A Reflection Report for Attendance at Mathematical Methods for Cryptography workshop

September (4-8th), 2017, Lofoten (Norway)

Navid Ghaedi Bardeh

University of Bergen

I got funding from COINS research school to attend Mathematical Methods for Cryptography workshop in Lofoten, Norway, in Setember 2017.

The workshop organizer invited a lot of famous researchers in field of cryptography. It was a great opportunity to meet researchers from the common field of research. Kaisa Nyberg, Claude Carlet, Joan Daemen, Thomas Johansson, Bart Preneel and Christian Rechberger are invited to give lecture in this workshop.

Full program of the workshop, as well as presentation slides can be downloaded from the webpage of the program[1]. The program constructed with a series of 18 tutorial talks by the listed invited speakers.

The workshop consisted of both invited and submitted presentations, with wide variations of topics. The following is a short summary of some of the invited talks:

Gregor Leander, "Quantum Attacks on Symmetric Cryptography": Gregor Leander talked about "Quantum Attacks on Symmetric Cryptography". He presented a quantum algorithm that breaks the construction with whitening keys in essentially the same time complexity as Grover's original algorithm breaks the underlying block cipher. Technically his result is based on the combination of the quantum algorithms of Grover and Simon.

Bart Preneel, "A Perspective on Cryptocurrencies": Bart Preneel explained about the technological innovations created by cryptocurrencies such as Bitcoin. During his lecture, he explained the principles of distributed currencies and evaluate their strengths and weaknesses. He also gave us an overview of cryptographic research challenges related to cryptocurrencies.

Joan Daemen, "Column-parity mixing layers": Daemen's talk focused on the design of linear layer in most modern block ciphers and permutations. He talked about the generalization of the mixing layer in Keccak-f, the permutation underlying the NIST standard SHA-3 and the authenticated encryption schemes Keyak and Ketje. He also talked about their algebraic and diffusion properties and implementation cost.

[1] http://people.uib.no/chunlei.li/workshops/lofoten/index.html#workshop

Then he presented a new 256-bit permutation with strong bounds for differential and linear trails.

Christian Rechberger, “Rasta and Picnic: Christian Rechberger’s talk was about the recent developments in the area of design, analysis, and applications of primitives in symmetric cryptography with few multiplications. He presented ’Rasta’, a design with an AND-depth of 2 (theoretical) and 4 (practical) that can be used to remove the huge ciphertext expansion in FHE schemes. He also presented ’Picnic’, a new approach to longterm-secure signature schemes relying solely on the security of symmetric primitives.

An interesting excursion also was organized in Wednesday. We had a boat tour to Trollfjorden, which was very nice experience for me. Then we departed to Henningsvær where we visited the art gallery Lofoten.

My overall impression about MMC 2017 was nice and majority of the talks were interesting and relevant. In the end, I would like to acknowledge COINS for their support to participate me at MMC 2017.

Here is a pic of me (Navid), Andrea and Irene from COINS Research School:

Figure 1: Irene (UiB), Andrea (UiB), and Me (Navid (UiB)) from COINS Research School at MMC 2017 workshop, Lofoten, Norway.