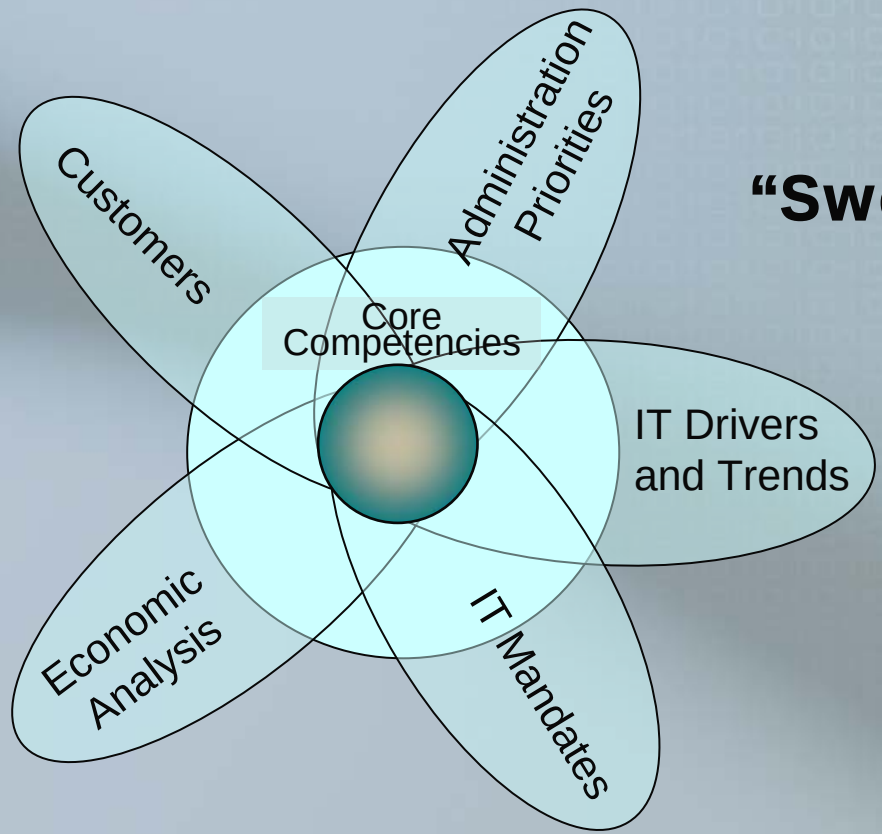
Information Technology Research at NIST

Cita M. Furlani
Director
Information Technology Laboratory

August 14, 2007

Building the IT Research Agenda at NIST

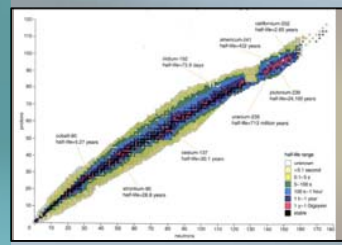


“Sweet Spot”

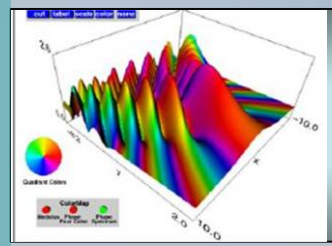
Core Competencies in IT Research

Technology Development

IT Measurement and Testing



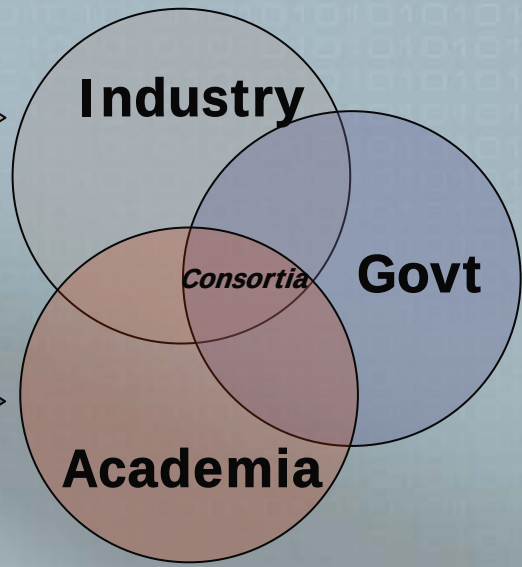
Mathematical and Statistical Analyses for Measurement Science



Modeling and Simulation for Measurement Science

IT Standards Development and Deployment

Customers



FY08 Administration R&D Priorities

- Homeland Security
- Energy Security
- **Advanced Networking and High-End Computing**
- National Nanotechnology Initiative
- **Understanding Complex Biological Systems**
- Environment

http://www.ostp.gov/html/budget/2008/m06-17.pdf

FY08 Administration R&D Priorities

- Advanced Networking and High-End Computing
  - High-end computing investments
  - Advanced networking technologies
    - Hardware, software, and tools (including large-scale testbeds) for the design of secure, reliable, and scalable data communication networks for high-speed transmission of extremely large data sets
    - Enhancing the utility and the scientific impact of federal high-end computing facilities
  - Cybersecurity
    - 2006 *Federal Plan for Cyber Security and Information Assurance R&D* (http://www.nitrd.gov/pubs/csia/FederalPlan_CSIA_RnD.pdf)

FY08 Administration R&D Priorities

- Understanding Complex Biological Systems
  - Development of a deeper understanding of complex biological systems, which will require collaborations among physical, computational, behavioral, social, and biological scientists and engineers
  - Need to develop the data management tools and platforms necessary to facilitate this research

ACI and IT Research: FY 2007 NIST Initiative Appropriations and FY 2008 Request

Initiative	FY 2007 Appropriation	FY 2008 Request
Cyber Security: Innovative Technologies for National Security	**$1.3M**	**$0.6M**
Enabling Nanotechnology from Discovery to Manufacture	$15.0M	$11.0M
NIST Center for Neutron Research (NCNR) Expansion and Reliability Improvements: A National Need	$10.0M	--
Enabling the Hydrogen Economy	$6.0M	$4.0M
Manufacturing Innovation through Supply Chain Integration	**$1.0M**	**$1.0M**
Quantum Information Science - Infrastructure for 21st Century Innovation	**$6.0M**	**$7.0M**
National Earthquake Hazard Reduction Program	$3.25M	

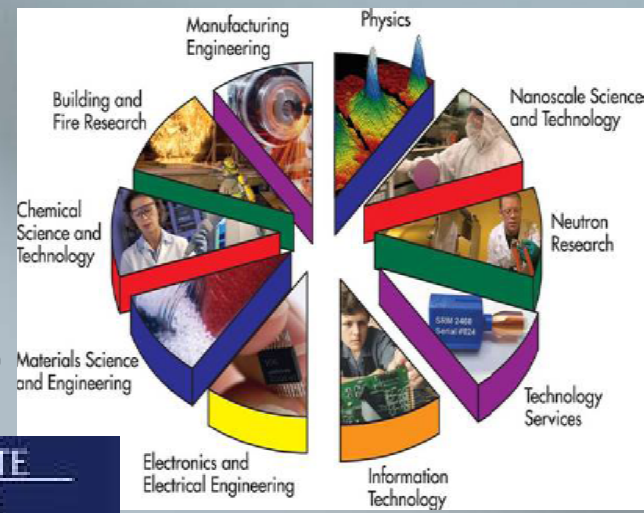
ACI and IT Research: FY 2007 NIST Initiative Appropriations and FY 2008 Request

Initiative	F2007 Appropriation	FY2008 Request
Structural Safety in Hurricanes, Fires, and Earthquakes	$2.0M	$4.0M
International Standards and Innovation: Opening Markets for American Workers and Exporters	$1.0M	$1.0M
Innovations in Measurement Science	$1.0M	$3.0M
Bioimaging: A 21st Century Toolbox for Medical Technology	**$3.0M**	**$1.0M**
Synchrotron Measurement Science and Technology: Enabling Next Generation Materials Innovation	$3.5M	$1.5M
Biometrics: Identifying Friend or Foe?	**$0.0M**	**$2.0M**
Measurements and Standards for the Climate Change Science Program	--	$5.0M

Selected IT Drivers and Trends

- **New fundamental technologies enabled by IT** – nanotech, quantum info, biotech
- **Globalization** – development and use of IT is distributed worldwide
- **Pervasiveness** of IT/software – IT invades all activities in personal and professional lives including critical infrastructure
- **Pace of evolution** – the speed of change is rapid
- **Moore's Law** – increased computing power enables collection of more data + more complexity of programs
- **Increasingly blurred line between the sciences**
- **Outsourcing of IT jobs and declining numbers of students in IT**
- Increase in **cyber warfare/crime/spam/virus**
- **Broadband access** – initiatives to get broadband to the home
- **Sophisticated tools for unsophisticated users** – tools need to maintain high 'standards'
- **Information explosion** leads to difficulty in identifying the right piece of information
- **Reliability, quality, security, and trustworthiness of computing is inadequate and questioned** by the end users
- **Emerging use of robotics** throughout the realm of human activity
- World is flat -> Distributed Manufacturing -> Internationally Accepted Measurement System -> **Increased Need For SI Traceability**

Representative Customers and Collaborators

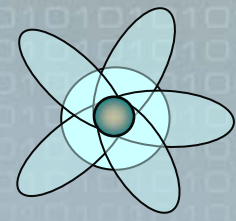


Specific IT Mandates

- Biometrics
  - USA PATRIOT Act
  - Enhanced Border Security and Visa Entry Reform Act
  - Homeland Security Presidential Directive #12: Policy for a Common Identification Standard for Federal Employees and contractors
  - 10-Print Transition: mandated by Homeland Security Council Deputies Committee
- Cyber Security
  - Federal Information Security Management Act (FISMA) of 2002 (Title III of the E-Government Act), including
    - Information Security and Privacy Advisory Board (ISPAB) mandate amended
  - Computer Security Research and Development Act of 2002
  - Homeland Security Presidential Directive #12
  - Conference Report on House Resolution 5441, Department of Homeland Security Appropriations Act, 2007: Title V - General Provisions (WHTI Certification effort)
  - OMB M04-04 E-Authentication Guidance for Federal Agencies
  - Information Technology Management Reform Act of 1996, Public Law 104-106
  - OMB Circular A-130 and OMB Directive 05-24
- Emergency Alert for wireless mobile devices
  - Warning, Alert, and Response Network Act
- Healthcare
  - Executive Order: Incentives for the Use of Health Information Technology and Establishing the Position of the National Health Information Technology Coordinator
- Internet Protocol version 6 (IPv6)
  - OMB memo M-05-22 on Transition Planning for IPv6 (August 2, 2005)
- Statistical methods for evaluating and expressing the uncertainty of NIST measurement results
  - NIST Administrative Manual Subchapter 4.09, Appendix E, 3b
- Voluntary Voting System Standards
  - Help America Vote Act

IT Research Focus Areas

- Complex Systems **“Sweet Spot”**
- Cyber Security
- Enabling Scientific Discovery
- Identity Management Systems
- Information Discovery, Use, and Sharing
- Pervasive Information Technology
- Trustworthy Networking
- Trustworthy Software
- Virtual Measurement Systems

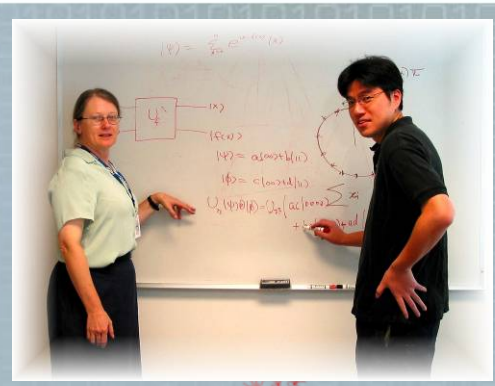


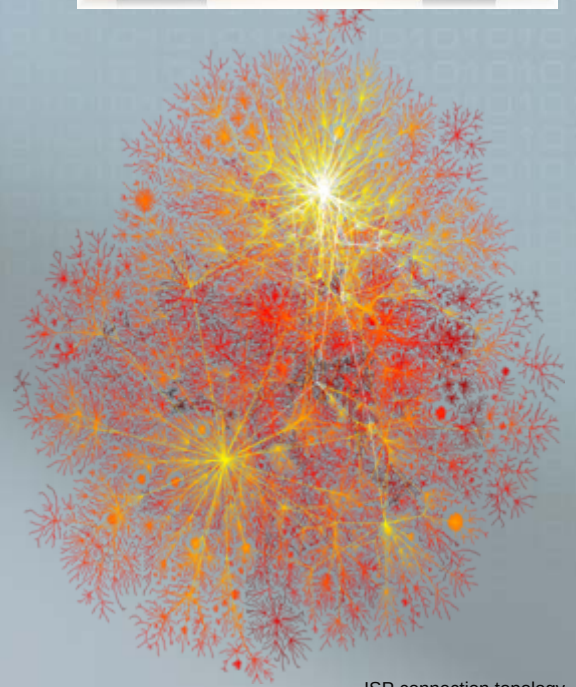
Complex Systems

- Measurement Science for Complex Information Systems (ITL)
- *Foundations of Measurement Science for Information Systems* (ITL)
- Factory Floor Integration Standards and Testbeds (MEL)
- Complex Systems Testbed (ITL)
- Cybernetic Building Systems (BFRL)
- Complex System Failure Analysis (BFRL, ITL)
- Grid Security Infrastructure (ITL)

Foundations of Measurement Science for Information Systems

- Large-scale information systems are built and deployed without fundamental understanding of their range of behaviors and security
- NIST will develop science base for characterization of information systems on par with the physical sciences
  - understanding => metrics => control
- New start in FY2007 with $1.3M Cyber Security: Innovative Technologies for National Security Initiative (ACI) funding
- Long-term research program in mathematical sciences
- *Initial foci:* model, characterize structure and dynamics of large-scale info systems; identify key (computable) measures





ISP connection topology.
Source: caida.org

Cyber Security

- Security implications of a quantum computer on classical networks (PL, ITL)
- Cryptography (ITL)
  - Cryptographic Testing and Validation
  - Hash Functions Competition
  - Standards Toolkit
  - Voting/HAVA
- Industrial Controls for Processes, Systems, and Buildings (MEL, BFRL, ITL)
  - *Industrial Control System Cyber Security*
- IT Security Standards and Guidelines (ITL)
- Security Forensics (ITL)
- Intrusion Detection (ITL)

Industrial Control System Cyber Security

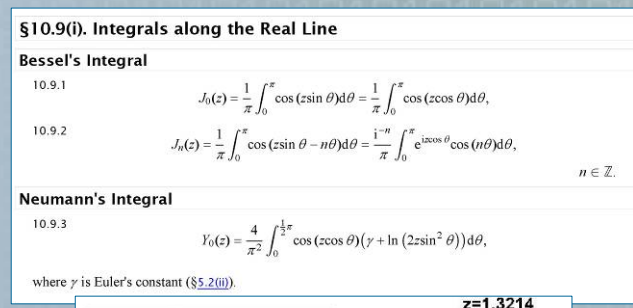
- Improve the cyber security of federally owned/operated Industrial Control Systems which are pervasive throughout all critical infrastructures
- Issue ICS security guidance
  - Develop guidance on applying FIPS 199 *Standards for Security Categorization of Federal Information and Information Systems* to ICS
  - Evolve SP 800-53 *Recommended Security Controls for Federal Information Systems to* better address ICS
  - Develop SP 800-82 *Guide to Supervisory Control and Data Acquisition (SCADA) and Industrial Control System Security*
- Improve the security of public and private sector ICS through standards, R&D and testing
  - Work with voluntary industry standards groups (e.g., The Instrumentation, Systems, and Automation Society--ISA) to develop ICS cyber security standards and guideline development and foster standards convergence
  - NIST ICS Security Testbed provides an industrial setting in which to validate standards for process control security and develop performance and conformance test methods

Enabling Scientific Discovery

- Genome Comparative Analysis Tools (CSTL)
- Tools to Model the Behavior of Nanostructures Embedded in the Appropriate Mesoscopic Environment (CNST)
- High Performance Computing Research (PL)
- *Digital Library of Mathematical Functions (ITL, PL)*
- Quantum Computing and Error Correction (PL, ITL)
- 2-D Adaptive Grid Technique for Schrodinger's Equation (PL, ITL)
- *OOMMF - Object Oriented Micro Magnetic Framework* (ITL, MSEL, EEEL)
- 3-D Chemical Imaging (PL)
- Modeling and Simulation in Nanotechnology
- Magnetic Metrology: Nanoscale Engineered Sensors and Ultra-low Magnetic Field Metrology (EEEL, MSEL, PL, ITL)
- Using Computational Methods to Study Intrinsically Disordered Proteins by Small-Angle Neutron Scattering (NCNR)
- Model-Based Manufacturing Validation Methods and Standards (MEL)
- Computer Modeling of Respiratory Protection for First Responders (BFRL)

Digital Library of Math Functions

- Provide validated scientific reference data related to special functions of applied mathematics
  - Enabling research & modeling in physics, chemistry, engineering
- A model for 21st century dissemination of math information
  - Representation & exchange of mathematical data
  - Search in mathematical databases
  - Development of visually correct 3D interactive graphical representations of complex math functions



§10.9(i). Integrals along the Real Line

Bessel's Integral

10.9.1

$$J_0(z) = \frac{1}{\pi}\int_0^{\pi} \cos(z\sin\theta)\,\mathrm{d}\theta = \frac{1}{\pi}\int_0^{\pi} \cos(z\cos\theta)\,\mathrm{d}\theta,$$

10.9.2

$$J_n(z) = \frac{1}{\pi}\int_0^{\pi} \cos(z\sin\theta - n\theta)\,\mathrm{d}\theta = \frac{\mathrm{i}^{-n}}{\pi}\int_0^{\pi} \mathrm{e}^{\mathrm{i}z\cos\theta}\cos(n\theta)\,\mathrm{d}\theta,$$

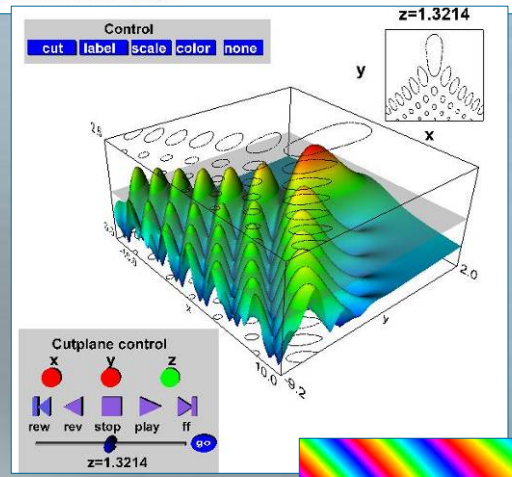
$n \in \mathbb{Z}$.

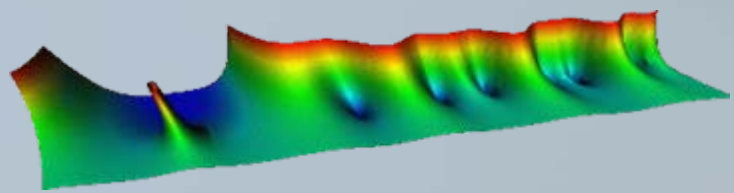
Neumann's Integral

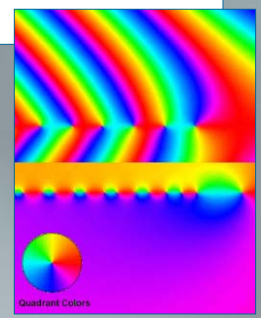
10.9.3

$$Y_0(z) = \frac{4}{\pi^2}\int_0^{\frac{1}{2}\pi} \cos(z\cos\theta)\left(\gamma + \ln\left(2z\sin^2\theta\right)\right)\mathrm{d}\theta,$$

where γ is Euler's constant (§5.2(ii)).

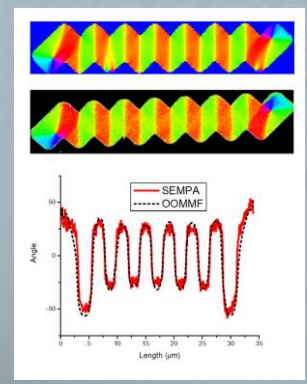


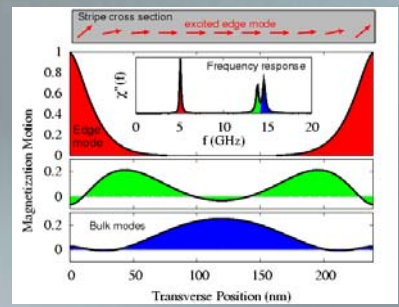




Micromagnetic Modeling

- Reference software, benchmark problems for nanoscale magnetic simulation
  - Improve understanding, reliability of underlying models and numerical methods
- OOMMF enables science at NIST
  - Nanoscale engineered sensors and ultra-low magnetic field metrology
    - *led researchers to understand scaling issues associated with magnetic zig-zags in thin films*
  - Film edge property measurements
    - *provides theoretical foundation: simulates possible experiments, identifies measurable quantities*
- OOMMF enables science at large
  - More than 475 peer-reviewed articles (including 3 in *Science*, 3 in *Nature*) acknowledge use of OOMMF





Identity Management Systems

- Biometric Standards and Technologies (ITL)
- ISO 24727 – Smart Card Standards (ITL)
- Personal Identity Verification (ITL)
- *Multimodal Biometric Application Resource Kit* (ITL)
- Global eID (ITL)
- Measurement Validation Systems for Forensic DNA Profiling (CSTL)
- Secure Biometric Match-On-Card (ITL)

Multimodal Biometric Application Resource Kit

- Building modern biometric applications that are flexible with respect to changes in sensors, workflow, configuration, and responsiveness, is difficult and costly
- The Multimodal Biometric application Resource Kit (MBARK) provides a platform for that reduces complexity and costs
  - Integrates fingerprint, face, and iris biometric sensors
  - Currently investigating palm, voice & vascular biometric sensors
  - Public domain source code that may be leveraged to rapidly develop the next-generation of biometric applications (clients)
  - Features:
    - Provides both a consistent user and software (API) interface
    - Interface designed in cooperation with usability experts
    - Provides true sensor interoperability and highly configurable
  - Key enabler of biometrics usability research

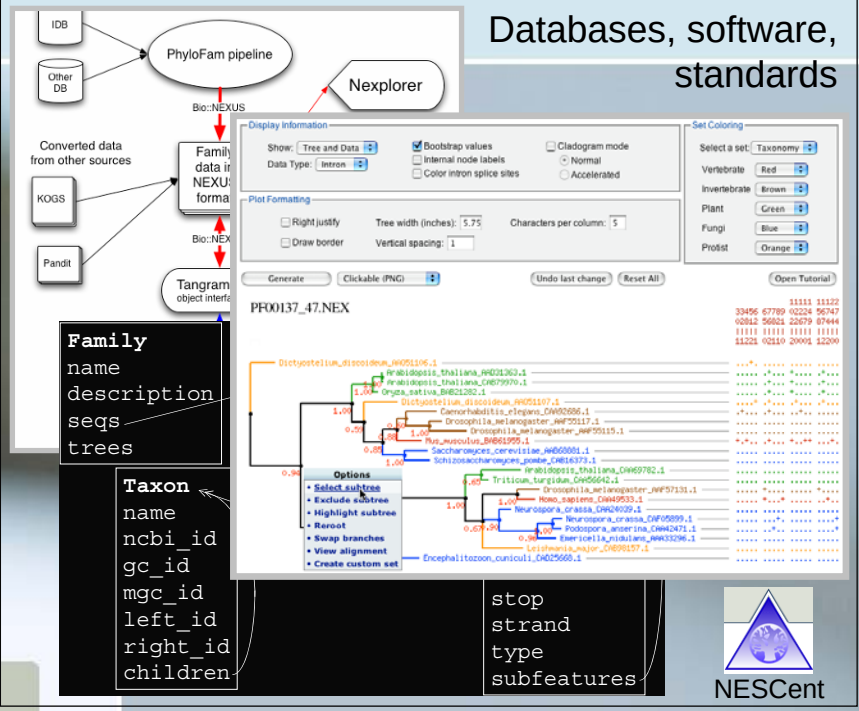
Copyright Robert Rafie

Information Discovery, Use, and Sharing

- Computational Biology (ITL, CSTL)
- Supply Chain (ITL, MEL, BFRL)
- Thermophysical Property Data "on Demand" (CSTL)
- *Bioinformatics* (CSTL)
- Data Classification Algorithms (EEEL)
- Product Lifecycle Standards and Test Methods (MEL)
- MS/MS Reference Libraries on Proteomics (CSTL)
- Semantic Ontologies for HIV and other Bioinformatics Databases (CSTL)
- Construction Integration and Automation Technology (BFRL)
- Human Language Technology (ITL)
- Multimedia Standards and testing (ITL)

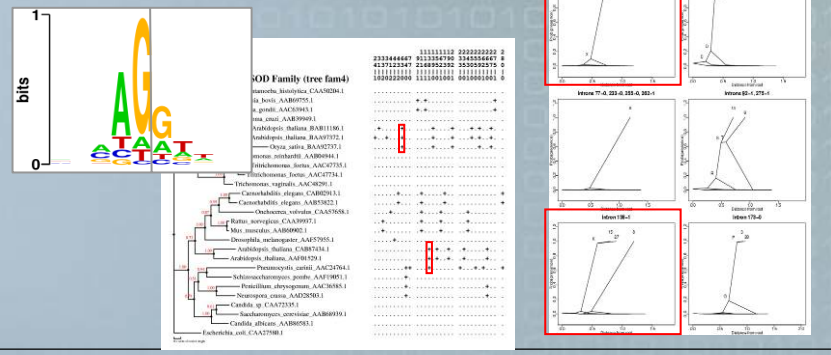
Bioinformatics

Databases, software, standards

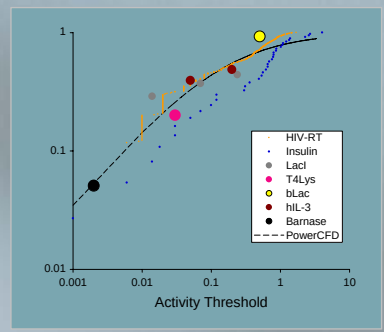


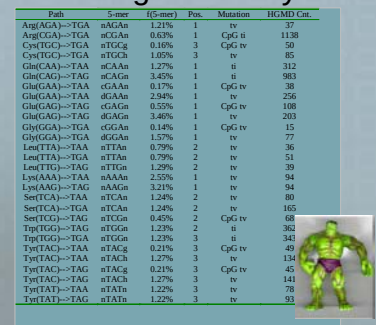
NESCent

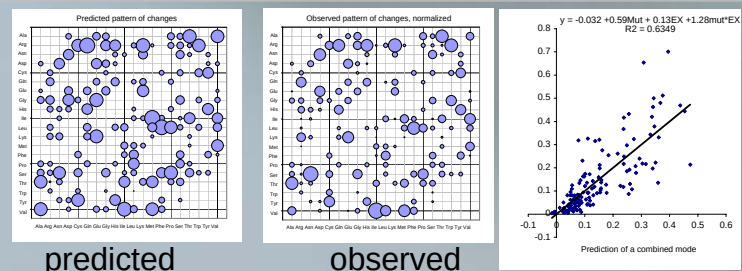
Evolution of introns and genes: analysis



Mutations and their effects: modeling and analysis

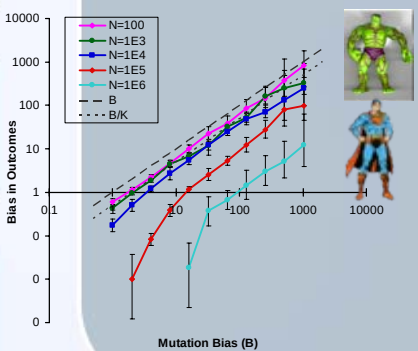


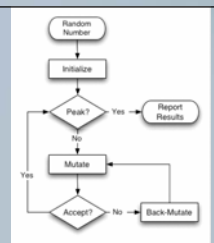


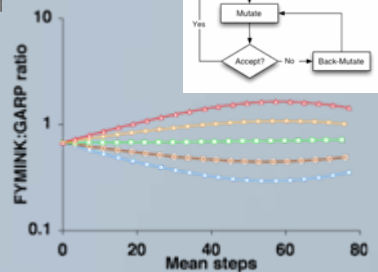


predicted observed

Evolutionary genetics: simulations





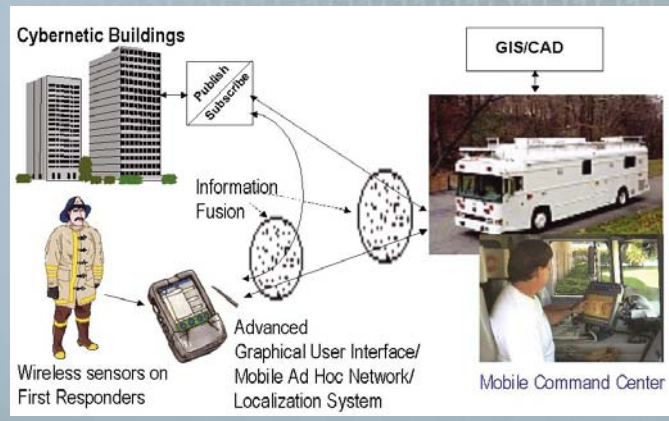


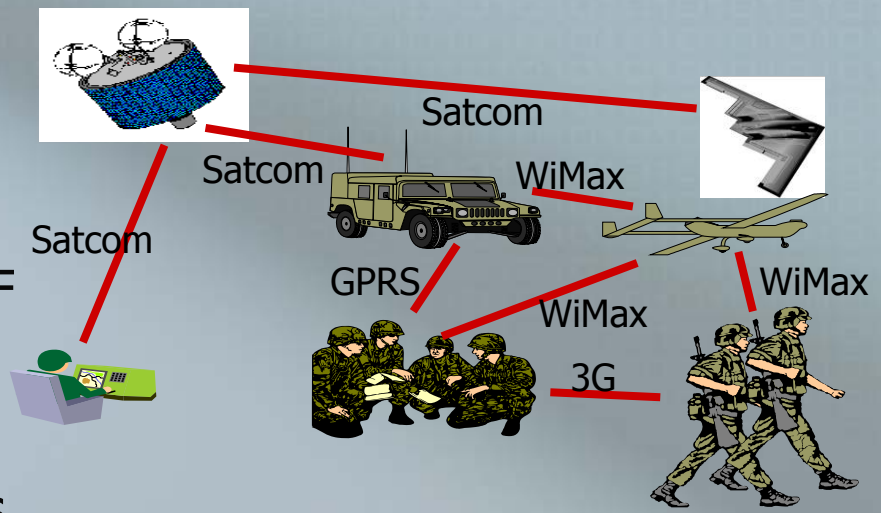
Pervasive Information Technology

- Radio Frequency Identification Standards and Interoperability (ITL, EEEL, BFRL)
- *Robust, Seamless and Secure Mobility* (ITL, BFRL, EEEL)
- Human Robot Interaction (ITL, MEL, BFRL)
- Public Safety Communication (ITL, BFRL)
- Smart Space (ITL)
- Test Methods and Standards for Next Generation Manufacturing Robotics (MEL)

Robust, Seamless and Secure Mobility

- Bridge the technological and measurement gap between stovepipe and heterogeneous access network technologies
- Develop novel analytical and simulation techniques in order to characterize the behaviours of network mobility protocols and assess their security characteristics
- Participate in standard developing organizations such as IEEE 802 and IETF in order to expedite the development of standards for mobility protocols
- Make tools and techniques available to the public





Trustworthy Networking

- *Quantum Communication* (PL, EEEL, ITL)
- Internet Infrastructure Protection (ITL)
  - DNSSEC (Domain Name System Security)
  - Network Routing
  - IPv6 (Internet Protocol, Version 6)
  - IPSec (Internet Protocol Security)
- Semiconductor Factory Floor Time Synchronization (EEEL)
- Standards And Test Methods For Industrial/Factory Floor Control Systems And Networks (MEL)
- Wireless Security Standards (ITL)
- Web Services Security (ITL)
- Mobile ad hoc Networks (MANET) Security (ITL)
- Medical Device Communication (ITL)

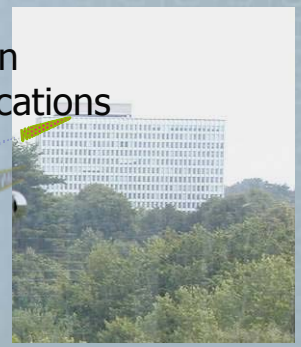
Broadband Quantum Key Distribution

NIST Quantum communications testbed investigates the limits of high-speed single-photon communication:

➔ *Quantum cryptography*
- → Provides verifiably secure cryptographic-key distribution
- → Want data rates compatible with modern telecommunications

➔ *High time resolution single-photon detection*

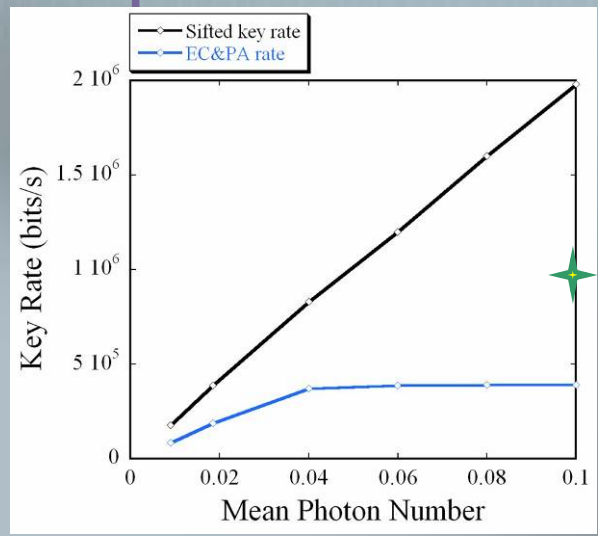
➔ *High rate sources of entangled photon pairs*



Quantum bits synchronized to a 1.25 Gbps free-space optical channel

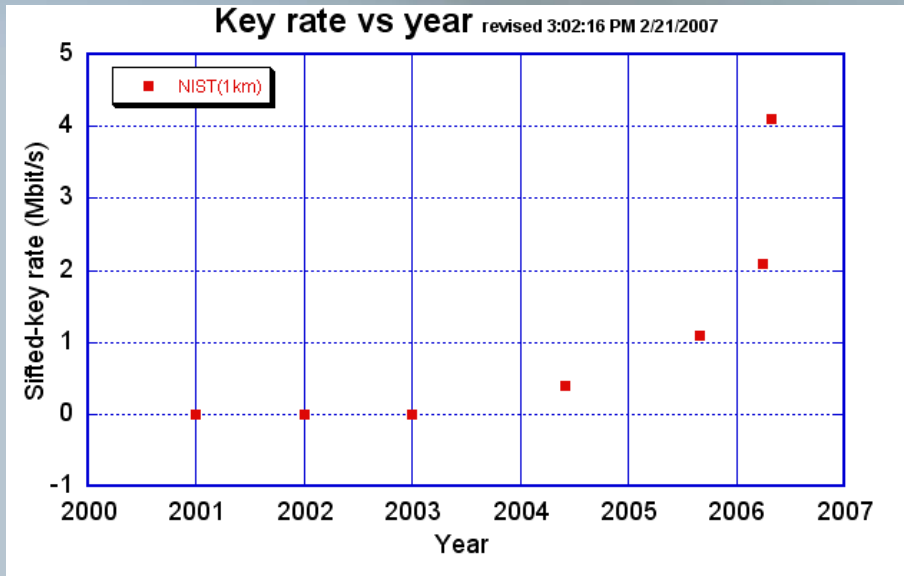
By adapting telecommunication techniques to quantum communications NIST has demonstrated free-space and fiber-based quantum cryptographic systems operating at GHz rates
-- Capable of quantum-encryption for streaming-video communications

Experimental Results



World Record for Sifted-Key Rate

- NIST high speed QKD system enables one-time pad encryption & decryption for video signals at 10 km fiber length
- ***This is the only complete system in the world that can perform such a demonstration***



05/2004, 0.4 Mbit/s (free space, 0.7 km, μ=0.1)
08/2005, 1.1 Mbit/s (fiber QKD, 1 km, μ=0.1)
03/2006, 2.1 Mbit/s (fiber QKD, 1 km, μ=0.1)
04/2006, 4.1 Mbit/s (fiber QKD, 1 km, μ=0.1)

Trustworthy Software

- Standards and Test Methods for Industrial/Factory Floor Control Systems and Networks (MEL, ITL)
- *Software Interoperability for Automotive Inventory Management* (MEL)
- Automatic Test Generation (ITL)
- Help America Vote Act (ITL)
- Health Information Technology (ITL)
  - Messaging Conformance
  - Telemedicine Standards
  - Cross-Enterprise Document Sharing
  - Electronic Health Record
- Software Assurance Tools/Test Methods (ITL)

Software Interoperability for Automotive Inventory Management

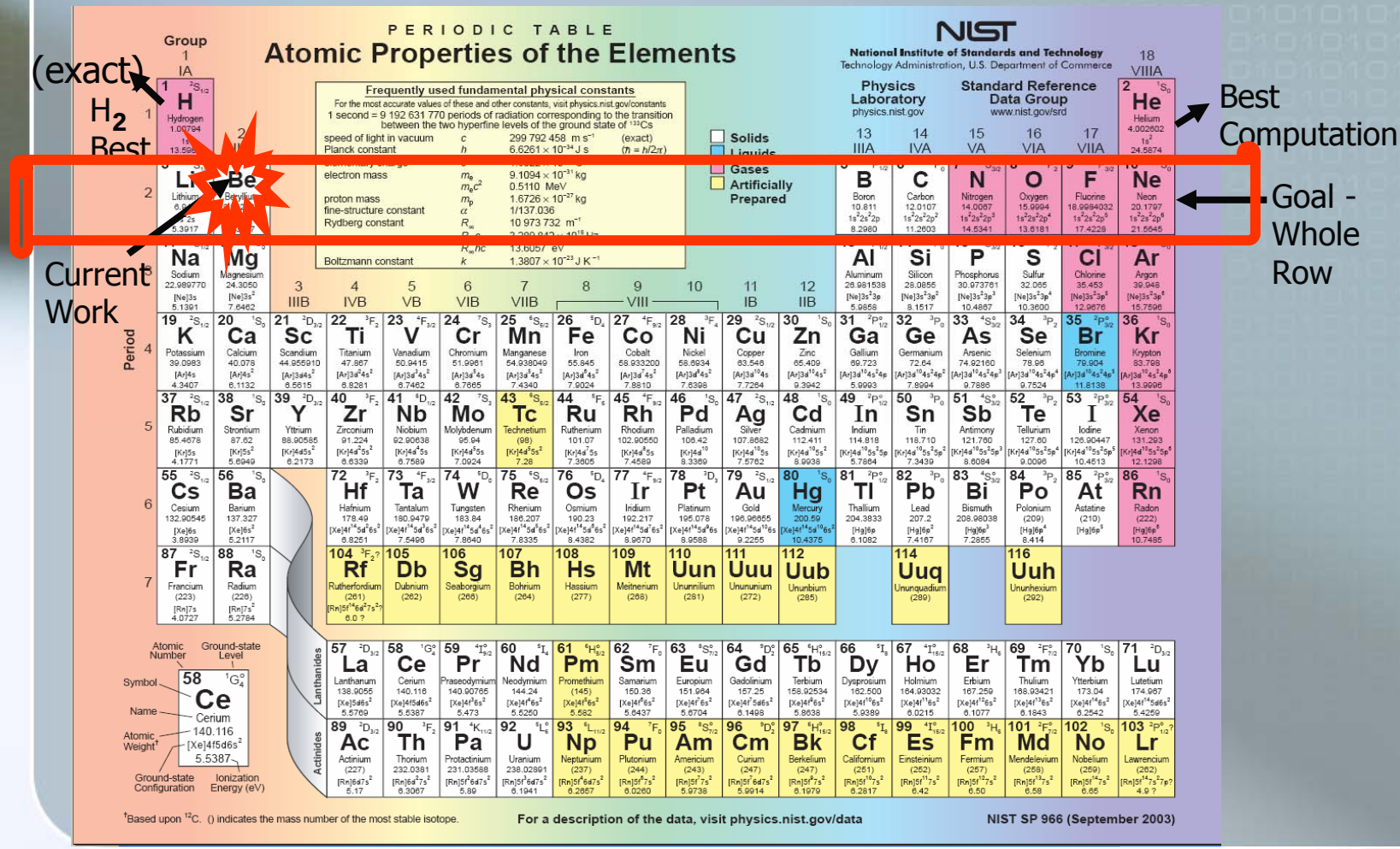
- Current inventory management is challenged by inaccurate forecasting, which results in costly inventory buffers, and dramatic inventory-level swings throughout entire supply chains
- Non-interoperability between different inventory visibility software products costs auto industry $255M annually
- Internet technologies can support near real-time material management, including planning, scheduling, inventory levels and shipping
- NIST developed standardized test methods and procedures to validate inventory management products in a neutral, objective environment, ensuring interoperability between software from different vendors

Virtual Measurement Systems

- *Very High Precision Measurements Of Atomic And Molecular Properties Through Computation* (ITL)
- Measurement Validation Systems for Forensic DNA Profiling (CSTL)
- *Tissue Engineering Metrology: Interactive Analysis of Scaffold Structure Using Immersive Visualization (MSEL, ITL)*
- Visualization Tools and Parallel Code for Nanotechnology and Nano-Optical Devices (PL)
- Model-based Manufacturing Validation Methods (MEL)
- Data Evaluation and Visualization Tools for Interlaboratory Studies (CSTL)
- Data Analysis and Visualization Environment (DAVE) - an integrated environment for the reduction, visualization and analysis of inelastic neutron scattering data (NCNR)

Very High Precision Measurements of Atomic and Molecular Properties Through Computation

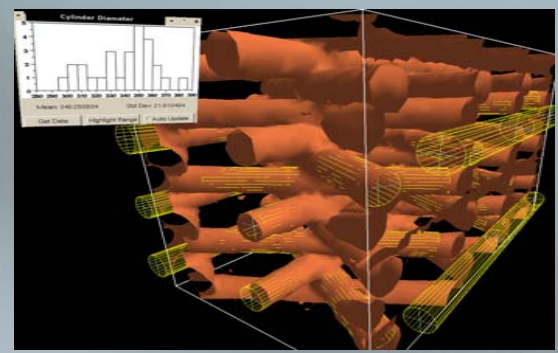
RESULTS: Most accurate computation of the ground state of dihydrogen (H_2) ever reached



Tissue Engineering Metrology

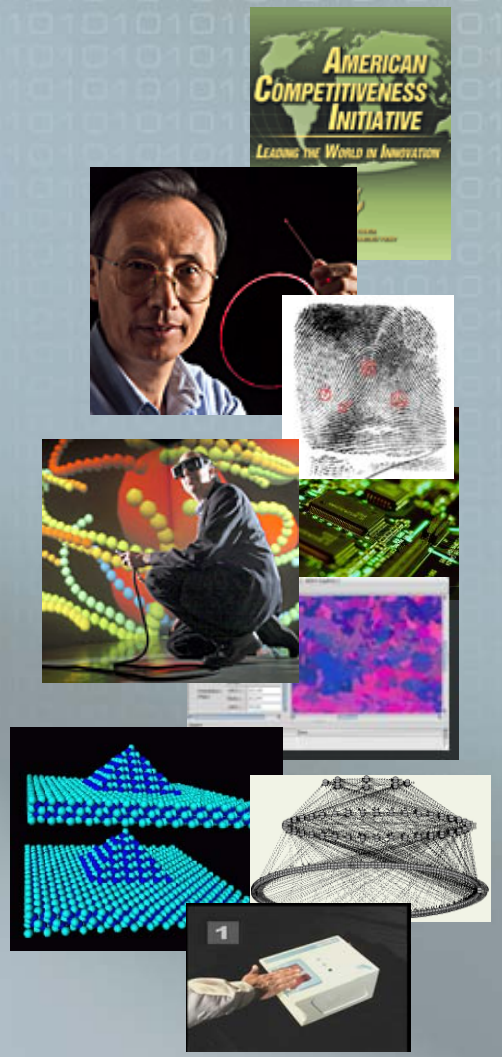
Interactive Analysis of Scaffold Structure Using Immersive Visualization

- Motivation
  - The tissue engineering scaffold structure affects the transport of nutrients and waste, which are properties critical to its success
  - Need for methods to simultaneously evaluate several structure descriptors
- Accomplishments
  - Immersive environment that allows users to evaluate locations and distributions of relevant features in tissue engineering scaffolds
  - Modular, expandable, can be automated
  - Software available to interactively compute, store, and recall scaffold metrics
  - Select histogram section to visually highlight the corresponding locations in the scaffold
- Impact
  - Sample scaffold descriptors such as strut width and aspect ratio can be quantified and analyzed



Building the IT Research Agenda at NIST

- Identifying critical U.S. IT measurement and standards research areas and potential impacts
- Advancements in IT measurements and standards are a key element in NIST's ability to respond to the ACI
  - IT research is a broad and rapidly changing area
  - Results of IT research are utilized in scientific endeavors
  - IT research is informed by scientific endeavors
  - IT research at NIST involves collaborations between all laboratories
- Focusing NIST efforts to address the intersection of critical areas and NIST's Core Competencies



Related Lab Tours

- *Using the Virtual World to Enable Spatially Separated Researchers to Perform Real-time Cooperative Analyses*
- *Quantum Computing With Trapped Ions*