A Reflection Report for Attendance at Boolean Functions and their Applications (BFA) Workshop

July (3-8), 2017, OS (Norway)

Navid Ghaedi Bardeh

University of Bergen

Boolean Functions and their Applications workshop was organized by Selmer Center, university of Bergen in Os, Norway in July 2017. I got funding from COINS research school to this workshop.

The workshop aim was bringing together famous researchers who are working on discrete functions and structures, particularly on Boolean functions, to exchange ideas and interests in open problems, and to further explore their applications in cryptography, error correcting codes and communications.

It was a great opportunity to meet researchers from the common field of research. Well-known cryptographers were also lecturing, among them, Kaisa Nyberg (Aalto University), Claude Carlet (University of Paris 8).

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

Most of lectures in first day concentrated on APN functions and their property. The most interesting lecture for me in first day was "Proving resistance of a block cipher against invariant attacks " given by Anne Canteaut.
In this lecture, she explained how invariant subspace attack and nonlinear invariant attack could find a weakness property on lightweight block cipher. Usually in lightweight block cipher, key schedule is omitted and the master key is Xored to state. So it is caused to create some subspaces after each round. Linear layer and round constants of block cipher have an important role to success/fail of those attacks. Canteaut showed that how choosing a linear layer and appropriate round constants could resistant against those cipher.

In the second day, most lectures concentrated on Boolean bent functions. Boolean bent functions were first introduced by Rothaus in 1976 as an interesting combinatorial object with the important property of having the maximum Hamming

[1] http://people.uib.no/chunlei.li/workshops/BFA2017/index.html

distance to the set of all affine functions. Later the research in this area was stimulated by the significant relation to the following topics in computer science: coding theory, sequences and cryptography. In cryptography, they usually use to design of stream ciphers and S-boxes for block ciphers.

Third day was dedicated to a fjord trip. It was an opportunity to pass through some of the most beautiful landscapes in Fjord Norway. The trip comprised a fjord tour, the Bergen Railway and Flåm Railway and was Norway's most popular round trip.

In last day. Chunlei Li given an interesting talk named “On the periodic sequences with maximal nonlinear complexity ”. Pseudo-random sequences are widely used in secure and reliable communications. In cryptographic applications, security characteristics like randomness and unpredictability of the sequences must be assessed. The linear complexity is used for assessing the cryptographic strength of binary sequences used in stream ciphers.
In that talk, he explained how linear feedback shift registers (LFSR) and nonlinear feedback shift registers (NFSR) work and also explained how their complexities can be computed.

All in all, this workshop was a very nice event, which really interested me on especially APN and AB Boolean functions. It gave me a nice knowledge of about mathematic concept of basic components used in designing the symmetric primitive.

I am deeply grateful for COINS supporting me to attend to Boolean Functions and their Applications workshop.