NISK 2018

Andrea Tenti's report for COINS research School

Longyearbyen. September 18-20, 2018

Between the 18th and the 20th of September I took part to the COINS Ph.D. seminar and to the *Norwegian Information Security Conference* (NISK) conference held in Longyearbyen supported by COINS. The conference NISK was part of a series of conferences held at the same time, called *Norwegian ICT conference for research and education 2018*, organized by the University of Oslo. The complete program description can be found at `http://nikt2018.ifi.uio.no/program_overview_en.html`.

The first day of our staying in Svalbard was dedicated to the COINS Ph.D. seminar, which consisted in several presentations by COINS students. Most of them regarded their research, while other were summaries of Ph.D. experiences from alumni about life during and after a Ph.D. Particularly relevant in this category I have found Bo Sun's presentation. As always, with COINS seminars, rarely the topics presented by students are closely related to my own research and they are, therefore, an amazing opportunity to broaden the spectrum of my knowledge of the broad field of secure communications.

I should notice that I took part to the first hour of the Workshop called *Student active-learning and project work in the development of IT systems*, which offered me some insight on some precious practises that teacher can adopt when they design courses. Unfortunately the language chosen was Norwegian and after the first presentation, the participants were asked to interact, something that I am not particularly confident at the moment.

Day two was dedicated to Cryptographic primitives and, cryptographic protocols and security analysis. The last was the single session I was most interested in. Of particular note have been:

- Martha Norberg Hovds talk, titled *A successful subfield lattice attack on a fully homomorphic encryption scheme*,
- Slobodan Petrovic's talk, titled *Improving the generalized correlation attack against stream ciphers by using bit.*

The third day of presentations was the one I was the least interested in, for the distance between the selected topics and my area of interest is vast. To my great surprise, the quality of the talks was extremely high and the speakers managed to keep me interested, defying my expectations. In this sense, it is worth mentioning the talks:

- *Fake chatroom profile detection*, by Patrick Bours, Parisa Reazaee Borj, and Guoqiang Li,
- *Debunking blockchain myths*, by Roman Vitenberg,
- *Towards Fingerprint Presentation Attack Detection Based on Short Wave Infrared Imaging and Spectral Signatures*, by Marta Gomez-Barrero, Jascha Kolberg, and Christoph Busch.

The experience has been, overall, important for my growth as a researcher, both for the breadth of the selected topics and for the opportunity to strengthen my network with fellow researchers who work in Norway. I am, therefore, grateful to COINS for the economic support provided.