Quantum Computation and Quantum Cryptography: PH 441

INTRODUCTION

PROF. AMARENDRA KUMAR SARMA, IIT GUWAHATI, PHYSICS DEPARTMENT

OUTLINE

- COURSE STRUCTURE
- EVALUATION SCHEME
- STUDENT STATISTICS
- LECTURE STRATEGY

- QUANTUM PHYSICS AS A TOOL IN TECHNOLOGY

- QUANTUM SUPREMACY

- *BASIC QUANTUM PHYSICS CONCEPTS-A QUICK LOOK*

- CLASSICAL VS QUANTUM COMPUTER

- ROUTES TO QUANTUM COMPUTER

Course Structure

- Basic QM: (2-level atomic systems; Bloch Sphere representation)
- Quantum Gates
- Quantum Circuits
- Quantum Entanglement
- Quantum Teleportation
- Measurement
- **Quantum Algorithms**
- Quantum Error Correction
- Classical Information Theory
- Quantum Cryptography
- Physical Realization of Quantum Computer

Evaluation Schemes

- Continuous evaluation (60%)
  - ✓ Short Quiz
  - ✓ Assignment
- End Semester Examination (40%)

STUDENT STATISTICS

Number of registered students till date

- Computer Science and Engineering: 04?
- Engineering Physics: 12?
- Chemical Science and Technology: 01?
- Electronics and Electrical Engineering: 08?
- Biotechnology: 03?
- Civil Engineering: 04?

? *More students are willing to register*

LECTURE STRATEGY

- Class-Time
  - Monday 12 pm
  - Tuesday 12 pm
  - Friday 11 am
- Classes using Microsoft Team!
- *If unable to take classes, recorded Lectures will be uploaded on my YouTube channel!*
- Lectures/reading materials will be uploaded in the course webpage, time-to-time.

VERY IMPORTANT NOTICE!

I may upload recorded Lectures on YouTube and Come for discussions over Microsoft Team once a week. It will help students having network problems. I shall announce it after a discussion with all the students.

Quantum Mechanics is a strange animal!

Quantum Mechanics is bizarre!

"Anyone who thinks he can contemplate quantum mechanics without getting dizzy hasn't properly understood it."
-Niels Bohr

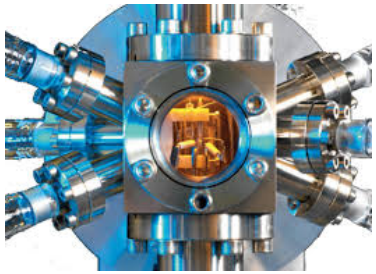
"Anyone who thinks they know quantum mechanics doesn't"
-Richard Feynman

"I don't like it, and I'm sorry I ever had anything to do with it."-Erwin Schrodinger

Yet, Quantum Mechanics is Useful!

Quantum Physics is the foundation of many modern technologies.

The first generation of Quantum technology



Lasers
Atomic clocks
Satellite positioning (GPS)
Entire field of Electronics
Computers
Internet
Mobile communications

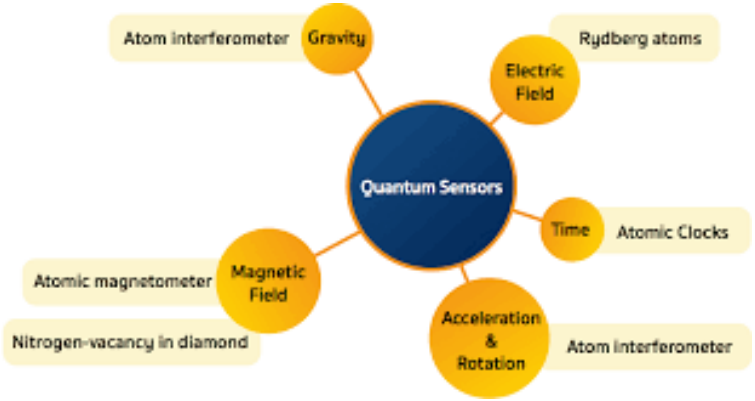
Second generation of Quantum Technology- dawn of a new era!

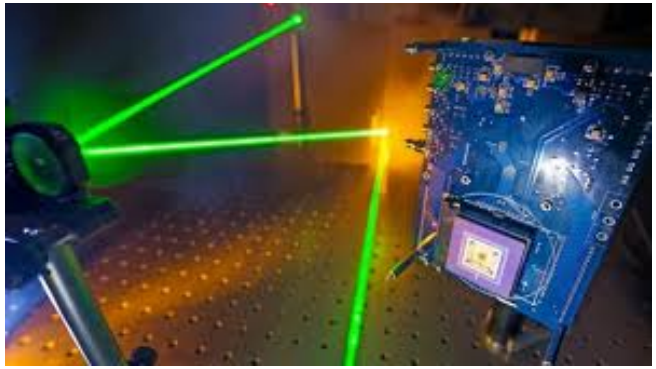
Data encryption using **quantum cryptography**. In April 2004, the first **bank transfer** using a protocol with quantum cryptography was made in Vienna

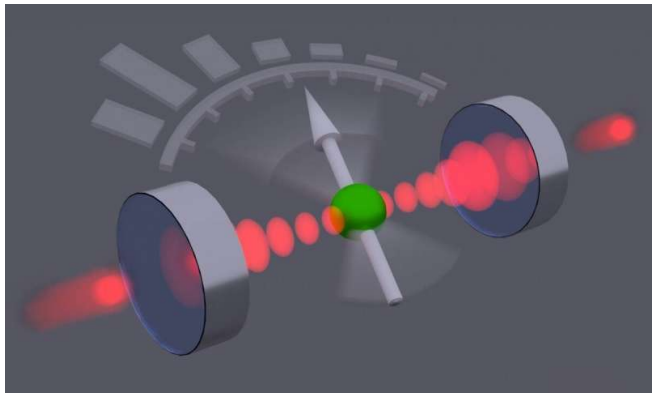
Switzerland used quantum cryptography for the first time in its National Council elections in 2007 to secure networks for vote counting against tampering.

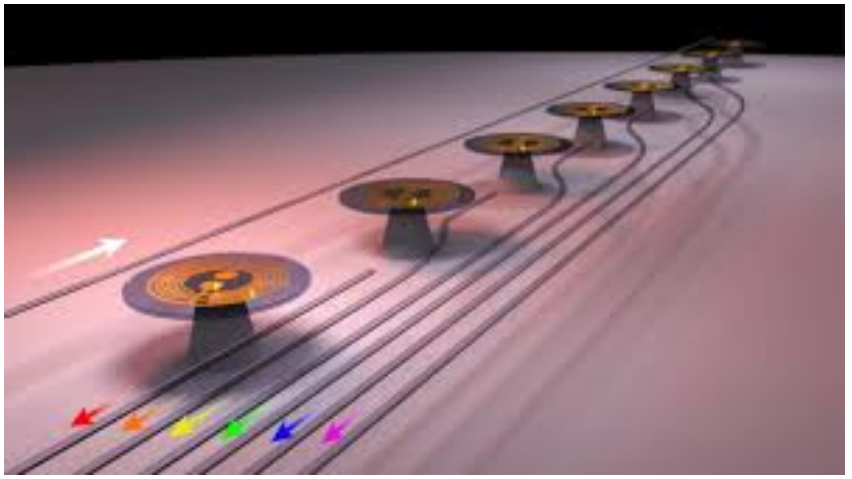
Quantum Sensors

- Changes in the environment, such as a rise in sea level due to climate change, could be monitored with great accuracy using quantum sensors.
- capable of delivering more precise measurements of gravity in the Earth's magnetic field and rotation
- Improving Cancer treatment









TheScientist
EXPLORING LIFE, INSPIRING INNOVATION

Quantum Biology May Help Solve Some of Life's Greatest Mysteries

From the remarkable speed of enzyme-catalyzed reactions to the workings of the human brain, numerous biological puzzles are now being explored for evidence of quantum effects.

Major Focus!

QUANTUM COMPUTERS!

Nature isn't classical, dammit,
and if you want to make a simulation of nature,
you'd better make it quantum mechanical.

Richard Feynman

FANTASY!

What if we could do chemistry inside a computer instead of in a test tube or beaker in the laboratory? What if running a new experiment was as simple as running an app and having it complete in a few seconds?

For this to really work, we would want it to happen with full fidelity. The atoms and molecules as modeled in the computer should behave exactly like they do in the test tube. The chemical reactions that happen in the physical world would have precise computational analogs. We would need a fully faithful simulation.

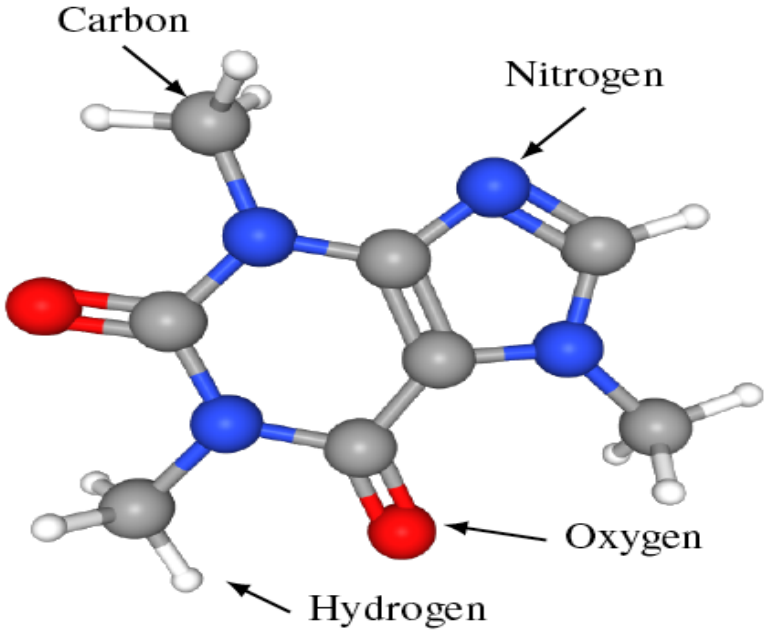
IF THE FANTASY TURNS INTO A REALITY!

"If we could do this at scale, we might be able to compute the molecules we want and need. These might be for new materials for shampoos or even alloys for cars and airplanes. Perhaps we could more efficiently discover medicines that are customized to your exact physiology. Maybe we could get better insight into how proteins fold, thereby understanding their function, and possibly creating custom enzymes to positively change our body chemistry."

How reasonable these fantasies are?

(*After all, fantasies are always fantasies!* ☺)

We have massive supercomputers that can run all kinds of simulations. Can we model molecules in the above ways today?

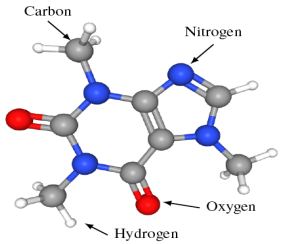


Caffeine

$C_8H_{10}N_4O_2$ – 1,3,7-Trimethylxanthine

An 8 ounce cup of coffee contains approximately 95 mg of caffeine, and this translates to roughly 2.95×10^{20} molecules

Can we model caffeine exactly in a computer? We don't have to model the huge number of caffeine molecules in a cup of coffee, but can we fully represent a single molecule at a single instant?



Caffeine is a small molecule and contains protons, neutrons, and electrons. In particular, if we just look at the energy configuration that determines the structure of the molecule and the bonds that hold it all together, the amount of information to describe this is staggering. In particular, the number of bits, the 0s and 1s, needed is approximately 10^{48}. This is comparable to 1% to 10% of the number of atoms on the Earth!

This is just one molecule! Yet somehow nature manages to deal quite effectively with all this information. It handles the single caffeine molecule, to all those in your coffee, tea, or soft drink, to every other molecule that makes up you and the world around you.

How does it do this?

We don't know!

In the traditional sense, we have no hope of providing storage to hold this much of information. Our dream of exact representation appears to be dashed. This is what Richard Feynman meant!

THERE IS HOPE!

Bring Qubits aka Quantum Computer!

160 qubits (quantum bits) could hold $2^{160} \approx 1.46 \times 10^{48}$ bits while the qubits were involved in computation.

In the classical case, we will never fully represent the caffeine molecule. In the future, with enough very high quality qubits in a powerful enough quantum computing system, we may be able to perform chemistry in a computer.

NEWS · 23 OCTOBER 2019

Hello quantum world! Google publishes landmark quantum supremacy claim

The company says that its quantum computer is the first to perform a calculation that would be practically impossible for a classical machine.

Article

Quantum supremacy using a programmable superconducting processor

https://doi.org/10.1038/s41586-019-1666-5

Received: 22 July 2019

Accepted: 20 September 2019

Published online: 23 October 2019

Frank Arute[1], Kunal Arya[1], Ryan Babbush[1], Dave Bacon[1], Joseph C. Bardin[1,2], Rami Barends[1], Rupak Biswas[3], Sergio Boixo[1], Fernando G. S. L. Brandao[1,4], David A. Buell[1], Brian Burkett[1], Yu Chen[1], Zijun Chen[1], Ben Chiaro[5], Roberto Collins[1], William Courtney[1], Andrew Dunsworth[1], Edward Farhi[1], Brooks Foxen[1,5], Austin Fowler[1], Craig Gidney[1], Marissa Giustina[1], Rob Graff[1], Keith Guerin[1], Steve Habegger[1], Matthew P. Harrigan[1], Michael J. Hartmann[1,6], Alan Ho[1], Markus Hoffmann[1], Trent Huang[1], Travis S. Humble[7], Sergei V. Isakov[1], Evan Jeffrey[1], Zhang Jiang[1], Dvir Kafri[1], Kostyantyn Kechedzhi[1], Julian Kelly[1], Paul V. Klimov[1], Sergey Knysh[1], Alexander Korotkov[1,8], Fedor Kostritsa[1], David Landhuis[1], Mike Lindmark[1], Erik Lucero[1], Dmitry Lyakh[9], Salvatore Mandrà[2,10], Jarrod R. McClean[1], Matthew McEwen[5], Anthony Megrant[1], Xiao Mi[1], Kristel Michielsen[11,12], Masoud Mohseni[1], Josh Mutus[1], Ofer Naaman[1], Matthew Neeley[1], Charles Neill[1], Murphy Yuezhen Niu[1], Eric Ostby[1], Andre Petukhov[1], John C. Platt[1], Chris Quintana[1], Eleanor G. Rieffel[3], Pedram Roushan[1], Nicholas C. Rubin[1], Daniel Sank[1], Kevin J. Satzinger[1], Vadim Smelyanskiy[1], Kevin J. Sung[13,2], Matthew D. Trevithick[1], Amit Vainsencher[1], Benjamin Villalonga[1,14], Theodore White[1], Z. Jamie Yao[1], Ping Yeh[1], Adam Zalcman[1], Hartmut Neven[1] & John M. Martinis[1,5]✉

The promise of quantum computers is that certain computational tasks might be executed exponentially faster on a quantum processor than on a classical processor[1]. A fundamental challenge is to build a high-fidelity processor capable of running quantum algorithms in an exponentially large computational space. Here we report the use of a processor with programmable superconducting qubits[2–7] to create quantum states on 53 qubits, corresponding to a computational state-space of dimension 2^{53} (about 10^{16}). Measurements from repeated experiments sample the resulting probability distribution, which we verify using classical simulations. Our Sycamore processor take about 200 seconds to sample one instance of a quantum circuit a million times—our benchmarks currently indicate that the equivalent task for a state-of-the-art classical supercomputer would take approximately 10,000 years. This dramatic increase in speed compared to all known classical algorithms is an experimental realization of quantum supremacy[8–14] for this specific computational task, heralding a much-anticipated computing paradigm.

“Today we published the results of this quantum supremacy experiment in the Nature article, “Quantum Supremacy Using a Programmable Superconducting Processor”. We developed a new 54-qubit processor, named “Sycamore”, that is comprised of fast, high-fidelity quantum logic gates, in order to perform the benchmark testing. Our machine performed the target computation in 200 seconds, and from measurements in our experiment we determined that it would take the world’s fastest supercomputer 10,000 years to produce a similar output.”

John Martinis, Chief Scientist Quantum Hardware and Sergio Boixo, Chief Scientist Quantum Computing Theory, Google AI Quantum

Google claims quantum computing ‘supremacy’ in major milestone

By **Christopher Carbone** | **Fox News**

THE HINDU

TECHNOLOGY

Google claims quantum computing breakthrough; others say hold on a qubit

REUTERS

BERLIN, OCTOBER 23, 2019 21:29 IST
UPDATED: OCTOBER 23, 2019 22:02 IST

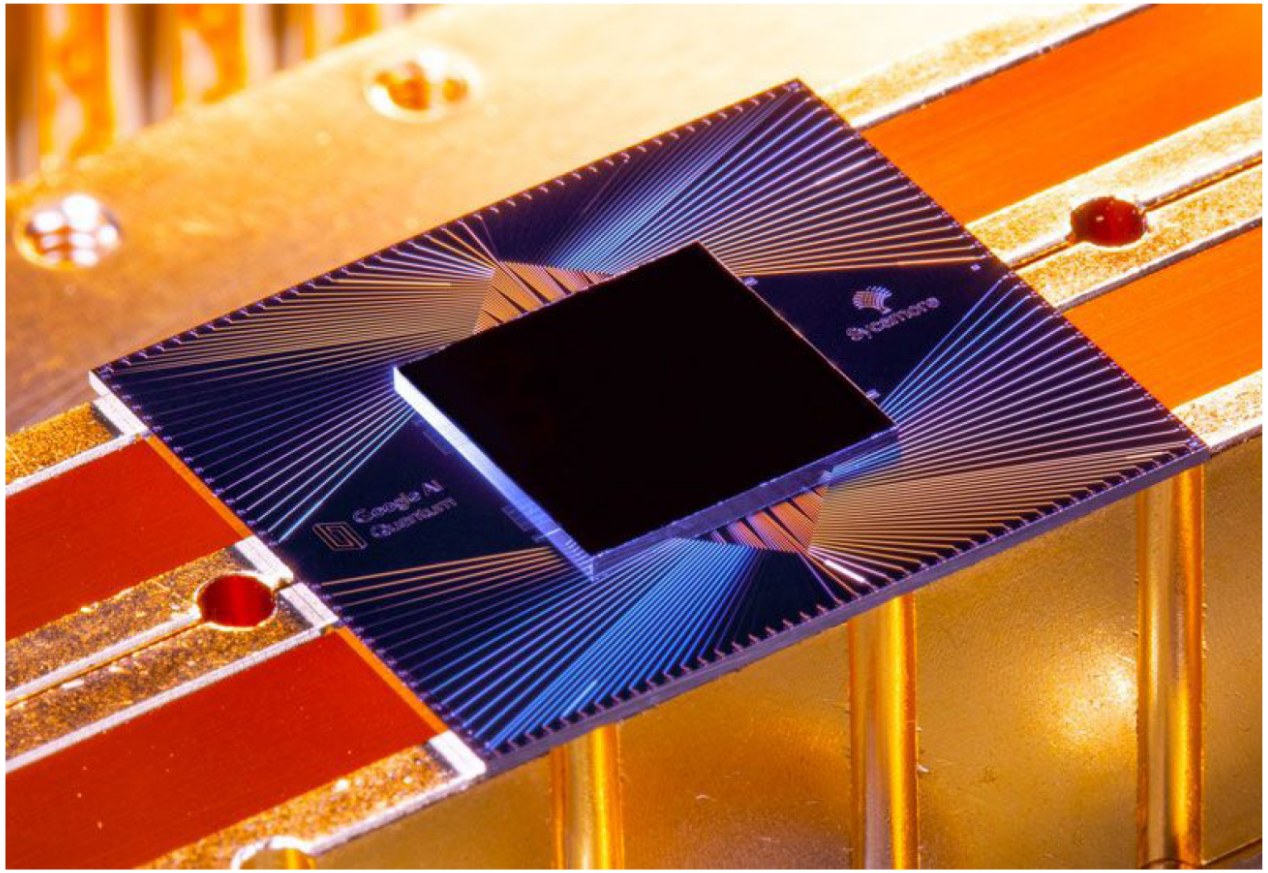
Quantum computers overtake classical supercomputers, says Google; CEO Sundar Pichai compares the achievement to building the first rocket to leave the Earth's atmosphere; IBM says Google hypes achievement, risks misleading public.

ience journal *Nature*, after weeks of controversy following the leak of a draft, over whether Google's
mputer scientists have for decades sought to harness the behaviour of sub-atomic particles that
n simultaneously exist in different states — in contrast to the "real" world that people perceive

Penn Today

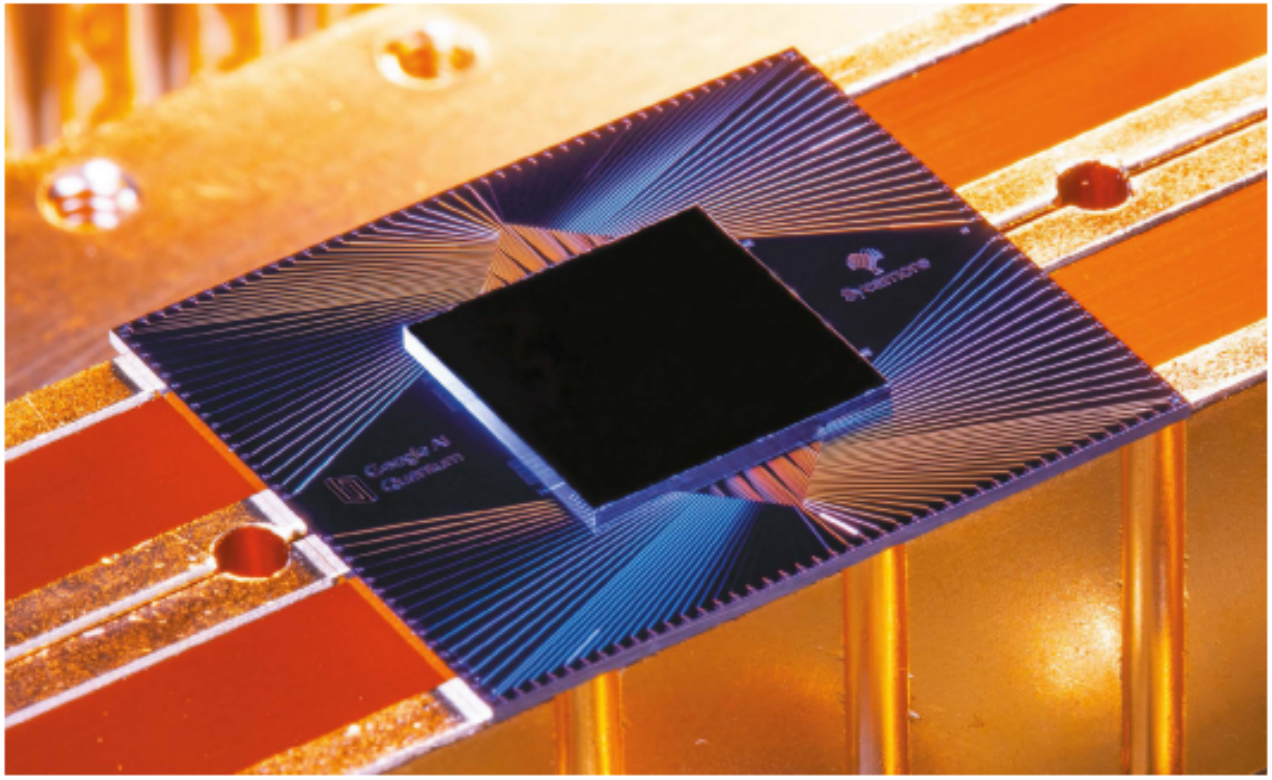
SCIENCE & TECHNOLOGY

Google's claims of quantum supremacy: Groundbreaking, overhyped, or both?



The Sycamore chip, with 54 qubits each made of loops of superconducting wires, was the device behind Google's landmark paper describing the first-ever fully programmable quantum computer. (Image: Erik Lucero)

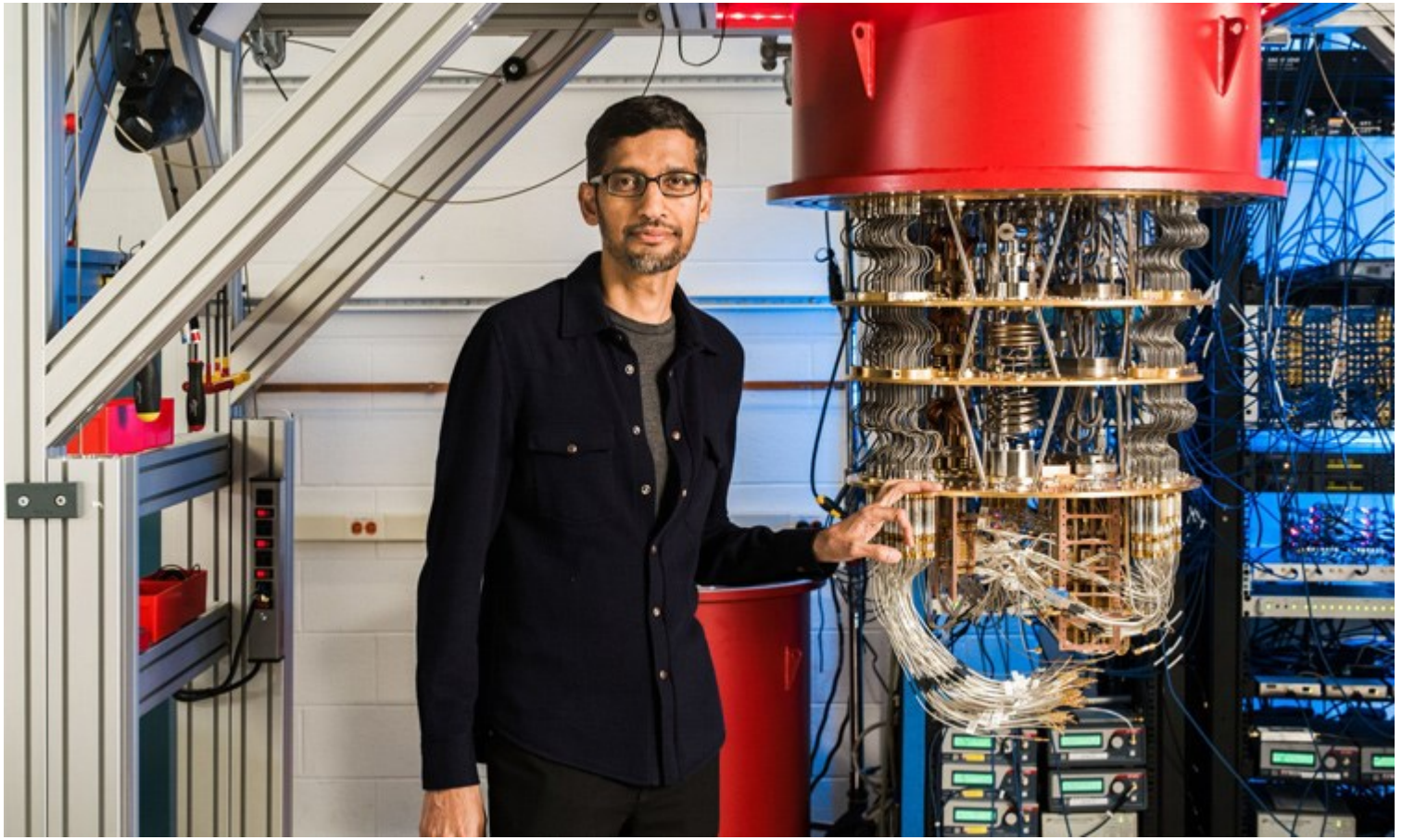
News in focus



The Sycamore chip is composed of 54 qubits, each made of superconducting loops.

GOOGLE PUBLISHES LANDMARK QUANTUM SUPREMACY CLAIM

The company says that its quantum computer is the first to perform a calculation that would be practically impossible for a classical machine.



Google CEO Sundar Pichai next to the company's quantum computer.

WHAT IS QUANTUM SUPREMACY?

Oversimplifying, quantum supremacy is the ability of a quantum computer to solve a computational problem very quickly which cannot be solved in a reasonable amount of time on any classical computer, even the largest supercomputers.

*In addition quantum supremacy generally means that a quantum solution offers an exponential speedup compared to a classical solution, meaning that far fewer quantum resources are needed to process a given input than a classical solution would require as the size of the input grows. **

* ***Jack Krupansky***

WHAT IS QUANTUM SUPREMACY?

Given the task of finding a pattern in a seemingly random series of numbers, Google's quantum computer produced an answer in 3 minutes and 20 seconds. It estimates that the Summit supercomputer at the Oak Ridge National Laboratory in Tennessee would take 10,000 years to complete the task.

BASIC QUANTUM MECHANICS: A RAPID LOOK!

Quantization

In classical physics, the energy in a beam of light can take on a continuous range of values.

For example, a 100 W light bulb.

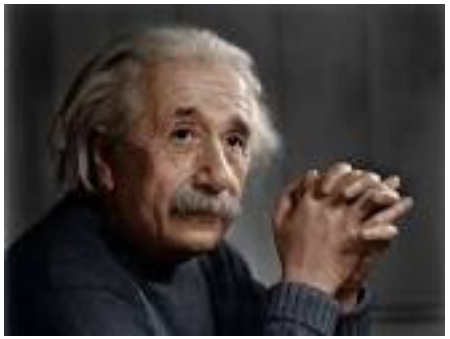
In quantum mechanics, the energy in a beam of light is quantized:

$$E = nh\nu$$

n is an integer

h = Planck's constant

ν = the frequency



Individual particles of light are known as photons.

This laser pointer emits approximately 10^{18} photons per second.

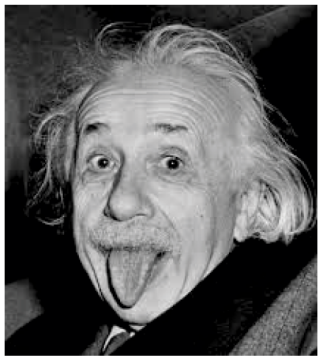
We can detect single photons with a high probability.

BASIC QUANTUM MECHANICS: A RAPID LOOK!

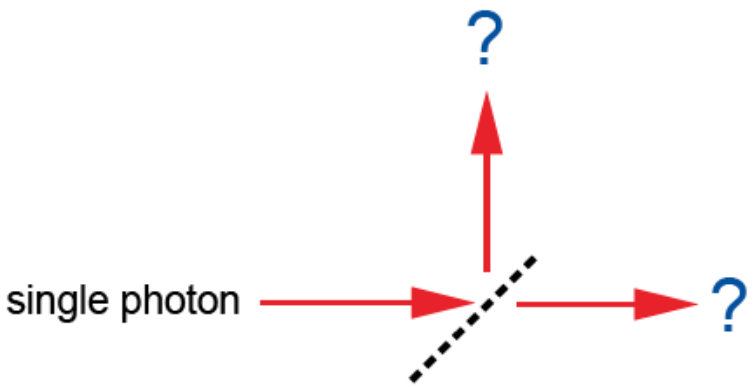
Quantum mechanics is inherently random.

We cannot predict the outcome of certain experiments, even in principle.

Einstein didn't believe this: "God does not play dice with the universe".



Simple example: A single photon incident on a beam splitter (half-silvered mirror):

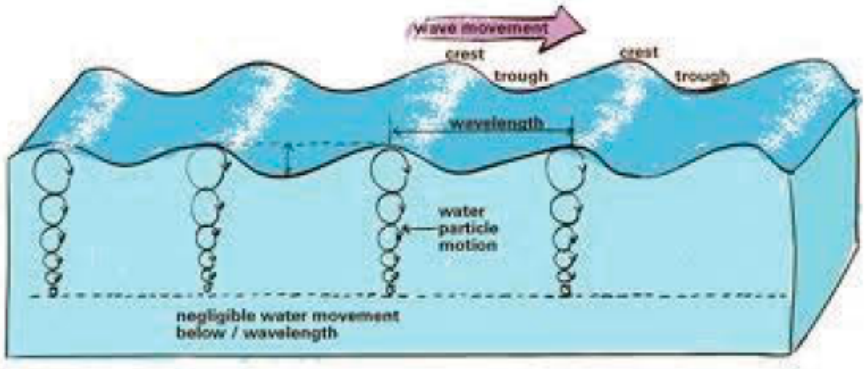


BASIC QUANTUM MECHANICS: A RAPID LOOK!

Particles and Waves

In classical physics, waves are very different from particles:

Wave patterns oscillate as they move along:

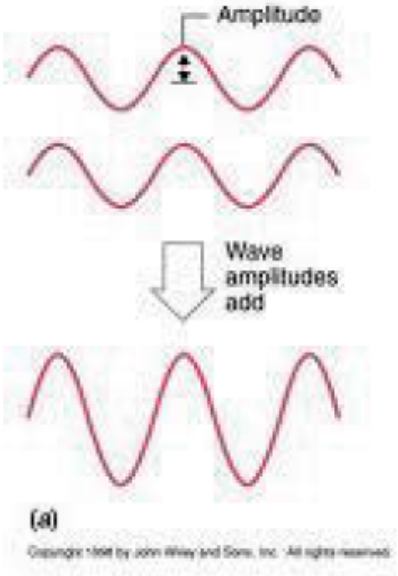


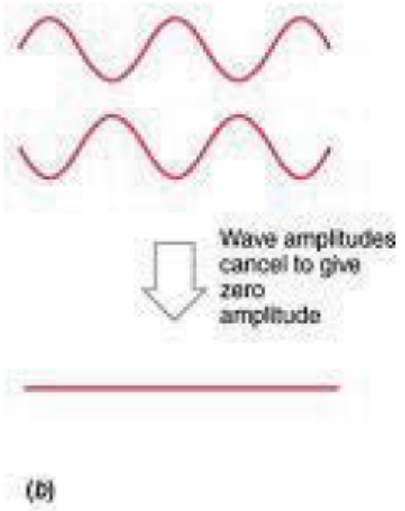
BASIC QUANTUM MECHANICS: A RAPID LOOK!

Interference of Waves

Two different waves can add to become stronger.

Or subtract to become weaker.



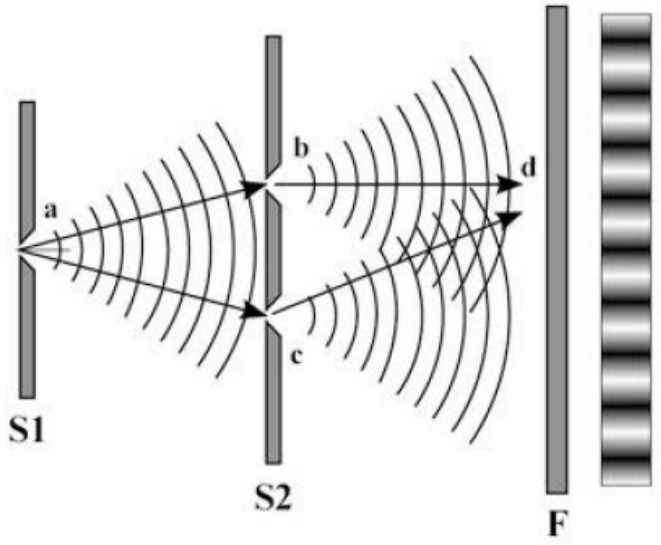


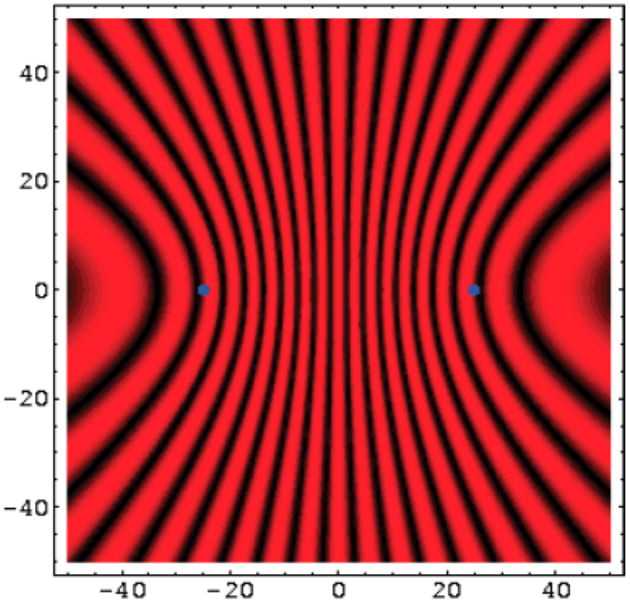
"in phase" "out of phase"

BASIC QUANTUM MECHANICS: A RAPID LOOK!

Interference of Light

Because light is a wave, two light waves can interfere to produce a stronger or weaker wave:





BASIC QUANTUM MECHANICS: A RAPID LOOK!

Particles and Waves in QM

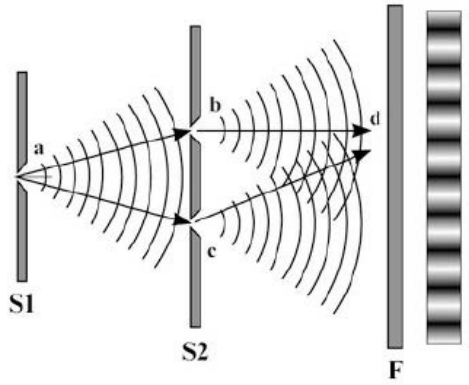
In quantum mechanics, particles are described by a wave function $\psi(x)$.

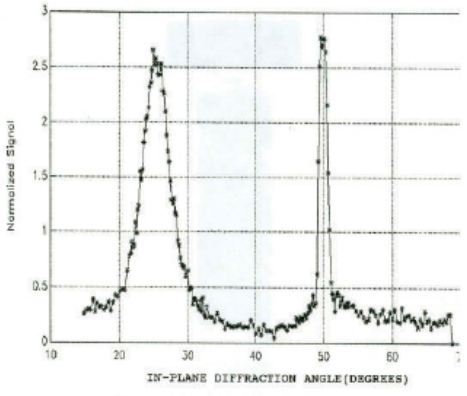
The probability of find the particle at position x is given by the square of the wave function:

$$P = |\psi(x)|^2$$

As a result, a beam of atoms can give all the same interference effects of a wave:

atoms





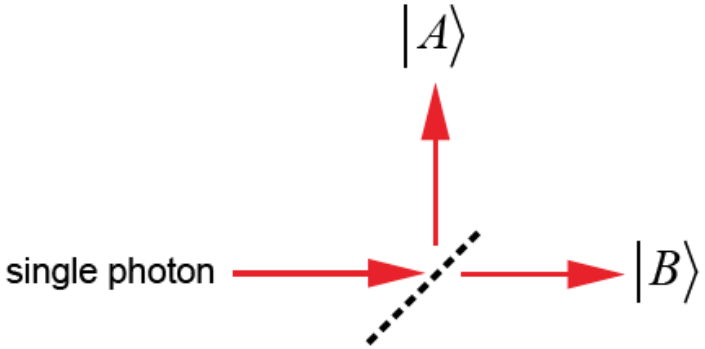
Helium Diffraction pattern

BASIC QUANTUM MECHANICS: A RAPID LOOK!

Superposition States

In quantum mechanics, we can have a "superposition" of two states that are incompatible with each other.

For example, consider a single photon after it has passed through a beam splitter:



$$|\psi\rangle = |A\rangle + |B\rangle$$

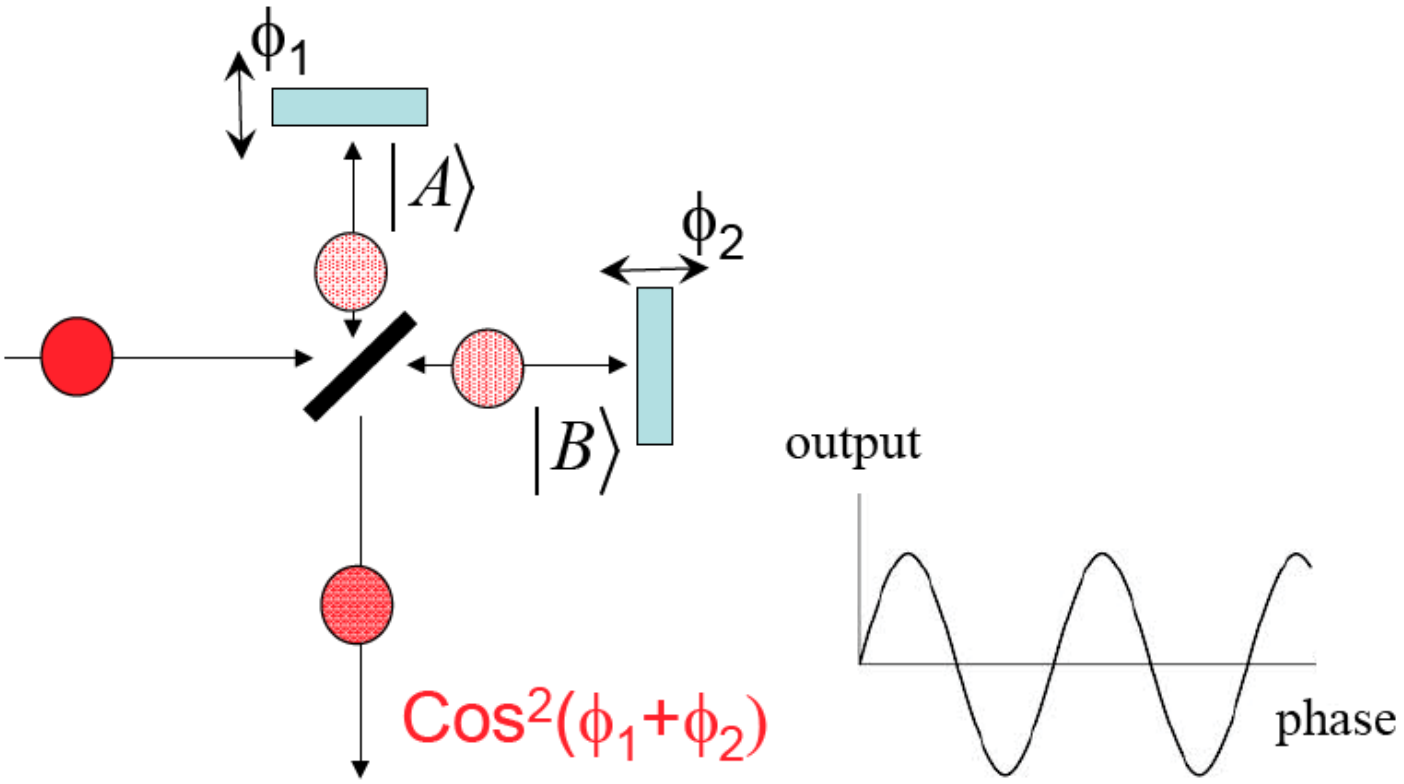
$|\psi\rangle$ is the "state" of the system

The photon is assumed to be in both states simultaneously.

Single-photon Interference

How do we know the photon is really in both states at the same time?

Put mirrors in each path to produce interference between the two states $|A\rangle$ and $|B\rangle$:



Quantum Superposition

Schrodinger Equation

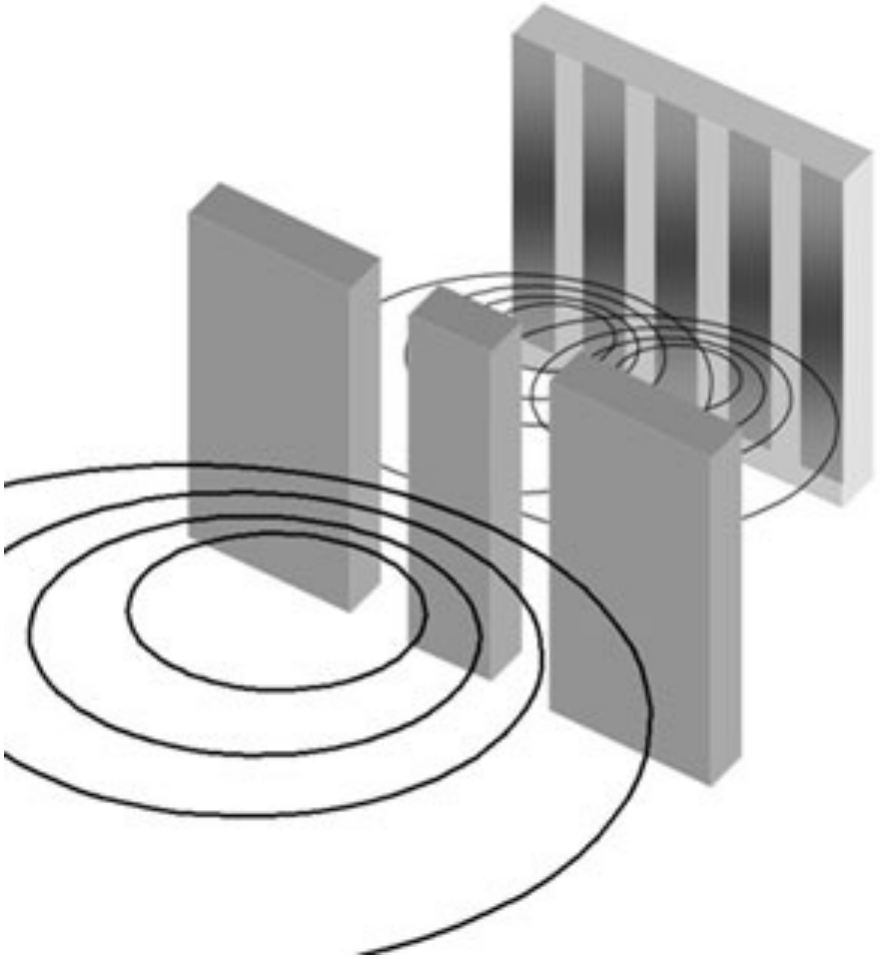
$$i\hbar\,\frac{\partial\psi(x,t)}{\partial t} \;=\; -\frac{\hbar^2}{2m}\,\frac{\partial^2\psi(x,t)}{\partial x^2} + V(x,t)\,\psi(x,t)$$

Schrödinger equation is a linear, partial differential equation and if ψ_1 and ψ_2 are solutions of Schrödinger equation then $a_1\psi_1+a_2\psi_2$ is also a solution for arbitrary a_1 and a_2. A possible physical state of a system is a linear superposition of many wave functions, each describing various permissible physical state of the system,

$$\psi \;=\; \sum_i a_i\,\psi_i.$$

Quantum Superposition

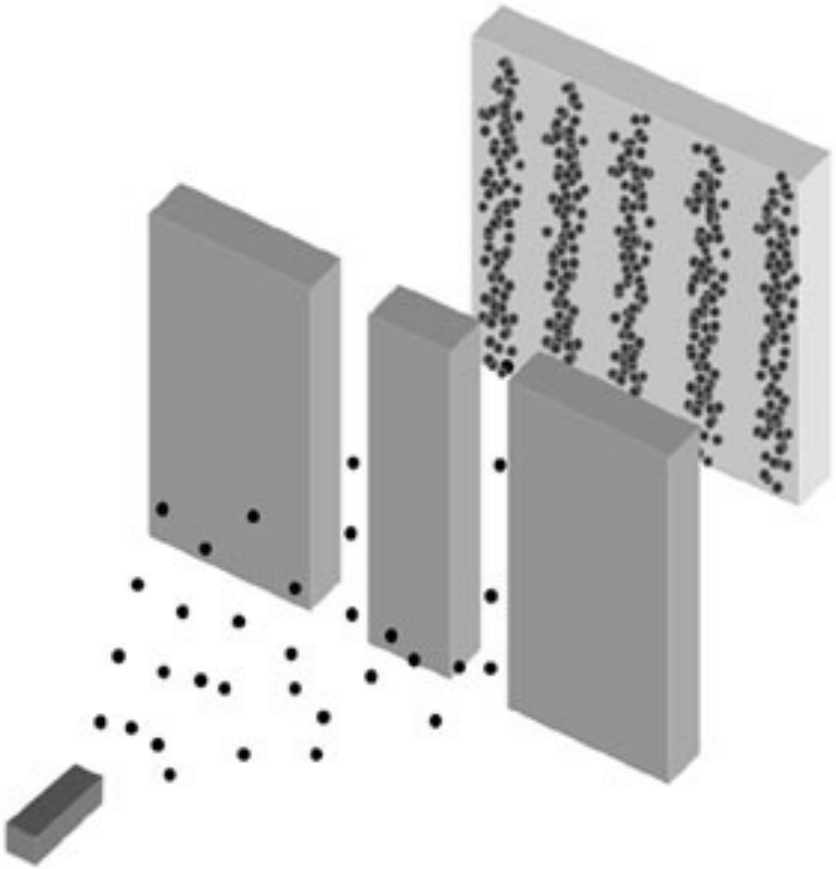
The double slit experiment



Interference of water waves

Quantum Superposition

The double slit experiment

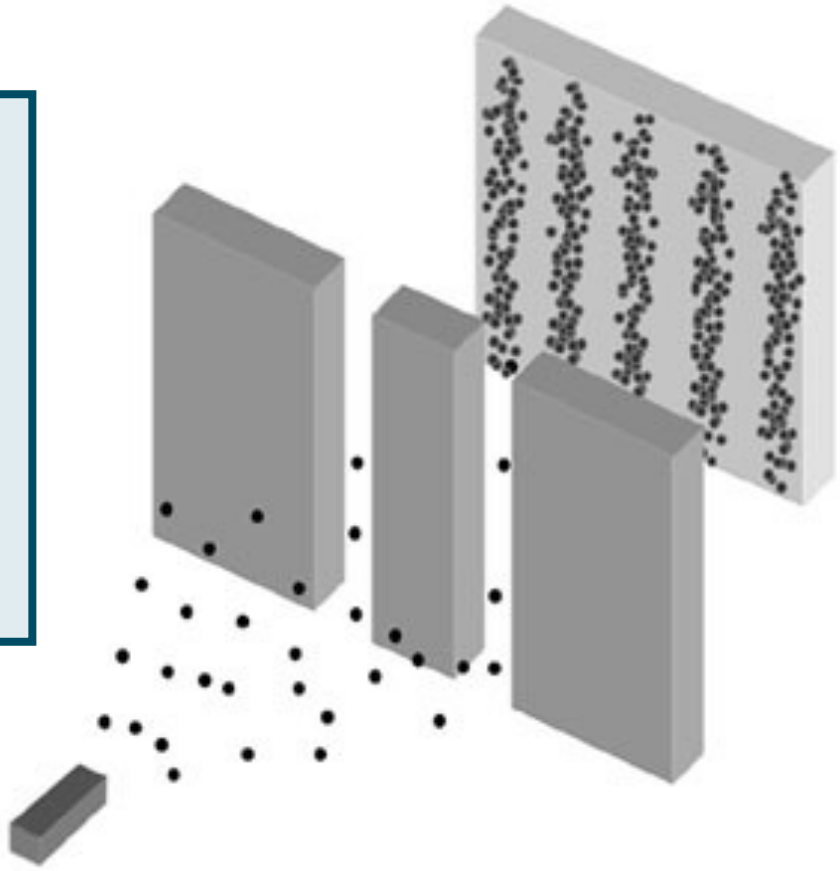


Interference of electrons

Quantum Superposition

The double slit experiment

Which slit does an electron pass through ?

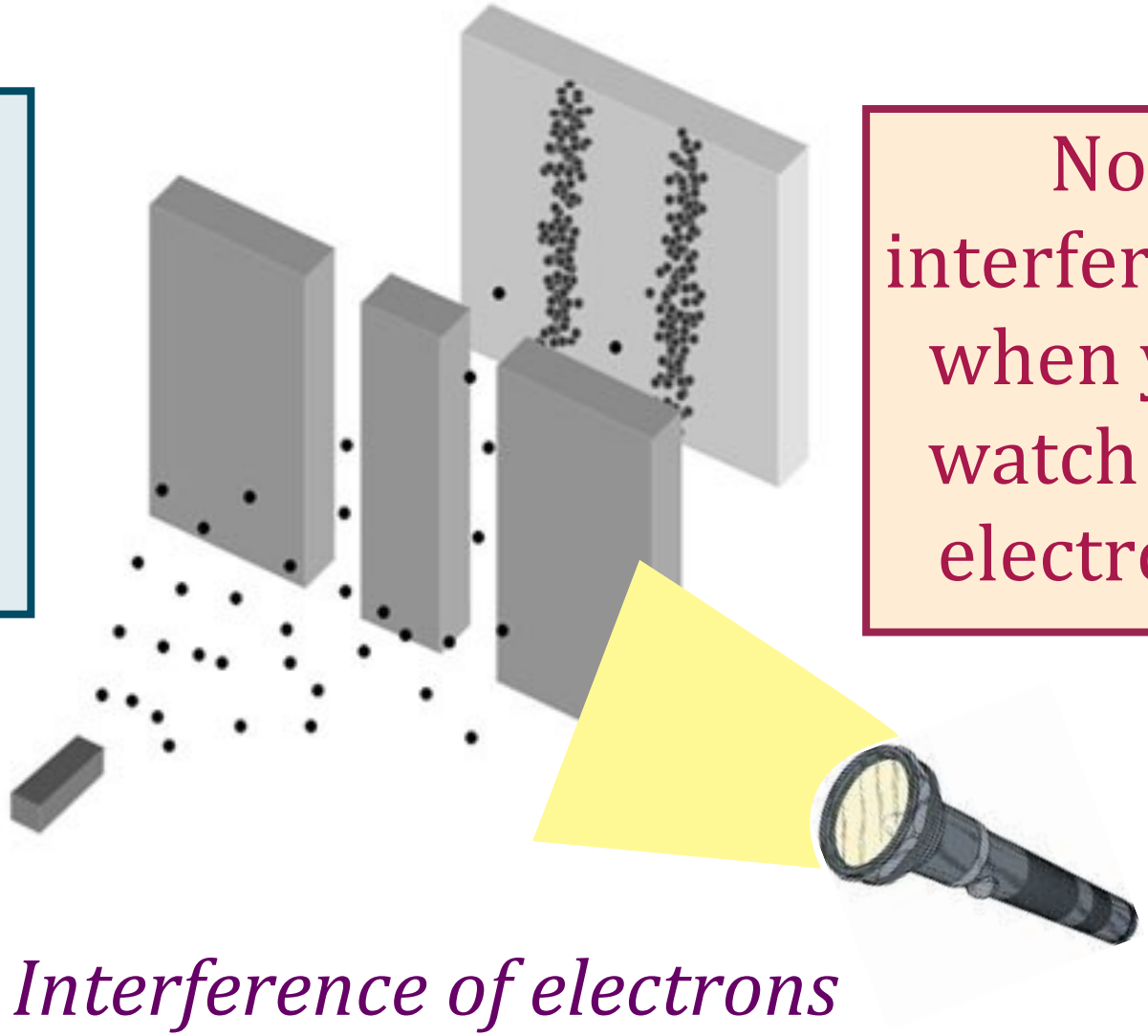


Interference of electrons

Quantum Superposition

The double slit experiment

Which slit does an electron pass through ?



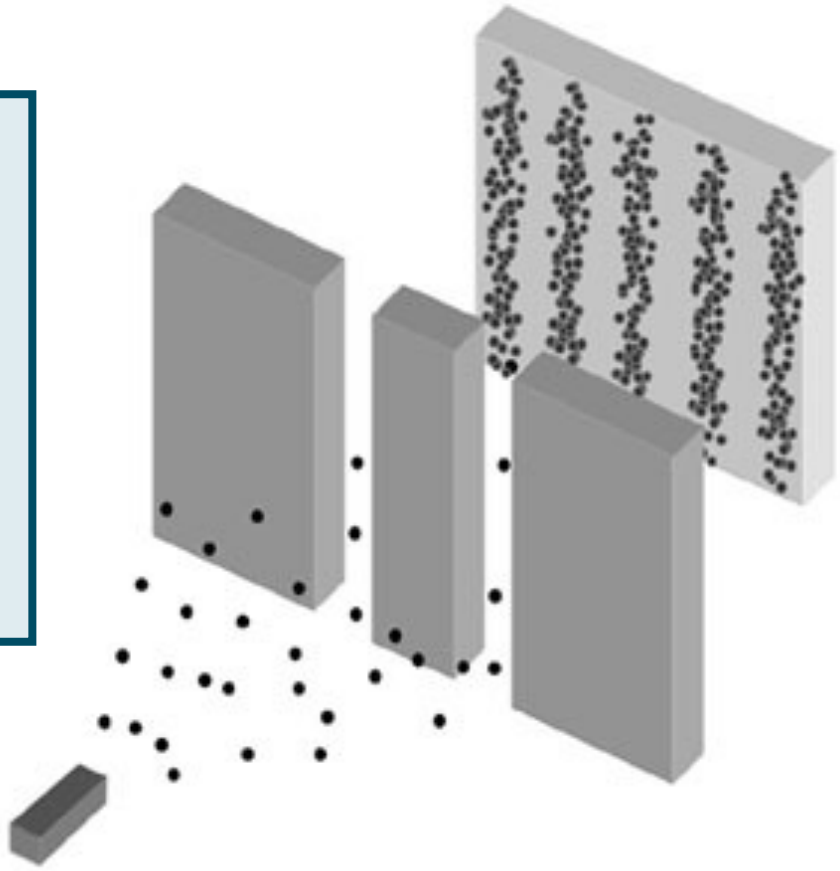
No interference when you watch the electrons

Interference of electrons

Quantum Superposition

The double slit experiment

Which slit does an electron pass through ?

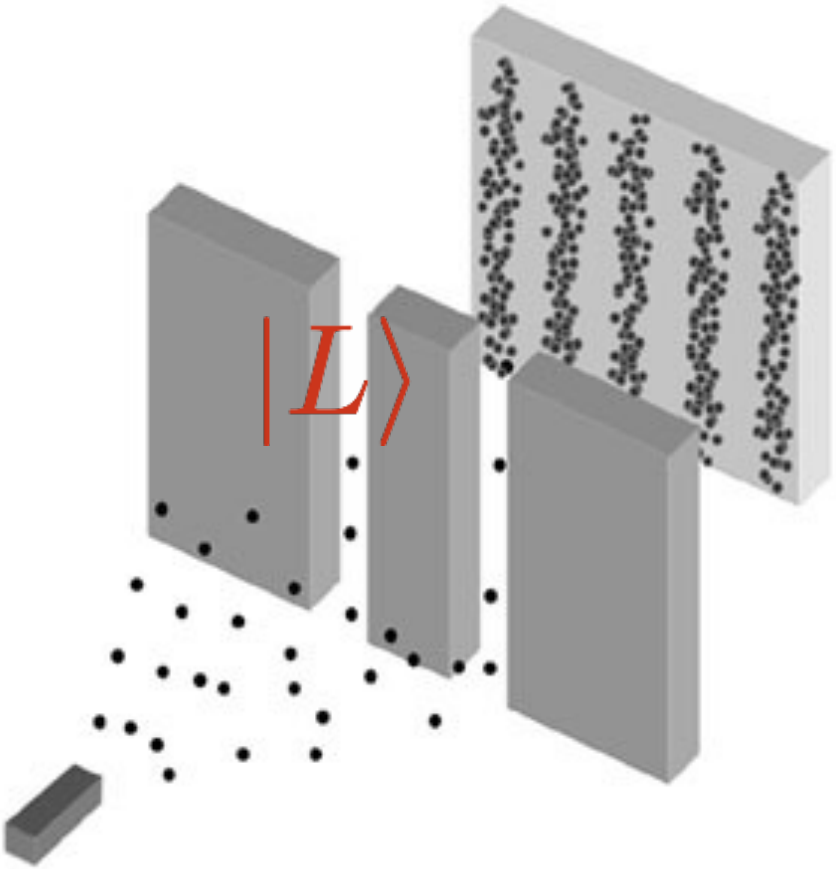


Each electron passes through both slits !

Interference of electrons

Quantum Superposition

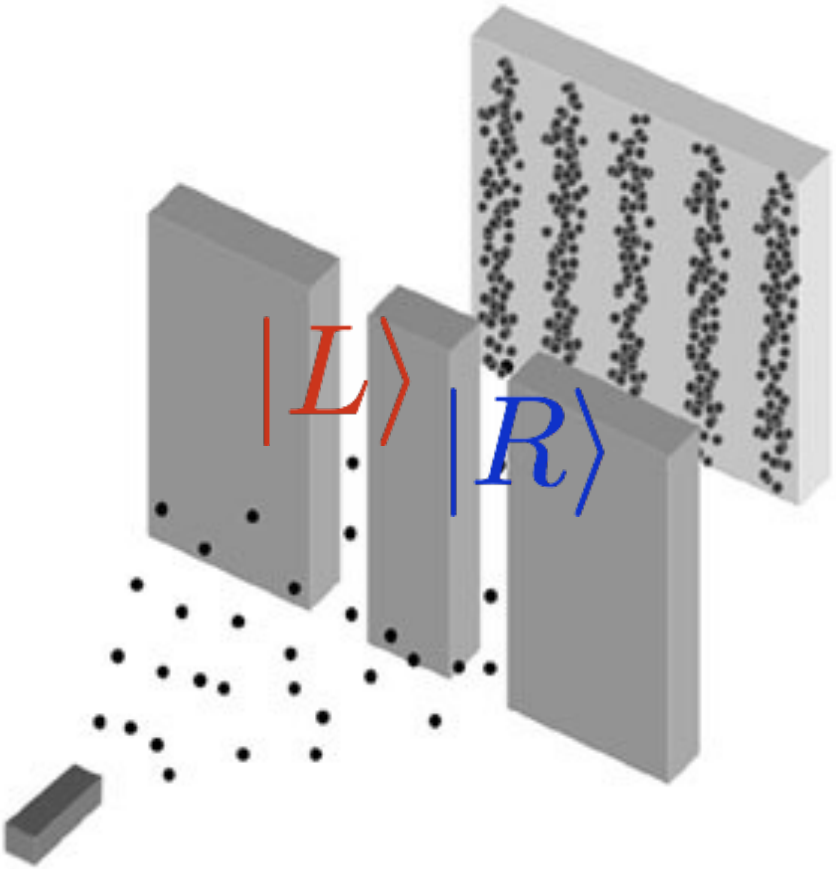
The double slit experiment



Let $|L\rangle$ represent the state with the electron in the left slit

Quantum Superposition

The double slit experiment

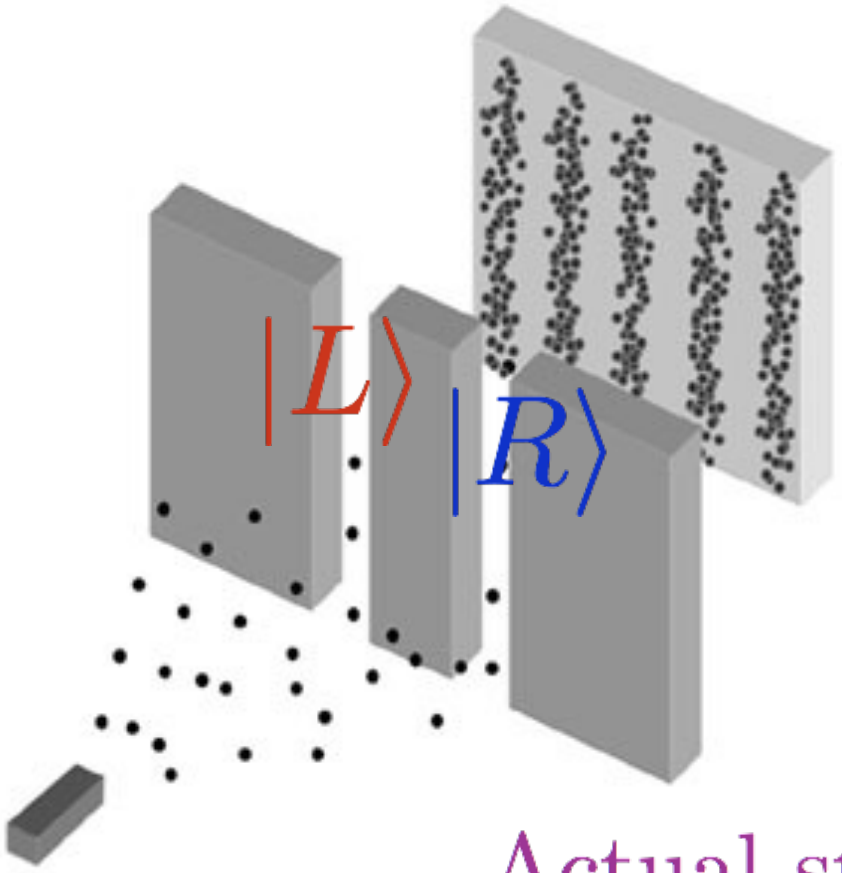


Let $|L\rangle$ represent the state with the electron in the left slit

And $|R\rangle$ represents the state with the electron in the right slit

Quantum Superposition

The double slit experiment

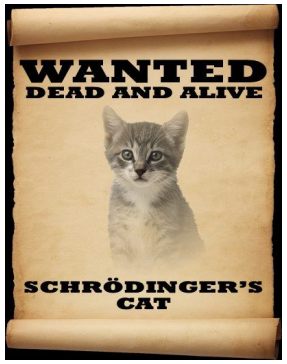


Let $|L\rangle$ represent the state with the electron in the left slit

And $|R\rangle$ represents the state with the electron in the right slit

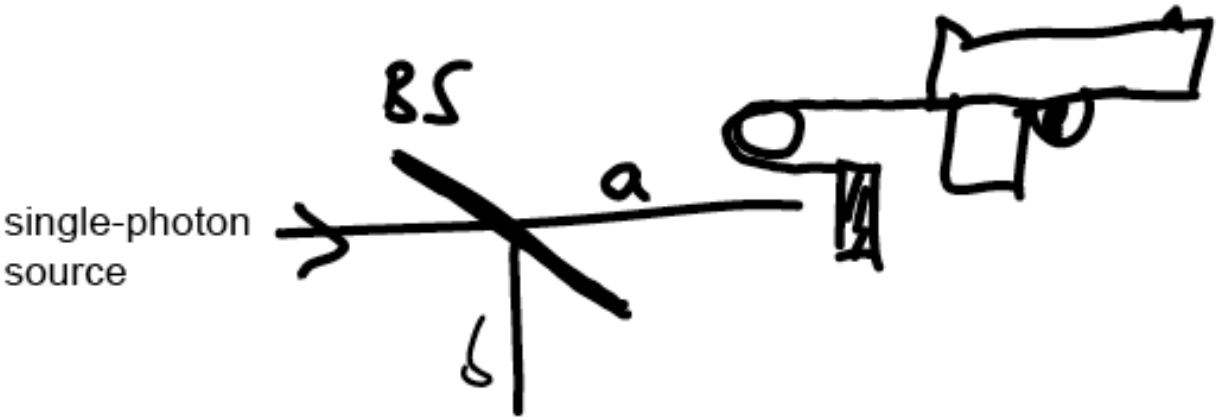
Actual state of the electron is

$$|L\rangle + |R\rangle$$



Schrodinger's Cat!

$$|\psi\rangle = |alive\rangle + |dead\rangle ?$$

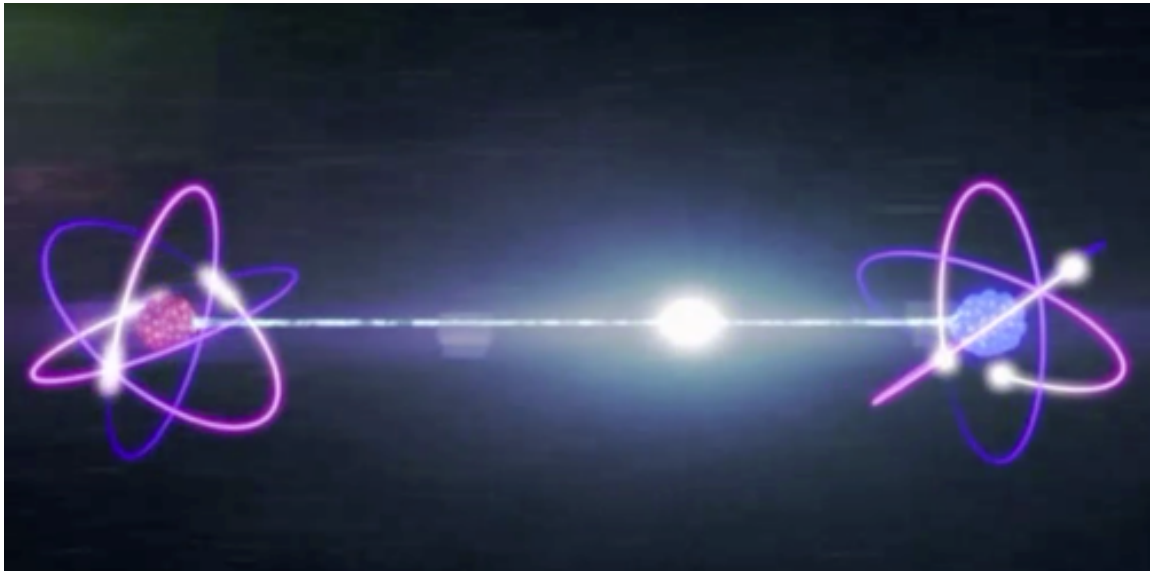


$$|0\rangle_a + |1\rangle_a \rightarrow |0\rangle_a |\text{cat}\rangle + |1\rangle_a |\text{cat}\rangle$$

Schrodinger Cat state and the photon is entangled!

QUANTUM ENTANGLEMENT

It says that two particles can be connected to each other regardless of the distance that separates them, that is, if we place a particle here and another in the Andromeda galaxy that is 2573 light years from the earth (this means that a radio wave common would take 2573 years to get there) would change instantly with its counterpart.



QUANTUM ENTANGLEMENT

ANY TIME TWO ENTITIES INTERACT, they entangle. It doesn't matter if they are photons (bits of light), atoms (bits of matter), or bigger things made of atoms like dust motes, microscopes, cats, or people. The entanglement persists no matter how far these entities separate, as long as they don't subsequently interact with anything else—an almost impossibly tall order for a cat or a person, which is why we don't notice the effect.

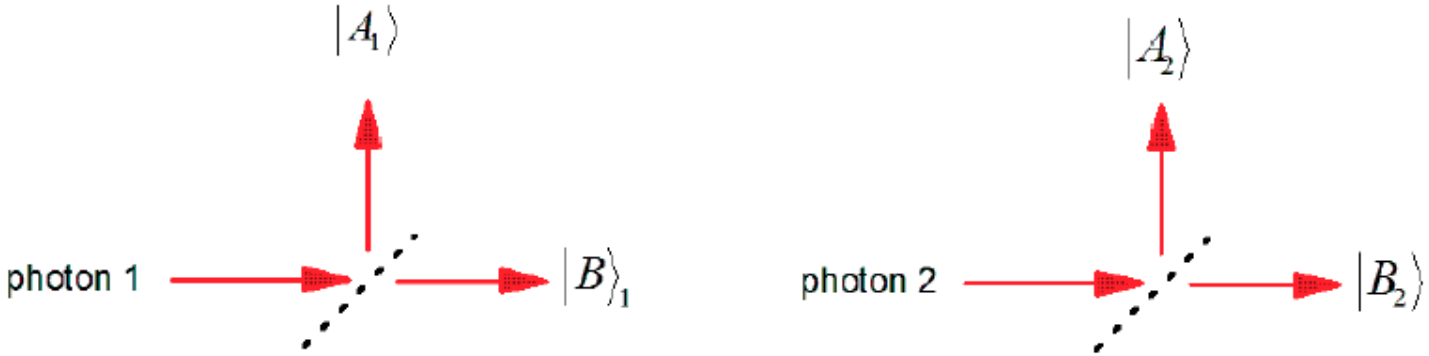
But the motions of subatomic particles are dominated by entanglement. It starts when they interact; in doing so, they lose their separate existence. No matter how far they move apart, if one is tweaked, measured, observed, the other seems to instantly respond, even if the whole world now lies between them. And no one knows how.

The Age of Entanglement

ENTANGLEMENT

Schrodinger also considered a situation where two distant systems are in a correlated superposition state.

For example, consider two photons and two beam splitters



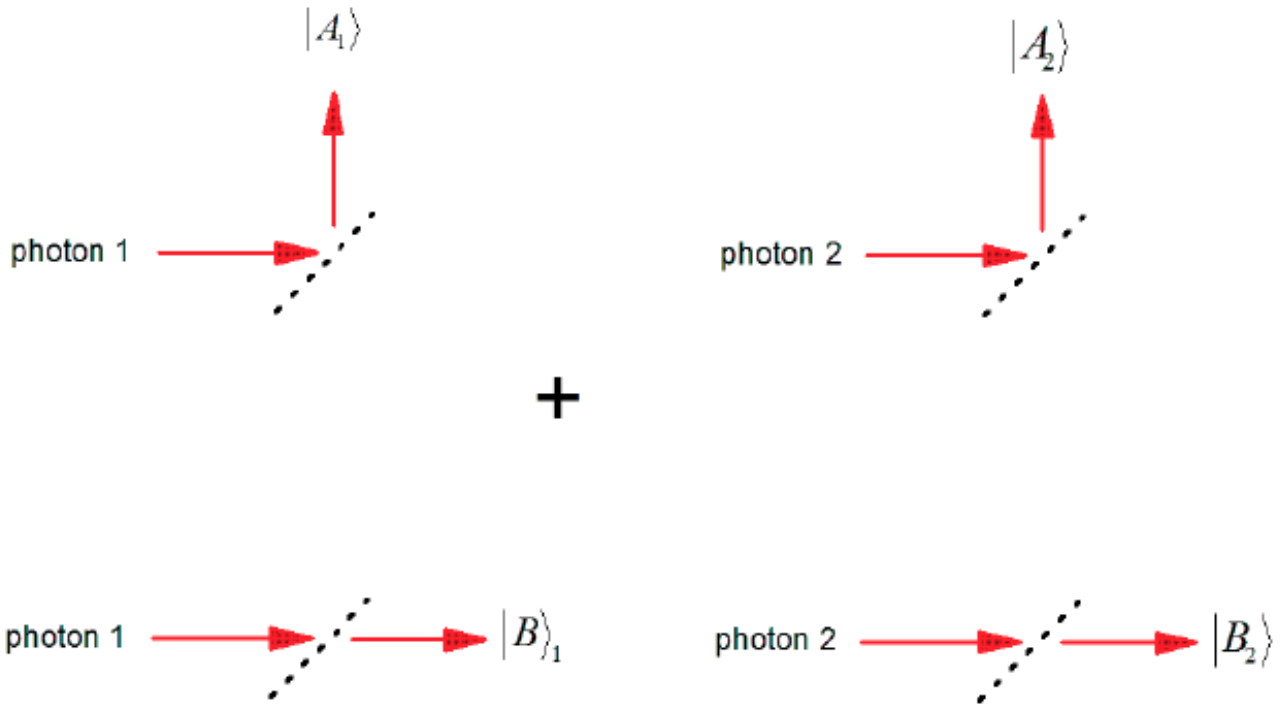
We can create an "entangled" state where

$$|\psi\rangle = |A_1\rangle|A_2\rangle + |B_1\rangle|B_2\rangle$$

The paths are totally correlated.

ENTANGLEMENT

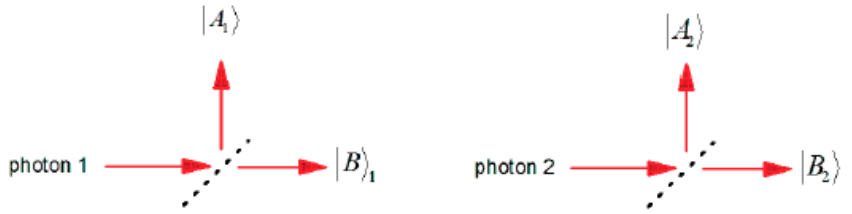
The entangled state $|\psi\rangle = |A_1\rangle|A_2\rangle + |B_1\rangle|B_2\rangle$ can be viewed as:



Both of these states exist simultaneously.

ENTANGLEMENT

Consider an entangled state where the paths of two photons are correlated:



$$|\psi\rangle = |A_1\rangle|A_2\rangle + |B_1\rangle|B_2\rangle$$

Suppose we use a single-photon detector to measure which path photon 1 is in.

And find that it is in path A_1 .

Then photon 2 must be in path A_2 and the state instantly "collapses" to

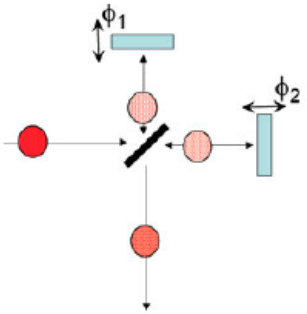
$$|\psi\rangle = |A_1\rangle|A_2\rangle$$

This has physical effects at location 2.

ENTANGLEMENT

How do we know that both states in an entangled state really exist at the same time?

Recall that, for a single photon and a beam splitter, quantum interference shows that both states must exist:

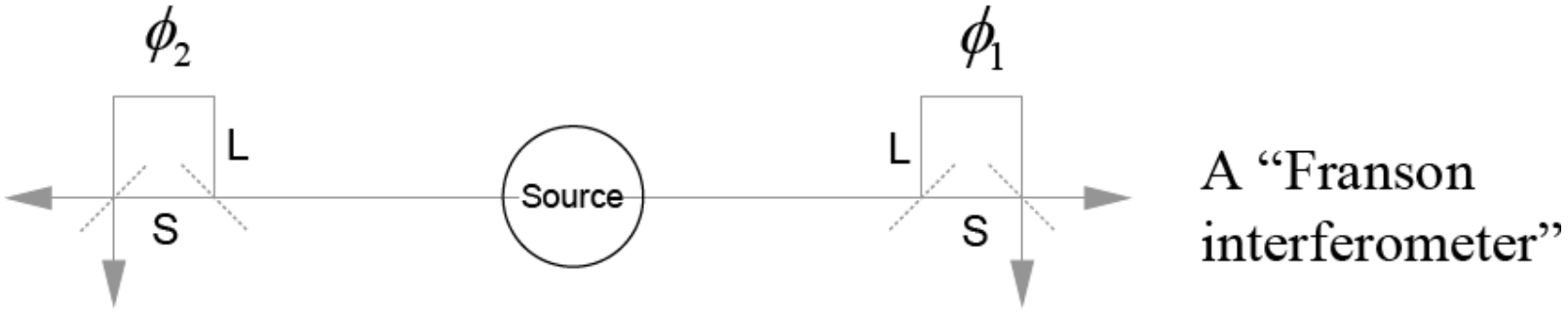


For two entangled photons, we can use “nonlocal interference” to show the same thing.

ENTANGLEMENT

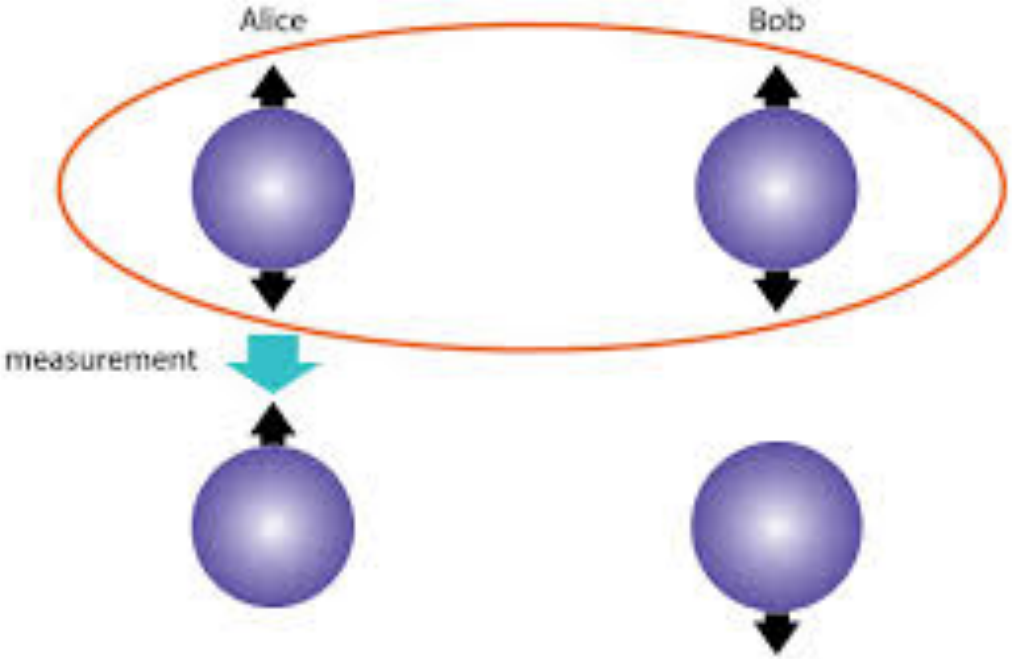
We can generate an entangled state in which two photons were created at exactly the same time.

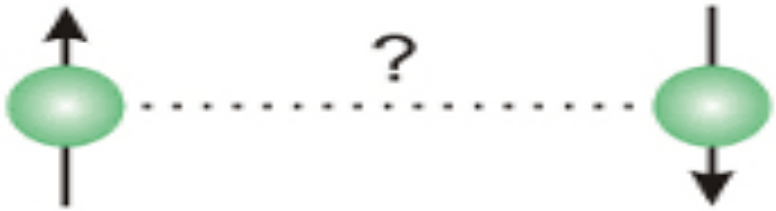
Suppose the two photons travel in opposite directions to two single-photon interferometers:



The two photons will interfere with each other regardless of how far apart they are.

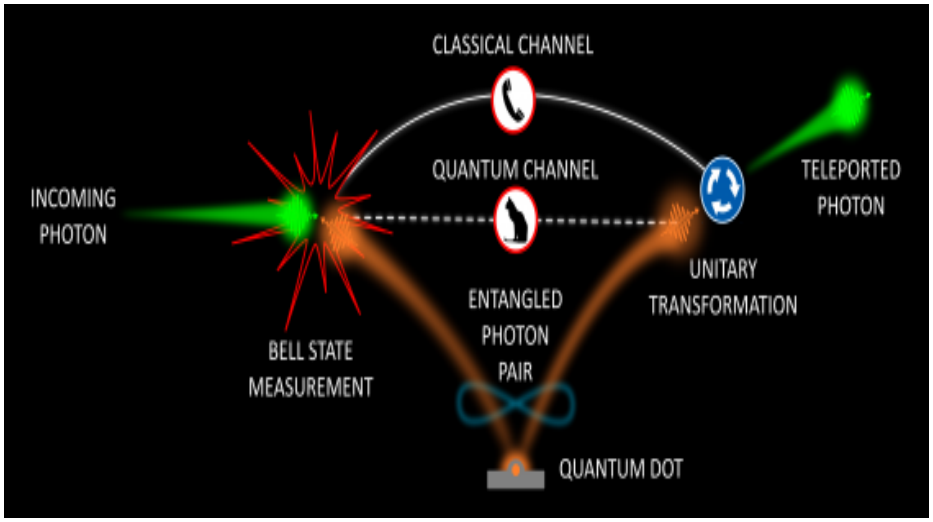
ENTANGLEMENT



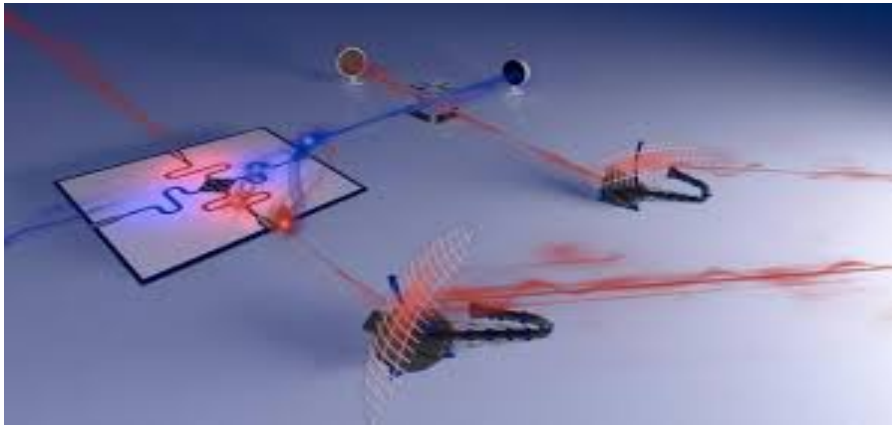


observed
"here"

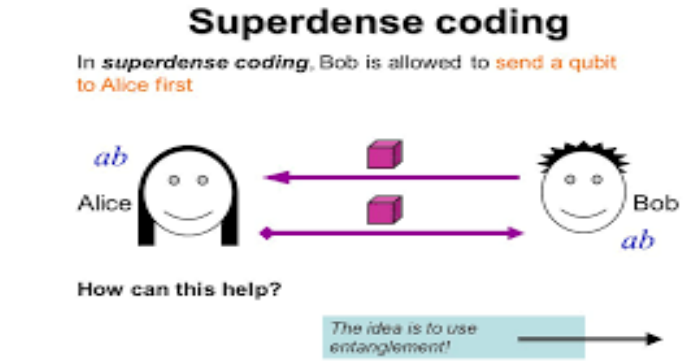
affected
"over there"



Quantum Teleportation



Quantum entanglement aids radar detection



Super-dense coding

Back to Quantum Computer…!

What is a Quantum Computer?

A quantum computer is a device that leverages specific properties described by quantum mechanics to perform computation

Every classical (that is, non-quantum) computer can be described by quantum mechanics since quantum mechanics is the basis of the physical universe. However, a classical computer does not take advantage of the specific properties and states that quantum mechanics affords us in doing its calculations.

Before we go further …

Some More Fundamentals

- **Bit**

The smallest unit of information is a bit, and that can represent either the value 0 or the value 1.

- **Byte**

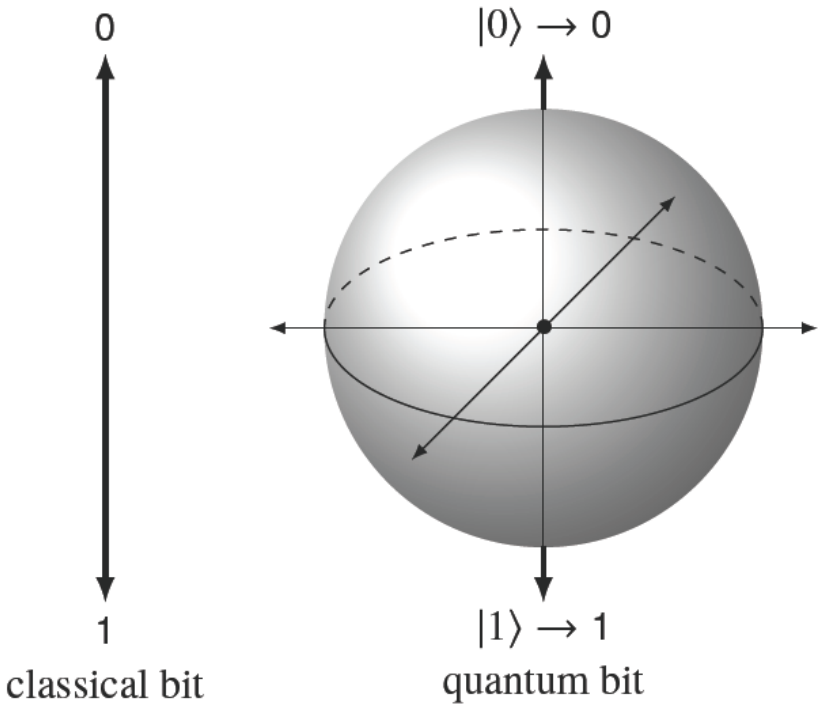
A byte is 8 bits

Bits	Character	Bits	Character
0100001	!	0111111	?
0110000	0	1000001	A
0110001	1	1000010	B
0110010	2	1100001	a
0111100	<	1100010	b

We number the bits from right to left, starting with o:

character 'a':	1	1	0	0	0	0	1
	↑	↑	↑	↑	↑	↑	↑
position:	6	5	4	3	2	1	0

Qubit



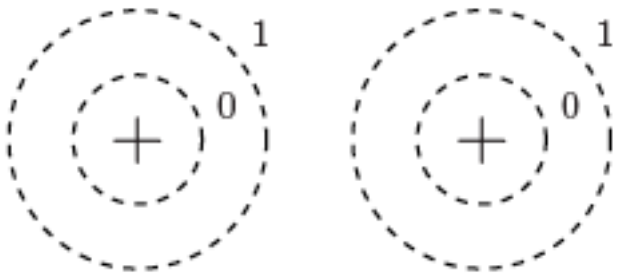
Traditional computing relies on bits, or ones and zeros, quantum computing uses quantum bits, or qubits, that can be both one and zero at the same time.

The qubit always becomes the state |0> or |1> when we read information from it by a process called measurement. However, it is possible to move it to an infinite number of other states and change from one of them to another while we are computing with the qubit before measurement.

Measurement says "ok, I'm going to peek at the qubit now" and the result is always a 0 or 1 once you do so. We can then read that out as a bit value of 0 or 1, respectively.

THIS IS WEIRD!

TWO-QUBITS



Consider two electrons in two hydrogen atoms, each regarded as a 2-state quantum system

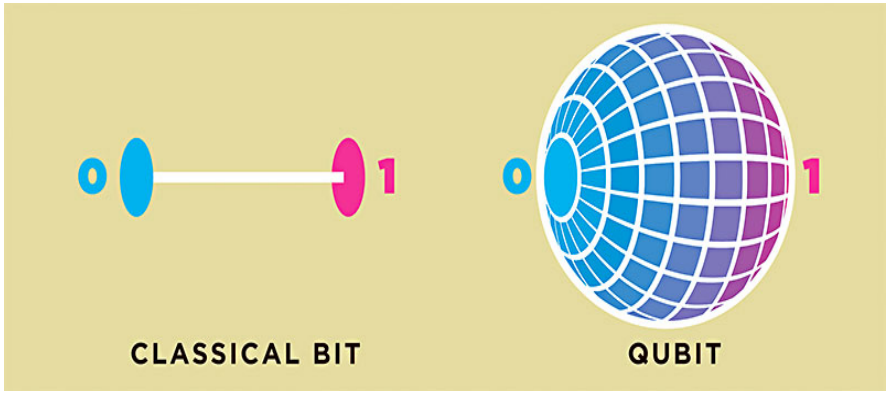
Since each electron can be in either of the ground or excited state, classically the two electrons are in one of four states: 00, 01, 10, or 11 and represent 2 bits of classical information.

By the superposition principle, the quantum state of the two electrons can be any linear combination of these four classical states:

$$|\psi\rangle = \alpha_{00}|00\rangle + \alpha_{01}|01\rangle + \alpha_{10}|10\rangle + \alpha_{11}|11\rangle$$

Qubit

- Bits are not merely ON and OFF, they can be in **superposition**
- Bits are not independent of each other, they can be **entangled**



A *qubit*—a *quantum bit*—is the fundamental unit of quantum information. At any given time, it is in a superposition state represented by a linear combination of vectors $|0\rangle$ and $|1\rangle$ in $\mathbb{C}^2$:

$$a|0\rangle + b|1\rangle \quad \text{where} \quad |a|^2 + |b|^2 = 1 \ .$$

Through *measurement*, a qubit is forced to collapse irreversibly through projection to either $|0\rangle$ or $|1\rangle$. The probability of its doing either is $|a|^2$ and $|b|^2$, respectively. a and b are called *probability amplitudes*.

If necessary, we can convert ("read out") $|0\rangle$ and $|1\rangle$ to classical bit values of 0 and 1.

Home Computer Vs. Quantum Computer

- A 64 bit Home computer can process 64 bytes in each step.
- A 64 bit Quantum Computer can process 36 billion billion bytes in each step, i.e. 36×10^{20} bytes/step!
- Quantum bits provides exponential processing powers.

Classical vs. Quantum Computing

Classical

- Classical computing is what drives smartphones, laptops, Internet servers, mainframes, high performance computers, and even the processors in automobiles.

Quantum

- Quantum computing may someday help us solve problems that are today intractable using classical methods on classical computers.
- RSA (foundation of secure internet and cryptographic protocols) can be cracked
- Protein folding can be simulated
- New medicines and treatments

Classical vs. Quantum Computing

Classical

- Classical computing is based on *von Neumann* architecture.
- CPU + Memory (CPU performs computation on data stored in the memory

John von Neumann

Quantum

- CPU+ Memory model does not apply to Quantum computing architecture.
- Quantum computers are designed like a digital circuits with gates
- Instead of bits, Gates operates on quantum bits.
- Qubits are superposed and entangled
- This makes us to develop algorithm in a new way!

Classical vs. Quantum Computing

Whereas a classical computer processes data sequentially, a quantum computer should operate as a massively parallel processor. It does so thanks to the fact that each qubit—encoded in quantum particles such as atoms, electrons or photons—can exist in a superposition of the "0" and "1" states, rather than simply one or the other, and because the qubits are linked together through entanglement.

- Your phone or laptop uses bytes as the individual units of memory or storage. That's where we get phrases like "megabyte," which means one million bytes of information. A byte is further broken down into eight bits. Each bit can be 0 or 1. Doing the math, each byte can represent $2^8 = 256$ different numbers composed of eight 0s or 1s, but it can only hold one value at a time.
- Eight qubits can represent all 256 values at the same time. This is through superposition, but also through *entanglement*, the way we can tightly tie together the behavior of two or more qubits. This is what gives us the (literally) exponential growth in the amount of working memory that we saw with a quantum representation of caffeine.

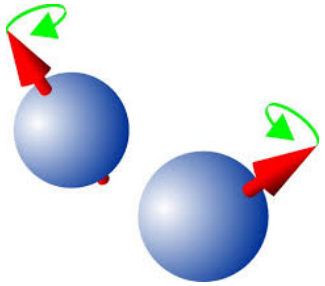
The fact that qubits can be entangled with one another means that N of them can in principle process 2^N states simultaneously, making such a computer exponentially faster than a classical device.

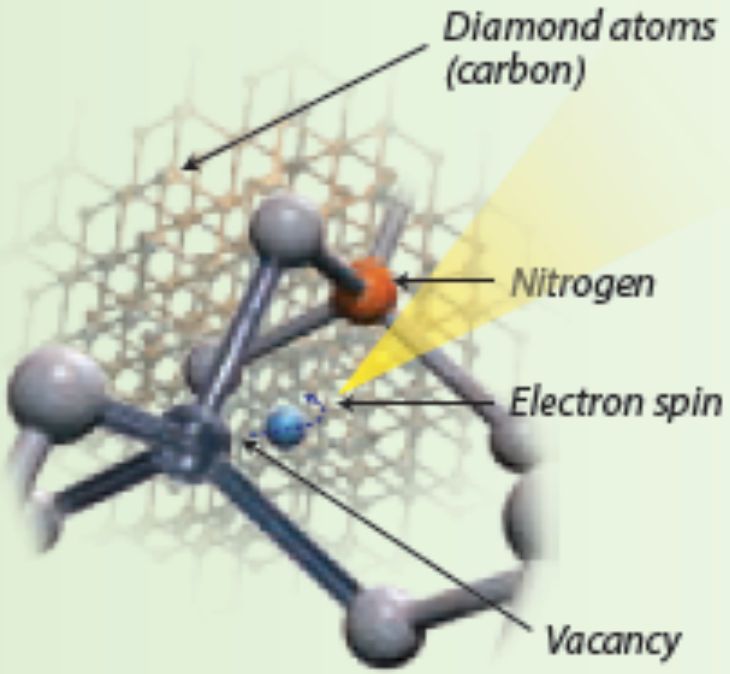
Yet quantum computers are extremely complex. Qubits must first be encoded using the quantum states of particular physical objects, such as the spin of electrons or atomic nuclei.

The qubits are then manipulated via quantum logic gates consisting of laser beams, microwaves, electric fields or other probes, designed to evolve the system's wavefunction in a well-defined way such that, upon measurement, there's a high probability that the wave function will collapse to the classical state corresponding to the right answer for the algorithm in question.

FOUR ROUTES TO QUANTUM COMPUTING

SPIN QUBITS



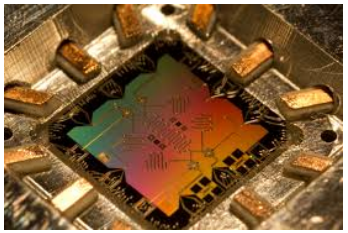


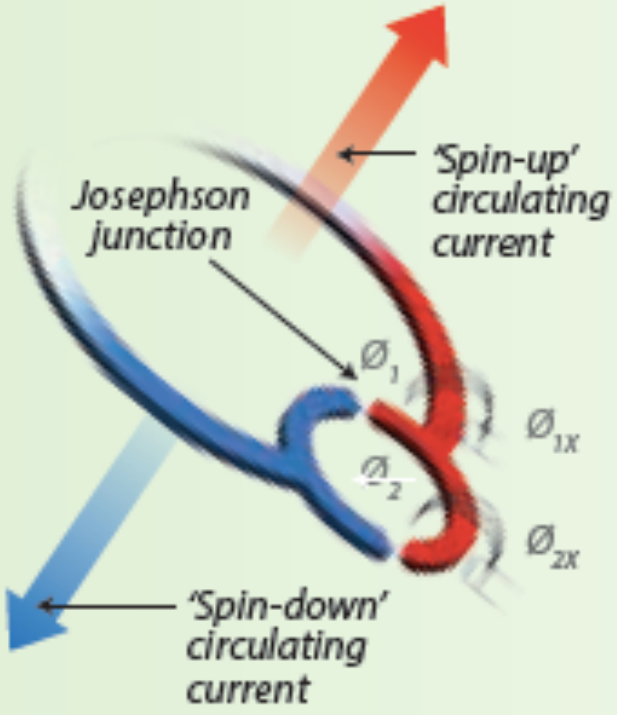
1 Spin qubits

Made from spins of electrons or nuclei trapped in a solid substrate, such as nitrogen vacancy centers in diamond. Can remain in superposition states for up to several seconds and can be compatible with current chip-manufacturing technology. Noise from solid-state environment could hamper scaling up.

FOUR ROUTES TO QUANTUM COMPUTING

SUPERCONDUCTING CIRCUITS



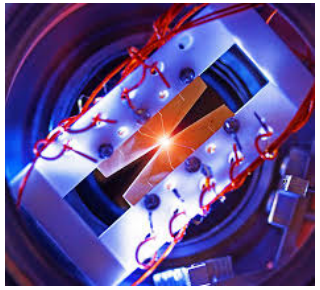


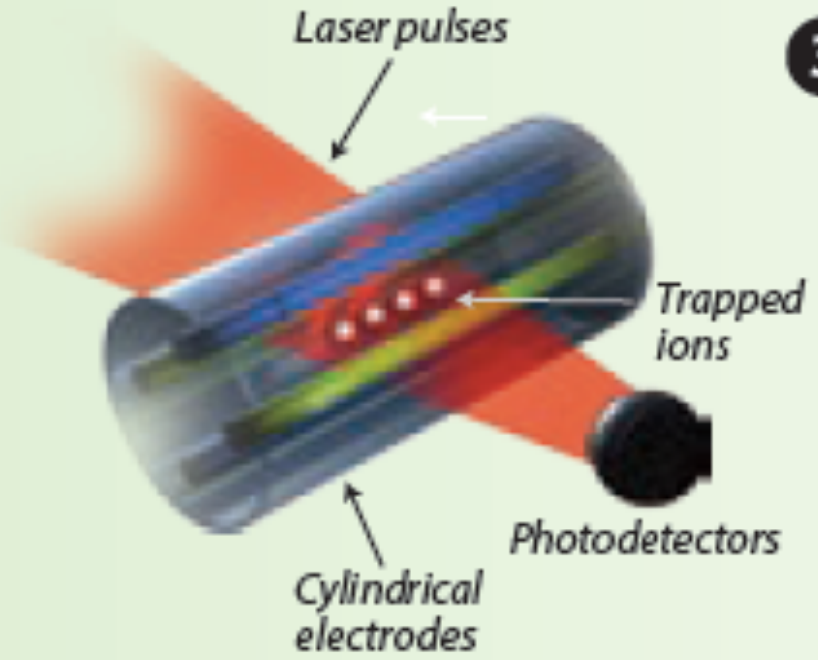
2 Superconducting circuits

Superpositions of currents flowing in opposite directions around a superconductor at the same time. Being solid state, they are potentially easy to manufacture, but have relatively short coherence times and require low temperatures to operate.

FOUR ROUTES TO QUANTUM COMPUTING

ION TRAPS



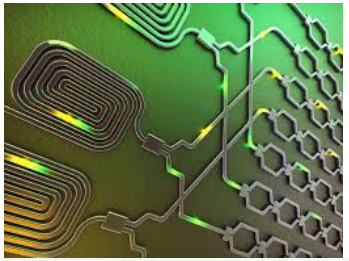


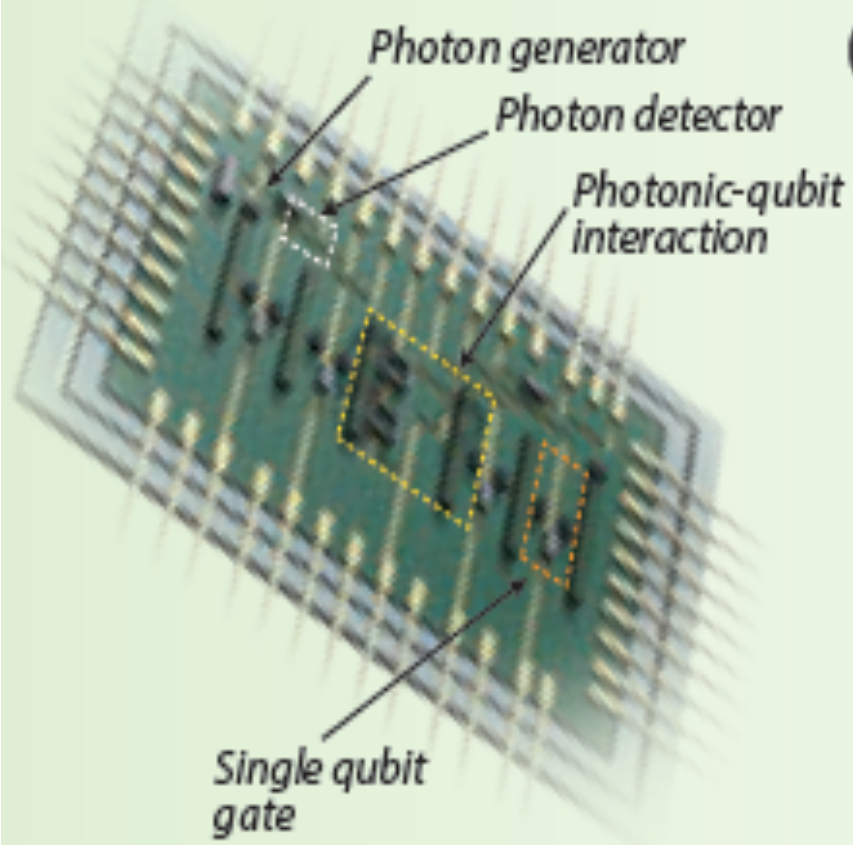
3 Ion traps

Qubits reside in arrays of ions trapped in electric fields, with their quantum states manipulated by lasers. Very clean systems that don't suffer from defects, allowing for logic gates with low error rates—but scaling up will require new fabrication infrastructure.

FOUR ROUTES TO QUANTUM COMPUTING

PHOTONIC CIRCUITS





4 Photonic circuits

Qubits are encoded in the quantum states of photons travelling around circuits in silicon chips, which include etched waveguides and tiny linear optical components. Need for qubit redundancy could be minimized by photons' resistance to interference, but building photonic logic gates is difficult, and single-photon sources pose a technical challenge.

Quantum Computer-*challenges ahead*!

- *Among the algorithms developed to date are one for factorization put forward by Peter Shor in 1995, and another for searching databases proposed by Lov Grover a year later. However, the complexities of quantum physics mean that devising new algorithms is a tricky business.*

- *Actually building a quantum computer is tougher still. Qubits must be manipulated, yet simultaneously protected from the tiniest external sources of heat or electromagnetic radiation, which would destroy their fragile superposition in a process known as decoherence.*

- *Quantum computers' potential has been exaggerated in the past, but believes that has helped attract interest and funding to the field. As a result, science and technology could go in unexpected directions, no matter when, or even if, a universal quantum computer gets built."*

"Like Columbus, who wanted to get to India but ended up discovering America, someone will find something if they are serious about searching".