Mathematical Methods for Cryptography 2017

Canales-Martínez, Isaac Andrés

September 4-8, 2017
Svolvær, Lofoten, Norway

In September 2017, COINS supported me to attend the workshop "Mathematical Methods for Cryptography 2017" (MMC 2017). This event took place during 4-8 September 2017 in Svolvær, Lofoten archipelago, Norway.

This workshop served as a meeting point for researchers, professionals and practitioners of cryptography who work in both, theoretical and applied cryptography. MMC 2017 gathered as speakers a great number of leading researchers and professionals from all over the world. As the name of the workshop suggests, there was a special focus on the mathematical aspects, being boolean functions, discrete logarithm, quantum-resistant cryptography, cryptanalysis and some implementations, the main topics that were addressed. The full program of the workshop, the abstract and the actual slides of most of the talks given, can be downloaded from the event web-page: `http://people.uib.no/chunlei.li/workshops/lofoten/index.html`.

Broadly, the organisation of the workshop was as follows:

- During the first day, quantum-resistant cryptography, cryptocurrencies, cryptographic hardware design, cryptanalysis and cryptanalytic tools were the main topics.
- Day 2 focused on statistical cryptanalysis, boolean functions, Kloosterman sums and filtering functions.
- In the third day of conferences, decoding, error correcting codes, code-based quantum-resistant cryptography and mathematical approaches for cryptanalysis and design of cryptographic primitives, were the subject of the talks.
- Finally, special topics on design and applications of block ciphers, cloud-based applications and services, and distributed data analysis, were the subjects in the fourth day.

Currently, my research is focused on analysis of stream ciphers. Although many talks were related to my research topic, the ones that I found most useful and content-relevant were:

- "Current trends in linear cryptanalysis" by Kaisa Nyberg,
- "Re-linearization and elimination of variables in boolean equation systems" by Bjørn M. Greve,
- "Separable statistics in linear cryptanalysis" by Igor Semaev,
- "An algebraic approach to the design of block ciphers" by Óscar Pereira, and
- "Column-parity mixing layers" by Joan Daemen.

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

- "Combinatorial methods for solving LWE" by Thomas Johansson,
- "A perspective on cryptocurrencies" by Bart Preneel,
- "Hardware design for supersingular isogeny Diffie-Hellman key exchange" by Lejla Batina,
- "Representing integer multiplication using binary decision diagrams" by Håvard Raddum,
- "Computing low-weight discrete logarithms" by Henry Ryan,
- "Code-based post-quantum cryptography" by Jong-Seon No, and
- "A new DDH-based PRF with application to distributed private data analysis" by Filipp Valovich.

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 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 MMC 2017.