Travel report from ISC15

Martin Strand, martin.strand@math.ntnu.no

For a good overview over the the scientific content at the conference, I refer to Tetiana Yarygina's report. My occupation during the conference was to help the organisers, Colin Boyd and Danilo Gligoroski. This also results in a somewhat short report.

My primary tasks were

- Transport of conference material to the venue.
- Help with registration.
- Be available for questions from the participants
- Set up the technical equipment, including connecting a computer to the hotel sound system so that we could use the microphones in the room to communicate with the speakers, and hear them through the loudspeakers.[1]
- Give information on social events in Trondheim the following weekend, and how to find transportation to the airport.
- Assist Colin and Danilo with anything unforseen.

In sum, the days at ISC gave me useful insight into how to organise a scientific conference and handle any challenges that might suddenly arise.

Scientific input

I also tried to attend some of the talks. Admittedly, only a few were relevant to my work in fully homomorphic encryption (FHE). The best exception was Massimo Chenal's preentation of his and Tang's paper "Key Recovery Attacks against NTRU-based Somewhat Homomorphic Encryption Schemes", which completes a series of work to show that hardly any of today's SHE schemes are CCA1-secure. (It is a very easy argument to show that none can be CCA2-secure, and the only known technique today for achieving FHE from SHE will by design break any CCA1 security.)

I had been looking forward to a presentation of "Leveled Strongly-Unforgeable Identity-Based Fully Homomorphic Signatures" by Wang, Wang, Li and Gao. Unfortunately, this talk was cancelled as no speaker turned up.

On the social side, I'd particulary like to mention the very enjoyable evening together with the other COINS members. That was the sort of networking that may become useful further down the road.

[1] However, there were no questions to any of the remote talks, so the microphone setup was technically nice and a good learning experience, but strictly speaking not necessary