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

| **Wednesday 13 December** | |
|---|---|
| 0940 – 1040 | **Invited Talk**<br>A Decade of Direct Anonymous Attestation - From Research to Standard to Research<br>*Jan Camenisch* |
| 1040 – 1155 | **Bilinear & Multilinear Maps** |
| 1040 – 1105 | Bilinear cryptography using groups of nilpotency class 2<br>*Ayan Mahalanobis, Pralhad Shinde* |
| 1105 – 1130 | Notes On GGH13 Without The Presence Of Ideals<br>*Martin Albrecht, Alex Davidson and Enrique Larraia* |
| 1130 – 1155 | **Break** |
| 1155 – 1245 | **Signatures** |
| 1155 – 1220 | Attribute-Based Signatures with User-Controlled Linkability without Random Oracles<br>*Ali El Kaafarani, Essam Ghadafi* |
| 1220 – 1245 | How Low Can You Go? Short Structure-Preserving Signatures for Diffie-Hellman Vectors<br>*Essam Ghadafi* |
| 1245 – 1345 | **Lunch** |
| 1345 – 1445 | **Invited Talk**<br>Quantum Safe Cryptography from Codes: Present and Future<br>*Nicolas Sendrier* |
| 1445 – 1600 | **Post-Quantum Cryptography** |
| 1445 – 1510 | CAKE: Code-based Algorithm for Key Encapsulation<br>*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<br>*Sarah McCarthy, Neil Smyth and Elizabeth O'Sullivan* |
| 1535 – 1600 | A note on the implementation of the Number Theoretic Transform<br>*Michael Scott* |
| 1600 – 1625 | **Break** |
| 1625 – 1715 | **Homomorphic Signatures** |
| 1625 – 1650 | A Linearly Homomorphic Signature Scheme From Weaker Assumptions<br>*Lucas Schabhüser, Johannes Buchmann and Patrick Struck* |
| 1650 – 1715 | Subset Signatures with Controlled Context-Hiding<br>*Essam Ghadafi* |
| 1900 | **Conference Dinner** |

| Thursday 14 December | |
|---|---|
| 0940 – 1040 | **Invited Talk**<br>Falcon: Fast-Fourier, Lattice-based, Compact Signatures over NTRU<br>*Thomas Prest* |
| 1040 – 1105 | **Symmetric Cryptography** |
| 1040 – 1105 | Orthogonal MDS Diffusion Matrices over Galois Rings<br>*Chik How Tan and Theo Fanuela Prabowo.* |
| 1105 – 1130 | **Break** |
| 1130 – 1245 | **Cryptanalysis** |
| 1130 – 1155 | MILP-based Cube Attack on the Reduced-Round WG-5 Lightweight Stream Cipher<br>*Raghvendra Rohit, Riham Altawy and Guang Gong* |
| 1155 – 1220 | Lattice Attacks on Pairing-Based Signatures<br>*Thierry Mefenza and Damien Vergnaud* |
| 1220 – 1245 | Lattice Reductions over Euclidean Rings with Applications to Cryptanalysis<br>*Taechan Kim and Changmin Lee* |
| 1245 – 1250 | **Closing Remarks** |
| 1250 – 1350 | **Lunch** |

**This conference is supported by**

SAFEcrypto