Securing Cyberspace: Applications and Foundations of Cryptography and Computer Security-Tutorials

Tuesday September 12, 2006

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

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

9:00–10:00 **Dan Boneh** (Stanford University)
Pairing-based Cryptography

10:00–10:15 *Break*

10:15–11:00 **Dan Boneh** (Stanford University)
Pairing-based Cryptography

11:00–11:15 *Break*

11:15–12:00 **Dan Boneh** (Stanford University)
Pairing-based Cryptography

12:00–2:00 *Lunch (on your own)*

2:00–3:00 *Panel Discussion*

3:00–3:15 *Break*

3:15–4:00 *Panel Discussion*

4:00–4:15 *Break*

4:15–5:00 *Panel Discussion*

Wednesday September 13, 2006

8:00–9:00 *Breakfast (Hosted by IPAM)*

9:00–10:00 **Jonathan Katz** (University of Maryland)
Black-Box Reductions, Impossibility Results and Efficiency Lower Bounds

10:00–10:15 *Break*

10:15–11:00 **Jonathan Katz** (University of Maryland)
Black-Box Reductions, Impossibility Results and Efficiency Lower Bounds

11:00–11:15 *Break*

(Wednesday schedule continued on next page)

(Wednesday schedule continued from previous page)

11:15–12:00 **Jonathan Katz** (University of Maryland)
Black-Box Reductions, Impossibility Results and Efficiency Lower Bounds

12:00–2:00 *Lunch (on your own)*

2:00–3:00 **Rafail Ostrovsky** (UCLA)
A survey on Private Information Retrieval

3:00–3:15 *Break*

3:15–4:00 **Rafail Ostrovsky** (UCLA)
A survey on Private Information Retrieval

4:00–4:15 *Break*

4:15–5:00 **Rafail Ostrovsky** (UCLA)
A survey on Private Information Retrieval

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

Thursday September 14, 2006

8:00–9:00 *Breakfast (Hosted by IPAM)*

9:00–10:00 **Kobbi Nissim** (Ben Gurion University of the Negev)
Database Privacy

10:00–10:15 *Break*

10:15–11:00 **Kobbi Nissim** (Ben Gurion University of the Negev)
Database Privacy

11:00–11:15 *Break*

11:15–12:00 **Kobbi Nissim** (Ben Gurion University of the Negev)
Database Privacy

12:00–1:30 *Lunch (on your own)*

2:00–3:00 **Yuval Ishai** (Technion - Israel Institute of Technology)
Randomization techniques and parallel cryptography

3:00–3:15 *Break*

3:15–4:00 **Yuval Ishai** (Technion - Israel Institute of Technology)
Randomization techniques and parallel cryptography

4:00–4:15 *Break*

4:15–5:00 **Yuval Ishai** (Technion - Israel Institute of Technology)
Randomization techniques and parallel cryptography

Friday September 15, 2006

8:00–9:00 *Breakfast (Hosted by IPAM)*

9:00–10:00 **Ran Canetti** (IBM Thomas J. Watson Research Center)
Security and composition of cryptographic protocols

10:00–10:15 *Break*

10:15–11:00 **Ran Canetti** (IBM Thomas J. Watson Research Center)
Security and composition of cryptographic protocols

11:00–11:15 *Break*

11:15–12:00 **Ran Canetti** (IBM Thomas J. Watson Research Center)
Security and composition of cryptographic protocols

12:00–12:00 *Conclusion*