Dagstuhl Seminar 08491: Preliminary schedule of talks

Monday:

8:50 - 9:00	Welcome (Ran, Shafi, Guenter, Rainer)
9:00 - 10:00	Chris Peikert: *Public-Key Cryptosystems from the Worst-Case Shortest Vector Problem*
10:00- 11:00	Guy Rothblum: *When and How Can Data be Efficiently Released with Privacy?*
11:00-11:30:	Break
11:30-12:10	Aggelos Kiayas: *Sound and Fine-grain Specification of Ideal Functionalities*
12:15:	Lunch
2:00 – 2:30	Ralf Kuesters: *Joint State Theorems for Public-Key Encryption and Digital Signature Functionalities with Local Computation*
2:30 – 3:15	Krzysztof Pietrzak: *Leakage-Resilient Cryptography: Theoretical Foundations of Side-Channel Security*
3:15	Coffee
4:15 – 5:00	Yael Kalai: *Network Extractor Protocols*
5:00 - 5:45	Gil Segev: *Chosen-Ciphertext Security via Correlated Products*
6:00	Supper
7:30-8:00	Max Tuengerthal: *A Functionality for Symmetric Encryption in Simulation-based Security*
8:00-8:30	Chris Peikert
8:30-9:00	Yael Kalai

Tuesday:

9:00- 10:00	Moni Naor: *How Fair Can a Coin Toss Be?*
10:00 -11:00	Jonathan Katz: *Partial Fairness in Secure Two-Party Computation*
11:00-11:15	Break
11:15 -12:15	Rafael Pass: *Game theory with costly computation*
12 :15	Lunch
2:30-3:15	Vinod Vaikuntanathan: *A Framework for Efficient and Composable Oblivious Transfer*
3:15-4:00	Iftach Haitner: *Accessible Entropy*
4:00	Coffee
4:40 - 5:20	Dennis Hofheinz: *Practical chosen-ciphertext secure encryption from factoring*
5:20 - 6:00	Jens-M. Bohli: *Relations Among Privacy Notions*
6:00:	Supper
7:30-8:15	Mayank Varia: *Non-malleable Obfuscation*

Wednesday:

9:00-10:00	Tal Malkin: *Simple, Black-Box Constructions of Adaptively Secure Protocols*
10:00 -11:40	Craig Gentry: *Fully homomorphic encryption*
12:15	Lunch
2:00-2:45	Olivier Pereira: *Modeling Computational Security in Long-Lived Systems*
2:45-3:30	Yevgeniy Dodis: *Message Authentication Codes from Unpredictable Block Ciphers*
3:30-4:10	Zvika Brakerski: *Weak Verifiable Pseudorandom Functions*
4:10:	Coffee
4:40-5:20	Joern Mueller-Quade: *Wireless Physical Layer Key Exchange*
5:20-6:00	Christoph Sprenger: *Abstractions for Cryptographically Faithful Proofs of Security Protocols*
6:00:	Supper

Thursday:

9:00-9:40	Dominique Unruh: *Security of public key encryption under key dependent messages*
9:40-10:20	Alon Rosen: *Fairness with an honest minority and a rational majority*
10:20-10:35	Break
10:35 -11:25	Manoj Prabhakaran: *Founding Cryptography on Oblivious Transfer – Efficiently*
11:25- 12:15	Ronald Cramer: *Reduction of the Threshold Gap in Algebraic Geometric Secret Sharing*
12:15:	Lunch

Afternoon: excursion/no technical program

6:00: Supper

Friday:

9:00- 10:00	Yevgeniy Dodis: *One-Round Authenticated Key Agreement from Weak Secrets*
10:20-11:00	Guy Rothblum: *One Time Programs*
11:00:	Closing: Dagstuhl proceedings etc.
12:15:	Lunch