TCC 2005 Program

Wednesday, February 9, 2005

6:30-8:30pm **Welcome Reception**

Stata Center, 4th floor R&D space.

Thursday, February 10, 2005

All Thursday events will take place at Hotel@mit

8:00-9:30 **Welcome and Registration**

9:30-11:00 **Hardness Amplification and Error Correction**

Session Chair: Boaz Barak

Optimal Error Correction Against Computationally Bounded Noise
Silvio Micali, Chris Peikert, Madhu Sudan and David A. Wilson

Hardness amplification of weakly verifiable puzzles
Ran Canetti, Shai Halevi and Michael Steiner

On Hardness Amplification of One-Way Functions
Henry Lin, Luca Trevisan and Hoeteck Wee

11:00-11:30 **Break**

11:30-12:30 **Graphs and Groups**

Session Chair: Amos Beimel

Cryptography in Subgroups of $\boldsymbol{Z}_n^*$
Jens Groth

Efficiently Constructible Huge Graphs that Preserve First Order Properties of Random Graphs
Moni Naor, Asaf Nussboim and Eran Tromer

12:30-2:00 **Lunch (catered)**

2:00-3:30 **Simulation and Secure Computation**

Session Chair: Alon Rosen

Comparing Two Notions of Simulatability
Dennis Hofheinz and Dominique Unruh

Relaxing Environmental Security: Monitored Functionalities and Client-Server Computation
Manoj Prabhakaran and Amit Sahai

Handling Expected Polynomial-Time Strategies in Simulation-Based Security Proofs
Jonathan Katz and Yehuda Lindell

3:30-4:00 **Break**

4:00-5:30 **Security of Encryption**

Session Chair: Leonid Reyzin

Adaptively Secure Non-Interactive Public-Key Encryption
Ran Canetti, Shai Halevi and Jonathan Katz

Adaptive Security of Symbolic Encryption
Daniele Micciancio and Saurabh Panjwani

Chosen-Ciphertext Security of Multiple Encryption
Yevgeniy Dodis and Jonathan Katz

8:00-10:00pm **Business Meeting and Rump Session**

Business Meeting Chair: Amit Sahai

Rump Session Chair: Louis Salvail

Friday, February 11, 2005

All events will take place at the Stata Center, MIT
Talks until 3:30 will be in Room 32-141
The panel discussion will be in Room 32-123

9:00-10:30 **Steganography and Zero Knowledge**

Session Chair: Rafail Ostrovsky

Public-Key Steganography with Active Attacks
Michael Backes and Christian Cachin

Upper and Lower Bounds on Black-Box Steganography
Nenad Dedić, Gene Itkis, Leonid Reyzin and Scott Russell

Fair Zero Knowledge
Matt Lepinski, Silvio Micali and abhi shelat

10:30-11:00 **Break**

11:00-12:30 **Secure Computation I**

Session Chair: Tal Malkin

How to Securely Outsource Cryptographic Computations
Susan Hohenberger and Anna Lysyanskaya

Secure Computation of the Mean and Related Statistics
Eike Kiltz, Gregor Leander and John Malone-Lee

Keyword Search and Oblivious Pseudorandom Functions
Michael J. Freedman, Yuval Ishai, Benny Pinkas and Omer Reingold

12:30-2:00 **Lunch (catered)**

2:00-3:30 **Secure Computation**

Session Chair: Amit Sahai

Evaluating 2-DNF Formulas on Ciphertexts
Dan Boneh, Eu-Jin Goh and Kobbi Nissim

Share conversion, pseudorandom secret-sharing and applications to secure distributed computing
Ronald Cramer, Ivan Damgård and Yuval Ishai

Toward Privacy in Public Databases
Shuchi Chawla, Cynthia Dwork, Frank McSherry, Adam Smith and Hoeteck Wee

3:30-4:00 **Break**

4:00-5:30 **Panel Discussion (Room 32-123)**

Session Chair: Anna Lysyanskaya

Mihir Bellare, Cynthia Dwork, Hugo Krawczyk and Adi Shamir

Saturday, February 12, 2005

All Saturday events will take place at the Stata Center, MIT, Room 32-123

9:00-10:30 **Quantum Cryptography and Universal Composability**

Session Chair: Alon Rosen

The Universal Composable Security of Quantum Key Distribution
Michael Ben-Or, Michał Horodecki, Debbie Leung, Dominic Mayers and Jonathan Oppenheim

Universally Composable Privacy Amplification Against Quantum Adversaries
Renato Renner and Robert König

A Universally Composable Secure Channel Based on the KEM-DEM Framework
Waka Nagao, Yoshifumi Manabe and Tatsuaki Okamoto

10:30-11:00 **Break**

11:00-12:30 **Cryptographic Primitives and Security**

Session Chair: Tal Rabin

Sufficient Conditions for Collision-Resistant Hashing
Yuval Ishai, Eyal Kushilevitz and Rafail Ostrovsky

The Relationship between Password-Authenticated Key Exchange and Other Cryptographic Primitives
Minh-Huyen Nguyen

On the Relationships Between Notions of Simulation-Based Security
Anupam Datta, Ralf Kuesters, John C. Mitchell and Ajith Ramanathan

12:30-2:00 **Lunch (catered)**

2:00-3:30 **Encryption and Signatures**

Session Chair: Leonid Reyzin

A new Cramer-Shoup like methodology for group based provably secure encryption schemes
María Isabel González, Consuelo Martínez, Rainer Steinwandt and Jorge L. Villar

Further Simplifications in Proactive RSA Signature Schemes
Stanislaw Jarecki and Nitesh Saxena

Proof of Plaintext Knowledge for the Ajtai-Dwork Cryptosystem
Shafi Goldwasser and Dmitriy Kharchenko

3:30-4:00 **Break**

4:00-5:30 **Information Theoretic Cryptography**

Session Chair: Louis Salvail

Entropic Security and the Encryption of High-Entropy Messages
Yevgeniy Dodis and Adam Smith

Error Correction in the Bounded Storage Model
Yan Zong Ding

Characterizing Ideal Weighted Threshold Secret Sharing
Amos Beimel, Tamir Tassa and Enav Weinreb