A Reflection Report for Attendance at Symmetric Cryptography and Blockchain School

February (19-23), 2018, Torremolinos, Spain

Navid Ghaedi Bardeh

University of Bergen

Symmetric Cryptography and Blockchain School was organized by COSIC- KU leuven in February 2018. I got funding from COINS research school to attend this school. The school aim was to give students a thorough introduction to the state-of-the-art within symmetric cryptology covering both the theoretical side (design and cryptanalysis of symmetric cryptographic primitives and provable security) and the practical side (practical cryptanalysis in exercise sessions).

Full program of the school, as well as presentation slides can be downloaded from the webpage of the program[1]. The following is a short summary of some talks.

The first lecture in school was "Introduction to Symmetric Cryptography " given by Stefan Kölbl. He gave us a brief description of Symmetric Cryptography especially Block ciphers. Usually block cipher takes n bits plaintext and k bits key as input and give n bits ciphertext as output. A block cipher can be seen as a family of 2^k n-bit bijections. Then he explained the specification of DES and AES, which are two famous block ciphers. Then he explained in details differential and linear cryptanalysis which are two strong attacks against block ciphers and some ciphers were broken by these two techniques. We also tried to partially implement these techniques with some programming.

In the second day, Anne Canteaut gave an interesting lecture on "Exploiting algebraic properties of block ciphers". She explained how one could compute Algebraic Normal Form (ANF) of S-box and how ANF of random function looks like. Then she explained higher- order differential attack and it's complexity then explained in detail how one could compute the degree of iterated block cipher over several rounds. She gave us several examples and at the end she showed how we could mount this attack against a specific block cipher.

[1] https://www.cosic.esat.kuleuven.be/events/cost-school-symmetric-cryptography-blockchain/programme/

The most interesting lecture for me was “How Not to Use a Block cipher ” given by Gaëtan Leurent. This lecture was interesting for me because I always heard about how we can use block cipher. At first, he gave some basic concepts of block cipher. Then he explained in detail the following ways which one should aware to not use block ciphers:

- No mode of operation (or ECB)
- Repeated nonces
- Pridectible IVs (CBC)
- Metadata leaks information
- Encryption without authentication
- Padding oracles
- Methadata not authentication
- Too much data with the same key

Christian Rechberger gave a lecture on “Symmetric Cryptography for New Applications”. Symmetric cryptography primitives are needed in recent practical applications of secure multi-party computation (MPC), fully homomorphic encryption (FHE), and zero-knowledge proofs (ZK). During the lecture, he explained design criterions for these primitives.

Bart Mennink gave a lecture on “Security of Authenticated Encryption Modes ”. He gave a short introduction of authenticated encryption (AE) then he talked about the recent competition in this topic, Competition for Authenticated Encryption: Security, Applicability, and Robustness (CAESAR competition). Then he explained a generic composition to construct AE which first data is encrypted (E) then apply MAC (M). There is 3 basic approaches to achieve this, E&M, MtE and EtM. He also explained Tweakable Block ciphers and showed how one could use this in some basic constructions of symmetric cryptography.

All in all, this school was a very nice event, which really interested me on especially modes operation of block cipher. I am deeply grateful for COINS supporting me to attend to Symmetric Cryptography and Blockchain.