Oxford Post-Quantum Cryptography Workshop 2019

Oxford, 18-22 March, 2019

1 Workshop Overview

The Workshop will take place in March (18-22th), 2019 at the Mathematical Institute, University of Oxford. The event, that is by invitation only, is meant to bring together the top researchers in the field of Post-Quantum Cryptography for a week of fruitful discussions and exchange of ideas. During the week, each morning there will be 2 talks on various Post-Quantum fields. Each talk will be an overview of the techniques used in each PQ field - lattice-based cryptography, hash-based cryptography, code-based cryptography, isogeny-based cryptography and multivariate cryptography - with a dedicated focus to NIST submissions, and their state-of-the-art cryptanalysis. One of the talks will be on the NIST standardization process by Dustin Moody (NIST). The morning talks will be followed by (group) working sessions, where teams will work on research problems.

Target Audience: Post-Quantum Cryptography researches

2 Schedule

Rooms: **L2** on Mon, Tue, Thu - **L3** on Wed, Fri (Mezzanine floor)

Social Dinner sponsored by PQShield: St John's College, St Giles', Oxford OX1 3JP

	Monday	Tuesday	Wednesday	Thursday	Friday
08.30-09.00	Registration	Arrival-Coffee	Arrival-Coffee	Arrival-Coffee	Arrival-Coffee
09.00-09.45	A. Huelsing	E. Persichetti	D. Moody	C. Peikert	C. Martindale
09.45-10.30	E. Persichetti	B. Yang	C. Costello	C. Peikert	Groups talks
10.30-11.00	Coffee Break	Coffee Break	Coffee Break	Coffee Break	Coffee Break
11.00-12.00	Group session	Group session	Group session	Group session	Groups talks
12.00-12.30	Group session	Group session	Group session	Group session	Groups talks
12.30-13.30	Lunch	Lunch	Free afternoon	Lunch	Lunch
13.30-15.30	Group session	Group session		Group session	
15.30-16.00	Tea	Tea		Tea	
19.00-21.00				Dinner sponsored by PQShield	

- Andreas Huelsing: hash-based cryptography.
- Edoardo Persichetti: code-based cryptography.
- Bo-Yin Yang: multivariate cryptography.
- Dustin Moody: NIST standardization process.
- Chris Peikert: lattice-based cryptography.
- Craig Costello: isogeny-based cryptography.
- Chloe Martindale: isogeny-based cryptography.

For more details, visit:
https://www.maths.ox.ac.uk/events/conferences/oxford-post-quantum-cryptography-workshop