Brief overview of quantum computers, post-quantum cryptography

CSE 548 Spring 2026

jedimaestro@asu.edu

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

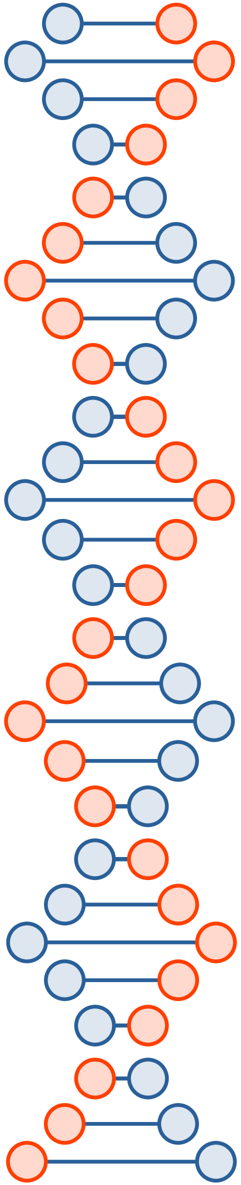
(Network security is profoundly affected by the answer, *e.g.*, TLS and SSH.)

Open question: Does the universe permit *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.)

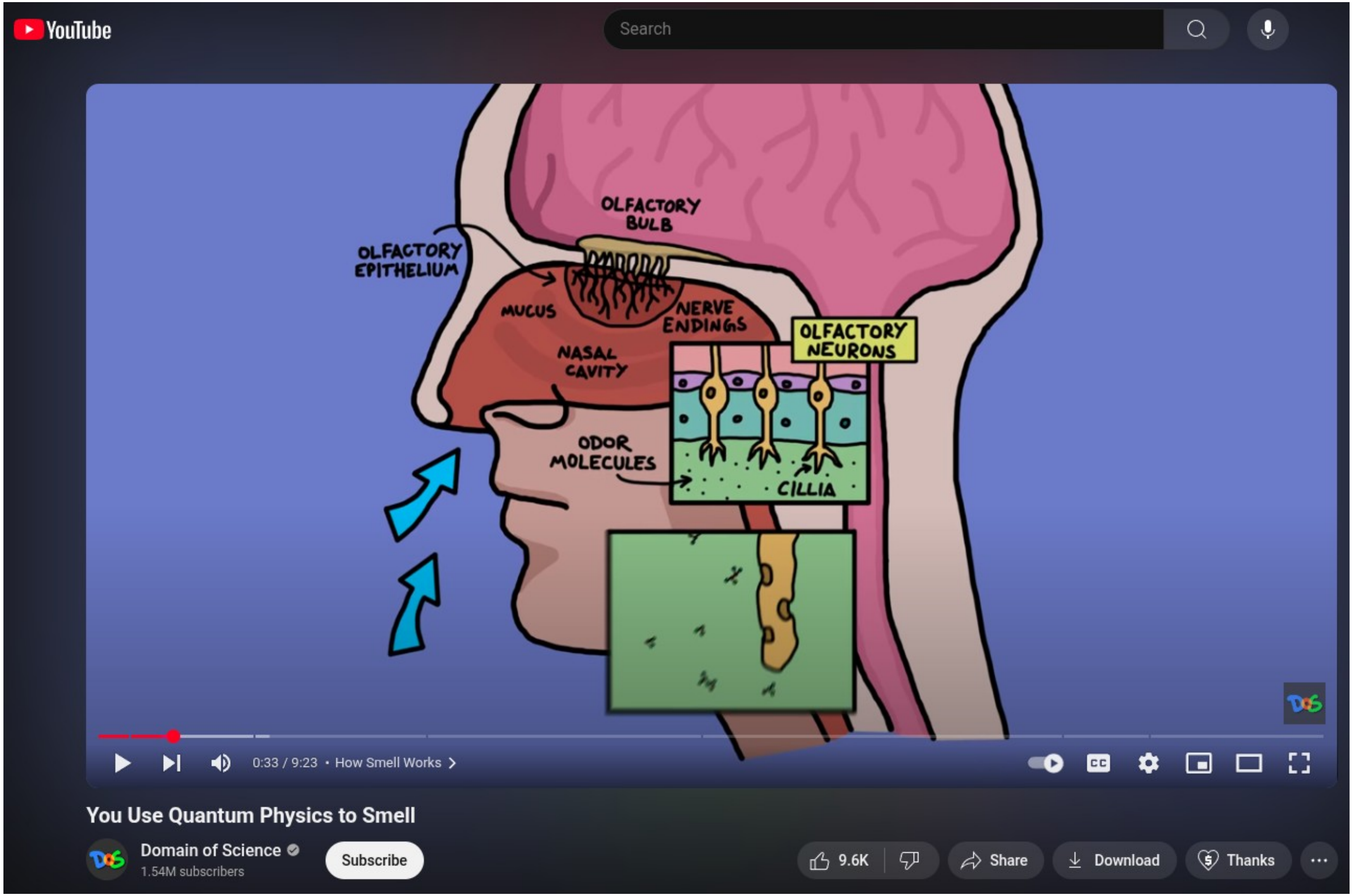
Why do we care?

- 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 (at least, last I checked) not "future proofed" against quantum computers
  - Signal is, but only since 2023, and not against mitm



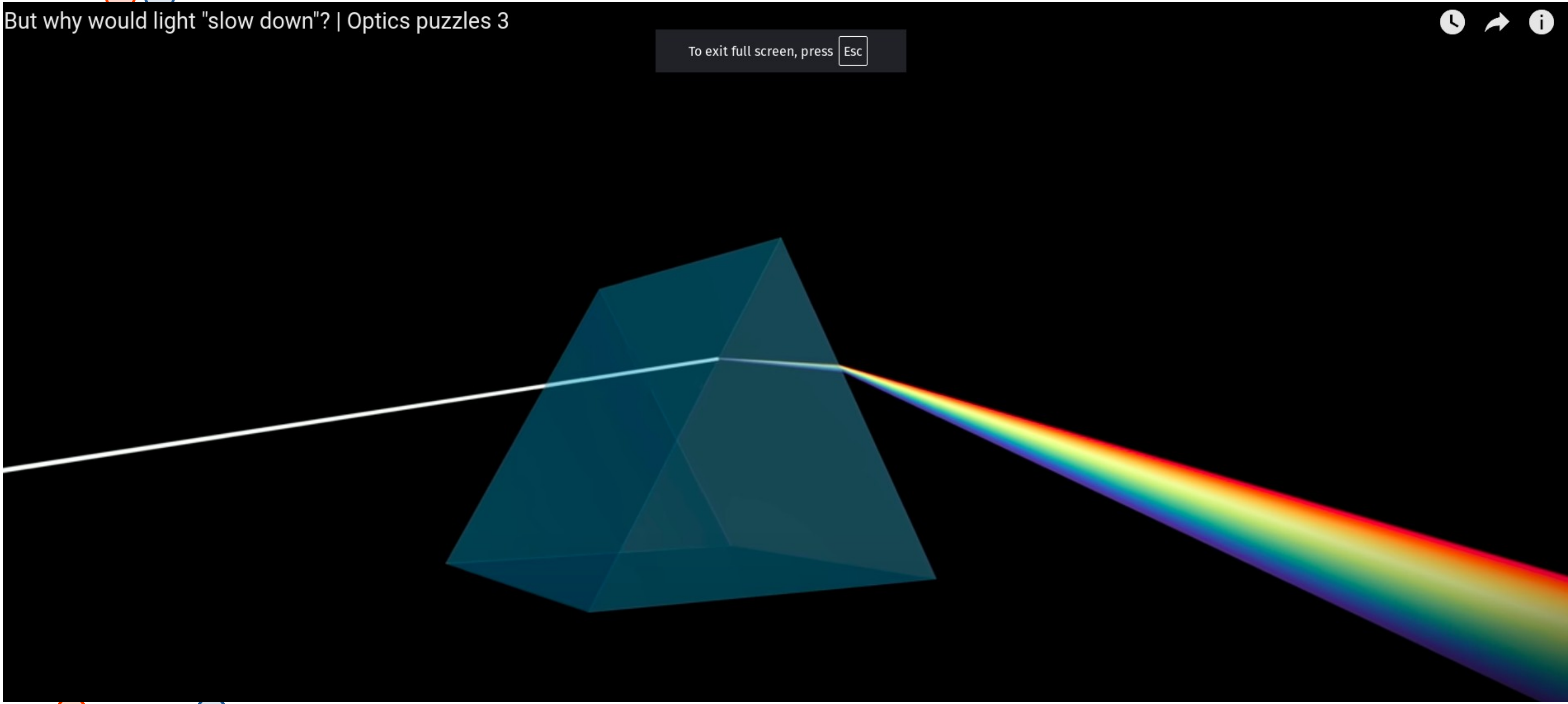
Quantum computation is all around you...

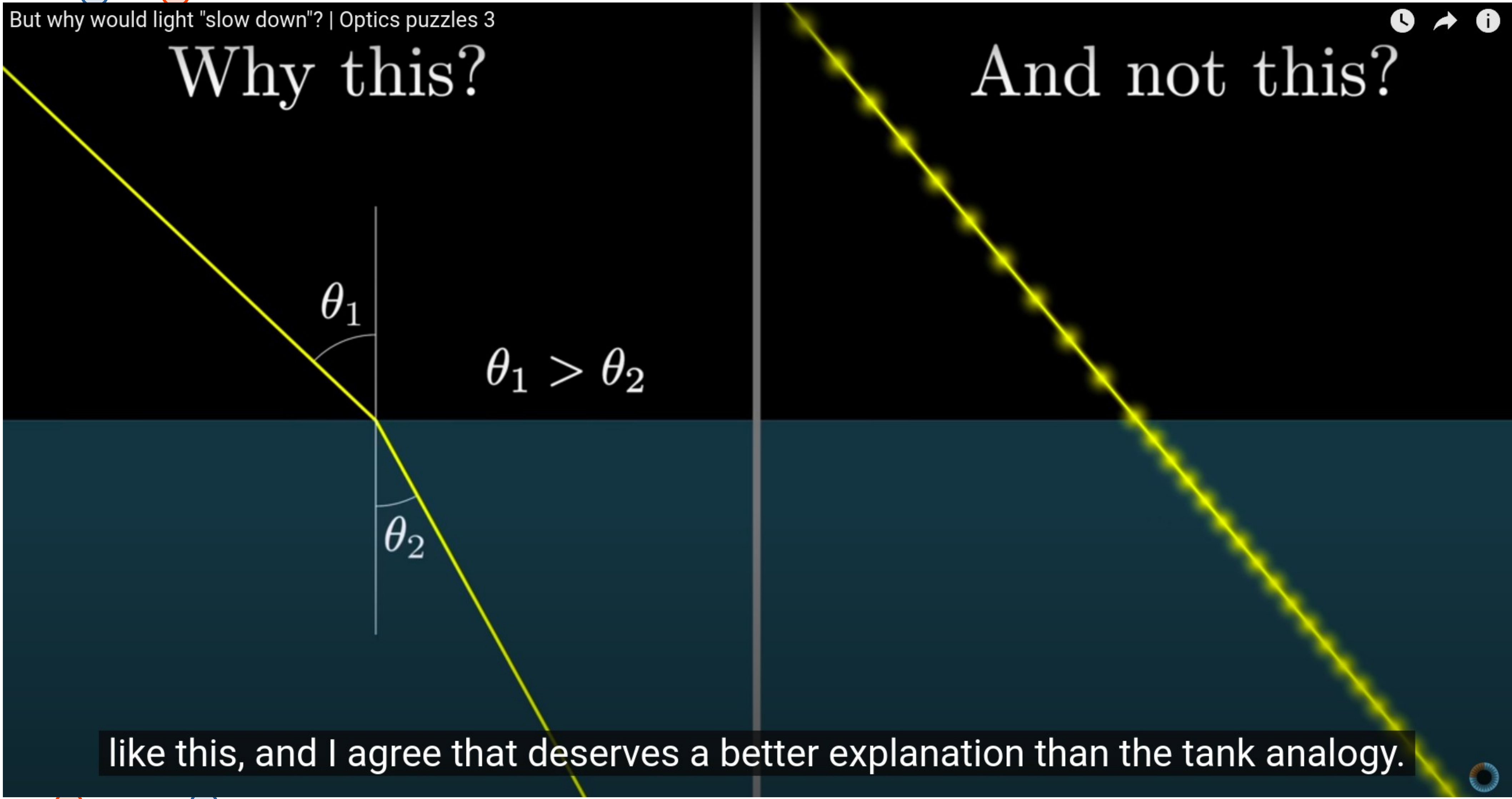
https://www.youtube.com/watch?v=DJsJIVXkrGQ

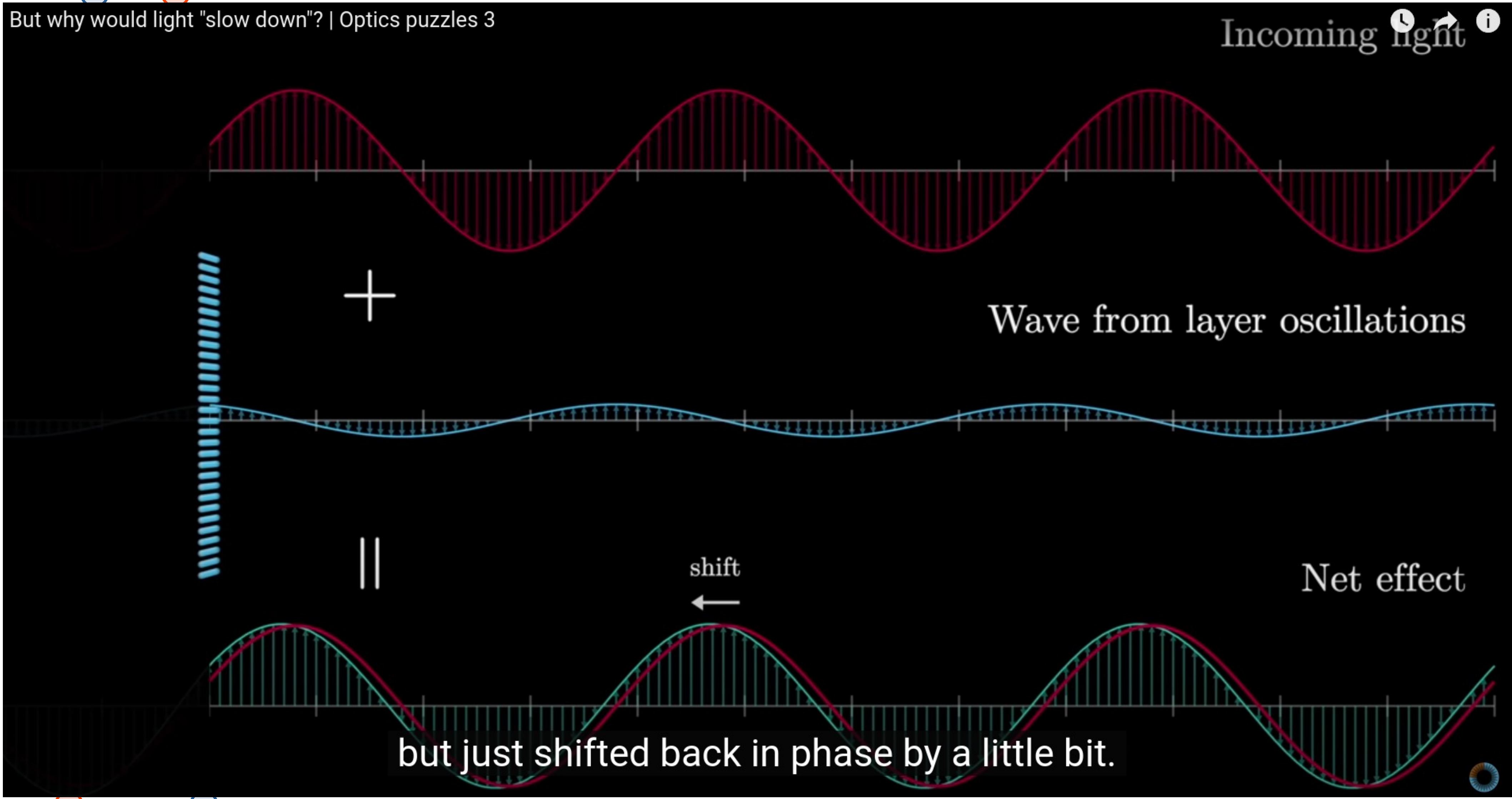


https://en.wikipedia.org/wiki/Sunstone_%28medieval%29

3brown1blue on YouTube...




But why would light "slow down"? | Optics puzzles 3
Why this?
And not this?
θ_1
$\theta_1 > \theta_2$
θ_2
like this, and I agree that deserves a better explanation than the tank analogy.



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

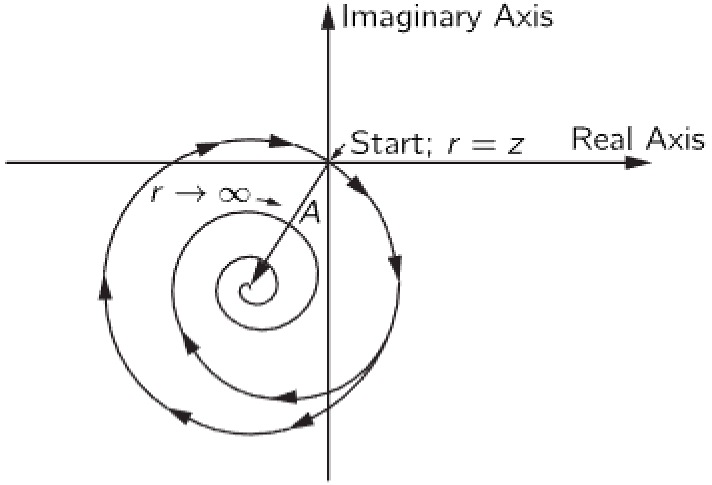
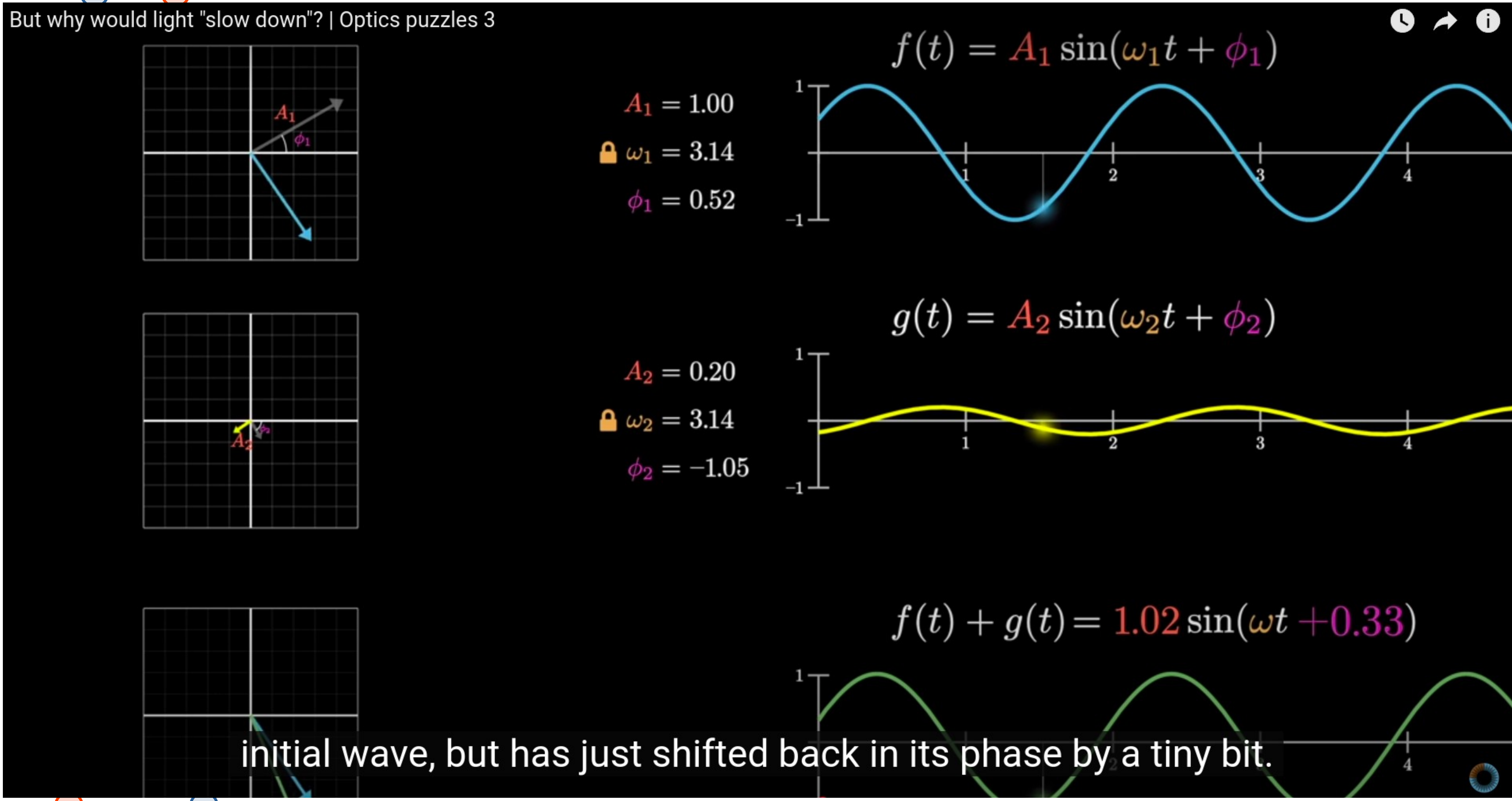


Fig. 30–12. Graphical solution of $\int_z^\infty \eta e^{-i\omega r/c}\,dr$.

Called an Euler spiral, or Cornu spiral.

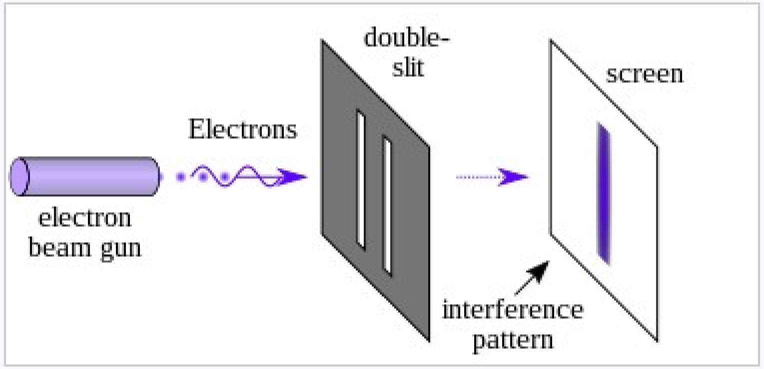

But why would light "slow down"? | Optics puzzles 3
$f(t) = A_1 \sin(\omega_1 t + \phi_1)$
$A_1 = 1.00$
$\omega_1 = 3.14$
$\phi_1 = 0.52$
$g(t) = A_2 \sin(\omega_2 t + \phi_2)$
$A_2 = 0.20$
$\omega_2 = 3.14$
$\phi_2 = -1.05$
$f(t) + g(t) = 1.02 \sin(\omega t + 0.33)$
initial wave, but has just shifted back in its phase by a tiny bit.

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

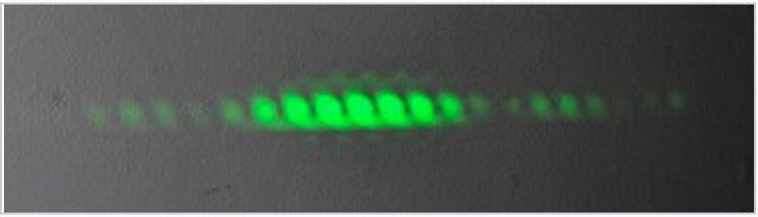
https://www.youtube.com/watch?v=v-1zjdUTu0o

Photoelectric effect

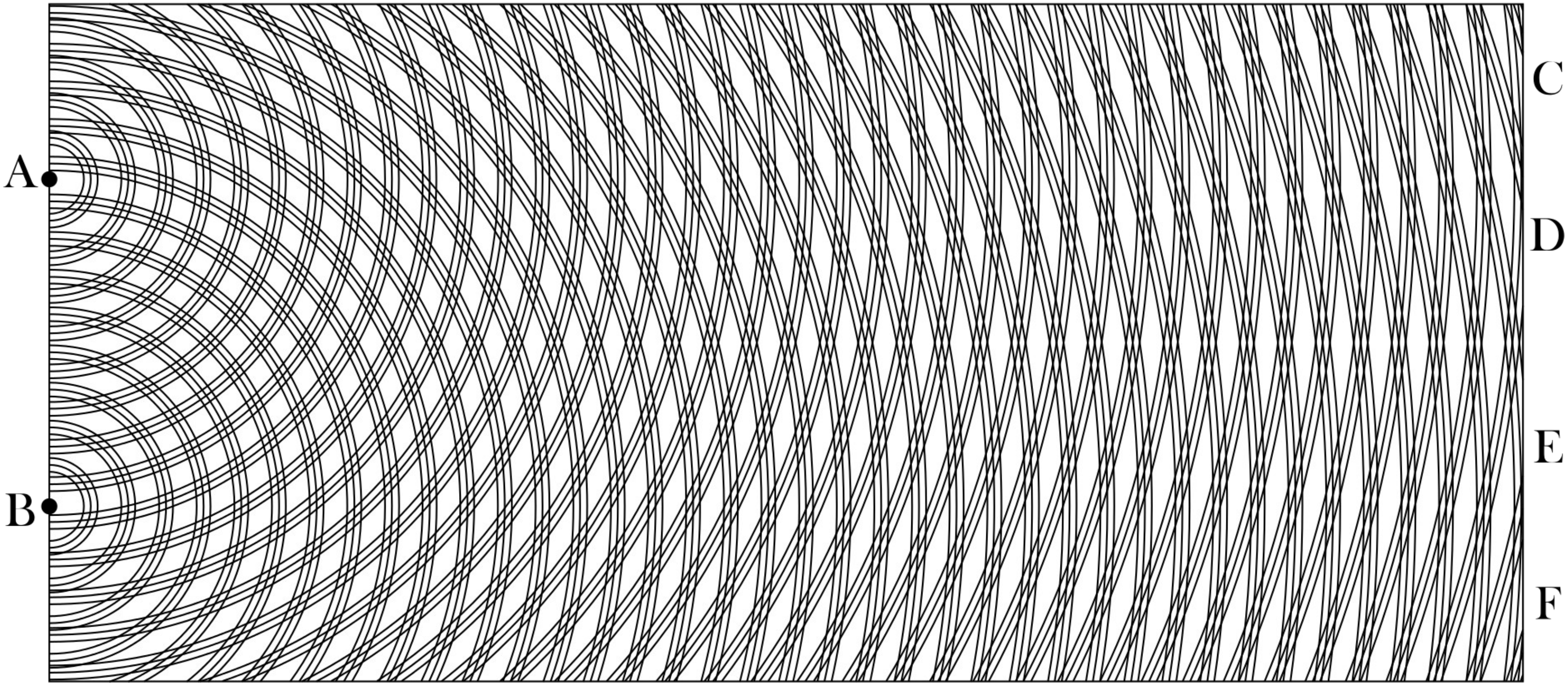
https://en.wikipedia.org/wiki/Double-slit_experiment

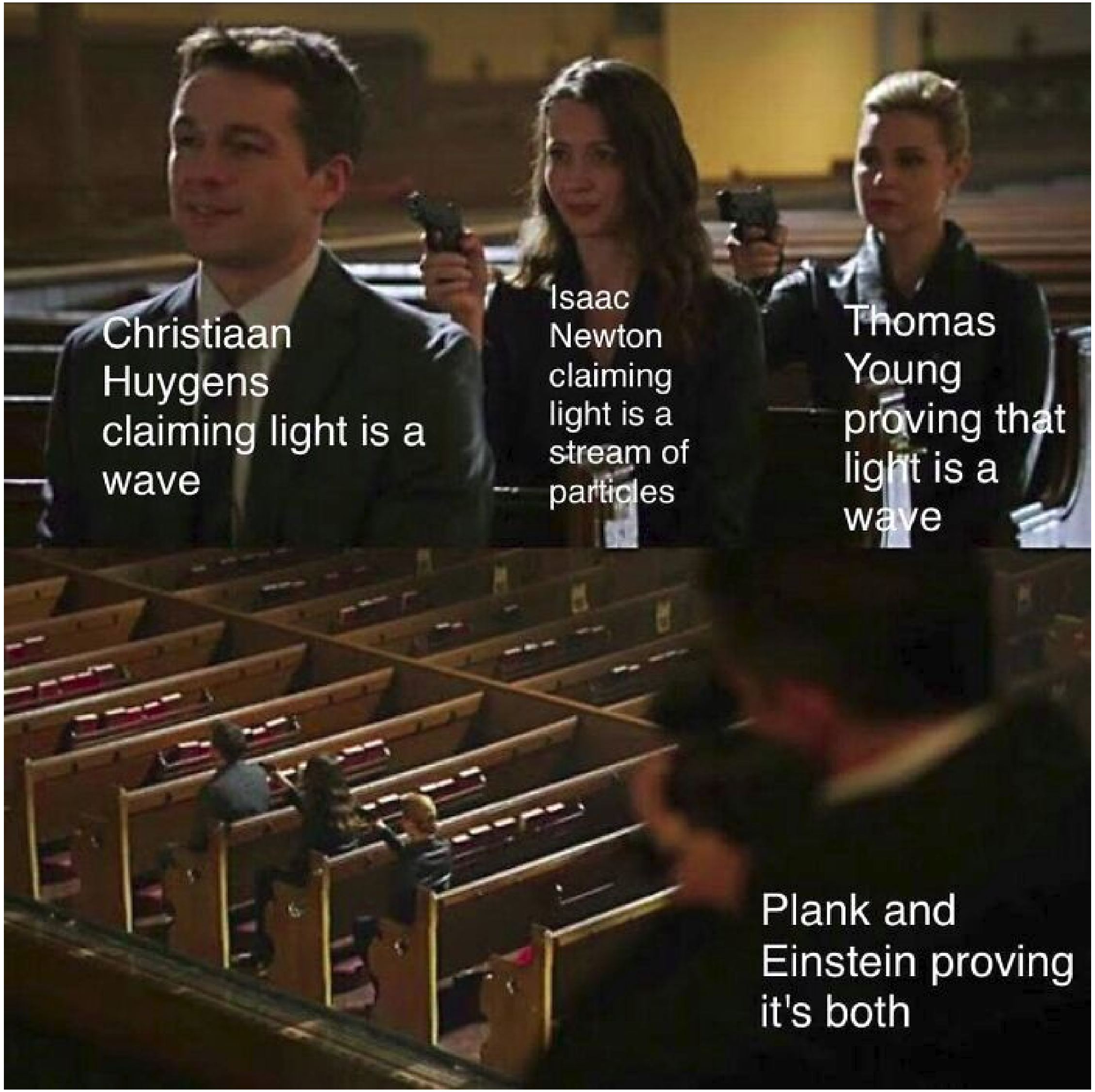


Photons or matter (like electrons) produce an interference pattern when two slits are used



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



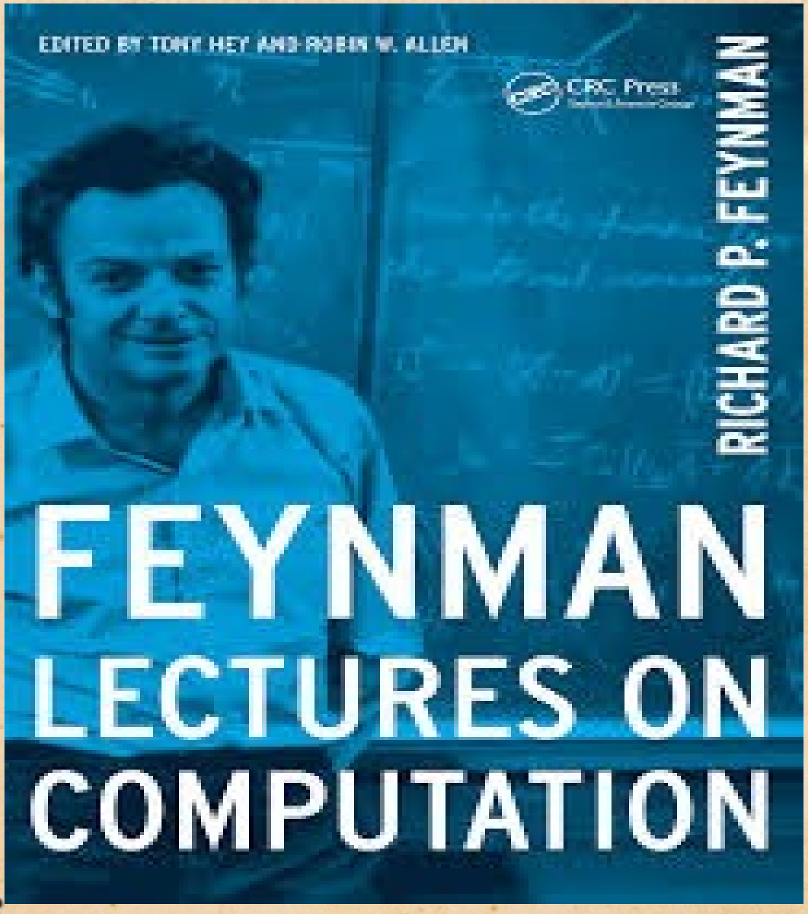

Christiaan Huygens claiming light is a wave
Isaac Newton claiming light is a stream of particles
Thomas Young proving that light is a wave
Plank and Einstein proving it's both

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*."

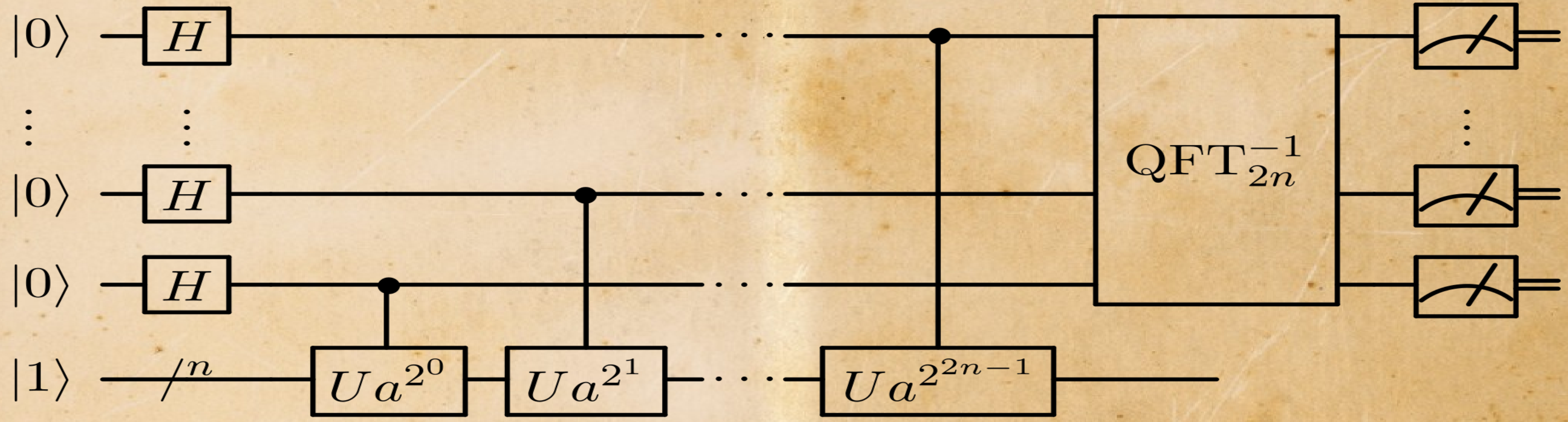
https://www.feynmanlectures.caltech.edu/III_01.html



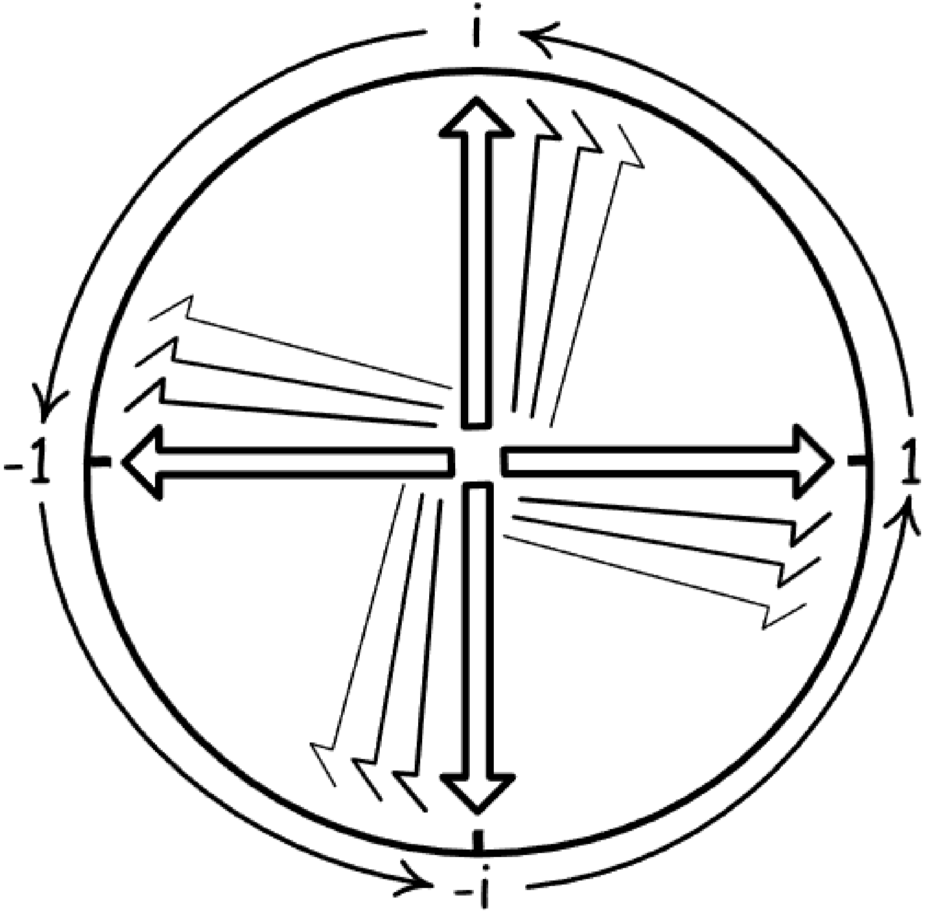
Lectures given 1983 through 1986...

“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

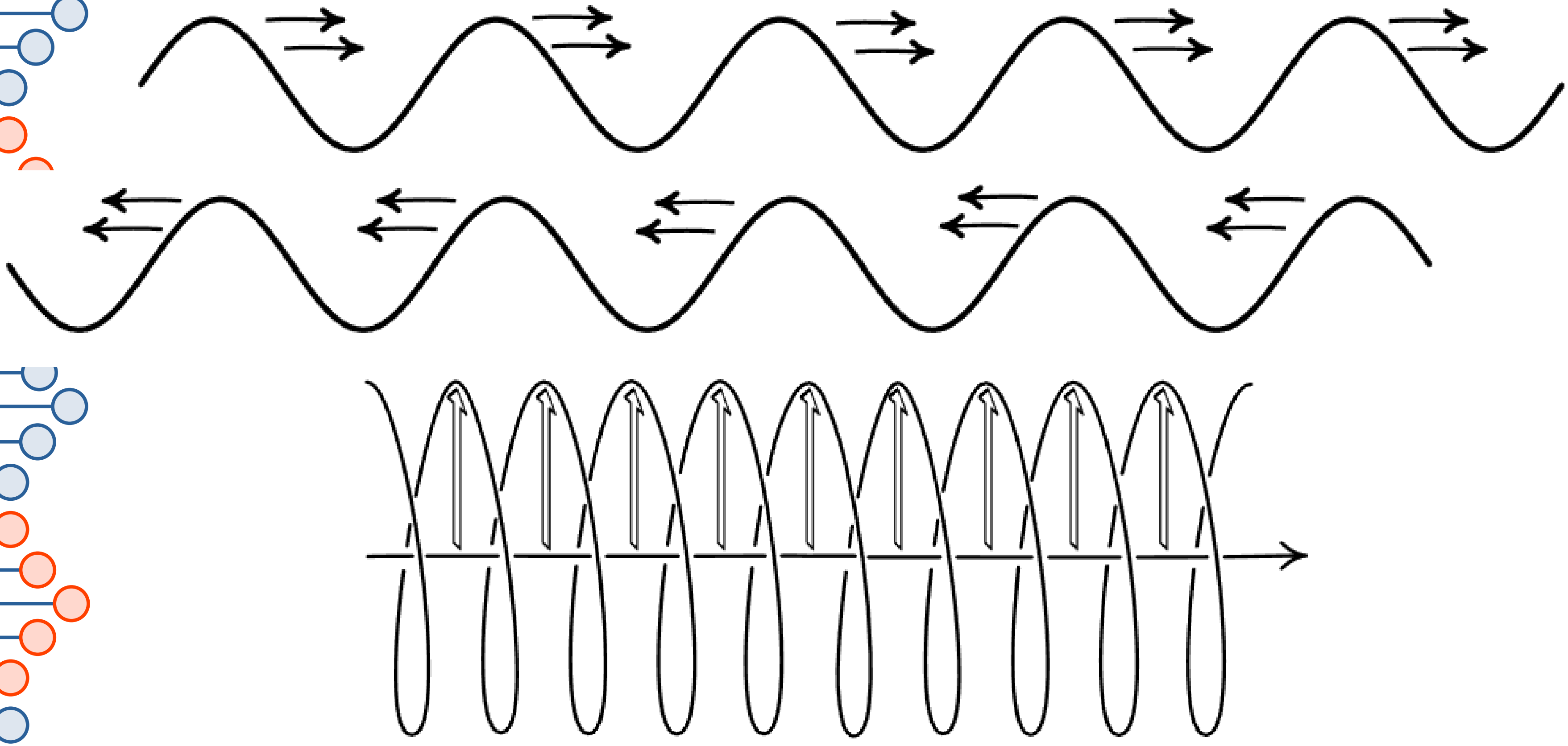


Complex waves are different...



https://sites.pitt.edu/~jdnorton/teaching/HPS_0410/chapters/quantum_theory_complex/complex.html

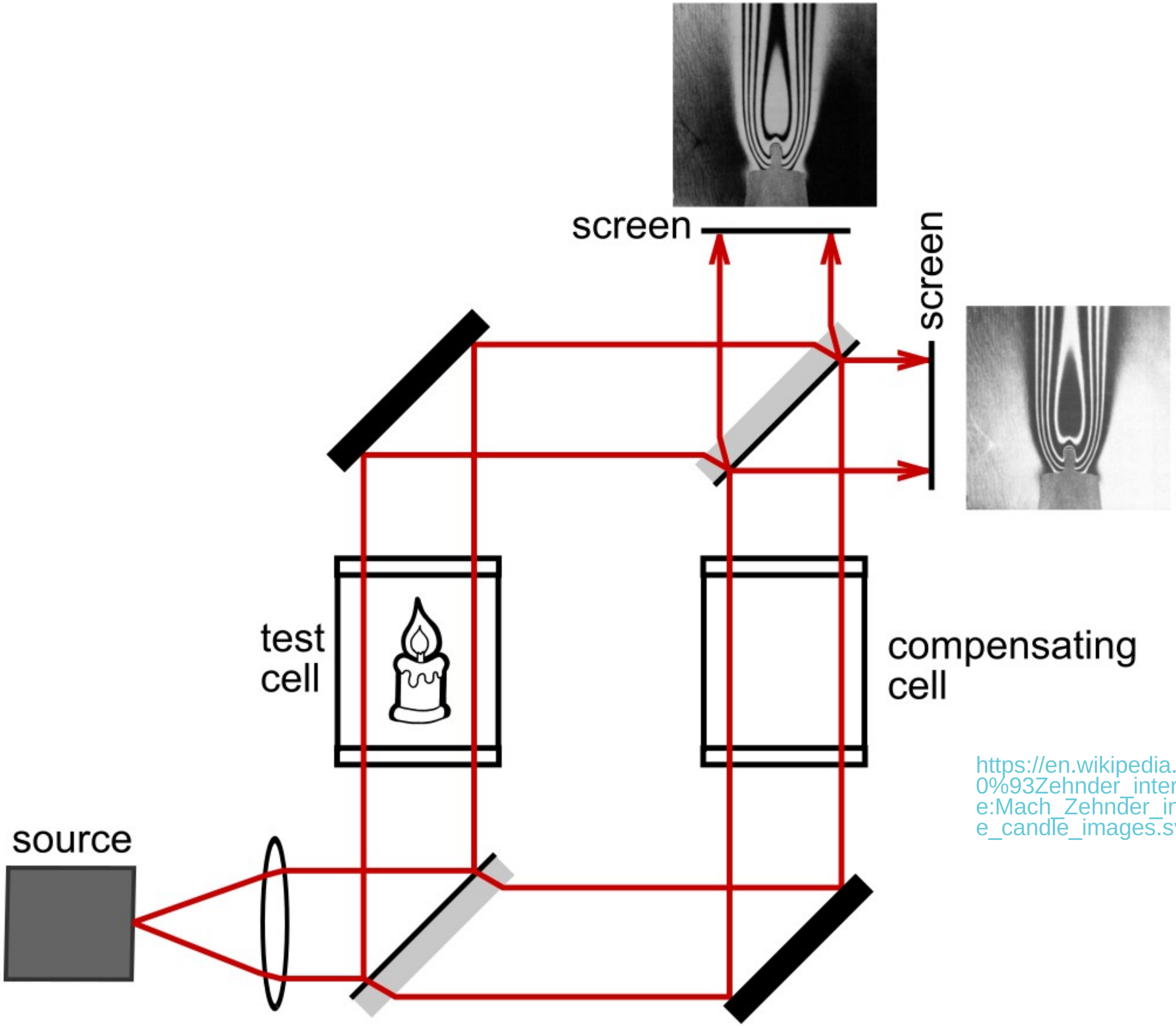
Complex waves have direction...



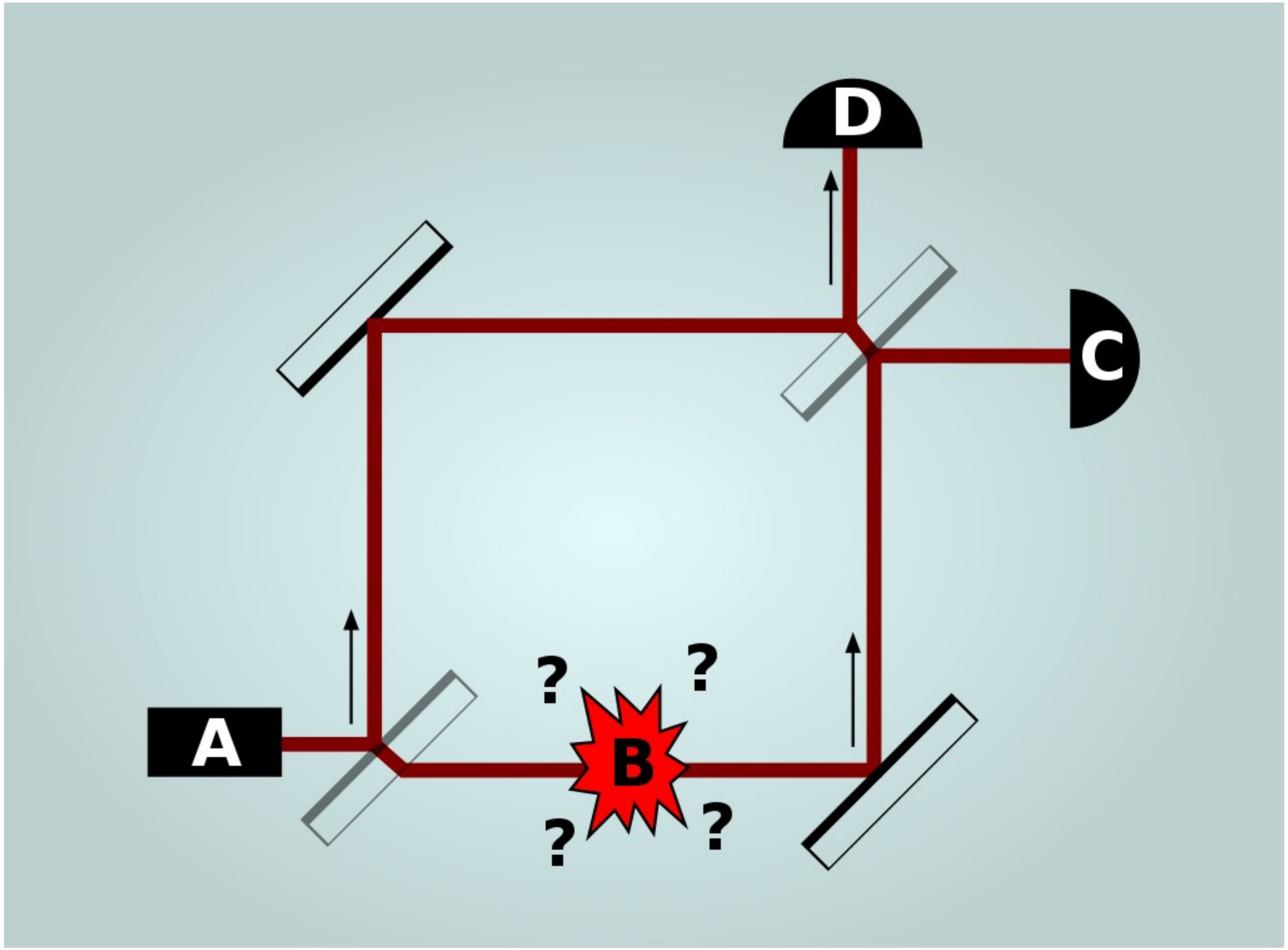
https://sites.pitt.edu/~jdnorton/teaching/HPS_0410/chapters/quantum_theory_complex/complex.html

$$\int e^{i\theta}\, d\theta = -i\, e^{i\theta} + \text{constant}$$

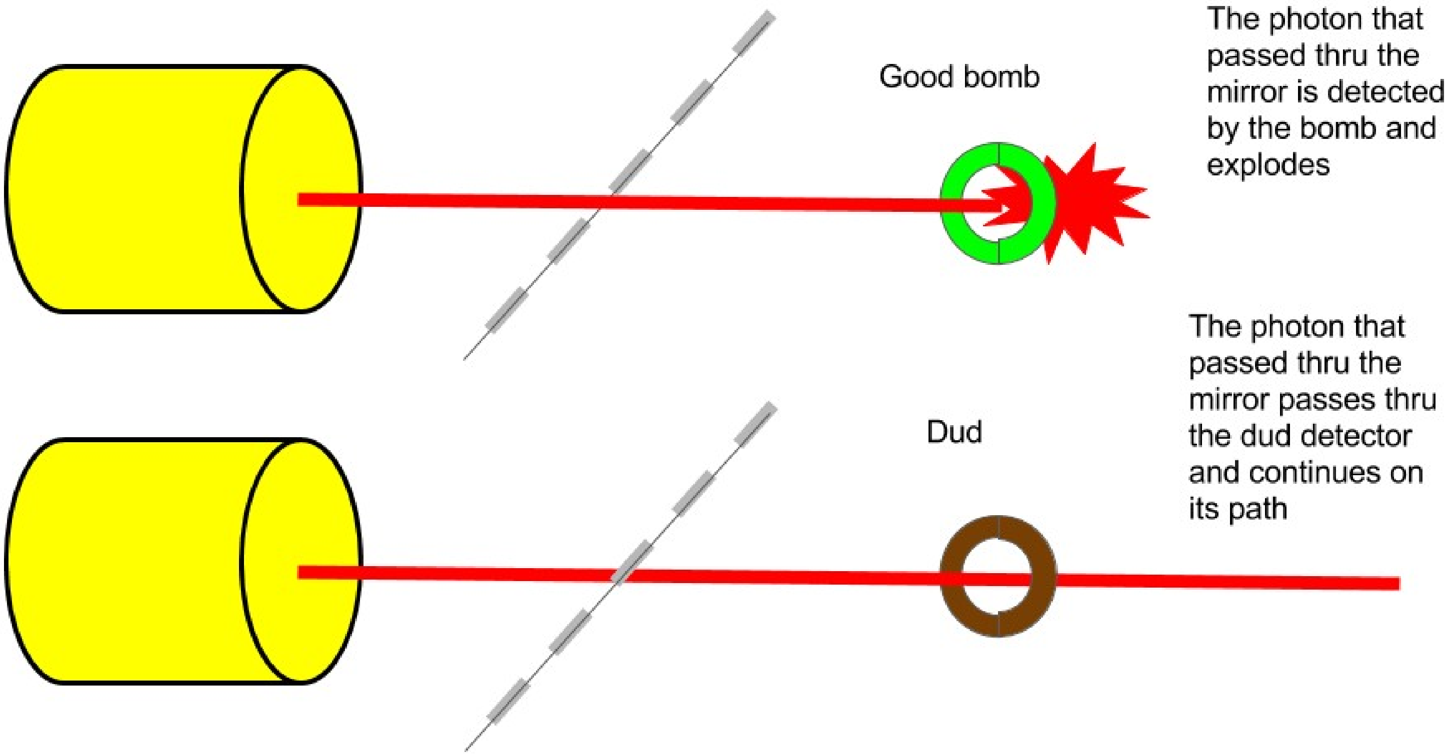
$$\frac{d}{d\theta}\left(e^{i\theta}\right) = i\, e^{i\theta}$$



https://en.wikipedia.org/wiki/Mach%E2%80%93Zehnder_interferometer#/media/File:Mach_Zehnder_interferometer_alternate_candle_images.svg https://en.wikipedia.org/wiki/Elitzur%E2%80%93Vaidman_bomb_tester

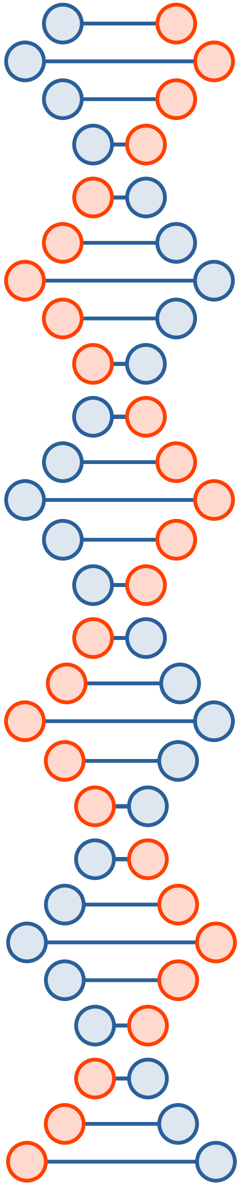


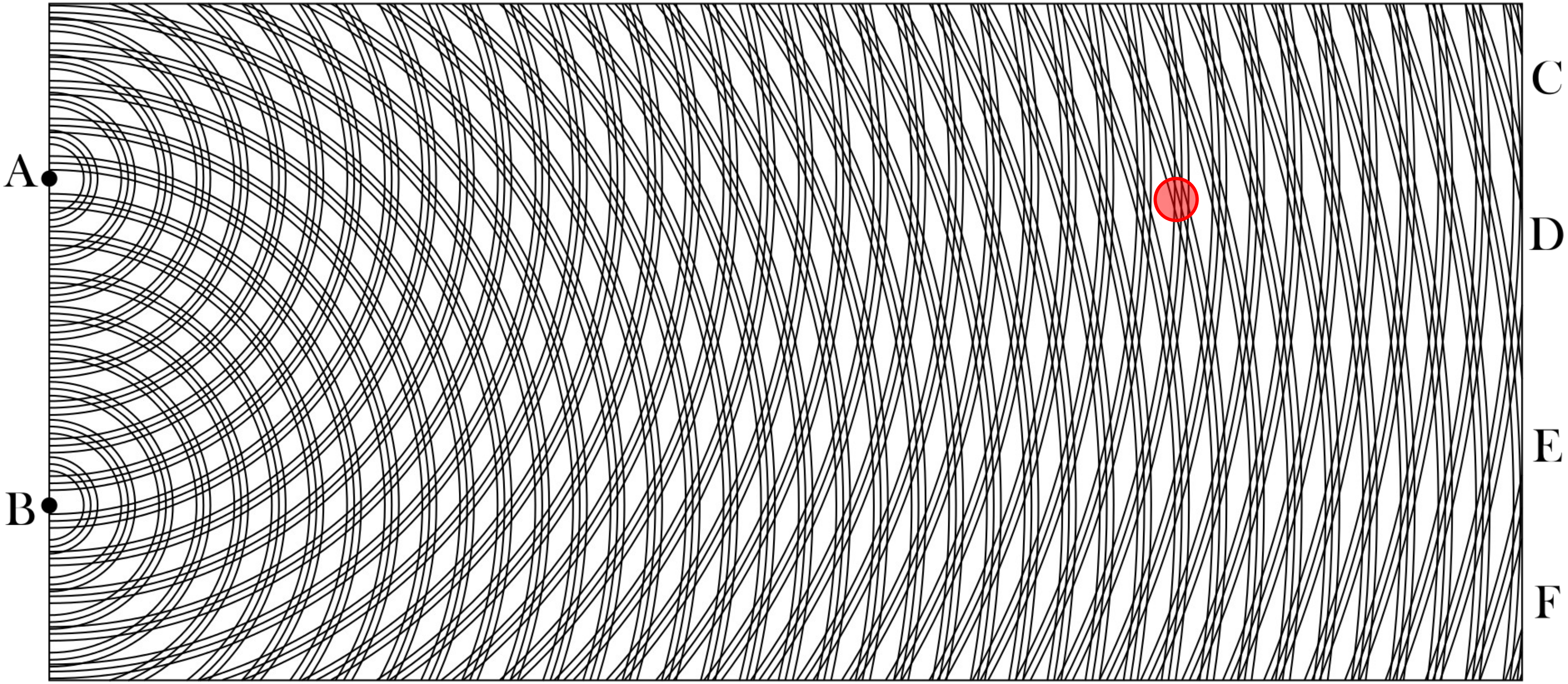
Bomb is either live or a dud



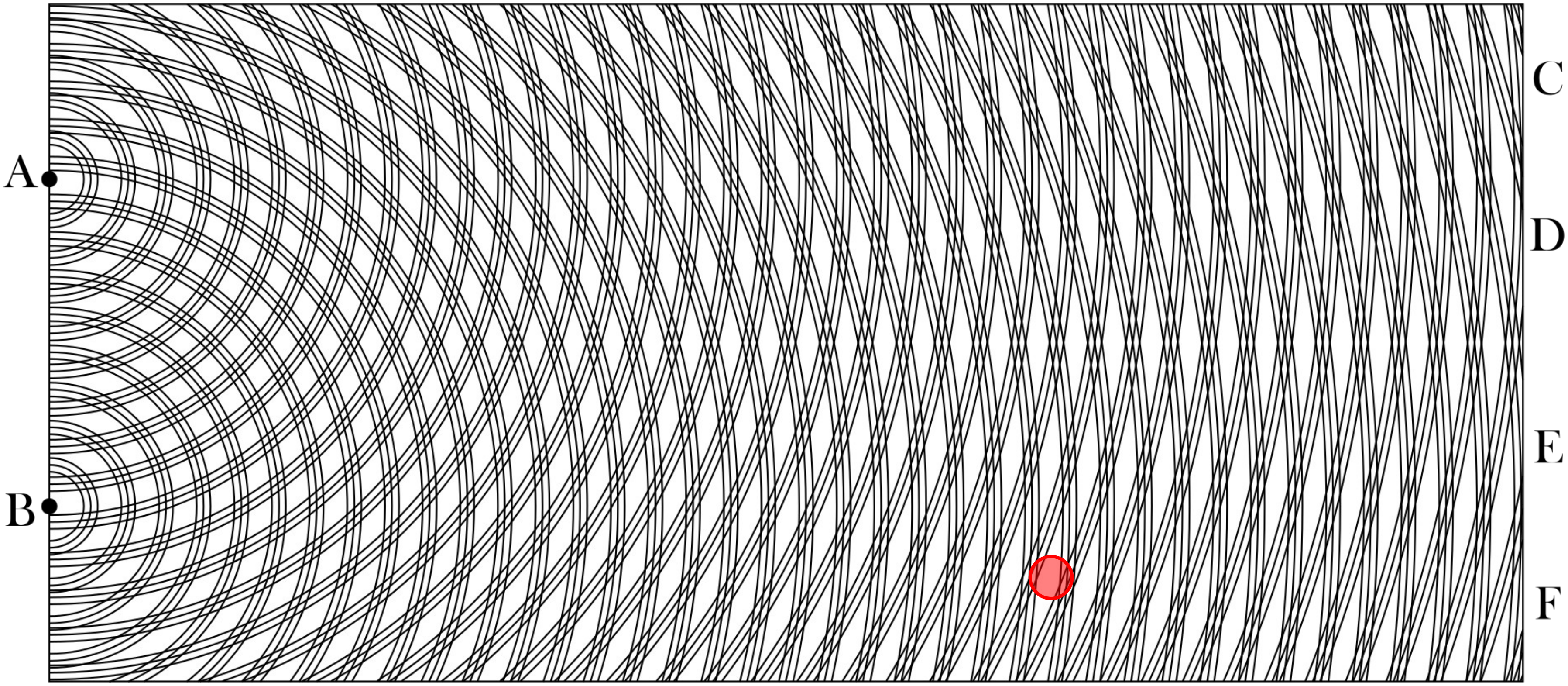
"Due to the way in which the interferometer is constructed, a photon going through the second mirror from the lower path towards detector D will have a phase shift of half a wavelength compared to a photon being reflected from the upper path towards that same detector..."

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

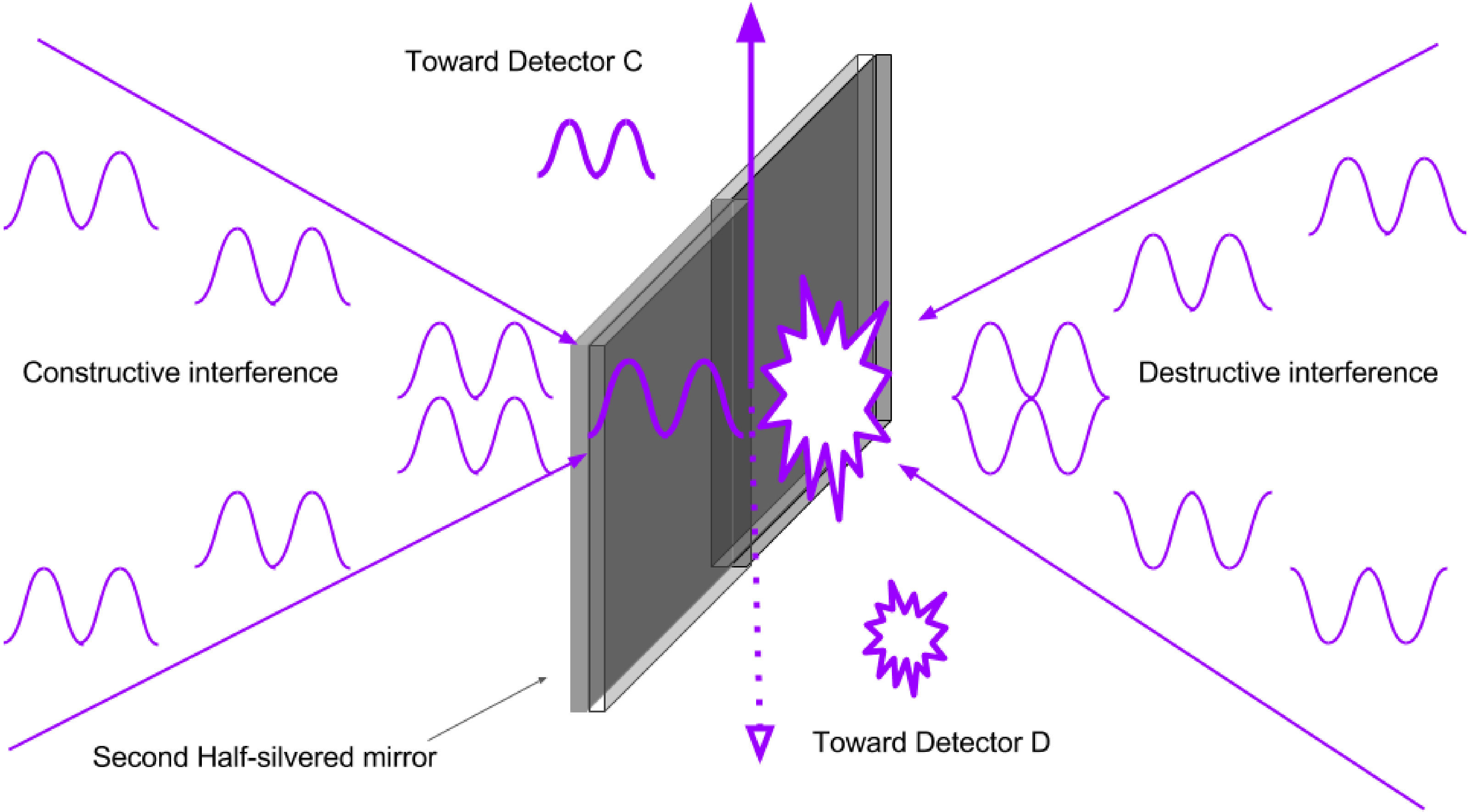




Put D, *e.g.*, here...



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



Balanced → destructive interference

Unbalanced → constructive interference

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*.
  - Think "bomb parity" of the two paths
- 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

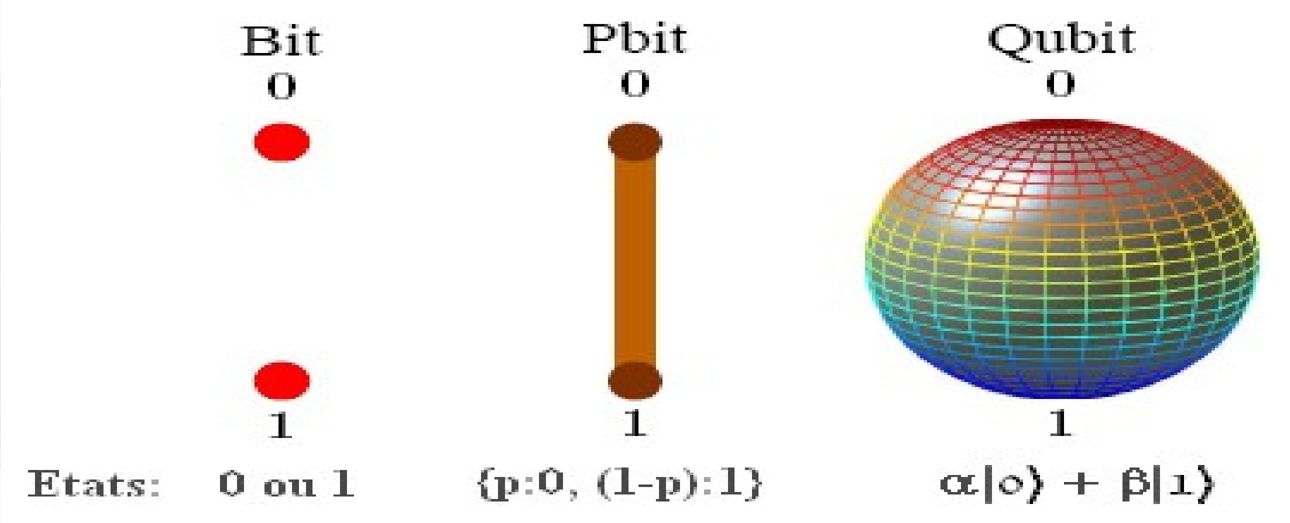
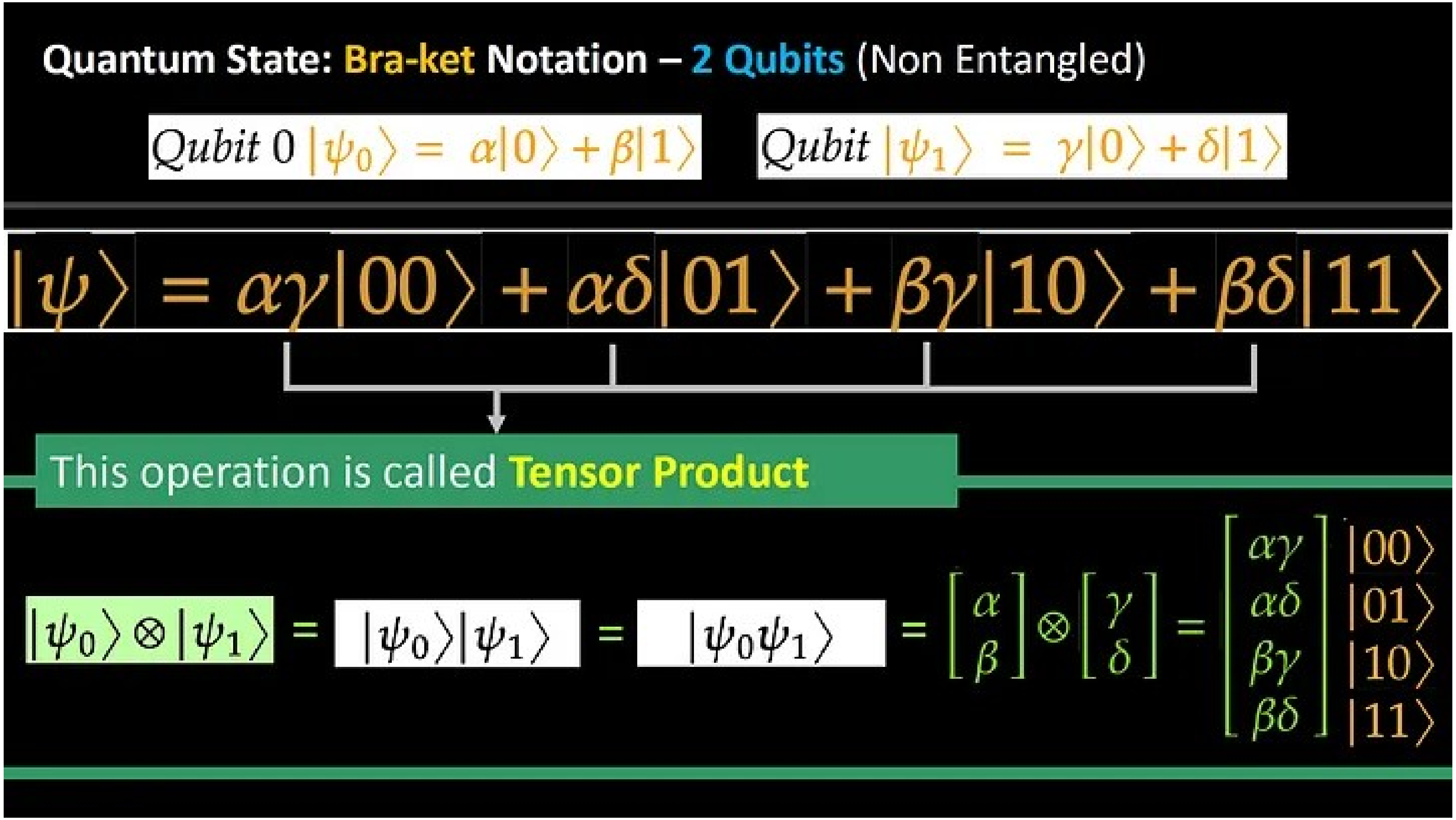


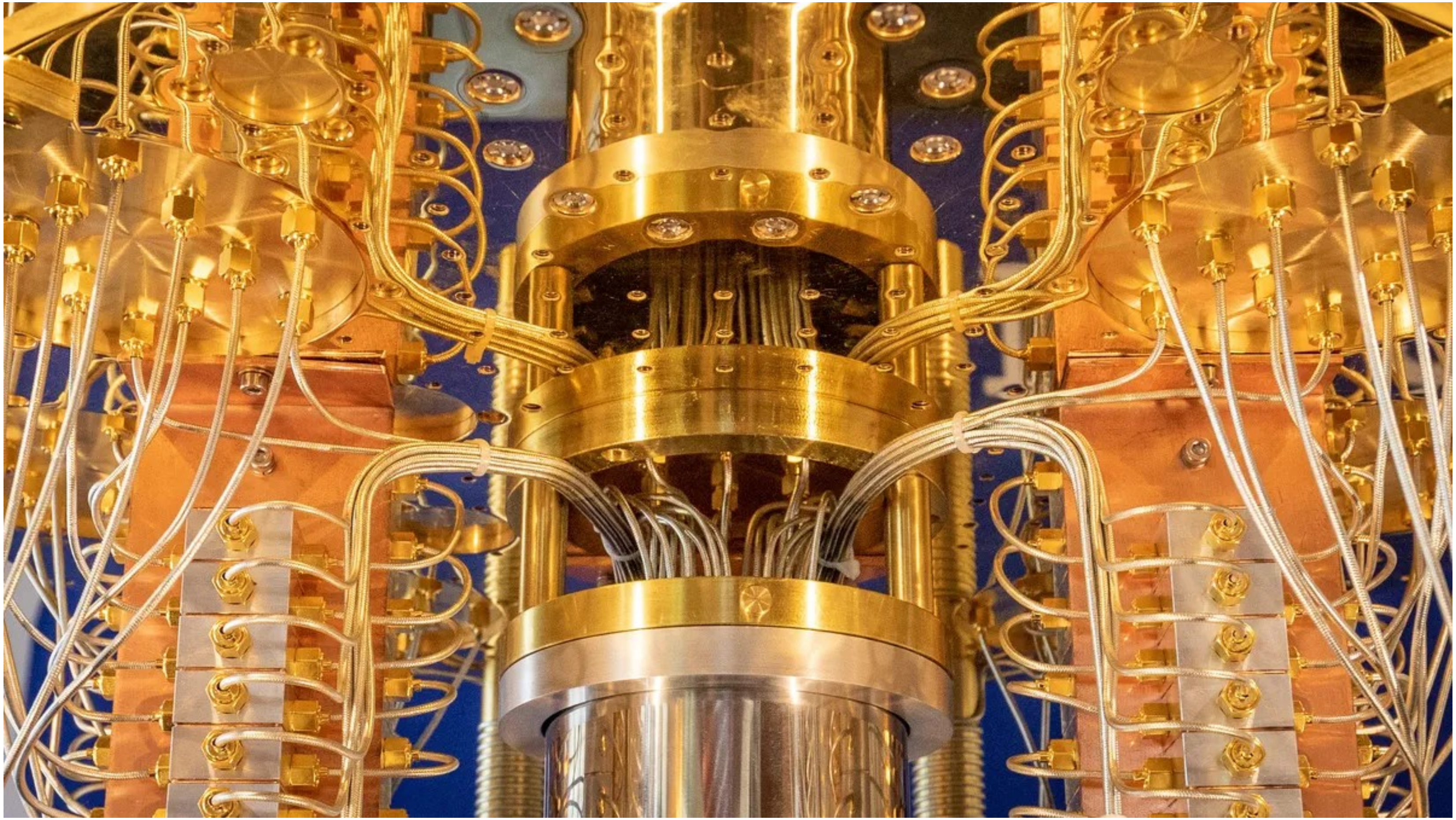
Image taken from http://filipchsqroom.blogspot.com/

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



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

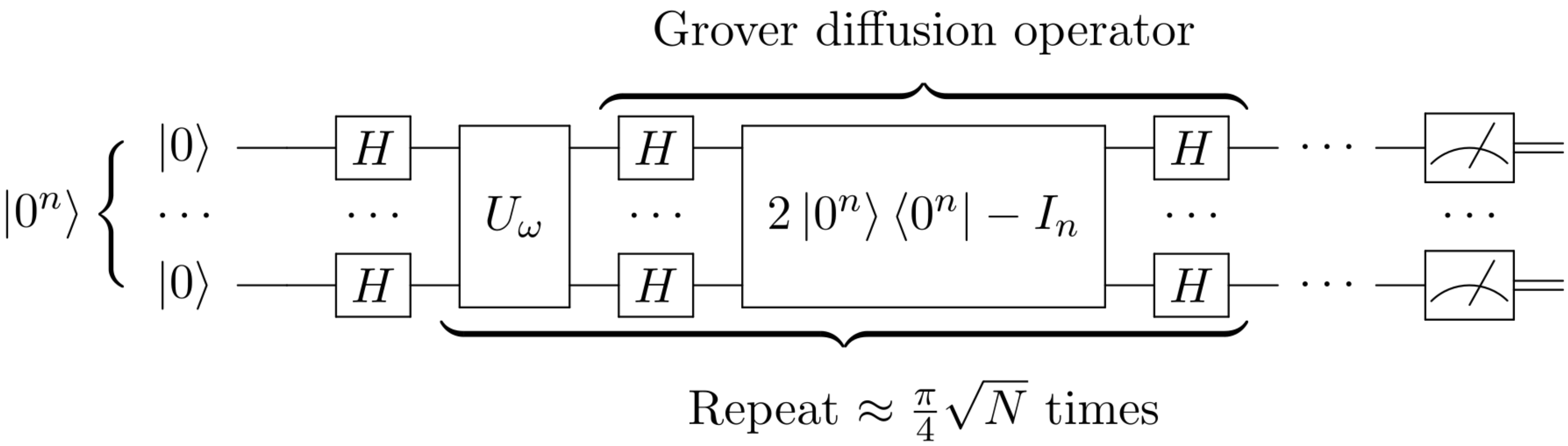


https://www.cnet.com/tech/computing/quantum-computer-makers-like-their-odds-for-big-progress-soon/

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

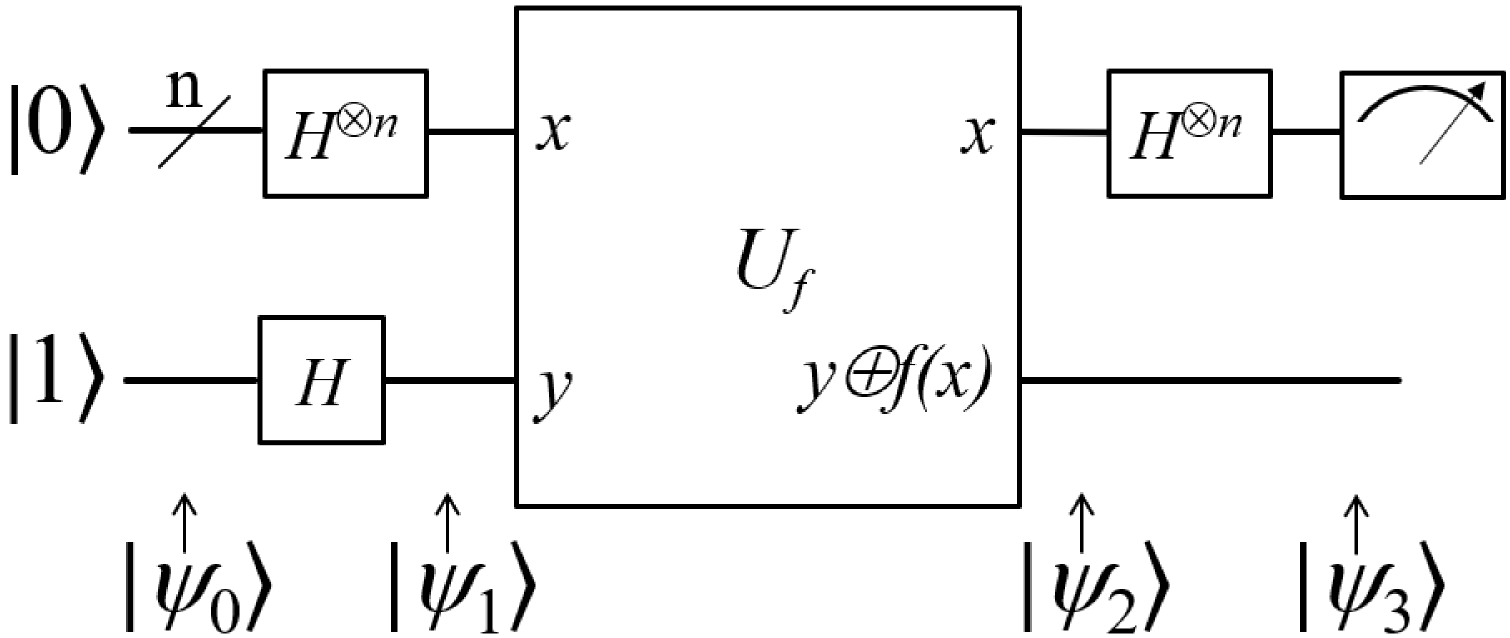
Symmetric crypto

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

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)
- 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

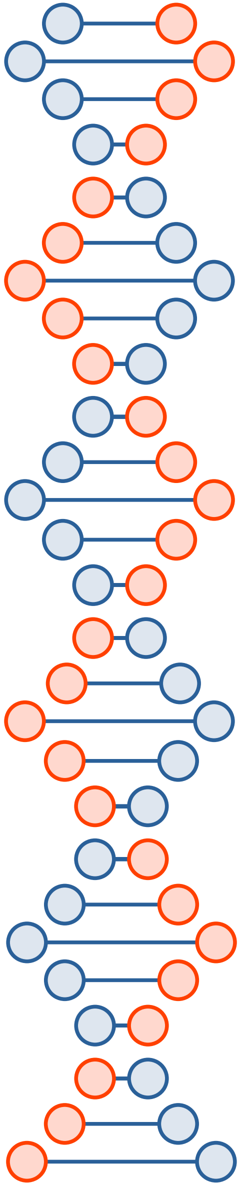
1-bit input case...

- p = Probability of measuring |0>

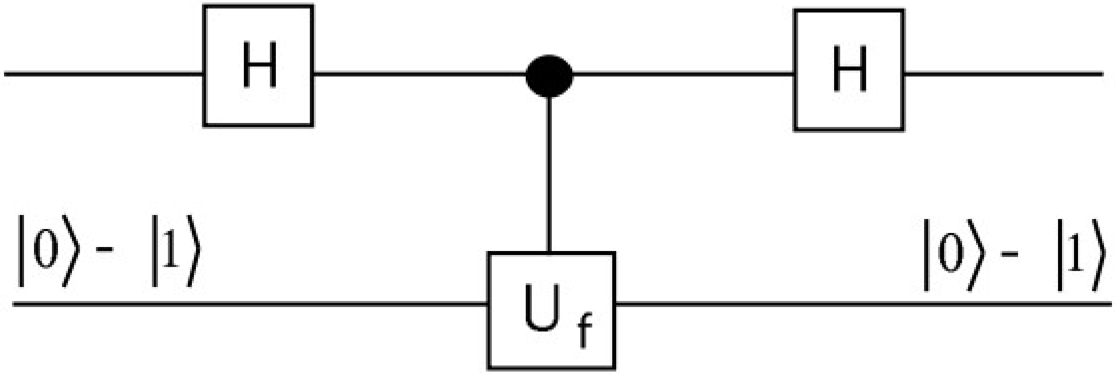
$$|(1/2)(-1)^{f(0)} + (1/2)(-1)^{f(1)}|$$

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

A balanced function cancels itself out because of destructive interference



Balanced → destructive interference
Unbalanced → constructive interference



$$|\,x\rangle\,|\,y\rangle \overset{f-c-N}{\longrightarrow} |\,x\rangle\,|\,y \oplus f(x)\rangle \;. \tag{2.1}$$

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

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

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

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

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 $|y \oplus f(x)\rangle$.

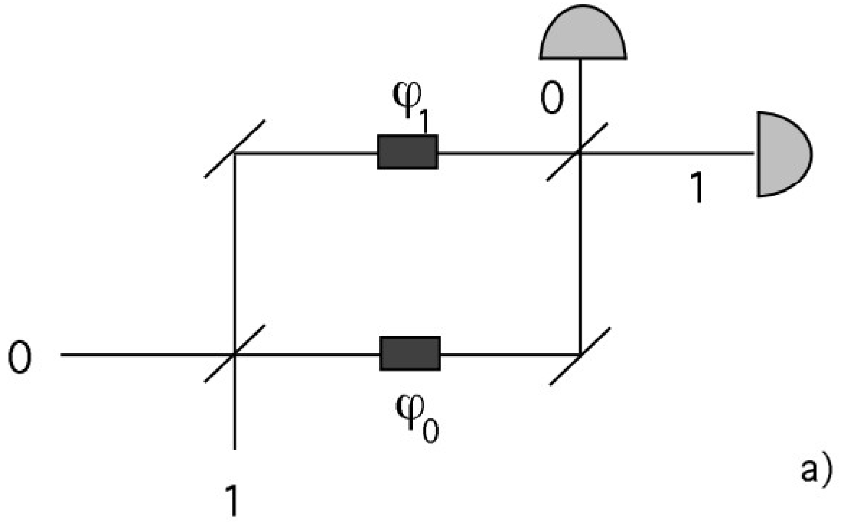
This state can also be written as

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

which, after applying the second Hadamard transform, becomes

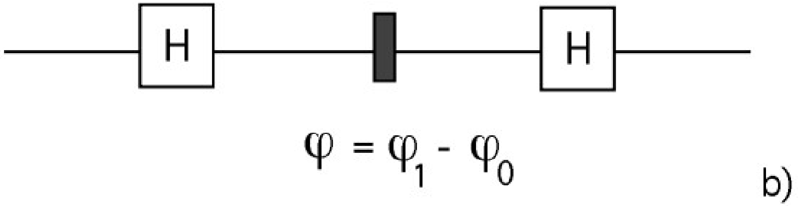
$$(-1)^{f(0)}|f(0) \oplus f(1)\rangle\,. \tag{2.5}$$

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

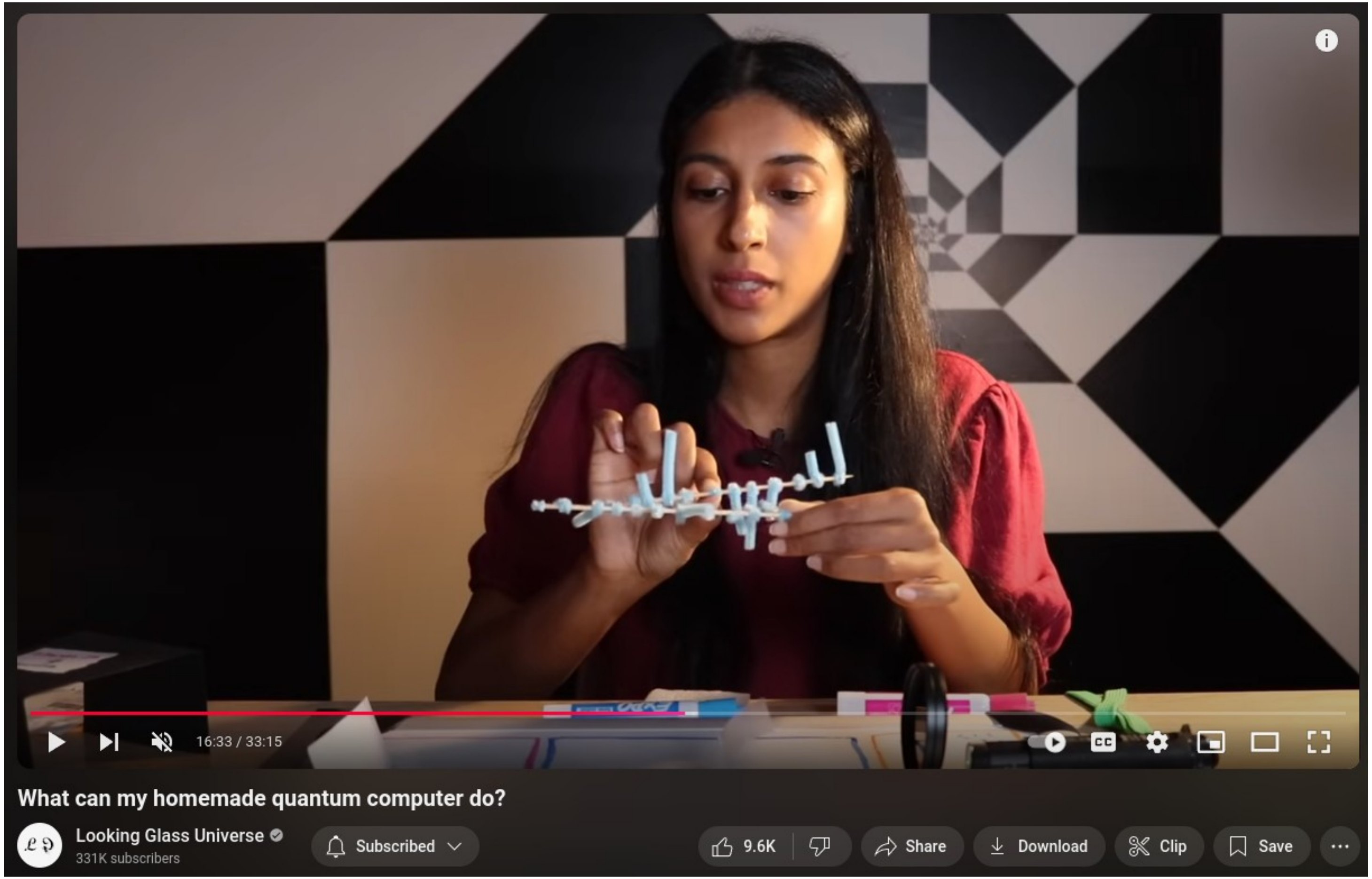


$$|0\rangle \xrightarrow{H} \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$$

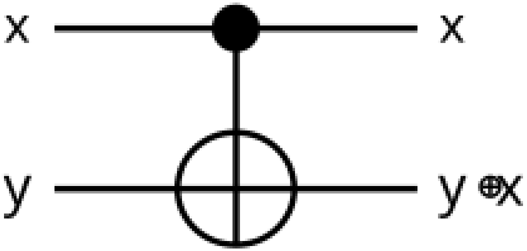
$$|1\rangle \xrightarrow{H} \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

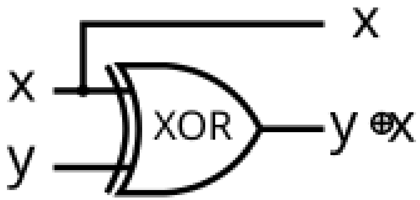


https://www.youtube.com/watch?v=tHfGucHtLqo



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}	$\frac{1}{2}(\|00\rangle - \|01\rangle - \|11\rangle + \|10\rangle)$	$\|+-\rangle$

https://en.wikipedia.org/wiki/File:Quantum_Logic_Gates.png

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

https://en.m.wikipedia.org/wiki/Hadamard_transform

$$H_0 = +(1)$$

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

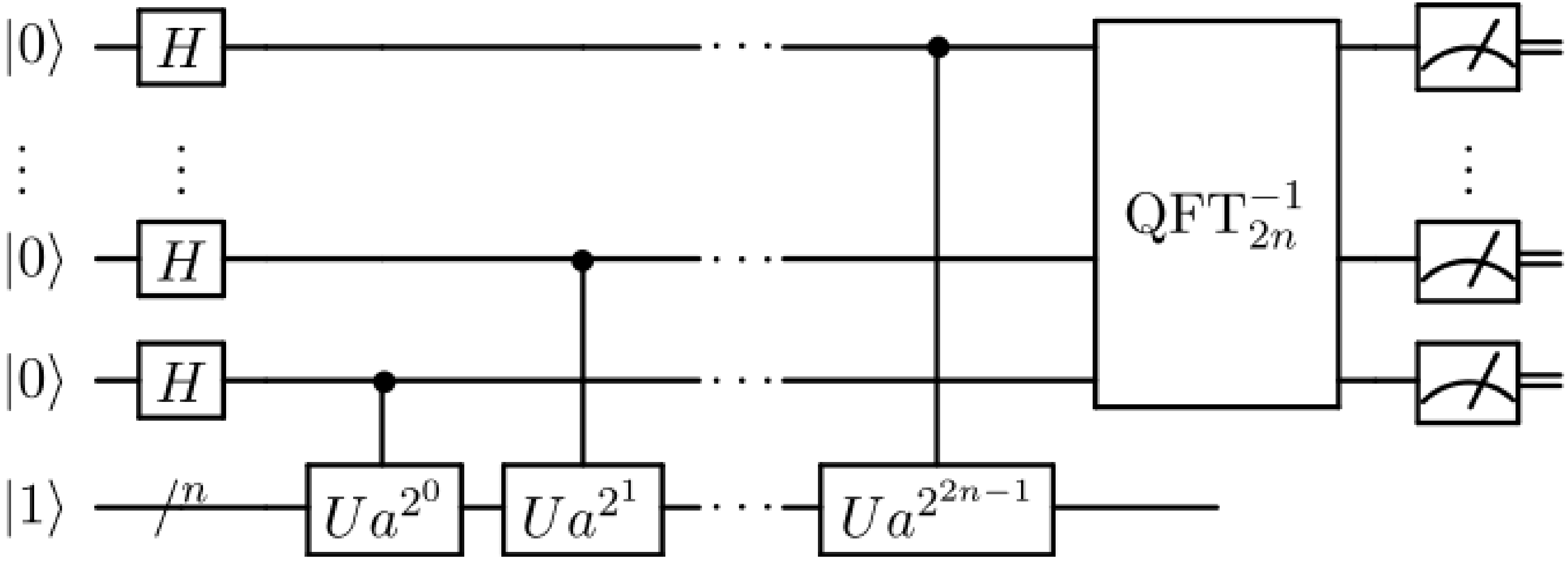
$$H_2 = \frac{1}{2} \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{pmatrix}$$

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

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

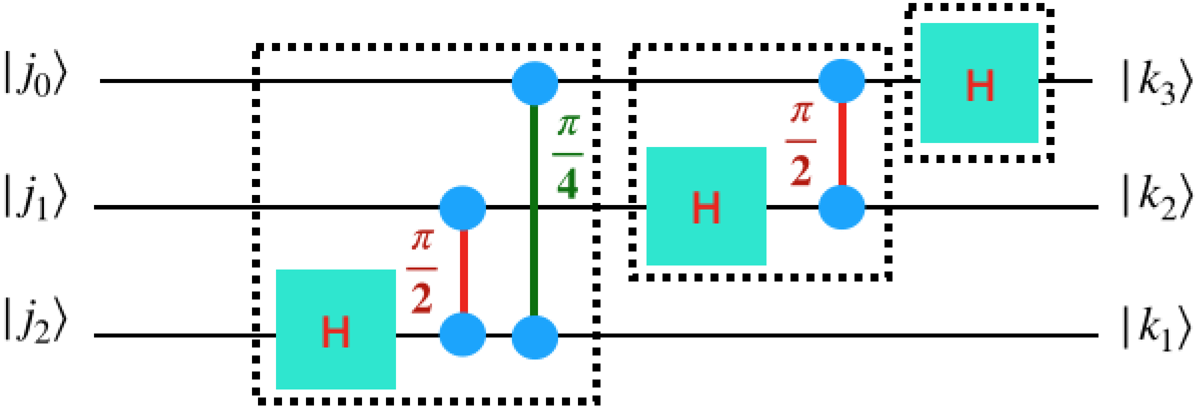
Shor’s algorithm



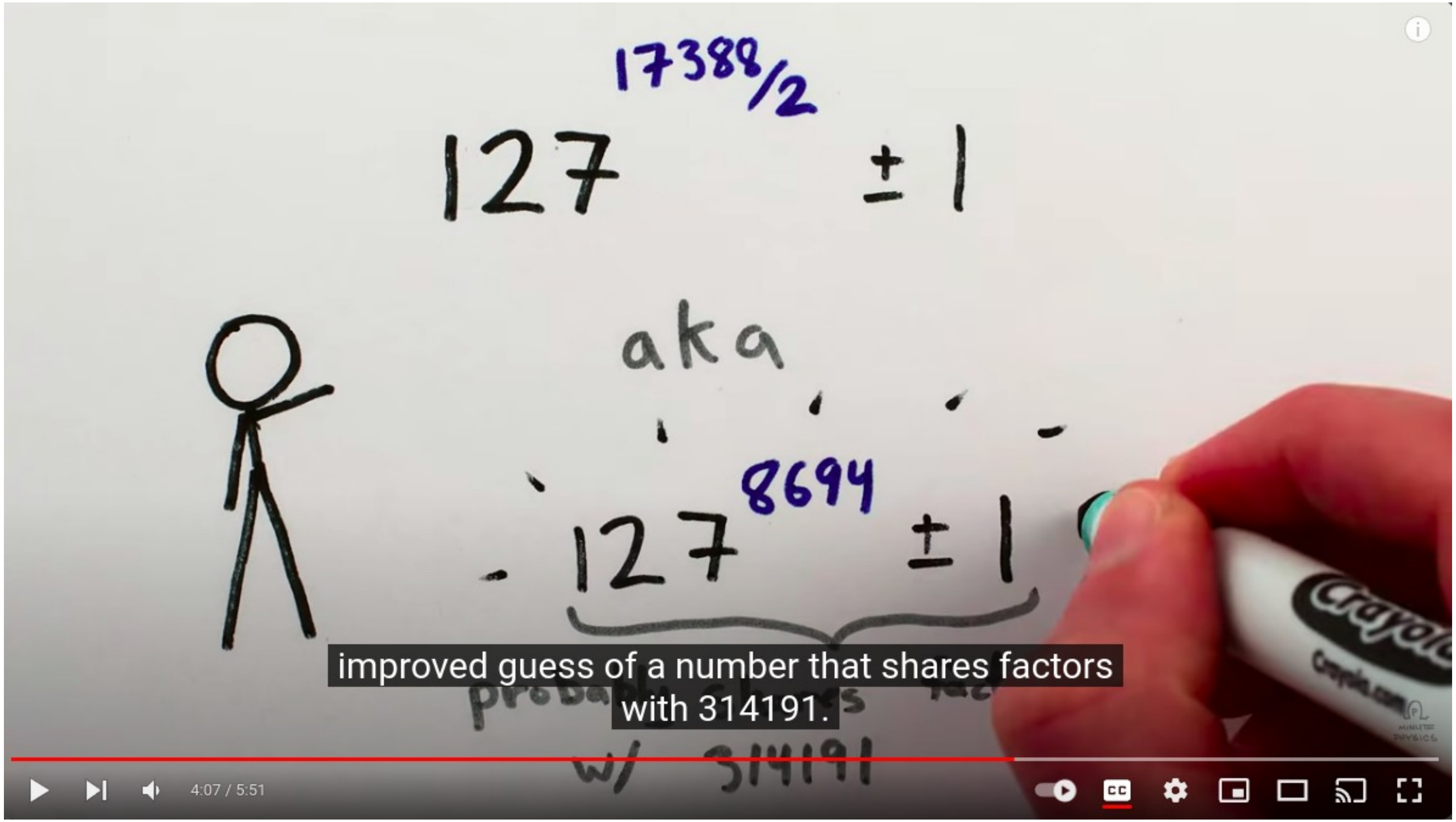
https://en.wikipedia.org/wiki/Shor%27s_algorithm#/media/File:Shor's_algorithm.svg

Haddamard *vs.* FFT

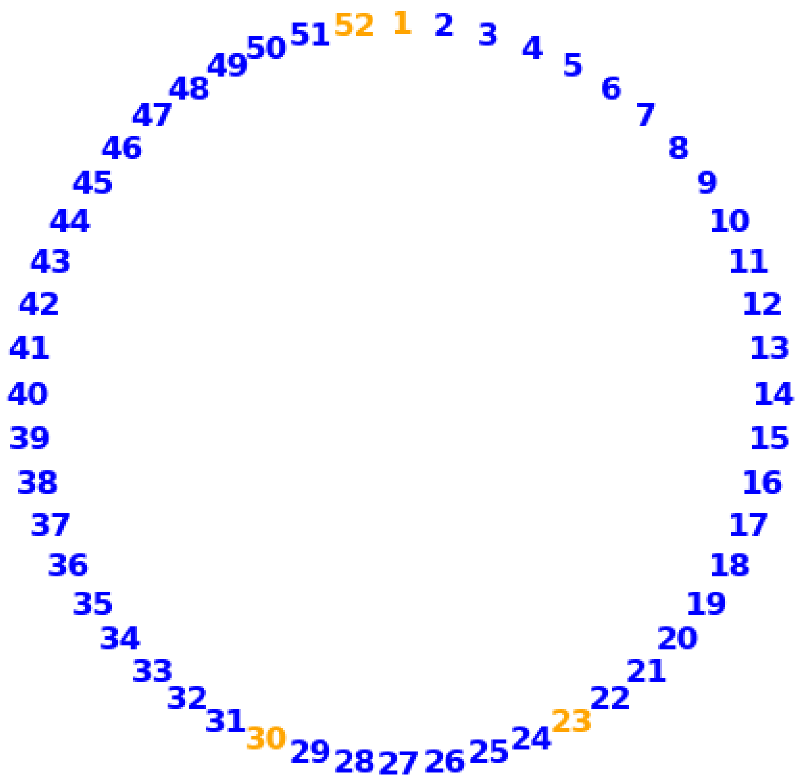
- Haddamard <u>is</u> an FFT
  - Just not the one we want
- Same butterfly pattern + twiddle factors gives the FFT we want



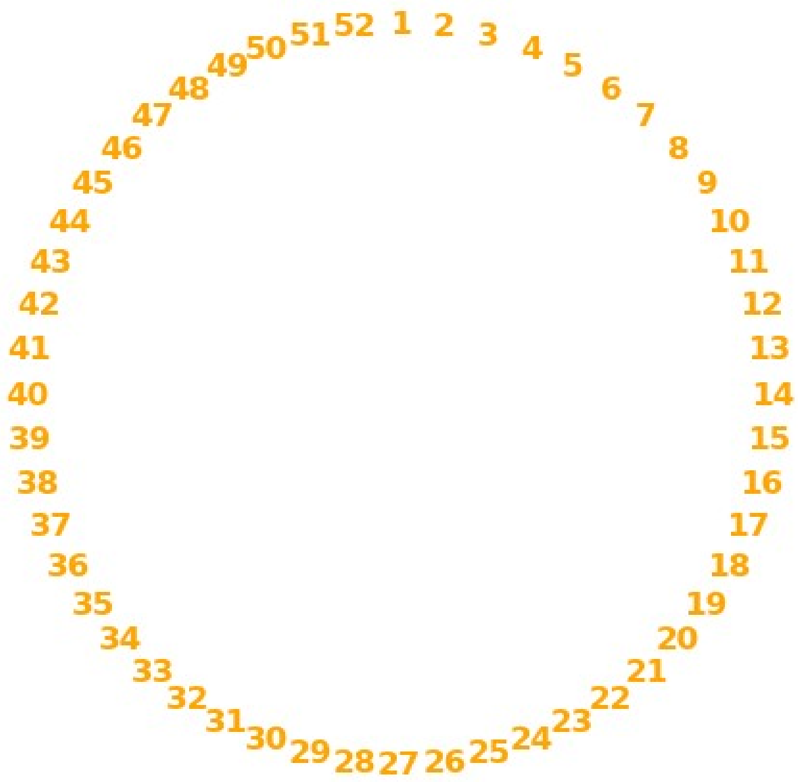
https://courses.physics.illinois.edu/phys498cmp/sp2022/QC/QFT.html https://www.youtube.com/watch?v=FRZQ-efABeQ



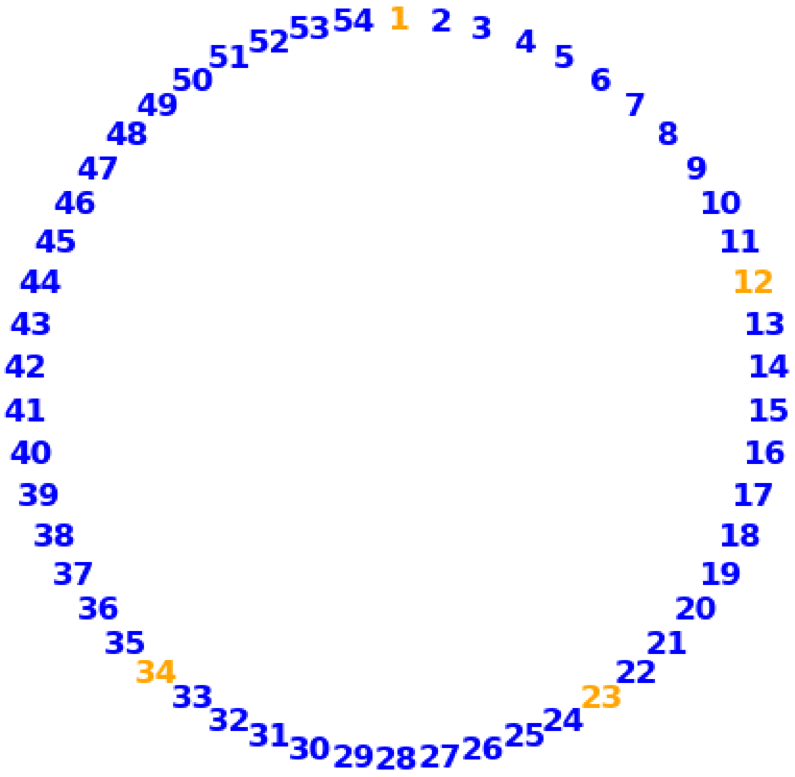
Orange are powers of 30 mod 53
Order is 4



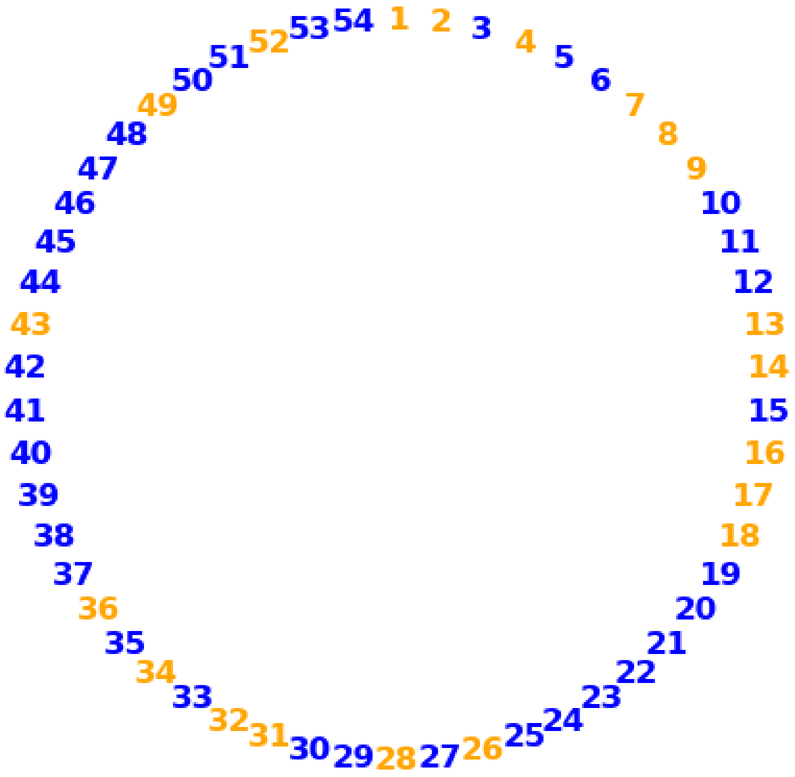
Orange are powers of 12 mod 53
Order is 52



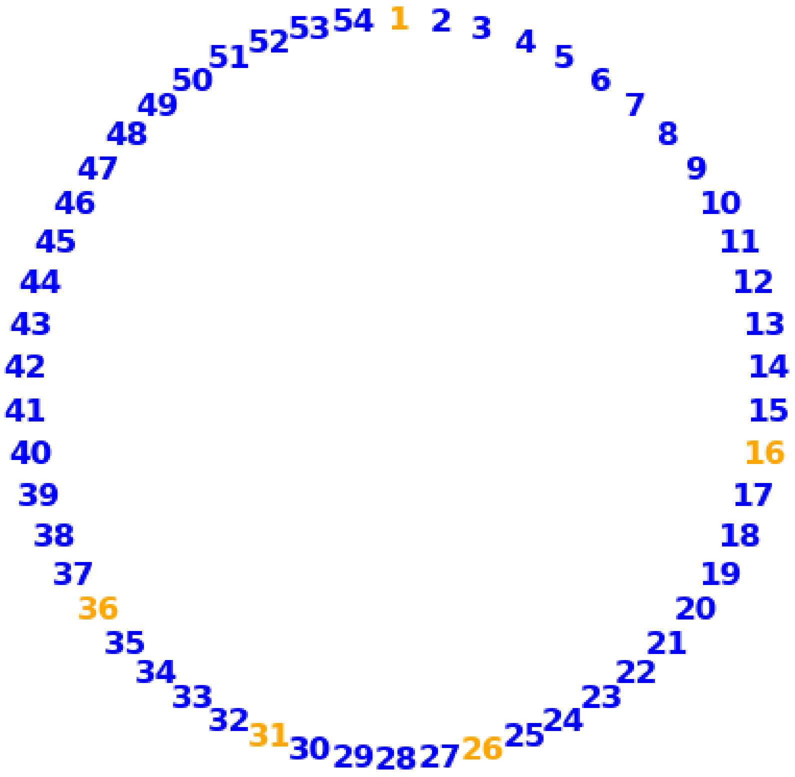
Orange are powers of 12 mod 55
Order is 4

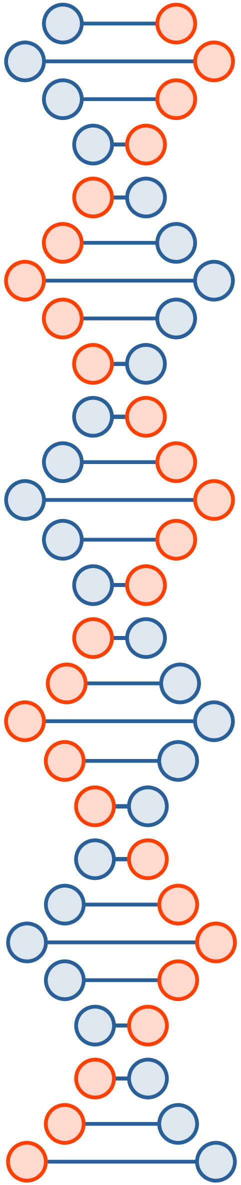


Orange are powers of 13 mod 55
Order is 20



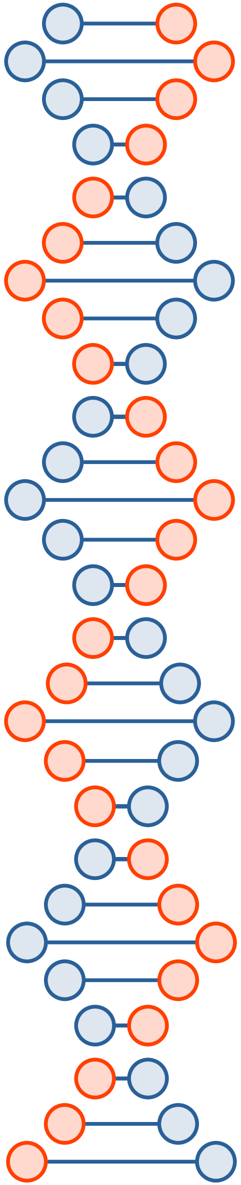
Orange are powers of 16 mod 55
Order is 5

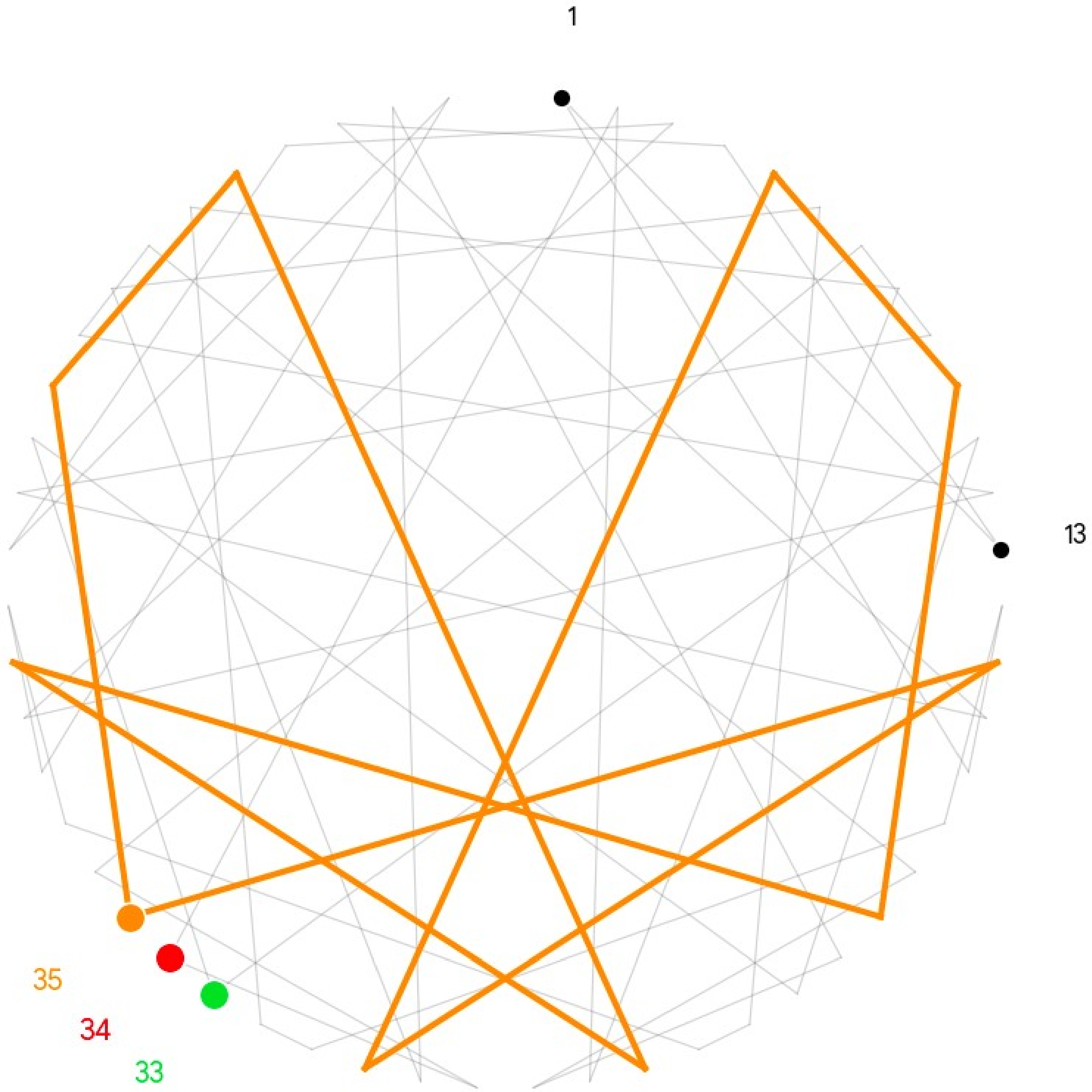


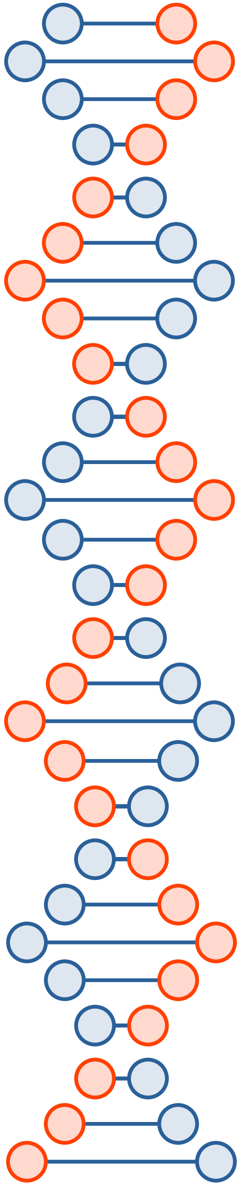


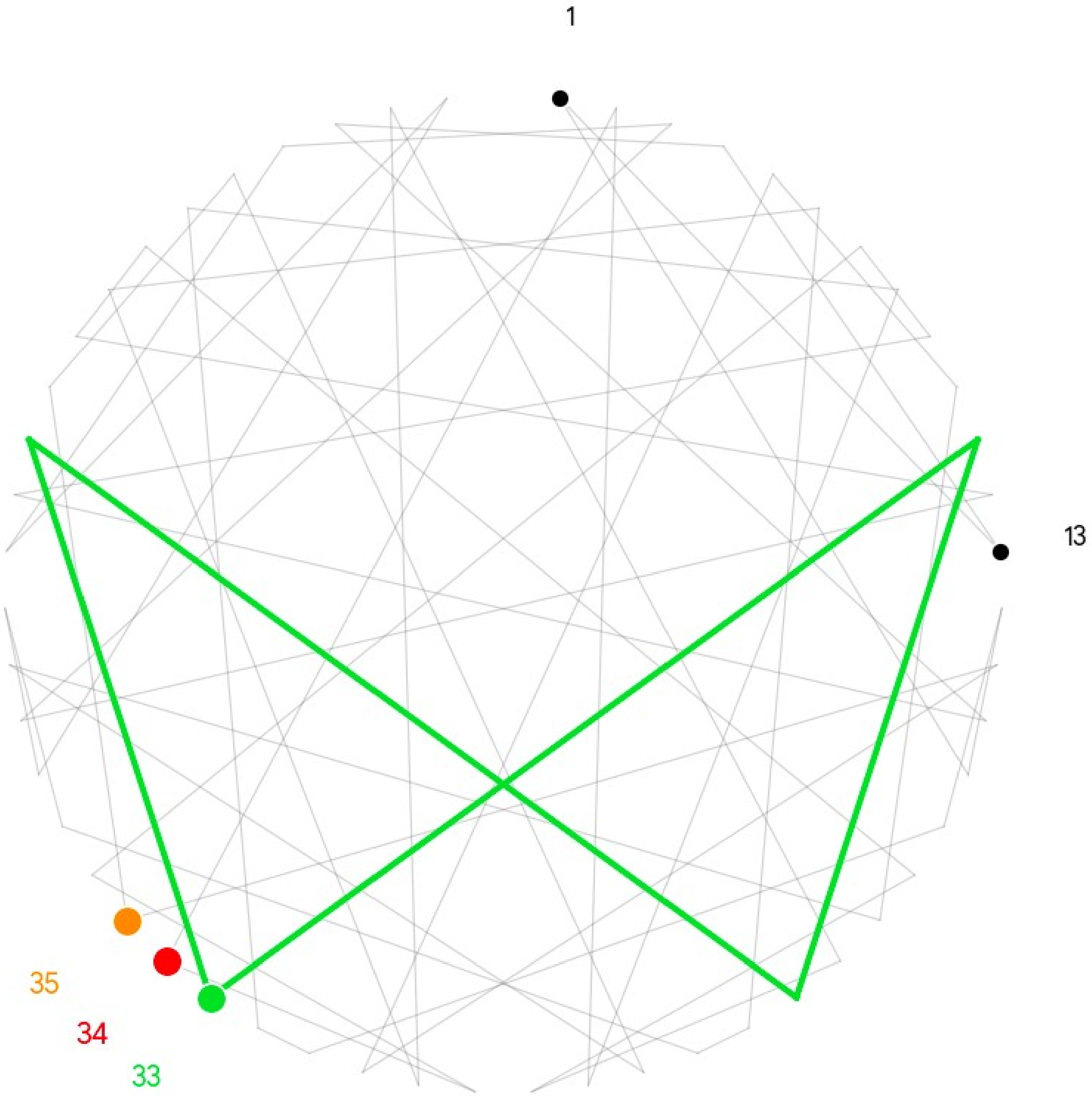
$$(13^{10} + 1) \bmod 55 = 35$$

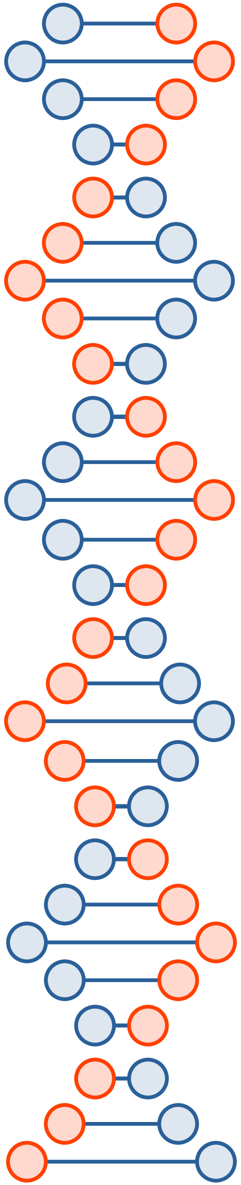
$$\gcd(35, 55) = 5$$

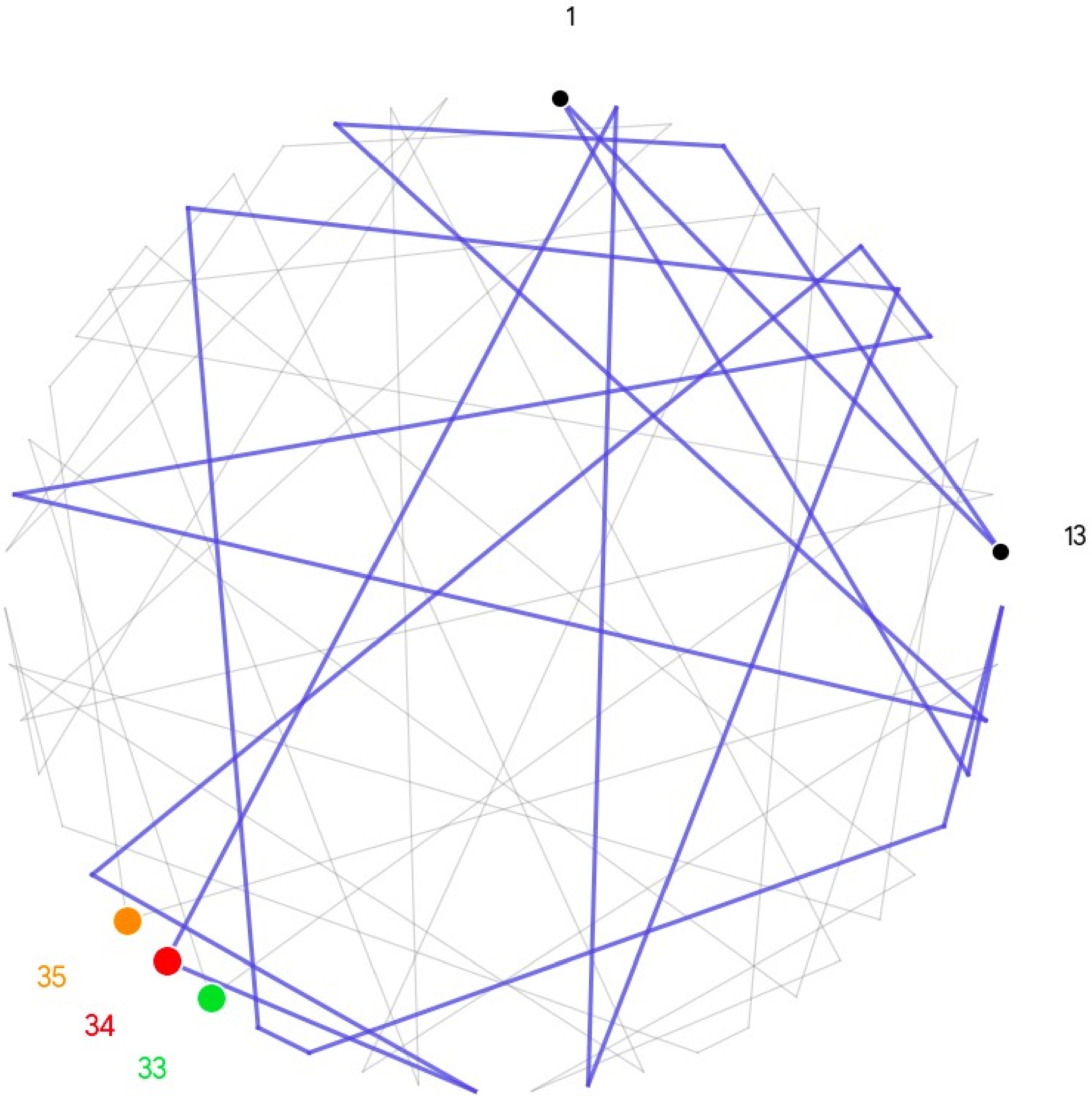


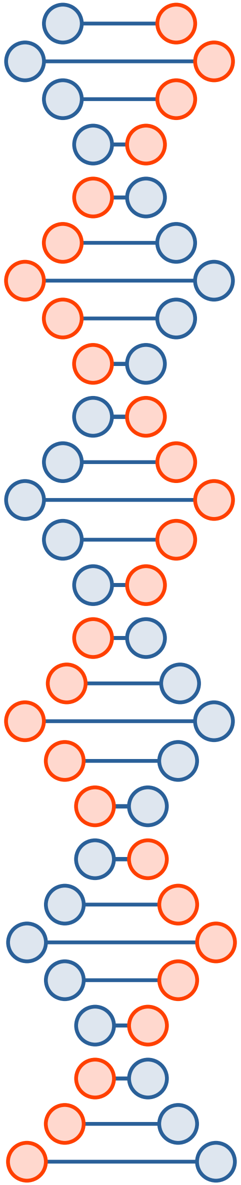

1
13
35
34
33

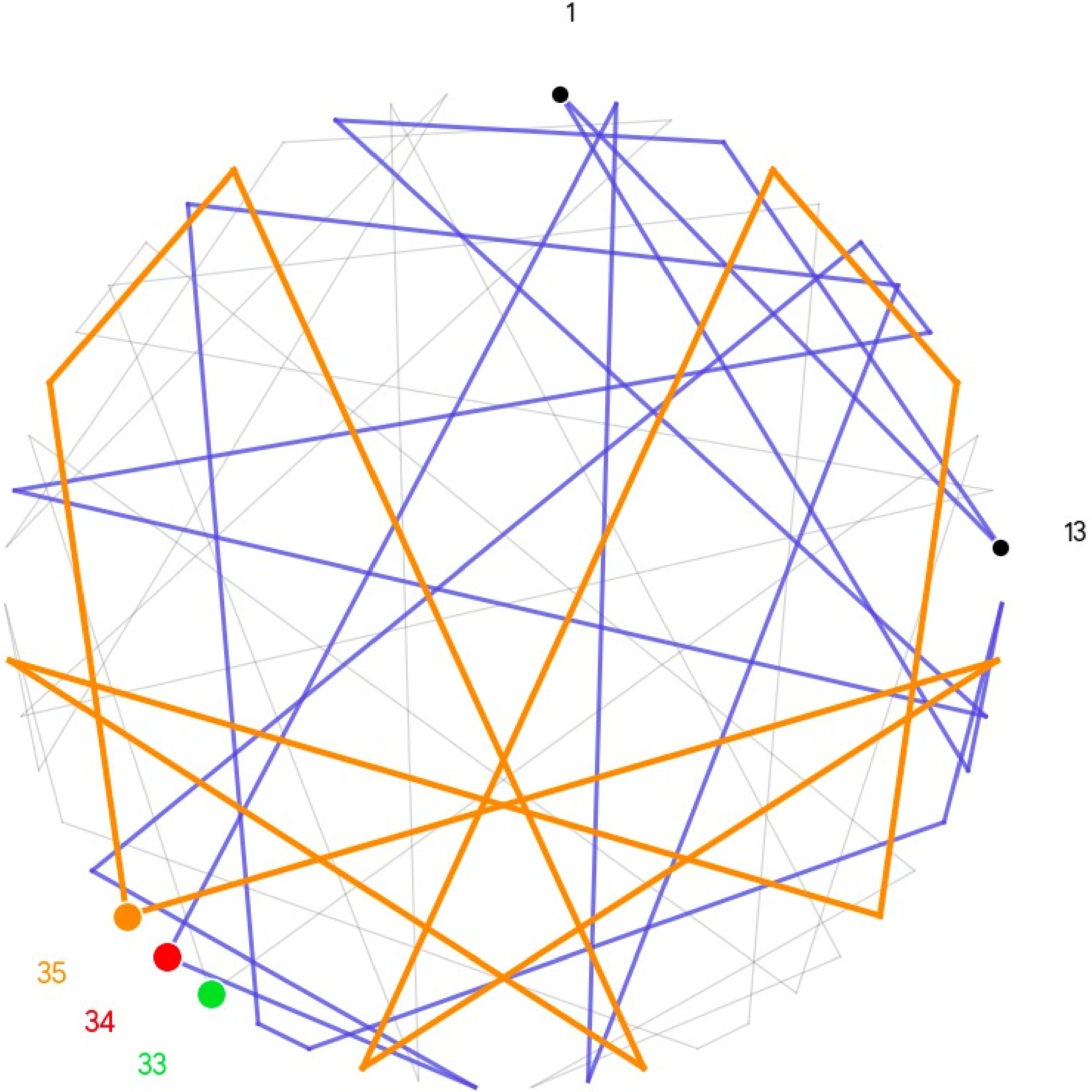


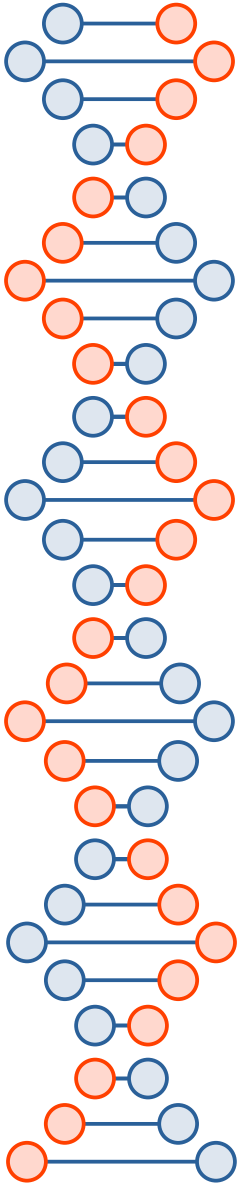

1
13
35
34
33

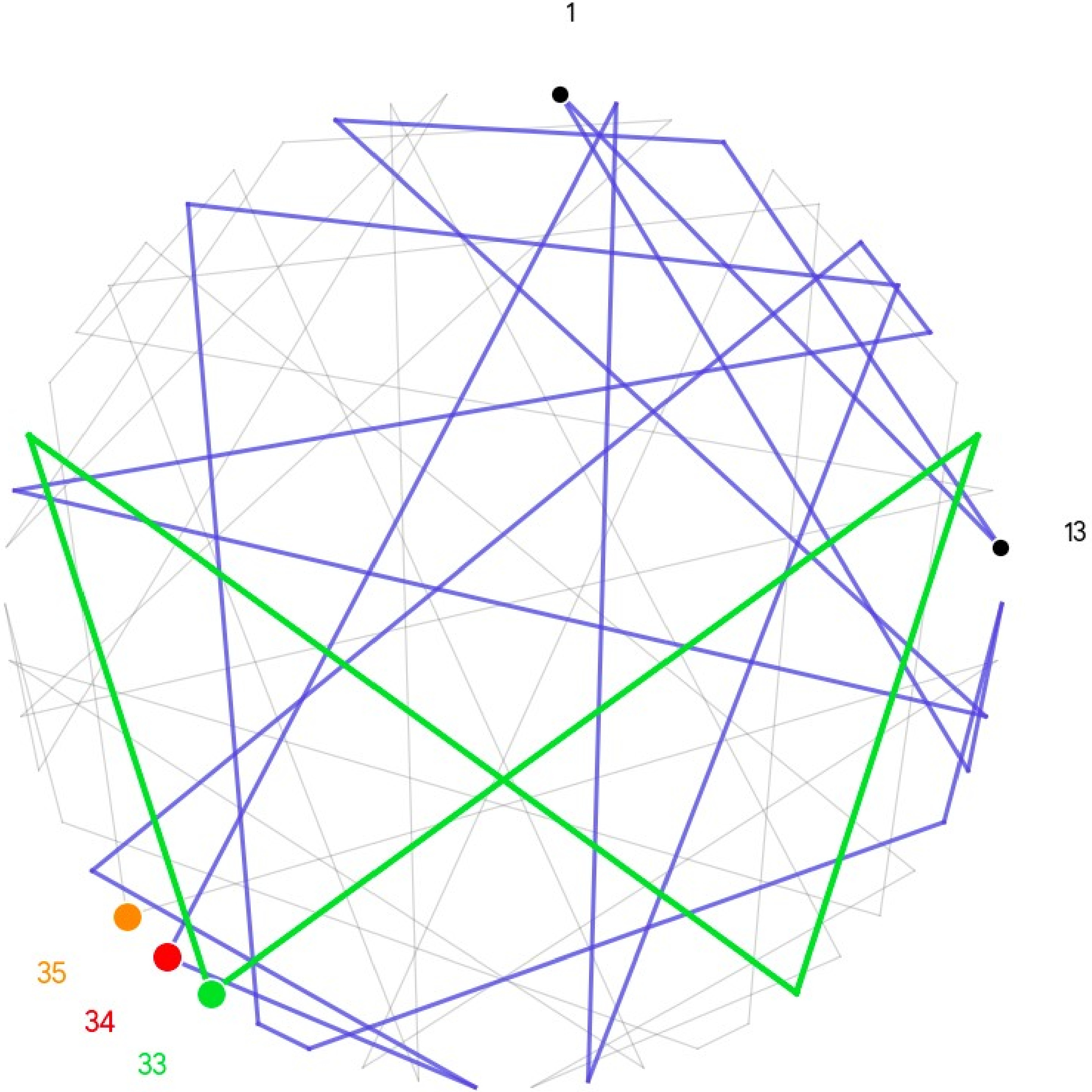


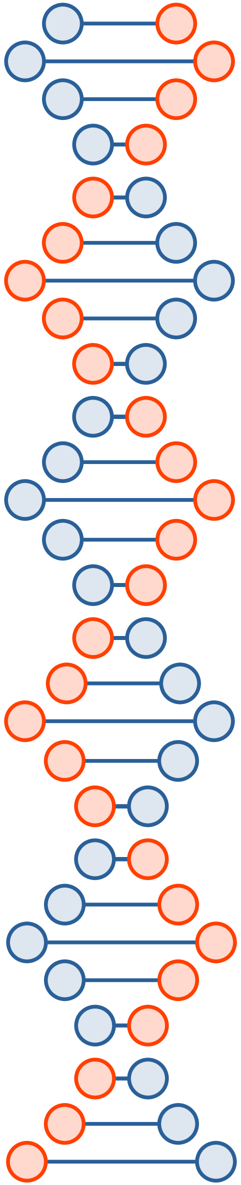

1
13
35
34
33

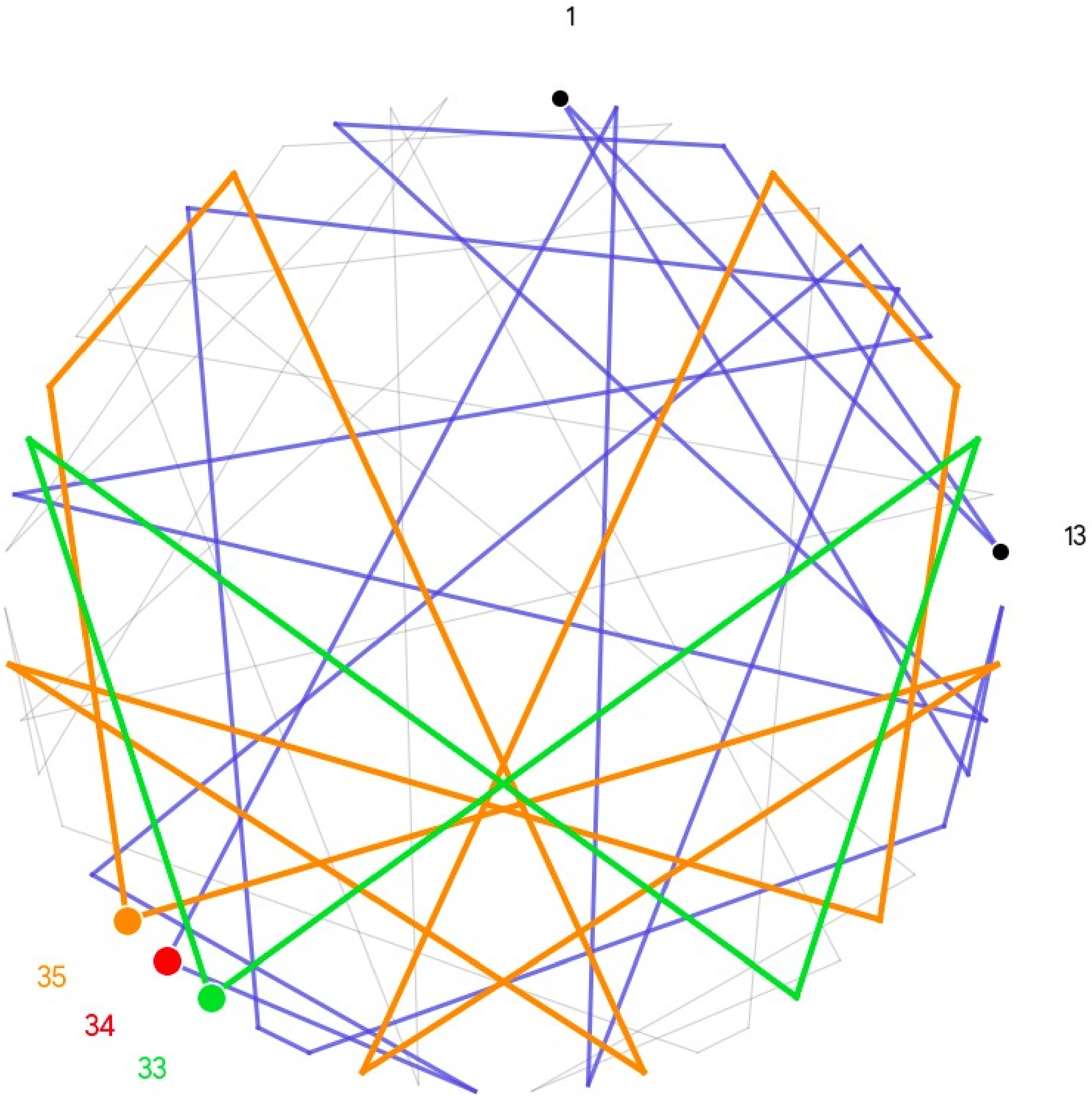


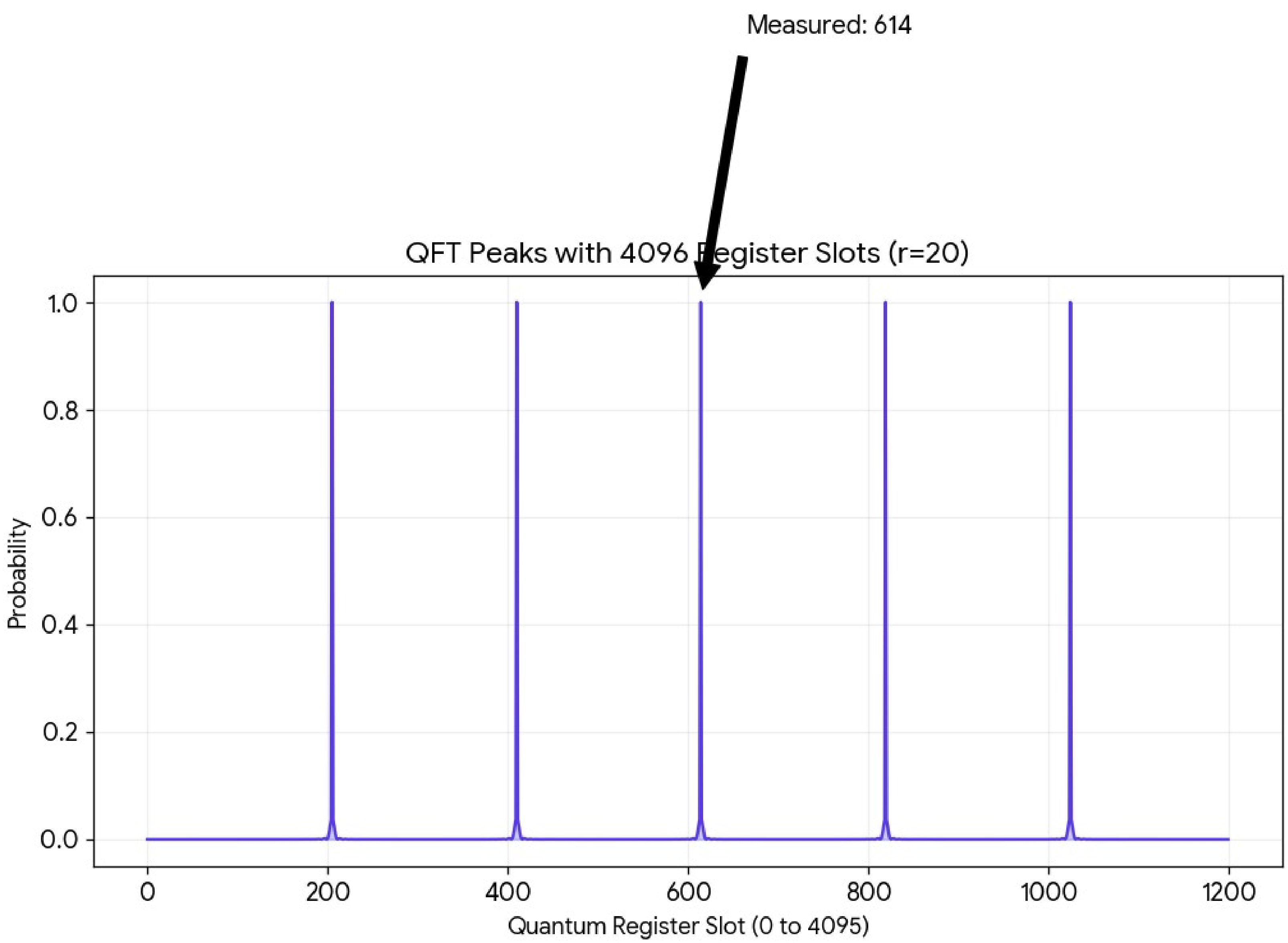

1
13
35
34
33




1
13
35
34
33




1
13
35
34
33


Measured: 614
QFT Peaks with 4096 Register Slots (r=20)
1.0
0.8
0.6
0.4
0.2
0.0
Probability
0
200
400
600
800
1000
1200
Quantum Register Slot (0 to 4095)

Continued fractions

We start with π and repeatedly subtract the integer part, then take the reciprocal:

1. **Start with $\pi \approx 3.14159265...$**
   1. **Strip** the 3. Remaining: $0.14159265...$
   2. **Flip**: $1/0.14159265 \approx \mathbf{7}.0625...$
2. **Strip the 7**
   1. Remaining: $0.062513...$
   2. **Flip**: $1/0.062513 \approx \mathbf{15}.996...$

3. **Strip the $\mathbf{15}$**

   1. Remaining: $0.9965...$
   2. **Flip**: $1/0.9965 \approx \mathbf{1}.0034...$

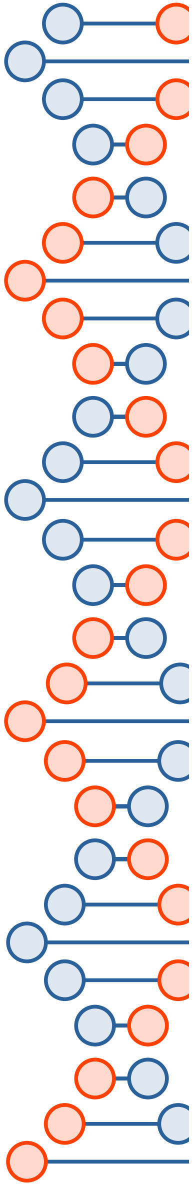
4. **Strip the $\mathbf{1}$**

   1. Remaining: $0.0034...$
   2. **Flip**: $1/0.0034 \approx \mathbf{292}.63...$

The coefficients we found are $\mathbf{[3; 7, 15, 1, 292]}$.

Now we reassemble these coefficients into fractions. This is where the math "locks on" to the target:

- **Rung 1:** Just the first number: **3/1**
- **Rung 2:** $3 + 1/7 =$ **22/7** (The standard school estimate)
- **Rung 3:** $3 + \frac{1}{7+\frac{1}{15}} = 3 + \frac{15}{106} = \mathbf{333/106}$
- **Rung 4:** $3 + \frac{1}{7+\frac{1}{15+\frac{1}{1}}} = 3 + \frac{1}{7+\frac{1}{16}} = 3 + \frac{16}{113} = \mathbf{355/113}$



Quantum Estimate: 614/4096 ≈ 0.14990

Rung 1:	0/1	▯ Noise
Rung 2:	1/6	▯ Noise
Rung 3:	1/7	▯ Noise
Rung 4:	3/20	▯ Exact Period (r=20)!
Rung 5:	76/507	▯ Noise

To solve $g^x \equiv A \pmod{p}$, the algorithm defines a function f with two input variables, α and β:

$$f(\alpha, \beta) = g^{\alpha} A^{-\beta} \pmod{p}$$

Since $A = g^x$, this can be rewritten as:

$$f(\alpha, \beta) = g^{\alpha} (g^x)^{-\beta} = g^{\alpha - x\beta} \pmod{p}$$

2. Identifying the Periodicity

The function $f(\alpha, \beta)$ is periodic. Specifically, it has a "hidden" period whenever the exponent $(\alpha - x\beta)$ results in the same value. Project Eleven

- If we add a pair (ω_1, ω_2) to our inputs such that $f(\alpha + \omega_1, \beta + \omega_2) = f(\alpha, \beta)$, it implies that $g^{\omega_1} A^{-\omega_2} = 1$.
- Substituting $A = g^x$, we get $g^{\omega_1 - x\omega_2} \equiv 1 \pmod{p}$.
- This means the exponent must be a multiple of the group order r: $\omega_1 - x\omega_2 \equiv 0 \pmod{r}$. Cryptography Stack Exchange

https://crypto.stackexchange.com/questions/37018/using-shors-algorithm-to-solve-the-discrete-logarithm-problem#:~:text=Indeed%2C%20one%20has%20f(x,Add%20a%20comment

A couple of more links...

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

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

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).

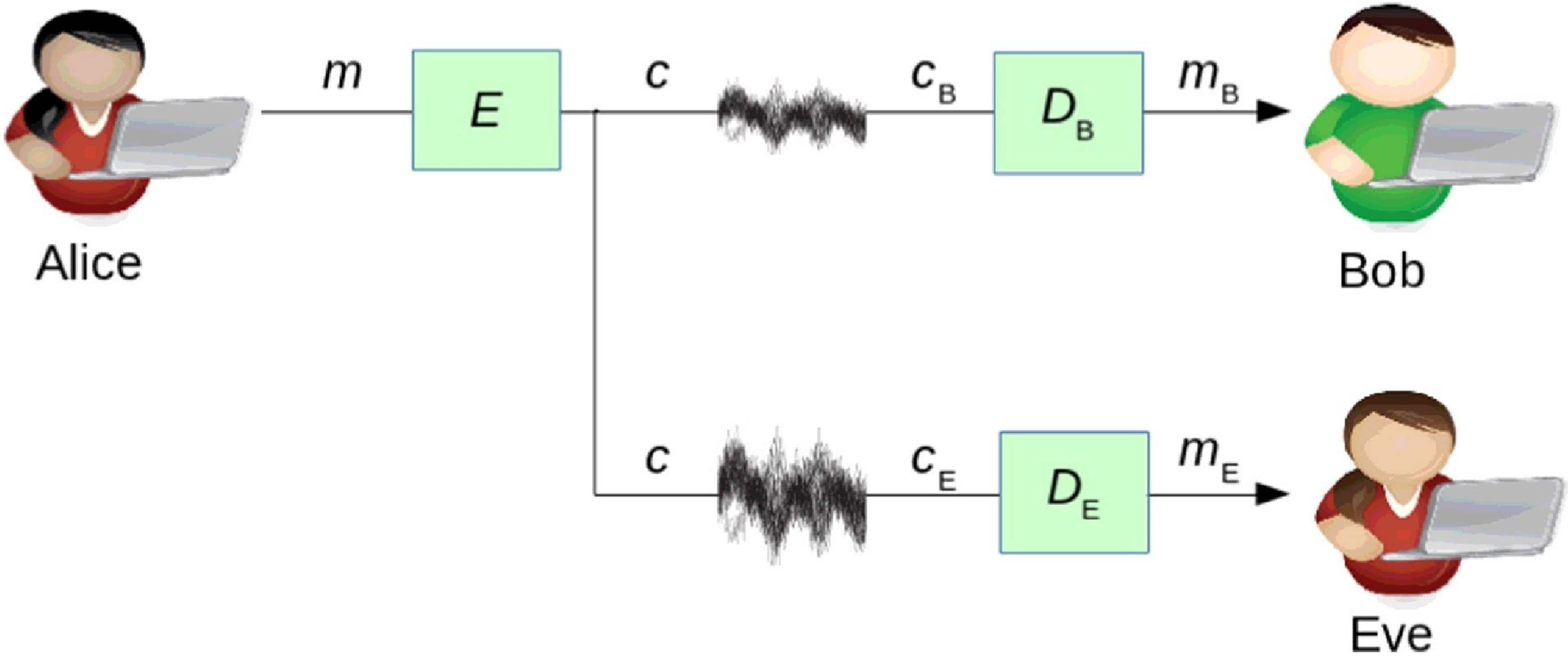
RSA, DH, ECDH, DSA, *etc*. all broken. Need something else instead...

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

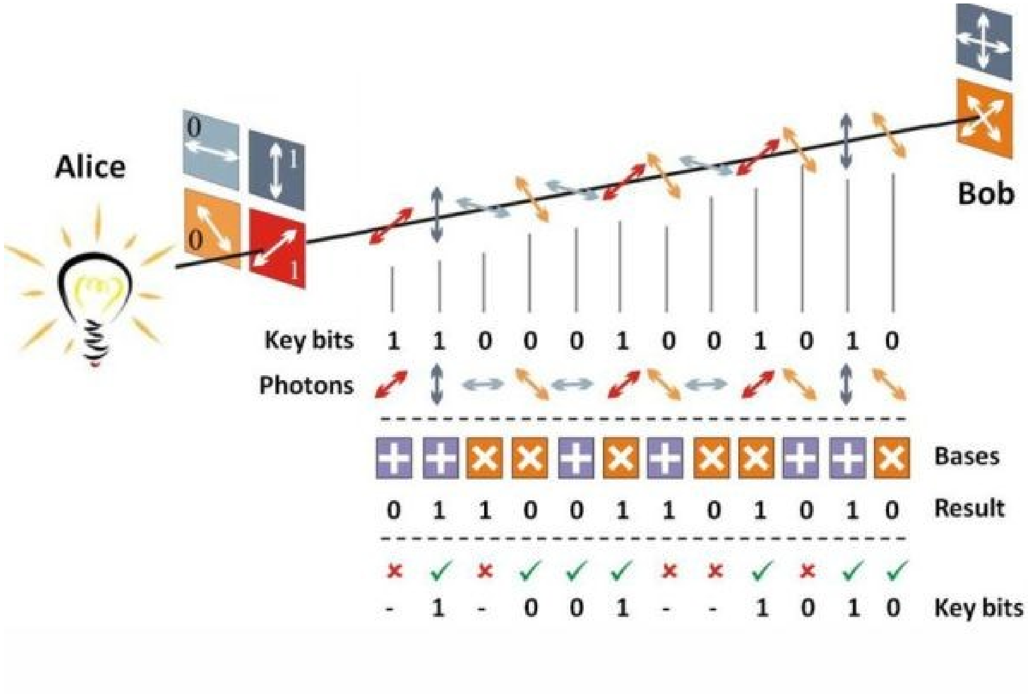
https://en.wikipedia.org/wiki/Lamport_signature

Wiretap channel



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

Quantum Key Distribution



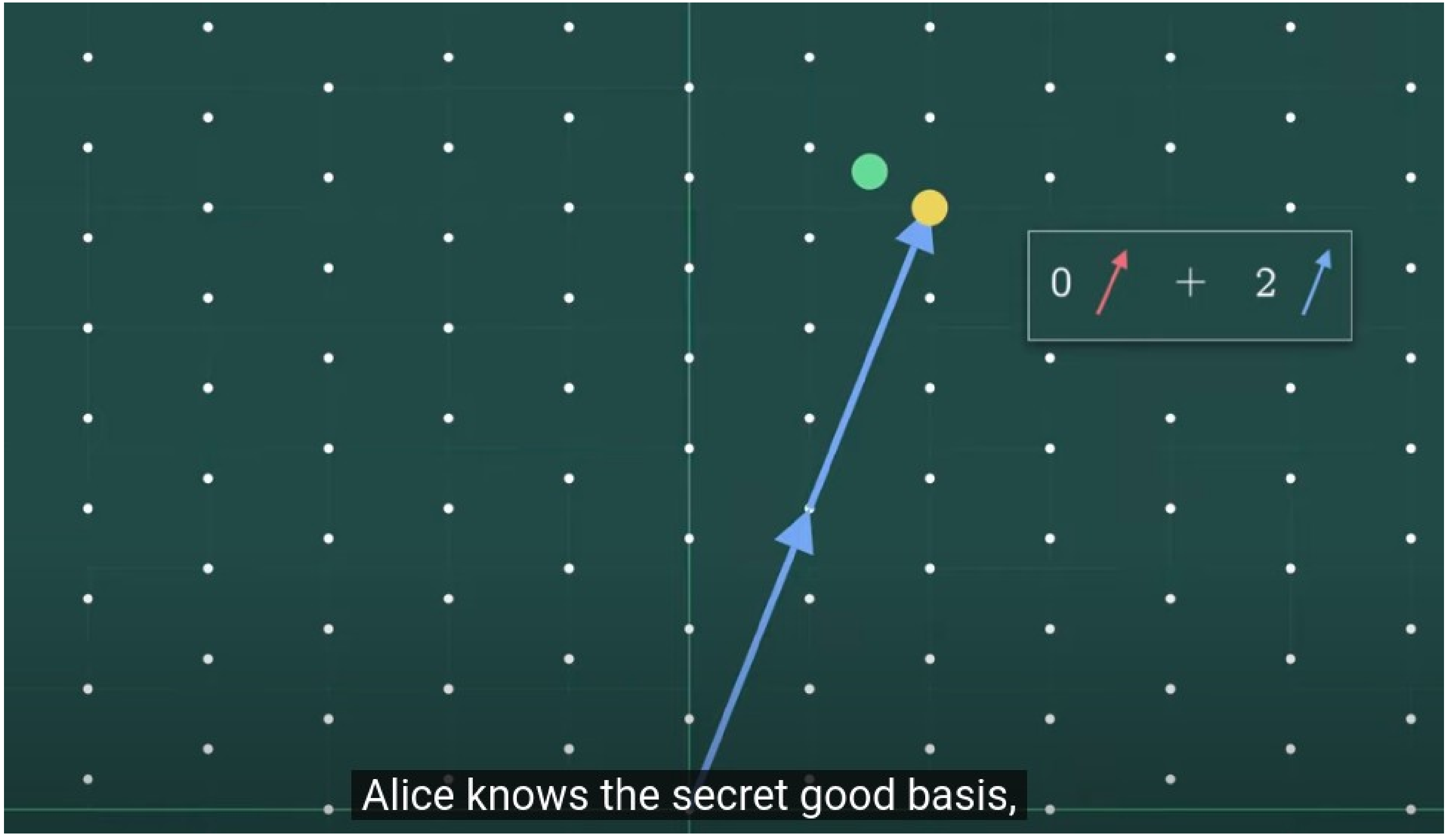
https://imrmedia.in/quantum-key-distribution-test-successfully-demonstrated/

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

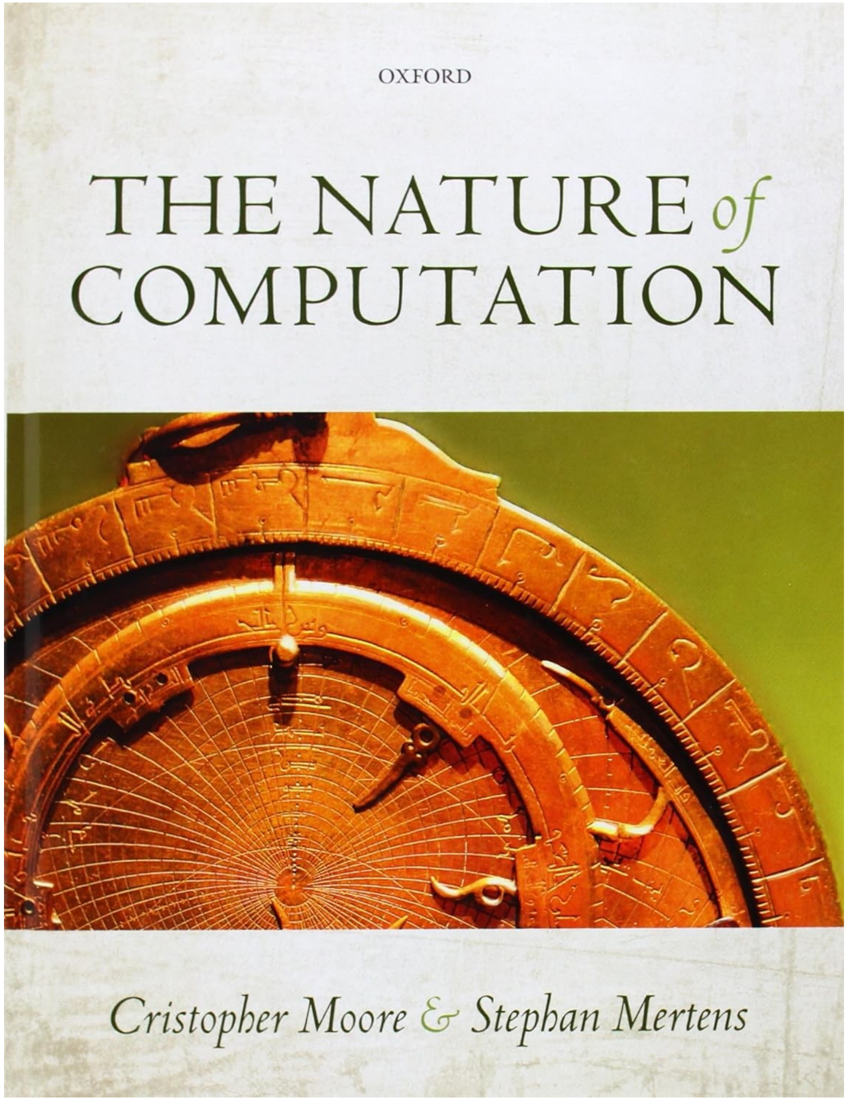


Take-aways…

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


OXFORD
THE NATURE of COMPUTATION
Cristopher Moore & Stephan Mertens