Information, Quantum Mechanics and the Universe

Jeremy Levy

Pittsburgh Quantum Institute (pqi.org)

University of Pittsburgh (levylab.org)

<P|Q|I>

SAC-PA2: Towards Security Assured Cyberinfrastructure in Pennsylvania

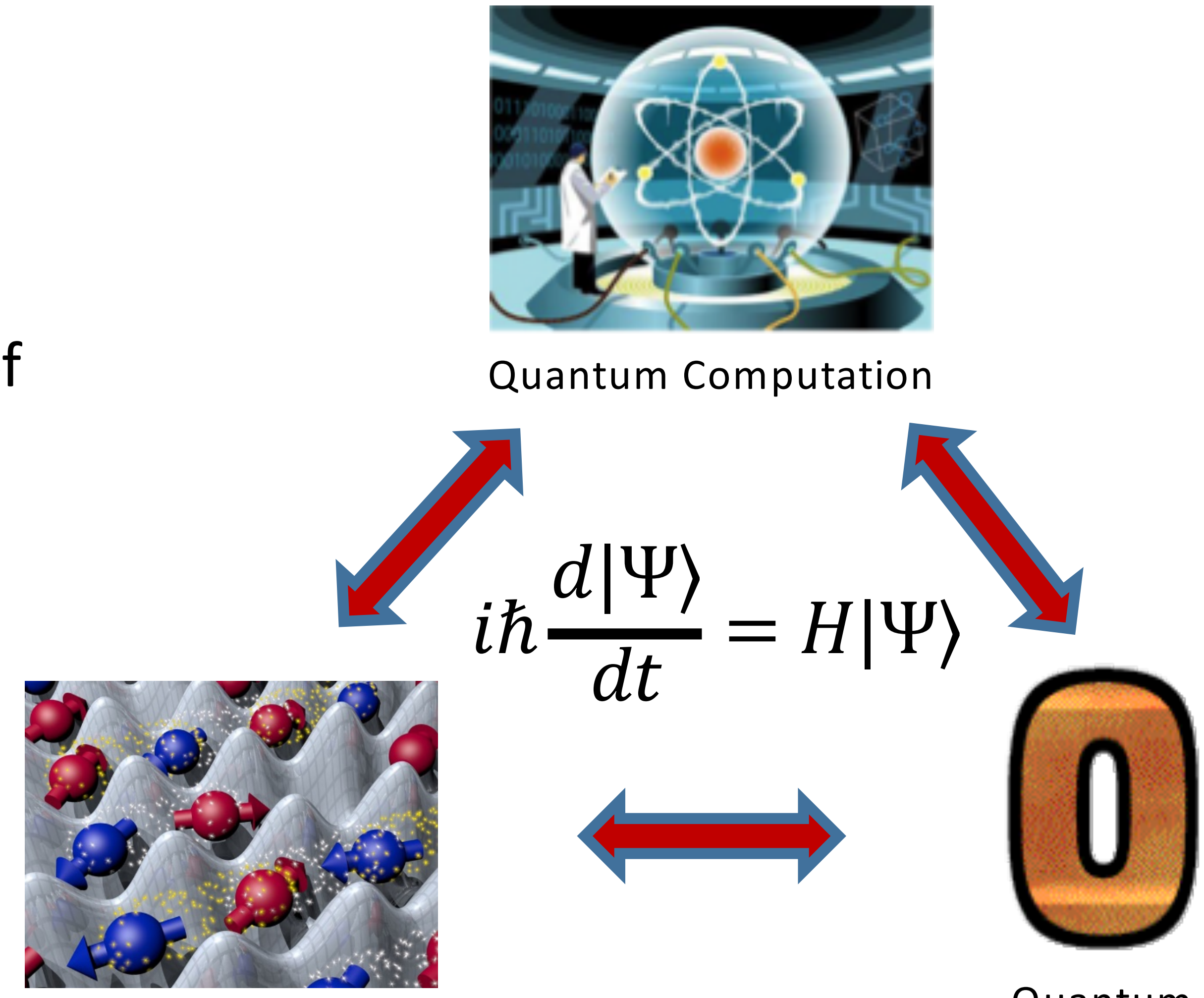
University of Pittsburgh School of Computing and Information

15 June 2018

Quantum Computing Essentials

Three Key Concepts

- Quantum computation
  - Massive speedup of certain types of computation
- Quantum bits (qubits)
  - Building block of quantum computers…
  - …and quantum matter
- Quantum matter
  - Form the basis of all qubits



Quantum Computation

$$i\hbar\frac{d|\Psi\rangle}{dt} = H|\Psi\rangle$$

Quantum Matter

Quantum Bits

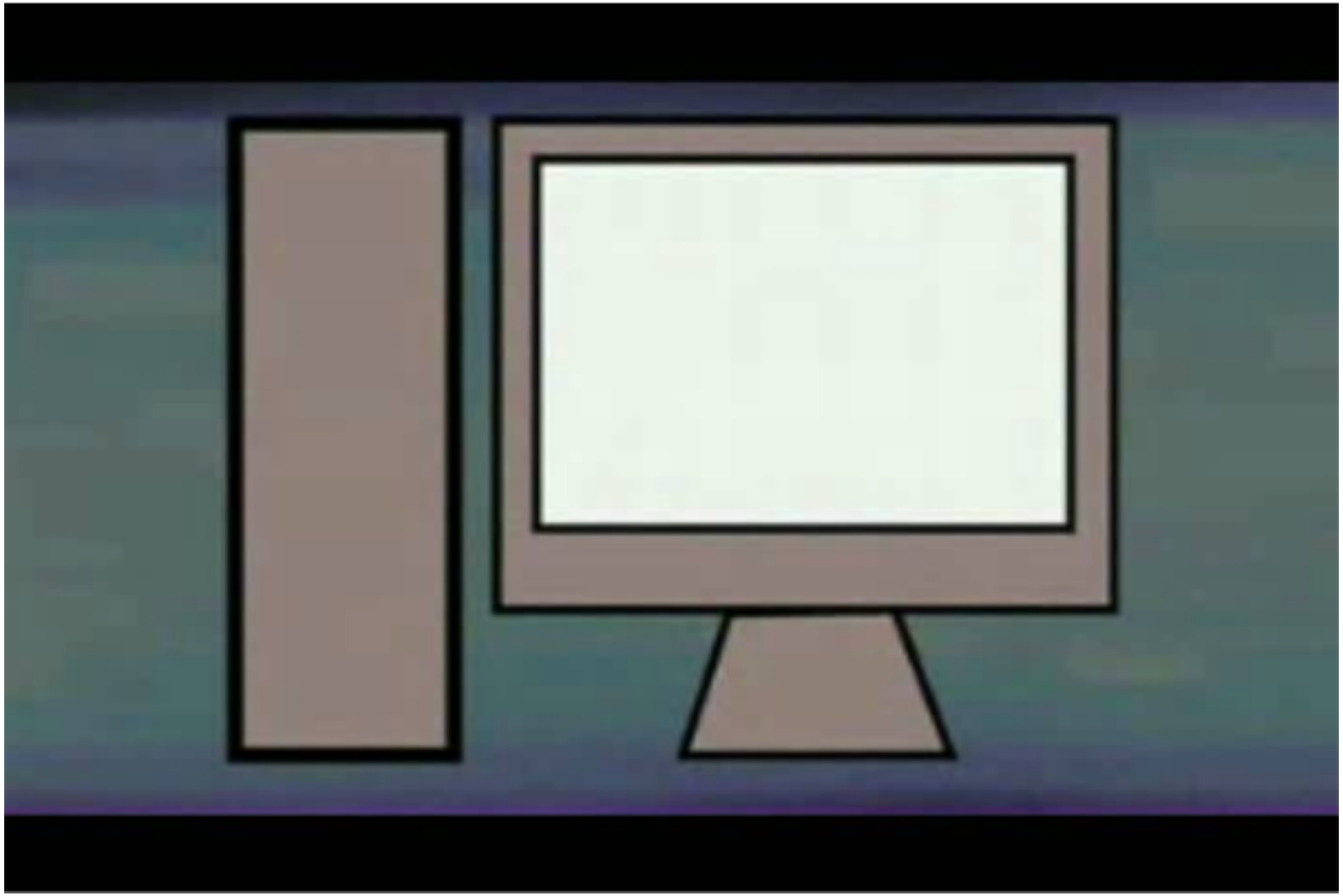
Start with big picture…

Information and the Universe

What is information?

Bits of Information

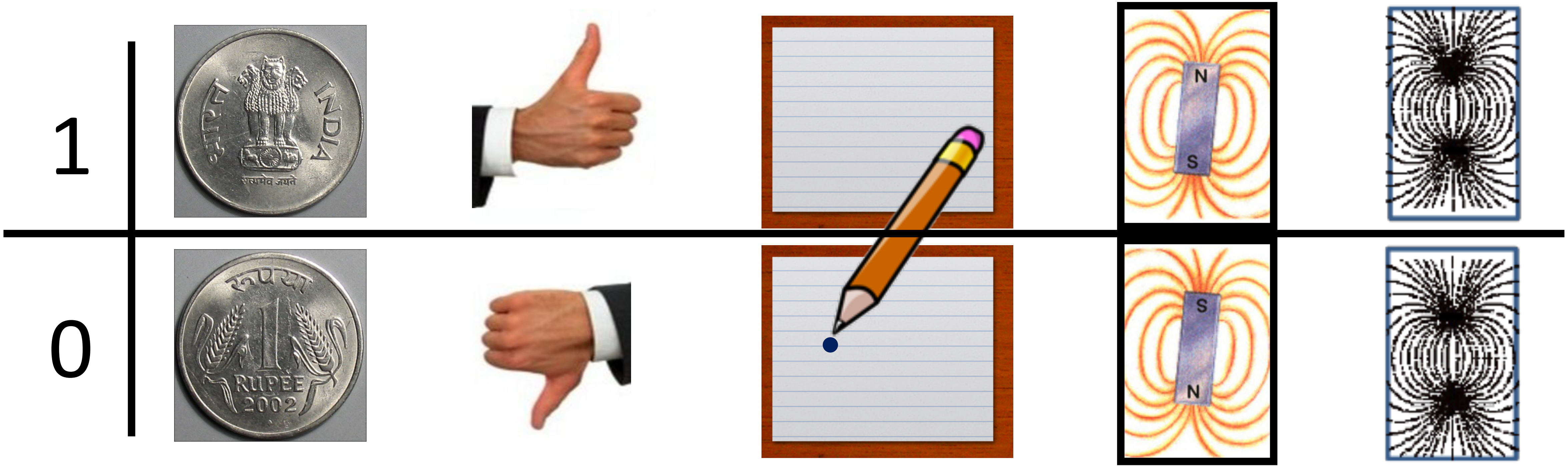
- All digital information stored as bit sequences



Information is Physical

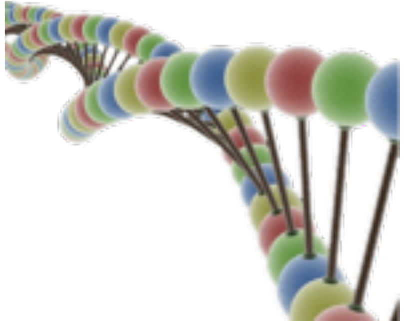
--Rolf Landauer

- Information is inseparable from its physical embodiment



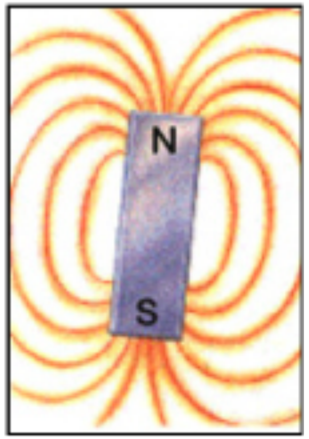
- Biological example: DNA

  2 bits per base pair



Best Bits of Today

Electric



Magnetic

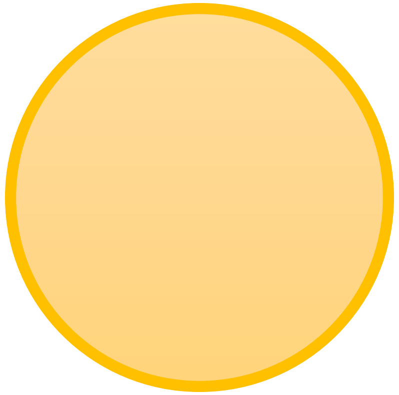
Dynamic Random Access Memory (DRAM)

FLASH Memory

Magnetic hard disk drive

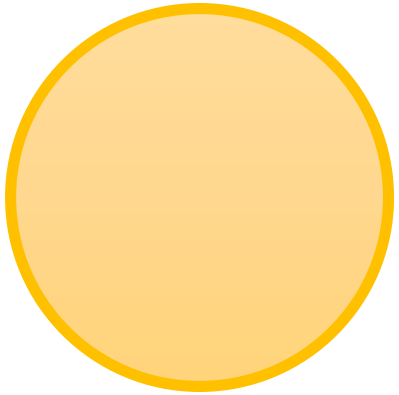
Others: optical (CD/DVD/Bluray), MRAM, Ferroelectric RAM,…

Symmetry Breaking and Information

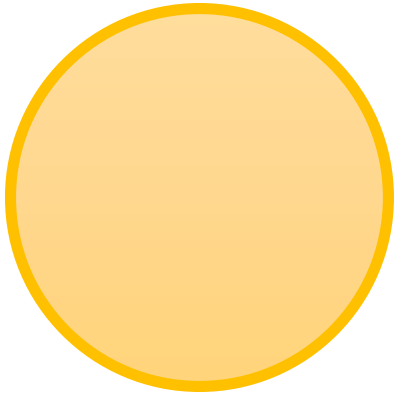


Circle has high symmetry (looks same if rotated)

Symmetry Breaking and Information



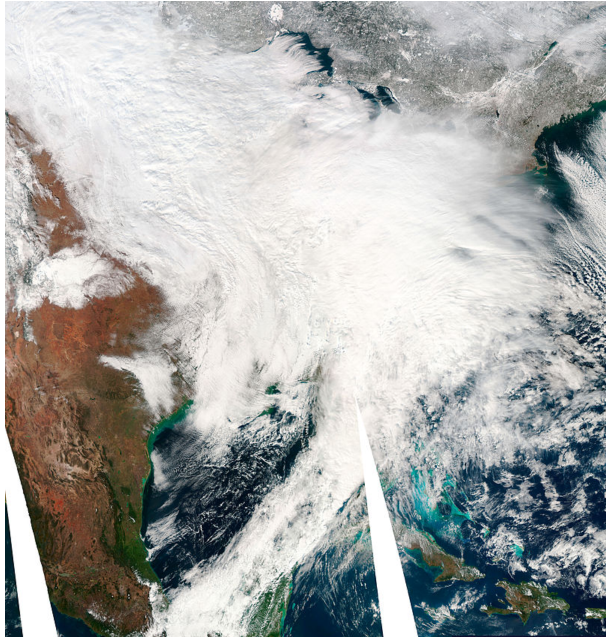
0



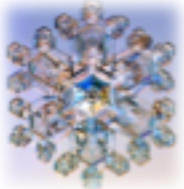
1

Ellipse has reduced symmetry: can store information!

Water Drops and Snow flakes



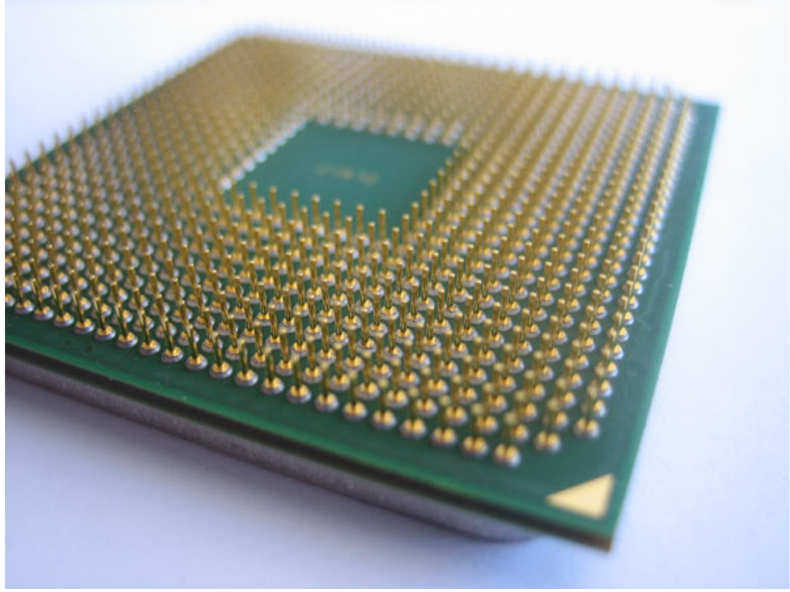
“Snowpocalypse, 2/5/2010”



SnowCrystals.com

Information Processing

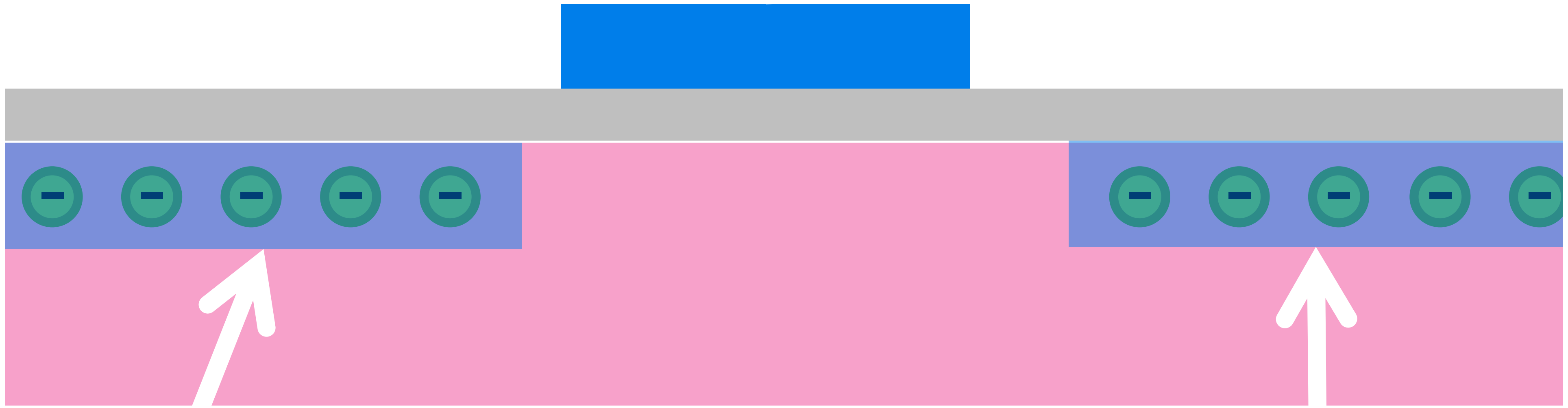
- Need logic to process information



CPU (Central Processing Unit)

Field Effect Transistor

Gate off

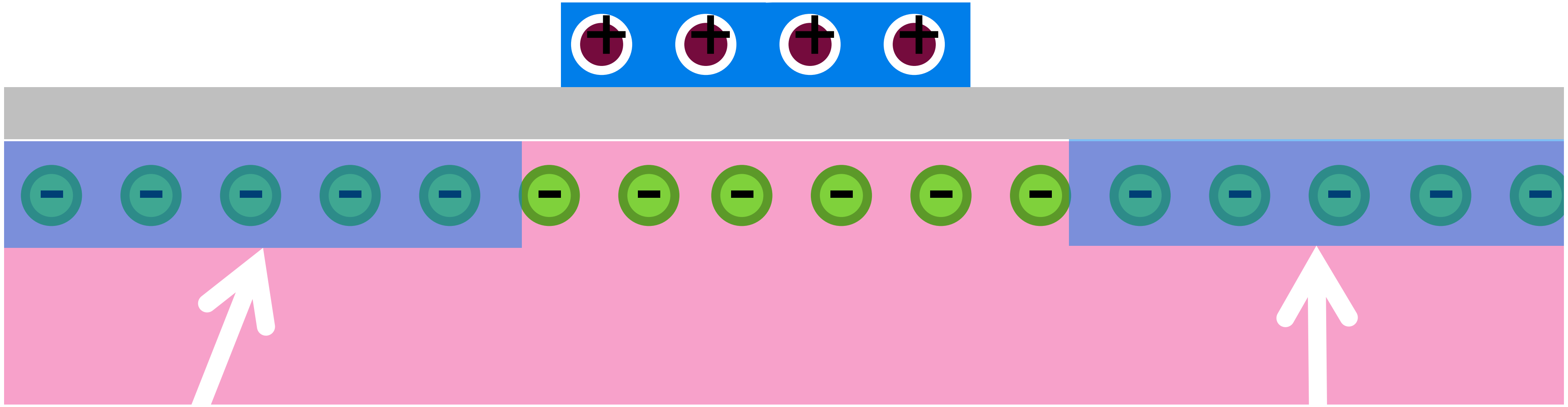


Source

Drain

Field Effect Transistor

Gate on

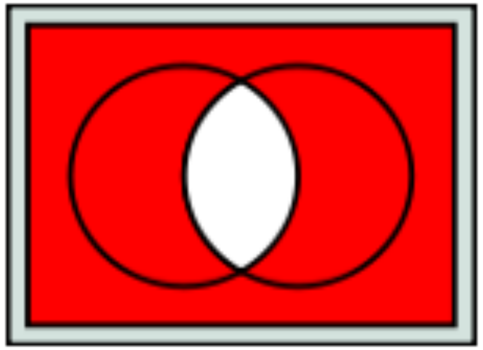


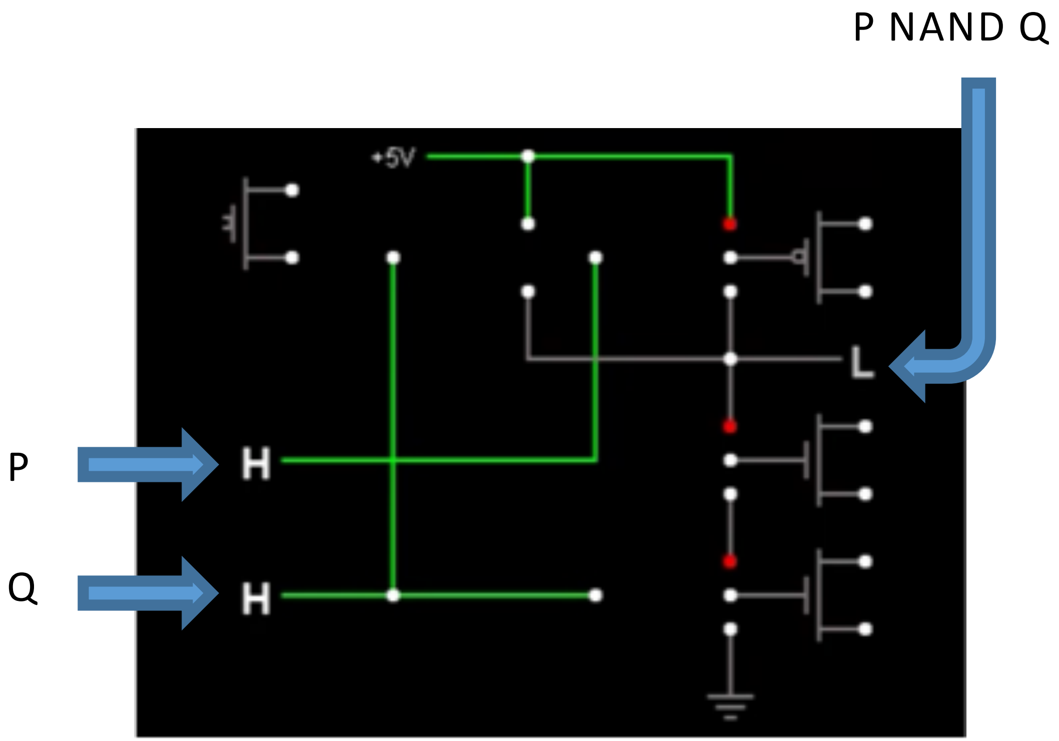
Source

Drain

Universal Logic

P	Q	P NAND Q
H	H	L
H	L	H
L	H	H
L	L	H





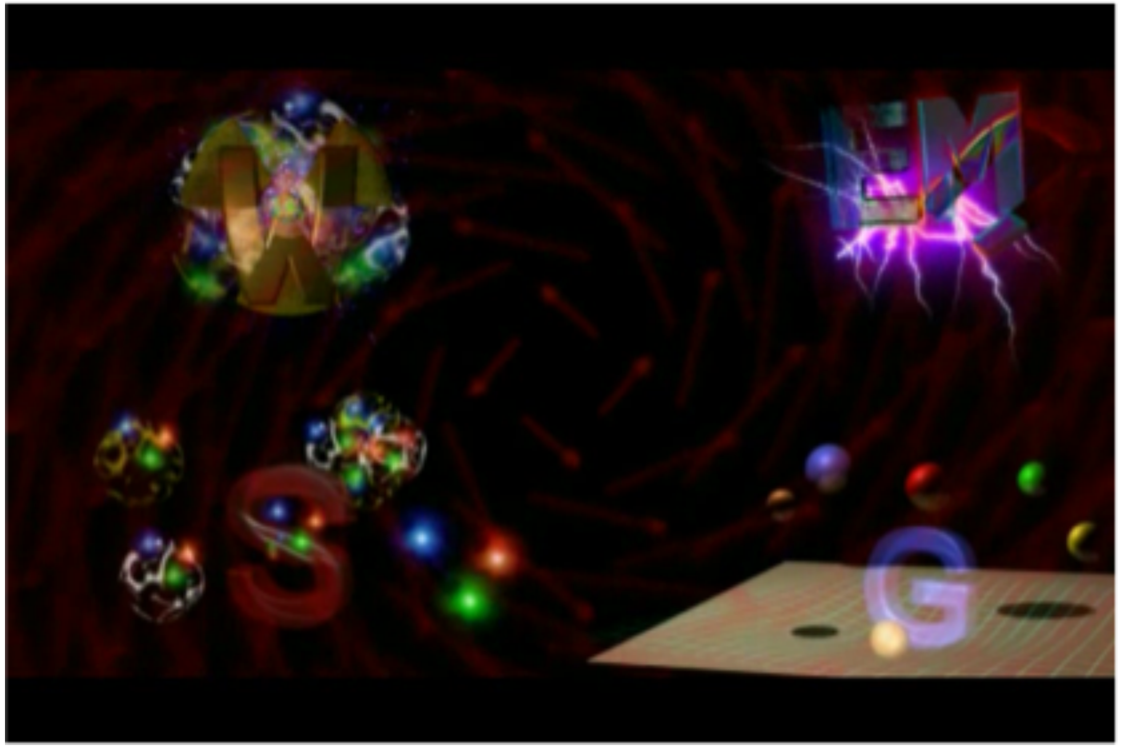
NAND="not and"

All computations can be built from this single type of logic gate

Information in the Universe

- Fundamental forces
  - Arise from **symmetry breaking** of Higgs field
- Symmetry breaking leads to information capacity
- Estimated[*] information capacity of the Universe: 10^{120} logic operations on 10^{90} bits

[*] S. Lloyd, Phys. Rev. Lett. **88**, 237901 (2002).



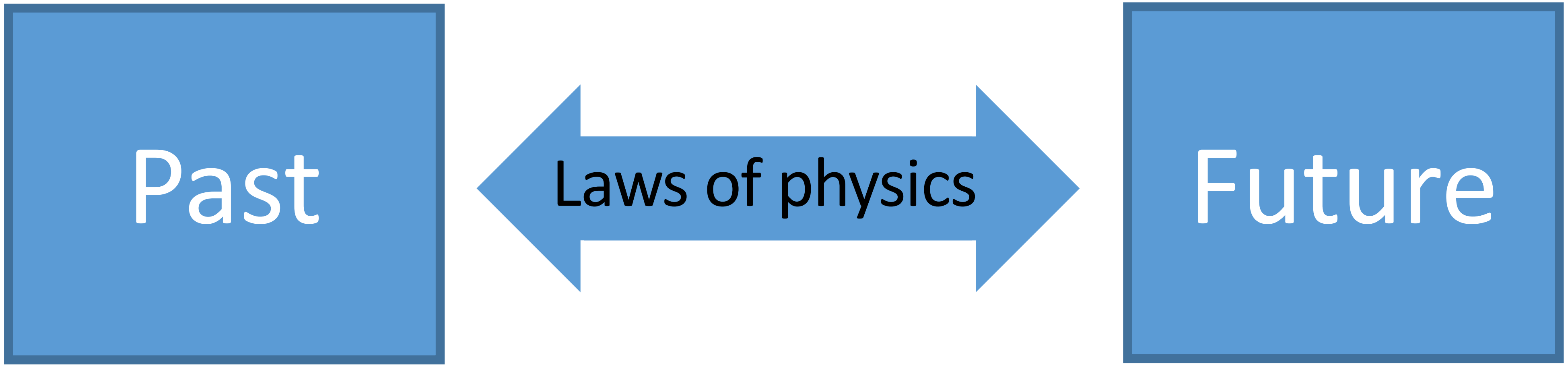
Four fundamental forces in nature:
Weak, ElectroMagnetic, Strong, Gravity

googol = 10^{100} $\neq$ google

“Matrix” Epiphany

Universe as computational engine, computing our future

“Matrix” Analogy



Memory state

Processor

Memory state

But the universe is quantum…

Can we use the laws of quantum mechanics to build a better computer?

Quantum Computation

What is a Quantum Computer?

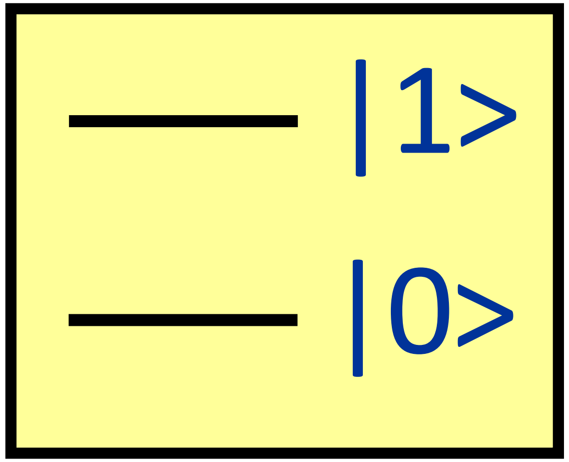
- Computers process information
- Quantum computers process quantum information

What is quantum information?

- Information is stored in bits: 0,1
- Quantum information is stored in quantum bits (qubits)

What is quantum information?

- Information is stored in bits: 0,1
- Quantum information is stored in quantum bits (qubits)



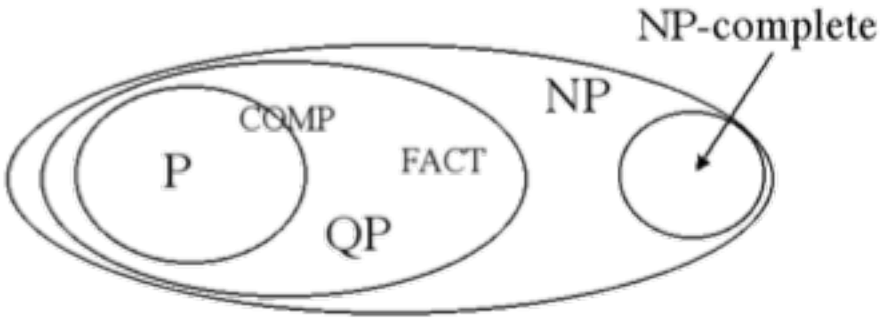
same notation!

http://www.qubit.org/

Qubit can be in a quantum superposition of |0> and |1>

What can quantum computers do?

- Nothing that computers cannot do
  - Some things faster (new complexity class QP)



- Example: quantum computers can factor numbers exponentially faster than classical computers (Shor, 1994)

Difficulty of factoring numbers is
foundation of public key encryption

123018668453011775513049495838496272077
28535695953347921973224521517264005
072636575187452021997864693899564749427
74063845925192557326303453731548268
507917026122142913461670429214311602221
24047927473779408066535141959745985
6902143413

=

334780716989568987860441698482126908177
04794983713768568912431388982883793
878002287614711652531743087737814467999
489

x

367460436667995904282446337996279526322
79158164343087642676032283815739666
511279233373417143396810270092798736308
917

= "RSA-768"

Database Search

Telephone book
with N=1,000,000 entries

Task: find name of person whose number is: (412) 275-0032

Ordinary Phonebook

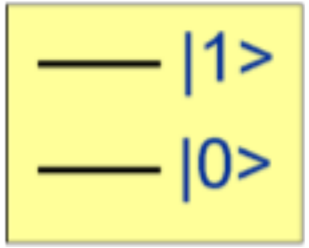
Number found after
~N/2=500,000 attempts

Quantum Phonebook

Number found after
~$N^{1/2}$ =1000 attempts

Why are quantum computers so much faster?

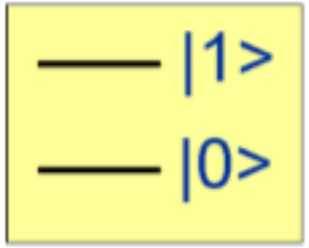
Qubit Phase Space



- A single qubit exists in a 2-dimensional space

$$|\psi\rangle = a_0|0\rangle + a_1|1\rangle, \qquad |a_0|^2 + |a_1|^2 = 1$$

Qubit Phase Space



- A single qubit exists in a 2-dimensional space

$$|\psi>=a_0|0>+a_1|1>, \qquad |a_0|^2+|a_1|^2=1$$

- For *n*-qubit system, 2^n complex numbers required

$$|\psi>=a_0|000\ldots00>+a_1|000\ldots01>+a_2|000\ldots10>+\cdots+a_{2^n-1}|111\ldots11>$$

A state with *n*=300 qubits is specified by 2^{300} ⍰ 10^{100} coefficients !

A quantum program is specified by $(2^{300})^2$ ⍰ 10^{100} coefficients !!

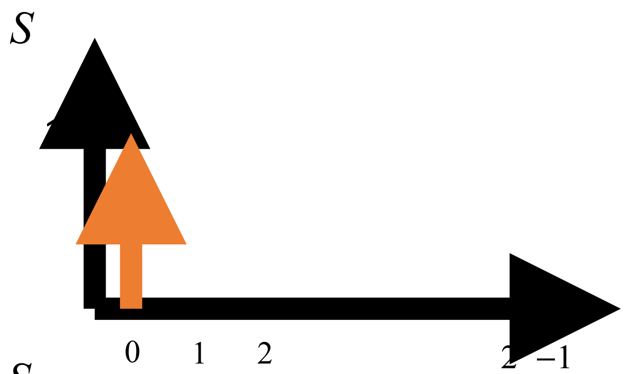
(Final answer is a string of *n=300* classical bits)

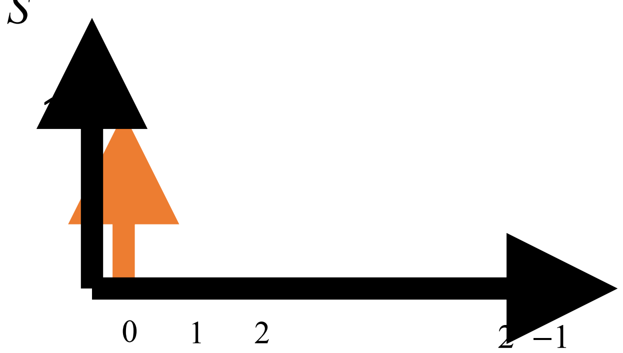
How do quantum computers work?

General Structure of Computer Programs

Step 1: Initialize (boot) computer.

$$S(0)=1$$



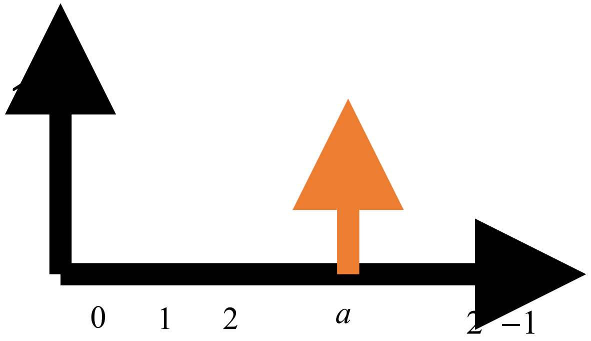


Step 2: Gating

$$S \to F[S]$$

Step 3: Read out answer a

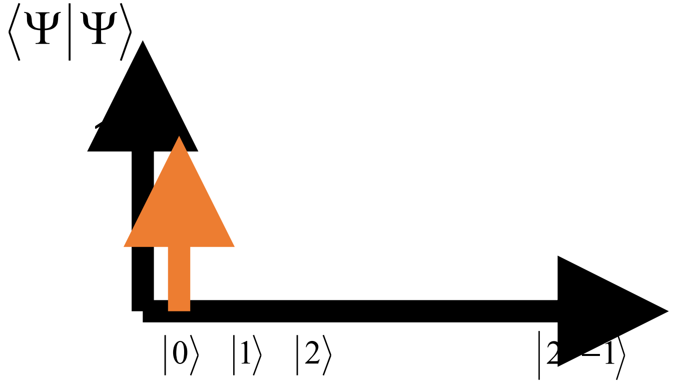
$$F[S](a)=1$$



General Structure of Quantum Computer Programs

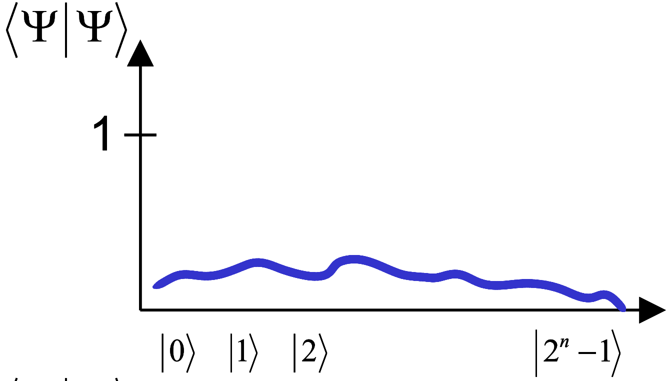
Step 1: Initialize quantum computer.

$$\left|\Psi_0\right\rangle = \left|0\right\rangle$$



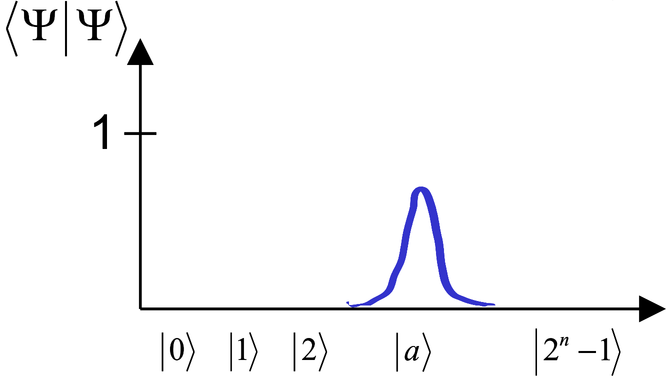
Step 2: Quantum gating

$$i\hbar\frac{\partial\left|\Psi\right\rangle}{\partial t} = \hat{H}(t)\left|\Psi\right\rangle$$



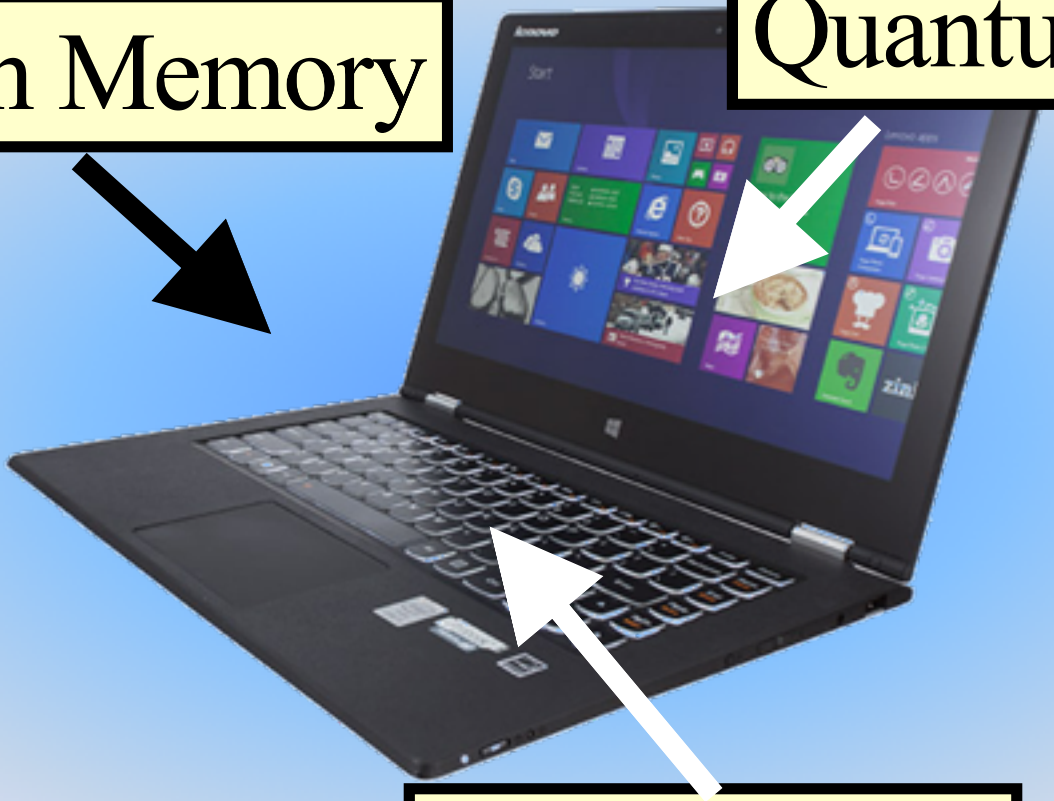
Step 3: Quantum measurement

$$P(a) = \left|\left\langle a|\Psi\right\rangle\right|^2$$



Five Requirements for Quantum Computation

Divincenzo, *Fortschr. Phys.* **48**, 771 (2000)



Quantum Memory

Quantum CPU

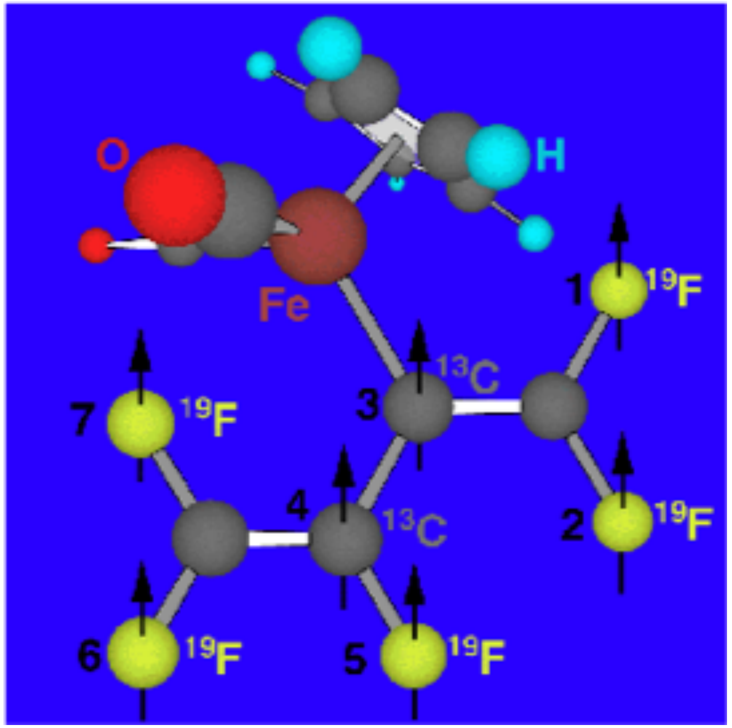
Quantum Coherence

Quantum Coherence

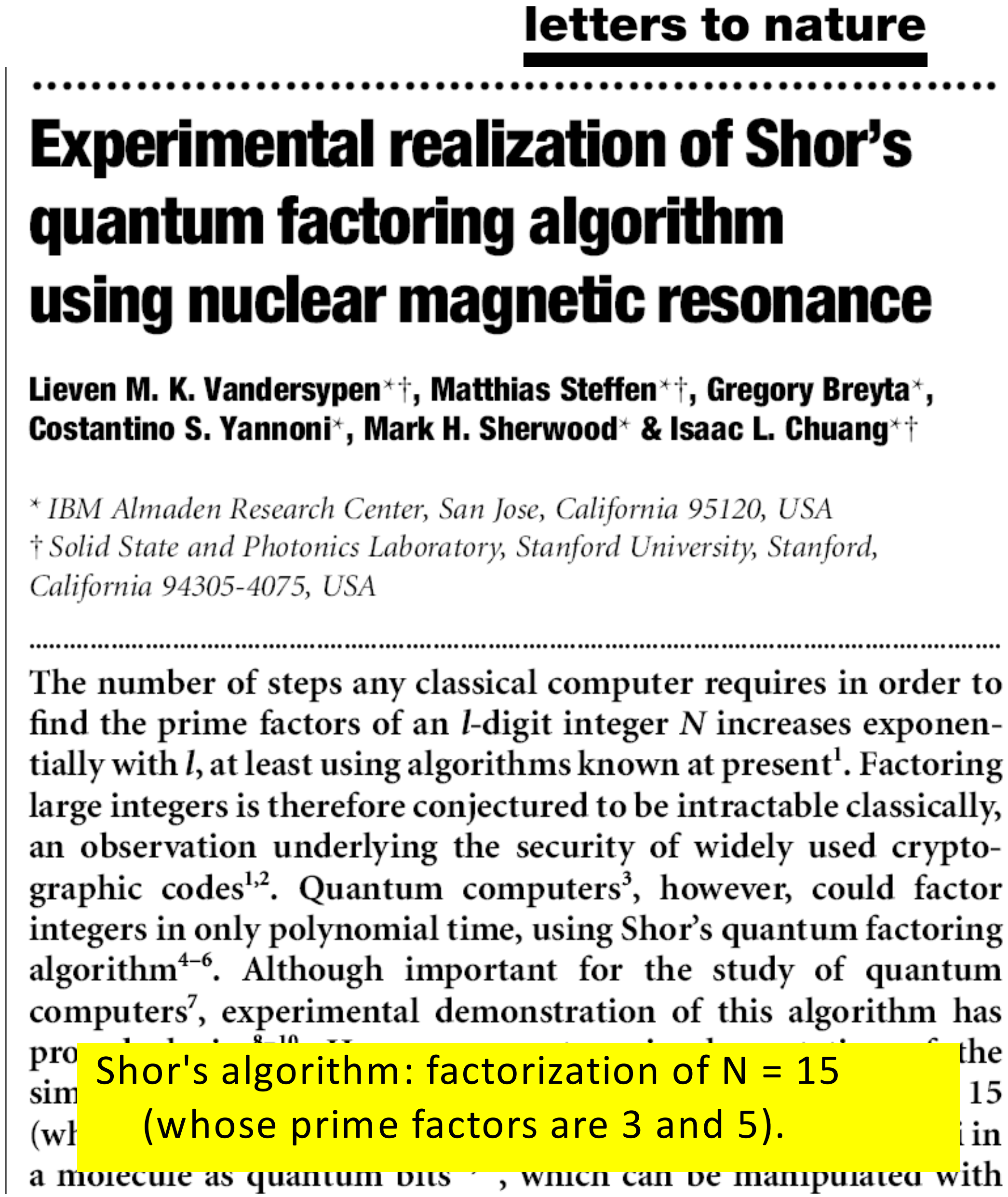
Quantum I/O

NMR Quantum Computing

- Use nuclear spins on molecules for QC
  - Nuclear Magnetic Resonance techniques for manipulating, reading spin
  - Large ensembles of spins



http://www.research.ibm.com/resources/news/20011219_quantum.shtml



letters to nature

Experimental realization of Shor's quantum factoring algorithm using nuclear magnetic resonance

Lieven M. K. Vandersypen*†, Matthias Steffen*†, Gregory Breyta*, Costantino S. Yannoni*, Mark H. Sherwood* & Isaac L. Chuang*†

* *IBM Almaden Research Center, San Jose, California 95120, USA*
† *Solid State and Photonics Laboratory, Stanford University, Stanford, California 94305-4075, USA*

The number of steps any classical computer requires in order to find the prime factors of an l-digit integer N increases exponentially with l, at least using algorithms known at present[1]. Factoring large integers is therefore conjectured to be intractable classically, an observation underlying the security of widely used cryptographic codes[1,2]. Quantum computers[3], however, could factor integers in only polynomial time, using Shor's quantum factoring algorithm[4–6]. Although important for the study of quantum computers[7], experimental demonstration of this algorithm has
pro the
sim 15
(wh in
a molecule as quantum bits, which can be manipulated with

Shor's algorithm: factorization of N = 15
(whose prime factors are 3 and 5).

Quantum Materials and Approaches

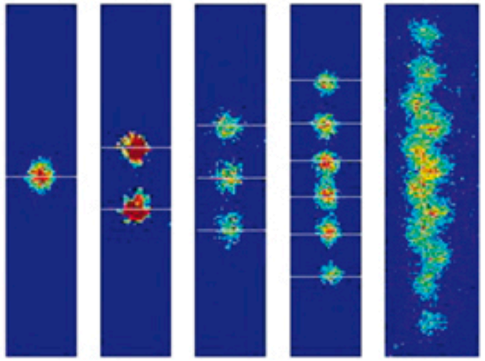
MRS Bulletin

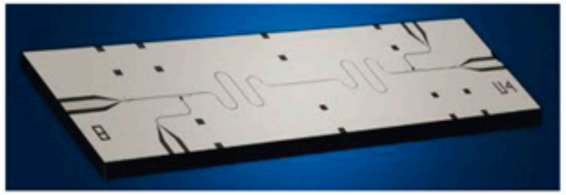
MRS MATERIALS RESEARCH SOCIETY

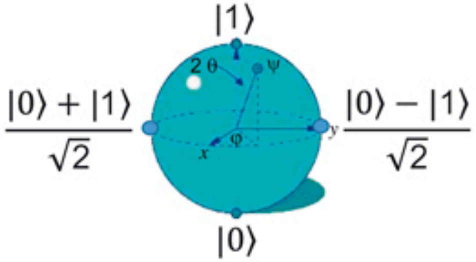
Materials issues for quantum computation

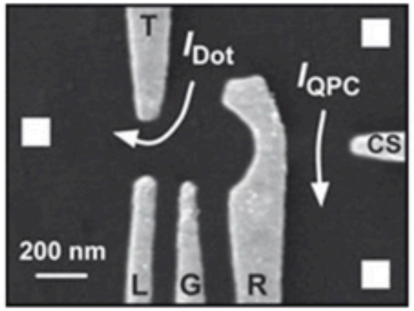
ALSO IN THIS ISSUE

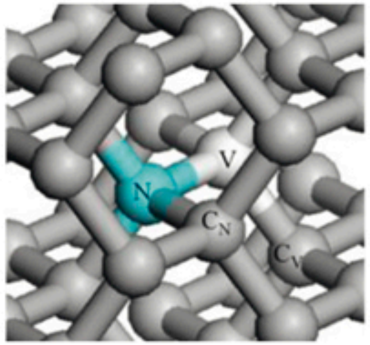
Cell and organ printing turns 15

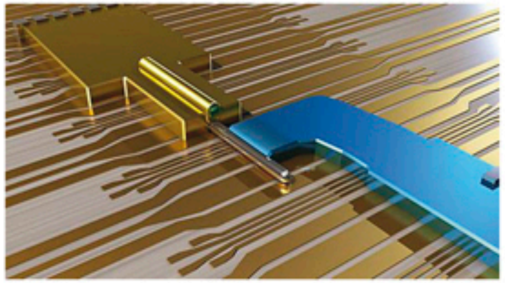




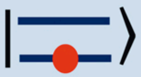
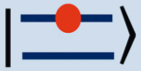
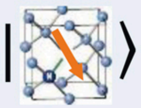
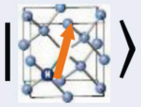
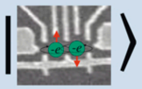
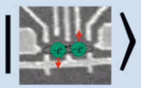
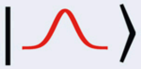
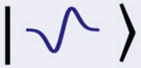

$|1\rangle$
2θ
ψ
$\frac{|0\rangle + |1\rangle}{\sqrt{2}}$
x
φ
y
$\frac{|0\rangle - |1\rangle}{\sqrt{2}}$
$|0\rangle$

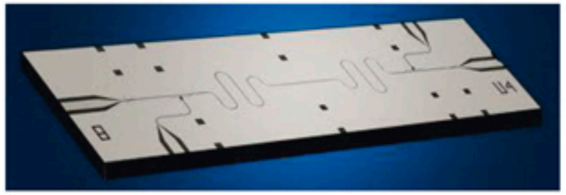


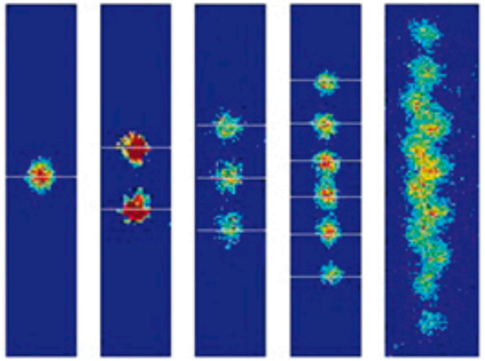


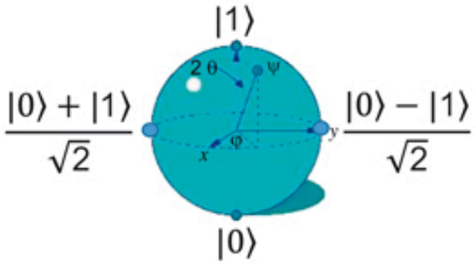


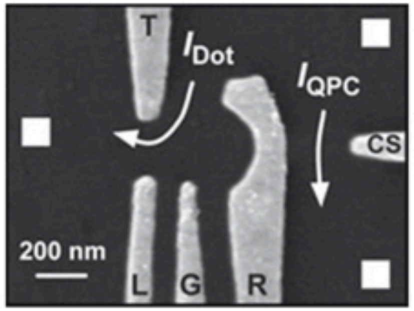
Quantum Materials and Approaches

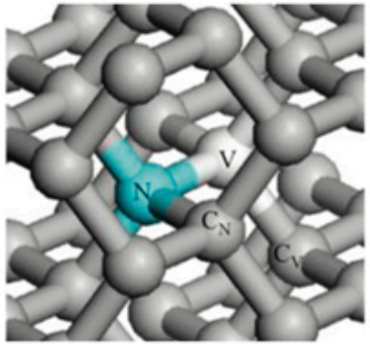
Material System	$\|0\rangle$	$\|1\rangle$
Ion traps		
Defects in solids		
Semiconductor quantum dot		
Superconducting		
Topological nanowire		

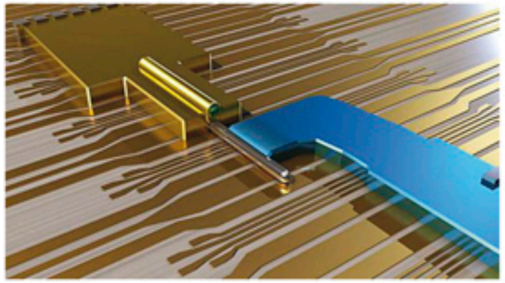


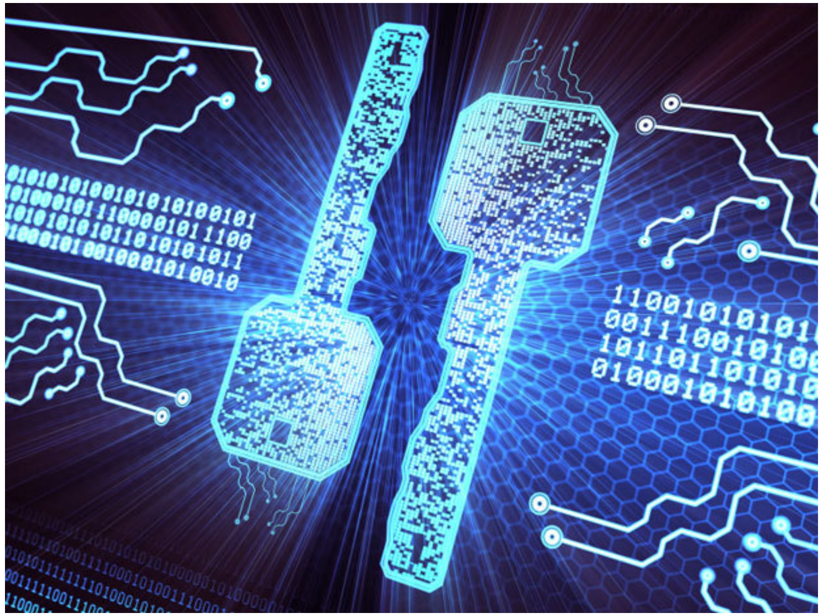



$|1\rangle$
2θ
ψ
$\frac{|0\rangle + |1\rangle}{\sqrt{2}}$
$\frac{|0\rangle - |1\rangle}{\sqrt{2}}$
x
φ
y
$|0\rangle$









https://spectrum.ieee.org/tech-talk/computing/networks/quantum-cryptography-with-conventional-lasers

Quantum Cryptography

Secure communication using the laws of physics

Alice, Bob and Eve

Alice

Eve

Bob

- Alice and Bob want to communicate securely.
- In order to prevent Eve from eavesdropping, they must encode their data.

Encryption and Decryption with a Shared Key

Alice

Eve

Bob

- With a shared encryption key K=0100110101011010 (random string of 0 and 1), secure communication over public channels is possible
  - Bob encodes message M=1010110100101101 by XOR-ing ($\oplus$) with K
    - $M \oplus K = 1110000001110111 = M'$
  - Bob sends message M’ over internet to Alice
  - Alice decodes message
    - $M' \oplus K = 1010110100101101$
- This method works if Alice and Bob have the ability to pre-share K.

Key Distribution

Alice

Eve

Bob

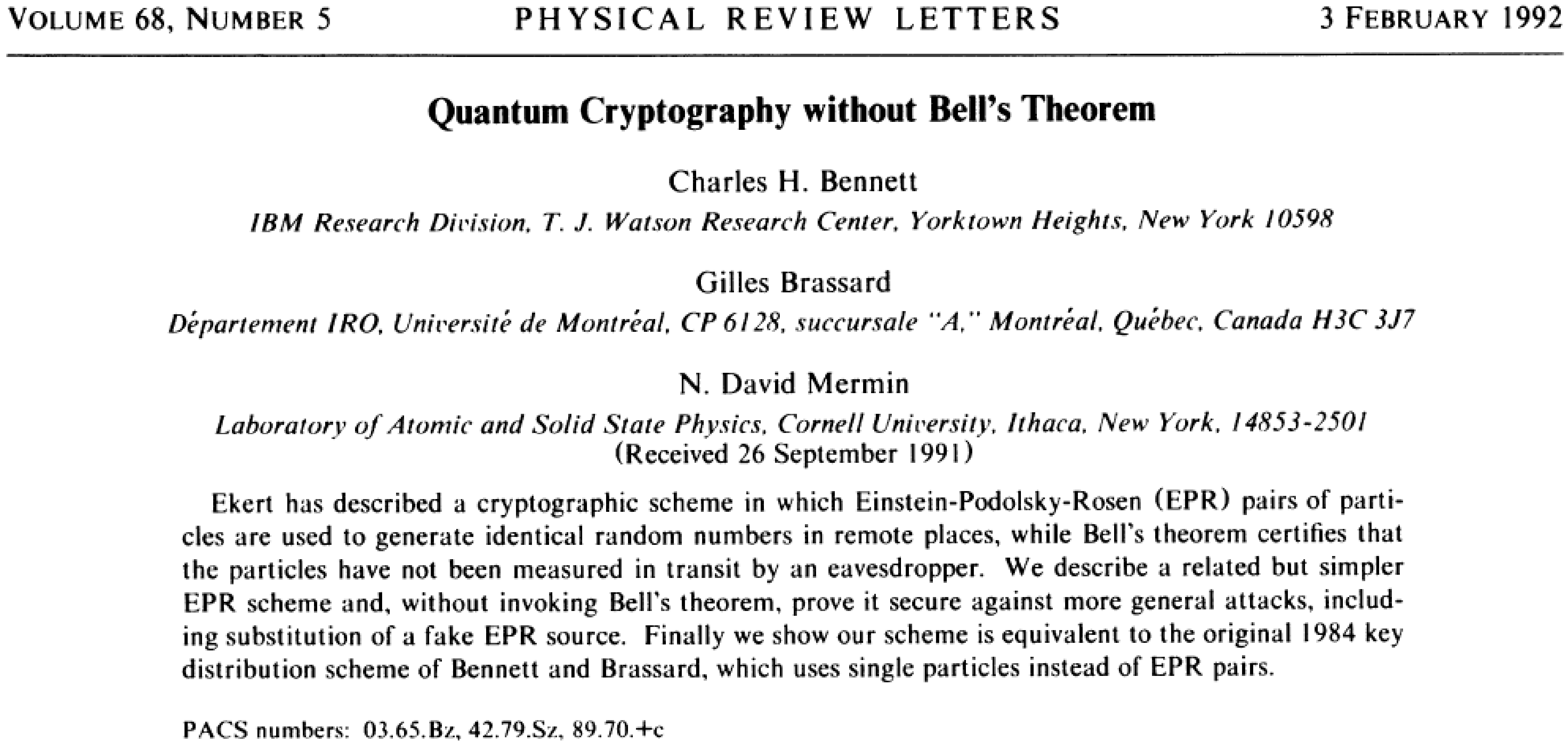
- Quantum mechanics offers a way to distribute a secure key.

How *Not* to Share a Key

$$\left|H\right\rangle,\left|H\right\rangle,\left|V\right\rangle,\left|H\right\rangle,\left|V\right\rangle,\left|V\right\rangle,\ldots$$

- Alice sends a string of orthogonally polarized photons
- Bob, knowing the two possible choices, uses a polarizing beamsplitter and measures the polarization of the transmitted photon
- Problem: Eve can intercept the photon and send a duplicate, without Bob and Alice realizing.

Bennett& Brassard Two-State Protocol



VOLUME 68, NUMBER 5 PHYSICAL REVIEW LETTERS 3 FEBRUARY 1992

Quantum Cryptography without Bell's Theorem

Charles H. Bennett
IBM Research Division, T. J. Watson Research Center, Yorktown Heights, New York 10598

Gilles Brassard
Département IRO, Université de Montréal, CP 6128, succursale "A," Montréal, Québec, Canada H3C 3J7

N. David Mermin
Laboratory of Atomic and Solid State Physics, Cornell University, Ithaca, New York, 14853-2501

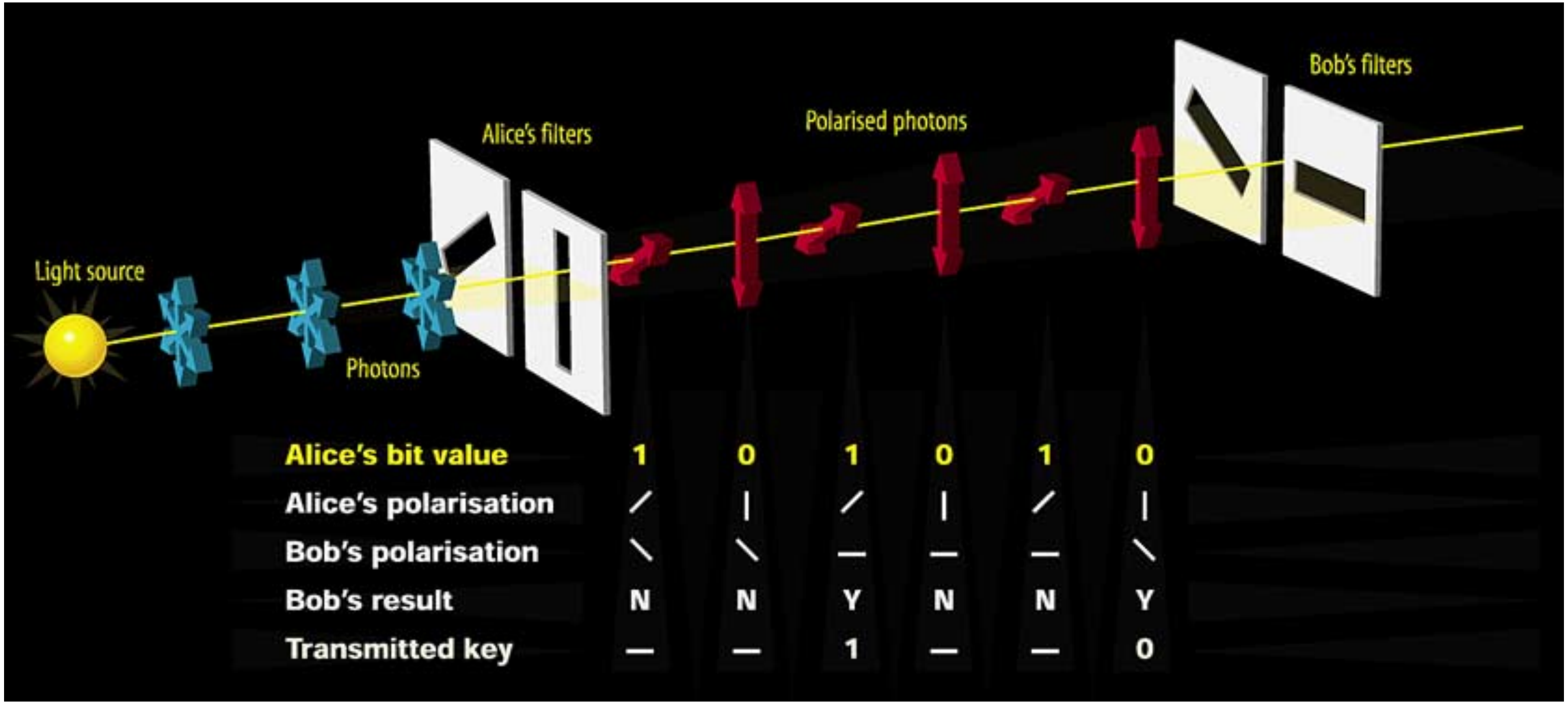
(Received 26 September 1991)

Ekert has described a cryptographic scheme in which Einstein-Podolsky-Rosen (EPR) pairs of particles are used to generate identical random numbers in remote places, while Bell's theorem certifies that the particles have not been measured in transit by an eavesdropper. We describe a related but simpler EPR scheme and, without invoking Bell's theorem, prove it secure against more general attacks, including substitution of a fake EPR source. Finally we show our scheme is equivalent to the original 1984 key distribution scheme of Bennett and Brassard, which uses single particles instead of EPR pairs.

PACS numbers: 03.65.Bz, 42.79.Sz, 89.70.+c

Original version "BB84" described in IEEE conference proceedings

Quantum Key Distribution



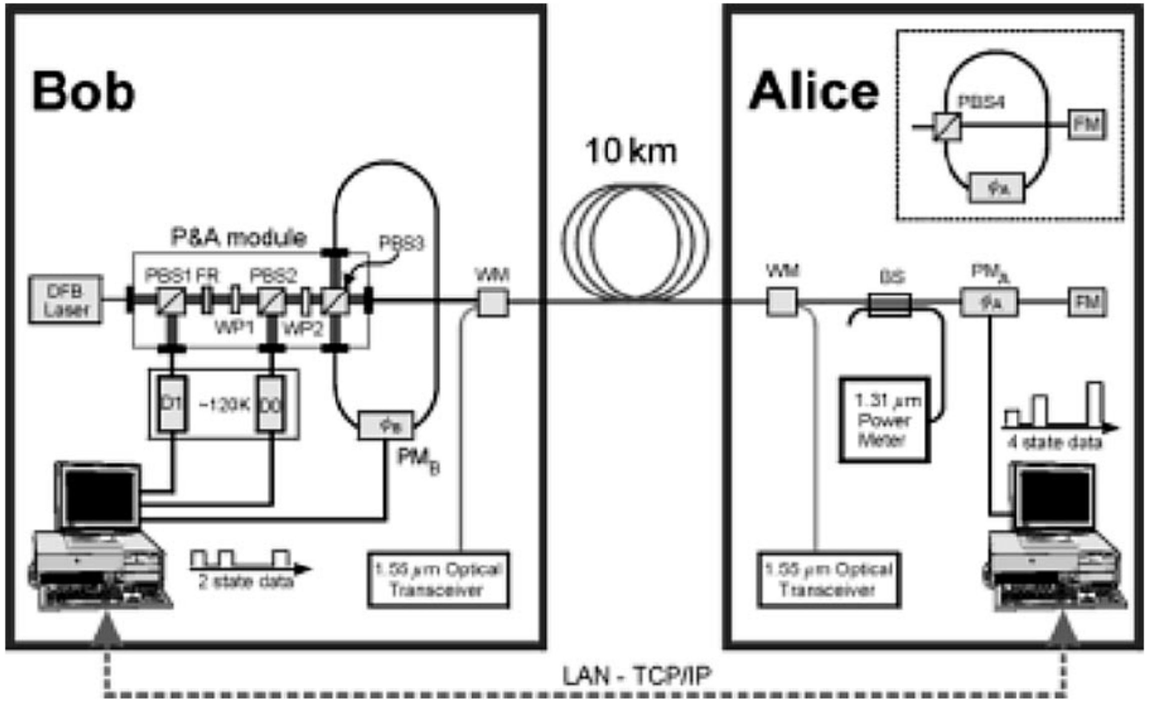
Alice's bit value	1	0	1	0	1	0
Alice's polarisation	/	|	/	|	/	|
Bob's polarisation	\	\	—	—	—	\
Bob's result	N	N	Y	N	N	Y
Transmitted key	—	—	1	—	—	0

What about Eve?

- Because photon polarizations are non-orthogonal, Eve must guess what kind of photon to "replace"
  - Will introduce errors at 25% rate minimum
- After Alice and Bob have their keys, they can compare the parity P of both keys
  - P(011010101)=1 ; P(011010100)=0
  - Discard one bit after each parity check
- If Eve is replacing photons, a detectable error rate between two keys will be measured, foiling Eve

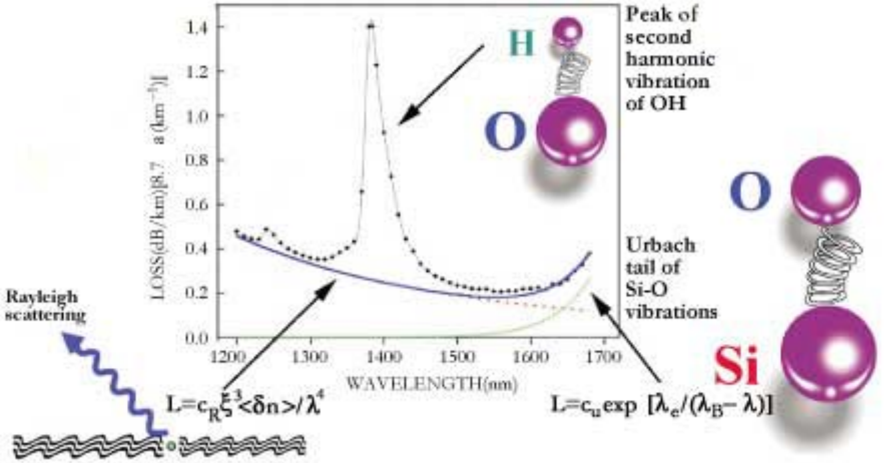
Fiber-Optic Quantum Cryptography

- D. S. Bethune and W. P. Risk, "An autocompensating fiber-optic quantum cryptography system based on polarization splitting of light," IEEE Journal of Quantum Electronics **36** (3), 340-7 (2000).



Limits of Fiber-Based Quantum Communication

- Attenuation of optical fibers limits max distance
  - ~10km for λ=1.55μm
- Need quantum repeaters
  - Accept photon qubits
  - Correct errors without “measuring” state
  - Regenerate photons with high quantum efficiency

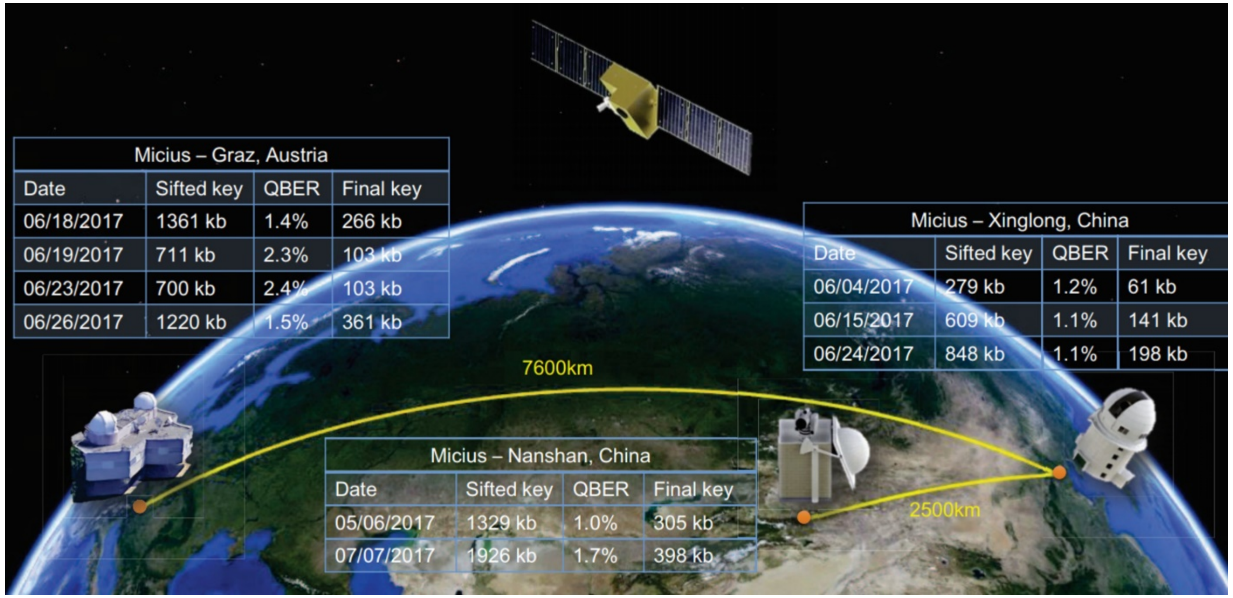


Sept. 2000 issue of Physics Today

https://www.dreamstime.com/stock-photos-global-telecommunications-background-design-image8982023

China's "Quantum" Satellite

- Entangled photon pairs detected 1200 km apart (record)
- Can be used for quantum key distribution



Micius – Graz, Austria

Date	Sifted key	QBER	Final key
06/18/2017	1361 kb	1.4%	266 kb
06/19/2017	711 kb	2.3%	103 kb
06/23/2017	700 kb	2.4%	103 kb
06/26/2017	1220 kb	1.5%	361 kb

Micius – Xinglong, China

Date	Sifted key	QBER	Final key
06/04/2017	279 kb	1.2%	61 kb
06/15/2017	609 kb	1.1%	141 kb
06/24/2017	848 kb	1.1%	198 kb

Micius – Nanshan, China

Date	Sifted key	QBER	Final key
05/06/2017	1329 kb	1.0%	305 kb
07/07/2017	1926 kb	1.7%	398 kb

https://doi.org/10.1103/PhysRevLett.120.030501

Pittsburgh Quantum Institute

UNIFYING AND PROMOTING
QUANTUM SCIENCE AND ENGINEERING
IN PITTSBURGH SINCE 2012

PQI Mission

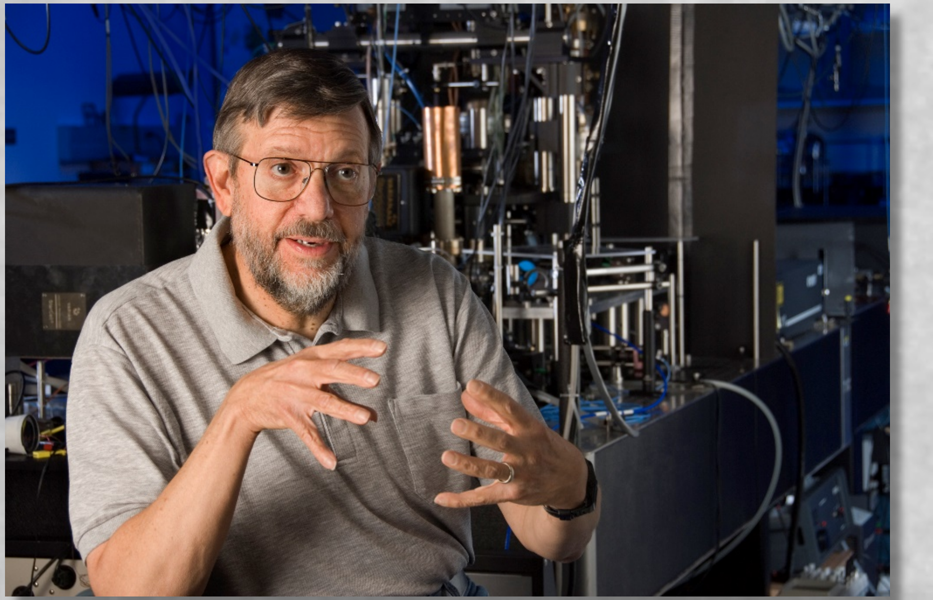
To help unify and promote quantum science and engineering in Pittsburgh

https://www.kitp.ucsb.edu/activities/qinfo-c17

The Quantum Frontier

A vision for quantum science and engineering in the 21st century

<PIQI|> PITTSBURGH QUANTUM INSTITUTE



Inaugural PQI Public Lecture

"Quantum Information: a scientific and technological revolution for the 21st century”

Bill Phillips, Nobel Laureate, 1997

*“**Two of the great scientific and technical revolutions of the 20th century** were the **discovery of the quantum nature of the submicroscopic world**, and the **advent of information science and engineering**. Both of these have had a profound effect not only on our daily lives but on our worldview. Now, at the beginning of the **21st century**, we see a **marriage of quantum mechanics and information science in a new revolution: quantum information**. Quantum computation and quantum communication are two aspects of this revolution. The first is highly speculative: a new paradigm more different from today’s digital computers than those computers are from the ancient abacus. The second is already a reality, providing information transmission whose security is guaranteed by the laws of physics.”*

<P|Q|I> PITTSBURGH QUANTUM INSTITUTE

Two Quantum Revolutions

First Quantum Revolution (20th century): *understanding of quantum phenomena that brought about semiconductor devices, microprocessors, lasers, nuclear energy, …*

Second Quantum Revolution (21st century): *manipulation of quantum phenomena; actively creating, manipulating and probing quantum states of matter, often using superposition and entanglement for sensing, simulation, computing, information*

Information, Quantum Mechanics and the Universe

Jeremy Levy
Pittsburgh Quantum Institute (pqi.org)
University of Pittsburgh (levylab.org)

<P|Q|I>

SAC-PA2: Towards Security Assured Cyberinfrastructure in Pennsylvania

University of Pittsburgh School of Computing and Information

15 June 2018