

FY 2001 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
Anderson, D. M., McFadden, G. B., Wheeler, A. A.	A Phase-Field Model with Convection: Sharp-Interface Asymptotics	NISTIR 6568 and Physica D	10/25/00

We have previously developed a phase-field model of solidification that includes convection in the melt. This model represents the two phases as viscous liquids, where the putative solid phase has a viscosity much larger than the liquid phase. The object of this paper is to examine in detail a simplified version of the governing equations for this phase-field model in the sharp-interface limit to derive the interfacial conditions of the associated free-boundary problem. The importance of this analysis is that it reveals the underlying physical mechanisms built into the phase-field model in the context of a free-boundary problem and, in turn, provides a further validation of the model. In equilibrium we recover the standard interfacial conditions including the Young-Laplace and Clausius--Clapeyron equations that relate the temperature to the pressures in the two bulk phases, the interface curvature and material parameters. In nonequilibrium we identify boundary conditions associated with classical hydrodynamics, such as the normal mass flux condition, the no-slip condition and stress balances. We also identify the heat flux balance condition which is modified to account for the flow, interface curvature and density difference between the bulk phases. The interface temperature satisfies a nonequilibrium version of the Clausius--Clapeyron relation which includes the effects of curvature, attachment kinetics and viscous dissipation.

Badre, A., Laskowski, S.J.	The Cultural Context of Web Genres: Content vs. Style	Human Factors and the Web 2001 Conference
----------------------------	---	---

The question we raise here is whether what is culturally established for a given genre in the brick and mortar world applies equally on the World Wide Web. Can we effectively use the styles of one genre to design the site of another genre? Are we wedded to the culturally established attributes of the real world when designing for the Web? We compared users' performance and preference for shopping- vs. news-styled sites. We found that on the whole users liked the "shopping" layout better than the news layout, even when viewing news content. This was especially surprising in light of the fact that our users had so much more experience with news sites over shopping sites. This perhaps shows how popular the shopping style is in our culture. People chose News as Shopping as their favorite site, even though it was difficult to use. People who preferred News as Shopping did better on both News as Shopping and News as News, than those who preferred News as News. This suggests a potential relationship between performance on the World Wide Web and preference for the shopping style.

Barker, E.B.	Cryptographic Protection for the Twenty-First Century	Internet Security Conference Newsletter (TISC Insight)
--------------	---	--

In 2000, the National Institute of Standards and Technology (NIST) announced the selection of a new encryption algorithm that will be used to protect sensitive (unclassified) government information. This algorithm, to be proposed as the Advanced Encryption Standard (AES), is the

that interact through this API. We focus first on “Annotation Graphs”, a graph model for annotations on linear signals (such as text and speech) indexed by intervals, for which efficient database storage and querying techniques are applicable. We note how a wide range of existing annotated corpora can be mapped to this annotation graph model. This model is then generalized to encompass a wider variety of linguistic “signals” including both naturally occurring phenomena (as recorded images, video, multi-modal interactions, etc.) as well as the derived resources that are increasingly important to the engineering of natural language processing systems (such as word lists, dictionaries, aligned bilingual corpora, etc.). We conclude with a review of the current efforts towards implementing key pieces of this architecture.

Blackburn, D., Bones, M., Phillips, P.J., Grother, P.J. Facial Recognition Vendor Test 2000 NISTIR

The biggest change in the facial recognition community since the completion of the FERET program has been the introduction of facial recognition products to the commercial market. Open market competitiveness has driven numerous technological advances in the algorithms tested in the FERET program and significantly lowered system costs. Today, there are dozens of facial recognition systems available that have the potential to meet performance requirements for numerous applications. But which of these systems best meet the performance requirements for given applications? Repeated inquiries from numerous government agencies on the current state of facial recognition technology prompted the DoD Counterdrug Technology Development Program Office to establish a new set of evaluations. The Facial Recognition Vendor Test 2000 (FRVT 2000), was co-sponsored by the DoD Counterdrug Technology Development Program Office, the National Institute of Justice, and the Defense Advanced Research Projects Agency, and was administered in May-June 2000.

Blue, James. L. Fair Selection of Jury Panels from Jury Pools NISTIR 6569 10/25/00

A standard problem of courts at all levels is the selection of a panel of potential jurors from a jury pool, which is a list of people who are eligible to serve as jurors. The problem is to select N people out of the M possible people in a fair way. One definition of “fair” is that each of the M people has an equal chance to be selected for any jury pool. A much more rigorous definition is that each of the possible combinations of N people has an equal chance to be selected as the entire jury pool. A working computer program incorporating a fair algorithm for the problem stated above has been produced, together with a brief testing program. The properties of this algorithm are discussed, and an improved version of a program developed previously is presented.

Boisvert, R. F., Donahue, M. J., Lozier, D. W., McMichael, R., Rust, B. W. Mathematics and Measurement NIST Journal of Research, Vol. 106, No. 1, January-February 2001 2/28/01

In this paper we describe the role that mathematics plays in measurement science at NIST. We first survey the history behind NIST’s current work in this area, starting with the NBS Math Tables project of the 1930s. We then provide examples of more recent efforts in the application of mathematics to measurement science, including the solution of ill-posed inverse problems, characterization of the accuracy of software for micromagnetic modeling, and in the development and dissemination of mathematical reference data. Finally, we comment on emerging issues in measurement science to which mathematicians will devote their energies in coming years.

Boisvert, R. F., Moreira, J., Philippsen, M., Pozo, R. Numerical Computing in Java™

Accepted by Computing in Science and Engineering

We discuss the advantages and disadvantages of using Java(TM) for numerical computing. We provide examples of current performance levels and propose several additional language features that would make Java more easily applied in scientific applications.

Boisvert, R., Lozier, D.

Handbook of Mathematical Functions

A Century of Excellence in Measurements, Standards, and Technology: Selected Publications of NBS/NIST, 1901-2000, D. Lide, Ed., pp. 135-139.

1/31/01

Burr, W.E.

Digital Rights Management: How Much Can Cryptography Help? Included in NISTIR 6591, Digital Cinema 2001 Proceedings

1/11/01

Cryptography offers powerful techniques for data protection in "classical" communications applications. Claims are often made that some new "technology" will enable or make electronic publishing "safe." This talk sounds a cautionary note, at least for large scale, controlled distribution of digital content to millions of consumers or subscribers. The essential difference is that both the sender and the receiver are trusted parties in a communications protocol (an attacker is a third party), but in Digital Rights Management (DRM) applications the consumer who receives the data is the likely attacker. This is a much more difficult problem. Cryptography may also offer small comfort to traditional intellectual property rights holders in the face of changing ethics and notions of property rights, and evolving business models, all of which are driven by new digital technologies.

Burr, W.E.

Data Encryption Standard

A Century of Excellence in Measurements, Standards, and Technology: Selected Publications of NBS/NIST, 1901-2000, D. Lide, Ed., pp. 250-253.

1/31/01

Carasso, A.S.

Direct Blind Deconvolution II. Substitute Images and the Beak Method

NISTIR 6570 and SIAM Journal on Applied Mathematics

11/1/00

The BEAK method is an FFT-based direct blind deconvolution technique previously introduced by the author, and applied to a limited but significant class of blurs that can be expressed as convolutions of 2-D symmetric Lévy probability density functions. This class includes and generalizes Gaussian and Lorentzian distributions, but does not include defocus blurs. The method requires a-priori information on the Fourier transform $f_e(?,?)$ of the unknown exact image $f_e(x,y)$, namely, the gross behavior of $\log |f_e(?,?)|$ along a single line through the origin in the $(?,?)$ plane. The present paper significantly extends the applicability of the BEAK method. It is shown that images of similar objects often display approximately equal gross behavior, and that gross behavior in such substitute images can be used successfully in numerous

stopping power reduction factor to be 5.06 +/- 0.35 percent. When we reduce the TRIM prediction by this factor, we get good agreement between the observed and predicted NDP measurements.

Coakley, K. J., Levenson, M. S. Commentary for Special Issue on International Journal of Imaging
Quantitative Imaging Systems and Technology

Kevin Coakley and Mark Levenson were invited to solicit papers on Quantitative Imaging for a special issue of the International Journal of Imaging Systems and Technology. They briefly describe the papers in a commentary that will appear in the special issue.

Coriell, S.R., McFadden, G.B. Applications of Morphological Stability Journal of Crystal Growth
Theory

Recent applications of morphological stability theory are reviewed. For growth of a binary alloy from the melt, the temperature-dependence of the solute diffusivity can have a significant effect on the critical wavelength at the onset of instability. The response of the interface velocity to an electrical current pulse has been calculated by a linear perturbation analysis. The effect of a parallel shear flow and anisotropic interface kinetics on the onset of instability during growth from a supersaturated solution has been analyzed. The kinetic anisotropy arises from a model of step motion in which the morphological instability corresponds to step bunching. Kinetic anisotropy causes traveling waves along the crystal-solution interface and an enhancement of morphological stability. A shear flow in the direction of the step motion promotes morphological instability, while flow in the opposite direction is stabilizing. Oscillatory (in time) shear flows can be studied by Floquet theory.

Coriell, S.R., McFadden, G.B., Effect of Flow Due to Density Change on Accepted by Journal of Crystal Growth
Mitchell, W.F., Murray, B.T., Andrews, Eutectic Growth
J.B., Arikawa, Y.B.

The Jackson-Hunt model of eutectic growth is extended to allow for different densities of the phases. The density differences give rise to fluid flow which is calculated from a series solution of the fluid flow equations in the Stokes flow approximation. The solute diffusion equation with flow terms is then solved numerically using an adaptive refinement and multigrid algorithm (PLTMG). The interface undercoolings and volume fractions are calculated for the tin-lead and iron-carbon eutectic alloys and for the aluminum- indium monotectic alloy. The numerical results are compared with various approximations based on the Jackson-Hunt analysis.

Croarkin, M.C. Realistic Evaluation of the Precision and A Century of Excellence in 1/31/01
Accuracy of Instrument Calibration Measurements, Standards, and
Systems Technology: Selected Publications of
NBS/NIST, 1901-2000, D. Lide, Ed., pp.
129-131.

Croarkin, M.C. Statistics and Measurement NIST Journal of Research, Vol. 106, No. 1/31/01
1, pp. 279-292, January-February 2001

For more than 50 years, the Statistical Engineering Division (SED) has been instrumental in the success of a broad spectrum of metrology projects at NBS/NIST. This paper highlights fundamental contributions of NBS/NIST statisticians to statistics and to measurement science and technology. Published methods developed by SED staff, especially during the early years, endure as cornerstones of statistics not only in metrology and standards applications, but as data-analytic resources used across all disciplines. The history of statistics at NBS/NIST, began with the formation of what is now the SED. Examples from the first five decades of the SED illustrate the critical role of the division in the successful resolution of a few of the highly visible, and sometimes controversial, statistical studies of national importance. A review of the history of major early publications of the division on statistical methods, design of experiments, and error analysis and uncertainty is followed by a survey of several thematic areas. The accompanying examples illustrate the importance of SED in the history of statistics, measurements and standards: calibration and measurement assurance, interlaboratory tests, development of measurement methods, Standard Reference Materials, statistical computing, and dissemination of measurement technology. A brief look forward sketches the expanding opportunity and demand for SED statisticians created by current trends in research and development at NIST.

Croarkin, M.C.	Experimental Statistics	A Century of Excellence in Measurements, Standards, and Technology: Selected Publications of NBS/NIST, 1901-2000, D. Lide, Ed., pp. 132-134.	1/31/01
Cugini, J.V.	The FLUD Format: Logging Usability Data from Web-Based Applications	NIST SP 500-247 (web only at http://www.itl.nist.gov/iaui/vvrg/cugini/wbmet/flud/specification.html)	1/3/01
<p>This paper presents a proposed format for representing the behavior of users as they interact with a Web-based application. The captured log data can be valuable for analyzing and improving the usability of such applications. The background and motivation of this effort are briefly described. The detailed syntax and semantics of the format are then defined.</p>			
Cugini, J.V.	FORTRAN Test Programs	A Century of Excellence in Measurements, Standards, and Technology: Selected Publications of NBS/NIST, 1901-2000, D. Lide, Ed., pp. 258-259.	1/31/01
Cugini, J.V., Laskowski, S.J.	Design of a File Format for Logging Website Information	NIST SP 500-248 (web only at http://www.itl.nist.gov/iaui/vvrg/cugini/wbmet/flud/design-paper.html)	4/11/01

The logging of user behavior in support of web usability testing is constrained by the difficulty of capturing and analyzing large amounts of

logged data. However, there is great potential for the development of tools to support automated recording and analysis, especially for remote or large scale testing. In this paper, we propose a format for the representation of user interaction with a website. A widely accepted format enables the development of a set of software tools to process the data, the sharing of data sets for longer term analysis and research, and provides a common language for expressing user interaction with a website.

Dabrowski, C.E.	Characteristics of ADLs That Support Good Architecture Documentation: A Position Paper for the SEI Software Architecture Workshop	Proceedings of Software Engineering Documentation Workshop, January 16-17, 2001	1/16/01
-----------------	---	---	---------

One of the potential benefits of describing software architecture is the ability to provide greater clarity and understanding than what is possible in program code. The concise representation of the essential aspects of the functional components of a system, their connections and interactions, and their behavior provides a basis for communicating system design. This serves as documentation for different stakeholders and participants in the system design process, including system analysts, designers, implementers, maintainers, and managers. In current software practice, the development of comprehensive documentation of any aspect of a system--including its architecture--is often lengthy and tedious. This is particularly the case when describing a system using a terminology familiar to customers or when it is necessary to provide alternative views of a system to different stakeholders. To provide the greatest benefit with the least amount of effort, it should be possible for an architecture description to be stated completely in a specification created using the ADL. That is, a specification written in an ADL should be as self-documenting as possible. While additional text will always be required to provide context and design rational, the actual specification of software architecture in the ADL should be definitive enough not to require large amounts of additional explanation and comments. This position paper makes recommendations on good characteristics of architecture documentation and discusses ADL features that support such characteristics.

Davies, M. A., Pratt, J. R., Dutterer, B., Burns, T. J.	Regenerative Stability Analysis of Highly Interrupted Machining	Proceedings of the Third International Conference on Metal Cutting and High Speed Machining, June 27-29, 2001, Metz, France
---	---	---

We discuss theoretical and experimental work that supports the use of very low radial immersion in the high-speed milling of difficult-to-machine materials, such as titanium alloys. Our theory is based upon modeling the cutting process by a kicked harmonic oscillator with delay. Traditional regenerative chatter theory predicts that, for a single degree of freedom system, the most stable speeds are at integral multiples of the natural frequency of the system. The new theory predicts a set of stable speeds at fractions of the damped natural frequency. For small damping, a subset of these stable speeds is approximately the same as predicted by the traditional theory. From a practical point of view, the most important prediction of our new theory is that the number of optimally stable speeds doubles as the ratio r of time per revolution of tool contact with the material to the spindle period becomes small, i.e. $r \ll 1$. Co-authors on this work are M.A. Davies, J.R. Pratt, and B. Dutterer of the NIST Manufacturing Engineering Laboratory.

Devaney J.E., Hagedorn, J.G., Nicolas, O.P., Garg, G., Samson, A., Michel, M.	A Genetic Programming Ecosystem	15th Annual International Parallel & Distributed Processing Symposium, IPDPS 2001, Workshop on Biologically
---	---------------------------------	---

Inspired Solutions to Parallel Processing Problems

Algorithms are needed in every aspect of parallel computing. Genetic Programming is an evolutionary technique for automating the design of algorithms through iterative steps of mutation and crossover operations on an initial population of randomly generated computer programs. This paper describes a parallel genetic programming (GP) system inspired by the symbiogenesis model of evolution, wherein new organisms are generated through the absorption of different life-forms in addition to the usual mutation and crossover operations. Different organisms are expressed in this GP system through multiple program representations. Two program representations considered in this paper are the procedural representation (PR) and the tree representation (TR). Populations of these representations evolve separately. Individuals in each population migrate to the other and participate in evolution via representation change algorithms. Parallelism is achieved through use of the AutoMap/AutoLink MPI library. The differences in the locality properties of the representations serve as a source of new ideas for creating the final algorithm.

Dienstfrey, A., Greengard, L.	Analytic Continuation, Singular Value Expansions, and Kramers-Kronig Analysis	Inverse Problems	3/30/01
-------------------------------	---	------------------	---------

We describe a systematic approach to the recovery of a function analytic in the upper half plane, $\{C\}^+$, from measurements over a finite interval on the real axis, $D \subset R$. Analytic continuation problems of this type are well-known to be ill-posed. Thus, the best one can hope for is a simple, linear procedure which exposes this underlying difficulty and solves the problem in a least squares sense. To accomplish this, we first construct an explicit analytic approximation of the desired function and recast the continuation problem in terms of a "residual function" defined on the measurement window D itself. The resulting procedure is robust in the presence of noise and we demonstrate its performance with some numerical experiments.

Eggleston, J. J., McFadden, G. B., Voorhees, P. W.	A Phase-Field Model for Highly Anisotropic Interfacial Energy	NISTIR 6706 and Physica D	1/15/01
--	---	---------------------------	---------

A computationally efficient phase-field model is developed for two-phase systems with anisotropic interfacial energy. The approach allows for anisotropies sufficiently high that the interface has corners or missing crystallographic orientations. The method employs a regularization that enforces local equilibrium at the corners and allows corners to be added or removed without explicitly tracking their location. Numerical simulations for various degrees of anisotropy were performed and they show excellent agreement with analytical equilibrium shapes and yield accurate time dependent solutions for a wide variety of initial conditions.

Fenimore, C., Floyd, M.	Digital Cinema 2001 Conference Proceedings	NISTIR 6591	1/11/01
-------------------------	--	-------------	---------

This Proceeding provides papers and slides for the presentations at digital Cinema 2001 Conference. The conference addresses a variety of business and technical issues arising in developing digital cinema. Speakers address: on overview of digital cinema, studio and theater owners perspectives, compression, standards, measurement of projected image quality, digital rights management, storage and other topics.

Fiscus, J.G., Doddington, G.R.	Results of the 1999 Topic Detection and	6th International Conference on Spoken	
--------------------------------	---	--	--

Tracking Evaluation in Mandarin and English

Language Processing (ICSLP) Beijing, China

The National Institute of Standards and Technology (NIST) administered the second open evaluation of Topic Detection and Tracking (TDT) technologies in 1999. The TDT project supports development of technologies that automatically organize event-related news stories. The program leverages expertise in core technologies, Automatic Speech Recognition (ASR), Document Retrieval (DR), and Machine Translation (MT) to build the TDT technologies. The 1999 TDT project extended the 1998 TDT project in two dimensions, first by adding Mandarin Chinese audio and text sources and second by adding two new evaluation tasks. Through experimental controls and conditioned analysis of system performance, the 1999 evaluation yielded numerous insights into the effects of multilingual texts on TDT technologies. Three notable generalizations arise from the evaluation: (1) English and Mandarin story segmentation performance is similar, (2) cross-lingual topic tracking performance is 44% worse than monolingual tracking, and (3) multilingual topic detection performance is 37% worse than monolingual topic detection.

Fong, E. N., Ivezic, N., Rhodes, T. R., Peng, Y.

Agent-Based Services for B2B Electronic Commerce

Conference Proceedings of SPIE (International Society for Optical Engineering) – Session VV13

The potential of agent-based systems has not been realized yet, in part, because of the lack of understanding how the agent technology support industrial needs and emerging standards. The area of business-to-business electronic commerce (b2b e-commerce) is one of the most rapidly developing sectors of industry with huge impact on manufacturing practices. Our intent in this paper is to investigate the current state of agent technology and the feasibility of applying agent-based computing to b2b e-commerce in the circuit board manufacturing sector. We identify critical tasks and opportunities in the b2b e-commerce area where agent-based services can best be deployed. We describe an implemented agent-based system to facilitate the bidding process for printed circuit board manufacturing and assembly. These activities are taking place within the Internet Commerce for Manufacturing (ICM) project, the NIST-sponsored project working with industry to create an environment where small manufacturers of mechanical and electronic components may participate competitively in virtual enterprises that manufacture printed circuit assemblies.

Frankel, S.

An Introduction to IPsec (Internet Protocol Security)

ITL Bulletin, March 2001

3/30/01

IPsec (Internet Protocol Security) is an attempt to utilize cryptographic techniques in a global solution to the problem of Internet security. Rather than requiring each email program or Web browser to implement its own security mechanisms, IPsec involves a change to the underlying networking facilities that are used by every application. It also allows network managers to apply protection to network traffic without involving the end users. This security bulletin discusses the types of protection provided by IPsec, its major components, current uses, and future potential.

Gallagher, L.J., Offutt, A.J.

Integration Testing of Object-Oriented Components Using Finite State Machines

Software Testing, Verification and Reliability Wiley Inter Science, John Wiley & Sons, Ltd.

In object-oriented terms, integration testing tries to ensure that messages from objects in one class or component are sent and received in

described in this report begins with adding perturbation terms to the characterization coefficients of the geometric-thermal model. These coefficients are estimated by an “inverse” process, using residual systematic errors, determined from part measurements on a coordinate measuring machine. The main tool used in identifying the perturbation terms is called a generalized or pseudo inverse matrix. This matrix is applied to the residual error vector to obtain a “best” approximate solution to the least squares problem.

Golmie, N., Van Dyck, R.E., Soltanian, A., El Bakkouri, I.	Performance Evaluation of Bluetooth and IEEE 802.11 Devices Operating in the 2.4 GHz ISM Band	Proceedings of the 7th Annual International Conference on Mobile Computing and Networking (MobiCom) 2001, Rome, Italy, July 16-21, 2001
--	---	---

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 co-located in the same environment. The main goal of this paper is to present a performance evaluation of these radio systems sharing the same air space based on an integrated MAC and PHY simulation model. Our results focus on the impact of interference on Bluetooth and IEEE 802.11. We use several simulation scenarios and measure performance in terms of packet loss, residual number of errors, and access delay.

Gray, M.M.	Code for Information Interchange	A Century of Excellence in Measurements, Standards, and Technology: Selected Publications of NBS/NIST, 1901-2000, D. Lide, Ed., pp. 172-173.	1/31/01
------------	----------------------------------	--	---------

Grother, P., Casasent, D.	New MTF Measurement Method for Electrically Addressed SLMs	Applied Optics
---------------------------	--	----------------

The modulation transfer function (MTF) using amplitude modulation (mA) data is a vital coherent optical performance measure for a spatial light modulator (SLM). A new image plane MTF (amplitude MTF) measurement method is presented for electrically addressed SLMs. It involves digital analysis of the output image of a square-wave pattern written onto the SLM. Modulation level effects are also addressed. Optical laboratory results are presented for two liquid crystal SLMs. The need to consider amplitude not intensity modulation (when coherent optical processing applications are considered) is noted in terms of SLM biasing.

Gurski, K. F., Pego, R. L.	Normal Modes for a Stratified Viscous Fluid Layer	Proceedings of the Royal Society of Edinburgh
----------------------------	---	---

We consider internal gravity waves in a stratified fluid layer with rigid horizontal boundaries and periodic boundary conditions on the sides at constant temperature with a small constant viscosity, modeled using the incompressible Navier-Stokes equations. Using operator-theoretic methods to study the damping rates of internal waves, we prove there are non-oscillatory wave modes with arbitrarily small damping rates. We provide an asymptotic approximation for these non-oscillatory modes. Additionally we find that the eigenvalues for damped oscillations are in an explicitly describable half ring.

Gutta, S., Huang, J., Phillips, P.J., Wechsler, H. Mixture of Experts for Classification of Gender, Ethnic Origin, and Pose of Human Faces IEEE Transactions Neural Networks

In this paper we describe the application of mixtures of experts on gender and ethnic classification of human faces, and pose classification, and show their feasibility on the FERET database of facial images. The FERET database allows us to demonstrate performance on hundreds or thousands of images. The mixture of experts is implemented using the "divide and conquer" modularity principle with respect to the granularity and/or the locality of information. The mixture of experts consists of an ensembles of radial basis functions (RBF). Inductive decision trees (DT) and support vector machines (SVM) implement the "gating network" components for deciding which of the experts should be used to determine the classification output and to restrict the support of the input space. Both the Ensemble of RBFs (ERBF) and SVM use the RBF kernel ("expert") for gating the inputs. Our experimental results yield an average accuracy rate of 96% on gender classification and 92% on ethnic classification using the ERBF / DT approach from frontal face images, while the SVM yield 100% on pose classification.

Harman, D., Braschler, M., Hess, M., Kluck, M., Peters, C., Schauble, P., Sheridan, P. CLIR Evaluation at TREC Proceedings of the Cross-Language Evaluation ForumSpringer – Lecture Notes in Computer Science Series

Starting in 1997, the National Institute of Standards and Technology conducted 3 years of evaluation of cross-language information retrieval systems in the Text REtrieval Conference (TREC). Twenty-two participating systems used topics (test questions) in one language to retrieve documents written in English, French, German, and Italian. A large-scale multilingual test collection has been built and a new technique for building such a collection in a distributed manner was devised.

Hersch, W., Over, P. TREC-9 Interactive Track Report Included in NIST SP 500- , TREC-9

The TREC-9 Interactive Track has the goal of investigating interactive information retrieval by examining the process as well as the results. In TREC-9, six research groups ran a total of 12 interactive information retrieval (IR) system variants on a shared problem: a fact-finding task, eight questions, and newspaper/newswire documents from the TREC collections. This report summarizes the shared experimental framework, which for TREC-9 was designed to support analysis and comparison of system performance only within sites. The report refers the reader to separate discussions of the experiments performed by each participating group – their hypotheses, experimental systems and results. The papers from each of the participating groups and the raw and evaluated results are available via the TREC home page (trec.nist.gov).

Hogan, M. D., Carnahan, L. J., Carpenter, R. J., Flater, D. W., Fowler, J. E., Frechette, S. P., Gray, M. M., Johnson, L. A., McCabe R. M., Montgomery, D., Radack, S. M., Rosenthal, R., Shakarji, C. M. Information Technology (IT) Measurement and Testing Activities at NIST NIST Journal of Research, Vol. 106, No. 1, January-February 2001 2/28/01

Our high technology society continues to rely more and more upon sophisticated measurements, technical standards, and associated testing

activities. This was true for the industrial society of the 20th century and remains true for the information society of the 21st century. Over the last half of the 20th century, information technology (IT) has been a powerful agent of change in almost every sector of the economy. The complexity and rapidly changing nature of IT have presented unique technical challenges to NIST and to the scientific measurement community in developing a sound measurement and testing infrastructure for IT. This measurement and testing infrastructure for the important non-physical and non-chemical properties associated with complex IT systems is still in an early stage of development. This paper explains key terms and concepts for IT metrology, briefly reviews the history of NBS/NIST in the field of IT, and reviews NIST's current capabilities and work in measurement and testing for IT. It concludes with a look at what is likely to occur in the field of IT over the next ten years and what metrology roles NIST is likely to play.

Jansen, W.A.

A Privilege Management Scheme for Mobile Autonomous Agents Conference,
Agent Systems SEMAS Workshop

In this paper, we describe a general method for controlling the behavior of mobile agent-system entities through allocation of privileges. Privileges refer to policy rules that govern the access and use of computational resources and services. The scheme is based on the capability of most mobile agent systems to extend the platform processing environment and the use of two forms of privilege management certificates: attribute certificates and policy certificates. Privilege management certificates are digitally signed objects that allow various policy setting principles to govern the activities of mobile agents through selective privilege assignment. This approach overcomes a number of problems in existing agent systems and provides a means for attaining improved interoperability of agent systems designed and implemented independently by different manufacturers. We also describe applying the scheme to Java-base agent systems.

Kacker, R.N.

Towards a Simpler Bayesian Guide to the Expression of Uncertainty in Measurement Proceedings of the Measurement Science Conference 2001

The impact of the Guide to Expression of Uncertainty in Measurement is spreading from the national measurement institutes to the industrial measurement laboratories. The Guide is written such that it can be loosely interpreted either from the frequentist or the Bayesian viewpoint. This paper presents a coherent interpretation of The Guide from a Bayesian viewpoint. This interpretation links The Guide with Bayesian statistics. This linkage should make the Guide more appealing to those interested in philosophical coherence. The Guide is not limited by the proposed interpretation. An immediate benefit of the Bayesian viewpoint is that it leads to a simpler and more reliable alternative to using a t-distribution with effective degrees of freedom as determined by Welch-Satterthwaite formula to account for a small number of measurements.

Ketcham, P.M., Feder, D.L., Clark,
C.W., Satterfield, S.G., Griffin, T.J.,
George, W.L., Reinhardt, W.

Volume Visualization of Bose-Einstein
Condensates NISTIR 6739

An active area of research in the physics community is the study of Bose-Einstein condensation. Theoretical aspects of Bose-Einstein condensates are investigated by conducting computer simulations of their behavior. Scientific visualization techniques are employed in order to examine the large amount of data generated by simulation. Visualization of this simulated data demonstrates theoretical predictions, influences the research process, accelerates scientific understanding, and stimulates further investigation.

Kirsch, R.A. Computer Development at the National Bureau of Standards A Century of Excellence in Measurements, Standards, and Technology: Selected Publications of NBS/NIST, 1901-2000, D. Lide, Ed., pp.86-89. 1/31/01

Kuhn, D.R. A Hybrid Authentication Protocol Using Quantum Entanglement and Symmetric Cryptography NISTIR 6741

This paper presents a hybrid cryptographic protocol, using quantum and classical resources, for authentication and authorization in a network. One or more trusted servers distribute streams of entangled photons to individual resources that seek to communicate. It is assumed that each resource shares a previously distributed secret key with the trusted server, and that resources can communicate with the server using both classical and quantum channels. Resources do not share secret keys with each other, so that the key distribution problem for the network is reduced from to . Some advantages of the protocol are that it avoids the requirement for timestamps used in classical protocols, guarantees that the trusted server cannot know the authentication key, can provide resistance to multiple photon attacks [Brassard et al., 1999; Felix et al., 2001] and can be used with BB84 [Bennett84] or other quantum key distribution protocols.

Langer, S.A., Carter, W.C., Fuller, E.R. OOF: Image-Based Finite Element Analysis of Material Microstructure IEEE Computing in Science and Engineering

The determination of macroscopic properties of a material given its microscopic structure is of fundamental importance to materials science. We present an overview of two public domain programs which jointly predict macroscopic behavior, starting from an image of the microstructure and ending with results from finite element calculations. The first program reads an image and assigns material properties to microscopic features. The second program reads the output of the first and performs virtual tests to deduce macroscopic behavior.

Lavery, J.E., Gilsinn, D.E. Multiresolution Representation of Terrain By Trends in Approximation Theory Cubic LI Splines (ed)Kirill Kopotun, Tom Lyche and Mike Neamtu Vanderbilt Univ. Press

Cubic L1 and L2 interpolating splines based on C1 smooth piecewise cubic Sibson elements on a tensor-product grid are investigated. Computational tests were carried out for a 102.4 km area of Fort Hood, Texas, represented by a 1025 x 1025 set of 100-meter-spacing (posting) DTED1 terrain data obtained from the National Imagery and Mapping Agency. L1 and L2 interpolating splines were calculated for this area using data at coarser spacings of 800 m, 1600 m, 3200 m, 6400 m, 12800 m and 25600 m. The I1 and I2 errors of the L1 spline for a given spacing. In half of the cases, the I error of the L1 spline is smaller than the I error of the corresponding L2 spline. In the other half of the cases, it is larger. Overall, this evidence indicates that L1 splines preserve shape better for this terrain data set than do L2 splines.

Lavery, J.E., Gilsinn, D.E. Multiresolution Representation of Urban Terrain By LI Splines, L2 Splines, and Proceedings 22nd Army Science Conference, Baltimore, Maryland 12/11/00

Piecewise Planar Surfaces

Cubic L1 and L2 interpolating splines based on C1 smooth piecewise cubic Sibson elements on a tensor-product grid are investigated. Computational tests were carried out for an 800 m by 800 m area of Baltimore, MD represented by an 800 x 801 set of 100-meter-spacing (posting) data set. Interpolating splines at coarser resolutions were computed along with L_1 , L_2 and L_∞ errors relative to the 800 m by 800 m data set. Piecewise planar interpolations at the coarser resolutions were also computed along with the above errors for comparative purposes.

Lennon, E. B., Simon, K.K., Helfer, M. ITL Technical Accomplishments 2000 NISTIR 6558 10/31/00

The ITL Technical Accomplishments 2000 report presents the achievements and highlights of NIST's Information Technology Laboratory (ITL) during FY 2000. Technical projects in eight divisions are described, followed by industry interactions, international activities, staff recognition, and service to the NIST staff and public.

Lyon, G.E. Comparison of Two Scalability Tests Information Processing Letters

When a computer system is expensive to use or is not often available, one may want to tune software for it via analytical models that run on more common, less costly machines. In contrast, if the host system is readily available, the attraction of analytical models is far less. One instead employs the actual system, testing and tuning its software empirically. Two examples of code scalability testing illustrate how these approaches differ in objectives and costs, and, how they complement each other in usefulness.

Lyon, G.E., Tang, H.C. Assurance Hierarchies in B2C Electronic Commerce NISTIR 6713 2/14/01

Electronic commerce (e-commerce) is defined as a broad, interdisciplinary field addressing the automation of business practices via open, globally spanning, Internet public access. E-commerce shows great promise in improving the efficiency of current business practices and in fostering completely new forms of business transactions. However, business concerns must be addressed in pursuing commercial objectives on the Internet. Assurance is among these: Identity, trust, and reputation are essential elements in any business deal. Unfortunately, with physical presence lacking, Internet business participants must rely upon other means to establish identity and assess reputation. The discussion explores frameworks for establishing assurance within constraints of the e-commerce process.

Marbukh, V. Network Management under Incomplete Information on the Operational Environment Proceedings of International Symposium on Information Theory & Applications (ISITA 2000), Honolulu, HI, 11/5-8/00 11/5/00

This paper proposes an approach to network management under incomplete information on the operational environment. The approach employs a combination of the minimax and Bayes' methodologies for making network management decisions under uncertainty. As an example we consider loss networks.

McFadden, G.B., Wheeler, A.A. On the Gibbs Adsorption Equation for Diffuse Interface Models NISTIR 6732 and Proceedings of the Royal Society of London

Mitchell, W.F.	A Refinement-Tree Based Partitioning Method for Adaptively Refined Grids	Accepted by Proceedings of the Tenth SIAM Conference on Parallel Processing for Scientific Computing	
<p>The partitioning of an adaptive grid for distribution over parallel processors is considered in the context of adaptive multilevel methods for solving partial differential equations. A k-way refinement-tree based partitioning method is presented. Numerical results comparing it with recursive coordinate bisection and a multilevel diffusive method from ParMETIS show that it runs an order of magnitude faster than the multilevel diffusive method and produces partitions of similar quality.</p>			
Morse, E.L., Steves, M.P.	A Visualization Approach to Dealing with Log Data	Website of the Workshop on Data Log Mining of the Computer Supported Cooperative Work Conference	
<p>The CollabLogger is a visual tool that supports usability analyses of human-computer interaction in a team environment. Participants in our computer-mediated activity were engaged in a small-scale manufacturing testbed project. Interactions of the group were mediated by Teamwave Workplace and the members performed both synchronous and asynchronous activities depending on their availability, project requirements, and due to chance meetings in the collaborative space. The software was instrumented to log users' interactions with the system and each other. The CollabLogger addresses the problem of helping investigators analyze the volumes of log data that groupware tools can generate. Visual tools are powerful when large amounts of diverse data present themselves. The place-based collaboration environment offered by Teamwave Workplace provided a level of organization that allowed us to create a visual interface with which to perform exploratory sequential data analysis. Preliminary use of the tool shows that usability engineers can employ the visual display to form hypotheses about subject's interactions with the GUI interface and with each other.</p>			
O'Leary, D.	Methods of Conjugate Gradients for Solving Linear Systems	A Century of Excellence in Measurements, Standards, and Technology: Selected Publications of NBS/NIST, 1901-2000, D. Lide, Ed., pp. 81-85.	1/31/01
O'Leary, D.	Iteration Method for the Solution of the Eigenvalue Problem of Linear Differential and Integral Operators	A Century of Excellence in Measurements, Standards, and Technology: Selected Publications of NBS/NIST, 1901-2000, D. Lide, Ed., pp. 77-80.	1/31/01
Phillips, P.J., Newton, E.M.	Meta-Analysis of Face Recognition Algorithms	NISTIR 6719 and Proceedings of International Conference on Computer	

Micromagnetic Model to Non-Uniform Thickness

A two-dimensional micromagnetic model is extended to support simulation of films with non-uniform thickness. Zeeman and crystalline anisotropy energies are scaled by the local thickness, and exchange interaction between neighbor elements is scaled by the thickness of the thinner element. The self-magnetostatic energy is computed by scaling the moment of each calculation element by the local thickness, and adding a local correction to the out-of-plane field to properly balance the demagnetization factors of each element. The calculation of the magnetostatic field for a $10 \times 10 \times 1$ oblate spheroid is shown to be more accurate by the non-uniform thickness model than by a uniform thickness model. With the extended model a $530 \times 130 \times 10$ nm film in the shape of a truncated pyramid with tapering over the 15 nm nearest the edges is shown to have smaller switching field and different reversal mechanism compared with uniform thickness films of similar size and shape.

Prins, J. NIST/SEMATECH Engineering Statistics Handbook Chapter 6: Process or Product Monitoring and Control Web

This chapter presents techniques for monitoring and controlling processes and signaling when corrective actions are necessary. It covers both statistical process control (SPC) and statistical quality (SQC). SPC is based on a comparison of what is happening today with what happened previously to guarantee that process has not degraded. SQC is a technique for inspecting enough product from given lots to ensure a specified quality level.

Remington, K.A., Pozo, R. NIST Sparse BLAS User's Guide NISTIR

This document provides a guide and reference manual for a portable numerical library for sparse matrix computations. These Basic Linear Algebra Subprograms (BLAS) provide kernels for forming sparse matrix products (of the form $C = aAB + bC$, where a and b are scalars, B and C are dense matrices, and A is a sparse matrix) and solution of triangular systems with left and right scaling ($C = aLATRB + bC$, where a and b are scalars, L and T are diagonal matrices, T is the conceptual inverse of a triangular sparse system, and B and C are dense matrices). Complete function listings for the ANSI C programming language are provided.

Ressler, S. A Web-Based 3D Glossary for Anthropometric Landmarks HCI International 2001, New Orleans, LA, August 5-10, 2001

We have created a visual 3D anthropometric landmark glossary usable over the Web. Implemented using VRML, the Virtual Reality Modeling Language, users may easily locate and determine the names of these landmarks. Landmarks are visualized as small spheres located over the body. Users can select the landmark name and the display is adjusted to place the viewer in front of that location. In addition users can select from among different landmark nomenclatures. The landmarks also highlight when selected, giving visual feedback. In addition a number of reference planes, such as the Frankfort plane and the coronal, sagittal and transverse planes can be turned on or off. Additional display controls are available via a movable control panel. The initial set of landmark names comes from the CAESAR (Civilian American and European Surface Anthropometry Resource) project. Three versions of the system have been implemented. The first is a head only model. Names for the head model are displayed simply by moving the cursor over the spheres and no selection is needed. The other two versions, requiring the user to click a selection, function identically and illustrate the landmarks for a standing male and for a male in a wheel chair.

Ressler, S., Antonishek, B., Wang, Q., Godil, A. Integrating Active Tangible Devices with a Synthetic Environment for Collaborative Engineering Web3D 2001 Symposium, Paderborn, Germany, February 19-22, 2001 2/19/01

This paper describes the creation of an environment for collaborative engineering. In which the goal is to improve the user interface by using haptic manipulation with synthetic environments. We have integrated a multiuser synthetic environment with physical robotic devices to create a work environment. These devices can move under computer control or may be manipulated directly by the user. The work environment represents objects from the application domain such as a building construction environment or manufacturing cell. Collaborating engineers can discuss object interactions, such as crane planning or building placement using this environment. A physical representation of a work environment enables the user to perform direct, tangible manipulations of the devices which are mirrored in the synthetic environment. The direct physical manipulation of robotic devices offers the users a natural and efficient method of interacting with the synthetic environment.

Roberts, J.W., Kelley, E.F. Measurements of Static Noise in Display Images SPIE Electronic Imaging '01 Conference

The appearance of noise on a display is an important usability issue. Sources of noise include electrical interference, display driver artifacts, resampling artifacts, transmission artifacts, compression artifacts, and any intrinsic noise artifacts produced within a display device. Issues for the severity of the noise problem include total magnitude of noise, noise spatial frequencies, proximity of the noise spatial frequencies to the spatial frequencies of the desired information content and the human-eye response to that information content, uniformity of the distribution of noise, and appearance of any visible or regular patterns in the noise. Whatever the source, an accurate method to measure noise may be required to properly assess the influence of the noise. We investigate the intricacies of using a digital camera to accurately measure noise in a static image on a flat panel display (FPD). The electro-optical transfer function of the FPD is measured. A known noise pattern is displayed and measured using the digital camera whereby the predicted noise is compared to the measured noise. Complications and limitations in the metrology will be discussed.

Rosenthal, L.S., Brady, M.C. What is this Thing Called Conformance? ITL Bulletin, January 2001, and XML 2000 Conference Proceedings, December 2000 1/9/01

XML developers claim they do it. OASIS, NIST, and W3C are building it. And, standards often require it. What is it? Conformance is usually defined as a way to determine if an implementation faithfully meets the requirements of a standard or specification. There are many types of testing including testing for performance, robustness, behavior, functions and interoperability. Although conformance testing may include some of these kinds of tests, it has one fundamental difference -- the requirements or criteria for conformance must be specified in the standard or specification. Conformance testing is meant to provide the software developers and users of conforming products some assurance or confidence that the product behaves as expected, performs functions in a known manner, or has an interface or format that is known. Determining whether a product faithfully implements the W3C Recommendations will be essential to creating robust, interoperable solutions. In this session, we will present an overview of conformance including what it is, how it works, and what are the benefits. Following the general conformance discussion will be specific examples from available conformance test suites including, XML, DOM, and XSLT. In addition, we will discuss particular problems that we have uncovered as a result of developing the tests, and give an indication of how various

implementations fare against the available test suites.

Rossiter, W.J., Jr., Vangel, M.G., Anodic Stripping Voltammetry for NISTIR
McKnight, M.E., Signor, A., Byrd, W.E. Determining Lead in Household Paint: A
Laboratory Evaluation

A laboratory study was conducted to evaluate the reliability of ultrasonic extraction-anodic stripping voltammetry (UE/ASV) for determining the lead levels of laboratory-prepared paint films when tests were performed by certified lead inspectors trained to conduct UE/ASV testing. Two commercial, factory-calibrated UE/ASV apparatuses from the same supplier were purchased and used to conduct an experiment investigating the effects of lead level, apparatus, lead pigment type, operator, paint-film substrate, and overlayer applied to the lead-based paint film. Test panels, with either white lead (i.e., basic lead carbonate) or lead chromate pigments, had 10 lead levels ranging from 0 mg/cm² to 3.5 mg/cm². The lead-based paint films were adhered to steel or plaster substrates, which were considered for experimental design purposes to be difficult or easy to sample, respectively. The overlayers were either an oil-based paint applied thick (about 0.75 mm to 1.4 mm) or a latex paint applied thin (about 0.13 mm to 0.28 mm). The five operators were trained by a UE/ASV supplier's representative to conduct the tests using a written protocol developed from the supplier's instructions. The study showed that one of the two apparatuses was in calibration, whereas the response of the second apparatuses was low at the lower lead concentrations used to check the instrument calibration. Consequently, the data were analyzed both as "unadjusted for calibration" and "adjusted for calibration." Lead levels determined by the UE/ASV tests were often considerably less than the lead levels in the test panels. Depending on the combination of five experimental factors—apparatus, operator, lead pigment type, substrate type, and overlayer—the recovered lead for the data adjusted for calibration ranged from 28 % to 94 %, with the median recovery being 63 %. These findings are in sharp contrast with previously published results of an UE/ASV field study in which lead recoveries ASV generally ranged from 75 % to more than 100 %. A key contributor to the low lead recoveries in the present study appeared to be incomplete lead solubilization during paint specimen sonication. The major experimental factor affecting UE/ASV response was overlayer, with test panels having thick-oil overlayers yielding lower lead recoveries than those with thin-latex overlayers. It may have been that thick-oil overlayers were more difficult to sonicate, and/or grind before sonication, than thin-latex overlayers. Effects of the other experimental factors on UE/ASV response were considered primarily for the calibration-adjusted data. Operator and substrate factors were found to have a significant effect; whereas no effects were found for lead pigment type or apparatus.

Scholtz, J.C. A Research Agenda for Context-Aware Human Computer Interaction Journal
Computing

This paper discusses a broader sense of context for use in context-aware computing. Three types of context are presented: the user's context - task, social situation, emotional state, location; the environmental context - noise, light, indoors/outdoors, cold/hot; the computing resource context - energy left, computational power, input capabilities, output capabilities. Evaluation methodologies for identifying various aspects of context, interpreting context and adapting the interaction methodology based on context are presented.

Scholtz, J.C., Laskowski, S.J., Morse, Quantifying Usability: The Industry "Interacting With Computers" special
E.L., Wichansky, A., Butler, K. Usability Reporting Project edition based on submissions of the
Conference on Universal Usability

Usability is an important concept for both the users of software and the producers of software. But, what exactly is usability? How can usability be measured or quantified? How much does usability testing save or cost? Can an environment be created that encourages incorporating usability engineering into the software development lifecycle? The Industry USability Reporting (IUSR) Project seeks to help potential corporate consumers of software obtain information about the usability of supplier products, to measure the benefit of more usable software, and to increase communication about usability needs between consumers and suppliers. There are two parts to the IUSR Project: 1) a proposed format for sharing usability information and a pilot study in which both supplier (the developer) and consumer (the purchaser) companies to test the effectiveness of using usability test results as procurement criteria, and 2) a pilot study to verify the usefulness of the reporting format. These are the first steps along a path to creating usability tools and techniques that can serve to increase communications across corporate boundaries.

Sekerka, R.F., Coriell, S.R., Separation of Scales for Growth of an Alloy Metallurgical Transactions A (letters)
 McFadden, G.B. Needle Crystal

We reexamine the problem of a needle crystal (a model for a dendrite primary stalk) having the shape of a paraboloid of revolution growing at constant velocity from a supercooled binary alloy with given bulk concentration and far-field temperature. The coupled problem of thermal and solutal diffusion has been studied by a number of authors, including Ivantsov, Bolling & Tiller, Langer, and Lipton, Glicksman, & Kurz. We discuss the form of the analytical relation between the growth rate and the undercooling. For typical material properties in a metallic system, there is an obvious separation of scales of thermal and solutal effects, and this relation has the form of a doubly sigmoidal function, with a nearly flat intermediate region where the two sigmoids join. To the left of this nearly flat region, the dendrites are 'solutal' with negligible contributions from the thermal field, whereas to the right of this region, they are 'thermal' with the solutal contribution fixed at its value for unit supersaturation.

Sims, J.S., Hagedorn, J.G., Ketcham, Accelerating Scientific Discovery Through NISTIR 6709 and NIST Journal of 1/1/01
 P.M., Satterfield, S.G., Griffin, T.J., Am Computation and Visualization Research, Vol. 105, No. 6,
 Ende, B.A., Hung, H.K., Martys, N.S., November-December 2000
 Bouldin, C.P., Warren, J.A., Feder,
 D.L., Clark, C.W., Fowler, H.A., Filla,
 B.J., Devaney, J.E.

Scientific discovery can be accelerated through computation and visualization. This acceleration results from the synergy of expertise, computing tools and hardware for enabling high-performance computation, information science and visualization that is provided by a team of computation and visualization scientists collaborating in a peer-to-peer effort with the research scientists. In the context of this discussion, {em high performance} refers to capability beyond the current state of the art in desktop computing. To be effective in this arena, a team comprising a critical mass of talent, parallel computing techniques, visualization algorithms, advanced visualization hardware and a recurring investment is required to stay beyond the desktop capabilities. This article describes, through examples, how the Scientific Applications and Visualization Group (SAVG) at NIST has utilized high performance parallel computing and visualization to accelerate scientific discovery. The examples include scientific collaborations that have advanced research in the following areas: (1) Bose-Einstein Condensate Modeling, (2) Fluid Flow in Porous Materials and in Other Complex Geometries, (3) Flows in Suspensions, (4) X-ray Absorption, (5) Dielectric Breakdown Modeling, and (6) Dendritic Growth in Metallic Alloys.

Snouffer, S.R., Lee, A., Oldehoeft, A.E. A Comparison of the Security Requirements NIST SP 800-29 for Cryptographic Modules in FIPS 140-1 and FIPS 140-2

Federal agencies, industry, and the public now rely on cryptography to protect information and communications used in critical infrastructures, electronic commerce, and other application areas. Cryptographic modules are implemented in these products and systems to provide cryptographic services such as confidentiality, integrity, non-repudiation and identification and authentication. A documented methodology for conformance testing through a defined set of security requirements in FIPS 140-1&2 and other cryptographic standards is specified in the Derived Test Requirements. FIPS 140-1 is one of NIST's most successful standards and forms the very foundation of the Cryptographic Module Validation Program. FIPS 140-2 addresses lessons learned from questions and comments and reflects changes in technology. The standard was strengthened, but not changed in focus or emphasis. Also, the standard was minimally restructured to:- Standardize the language and terminology to add clarity and consistency, - Remove redundant and extraneous information to make the standard more concise, and - Revise or remove vague requirements. Finally, a new section was added detailing new types of attacks on cryptographic modules that currently do not have specific testing available. This differences paper summarizes the changes from FIPS 140-1 to FIPS 140-2 and documents the detailed requirements.

Sterling, D.G. Self-Synchronizing Ergodic Maps and Chaotic Modulation IEEE Transactions on Circuits and Systems - Part I

Self-synchronizing chaotic systems can be used as synchronous pseudo-random sequence generators, though physical applications have been limited by the sensitivity of the synchronous state to noise. Using two separate time scales in conjunction with a digital filter suppresses the noise in the coupling signal. We find this gives stable synchronous motion even for signal-to-noise ratios less than 1. As an application of these pseudo-random sequence generators we propose a chaotic modulation scheme based on ergodic maps. We characterize the performance of this system by bounding the mean synchronization time and estimating the resulting bit energy.

Stoneburner, G.R., Hayden, C., Feringa, A. Engineering Principles for IT Security NIST SP 800-27

The Engineering Principles for Information Technology (IT) Security (EP-ITS) presents a list of system-level security principles to be considered in the design, development, and operation of an information system. This document is to be used by IT security stakeholders and the principles introduced can be applied to general support systems and major applications. EP-ITS presents principles that apply to all systems, not ones tied to specific technology areas. These principles provide a foundation upon which a more consistent and structured approach to the design, development, and implementation of IT security capabilities can be constructed. While the primary focus of these principles remains on the implementation of technical countermeasures, these principles highlight the fact that, to be effective, a system security design should also consider non-technical issues, such as policy, operational procedures, and user education.

Stutzman, P.E., Leigh, S. Compositional Analysis of NIST Reference Material Clinker 8486 Accuracy in Posder Diffraction Conference, NIST, April 2001 3/20/01

Certification of the phase compositions of the NIST Reference Clinkers often is based upon more than one independent method. The current certificate values were established using an optical microscope examination, and additional microscope data taken from an ASTM C 1356

round robin. The X-ray powder diffraction (XRD) study provides the second, independent estimate of the phase abundances, with the experiment designed to evaluate inter- and intra-vial homogeneity. Reitveld analysis of the powder diffraction patterns allowed calculation of a set of best-fit reference patterns and their scale factors. Because of significant contrast in the linear absorption coefficients of ferrite and periclase relative to the estimated mean matrix linear absorption coefficient, the scale factors were adjusted for microabsorption effects using the and the adjusted scale factors used to calculate phase abundance. The XRD data agree with the optical data with the exception of aluminate. This disagreement may reflect the difficulty in resolving this finely-crystalline phase using the optical microscope. The XRD data did show greater precision than replicate measurements by microscopy.

Measurements from different sources, laboratories, instruments, and from different methods can exhibit significant between-method variability, as well as distinct within-method variances. The two data sets are treated using three methods to establish the best-consensus values and to provide meaningful uncertainties. While the mean values of the individual phase abundances do not vary, the 95 % uncertainty level values do. One method of combining the data sets was favored as this method produces a weighted mean whose weighting scheme does not necessarily skew the consensus value in the direction of the large number of XRD values.

Tang, X., Zheng, J.	Reflectance Calibration Standard for Optical Discs	Proceedings of Optical Data Storage Topical Meeting 2001, Santa Fe, New Mexico, April 22-25, 2001	4/22/01
---------------------	--	---	---------

An accurate method for the determination of reflectance of reference discs has been developed at NIST. The discs can be used as a traceable industry standard in the calibration of optical disc testing equipment.

Toth, P.R.	Understanding the Common Criteria Evaluation and Validation Scheme	ITL Bulletin, October 2000	10/5/00
------------	--	----------------------------	---------

This ITL Bulletin describes the Common Criteria Evaluation and Validation Scheme.

Van Dyck, Robert E.	Classified Zerotree Wavelet Image Coding and Adaptive Packetization for Low Bit Rate Transport	IEEE Transactions on Circuits and Systems for Video Technology	
---------------------	--	--	--

In this paper, we suggest a novel robust image coding and adaptive packetization algorithm suitable for very low bit rate transport. This algorithm can be applied to any zerotree-based encoder such as the embedded zerotree wavelet coder of Shapiro and set partitioning in hierarchical trees by Said and Pearlman. We propose a very explicit segmentation and packetization method of an image bit stream, where the lowest frequency subband is separately encoded from the higher frequency subbands for unequal protection over a noisy channel. The trees in the higher frequency subbands are split, classified, and assembled for efficient image coding and packetization according to their initial threshold and subband. The use of these classified trees enables one to make robust packets, while giving priority to some packets. Each packet has a different initial threshold and can be decoded independently. In spite of relatively heavy overhead for packetization, our algorithm is comparable to the original zerotree-based image coders used in ours at low bit rates. Additionally, simulation results show that the new method is resilient under severe packet losses.

Van Vaerenbergh, S., Coriell, S.R., McFadden, G.B.	Morphological Stability of a Binary Alloy: Temperature-Dependent Diffusivity	NISTIR 6586 and Journal of Crystal Growth	11/17/01
--	--	---	----------

The effect of the temperature dependence of the diffusion coefficient on the morphological stability of a binary alloy during directional solidification is treated by a linear stability analysis. The Soret effect is also included in the analysis. Specific calculations are carried out for a tin alloy containing silver for which the diffusion coefficient has a linear dependence on temperature. Although the temperature dependence of the diffusion coefficient has little effect on the critical concentration for the onset of morphological stability, it causes a significant effect on the wavelength at the onset of instability.

Witzgall, C.

Paths, Trees, and Flowers

A Century of Excellence in
Measurements, Standards, and
Technology: Selected Publications of
NBS/NIST, 1901-2000, D. Lide, Ed., pp.
140-144.

1/31/01