Quantum Information Science, NIST, and Future Technological Implications

Carl J. Williams, Chief
Atomic Physics Division
National Institute of Standards & Technology

http://qubit.nist.gov

What is Quantum Information?

"Quantum information is a radical departure in information technology, more fundamentally different from current technology than the digital computer is from the abacus."

W. D. Phillips, 1997 Nobel Prize Winner in Physics

A convergence of two of the 20th Century's great revolutions

A new science!

Quantum Mechanics
(i.e. atoms, photons, JJ's, physics of computation)

Information Science
(*i.e.* computer science, communications, cryptology)

The second quantum revolution

Second Quantum Revolution

We are witnessing the second quantum revolution

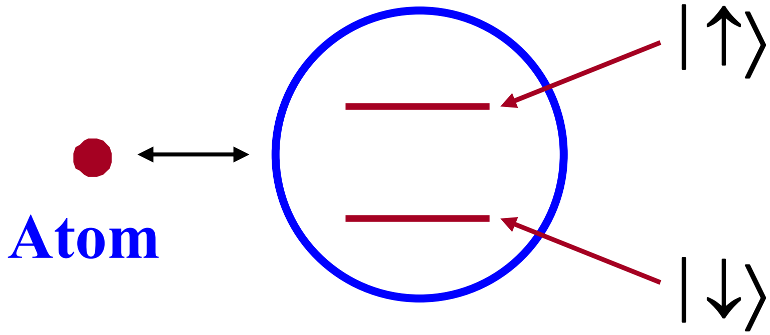
- **First quantum revolution (1920's - 1980's)**
  - **Described how nature works at the quantum level**
  - **Weirdness of QM discovered and debated**
    - Wave-particle duality -> Wavefunctions
    - Spooky action at a distance -> Entanglement
  - **Technology uses semiclassical properties – quantization & wave properties**
- **Second quantum revolution (starts ~1980's -)**
  - **Exploits how nature works at the quantum level**
    - Interactions are how Nature computes!
  - **Weirdness of QM exploited**
    - Information storage capacity of superposed wavefunctions
    - Information transmittal accomplished by entanglement, teleportation
    - Information exchange accomplished by interactions
  - **Technology uses the weird properties of quantum mechanics**

Classical Bits vs. Quantum Bits

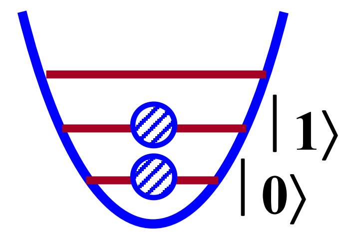
- **Classical Bits: two-state systems**

  Classical bits: 0 (off) or 1 (on) (switch)

- **Quantum Bits *are also two-level(state) systems***



Internal State



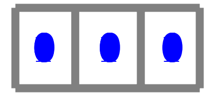
Motional State

⇨ **But: Quantum Superpositions are possible**

$$\Psi = \alpha|\downarrow\rangle + \beta|\uparrow\rangle$$
$$= \alpha|0\rangle + \beta|1\rangle$$

Scaling of Quantum Information

- **Classically,** **information stored in a bit register: a 3-bit register stores one number, from 0 – 7.**



- **Quantum mechanically,** **a 3-qubit register can store all of these numbers in a *superposition*:**

$$|000\rangle + |001\rangle + |010\rangle + |011\rangle + |100\rangle + |101\rangle + |110\rangle + |111\rangle$$

- **Result:**
  - **Classical:** **one 3-bit number**
    one N-bit number
  - **Quantum:** **2^3 (all possible) 3-bit numbers**
    2^N (all possible) N-bit numbers

Scaling of Quantum Information (2)

- Consequence of Quantum Scaling
  - Calculate all values of f(x) at once and in parallel
  - Quantum Computer will provide "Massive" Parallelism
- But wait …
  - When I "*readout the result*" I obtain only one value of f(x)
  - For the previous 3-qubit example each value of f(x) appears with probability 1/8
- Thus must measure some global property of f(x)
  - *e.g.* periodicity

Note!

300-qubit register can store more combinations than there are particles in the whole universe

A computer based on this processor would be awesome

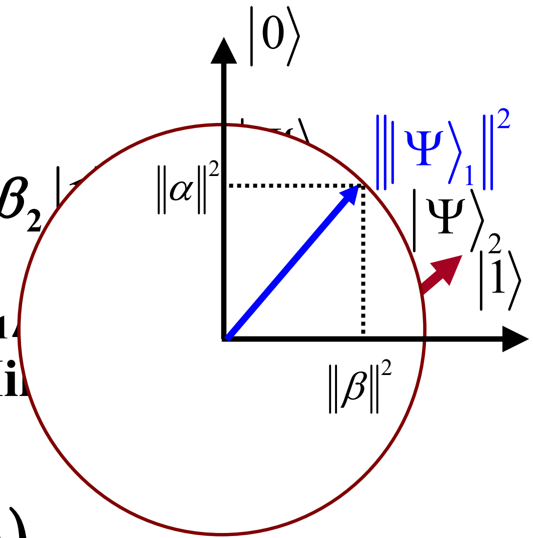
Quantum Entanglement

- **Single Qubit:** $|\Psi\rangle_1 = \left(\alpha|0\rangle_1 + \beta|1\rangle_1\right)$
- **2-Qubit State:**

$$|\Psi\rangle_1 \otimes |\Psi\rangle_2 = \left(\alpha_1|0\rangle_1 + \beta_1|1\rangle_1\right)\otimes\left(\alpha_2|0\rangle_2 + \beta_2 \ldots\right.$$

$$= \alpha_1\alpha_2|00\rangle + \alpha_1\beta_2|01\rangle + \beta_1\alpha_2|10\rangle + \beta_1 \ldots$$

⇨ **product states span a 2-dimensional Hi…**



- **2-Qubit Entangled State:**

$$|\Psi\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle_1|0\rangle_2 + |1\rangle_1|1\rangle_2\right) = \frac{1}{\sqrt{2}}\left(|00\rangle + |11\rangle\right)$$

⇨ **<u>not</u> a product state; can span a 4-dimensional Hilbert space**

⇨ **Entanglement creates a "shared fate" ** Schrodinger's Cat ****

Entanglement is a unique *<u>quantum</u>* resource:

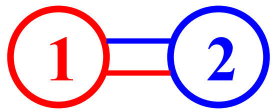
" … fundamental resource of nature, of comparable importance to energy, information, entropy, or any other fundamental resource."

Nielsen & Chuang, <u>Quantum Computation and Quantum Information</u>

Einstein-Podolsky-Rosen Paradox

$$|\uparrow\rangle_1 |\uparrow\rangle_2 + |\downarrow\rangle_1 |\downarrow\rangle_2$$

(1) Prepare 2-qubits in an entangled state



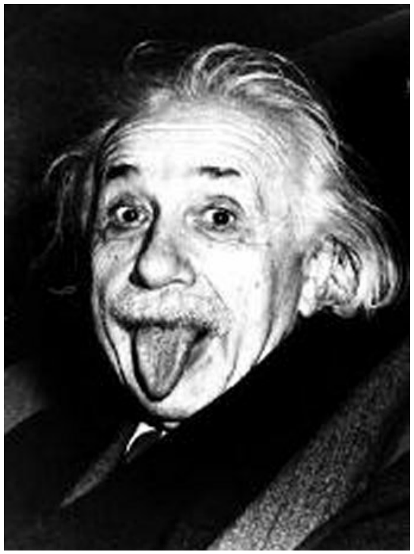
(2) Send qubit 1 with Alice to Paris and qubit 2 with Bob to Tokyo

Entanglement is a unique *quantum* resource:

"… fundamental resource of nature, of comparable importance to energy, information, entropy, or any other fundamental resource."

Nielsen & Chuang, Quantum Computation and Quantum Information

Einstein was not always right…



MAY 15, 1935 PHYSICAL REVIEW VOLUME 47

Can Quantum-Mechanical Description of Physical Reality Be Considered Complete?

A. EINSTEIN, B. PODOLSKY AND N. ROSEN, *Institute for Advanced Study, Princeton, New Jersey*

(Received March 25, 1935)

In a complete theory there is an element corresponding to each element of reality. A sufficient condition for the reality of a physical quantity is the possibility of predicting it with certainty, without disturbing the system. In quantum mechanics in the case of two physical quantities described by non-commuting operators, the knowledge of one precludes the knowledge of the other. Then either (1) the description of reality given by the wave function in quantum mechanics is not complete or (2) these two quantities cannot have simultaneous reality. Consideration of the problem of making predictions concerning a system on the basis of measurements made on another system that had previously interacted with it leads to the result that if (1) is false then (2) is also false. One is thus led to conclude that the description of reality as given by a wave function is not complete.

W. Pauli – "Einstein has once again expressed himself publicly on quantum mechanics, indeed in the 15 May issue of *Physical Review*. As is well known, every time this happens it is a catastrophe."

NIST Quantum Information Efforts

http://qubit.nist.gov

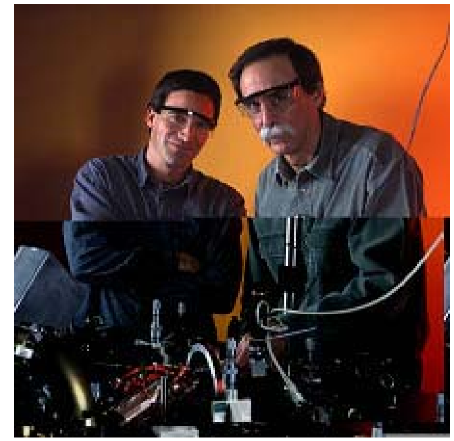
- **Quantum Computing**
  - **Ion Traps: David Wineland (PL, Boulder)**
  - **Neutral Atoms: William Phillips (PL, Gaithersburg)**
  - **Josephson Junctions: Ray Simmonds (EEEL, Boulder)**
  - **Device Physics & Architectures: Carl Williams (PL, Gaithersburg)**
  - **Quantum Information Theory & Error Corr.: Manny Knill (ITL, Boulder)**
- **Quantum Communication**
  - **1.25 GHz Test-Bed: Joshua Bienfang (PL), Xiao Tang (ITL) (Gaithersburg)**
  - **Single Photon Metrology: Alan Migdall (PL, Gaithersburg)**
  - **Single Photon Sources**
    - Parametric Down Converters: **Alan Migdall (PL, Gaithersburg)**
    - Quantum-Dot Photonics: **Richard Mirin (EEEL, Boulder)**
  - **Single Photon Detectors:**
    - Transition Edge Sensor (88% QE at 1550 nm): **Sae Woo Nam (EEEL, Boulder)**
    - High-speed superconducting detector at 1550 possible: **Sae Woo Nam**
    - Quantum Dot Gated Field Effect Transistor: **Richard Mirin (EEEL, Boulder)**
  - **Q. Communication Protocols: A. Nakassis, R. Kuhn (ITL, Gaithersburg)**

Recent NIST Highlights

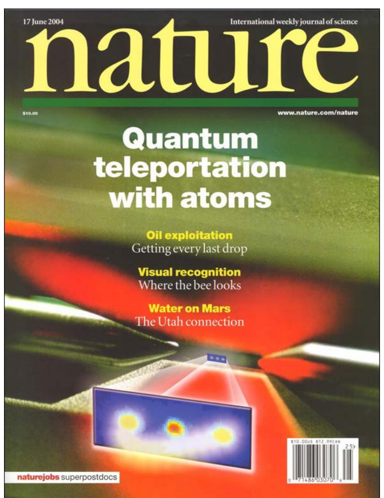
- Operations of a high-speed quantum key distribution (QKD) producing > 1 Mbit of key per second – free space & fiber
- Demonstration of a photon number resolving detector at telecom wavelengths with 88% quantum efficiency
- Demonstration of a single photon source with certification
- First teleportation of state of a material qubit (ion)
- Realization of quantum error correction in a potentially scalable system
- Demonstration of quantum dense coding with ions
- Demonstration of an engineered quantum state useful for improved atomic clock
- Massive register initialization with neutral atoms
- Full spectroscopy of Josephson Junction shows potential material limitations – key to future improvements
- Improved quantum error thresholds and quantum error correcting codes
- Novel approaches to quantum architectures
- Quantum Logic Clock

Most Advanced Quantum Computing Effort

David Wineland’s ion trap quantum computing effort is the most advanced in the world:

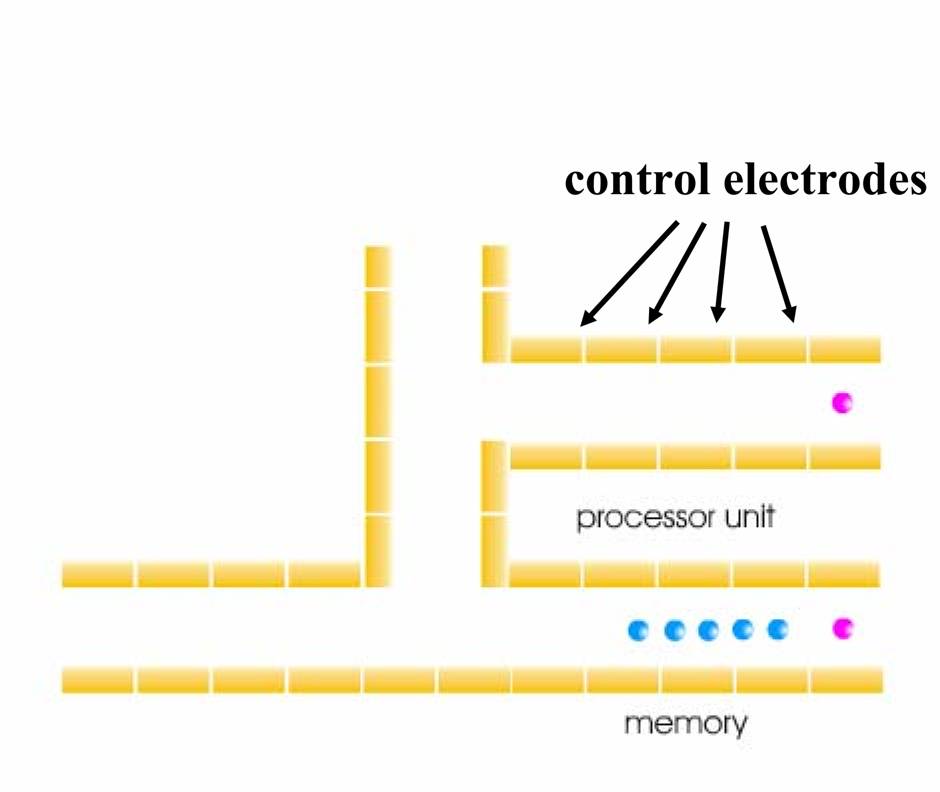


- **Passes all of the DiVincenzo Criteria for Scalability**
  - a) Well characterized, scalable qubits
  - b) Ability (re)initiate to a starting state
  - c) Decoherence times longer than operation time
  - d) A universal set of one- and two-qubit gates
  - e) State specific readout
  - f) Efforts toward photon-ion coupling showing promise



- **Teleportation of quantum state of an ion**
- **Separation & movement of entangled ions**
- **Quantum error correction demonstrated**
- **Quantum dense coding**
- **Quantum Fourier transform ran**
- **Demonstration of quantum logic clock**
- **8-qubits entangled, 6-qubit GHZ state**

Multiplexed Ion Trap Architecture



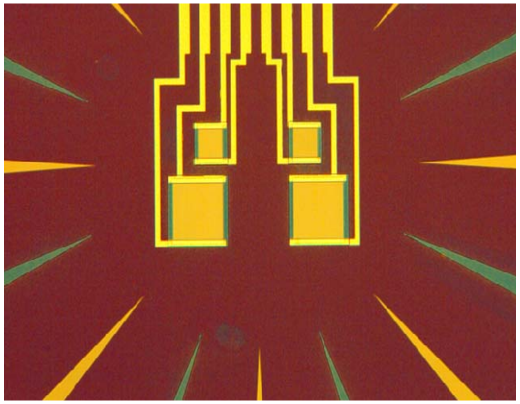
- Interconnected multi-trap structure
- Route ions by controlling electrode potentials
- Processor sympathetically cooled
- No individual optical addressing during two-qubit gates (can do gates in strong trap ⇒ fast)
- One-qubit gates in subtrap
- Readout in subtrap

- Wineland *et al.*, *J. Res. NIST*. 103, 259 (1998).
- Kielpinski, Monroe, Wineland, *Nature* 417, 709 (2002).

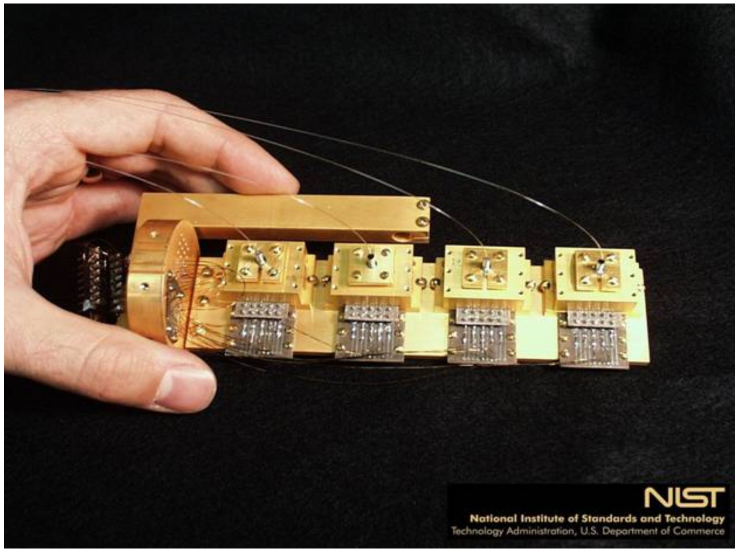
Other proposals: DeVoe, *Phys. Rev. A* 58, 910 (1998). Cirac and Zoller, *Nature* 404, 579 (2000) .

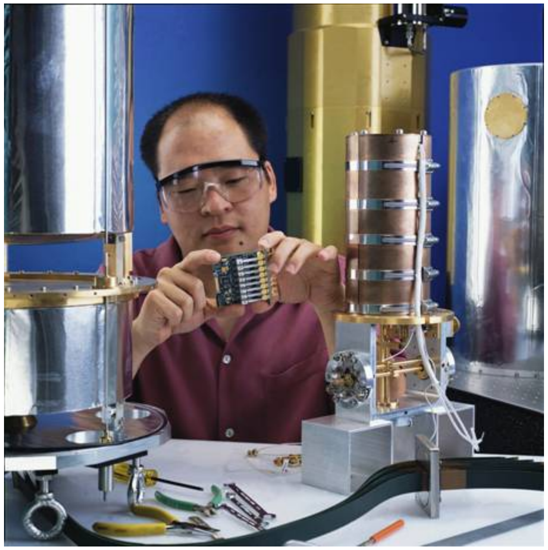
Superconducting Photon Detectors

- Demonstrated Transition Edge Sensor with QE of 88%
- Developing improved materials for detectors
- Explore high-speed single photon superconducting detectors



TES Detector





[Sae Woo Nam]

Used to set new QKD distance record of 200 km!

Quantum Information may be Inevitable

The limits of miniturization:

At atomic scale sizes quantum mechanics rules

– **Since objects and electronic components continue to be miniaturized, inevitably we will reach feature sizes that are *atomic* in scale**
– **In general, attempts to make *atomic-size* circuits behave classically will fail due to their inability to dissipate heat and their quantum character**

Thus quantum information may be inevitable!

- **Clearly, at the smallest scale, we need to take full advantage of quantum properties.**
- **This *emphasizes a different* view of the usefulness of quantum information why it *may ultimately lead* to quantum engineering.**

- **A quantum computer if it existed could break all present-day public key encryption systems**
- **Quantum encryption can defeat any computational attack**

Quantum Information's Impact

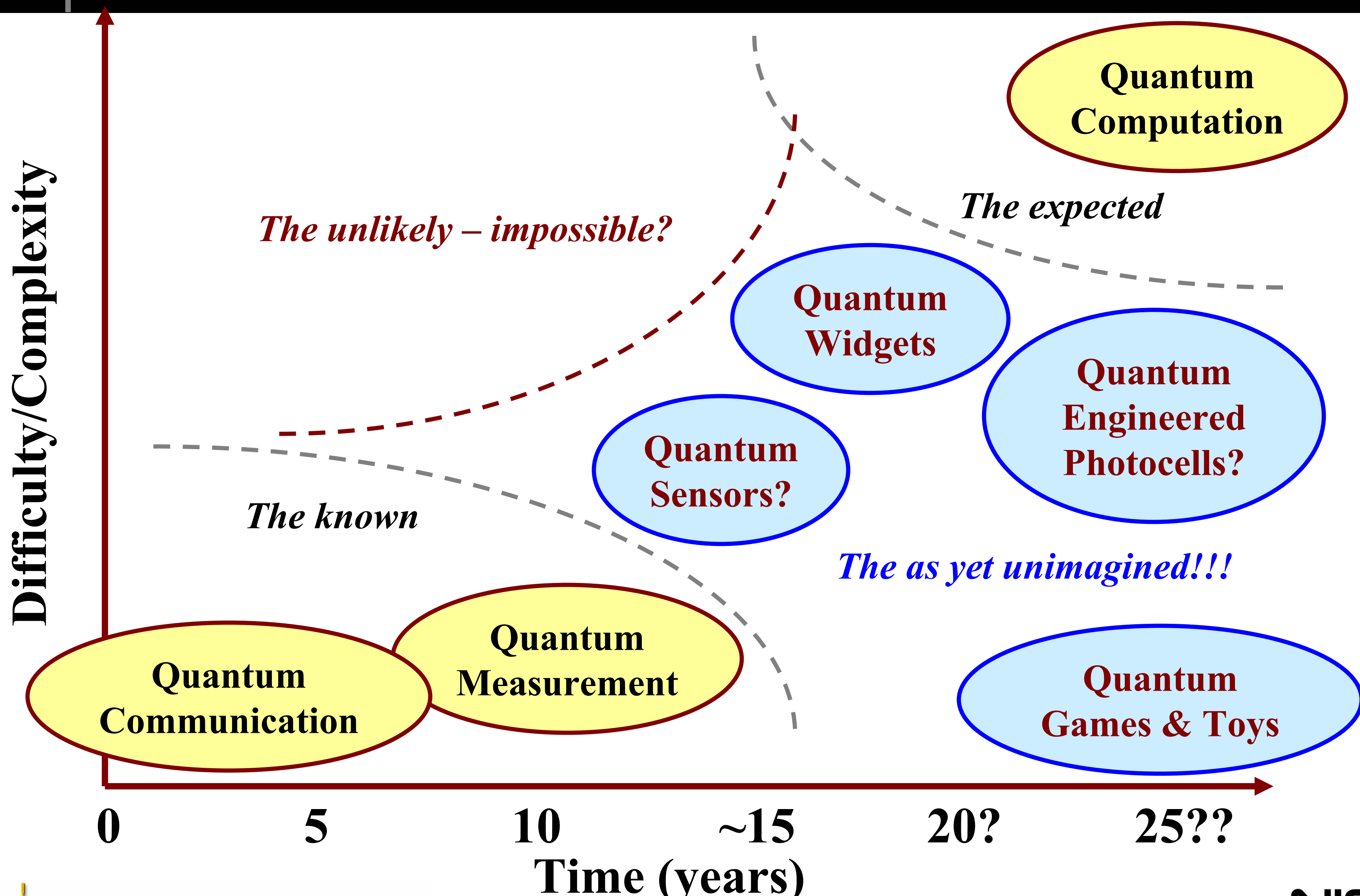
- **Revolutionary**
  - Builds the physical foundation for information theory
  - Teaches us to examine the information content in real systems
  - Help us to develop a language to move quantum mechanics from a scientific to an engineering field
  - Quantum Limited Measurement will become available
- **20th Century we used the particle/wave aspects of Quantum Mechanics:** Televisions, CRT's, NMR …
- **21st Century we will use the coherence of quantum mechanics to build new types of devices:**

Let me speculate: Quantum engineering will come and will allow us to extend the Moore's Law paradigm based not on making things smaller but making them more powerful by using the laws of quantum mechanics.

Possible Applications of Q. Computers

- **Solution of basics physics problems including:**
  - Lattice Quantum Electro/Chromo-Dynamics (QED/QCD)
  - Simulations of Condensed Matter Hamiltonians – High T_c Superconductivity
- **Optimization of commercially important problems:**
  - Electronic Circuit layout
  - Airline Schedules (efficiency here – even at a fraction of a penny per mile can drive out competitors)
- **Accelerated search of large databases (numerous possibilities)**
- **Simulation of important physical systems:**
  - Applications to biological problems such as protein folding and pharmaceutical binding
  - Potential design of new commercial materials with as yet unimagined properties
- **Other undreamt of applications – remember:**
  - In 1960 nobody believed the laser would be used for eye surgery, welding, …
  - In 1950 nobody guessed the transistor would lead to the information revolution, little own the integrated circuit and personal PC!!!

Quantum Information Timeline



NIST Physics Laboratory

NIST – Atomic Physics Division
Carl J. Williams, Chief

National Institute of Standards and Technology
Technology Administration, U.S. Department of Commerce

Importance of QC to US Competitiveness

- QI has the potential of having as much impact on the 21st century as classical computing and information technology had on the 20th century.
- We know that QI allows for increased power and capabilities compared to classical information
- Learning to exploit this information may have profound impact on what we can engineer and how we understand nature
- If QI becomes a major technology innovator then loss of leadership could threaten US Economic leadership in an increasingly competitive world and thus undermine US security

Potential Impact of QC on US Financial System

- While the $ value of the loss of public key cryptography (PKC) is hard to quantify, the damage to electronic commerce and the economy would be huge.
- PKC is the basis for SSL, secure websites, security on blackberries, digital signatures, …
- A Quantum computer destroys PKC
- All symmetric key systems and all PKC applications would have to be replaced by new *much, much larger* keys and technical infrastructure for replacing, replenishing and securing these keys would have to be in place
- New approaches to digital signatures would have to be developed

Why NIST and QI?

- QI may have as much impact on the 21st century IT as its classical analog had on the 20th century.
- QI allows for increased power and capabilities compared to classical information processing
- Exploiting this information may have profound impact on what we can engineer & how we understand nature
- If QI becomes a major technology innovator then US Economic leadership in an increasingly competitive world is necessary
- As a National Measurement Institute (NMI), NIST needs to create the measurement infrastructure for this new technology

Possible Applications of Q. Computers

- **Solution of basics physics problems including:**
  - Lattice Quantum Electro/Chromo-Dynamics (QED/QCD)
  - Simulations of Condensed Matter Hamiltonians – High T_c Superconductivity
- **Optimization of commercially important problems:**
  - Electronic Circuit layout
  - Airline Schedules (efficiency here – even at a fraction of a penny per mile can drive out competitors)
- **Accelerated search of large databases (numerous possibilities)**
- **Simulation of important physical systems:**
  - Biological applications: e.g. protein folding & pharmaceutical binding
  - Potential design of new commercial materials with unimagined properties
- **Other undreamt of applications – remember:**
  - In 1960 nobody believed the laser would be used for eye surgery, welding, …
  - In 1950 nobody guessed the transistor would lead to the information revolution, little own the integrated circuit and personal PC!!!

NIST's Response

- NIST is responsible for secure business communication
- QI is part of the American Competitiveness Initiative
- We believe that QI and its technological spin-offs will be a major technical thrust in the 21st Century
- We currently are focusing our metrological efforts on photons but new areas such as clocks are developing
- Together with the University of Maryland and LPS/NSA, NIST has established the Joint Quantum Institute
- We have world leading programs in atoms, ion, photons, Josephson Junctions, and quantum materials
- A effort in quantum analog simulations is starting
- We believe other NMI's will follow
- NIST spent ~$9M FY06 – should grow to ~$15M in FY07

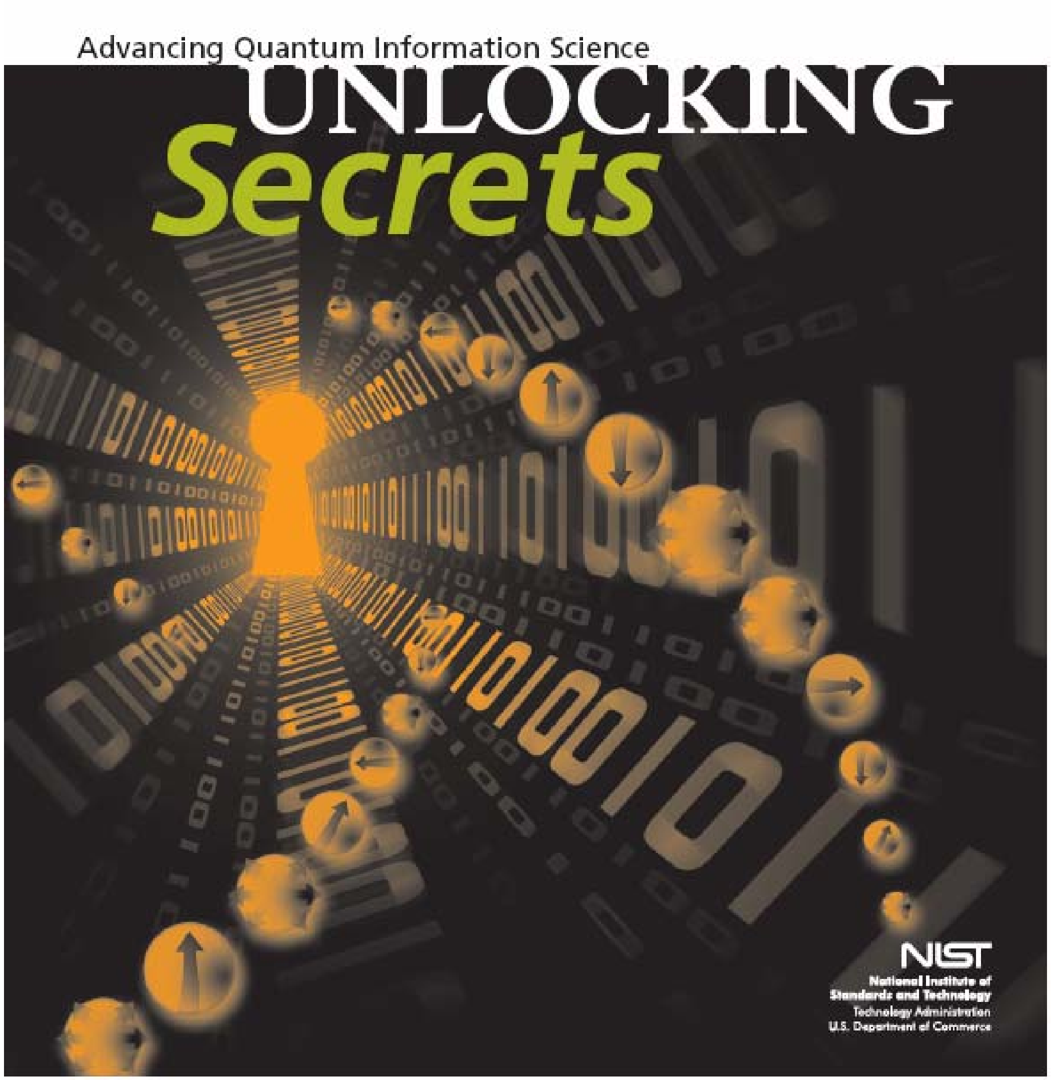
The Joint Quantum Institute

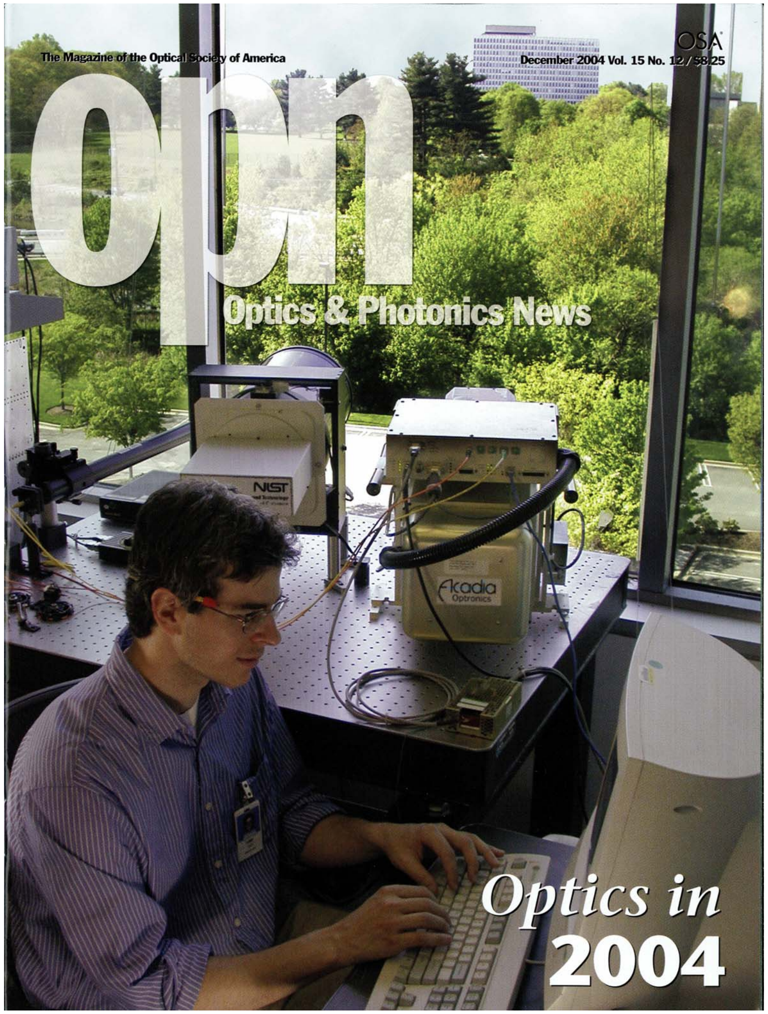
- Established in September 2006 among three participating institutions: UMd, NIST, and LPS/NSA – patterned on JILA
- An initial budget of ~$6M/yr (~$4M/yr from NIST)
- Run by the Fellows of the JQI (12 NIST Scientists and 10 UMd Scientists – including 16 APS Fellows)
- Several new hires are planned with an ultimate size of 25-30
- A NIST and UMD Co-Director (CJW & Chris Lobb)
- A Liaison to LPS/NSA (Keith Miller)
- A synergistic activity between AMO, CM, and QI scientists
- 10000 sq ft of space to be provided Fall 2007
- By 2011 60000 sq ft, much of it world class lab space will be provide in a new Physical Science Complex

Goals of the JQI

- Develop a world-class research institute that will build the scientific foundation for understanding coherent quantum phenomena and thereby lay the foundation for engineering and controlling complex quantum systems capable of using the coherence and entanglement of quantum mechanics
- Maintain and enhance the nation's leading role in high technology through the creation of a powerful collaboration among NIST, UM and NSA; and
- Establish a unique, interdisciplinary center for the interchange of ideas among atomic physics, condensed matter and quantum information scientists.

Propaganda


Advancing Quantum Information Science
UNLOCKING
Secrets
NIST
National Institute of Standards and Technology
Technology Administration
U.S. Department of Commerce


The Magazine of the Optical Society of America
OSA
December 2004 Vol. 15 No. 12 / $8.25
opn
Optics & Photonics News
Optics in 2004