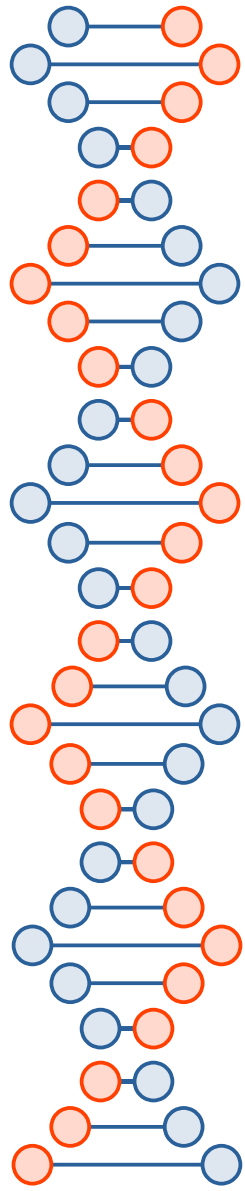


Brief overview of quantum computers, post-quantum cryptography

CSE 468 Fall 2024
jedimaestro@asu.edu



Open question: Does the universe permit private communications in the presence of an eavesdropper using only classical computation?

(Network security is profoundly affected by the answer, *e.g.*, TLS and SSH.)



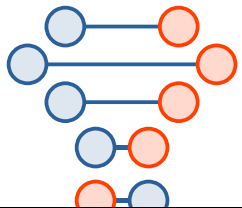
Open question: Does the universe permit ~~private communications~~ *non-repudiability* in the presence of an eavesdropper using only classical computation?

(Network security is profoundly affected by the answer, *e.g.*, TLS and SSH.)



Some videos...

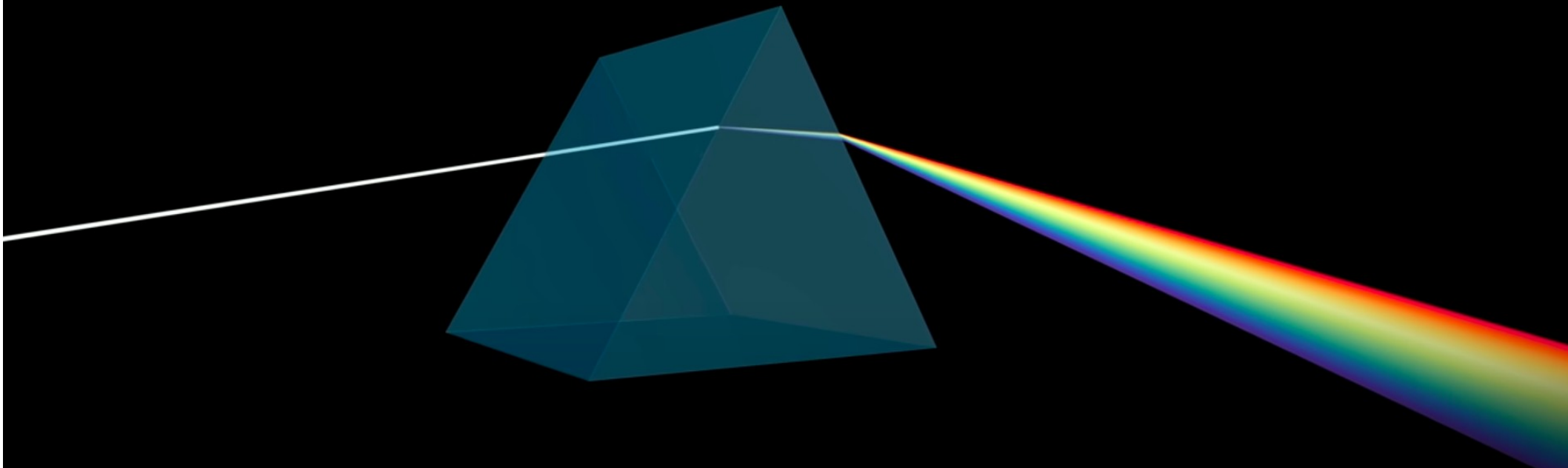
- https://www.youtube.com/watch?v=_C5dkUiiQnw
- <https://www.youtube.com/watch?v=QDdOoYdb748>
- <https://www.youtube.com/watch?v=K026C5YaB3A>
- <https://www.youtube.com/watch?v=KTzGBJPuJwM>



3brown1blue on YouTube...

But why would light "slow down"? | Optics puzzles 3

To exit full screen, press Esc



Why this?

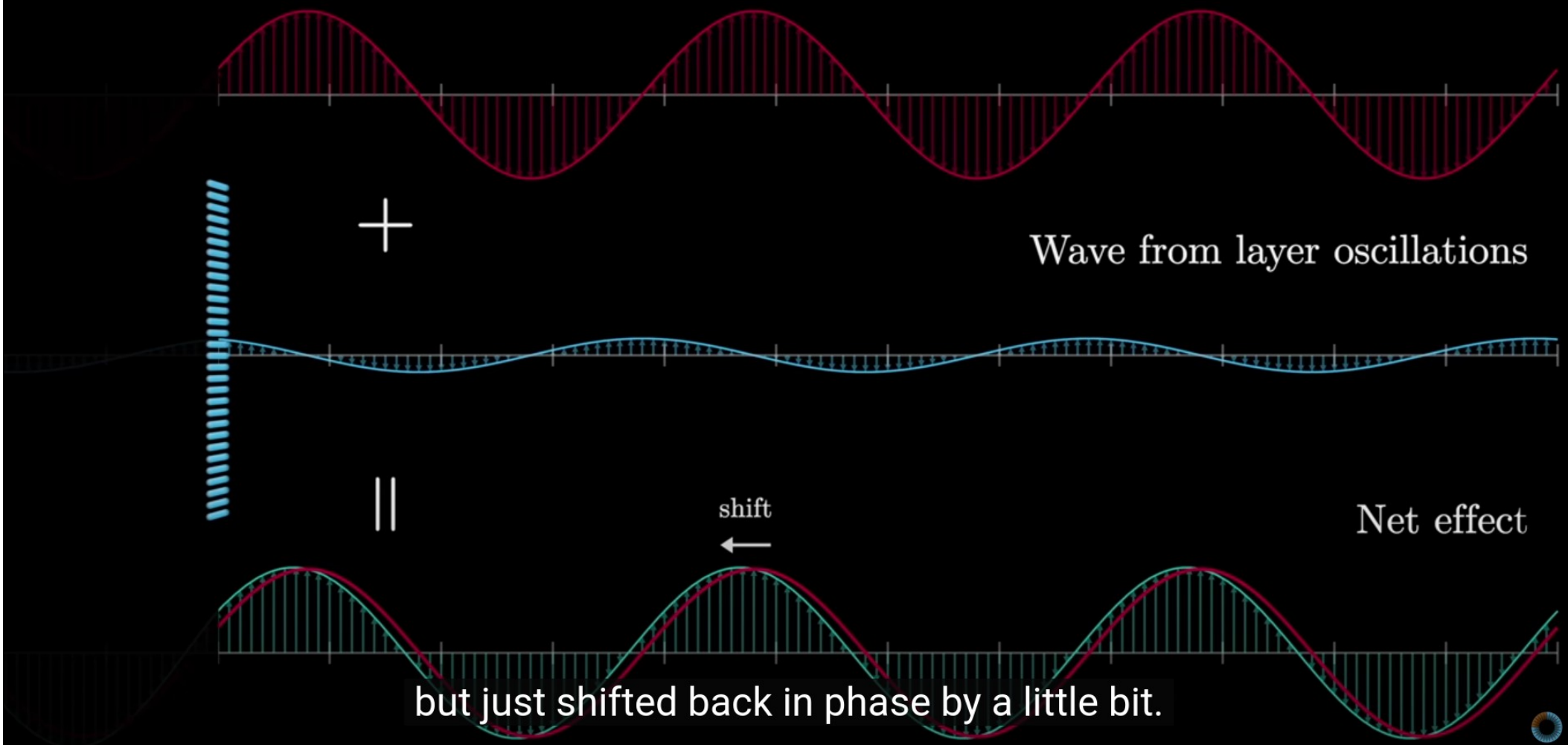
θ_1

$$\theta_1 > \theta_2$$

θ_2

And not this?

like this, and I agree that deserves a better explanation than the tank analogy.



https://www.feynmanlectures.caltech.edu/I_30.html

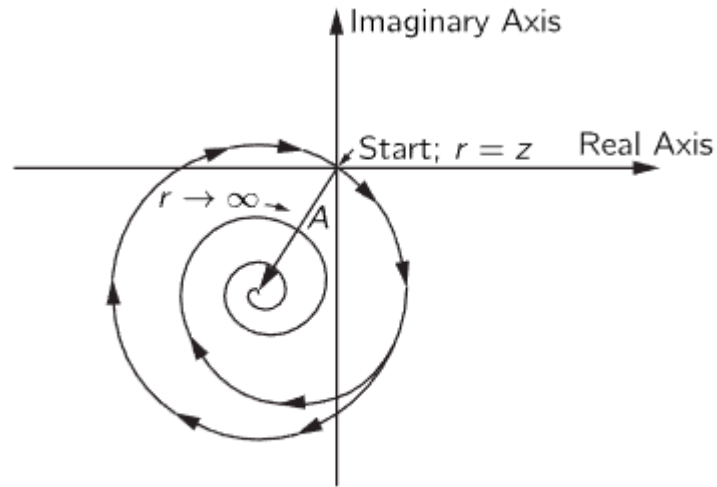
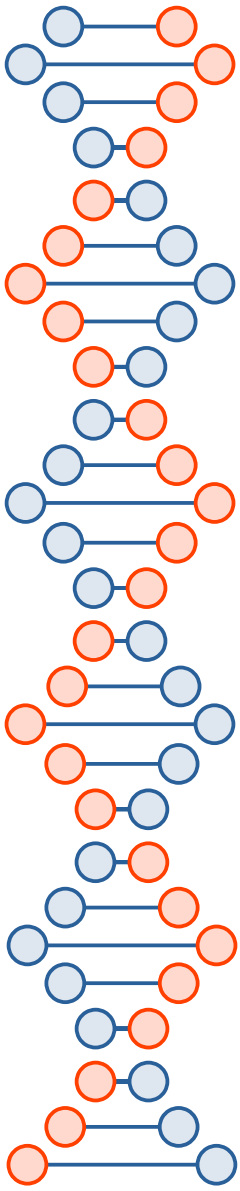
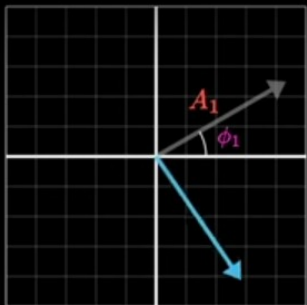


Fig. 30-12. Graphical solution of $\int_z^{\infty} \eta e^{-i\omega r/c} dr$.



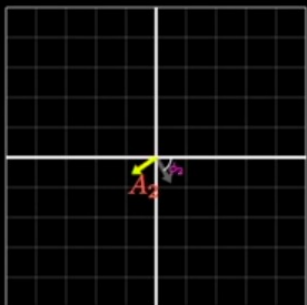
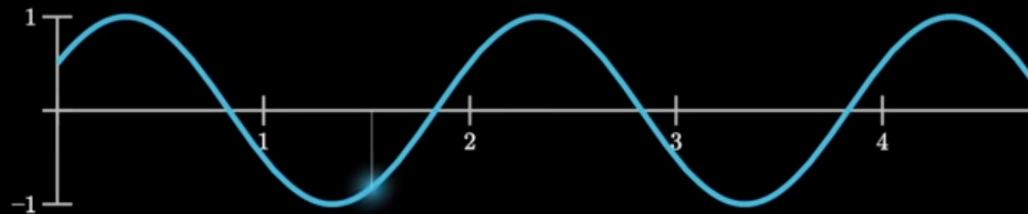


$$A_1 = 1.00$$

$$\omega_1 = 3.14$$

$$\phi_1 = 0.52$$

$$f(t) = A_1 \sin(\omega_1 t + \phi_1)$$

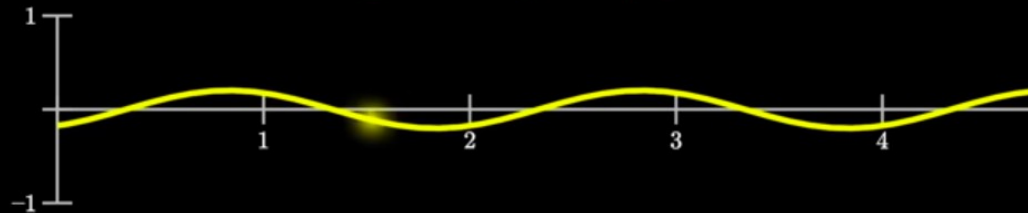


$$A_2 = 0.20$$

$$\omega_2 = 3.14$$

$$\phi_2 = -1.05$$

$$g(t) = A_2 \sin(\omega_2 t + \phi_2)$$

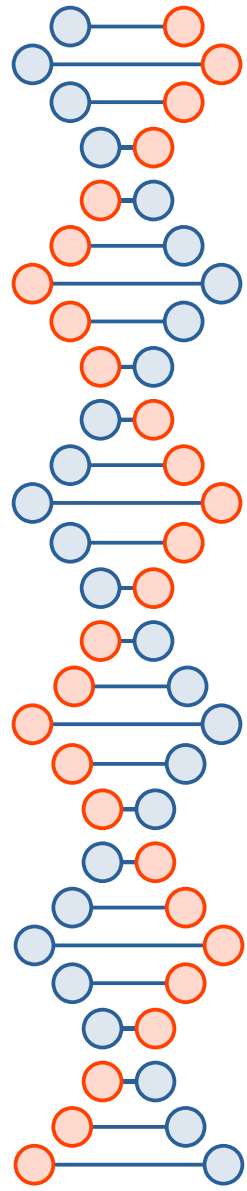


$$f(t) + g(t) = 1.02 \sin(\omega t + 0.33)$$



initial wave, but has just shifted back in its phase by a tiny bit.





<https://arxiv.org/pdf/1011.3245>

The Computational Complexity of Linear Optics

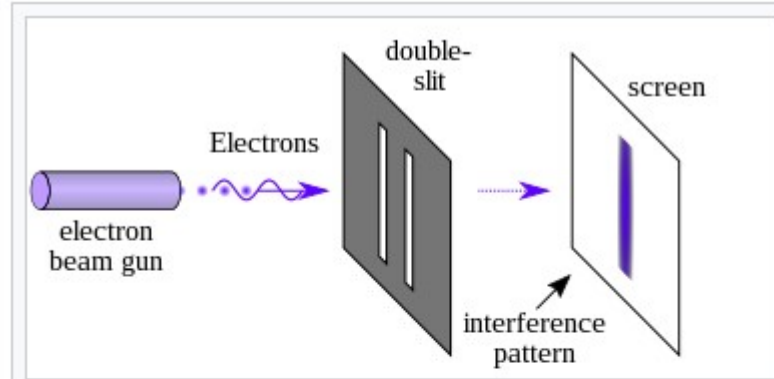
Scott Aaronson*

Alex Arkhipov†

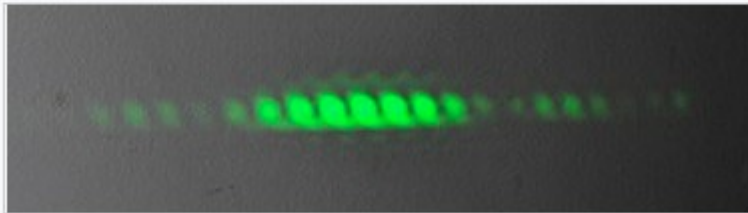
Abstract

We give new evidence that quantum computers—moreover, rudimentary quantum computers built entirely out of linear-optical elements—cannot be efficiently simulated by classical computers. In particular, we define a model of computation in which identical photons are generated, sent through a linear-optical network, then nonadaptively measured to count the number of photons in each mode. This model is not known or believed to be universal for quantum computation, and indeed, we discuss the prospects for realizing the model using current technology. On the other hand, we prove that the model is able to solve sampling problems and search problems that are classically intractable under plausible assumptions.

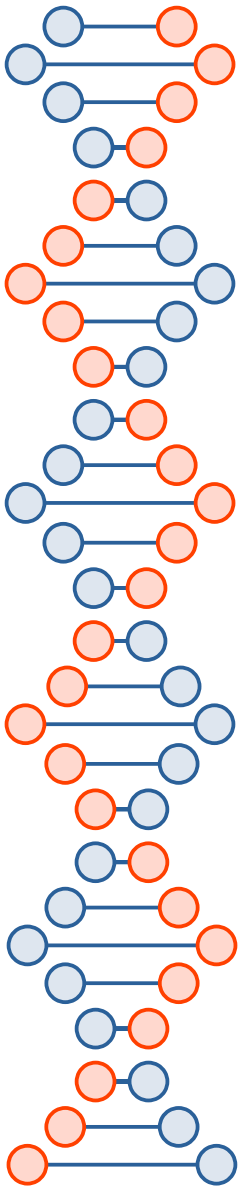
https://en.wikipedia.org/wiki/Double-slit_experiment



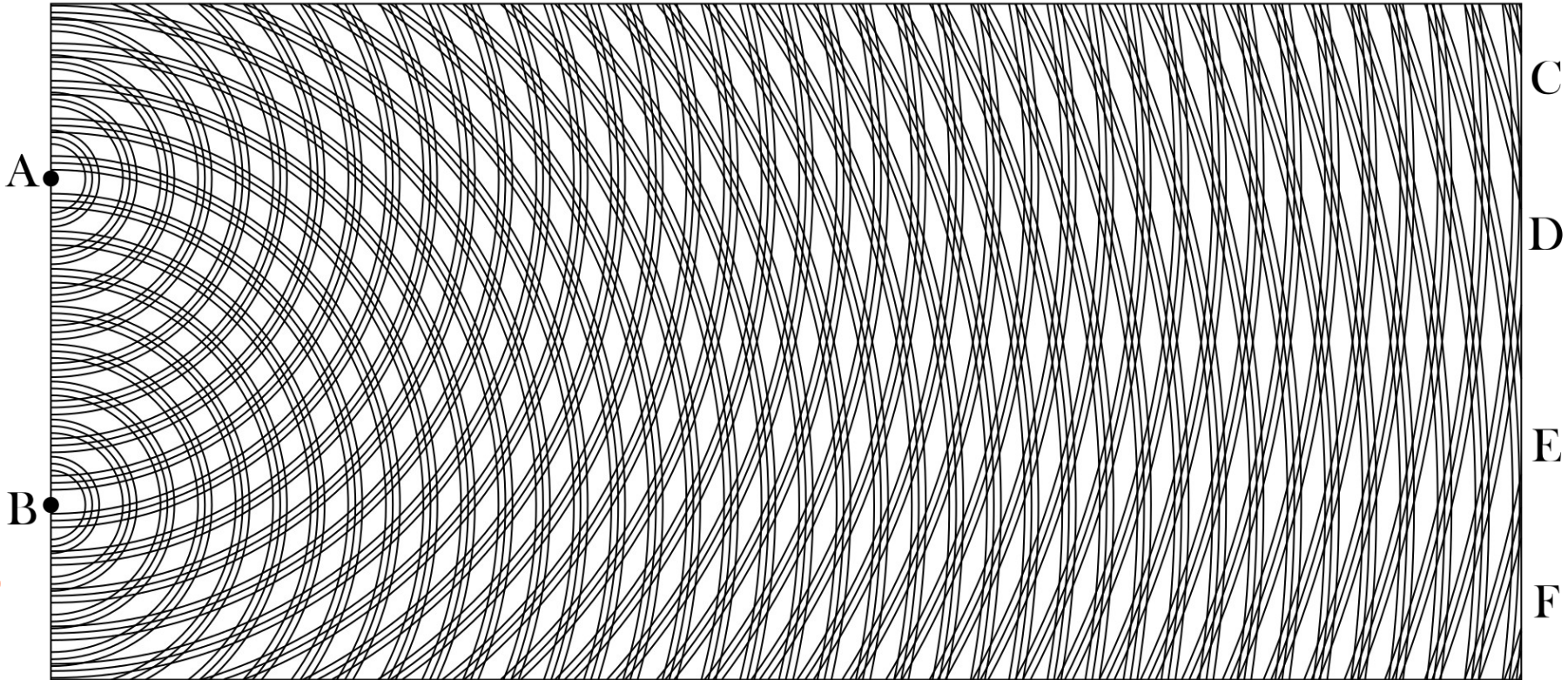
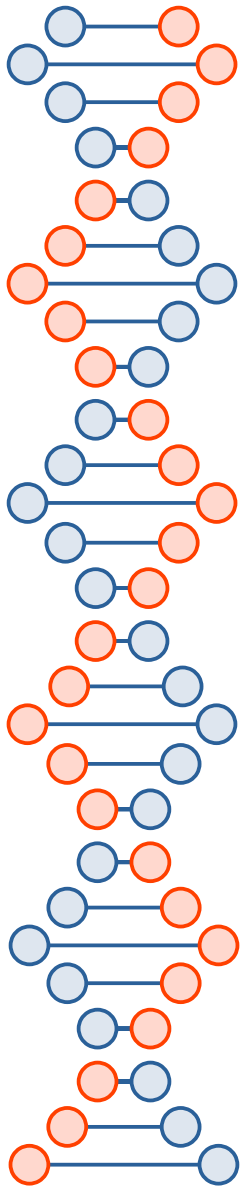
Photons or matter (like electrons) produce an interference pattern when two slits are used

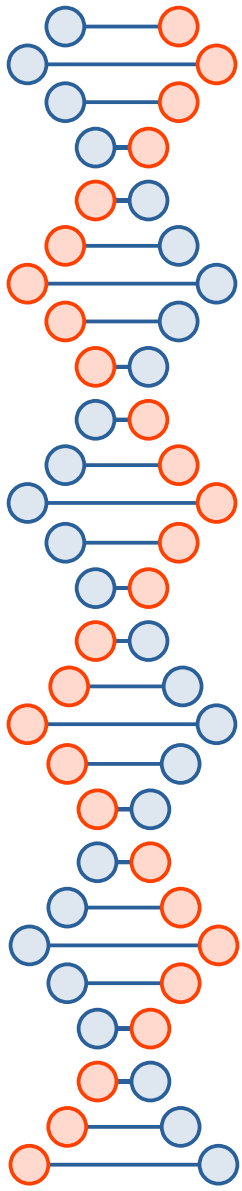


Light from a green laser passing through two slits 0.4mm wide and 0.1mm apart

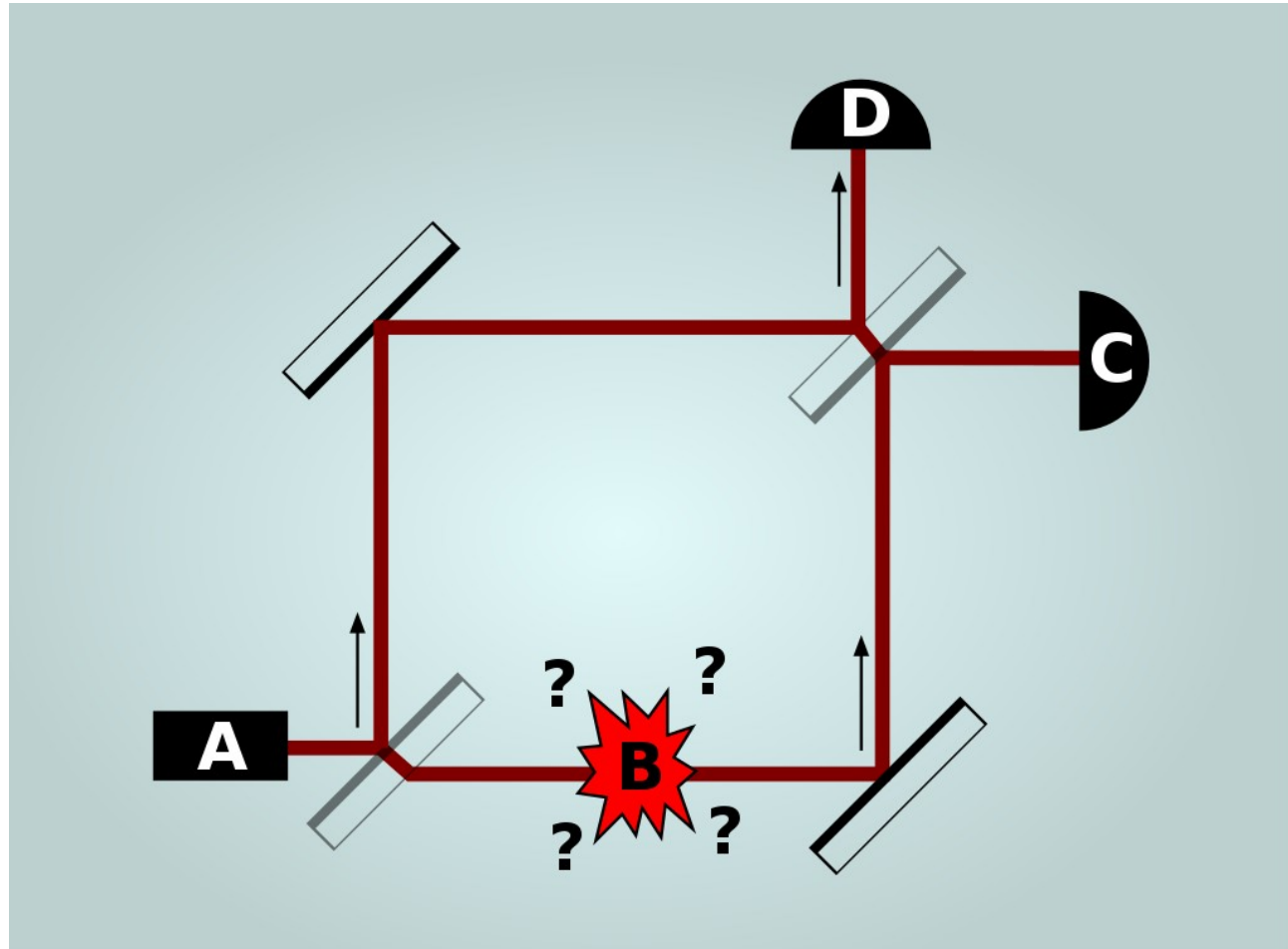


https://en.wikipedia.org/wiki/Double-slit_experiment

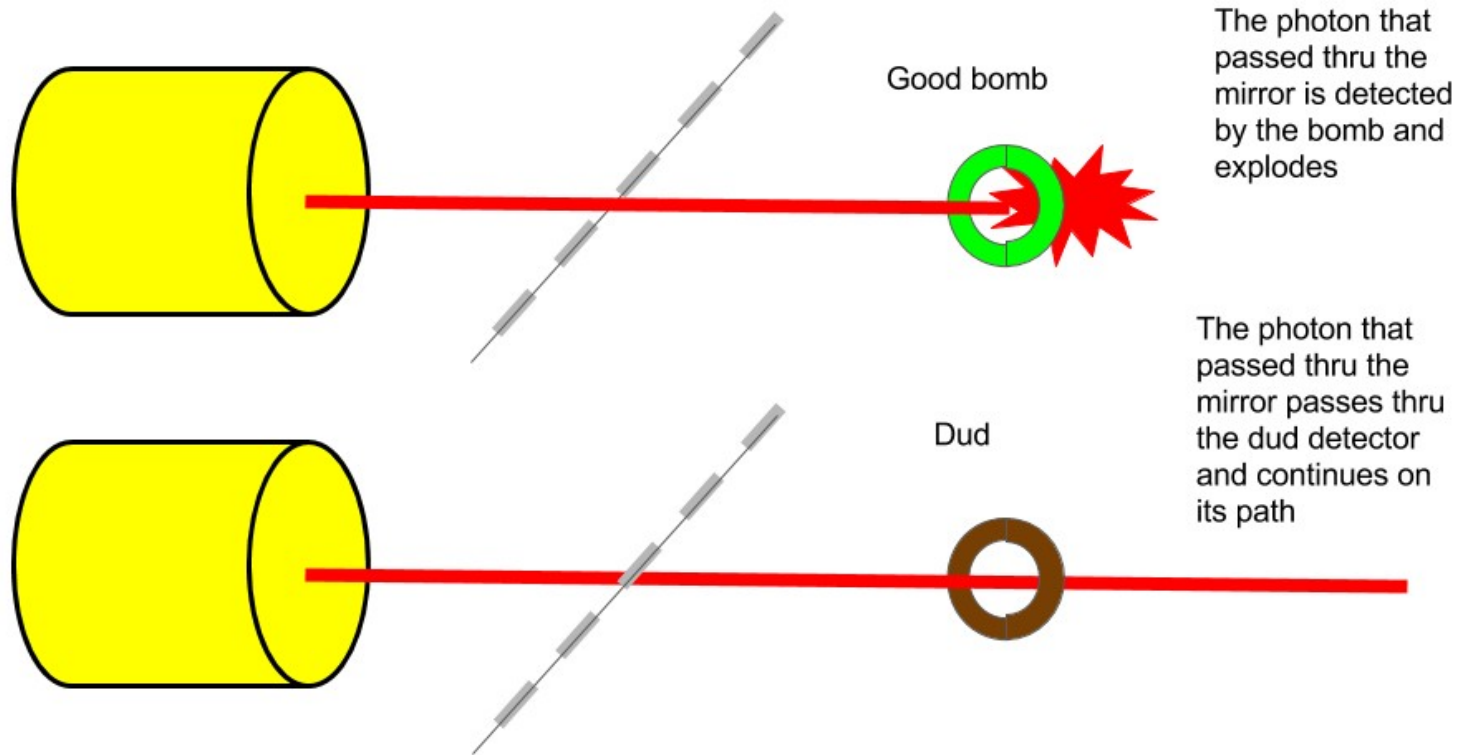
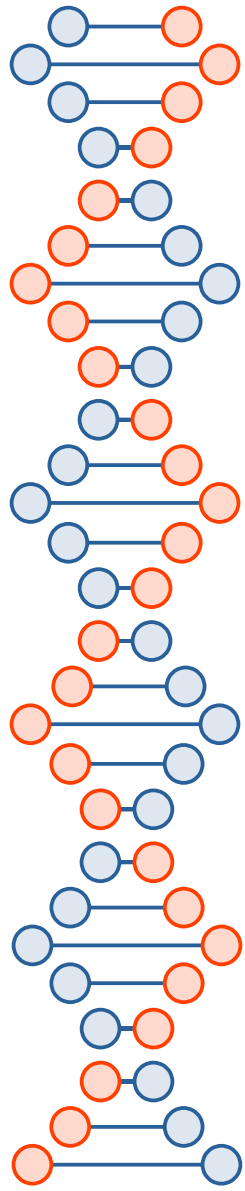




https://en.wikipedia.org/wiki/Elitzur%E2%80%93Vaidman_bomb_tester



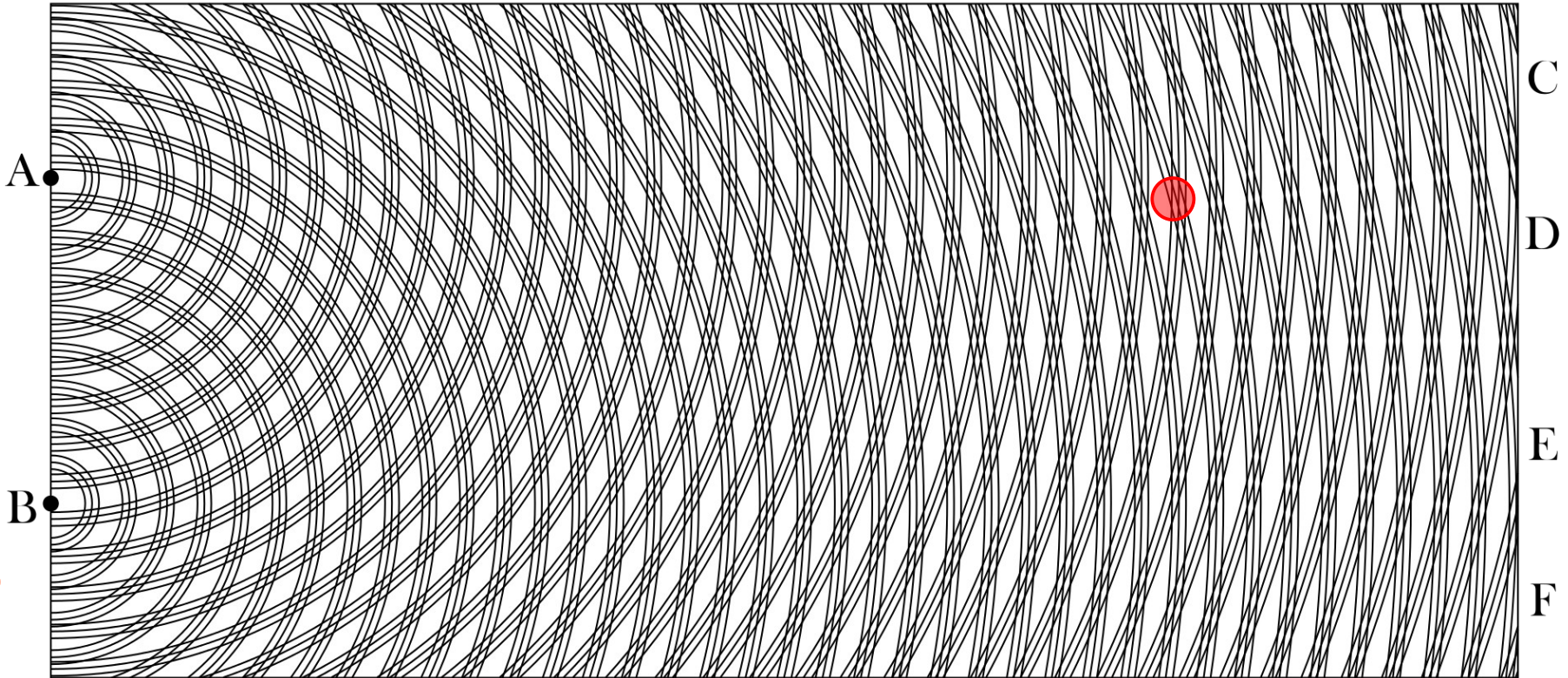
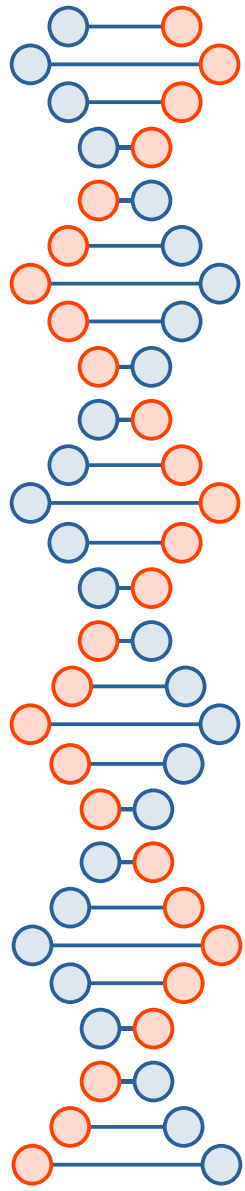
Bomb is either live or a dud



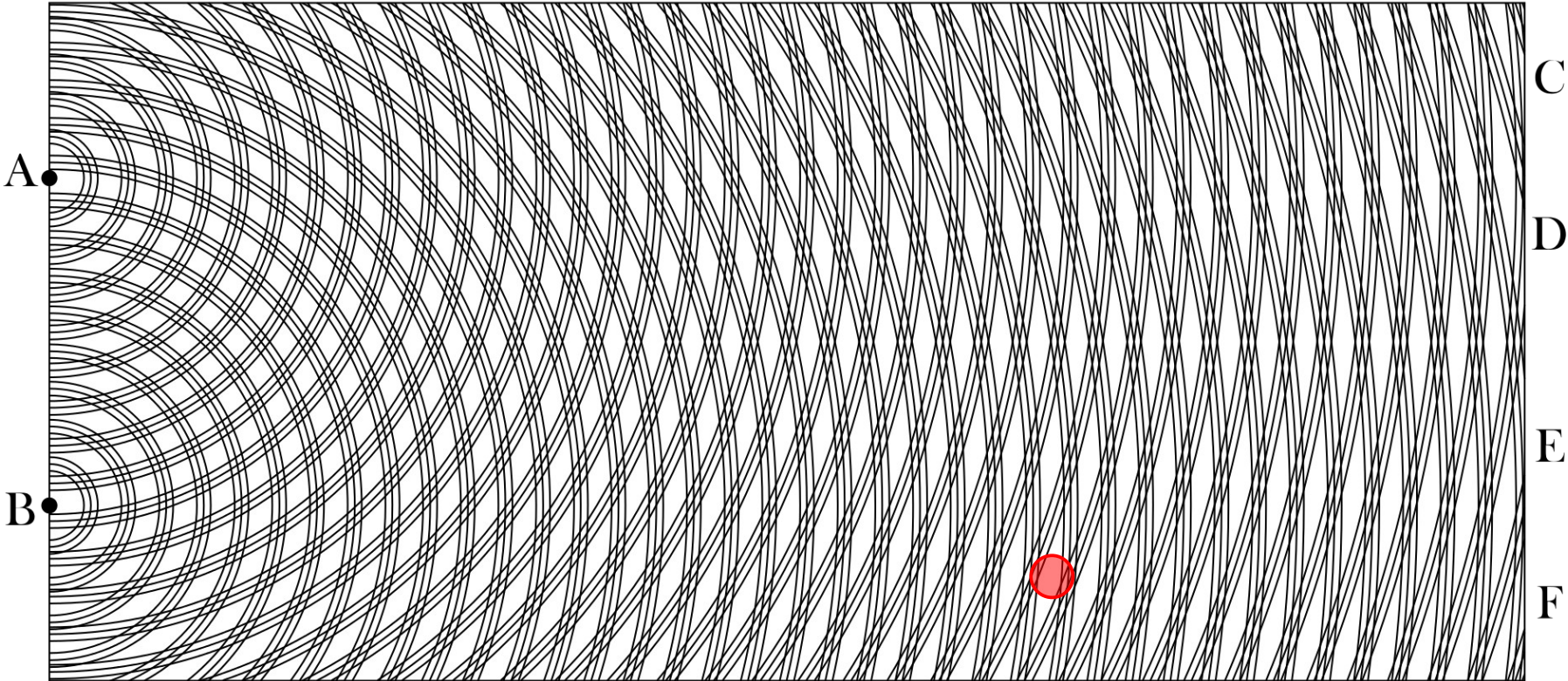
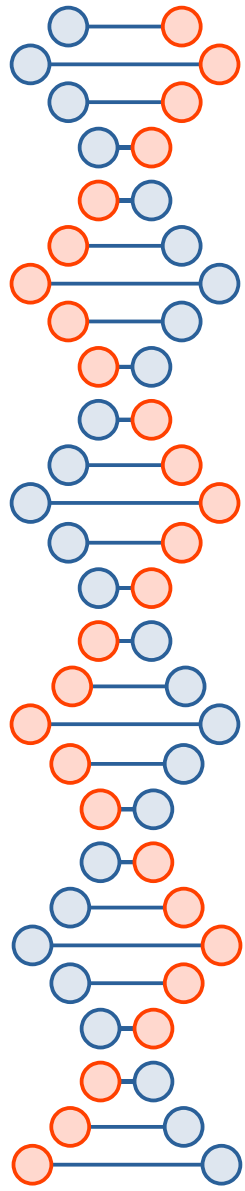


“Due to the way in which the interferometer is constructed, a photon going through the second mirror from the lower path towards detector D will have a phase shift of half a wavelength compared to a photon being reflected from the upper path towards that same detector...”

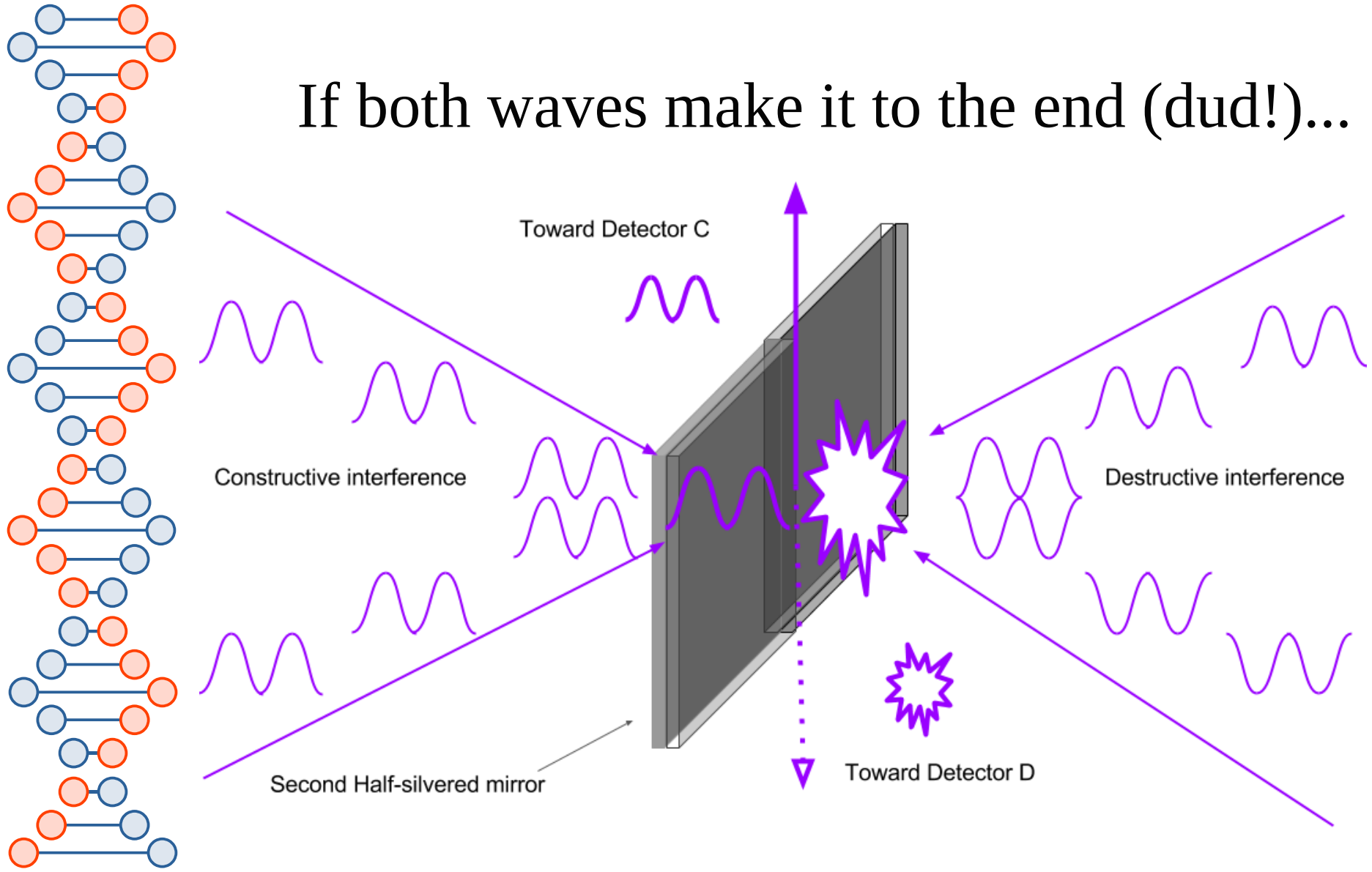
Put C, *e.g.*, here...



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



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



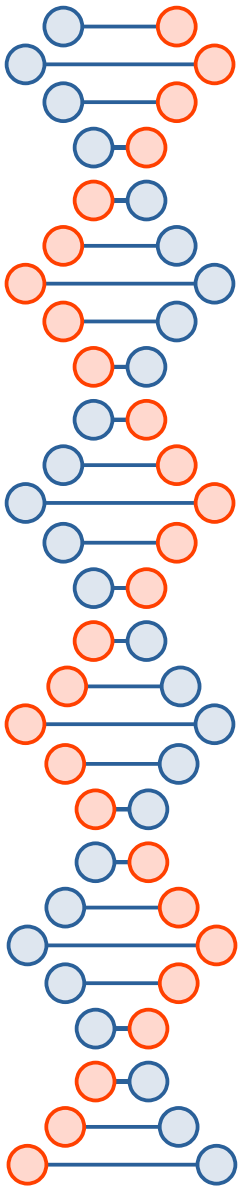


We will never detect a photon at
D if the bomb is a dud.

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

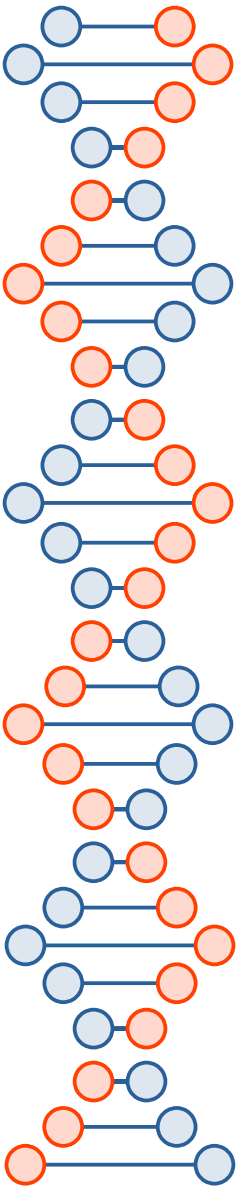
Case #1: Bomb is a dud

- 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



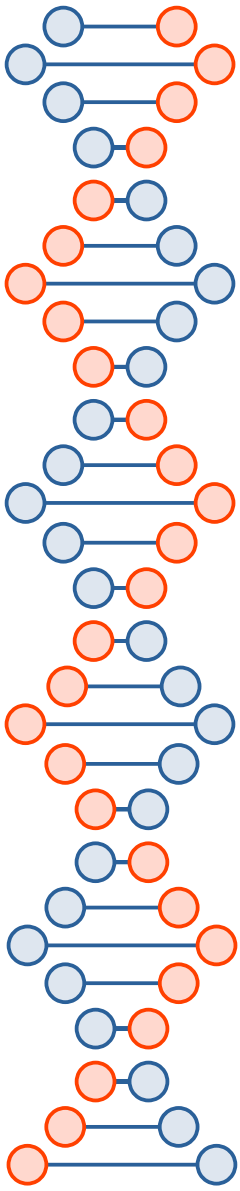
Case #2: Bomb is live

- 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 at D
 - No boom, but we're certain the bomb is live





WTF?

- With a decent probability ($1/3$), we learn information about something that could 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

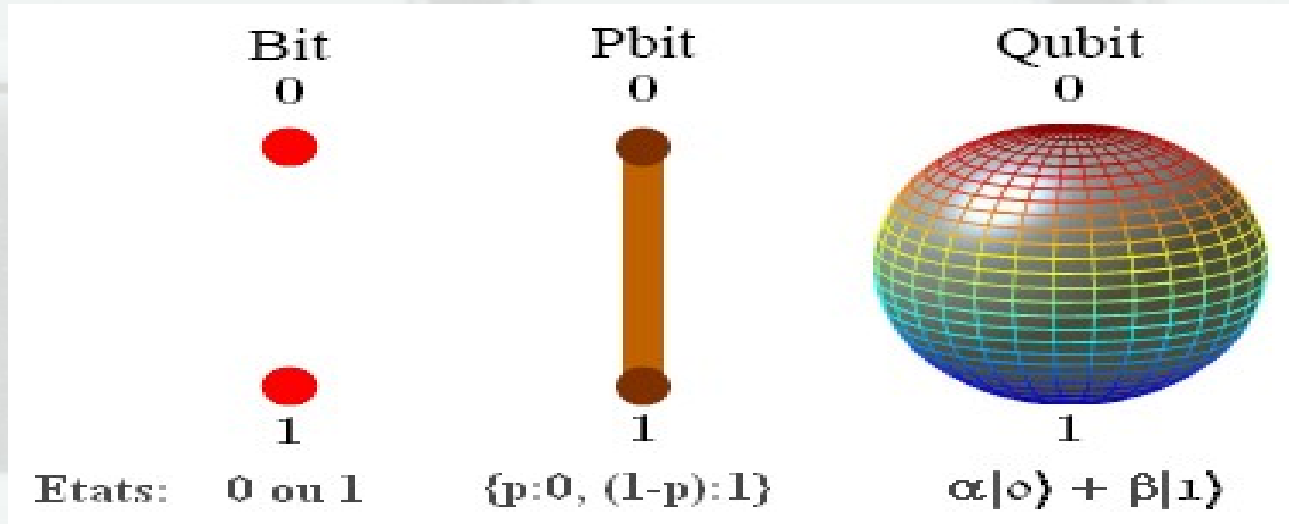
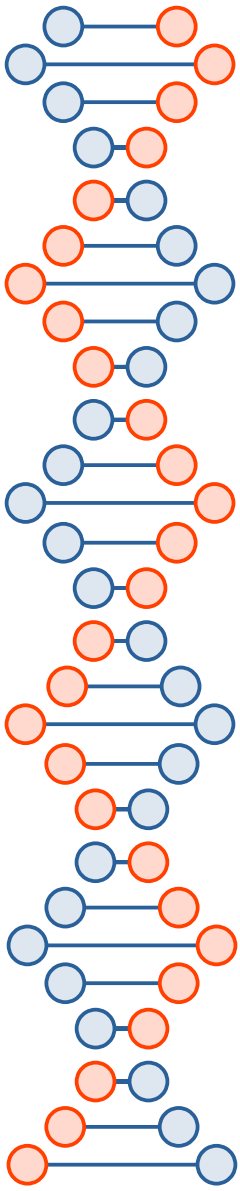


Image taken from <http://filipchsqroom.blogspot.com/>

Is superposition enough?

- As far as I know (but actual physicists are not in complete agreement on this) qubits have to be mutually entangled in very specific ways to implement useful quantum computations with more than 1 or 2 qubits
 - Quantum decoherence is a major challenge





Quantum State: Bra-ket Notation – 2 Qubits (Non Entangled)

$$\text{Qubit 0 } |\psi_0\rangle = \alpha|0\rangle + \beta|1\rangle$$

$$\text{Qubit } |\psi_1\rangle = \gamma|0\rangle + \delta|1\rangle$$

$$|\psi\rangle = \alpha\gamma|00\rangle + \alpha\delta|01\rangle + \beta\gamma|10\rangle + \beta\delta|11\rangle$$

This operation is called **Tensor Product**

$$|\psi_0\rangle \otimes |\psi_1\rangle = |\psi_0\rangle|\psi_1\rangle = |\psi_0\psi_1\rangle = \begin{bmatrix} \alpha \\ \beta \end{bmatrix} \otimes \begin{bmatrix} \gamma \\ \delta \end{bmatrix} = \begin{bmatrix} \alpha\gamma \\ \alpha\delta \\ \beta\gamma \\ \beta\delta \end{bmatrix} \begin{matrix} |00\rangle \\ |01\rangle \\ |10\rangle \\ |11\rangle \end{matrix}$$

<https://andisama.medium.com/qubit-an-intuition-2-inner-product-outer-product-and-tensor-product-in-bra-ket-notation-9d598cbd6bc>

History of Quantum Entanglement

$$|\beta_{00}\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}} = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 1 \end{pmatrix}$$

$$|\beta_{01}\rangle = \frac{|01\rangle + |10\rangle}{\sqrt{2}} = \begin{pmatrix} 0 \\ 1 \\ 1 \\ 0 \end{pmatrix}$$

$$|\beta_{10}\rangle = \frac{|00\rangle - |11\rangle}{\sqrt{2}} = \begin{pmatrix} 1 \\ 0 \\ 0 \\ -1 \end{pmatrix}$$

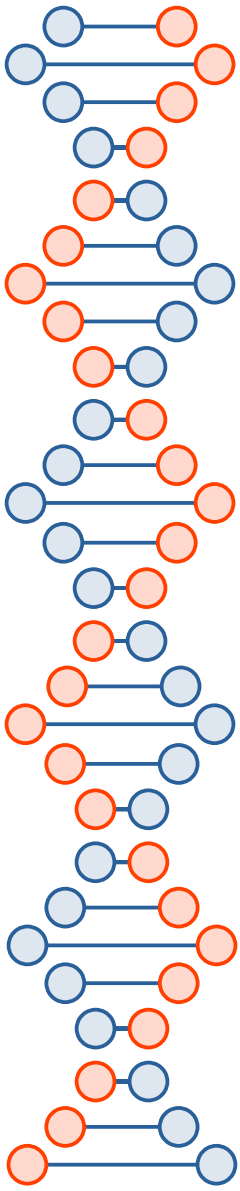
$$|\beta_{11}\rangle = \frac{|01\rangle - |10\rangle}{\sqrt{2}} = \begin{pmatrix} 0 \\ 1 \\ -1 \\ 0 \end{pmatrix}$$

- Normalized: $\langle \beta_{00} | \beta_{00} \rangle = \frac{\langle 00 | + \langle 11 |}{\sqrt{2}} \cdot \frac{|00\rangle + |11\rangle}{\sqrt{2}} = \frac{1}{\sqrt{2}}(1+1) = 1$

- Orthogonal : $\langle \beta_{01} | \beta_{00} \rangle = \frac{\langle 01 | + \langle 10 |}{\sqrt{2}} \cdot \frac{|00\rangle + |11\rangle}{\sqrt{2}}$
 $= \langle 0|0\rangle\langle 1|0\rangle + \langle 0|1\rangle\langle 1|1\rangle + \langle 1|0\rangle\langle 0|0\rangle + \langle 1|1\rangle\langle 0|1\rangle = 0$

- Expansion:
 $|\alpha\beta\rangle = |\beta_{00}\rangle\langle\beta_{00}|\alpha\beta\rangle + |\beta_{01}\rangle\langle\beta_{01}|\alpha\beta\rangle + |\beta_{10}\rangle\langle\beta_{10}|\alpha\beta\rangle + |\beta_{11}\rangle\langle\beta_{11}|\alpha\beta\rangle$

<https://galileo-unbound.blog/2022/11/26/a-short-history-of-quantum-entanglement/>

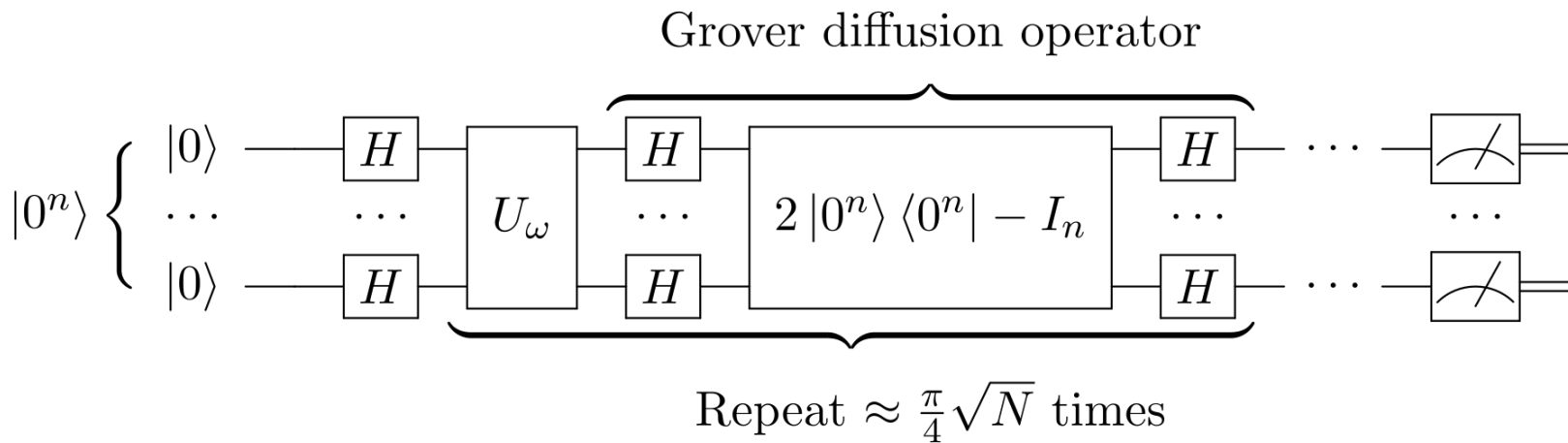
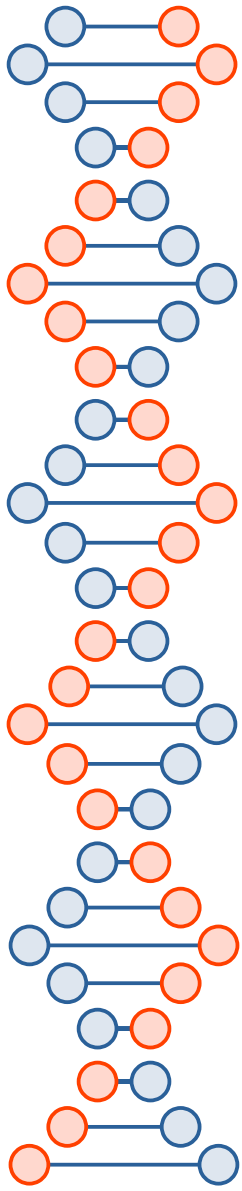


<https://www.cnet.com/tech/computing/quantum-computer-makers-like-their-odds-for-big-progress-soon/>

What we need for the Internet to work...

- Symmetric crypto
 - Encryption
 - Authentication
 - Secure hashes
 - Others?
- Asymmetric crypto
 - 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

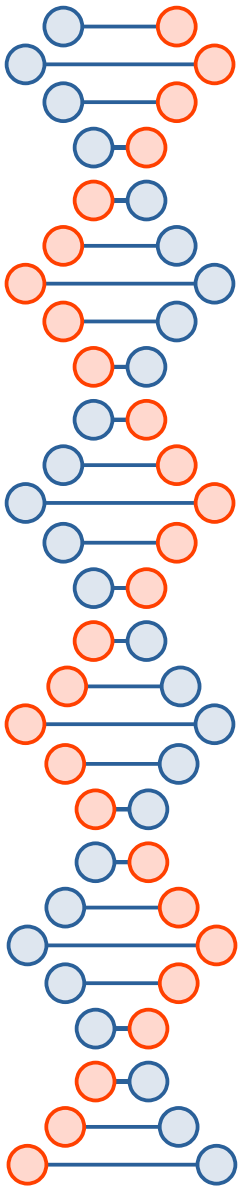


Symmetric crypto

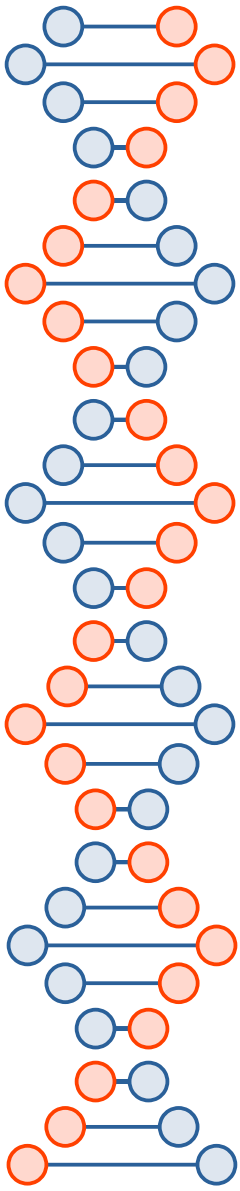
- Just double the key size, we'll be okay (for the most part)...
 - $\text{sqrt}(2^{2n}) = 2^n$
 - $\text{sqrt}(2^{256}) = 2^{128}$

Asymmetric Crypto

- Quantum computers seem to be good at the same kinds of things that make good, simple 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)



What tools have we used to crack crypto this semester?





What tools have we used to crack crypto this semester?

- XOR



What tools have we used to crack crypto this semester?

- XOR
- Frequency analysis



What tools have we used to crack crypto this semester?

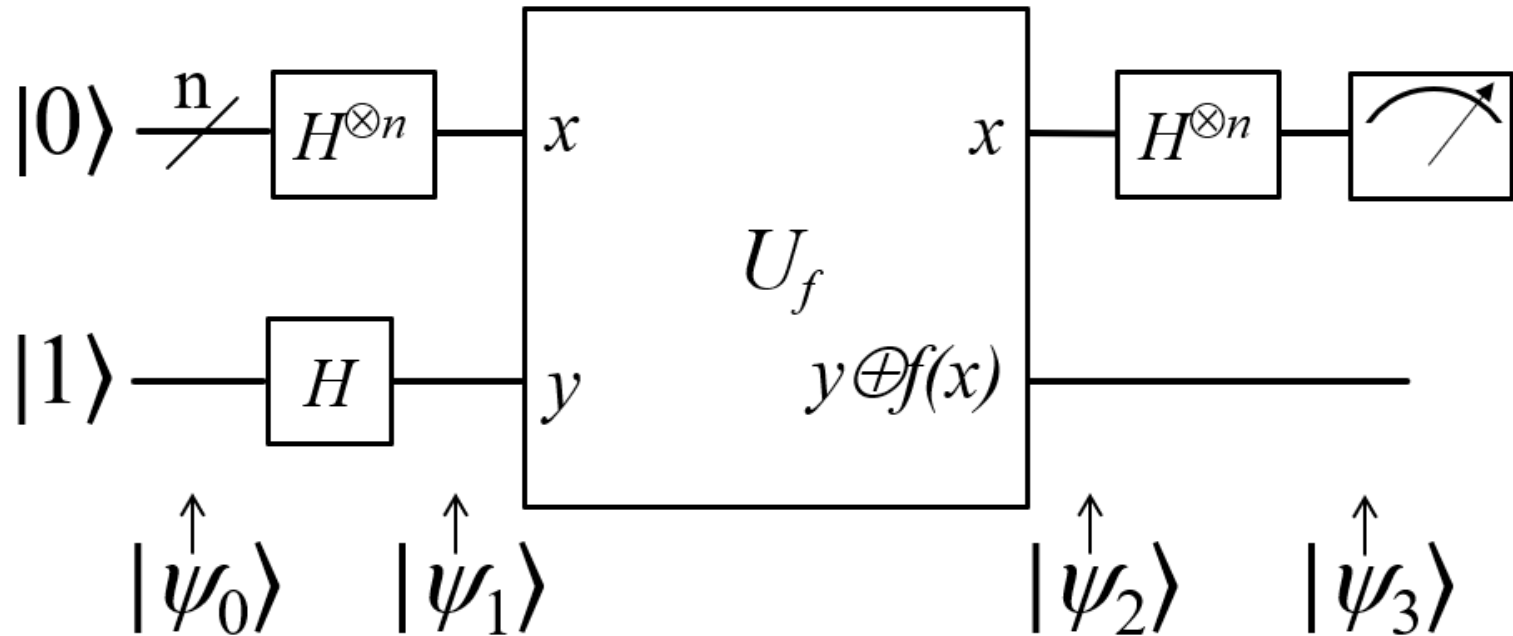
- XOR
- Frequency analysis
- Side channels



What tools have we used to crack crypto this semester?

- XOR
- Frequency analysis
- Side channels
- ???

Deutsch-Jozsa algorithm



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



1-bit input case...

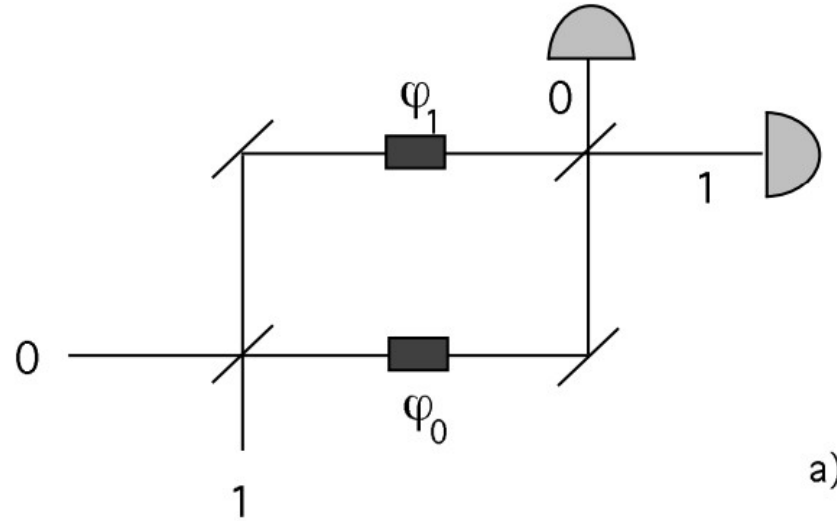
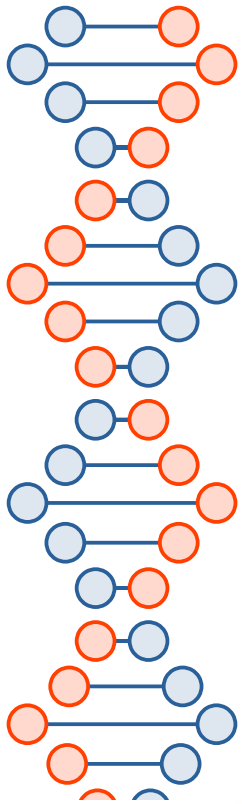
- p = Probability of measuring $|0\rangle$

$$\left| \left(\frac{1}{2} \right) (-1)^{f(0)} + \left(\frac{1}{2} \right) (-1)^{f(1)} \right|$$

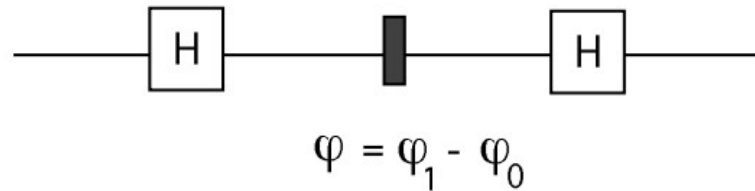
A balanced function cancels itself out because of destructive interference

$f(0)$	$f(1)$	p
0	0	1
0	1	0
1	0	0
1	1	1

<https://arxiv.org/abs/quant-ph/9708016>



a)

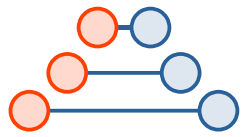


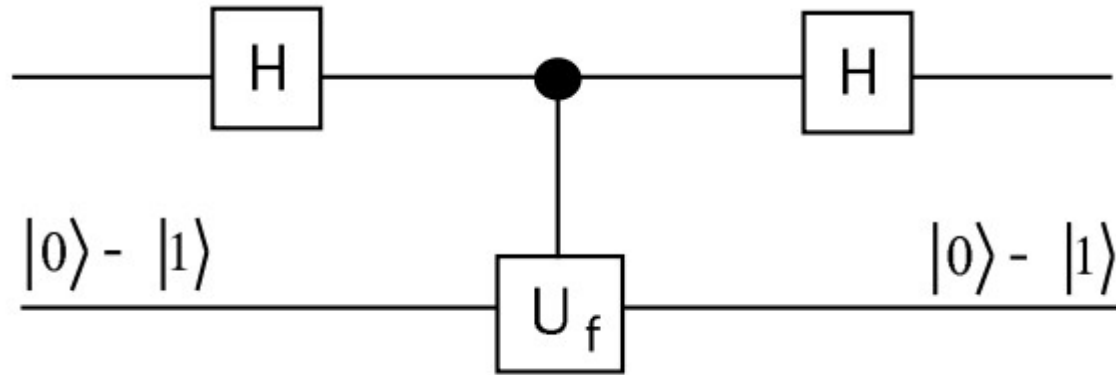
$$\varphi = \varphi_1 - \varphi_0$$

b)

$$|0\rangle \xrightarrow{H} \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$$

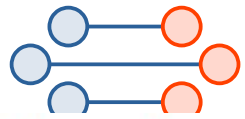
$$|1\rangle \xrightarrow{H} \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$





$$|x\rangle |y\rangle \xrightarrow{f-c-N} |x\rangle |y \oplus f(x)\rangle . \quad (2.1)$$

The initial state of the qubits in the quantum network is $|0\rangle$ ($|0\rangle - |1\rangle$) (apart from a normalization factor, which will be omitted in the following). After the first Hadamard transform, the state of the two qubits has the form $(|0\rangle + |1\rangle)(|0\rangle - |1\rangle)$. To determine the effect of the f -controlled-NOT on this state, first note



that, for each $x \in \{0, 1\}$,

$$|x\rangle (|0\rangle - |1\rangle) \xrightarrow{f^{-c-N}} |x\rangle (|0 \oplus f(x)\rangle - |1 \oplus f(x)\rangle) = (-1)^{f(x)} |x\rangle (|0\rangle - |1\rangle) . \quad (2.2)$$

Therefore, the state after the f -controlled-NOT is

$$((-1)^{f(0)} |0\rangle + (-1)^{f(1)} |1\rangle)(|0\rangle - |1\rangle) . \quad (2.3)$$

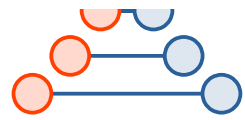
That is, for each x , the $|x\rangle$ term acquires a phase factor of $(-1)^{f(x)}$, which corresponds to the eigenvalue of the state of the auxiliary qubit under the action of the operator that sends $|y\rangle$ to $|y \oplus f(x)\rangle$.

This state can also be written as

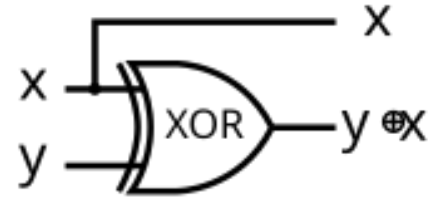
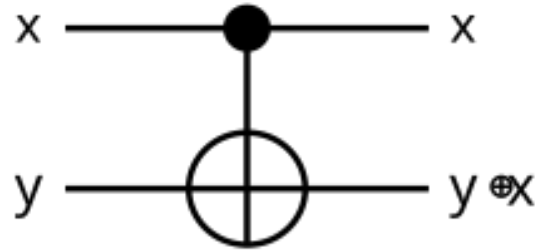
$$(-1)^{f(0)} (|0\rangle + (-1)^{f(0) \oplus f(1)} |1\rangle) , \quad (2.4)$$

which, after applying the second Hadamard transform, becomes

$$(-1)^{f(0)} |f(0) \oplus f(1)\rangle . \quad (2.5)$$

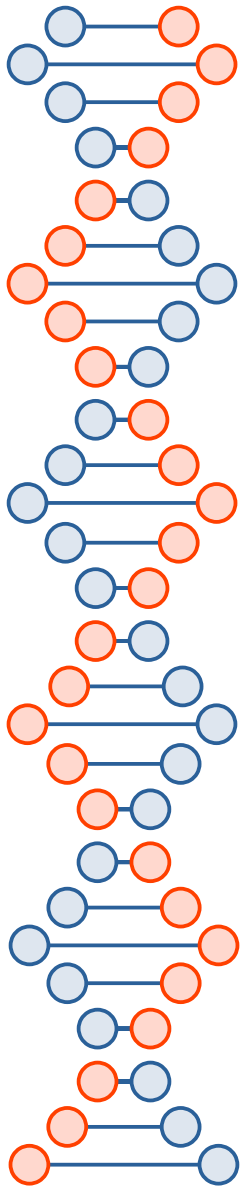


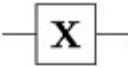



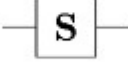

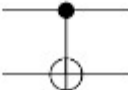
CNOT (Wikipedia)

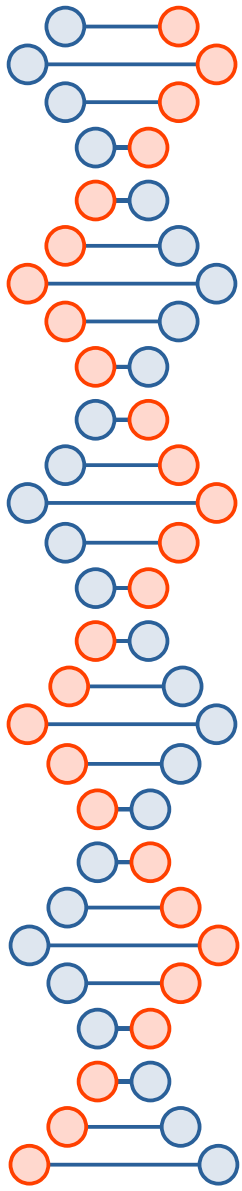


input		output	
x	y	x	y+x
0⟩	0⟩	0⟩	0⟩
0⟩	1⟩	0⟩	1⟩
1⟩	0⟩	1⟩	1⟩
1⟩	1⟩	1⟩	0⟩

input		output	
X	y	X	y+X
0	0	0	0
0	1	0	1
1	0	1	1
1	1	1	0



Operator	Gate(s)	Matrix
Pauli-X (X)	 \oplus	$\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$
Pauli-Y (Y)		$\begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}$
Pauli-Z (Z)		$\begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$
Hadamard (H)		$\frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$
Phase (S, P)		$\begin{bmatrix} 1 & 0 \\ 0 & i \end{bmatrix}$
$\pi/8$ (T)		$\begin{bmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{bmatrix}$
Controlled Not (CNOT, CX)		$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$

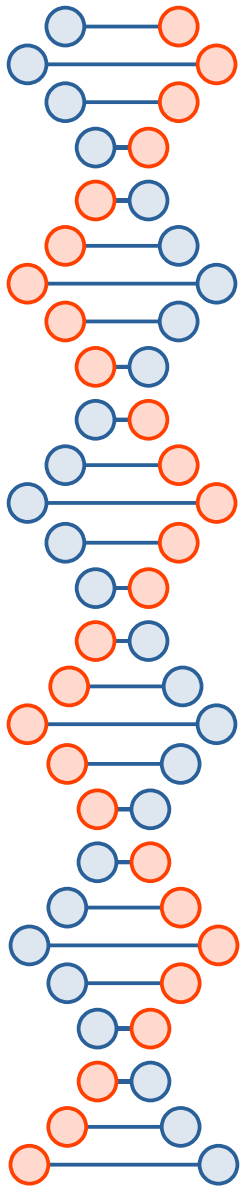


$$H_0 = +(1)$$

$$H_1 = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

$$H_2 = \frac{1}{2} \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{pmatrix}$$

$$H_3 = \frac{1}{2^{3/2}} \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 & 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 & 1 & -1 & -1 & 1 \\ 1 & 1 & 1 & 1 & -1 & -1 & -1 & -1 \\ 1 & -1 & 1 & -1 & -1 & 1 & -1 & 1 \\ 1 & 1 & -1 & -1 & -1 & -1 & 1 & 1 \\ 1 & -1 & -1 & 1 & -1 & 1 & 1 & -1 \end{pmatrix}$$



<https://www.youtube.com/watch?v=tHfGucHtLqo>

What can my homemade quantum computer do?

Looking Glass Universe
331K subscribers

9.6K

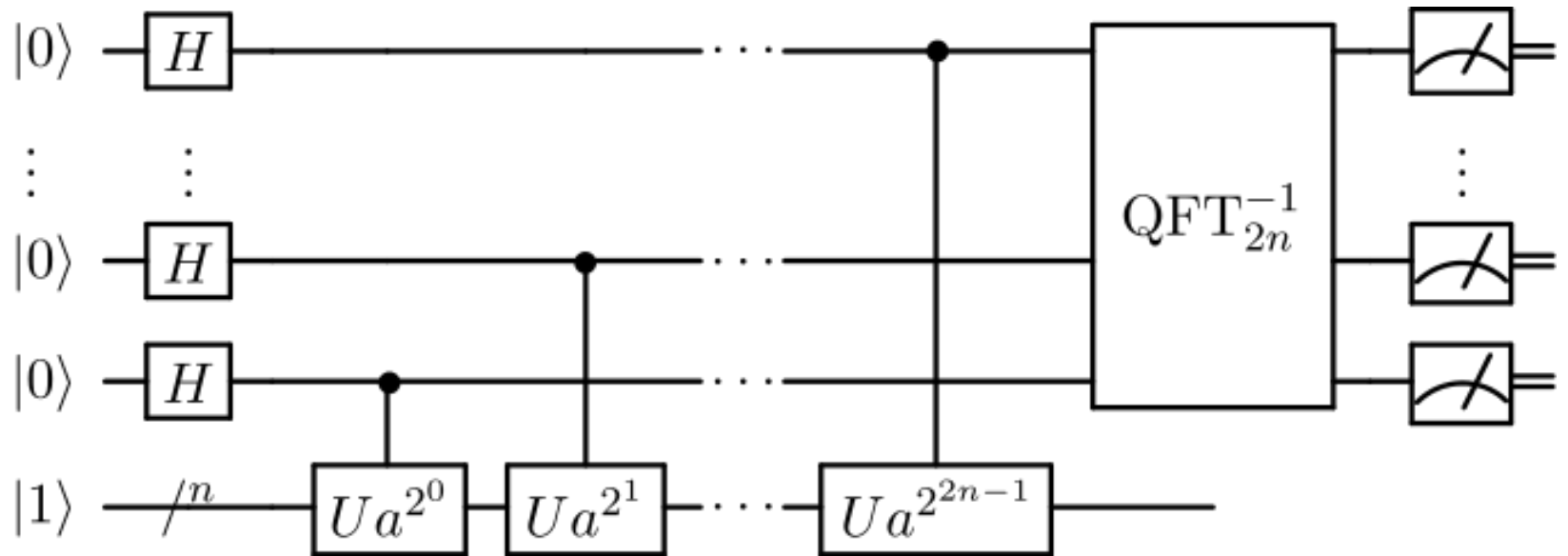
Share

Download

Clip

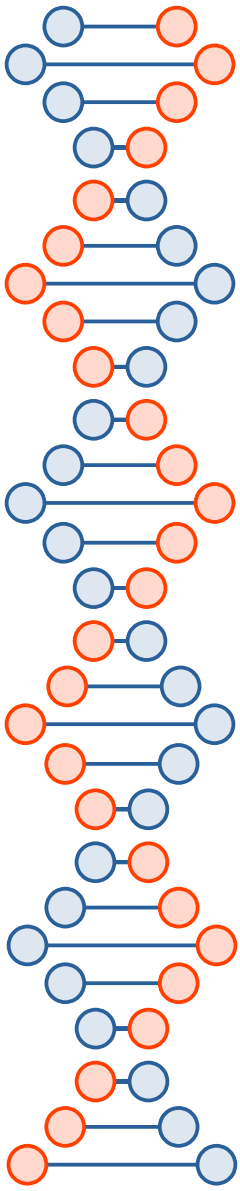
Save

Shor's algorithm



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

<https://www.youtube.com/watch?v=FRZQ-efABeQ>



17388/2

$$127 \pm 1$$

aka

$$127 \pm 1$$

8694

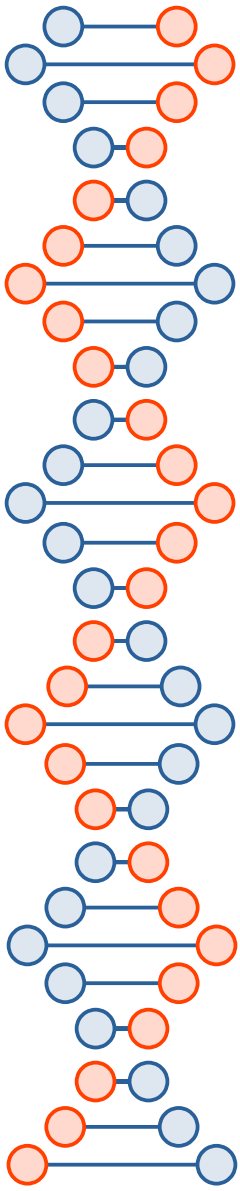
improved guess of a number that shares factors with 314191.

probab...
w/ 314191

4:07 / 5:51

Digital Artifact assignment #4

- The server had the private key and wouldn't share it with the attacker, but the attacker exploited a side channel to learn the plaintext bit-by-bit
 - Whether you realized it or not, *what could have happened and didn't* is as important to the flow of information in a padding oracle attack as what did happen
- Shor's algorithm is a little bit like that...
 - The universe knows what the factors are
 - The wrong answers cancel each other out





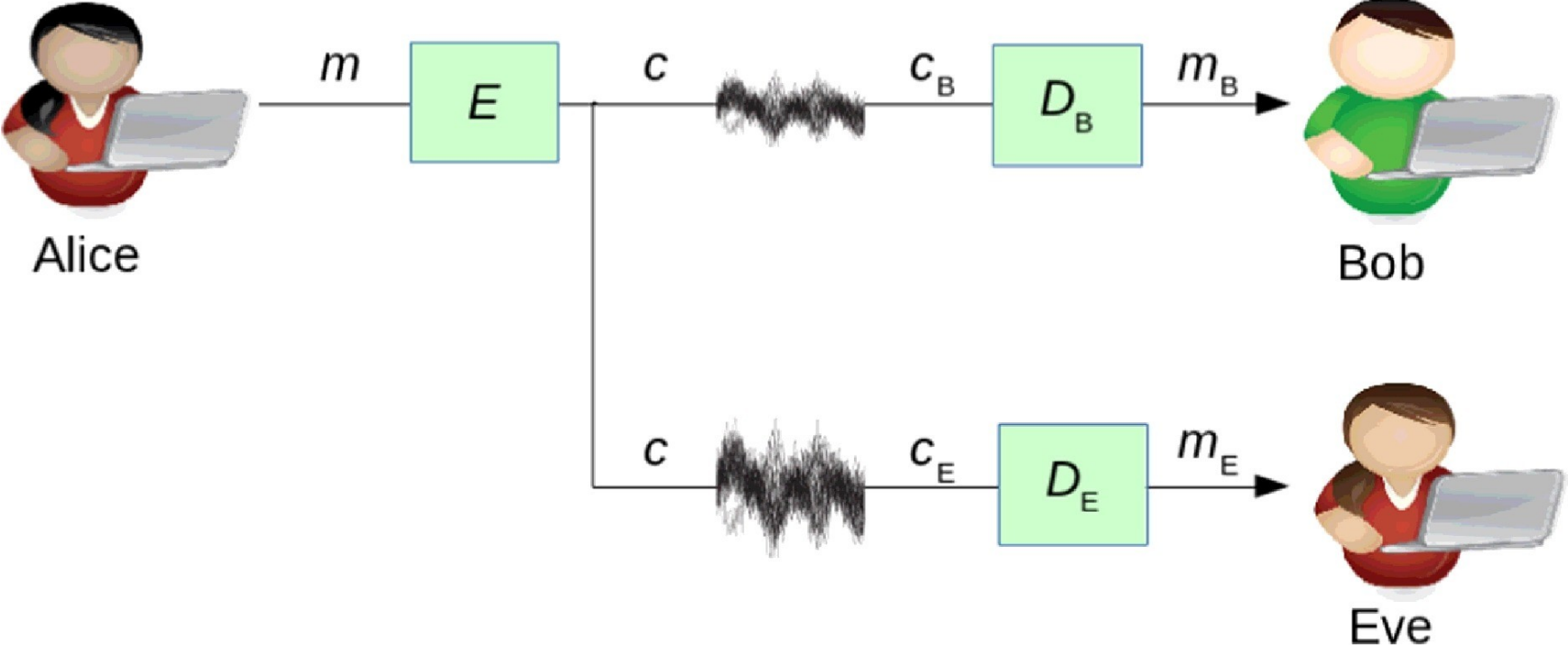
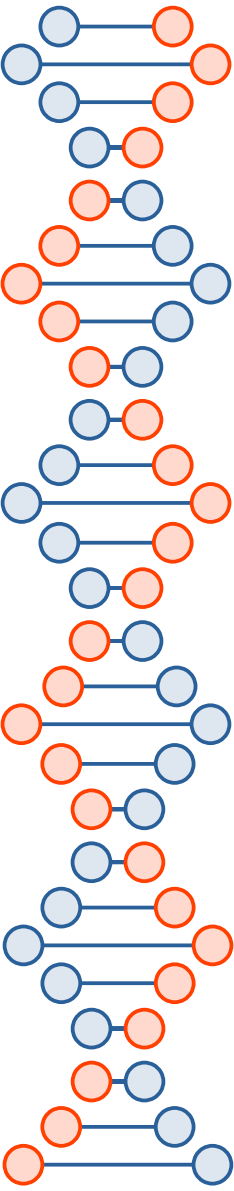
RSA, DH, ECDH, DSA, *etc.* all broken. Need something else instead...

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

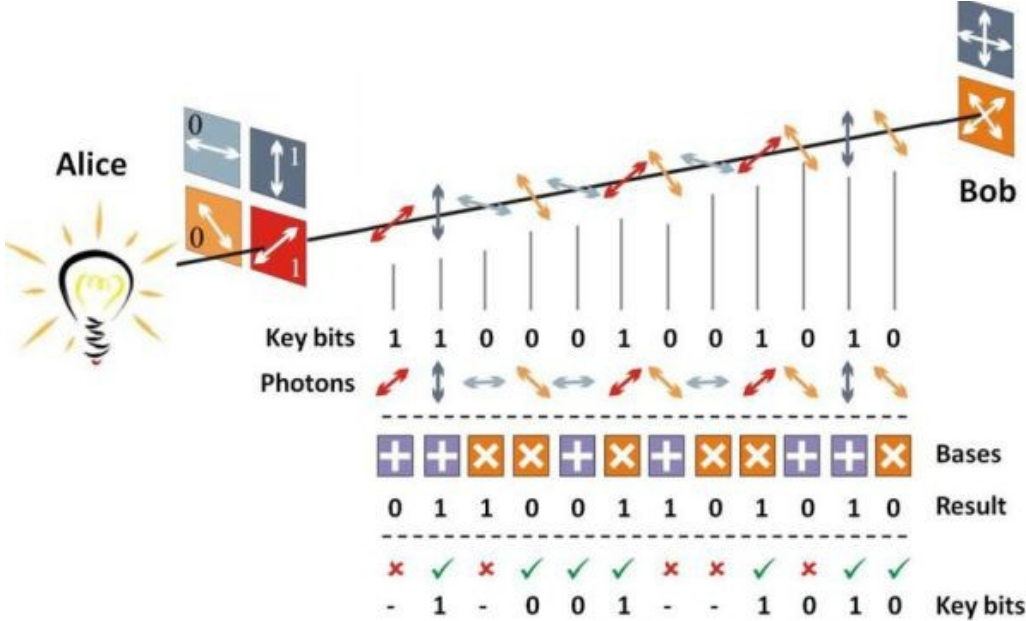
https://en.wikipedia.org/wiki/Lamport_signature

Wiretap channel



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

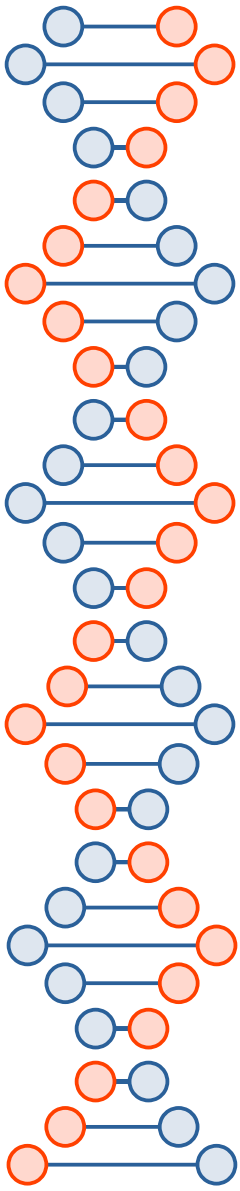
Quantum Key Distribution

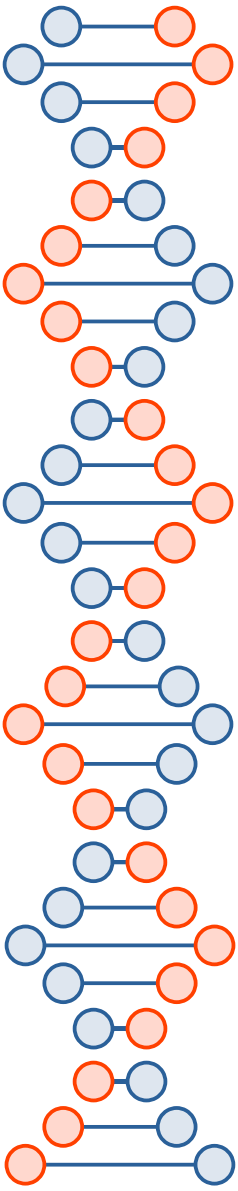


<https://imrmedia.in/quantum-key-distribution-test-successfully-demonstrated/>

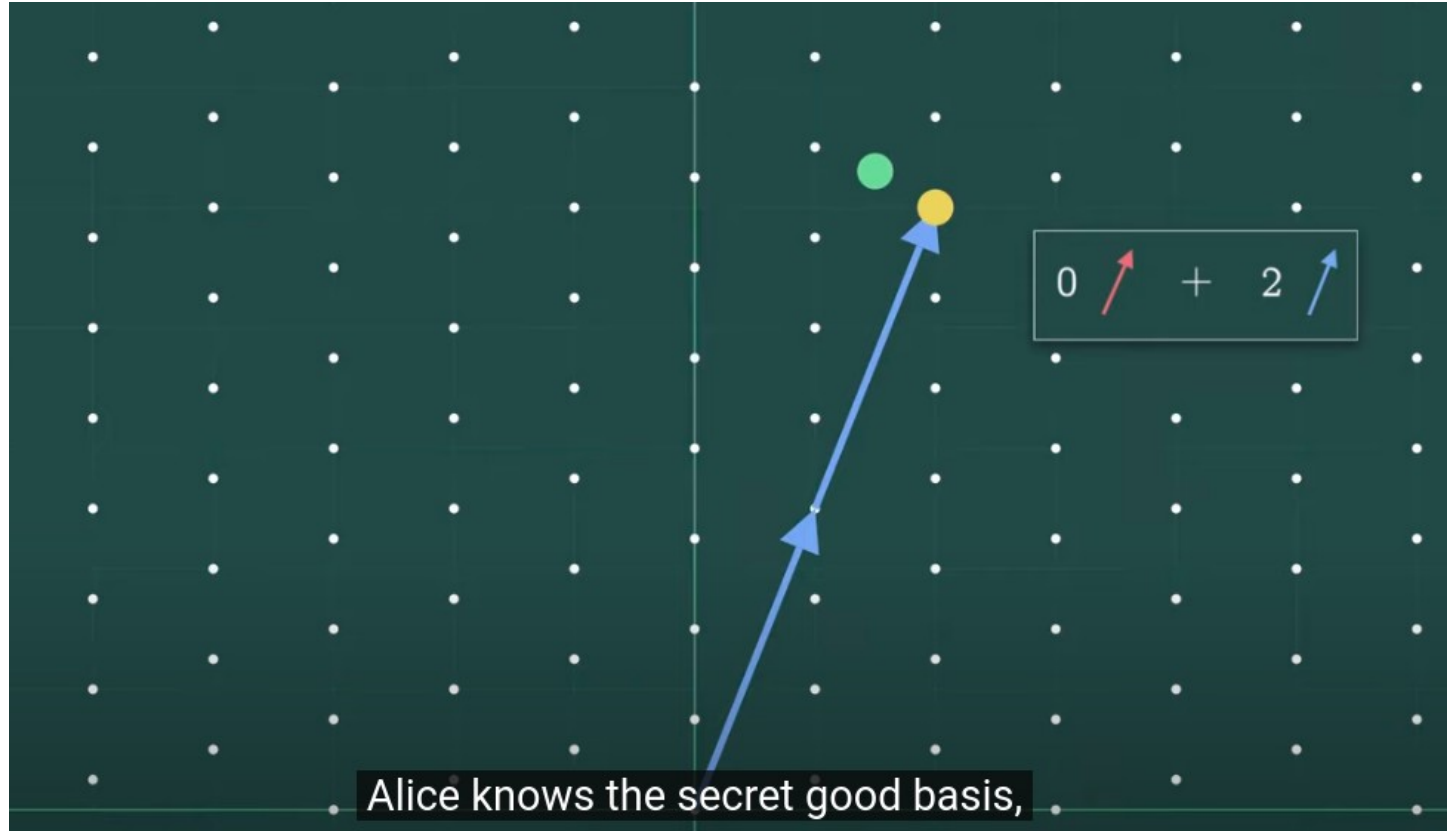
QKD vs. Quantum-resistant

- 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
 - *E.g.*, based on non-abelian hidden subgroup problem instead of abelian





<https://www.youtube.com/watch?v=QDdOoYdb748>
Lattice-based cryptography: The tricky math of dots



Alice knows the secret good basis,



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
 - Wrong answers cancel each other out *via* negative interference



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 for the past year or two