Winter School on Secure Computation and Efficiency

Organizers

Yehuda Lindell and Benny Pinkas, Computer Science Dept., Bar-Ilan University, Israel

Location

Beck Hall, Bar-Ilan University, Ramat Gan (greater Tel-Aviv area), Israel

Speakers

Shai Halevi (IBM), Yuval Ishai (Technion), Yehuda Lindell (Bar-Ilan University), Benny Pinkas (Bar-Ilan University)

Website

http://www.cs.biu.ac.il/~lindell/mpcschool.html

Background

The target audience is graduate students and postdocs in cryptography (we will assume background in cryptography, but not secure computation). However, faculty, undergrads and professionals with the necessary background are welcome. The winter school is open to participants from all over the world; all talks will be in English.

Dates

January 30 – February 1, 2011 (during the semester break of all the universities in Israel)

Cost

- Registration is FREE and includes participation, materials, food (including lunch and coffee breaks) and the social event on Monday evening.
- Hotel and airfare will be covered by the participants. Some stipends of $800 each (for flight and accommodation) are available for overseas students needing support. Please have your advisor send a letter justifying the need for financial support.

Registration

Those who wish to participate should register by sending their name and affiliation to mpcschool.biu@gmail.com. **The registration deadline is 31/12/2010.** After this date, registration may be possible upon availability.

Hotel

We have arranged a special rate at the Kfar Maccabiah hotel for overseas participants and for Israeli participants who wish to stay close to Bar-Ilan University. See the school website for details.

Day 1 – Sunday 30/1/2011 - Background, Definitions and Feasibility

08:30-09:00	Registration & Refreshments
09:00-09:10	Opening Remarks
09:10-10:40	Background and Definitions (Yehuda Lindell)
10:40-11:00	Coffee Break
11:00-12:30	The Yao Construction and its Proof of Security (Yehuda Lindell)
12:30-13:45	Lunch
13:45-15:15	The GMW Construction: the Multiparty Case and Security for Malicious (Benny Pinkas)
15:15-15:45	Break & Snacks
15:45-17:15	The BGW Construction for the Information Theoretic Setting (Benny Pinkas)

Day 2 – Monday 31/1/2011 - Efficient Secure Computation

09:00-10:30	Sigma Protocols (Yehuda Lindell)
10:30-11:00	Coffee Break
11:00-12:30	Oblivious Transfer (Benny Pinkas)
12:30-13:45	Lunch
13:45-15:15	Two-Party Secure Computation for Malicious Adversaries (Yehuda Lindell)
15:15-15:45	Break & Snacks
15:45-17:15	Constructions for Specific Functions of Interest (Benny Pinkas)
17:15	Social event & Dinner

Day 3 – Tuesday 1/2/2011 - New Results in Secure Computation

09:00-10:30	Fully Homomorphic Encryption (Shai Halevi)
10:30-11:00	Coffee Break
11:00-12:30	Fully Homomorphic Encryption (Shai Halevi)
12:30-13:45	Lunch
13:45-15:15	Efficient Secure Computation with an Honest Majority (Yuval Ishai)
15:15-15:45	Break & Snacks
15:45-17:15	The IPS Compiler and Related Constructions (Yuval Ishai)

Bar-Ilan University
Department of Computer Science
Cryptography & Security Research Group