Trip Report Norsk Kryptoseminar 2020

Morten Øygarden, PhD-Student SimulaUiB

Overview

This is a trip report for the COINS Research School of Computer and Information Security, which supported my travel expenditure to Norsk Kryptoseminar (NKS) 2020. NKS 2020 took place on the 30th of January 2020, in Kjeller, and has been held irregularly since 1998. The event aims to gather cryptographers from academia, industry and governmental organizations in Norway, and includes a day of presentations, followed by a social dinner.

After briefly describing the logistics of the trip, I will describe some of (what I found to be) the highlights of the presentations. Finally, I will conclude with some overall thoughts on the seminar.

Logistics

I took the night train from Bergen to Oslo, arriving at Oslo central station in the early hours of the 30th of January. From there, I boarded the local train to Lillestrøm, and took the bus to Kjeller. After the event, I slept over at a friend's house, and took the train from Lillestrøm to Bergen on the 31st of January.

Highlights from the presentations

- After initial introductions, the first presentation was held by Thomas Gregersen from the Norwegian National Security Authority (NSM). Gregersen started his talk about how the cryptographic community in Norway has developed from the second world war, up to this day. It is a rich history, including a cooperation between Defence and industry which has provided several cryptographic devices for communication in the NATO alliance. This community has also played a key role in the establishment of related mathematical groups in Norwegian academia.

  The later parts of the presentation centered around the current tasks of NSM, as well as what they intend to focus on in the future. On the theoretic side, much of their work has been on the analysis and development of symmetric ciphers. They are currently also looking into asymmetric cryptography, a field which has received increasing global attention due to the potential advent of large-scale quantum computers. The latter area is also very close to my own heart, and will be discussed further in the last presentation session.

- Next session consisted of two industry talks. Yiorgis Gozadinos held the first talk named "Crypto for the Commoners", about their company Crypho. Crypho provides a communications app that is especially aimed at companies and departments where information security and privacy are particularly important.

  The second talk, "Kryptografi på satellitter", was held by Einar Andreas Øvreness from Eidel. Eidel focuses on products related to Defence, space and telemetry, and Øverness talked about the challenges that arise in this setting.

- The third session was an orientation from the research institutes: NTNU, Simula UiB and FFI. To me, it was particularly interesting to learn more about what projects the other research institutes (NTNU and FFI) are working on, as well as what kind of research ares they are intersted in.

- The last sessions of the seminar consisted of presentations by PhD Students. I will briefly focus on the very last session about post–quantum cryptography, which include the majority of my own research interests. The motivation is that large–scale quantum computers are expected to break the asymmetric cryptography in use today. Post–quantum cryptography is the study of primitives and protocols that will remain secure against this potential threat.

  Mattia Veroni presented the mathematical problems that are typically used to construct primitives in the post–quantum setting. Lise Millerjord presented 'Picnic', one of the signature algorithms that is currently being evaluated for standardization. Bor de Kock discussed topics related to post–quantum key exchange, and Tjerand Silde presented a scheme for post–quantum E–voting. Finally, my own presentation focused on algebraic techniques that are relevant to certain post–quantum schemes.

Concluding Thoughts

In my opinion, NKS succeeded in providing a good overview of the Norwegian cryptographic community. It is always interesting to have an idea of the interests among the different institutions and departments. I was particularly happy about the wide interest in post–quantum security, and find it useful to my own work to have an idea of what "local" expertise there is in this direction.

There was also ample of opportunities for further discussion among the participants in the lunch– and coffee–breaks, as well as the dinner in the evening. I hope to be able to attend another year.