A Reflection Report for Attendance at Eurocrypt 2019 Conference

May (19-23), 2019, Darmstadt (Germany)

Navid Ghaedi Bardeh

University of Bergen

Eurocrypt 2019 is the 38th Annual International Conference on the Theory and Applications of Cryptographic Techniques. Eurocrypt is one of the three flagship conferences of the International Association for Cryptologic Research (IACR).

Eurocrypt 2019 took place in Darmstadt, Germany on May 19-23 2019. It is organized by the Cryptoplexity group of TU Darmstadt. I got funding from COINS research school to attend Eurocrypt 2019 in Darmstadt, Germany on May 19-23, 2019.

Full program of the Conference, as well as presentation slides can be downloaded from the webpage of the program[1].

The sessions in the first day were most relevant to me. In the morning, there were two parallel tracks: Obfuscation and Block ciphers. I attended to Block ciphers track since my research topic is symmetric cryptanalysis and block ciphers play a main role there. Two of talks have been extremely interesting for me:

DLCT: A New Tool for Differential-Linear Cryptanalysis by Achiya Bar-On, Orr Dunkelman, Nathan Keller and Ariel Weizman: Both linear cryptanalysis and differential cryptanalysis are the most powerful tools in the security evaluation of block ciphers. Differential-Linear Cryptanalysis is combination of these two techniques. In this paper, they focus on dependency between two subcipher and study how this dependency affects the complexity of Differential-Linear Cryptanalysis. They define a new table called the Differential-Linear Connectivity Table (DLCT) which allows to take into account the dependency between two subcipher.

Linear Equivalence of Block Ciphers with Partial Non-Linear Layers: Application to LowMC by Itai Dinur, Daniel Kales, Angela Promitzer Sebastian Ramacher, and Christian Rechberger: LowMC is a block cipher family and it is used for practical instantiations of multi-party computation, fully homomorphic encryption, and zero-knowledge proofs. In this paper, the authors present a linear equivalence of a certain LowMc instantiation.

On wendesday, the invited talk, Daniele Micciancio gave an interesting talk on "Fully Homomorphic Encryption from the Ground Up" which I found it pretty interesting

[1] https://eurocrypt.iacr.org/2019/program.html

and helped me to have a better understanding of how Fully Homomorphic Encryption are worked.

One session of last day was about Cryptanalysis which I really enjoyed. A interesting talk was about:

From Collisions to Chosen-Prefix Collisions - Application to Full SHA-1 by Gaetan Leurent and Thomas Peyrin: A collision attack on a cryptographic hash function tries to find two inputs producing the same hash value, i.e. a hash collision. A chosen-prefix collision attack is a stronger variant of a collision attack. In this paper, the authors found a chosen-prefix collision with complexity of 2^{67} encryption. The classical collision requires $2^{64.7}$ encryption. So, within a small factor, a stronger collision attack can be applied.

My overall impression about Eurocrypt 2019 was nice. During the conference I met a lot of famous professors and researchers and got change to discuss with them about my research filed and some other topics. In the end, I would like to acknowledge COINS for their support to participate me at Eurocrypt 2019.

Here is a pic of me at Eurocrypt 2019: