Institute of mathematics & its applications

16th IMA International Conference on Cryptography and Coding

Tuesday 12 - Thursday 14 December 2017, St Catherine's College, University of Oxford

Programme

Tuesday 12 December	
0830 – 0930	Registration
0930 – 0940	Opening remarks
0940 – 1040	**Invited Talk** *Chair: Anthony Barnett* Fully Homomorphic Encryption, recent constructions and open problems *Daniele Micciancio*
1040 – 1105	**Order Revealing Encryption** *Chair: Anthony Barnett*
1040 – 1105	Revealing Encryption for Partial Ordering *Helene Haagh, Claudio Orlandi, Chenxing Li, Yue Ji and Yifan Song.*
1105 – 1130	**Break**
1130 – 1245	**Homomorphic Encryption and Secure Computation** *Chair: Guang Gong*
1130 – 1155	Dynamic Multi Target Homomorphic Attribute-Based Encryption *Ryo Hiromasa and Yutaka Kawai.*
1155 – 1220	Practical Homomorphic Encryption Over the Integers for Secure Computation in the Cloud *James Dyer, Martin Dyer and Jie Xu*
1220 – 1245	When It's All Just Too Much: Outsourcing MPC-Preprocessing *Peter Scholl, Nigel Smart and Timothy Wood*
1245 – 1345	**Lunch**
1345 – 1525	**Special Session: Lattice-Based Cryptographic Constructions & Architectures** *Chairs: Martin Albrecht, Máire O'Neill*
1345 – 1410	If and how implementation attacks shape the design of lattice-based signature schemes *Nina Bindel*
1410 – 1435	Efficient Implementation of Lattice-based Cryptography for Embedded Devices *Tim Güneysu, Tobias Oder*
1435 – 1500	Exploring Fault Attacks Resistance and Possible Countermeasures for Lattice Based Cryptography *Francesco Regazzoni*
1500 - 1525	Practical Post-quantum (H)IBE *Peter Campbell, Michael Groves*
1525 – 1550	**Break**
1550 – 1640	**Coding Theory** *Chair: Edoardo Persichetti*
1550 – 1615	On the probability of incorrect decoding for linear codes *Marco Frego*
1615 – 1640	Improvement on minimum distance of symbol-pair codes *Han Zhang*
1640 - 1740	**Drinks reception**

Wednesday 13 December	
0940 – 1040	**Invited Talk** *Chair: Máire O'Neill* A Decade of Direct Anonymous Attestation - From Research to Standard to Research *Jan Camenisch*
1040 – 1105	**Cryptanalysis** *Chair: Yvo Demesdt*
1040 – 1105	MILP-based Cube Attack on the Reduced-Round WG-5 Lightweight Stream Cipher *Raghvendra Rohit, Riham Altawy and Guang Gong*
1105 – 1130	**Bilinear & Multilinear Maps** *Chair: Yvo Demesdt*
1105 – 1130	Notes On GGH13 Without The Presence Of Ideals *Martin Albrecht, Alex Davidson and Enrique Larraia*
1130 – 1155	**Break**
1155 – 1245	**Signatures** *Chair: Chik How Tan*
1155 – 1220	Attribute-Based Signatures with User-Controlled Linkability without Random Oracles *Ali El Kaafarani, Essam Ghadafi*
1220 – 1245	How Low Can You Go? Short Structure-Preserving Signatures for Diffie-Hellman Vectors *Essam Ghadafi*
1245 – 1345	**Lunch**
1345 – 1445	**Invited Talk** *Chair: Francesco Regazonni* Quantum Safe Cryptography from Codes: Present and Future *Nicolas Sendrier*
1445 – 1600	**Post-Quantum Cryptography** *Chair: Francesco Regazonni*
1445 – 1510	CAKE: Code-based Algorithm for Key Encapsulation *Paulo S. L. M. Barreto, Shay Gueron, Tim Guneysu, Rafael Misoczki, Edoardo Persichetti, Nicolas Sendrier and Jean-Pierre Tillich*
1510 – 1535	A Practical Implementation of Identity-Based Encryption over NTRU Lattices *Sarah McCarthy, Neil Smyth and Elizabeth O'Sullivan*
1535 – 1600	A note on the implementation of the Number Theoretic Transform *Michael Scott*
1600 – 1625	**Break**
1625 – 1715	**Homomorphic Signatures** *Chair: Claudio Orlandi*
1625 – 1650	A Linearly Homomorphic Signature Scheme From Weaker Assumptions *Lucas Schabhüser, Johannes Buchmann and Patrick Struck*
1650 – 1715	Subset Signatures with Controlled Context-Hiding *Essam Ghadafi*
1900	**Conference Dinner**

Thursday 14 December	
0940 – 1040	**Invited Talk** *Chair: Ciara Rafferty* A journey in the land of (hash-and-sign) lattice-based signatures *Thomas Prest*
1040 – 1105	**Symmetric Cryptography** *Chair: Ciara Rafferty*
1040 – 1105	Orthogonal MDS Diffusion Matrices over Galois Rings *Chik How Tan and Theo Fanuela Prabowo.*
1105 – 1130	**Break**
1130 – 1245	**Cryptanalysis** *Chair: Michael Scott*
1130 – 1155	Lattice Attacks on Pairing-Based Signatures *Thierry Mefenza and Damien Vergnaud*
1155 – 1220	Lattice Reductions over Euclidean Rings with Applications to Cryptanalysis *Taechan Kim and Changmin Lee*
1220	**Closing Remarks**
1250 – 1350	**Lunch served in the Dining Hall**

This conference is supported by

SAFE crypto