NORSK KRYPTOSEMINAR 2020

Trip report by Bor de Kock, Lise Millerjord, Magnus Ringerud,
Tjerand Silde, Morten Solberg, Thor Tunge, Mattia Veroni

January 30th, 2020
Kunnskapsbyens hus, Kjeller

Introduction

The Norsk Kryptoseminar (Norwegian Crypto Seminar) has been organised on a non-regular basis since 1998, with the aim to promote theory and applications of cryptography in Norway. The seminar is open to everyone who works with cryptology in Norway, both in academia, research centers and industry.
The seminar was organised by Tjerand Silde (NTNU), Kristian Gjøsteen (NTNU) and Martin Strand (FFI). The full programme, slides and further details can be found at https://wiki.math.ntnu.no/nks/nks20.

The travel

There are two ways to travel from Trondheim to Kjeller: by plane from Værnes to Gardermoen and continue by train, or directly by train from Trondheim Sentralstasjon to Lillestrøm, at walking distance from Kjeller. In order to keep our carbon footprint as low as possible, the seven of us agreed to take the night train from Trondheim to Lillestrøm. We also took the night train back to Trondheim after the seminar. The train ride was the most time-efficient solution, although not the most comfortable for those who are not used to sleeping on trains.

The seminar

The seminar opened with registration at 9:00 and ended around 16:00. After a short introduction from the organisers, we had three sessions: the first one with talks from NSM and industry, then we had an orientation session from the research centers, and the last one with presentations from all the attending PhD students.

Invited talk:

- "Nasjonal kryptografi i dag og i fremtiden" - *Thomas Gregersen, NSM*
  Thomas Gregersen is a researcher at Nasjonal Sikkerhetsmyndighet (NSM) focusing on cryptography. The national security agency has traditionally focused mostly on symmetric key cryptography, and he gave us an overview over the past 80 years of cryptographic work and research in Norway. Nowadays they also closely follow the development of post-quantum cryptography and the standardization process from NIST,

and NSM have several researchers focusing on the ongoing research and cryptanalysis of e.g. lattice-based key-exchange and code-based signatures.

Industry talks:

- "Crypto for the Commoners" - *Yiorgis Gozadinos (Crypho)*
  Yiorgis is one of the two founders of Crypho, a service for messaging and chat, available both in the desktop and app version. With the most desirable features for messaging, calling and file sharing, it aims to guarantee top-level security without compromising a user-friendly experience. It was a very interesting insight in the planning and realisation of a daily-use application deploying different cryptographic tools such as SCRYPT, AES, ElGamal and MPC protocols.

- “Kryptografi på satellitter” - *Einar Andreas Øvreness (Eidel)*
  Einar gave an overview of the different working areas of Eidel, who provide cryptographic systems for all kinds of applications. The more in-depth focus on the talk was deploying cryptography for satellite-communication, thus actually running cryptographic code on space-grade hardware. The challenges that come with this are naturally different than with ordinary cryptosystems, both in terms of actual hardware/software requirements, as well as upgradeability and maintainability.

Orientation from the research institutions:

- NTNU - Kristian Gjøsteen
- Simula UiB - Øyvind Ytrehus
- FFI - Jan Henrik Wiik

Student presentations:

- "Formal Verification of Cryptographic Voting Schemes" - *Morten Solberg (NTNU)*
  Morten is currently working on security proofs and formal verification of such proofs, for electronic voting protocols. Morten began his presentation with some motivational words regarding why e-voting is interesting. Furthermore, he described how formally modelling and verifying the security of voting protocols may increase the trust in the pen-and-paper security proofs. Finally, Morten said a few words about the proof assistant EasyCrypt, and his current work, namely proving and verifying ballot privacy of Selene.

- "Formal Treatment of Practical Signature Schemes" - *Magnus Ringerud (NTNU)*
  Magnus is working on security reductions from single to multi-user security for signature schemes obtained from a specific transformation. He started by talking about the motivation for doing this, which is to construct a scheme that is secure in the multi-user setting, with security based on a search assumption instead of a decision assumption. He then presented a scheme which has the desired properties in the programmable random oracle model, and talked briefly about the next step, which is to construct a scheme with the same properties in the standard model.

- "The Wiretap Channel" - *Thor Tunge (NTNU)*
  This was a talk aimed to give an introduction to a different way of doing cryptography, namely using the wiretap channel. By assuming that the channel between honest parties is less noisy than the eavesdropped (or wiretapped) channel, the honest parties can leverage this to exchange messages in secrecy. Thor wanted to define security for a key exchange scheme in the wiretap channel, and build a framework for a more cryptographic view of schemes using the wiretap channel.

- "Hybrid Encryption in a Multi-User Setting" - *Hans Heum (Simula UiB)*
  Hans opened his presentation talking about his research interests. First, he briefly discussed provable security: how to construct an adversary and the game-based structure. He then compared asymptotic security with concrete security, the latter of which allows us to choose exact parameters which guarantee a target security level. He then posed the following question: if we let the adversary attack any of n systems, how does that affect the security of the rest? The last part of his talk was about his actual research work, which focuses on hybrid systems of key encapsulation and decapsulation mechanisms to build public-key encryption schemes.

- "Post-Quantum Primitives" - *Mattia Veroni (NTNU)*
  This was the first of 4 talks on Post-Quantum Cryptography, and as such it was meant to be an introduction to the field of Post-Quantum cryptography. Mattia started his talk discussing the current security offered by classical security, showing then how the quantum menace will threaten it. In the second part of the presentation he introduced the five families of Post-Quantum candidates to the NIST's Post-Quantum Standardization process. For each of them he briefly discussed the underlying mathematical problem, underlining strengths and weaknesses of each category.

- "Post-Quantum Signatures" - *Lise Millerjord (NTNU)*
  Lise is currently working on post-quantum secure signature schemes and key exchange for lightweight applications. The topic of this talk was an introduction to the post-quantum signature scheme Picnic, which is a candidate in the NIST Post-Quantum Standardization process. The talk introduced the different components that make up the system and its security reduction to the symmetric cryptographic primitive of choice. The design choices made were discussed including the reasons for choosing LowMC as the symmetric encryption primitive, and the design of ZKBoo, which is the zero knowledge proof used. In the end, the way these components are put together to form Picnic was shown and some research questions were posed regarding the design choices and the security models that are employed.

- "Post-Quantum Key-Exchange" - *Bor de Kock (NTNU)*
  The talk was about lesser-researched topics that apply or modify key exchange in some way, pitching the speaker's research interests. These are all topics that are not that

well-researched in pre-quantum crypto, and even lesser so in the post-quantum scenario. An overview was given for Password-Authenticated Key Exchange, Secure Remote Password and for Group-Diffie Hellman, giving both an example of a pre-quantum and a post-quantum solution for those.

- "Post-Quantum E-Voting" - *Tjerand Silde (NTNU)*
  Tjerand is aiming to design new post-quantum protocols, especially focusing on lattice-based zero-knowledge proofs. This talk was about a new paper presenting a new post-quantum e-voting scheme that can handle complex ballots (not only yes/not-votes). It is based on lattice-based commitments, and the heart of the scheme is a protocol to verifiably shuffle a set of commitments. Given two sets of commitments, we use the protocol to prove that the sets contain the same underlying set of votes, where the order of the votes in the second set is in a secret permuted order of the first set. This makes it possible to achieve both privacy and integrity of the votes submitted to an election, as we break the connection between the voter and his vote when we shuffle all the votes.

- "Algebraic Attacks in Post-Quantum Cryptography" - *Morten Øygarden (Simula UiB)*
  Morten started his talk with an introduction to systems of quadratic polynomials over finite fields, which are the basis for multivariate public-key cryptosystems deployed both in pre- and post-quantum cryptography. He then discussed the construction of Big-Field multivariate schemes for encryption and signature, highlighting some of their weaknesses. After mentioning some algebraically simple symmetric ciphers introduced in the last decade, he concluded his presentation talking about Rank-Metric code based encryption schemes, showing their vulnerability to Gröbner basis attacks.

Conclusion

The Norsk Kryptoseminar has been a forming and informing experience we all enjoyed. The quality of the talks was high and we had the opportunity to talk with some representatives of other research centers and businesses in Norway. We all hope that this seminar will be organised on a yearly basis.