Programme

Workshop: Theory and Practice of Secure Multiparty Computation

My 5 to 9, 2014
Aarhus University, Denmark

SCIENTIFIC ORGANIZERS

Ivan Bjerre Damgård
Claudio Orlandi
Jesper Buus Nielsen
Aarhus University
Department of Computer Science

cfem.dk
THE ELECTRONIC MARKETS OF THE FUTURE

CTIC
交互计算

Monday, May 5, 2014

TIME	ACTIVITIES
1200	*Registration opens*
1300-1430	**Tutorial: Candidate Multilinear Maps** Sanjam Garg
1430-1500	*Break*
1500-1630	**Tutorial: Garbled Circuits Old and New** Vinod Vaikuntanatan

Tuesday, May 6, 2014

TIME	ACTIVITIES
0900-0945	**Outsourcing RAM Computation** Daniel Wichs
0945-1030	**Efficient Oblivious Transfer Extensions and Applications** Thomas Schneider
1030-1100	*Break*
1100-1145	**Reconstructing a shared secret in the presence of faulty shares - a survey** Serge Fehr
1145-1230	**Practical Private Database Querying** Vladimir Kolesnikov
1230-1400	*Lunch (on your own)*
1400-1445	**Structured Encryption and Leakage Suppression** Seny Kamara
1445-1530	**Size-Hiding Secure Computation: Revisiting the Ideal Model** Melissa Chase
1530-1600	*Break*
1600-1645	**Arithmetic Cryptography** Benny Applebaum

Wednesday, May 7, 2014

TIME	ACTIVITIES
0900-0945	**5 years of FHE** Zvika Brakerski
0945-1030	**Outsourced Pattern Matching** Carmit Hazay
1030-1100	*Break*
1100-1145	**On the Intrinsic Complexity of Broadcast** Martin Hirt
1145-1230	**Faster Private Set Intersection based on OT Extension** Benny Pinkas
1230-1330	*Lunch for all (included)*
1330-1600	Outing to The Old Town

Thursday, May 8, 2014

TIME	ACTIVITIES
0900-0945	**Circuits Resilient to Additive Attacks with Applications to Secure Computation** Yuval Ishai
0945-1030	**Distributed Obfuscation and Non-Interactive Secure Multiparty Computation** Eyal Kushilevitz
1030-1100	*Break*
1100-1145	**Indistinguishability Obfuscation from Semantically-Secure Multilinear Encodings** Rafael Pass
1145-1230	**2-party Secure Computation & Applications** Abhi Shelat
1230-1400	*Lunch (on your own)*
1400-1445	**Large-Scale Secure Computation** Elette Boyle
1445-1530	**FleXOR: Flexible garbling for XOR gates that beats free-XOR** Mike Rosulek
1530-1600	*Break*
1600-1645	**Performance Optimization of Linear Secret Sharing MPC for Real Applications** David Archer
1730-1815	**Rump Session** Part 1 Session Chair: Carmit Hazay
1815-1915	**Demo Session & Workshop Dinner –** main course
1915-2000	**Rump Session** Part 2 Session Chair: Carmit Hazay
2000-2100	**Demo Session & Dessert**
2100	**Goodnight**

■ Friday, May 9, 2014

TIME	ACTIVITIES
0900-0945	**TBD** Elaine Shi
0945-1030	**Advances in Obfuscation** Amit Sahai
1030-1100	*Break*
1100-1145	**Private Function Evaluation: A General Framework and Efficient Instantiations** Payman Mohassel
1145-1230	**Adaptive MPC from New Notions of Non-Malleability** Muthu Ramakrishnan Venkitasubramaniam
1230-	Wrap-up and end of workshop

For abstracts and more information about the speakers, please visit www.cfem.au.dk