

FY 2004 ITL Publications

Note that some documents are published in more than one place. Due to the large number of documents, publications listed in previous ITL Technical Accomplishment reports are not repeated.

Author	Title	Place of Publication	Date
--------	-------	----------------------	------

Ayers, R., Jansen, W.

PDA Forensic Tools

NISTIR

Digital handheld devices, such as Personal Digital Assistants (PDAs), are becoming more affordable and commonplace in the workplace. They provide highly mobile data storage in addition to computational and networking capabilities for managing appointments and contact information, reviewing documents, communicating via electronic mail, and performing other tasks. Individuals can store and process personal and sensitive information independently of a desktop or notebook computer, and optionally synchronize the results at some later time. As digital technology evolves, the capabilities of these devices also continues to improve rapidly, taking advantage of new forms of removable media, faster processors that consume less power, touch screens with higher pixel resolution, and other components designed specifically for mobile devices. When handheld devices are involved in a crime or other incident, forensic specialists require tools that allow the proper retrieval and speedy examination of information present on the device. This report gives an overview of current forensics software, designed for acquisition, analysis, reporting of data discovered on PDAs, and an understanding of their capabilities and limitations.

Balachandran, B., Gilsinn, D.

Nonlinear Oscillations of Milling

Mathematical and Computer
Modeling of Dynamical Systems

Principal features of two mathematical models that can be used to study nonlinear oscillations of a workpiece-tool system during a milling operation are presented and explained in this article. These models are nonlinear, nonhomogeneous, delay-differential systems with time-periodic coefficients. In the treatment presented here, the sources of nonlinearities are the multiple regenerative effect and the loss-of-contact effect. The time-delay effect is taken into account, and the dependence of this delay effect on the feed rate is modeled. A variable time delay is introduced to capture the feed-rate influence in one of the models. Two formulations that can be used to carry out stability analysis of periodic solutions are presented. The models presented and the stability-analysis formulations are relevant for predicting and understanding chatter in milling.

Author	Title	Place of Publication	Date
Barker, W.C., Howard, D., Grance, T., Eyuboglu, L.	Card Technology Developments and Gap Analysis Interagency Report	NISTIR 7056	
<p>This Card Technology Developments and Gap Analysis Interagency Report (IR) provides information regarding current technical capabilities and limitations, current user requirements for individual and integrated technologies, and major impediments to technology exploitation. The report also identifies existing standards governing card technologies. The report identifies gaps in standards coverage for card-based storage and processor technologies. The Card Technology Developments and Gap Analysis Interagency Report captures findings from a July 2003 NIST-sponsored Storage and Processor Card-Based Technologies Workshop, government and industry questionnaires, and feedback from government managers. It makes recommendations regarding policies, infrastructures, standards, and specifications and identifies issues associated with integrating multi-technology composition, security, and interoperability. The intended audience for this document includes federal government, private industry, and public sector interests responsible for developing and implementing storage and processor</p>			
Beichl, I., Bullock, S.S., Song, D.	A Quantum Algorithm Detecting Concentrated Maps	Mathematical Association of America (MAA) Monthly	
<p>We consider an arbitrary mapping for n, some number of quantum bits. Using n calls to a classical oracle evaluating f and an classical bit data store, it is possible to determine whether f is one-to-one. For some radian angle θ, we say f is θ-concentrated iff f for some fixed n and any θ. This manuscript presents a quantum algorithm that distinguishes a θ-concentrated f from a one-to-one f in n calls to a quantum oracle function f with high probability. For $\theta = \pi/4$, the quantum algorithm outperforms a classical analog on average, with maximal outperformance at $\pi/4$. Thus, the constructions generalize Deutsch's algorithm, in that quantum outperformance is robust for (slightly) nonconstant f.</p>			
Black, P.E., Lane, A.W.	Modeling Quantum Information	Quantum Information and Quantum Computing II, Defense and Security, SPIE, Orlando, Florida,	
<p>A simulator for quantum information systems cannot be both general, that is, easily used for every possible system, and efficient. Therefore, some systems will have aspects which can only be simulated by cunning modeling. On the other hand, a simulation may conveniently do extra-systemic processing that would be impractical in a real system. We illustrate with examples from our quantum computing simulator, QCSim. We model the [3,1] Hamming code in the presence of random bit flip or generalized amplitude damping noise, and calculate the expected result in one simulation run, as opposed to, say, a Monte Carlo simulation, and keep the original state to compute the chance of successful transmission, too. We also model the BB84 protocol with eavesdropping and random choice of basis and compute the chance of information received faithfully. Finally, we present our simulation of teleportation as an example of the trade-off between complexity of the simulation model and complexity of simulation inputs and as an example of modeling measurements and classical bits.</p>			

Author	Title	Place of Publication	Date
Brewer-Joneas, T.L.	Computer Security Division 2003 Annual Report	NISTIR	
<p>This report covers the work conducted within the National Institute of Standards and Technology's Computer Security Division during the Fiscal Year 2003. It discusses all projects and programs within the Division, staff highlights, and publications. For many years, the Computer Security Division (CSD) has made great contributions to help secure the nation's sensitive information and information systems. CSD's work has paralleled the evolution of information technology (IT), initially focused principally on mainframe computers, to now encompass today's wide gamut of information technology devices. CSD's important responsibilities were re-affirmed by Congress with passage of the Federal Information Security Management Act (FIMSA) of 2002 and the Cyber Security Research and Development Act of 2002. Beyond the role to serve the Federal Agencies under FISMA, CSD standards and guidelines are often voluntarily used by U.S. industry, global industry, and foreign governments as sources of information and direction for securing information systems. CSD's research also contributes to securing the nation's critical infrastructure systems. Moreover, the Division has an active role in both national and international</p>			
Brown, C.T., Bullen IV, H.W., Kelley, S.P., Xiao, R.K., Satterfield, S.G., Hagedorn, J.G., Devaney,	Visualization and Data Mining in an 3D Immersive Environment: Summer Project 2003	NISTIR 7067 and http://math.nist.gov/mcsd/savg/papers/index.html	10/31/2003
<p>We describe the application of some simple data-mining tools and visualization of the results in the NIST RAVE, an immersive 3D environment. The project builds upon several previous software development efforts, most notably the Glyph ToolBox, a set of tools used for creating three-dimensional glyphs. The visualizations consist of 3D and 2D representations of the data and of the data mining output combined in various layouts designed to aid ease of interpretation. These were in some cases equipped to allow user interactivity in the RAVE. We determined which methods were most and least effective in analyzing the data, providing examples for each, based on our experiences. We also describe the development of new capabilities for the Glyph</p>			
Buckley, C., Voorhees, E. M.	Retrieval Evaluation with Incomplete Information	Proceedings of the Twenty-Seventh Annual International ACM SIGIR Conference on Research and Development in Information Retrieval, Sheffield, UK, July 2004	
<p>This paper examines whether the Cranfield evaluation methodology is robust to gross violations of the completeness assumption (i.e., the assumption that all relevant documents within a test collection have been identified and are present in the collection). We show that current evaluation measures are not robust to substantially incomplete relevance judgments. A new measure is introduced that is both highly correlated with existing measures when complete judgments are available and more robust to incomplete judgment sets. This finding suggests that substantially larger or dynamic test collections built using current pooling practices should be viable laboratory tools, despite the fact that the relevance information will be incomplete and imperfect.</p>			

Author	Title	Place of Publication	Date
--------	-------	----------------------	------

Bullock, S.S.	Note on the Khaneja-Glaser Decomposition	Quantum Information and Computation, http://arXiv.org	
---------------	--	--	--

Recently, Vatan-Williams utilize a matrix decomposition of $SU(2n)$ introduced by Khaneja-Glaser to produce CNOT-efficient circuits for arbitrary three-qubit unitary evolutions. In this note, we place the Khaneja-Glaser decomposition in context as a $SU(2n) = KAK$ decomposition by proving that its Cartan involution is type AIII. The standard type AIII involution is the cosine-sine decomposition (CSD), a well-known decomposition among specialists in numerical linear algebra which may be computed using mature, stable numerical algorithms. In the course of our proof that the new decomposition is type AIII, we further establish the following. Khaneja and Glaser allowed for a particular degree of freedom, namely the choice of a commutative algebra \mathcal{A} , in their construction. Let U be a SWAP gate applied on lines 1, n . Then $U = k_1 U_1$; U_1 is a KGD for \mathcal{A} .

Bullock, S.S., Brennen, G.K.	Two Qubit Quantum Logic Circuits with Measurement Gates	Proceedings of the Design Automation Conference 2004, San Diego, California, June 7-11, 2004	
------------------------------	---	--	--

A physical process on an n -qubit state is any sequence of unitary evolutions (quantum computations) and measurements. Measurements change pure quantum states encoded by state vectors $|\psi\rangle$ into probability densities spread across multiple pure states. These densities may be encoded by Hermitian density matrices ρ . We define a gate library which includes a unitary-universal gate library and also variable sensitivity one-qubit measurements. Using this library, we describe an algorithm for quantum logic synthesis of certain physical processes (stochastic superoperators) in two-qubits. The logic circuits input stochastic data in the form of some ρ and contain one-qubit-measurement gates. The logic circuit then realizes a given stochastic superoperator $\mathcal{S}(\rho) = \sum_i g_i \rho g_i^\dagger$ for g an invertible positive 4×4 complex matrix, with probability $\text{Tr}(g \rho g^\dagger)$. (Every physical process realizing $\mathcal{S}(\rho) = \sum_i g_i \rho g_i^\dagger$ does so with this probability, although the other outcomes and their probabilities may differ.) The circuit diagram uses at most 39 gates containing 3 one-qubit measurements, versus lower bounds of 32 gates and 2

Author	Title	Place of Publication	Date
Bullock, S.S., Brennen, G.K.	Characterizing the Entangling Capacity of n-qubit Computations	Proceedings of the SPIE, SPIE Defense & Security Symposium, Orlando, Florida, April 13-15, 2004	4/13/2004

The state space of n quantum bits of data is exponentially large, having dimension 2^n . The (pure) local states correspond to each individual quantum bit being in an isolated one-qubit state, i.e., those which are tensor products, form a much smaller orbit of linear dimension within the state space. Hence most states are non-local, or entangled. The concurrence function on quantum data states is one measure of entanglement, intuitively capturing an exponentially small fraction of the phenomenon. This paper reports numerical tests of how concurrence changes as one applies a quantum computation to a pure n quantum-bit data state. We make strong use of a mathematical tool for factoring into subcomputations, namely the CCD matrix decomposition. The concurrence dynamics of a computation are in a certain sense localized to the 2^n factor, and so our actual numerics concentrate of 2^n . This is a great simplification, since an arbitrary unitary evolution may vary over 2^{2^n} real degrees of freedom, while the 2^n of the appropriate form for the CCD matrix decomposition may vary over 2^n or as 2^n .

Bullock, S.S., Brennen, G.K., O'Leary, D.P.	Time Reversal and n-qubit Canonical Decompositions	Communications in Mathematical Physics and http://arXiv.org
---	--	--

The n -qubit concurrence canonical decomposition (CCD) is a generalization of the two-qubit canonical decomposition $SU(4)=[SU(2) \otimes SU(2)] \otimes [SU(2) \otimes SU(2)]$, where \otimes is the commutative group which phases the maximally entangled Bell basis. A prequel manuscript creates the CCD as a particular example of the $G=KAK$ metadecomposition theorem of Lie theory. We hence denote it by $SU(2n)=KAK$. If $C_n(|\psi\rangle)=|\langle \psi^* | (-i\sigma_y) \otimes \dots \otimes (-i\sigma_y) | \psi \rangle|$ is the concurrence entanglement monotone, then computations in the K group are symmetries of a related bilinear form and so do not change the concurrence. Hence for a quantum computation $v=k_1 a k_2$, analysis of a in $e A$ allows one to study one aspect of the entanglement dynamics of the evolution v , i.e. the concurrence dynamics. Note that analysis of such an a in $e A$ is simpler than the generic case, since A is a commutative group whose dimension is exponentially less than that of $SU(N)$. In this manuscript, we accomplish three main goals. First, we expand upon the treatment of the odd-qubit case of the sequel, in that we (i) present an algorithm to compute the CCD in case $n=2p-1$ and (ii) characterize the maximal odd-qubit concurrence capacity in terms of convex hulls. Second, we interpret the CCD in terms of a time-reversal symmetry operator, namely the quantum bit flip $|\psi\rangle \otimes \dots \otimes (-i\sigma_y) \otimes \dots \otimes (-i\sigma_y) | \psi^* \rangle$. In this context, the CCD allows one to write any unitary evolution as a two-term product of a time-reversal symmetric and anti-symmetric evolution; no Trotterization is required. Finally, we use these constructions to study time-reversal symmetric Hamiltonians. In particular, we show that any $|\psi\rangle$ in the ground state of such an H must either develop a Kramer's degeneracy or be maximally entangled in the sense that $C_n(|\psi\rangle)=1$. Many time-reversal symmetric Hamiltonians are known to be nondegenerate and so produce maximally concurrent ground states.

Thursday, April 22, 2004

Author	Title	Place of Publication	Date
Burns, T.J., Davies, M.A., Rhorer, R.L., Yoon, H.W., Fields, R.J., Levine, L.E., Whitenton, E.P., Kennedy, M.D., Ivester, R.	Influence of Heating Rate on Flow Stress in High-Speed Machining	Proceedings of 7th CIRP International Workshop on Modeling of Machining that will be held at the ENSAM, Cluny, France, May 5-6,	

For several decades, a major focus of machining research has been the measurement and prediction of temperature. Here, the influence of the rate of heating on the flow stress, and the implications of this for finite-element modeling of high speed metal-cutting processes, will be discussed. First, for a range of chip thicknesses, a description will be given of some infrared microscopic measurements, performed at NIST, of the temperature field at the tool-chip interface during steady-state orthogonal machining of AISI 1045 steel. Next, some unsuccessful attempts to predict these thermal fields using commercial finite-element software will be discussed. Following this, results will be presented of some recent NIST research using a split-Hopkinson (Kolsky) bar with a rapid preheating capability. This work implies that, in AISI 1045 steel and related mild steels of interest in manufacturing, the thermal-softening effect during high-speed machining is significantly smaller than predicted by current constitutive response models. Finally, it will be shown that improved finite-element predictions of the maximum

Campbell, J.P., Nakasone, H., Cieri, C., Miller, D., Walker, K., Martin, A.F., Przybocki, M.A.	The MMSR Bilingual and Crosschannel Corpora for Speaker Recognition Research and Evaluation	Proceedings of Odyssey 2004, The Speaker and Language Recognition Workshop, Toledo, Spain, May 31-June 3, 2004	
--	---	--	--

We describe efforts to create corpora to support and evaluate systems that meet the challenge of speaker recognition in the face of both channel and language variation. In addition to addressing ongoing evaluation of speaker recognition systems, these corpora are aimed at the bilingual and crosschannel dimensions. We report on specific data collection efforts at the Linguistic Data Consortium, the 2004 speaker recognition evaluation program organized by the National Institute of Standards and Technology (NIST), and the research ongoing at the US Federal Bureau of Investigation and MIT Lincoln Laboratory. We cover the design and requirements, the collections and evaluation integrating discussions of the data preparation, research, technology

Carson, M., Santay, D.	Micro-Time-Scale Network Measurements and Harmonic Effects	PAM 2004 – The 5th Passive and Active Measurement Workshop	
------------------------	--	--	--

As network transmission speeds increase, packet streams increasingly uncover fine details of the interior behavior of router hardware and software. This behavior reveals itself as a set of harmonic effects, as interior clocks periodically interrupt packet forwarding, and interior queues periodically empty and fill. We examine this behavior with a Linux-based router employing a variety of gigabit Ethernet interfaces, with a view toward two goals: the creation of harmonic models of router forwarding performance which are accurate and yet mathematically simple and fast; and the analysis of the potential for an undesirable succession of positively reinforcing router "reverberations."

Author	Title	Place of Publication	Date
Chevrollier, N., Van Dyck, R.E.	Packet Filtering for Aggregate-based Congestion Control	Proceedings for Conference on Information Sciences and Systems (CISS 2004), Princeton, New Jersey, March 17-19, 2004	3/17/2004

We provide a short overview of the problem of congestion control in IP networks, including a discussion of some related work in countering denial-of-service attacks and packet classification. Then, we propose an adaptive packet filtering method for achieving aggregate-based congestion control. The method emphasizes approaches based on unsupervised learning, in combination with congestion detection. Initial simulation results suggest substantial improvements can sometimes be obtained.

Coakley, K.J., McKinsey, D.N.	Neutrino and Dark Matter Detection With CLEAN	Physics Letters B
-------------------------------	---	-------------------

This article describes CLEAN, an approach to the detection of low energy solar neutrinos, weakly interacting massive particles (WIMPs), and neutrinos released from supernovas. The CLEAN concept is based on the detection of elastic scattering events (neutrino-electron scattering, neutrino-nuclear scattering, and WIMP-nuclear scattering) in liquefied noble gases, such as liquid helium, liquid neon, and liquid xenon, all of which scintillate brightly in the ultraviolet. Key to the CLEAN technique is the use of a thin film of wavelength shifting fluor to convert the ultraviolet scintillation light to the visible. This allows the same liquid to be used as both passive shielding medium and active self-shielding detector, allowing lower intrinsic radioactive backgrounds at low energies. Liquid neon is a particularly promising medium for CLEAN. Because liquid neon has a high scintillation yield, has no long-lived radioactive isotopes, and can be easily purified using cold traps, it is an ideal medium for the detection of rare nuclear events. In addition, neon is inexpensive, dense, and transparent to its own scintillation light, making it practical for use in a large self-shielding apparatus. If liquid neon is used in CLEAN, the center of the full-sized detector would be a stainless steel tank holding approximately 135 metric tons of liquid neon. Inside the tank and suspended in the liquid neon would be several thousand photomultipliers. Monte Carlo simulations of gamma ray backgrounds have been performed assuming liquid neon as both shielding and detection medium. Gamma ray events occur with high probability in the outer parts of the detector. In contrast, neutrino and WIMP scattering events occur uniformly throughout the detector. We discriminate background gamma ray events from events of interest based on a spatial maximum likelihood method estimate of event location. Background estimates for CLEAN are presented, as well as an evaluation of the sensitivity of the detector for p-p neutrinos and WIMPs. Backgrounds and WIMP sensitivity are also determined for a possible 1-tonne prototype, filled with either liquid neon or liquid xenon. Given these simulations, the physics potential of the CLEAN approach is evaluated.

Della Torre, E., Yanik, L., Yarimbayik, A.E., Donahue, M.J.	A Differential Equation Accommodation Model	IEEE Transactions on Magnetics
--	---	--------------------------------

In this paper, we use the differential equation method of computing the accommodation magnetization in a modified Preisach model. The properties of this model are presented for a Gaussian medium. We show that the resulting model had neither the congruency property nor the deletion property.

Author	Title	Place of Publication	Date
--------	-------	----------------------	------

Devaney, J.E., Satterfield, S.G.,
Hagedorn, J.G.

Science at the Speed of Thought

Workshop On Ambient Intelligence
for Scientific Discovery, Vienna,
Austria, April 24-29, 2004

In this paper, we describe a flexible environment that combines scientific data mining with parallel computing in an immersive visualization environment. The goal is to minimize the time between the generation of a scientific hypothesis and the test of that idea, or science at the speed of thought.

Drury, J., Scholtz, J.

Evaluating Inter-Organizational
Information Systems

Book chapter submitted for the
book titled, "Inter-Organizational
Information Systems in the Internet
Age," Sean B. Eom, Editor

This chapter describes different means of evaluating the usability and suitability of computer-based inter-organizational information systems (IOISs). It describes why doing so is important yet difficult, and provides an assessment of the advantages and disadvantages of the major types of evaluation. It presents a case study focusing on determining whether an application provides the necessary insight into other collaborators' identities, presence, and activities while keeping sensitive

Dworkin, M.J.

Recommendation for Block Cipher
Modes of Operation: The CCM Mode for
Authentication and Confidentiality

NIST SP 800-38C

This Recommendation defines a mode of operation, called CCM, for a symmetric key block cipher algorithm. CCM may be used to provide assurance of the confidentiality and the authenticity of computer data by combining the techniques of the Counter (CTR) mode and the Cipher Block Chaining-Message Authentication Code (CBC-MAC) algorithm.

Ellison, C.M., Polk, W.T., Hastings,
N.E., Smith, S. W.

2nd Annual PKI Research Workshop
Proceedings

NISTIR 7085

NIST hosted the second annual Public Key Infrastructure (PKI) Research Workshop on April 28-29, 2003. The two-day event brought together PKI experts from academia, industry, and government to explore the remaining challenges in deploying public key authentication and authorization technologies, and to develop a research agenda to address those outstanding issues. This proceedings includes the refereed papers, and captures the essence of the panels and interaction at the workshop. The workshop consisted of the presentation of 11 referred papers, three panel discussions, a work-in-progress session and a birds-of-a-feather session. Participants included presenters were from the United States, Canada, Brazil, Japan, Germany, Estonia, and Finland; making the workshop an international event. Based on participant feedback, the workshop provided the most up-to-date information on PKI research and deployment. Due to the success of this event, an expanded workshop is planned for 2004.

Author	Title	Place of Publication	Date
--------	-------	----------------------	------

Fanto, M.A.	Configuring SSL Web Servers and Clients to Use FIPS-Approved Cryptographic Algorithms	NISTIR 7058	
-------------	---	-------------	--

The Secure Sockets Layer (SSL) and Transport Layer Security (TLS) protocols provide a method for entity and message authentication, message integrity, and confidential (encrypted) communications between clients and servers on the Internet. This paper reviews the implementations of SSL in various web browser and web server products with respect to support for FIPS-approved cryptographic algorithms. Where possible, the paper also provides a configuration guide to control each product to use only Federal Information Processing Standards (FIPS) based cipher suites. Products were selected for testing based exclusively on market penetration. Tested products included: the Apache web server, the Microsoft IIS web server, Internet Explorer, and Netscape Navigator. Of the servers tested, Apache was found to have the most flexibility in the configuration of cipher suites, while Netscape and Mozilla provided the most configuration options on the client side.

Fenimore, C.P., Nikolaev, A.I.	Assessment of Resolution and Dynamic Range for Digital Cinema	Image and Video Communications and Processing 2003, SPIE Volume 5022	
--------------------------------	---	--	--

The proponents of digital cinema seek picture quality exceeding that of the best film-based presentation. Quantifying the performance of systems for the presentation of high quality imagery presents several challenges. One is the dynamic range and the resolution may not be simply related to the nominal characteristics of bit-depth and pixel counts. We review some of the measurement methods that have been applied to determining these characteristics. One of the presumed advantages of high bit depth systems is to reduce the visibility of image banding. Non-uniformity of the display can be compensated in test pattern design to enable the measurement of banding contrast. The subjective assessment of banding is compared to a contrast-weighted model of just noticeable image differences. Applied to a class of image banding test patterns, the metric relates dynamic range to contouring. The model produces an estimate of the visibility threshold for image contouring in a 10-bit system, superior to a simple Weber model. These measurement issues will continue to be challenges as d-cinema systems

Fong, J.T.	From Kane to World Trade Center: A 40-Year Journey in Computational Mechanics and Applied Physics	Analytical Dynamics & Applied Mechanics – Anniversary Volume in Honor of Prof. T.R. Kane	
------------	---	--	--

In this essay, I will relate a 40-year journey from the day I took Prof. Kane's course in "Analytical Dynamics" in October 1963 at Stanford, to a dinner I had on September 2, 2003 with Prof. and Mrs. Kane, Prof. and Mrs. Charles Steele, and Prof. Ingram Olkin, all of Stanford University. Along the way, I recall many lessons I learned from Prof. Kane, for which I am very grateful. This essay is dedicated to him on this 80th birthday.

Author	Title	Place of Publication	Date
Garcia, R.E., Carter, W.C., Langer, S.A.	The Effect of Texture on the Macroscopic Properties of Polycrystalline Piezoelectrics: Application to Barium Titanate and	Journal of the American Ceramics Society	
<p>The effects of crystallographic texture and grain size microstructure are analyzed for polycrystalline tetragonal Barium Titanate, pseudotetragonal PZN-PT, and cubic Barium Titanate. For tetragonal Barium Titanate and pseudotetragonal PZN-PT, we demonstrate that a high anisotropy of the single-crystal properties induces an apparent enhancement in the macroscopic piezoelectric response. For tetragonal Barium Titanate, the macroscopic, predicted value of d_{31} and d_{33} is enhanced with respect to its single-crystal response at the expense of the spatial contributions from d_{15}. An optimal response is predicted for samples that are not perfectly textured in a particular orientation. Similarly, an apparent enhancement in d_{15} is predicted for PZN-PT. For cubic Barium Titanate, the low anisotropy of the underlying crystal structure induces a uniform decrease of the macroscopic electrostrictive constant, Q_{11}, with decreasing texture. A completely random polycrystal provides 0.85 ± 0.05</p>			
Garcia, R.E., Carter, W.C., Langer, S.A.	Finite Element Implementation of a Thermodynamic Description of Piezoelectric Microstructures	Accepted by Journal of the American Ceramics Society	
<p>A model and numerical framework is developed for piezoelectric materials. The model treats the piezoelectric and electrostrictive effects by incorporating orientation-dependent, single-crystal properties. The method is implemented in OOF, a public domain finite element code, so it can be applied to arbitrary two-dimensional microstructures with crystallographic anisotropy. The model is validated against analytic solutions. Consistency of the method for known cases permits application of the technique to more complicated two-dimensional systems. The piezoelectric and electrostrictive response is determined for a few simple device geometries and provides insight for design and convergence criteria.</p>			
Garcia, R.E., Reid, A.C.E., Langer, S.A., Carter, W.C.	Microstructural Modeling of Multifunctional Material Properties: The	Continuum Scale Simulation of Engineering Materials	
<p>Recent advances in and applications of the public domain Object Oriented Finite Element software for Materials Science (OOF) are discussed. The OOF software calculates the macroscopic properties from two-dimensional microstructures. It operates directly from microstructural image data to create a computational model that has the same spatial properties as the two-dimensional material microstructure. Recent progress in the code couples applied continuum thermal, electrostatic, elastic and chemical potential fields. We illustrate the application of the software by computing the macroscopic properties of polycrystalline piezoelectrics. We also demonstrate the effect of microstructure on the response of a porous cathode in a rechargeable lithium ion battery, and calculate the resulting chemically induced (Vegard) stresses. We also discuss the new release of this code, OOF2, which allows the user to simulate nearly arbitrary sets of applied fields and nearly arbitrary material</p>			

Author	Title	Place of Publication	Date
Garofolo, J.S., Laprun, C.D., Michel, M., Stanford, V.M., Tabassi,	The NIST Meeting Room Pilot Corpus	2004 International Language Resources and Evaluation Conference (LREC), Lisbon, Portugal, May 26-28, 2004, http://www.lrec-conf.org/lrec2004	

One of the next big challenges in Automatic Speech Recognition (ASR) is the transcription of speech in meetings. This task is particularly problematic for current recognition technologies because, in most realistic meeting scenarios, the vocabularies are unconstrained, the speech is spontaneous and often overlapping, and the microphones are inconspicuously placed. To support the development of meeting recognition technologies by both the speech recognition and video extraction research communities, NIST is providing a development and evaluation infrastructure including: a multi-media corpus of audio and video from meetings collected at NIST using a variety of microphones and video cameras, new evaluation protocols, metrics, software, rich transcription conventions, sponsoring evaluations and workshops, facilitating multi-site data pooling, and helping bring the community together to focus on the technical challenges. To date, NIST has collected a pilot corpus of 15 hours of meetings in its specially-instrumented Meeting Data Collection Laboratory. The corpus includes digital recordings from close-talking mics, lapel mics, distantly-placed mics, 5 digitally-recorded camera views, and full speaker/word-level transcripts. This data is being used in the development and evaluation of speech technologies and by the video extraction community under the auspices of the Advanced Research and Development Activity (ARDA) Video Analysis and Content Exploitation (VACE) program.

Gavrila, S., Fong, E.	Forensic Software Testing Support Tools: Test Summary Report	NISTIR	
-----------------------	---	--------	--

The Computer Forensic Tool Testing (CFTT) project at the National Institute of Standards and Technology (NIST), an agency of the United States Department of Commerce, provides a measure of confidence in the software tools used in computer forensic investigation. CFTT focuses on a class of tools called disk-imaging tools that copy or "image" hard disk drives. Forensic Software Testing Support Tools (FS-TST) is a software package that supports the testing of disk imaging tools. FS-TST includes 15 tools that perform hard disk initialization, faulty disk simulation, hard disk comparisons, extraction of information from the hard disk, and copying of disk or disk partitions. This NIST Interagency/Internal Report consists of two parts. Part A, which is this document, covers the planning, design and specification of testing tools included in the FS-TST package. Part B, which is a companion document, covers the test summary report. The testing was independently performed by VDG, Inc. under contract to

Author	Title	Place of Publication	Date
Gavrila, S., Fong, E.	Forensic Software Testing Support Tools. Test Plan, Test Design Specification, Test Case Specification	NISTIR	
<p>The Computer Forensic Tool Testing (CFTT) project at the National Institute of Standards and Technology (NIST), an agency of the United States Department of Commerce, provides a measure of confidence in the software tools used in computer forensic investigation. CFTT focuses on a class of tools called disk-imaging tools that copy or "image" hard disk drives. Forensic Software Testing Support Tools (FS-TST) is a software package that supports the testing of disk imaging tools. FS-TST includes 15 tools that perform hard disk initialization, faulty disk simulation, hard disk comparisons, extraction of information from the hard disk, and copying of disk or disk partitions. This NIST Interagency/Internal Report consists of two parts. Part A, which is this document, covers the planning, design and specification of testing tools included in the FS-TST package. Part B, which is a companion document, covers the test summary report. The testing was independently performed by VDG, Inc. under contract to</p>			
Gentile, C., Klein-Berndt, L.	Robust Location Using System Dynamics and Motion Constraints	IEEE International Conference on Communication 2004	
<p>To our knowledge, the indoor location system which currently achieves the best performance using inexpensive off-the-shelf equipment locates a mobile within 1.5 meters with probability 77 percent in hallways. Even while maintaining this accuracy, the system often reports logical errors such as the mobile in the wrong cubicle of an office or even on the wrong side of a wall when broadening the domain of application to within rooms. We propose an extension of the work using the same Markov localization framework, however incorporating system dynamics (necessitating no post-processing of the output) and motion constraints which implicitly encode the physical properties of the survey area. Our system retains the advantages of its predecessor of low cost, wireless LAN connectivity and security and large-scale deployment, however extending the survey area from simple hallways to the whole office environment, while maintaining the same precision without logical errors.</p>			
George, W.L., Hagedorn, J.G., Devaney, J.E.	Parallel Programming with Interoperable MPI	Dr. Dobbs Journal, February 1, 2004, pp. 49-53, and NISTIR 7066	12/1/2003
<p>This paper describes the purpose and use of the Interoperable Message Passing Interface (IMPI) protocols. These protocols, when implemented within MPI (Message Passing Interface) libraries, allow the processors of multiple parallel machines to act as a single large parallel machine when running parallel programs that use the MPI (Message Passing Interface) library for</p>			

Author	Title	Place of Publication	Date
Gharavi, H., Ban, K.	Dynamic Adjustment Packet Control for Video Communications over Ad-hoc Networks	IEEE International Conference on Communications (ICC 2004)	

This paper is concerned with transporting video information via multihop mobile ad-hoc channels. The major problem with transmitting real-time video information over these channels is the issue of link reliability. To improve the quality of the video reception we propose a cross layer feedback control mechanism that can allow the application layer to adapt itself to a dynamically changing network topology. We also present packet transmission strategies capable of recovering video signals under long bursts of packet drops, typical of a route change condition. This feedback control scheme has been developed for transmission of RTP/UDP/IP packets using the emerging H.264/AVC video-coding standard.

Gharavi, H., Ban, K., Cambiotis, J.	RTCP-Based Frame-Synchronized Feedback Control for IP-Video Communications over Multipath Fading Channels	IEEE International Conference on Communications (ICC 2004)	
-------------------------------------	---	--	--

This paper presents a packet-loss feedback tracking scheme for the transmission of video signals over mobile channels. The proposed feedback scheme is based on the real time transport control protocol (RTCP), which is designed to provide an end-to-end feedback assessment of transmitted packets on a frame-by-frame basis (video frame). In addition, the frame synchronized RTCP-based feedback scheme is designed to take care of losses of RTCP packets due to bad channels. The video encoder, upon receiving its feedback report, can identify the exact location of the missing packets in the transmitted video frame. The feedback scheme is then applied to transport H.264/RTP/UDP/IP packets in real-time. A packet-loss compensation strategy has been used to assess the quality of the received signal under multipath fading channel conditions.

Author	Title	Place of Publication	Date
Gilsinn, D.E., McClain, M.A., Witzgall, C.J.	Using Nonoscillatory Splines to Model Urban Environments	Proceedings, 2003 SIAM Conference on Geometric Design and Computing, Seattle, Washington, November 10-13, 2003	11/10/2003

In this paper we propose an approach to modeling potentially unstructured point sets representing objects with surface discontinuities, such as sharp edges. Such data are obtained, for instance, by LADAR scans of urban scenes. Commonly used methods, such as multivariate splines or differentiable finite elements, produce unwanted oscillations along sharp edges. Those methods are defined by minimizing functionals that are energy related integrals of quadratic forms. A new paradigm for nonoscillatory splines, introduced by J. E. Lavery, replaces such quadratic forms by sums of absolute values. In our work, this approach is modified in order to reduce the heavy computational load of the Lavery algorithm and also to achieve planar rotational invariance. It involves an iterative approach minimizing a weighted sum of thin plate energies of finite elements, such as Hsieh-Clough-Tocher (rHCT) elements. The weights are the reciprocal square-roots of the thin plate energies, enabling elements with the high curvature required to produce sharp edges. Initial computational results are reported on rHCT elements,

Godil, A.	VISA: Video Segmentation and	Usability Professional's Association 2004 Conference
-----------	------------------------------	---

Screen video recording is a common component of usability testing. We have developed tools for reviewing and analyzing the video more efficiently. The tool: 1) breaks up a video into shorter segments and provides a compact pictorial summarization of the video; 2) provides a variety of ways for accessing video; 3) allows web-based reviews of video; and 4) provides a web-based way to post and view annotations of the video.

Godil, A., Ressler, S., Grother, P.	Face Recognition Using 3D Facial Shape and Color Map Information: Comparison and Combination	SPIE, Biometric Technology for Human Identification Conference
-------------------------------------	--	---

In this paper, we investigate the use of 3D surface geometry for face recognition and compare it to one based on color map information. The 3D surface and color map data are from the CAESAR anthropometric database. We find that the recognition performance is not very different between 3D surface and color map information using a principal component analysis algorithm. We also discuss the different techniques for the combination of the 3D surface and color map information for multi-modal recognition by using different fusion approaches and show that there is significant improvement in results. The effectiveness of various techniques is compared and evaluated on a dataset with 200 subjects in two different positions.

Author	Title	Place of Publication	Date
--------	-------	----------------------	------

Golmie, N., Chevrollier, N., Rebala,	Bluetooth and WLAN Coexistence: Challenges and Solutions	IEEE Wireless Communications Magazine, December 2003	
--------------------------------------	--	--	--

In this article we discuss solutions to the interference problem caused by the proximity and simultaneous operation of Bluetooth and WLAN networks. We consider different techniques that attempt to avoid time and frequency collisions of WLAN and Bluetooth transmissions. We conduct a comparative analysis of their respective performance and discuss the trends and trade-offs they bring for different applications and interference levels. Performance is measured in terms of packet loss, TCP

Golmie, N., Cypher, D., Rebala, O.	Performance Evaluation of Low Rate WPANS for Sensors and Medical Applications	Proceedings for International Workshop on Theoretical Aspects of Wireless Ad hoc, Sensor, and Peer to Peer Networks, Chicago, Illinois, June 11-12, 2004	
------------------------------------	---	--	--

In this article we consider the emerging low-rate Wireless Personal Area Network (WPAN) technology as specified in the IEEE 802.15.4 standard and evaluate its suitability for sensor and medical applications. The main objective for this effort is to develop a universal and interoperable interface for medical equipments. We focus on scalability issues and the need to support several communicating devices in a patient's hospital room. Given the nature and the diversity of the clinical environment, it is most likely that different medical applications will use different wireless technologies. We choose to quantify the performance of IEEE 802.15.4 devices in the presence of IEEE 802.11b devices since it may be the technology of choice for most web

Golmie, N., Cypher, D., Rebala, O.	Performance Analysis of Low Rate Wireless Technologies for Medical Applications	Proceedings for IEEE GLOBECOM 2004 Workshop, Dallas, Texas, November 29-December 3, 2004	
------------------------------------	---	--	--

In this article we discuss what wireless technologies can be used for medical applications and how well they perform in a healthcare/hospital environment. We consider the emerging low-rate Wireless Personal Area Network (WPAN) technology as specified in the IEEE 802.15.4 standard and evaluate its suitability to the medical environment. We focus on scalability issues and the need to support tens of communicating devices in a patient's hospital room. We evaluate the effect of packet segmentation and backoff parameters tuning to improve the overall network performance that is measured in terms of packet

Author	Title	Place of Publication	Date
Golmie, N., Cypher, D., Rebala, O.	Performance Analysis of Low Rate Wireless Technologies for Medical Applications	Mobile Networks and Applications Journal, 2004	
<p>In this article we discuss what wireless technologies can be used for medical applications and how well they perform in a healthcare/hospital environment. We consider the emerging low-rate Wireless Personal Area Network (WPAN) technology as specified in the IEEE 802.15.4 standard and evaluate its suitability to the medical environment. We focus on scalability issues and the need to support tens of communicating devices in a patient's hospital room. We evaluate the effect of packet segmentation and backoff parameter tuning to improve the overall network performance that is measured in terms of packet loss, goodput, and access delay. We also evaluate the performance of 802.15.4 devices under interference conditions caused by other 802.15.4 devices and by wireless local area networks using IEEE 802.11b.</p>			
Golmie, N., Van Dyck, R., Soltanian, A., Tonnerre, A., Rebala,	Interference Evaluation of Bluetooth and IEEE 802.11b Systems	ACM Wireless Networks 2003, Vol. 9, pp. 201–211	
<p>The emergence of several radio technologies, such as Bluetooth and IEEE 802.11, operating in the 2.4 GHz unlicensed ISM frequency band, may lead to signal interference and result in significant performance degradation when devices are collocated in the same environment. The main goal of this paper is to evaluate the effect of mutual interference on the performance of Bluetooth and IEEE 802.11b systems. We develop a simulation framework for modeling interference based on detailed MAC and PHY models. First, we use a simple simulation scenario to highlight the effects of parameters, such as transmission power, offered load, and traffic type. We then turn to more complex scenarios involving multiple Bluetooth piconets and WLAN</p>			
Grance, T., Hash, J., Stevens, M.	Security Considerations in the Information System Development Life	NIST SP 800-64, http://csrc.nist.gov/publications/nist_pubs/index.html	10/10/2003
<p>The need to provide protection for federal information systems has been present since computers were first used. Including security early in the acquisition process for an information system will usually result in less expensive and more effective security than adding it to an operational system once it has entered service. This guide presents a framework for incorporating security into all phases of the information system development life cycle (SDLC) process, from initiation to disposal. This document is a guide to help organizations select and acquire cost-effective security controls by explaining how to include information system security requirements in the SDLC. Five phases of a general SDLC are discussed in this guide and include the following phases: initiation, acquisition/development, implementation, operations/maintenance, and disposition. Each of these five phases includes a minimum set of security steps needed to effectively incorporate security into a system during its development. An organization will either use the general SDLC described in this document or will have developed a tailored SDLC that meets their specific needs. In either case, NIST recommends that organizations incorporate the associated IT security</p>			

Author	Title	Place of Publication	Date
Grance, T., Hash, J., Stevens, M., O'Neal, K., Bartol, N.	Guide to Information Technology Services: Recommendation of the National Institute of Standards and Technology	NIST SP 800-35, http://csrc.nist.gov/publications/nist_pubs/index.html	10/10/2003

Organizations frequently must evaluate and select a variety of information technology (IT) security services in order to maintain and improve their overall IT security program and enterprise architecture. IT security services, which range from security policy development to intrusion detection support, may be offered by an IT group internal to an organization, or by a growing group of vendors. It is difficult and challenging to determine service provider capabilities, measure service reliability and navigate the many complexities involved in security service agreements. This guide provides assistance with the selection, implementation, and management of IT security services by guiding organizations through the various phases of the IT security services life cycle. This life cycle provides a framework that enables the IT security decision makers to organize their IT security efforts from initiation to closeout. The factors to be considered when selecting, implementing, and managing IT security services include: the type of service arrangement; service provider qualifications, operational requirements and capabilities, experience, and viability; trustworthiness of service provider employees; and the service provider's capability to deliver adequate protection

Grance, T., Kent, K., Kim, B.	Computer Security Incident Handling Guide	NIST SP 800-61, http://csrc.nist.gov/publications/nist_pubs/index.html	1/15/2004
-------------------------------	--	--	-----------

NIST Special Publication 800-61, Computer Security Incident Handling Guide, assists organizations in mitigating the potential business impact of information security incidents by providing practical guidance on responding to a variety of incidents effectively and efficiently. Specifically, this document discusses the following items: 1) establishing a computer security incident response capability, including policy, procedure, and guideline creation; 2) selecting appropriate staff and building and maintaining their skills; 3) emphasizing the importance of incident detection and analysis throughout the organization; 4) maintaining situational awareness during large-scale incidents; and 5) handling incidents from initial preparation through the post-incident lessons learned phase, including specific advice on five common categories of incidents. While the guide is rather technical in nature, all guidance is independent of particular hardware platforms, operating systems, and applications.

Author	Title	Place of Publication	Date
Grance, T., Stevens, M., Myers, M.	Guide to Selecting IT Security Products	NIST SP 800-36, http://csrc.nist.gov/publications/nist-pubs/index.html	10/10/2003

The selection of IT security products is an integral part of the design, development and maintenance of an IT security infrastructure that ensures confidentiality, integrity, and availability of mission critical information. The guide seeks to assist in choosing IT security products that meet an organization's requirements. It should be used with other NIST publications to develop a comprehensive approach to meeting an organization's computer security and information assurance requirements. This guide defines broad security product categories, specifies product types within those categories, and then provides a list of characteristics and pertinent questions an organization should ask when selecting a product from within these categories.

Griffith, D.	The GMPLS Control Plane Architecture for Optical Networks	Chapter 1 of book entitled Optical WDM Networks, Past Lessons and Path Ahead, Kluwer Academic Publishers, 2004
--------------	---	--

Optical networking technology underwent a major revolution in the 1990s as the old paradigm of SONET/SDH systems to support circuit-switched connections began to give way to a new mesh network of transparent, high-speed optical switches with the capability to support a variety of higher-layer traffic types and services. In order for such a network to operate efficiently, it is essential that it employ a control plane that is capable of managing both legacy framed traffic and new traffic types. Also, the optical control plane must be able to operate across network boundaries, both at the edge interface to the customer's equipment and at administrative domain boundaries in the core network. The Internet Engineering Task Force (IETF) has tasked several working groups to develop the architecture for such a control plane as well as protocols to support its functioning. These groups' work has built on previous work in the IETF on Multi-Protocol Label Switching (MPLS), which was developed to allow packet routers to operate more efficiently. In this chapter, we describe the GMPLS architecture and related protocols,

Author	Title	Place of Publication	Date
Griffith, D., Sriram, K., Krivulina, L., Golmie, N.	Resource Planning and Bandwidth Allocation in Hybrid Fiber-Coax Residential Networks	Proceedings of BroadNets 2004, Broadband Optical/Wireless Networking Symposium, San Jose, California, October 25-29, 2004	

The introduction of new high bandwidth services such as video-on-demand by cable operators will put a strain on existing resources. It is important for cable operators to know how many resources to commit to the network to satisfy customer demands. In this paper, we develop models of voice and video traffic to determine the effect on demand growth on hybrid fiber-coax networks. We obtain a set of guidelines that network operators can use to build out their networks in response to increased demand. We begin with one type of traffic and generalize to an arbitrary number of high-bandwidth CBR-like services to obtain service blocking probabilities. These computations help us to determine how cable networks would function under various conditions (i.e., low, medium, and heavy loads). We also consider how the growth rate of the popularity of such services would change over time, and how this impacts network planning. Our findings will help cable operators estimate how much bandwidth they need to provision for a given traffic growth model and connection blocking requirement.

Griffith, D., Sriram, K., Lee, S., Golmie, N.	Restorability versus Efficiency in (1:1) _n Protection Schemes for Optical	Proceedings for 2004 International Conference on Communications (ICC 2004), Paris, France, June 20-24, 2004	
---	--	---	--

As network utilization continues to grow in the coming years, there will be increased pressure on network operators to use traffic engineering to provision resources more efficiently. One way to do this is to allow backup paths associated with disjoint working paths to share bandwidth. Increasing the amount of sharing will naturally increase the risk that a failed working path will either be unrecovered or forced to use dynamic recovery mechanisms. We examine the trade-offs between robustness and efficiency by developing theoretical models for (1:1)_n recovery schemes in order to develop lower and upper performance bounds. We confirm our results using simulations of uncorrelated failures in a wide-area optical network with various degrees of resource

Grother, P.J.	Face Recognition Vendor Test 2002 Supplemental Report	NISTIR 7083	
---------------	---	-------------	--

Further analyses of the systems tested in the Face Recognition Vendor Test 2002 are reported. These supplement those covered in the primary Evaluation Report of March 2003. Specifically this report is intended to appeal to a more specialized audience; it contains results on multi-sample and multi-vendor fusion, score normalization, performance on an ethnic subpopulation, and the effect on performance of image-specific quality metrics. The report also includes methods for

Author	Title	Place of Publication	Date
--------	-------	----------------------	------

Grother, P.J., Phillips, P.J.

Models of Large Population Recognition Performance

Conference on Computer Vision and Pattern Recognition 2004

We formulate new binomial models of both open- and closed-set identification recognition performance, giving explicit formulae for identification rates and false match rates as functions of database size, match rank and operating threshold. We compare these with previously published models and with empirical results from face recognition systems tested on populations of size 40000. In addition, we note that verification is a special case of open-set identification and relate area under the receiver operating characteristic to closed-set identification. We find the binomial model to be a good predictor of performance for low false match rates but that it underestimates identification rates on closed sets. We implicate the well known binomial iid assumption, but show a conditioning method, and a score transformation, that ameliorate this.

Harman, D., Buckley, C.

The NRRC Reliable Information Access (RIA) Workshop

Proceedings of the ACM Special Interest Group for Information Retrieval (SIGIR)

In the summer of 2003 NIST organized a 6-week workshop as part of the ARDA NRRC Summer Workshop series. The goal of this workshop (RIA) was to understand the contributions of both system variability factors and topic variability factors to overall retrieval variability. The workshop brought together seven different top research IR systems and set them to common tasks. Comparative analysis of these different systems enabled system variability factors to be isolated in a way that had never

Henrard, S.

Preliminary Instrumentation for the Efficient Use of Web-Based Electronic Health Records

Computer-Based Medical Systems 2004 Proceedings

NIST has devised preliminary elements (technical “hooks”) of a convenient logging method for Web-based electronic health record (EHR) dialogues. These can identify fields, record times spent at each (by whomever), and log a sequence of visits. The next step will be to refine this promising start, to begin building upon it a more polished and user-friendly system. We present our results to gain impressions from users of the worth of simple, open tools for tuning and improving e-record flows and their

Author	Title	Place of Publication	Date
Hunt, F. Y., Kearsley, A.J., O’Gallagher, A.	Constructing Sequence Alignments from a Markov Decision Model with Estimated Parameter Values	2003 Proceedings of the Biological Language Conference, Pittsburgh, Pennsylvania, Nov. 20-21, 2003, and Applied Bioinformatics	11/20/2003

Current methods for aligning biological sequences are based on dynamic programming algorithms. If large numbers of sequences or a number of long ones are to be aligned the required computations are expensive in memory and CPU time. In an attempt to bring the tools of large scale linear programming (LP) methods to bear on this problem, we formulate the alignment process as a controlled Markov chain and construct a suggested alignment based on policies that minimize the expected total

Hunt, F.Y.	Sample Path Optimality for a Markov Optimization Problem	Stochastic Analysis and
------------	---	-------------------------

We study a unichain Markov decision process, i.e., a controlled Markov process whose state process under a stationary policy is an ergodic Markov chain. Here the state and action spaces are assumed to be countable. When the state process is uniformly ergodic and the immediate cost is bounded then a policy that minimizes the long term expected average cost is one that almost surely produces an n stage sample path cost that is less than or equal to the nth stage cost of any other stationary policy as n

Hunt, F.Y., Kearsley, A.J., O’Gallagher, A.	A Tutorial on Multiple Sequence Alignment of Biological Sequences	Proceedings of the Sixth Conference for African American Researchers in the Mathematical Sciences, Princeton, New Jersey, June 16-18, 2002
--	--	--

In this paper, multiple sequence alignment is recast as an optimization problem using Markov decision theory. An objective or cost function is constructed whose critical points correspond to efficient alignments. A large collection of linear data-dependent constraints are constructed such that satisfaction of these constraints ensures that solution alignments obey statistical properties defined by a Markov decision model. In this setting, the problem can be posed as a linear programming problem which can be efficiently solved using modern numerical methods.

Author	Title	Place of Publication	Date
Indovina, M., Uludag, U., Snelick, R., Mink, A., Jain, A.	Multimodal Biometric Authentication Methods: A COTS Approach	Workshop on Multimodal User Authentication, Santa Barbara, California, December 11-12, 2003	12/11/2003

We examine the performance of multimodal biometric authentication systems using state-of-the-art Commercial Off-the-Shelf (COTS) fingerprint and face biometrics on a population approaching 1000 individuals. Prior studies of multimodal biometrics have been limited to relatively low accuracy non-COTS systems and populations approximately 10 percent of this size. Our work is the first to demonstrate that multimodal fingerprint and face biometric systems can achieve significant accuracy gains over either biometric alone, even when using already highly accurate COTS systems on a relatively large-scale population. In addition to examining well-known multimodal methods, we introduce novel methods of fusion and normalization that improve

Iyer, H.K., Wang, C.M.	Propagation of Uncertainties in Measurements using Structural	Metrologia
------------------------	---	------------

The ISO Guide to the Expression of Uncertainty in Measurement (GUM) recommends the use of a first-order Taylor series expansion for propagating errors and uncertainties. The GUM also permits the use of "Other analytical or numerical methods" when the conditions for using the Taylor expansion do not apply. In this paper, we propose an alternative approach for evaluating measurement uncertainty based on the concept of structural inference originally described by D.A.S. Fraser. We use three examples from the GUM to illustrate the implementation of the structural approach for the calculation of uncertainties in

Iyer, H.K., Wang, C.M., Vecchia,	Consistency Tests for Key Comparison Data	Metrologia
----------------------------------	---	------------

Results of International Key Comparisons of National Measurement Standards provide the technical basis for the Mutual Recognition Arrangement (MRA) formulated by Le Comite International des Poids et Mesures (CIPM). With many key comparisons already completed and a number of new key comparison experiments currently under way, we now have a better understanding of the statistical issues that need to be addressed for successfully analyzing key comparisons data and making proper interpretations of the results. There is clearly a need for a systematic approach for statistical analyses of key comparison data that can be routinely implemented by all participating laboratories. The determination of a key comparison reference value (KCRV) and its associated uncertainty, and the degrees of equivalence are the central tasks in the evaluation of key comparison data. A satisfactory definition of a KCRV, however, is based on the assumption that all laboratories are estimating the same unknown quantity of the common measurand. That is, the results from the different laboratories are mutually consistent. In this paper, we compare a number of statistical procedures for testing the consistency assumption.

Author	Title	Place of Publication	Date
--------	-------	----------------------	------

Jansen, W.A.	Authenticating Mobile Device Users Through Image Selection	Data Security 2004	
--------------	--	--------------------	--

Adequate user authentication is a persistent problem, particularly with mobile devices such as Personal Digital Assistants (PDAs), which tend to be highly personal and at the fringes of an organization's influence. Yet these devices are being used increasingly in military and government agencies, hospitals, and other business settings, where they pose a risk to security and privacy, not only from sensitive information they may contain, but also from the means they typically offer to access such information over wireless networks. User authentication is the first line of defence for a mobile device that falls into the hands of an unauthorized individual. However, motivating users to enable simple PIN or password mechanisms and periodically update their authentication information is difficult at best. This paper describes a general-purpose mechanism for authenticating users through image selection. The underlying rationale is that image recall is an easy and natural way for users to authenticate, removing a serious barrier to users' compliance with corporate policy. The approach described distinguishes itself from other attempts in this area in several ways, including style dependent image selection, password reuse, and embedded salting, which collectively overcome a number of problems in employing knowledge-based authentication on mobile devices.

Kacker, R., Datla, R., Parr, A.	Statistical Analysis of CIPM Key Comparisons Based on the ISO Guide	Metrologia	
---------------------------------	---	------------	--

An international Advisory Group on Uncertainties has published guidelines for the statistical analysis of a simple key comparison carried out by Consultative Committees of the International Committee for Weights and Measures (CIPM) where a traveling standard of stable value is circulated among the participants. We discuss several concerns with these guidelines. Then, we describe a statistical model based on the Guide to the Expression of Uncertainty in Measurement that gives reasonable expressions for the key comparison reference value, the degrees of equivalence, and their associated standard uncertainties. The proposed statistical model applies to all those CIPM key comparisons where the laboratory results are mutually comparable

Knill, E.H.	Scalable Quantum Computation in the Presence of Large Detected-Error	Physical Review A and http://www.arXiv.org	
-------------	--	---	--

The tolerable erasure error rate for scalable quantum computation is shown to be at least .293, given standard scalability assumptions. This bound is obtained by implementing computations with generic stabilizer code teleportation steps that combine the necessary operations with error-correction. An interesting consequence of the technique is that the only errors that affect the maximum tolerable error rate are storage and Bell measurement errors. If storage errors are negligible, then any detected Bell measurement error below 1/2 is permissible. Another consequence of the technique is that the maximum tolerable depolarizing error rate is dominated by Howell one can prepare the required encoded states. For example, if storage and Bell measurement errors are relatively small, then independent depolarizing errors with error rate close to .1 per qubit are tolerable in the prepared states. The implementation overhead is dominated by the efficiency with which the required encoded states can be prepared. At present, this efficiency is very low, particularly for error rates close to the maximum tolerable ones.

Author	Title	Place of Publication	Date
Knill, E.H.	Fault-Tolerant Postselected Quantum Computation: Threshold Analysis	http://arXiv.org/quant-ph	
<p>The schemes for fault-tolerant postselected quantum computation given in quant-ph/0402171 ("Fault-Tolerant Postselected Quantum Computation: Schemes") are analyzed to determine their error-tolerance. The analysis is based on computer-assisted heuristics. It suggests that if classical and quantum communication latencies are negligible, then scalable qubit-based quantum computation is possible with errors above 1 percent per elementary quantum gate.</p>			
Knill, E.H.	Fault-Tolerant Postselected Quantum Computation: Schemes	http://arXiv.org/PS_cache/quant-ph/pdf/0402/0402171.pdf	
<p>Postselected quantum computation is distinguished from regular quantum computation by accepting the output only if measurement outcomes satisfy predetermined conditions. The output must be accepted with non-zero probability. Methods for implementing postselected quantum computation with noisy gates are proposed. These methods are based on error-detecting codes. Conditionally on detecting no errors, it is expected that the encoded computation can be made to be arbitrarily accurate. Although the success probability of the encoded computation decreases dramatically with accuracy, it is possible to apply the proposed methods to the problem of preparing arbitrary stabilizer states in large error-correcting codes with local residual errors. Together with teleported error-correction, this may improve the error tolerance of non-postselected quantum computation.</p>			
Kuhn, D.R., Wallace, D.R., Gallo,	Software Fault Complexity and Implications for Software Testing	IEEE Transactions on Software Engineering	
<p>Exhaustive testing of computer software is intractable, but empirical studies of software failures suggest that testing can in some cases be effectively exhaustive. Data reported in this study and others show that software failures in a variety of domains were caused by combinations of relatively few conditions. These results have important implications for testing. If all faults in a system can be triggered by a combination of n or fewer parameters, then testing all n-tuples of parameters is effectively equivalent to exhaustive testing for variables with a small set of discrete values.</p>			

Author	Title	Place of Publication	Date
Kumar, S., Marbukh, V.	On Route Exploration Capabilities of Multi-Path Routing in Variable Topology Ad hoc Networks	Proceedings for Instrumentation and Measurement Technology Conference (IMTC 2004), Como, Italy, May 18-20, 2004	

Observation [1] that while the ultimate goal of routing protocol is delivering data along the optimal in some sense (primary) route, maintaining multiple routes through multipath routing may have beneficial effect on the network performance due to keeping track of the optimal route in a variable topology network. Topology changes may be due to node mobility in mobile ad hoc networks, or limited node reliability and power supply in sensor networks. Proposed in [2] decision theoretic framework for performance/resilience optimized multi path routing in networks with unstable topologies frames the problem as a minimum cost routing with uncertain link costs. The potential benefit of this formulation is leveraging of the existing extensive body of analytical and computational decision theoretic approaches and results for performance evaluation and optimization of the multi path routing in variable topology networks. This paper (a) extends framework [2] by assuming that uncertainty in the link costs may be reduced by increasing the data transmission rate over this link due to higher rate of acknowledgements arriving at the source, and (b) proposes an approximation for the optimal load split among feasible routes. Future efforts should be directed

Laskowski, S. J., Autry, M., Cugini, J., Killam, W., Yen, J.	Improving the Usability and Accessibility of Voting Systems and	Report to Congress by the Election Assistance Commission	
--	---	--	--

In the Help America Vote Act (HAVA) of 2002, Public Law 107-252, the Election Assistance Commission, in consultation with the National Institute of Standards and Technology, is mandated to submit a report on human factors, usability, and accessibility to Congress. This report was written to address this mandate. The report describes how research and best practices from the human factors, human-machine and human-computer interaction, and usability engineering disciplines can be brought to bear to improve the usability and accessibility of voting products and systems. A major contribution of the report is a set of ten recommendations for developing standards, accompanying test methods, and guidelines that can measurably improve levels of

Lennon, E.B., Hawes, K. (Photography)	2003 ITL Technical Accomplishments	NISTIR 7034	1/8/2004
--	------------------------------------	-------------	----------

This report presents the achievements and highlights of NIST's Information Technology Laboratory during FY 2003. Following the Director's Foreword and the ITL overview, technical projects in ITL's research program are described, followed by selected cross-cutting themes, industry and international interactions, and staff recognition.

Author	Title	Place of Publication	Date
Liggett, W., Cazares, L.	A Look at Mass Spectral Measurement	Chance	
<p>Analytical instruments with functional responses such as SELDI-TOF mass spectra offer a basis for biomarker development. This paper describes an approach to improving measurement reliability, that is, to improving the consistency of the instrument response, through assessment of sources of variation. The approach is suitable for instruments with functional responses and can therefore be applied even if clinical interpretation of the response has not yet been fully specified. The approach involves and experiment in which measurement of a reference material is replicated with a source of variation sometimes held fixed and sometimes not. The experimental results are interpreted by means of functional principal components analysis. In our illustration, the functional responses are SELDI-TOF mass spectra, and the source of variation is the difference between protein biochips. Among other things, the experiments show that the measurement-to-measurement deviations in the heights of spectral peaks have complicated statistical dependencies. The chip-to-chip variation contributes to these deviations but not in an overwhelming way. The paper concludes with a discussion of the need for addition of metrological studies such as the one</p>			
Liu, H.K., Guthrie, W.F., Malec, D., Yang, G.L.	MCMD in StRD	Proceedings of the Joint Statistical Meetings	
<p>The numerical inaccuracies caused by floating point arithmetic, although often not important, can change the conclusions of an analysis. Computational accuracy is of increasing concern because the number of software packages has exploded as computers have evolved and statistical software is increasingly written and used by non-statisticians who may not be aware of potential computational problems. To address this problem, SED developed the Statistical Reference Datasets (StRD) web site (http://www.itl.nist.gov/div898/strd/index.html) which provides datasets with certified values for assessing the numerical accuracy of software. Four areas of statistical computation were originally addressed, univariate statistics, linear regression, nonlinear regression, and analysis of variance. Recently Markov chain Monte Carlo (MCMC) has become popular and is a new area in which intensive statistical computations are used. Despite its importance, the numerical accuracy of the software for MCMC is largely unknown. By way of specific datasets, we demonstrate in this paper some of the anomalies in MCMC</p>			
Liu, H-K., Guthrie, W.F., Malec, D., Yang, G.L.	Statistical Reference Datasets (StRD) for Assessing the Numerical Accuracy of Markov Chain Monte Carlo Software	http://www.itl.nist.gov/div898/strd/index.html	12/1/2003
<p>In the Statistical Reference Datasets (StRD) project, NIST provided datasets on the web (http://www.itl.nist.gov/div898/strd/) with certified values for assessing the numerical accuracy of software for univariate statistics, linear regression, nonlinear regression, and analysis of variance. Bayesian analysis using Markov chain Monte Carlo (MCMC) is a relatively new area in statistical computing for which the numerical accuracy of both popular and research software is largely unknown. In this addition to the StRD website, new datasets with certified values are provided for assessing the numerical accuracy of MCMC software.</p>			

Author	Title	Place of Publication	Date
Liu, Z.-K., Chen, L.-Q., Raghavan, P., Du, Q., Sofo, J.O., Langer, S., Wolverton, C.	An Integrated Framework for Multi-Scale Materials Simulation and	Journal of Computer-Aided Materials Design	

In this paper, we describe initial results of an ongoing collaborative research activity involving materials scientists, computer scientists, mathematicians, and physicists from academia, industry and a national laboratory. The main objective of the project is to develop a set of integrated computational tools to predict the relationships among the chemical, microstructural and mechanical properties of multicomponent systems. Our goal is to develop a prototype grid-enabled package for multicomponent materials design with efficient information exchange between structure scales and effective algorithms and parallel computing schemes within individual simulation/modeling stages. Our multicomponent materials design framework involves four major computational steps: (1) Atomic-scale first principles calculations to predict thermodynamic properties, lattice parameters, and kinetic data of unary, binary and ternary compounds and solutions phases; (2) CALPHAD data optimization approach to compute thermodynamic properties, lattice parameters, and kinetic data of multicomponent systems; (3) Multicomponent phase-field approach to predict the evolution of microstructures in one to three dimensions (1-3D); and (4) Finite element analysis to generate the mechanical response from the simulated microstructure. These four stages are to be integrated with advanced discretization and parallel algorithms and a software architecture for distributed computing systems.

Lyle, J.R.	NIST CFTT: Testing Computer Forensics Tools	Symposium of Santa Caterina on Challenges in Internet and Interdisciplinary Research	
------------	---	--	--

There is a critical need in the law enforcement community to ensure the reliability of computer forensic tools. A capability is required to ensure that forensic software tools consistently produce accurate and objective results. The goal of the Computer Forensic Tool Testing (CFTT) project at NIST is to establish a methodology for testing computer forensic software tools by development of general tool specifications, test procedures, test criteria, test sets, and test hardware. The results provide the information necessary for toolmakers to improve tools, for users to make informed choices about acquiring and using computer forensics tools, and for interested parties to understand the tools capabilities. Our approach for testing computer forensic tools is based on well-recognized international methodologies for conformance testing and quality testing.

Author	Title	Place of Publication	Date
Lyle, J.R.	Setup and Test Procedures For Testing Interrupt 0x13 Based Software Write Block Tools	http://www.cfft.nist.gov	
<p>This document describes the procedures for testing of interrupt 0x13 based software write block tools using test cases described in Software Write Block Tool Specification & Test Plan Version 3.0. The main objective of this document is to describe the test procedures that shall be followed to accomplish the testing of an interrupt 0x13 based software write block tool. This document also provides enough information about the testing process for either an independent evaluation of the process or independent replication of the results. The intended audience for this document should be familiar with the DOS operating system, Linux (or some UNIX like) operating system, computer operation, computer hardware components such as hard drives, hard drive interfaces (e.g., IDE or SCSI) and computer forensics.</p>			
Lyle, J.R.	SWBT 1.0: Software Write Block Testing Tools Requirements, Design Notes and User Manual	http://www.cfft.nist.gov	3/22/2004
<p>This document describes Release 1.0 of a software package developed to aid the testing of software write block tools typically used in forensic investigations. The package includes programs that monitor the interrupt 13h BIOS disk interface and send selected commands to a software write block tool under test. The software is written in either Borland C++ 4.5 or Borland Assembler. The software can be used in the DOS environment to test an interrupt 0x13 based write block tool, measure the results and aid in documenting test runs. The intended audience for this document should be familiar with the DOS operating system, computer operation, computer hardware components such as hard drives, hard drive interfaces (e.g., IDE or SCSI) and computer forensics. A working knowledge of C and Assembly programming is not necessary for understanding but would be</p>			
Mack, G.A., Lonergan, K., Hale, C.R., Scholtz, J., Steves, M.	A Framework for Metrics in Complex Systems	IEEE Aerospace Conference 2004, March 6-13, 2004	3/6/2004
<p>The Terrorism Information Awareness (TIA) Program established the TIA Metrics Project Team to assist in providing understanding insight into the status of the program and to guide the direction of the research in structured discovery, link and group understanding, decision-making with corporate memory, context-aware visualization, and, ultimately, collaborative problem solving in an environment with real data, real users, and real missions. This paper presents the conceptual basis of the TIA Metrics effort, the methodological approach, and some lessons learned after participation in five large-scale experiments.</p>			

Author	Title	Place of Publication	Date
Malec, D., Toman, B.	A Bayesian Approach to Gas Chromatography Calibration and Prediction for Multiple Laboratory Experiments with Co-Extracted Material	Technometrics	
	<p>Multivariate data obtained by gas chromatography in the process of certification of Standard Reference Materials is usually analyzed one compound at a time. In this article we propose a method of analysis of multiple laboratory experiments, based on the underlying physical measurement model, which is multivariate and thus able to capture laboratory by compound interactions and systematic laboratory effects. We illustrate the method on data from the certification of the Lake Superior Fish Tissue</p>		
Marbukh, V.	Towards Flexible Service Level Agreements	Proceedings for Conference on Information Sciences and Systems (CISS 2004), Princeton, New Jersey, March 17-19, 2004	3/17/2004

A fundamental difficulty of network management and provisioning is that despite the optimal decisions may be very sensitive to the external demands, these demands typically change too fast to allow for the adjustment of the corresponding control actions. Making network provisioning decisions on the basis of the "worst-case" scenario for the demands typically results in significant network over provisioning, while using the "average-case" scenario may result in unacceptable network under provisioning. For temporally variable demands effective bandwidth quantifies the corresponding "intermediate-case" scenario. For spatially variable demands hose service interface has advantages of providing the dependable, dynamic connectivity among endpoints, with the network expected to accommodate any traffic matrix conforming to the hose contract. Since the service contracts based on effective bandwidth are suitable for temporally variable demands and hose contracts are suitable for spatially variable demands, it seems natural to combine these two types of contracts into a flexible Service Level Agreement (SLA) suitable for the customers with demands exhibiting both, temporal and spatial variability. This paper proposes such a combination, and, also discusses possible approaches to a difficult problem of provisioning and pricing of these flexible SLAs.

Author	Title	Place of Publication	Date
Marbukh, V.	Towards Market Approach to Providing Survivable Services	Proceedings for Conference on Information Sciences and Systems (CISS 2004), Princeton, New Jersey, March 17-19, 2004	3/17/2004

Providing reliable networking services under adverse conditions requires additional resources, e.g., link bandwidth, storage memory, transmission power, etc., as compared to best effort services. Adverse conditions may be a result of limited reliability of the network elements, such as network links and/or nodes, as well as a result of malicious attempts to disrupt the network services by adversary/adversaries. Additional network resources are needed for redundant transmissions in order to counteract such adverse conditions. This creates numerous trade-offs among using the network resources for providing survivability, improving quality of service, or increasing the throughput. Two different frameworks to resolving these trade-offs by choosing the operating point on the corresponding Pareto optimal frontier are possible. A centralized framework offers a limited number of solutions controlled by the network. Another, market framework prices either the network resources or directly service contracts, and leaves the choice of the service contracts to the elastic users [1] capable of changing their requirements in an attempt to maximize the individual net utilities, which are the difference between obtained utility and price paid. In this short paper we demonstrate that proposed in [2] framework for fair bandwidth allocation for elastic users can be extended to include survivability issues.

Marbukh, V.	On Aggregate Utility Maximization Based Network Management: Challenges and Possible Approaches	Proceedings for IEEE International Conference on Communications (ICC 2004) Paris, France, June
-------------	--	--

F. P. Kelly et al. have proposed the aggregate utility maximization framework for fair bandwidth sharing among competing elastic demands. This paper advocates extending the aggregate utility maximization framework for balancing a wide range of conflicting requirements of elastic users/contracts. An elastic user/contract is capable of adjusting not only its transmission rate, but also a wide range of burstiness and quality of service parameters as well as willingness to expend resources, such as battery power in a wireless network. The extended framework attempts to maximize the aggregate utility assuming that each elastic user/contract quantifies its preferences with respect to the contract parameters in terms of the individual utility function, and the aggregate utility is a sum of individual utilities of all users. Decentralized maximization of the aggregate utility leads to the minimum cost routing solution, typically with more than one feasible route having minimum cost among all feasible routes. The paper suggests that instability problems of such equal cost multipath routing can be alleviated with an Optimized Multi Path Shortest Path First (OMP-SPF) routing algorithm. The paper also discusses specific cases of network management solutions, including survivability of network services and self-organization in a wireless network by resolving trade-offs between user willingness to transmit and depleting the battery power affecting the network life expectancy. Future efforts should be directed towards developing decentralized pricing schemes for complex contracts capable of maximizing the aggregate utility.

Thursday, April 22, 2004

Author	Title	Place of Publication	Date
Marbukh, V., Van Dyck, R.E.	On the Effect of Limited Competition between Greedy ASs on Internet	Proceedings of the 2004 IEEE International Symposium on Information Theory (ISIT2004), Chicago, Illinois, June 27-July 2,	
<p>We consider the effect of competition between two greedy Autonomous Systems (ASs) on pricing and availability Internet services with elastic demand by formalizing this situation as a non-cooperative game. We assume that ASs attempt to maximize their profits by adjusting prices and bandwidths according to a natural evolutionary algorithm. We numerically investigate the corresponding differential equations describing this adjustment process in continuous time. We demonstrate the possibility of existence of several locally stable equilibria for the evolutionary process, discuss the relation between these equilibria and Nash equilibria in the corresponding game, and give an economic interpretation to obtained results.</p>			
Marbukh, V., Van Dyck, R.E.	On Competition between Greedy Autonomous Systems in Providing Internet Services: Emergent Behavior	Proceedings for Conference on Information Sciences and Systems (CISS 2004), Princeton, New Jersey, March 17-19, 2004	3/17/2004
<p>We consider the effect of competition between two greedy autonomous systems on pricing and availability of Internet services with elastic demand. The problem is formalized in two different ways: (1) as a non-cooperative game, where the autonomous systems attempt to maximize their profits by adjusting prices and bandwidths, and (2) as a natural evolutionary algorithm, where the behaviors of the autonomous systems are modeled by a system of nonlinear differential equations. To investigate the stability of this evolutionary system, we also consider a system of fixed-point equations describing the global behavior. Necessary conditions are presented for equilibria of the game and the evolutionary algorithm, and analytical solutions are found that give the optimal capacities and the corresponding utilities. The economic implications of competition on both the users and</p>			
Martin, A.F., Garofolo, J.S., Fiscus, J.C., Le, A.N., Pallett, D.S., Przybocki, M.A., Sanders, G.A.	NIST Language Technology Evaluation Cookbook	Proceedings of the 4th International Conference on Language Resources and Evaluation, Lisbon, Portugal, May 26-28, 2004	
<p>We review some of the methodology applied to the various NIST language technology evaluations. We discuss the elements included in each evaluation plan, and suggest what we believe are key practices for successful evaluations, and what pitfalls should be avoided. A couple of lessons learned are noted.</p>			

Author	Title	Place of Publication	Date
Martin, A.F., Miller, D., Przybocki, M.A., Campbell, J.P., Nakasone, H.	Conversational Telephone Speech Corpus Collection for the NIST Speaker Recognition Evaluation 2004	Proceedings of the 4th International Conference on Language Resources and Evaluation, Lisbon, Portugal, May 26-28, 2004	

This paper discusses some of the factors that should be considered when designing a speech corpus collection to be used for text-independent speaker recognition evaluation. The factors include telephone handset type, telephone transmission type, language, and (non-telephone) microphone type. The paper describes the design of the new corpus collection being undertaken by the Linguistic Data Consortium (LDC) to support the 2004 and subsequent NIST speech recognition evaluations. Some preliminary information on the resulting 2004 evaluation test set is offered.

Miller, L.E.	Models for UWB Pulses and Their Effects on Narrowband Direct Conversion Receivers	IEEE Conference on Ultra Wideband Systems and	
--------------	---	---	--

A methodology is shown for predicting the effect of pulsed UWB communication waveforms on direct conversion quadrature (I/Q) receivers at baseband by analysis or simulation, making use of mathematical models of UWB pulses, of which several examples are given. The unique characteristics of UWB pulses are used to derive predictions of the UWB interference at baseband using both time- and frequency-domain calculations of the baseband filter's response to the pulses. The final result of this analysis is an estimate of the rise in receiver noise level due to the UWB interference.

Miller, L.E., Kwak, B., Song, N.	Performance Analysis of Exponential Backoff	IEEE/ACM Transactions on Networking	
----------------------------------	---	-------------------------------------	--

New analytical results are given for the performance of the exponential backoff (EB) algorithm. Most available studies on EB focus on the stability of the algorithm and little attention has been paid to the performance analysis of EB. In this paper, we analyze EB and obtain saturation throughput and medium access delay of a packet for a given number of nodes, N. The analysis considers the general case of EB with backoff factor r ; binary exponential backoff (BEB) algorithm is the special case with $r=2$. We also derive the analytical performance of EB with maximum retry limit M (EB-M), a practical version of EB. The

Author	Title	Place of Publication	Date
Miller, L.E., Kwak, B., Song, N.	A Standard Measure of Mobility for Evaluating Mobile Ad Hoc Network Performance	IEICE (Institute of Electronics, Information and Communications Engineers) Transactions on Communications, Vol. E86B, No. 11	

The performance of a mobile ad hoc network (MANET) is related to the efficiency of the routing protocol in adapting to changes in the network topology and the link status. However, the use of many different mobility models without a unified quantitative “measure” of the mobility has made it very difficult to compare the results of independent performance studies of routing protocols. In this paper, a mobility measure for MANETs is proposed that is flexible and consistent. It is flexible because one can customize the definition of mobility using a remoteness function. It is consistent because it has a linear relationship with the rate at which links are established or broken for a wide range of network scenarios. This consistency is the strength of the proposed mobility measure because the mobility measure reliably represents the link change rate regardless of network

Mills, K., Rose, S., Quirolgico, S., Britton, M., Tan, C.	An Autonomic Failure-Detection Algorithm for Distributed Object	4th International Workshop on Software Performance (WoSP)	
---	---	---	--

Designs for distributed systems must consider the possibility that failures will arise, and must adopt specific failure detection and recovery strategies. In this paper, we describe and analyze a self-regulating failure-detection algorithm for distributed object systems. The algorithm bounds resource usage and failure-detection latency, while automatically reassigning resources to achieve the best available failure-detection latency as system size varies dynamically. We apply the algorithm to three different mechanisms found in service-discovery systems: (1) leasing in Jini, (2) service registration in the Service Location Protocol (SLP), and (3) service polling in SLP. For Jini, we compare analytical and simulation predictions against measured performance. For SLP, we compare analytical and simulation predictions. We also identify some other applications for the

Mills, K., Yuan, J.	Monitoring the Macroscopic Effect of DDoS Flooding Attacks	IEEE Transactions on Dependable and Secure Computing	
---------------------	--	--	--

Creating defenses against flooding-based, distributed denial-of-service (DDoS) attacks requires real-time monitoring of network-wide traffic to obtain timely and significant information. Unfortunately, continuously monitoring network-wide traffic for suspicious activities presents difficult challenges because attacks may arise anywhere at any time, and because attackers constantly modify attack dynamics to evade detection. In this paper, we propose an efficient method for early attack detection. Using only a few observation points, our proposed method can monitor the macroscopic effect of DDoS flooding attacks. We show that such macroscopic-level monitoring might be used to capture shifts in spatial-temporal traffic patterns caused by various DDoS attacks, and then to inform more detailed detection systems about where and when a DDoS attack probably arises in transit or source networks. We also show that such monitoring enables DDoS attack detection without any traffic

Author	Title	Place of Publication	Date
--------	-------	----------------------	------

Mitchell, W.F., Tiesinga, E.	Adaptive Grid Refinement for a Model of Two Confined and Interacting Atoms	Applied Numerical Mathematics	
------------------------------	--	-------------------------------	--

We have applied adaptive grid refinement to solve a two-dimensional Schroedinger equation in order to study the feasibility of a quantum computer based on extremely-cold neutral alkali-metal atoms. Qubits are implemented as motional states of an atom trapped in a single well of an optical lattice of counter-propagating laser beams. Quantum gates are constructed by bringing two atoms together in a single well leaving the interaction between the atoms to cause entanglement. For special geometries of the optical lattices and thus shape of the wells, quantifying the entanglement reduces to solving for selected eigenfunctions of a Schroedinger equation that contains a two-dimensional Laplacian, a trapping potential that describes the optical well, and a short-ranged interaction potential. The desired eigenfunctions correspond to eigenvalues that are deep in the interior of the spectrum where the trapping potential becomes significant. The spatial range of the interaction potential is three orders of magnitude smaller than the spatial range of the trapping potential, necessitating the use of adaptive grid refinement.

Nakassis, A.	Expeditious Reconciliation for Practical Quantum Key Distribution	SPIE Conference on Quantum Information and Computation II	
--------------	---	---	--

The optimization criterion of the extant algorithms for the reconciliation step of the BB84 protocol is bit-preservation. While bit-preservation is paramount when the throughput of the quantum channel is sparse, the relevant criterion must be the rate at which secrets are created and researchers report that Cascade-flavor reconciliation can be six times slower than Quantum transmission [HU, AU]. Just over the horizon improvements in single-photon sources and detectors are expected to improve the quantum channel throughput by two or three orders of magnitude and make the reconciliation delay even less acceptable. This paper addresses the issue of speeding-up existing algorithms to make them compatible with higher quantum channel throughputs. First, we combine parameter estimation and segmentation, thereby streamlining the initial phase of reconciliation. Then we relax the bit-preservation constraint and discard low-yield, high-error segments. In the reconciliation of the remaining segments we incorporate Forward Error Correction techniques in our Cascade-type algorithm to reduce informational round trips. When most of the errors have been detected, we use Error Detection techniques to discard segments with errors so as to converge fast while keeping the average cost down. Finally we discuss algorithm modifications necessary to account for false error corrections, and also real-world operation, in which historical data and appropriate escape mechanisms can be used to optimize the reconciliation. Our estimates indicated that we should achieve speed-ups by a factor between 3 and 6 while obtaining 80% to 90% as many bits as Cascade, for a compound throughput improvement by a factor between 2.4 and 5.4. Nevertheless, the actual data show that that the time needed for reconciliation is not proportional to the length of the bitstring reconciled and that significant speedups can be obtained by operating on big blocks of data (between 100Kbits and 1Mbit).

Thursday, April 22, 2004

Author	Title	Place of Publication	Date
Newton, J.J.	Assuring Semantic Consistency for Data Interchange: How XML Users Can Benefit From Using a Metadata	The Data Administration Newsletter, TDAN.com, Issue 27, First Quarter 2004, http://www.tdan.com/i027fe04.htm	1/15/2004

The adoption of XML as the data interchange format for the Web presents a set of challenges and opportunities for data managers. While XML makes it easy to describe the format of information objects and the relationships among them, it does nothing to assure their semantic consistency. Supplementing XML schema descriptions with some mechanism to document the metadata helps determine the meaning of each object in relation to similar objects.

One way to associate meaning with XML elements and attributes is through linkage to a metadata registry (MDR). Namespaces are used by XML structures. It is possible to apply principles developed for the establishment of standardized names through naming conventions to namespaces and the objects contained in namespaces. A metadata registry can be used to store names and assist with issues of naming and identification, metadata description and organization for XML artifacts.

An MDR can assist XML users to maintain the link between XML components and their sources, and store metadata that would make XML structures unwieldy yet still retain access to the information. Meaning is maintained by using semantic components to form names; by using conventions within namespaces; and by using an MDR as a rich metadata resource to augment the sparse metadata descriptive mechanisms XML provides.

Okun, V., Black, P. E., Yesha, Y.	Comparison of Fault Classes in Specification-Based Testing	Information and Software
-----------------------------------	--	--------------------------

Our results extending Kuhn's fault class hierarchy provide a justification for the focus of fault-based testing strategies on detecting particular faults and ignoring others. We develop a novel analytical technique that allows us to elegantly prove that the hierarchy applies to arbitrary expressions, not just those in disjunctive normal form. We also use the technique to extend the hierarchy to a wider range of fault classes. To demonstrate broad applicability, we compare faults in practical situations and analyze previous results. In particular, using our technique, we show that the basic meaningful impact strategy of Weyuker et al.

Thursday, April 22, 2004

Author	Title	Place of Publication	Date
--------	-------	----------------------	------

Over, P.	TREC Video Retrieval Evaluation (TRECVID)	IEEE Multimedia Magazine	
----------	---	--------------------------	--

Within NIST's Information Technology Laboratory, the Information Access Division (IAD) is charged with providing measurements and standards to advance technologies dealing with multimedia and other complex information. Open, metrics-based evaluations organized by IAD using standard data, tasks, and measures, have demonstrated their value in accelerating progress in development of automatic speech recognition and text information retrieval systems. With this in mind, IAD's Retrieval Group launched a benchmarking effort with interested researchers in 2001 aimed at establishing a common evaluation framework for the scientific comparison of digital video retrieval technologies and systems – the TREC Video Retrieval Evaluation (TRECVID). The running of TRECVID is funded by the US Advanced Research and Development Agency

Over, P., Smeaton, A.F., Kraaij, W.	The TREC Video Retrieval Evaluation (TRECVID): A Case Study and Status Report	RAIO 2004 Conference	
-------------------------------------	---	----------------------	--

The TREC Video Retrieval Evaluation (TRECVID) is an annual international effort, funded by the U.S. Advanced Research and Development Activity (ARDA) and the National Institute of Standards and Technology (NIST) to promote progress in content-based retrieval from digital video via open, metrics-based evaluation. Now beginning its fourth year, TRECVID aims over time to develop both a better understanding of how systems can effectively accomplish video retrieval and how one can reliably benchmark their performance. This paper is a case study in the development of video retrieval systems and their evaluation as well as a report on the TRECVID status to-date. After an introduction to the evolution of TRECVID over the past 3 years, we report on the most recent evaluation TRECVID 2003 in terms of the 4 tasks (shot boundary determination, high-level feature extraction, story segmentation and classification, search), the data (133 hours of U.S. television news, the

Porter, D.G., Donahue, M.J.	Velocity of Transverse Domain Wall Motion Along Thin, Narrow Strips	Accepted by Journal of Applied Physics	
-----------------------------	---	--	--

Micromagnetic simulation of domain wall motion in thin, narrow strips leads to a simplified analytical model. The model accurately predicts the same domain wall velocity as full micromagnetic calculations, including dependence on strip width, thickness, and magnitude of applied field pulse. Domain wall momentum and retrograde domain wall motion are both observed and explained by

Author	Title	Place of Publication	Date
Przybocki, M. A., Martin, A. F.	NIST Speaker Recognition Evaluation Chronicles	Proceedings of Odyssey 2004, The Speaker and Language Recognition Workshop, Toledo, Spain, May 31-June 3, 2004	
<p>NIST has coordinated annual evaluations of text-independent speaker recognition since 1996. During the course of this series of evaluations there have been notable milestones related to the development of the evaluation paradigm and the performance achievements of state-of-the-art systems. We document here the variants of the speaker detection task that have been included in the evaluations and the history of the best performance results for this task. Finally, we discuss the data collection and protocols for the 2004 evaluation and beyond.</p>			
Radack, S.M., Editor	Federal Information Processing Standard (FIPS) 199, Standards for Security Categorization of Federal Information and Information Systems	ITL Bulletin, March 2004, http://csrc.nist.gov/publications	3/17/2004
<p>This bulletin describes FIPS 199, Standards for Security Categorization of Federal Information and Information Systems, which is an important component of a suite of standards and guidelines that NIST is developing to improve the security in federal information systems, including those systems that are part of the nation's critical infrastructure. FIPS 199 will enable agencies to meet the requirements of the Federal Information Security Management Act (FISMA) and improve the security of federal information systems. The security standard will also make it possible for federal agencies to establish priorities for protecting their information systems, ranging from very sensitive, mission-critical operations to lower-priority systems performing less</p>			
Radack, S.M., Editor	Security Considerations in the Information System Development Life	ITL Bulletin, December 2003, http://csrc.nist.gov/publications	12/19/2003
<p>This ITL Bulletin summarizes NIST Special Publication (SP) 800-64, Security Considerations in the Information System Development Life Cycle, to help organizations include security requirements in their planning for every phase of the system life cycle, and to select, acquire, and use appropriate and cost-effective security controls. The guide discusses the selection of a life cycle model by the organization and the responsibilities of the organization's managers and staff members for conducting</p>			

Author	Title	Place of Publication	Date
Radack, S.M., Editor	Selecting Information Technology Security Products	ITL Bulletin, April 2004, http://csrc.nist.gov/publications	4/21/2004
<p>This ITL Bulletin summarizes NIST Special Publication (SP) 800-36, Guide to Selecting Information Technology Security Products, which helps organizations select cost-effective and useful products for their systems. Written by Timothy Grance, Marc Stevens, and Marissa Myers, NIST SP 800-36 defines broad security product categories and specifies product types, product characteristics, and environment considerations within those categories.</p>			
Radack, S.M., Editor	Network Security Testing	ITL Bulletin, November 2003, http://csrc.nist.gov/publications	11/20/2003
<p>This ITL Bulletin summarizes NIST Special Publication 800-42, Guideline on Network Security Testing, by John Wack, Miles Tracy, and Murugiah Souppaya, which assists organizations in testing their Internet-connected and operational systems. The guide provides an approach to adopting effective procedures that can help organizations uncover unknown vulnerabilities, institute security controls, and prevent incidents and attacks.</p>			
Radack, S.M., Editor	Computer Security Incidents: Assessing, Managing, and Controlling	ITL Bulletin, January 2004, http://csrc.nist.gov/publications	1/28/2004
<p>This ITL Bulletin summarizes NIST Special Publication (SP) 800-61, Computer Security Incident Handling Guide: Recommendations of the National Institute of Standards and Technology. Written by Tim Grance, Karen Kent, and Brian Kim, SP 800-61 provides practical guidance to help organizations establish an effective incident response program, analyze and respond to information security incidents, and reduce the risks of future incidents.</p>			
Ranganathan, M., Deruelle, J., Montgomery, D.	Programmable Active Services for SIP	Middleware 2004	
<p>SIP-Based IP Telephony offers the promise of rapid service creation and dynamic deployment. SIP Services are fragments of code that are triggered by SIP Messages and can perform actions on behalf of registered users. We present Programmable Active Services for SIP (PASS), a technique that uses Java™ Security and Java Bytecode re-writing to allow untrusted users to upload new services to SIP Signaling Servers. Our technique allows users to write and upload services as Java classes with no a priori constraints on the structure or content of the programs. This generality permits users to leverage the extensive Java libraries and to program in familiar environments. We define an extended, SIP specific, Java security model that restricts the behavior of the executing SIP service and that constrains the computational resources that it consumes.</p>			

Author	Title	Place of Publication	Date
Roberts, J.W.	A New Refreshable Tactile Graphic Display Technology for the Blind and Visually Impaired	Society for Information Display '03 Conference	

Existing electronic Braille displays for accessibility are limited to text-based information. A new technology enables affordable electronic displays for viewing images by the sense of touch on a reusable surface. Applications include education, engineering/artistic design, web surfing, and viewing of art and photographs. A refreshable tactile graphic display has long been sought by the blind and visually impaired for applications where multiple images are needed, but the cost of conventional technology has been prohibitive. The new technology described in this paper reduces cost by a factor of 20 while maintaining

Roberts, J.W.	Temporal Capture and Sequence Reconstruction for Evaluation of Display Systems and Video Content	SPIE Electronic Imaging '03 Conference	
---------------	--	--	--

It is being increasingly recognized that temporal measures are an extremely important addition to conventional measures such as brightness, color, and contrast. In addition to flicker, color breakup, and visible flashes, inaccuracies in the portrayal of motion can greatly affect user acceptance of a system. The project team has previously reported on the use of image capture systems that can capture many images of the display for analysis to determine image characteristics and to reconstruct the temporal behavior of the display. This paper will describe how this technique can be extended to produce useful observation of multi-frame sequences. Issues for proper use of this technique include: 1) frame identification by cues in the frame image or other means, 2) externally generated image timestamps for both intra-frame and inter-frame timing, 3) tying image capture to the display's pixel transition timing to avoid erroneous measures taken during pixel transitions, 4) formatting test material to ensure repeatable display performance, and 5) proper sequence reconstruction and analysis to ensure that the reconstructed sequence is accurately representative of system behavior. Finally, the paper will discuss ways in which measurements taken

Author	Title	Place of Publication	Date
Ross, R., Swanson, M., Stoneburner, G., Johnson, A.,	Guide for the Security Certification and Accreditation of Federal Information Systems	NIST SP 800-37	

NIST Special Publication 800-37 provides guidelines for certifying and accrediting information systems supporting the executive agencies of the federal government. The guidelines have been developed to help achieve more secure information systems within the federal government by: (i) enabling more consistent, comparable, and repeatable assessments of security controls in federal information systems; (ii) promoting a better understanding of agency-related mission risks resulting from the operation of information systems; and (iii) creating more complete, reliable, and trustworthy information for authorizing officials—facilitating more informed accreditation decisions. The guidelines provided in this special publication are applicable to all federal information systems other than those systems designated as national security systems as defined in 44 U.S.C., Section 3542. The guidelines have been broadly developed from a technical perspective so as to be complementary to similar guidelines for national security systems. This publication provides augmented, updated security certification and accreditation information to federal agencies and will functionally replace Federal Information Processing Standards (FIPS) Publication 102, Guidelines for Computer Security Certification and Accreditation, September 1983, (though not formally as a FIPS) when it is rescinded. State, local, and tribal governments, as well as private sector organizations comprising the critical infrastructure of the United States, are encouraged to consider the use of these guidelines, as appropriate.

Ross, R.S.	The New FISMA Standards and Guidelines---Changing the Dynamic of Information Security for the Federal Government	IEEE Journal for Security and Privacy, ITL Bulletin, and http://csrc.nist.gov/sec-cert/	2/19/2004
------------	---	--	-----------

This manuscript describes the new Federal Information Security Management Act (FISMA) standards and guidelines being produced by the Computer Security Division at the National Institute of Standards and Technology in response to recent Congressional legislation. The flagship security standard, Federal Information Processing Standard (FIPS) Publication 199, in the suite of seven publications, provides an approach for categorizing Federal information and information systems according to the potential impact on agency operations (including mission, functions, image, or reputation), agency assets, or individuals should there be a breach in security resulting in the loss of confidentiality, integrity, or availability. Security categorization facilitates the selection of appropriate security controls for Federal information systems in order to adequately protect those systems from serious and ongoing threats. The FISMA-related security standards and guidelines are intended to help Federal agencies, build, implement, operate, and maintain more secure information systems including those systems that support and

Thursday, April 22, 2004

Author	Title	Place of Publication	Date
Ross, R.S., Swanson, M.	Categorization of Federal Information and Information Systems	FIPS 199, http://csrc.nist.gov/publications/fips	2/11/2004
<p>The purpose of this document is to provide a standard for categorizing federal information and information systems according to an agency's level of concern for confidentiality, integrity, and availability and the potential impact on agency assets and operations should their information and information systems be compromised through unauthorized access, use, disclosure, disruption, modification, or destruction.</p>			
Rukhin, A.L., Bebu, I.	Stochastic Model for the Number of Atoms in a Magneto-Optical Trap	Probability in the Engineering and Informational Sciences	
<p>In this paper a Markov Chain for distribution of single atoms is suggested and studied. We explore a recursive model for the number of atoms present in a magneto-optical trap at any given time under the feedback regime with a Poisson distributed loss. Formulas for the stationary distribution of this process are derived. They can be used to adjust the loading rate of atoms to maximize the proportion of time that a single atom is in the trap. The (approximate) optimal regime for the Poisson loading and loss processes are found. In other terms the values of the loading and loss parameters which maximize the probability of exactly one atom in the trap are determined and confirmed through Monte-Carlo simulations. These results are based on the</p>			
Rukhin, A.L., Volkovich, Z.	Testing Randomness via Aperiodic	Journal of Statistical Plannings and Inference	
<p>The properties of statistical procedures based on numbers of occurrences of aperiodic patterns in a random text are summarized. The asymptotic formulas for the expected value of the number of aperiodic words occurring a given number of times, and for the covariance matrix are given. The form of the optimal linear test based on these statistics is established. These procedures are applied to testing for the randomness of a string of binary digits originating from block ciphers.</p>			
Rust, B.W.	Student Exercises on Fossil Fuels, Global Warming, and Gaia	Lecture Notes in Computer Science (Springer-Verlag)	
<p>A recent series of tutorial papers on data fitting [published by the author in the journal "Computing in Science & Engineering," Volumes 3-5 (2001-2003)] has presented an extensive analysis of measured time series records for global temperature variations and global fossil fuel carbon dioxide emissions. The two records were modeled by related combinations of polynomials, exponentials, and sinusoids in a series of least squares fits that could easily be done by students with a better grounding in practical statistics than most now receive. The analysis showed that global temperatures cycle around a monotonically increasing, accelerating baseline with a period of approximately 65 years and that the growth rate of fossil fuel emissions varies inversely with this cycle. The Gaia hypothesis suggests that the biosphere adjusts the atmospheric greenhouse gases to maintain an optimal temperature for life. The previous analysis is here extended with a series of fitting</p>			

Author	Title	Place of Publication	Date
Scholtz, J.	Usability Evaluation	Encyclopedia of Human-Computer Interaction	
This article describes methods of usability evaluation: empirical studies; expert evaluations; and models.			
Scholtz, J., Antonishek, B., Young,	Evaluation of a Human-Robot Interface: Development of a Situational Awareness Methodology	Hawaii International Conference on System Science (HICSS) 37, January 5-8, 2004	1/5/2004
This paper outlines a methodology to evaluate supervisory user interfaces for robotic vehicles based on an assessment of situational awareness.			
Scholtz, J., Belkin, N., Dumais, S., Wilkinson, R.	Evaluating Interactive Information Retrieval Systems: Opportunities and Challenges	CHI 2004 Extended Abstracts, April 2004	
This special interest group seeks to articulate some of the challenges and designing and evaluating interactive information retrieval systems.			
Scholtz, J., Consolvo, S.	Towards a Discipline for Evaluating Ubiquitous Computing Applications	NISTIR 7091	
The paper presents a framework for developing and reporting evaluation studies for ubicomp applications. This framework should give researchers a common vocabulary to facilitate sharing of results and learning across evaluations.			
Scholtz, J., Drury, J.L., Hestand, D., Yanco, H.A.	Design Guidelines for Improved Human-Robot Interaction	CHI 2004 Extended Abstracts, April 2004	
This poster presents some initial design guidelines for HRI as a result of our analysis of HRI awareness anomalies.			

Author	Title	Place of Publication	Date
--------	-------	----------------------	------

Scholtz, J., Morse, E.

In Depth Observational Studies of Professional Intelligence Analysts

Human Performance, Situation Awareness and Automation Technology Conference, March 22-25, 2004

Our goal is to produce metrics for measuring effectiveness of software tools and environments produced for the intelligence community. To this end we need to understand the analytic process and to determine which data need to be captured to meaningfully measure process and effectiveness. In this paper we compare data from observational studies of professional intelligence analysts with data collected from an instrumented environment. We discuss some findings and their implications for possible metrics and for additional data needed to compute potential measures.

Scholtz, J., Morse, E.

Using Consumer Demands to Bridge the Gap between Software Engineering and Usability Engineering

Software Process Improvement and Practice Journal

The Common Industry Format (CIF) is a standard reporting format developed to facilitate adding usability as a criterion for software procurement. We describe the CIF and how it can be used by consumers to request software that includes usability engineering in the development process.

Scholtz, J., Young, J., Yanco, H.A., Drury, J.L.

Evaluation of Human-Robot Interaction Awareness in Search and Rescue

International Conference on Robotics and Automation, (ICRA 2004), New Orleans, Louisiana, April 26-May 1, 2004

The paper describes human-robot awareness and analyzes violations of awareness in a search and rescue competition. The critical incidents that arise from these violations are described.

Author	Title	Place of Publication	Date
Sedransk, N., Rukhin, A.L., Toman,	Meta Analysis Procedures in Key Comparisons and Interlaboratory	Technometrics	

Statistical modeling and analysis of international key comparisons data pose several fundamental questions for statistical methodology. In the absence of a common approach to statistical analysis of the key comparisons data, Le Comite International des Poids et Mesures (CIPM) put forward a suggested procedure. Controversy remains involving the derivation of the key comparison reference value (KCRV) and its associated uncertainty. This paper investigates issues that arise in statistical modeling and analysis of international key comparisons data. First new procedures are derived for KCRV evaluation along with estimates of the uncertainty of this value. In particular, the dependence of the estimators on reported uncertainties based on statistical estimates of standard deviations (Type A) and on scientific judgment (Type B) of participating laboratories is examined. An alternative approach to the analysis of key comparisons data is proposed using a model often employed in meta-analysis and assuming Gaussian distributions and equivalent qualification of all participating laboratories. The relationship of this problem to an analysis of data from interlaboratory studies is explored. A class of weighted means statistics used in meta-analysis for the reference value estimation and a method to assess their uncertainty are given. These estimates lead to associated confidence intervals for the key comparison reference value. Monte Carlo simulation results along with the practical application of these procedures in a key comparison study of accelerometers are also reported.

Shende, V.V., Bullock, S.S., Markov, I.L.	Recognizing Small-Circuit Structure in Two-Qubit Operators	Proceedings of the 41st Design Automation Conference, San Diego, California, June 7-11, 2004	
--	--	--	--

This work proposes numerical tests which determine whether a two-qubit operator has an atypically simple quantum circuit. Specifically, we describe formulae, written in terms of matrix coefficients, characterizing operators implementable with exactly zero, one, or two controlled-not (CNOT) gates and all other gates being local unitary. Circuit diagrams are provided in each case. We expect significant impact in physical implementations where CNOT gates are more difficult to implement than one-qubit operators. Our results can be contrasted with those by Zhang et al., Bullock and Markov, Vidal and Dawson, and Shende et al., where small quantum circuits are built for arbitrary two-qubit operators. The latter two prove that three CNOT gates suffice. However, unitary operators with the sort of structure described above may not be detected. Our work provides results similar to those by Song and Klappenecker but for a wider range of operators.

Author	Title	Place of Publication	Date
Shende, V.V., Markov, I.L., Bullock, S.S.	Finding Small Two-Qubit Circuits	Proceedings of the SPIE Defense and Security Symposium, Kissimmee, Florida, April 12-14,	4/12/2004

It has been shown that the Controlled-NOT (CNOT), CNOT^2 , and CNOT^3 gates suffice to simulate an arbitrary quantum computation. In this paper, we seek minimal circuits in the case of two-qubit operators. Our results can be summarized as follows. To construct an arbitrary two-qubit state from $|00\rangle$, one CNOT gate suffices, and is necessary for generic states. To simulate an arbitrary two-qubit operator up to global phase, two CNOTs suffice, and are necessary in the generic case. To simulate an arbitrary two-qubit operator up to global phase, three CNOTs suffice. We also contribute a simple procedure to determine the minimal number of CNOT gates necessary to simulate a given two-qubit operator up to global phase. In particular, we prove that the SWAP gate requires three CNOTs and give an optimal two-qubit circuit for the two-qubit Quantum Fourier Transform. We also discuss timing a given Hamiltonian to simulate a CNOT, modulo one-qubit gates, when this is possible. In all cases, we give explicit circuit constructions realizing lower bounds. To compute gate parameters, we only use closed-form algebraic expressions. In particular, we only rely on matrix exponentials in the case of Hamiltonian timing. Our algorithms have been coded in C++.

Sheppard, C.L., LaPlant, B., Nevile,	Dublin Core and the Alternative Interface Access Protocol	NISTIR
--------------------------------------	---	--------

This paper is a report on a metadata effort that aims to make all of our lives easier, especially the lives of people with disabilities. The metadata will be used to enable interoperability between a "Universal Remote Console (URC)" and a variety of 'intelligent' objects including appliances, consumer electronics, environmental controls, and Internet services in a way that is designed to provide users with a single look-and-feel interface. Developing this metadata raises issues of compatibility with current metadata sets and it is hoped that through collaboration with the Dublin Core community, advances can be made in the

Sims, J.S., Hagstrom, S.A.	Math and Computational Science Issues in High Precision Hylleraas-Configuration Interaction (Hy-CI) Calculations. I. Three-Electron	Journal of Physics B: Atomic, Molecular, and Optical Physics
----------------------------	---	--

The most difficult integral arising in Hylleraas-Configuration Interaction (Hy-CI) calculations, the three-electron triangle integral, is discussed. We focus on recursive techniques at both the double precision and quadruple precision level of accuracy while trying to minimize the use of higher precision arithmetic. Also, we investigate the use of series acceleration to overcome problems of slow convergence of certain integrals defined by infinite series. We find that a direct + tail Levin u -transformation convergence acceleration overcomes problems that arise when using other convergence acceleration techniques, and is the best method for overcoming the slow convergence of the triangle integral. The question of calibrating an acceleration method is also discussed, as well as ways to improve our work.

Author	Title	Place of Publication	Date
Smith, S.W., Polk, W.T., Hastings, N.E.	1st Annual PKI Research Workshop Proceedings	NISTIR 7059	10/30/2003
<p>NIST hosted the first annual Public Key Infrastructure (PKI) Research Workshop on April 24-25, 2002. The two-day event brought together PKI experts from academia, industry, and government to explore the remaining challenges in deploying public key authentication and authorization, and to develop a research agenda to address those outstanding issues. The workshop consisted of the presentation of 14 referred papers, four panel discussions, and a work-in-progress session. About 100 participants from the United States, United Kingdom, Canada, Spain, Sweden, Ireland, Taiwan, and South Korea made the workshop an international event. Based on participant feedback, the workshop provided the most up-to-date information on PKI research and deployment. This proceedings includes the refereed papers, and captures the essence of the panels and</p>			
Soboroff, I.M., Harman, D.K.	Overview of the TREC 2003 Novelty	Included in NIST SP 500-255, The Twelfth Text Retrieval Conference, http://trec.nist.gov	
<p>The novelty track was first introduced in TREC 2002. Given a TREC topic and an ordered list of documents, systems must find the relevant and novel sentences that should be returned to the user from this set. This task integrates aspects of passage retrieval and information filtering. This year, rather than using old TREC topics and documents, we developed fifty new topics specifically for the novelty track. These topics were of two classes: "events" and "opinions." Additionally, the documents were ordered chronologically, rather than according to a retrieval status value. There were four tasks which provided systems with varying amounts of relevance or novelty information as training data. Fourteen groups participated in the track this year.</p>			
Sriram, K., Griffith, D., Su, R., Golmie, N.	Static Vs. Dynamic Regenerator Assignment in Optical Switches: Models and Cost Trade-Offs	Proceedings for Workshop on High Performance Switching and Routing (HPSR 2004), Phoenix, Arizona, April 8-21, 2004	4/8/2004
<p>Agile all optical switches (OXC) currently use an architecture in which regenerators and transceivers have preassigned fixed directionality. However, technology is evolving to enable new OXC architectures in which the directionality of regenerators and transceivers can be dynamically assigned on demand. In this paper, we quantify the performance and cost benefits of regenerators and transceivers with dynamically assignable directionality. We show that fewer regenerators and transceivers need to be used with the new architecture because of sharing of resources across all directionality combinations. This translates to significant cost savings for the new architecture, especially as the traffic load in the network increases.</p>			

Author	Title	Place of Publication	Date
Stanford, V.M., Kasianowicz, J.J.	Transport of DNA Through a Single Nanometer-Scale Pore: Evolution of Signal Structure	IEEE Workshop on Genomic Signal Processing and Statistics (GENSIPS) 2004 Proceedings	
<p>Single-stranded DNA can be driven through a single nanometer-scale pore. This process causes the ionic current that otherwise flows through the pore to decrease for characteristic times that a polynucleotide and the pore interact. We previously reported a method for characterizing these signals using ergodic, but persistent Hidden Markov Models (HMMs). Gaussian mixture models (GMMs) were used as output distributions to obtain a maximum likelihood estimate of state sequence and lifetime. We show here that a more economical state description can be applied to signals from shorter lifetime events. The results are consistent with the known structure of the nanopore and may suggest approaches to more detailed interrogation of the information stored in</p>			
Strawderman, W.E., Rukhin, A.L.	Statistical Aspects of Linkage Analysis in Interlaboratory Studies	Journal of American Statistical Association	
<p>This paper investigates issues that arise in statistical inference in interlaboratory studies known as Key Comparisons when one has to link several comparisons to or through existing studies. A new approach to the analysis of such a data is proposed using a Gaussian distributions model often employed in meta-analysis. We develop conditions for the set of sufficient statistics to be complete and characterize unique uniformly minimum variance unbiased estimators of the contrast parametric functions. New procedures are derived for estimating these functions with estimates of their uncertainty. In particular, the dependence of these procedures on reported uncertainties based on statistical estimates of standard deviations (Type A) and on scientific judgment (Type B) of participating laboratories is examined. These estimates lead to associated confidence intervals for the laboratories (or studies) contrasts. Several examples demonstrate statistical inference for contrasts based on linkage through the pilot laboratories. Monte Carlo simulation results on performance of approximate confidence intervals are also reported.</p>			
Toman, B.	A Bayesian Approach to Assessing Uncertainty and Calculating a Reference Value in Key Comparison	Technometrics	
<p>International experiments called Key Comparisons may be required to provide an estimate of a physical constant or quantity called a Reference Value. While there are many possible forms that this estimator can take, none have so far been accepted as a standard. Recently, this topic has received much international attention. In this paper, it is argued that a fully Bayesian approach is compatible with the current practice of metrology and provides estimators which perform well compared to the most commonly used estimator based on the weighted mean of the participating laboratories' measurements.</p>			

Author	Title	Place of Publication	Date
Van Dyck, R.E., Mahapakulchai, S.	Design of Ring Convolutional Trellis Codes for MAP Decoding of MPEG-4 Images	IEEE Transactions on Communications 2004	
	<p>We propose a trellis coded modulation system using CPFSK and ring convolutional codes for transmitting the bits generated by an embedded zerotree wavelet encoder. Improved performance is achieved by using maximum a posteriori decoding of the zerotree symbols, and ring convolutional trellis codes are determined for this decoding method. The CPFSK transmitter is decomposed into a memoryless modulator and a continuous phase encoder over the ring of integers modulo 4; the latter is combined with a polynomial convolutional encoder over the same ring. In the code design process, a search is made of the combined trellis, where the branch metrics are modified to include the source transition matrix. Simulation results of image transmission are provided using the optimized system, including mismatched channel cases.</p>		
Voorhees, E.M.	Overview of the TREC 2003 Robust Retrieval Track	Included in NIST SP 500-255, The Twelfth Text Retrieval Conference, http://trec.nist.gov	3/25/2004
	<p>The robust retrieval track is a new track in TREC 2003. The goal of the track is to improve the consistency of retrieval technology by focusing on poorly performing topics. In addition, the track brings back a classic, ad hoc retrieval task to TREC that provides a natural home for new participants.</p>		
Voorhees, E.M.	Measuring Ineffectiveness	ACM SIGIR Conference, Sheffield, England, July 26-29, 2004	
	<p>An evaluation methodology that targets ineffective topics is needed to support research on obtaining more consistent retrieval across topics. Using average values of traditional evaluation measures is not an appropriate methodology because it emphasizes effective topics: poorly performing topics' scores are by definition small, and they are therefore difficult to distinguish from the noise inherent in retrieval evaluation. We examine two new measures that emphasize a system's worst topics. While these measures focus on different aspects of retrieval behavior than traditional measures, the measures are less stable than traditional measures and the margin of error associated with the new measures is large relative to the observed</p>		

Author	Title	Place of Publication	Date
Voorhees, E.M.	Overview of the TREC 2003 Question Answering Track	Included in NIST SP 500-255, The Twelfth Text Retrieval Conference, http://trec.nist.gov	3/25/2004

The TREC 2003 question answering track contained two tasks, the passages task and the main task. In the passages task, systems returned a single text snippet in response to factoid questions; the evaluation metric was the number of snippets that contained a correct answer. The main task contained three separate types of questions, factoid questions, list questions, and definition questions. Each of the questions was tagged as to its type and the different question types were evaluated separately. The final score for a main task run was a combination of the scores for the separate question types. This paper defines the various tasks included in the track and reports the evaluation results. Since the TREC 2003 track was the first time for significant participation in the definition and list subtasks, the paper also examines the reliability of the evaluation for these

Voorhees, E.M.	Overview of TREC 2003	Included in NIST SP 500-255	
<p>The twelfth Text REtrieval Conference, TREC 2003, was held at the National Institute of Standards and Technology (NIST) November 18--21, 2003. The conference was co-sponsored by NIST, the U.S. Department of Defense Advanced Research and Development Activity (ARDA), and the Defense Advanced Research Projects Agency (DARPA). This paper serves as an introduction to the research described in detail in the remainder of the proceedings.</p>			
Wack, J., Tracy, M., Souppaya, M.	Guideline on Network Security Testing	NIST SP 800-42, http://csrc.nist.gov/publications/nist_pubs/index.html	10/10/2003

The purpose of this document is to provide guidance for security program manager, technical managers, functional managers, and other information technology (IT) staff members who deal with systems concerning when and how to perform tests for network security vulnerabilities and policy implementation. This document identifies network testing requirements and how to prioritize testing activities with limited resources. It describes security testing techniques and tools. This document provides guidance to assist organizations in avoiding redundancy and duplication of effort by providing a consistent approach to network security testing throughout an organization's networks. Furthermore, this document provides a feasible approach for organizations by offering varying levels of network security testing as mandated by an organization's mission and security objectives. The main focus of this document is the basic information about techniques and tools for individuals to begin a testing program. This document is by no means all-inclusive and individuals and organizations should consult the references

Author	Title	Place of Publication	Date
Walsh, T.J., Kuhn, D.R.	Securing Voice Over IP Networks	IEEE Computer Security and	
<p>Voice over IP – the transmission of voice over traditional packet-switched IP networks – is one of the hottest trends in telecommunications. As with any new technology, VOIP introduces both opportunities and problems. Lower cost and greater flexibility are among the promises of VOIP for the enterprise, but security administrators will face significant challenges. Administrators may assume that since digitized voice travels in packets, they can simply plug VOIP components into their already-secured networks. Unfortunately, many of the tools used to safeguard today’s computer networks, namely firewalls, Network Address Translation (NAT), and encryption, carry a hefty price when incorporated into a VOIP network. This paper introduces the security issues with VOIP and outlines steps that can be taken to operate a VOIP system securely.</p>			
Wilson, C.L., Garris, M.D., Watson, C.I.	Matching Performance for the US-Visit IDENT System Using Flat Fingerprints	NISTIR	
<p>This report discusses the flat to flat matching performance of the US-VISIT fingerprint matching system. Both one-to-many matching used to detect duplicate visa enrollments and one-to-one matching used to verify the identity of the visa holder are discussed. With the proper selection of an operating point, the one-to-many accuracy for a two-finger comparison against database of 6,000,000 subjects is 95% with a false match rate of 0.08%. Using two fingers, the one-to-one matching accuracy</p>			
Wilson, M., Hash, J.	Building an Information Technology Security Awareness and Training	NIST SP 800-50, http://csrc.nist.gov/publications/nist_pubs/index.html	10/10/2003
<p>NIST Special Publication 800-50, Building An Information Technology Security Awareness and Training Program, provides guidance for building an effective information technology (IT) security program and supports requirements specified in the Federal Information Security Management Act (FISMA) of 2002 and the Office of Management and Budget (OMB) Circular A-130, Appendix III. The document identifies the four critical steps in the life cycle of an IT security awareness and training program: 1) awareness and training program design (Section 3); 2) awareness and training material development (Section 4); 3) program implementation (Section 5); and 4) post-implementation (Section 6).The document is a companion publication to NIST Special Publication 800-16, Information Technology Security Training Requirements: A Role- and Performance-Based Model. The two publications are complementary – SP 800-50 works at a higher strategic level, discussing how to build an IT security awareness and training program, while SP 800-16 is at a lower tactical level, describing an approach to role-based IT security</p>			

Author	Title	Place of Publication	Date
Wilson, M., Hash, J.	Information Technology Security Awareness, Training, Education, and Certification	ITL Bulletin, October 2003, http://csrc.nist.gov/publications	10/16/2003

This ITL Bulletin summarizes NIST SP 800-50, Building an Information Technology Security Awareness and Training Program. It provides guidelines for building and maintaining a comprehensive awareness and training program, as part of an organization's IT

Wood, S.S., Wilson, C.L.	Studies of Plain-to-Rolled Fingerprint Matching Using the NIST Algorithmic Test Bed (ATB)	NISTIR
--------------------------	---	--------

A series of fingerprint matching studies have been conducted on an experimental laboratory system called the Algorithmic Test Bed (ATB), a system used to test the automated fingerprint identification system (AFIS) component of the FBI's Integrated AFIS (IAFIS). The ATB was designed to match rolled images to a rolled database. These studies measured its performance when making plain to rolled (and plain to plain) matches. Six sets of data were obtained from government sources. Two were civil; four were law enforcement. One set of law enforcement data, from Ohio's Bureau of Criminal Identification and Investigation (BCII), contained five subsets; each subset contained fingerprint records of the same 925 subjects, but each subset came from a different source. The three foci of the studies were differences in the ATB's performance among the subsets of BCII, similarities among all the sets, and accuracy of the ATB as a model of IAFIS. There were clear differences among the BCII subsets, but the interclass difference (between rolled and plain) was smaller than the intraclass differences. There were similarities among all the sets; the invariance of the true accept rate (TAR) over gallery size and the essentially linear relationship of the false accept rate (FAR) to gallery size were both notable. Plain to plain matching produced results similar to plain to rolled. The ATB was found to be an accurate model of IAFIS.

Yanco, H.A., Drury, J.L., Scholtz,	Beyond Usability Evaluation: Analysis of Human-Robot Interaction at a Major Robotics Competition	Special Issue of Human-Computer Interaction, Vol. 19 (2004), Nos. 1 and 2
------------------------------------	--	---

Our study applied robotics, human-computer interaction (HCI), and Computer Supported Cooperative Work (CSCW) expertise to gain experience with HCI/CSCW evaluation techniques in the robotics domain. We used as our case study four different robotics systems that competed in the 2002 American Association of Artificial Intelligence (AAAI) Robot Rescue Competition.

Author	Title	Place of Publication	Date
--------	-------	----------------------	------

Zevin, S.F.	Testing: A Key to Building Trust and Confidence in IT Systems	The Standards Edge: Dynamic Tension	
-------------	---	-------------------------------------	--

The ubiquitous computer now touches nearly every aspect of human life. The promise of information technology is improvement to the quality of life. Maintaining trust and confidence in information technology is central to keeping that promise. This is difficult when most information technology systems fail to meet key user expectations, are difficult to use, fail unexpectedly, contain hidden security vulnerabilities, and are delivered full of bugs. Building the trust of users of IT systems requires a significant new focus on techniques and tools to improve IT systems, from hardware, to system and application software, and to the interactions between the system and the user. Developing the connections between expectations and measurable system attributes enables the user to better understand and establish the level of trust that can be placed in an IT system. NIST concentrates on the development of measurement technologies and testing programs commensurate with life-cycle phases of software development to foster this understanding. Testing methods range from simple code- checking to formal implementations of validation and certification programs conforming to international standards for laboratory testing programs. Future work must address testing beyond component development to the interoperation of components in integrated systems. And, as systems become more complex, dynamic, scalable and changeable, new testing paradigms must be developed.

Zhang, N.F.	Estimating the Variance of the Graybill-Deal Estimator of a Common	Biometrics	
-------------	--	------------	--

The Graybill-Deal estimator has been used to estimate the common mean of several populations with possible unknown and different variances. However, the traditional estimator of the variance of the Graybill-Deal estimator underestimates the true variance. Two new variance estimators are proposed with smaller biases while the correspondingly formed intervals have much better coverage of the true mean.

Zhang, N.F., Liu, H.K., Sedransk, N., Strawderman, W.	Statistical Analysis of Key Comparisons with Linear Trends	Metrologia	
---	--	------------	--

A statistical analysis for Key Comparisons with linear trend is proposed. The approach has the advantage that it is consistent with the case in which there is no trend. The uncertainties for KCRV and the degrees of equivalence are also provided. As an example, the approach is applied to Key Comparison CCEM-K2.