Report Eurocrypt 2018 - Alessandro Budroni

On Saturday 28th of April, I flew, together with my colleagues Andrea Tenti and Isaac Andrés Canales Martinez, from Bergen to Tel-Aviv. We went there in order to attend the conference Eurocrypt 2018, considered one of the most important conferences related to Cryptography. In order to fly with the cheapest solution, we had to stopover first in Oslo and then in Munich. We arrived in Tel-Aviv on Sunday morning and at 1 pm we got our rooms at the Hotel Leonardo Beach. At 7 pm we had the registration to the conference at the Hotel Dan Panorama, which was about 30 minutes walking from our hotel.

The first day of sessions was the most relevant for me. In the morning there were two parallel tracks: one about Lattices and one about Foundations. I attended to the former since Lattice-Based Cryptography is the topic of my PhD. Two of the talks have been extremely interesting for me: Shortest Vector from Lattice Sieving: a Few Dimensions for Free by Léo Ducas and On the Ring-LWE and Polynomial-LWE problems by Miruna Rosca, Damien Stehlé and Alexandre Wallet. After a coffee break, there were again two parallel tracks of sessions, I followed the one about Fully Homomorphic Encryption. Attending to talks about cryptographic protocols helped me a lot to keep myself updated with this other aspect of Cryptography which I am not investigating in details for my current PhD project.
After a hearty lunch, there was the first invited talk held by Anne Canteaut with the title Desperately Seeking S-boxes, which I found it pretty interesting and helped me to have a better understanding of how boolean functions are applied nowadays in Cryptography. After another coffee break, I followed the sessions about Attribute-Based Encryption, related to the topics which I treated during my previous job, and afterwards the sessions about Secret Sharing.

The second day I attended four sessions about Blockchain. Since it is nowadays one of the hottest topics in Cryptography, it was a good chance to hear new ideas about it. Then, after a coffee break, I attended the sessions about Masking. After the lunch, there was the presentation of the Best Young Researcher Award, which was about The Discrete Logarithm Problem, and the three Best Paper Awards. In the evening, starting from half-past seven, there has been the rump session which I enjoyed it very much.

The third day I attended to topics about Symmetric Cryptanalysis, Zero-Knowledge and Non-Interactive Zero-Knowledge. In particular, I enjoyed the remarkable result in the talk Efficient Designated-Verifier Non-Interactive Zero-Knowledge Proofs of Knowledge by Pyrros Chaidos and Geoffroy Couteau. At seven o'clock we went to a restaurant on the beach for the Banquet organized by the conference. There was first an aperitif on the balcony outside, then the dinner. I had the chance to meet and talk with other researchers from all around the world while tasting typical Israeli food.

The fourth and last day of the conference I attended sessions about Isogeny-Based encryption, Key Exchange protocols and Non-malleable Codes. I am very fascinated by the first topic and I consider it one of the areas that nowadays needs more investigation.

The conference ended on Thursday 5th of May but we decided to stay two days more (at our expense) to visit Jerusalem and Masada. The conference was extremely inspiring from many points of views. Some of the sessions, especially the first talk about lattices, suggested me new directions for my research. Furthermore, I consider very usefully to hear news from different aspects of Cryptography which I do not treat in my PhD project, such us protocol security proofs and Blockchain technology. Finally, I had the chance to meet a lot of interesting people from the different country who work in my field.

I thank Coins for giving me the chance to attend to Eurocrypt2018. This conference motivated me to continue with my job and aim to publish it in one of the IACR conferences in the future.