Microsoft Research

Microsoft

Quantum High Performance Computing

Matthias Troyer
Station Q QuArC, Microsoft

Microsoft Spends Big to Build a Computer Straight Out of Science Fiction

By JOHN MARKOFF

SAN FRANCISCO — Microsoft is putting its considerable financial and engineering muscle into the experimental field of quantum computing as it works to build a machine that could tackle problems beyond the reach of today's digital computers.

There is a growing optimism in the tech world that quantum computers, superpowerful devices that were once the stuff of science fiction, are possible — and may even be practical. If these machines work, they will have an impact on work in areas such as drug design and artificial intelligence, as well as offer a better understanding of the foundations of modern physics.

Microsoft's decision to move from pure research to an expensive effort to build a working prototype underscores a global competition among technology companies, including Google and IBM, which are also making significant investments in search of breakthroughs.

In the exotic world of quantum physics, Microsoft has set itself apart from its competitors by choosing a different path. The company's approach is based on "braiding" particles known as anyons — which physicists describe as existing in just two dimensions — to form the building blocks of a supercomputer that would exploit the unusual physical properties of subatomic parti-

edge that barriers still remain to building useful quantum machines, both at the level of basic physics and in developing new kinds of software to exploit certain qualities of devices known as qubits that hold out the possibility of computing in ways not possible for today's digital systems.

Unlike conventional transistors, which can be only on or off at any one time, representing a dig-

Planning a prototype of a superpowerful quantum computer.

ital 1 or 0, qubits can exist in superposition, or simultaneously in both states. If qubits are placed in an "entangled" state — physically separated but acting as though they are deeply intertwined — with many other qubits, they can represent a vast number of values simultaneously. A quantum computer would most likely consist of hundred or thousands of qubits.

Microsoft began funding research in the field in 2005 when it quietly set up a laboratory known as Station Q under the leadership of the mathematician Michael Freedman.

Microsoft now believes that it is close enough to designing the basic qubit building block that the company ...

Todd Holmdahl, a veteran engineering manager who will direct the Microsoft effort. Over the years, he has led various Microsoft projects, including its Xbox video game machine and the yet-to-be-released HoloLens augmented reality system.

"Once we get the first qubit figured out, we have a road map that allows us to go to thousands of qubits in a rather straightforward way," Mr. Holmdahl said.

There is still a debate among physicists and computer scientists over whether quantum computers that perform useful calculations will ever be created.

A variety of alternative research programs are trying to create qubits using different materials and designs. The Microsoft approach, known as topological quantum computing, is based on a field that took on new energy when this year's Nobel Prize in Physics was awarded to three scientists who had done fundamental work in forms of matter that may exist in just two dimensions.

Mr. Holmdahl's project will also include the physicists Leo Kouwenhoven of Delft University, Charles M. Marcus of the University of Copenhagen, David Reilly of the University of Sydney and Matthias Troyer of E.T.H. Zurich.

They will all become Microsoft employees as part of the Artificial Intelligence and Research Group that Microsoft recently created under the leadership of one of its top technical ...

IAN C. BATES FOR THE NEW YORK TIMES

Todd Holmdahl, who has led Microsoft projects like the Xbox gaming console, will direct the quantum computing efforts.

cists say the decision to try to build a topological ...

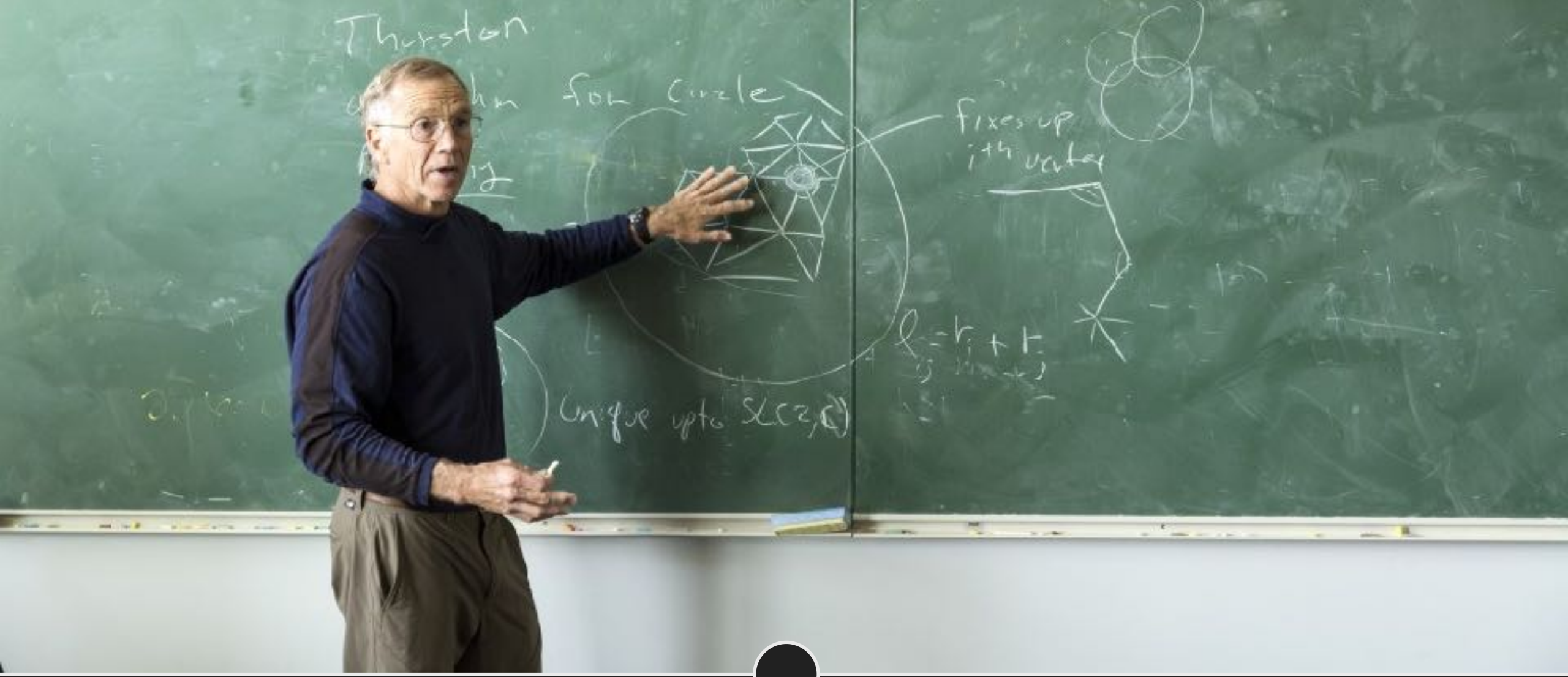
confidence that the company ...

and superconductors," Dr. Marcus said. The researchers recently made a "remarkable breakthrough" in their ability to control the materials used to form qubits, he said. Most of the competing approaches involve cooling quantum computers to near absolute zero temperatures.

So far, there are relatively few proven algorithms that could be used to solve problems more quickly than today's digital computers. One early effort, known as Shor's algorithm, would be used to factor numbers, giving hope that quantum computers might be used in the future for breaking codes.

That would potentially have world-shaking consequences because modern electronic commerce is built on cryptographic systems that are largely unbreakable using conventional digital computers. Other proposed approaches might allow faster searching of databases or perform machine learning algorithms which are being used to make advances in computer vision and speech recognition.

More immediately, however, these tools might advance the basic understanding of physics, a possibility the physicist Richard P. Feynman mentioned when he speculated about the idea of a quantum computer in 1981 ...

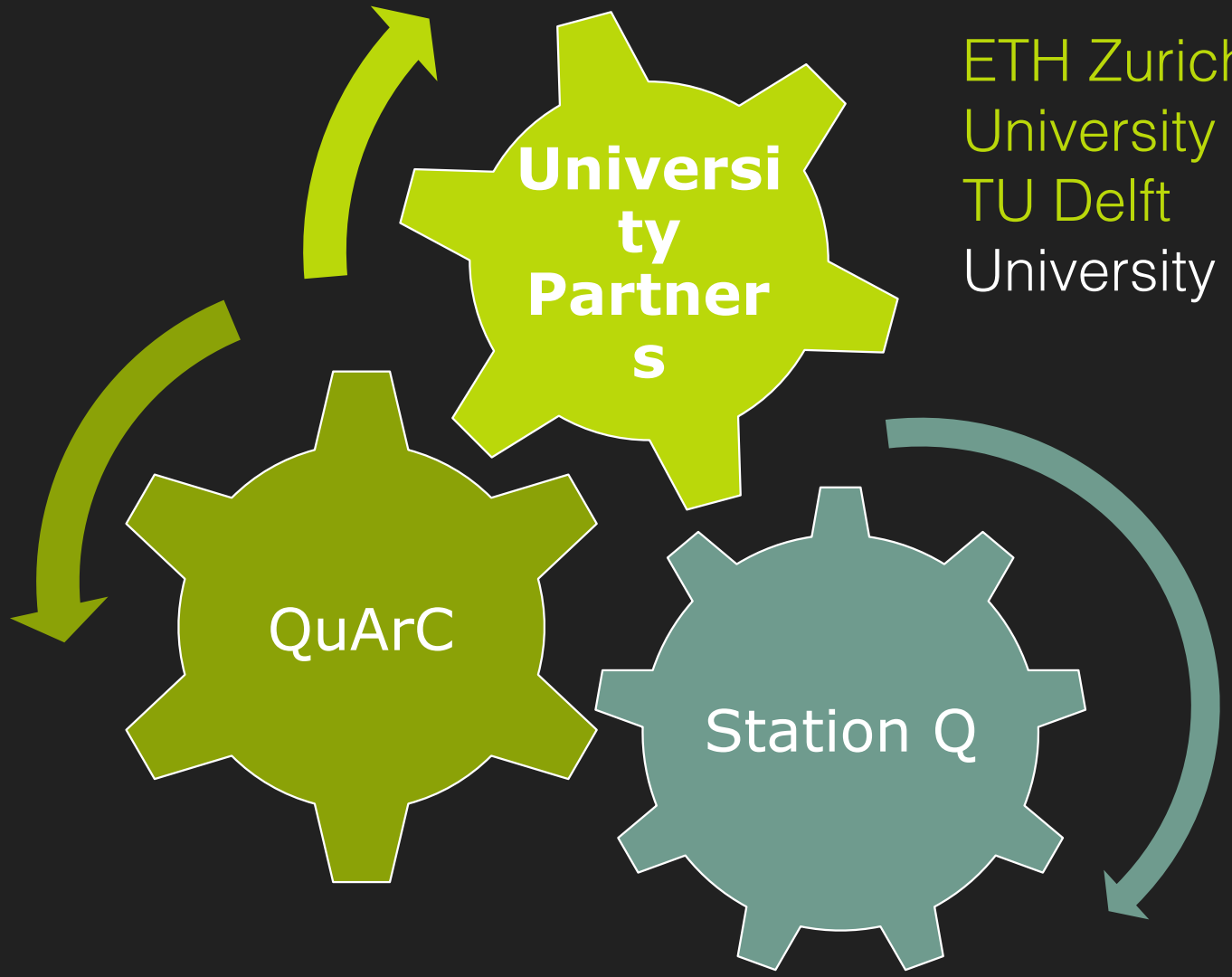


2000

STATION Q

2006

Station Q – A worldwide consortium



ETH Zurich
University of Copenhagen
TU Delft
University of Sydney

Charlie Marcus' lab in Copenhagen, Denmark

One of our primary experimental labs

Photos courtesy of: Professor Charlie Marcus

"MAJORANA PARTICLE GLIMPSED IN LAB."

BBC NEWS

2012

with TU Delft

Microsoft “acquires" the academic groups of the StationQ consortium

B4 THE NEW YORK TIMES, MONDAY, NOVEMBER 21, 2016

Bits

Microsoft Spends Big to Build a Computer Straight Out of Science Fiction

By JOHN MARKOFF

SAN FRANCISCO — Microsoft is putting its considerable financial and engineering muscle into the experimental field of quantum computing as it works to build a machine that could tackle problems beyond the reach of today's digital computers.

There is a growing optimism in the tech world that quantum computers, superpowerful devices that were once the stuff of science fiction, are possible — and may even be practical. If these machines work, they will have an impact on work in areas such as drug design and artificial intelligence, as well as offer a better understanding of the foundations of modern physics.

Microsoft's decision to move from pure research to an expensive effort to build a working prototype underscores a global competition among technology companies, including Google and IBM, which are also making significant investments in search of breakthroughs.

In the exotic world of quantum physics, Microsoft has set itself apart from its competitors by choosing a different path. The company's approach is based on "braiding" particles known as anyons — which physicists describe as existing in just two dimensions — to form the building blocks of a supercomputer that would exploit the unusual physical properties of subatomic particles that harness the fragile state known as superposition, or simultaneously in both states. If qubits are placed in an "entangled" state — physically separated but acting as though they are deeply intertwined — with many other qubits, they can represent a vast number of values simultaneously. A quantum computer would most likely consist of hundred or thousands of qubits.

Planning a prototype of a superpowerful quantum computer.

Microsoft began funding research in the field in 2005 when it quietly set up a laboratory known as Station Q under the leadership of the mathematician Michael Freedman.

Microsoft now believes that it is close enough to designing the basic qubit building block that the company is ready to [illegible]

Todd Holmdahl, a veteran engineering manager who will direct the Microsoft effort. Over the years, he has led various Microsoft projects, including its Xbox video game machine and the yet-to-be-released HoloLens augmented reality system.

"Once we get the first qubit figured out, we have a road map that allows us to go to thousands of qubits in a rather straightforward way," Mr. Holmdahl said.

There is still a debate among physicists and computer scientists over whether quantum computers that perform useful calculations will ever be created.

A variety of alternative research programs are trying to create qubits using different materials and designs. The Microsoft approach, known as topological quantum computing, is based on a field that took on new energy when this year's Nobel Prize in Physics was awarded to three scientists who had done fundamental work in terms of matter that may exist in just two dimensions.

Mr. Holmdahl's project will also include the physicists Leo Kouwenhoven of Delft University, Charles M. Marcus of the University of Copenhagen, David Reilly of the University of Sydney and Matthias Troyer of E.T.H. Zurich.

They will all become Microsoft employees as part of the Artificial Intelligence and Research Group that Microsoft recently created under the leadership of one of its top technical employees. [illegible]

IAN C. BATES FOR THE NEW YORK TIMES

Todd Holmdahl, who has led Microsoft projects like the Xbox gaming console, will direct the quantum computing efforts.

cists say the decision to try to build a topological quantum com[illegible] confidence that the company will

and superconductors," Dr. Marcus said. The researchers recently made a "remarkable breakthrough" in their ability to control the materials used to form qubits, he said. Most of the competing approaches involve cooling quantum computers to near absolute zero temperatures.

So far, there are relatively few proven algorithms that could be used to solve problems more quickly than today's digital computers. One early effort, known as Shor's algorithm, would be used to factor numbers, giving hope that quantum computers might be used in the future for breaking codes.

That would potentially have world-shaking consequences because modern electronic commerce is built on cryptographic systems that are largely unbreakable using conventional digital computers. Other proposed approaches might allow faster searching of databases or perform machine learning algorithms, which are being used to make advances in computer vision and speech recognition.

More immediately, however, these tools might advance the basic understanding of physics, a possibility the physicist Richard P. Feynman mentioned when he speculated about the idea of a quantum computer in 1982.

2016

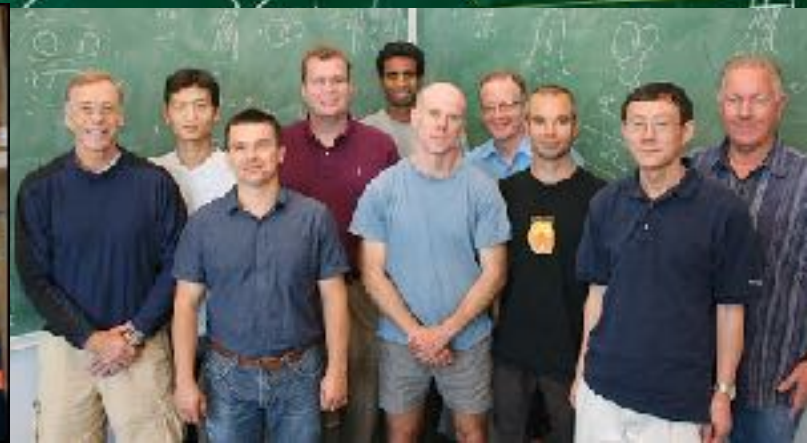
STATION Q

stationq.microsoft.com

REDMOND SYDNEY, DELFT, COPENHAGEN SANTA BARBARA





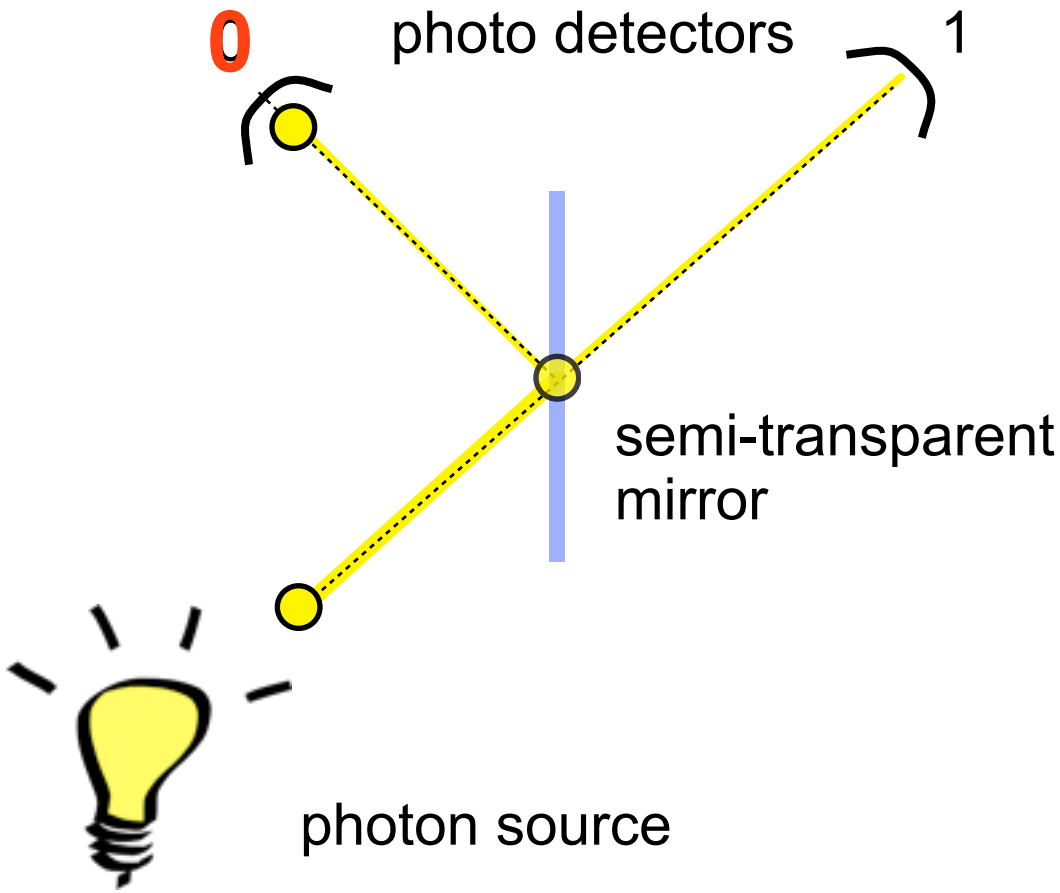


Developing the full quantum stack

- Commercial quantum applications
- Quantum algorithms
- Quantum and classical libraries
- Quantum compilers
- Cryogenic runtime operating system
- Cryogenic classical control and memory
- Quantum bits and quantum gates
- Semiconductor/superconductor fab
- Materials and Device Simulations on HPC machines

True and perfect randomness

Quantum mechanics can give true and perfect random numbers



1. Photon source emits a photon
2. Photon hits semi-transparent mirror
3. Photon follows both paths
4. The photo detectors see the photon only in one place: **a random bit**

The quantum bit (qubit)

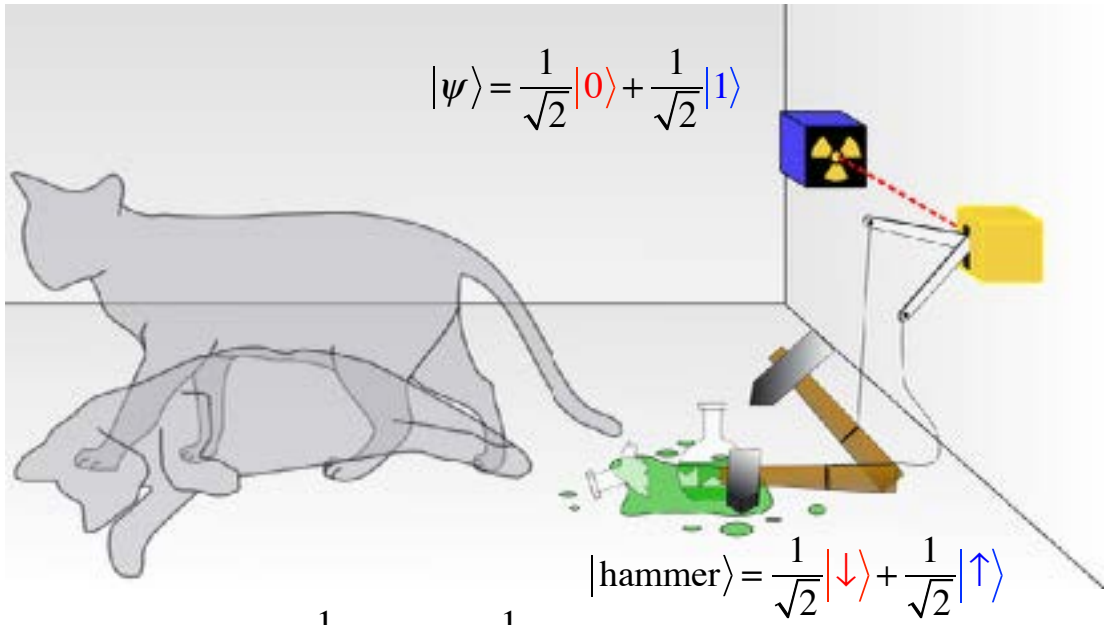
Classical bits can be $|0\rangle$ or $|1\rangle$

Qubits can be both at once

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle = \begin{pmatrix} \alpha \\ \beta \end{pmatrix}$$

“quantum superposition”

Schrödinger’s cat paradox



$$|\text{cat}\rangle = \frac{1}{\sqrt{2}}|\text{dead}\rangle + \frac{1}{\sqrt{2}}|\text{alive}\rangle$$

Measuring a quantum superposition

- when measuring (looking) we only ever get one classical bit: 0 or 1

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle \longrightarrow \begin{array}{ll} 0 & \text{with probability } |\alpha|^2 \\ 1 & \text{with probability } |\beta|^2 \end{array}$$

$$|\alpha|^2 + |\beta|^2 = 1$$

- When we measure we always get either 0 or 1!

- Quantum random number generator:

  prepare and the state $|\psi\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$ and measure

An application for a 1-qubit quantum computer!

The magic of “quantum entanglement”

A single qubit gives a random bit when measured $|\psi\rangle = \frac{1}{\sqrt{2}}\left[|0\rangle + |1\rangle\right]$

“Entangled states” can give random but identical results $|\psi\rangle = \frac{1}{\sqrt{2}}\left[|0\rangle_A|0\rangle_B + |1\rangle_A|1\rangle_B\right]$

Measuring qubit *A* gives a random result *a*
Measuring qubit *B* gives a random result *b*

However, always *a*=*b* no matter how far apart the qubits are

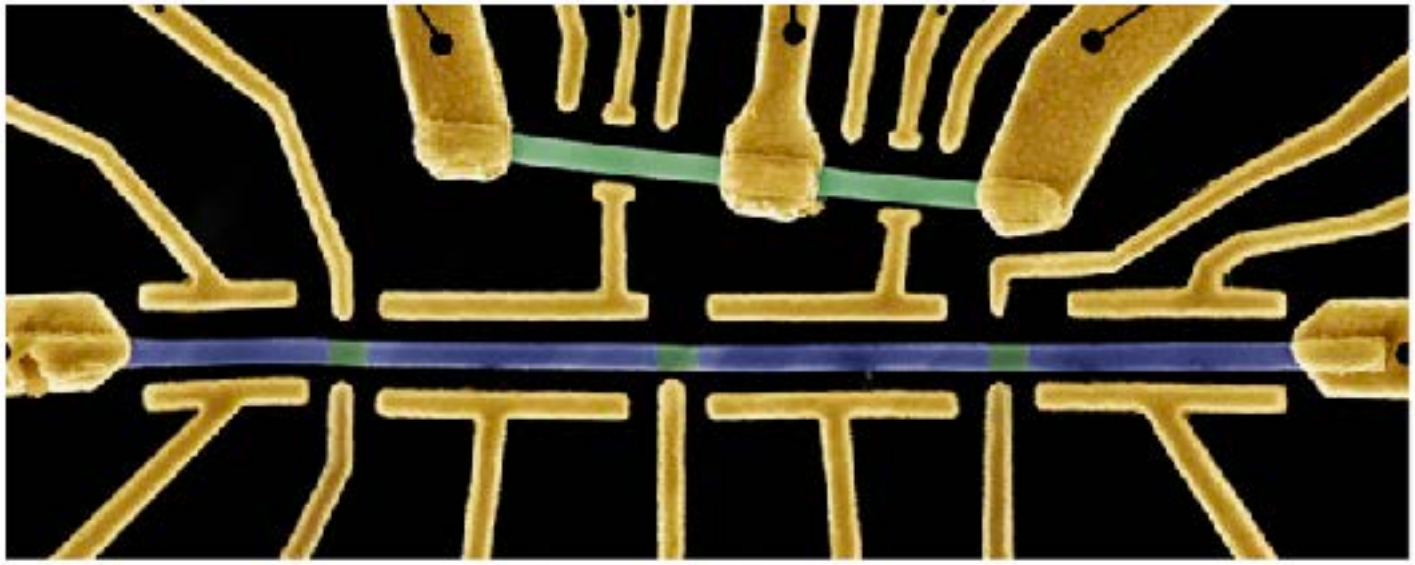
A shared secret key that an be made provably secure!

Interlude: quantum hardware

Topological quantum bits: hope for a disruptive breakthrough

Encoding the information into a non-local (topological property) makes it robust and creates a long-lived “Schrödinger cat”

Split $|0\rangle$ or $|1\rangle$ electrons into two “Majorana” particles and separate them



Simulating quantum computers on classical computers

Simulating a quantum gate acting on N qubits needs $O(2^N)$ memory and operations

Qubits	Memory	Time for one operation
10	16 kByte	microseconds on a smartwatch
20	16 MByte	milliseconds on smartphone
30	16 GByte	seconds on laptop
40	16 TByte	seconds on cluster
50	16 PByte	minutes on top supercomputers?
60	16 EByte	hours on exascale supercomputer?
70	16 ZByte	days on hypothetical future supercomputer?
…	…	…
250	size of visible universe	age of the universe

arXiv.org > quant-ph > arXiv:1704.01127

Quantum Physics

0.5 Petabyte Simulation of a 45-Qubit Quantum Circuit

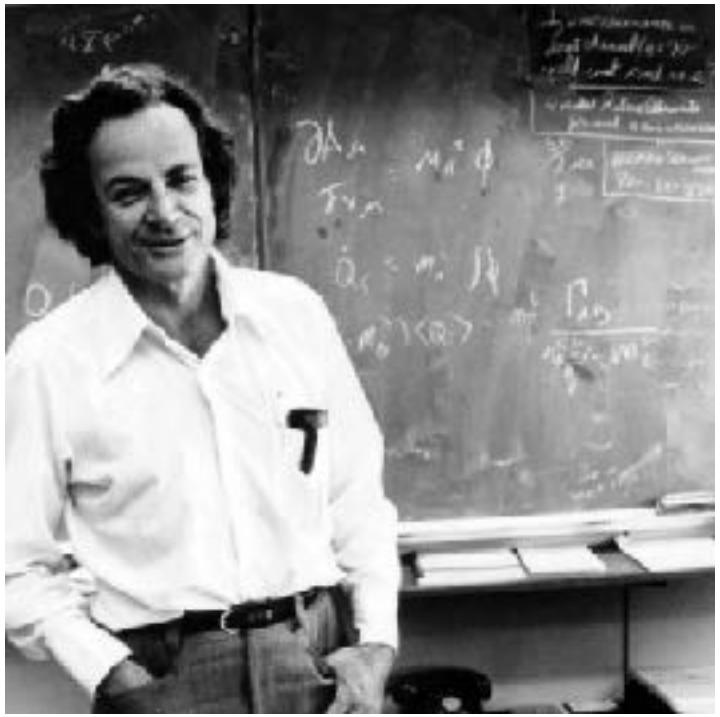
Thomas Häner, Damian S. Steiger

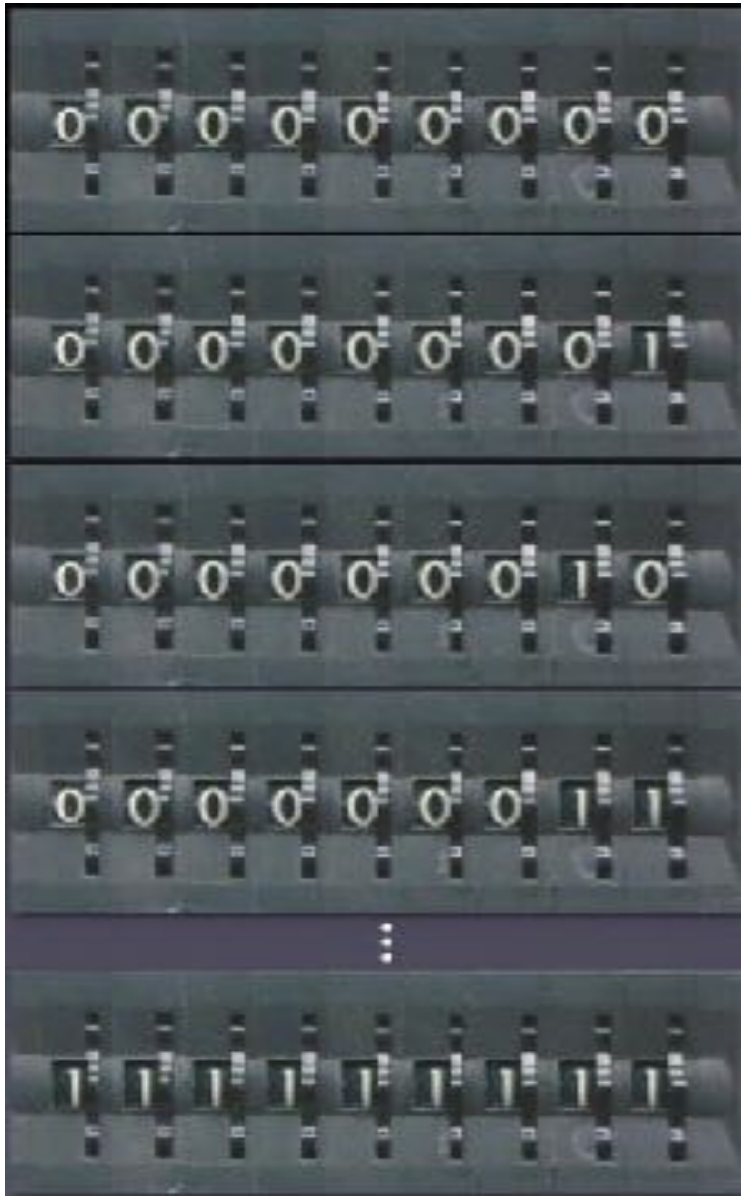
(Submitted on 4 Apr 2017)

Using Quantum Mechanics for Computing

Quantum mechanics considers all paths at once

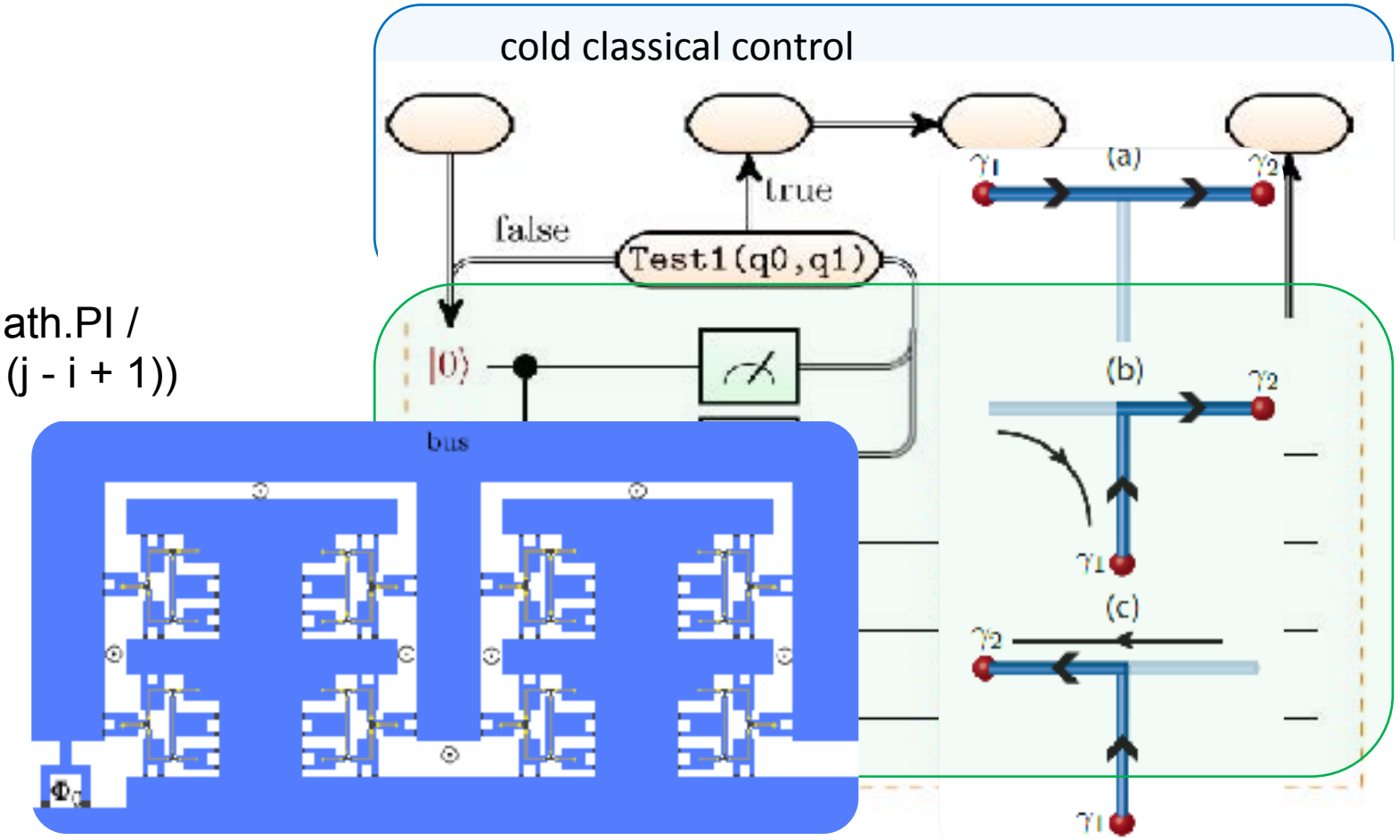
It enormously accelerates some calculations by operating on all inputs simultaneously





Quantum programming and compilation

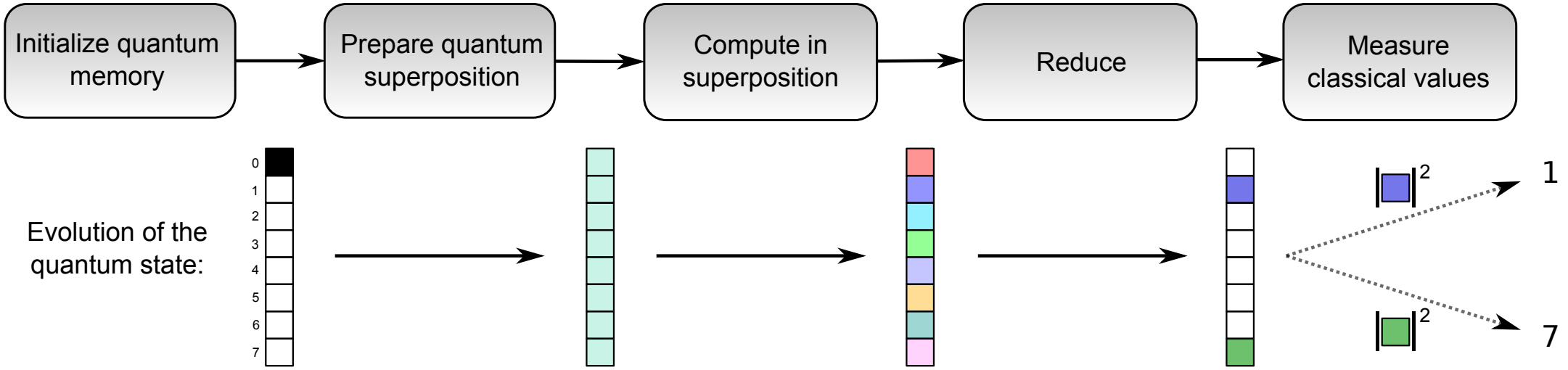
```
let QFT (qs : Qs) =
    let n = qs.Length - 1
    for i = 0 to n do
        let q = qs.[i]
        H q
        for j = (i + 1) to n do
            let theta = 2.0 * Math.PI /
                float(1 <<< (j - i + 1))
            CRz theta qs.[j] q
    for i = 0 to ((n - 1) / 2) do
        SWAP qs.[i] qs.[n - i]
```



Mixed classical and quantum operations

A classical computer architecture view of quantum algorithms

- “A quantum computer can compute on all inputs at once”



- Pros: An extreme SIMD machine with exponential “vector length”
- Cons:
  - pure SIMD, only reversible logic
  - very limited readout and small set of reduction operations

Quantum computing beyond exa-scale

What are the important applications …

… that we can solve on a quantum computer …

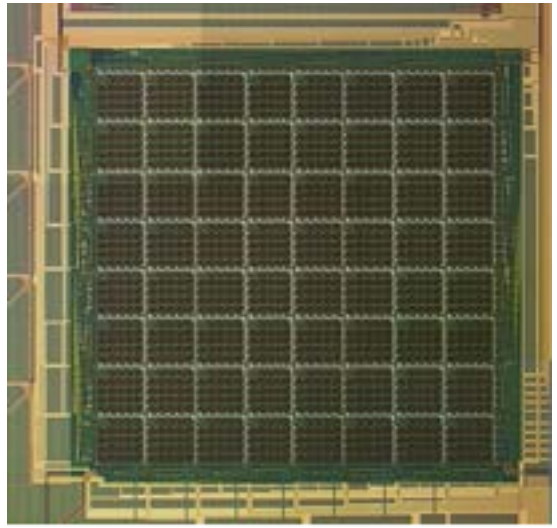
… but not special purpose post-exa-scale classical hardware that we may build in ten years?

The D-Wave quantum annealer

An analog quantum device to solve quadratic binary optimization problems

$$C(x_1,\ldots,x_N)=\sum_{ij} a_{ij}x_i x_j+\sum_i b_i x_i$$

$$\text{with} \qquad x_i=0,1$$



Can be built with imperfect qubits

Significant engineering achievement to scale it to two thousand qubits

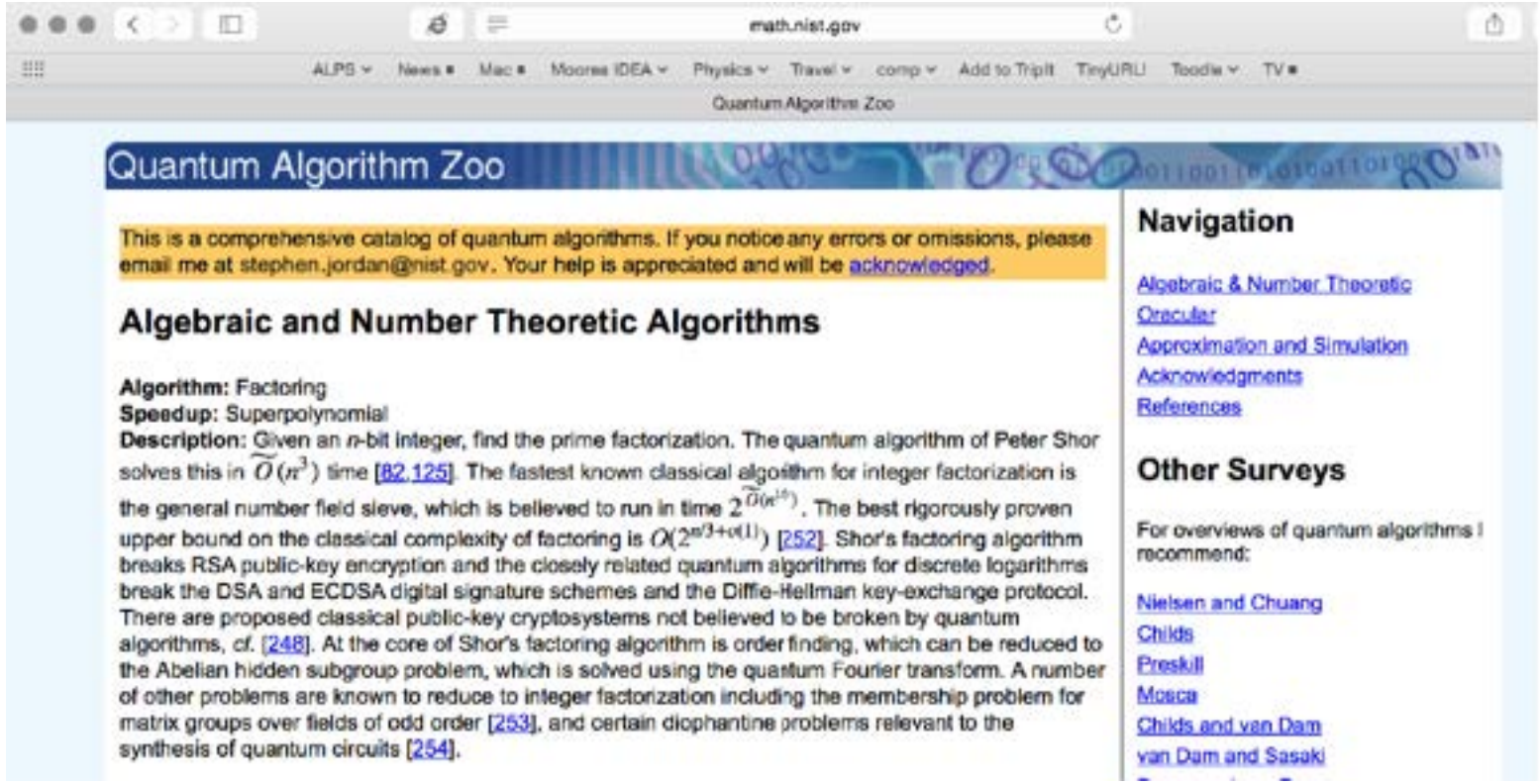
Nobody knows if it can solve NP-hard problems better than a classical computer

So far no (scaling) advantage has been observed

Quantum algorithms with quantum speedup

50+ quantum algorithms with quantum speedup, that is better asymptotic scaling than any classical computer

http://math.nist.gov/quantum/zoo/



Shor's algorithm for factoring

Factoring small numbers is easy: 15 = 3 x 5

Factoring large numbers is hard classically: $O(\exp(N^{1/3}))$ time for N digit-numbers

5369396836426911946079505415332600518604181838930231166202317318847061358416977779
8124777555435596464904452615804209177029240538156141035272554197625377862483O290
518096150501270434149272610204114236496946309670910771714302797950221151202416796
22849447805650987368350247829683054309216276674509735105639240298977591783205062
1619158848593319454766098482875128834780988979751083723214381986678381350567167

=

4363637625931498167701061252972058930130370651588109946621952523434903606572651613287
3421237667900245913537253744354928238018040554845306796065865605354860834270732796989
4210413710440109013191728001673

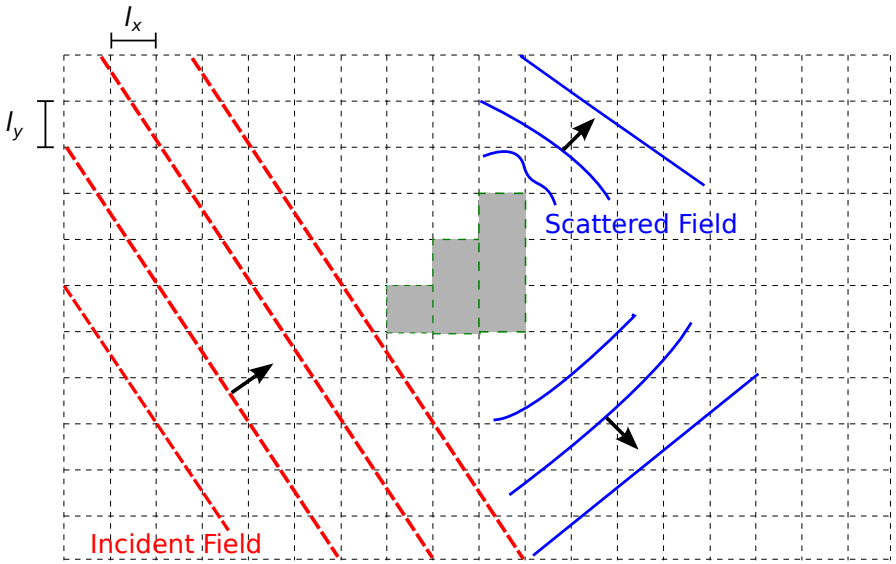
*

1230486419064350262435007521990111788816176581586683476039159532309509792696707176253
0052007668467350605879541695798973080376300970096911310297914332946223591672260748684
8670728527914505738619291595079

Polynomial time on a quantum computer (P. Shor)

Solving linear systems of equations

- Solve linear system $Ax=b$ in log(N) time
  Harrow, Hassidim, Lloyd, PRL (2009)
- Time evolution using the matrix A needs to be implemented efficiently $e^{-iAt}|b\rangle$
- Exponential speedup for wave scattering problem (Clader et al, PRL, 2013)!
- Estimated to use 10^{29} gate operations for a problem that is still tractable on a classical supercomputer (arXiv:1505.06552). Significant optimization is required!



International Journal of Theoretical Physics, Vol. 21, Nos. 6/7, 1982

Simulating Physics with Computers

Richard P. Feynman

Department of Physics, California Institute of Technology, Pasadena, California 91107

Received May 7, 1981

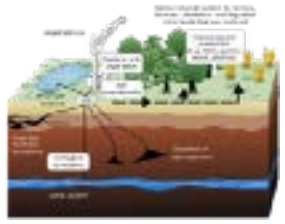
Feynman proposed to use quantum computers to simulate quantum physics

We can surpass the best classical computers with only 50 qubits!

Simulating quantum materials on a quantum computer

Can we use quantum computers to design new quantum materials?

- A room-temperature superconductor?
- Non-toxic designer pigments?
- A catalyst for carbon sequestration?
- Better catalysts for nitrogen fixation (fertilizer)?



Solving materials challenges with strong correlations has

- exponentially complexity on classical hardware
- polynomial complexity on quantum hardware!

The polynomial time quantum shock

- Estimates for an example molecule: Fe_2S_2 with 118 spin-orbitals

Gate count	10^{18}
Parallel circuit depth	10^{17}
Run time @ 100ns logical time	300 years

Quantum software optimization

- Estimates for an example molecule: Fe_2S_2 with 118 spin-orbitals

Gate count	10^{18}
Parallel circuit depth	10^{17}
Run time @ 100ns logical time	300 years

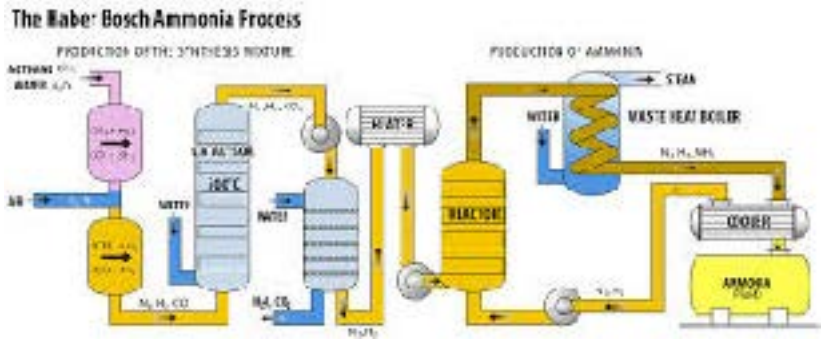
Reduced gate count	10^{11}
Parallel circuit depth	10^{10}
Run time @ 100ns gate time	20 minutes

- Attempting to reduce the horrendous runtime estimates we achieved
  Wecker *et al.*, PRA (2014), Hastings *et al.*, QIC (2015), Poulin *et al.*, QIC (2015)
  - Reuse of computations: $O(N)$ reduction in gates
  - Parallelization of terms: $O(N)$ reduction in circuit depth
  - Optimizing circuits: 4x reduction in gates
  - Smart interleaving of terms: 10x reduction in time steps
  - Multi-resolution time evolution: 10x reduction in gates
  - Better phase estimation algorithms: 4x reduction in rotation gates

Nitrogen fixation: a potential killer-app

Fertilizer production using Haber-Bosch process (1909)

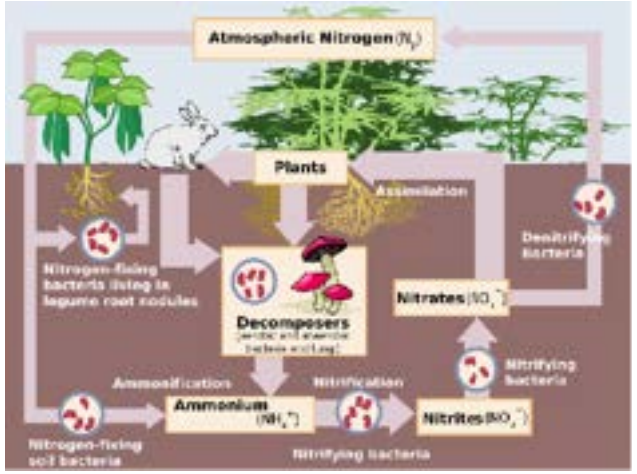
- Requires high pressures and temperatures
- 3-5% of the world's natural gas
- 1-2% of the world's annual energy

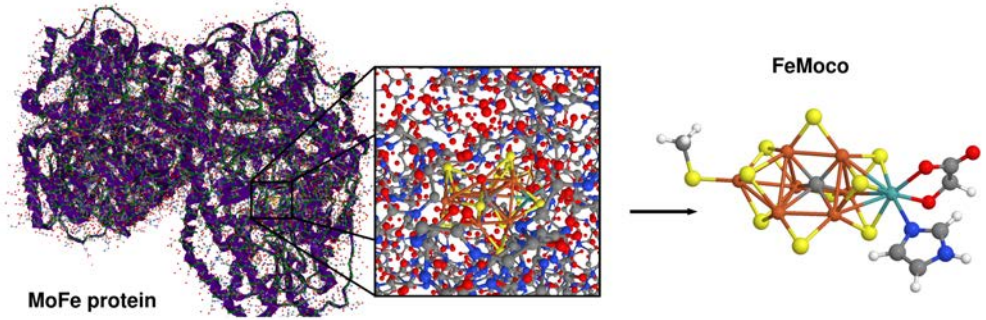


But bacteria can do it at room temperature!

Quantum solution using about 200 qubits

- Understand how bacteria manage to turn air into ammonia!
- Design a catalyst to enable inexpensive fertilizer production?





Quantum computers are around the corner

- Will solve some problems exponentially faster than the best classical algorithms
  - Break RSA and ECC cryptography
  - Accurately solve problems in quantum chemistry and materials science
  - Accelerate solving linear systems of equations and machine learning
- Quantum computers require radically different programming paradigms: reversible computing and “extreme SIMD” algorithms
- First devices will have limited number of qubits, making algorithmic optimization and hardware-software co-design crucial

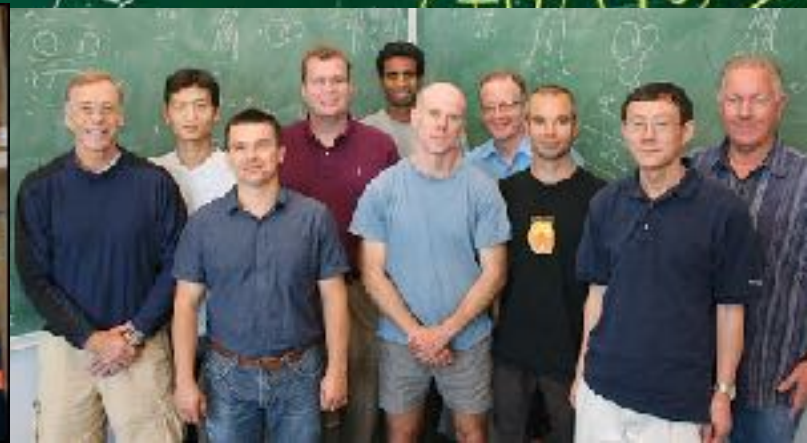
STATION Q

stationq.microsoft.com

REDMOND SYDNEY, DELFT, COPENHAGEN SANTA BARBARA

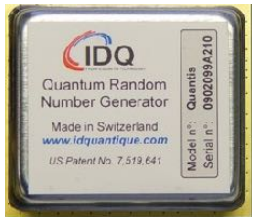






Computation is becoming quantum

- First devices can be bought
  - Quantum random numbers



  - Quantum communication
- Analog devices for solving problems
  - "solve" quantum models by implementing them in the lab

  - solve optimization problems through quantum annealing
- Quantum computers will revolutionize computing
  - Breaking of RSA encryption (?)
  - Design of catalysts and materials
  - Secure and private cloud computing

Need quantum software engineers to find more applications!

New ideas by bright students! Quantum games, quantum Facebook ….