EUROCRYPT 2019

19-23 MAY 2019
Mattia Veroni

Supported by COINS, I attended EUROCRYPT 2019, the main European conference on Cryptography and its applications.
This year's edition has been held in Darmstadt, a relatively small city in Germany. The most practical way to reach the city from Trondheim is to fly (with one layover) to Frankfurt and then take a bus to the city of Darmstadt.

As a group, all of us from NTNU Trondheim chose to stay at the Welcome hotel, situated only a few hundred meters from the conference venue. The strategical position of the hotel and the high standards that it meets made our choice the best possible in terms of convenience. The food (breakfast) was amazing, the rooms tidy and cozy, the receptionists always available and kind. The hotel has also an underground connection with the Darmstadium, which turned to be very practical due to the heavy rain we had during our stay.

The conference had an incredibly large number of talks (76, divided in 2 sessions) and sometimes it has been difficult to choose among two equally interesting ones which took place at the same time. A full list of the papers can be found in the "Program" section at Eurocrypt 2019 webpage (link can be found at the bottom of this file).
The following are those that I preferred in terms of waltz of the talk and personal interest in the subject:

- "Quantum Circuits for the CSIDH: Optimizing Quantum Evaluation of Isogenies", by Daniel J. Bernstein. The paper is quite technical in terms of implementative details and performances analysis, but Bernstein gave an amazing talk, very involving and clear;
- "Fully homomorphic encryption from the ground up", by Daniele Micciancio. Professor Micciancio gave an invited talk on the very hot topic of bootstrapping techniques for FHE schemes. In particular he focus on Lattice-based cryptography, due to simplicity and speed that this solution offers;
- "Efficient Verifiable Delay Functions", by Benjamin Wesolowski. I already had the chance to listen to him during the Winter school that I attended in March 2019 (supported by COINS) and he confirmed himself to be a very good speaker. He talked about the VDF they have been able to obtain by exploiting squarings in a group. The underlying mathematics is quite simple and elegant, two great attributes that have earned him the Best Young Researcher Paper Award at this conference.
- "SeaSign: Compact Isogeny Signatures from Class Group Actions", by Luca de Feo. One of the most famous researchers in the field, Luca gave an incredibly clear and effective talk, despite of the hardness of the topic. He has been able to explain the ideas of the paper without falling in the rabbit hole made of technicalities and algebraic tricks. The result is not efficient enough to be deployed in practice, but it is a great starting point to find better ideas in terms of usability.

Two whole sessions were dedicated to Post-quantum cryptography, the exact topic of my PhD research program. I had the chance to discuss isogeny-based cryptography with Luca de Feo and Chloe Martindale, two young and gifted researchers in this area.

Although it was an option, I decided to not attend any workshops, who took place on Saturday and Sunday before the conference start. Some colleagues of mine have attended an handful of them and were very satisfied by the quality and effectiveness.

During my staying I met many other PhD students, PostDocs and professors and created a good network with them. This conference has represented a great opportunity to connect with other researchers and exchange ideas and knowledge. I also had the chance to meet my Master's thesis supervisor and we discussed the eventuality to work on a joint paper.

Overall it has been a very satisfactory experience and I would strongly suggest Eurocrypt to anyone who looks for a top level conference. For anyone interested, it is possible to download all the slides of the talk at
https://eurocrypt.iacr.org/2019/index.html