# Quantum Information at NIST and the Federal Research Agenda

Carl J. Williams
National Institute of Standards & Technology

http://qubit.nist.gov

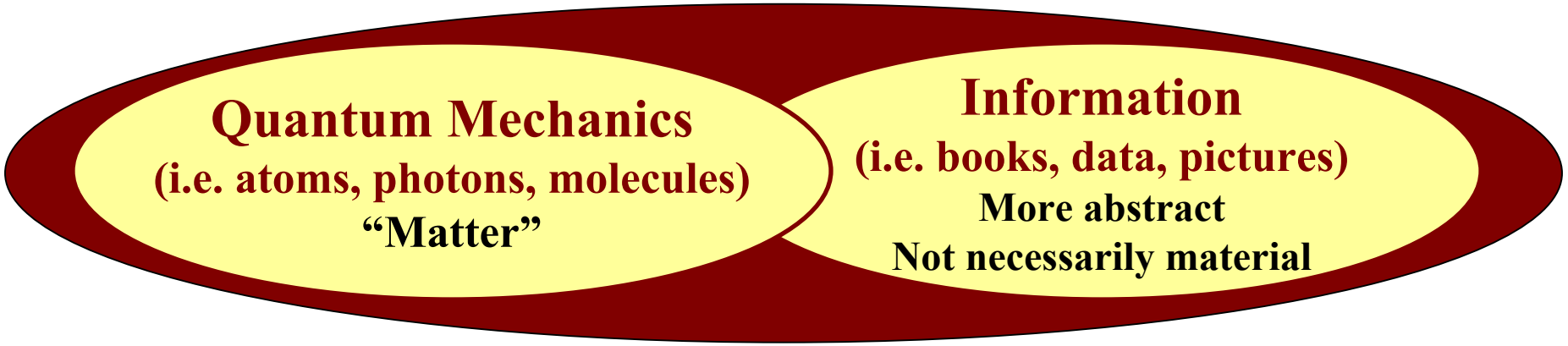


NIST
National Institute of Standards and Technology
Technology Administration, U.S. Department of Commerce

# What is Quantum Information?

***A radical departure in information technology, more fundamentally different from current IT than the digital computer is from the abacus.***

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




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

# 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 why quantum information is useful and also show why it *may ultimately lead* to quantum engineering.

**Belief: Quantum Information and Quantum Engineering will have a *tremendous economic impact* in the 21st Century**

# QISCoG

**Quantum Information Science Coordinating Group**

– **an informal government coordinating group that meets twice yearly to discuss and coordinate government activities in Quantum Information Science**

**Chair: Henry Everitt (ARO)**

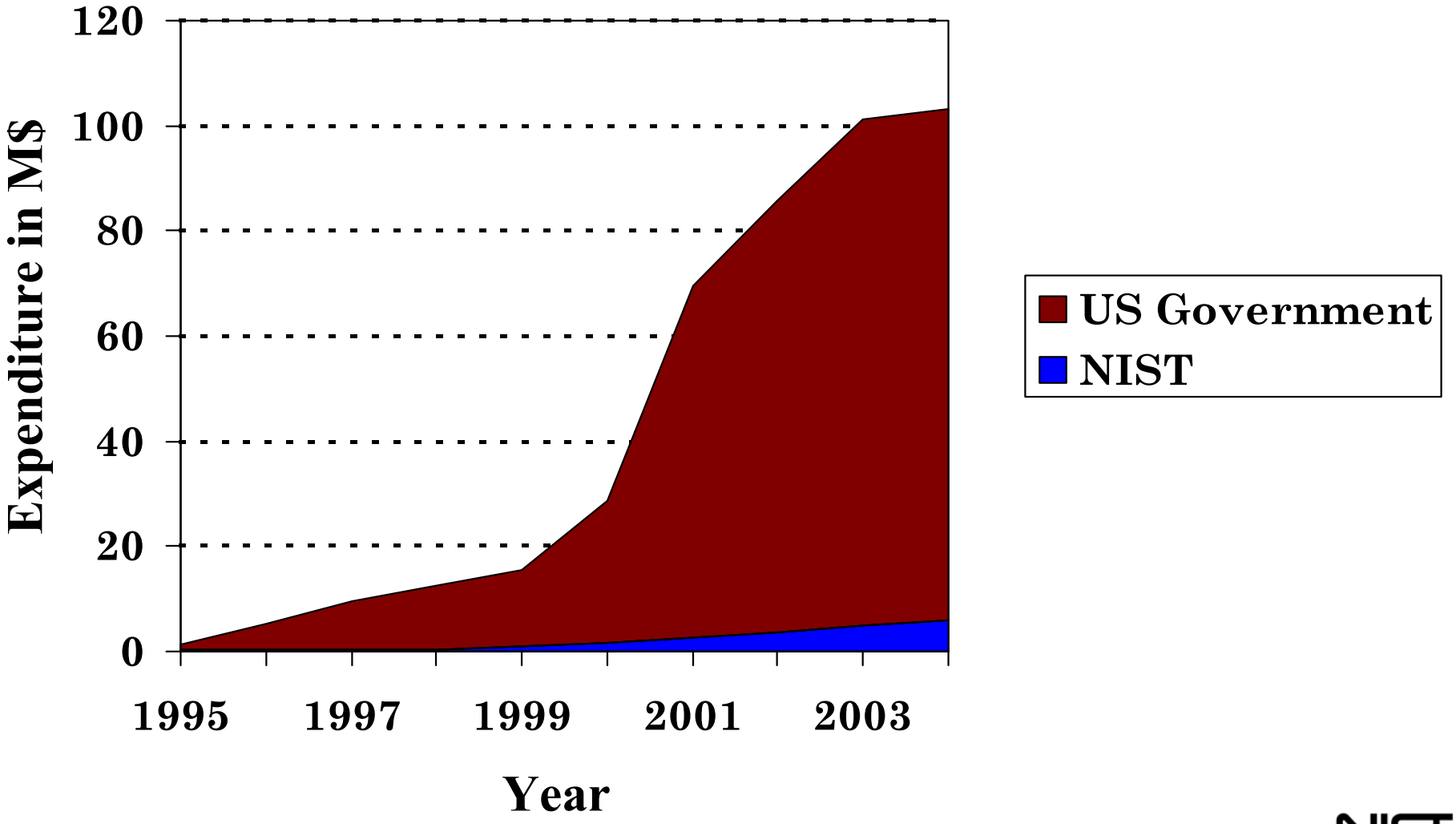
**NIST Representative: Carl J. Williams**

**Last Meeting: Mid-April 2004**

**For Roadmap see: http://qist.lanl.gov**

**Henry Everitt: Handles most BAA's and NSA/ARDA funding of educational institutions**

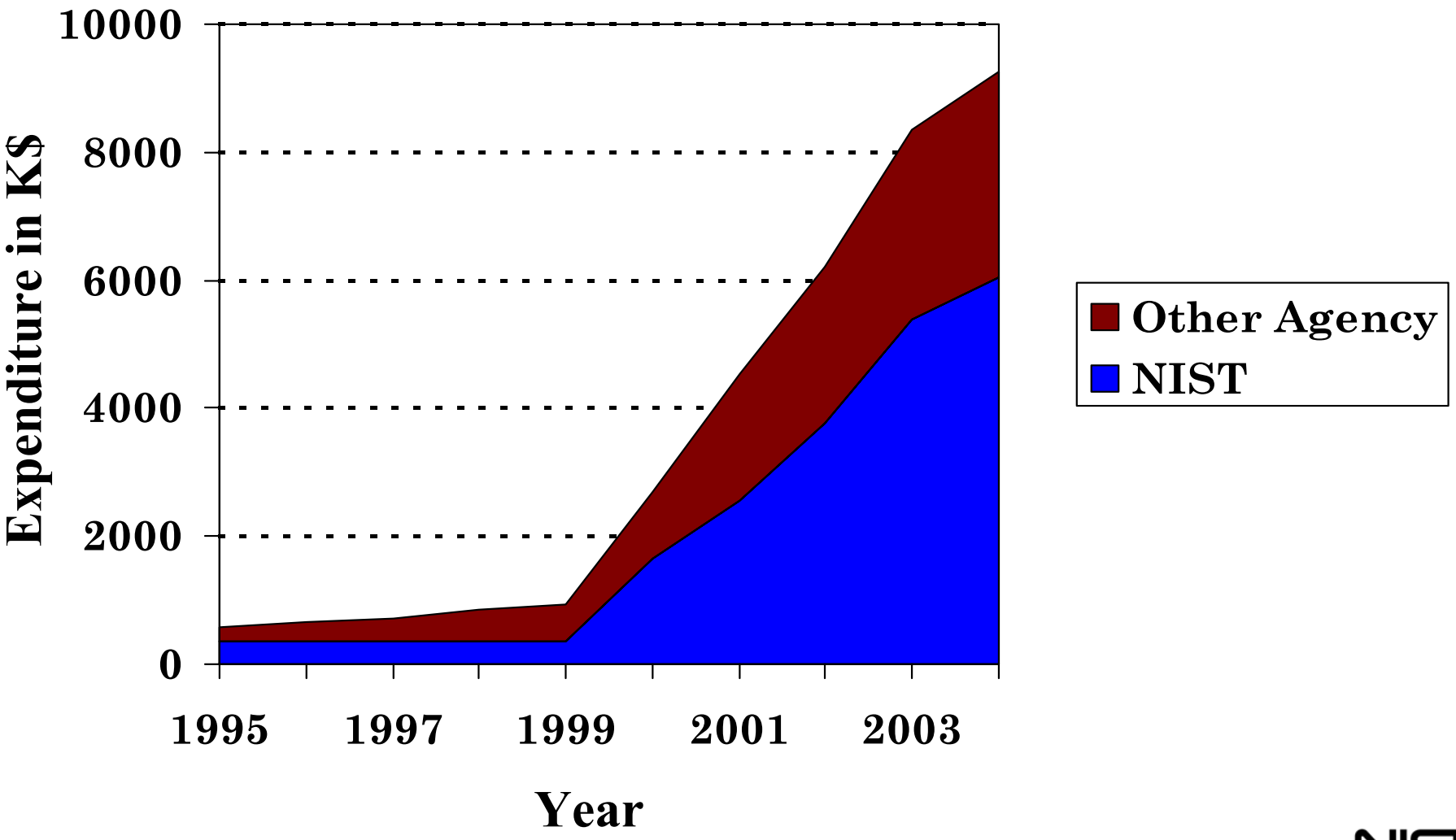
# US Funding of QIS






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

# Quantum Funding at NIST






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

# QIS View -- Rest of the World

- **European Wide Program**
  - **Physics of Q Information ~ 0.3M∈**
  - **EQCSPOT ~ 0.5M ∈**
  - **European Science Foundation ~ 0.2M ∈**
  - **New QIPC Initiative ~ 8.0M ∈**
- **EuropeanNational Programs (2000): Total ~ 10M ∈**
  - **Italy, Germany, UK, Switzerland, Austria, France, Denmark & Holland**
- **Japanese Program**
  - **Ministry of Posts and Telecommunication (MPT): $2.5M (2001)**
    Quantum Information Tech. Initiative Requested $400M/10 years
  - **Japanese Science and Technology Corp. (JST): $6M (2001)**
  - **Ministry of International Trade and Industry (MITI): $8M/yr**
- **Korea Program: ~ $1.3M**
- **China: ~ 4M RMB**
- **Australia: ~$A 5M *Center for Quantum Commputation***

# Quantum Information in the US

- ARDA/NSA – Quantum Computation Program
  Quantum Computing Roadmap
- ARDA/NSA – Device Physics for Quantum Communication
  Quantum Communication Roadmap
- DARPA – Quantum Information Science and Technology
  Focus on Quantum Systems (FoQuS)
- NSF – Basic Research and Education – *i.e.* largest funding agent for universities
- DoE – Primarily Los Alamos
- NASA, DoE, AFOSR, ARO/ARL, NRL
- NIST

# How can we use Quantum Information?

- **Quantum Communication - 100% physically secure**
  - Quantum key distribution – generation of classical key material
  - Quantum Teleportation
  - Quantum Dense Coding
- **Universal Quantum Logic:** ***all*** **quantum computations –** ***i.e. any arbitrary*** **unitary operations – may be efficiently constructed from 1- and 2-qubit gates**
- **Quantum Algorithms**
  - Factorization of large primes (Shor's algorithm)
  - Searching large databases (Grover's algorithm)
  - Quantum Fourier Transforms
  - Potential attack of NP problems
  - Simulation of large-scale quantum systems
- **Quantum Measurement – improved accuracy**
  - Heisenberg limit $\propto 1/N$ vs Shot-Noise limit $\propto 1/\mathrm{Sqrt}(N)$
  - Better Atomic Clocks
- **Quantum Engineering – specialized quantum devices**

# Quantum Information at NIST

- **Quantum Computing**
  - **Ion Traps: David Wineland (PL, Boulder)**
  - **Neutral Atoms: William Phillips (PL, Gaithersburg)**
  - **SQuIDS: John Martinis, Ray Simmonds (EEEL, Boulder)**
  - **Device Physics & Architectures: Carl Williams (PL, Gaithersburg)**
  - **Quantum Information Theory: Manny Knill (ITL, Boulder)**
- **Quantum Communication**
  - **Test-Bed: Joshua Bienfang, Alan Mink, Tassos Nakassis (Gaithersburg)**
  - **Single Photon Sources**
    - Parametric Down Converters: **Alan Migdall (PL, Gaithersburg)**
    - Quantum-Dot Photonics: **Richard Mirin (EEEL, Boulder)**
  - **Single Photon Detectors: Sae Woo Nam (EEEL, Boulder)**
  - **QComm Internet Protocols: A. Nakassis, R. Kuhn (ITL, Gaithersburg)**

**http://qubit.nist.gov**

# Historical View of QI at NIST

**1992 – Dave Wineland suggests "*GHZ states*" good for clocks**

**1994 – NIST pursues spin squeezing for clocks**
- **Shor's Algorithm**
- **First NIST meeting on Quantum Information**

**1995 – Cirac/Zoller write ion gate paper**
- **Wineland demonstrates first quantum gate**

**2000 – NIST funds single photon turnstile effort**
- **Seed funding for NIST QI Program**
- **Second NIST meeting on Quantum Information**

**2001 – NIST QIP officially starts**
- **NIST funded by DARPA QuIST (primarily Q. Comm.)**

**2003 – NIST QIP effort expanded (Martinis, Knill, …)**

**2004 – Third NIST meeting on Quantum Information**

# Relevance to NIST Mission

- **Improved fundamental metrology**
  - Attain Heisenberg limit in quantum measurements
  - Better atomic clocks
- **Physically secure transmission of information for E-Commerce and Business**
  - Quantum cryptographic key exchange
  - Internet and Security Protocols
  - Development of metrology of single photon sources and detectors
- **Information Standards and Protocols**

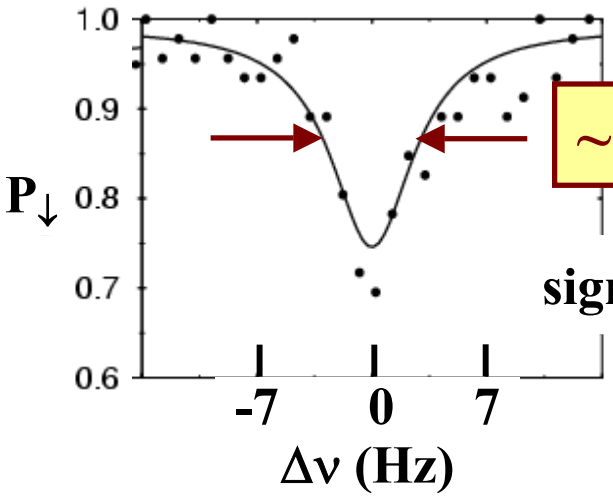
- **Create the foundations for quantum information processing: a new paradigm for computation, measurement and standards at the quantum limit**

  ***Quantum Information, Processing, and Computing***

  **⇒ Quantum Engineering**

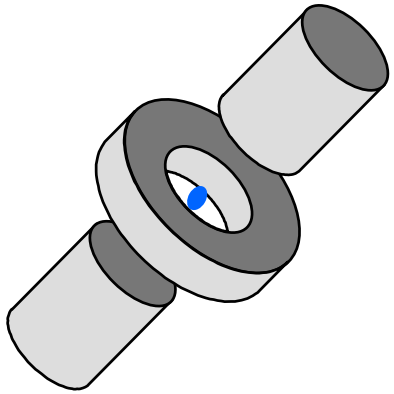
# Quantum Processing and Clocks

- **Current ion clock status:**




**~ 6.5 Hz, Q = $1.6 \times 10^{14}$**

**signal is lifetime limited**



**$^{199}Hg^{+}$ has a quadrupole moment and thus a quadrupole shift  a different ion**

- **Basis ion clock with quantum processing:**

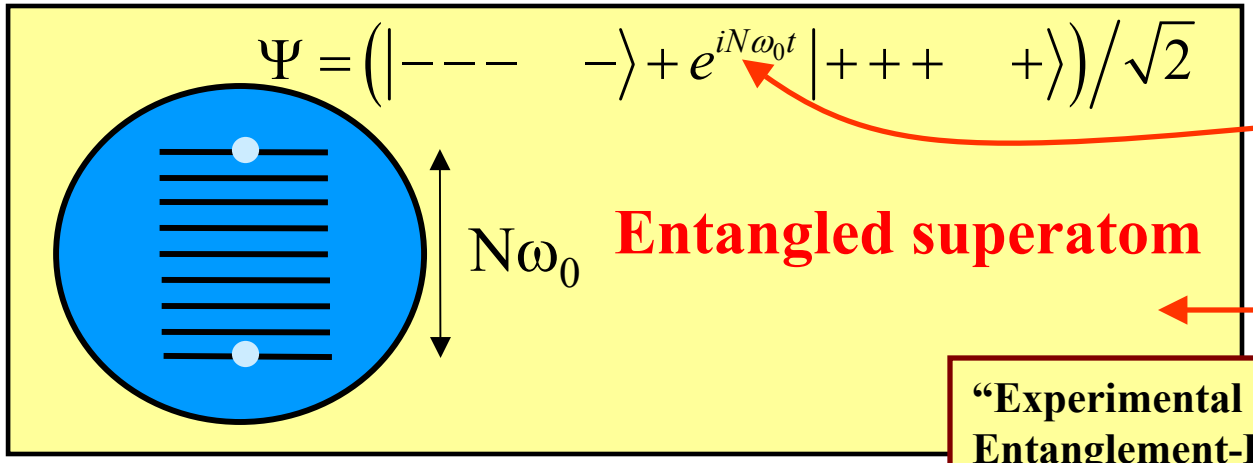
  **Sympathetically cool and detect Clock ion with Logic ion**

**"Logic" ion (*e.g.*, $^{9}Be^{+}$)**

**"Clock" ion**

**Heinzen & DJW, PRA 42, 2977 (1990)**

# Maximally Entangled States




clock provides N times as many ticks in a given t

Entangled atom clock

"Experimental Demonstration of Entanglement-Enhanced Rotation Angle Estimation Using Trapped Ions," V. Meyer *et al.*, *PRL*, June 2001.

**Demonstrated gain with 3 forms of "spin-squeezing" (N = 2)**

- GHZ states are "maximally entangled" and provide an ideal resource for precision measurement.
- Resolution improved by N where N is the number of qubits
- Recent results for N=3 and planning for large N underway



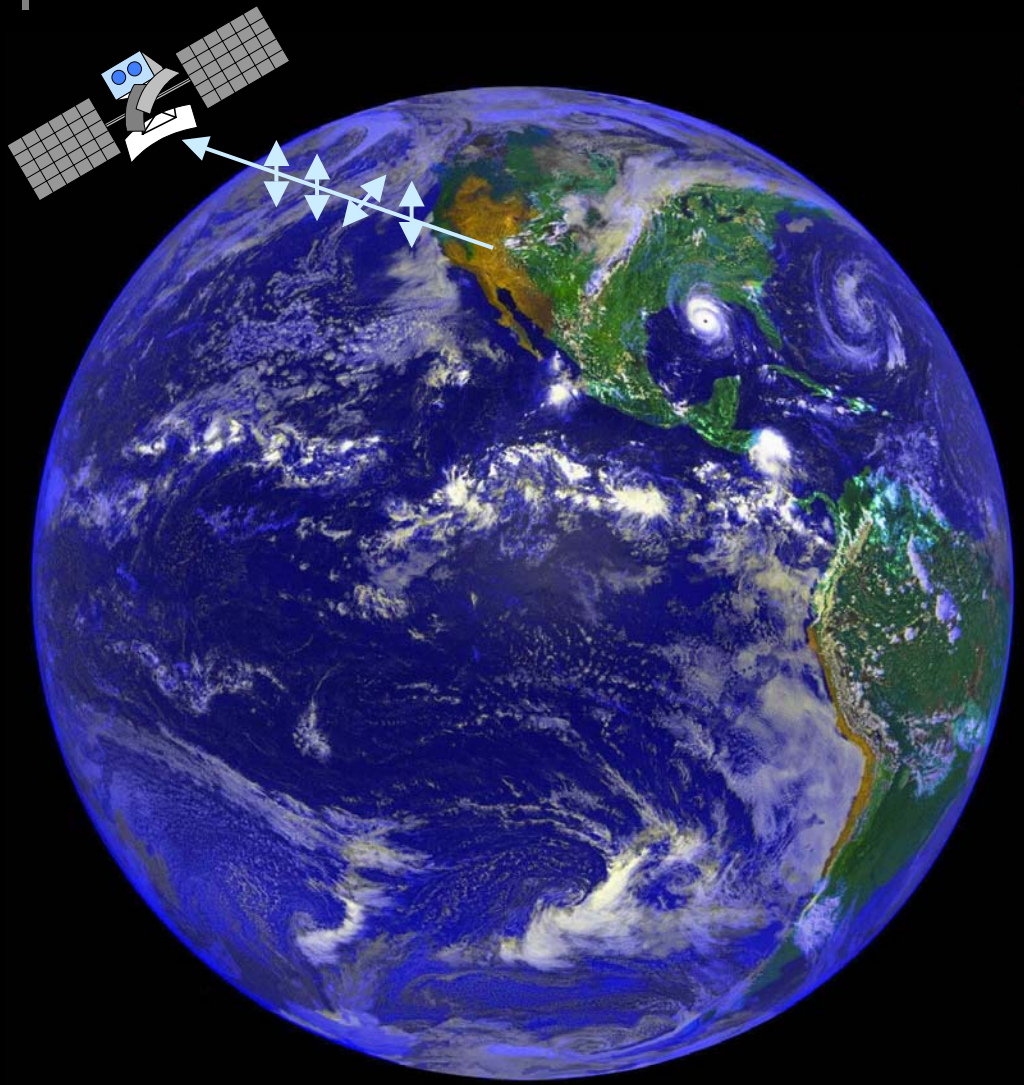
NIST
National Institute of Standards and Technology
Technology Administration, U.S. Department of Commerce

# Quantum Communication

- **Quantum Key Distribution – attenuated or single photon sources with known but arbitrary selected polarization and an authenticated classical channel**
- **Quantum Teleportation – *i.e.* "sending" of an unknown quantum state – requires shared Bell's (entangled) states and an authenticated classical channel**
- **Quantum Communication:**
  - **with attenuated sources is 100% physically secure and has been demonstrated over kilometer distances**
  - **in fibers over distances larger than ~100 km will require quantum repeaters**
  - **~ 10 qubit quantum processors can serve as quantum repeaters**
  - **Re-keying of satellites on the horizon**
  - **NIST has a new high speed free space QKD system that is a factor of 100 improvement over current systems**

# QKD for Satellite Communications

Richard J. Hughes
Physics Division, LANL
(505) 667-3876
hughes@lanl.gov



- On-orbit key update
- Offers long-term security guarantees with reliable security lifetime estimates
- Key transfer between ground-based users
- Transportable ground station feasible
- Cryptographically useful key rates possible day (LEO) or night (LEO, Molniya and GEO)

# Quantum Communications at NIST

- **Quantum Communications Test-Bed (PL/ITL Gaithersburg)**
- **Single Photon Sources**
  - **Parametric Down Converters (PL, Gaithersburg)**
    **Stefania Castelletto, Michael Ware, Alan Migdall**
  - **Quantum-Dot Photonics (EEEL, Boulder)**
    **Joe Berry, David Su, Mark Keller, Richard Mirin**
- **Single Photon Detector (EEEL, Boulder)**
  **Danna Rosenberg, Sae Woo Nam, John Martinis, Aaron Miller**
- **Protocols**
  - **Internet Interface: Anastase Nakassis (ITL, Gaithersburg)**
  - **Authentication and Security: Richard Kuhn (ITL, Gaithersburg)**
  - **New QKD Protocols: David Song (ITL, Gaithersburg)**

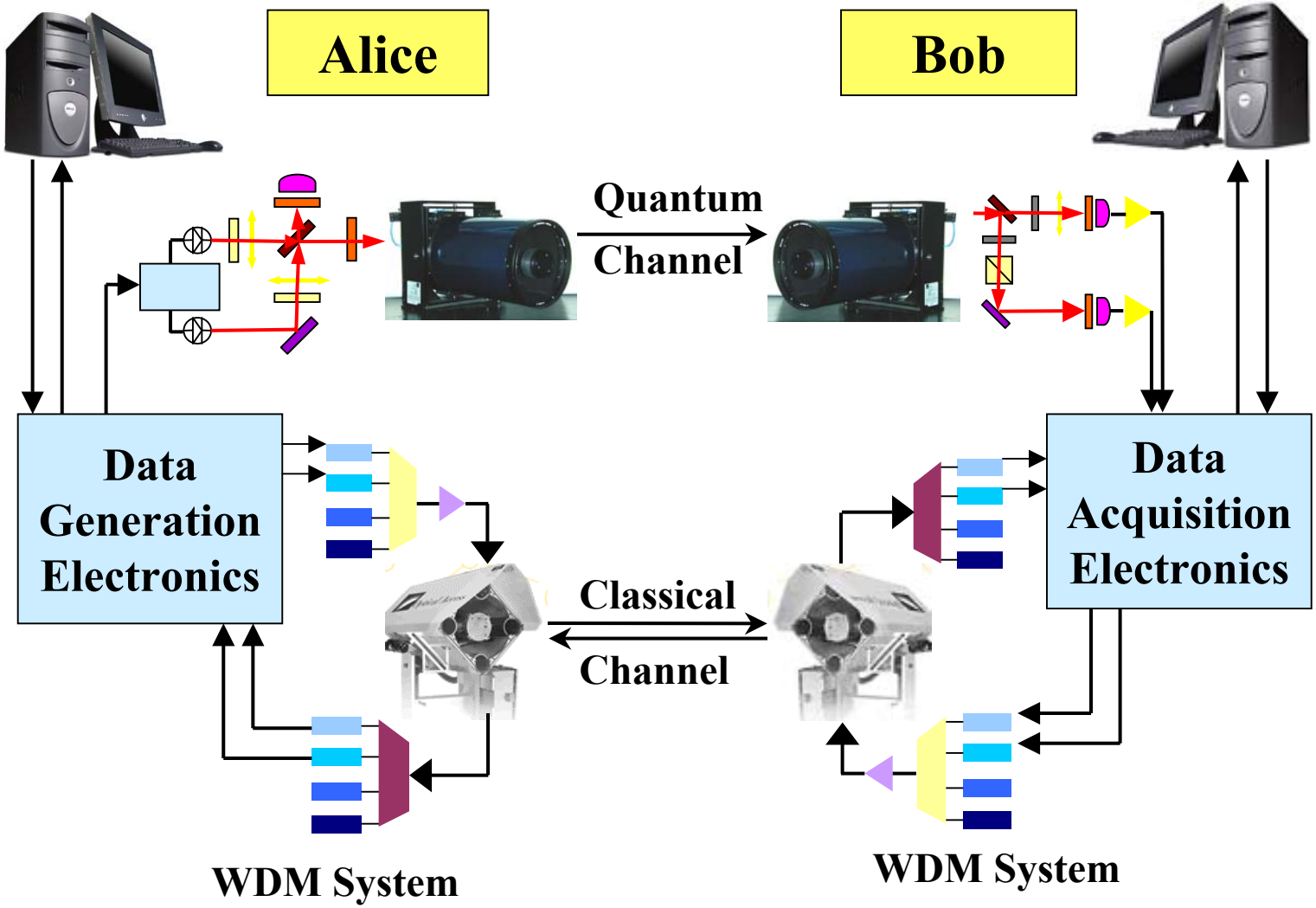
# Quantum Communication Test-Bed

## What is special about the NIST system?

- **Dual Classical & Quantum Channels running at 1.25 GHz**
- **Network – Internet interfaced (Also BBN)**
  - **Security Protocols – SSL, Authentication**
- **Quantum Link**
  - **Attenuated VCSEL transmitters (initially)**
  - **850 nm free space optics**
  - **Si avalanche detectors**
- **Two classical links near 1550 nm**
  - **8B/10B encoded path for timing/framing**
  - **Dedicated gigabit ethernet channel**
    - Sifting, Error correction, and Reconciliation
    - Privacy amplification


**Joshua Bienfang, Alan Mink, Alex Gross, Xiao Tang, Richang Lu, Barry Hershman, Jesse Wen, Ed Hagley, David Su, Charles Clark, Carl Williams**

# Testbed Structure



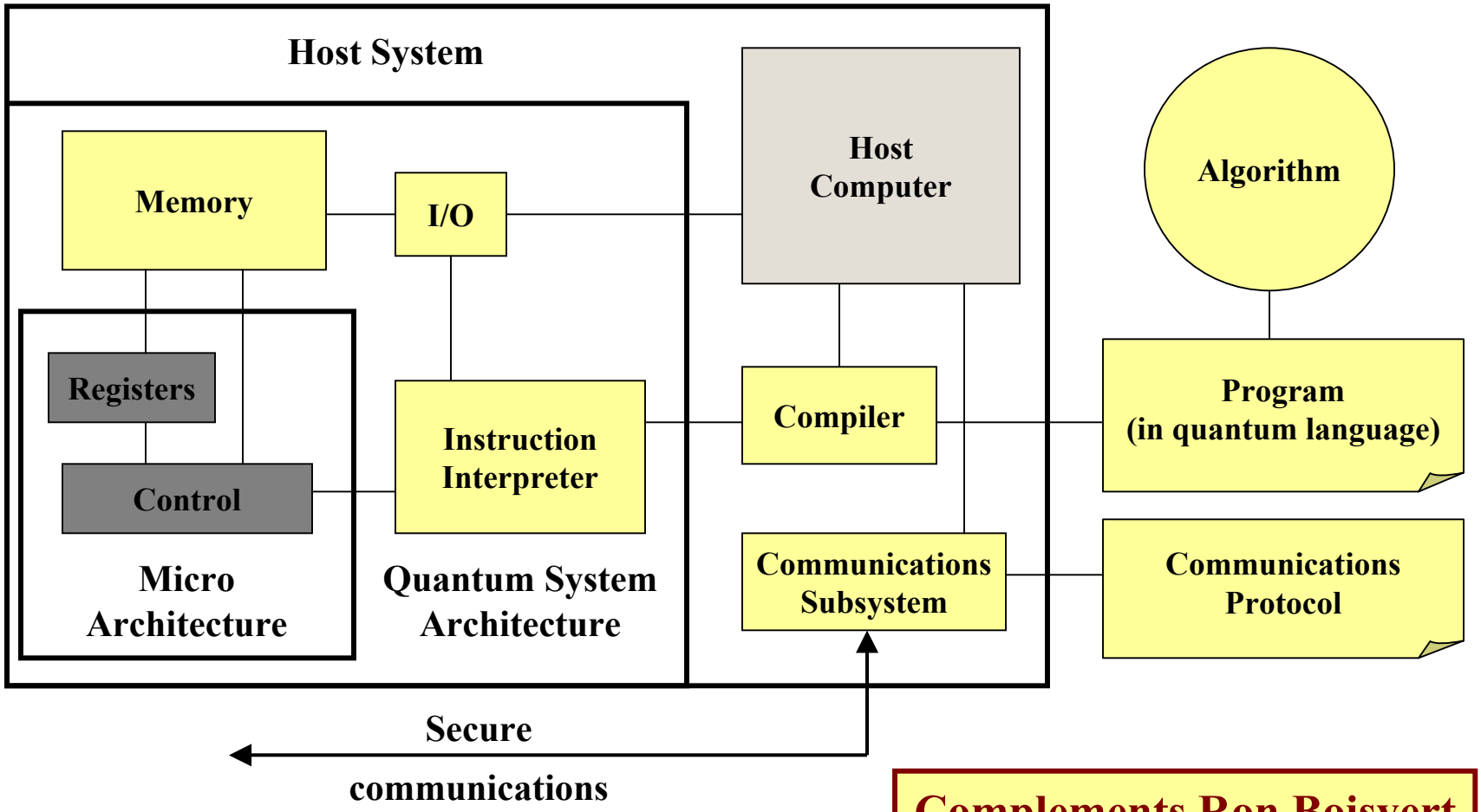



NIST
National Institute of Standards and Technology
Technology Administration, U.S. Department of Commerce

# Quantum Computing at NIST

- **Ion Traps (PL, Boulder)**
  **Murray Barrett, Amit Ben-Kish, Joe Britten, John Chiaverini, Brian DeMarco, John Jost, Brana Jelenkovic, Chris Langer, *Didi Leibfried*, David Lucas, Volker Meyer, Jim Beall, Wayne Itano, David Wineland**
- **Neutral Atoms (PL, Gaithersburg)**
  **Bruno Laburthe, Ken O'Hara, Johnny Huckans, Chad Fertig, William Phillips, Trey Porto, Steve Rolston**
- **Josephson Junctions (EEEL, Boulder)**
  **Kristine Lang, Ray Simmonds, Jose Aumentado, John Martinis, Sae Woo Nam**
- **Device Physics & Theory (PL, Gaithersburg)**
  **Gavin Brennen, Tommaso Calarco, Guido Pupillo, Ana-Marie Reyes, Charles Clark, Paul Julienne, Eite Tiesinga, Carl Williams**
- **Architectures, Error Correction, & Algorithms (PL/ITL)**
  **Gavin Brennen, Stephen Bullock, David Song, Isabel Beichl, Manny Knill, Carl Williams**

# Building a (Quantum) Computer




**Complements Ron Boisvert**

**Whole pieces do not yet exist and even within the quantum micro-architecture how do arbitrary qubits communicate?**

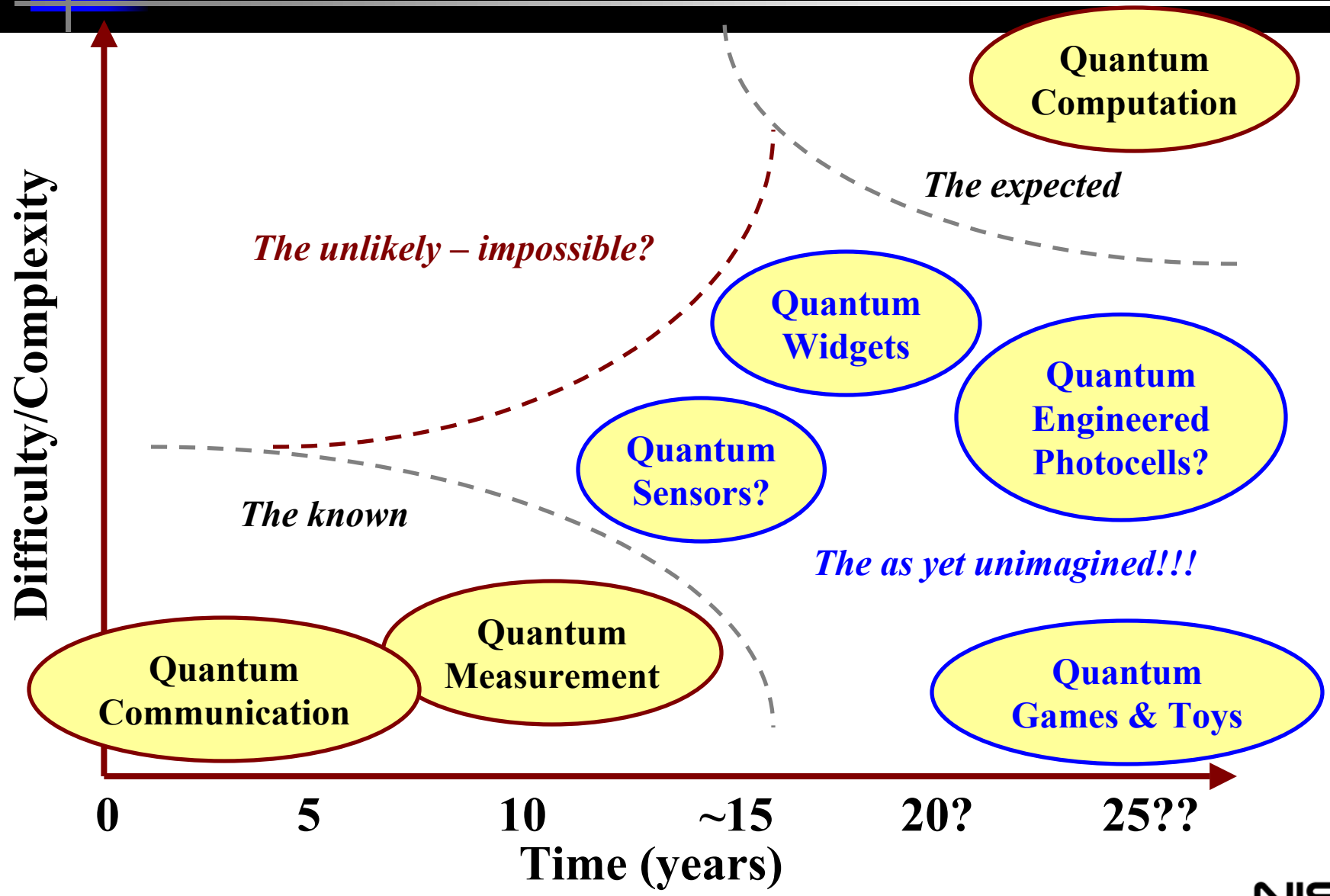
# World Class Competition

US does not lead in all technology areas

Example: "Center for Quantum Computing Technology" led by Prof. R. Clark, University of New South Wales (http://www.qcaustralia.org)

- Effort focussed on on embedding single P atoms in Si
- Single approach is large compared to any US program
- Asian Technology Information Program (ATIP) – May 6, 2003 report (ATIP03.028: Quantum Computation at ANU) states that the Australian National University (ANU) "group has a mission to develop and secure intellectual property (IP) in the area of solid-state quantum computing."
- ATIP report dated April 10, 2003 (ATIP03.021: Solid State & Optical Approaches to Quantum Information Science) describes relevance and application of the solid state approach to nano-scale fabrication and lithography.

# Quantum Information Timeline






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

# 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.

# Vision and Future

**VISION: NIST will enable quantum measurement, metrology, and engineering and will help to develop first applications**

- **Measurement beyond standard quantum limit**
  - N=2 demonstrated
  - N=3 underway
  - Large N planned
- **Applications to atomic clocks**
  - Limits understood – quadrupole moment issue
  - Cooling and Readout with other species possible
  - Large GHZ state N possible with $B^+$ or $Al^+$
- **Additional applications being sought**
- **Potential use as a quantum repeater remains an option and could be integrated with test-bed**

# Homeland Security

- **Quantum Communication**
  - **Provides 100% provable physical security**
    Note: Provable security applies only to the "quantum channel."
    The classical systems and people at each end will remain insecure
  - **Allows "teleportation" of quantum *encoded* information**
- **Quantum Information**
  - **Secure counterfeit proof "quantum money"**
  - **Digital quantum signatures**
  - **No quantum bit commitment – quantum cheating**
- **Quantum Computers**
  - **Puts at risk the RSA and public key systems**
  - **Creates new risk structure for anything but one time pads**
  - **Improved Image Processing and Pattern Recognition Likely**
  - **Data searching, sorting and verification possible**

**Summary: What quantum computers takes away quantum communication gives back**