SAND2019-12384PE

Quantum Information Science 101

Shaking the foundations of secrecy, sensing, and simulation

Dr. Rick Muller, Sandia National Laboratories

Senior Manager, Advanced Microsystems Group

Sandia National Laboratories is a multimission laboratory managed and operated by National Technology & Engineering Solutions of Sandia, LLC, a wholly owned subsidiary of Honeywell International Inc., for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-NA0003525.

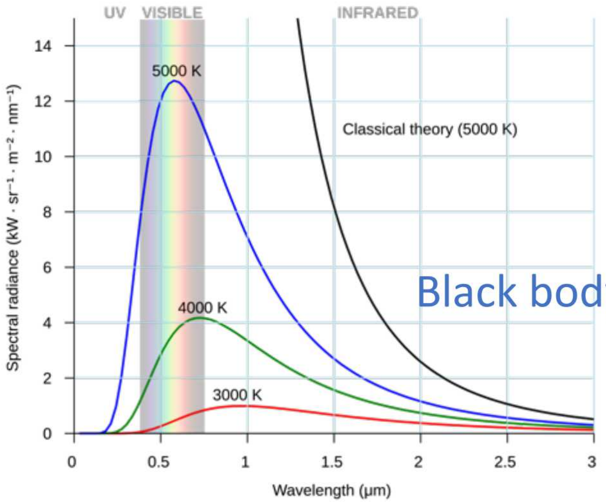
Take-Away: Quantum science impacts national security

1. QIS shakes the foundation of secrecy, sensing, and simulation
   - Computing: Breaking encryption, simulating physical systems
   - Communications: Secure communication
   - Sensing: Detecting signals
2. QIS faces challenges along the way
   - Quantum computing companies exist and sell products, but only as technology demonstrations
   - QKD companies exist and sell products, but implementation concerns persist
   - Sensing devices exist, but at R&D stage
3. Industry, academia, and other nations are awake to the Possibilities
   - Not clear whether near-term progress will sustain early hype

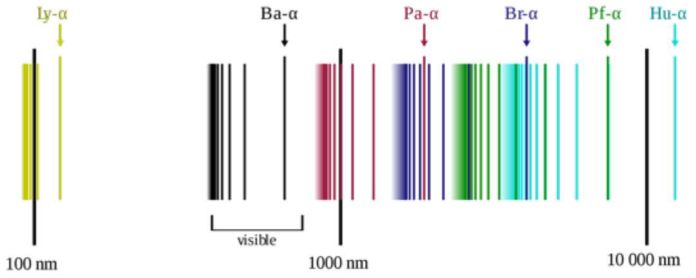
Quantum mechanics governs the physics of the small

- Physics that governs the small: atoms, molecules, small devices
- Dramatically different behavior from large-scale effects

Paradoxes



Black body radiation



Hydrogen emissions wavelengths

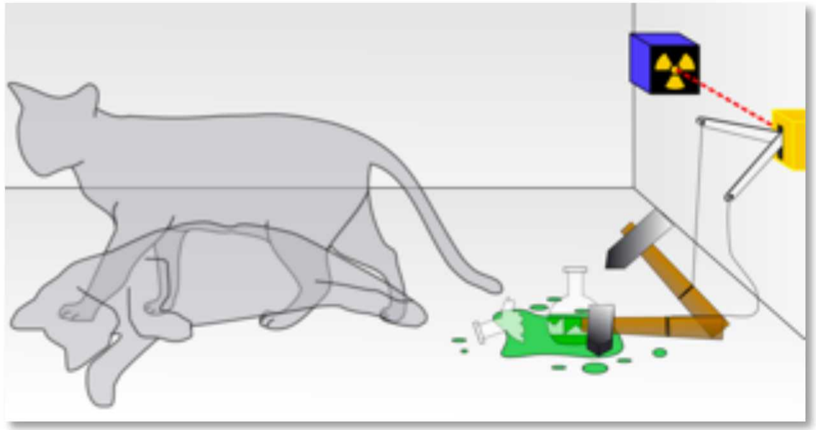
- A single theory resolved a number of paradoxes and led to transistors, lasers, medical imaging, superconductors, …

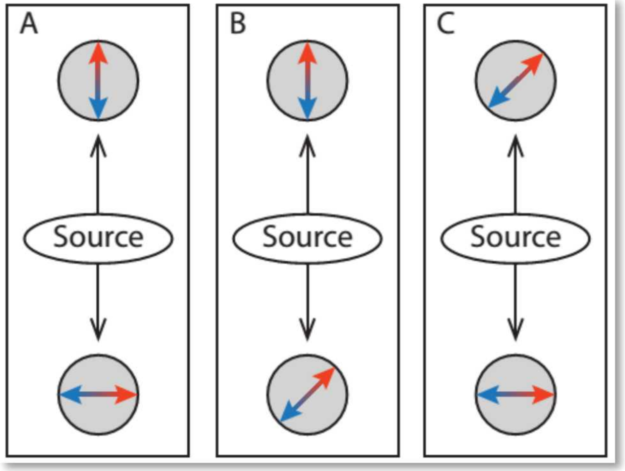
Erwin Schrodinger

Werner Heisenberg

Quantum weirdness has real implications

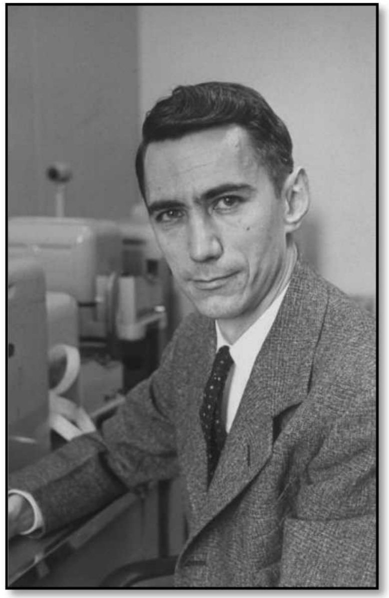
- Quantum has some celebrated oddities that aren't intuitive:
  - Schrodinger's Cat is a thought experiment demonstrating quantum superpositions: that a particle could be in multiple states at once.
  - Bell's Theorem considers the implications of quantum entanglement.
- What is surprising is that superpositions and entanglement have important implications when you combine them with information theory.





Information science tells us what we can do with information

- The science of quantifying, storing, and communicating information. Proposed by Claude Shannon in 1948.
- Understand how perfect information can be transmitted over imperfect channels.
- How we understand data compression, communication over wired and wireless channels, and the internet.
- Information is physical, and therefore obeys physical laws.



Claude Shannon
Father of Information Theory

Combining quantum with information science is transformative

- QIS considers the implications of quantum mechanics on information science.
- Computers can be more/differently powerful: “Let the computer itself be built of quantum mechanical elements which obey quantum mechanical laws.” – Feynman
- Mathematical functions could be more/differently powerful on quantum hardware: Deutsch-Jozsa demonstrates first exponential speedup.
- Shor’s factoring algorithm (1996): quantum computers could be used to factor numbers.

Dick Feynman

Peter Shor

Quantum science impacts US national security

- "Unbreakable" cryptography based on the presumed difficulty of certain math problems could be readily cracked using a sufficiently large quantum computer
- "Unsolvable" problems in pharmaceuticals and energy science could be solved using a sufficiently large quantum computer
- Networked quantum communications are plausible in the near-term, and could be provably secure
- Quantum sensing and detection devices could improve sensitivity by 10-1000
- We still don't know the full landscape of applications

"The United States' large stake in all these potential applications warrants a cohesive national effort to achieve and maintain leadership in the rapidly emerging field of quantum information science."
-Dr. Jack Marburger, former DOSTP, 1/2009

From A Federal Vision for Quantum Information Science.

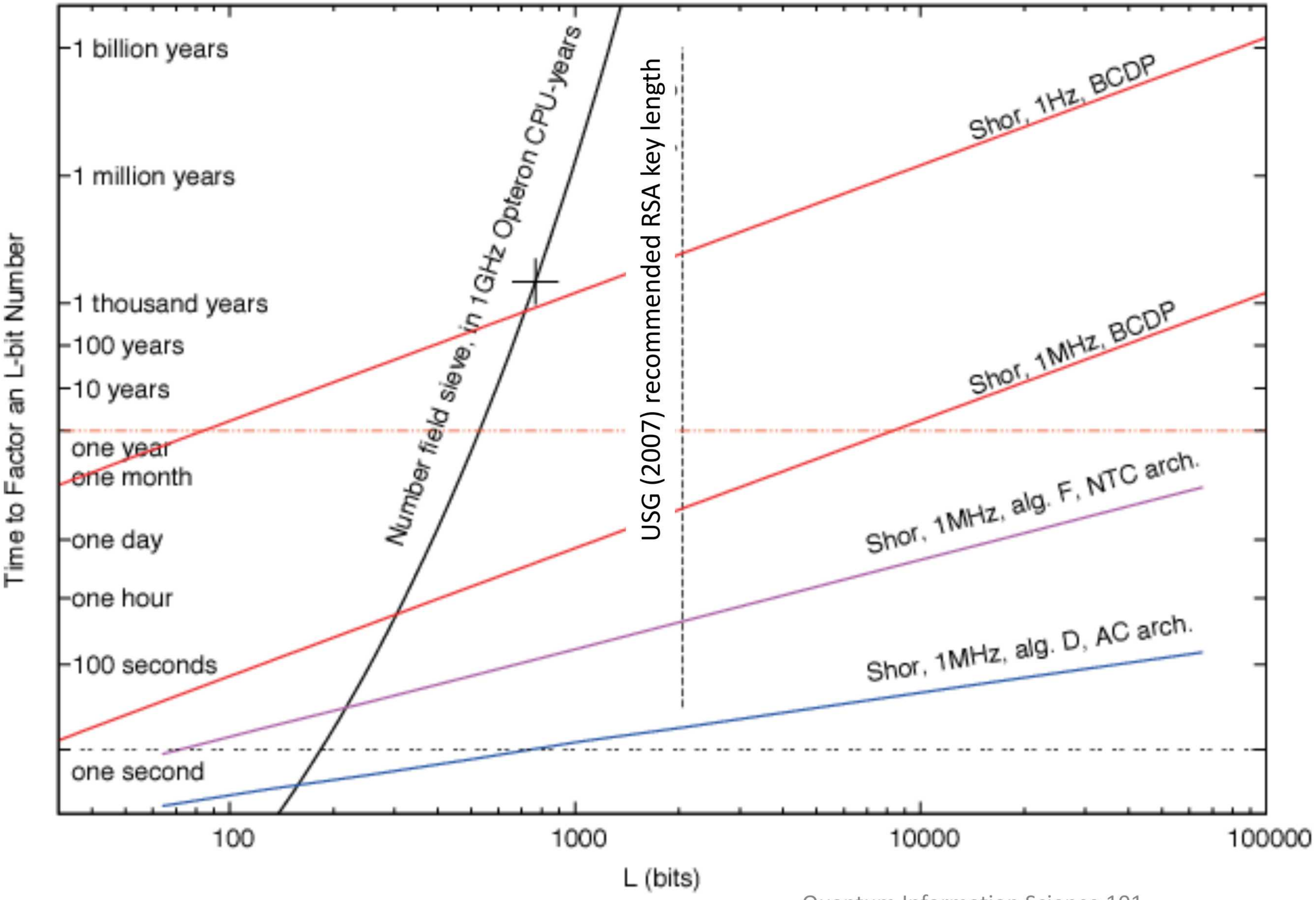
Introduction to Cryptography

- One-time pads can yield unbreakable codes, provided the keys can be securely distributed.
- Mechanical cypher machines like the Enigma Machine were early attempts to distribute keys more securely.
- Public key cryptography uses a one-way function to distribute keys:
  - Problem like multiplication/factoring:
    - Easy to multiply 1000-digit numbers,
    - Hard to factor 1,000,000-digit number
  - Depends upon hardness of the one-way function:
    - If a way to factor numbers quickly is discovered, security of encryption is jeopardized.

Part of a one-time pad. Source Wikipedia.

Enigma machine, National Cryptologic Museum.

Quantum shakes the foundations of cryptanalysis



NIST recommended RSA key length:

- Classical (black): Requires trillions of years on a classical computer
- Quantum (red-purple): Could be solved in seconds-days on a quantum computer.

A blueprint for building a quantum computer, R. van Meter & C. Horsman, *Comm. ACM*, (2013) doi:10.1145/2494568

Quantum shakes the foundation of chemistry

- The Haber process converts nitrogen into ammonia, and consumes roughly 2% of the world's energy supply.

$$\underbrace{\mathrm{N_2} + 3\,\mathrm{H_2}}_{\Delta H^\circ = 0\,\mathrm{kJ}} \longrightarrow \underbrace{2\,\mathrm{NH_3}}_{\Delta H^\circ = -91.8\,\mathrm{kJ\cdot mol^{-1}}}$$

- The Haber process requires large factories with high temperatures and pressures, but plants perform nitrogen fixation every day.
- With technology that could be developed in the next 20 years, a quantum computer could unravel biological nitrogen fixation.

Fritz Haber

Elucidating Reaction Mechamisms on a Quantum Computer. Reiher et al., PNAS (2017)

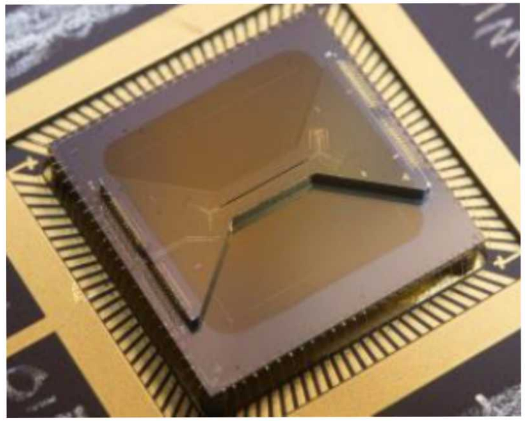
Important to separate quantum hype from reality

- Creating, distributing, and maintaining quantum coherence remains a major challenge to all areas of quantum information sciences.
- Quantum states are *fragile*: with the power of quantum applications comes sensitivity to *noise*, and *quantum decoherence*.
- Quantum error correction is possible, but requires large overhead.
- Finding applications that can make use of non-error-corrected hardware is a major priority.

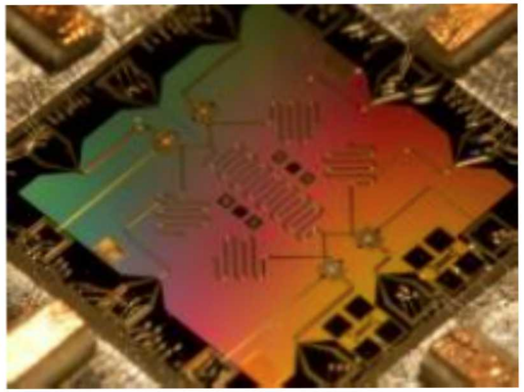
The vast majority of what a quantum computer will do is correct its own errors.

Examples of qubits

Today

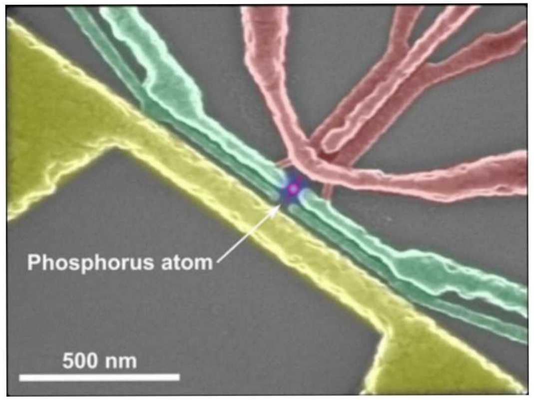


Trapped ions

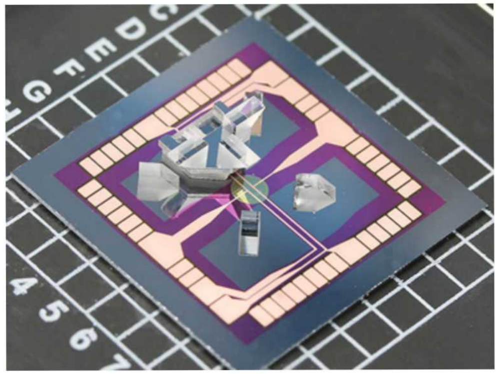


Superconducting

Tomorrow

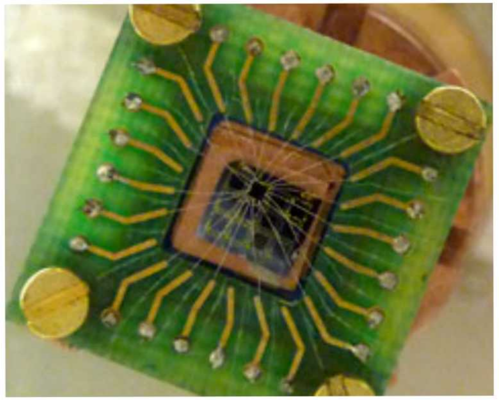


Semiconducting

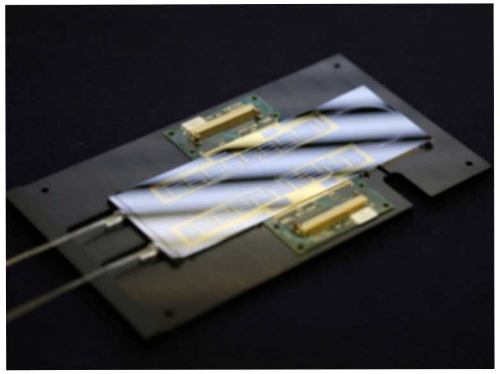


Trapped atoms

Future



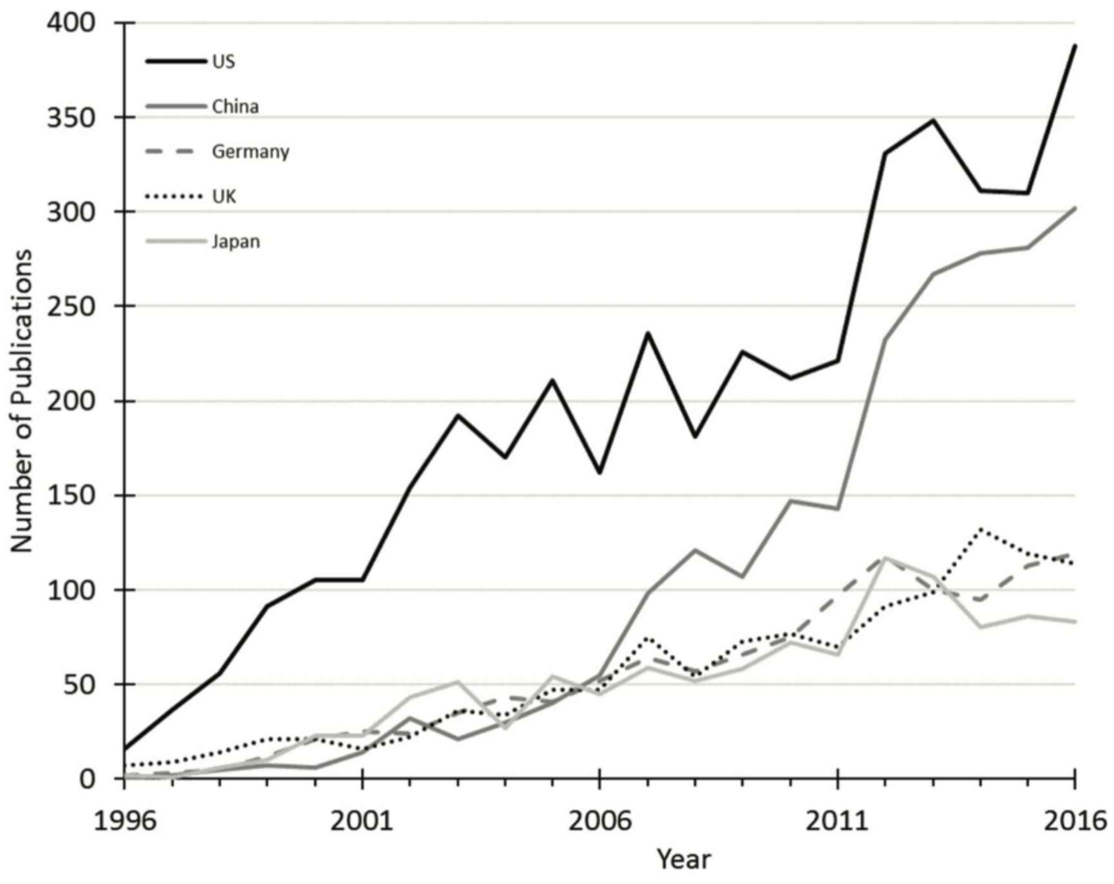
Topological



Photonic

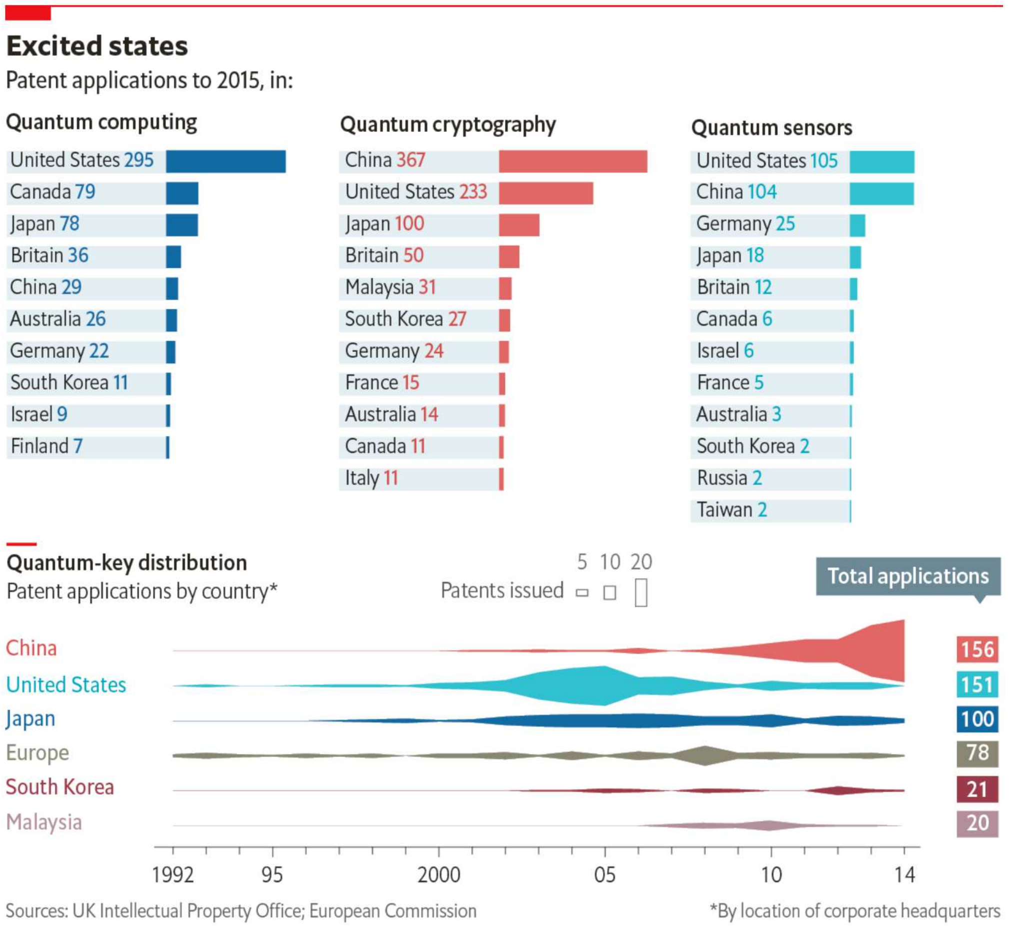
Quantum is growing worldwide

Publications



Quantum Computing: Progress and Prospects. *National Academy of Sciences,* 2019

Patent Applications



Quantum Technology is Beginning to Come Into Its Own. *Economist,* 2017

Take-Away: Quantum science impacts national security

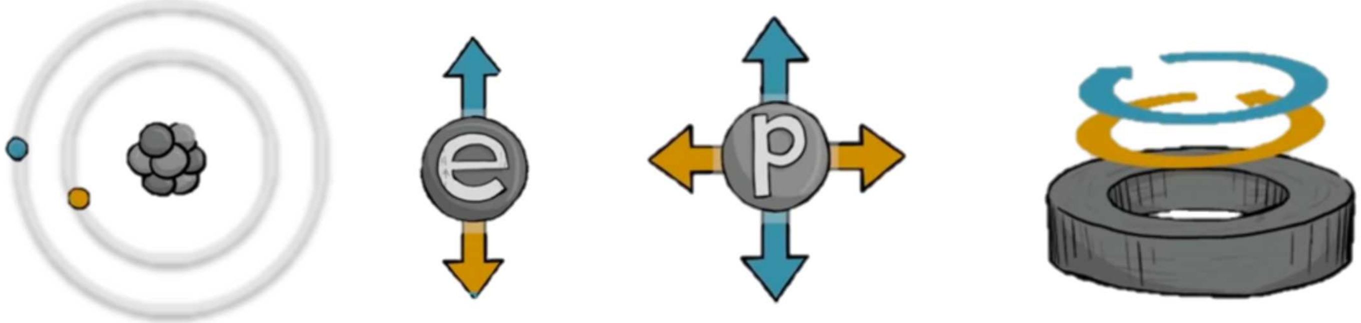
1. QIS shakes the foundation of secrecy, sensing, and simulation
   - Computing: Breaking encryption, simulating physical systems
   - Communications: Secure communication
   - Sensing: Detecting signals
2. QIS faces challenges along the way
   - Quantum computing companies exist and sell products, but only as technology demonstrations
   - QKD companies exist and sell products, but implementation concerns persist
   - Sensing devices exist, but at R&D stage
3. Industry, academia, and other nations are awake to the Possibilities
   - Not clear whether near-term progress will sustain early hype

Backup slides

Requirements for building a quantum computer

The DiVincenzo criteria (simplified)

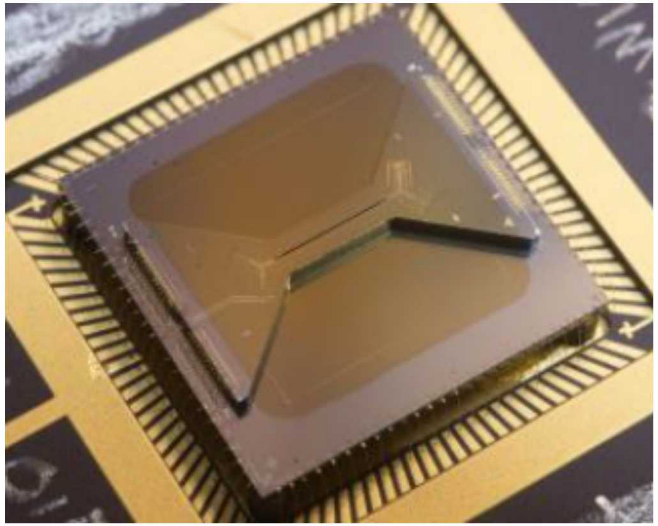
1. A scalable, high-fidelity qubit processing technology
2. A computer architecture for organizing the components
3. Methods for suppressing runtime errors

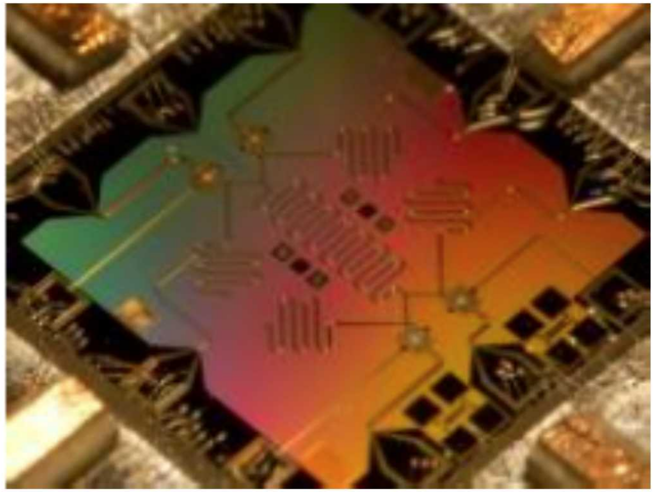


Atomic state **Electron spin** **Photon polarization** **Superconducting current**

The vast majority of what a quantum computer will do is correct its own errors.

Current qubits: ions and superconductors

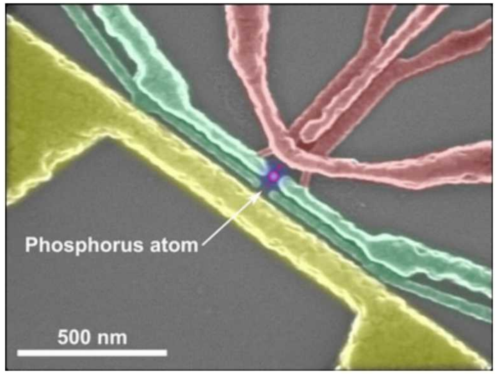


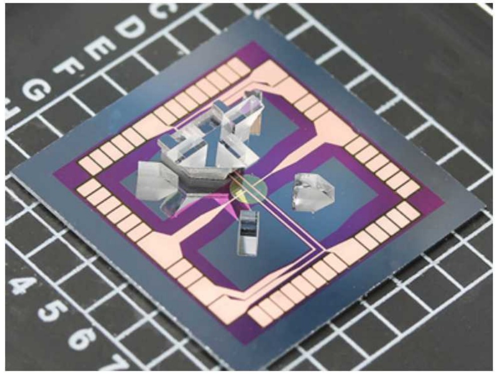


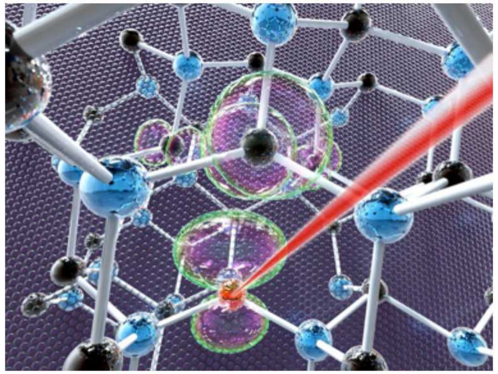
- Trapped-ion chip
  - RF, DC control electrodes confine ions
  - Be, Ca, Sr, Yb ions are common
  - Demos: Q. error correction, q. algorithms,
  - Scale: 219 entangled, only 14 controllable
  - Expertise: Sandia, NIST, IonQ, Honeywell
- Superconducting Josephson junctions
  - Microwaves travel in aluminum transmission lines
  - Charge, flux, or phase used as the qubit
  - Demos: Q. error correction, q. algorithms
  - Scale: 20 entangled and controllable
  - Expertise: Google, IBM, Intel

Next-generation qubits: semiconductors and atoms

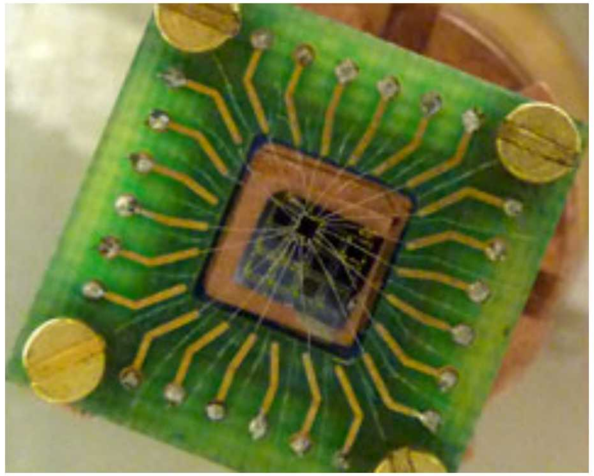
- Silicon quantum chip
  - Quantum dots or donors trap individual electrons
  - Leverages $3T silicon chip industry
  - Expertise: Sandia, Intel, UNSW
- Trapped-atom chip
  - Cs atoms trapped in an optical lattice above the chip
  - 3,000-atom entanglement demonstrated
  - Expertise: Harvard, Wisconsin, Sandia
- Diamond-defect chip
  - Nitrogen vacancies (NVs) form qubits
  - Operates at room temperature
  - Expertise: Chicago, Harvard, Melbourne

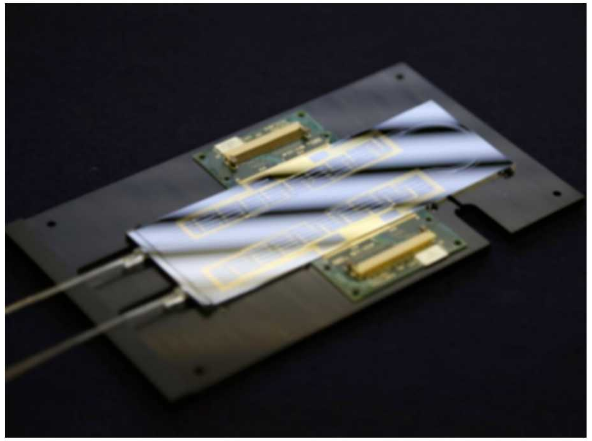






Disruptive qubit technology: topological and photonics





- Topological qubit chip
  - “Anyons” interact topologically in semiconductors
  - May require multiple Nobel Prize discoveries
  - Drastic reduction in QEC anticipated
  - Expertise: Microsoft, Purdue
- Photonic chip
  - All-optical quantum computing
  - New modes of QEC may be required
  - Eliminates matter/photon qubit transducers
  - Expertise: Psi-Quantum

Quantum Teleportation

$\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ Create Entanglement

Distribute it to Alice and Bob

$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$

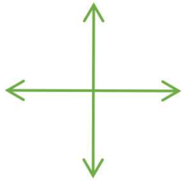
$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$

Alice

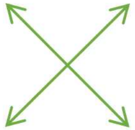
Two classical bits

Bob

BB84 (Measurement-Based) QKD



Rectilinear Basis



Diagonal Basis

- Quantum information encoded in photon polarization
- Commercially available
  - id Quantique, MagiQ, SmartQuantum

N = length of key

Alice

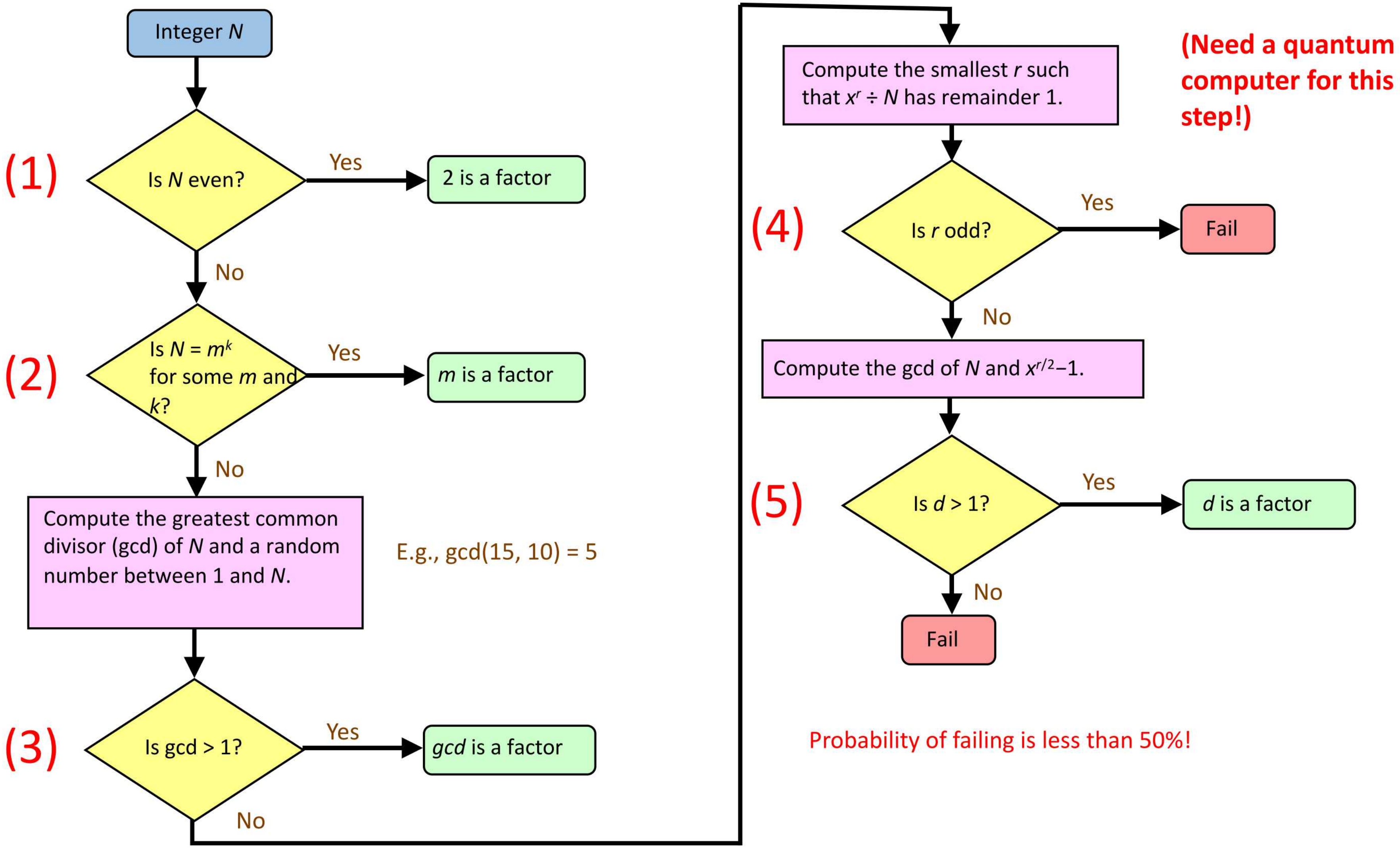
4*N photons, random bases

On average, Bob got 50% right.

Bob

Measure photons using randomly selected bases

Quantum factoring in five easy steps

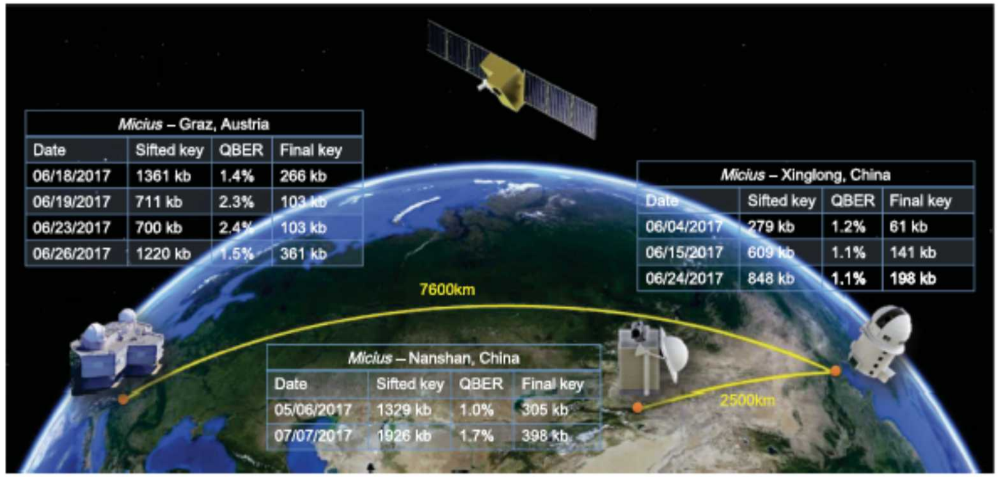


Gary Miller, PhD 1975

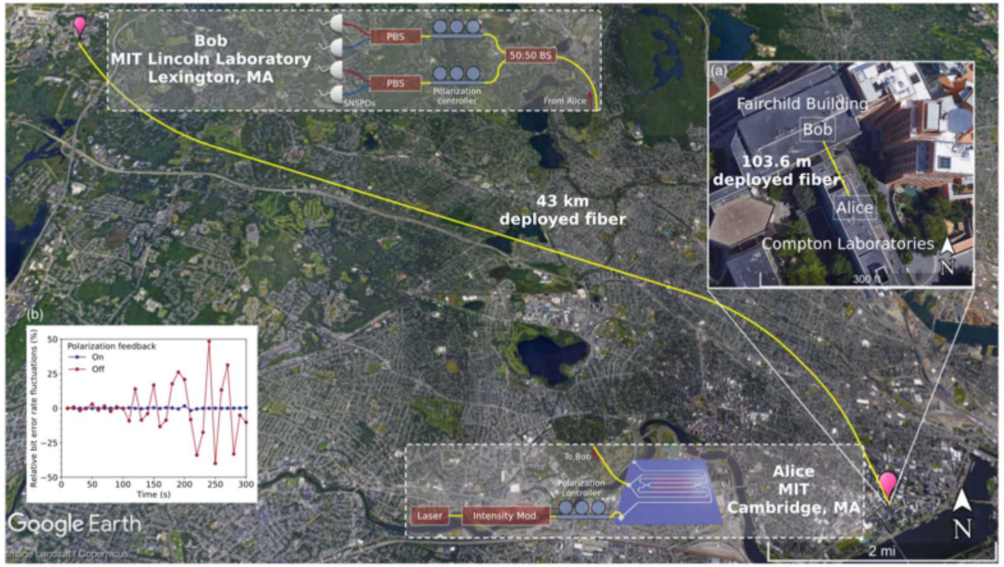
Deploying QKD: Fiber, free space, and networks

- State of the art
  - 500-1400 km ground-satellite QKD and state teleportation (Pan, 2017)
  - …used to distribute QKD keys between Europe-China (Pan, 2017)
  - On-chip silicon photonics used for Metropolitan Boston QKD (SNL,BYU,MIT, 2018)
  - ~100 MHz QKD rate

PHYSICAL REVIEW LETTERS 120, 030501 (2018)



Satellite-linked Europe-China QKD



43 km Boston fiber QKD link