PARTICIPANTS

Program

Workshop: Theory and Practice of Multiparty Computation

June 4 to 8, 2012
Aarhus University, Denmark

SCIENTIFIC ORGANIZERS

Ivan Damgaard
Carmit Hazay
Jesper Buus Nielsen
Aarhus University
Department of Computer Science

cfem.dk THE ELECTRONIC MARKETS OF THE FUTURE

CTIC 交互计算

Danmarks Grundforskningsfond Danish National Research Foundation

The Danish Council for Strategic Research

Venues

All lectures take place at:
Aarhus University
Department of Computer Science
Entrance: Finlandsgade 19-21
DK-8200 Aarhus N

Nygaard – building no. 5335
Lecture room: 'Peter Bøgh Andersen' Nygaard-016

Note! *Due to a national holiday on June 5, the entrances are locked. Please use the pin code on the back of your name tag.*

Lunch on June 5 takes place at:
INCUBA Science Park
Aabogade 15
8200 Aarhus N

Download map of the workshop area (pdf)

Please note that the program may be subject to last-minute changes.

■ Monday, June 4 2012	
TIME	**ACTIVITIES**
08:15-09:00	Registration
09:00-10:30	**Jesper Buus Nielsen** – *Aarhus University* Tutorial: Introduction to Multiparty Computation, basic concepts and definitions
10:30-11:00	*Coffee and networking*
11:00-12:30	**Ivan Bjerre Damgård** – *Aarhus University* Tutorial: MPC protocols for honest majority
12:30-14:00	*Lunch break (food not included)*
14:00-15:30	**Benny Pinkas** – *Bar Ilan University and Google* Tutorial: MPC protocols for dishonest majority
15:30-?	*Coffee and networking*

■ Tuesday, June 5 2012	
TIME	**ACTIVITIES**
09:00-09:45	**Janus Dam Nielsen** – *the Alexandra Institute* An introduction to FRESCO - Framework for Realizing Efficient Secure Computations
09:45-10:30	**Thomas Schneider** – *TU Darmstadt* Secure Set Intersection with Untrusted Hardware Tokens
10:30-11:00	*Coffee and networking*
11:00-11:45	**Benny Pinkas** – *Bar Ilan University and Google* Secure Computation on the Web: Computing without Simultaneous Interaction
11:45-12:30	**Tal Malkin** – *Columbia University* Multi-Party Computation for Polynomials and Branching Programs without Simultaneous Interaction
12:30-14:00	*Lunch in INCUBA Science Park, Aabogade 15, Aarhus N*
14:00-14:45	**Shai Halevi** – *IBM Research* Fully Homomorphic Encryption with Polylog Overhead
14:45-15:30	**Ran Canetti** – *Boston University and Tel Aviv University* How to Bootstrap a SNARK in Public
15:30-16:00	*Coffee and networking*
16:00-16:45	**Abhi Shelat** – *University of Virginia* Billion Gate Malicious Yao
18:30- ?	*Rump session buffet outside the lecture room*

■ Wednesday, June 6 2012	
TIME	**ACTIVITIES**
09:00-09:45	**Ivan Damgård** – *Aarhus University* Multiparty Computation in the preprocessing model
09:45-10:30	**Ueli Maurer** – *ETH Zürich* Constructive cryptography and secure multi-party computation
10:30-11:00	*Coffee and networking*
11:00-11:45	**Jonathan Katz** – *Maryland University* Recent results on game theory and secure computation
11:45-12:30	**Marcel Keller** – *University of Bristol* AES in MPC on FHE is 10^5 faster than AES in FHE
12:30-14:00	*Lunch break (food not included)*
14:00-14:45	**Tal Rabin** – *IBM Research* Perfectly-Secure Multiplication for Any $t < n/3$
14:45-15:30	**Yuval Ishai** – *Technion* Share Conversion and Private Information Retrieval
15:30-16:00	*Coffee and networking*
16:00-16:45	**Rafael Pass** – *Cornell University* An Epistemic Approach to Mechanism Design

■ Thursday, June 7 2012	
TIME	**ACTIVITIES**
09:00-09:45	**Jesper Buus Nielsen** – *Aarhus University* A New Approach to Practical Active-Secure Two-Party Computation
09:45-10:30	**Benny Appelbaum** – *Tel Aviv University* New Advances in Garbling Circuits
10:30-11:00	*Coffee and networking*
11:00-11:45	**Eyal Kushilevitz** – *Technion* On the Power of Correlated Randomness in Secure Computation
11:45-12:30	**Dan Bogdanov** – *Cybernetica* Easily programmable secure multi-party computation on integers, strings and floating point numbers
12:30-14:00	*Lunch break (food not included)*
14:00-14:45	**Martin Hirt** – *ETH Zürich* Hyper-Invertible Matrices and Applications
14:45-15:30	**Serge Fehr** – *CWI Amsterdam* Near-Linear Unconditionally-Secure Multiparty Computation with a Dishonest Minority
15:30-16:00	*Coffee and networking*

■ Friday, June 8 2012	
TIME	**ACTIVITIES**
09:00-09:45	**Claudio Orlandi** – *Bar Ilan University* Hiding the Input-Size in Secure Two-Party Computation
09:45-10:30	**Juan A. Garay** – *AT&T Labs – Research* Secure Computation and the Combinatorics of Hidden Diversity
10:30-11:00	*Coffee and networking*
11:00-11:45	**Hoeteck Wee** – *George Washington University* Functional Encryption with Bounded Collusions via Multi-Party Computation
11:45-12:30	**Craig Gentry** – *IBM Research* Quadratic Span Programs and Succinct NIZKs without PCPs

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