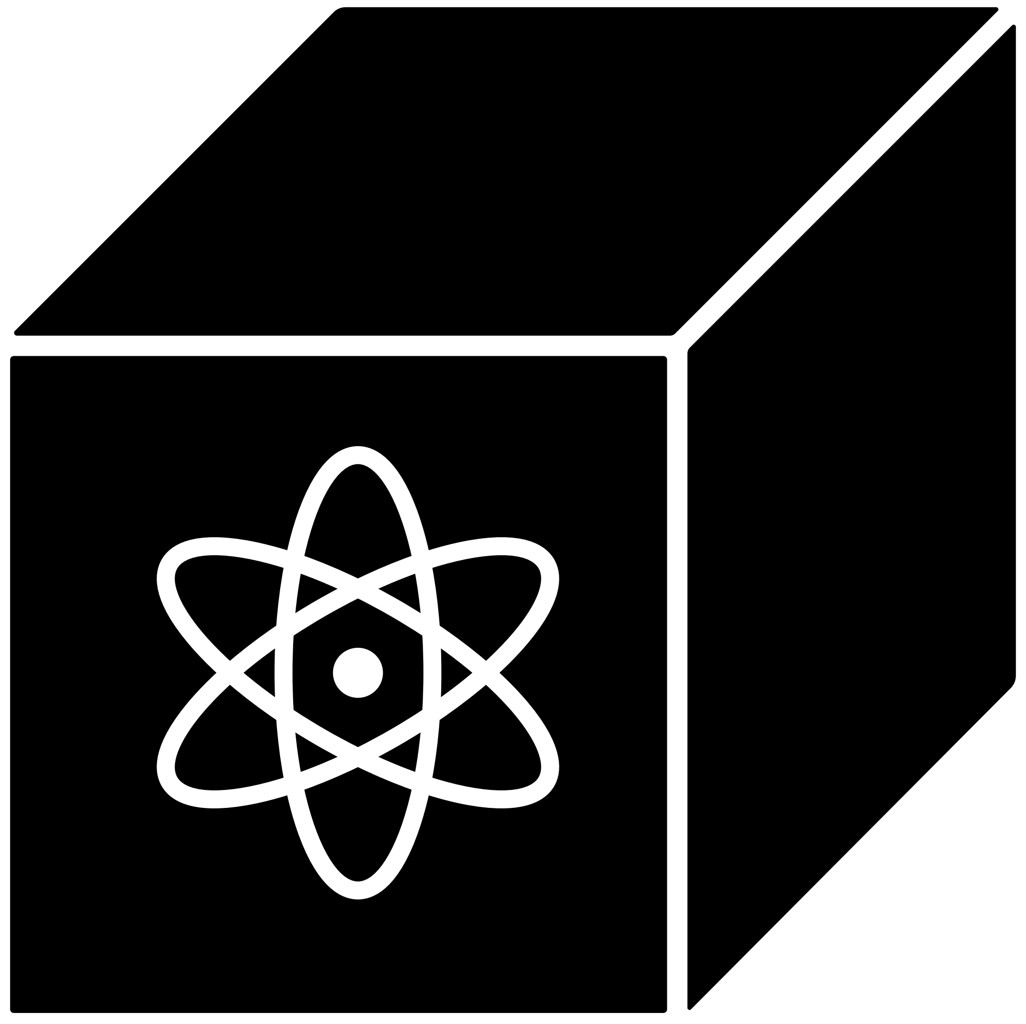
Introduction to Quantum Computing

CS 498QC (Spring 2025)

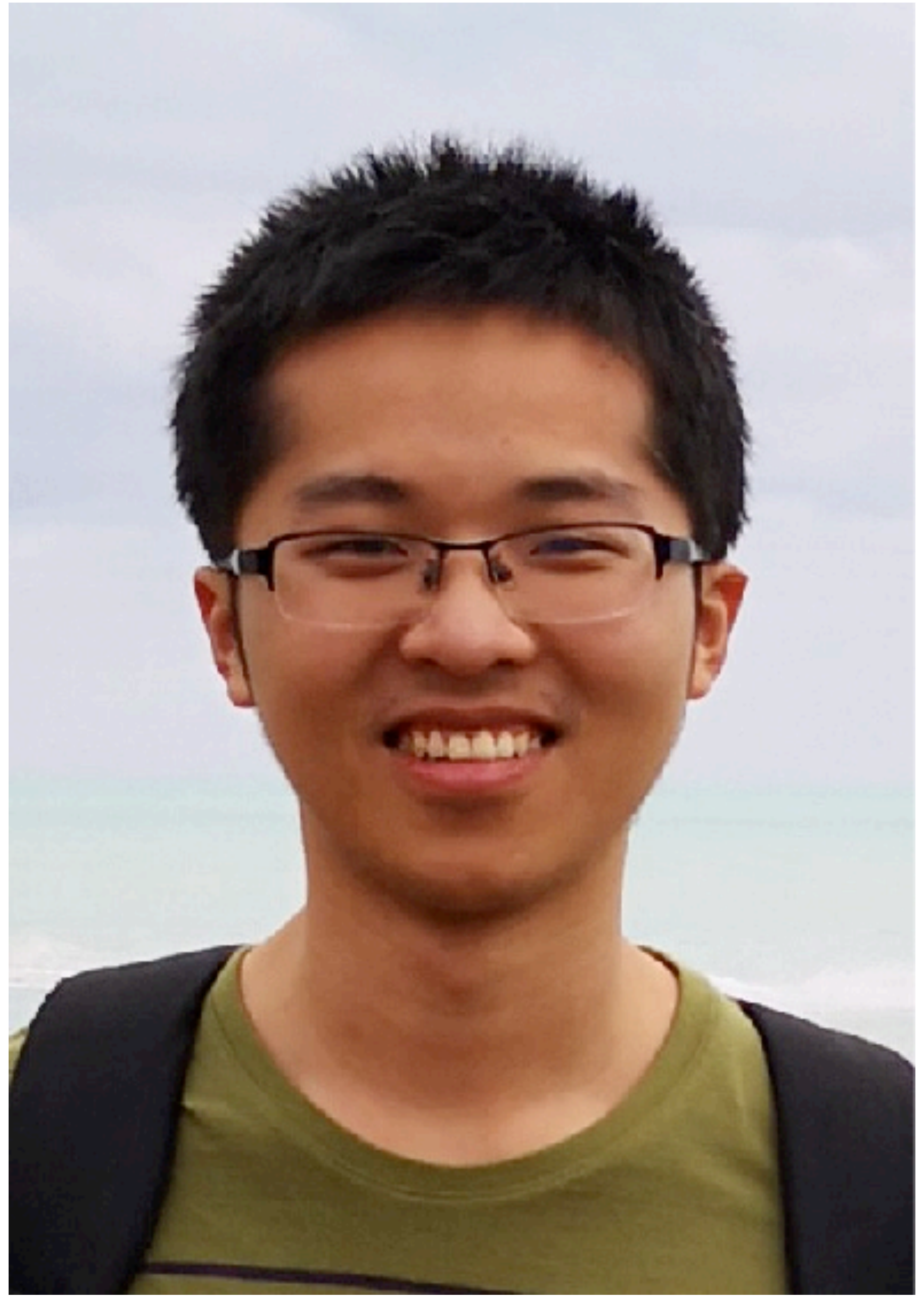
Makrand Sinha and Fernando Granha Jeronimo



*Based on Henry Yuen's introductory slides from a course at Columbia University

Makrand Sinha

Fernando Jeronimo



Yuchen Pang

TA


QUANTUM
COMPUTER


QUANTUM
COMPUTER

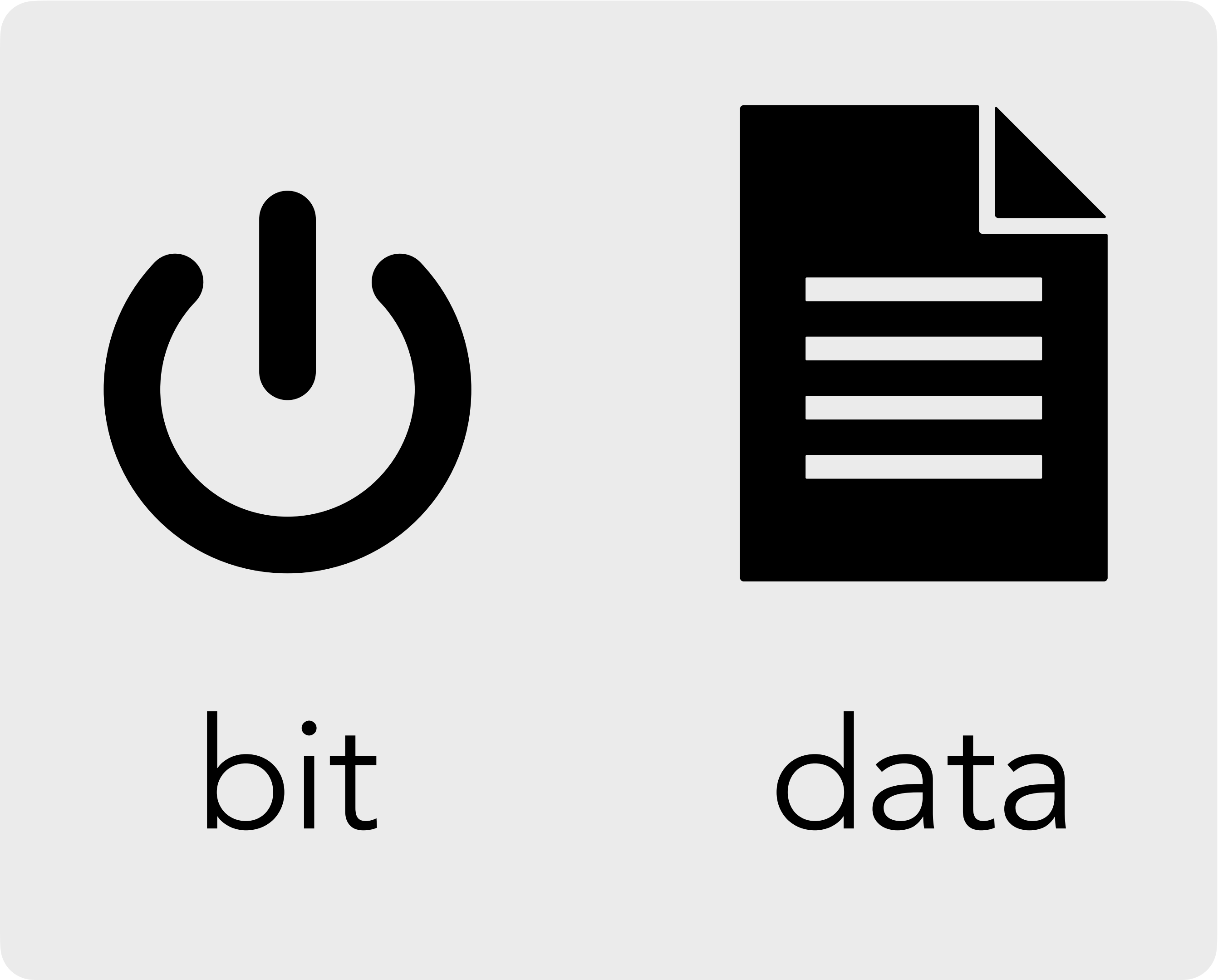
A Brief History

Organization

Mathematics of Quantum Information

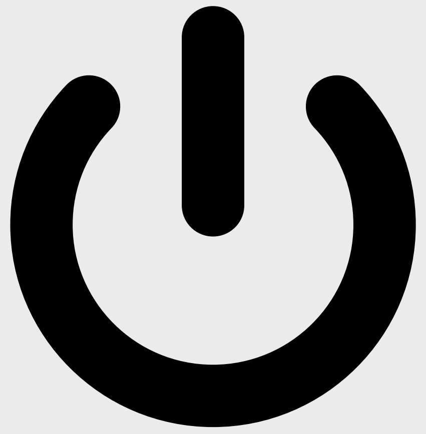
Classical Computation

Classical Computation

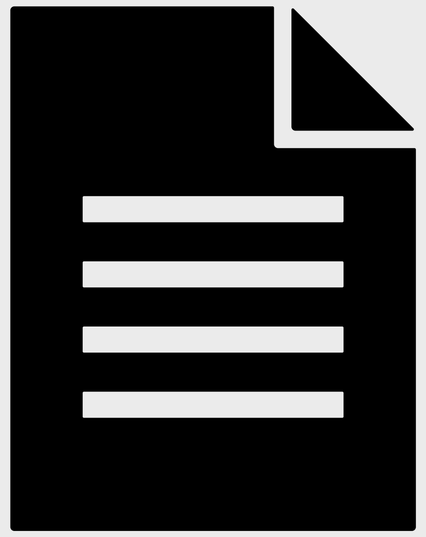


How to represent information?

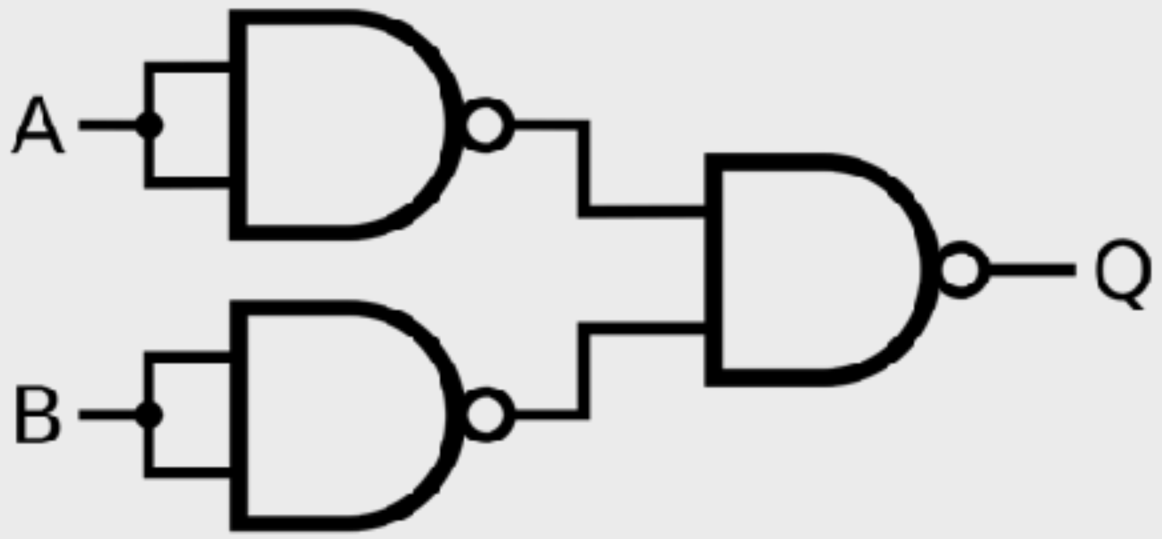
Classical Computation



bit



data

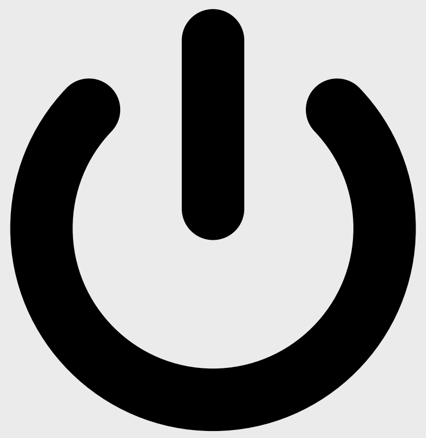


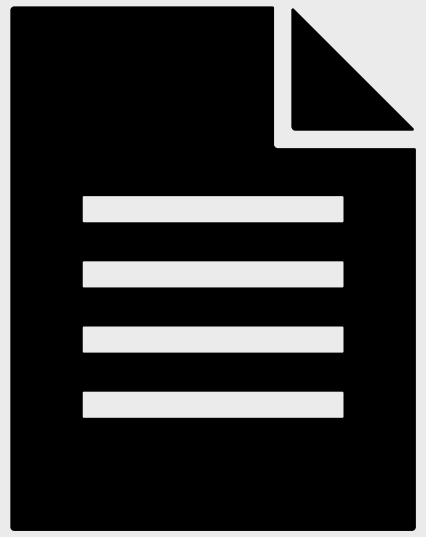
circuits

How to represent information?

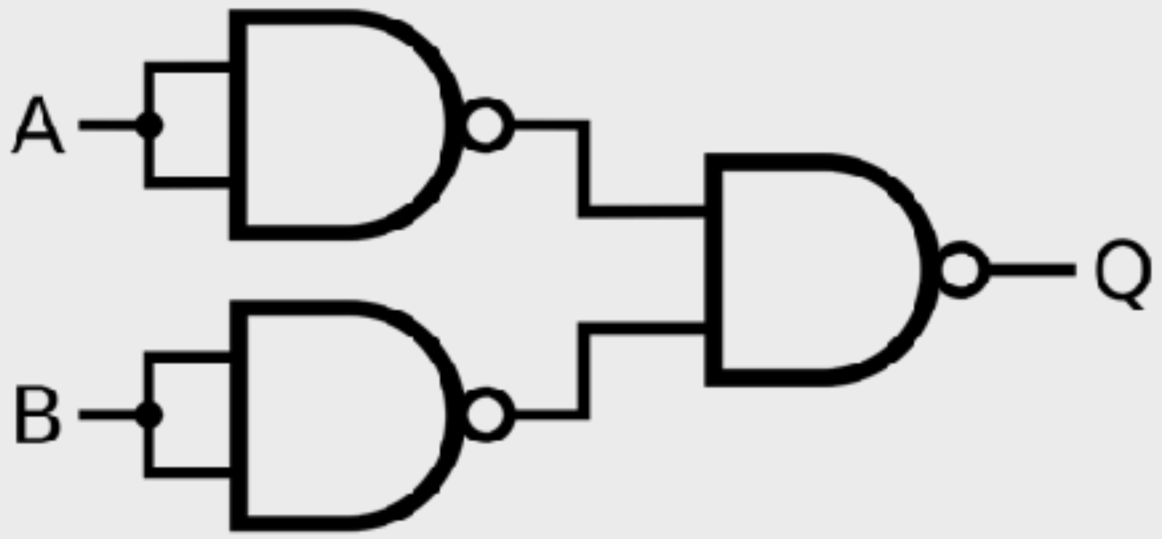
How to perform basic computation?

Classical Computation





bit data



circuits

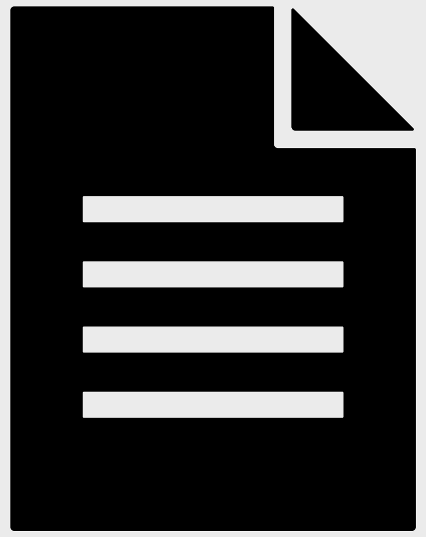
algorithms

How to represent information?

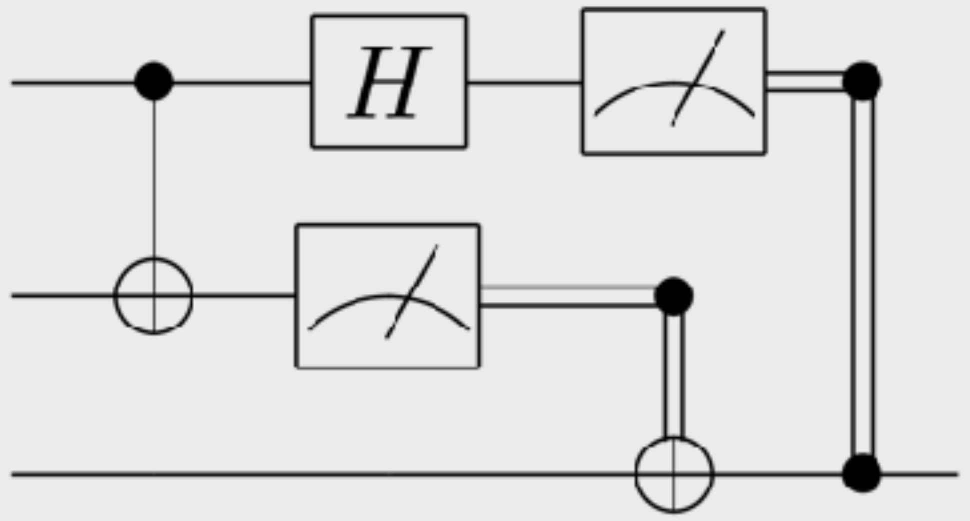
How to perform basic computation?

How to design algorithms?

Quantum Computation



qubit state



circuit

algorithm

Computation based on the principles of *quantum mechanics*

Quantum Mechanics

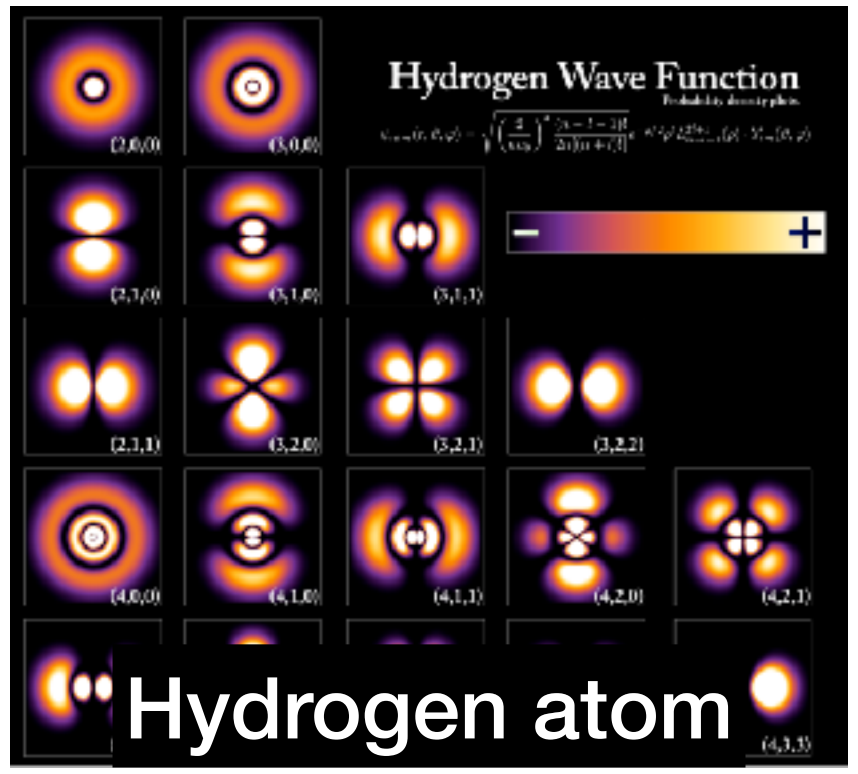
- Developed in 1920s
- Explains fundamental properties of nature at atomic and sub-atomic scales
- Classical physical theories follow from approximations at macroscopic scales

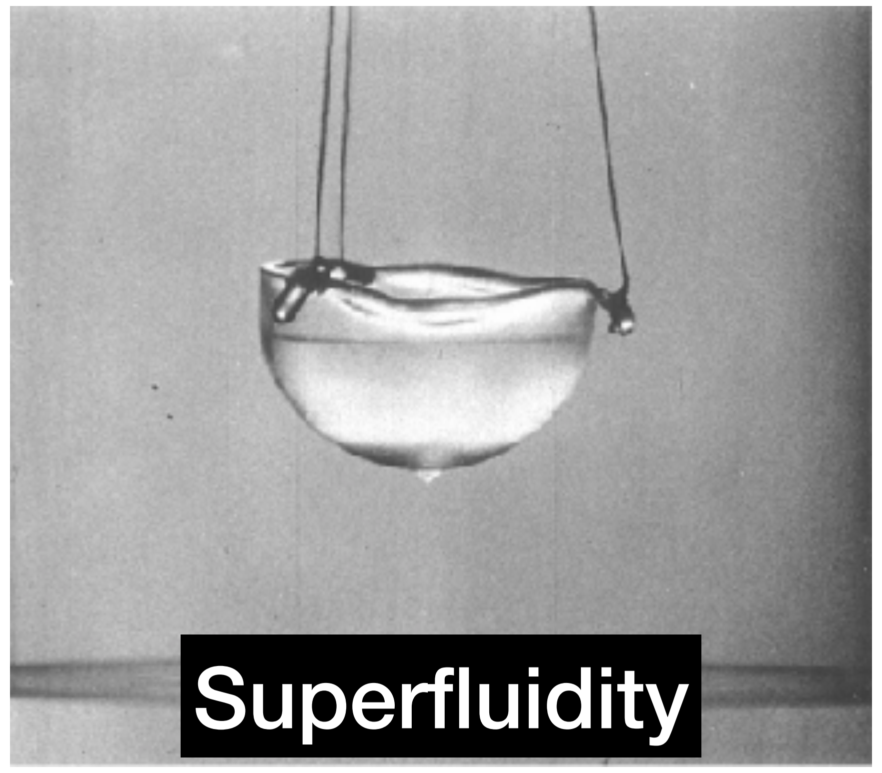
Quantum Mechanics

- Developed in 1920s

- Explains fundamental properties of nature at atomic and sub-atomic scales

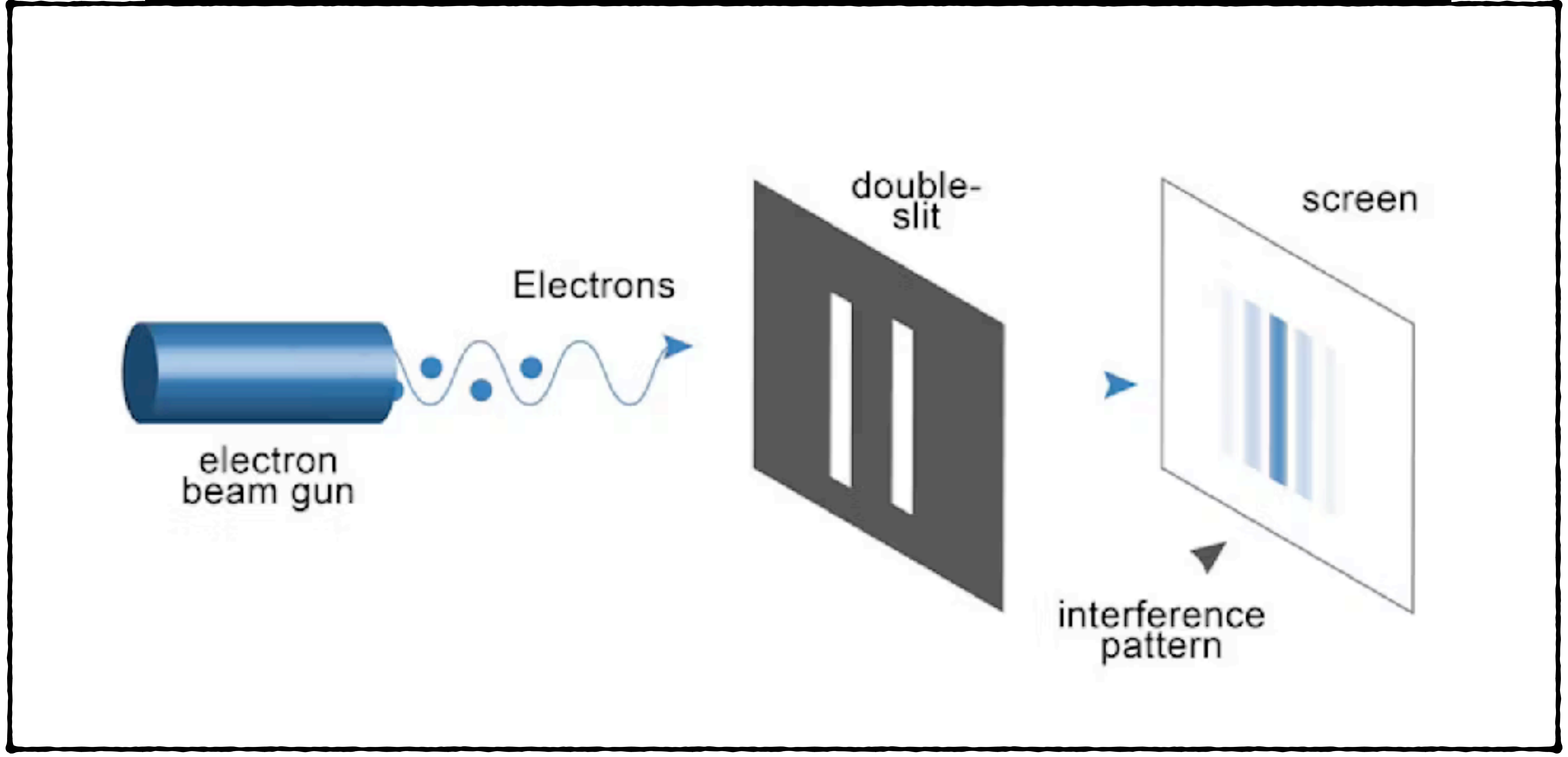
- Classical physical theories follow from approximations at macroscopic scales





Quantum Mechanics

Double-slit Experiment



Showed wave-particle duality

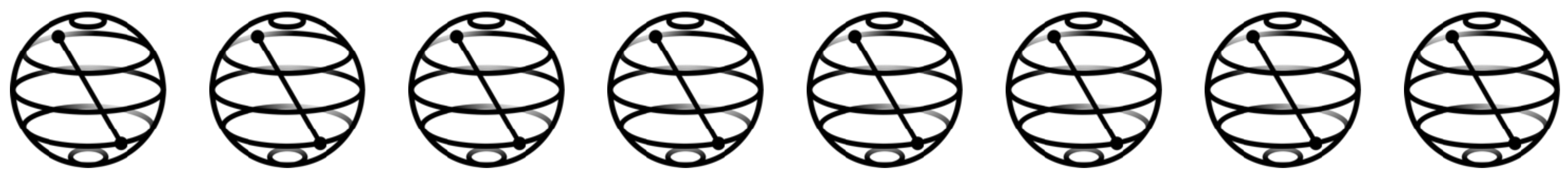
Interference

Observing which slit the electron passes through changes the outcome

Why use Quantum Mechanics for computation?

Exponentially of Quantum Mechanics

State of n particles is described by 2^n complex numbers



$$|\psi\rangle = \begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_{2^n} \end{pmatrix} \in \mathbb{C}^{2^n}$$

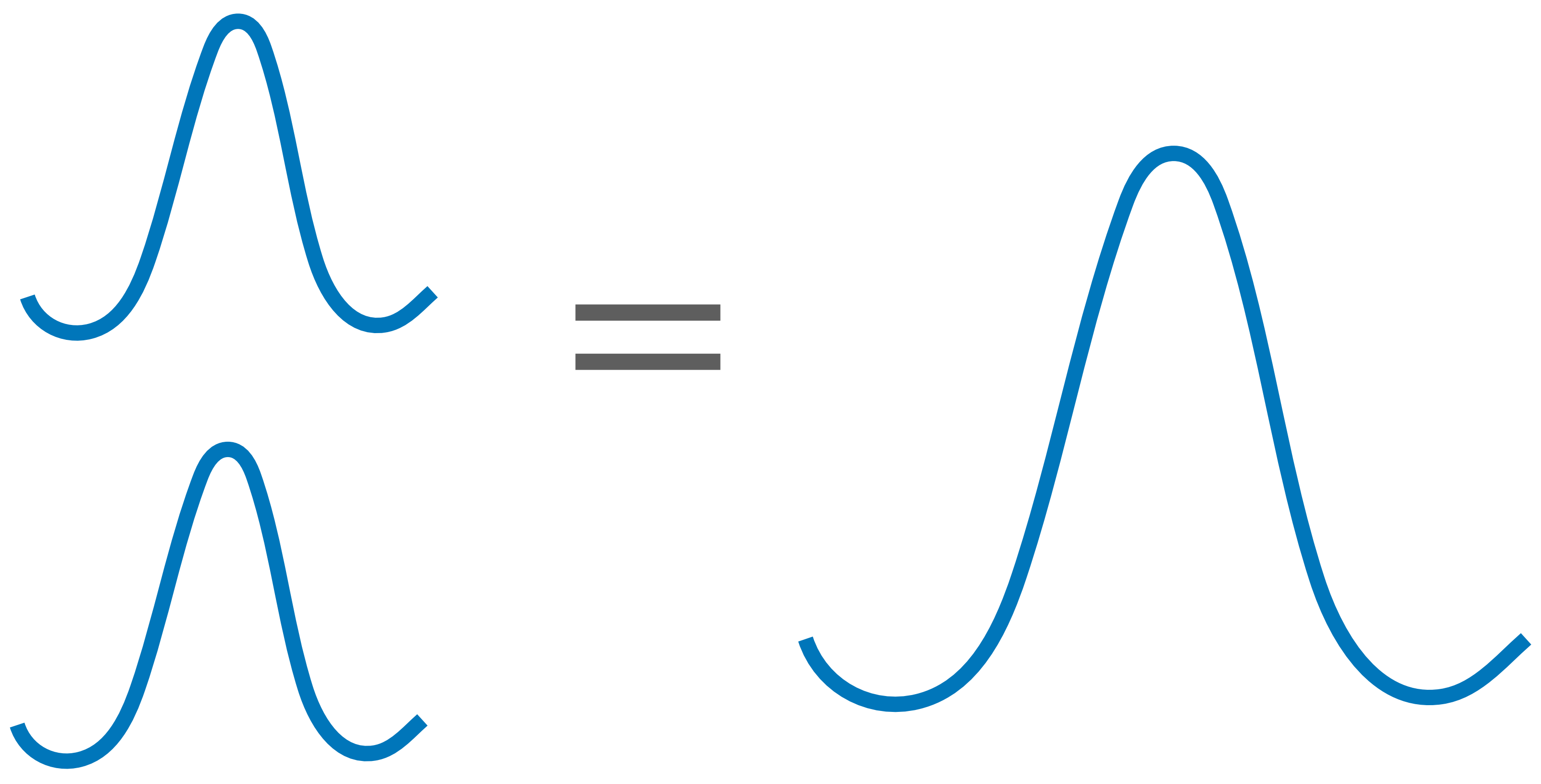
"…Nature isn't classical, damnit, and if you want to make a simulation of nature, you'd better make it quantum mechanical. By golly, it's a wonderful problem, because it doesn't look so easy."

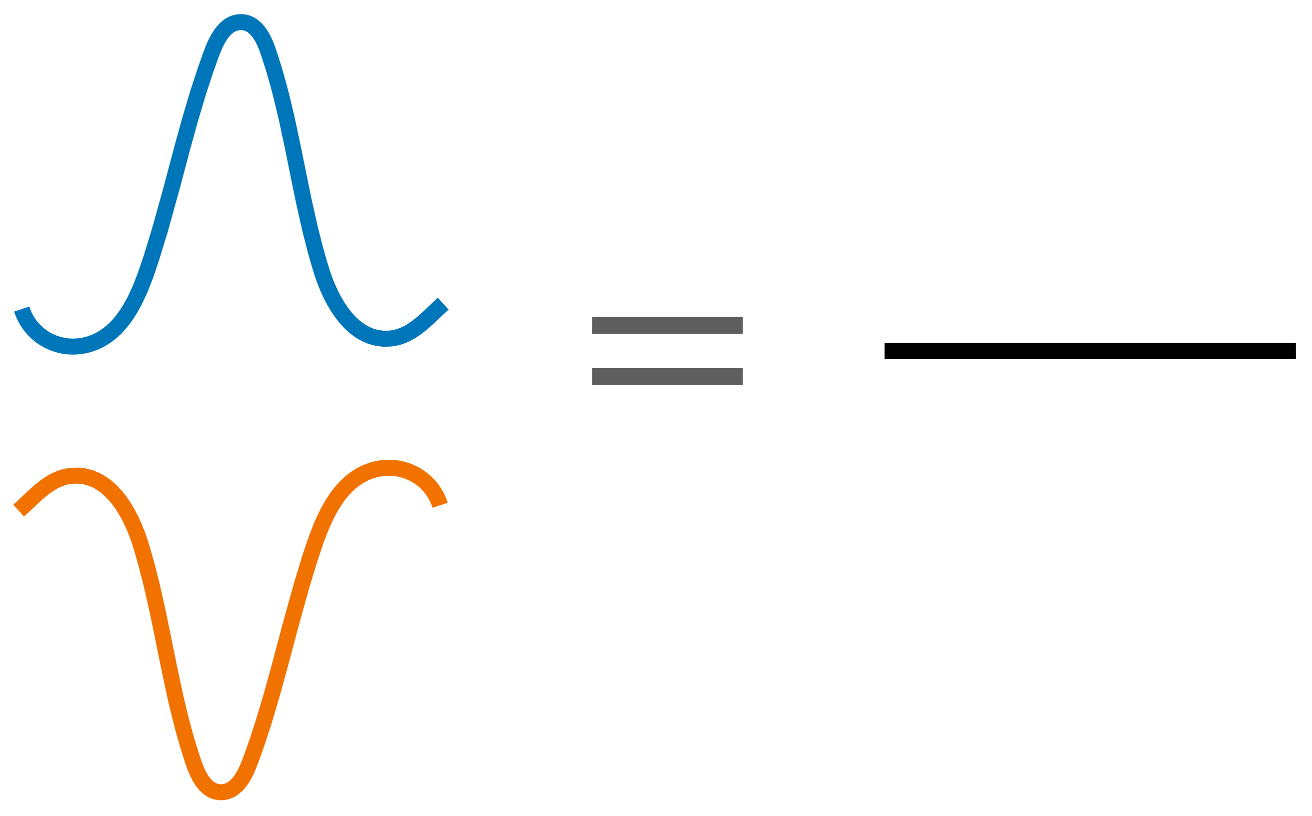
Richard Feynman (1981)

Quantum Computation

- R. Feynman, David Deutsch, Paul Benioff, Yuri Mann came up with the idea of computing based on quantum mechanical principles

- Quantum computation is about orchestrating interference in such a way that the "interference pattern" tells us something useful, e.g. the solution to a problem!





Early Days

- Feynman's motivation for quantum computers is the most obvious one: simulating quantum systems
- But to computer scientists in the 80s, this was probably a strange idea
- 1984: Deutsch found example of a (non-physics) problem with a constant factor speedup on a quantum computer
- 1992: Bernstein-Vazirani and Dan Simons found examples of problems with super-polynomial speedups on a quantum computer

Quantum Algorithm for Factoring

- Peter Shor in 1994 came up with an algorithm for factoring

Given an n-bit integer, find its prime factorization

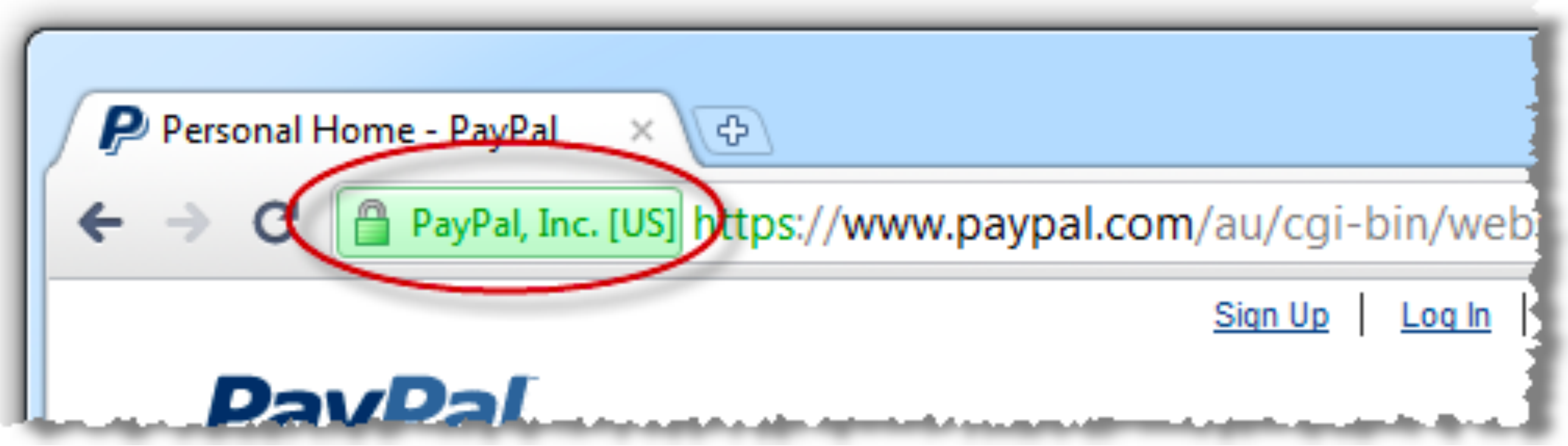
- Modern crypto systems such as RSA are based on the assumption that factoring large integers (512-1024 bit) is hard for classical computers

Quantum Algorithm for Factoring

- Peter Shor in 1994 came up with an algorithm for factoring

Given an n-bit integer, find its prime factorization

- Modern crypto systems such as RSA are based on the assumption that factoring large integers (512-1024 bit) is hard for classical computers

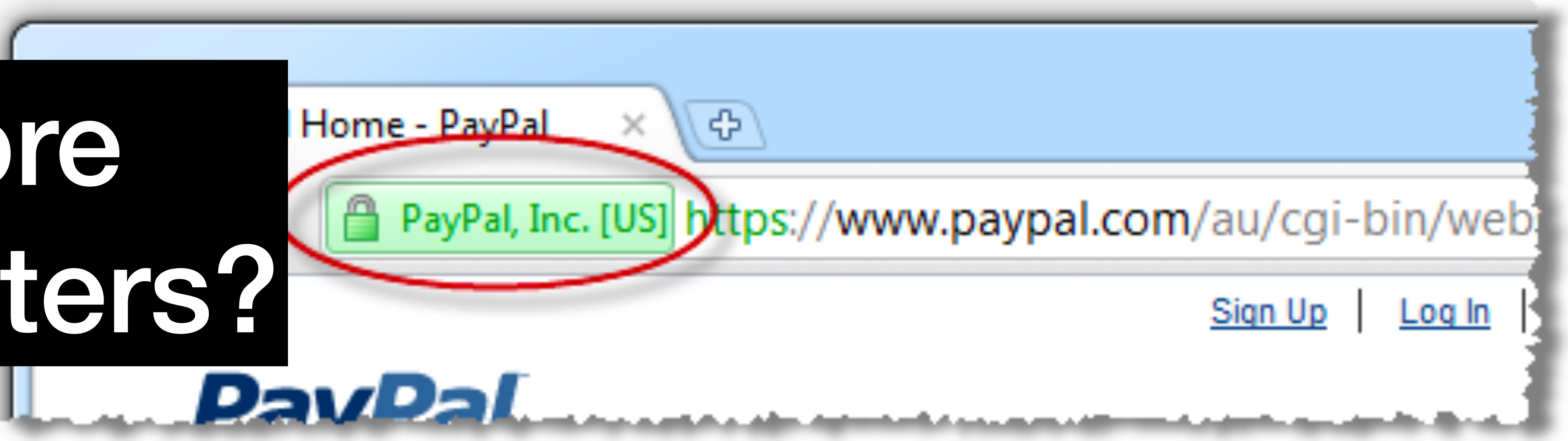


Quantum Algorithm for Factoring

- Peter Shor in 1994 came up with an algorithm for factoring

Given an n-bit integer, find its prime factorization

- Modern crypto systems such as RSA are based on the assumption that factoring large integers (512-1024 bit) is hard for classical computers



Are quantum computers more powerful than classical computers?

Present day

- **Engineering**
  primitive quantum computers are being built

- **Theoretical developments**
  new algorithms, new cryptographic protocols,
  new insights into how quantum computing compares to classical computing

- **Connections to other sciences**
  condensed matter physics, quantum gravity, materials science, chemistry,
  computer science, pure mathematics

Emerging Quantum Computers

- Until 2017 or so, quantum devices were very small ~10 qubits
- New developments in hardware in the last 5 years: Superconducting qubits, ion traps, photonic systems, topological qubits, …
- Many companies racing to build large-scale quantum computers

Microsoft Google IBM amazon rigetti IONQ Alibaba XANADU D-Wave

Emerging Quantum Computers

- **Present day**

  quantum computers with ~100 qubits

- **Problem**

  devices are very noisy and

  not capable of running Shor's algorithm

- **"NISQ" era**

  Noisy Intermediate-Scale

  Quantum Computers

Emerging Quantum Computers

- **Present day**

  quantum computers with ~100 qubits

- **Problem**

  devices are very noisy and

  not capable of running Shor's algorithm

- **"NISQ" era**

  Noisy Intermediate-Scale

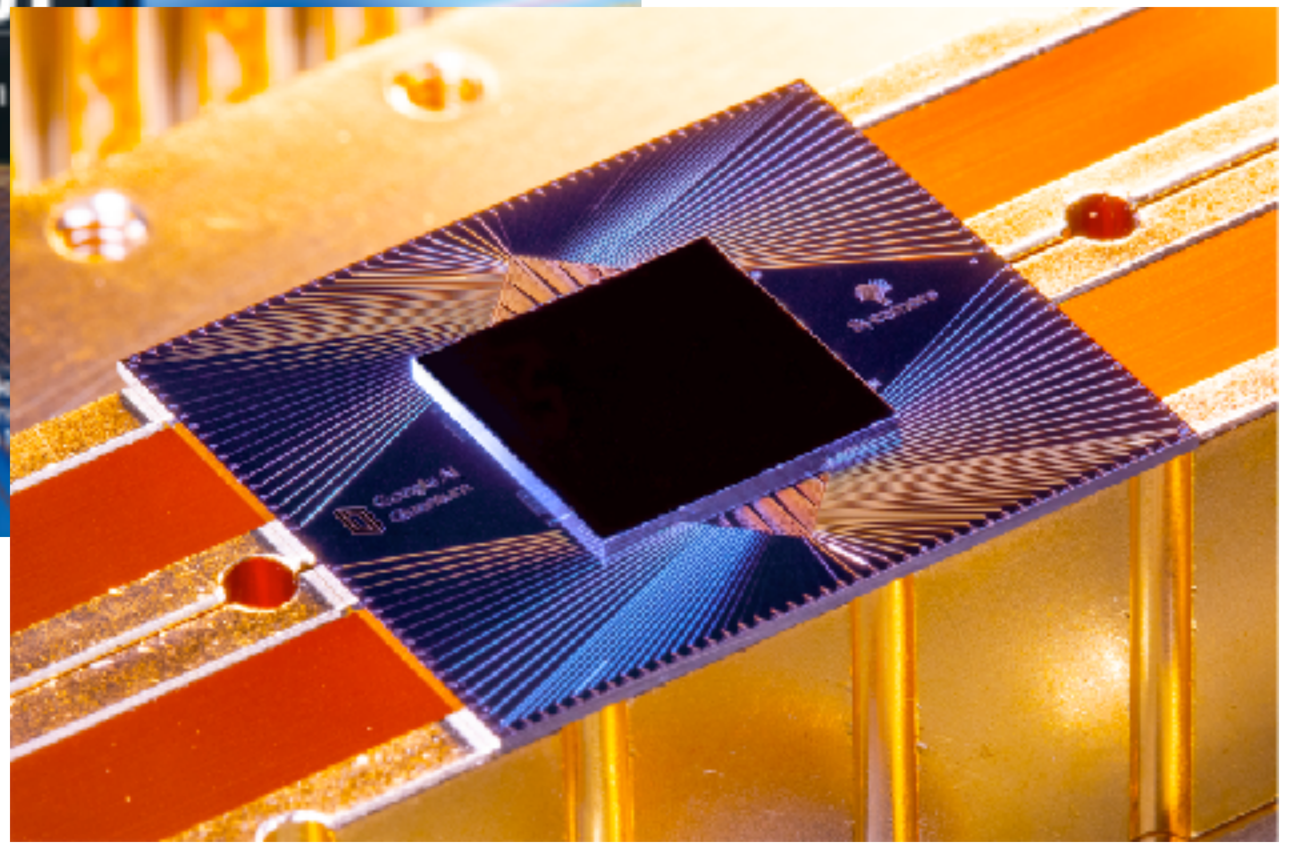
  Quantum Computers

Can we solve classically intractable tasks with NISQ devices?

"Quantum Advantage" or "Quantum Supremacy"

- In 2019, Google announced that they had achieved "Quantum Supremacy" using their 53-qubit Sycamore quantum processor

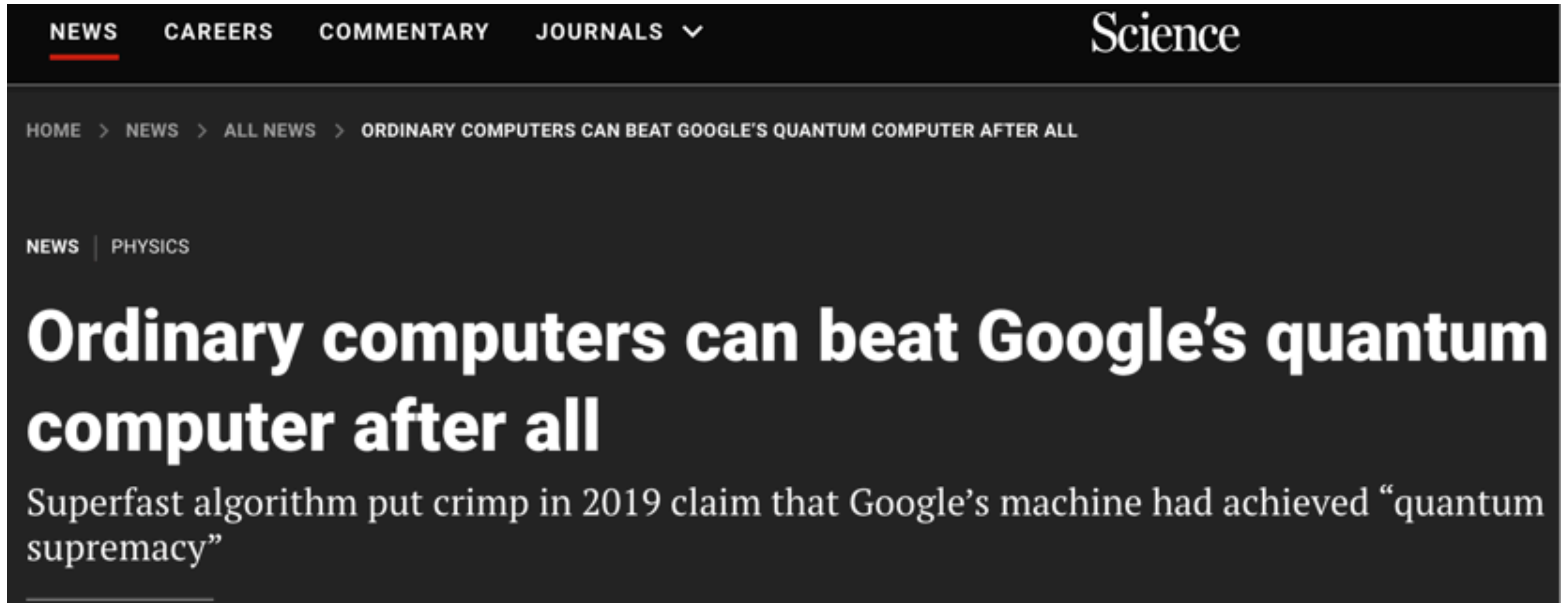
- **Quantum supremacy:** a convincing real-world demonstration of a quantum computer accomplishing a task that cannot feasibly be performed by a classical computer.



Quantum vs Classical

- Google's processor took 200 seconds and they estimated that a state-of-the-art supercomputer would require ~10,000 years

- Clever classical algorithms by various groups showed that the task is feasible on classical super-computers



NEWS CAREERS COMMENTARY JOURNALS Science

HOME > NEWS > ALL NEWS > ORDINARY COMPUTERS CAN BEAT GOOGLE'S QUANTUM COMPUTER AFTER ALL

NEWS | PHYSICS

Ordinary computers can beat Google's quantum computer after all

Superfast algorithm put crimp in 2019 claim that Google's machine had achieved "quantum supremacy"

Most recent estimates by Google itself suggests that it would take 6.18s with classical supercomputers to do the 2019 experiments

Quantum vs Classical

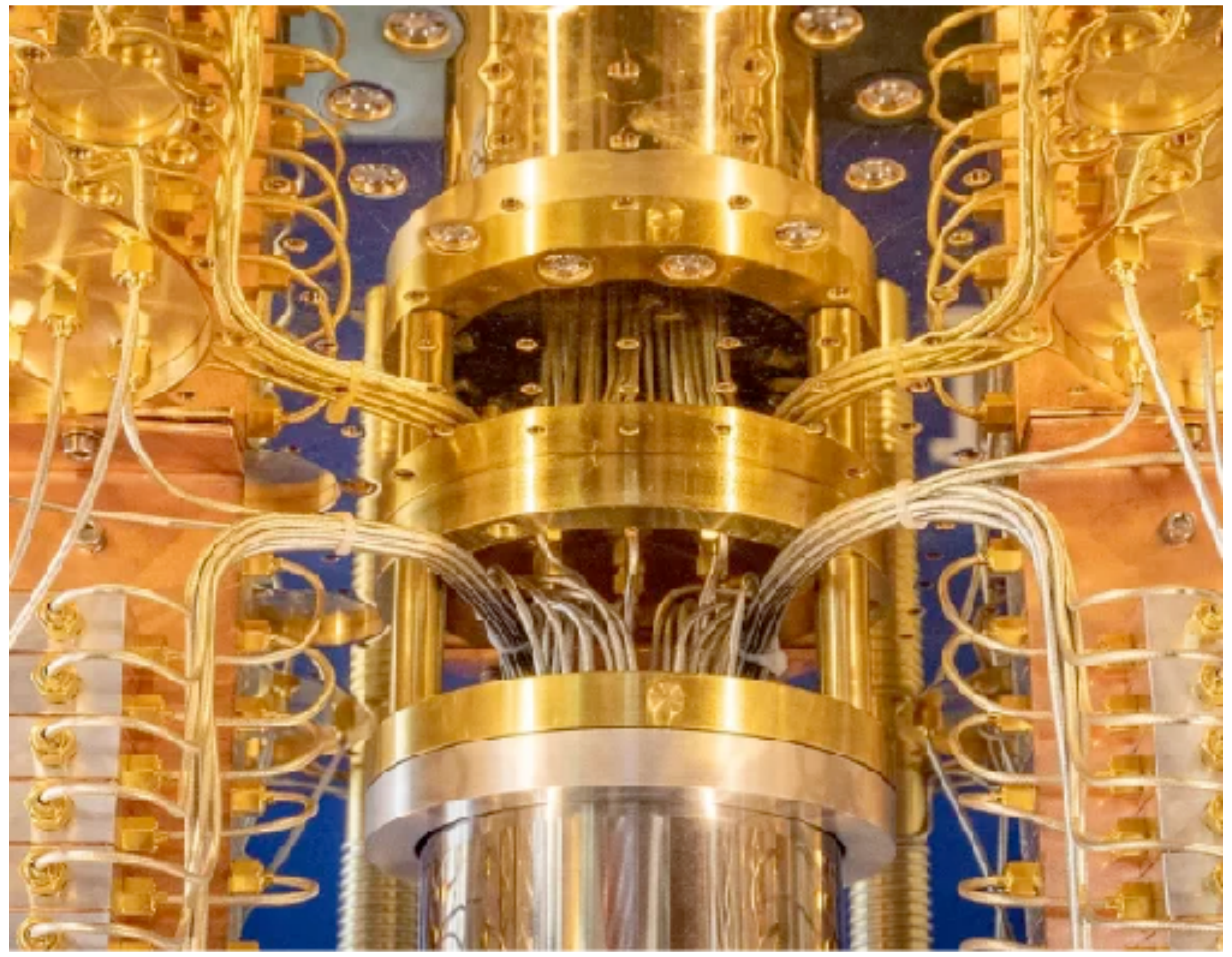
- Google in 2023 proposed a 70 qubit experiment which they estimate would require 47 years on a classical supercomputer

- Other research groups have also announced quantum advantage results based on other computational tasks

- The quest to find clever algorithm and provably demonstrate quantum advantage continues…

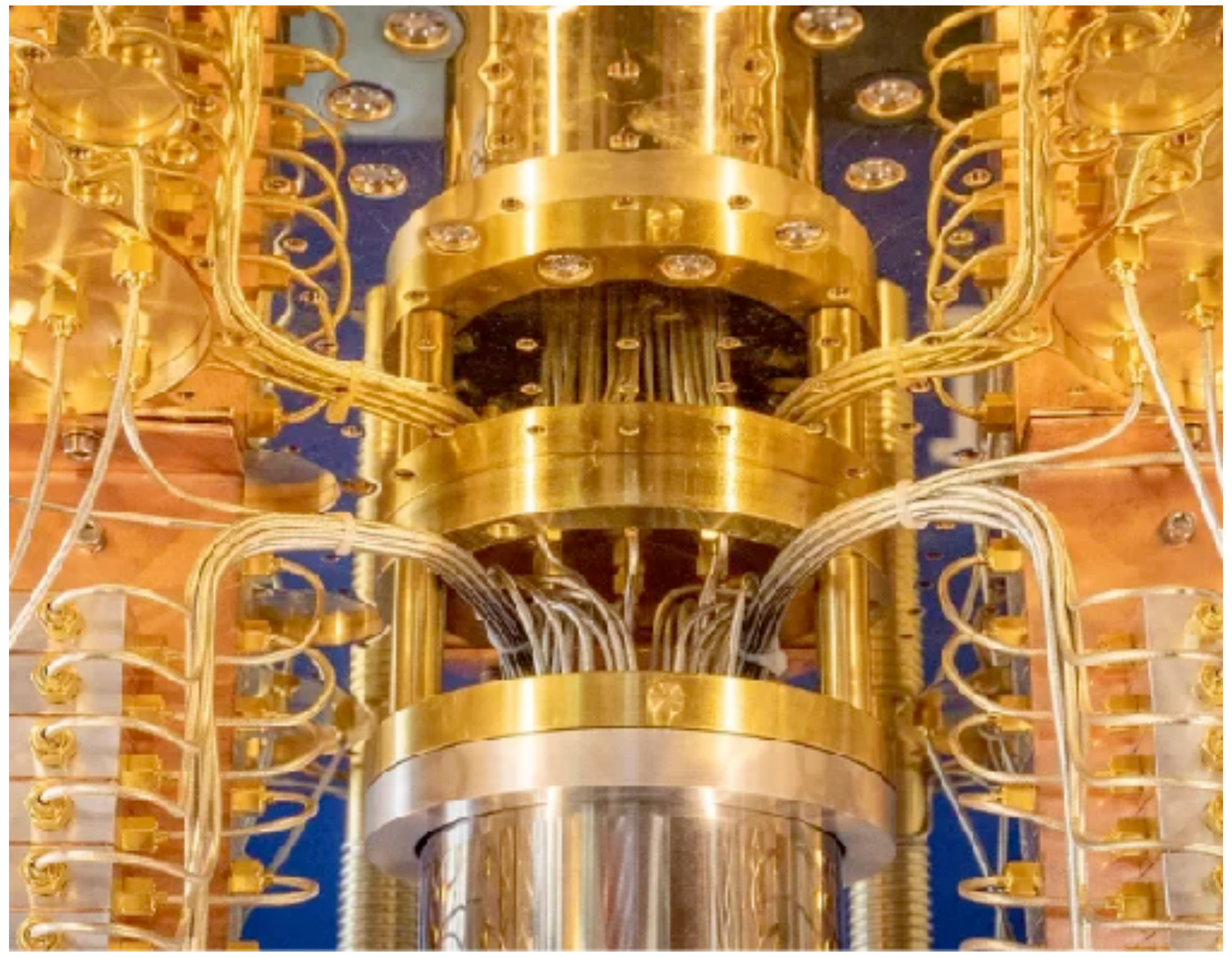
Summary of Hardware Efforts

- We are in the **"NISQ"** era
- There is a qubit-race going on, but qubit count is not everything!
- Scaling up (i.e. more qubits, better qubits) is a tough engineering challenge, but no fundamental obstacles to building QCs with 10^6 noiseless qubits



- Still, large-scale fault-tolerant QCs look like they are many years away

Summary of Hardware Efforts



- We are in the **"NISQ"** era
- There is a qubit-race going on, but qubit count is not everything!
- Scaling up (i.e. more qubits, better qubits) is a tough engineering challenge, but no fundamental obstacles to building QCs with 10^6 noiseless qubits
- Still, large-scale fault-tolerant QCs look like they are many years away

What interesting problems can be solved with near-term quantum computers?

Quantum Algorithms

- **Exponential speedups** for structured, algebraic problems
  - Factoring (Shor's algorithm)
  - Hidden subgroup problem
- **Polynomial speedups** for unstructured search problems
  - Grover search
- Hope: **Exponential speedups** for simulating quantum systems
  - Design materials
  - Understand quantum phenomena

Quantum Algorithms

- **Exponential speedups** for structured, algebraic problems

  N = pq

  Factoring (Shor's algorithm)

  Hidden subgroup problem

- **Polynomial speedups** for unstructured search problems

  Grover search

- Hope: **Exponential speedups** for simulating quantum systems

  Design materials

  Understand quantum phenomena

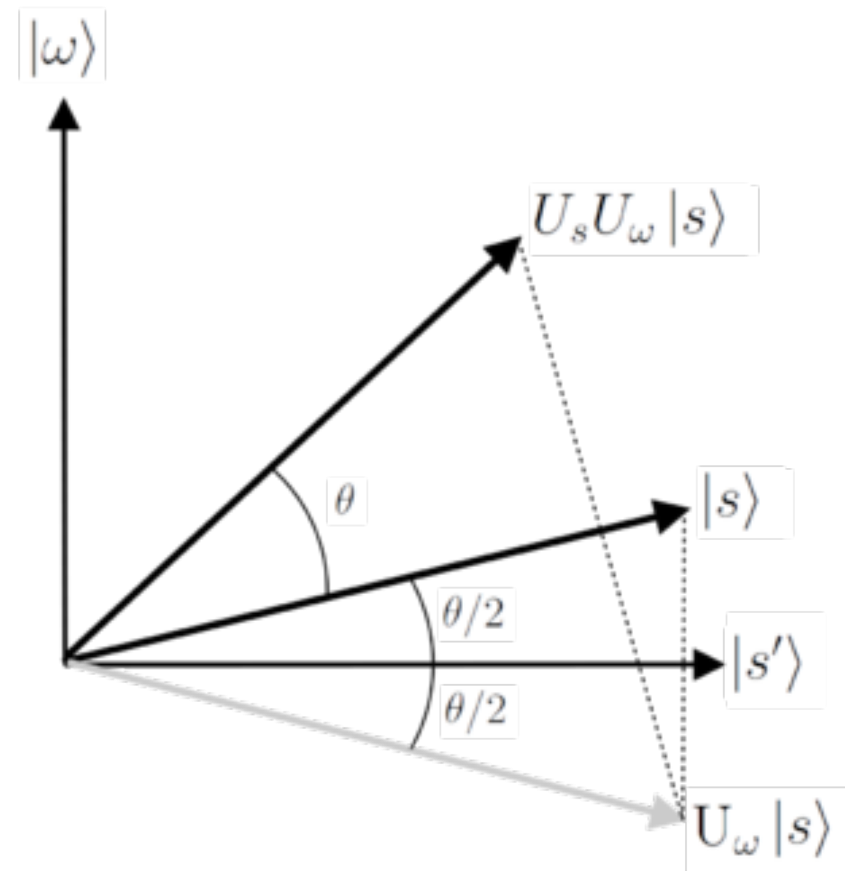
Quantum Algorithms

- **Exponential speedups** for structured, algebraic problems

  Factoring (Shor's algorithm)

  Hidden subgroup problem

N = pq



- **Polynomial speedups** for unstructured search problems

  Grover search

- Hope: **Exponential speedups** for simulating quantum systems

  Design materials

  Understand quantum phenomena

Quantum Algorithms

- **Exponential speedups** for structured, algebraic problems

  Factoring (Shor's algorithm)

  Hidden subgroup problem

- **Polynomial speedups** for unstructured search problems

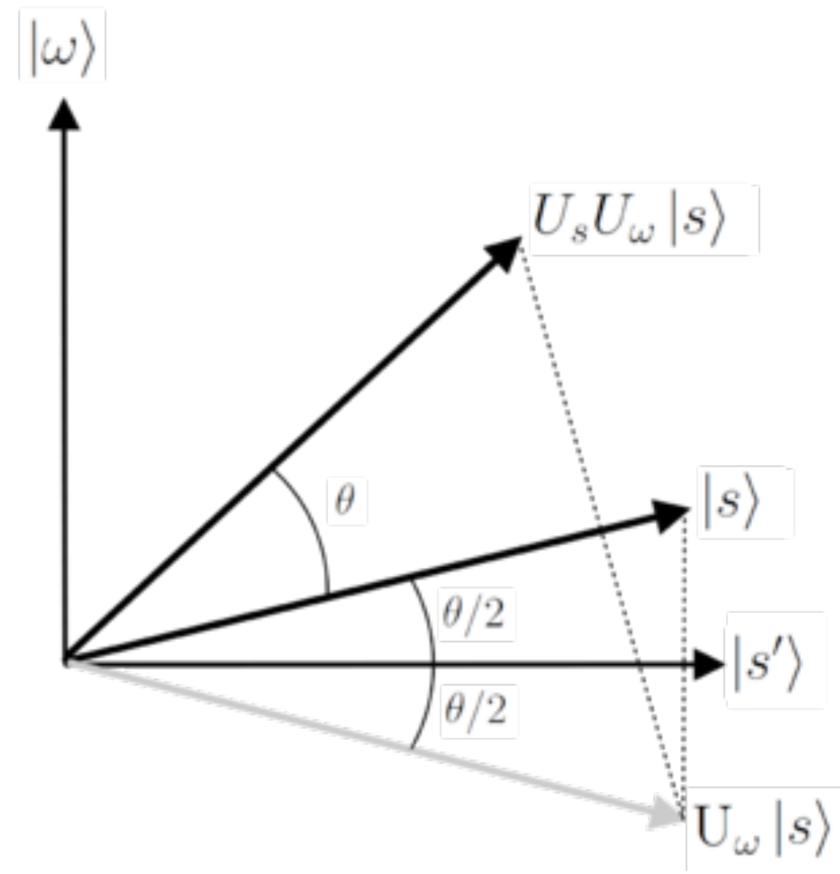
  Grover search

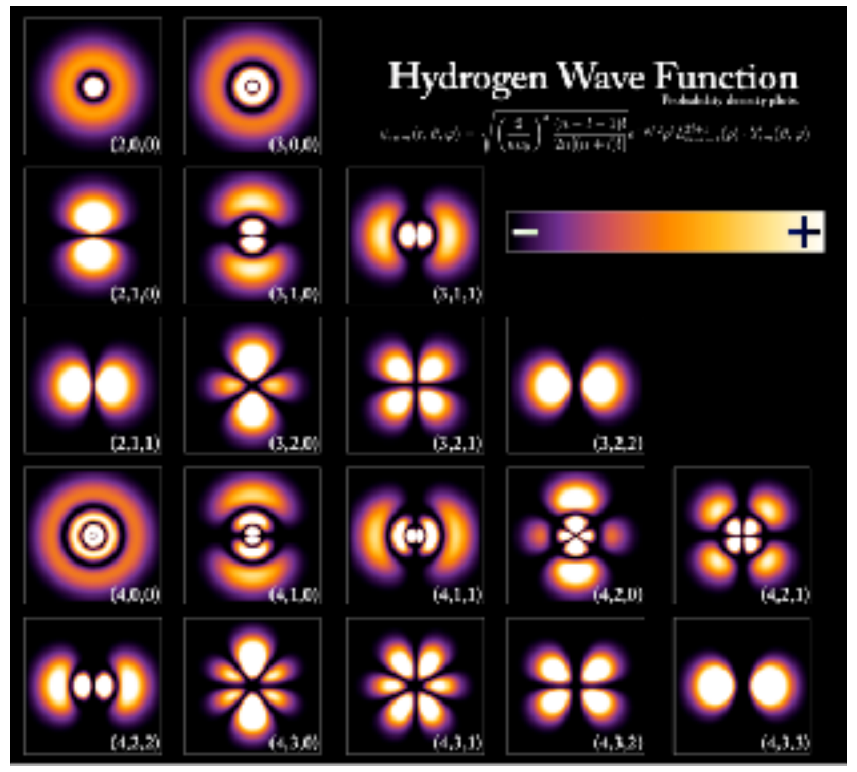
- Hope: **Exponential speedups** for simulating quantum systems

  Design materials

  Understand quantum phenomena

N = pq





Quantum Algorithms

- **Near-term quantum algorithms**

  Variational Quantum Eigensolvers

  Classical-quantum hybrid algorithms

- **Quantum Machine Learning**

  Solving linear systems/SDPs/Convex programs

  Recommendation systems

Quantum Algorithms

- **Near-term quantum algorithms**

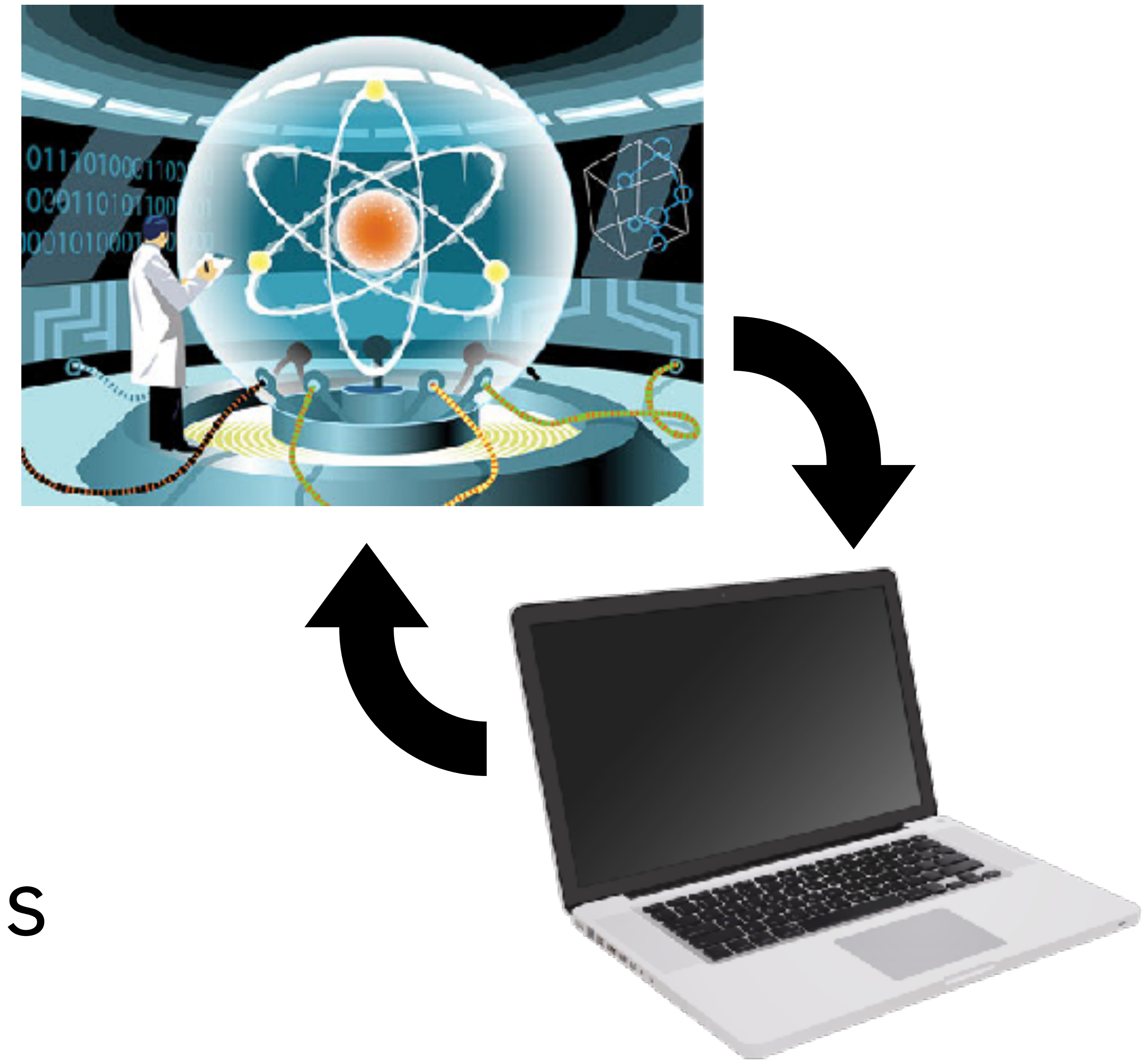
  Variational Quantum Eigensolvers

  Classical-quantum hybrid algorithms

- **Quantum Machine Learning**

  Solving linear systems/SDPs/Convex programs

  Recommendation systems



Quantum Algorithms

- **Near-term quantum algorithms**

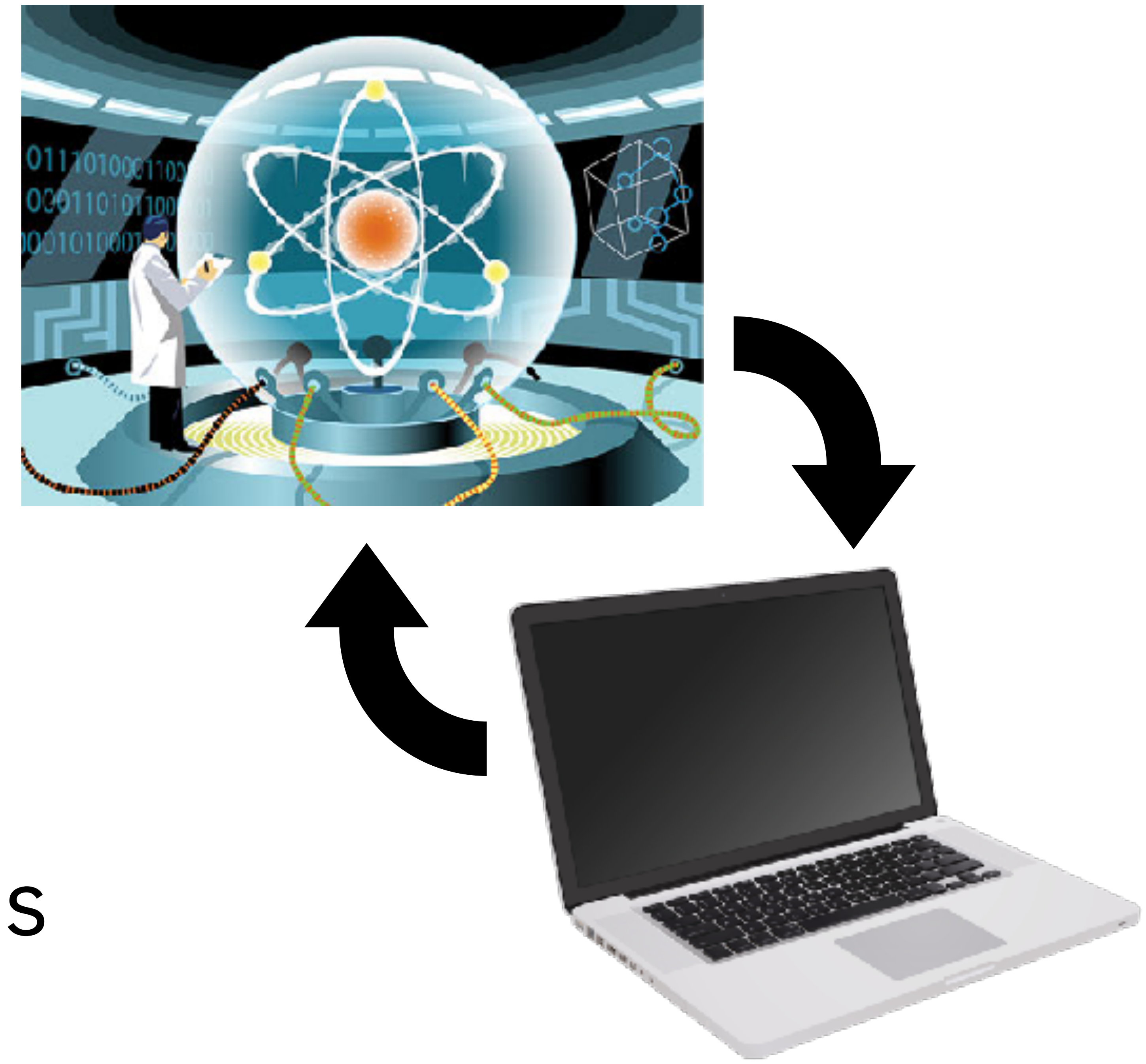
  Variational Quantum Eigensolvers

  Classical-quantum hybrid algorithms

- **Quantum Machine Learning**

  Solving linear systems/SDPs/Convex programs

  Recommendation systems



What types of problems admit a quantum advantage?

Connections with Fundamental Physics

- **Quantum Gravity**

  The key to a theory of Quantum Gravity could be quantum entanglement, and quantum error correcting codes.

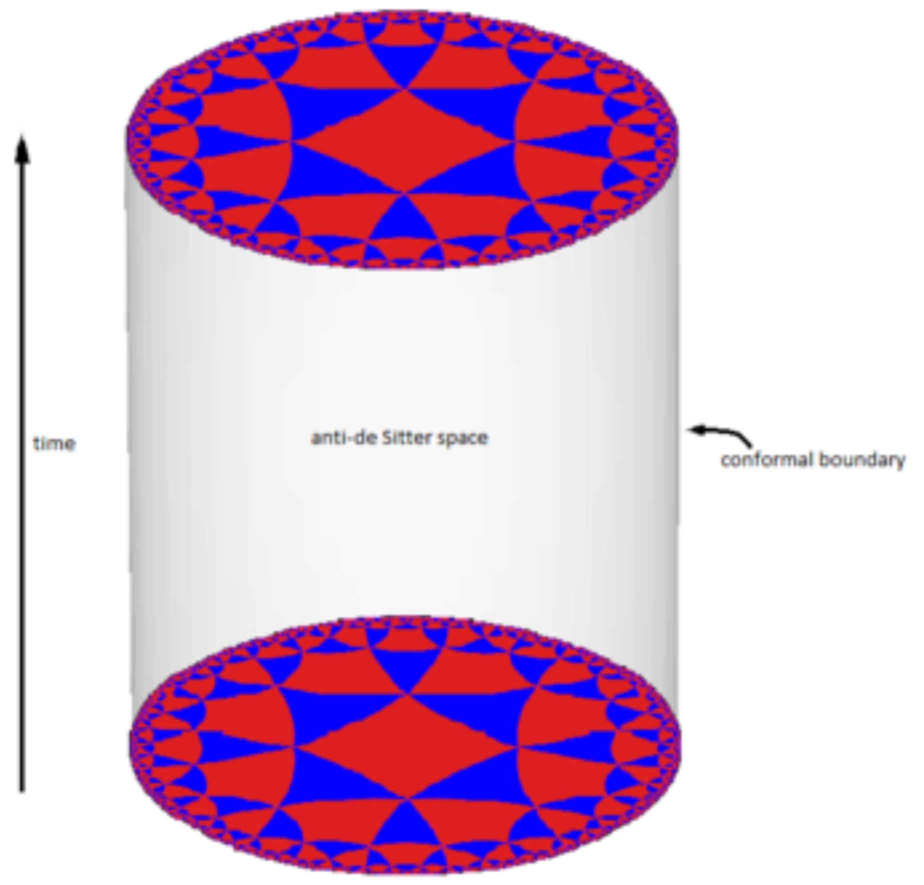
- **Black Holes**

  The "**Blackhole Firewall Paradox**" is an issue about quantum information, and possible resolutions involve quantum cryptography.

Connections with Fundamental Physics

- **Quantum Gravity**

  The key to a theory of Quantum Gravity could be quantum entanglement, and quantum error correcting codes.



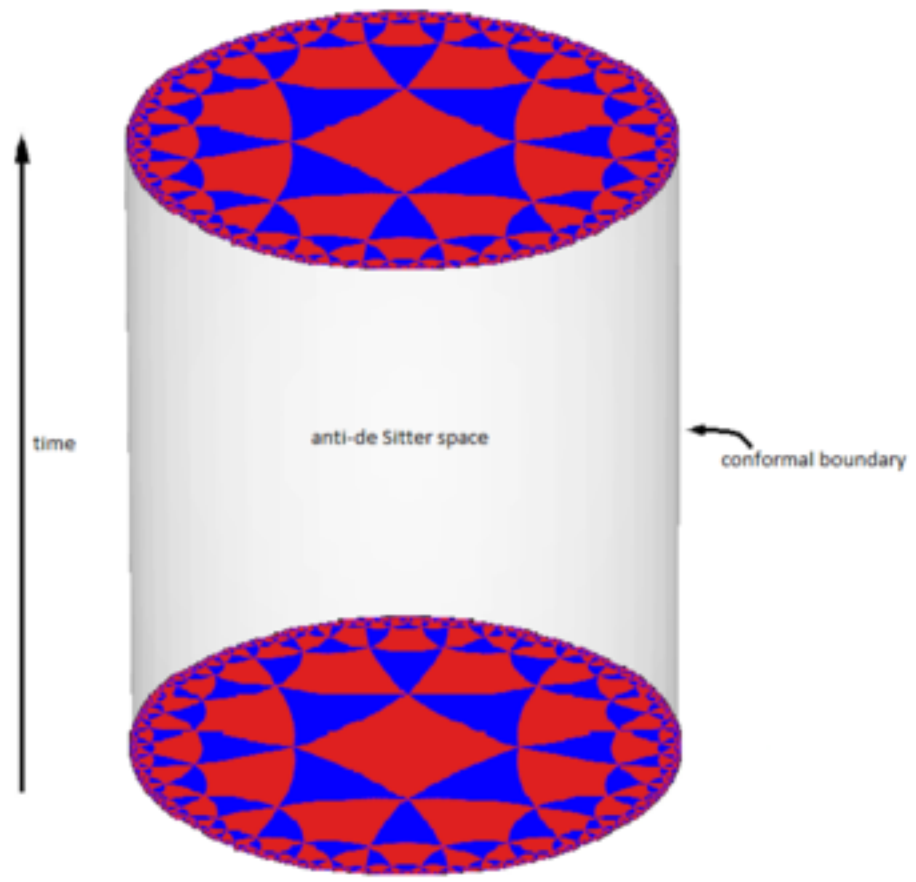
- **Black Holes**

  The "**Blackhole Firewall Paradox**" is an issue about quantum information, and possible resolutions involve quantum cryptography.

Connections with Fundamental Physics

- **Quantum Gravity**

  The key to a theory of Quantum Gravity could be quantum entanglement, and quantum error correcting codes.



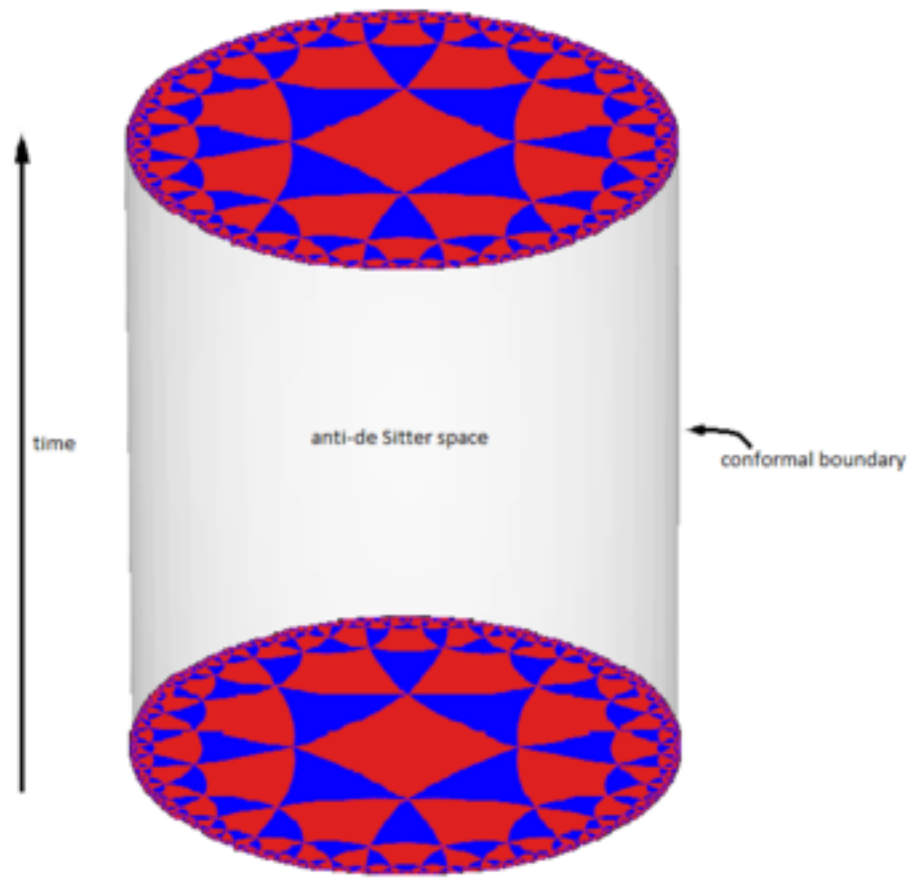
- **Black Holes**

  The "**Blackhole Firewall Paradox**" is an issue about quantum information, and possible resolutions involve quantum cryptography.

Connections with Fundamental Physics

- **Quantum Gravity**

  The key to a theory of Quantum Gravity could be quantum entanglement, and quantum error correcting codes.



- **Black Holes**

  The "**Blackhole Firewall Paradox**" is an issue about quantum information, and possible resolutions involve quantum cryptography.

What can quantum computing tell us about nature?

What you can hope to learn from this class

- Learn the basic principles of quantum information and computation
- Learn fundamental quantum algorithms and quantum protocols
- Get an idea of the current state of the field
- Get an idea of what the big questions are

Target Audience

- **Who this class is intended for**
  - Computer Scientists
  - People with a solid background in linear algebra and probability
  - People who want to learn about the **theory** of quantum computing
- **Who this class is NOT intended for**
  - People who want to learn how to build a quantum computer
  - People who want to learn quantum programming
  - People who want to learn quantum physics

Prerequisites

- **Basic Linear Algebra** Important

  Vector space (subspaces, orthogonal complements, dimension, linear independence, basis, span,…). Inner products. Row vs column vectors. Linear operators (invertibility, matrix representation, composition of linear operators, transpose, adjoint). Eigenvalues and eigenvectors. Trace.

- **Basic Probability Theory** Important

  Bayes' rule, conditional distributions. Joint probability spaces. Independent random variables. Mean, variance, etc.

- **Theoretical Computer Science** Very helpful

  Analysis and design of algorithms. Complexity theory. Discrete math.

A Brief History

Organization

Mathematics of Quantum Information

Grading

- **Homeworks 30%**

  Homework 0 due on Jan 30th, 9pm

- **Midterm and Final Exam 30% each**
- **Group Participation 10%**

- Homework 0 (5% of your grade, cannot be dropped), Homeworks 1-6 (lowest scoring homework dropped, each non-dropped homework 5% of your grade)
- Homework 0 submitted individually, afterwards submission in groups of up to three
- 3 late submission tokens: extend deadline by 24 hours
- No collaboration on homework 0. For later homeworks, free to collaborate with anyone in the class but not allowed to look up solutions online or use tools like GPT

Class Resources

- **Course Webpage:** https://courses.grainger.illinois.edu/cs498qcg

Basic Information
Lecture Notes
Additional Resources

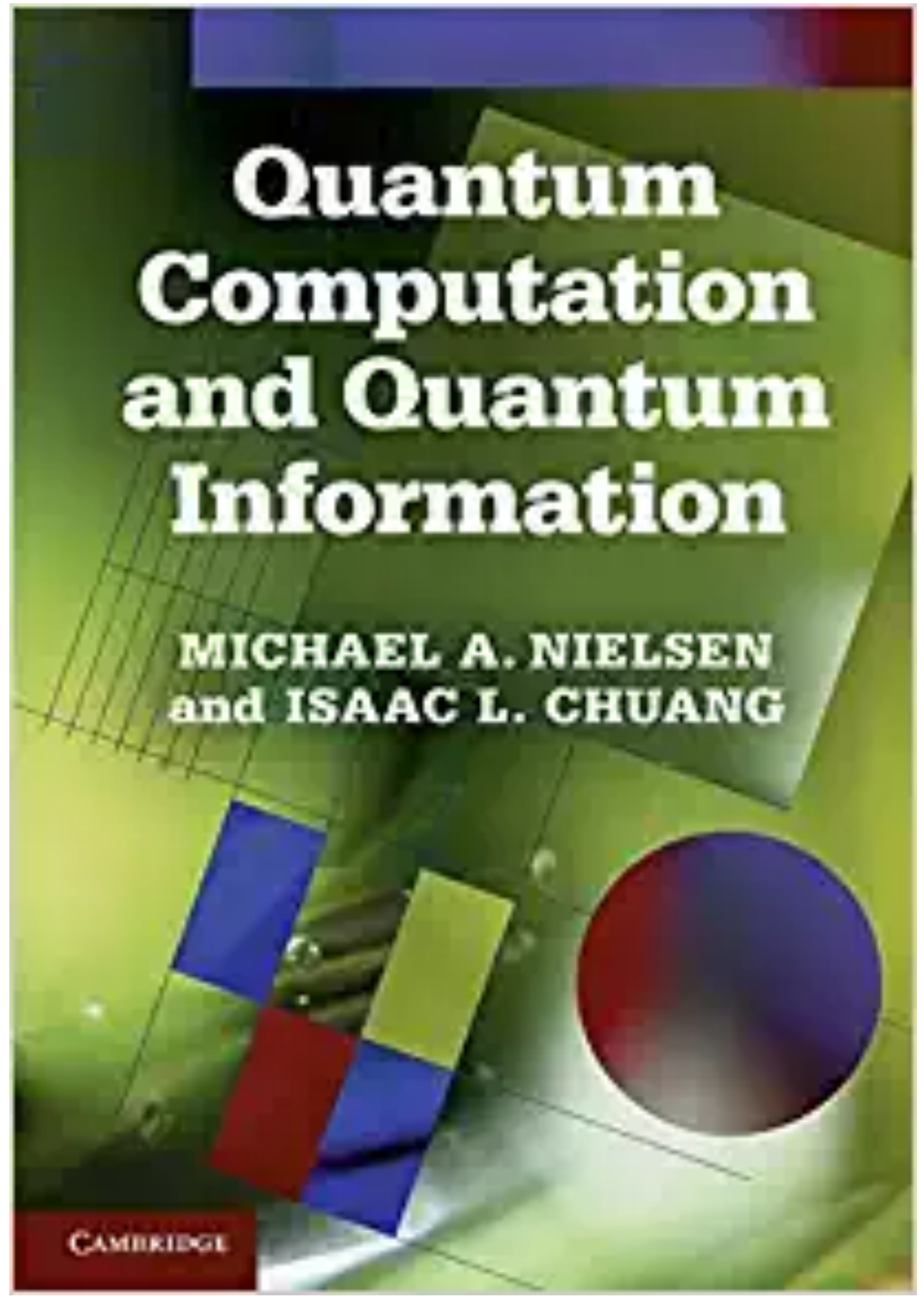
- **Course Announcements, Policies, Homework, Q&A posted on Ed Discussion**

  Use the **chat feature** on Ed Discussion to send a direct message to the course staff instead of email

- **Homework submission:** Gradescope

- **Office Hours:** Makrand (Thursdays 10:45am-noon in Siebel 3222)
  Yuchen (Tuesdays 1-2pm in Siebel Basement, starting January 28th)

Textbook and Other Resources



Recommended Textbook

- Course by Andrea Coladangelo at University of Washington
- Course by Henry Yuen at Columbia
- Course by Ryan O'Donnell at CMU
- Lecture Notes by Scott Aaronson at UT Austin
- Lecture Notes by Ronald de Wolf at University of Amsterdam

*Some of the material in this course will be based on the above courses
You are encouraged to check them out for different perspectives

A Brief History

Organization

Mathematics of Quantum Information