Norwegian Information Security Conference

Canales-Martínez, Isaac Andrés

September 18-20, 2018
Longyearbyen, Svalbard, Norway

In September 2018, COINS supported me to attend the "Norwegian ICT conference for research and education 2018". This event took place during 18-20 September 2018 in Longyearbyen, Svalbard, Norway. The Norwegian ICT conference was organized by the University of Oslo as a joint conference consisting of:

- Norwegian Informatics Conference (NIK),
- Norwegian Conference for Organizations' Use of IT (NOKOBIT),
- Norwegian Information Security Conference (NISK), and
- Norwegian Conference for Education and Didactics in IT subjects (UDIT).

From these, NISK was the conference that I attended given that its main topics were cryptography, security and privacy.

This conference served as a meeting point for researchers and students of cryptography and security who work in both, theoretical and applied aspects of these disciplines. The full program of the conference can be found in the event web-page: `http://nikt2018.ifi.uio.no/program_nisk_en.html`. Broadly, the organisation of the conference was as follows:

- During the first day, cryptographic primitives, cryptographic protocols and security analysis were the main topics.
- Day 2 focused on biometrics and malware.

Also, both days presented the opportunity to attend plenary talks that were aimed at participant of all four conferences. The first talk was titled "Learning Analytics: What is it and what is its role in education?", and the talk on the second day was "Developing for the long term - Lessons learned through

20 years of Qt". I found particularly interesting to have a talk on Qt, which is a very popular open-source application framework for creating graphical user interfaces, because it was created here in Scandinavia.

My research is focused on algebraic and statistical analysis of ciphers, but I am interested on different aspects of cryptography and mathematical cryptography. The talks that I found most useful and content-relevant were:

- "Improving the generalized correlation attack against stream ciphers by using bit" by Slobodan Petrovic,
- "A Successful Subfield Lattice Attack on a Fully Homomorphic Encryption Scheme" by Martha Norberg Hovd, and
- "Distributed Personal Password Repository using Secret Sharing" by Merete Elle, Stig Frode Mjølsnes and Ruxandra F. Olimid.

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

- "Fake Chatroom Profile Detection" by Patrick Bours, Parisa Rezaee Borj and Guoqiang Li,
- "Debunking blockchain myths" by Roman Vitenberg,
- "The tension between anonymity and privacy" by Staal Vinterbo,
- "Source Code Patterns of Cross Site Scripting in PHP" by Felix Schuckert, Max Hildner, Basel Katt and Hanno Langweg, and
- "Comparing Open Source Search Engine Functionality, Efficiency and Effectiveness with Respect to Digital Forensic Search" by Joachim Hansen, Andrii Shalaginov, Kyle Porter and Katrin Franke.

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, security and privacy. 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. Particularly, this conference included a bus trip within Longyearbyen and the surrounding areas, as well as a particular dinner in a camp outside of the city. This was definitely an amazing experience!

I finalise this report thanking COINS for having supported me to attend to NISK 2018.