

Information Technology Laboratory Newsletter

INSIDE THIS ISSUE

ITL Announces the Winner of the Secure Hash Algorithm (SHA)-3 Competition

Handbook of Mathematical Functions Sees 300th Citation

ITL Awards Pilot Projects Grants to Promote Online Security and Privacy

ITL Staff Recognition

Selected New Publications

Upcoming Technical Conferences



ITL SHA-3 Competition Team: Back Row (L-R): Donna Dodson, Sara Caswell, Morris Dworkin, John Kelsey, Meltem Sönmez Turan (NIST Associate), Quynh Dang, Andrew Regenscheid, Ray Perlner. Seated (L-R): Elaine Barker, Shujen Chang, William Burr (NIST Associate), Lily Chen, Rene Peralta. Not pictured: Lawrence Bassham, Donghoon Chang (NIST Associate), James Nechvatal, Souradyuti Paul (NIST Associate), and William (Tim) Polk.

Credit: Murugiah Souppaya (NIST)

November—December 2012

Issue 120

ITL Announces the Winner of the Secure Hash Algorithm (SHA)-3 Competition

On October 2, 2012, ITL announced KECCAK (Ke-tchak) as the winner of the [SHA-3 Cryptographic Hash Algorithm competition](#) and officially ended the five-year "SHA-3" competition. KECCAK was designed by a team of cryptographers from Belgium and Italy; they are:

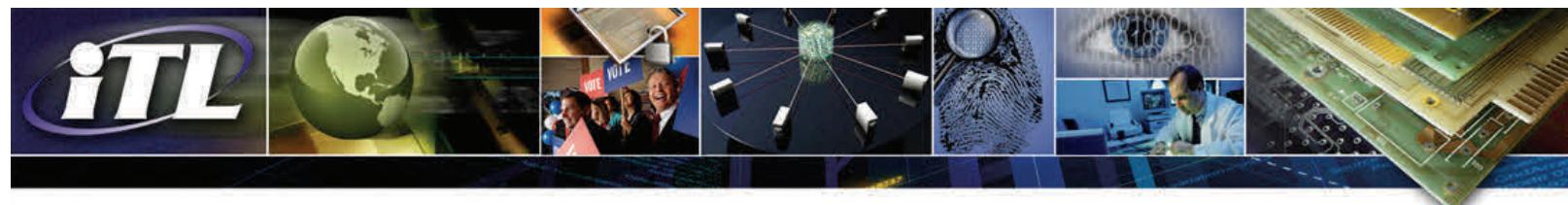
Guido Bertoni (Italy) of STMicroelectronics;
Joan Daemen (Belgium) of STMicroelectronics;
Michaël Peeters (Belgium) of NXP Semiconductors; and
Gilles Van Assche (Belgium) of STMicroelectronics.

KECCAK will become ITL's new SHA-3 hash algorithm, and will augment the hash algorithms currently specified in Federal Information Processing Standard (FIPS) 180-4, *Secure Hash Standard (SHS)*.

ITL announced the SHA-3 competition on November 2, 2007, in response to advances in the cryptanalysis of hash algorithms. ITL received 64 submissions from cryptographers around the world by October 2008, and announced 51 first-round candidates in December 2008, 14 second-round candidates in July 2009, and 5 finalists – BLAKE, Grøstl, JH, KECCAK, and Skein, on December 9, 2010.

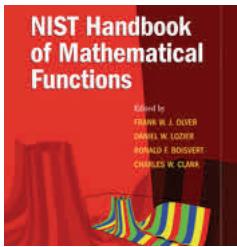
The cryptographic community provided an enormous amount of expert feedback throughout the competition. ITL also hosted three open candidate conferences to obtain public feedback. Based on the public comments and internal review, ITL selected KECCAK as the winner of the SHA-3 competition.

A new report summarizes the evaluation of the five finalists and the selection of the SHA-3 winner. [NISTIR 7896, Third-Round Report of the SHA-3 Cryptographic Hash Competition](#), gives a detailed account of the strengths and weaknesses of the five finalists and the reasons for the selection of the winning candidate.



Handbook of Mathematical Functions Sees 300th Citation

The NIST Handbook of Mathematical Functions, published by Cambridge University Press in May 2010, has passed the 300 citation mark on [Google Scholar](#). The Handbook provides a succinct reference on the properties of the special functions of applied mathematics, which are a staple of mathematical modeling in many fields. Recent citations have come from published work on light scattering, instabilities in rocks, cosmology, elementary quantum systems, quantum field theory, general relativity, statistical mechanics, nanophotonics, and search algorithms. The NIST [Digital Library of Mathematical Functions \(DLMF\)](#), a parallel free online resource, has satisfied more than 4 million full-page requests from more than 520,000 users over the same 28-month period.



The main goal of the DLMF project, conceived nearly 15 years ago and carried out by ITL and the NIST Physical Measurement Laboratory, was to develop a 21st century successor to the legendary Handbook of Mathematical Functions, a classic 1964 NBS publication edited by Milton Abramowitz and Irene Stegun (A&S). The most cited publication in NIST history, A&S still holds the lead in citations, with more than 60,000 recorded on Google Scholar, albeit with nearly a 50-year head start over DLMF. Together, A&S and DLMF present a vibrant face of NIST to the technical community, one of great heritage, the other looking forward.

ITL Awards Pilot Projects Grants to Promote Online Security and Privacy

ITL recently announced more than \$9 million in grant awards to support the [National Strategy for Trusted Identities in Cyberspace \(NSTIC\)](#). Five U.S. organizations will pilot identity solutions that increase confidence in online transactions, prevent identity theft, and provide individuals with more control over how they share their personal information.

NSTIC is a White House initiative to work collaboratively with the private sector, advocacy groups, and public sector agencies. NSTIC envisions an “Identity Ecosystem” in which technologies, policies, and consensus-based

standards support greater trust and security when individuals, businesses, and other organizations conduct sensitive transactions online.

The selected pilot proposals advance the NSTIC vision that individuals and organizations adopt secure, efficient, easy-to-use, and interoperable identity credentials to access online services in a way that promotes confidence, privacy, choice, and innovation. The pilots span multiple sectors, including healthcare, online media, retail, banking, higher education, and state and local government, and will test and demonstrate new solutions, models, or frameworks that do not exist in the marketplace today.

2012 ITL STAFF RECOGNITION

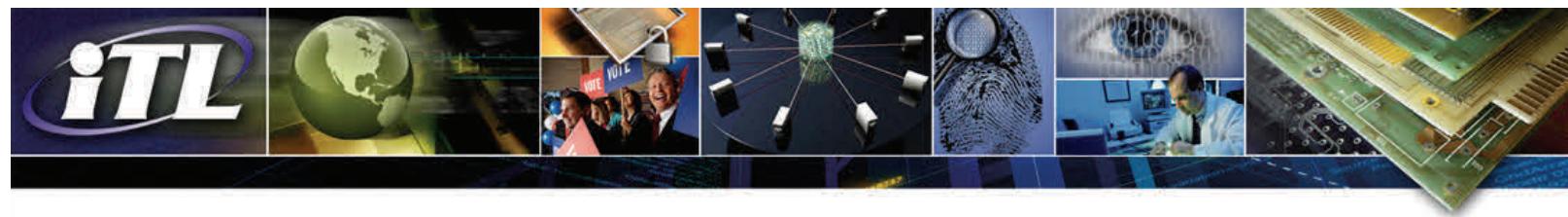
Jeffrey Voas was one of four NIST researchers to be elected as Fellow of the American Association for the Advancement of Science (AAAS). Voas was honored for the development of trustworthy software systems and advanced software fault injection-based testing techniques.

Donna Dodson, Chief, Computer Security Division, was named one of the ten most influential people in government IT security by GovInfoSecurity for creating IT security guidance requiring strong collaboration between NIST and its stakeholders.

Geoffrey McFadden was named a Fellow of the Society for Industrial and Applied Mathematics (SIAM). McFadden also received the 2012 Washington Academy of Sciences Award for merit and distinction in mathematics and computer science.

Ronald Boisvert, Chief, Applied and Computational Mathematics Division, was named an Outstanding Alumnus by the Department of Computer Science at Purdue University. Boisvert was one of 19 alumni selected by 8 departments within the Purdue College of Science “to honor graduates who have achieved success and recognition within their respected fields.”

Elham Tabassi, an electronics engineer in the Information Access Division, received the American National Standards Institute (ANSI) 2012 Next Generation Award. The award “honors individuals who have been engaged in standardization or conformity assessment activities for less than eight years and who have, during this time, demonstrated vision, leadership, dedication, and significant contributions to their chosen field of activity.”



Selected New Publications

Conformance Testing Methodology for ANSI/NIST-ITL 1-2011, Data Format for the Interchange of Fingerprint, Facial & Other Biometric Information Release 1.0

By Fernando Podio, Dylan Yaga, and Christofer McGinnis
NIST Special Publication 500-295
August 2012

ITL sponsored the development of a conformance testing methodology for ANSI/NIST-ITL 2011, *Data Format for the Interchange of Fingerprint, Facial & Other Biometric Information (AN-2011)*. The testing methodology supports the development of conformance test tools designed to test implementations of AN-2011 transactions and promotes biometrics conformity assessment efforts.

Guide for Conducting Risk Assessments

By the Joint Task Force Transformation Initiative
NIST Special Publication 800-30, Revision 1
September 2012

This document provides guidance for conducting risk assessments of federal information systems and organizations. It describes how to carry out each of the four steps in the risk assessment process and how risk assessments and other organizational risk management processes complement and inform each other.

Computer Security Incident Handling Guide

By Paul Cichonski, Tom Millar, Tim Grance, and Karen Scarfone
NIST Special Publication 800-61, Revision 2
August 2012

This publication assists organizations in establishing computer security incident response capabilities and handling incidents efficiently and effectively. The guidelines can be followed independently of particular hardware platforms, operating systems, protocols, or applications.

Recommendation for Applications Using Approved Hash Algorithms

By Quynh Dang
NIST Special Publication 800-107, Revision 1
August 2012

Hash functions that compute a fixed-length message digest from arbitrary length messages are widely used for many purposes in information security. This document provides security guidelines for achieving the required or desired security strengths when using cryptographic applications that employ the approved hash functions specified in Federal Information Processing Standard (FIPS) 180-4. These include functions such as digital signatures, Keyed-hash Message Authentication Codes

(HMACs), and Hash-based Key Derivation Functions (Hash-based KDFs).

Notional Supply Chain Risk Management Practices for Federal Information Systems

By Jon M. Boyens, Celia Paulsen, Nadya Bartol, Rama Moorthy, and Stephanie Shankles
NISTIR 7622
October 2012

This publication provides a wide array of practices that, when implemented, will help mitigate supply chain risk to federal information systems. It seeks to equip federal agencies with a notional set of repeatable and commercially reasonable supply chain assurance methods and practices that offer a means to obtain an understanding of, and visibility throughout, the supply chain.

An Exploration of the Operational Ramifications of Lossless Compression of 1000 ppi Fingerprint Imagery

By Shahram Orandi, John M. Libert, John G. Granthan, Kenneth Ko, Stephen S. Wood, Jin Chu Wu, Lindsay M. Petersen, and Bruce Bandini
NISTIR 7779
August 2012

This paper presents the findings of a study initially conducted to measure the operational impact of JPEG 2000 lossy compression on 1000 ppi fingerprint imagery at various levels of compression, but later expanded to include lossless compression. The study examines several such compression algorithms and compares them using criteria used to measure the effectiveness of the compression algorithm as well as its throughput using actual fingerprint imagery.

A New Measure in Cell Image Segmentation Data Analysis

By Jin Chu Wu, Michael Halter, Raghu N. Kacker, and John T. Elliott
NISTIR 7871
July 2012

Cell image segmentation (CIS) is critical for quantitative imaging in cytometric analyses. The data derived after segmentation can be used to infer cellular function. To evaluate CIS algorithms, first for dealing with comparisons of single cells treated as two-dimensional objects, a misclassification error rate (MER) is defined as a weighted sum of the false negative rate and the false positive rate. Then, all cells' MERs are aggregated to constitute a new measure called the total error rate, which statistically takes account of the sizes of the cells in such a way that an algorithm pays larger penalty if larger sizes of cells are not segmented correctly. This total error rate is used to measure the performance level of CIS algorithms.



Upcoming Technical Conferences

Forensics@NIST 2012

Dates: November 28-30, 2012

Place: NIST, Gaithersburg, Maryland

Audience: Industry/Government/Academia

Sponsors: NIST Engineering Laboratory, NIST Information Technology Laboratory, NIST Office of Law Enforcement Standards, NIST Material Measurement Laboratory, and NIST Physical Measurement Laboratory

Cost: None

This three-day symposium will showcase cutting-edge forensic science research being performed at NIST. The symposium will feature over 45 lecture presentations and 40 poster presentations by NIST scientists and their collaborators on relevant forensic science projects. To ensure optimum utilization of this opportunity, attendees are asked to sign up for only the specific day they plan to attend; ITL's forensic science work will be featured on Friday, November 30, 2012, in the following disciplines: computer forensics; fingerprints and biometrics; and multimedia forensics. ITL contact: Martin Herman, martin.herman@nist.gov

Random Bit Generation Workshop 2012

Dates: December 5-6, 2012

Place: NIST, Gaithersburg, Maryland

Audience: Industry/Government

Cost: \$20

Cryptography and security applications make extensive use of random numbers and random bits, particularly for the generation of cryptographic keying material. ITL is completing the development of approved methods for random bit generation. NIST Special Publication (SP) 800-90A specifies approved Deterministic Random Bit generator mechanisms for generating random bits, and two additional publications have recently been released for public review: SP 800-90B and SP 800-90C. This

workshop will discuss these documents and their validation by ITL's validation programs.

NIST contact: Elaine Barker, elaine.barker@nist.gov

ANSI/NIST-ITL Standard Workshop 2013

Dates: January 28-30, 2013

Place: NIST, Gaithersburg, Maryland

Cost: None

The workshop will provide an opportunity to review current developments on the Dental and Oral Forensics Supplement to the standard; the Forensic and Investigatory Voice Supplement to the standard; best practices for data transfer concerning Unknown Deceased and Living Amnesiacs; a new approach to mobile biometric data transmission "ANSI/NIST-ITL LITE"; and a concept of having a standard for data transmission concerning object identification, such as cartridges, bullets, tire tracks, shoe prints, and inks.

ITL contact: Brad Wing, bradford.wing@nist.gov

26th Annual Federal Information System Security Education Association (FISSEA) Conference

Dates: March 19-21, 2013

Place: NIST, Gaithersburg, Maryland

Audience: Government/Industry/Academia

Sponsors: NIST and FISSEA

Cost: TBD

Founded in 1987, FISSEA is an organization run by and for federal information systems security professionals. FISSEA assists federal agencies in meeting their computer security training responsibilities. The theme of their 2013 conference is "Making Connections in Cybersecurity and Information Security Education." NIST contacts: Patricia Toth, patricia.toth@nist.gov, and Peggy Himes, peggy.himes@nist.gov

Disclaimer: Any mention of commercial products or reference to commercial organizations is for information only; it does not imply recommendation or endorsement by the National Institute of Standards and Technology nor does it imply that the products mentioned are necessarily the best available for the purpose.



The Information Technology Laboratory (ITL) is a major research component of the National Institute of Standards and Technology (NIST). As a world-class measurement and testing laboratory encompassing a wide range of areas of computer science, mathematics, statistics, and systems engineering, our research program supports NIST's mission to promote U.S. innovation and industrial competitiveness by advancing measurement science, standards, and technology in ways that enhance economic security and improve our quality of life. ITL cybersecurity experts collaborate to develop cybersecurity standards, guidelines, and associated methods and techniques for federal agencies and industry. Our mathematicians and statisticians collaborate with measurement scientists across NIST to help ensure that NIST maintains and delivers the world's leading measurement capability. ITL computer scientists and other research staff provide technical expertise and development that underpins national priorities such as cloud computing, the Smart Grid, homeland security, information technology for improved healthcare, and electronic voting. We invite you to learn more about how ITL is enabling the future of the nation's measurement and standards infrastructure for information technology by visiting our website at <http://www.itl.nist.gov>.

ITL Editor: Elizabeth B. Lennon
National Institute of Standards and Technology
100 Bureau Drive, Stop 8900
Gaithersburg, MD 20899-8900
Phone: (301) 975-2832
Fax: (301) 975-2378
Email: elizabeth.lennon@nist.gov

The NIST campus at
Gaithersburg, Maryland.

Credit: NIST

TO SUBSCRIBE TO THE
ELECTRONIC EDITION OF THE
ITL NEWSLETTER, GO TO
[ITL HOMEPAGE](#)