Spring School on Lattice-Based Cryptography

Oxford, 20-24 March, 2017

1 School Overview

The Spring school will take place in March (20-24th), 2017 at the Mathematical Institute, University of Oxford. It aims at covering lattices, their role in modern cryptography, and their potential use in the post-quantum era. Namely, it will cover the basics of lattices, "hard" lattice-problems and the reductions between them, and advanced lattice-based cryptography constructions (e.g. Fully Homomorphic Encryption). The school will also have practical sessions using SageMath.

Target Audience: Graduate students and Postdocs.

2 Schedule

	Monday	Tuesday	Wednesday	Thursday	Friday
08.30-09.00			Arrival-Coffee		
09.00-11.00	R. Pinch	R. Pinch	P. Nguyen	Nguyen/Ducas	C. Gentry
11.00-11.30			Coffee Break		
11.30-12.30	L. Ducas	D. Shepherd	M. Albrecht	C. Gentry	D. Shepherd
12.30-13.30			Lunch		
13.30-14.30	D Shepherd	N. Smart	D. Shepherd	C. Gentry	P. Nguyen
14.30-15.00			Tea		
15.00-17.00	–	D. Pasechnik	Albrecht/Ducas	Albrecht/Ducas	L. Ducas (1 hour)

- R. Pinch: Mathematical Introduction to Lattices.
- L. Ducas: Cryptanalysis, Constructions and Implementation.
- N. Smart: Guest Lecturer.
- P. Nguyen: Cryptanalysis.
- D. Shepherd: Quantum Attacks on Lattices.
- C. Gentry: Fully Homomorphic Encryption.
- M. Albrecht: Cryptanalysis, Constructions and Implementation.
- D. Pasechnik: Introduction to SageMath/Python.

For more details, visit
`https://www.maths.ox.ac.uk/groups/cryptography/spring-school-lattice-based-cryptography`