Workshop III: Foundations of secure multi-party computation and zero-knowledge and its applications

Monday November 13, 2006

8:00–9:45 *Check-In/Light Breakfast (Hosted by IPAM)*

9:45–10:00 *Welcome and Opening Remarks*

10:00–11:00 **Jens Groth** (UCLA)
New Techniques for Non-interactive Zero-Knowledge

11:00–11:15 *Break*

11:15–12:15 **Amit Sahai** (UCLA)

12:15–2:00 *Lunch (on your own)*

2:00–3:00 **Hoeteck Wee** (UC Berkeley)
One Way Permutations, Interactive Hashing and Statistically Hiding Commitments

3:00–3:30 *Break*

3:30–4:30 **Nishanth Chandran** (UCLA)
Covert Multi-party Computation

4:30–5:30 **Enav Weinreb** (Technion - Israel Institute of Technology)
Private Approximation of Search Problems

5:30–6:30 *Wine/Cheese Reception (Hosted by IPAM)*

Tuesday November 14, 2006

9:00–10:00 *Continental Breakfast*

10:00–11:00 **Tal Rabin** (IBM Thomas J. Watson Research Center)
Information-Theoretic Security and Security under Composition

11:00–11:15 *Break*

(Tuesday schedule continued on next page)

(Tuesday schedule continued from previous page)

11:15–12:15 **Leonid Reyzin** (Boston University)
Robust Fuzzy Extractors and Authenticated Key Agreement from Close Secrets

12:15–2:00 *Lunch (on your own)*

2:00–3:00 **Adam Smith** (UCLA)
Cryptography with Quantum Data

3:00–3:30 *Break*

3:30–4:30 **Jonathan Katz** (University of Maryland)
On Expected Constant-Round Protocols for Broadcast

4:30–5:30 **Chiu-Yuen Koo** (University of Maryland)
Round-Efficient Multi-Party Computation in Point-to-Point Networks

Wednesday November 15, 2006

9:00–10:00 *Continental Breakfast*

10:00–11:00 **Manoj Prabhakaran** (University of Illinois at Urbana-Champaign)
Angels and Monitors

11:00–11:15 *Break*

11:15–12:15 **Ran Canetti** (IBM Thomas J. Watson Research Center)
Universally Composable Security with Global Setup

12:15–2:00 *Lunch (on your own)*

2:00–3:00 **Danny Harnik** (Technion - Israel Institute of Technology)
On the Compressibility of NP Instances and Cryptographic Applications

3:00–3:30 *Break*

3:30–4:30 **Rafael Pass** (Cornell University)
Precise Zero Knowledge

4:30–5:30 **Ivan Visconti** (Università di Salerno)
Concurrent Non-Malleable Witness Indistinguishability

Thursday November 16, 2006

9:00–10:00 *Continental Breakfast*

10:00–11:00 **Yevgeniy Dodis** (New York University)
Does Privacy Require True Randomness?

11:00–11:15 *Break*

11:15–12:15 **Serge Fehr** (CWI (Center for Mathematics and Computer Science))
Combinatorial Codes for Detection of Algebraic Manipulation

12:15–2:00 *Lunch (on your own)*

2:00–3:00 **Anna Lysyanskaya** (Brown University)
On Signatures of Knowledge

3:00–3:30 *Break*

3:30–4:30 **Salil Vadhan** (Harvard University)
The Complexity of Zero Knowledge

4:30–5:30 **Shien Jin Ong** (Harvard University)
Statistical Zero-Knowledge Arguments for NP from Any One-Way Function

Friday November 17, 2006

9:00–10:00 *Continental Breakfast*

10:00–11:00 **Eyal Kushilevitz** (Technion - Israel Institute of Technology)
ZK from MPC

11:00–11:15 *Break*

11:15–12:15 **Juan Garay** (Lucent Technologies Bell Laboratories)
Towards Optimal and Efficient Perfectly Secure Message Transmission

12:15–2:00 *Lunch (on your own)*

2:00–3:00 **Alon Rosen** (Harvard University)
Input-Indistinguishable Computation

3:00–3:30 *Break*

3:30–4:30 **Stanislaw Jarecki** (University of California, Irvine)
Efficient Secure Two-Party Computation on Committed Inputs

4:30–5:30 **Benny Applebaum** (Technion - Israel Institute of Technology)
On Pseudorandom Generators with Linear Stretch in NC0