Meeting on Privacy-Enhancing Cryptography
- AGENDA -

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

DAY 1 – December 8, 2011

7:30	Shuttle arrives at Holiday Inn
7:45	Shuttle departs Holiday Inn for NIST
8:30 – 9:00	Check-in and Coffee Reception (Administration Bldg. 101/Green Auditorium)
9:00 – 9:15	Welcome & Opening Remarks, Tim Polk, NIST, Manager, Cryptographic Technology Group.
9:15– 9:45	Secure Multiparty Computation, Serge Fehr, CWI, Amsterdam.
9:45 – 10:15	The Danish Sugar Beet Auctions, Tomas Toft, University of Aarhus.
10:15 – 10:30	Coffee Break
10:30 – 11:00	PIR, Oblivious RAMs and Secure Two-Party Computation, Rafail Ostrovsky, UCLA.
11:00 – 11:30	Functional encryption, Dan Boneh, Stanford.
11:30 – 12:00	SPAR/NICECAP pilots, Stanislaw Jarecki, UC Irvine.
12:00 – 13:00	Lunch Break (West Square Cafeteria) *[2nd lunch room entrance on the right]*
13:00 – 13:30	Group Signatures, Kazue Sako, NEC.
13:30 – 14:00	Schemes For Encrypting Personal Health Records, Melissa Chase, Microsoft.
14:00 – 14:45	Panel on medical (and other sensitive) databases, Peter Gershkovich (Yale), Melissa Chase (Microsoft), Rafail Ostrovsky (UCLA), Jeffrey Friedhoffer (MIT Lincoln Laboratory).
14:45 – 15:00	Coffee Break
15:00 – 15: 30	Format Preserving Encryption, Terence Spies, Voltage.
15:30 – 16:00	Smart metering, George Danezis, Microsoft.
16:00 – 16:45	Panel on smart metering, George Danezis (Microsoft), Claire Vishik (Intel), Stephen Chasko (Landis+Gyr).
16:45	Adjourn for the day.
16:45	Shuttle departs NIST to return to Holiday Inn
18:00-21:00	Reception and Cash Bar Social (Holiday Inn / Walker Room)

DAY 2 – December 9, 2011

7:30	Shuttle arrives at Holiday Inn
7:45	Shuttle departs Holiday Inn for NIST
8:00 – 8:20	Check-in and Coffee Reception (Administration Bldg 101/Green Auditorium)
8:20 – 8:30	Welcome. Donna F. Dodson, NIST, Chief, Computer Security Division.
8:30 – 9:00	Direct Anonymous Attestation: Revocation and Anonymity, Benjamin Benoy, National Security Agency.
9:00 - 9:30	EPID, Ernie Brickell, Intel.
9:30 – 10:00	Conditional And Revocable Anonymity, Anna Lysyanskaya, Brown.
10:00 – 10:30	Hidden diversity can make multiparty computation more robust, Juan Garay, AT&T.
10:30 – 10:45	Coffee Break
10:45 – 11:15	U-Prove, Christian Paquin, Microsoft.
11:15 – 11:45	Idemix, Gregory Neven, IBM Zurich.
11:45 – 12:15	Why we should care about privacy in the identification domain, Marc Rotenberg, EPIC.
12:15 – 13:15	Lunch Break (West Square Cafeteria) *[2nd lunch room entrance on the right]*
13:15 – 14:15	Panel on privacy in the identification domain, Brian LaMacchia(Microsoft), Francisco Corella (Pomcor), Anna Lysyanskaya (Brown), Thomas Smedinghoff (Edwards Wildman Palmer LLP), Jeremy Grant (NIST), Gregory Neven (IBM Zurich), Eric Le Saint (ActivIdentity).
14:15 – 15:00	Panel discussion: where to go from here, Gene Itkis (MIT Lincoln Laboratory), Claire Vishik (Intel), Tim Polk (NIST), Seth Schoen (Electronic Frontier Foundation).
15:00	Closing Remarks & Adjourn
Close of meeting	Shuttle departs NIST for Holiday Inn