FOUNDATIONS AND APPLICATIONS OF LATTICE-BASED CRYPTOGRAPHY	
MONDAY 25 JULY 2022	
08.30 - 09.25	Registration
09.25 – 09.30	ICMS Welcome and Housekeeping
09.30 – 11.00	**Introduction to lattice-based Cryptography** Damien Stehlé (ENS Lyon)
11.00 - 11.30	Refreshment Break
11.30 - 12.30	**Introduction to lattice-based Cryptography** Damien Stehlé (ENS Lyon)
12.30 - 14.00	Lunch
14.00 - 15.00	**Lightning Talks (Session 1)**
15.00 - 15.30	Refreshment Break
15.30 - 17.00	**Algebraic lattices for cryptography** Alice Pellet-Mary (CNRS and Bordeaux University)
17.00 – 18.00	Welcome Reception, ICMS
TUESDAY 26 JULY 2022	
09.00 - 10.30	**Solving the Learning with Errors Problem** Martin Albrecht (Royal Holloway, University of London)
10.30 - 11.00	Refreshment Break
11.00 - 12.00	**Introduction to FHE and the TFHE scheme** Ilaria Chillotti (ZAMA)
12.00 - 14.00	Lunch
14.00 - 15.00	**Cryptanalysis (Lab Session)** Martin Albrecht (Royal Holloway, University of London)
15.00 - 15.30	Refreshment Break
15.30 - 17.00	**Introduction to FHE and the TFHE scheme** Ilaria Chillotti (ZAMA)
18.00 - 19.00	Public Lecture by Luca De Feo (IBM Research Europe), G.03 Bayes Centre
WEDNESDAY 27 JULY 2022	
09.00 - 10.30	**Challenges and open problems in Fully Homomorphic Encryption** Anamaria Costache (Norwegian University of Science and Technology)
10.30 - 11.00	Refreshment Break
11.00 - 12.00	**Lightning Talks (Session 2)**
12.00 - 14.00	Lunch
14.00 - 15.00	**Algebraic lattices for cryptography** Alice Pellet-Mary (CNRS and Bordeaux University)
15.00 - 15.30	Break
15.30 - 17.00	Research Area Mixer, ICMS, Bayes Centre
18.00 – 20.00	Workshop Dinner, Blonde Restaurant, 71-75 St. Leonard's St, Edinburgh
THURSDAY 28 JULY 2022	
09.00 - 10.30	**Isogeny-based cryptography: why, how, and what next?** Chloe Martindale (University of Bristol)
10.30 - 11.00	Refreshment Break
11.00 - 12.00	**Unexpected discoveries and challenges in isogeny based cryptography** Luca De Feo (IBM Research Europe)
12.00 - 14.00	Lunch and End of Workshop

Sponsors and Funders:

ICMS

PQSHIELD

ZAMA