Reflection report - Eurocrypt 2018

Canales Martínez, Isaac Andrés

COINS supported me to attend Eurocrypt 2018, the 37th Annual International Conference on the Theory and Applications of Cryptographic Techniques. This event took place during April 29 - May 3, 2018 in Tel Aviv, Israel. Eurocrypt is one of the flagship conferences of the International Association for Cryptologic Research (IACR). This conference served as a meeting point for world leading researchers, professionals and practitioners who work in both, theoretical and applied cryptography.

Given the importance of this conference, a great number of papers were presented and the talks were held in two conference rooms simultaneously. Sometimes it was very difficult for me to choose which talk to attend. The full program of the conference, and the actual slides of most of the talks, can be found in the web-page of Eurocrypt 2018: `https://eurocrypt.iacr.org/2018/program.html`.

Broadly, the organisation of the workshop was as follows:

- During the first day, foundational aspects of cryptography, the Random Oracle Model, permutations, modes of operations (Galois counter mode), lattices, fully homomorphic encryption, and attribute-based encryption were the main topics.

- Day 2 focused on Blockchain, private simultaneous messages, multi-collision resistance, signatures and masking. Also, in the afternoon session the best paper award and best young researcher award talks were given. And in the evening, we had the amusing rump session.

- On the third day of the conference, the talks focused on multiparty computation (both, theoretical and implementation aspects), obfuscation, zero knowledge, symmetric cryptanalysis and anonymous communication. This day looked as the most interesting to me given my research topic.

- Finally, Isogeny-based cryptography, key exchange, non-malleable codes, provable symmetric cryptography and postquantum cryptography, were the subjects in the fourth day.

Currently, my research is focused on symmetric key cryptography, particularly on cryptanalysis of stream ciphers. The first invited talk “Desperately Seeking Sboxes” by Anne Canteaut was particularly interesting for me. Anne is a very well known researcher in symmetric key cryptography. In fact, many papers that I have used within my research are authored or co-authored by her.

Although many talks were somehow related to my research topic, the ones that I found most useful and content-relevant were:

- “Desperately Seeking Sboxes” by Anne Canteaut (as already mentioned),
- “Boomerang Connectivity Table: A New Cryptanalysis Tool”,
- “Correlation Cube Attacks: From Weak-Key Distinguisher to Key Recovery”,
- “The Missing Difference Problem, and its Applications to Counter Mode Encryption”, and
- “Fast Near Collision Attack on the Grain v1 Stream Cipher ”.

Additionally, many talks were not directly related to my research, but I found particularly interesting:

- “Naor-Reingold Goes Public: The Complexity of Known-key Security”,
- “Supersingular Isogeny Graphs and Endomorphism Rings: Reductions and Solutions”,
- “Multi-Collision Resistant Hash Functions and their Applications”,
- “Collision Resistant Hashing for Paranoids: Dealing with Multiple Collisions”,
- “Shortest Vector from Lattice Sieving: a Few Dimensions for Free”, and
- “On the Ring-LWE and Polynomial-LWE problems”.

There is no doubt that the highest motivation for attending events like this, is the opportunity to be in touch with cutting-edge research and world leading researchers, as well as to get to know new results and techniques in cryptography. Nevertheless, I would like to mention that these events also serve as a leverage for establishing new personal and professional connections, and are valuable opportunities to get to discover new places.

I finalise this report thanking COINS for having supported my attendance to Eurocrypt 2018.