Foundations and Applications of Zero-Knowledge Proofs

Monday 2 – Friday 6 September 2024

The programme is subject to change. All times are British Summer Time (BST).

MONDAY 2 SEPTEMBER 2024	
09.15 - 10.00	Registration and Refreshments
10.00 - 10.30	Welcome and Housekeeping
10.30 - 11.30	**Jonathan Katz**, Google / University of Maryland *Introduction 1*
11.30 - 12.00	Refreshments
12.00 - 13.00	**Michele Ciampi**, University of Edinburgh *Introduction 2*
13.00 - 14.30	Lunch
14.30 - 15.30	**Michele Ciampi**, University of Edinburgh *Introduction 3*
15.30 - 16.00	Refreshments
16.00 - 17.00	**Jonathan Katz**, Google / University of Maryland *Introduction 4*
17.00 - 18.00	Welcome Reception

TUESDAY 3 SEPTEMBER 2024	
09.15 - 10.00	**Carsten Baum**, Technical University of Denmark *ZK from Symmetric Primitives 1*
10.00 - 10.30	Refreshments
10.30 - 11.30	**Carsten Baum**, Technical University of Denmark *ZK from Symmetric Primitives 2*
11.30 - 12.00	Refreshments
12.00 - 13.00	**Peter Scholl**, Aarhus University *ZK from Symmetric Primitives 3*
13.00 - 14.30	Lunch
14.30 - 15.30	**Q&A Session**
18.00 - 20.00	Public Lecture, hosted in G.03 (ground floor) **Jonathan Katz**, Google / University of Maryland *What do Cryptographers Work On?*

WEDNESDAY 4 SEPTEMBER 2024	
09.15 - 10.00	**Carla Ràfols**, Universitat Pompeu Fabra *Group/pairing zk-SNARKs 1*
10.00 - 10.30	Refreshments
10.30 - 11.30	**Carla Ràfols**, Universitat Pompeu Fabra *Group/pairing zk-SNARKs 2*
11.30 - 12.00	Refreshments
12.00 - 13.00	**Arantxa Zapico**, Ethereum Foundation *Polynomial Commitments*
13.00 - 14.30	Lunch
14.30 - 15.30	**Lightning Talks**
15.30 - 16.00	Refreshments
16.00 - 17.00	**Anca Nitulescu**, Input Output *Zero-knowledge proofs for Blockchains*

THURSDAY 5 SEPTEMBER 2024	
09.15 - 10.00	**Lisa Kohl**, CWI Amsterdam *Compressed Sigma Protocols*
10.00 - 10.30	Refreshments
10.30 - 11.30	**Lisa Kohl**, CWI Amsterdam *Lattice-Based Sigma Protocols*
11.30 - 12.00	Refreshments
12.00 - 13.00	**Ngoc Khanh Nguyen**, King's College London *Exact Lattice-Based Zero-knowledge Proofs*
13.00 - 14.30	Lunch
14.30 - 15.30	**Ngoc Khanh Nguyen**, King's College London *Towards Fast Verification: Polynomial Commitments from Lattices*
15.30 - 16.00	Refreshments
16.00 - 17.00	**Lightning Talks**
19.00 - 22.00	Workshop Dinner

FRIDAY 6 SEPTEMBER 2024	
09.15 - 10.00	**Dario Fiore**, IMDEA Software Institute *Zero-Knowledge Proofs for Secure and Private Machine Learning*
10.00 - 10.30	Refreshments
10.30 - 11.30	**Dario Fiore**, IMDEA Software Institute *Zero-Knowledge Proofs for Verifiable Computation on Encrypted data*
11.30 - 12.00	Refreshments
12.00 - 13.00	**Anca Nitulescu**, Input Output *Zero-knowledge Proofs: How fast can we go?*
13.00 - 14.30	Lunch and End of Workshop