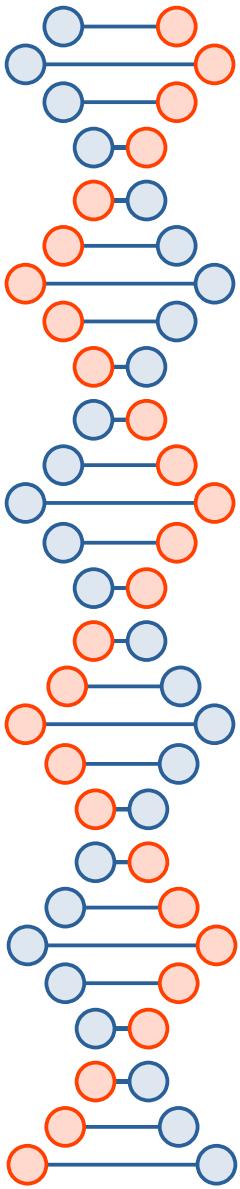


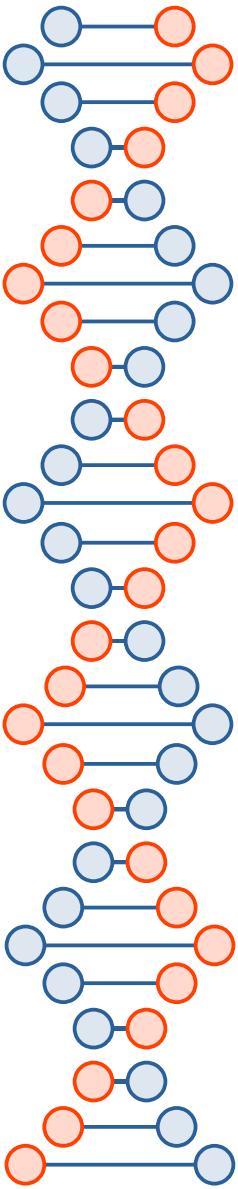
Brief overview of quantum computers, post-quantum cryptography

CSE 468 Fall 2025
jedimaestro@asu.edu



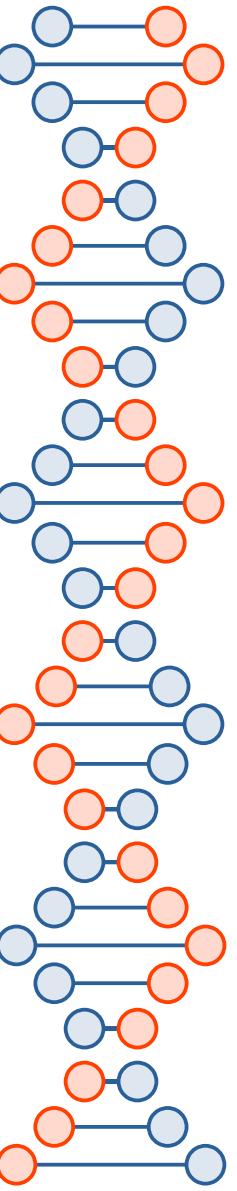
Open question: Does the universe permit private communications in the presence of an eavesdropper using only classical computation?

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



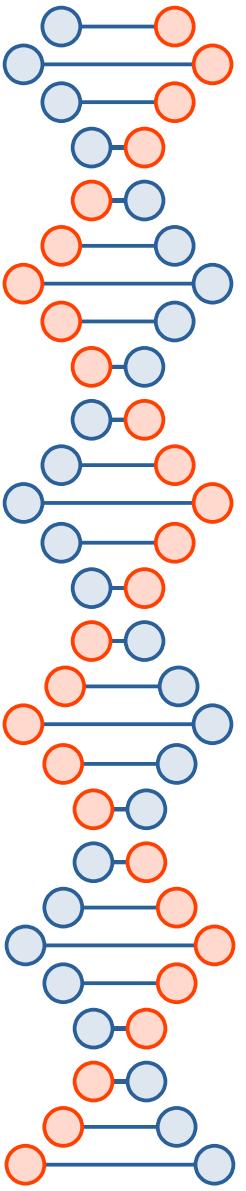
Open question: Does the universe permit ~~private communications~~ *non-repudiability* in the presence of an eavesdropper using only classical computation?

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

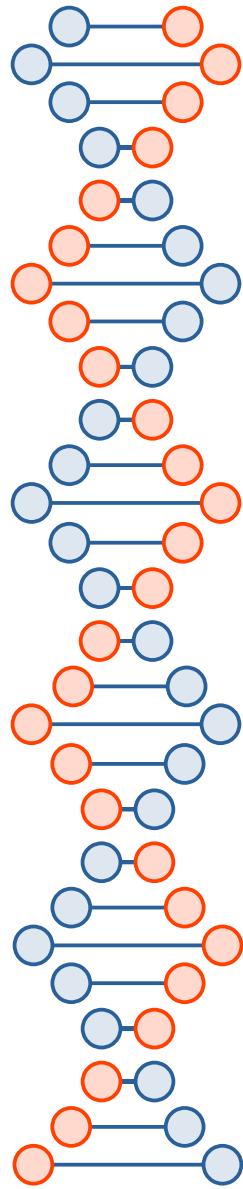


Why do we care?

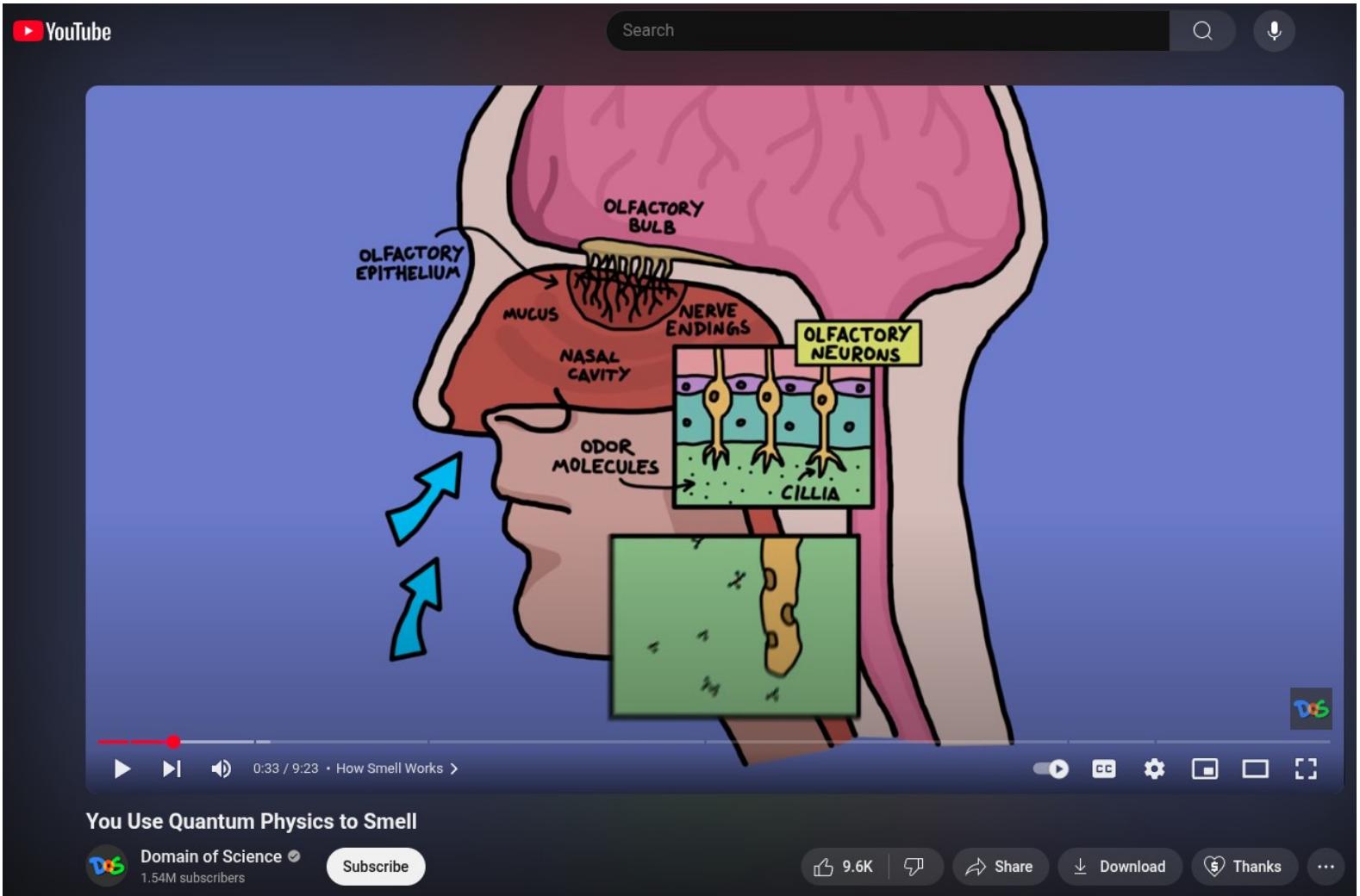
- Even schemes with perfect forward secrecy aren't secure against a quantum computer if they're not quantum resistant
 - Can be recorded now, broken later
- TLS, Tor, HTTPS certificates, WPA2, WPA3, 4G, 5G, WhatsApp, etc. are currently not "future proofed" against quantum computers
 - Signal is, but only for the past couple of years

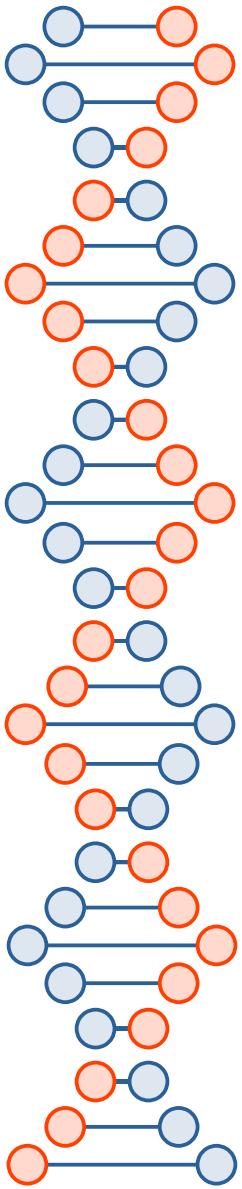


Quantum computation is all around you...

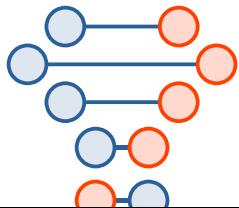


<https://www.youtube.com/watch?v=DJsJIVXkrGQ>





https://en.wikipedia.org/wiki/Sunstone_%28medieval%29

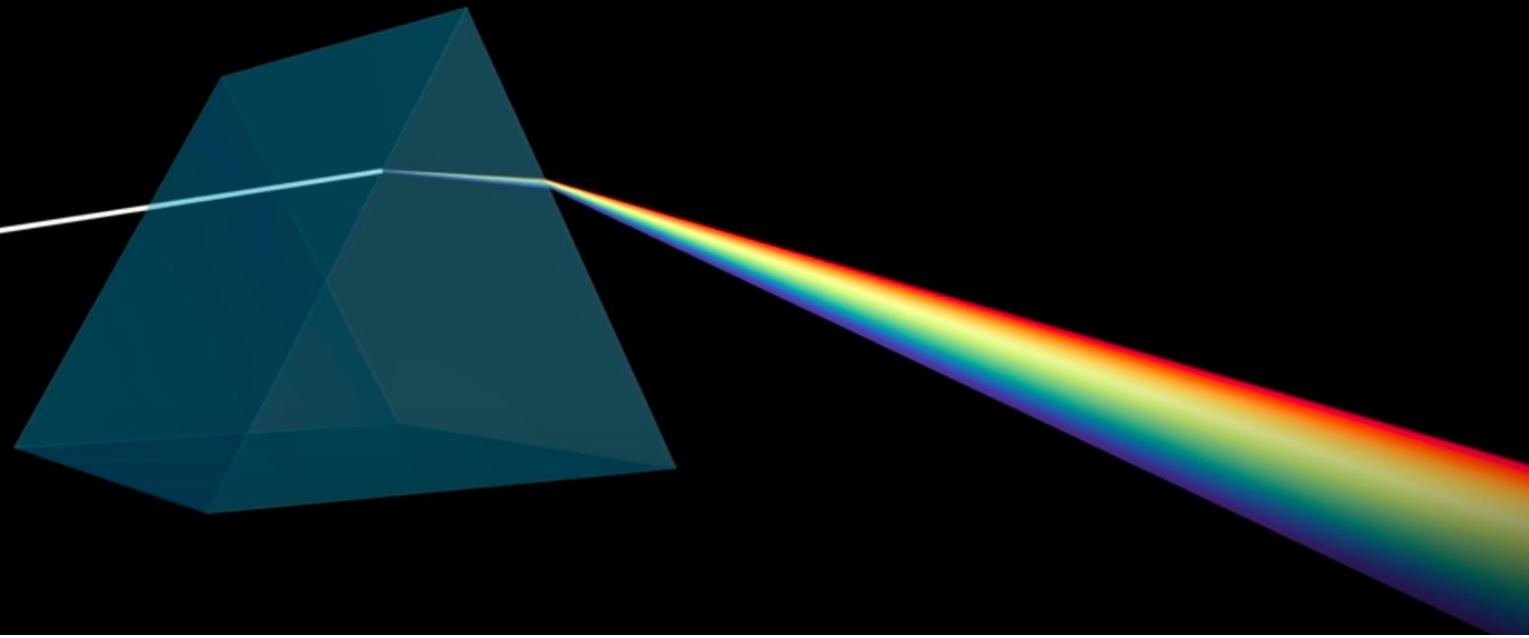


3brown1blue on YouTube...

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

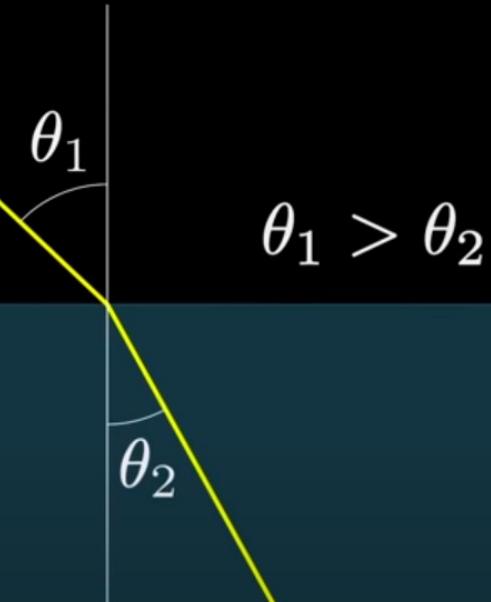


To exit full screen, press **Esc**

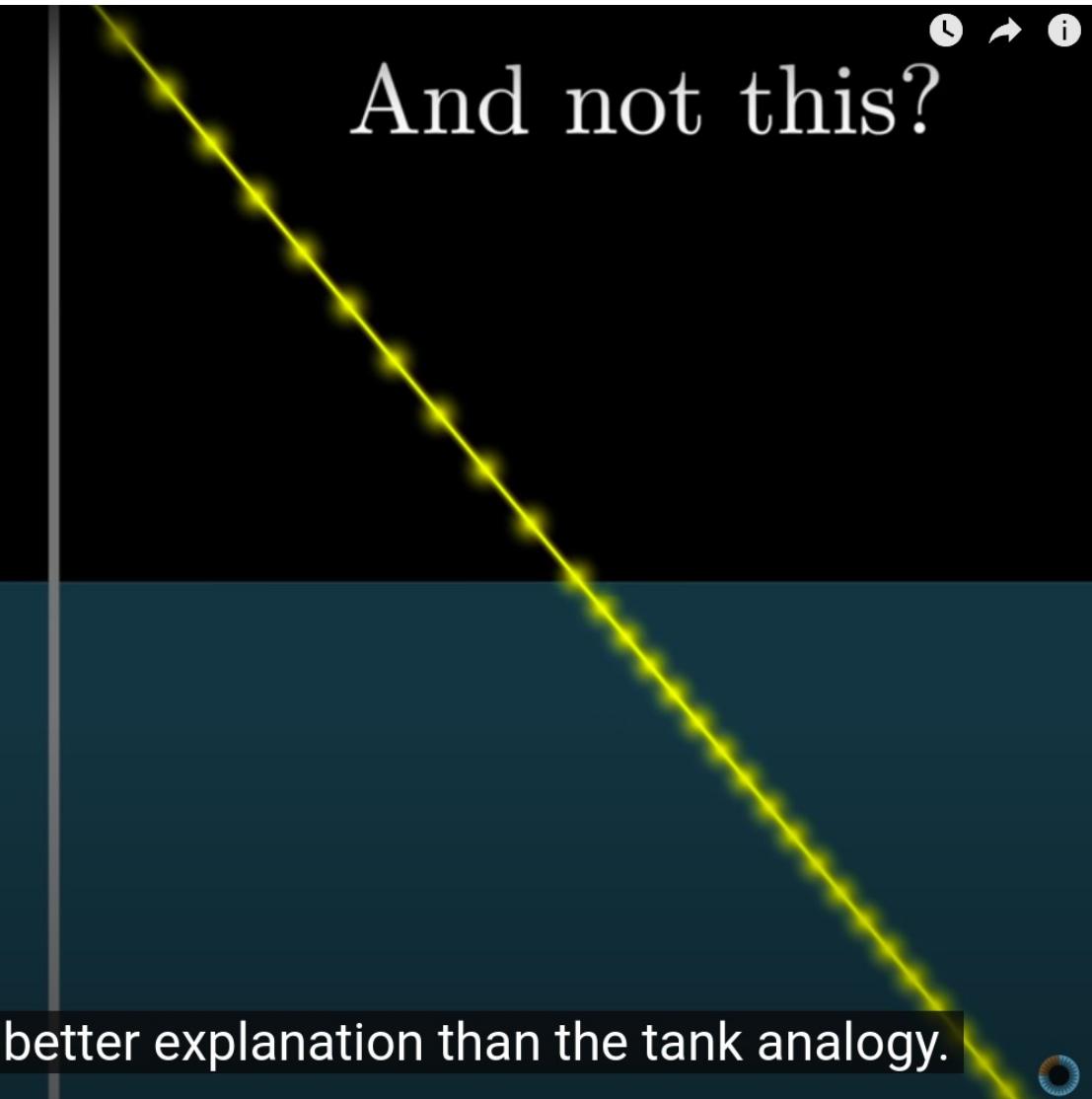




Why this?

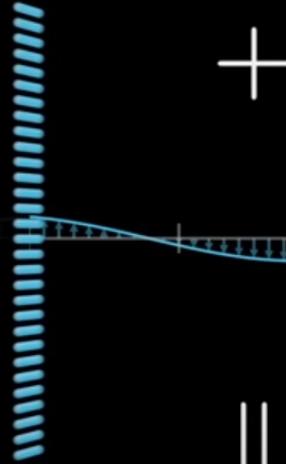
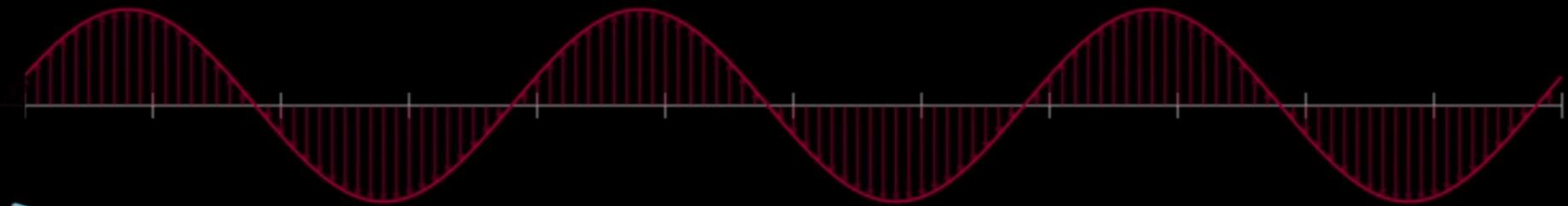


And not this?



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





Wave from layer oscillations

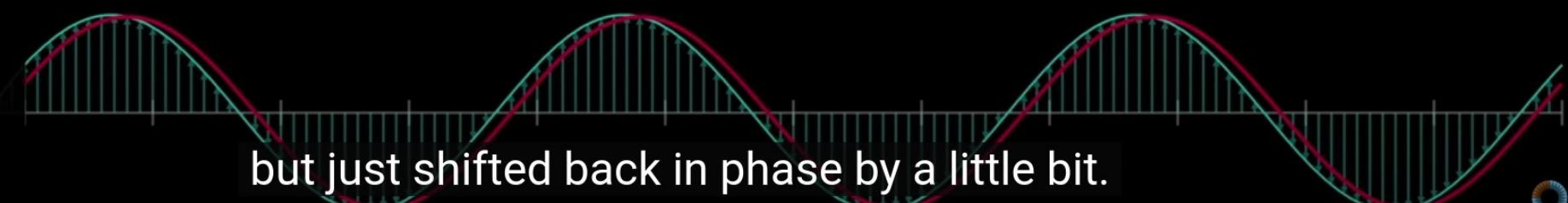


||

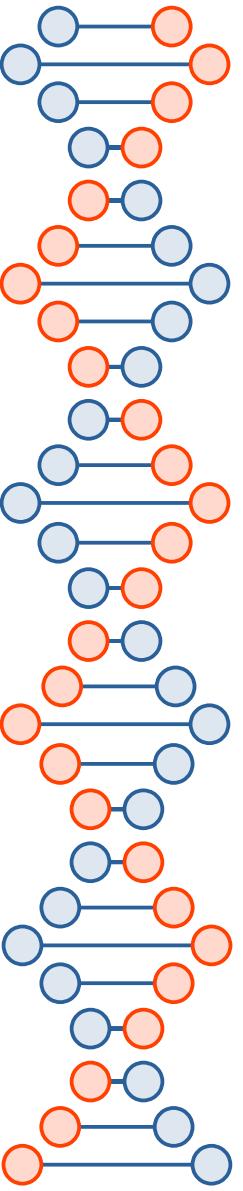
shift



Net effect



but just shifted back in phase by a little bit.



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

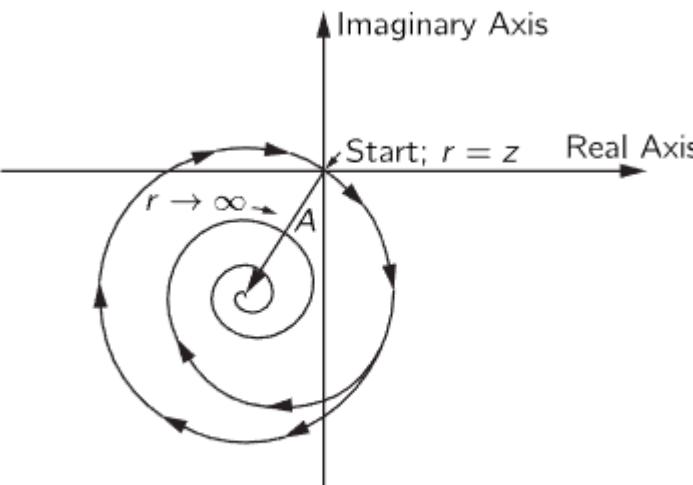
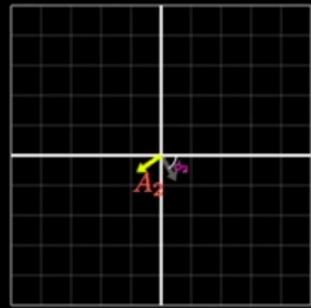
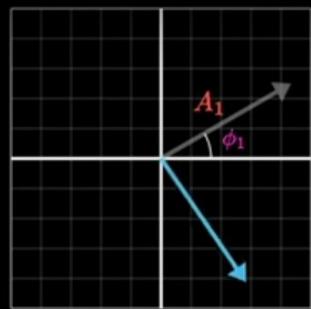


Fig. 30-12. Graphical solution of $\int_z^{\infty} \eta e^{-iwr/c} dr$.

Called an Euler spiral, or Cornu spiral.



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

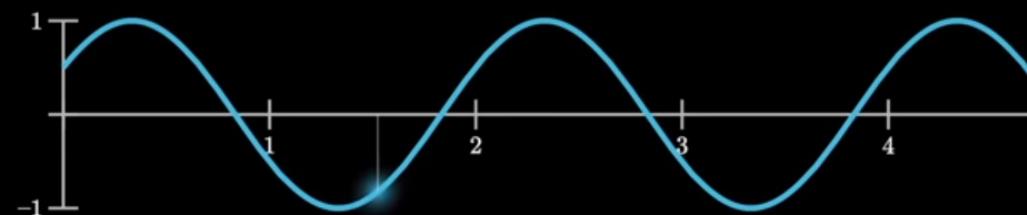


$$A_1 = 1.00$$

🔒 $\omega_1 = 3.14$

$$\phi_1 = 0.52$$

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

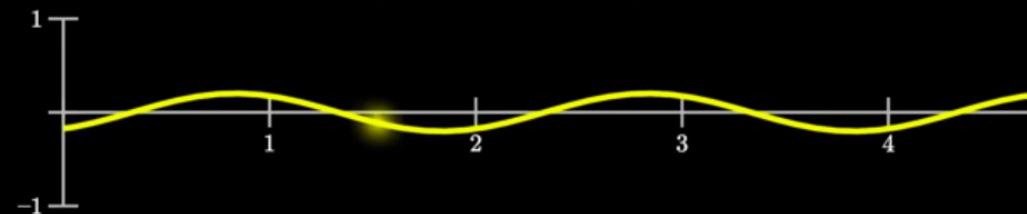


$$A_2 = 0.20$$

🔒 $\omega_2 = 3.14$

$$\phi_2 = -1.05$$

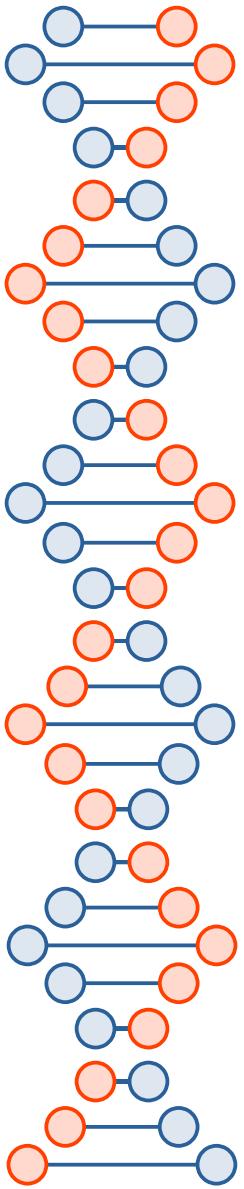
$$g(t) = A_2 \sin(\omega_2 t + \phi_2)$$



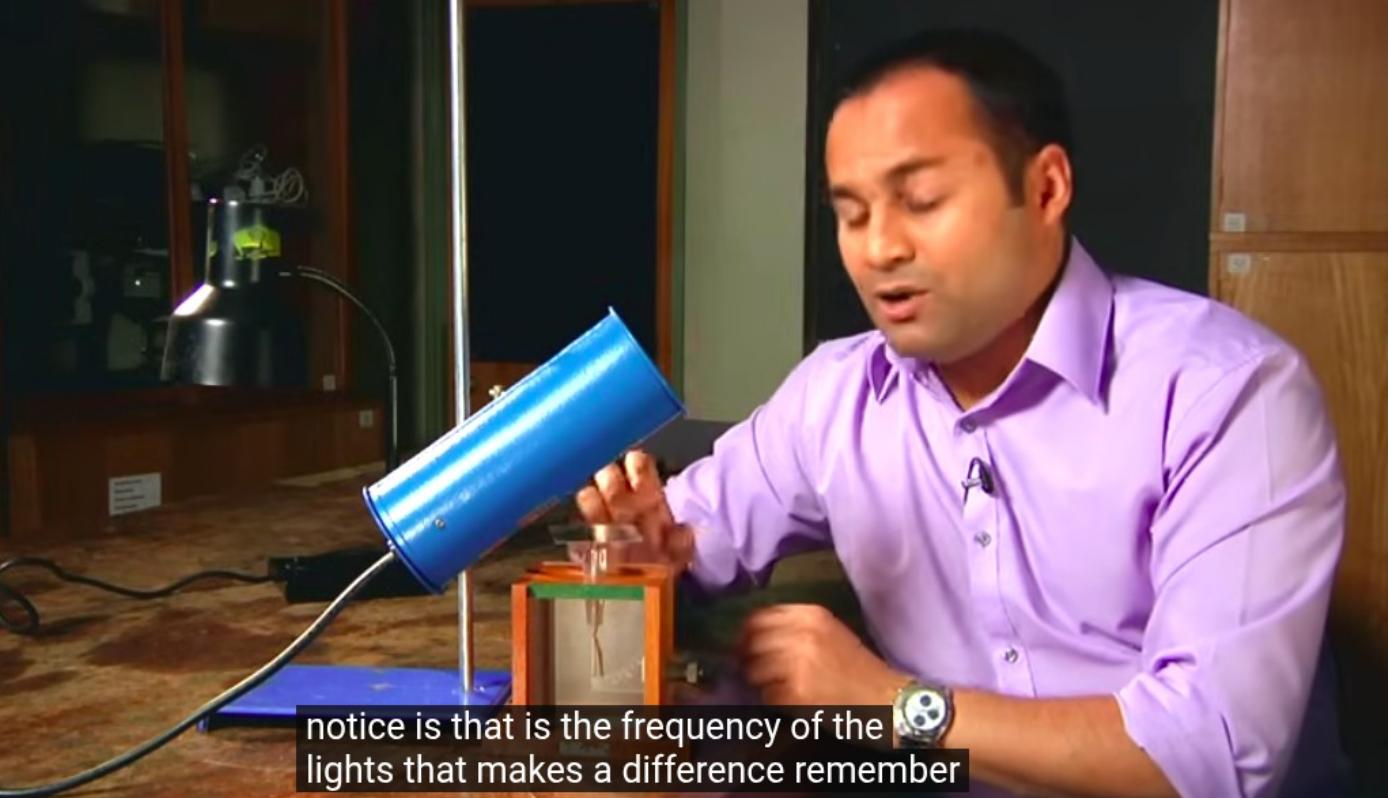
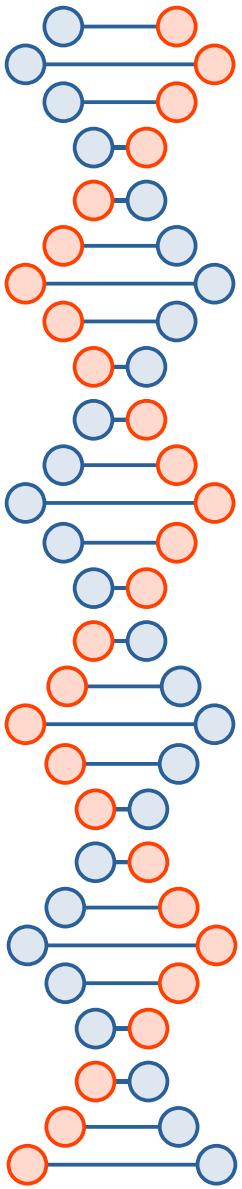
initial wave, but has just shifted back in its phase by a tiny bit.

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

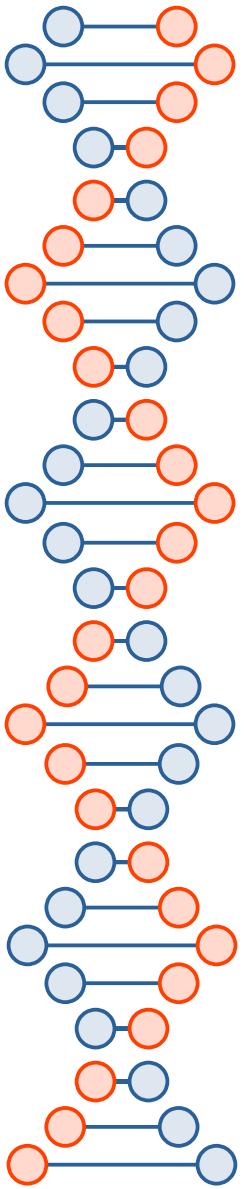




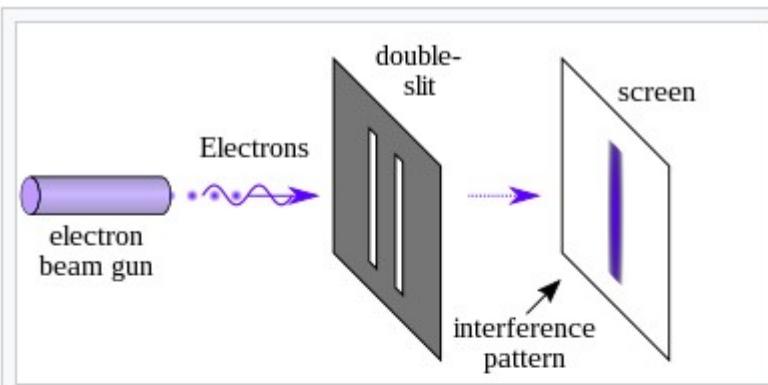
Is light a wave or a particle? Both? Sometimes one, sometimes the other? Neither?



<https://www.youtube.com/watch?v=v-1zjdUTu0o>



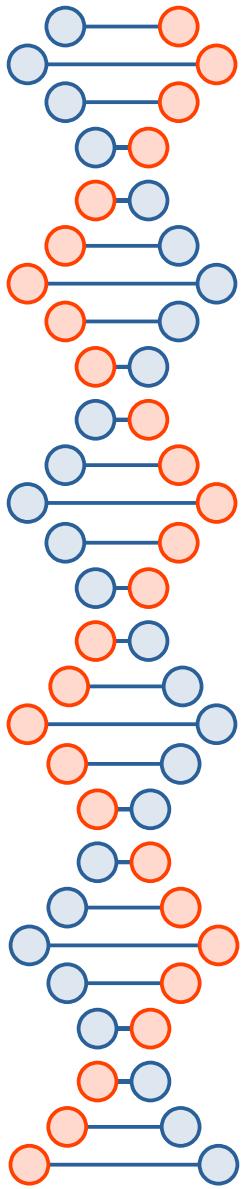
https://en.wikipedia.org/wiki/Double-slit_experiment



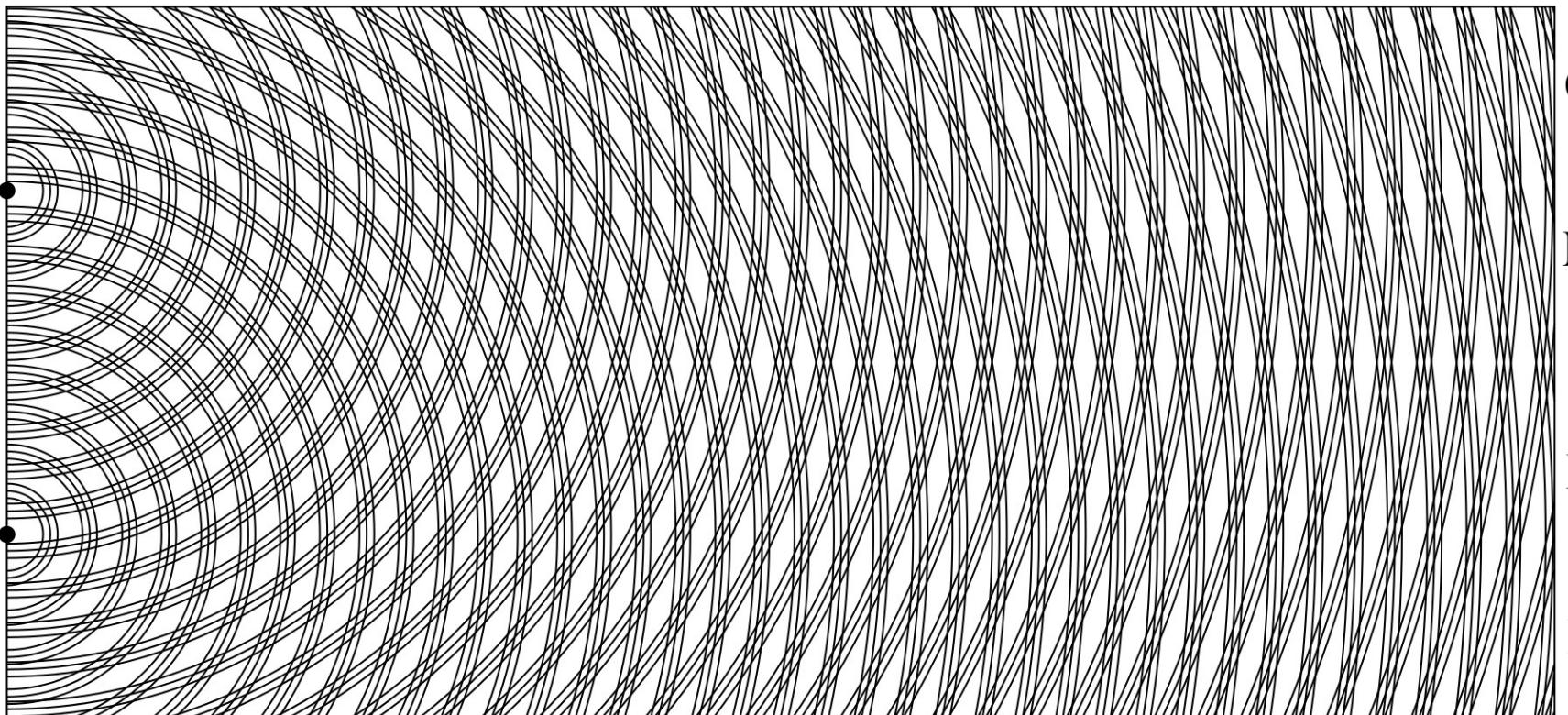
Photons or matter (like electrons) produce an interference pattern when two slits are used

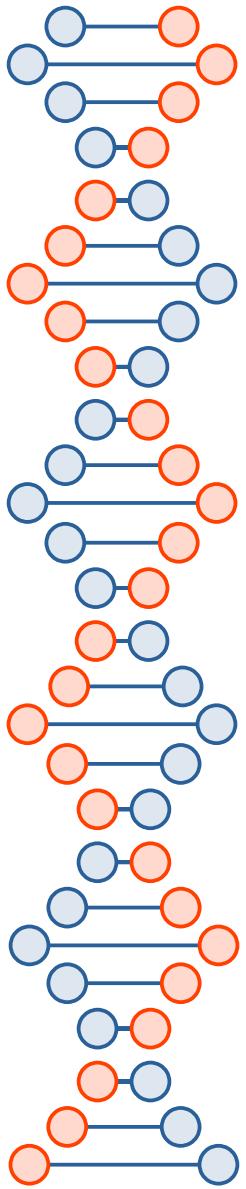


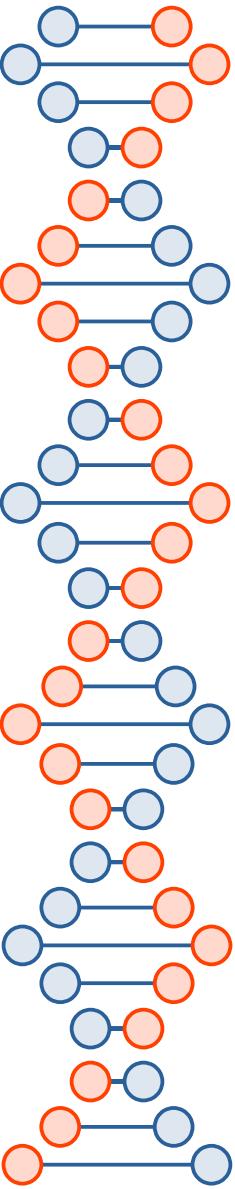
Light from a green laser passing through two slits 0.4mm wide and 0.1mm apart



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





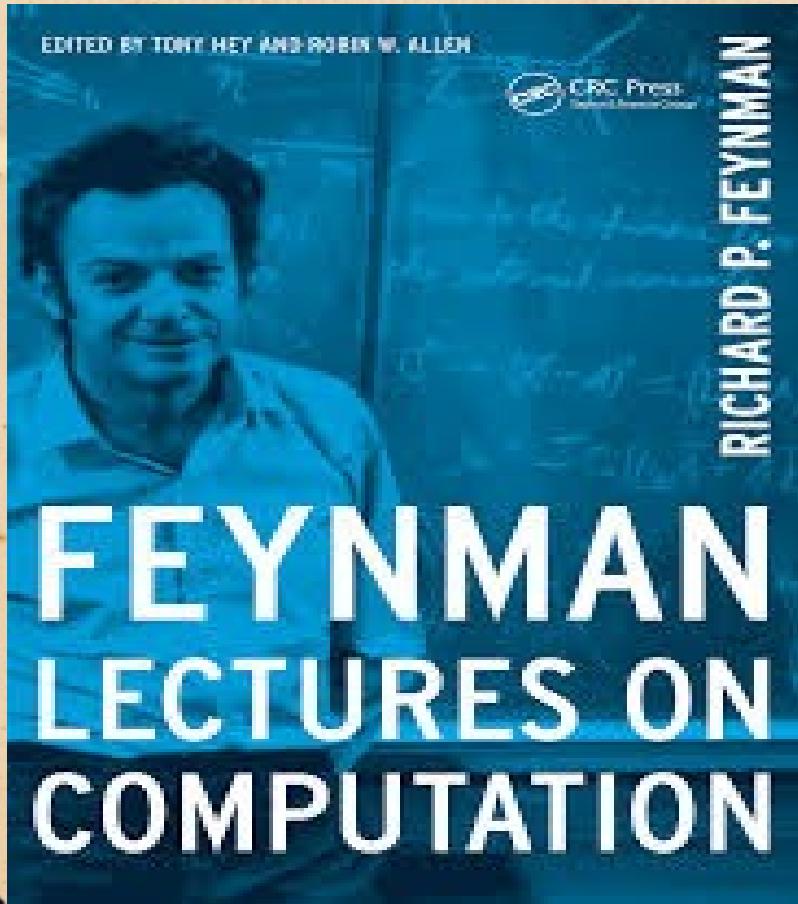


1–1 Atomic mechanics

“Quantum mechanics” is the description of the behavior of matter and light in all its details and, in particular, of the happenings on an atomic scale. Things on a very small scale behave like nothing that you have any direct experience about. They do not behave like waves, they do not behave like particles, they do not behave like clouds, or billiard balls, or weights on springs, or like anything that you have ever seen.

Newton thought that light was made up of particles, but then it was discovered that it behaves like a wave. Later, however (in the beginning of the twentieth century), it was found that light did indeed sometimes behave like a particle. Historically, the electron, for example, was thought to behave like a particle, and then it was found that in many respects it behaved like a wave. So it really behaves like neither. Now we have given up. We say: “It is like *neither*.”

https://www.feynmanlectures.caltech.edu/III_01.html

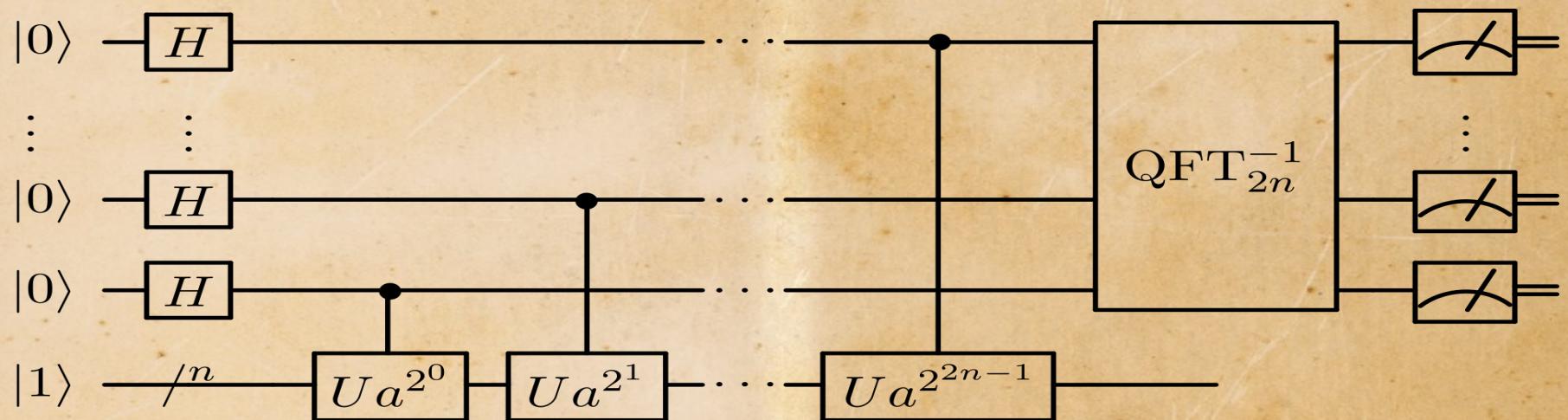


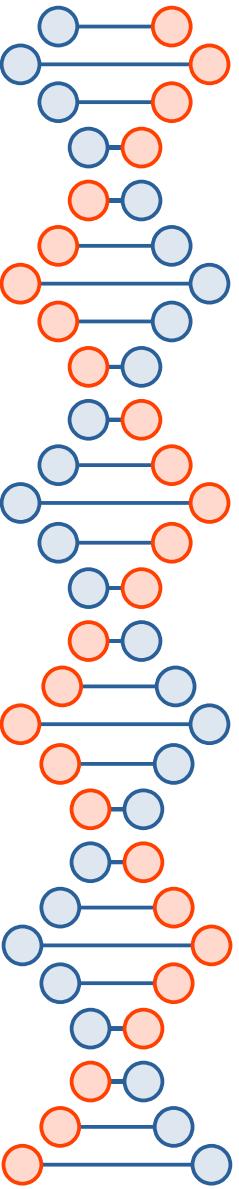
Lectures given 1983 through 1986...

“Another similar problem deals with factorization: I give you a number m , and tell you that it is the product of two primes, $m=pq$ It is possible to build our ignorance of the general solution of this mathematical problem into a ciphering message. ... The moment some clever guy cracks it ... we'd better find another one.” (page 91)

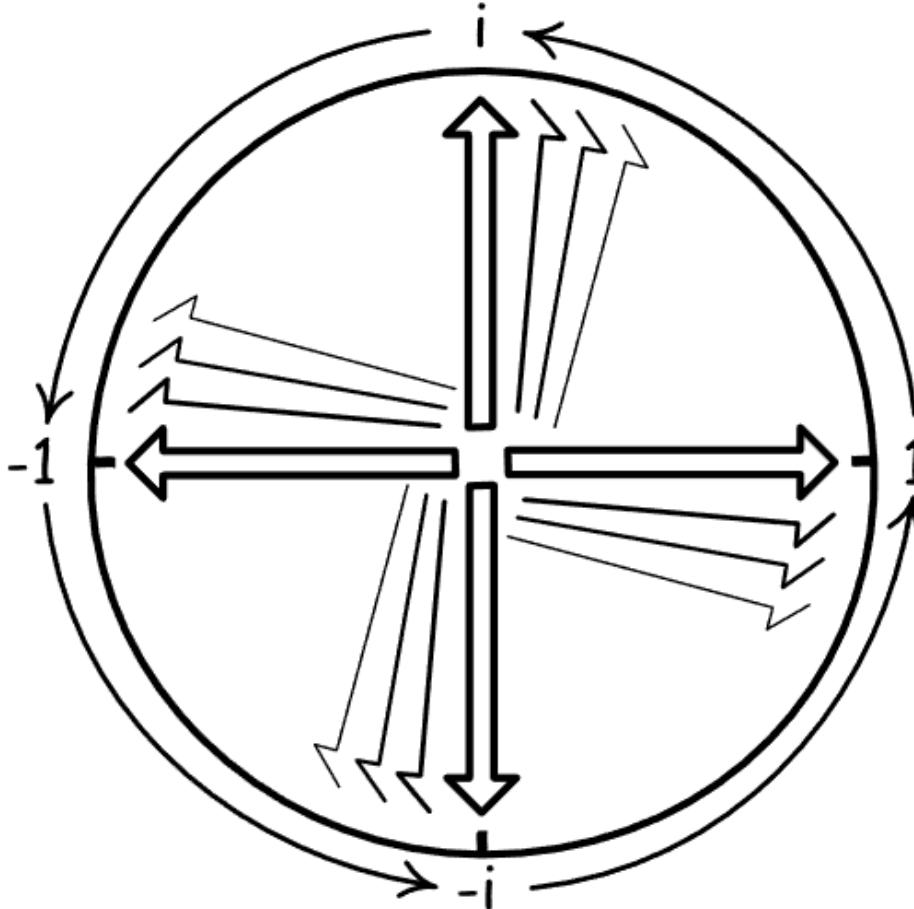
“What can be done, in these reversible quantum systems, to gain the speed available by concurrent operation has not been studied here.” (page 210)

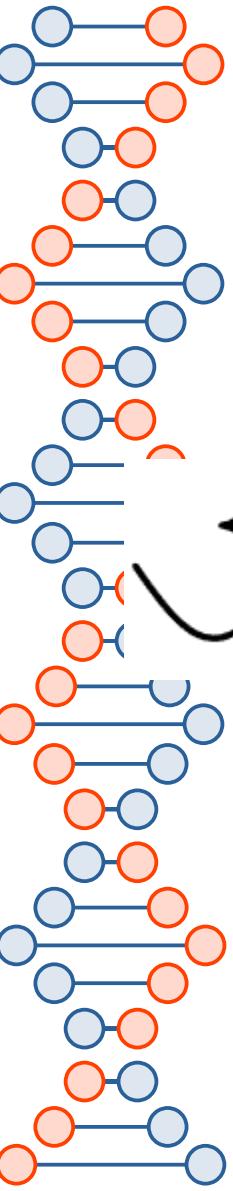
https://en.wikipedia.org/wiki/Shor%27s_algorithm



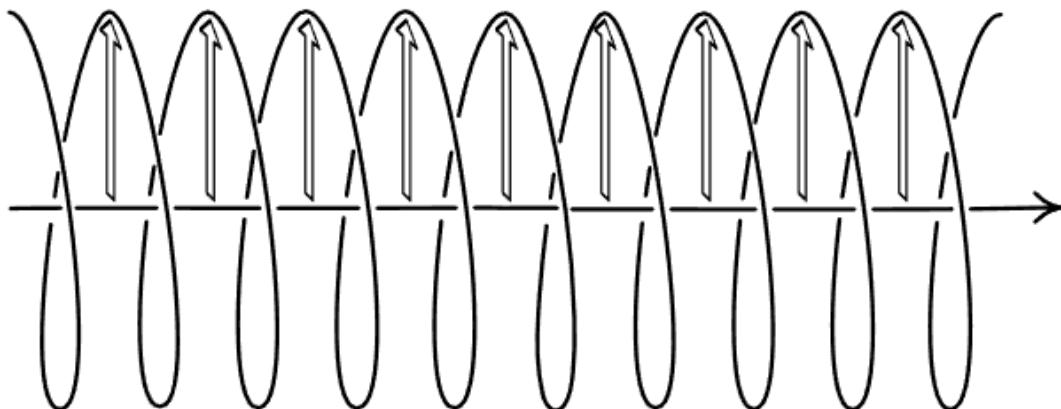
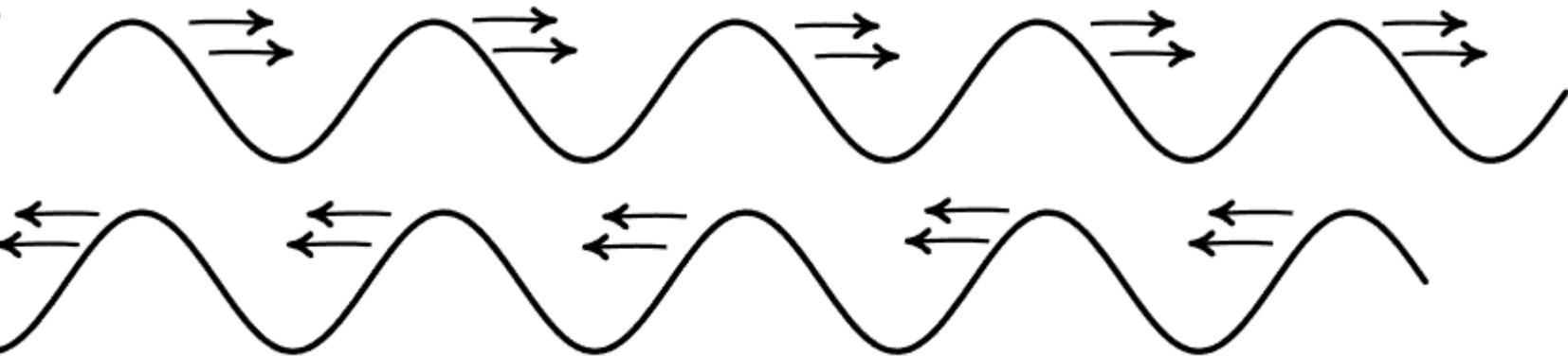


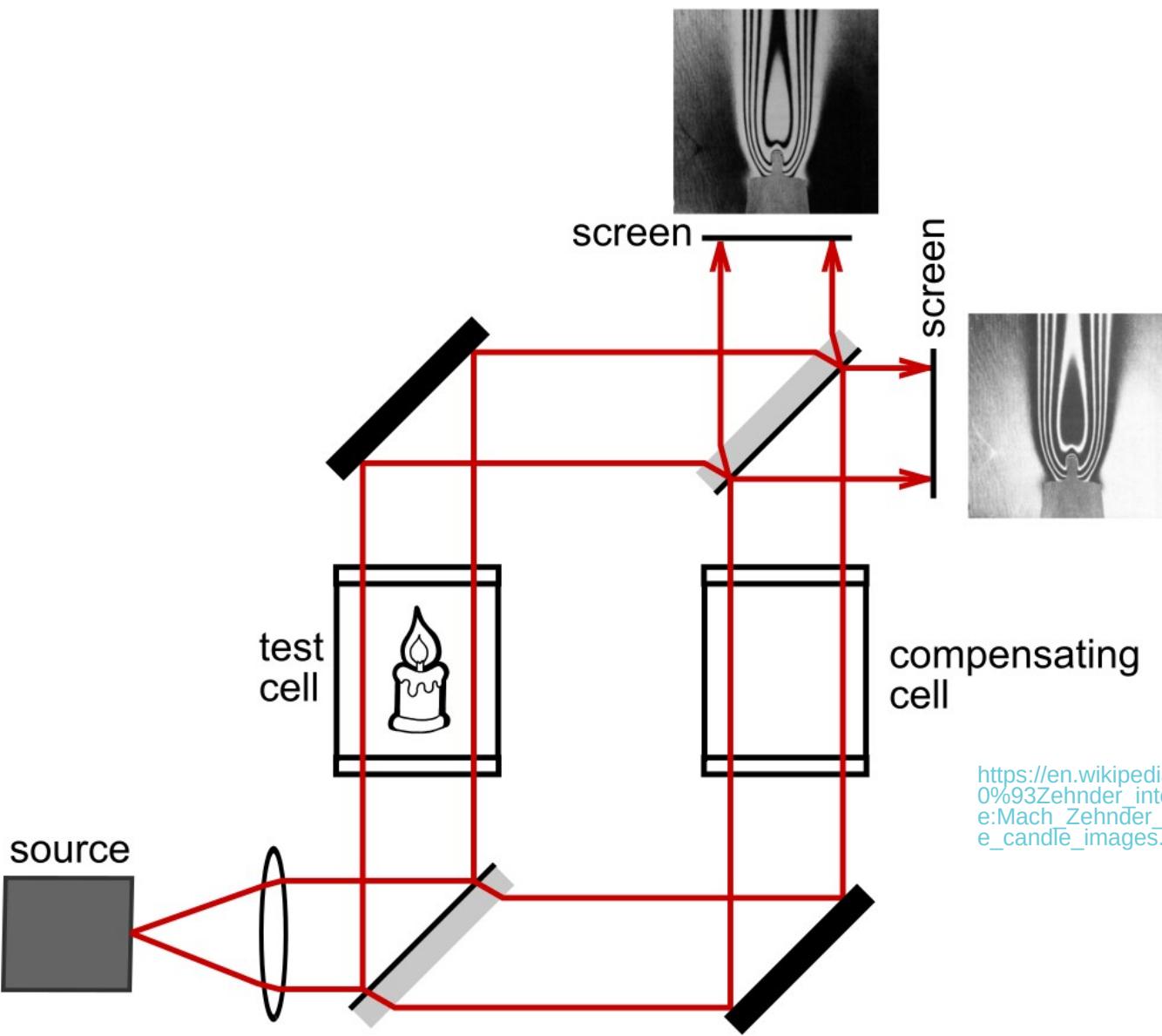
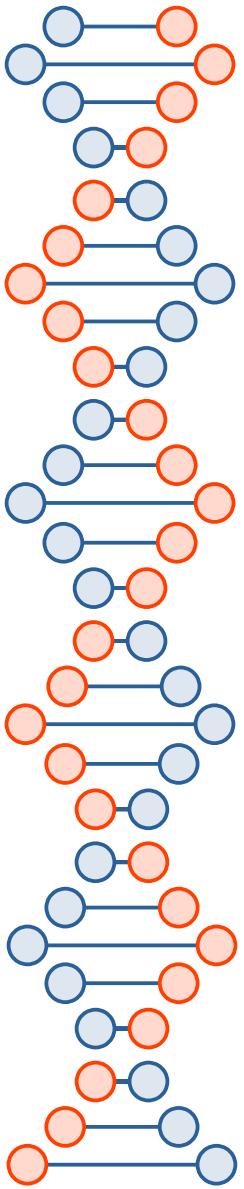
Complex waves are different...



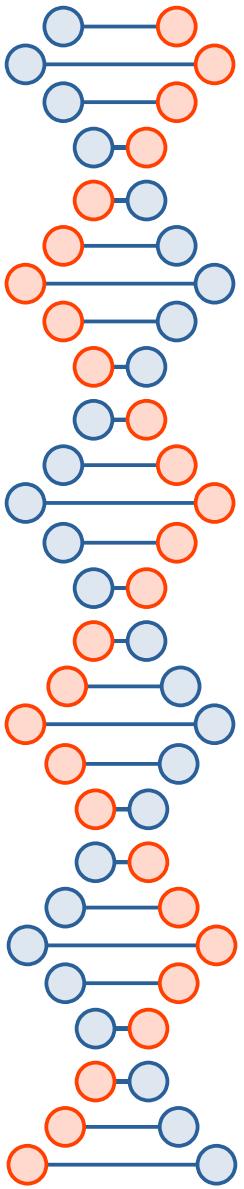


Complex waves have direction...

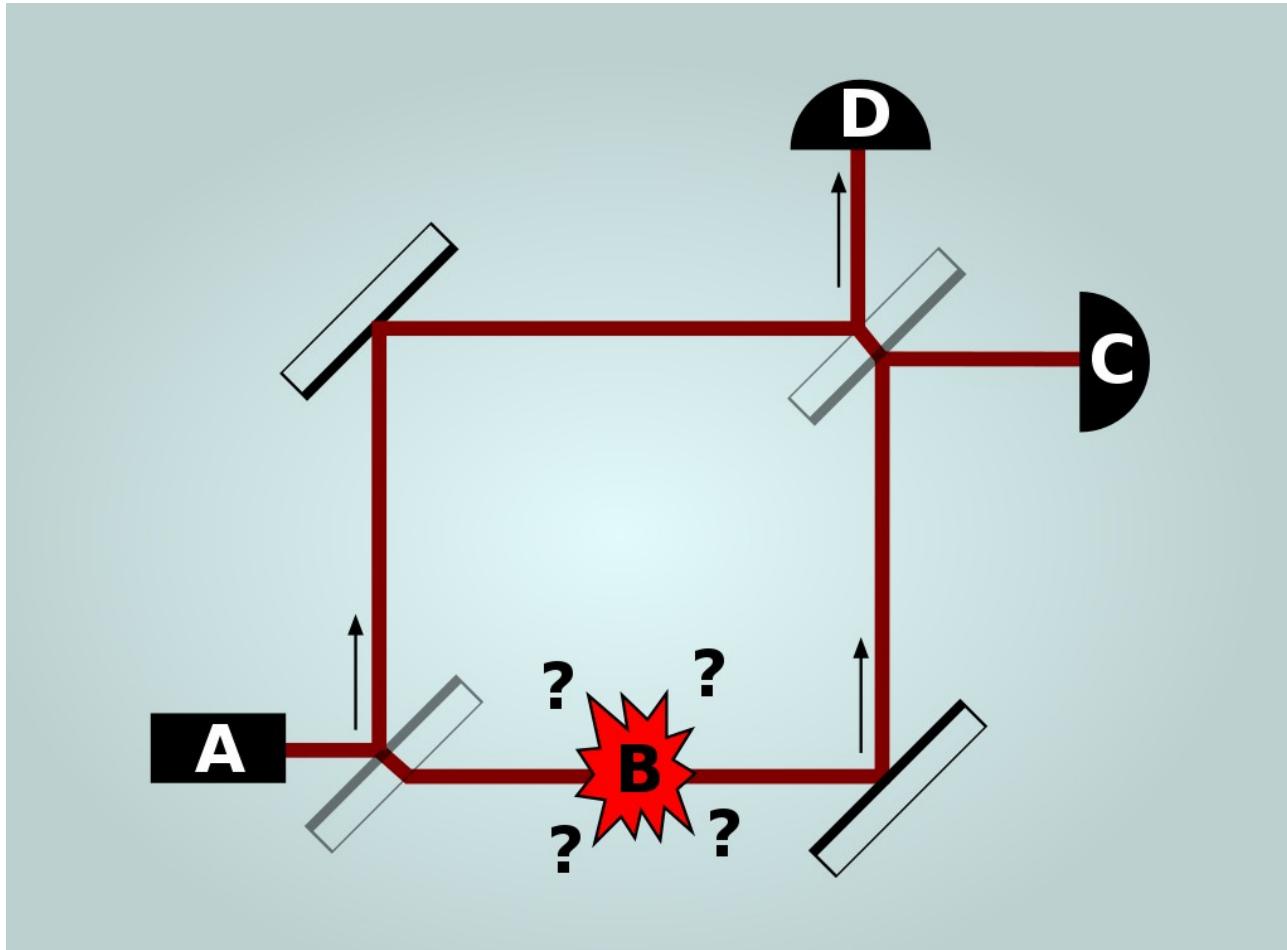


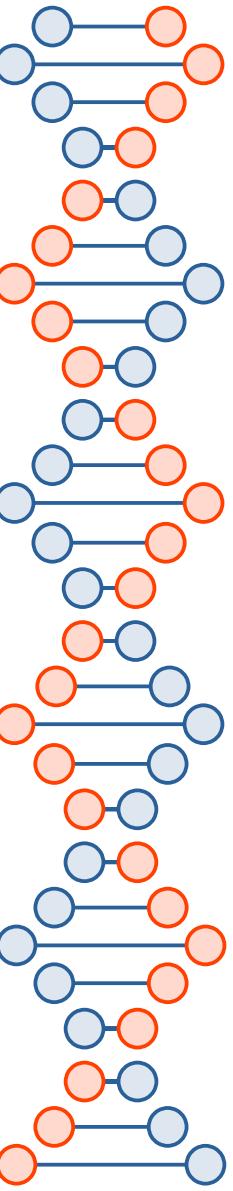


https://en.wikipedia.org/wiki/Mach%20Zehnder%20interferometer#/media/File:Mach_Zehnder_interferometer_alternate_candle_images.svg

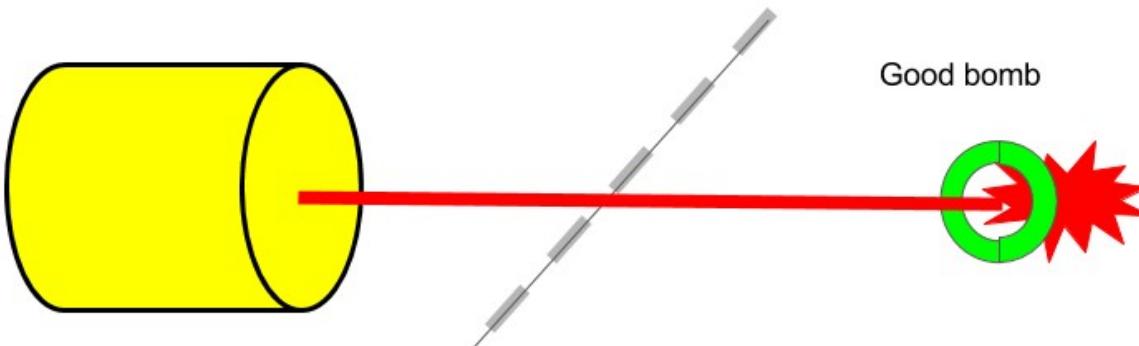


https://en.wikipedia.org/wiki/Elitzur%20Vaidman_bomb_tester

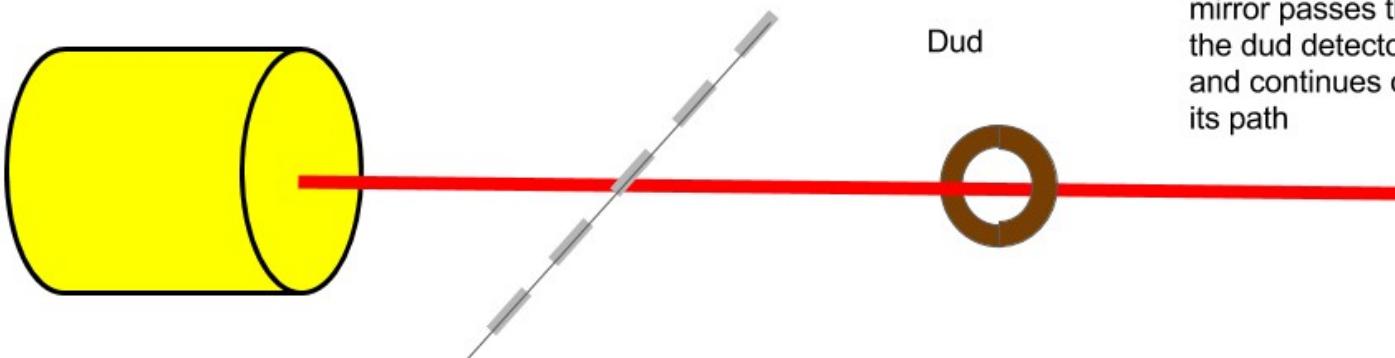




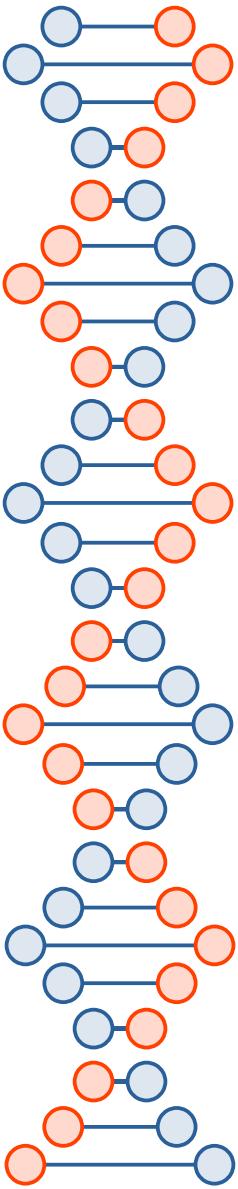
Bomb is either live or a dud



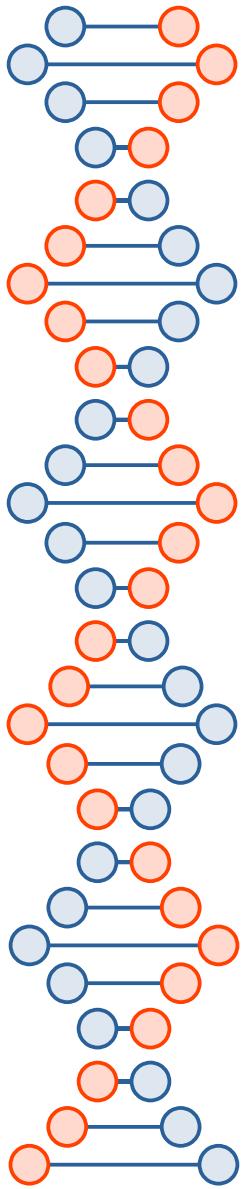
The photon that passed thru the mirror is detected by the bomb and explodes



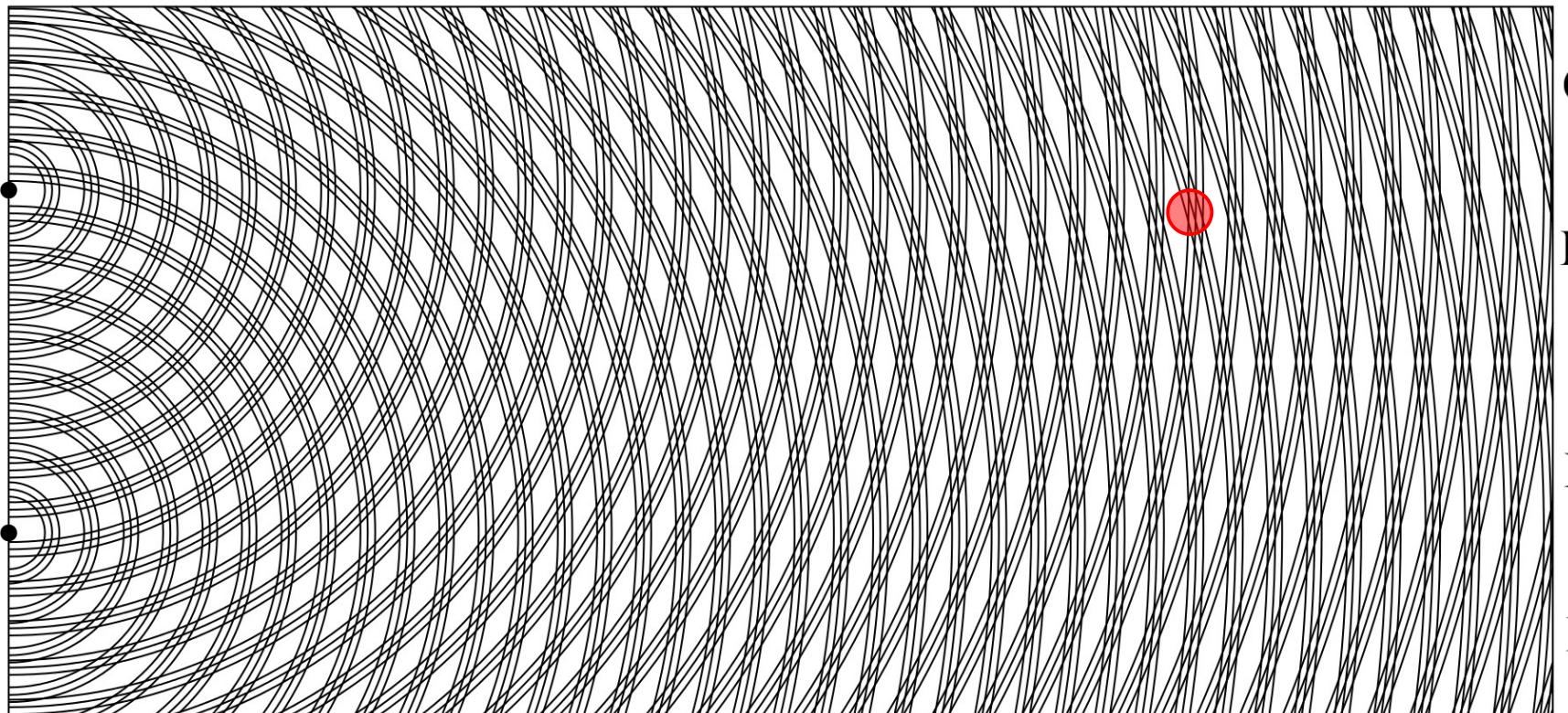
The photon that passed thru the mirror passes thru the dud detector and continues on its path

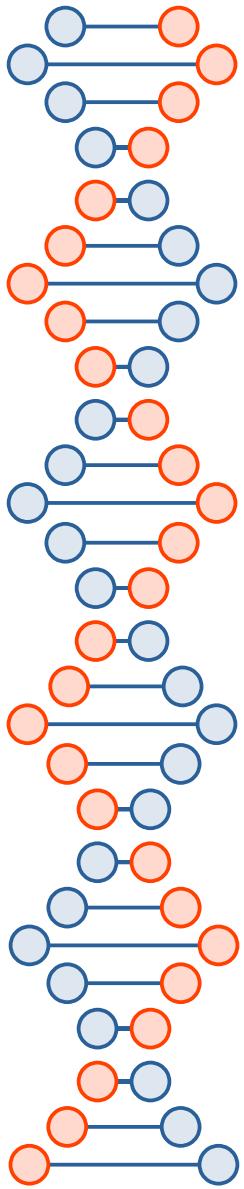


“Due to the way in which the interferometer is constructed, a photon going through the second mirror from the lower path towards detector D will have a phase shift of half a wavelength compared to a photon being reflected from the upper path towards that same detector...”

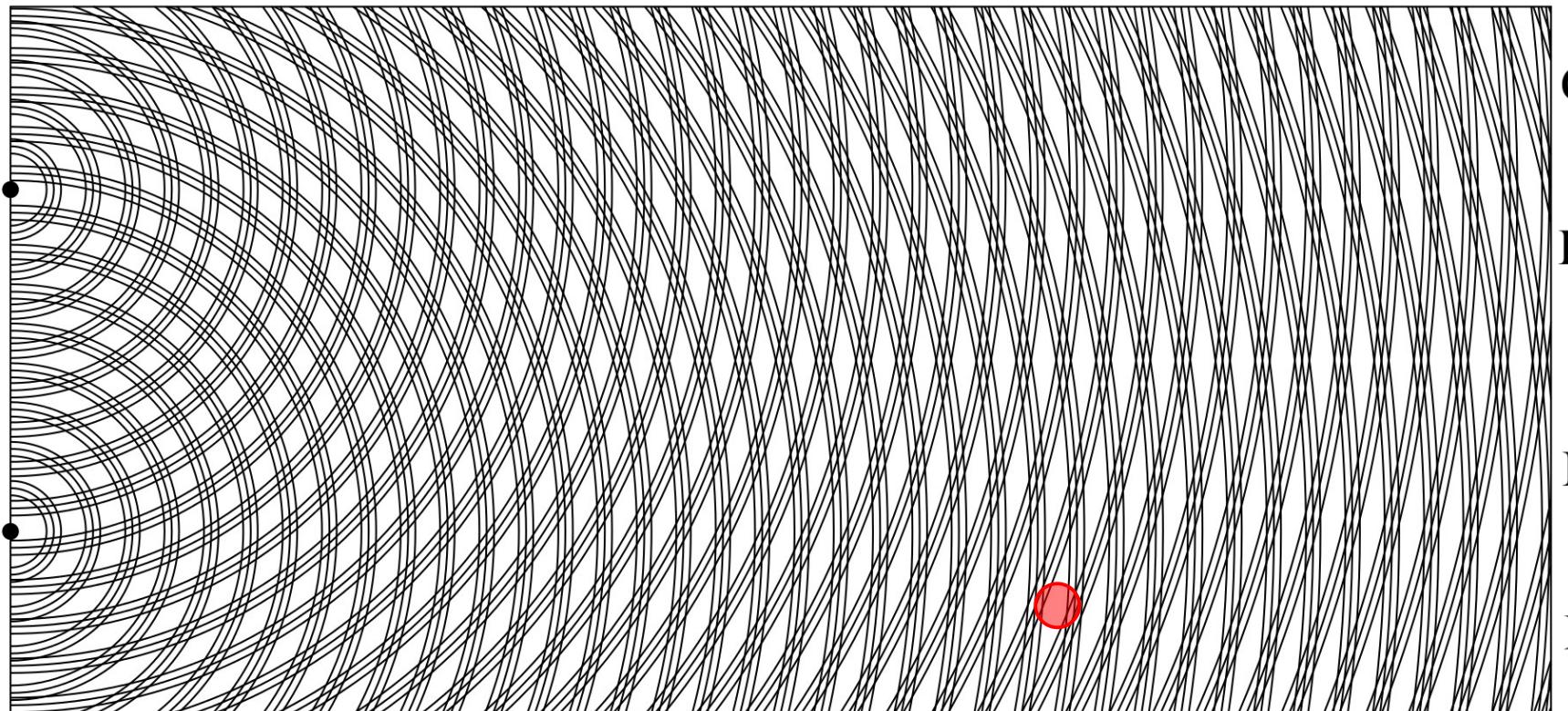


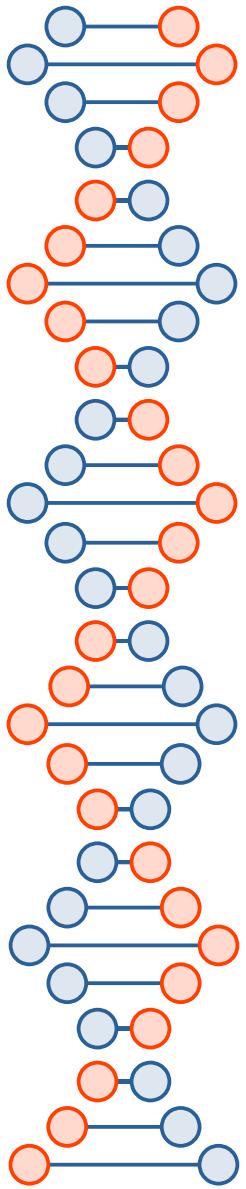
Put C, *e.g.*, here...



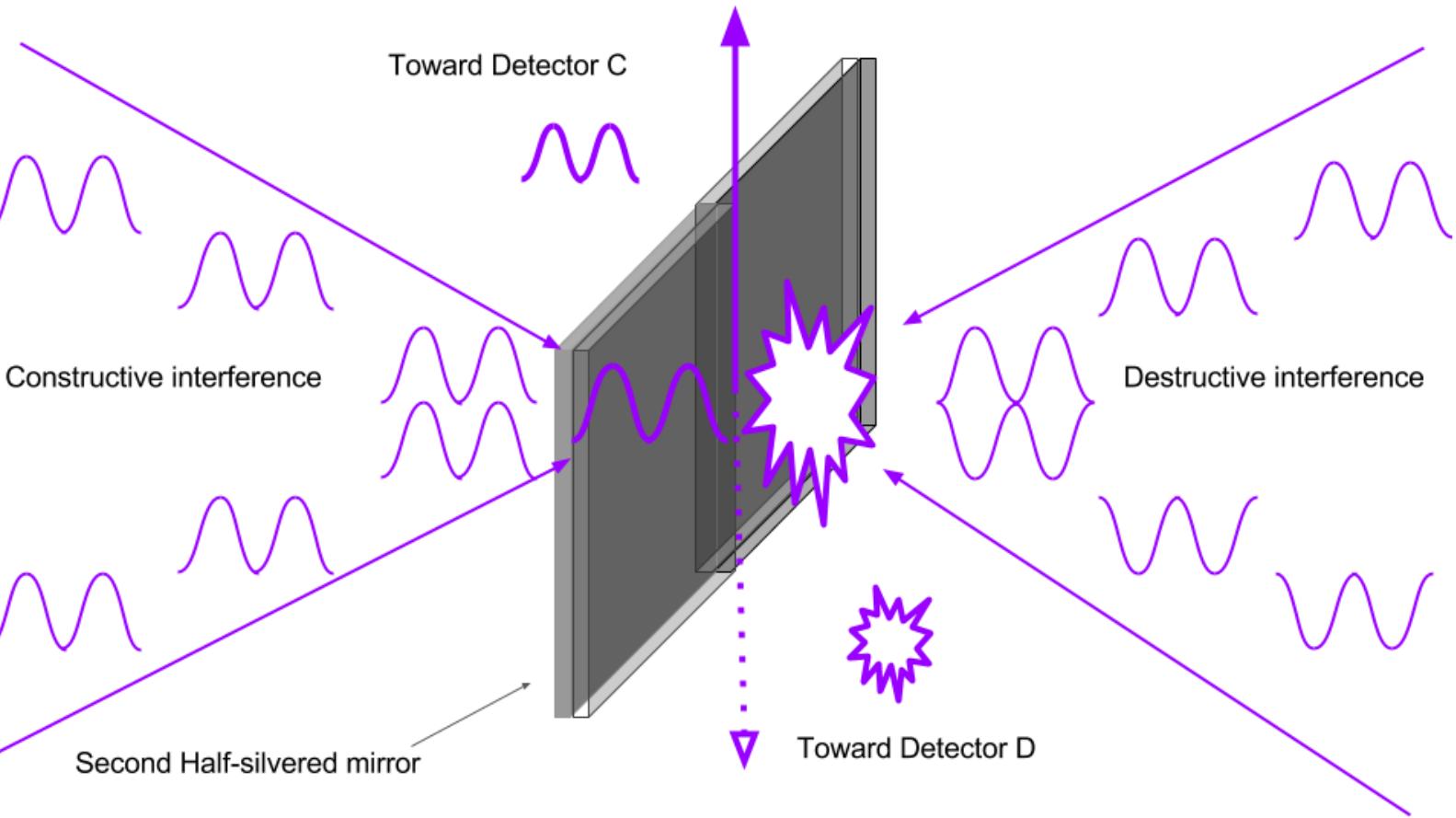


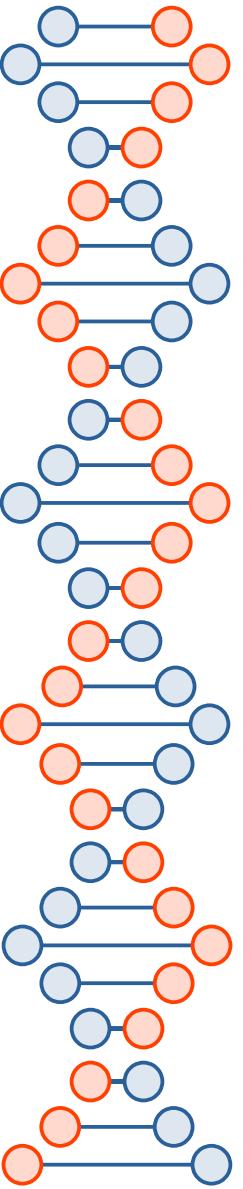
Put D, e.g., here...





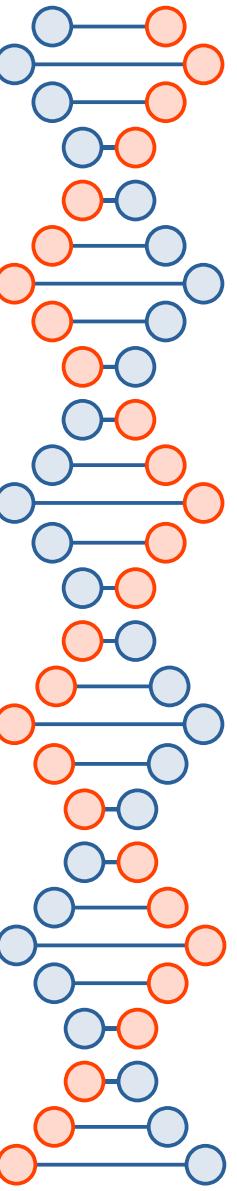
If both waves make it to the end (dud!)...





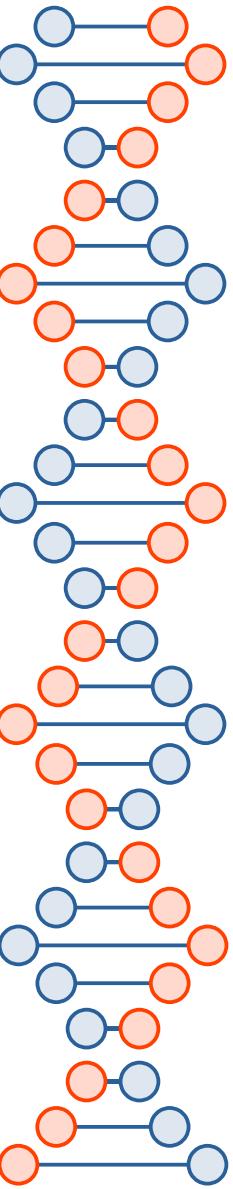
We will never detect a photon at D if the bomb is a dud.

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



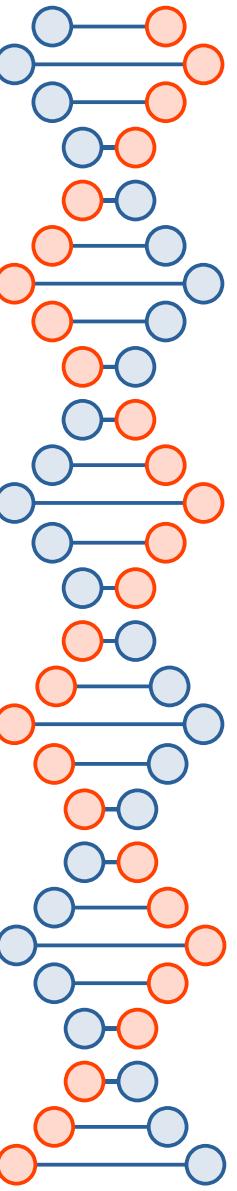
Case #1: Bomb is a dud

- 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



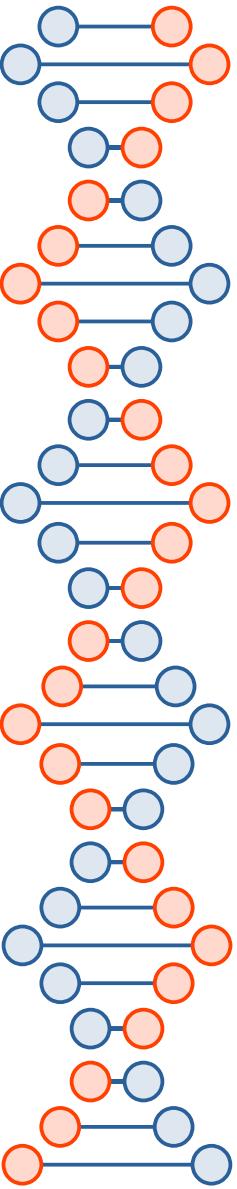
Case #2: Bomb is live

- 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
 - Live bomb detected!



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 states until you observe it
 - These probabilities can be entangled

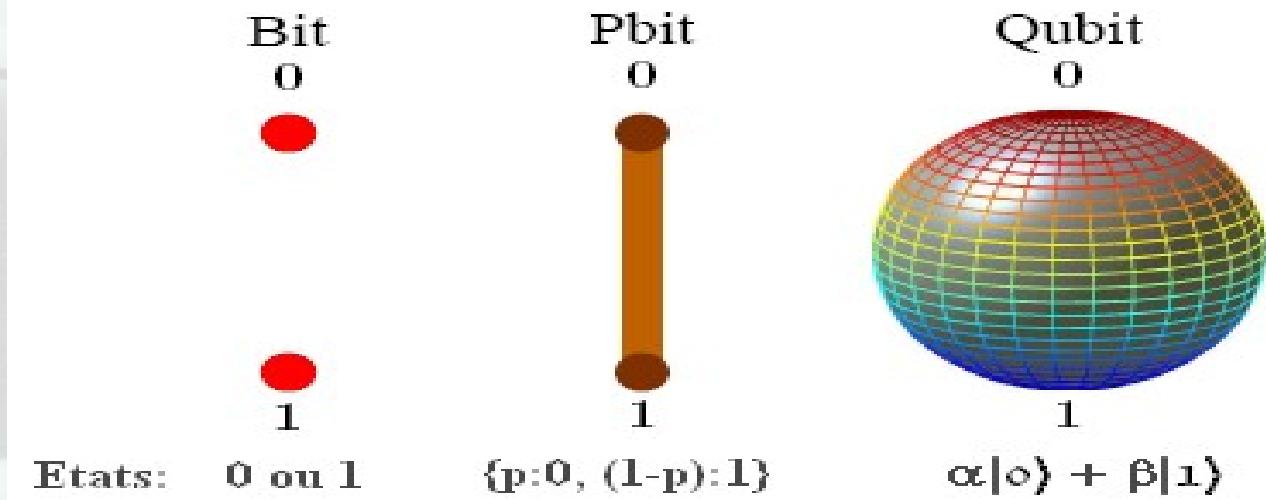
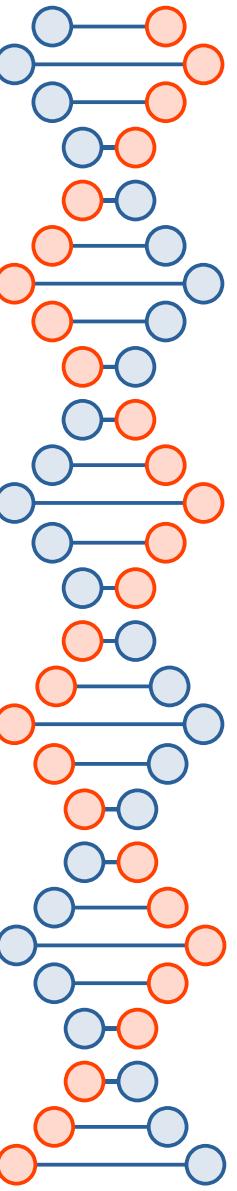
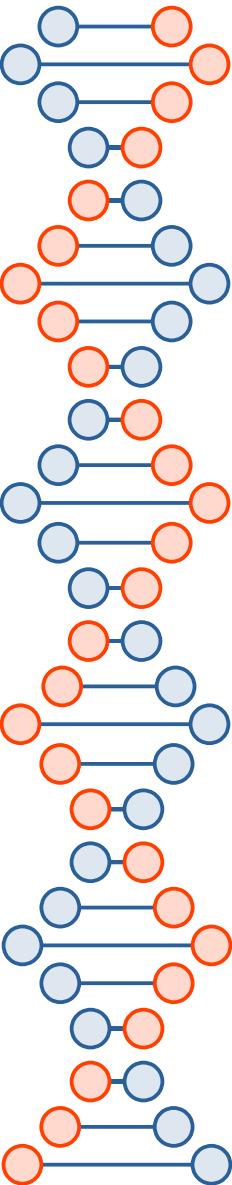


Image taken from <http://filipchsqroom.blogspot.com/>



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)

$$\text{Qubit 0 } |\psi_0\rangle = \alpha|0\rangle + \beta|1\rangle \quad \text{Qubit } |\psi_1\rangle = \gamma|0\rangle + \delta|1\rangle$$

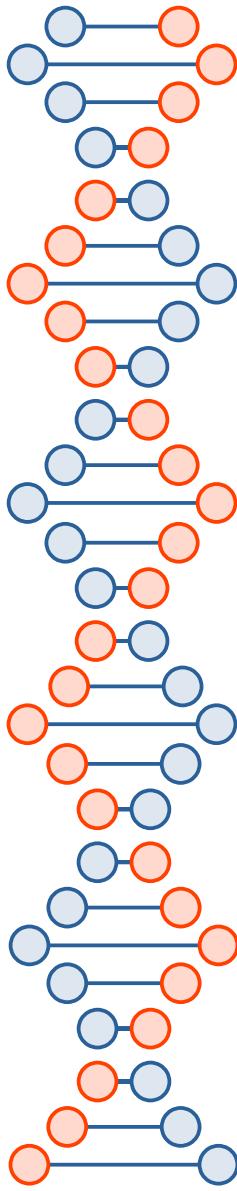
$$|\psi\rangle = \alpha\gamma|00\rangle + \alpha\delta|01\rangle + \beta\gamma|10\rangle + \beta\delta|11\rangle$$



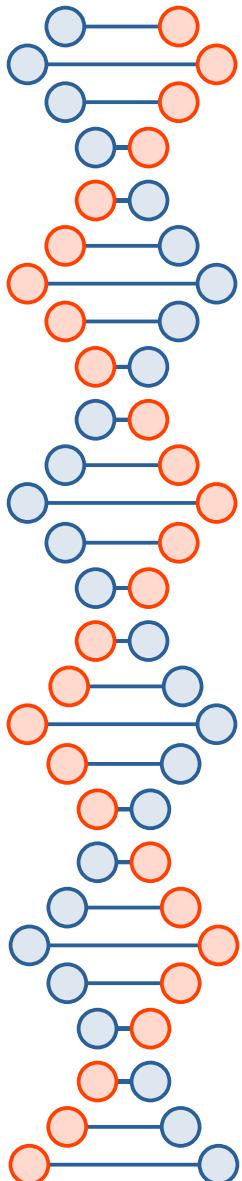
This operation is called **Tensor Product**

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

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



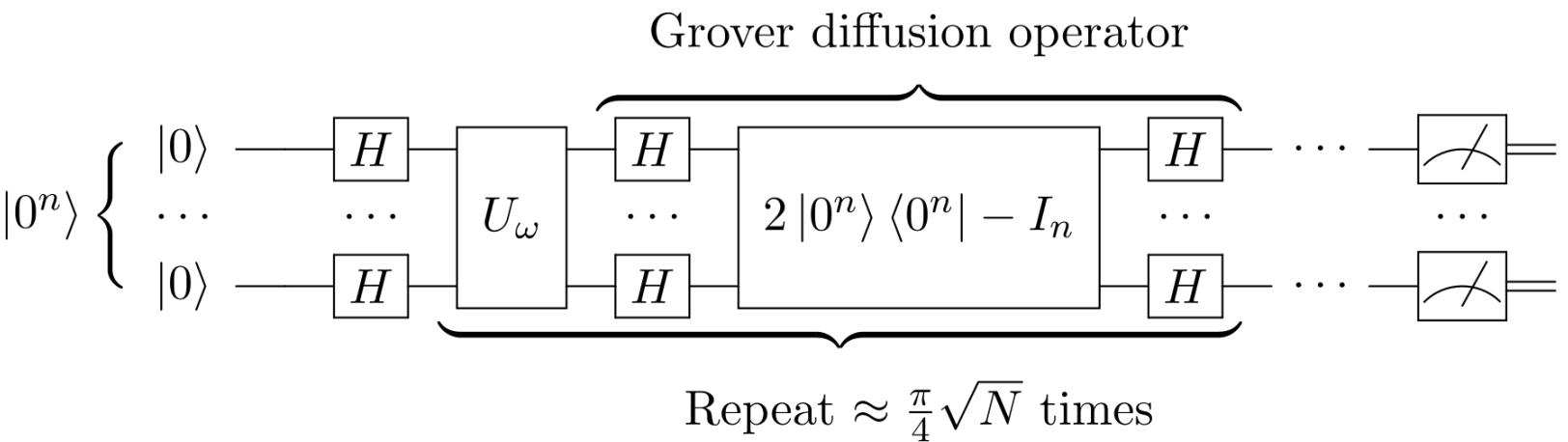
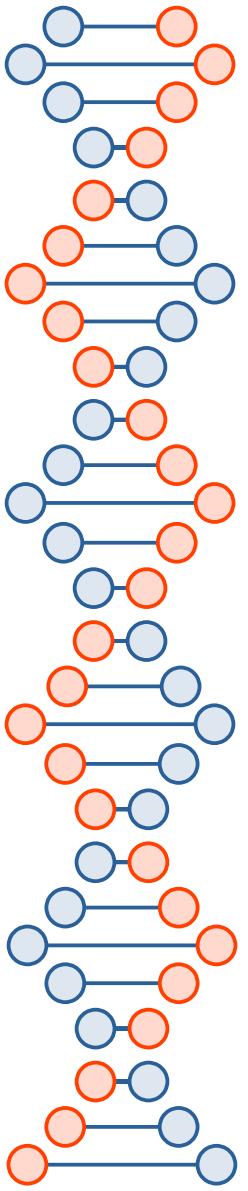
<https://www.cnet.com/tech/computing/quantum-computer-makers-like-their-odds-for-big-progress-soon/>



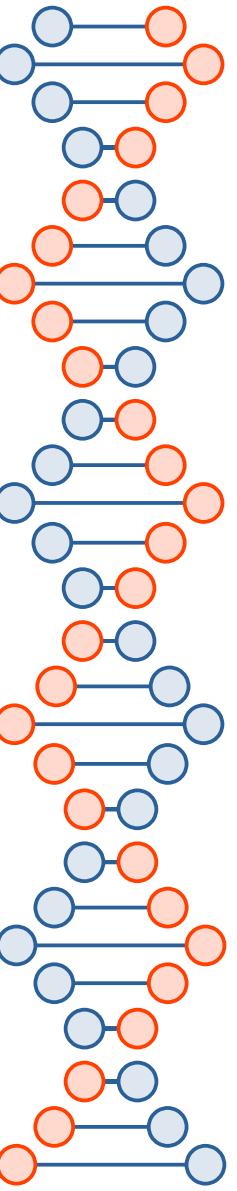
What we need for the Internet to work...

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

Grover's algorithm

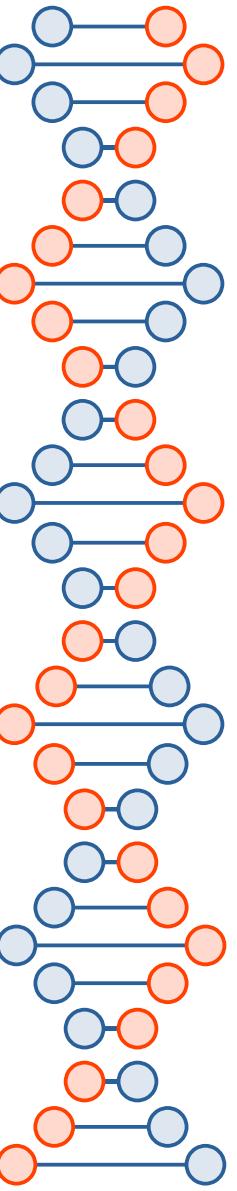


https://en.wikipedia.org/wiki/Grover%27s_algorithm#/media/File:Grover's_algorithm_circuit.svg



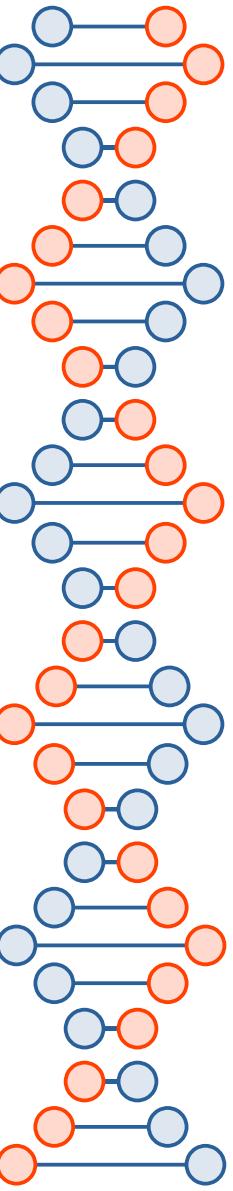
Symmetric crypto

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

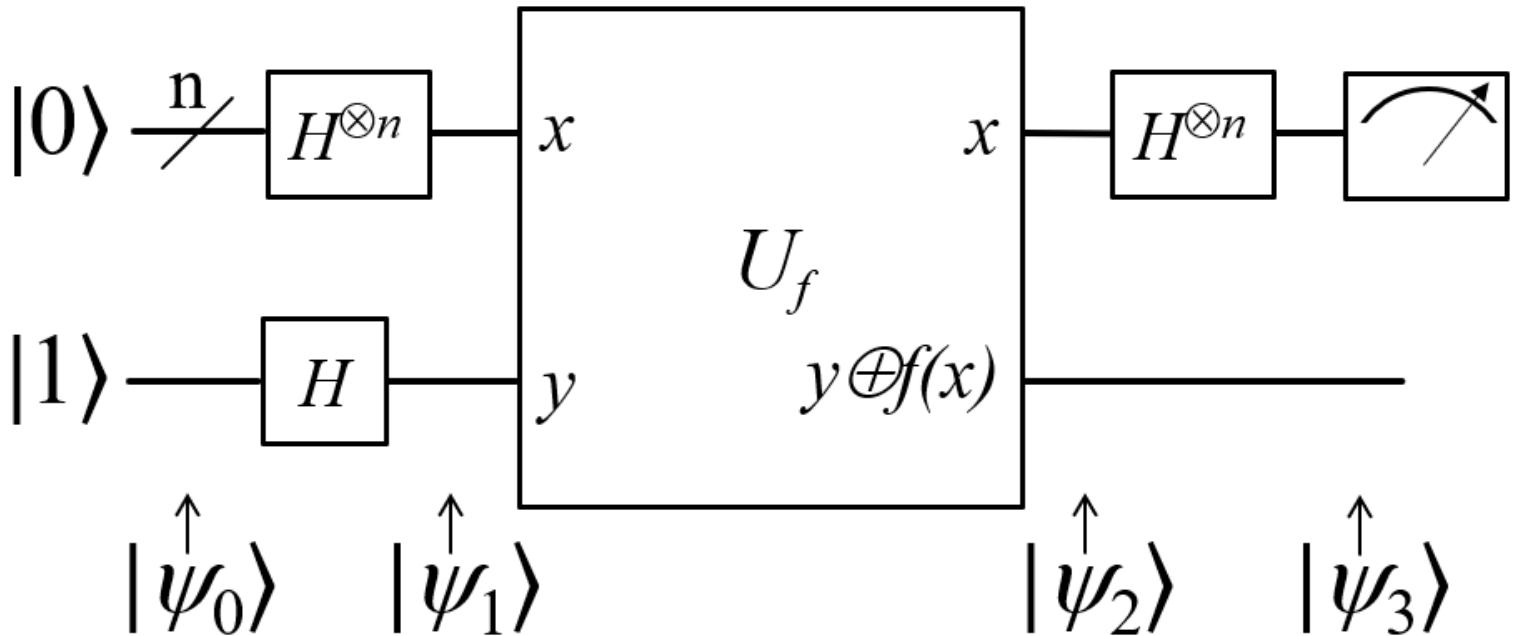


Asymmetric Crypto

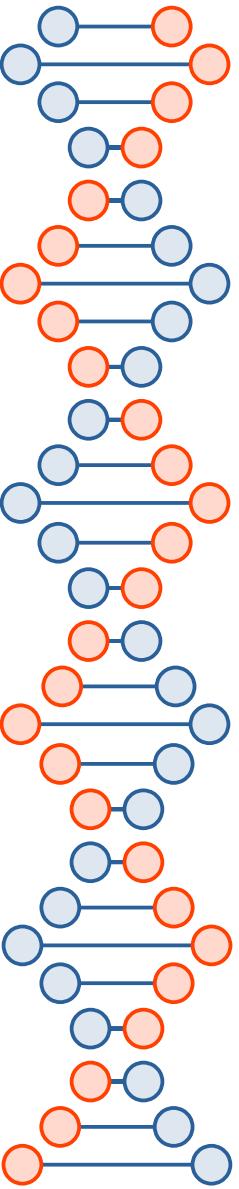
- Quantum computers seem to be good at the same kinds of things that make good, simple trapdoor functions for asymmetric crypto (factorization, discrete log, etc.)
 - But not everything
 - Older schemes (e.g., Merkle's signature scheme)
 - Newer schemes (e.g., lattice-based)
- Specifically, Shor's algorithm solves the abelian hidden subgroup problem
 - But maybe quantum computers can't solve the non-abelian hidden subgroup problem



Deutsch-Jozsa algorithm



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



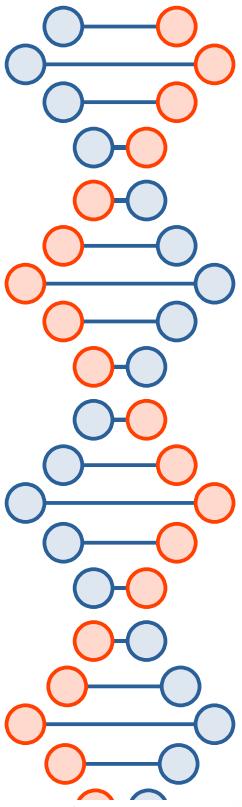
1-bit input case...

- $p = \text{Probability of measuring } |0\rangle$

$$|(1/2)(-1)^{f(0)} + (1/2)(-1)^{f(1)}|$$

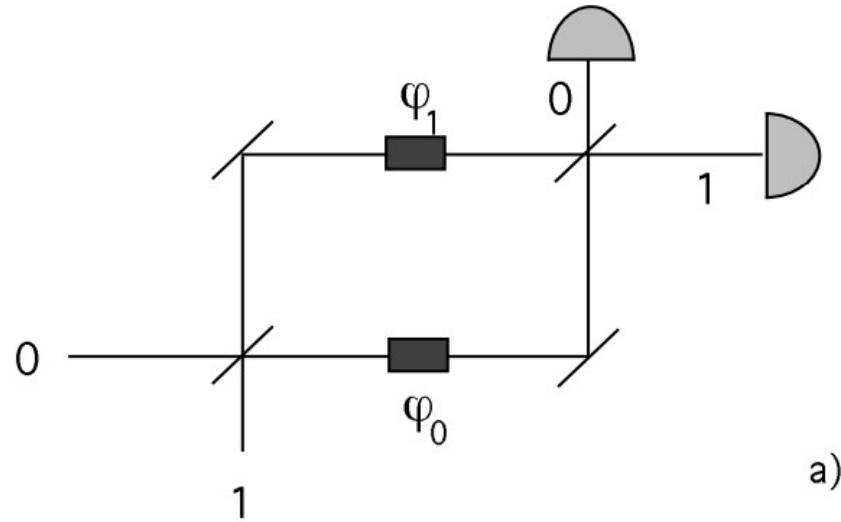
A balanced function cancels itself out because of destructive interference

| $f(0)$ | $f(1)$ | p |
|--------|--------|-----|
| 0 | 0 | 1 |
| 0 | 1 | 0 |
| 1 | 0 | 0 |
| 1 | 1 | 1 |

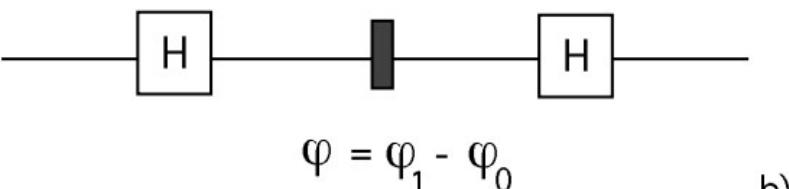


<https://arxiv.org/abs/quant-ph/9708016>

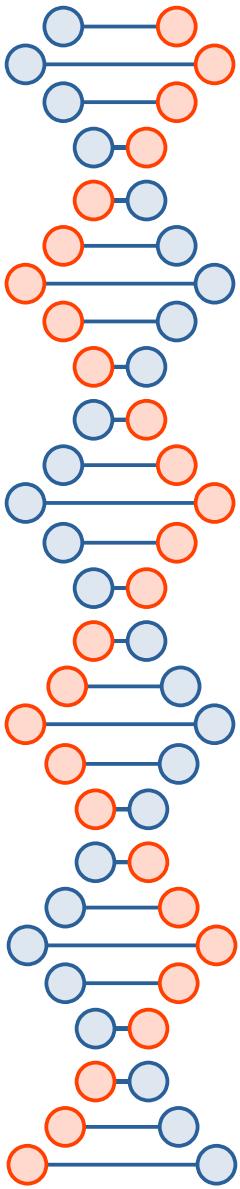
$$\begin{aligned}
 |0\rangle &\xrightarrow{H} \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \\
 |1\rangle &\xrightarrow{H} \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)
 \end{aligned}$$



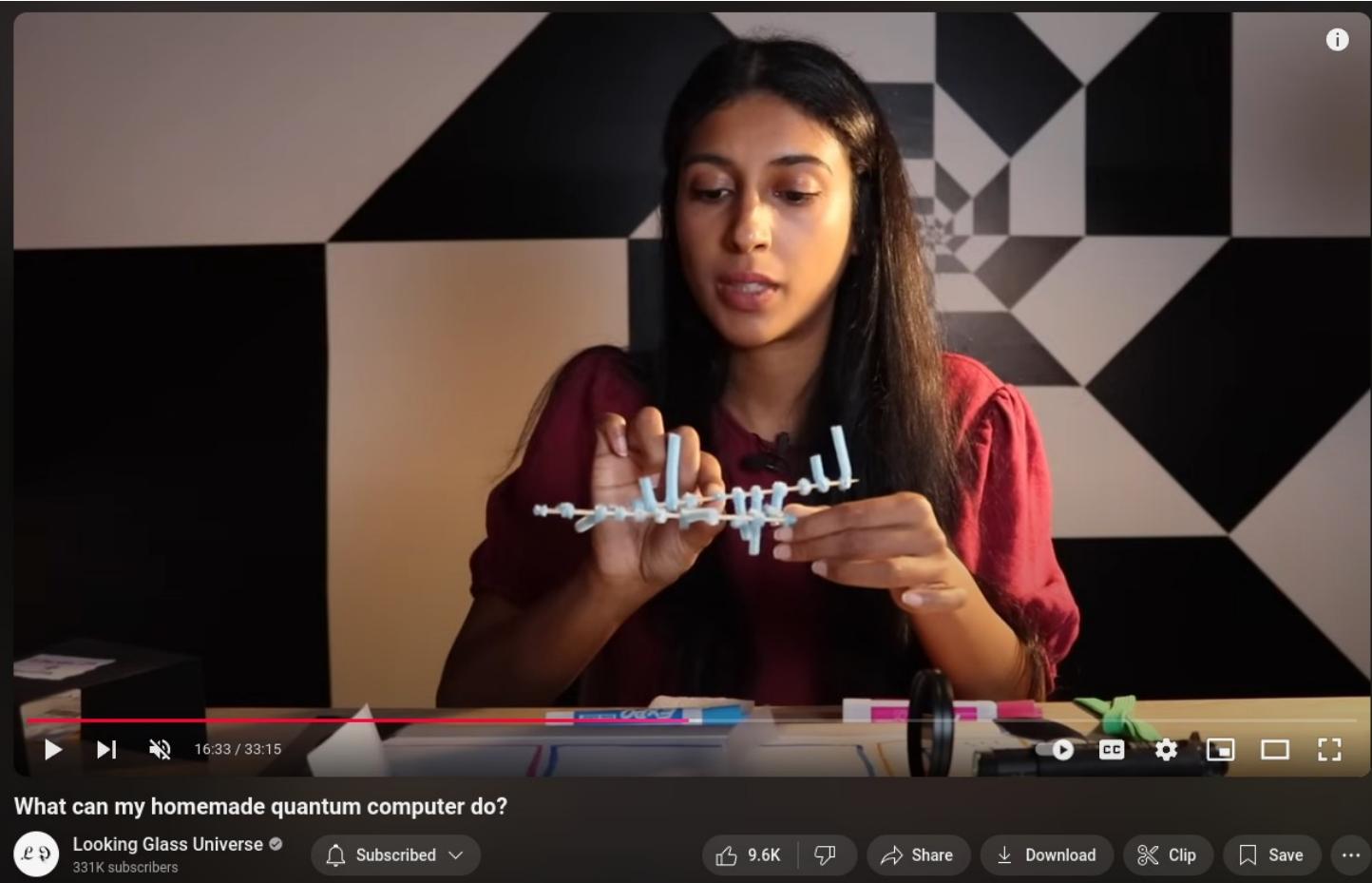
a)

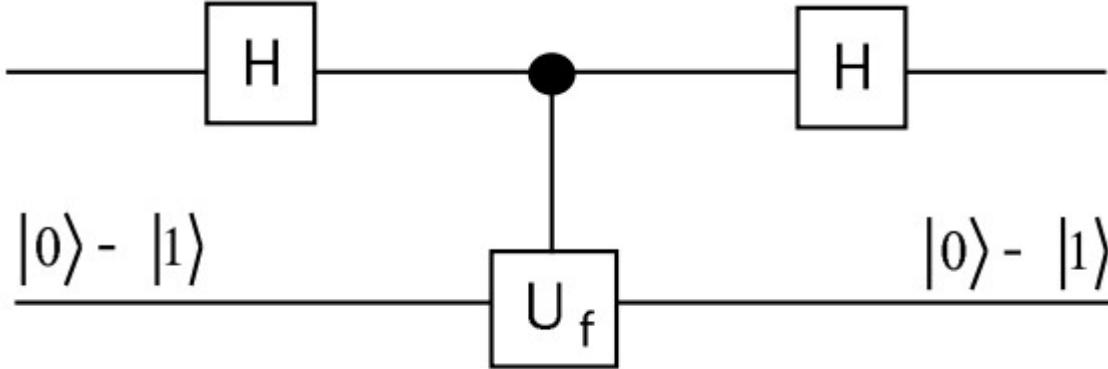
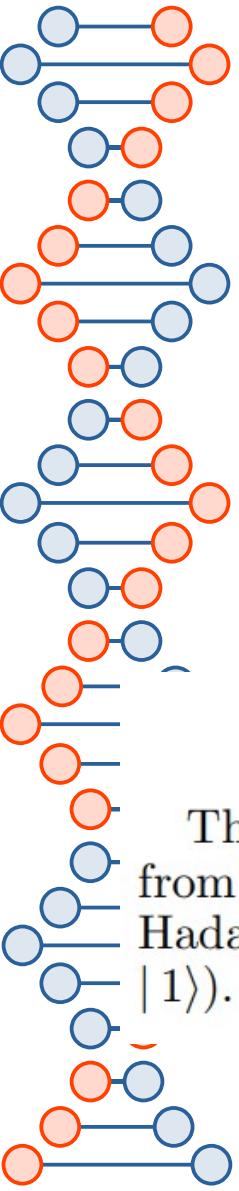


b)



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





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

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 $x \in \{0, 1\}$,

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

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

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

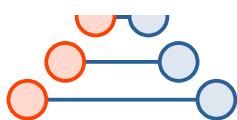
That is, for each x , the $|x\rangle$ term acquires a phase factor of $(-1)^{f(x)}$, which corresponds to the eigenvalue of the state of the auxiliary qubit under the action of the operator that sends $|y\rangle$ to $|y\oplus f(x)\rangle$.

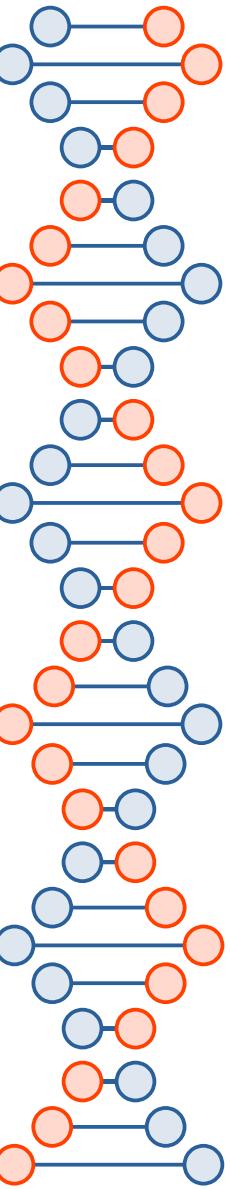
This state can also be written as

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

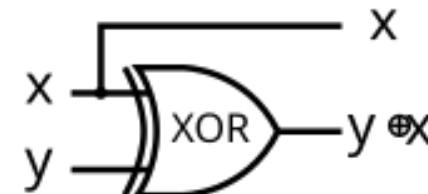
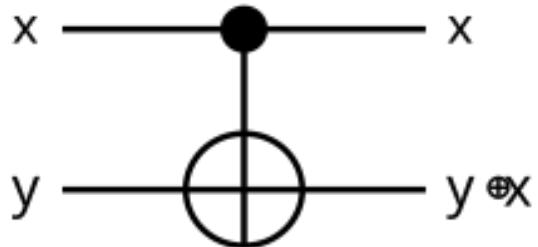
which, after applying the second Hadamard transform, becomes

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



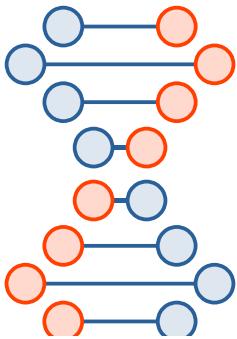


CNOT (Wikipedia)



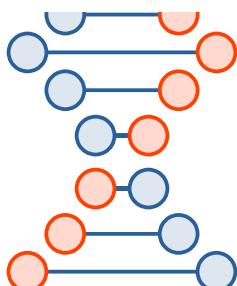
| input | | output | |
|-------------|-------------|-------------|-------------|
| x | y | x | y+x |
| $ 0\rangle$ | $ 0\rangle$ | $ 0\rangle$ | $ 0\rangle$ |
| $ 0\rangle$ | $ 1\rangle$ | $ 0\rangle$ | $ 1\rangle$ |
| $ 1\rangle$ | $ 0\rangle$ | $ 1\rangle$ | $ 1\rangle$ |
| $ 1\rangle$ | $ 1\rangle$ | $ 1\rangle$ | $ 0\rangle$ |

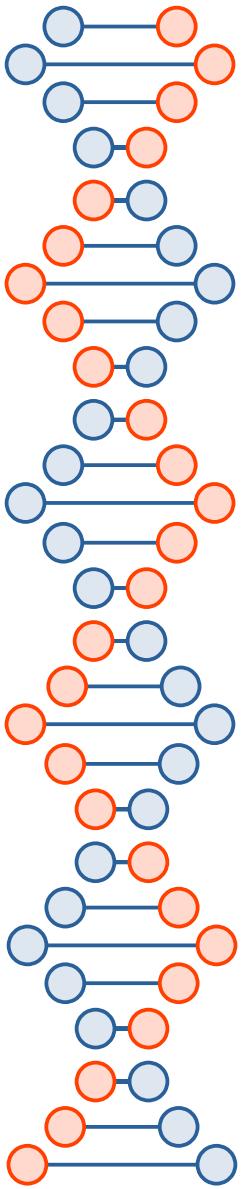
| input | | output | |
|-------|---|--------|-----|
| x | y | x | y+x |
| 0 | 0 | 0 | 0 |
| 0 | 1 | 0 | 1 |
| 1 | 0 | 1 | 1 |
| 1 | 1 | 1 | 0 |



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

| Initial state in Hadamard basis | Equivalent state in computational basis | Apply operator | State in computational basis after C_{NOT} | Equivalent state in Hadamard basis |
|---------------------------------|--|----------------|--|------------------------------------|
| $ ++\rangle$ | $\frac{1}{2}(00\rangle + 01\rangle + 10\rangle + 11\rangle)$ | C_{NOT} | $\frac{1}{2}(00\rangle + 01\rangle + 11\rangle + 10\rangle)$ | $ ++\rangle$ |
| $ +-\rangle$ | $\frac{1}{2}(00\rangle - 01\rangle + 10\rangle - 11\rangle)$ | C_{NOT} | $\frac{1}{2}(00\rangle - 01\rangle + 11\rangle - 10\rangle)$ | $ --\rangle$ |
| $ -+\rangle$ | $\frac{1}{2}(00\rangle + 01\rangle - 10\rangle - 11\rangle)$ | C_{NOT} | $\frac{1}{2}(00\rangle + 01\rangle - 11\rangle - 10\rangle)$ | $ -+\rangle$ |
| $ --\rangle$ | $\frac{1}{2}(00\rangle - 01\rangle - 10\rangle + 11\rangle)$ | C_{NOT} | $\frac{1}{2}(00\rangle - 01\rangle - 11\rangle + 10\rangle)$ | $ +-\rangle$ |





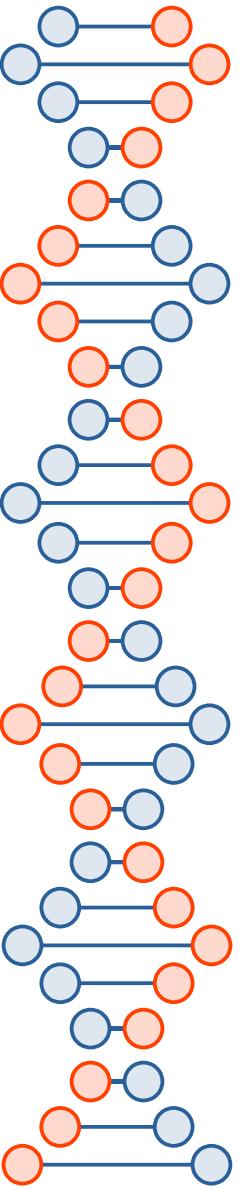
| Operator | Gate(s) | Matrix |
|----------------------------------|---------|--|
| Pauli-X (X) | | \oplus $\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$ |
| Pauli-Y (Y) | | $\begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}$ |
| Pauli-Z (Z) | | $\begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$ |
| Hadamard (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) | | $\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$ |

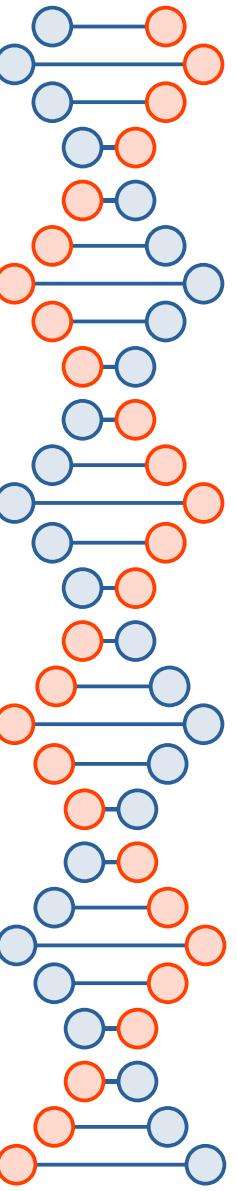
$$H_0 = + (1)$$

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

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

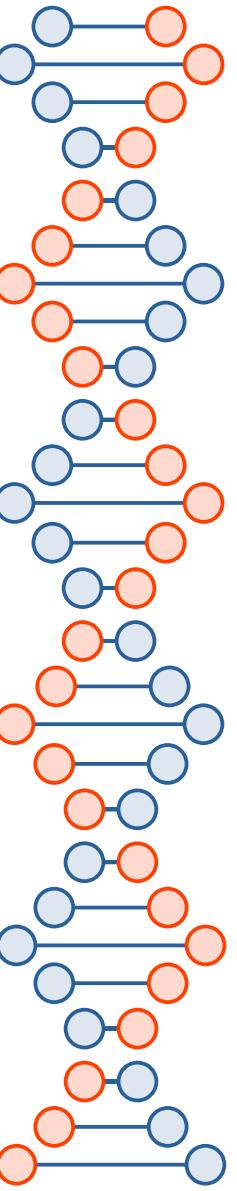
$$H_3 = \frac{1}{2^{3/2}} \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 & 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 & 1 & -1 & -1 & 1 \\ 1 & 1 & 1 & 1 & -1 & -1 & -1 & -1 \\ 1 & -1 & 1 & -1 & -1 & 1 & -1 & 1 \\ 1 & 1 & -1 & -1 & -1 & -1 & 1 & 1 \\ 1 &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



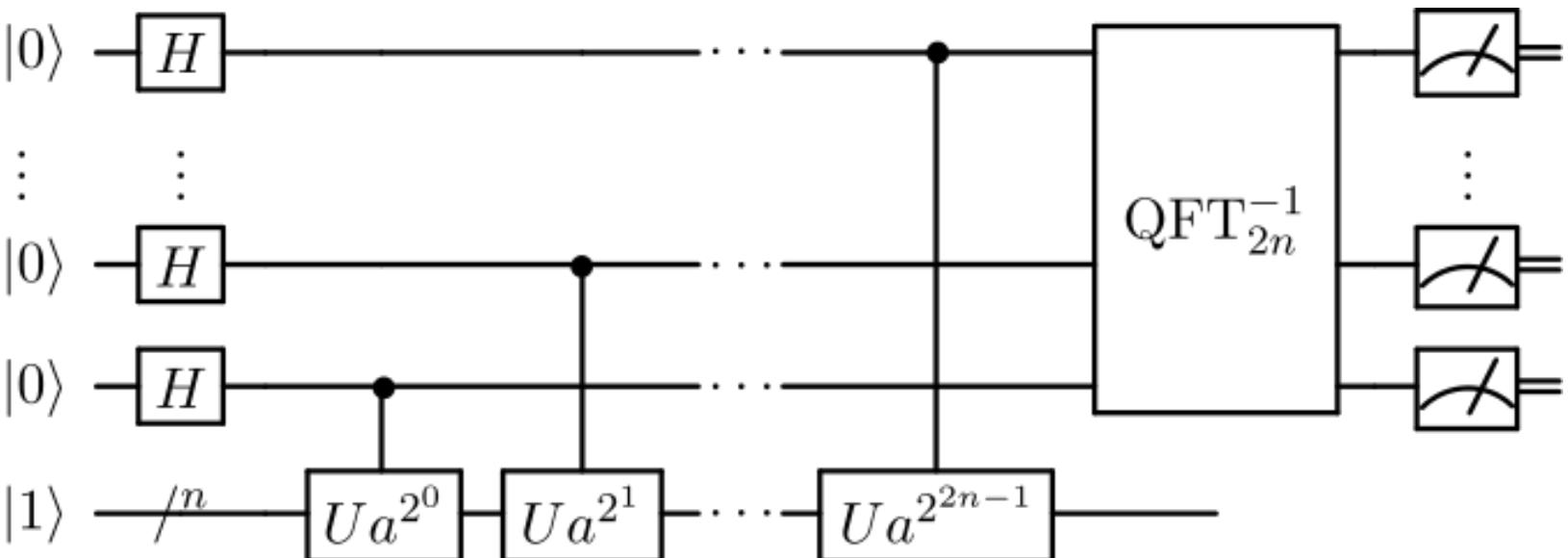


How to attack crypto...

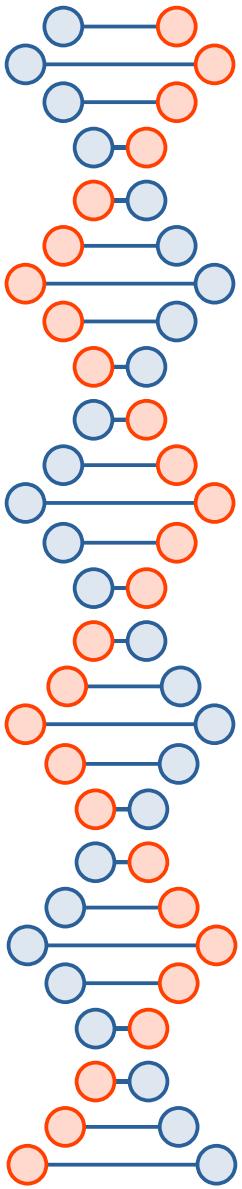
- XOR properties → Quantum computers can do a form of XOR where causality is reversed
- Frequency analysis → Quantum computers are really good at this
 - Balanced vs. unbalanced is a simple case of frequency analysis of a function.
- Side channels → Quantum computers can give us info about things that could have happened, but didn't



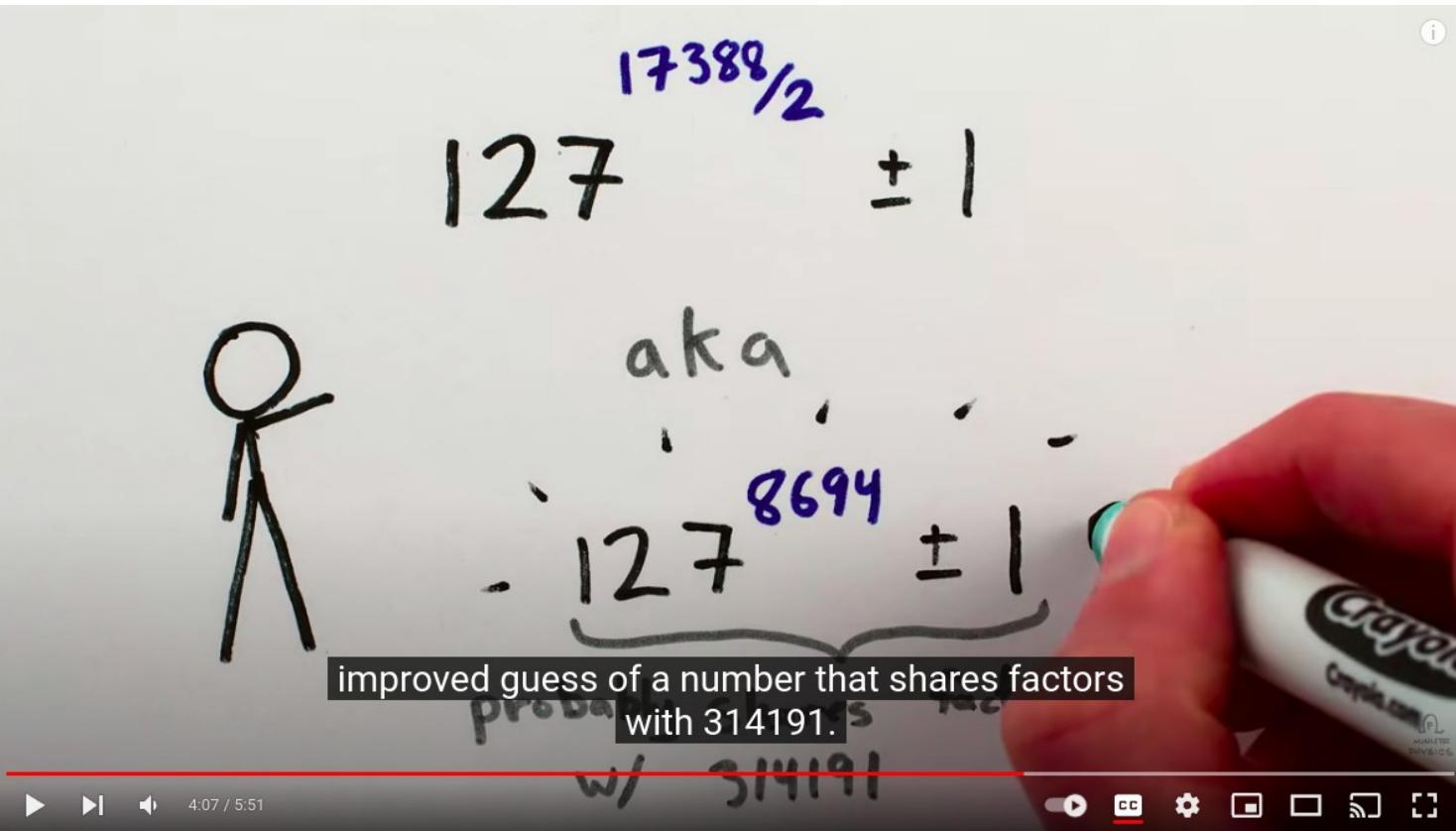
Shor's algorithm

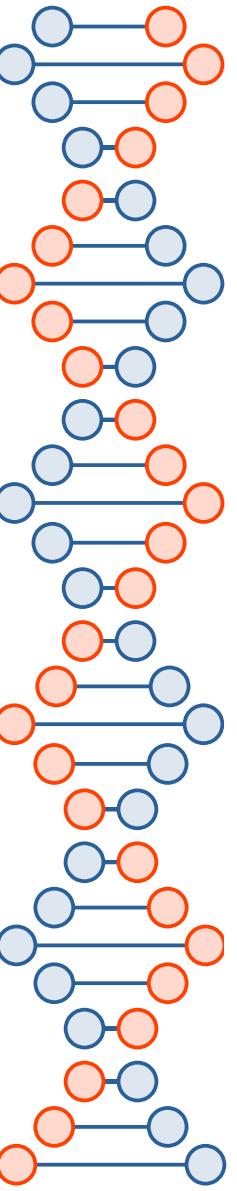


https://en.wikipedia.org/wiki/Shor%27s_algorithm#/media/File:Shor's_algorithm.svg



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



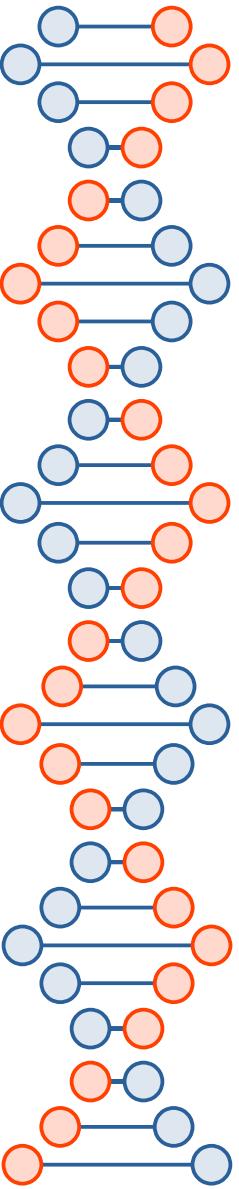


A couple of more links...

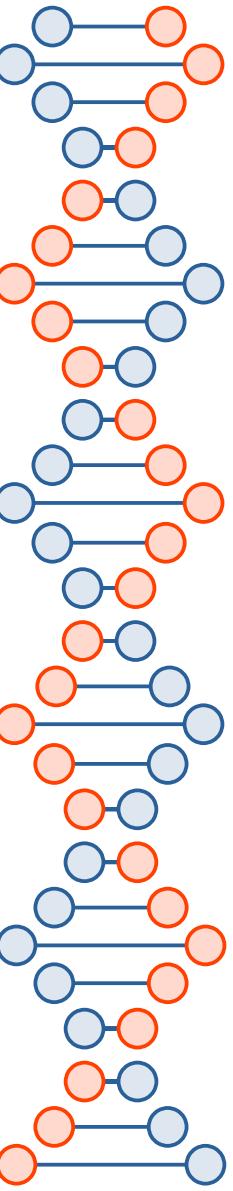
- <https://scottaaronson.blog/?p=208>
- <https://crypto.stackexchange.com/questions/3932/in-laymans-terms-how-does-shors-algorithm-work>

$x \bmod N, x^2 \bmod N, x^3 \bmod N, x^4 \bmod N, \dots$

Then provided x is not divisible by p or q , the above sequence will repeat with some period that evenly divides $(p-1)(q-1)$.



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

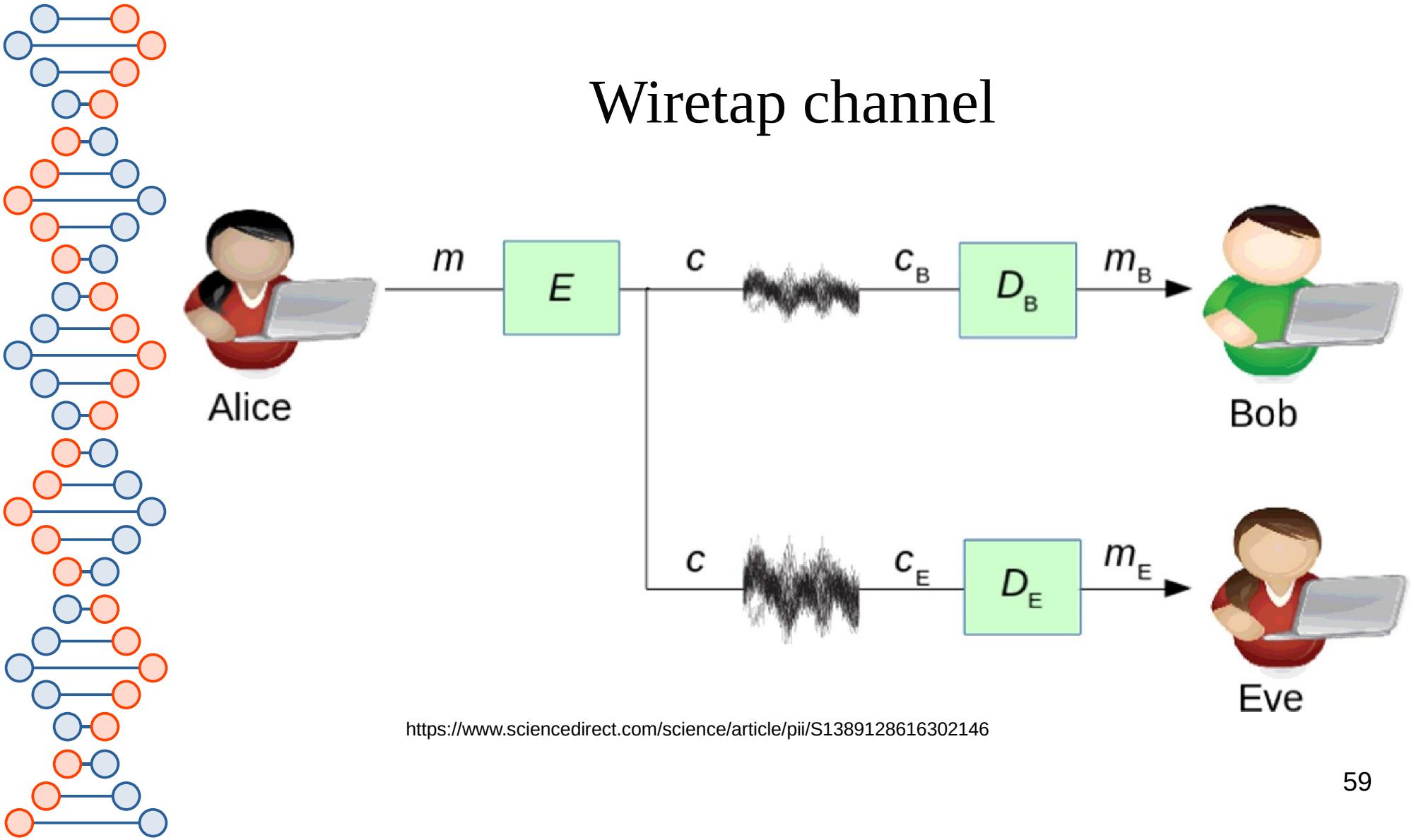


Lamport signature (1979)

- 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

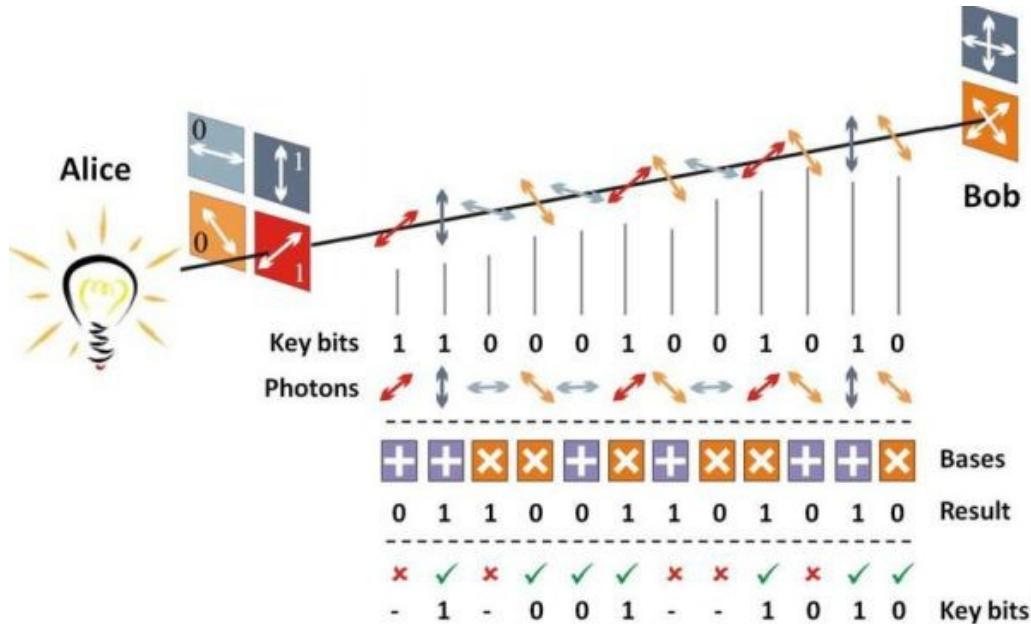
https://en.wikipedia.org/wiki/Lamport_signature

Wiretap channel

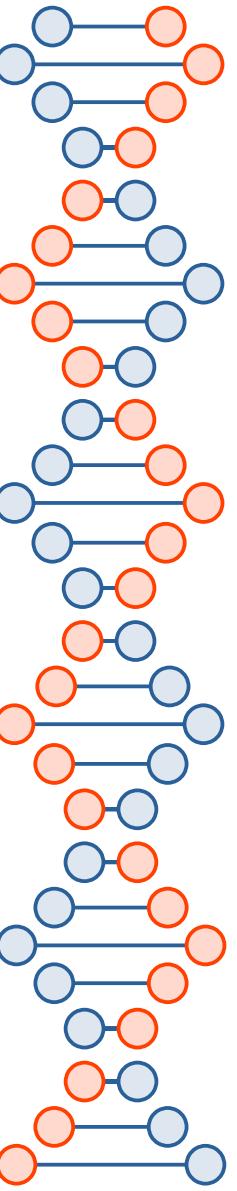


<https://www.sciencedirect.com/science/article/pii/S1389128616302146>

Quantum Key Distribution

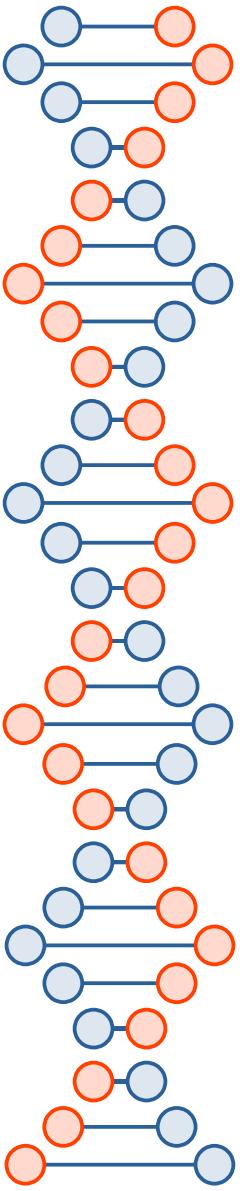


<https://imrmedia.in/quantum-key-distribution-test-successfully-demonstrated/>



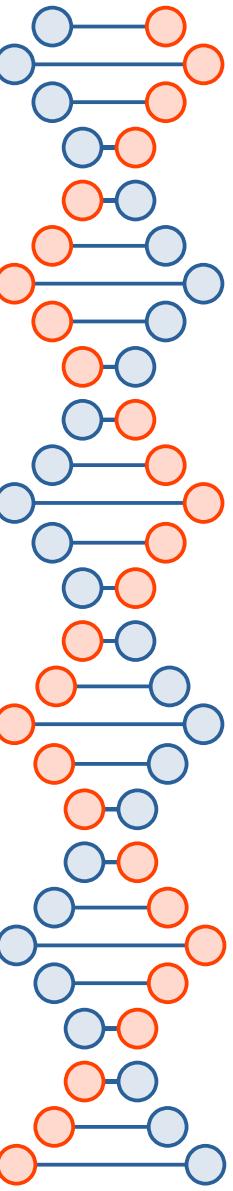
QKD vs. Quantum-resistant

- 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



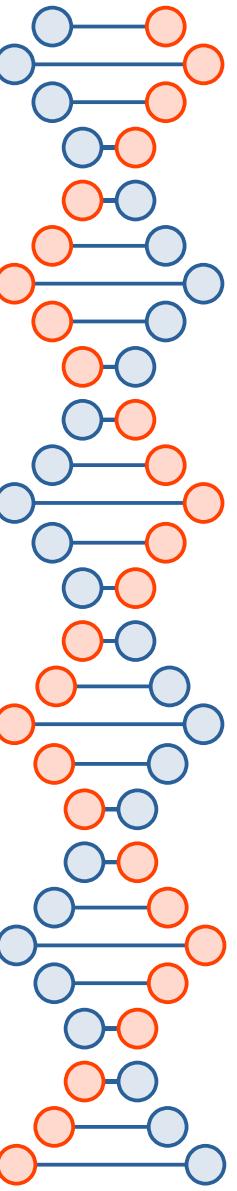
<https://www.youtube.com/watch?v=QDdOoYdb748>
Lattice-based cryptography: The tricky math of dots





Take-aways...

- 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
- But they are exponentially faster at the abelian hidden subgroup problem
 - So we need to redo all the crypto on the Internet, soon!



Some videos...

- https://www.youtube.com/watch?v=_C5dkUiQnw
- <https://www.youtube.com/watch?v=QDdOoYdb748>
- <https://www.youtube.com/watch?v=K026C5YaB3A>
- <https://www.youtube.com/watch?v=KTzGBJPuJwM>