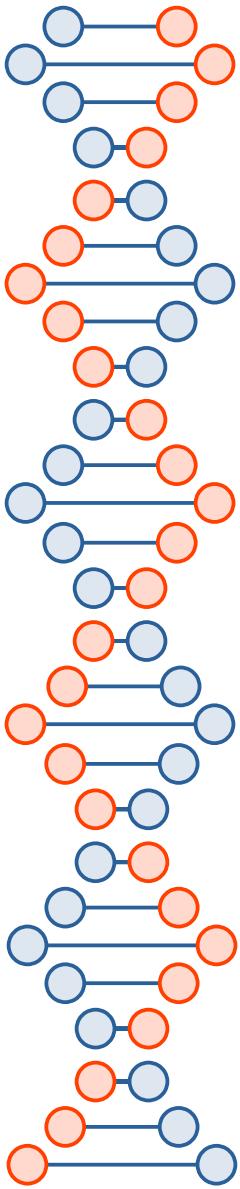


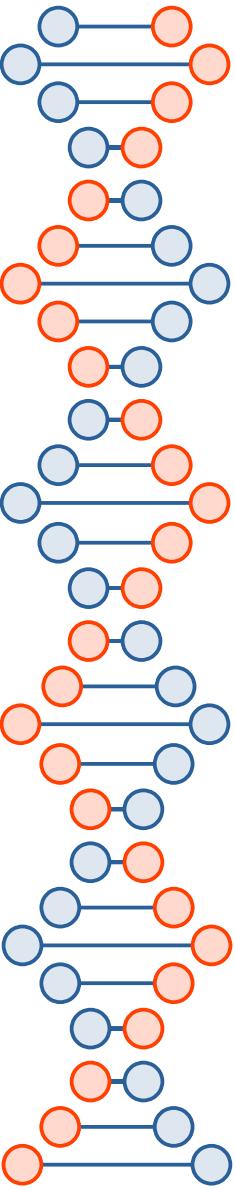
# Brief overview of quantum computers, post-quantum cryptography

CSE 548 Spring 2025  
[jedimaestro@asu.edu](mailto:jedimaestro@asu.edu)



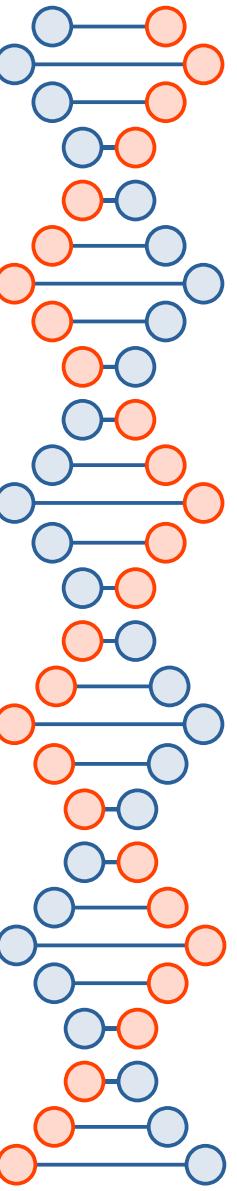
Open question: Does the universe permit private communications in the presence of an eavesdropper using only classical computation?

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



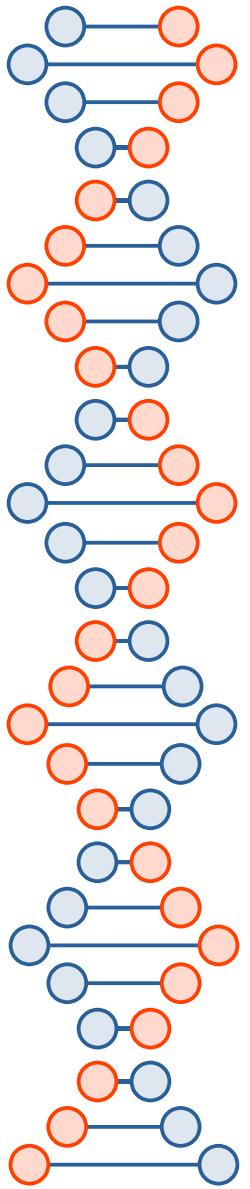
Open question: Does the universe permit ~~private communications~~ *non-repudiability* in the presence of an eavesdropper using only classical computation?

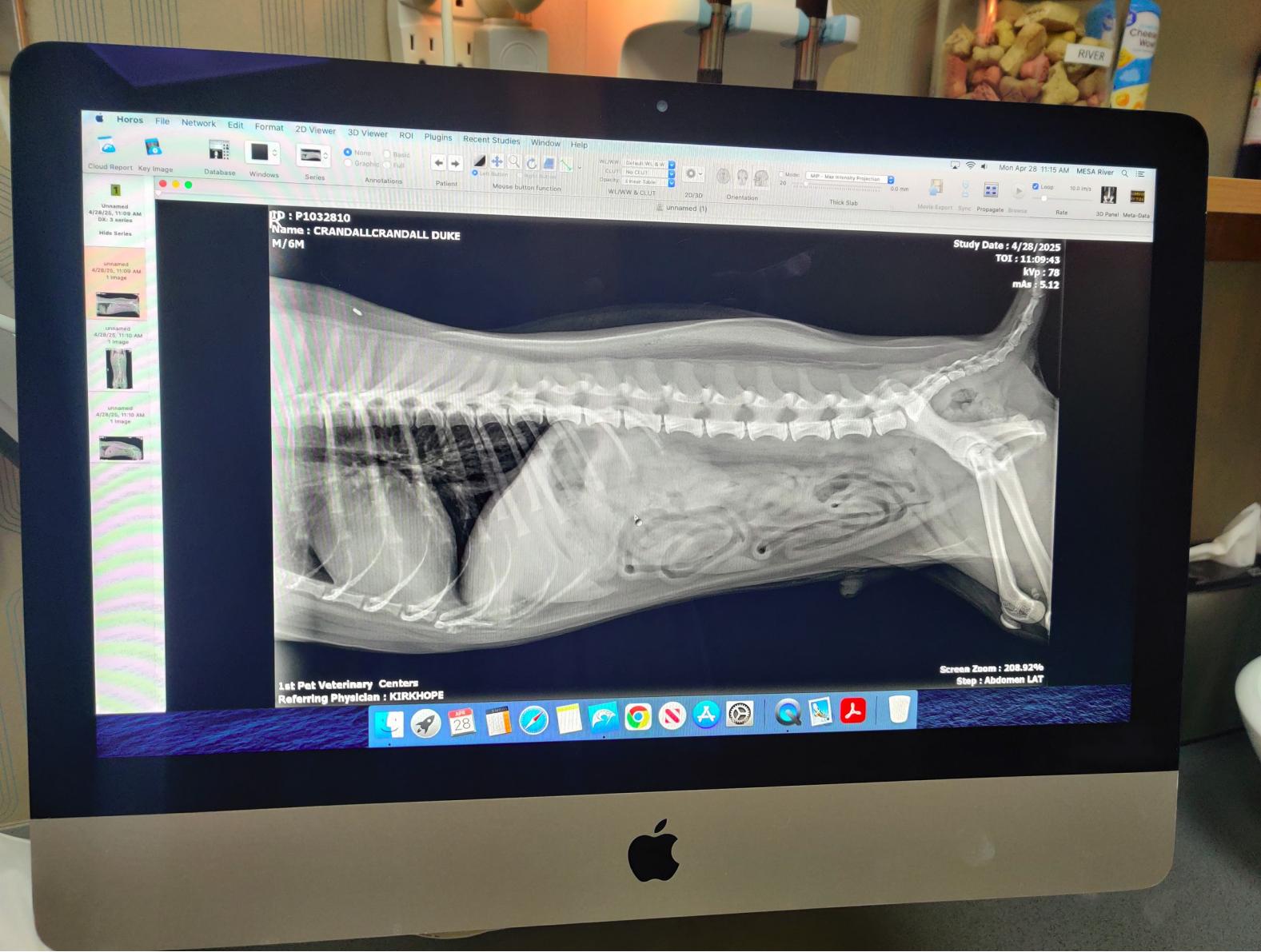
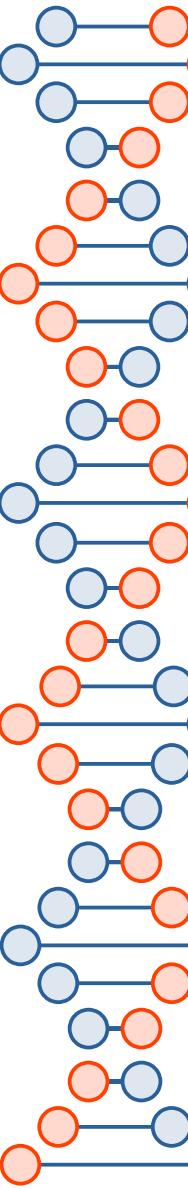
(Network security is profoundly affected by the answer, *e.g.*, TLS and SSH.)

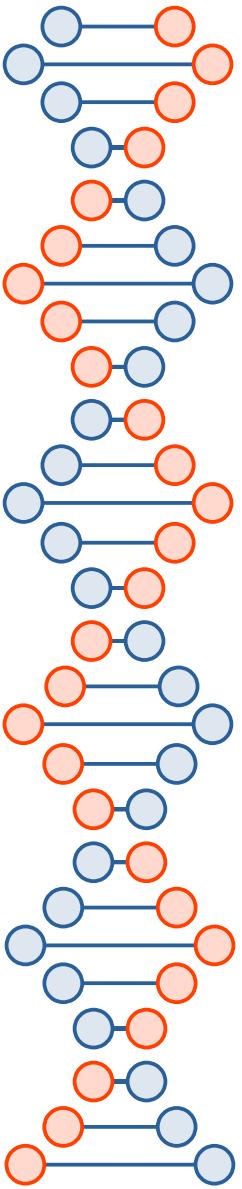


# Why do we care?

- 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 year or two







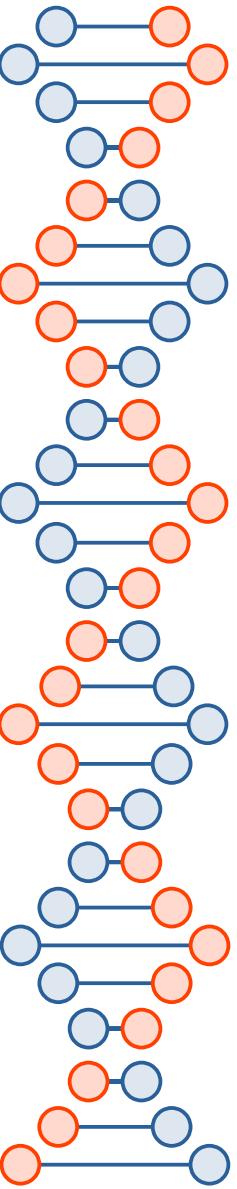
No crayons → brown

Brown crayon → brown

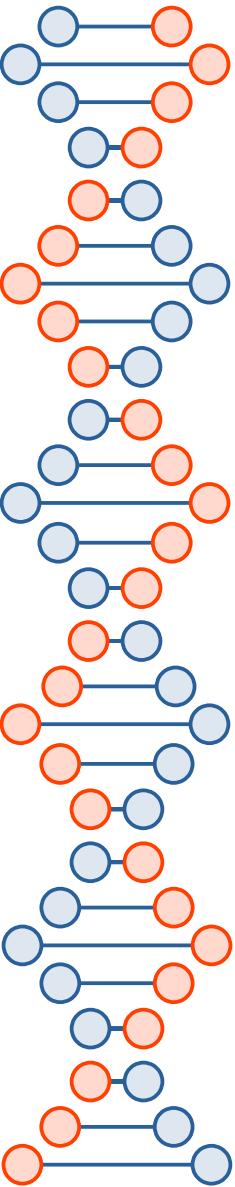
Orange crayon → orange

Blue crayon → blue

Blue + Orange crayons → brown

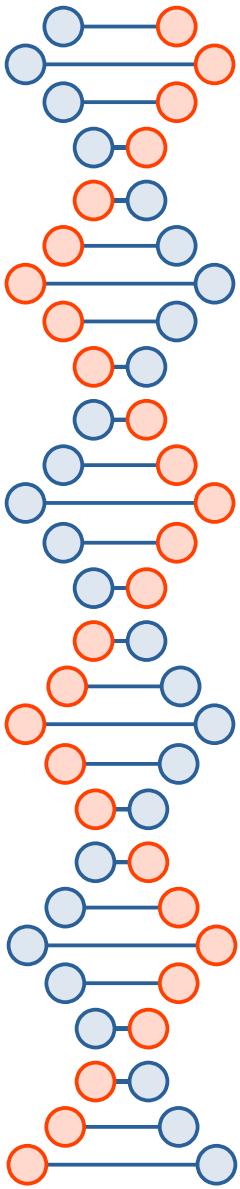


Problem statement: we want to determine if a function  $f(x)$ , which takes a single bit as input and produces a single bit as output, is balanced or unbalanced in its output.



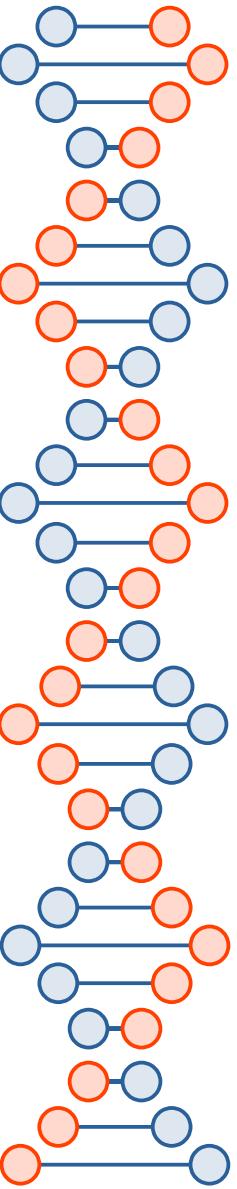
# Define a function $f(x)$ in Duke's tummy...

- Balanced function #1:  
 $f(\text{brown}) = \text{blue}$
- $f(\text{blue}) = \text{brown}$
- Balanced function #2:  
 $f(\text{brown}) = \text{brown}$   
 $f(\text{blue}) = \text{blue}$
- Unbalanced function #1:  
 $f(\text{brown}) = \text{brown}$   
 $f(\text{blue}) = \text{brown}$
- Unbalanced function #2:  
 $f(\text{brown}) = \text{blue}$   
 $f(\text{blue}) = \text{blue}$



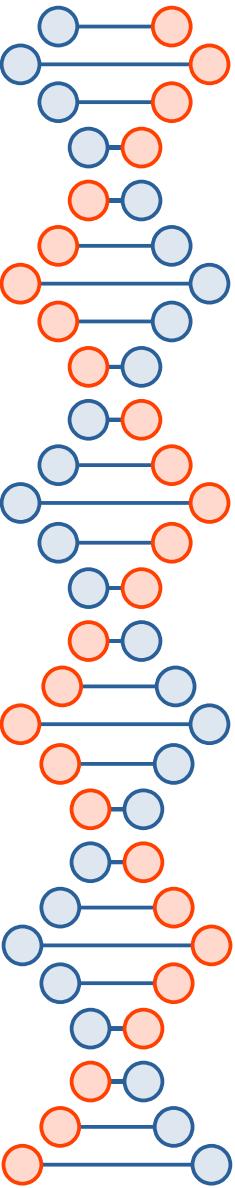
# Classical computation – Duke's tummy is $f(x)$ (costs two crayons)

- Feed Duke a **brown** crayon
  - Observe the color of his
- Feed Duke a **blue** crayon
  - Observe the color of his
- If both  $s$  are the same color...
  - $f(x)$  is a balanced function
- If the  $s$  are different colors...
  - $f(x)$  is an unbalanced function



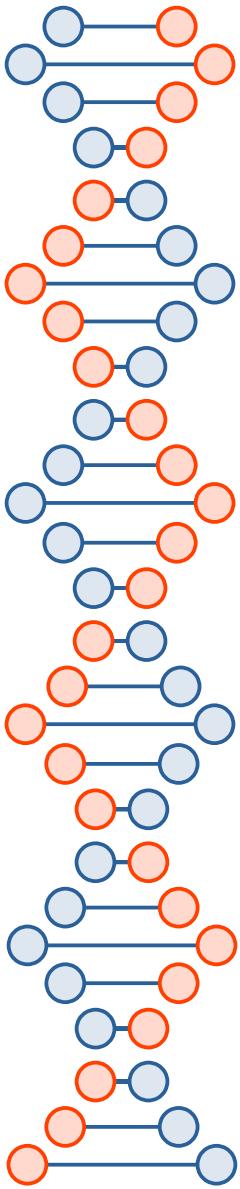
Quantum computation  
Duke's tummy becomes complicated  
(costs one quantum crayon)

...

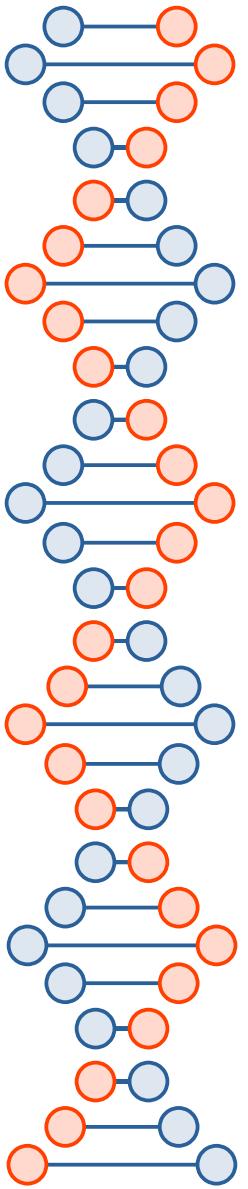


# Define a function $f(x)$ in Duke's tummy...

- Balanced function #1:  
 $f(\text{brown}) = \text{blue}$
- $f(\text{blue}) = \text{brown}$
- Balanced function #2:  
 $f(\text{brown}) = \text{brown}$   
 $f(\text{blue}) = \text{blue}$
- Unbalanced function #1:  
 $f(\text{brown}) = \text{brown}$   
 $f(\text{blue}) = \text{brown}$
- Unbalanced function #2:  
 $f(\text{brown}) = \text{blue}$   
 $f(\text{blue}) = \text{blue}$



- Feed Duke an input crayon that is in a quantum superposition of **brown** and **blue**
  - Duke's tummy...  $f(x) \oplus y$
  - Target crayon,  $y$ , is a superposition of **brown** and **orange**
- DO NOT observe his
  - It will be in a superposition of **orange** and **brown**
  - If you look at it, it'll turn **orange** or **brown** and ruin the computation you're trying to achieve
- The input crayon you fed him is still in your hand, rotate it 90 degrees so that...
  - If it's still in a superposition of **brown** and **blue**, it'll turn **brown**
  - If it's now in a superposition of **orange** and **brown**, it'll turn **blue** (or **orange**)

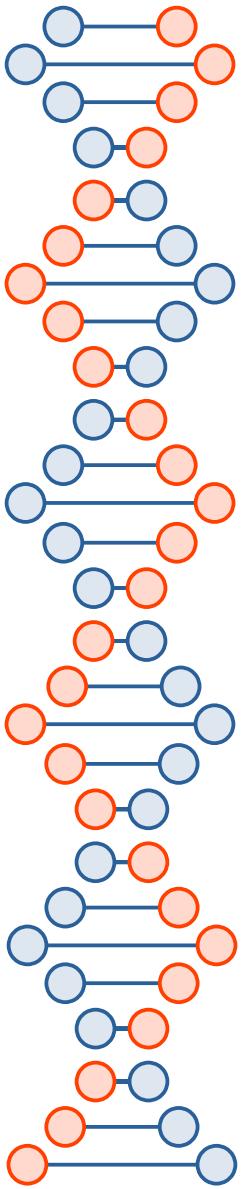


Brown/orange

Brown

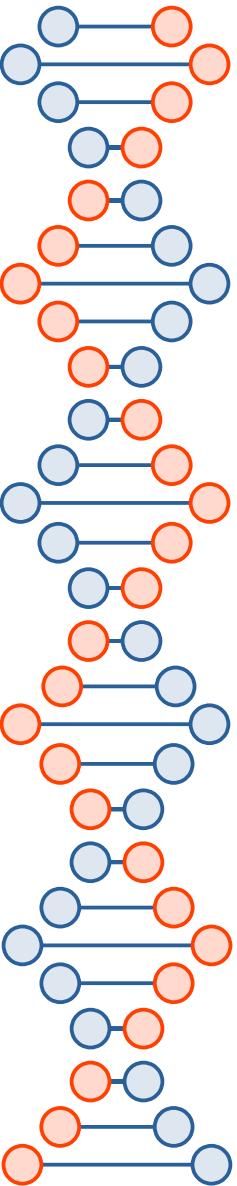
Brown/blue

Blue (or orange)



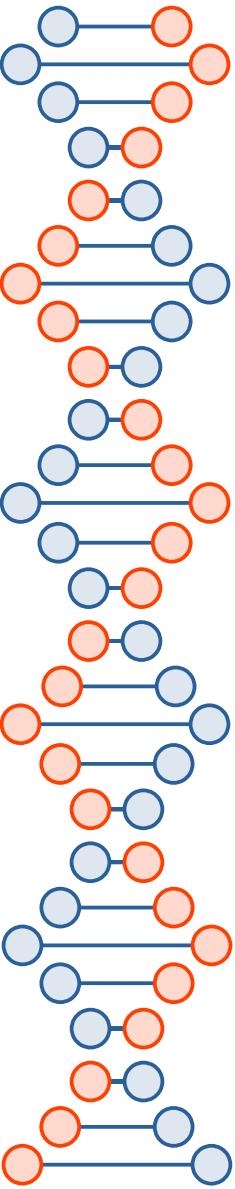
$$f(x) = 0$$

- Nothing changes in the quantum state of the system
  - input crayon is still in a superposition of **blue** and **brown**
  - output crayon is still in a superposition of **orange** and **brown**



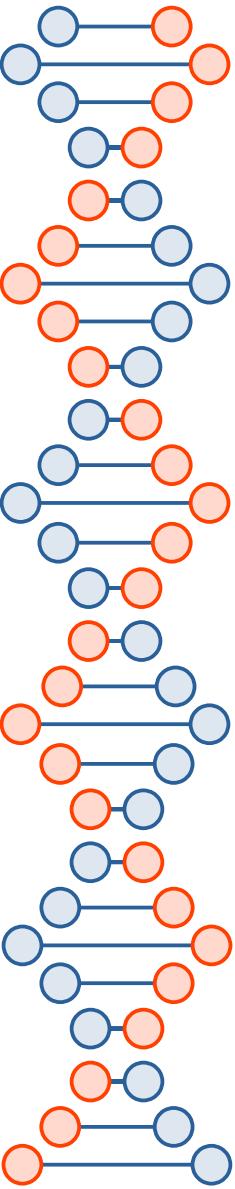
$$f(x) = 1$$

- The quantum state of the system is changed in the following way:
  - Output crayon undergoes phase change
    - Changes from a superposition of orange and brown into a superposition of brown and orange
  - This causes a global phase change
    - Input crayon changes from a superposition of blue and brown to a superposition of brown and blue
      - Brown and blue have the same phase



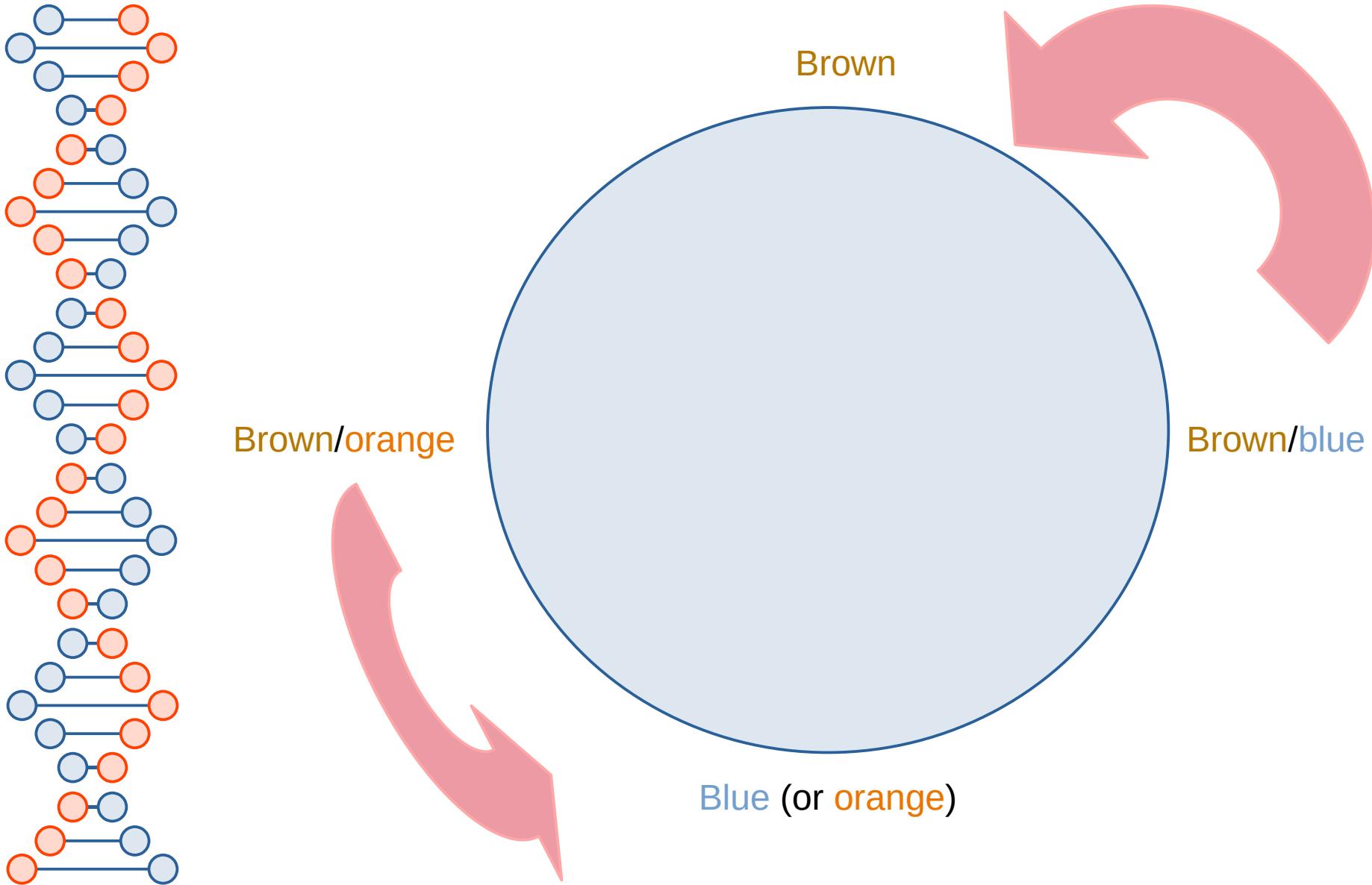
$$f(x) = x$$

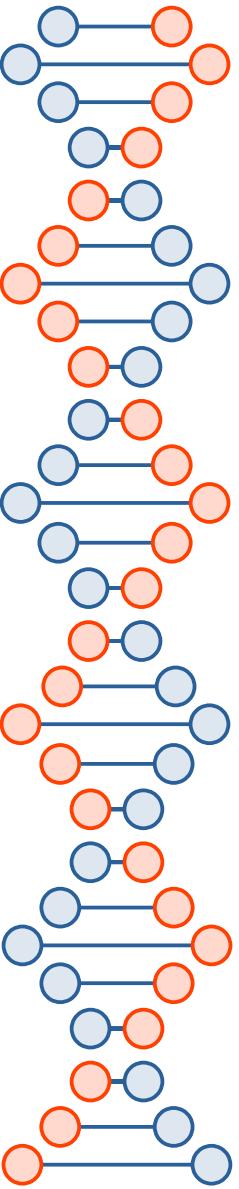
- The quantum state of the system is changed in the following way:
  - input crayon is **brown** → nothing changes
  - input crayon is **blue** → **brown** and **orange** swap phases in the output crayon → this phase change gets “kicked back” only into possibilities where the input crayon is **blue** → **blue** becomes **orange** and **brown** is left alone in the input crayon



$$f(x) = \bar{x}$$

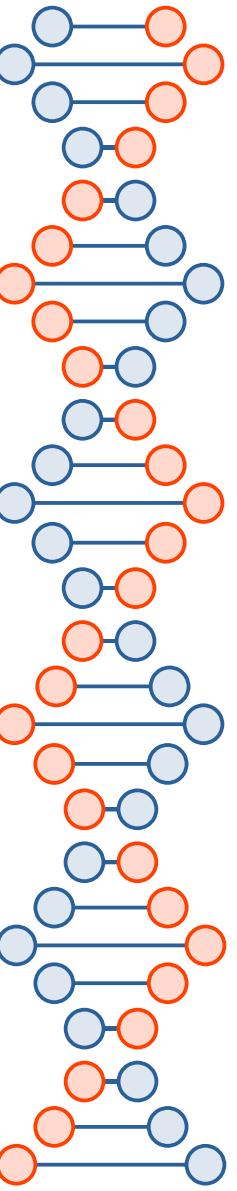
- The quantum state of the system is changed in the following way:
  - input crayon is **brown** → **brown** and **orange** swap phases in the output crayon → this phase change gets “kicked back” only into possibilities where the input crayon is **brown** → **brown** is now out of phase with **blue** in the input crayon, so **blue** effectively becomes **orange**
  - input crayon is **blue** → nothing changes
    - but **blue** is now **orange**





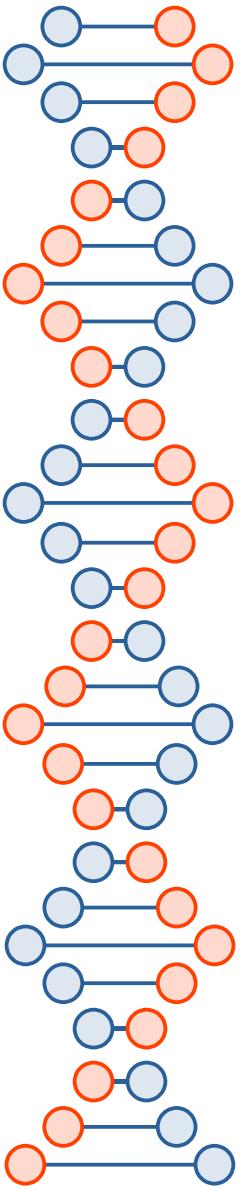
We can tell if a function is balanced or unbalanced by applying it only once.

(Deutsch's algorithm)

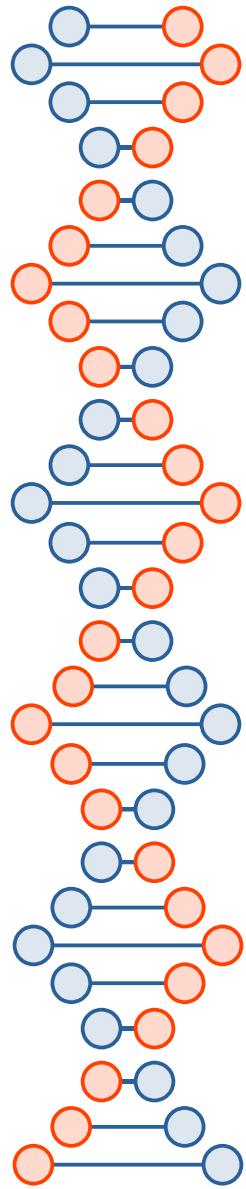


## Some videos...

- [https://www.youtube.com/watch?v=\\_C5dkUiQnw](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>



Quantum computation is all around you...



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

YouTube

The diagram illustrates the olfactory system. At the top, the brain is shown with the Olfactory Bulb highlighted. Below it, the Nasal Cavity contains the Olfactory Epithelium, which is covered in Mucus. Odor Molecules are shown entering the nasal cavity and interacting with the Cilia of Olfactory Neurons embedded in the epithelium. Nerve Endings from these neurons connect to the Olfactory Bulb. A zoomed-in inset provides a detailed view of the neurons and their cilia.

Search

OLFACTORY BULB

OLFACTORY EPITHELIUM

MUCUS

NASAL CAVITY

NERVE ENDINGS

ODOR MOLECULES

OLFACTORY NEURONS

CILLIA

0:33 / 9:23 • How Smell Works >

You Use Quantum Physics to Smell

Domain of Science 1.54M subscribers

Subscribe

9.6K

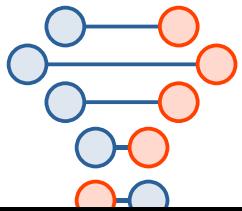
Share

Download

Thanks

DOS

23

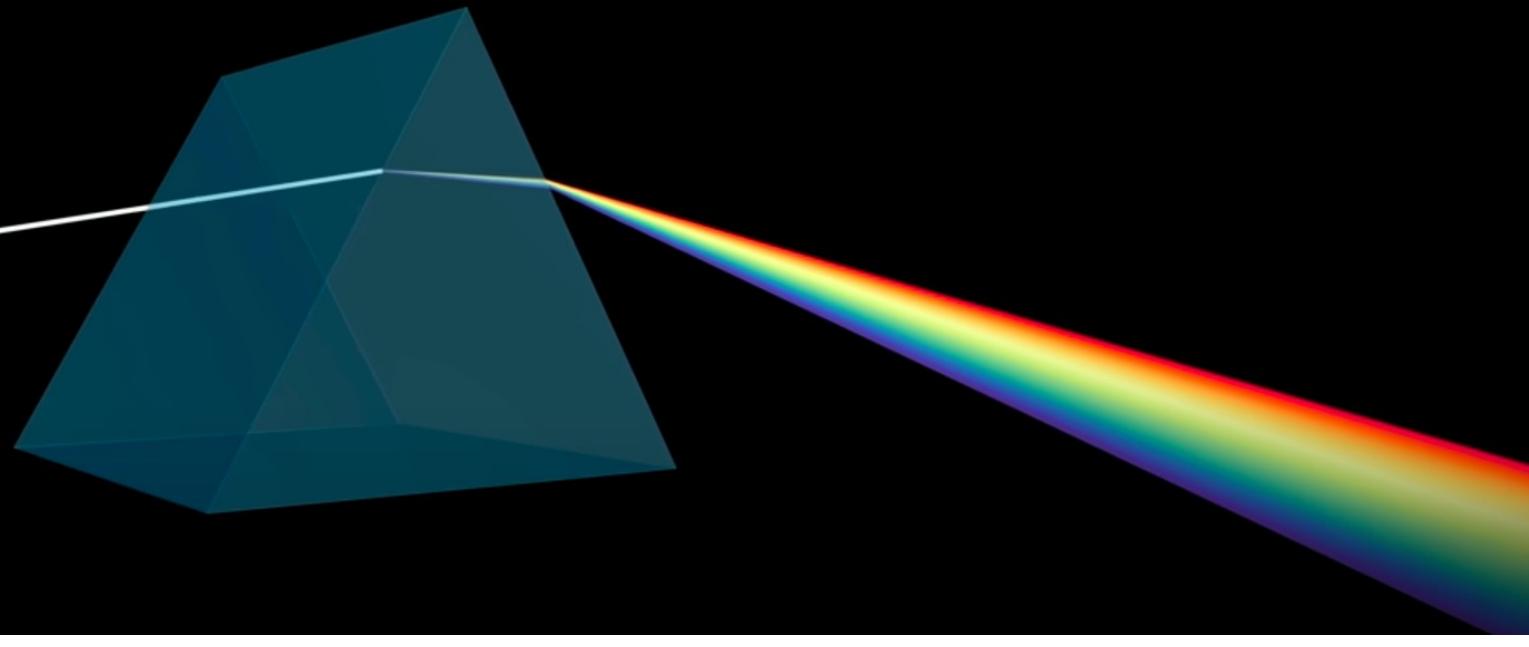


# 3brown1blue on YouTube...

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



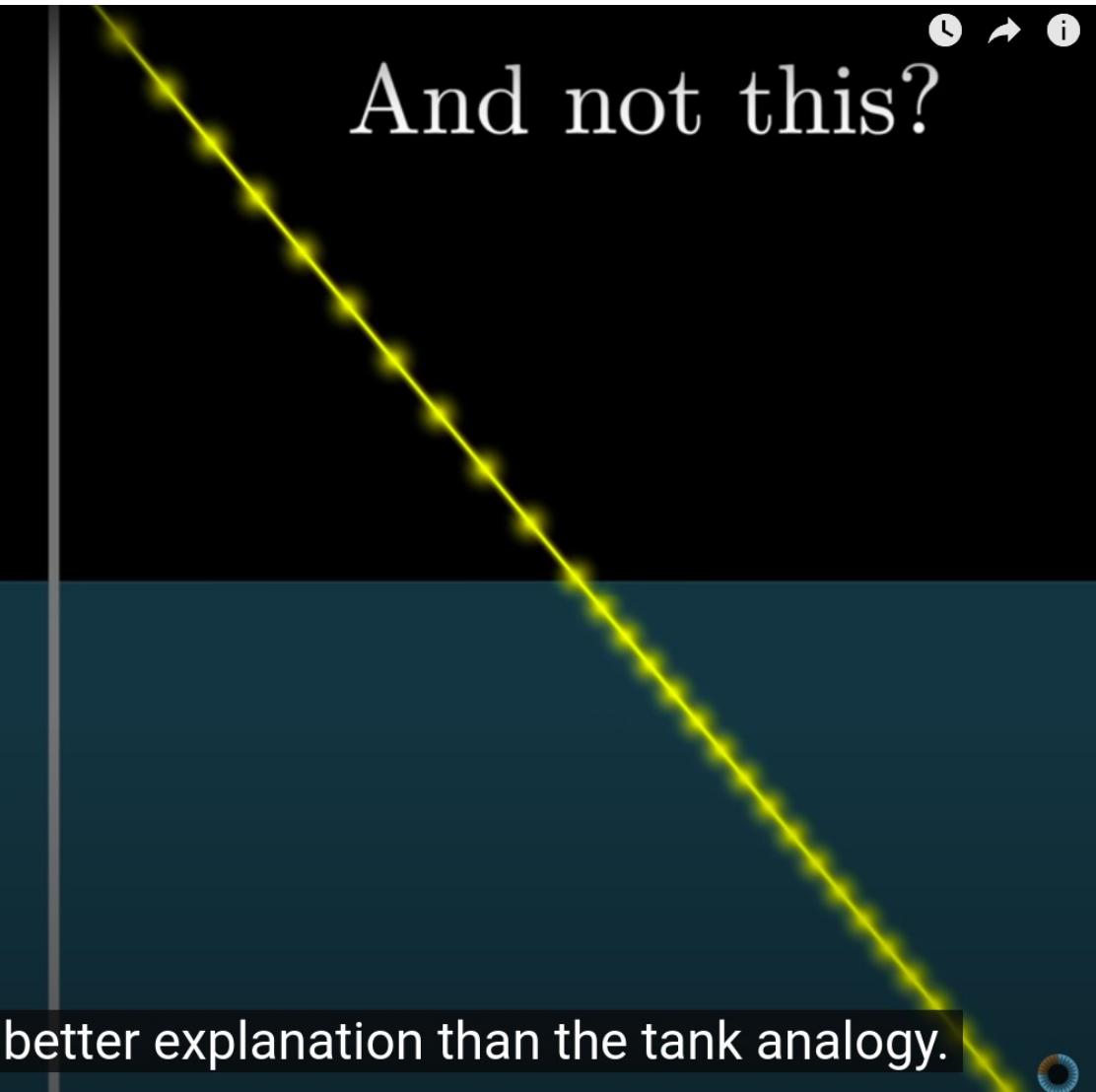
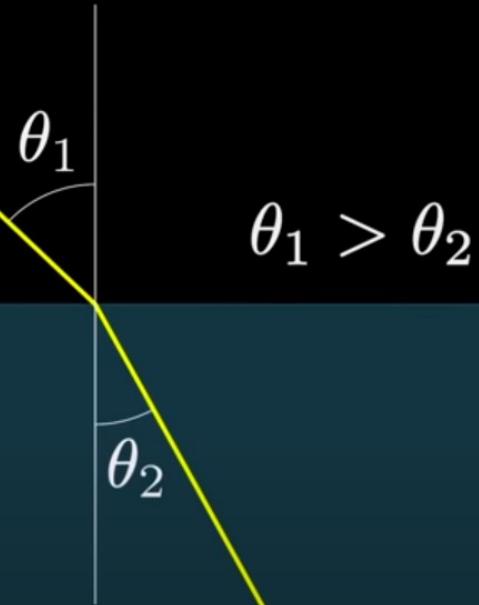
To exit full screen, press Esc





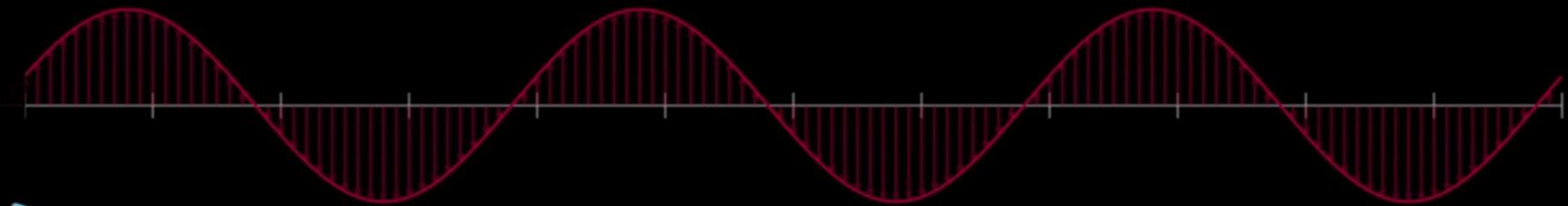
# Why this?

# And not this?



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

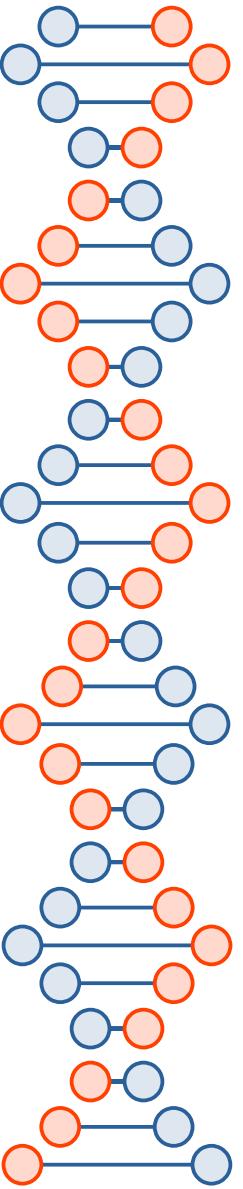




Wave from layer oscillations

Net effect

but just shifted back in phase by a little bit.



[https://www.feynmanlectures.caltech.edu/I\\_30.html](https://www.feynmanlectures.caltech.edu/I_30.html)

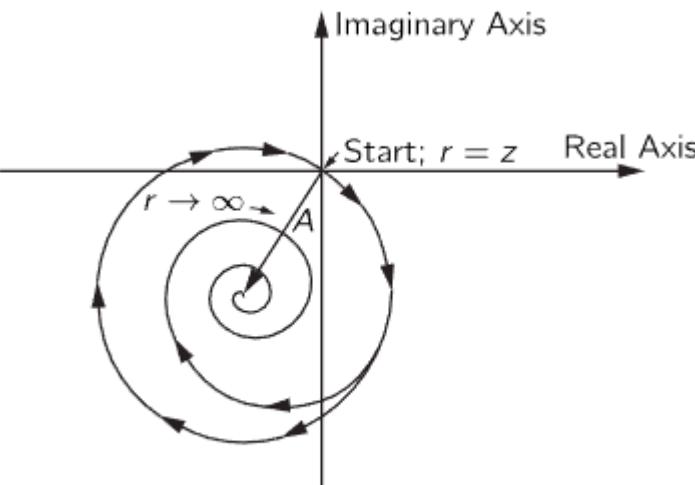
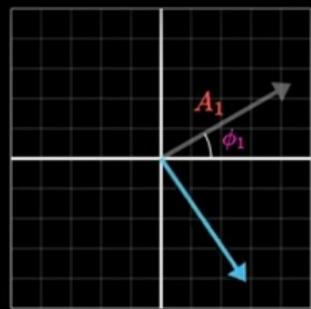


Fig. 30–12. Graphical solution of  $\int_z^\infty \eta e^{-iwr/c} dr$ .

Called an Euler spiral, or Cornu spiral.



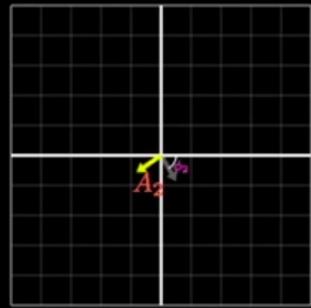
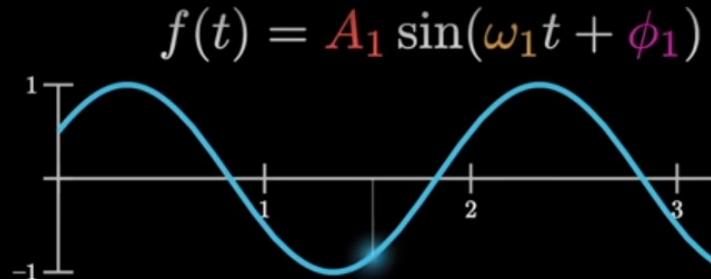
## But why would light "slow down"? | Optics puzzles 3



$$A_1 = 1.00$$

🔒  $\omega_1 = 3.14$

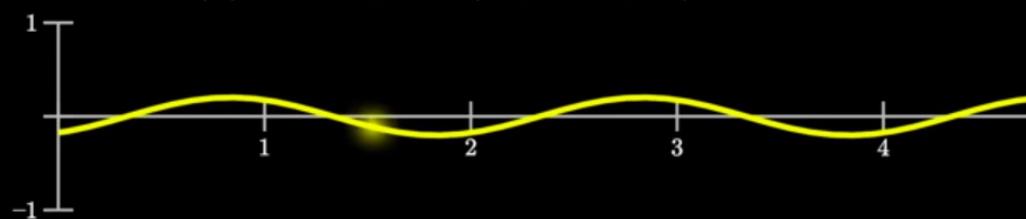
$$\phi_1 = 0.52$$



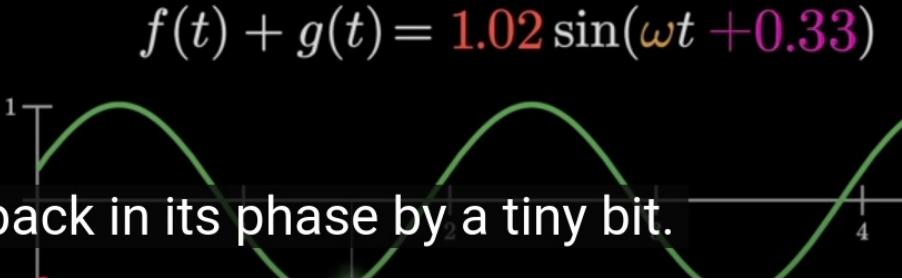
$$A_2 = 0.20$$

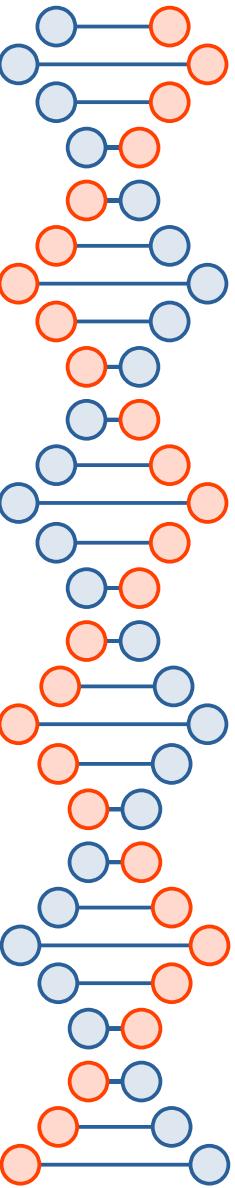
🔒  $\omega_2 = 3.14$

$$\phi_2 = -1.05$$



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





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

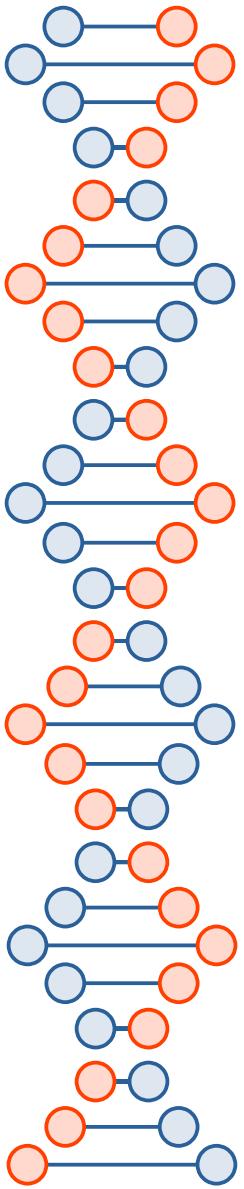
# The Computational Complexity of Linear Optics

Scott Aaronson\*

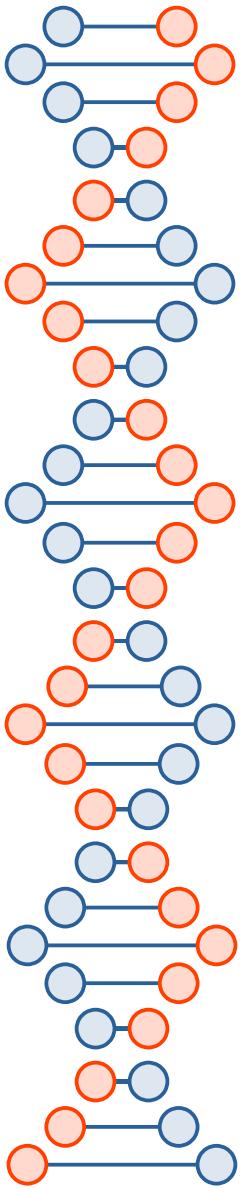
Alex Arkhipov†

## Abstract

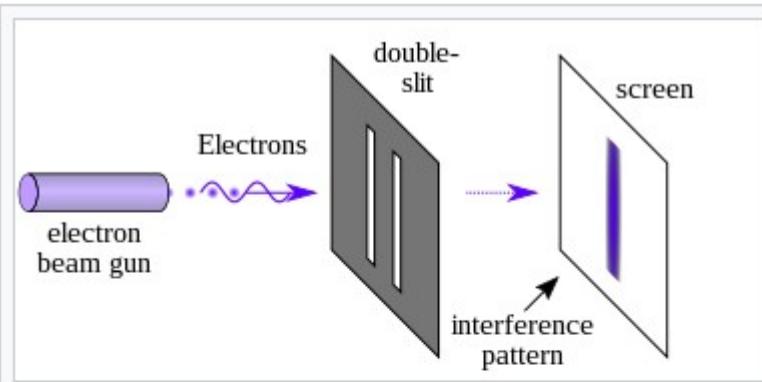
We give new evidence that quantum computers—moreover, rudimentary quantum computers built entirely out of linear-optical elements—cannot be efficiently simulated by classical computers. In particular, we define a model of computation in which identical photons are generated, sent through a linear-optical 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.



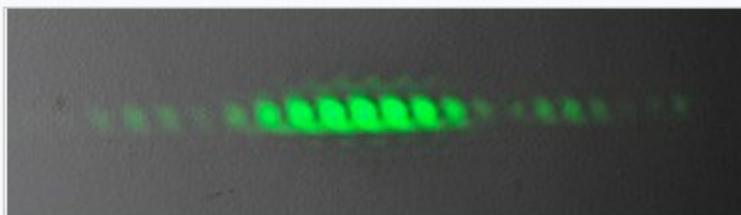
Is light a wave or a particle? Both? Sometimes one, sometimes the other? Neither?



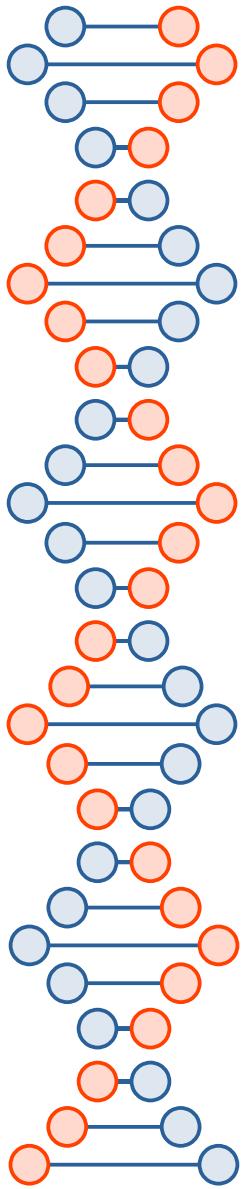
[https://en.wikipedia.org/wiki/Double-slit\\_experiment](https://en.wikipedia.org/wiki/Double-slit_experiment)



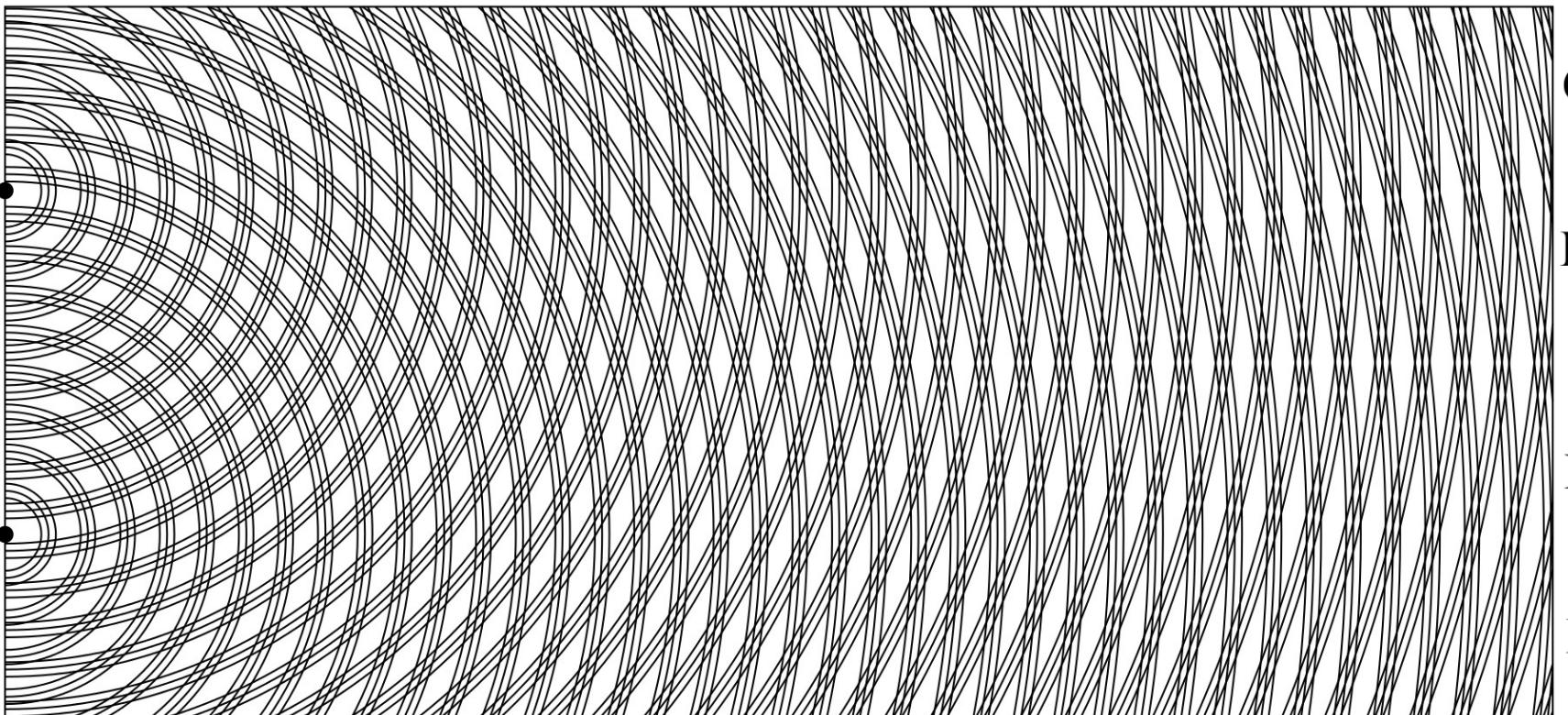
Photons or matter (like electrons) produce an interference pattern when two slits are used

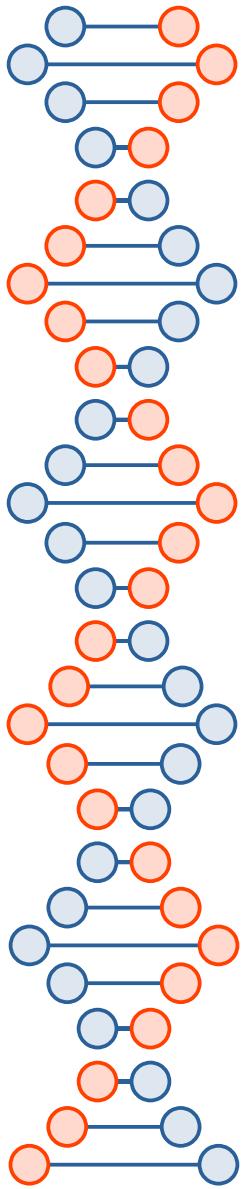


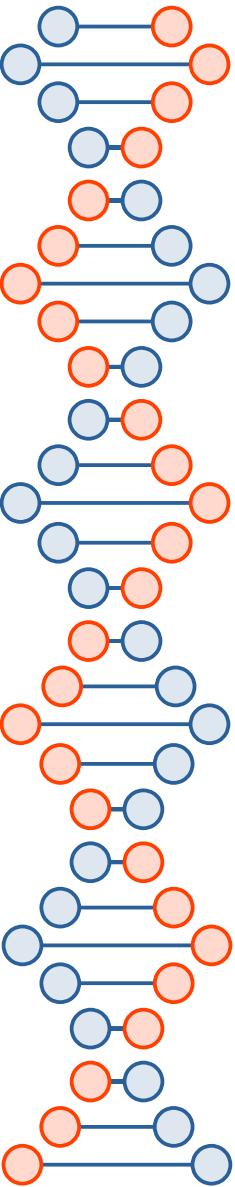
Light from a green laser passing through two slits 0.4mm wide and 0.1mm apart



[https://en.wikipedia.org/wiki/Double-slit\\_experiment](https://en.wikipedia.org/wiki/Double-slit_experiment)





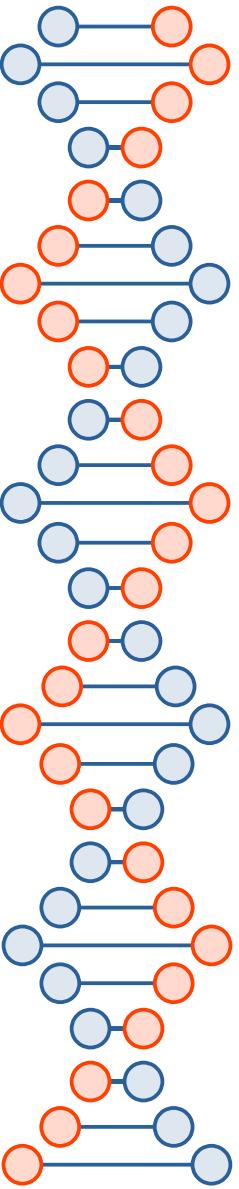


## 1–1 Atomic mechanics

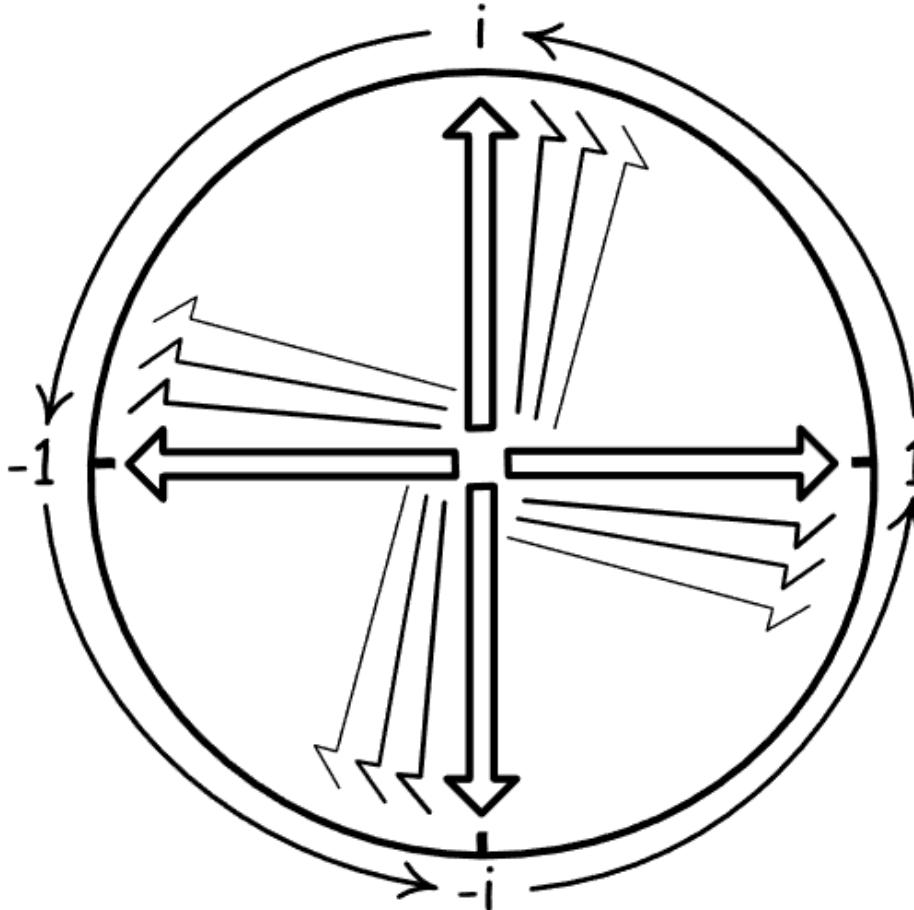
“Quantum mechanics” is the description of the behavior of matter and light in all its details and, in particular, of the happenings on an atomic scale. Things on a very small scale behave like nothing that you have any direct experience about. They do not behave like waves, they do not behave like particles,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

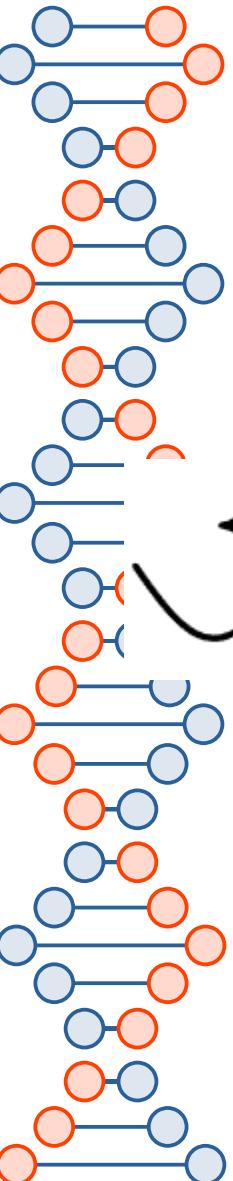
Newton thought that light was made up of particles, but then it was discovered that it behaves like a wave. Later, however (in the beginning of the twentieth century), it was found that light did indeed sometimes behave like a particle. Historically, the electron, for example, was thought to behave like 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](https://www.feynmanlectures.caltech.edu/III_01.html)

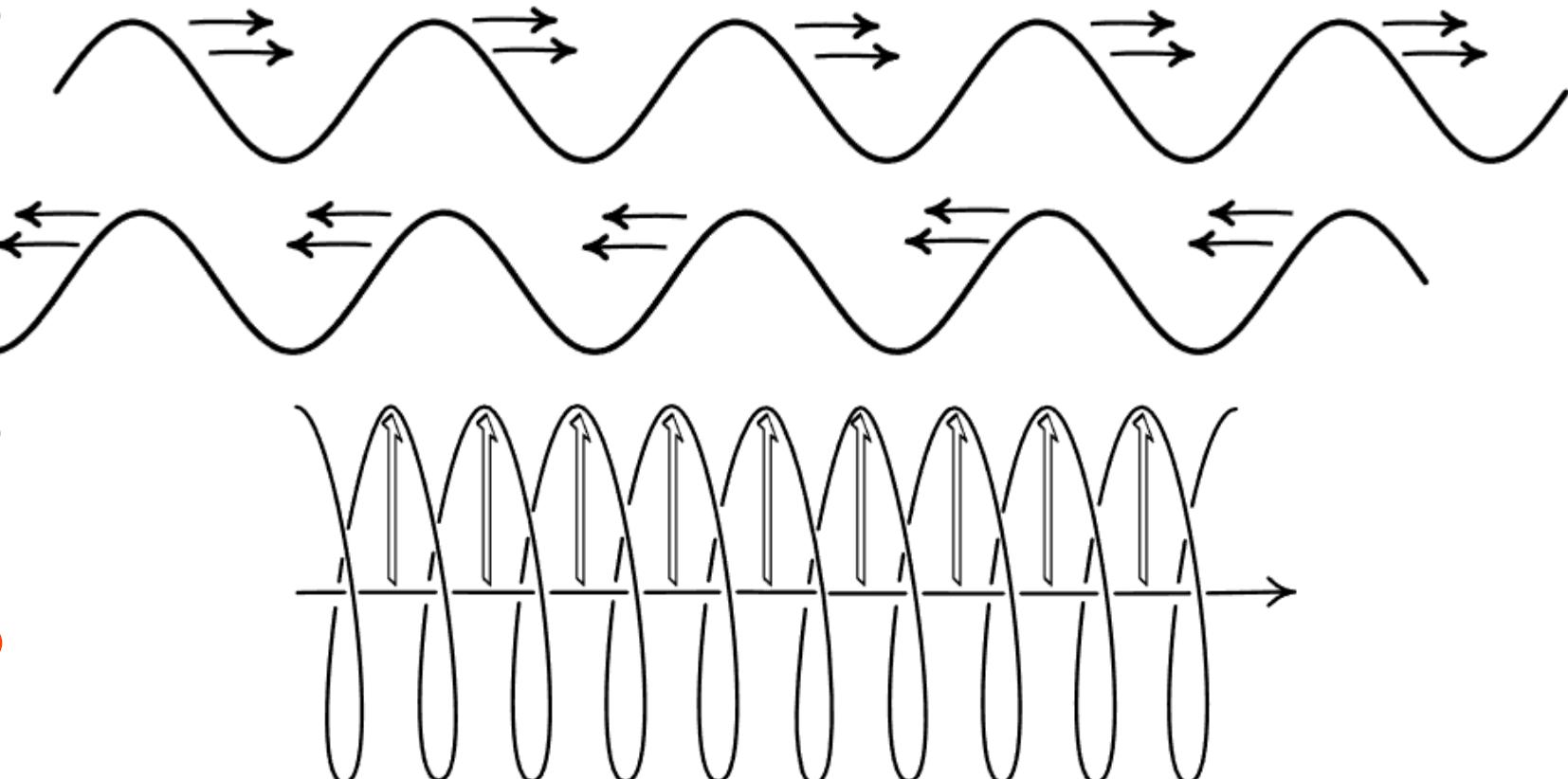


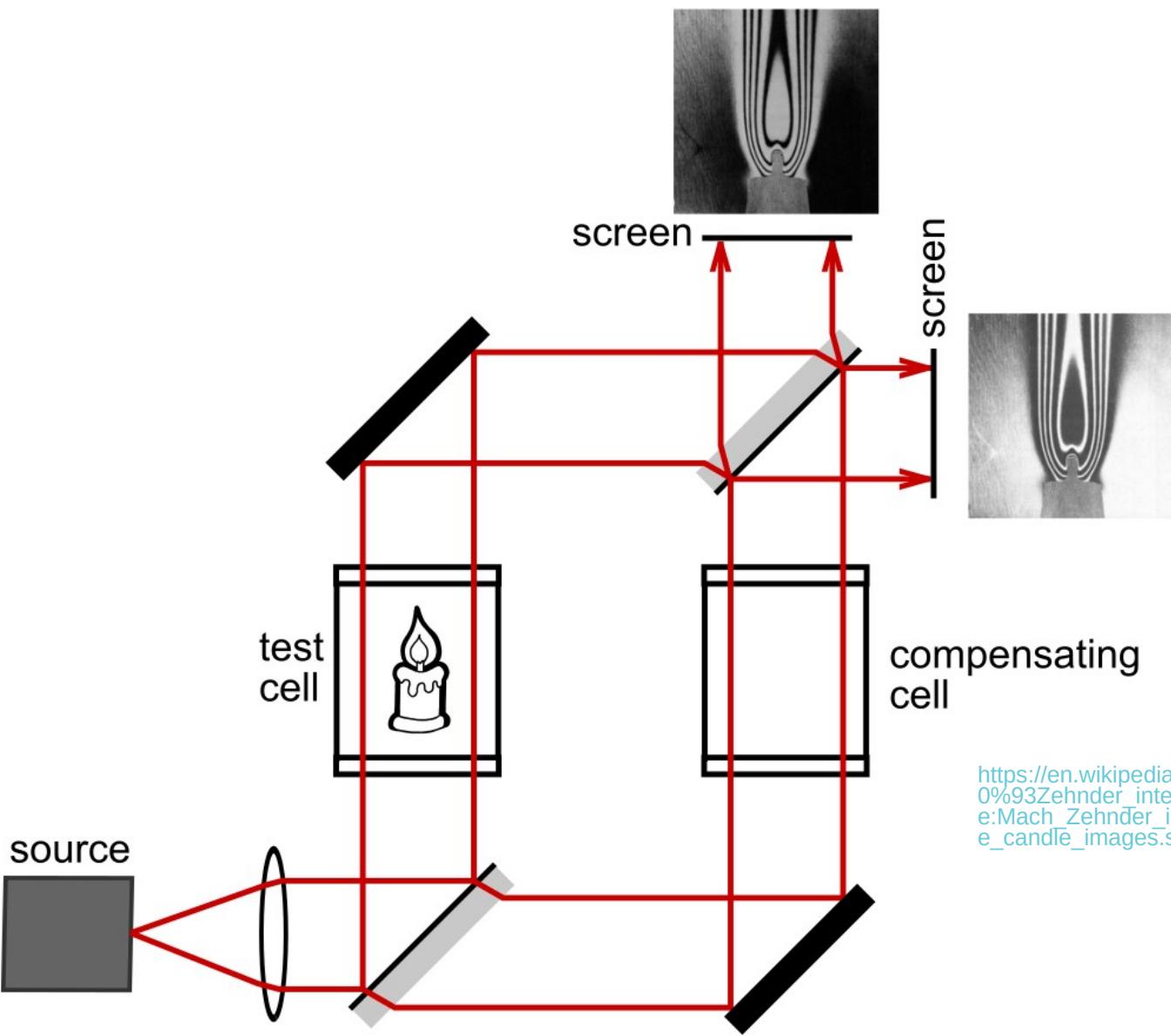
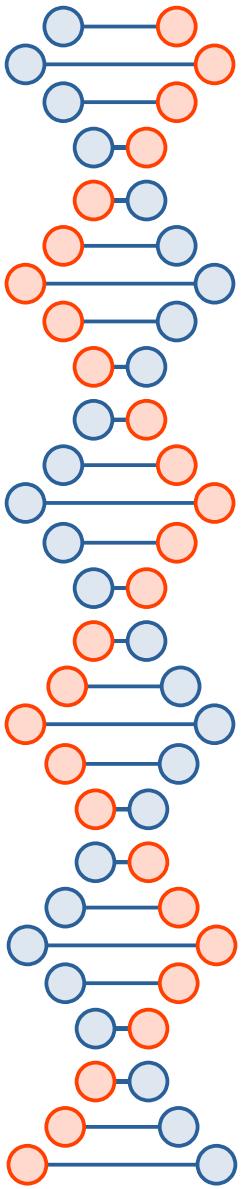
# Complex waves are a little different...



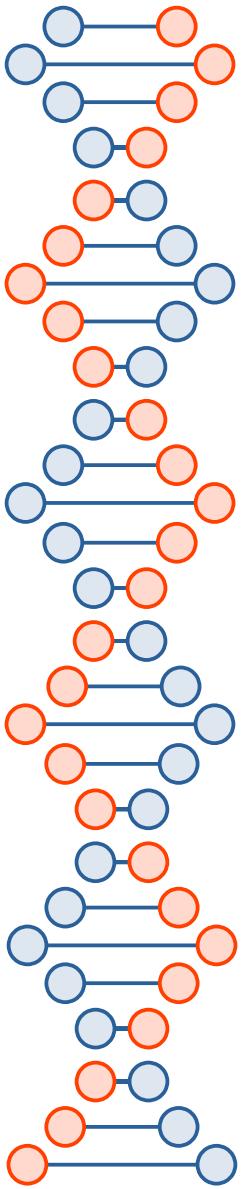


# Complex waves have direction...

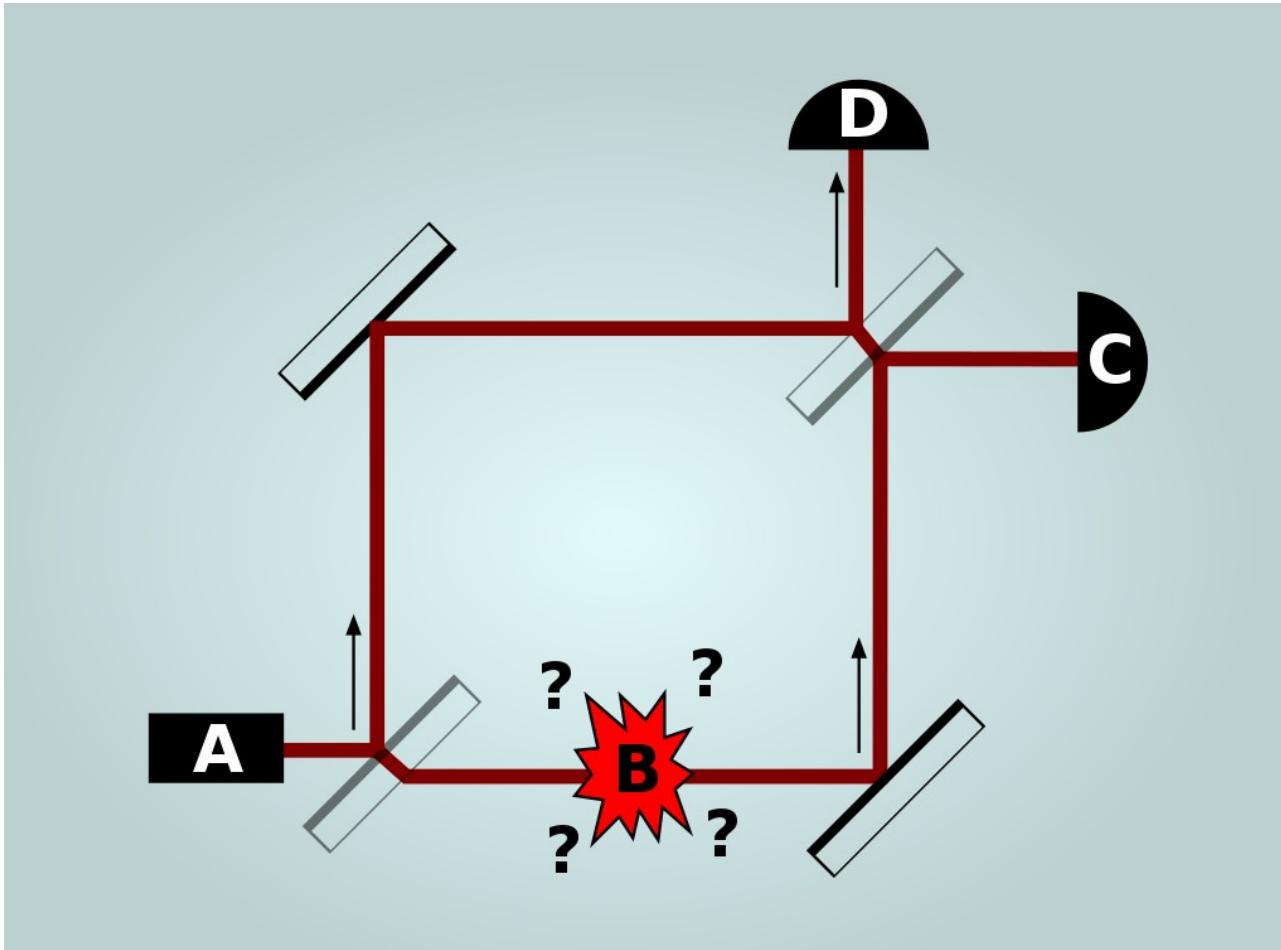


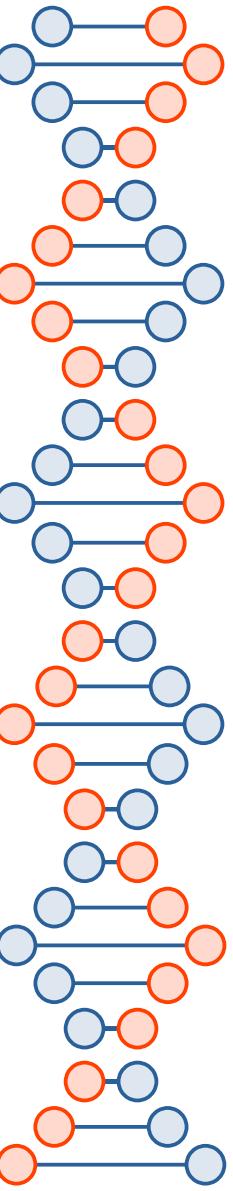


[https://en.wikipedia.org/wiki/Mach%20Zehnder\\_interferometer#/media/File:Mach\\_Zehnder\\_interferometer\\_alternate\\_candle\\_images.svg](https://en.wikipedia.org/wiki/Mach%20Zehnder_interferometer#/media/File:Mach_Zehnder_interferometer_alternate_candle_images.svg)

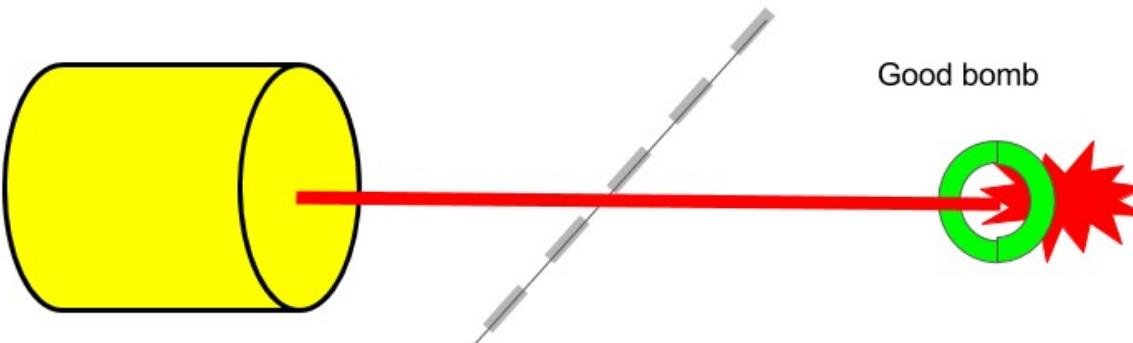


[https://en.wikipedia.org/wiki/Elitzur%20Vaidman\\_bomb\\_tester](https://en.wikipedia.org/wiki/Elitzur%20Vaidman_bomb_tester)



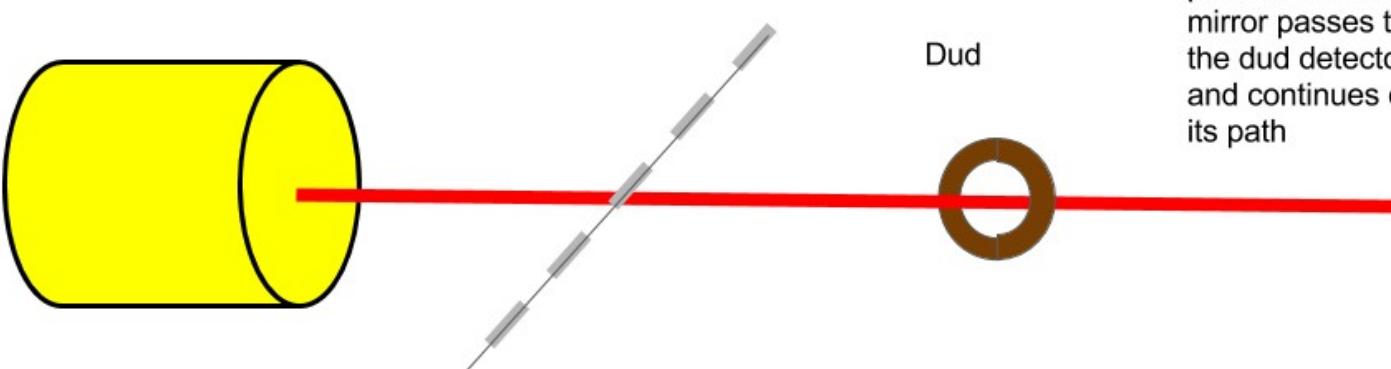


# Bomb is either live or a dud



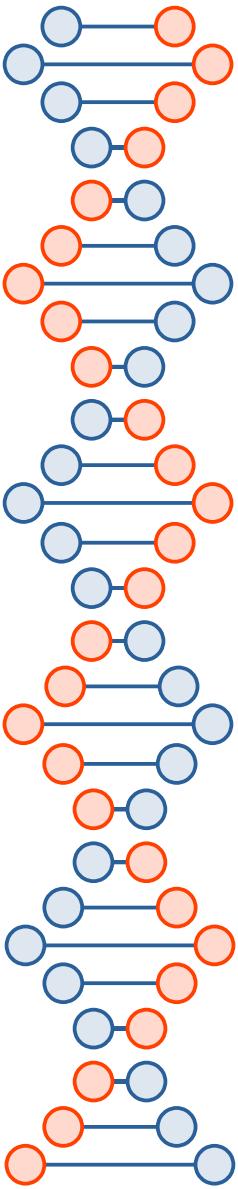
Good bomb

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

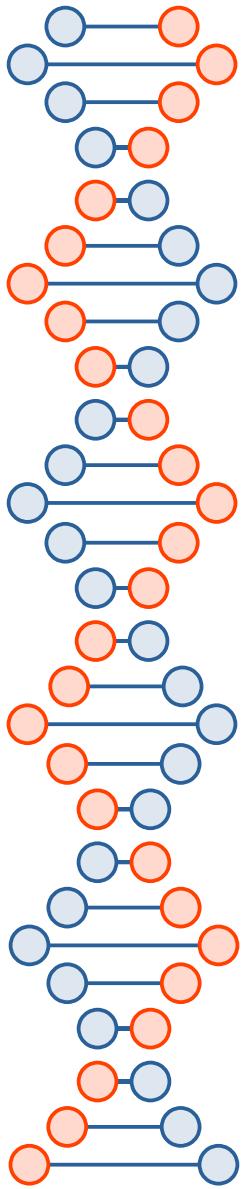


Dud

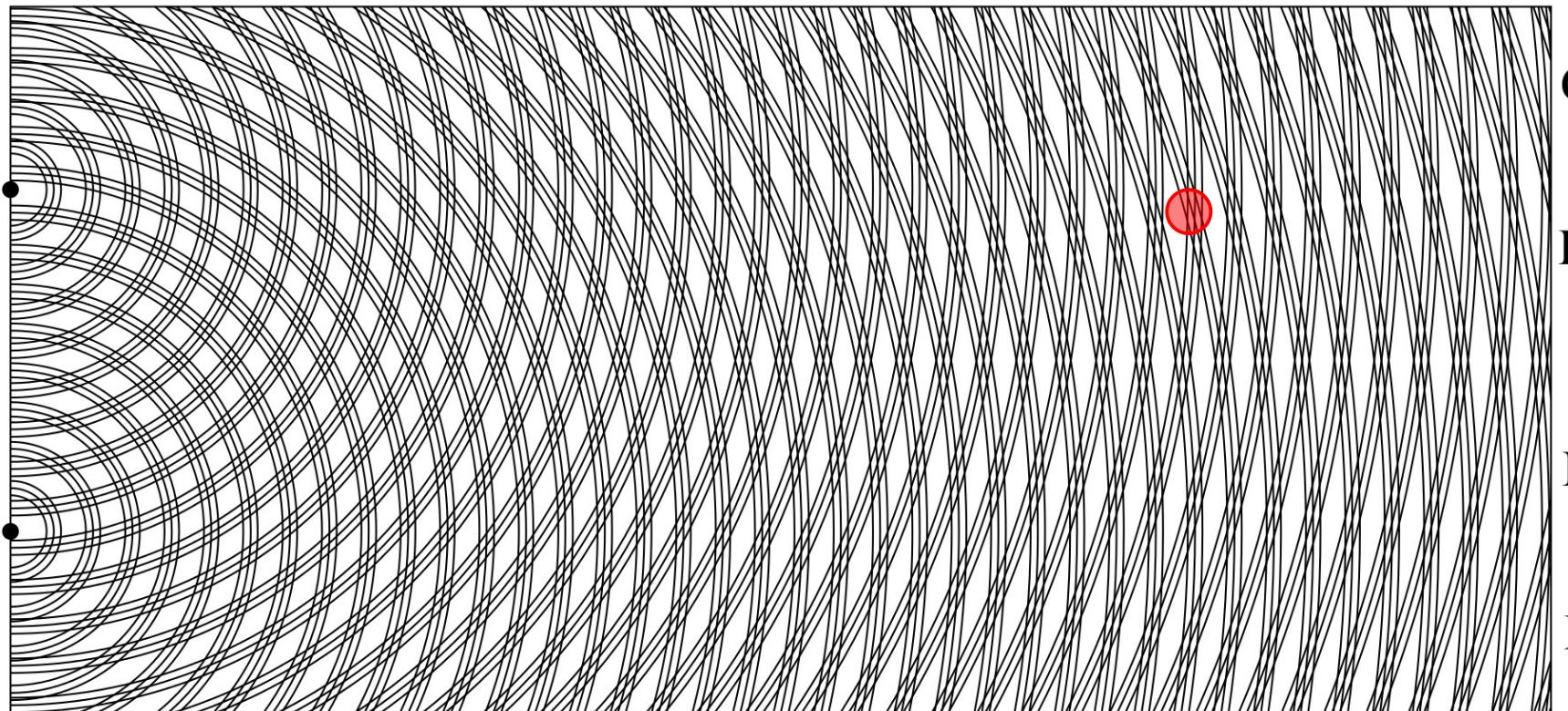
The photon that passed thru the mirror passes thru the dud detector and continues on its path

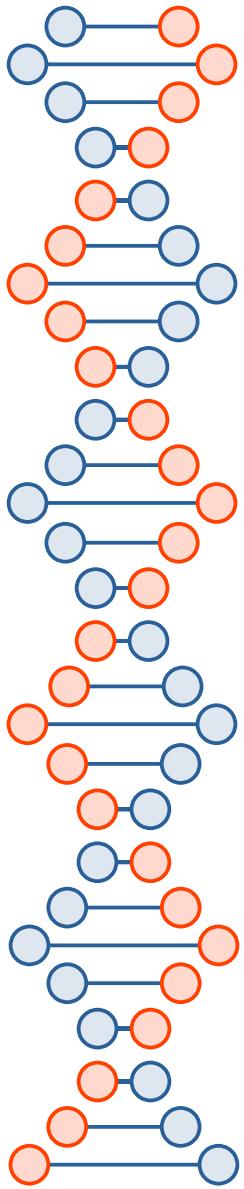


“Due to the way in which the interferometer is constructed, a photon going through the second mirror from the lower path towards detector D will have a phase shift of half a wavelength compared to a photon being reflected from the upper path towards that same detector...”

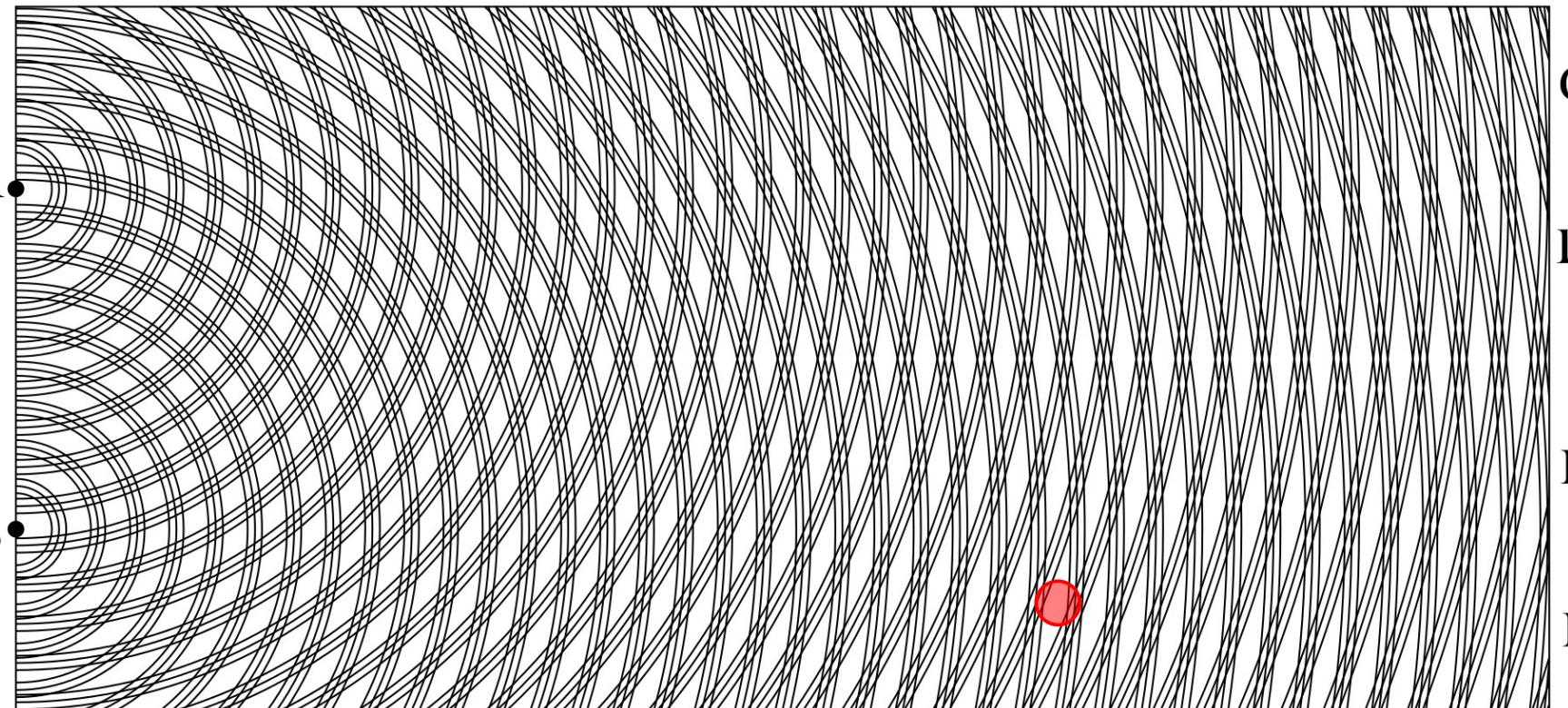


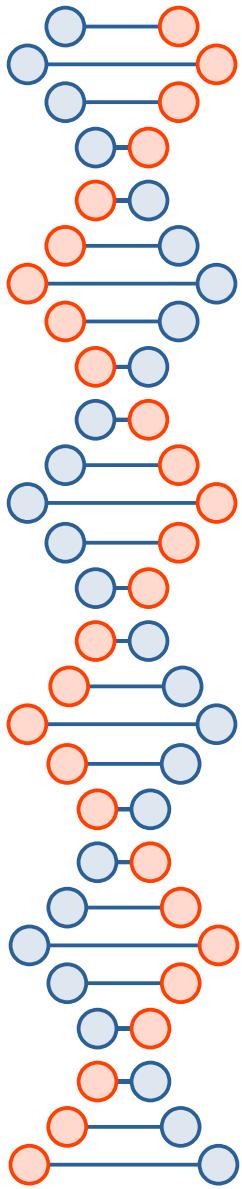
Put C, e.g., here...



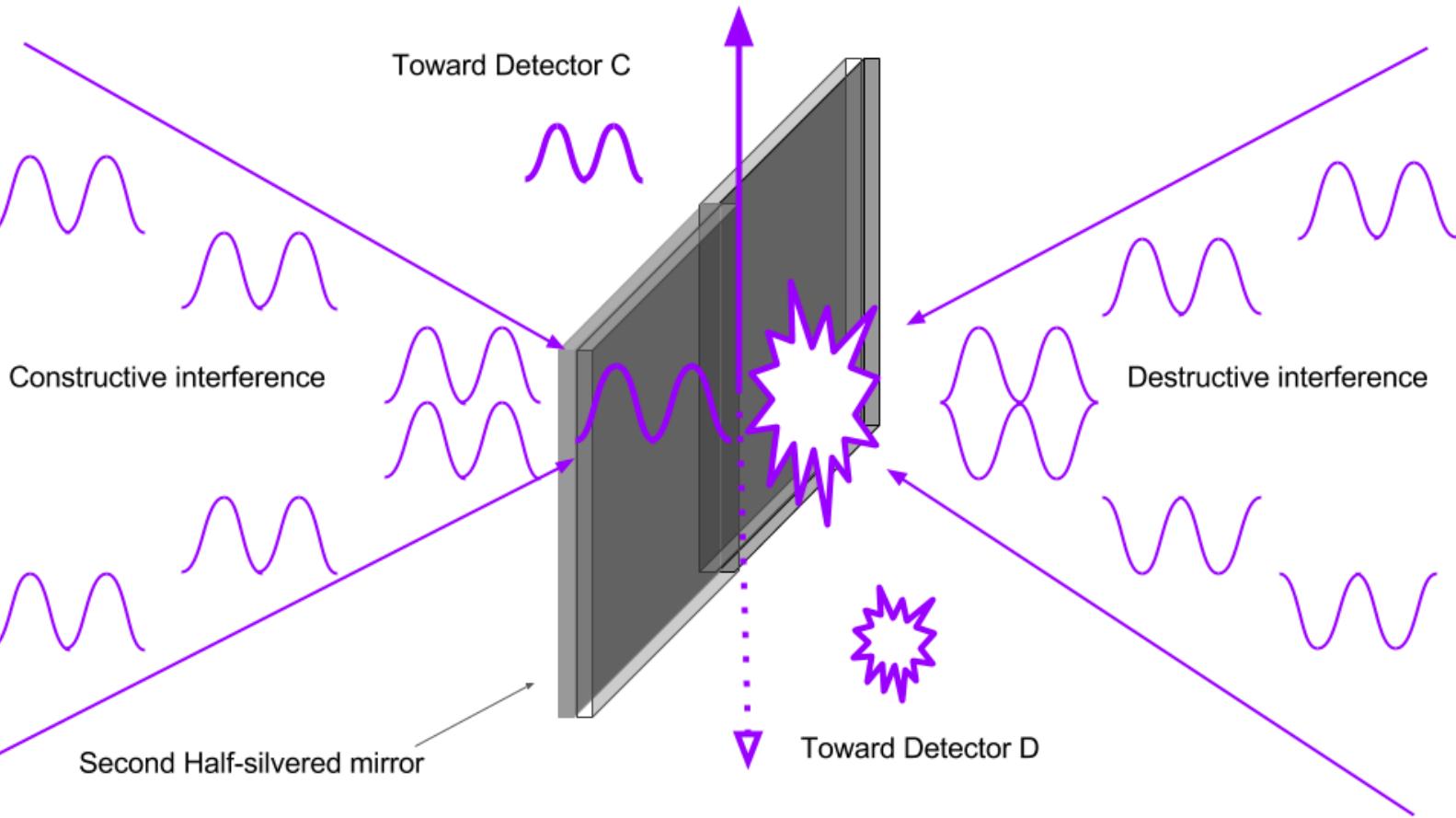


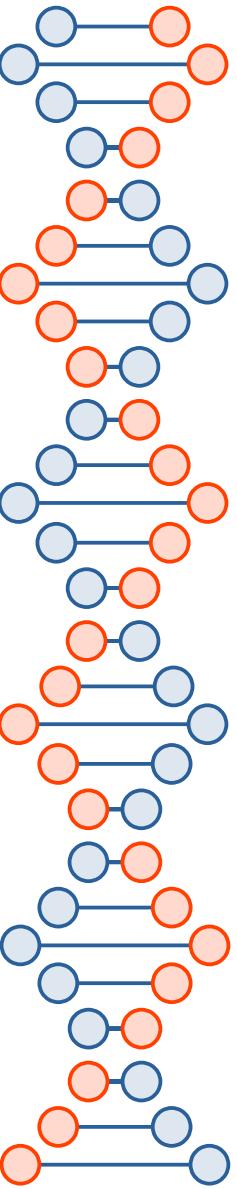
Put D, e.g., here...





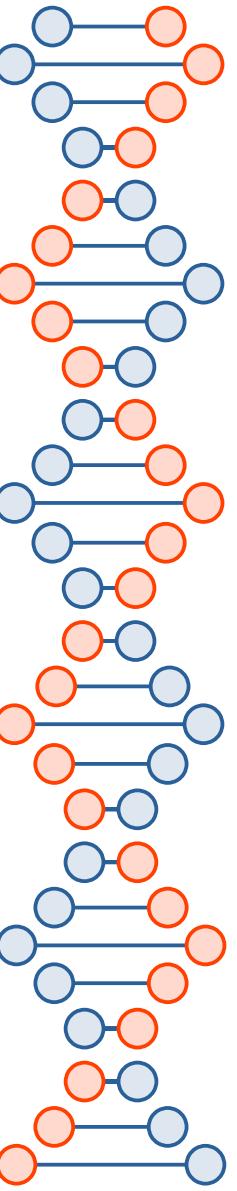
# If both waves make it to the end (dud!)...





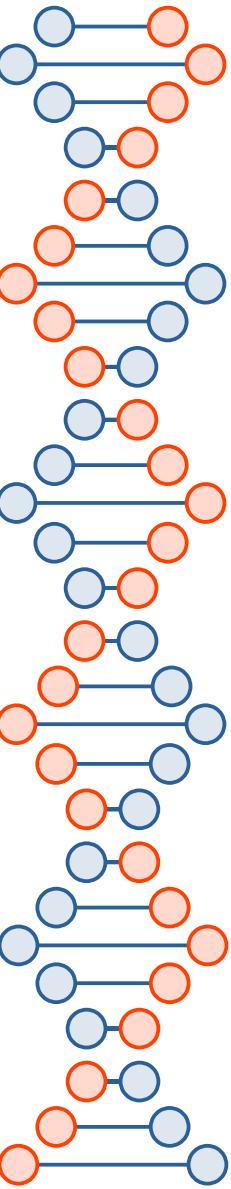
We will never detect a photon at D if the bomb is a dud.

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



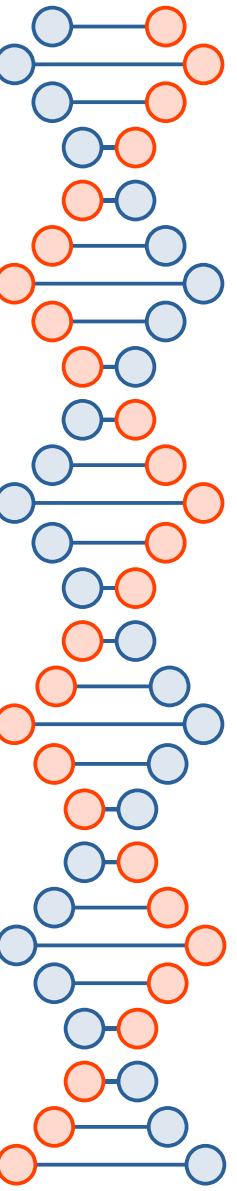
## Case #1: Bomb is a dud

- 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



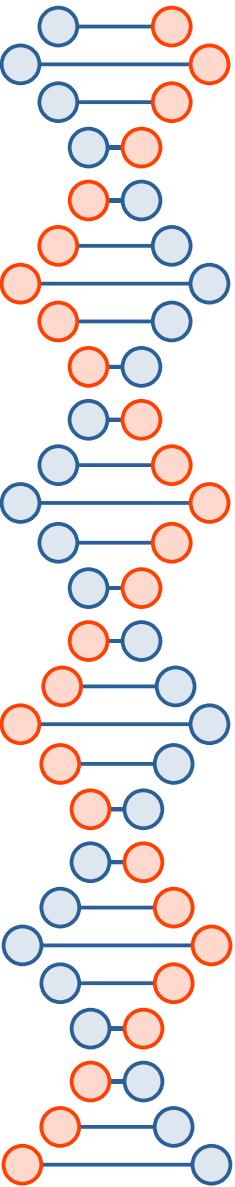
## Case #2: Bomb is live

- 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!



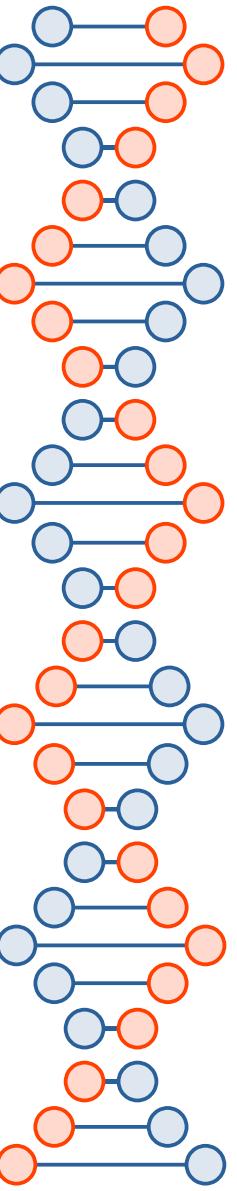
# Bomb is live (keep repeating)

- 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



# Quantum bombs vs. dog

- In Duke's tummy, an unbalanced function is like a bomb, it changes the phase on one path but not the other

Bit  
0



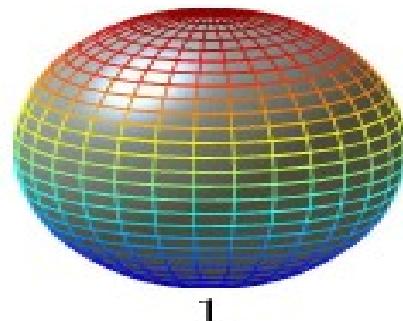
Etats: 0 ou 1

Pbit  
0



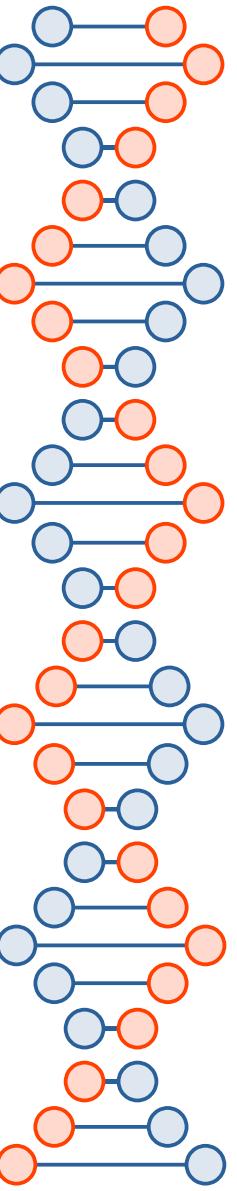
{p:0, (1-p):1}

Qubit  
0



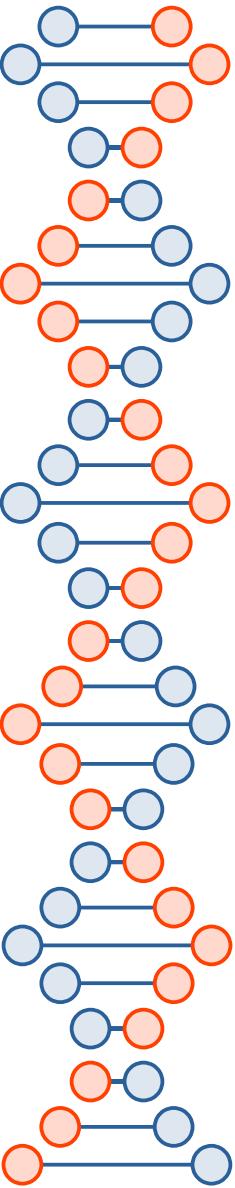
$\alpha|0\rangle + \beta|1\rangle$

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)

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

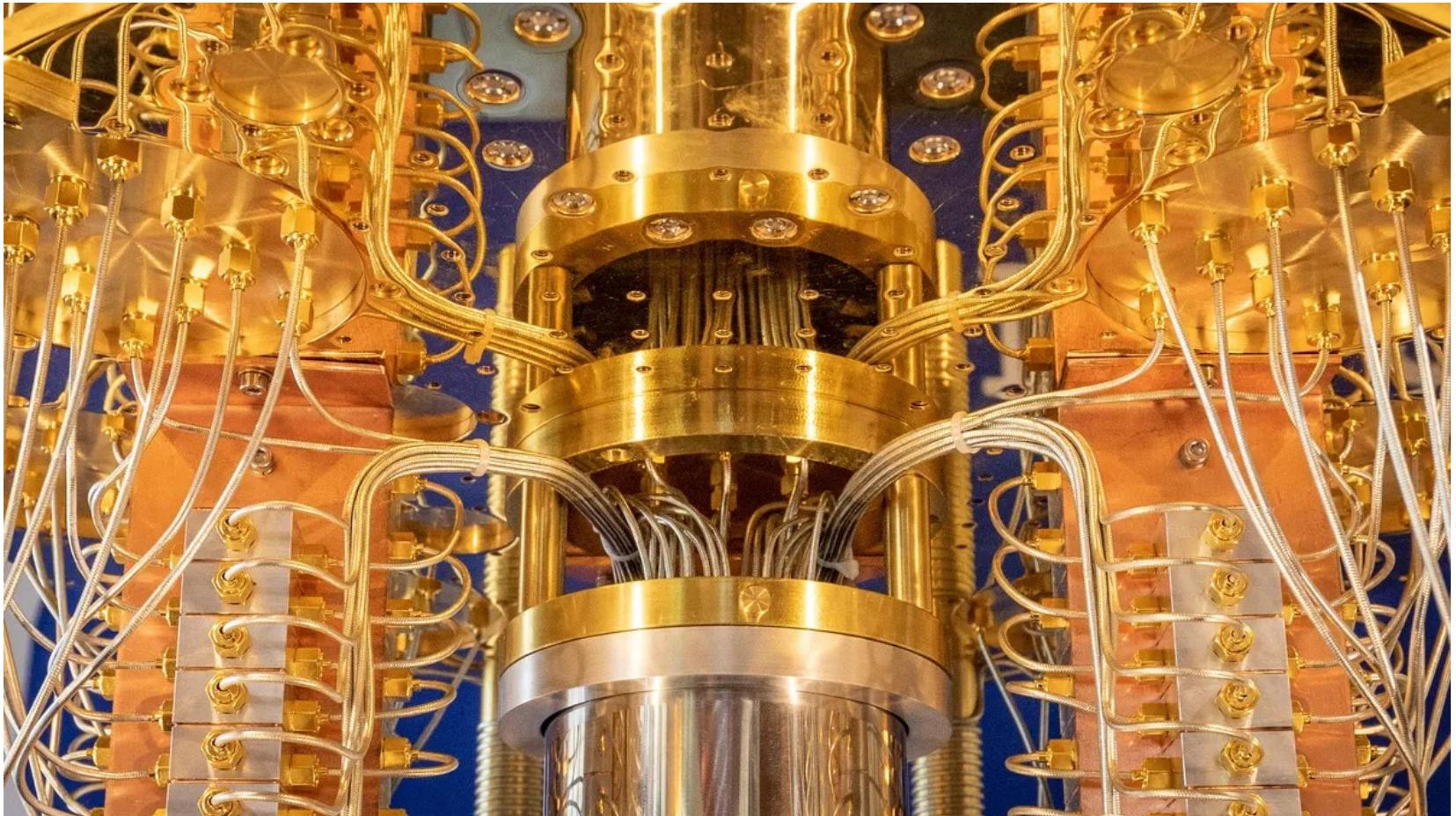
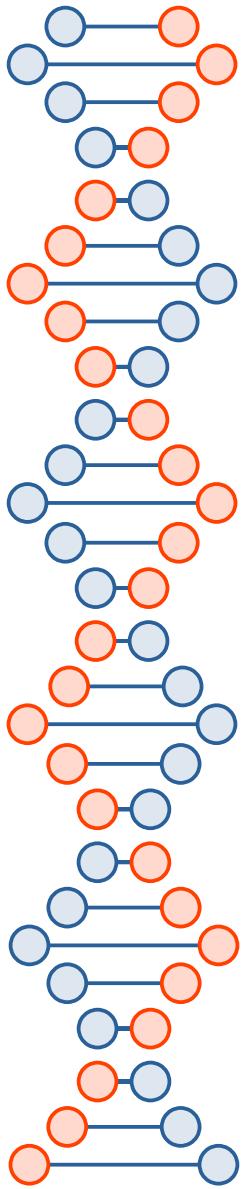
$$|\psi\rangle = \alpha\gamma|00\rangle + \alpha\delta|01\rangle + \beta\gamma|10\rangle + \beta\delta|11\rangle$$



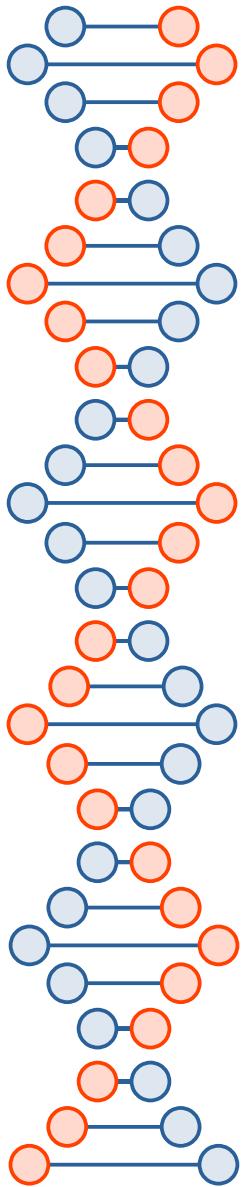
This operation is called **Tensor Product**

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

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



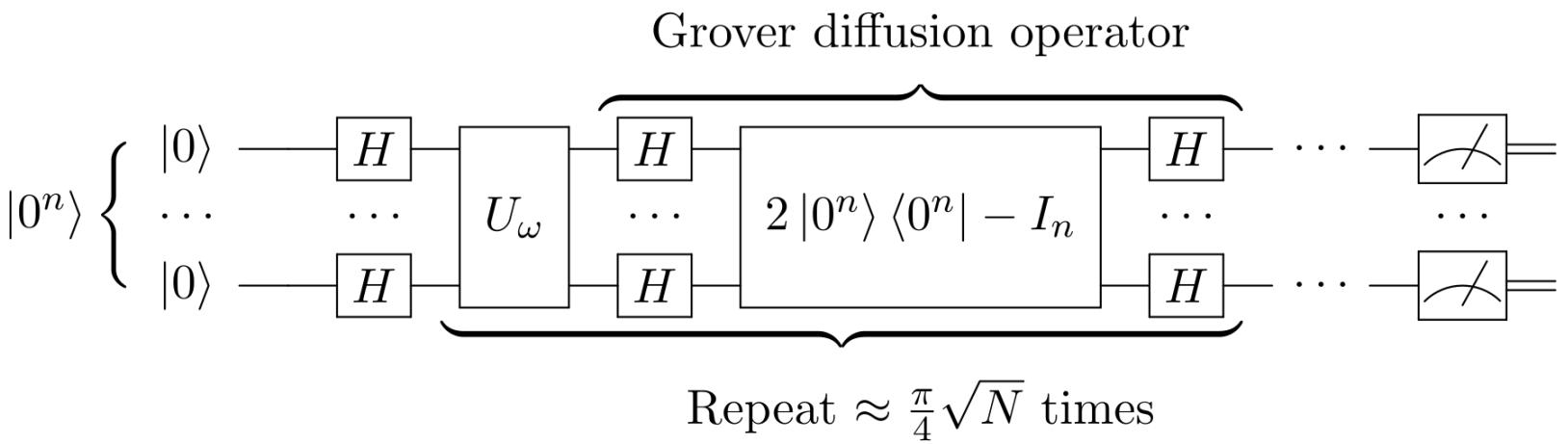
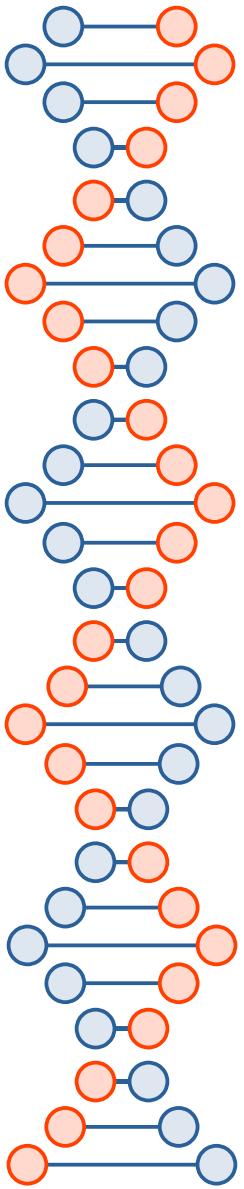
<https://www.cnet.com/tech/computing/quantum-computer-makers-like-their-odds-for-big-progress-soon/>



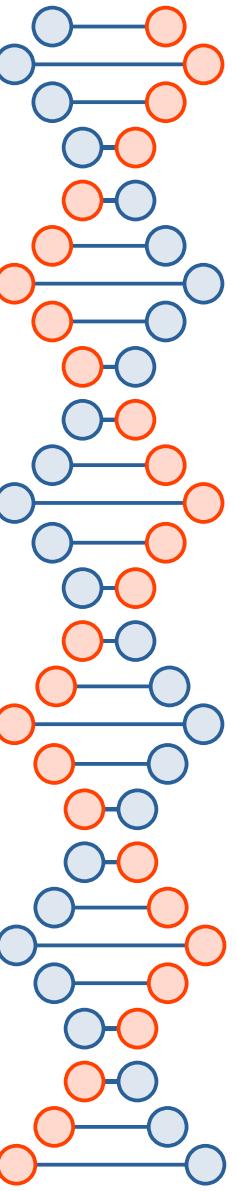
# What we need for the Internet to work...

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

# Grover's algorithm

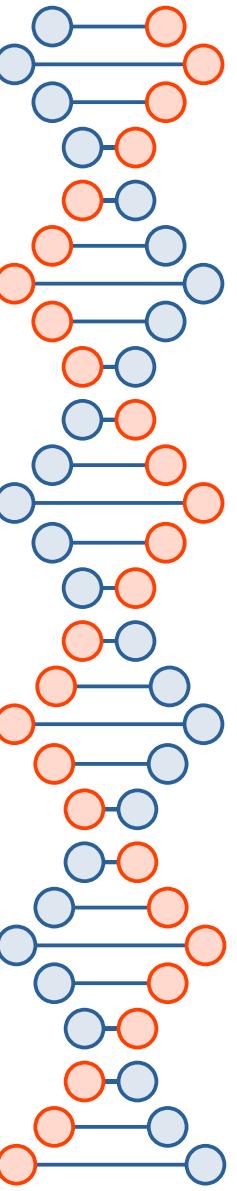


[https://en.wikipedia.org/wiki/Grover%27s\\_algorithm#/media/File:Grover's\\_algorithm\\_circuit.svg](https://en.wikipedia.org/wiki/Grover%27s_algorithm#/media/File:Grover's_algorithm_circuit.svg)



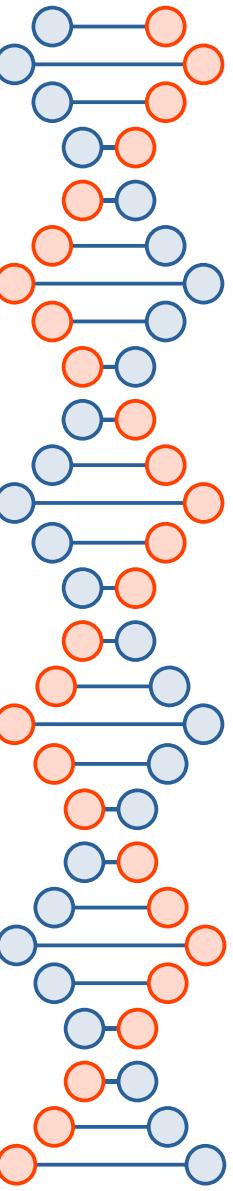
# Symmetric crypto

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

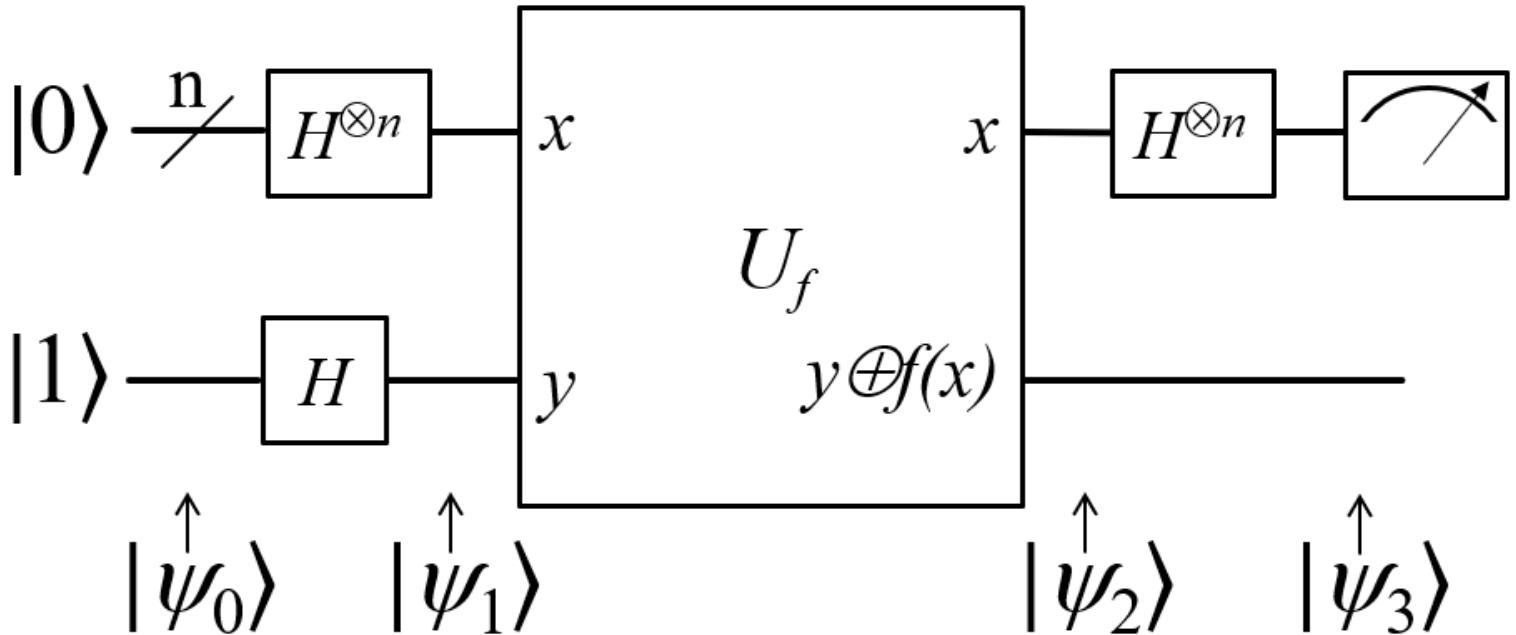


# Asymmetric Crypto

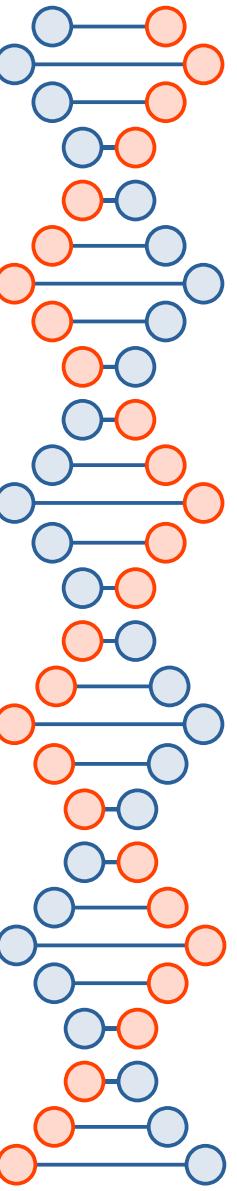
- Quantum computers seem to be good at the same kinds of things that make good, simple trapdoor functions for asymmetric crypto (factorization, discrete log, etc.)
  - But not everything
    - Older schemes (e.g., Merkle's signature scheme)
    - Newer schemes (e.g., lattice-based)
- Specifically, Shor's 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](https://en.wikipedia.org/wiki/Deutsch%E2%80%93Jozsa_algorithm#/media/File:Deutsch-Jozsa-algorithm-quantum-circuit.png)



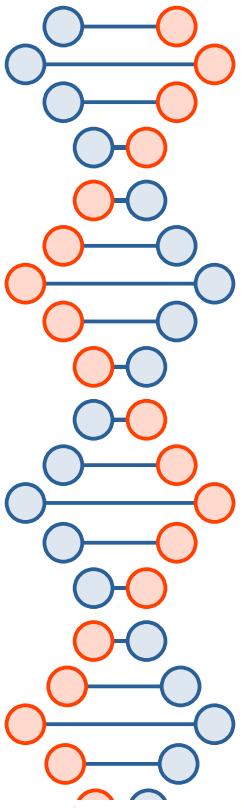
## 1-bit input case...

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

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

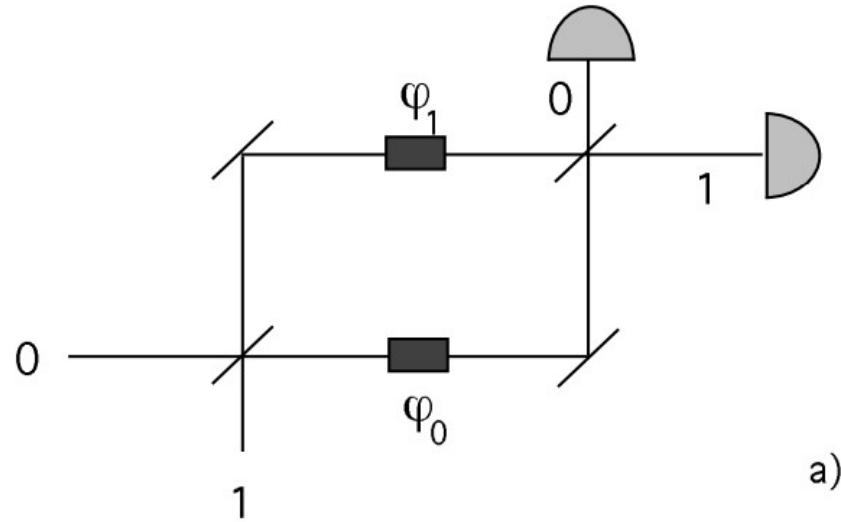
A balanced function cancels itself out because of destructive interference

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

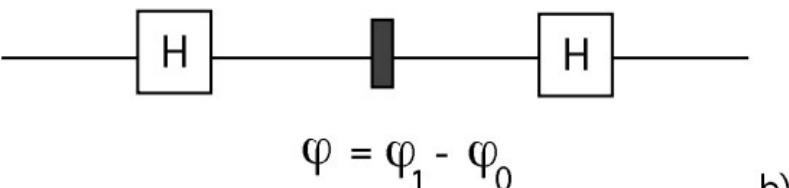


<https://arxiv.org/abs/quant-ph/9708016>

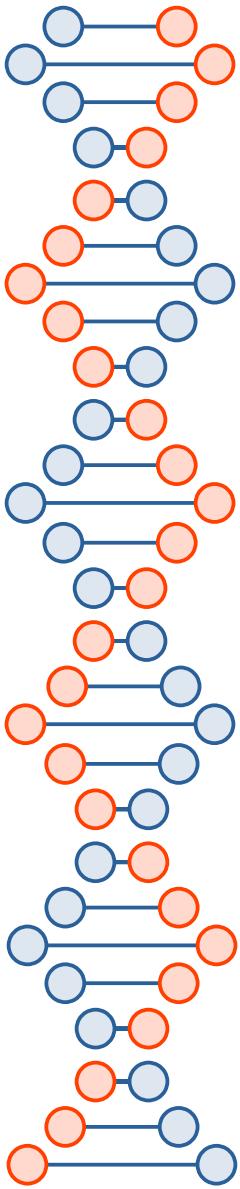
$$\begin{aligned} |0\rangle &\xrightarrow{H} \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \\ |1\rangle &\xrightarrow{H} \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \end{aligned}$$



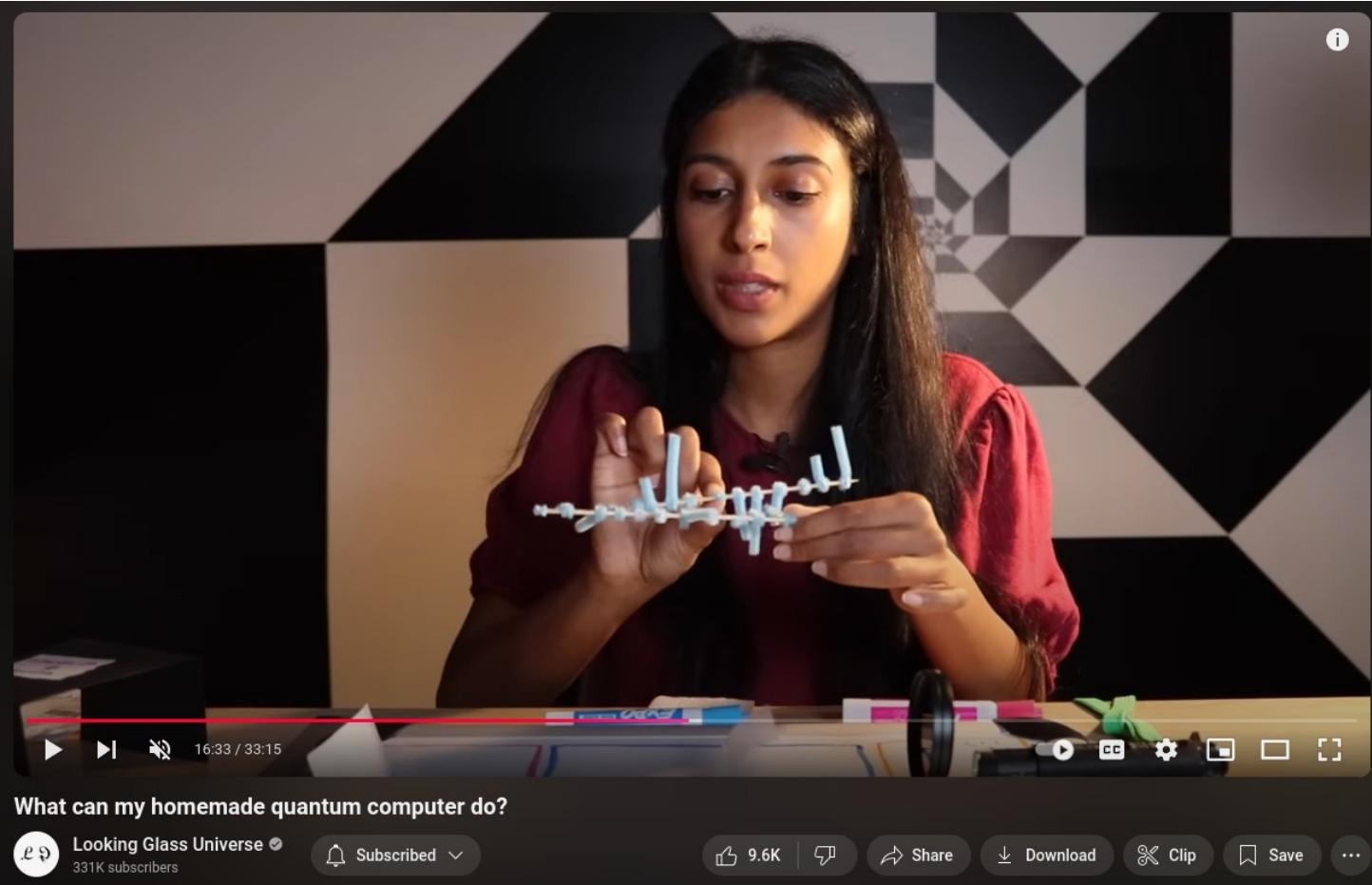
a)

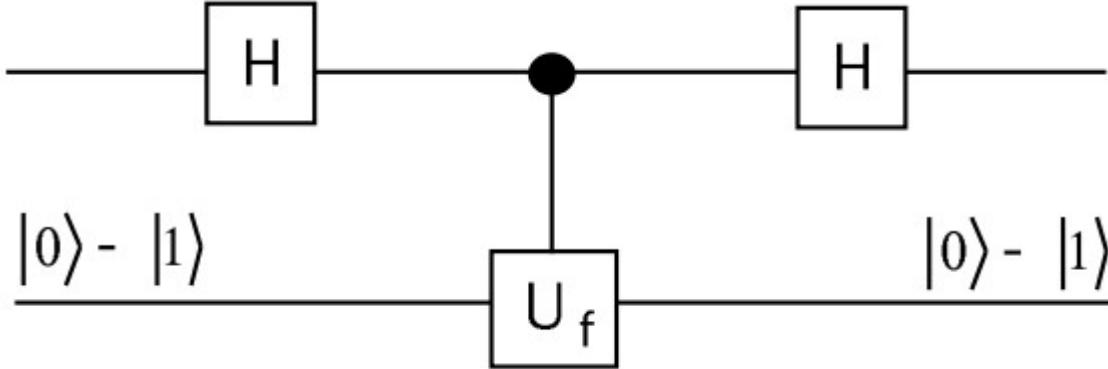
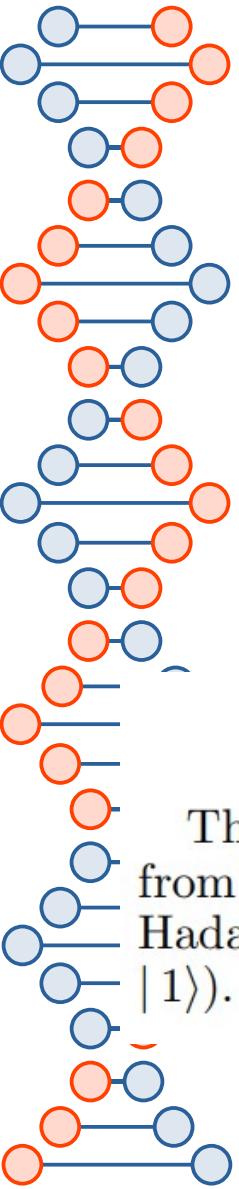


b)



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

$$|x\rangle(|0\rangle - |1\rangle) \xrightarrow{f\text{-controlled-NOT}} |x\rangle(|0\oplus f(x)\rangle - |1\oplus f(x)\rangle) = (-1)^{f(x)} |x\rangle(|0\rangle - |1\rangle). \quad (2.2)$$

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

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

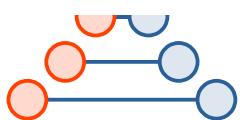
That is, for each  $x$ , the  $|x\rangle$  term acquires a phase factor of  $(-1)^{f(x)}$ , which corresponds to the eigenvalue of the state of the auxiliary qubit under the action of the operator that sends  $|y\rangle$  to  $|y\oplus f(x)\rangle$ .

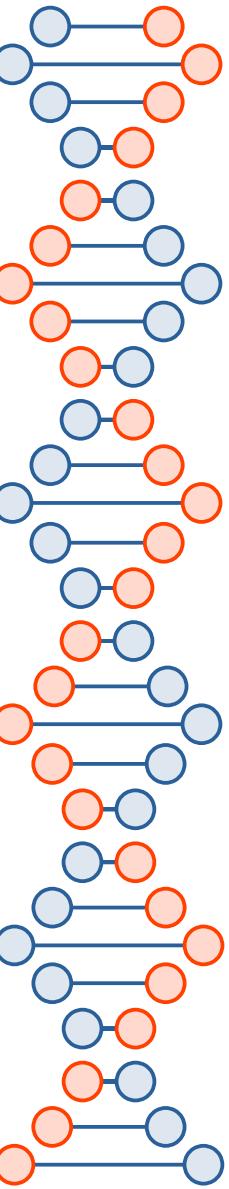
This state can also be written as

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

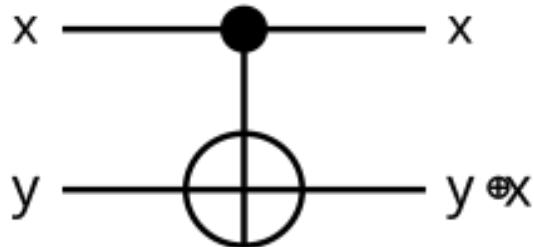
which, after applying the second Hadamard transform, becomes

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



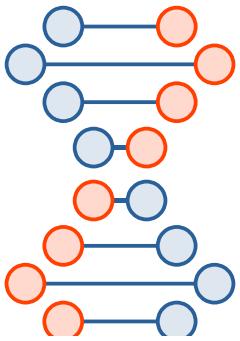


# CNOT (Wikipedia)



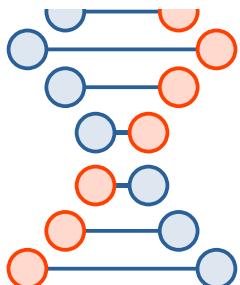
input		output	
x	y	x	y+x
$ 0\rangle$	$ 0\rangle$	$ 0\rangle$	$ 0\rangle$
$ 0\rangle$	$ 1\rangle$	$ 0\rangle$	$ 1\rangle$
$ 1\rangle$	$ 0\rangle$	$ 1\rangle$	$ 1\rangle$
$ 1\rangle$	$ 1\rangle$	$ 1\rangle$	$ 0\rangle$

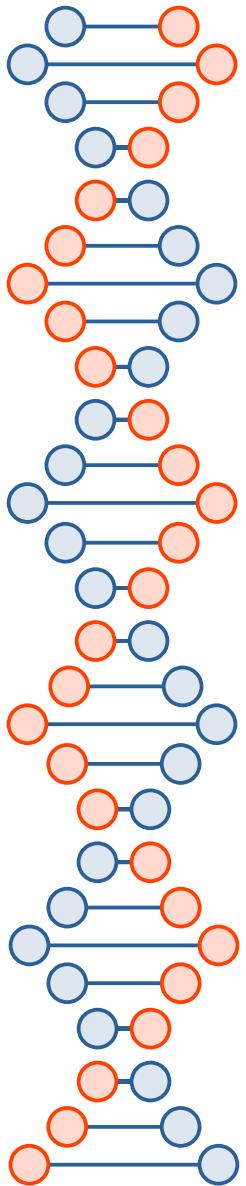
input		output	
x	y	x	y+x
0	0	0	0
0	1	0	1
1	0	1	1
1	1	1	0



[https://en.wikipedia.org/wiki/Controlled\\_NOT\\_gate](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$





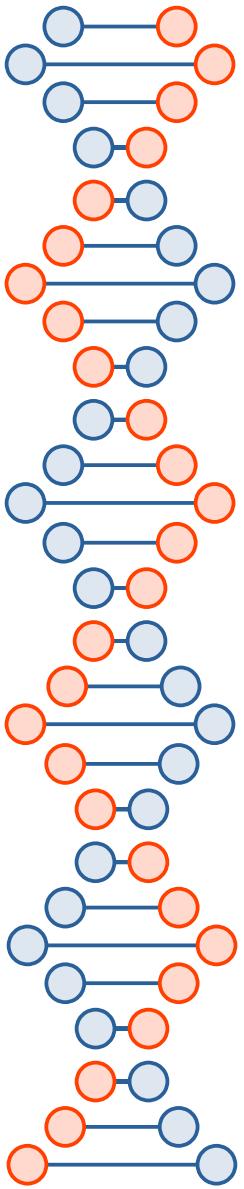
Operator	Gate(s)	Matrix
<b>Pauli-X (X)</b>		$\oplus$ $\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$
<b>Pauli-Y (Y)</b>		$\begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}$
<b>Pauli-Z (Z)</b>		$\begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$
<b>Hadamard (H)</b>		$\frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\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

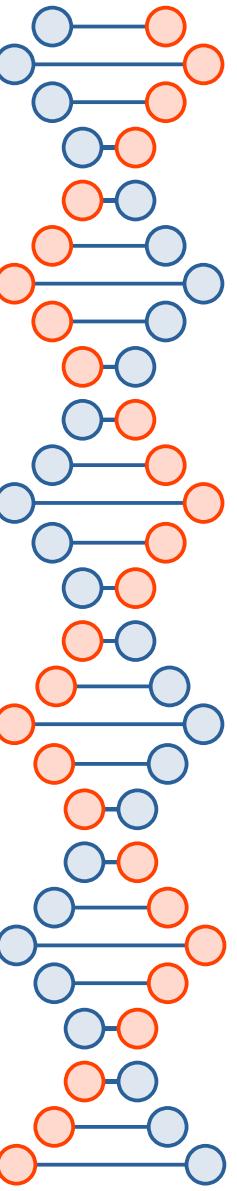
$$H_0 = +(\mathbf{1})$$

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

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

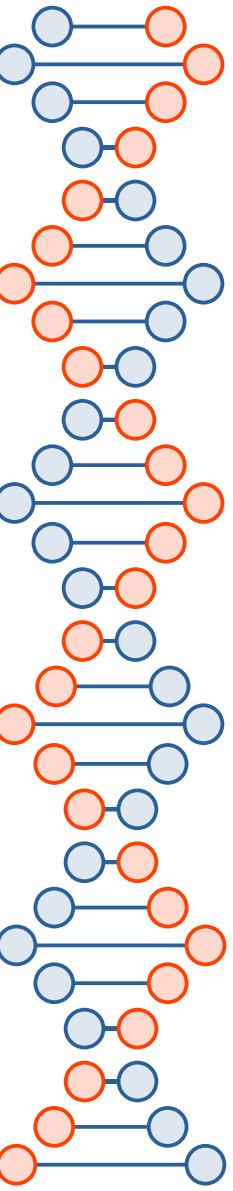
$$H_3 = \frac{1}{2^{3/2}} \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 & 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 & 1 & -1 & -1 & 1 \\ 1 & 1 & 1 & 1 & -1 & -1 & -1 & -1 \\ 1 & -1 & 1 & -1 & -1 & 1 & -1 & 1 \\ 1 & 1 & -1 & -1 & -1 & -1 & 1 & 1 \\ 1 &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



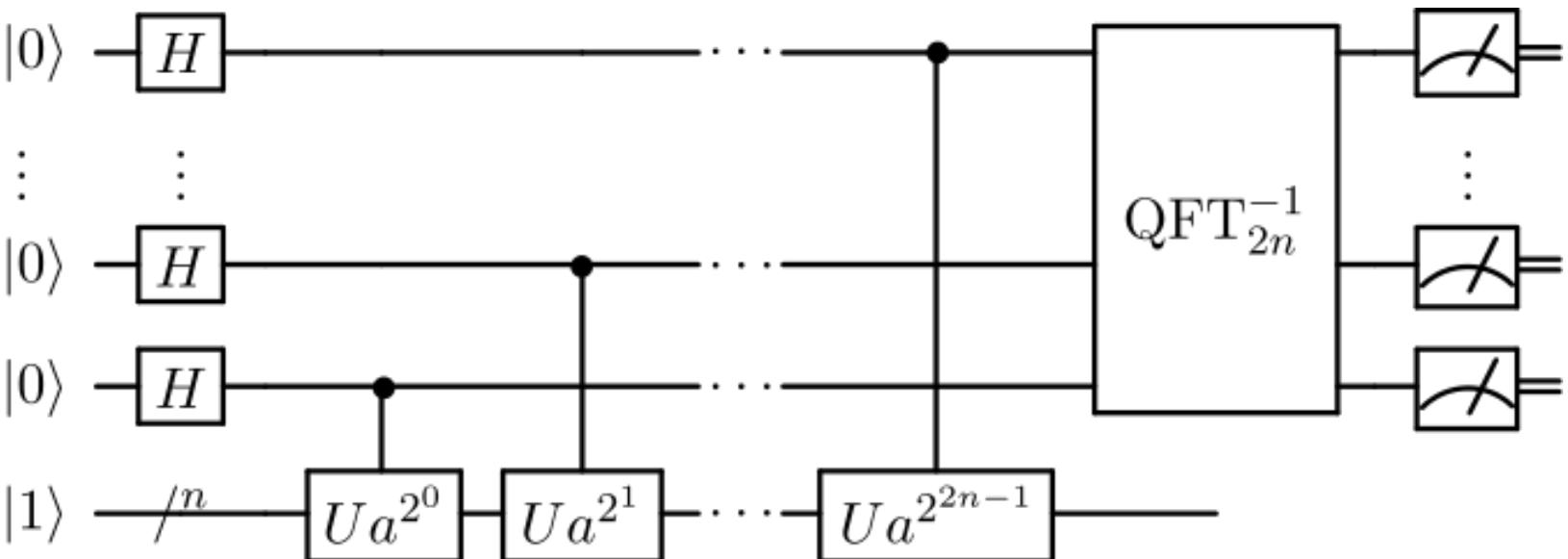


# How to attack crypto...

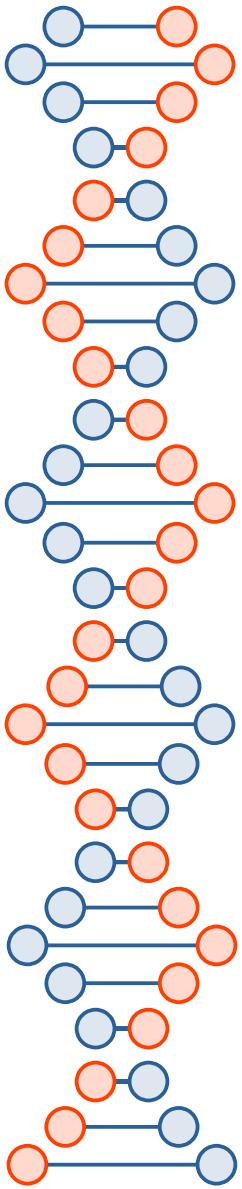
- XOR properties → Quantum computers can do a form of XOR where causality is reversed
- Frequency analysis → Quantum computers are really good at this
  - Balanced vs. unbalanced is a simple case of frequency analysis of a function.
- Side channels → Quantum computers can give us info about things that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



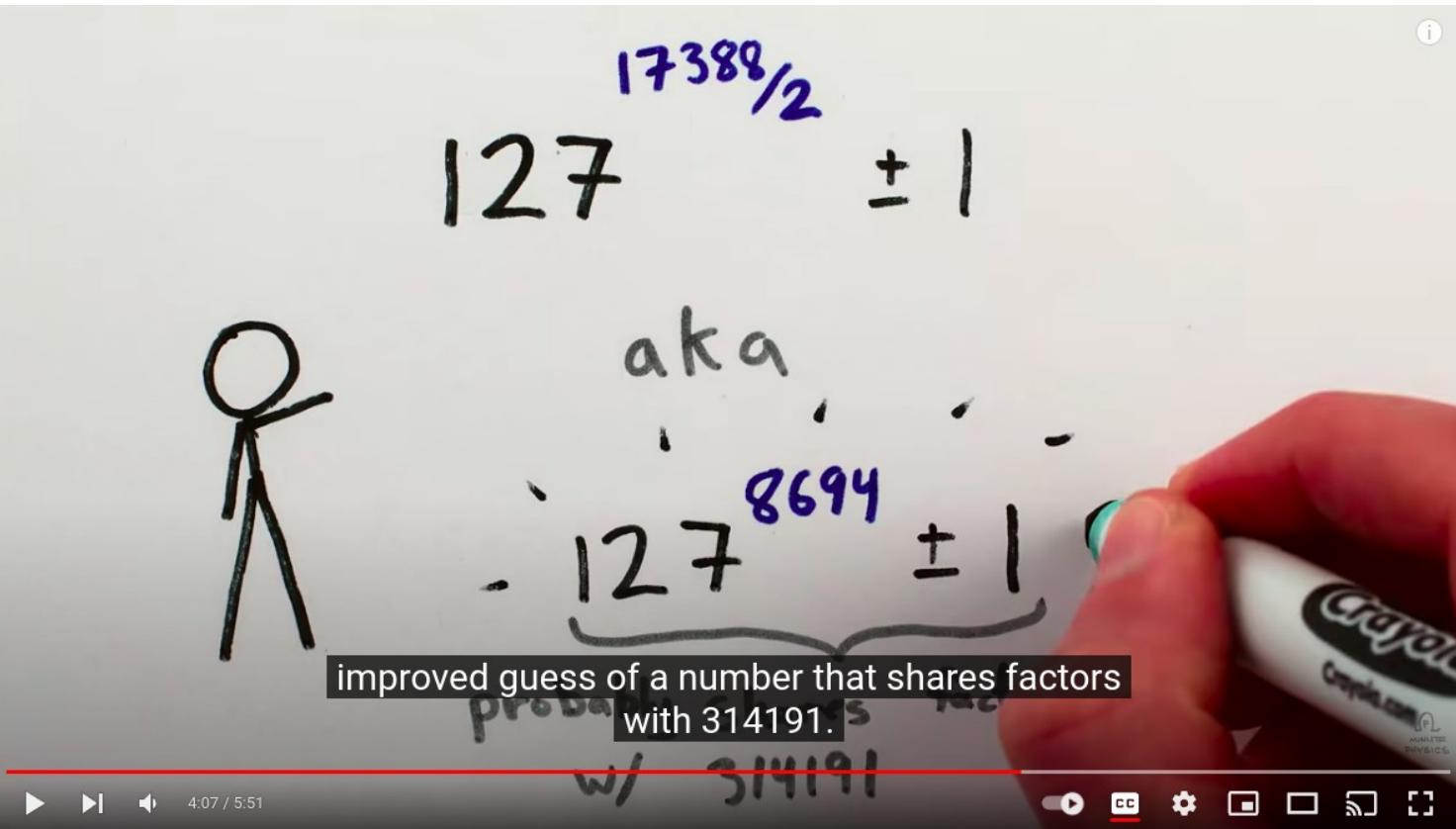
# Shor's algorithm

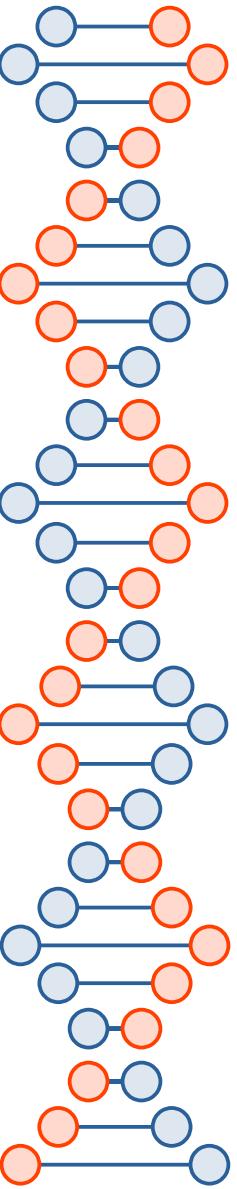


[https://en.wikipedia.org/wiki/Shor%27s\\_algorithm#/media/File:Shor's\\_algorithm.svg](https://en.wikipedia.org/wiki/Shor%27s_algorithm#/media/File:Shor's_algorithm.svg)

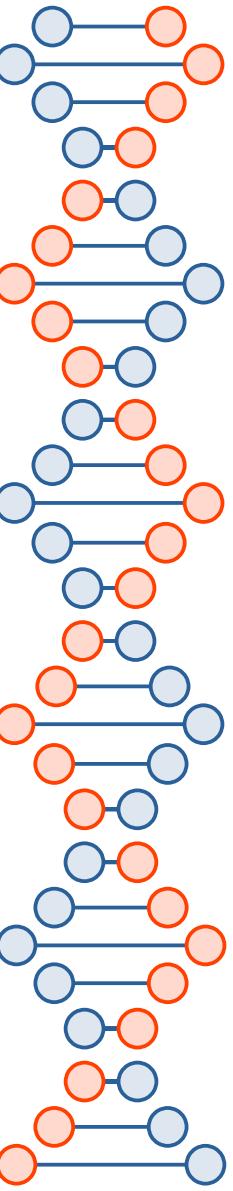


<https://www.youtube.com/watch?v=FRZQ-efABeQ>





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

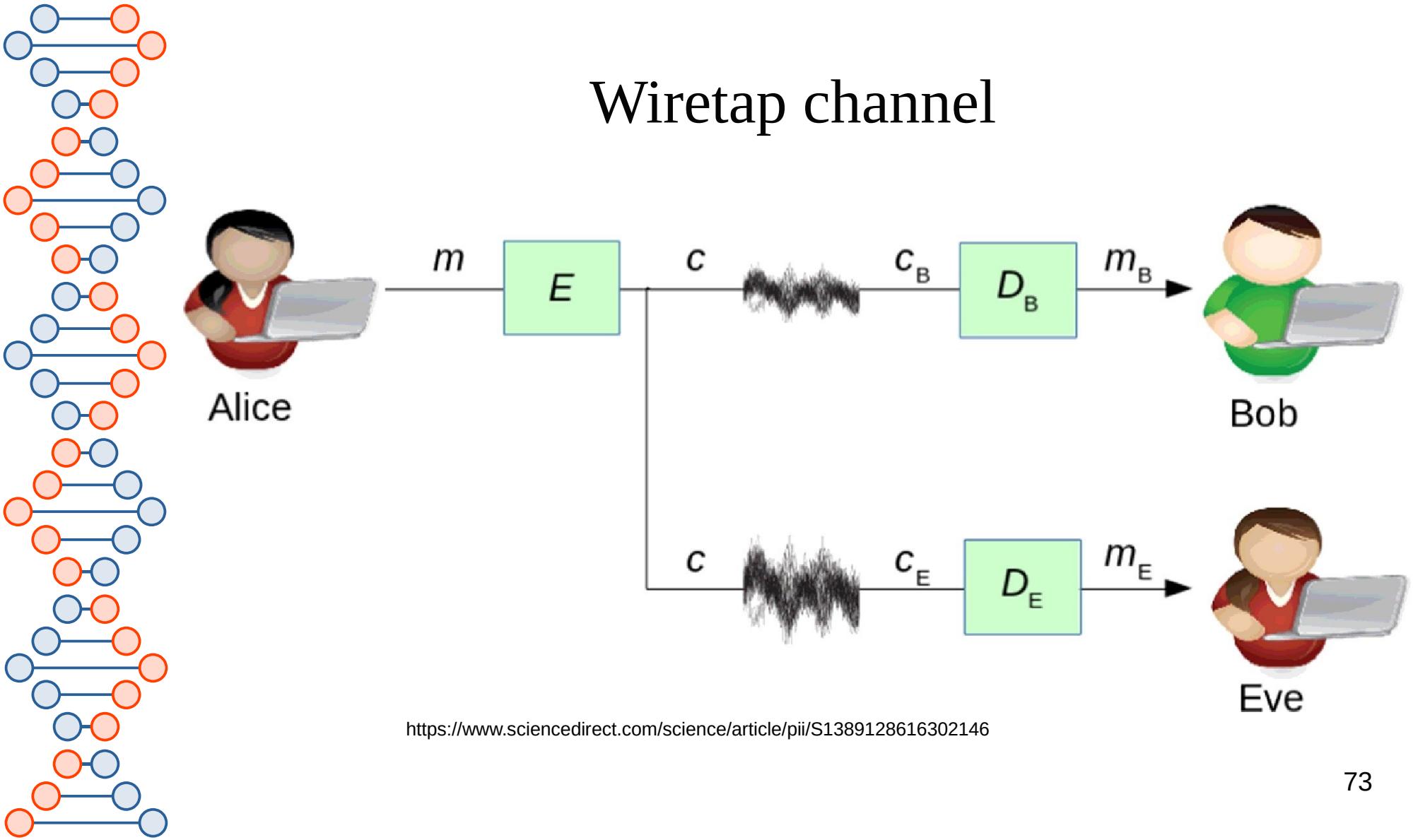


# Lamport signature (1979)

- 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

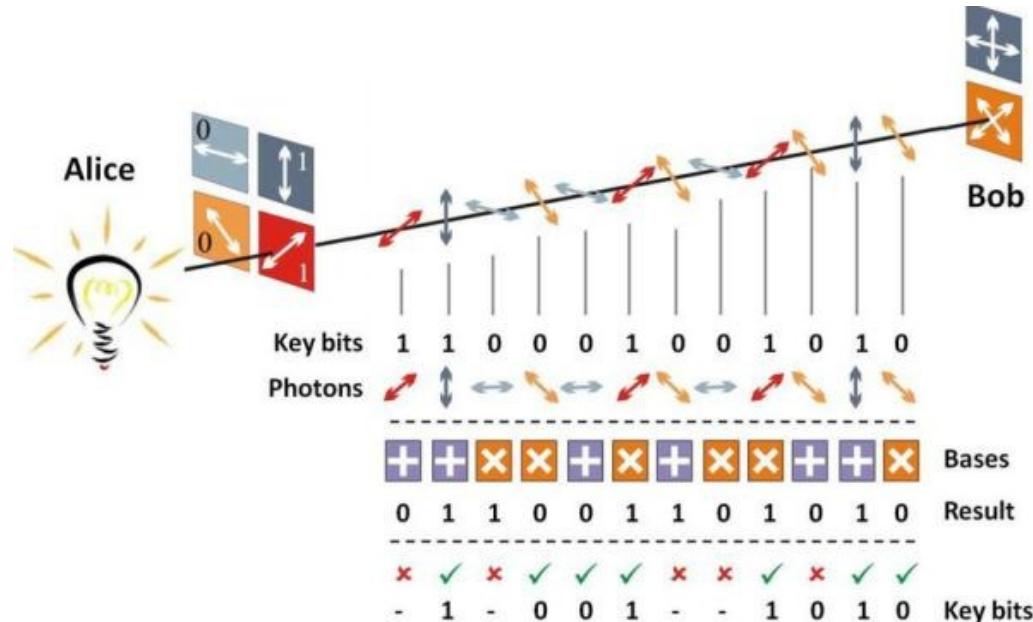
[https://en.wikipedia.org/wiki/Lamport\\_signature](https://en.wikipedia.org/wiki/Lamport_signature)

# Wiretap channel

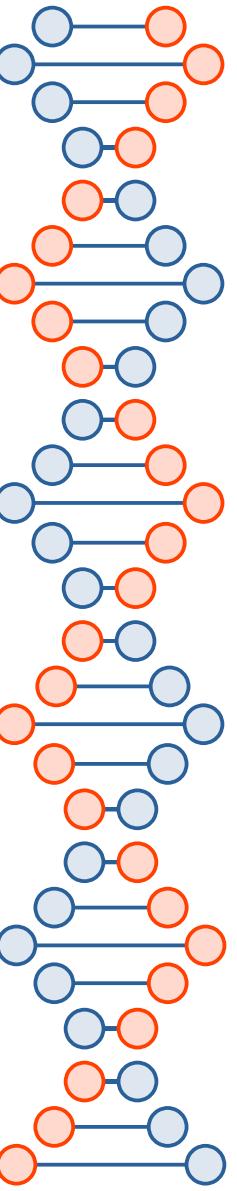


<https://www.sciencedirect.com/science/article/pii/S1389128616302146>

# Quantum Key Distribution

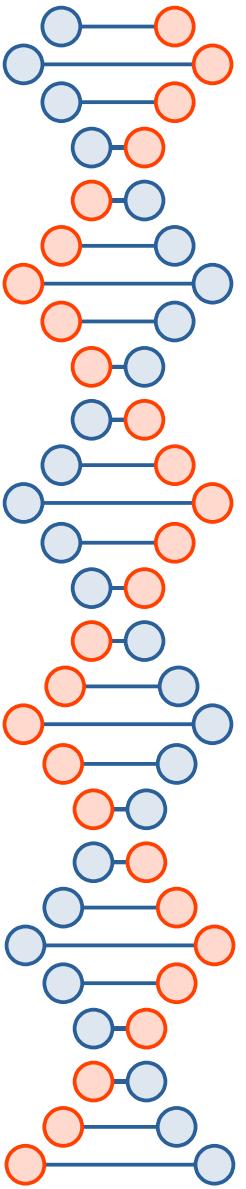


<https://imrmedia.in/quantum-key-distribution-test-successfully-demonstrated/>



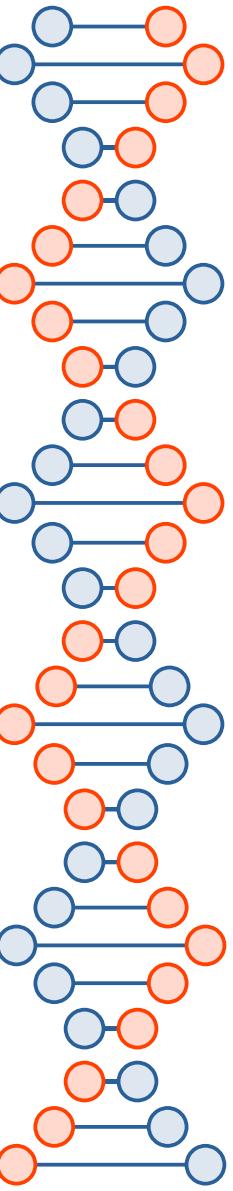
# QKD vs. Quantum-resistant

- 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!