An Introduction to Cryptography

Part 3: Quantum & Post-Quantum Crypto

Anthony Kosednar

My Background

- Education
  - Number Theory, Field Theory, Cryptography and Statistics @ ASU
  - Aerospace Engineering - Astronautics @ ASU
  - DHS Cybersecurity Training for Industrial Control Systems – SCADA, DCS, PLC, Embedded Control
  - GIAC Exploit Researcher and Advanced Penetration Tester - GXPN
- Career Highlights
  - Built a natural air-cooled datacenter in under 6 months
  - Lead encryption for a large fortune 50 financial institution
  - Prevented cyber attacks for large events (Arizona Cardinals, Arizona Board of Tourism, NFL, Super Bowl XLIX, Fiesta Bowl)

Quantum Computers – Common Fears

Is the security of the internet at risk?

Will all financial institutions be at risk?

Will I never win the lottery?

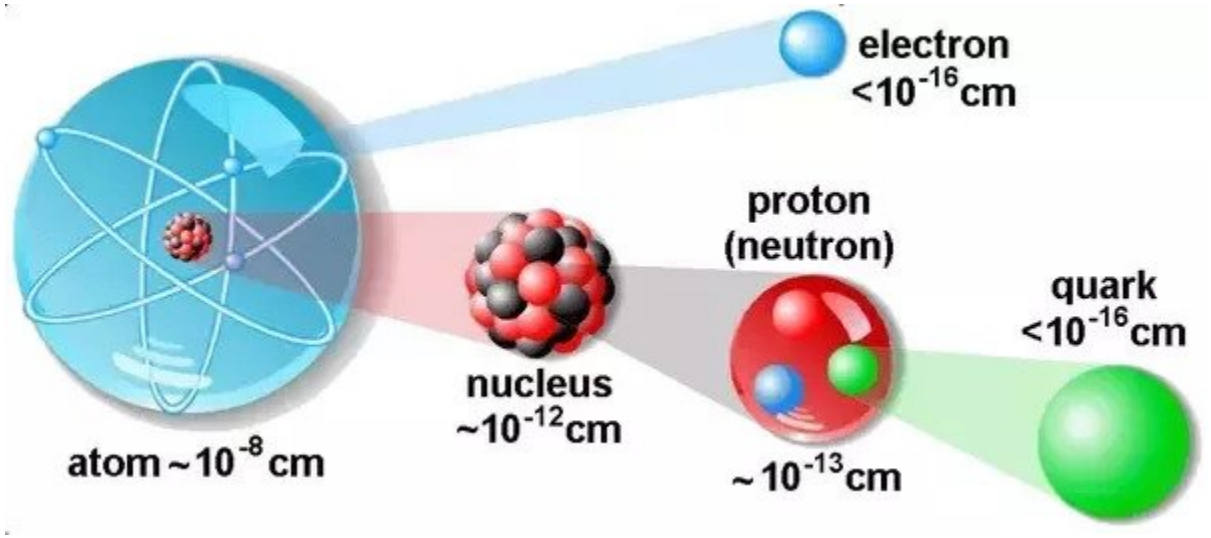
I’m here to help!

First some background

A Simple Overview Quantum Mechanics

What is Quantum Mechanics?

- Describes nature at the smallest scales of energy (atoms & subatomic particles)



Quantum Mechanics - Popular View

- Quantum Mechanics is weird!
- Quantum objects can both be waves and particles: ***wave-particle duality***
- Quantum objects can be in more than one state at once: ***superposition***
- You can't simultaneously know exactly two properties of a quantum object: ***Heisenberg's uncertainty principle***
- Quantum objects can affect one another instantly over huge distances ("spooky action at a distance"): ***entanglement***
- You can't measure anything without disturbing it, and so quantum mechanics is subjective

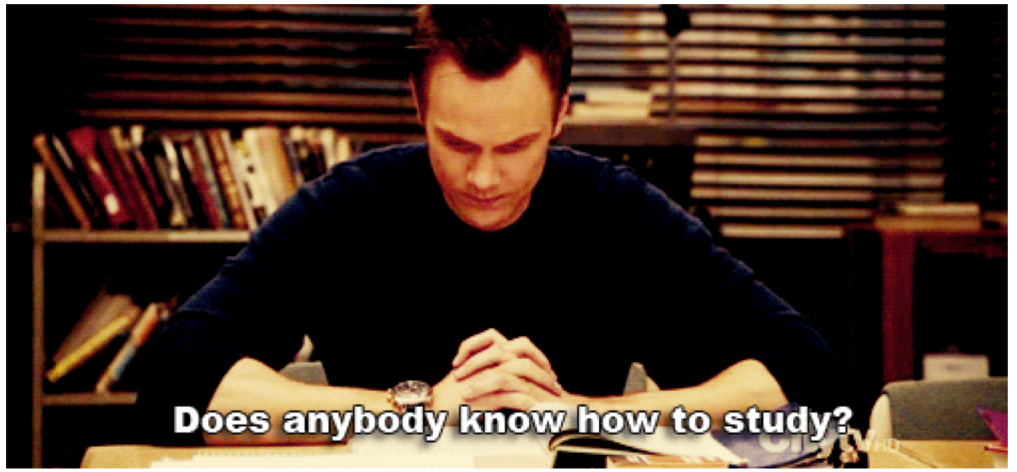
Quantum Mechanics - Popular View

- Quantum Mechanics is weird!
- Quantum objects can both be waves and particles: wave-particle duality
- Quantum objects can be in more than one state at once: superposition
- You can't simultaneously know exactly two properties of a quantum object: Heisenberg's uncertainty principle
- Quantum objects can affect one another instantly over huge distances ("spooky action at a distance"): *entanglement*
- You can't measure anything without disturbing it, and so quantum mechanics is subjective

Not Exactly Right

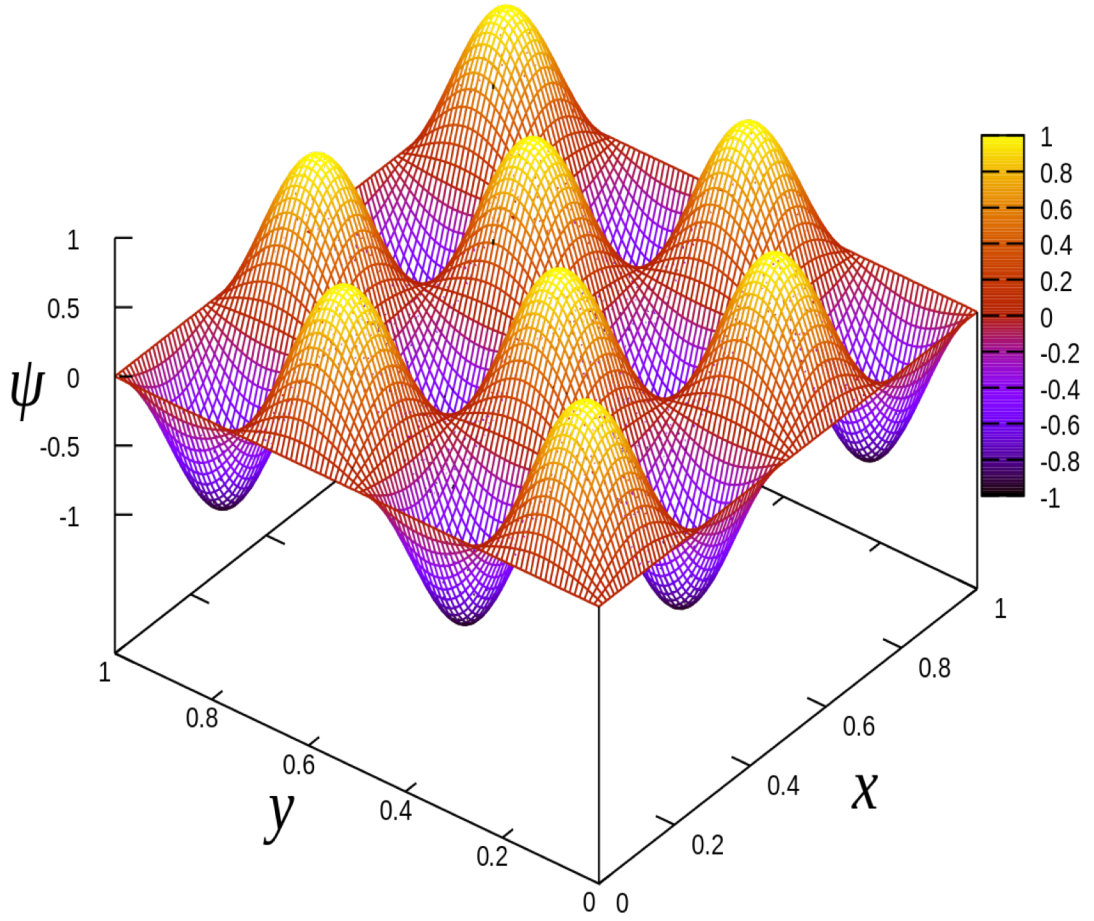
Why is Quantum Mechanics Hard?

- Traditional Newtonian Mechanics – (what you are use to):
  - It’s obvious
  - We don’t need to ask questions around our definitions
  - We have an idea with a position, path and force are
- Quantum Mechanics:
  - Non-definitive
  - Influenced by us measuring
  - We don’t know all the answers



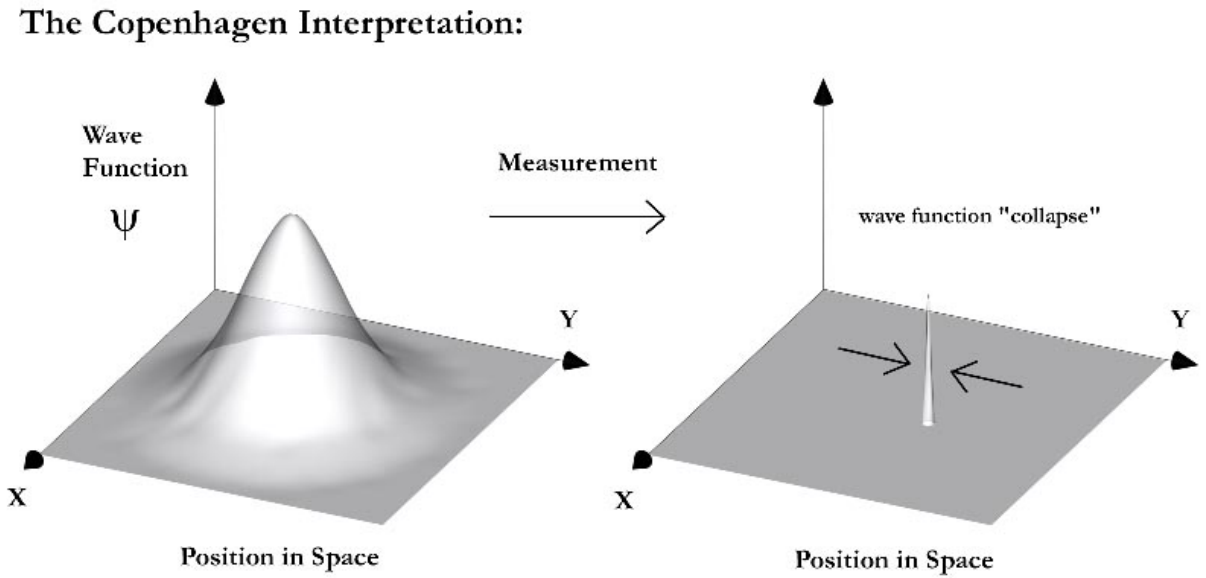
Wave-Particle Duality
Schrodinger's Wave Function

- Schrodinger created function to show particles might act as a wave
- Doesn't tell us the protectory of a particle but rather where we might find a particle; What properties it might have.
- Often said the particle is spread out all over the place
- However is a math functions to represent the possible measurement outcomes (and probability to make that result).
- Tells us the chance of where we find it if we look



Collapse of the Wave Function

- When we make a measurement suddenly it collapses to a single position because now we know where it is
- No way of describing this in Quantum Mechanics
- Quantum Mechanics says:
  - There were different probabilities that a measurement would reveal a particle at a particular place
  - After measuring you know it's "THERE"



Spin!

Spin Up

(1)

Spin Down

(0)

Spin!

Spin Up (1)

Spin Down (0)

Basis of quantum computers because we can record binary data!

Act as quantum bits or QBits!

Spin!

Spin Up (1)

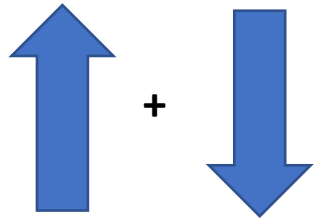
Spin Down (0)

Basis of quantum computers because we can record binary data!

Act as quantum bits or Qubits!

However it is said it can be often in both states at once

Superposition



Spin!

Spin Up (1)

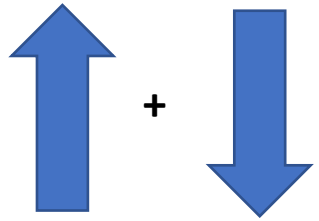
Spin Down (0)

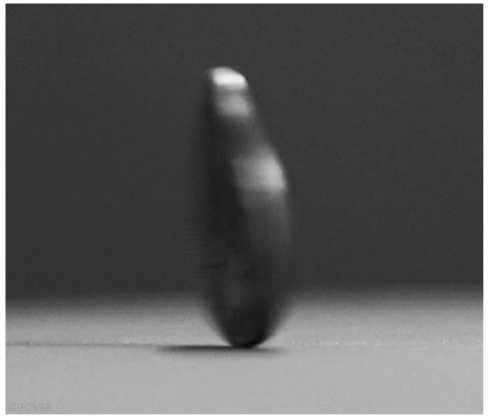
Basis of quantum computers because we can record binary data!

Act as quantum bits or QBits!

It is said it can be often in both states at once

Superposition





Spin!

Spin Up (1)

Spin Down (0)

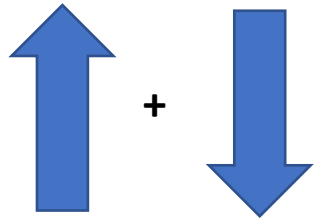
Basis of quantum computers because we can record binary data!

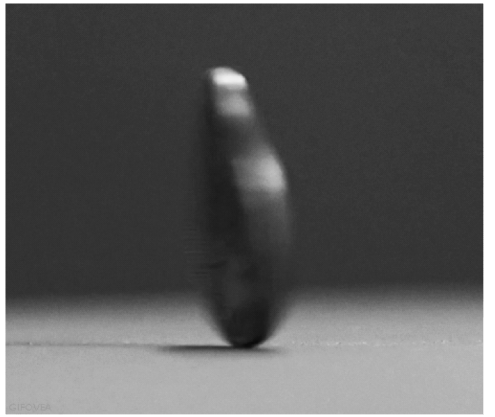
Act as quantum bits or QBits!

Wave function only tells us what to expect when we make a measurement

WRONG ~~It is said it can be often in both states at once~~

Superposition

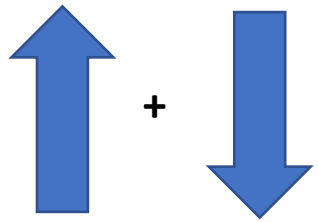


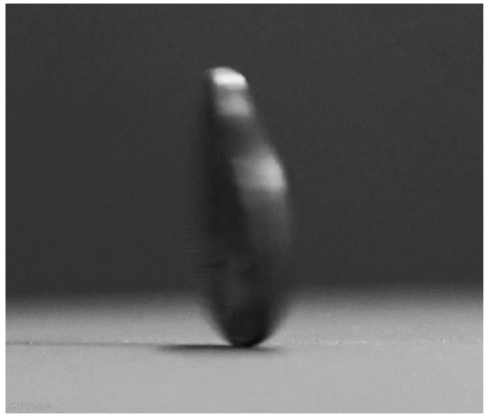


Spin!

- What the wave function says:
  - A measurement might give us an up or a down spin
- Before measurement?
  - Quantum mechanics doesn't really tell us

Superposition



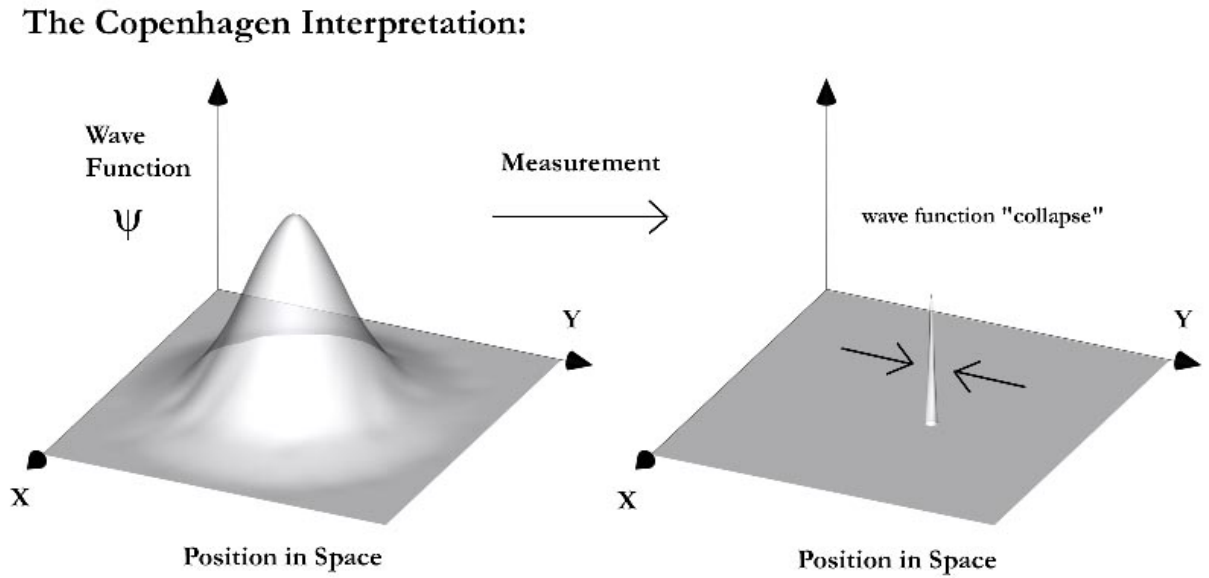


Entanglement

- Two quantum objects that collide become entangled or linked
- When measured you'd be able to predict the measurement of the other
- Quantum objects that are entangled do not have properties that are located in the object
    - Example: The blackness of two quantum entangled objects are not local to their locality but quantumly existing

More Quantum Properties

- As a quantum object interacts with it's environment, it becomes harder to see it's super position in the environment. The quantum-ness gets washed away – decoherence.
- After this, they start to become more like classical objects



Quantum Mechanics – Reality

- Not – here it is a particle, there it is a wave
- But Rather - if measured, a quantum object behaves in a manner we associate with particles; but if we measure it, it behaves as if it's a wave
- Not - the particle is in two states at once
- But – if measured, we will detect this state with probability X, and that state with probability Y

Classical vs Quantum Computing

A Note on Mindset

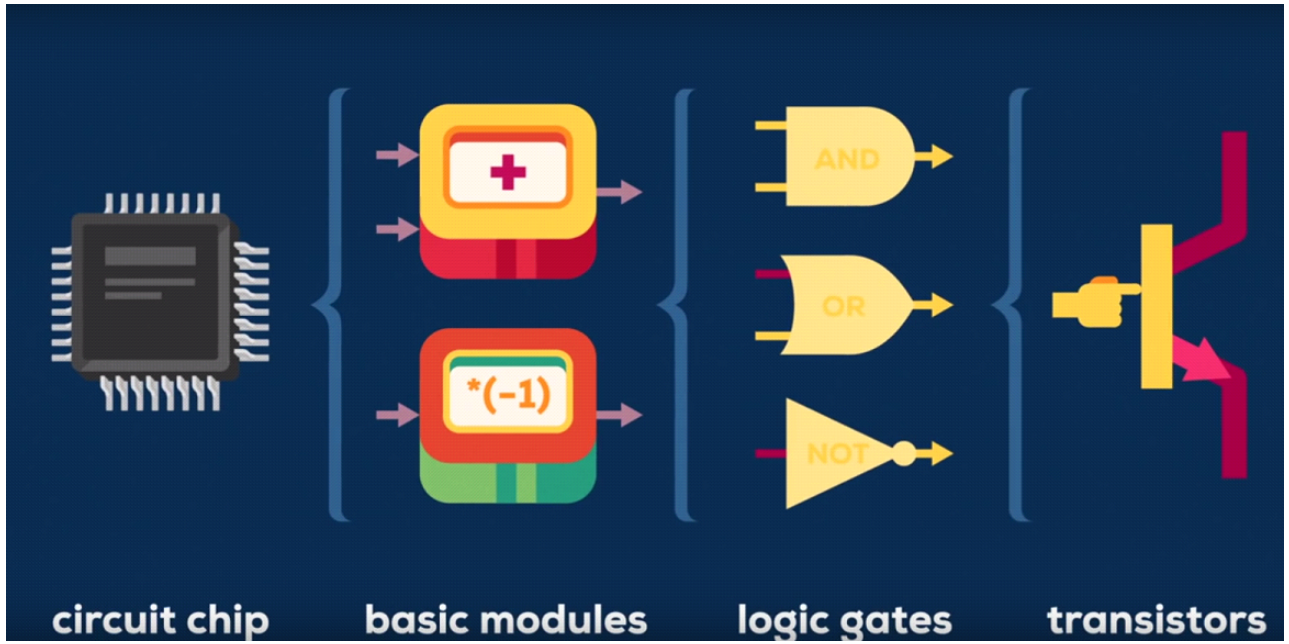
- A light bulb is not a more powerful version of the candle. They execute similar functions but are based on different technologies. They execute their task in different ways.

A Note on Mindset

- A light bulb is not a more powerful version of the candle. They execute similar functions but are based on different technologies. They execute their task in different ways.
- Similarly….a quantum computer is not a more powerful version of a classical computer!

How do classical computers work?

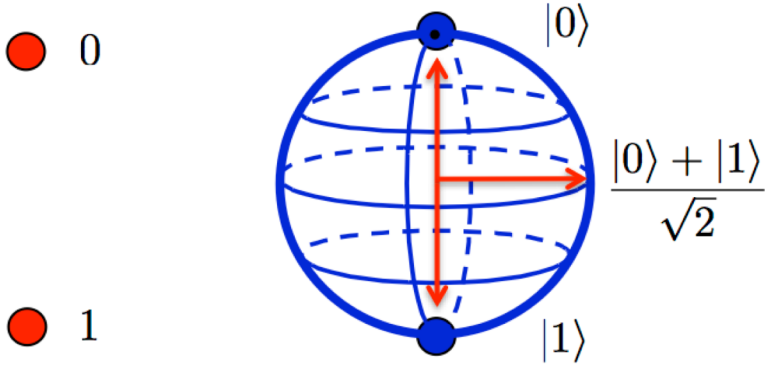
- Bits (16 combinations)
  - 1 or 0 - on or off
- Transistors
- Logic Gates
- Modules



Bits vs Qubits

Bits:

- Computes by manipulating bits with the help of logical gates
- Has a memory made up of bits where each bit holds either a one or a zero



Classical Bit **Qubit**

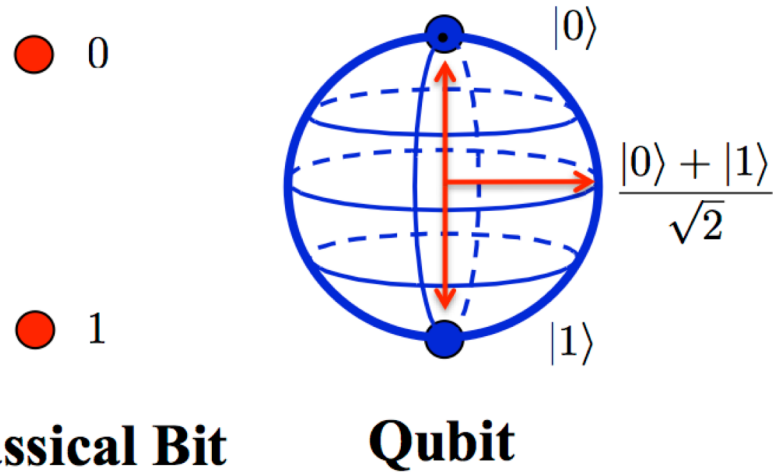
Qubits:

- Device computes by manipulating bits with the help of quantum logic gates.
- A qubit when can hold a one, zero, or a super position of those until measured
- Once measured it’s non-quantum

Bits vs Qubits

Bits:

- Computes by manipulating bits with the help of logical gates
- Has a memory made up of bits where each bit holds either a one or a zero



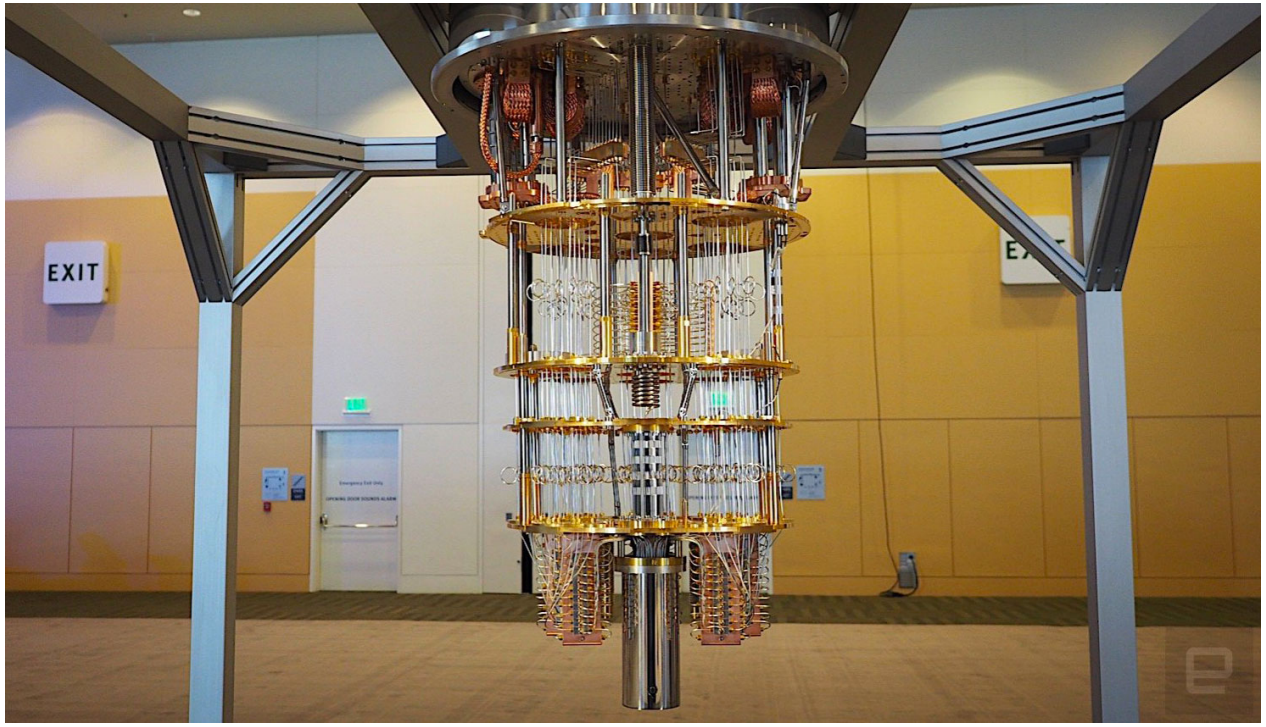
Qubits:

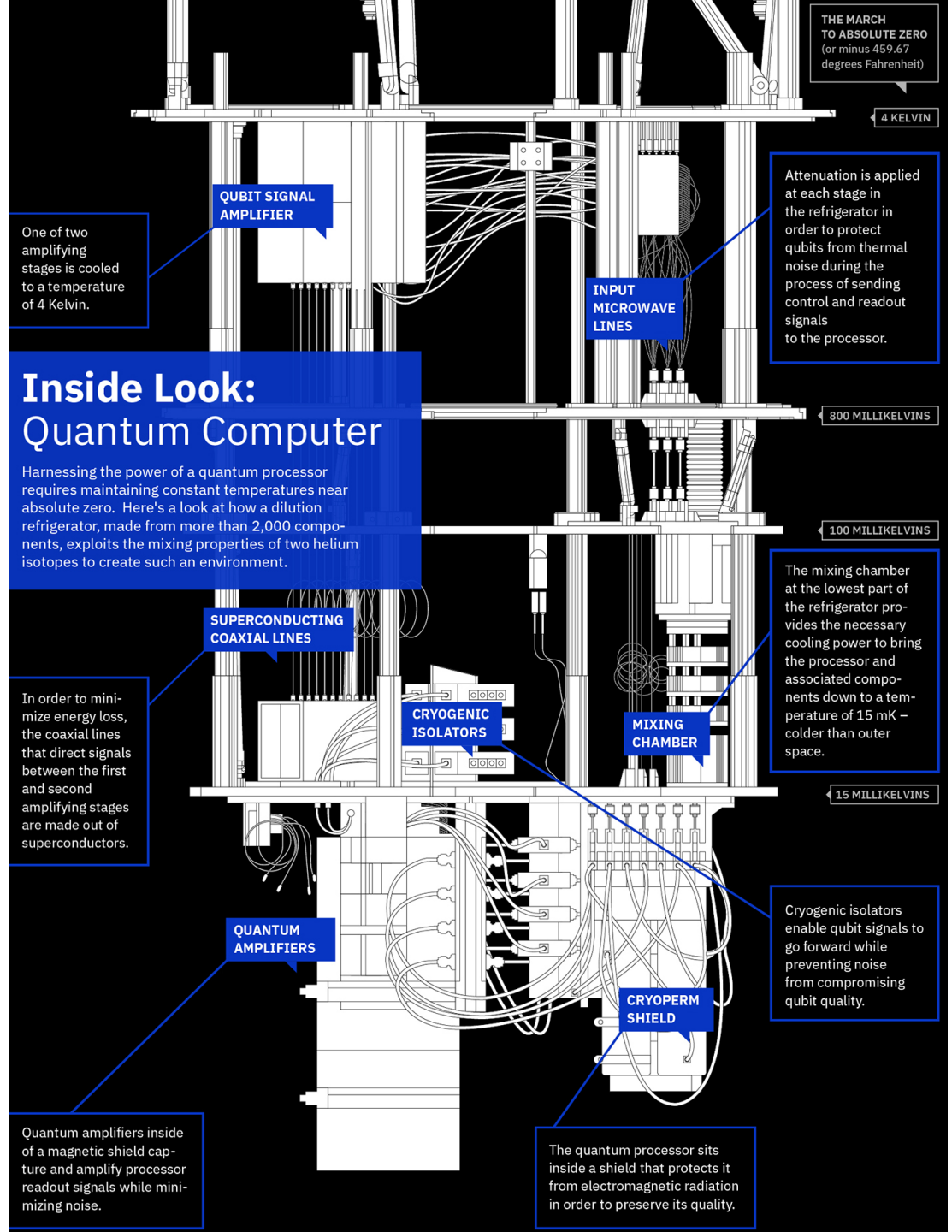
- Device computes by manipulating bits with the help of quantum logic gates.
- A qubit when can hold a one, zero, or a super position of those until measured
- Once measured it's non-quantum
- **We can only keep it quantum for so long!**

Quantum Computer!

- Has a physical qubit that can be put into the spin states
  - Typically atoms, ions, or other super conducting materials
  - Controlled and measured via microwave pulses
- Very sensitive to noise and environmental affects
- Can only keep information quantum for so long

Quantum Computer!




THE MARCH TO ABSOLUTE ZERO (or minus 459.67 degrees Fahrenheit)
4 KELVIN
QUBIT SIGNAL AMPLIFIER
One of two amplifying stages is cooled to a temperature of 4 Kelvin.
Attenuation is applied at each stage in the refrigerator in order to protect qubits from thermal noise during the process of sending control and readout signals to the processor.
INPUT MICROWAVE LINES
Inside Look:
Quantum Computer
Harnessing the power of a quantum processor requires maintaining constant temperatures near absolute zero. Here's a look at how a dilution refrigerator, made from more than 2,000 components, exploits the mixing properties of two helium isotopes to create such an environment.
800 MILLIKELVINS
100 MILLIKELVINS
The mixing chamber at the lowest part of the refrigerator provides the necessary cooling power to bring the processor and associated components down to a temperature of 15 mK – colder than outer space.
SUPERCONDUCTING COAXIAL LINES
In order to minimize energy loss, the coaxial lines that direct signals between the first and second amplifying stages are made out of superconductors.
CRYOGENIC ISOLATORS
MIXING CHAMBER
15 MILLIKELVINS
Cryogenic isolators enable qubit signals to go forward while preventing noise from compromising qubit quality.
QUANTUM AMPLIFIERS
CRYOPERM SHIELD
Quantum amplifiers inside of a magnetic shield capture and amplify processor readout signals while minimizing noise.
The quantum processor sits inside a shield that protects it from electromagnetic radiation in order to preserve its quality.

Breaking Cryptography with a Quantum Computer

Shor’s Algorithm and Breaking RSA Encryption

(Asymmetric Cryptography)

Review!: RSA

- Widely used:
  - Digital signatures
  - Key distribution
- Works by taking two large prime numbers, multiplying them together and combining them with a pair of exponents
  - Ex: 15 = 3 * 5
- Security depends on the difficulty of finding those prime factor

Lh_f Fincta&

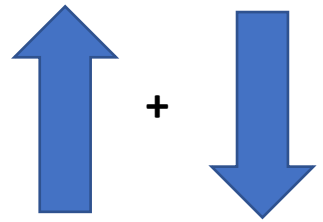
Traditional Breaking of RSA

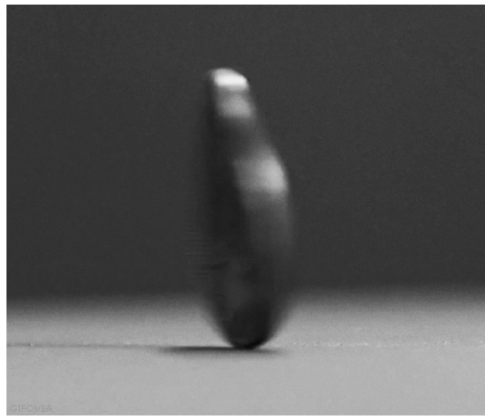
- How – the best methods guess the factors, check, and try again!
- Super slow
  - Even with the fast ways to make good guesses!
- RSA-768 takes over 2,000 years of computer processing time break
  - 1 month in a proper computing cluster

The Quantum Computing Way

- Easy due to
  - Quantum super positioning
  - Quantum interference
- Uses Shor's Algorithm with some tricks!

Superposition





Shor's Algorithm

- Start with a guess of what might share a factor but probably doesn't
- Algorithm turns it into a better guess that might share a factor!
- Nothing quantum about this on the surface
- Can do it on a classical computer
  - However Turning a bad guess to a good one takes a long time on normal computers!
- Super fast on quantum computers

How it works?

To find a factor of N we don’t have to guess a factor of N!

1. Starts with a big number, N, that we need to find the factors of to break into encrypted data
2. We make a guess, g, that is some number less that N
   - Doesn’t need to be a pure factor of N but a number that shares some factors
   - Ex: 4 isn’t a factor of 6 but shares some factors with it. 4 = 2*2 , 6 = 2*3
3. We can guess numbers that share a factor - because of Euclid’s Algorithm
   - Hard though because it is extremely unlikely a guess with share a factor

We have a trick!

- Let's convert a crappy guess into a pair of great guesses
  - $g \rightarrow g^{\frac{P}{2}} \mp 1$
- For any pair of whole numbers that don't share a factor if you multiply one by it's self enough times you'll eventually get:
  - $A, B \rightarrow A * A * A \ldots . * A = something \ * B + 1$
  - $A^P = m * B + 1$
- Ex:
  - 7, 15
  - $7^4 = 160 * 15 + 1$

We have a trick!

- Let's convert a crappy guess into a pair of great guesses
  - $g \rightarrow g^{\frac{P}{2}} \mp 1$
- For any pair of whole numbers that don't share a factor if you multiply one by it's self enough times you'll eventually get:
  - N,g
  - $\mathrm{g}, N \rightarrow g * g * g \ldots . * g = something * N + 1$
  - $g^P = m * N + 1$
- Ex:
  - 7, 15
  - $7^4 = 160 * 15 + 1$

We have a trick!

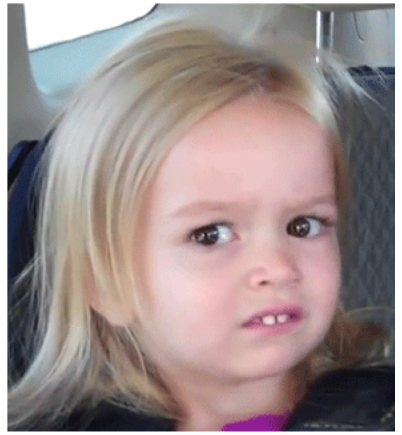
- Let's rearrange the equation
  - N,g
  - $\mathrm{g}, N \rightarrow g * g * g \ldots . * g = something * N + 1$
  - $g^P = m * N + 1$
  - $g^P - 1 = m * N$
  - $\left(g^{\frac{P}{2}} + 1\right) * \left(g^{\frac{P}{2}} - 1\right) = m * N$
- Simplified:
  1. Take crappy guess
  2. Multiply itself P/2 times
  3. Then add or subtract 1

We have a trick!

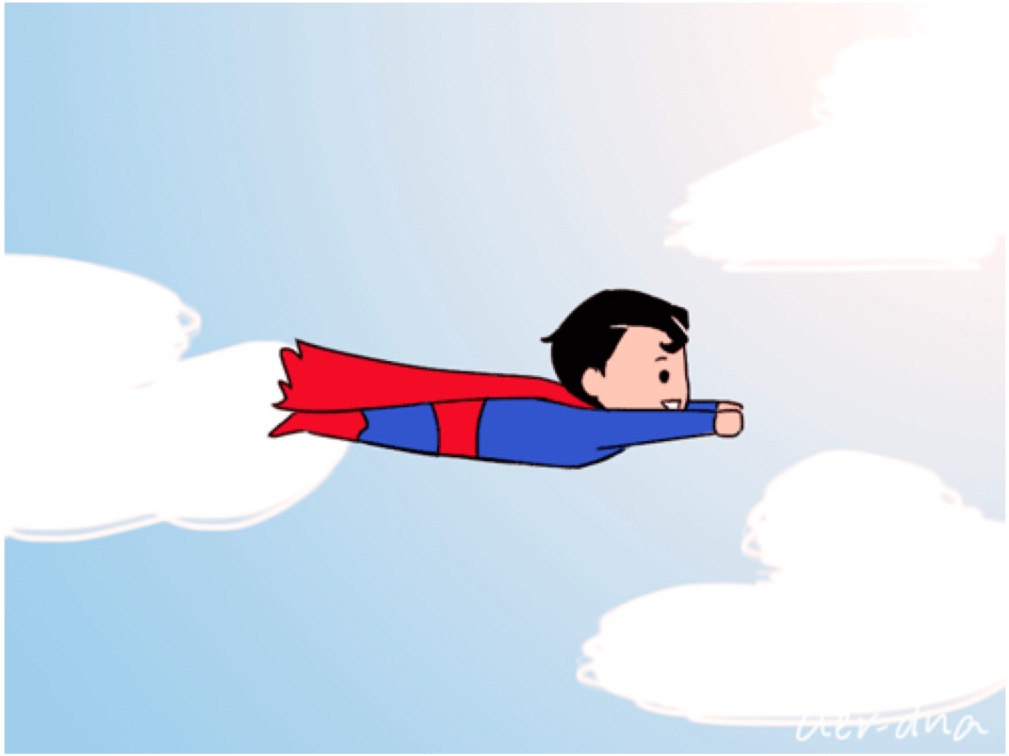
- Our equation
  - N,g
  - $\left(g^{\frac{P}{2}}+1\right)*\left(g^{\frac{P}{2}}-1\right)=m\ *N$
- Note factors on either side may be a multiple of the factor
- We can use Euclid's Algorithm to solve that
- Then the encryption is broken!

Why is this hard for classical computers?

- Problems:
  - P might be odd
  - $\left(g^{\frac{P}{2}} \pm 1\right)$ might not be a multiple of N
- However – these two problems only exist 37.5% of the time
- But…..finding p takes a long time for a classical computer to guess
  - Longer than brute forcing the actual prime



Let’s do it the Quantum Way!



Let’s do it the Quantum Way!

- Our equation
  - N,g
  - $g^P = m * N + 1$
  - $\left(g^{\frac{P}{2}} + 1\right) * \left(g^{\frac{P}{2}} - 1\right) = m * N$
- Setup a quantum superposition to represent all possible P’s for our g
  - We need to keep track of all P’s and all g^P ‘s
  - $|P, g^P >$
- Then superposition of how much bigger than m*N it is.
  - $|P, +r >$
- Note – superpositions allow us to simultaneously represent all possibilities

Let’s do it the Quantum Way!

- Problem – We can’t just measure to get the outcome because superpositions are a probability. We would be a random element of the superposition steps.
- We have to get all the bad answers to cancel out while in the quantum superposition to leave the right answer.
  - $|P, +1>$

Some relationships to help…

- Our guess, g, to some random power, x, is most likely some multiple of N plus some other number
  - $g^x = m * N + r$
- But something cool….
  - $g^{x+P} = m_1 * N + r$
  - $g^{x+2P} = m_2 * N + r$
- So….power P has a repeating property where the “r” stays the same
- We can take advantage of a superposition of all possible powers to take advantage of this!
- Those numbers in the superposition will repeat with a period of P.
  - Frequency -> $f = \frac{1}{P}$
  - If we find the frequency we break the encryption!

Quantum Fourier Transform!

- Best thing to find the frequency of things is a Fourier Transform
- We use the quantum version of the formula to make all the frequencies that don't exist to interfere and leave the single quantum state
  - $|\frac{1}{P}>$
- How does Quantum Fourier Transform work?
  - A single number inputted will represent a superpositions of numbers with weights - that looks like a sinewave with the frequency of the inputted number
  - When you put in a superposition of numbers you get out a superposition of superpositions where the sinewaves subtract and cancel out.
  - This then leaves you with the single quantum state $|\frac{1}{P}>$
- Now finally…as long as P is even
  - We take out guess, g, to compute $\left(g^{\frac{P}{2}} \pm 1\right)$
  - As long as $\left(g^{\frac{P}{2}} \pm 1\right)$ is not a multiple of N then that shares some factor with N
  - Then using Euclid's algorithm we can quickly find N -> N=a*b
  - We now have it decrypted!!

The reality of the risk

- We only have computers with enough qubits for unknown primes in the thousands (less than 50bits).
- Typical RSA encryption has around 2048 to 4096 bits of encryption

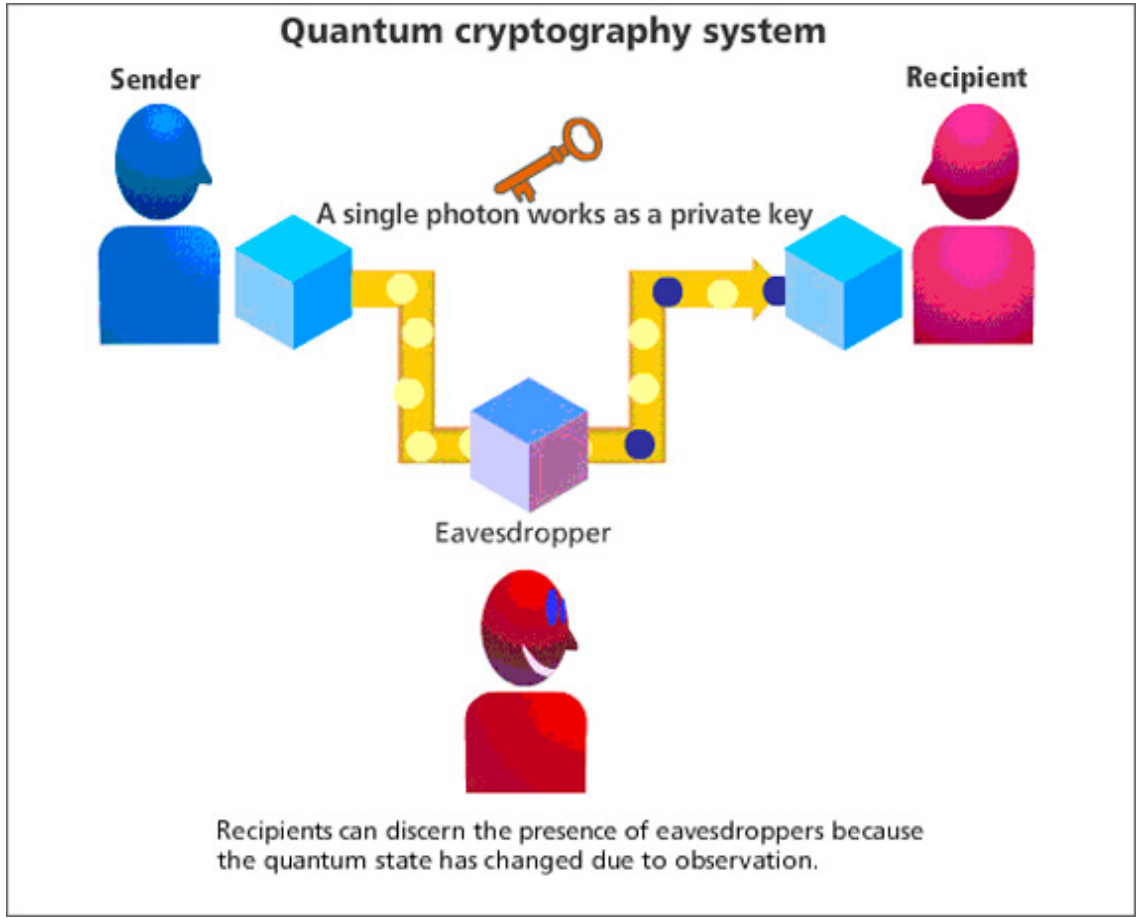
….Thus we don’t expect this attack to be viable for ~10 years.

Want to try this on your own?

- Signup for computing time on IBM Q
  - https://quantum-computing.ibm.com
- Run the implementation of shor's algorithm for quantum computers
  - https://github.com/ttlion/ShorAlgQiskit – python
- Remember it only works for small numbers (ex: 15) because the amount of qubits that quantum computer has but it's still cool!

Quantum Computing Can Be Used to Improve Cryptographic Systems!

Using Quantum Mechanics to Improve Cryptography

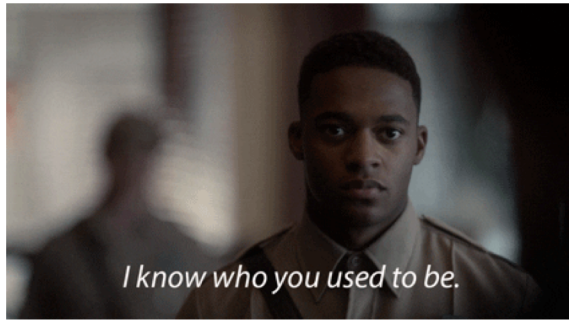


Post-Quantum Cryptography

Quantum Resistant Algorithms

Post-Quantum Cryptography

- We have some traditional cryptography methods still
  - Symmetric key quantum resistance
  - Hash-based cryptography
- And…we also have new more symmetric like algorithms
  - Lattice-based cryptography
  - Multivariate cryptography
  - Supersingular elliptic curve isogeny cryptography



Post-Quantum Cryptography

Symmetric key quantum resistance

- Provided one uses sufficiently large key sizes, the symmetric key cryptographic systems like AES are already resistant to attack by a quantum computer!
- As a general rule, for 128 bits of security in a symmetric-key-based system, one can safely use key sizes of 256 bits.

- Grover's algorithm allows brute-forcing a key on quantum computers but….
  - The time to brute force a n-bit key is speed up only to O($2^{\frac{n}{2}}$) time instead of O(2^n) with traditional computers
  - A speed up but not as significant as the asymmetric attacks!

Reminder – Pros vs Cons of Symmetric Crypto

- Pros
  - Fast and simple computations
  - Effective confidentiality
  - Strong algorithms that are normally only cracked through “brute force”
  - Good for bulk data
- Cons
  - Difficult to securely store and share the secret key
  - Often lacks authentication and data integrity
  - Data retention cases require key retention which can result in many secret
  - keys

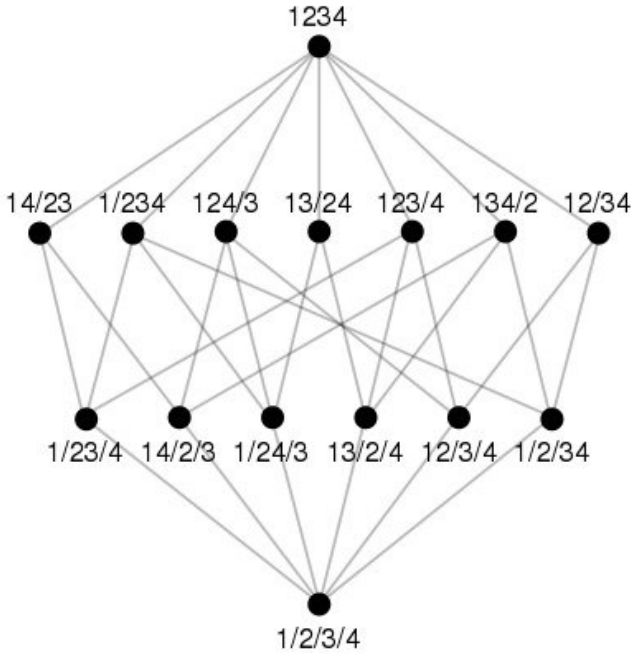
Post-Quantum Cryptography

Hash-based cryptography

- Single direction functions like traditional hash encryption
- Limited to digital signatures

Post-Quantum Cryptography

- Lattice-based cryptography
  - A partially ordered set of numbers in which every two elements have a unique upper bound and greatest lower bound.



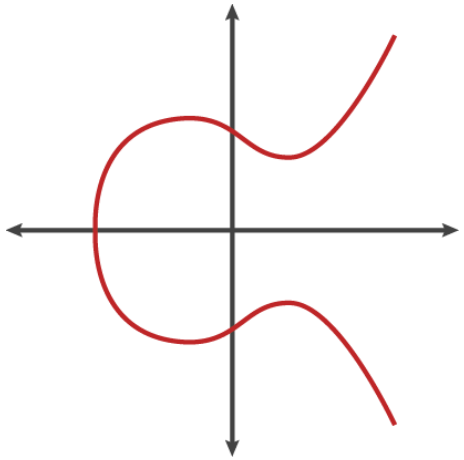
Post-Quantum Cryptography

- Multivariate cryptography
  - Asymmetric cryptography using multivariate polynomials (function such as $x^2 - 4x + 7$) over a finite field

Post-Quantum Cryptography

Supersingular elliptic curve isogeny cryptography

- Relies on the properties of supersingular elliptic curves and supersingular isogeny graphs to create a Diffie-Hellman replacement with forward secrecy.
- Supersingular elliptic curves form a certain class of elliptic curves over a field of characteristic $p > 0$ with unusually large endomorphism rings.
- An elliptic curve is a plane algebraic curve defined by an equation of the form



Post-Quantum Cryptography

- NIST is currently reviewing the new algorithms for standardization
  - https://csrc.nist.gov/Projects/Post-Quantum-Cryptography
  - Expected draft standards available in 2022-2024
- TLS 1.3 already supports quantum resistant algorithms that are draft standards by NIST
- Cloudflare's edge implementation of TLS 1.3 supports:
  - One based on lattices (NTRU-HRSS: big key, low CPU)
  - One based on isogenies (SIDH: small key, high CPU)
- Evolving into production use but…
  - A lot of work is being done still in this area
  - Some flaws may not have been discovered yet

The Risk - Cryptographic Recommendations

Algorithm Type	Data Protection for < 10 years	Data Protection for 10+ years
Symmetric Use cases	AES-256	AES-256
Asymmetric Use cases	RSA-4096	SIDH or NTRU-HRSS algorithms

Remember! Cryptography is a deterrent. It is not a guarantee that someone can't get it. Typically cryptography makes it not worth someone's time to try to break your encryption.

Think locks and bars on the windows/doors of a house.

In summary…

We are not doomed ☺

Questions?

Anthony.Kosednar@gmail.com

Some Useful Resources

- https://github.com/ttlion/ShorAlgQiskit
- https://www.gcppodcast.com/post/episode-123-post-quantum-cryptography-with-nick-sullivan-and-adam-langley/
- https://blog.cloudflare.com/disruptive-cryptography/
- http://www.ams.org/journals/notices/201605/rnoti-p508.pdf
- https://csrc.nist.gov/Projects/Post-Quantum-Cryptography/Workshops-and-Timeline
- http://hdc.amongbytes.com/post/201810-baby-steps-to-pq-https-server/
- http://hdc.amongbytes.com/post/20190130-pqc-round2/
- https://www.youtube.com/watch?v=q7v5NtV8v6I&feature=youtu.be
- https://www.youtube.com/watch?v=SCdaYAFx7hw
- https://twitter.com/_henrycase
- https://twitter.com/grittygrease/status/1086339192416743424
- https://twitter.com/grittygrease?lang=en
- https://blog.cloudflare.com/tls-1-3-explained-by-the-cloudflare-crypto-team-at-33c3/
- https://csrc.nist.gov/Projects/Post-Quantum-Cryptography/Round-1-Submissions
- https://blog.cloudflare.com/sidh-go/
- http://www.ams.org/journals/notices/201605/rnoti-p508.pdf