CSU
Hashdump Club
Presentation

Quantum Computing

Dr. Joseph Gersch, Assistant Professor, Dept of Computer Science

COLLEGE OF
NATURAL SCIENCES
COLORADO STATE UNIVERSITY

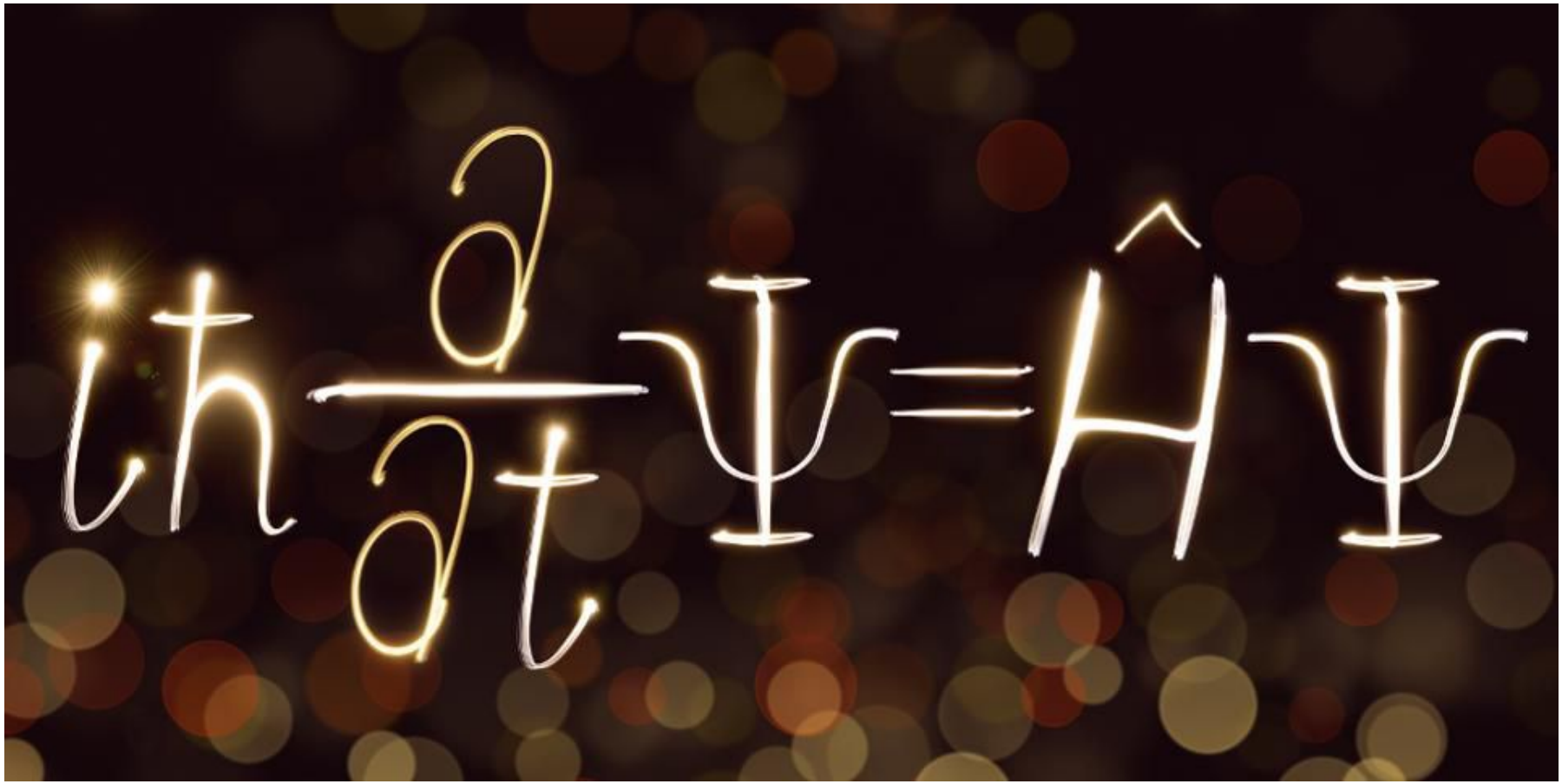
DISCOVERY BEGINS HERE

Topics

- The Quantum World
  - Quantum Physics
  - Quantum Superposition & Entanglement
  - Quantum Communication
  - Quantum Teleportation
  - Quantum Computing
- Quantum Code Breaking
  - Sound the Alarm: "Cryptogeddon"
- Quantum Cryptography
- Post-Quantum Encryption

COMPUTER SCIENCE
COLORADO STATE UNIVERSITY

Quantum Physics

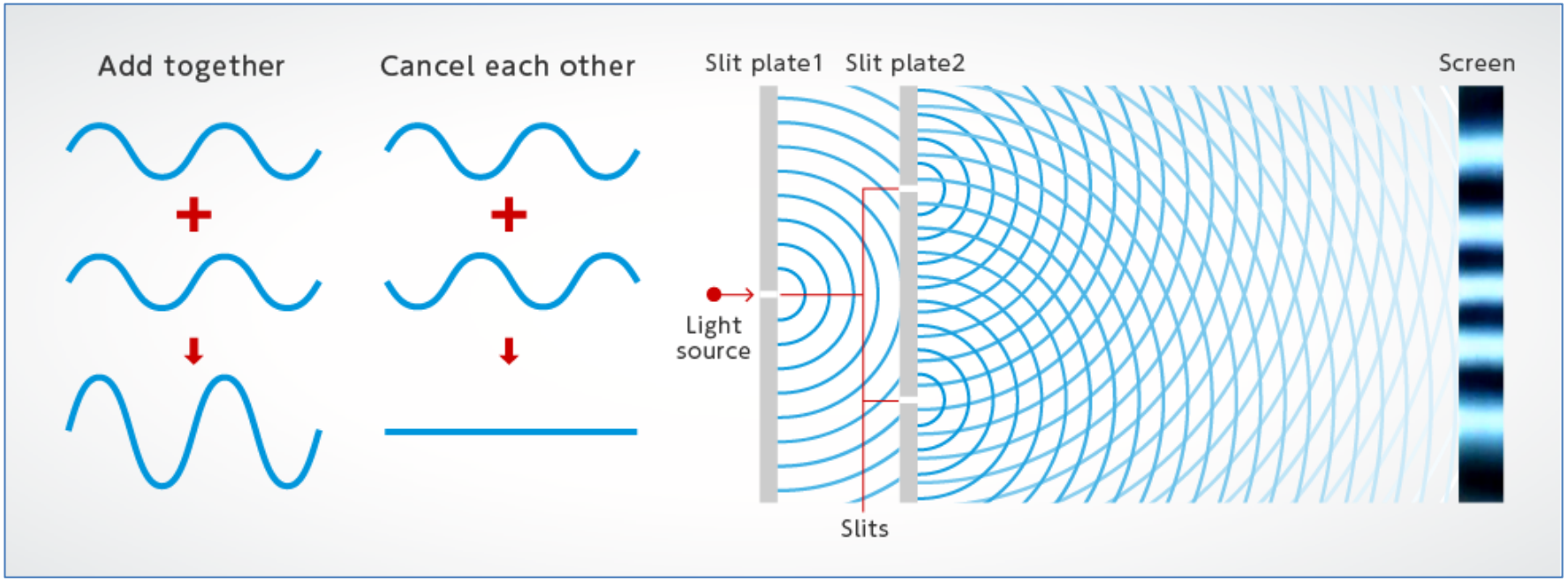


Quantum Physics seems weird because it runs counter to our everyday intuitions about how the world works.

- Newton's "deterministic" laws of motion don't apply
- Schroedinger's Wave Equation – derives probabilities
  - Schroedinger's cat!!!
- Heisenberg Uncertainty Principle
- Superposition of Waves → state superposition
- Collapse of the Wave Function due to "Observation"

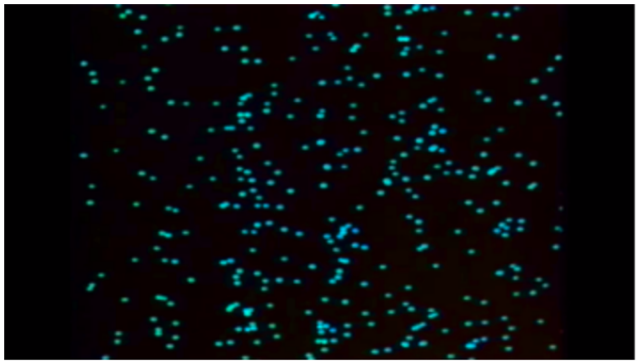
COMPUTER SCIENCE
COLORADO STATE UNIVERSITY

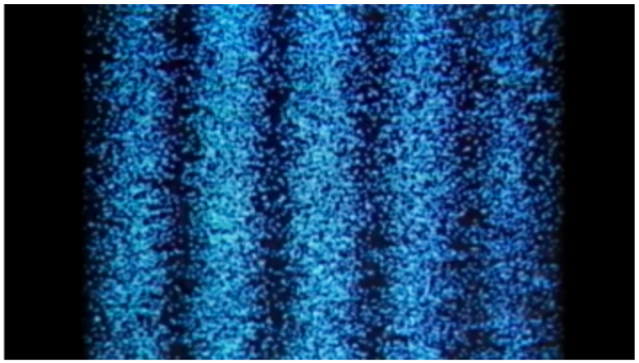
Wave-Particle Duality



COMPUTER SCIENCE
COLORADO STATE UNIVERSITY

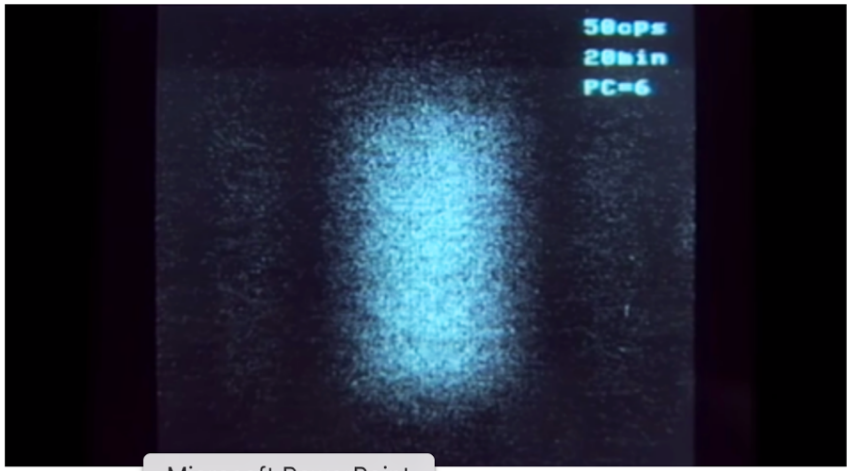
Wave-Particle Duality





When light weakened to an extreme brightness limit and projected on a screen is detected, it behaves like a particle as seen on the left. However when the recorded particle count increases, an interference fringe appears as seen on the right. One can see from this that light also behaves as a wave.

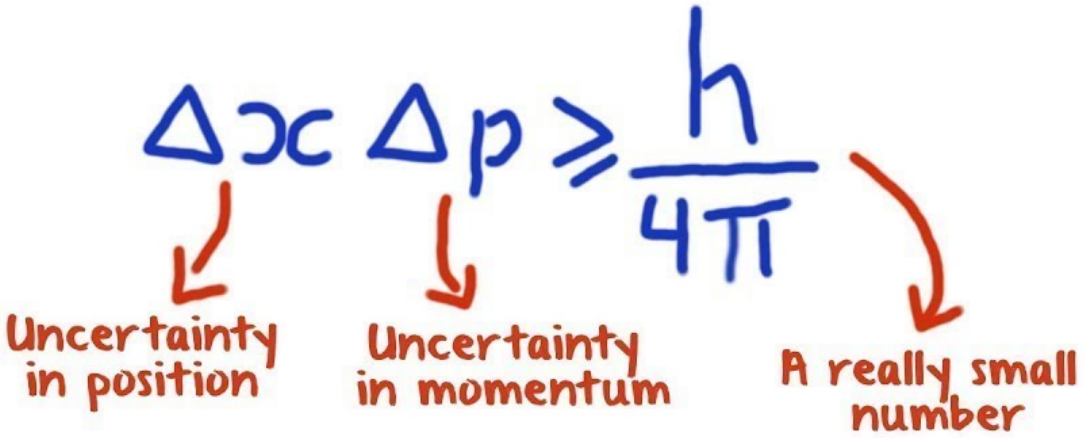
When one of the two slits in the experiment is closed so that one photon particle can only pass through the other slit, then no interference fringe appeared. This demonstrated that in the double-slit interference experiment, one photon particle simultaneously passed through the two slits and interfered by itself.



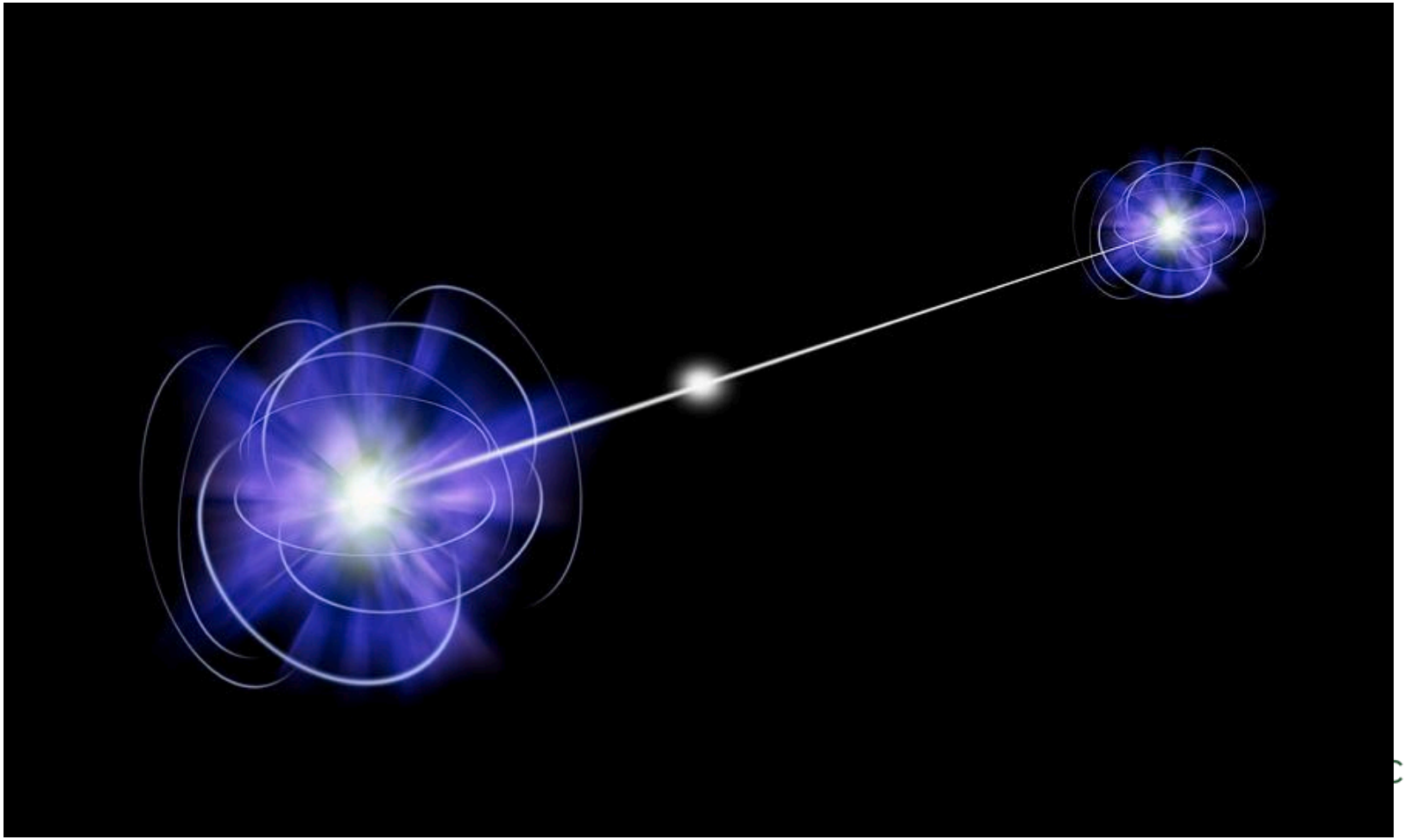
Microsoft PowerPoint

No interference fringe appears when one of the slits is closed.

Heisenberg's Uncertainty Principle



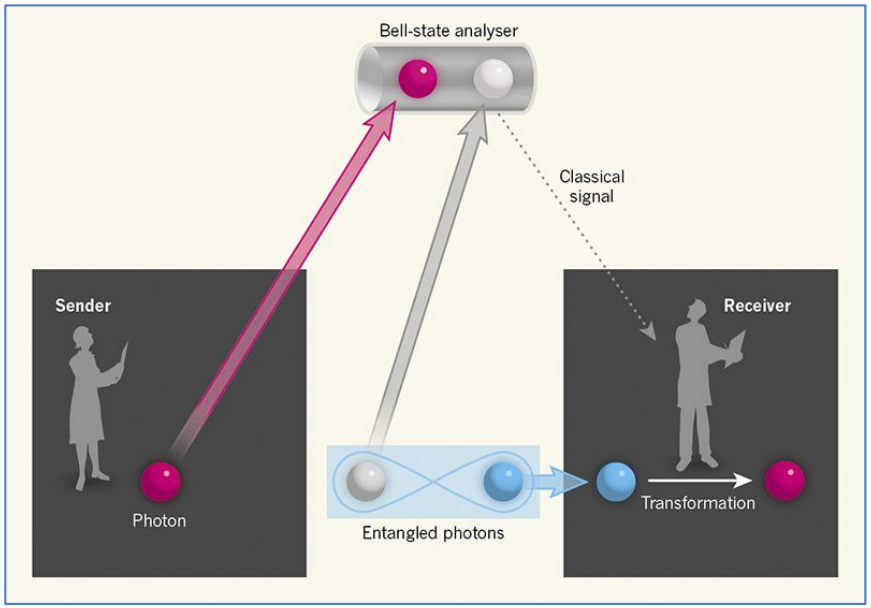
Quantum Entanglement



Quantum Teleportation

Teleportation techniques:

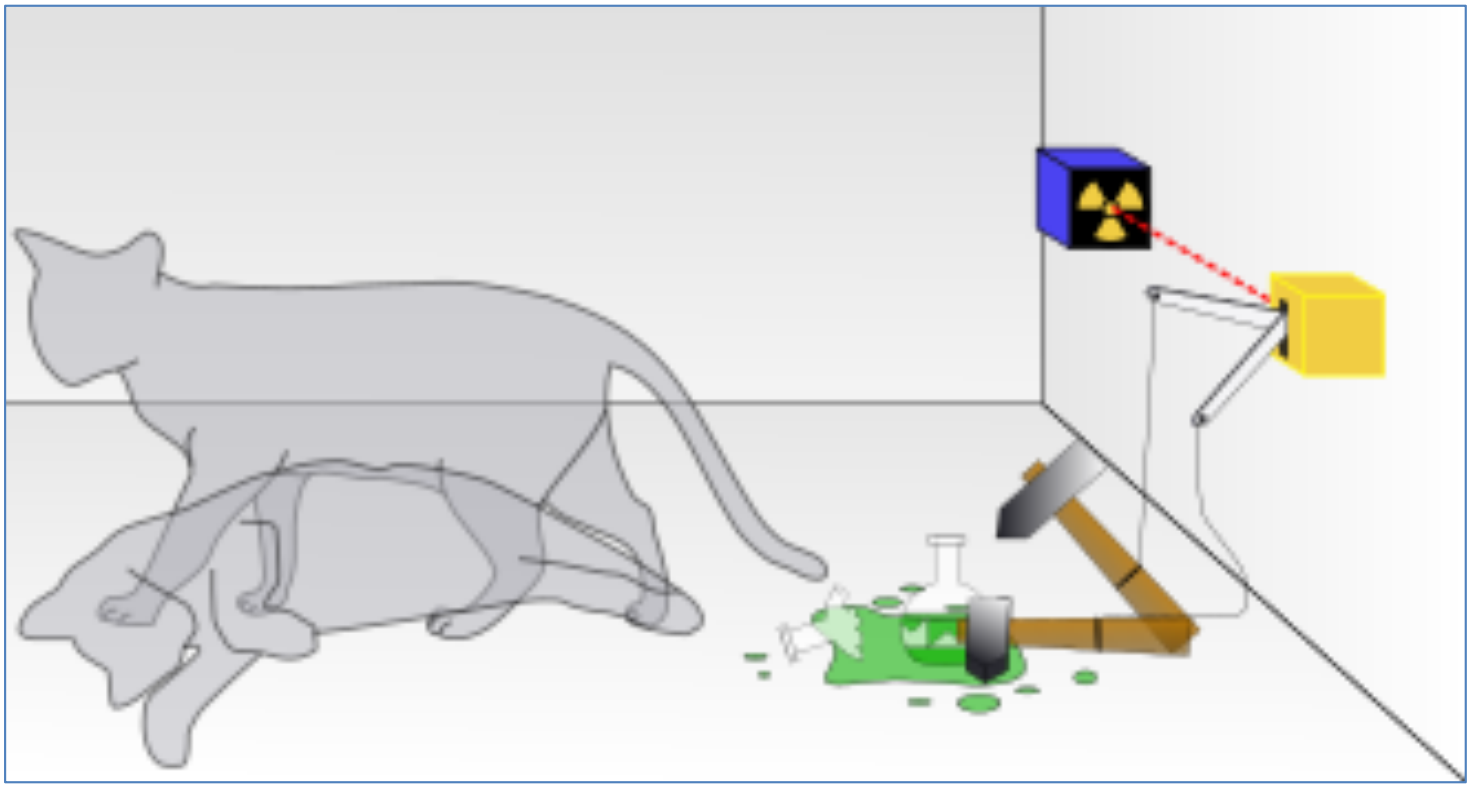
1. transport through a wormhole
2. star-trek disassemble-reassemble
3. quantum: build from info transfer



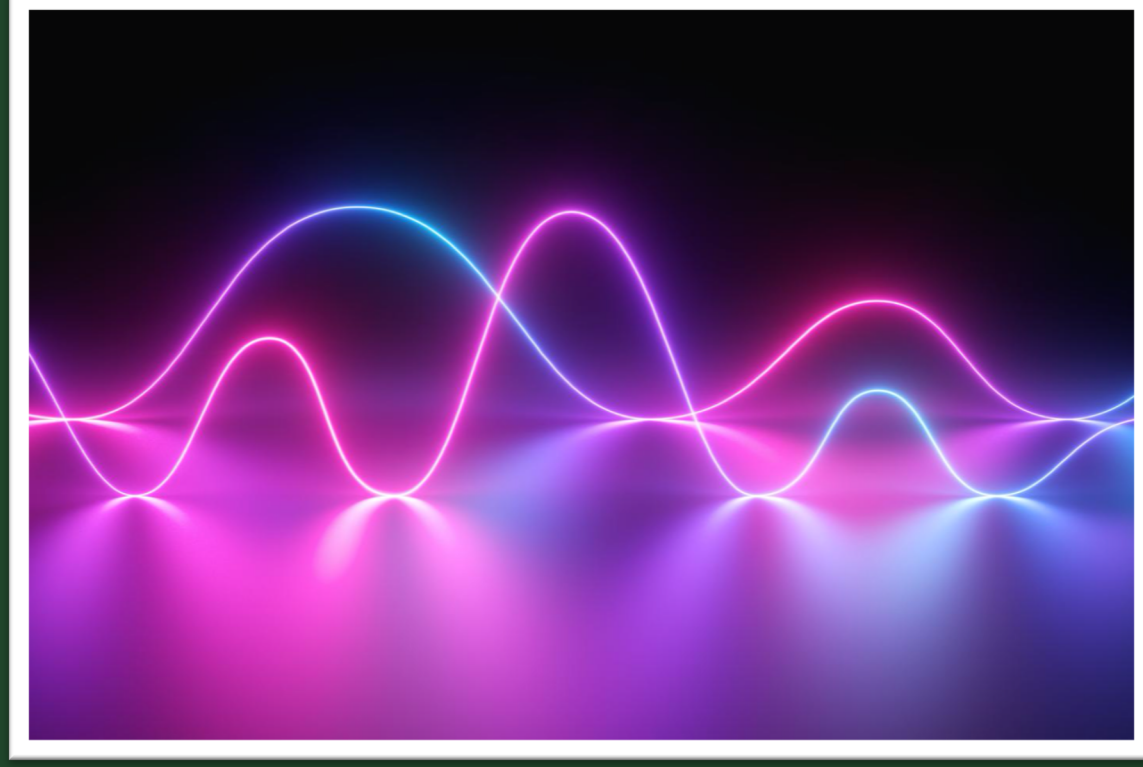
COMPUTER SCIENCE
COLORADO STATE UNIVERSITY

Quantum Superposition

Wanted, dead and alive: Schroedinger's Cat



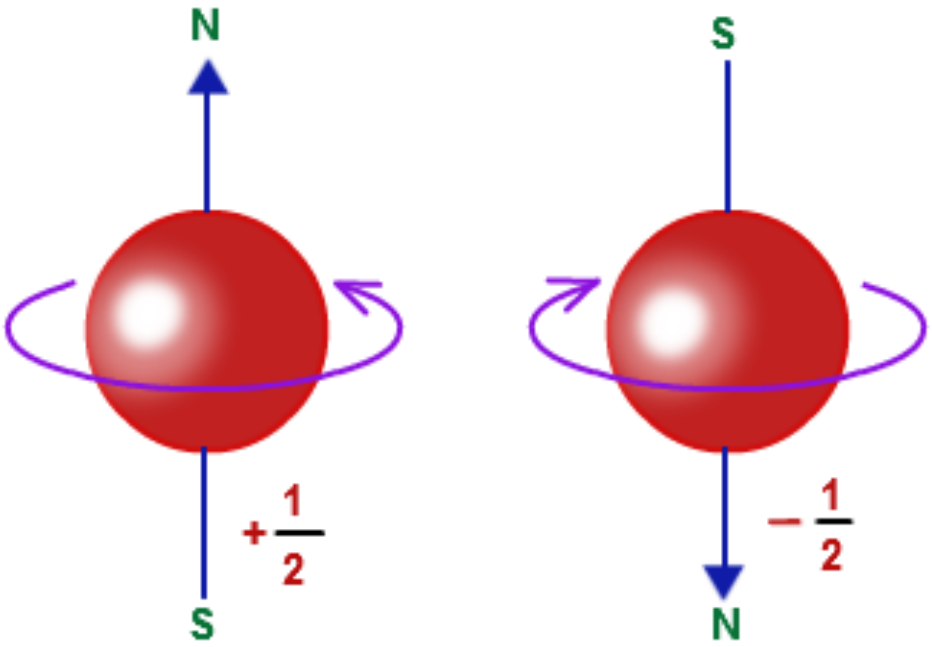
COMPUTER SCIENCE
COLORADO STATE UNIVERSITY



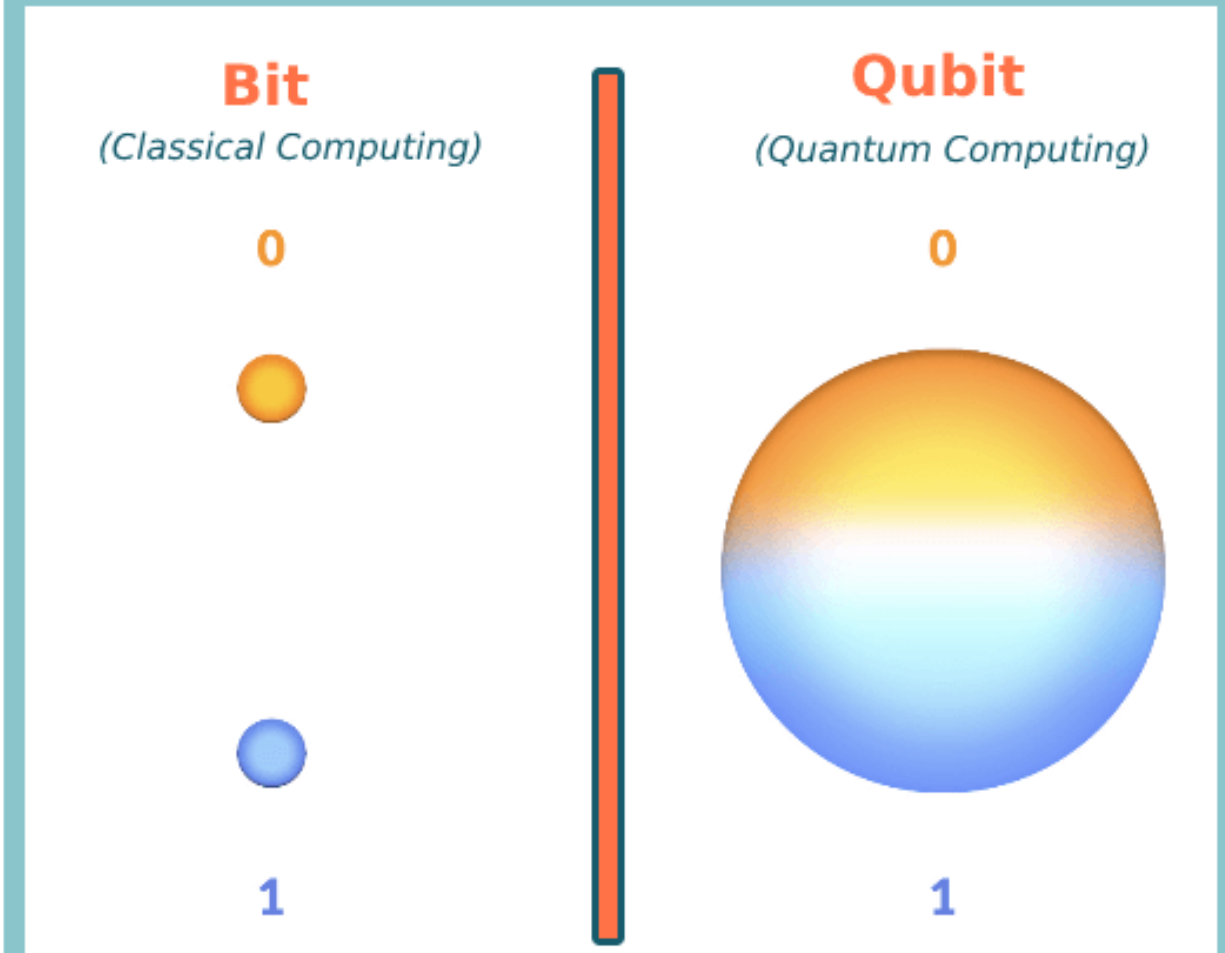
Quantum Computing

COMPUTER SCIENCE
COLORADO STATE UNIVERSITY

Quantum Superposition



The spin of an electron can be positive or negative depending on which direction it turns. But sometimes you can see that it has both values at the same time being the same electron and unable to divide, the only explanation is that it is in two places at the same time!



The classical computers take, process and store everything in only two states: 0 or 1. Keep in mind that it can only be 0 or 1 at a time, not both. This is exactly where Quantum computers differ from classical computers. Quantum computers use Qubits instead of Bits. Unlike the classical computers, the Quantum computers can run both 0 and 1 at the same time. As shown in the above picture, Bits exist either at the north pole or south pole, not both. Whereas the Qubits can exist anywhere on the sphere. This is

called ‘Superposition’.

Quantum Cryptography

CODE-BREAKING

COMPUTER SCIENCE
COLORADO STATE UNIVERSITY

Review: RSA encryption uses PRIME NUMBERS

- Can you find the prime factors of 33?
  - (you should have learned in the fifth grade....)

- Can you find the prime factors of
  6784578994572859509348579856944875935693048176987467
  4395930856709345738495704973948570394750394756398385
  7489670493248758945748978486788211283438038000979283
  7643846856785764987698664531?

- A BIG PRIME NUMBER (e.g. 100 digits) times another BIG PRIME is really really BIG. And practically impossible to factor to get the prime numbers back again.

Review: RSA Brute Force Attack

For N with 2048 you need primes p,q with 1024 bit each. There are 2^{1023} numbers with this length.

According to the prime number theorem, we get this:

$$\pi(2^{1024}) \approx \frac{2^{1024}}{ln(2^{1024})} \approx \frac{2^{1024}}{710} \approx 2^{1014.53}$$

Similarly, you can approximate the number $\pi(2^{1023})$ to almost exactly 1 bit less and subtract those primes (all the primes with lower length). This leaves still over 2^{1013} prime numbers of the according size.

However, the list of all prime numbers is way too huge and does not exist. This is beyond the capability of all computation power on earth for a couple of millenia.

A **VERY BASIC** explanation of qubits breaking codes

COMPUTER SCIENCE
COLORADO STATE UNIVERSITY

Shor's Algorithm

1. N = p * q (assume N = 35)
2. Guess a number 'a' smaller than N find GCD (Euclidean method), if =1 they are relatively prime (e.g. ; a = 8)
3. compute the period: r = a mod N (must be even) (r = 4)
4. rearrange: $(a^{r/2} - 1)(a^{r/2} + 1) = k*p*q$ $(8^2 - 1)(8^2 + 1) = k*35$
5. solve for p and q $p = GCD(8^2 - 1, N)$ $q=GCD(8^2 + 1,N)$

But step 3 is hard (exponentially long time); so use a quantum computer

https://www.youtube.com/watch?v=12Q3Mrh03Gk
https://www.youtube.com/watch?v=wUwZZaI5u0c&t=66s

Shor's Algorithm

Finding the period, r, is a global property of the quantum superposition of all the solutions. We can use the quantum fourier transform to find resonances to amplify the basic state of the answer we want and the incorrect answers deconstructively interfere.

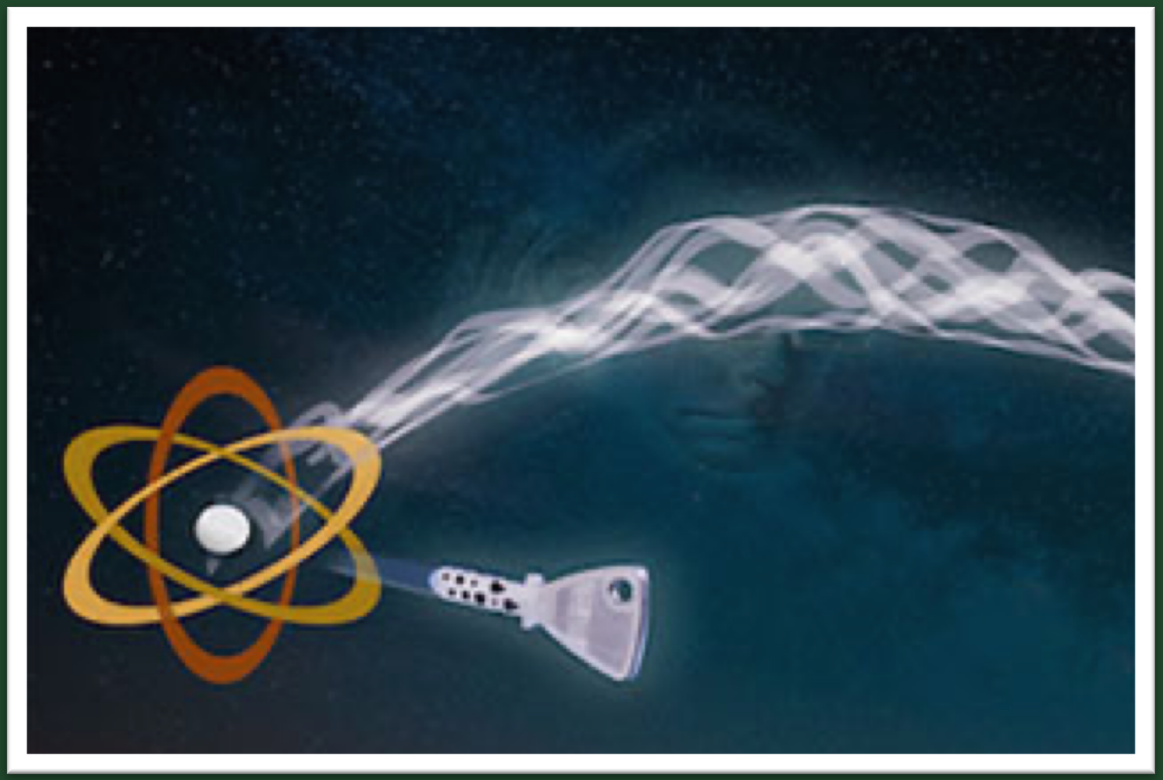
The highest probability quantum state will be observed and is likely the answer.

Shor's Factoring Algorithm - Peter Shor,, AT&T

n^3 time for n bits as opposed to exponential time

Grover Operator

Cryptographic Algorithm	Type	Purpose	Impact from large-scale quantum computer
AES	Symmetric key	Encryption	Larger key sizes needed
SHA-2, SHA-3	----------	Hash functions	Larger output needed
RSA	Public key	Signatures, key establishment	No longer secure
ECDSA, ECDH (Elliptic Curve Cryptography)	Public key	Signatures, key exchange	No longer secure
DSA (Finite Field Cryptography)	Public key	Signatures, key exchange	No longer secure



Quantum Cryptography

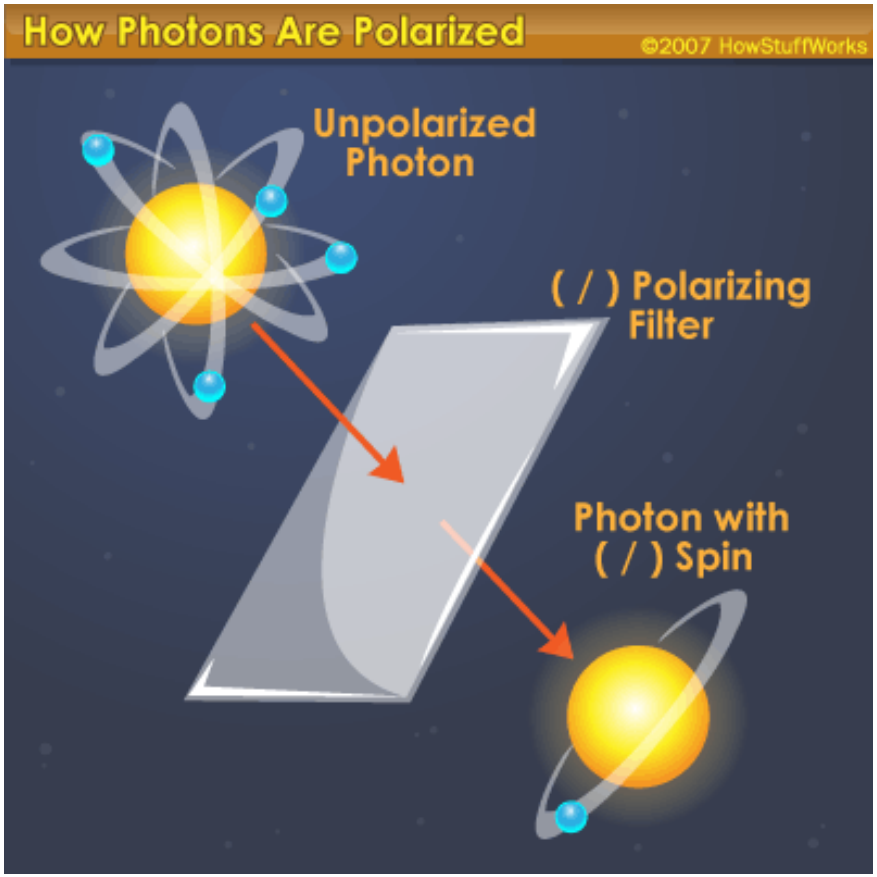
ENCRYPTION

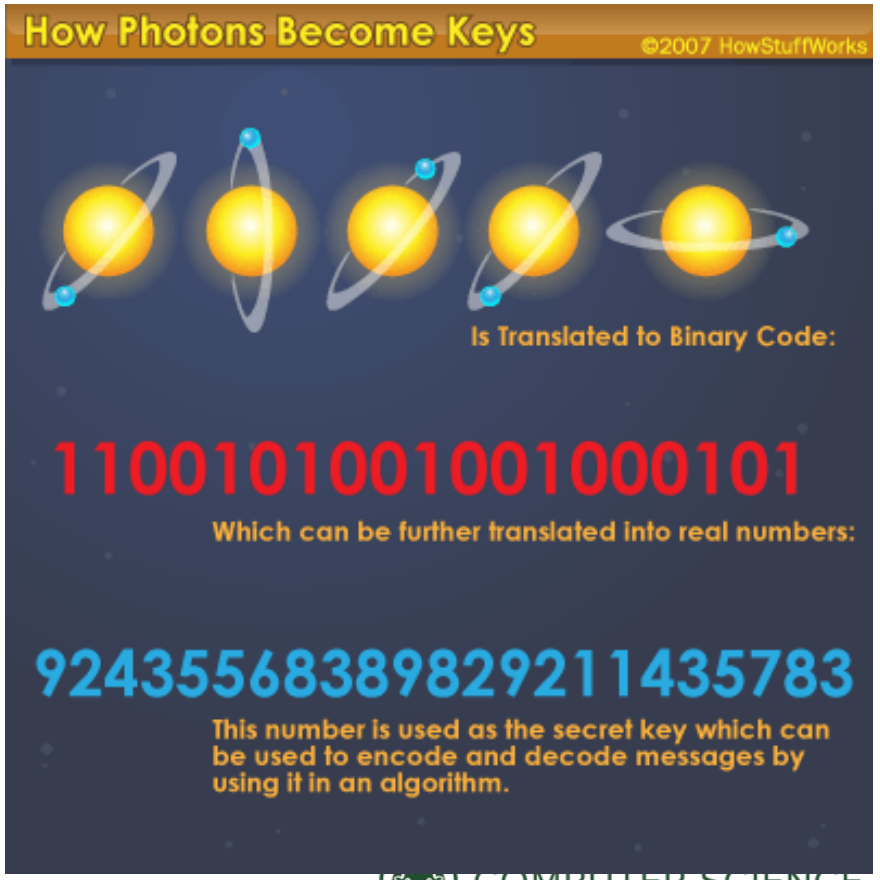
COMPUTER SCIENCE
COLORADO STATE UNIVERSITY

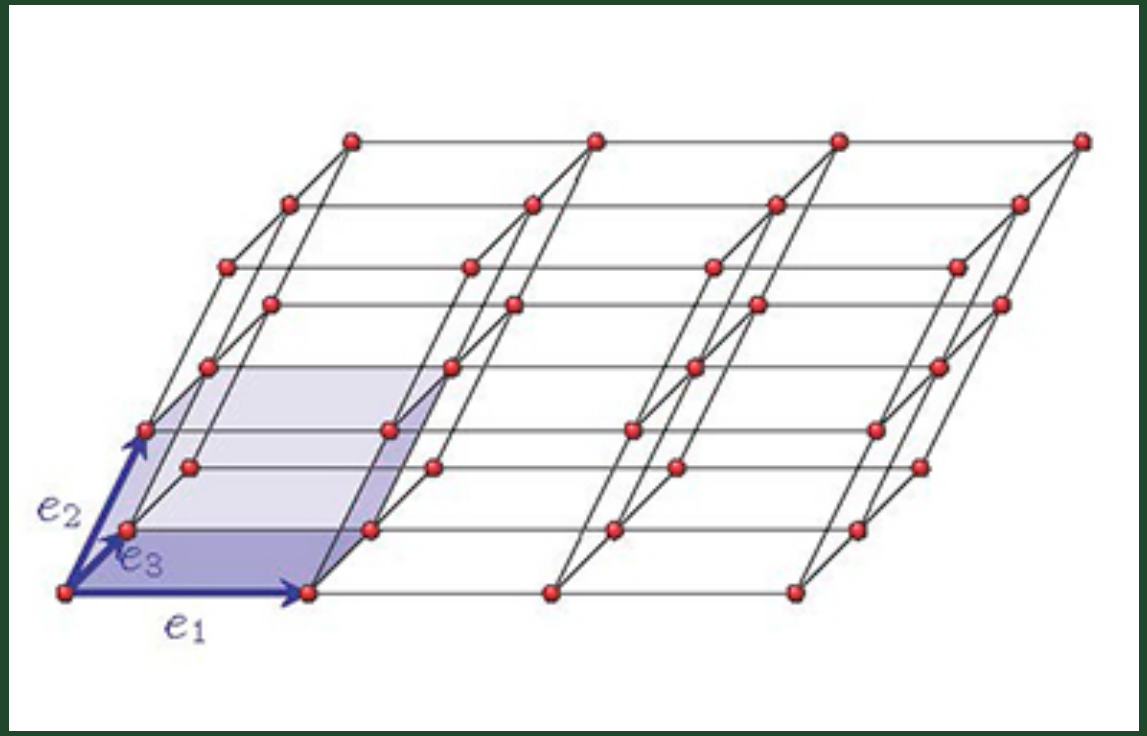
Secure Communications Using Quantum Key Distribution

Qubits can be used to distribute a key from sender to recipient without the possibility for the eavesdropper to obtain a copy without being discovered.

While QKD isn't in widespread use, it has been in commercial use in Europe since 2007, and in the US since 2010. For high-value transactions like inter-bank communication and election result transmission, the benefits of QKD are sometimes worth the cost.


How Photons Are Polarized
©2007 HowStuffWorks
Unpolarized Photon
(/) Polarizing Filter
Photon with (/) Spin


How Photons Become Keys
©2007 HowStuffWorks
Is Translated to Binary Code:
11001010010010001O1
Which can be further translated into real numbers:
924355683898292 11435783
This number is used as the secret key which can be used to encode and decode messages by using it in an algorithm.



Post-Quantum Encryption Algorithms

COMPUTER SCIENCE
COLORADO STATE UNIVERSITY

Post-Quantum Cryptography

Can’t use polynomial or exponential functions anymore…

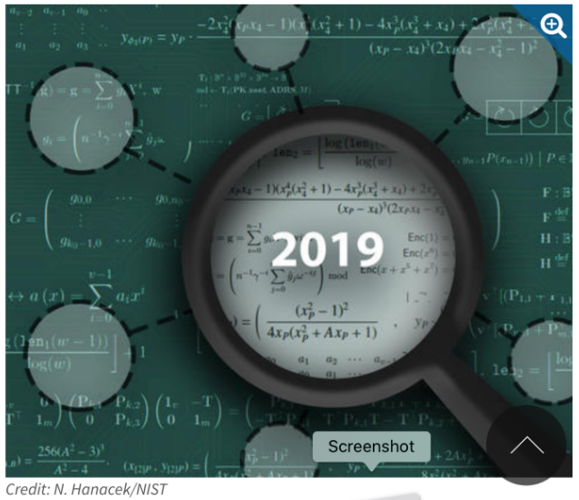
Recently, NIST initiated a process for standardizing post-quantum cryptography and is currently reviewing first-round submissions. The most promising of these submissions included cryptosystems based on lattices, isogenies, hash functions, and codes.

NIST Reveals 26 Algorithms Advancing to the Post-Quantum Crypto ‘Semifinals’

January 30, 2019

The field has narrowed in the race to protect sensitive electronic information from the threat of quantum computers, which one day could render many of our current encryption methods obsolete.

As the latest step in its program to develop effective defenses, the National Institute of Standards and



Credit: N. Hanacek/NIST

COMPUTER SCIENCE
COLORADO STATE UNIVERSITY

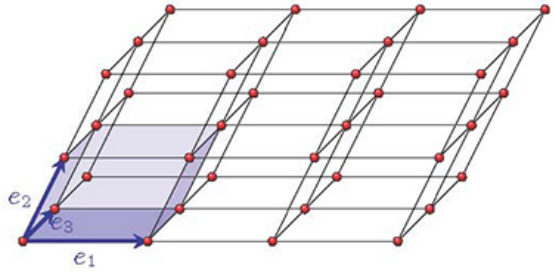
Algorithm Space

- Lattice based
  - Krystals Kyber
  - Frodo KEM
  - LAC
  - New Hope
  - NTRU/NTRU-prime
  - Round5
  - SABER
  - Three Bears
- Code based
  - Bike
  - Classic McElicee
  - HQC
  - LEDACrypt NTS-KEM
  - Rollo
  - RQC

LWE Lattices

… In the cryptographic literature this is known as the Learning With Errors problem (LWE).

The reason cryptography based on LWE gets called lattice-based cryptography is because the proof that LWE is hard relies on the fact that finding the shortest vector in something called a lattice is known to be NP-Hard. We won't go into the mathematics of lattices in much depth here, but one can think of lattices as a tiling of n-dimensional space



HW Accelerators and Crypto

Sanjay Rajopadhye & Anton Betten

- Crypto hardware accelerators are essential
  - best software-only systems can be easily broken by HW-enabled adversaries
- Hardware accelerators require huge NRE to deploy (Moore's Law consequences on chip fabrication costs)
  - Even when the algorithm is well known and fixed
- Challenge: post quantum crypto algorithms are in flux

COMPUTER SCIENCE
COLORADO STATE UNIVERSITY

Solution: Re-use HW while algorithms evolve

Two options:

- Instruction set programmable (ISP) hardware
  - Programmed using conventional software stack
  - Acceleration using domain specificity
    - GPGPU, VLIW
- Directly hardware programmable (DHP)
  - "Programmer" designs a chip, and implements it on reusable/reconfigurable platform (e.g., FPGA)
  - Each new design is a new circuit (but hardware can be reused/redeployed)

Reusable Hardware

ISP vs FPGAs pros/cons

- ISPs way easier to “program”
- FPGAs order of magnitude better in energy efficiency (cost metric subsumes speed)
- FPGAs still order of magnitude worse than ASICs in speed/energy (but ASICs not viable while algorithms in flux)

FPGA based reconfigurable logic is the only viable option for first-to-market solution while algorithms are evolving

Long-Term Vision

Simultaneous exploration of Math-CS-ECE space

- Automation: guided by tools
- Super compiler from Mathematical specification of algorithm to hardware
  - Automatic (design space exploration)
  - optimal mapping for multiple metrics: speed/energy/area

Recent News

COMPUTER SCIENCE
COLORADO STATE UNIVERSITY

Google says it's achieved quantum supremacy

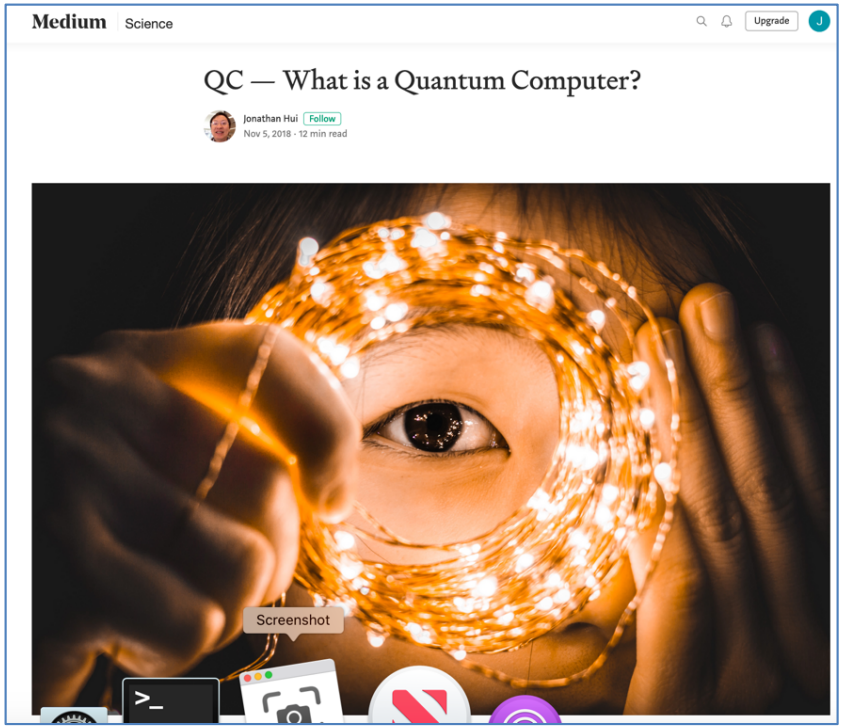
Google is standing by its claim that it's achieved quantum supremacy. Why is that a big deal? Google's paper explains how its 53-bit quantum computer—named Sycamore—took just 200 seconds to perform a calculation that would have taken the world's fastest supercomputer ***10,000 years***! While no practical use has come from this amazing feat, the fact that it's possible shows the potential QC has for everyday issues, if developers are prepared to start using it....

Google Claims Achievement of Quantum Supremacy, But IBM Issues Rebuttal

To learn more:

- see youtube videos listed earlier
- and this 10-part article on MEDIUM at

https://medium.com/@jonathan_hui/qc-what-is-a-quantum-computer-222edc3a887d



COMPUTER SCIENCE
COLORADO STATE UNIVERSITY

Quantum is real

- When?
- Impact on Computing
- Impact on Security

COMPUTER SCIENCE
COLORADO STATE UNIVERSITY