Report for School in Malaga

Dan Zhang
Department of Informatics
University of Bergen
Bergen, Norway
Dan.Zhang@uib.no

1 Information about the summer school

The School on applied cryptography and its impact on society, innovation and entrepreneurship was organised by the ECRYPT-NET Research Network and took place on 5-8 February, 2019 in Malaga, Spain.

The school focused on novel and advanced applications of cryptography and discussed the impact of crypto research to society in a broader context. There were also lectures on good practices of innovation in cryptography and entrepreneurship as well as certification and standardisation of cryptographic primitives.

Since this was the last event of the ECRYPT-NET, the fellows from the network presented the research they had been performing during the last 3 years and to reflect on their experience and future opportunities.

More information about the summer school, including a detailed program and a full list of mini courses and talks, can be found on the summer school's official website at https://www.cosic.esat.kuleuven.be/events/ecrypt-net-school-malaga2018/.

2 My experience at Malaga

The first thing that I would like to mention is that I felt much appreciation to COINS for giving me such a wonderful opportunity to freely travel for learning. I felt a great pleasure to attend the event with my COINS T-shirt, which I view as a symbol of Norway and of Norwegian universities.

The second thing worth noting is that I liked the topic of this school since it was about practical cryptography. What I learned at school is mostly about theory. I want to prepare myself with applied cryptography, which made this school perfectly match my interests.

Besides, I also had a good time in Malaga. I enjoyed myself at the city. Always bright sunshine, wonderful views and pleasant temperature made me feel great here.

3 Some outcomes from the summer school

The school started with presentations from ESR Fellows, which is about the research they had done during the last three years. The first one is about zero-correlation attacks on tweakable block ciphers with linear tweakey expansion, which is currently best attack on QARMA and independent of keyed middle rounds.

The second speaker is Chaoyun Li, from KU Leuven. His talk was about new methods for analysis and design of symmetric key primitives. He talked about cryptanalysis of symmetric key primitives with low algebraic degree, after which he presented designs of lightweight linear layers for block ciphers and authenticated encryption algorithms.

Another interesting talk was from Junwei Wang, University of Paris 8. His talk was about gray-box attack against white-box implementations, which was quite interesting. There were some other topics that I was really interested in. For instance, Dusan Bozilov's talk, which was about lightweight block ciphers resisting combined side-channel and fault attacks.

After these research reports, we had several talks about the relationship between theoretical cryptography and applied cryptography and how to build a bridge between them. Apart from this, we were taught how to build a startup and teamed up to do business opportunity plan exercise.


Malagueta