

Workshop on Cryptographic Protocols

<http://www.zurich.ibm.com/bertinoro07/>

Sunday, 4 March 2007

- 15:00 Welcome Reception,
University Residential Center
- 20:00 Dinner

Monday, 5 March 2007

- 9:00 Statistically-Hiding Commitment from Any One-Way Function Omer Reingold
- Efficient Arguments without Short PCPs Yuval Ishai
- 12:45 Coffee
- 11:00 ZK from MPC Eyal Kushilevitz
- Almost-Everywhere Secure Computation Juan A. Garay
- 12:45 Lunch
- 14:30 Tweaking Kurosawa and Desmedt: A New Approach for Building Efficient CCA-Secure Encryption based on DDH Eike Kiltz
- New Lower Bound on Oblivious Transfer Reduction Kaoru Kurosawa
- The Need for Automated Design of Cryptographic Protocols Yvo Desmedt
- 16:30 Coffee/Tea
- 17:00 Non-Malleable Hash Functions Marc Fischlin
- Deniability and Composability Joern Müller-Quade
- 18:30 End
- 20:00 Dinner (Rest. Belvedere, village main square)

Tuesday, 6 March 2007

- 9:00 Key-Dependent Message Security in the Standard Model Dennis Hofheinz
- Identity-based Authenticated Key Exchange in the Standard Model Kenneth Paterson
- 10:30 Coffee

11:00	Secure Multi-Party Computation vs. Secure Function Evaluation	Martin Hirt
	Universally Composable Security with Global Setup	Yevgeniy Dodis
12:45	Lunch	
14:30	Some Comments on Security Goals in the Presence of Malicious Insiders	Rainer Steinwandt
	Adaptive Oblivious Transfer from Blind Signatures	Gregory Neven
	Adaptive Security and Practical Blind Signatures	Aggelos Kiayias
16:30	Coffee/Tea	
17:00	New Techniques for Ring Signatures and Beyond	Xavier Boyen
	Improved On-line/Off-line Threshold Signatures	Emmanuel Bresson
18:30	End	
19:00	Visit to Inter-Faith Museum	
20:00	Dinner (Canteen, University Residential Center)	

Wednesday, 7 March 2007

9:00	Concurrent Non-Malleability Secure Proof Systems Under Man-in-the-Middle Attacks	Giuseppe Persiano Ivan Visconti
10:30	Coffee	
11:00	Smooth Sensitivity and Sampling in Private Data Analysis	Adam Smith
	Privacy-Preserving Imputation of Missing Data	Rebecca Wright
	A Privacy-Protecting Multi-Coupon Scheme with Stronger Protection against Splitting	Hans Löhr
12:45	Lunch	
14:30	Departure for Sightseeing tour to Ravenna (with dinner)	

Thursday, 8 March 2007

9:00	(Password) Authenticated Key Establishment	Michel Abdalla
	Faster and Shorter Password-Authenticated Key Exchange	Rosario Gennaro
10:30	Coffee	
11:00	Simulatable VRFs and applications for NIZK	Anna Lysyanskaya

	Impossibility of Perfect NIZK with Adaptive Soundness under Standard Assumptions	Masayuki Abe
12:45	Lunch	
14:30	On Relationship of Three Cryptographic Channels	Tatsuaki Okamoto
	Specifications and analysis of modular, layered applied security protocols	Amir Herzberg
	On Cutting Protocols In Smaller Pieces	Douglas Wikstrom
16:30	Coffee/Tea	
17:00	An Efficient Protocol for Secure Two-Party Computation in the Presence of Malicious Adversaries	Benny Pinkas
	Practical and Secure Solutions for Integer Comparison	Berry Schoenmakers
18:30	End	
20:00	Dinner (Osteria della Serafina, Via Roma, 29)	

Friday, 9 March 2007

9:00	Auxiliary Input in the Random Oracle Model	Dominique Unruh
	Introduction to Bounded-Retrieval Model	Stefan Dziembowski
10:30	Coffee	
11:00	Strongly Multiplicative Hierarchical Threshold Secret Sharing	Emilia Käsper
	Strong Corruptions in Group Key Exchange	Mark Manulis
12:45	Lunch	