



Institute of
mathematics
& its applications

19th IMA International Conference on Cryptography and Coding

PROGRAMME

Tuesday 12th December

10.00-10.20	Registration and welcome coffee
10.20 -10.30	Welcome from Chair
	Session I - Zero-Knowledge Protocols
10.30-11.00	zk-SNARKs from Codes with Rank Metrics - <i>Xuan-Thanh Do, Dang-Truong Mac and Quoc-Huy Vu</i>
11.00-11.30	Zero-Knowledge Systems from MPC-in-the-Head and Oblivious Transfer Cyprien Delpech de Saint Guilhem, Ehsan Ebrahimi and Barry van Leeuwen
11.30-12.00	ZK-for-Z2K: MPC-in-the-Head Zero-Knowledge Proofs for Z2k - <i>Lennart Braun, Cyprien Delpech de Saint Guilhem, Robin Jadoul, Emmanuela Orsini, Nigel P. Smart and Titouan Tanguy</i>
12.00-13.30	Lunch
13.30-14.30	Invited Talk - <i>Carla Ràfols</i> (Pompeu Fabra University)
14.30-15.00	Coffee break
	Session II - Digital Signature Schemes and Extensions
15.00-15.30	Efficient Secure Two Party ECDSA - <i>Sermin Kocaman and Younes Talibi Alaou</i>
15.30-16.00	Selective Delegation of Attributes in Mercurial Signature Credentials - <i>Colin Putman and Keith M. Martin</i>
16.00-17.00	Poster session and Reception drinks

Wednesday 13th December

10.00-10.30	Welcome coffee
	Session III - Post-Quantum Cryptography
10.30-11.00	Middle-Products of Skew Polynomials and Learning with Errors - <i>Andrew Mendelsohn and Cong Ling</i>
11.00-11.30	Identity-Based Threshold Signatures from Isogenies - <i>Shahla Atapoor</i>
	Session IV - Cryptography in Practice: Analyses and Constructions
11.30-12.00	Dynamic Security Aspects of Onion Routing - <i>Alessandro Melloni, Martijn Stam and Øyvind Ytrehus</i>
12.00-12.30	Practical and Efficient FHE-based MPC - <i>Nigel P. Smart</i>
12.30-14.00	Lunch
14.00-15.00	Invited Talk - <i>Dario Fiore</i> (IMDEA Software Institute)
15.00-15.30	Coffee break
	Session V - Symmetric Cryptography
15.30-16.00	Feistel Ciphers Based on A Single Primitive - <i>Kento Tsuji and Tetsu Iwata</i>
16.00-16.30	Rectangle Attacks on Reduced Versions of the FBC Block Cipher - <i>Wenchang Zhou and Jiqiang Lu</i>
16.30	Session ends
17.30-20.30	Conference dinner

14th December 2023

10.00-10.30	Welcome coffee
	Session VI - Coding Theory
10.30-11.00	An Upper-Bound on the Decoding Failure Probability of the LRPC Decoder - <i>Étienne Burle and Ayoub Otmani</i>
11.00-11.30	Coset leaders of the first order Reed-Muller codes in the classes of Niho functions and Threshold functions - <i>Serge Christian Feukoua Jonzo</i>
11.30-12.00	Revisiting Nearest-Neighbor-Based Information Set Decoding- <i>Andre Esser</i>
12.00	Conference ends