Quantum Computing

Prof. Jim Marshall

Fall 2022
Sarah Lawrence College

science.slc.edu/jmarshall/quantum

What is Quantum Computing?

The effort to design and build computers that perform computations by exploiting the weird properties of quantum physics

- Ordinary computers rely on **classical physics** in an essential way to perform computations
- Quantum computers rely on **quantum physics** in an essential way to perform computations

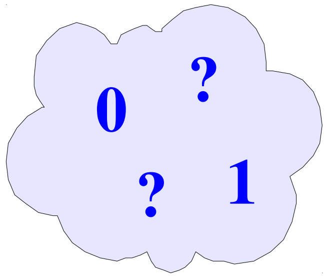
What is Quantum Computing?

The effort to design and build computers that perform computations by exploiting the weird properties of quantum physics

- Weird Property #1: **Superposition**
- Weird Property #2: **Entanglement**

What is Quantum Computing?

- A **conventional bit**: either definitely **0** or definitely **1** (e.g., voltage on a wire)
- A **quantum bit** (**qubit**):



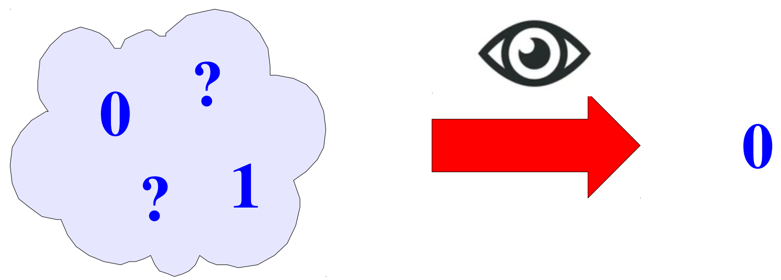
"superposition of states"

(e.g., spin of an electron, polarization of a photon)

- To completely describe the state of a **conventional bit**, we need a **single binary number** (e.g., **0** or **1**)
- To completely describe the state of a **qubit**, we need **two complex numbers** (e.g., **0.5+0.5*i*** and **0.5–0.5*i***)

What is Quantum Computing?

- When we **observe** or **measure** a qubit, it probabilistically "collapses" to either 0 or 1



- The two **complex numbers** determine the **probabilities**

- These numbers **cannot** be directly observed

- After measurement, the qubit behaves like (the same) ordinary **conventional bit** from then on, no matter how many times we re-measure it

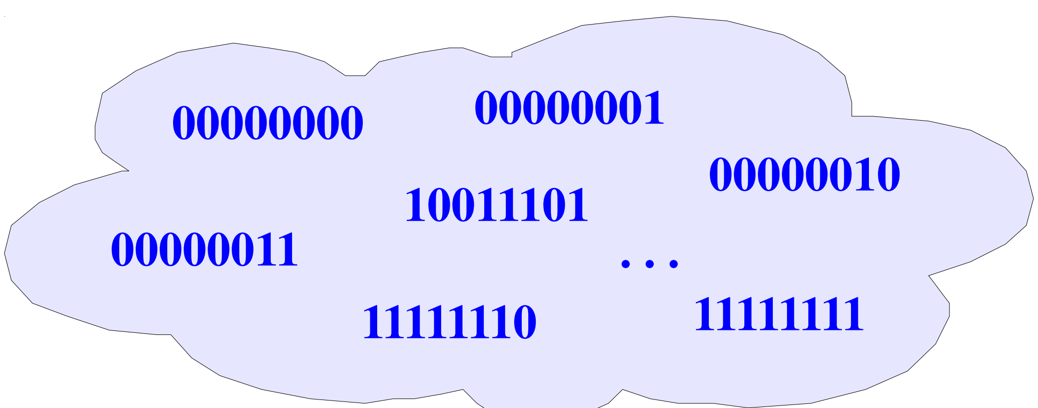
What is Quantum Computing?

- State of a conventional **8-bit** memory register:

10011101

8 binary numbers representing the single 8-bit pattern

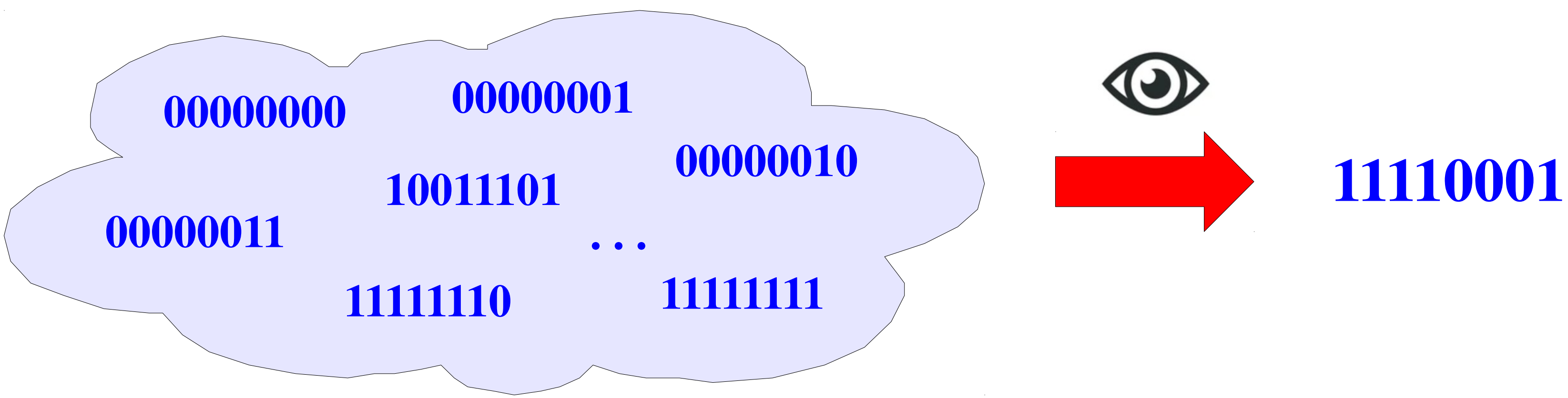
- State of an **8-qubit** quantum memory register:



256 complex numbers representing all 256 possible 8-bit patterns at once!

What is Quantum Computing?

- When we **measure** the register, it probabilistically “collapses” to **one** of the 256 possible bit patterns

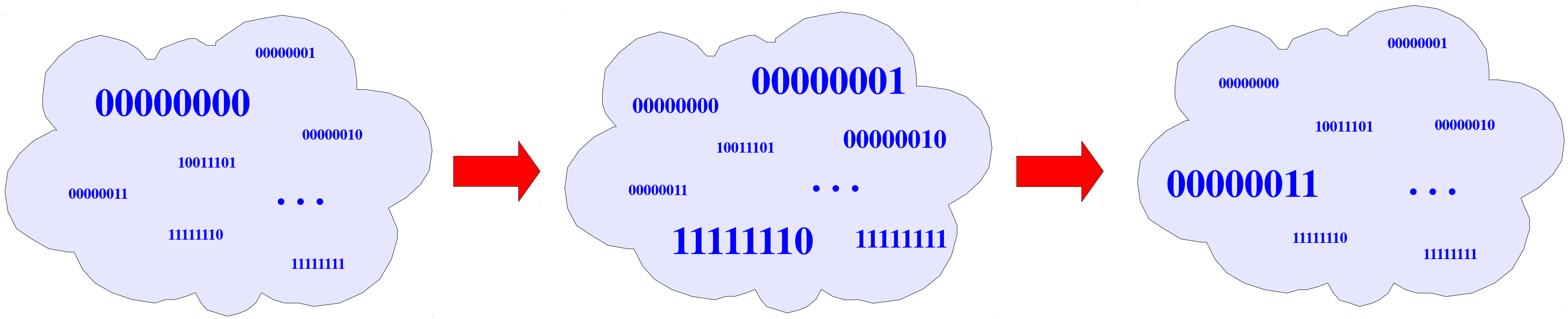


- The **256 complex numbers** determine the **probabilities**

- These numbers **cannot** be directly observed

What is Quantum Computing?

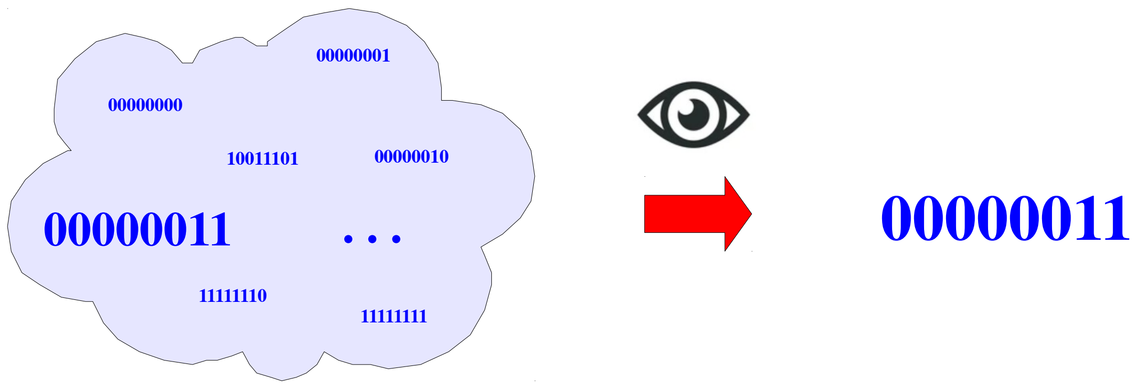
- We can manipulate the register with **quantum gates**, while being careful to avoid observing or measuring it



- Quantum gates **change the balance of probabilities** by “remixing” the complex numbers in precise ways

What is Quantum Computing?

- After applying a sequence of quantum gates, we then **measure** the register, which yields a final answer



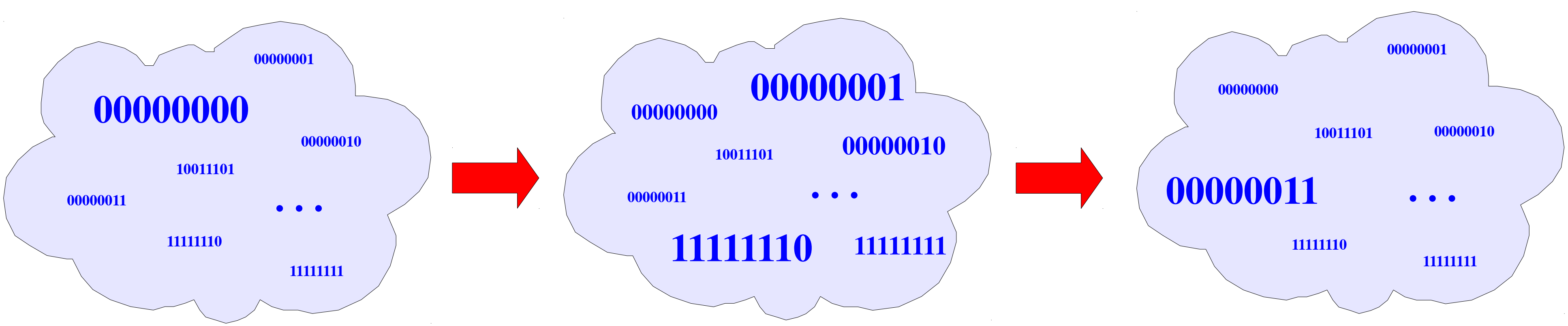
- With the right sequence of operations, we can ensure that the answer is correct with **very high probability**

What is Quantum Computing?

- Conventional computers transform bit-patterns **one bit-pattern at a time**

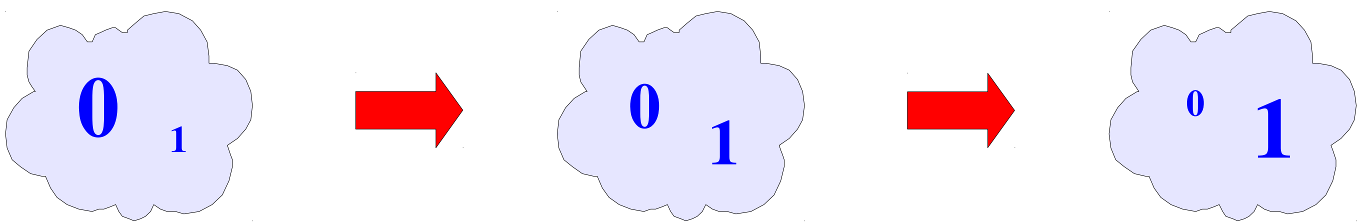
00000000 → 10011100 → 01010101

- Quantum computers in effect transform **exponentially many bit-patterns at a time**

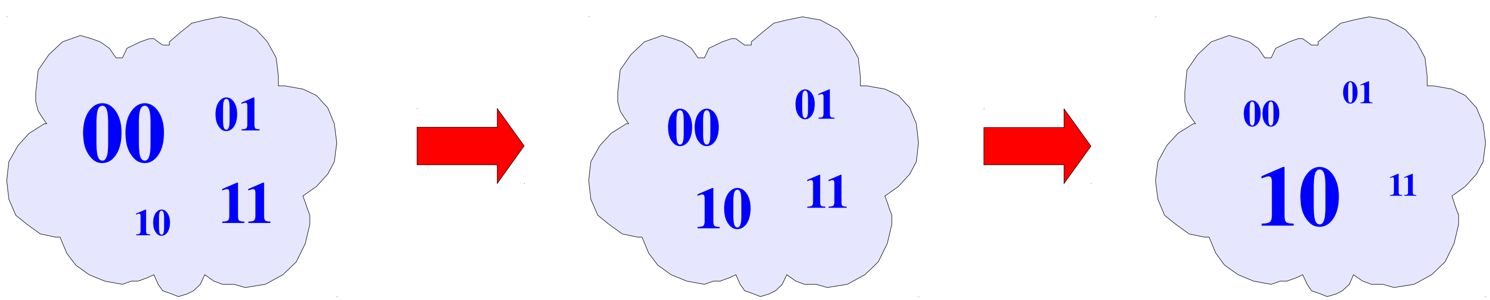


What is Quantum Computing?

- With **1 qubit**, a quantum computer can operate on 2 bit-patterns (**2^1**) at a time in superposition

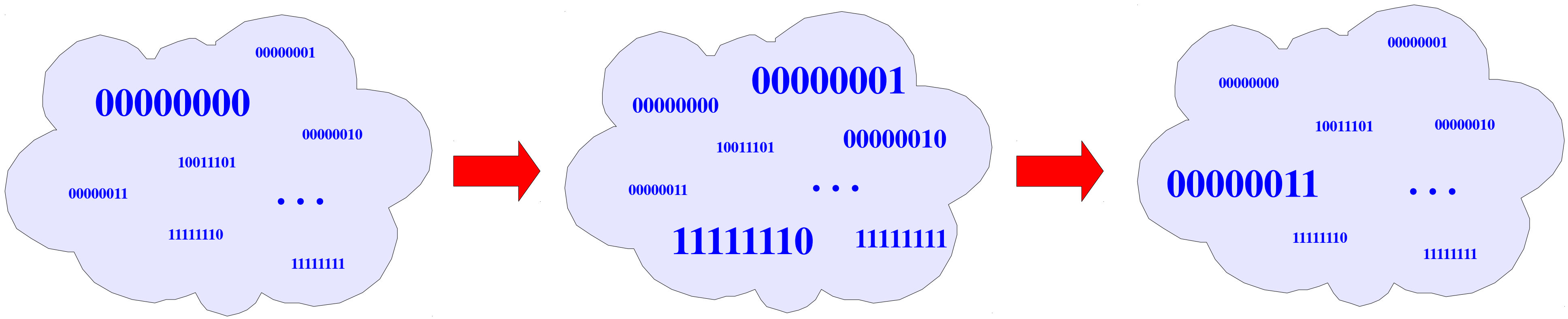


- With **2 qubits**, a quantum computer can operate on 4 bit-patterns (**2^2**) at a time in superposition



What is Quantum Computing?

- With **8 qubits**, 256 (**2^8**) bit-patterns at a time



- With **30 qubits**, a **billion (2^{30})** bit-patterns at a time
- With **100 qubits**, over a **million trillion trillion** (**2^{100}**) bit-patterns at a time

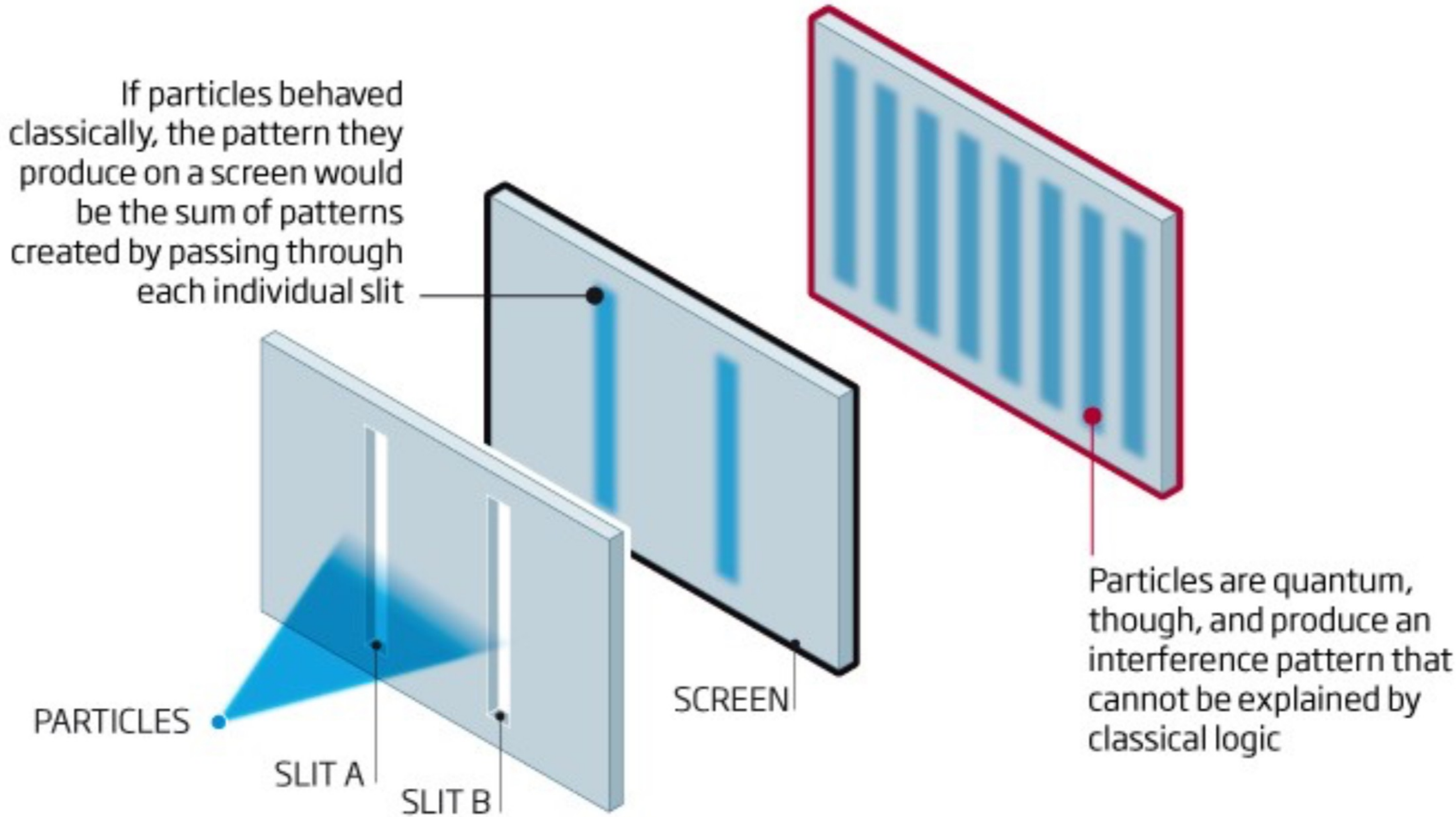
What is Quantum Computing?

- … and so on

- In principle, problems requiring **trillions of years** on the fastest modern supercomputers could be solved in **minutes or hours** on a quantum computer with a sufficient number of qubits

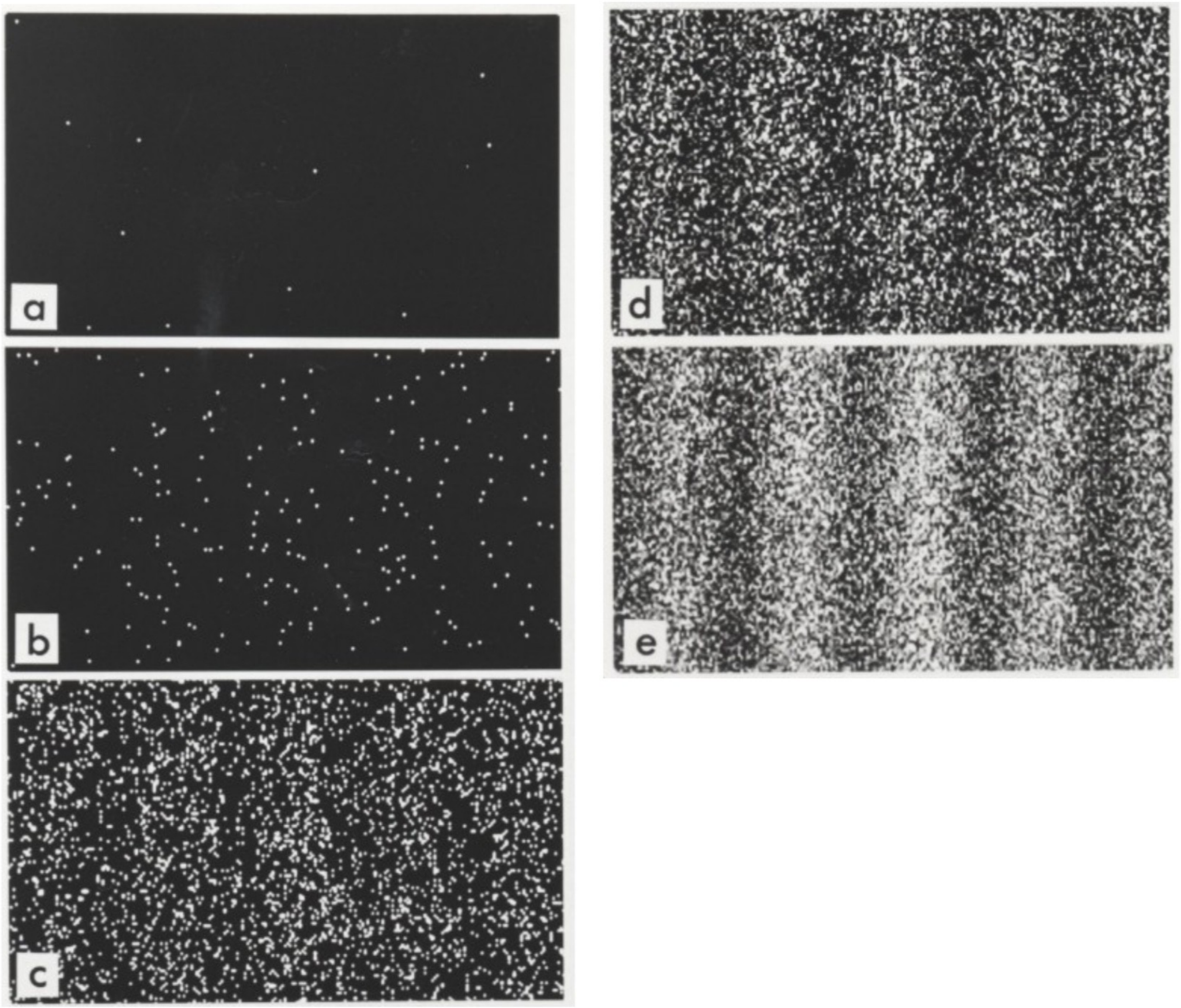
Quantum Weirdness: Wave/Particle Duality

- The Double-Slit Experiment (Thomas Young, 1801)



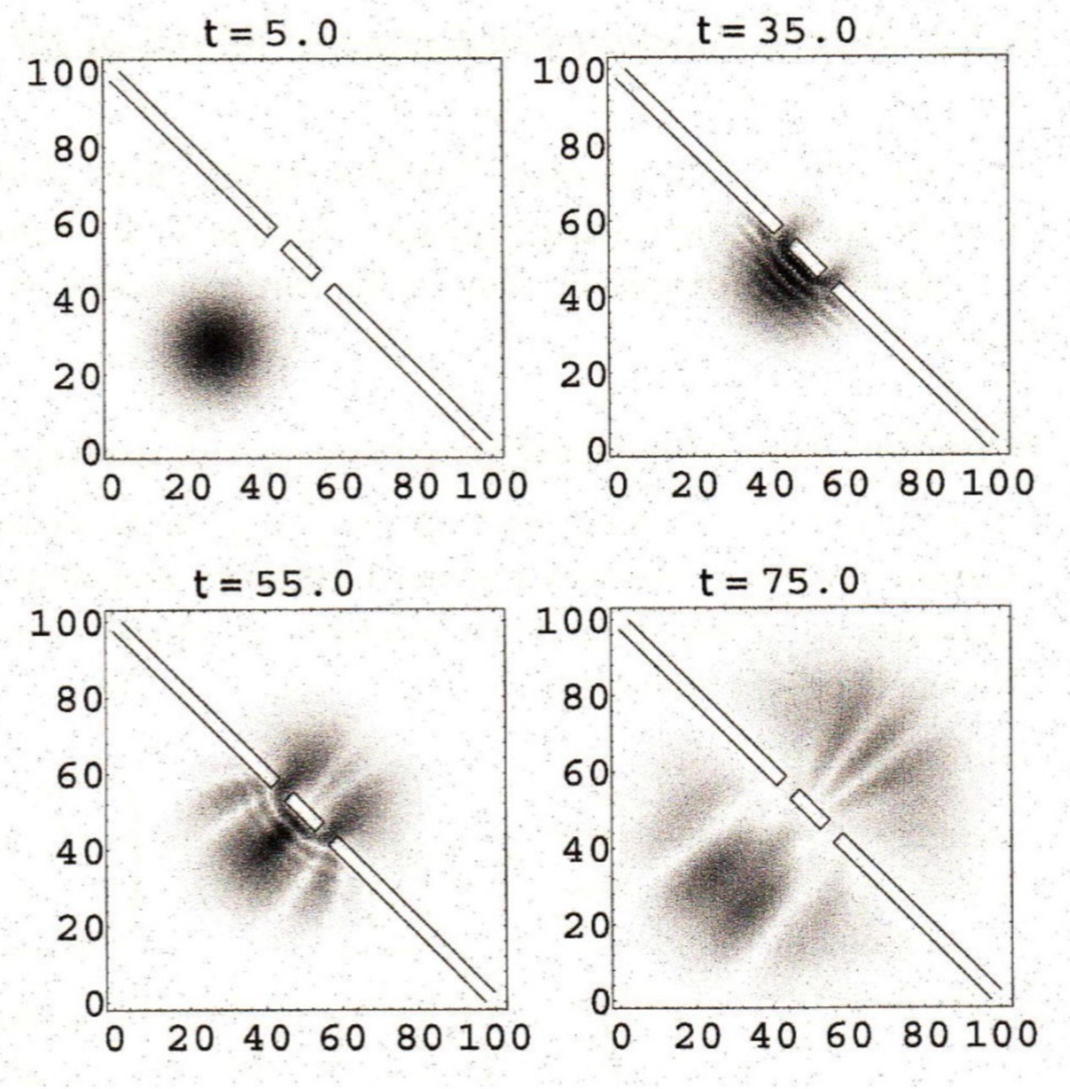
Quantum Weirdness: Wave/Particle Duality

- The Double-Slit Experiment — one particle at a time



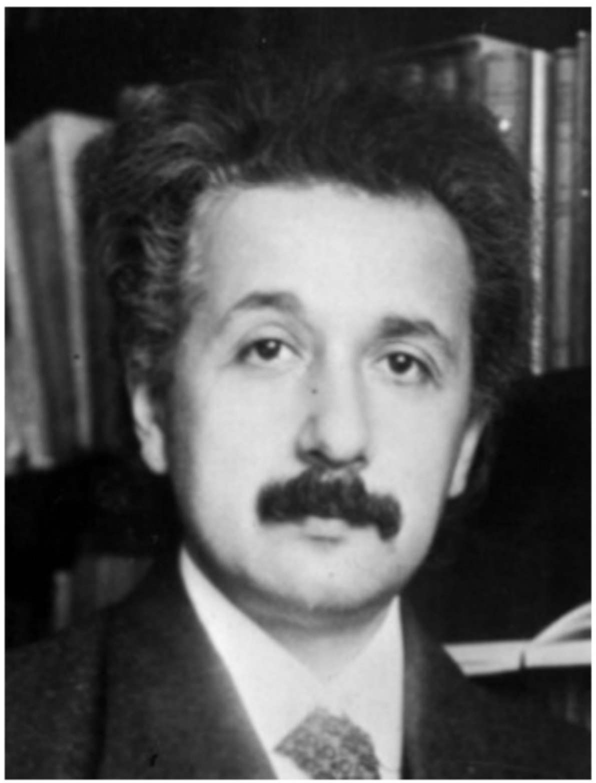
Quantum Weirdness: Wave/Particle Duality

- A "particle" is a wave of probability



Whence Cometh Quantum Computing?

- Development of quantum mechanics (1900-1920s)



Albert Einstein in 1905

Werner Heisenberg

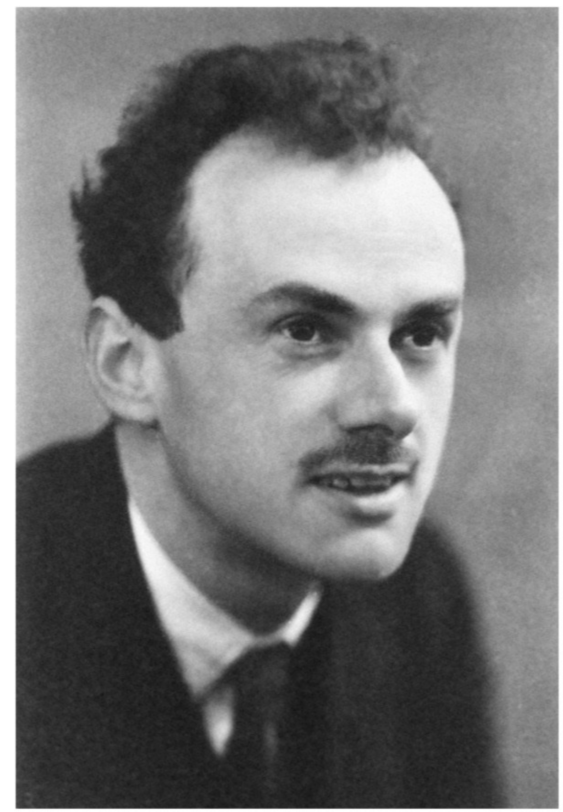
Erwin Schrödinger

Whence Cometh Quantum Computing?

- Development of quantum mechanics (1900-1920s)

Niels Bohr

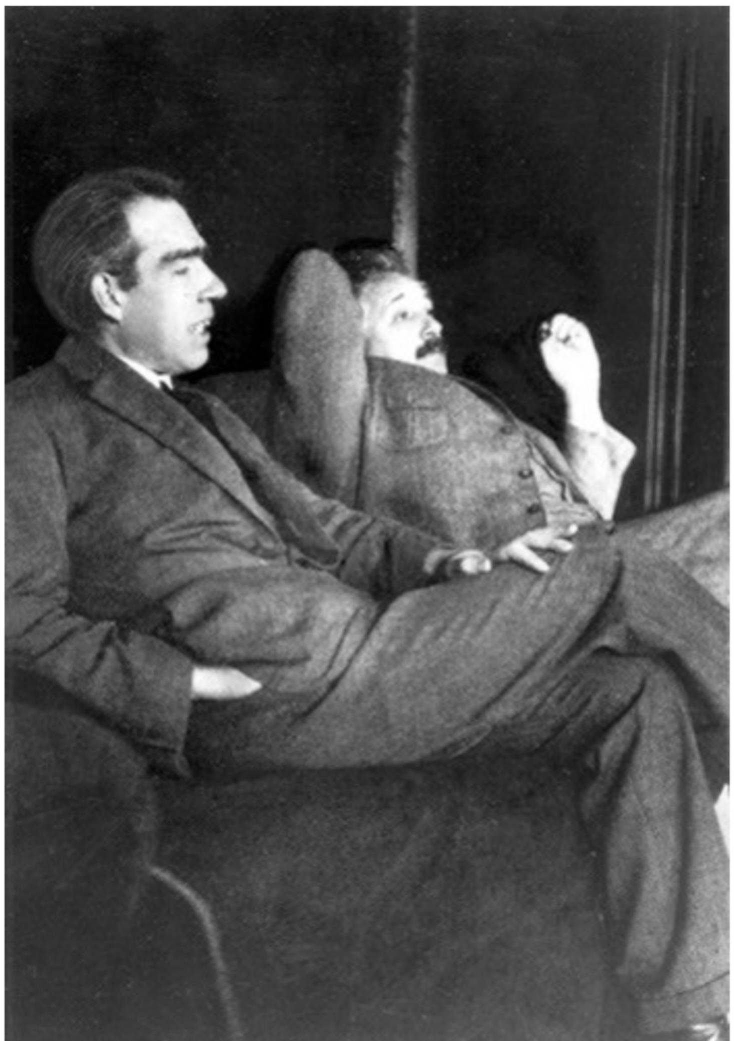
Wolfgang Pauli



Paul Dirac

Whence Cometh Quantum Computing?

- Development of quantum mechanics (1900-1920s)

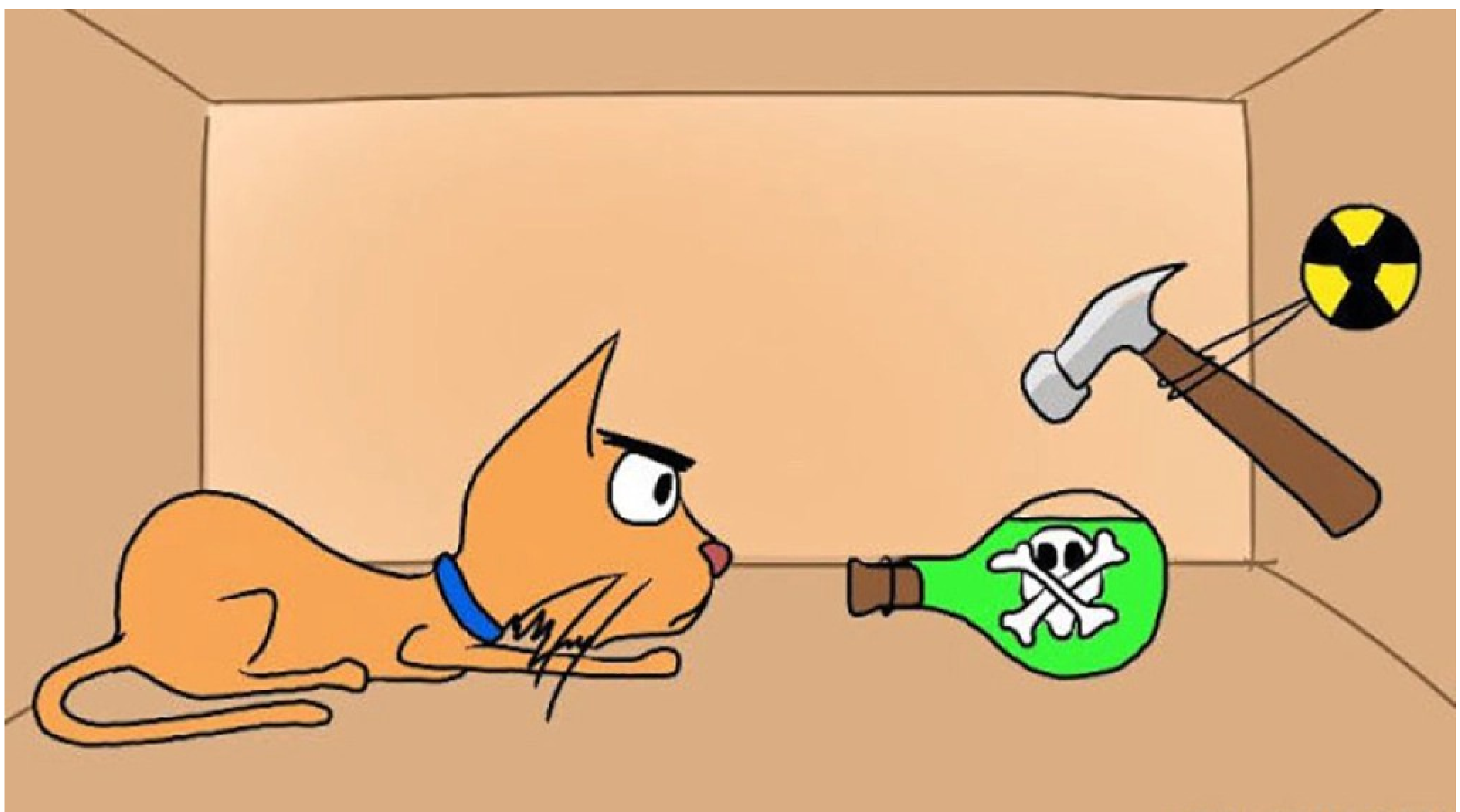


Bohr and Einstein often debated the meaning of quantum theory

Whence Cometh Quantum Computing?

- Development of quantum mechanics (1900-1920s)

- “Schrödinger's Cat” thought experiment (1935)



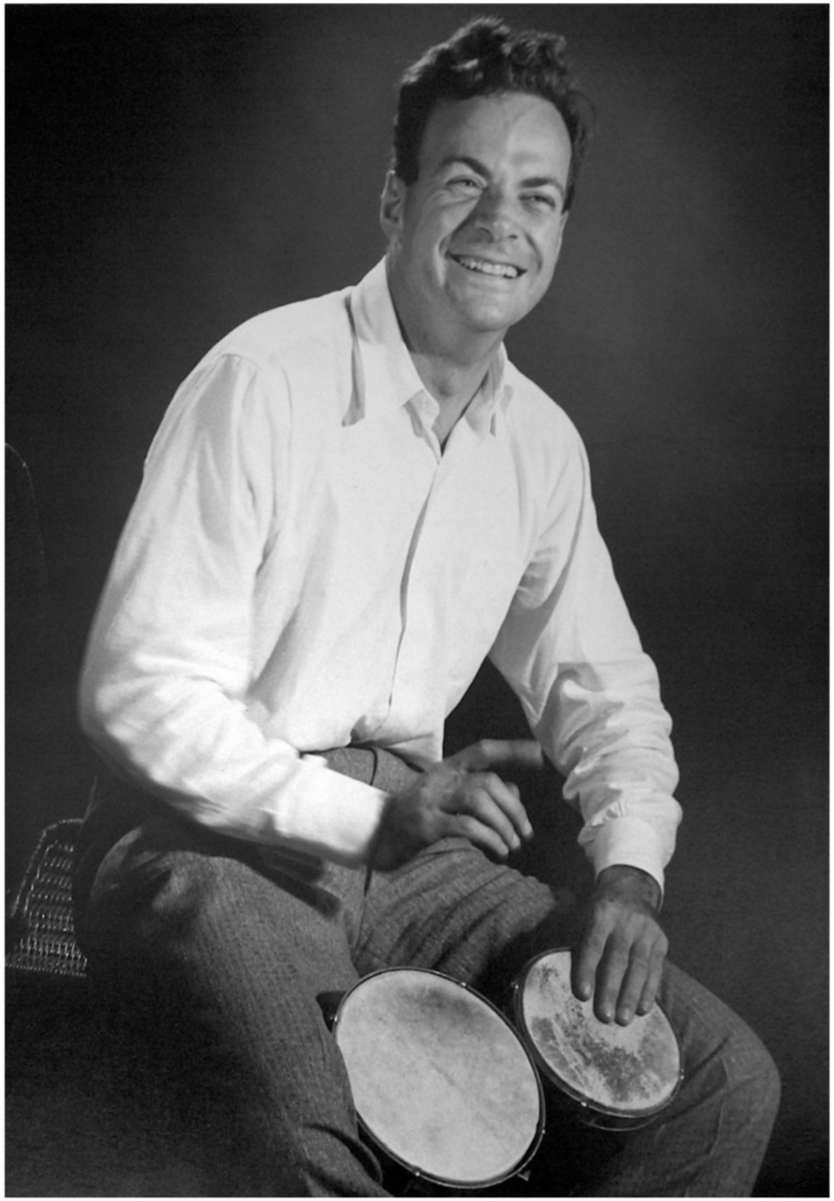
Whence Cometh Quantum Computing?

- Development of quantum mechanics (1900-1920s)
- “Schrödinger's Cat” thought experiment (1935)

Whence Cometh Quantum Computing?

- Development of quantum mechanics (1900-1920s)
- “Schrödinger's Cat” thought experiment (1935)
- “Spooky action at a distance” (Einstein, 1935)
- Spooky action observed in the lab (1970s and 1980s)
- Computer scientists start to think of ways to exploit quantum behavior for computation (1980s)

Whence Cometh Quantum Computing?



Richard Feynman

Simulating Physics with Computers, *International Journal of Theoretical Physics*, Vol. 21, Nos. 6/7, 1982

Whence Cometh Quantum Computing?

Just to give you an idea of how the theory has been put through the wringer, I'll give you some recent numbers: experiments have Dirac's number at 1.00115965221 (with an uncertainty of about 4 in the last digit); the theory puts it at 1.00115965246 (with an uncertainty of about five times as much). To give you a feeling for the accuracy of these numbers, it comes out something like this: If you were to measure the distance from Los Angeles to New York to this accuracy, it would be exact to the thickness of a human hair. That's how delicately quantum electrodynamics has, in the past fifty years, been checked—both theoretically and experimentally. By the way, I have chosen only one number to show you. There are other things in quantum electrodynamics that have been measured with comparable accuracy, which also agree very well. Things have been checked at distance scales that range from one hundred times the size of the earth down to one-hundredth the size of an atomic nucleus. These numbers are meant to intimidate you into believing that the theory is probably not too far off!

—Richard Feynman, *QED*, 1985

Whence Cometh Quantum Computing?

David Deutsch

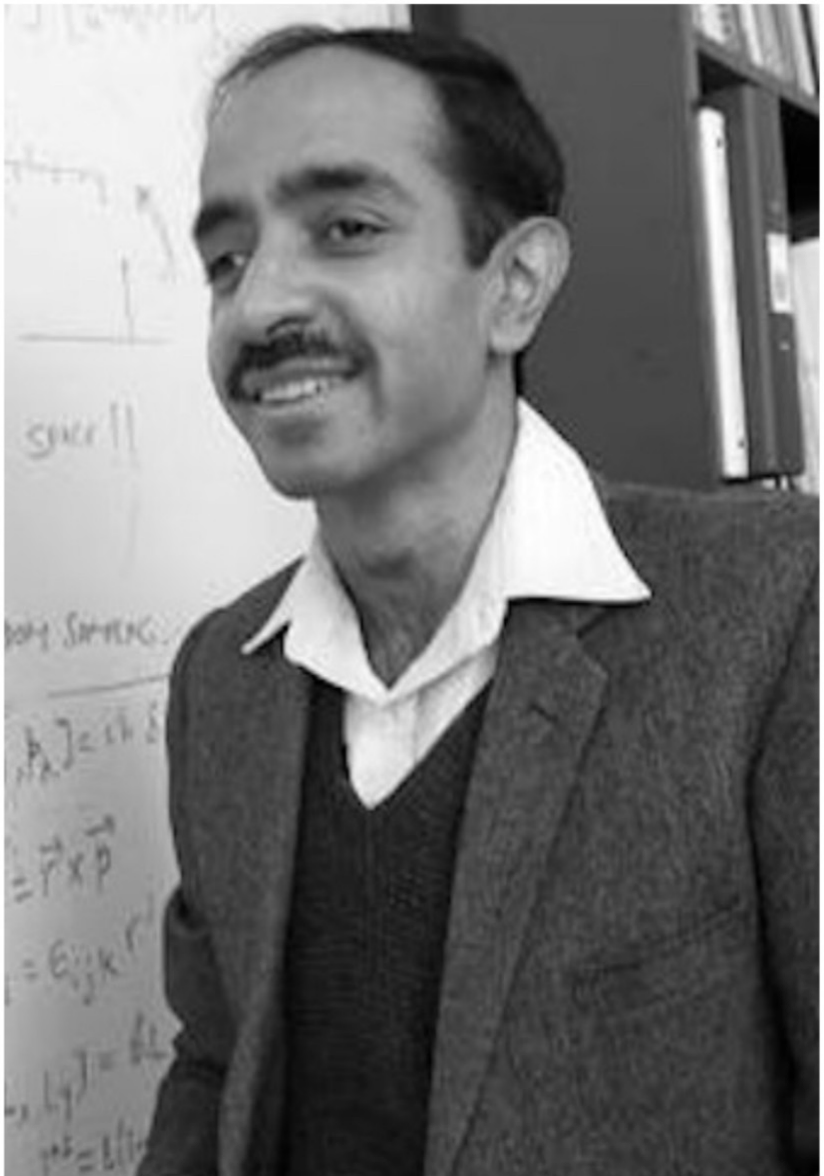
Quantum Theory, the Church-Turing Principle and the Universal Quantum Computer, *Proceedings of the Royal Society of London A*, Vol. 400, pp. 97-117, 1985

Whence Cometh Quantum Computing?

Peter Shor

Algorithms for Quantum Computation: Discrete Logarithm and Factoring, *Proceedings of the 35th Annual Symposium on Foundations of Computer Science*, pp. 124-134, 1994

Whence Cometh Quantum Computing?



Lov Grover

A Fast Quantum Mechanical Algorithm for Database Search, *Proceedings of the 28th Annual ACM Symposium on the Theory of Computing*, 1996