Oxford PQC Workshop - Alessandro Budroni

On Sunday 17th of March, I travelled to Oxford to attend to the Oxford Post-Quantum Cryptography Workshop.

This event, organized by the Mathematical Institute of University of Oxford, consisted in many seminars on many different topics related to Post-Quantum Cryptography: Hash-based Cryptography, Lattice-based Cryptography, Isogeny-based Cryptography, Code-based Cryptography, and Multivariate-based Cryptography. Those seminars were held by some of the most proficient researchers of the fields.

In particular I enjoyed very much the talk about Chris Peikert from University of Michigan (US) on Lattice-based Cryptography, with a particular focus on the NIST applications. Since my PhD main topic is cryptanalysis on Learning With Errors (LWE), which is a lattice-related hard problem, this was of fundamental interest to me. I have been able to follow in details all the presentation and I got many clarifications on other aspects of the field which I had not investigated yet.

I also benefited from the talk by Edoardo Persichetti from Florida Atlantic University on Code-based Cryptography. Even if it is not exactly my field, this field is strictly related to it, and my background on coding-theory allowed me to get a good understanding on which are its open problems.

Another seminar which was extremely beneficial was held by Dustin Moody from NIST. He talked about the NIST standardization process on Post-Quantum Cryptography, and, in particular, he described the acceptance criteria for the NIST competition.

However, a big part of the workshop consisted in group sessions where the participants were asked to work on a problem together. There were eleven different group which covered some of the most important open problems in Post-Quantum Cryptography. I spent all the five days on the same one: “Effects of decryption failures”. It was led by Jan-Pieter D'Anvers, who is an expert on the field.

The first day we revised the background of the field and the last results. Then we started working on the problem itself. The last day we actually got some small result which we presented quickly to all the participant of the workshop the last day.

I finally came back to Bergen the 22th of March together with my colleague Wrya Kadir, who also attended to the Workshop.

In addition to improving and deepening my knowledge, this event served to me as an opportunity to make connections and grow my network among the best researchers of the field. Furthermore I had many input for open problems on which I would like to work on.

I greatly thank Coins for supporting me financially to attend to the Oxford Post-Quantum Cryptography Workshop. It was probably one of the experiences I have benefited most.