Workshop II: Locally decodable codes, private information retrieval, privacy-preserving data-mining, and public key encryption with special properties

Wednesday October 25, 2006

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

8:45–9:00 *Welcome and Opening Remarks*

9:00–9:45 **Dan Boneh** (Stanford University)

9:45–10:30 **Brent Waters** (SRI International)
Attribute-Based Encryption

10:30–11:00 *Break*

11:00–11:45 **Rafail Ostrovsky** (UCLA)
Private Searching on Streaming data

11:45–12:30 **Amos Beimel** (Ben Gurion University of the Negev)
Secret Sharing: Linear vs. Nonlinear Schemes

12:30–1:30 *Lunch (on your own)*

1:30–2:15 **Rebecca Wright** (Stevens Institute of Technology)
Privacy-Preserving Bayesian Network Learning and Other Recent Results in Privacy-Preserving Data Mining

2:15–3:00 **Benny Pinkas** (Haifa University)
An Efficient Protocol for Secure Two-Party Computation in the Presence of Malicious Adversaries

3:00–3:30 *Break*

3:30–4:15 **Zeev Dvir** (Weizmann Institute of Science)
Locally Decodable Codes with 2 queries and Polynomial Identity Testing for depth 3 circuits

4:15–5:00 **Sergey Yekhanin** (Massachusetts Institute of Technology)
Title: New Locally Decodable Codes and Private Information Retrieval Schemes

5:00–6:30 *Reception (Location: IPAM Lobby)*

Thursday October 26, 2006

8:00–8:45 *Breakfast (Hosted by IPAM)*

8:45–9:30 **Iordanis Kerenidis** (Centre National de la Recherche Scientifique (CNRS))
An introduction to Quantum Information Theory and applications to Locally Decodable Codes

9:30–10:15 **Ronald de Wolf** (CWI, Amsterdam & Math Inst, Leiden□□University)
Exponential Lower Bound for 2-Query Locally Decodable Codes via a Quantum Argument

10:15–10:45 *Break*

10:45–11:30 **Alex Samorodnitsky** (Hebrew University)
An attempt to de-quantify the lower bound for 2-query Locally Decodable Codes

11:30–12:15 **Stephanie Wehner** (CWI, Amsterdam & Math Inst, Leiden□□University)
Improved Lower Bounds for Locally Decodable Codes and Private Information Retrieval

12:15–1:30 *Lunch (on your own)*

1:30–2:15 **Sergey Yekhanin** (Massachusetts Institute of Technology)
An Omega(n^{1/3}) Lower Bound for Bilinear Group Based Private Information Retrieval

2:15–3:00 **David Woodruff** (Massachusetts Institute of Technology)
Some New Lower Bounds for General Locally Decodable Codes

3:00–3:30 *Break*

3:30–4:15 **William Skeith** (UCLA)

Friday October 27, 2006

8:00–8:45 *Breakfast (Hosted by IPAM)*

8:45–9:30 **Adi Akavia** (Massachusetts Institute of Technology)

9:30–10:15 **Yuval Ishai** (Technion - Israel Institute of Technology)
Efficient Arguments without Short PCPs

10:15–10:45 *Break*

(Friday schedule continued on next page)

(Friday schedule continued from previous page)

10:45–11:30 **Jonathan Katz** (University of Maryland)
Concurrently-Secure Blind Signatures without Random Oracles or Setup Assumptions

11:30–12:15 **Moni Naor** (Weizmann Institute of Science)

12:15–1:30 *Lunch (on your own)*

1:30–2:15 **Iftach Haitner** (Weizmann Institute of Science)
A New Interactive Hashing Theorem

2:15–3:00 **Yael Kalai** (Massachusetts Institute of Technology)
Succinct Non-Interactive Zero-Knowledge Proofs with Preprocessing for LOGSNP.

3:00–3:30 *Break*

3:30–4:15 **Seny Kamara** (Johns Hopkins University)
Searchable Symmetric Encryption

Saturday October 28, 2006

8:00–8:45 *Breakfast (Hosted by IPAM)*

8:45–9:30 **Tal Malkin** (Columbia University)
Towards a Separation of Semantic and CCA Security for Public Key Encryption

9:30–10:15
TBA

10:15–10:30 *Break*

10:30–11:15 **Adam Smith** (UCLA)
Interaction and Locality in Private Data Analysis

11:15–12:00 **Cynthia Dwork** (Microsoft Research)

12:00–1:00 *Lunch (on your own)*

1:00–1:45
TBA