Quantum information: What is it and why you should care

Edo Waks

Department of Electrical and Computer Engineering

University of Maryland College Park

A. JAMES CLARK SCHOOL OF ENGINEERING

JOINT QUANTUM INSTITUTE

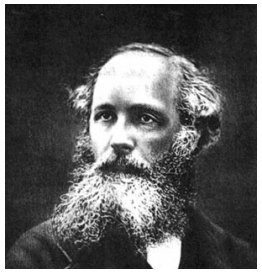
What is quantum mechanics?

Classical Physic: Macroscopic objects

Isaac Newton

$$\mathbf{F} = m\mathbf{a}$$

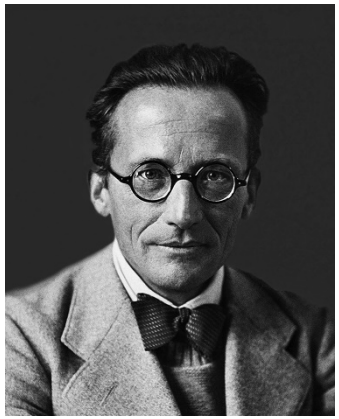
James Clerk Maxwell



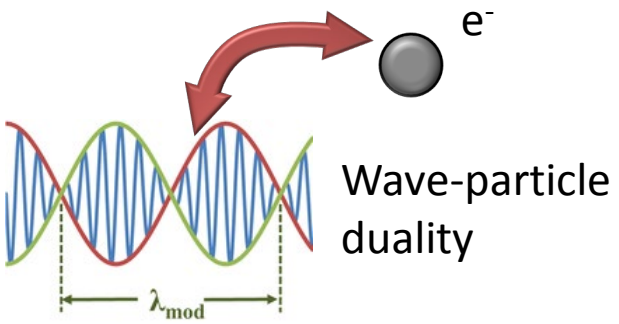
$$\nabla \times \mathbf{B} = \mu_0 \varepsilon_0 \frac{\partial \mathbf{E}}{\partial t}$$

Quantum Physics: Microscopic objects

Erwin Schrodinger



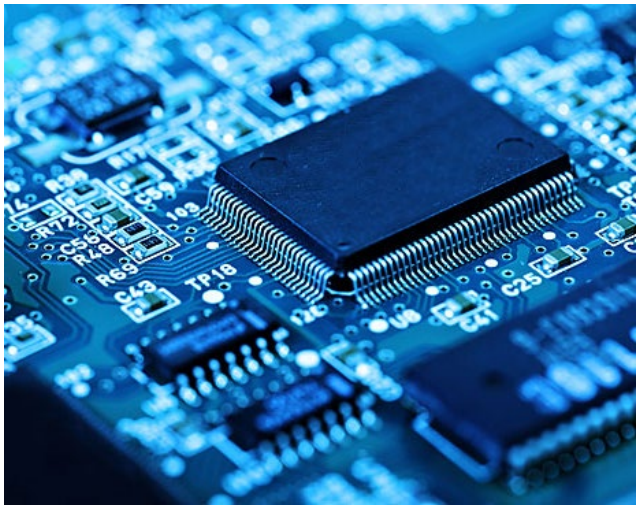
$$i\mathrm{h}\frac{\partial \psi}{\partial t} = -\mathrm{h}^2 \frac{\nabla^2 \psi}{2m}$$



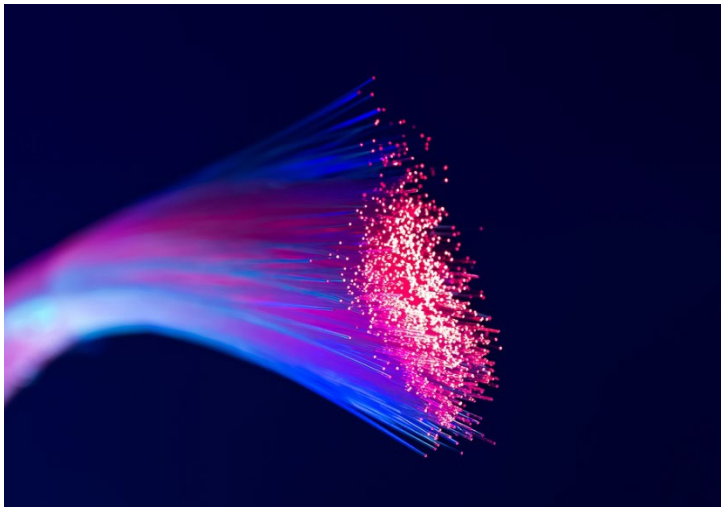
Wave-particle duality

Today's information technology is classical

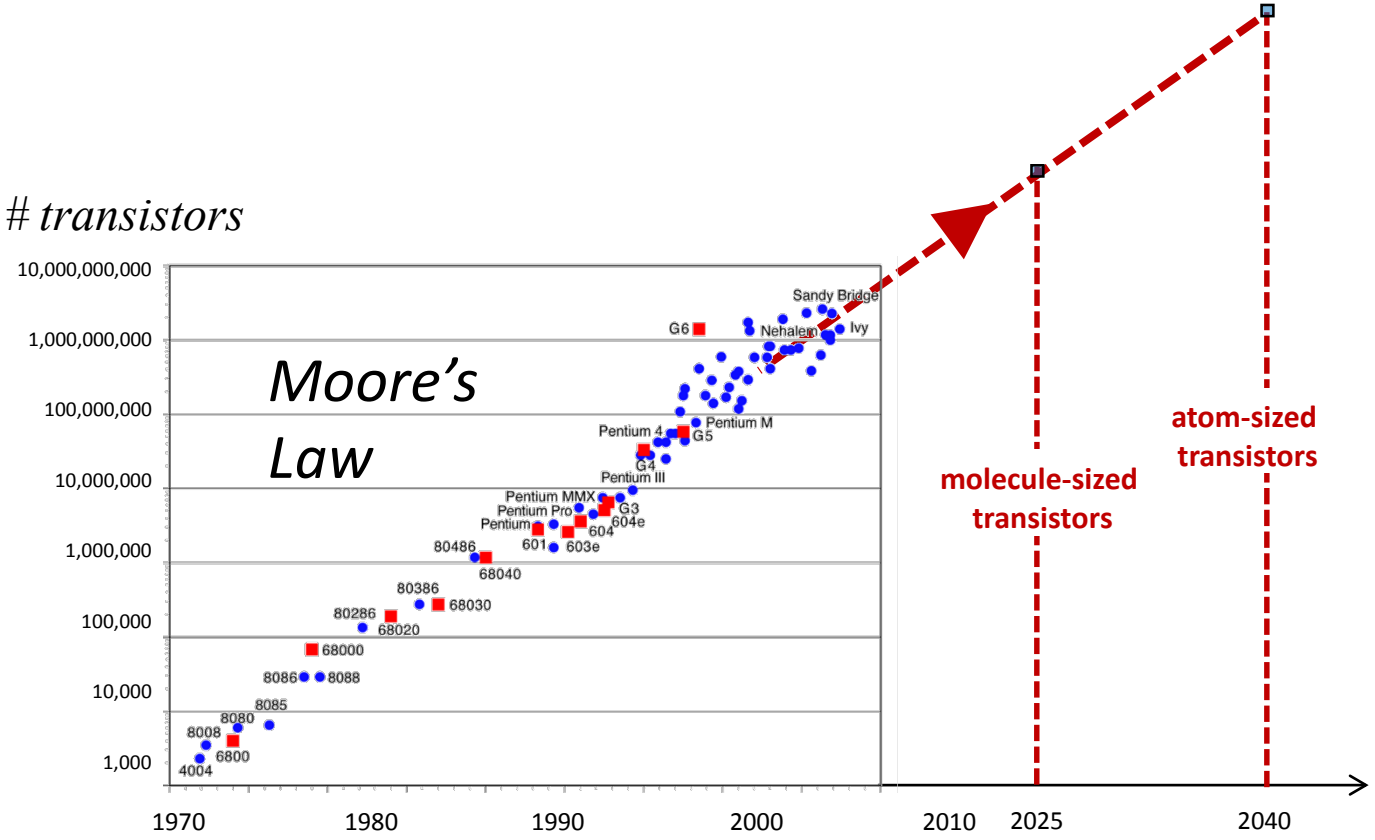
Many atoms/electrons



Many photons



Electronics is shrinking



Richard Feynman

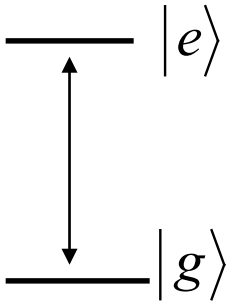
"Atoms on a small scale behave like nothing on a large scale, for they satisfy the laws of quantum mechanics…"

Bits are the fundamental units of information

Classical Bit

0 – Switch up
1 – Switch down

Quantum Bit (qubit)



0 – atom is in ground state $|g\rangle$

1 – atom is in excited state $|e\rangle$

$$\text{Ground state} = |0\rangle$$

$$\text{Excited state} = |1\rangle$$

Qubits can do things that classical bits can't

Superposition states:

Qubits can exist in two states at once

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

Measurement back-action:

By looking you destroy

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

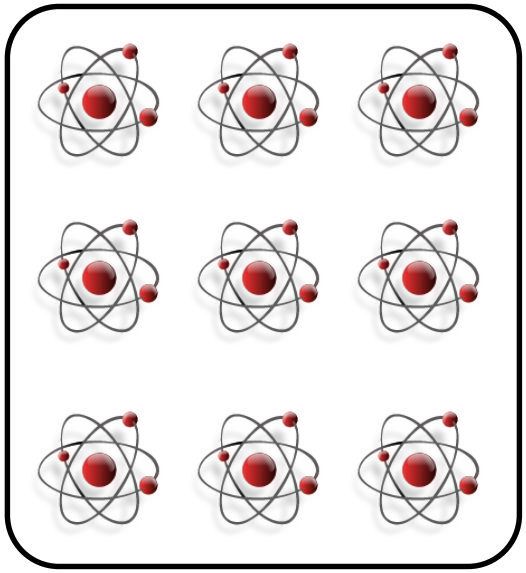
$$|\alpha|^2 = P(0)$$

$$|\beta|^2 = P(1)$$

$$|0\rangle \qquad |1\rangle$$

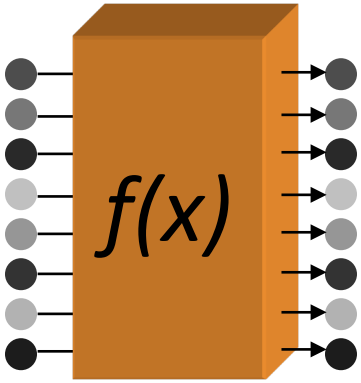
Quantum computers exhibit massive quantum parallelism…

Quantum Computer



$$\underbrace{|x_1\rangle|x_2\rangle\mathsf{L}\ |x_n\rangle}_{\text{Inputs}}\underbrace{|y_1\rangle|y_2\rangle\mathsf{L}\ |y_n\rangle}_{\text{Outputs}} = |i\rangle|j\rangle$$

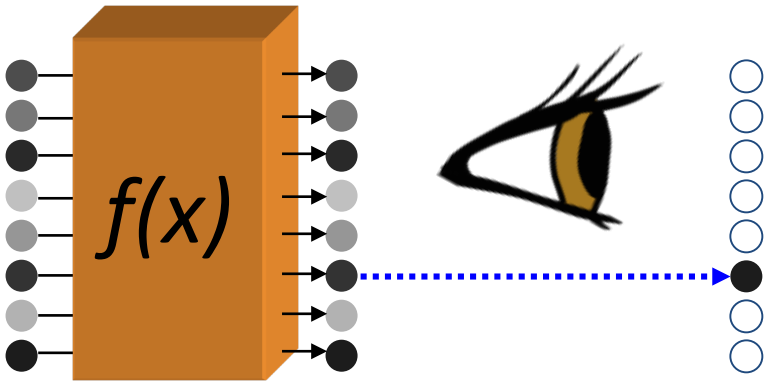
$$|k\rangle|0\rangle \rightarrow |k\rangle|f(k)\rangle$$



Quantum algorithms:

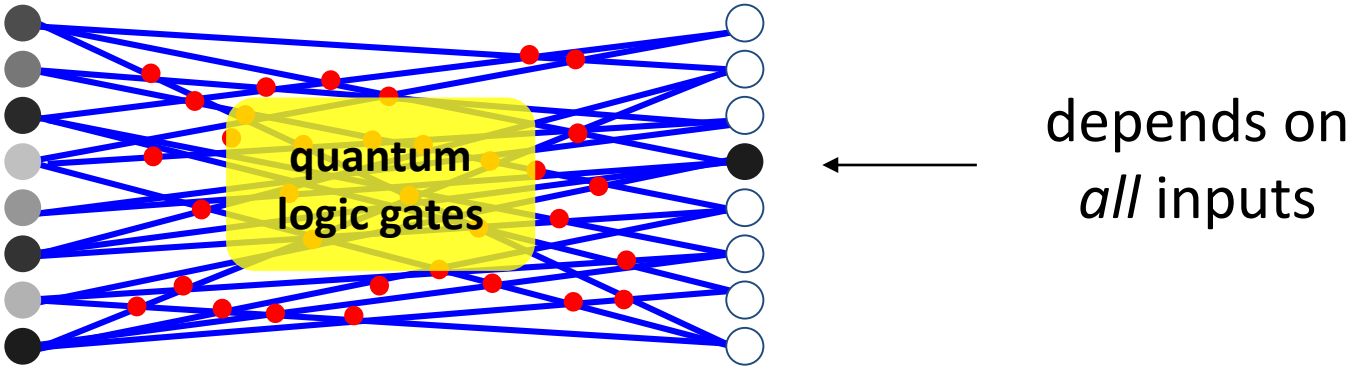
$$|\psi_i\rangle = \frac{1}{\sqrt{2^n}}\sum_k |k\rangle|0\rangle \rightarrow \frac{1}{\sqrt{2^n}}\sum_k |k\rangle|f(k)\rangle$$

…but only if you don't look at the result!



We get one random result

Quantum algorithms extract global properties using quantum interference



Example: Quantum algorithms factor prime numbers exponentially faster

Peter Shor

- Best classical algorithm: $O\left(2^{n^{1/3}}\right)$ – Exponential time

Public Key Cryptography (RSA) relies on this!

- Shor's algorithm: $O\left(n^3\right)$ – Polynomial time

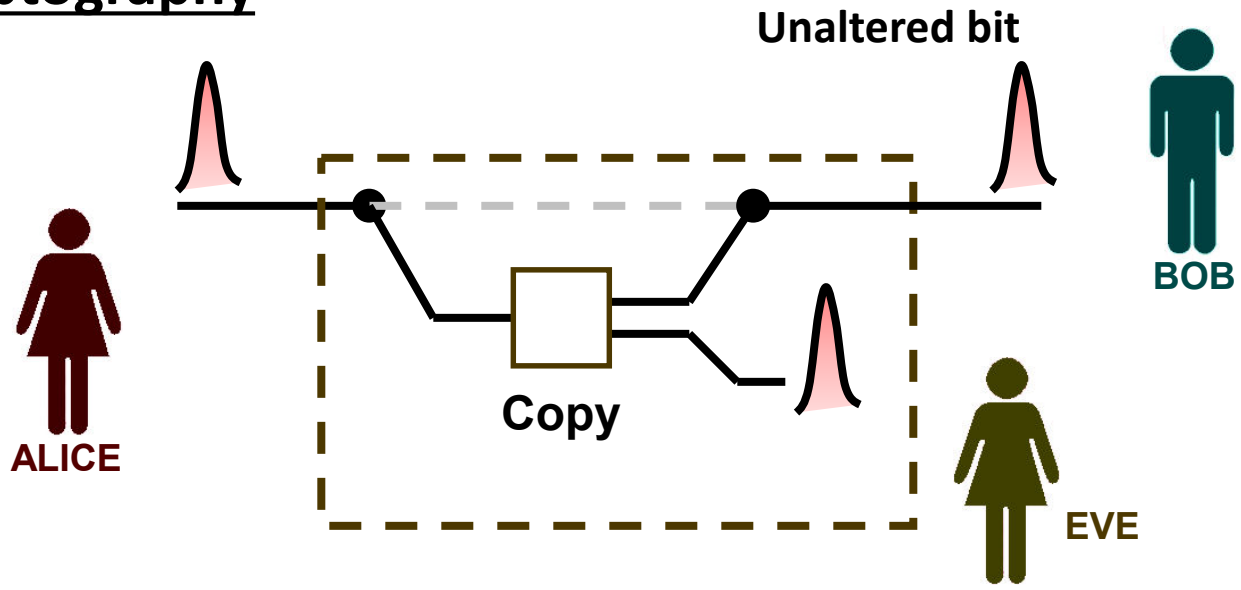
A zoo of quantum algorithms

- Quantum search
- Pattern matching
- Quantum Chemistry
- Optimization
- Machine learning

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

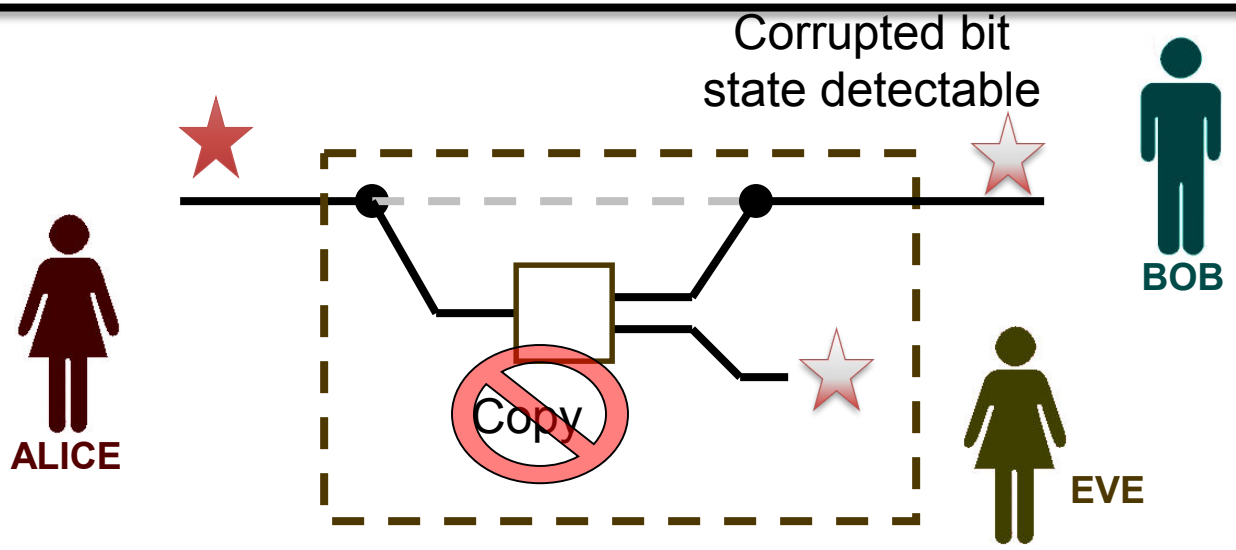
Measurement back-action can be a good thing

Cryptography



- We need to introduce additional assumptions
- Assumptions invalid → all past and present communication insecure

Quantum cryptography delivers unconditional physics-based security



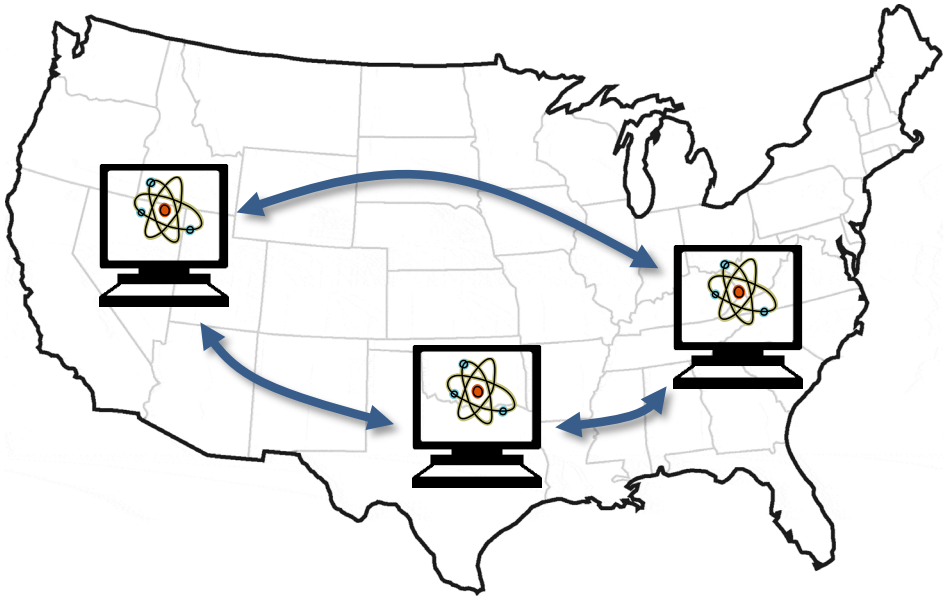
- Security guaranteed by laws of quantum physics.
  - Uncertainty principle
  - Bell's Theorem
- Security is guaranteed for all time; Eve cannot copy a quantum signal.

Available at a store near you

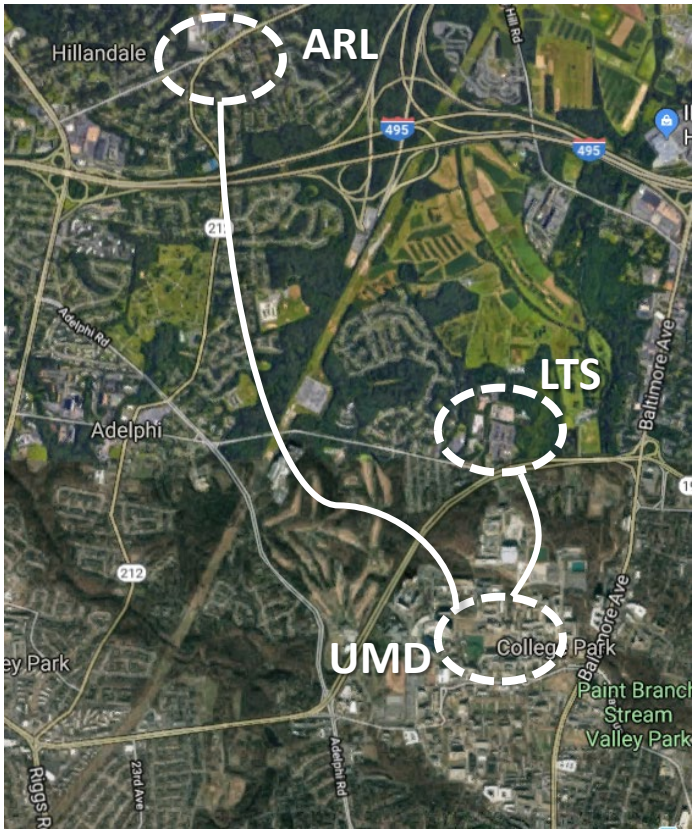
id Quantique

A Quantum Leap for Cryptography

A quantum internet connects quantum computers with photons



A local quantum network

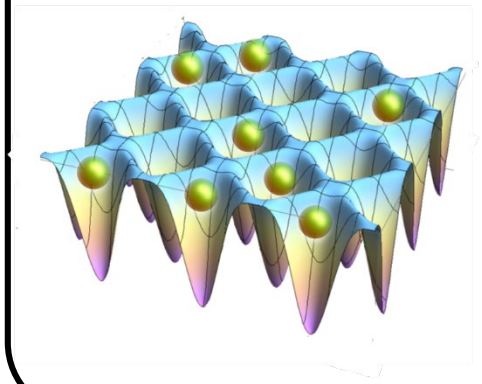


Quantum systems are sensitive to the environment

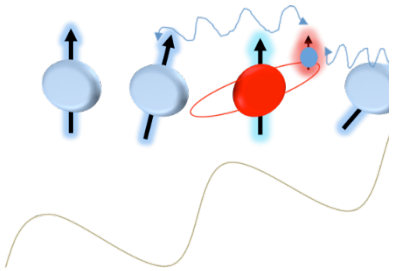
- **Bad for quantum computing (decoherence)**
- **Good for sensors**

Quantum sensors

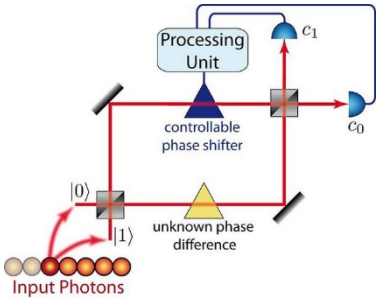
Quantum gyroscope



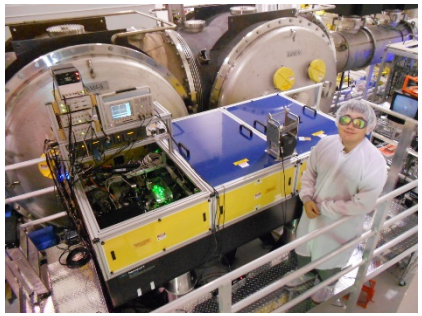
Magnetometer



Precision phase sensor

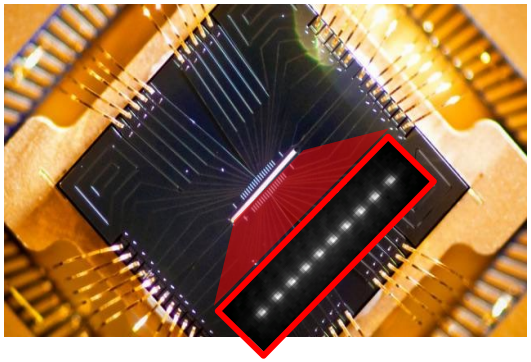


Gravitational waves

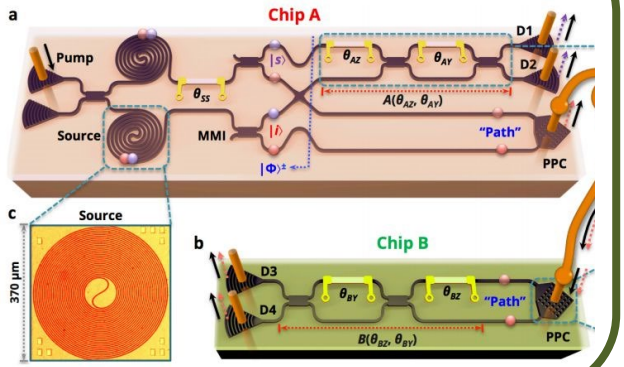


The best hardware remains anyone's guess

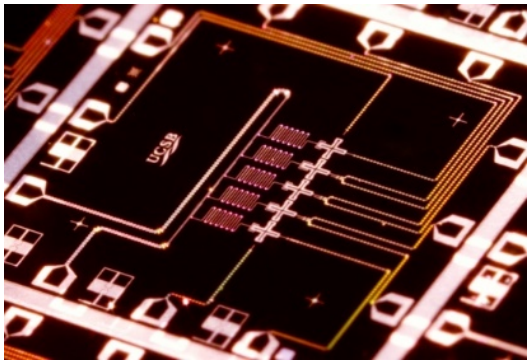
Atoms



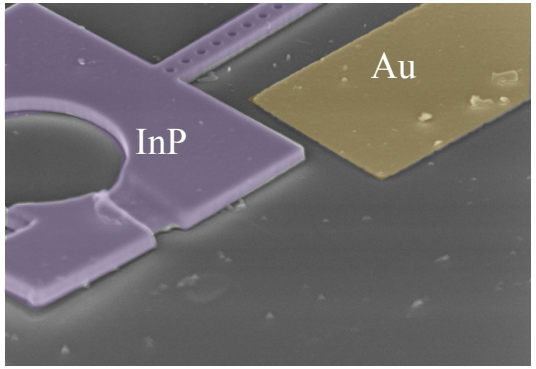
Photonics



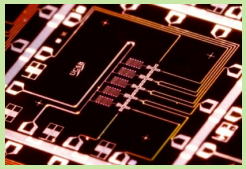
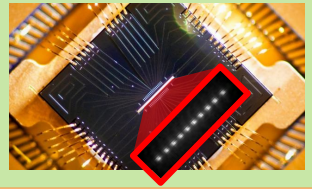
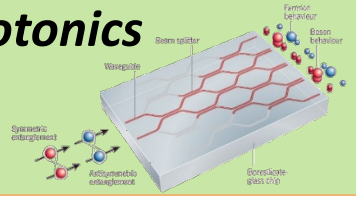
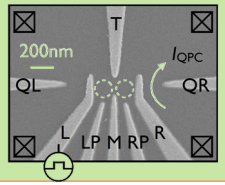
Superconductors



Semiconductors



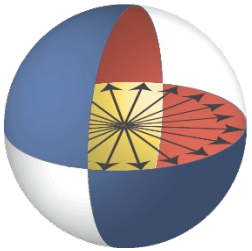
A new industry is emerging

Superconductors 	IBM Google Intel Northrop Raytheon-BBN	D-Wave Systems (Vancouver) Rigetti Computing (Berkeley) Quantum Circuits, Inc. (New Haven)
Atomic Systems 	Honeywell	IonQ, Inc. (College Park)
Photonics 	Hewlett-Packard	ID Quantique (Geneva) MagiQ (Cambridge, MA) Sparrow Quatum (Copenhagen) PsiCorp (San Jose)
Semiconductors 	Intel Microsoft Hughes Research	

UMD is the premier institute for quantum science

JOINT QUANTUM INSTITUTE

- 30 Principal Investigators
- 150 postdoctoral & graduate researchers



JOINT CENTER FOR QUANTUM INFORMATION AND COMPUTER SCIENCE

- 10-12 Principal Investigators
- 20-30 postdoctoral & graduate researchers

QTC **Quantum technology Center**

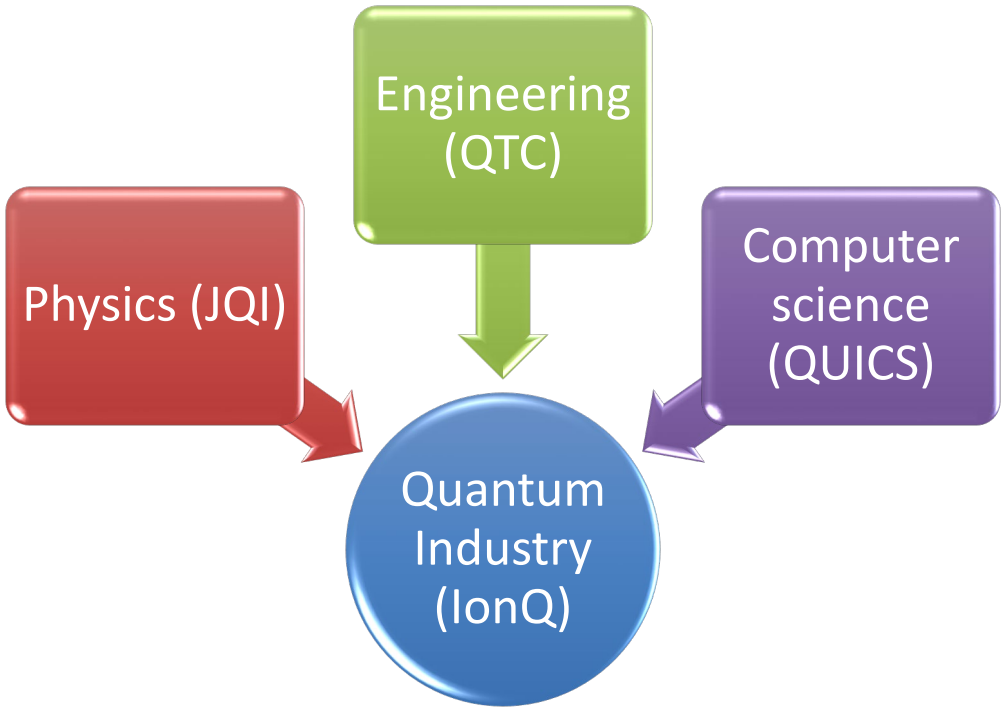
- 8 Faculty
- Hiring 2 more

NIST

DARPA

IARPA
BE THE FUTURE

Maryland is in a position to lead this new industry

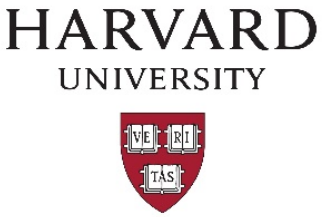


Effort across many departments

Physics
Electrical Engineering
Computer Science
Material Science
Chemistry
Mechanical Engineering

The competition is fierce

Universities



Industry

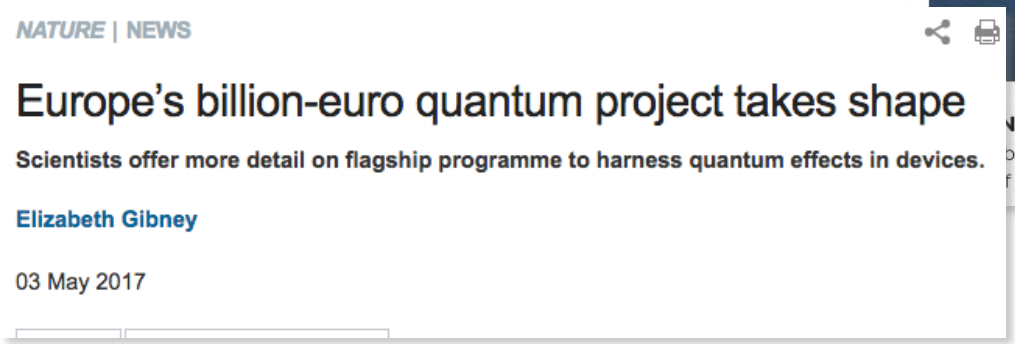
A Quantum Arms Race?

UK : $400 M

NAL LABORATORY FOR QUANTUM INFORMATION SCIENCES

billion National Laboratory for Quantum Information Sciences in Hefei will be the
China's attempt to take the global lead in quantum computing and sensing.

China : $10 B



NATURE | NEWS

Europe's billion-euro quantum project takes shape

Scientists offer more detail on flagship programme to harness quantum effects in devices.

Elizabeth Gibney

03 May 2017

EU : $1.3 B

Current US : ~ $200 M per year?

National Quantum Initiative

- Grew out of a National Photonics Initiative (OSA SPIE)
- Support from previous efforts at OSTP
- Very likely to be announced soon
- *5 NQI Centers, funded at $25M per year for five years?*
  - *and we hope to have one at UMD!*
  - *Each center would include University, Fed Lab, Industry*

Outlook

- Quantum could revolutionize computation, communication, and sensing

- Quantum technology is becoming a reality

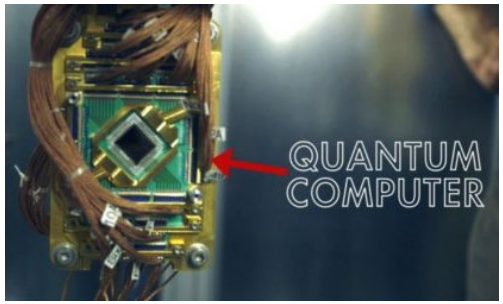
Maryland could be the center of a new industry

Thank You!

Backups

A new industry is emerging

Superconducting



Google

rigetti

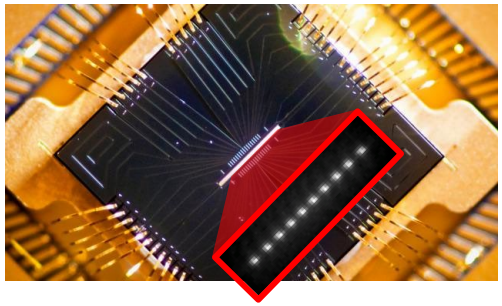
IBM

intel

NORTHROP GRUMMAN

Raytheon
BBN Technologies

Atoms

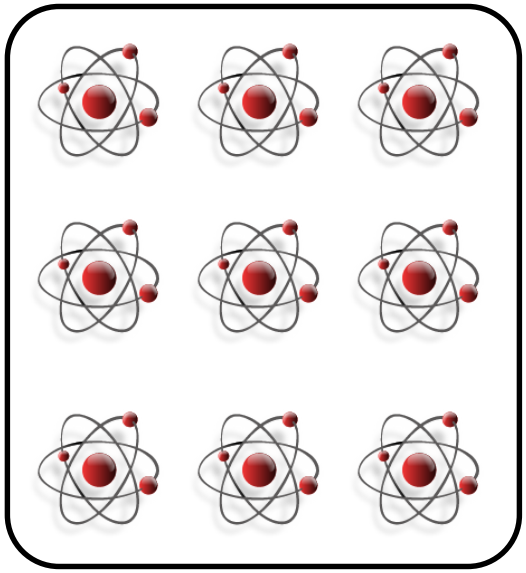


IONQ

Honeywell

Quantum computers exhibit massive quantum parallelism…

Quantum Computer

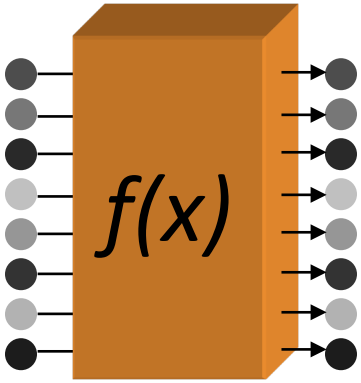


$$|x_1\rangle|x_2\rangle\mathsf{L}\ |x_n\rangle|y_1\rangle|y_2\rangle\mathsf{L}\ |y_n\rangle = |i\rangle|j\rangle$$

Inputs Outputs

$$x_i, y_i - [0,1] \qquad i, j - [0,2^n - 1]$$

$$|k\rangle|0\rangle \rightarrow |i\rangle|f(i)\rangle$$



Quantum algorithms:

$$|\psi_i\rangle = \frac{1}{\sqrt{2^n}}\sum_k |k\rangle|0\rangle \rightarrow \frac{1}{\sqrt{2^n}}\sum_k |k\rangle|f(k)\rangle$$