

# Cryptography for Emerging Technologies and Applications Workshop - AGENDA -

National Institute of Standards and Technology  
100 Bureau Drive, Gaithersburg, MD 20899

## DAY 1 – November 7, 2011

8:30 – 9:00	<b>Check-in and Coffee Reception</b> <i>(Administration Bldg 101/Green Auditorium)</i>
9:00 – 9:15	<b>Welcome &amp; Opening Remarks</b> Donna Dodson, Chief, NIST/ITL/Computer Security Division
9:15 – 10:00	<b>Workshop Keynote: Turning Points in Cryptography</b> Dr. Whitfield Diffie, Chief Cryptographer, Revere Security and Vice President for Information Security at ICANN
10:00 – 10:25	<b>Crypto Strength and Attacks,</b> John Kelsey, NIST
10:25 – 10:35	<b>Constrained Environments and Many-Core Devices,</b> Larry Bassham, NIST
10:35 – 10:50	<b>Pairing-based Cryptography,</b> Dustin Moody, NIST
10:50 – 11:05	<b>Coffee Break</b>
11:05 – 11:30	<b>Cryptography for Highly Constrained Networks,</b> Rene Struik, Struik Security Consultancy
11:30 – 11:55	<b>Cryptographic Challenges for Smart Grid Home Area Networks Secure Networking,</b> Apurva Mohan, Honeywell ACS Labs
11:55 – 12:20	<b>FIPS-140-2 Validation of OpenSSL for Android Devices,</b> Tom Karygiannis, NIST and Steve Marquess, OpenSSL Foundation
12:20 – 12:45	<b>Secure App Execution On Commercial Mobile Devices By Means Of Bare Metal Hypervisors,</b> Katrin Hoeper, Motorola Solutions, Inc.
12:45 – 13:45	<b>Lunch Break</b>
13:45 – 14:10	<b>Compact Asymmetric Authentication using Hash-based Signatures,</b> David McGrew, CISCO
14:10 – 14:35	<b>Stream Ciphers for Constrained Environments,</b> Meltem Sonmez Turan, NIST
14:35 – 15:00	<b>A Framework for the Evaluation of Physical Unclonable Functions,</b> Abhranil Maiti, Virginia Tech
15:00 – 15:15	<b>Coffee Break</b>
15:15 – 15:40	<b>A Symmetric Key Generation System (KGS) Suitable for Sensor/Building Networks,</b> David McGrew, CISCO
15:40 – 16:05	<b>Key Security Challenges in Smart Swarm of Things (SSoT),</b> Oscar Garcia-Morchon, Philips Research Europe
16:05 – 16:30	<b>Securing the Next Wave of Technology,</b> Dr. Daniel Engels, CTO, Revere Security
16:30	<b>Closing remarks for the day</b>

## DAY 2 – November 8, 2011

8:30 – 9:00	<b>Check-in and Coffee Reception</b> ( <i>Administration Bldg 101/Green Auditorium</i> )
9:00 – 9:10	<b>Welcome &amp; Opening Remarks</b> Tim Polk, NIST
9:10 – 9:55	<b>Session Keynote: Introduction to Delay-Tolerant Networks,</b> Angela Hennessy, Laboratory for Telecommunications Sciences (LTS)
9:55 - 10:30	<b>Cryptographic Module Design with Domain Specific Languages,</b> John Launchbury, Chief Scientist, Galois
10:30 – 10:55	<b>NIST's Cryptographic Toolkit,</b> Elaine Barker, NIST
10:55 – 11:10	<b>Coffee Break</b>
11:10 – 11:35	<b>The Need for Parallel Ultra Fast Cryptographic Designs for Emerging Technologies,</b> Danilo Gligoroski, Department of Telematics, NTNU, Norway
11:35 – 12:00	<b>Secret Sharing and Reliable Cloud Computing,</b> Yvo Desmedt, University College London
12:00 – 12:25	<b>Privacy-preserving Electronic Transactions,</b> Rene Peralta, NIST
12:25 – 12:50	<b>Security/Privacy Models for "Internet of things": What should be studied from RFID-schemes?</b> Daisuke Moriyama, NICT
12:50 – 13:50	<b>Lunch Break</b>
13:50 – 14:50	<b>Open floor discussions</b>
14:50	<b>Closing Remarks &amp; Adjourn</b>