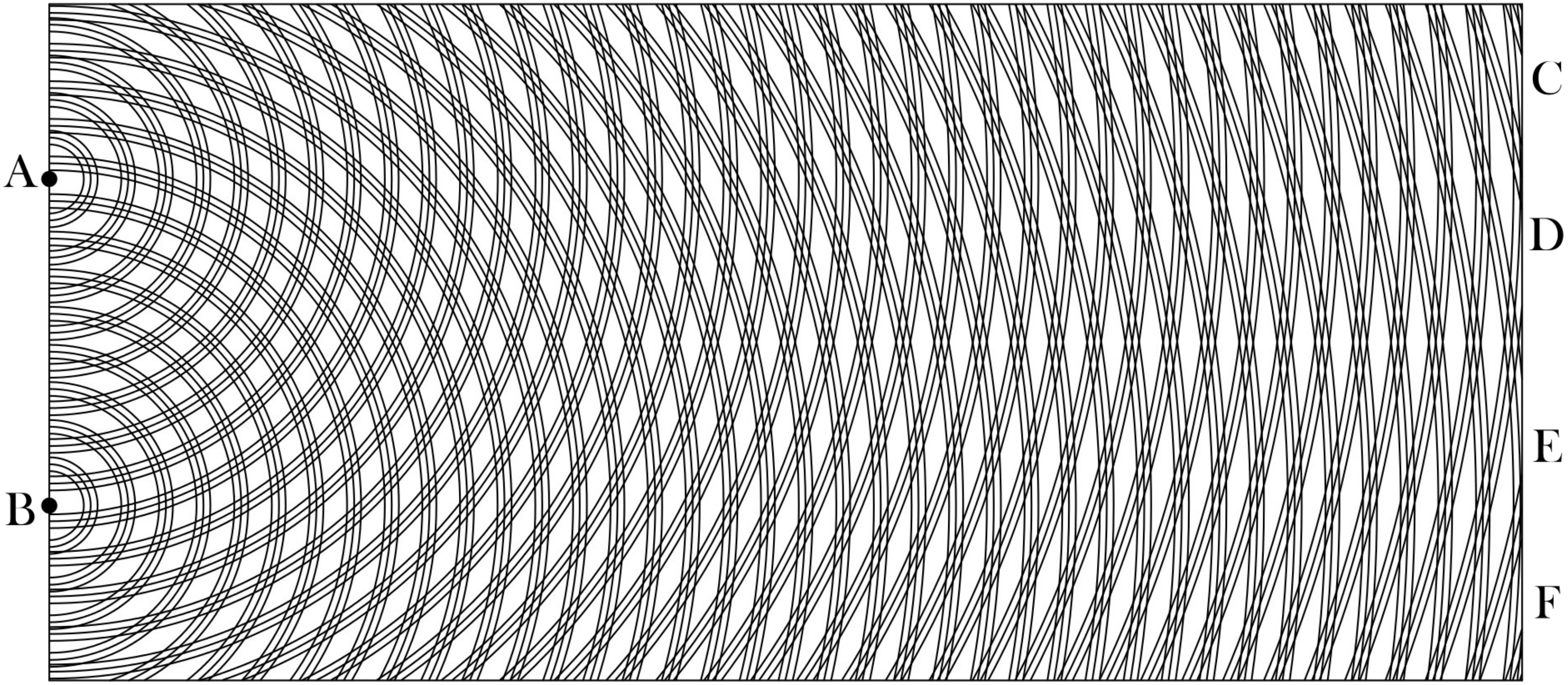
https://en.wikipedia.org/wiki/Double-slit_experiment



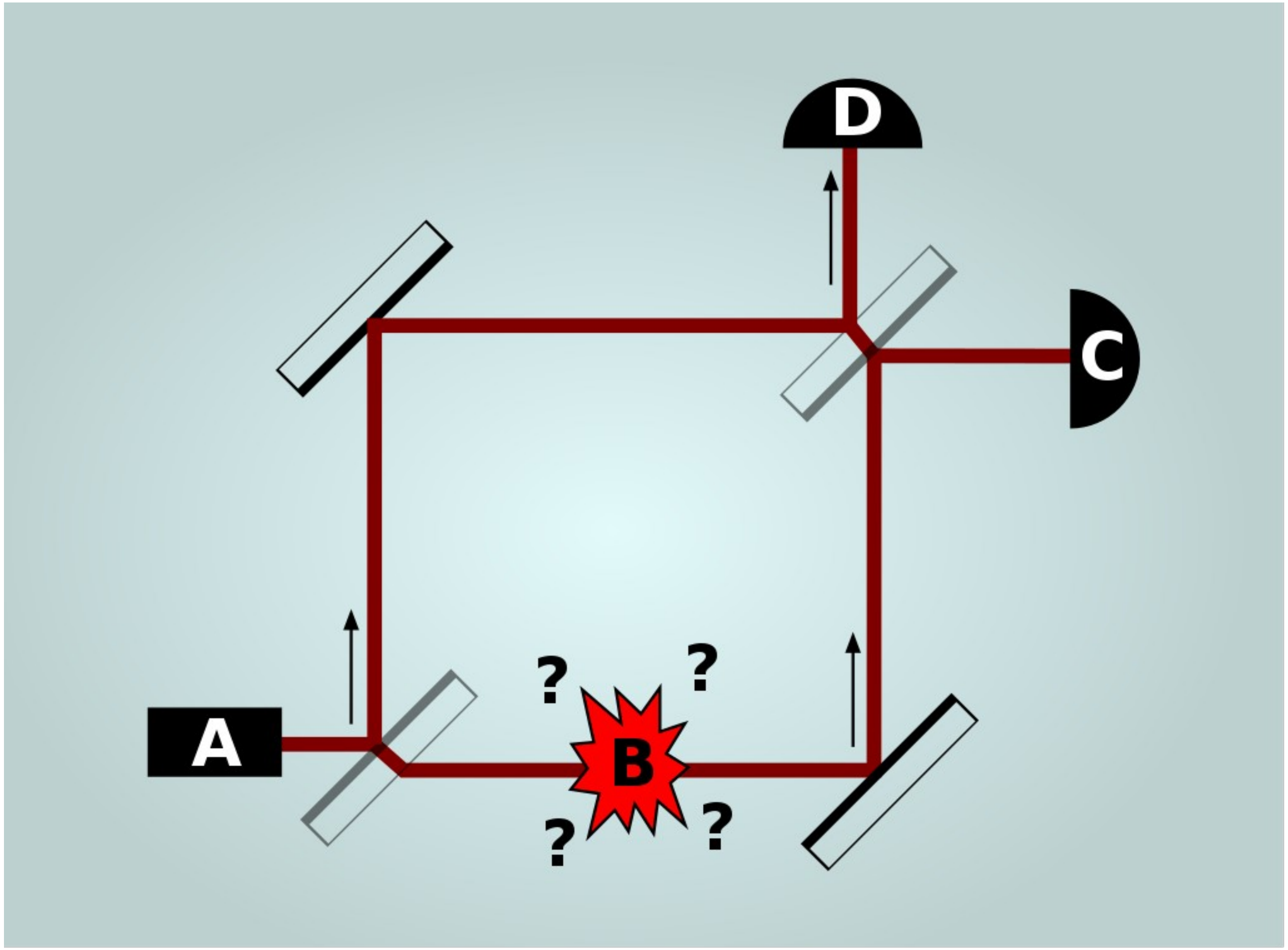

Photons or matter (like electrons) produce an interference pattern when two slits are used



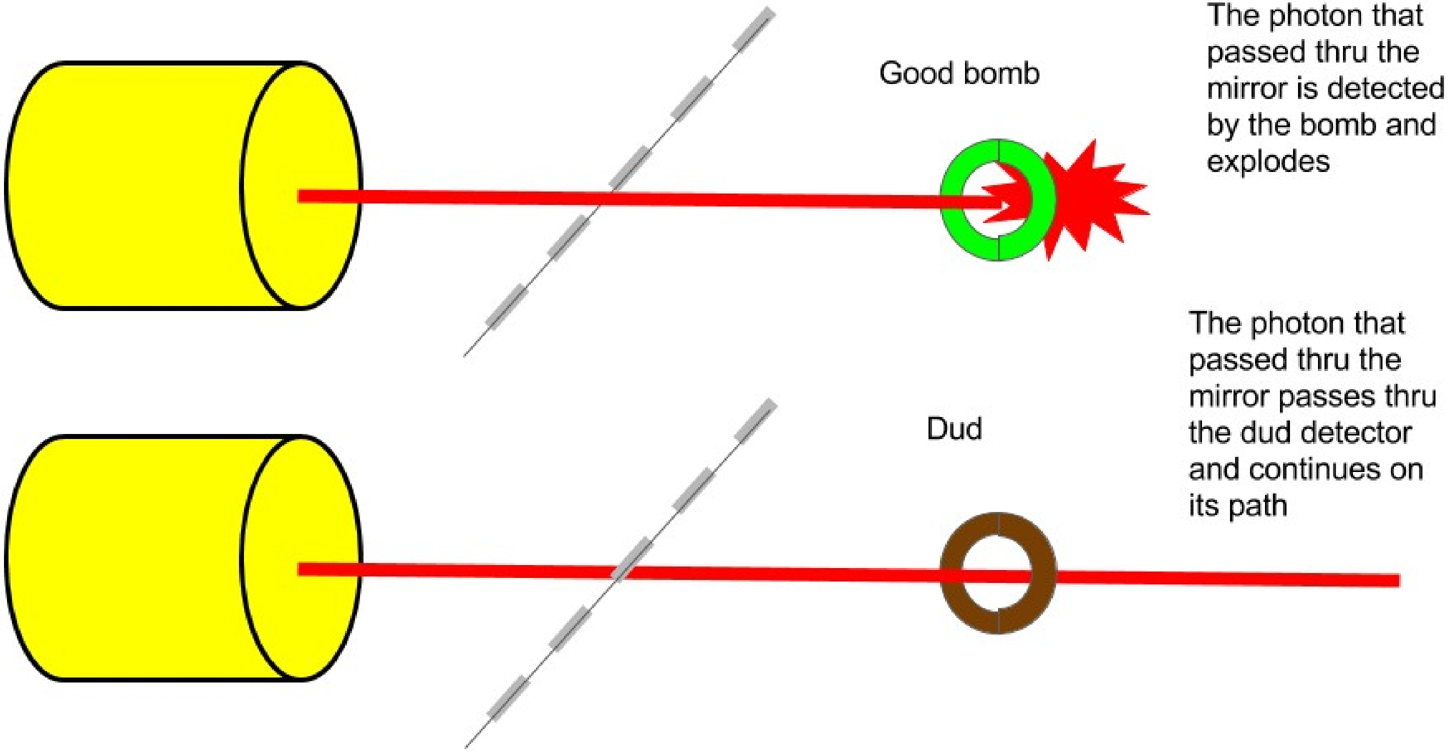
Light from a green laser passing through two slits 0.4mm wide and 0.1mm apart https://en.wikipedia.org/wiki/Double-slit_experiment



https://en.wikipedia.org/wiki/Elitzur%E2%80%93Vaidman_bomb_tester

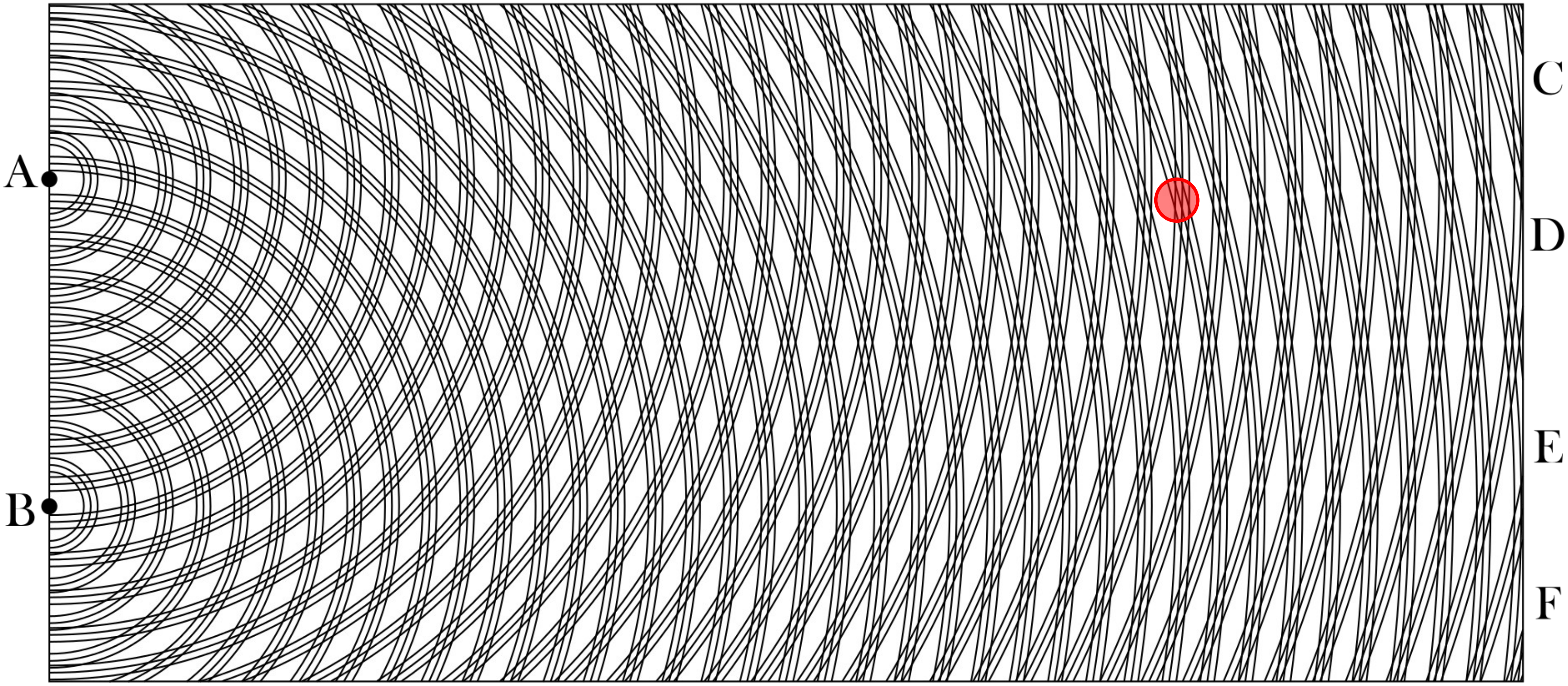


# Bomb is either live or a dud

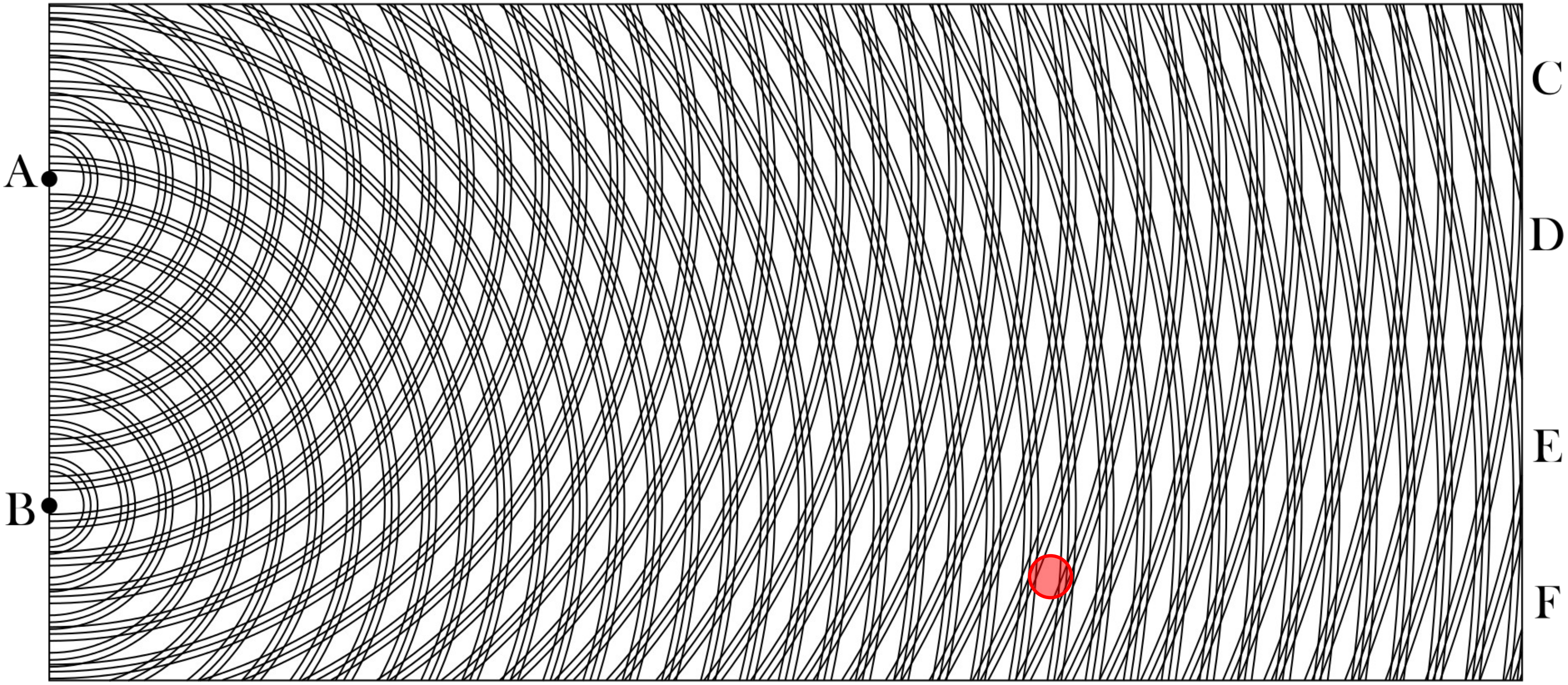


“Due to the way in which the interferometer is constructed, a photon going through the second mirror from the lower path towards detector D will have a phase shift of half a wavelength compared to a photon being reflected from the upper path towards that same detector...”

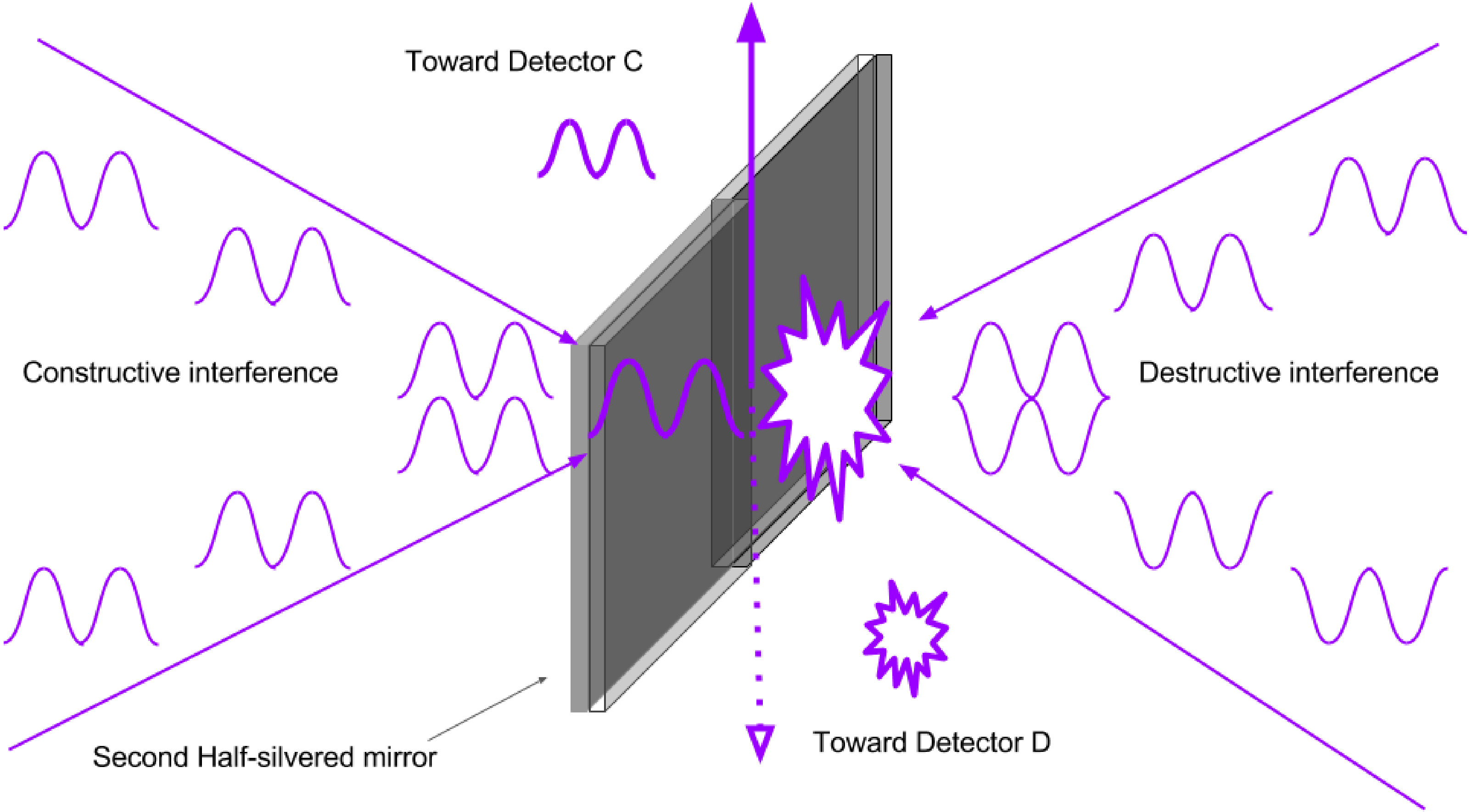
Put C, *e.g.*, here...



# Put D, *e.g.*, here...



# If both waves make it to the end (dud!)...



We will never detect a photon at D if the bomb is a dud.

(*I.e.*, if we detect a photon at D then the bomb is not a dud.)

# Bomb is a dud

- Experiment will keep showing a photon detected at C
- Keep repeating until we’re as sure as we want to be that the bomb is in fact a dud

# Bomb is live

- 50% chance photon takes the lower path
  - Boom!
- 50% chance the photon takes the upper path
  - 50% chance (25% conditional) that the single photon (no longer a wave) goes to detector C
    - Have to repeat
  - 50% chance (25% conditional) that the single photon (no longer a wave) goes to detector D

# Bomb is live (keep repeating)

- 2/3rds chance we blow ourselves up
- 1/3rd chance we eventually detect a photon a D
  - No boom, but we’re certain the bomb is live

# WTF?

- With a decent probability (1/3), we learn information about something that *might have happened but didn't*.
- Interaction free experiment
  - Possible in classical physics, *e.g.*, I give you two envelopes and tell you a letter is in one and the other is empty, if you open one you know something about the other.
  - At quantum scales the letter is in a superposition of both envelopes until you observe it
    - These probabilities can be entangled

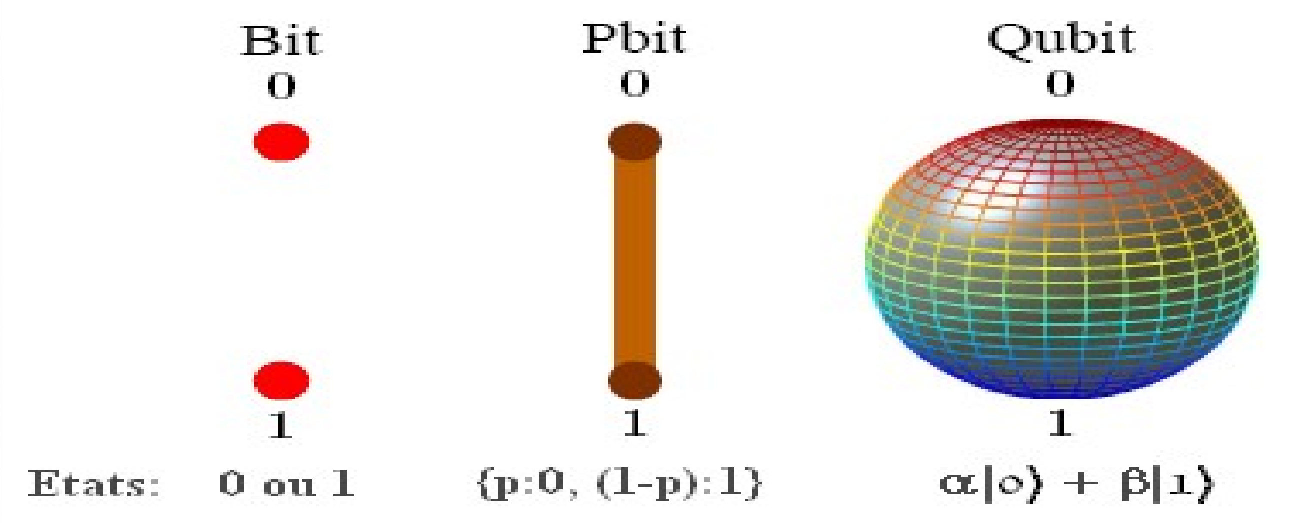
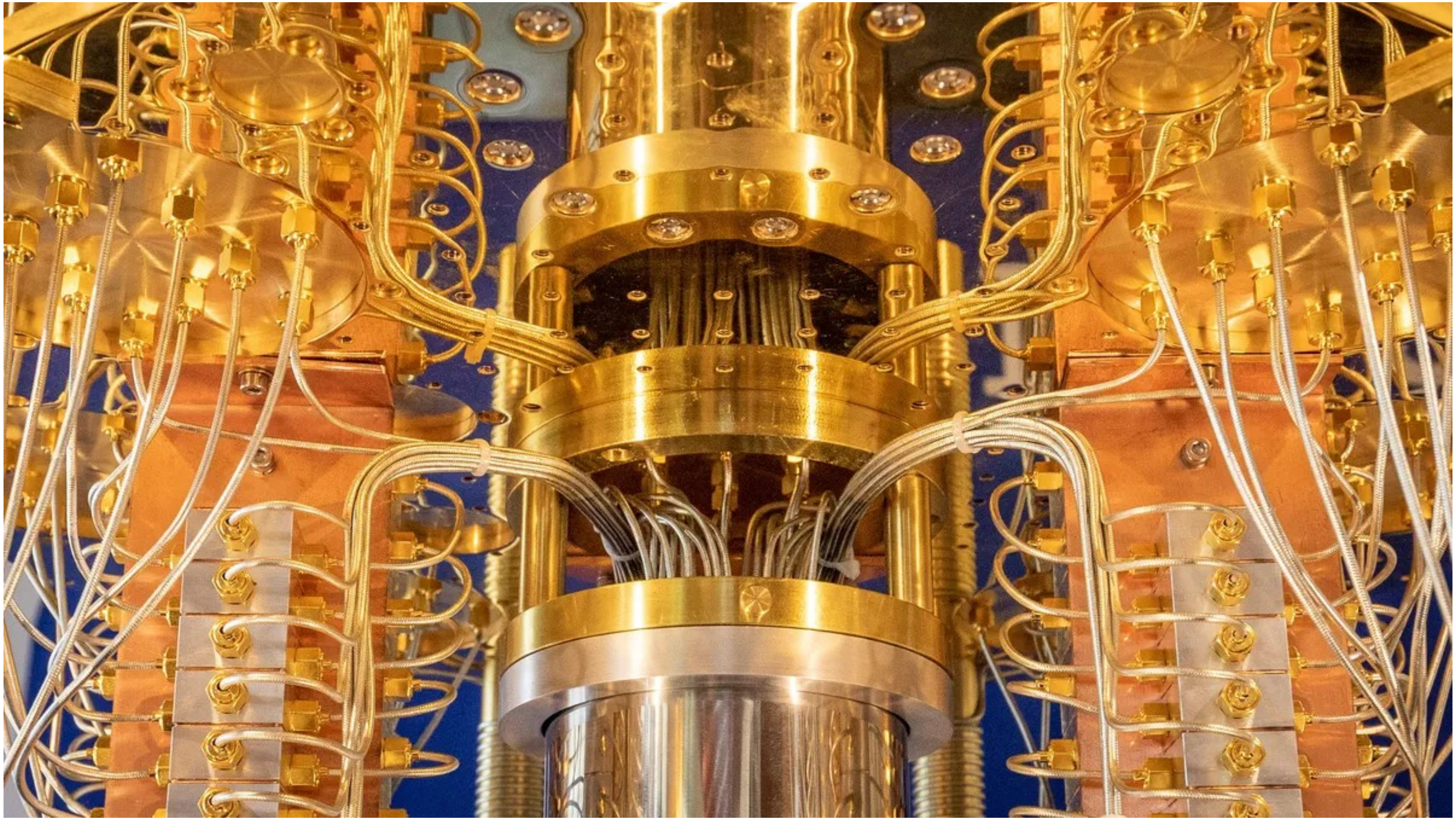



Image taken from http://filipchsqroom.blogspot.com/

# Superposition is not enough

- Qubits have to be mutually entangled in very specific ways to implement useful quantum computations
  - Quantum decoherence is a major challenge

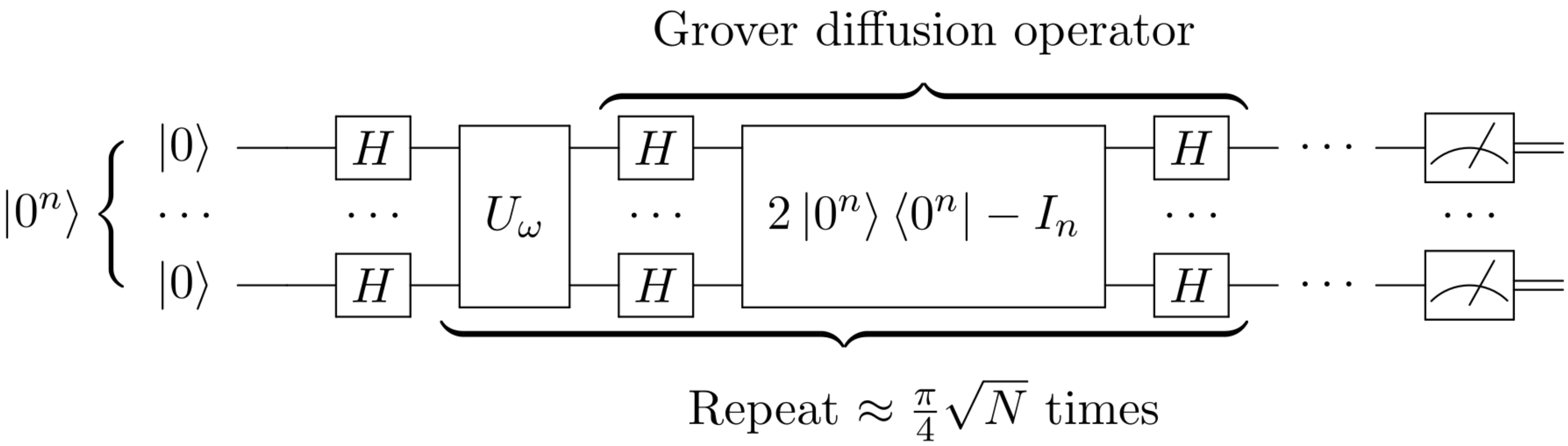


https://www.cnet.com/tech/computing/quantum-computer-makers-like-their-odds-for-big-progress-soon/

# What we need for the Internet to work...

- Symmetric
  - Encryption
  - Authentication
  - Secure hashes
  - Others?
- Asymmetric
  - Encryption
  - Non-repudiability (signatures)
  - Key exchange
  - Others? (*e.g.*, homomorphic)

# Grover’s algorithm




https://en.wikipedia.org/wiki/Grover%27s_algorithm#/media/File:Grover's_algorithm_circuit.svg

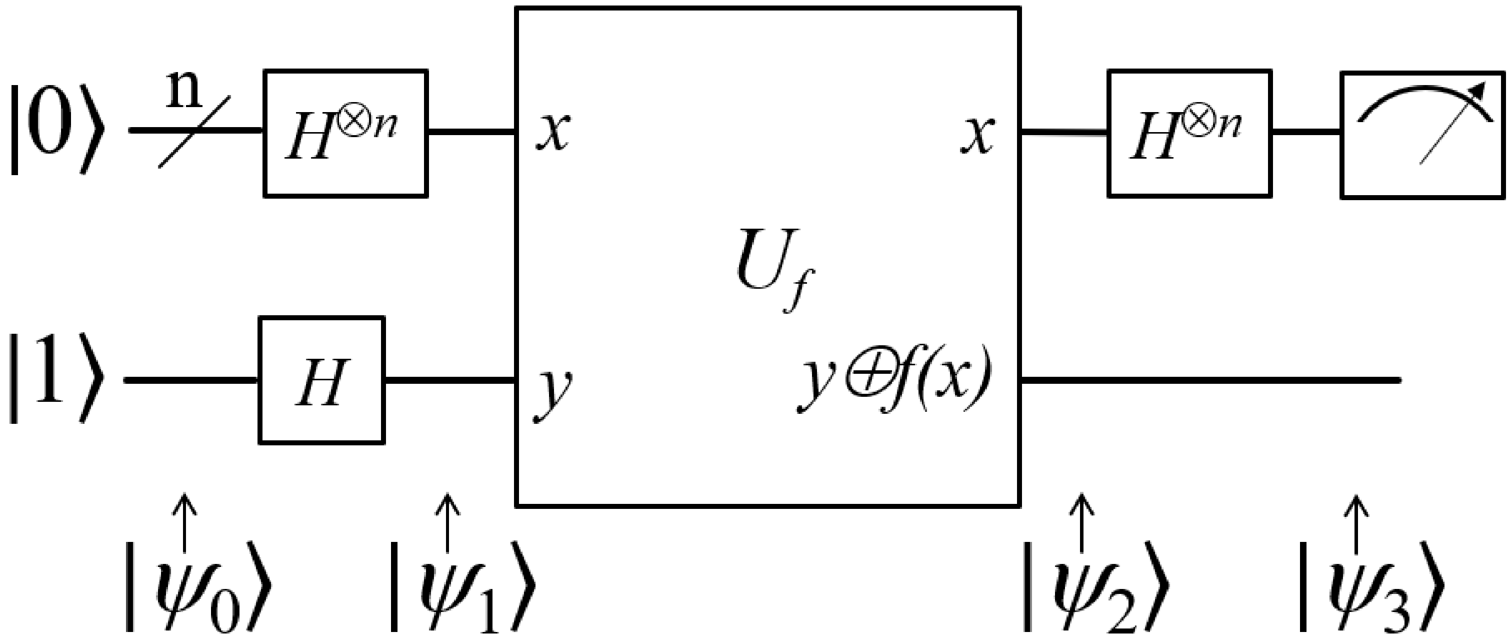
# Symmetric crypto

- Double the key size
  - $\text{sqrt}(2^{2n}) = 2^n$
  - $\text{sqrt}(2^{256}) = 2^{128}$

# Asymmetric Crypto

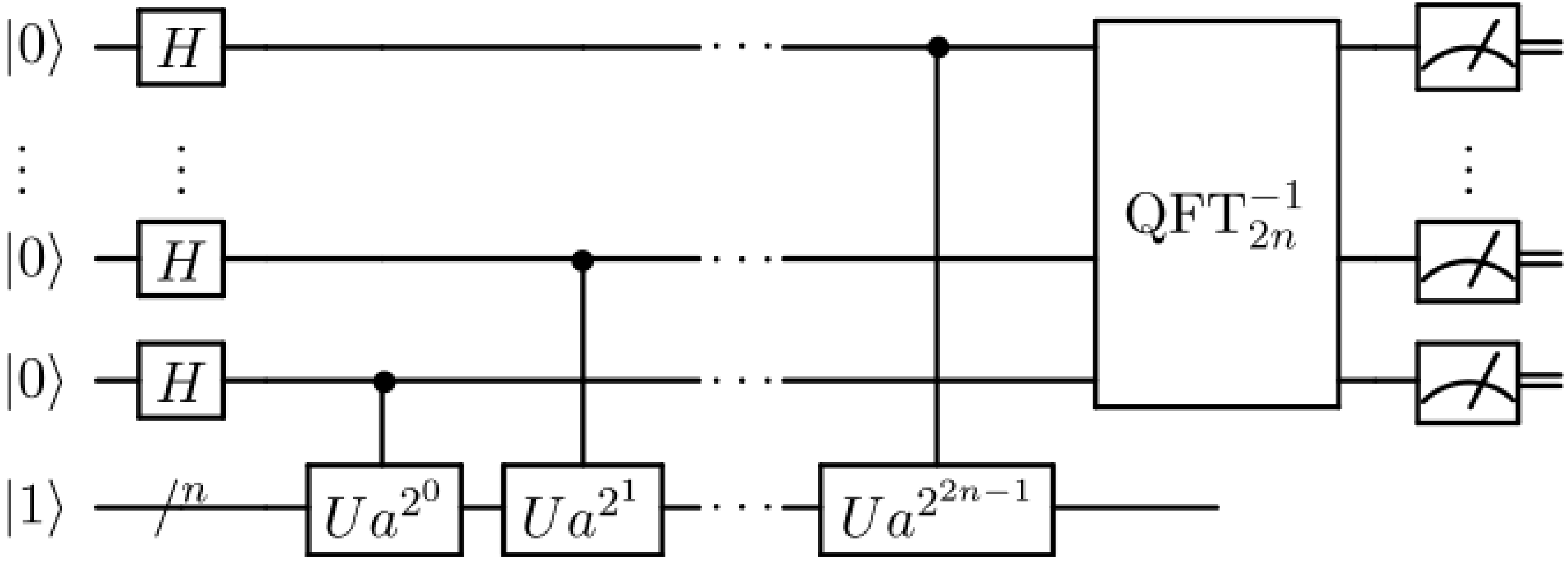
- Quantum computers seem to be good at the same kinds of things that make good trapdoor functions for asymmetric crypto (factorization, discrete log, *etc.*)
  - But not everything
    - Older schemes (*e.g.*, Merkle’s signature scheme)
    - Newer schemes (*e.g.*, lattice-based)

# Deutsh-Jozsa algorithm




https://en.wikipedia.org/wiki/Deutsch%E2%80%93Jozsa_algorithm#/media/File:Deutsch-Jozsa-algorithm-quantum-circuit.png

# Shor's algorithm




https://en.wikipedia.org/wiki/Shor%27s_algorithm#/media/File:Shor's_algorithm.svg

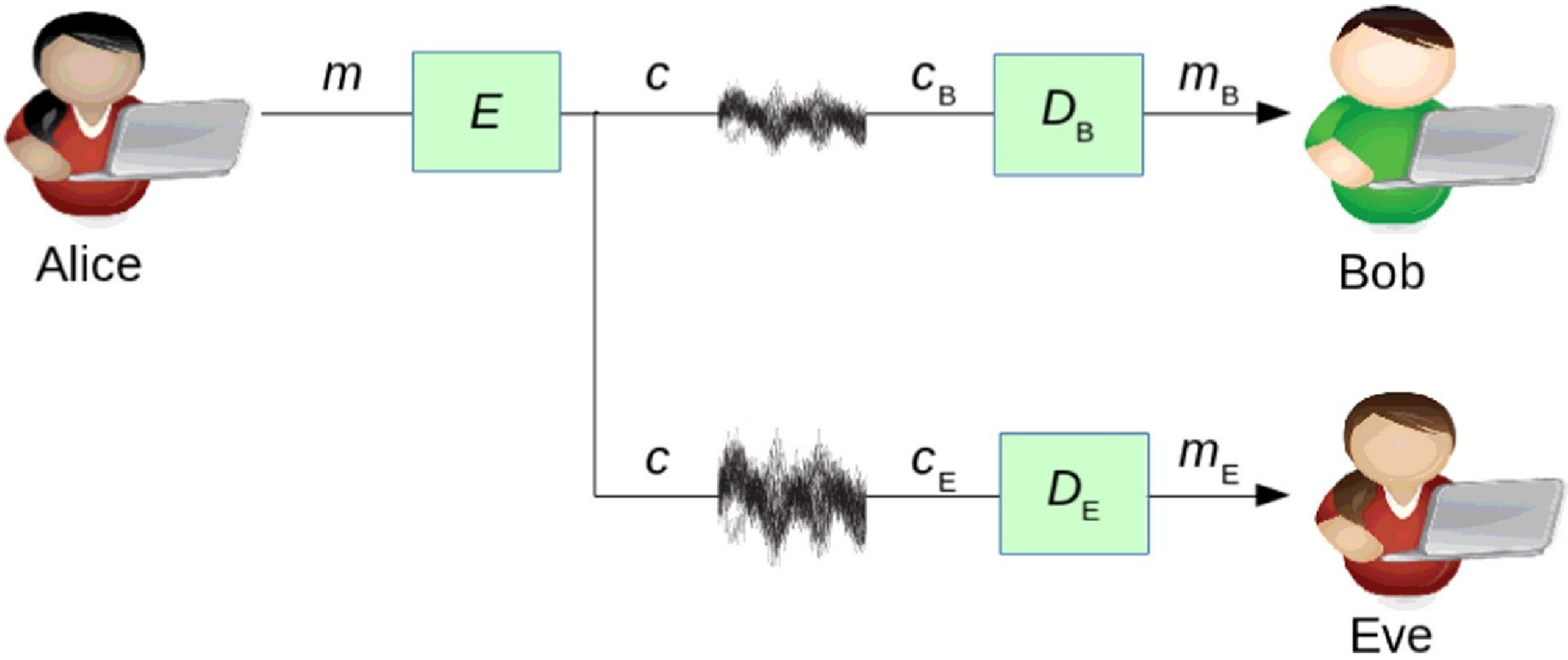
RSA, DH, ECDH, DSA, *etc.* all broken. Need something else instead...

# Lamport signature (1979)

- How to sign a 256-bit message digest...
  - Generate 512 random 256-bit integers (256 pairs of them)
    - Private key
  - For all 512 generate corresponding hash
    - Public key (single use)
  - When you want to sign something, reveal one unhashed private version per pair for corresponding to the bit being 0 or 1 (*i.e.*, the first of the pair for 0, the other for 1)
    - 64 Kbits

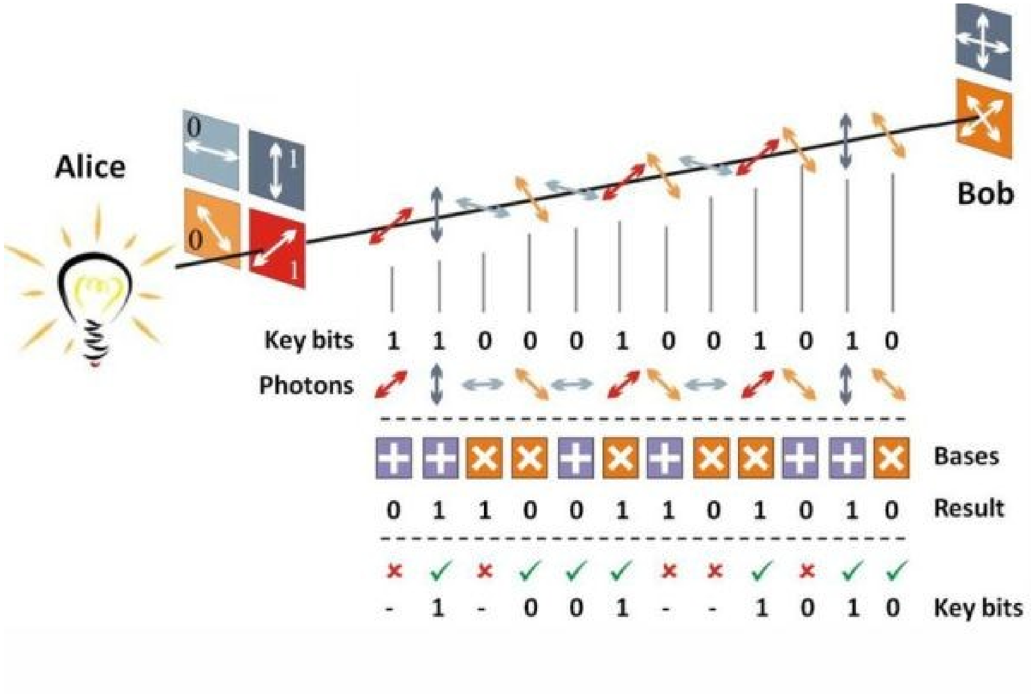
https://en.wikipedia.org/wiki/Lamport_signature

# Wiretap channel




https://www.sciencedirect.com/science/article/pii/S1389128616302146

# Quantum Key Distribution



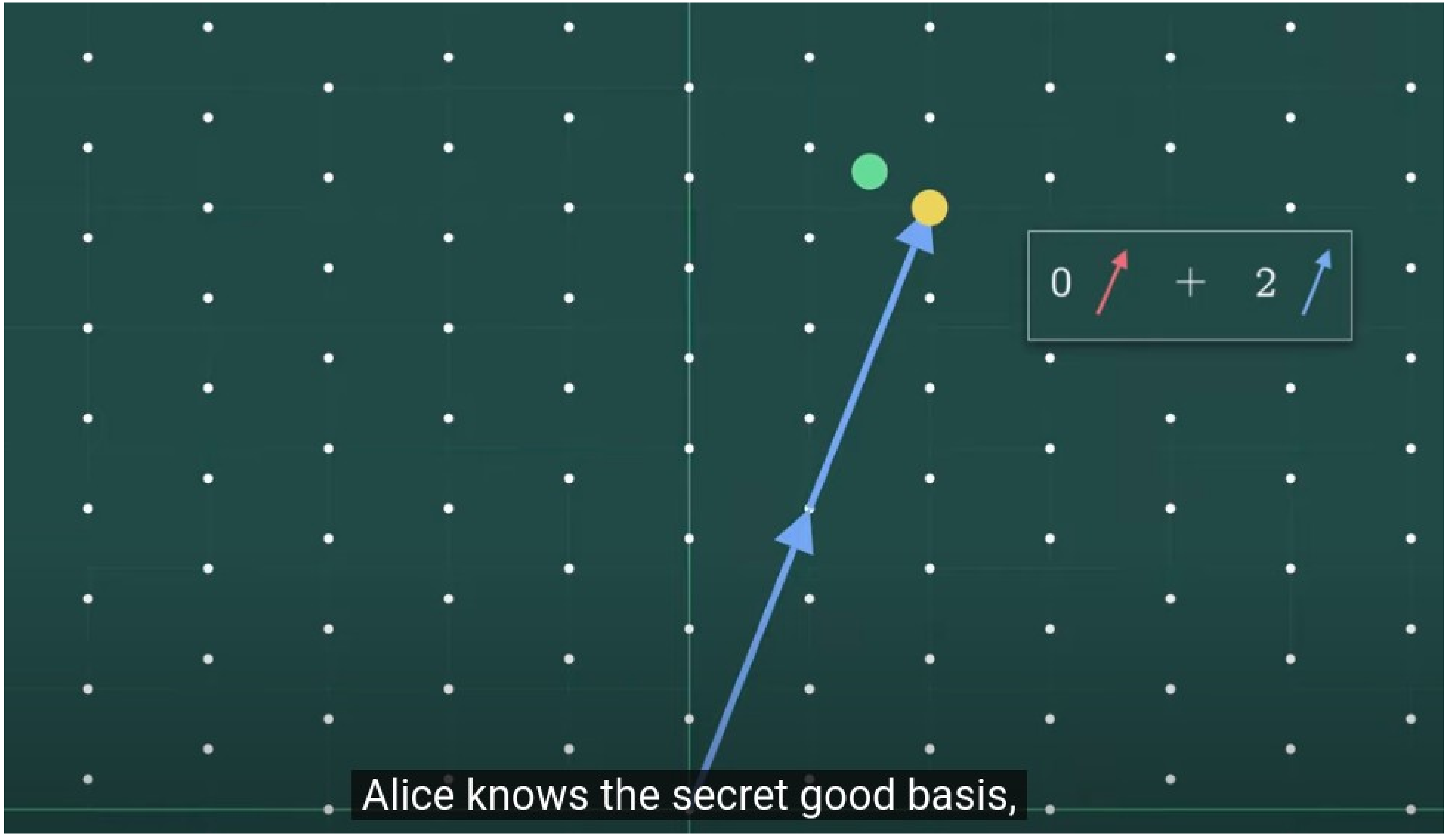

https://imrmedia.in/quantum-key-distribution-test-successfully-demonstrated/

# QKD *vs.* Quantum-resistant

- QKD uses quantum physics
- Quantum-resistant crypto is performed on classical computers using one-way trapdoor functions that we believe will resist cryptanalysis using quantum computers

https://www.youtube.com/watch?v=QDdOoYdb748

Lattice-based cryptography: The tricky math of dots



# Themes

- In schemes based on information theory or physics the eavesdropper has some noise or uncertainty the receiver doesn’t have
  - We see this in post-quantum crypto (*e.g.*, learning with errors)
- Quantum computers aren’t necessarily faster at everything
  - There’s usually a “trick at the end” where all the quantum information gets destroyed but the classical information measured still means something

# Why do we care?

- Even schemes with perfect forward secrecy aren’t secure against a quantum computer if they’re not quantum resistant
  - Can be recorded now, broken later
- TLS, HTTPS certificates, WPA2, WPA3, 4G, 5G, WhatsApp, *etc.* are currently not “future proofed” against quantum computers
  - Signal is, but only very recently