Report for BFA 2018

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

The 3rd International Workshop on Boolean Functions and their Applications (BFA) was taken place in Loen, Norway during June 17-22, 2018. This workshop was organized by Selmer Center, University of Bergen. This workshop was to provide a forum for researchers who are working on discrete functions and structures, particularly on Boolean functions, to exchange ideas and interests in open problems, and to explore their applications in cryptography, error correcting codes and communications. More information about the BFA conference, including a detailed program and a full list of talks, can be found on the BFA's official website at https://people.uib.no/chunlei.li/workshops/BFA2018/.

First, I would like to thank COINS to support my travelling to this conference. I felt a great pleasure to attend the event with my COINS T-shit and felt much appreciation to COINS for giving me such a wonderful opportunity to freely travel for learning. The topics of BFA are very close to my research interests. So the talks and activities were very interesting for me. I will highlight some talks in the following.

The first section was about the equivalence relation of functions. The equivalence relation is important in the sense that we can generate one class of functions having the same properties by the equivalence relation. It also allows researchers to classify all the known functions into different classes. Thus, it helps researchers to claim that they find new functions with the same properties. The non-linearity and differential uniformity are important properties of a Boolean function, which are used to measure its resistance to linear and differential attacks. The CCZ-equivalence is the most general known equivalence relation of functions for which the non-linearity and the differential uniformity are invariant. Apart from the CCZ-equivalence, there are also EA-equivalence and affine equivalence. The speaker also talked about the relations among these different equivalence relations, after which classification of APN functions were discussed.

Another interesting topic is about constructions of complete permutation polynomials. Let F_q denote the finite filed with q elements. A polynomial $f(x)$ over F_q is called a complete permutation polynomial (CPP) if both $f(x)$ and $f(x)+x$ are permutations of F_q. These polynomials were introduced by Mann in the construction of orthogonal Latin squares. Niederreiter and Robinson later gave a detailed study of CPPs over finite fields. CPPs over finite fields F_q in even characteristic are the same as the orthomorphisms, which have a single fixed point and map each maximal subgroup of the additive group ofF_q half into itself and half into its complement. CPPs (or orthomorphisms) with these properties are of cryptographic interest and were firstly utilized by Mittenthal in the de- sign of nonlinear dynamic substitution device. Researchers also investigated the applications of CPPs in the Lay-Massey scheme, the block cipher SMS4, the stream cipher Loiss, the de- sign of Hash functions, quasigroups, and also in the constructions of some cryptographically strong functions. However, CPPs are rare objects and there are a limited number of known constructions. The reason why I am interested in this topic is because this is related with my own research. It is really helpful information.

It was a nice conference and I have learned something new related with my own research.