Reflection report for
ECRYPT-NET School on Applied Cryptography and its Impact on Society, Innovation and Entrepreneurship

Irene Villa

5 - 8 February 2019
Malaga, Spain

From the 5th to the 8th of February the ECRYPT-NET School on Applied Cryptography and its Impact on Society, Innovation and Entrepreneurship took place in Malaga, beautiful city in the south of Spain. This was one of the events organized by ECRYPT-NET, a research network of six universities and two companies, and seven associated companies. This network, focused on developing advanced cryptographic techniques for the Internet of Things and the Cloud and creating efficient and secure implementations of those techniques on a broad range of platforms, educated a group of 15 PhD students. Since the School in Malaga was the last event for ECRYPT-NET, some of the fellows from the network had the opportunity to present the research during the last 3 years.

On the first day of the school, the presentations of the PhD students took place. They presented briefly their researches. In the following a list of the topics covered.

- Advanced Methods for Symmetric Cryptanalysis,
- Cryptography for Passively-Powered Devices,
- Fully Homomorphic Encryption,
- Design and Analysis of Efficient and Lightweight Authenticated Encryption Schemes,
- Multiparty Computation based on Homomorphic Encryption and Oblivious Transfer,
- Leakage Resilience from Lattices,
- White-box cryptography: attack techniques and secure constructions,
- Lightweight ciphers resisting combined side-channel and fault attacks.

In the following days, many different speakers gave a talk, particularly focused on innovation in cryptography and entrepreneurship.

Harry Halpin, a visiting researcher at Inria de Paris, talked about *How to build a cryptocurrency startup from academic research.* Pascal Paillier, CEO at CryptoExperts, gave a talked on *Cryptography at a global scale: an entrepreneurial experience.* Mihaela Ion, software engineer at Google, presented *Privacy Preserving Analytics via MPC.* Nigel Smart, professor at COSIC in Leuven, talked about *Turning MPC from theory into product.* Robin Ankele, Co-founder and CTO at Aufido, gave a talk on *Aufido - Insights from an early stage cryptography startup.* Karel Wouters, Information Security Officer at Bancontact Company, talked about *Cryptography used in (card) payments.* Willi Mannheims, Managing Partner at eCAPITAL entrepreneurial Partners AG, gave a talk on *Venture Capital in Cyber Security, our Cybersecurity Fonds and Entrepreneurship case studies.*

The last day and half of school we were divided in groups and, taking inspiration and tips from the talks we attended, we had to come up with a plan for a business opportunity. We had to find an idea, related to cryptography, and transform it into a business.

This last part of the event was really interesting because it highlighted the fact that just a good idea is not enough. Indeed many other questions have to be answered. Some of them are:

- is it possible to transform your idea into something practical?
- is the marked interested in your idea?
- who are your competitors?
- can you sell your product to investors?

At the end of the school the groups had to present plans as if they were presented their business in front of potential investors. I am proud to say that my group, even if it did not win, was mention as the one with the best idea, but not developed enough.

I am very grateful to COINS that gave me the opportunity to attend this interesting event.