Travel report for ArcticCrypt 2016

Stian Fauskanger

October, 2016

I got funding from COINS research school to attend ArcticCrypt 2016 in Longyearbyen, Svalbard, in July 2016. ArcticCrypt 2016 was organized by Tor Helleseth (University of Bergen), Bart Preneel (University of Leuven) and Øyvind Ytrehus (University of Bergen, simula@uib). It was a 5 day program with one full day booked for an excursion by boat.

1 Socially

Several of my colleagues and I went to Svalbard 2 days before the workshop started to help the organizers get set up, and to get som enjoy some of the possible activites in the arctic desert. We got to rent ATVs, go fossil hunting at the end of the glacier, and we got to take a ride on a "dog-sledge" with wheels. All this before the conference even started.

None of the participants from Bergen that came to Svalbard the same day as me got their luggage, which was stuck in Oslo. Because of heavy fog no more airplaines could land for a while which lead to several people being delayed, and for our luggage to be stuck in Oslo for even longer.

The organizers of ArcticCrypt had booked a full day excursion to a

Russion city called Pyramiden. We went there by boat, where we got to see some whales, birds and very nice nature. The attached photo is taken onboard this boat. Pyramiden was abandoned in 1998, and was empty for 9 year. There are now around 30 workers at a hotel there, but there are very few permanent residents.

2 Academically

ArcticCrypt 2016 was located at Radisson Blu Polar Hotel, Spitsbergen. The program can be found at
`http://arcticcrypt.b.uib.no/program`.

The program at Svalbard was very good. In addition to the good accepted speakers, there were several "great names" among the invited speakers which had very interesting presentations. The presentations that I liked the most was

- "How Can Drunk Cryptographers Locate Polar Bears", Invited Talk by Adi Shamir.
- "Generic security of full-state keyed duplex", Invited Talk by Joan Daemen.
- "NTRU Prime", Invited Talk by Dan Bernstein.

Shamir's presentation was the one most relevant to my Ph.D. project where he talked about "finding the needle in the haystack", for example finding a specific key among a large set of possible keys. Part of my my Ph.D. project is to generalize linear cryptanalysis, where we do exactly that.

It's also very nice to meet Ph.D. students and researchers from other universities, both in Norway and in other countries. I felt that ArcticCrypt was a very social workshop (compared to the few other conferences I'v been to). Longyearbyen is such a small place with so few

hotells so that you meet the other participants all the time.

All in all ArcticCrypt was an very good week both socially and academically, and I'm grateful for COINS' support to go there.