Celebration of the work of Shafi Goldwasser and Silvio Micali

Visions of Cryptography

December 11th-12th, 2013

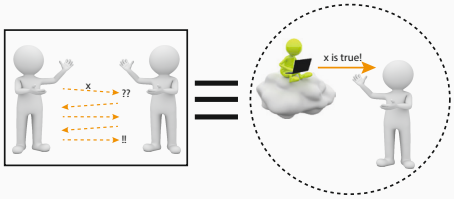
The David Lopatie Conference Centre, Weizmann Institute of Science, Israel

Wednesday December 11th

10:00	**Opening Notes, Oded Goldreich**	
Session 1	Chair: Moni Naor	
10:05-11:05	**Daniele Micciancio and Chris Peikert**	*Lattices - from complexity to cryptography*
11:20-12:20	**Shai Halevi**	*Multilinear maps*
	Lunch	
Session 2	Chair: Ivan Damgard	
14:00-14:45	**Stefano Tessaro**	*Ideal Models in Symmetric Cryptography*
15:00-15:10	**Krzysztof Pietrzak**	*Nesting Hybrids*
15:15-15:30	**Vipul Goyal**	*Non-Black Box Simulation in Fully Concurrent Setting*
15:35-15:45	**Jesper Buus Nielsen**	*Limits on the Power of Cryptographic Cheap Talk*
	Coffee Break	
Session 3	Chair: Zvika Brakerski	
16:15-17:05	**Nir Bitansky**	*Extractable Functions: Fiction or Reality?*
17:15-18:15	**Panel discussion on Assumptions**	*Boaz Barak, Ran Canetti, Craig Gentry, Eike Kiltz, Moni Naor, and Rafael Pass*
18:20	**A mid-way note: Oded Goldreich**	
	Dinner	
	An open problem / rump session, organized by Tal Rabin	

Thursday, December 12th

10:00	**Re-Opening Notes: Oded Goldreich**	
Session 4	Chair: Phil Rogaway	
10:05-10:50	**Benny Applebaum**	*Recent advances in garbling circuits*
11:10-12:00	**Rafail Ostrovsky and Daniel Wichs**	*Private RAM Computation*
	Lunch	
Session 5	Chair: Ran Canetti	
13:45-14:30	**Iftach Haitner**	*Coin Flipping Implies One-Way Functions*
14:50-15:50	**Abhishek Jain and Huijia (Rachel) Lin**	*Concurrent Security - A Survey*
	Coffee Break	
Session 6	Chair: Eyal Kushilevitz	
16:20-16:35	**Yevgeniy Dodis**	*Key derivation without entropy waste*
16:40-17:40	**Amit Sahai and Brent Waters**	*The Cryptographic Lens, General-Purpose Obfuscation and its Applications*
17:50-18:20	**Panel discussion on Future Directions**	*Ivan Damgard, Yuval Ishai, Tal Malkin, Daniele Micciancio, and Amit Sahai*
18:25	**A closing note: Oded Goldreich**	
	Dinner (in Jaffa, provided incl transportation)	



Supported by the I- CORE program of the planning and budgeting committee and the Israel science foundation