EUROCRYPT 2019 Darmstadt
COINS Trip Report

Bor de Kock
Norwegian University of Science and Technology, Trondheim

June 14, 2019

1 Introduction

I was lucky to obtain funding from the COINS Research School for attending the 2019 EUROCRYPT conference, which took place in Darmstadt, Germany this year from the 19th to the 23rd of May this year, with some affiliated events in the weekend before. We attended the event with the majority of the NaCl group — NTNUs Applied Cryptography Lab — and for me it was the first conference to attend since starting my PhD studies at NTNU.

2 Affiliated event: SPY (Security, Privacy and You)

On the Sunday before EUROCRYPT started I attended the SPY workshop, which was hosted by Dan Bernstein, Jean Paul Degabriele, Tanja Lange and Sogol Mazaheri. The workshop theme was in line with the *Security in Times of Surveillance* symposium series Lange and Bernstein have hosted at the Eindhoven University of Technology in previous years, and the set-up was similar: talks from a broad perspective with views on not only the technical side of security research and the development of secure systems for the internet, but also the societal impact the information age has and the way research could and should influence the way we live our lives.

To highlight one of the seven talks: Orr Dunkelman's *Hunting Political Bots on Twitter – Joining Captain Ahab* took place very much on the intersection of these different themes, explaining the way fake twitter accounts has influenced the political discourse in Israel over previous years. He managed to dive into the numbers and the 'how', while also managing to explain the links to the complicated political situation in Isreal (but somehow without making the talk too intense).

3 The conference itself

The conference itself consisted of 12 sessions with parallel paper presentations, and a few plenary talks: the winners of the best paper awards, the Distinguished Lecture, a few distinguished speakers and the general IACR events like the members' meeting and the fellows ceremony.

Three personal highlights from the talks we saw, in no particular order:

- *Minicrypt Primitives with Algebraic Structure and Applications* (Navid Alamati, Hart Montgomery, Sikhar Patranabis and Arnab Roy)

This work was particularly interesting to me because it shows on an abstract level which kinds of cryptosystems you can make based on sets of assumptions. Some of the relations they showed were intuitive, others weren't, but overall it was nice to be introduced into the Cryptomania and Minicrypt concepts using concreter examples.

- *The General Sieve Kernel and New Records in Lattice Reduction* (Martin R. Albrecht, Léo Ducas, Gottfried Herold, Elena Kirshanov, Eamonn W. Postlethwaite and Marc Stevens)

  I have been reading a lot about cryptanalysis using lattices, but it is hard to get a good grasp on what exactly is happening "under the hood" when reducing. The talk was a good high-level overview about new techniques for lattice sieving while being technical enough to trigger new insights. Aditionally, while I was aware of the G6K framework I wasn't aware yet that it is pronounced essentially like *Jessica*.

- *Misuse Attacks on Post-quantum Cryptosystems* (Ciprian Băetu, F. Betül Durak, Loïs Huguenin-Dumittan, Abdullah Talayhan, Serge Vaudenay)

  This kind of "practical" cryptanalysis (i.e. the kind of attacks that make a more "real-world" set of assumptions about protocols) is very nice to read. I like that there is room in the cryptographic field to be busy not only with mathematical primitives, proofs and assumptions, but also with the more concrete questions about what would happen in the real world. Really nice work.

4 Other

Since this was my first conference since I moved to Norway in October, the conference and its reception, rump session and conference dinner were a nice occasion to reunion with people I hadn't seen in a while, including my old group and MSc advisor from Eindhoven, the supervisor from my exchange semester to the US and some people from a summer school two years ago with whom I failed to stay in touch. I also met quite some new people from other places in the world and hope to get some cooperation with them going in the years to come.

The conference itself was well-organized, and the full schedule of talks and social events made the four days feel like a significantly longer period of time. For the group from Trondheim this was also the moment we officially heard that we will be hosting EUROCRYPT 2021, which is of course a very exciting development.

5 Evaluation

Attending EUROCRYPT 2019 was a very nice experience: I networked with a lot of interesting people I knew, got to know a lot of others and although a lot of information comes your way in a short period of time I feel like I learned a lot as well, both in 'my own' area of cryptography as well as all kinds of related fields I did not know a lot about beforehand. Talks are of course short, but I returned home after the conference with a long list of "papers I should definitely read when I find the time". I am grateful to the COINS research school for providing us the opportunity to attend such an event and am sure I will be able to use the experiences from this week to further myself and my research.