Калининград Summerschool Euclidian Lattices

COINS Trip Report

Bor de Kock

Norwegian University of Science and Technology, Тронхейм

August 5, 2019

1 Introduction

Together with my colleague Thor Tunge I participated the Summerschool *Euclidian Lattices: Theory and Applications* which took place in Kaliningrad, Russia from the 15th to the 19th of July. The summerschool was organized primarily by Elena Kirshanova, Ekaterina Malygina and Semen Novoselov from the БФУ им. И. Канта, aka Immanuel Kant Baltic Federal University.

The summerschool is an official IACR-supported venue and we were glad to obtain funding from the COINS Research School to facilitate our participation in the event.

2 Russian Adventures

The fact that the summerschool took place in Russia caused some extra logistic challenges for us, for example that we needed to obtain a visa for the Russian Federation: this involved getting an official invitation letter from БФУ, which took longer than expected, and then delivering our passports to a Russian embassy (in Oslo) or consulate (in Kirkenes or Svalbard). In the end this could luckily be done via mail. We got back our passports in time with a few days to spare.

Thor and I both visited Russia for the first time. To enhance the authenticity of the experience we chose to rent an apartment in a soviet-era block near the university instead of opting for a more western hotel chain, and we took some extra days in town to go sightseeing and exploring. Listing Kaliningrad sights is mildly out of scope for this report, but it should be mentioned that we paid a visit to the birthplace of graph theory by walking the remaining two bridges from Euler's *Seven Bridges of Königsberg*. Additionally an excursion to the *Curonian Spit* was planned by the organizers, which was a very nice experience.

Per NTNU policy (and government advice) it is not allowed to take our normal laptops to Russia — to be able to do the Sage exercises we took a burner laptop which was wiped before the visit as well as afterwards.

3 The Summerschool

Compared to the other summerschools I visited, this one was the most school-like. The two lecturers — Alexander May and Damien Stehlé — each gave a 1.5-hour blackboard-style lecture every day in the morning. Most afternoons were then dedicated to classical instruction sessions were problems

related to the lectures were solved individually or in groups, and the correct solutions were shared on the blackboard.

The lectures by Stehlé closely followed the theme of the school, namely lattices, lattice problems, reduction and enumeration techniques and so on. May focussed more on the representation technique and how it can be used to solve problems like discrete log, Subset-sum and decoding.

A more concrete overview of the school content:

	Alexander May	**Damien Stehlé**
mo.	Introduction into representations. Using a Meet-in-the-Middle approach for the normal DLP (decomposing x), for small-weight, faulty or multiple DLP.	Introduction into lattices with mostly definitions, invariants, problems, kissing numbers and Minkovski's theorem.
tu.	Collision finding and cycle finding, using this 'rho-method' for DLP and for Subset-sum problems.	Lattice reductions using Lenstra / Lenstra / Lovász (LLL) and Block / Korkine / Zolotarev (BKZ), Gram-Schmith orthogonalization.
we.	Paralellized collision search (Wiener / Van Oorschot) for multiple-DLP, DLP as a Subset-sum problem, the Schoeppel-Shamir, 0.75 and Becker / Coron / Jony algorithms	Lattice enumerations and the SIS problem (Ajtai '96).
th.	A Subset-sum algorithm using Schoeppel / Shamir, the Howgrave / Joux algorithm, decoding McEliece.	Reductions between different lattice problems, collision-resistant hashing, Schnorr-signatures, SWIFFT.
fr.	Closing overview *recent advances in decoding random binary linear codes* and on the implications of quantum computers for cryptography.	The LWE-problem and the implications of lattice reductions as an attack mechanism, Arora-Ge attack.

4 Other

The Friday afternoon was used for a poster session in which several of the participants shared recent research. It was interesting to see how big the difference was between the work, from very cryptographic up until lattices in coding theory. Although the summer school did not have a dedicated venue where everyone had to stay, there was a lot of social interaction between the different participants. Some people took the initiative to get all these smaller groups together for an unofficial summer school dinner on Thursday that was a great opportunity for getting to know even more of the participants (but made us happy the Friday lectures were not very heavy in terms of new material).

5 Evaluation

The summer school was a great week both in terms of speakers and socially. Although I was initially a bit disappointed that the topic was less about lattice attacks (and lattices in general) than I had hoped I learned a lot. Additionally it was a good way of getting to know researchers in the field and areas related to it, and of course also to make new friends and visit a new country. A big thanks goes to the organizers in Kaliningrad, the fellow participants and of course to COINS for making the trip financially possible.