Mathematics of Information-Theoretic Cryptography

Monday February 28, 2011

8:00–8:50 *Check-In/Light Breakfast (Hosted by IPAM)*

8:50–9:00 *Welcome and Opening Remarks*

9:00–9:40 **Yuval Ishai** (Technion - Israel Institute of Technology)
Why are we here?

9:50–10:05 *Break*

10:05–10:45 **Ronald Cramer** (CWI Amsterdam & Mathematical Institute, Leiden University)
The Arithmetic Codex

10:55–11:10 *Break*

11:10–11:50 **Alp Bassa** (Nanyang Technological University)
How many rational points can a curve over a finite field have?

12:00–2:00 *Lunch (on your own)*

2:00–2:40 **Chaoping Xing** (Nanyang Technological University)

2:50–3:05 *Break*

3:05–3:45 **Ignacio Cascudo** (CWI (Center for Mathematics and Computer Science))
The Torsion Limit for Algebraic Function Fields and Applications in Cryptography and Complexity

3:55–4:10 *Break*

4:10–4:50 **Ivan Damgård** (Aarhus University)
Using Information Theoretic MAC's in Multiparty Computation with Dishonest Majority.

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

Tuesday March 1, 2011

8:00–9:00 *Continental Breakfast*

9:00–9:40 **Carles Padro** (Nanyang Technological University)
On the Optimization of Secret Sharing Schemes for General Access Structures

9:50–10:05 *Break*

(Tuesday schedule continued on next page)

(Tuesday schedule continued from previous page)

10:05–10:45 **David Zuckerman** (University of Texas at Austin)
Randomness Extraction: A Survey

10:55–11:10 *Break*

11:10–11:50 **Leonid Reyzin** (Boston University)
Information-Theoretic Key Agreement from Close Secrets: A Survey.

12:00–2:00 *Lunch (on your own)*

2:00–2:40 **Sergey Yekhanin** (Microsoft Research)
Locally decodable codes.

2:50–3:05 *Break*

3:05–3:45 **Iwan Duursma** (University of Illinois at Urbana-Champaign)
Coding theory aspects of linear secret sharing schemes.

3:55–4:10 *Break*

4:10–4:50 **Omer Reingold** (Microsoft Research)
The Many Entropies of One-Way Functions

Wednesday March 2, 2011

8:00–9:00 *Continental Breakfast*

9:00–9:40 **Madhu Sudan** (Microsoft Research New England)
Local List Decoding

9:50–10:05 *Break*

10:05–10:45 **Yael Kalai** (Microsoft Research)
Cryptography with Tamperable and Leaky Memory

10:55–11:10 *Break*

11:10–11:50 **Kristin Lauter** (Microsoft Research)
Elliptic Curve Cryptography and Applications.

12:00–2:00 *Lunch (on your own)*

2:00–2:40 **Arnaldo Garcia** (Institute of Pure and Applied Mathematics (IMPA))
On explicit towers over finite fields

2:50–3:05 *Break*

3:05–5:30 *Hot Topic Session*

Thursday March 3, 2011

8:00–9:00 *Continental Breakfast*

9:00–9:40 **Amos Beimel** (Ben Gurion University of the Negev)
Using Secret Sharing to Construct Protocols for Multiparty Coin Toss With Dishonest Majority

9:50–10:05 *Break*

10:05–10:45 **Venkat Guruswami** (Carnegie-Mellon University)
Bridging Shannon and Hamming: Codes for computationally simple channels

10:55–11:10 *Break*

11:10–11:50 **Yevgeniy Dodis** (New York University)
Leftover Hash Lemma, Revisited

12:00–2:00 *Lunch (on your own)*

2:00–2:40 **Rafail Ostrovsky** (University of California, Los Angeles (UCLA))
Improved Fault Tolerance and Secure Computation on Sparse Networks.

2:50–3:05 *Break*

3:05–3:45 **Krzysztof Pietrzak** (CWI (Center for Mathematics and Computer Science))
Subspace LWE & Applications

3:55–4:10 *Break*

4:10–4:50 **Amit Sahai** (University of California, Los Angeles (UCLA))
Potent Tree Codes and Their Applications

Friday March 4, 2011

8:00–9:00 *Continental Breakfast*

9:00–9:40 **Michael Zieve** (University of Michigan)
Automorphism groups of curves

9:50–10:05 *Break*

10:05–10:45 **Jürg Wullschleger** (University of Montreal)
Constant-Rate Oblivious Transfer from Noisy Channels

10:55–11:10 *Break*

(Friday schedule continued on next page)

(Friday schedule continued from previous page)

11:10–11:50 **Serge Fehr** (CWI (Center for Mathematics and Computer Science))
Secure Authentication from a Weak Key, Without Leaking Information

12:00–2:00 *Lunch (on your own)*

2:00–2:40 **Frantisek Matus** (Czech Academy of Sciences (AVCR))
Almost entropic matroids

2:50–3:05 *Break*

3:05–3:45 **Amnon Ta-shma** (Tel Aviv University)
Constructing Small-Bias Sets from Algebraic-Geometric Codes

3:55–4:10 *Break*

4:10–4:50 **Manoj Prabhakaran** (University of Illinois at Urbana-Champaign)
Assisted Common Information and its Applications to Secure Two-Party Computation.